База знаний РЕД ОС

- О РЕД ОС
  - Описание программного продукта

- РЕД ОС 7.3
  - Установка РЕД ОС
    - Системные требования
    - Создание загрузочных носителей
    - Последовательность установки
    - Начало установки
    - Язык интерфейса программы установки
    - Обзор установки
    - Ручная разметка диска
    - Установка системы
    - Действия после установки ОС
    - Альтернативные способы установки
      - Общие понятия
      - Установка РЕД ОС в текстовом режиме
      - Установка РЕД ОС на программный массив RAID
        - Обзорная инструкция про RAID
        - Создание программного массива уровня RAID0 и RAID1
        - Создание программного массива уровня RAID 6
        - Создание программного массива уровня RAID 10
        - Установка РЕД ОС на программный массив RAID1 и RAID10
      - Сетевая установка РЕД ОС
        - Автоматизация развертывания (kickstart)
        - Подготовка PXE-сервера для развертывания РЕД ОС с загрузкой в UEFI или Legacy в РЕД ОС 7.3
        - Настройка установки РЕД ОС по PXE через VNC в РЕД ОС 7.3
    - Установка РЕД ОС на один диск с ОС Windows (dual-boot)
    - Загрузка РЕД ОС в SecureBoot-режиме
    - Работа с РЕД ОС в сессии LiveUSB
    - Решение возникающих проблем
      - Проблемы загрузки ОС
        - Проблемы с монтированием домашнего каталога /home
        - Пользователь забыл свой пароль и пароль root
        - Система не монтирует корневой раздел
        - ОС запускается, но зависает на экране загрузки
        - Не загружается РЕД ОС из-за неправильного UUID раздела SWAP
        - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС
      - Решение проблем при установке РЕД ОС
        - Проблемы при установке ОС
        - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС
  - Начало работы с РЕД ОС
    - Общие положения
    - Аутентификация пользователя
    - Окно настройки РЕД ОС
    - Графические оболочки рабочего стола в РЕД ОС
      - Графическое окружение MATE
      - Графическое окружение Cinnamon
      - Оконный менеджер Openbox
      - Установка графической оболочки в РЕД ОС 7.3
      - Выбор графической оболочки для пользователя по умолчанию
    - Специальные возможности в РЕД ОС
      - Специальные возможности в графическом окружении MATE
      - Экранный диктор
    - Настройка внешнего вида
      - Установка дополнительных шрифтов
      - Настройка внешнего вида графического окружения MATE в РЕД ОС 7.3
    - Работа пользователя в РЕД ОС
    - Настройка среды рабочего стола
    - Привилегии и root
    - Блокирование сеанса и завершение работы с РЕД ОС
  - Основные понятия
    - Ядро ОС
    - Загрузчик ОС
    - Файловая система в РЕД ОС
    - Система управления пакетами
      - Общие сведения
        - Введение: пакеты, зависимости и репозитории
        - Назначение DNF
        - Основные команды DNF и утилиты dnf repoquery
        - Работа с историей DNF
        - Источники программ (репозитории)
        - Управление пакетами
      - Менеджер пакетов Dnfdragora
      - Настройка оповещения и автоматического обновления пакетов в РЕД ОС 7.3
      - Менеджер пакетов RPM
        - Назначение RPM
        - Основной список команд RPM
      - Преобразование форматов систем управления пакетами с помощью alien

- Процессы в РЕД ОС
  - Процессы в РЕД ОС
  - Получение сведений о процессах в РЕД ОС
- Журналирование событий в РЕД ОС
- Пользователи в РЕД ОС
  - Общая информация
  - Роли пользователей
- Работа в терминале
  - Командные оболочки (интерпретаторы)
  - Основные утилиты в консоли РЕД ОС
  - Получение справочной информации об использовании утилит с помощью man

- Безопасность в РЕД ОС
  - Общие рекомендации
  - Аудит в РЕД ОС
  - Контроль целостности системы
  - Расчет контрольных сумм файлов
  - Замкнутая программная среда
  - Проверка контрольной суммы ISO-образа
  - Система принудительного контроля доступа SELinux
    - SELinux - система принудительного контроля доступа
    - Отключение SELINUX
  - Настройка системы аутентификации
    - Подключаемые модули аутентификации (PAM). Общие сведения
    - Настройка двухфакторной аутентификации с помощью модуля pam_usb
    - Локальная аутентификация с использованием Рутокен MFA
  - Безопасное хранение паролей пользователей
    - Разблокировка связки ключей
    - Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012
    - Менеджер паролей keepassxc
  - Работа с политиками Polkit
  - Списки контроля доступа ACL
  - Ограничение полномочий пользователей по использованию виртуальных терминалов
  - Шифрование дисков и отдельных файлов
  - Защитное преобразование файлов и каталогов по ГОСТ Р 34.12–2015
  - Безопасное удаление файлов
  - Настройка USB
    - Отключение CD-ROM
    - Ограничение доступа к USB-накопителям
    - Настройка протоколирования событий подключения USB-накопителей
    - Настройка принадлежности USB-накопителей
    - Настройка учета USB-накопителей
    - Ограничение доступа USB-устройств по defines class code
    - Утилита по созданию правил для монтирования USB-накопителей
    - USBIP - утилита для подключения удаленных USB-устройств
  - Сканер уязвимостей OpenSCAP
  - Тестирование аппаратного обеспечения
  - Аудит безопасности сети
    - Исследование сети с помощью консольной утилиты nmap
    - Исследование сети с помощью графической утилиты zenmap
  - Настройка SSL
    - Настройка SSL для веб-серверов
    - Поддержка российских сертификатов безопасности
    - Настройка ГОСТ в OpenSSL в РЕД ОС 7.3
  - Fail2Ban - сервис блокировки хостов
  - XCA - программа для управления асимметричными ключами
  - Блокировка макросов в LibreOffice
  - Сторонние средства защиты информации
    - КриптоПРО
      - Установка КриптоПро CSP 4.0
      - Установка КриптоПро CSP 5.0
      - Работа с электронной подписью в РЕД ОС под Байкал-М
      - Графические утилиты для работы с КриптоПро CSP
      - Работа с сертификатами КриптоПро
      - Установка плагинов Госуслуг и КриптоПро в браузерах Chromium, Яндекс.Браузер, Firefox
    - Vipnet
      - ViPNet IDS HS Agent - система обнаружения вторжений
      - ViPNet PKI Client - ПО для работы с электронной подписью
      - Программный комплекс для защиты рабочих мест ViPNet Client
      - Криптопровайдер VipNet CSP
    - СКЗИ Континент АП
    - Криптографический комплекс КАРМА
    - Антивирусные программы
      - Установка Kaspersky Endpoint Security
      - Установка Kaspersky Security Center
      - Установка Dr.Web

- Настройка сетевых подключений
  - Настройка DHCP
    - О DHCP
    - Базовая настройка DHCP

        - Отказоустойчивый сервер DHCP

    - Настройка DNS
        - О службе DNS (bind)
        - Настройка DNS-сервера bind
        - Настройка репликации DNS-сервера bind
        - Настройка кеширования DNS с помощью dnsmasq
        - Расширенная настройка DNS-сервера
        - Решение возникающих проблем
            - Проверка работоспособности DNS с помощью nslookup

    - Настройка сетевых соединений
        - Настройка сетевого адаптера
        - Настройка сетевых соединений с помощью networkctl
        - Настройка bonding с использованием инструмента nmcli
        - Управление пропускной способностью сетевого интерфейса
        - Управление маршрутизацией
        - Настройка Wi-Fi в РЕД ОС

    - Настройка прокси-сервера
        - Кеширующий прокси-сервер squid
            - Основные понятия squid
            - Установка и настройка squid
            - Настройка автоматической авторизации доменных пользователей IPA в squid

        - Настройка высокодоступного прокси-сервера HAProxy
        - Настройка прокси-сервера 3proxy
        - Настройка ЕСПД (Единая Сеть Передачи Данных от Ростелеком)
        - Настройка прокси на клиентских ПК

    - Настройка межсетевого экрана
        - Настройка брандмауэра Firewall
        - Настройка iptables

    - Мониторинг сети
        - Тестирование пропускной способности сети с помощью iperf3
        - Вывод информации об активных сетевых соединениях с помощью iftop
        - Мониторинг сетевого трафика с помощью nethogs
        - Отображение информации о сетевых сокетах с помощью ss
        - Мониторинг использования сетевого канала с помощью trafshow

    - Анализ и фильтрация сетевых пакетов с помощью tcpdump
    - Механизм защиты сервера Port Knocking
        - Настройка сервера Port Knocking
        - Подключение клиента Port Knocking

    - Настройка FTP-сервера
    - Настройка ProFTPD
    - Настройка NFS
    - Настройка iSCSI
    - Настройка веб-серверов
        - Установка и настройка веб-сервера nginx
        - Настройка прокси-сервера nginx для веб-приложений на Node.js
        - Установка и настройка веб-сервера apache
        - WordPress - инструмент управления сайтами

- Организация удаленного доступа
    - Настройка доступа по SSH
        - Общие сведения о протоколе SSH
        - Служба SSHD
        - Конфигурационный файл SSHD_CONFIG
        - Работа с клиентом и сервером SSH
        - Muon – графический SSH-клиент
        - Сторонние SSH-клиенты
            - Snowflake - графический SSH-клиент

        - Создание SSH-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015
        - Аутентификация по протоколу SSH с использованием RSA-ключа

    - Настройка доступа по XRDP
        - Установка и настройка xrdp-сервера в РЕД ОС 7.3
        - Дополнительная настройка xrdp-сервера

    - Установка и настройка TigerVNC
    - Настройка X2GO
    - Настройка SPICE
    - Настройка X11VNC
    - Работа с FreeRDP и RemoteApp
    - Настройка guacamole
    - Remmina – клиент для подключения к удаленному рабочему столу
    - Сервер для подключения к удаленному рабочему столу vino
    - Утилита удаленного запуска графических приложений xpra
    - Клиентская программа для работы с сетевыми протоколами PuTTY
    - Сторонние средства удаленного доступа
        - AnyDesk
        - МойАссистент
        - LiteManager
        - RuDesktop

- Настройка оборудования

- Работа с дисковой подсистемой
  - Добавление жесткого диска в РЕД ОС
  - Монтирование устройств через systemd
  - Gnome-disk-utility – утилита для управления дисками
  - Gparted – работа с дисковыми разделами
  - Blivet-gui – управление разделами и дисками
  - Baobab – программа для анализа использования разделов диска
  - Менеджер логических томов LVM
  - Примеры использования LVM
  - Утилиты для работы с дисковым пространством
  - Мониторинг файловой системы с помощью duf
  - Квоты для директорий в РЕД ОС (ограничение размера каталога)
  - Уменьшение размера диска для установки ОС Windows на один диск с РЕД ОС
  - BleachBit - утилита для выполнения очистки диска
  - DisLocker - инструмент для чтения зашифрованных разделов

- Использование твердотельных накопителей (SSD)
  - TRIM
  - Планировщик ввода/вывода
  - Уменьшение числа операций чтения/записи

- Работа с bluetooth-устройствами
  - Работа с bluetooth

- Настройка USB
  - Отключение CD-ROM
  - Ограничение доступа к USB-накопителям
  - Настройка протоколирования событий подключения USB-накопителей
  - Настройка принадлежности USB-накопителей
  - Настройка учета USB-накопителей
  - Ограничение доступа USB-устройств по defines class code
  - Утилита по созданию правил для монтирования USB-накопителей
  - USBIP - утилита для подключения удаленных USB-устройств

- Настройка драйвера для видеокарты
  - Установка драйвера Nvidia в РЕД ОС 7.3
  - Установка драйвера AMDGPU
  - Envycontrol - утилита для переключения режимов графического процессора

- Управление питанием
  - Настройка ИБП
    - Установка и настройка NUT
  - PowerTOP - утилита управления питанием
  - TLP и TLPUI — утилиты для управления питанием

- Тестирование аппаратного обеспечения
  - Получение технической информации о ПК
  - hardinfo – подробная информация о системе
  - hdparm – получение информации о параметрах жестких дисков
  - smartctl и hddtemp – мониторинг состояния жестких дисков
  - sysbench - утилита тестирования производительности
  - glxgear и glxinfo – тестирование производительности графического ускорителя
  - sensors - утилита для мониторинга датчиков температуры
  - screentest – утилита тестирования мониторов
  - glmark2 – тестирование графических процессоров
  - stress-ng – утилита нагрузочного тестирования аппаратного обеспечения
  - Проверка состояния жесткого диска
  - Тестирование оперативной памяти

- minicom - программа настройки параметров COM-портов
- IMSProg - I2C/MicroWire/SPI программатор для CH341a
- Настройка принтеров
  - Подключение принтеров HP
  - Подключение принтеров Canon
  - Установка драйверов Pantum
  - Настройка cups
  - Подключение сетевого принтера по IPP
  - Подключение к РЕД ОС принтера, открытого в общий доступ на ОС Windows
  - Подключение принтера к РЕД ОС и Windows открытого в общий доступ на РЕД ОС
  - Установка драйверов foo2zjs
  - Установка принтеров Samsung

- Настройка сканеров
  - Настройка сканеров
  - Сканирование документа по сети

- Решение пользовательских задач
  - Настройка графического окружения
    - Смена менеджера входа в систему (lightdm и sddm)
    - Отключение информационного сообщения при входе в сеанс пользователя
    - Добавление системной панели на второй монитор
    - Управление с помощью dconf
    - Настройка режимов работы мониторов с помощью XRandR
    - RedShift - утилита изменения цветового профиля экрана
    - Панель быстрого запуска Plank
    - Shotwell - утилита для автоматической смены обоев рабочего стола (слайд-шоу)

  - Работа с диалоговыми окнами
    - Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев
    - Yad — утилита для создания диалоговых окон с использованием терминала или сценариев

        - Dialog – утилита для создания диалоговых окон в консольных приложениях

- Текстовые редакторы
    - Полноэкранный редактор VI и улучшенный редактор VIM
    - Текстовые редакторы в РЕД ОС
    - Альтернативные офисные пакеты
        - WPS Office
        - OnlyOffice
        - МойОфис
        - Р7-Офис

    - Texmacs — программа для редактирования документов

- Работа с файлами
    - Файловые менеджеры
        - Файловый менеджер Double Commander
        - Файловый менеджер Midnight Commander
        - Расширения файлового менеджера caja
            - Ручное добавление расширений caja
            - caja-extension-actions

    - Поиск дубликатов
        - Fdupes – программа проверки наличия дубликатов файлов
        - FSlint – графическая утилита поиска дубликатов файлов

    - Утилиты для архивирования, восстановления и копирования файлов в терминале
    - Сохранение в файл вывода консоли
    - Recoll – поиск документов по содержимому
    - Ripgrep — рекурсивный поиск в текущем каталоге шаблона регулярного выражения
    - Просмотр и управление файлами и каталогами с помощью утилиты tree
    - tre-command - утилита для отображения структуры директорий
    - zoxide - легкая навигация по каталогам

- Работа с графикой
    - Просмотрщики документов
        - Atril - универсальный просмотрщик документов
        - Okular - универсальный просмотрщик документов

    - Создание скриншотов и скринкастов
        - Создание скриншотов с помощью Flameshot
        - Создание скриншотов с помощью kSnip
        - Создание скриншотов с помощью mate-screenshot

    - Работа с PDF
        - LibreOffice Draw – программа редактирования PDF-файлов
        - PDFedit – программа для редактирования PDF-файлов
        - PDFShuffler – программа для пакетной обработки PDF-файлов
        - poppler – утилита конвертации PDF в различные форматы
        - Сторонние средства для работы с PDF
            - Adobe Acrobat Reader

    - Утилиты для распознавания текста
        - Распознавание текста с помощью YAGF
        - Распознавание текста с помощью gImageReader

    - Графические редакторы
        - Простые графические редакторы
        - Графический редактор Krita

    - Сканирование файлов
        - Программы для сканирования в РЕД ОС
        - gscan2pdf - программа для сканирования и обработки документов
        - NAPS2 – программа для сканирования документов и изображений

    - Каталогизаторы фотоальбомов
    - Darktable — программа каталогизации и обработки цифровых фотографий в формате RAW
    - GUVCView — программа для работы с веб-камерами
    - Synfig Studio — создание векторной анимации
    - Imagination — программа для создания слайд-шоу
    - Создание диаграмм с помощью drawio
    - KolourPaint — растровый графический редактор
    - IrfanView — программа для работы с графическими файлами
    - Scribus — программа для вёрстки страниц
    - Редактор шрифтов FontForge

- Аудио и видео
    - Работа с аудио
        - Аудиоплеер Audacious
        - AlsaMixer - настройка звуковых карт
        - hdajackretask - управление портами звуковых устройств
        - Настройка звука с помощью PulseAudio
        - Audacity - редактор звуковых файлов
        - DeaDBeef - мультимедийный проигрыватель
        - Rhythmbox — музыкальный проигрыватель

    - Работа с видео
        - Видеоредактор Kdenlive
        - Видеоредактор Shotcut
        - Видеоредактор OBS Studio
        - SimpleScreenRecorder — программа записи экрана
        - Видеоредактор VLC

        - Сторонние средства работы с видео
            - DaVinci Resolve - редактирование видео
        - Решение проблем со звуком
    - Настройка почтовых клиентов
        - Почтовый клиент Evolution
        - Почтовый клиент Thunderbird
        - Настройка в Evolution подключения к MS Exchange
        - Настройка календаря Exchange в Thunderbird
        - Thunderbird запуск Google-почты
    - Браузеры
        - Firefox
        - Яндекс.Браузер
        - Сквозная аутентификация в браузерах
        - Сторонние браузеры
            - Opera
            - Vivaldi
        - Сбор и просмотр диагностической информации браузеров
    - Общение и чат
        - Настройка Openfire
        - Настройка SSO openfire
        - Pidgin
        - PSI
        - Jitsi
        - Linphone
        - Telegram
        - Gajim
        - Сторонние средства связи
            - Skype
            - Zoom
            - TrueConf
            - Discord
    - Работа с WINE
        - Установка WINE
        - Работа с программами в WINE
        - Префиксы WINE
        - Установка winetricks
        - Дополнительные возможности WINE
    - Игры в РЕД ОС
        - Установка и запуск игр
    - Полезные утилиты
        - Автоматическое исправление ввода текста с помощью XNeuralSwitcher
        - CherryTree – программа систематизации и ведения заметок
        - ClipIt – менеджер буфера обмена
        - Торренты
        - Автоматическое обнаружение сторонних ОС с помощью os-prober
        - Оптимизация команд с помощью hyperfine
        - Улучшение визуализации различий в коде с утилитой diff-so-fancy
        - Ведение финансового учета с помощью kmymoney
- Администрирование ОС
    - Создание образов системы
        - Livemedia-creator – создание образа системы
        - ISO Master – утилита для редактирования ISO-образов
        - genisoimage - утилита создания ISO-образов файловой системы
        - Dracut - ПО для создания загрузочного образа (initramfs)
    - Обслуживание репозиториев
        - О репозиториях
        - Создание локального репозитория
        - Создание локального репозитория с использованием HTTPS
        - Настройка синхронизации локального репозитория
    - Ядро ОС
        - Модули ядра
        - Настройка zswap
        - Поддержка оборудования в ядре ОС
        - kernel-manager - утилита управления ядрами
        - kdump — инструмент для анализа причин сбоев ядра
    - Загрузчик ОС
        - grubby - утилита настройки загрузчика ОС
        - grub-customizer - утилита редактирования загрузчика ОС
        - Назначение пароля на загрузчик GRUB2
        - Восстановление загрузчика GRUB2
    - Файловая система в РЕД ОС
        - Принципы работы с файловой системой btrfs
            - Описание процесса разметки диска
            - Работа с квотами диска
        - findmnt - получение информации о подключенных файловых системах
        - Проверка файловой системы на наличие ошибок

- Процессы в РЕД ОС
  - Получение сведений о процессах в РЕД ОС
  - Изменение приоритета процесса
  - Мониторинг процессов
    - Интерактивные утилиты динамического мониторинга процессов
      - Системный монитор
      - top
      - htop
      - atop
      - atopsar — встроенный анализатор логов atop
      - iotop - утилита мониторинга использования диска
      - sar
      - pmap
      - nmon
      - vmstat
      - dstat

    - SysMonTask - диспетчер задач РЕД ОС
    - Systemd-analyze - анализ системных процессов
    - Pidstat — утилита для мониторинга и отчётности по статистике производительности процессов

- События в РЕД ОС
  - Журналирование событий
    - Просмотр системных журналов
      - Просмотр системных журналов с помощью графического интерфейса
      - Утилита tail
      - Утилита less

    - Настройка журналов с помощью утилиты journalctl
    - Средство просмотра журналов Log File Navigator (LNAV)

  - Мониторинг событий в файловой системе
    - Утилита incron
    - Утилиты inotifywatch и inotifywait
    - Утилита fswatch

  - Rsyslog – сервис управления системными журналами
  - LogAnalyzer – веб-приложение для просмотра системных журналов
  - Logrotate – настройка ротации (хранения) системных журналов
  - Решение возникающих проблем
    - Сбор диагностической информации о РЕД ОС (loginfo)
    - Настройка systemd-coredump для автоматического сбора дампов в РЕД ОС 7.3
    - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

  - Рекомендации по анализу журналов и дампов

- Работа в терминале
  - Командные оболочки (интерпретаторы)
  - Основные утилиты в консоли РЕД ОС
  - Получение справочной информации об использовании утилит с помощью man
  - Менеджер сервисов systemd
  - Управление задачами в командной строке
  - Добавление команд в автозагрузку
  - Создание псевдонимов команд с помощью alias
  - Утилита записи терминальной сессии asciinema
  - Терминальные мультиплексоры
    - Screen - запуск виртуальных терминалов в режиме сессий
    - Менеджер терминалов tmux
    - Эмулятор терминала terminator

  - expect - инструмент для автоматизации и тестирования

- Управление пользователями
  - Общая информация
  - Роли пользователей
  - Пароли пользователей
  - Утилита passwd
  - Добавление нового пользователя
  - Редактирование имеющихся пользовательских записей
  - Удаление пользователей
  - Управление пользователями и группами из консоли
  - Управление пользователями с помощью графической утилиты system-config-users
  - Автоматическая авторизация пользователя (автовход)
  - Создание и настройка собственного default-профиля пользователя при помощи SKEL
  - Управление сеансами пользователей с помощью systemd-logind
  - Ограничение ресурсов пользователя
  - Управление дисковыми квотами
  - Настройка прав доступа к файлам и каталогам
  - Режим Киоска в РЕД ОС
  - multiseat - настройка нескольких рабочих мест

- Настройка даты и времени
  - Особенности служб синхронизации времени
  - Установка и настройка ntp
  - Утилита синхронизации времени ntpdate
  - Установка и настройка chrony
  - Настройка systemd-timesyncd
  - Утилита настройки системной локали localectl
  - Диспетчер настройки даты и времени
  - Утилита настройки даты и времени system-config-date
  - Утилита настройки даты и времени timedatectl

- Планирование заданий
  - Настройка и использование systemd-таймеров
  - Планировщик заданий crontab
  - Планировщик заданий at
  - Планировщик заданий anacron
  - Графическая утилита для планирования заданий zeit

- Настройка почтовых служб
  - Сервер электронной почты postfix
  - Настройка Iredmail
    - Установка Iredmail на РЕД ОС 7.3
    - Интеграция Iredmail с MS AD

  - Настройка почтовых клиентов
    - Почтовый клиент Evolution
    - Почтовый клиент Thunderbird
    - Настройка в Evolution подключения к MS Exchange
    - Настройка календаря Exchange в Thunderbird
    - Thunderbird запуск Google-почты

- Подключение РЕД ОС к облачным сервисам
  - Облачное хранилище NextCloud
    - Настройка NextCloud с СУБД MySQL и ПО для веб-сервера Apache
    - Настройка NextCloud с СУБД PostgreSQL и ПО для веб-сервера Nginx
    - Настройка автоматического входа в NextCloud в домене IPA

  - Облачный сервис Яндекс.Диск
    - Подключение РЕД ОС к облачным сервисам

  - WebDAV, neon и chezdav для настройки облачного сервиса

- Удаленное администрирование
  - Webmin - программный комплекс для удаленного администрирования
  - Ansible - система автоматизации настройки и развертывания ПО
  - Puppet - централизованное управление конфигурацией ОС и ПО
  - Citrix Linux VDA

- Виртуализация и эмуляция
  - VirtualBox
    - Установка VirtualBox
    - Установка РЕД ОС в VirtualBox
    - Автостарт виртуальной машины в VirtualBox при запуске системы
    - Настройка общей папки в VirtualBox
    - Установка эмулятора Android-x86

  - QEMU-KVM
    - Установка и настройка QEMU-KVM
    - Конвертация образа машины VirtualBox для KVM

  - Установка cloud-init, сценарии и использование в облачных средах
  - Сторонние средства виртуализации
    - VMware
      - Установка VMware
      - Установка РЕД ОС в VMware
      - Установка VMware Tools

    - Hyper-V
      - Установка РЕД ОС 7.3 в Hyper-V
      - Взаимодействие Hyper-V с РЕД ОС 7.3

  - DOSBox - программный эмулятор DOS

- Контейнеризация
  - Установка и настройка docker
  - Kubernetes - управление контейнеризованными приложениями
    - Kubernetes. Основные понятия
    - Установка kubernetes с использованием контейнерного движка containerd
    - Установка kubernetes с использованием контейнерного движка cri-o
    - Установка kubernetes с использованием контейнерного движка cri-dockerd
    - Использование kubernetes в закрытой сети (без доступа в Интернет)
      - Установка kubernetes с использованием контейнерного движка cri-o без доступа в Интернет
      - Установка kubernetes с использованием контейнерного движка containerd без доступа в Интернет
      - Установка kubernetes с использованием контейнерного движка cri-dockerd без доступа в Интернет

- Запуск приложений в изолированной среде
  - Flatpak - изолированная среда для запуска приложений
  - Snap - изолированная среда для запуска приложений
  - Firejail - система изолированного запуска приложений

- Запуск приложений сторонних систем
  - AppImage - запуск приложений без установки
  - PlayOnLinux - программа запуска приложений Windows

- Объединённая служба каталога (LDAP)
- Работа с доменом
  - Подключение сетевых каталогов
    - Настройка доступа к компьютеру по его сетевому имени
    - Подключение сетевых директорий с помощью графического приложения
    - Подключение сетевых директорий с помощью fstab
    - Подключение сетевых директорий с использованием automount (autofs)
    - Подключение сетевых директорий с помощью fstab и механизма Kerberos

        - Подключение сетевых директорий с использованием automount (autofs) и механизма Kerberos
        - Подключение сетевых директорий с помощью NFS
        - Автоматическое монтирование ресурсов при входе пользователя с помощью pam_mount
        - Подключение сетевых директорий через сервис systemd
        - РЕД ОС в рабочей группе
        - Подключение сетевых директорий с помощью утилиты connectfolder
        - Подключение сетевых директорий с помощью GIO

    - Работа с доменом MSAD
        - Предварительная подготовка компьютера к вводу в домен
        - Ввод РЕД ОС в домен MSAD с помощью утилиты join-to-domain
        - Ввод РЕД ОС в домен MSAD с помощью консольных команд
        - Настройка отображения общих ресурсов
        - Создание кнопки запуска доступа к сетевому ресурсу
        - Отключение отображения определенного пользователя на экране входа в систему
        - Предоставление права пользователям домена выполнять команды от пользователя root
        - Вывод РЕД ОС из домена MSAD
        - Каталог общего сетевого доступа на РЕД ОС в домене MSAD

    - Организация домена IPA
        - О домене IPA
        - Рекомендации по развертыванию
        - Установка сервера IPA
        - Настройка репликации IPA
        - Настройка резервного копирования домена IPA
        - Создание доверительных отношений IPA и MSAD в РЕД ОС 7.3
        - Ввод клиентских машин в домен IPA
        - Интеграция файлового сервера SAMBA с IPA

    - Организация домена SAMBA
        - Основные понятия
        - Samba с использованием DNS backend - SAMBA_INTERNAL
            - Установка сервера SAMBA DC
            - Администрирование контроллера SAMBA
            - Настройка доверительных отношений SAMBA и MSAD

        - Samba с использованием DNS backend - BIND9_DLZ
            - Установка сервера SAMBA DC
            - Администрирование контроллера SAMBA

        - Ввод клиентских машин в домен SAMBA
        - Управление пользователями и группами в домене SAMBA DC
        - Настройка сетевого хранилища
            - Доступ к предыдущим версиям файлов с помощью shadow_copy
            - Пример настройки файлового хранилища SAMBA
            - Каталог общего сетевого доступа на РЕД ОС в домене MSAD
            - Интеграция файлового сервера SAMBA с IPA
            - Журналирование событий SAMBA

        - Резервное копирование домена SAMBA DC

    - smbpass – графическая утилита изменения пароля доменного пользователя (MSAD или SAMBA)
    - Сравнение функций Winbind и SSSD

- Отказоустойчивый кластер
    - Организация отказоустойчивого кластера

- СУБД
    - Установка PostgreSQL
    - Установка Firebird
    - Установка СУБД Ред База Данных
    - pgAdmin4 - администрирование и разработка баз данных

- Система программ 1С:Предприятие
    - Настройка Postgresql для 1С
    - 1С-сервер для РЕД ОС 7.3
    - Публикация БД на web-сервере 1С
    - 1С-клиент
    - 1С-клиент. Установка нескольких версий
    - Сбор логов сервера 1С

- Специализированное стороннее ПО
    - Справочно-правовая система Консультант Плюс
    - Тест драйвера ККМ АТОЛ
    - Установка ПО ГРАНД-Смета

- Оценка производительности системы
    - Conky - программа для системного мониторинга
    - Glances - инструмент для мониторинга системы
    - iostat - утилита анализа загруженности системы
    - iotop - утилита мониторинга использования диска
    - nfsiostat - утилита отображения статистики для файловых систем NFS
    - perf - анализ производительности ПО
    - tuned - служба оптимизации производительности системы
    - Тестирование производительности дисков с помощью fio
    - Анализ производительности блочных устройств (blktrace) и построение графиков на основе собранных данных (iowatcher)

- Мониторинг системы
    - Настройка сервера и агента ZABBIX
        - Настройка сервера на postgresql 13 и zabbix 6.2

            - Настройка сервера на mysql и zabbix 6.2
            - Настройка агента zabbix

        - Настройка Prometheus с применением системы визуализации данных Grafana
        - Настройка GLPI-сервера (для инвентаризации оборудования)
        - OpenSearch — система распределенного поиска, сбора, анализа и визуализации данных
        - Graylog — инструмент для централизированного сбора, хранения и анализа системных журналов

    - Резервное копирование и восстановление
        - Создание резервных копий с помощью утилиты cp
        - Создание резервных копий с помощью утилиты fsbackup
        - Работа с графической утилитой fwbackups
            - Начало работы
            - Использование fwbackups
            - Техническая информация

        - Testdisk - утилита для восстановления утраченных данных
        - Timeshift. Работа со снимками ОС
        - SyncThing — утилита для синхронизации файлов
        - Burp - программа резервного копирования
        - Создание бэкапов с помощью Butterfly Backup
        - Сторонние средства резервного копирования и восстановления
            - Rescuezilla - программа для создания и восстановления резервных копий
            - Clonezilla - программа клонирования дисков
                - Локальное клонирование жесткого диска
                - Клонирование жесткого диска на SAMBA-сервер
                - Клонирование жесткого диска на SSH-сервер

            - Создание резервных копий в Кибер Бекап

- Организация образовательного процесса
    - ПО для образовательного процесса – redos-education
    - Организация учебного процесса
        - OpenBoard - программа для работы с интерактивными досками
        - Veyon - программа управления компьютерным классом

    - Химия и химические вычисления
        - OpenBabel – программа для работы с химическими структурами и молекулярными системами
        - XDrawChem – программа для рисования и анализа химических структур и реакций
        - Kalzium - периодическая система химических элементов
        - Avogadro - программа просмотра и редактирования молекул
        - InChI — химический идентификатор на основе молекулярной структуры
        - OpenMolcas — программа для квантовой химии

    - Словари и переводчики
        - Работа со словарями
        - Сторонние сервисы для перевода
            - ПО для машинного перевода документов Promt Translation Server и PROMT Agent

    - QGIS — геоинформационная система
    - Weasis — программа просмотра диагностических изображений в формате DICOM
    - Клавиатурный тренажер KTouch
    - ПО для автоматизированного проектирования (CAD-системы)
        - LibreCAD
        - Сторонние CAD-системы
            - NanoCAD 24.1
            - FreeCAD
            - КОМПАС-3D

    - Marble — виртуальный глобус
    - Система программирования КуМир
    - GNU Octave — программа для математических вычислений

- Средства разработки
    - Среды разработки (IDE)
        - Установка Geany
        - Установка Lazarus
        - Установка QT Creator
        - Установка Glade
        - Установка Code::Blocks
        - Установка Visual Studio Code
        - Установка VSCodium
        - Установка Atom
        - Установка Arduino IDE
        - Установка PhpStorm
        - Установка PyCharm
        - BlueFish - ПО для создания и редактирования интернет-приложений

    - Создание RPM-пакетов прикладных программ
        - Определение RPM
            - Основные понятия
            - Преимущества RPM
            - Поименование пакетов

        - Инфраструктура сборки
            - Сборочное окружение
            - Файл спецификации
            - Основные макросы
            - Скриптлеты
            - Условные операторы
            - Сборка исходных и двоичных пакетов

            - Цифровая подпись пакета

        - Примеры создания пакетов
            - Сборка пакета стороннего ПО
            - Сборка мета-пакета

    - Компиляторы и интерпретаторы языков программирования
        - Установка .NET
        - FPC – компилятор для разработки программ на языке Pascal
        - Установка Julia
        - Tarantool — оптимизированный интерпретатор Lua
        - Java OpenJDK в РЕД ОС
        - PHP 8.X на РЕД ОС

- Решение возникающих проблем
    - Сбор диагностической информации о РЕД ОС (loginfo)
    - Проверка файловой системы на наличие ошибок
    - Проверка состояния жесткого диска
    - Восстановление загрузчика GRUB2
    - Решение проблем загрузки ОС
        - Проблемы с монтированием домашнего каталога /home
        - Пользователь забыл свой пароль и пароль root
        - Система не монтирует корневой раздел
        - ОС запускается, но зависает на экране загрузки
        - Не загружается РЕД ОС из-за неправильного UUID раздела SWAP
        - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

    - Решение проблем при установке ОС
        - Проблемы при установке ОС
        - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

    - Решение проблем со звуком
        - Решение проблем со звуком

    - Решение проблем с драйверами
        - Realtek RTL8821CE
        - Intel i915

    - Тестирование оперативной памяти
    - Поддержка оборудования в ядре ОС
    - Настройка systemd-coredump для автоматического сбора дампов в РЕД ОС 7.3
    - kdump — инструмент для анализа причин сбоев ядра
    - Рекомендации по анализу журналов и дампов
    - Проверка работоспособности DNS с помощью nslookup

- РЕД ОС 8
    - Установка РЕД ОС
        - Системные требования
        - Создание загрузочных носителей
        - Последовательность установки
        - Начало установки
        - Язык интерфейса программы установки
        - Обзор установки
        - Ручная разметка диска
        - Установка системы
        - Действия после установки ОС
        - Альтернативные способы установки
            - Общие понятия
            - Установка РЕД ОС в текстовом режиме
            - Установка РЕД ОС на программный массив RAID
                - Обзорная инструкция про RAID
                - Создание программного массива уровня RAID0 и RAID1
                - Создание программного массива уровня RAID 6
                - Создание программного массива уровня RAID 10
                - Установка РЕД ОС на программный массив RAID1 и RAID10

            - Сетевая установка РЕД ОС
                - Автоматизация развертывания (kickstart)
                - Подготовка PXE-сервера для развертывания РЕД ОС с загрузкой в UEFI или Legacy в РЕД ОС 8
                - Настройка установки РЕД ОС по PXE через VNC в РЕД ОС 8

        - Установка РЕД ОС на один диск с ОС Windows (dual-boot)
        - Загрузка РЕД ОС в SecureBoot-режиме
        - Работа с РЕД ОС в сессии LiveUSB
        - Решение возникающих проблем
            - Проблемы загрузки ОС
                - Проблемы с монтированием домашнего каталога /home
                - Пользователь забыл свой пароль и пароль root
                - Система не монтирует корневой раздел
                - ОС запускается, но зависает на экране загрузки
                - Не загружается РЕД ОС из-за неправильного UUID раздела SWAP
                - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

            - Решение проблем при установке РЕД ОС
                - Проблемы при установке ОС
                - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

    - Начало работы с РЕД ОС
        - Общие положения
        - Аутентификация пользователя
        - Окно настройки РЕД ОС

- Графические оболочки рабочего стола в РЕД ОС
  - Графическое окружение MATE
  - Графическое окружение KDE Plasma
  - Графическое окружение GNOME
  - Оконный менеджер Openbox
  - Графический сервер Wayland
  - Установка графической оболочки в РЕД ОС 8

- Специальные возможности в РЕД ОС
  - Специальные возможности в графическом окружении MATE
  - Специальные возможности в графическом окружении KDE
  - Специальные возможности в графическом окружении GNOME
  - Экранный диктор

- Настройка внешнего вида
  - Установка дополнительных шрифтов
  - Настройка внешнего вида графического окружения MATE в РЕД ОС 8
  - Настройка внешнего вида графического окружения KDE Plasma
  - Настройка внешнего вида графического окружения GNOME
  - Тема оформления рабочего стола WindowsLike

- Работа пользователя в РЕД ОС
- Настройка среды рабочего стола
- Привилегии и root
- Блокирование сеанса и завершение работы с РЕД ОС

- Основные понятия
  - Ядро ОС
  - Загрузчик ОС
  - Файловая система в РЕД ОС
  - Система управления пакетами
    - Общие сведения
      - Введение: пакеты, зависимости и репозитории
      - Назначение DNF
      - Основные команды DNF и утилиты dnf repoquery
      - Работа с историей DNF
      - Источники программ (репозитории)
      - Управление пакетами

    - Менеджер пакетов Dnfdragora
    - Менеджер пакетов RPM
      - Назначение RPM
      - Основной список команд RPM

    - Преобразование форматов систем управления пакетами с помощью alien

  - Процессы в РЕД ОС
    - Процессы в РЕД ОС
    - Получение сведений о процессах в РЕД ОС

  - Журналирование событий в РЕД ОС
  - Пользователи в РЕД ОС
    - Общая информация
    - Роли пользователей

  - Работа в терминале
    - Командные оболочки (интерпретаторы)
    - Основные утилиты в консоли РЕД ОС
    - Получение справочной информации об использовании утилит с помощью man

- Безопасность в РЕД ОС
  - Общие рекомендации
  - Аудит в РЕД ОС
  - Расчет контрольных сумм файлов
  - Замкнутая программная среда
  - Проверка контрольной суммы ISO-образа
  - Система принудительного контроля доступа SELinux
    - SELinux - система принудительного контроля доступа
    - Отключение SELINUX

  - Настройка системы аутентификации
    - Подключаемые модули аутентификации (PAM). Общие сведения
    - Настройка двухфакторной аутентификации с помощью модуля pam_usb
    - Локальная аутентификация с использованием Рутокен MFA

  - Безопасное хранение паролей пользователей
    - Разблокировка связки ключей в MATE
    - Управление паролями в KDE Plasma
    - Разблокировка связки ключей в GNOME
    - Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012 в РЕД ОС 8
    - Менеджер паролей keepassxc

  - Работа с политиками Polkit
  - Списки контроля доступа ACL
  - Ограничение полномочий пользователей по использованию виртуальных терминалов
  - Шифрование дисков и отдельных файлов
  - Защитное преобразование файлов и каталогов по ГОСТ Р 34.12–2015
  - Безопасное удаление файлов
  - Настройка USB
    - Отключение CD-ROM
    - Ограничение доступа к USB-накопителям

        - Настройка протоколирования событий подключения USB-накопителей
        - Настройка принадлежности USB-накопителей
        - Настройка учета USB-накопителей
        - Ограничение доступа USB-устройств по defines class code
        - Утилита по созданию правил для монтирования USB-накопителей
        - USBIP - утилита для подключения удаленных USB-устройств
    - Тестирование аппаратного обеспечения
    - Аудит безопасности сети
        - Исследование сети с помощью консольной утилиты nmap
        - Исследование сети с помощью графической утилиты zenmap
    - Настройка SSL
        - Настройка SSL для веб-серверов
        - Поддержка российских сертификатов безопасности
        - Настройка ГОСТ в OpenSSL в РЕД ОС 8
    - Fail2Ban - сервис блокировки хостов
    - XCA - программа для управления асимметричными ключами
    - Блокировка макросов в LibreOffice
    - Сторонние средства защиты информации
        - КриптоПРО
            - Установка КриптоПро CSP 4.0
            - Установка КриптоПро CSP 5.0
            - Графические утилиты для работы с КриптоПро CSP
            - Работа с сертификатами КриптоПро
            - Установка плагинов Госуслуг и КриптоПро в браузерах Chromium, Яндекс.Браузер, Firefox
        - Vipnet
            - ViPNet IDS HS Agent - система обнаружения вторжений
            - ViPNet PKI Client - ПО для работы с электронной подписью
            - Криптопровайдер VipNet CSP
        - СКЗИ Континент АП
        - Криптографический комплекс КАРМА
        - Антивирусные программы
            - Установка Kaspersky Endpoint Security
            - Установка Kaspersky Security Center
            - Установка Dr.Web

- Настройка сетевых подключений
    - Настройка DHCP
        - О DHCP
        - Базовая настройка DHCP
        - Отказоустойчивый сервер DHCP
    - Настройка DNS
        - О службе DNS (bind)
        - Настройка DNS-сервера bind
        - Настройка репликации DNS-сервера bind
        - Настройка кеширования DNS с помощью dnsmasq
        - Настройка локального кеширующего DNS-сервера systemd-resolved
        - Расширенная настройка DNS-сервера
        - Решение возникающих проблем
            - Проверка работоспособности DNS с помощью nslookup
    - Настройка сетевых соединений
        - Настройка сетевого адаптера
        - Настройка сетевых соединений с помощью networkctl
        - Настройка bonding с использованием инструмента nmcli
        - Управление пропускной способностью сетевого интерфейса
        - Управление маршрутизацией
        - Настройка Wi-Fi в РЕД ОС
    - Настройка прокси-сервера
        - Кеширующий прокси-сервер squid
            - Основные понятия squid
            - Установка и настройка squid
            - Настройка автоматической авторизации доменных пользователей IPA в squid
        - Настройка высокодоступного прокси-сервера HAProxy
        - Настройка прокси-сервера 3proxy
        - Настройка ЕСПД (Единая Сеть Передачи Данных от Ростелеком)
        - Настройка прокси на клиентских ПК
    - Настройка межсетевого экрана
        - Настройка брандмауэра Firewall
        - Настройка iptables
    - Мониторинг сети
        - Тестирование пропускной способности сети с помощью iperf3
        - Вывод информации об активных сетевых соединениях с помощью iftop
        - Мониторинг сетевого трафика с помощью nethogs
        - Отображение информации о сетевых сокетах с помощью ss
        - Мониторинг использования сетевого канала с помощью trafshow
    - Анализ и фильтрация сетевых пакетов с помощью tcpdump
    - Механизм защиты сервера Port Knocking
        - Настройка сервера Port Knocking
        - Подключение клиента Port Knocking

- Настройка FTP-сервера
- Настройка ProFTPD
- Настройка NFS
- Настройка iSCSI
- Настройка веб-серверов
  - Установка и настройка веб-сервера nginx
  - Настройка прокси-сервера nginx для веб-приложений на Node.js
  - Установка и настройка веб-сервера apache
  - WordPress - инструмент управления сайтами

- Организация удаленного доступа
  - Настройка доступа по SSH
    - Общие сведения о протоколе SSH
    - Служба SSHD
    - Конфигурационный файл SSHD_CONFIG
    - Работа с клиентом и сервером SSH
    - Muon – графический SSH-клиент
    - Сторонние SSH-клиенты
      - Snowflake - графический SSH-клиент
    - Создание SSH-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015
    - Аутентификация по протоколу SSH с использованием RSA-ключа
  - Настройка доступа по XRDP
    - Установка и настройка xrdp-сервера в РЕД ОС 8
    - Дополнительная настройка xrdp-сервера
  - Установка и настройка TigerVNC
  - Настройка X2GO
  - Настройка X11VNC
  - Работа с FreeRDP и RemoteApp
  - Настройка guacamole
  - Remmina – клиент для подключения к удаленному рабочему столу
  - Утилита удаленного запуска графических приложений xpra
  - Клиентская программа для работы с сетевыми протоколами PuTTY
  - Сторонние средства удаленного доступа
    - AnyDesk
    - МойАссистент
    - LiteManager
    - RuDesktop

- Настройка оборудования
  - Работа с дисковой подсистемой
    - Добавление жесткого диска в РЕД ОС
    - Монтирование устройств через systemd
    - Gnome-disk-utility – утилита для управления дисками
    - Gparted – работа с дисковыми разделами
    - Blivet-gui – управление разделами и дисками
    - Baobab – программа для анализа использования разделов диска
    - Менеджер логических томов LVM
    - Примеры использования LVM
    - Утилиты для работы с дисковым пространством
    - Мониторинг файловой системы с помощью duf
    - Квоты для директорий в РЕД ОС (ограничение размера каталога)
    - Уменьшение размера диска для установки ОС Windows на один диск с РЕД ОС
    - BleachBit - утилита для выполнения очистки диска
    - DisLocker - инструмент для чтения зашифрованных разделов
  - Использование твердотельных накопителей (SSD)
    - TRIM
    - Планировщик ввода/вывода
    - Уменьшение числа операций чтения/записи
  - Работа с bluetooth-устройствами
    - Работа с bluetooth
  - Настройка USB
    - Отключение CD-ROM
    - Ограничение доступа к USB-накопителям
    - Настройка протоколирования событий подключения USB-накопителей
    - Настройка принадлежности USB-накопителей
    - Настройка учета USB-накопителей
    - Ограничение доступа USB-устройств по defines class code
    - Утилита по созданию правил для монтирования USB-накопителей
    - USBIP - утилита для подключения удаленных USB-устройств
  - Настройка драйвера для видеокарты
    - Установка драйвера Nvidia в РЕД ОС
    - Envycontrol - утилита для переключения режимов графического процессора
  - Управление питанием
    - Настройка ИБП
    - PowerTOP - утилита управления питанием
    - TLP и TLPUI — утилиты для управления питанием
  - Тестирование аппаратного обеспечения
    - Получение технической информации о ПК
    - hardinfo – подробная информация о системе
    - hdparm – получение информации о параметрах жестких дисков
    - smartctl и hddtemp – мониторинг состояния жестких дисков

        - sysbench - утилита тестирования производительности
        - glxgear и glxinfo – тестирование производительности графического ускорителя
        - sensors - утилита для мониторинга датчиков температуры
        - screentest – утилита тестирования мониторов
        - glmark2 – тестирование графических процессоров
        - stress-ng – утилита нагрузочного тестирования аппаратного обеспечения
        - Проверка состояния жесткого диска
        - Тестирование оперативной памяти

    - minicom - программа настройки параметров COM-портов
    - IMSProg - I2C/MicroWire/SPI программатор для CH341a
    - Настройка принтеров
        - Подключение принтеров HP
        - Подключение принтеров Canon
        - Установка драйверов Pantum
        - Настройка cups
        - Подключение сетевого принтера по IPP
        - Подключение к РЕД ОС принтера, открытого в общий доступ на ОС Windows
        - Подключение принтера к РЕД ОС и Windows открытого в общий доступ на РЕД ОС
        - Установка драйверов foo2zjs
        - Установка принтеров Samsung

    - Настройка сканеров
        - Настройка сканеров

- Решение пользовательских задач
    - Настройка графического окружения
        - Смена менеджера входа в систему (lightdm и sddm)
        - Отключение информационного сообщения при входе в сеанс пользователя
        - Добавление системной панели на второй монитор
        - Управление с помощью dconf
        - Настройка режимов работы мониторов с помощью XRandR
        - RedShift - утилита изменения цветового профиля экрана
        - Панель быстрого запуска Plank
        - Shotwell - утилита для автоматической смены обоев рабочего стола (слайд-шоу)

    - Работа с диалоговыми окнами
        - Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев
        - Yad — утилита для создания диалоговых окон с использованием терминала или сценариев
        - Dialog – утилита для создания диалоговых окон в консольных приложениях

    - Текстовые редакторы
        - Полноэкранный редактор VI и улучшенный редактор VIM
        - Текстовые редакторы в РЕД ОС
        - Альтернативные офисные пакеты
            - WPS Office
            - OnlyOffice
            - МойОфис
            - Р7-Офис

        - Texmacs — программа для редактирования документов

    - Работа с файлами
        - Файловые менеджеры
            - Файловый менеджер Double Commander
            - Файловый менеджер Midnight Commander

        - Поиск дубликатов
            - Fdupes – программа проверки наличия дубликатов файлов
            - FSlint – графическая утилита поиска дубликатов файлов

        - Утилиты для архивирования, восстановления и копирования файлов в терминале
        - Сохранение в файл вывода консоли
        - Recoll – поиск документов по содержимому
        - Ripgrep — рекурсивный поиск в текущем каталоге шаблона регулярного выражения
        - Просмотр и управление файлами и каталогами с помощью утилиты tree
        - tre-command - утилита для отображения структуры директорий
        - zoxide - легкая навигация по каталогам

    - Работа с графикой
        - Просмотрщики документов
            - Atril - универсальный просмотрщик документов
            - Okular - универсальный просмотрщик документов

        - Создание скриншотов и скринкастов
            - Создание скриншотов с помощью Flameshot
            - Создание скриншотов с помощью kSnip
            - Создание скриншотов с помощью mate-screenshot

        - Работа с PDF
            - LibreOffice Draw – программа редактирования PDF-файлов
            - PDFArranger - программа для обработки PDF-файлов
            - poppler – утилита конвертации PDF в различные форматы
            - Сторонние средства для работы с PDF
                - Adobe Acrobat Reader

        - Утилиты для распознавания текста
            - Распознавание текста с помощью YAGF
            - Распознавание текста с помощью gImageReader

        - Графические редакторы

        - Простые графические редакторы
        - Графический редактор Krita

    - Сканирование файлов
        - Программы для сканирования в РЕД ОС
        - gscan2pdf - программа для сканирования и обработки документов
        - NAPS2 – программа для сканирования документов и изображений

    - Каталогизаторы фотоальбомов
    - Darktable — программа каталогизации и обработки цифровых фотографий в формате RAW
    - GUVCView — программа для работы с веб-камерами
    - Synfig Studio — создание векторной анимации
    - Imagination - программа для создания слайд-шоу
    - KolourPaint — растровый графический редактор
    - IrfanView — программа для работы с графическими файлами
    - Scribus — программа для вёрстки страниц
    - Редактор шрифтов FontForge

- Аудио и видео
    - Работа с аудио
        - Аудиоплеер Audacious
        - AlsaMixer - настройка звуковых карт
        - hdajackretask - управление портами звуковых устройств
        - Настройка звука с помощью PulseAudio
        - Audacity - редактор звуковых файлов
        - DeaDBeef - мультимедийный проигрыватель
        - Rhythmbox — музыкальный проигрыватель

    - Работа с видео
        - Видеоредактор Kdenlive
        - Видеоредактор Shotcut
        - Видеоредактор OBS Studio
        - SimpleScreenRecorder — программа записи экрана
        - Видеоредактор VLC

    - Сторонние средства работы с видео
        - DaVinci Resolve - редактирование видео

    - Решение проблем со звуком

- Настройка почтовых клиентов
    - Почтовый клиент Evolution
    - Почтовый клиент Thunderbird
    - Настройка в Evolution подключения к MS Exchange
    - Настройка календаря Exchange в Thunderbird
    - Thunderbird запуск Google-почты

- Браузеры
    - Firefox
    - Яндекс.Браузер
    - Сквозная аутентификация в браузерах
    - Сторонние браузеры
        - Opera
        - Vivaldi

    - Сбор и просмотр диагностической информации браузеров

- Общение и чат
    - Настройка Openfire
    - Настройка SSO openfire
    - Pidgin
    - PSI
    - Jitsi
    - Linphone
    - Telegram
    - Gajim
    - Сторонние средства связи
        - Skype
        - Zoom
        - TrueConf

- Работа с WINE
    - Установка WINE
    - Работа с программами в WINE
    - Префиксы WINE
    - Установка winetricks
    - Дополнительные возможности WINE

- Игры в РЕД ОС
    - Установка и запуск игр

- Полезные утилиты
    - CherryTree – программа систематизации и ведения заметок
    - ClipIt – менеджер буфера обмена
    - Торренты
    - Автоматическое обнаружение сторонних ОС с помощью os-prober
    - Оптимизация команд с помощью hyperfine
    - Улучшение визуализации различий в коде с утилитой diff-so-fancy
    - Ведение финансового учета с помощью kmymoney

- Администрирование ОС

- Создание образов системы
  - Livemedia-creator – создание образа системы
  - ISO Master – утилита для редактирования ISO-образов
  - genisoimage - утилита создания ISO-образов файловой системы
  - Dracut - ПО для создания загрузочного образа (initramfs)

- Обслуживание репозиториев
  - О репозиториях
  - Создание локального репозитория
  - Создание локального репозитория с использованием HTTPS
  - Настройка синхронизации локального репозитория

- Ядро ОС
  - Модули ядра
  - Настройка zswap
  - Поддержка оборудования в ядре ОС
  - kernel-manager - утилита управления ядрами
  - kdump — инструмент для анализа причин сбоев ядра

- Загрузчик ОС
  - grubby - утилита настройки загрузчика ОС
  - grub-customizer - утилита редактирования загрузчика ОС
  - Назначение пароля на загрузчик GRUB2
  - Восстановление загрузчика GRUB2

- Файловая система в РЕД ОС
  - Принципы работы с файловой системой btrfs
    - Описание процесса разметки диска
    - Работа с квотами диска

  - findmnt - получение информации о подключенных файловых системах
  - Проверка файловой системы на наличие ошибок

- Процессы в РЕД ОС
  - Получение сведений о процессах в РЕД ОС
  - Изменение приоритета процесса
  - Мониторинг процессов
    - Интерактивные утилиты динамического мониторинга процессов
      - Системный монитор
      - top
      - htop
      - atop
      - atopsar — встроенный анализатор логов atop
      - iotop - утилита мониторинга использования диска
      - sar
      - pmap
      - nmon
      - vmstat
      - dstat

    - SysMonTask - диспетчер задач РЕД ОС
    - Systemd-analyze - анализ системных процессов
    - Pidstat — утилита для мониторинга и отчётности по статистике производительности процессов

- События в РЕД ОС
  - Журналирование событий
    - Просмотр системных журналов
      - Просмотр системных журналов с помощью графического интерфейса
      - Утилита tail
      - Утилита less

    - Настройка журналов с помощью утилиты journalctl
    - Средство просмотра журналов Log File Navigator (LNAV)

  - Мониторинг событий в файловой системе
    - Утилита incron
    - Утилиты inotifywatch и inotifywait
    - Утилита fswatch

  - Rsyslog – сервис управления системными журналами
  - Logrotate – настройка ротации (хранения) системных журналов
  - Решение возникающих проблем
    - Сбор диагностической информации о РЕД ОС (loginfo)
    - Настройка systemd-coredump для автоматического сбора дампов
    - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

  - Рекомендации по анализу журналов и дампов

- Работа в терминале
  - Командные оболочки (интерпретаторы)
  - Основные утилиты в консоли РЕД ОС
  - Получение справочной информации об использовании утилит с помощью man
  - Менеджер сервисов systemd
  - Управление задачами в командной строке
  - Добавление команд в автозагрузку
  - Создание псевдонимов команд с помощью alias
  - Утилита записи терминальной сессии asciinema
  - Терминальные мультиплексоры
    - Screen - запуск виртуальных терминалов в режиме сессий
    - Менеджер терминалов tmux
    - Эмулятор терминала terminator

    - expect - инструмент для автоматизации и тестирования

- Управление пользователями
    - Общая информация
    - Роли пользователей
    - Пароли пользователей
    - Утилита passwd
    - Добавление нового пользователя
    - Редактирование имеющихся пользовательских записей
    - Удаление пользователей
    - Управление пользователями и группами из консоли
    - Автоматическая авторизация пользователя (автовход)
    - Создание и настройка собственного default-профиля пользователя при помощи SKEL
    - Управление сеансами пользователей с помощью systemd-logind
    - Ограничение ресурсов пользователя
    - Управление дисковыми квотами
    - Настройка прав доступа к файлам и каталогам
    - Режим Киоска в РЕД ОС

- Настройка даты и времени
    - Особенности служб синхронизации времени
    - Установка и настройка ntpsec
    - Утилита синхронизации времени ntpdate
    - Установка и настройка chrony
    - Настройка systemd-timesyncd
    - Утилита настройки системной локали localectl
    - Диспетчер настройки даты и времени
    - Утилита настройки даты и времени timedatectl

- Планирование заданий
    - Настройка и использование systemd-таймеров
    - Планировщик заданий crontab
    - Планировщик заданий at
    - Планировщик заданий anacron
    - Графическая утилита для планирования заданий zeit

- Настройка почтовых служб
    - Сервер электронной почты postfix
    - Настройка Iredmail
    - Настройка почтовых клиентов
        - Почтовый клиент Evolution
        - Почтовый клиент Thunderbird
        - Настройка в Evolution подключения к MS Exchange
        - Настройка календаря Exchange в Thunderbird
        - Thunderbird запуск Google-почты

- Подключение РЕД ОС к облачным сервисам
    - Облачное хранилище NextCloud
        - Настройка NextCloud с СУБД MySQL и ПО для веб-сервера Apache
        - Настройка NextCloud с СУБД PostgreSQL и ПО для веб-сервера Ngnix
        - Настройка автоматического входа в NextCloud в домене IPA

    - Облачный сервис Яндекс.Диск
        - Подключение РЕД ОС к облачным сервисам

    - WebDAV, neon и chezdav для настройки облачного сервиса

- Удаленное администрирование
    - Webmin - программный комплекс для удаленного администрирования
    - Ansible - система автоматизации настройки и развертывания ПО
    - Puppet - централизованное управление конфигурацией ОС и ПО

- Виртуализация и эмуляция
    - VirtualBox
        - Установка VirtualBox
        - Установка РЕД ОС в VirtualBox
        - Автостарт виртуальной машины в VirtualBox при запуске системы
        - Установка эмулятора Android-x86

    - QEMU-KVM
        - Установка и настройка QEMU-KVM
        - Конвертация образа машины VirtualBox для KVM

    - Установка cloud-init, сценарии и использование в облачных средах
    - Сторонние средства виртуализации
        - VMware
            - Установка VMware
            - Установка РЕД ОС в VMware
            - Установка VMware Tools

        - Hyper-V
            - Установка РЕД ОС в Hyper-V
            - Взаимодействие Hyper-V с РЕД ОС

    - DOSBox - программный эмулятор DOS

- Запуск приложений в изолированной среде
    - Flatpak - изолированная среда для запуска приложений
    - Snap - изолированная среда для запуска приложений
    - Firejail - система изолированного запуска приложений

- Запуск приложений сторонних систем
  - AppImage - запуск приложений без установки
  - PlayOnLinux - программа запуска приложений Windows

- Объединённая служба каталога (LDAP)
- Работа с доменом
  - Работа с доменом MSAD
    - Предварительная подготовка компьютера к вводу в домен
    - Ввод РЕД ОС в домен MSAD с помощью утилиты join-to-domain
    - Ввод РЕД ОС в домен MSAD с помощью консольных команд
    - Настройка отображения общих ресурсов
    - Создание кнопки запуска доступа к сетевому ресурсу
    - Отключение отображения определенного пользователя на экране входа в систему
    - Предоставление права пользователям домена выполнять команды от пользователя root
    - Вывод РЕД ОС из домена MSAD
    - Каталог общего сетевого доступа на РЕД ОС в домене MSAD

  - Организация домена IPA
    - О домене IPA
    - Рекомендации по развертыванию
    - Установка сервера IPA
    - Настройка репликации IPA
    - Настройка резервного копирования домена IPA
    - Создание доверительных отношений IPA и MSAD
    - Ввод клиентских машин в домен IPA
    - Интеграция файлового сервера SAMBA с IPA

  - Организация домена SAMBA
    - Основные понятия
    - Samba с использованием DNS backend - SAMBA_INTERNAL
      - Установка сервера SAMBA DC
      - Администрирование контроллера SAMBA
      - Настройка доверительных отношений SAMBA и MSAD

    - Ввод клиентских машин в домен SAMBA
    - Управление пользователями и группами в домене SAMBA DC
    - Настройка сетевого хранилища
      - Доступ к предыдущим версиям файлов с помощью shadow_copy
      - Пример настройки файлового хранилища SAMBA
      - Каталог общего сетевого доступа на РЕД ОС в домене MSAD
      - Интеграция файлового сервера SAMBA с IPA
      - Журналирование событий SAMBA

    - Резервное копирование домена SAMBA DC

  - smbpass – графическая утилита изменения пароля доменного пользователя (MSAD или SAMBA)
  - Сравнение функций Winbind и SSSD
  - Подключение сетевых каталогов
    - Настройка доступа к компьютеру по его сетевому имени
    - Подключение сетевых директорий с помощью графического приложения
    - Подключение сетевых директорий с помощью fstab
    - Подключение сетевых директорий с использованием automount (autofs)
    - Подключение сетевых директорий с помощью fstab и механизма Kerberos
    - Подключение сетевых директорий с использованием automount (autofs) и механизма Kerberos
    - Подключение сетевых директорий с помощью NFS
    - Автоматическое монтирование ресурсов при входе пользователя с помощью pam_mount
    - Подключение сетевых директорий через сервис systemd
    - РЕД ОС в рабочей группе
    - Подключение сетевых директорий с помощью утилиты connectfolder
    - Подключение сетевых директорий с помощью GIO

- Отказоустойчивый кластер
  - Организация отказоустойчивого кластера

- СУБД
  - Установка PostgreSQL
  - Установка Firebird
  - Установка СУБД Ред База Данных
  - pgAdmin4 - администрирование и разработка баз данных

- Система программ 1С:Предприятие
  - Настройка Postgresql для 1С
  - 1С-сервер для РЕД ОС
  - Публикация БД на web-сервере 1С
  - 1С-клиент
  - 1С-клиент. Установка нескольких версий
  - Сбор логов сервера 1С

- Специализированное стороннее ПО
  - Справочно-правовая система Консультант Плюс
  - Тест драйвера ККМ АТОЛ
  - Установка ПО ГРАНД-Смета

- Оценка производительности системы
  - Conky - программа для системного мониторинга
  - Glances - инструмент для мониторинга системы
  - iostat - утилита анализа загруженности системы
  - iotop - утилита мониторинга использования диска
  - nfsiostat - утилита отображения статистики для файловых систем NFS
  - perf - анализ производительности ПО
  - tuned - служба оптимизации производительности системы

        - Тестирование производительности дисков с помощью fio
        - Анализ производительности блочных устройств (blktrace) и построение графиков на основе собранных данных (iowatcher)

    - Мониторинг системы
        - Настройка сервера и агента ZABBIX
            - Настройка сервера на postgresql 13 и zabbix 6.4
            - Настройка сервера на MySQL и Zabbix 6.4
            - Настройка агента zabbix

        - Настройка Prometheus с применением системы визуализации данных Grafana
        - Настройка GLPI-сервера (для инвентаризации оборудования)
        - OpenSearch — система распределенного поиска, сбора, анализа и визуализации данных
        - Graylog — инструмент для централизированного сбора, хранения и анализа системных журналов

    - Резервное копирование и восстановление
        - Создание резервных копий с помощью утилиты cp
        - Работа с графической утилитой fwbackups
            - Начало работы
            - Использование fwbackups
            - Техническая информация

        - Testdisk - утилита для восстановления утраченных данных
        - Timeshift. Работа со снимками ОС
        - SyncThing — утилита для синхронизации файлов
        - Burp - программа резервного копирования
        - Создание бэкапов с помощью Butterfly Backup
        - Сторонние средства резервного копирования и восстановления
            - Rescuezilla - программа для создания и восстановления резервных копий
            - Clonezilla - программа клонирования дисков
                - Локальное клонирование жесткого диска
                - Клонирование жесткого диска на SAMBA-сервер
                - Клонирование жесткого диска на SSH-сервер

            - Создание резервных копий в Кибер Бекап

- Организация образовательного процесса
    - ПО для образовательного процесса – redos-education
    - Организация учебного процесса
        - OpenBoard - программа для работы с интерактивными досками
        - Veyon - программа управления компьютерным классом

    - Химия и химические вычисления
        - OpenBabel – программа для работы с химическими структурами и молекулярными системами
        - XDrawChem – программа для рисования и анализа химических структур и реакций
        - Kalzium - периодическая система химических элементов
        - InChI — химический идентификатор на основе молекулярной структуры
        - OpenMolcas — программа для квантовой химии

    - Словари и переводчики
        - Работа со словарями
        - Сторонние сервисы для перевода
            - ПО для машинного перевода документов Promt Translation Server и PROMT Agent

    - QGIS — геоинформационная система
    - Weasis — программа просмотра диагностических изображений в формате DICOM
    - Клавиатурный тренажер KTouch
    - ПО для автоматизированного проектирования (CAD-системы)
        - LibreCAD
        - Сторонние CAD-системы
            - NanoCAD 24.1
            - КОМПАС-3D

    - Marble — виртуальный глобус
    - Система программирования КуМир
    - GNU Octave — программа для математических вычислений

- Средства разработки
    - Среды разработки (IDE)
        - Установка Geany
        - Установка Lazarus
        - Установка QT Creator
        - Установка Glade
        - Установка Code::Blocks
        - Установка Visual Studio Code
        - Установка VSCodium
        - Установка Arduino IDE
        - Установка PhpStorm
        - Установка PyCharm
        - BlueFish - ПО для создания и редактирования интернет-приложений

    - Создание RPM-пакетов прикладных программ
        - Определение RPM
            - Основные понятия
            - Преимущества RPM
            - Поименование пакетов

        - Инфраструктура сборки
            - Сборочное окружение
            - Файл спецификации
            - Основные макросы

            - Скриптлеты
            - Условные операторы
            - Сборка исходных и двоичных пакетов
            - Цифровая подпись пакета

        - Примеры создания пакетов
            - Сборка пакета стороннего ПО
            - Сборка мета-пакета

    - Компиляторы и интерпретаторы языков программирования
        - Установка .NET
        - FPC – компилятор для разработки программ на языке Pascal
        - Установка Julia
        - Tarantool — оптимизированный интерпретатор Lua
        - Java OpenJDK в РЕД ОС
        - PHP 8.X на РЕД ОС

- Решение возникающих проблем
    - Сбор диагностической информации о РЕД ОС (loginfo)
    - Проверка файловой системы на наличие ошибок
    - Проверка состояния жесткого диска
    - Восстановление загрузчика GRUB2
    - Решение проблем загрузки ОС
        - Проблемы с монтированием домашнего каталога /home
        - Пользователь забыл свой пароль и пароль root
        - Система не монтирует корневой раздел
        - ОС запускается, но зависает на экране загрузки
        - Не загружается РЕД ОС из-за неправильного UUID раздела SWAP
        - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

    - Решение проблем при установке ОС
        - Проблемы при установке ОС
        - Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

    - Решение проблем со звуком
        - Решение проблем со звуком

    - Решение проблем с драйверами
        - Realtek RTL8821CE
        - Intel i915

    - Тестирование оперативной памяти
    - Поддержка оборудования в ядре ОС
    - Настройка systemd-coredump для автоматического сбора дампов
    - kdump — инструмент для анализа причин сбоев ядра
    - Рекомендации по анализу журналов и дампов
    - Ошибка HTTPS-соединения
    - Проверка работоспособности DNS с помощью nslookup

- Обновление РЕД ОС
    - Обновление РЕД ОС с 7.3 на 8
    - Обновление ядра Linux до версии 5.15 в РЕД ОС 7.3
    - Обновление ядра Linux до версии 6.1 в РЕД ОС 7.3
    - Установка realtime-ядра в РЕД ОС 8
    - Обновление системы в рамках корректирующих релизов РЕД ОС 7.3
    - Версии РЕД ОС и сроки поддержки
    - Рекомендации по организации процесса тестирования и установки обновлений РЕД ОС
    - Списки изменений
        - Список изменений в РЕД ОС 7.3.1
        - Список изменений в РЕД ОС 7.3.2
        - Список изменений в РЕД ОС 7.3.3
        - Список изменений в РЕД ОС 7.3.4
        - Список изменений в РЕД ОС 7.3.5
        - Список изменений в РЕД ОС 8
        - Список изменений в РЕД ОС 8 (декабрь 2024)

- Программное обеспечение в составе РЕД ОС
    - Список пользовательского ПО
    - Список серверного ПО

- Поддерживаемое оборудование
    - Оборудование, совместимое с РЕД ОС
    - Печатающее и сканирующее оборудование, совместимое с РЕД ОС (из практики)
    - Печатающее и сканирующее оборудование, несовместимое с РЕД ОС (из практики)
    - Архив списков совместимого оборудования
        - Сканеры, поддерживаемые РЕД ОС
        - Список видеокарт, поддерживаемых РЕД ОС
        - Список сетевых карт, поддерживаемых РЕД ОС
        - Печатающие устройства производства Alps, Anitech, Apollo, Apple
        - Печатающие устройства производства Brother
        - Печатающие устройства производства Canon
        - Печатающие устройства производства CIAAT, Citizen, Compaq
        - Печатающие устройства производства Dai Nippon, DatamaxONeil, DEC, Dell
        - Печатающие устройства производства Epson
        - Печатающие устройства производства Fuji, Genicom
        - Печатающие устройства производства Gestetner
        - Печатающие устройства производства Heidelberg, Hitachi, HP
        - Печатающие устройства производства IBM, Imagen, Imagistics, infoPrint
        - Печатающие устройства производства Kodak, Konica Minolta
        - Печатающие устройства производства Kyocera
        - Печатающие устройства производства Lanier
        - Печатающие устройства производства Lexmark

        - Печатающие устройства производства Minolta, Mitsubishi, NEC
        - Печатающие устройства производства NRG
        - Печатающие устройства производства Oce, Oki
        - Печатающие устройства производства Olivetti, Olympus, Panasonic, Pantum, PCPI, QMS, Raven
        - Печатающие устройства производства Ricoh
        - Печатающие устройства производства Samsung
        - Печатающие устройства производства Savin
        - Печатающие устройства производства Seiko, Shinko, Sinfonia, SiPix, Sony
        - Печатающие устройства производства Sharp
        - Печатающие устройства производства Tally, Tektronix, Texas Instruments, Toshiba
        - Печатающие устройства производства Xante, Xerox
        - Модели производителя ARBYTE

- Часто задаваемые вопросы
    - Часто задаваемые вопросы по РЕД ОС (FAQ)

- РЕД Виртуализация
    - Описание программного продукта
    - Документация
    - Системные требования
        - Аппаратная часть
        - Аппаратное и программное оснащение клиентов
        - Гипервизор
        - Хранилище
        - Ограничения РЕД Виртуализации

    - Подготовка сетевого хранилища: NFS
    - Установка РЕД Виртуализации
        - Установка в режиме Standalone
        - Установка в режиме Host
        - Установка в режиме Gluster Hyperconverged для одного узла
        - Установка в режиме Gluster Hyperconverged для нескольких узлов
        - Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Standalone с помощью стороннего центра сертификации
        - Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Hosted Engine с помощью стороннего центра сертификации

    - Инструмент для смены доменного имени Engine
    - Хосты со статусом «Non Responsive»
    - Настройка параметров расширения "тонких" дисков ВМ
    - Часто задаваемые вопросы (FAQ)
    - Информация об обновлениях

- РЕД АДМ
    - Описание РЕД АДМ
    - Системные требования для РЕД АДМ
    - Подготовка окружения
    - Установка РЕД АДМ Стандартная редакция
        - Установка РЕД АДМ Сервер
        - Установка РЕД АДМ Клиент

    - Обновление РЕД АДМ
        - Обновление РЕД АДМ Сервер версии 1.9.1
        - Обновление РЕД АДМ Сервер версии 1.10
        - Обновление РЕД АДМ Клиент

    - Диагностика проблем
    - Часто задаваемые вопросы (FAQ)

- РЕД База Данных
    - Описание продукта
    - Документация
    - Системные требования
    - Установка РЕД База Данных (Открытая редакция)
    - Обновление СУБД РЕД База Данных (Открытая редакция)
    - Диагностика проблем
    - Часто задаваемые вопросы по СУБД РЕД База Данных (FAQ)

Описание программного продукта

Описание и область применения операционной системы
Основные функции РЕД ОС

Описание и область применения операционной системы

РЕД ОС является многопользовательской, многозадачной ОС, которая предоставляет платформу унифицированной функциональной универсальной доверенной среды для выполнения прикладного программного обеспечения.

РЕД ОС на уровне драйверов поддерживает широкий перечень оборудования актуальных версий, доступного на рынке средств вычислительной техники (СВТ), а также оборудования, снятого с производства, но поддерживаемого производителями.

В РЕД ОС поддерживается установка с оптических носителей информации, флеш-накопителей, разделов локального жёсткого диска, а также установка по сети передачи данных.

Основные функции РЕД ОС

РЕД ОС может обеспечивать обслуживание от одного до нескольких пользователей одновременно. После успешного входа в систему пользователи имеют доступ в главную вычислительную среду, позволяющую запускать пользовательские приложения, создавать и получать доступ к файлам, задавать директивы пользователя на уровне оболочки командного процессора. РЕД ОС предоставляет адекватные механизмы для разграничения пользователей и защиты их данных. Использование привилегированных команд ограничено и доступно только административным пользователям.

РЕД ОС конфигурируется по умолчанию для работы в режиме дискреционного управления доступом (DAC).

Любой пользователь с ролью, которая позволяет выполнять административные действия, считается административным пользователем. Кроме того, РЕД ОС поддерживает типы, которые могут быть связаны с объектами, и домены, которые могут быть связаны с процессами. Роли определяются доменами, к которым они имеют доступ. Предопределённый файл политики, который является частью конфигурации РЕД ОС, определяет правила между доменами и типами. С вышеизложенным определением ролей и прав доступа, подразумеваемых индивидуальными ролями, РЕД ОС выполняет требования ролевого доступа.

РЕД ОС предназначена для работы в сетевом окружении с другими экземплярами РЕД ОС, а также с иными совместимыми серверными и клиентскими системами одного и того же управляемого домена. Все эти системы должны конфигурироваться в соответствии с определённой общей политикой безопасности.

РЕД ОС разрешает использование многими пользователями одного или более процессоров, присоединённых внешних и запоминающих устройств для выполнения разнообразных функций, требующих управляемого распределенного доступа к данным, хранимым в системе. Такие инсталляции типичны для вычислительных систем рабочих групп или предприятий, к которым обращаются локальные пользователи, или компьютерных систем с иначе защищённым доступом.

Предполагается, что ответственность за сохранение данных, защищаемых РЕД ОС, может делегироваться пользователям РЕД ОС. Все данные находятся под управлением механизмов безопасности РЕД ОС. Данные сохраняются в поименованных объектах, и РЕД ОС может связать с каждым поименованным объектом описание прав доступа к этому объекту. Всем пользователям назначаются уникальные идентификаторы. Этот идентификатор пользователя используется вместе с атрибутами и ролями, назначенными пользователю, как основание для решений по управлению доступом. РЕД ОС подтверждает подлинность предъявленного идентификатора пользователя до того, как разрешать ему выполнять дальнейшие действия. РЕД ОС внутри себя сопровождает ряд идентификаторов, связанных с процессами, которые получаются из уникального идентификатора пользователя, предъявляемого при входе в систему. Некоторые из этих идентификаторов могут изменяться во время выполнения процесса согласно политике, реализуемой РЕД ОС.

РЕД ОС предоставляет такие меры безопасности, при которых доступ к объектам данных осуществляется только в соответствии с ограничениями на доступ, наложенными на этот объект его владельцем, административными пользователями и типом объекта. Права владения на поименованные объекты могут передаваться под контролем политики управления доступом.

На объекты данных могут быть назначены дискреционные права доступа (например, чтение, запись, выполнение) субъектов (пользователей). Как только субъекту предоставляется доступ к объекту, его содержание может быть свободно использовано для воздействия на другие доступные этому субъекту объекты.

РЕД ОС имеет существенные расширения элементов безопасности по сравнению со стандартными системами UNIX:

- списки управления доступом;
- реализацию доменов и типов;
- журналируемая файловая система (ext4);
- подключаемые модули аутентификации (PAM);
- специализированная система аудита, которая позволяет учитывать критичные события безопасности и предоставляет административному пользователю инструментальные средства конфигурирования системы аудита и оценки записей аудита;

- базовые функции проверки комплекта оборудования позволяют по требованию административного пользователя проверять, правильно ли обеспечиваются основные функции безопасности аппаратных средств, на которые полагаетсяобъект оценки (ОО).

Развёрнутую ОС применяют в качестве программной платформы для разработок защищённых систем, требования к безопасности которых не превышают указанных показателей. В частности, такие требования предъявляются к защищённым программным системам, работающим с конфиденциальной информацией и персональными данными.

Системные требования

В данной статье приведены минимальные системные требования для установки операционной системы **РЕД ОС** в конфигурациях «**Рабочая станция**» и «**Сервер**» для версии **7.3 и 8**.

Системные требования для **РЕД ОС 7.3** и **8**:

Конфигурация	Рабочая станция	Сервер	Сервер минимальный
Процессор	X86_64 1.6 ГГц 2 ядра	X86_64 1.6 ГГц 2 ядра	X86_64 1.6 ГГц 1 ядро
Объем оперативной памяти	2 Гб	2 Гб	1 Гб
Объем свободного дискового пространства	20 Гб	20 Гб	8 Гб
Видеоадаптер	Поддержка режима SVGA800x600	Поддержка режима SVGA800x600	Поддержка режима SVGA800x600

Создание загрузочных носителей

Определение схемы разделов жёстких дисков
balenaEtcher
MultiWriter
dd
kindd
Rufus для Windows
Brasero
win32 disk imager для Windows
rawrite32 для Windows

Вы можете подробнее ознакомиться с возможностью создания загрузочных носителей и записи ISO-образов, просмотрев наши обучающие видео:

- на **RuTube**:
  - Запись iso-образа РЕД ОС и установка рядом с Windows;
  - Создание загрузочных носителей flash, cd, dvd.
- в **Яндекс.Дзен**:
  - Запись iso-образа РЕД ОС и установка рядом с Windows;
  - Создание загрузочных носителей flash, cd, dvd.
- в **VK Видео**:
  - Запись iso-образа РЕД ОС и установка рядом с Windows;
  - Создание загрузочных носителей flash, cd, dvd.

На наших каналах вы также сможете найти много другой полезной информации.

Определение схемы разделов жёстких дисков

Прежде чем приступить к установке РЕД ОС и начать работу с разделами жёсткого диска, необходимо определить, какая схема разделов на нём использована. Возможны 2 варианта схемы разделов:

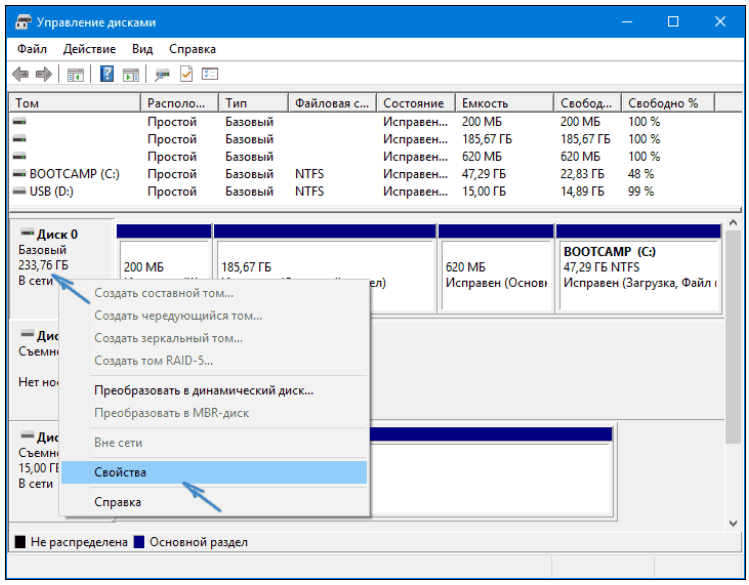
- **MBR** (Главная загрузочная запись);
- **GPT** (Таблица разделов GUID).

Они представляют собой два различных способа хранения информации о разделах диска. Сюда входят данные о начале и конце разделов, чтобы система знала, к какому разделу принадлежит каждый сектор, и какой раздел является загрузочным.

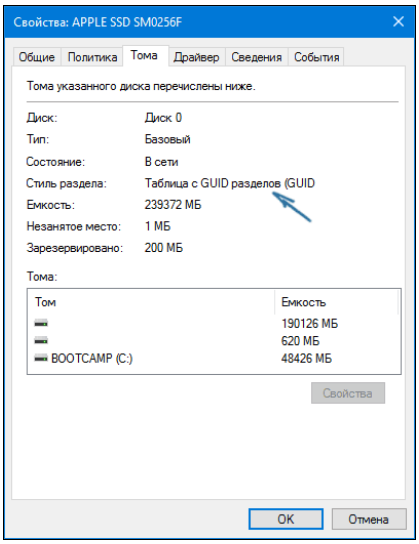
Верное определение схемы разделов жёсткого диска имеет значение для правильной подготовки загрузочного носителя. Несовпадение схем разделов жёсткого диска, на который устанавливается система, со схемой разделов загрузочного носителя, может привести к невозможности загрузки установщика.

Чтобы определить стиль схемы разделов Windows, запустите утилиту «**Управление дисками**» нажмите клавиши **Win+R**, введите **diskmgmt.msc** и нажмите **Enter**.

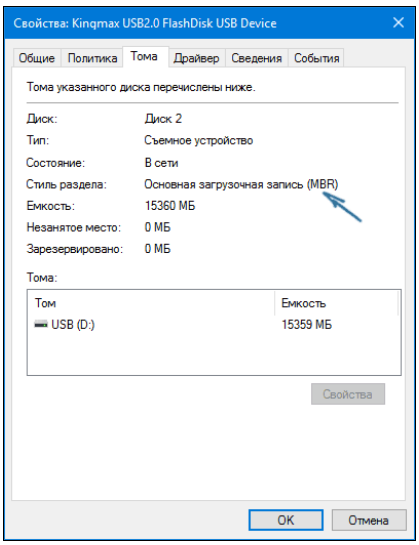
1.В нижней части утилиты «**Управление дисками**» кликните по имени диска правой кнопкой мыши и выберите пункт меню «**Свойства**».



2.В свойствах откройте вкладку «**Тома**». Если в пункте «**Стиль раздела**» указано «**Таблица с GUID разделов**» — у вас GPT-диск.



Если в этом же пункте указано «**Основная загрузочная запись (MBR)**» — у вас MBR-диск.



1 способ - balenaEtcher

balenaEtcher — свободное программное обеспечение с открытым исходным кодом, предназначенное для записи файлов образов дисков, таких как **.iso** и **.img**, а также архивов для создания LiveUSB флэш-накопителей. Скачать утилиту можно по ссылке. Существуют версии для Linux, Windows и macOS. Процедура записи образа аналогична для всех видов ОС.

Для Windows можно скачать и установить программу или запустить версию **portable** (без установки).

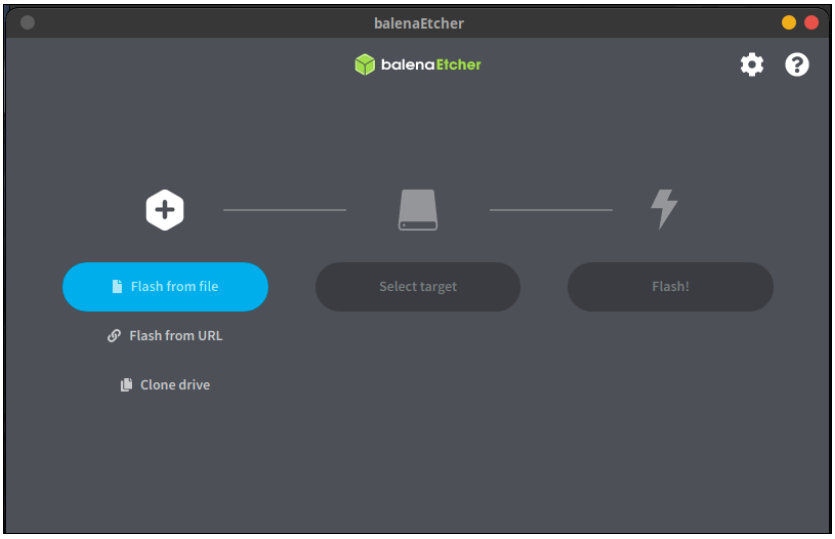
Для Linux - программа распространяется в формате **AppImage**. После ее загрузки перейдите в папку с файлом и предоставьте права на исполнение для полученного файла:

```
chmod +x balenaEtcher-1.18.11-x64.AppImage
```

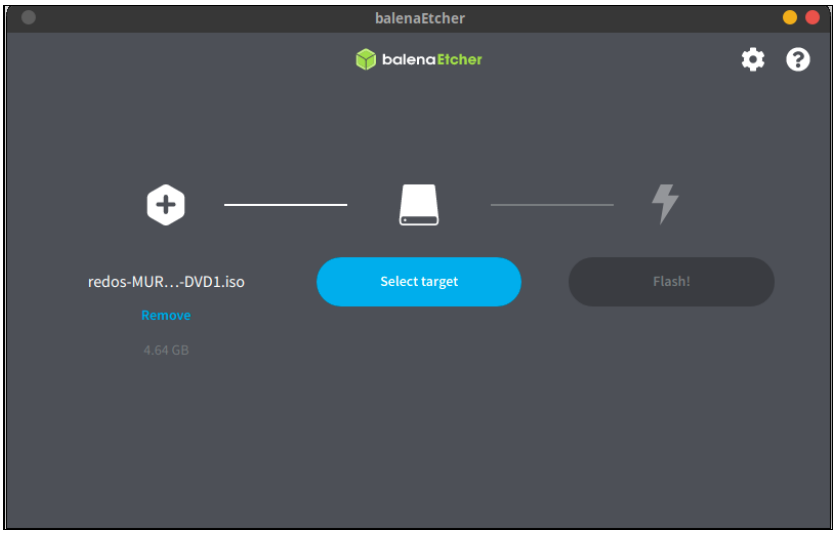
Запустить программу можно двойным кликом по файлу, либо выполнив команду в терминале:

```
./balenaEtcher-1.18.11-x64.AppImage
```

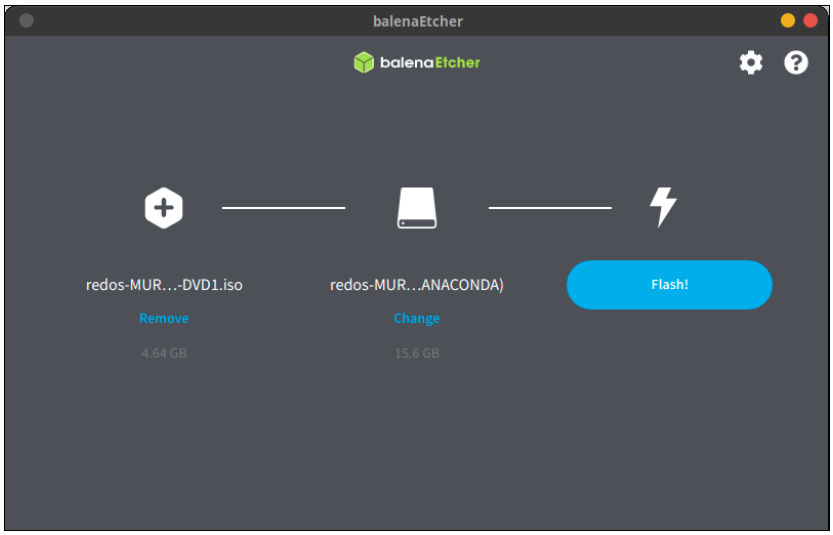
Для записи образа выберите файл, нажав на «**Flash form file**»:



Далее выберите устройство, на которое будет записан образ:



После выбора устройства нажмите «**Flash!**»:



Далее будет запрошен пароль администратора, после успешной аутентификации начнется запись образа.

2 способ - MultiWriter

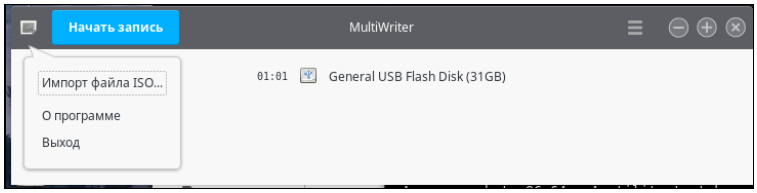
Для записи iso-образов на USB-флеш-накопитель воспользуйтесь приложением **MultiWriter**.

Установка **MultiWriter**:

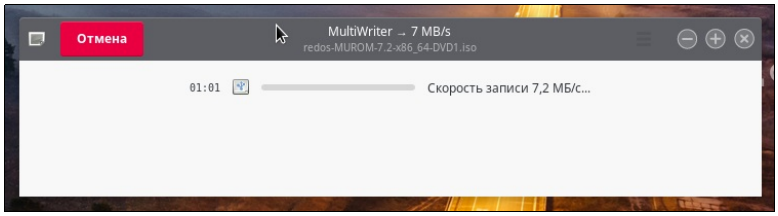
```
dnf install gnome-multi-writer
```

Откройте программу через «**Меню**» - «**Администрирование**» - «**MultiWriter**».

Импортируйте файл iso-образа:



Нажмите на кнопку «**Запись**», в результате начнется запись iso-образа на flash-носитель.



3 способ - dd

Определить имя flash-носителя, например, **sd[x]**:

```
sudo fdisk -l
```

Перейдите в консоли в каталог с iso-образом:

```
cd /путь/до/образа
```

Запись iso-образа:

```
dd if=redos-MUROM-7.2-20190523.0-Everything-x86_64-DVD1.iso of=/dev/sd[x] bs=8MB status=progress oflag=direct
```

ВАЖНО!

Вместо sd[x] укажите свое имя носителя.
При этом будут стерты все данные на USB накопителе и записаны новые!

Для систем с **UEFI** и таблицей разделов **GPT** следует подготовить flash-носитель, выполнив список команд:

```
parted -s /dev/sd[x] mklabel gpt
parted -s --align=optimal /dev/sd[x] mkpart REDOS fat32 1MiB 100%
parted -s /dev/sd[x] set 1 boot on
mkfs.vfat -F 32 /dev/sd[x]
```

Запись iso-образа:

```
dd if=redos-MUROM-7.2-20190523.0-Everything-x86_64-DVD1.iso of=/dev/sd[x] bs=8MB status=progress oflag=direct
```

4 способ - kindd (gui для dd)

Kindd — графический (gui) интерфейс для команды **dd**, бесплатный инструмент с открытым исходным кодом, написанный на **Qt**. Данный инструмент может быть очень полезен новичкам для записи образов дисков.

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

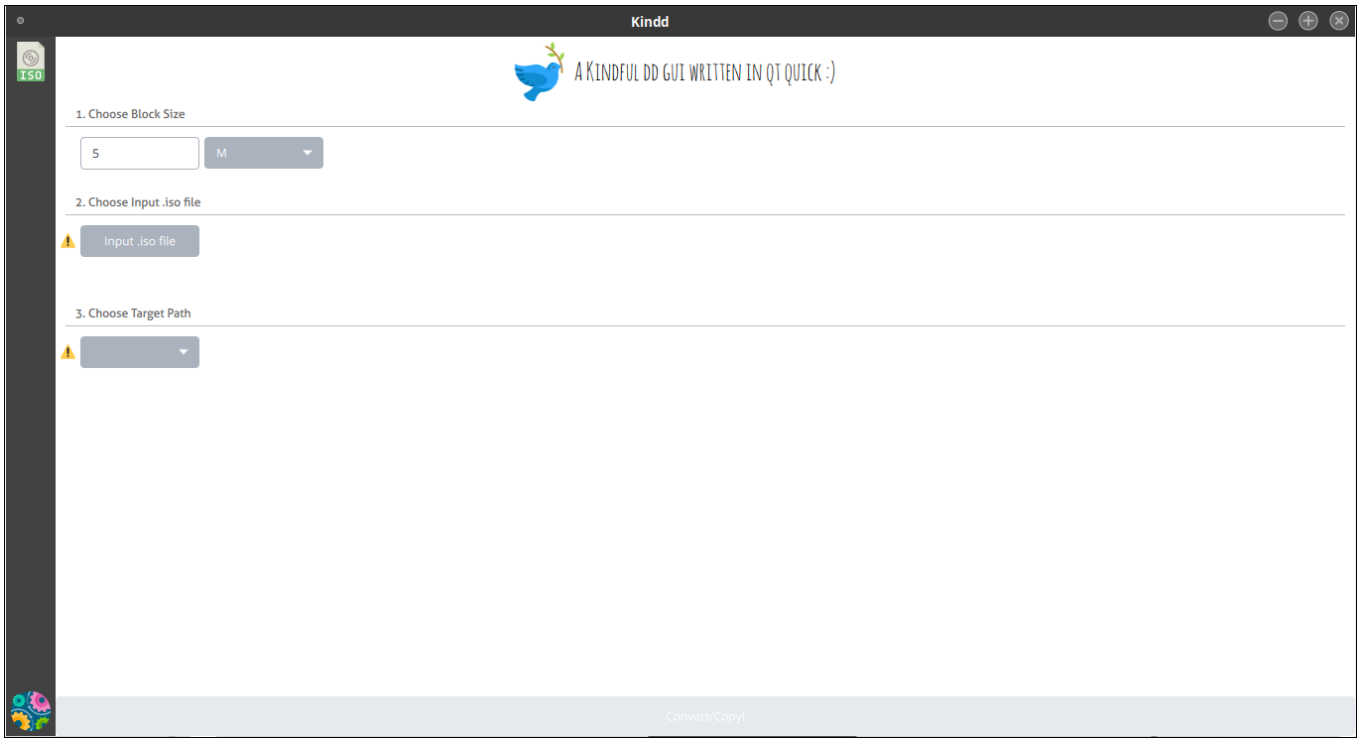
и выполните команду:

```
dnf install kindd
```

После установки запуск утилиты доступен из «**Главного меню**» - «**Стандартные**» - «**Графическая оболочка для dd**» или через терминал командой:

```
kindd
```

После запуска откроется окно утилиты:



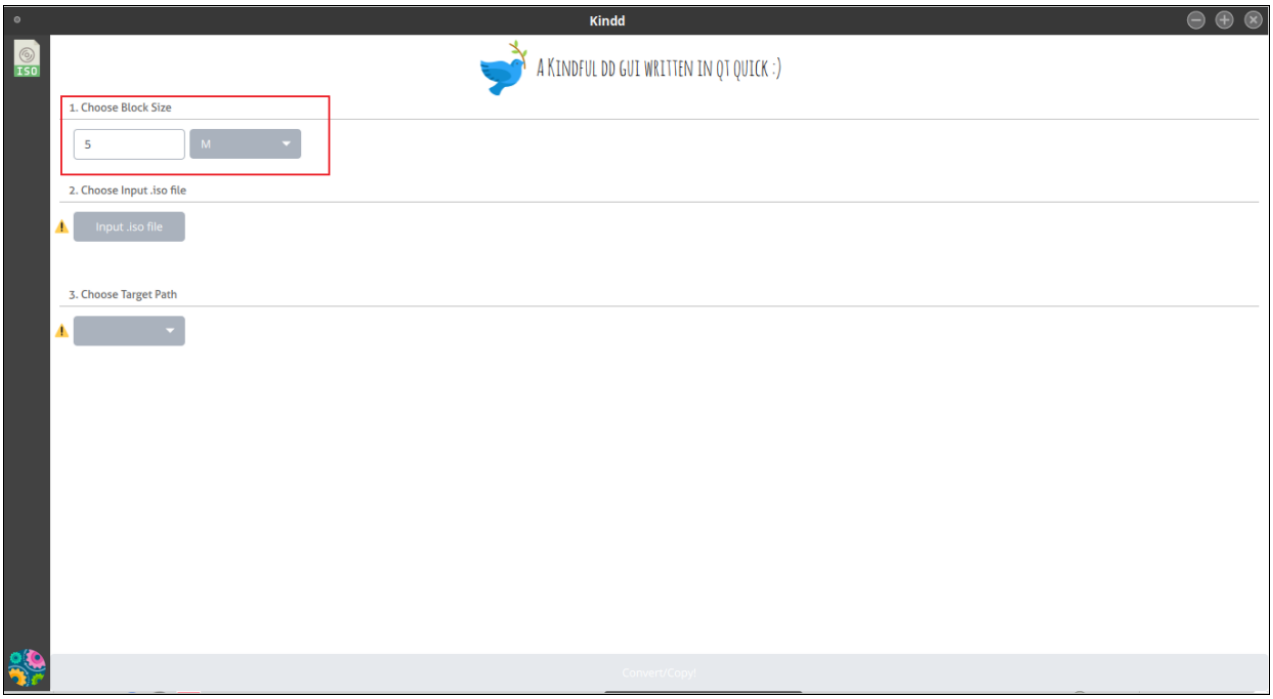
Алгоритм работы с kindd

Интерфейс **kindd** состоит из двух разделов: «**Создать загрузочный .iso**» (открывается по умолчанию) и «**Настройки**». На вкладке «**Настройки**» устанавливаются параметры внешнего вида программы.

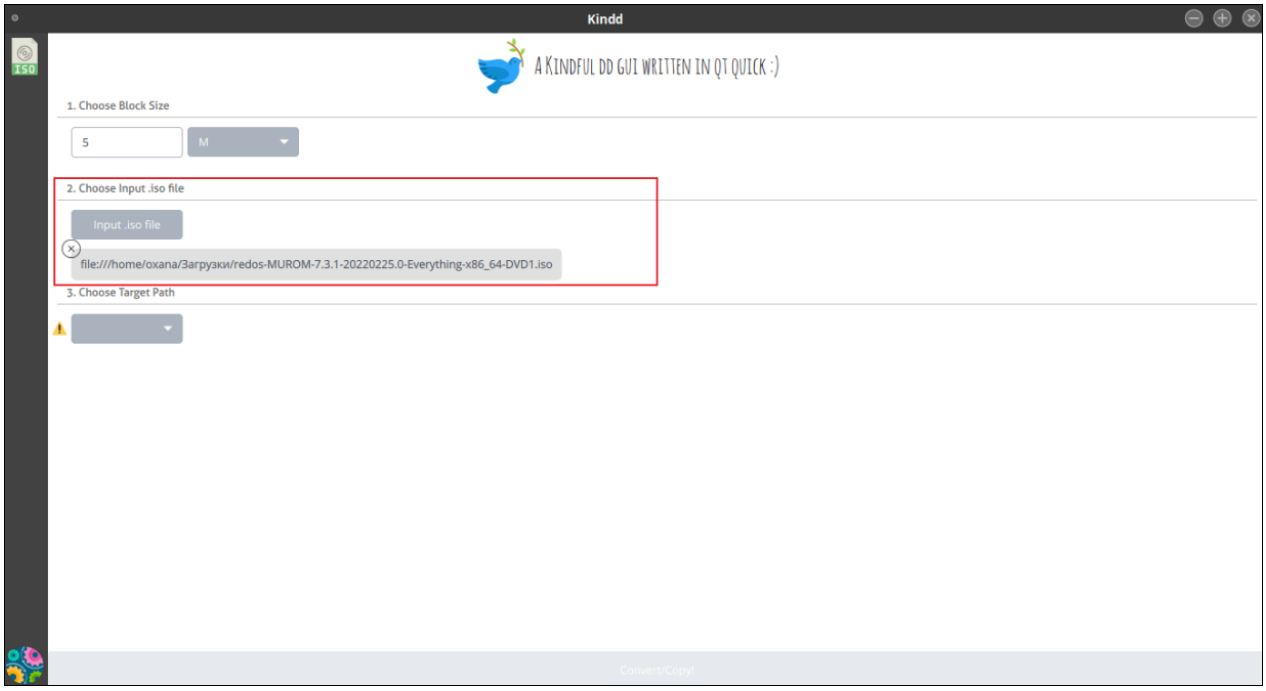
Для работы с утилитой понадобится USB-накопитель и ISO-файл.

Чтобы создать загрузочный USB-накопитель из ISO, подключите USB-накопитель, а затем запустите **kindd**.

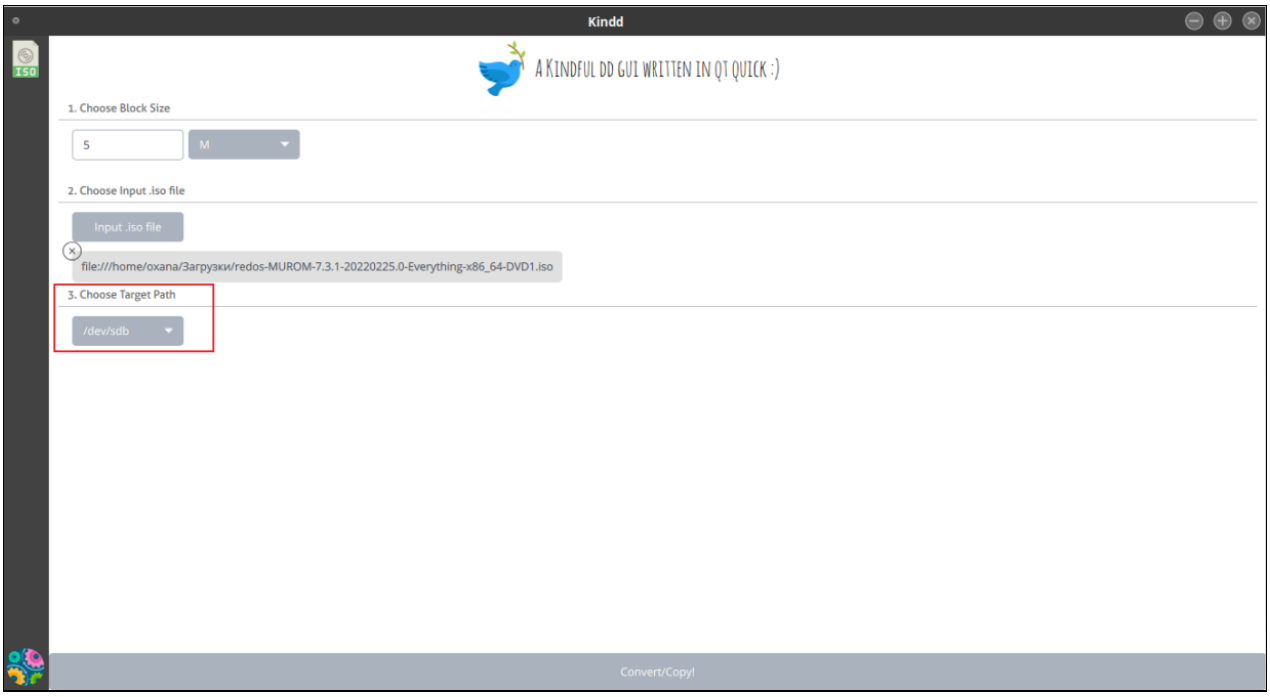
1. Укажите размер блока записи (можно оставить по умолчанию).



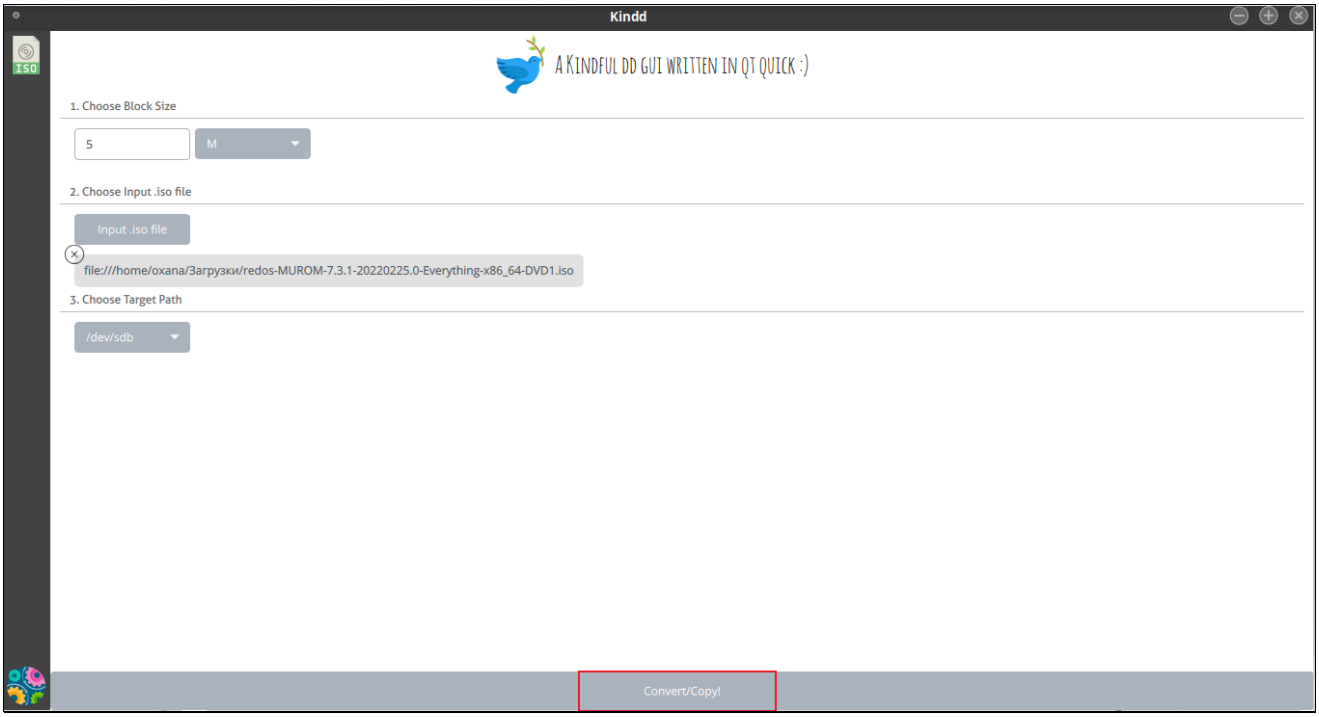
2. Выберите путь к файлу ISO.



3. Выберите устройство для записи.



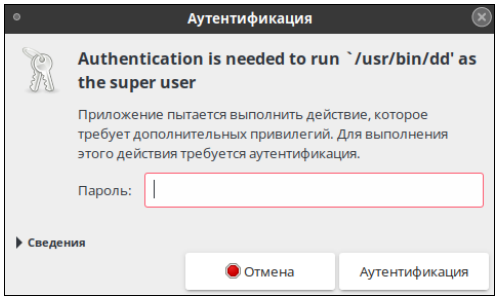
4. Нажмите кнопку **Convert/Copy**, чтобы начать создание загрузочного ISO.



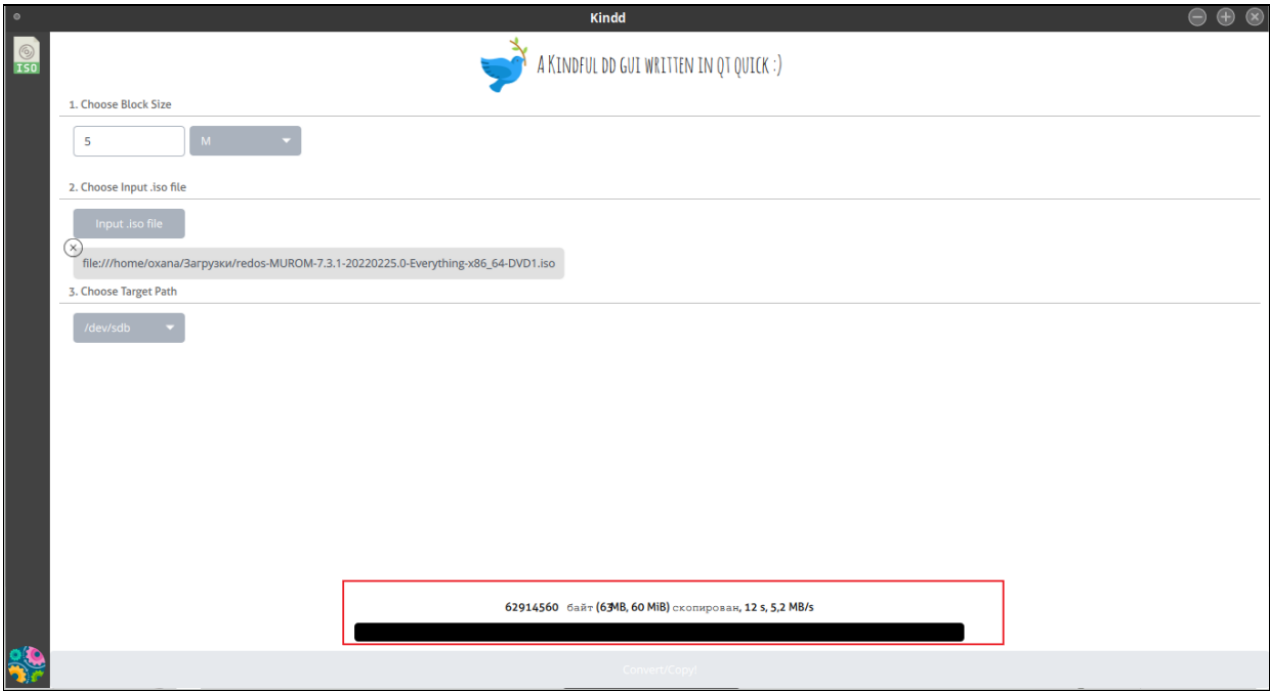
5. Появится сообщение: «**Вы уверены, что хотите продолжить?**» Нажмите «**Yes, i'm sure**».



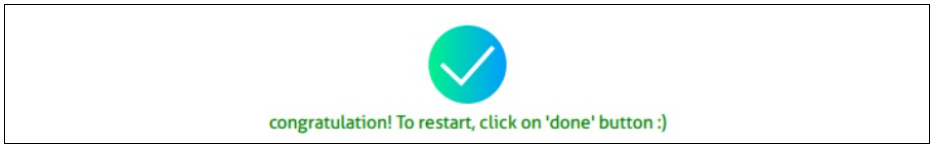
6. Далее необходимо ввести пароль суперпользователя.



7. После успешной аутентификации начнется загрузка:



8. При успешном завершении записи вы увидите следующее сообщение:



После этого можно проверить загрузку системы с USB-устройства.

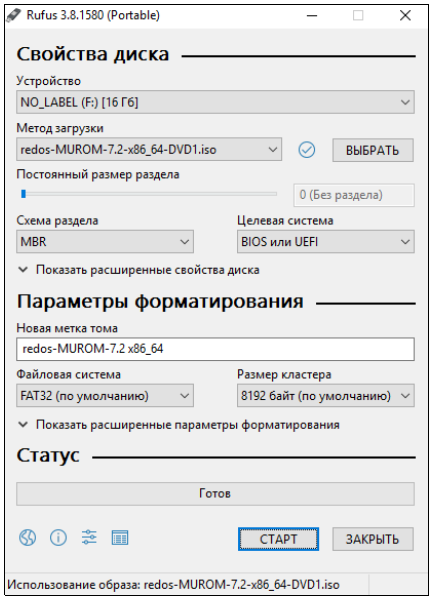
5 способ - Rufus для Windows

Примечание.

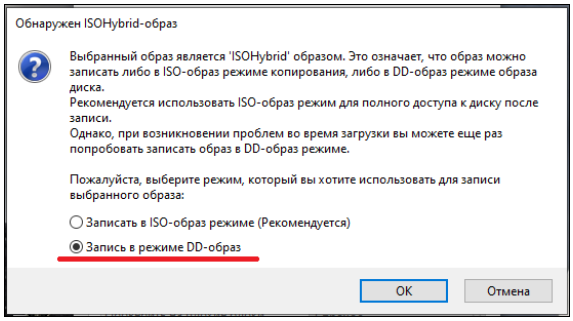
Если для установки РЕД ОС планируется использовать образ **live-usb**, то запись установочного образа с использованием ПО **Rufus** нужно производить в режиме **ISO**.

Для записи iso-образов в **Windows** на flash-накопитель можно воспользоваться утилитой **Rufus**, которая доступна по ссылке.

Из списка «**Устройство**» необходимо выбрать ваше устройство, затем нажать кнопку «**Выбрать**».

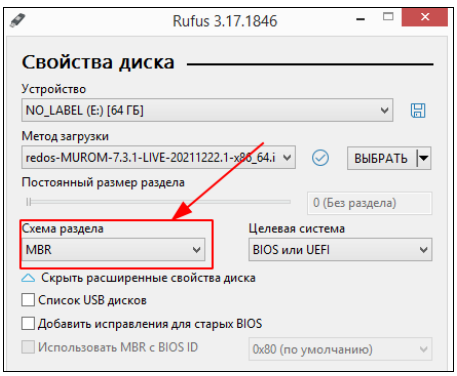


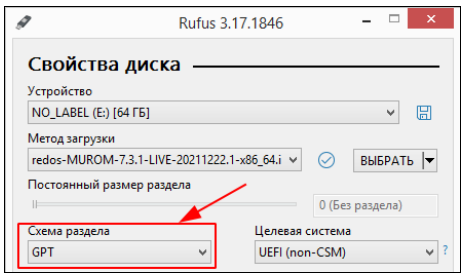
При записи образа РЕД ОС через Rufus, необходимо выбрать режим **DD**. Окно с запросом о выборе режима появляется после нажатия кнопки «**СТАРТ**».



Также при создании загрузочного носителя обратите внимание, что схема разделов загрузочного носителя должна совпадать со схемой разделов жёсткого диска вашего ПК.

Если на жёстком диске вашего ПК используется схема разделов **MBR**, то при создании образа в пункте «**Схема раздела**» необходимо выставить параметр «**MBR**». Соответственно, если вы используете ПК со схемой разделов жёсткого диска с **GPT**, то при создании образа в пункте «**Схема раздела**» необходимо выставить параметр «**GPT**».





6 способ - Brasero

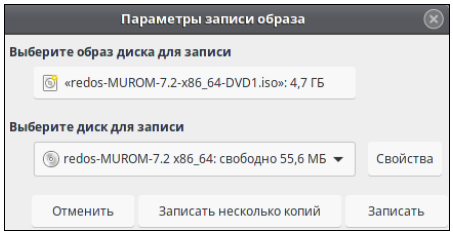
Для записи iso-образов на CD/DVD используйте приложение «**Brasero**». Если **Brasero** не установлено, его можно установить командой:

```
dnf install brasero
```

Приложение открывается из «**Меню**» - «**Аудио и видео**» - «**Brasero**».

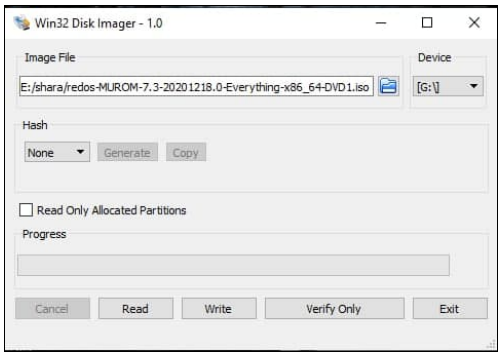
В приложении выберите пункт записать образ.

В открывшемся окне выберите iso-образ и диск.



7 способ - win32 disk imager для Windows

Для записи iso-образов в **Windows** на flash можно также воспользоваться утилитой **win32 disk imager**, которая доступна по ссылке.

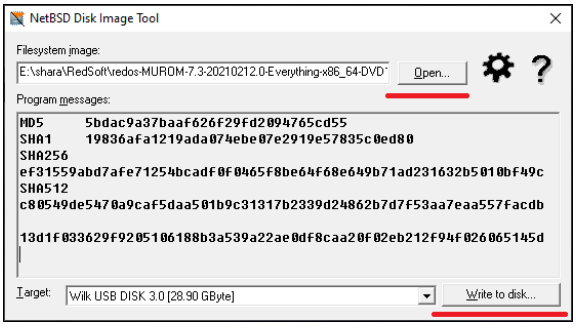


В открывшемся окне выберите iso-образ, flash-накопитель (в поле **Device**) и нажмите кнопку «**Write**».

8 способ - rawrite32 для Windows

Еще один способ для записи iso-образов в **Windows** на flash - использование утилиты **rawrite32**, которая доступна по ссылке.

Все что нужно сделать, это выбрать образ, flash-накопитель (в поле **Target**) и нажать «**Write to disk**».



Последовательность установки

До того, как будет произведена установка РЕД ОС на жесткий диск СВТ, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования СВТ завершилась успешно, будет запущен псевдографический интерфейс программы-установщика (**anaconda**). Процесс установки реализован в виде «мастера» установки, который представляет из себя интерактивный графический интерфейс, в котором пользователю предлагается отвечать на вопросы и указывать необходимые опции РЕД ОС. Мастер установки разделен на шаги, каждый шаг посвящен настройке или установке определенного сервиса системы. Шаги нужно проходить последовательно, переход к следующему шагу происходит по нажатию кнопки «**Далее**». При помощи кнопки «**Назад**», при необходимости, можно вернуться к уже пройденному шагу и изменить настройки. На некоторых этапах установки возможность перехода к предыдущему шагу ограничена теми шагами, где нет зависимости от данных, введенных ранее.

Если по каким-то причинам возникла необходимость прекратить установку, нажмите ***Reset*** на системном блоке компьютера. Помните, что совершенно *безопасно* прекращать установку только до шага «**Подготовка диска**», поскольку до этого момента не производится никаких изменений на жестком диске. Если прервать установку между шагами «**Подготовка диска**» и «**Установка загрузчика**», вероятно, что после этого с жесткого диска не сможет загрузиться ни одна из установленных систем.

Технические сведения о ходе установки можно посмотреть, нажав *«Ctrl+Alt+F1»*, вернуться к программе установки - *«Ctrl+Alt+F6»*. По нажатию *«Ctrl+Alt+F2»* откроется отладочная виртуальная консоль.

Во время установки РЕД ОС выполняются следующие шаги:

- Выбор типа накопителя СВТ;
- Присвоение имени компьютера в сети и настройка сетевых интерфейсов;
- Выбор часового пояса;
- Задание пароля администратора системы;
- Подготовка разделов диска;
- Выбор типа установки: сервер или рабочая станция;
- Установка системы;
- Установка загрузчика;
- Перезагрузка системы;
- Лицензионный договор;
- Создание системного пользователя;
- Установка даты и времени;
- Сохранение настроек;
- Завершение установки.

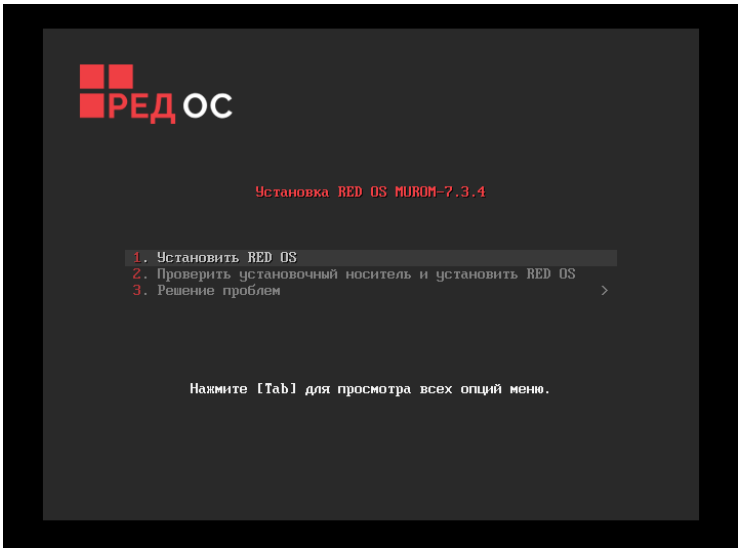
Начало установки

Системные требования

Системные требования к составу технических средств приведены в нашей статье «Системные требования».

Начало установки

Перед началом установки РЕД ОС необходимо настроить BIOS рабочей станции на загрузку с носителя информации (DVD-диска или флеш-накопителя), куда записан дистрибутив. Способ входа в меню BIOS и расположение конкретных настроек может сильно отличаться, в зависимости от используемой материнской платы оборудования рабочей станции. Чаще всего для входа в BIOS необходимо нажать функциональную клавишу *Delete* на стационарных рабочих станциях или функциональную клавишу *F1 (F9)* на мобильных рабочих станциях (ноутбуках) в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.



Загрузка с установочного носителя начинается с меню, в котором перечислено несколько вариантов загрузки, причем установка системы - это только одна из возможностей. Из данного меню можно:

- запустить тестирование носителя данных и только после этого перейти к процедурам установки ОС;
- используя меню «**Решение проблем**», запустить проверку памяти и диагностику оборудования;
- запустить уже установленную ОС на жестком диске;
- загрузить ОС в аварийном режиме.

Манипулятор графической информации (мышь) на этом этапе установки не поддерживается, поэтому для выбора различных вариантов и опций установки необходимо воспользоваться функциональными клавишами клавиатуры - стрелками. Можно скорректировать параметры запуска любого пункта начального меню установки РЕД ОС, нажав функциональную клавишу клавиатуры *TAB.*

Установка РЕД ОС автоматически осуществляется в графическом режиме с выводом текстовой информации на выбранном в начале процесса установки языке.

По умолчанию при установке используется графический видеорежим (разрешение экрана) 800x600. При возникновении проблем запуска установки в графическом режиме существует возможность альтернативной установки системы - не графический (текстовый) режим. Подробнее об установке РЕД ОС в текстовом режиме см. в нашей статье «Установка РЕД ОС в текстовом режиме».

Чтобы начать процесс установки, нужно клавишами перемещения курсора «вверх»/«вниз» выбрать пункт меню «**Установить RED OS**» и нажать *Enter.* В начальном загрузчике установлено небольшое время ожидания продолжительностью 1 минута. Если в этот момент не предпринимать никаких действий, то будет загружена установка системы с проверкой установочного носителя. Если пропущен нужный момент, нужно перезагрузить компьютер и до истечения установленного времени ожидания выбрать нужный пункт в меню загрузчика.

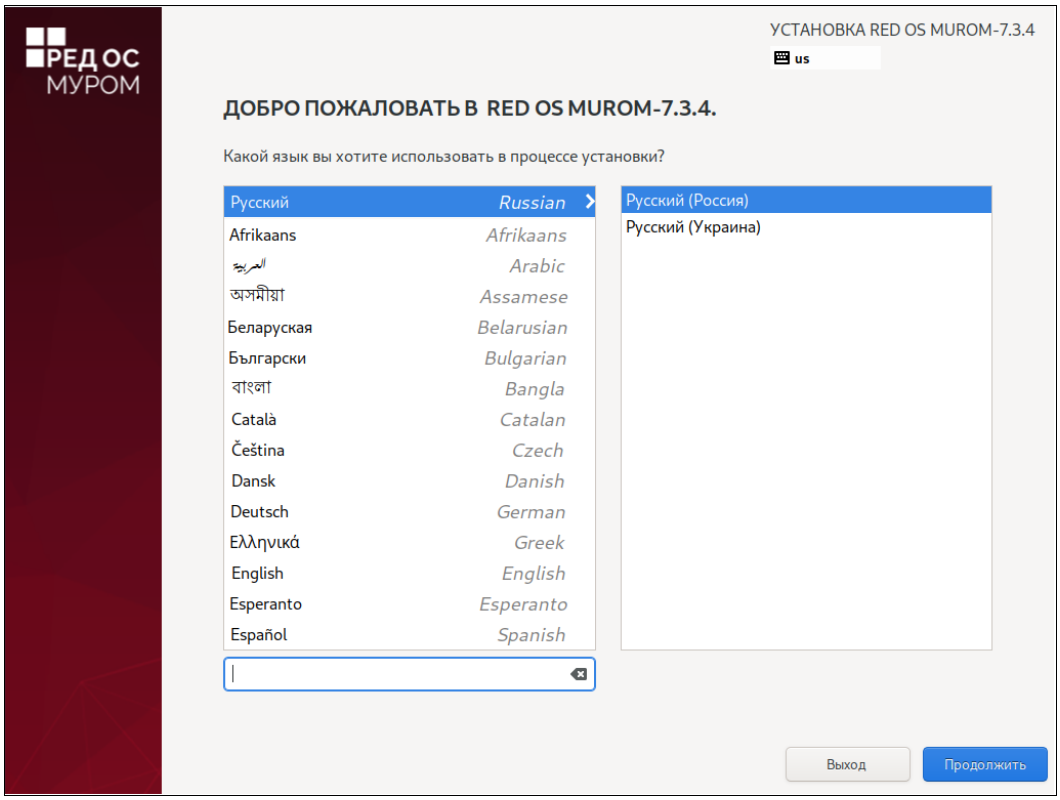
Начальный этап установки не требует вмешательства пользователя: происходит автоматическое определение оборудования и запуск компонентов программы установки. Прервать начальный этап установки и вернуться в начальное меню установки РЕД ОС можно, нажав клавишу *ESC.*

Язык интерфейса программы установки

Язык интерфейса программы установки можно выбрать на самом первом этапе процесса установки. Язык устанавливаемой РЕД ОС будет русским, если был выбран русский язык, или английским, если был выбран любой другой язык.

Дополнительным языком РЕД ОС является английский язык. Другие дополнительные языковые пакеты можно установить из репозитория после завершения установки РЕД ОС.

Переключение раскладки клавиатуры при установке РЕД ОС и в графическом интерфейсе РЕД ОС выполняется нажатием комбинации функциональных клавиш *«Alt+Shift»*.



Обзор установки

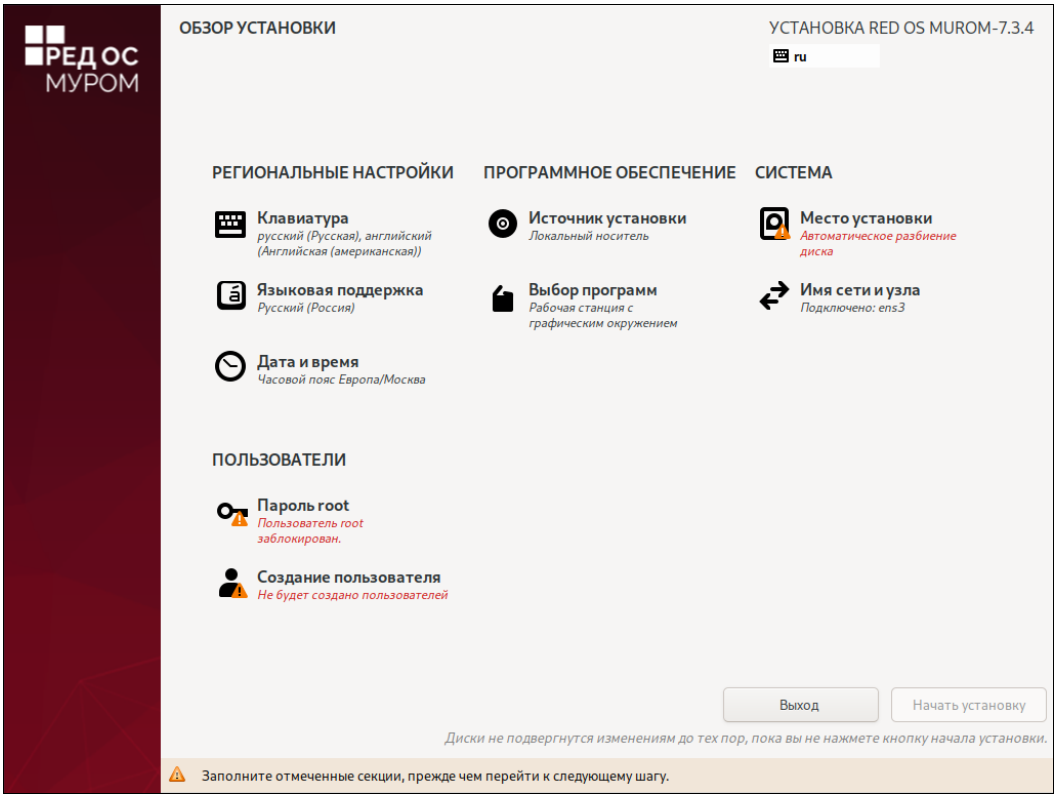
Дата и время
Клавиатура
Языковая поддержка
Источник установки
Выбор программ
Место установки
Сеть и имя узла
Создание пароля администратора

Вы можете подробнее ознакомиться с каждым этапом установки системы, просмотрев наши обучающие видео:

- на **RuTube** — Установка РЕД ОС;
- в **Яндекс.Дзен** — Установка РЕД ОС;
- в **VK Видео** — Установка РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

После выбора языка необходимо произвести первоначальную конфигурацию установщика и параметров будущей системы.

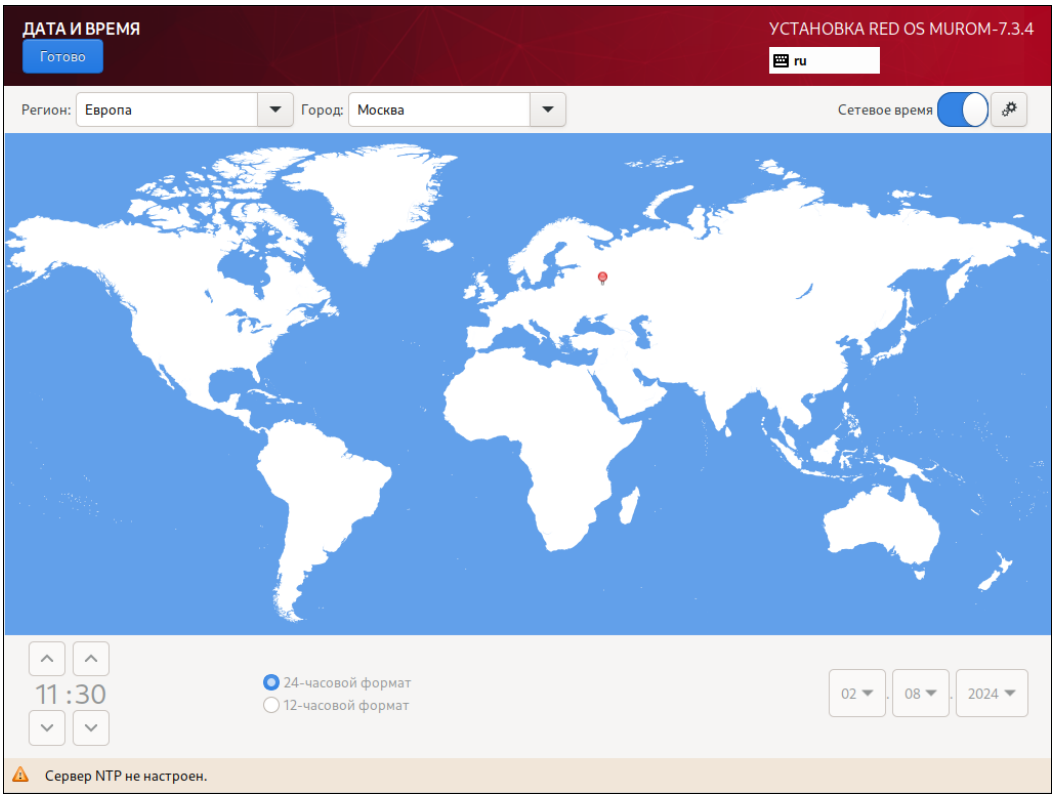


В этом окне необходимо задать региональные настройки, состав программного обеспечения и системные настройки. Здесь и в последующих окнах установщика красным цветом выводятся подсказки у тех вкладок, которые должны быть обязательно заполнены до перехода к следующему шагу установки.

Рассмотрим подробнее каждую вкладку окна.

Дата и время

В окне настройки даты и времени можно выбрать текущий регион и город и установить используемое локальное время, дату и формат времени.



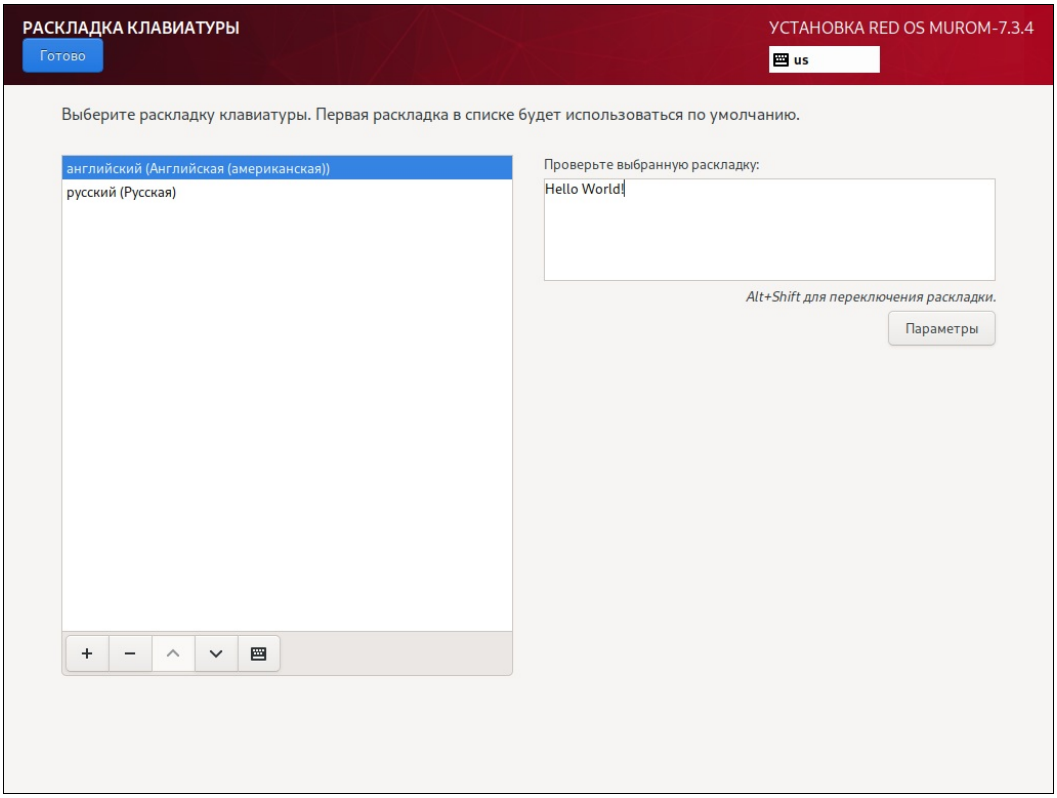
Если установлена сеть, и есть доступ к глобальной сети, можно разрешить автоматическую настройку времени с помощью службы **ntp** — сетевое время.

Данную настройку можно изменить после завершения установки РЕД ОС. По умолчанию устанавливается часовой пояс UTC+03:00 (Европа/Москва).

Здесь и далее возврат в предыдущее меню осуществляется с помощью кнопки «Готово».

Клавиатура

В окне настройки клавиатуры можно выбрать используемые в ОС раскладки.

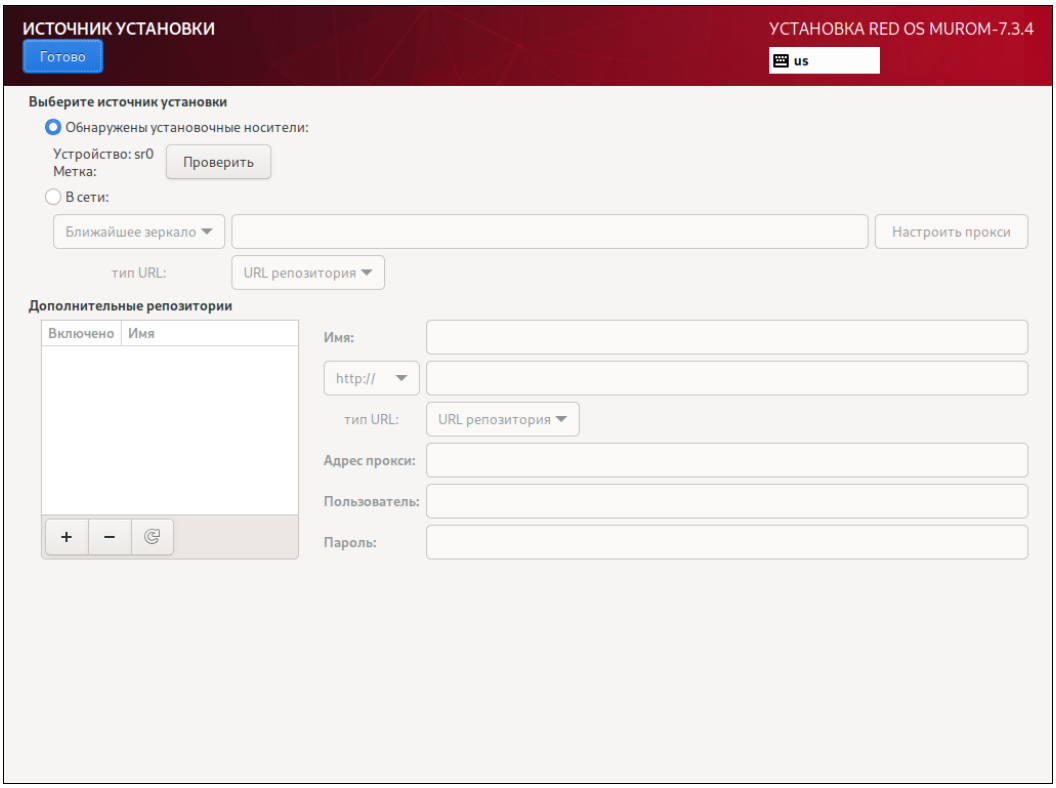


В отдельном поле ввода можно проверить корректность отображения вводимых символов.

Первая раскладка в списке будет использоваться по умолчанию.

Источник установки

В меню выбора источников установки можно задать, откуда система будет получать пакеты в процессе установки.

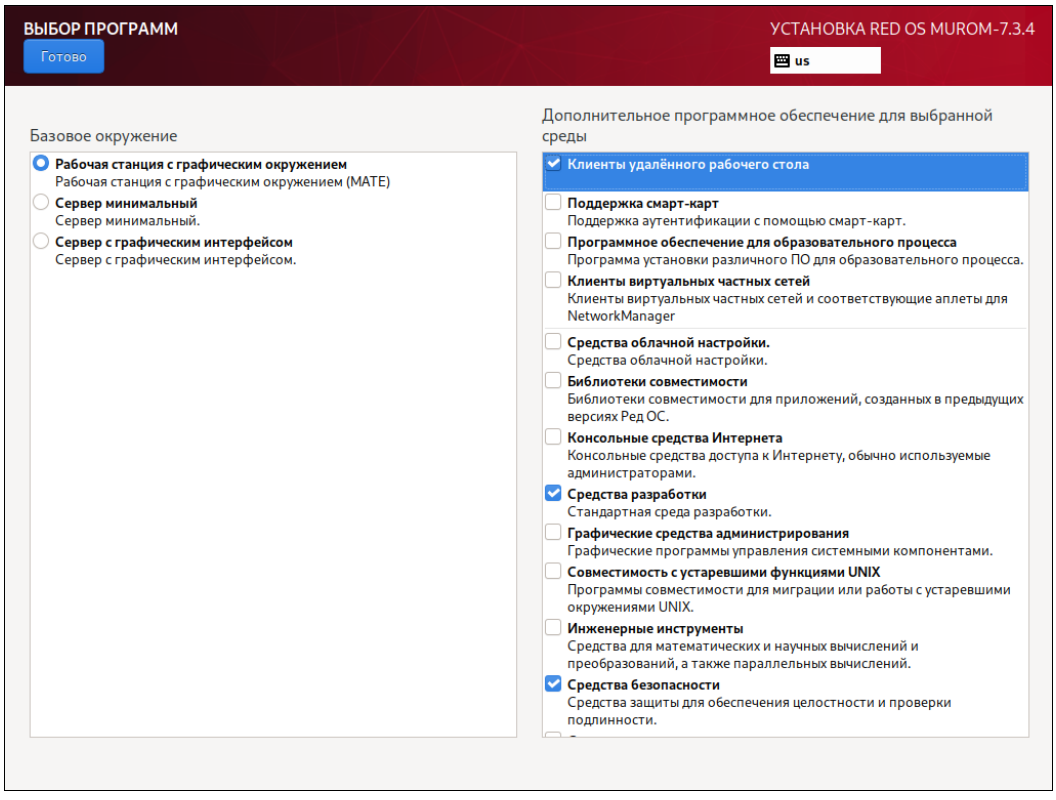


Источниками установки могут быть локальные носители или сетевые источники.

Выбор программ

В меню выбора программ можно задать, какая конфигурация из числа базового окружения будет установлена:

- рабочая станция,
- сервер минимальный,
- сервер с графическим интерфейсом.



Дополнительно для каждой из выбранных конфигураций можно настроить группы пакетов, которые будут установлены.

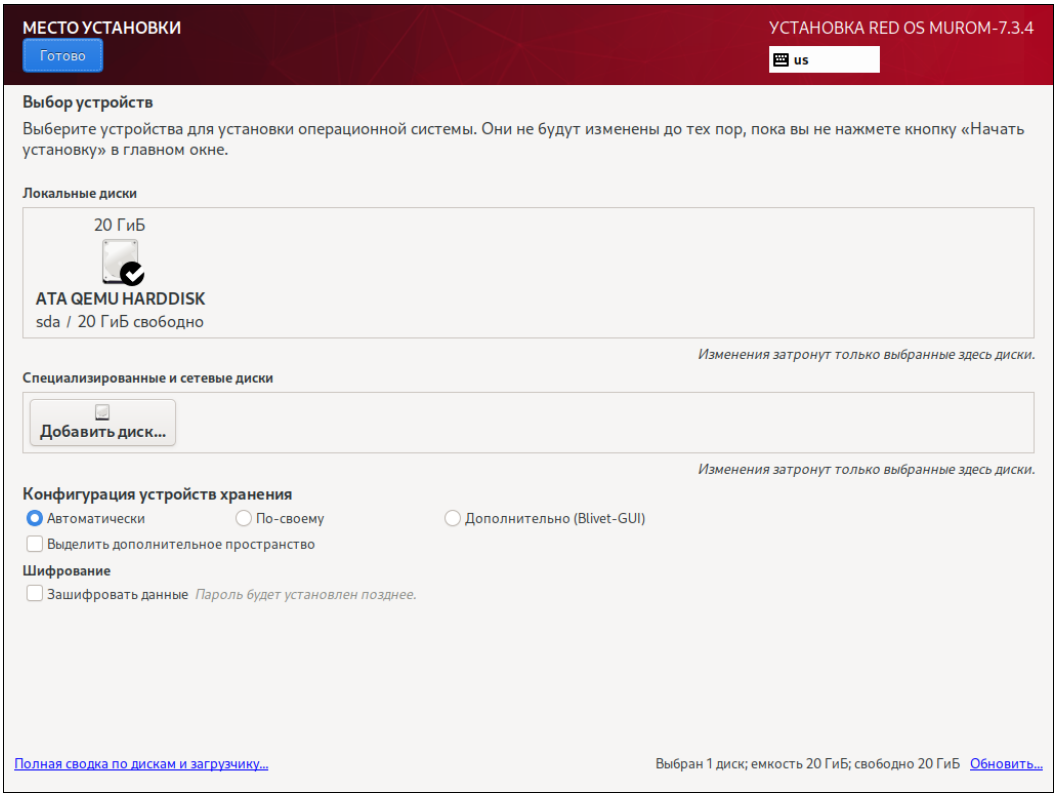
В любом дистрибутиве Linux доступно значительное количество программ (до нескольких тысяч), часть из которых составляет саму ОС, а все остальные - это прикладные программы и утилиты.

В РЕД ОС все операции установки и удаления производятся над пакетами - отдельными компонентами системы. Пакет и программа соотносятся неоднозначно: иногда одна программа состоит из нескольких пакетов, иногда один пакет включает несколько программ.

В процессе установки РЕД ОС обычно не требуется детализированный выбор компонентов на уровне пакетов - это требует слишком много времени и знаний от проводящего установку. Тем более, что комплектация дистрибутива подбирается таким образом, чтобы из имеющихся программ можно было составить полноценную рабочую среду для соответствующей аудитории пользователей. Поэтому в процессе установки РЕД ОС пользователю предлагается выбрать из небольшого списка конфигураций, объединяющих пакеты, необходимые для решения наиболее распространённых задач.

Место установки

В меню выбора расположения установки можно выбрать устройство для установки операционной системы.



Переход к этому шагу может занять некоторое время. Время ожидания может быть разным и зависит от производительности компьютера, объёма и типов используемых накопителей, количества существующих разделов на них.

На этом этапе подготавливается площадка для установки РЕД ОС, в первую очередь - выделяется свободное место на диске.

Можно выбрать и использовать профили разбиения диска. Профиль - это шаблон распределения места на диске для установки РЕД ОС.

Можно выбрать:

- автоматически;
- по-своему;
- дополнительно (Blivet-GUI).

Первый профиль предполагает автоматическое разбиение диска. Будет выбрано оптимальное расположение ОС. Необратимые изменения разделов на жёстком диске требуют подтверждения со стороны пользователя. После подтверждения внесённые изменения сохраняются на жестком диске/дисках СВТ.

Если для применения одного из профилей автоматической разметки доступного места окажется недостаточно, будет выведено сообщение о невозможности выполнения операции разбиения диска.

При необходимости можно освободить часть дискового пространства, для этого следует воспользоваться профилем разбиения вручную. Можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «Готово» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке «Файловая система».

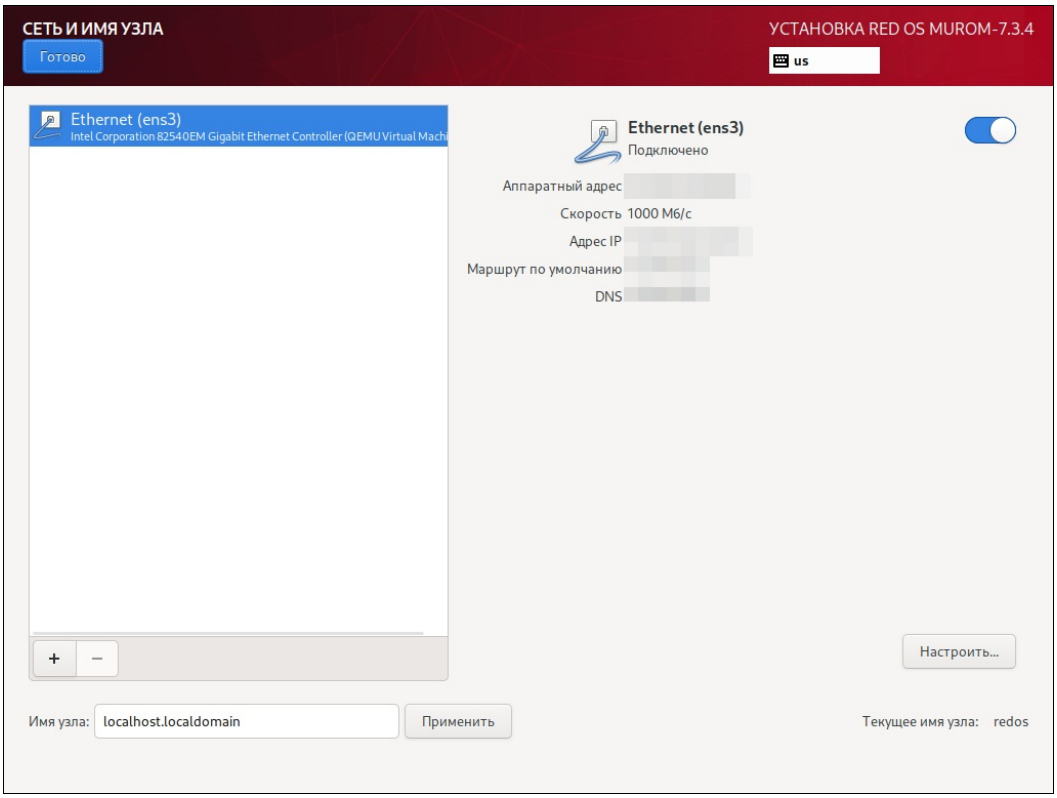
ВАЖНО!

Не следует форматировать разделы с теми данными, которые необходимо сохранить, например, с пользовательскими данными (/home) или с другими операционными системами. С другой стороны, отформатировать можно любой раздел, который необходимо «очистить» (т.е. удалить все данные).

Blivet-gui является обособленной реализацией механизмов управления разделами и дисками, снабжённой привычным интерфейсом в стиле **GParted**. Программа поддерживает управление дисковыми разделами и хранилищами **LVM2** (включая шифрованные разделы LUKS, логические тома и группы томов). Так же как и в **GParted**, изменения в **blivet-gui** применяются не сразу, а после подтверждения внесённого набора изменений.

Сеть и имя узла

В меню выбора настройки сети можно активировать соединение с сетью и задать имя узла.



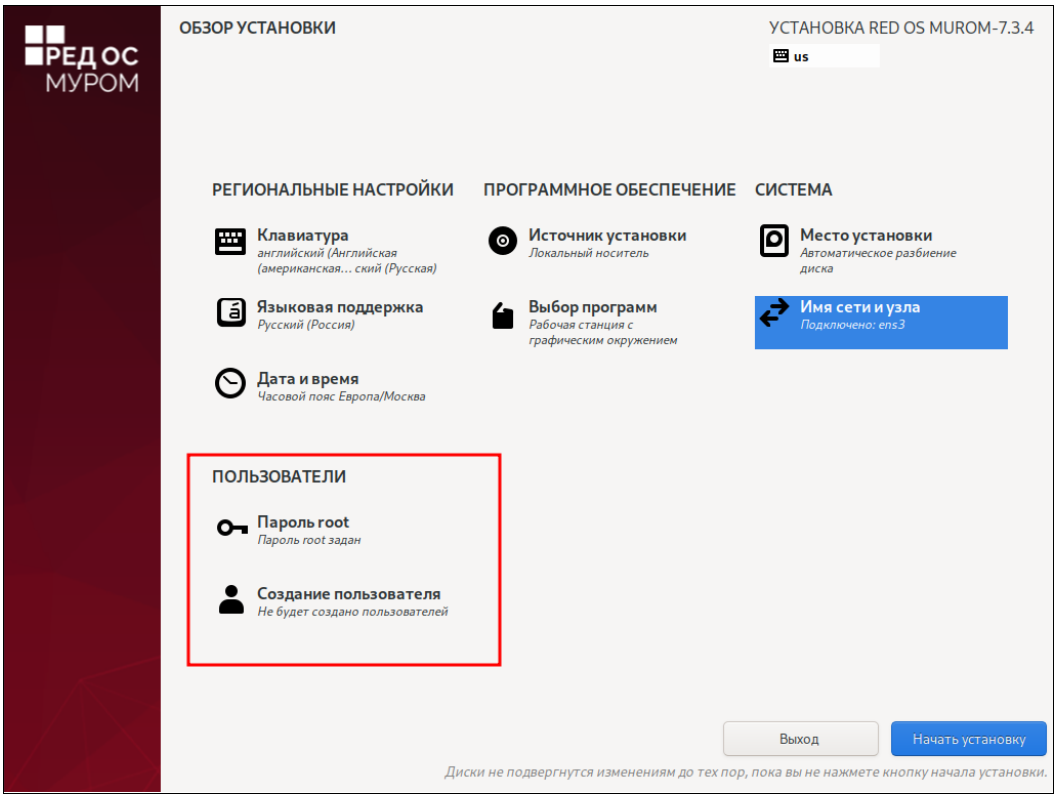
На данном этапе необходимо задать имя компьютера в сети (хоста). При наличии сети имя компьютера используется для однозначного определения каждого компьютера. Имя компьютера состоит непосредственно из имени компьютера и имени домена в сети, к которому принадлежит компьютер. Имя компьютера и имя домена разделяются знаком «.» . При наличии домена сети имя должно даваться полностью. При отсутствии сети домену также может быть дано произвольное имя.

В качестве букв в имени компьютера разрешаются только буквы латиницы. В имени компьютера не допускается использование заглавных букв, пробелов и специальных символов.

Также на данном этапе можно сконфигурировать параметры настройки сетевых интерфейсов: автоматическое включение интерфейсов, MAC-адреса сетевых интерфейсов, параметры сетевых протоколов.

Создание пароля администратора

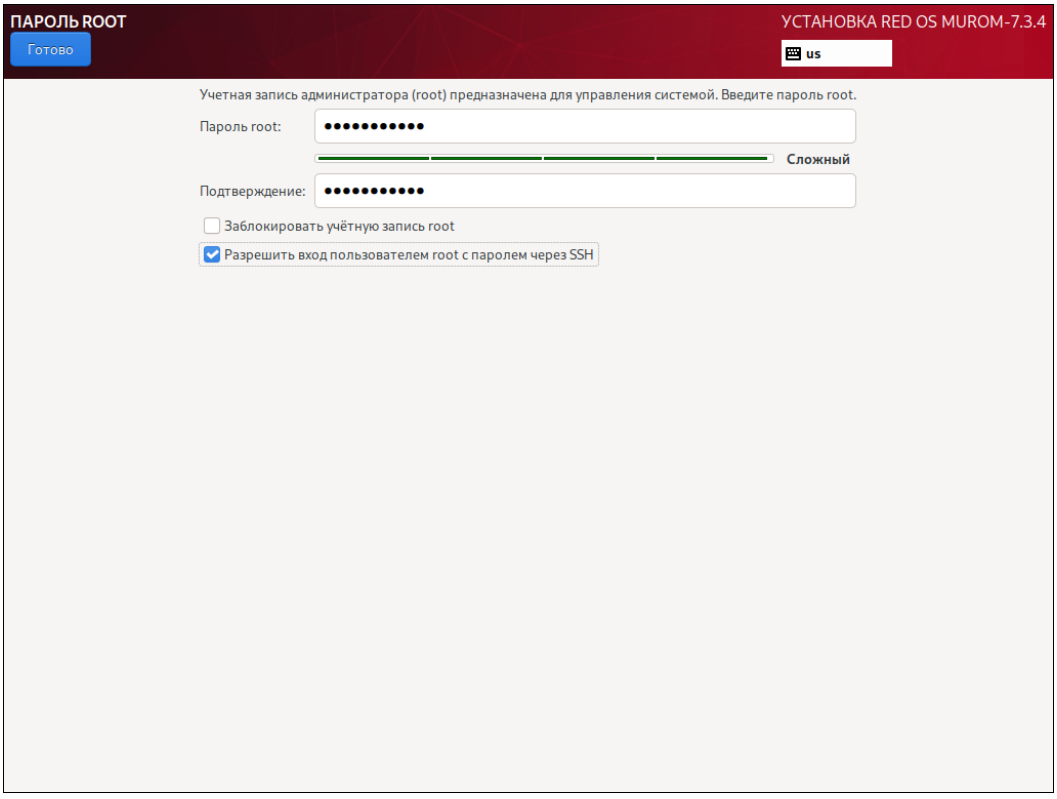
После того как предварительная настройка системы завершена, начинается непосредственная установка системы. Параллельно с установкой необходимо настроить пароль администратора **root** и, при необходимости, создать учетные записи пользователей.



РЕД ОС - это многопользовательская операционная система. На практике это означает, что для работы в системе нужно в ней *зарегистрироваться*, т.е. дать понять системе, кто именно находится за монитором и клавиатурой. Наиболее распространённый способ регистрации на сегодняшний день - использование системных имён (**login name**) и паролей. Это надёжное средство убедиться, что с системой работает тот, кто нужно, если пользователи хранят свои пароли в секрете и если пароль достаточно сложен и не слишком короток (иначе его легко угадать или подобрать).

В любой системе Linux всегда присутствует один специальный пользователь - администратор, он же суперпользователь или администратор РЕД ОС, для него зарезервировано стандартное системное имя - **root**.

Необходимо запомнить пароль **root** - его нужно будет вводить, чтобы получить право изменять настройки системы с помощью стандартных средств настройки РЕД ОС.

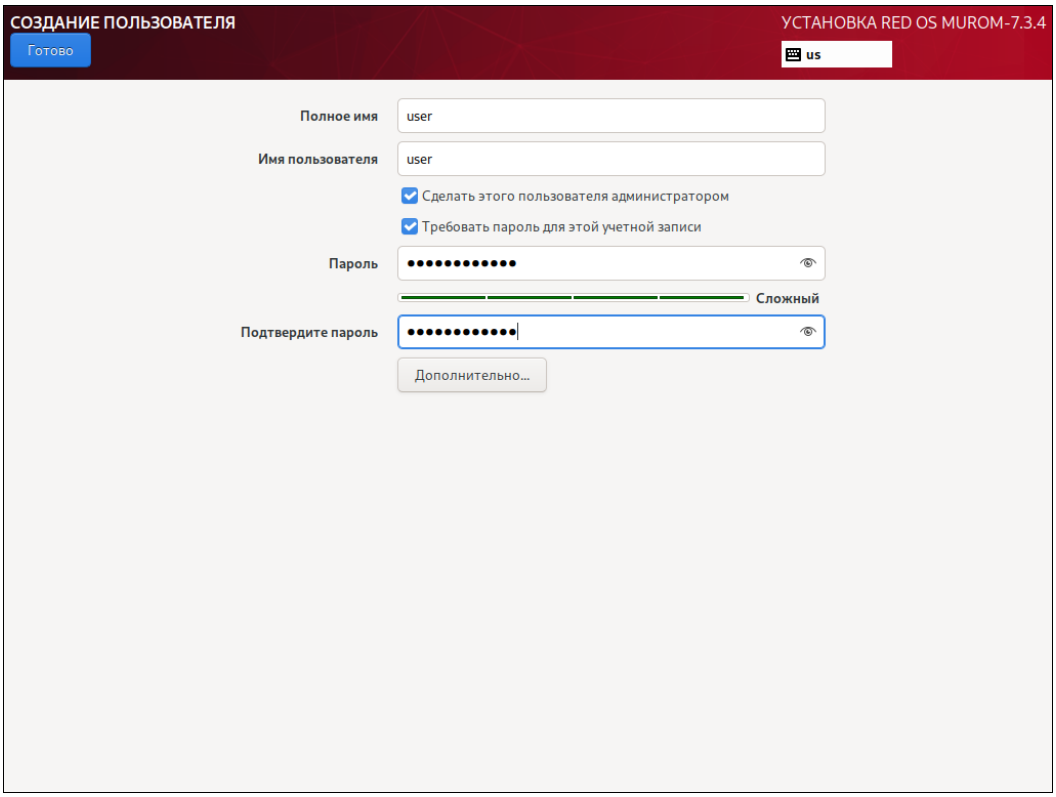


Ввод пароля защищен, при наборе пароля вместо символов на экране отображаются специальные символы. Чтобы избежать опечатки при вводе пароля, его предлагается ввести дважды. К введенному паролю в режиме реального времени применяется политика сложности пароля, т.е. производится его проверка, и при слишком простом пароле или совпадении пароля с парольной последовательностью из словаря паролей системой будет предложено произвести смену пароля администратора РЕД ОС.

Администратор отличается от всех прочих пользователей тем, что ему позволено производить любые, в том числе самые разрушительные, изменения в системе. Поэтому выбор пароля администратора РЕД ОС - очень важный момент для безопасности: любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе. Даже ваши собственные неосторожные действия от имени **root** могут иметь катастрофические последствия для всей системы.

Помимо администратора РЕД ОС (**root**) в систему необходимо добавить, по меньшей мере, одного обычного пользователя. Работа от имени администратора РЕД ОС считается опасной (можно по неосторожности повредить систему), поэтому повседневную работу в РЕД ОС следует выполнять от имени обычного пользователя, полномочия которого ограничены.

При добавлении пользователя предлагается ввести имя учётной записи (login name) пользователя. Имя учётной записи всегда представляет собой одно слово, состоящее только из строчных латинских букв (заглавные запрещены), цифр и символа подчёркивания «_» (причём цифра и символ «_» не могут стоять в начале слова). Чтобы исключить опечатки, пароль пользователя вводится дважды. Так же, как при выборе пароля администратора РЕД ОС (**root**), действуют требования по сложности пароля.



В процессе установки предлагается создать только одну учётную запись обычного пользователя - чтобы от его имени системный администратор РЕД ОС мог выполнять задачи, которые не требуют привилегий суперпользователя.

Учётные записи для всех прочих пользователей системы можно будет создать в любой момент после её установки.

Ручная разметка диска

Общая информация
Схемы разметки дисков
Создание разделов, описание интерфейса разметки
Как создать и зачем выделять home?
Разделы swap, boot, home
Пример с размещением home на отдельном диске
Сохранение раздела /home

Общая информация

Прежде чем приступить к разметке дисковой подсистемы при установке ОС, вспомним про устройство файловой системы РЕД ОС.

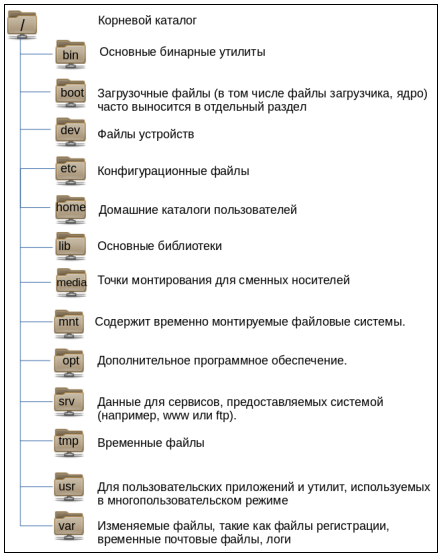


Рисунок 1 - Описание иерархии каталогов

Как мы можем видеть из рисунка, каждый каталог используется под определенные задачи. При установке РЕД ОС в ручном режиме разметки диска можно определенным образом организовать дисковое пространство под ОС, например, для основного корневого раздела **/** , директорий **/home**, **/boot** или **/var** выделить отдельные разделы диска или вообще вынести какой-либо каталог на отдельный диск.

Такое разбиение изолирует их один от другого, что может быть полезным в случае, например, если на домашнем (**/home**) каталоге, вынесенном на отдельный раздел, закончится место, то система все еще сможет нормально работать, потому что это никак не касается корневого раздела. Также, в целях удобства, выделение для **home** отдельного раздела позволит переустановить операционную систему, сохранив пользовательские данные. Таким образом, каталоги могут быть разграничены не только по задачам, но и по своему местонахождению: на разных разделах одного диска или разделах других дисков. Кроме того, ручная разметка дает возможность создавать программный **RAID** и более гибко настраивать файловую подсистему, чем в автоматическом режиме.

Вы можете подробнее ознакомиться с информацией по ручной разметке диска, просмотрев наши обучающие видео:

- на **RuTube** — Ручная разметка диска;
- в **Яндекс.Дзен** — Ручная разметка диска.
- в **VK Видео** — Ручная разметка диска.

На наших каналах вы также сможете найти много другой полезной информации.

Приступаем к разметке диска. В мастере установки ОС выберем жесткие диски для установки РЕД ОС. В нижнем правом углу виден признак количества выбранных дисков. Укажите «**Я настрою разделы**». В результате мы перейдем к ручной разметке дисков.

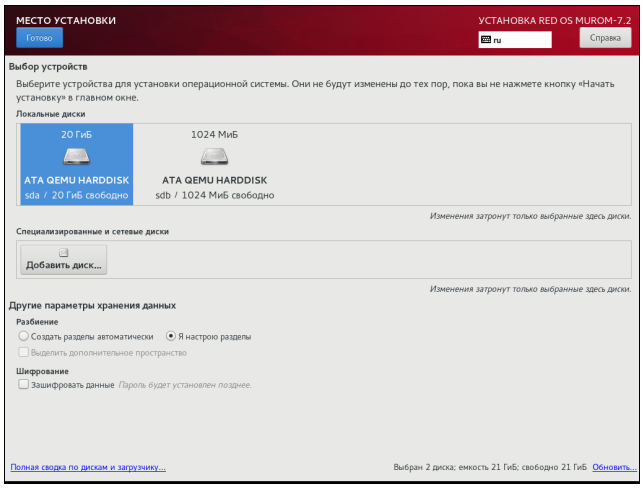


Рисунок 2 — Выбор дисков

На следующем шаге предлагается выбирать схему разбиения диска.

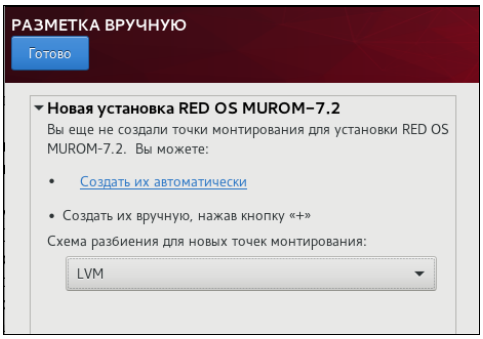


Рисунок 3 — Выбор схемы разбиения диска

Схемы разметки дисков

Стандартный раздел - позволяет создать обычные дисковые разделы, простые в управлении.

Btrfs (можно произносить как «*Butter FS*», «*Better FS*» или «*B-Tree FS*») - файловая система, которая может работать с большим числом файлов, файлами и томами гораздо большего размера, по сравнению с **ext2**, **ext3** и **ext4**, имеется поддержка снапшотов, сжатие и подтома.

Минусы: хотя **btrfs** активно развивается и перешла уже в статус стабильной, у пользователей все еще встречаются проблемы, приводящие к потере данных, а также высокая подверженность фрагментации.

LVM - позволяет создавать логические группы и тома хранения данных без непосредственной переразметки жесткого диска. Например, если у вас используется несколько жестких дисков, то при использовании LVM-разметки можно создать несколько или одну логическую группу, а в ней уже логические тома, которые в дальнейшем можно разбить на разделы и отформатировать под необходимую вам файловую систему — **ext4**, **ext3**, **ntfs** и другие.

Возможности:

- способность объединять диски в один логический том;
- изменение размера файловых систем, легкость при добавлении дисков в то время, когда система активна;
- использование RAID (чередование и зеркалирование);
- поддержка моментальных снимков;

Недостатки:

- сложность управления (предъявляются довольно высокие требования по администрированию файловой системы);
- трудный процесс восстановления данных в случае сбоя LVM из-за более сложных структур на диске;
- снимки сложны в использовании, медленны и содержат ошибки.

Динамический LVM - перераспределяет свободное пространство между устройствами в зависимости от требований программ и при необходимости пул пространства может наращиваться динамически.

Пример схемы LVM-разметки 4-х физических дисков, из которых, в свою очередь, создаются два физических тома, а из них одна большая логическая группа объемом, равным объему всех физ. дисков. В дальнейшем из группы VG создаются логические тома с точками монтирования см. Рисунок 4.

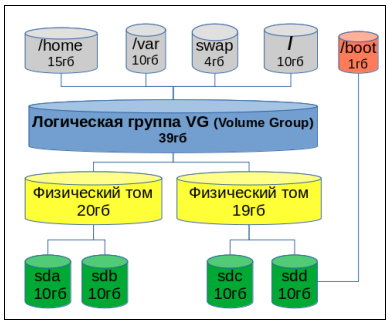


Рисунок 4 - Пример LVM-разметки дисков

Создание разделов, описание интерфейса разметки

Выберем схему со стандартной разметкой диска, которая является более простой, как в плане понимания, так и в сопровождении по сравнению с LVM.

Для обычных пользователей РЕД ОС рекомендуем создавать следующие разделы:

- **swap** (раздел для подкачки ОЗУ);
- **/boot** (загрузочный раздел);
- **/home** (данные пользователей);
- **/** (корневой раздел).

Выбираем схему разбиения «**Стандартный раздел**»,

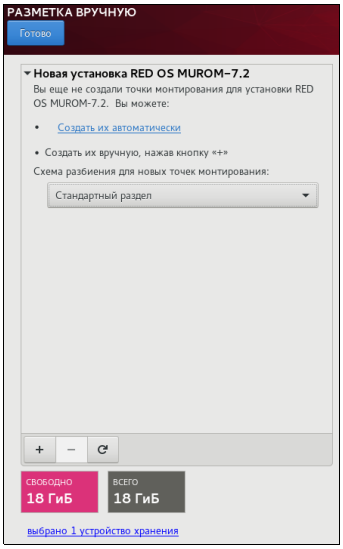


Рисунок 5 - Схема разбиения

далее можно создать все разделы вручную — кнопка плюс (**+**), кнопка минус (**-**) удаляет выбранный раздел.

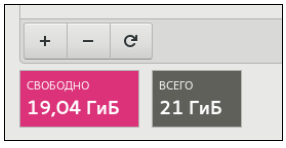


Рисунок 6 - Добавление разделов

Но если нажать на кнопку «**Создать их автоматически**», то в результате будут созданы все необходимые разделы для установки ОС: **boot**, **swap**, **/** и нам не придется их создавать, а останется выделить только раздел **/home** для домашнего каталога.

Как создать и зачем выделять home?

Как видим, корневой раздел / самый большой, поэтому возьмем от него часть для домашнего раздела **/home**. Уменьшаем размер, указав в окне «**Требуемый размер**» размер раздела, указываем меньше, чем сейчас есть, нажимаем кнопку «**Применить**». Заметим, при разметке диска нужно учитывать, что и для корневого раздела нужно оставить свободное место, минимально допустимый размер для корня / - не менее 10 ГБ.

Далее нажмите на плюс (+), выберите точку монтирования **/home**, размер оставляем пустым (но можно и указать необходимый). Таким образом, под **/home** выделится все остальное свободное место, которое мы забрали у корневого **/**. Тип файловой системы оставим по умолчанию — **ext4**, как более технологически продвинутую, но также в окне инсталлятора представлены и другие файловые системы.

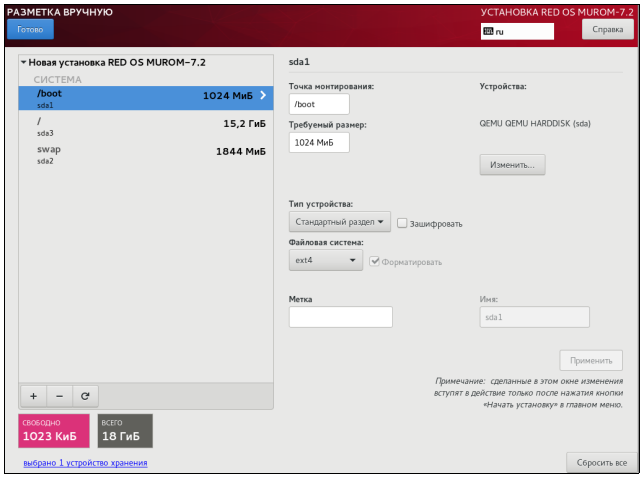


Рисунок 7.1 — Стандартная разметка диска

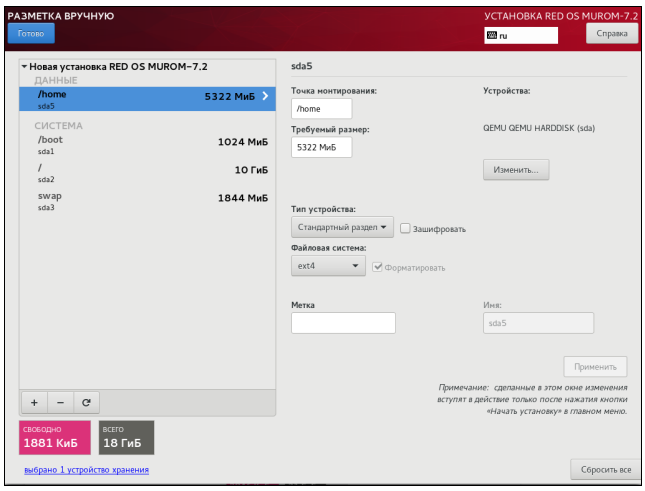
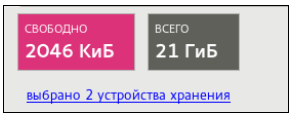


Рисунок 7.2 — Стандартная разметка диска

Другие параметры диалога разметки диска:

- Точка монтирования: указывается директория для подключения будущего раздела;
- Требуемый размер: указывается размер раздела;
- Устройство: выбирается физическое устройство, на котором будет располагаться раздел;
- Тип устройства: стандартный раздел, LVM, динамический LVM, RAID, btrfs;
- Файловая система: выбирается файловая система для раздела;
- Метка: назначается имя разделу под понятным вам именем, не обязательный параметр;
- Имя: имя раздела;
- В нижнем левом углу показывается оставшееся свободное и израсходованное место под разметку.



Разделы swap, boot, home

Рассмотрим для чего предназначен каждый из созданных разделов.

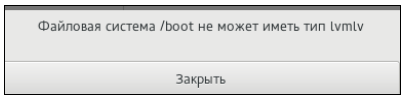
Раздел swap используется для поддержки виртуальной памяти. Данные попадают в раздел подкачки, когда системе не хватает оперативной памяти для их обработки.

Размер раздела для **swap** - минимум половина от ОЗУ, это если пользователь не собирается использовать режим глубокого сна (гибернации). При гибернации вся оперативная память перемещается в **swap**, в этом случае его размер должен быть не меньше размера оперативной памяти!

Раздел /boot содержит ядро операционной системы и файлы начальной загрузки **grub2** 1024 МБ (1 ГБ) будет достаточно для данного раздела. Раздел **boot** лучше создать вне группы томов, а создавать его как отдельный стандартный раздел.

Ряд ограничений, по которым boot выделяется в отдельный стандартный раздел:

- раздел **boot** не может располагаться на шифрованных разделах;
- раздел **boot** не может находится на разделах, файловая система которых не поддерживается загрузчиком **grub2**;
- загрузчик быстрее обнаружит свои файлы, если они находятся на небольшом разделе в начале диска;
- файловая система раздела /boot не может иметь тип LVM (для случая, когда используется LVM-разметка диска).



Раздел /home используется для хранения профилей пользователя, настроек рабочего окружения и документов. Как мы уже говорили, выделение отдельного раздела для каталога **/home** позволяет отделить пространство хранения пользовательских данных от системных. Пользовательские данные, размещенные на отдельном разделе, не пострадают при переустановке системы, а также надежнее защищены от ошибок пользователя во время переноса данных. При переполнении домашнего каталога видео, музыкой и прочим, это не скажется на работе системы в целом, как если бы **home** был на одном разделе с корневой файловой системой, в результате чего закончилось бы все дисковое пространство.

В корневом разделе / будут находиться все системные файлы и к нему будут монтироваться (подключаться) все выше созданные разделы. Минимальный рекомендуемый размер раздела - 10 ГБ.

Пример с размещением home на отдельном диске

Если в компьютере имеется несколько жестких дисков, то для надежности и, в дальнейшем, простоты администрирования можно, например, точку монтирования /home разместить на **отдельном диске**, тем самым изолировав ее от основной файловой системы. Давайте разместим каталог пользователя (**home**) на диске sdb, размер которого в нашем примере 1 Гб. Это легко сделать, выбрав для точки монтирования **/home** нужный диск. Раздел «**Устройство**» - «**Изменить**». Для сохранения настроек нажмите «**Применить**».

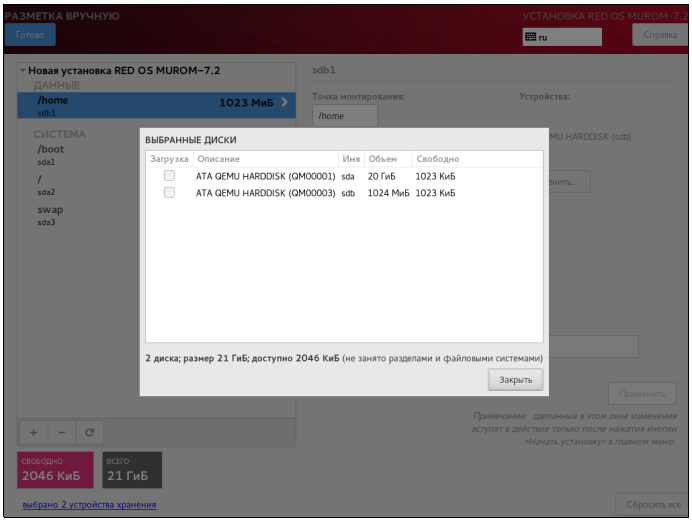
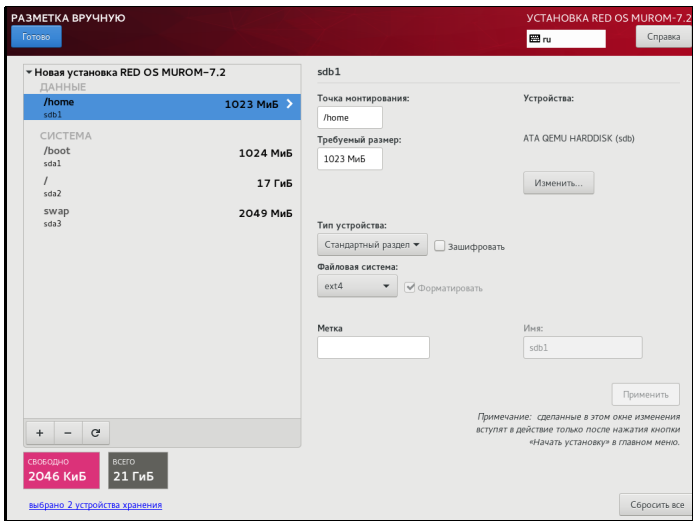


Рисунок 8 — Выбранные диски

Таким образом, под **/home** (домашний каталог профилей пользователей) был выделен отдельный физический диск sdb размером 1 Гб. Остальные разделы boot (sda1), swap (sda3) и корень (sda2) мы разместили на другом физическом диске sda размером 20 Гб.

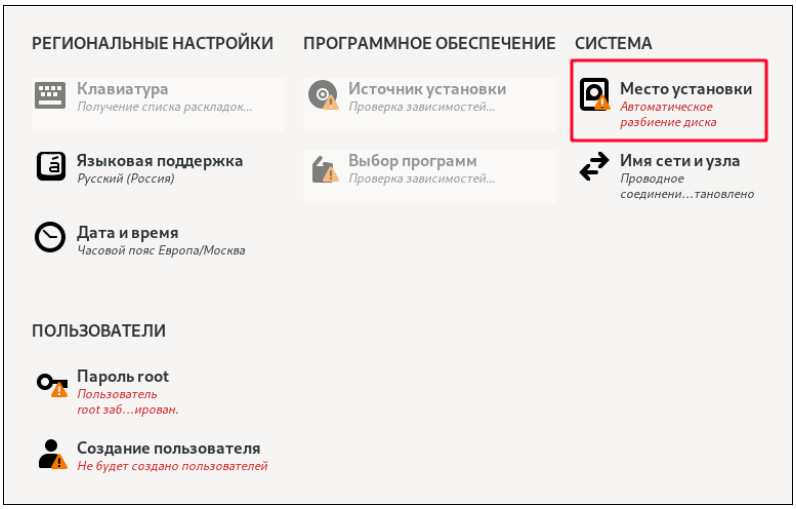


Нажимаем на кнопку «**Готово**» и приступаем к дальнейшим шагам установки РЕД ОС.

Сохранение раздела /home

Далее рассмотрим порядок настройки диска для сохранения (без изменения или удаления) домашнего раздела (**/home**) при переустановке РЕД ОС.

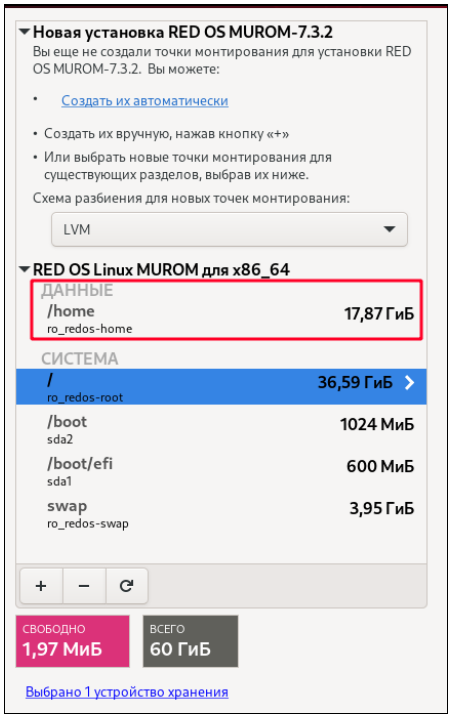
Запустите новую установку РЕД ОС, в мастере установки ОС перейдите в пункт «**Место установки**». Выберите конфигурацию для разметки диска «**По-своему**».



Убедитесь, что на диске присутствует отдельный раздел **/home**.

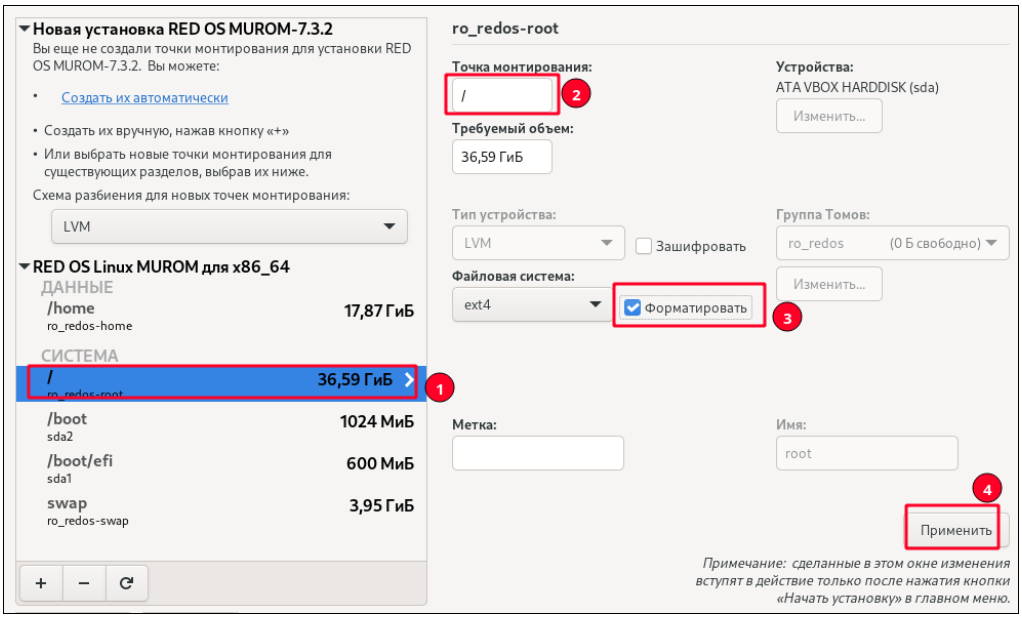
Примечание.

Данный раздел может отсутствовать, если ранее ОС установили с использованием автоматической разметки на жесткий диск, размер которого был менее 50 ГБ, в этом варианте домашний каталог (**/home**) размещается в корневом разделе (**/**), а не на отдельном. В результате при переустановке ОС корневой раздел будет неизбежно отформатирован вместе с домашним каталогом пользователя. В этом случае, перед установкой необходимо сделать резервную копию **/home** и после установки ОС восстановить данные.



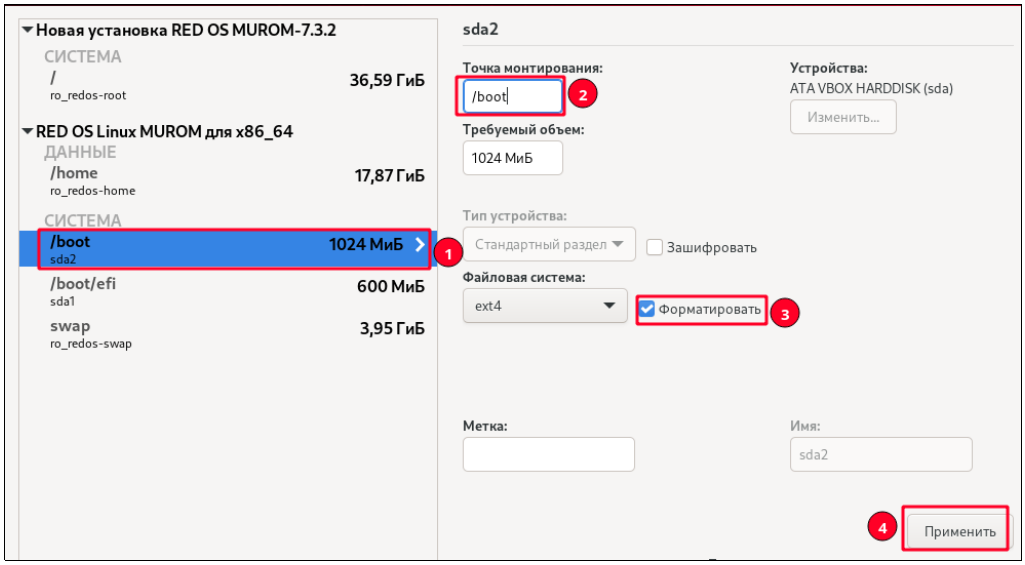
Именно этот раздел (**/home**), содержащий профили пользователей с их данными, **не будет отформатирован**. Остальные разделы необходимо настроить.

Для корневого раздела укажите точку монтирования «/», файловую систему **ext4**, а также установите флаг «**Форматировать**», далее нажмите кнопку «**Применить**».

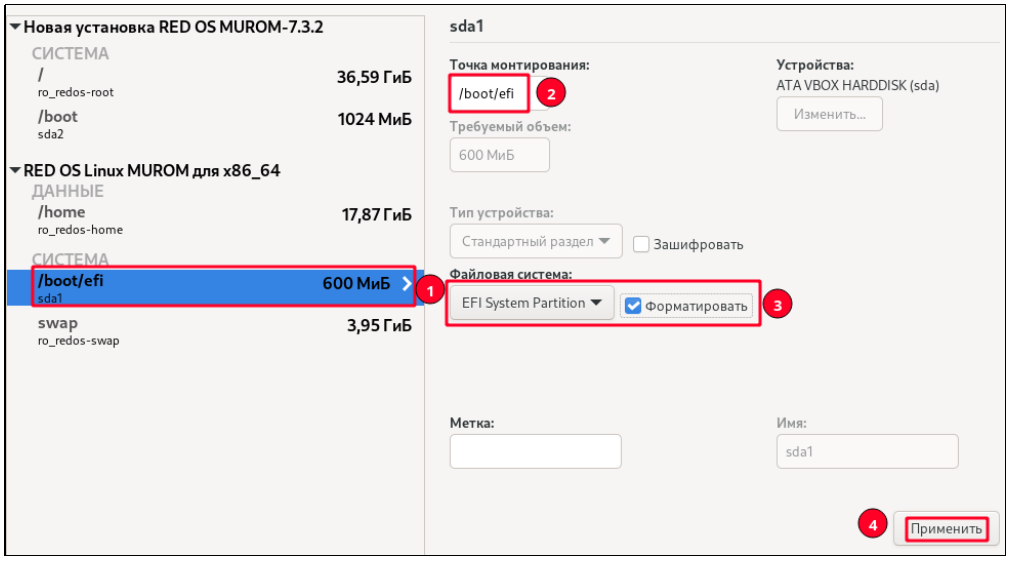


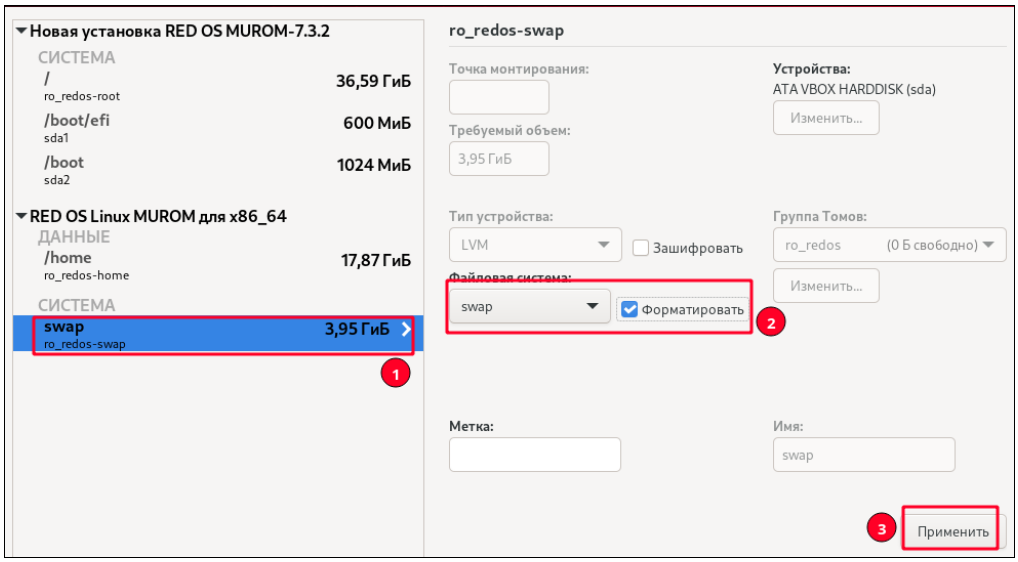
Результат изменения появится в разделе «**Новая установка RED OS 8**».

Следующим шагом выберите раздел **/boot** и присвойте ему точку монтирования **/boot**, файловую систему **ext4** и установите флаг «**Форматировать**», нажмите «**Применить**».



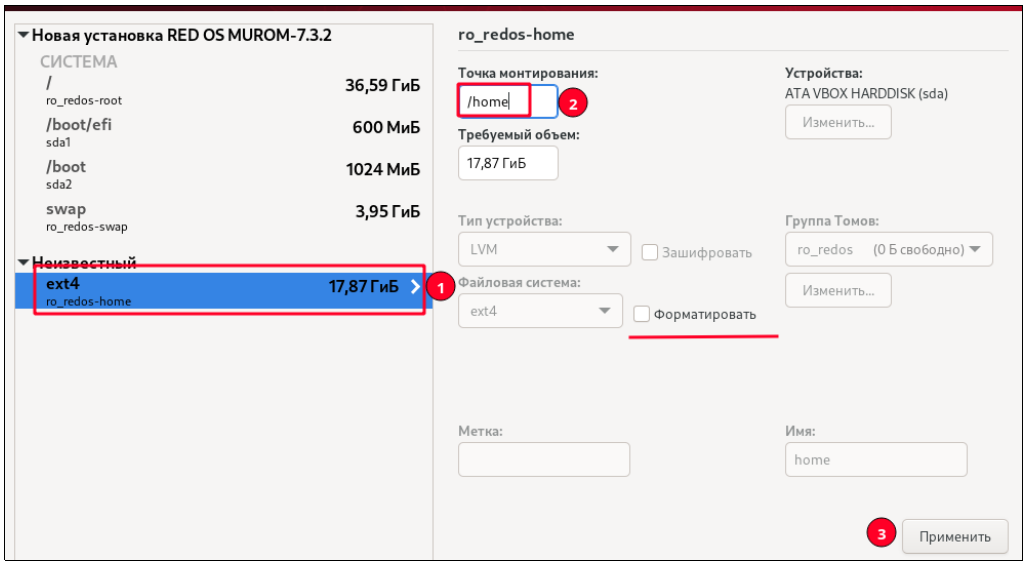
Аналогичные действия выполните для раздела **/boot/efi** и **swap** так, как это показано на нижеприведенных рисунках.





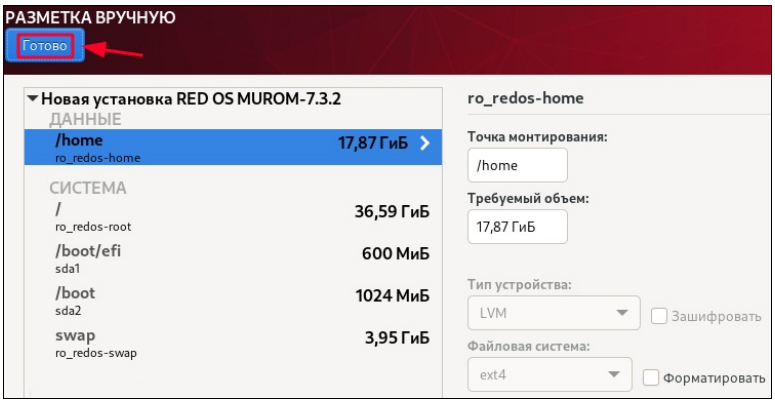
ВАЖНО!

Остался раздел, на котором ранее был размещен **/home**. Для него укажите точку монтирования **/home**, но флаг «**Форматировать**» не устанавливайте. Нажмите кнопку «**Применить**».

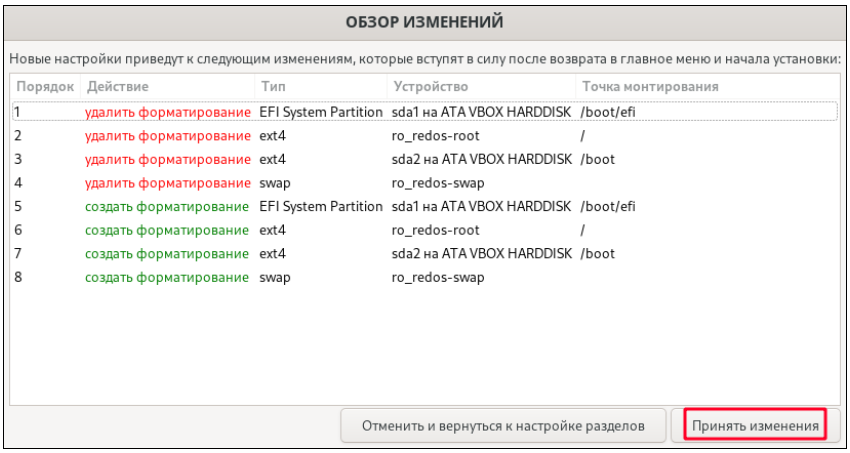


Готовая конфигурация разметки диска показана на рисунке ниже.

Обратите внимание, что для раздела **/home** не был установлен признак форматирования. Но для корневого раздела (**/**), а также для **/boot/efi**, **/boot** и **swap** признак «**Форматировать**» был присвоен, т.е. все данные перед установкой на этих разделах будет удалены. Нажмите на кнопку «**Готово**» для продолжения.



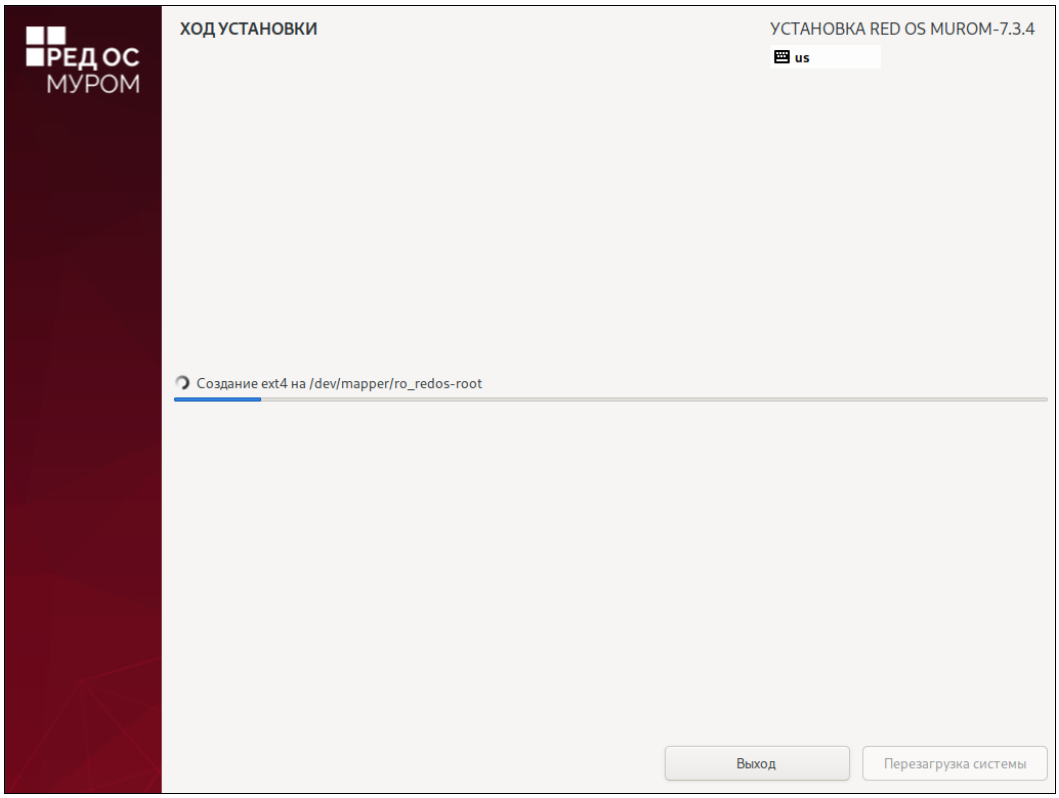
В результате появится итоговая таблица изменений, которые будут выполнены перед установкой ОС.



Примените изменения и продолжите настройку других параметров для установки РЕД ОС.

Установка системы

Этап установки представляет собой установку набора программ, необходимых для работы системы.



Получение пакетов осуществляется с источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу **FTP** и/или **HTTP**) время выполнения этого шага будет зависеть от скорости соединения и может быть значительно большим, чем при установке с дистрибутивного DVD-диска.

Начиная с этого шага, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включённых в дистрибутив.

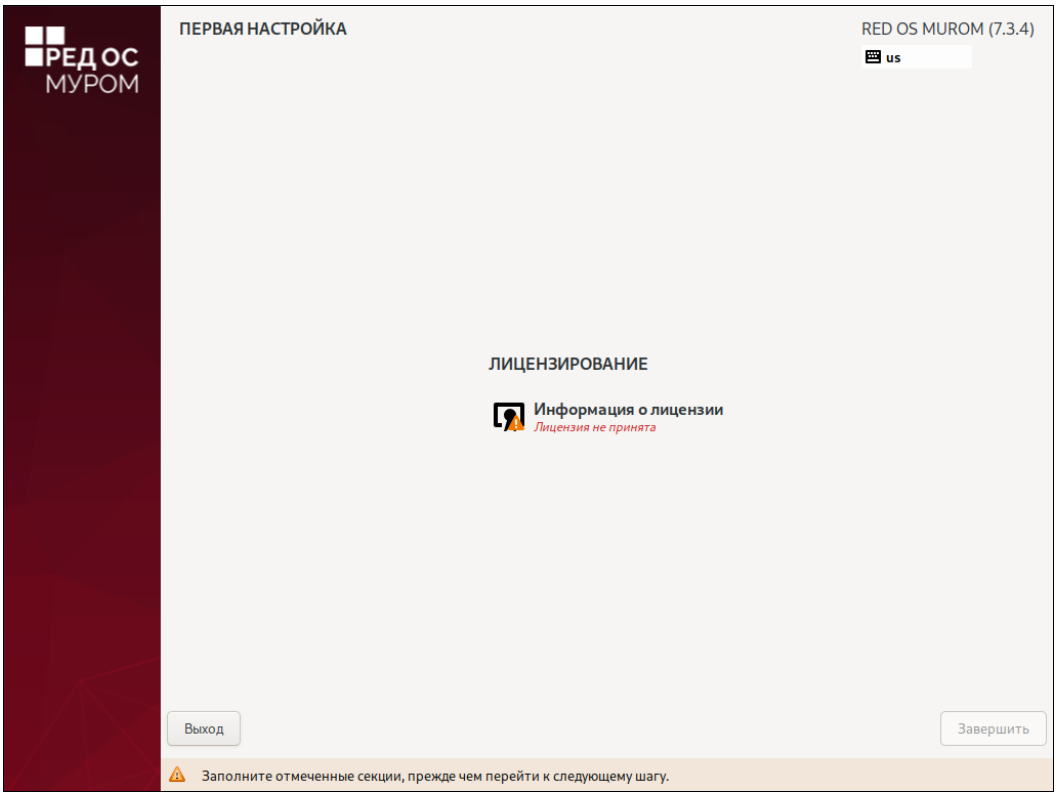
Загрузчик Linux — программа, которая позволяет загружать Linux и другие операционные системы. При автоматическом разбиении разделов накопителя на жестких дисках средства вычислительной техники загрузчик автоматически устанавливается в начальный раздел диска.

Если же планируется использовать и другие операционные системы, уже установленные на этом компьютере, тогда имеет значение, на каком жестком диске или разделе будет расположен загрузчик. В большинстве случаев программа установки правильно подберет расположение загрузчика.

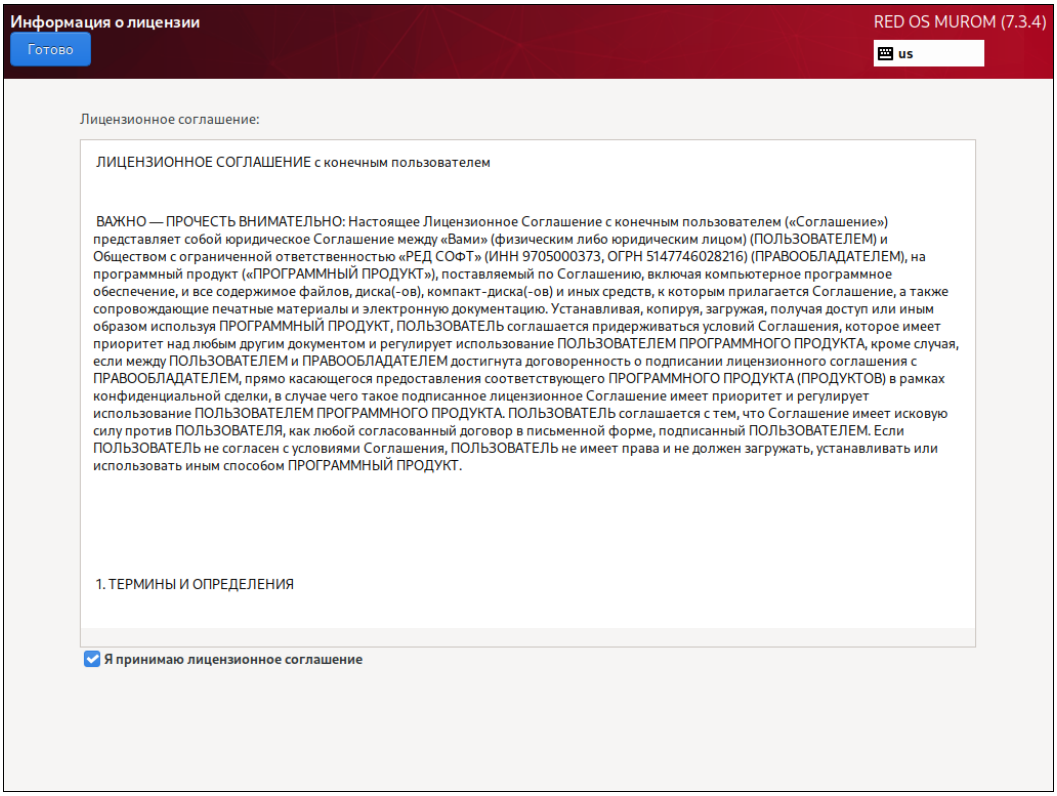
После выполнения копирования файлов РЕД ОС и установки загрузчика пользователю предлагается произвести перезагрузку РЕД ОС кнопкой «**Перезагрузить**».

Соглашение пользователя и Лицензионный договор

После успешной перезагрузки и перед продолжением установки следует внимательно прочитать условия пользовательского соглашения.



В лицензии говорится о правах распространения и гарантиях производителя.



При приобретении дистрибутива данное лицензионное соглашение прилагается в печатном виде к копии дистрибутива на вкладыше комплекта дистрибутива. Лицензия относится ко всему дистрибутиву РЕД ОС.

Завершение установки

После сохранения настроек и перезапуска системы пользователю предоставляется экран приветствия и приглашения к авторизации. На этом установка и настройка РЕД ОС завершена, и РЕД ОС полностью готова к использованию.

Действия после установки ОС

После установки РЕД ОС не все функции безопасности включены по умолчанию. Администратор должен определить функциональную роль установленной копии ОС, перечень решаемых задач, и, в соответствии с действующими политиками безопасности организации, произвести активацию необходимых служб, сервисов и приложений. А именно:

- сконфигурировать перечень отслеживаемых событий безопасности;
- настроить действия в случае обнаружения критически важных событий безопасности;
- настроить действия для предотвращения потери данных аудита;
- настроить защищенную передачу данных аудита;
- создать необходимое количество пользователей, групп, ролей и связать пользователей с группами и ролями, исходя из необходимых им полномочий;
- установить права доступа на создаваемые вновь каталоги и файлы;
- определить правила установки программ и правила запуска компонентов программного обеспечения;
- определить и настроить используемые механизмы идентификации и аутентификации, сроки действия учетных записей и паролей, требования, предъявляемые к аутентификационным данным;
- создать необходимые резервные копии данных и системных настроек и проводить периодическое их тестирование;
- настроить доверенные сервера точного времени;
- проверить целостность важных данных и системных файлов;
- организовать отказоустойчивый кластер при необходимости обеспечения повышенной отказоустойчивости;
- определить квоты и приоритеты, выделяемые пользователям;
- установить необходимые ограничения на сеансы пользователей;
- установить продолжительность бездействия пользовательского сеанса, после которого сеанс будет заблокирован или завершен.

Общие понятия

Для штатной установки дистрибутива РЕД ОС используется загрузочный оптический носитель информации - DVD-диск из комплекта поставки дистрибутива РЕД ОС.

Установка с оптического носителя информации (DVD-диска) - это лишь один из возможных способов установки РЕД ОС. Он подходит для большинства случаев, но не работает, например, в случае отсутствия на компьютере накопителя на оптических носителях информации - DVD-привода. Для таких случаев поддерживаются альтернативные методы установки. Важно понимать, что для начала установки необходимо иметь две вещи: возможность загрузить компьютер и доступ к установочным файлам. В случае установочного дистрибутивного DVD-диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все необходимые для установки файлы. Однако вполне допустим и такой вариант: первоначальная загрузка происходит со специально подготовленного flash-диска, а установочные файлы берутся с FTP-сервера сети.

Таким образом, для установки дистрибутива необходимо:

- Выбрать способ первоначальной загрузки компьютера;
- Выбрать источник установки.

Для загрузки компьютера с целью установки операционной системы необходимо воспользоваться носителем, содержащим начальный загрузчик. Таким носителем может быть, как сам загрузочный оптический диск, так и, например, flash-накопитель, который можно сделать загрузочным, воспользовавшись одним из способов, описанных в нашей статье «Создание загрузочных носителей».

После первоначальной загрузки с одного из поддерживаемых носителей можно выбрать *источник установки* - место, откуда программа установки будет брать все необходимые при установке данные (прежде всего, устанавливаемое ПО). Так как установка системы возможна не только с лазерного диска, то можно выбрать один из поддерживаемых альтернативных источников установки.

Источники установки:

- Сетевые:
  - FTP-сервер;
  - NFS-сервер;
  - HTTP-сервер.

- Локальные:
  - Загрузочный флеш-диск.

Условием для всех способов установки является доступность дерева файлов, аналогичного содержимому установочного диска.

Установка РЕД ОС в текстовом режиме

Установка в текстовом режиме предлагает интерактивный, не графический интерфейс для установки РЕД ОС. Это может быть полезно в системах без графических возможностей. Однако необходимо учитывать ограничения, накладываемые на текстовый режим, и рассмотреть иные доступные альтернативы перед началом текстовой установки.

Для установки РЕД ОС в текстовом режиме необходимо:

1. После появления загрузчика инсталлятора (Рисунок 1) выбрать пункт меню «Установить RED OS» и нажать *«TAB»* на клавиатуре.

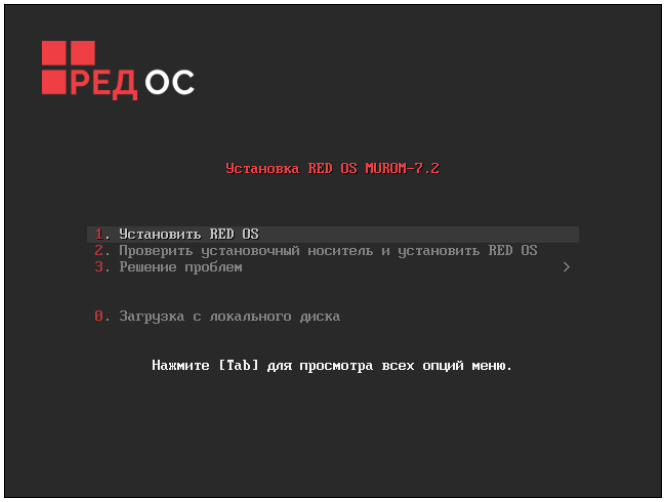


Рисунок 1 – Стартовое окно установки

2. В появившейся нижней части экрана в командной строке загрузчика (Рисунок 2) добавить текст:

```
inst.text
```

и нажать клавишу *«Enter»*.

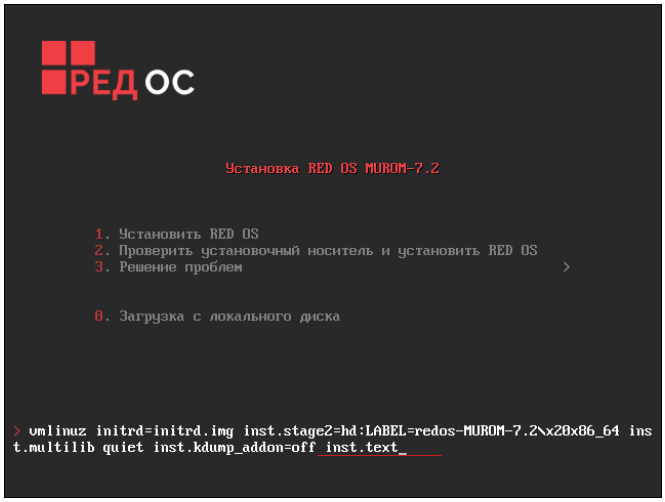


Рисунок 2 – Командная строка загрузчика

Установка в текстовом режиме (Рисунок 3) происходит по схеме, аналогичной графической установке: нет единого фиксированного порядка настройки. Пользователь может настроить все доступные параметры в любом порядке, используя главный экран инсталлятора.

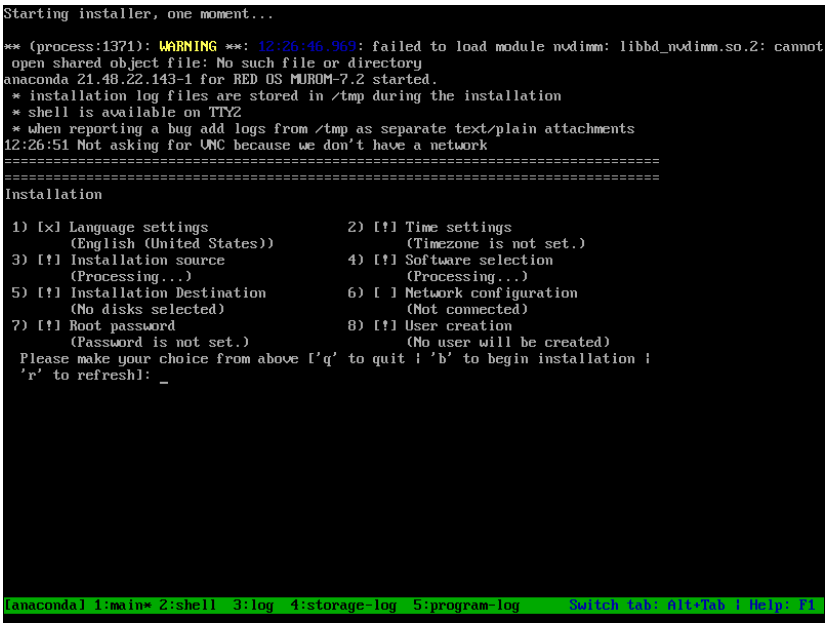


Рисунок 3 – Настройка параметров

Экраны, которые уже были настроены автоматически или корректно настроены самим пользователем, помечаются как **[x]**, а экраны, которые требуют обязательной настройки до начала установки, помечаются как **[!]**. Доступные команды отображаются под списком доступных опций. Выбор пункта меню осуществляется в строке ввода нажатием соответствующей цифровой клавиши.
Например, чтобы в меню, показанном на Рисунке 3, назначить пароль для администратора root, необходимо нажать на клавиатуре последовательно цифру *«7»* и *«Enter»*.
По умолчанию используются следующие клавиши:

- *q* – для выхода из текущего меню;
- *r* – для обновления содержимого;
- *b* – для начала процесса установки в главном меню;
- *c* – для подтверждения действия.

Примечание.
При выполнении связанных фоновых задач некоторые пункты меню могут быть временно недоступны или отображать «Processing...». Чтобы обновить текущее состояние элементов текстового меню, используйте команду «r» в приглашении текстового режима.

В нижней части экрана в текстовом режиме (Рисунок 3) отображается зеленая полоса с пятью вариантами меню. Эти параметры представляют собой различные экраны в мультиплексоре терминала **tmux** (по умолчанию пользователь запускается на экране 1). Пользователь может использовать сочетания клавиш для переключения на другие экраны, которые содержат журналы и интерактивную командную строку.

ВАЖНО!

Ограничения установки интерактивного текстового режима включают в себя:

- установщик всегда будет использовать английский язык и английскую раскладку клавиатуры. Пользователь может настроить язык и параметры клавиатуры, но эти параметры будут применяться только к установленной системе, а не к самой установке;
- пользователь не может настроить какие-либо расширенные методы хранения (LVM, программный RAID, FCoE, zFCP и iSCSI);
- настроить пользовательское разбиение на разделы невозможно – необходимо использовать один из параметров автоматического разбиения на разделы. Пользователю также недоступна настройка места, куда будет установлен загрузчик;
- пользователь не может установить дополнительные пакеты, они должны быть добавлены после завершения установки с помощью диспетчера пакетов DNF.

Для конфигураций "Рабочая станция" и "Сервер с графикой", после полного завершения установки ОС и входа под пользователем в терминальном режиме требуется выполнить команду:

```
systemctl set-default graphical.target
```

И выполните перезагрузку:

```
reboot
```

Обзорная инструкция про RAID

Определение RAID
Виды RAID. RAID 0
Виды RAID. RAID 1
Виды RAID. RAID 2
Виды RAID. RAID 5
Виды RAID. RAID 6
Виды RAID. RAID 10
Аппаратные RAID-контроллеры
Программный RAID

Определение RAID

RAID – это дисковый массив из нескольких жестких дисков. Он используется для повышения надежности хранения данных или для увеличения скорости чтения/записи.

Разные типы этих конфигураций как раз и отмечаются разными номерами: **1**, **2**, **3**, **4** и, соответственно, выполняют разные функции.

- **RAID 0** — дисковый массив повышенной производительности с чередованием без отказоустойчивости;
- **RAID 1** — зеркальный дисковый массив;
- **RAID 2** — зарезервирован для массивов, которые применяют код Хемминга;
- **RAID 3** — дисковый массив с выделенным диском чётности;
- **RAID 4** — дисковый массив с чередованием и выделенным диском чётности;
- **RAID 5** — дисковый массив с чередованием, в том числе данных чётности;
- **RAID 6** — дисковый массив с чередованием, использующий две контрольные суммы, вычисляемые двумя независимыми способами;
- **RAID 10** — массив **RAID 0**, построенный из массивов **RAID 1**.

Вы можете подробнее ознакомиться с дисковыми массивами **RAID**, просмотрев наши обучающие видео:

- на **RuTube** — Создание программного RAID массива на РЕД ОС;
- в **Яндекс.Дзен** — Создание программного RAID массива на РЕД ОС;
- в **VK Видео** — Создание программного RAID массива на РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Виды RAID

RAID 0

RAID 0 (чередование дисков) – на данном уровне задействован процесс разделения массива данных на блоки с последующим их распределением по нескольким устройствам хранения, объединенных в одну совокупную группу. Блоки распределяются последовательно и содержат каждый свою часть данных на отдельном диске.

Распределение данных в **RAID-массиве** нулевого уровня происходит без данных четности и не имеет избыточности или отказоустойчивости. Это означает, что в случае сбоя какого-то одного диска происходит разрушение всего дискового массива, и восстановить информацию в полном объеме не получится без использования данных с неисправного накопителя.

Системы хранения выполняют чередование дисков по-разному. Система может чередовать данные на уровне байтов, блоков или разделов, или чередовать данные на всех или некоторых дисках кластера.

RAID 0 лучше всего использовать для хранилища, наличие защиты от потери данных в котором не критично, но требуется поддержка высокоскоростного режима чтения и записи. Например, это могут быть задачи по обработке потокового видео в реальном времени и редактирование файлов медиа-формата, хранение временных данных.

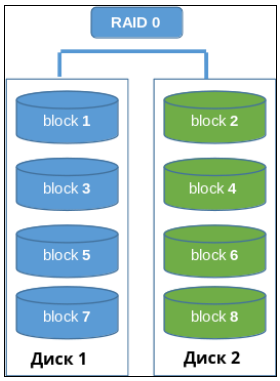
Преимущества **RAID 0**:

- Повышенная производительность чтения и записи;
- Использование полной мощности накопителей;
- Легко реализуется.

Недостатки **RAID 0**:

- Отсутствует отказоустойчивость.

Наглядная схема **RAID 0** состоящая из двух дисков представлена на рисунке.



RAID 1

RAID 1 - массив из двух (или более) дисков, являющихся полными копиями друг друга. Самая простая система **RAID-массивов** из всех возможных. Представляет собой параллельную запись информации с основного диска на другие — дублирующие. Повышение производительности происходит только при чтении данных, за счёт распараллеливания запросов. Зеркальное копирование дисков особенно полезно для сценариев аварийного восстановления, поскольку обеспечивает мгновенное восстановление требуемых, для критически важных приложений, данных сразу после отказа диска. Если первичные диски в массиве повреждены или не могут быть использованы, произойдет переключение на вторичные или зеркальные резервные диски, обладающие работоспособными копиями, и функционирование приложений, обращающихся к востребованным данным, не будет нарушено.

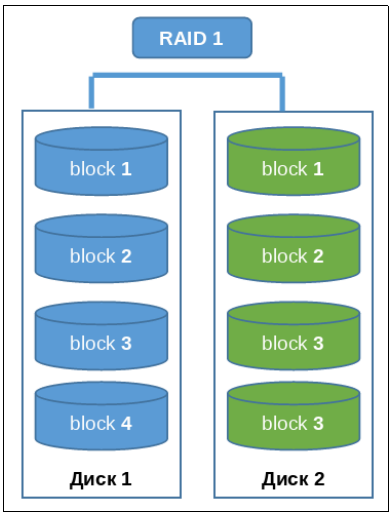
Достоинства:

- Обеспечивает приемлемую скорость записи и выигрыш по скорости чтения при распараллеливании запросов.
- Имеет высокую надёжность — работает до тех пор, пока функционирует хотя бы один диск в массиве. Вероятность выхода из строя сразу двух дисков равна произведению вероятностей отказа каждого диска, то есть значительно ниже вероятности выхода из строя отдельного диска.

Недостатки:

- По цене двух жестких дисков пользователь получает объём одного.

Наглядная схема **RAID 1**.



RAID 2

Массивы такого типа основаны на использовании кода Хэмминга. Но поскольку современные жесткие диски также используют самоконтролирующийся код Хемминга, то уровень «**RAID 2**» теперь считается устаревшим. Чтобы получить **RAID** данного типа, создаются две группы дисков – одна для хранения данных, другая - для кодов исправления ошибок.

Данный код исправления ошибок позволяет производить анализ данных, которые считываются или пересылаются, и, при необходимости, исправлять их непосредственно во время процесса передачи.

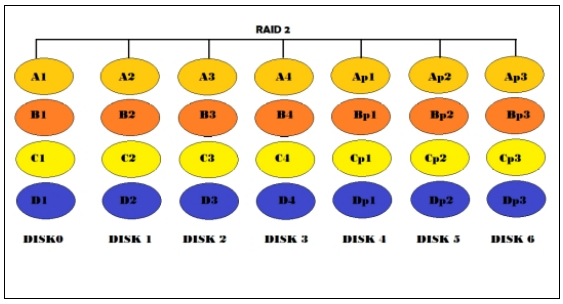
Достоинства:

- Быстрое исправление ошибок, без снижения скорости передачи данных между дисковым массивом и процессором.

Недостатки:

- Минимальное количество дисков 7, только начиная с этого количества для него требуется меньше дисков, чем для **RAID 1** (4 диска с данными, 3 диска с кодами коррекции ошибок), в дальнейшем избыточность уменьшается по экспоненте.

Наглядная схема **RAID 2**.



RAID 5

RAID 5 — дисковый массив с чередованием блоков данных и контролем чётности.

Схож по своему принципу работы с **RAID 1**. Только теперь потребуется минимум 3 накопителя, на одном из которых будет храниться продублированная информация. Избыточный массив конфигурации независимых дисков подобного формата основан в соответствии с принципом чередования на уровне блоков четности. Данные и информация о четности распределяются равномерно по всем дискам, что влечет за собой снижение критичной уязвимости отдельного запоминающего накопителя из организованного объединения, и позволяет массиву «**RAID 5**» функционировать даже в случае сбоя какого-нибудь одного диска, а также даже восстановить данные за счёт чередования, утраченные с проблемного устройства.

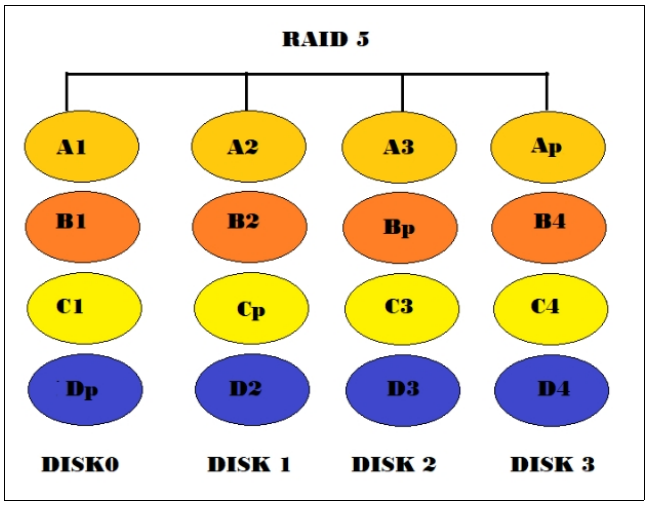
Достоинства:

- **RAID 5** получил широкое распространение, в первую очередь благодаря своей экономичности. С увеличением количества дисков в массиве экономия (по сравнению с другими уровнями **RAID**, обладающими отказоустойчивостью) продолжает увеличиваться.
- **RAID 5** обеспечивает высокую скорость чтения — выигрыш достигается за счёт независимых потоков данных с нескольких дисков массива, которые могут обрабатываться параллельно.

Недостатки:

- Производительность **RAID 5** заметно ниже на операциях записи в произвольном порядке, при которых производительность падает на 10-25 % от производительности **RAID 0** (или **RAID 10**), так как требует большего количества операций с дисками. Каждая операция записи заменяется на контроллере **RAID** на четыре — две операции чтения и две операции записи.

Наглядная схема **RAID 5**.



RAID 6

RAID 6 — массив из четырёх или более дисков, обеспечивающий двойной контроль четности хранимой информации. Разработанный для защиты от потери данных при выходе из строя сразу двух жестких дисков в массиве. За счёт двух дисков избыточности он имеет более высокую степень надёжности. Среди дисковых массивов **RAID 6** — самый надёжный, но и самый медленный. Архитектурное построение «**RAID 6**» представляет собой одну из нескольких схем «**RAID**», которая функционирует, размещая данные на нескольких дисках и позволяя операциям ввода/вывода («I/O») перекрываться сбалансированным образом. Использование дополнительной четности позволяет массиву продолжать свое функционирование, даже если два диска выходят из строя одновременно

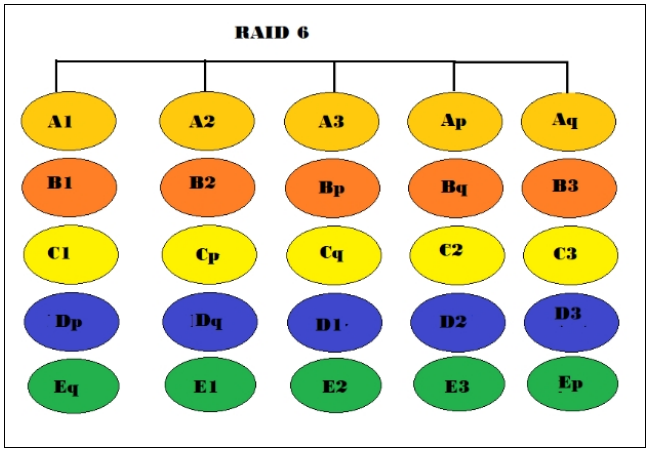
Достоинства:

- Надёжность — она максимальна из всех массивов данных **RAID**.
- Если два диска выйдут из строя, и их придется заменить, вы все равно будете иметь доступ ко всем данным.

Недостатки:

- Отказы дисков влияют на производительность массива;
- Операции записи медленнее, чем в **RAID 5**, из-за дополнительных блоков четности, принимающих участие в вычислениях.

Наглядная схема **RAID 6**.



RAID 10

RAID 10 (**RAID 1+0**) — зеркалированный массив, данные в котором записываются последовательно на несколько дисков, как в **RAID 0**. Диски вложенного массива объединяются в «зеркала» **RAID 1**. Эти зеркальные пары затем преобразуются в общий массив с использованием чередования **RAID 0**. Вам потребуется минимум 4 носителя, и их количество всегда должно быть четным. В данном массиве вы получаете высокую производительность и высокую надежность. Однако, как в случае и с **RAID 1**, вам будет доступна лишь половина от общего объема всей системы.

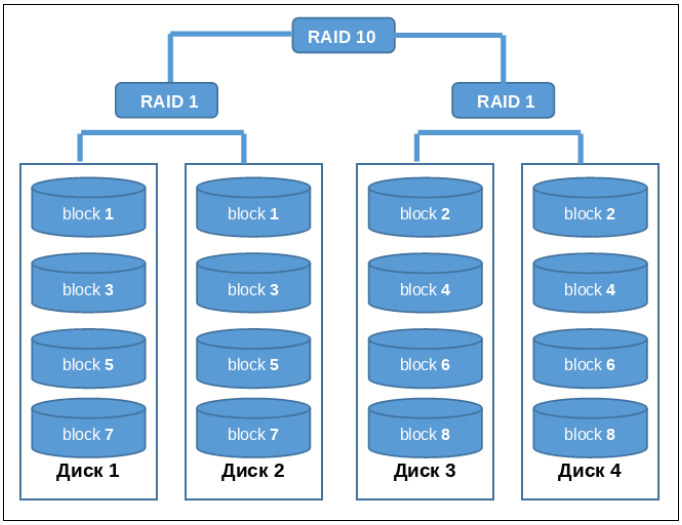
Достоинства:

- **RAID 10** объединяет в себе высокую отказоустойчивость и производительность.
- **RAID 10** является достаточно надёжным вариантом для хранения данных в связи с тем, что весь массив **RAID 10** будет выведен из строя только после выхода из строя всех накопителей в одном и том же массиве **RAID 1**.

Недостатки:

- Эффективность дискового пространства 50%.

Наглядная схема **RAID 10**.



Аппаратные RAID-контроллеры

Представляют собой плату расширения либо размещаются вне сервера (например, в составе внешней дисковой подсистемы либо **NAS**). Имеют собственный процессор, многие имеют кэш-память для ускорения работы. При значительной нагрузке на систему дисков, которая требует от сервера обработки больших объемов данных, может работать только отдельное оборудование **RAID-контроллера**.

Он подключается через разъем **PCI** к материнской плате и самостоятельно решает задачи управления массивом жестких дисков.

Для подключения дисков контроллер может иметь внутренние либо внешние порты, либо и те, и другие.

Контроллеры различных производителей, как правило, не совместимы и не взаимозаменяемы между собой — это следует иметь в виду в случае выхода из строя платы контроллера. Информация о конфигурации **RAID-массива** хранится на дисках, но прочитать её, даже с полностью исправных дисков, и воссоздать массив сможет только контроллер того же производителя. Программные **RAID-массивы** также лишены этого недостатка.

Программный RAID

Дисковый массив, который создается в операционной системе, называется программным **RAID**. Для реализации **RAID** можно применять не только аппаратные средства, но и полностью программные компоненты (драйверы). Управлять **RAID**-устройствами в РЕД ОС можно с помощью утилиты **mdadm**.

Главное преимущество программной реализации – невысокая стоимость.

Недостатки – низкая производительность и постоянная дополнительная нагрузка на процессор.

Получается, программная реализация лучше всего проявляет себя в работе с теми массивами дисков, которые не требуют объемных вычислений.

Создание программного массива уровня RAID0 и RAID1

Подготовка к созданию RAID-массива
Создание программного массива уровня RAID 0
Создание программного массива уровня RAID1
Создание автоматического монтирования RAID 0

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Подготовка к созданию RAID-массива

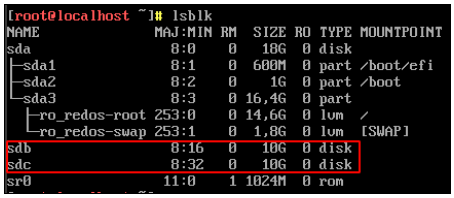
В примере для создания RAID-массива **нулевого уровня** будем использовать **два диска** объемом **10 Гб**. Описание и особенности работы **RAID0** можно найти по ссылке.

Для выполнения дальнейших действий требуется перейти в сеанс пользователя **root**:

```
su -
```

Для того чтобы посмотреть текущую информацию об устройствах хранения, выполните команду:

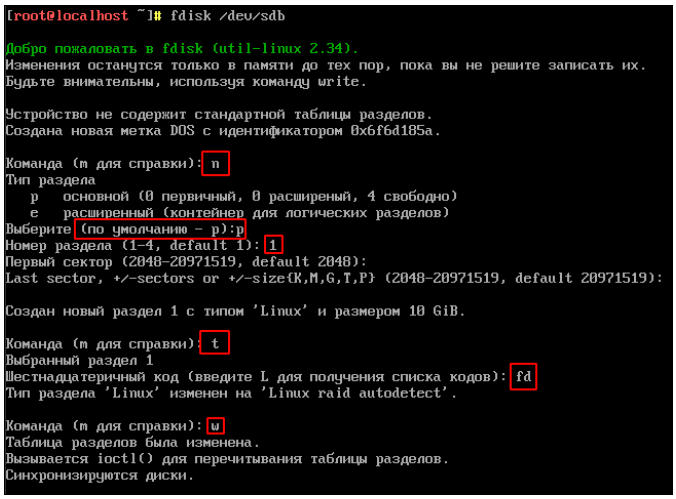
```
lsblk
```



Здесь **sdb**, **sdc** – это те диски, которые мы будем использовать для создания **RAID 0**.

Далее необходимо создать разделы на каждом из дисков **sdb** и **sdc**, для этого воспользуемся утилитой fdisk. Создадим таблицу разделов для диска **/dev/sdb**:

```
fdisk /dev/sdb
```



Последовательность указания ключей **fdisk** при создании разделов и их описание:

- создание раздела (**n**);
- тип раздела primary (**p**);
- номер раздела (**1**).
- начальный и конечный блоки;
- изменение id раздела (**t**);

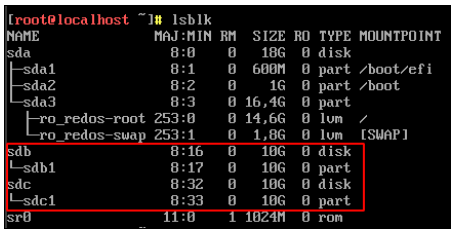
- установка id раздела в Linux raid autodetect (**fd**);
- применение изменений и выход (**w**).

Аналогично создаем таблицу разделов для диска **/dev/sdc**.

```
fdisk /dev/sdc
```

Выведем информацию о разделах:

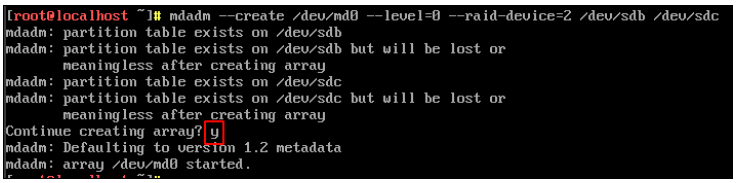
```
lsblk
```



Создание программного массива уровня RAID 0

Для создания программного RAID-массива в РЕД ОС используется утилита mdadm.

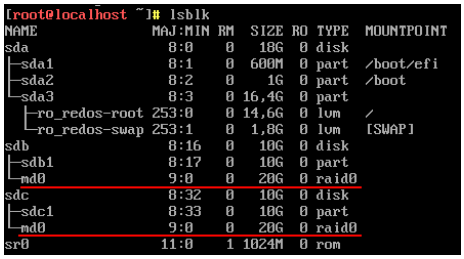
```
mdadm --create /dev/md0 --level=0 --raid-device=2 /dev/sdb /dev/sdc
```



Описание параметров **mdadm**:

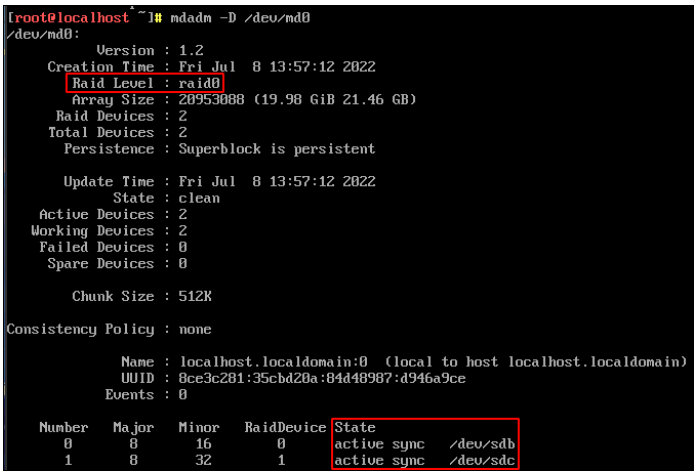
- **/dev/md0** – имя устройства **RAID**;
- **--level=0** – уровень **RAID**;
- **--raid-devices=2** – количество дисков, которые участвуют в сборке **RAID**;
- **/dev/sdb, /dev/sdc** – имена дисков, участвующих в сборке массива.

Снова выполните команду lsblk, теперь в выводе видно, что создано устройство **md0** с типом **RAID0**.



Следующая команда покажет детальную информацию о массиве:

```
mdadm -D /dev/md0
```



Создание программного массива уровня RAID1

Для создания **RAID 1** необходимо выполнить аналогичные действия, которые производились для создания программного массива **RAID 0**, различие лишь в том, что необходимо указать первый класс (**--level=1**) массива данных в параметрах утилиты `mdadm`:

```
mdadm --create /dev/md1 --level=1 --raid-device=2 /dev/sdb /dev/sdc
```

Создание автоматического монтирования RAID 0

Создадим файловую систему **ext4** на RAID-устройстве **/dev/md0** и смонтируем массив в каталог **/mnt/raid0/**.

```
mkfs.ext4 /dev/md0
mkdir /mnt/raid0
mount /dev/md0 /mnt/raid0
ls -l /mnt/raid0/
```

Для автоматического подключения **RAID** добавим запись в конец файла **/etc/fstab**, для этого в терминале выполните команду:

```
echo "/dev/md0 /mnt/raid0 ext4 defaults 0 0" >> /etc/fstab
```

Сохраните конфигурацию **RAID**, чтобы во время загрузки системы происходило ее считывание.

```
mdadm --detail --scan --verbose >> /etc/mdadm.conf
```

Создание программного массива уровня RAID 6

Подготовка к созданию RAID-массива
Создание RAID-массива
Создание автоматического монтирования RAID

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Подготовка к созданию RAID-массива

В данной инструкции рассмотрено создание программного RAID-массива из **4 дисков**, размером в **1 ГБ**. Это минимально возможное количество дисков, которое требуется для создания RAID-массива класса 6.

Для выполнения дальнейших действий требуется перейти в сеанс пользователя **root**:

```
su -
```

Для того чтобы посмотреть текущую информацию об устройствах хранения, выполните команду:

```
lsblk
```

```
[root@localhost admin]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda           8:0    0   25G  0 disk
├─sda1        8:1    0    1G  0 part /boot
└─sda2        8:2    0   24G  0 part
  ├─ro-root 254:0    0 21,5G  0 lvm  /
  └─ro-swap 254:1    0  2,5G  0 lvm  [SWAP]
sdb           8:16   0    1G  0 disk
sdc           8:32   0    1G  0 disk
sdd           8:48   0    1G  0 disk
sde           8:64   0    1G  0 disk
sr0          11:0    1    4G  0 rom  /run/media/admin/redos-MUROM-7.2 x86_64
[root@localhost admin]#
```

Здесь **sdb**, **sdc**, **sdd** и **sde** – диски, из которых будет собран программный **RAID 6**.

Проверим подключенные диски на отсутствие метаданных **RAID**.

```
mdadm -E /dev/sd[b-e]
```

```
[root@localhost admin]# mdadm -E /dev/sd[b-e]
mdadm: No md superblock detected on /dev/sdb.
mdadm: No md superblock detected on /dev/sdc.
mdadm: No md superblock detected on /dev/sdd.
mdadm: No md superblock detected on /dev/sde.
[root@localhost admin]#
```

Из вывода команды видно, что признаки **RAID** на дисках отсутствуют.

Создадим на каждом диске раздел с помощью следующей команды:

```
fdisk /dev/sdd
```

```
[root@localhost admin]# fdisk /dev/sdd

Добро пожаловать в fdisk (util-linux 2.30.2).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.

Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0x1e0bad61.

Команда (m для справки): n
Тип раздела
   p   основной (0 первичный, 0 расширеный, 4 свободно)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p
Номер раздела (1-4, default 1): 1
Первый сектор (2048-2097151, default 2048):
Последний сектор + число секторов или + размер{K,M,G,T,P} (2048-2097151, default
 2097151):

Создан новый раздел 1 с типом 'Linux' и размером 1023 MiB.

Команда (m для справки): t
Выбранный раздел 1
Шестнадцатеричный код (введите L для получения списка кодов): fd
Тип раздела 'Linux' изменен на 'Linux raid autodetect'.

Команда (m для справки): w
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

В консоли **fdisk** выберите:

- Создание раздела (**n**);
- Тип раздела primary (**p**);
- Номер раздела (**1**).
- Начальный и конечный блоки (**Enter**);
- Для изменения типа раздела (**t**);
- Шестнадцатеричный код (**fd**);
- Применение изменений и выход (**w**).

Создание RAID-массива

Для создания программного **RAID**-массива в РЕД ОС используется утилита **mdadm**.

```
mdadm --create /dev/md0 --level=6 --raid-devices=4 /dev/sd[b-e]1
```

Здесь:
/dev/md0 – имя устройства **RAID**;
--level=6 – уровень **RAID**;
--raid-devices=4 – количество дисков, участвующих в сборке массива;
/dev/sd[b-e]1 – имена дисков участвующих в сборке массива.

```
[root@localhost admin]# mdadm --create /dev/md0 --level=6 --raid-devices=4 /dev/
sd[b-e]1
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
[root@localhost admin]#
```

Проверим состояние созданного RAID-массива:

```
cat /proc/mdstat
```

```
[root@localhost admin]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid6 sde1[3] sdd1[2] sdc1[1] sdb1[0]
      2093056 blocks super 1.2 level 6, 512k chunk, algorithm 2 [4/4] [UUUU]

unused devices: <none>
[root@localhost admin]#
```

Создание автоматического монтирования RAID

Создадим файловую систему **ext4** на **RAID**-устройстве **/dev/md0** и смонтируем массив в каталог **/mnt/raid6/**.

```
mkfs.ext4 /dev/md0
mkdir /mnt/raid6
mount /dev/md0 /mnt/raid6
```

Для автоматического монтирования **RAID** добавим запись:

```
/dev/md0                /mnt/raid6              ext4    defaults        0 0
```

в **/etc/fstab**.

```
  nano 2.6.1                  Файл: /etc/fstab                      Изменён


#
# /etc/fstab
# Created by anaconda on Tue Sep 14 19:27:19 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/ro-root     /                       ext4    defaults        1 1
UUID=961ec5ba-2489-4971-8b9d-3f07b1a7fc5a /boot                   ext4    defau$
/dev/mapper/ro-swap     swap                    swap    defaults        0 0
/dev/md0                /mnt/raid6              ext4    defaults        0 0
```

А также необходимо сохранить конфигурацию **RAID**, чтобы во время загрузки системы происходило ее считывание.

```
mdadm --detail --scan --verbose > /etc/mdadm.conf
```

Выполним команду **lsblk**, при этом в ее выводе будет видно, что тип дисков изменился на **RAID6**.

```
[root@localhost admin]# lsblk
NAME         MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda            8:0    0   25G  0 disk
├─sda1         8:1    0    1G  0 part  /boot
└─sda2         8:2    0   24G  0 part
  ├─ro-root 254:0    0 21,5G  0 lvm   /
  └─ro-swap 254:1    0  2,5G  0 lvm   [SWAP]
sdb            8:16   0    1G  0 disk
└─sdb1         8:17   0 1023M  0 part
  └─md0        9:0    0    2G  0 raid6 /mnt/raid6
sdc            8:32   0    1G  0 disk
└─sdc1         8:33   0 1023M  0 part
  └─md0        9:0    0    2G  0 raid6 /mnt/raid6
sdd            8:48   0    1G  0 disk
└─sdd1         8:49   0 1023M  0 part
  └─md0        9:0    0    2G  0 raid6 /mnt/raid6
sde            8:64   0    1G  0 disk
└─sde1         8:65   0 1023M  0 part
  └─md0        9:0    0    2G  0 raid6 /mnt/raid6
sr0           11:0    1    4G  0 rom   /run/media/admin/redos-MUROM-7.2 x86_64
[root@localhost admin]#
```

Создание программного массива уровня RAID 10

Подготовка к созданию RAID-массива
Создание RAID-массива
Создание автоматического монтирования RAID
Замена неисправного диска при сбое, добавление запасного диска
Удаление диска из массива
Расширение массива

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Подготовка к созданию RAID-массива

В инструкции рассмотрено создание программного RAID-массива из **4 дисков**, размером в **1 ГБ**. Это минимально возможное количество дисков, которое требуется для создания RAID-массива уровня 10. Массив показывает высокую производительность и высокую надежность. Однако, как в случае и с RAID 1 эффективность использования дискового пространства составляет 50%.

Для выполнения дальнейших действий требуется перейти в сеанс пользователя **root**:

```
su -
```

Чтобы посмотреть текущую информацию об устройствах хранения, выполните команду:

```
lsblk
```

```
[root@localhost admin]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda           8:0    0   25G  0 disk
├─sda1        8:1    0    1G  0 part /boot
└─sda2        8:2    0   24G  0 part
  ├─ro-root 254:0    0 21,5G  0 lvm  /
  └─ro-swap 254:1    0  2,5G  0 lvm  [SWAP]
sdb           8:16   0    1G  0 disk
sdc           8:32   0    1G  0 disk
sdd           8:48   0    1G  0 disk
sde           8:64   0    1G  0 disk
sr0          11:0    1    4G  0 rom  /run/media/admin/redos-MUROM-7.2 x86_64
[root@localhost admin]#
```

Здесь **sdb**, **sdc**, **sdd** и **sde** – диски, из которых будет собран программный **RAID 10**.

Убедимся, что на подключенных дисках отсутствуют метаданных типа RAID. Это можно сделать командой.

```
mdadm -E /dev/sd[b-e]
```

```
[root@localhost admin]# mdadm -E /dev/sd[b-e]
mdadm: No md superblock detected on /dev/sdb.
mdadm: No md superblock detected on /dev/sdc.
mdadm: No md superblock detected on /dev/sdd.
mdadm: No md superblock detected on /dev/sde.
[root@localhost admin]#
```

mdadm – специальная утилита для управления программными RAID массивами. В РЕД ОС уже предустановлена по умолчанию. В выводе команды видим сообщение ***«No md superblock detected»*** это означает, что признаки RAID на дисках отсутствуют.

Приступим к предварительной подготовке, а именно создадим на каждом диске раздел с помощью утилиты fdisk:

```
fdisk /dev/sdd
```

```
[root@localhost admin]# fdisk /dev/sdd

Добро пожаловать в fdisk (util-linux 2.30.2).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.

Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0x1e0bad61.

Команда (m для справки): n
Тип раздела
   p   основной (0 первичный, 0 расширеный, 4 свободно)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p
Номер раздела (1-4, default 1): 1
Первый сектор (2048-2097151, default 2048):
Последний сектор + число секторов или + размер{K,M,G,T,P} (2048-2097151, default
 2097151):

Создан новый раздел 1 с типом 'Linux' и размером 1023 MiB.

Команда (m для справки): t
Выбранный раздел 1
Шестнадцатеричный код (введите L для получения списка кодов): fd
Тип раздела 'Linux' изменен на 'Linux raid autodetect'.

Команда (m для справки): w
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

В консоли **fdisk** выберите:

- Создание раздела (n);
- Тип раздела primary (p);
- Номер раздела (1);
- Начальный и конечный блоки (Enter);
- Для изменения типа раздела (t);
- Шестнадцатеричный код раздела (fd);
- Применение изменений и выход (w).

Подобные действия повторяем и для оставшихся дисков: /dev/sdb, /dev/sdc, /dev/sde.

Создание RAID-массива

Для создания программного **RAID**-массива в РЕД ОС используется утилита **mdadm**.

```
mdadm --create /dev/md0 --level=10 --raid-devices=4 /dev/sd[b-e]1
```

Здесь:

- **/dev/md0** – имя устройства **RAID**;
- **--level=10** – уровень **RAID**;
- **--raid-devices=4** – количество дисков, участвующих в сборке массива;
- **/dev/sd[b-e]1** – имена дисков, участвующих в сборке массива.

```
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
```

Проверим состояние созданного RAID-массива:

```
cat /proc/mdstat
```

```
Personalities : [raid10]
md0 : active raid10 sde1[3] sdd1[2] sdc1[1] sdb1[0]
      2093056 blocks super 1.2 512K chunks 2 near-copies [4/4] [UUUU]

unused devices: <none>
```

Кроме этого следующая команда покажет более детальную информацию о созданном RAID массиве:

```
mdadm -D /dev/md0
```

Создание автоматического монтирования RAID

Создадим файловую систему **ext4** на **RAID**-устройстве **/dev/md0** и смонтируем массив в каталог **/mnt/raid10/**.

```
mkfs.ext4 /dev/md0
mkdir /mnt/raid10
mount /dev/md0 /mnt/raid10
```

```
ls -l /mnt/raid10/
```

Для автоматического подключения **RAID** добавим запись в конец файла /etc/fstab, для этого в терминале выполните команду:

```
echo "/dev/md0 /mnt/raid10 ext4 defaults 0 0" >> /etc/fstab
```

```
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/ro-root     /                       ext4    defaults        1 1
UUID=a4a309bc-6541-4c62-a675-4e5a17a4ffe8 /boot                   ext4    defau$
/dev/mapper/ro-swap     swap                    swap    defaults        0 0
/dev/md0                /mnt/raid10             ext4    defaults        0 0
```

А также сохраним конфигурацию **RAID**, чтобы во время загрузки системы происходило ее считывание.

```
mdadm --detail --scan --verbose >> /etc/mdadm.conf
```

Команда **lsblk** покажет, что тип дисков изменился на **RAID10**.

```
[root@localhost raid10]# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE   MOUNTPOINT
sda           8:0    0   25G  0 disk
├─sda1        8:1    0    1G  0 part   /boot
└─sda2        8:2    0   24G  0 part
  ├─ro-root 254:0    0 21,5G  0 lvm    /
  └─ro-swap 254:1    0  2,5G  0 lvm    [SWAP]
sdb           8:16   0    1G  0 disk
└─sdb1        8:17   0 1023M  0 part
  └─md0       9:0    0    2G  0 raid10 /mnt/raid10
sdc           8:32   0    1G  0 disk
└─sdc1        8:33   0 1023M  0 part
  └─md0       9:0    0    2G  0 raid10 /mnt/raid10
sdd           8:48   0    1G  0 disk
└─sdd1        8:49   0 1023M  0 part
  └─md0       9:0    0    2G  0 raid10 /mnt/raid10
sde           8:64   0    1G  0 disk
└─sde1        8:65   0 1023M  0 part
  └─md0       9:0    0    2G  0 raid10 /mnt/raid10
sr0          11:0    1    4G  0 rom    /run/media/admin/redos-MUROM-7.2 x86_64
[root@localhost raid10]#
```

Замена неисправного диска при сбое, добавление запасного диска

В RAID-массиве уровня 10 имеется возможность добавления запасного диска для быстрой замены при выходе из строя одного из основных устройств хранения.

Рассмотрим RAID-массив, состоящий из дисков **/dev/sdc**, **/dev/sdd**, **/dev/sde**, **/dev/sdf**.

```
[root@localhost user]# lsblk
NAME              MAJ:MIN RM  SIZE RO TYPE   MOUNTPOINT
sda                 8:0    0   15G  0 disk
├─sda1              8:1    0    1G  0 part   /boot
└─sda2              8:2    0   14G  0 part
  ├─ro_redos-root 253:0    0 12,5G  0 lvm    /
  └─ro_redos-swap 253:1    0  1,5G  0 lvm    [SWAP]
sdb                 8:16   0    1G  0 disk
sdc                 8:32   0    1G  0 disk
└─sdc1              8:33   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sdd                 8:48   0    1G  0 disk
└─sdd1              8:49   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sde                 8:64   0    1G  0 disk
└─sde1              8:65   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sdf                 8:80   0    1G  0 disk
└─sdf1              8:81   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sr0                11:0    1 1024M  0 rom
```

В примере диск **/dev/sdc** будет выведен из строя, а для его замены будет подключен новый диск **/dev/sdb**.

Проверим присутствие на диске метаданных RAID с помощью утилиты **mdadm**:

```
mdadm -E /dev/sdb
mdadm: No md superblock detected on /dev/sdb
```

Сообщение в выводе команды означает, что признаки RAID на диске отсутствуют.

Создадим на диске раздел с помощью утилиты **fdisk**:

```
fdisk /dev/sdb
```

```
[root@localhost user]# fdisk /dev/sdb

Добро пожаловать в fdisk (util-linux 2.34).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.

Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0xa18ed710.

Команда (m для справки): n
Тип раздела
   p   основной (0 первичный, 0 расширеный, 4 свободно)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p
Номер раздела (1-4, default 1): 1
Первый сектор (2048-2097151, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-2097151, default 2097151):

Создан новый раздел 1 с типом 'Linux' и размером 1023 MiB.

Команда (m для справки): t
Выбранный раздел 1
Шестнадцатеричный код (введите L для получения списка кодов): fd
Тип раздела 'Linux' изменен на 'Linux raid autodetect'.

Команда (m для справки): w
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

Далее повторно проверим раздел, добавим диск **/dev/sdb1** в массив **md0** и проверим добавление запасного диска в RAID-устройство:

```
mdadm --examine /dev/sdb1
mdadm: No md superblock detected on /dev/sdb1.

mdadm --add /dev/md0 /dev/sdb1
mdadm: added /dev/sdb1
```

Для отображения детальной информации о созданном RAID-массиве выполните:

```
mdadm --detail /dev/md0
```

```
[root@localhost user]# mdadm --detail /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Fri Feb  3 13:58:05 2023
        Raid Level : raid10
        Array Size : 2613760 (2.49 GiB 2.68 GB)
     Used Dev Size : 1045504 (1021.00 MiB 1070.60 MB)
      Raid Devices : 5
     Total Devices : 5
       Persistence : Superblock is persistent

       Update Time : Tue Feb  7 10:06:27 2023
             State : clean
    Active Devices : 5
   Working Devices : 5
    Failed Devices : 0
     Spare Devices : 0

            Layout : near=2
        Chunk Size : 512K

Consistency Policy : resync

              Name : localhost.localdomain:0  (local to host localhost.localdomain)
              UUID : 0ecf74ea:7be24e8d:715753c7:840fc39e
            Events : 75
```

Пометим диск **/dev/sdc1** в массиве **/dev/md0** как сбойный и проверим статус:

```
mdadm --manage --fail /dev/md0 /dev/sdc1
mdadm: set /dev/sdc1 faulty in /dev/md0

mdadm --detail /dev/md0
cat /proc/mdstat
```

```
[root@localhost user]# mdadm --detail /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Fri Feb  3 13:58:05 2023
        Raid Level : raid10
        Array Size : 2613760 (2.49 GiB 2.68 GB)
     Used Dev Size : 1045504 (1021.00 MiB 1070.60 MB)
      Raid Devices : 5
     Total Devices : 5
       Persistence : Superblock is persistent

       Update Time : Tue Feb  7 14:36:24 2023
             State : clean, degraded
    Active Devices : 4
   Working Devices : 4
    Failed Devices : 1
     Spare Devices : 0

            Layout : near=2
        Chunk Size : 512K

Consistency Policy : resync

              Name : localhost.localdomain:0  (local to host localhost.localdomain)
              UUID : 0ecf74ea:7be24e8d:715753c7:840fc39e
            Events : 77
```

После завершения процесса синхронизации статус будет изменен на **[UU]**. Для дисков большого размера процесс синхронизации может занять длительное время.

Удаление диска из массива

Утилита **mdadm** с ключом **--remove** удалит из массива указанный команде диск. Удалим диск **/dev/sdc1** из **/dev/md0**, который ранее был помечен как сбойный и проверим статус:

```
mdadm --remove /dev/md0 /dev/sdc1
mdadm: hot removed /dev/sdc1 from /dev/md0

cat /proc/mdstat
Personalities : [raid10]
md0 : active raid10  sdb1[4]  sdf1[3]  sde1[2]  sdd1[1]
     2091008 blocks super 1/2  512K chunks  2  near-copies [4/4] [UUUU]

unused devices: <none>
```

Расширение массива

Проверим отображение нового подключенного диска (**/dev/sdg**) с помощью **lsblk**.

```
[root@localhost user]# lsblk
NAME              MAJ:MIN RM  SIZE RO TYPE   MOUNTPOINT
sda                 8:0    0   15G  0 disk
├─sda1              8:1    0    1G  0 part   /boot
└─sda2              8:2    0   14G  0 part
  ├─ro_redos-root 253:0    0 12,5G  0 lvm    /
  └─ro_redos-swap 253:1    0  1,5G  0 lvm    [SWAP]
sdb                 8:16   0    1G  0 disk
└─sdb1              8:17   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sdc                 8:32   0    1G  0 disk
└─sdc1              8:33   0 1023M  0 part
sdd                 8:48   0    1G  0 disk
└─sdd1              8:49   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sde                 8:64   0    1G  0 disk
└─sde1              8:65   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sdf                 8:80   0    1G  0 disk
└─sdf1              8:81   0 1023M  0 part
  └─md0             9:0    0    2G  0 raid10 /mnt/raid10
sdg                 8:96   0    1G  0 disk
sr0                11:0    1 1024M  0 rom
```

Затем добавим диск в массив, увеличим размер массива и проверим статус RAID следующими командами:

```
mdadm --add /dev/md0 /dev/sdg1
mdadm --grow --raid-devices=5 /dev/md0
mdadm --detail /dev/md0
cat /proc/mdstat
```

Сохраним конфигурацию RAID в **/etc/mdadm.conf** командой:

```
mdadm --detail --scan >> /etc/mdadm.conf
```

Установка РЕД ОС на программный массив RAID1 и RAID10

Установка РЕД ОС на программный массив уровня RAID 1 для систем с UEFI
Решение проблемы недоступности одного из дисков
Установка РЕД ОС на программный массив уровня RAID 10

Особенности программного RAID-массива:

- *Гибкость*: управление RAID происходит с помощью операционной системы, поэтому такой массив можно настроить из работающей системы без перенастройки оборудования.
- *Открытый исходный код*: реализация программного RAID-массива основана открытом программном коде.
- *Никаких дополнительных расходов*: программный RAID не требует специального аппаратного обеспечения и не привязан к конкретному оборудованию.
- *Ресурсные затраты*: в течение всего срока существования программный RAID критикуют за повышенное использование аппаратных ресурсов. Такие программные реализации как mdadm практически полностью устраняют эту проблему на современном оборудовании.

Установка РЕД ОС на программный массив уровня RAID 1 для систем с UEFI

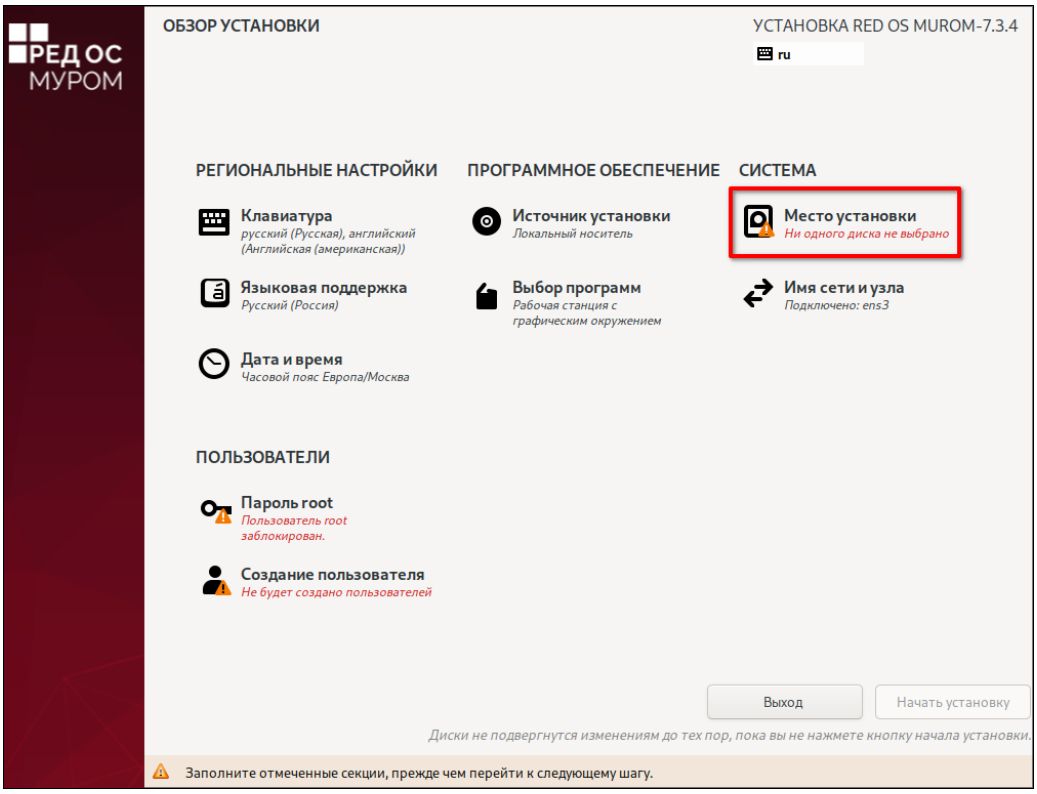
RAID 1 состоит из так называемого «зеркалирования» данных без их контроля четности и чередования. В такой реализации данные записываются идентично на два или более дисков, тем самым создавая «зеркальный набор» дисков. Таким образом, все диски в массиве являются полными копиями друг друга, что обеспечивает высокую надежность, но в то же время появляется избыточность данных.

Для установки РЕД ОС на **RAID 1** выполните следующие действия:

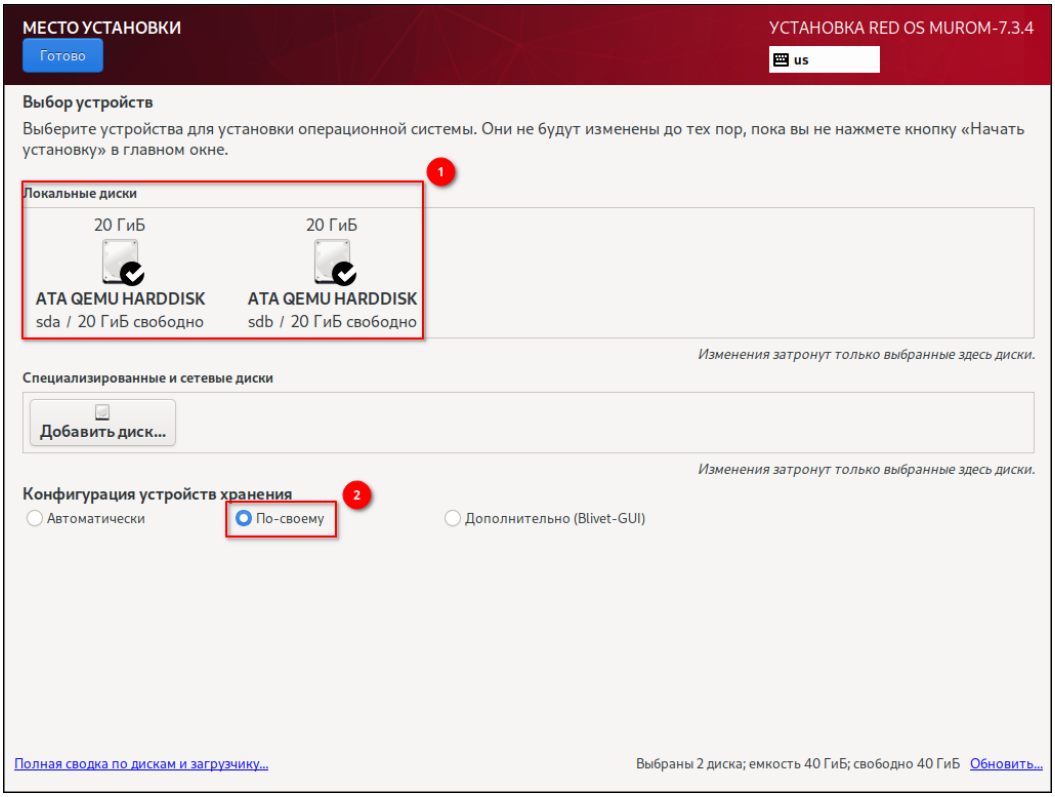
1. Выберите первый пункт «**Установить RED OS**».



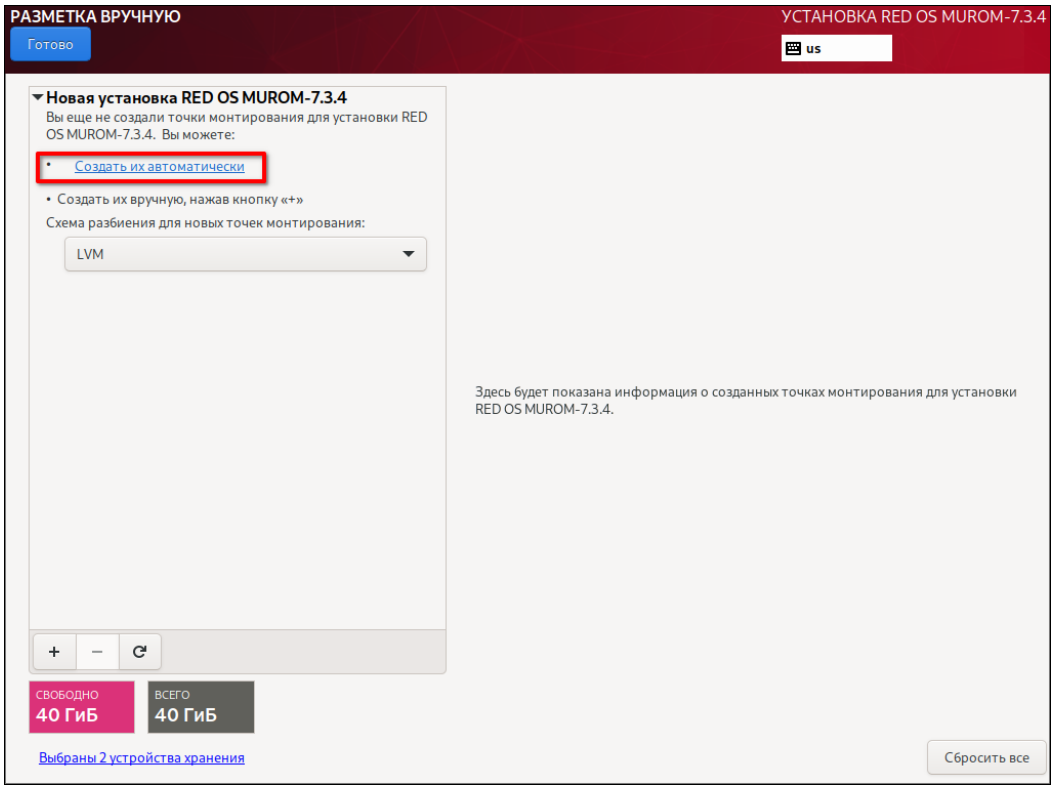
2. Перейдите в раздел для разметки дисков, выбрав пункт «**Место установки**».



3. В окне «**Место установки**» выберите необходимые для разметки диски (в примере отмечены два диска по 20 ГБ), активируйте чекбокс для варианта «**По-своему**», а затем нажмите «**Готово**».



4. Создайте необходимые разделы, нажав «**Создать их автоматически**».

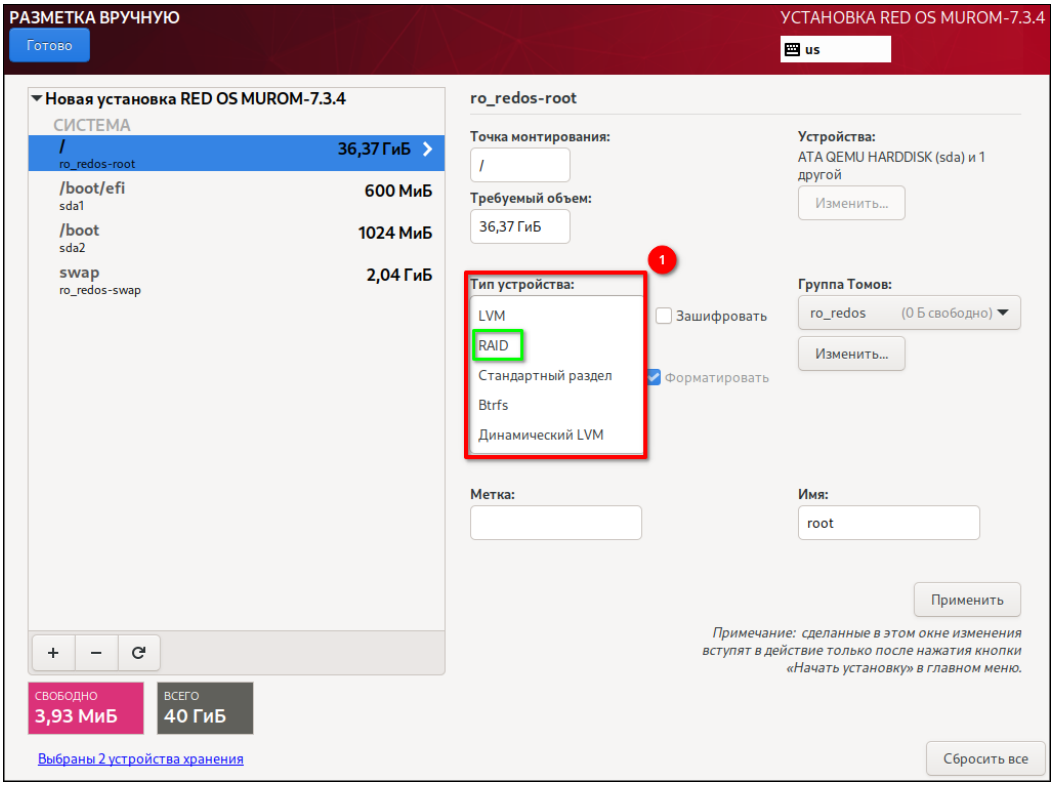


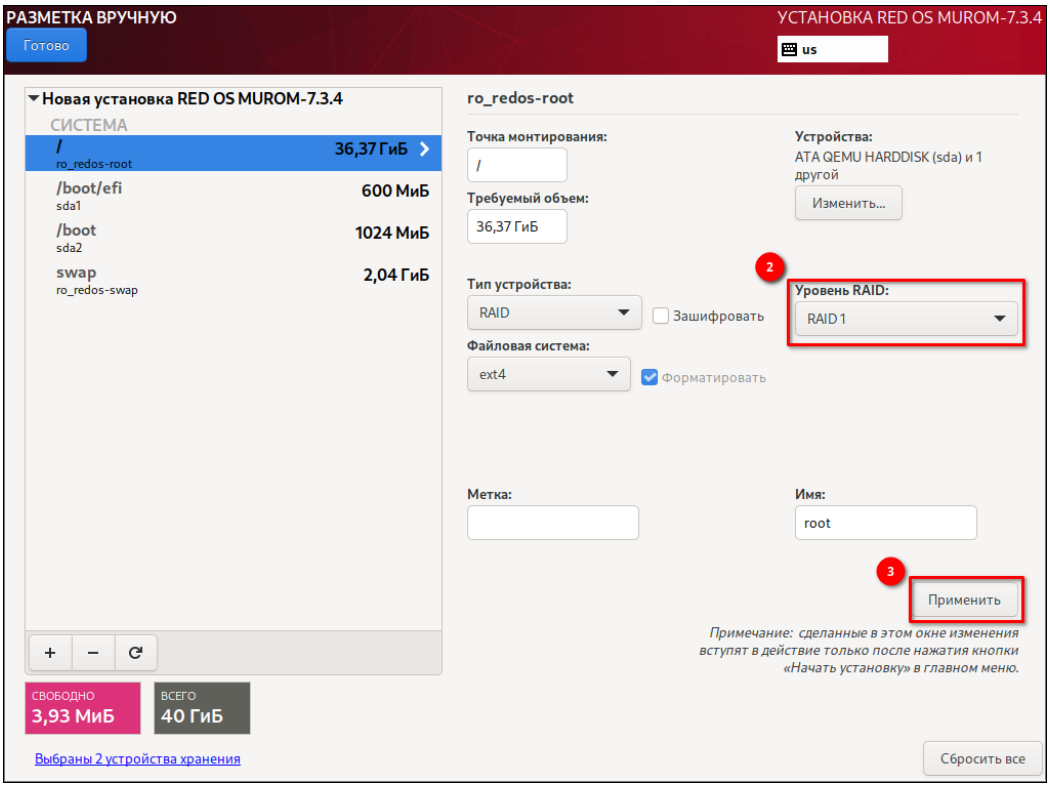
5. После разметки в правой части окна выполните следующие действия:

5.1 Выбрать «**Тип устройства**» — **RAID**.

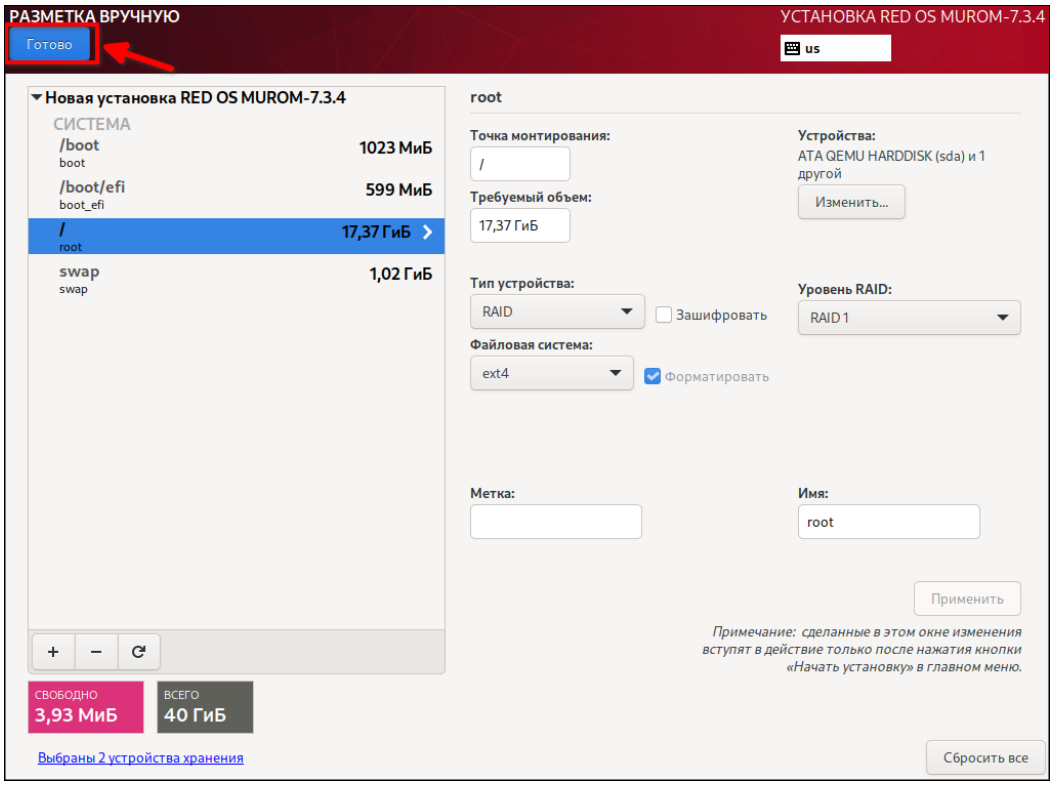
5.2 В группе «**Уровень RAID**» — указать необходимый тип RAID-массива (в примере выбран **RAID1**).

5.3 Нажмите кнопку «**Применить**».





6. Повторите операцию выбора типа устройства (**RAID**) и уровня **RAID** для всех остальных разделов: **/boot/efi**, **/boot**, **swap**.



7. По нажатии кнопки «**Готово**» будет открыто окно с итоговой таблицей разметки – при необходимости проверьте установленные параметры и, если все настроено верно, нажмите «**Принять изменения**».

8. Далее установите ОС в штатном режиме.

Решение проблемы недоступности одного из дисков

Для подготовки разделов диска на случай, если один из дисков будет недоступен, необходимо:

1. Вывести и запомнить идентификаторы (**UUID**) дисков командой:

```
lsblk -fs
```

2. Изменить **UUID** для **sdb1** и **sdb2** из вывода команды `lsblk -fs`:

```
mkdosfs -i <UUID_sda1> /dev/sdb1
e2fsck -f /dev/sdb2
tune2fs /dev/sdb2 -U <UUID_sda2>
```



3. Скопировать данные на **/dev/sdb1** для EFI-раздела:

```
mount /dev/sdb1 /mnt
cp -R /boot/efi/EFI/ /mnt
```

После чего отмонтировать раздел:

```
umount /dev/sdb1
```

4. Скопировать на **/dev/sdb2** данные из **/dev/sda2** для **boot**-раздела:

```
mount /dev/sda2 /media
mount /dev/sdb2 /mnt
```

```
cp -R /media/* /mnt/
umount /media /mnt
```

После этого система с **UEFI** сможет найти загрузчик на любом из дисков, который будет доступен.

В случае если система с **UEFI** не смогла самостоятельно обнаружить загрузочную запись, можно прописать ее самостоятельно. Для этого:

1. Загрузитесь в rescue с USB/DVD-диска:

```
chroot /mnt/sysroot
```

2. Переведите SELinux в режим permissive:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

3. Выведите информацию о загрузочных записях:

```
efibootmgr -v
```

4. Пропишите загрузчик командой:

```
efibootmgr -c -d /dev/sdb -p 1 -L "RED OS 2" -l "\EFI\redos\shimx64.efi"
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

```
[root@localhost ~]# efibootmgr -v
BootCurrent: 0005
Timeout: 0 seconds
BootOrder: 0008,0005,0000,0001,0002,0003,0004,0006
Boot0000* UiApp FvVol(7cb8bdc9-f8eb-4f34-aaea-3ee4af6516a1)/FvFile(462caa21-7614-4503-836e-8ab6f4662331)
Boot0001* UEFI VBOX CD-ROM VB2-01700376         PciRoot(0x0)/Pci(0x1,0x1)/Ata(1,0,0)N.....YM....R,Y.
Boot0002* UEFI VBOX HARDDISK VB4eb3ffe3-127cf754        PciRoot(0x0)/Pci(0xd,0x0)/Sata(0,65535,0)N.....YM....R,Y.
Boot0003* UEFI VBOX HARDDISK VB241a0996-68ce5c4d        PciRoot(0x0)/Pci(0xd,0x0)/Sata(1,65535,0)N.....YM....R,Y.
Boot0004* EFI Internal Shell    FvVol(7cb8bdc9-f8eb-4f34-aaea-3ee4af6516a1)/FvFile(7c04a583-9e3e-4f1c-ad65-e05268d0b4d1)
Boot0005* RED OS        HD(1,GPT,ec410ecf-c449-4fd1-b696-e38825b1dd91,0x800,0x12c000)/File(\EFI\redos\shimx64.efi)
Boot0006* UEFI PXEv4 (MAC:080027388CEE) PciRoot(0x0)/Pci(0x3,0x0)/MAC(080027388cee,1)/IPv4(0.0.0.00.0.0.0,0,0)N.....YM....R,Y.
Boot0008* RED OS 2      HD(1,GPT,390bc59e-4ecc-4262-9f98-155a2a826e1a,0x800,0x12c000)/File(\EFI\redos\shimx64.efi)
[root@localhost ~]#
```

Если потребуется удалить запись, выполните команду:

```
efibootmgr -b 6 -B
```

где:

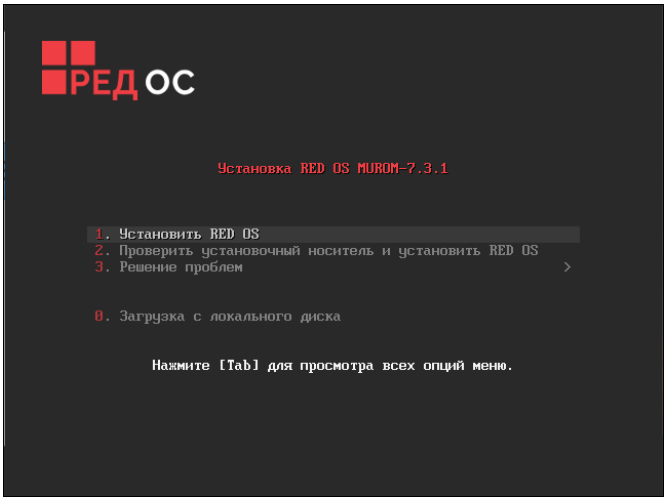
- **-b** (**--bootnum**) – указывает на номер записи;
- **-B** (**--delete-bootnum**) – указывает удалить запись.

Установка РЕД ОС на программный массив уровня RAID 10

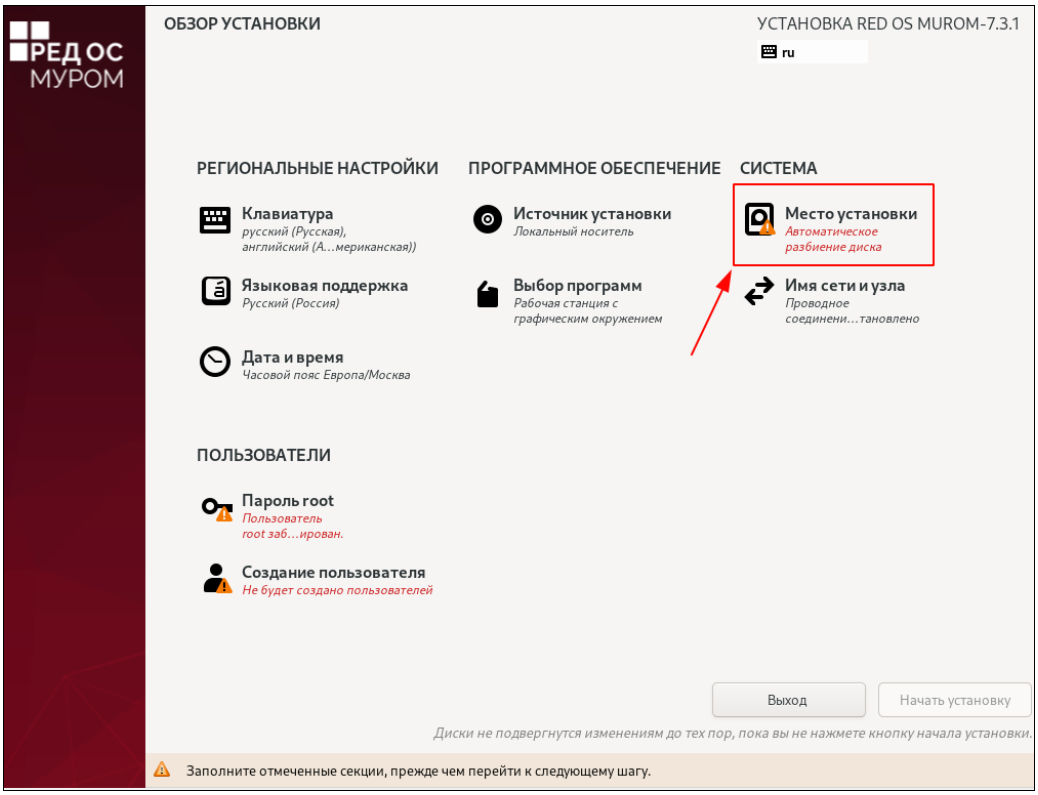
RAID 10 представляет собой объединение массивов **RAID 1** и **RAID 0**. Для создания **RAID 10** требуется **минимум четыре диска**, в которых данные чередуются на зеркальных парах. Пока один диск в каждой зеркальной паре функционирует, данные могут быть извлечены. В случае сбоя двух дисков в одной зеркальной паре все данные будут потеряны из-за отсутствия четности в чередующихся наборах.

Для установки РЕД ОС на **RAID 10** выполните следующие действия:

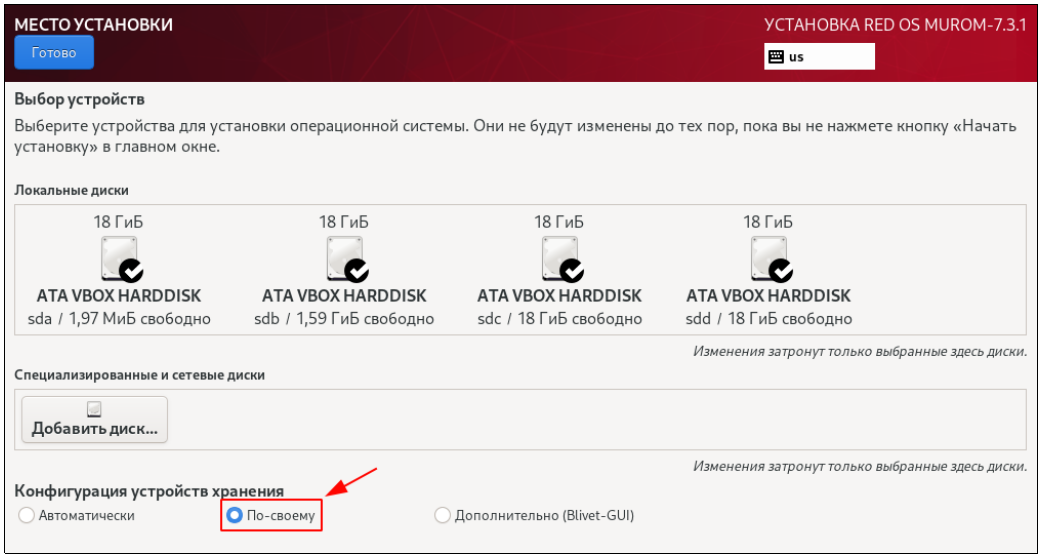
1. Выберите первый пункт «**Установить RED OS**».



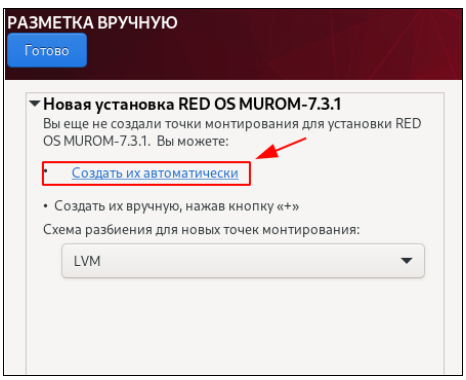
2. Перейдите в раздел для разметки дисков (пункт «**Место установки**»).



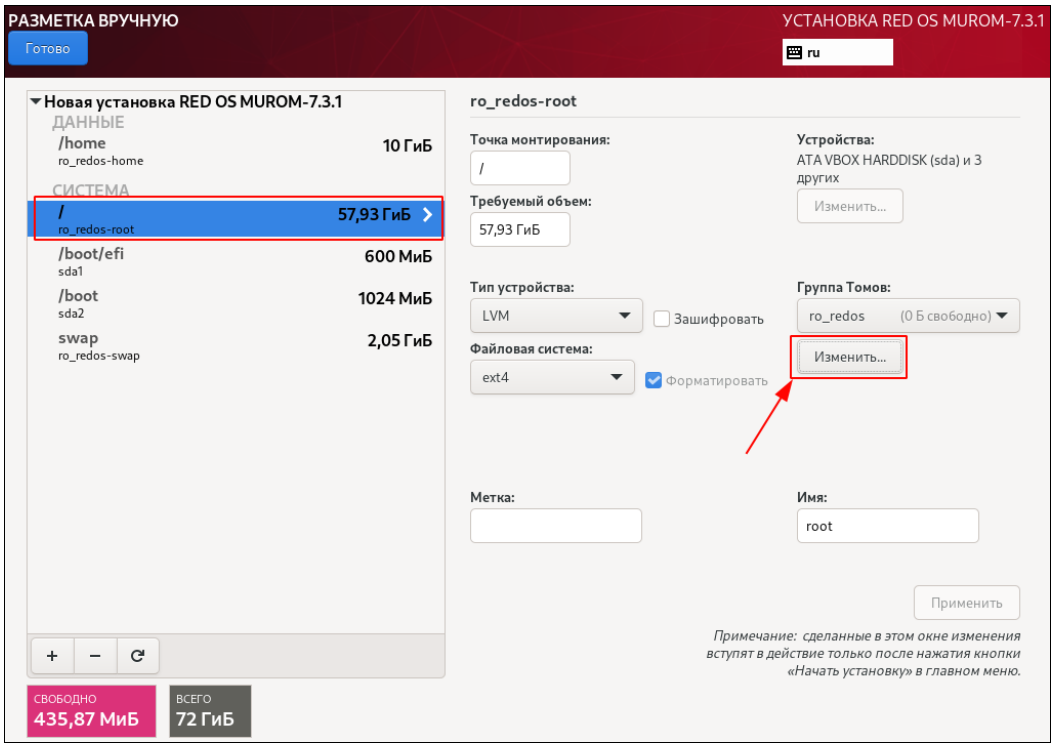
3. В данном окне отметьте все локальные диски, нажмите кнопку «**По-своему**», а затем «**Готово**».



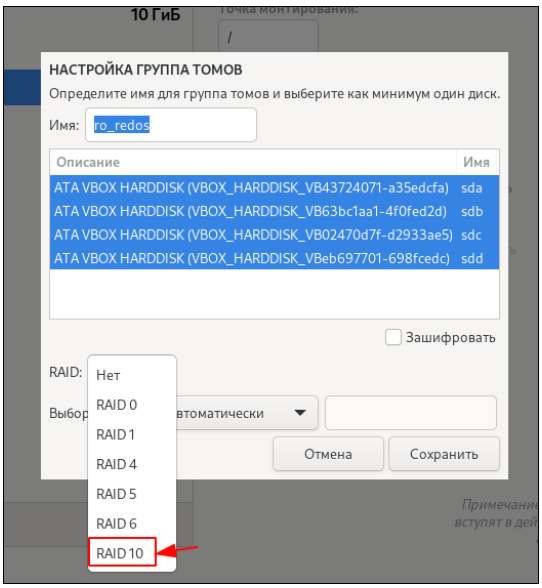
4. Нажмите на пункт «**Создать их автоматически**».



5. В конфигураторе разметки дисков определите нужный размер для корневого и домашнего раздела через параметр «**Требуемый объем**». После этого выберите корневой раздел и в группе томов нажмите на кнопку « **Изменить**».



6. В окне настройки группы томов из списка **RAID** выберите «**RAID 10**».



7. Итоговая таблица разметки:

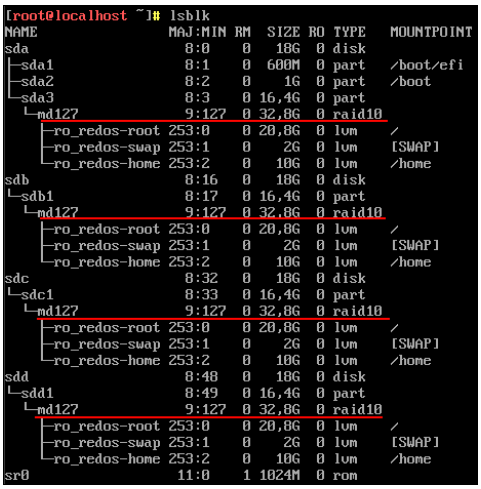
ОБЗОР ИЗМЕНЕНИЙ

Новые настройки приведут к следующим изменениям, которые вступят в силу после возврата в главное меню и начала установки:

Порядок	Действие	Тип	Устройство	Точка монтирования
3	удалить форматирование	Unknown	ATA VBOX HARDDISK (sdb)	
4	удалить форматирование	Unknown	ATA VBOX HARDDISK (sda)	
5	создать форматирование	таблица разделов (GPT)	ATA VBOX HARDDISK (sdd)	
6	создать устройство	partition	sdd1 на ATA VBOX HARDDISK	
7	создать форматирование	software RAID	sdd1 на ATA VBOX HARDDISK	
8	создать форматирование	таблица разделов (GPT)	ATA VBOX HARDDISK (sdc)	
9	создать устройство	partition	sdc1 на ATA VBOX HARDDISK	
10	создать форматирование	software RAID	sdc1 на ATA VBOX HARDDISK	
11	создать форматирование	таблица разделов (GPT)	ATA VBOX HARDDISK (sdb)	
12	создать устройство	partition	sdb1 на ATA VBOX HARDDISK	
13	создать форматирование	software RAID	sdb1 на ATA VBOX HARDDISK	
14	создать форматирование	таблица разделов (GPT)	ATA VBOX HARDDISK (sda)	
15	создать устройство	partition	sda1 на ATA VBOX HARDDISK	
16	создать форматирование	EFI System Partition	sda1 на ATA VBOX HARDDISK	/boot/efi
17	создать устройство	partition	sda2 на ATA VBOX HARDDISK	
18	создать форматирование	ext4	sda2 на ATA VBOX HARDDISK	/boot
19	создать устройство	partition	sda3 на ATA VBOX HARDDISK	
20	создать форматирование	software RAID	sda3 на ATA VBOX HARDDISK	
21	создать устройство	mdarray	MDRAID set (raid10) (pv00)	
22	создать форматирование	physical volume (LVM)	MDRAID set (raid10) (pv00)	
23	создать устройство	lvmvg	ro_redos	
24	создать устройство	lvmlv	ro_redos-root	
25	создать форматирование	ext4	ro_redos-root	/
26	создать устройство	lvmlv	ro_redos-home	
27	создать форматирование	ext4	ro_redos-home	/home
28	создать устройство	lvmlv	ro_redos-swap	

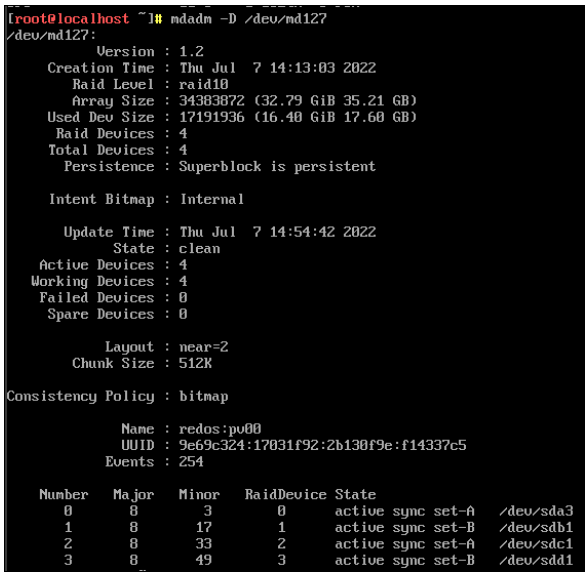
Отменить и вернуться к настройке разделов | Принять изменения

8. После установки можно просмотреть информацию о разделах на **RAID 10**:



Команда `lsblk` показывает, что **md127** – это **RAID 10**. Также видно, что на каждом из дисков **sda**, **sdb**, **sdc**, **sdd** созданы разделы с точками монтирования **swap**, **home** и **корень** (/), которые являются точными копиями друг друга. В RAID-массиве десятого уровня данные делятся на блоки и дублируются на паре дисков.

Команда `mdadm -D /dev/md127` выведет на экран детальную информацию о RAID-массиве.



```
[root@localhost ~]# mdadm -D /dev/md127
/dev/md127:
           Version : 1.2
     Creation Time : Thu Jul  7 14:13:03 2022
        Raid Level : raid10
        Array Size : 34383872 (32.79 GiB 35.21 GB)
     Used Dev Size : 17191936 (16.40 GiB 17.60 GB)
      Raid Devices : 4
     Total Devices : 4
       Persistence : Superblock is persistent

     Intent Bitmap : Internal

       Update Time : Thu Jul  7 14:54:42 2022
             State : clean
    Active Devices : 4
   Working Devices : 4
    Failed Devices : 0
     Spare Devices : 0

            Layout : near=2
        Chunk Size : 512K

Consistency Policy : bitmap

              Name : redos:pv00
              UUID : 9e69c324:17031f92:2b130f9e:f14337c5
            Events : 254

    Number   Major   Minor   RaidDevice State
       0       8        3        0      active sync set-A   /dev/sda3
       1       8       17        1      active sync set-B   /dev/sdb1
       2       8       33        2      active sync set-A   /dev/sdc1
       3       8       49        3      active sync set-B   /dev/sdd1
```

Автоматизация развертывания (kickstart)

Порядок установки
Создание файла кикстарта
Проверка файла кикстарт
Расположение файла кикстарта
Создание загрузочного диска
Начало установки
Запуск установки вручную
Автоматический запуск установки
Синтаксис кикстарта
Команды и интерпретаторы
Секция %packages
Секция %pre
Секция %post
Пример файла конфигурации

Процесс установки операционной системы можно автоматизировать, определив все необходимые данные (список пакетов, схемы разделов, часовой пояс, языковые настройки и т. д.) в одном файле — файле **kickstart**. Файлы кикстарта могут располагаться на отдельном сервере и подгружаться во время установки.

Данный способ очень удобен и является наиболее предпочтительным для сетевых и системных администраторов, т.к. один файл может использоваться для одновременной установки системы на нескольких компьютерах.

Сценарии и журналы кикстарта хранятся в каталоге **/tmp** для помощи в диагностике ошибок при установке.

Порядок установки

Автоматизированная установка может быть запущена с локального жесткого диска, DVD или с сервера NFS, FTP, HTTP, HTTPS.

Для этого необходимо:

1. Создать файл кикстарта.

2. Записать файл на локальный или удаленный носитель.

3. Создать загрузочный диск, с которого будет запускаться установка.

4. Предоставить доступ к установочной структуре.

5. Начать процесс установки.

Создание файла кикстарта

Файл кикстарта представляет собой обычный текстовый файл, содержащий параметры установки, каждый из которых определяется ключевым словом. Файл можно создать самостоятельно в любом текстовом редакторе, способном сохранять файлы в формате ASCII, например, в vim, либо модифицировать готовый шаблон, который автоматически создается в ходе установки системы, исходя из выбранных параметров. Файл (шаблон) **anaconda-ks.cfg** можно найти в каталоге **/root/**.

При создании файла кикстарта следует придерживаться нескольких рекомендаций:

- Секции файла должны быть упорядочены. Элементы внутри секций могут располагаться в любом порядке. Порядок секций следующий:
    - Раздел команд (обязательные параметры должны быть определены);
    - Раздел **%packages**;
    - Разделы **%pre** и **%post**, которые могут следовать в любом порядке и обязательными не являются.

ВАЖНО!

Секции **%packages**, **%post** и **%pre** должны завершаться директивой **%end**. В противном случае файл не будет обработан.

- Элементы, не отмеченные как обязательные, могут быть опущены;
- Если обязательный параметр не определен, программа установки предложит его ввести так же, как и во время обычной

установки. После получения ответа установка будет продолжена без вмешательства пользователя (если снова не столкнется с отсутствующим параметром);

- Строки, начинающиеся с символа **#**, интерпретируются как комментарии и игнорируются.

Проверка файла кикстарт

После создания файла кикстарта рекомендуется проверить его формат. Для этого в репозитории РЕД ОС имеется программа **ksvalidator** в составе пакета **pykickstart**.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install pykickstart
```

Для проверки формата файла выполните команду (с правами локального пользователя):

```
ksvalidator /<путь_к_файлу>/kickstart.ks
```

В параметре <путь_к_файлу> укажите свой актуальный путь.

Подробную информацию по использованию **ksvalidator** см. в справке `man ksvalidator`.

Примечание.

Возможности такой проверки **ограничены**. Структура файла может быть достаточно сложной и, несмотря на то, что **ksvalidator** проверит синтаксис файла и поможет убедиться в отсутствии устаревших параметров, это **не гарантирует** успех установки. Более того, секции *%pre*, *%post* и *%packages* **не проверяются**.

Расположение файла кикстарта

Файл кикстарта может быть расположен:

- на съемном носителе (DVD, USB);
- на локальном жестком диске;
- на доступном сетевом ресурсе.

Размещение файла кикстарта в сети используется чаще — для автоматизации установки в системах, подключенных к сети. Сначала устанавливаемая система загружается с PXE-сервера, затем файл кикстарта загружается с удаленного диска, а перечисленные в файле пакеты в дальнейшем будут установлены в системе.

Доступ программы установки к файлу кикстарта необходимо обеспечить аналогично тому, как это делается для установочных образов.

Создание загрузочного диска

Подробную информацию о создании загрузочных носителей и записи iso-образов см. в нашей инструкции «Создание загрузочных носителей».

Начало установки

Для запуска кикстарт-установки используется параметр `inst.ks=`.

Также установку можно запустить с PXE-сервера. В файл конфигурации загрузчика можно добавить параметр автоматического запуска установки. Этот подход позволяет полностью автоматизировать процесс загрузки.

Приведенные ниже инструкции являются общими и могут отличаться в зависимости от архитектуры.

Запуск установки вручную

Ручной запуск установки подразумевает некоторую степень взаимодействия с пользователем, например, добавление параметров в строке `boot:`.

Для запуска установки необходимо выполнить следующие действия:

1. Загрузить систему с локального носителя (CD, DVD, USB).

2. В строке приглашения загрузки добавить параметр **inst.ks=<путь_к_файлу>/kickstart.ks**, где вместо <путь_к_файлу> укажите свой путь. Если файл расположен на другом компьютере в сети, дополнительно потребуется определить параметр `ip=`. Обычно также требуется указать расположение пакетов с помощью `inst.repo=`.

3. Подтвердите выбранные параметры и начните установку.

Если файл кикстарта не содержит ошибок, процесс установки сможет завершиться без необходимости ввода каких-либо данных.

Автоматический запуск установки

Для автоматического запуска установки необходимо выполнить следующие действия:

1. Открыть файл конфигурации загрузчика на PXE-сервере и добавить параметр `inst.ks=`.

- для систем с **BIOS** можно использовать файл **default** или путь, определяемый с помощью IP-адреса. В конец строки **append** необходимо добавить параметр `inst.ks=`:

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
...
APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp method=http://192.168.1.38/images/REDOS/
devfs=nomount inst.ks=http://192.168.1.38/ks.cfg
...
```

- для систем с **UEFI** параметр `inst.ks=` добавляется к строке **kernel** в файле **grub.cfg**:

```
kernel vmlinuz inst.ks=http://192.168.1.38/ks.cfg
```

Пример grub.cfg:

```
function load_video {
insmod efi_gop
insmod efi_uga
insmod video_bochs
insmod video_cirrus
insmod all_video
}
load_video
set gfxpayload=keep
insmod gzio
menuentry 'REDOS 7.3' {
linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp kernel vmlinuz inst.repo=http://192.168.1.38/images/REDOS/
inst.ks=http://192.168.1.38/ks.cfg
initrd images/REDOS/images/pxeboot/initrd.img
}
```

2. Загрузить программу установки с сервера PXE.

Если файл кикстарта не содержит ошибок, процесс установки сможет завершиться без необходимости ввода каких-либо данных.

Синтаксис кикстарта

Примечание.

Если за параметром следует знак равенства, необходимо определить его значение. В приведенных примерах параметры в квадратных скобках (**[ ]**) не являются обязательными.

Ниже будут рассмотрены основные необходимые команды для создания файла кикстарта.

Команды и интерпретаторы

bootloader

bootloader (обязательный) — определяет порядок установки загрузчика.

Параметры:

- **--append=** — содержит список параметров ядра (указываются через запятую), например:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

Параметры **rhgb** и **quiet** используются по умолчанию, даже если они явно не заданы, или строка `--append=` вовсе не определена.

- **--boot-drive=** — диск, на который будет записан загрузчик и с которого будет загружаться система.
- **--driveorder** — определяет порядок загрузки в BIOS, например:

```
bootloader --driveorder=sda,hda
```

- **--location=** — место расположения загрузочной записи. Допустимые значения:
  - *mbr* (используется по умолчанию) - его поведение определяется наличием MBR или GPT;
  - *partition* — установка загрузчика в первый сектор раздела, содержащего ядро;
  - *none* — не устанавливать загрузчик.

В большинстве случаев этот параметр можно не определять.

- **--password=** — пароль GRUB2. Рекомендуется установить пароль для ограничения доступа к оболочке GRUB2 во избежание несанкционированной передачи параметров ядру.

Если пароль задан, будет предложено ввести имя пользователя. По умолчанию будет выбран пользователь **root**.

- **--iscrypted** — разрешает использование зашифрованного пароля, который изначально был создан помощью параметра `--password=`. В противном случае пароль хранится в открытой форме.

Пароль можно зашифровать с помощью команды `grub2-mkpasswd-pbkdf2`. Скопируйте код из строки вывода, начинающейся с `grub.pbkdf2`, и сохраните его в файл кикстарта. Пример записи с зашифрованным паролем:

```
bootloader --iscrypted --
password=grub.pbkdf2.sha512.10000.5520C6C9832F3AC3D149AC0B24BE69E2D4FB0DBEEDBD2<...>95CA4BA4381F8550510B75E8E0BB2938990.
C688B6F0EF935701FF9BD1A8EC7FE5B<...>EA3384E56EB38A2E39102F5334C47405E
```

- **--timeout=** — время ожидания в секундах, по истечении которого начнется загрузка в соответствии с параметром `--default=`.
- **--default=** — определяет загрузочный образ, который будет использоваться по умолчанию.

clearpart

clearpart (дополнительный) — удаляет разделы с диска, прежде чем создавать новые. По умолчанию разделы не удаляются.

Параметры:

- **--all** — удаляет все разделы.
- **--drives=** — удаляет разделы на заданных дисках:

```
clearpart --drives=hda,hdb --all
```

- **--list=** — список разделов для удаления. Допускается выбор разделов на разных дисках. Этот параметр переопределяет **--all** и **--linux**.

```
clearpart --list=sda2,sda3,sdb1
```

- **--initlabel** — метка диска, которая будет выбираться по умолчанию для заданной архитектуры (например, msdos для x86).

Используется вместе с **--all**.

- **--linux** — удаляет разделы Linux.
- **--none** (по умолчанию) — не удалять разделы.

keyboard

keyboard (дополнительный) — выбор раскладки клавиатуры.

Параметры:

- **--vckeymap=** — определяет раскладку VConsole. В качестве значения можно выбирать имена файлов из **/usr/lib/kbd/keymaps/*** без расширения **.map.gz**.
- **--xlayouts=** — список раскладок X через запятую без пробелов. Значения можно определить в форме `<раскладка>` (например, cz) или `<раскладка_(вариант)>` (например, cz (qwerty)).

Полный список раскладок можно найти на справочной странице `xkeyboard-config(7)`, в секции **Layouts**.

- **--switch=** — комбинации клавиш для переключения между раскладками. Несколько значений разделяются запятыми без пробелов. Например, переключение раскладки клавиатуры сочетанием «*Alt+Shift*» выглядит следующим образом:

```
keyboard --xlayouts=us,ru --switch=grp:alt_shift_toggle
```

Описание дополнительных параметров можно найти на справочной странице `xkeyboard-config(7)`, в секции **Options**.

ВАЖНО!

Опции **--vckeymap=** и **--xlayouts=** не должны использоваться вместе.

lang

lang (обязательный) — определяет язык, который будет использоваться в ходе установки и по умолчанию — в установленной системе. Пример выбора английского языка:

```
lang en_US
```

Список кодов языков приведен в файле **/usr/share/system-config-language/locale-list**, в первом столбце.

Некоторые языки, в частности китайский, японский, корейский и языки индийской группы, не поддерживаются в текстовом режиме установки. Если такого рода язык задан с помощью команды **lang**, установка будет продолжена на английском, а указанный язык будет включен в готовой системе.

Параметры:

- **--addsupport=** — список дополнительных языков через запятую без пробелов.

```
lang en_US --addsupport=ru_RU,de_DE
```

logvol

logvol (дополнительный) — помогает создать логический том LVM.

Формат команды:

```
logvol <точка_монтирования> --vgname=<имя_группы> --size=<размер> --name=<имя> [<параметры>]
```

Параметры:

- **--noformat** — использует существующий логический том без форматирования.
- **--useexisting** — использует существующий логический том и повторно его форматирует.
- **--fstype=** — тип файловой системы: xfs, ext2, ext3, ext4, swap или vfat.
- **--fsoptions=** — строка параметров монтирования файловой системы, заключенная в кавычки. В готовой системе эта строка будет

записана в **/etc/fstab**.

- **--label=** — метка логического тома.
- **--grow** — увеличить размер логического тома до заданной величины или заполнить все свободное место.
- **--size=** — минимальный размер тома в мегабайтах.
- **--maxsize=** — максимально допустимый размер тома в мегабайтах. Укажите целое значение без единиц, например 500.
- **--resize** — изменение размера тома. Также надо будет определить параметры **--useexisting** и **--size**.
- **--percent=** — размер увеличения логического тома в процентной доле от доступного места в группе томов. Используется вместе с **--size** и **--grow**.

Сначала необходимо создать раздел, затем группу логических томов, а уже потом — логический том:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

network

network (дополнительный) — настройка сетевого окружения. По умолчанию будет включено первое указанное в команде устройство. Активацию конкретного устройства можно явно запросить с помощью **--activate**.

Параметры:

- **--activate** — отвечает за активацию устройства.

Если этот параметр указан применительно к уже активному устройству, будет выполнена его повторная активация согласно настройкам в файле кикстарта.

- **--nodefroute** — запрещает использовать стандартный маршрут.
- **--bootproto=** — может принимать одно из следующих значений: *dhcp* (используется по умолчанию), *bootp*, *static*.

В режиме DHCP для получения сетевых настроек используется DHCP-сервер. Как можно догадаться, в случае с BOOTP для получения сетевых настроек подобным образом используется сервер BOOTP. Чтобы настроить функции DHCP, добавьте:

```
network --bootproto=dhcp
```

Чтобы настроить получение сетевой конфигурации с помощью BOOTP, добавьте в файл кикстарта:

```
network --bootproto=bootp
```

Для метода **static** в файле кикстарта необходимо определить *IP*, *маску сети*, *шлюз* и *сервер имен*. Эти данные не изменяются и используются во время и после установки.

Все данные статической конфигурации должны быть указаны в одной строке.

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 --gateway=10.0.2.254 --nameserver=10.0.2.1
```

- **--device=** — сетевое устройство.

Если в первом вхождении команды network не указан параметр `--device=`, по умолчанию будет использоваться значение параметра загрузки `ksdevice=`. Это поведение считается устаревшим, поэтому рекомендуется явно определить значение `--device=`.

Для всех последующих команд **network** необходимо явно определить `--device=`.

Устройства могут быть заданы:

- по *имени* интерфейса, например eth0,
- по *MAC-адресу*, например 01:23:45:67:89:ab,
- по ключевому слову *link*, которое определяет первый интерфейс со статусом up.
- по ключевому слову *bootif* с целью наследования адреса MAC из переменной BOOTIF. Чтобы pxelinux смог определить переменную BOOTIF, включите **IPAPPEND 2** в файл **pxelinux.cfg**.

Например:

```
network --bootproto=dhcp --device=em1
```

- **--ip=** — адрес устройства.
- **--ipv6=** — IPv6-адрес устройства в формате `<адрес>[/<префикс> <длина>]`, например **3ffe:ffff:0:1::1/128**. Если префикс не задан, по умолчанию будет использоваться 64. Другие допустимые значения включают *auto* (автоматическая конфигурация) и *dhcp* (DHCPv6).
- **--gateway=** — IPv4-адрес шлюза.
- **--ipv6gateway=** — IPv6-адрес шлюза.
- **--nodefroute** — определяет, что выбранный интерфейс не может использоваться по умолчанию. Обычно устанавливается при активации дополнительных устройств с помощью `--activate=` — например для сетевой карты в другой подсети или цели iSCSI.
- **--nameserver=** — IP-адрес сервера имен. Несколько серверов разделяются запятыми.
- **--nodns** — не настраивать DNS-сервер.
- **--netmask=** — маска сети.
- **--hostname=** — имя устанавливаемой системы.
- **--wepkey=** — ключ WEP беспроводной сети.
- **--wpakey=** — ключ WPA беспроводной сети.
- **--onboot=** — активация устройства при загрузке.
- **--dhcpclass=** — класс DHCP.
- **--noipv4** — отключает IPv4.
- **--noipv6** — отключает IPv6.

part, partition

part, partition (обязательный) — отвечает за создание раздела.

> **ВАЖНО!**
>
> Если параметры **--noformat** и **--onpart** не определены, создаваемые разделы будут форматироваться в процессе установки.

Формат команды:

```
part|partition <точка_монтирования> --name=<имя> --device=<устройство> --rule=<правило> [<параметры>]
```

Параметры:

- параметр `<точка_монтирования>` может принимать следующие значения:
  - **/<путь>** - например: /, /usr, /home.
  - **swap** — раздел подкачки. Чтобы автоматически выбрать размер раздела подкачки, добавьте аргумент **--recommended**:

```
swap --recommended
```

Будет выбран подходящий, но не обязательно оптимальный размер.

  - **raid.id** — программный RAID-массив.
  - **pv.id** — раздел LVM.
  - **biosboot** — загрузочный раздел BIOS. На платформах с BIOS, использующих таблицу разделов GPT, необходимо создать загрузочный раздел размером 1 МБ. Именно в этот раздел будет установлен загрузчик. В системах с UEFI этот раздел не требуется. Подробную информацию см. в описании команды bootloader.
  - **efi** — системный раздел EFI. На платформах с UEFI необходимо создать раздел с минимальным размером 50 МБ (рекомендуется 200 МБ). В системах с BIOS этот раздел не требуется. Подробную информацию см. в описании команды `bootloader`.
- **--size=** — минимальный размер раздела в мегабайтах. Введите целое значение без указания единиц, например 500.

ВАЖНО!

Если значение **--size** недостаточно велико, установка будет прекращена.

- **--grow** — увеличить размер раздела до заданной величины или заполнить все свободное место.

Примечание.

Если для раздела подкачки определен параметр **--grow=** без **--maxsize=**, Anaconda ограничит его максимальный размер, руководствуясь следующими правилами: в системах с физической памятью **<2 ГБ** максимальный размер будет равен двойному объему памяти, а в системах с памятью **>2 ГБ** максимальный размер будет равен объему памяти плюс 2 ГБ.

- **--maxsize=** — максимальный размер раздела в мегабайтах. Укажите целое значение без единиц, например 500.
- **--noformat** — использует существующий логический том без форматирования. Используется вместе с **--onpart**.
- **--onpart=** или **--usepart=** — устройство, где будет создан раздел.

```
partition /home --onpart=hda1
```

Эта команда создаст раздел **/home** на **/dev/hda1**.

Пример создания раздела в пределах логического тома:

```
partition pv.1 --onpart=hda2
```

Устройство уже должно существовать.

- **--fsprofile** — определяет профиль для передачи программе создания файловой системы. Профиль содержит набор параметров файловой системы. Этот аргумент требует наличия файла конфигурации. Так, в файловых системах ext2, ext3, ext4 файл расположен в /etc/mke2fs.conf.
- **--fstype=** — тип файловой системы: xfs, ext2, ext3, ext4, swap, vfat, efi, biosboot.
- **--fsoptions=** — строка параметров монтирования файловой системы, заключенная в кавычки. В готовой системе эта строка будет записана в **/etc/fstab**.
- **--label=** — метка раздела.

rootpw

rootpw (обязательный) — позволяет установить пароль **root**.

Формат команды:

```
rootpw [--iscrypted|--plaintext] [--lock] <пароль>
```

Параметры:

- **--iscrypted** — сообщает, что пароль зашифрован. Параметры **--plaintext** и **--iscrypted** являются взаимоисключающими. Зашифровать пароль можно следующим образом:

```
python -c 'import crypt; print(crypt.crypt("my_password", crypt.mksalt(crypt.METHOD_SHA512)))'
```

Эта команда создаст шифр SHA512 с использованием заданной случайной строки.

- **--plaintext** — сообщает, что пароль определен в открытом виде. Параметры **--plaintext** и **--iscrypted** являются взаимоисключающими.
- **--lock** — блокирует учетную запись. Авторизация пользователя root из консоли будет недоступна.

timezone

timezone (обязательный) — устанавливает часовой пояс. Для просмотра полного списка часовых поясов выполните:

```
timedatectl list-timezones
```

Формат команды:

```
timezone <часовой_пояс> [<параметры>]
```

Параметры:

- **--utc** — если задан, подразумевается, что системные часы установлены по Гринвичу.
- **--nontp** — отключает автоматический запуск NTP.
- **--ntpservers** — список NTP-серверов через запятую без пробелов.

user

user (дополнительный) — создание пользователя.

Формат команды:

```
user --name=<пользователь> [<параметры>]
```

Параметры:

- **--username=** — обязательное имя пользователя.
- **--gecos=** — строка параметров GECOS через запятую. Типичные параметры включают полное имя пользователя, номер офиса, и т.п. Подробную информацию можно найти на справочной странице passwd(5).
- **--groups=** — список групп пользователя, разделенных запятой. Список должен содержать существующие группы (см. описание команды **group**).
- **--homedir=** — домашний каталог пользователя. По умолчанию используется /home/пользователь.
- **--lock** — блокирует учетную запись, то есть пользователи не смогут авторизоваться из консоли.
- **--password=** — пароль пользователя. Если не задан, учетная запись будет заблокирована.
- **--shell=** — оболочка пользователя. По умолчанию используются системные настройки.

volgroup

volgroup (дополнительный) — создание группы LVM.

Формат команды:

```
volgroup <имя> <раздел> [<параметры>]
```

Параметры:

- **--noformat** — использует существующую группу томов без форматирования.
- **--useexisting** — использует существующую группу томов и повторно ее форматирует.
- **--pesize=** — размер физических экстентов.
- **--reserved-space**= — размер пространства в мегабайтах, которое должно быть зарезервировано в группе томов. Применимо только к новым группам томов.
- **--reserved-percent=** — процентная доля пространства, зарезервированного в группе томов.

Пример создания раздела, группы логических томов и отдельного тома:

```
part pv.01 --size 10000
volgroup volgrp pv.01
logvol / --vgname=volgrp --size=2000 --name=root
```

xconfig

xconfig (дополнительный) — настраивает X Window System. Если в файле кикстарта есть запись для установки X, но нет команды **xconfig**, настройки X потребуется определить вручную.

Не следует добавлять эту команду в файл кикстарта, если вы не планируете устанавливать X Window System.

Параметры:

- **--defaultdesktop=** — рабочее окружение. Чтобы выбрать графическое окружение, необходимо, чтобы они также присутствовали в секции **%packages**.
- **--startxonboot** — графическая авторизация в установленной системе.

Секция %packages

Команда **%packages** отмечает начало секции устанавливаемых пакетов.

В этой секции можно указать отдельный пакет, группу или целое окружение.

Список групп и окружений можно найти в файле **repodata/*-comps-Everything.<архитектура>.xml** на установочном образе РЕД ОС.

В ***-comps-Everything.<архитектура>.xml** окружения отмечены тегом **<environment>**, а группы — тегом <group>. Каждая запись имеет свой идентификатор, признак отображения для пользователей, название, описание и список пакетов. Пакеты, отмеченные в как обязательные (mandatory), будут всегда устанавливаться при установке группы, пакеты **default** автоматически выбираются при выборе группы, а пакеты **optional** должны быть заданы явно.

Группы и окружения можно выбрать по имени (тег **<name>**) и идентификатору (тег **<id>**).

ВАЖНО!

Если в процессе установки не была установлена X Window System и не включены возможности графической авторизации, то после перезагрузки этап первоначальной настройки будет пропущен, и только пользователь root сможет авторизоваться в системе. Чтобы создать другие учетные записи, то прежде чем приступить к установке других систем, добавьте параметр user в файл кикстарта или авторизуйтесь как root в виртуальной консоли и добавьте пользователей вручную с помощью команды adduser.

Секция **%packages** должна завершаться директивой **%end**.

Выбор окружения

Секция **%packages** может содержать не только пакеты, но и целые окружения.

```
%packages
@^desktop-environment
%end
```

Данный фрагмент установит окружение desktop-environment - рабочая станция с графическим окружением **Mate**. Файл кикстарта должен содержать только одно окружение.

Выбор групп

В каждой строке определяется по одной группе, начиная со знака **@**. Имена групп должны соответствовать записям в файле ***-comps-Everything.<архитектура>.xml**.

```
%packages
@X Window System
@Development Tools
@Smart Card Support
%end
```

Основные группы пакетов будут выбраны по умолчанию, поэтому их не надо указывать в разделе **%packages**.

Выбор отдельных пакетов

Отдельные пакеты вводятся по одному в строке. Допускается использование шаблонов (*), например:

```
%packages
sqlite
curl
```

```
aspell
docbook*
%end
```

В примере запись **docbook*** охватывает пакеты **docbook-dtds**, **docbook-simple**, **docbook-slides** и т.п.

Исключение окружений, групп и пакетов

Добавление дефиса перед именем пакетов и групп исключает их из списка установки:

```
%packages
-@Graphical Internet
-autofs
-ipa*fonts
%end
```

ВАЖНО!

Установка всех доступных пакетов с использованием только символа * в файле кикстарта **не допускается**.

Поведение секции **%packages** можно контролировать с помощью параметров.

Общие параметры выбора пакетов

Ниже перечислены параметры секции **%packages**. Параметры добавляются в конец заголовка секции, например:

```
%packages --multilib --ignoremissing
```

Параметры:

- **--nobase** — не устанавливает группу **@base**. Используется, если целью является создание компактной системы.
- **--ignoremissing** — игнорирует недостающие пакеты вместо того, чтобы приостановить установку и ожидать подтверждения продолжения.
- **--excludedocs** — исключает документацию пакетов. В большинстве случаев это означает исключение файлов из **/usr/share/doc***.
- **--multilib** — разрешает установку 32-битных пакетов в 64-битных системах.

Обычно на платформах AMD64 и Intel 64 по умолчанию устанавливаются пакеты, предназначенные для заданной архитектуры (например, **x86_64**) и стандартные пакеты (**noarch**). Однако данный параметр разрешает установку 32-битных пакетов (**i686**).

Этот подход применим только к пакетам в секции **%packages**. Если же пакет участвует в решении зависимостей, будет установлена только необходимая версия.

Параметры для отдельных групп

Чтобы определить параметры для конкретной группы пакетов, надо добавить их после названия группы.

```
%packages
@Internet Applications --optional
%end
```

Параметры:

- **--nodefaults** — устанавливает только обязательные пакеты, а не стандартный набор.
- **--optional** — установка дополнительных пакетов группы согласно списку в ***-comps-Everything.<архитектура>.xml**.

Секция %pre

В секции **%pre** определяются команды, которые будут выполняться сразу после обработки файла кикстарта, но до начала установки.

Секция должна располагаться ближе к концу файла, начинаться с директивы **%pre** и заканчиваться директивой **%end**. Порядок

секций **%pre** и **%post** не имеет значения.

В секции **%pre** можно обращаться к сети, но так как на данном этапе служба имен еще не настроена, следует использовать IP-адреса.

> **Примечание.**
>
> Сценарий **%pre** не выполняется в окружении **chroot** в отличие от **%post**.

Ниже перечислены параметры **%pre**. Они добавляются в конец заголовка секции:

```
%pre --interpreter=/usr/bin/bash
--- <исполняемый_скрипт> --
%end
```

Параметры:

- **--interpreter=** — язык сценариев, например **/usr/bin/sh**, **/usr/bin/bash** или **/usr/bin/python**.
- **--erroronfail** — при сбое сценария показывает сообщение об ошибке и прерывает установку.
- **--log**= — вывод сообщений сценария в заданный файл:

```
%pre --log=/mnt/sysimage/root/ks-pre.log
```

Секция %post

В секции **%post** определяются команды, которые будут выполняться после установки, но до перезагрузки системы. Эта секция должна располагаться после секции команд ближе к концу файла, начинаться с директивы **%post** и заканчиваться директивой **%end**. Порядок секций **%pre** и **%post** не имеет значения.

В этой секции можно установить дополнительные программы или настроить сервер имен. Сценарий **%post** выполняется в окружении **chroot**, поэтому некоторые задачи (такие как копирование сценариев и пакетов с установочных носителей) выполнить не удастся. Это поведение можно изменить с помощью **--nochroot**.

> **ВАЖНО!**
>
> Если вы используете статическую настройку IP, в секции **%post** можно обращаться к сети с разрешением IP-адресов. Если используется DHCP, файл **/etc/resolv.conf** еще не будет сформирован к моменту обработки **%post**, поэтому при обращении к сети необходимо использовать IP-адреса.

Ниже перечислены параметры **%post**. Параметры добавляются в конец заголовка секции:

```
%post --interpreter=/usr/bin/bash
--- <исполняемый_скрипт> ---
%end
```

Параметры:

- **--interpreter=** — определяет язык сценариев, например **bash**.

```
%post --interpreter=/usr/bin/python
```

Здесь можно указать любой установленный язык, например **/usr/bin/sh**, **/usr/bin/bash** или **/usr/bin/python**.

- **--nochroot** - позволяет определить команды для выполнения вне окружения **chroot**.

В следующем примере файл **/etc/resolv.conf** будет скопирован в созданную файловую систему.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
%end
```

- **--erroronfail** — при сбое сценария показывает сообщение об ошибке и прерывает установку.
- **--log=** — сохраняет протокол выполнения сценария в файл. Путь должен учитывать наличие **--nochroot**. Пример без **--nochroot**:

```
%post --log=/root/ks-post.log
```

Пример с **--nochroot**:

```
%post --nochroot --log=/mnt/sysimage/root/ks-post.log
```

Пример файла конфигурации

Стандартный файл кикстарта (шаблон) имеет следующее содержимое:

```
# Generated by Anaconda 33.25.4
# Generated by pykickstart v3.30
# Use graphical install
graphical


%packages --multilib
@^desktop-environment

%end

# Keyboard layouts
keyboard --xlayouts='us','ru' --switch='grp:alt_shift_toggle'
# System language
lang ru_RU.UTF-8

# Network information
network  --bootproto=dhcp --device=ens18 --ipv6=auto --activate
network  --hostname=localhost.localdomain

# Use CDROM installation media
cdrom

# Run the Setup Agent on first boot
firstboot --enable

# Generated using Blivet version 3.3.0
ignoredisk --only-use=sda
autopart
# Partition clearing information
clearpart --none --initlabel

# System timezone
timezone Europe/Moscow --utc

# Root password
rootpw --iscrypted
$6$3zZ3MWYmRB5UU2Nb$f7ZKDB1tQJ/9Q4VRoRVvFfqK8DBjO8.HO9AZ8nTOvhPeJ3JNBKBJ7lO.UFqH4fWykCE.Emiie1JHCvIq1Nhgu1
user --groups=wheel --name=user --
password=$6$AywHyJ1Jw8ffZbCs$642L93KbjyltoS79aJs1Vng8IjMs.UlBcnzoC0TaBxMs4/ULbYOTRLejpPXDiW20/c5xIs7JwYwIi.ep2P7Yi/ --
iscrypted --gecos="user"
```

Подготовка PXE-сервера для развертывания РЕД ОС с загрузкой в UEFI или Legacy в РЕД ОС 7.3

Для успешной загрузки среды установки РЕД ОС **PXE-клиент** должен располагать как **минимум 3 ГБ** оперативной памяти.

Вы можете подробнее ознакомиться с информацией по установке и настройке PXE-сервера, просмотрев наши обучающие видео:

- на **RuTube** — Настройка PXE с аутентификацией и KICKSTART;
- в **Яндекс.Дзен** — Настройка PXE с аутентификацией и KICKSTART;
- в **VK Видео** — Настройка PXE с аутентификацией и KICKSTART.

На наших каналах вы также сможете найти много другой полезной информации.

1. Сначала установите необходимые пакеты на сервер. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install dhcp tftp-server syslinux httpd dnf-plugins-core
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

2. Создайте следующие каталоги:

```
mkdir /var/lib/tftpboot/pxelinux.cfg
mkdir /var/lib/tftpboot/uefi
mkdir -p /var/lib/tftpboot/images/REDOS
```

3. Следующей командой скопируйте файлы для запуска установки РЕД ОС в режиме **legacy** через **PXE**:

```
cp /usr/share/syslinux/{chain.c32,mboot.c32,memdisk,menu.c32,pxelinux.0,ldlinux.c32,libutil.c32} /var/lib/tftpboot/
chmod 777 /var/lib/tftpboot/pxelinux.0
```

4. Скопируйте файлы для **UEFI** режима установки РЕД ОС в каталог **/var/lib/tftpboot/uefi**.

Для этого выполните последовательность команд:

```
dnf download shim-x64 grub2-efi-x64 --downloaddir=/root/
cd /root/
rpm2cpio shim-x64-*.rpm | cpio -dimv
rpm2cpio grub2-efi-x64-*.rpm | cpio -dimv
cp ./boot/efi/EFI/BOOT/BOOTX64.EFI /var/lib/tftpboot/uefi
cp ./boot/efi/EFI/redos/grubx64.efi /var/lib/tftpboot/uefi

chmod 777 /var/lib/tftpboot/uefi/*.*
```

5. Подключите загрузочный USB-носитель с РЕД ОС 7.3 и скопируйте его содержимое в каталог **/var/lib/tftpboot/images/REDOS**:

```
cp -vR "/run/media/user/redos-MUROM-7.3.4 x86_64/." /var/lib/tftpboot/images/REDOS
```

Также возможен вариант копирования из iso-образа.

Смонтируйте образ:

```
mount -t iso9660 -o loop redos-MUROM-7.3.4-20231220.0-Everything-x86_64-DVD1.iso /mnt/
```

Скопируйте все содержимое в каталог **/var/lib/tftpboot/images/REDOS/**:

```
cp -vR /mnt/* /var/lib/tftpboot/images/REDOS/
```

Размонтируйте образ:

```
umount /mnt/
```

6. Конфигурирование DHCP-сервера.

В файле **/etc/dhcp/dhcpd.conf** укажите свои значение для вашей подсети, а именно шлюз и выдаваемый диапазон IP-адресов. Параметру next-server назначается IP-адрес DHCP-сервера.

Зеленым цветом выделены сетевые параметры для изменения под вашу конфигурацию сети.

```
nano /etc/dhcp/dhcpd.conf
```

```
non-authoritative;
 allow bootp;
 option space pxelinux;
 option pxelinux.magic code 208 = string;
 option pxelinux.configfile code 209 = text;
 option pxelinux.pathprefix code 210 = text;
 option pxelinux.reboottime code 211 = unsigned integer 32;
 option architecture-type code 93 = unsigned integer 16;
 subnet 192.168.2.0 netmask 255.255.255.0 {
 option routers 192.168.2.1;
 range 192.168.2.70 192.168.2.80;
 class "pxeclients" {
 match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
 next-server 192.168.2.10;
 if option architecture-type = 00:07 {
 filename "uefi/grubx64.efi";
 }
 else {
 filename "pxelinux.0";
 }
 }
 }
```

Запустите службу **dhcpd**:

```
systemctl enable dhcpd --now
```

7.1 Создайте загрузочное меню для установки в режиме **legacy** с использованием **PXE**:

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
default menu.c32
 PROMPT 0
 TIMEOUT 150
 MENU TITLE PXE Menu
 LABEL REDOS 7.3
 MENU LABEL REDOS 7.3
 KERNEL images/REDOS/images/pxeboot/vmlinuz
 APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp inst.repo=http://192.168.2.10/images/REDOS/
```

7.2 Создайте загрузочное меню для установки в режиме **UEFI** с использованием **PXE**:

```
nano /var/lib/tftpboot/uefi/grub.cfg
```

```
function load_video {
 insmod efi_gop
 insmod efi_uga
 insmod video_bochs
 insmod video_cirrus
 insmod all_video
```

```
}
load_video
set gfxpayload=keep
insmod gzio
menuentry 'REDOS 7.3' {
linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp inst.repo=http://192.168.2.10/images/REDOS/
initrd images/REDOS/images/pxeboot/initrd.img
}
```

8. Конфигурирование web-сервера **httpd**.

WEB-сервер используется для публикации файлов дистрибутива РЕД ОС в локальной сети.

Создайте файл:

```
nano /etc/httpd/conf.d/pxeboot.conf
```

```
Alias /images /var/lib/tftpboot/images
 <Directory /var/lib/tftpboot/images>
 Options Indexes FollowSymLinks
 Require ip 127.0.0.1 192.168.2.0/24
 </Directory>
```

Настройте SELinux:

```
chcon -R -t httpd_sys_content_t /var/lib/tftpboot/images
```

Запустите службу **httpd**:

```
systemctl enable httpd --now
```

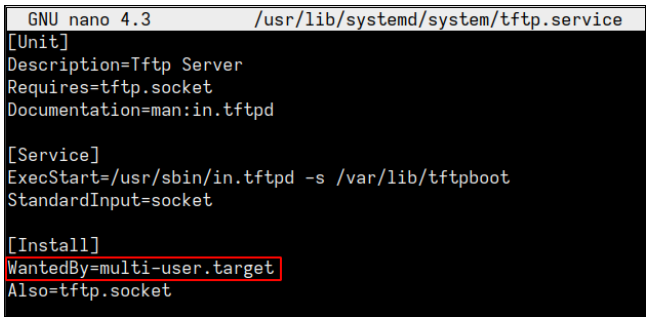
9. Настройка и запуск службы **tftp**.

Откройте файл:

```
nano /usr/lib/systemd/system/tftp.service
```

и добавьте строку в секцию [**Install**]:

```
WantedBy=multi-user.target
```



Откройте файл:

```
nano /usr/lib/systemd/system/tftp.socket
```

измените строку `ListenDatagram=69` на `ListenDatagram=0.0.0.0:69`, чтобы запустить **tftp** на **69** порту по IPv4-протоколу. По умолчанию порт публикуется на IPv6.

```
[Unit]
 Description=Tftp Server Activation Socket

 [Socket]
 ListenDatagram=0.0.0.0:69
```

```
[Install]
WantedBy=sockets.target
```

После изменения модулей **systemd** их нужно инициализировать:

```
systemctl daemon-reload
```

Добавьте службу **tftp** в автозапуск:

```
systemctl enable tftp --now
```

Настройка установки РЕД ОС по PXE через VNC в РЕД ОС 7.3

Подготовка рабочей станции

Для установки ОС на рабочей станции выбираем загрузку по сети: «**Network Boot Agent**» или «**PXE boot**».

ВАЖНО!

Необходимо, чтобы загрузка по PXE была активирована в **BIOS**. Настройка может называться по-разному, в зависимости от версии BIOS и производителя материнской платы. Необходимо ознакомиться со спецификацией на конкретную материнскую плату.

Настройка установки РЕД ОС по PXE через VNC

Создайте файл меню с содержимым:

- для систем, использующих **BIOS**:

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
default menu.c32
 PROMPT 0
 TIMEOUT 150
 MENU TITLE PXE Menu
 LABEL REDOS 7.3
 MENU LABEL REDOS 7.3
 MENU PASSWD $1$15opgKTx$dP/IaLNiCbfECiC2KPkDC0
 KERNEL images/REDOS/images/pxeboot/vmlinuz
 APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp method=http://192.168.1.38/images/REDOS/
devfs=nomount inst.vnc inst.vncpassword=password
```

- для систем, использующих **UEFI**:

```
nano /var/lib/tftpboot/uefi/grub.cfg
```

```
function load_video {
 insmod efi_gop
 insmod efi_uga
 insmod video_bochs
 insmod video_cirrus
 insmod all_video
 }
 load_video
 set gfxpayload=keep
 insmod gzio
 menuentry 'REDOS 7.3' {
 linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp inst.repo=http://192.168.2.10/images/REDOS/ inst.vnc inst.vncpassword=password
 initrd images/REDOS/images/pxeboot/initrd.img
 }
```

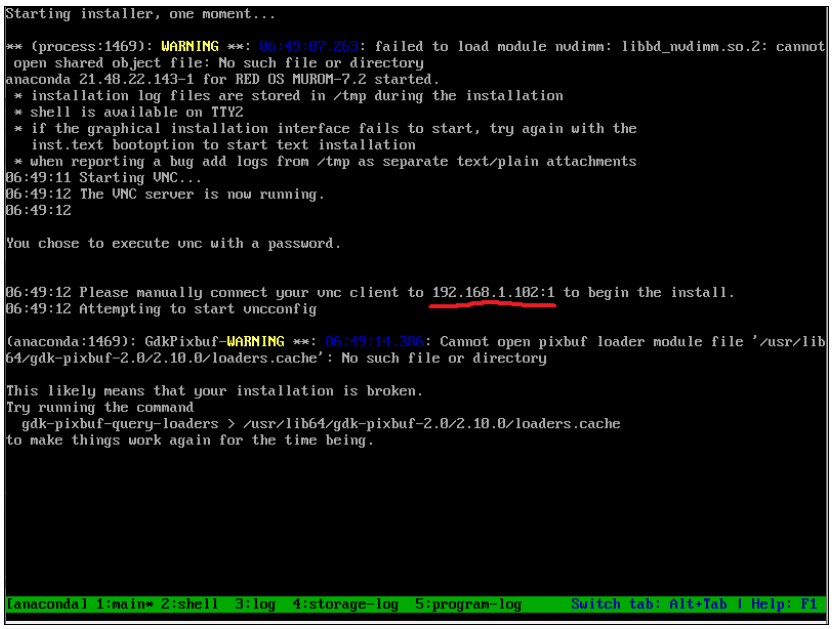
В данном файле конфигурации параметр **TIMEOUT 150** - счётчик времени, после которого будет запущена установка автоматически.

Параметры в конце строки **APPEND**:

```
inst.vnc inst.vncpassword=password
```

дают возможность подключиться по протоколу **VNC**, для удалённой настройки установки РЕД ОС, зная IP-адрес машины, порт и заданный пароль.

IP-адрес можно увидеть после того, как произойдёт первичная загрузка сервисов после меню:

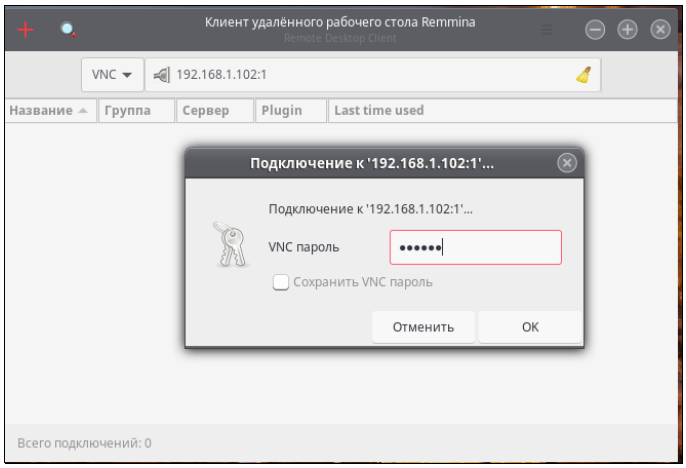


Вместо этих параметров можно указать:

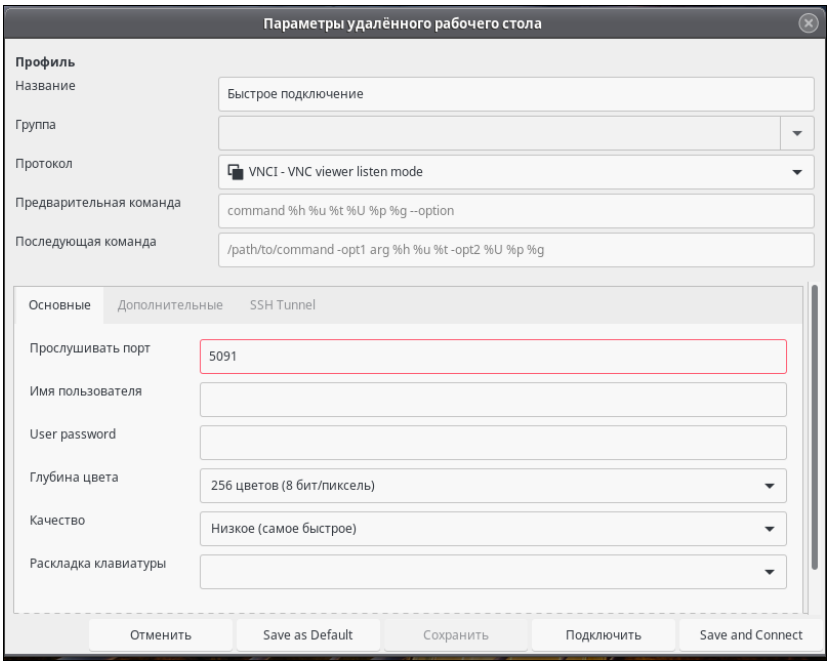
```
inst.vnc inst.vncconnect=<узел>:<порт>
```

Где **<узел>**:**<порт>** - это заранее известные ip-адрес и порт машины, с которой будет производиться настройка установки.

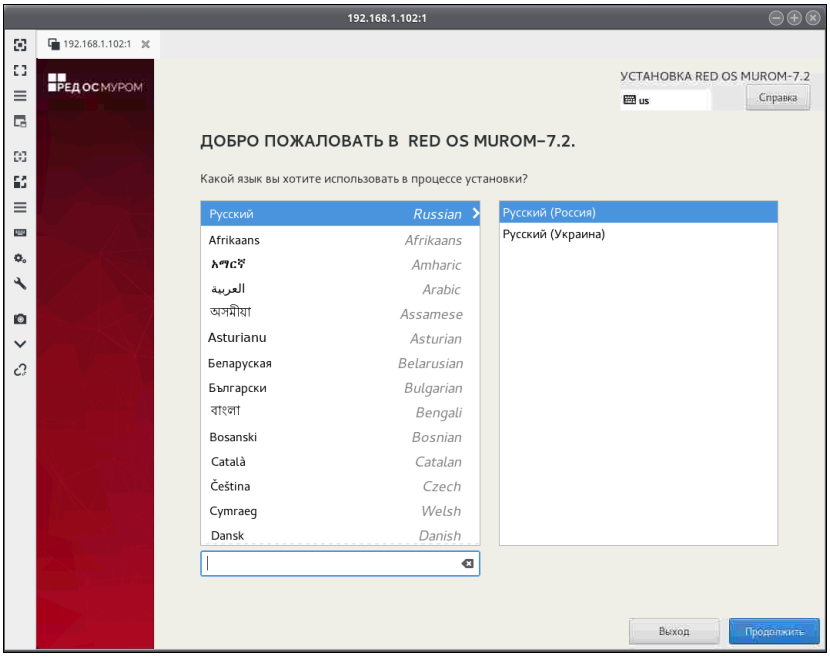
После того, как эти параметры заданы, на удалённой машине нужно запустить VNC-клиент «**Меню» - «Интернет» - «Remmina**», выбрать тип подключения **VNC** и ввести **<IP-адрес>**:**<порт>**. После этого придёт запрос пароля:



В случае, когда был настроен конкретный удалённый компьютер для контроля установки, в *Remmina* нажмите на кнопку «**Плюс**» слева вверху и введите настройки порта, на котором он будет ждать запрос:



Если всё настроено верно, то в итоге мы получим возможность удалённой настройки подключившись по **vnc**:



ВАЖНО!

РЕД ОС, установленная через VNC, по умолчанию запускается в текстовом режиме. Для включения графического режима воспользуйтесь нашей инструкцией «Установка графической оболочки в РЕД ОС 7.3 ».

Установка РЕД ОС на один диск с ОС Windows (dual-boot)

Выделение дискового пространства
Настройка BIOS

Примечание.

Данная инструкция носит исключительно рекомендательный характер. Данная инструкция описывает общую процедуру установки РЕД ОС 7.3 рядом с ОС Windows 10, без учёта различий возможных конфигураций аппаратного и программного обеспечения ПК, а также вносимых ими изменений, способных повлиять на работоспособность систем.

ВАЖНО!

В некоторых случаях для установки и работы РЕД ОС необходимо обновление **BIOS/UEFI** компьютера.

Вы можете подробнее ознакомиться с возможностью установки РЕД ОС на один диск с ОС Windows, просмотрев наши обучающие видео:

- на **RuTube** — Запись iso-образа РЕД ОС и установка рядом с Windows;
- в **Яндекс.Дзен** — Запись iso-образа РЕД ОС и установка рядом с Windows;
- в **VK Видео** — Запись iso-образа РЕД ОС и установка рядом с Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Выделение дискового пространства

ВАЖНО!

Перед началом работы с разделами жёстких дисков создайте резервную копию важных данных. При работе с несистемным разделом, например, D, E, F и т. д., достаточно просто скопировать файлы оттуда.

При необходимости наличия двух операционных систем (Windows и Linux) на компьютере пользователя, необходимо выделить отдельный раздел на жёстком диске для установки РЕД ОС.

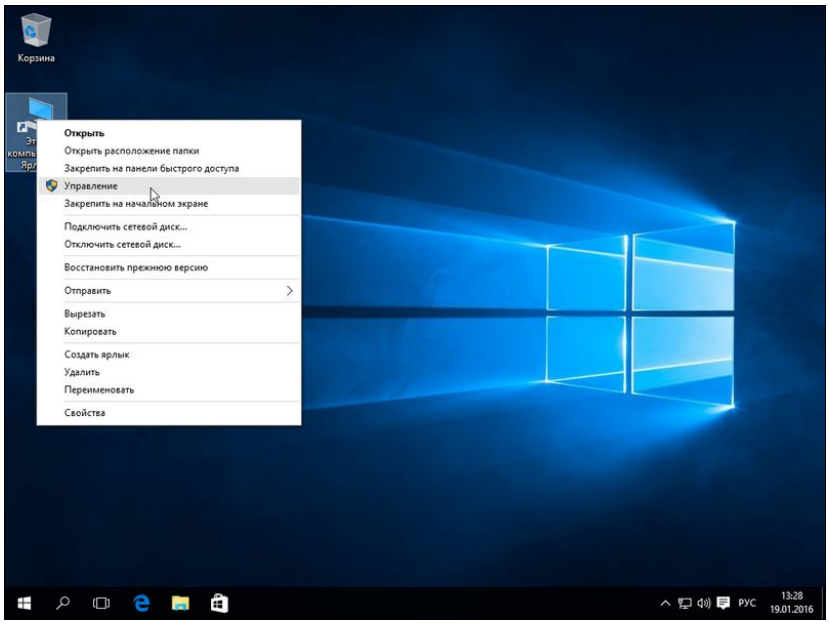
ВАЖНО!

Более корректным вариантом для организации **dual-boot** является использование отдельного жёсткого диска для установки РЕД ОС.

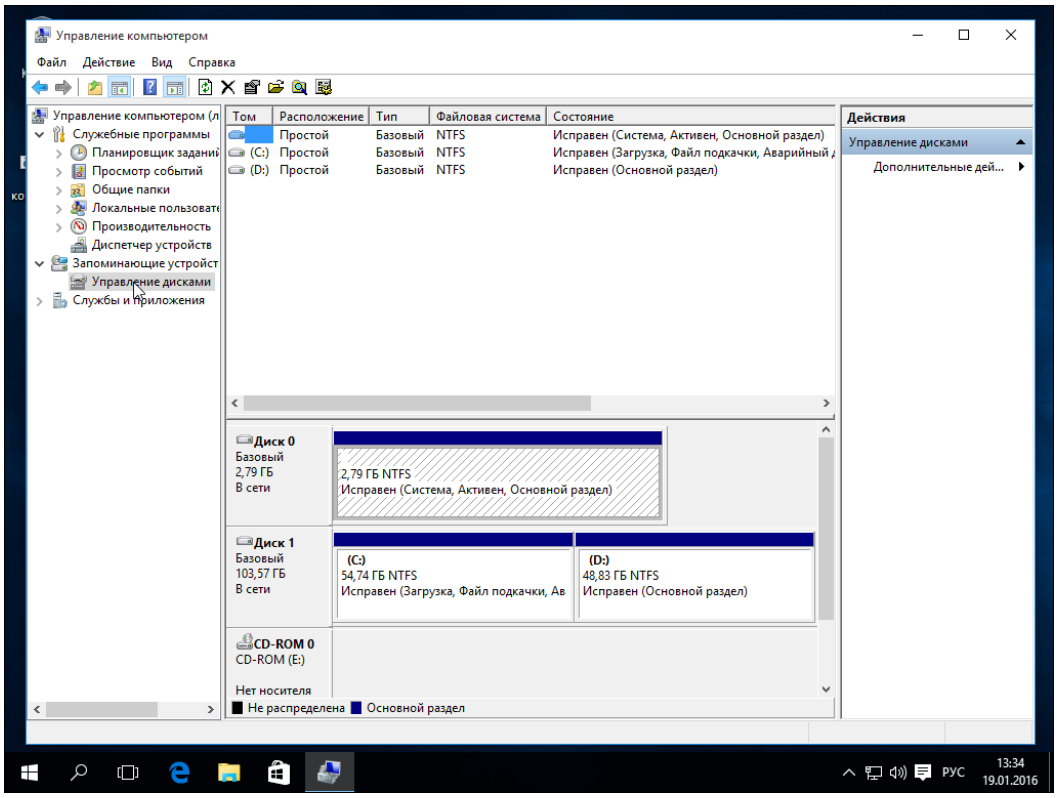
Имеется много вариантов для работы с разделами жёстких дисков (создание, удаление, форматирование). Это можно реализовать, как средствами специализированного ПО, так и средствами утилиты «**Управление дисками**» в составе операционной системы Windows.

В данной инструкции будет рассмотрен метод создания отдельного раздела на жёстком диске средствами утилиты «**Управление дисками**».

Кликните правой кнопкой мыши по значку «**Этот компьютер**» на рабочем столе и откройте пункт меню « **Управление**».

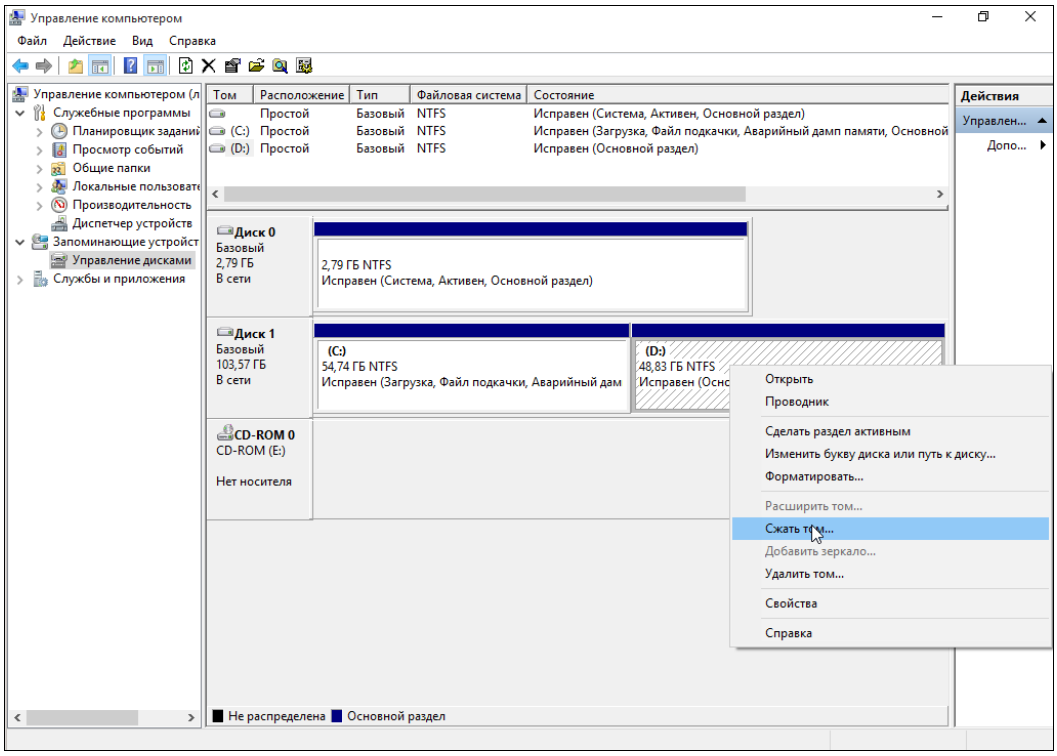


Далее работа производится в утилите «**Управление дисками**».

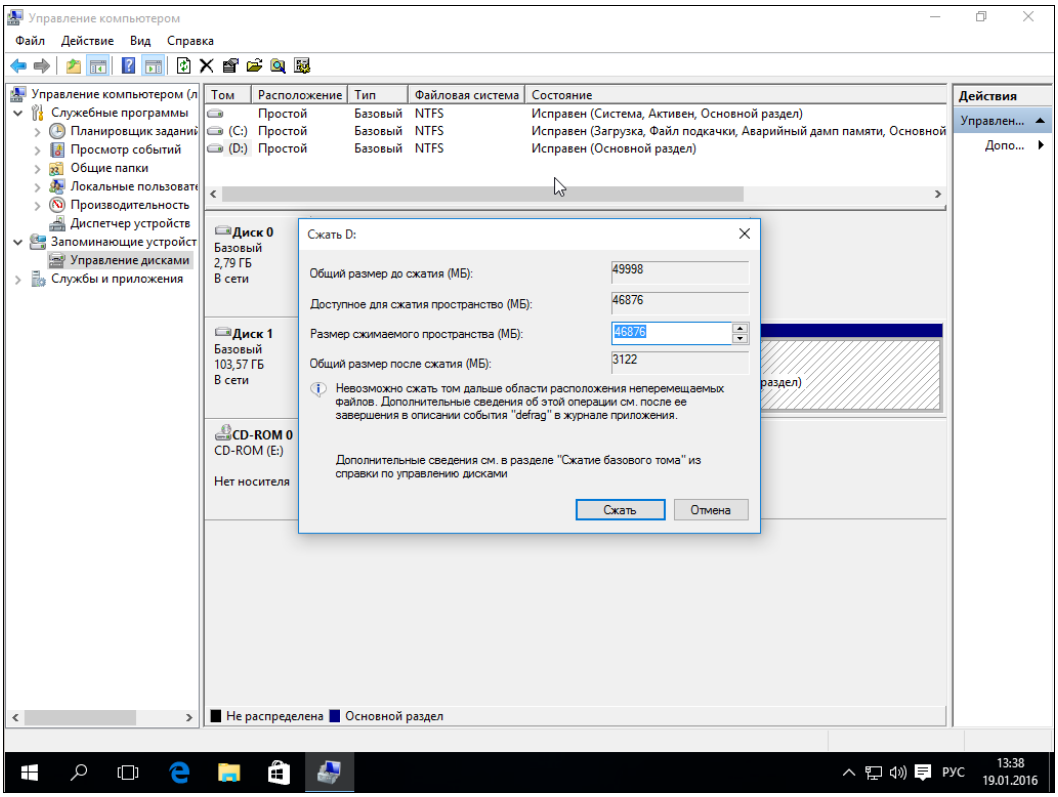


Внизу окна есть два диска: **C** (системный) и **D**. Рассмотрим пример изменения размера диска **D**.

Кликните по нужному диску правой кнопкой мыши и выберите опцию «**Сжать том**».

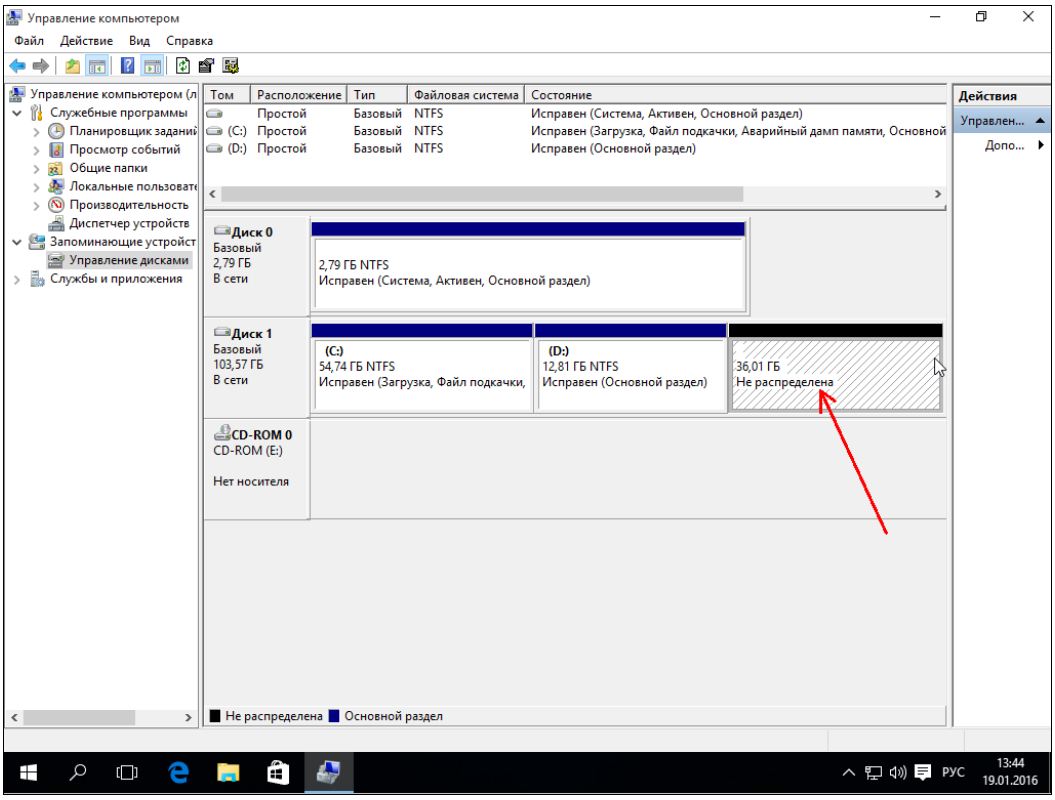


Откроется окно, в котором необходимо ввести размер создаваемого тома в поле «**Размер сжимаемого пространства**».



Обратите внимание, что вы не можете указать размер нового раздела больше, чем количество свободного места на диске.

Нажмите на кнопку «**Сжать**». После этого появится неразмеченное пространство, которое можно будет использовать для установки РЕД ОС.



Настройка BIOS

Перед установкой РЕД ОС необходимо настроить **BIOS** рабочей станции, на которую производится установка ОС, на загрузку с подготовленного флеш-накопителя. Для этого необходимо включить в **BIOS** рабочей станции опцию загрузки с CD/DVD-привода. Способ входа в меню **BIOS** и расположение конкретных настроек может отличаться, в зависимости от используемой материнской платы. Чаще всего для входа в **BIOS** необходимо нажать функциональную клавишу **Delete** на стационарных рабочих станциях или функциональную клавишу **F1** (**F9**) на мобильных рабочих станциях (ноутбуках) в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.

Также предварительно отключите в **BIOS** параметр **Secure Boot**, т. к. он может помешать нормальной установке и загрузке РЕД ОС.

Установка системы производится в штатном режиме согласно «Обзор установки».

Обратите внимание, что в меню выбора расположения установки РЕД ОС необходимо выбрать выделенный раздел диска или дополнительно выделенный диск.

При выборе разметки диска «**По-своему**», раздел с установленной ОС Windows будет отображаться как «**Неизвестный**» раздел. Не рекомендуется производить над данным разделом какие-либо действия посредством установщика РЕД ОС, т. к. это может привести к проблемам загрузки или полной неработоспособности установленной ОС Windows.

После завершения установки выберите в настройках **BIOS** основным загрузочным устройством жёсткий диск вашего ПК и загрузите его.

Иногда (в зависимости от производителя ПК и используемом в нём **BIOS/UEFI**) возникает необходимость в самостоятельном указании в **BIOS/UEFI** компьютера загрузчика РЕД ОС в качестве загрузчика по умолчанию, т. к. **Windows Boot Manager**, оставшись загрузчиком по умолчанию, автоматически запустит ОС Windows, не предоставив возможности выбора загрузки необходимой ОС.

На этом установка и настройка РЕД ОС завершена, и система полностью готова к использованию.

ВАЖНО!

Если вы планируете установку ОС Windows **после** установки РЕД ОС, учтите, что перезапись загрузчика **Windows Boot Manager** приведёт к нарушению корректной работы загрузчика **GRUB** и невозможности загрузки РЕД ОС.

Для решения данной проблемы необходимо восстановить **GRUB**. Подробную информацию о восстановлении загрузчика **GRUB** см. в нашей статье «**Восстановление загрузчика GRUB2**».

Загрузка РЕД ОС в SecureBoot-режиме

Для запуска РЕД ОС в **SecureBoot**-режиме необходимо произвести импорт сертификата в **BIOS**.

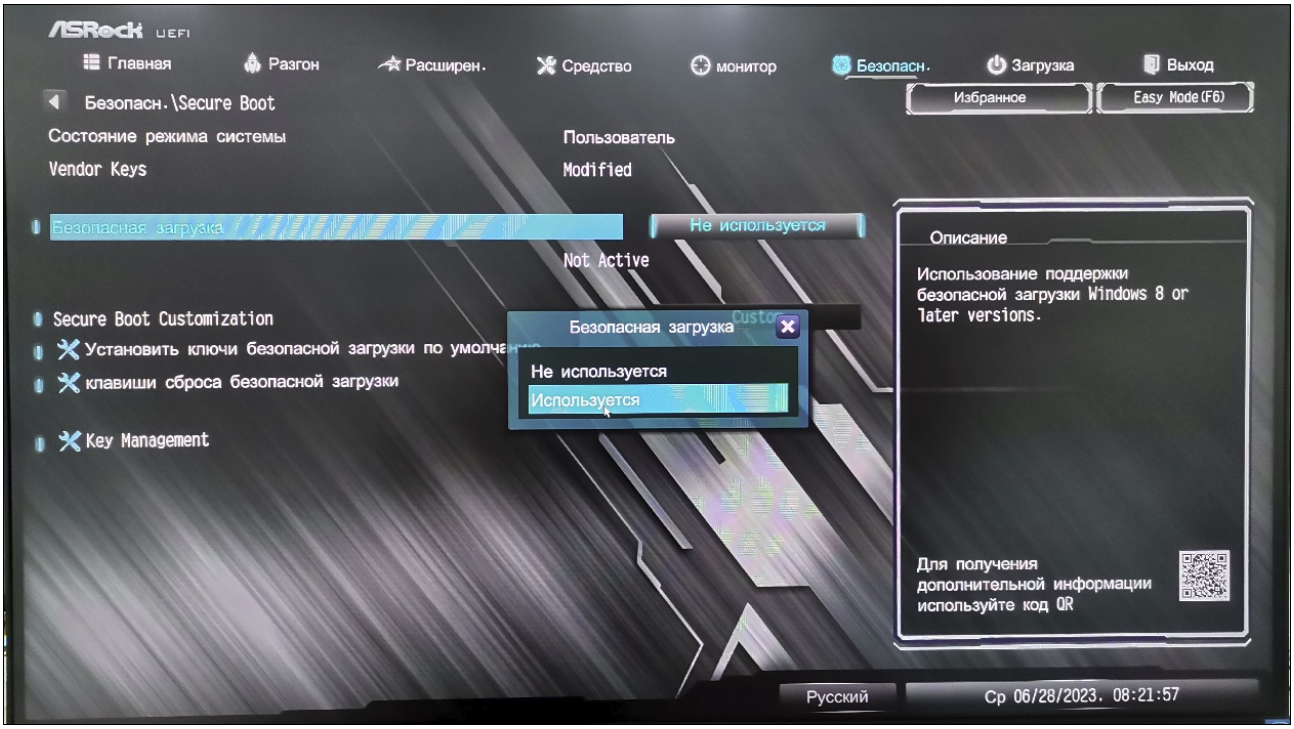
В данной статье рассмотрен общий случай настройки **BIOS**, т.к. настройка **BIOS** для разных производителей материнских плат может отличаться.

Запустите **BIOS**. Чаще всего для входа в **BIOS** необходимо нажать функциональную клавишу **Delete** на стационарных рабочих станциях или функциональную клавишу **F1** (**F9**) на мобильных рабочих станциях (ноутбуках) в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.

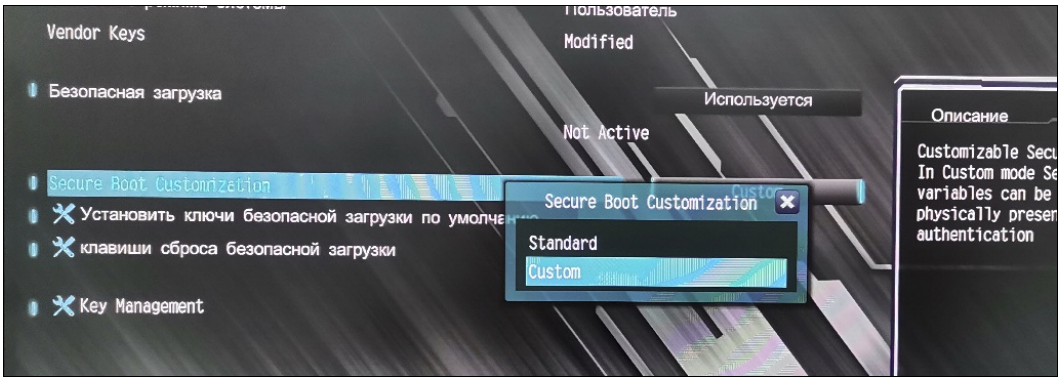
Перейдите в **Расширенный режим BIOS** (**Advanced Mode**).



В секции **Безопасность** необходимо активировать **SecureBoot**, если он выключен.



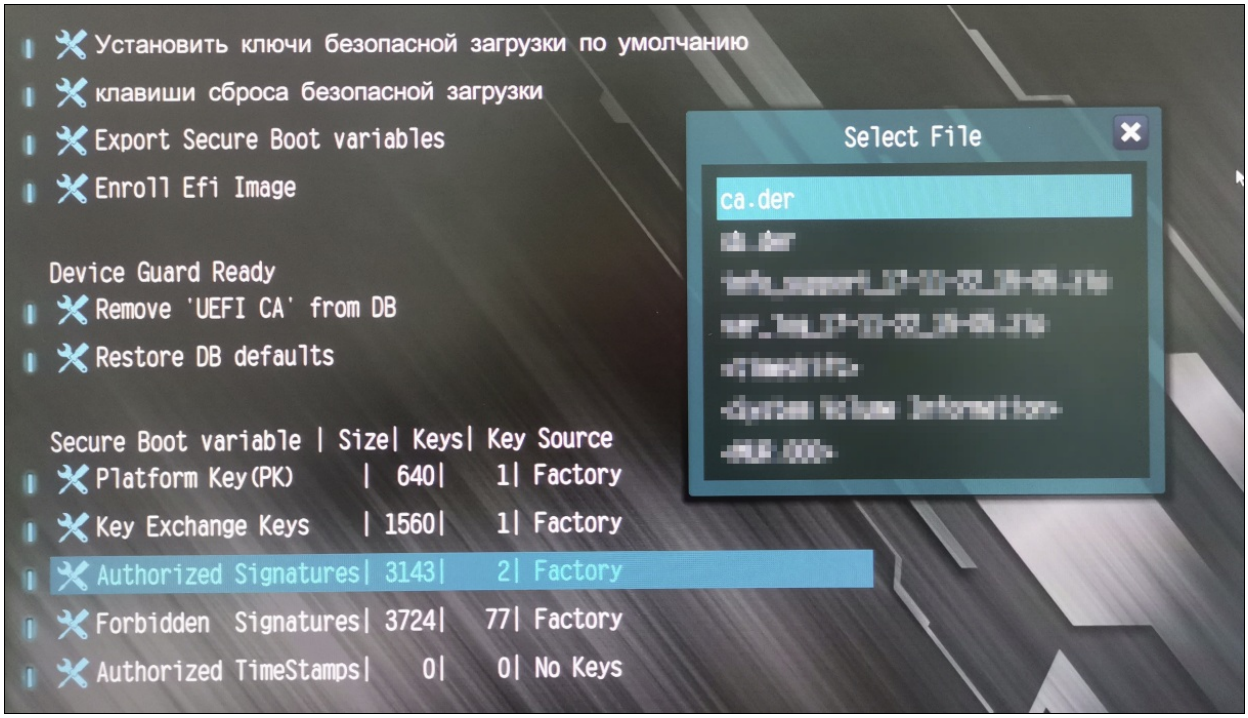
Далее необходимо переключить значение параметра **Secure Boot Customization** в **custom**, для того чтобы **BIOS** при загрузке считывал не только стандартные сертификаты.



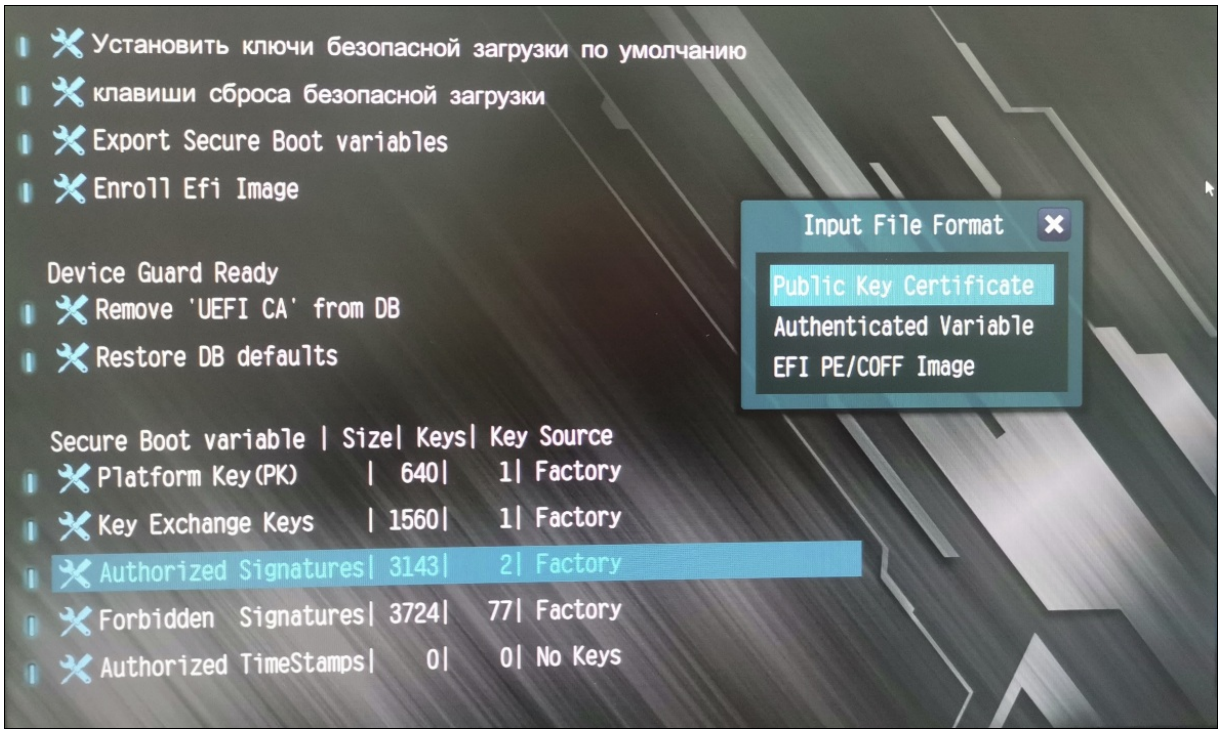
Затем необходимо установить сертификат. Для этого потребуется usb-flash накопитель с файловой системой **FAT32**, на который должен быть скопирован сертификат **ca.der**.

Выберите пункт **Authorized Signatures** – **Append**, чтобы добавить к уже существующим сертификатам новый.

После определения вашего устройства необходимо выбрать сам сертификат.



Тип необходимо указать **Public Key Certificate**.



На данном этапе настройка **BIOS** завершена – примените изменения и перезагрузите ПК.

В РЕД ОС проверить, активирован ли **SecureBoot**, можно командой:

```
mokutil --sb-state

SecureBoot enabled
```

Работа с РЕД ОС в сессии LiveUSB

Загрузочный экран LiveUSB
Графические программы LiveUSB
Консольные программы LiveUSB
Дополнительная информация

ISO-образ LiveUSB — представляет собой образ операционной системы, который можно записать на съёмный носитель (USB flash-накопитель) и ознакомиться с её функциональными возможностями без установки на жесткий диск ПК.

На текущий момент в РЕД ОС существует **ISO-образ LiveUSB**, который доступен к загрузке по ссылке.

Наименование **ISO-образа LiveUSB** производится в следующем формате:

```
redos—MUROM—<версия_ОС>—<архитектура>—LIVE.iso
```

Примечание.

Обратите внимание, что это именно **ознакомительный формат** ОС. Все изменения, которые производятся при работе с данным ISO-образом, **будут сброшены** после перезагрузки, за исключением изменений, которые производились на других носителях (не на том носителе, куда записан ISO-образ).

ISO-образ LiveUSB записывается на носитель идентично обычному образу.

Вы можете подробнее ознакомиться с работой системы РЕД ОС в сессии LiveUSB, просмотрев наши обучающие видео:

- на **RuTube** — Работа с РЕД ОС в сессии LiveUSB;
- в **Яндекс.Дзен** — Работа с РЕД ОС в сессии LiveUSB;
- в **VK Видео** — Работа с РЕД ОС в сессии LiveUSB.

На наших каналах вы также сможете найти много другой полезной информации.

Загрузочный экран LiveUSB

Загрузочный экран **LiveUSB** выглядит следующим образом:



Он предоставляет 2 варианта для выбора:

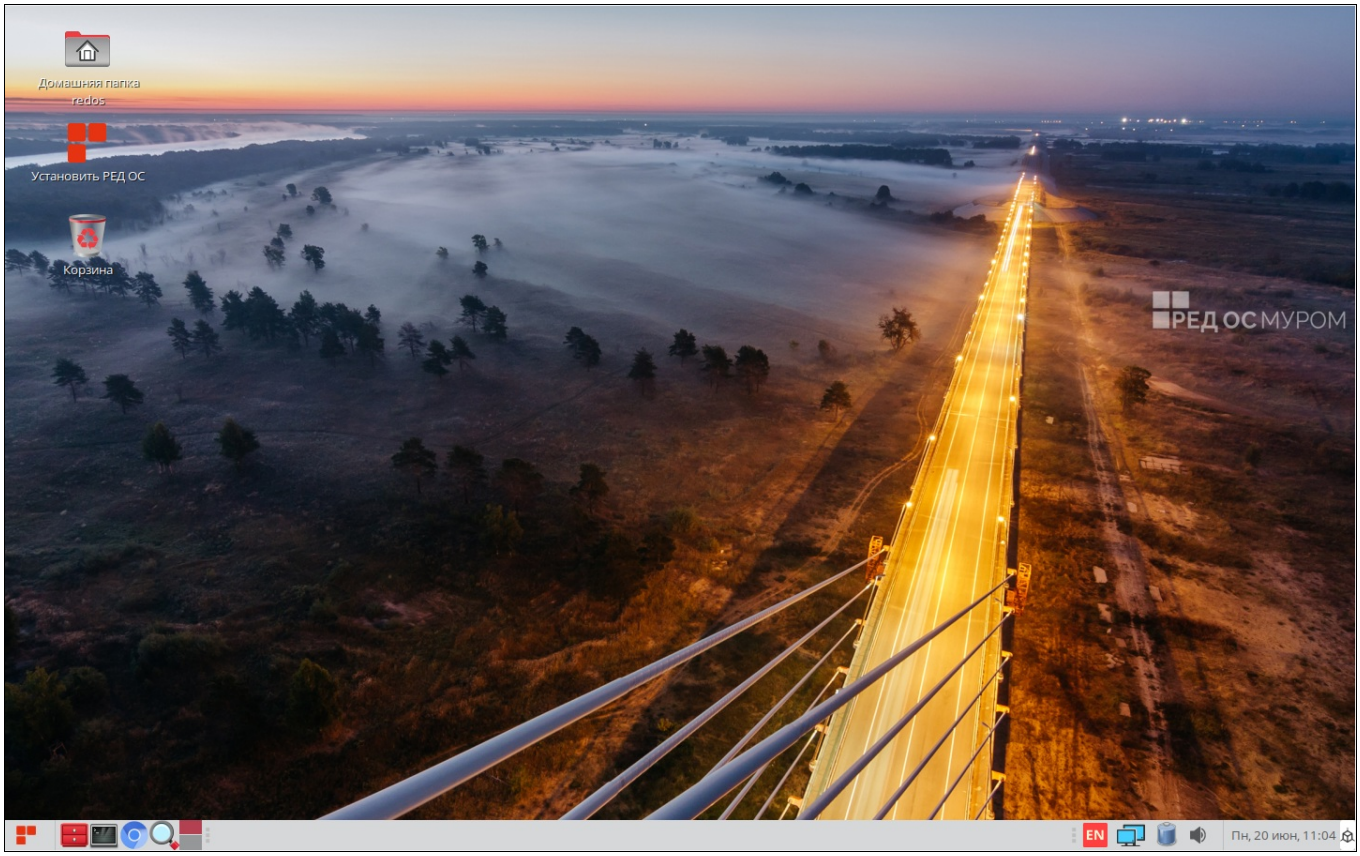
- произвести непосредственное ознакомление с ОС;
- прервать загрузку и запустить ОС, которая уже установлена на жестком диске.

Также вы можете изменить параметры загрузки ОС, если нажмете **TAB**.



Благодаря **ISO-образу LiveUSB** можно проводить тест на совместимость ваших комплектующих ПК с драйверами РЕД ОС. К примеру, в случае успешной работы драйвера и вашей видеокарты, вы увидите рабочий стол и сможете проверить через `inxi -G`, что ваша видеокарта нашла нужный ей видеодрайвер.

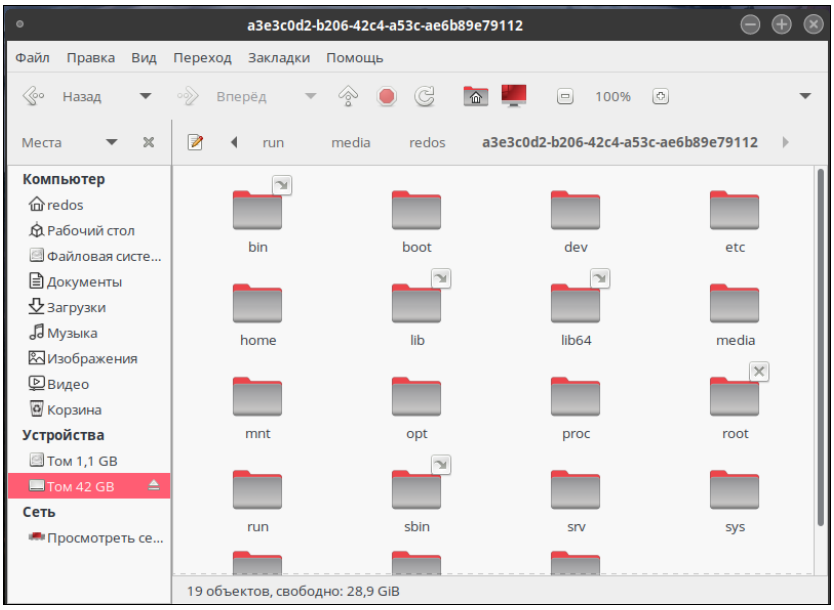
Рабочий стол **LiveUSB** выглядит так:



С него вы можете осуществить непосредственно установку ОС, нажав на ярлык «**Установить РЕД ОС**».

Если на ПК уже есть другая ОС, вы можете примонтировать ее «**Домашнюю папку**» для чтения/записи.

Если выбрать определенный диск из доступных, то он также будет примонтирован. Его содержимое можно будет скопировать или изменить.



Графические программы LiveUSB

Основной список доступных графических программ доступен в «**Главном меню**».

Список утилит, которые могут позволить восстановить работоспособность ОС, помочь записать диск или изменить разделы:

- Утилита **записи ISO-образов на USB-накопитель** - **MultiWriter** - подробная информация по ссылке;
- Утилита для работы **с дисковыми разделами** - **Gparted** - подробная информация по ссылке;
- Утилиты для **резервного копирования и восстановления данных** - подробная информация по ссылке;
- Утилита **сбора информации о системе** - **loginfo** - подробная информация по ссылке.

Консольные программы LiveUSB

Список основных доступных консольных команд:

- Утилита для отображения информации о системе и об аппаратной части ПК - **inxi** - подробная информация по ссылке;
- Утилита для проверки файловой системы и исправления ошибок - **fsck** - подробная информация по ссылке;
- Утилита для проверки контрольных сумм файлов - **md5sum** - подробная информация по ссылке;
- Утилита для отображения информации о модуле - **modinfo** - подробная информация по ссылке;
- Восстановление загрузчика **grub2** - подробная информация о командах по ссылке;
- И многие другие полезные программы как для анализа работы ОС, так и для различных других задач.

Дополнительная информация

Вы также можете просмотреть содержимое репозиториев РЕД ОС и проверить работу того или иного выбранного вами пакета. Главное - не забывать о том, что все внесенные вами изменения **будут сброшены** после перезагрузки ОС.

Ознакомиться с содержимым репозиториев вы можете как консольно, так и графически, через утилиты:

- Система управления пакетами - **dnf** - подробная информация по ссылке;
- Менеджер пакетов - **dnfdragora**.

Для восстановления работоспособности ОС, которая установлена на основном ПК, можно воспользоваться следующей информацией.

Проблемы с монтированием домашнего каталога /home

Суть данной проблемы заключается в том, что система вместо получения авторизации переходит в **emergency mode**, графический менеджер GDM не запускается.

```
Warning: dev/mapper/ro-root does not exist
Warning: dev/ro/root does not exist
Warning: dev/ro/swap does not exist

Generating “/run/initramfs/rdsosreport.txt“


Entering emergency mode. Exit the shell to continue.
Type “journalctl“ to view system logs.
You might want to save “/run/initramfs/rdsosreport.txt“ to a USB stick or /boot after mounting then and attach it to a bug report.
```

Проверим вывод команды `dmesg`. В выводе должны присутствовать ошибки вида «`/dev/sda3, run e2fsck manually`», где **/dev/sda3** - home-раздел. Для того чтобы узнать, за каким разделом закреплен **home**, необходимо проверить файл **/etc/fstab**. Проверка файловой системы осуществляется через утилиту **fsck**.

Запуск автоматической проверки `fsck -a /dev/sda3`, где ключ **-a** отвечает за автоматическую коррекцию ошибок файловой системы.

После успешной проверки необходимо перезагрузить компьютер. После этого графический менеджер GDM должен запуститься, и пользователь должен увидеть окно авторизации.

Пользователь забыл свой пароль и пароль root

Решением данной проблемы является сброс пароля **root**, согласно инструкции. Инструкцию предоставляет техническая поддержка, обратиться за инструкцией вы можете по ссылке.

Система не монтирует корневой раздел

Решение проблемы. Загрузка из более старого ядра
Неверное имя корневого раздела GRUB

Проблема монтирования корневого раздела выглядит следующим образом:

```
[ 1.719701] Hardware name: ECS IC780M-A2/IC780M-A2, BIOS 080015 11/03/2010
[ 1.719749] 0000000000000000 ffff88022c0b7df0 ffffffff8176cf38 ffffffff81a65048
[ 1.719951 0000000000008001 ffff88022c0b7e68 ffffffff81765306 ffffffff00000010
[ 1.720152] ffff88022c0b7e78 ffff88022c0b7e18 ffffffff81765e74 ffff88022c0b7e88
[ 1.720353] Call Trace:
[ 1.720402] [] dump_stack+0x64/0x82
[ 1.720449] [] panic+0xc8/0x206
[ 1.720494] [] ? printk+0x67/0x69
[ 1.720541] [] mount_block_root+0x225/0x2b0
[ 1.720587] [] mount_root+0x53/0x56
[ 1.720633] [] prepare_namespace+0x16c/0x1a4
[ 1.720679] [] kernel_init_freeable+0x1e1/0x1ee
[ 1.720725] [] ? initcall_blacklist+0xba/0xba
[ 1.720771] [] ? rest_init+0x80/0x80
[ 1.720817] [] kernel_init+0xe/0xf0
[ 1.720862] [] rest_from_fork+058/0x90
[ 1.720908] [] ? rest_init+0x80/0x80
[ 1.720974] Kernel Offset: 0x0 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 1.721043] ---[ end Kernel panic — not syncing: VFS: Unable to mount root fs on unknown-block (0,0)
_
```

Сообщение об ошибке «vfs unable to mount root fs on unknown block» может встречается во время загрузки Linux. Оно означает, что ядро не может примонтировать корневую файловую систему, и, следовательно, дальнейшая загрузка невозможна. Ошибка довольно серьёзная и, не исправив её, вы не сможете полноценно работать в своей операционной системе.

Все ситуации, в которых может появиться сообщение «error: vfs unable to mount root fs» можно разделить на два вида:

- Загрузка с жёсткого диска — вы загружаете свою основную операционную систему после внесения изменений в таблицу разделов, обновления или других действий, которые могли задеть диски;
- Вы загружаете LiveCD-систему с оптического диска или флешки.

Второй вариант сразу же отбросим. Здесь исправлять нечего. Ошибка означает, что либо образ был битый, либо он был неверно записан на диск. А вот первый случай интереснее, рассмотрим основные причины, которые могут его вызывать:

- Корневой раздел был переименован и теперь называется по-другому;
- Повреждена **initramfs**;
- Ядро не поддерживает файловую систему корневого раздела;
- Ошибка в конфигурации загрузчика, например, из-за недостаточного количества свободного места в папке **/boot**;
- Файловая система корневого раздела повреждена.

Рассмотрим возможные пути решения проблемы.

Решение проблемы. Загрузка из более старого ядра

После того, как система выдаст эту ошибку, случится **Kernel Panic** и компьютер перезагрузится. Вы снова окажетесь в меню загрузчика **GRUB**. Сначала следует попытаться загрузиться с помощью более старого ядра. Для этого выберите пункт «**Дополнительные параметры**» и выберите одно из более старых ядер.

Если система в этом случае загрузится, то можно сделать вывод, что не работает только новое ядро. Если вы собирали его сами, то, возможно, вы не включили в него все необходимые для работы файловые системы. Если это ядро из репозиториев, и система загрузилась с более старым ядром, то можно предположить, что у вас повреждена **initramfs** для нового ядра. Это тоже могло произойти из-за недостатка памяти при обновлении системы. Чтобы всё исправить, вам достаточно освободить место в каталоге **/boot/** и создать новую **initramfs**. Проверьте и освободите место в папке **/boot**, если его там мало:

```
df -h | grep boot
```

```
[root@localhost ~]# df -h | grep boot
/dev/sda2                974M          56M  851M            7% /boot
/dev/sda1                599M         6,4M  593M            2% /boot/efi
[root@localhost ~]#
```

На данном скриншоте занято только 7%, если будет 100% — надо освобождать. Для создания **initramfs** необходимо выполнить следующие действия:

```
cp -p /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak
dracut -f -v --regenerate-all
ls /boot
```

```
[root@localhost ~]# ls /boot
config-5.15.10-1.el7.x86_64
config-5.15.72-1.el7.3.x86_64
efi
grub
grub2
initramfs-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86.img
initramfs-5.10.29-3.el7.x86_64.img
initramfs-5.15.10-1.el7.x86_64.img
initramfs-5.15.72-1.el7.3.x86_64.img.bak
loader
lost+found
symvers-5.15.10-1.el7.x86_64.gz
symvers-5.15.72-1.el7.3.x86_64.gz
System.map-5.15.10-1.el7.x86_64
System.map-5.15.72-1.el7.3.x86_64
vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
vmlinuz-5.15.10-1.el7.x86_64
vmlinuz-5.15.72-1.el7.3.x86_64
```

Обновите конфигурацию загрузчика **grub**:

- если используется **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- если используется **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

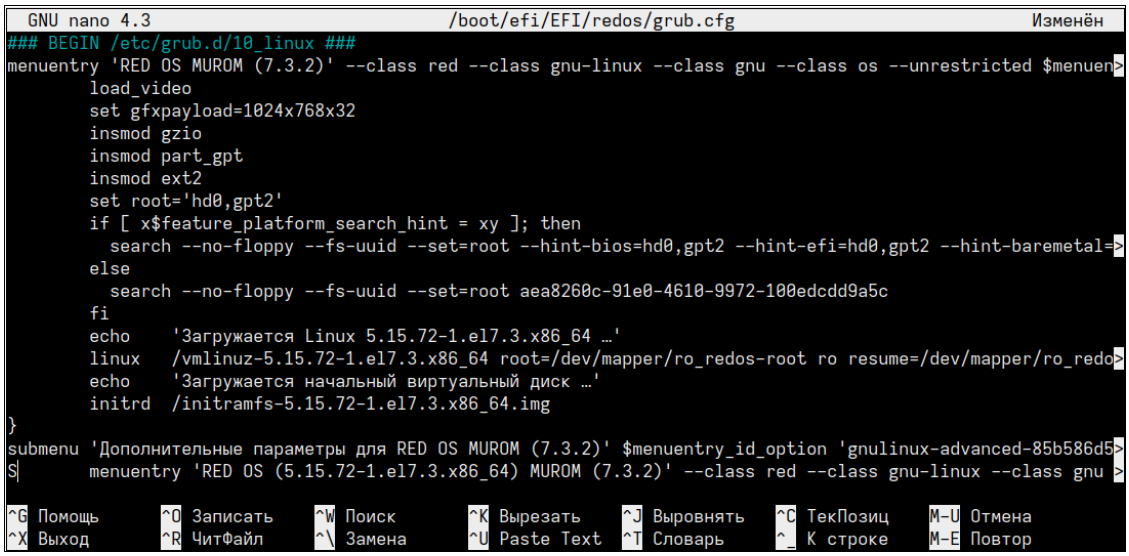
Если вы думаете, что проблема именно в свободном пространстве и **initramfs**, но загрузиться с помощью более старого ядра не можете, то попробуйте другой **LiveCD**-дистрибутив и попытайтесь всё исправить в *chroot*-окружении.

Неверное имя корневого раздела GRUB

Сейчас, в большинстве дистрибутивов, в конфигурационном файле **GRUB** имя корневого раздела передается ядру в формате **UUID**. И с этим обстоятельством есть одна проблема. Если вы каким-либо образом измените корневой раздел, например, измените его размер, то **UUID** изменится. И если вы выполните перезагрузку, не обновив конфигурацию **GRUB**, то система больше не загрузится, потому что ядро попросту не сможет найти нужного раздела.

Но попытаться решить проблему можно. Если вы точно знаете, на каком разделе у вас находится корень, то можно непосредственно в меню **GRUB** исправить конфигурацию. Для этого в меню выберете стрелками вверх и вниз нужный пункт, а затем нажмите кнопку **E**. Откроется редактор конфигурации. Вам нужно найти строчку, похожую на следующую:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro quiet splash
```



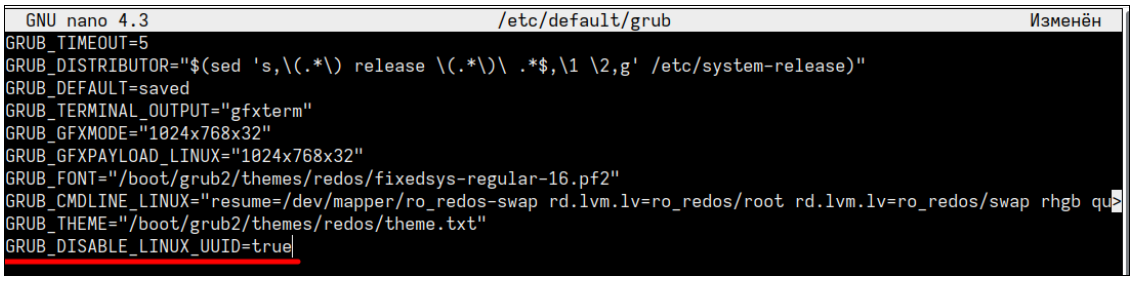
В ней надо заменить UUID=9d8d92de-74a6-4e64-8281-b8548c690e0c на обычное имя вашего корневого раздела, например, **/dev/sda2**. Для начала загрузки нажмите **F10**. Если система загрузится, значит проблема была именно в этом. В дальнейшем, можно просто обновить конфигурацию **GRUB**:

```
grub2-mkconfig
```

Или даже попросить **GRUB** больше не использовать **UUID** для обозначения корневого раздела:

```
nano /etc/default/grub
```

```
GRUB_DISABLE_LINUX_UUID=true
```



Далее необходимо снова обновить конфигурацию **GRUB**, используя команду **grub2-mkconfig**.

Если ошибка исчезла, но система всё ещё не загружается, обратите внимание, что **systemd** всё ещё использует файл **/etc/fstab** для монтирования файловых систем. И если корневая файловая система (и не корневая тоже) там указана неверно, система не загрузится. Для исправления этой проблемы можно использовать режим восстановления. Здесь тоже надо заменить **UUID** на обычную запись или же на правильный **UUID**. Такая проблема очень часто становится причиной медленной загрузки Linux.

В этом же режиме можно проверить корневой раздел на ошибки, но для проверки диска лучше использовать **LiveCD**.

Если файловая система корневого раздела повреждена, её необходимо проверить, исправить согласно инструкции «Проверка файловой системы на наличие ошибок».

ОС запускается, но зависает на экране загрузки

Скорее всего данное поведение может быть связано с некорректным поведением X-сервера и графических драйверов. Для диагностики ситуации и сбора информации с ПК вы можете запустить ПК в консольном режиме. Для этого вам потребуется перезагрузить ПК и на этапе выбора ядра для загрузки нажать «**e**».

Далее необходимо найти примерно такую строку (см. скриншот) и добавить в конец «**3**».



После этого для продолжения загрузки необходимо нажать сочетание клавиш «**Ctrl+X**», ОС будет запущена в текстовом режиме.

Следующим этапом потребуется собрать отладочную информацию через утилиту loginfo для дальнейшего изучения проблемы.

Не загружается РЕД ОС из-за неправильного UUID раздела SWAP

Диагностика проблемы
Устранение проблемы

Проблема характеризуется тем, что во время загрузки операционной системы РЕД ОС на экране появляется ошибка вида:

```
A start job is running for /dev/disk/by-uuid/03a83c83-3827-4fa3-8352-bdfb4d99a15b (10min 6s / no limit)
```

Загрузить операционную систему в безопасном режиме также не удается.

Диагностика проблемы

Ошибка «A start job is running for /dev/disk/by-uuid/...» связанна с разделом диска, который используется в системе. Операционная система не может подключить раздел, который имеет номер **UUID**, указанный в ошибке.

Для того чтобы узнать, с каким именно разделом имеются проблемы при загрузке, требуется проверить параметры загрузчика системы **grub**.

Чтобы увидеть параметры загрузки grub, нужно на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> quiet splash
```

В строке видно, что в параметре resume=UUID= записан тот номер **UUID**, из-за которого возникает проблема с запуском системы.



Параметр resume отвечает за указание файла подкачки (раздел **SWAP**) для возобновления работы системы после перехода в спящий режим. Из этого можно сделать вывод, что проблема связана с разделом **SWAP**.

Необходимо узнать, совпадает ли номер **UUID** раздела **SWAP**, который указан в параметрах grub, с его актуальным на данный момент **UUID**-номером.

Номер **UUID** всех разделов диска можно узнать с помощью команды:

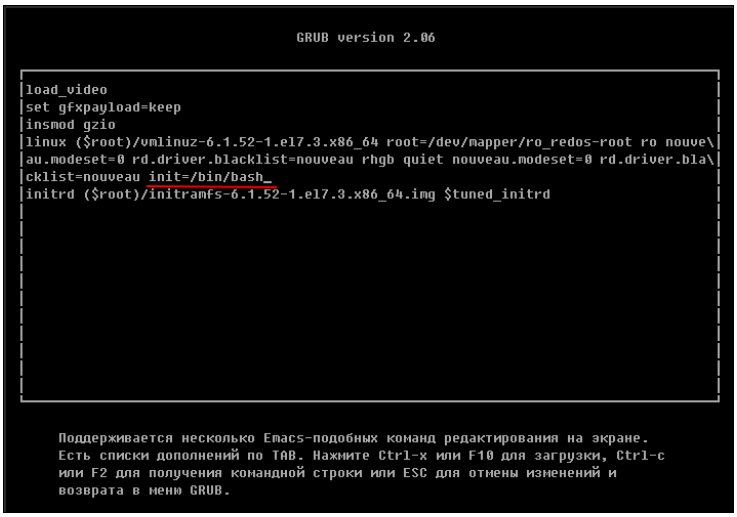
```
lsblk -o +uuid,name
```

Но т. к. операционная система РЕД ОС не может быть загружена ни в обычном, ни в безопасном режиме, то нужно выполнить загрузку системы сразу в командный интерпретатор **/bin/bash**.

Для этого необходимо открыть параметры загрузки **grub** — на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=номер_uuid ro resume=UUID=<номер_uuid> quiet splash
```

В строке необходимо удалить полностью параметр resume=UUID=<номер_uuid> и добавить параметр init=/bin/bash:



Для продолжения загрузки с введенными параметрами необходимо нажать сочетание клавиш **Ctrl+x** или **F10**.

Система сразу загрузится в командную оболочку **bash**.

Авторизуйтесь с правами пользователя **root** командой:

```
su root
```

Далее выполните монтирование корневого раздела командой:

```
mount -o remount,rw /
```

Нужно узнать **UUID**-номер, который имеет раздел **SWAP** в данный момент. Для этого необходимо выполнить команду:

```
lsblk -o +uuid,name
```

Вывод команды должен быть примерно следующим:

```
nvme0n1
│   259:0    0 476,9G  0 disk                                  nvme0n1
├─nvme0n1p1
│   259:1    0   600M  0 part /boot/efi   050C-89A6                    nvme0n1p1
├─nvme0n1p2
│   259:2    0     1G  0 part /boot      bef54c6a-a584-4147-9178-4218be5daedc   nvme0n1p2
└─nvme0n1p3
   259:3    0 475,4G  0 part          lA0CXd-ZuHw-7mqu-uhkH-igMU-c7wt-QBESxa nvme0n1p3
  ├─ro_redos-root
  │ 253:0    0    70G  0 lvm  /        832a877b-0293-4eec-a5f0-6a8d080aac03   ro_redos-srv-root
  ├─ro_redos-swap
  │ 253:1    0   7,5G  0 lvm  [SWAP]     fc46bf73-2759-4d70-a2d3-ab1f664ebf12   ro_redos-srv-swap
  └─ro_redos-home
    253:2    0 397,8G  0 lvm  /home      e5411e74-97de-4b84-aecd-e7f86e16ad5e   ro_redos-home
```

В данном примере раздел **SWAP** имеет **UUID - fc46bf73-2759-4d70-a2d3-ab1f664ebf12**.

Таким образом, можно сделать вывод, что номер **UUID** раздела **SWAP**, который записан в параметрах загрузки grub, и его актуальный **UUID** номер отличаются.

Устранение проблемы

Для устранения проблемы необходимо заменить неактуальный **UUID**-номер в параметрах загрузки **grub** на его актуальный номер, который был получен в результате диагностики.

Изменение параметра resume загрузчика GRUB

1. На этапе выбора ядра нажмите клавишу «**e**». Будут открыты параметры загрузки **grub**.

2. Замените старый номер **UUID**, прописанный в параметре `resume=UUID=`, на актуальный, который был получен в результате

диагностики командой `lsblk -o +uuid,name`.

В строке:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> quiet splash
```

3. Для продолжения загрузки с введенными параметрами нажмите сочетание клавиш **Ctrl+x** или **F10**.

Система должна загрузиться без ошибок.

Сохранение конфигурации загрузчика GRUB

При таком способе редактирования параметров загрузки **grub** введенные параметры не будут сохранены при следующей загрузке. Для сохранения внесенных изменений на постоянной основе измените параметр `resume=UUID=` в файле **/etc/default/grub**.

Для запуска терминала необходимо использовать сочетание клавиш **Ctrl+Alt+T** или запустить утилиту из **Главного меню** – **Системные** – **Терминал**.

Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

Откройте файл **/etc/default/gru**b с помощью текстового редактора командой:

```
nano /etc/default/grub
```

Найдите строку следующего вида:

```
GRUB_CMDLINE_LINUX="resume=UUID=..."
```

Номер **UUID** параметра `resume=UUID=` должен быть заменен на актуальный, с помощью которого удалось запустить систему.

Далее обновите файл загрузчика **grub** командой:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

После выполнения этих действий параметры загрузи **grub** будут сохранены для постоянного использования.

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

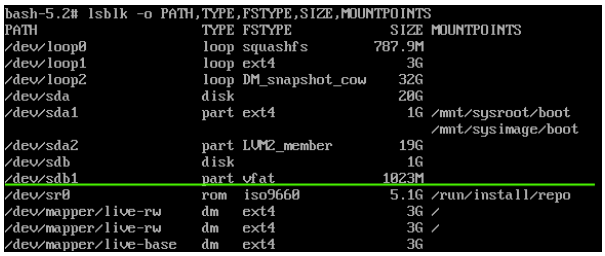
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

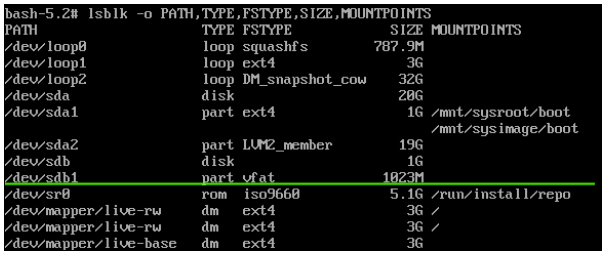
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

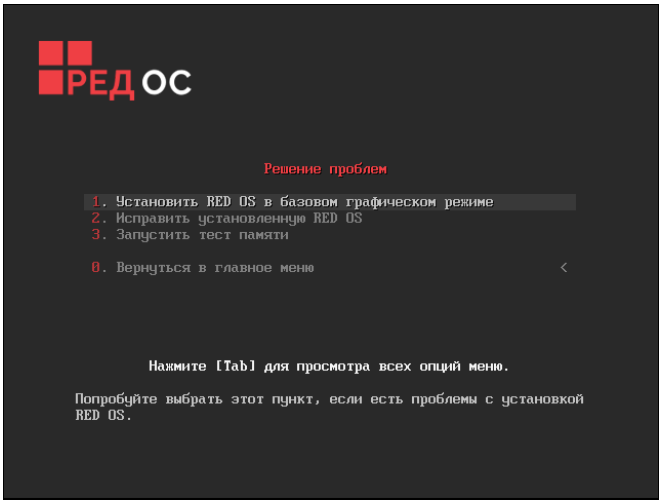
Проблемы при установке ОС

Установка ОС зависает на начальном этапе
ОС не запускается после установки с LiveUSB

Установка ОС зависает на начальном этапе

Бывают случаи, когда установка ОС зависает на этапе первичной загрузки до запуска окна *Anaconda*. В таких случаях рекомендуется произвести установку ОС в **базовом графическом режиме**, который также называется **nomodeset**.

Для загрузки ОС в режиме **nomodeset**, использующих **BIOS**, выберите пункт «**Решение проблем**» – «**Установить RED OS в базовом графическом режиме**».



Для загрузки ОС в режиме **nomodeset**, использующих **UEFI**, выберите пункт «**Troubleshooting**» – «**Install RED OS Murom-7.3.4 in basic graphics mode**».



ОС не запускается после установки с LiveUSB

Иногда бывают случаи, что после установки ОС с *LiveUSB* не происходит загрузка установленной ОС. Для таких случаев необходимо загрузиться обратно в Live-сессию и скопировать файл **initramfs** с установочного носителя на диск с ОС. Для этого выполните следующий алгоритм действий:

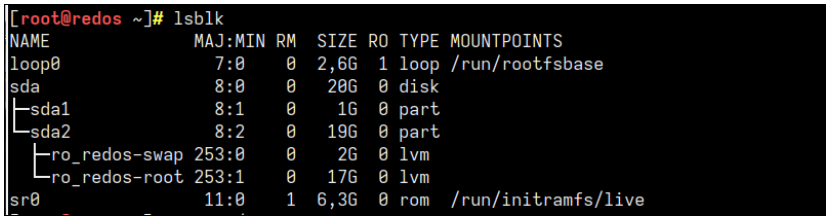
1. Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

2. Проверьте названия разделов установленной ОС командой:

```
lsblk
```

В ответе команды будут указаны разделы ОС и загрузчика, в данном случае — **/dev/ro_redos/root** и **/dev/sda1**.



3. Примонтируйте разделы установленной ОС следующими командами:

```
mkdir /OS
mount /dev/ro_redos/root /OS
mount /dev/sda1 /OS/boot
cp /run/initramfs/live/images/pxeboot/initrd.img /OS/boot/initramfs-5.15.72-1.el7.3.x86_64.img
```

4. Назначьте необходимые права:

```
chmod 600 /OS/boot/initramfs-5.15.72-1.el7.3.x86_64.img
chown root. /OS/boot/initramfs-5.15.72-1.el7.3.x86_64.img
```

5. Отмонтируйте разделы установленной ОС:

```
umount /OS/boot
umount /OS
```

6. Перезагрузите ПК в установленную ОС:

```
reboot
```

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

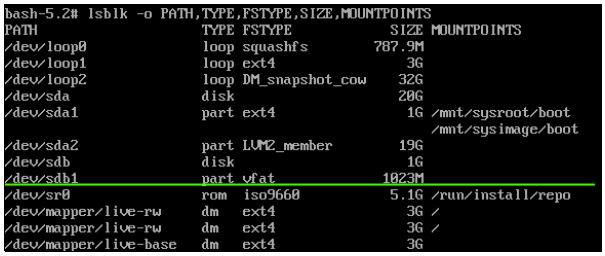
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

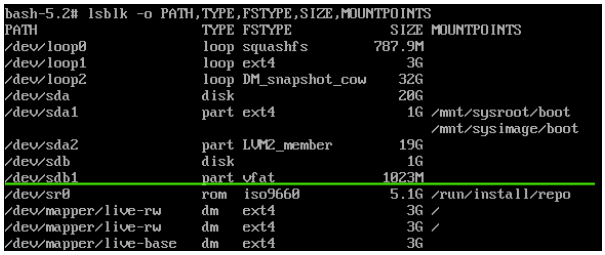
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

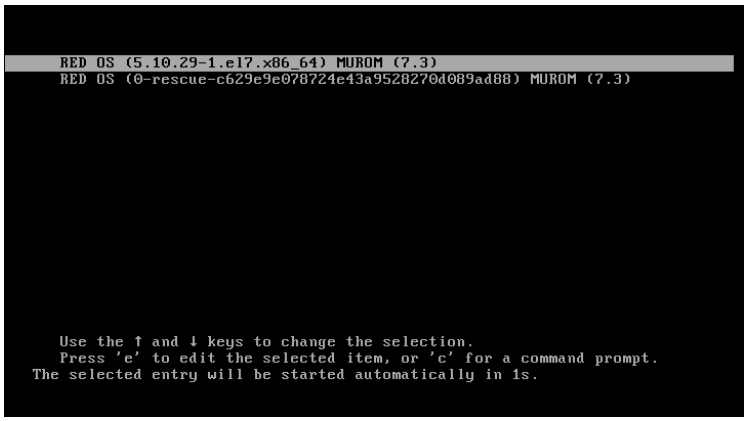
Общие положения

Перед началом работы с РЕД ОС пользователю необходимо изучить руководство администратора и руководство пользователя, поставляемые с техническими средствами ПК в составе оборудования рабочего места пользователя. Также пользователь должен пройти инструктаж по технике безопасности при работе с электроприборами и ПК.

Для начала работы в РЕД ОС пользователю необходимо убедиться в работоспособности ПК своего рабочего места. После проверки и подготовки рабочего места пользователь для начала работы с РЕД ОС должен произвести включение оборудования ПК рабочего места.

Базовая система ввода/вывода (BIOS) персонального компьютера пользователя должна быть настроена на автоматическую загрузку операционной системы с локального накопителя жестких дисков.

После включения питания ПК и выполнения загрузки BIOS производится запуск РЕД ОС. При запуске РЕД ОС в течение заданного интервала времени предоставляет пользователю возможность выбора варианта загрузки ОС, с которым будет произведена загрузка и работа РЕД ОС.



По умолчанию предлагаются 2 варианта загрузки: обычная загрузка в штатном режиме и загрузка ОС в режиме восстановления с минимальным числом настроек для возможности восстановления системы после сбоя.

Если в течение заданного интервала времени пользователь не выбрал вариант загрузки клавишами «вверх/вниз», то операционная система производит автоматическую загрузку варианта заданного по умолчанию.

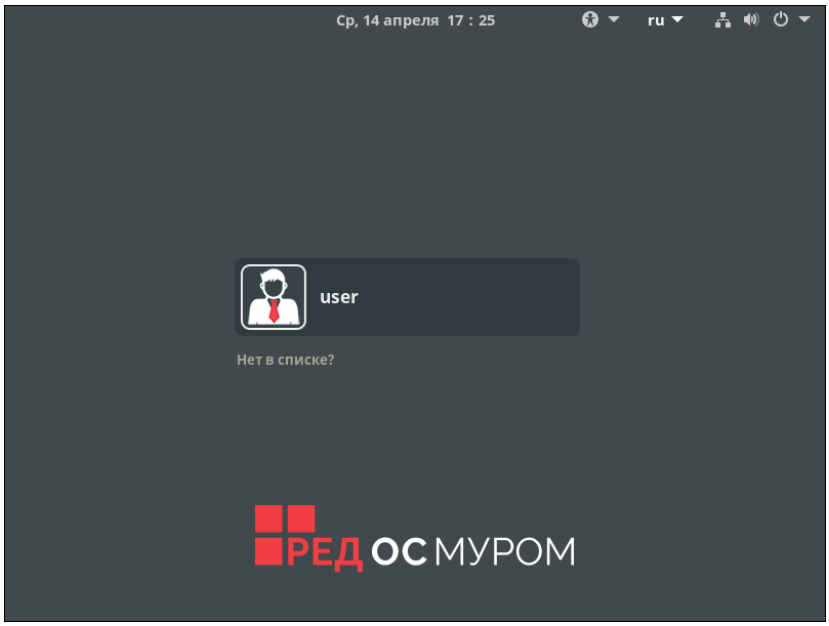
Далее производится загрузка РЕД ОС, которая визуально для пользователя может проходить двумя способами:

- **в текстовом режиме** с выводом лога загрузки, который отражает статус загрузки и старта модулей РЕД ОС. Текстовый режим загрузки производится до момента инициализации и старта графического сервера операционной системы. После старта графического сервера операционной системы загрузка РЕД ОС переходит в графический режим. При отказе оборудования или программного обеспечения, приводящем к невозможности старта графического сервера системы, загрузка ОС продолжается в текстовом режиме.
- **в графическом режиме**, в котором пользователю отображается графический экран загрузки ОС. Данный режим загрузки скрывает от пользователя текстовый лог загрузки ОС и выводит на экран анимированный прогресс-индикатор.

При зависании процесса загрузки ОС, выражающемся в сообщениях о сбоях в текстовом режиме загрузки или замирании на долгое время прогресс-индикатора загрузки, пользователю необходимо произвести выключение ПК, проверку подключенных к ПК периферийных устройств и произвести повторный запуск ОС. При повторном зависании загрузки пользователь должен выключить электрическое питание ПК и периферийных устройств и обратиться к администратору для устранения неисправности.

Аутентификация пользователя

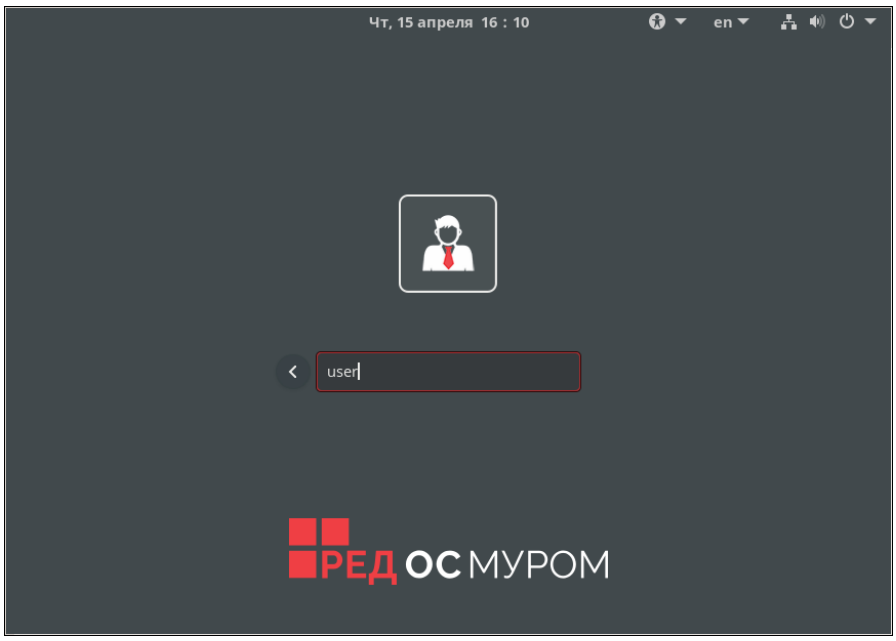
По окончании загрузки РЕД ОС пользователю отображается экран приветствия и приглашения к аутентификации, приведенный на рисунке ниже.



В РЕД ОС база данных пользователей может быть как локальной для операционной системы, так и являться частью единого пространства пользователей (ЕПП), функционирующего на основе протокола LDAP.

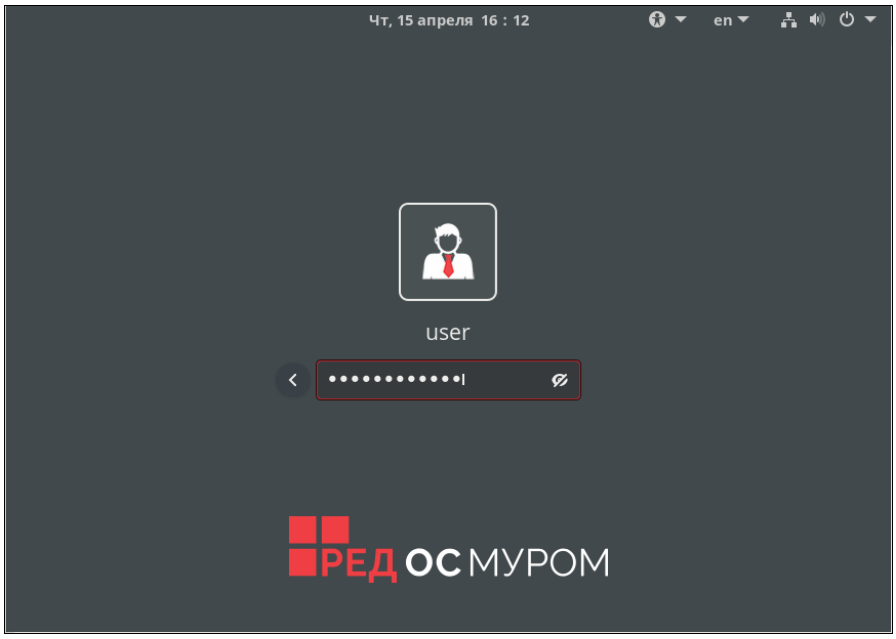
Если ЕПП не используется, аутентификация осуществляется с помощью локальной БД пользователей. При использовании ЕПП аутентификация пользователей осуществляется централизованно по протоколу LDAP. В ЕПП в качестве источника данных для идентификации и аутентификации пользователей применяются службы каталогов openldap.

Для аутентификации в операционной системе по локальной БД пользователей, в окне запроса аутентификационных данных необходимо выбрать соответствующего пользователя в списке пользователей или ввести имя пользователя (логин пользователя) в поле «**Имя пользователя**» нажав кнопку «**Нет в списке?**», ввести пароль учетной записи и нажать клавишу «**Enter**».

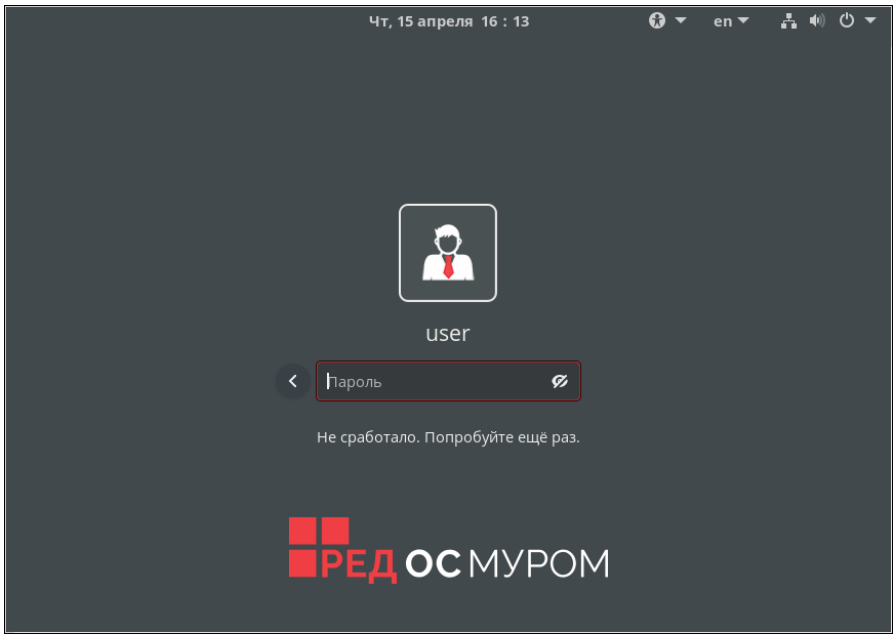


Если используется многофакторная аутентификация необходимо использовать дополнительные факторы аутентификации предоставленные администратором системы.

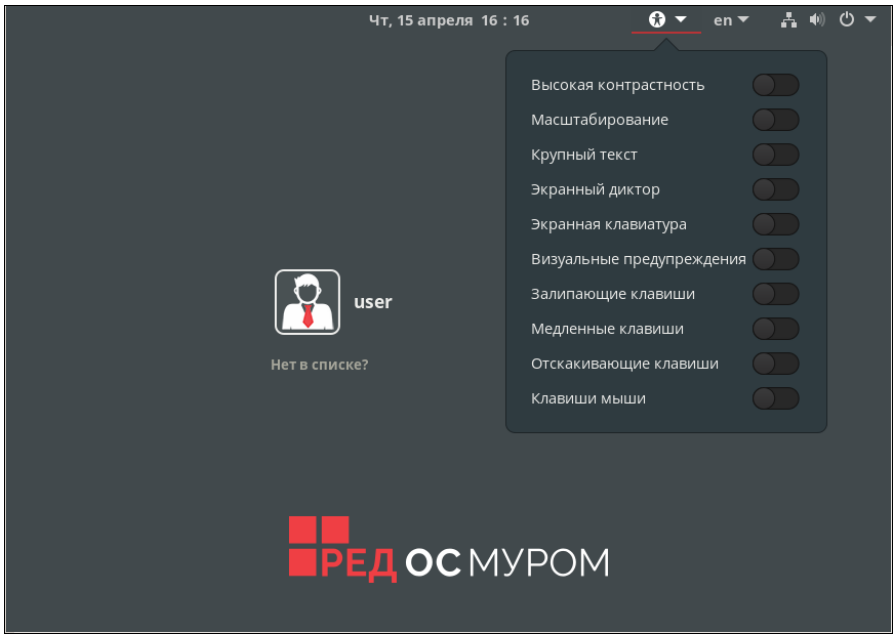
После ввода имени пользователя необходимо ввести пароль пользователя и нажать клавишу «**Enter**».



При неправильно указанных атрибутах пользователя (логин и/или пароль) РЕД ОС выводит предупреждение о сбое во время проверки данных. После этого РЕД ОС предлагает пользователю повторно ввести аутентификационную информацию.

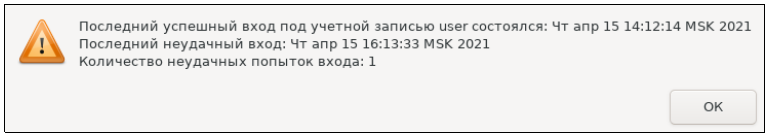


РЕД ОС при аутентификации предоставляет пользователям с ограниченными возможностями набор средств для облегчения процесса работы в ОС: экранная клавиатура; контрастные цветовые схемы; крупный экранный шрифт и т.д.

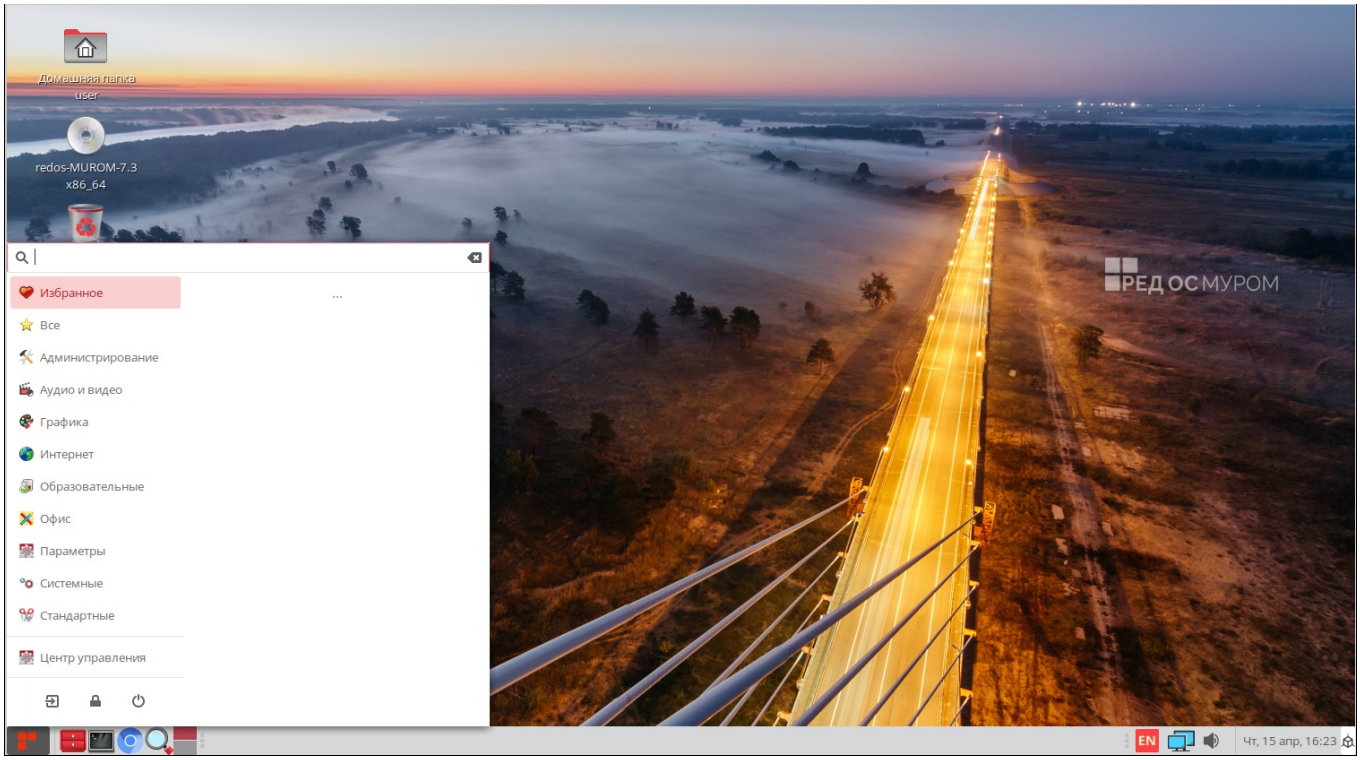


После того, как пользователь ввел корректные аутентификационные данные, РЕД ОС загружает рабочий стол пользователя.

До момента полной загрузки графического окружения пользователя выводится информационное окно с датой и временем последнего успешного входа в систему от имени этой учетной записи, дату и время последнего неудачного входа пользователя и количество неуспешных попыток ввода пароля.

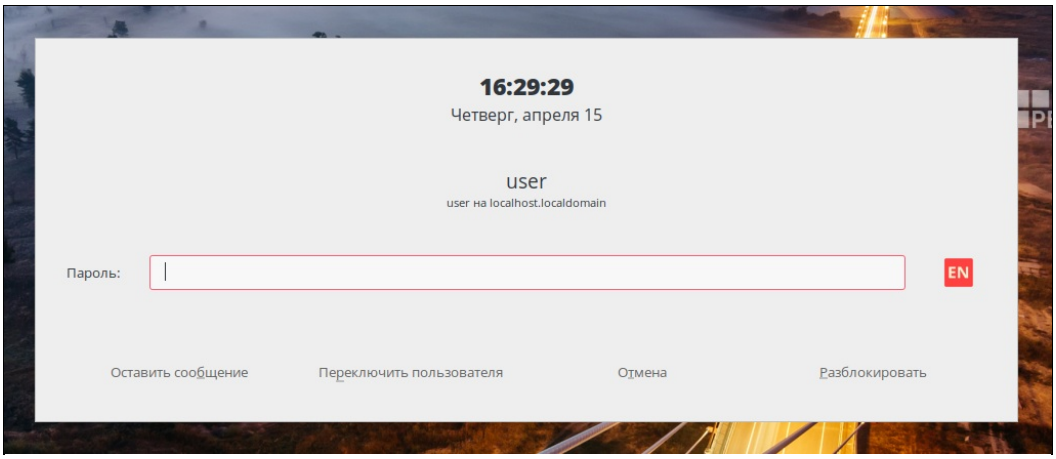


После этого происходит окончательная загрузка графического окружения пользователя.

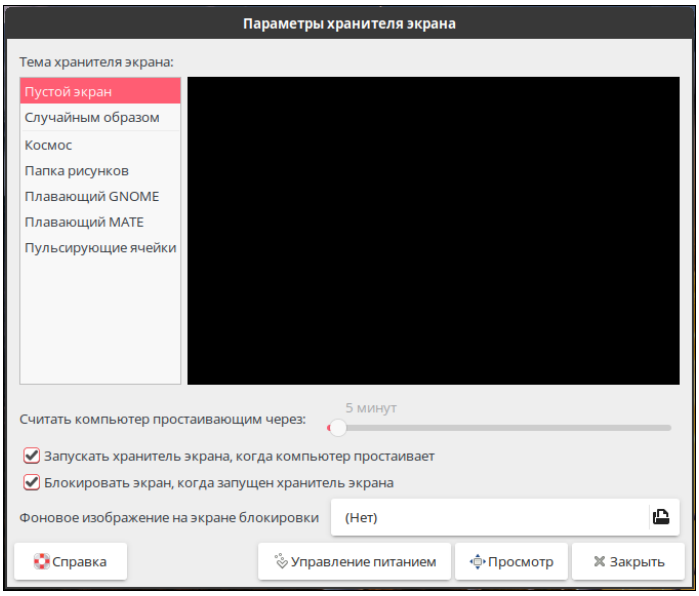


В правом нижнем углу рабочего стола отображается текущая дата и время, иконка с возможностью быстрого доступа к настройкам сетевого подключения и регулятор громкости. В левом нижнем углу вызывается меню приложения, осуществляется переход по каталогам файловой системы и доступ к утилитам системной настройки. Далее следуют иконки быстрого запуска наиболее часто используемых приложений.

При продолжительном бездействии пользователя рабочий стол пользователя блокируется, и для возобновления работы пользователю требуется провести повторную аутентификацию в РЕД ОС.



Значение продолжительности бездействия пользователя, после которого произойдет блокировка рабочего стола, определяется утилитой «**Хранитель экрана**». Данная утилита находится в «**Главном меню**» - «**Параметры**». Внешний вид утилиты управления хранителем экрана приведен на рисунке ниже.



Все действия пользователя при аутентификации, успешные и неуспешные попытки аутентификации фиксируются в системном журнале РЕД ОС.

Окно настройки РЕД ОС

Вкладка «Настройка системы»
Вкладка «Сторонние приложения»
Вкладка «Документация и Помощь»
Вкладка «О РЕД ОС»

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** redoswelcome-1.13.2-1

Вы можете подробнее ознакомиться с проведением первой настройки РЕД ОС, просмотрев наши обучающие видео:

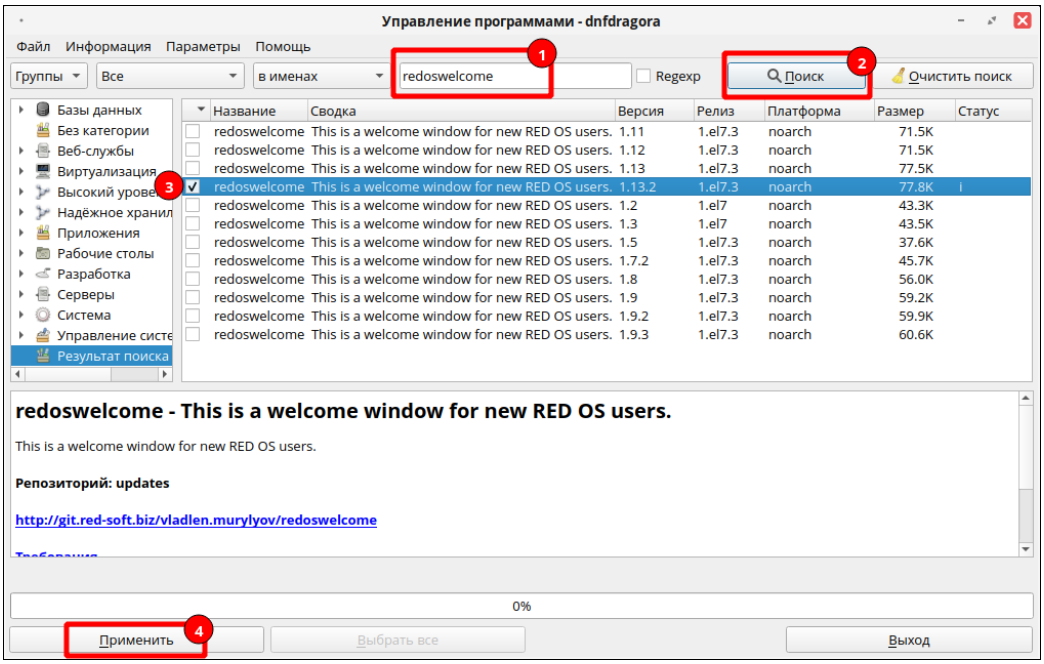
- на **RuTube** — Окно настройки РЕД ОС;
- в **Яндекс.Дзен** — Окно настройки РЕД ОС;
- в **VK Видео** — Окно настройки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

В репозитории РЕД ОС существует утилита «**Окно настройки РЕД ОС**», позволяющая пользователям ознакомиться с базовым функционалом ОС перед началом работы.

В более поздних версиях ОС данная утилита установлена по умолчанию.

Установка утилиты доступна через менеджер пакетов dnfdragora. Откройте «**Главное меню**» - «**Администрирование**» - «**Управление пакетами dnfdragora**», в строке поиска впишите название пакета **redoswelcome**, нажмите «**Поиск**». В окне результатов выберите последнюю из доступных версий пакета и нажмите кнопку «**Применить**».



Также доступен консольный вариант установки утилиты, для этого перейдите в сеанс пользователя **root**:

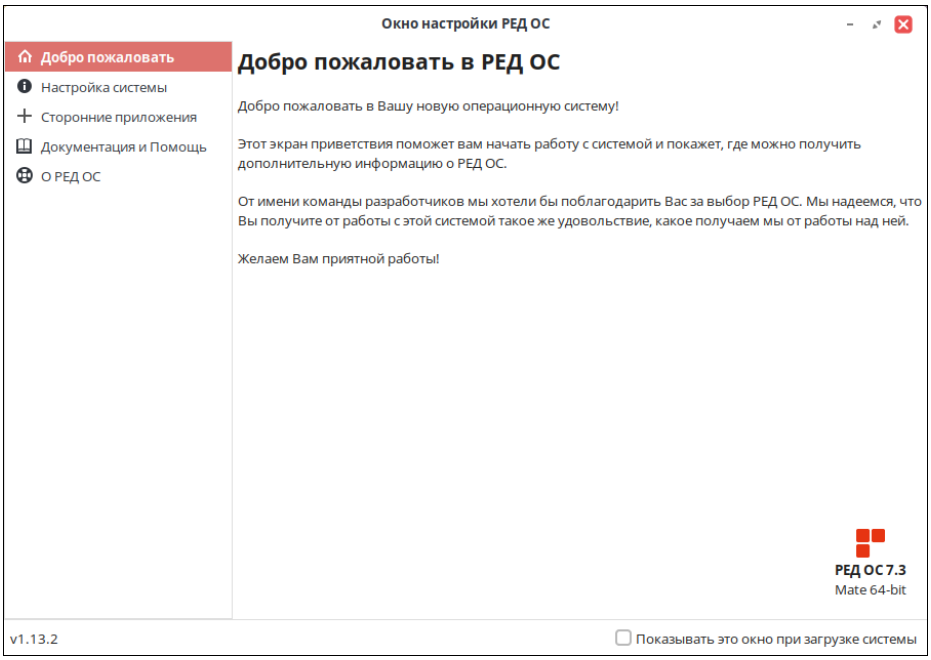
```
su -
```

и выполните команду:

```
dnf install redoswelcome
```

После установки программа будет доступна из «**Главного меню**» - «**Параметры**» - «**Окно настройки РЕД ОС**».

При первой авторизации пользователя в системе будет автоматически открыто следующее окно:



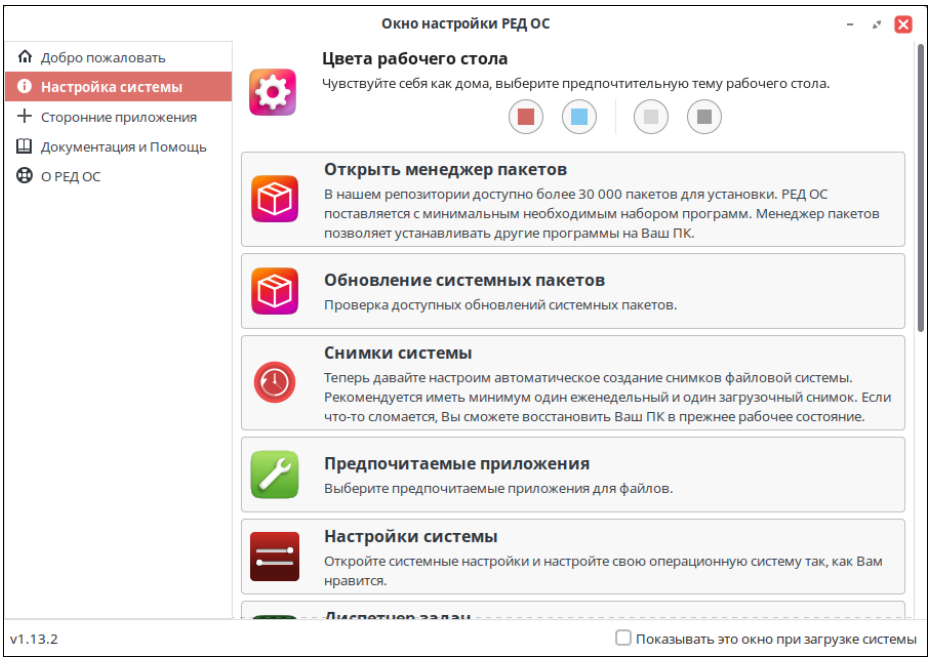
Стартовая страница утилиты позволяет пользователю:

- Ознакомиться с приветственным обращением от команды РЕД ОС;
- Включить или отключить возможность показа данной утилиты после авторизации пользователя;
- Переключаться между вкладками.

Вкладка «Настройка системы»

Функционал, доступный пользователю на данной странице:

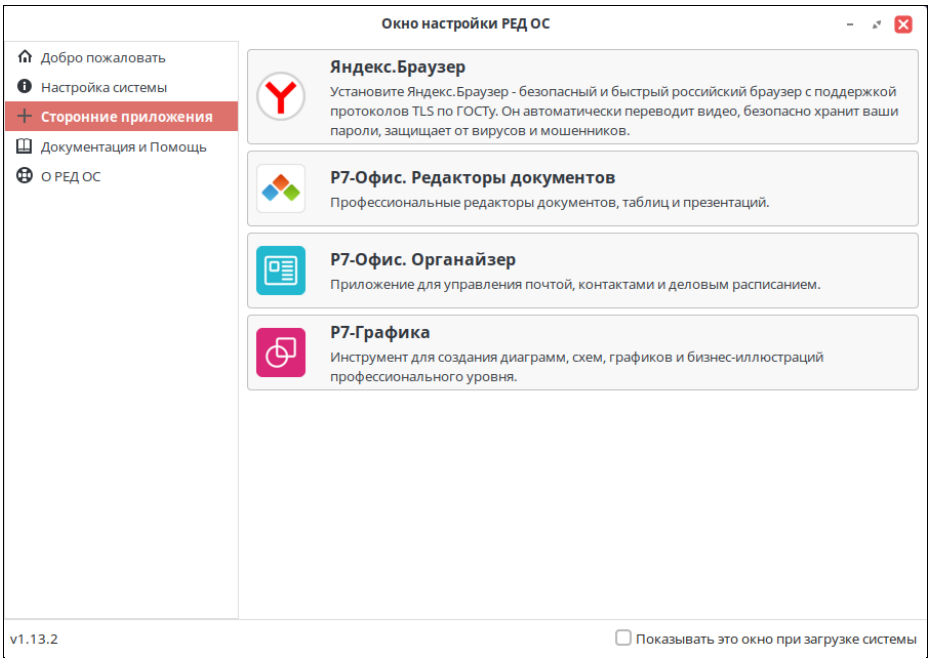
- Переключение оформления ОС между стандартными темами;
- Запуск для ознакомления предустановленного ряда программ (пакетов), перечисленных в списке.



Вкладка «Сторонние приложения»

На данной вкладке для установки доступны некоторые сторонние программы, такие как:

- Яндекс.Браузер;
- Р7-Офис. Редакторы документов;
- Р7-Офис. Органайзер;
- Р7-Графика.



Вкладка «Документация и Помощь»

Вкладка «**Документация и Помощь**» будет полезна как новичкам, так и администраторам. Здесь представлены публичные ресурсы компании, справочная информация о системе, а также существует возможность ознакомиться с другими продуктами компании.

Перечень основных ресурсов для поиска необходимой информации о работе в системе:

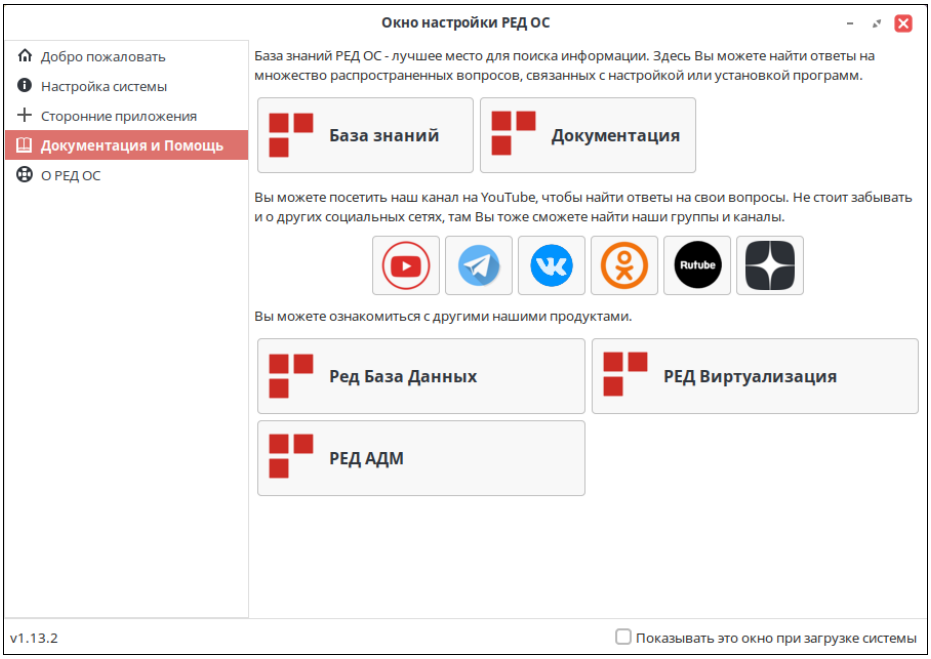
- База знаний;
- Документация.

Перечень доступных для посещения каналов, расположенных на следующих ресурсах:

- Telegram;
- ВКонтакте;
- Одноклассники;
- Rutube;
- Яндекс.Дзен.

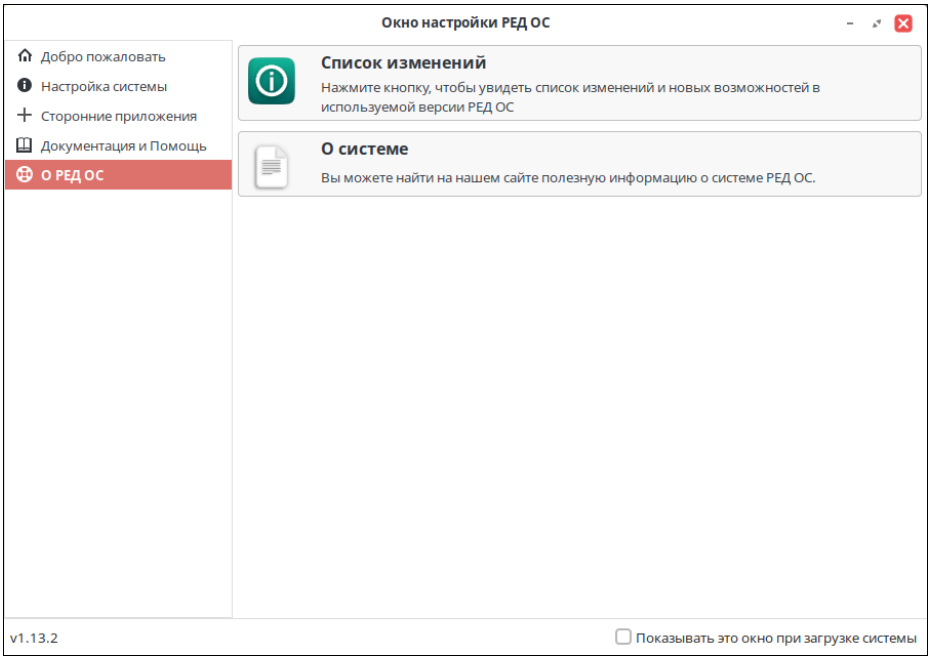
Другие продукты компании РЕД СОФТ, такие как:

- РЕД База Данных;
- РЕД Виртуализация;
- РЕД АДМ.



Вкладка «О РЕД ОС»

Здесь можно получить информацию о новых возможностях системы и перейти на сайт РЕД ОС.



Графическое окружение MATE

Апплеты
Настройка фона рабочего стола
Настройка системной панели
Настройка внешнего вида графического интерфейса РЕД ОС
Настройка шрифтов графического интерфейса РЕД ОС
Настройка хранителя экрана, блокировки и режима энергосбережения
Управление окнами графического интерфейса
Настройка рабочих областей
Работа с файловым менеджером
Автоматический запуск приложений
Настройка смены раскладки клавиатуры

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

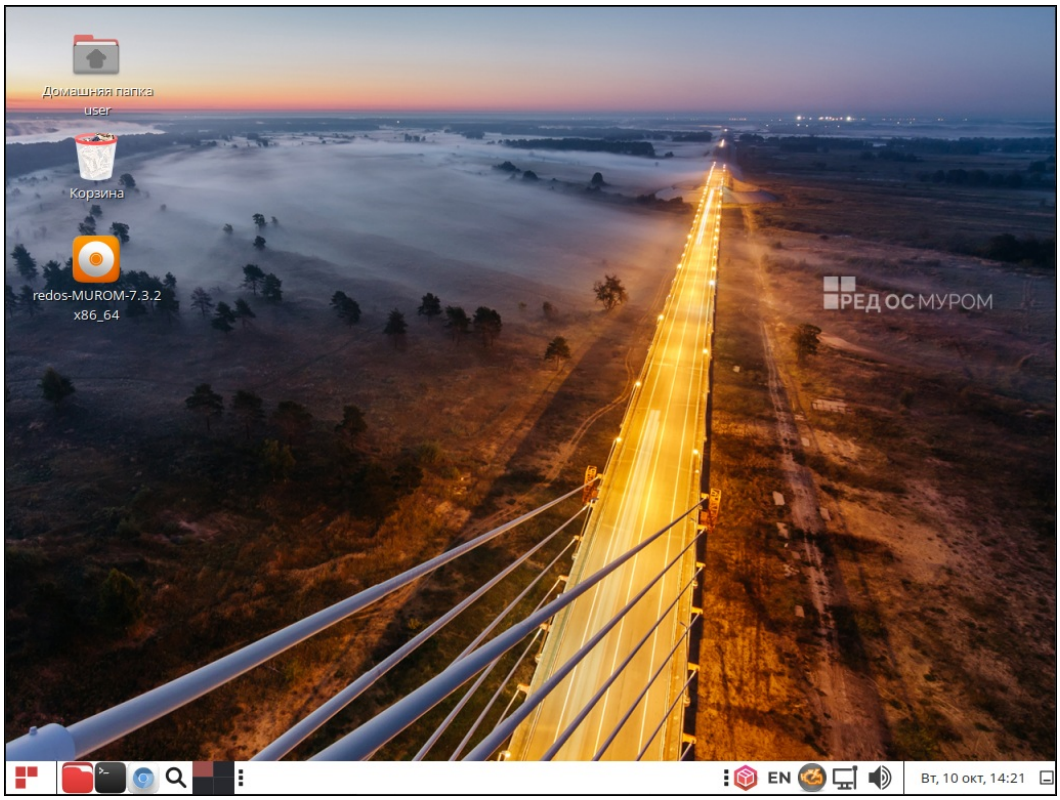
MATE – интегрированное графическое окружение рабочего стола в РЕД ОС.

Вы можете подробнее ознакомиться с возможностями графического окружения **MATE**, просмотрев наши обучающие видео:

- на **RuTube** — Основы работы с DE Mate;
- в **Яндекс.Дзен** — Основы работы с DE Mate.

На наших каналах вы также сможете найти много другой полезной информации.

Графическое окружение **MATE** выглядит следующим образом:

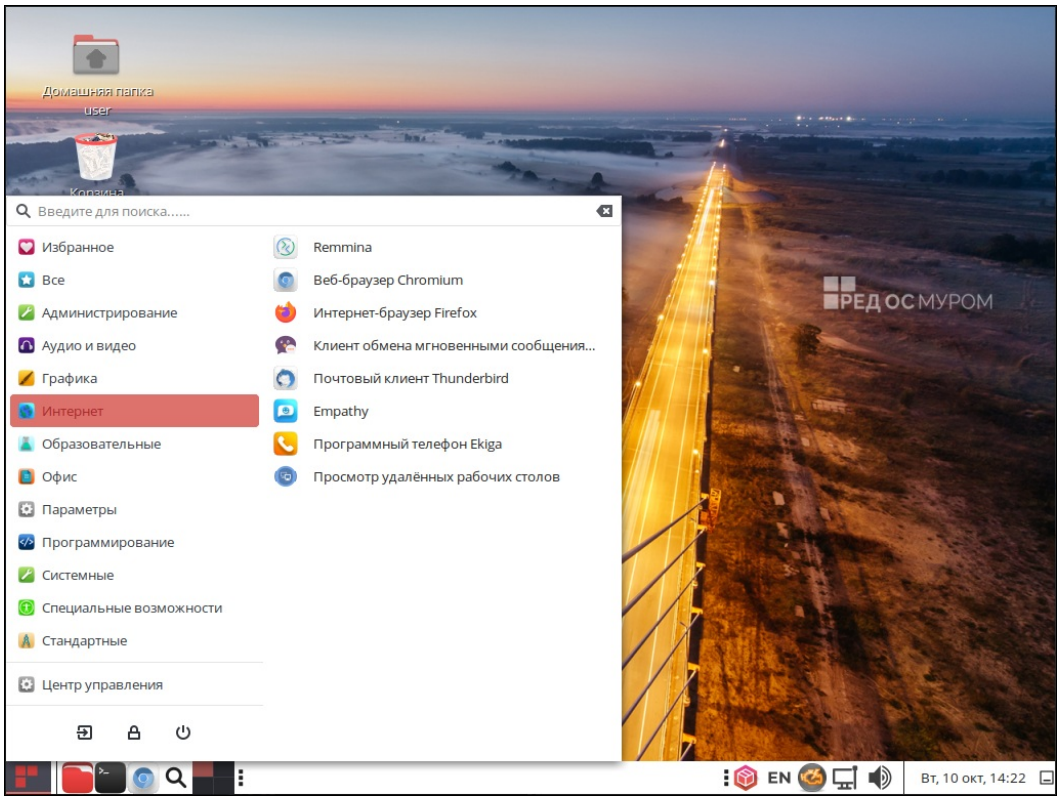


Главным элементом рабочего стола является системная панель, которая расположена в нижней части экрана и условно разделена на три основные части:

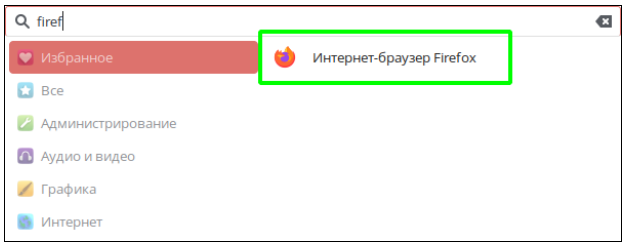
- Главное меню;
- Панель приложений;
- Панель апплетов.

Главное меню — представляет собой список установленных программ, разделенных на несколько категорий, таких как «Аудио и

видео», «Графика», «Интернет», «Офис» и т. д.

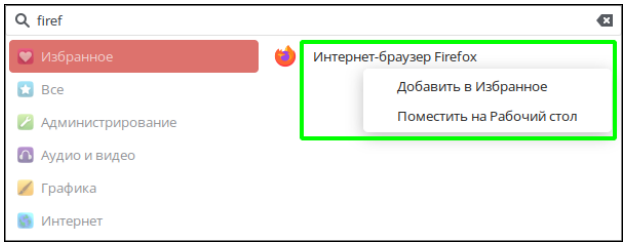


Поисковая строка здесь предназначена для поиска установленных приложений. Начните вводить ключевое слово, чтобы получить список только тех компонентов меню, которые его содержат.



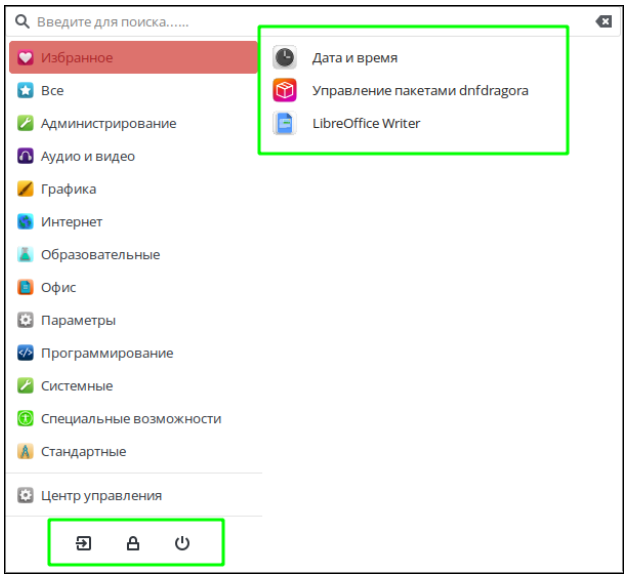
При нажатии ПКМ по какому-либо приложению можно выбрать несколько действий:

- добавить приложение на рабочий стол;
- добавить приложение в избранное.

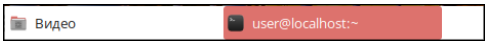


Список избранного изначально пуст.

Также здесь доступны кнопки блокировки экрана, выхода из сеанса и завершения работы.



Панель приложений представляет собой управляющую панель, которая по умолчанию располагается в нижней части экрана. Управляющая панель включает в себя следующие компоненты:

- кнопка Главного меню ( ) ;
- область запуска приложений — Panel Launcher ( );
- область открытых приложений — Window list ();

- область системных сообщений — Notifications ();

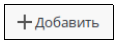
- системный лоток (трей) — System Tray, куда помещаются пиктограммы некоторых работающих в фоне приложений ();
- несколько пиктограмм разного назначения — модуль сетевых соединений, регулятор громкости, часы, индикатор раскладки клавиатуры и т. д. ().

Апплеты

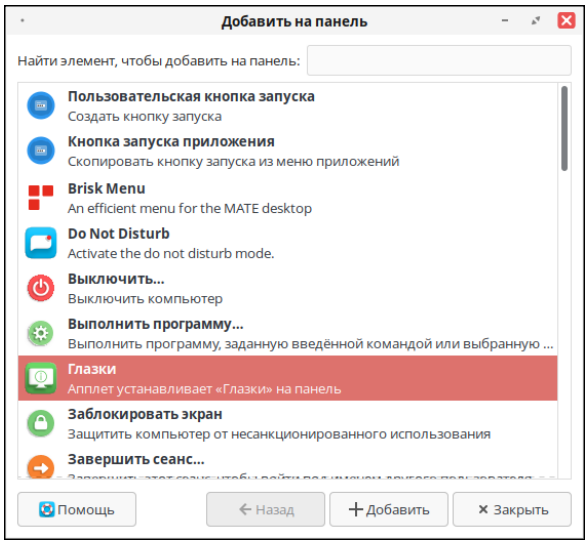
Все области и кнопки панели представляют собой так называемые апплеты – небольшие программы. Апплеты могут как добавляться на панель, так и удаляться с неё. Главное меню, системный лоток, менеджер сети, настройки пользователя — всё это апплеты.

Для добавления новых апплетов на панель нажмите ПКМ по системной панели и в появившемся контекстном меню выберите пункт «Добавить на панель...».

В открывшемся окне можно настроить доступные апплеты.

При выборе какого-либо установленного апплета становится активной строка управления, с помощью которой можно добавить апплет на панель () или закрыть окно апплетов ().

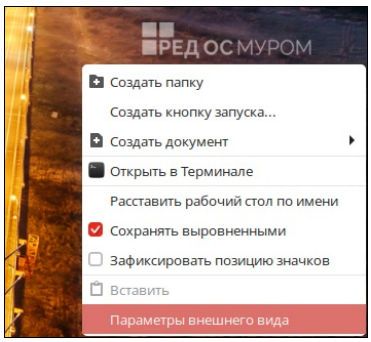
Кнопка «Помощь» вызывает справку по добавлению объектов на системную панель.



Настройка фона рабочего стола

Для смены изображения рабочего стола существует два варианта.

Вариант 1. Для смены фона рабочего стола необходимо в свободной части рабочего стола вызвать контекстное меню (нажав ПКМ). В открывшемся контекстном меню необходимо выбрать пункт «Параметры внешнего вида».

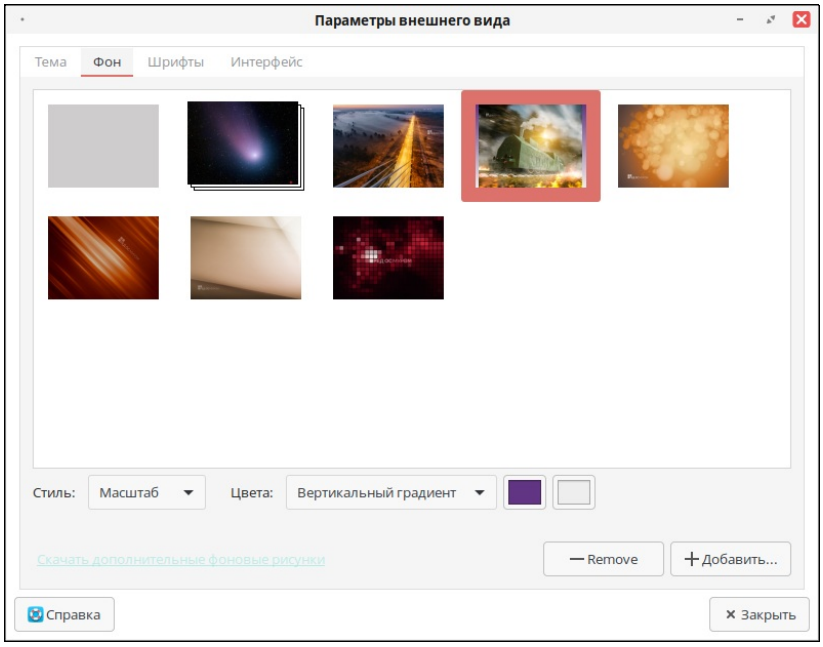


Вариант 2. Для смены фона рабочего стола пользователю необходимо в системной панели выбрать пункт «Главное меню» - «Параметры» - «Внешний вид».

На вкладке «Фон» можно выбрать изображение из имеющихся или добавить собственное, нажав кнопку «Добавить...».

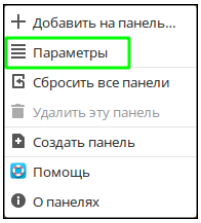
Ненужные изображения можно удалить, нажав «Remove».

Дополнительно можно выбрать стиль отображения фонового рисунка на рабочем столе — мозаика, масштаб, размещение по центру или растягивание, и выбрать вариант заполнения экрана и его цвет.



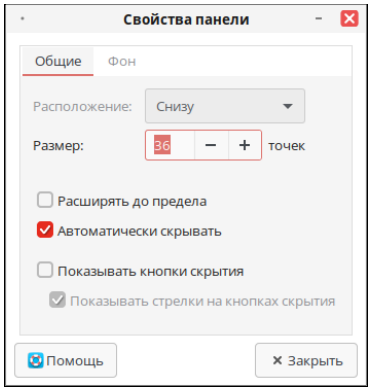
Настройка системной панели

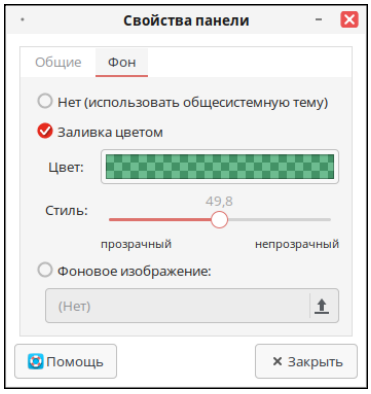
Для изменения параметров панели задач графической оболочки РЕД ОС **MATE** также нужно с помощью клика ПКМ по панели вызвать контекстное меню и выбрать соответствующий пункт меню.



При выборе пункта меню «Параметры» будет открыто окно, в котором на вкладке «Общие» доступны такие настройки, как расположение панели (сверху или снизу), размер панели, внешний вид панели (расширение панели до предела, автоматическое скрытие панели, отображение кнопок скрытия панели).

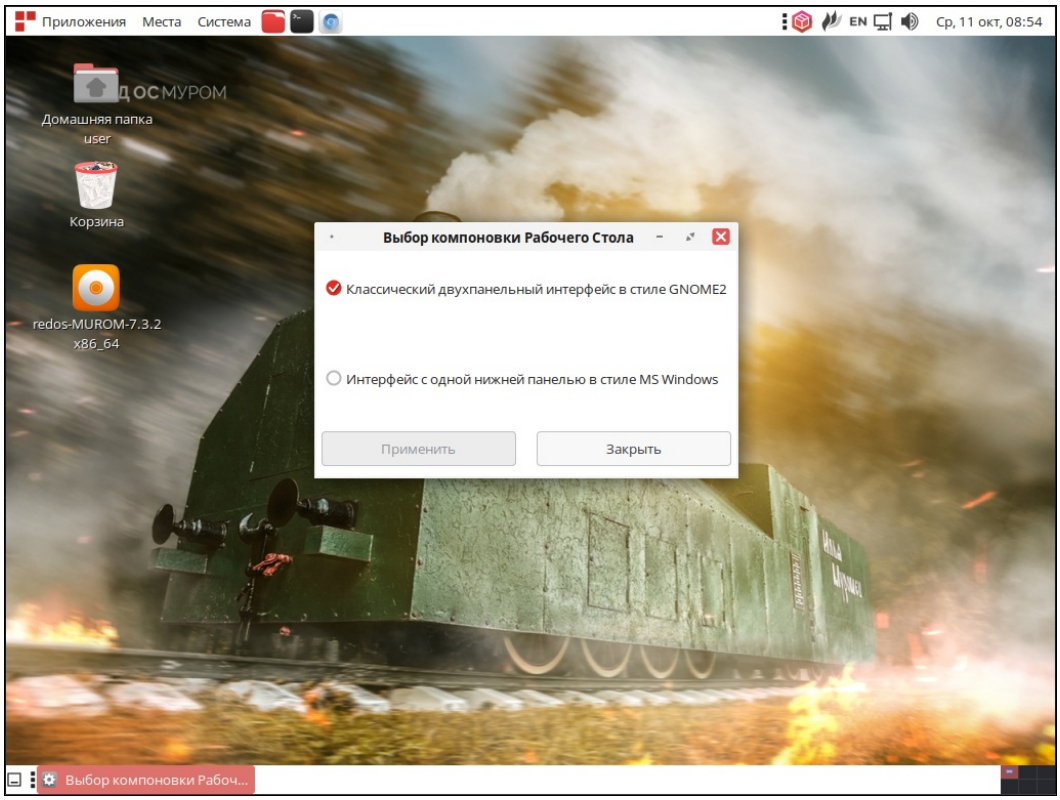
На вкладке «Фон» производится настройка фона системной панели — можно сделать сплошную заливку цветом или выбрать собственное изображение фона панели, а также задать прозрачность.





По умолчанию в графическом окружении **MATE** для удобства пользователей применяется интерфейс с одной нижней панелью, но можно настроить классический двухпанельный интерфейс MATE, открыв «Главное меню» - «Параметры» - «Компоновка панелей» и установив соответствующий параметр.

После применения настроек рабочий стол будет выглядеть следующим образом:



На верхней панели **Главное меню** разделяется на пункт «Приложения», где доступны установленные программы, и пункт «Система», где доступны настройки системы и кнопки выключения питания, завершения сеанса и блокировки экрана.

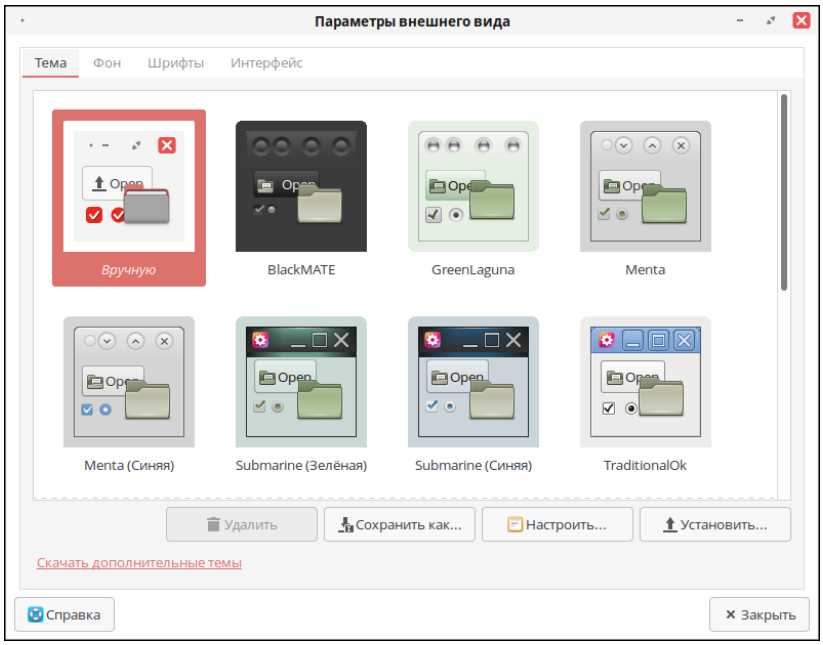
В пункте «Места» расположены доступные пользователю каталоги, настройка сети, инструмент поиска и недавние документы.

Также здесь отображаются закрепленные для быстрого доступа приложения и системный трей.

На нижней панели располагается кнопка для сворачивания всех открытых окон и открытия рабочего стола, список открытых окон и переключатель рабочих областей.

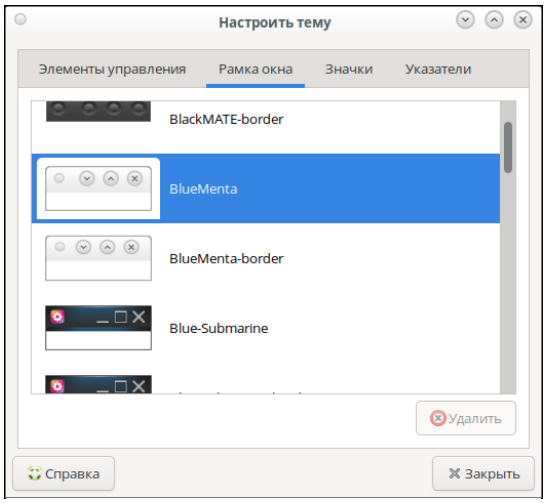
Настройка внешнего вида графического интерфейса РЕД ОС

Для смены внешнего вида окон графической оболочки РЕД ОС пользователю необходимо на свободной области рабочего стола вызвать контекстное меню (нажав ПКМ), выбрать пункт меню «Параметры внешнего вида» и перейти на вкладку «Тема».



Здесь можно обратиться к коллекции доступных тем. Для установки понравившейся темы нажмите «Установить».

Также можно задать стилевое оформление отдельных элементов интерфейса, полностью независимое друг от друга и от темы рабочего стола, нажав кнопку «Настроить».

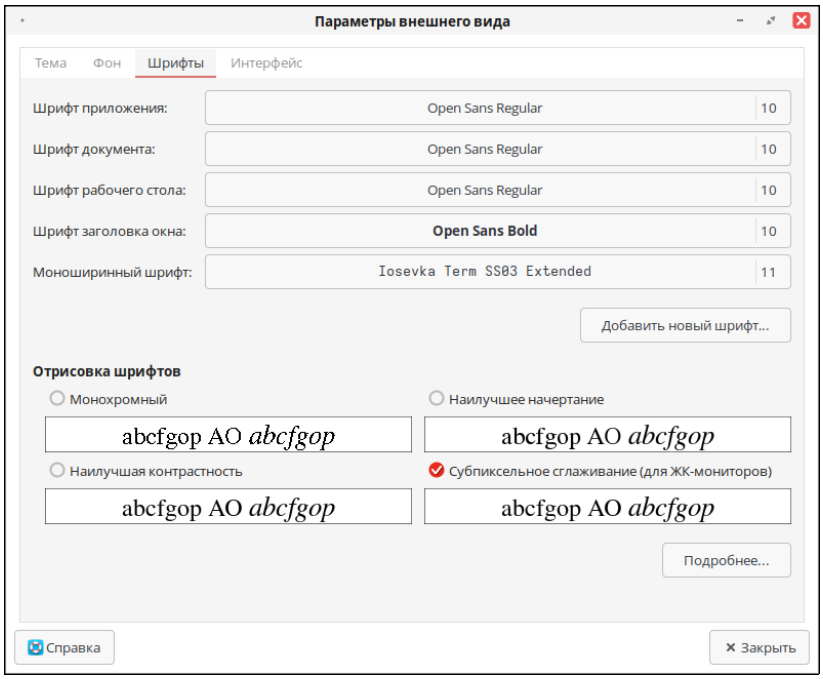


Большое количество доступных вариантов позволяют комбинировать элементы оформления интерфейса в широких пределах, достигая максимального визуального эффекта. Это имеет практическое значение, особенно для людей с плохим зрением или нарушением цветовосприятия.

Настройка шрифтов графического интерфейса РЕД ОС

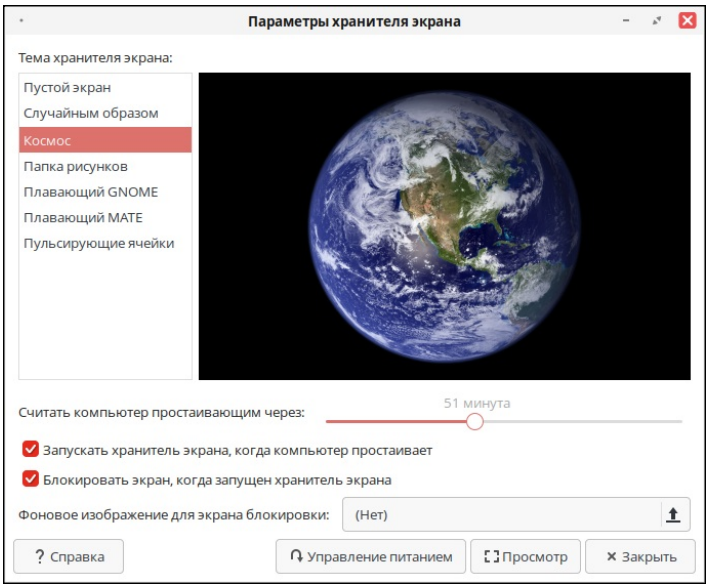
Для изменения используемых шрифтов графической оболочки РЕД ОС пользователю необходимо на свободной области рабочего стола вызвать контекстное меню (нажав ПКМ), выбрать пункт меню «Параметры внешнего вида» и перейти на вкладку «Шрифты».

В окне можно настроить шрифты как для заголовков окон, так и для документов.

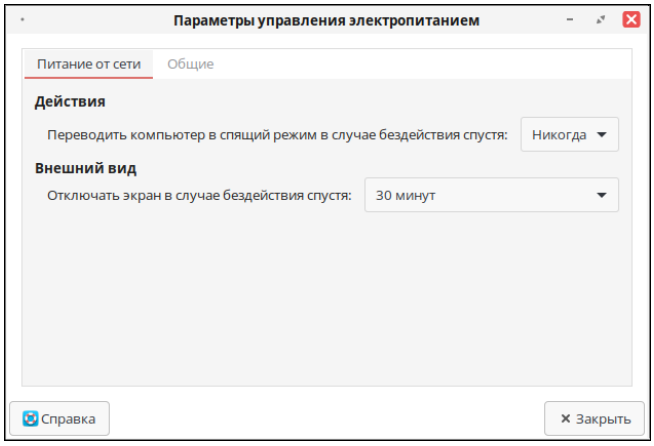


Настройка хранителя экрана, блокировки и режима энергосбережения

Настройка времени блокировки рабочего стола, настройка хранителя экрана, а также управление режимом энергосбережения определяется утилитой «Хранитель экрана». Данная утилита находится в «Главном меню» - «Параметры».



Утилита позволяет пользователю определить время, по истечении которого, при бездействии пользователя, рабочий стол системы будет заблокирован, выбрать тему хранителя экрана и определить режимы управления питанием.

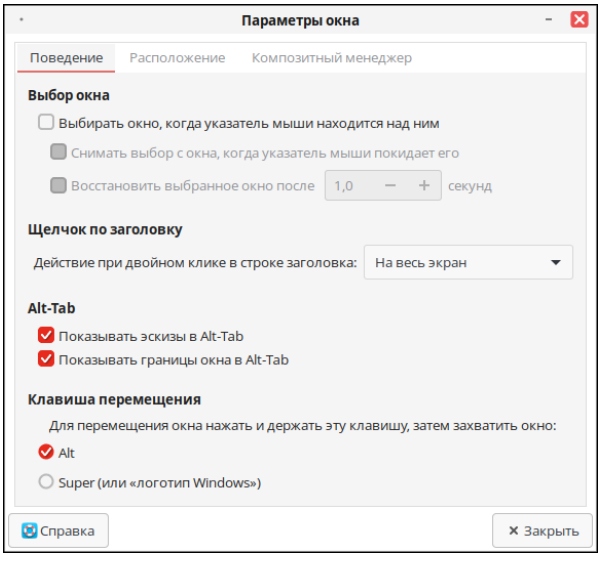


Управление окнами графического интерфейса

Управление окнами подразумевает в первую очередь переключение между ними.

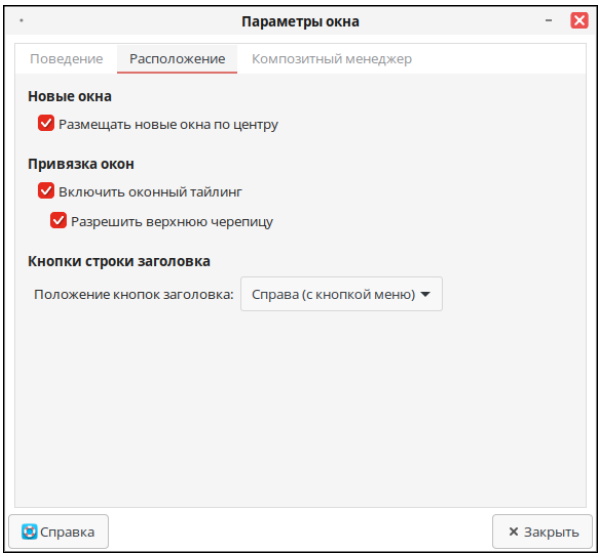
Для настройки параметров окон необходимо открыть «Главное меню» - «Параметры» - «Окна».

На вкладке «Поведение» можно настроить отклик окон на поведение мыши, а также настроить переключение между окнами при помощи комбинации клавиш **Alt+Tab**.

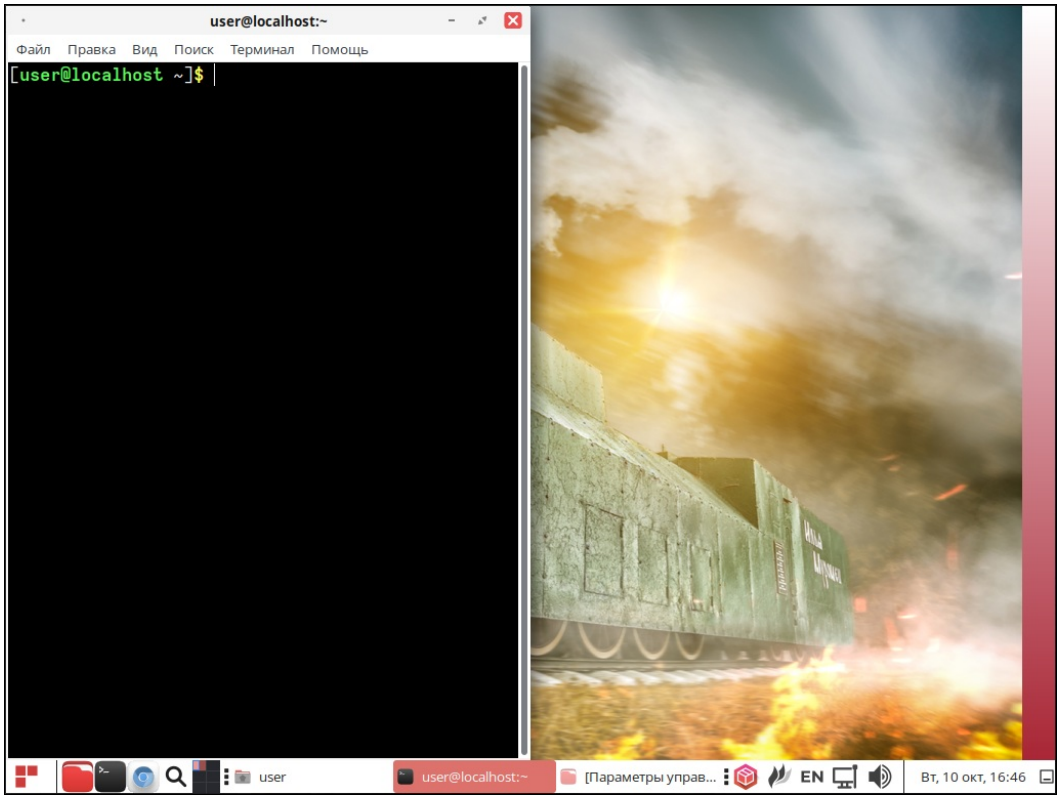


На вкладке «Расположение» настраивается положение новых окон и оконный тайлинг (привязка окна к какой-либо части экрана).

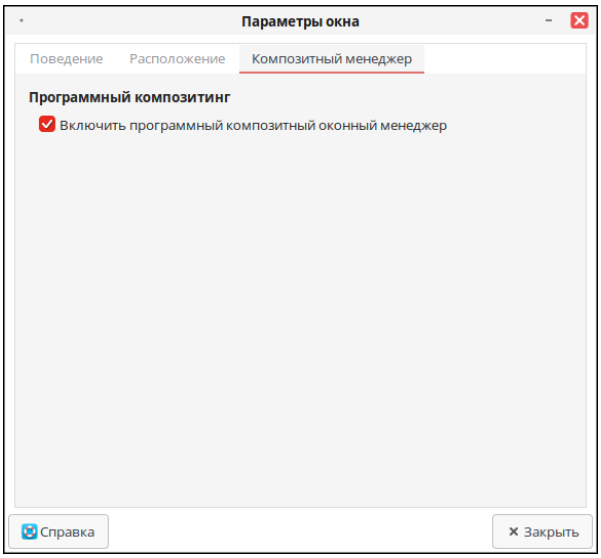
Также здесь можно сменить расположение кнопок заголовка — слева или справа.



При перетаскивании окна мышью к верхней границе экрана оно занимает верхнюю его половину. Аналогичное движение к нижней границе экрана разворачивает окно на нижнюю его половину. Перемещение окна к боковой стороне экрана (левой или правой) прикрепляет его на левую или правую половины, в зависимости от стороны перетаскивания.



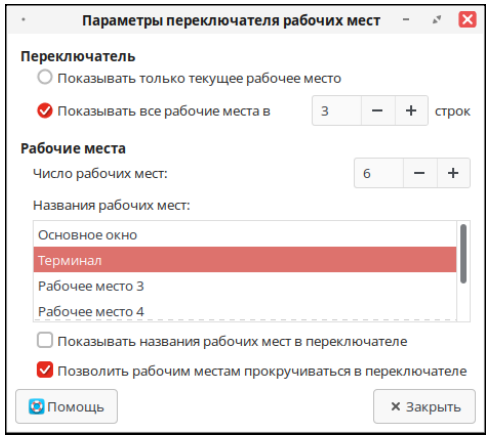
На вкладке «Композитный менеджер» включается или отключается использование композитного оконного менеджера.



Настройка рабочих областей

В **MATE** существуют дополнительные рабочие пространства, по умолчанию доступно 4 рабочие области. При нажатии клавиш **Ctrl+Alt+Up** (стрелка вверх) на экран выводятся все доступные рабочие области. Здесь можно легко переключиться на необходимую рабочую область. Для быстрого переключения между областями воспользуйтесь клавишами **Ctrl+Alt + Right** (стрелка вправо) или **Left** (стрелка влево).

Переключатель рабочих областей находится на системной панели. Задать нужные настройки, создать новые рабочие области и переименовать имеющиеся можно, кликнув ПКМ по апплету переключателя рабочих областей и выбрав в появившемся контекстном меню пункт «Настройка».



Работа с файловым менеджером

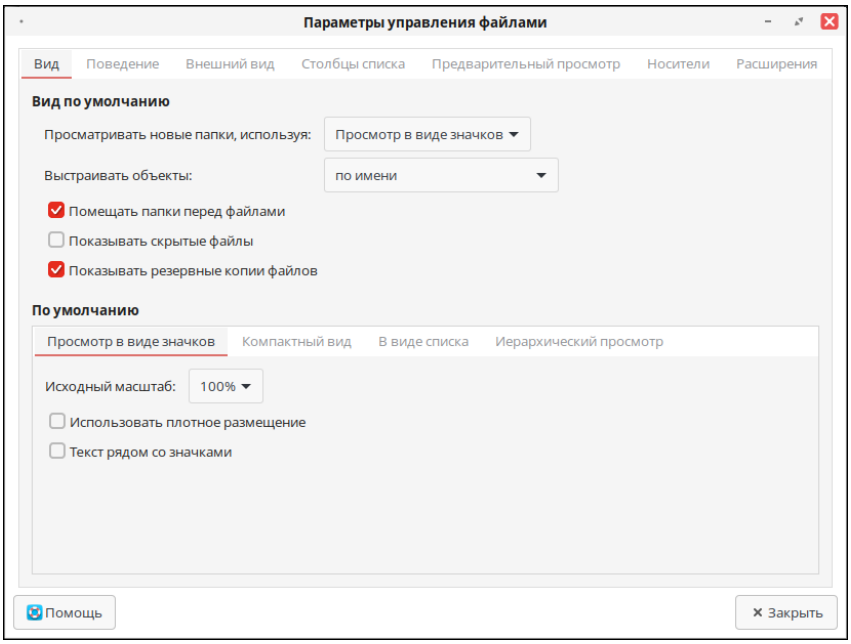
По умолчанию в **MATE** используется файловый менеджер **Caja**. Далее будут рассмотрены некоторые основные возможности файлового менеджера.

При нажатии клавиши **F3** можно разделить рабочую зону на две части.

При помощи сочетания клавиш **Ctrl+1**, **Ctrl+2**, **Ctrl+3** можно изменить вид отображения каталогов и файлов — значки, список или компактный вид.

Через пункт панели инструментов «Закладки» можно создавать новые закладки, прикреплять новые каталоги в быстрый доступ и т.д.

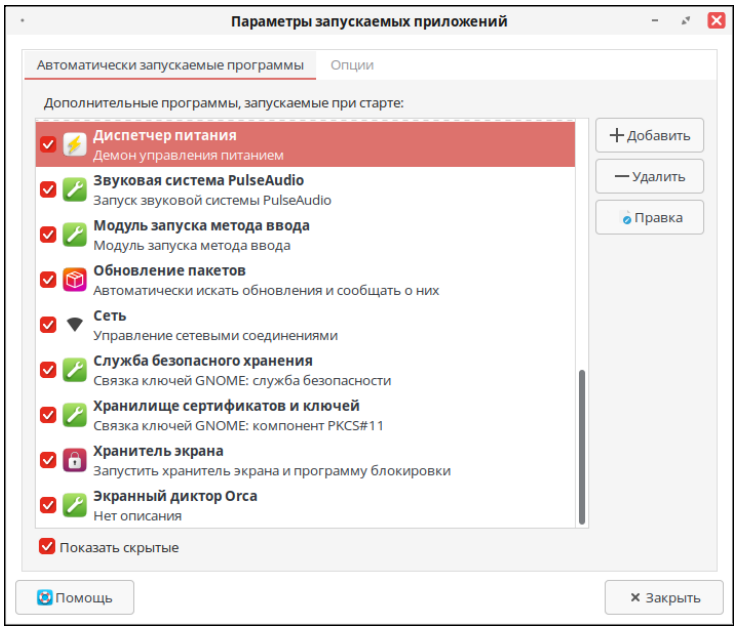
Для тонкой настройки отображения каталогов и их содержимого, поведения мыши, внешнего вида, списков, предварительного просмотра, внешних носителей и дополнительных расширений необходимо выбрать на панели инструментов пункт меню «Правка» - «Параметры».



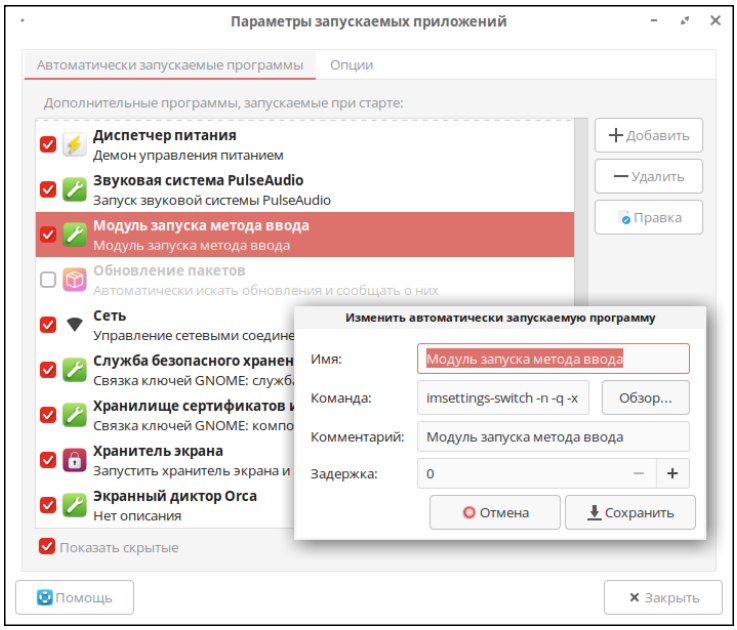
Также есть множество других настроек, которые позволят комфортно работать с файловым менеджером.

Автоматический запуск приложений

В «Главном меню» - «Параметры» - «Запускаемые приложения» доступна настройка автоматически запускаемых программ при старте системы.

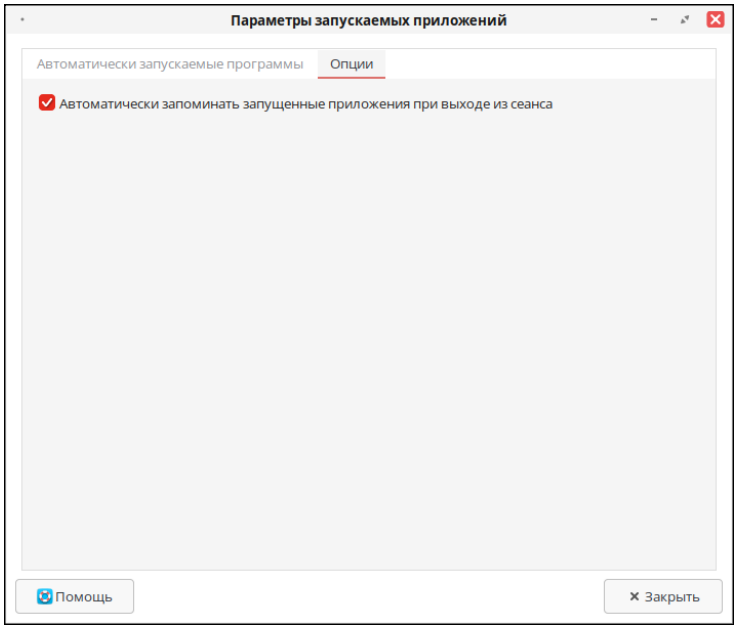


На вкладке «Автоматически запускаемые программы» можно отключить ненужные для запуска приложения, сняв флаг, установленный рядом с ним. Можно внести изменения в настроенные и включенные программы или просмотреть подробные сведения, нажав кнопку «Правка».



Также можно добавить новые необходимые для запуска программы или удалить из списка имеющиеся, нажав соответственно «Добавить» или «Удалить».

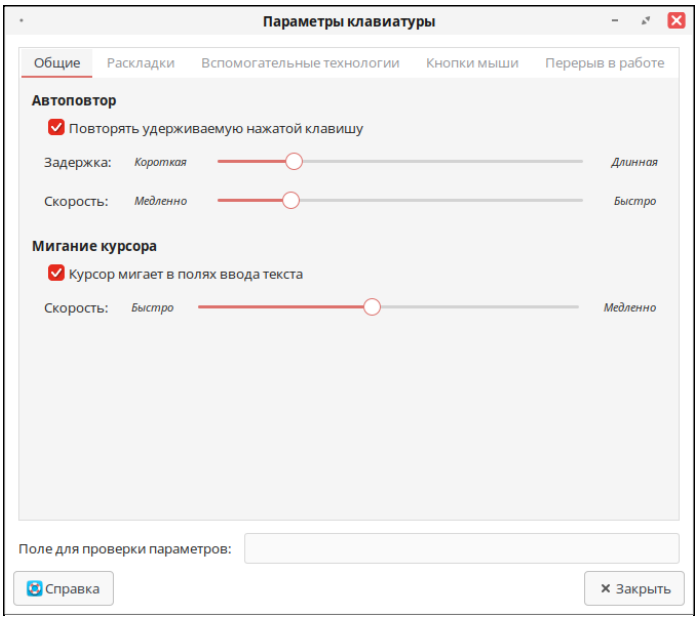
На вкладке «Опции» доступна настройка запоминания запущенных приложений при выходе из сеанса, т. е. при следующем старте системы открытые ранее программы будут автоматически запущены.



Настройка смены раскладки клавиатуры

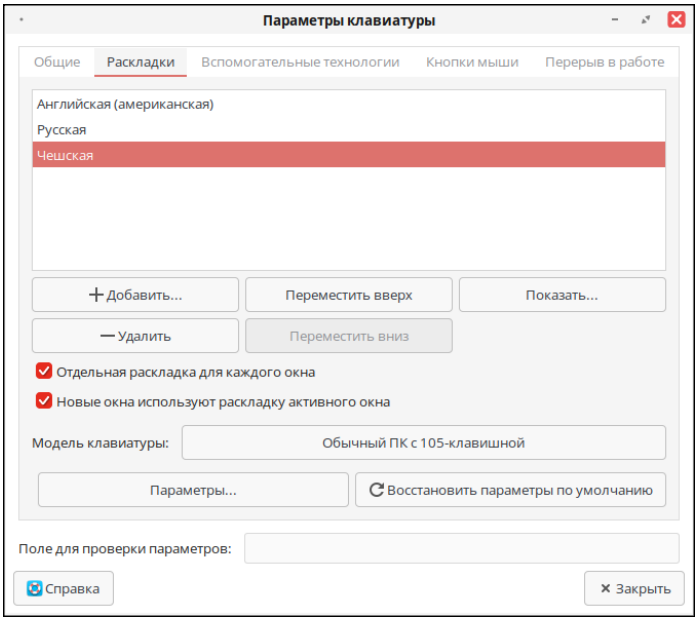
В РЕД ОС по умолчанию смена раскладки клавиатуры (языка ввода) осуществляется при одновременном нажатии функциональных клавиш клавиатуры **Shift+Alt** одновременно. Для изменения сочетания функциональных клавиш, применяемых для смены раскладки клавиатуры, необходимо в системной панели перейти в «Главное меню» - «Параметры» - «Клавиатура».

На вкладке «Общие» задается автоповтор нажатых клавиш и скорость мигания курсора в полях ввода.

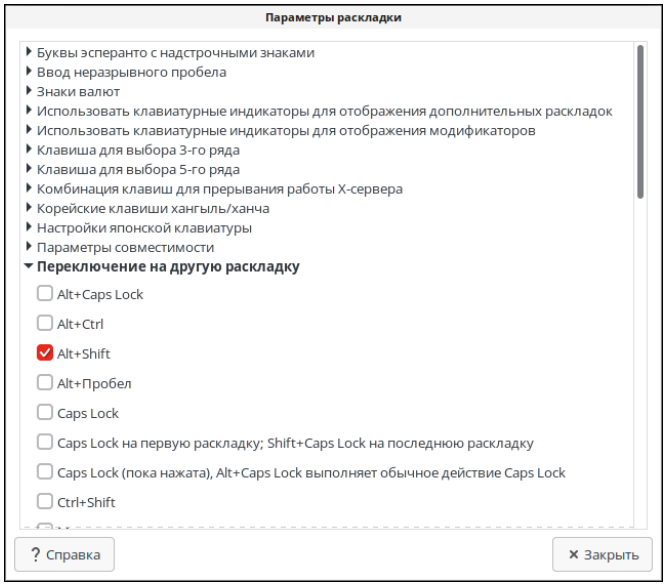


На вкладке «Раскладки» задается порядок раскладки клавиатуры, также можно добавить новые языки, переместить выбранную раскладку выше или ниже в списке, удалить ненужную раскладку.

Дополнительно можно выбрать модель клавиатуры, определить раскладки клавиатуры для других рабочих областей.

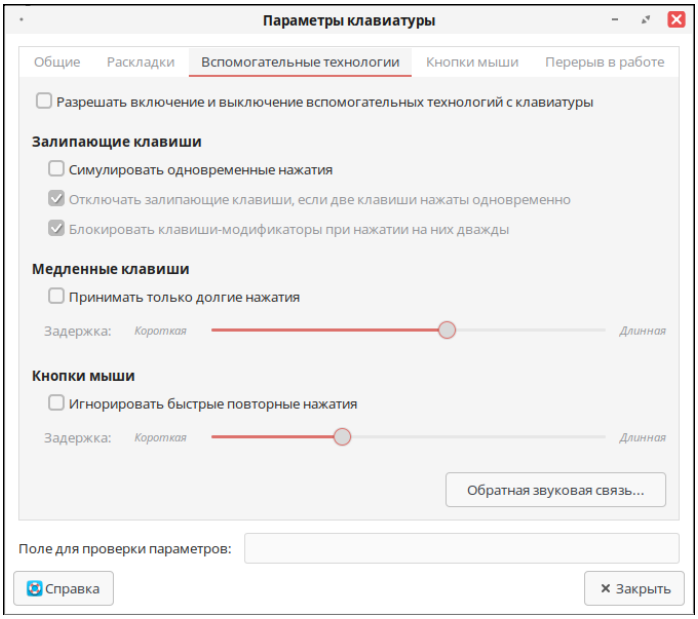


При нажатии на кнопку «Параметры» можно изменить сочетания клавиш клавиатуры по умолчанию.

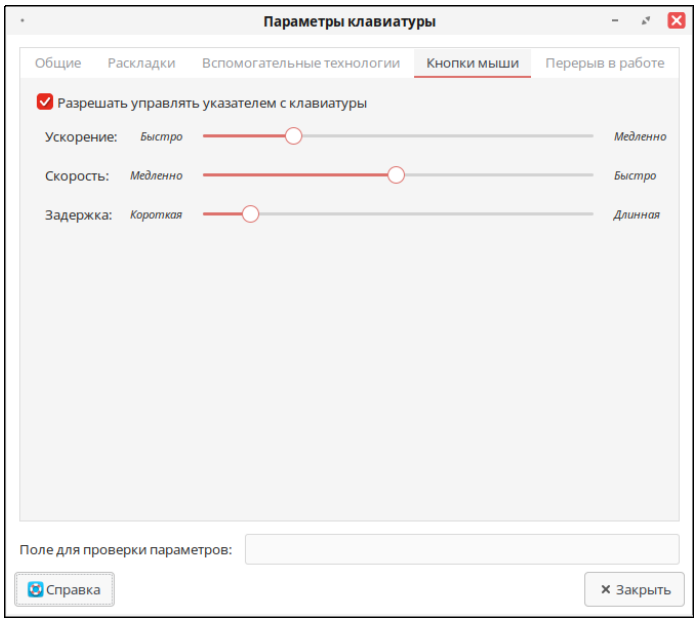


На вкладке «Вспомогательные возможности» определяется необходимость использования вспомогательных технологий с клавиатуры,

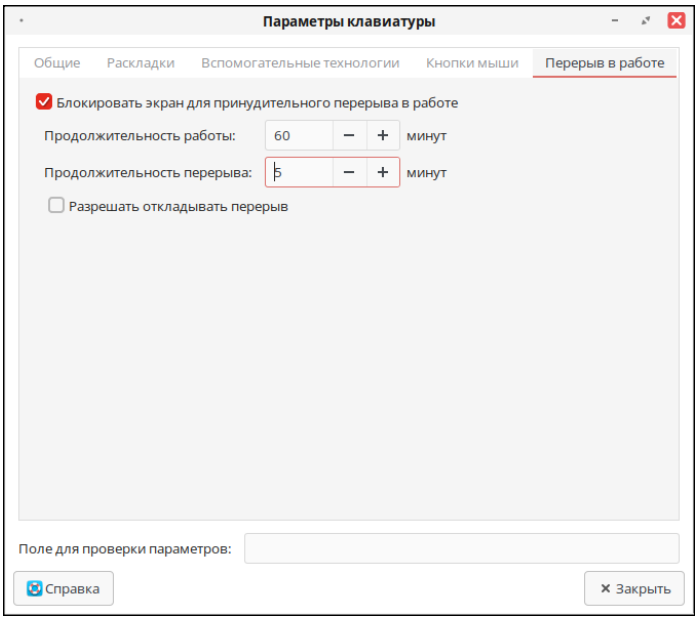
задается поведение залипающих клавиш, медленные нажатия и реагирование на кнопки мыши. Также можно настроить обратную звуковую связь, например, при активном **Caps Lock** и нажатии какой-либо клавиши будет подаваться звуковой сигнал.



На вкладке «Кнопки мыши» задается разрешение на управление курсором мыши с клавиатуры.



На вкладке «Перерыв в работе» можно задать продолжительность работы и перерыва. При достижении указанной продолжительности работы экран будет заблокирован.


Параметры клавиатуры
Общие
Раскладки
Вспомогательные технологии
Кнопки мыши
Перерыв в работе
Блокировать экран для принудительного перерыва в работе
Продолжительность работы:
60
минут
Продолжительность перерыва:
5
минут
Разрешать откладывать перерыв
Поле для проверки параметров:
Справка
Закрыть

Графическое окружение Cinnamon

Апплеты
Десклеты
Настройка фона рабочего стола
Настройки рабочего стола
Настройка системной панели
Настройка внешнего вида графического интерфейса РЕД ОС
Настройка шрифтов графического интерфейса РЕД ОС
Настройка хранителя экрана, блокировки и режима энергосбережения
Управление окнами графического интерфейса
Настройка рабочих областей
Настройка горячих углов
Работа с файловым менеджером
Настройка смены раскладки клавиатуры

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Cinnamon – графическое окружение рабочего стола, являющееся ответвлением от кодовой базы GNOME Shell.

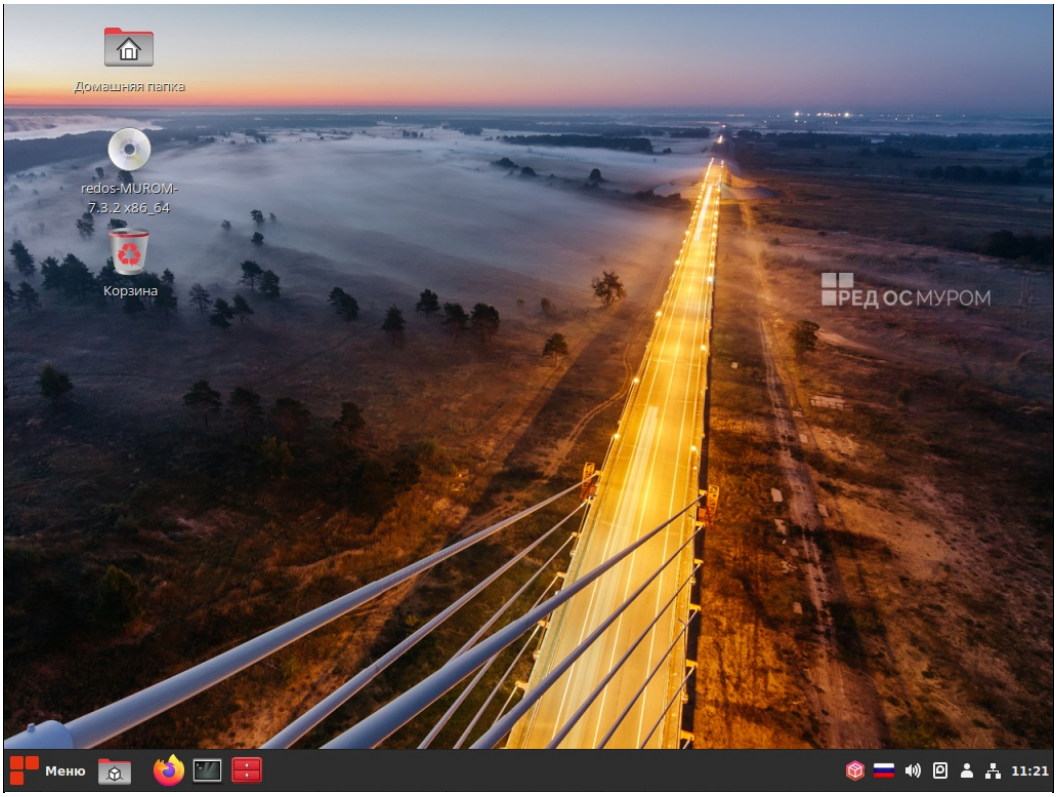
> **Примечание.**
>
> В РЕД ОС графическое окружение **Cinnamon** устанавливается дополнительно. Подробную информацию об установке можно посмотреть в нашей статье «Установка графической оболочки для ОС. Cinnamon».

Вы можете подробнее ознакомиться с возможностями графического окружения **Cinnamon**, просмотрев наши обучающие видео:

- на **RuTube** — Основы работы с DE Cinnamon;
- в **Яндекс.Дзен** — Основы работы с DE Cinnamon.

На наших каналах вы также сможете найти много другой полезной информации.

Графическое окружение **Cinnamon** выглядит следующим образом:



Главным элементом рабочего стола является системная панель, которая расположена в нижней части экрана и условно разделена на

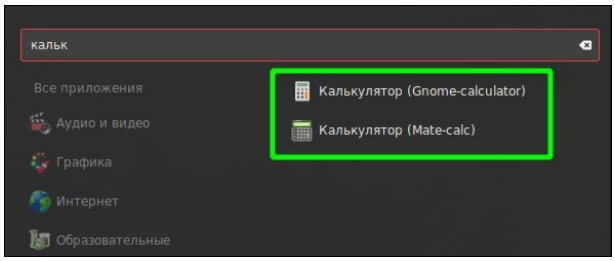
три основные части:

- Главное меню;
- Панель приложений;
- Панель апплетов.

Главное меню — представляет собой список установленных программ, разделенных на несколько категорий, таких как «Аудио и видео», «Графика», «Интернет», «Офис» и т. д.

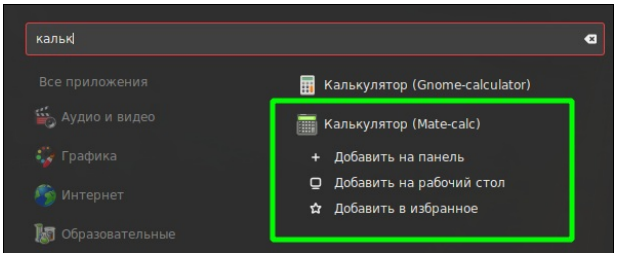


Поисковая строка здесь предназначена для поиска приложений. Начните вводить ключевое слово, чтобы получить список только тех компонентов меню, которые его содержат.



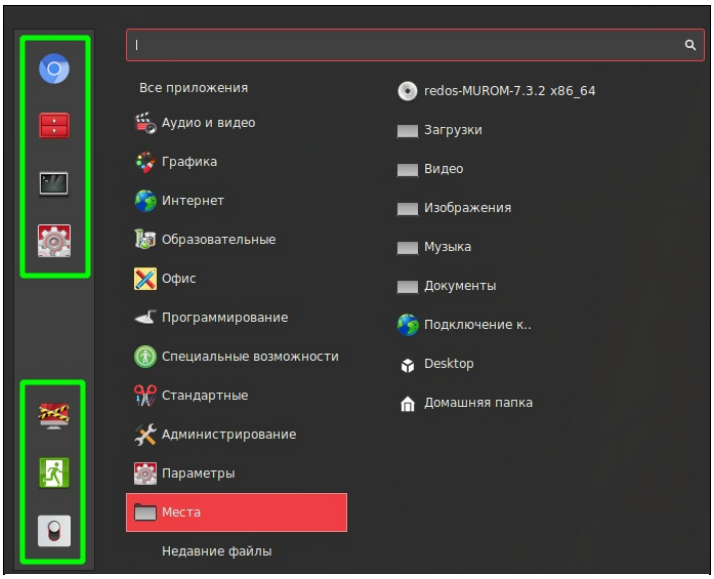
При нажатии ПКМ по какому-либо приложению можно выбрать несколько действий:

- добавить приложение на панель;
- добавить приложение на рабочий стол;
- добавить приложение в избранное.

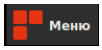
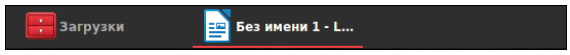


В избранном по умолчанию находятся веб-браузер **Chromium**, файловый менеджер **Nemo**, терминал и параметры системы.

Также здесь доступны кнопки блокировки экрана, выхода из сеанса и завершения работы.



Панель приложений представляет собой управляющую панель, которая по умолчанию располагается в нижней части экрана. Управляющая панель включает в себя следующие компоненты:

- кнопка Главного меню () ;
- область запуска приложений — Panel Launcher ();
- область открытых приложений — Window list ();
- область системных сообщений — Notifications ();
- системный лоток (трей) — System Tray, куда помещаются пиктограммы некоторых работающих в фоне приложений ();
- несколько пиктограмм разного назначения — модуль сетевых соединений, регулятор громкости, часы, индикатор раскладки клавиатуры и т. д. ().

Апплеты

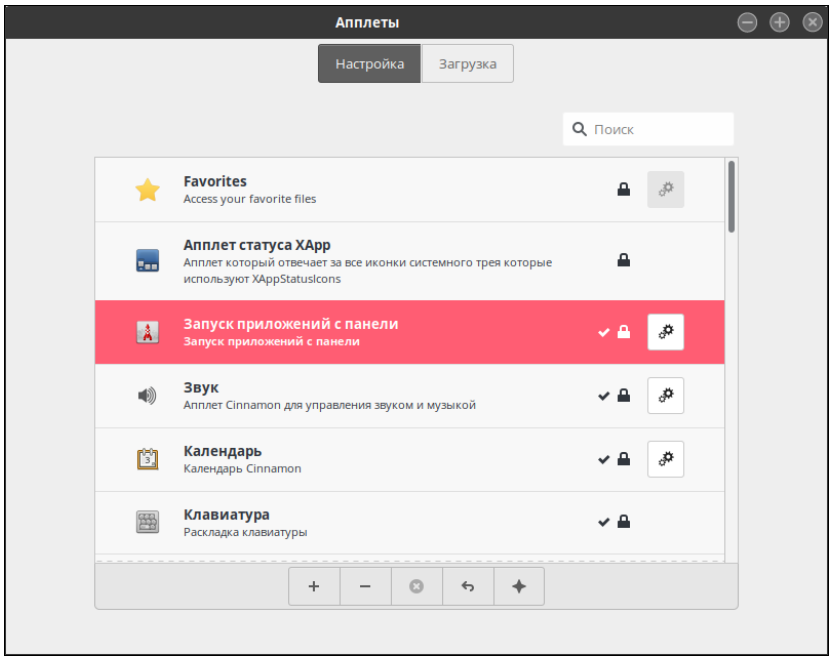
Все области и кнопки панели представляют собой так называемые **апплеты** – небольшие программы. Апплеты могут как добавляться на панель, так и удаляться с неё. Главное меню, системный лоток, менеджер сети, настройки пользователя — всё это апплеты.

Для добавления новых апплетов на панель или удаления ненужных нажмите ПКМ по системной панели и в появившемся контекстном меню выберите пункт «Апплеты».

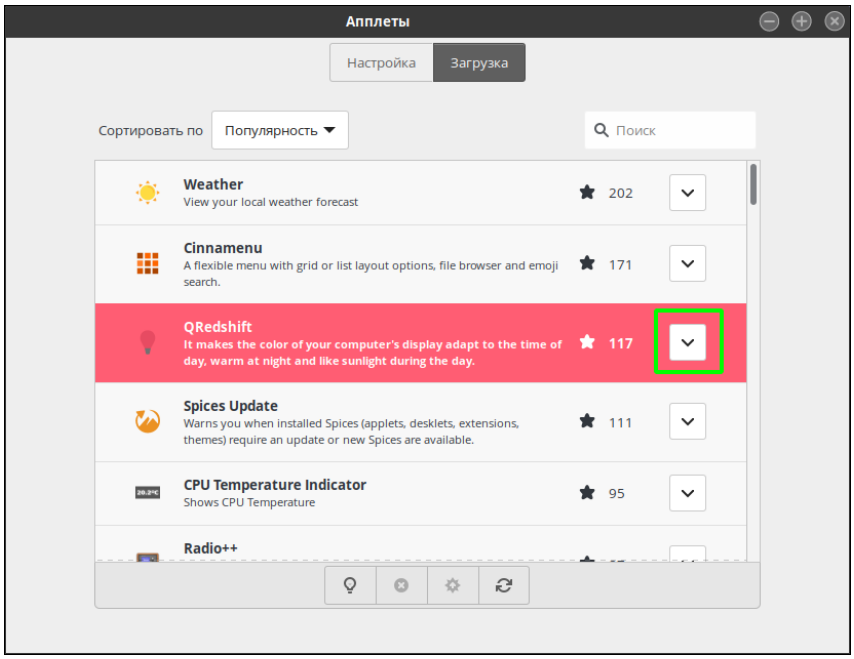
В открывшемся окне можно настроить или загрузить доступные апплеты.

На вкладке «Настройка» отображаются уже загруженные апплеты. При выборе какого-либо установленного апплета становится активной строка управления, с помощью которой можно:

- добавить апплет на рабочий стол ();
- удалить апплет с рабочего стола ();
- удалить апплет из загруженных ();
- удалить все апплеты ();
- просмотреть информацию об апплете ().

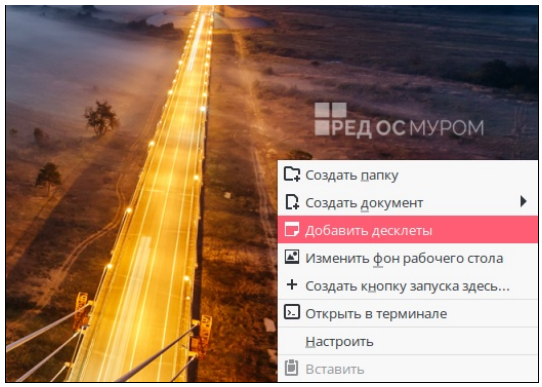


На вкладке «Загрузка» можно загрузить любой из доступных апплетов, а затем установить его. Для загрузки необходимо выбрать нужный апплет и нажать кнопку «Установить».



Десклеты

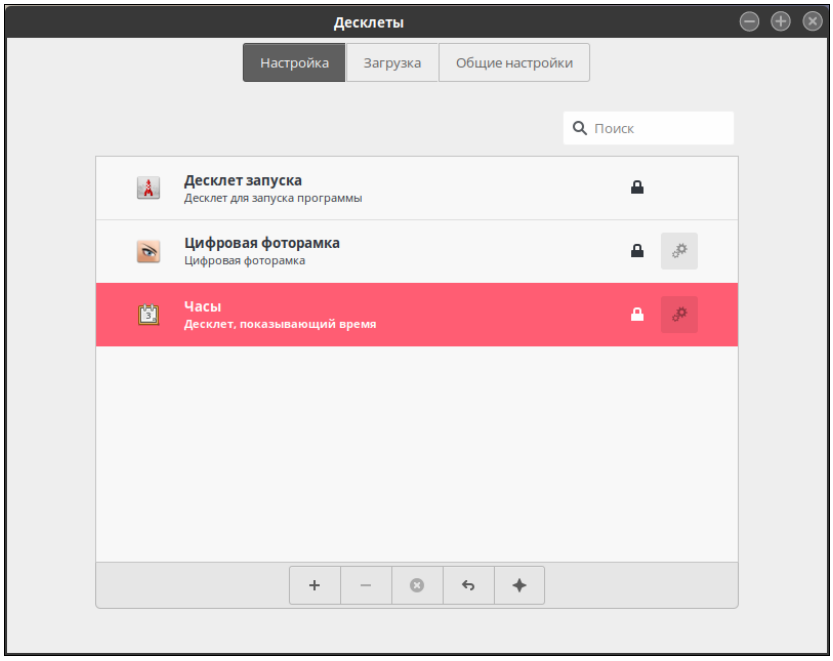
При нажатии ПКМ по рабочему столу будет открыто контекстное меню, в котором можно, например, добавить десклеты. Десклет — это название принято в Cinnamon для элементов, которые в других рабочих средах называют виджетами. В отличие от апплетов, которые встраиваются в панель рабочего стола, десклеты встраиваются непосредственно на рабочий стол.



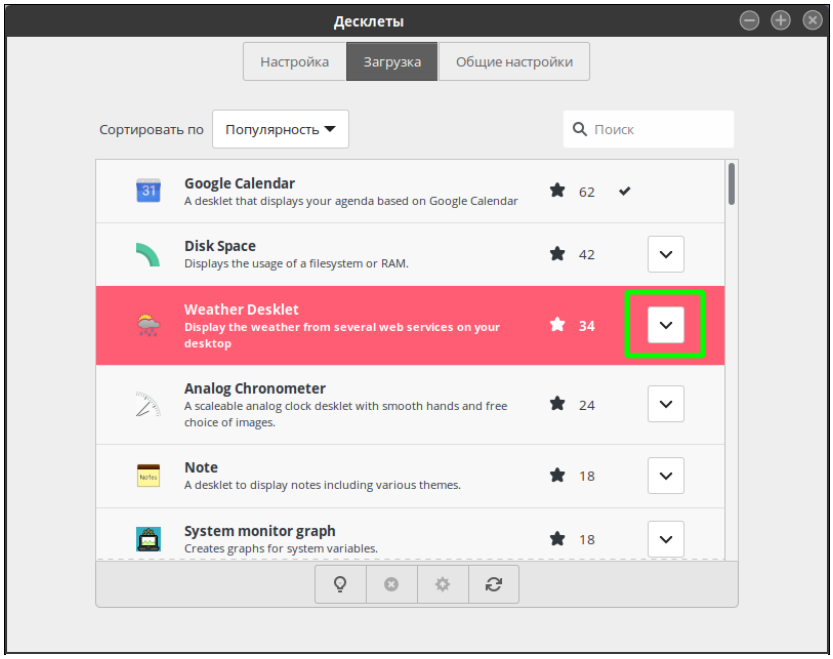
В открывшемся окне можно настроить и загрузить доступные десклеты.

На вкладке «Настройка» отображаются уже загруженные десклеты. При выборе какого-либо установленного декслета становится активной строка управления, с помощью которой можно:

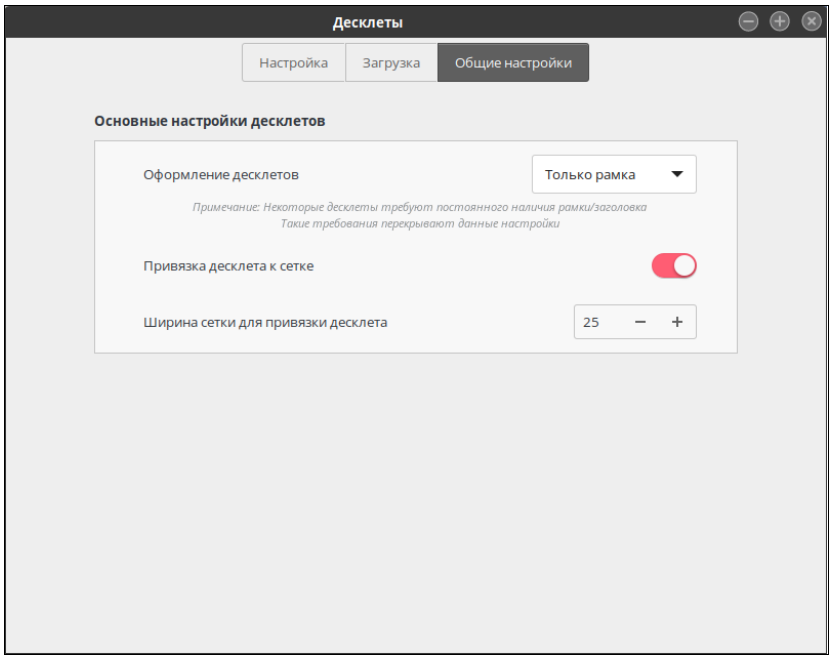
- добавить десклет на рабочий стол (+);
- удалить десклет с рабочего стола (−);
- удалить десклет из загруженных (⊗);
- удалить все десклеты (↩);
- просмотреть информацию о десклете (✦).



На вкладке «Загрузка» можно загрузить любой из доступных десклетов, а затем установить его. Для загрузки необходимо выбрать нужный десклет и нажать кнопку «Установить».



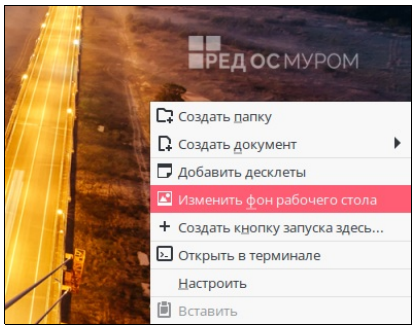
На вкладке «Общие настройки» можно выбрать оформление десклетов, установить привязку десклетов к сетке рабочего стола, а также указать ширину сетки.



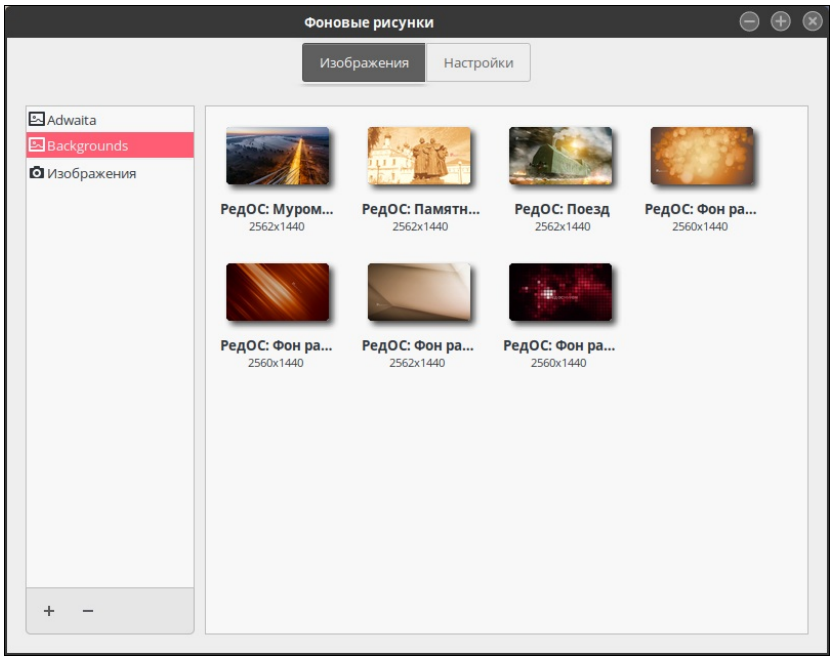
Настройка фона рабочего стола

Для смены изображения рабочего стола существует два варианта.

Вариант 1. Для смены фона рабочего стола необходимо в свободной части рабочего стола вызвать контекстное меню (нажав ПКМ). В открывшемся контекстном меню необходимо выбрать пункт «Изменить фон рабочего стола».

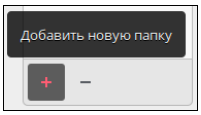


Вариант 2. Для смены фона рабочего стола необходимо в системной панели выбрать пункт «Меню» — «Параметры» — «Фоновые рисунки».

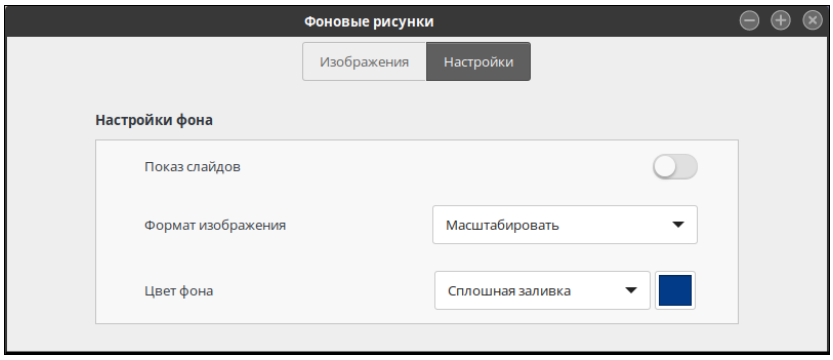


Можно также добавлять собственные изображения. Для этого нажмите на кнопку «Добавить новую папку» и выберите вашу папку с

фоновыми изображениями.

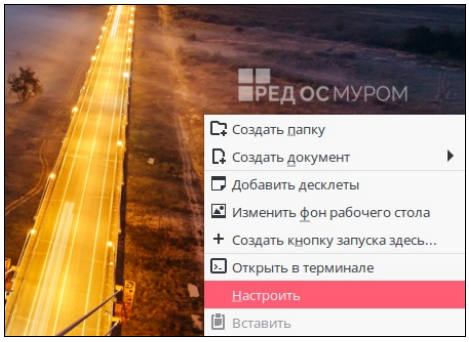


На вкладке «Настройки» можно задать показ слайдов, указать формат изображения и цвет фона.

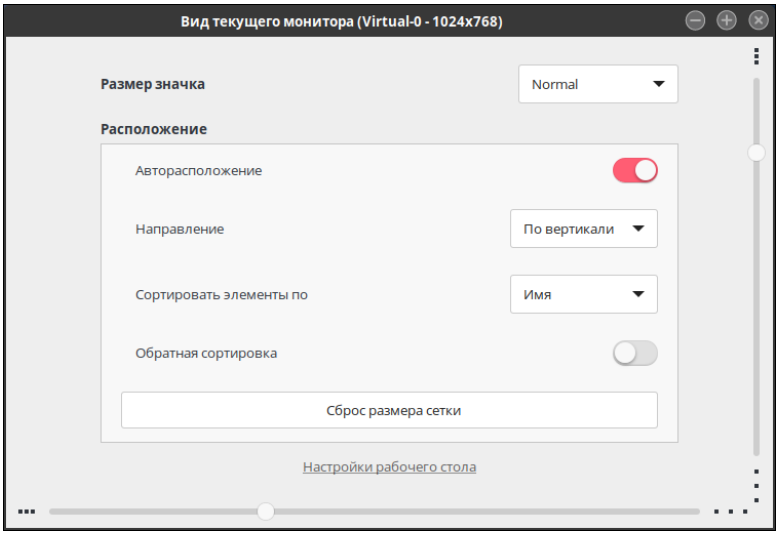


Настройки рабочего стола

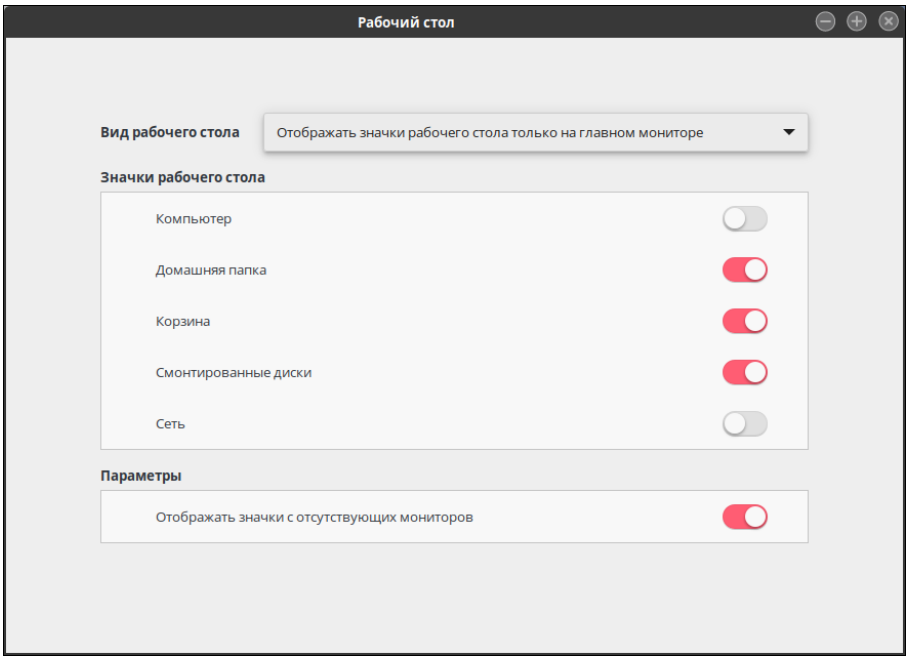
Для настройки внешнего вида элементов рабочего стола нажмите ПКМ по свободной части рабочего стола и в появившемся контекстном меню выберите «Настроить».



В открывшемся окне можно изменить размеры значков и их расположение. При выключении «Авторасположения» иконки рабочего стола можно будет перетаскивать в любое место. При включенном «Авторасположении» можно изменять направление расположения иконок (по горизонтали и по вертикали). Также доступно изменение типа сортировки, а также обратная сортировка.

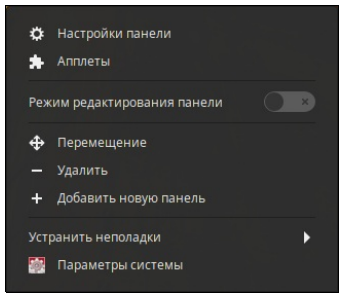


В нижней части окна присутствует кнопка «Настройки рабочего стола», где можно изменить отображение значков рабочего стола.

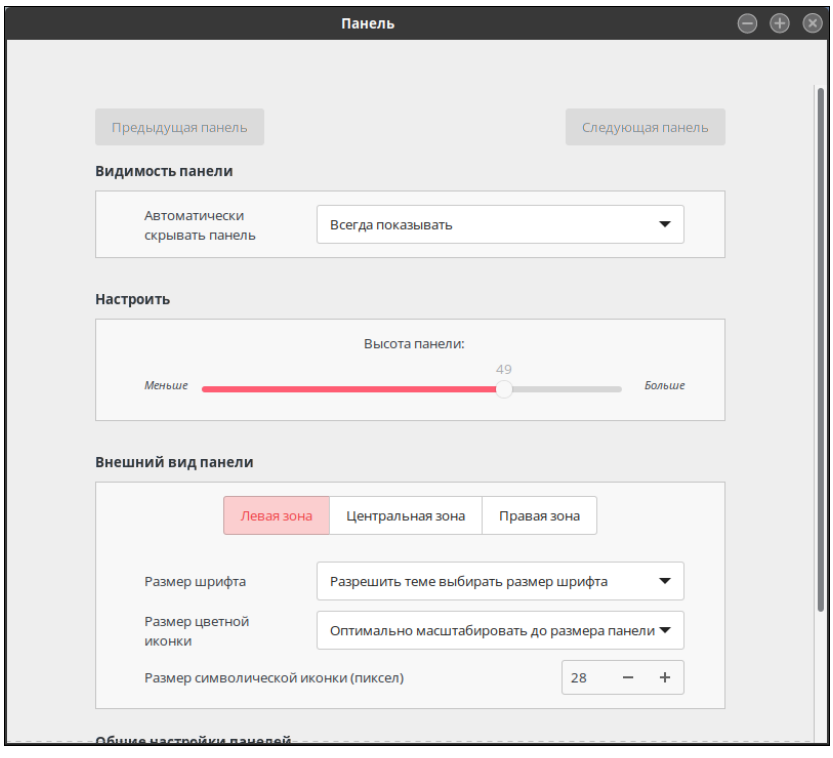


Настройка системной панели

Для изменения параметров панели задач графической оболочки РЕД ОС Cinnamon также нужно с помощью клика ПКМ по панели вызвать контекстное меню и выбрать нужный пункт меню.



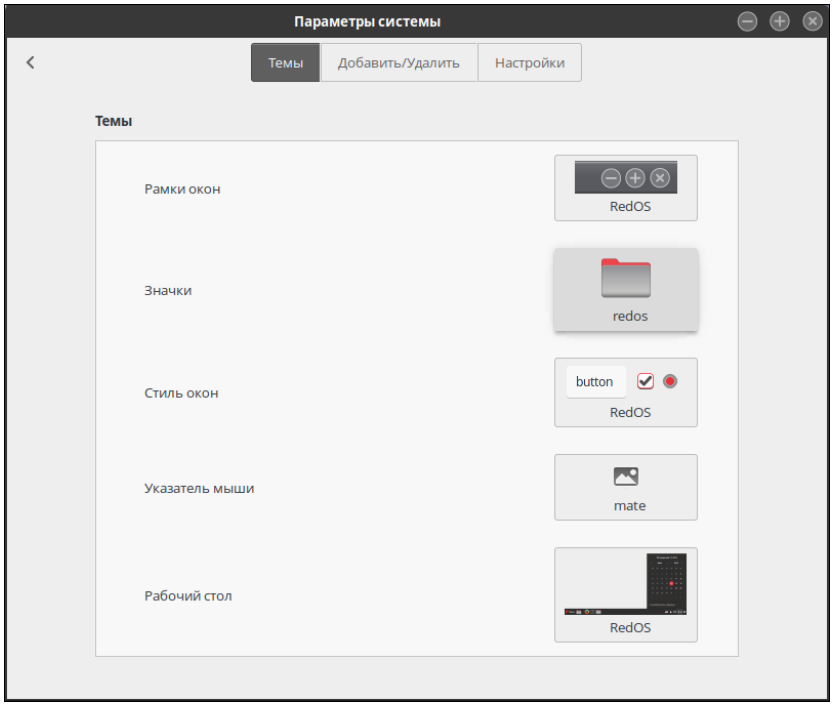
При выборе пункта меню «Настройки панели» будет открыто окно, в котором доступны такие настройки, как видимость панели, высота панели (в пикселях), внешний вид панели (шрифт, размер шрифта, размеры иконок приложений), а также общие настройки — добавление новых панелей, включение режима редактирования панели, а также возможность пропуска курсора мыши через границы панелей.



При выборе пункта меню «Режим редактирования панели» появляется возможность изменить положение (очередность) уже добавленных на панель апплетов.

Настройка внешнего вида графического интерфейса РЕД ОС

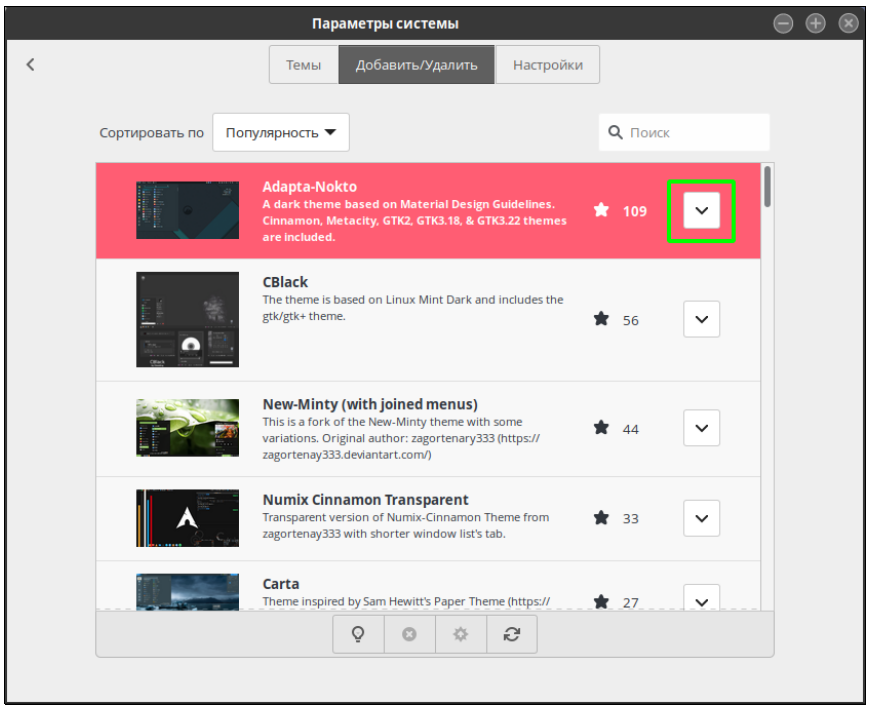
Для смены внешнего вида окон графической оболочки РЕД ОС пользователю необходимо в системной панели выбрать пункт меню «Параметры системы» и в разделе «Внешний вид» выбрать «Темы».



Здесь можно задать стилевое оформление отдельных элементов интерфейса полностью независимое друг от друга и от темы рабочего стола.

Большое количество доступных вариантов позволяют комбинировать элементы оформления интерфейса в широких пределах, достигая максимального визуального эффекта. Это имеет практическое значение, особенно для людей с плохим зрением или нарушением цветовосприятия.

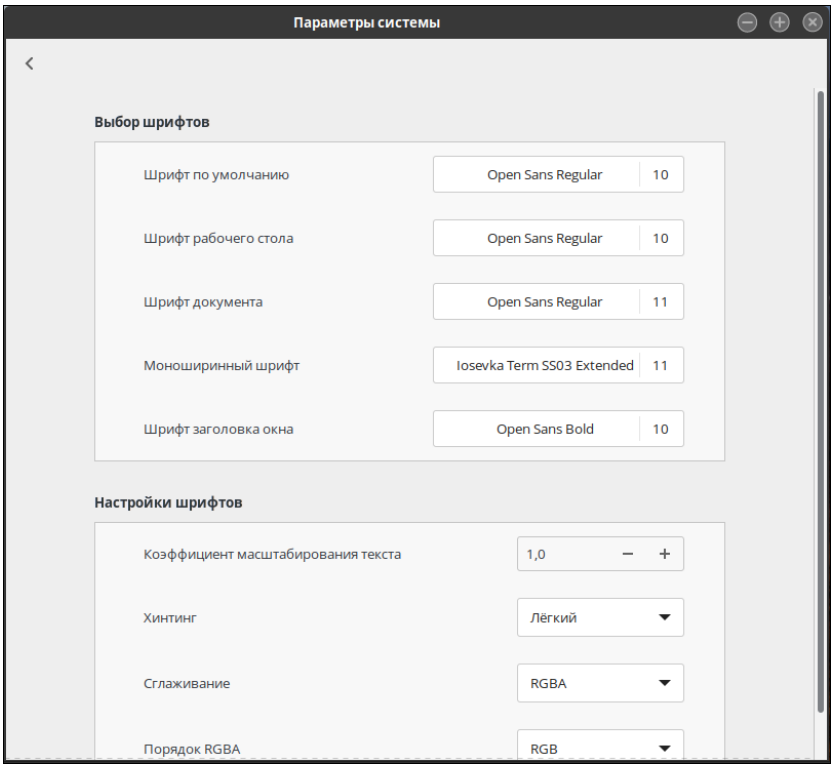
Можно также обратиться к коллекции тем, доступных на вкладке «Добавить/Удалить». Для установки понравившейся темы нажмите «Установить».



Настройка шрифтов графического интерфейса РЕД ОС

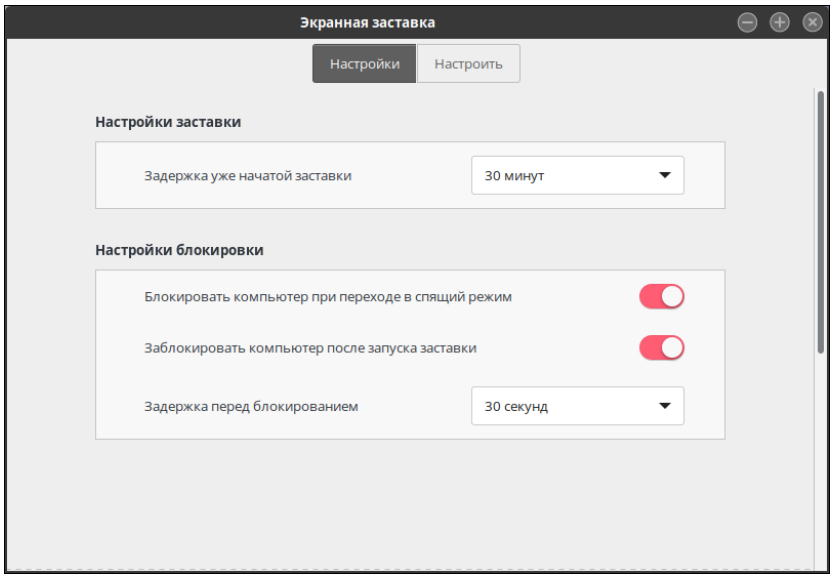
Для изменения используемых шрифтов графической оболочки РЕД ОС пользователю необходимо в системной панели выбрать пункт меню «Параметры системы» и в разделе «Внешний вид» открыть «Выбор шрифтов».

В окне можно настроить шрифты как для заголовков окон, так и для документов.



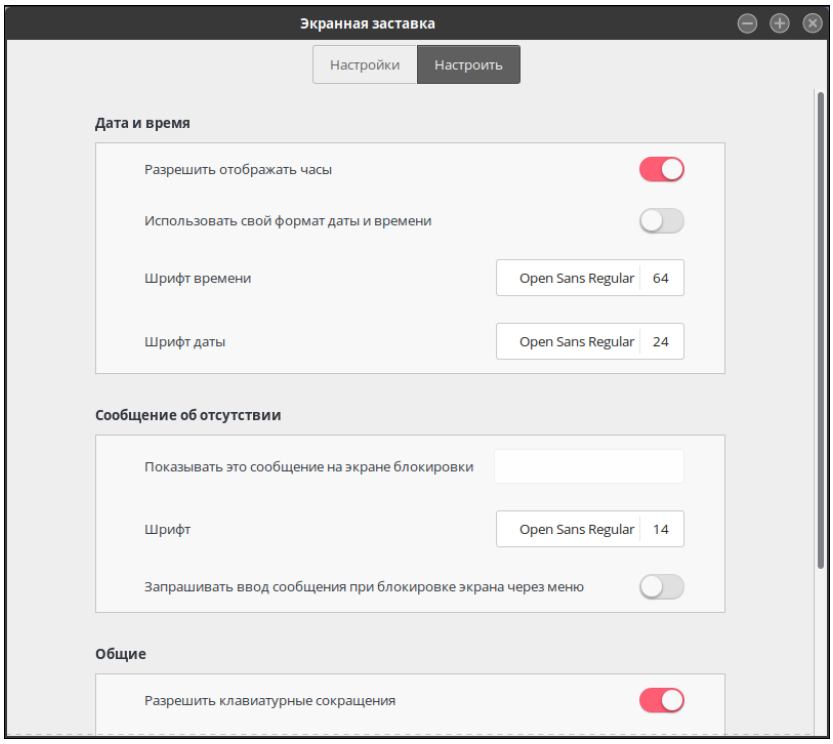
Настройка хранителя экрана, блокировки и режима энергосбережения

Настройка времени блокировки рабочего стола, настройка хранителя экрана, а также управление режимом энергосбережения определяется утилитой «Экранная заставка». Данная утилита находится в «Главном меню» - «Параметры».



Утилита позволяет пользователю определить время, по истечении которого, при бездействии пользователя, рабочий стол системы будет заблокирован, выбрать графический хранитель экрана и определить режимы управления питанием.

На вкладке «Настроить» доступны более тонкие настройки, например, отображение даты и времени на экране заставки, установка сообщения об отсутствии или просто произвольного текста, выбор шрифта и его размера, а также клавиатурные сокращения, управление медиапроигрывателем, показ обложки альбома, отображение информационной панели и возможность перемещения виджетов.



Управление окнами графического интерфейса

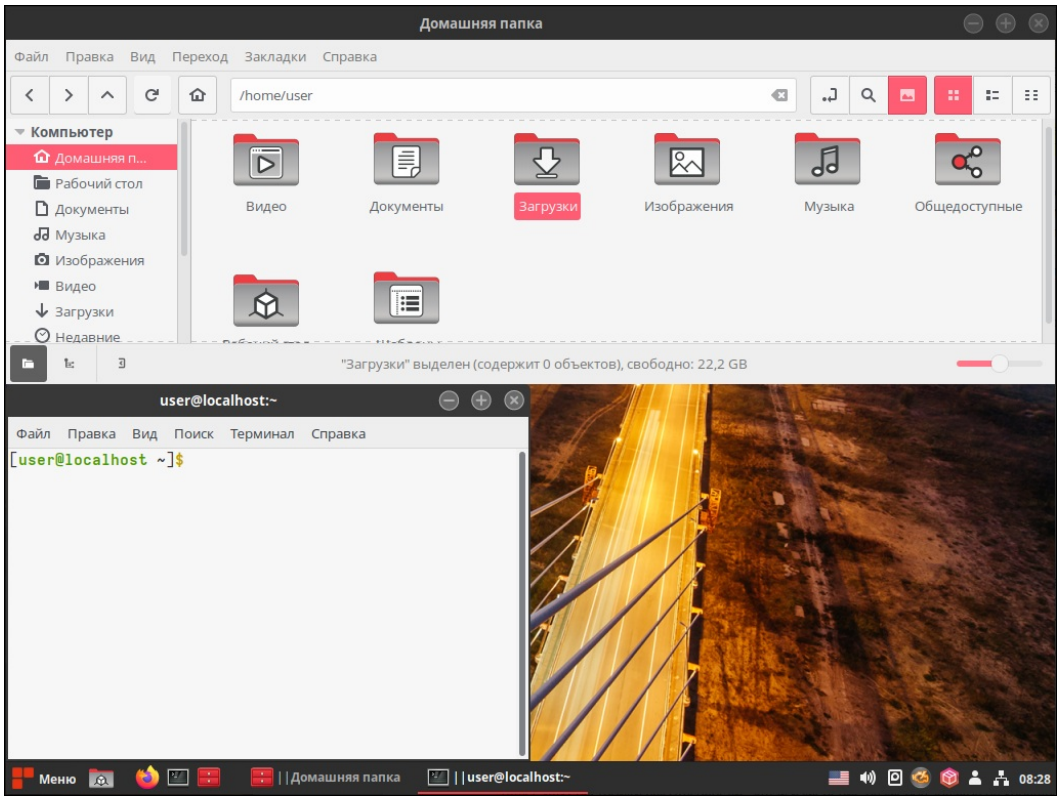
Управление окнами подразумевает в первую очередь переключение между ними. Универсальный способ переключения между окнами, существующий во всех графических средах, – комбинация клавиш **Alt+Tab**. Т.к. использование комбинации клавиш **Alt+Tab** является универсальным, далее будет рассмотрен вариант тайлинга окон.

Тайлинг - привязка окна к какой-либо части окна.

Тайлинг окон может выполняться двумя способами – посредством мыши и с помощью клавиатуры.

При перетаскивании окна мышью к верхней границе экрана оно занимает верхнюю его половину. Аналогичное движение к нижней границе экрана разворачивает окно на нижнюю его половину. Перемещение окна к боковой стороне экрана (левой или правой) прикрепляет его на левую или правую половины, в зависимости от стороны перетаскивания.

Если передвинуть окно в любой из углов дисплея, оно займёт соответствующую его четверть.



Тайлинг с клавиатуры осуществляется при помощи комбинации клавиш **Super** (левая Win) и одной из стрелок управления курсором.

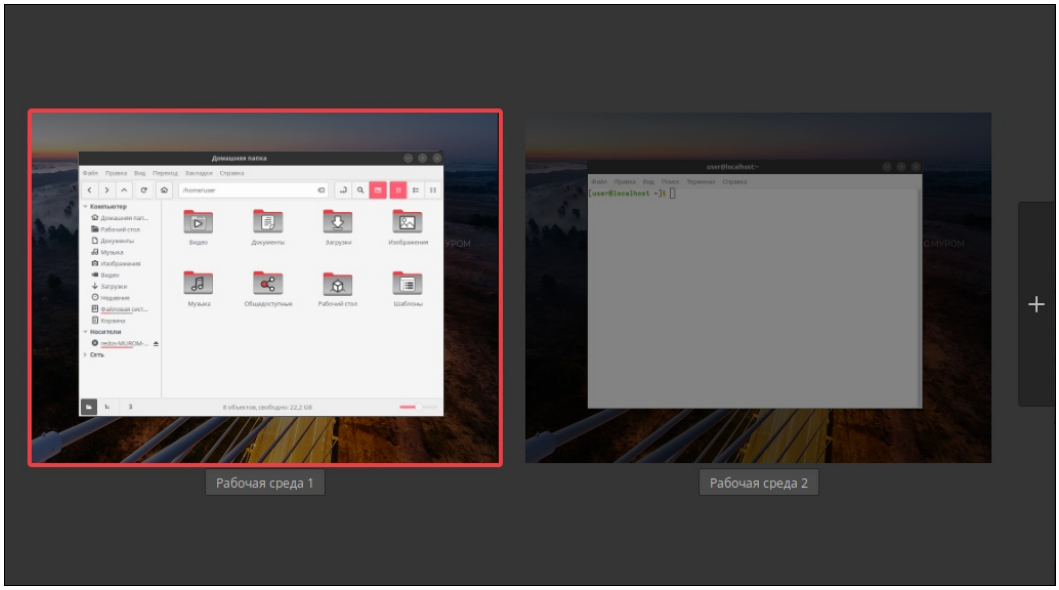
Комбинация **Super+Up** развернёт окно на верхнюю половину экрана, **Super+Down** – вернёт окно в исходное состояние. Из положения «половинка снизу» комбинация Super+Left превратит окно в «четвертинку» в левом нижнем углу, **Super+Right** – в «четвертинку» в правом нижнем углу.

Существует еще одна полезная функция окон. Для ее использования перейдите в «Главное меню» — «Параметры» — «Окна», в открывшемся окне в пункте «Действие при прокрутке на заголовке колеса мыши» активируйте опцию «Настройка прозрачности». Теперь при открытии окна поверх другого наведите мышь на заголовок и покрутите колесо мыши — верхнее окно станет полупрозрачным.

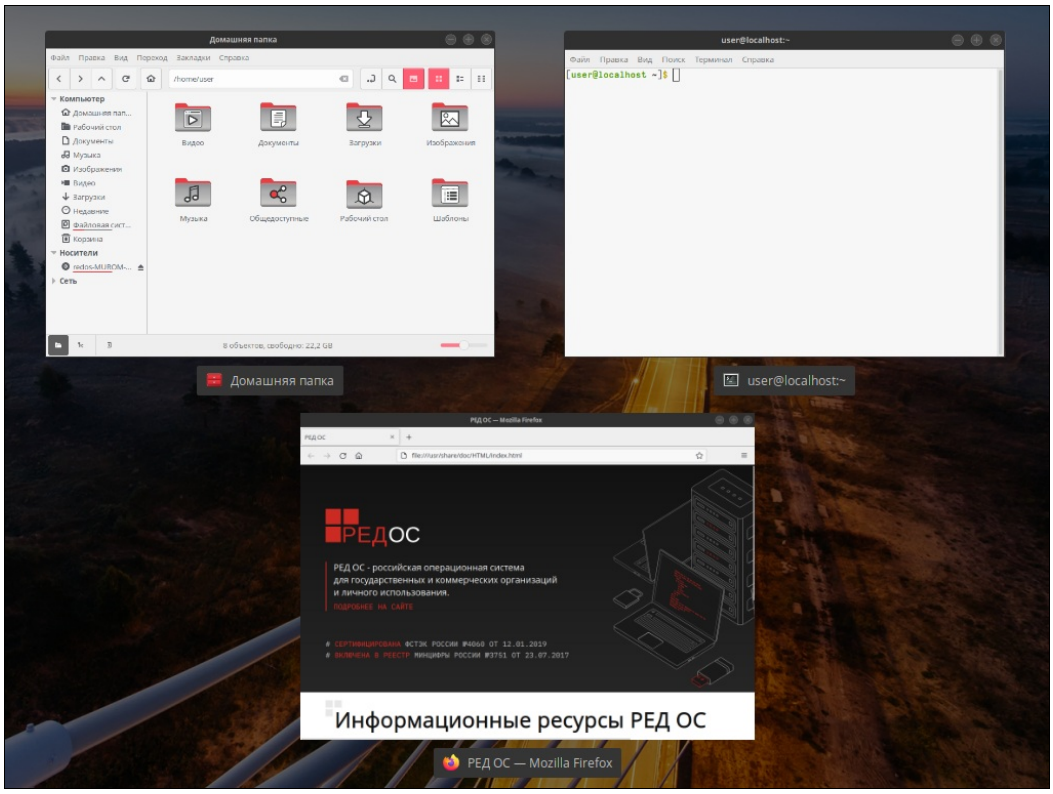
Благодаря такой функции можно смотреть обучающие видео в браузере и выполнять команды в открытом окне терминала, не переключаясь при этом между окнами.

Настройка рабочих областей

В **Cinnamon** есть множественные рабочие пространства, которые называются "workspaces". При нажатии клавиш **Ctrl+Alt+Up** (стрелка вверх) на экран выводятся все доступные рабочие области. Здесь можно легко переключиться на необходимую рабочую область, а также добавить новую. Для быстрого переключения между областями воспользуйтесь клавишами **Ctrl+Alt + Right** (стрелка вправо) или **Left** (стрелка влево).



Задействована и противоположная комбинация — **Ctrl+Alt+Down** (стрелка вниз), которая переводит **Cinnamon** в режим, который можно назвать экспонированием окон (или режимом масштабирования) - одновременный вывод всех окон открытых приложений текущей рабочей области, в том числе и свёрнутых.

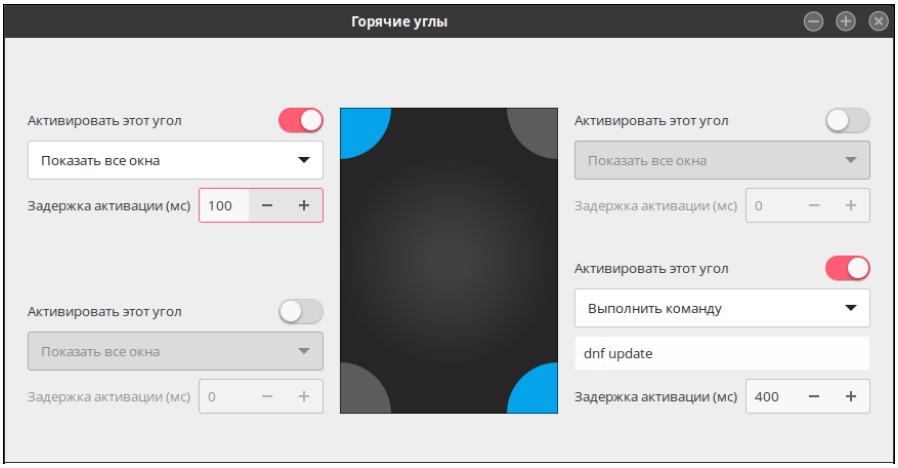


При необходимости можно сменить название рабочей области.

Настройка горячих углов

Следующая немаловажная и удобная функция – это горячие углы. Настройка доступна из «Главного меню» - «Параметры» - «Горячие углы», необходимо выбрать и активировать нужный угол и определить для него действие.

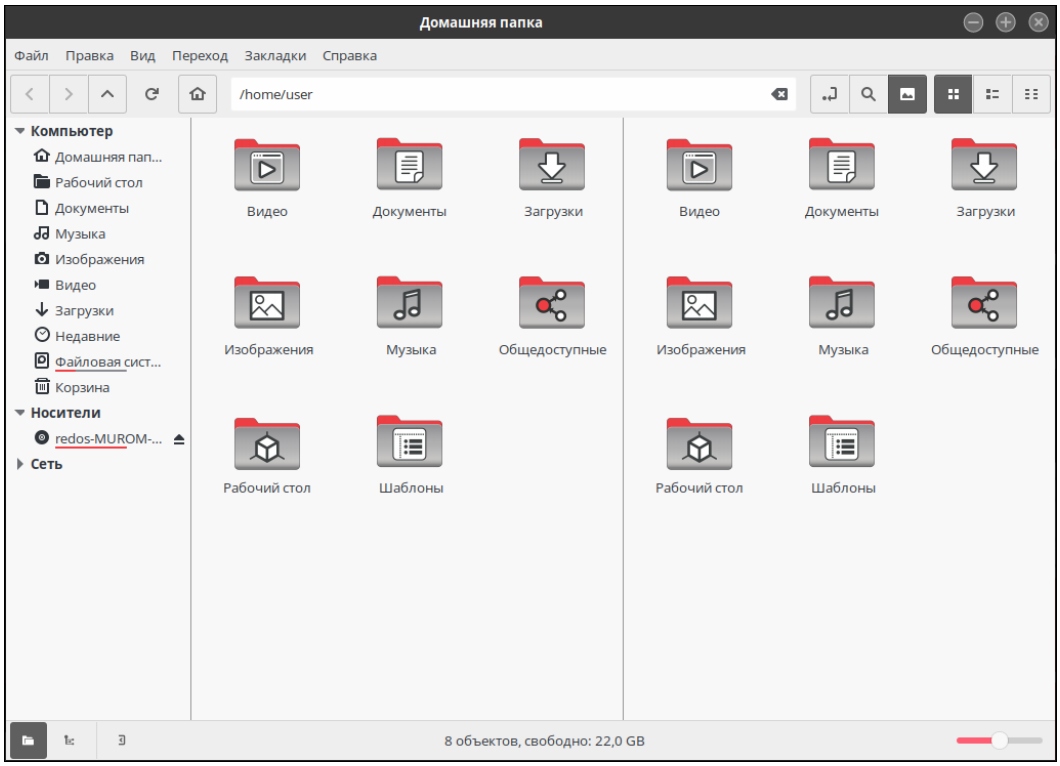
Действия выполняются при наведении курсора мыши на соответствующий угол. Повторное перемещение курсора в тот же угол возвращает **Cinnamon** в нормальный рабочий режим. Также можно добавить время задержки активации действия.



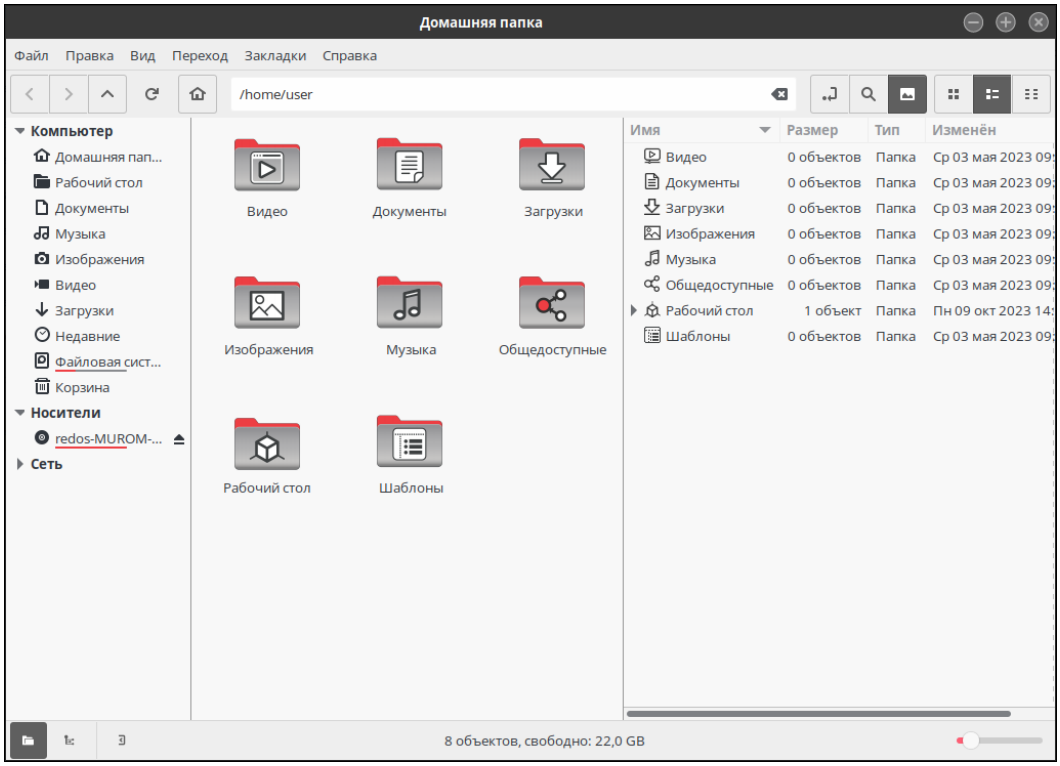
Работа с файловым менеджером

По умолчанию в **Cinnamon** используется файловый менеджер **Nemo**. Далее будут рассмотрены некоторые основные возможности файлового менеджера.

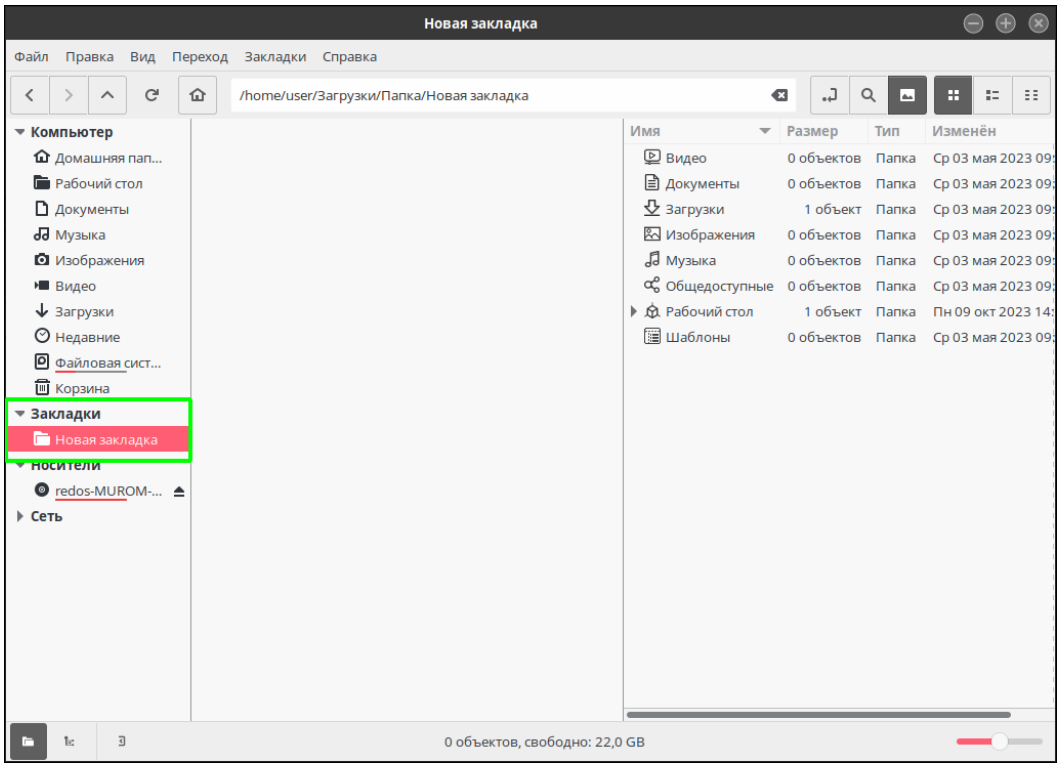
При нажатии клавиши **F3** можно разделить рабочую зону на две части.



При помощи сочетания клавиш **Ctrl+1**, **Ctrl+2**, **Ctrl+3** можно изменить вид отображения каталогов и файлов — значки, список или компактный вид.



Через пункт панели инструментов «Закладки» можно создавать новые закладки, прикреплять новые каталоги в быстрый доступ и т.д.



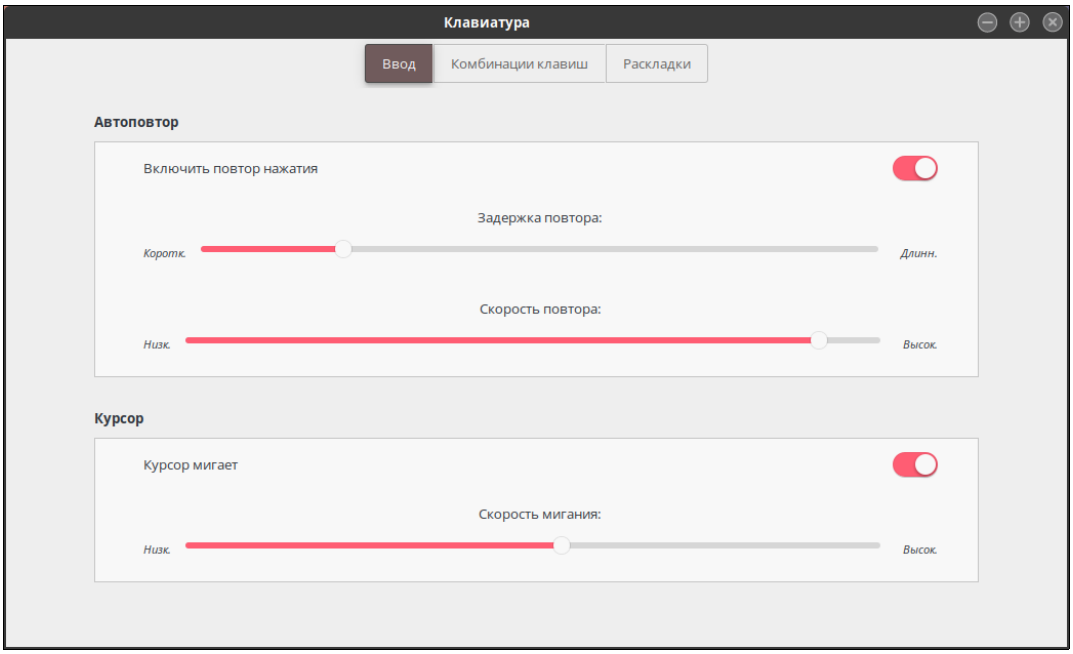
Также есть множество других настроек, которые позволят комфортно работать. **Nemo** предоставляет большинство возможностей, которые обычно ожидаются от современного файлового менеджера.

В других рабочих средах при изменении настроек обычно требуется перезапуск сеанса — с закрытием окон и запущенных приложений. В Cinnamon изменение настроек среды обычно вступает в силу сразу, однако если для применения изменений необходим перезапуск, можно использовать комбинацию клавиш **Alt+Ctrl+Esc** — новые настройки вступят в силу при сохранении всего текущего окружения.

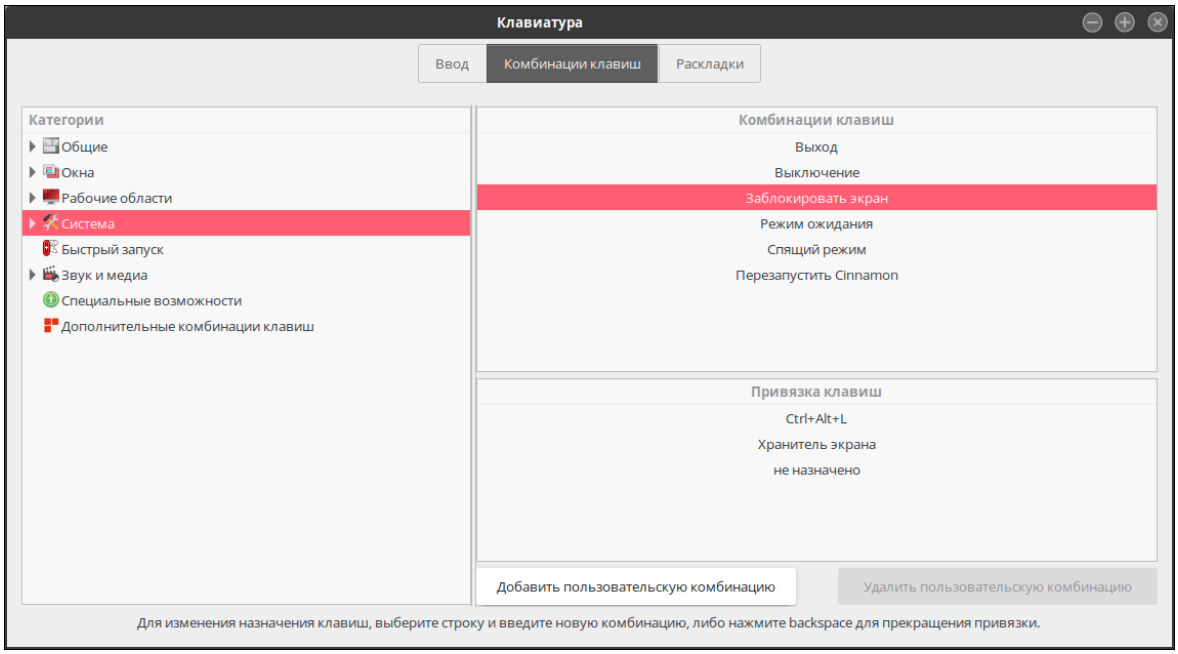
Настройка смены раскладки клавиатуры

В РЕД ОС по умолчанию смена раскладки клавиатуры (языка ввода) осуществляется при одновременном нажатии функциональных клавиш клавиатуры **Shift+Alt** одновременно. Для изменения сочетания функциональных клавиш, применяемых для смены раскладки клавиатуры, необходимо в системной панели перейти в «Главное меню» - «Параметры» - «Клавиатура».

На вкладке «Ввод» задается автоповтор нажатых клавиш и скорость мигания курсора в полях ввода.

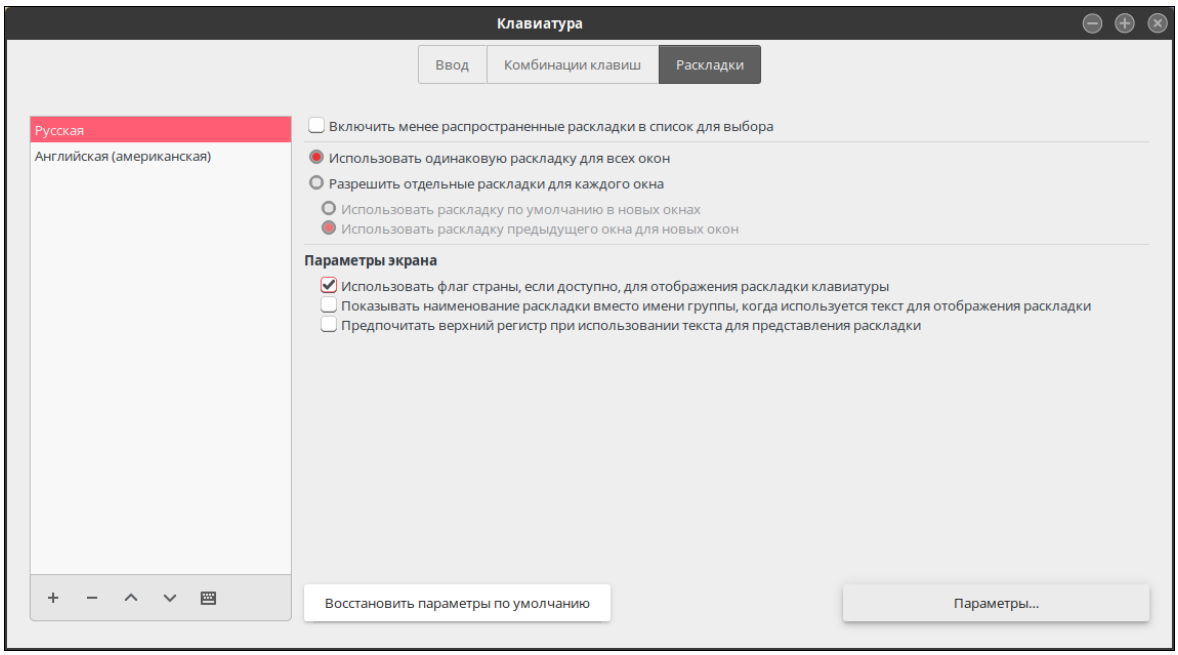


На вкладке «Комбинации клавиш» можно посмотреть заданный по умолчанию комбинации клавиш для тех или иных действий, а также назначить собственные.

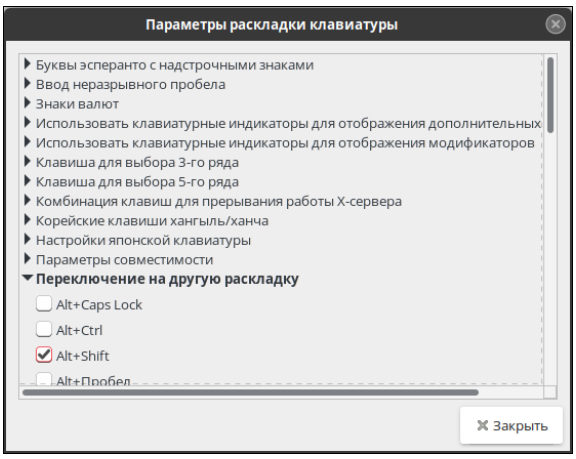


На вкладке «Раскладки» можно добавить новые языки, переместить выбранную раскладку выше или ниже в списке, удалить ненужную раскладку.

Дополнительно можно определить раскладки клавиатуры для других рабочих областей, а также задать отображение раскладки в трее.



При нажатии на кнопку «Параметры...» можно изменить сочетания клавиш клавиатуры по умолчанию.



Оконный менеджер Openbox

Установка openbox
Настройка openbox
Файл rc.xml
Файл menu.xml
Автозапуск приложений
Файл environment
Настройка тем (внешнего оформления)
Применение настроек
Настройка сочетания клавиш
Добавление панелей

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openbox-3.6.1-10

Openbox – это легкий и настраиваемый оконный менеджер, который предоставляет пользователю максимальную гибкость в управлении окнами на экране.

Openbox можно использовать как отдельный оконный менеджер или в качестве замены стандартного оконного менеджера своей среды рабочего стола. Он обеспечивает достаточную функциональность для работы на его основе, но также позволяет настроить большую часть своих функций и использовать плагины для улучшения его возможностей.

Основные возможности **Openbox** включают:

- настраиваемые горячие клавиши (клавиши быстрого доступа);
- поддержку декоративных элементов окон, включая кнопки закрытия и переключения виртуальных рабочих столов;
- поддержку управления окнами с помощью мыши;
- DAO-режим, который позволяет управлять поведением окон при открытии приложений;
- поддержку стандартов среды рабочего стола (**KDE**, **Xfce**).

К основным настройкам относятся:

- настройка переключения окон с помощью мыши или клавиатуры;
- настройка внешнего вида границ окон и их декорирование;
- настройка горячих клавиш для быстрого запуска приложений или выполнения команд;
- настройка виртуальных рабочих столов для организации рабочего пространства;
- установка и использование плагинов для расширения функциональности оконного менеджера.

Openbox имеет довольно простой и интуитивно понятный интерфейс, который делает его удобным для использования как начинающими, так и опытными пользователями.

Установка openbox

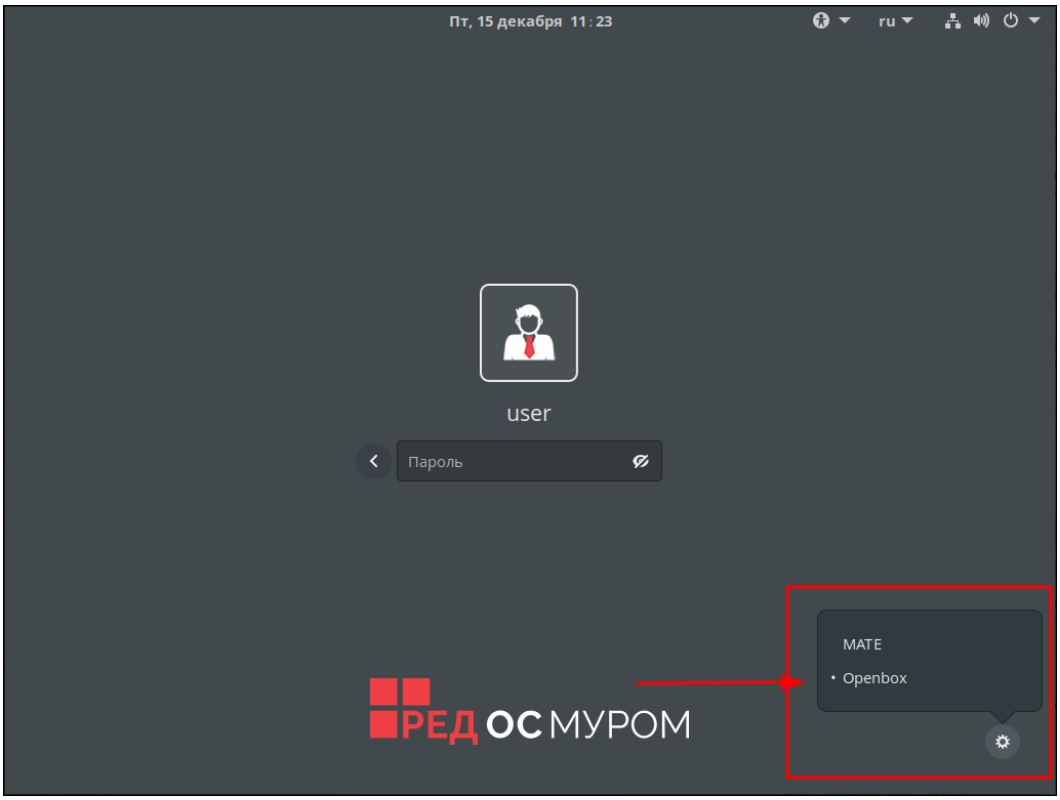
Для установки **openbox** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install openbox
```

Для загрузки в новом оконном менеджере необходимо выйти из текущего сеанса пользователя, выбрав в «**Главном меню**» пункт «**Завершить текущий сеанс**» – «**Завершить сеанс**». Затем в окне выбора пользователей выберите нужного пользователя, в правом нижнем углу нажмите на значок шестеренки и выберите из списка **Openbox**, введите пароль пользователя и авторизуйтесь в системе.



После запуска будет отображаться просто серый экран. Нажмите правую кнопку мыши по экрану — это вызовет меню **Openbox** и продемонстрирует, что всё успешно запустилось и работает.

Настройка openbox

> **Примечание.**
>
> Локальные файлы конфигурации имеют приоритет выше, чем глобальные.

Основу конфигурации openbox составляют четыре конфигурационных файла, каждый из которых выполняет свою роль: **rc.xml**, **menu.xml**, **autostart** и **environment**.

Перед настройкой рекомендуется создать локальный профиль **openbox** (специфичный для вашей учётной записи). Это можно сделать путём копирования глобального профиля **/etc/xdg/openbox** (который применяется для всех пользователей) в свой каталог настроек:

```
mkdir -p ~/.config/openbox
cp -a /etc/xdg/openbox/ ~/.config/
```

Файл rc.xml

> **Примечание.**
>
> Пользовательские сочетания клавиш должны добавляться в раздел `<keyboard>` этого файла и под заголовком `<!-- Keybindings for running aplications -->`

~/.config/openbox/rc.xml — это основной файл конфигурации, отвечающий за определение поведения и настроек всего сеанса, в том числе:

- сочетания клавиш (например, запуск приложений, регулировка громкости);
- темы оформления;
- настройки рабочего стола и виртуального рабочего стола;
- настройки окна приложения.

Файл имеет прописанные настройки по умолчанию, поэтому достаточно добавить необходимые изменения в соответствии с личными предпочтениями.

Примечание.

Настройки для каждого приложения, относящиеся к фиксированному размещению приложений на мониторе, будут работать только в том случае, если также были определены положения *x* и *y*.

Файл menu.xml

~/.config/openbox/menu.xml определяет поведение меню, открывающегося по нажатии ПКМ по рабочему столу. По умолчанию предоставляется статическое меню (которое не обновляется автоматически при установке новых приложений), но можно также использовать динамическое меню, которое будет обновляться автоматически.

Автозапуск приложений

openbox-session имеет два механизма автозапуска:

- **XDG Autostart** – работает, если установлен пакет **python-pyxdg**;
- свой собственный механизм.

Собственный механизм:

- считывает переменные из **/etc/xdg/openbox/environment**;
- считывает переменные из **~/.config/openbox/environment**;
- запускает **/etc/xdg/openbox/autostart**;
- запускает **~/.config/openbox/autostart**.

При возникновении проблем, связанных с выполнением команд в **~/.config/openbox/autostart** (команды выполняются не последовательно или наблюдается пропуск выполнения некоторых команд), рекомендуется добавить небольшие задержки. Например:

```
xset -b
(sleep 3s && nm-applet) &
(sleep 3s && conky) &
```

Файл environment

Файл **~/.config/openbox/environment** можно использовать для добавления связанных переменных окружения, например:

- определить новые пути при выполнении команд, которые требуют указания абсолютных путей до файлов;
- изменить языковые настройки;
- определить другие переменные, которые будут использоваться (например, здесь можно указать исправление для тем **GTK**).

Настройка тем (внешнего оформления)

Примечание.

Рекомендуется скопировать тему в домашний каталог пользователя вместо того, чтобы редактировать её напрямую в /usr/share/themes/. Это позволит оставить оригинал нетронутым, а также не удалит внесенные изменения при обновлении пакетов.

Стандартной утилитой для настройки внешнего вида **openbox** является **obconf**.

Для её установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install obconf
```

Запуск утилиты доступен из «**Меню**» – «**Preferences**» – «**Менеджер настройки Openbox**».

В менеджере можно изменить тему интерфейса, шрифты, размеры окон и пр.

Применение настроек

Openbox не всегда автоматически применяет изменения, внесённые в его файлы конфигурации в течение сеанса. Как следствие, необходимо вручную перезагрузить эти файлы после того, как они были изменены. Для этого выполните следующую команду:

```
openbox --reconfigure
```

Настройка сочетания клавиш

Все сочетания клавиш добавляются в файл **~/.config/openbox/rc.xml** под заголовком `<!-- Keybindings for running aplications -->`.

Для добавления собственных сочетаний клавиш откройте конфигурационный файл **rc.xml** с помощью команды:

```
nano ~/.config/openbox/rc.xml
```

и в конец файла добавьте следующие строки:

- для добавления сочетания клавиш:

```
<keybind key="новое_сочетание_клавиш">
  <action name="новое_действие">
    ...
  </action>
 </keybind>
```

- для выполнения внешней команды (используется действие execute):

```
<keybind key="новое_сочетание_клавиш">
  <action name="Execute">
    <command>новая_команда</command>
  </action>
 </keybind>
```

Добавление панелей

Openbox не содержит панелей, но их можно установить самостоятельно, например, с помощью утилиты **tint2**.

Для установки утилиты перейдите в сеанс пользователя **root**:

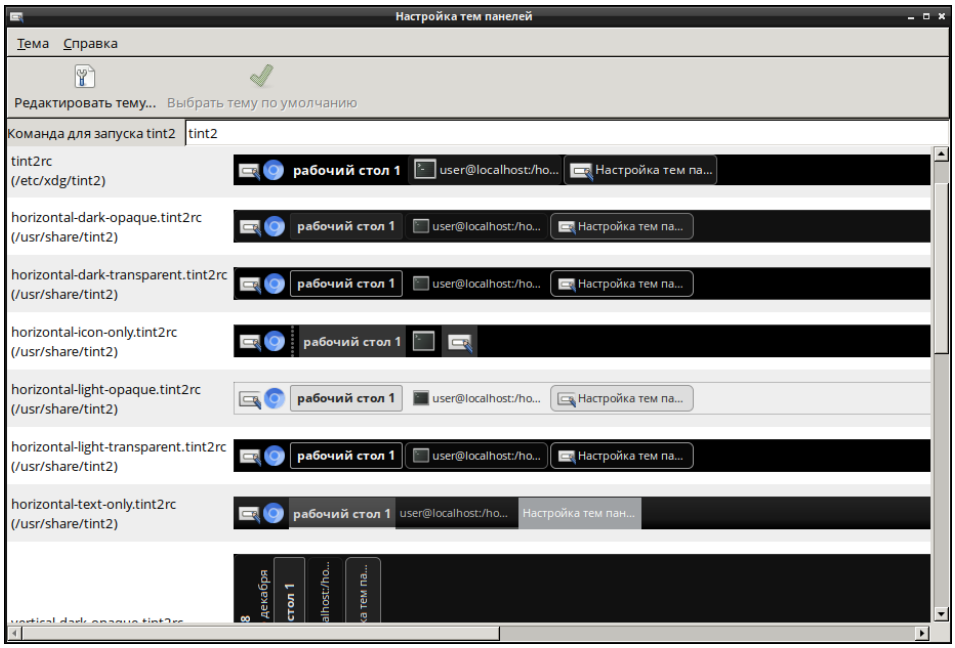
```
su -
```

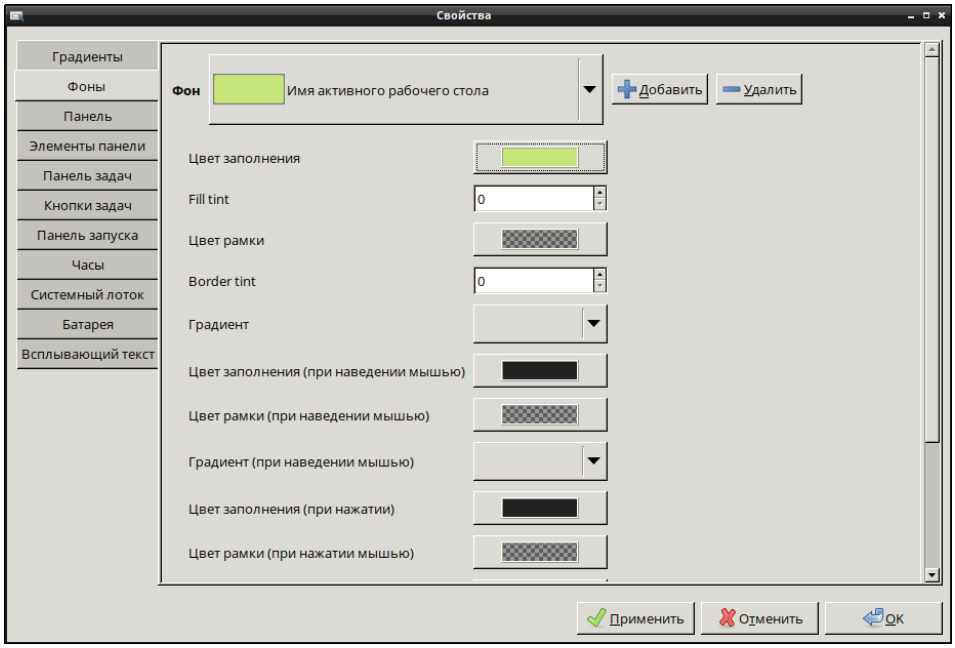
и выполните команду:

```
dnf install tint2
```

Запуск утилиты доступен из «**Меню**» – «**Preferences**» – «**Настройки tint2**».

Далее можно выбрать любую подходящую тему и редактировать её при необходимости.





Для применения изменений необходимо в файле конфигурации **~/.config/openbox/autostart** указать **tint2**:

```
nano ~/.config/openbox/autostart
```

```
tint2 &
```

а затем перезагрузить систему:

```
reboot
```

Установка графической оболочки в РЕД ОС 7.3

Mate
Cinnamon
Дополнительные пакеты для X-сервера
Графический режим работы
Удаление графической оболочки

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический

Вы можете подробнее ознакомиться с информацией по установке графических оболочек, просмотрев наши обучающие видео:

- на **RuTube** — Установка дополнительного графического окружения;
- в **Яндекс.Дзен** — Установка дополнительного графического окружения.

На наших каналах вы также сможете найти много другой полезной информации.

Mate

Для установки **MATE** в **РЕД ОС 7.3** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf groupinstall mate-desktop
```

Cinnamon

Для установки **Cinnamon** в **РЕД ОС 7.3** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install cinnamon
```

Дополнительные пакеты для X-сервера

Доустановить пакеты для X-сервера можно командой:

```
sudo dnf groupinstall x11
sudo dnf install vulkan-loader
```

Графический режим работы

Установить графический режим работы на сервере по умолчанию и установить тему РЕД ОС:

```
sudo systemctl set-default graphical.target
```

Перезагрузить сервер:

```
reboot
```

Удаление графической оболочки

Для удаления графической оболочки потребуется выполнить ряд действий.

Если установлено более одной графической оболочки и требуется удалить **только одну** из них:

1. Выберите графическую оболочку по умолчанию, в которой в дальнейшем хотите продолжить работу:

```
sudo nano /var/lib/AccountsService/users/<USERNAME>
```

где <**USERNAME**> — это имя пользователя.

В данном файле в строке `XSession=` впишите предпочитаемый тип графического окружения:

```
XSession=gnome

 или

XSession=mate
```

2. Перезагрузите ПК и войдите в систему как пользователь, для которого определили графическую оболочку.

3. Удалите ненужную оболочку. Пример удаления **Mate**:

```
sudo dnf remove mate-desktop
```

где **mate** - один из возможных вариантов графической оболочки.

Выбор графической оболочки для пользователя по умолчанию

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический

Среда рабочего стола - это, своего рода, графический интерфейс, с помощью которого пользователь может взаимодействовать со своим ПК. Иными словами, это все то, что мы видим после успешной авторизации в системе. На текущий момент в РЕД ОС представлены две среды рабочего стола - **Mate** и **Cinnamon**.

Если вы используете **mate**, то для того что бы поставить **cinnamon** необходимо выполнить:

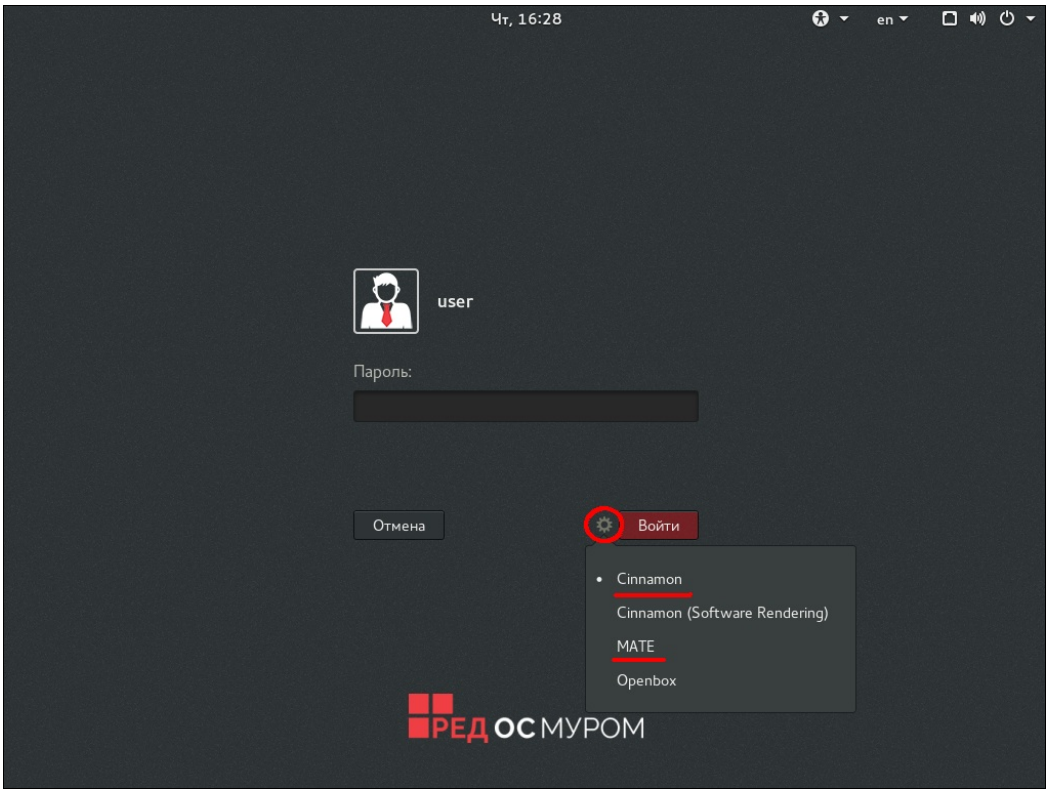
```
dnf groupinstall cinnamon
```

Если же используете **cinnamon**, то для установки **mate** необходимо выполнить:

```
dnf groupinstall mate
```

После подтверждения всех действий начнется установка среды рабочего стола.

Как только установка будет закончена необходимо перезапустить сеанс пользователя или просто перезагрузить ПК. Далее, когда будет предложена авторизация в системе, необходимо нажать на шестеренку около кнопки «**Войти**»:



Для выбора графической оболочки для пользователя по умолчанию отредактируйте файл:

```
nano /var/lib/AccountsService/users/<USERNAME>
<USERNAME> - это имя пользователя
```

В данном файле в строке **XSession=** впишите предпочитаемый тип DE **cinnamon** или **mate**.

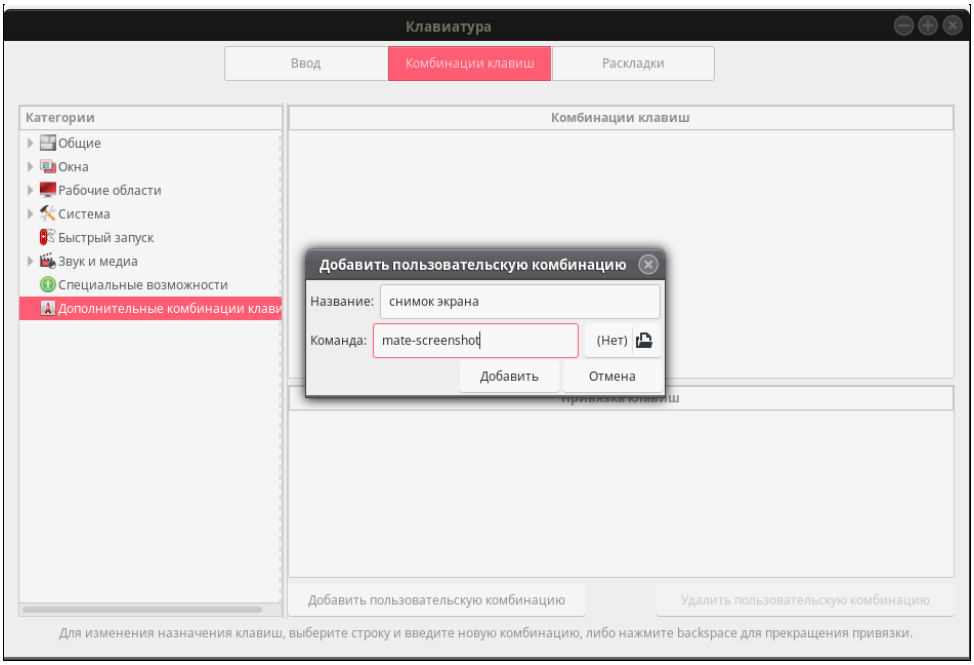
```
XSession=cinnamon
или
XSession=mate
```

Сохраните файл и выполните перезагрузку. Теперь для вашего пользователя будет загружаться выбранная вами DE.

Дополнительно стоит упомянуть, что при установке **Cinnamon** поверх **mate** необходимо настроить **mate-screenshot** для создания снимков экрана.

Для этого перейдем в «**Главное меню**»→«**Параметры**»→«**Клавиатура**»→«**Комбинации клавиш**» и в самом низу выберем «**Добавить**

пользовательскую комбинацию», в поле «**Название**» укажем удобное для нас название, например «**Снимок экрана**», а в поле «**Команда**», пропишем «**mate-screenshot**»:



Нажмем «**Добавить**» и назначим привязку клавиш в нижней половине окна.

Специальные возможности в графическом окружении MATE

Экранный диктор
Виртуальная клавиатура
Экранная лупа
Высококонтрастные темы

Тифлотехника — это отрасль приборостроения специального назначения, относящаяся к разработке технических средств для обучения, политехнической или производственной подготовки, трудовой деятельности и культурно-бытового обслуживания слепых, слабовидящих и слепоглухих, а также для коррекции, развития и восстановления зрения.

Основными задачами тифлотехники являются:

- уменьшение ограниченности в ориентировании слепых в пространстве, вызванной полной или частичной потерей зрения;
- создание необходимых технических условий для разностороннего развития и получения дополнительного необходимого образования;
- расширение возможности применения труда незрячих на современных механизированных производствах;
- облегчение ориентированности слепых в быту, создание возможности организации культурного отдыха и досуга.

В РЕД ОС доступно несколько специальных программ для облегчения работы слабовидящих в системе.

Вы можете подробнее ознакомиться с программами специального назначения, просмотрев наши обучающие видео:

- на **RuTube** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **Яндекс.Дзен** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **VK Видео** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника.

На наших каналах вы также сможете найти много другой полезной информации.

Экранный диктор

Средством для чтения текста (синтезатор речи) с экрана в РЕД ОС является **Orca**. Программа предоставляет доступ к рабочему столу для слабовидящих пользователей.

По умолчанию данная программа предустановлена в системе. Подробнее о работе экранного диктора **Orca** см. в нашей статье «Экранный диктор».

Виртуальная клавиатура

В РЕД ОС по умолчанию используется виртуальная клавиатура **Onboard**.

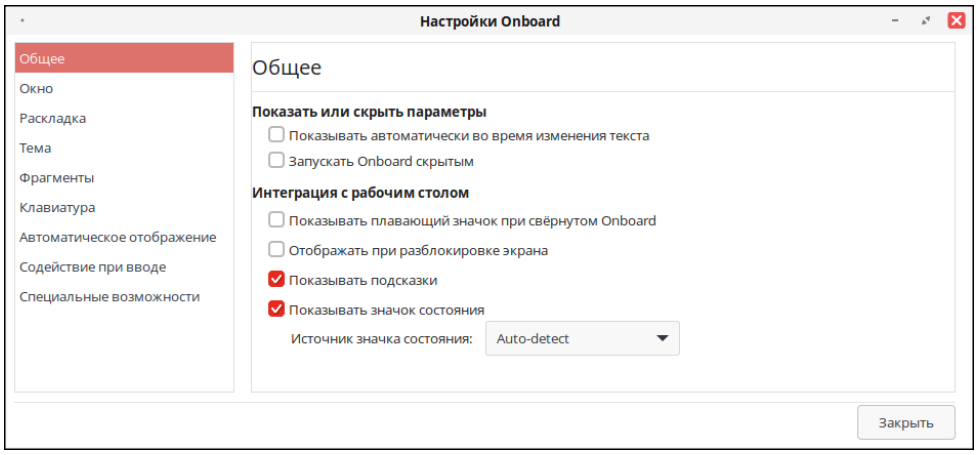
Если виртуальная клавиатура не установлена, перейдите в сеанс пользователя **root**:

```
su -
```

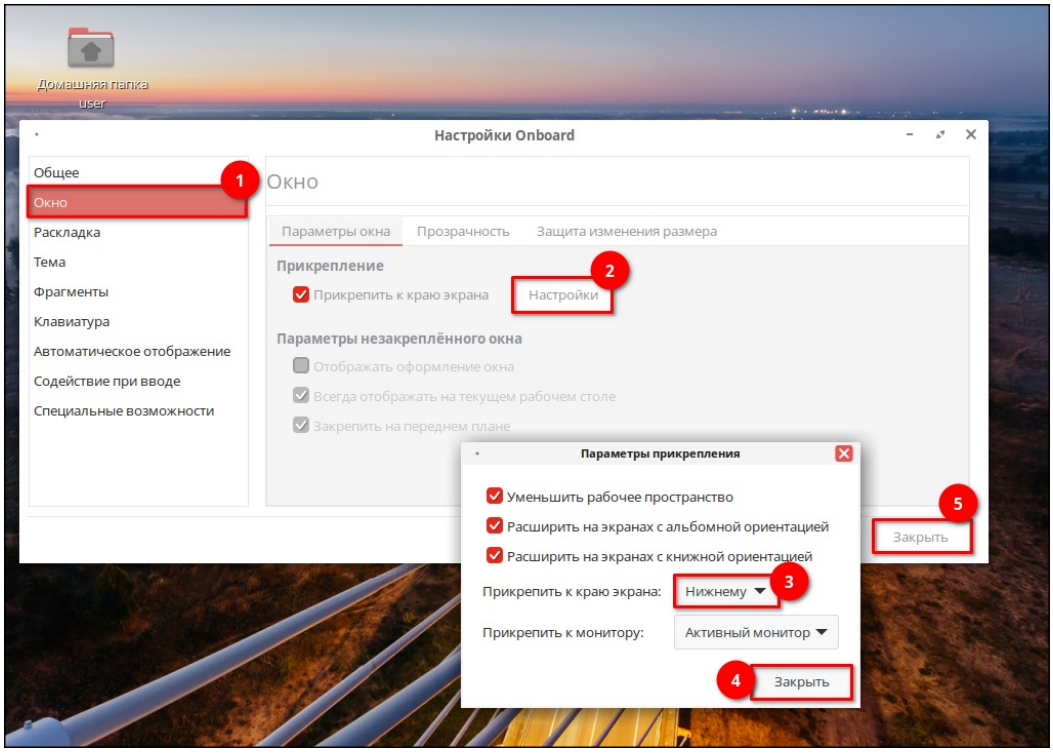
и выполните команду:

```
dnf install onboard
```

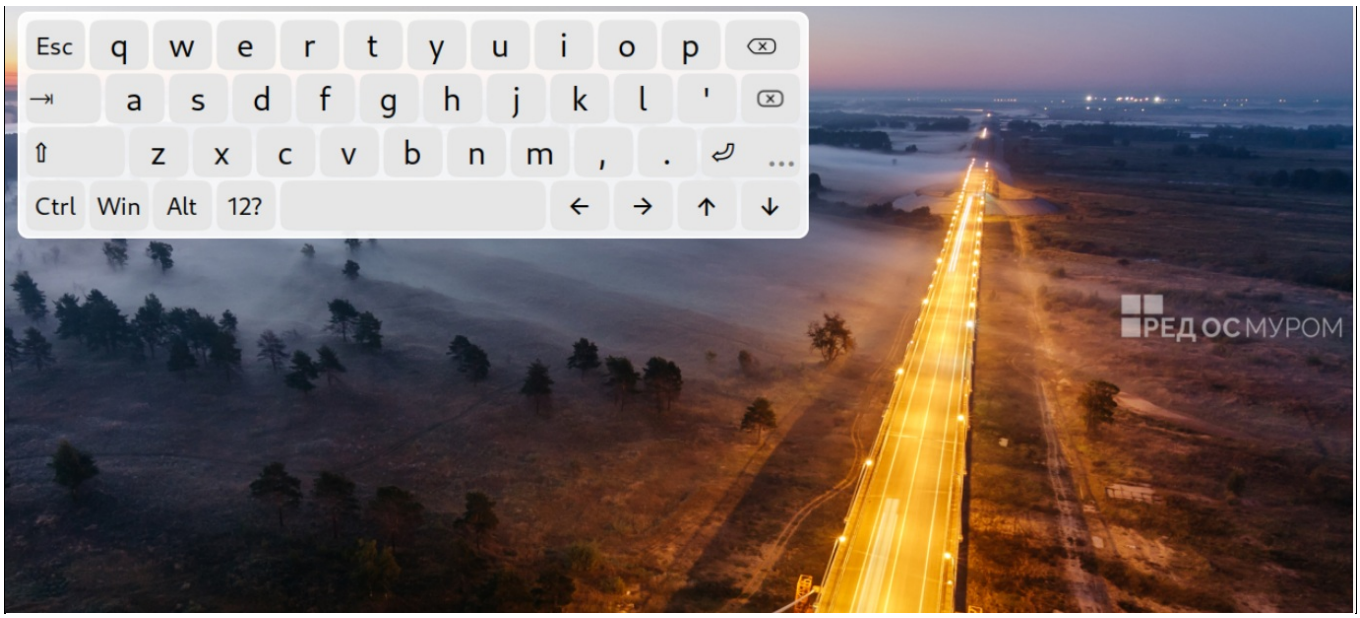
Для настройки клавиатуры перейдите в «**Главное меню**» — «**Параметры**» — «**Настройка Onboard**».



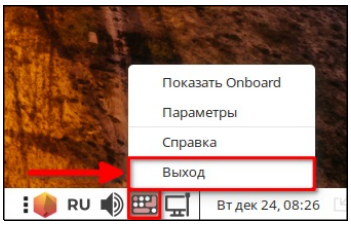
В **Настройках Onboard** в разделе «**Окно**» можно выбрать расположение клавиатуры. Для этого перейдите в «**Настройки**» и выберите вариант крепления клавиатуры к нужному краю экрана.



Для запуска виртуальной клавиатуры перейдите в «**Главное меню**» — «**Специальные возможности**» — «**Onboard**».



Клавиатуру можно свернуть, раскрыть или закрыть, нажав ПКМ на значок клавиатуры в системном трее, и выбрав в контекстном меню соответствующий пункт. Для закрытия экранной клавиатуры нажмите «**Выход**».



Экранная лупа

Также немаловажны инструменты для работы с изучением мелкого текста или фотографий.

Для данной цели существует приложение **KMagnifier** (**kmag**).

Для установки данного инструмента перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install kdeaccessibility
```

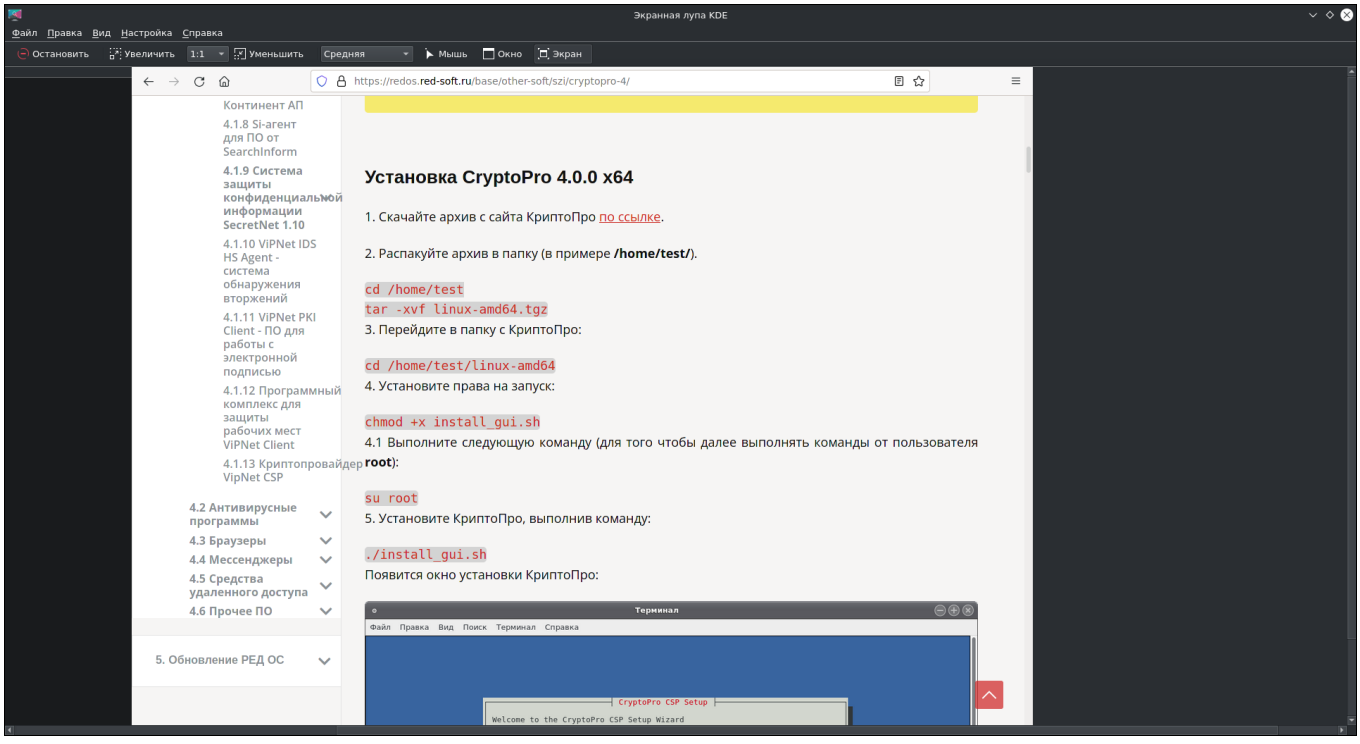
Для запуска **Kmagnifier** в графическом режиме перейдите в «**Главное меню**» - «**Специальные возможности**» - «**KMag**».

Данная программа поможет рассмотреть необходимый файл и сохранить увеличенный фрагмент на диск.

Рассмотрим, как можно воспользоваться данной программой.

Допустим, необходимо увеличить текст на странице браузера.

Для этого потребуется открыть нужный объект, который необходимо увеличить, затем перенести туда окно с экранной лупой.



Для сохранения увеличенного изображения необходимо нажать на «**Файл**» — «**Сохранить как**» и выбрать формат файла.

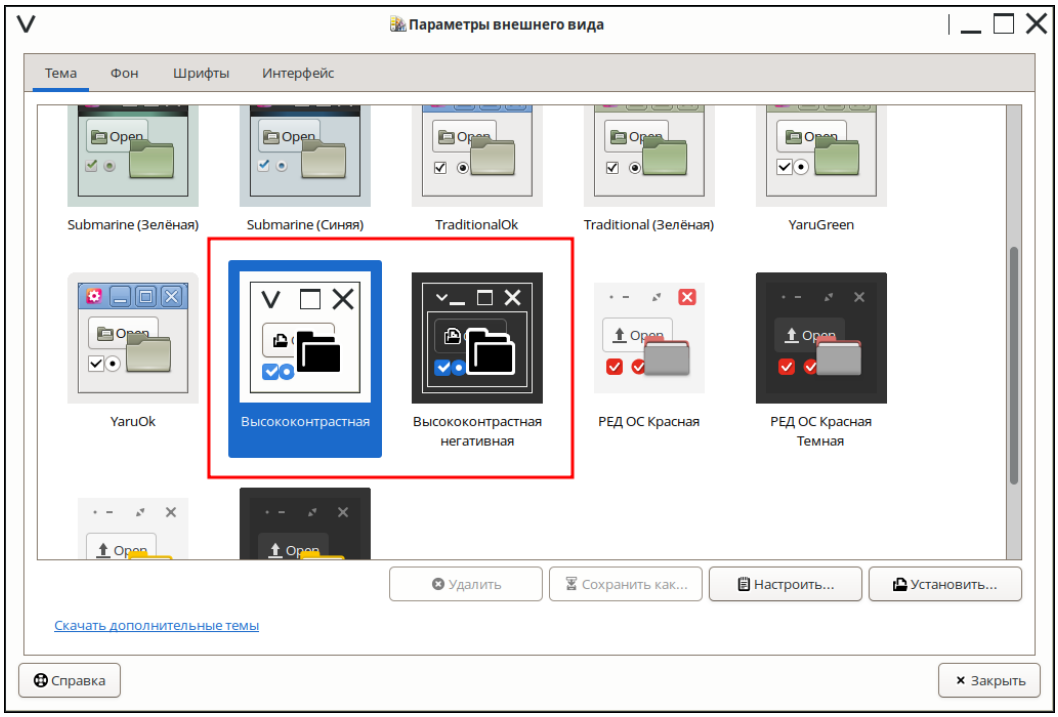
Высококонтрастные темы

Для пользователей с проблемами зрения в **MATE** предусмотрены высококонтрасные темы оформления рабочей среды. С помощью таких тем повышается контрастность окон и кнопок, чтобы их было лучше видно.

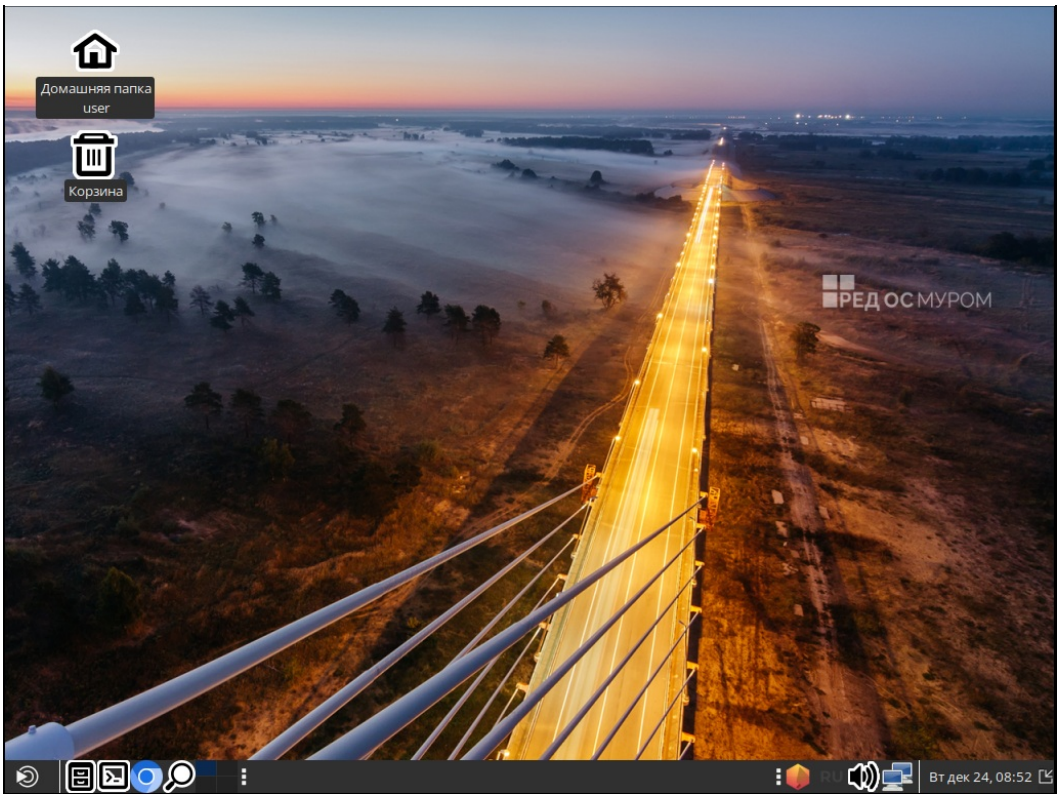
При применении высококонтрастной темы оформления иконки на рабочем столе заменяются черно-белыми аналогами, тема интерфейса приобретает монотонные цвета.

Для установки контрастной темы рабочей среды перейдите в «**Главное меню**» — «**Параметры**» — «**Внешний вид**» и на вкладке темы выберите предпочитаемую тему:

- Высококонтрастная (светлое оформление);
- Высококонтрастная негативная (темное оформление).



Внешний вид рабочего стола пользователя после применения высококонтрастной темы:



Экранный диктор

Экранный диктор Orca
Синтезатор речи RHVoice

Экранный диктор позволяет полноценно работать в системе пользователям с ограниченными возможностями по зрению путем озвучивания отдельных элементов пользовательского интерфейса.

Вы можете подробнее ознакомиться с программами специального назначения, просмотрев наши обучающие видео:

- на **RuTube** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **Яндекс.Дзен** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **VK Видео** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника.

На наших каналах вы также сможете найти много другой полезной информации.

Экранный диктор Orca

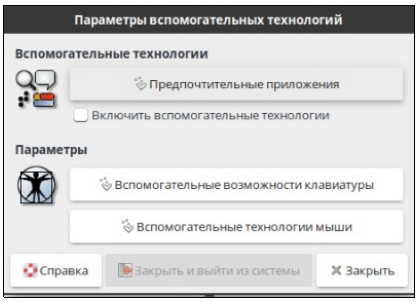
Orca в РЕД ОС является средством для чтения текста (синтезатор речи) с экрана, программа предоставляет доступ к рабочему столу для слабовидящих пользователей.

По умолчанию данная программа уже установлена в системе.

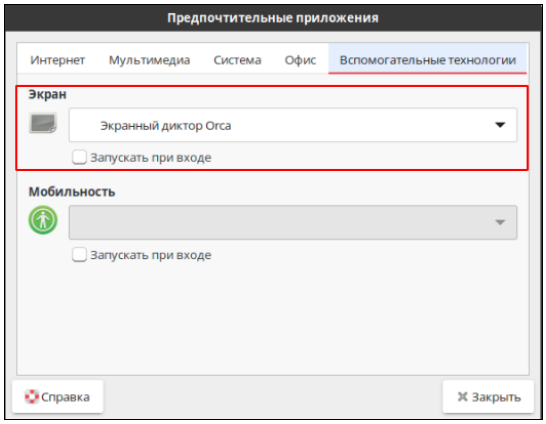
Графический режим

Для запуска экранного диктора в графическом режиме перейдите в «**Главное меню**» - «**Центр управления**» - «**Вспомогательные технологии**».

Необходимо активировать переключатель «**Включить вспомогательные технологии**» и нажать кнопку «**Предпочтительные приложения**».



В открывшемся окне можно выбрать приложение и настроить запуск программы при входе в систему.



Консольный режим

Справку по синтаксису утилиты можно увидеть через команду от *локального* пользователя:

```
orca --help
```

Использование:

```
orca [-h] [-v] [-r] [-s] [-l] [-e <параметр>] [-d <параметр>] [-p <имя>] [-u <каталог>] [--debug-file <файл>] [--debug]
```

Ключ	Описание
-h, --help	Показать данное справочное сообщение и выйти
-v, --version	Отобразить текущую версию
-r, --replace	Заменить уже работающий экземпляр экранного диктора
-s, --setup	Задать параметры пользователя (графическая версия)
-l, --list-apps	Вывести список известных запущенных приложений
-e <параметр>, --enable <параметр>	Принудительно использовать параметр
-d <параметр>, --disable <параметр>	Исключить использование параметра
-p <имя>, --profile <имя>	Загрузить профиль
-u <каталог>, --user-prefs <каталог>	Использовать другой каталог с параметрами пользователя
--debug-file <файл>	Записывать отладочные данные в указанный файл
--debug	Записывать отладочные данные в debug-<ГГГГ-ММ-ДД-ЧЧ:ММ:СС>.out

Синтезатор речи RHVoice

RHVoice — российский синтезатор речи с открытым исходным кодом, использование которого доступно на компьютере или телефоне любого пользователя с ограниченными возможностями зрения.

RHVoice использует статистический параметрический синтез. Он опирается на уже существующие речевые технологии с открытым исходным кодом (прежде всего **HTS** и связанные компоненты).

Голоса создаются на основе записей естественной человеческой речи. Они компактны, так как на компьютере пользователей хранятся только статистические модели.

Изначально **RHVoice** поддерживал только русский язык. Теперь он также поддерживает английский, бразильский португальский, эсперанто, грузинский, украинский, киргизский и татарский языки.

Для установки **RHVoice** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

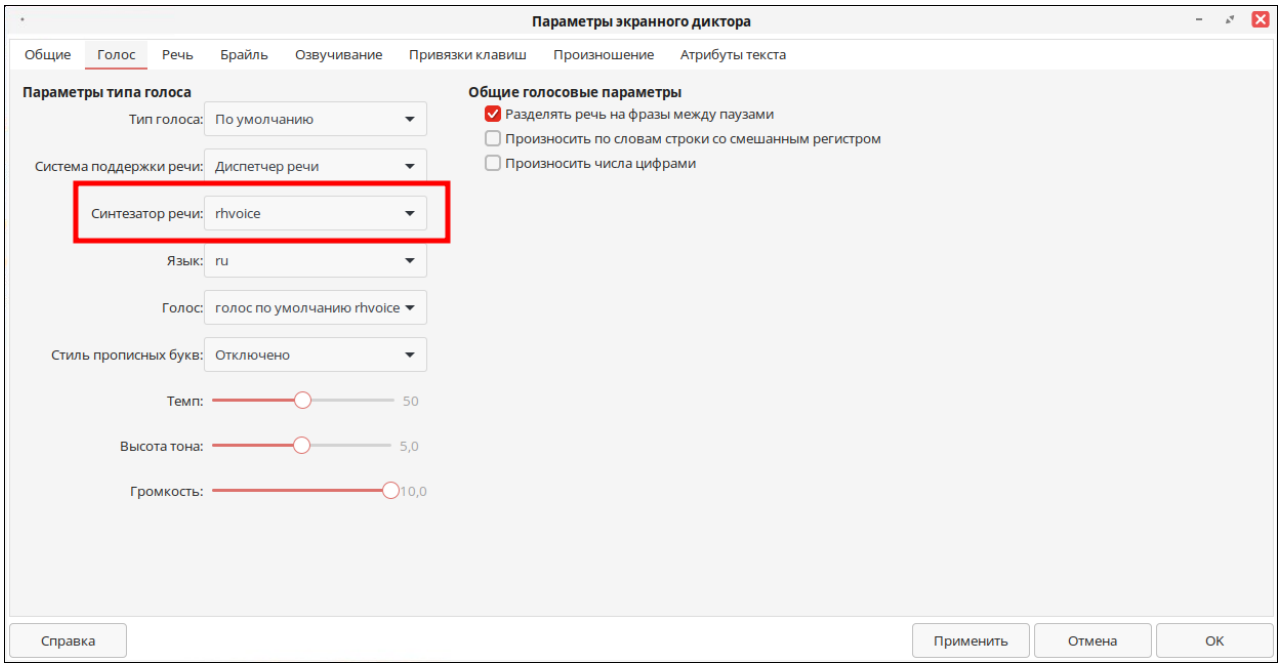
```
dnf install RHVoice
```

Для настройки **RHVoice** в качестве синтезатора речи по умолчанию в терминале выполните команду (от *локального* пользователя):

```
orca -s
```

В окне параметров перейдите на вкладку «**Голос**».

В пункте «**Синтезатор речи**» выберите «**rhvoice**».

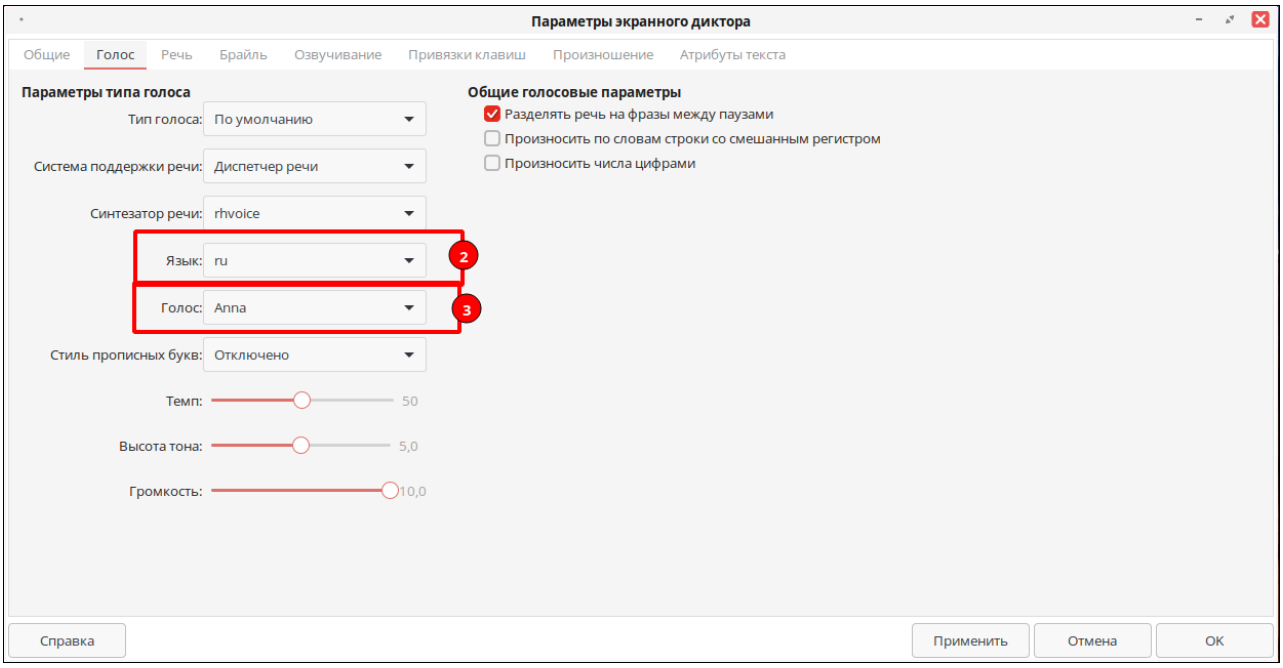


Нажмите «**OK**» и перезагрузите систему.

После перезагрузки с правами *локального* пользователя снова откройте параметры экранного диктора с помощью команды:

```
orca -s
```

На вкладке «**Голос**» в соответствующих пунктах выберите необходимый *язык* (**2**) и *голос озвучки* (**3**). Также в данном окне можно настроить все необходимые параметры для озвучки. Для применения изменений нажмите «**Применить**» и «**OK**».



Установка дополнительных шрифтов

Предварительная подготовка
Установка популярных шрифтов Windows
Установка шрифтов Bitmap Fonts для использования в терминале
Установка шрифта Inconsolata (доступно для РЕД ОС 8)
Установка шрифта Droid Sans Mono
Установка шрифта DejaVu Sans Mono
Установка сторонних шрифтов
Установка одиночного шрифта
Установка архива шрифтов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: msttcore-fonts-installer-2.6, bitmap-fonts-compat-0.3, google-droid-sans-mono-fonts-20120715, dejavu-lgc-sans-mono-fonts-2.35

По умолчанию в РЕД ОС предустановлено несколько основных шрифтов. Однако не все шрифты, используемые в ОС Windows, доступны в РЕД ОС. Необходимые шрифты можно доустановить. В рамках данной инструкции будет рассмотрено несколько способов добавления новых шрифтов в РЕД ОС.

Предварительная подготовка

Перед установкой шрифтов ОС Windows необходимо убедиться, что в системе доступны необходимые инструменты, такие как:

- **curl** – для загрузки файлов;
- **cabextract** – для извлечения файлов шрифтов Windows;
- **xorg-x11-font-utils** – для установки, преобразования и генерации шрифтов;
- **fontconfig** – для управления и настройки доступа к шрифтам.

В РЕД ОС они установлены по умолчанию, но рекомендуется проверить и установить недостающие пакеты.

Используйте нижеприведенную команду для установки (потребуются права **администратора**):

```
sudo dnf install curl cabextract xorg-x11-font-utils fontconfig
```

Установка популярных шрифтов Windows

В состав дистрибутива РЕД ОС входит пакет `msttcore-fonts-installer`, который содержит основные шрифты Microsoft:

- Andale Mono;
- Arial;
- Arial black;
- Calabri;
- Cambria;
- Candara;
- Consolas;
- Constantia;
- Corbel;
- Comic;
- Courier New;
- Impact;
- Tahoma;
- Times New Roman;
- Trebuchet;
- Verdana;
- Webdings.

Для установки пакета *msttcore-fonts-installer* выполните команду (потребуются права **администратора**):

```
sudo dnf install msttcore-fonts-installer
```

В результате будут установлены основные *шрифты Windows*.

Установка шрифтов Bitmap Fonts для использования в терминале

Bitmap Fonts — семейство растровых шрифтов. **Bitmap Fonts** содержит шрифты, предназначенные для использования в терминале. Формат шрифта основан на группе глифов, нарисованных внутри текстовых файлов, и наборе файлов конфигурации **JSON** для установки их параметров.

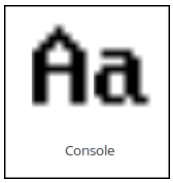
Моноширинные шрифты для использования в терминале можно установить из официального репозитория РЕД ОС с помощью пакета *bitmap-fonts-compat*.

Для добавления нового шрифта используется пакет *bitmap-fonts-compat*.

Для установки пакета *bitmap-fonts-compat* выполните команду (потребуются права **администратора**):

```
sudo dnf install bitmap-fonts-compat
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

```
sudo dnf remove bitmap-fonts-compat
```

Установка шрифта Inconsolata (доступно для РЕД ОС 8)

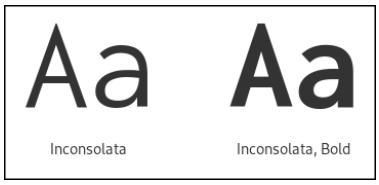
Inconsolata часто используется пользователями для работы в терминале — это четкий и легко читаемый моноширинный шрифт, разработанный Рафаэлем Левиеном. Шрифт имеет символ перечеркнутого нуля, чтобы отличить этот символ от заглавной буквы O, а также легко различимые символы для строчной буквы L и цифры 1.

Для добавления нового шрифта используется пакет *levien-inconsolata-fonts*.

Для установки пакета *levien-inconsolata-fonts* выполните команду (потребуются права **администратора**):

```
sudo dnf install levien-inconsolata-fonts
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

```
sudo dnf remove levien-inconsolata-fonts
```

Установка шрифта Droid Sans Mono

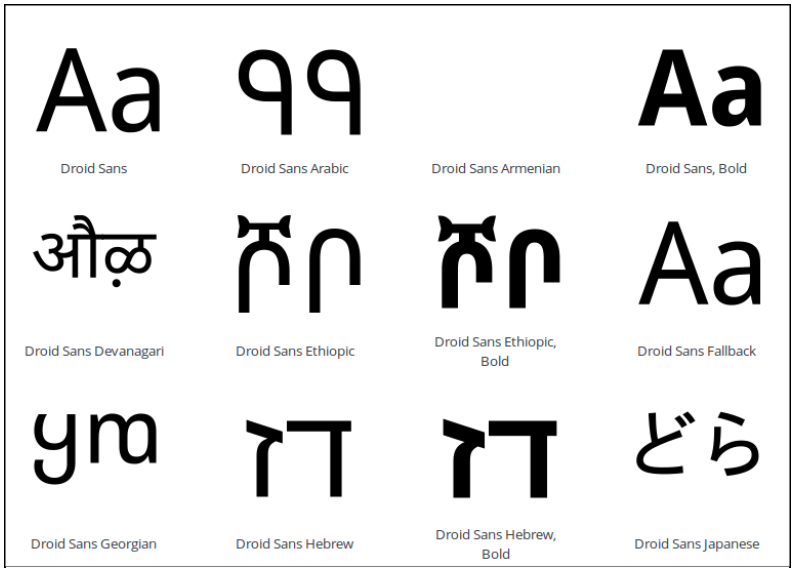
Droid Sans Mono — часть шрифтов семейства **Droid**, созданных компанией **Google**. Недостатком этого шрифта является отсутствие нуля с точками или косой чертой, из-за чего глиф нуля трудно отличить от заглавной буквы O.

Для добавления нового шрифта используется пакет *google-droid-sans-mono-fonts*.

Для установки пакета *google-droid-sans-mono-fonts* выполните команду (потребуются права **администратора**):

```
sudo dnf install google-droid-sans-mono-fonts
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

```
sudo dnf remove google-droid-sans-mono-fonts
```

Установка шрифта DejaVu Sans Mono

DejaVu Sans Mono — это шрифт, который относится к семейству шрифтов **DejaVu**. **DejaVu** — проект, целью которого является полное покрытие алфавитных сценариев, абджадов и символов всеми символами, которые являются частью подмножеств **Unicode MES-1**, **MES-2** и **MES-3**.

Для добавления нового шрифта используется пакет *dejavu-lgc-sans-mono-fonts*.

Для установки пакета *dejavu-lgc-sans-mono-fonts* выполните команду (потребуются права **администратора**):

```
sudo dnf install dejavu-lgc-sans-mono-fonts
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

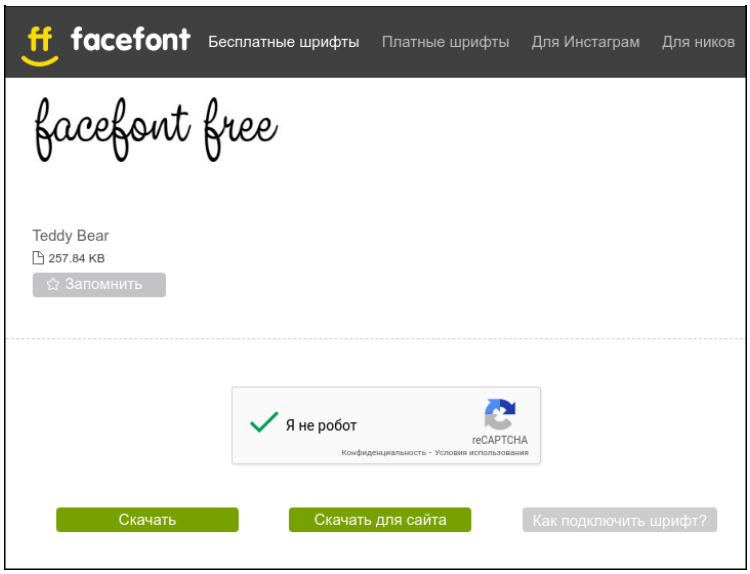
```
sudo dnf remove dejavu-lgc-sans-mono-fonts
```

Установка сторонних шрифтов

Установка одиночного шрифта

Для установки какого-либо определенного шрифта выполните следующий алгоритм действий:

1. Загрузите из сети Интернет файл нужного шрифта (в примере загружен шрифт **Teddy Bear**).



2. Скопируйте файл шрифта из каталога загрузок (в примере */home/user/Загрузки/*) в каталог хранения шрифтов */usr/share/fonts*:

```
cp /home/user/Загрузки/teddy-bear.ttf /usr/share/fonts
```

После этого новый шрифт будет доступен к использованию.



Установка архива шрифтов

Для установки какого-либо набора шрифтов выполните следующий алгоритм действий:

1. Загрузите из сети Интернет архив нужного шрифта (в примере с официального сайта **JetBrains** скачан архив шрифтов **JetBrains Mono**).

2. Перейдите в терминал и выполните команду для перехода в каталог с загруженными шрифтами (в примере */home/user/Загрузки/*):

```
cd /home/user/Загрузки/
```

3. Убедитесь, что установлен пакет для работы с архивами **unzip** (потребуются права **администратора**):

```
sudo dnf install unzip
```

4. Распакуйте архив с загруженными шрифтами с помощью команды:

```
unzip ./JetBrainsMono-2.304.zip
```

5. Скопируйте каталог шрифтов в каталог хранения шрифтов */usr/share/fonts/* (потребуются права **администратора**):

```
sudo cp -r ./fonts /usr/share/fonts/
```



Установка прочих шрифтов в РЕД ОС аналогична вариантам, приведенным выше.

Настройка внешнего вида графического окружения MATE в РЕД ОС 7.3

Настройка темы графической оболочки MATE
Установка темы через менеджер пакетов dnfdragora
Установка темы через терминал
Установка дополнительных тем
Создание собственных тем
Установка новых курсоров мыши
Установка новых тем значков (иконок)
Установка нового фона рабочего стола
Удаление параметра темы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Настройка темы графической оболочки MATE

Тема — это группа параметров, влияющих на визуальное представление частей рабочего стола. Тема влияет на различные параметры: элементы управления, цвета, рамку окна, значки, указатели.

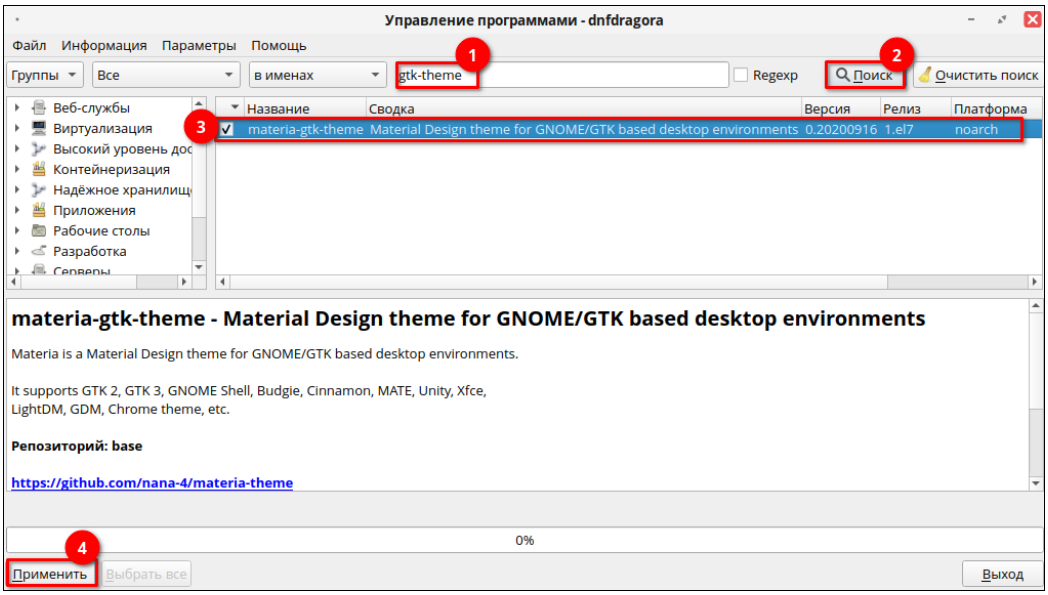
Для смены внешнего вида графической оболочки MATE в РЕД ОС необходимо вызвать контекстное меню, нажав ПКМ по свободной области рабочего стола, и выбрать пункт меню «**Параметры внешнего вида**», а затем вкладку «**Тема**».



Здесь можно обратиться к коллекции доступных встроенных тем. Для установки понравившейся темы щелкните по ней ЛКМ. Оформление темы будет применено автоматически.

Установка темы через менеджер пакетов dnfdragora

Для установки темы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову (например, «**gtk-theme**») и отметьте флагом нужный пакет. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Установка темы через терминал

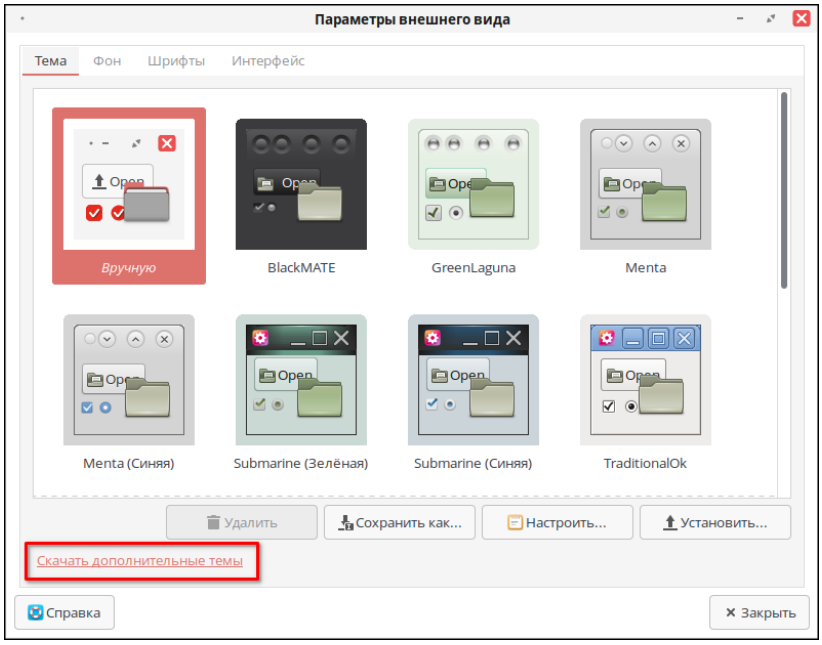
Для установки темы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install material-gtk-theme
```

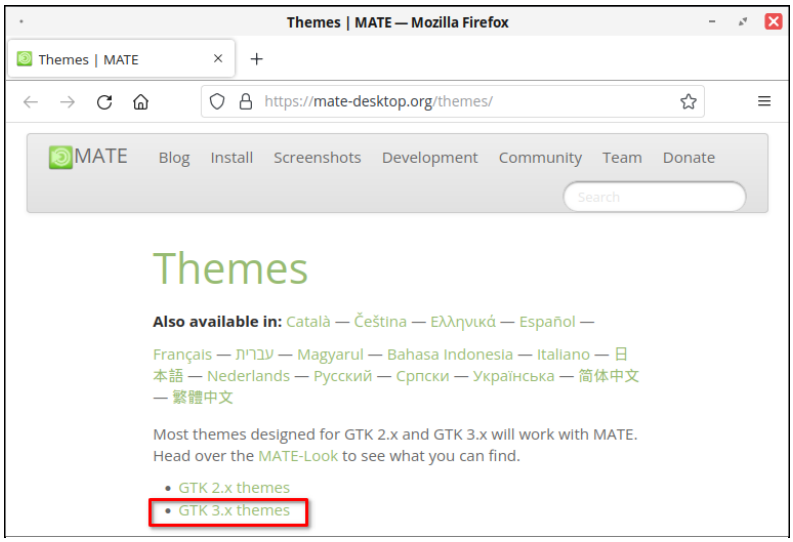
Установка дополнительных тем

Для установки сторонней темы и добавления ее в список доступных выполните следующий алгоритм действий:

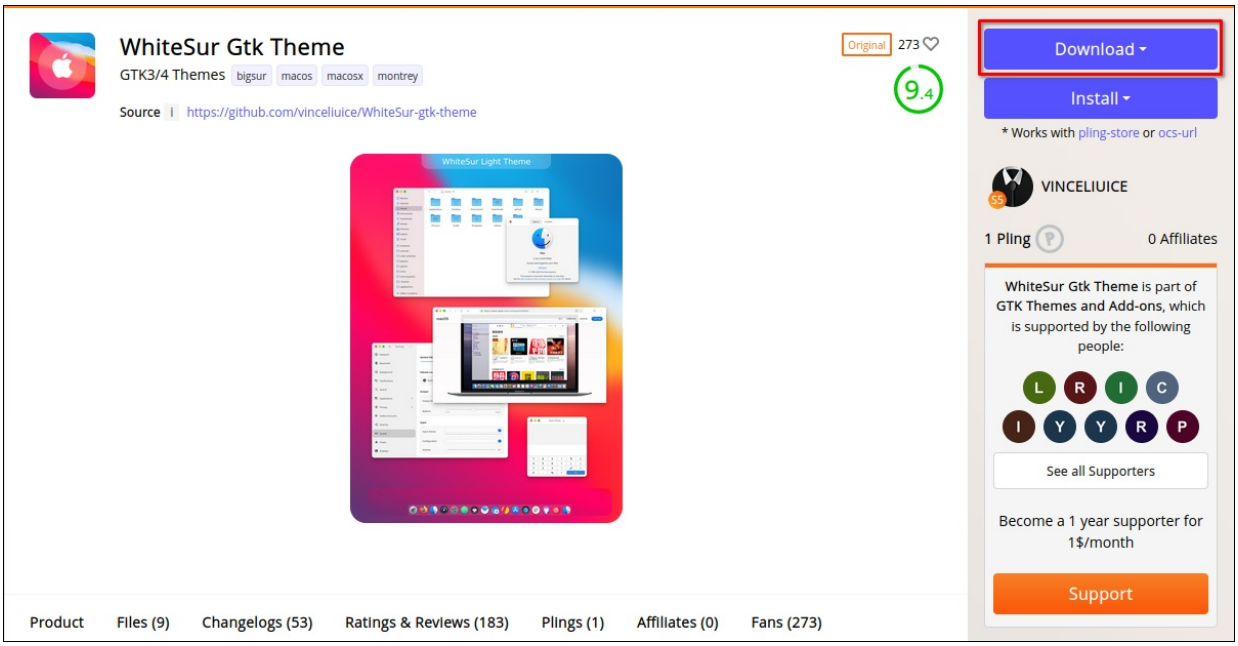
1. В «**Параметрах внешнего вида**» на вкладке «**Тема**» нажмите «**Скачать дополнительные темы**».



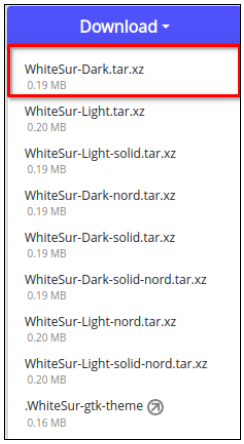
2. Будет выполнено автоматическое перенаправление на страницу с темами. На загруженной странице выберите «**GTK 3.x themes**».



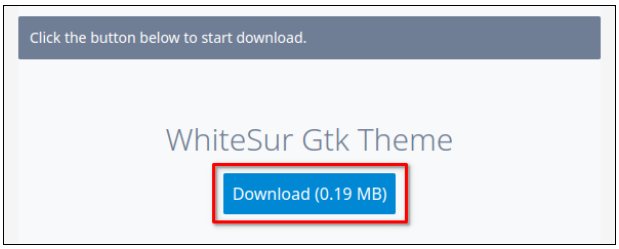
3. Выберите из списка понравившуюся тему и нажмите на нее. Будет открыто подробное описание темы. Для загрузки нажмите «**Download**».



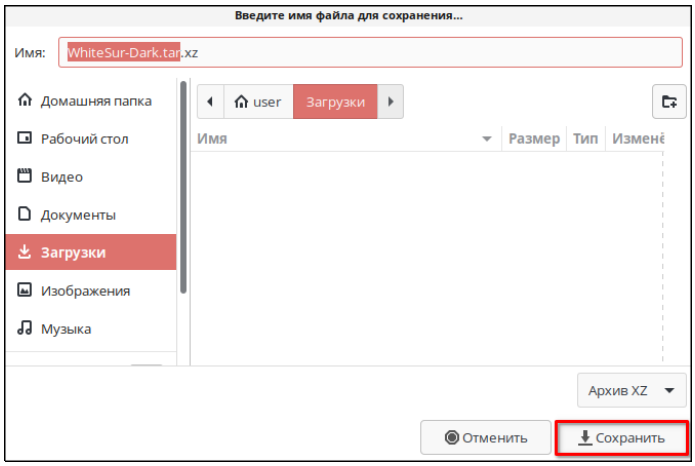
4. По нажатии на кнопку «**Download**» будет открыт список с доступным цветовым оформлением. Выберите любое цветовое оформление.



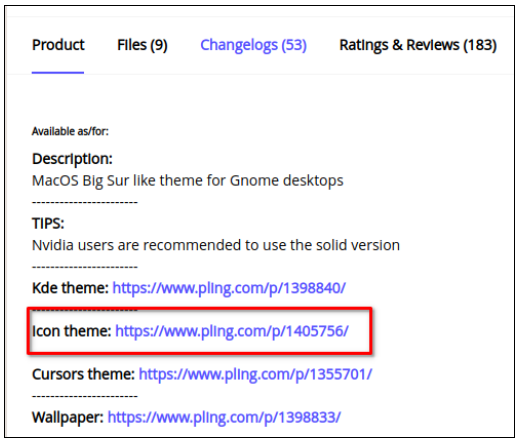
5. Начнется подготовка архива к скачиванию. Когда архив станет доступен для скачивания, нажмите на активную кнопку «**Download**».



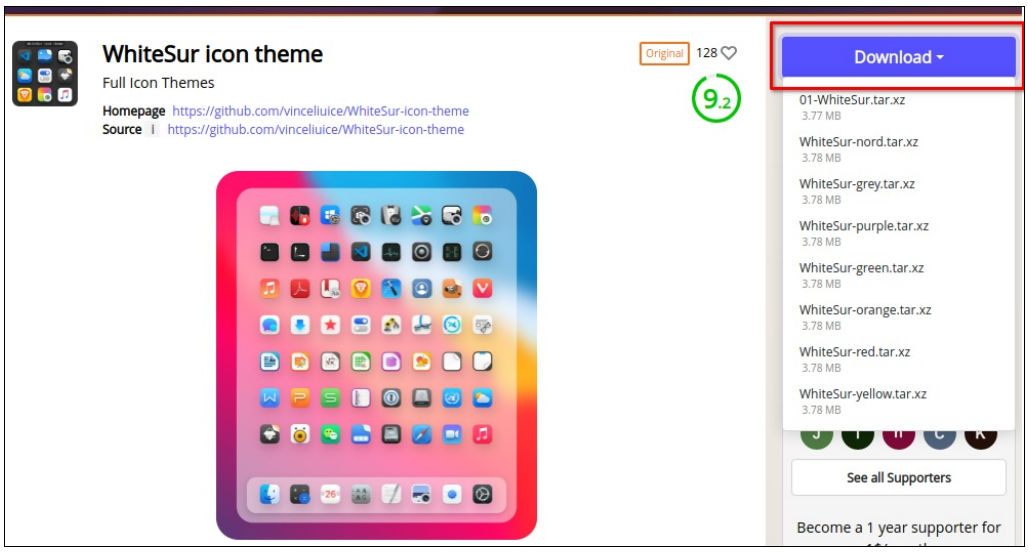
6. В диалоговом окне выбора каталога загрузок укажите удобный для скачивания каталог и нажмите «**Сохранить**».



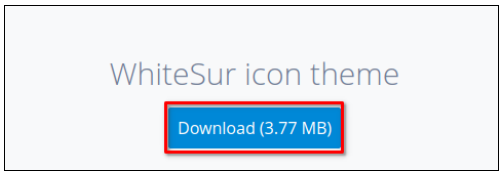
7. Далее необходимо дополнительно скачать оформление иконок для выбранной темы. Для этого пролистайте вниз до ссылки на иконки и перейдите по указанной ссылке.



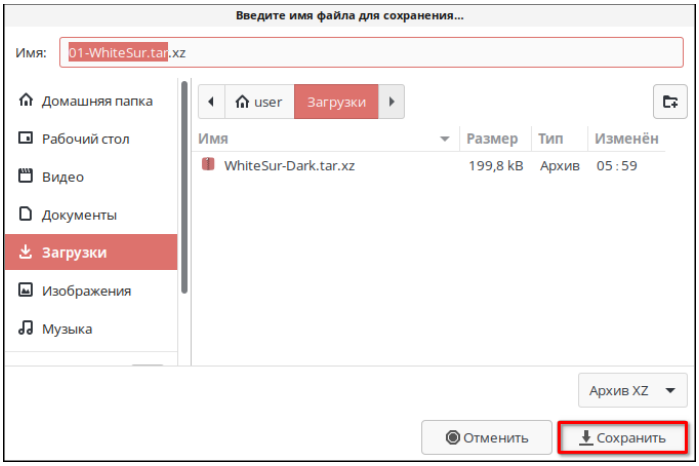
8. Для скачивания набора иконок нажмите кнопку «**Download**» и выберите цветовое оформление из списка.



9. Дождитесь подготовки архива и нажмите на кнопку «**Download**».



10. В диалоговом окне выбора каталога загрузок укажите удобный для скачивания каталог и нажмите «**Сохранить**».



11. Перейдите в терминал и выполните команду для перехода в каталог с загруженными архивами тем (в примере */home/user/Загрузки/*):

```
cd /home/user/Загрузки/
```

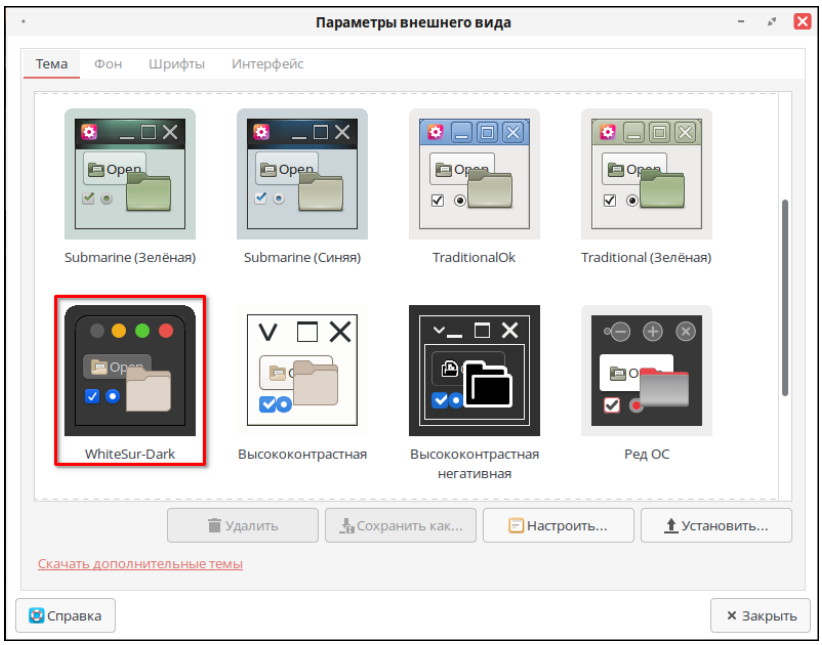
Распакуйте архив с основной темой с помощью команды:

```
tar -xvf ./WhiteSur-Dark.tar.xz
```

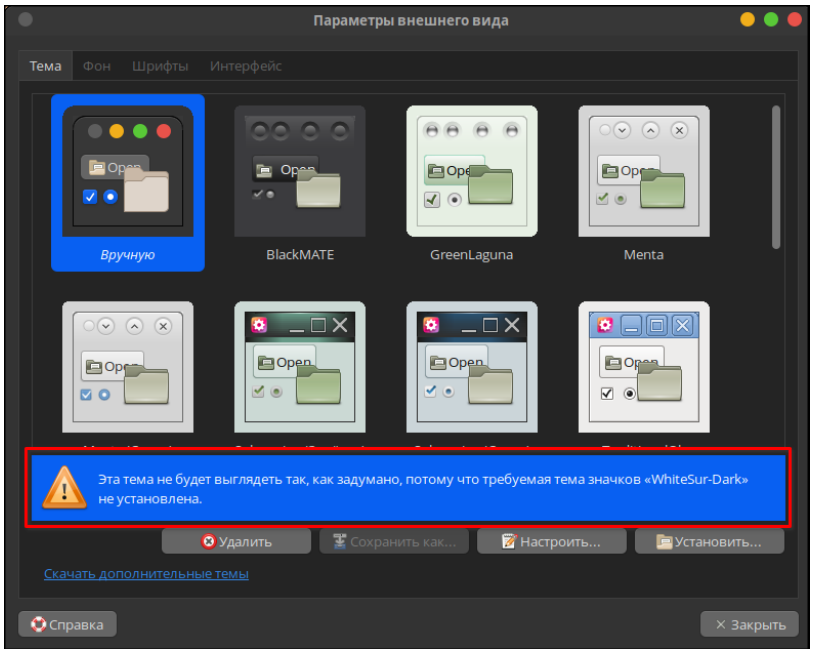
Скопируйте распакованный каталог темы в */usr/share/themes/* (потребуются права **администратора**):

```
sudo cp -r ./WhiteSur-Dark /usr/share/themes/
```

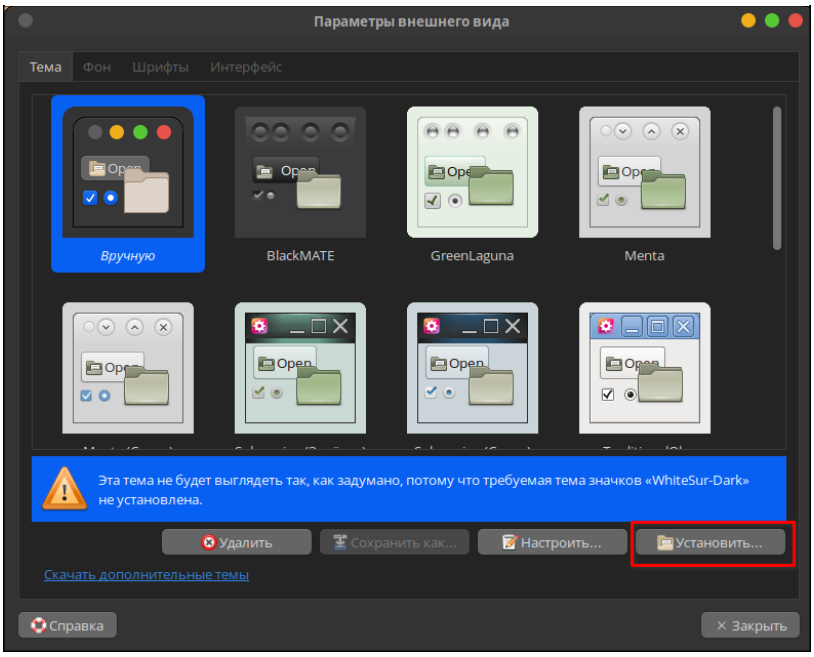
12. Закройте терминал и перейдите в «**Параметры внешнего вида**» — «**Тема**».



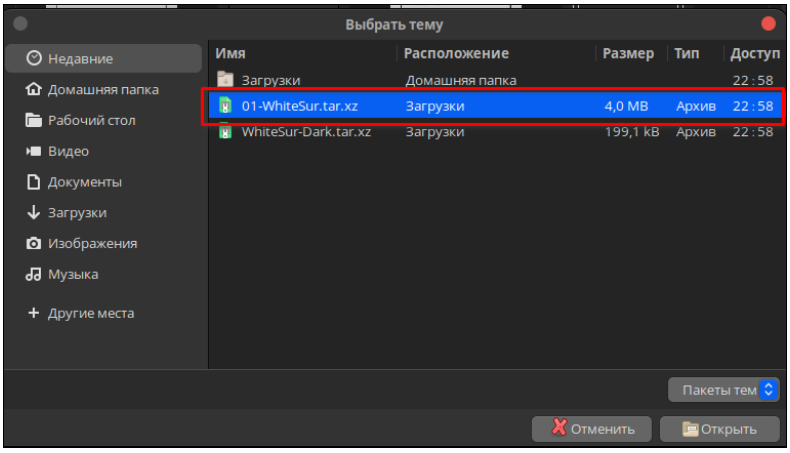
13. При выборе загруженной темы появится уведомление вида: «*Эта тема не будет выглядеть так, как задумано, потому что требуемая тема значков <название_темы> не установлена*».



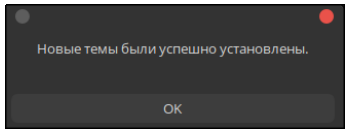
14. Нажмите «**Установить...**».



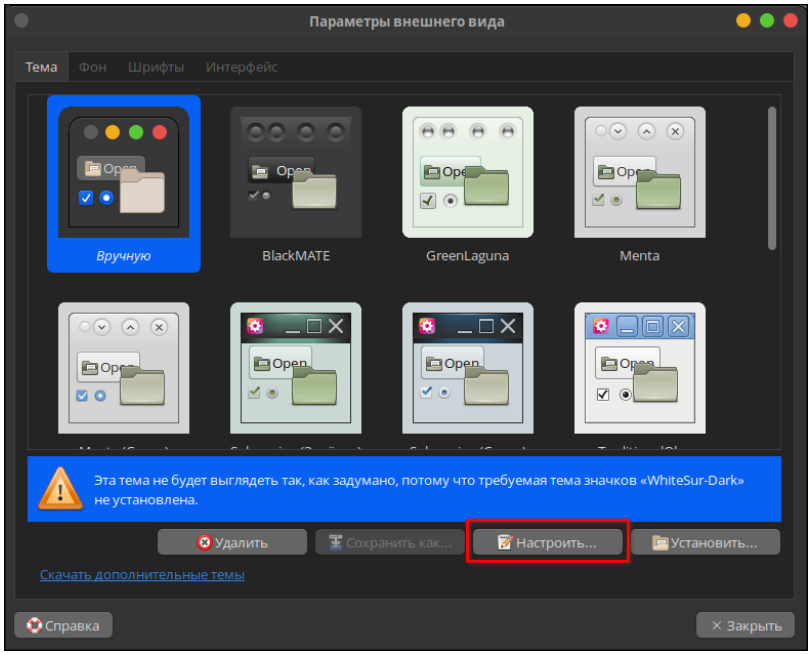
15. В открывшемся диалоговом окне двойным щелчком ЛКМ выберите тему оформления значков.



16. Появится сообщение о том, что новые темы были успешно установлены. Нажмите «**OK**».

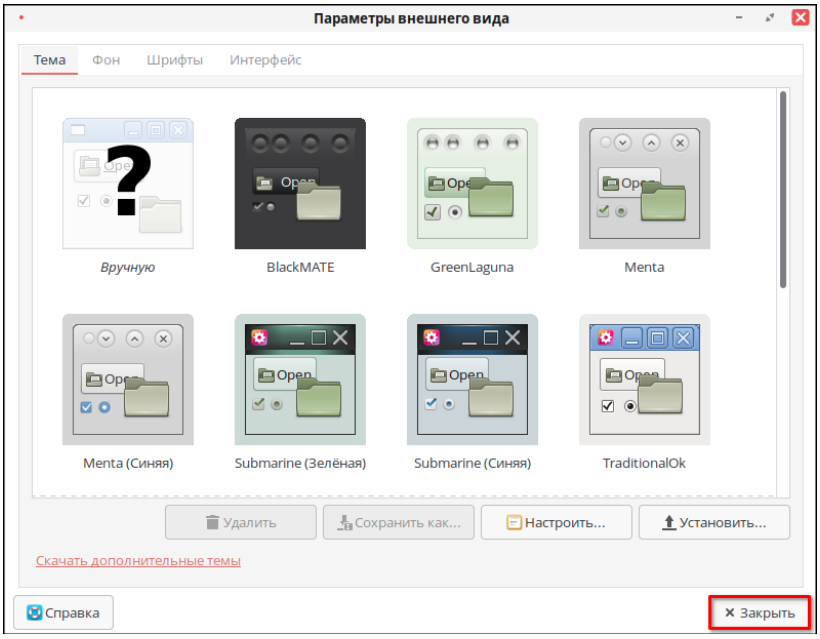


17. Далее нажмите «**Настроить...**» и перейдите на вкладку «**Значки**».

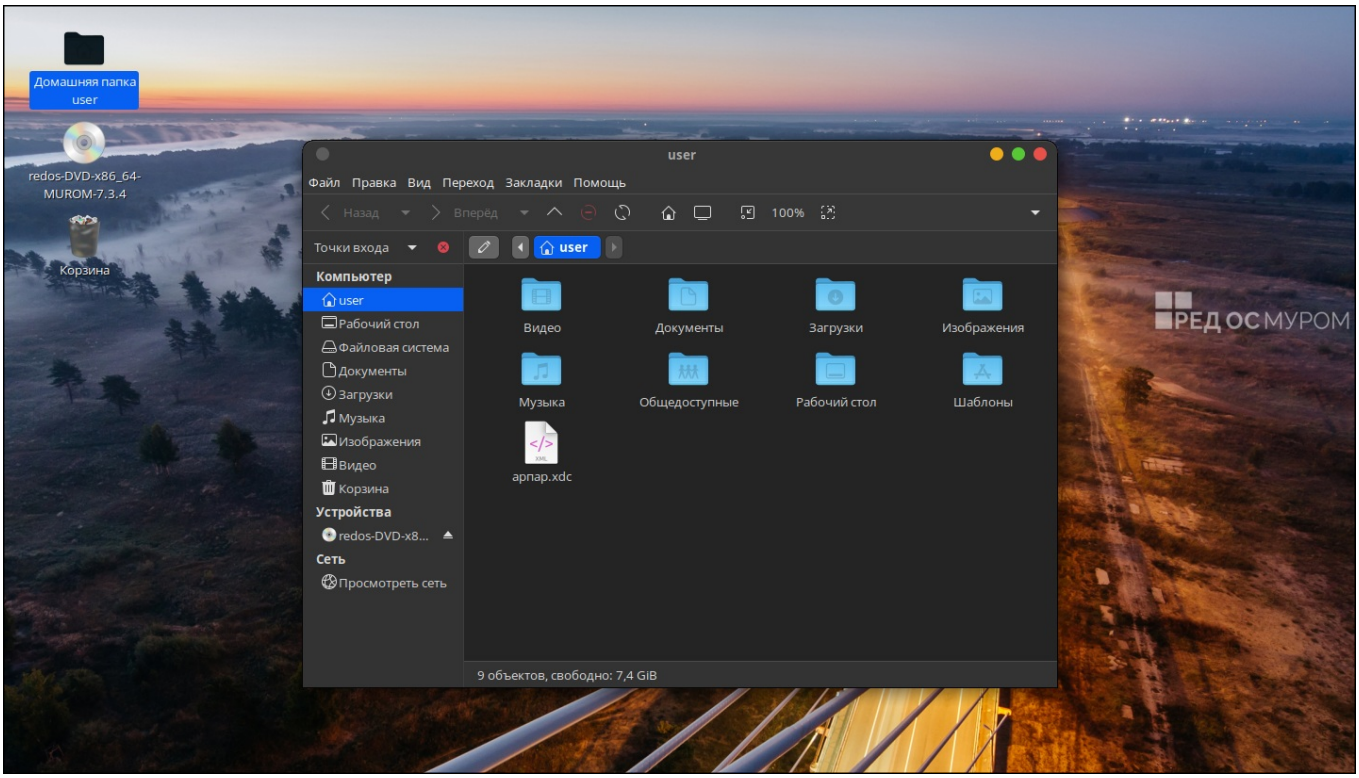


18. Выберите значки установленной темы и нажмите «**Закрыть**». Новая тема будет успешно применена к системе.

19. Закройте диалоговое окно «**Параметры внешнего вида**».



Новая тема будет успешно применена к системе.

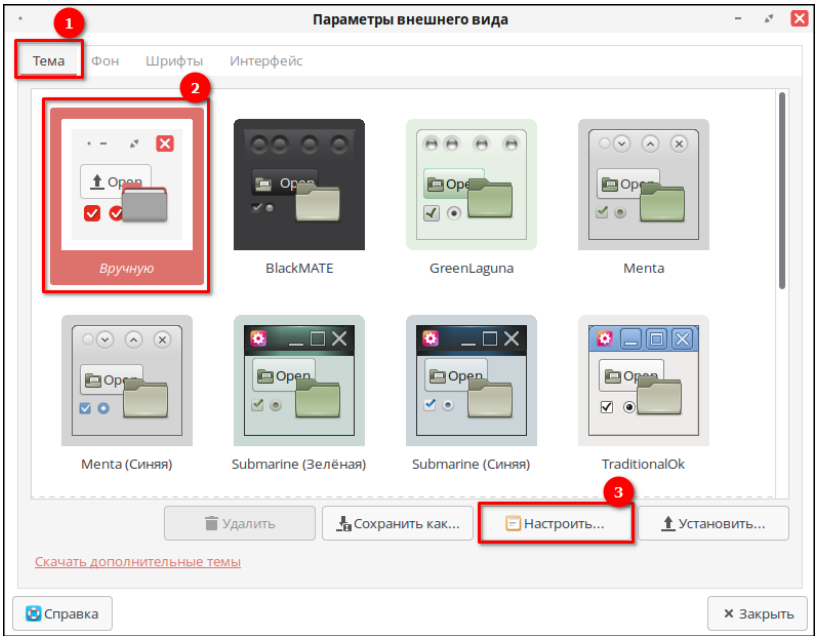


Создание собственных тем

Темы представляют собой различные комбинации параметров элементов управления. Вы можете создать собственную тему, в которой будет использоваться другая комбинация параметров элементов управления.

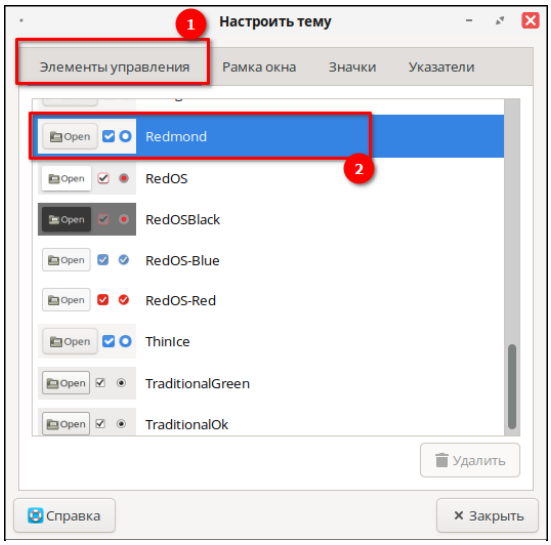
Для создания собственной темы выполните следующие действия:

1. Запустите инструмент «**Внешний вид**». Откройте вкладку «**Тема**» (1).

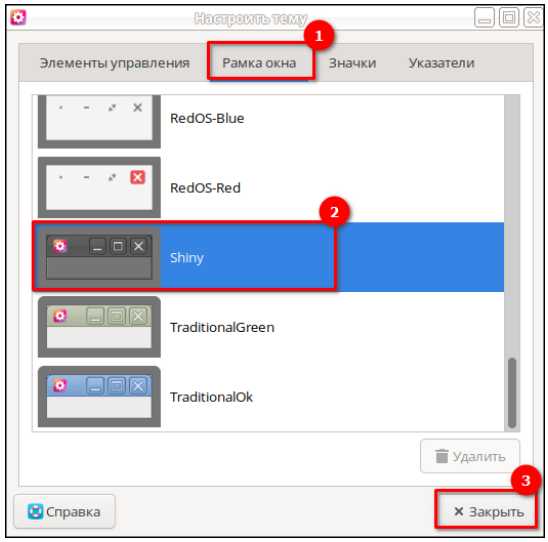


2. Выберите тему из списка (2) и нажмите кнопку «**Настроить**» (3).

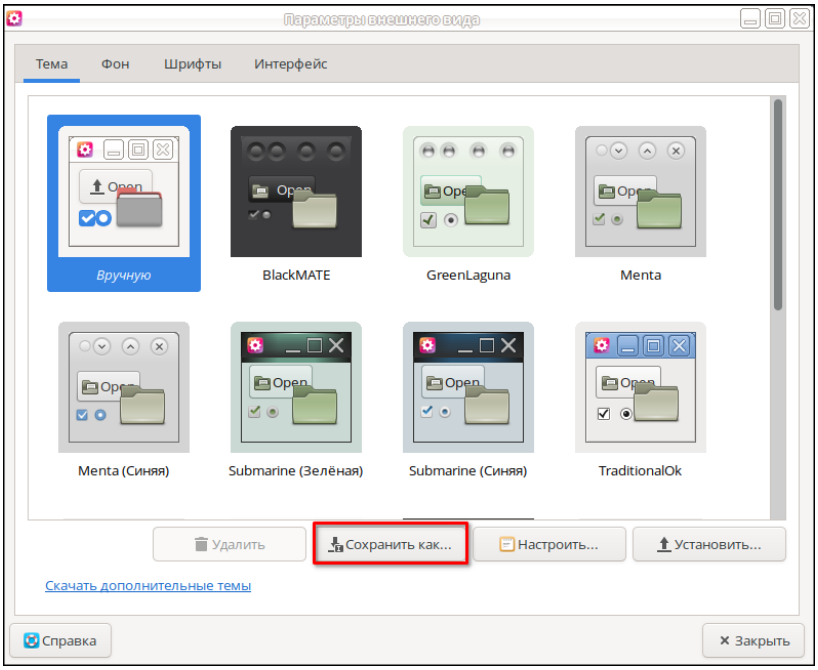
3. В появившемся диалоговом окне на вкладке «**Элементы управления**» (1) выберите параметр элементов управления (2), который необходимо использовать в теме.



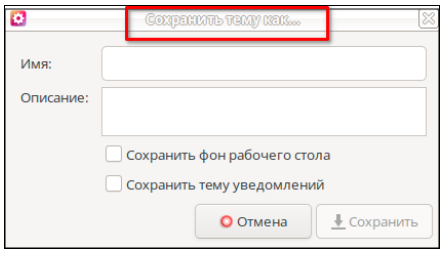
4. Щелкните по вкладке «**Рамка окна**» (1), выберите параметры рамки окна (2), который следует использовать в вашей собственной теме. Нажмите «**Закрыть**» (3).



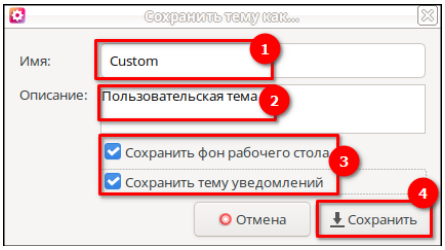
5. В инструменте настройки «**Внешний вид**» нажмите кнопку «**Сохранить как...**».



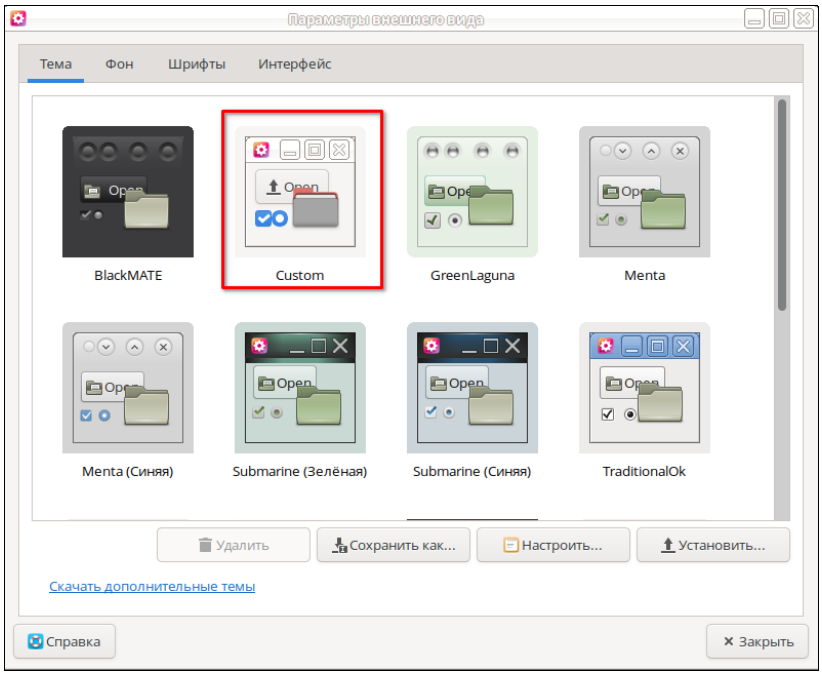
Появится диалоговое окно «**Сохранить тему как...**».



6. Введите в диалоговом окне название и краткое описание собственной темы, затем нажмите кнопку «**Сохранить**».



Тема появится в списке доступных тем.



Установка новых курсоров мыши

Для добавления новых курсоров (указателей мыши) можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**.

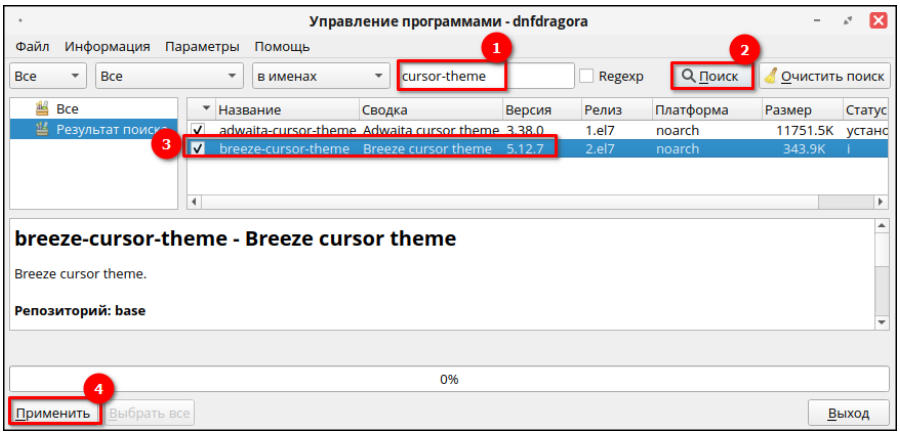
Для поиска новых курсоров через терминал выполните команду:

```
dnf search *-cursor-theme
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы курсора (потребуются права **администратора**), например:

```
dnf install breeze-cursor-theme
```

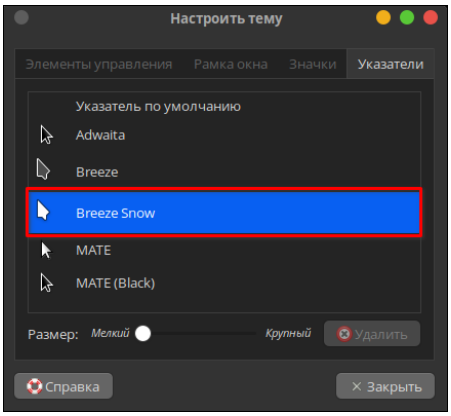
Для установки новой темы оформления указателя мыши через менеджер пакетов **dnfdragora** по шаблону – ***-cursor-theme** (1) выполните поиск темы (2), отметьте флагом необходимую тему (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



Для применения новой темы оформления курсора мыши перейдите в «**Параметры внешнего вида**» — «**Тема**» — «**Настроить**» — «**Указатели**».

Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.



Установка новых тем значков (иконок)

Для добавления новых значков (иконок) рабочего стола можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**.

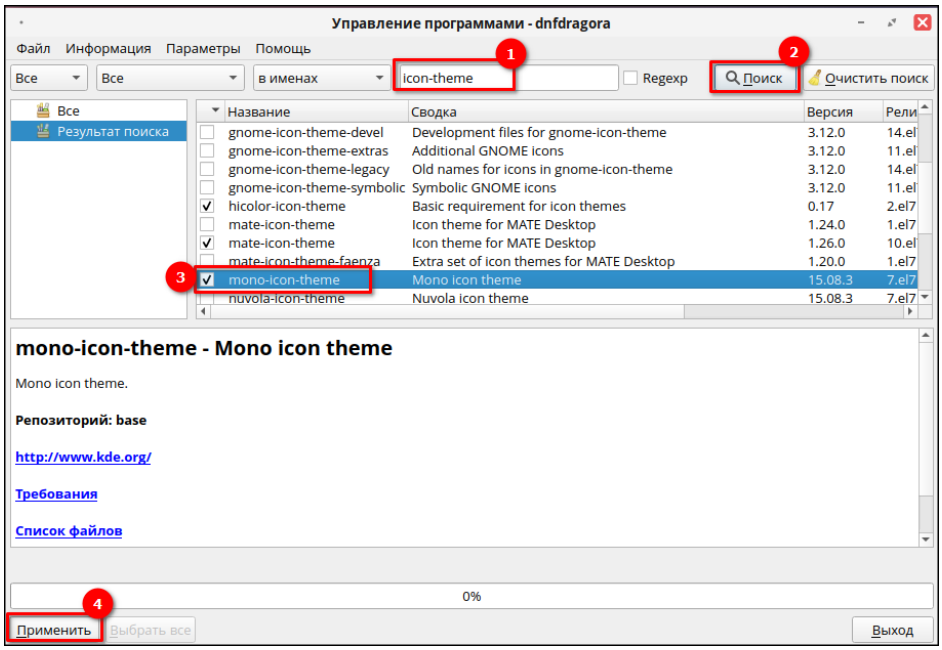
Для поиска новых тем значков через терминал выполните команду:

```
dnf search icon-theme
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы значков (потребуются права **администратора**), например:

```
dnf install nuvola-icon-theme
```

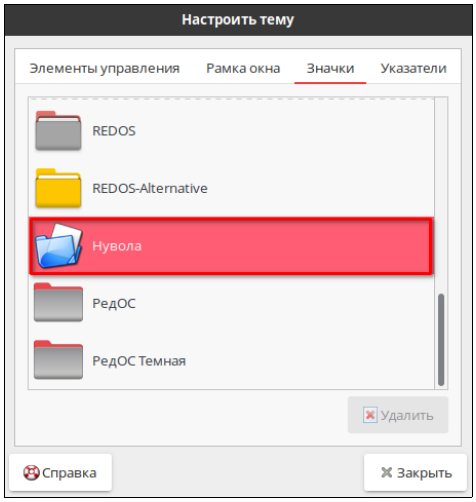
Для установки новой темы оформления значков рабочего стола через менеджер пакетов **dnfdragora** выполните поиск темы по шаблону — ***icon-theme**, выберите из списка актуальную версию пакета и нажмите кнопку « **Применить**».



Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

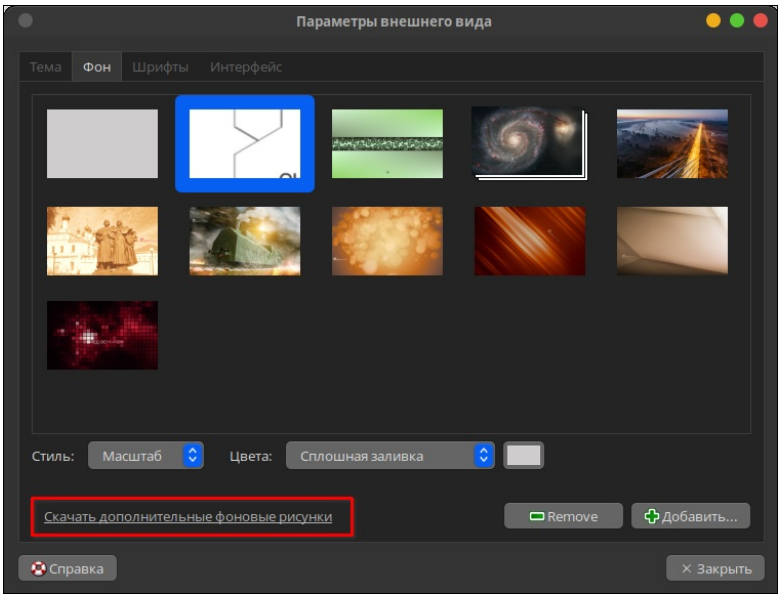
Для применения новой темы оформления значков рабочего стола перейдите в «**Параметры внешнего вида**» — «**Тема**» — «**Настроить**» — «**Значки**».



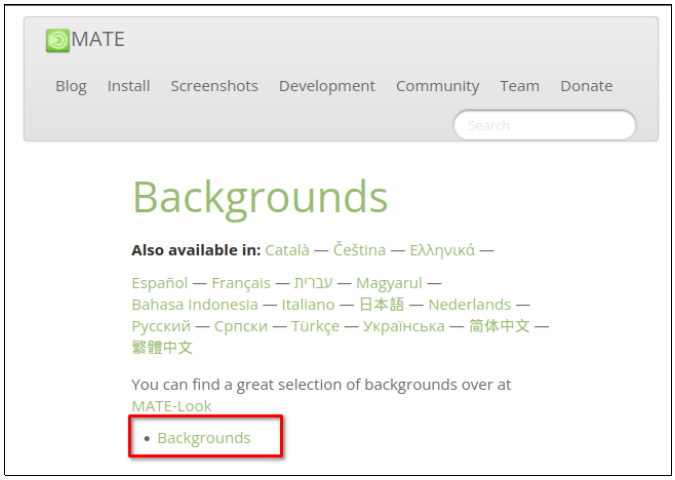
Установка нового фона рабочего стола

Для смены фона рабочего стола пользователю необходимо в системной панели выбрать пункт «**Главное меню**» — «**Параметры**» — «**Внешний вид**».

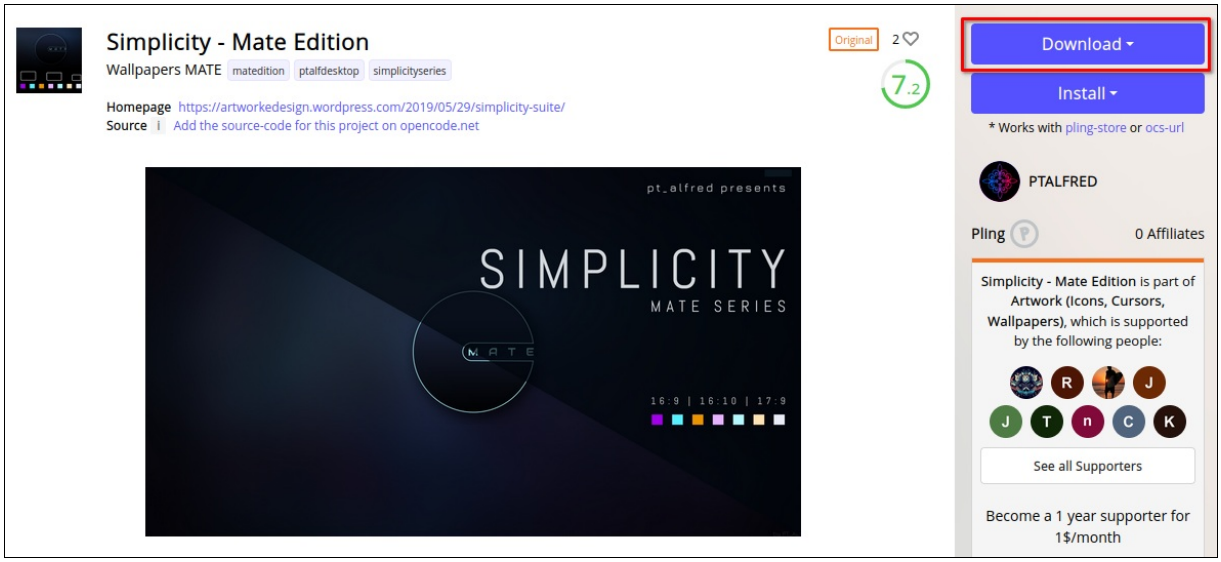
На вкладке «**Фон**» можно выбрать доступное изображение или добавить собственное, нажав кнопку «**Скачать дополнительные фоновые рисунки**».



Будет выполнено автоматическое перенаправление на страницу с изображениями рабочего стола. На загруженной странице выберите «**Backgrounds**».

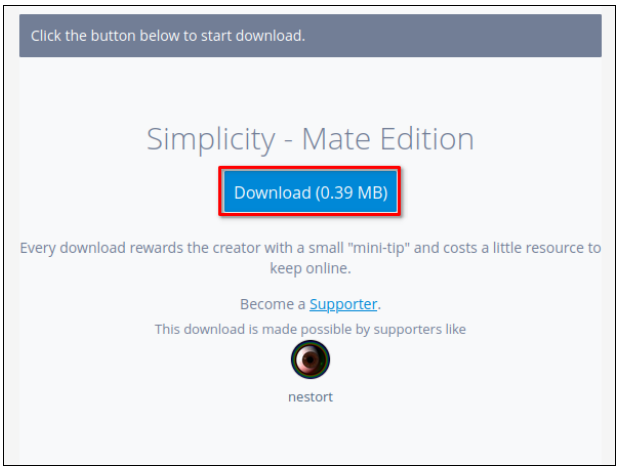


Выберите из списка понравившееся изображение и нажмите на него. Будет открыто подробное описание изображения. Для загрузки нажмите «**Download**».

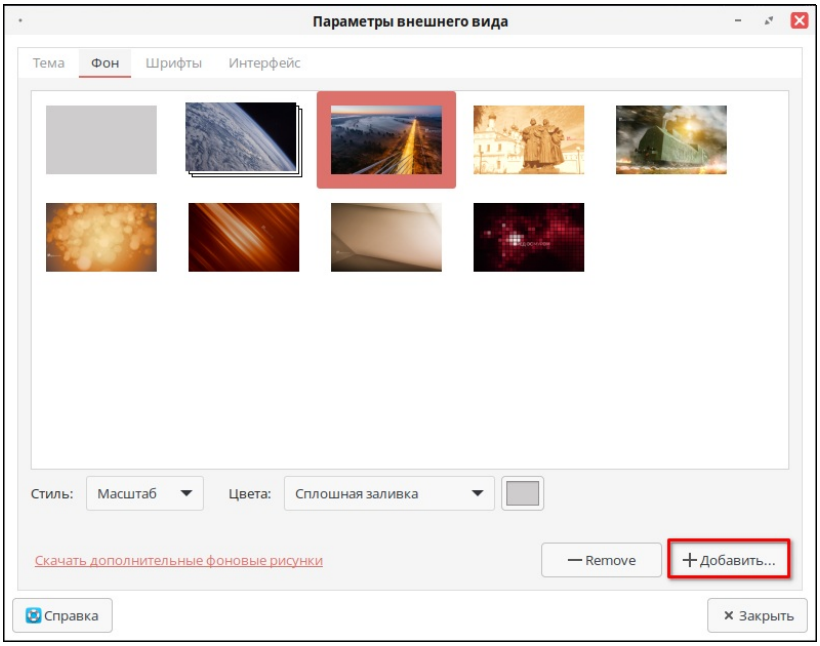


По нажатии на кнопку «**Download**» будет открыт список с доступными форматами изображения.

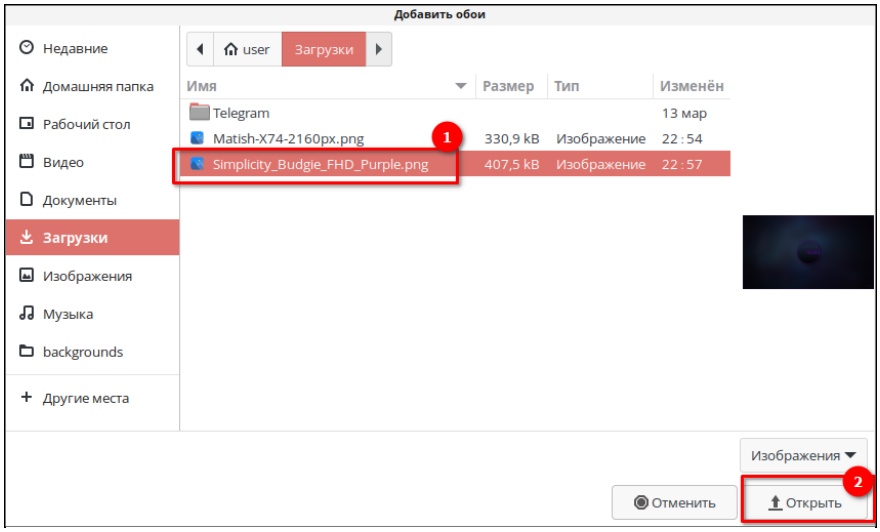
Начнется подготовка файла к скачиванию. Когда файл станет доступен для скачивания, нажмите на активную кнопку «**Download**».



Далее перейдите в «**Параметры внешнего вида**» и нажмите на кнопку «**Добавить**».



Выберите загруженное изображение для фона рабочего стола (1). Нажмите на кнопку «**Открыть**» (2).



Выбранное изображение автоматически будет установлено в качестве фона рабочего стола.

Удаление параметра темы

Можно удалять параметры элементов управления, рамок окна и значков. Для удаления какого-либо параметра выполните следующие действия:

1. Запустите инструмент «**Внешний вид**» — «**Тема**».

2. Нажмите «**Настроить**». Отобразится диалоговое окно «**Настроить тему**».

3. Щелкните по вкладке с параметром, который необходимо удалить и выберите параметр для удаления.

4. Нажмите кнопку «**Удалить**». Выбранный параметр будет удален.

Работа пользователя в РЕД ОС

Общие положения
Домашняя папка пользователя
Работа с папками и файлами
Пакет офисных приложений по работе с документами
Работа с мультимедиа
Средства коммуникации
Справочная система РЕД ОС

Вы можете подробнее ознакомиться с работой в системе, просмотрев наши обучающие видео:

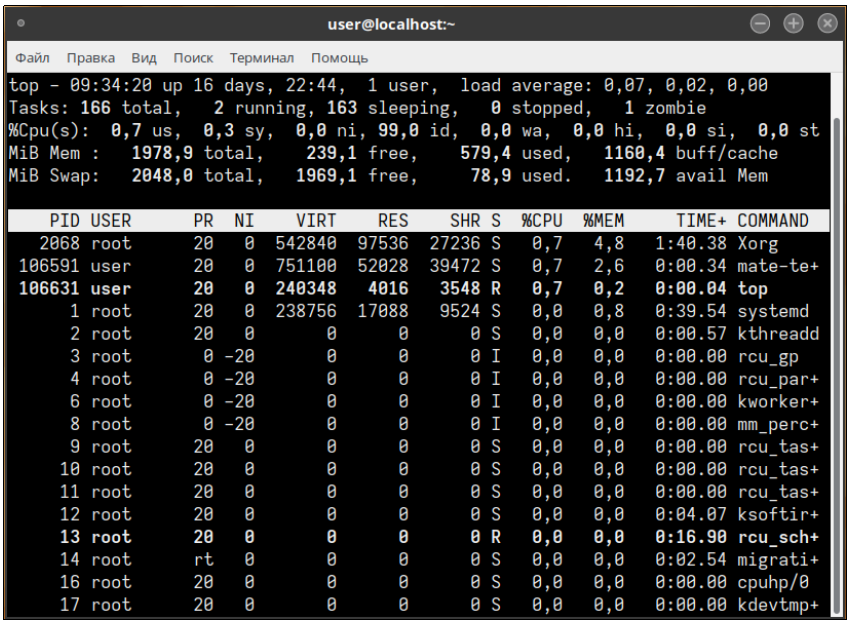
- на **RuTube** — РЕД ОС “Рабочая станция” в повседневных задачах;
- в **Яндекс.Дзен** — РЕД ОС “Рабочая станция” в повседневных задачах;
- в **VK Видео** — РЕД ОС “Рабочая станция” в повседневных задачах.

На наших каналах вы также сможете найти много другой полезной информации.

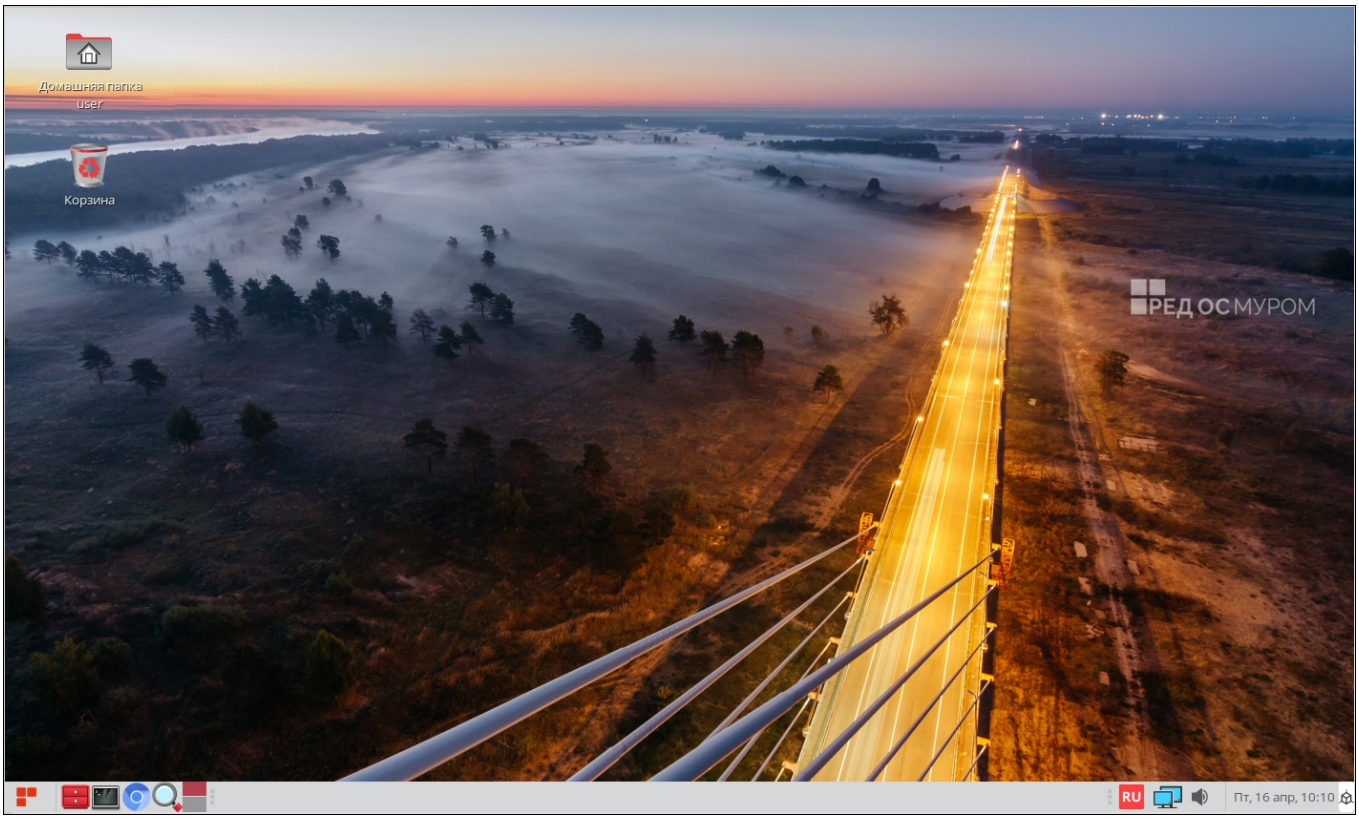
Общие положения

Работа пользователя в РЕД ОС может осуществляться в двух режимах: консольный режим и графический режим.

Консольный режим применяется в ограниченных случаях использования устаревшего программного обеспечения, конфигурирования РЕД ОС или невозможности старта графического сервера из-за сбоев РЕД ОС. Для консольного режима основным средством управления РЕД ОС является командная строка, в которой пользователь может вводить команды управления РЕД ОС. Результаты выполнения команд выводятся в консоли в виде текстовых или псевдографических сообщений.



Основным режимом работы пользователя в РЕД ОС является **графический** режим. Работа пользователя в графическом режиме производится на рабочем столе. Рабочий стол для каждого пользователя настраивается индивидуально. Настройки рабочего стола хранятся в **домашней папке** пользователя.



Навигационное пространство рабочего стола РЕД ОС состоит из трёх зон управления:

- **Системная панель** – панель, расположенная по умолчанию в нижней части экрана. Системная панель обеспечивает доступ пользователя к глобальному меню запуска всех установленных программ, содержит апплеты и элементы управления работой РЕД ОС;
- **Рабочее пространство** – все свободное пространство рабочего стола, предназначенное для расположения файлов данных и ярлыков часто используемых программ. Рабочее пространство может быть оформлено фоном рабочего стола;
- **Панель программ Mate** – панель, расположенная по умолчанию в нижней части экрана. В этой панели отображаются иконки уже запущенных программ, а также апплеты рабочих столов и корзины файлов и документов.

Управление графическим интерфейсом РЕД ОС пользователь может осуществлять при помощи мыши или клавиатуры. Правая клавиша мыши по умолчанию используется для вызова контекстных свойств любого графически представленного в интерфейсе РЕД ОС объекта. Левая клавиша мыши по умолчанию используется для инициации действий с любым графическим объектом в интерфейсе РЕД ОС.

Общие методы работы пользователя с графическим интерфейсом РЕД ОС являются общепринятыми методами работы пользователей с графическими интерфейсами операционных систем. Основными элементами графического интерфейса РЕД ОС являются окна, панели, кнопки, меню, поля ввода, списки выбора, апплеты, радиокнопки, скроллеры и т.д.

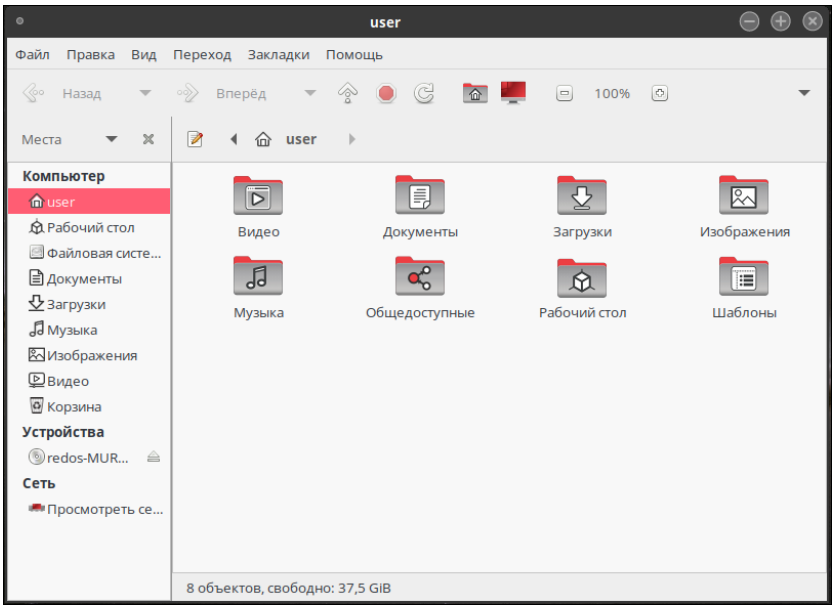
Вы можете подробнее ознакомиться с возможностями графического окружения **MATE**, просмотрев наши обучающие видео:

- на **RuTube** — Основы работы с DE Mate;
- в **Яндекс.Дзен** — Основы работы с DE Mate.

На наших каналах вы также сможете найти много другой полезной информации.

Домашняя папка пользователя

Для каждого пользователя в РЕД ОС автоматически формируется домашняя папка пользователя, которая содержит файлы и папки с данными пользователя.



Домашняя папка содержит пользовательские конфигурационные данные (профили) сервисов и функций РЕД ОС. Имена папок, начинающихся с точки и имеют атрибут «**скрытый**». Например:

/home/ivanov/.cups
/home/ivanov/.config

В домашней папке для пользователя автоматически создаются папки для хранения различных широко распространённых типов файлов. Например: «**Документы**», «**Изображения**», «**Музыка**», «**Видео**».

Все домашние папки пользователей расположены в едином каталоге пользователей **/home**.

Имена домашних папок пользователей совпадают с именами (логинами) пользователей в системе. Например:

/home/ivanov/
/home/sorokina/
/home/kiselev/

Пользователь может перейти в домашнюю папку по ссылке (ярлыку) на рабочем столе.

Все программы в РЕД ОС по умолчанию сохраняют редактируемые пользователем файлы в домашнюю папку пользователя.

Пользователь имеет полный доступ к файлам и папкам в своём домашнем каталоге. Однако пользователь имеет ограниченный доступ к домашним папкам и файлам в них других пользователей.

Работа с папками и файлами

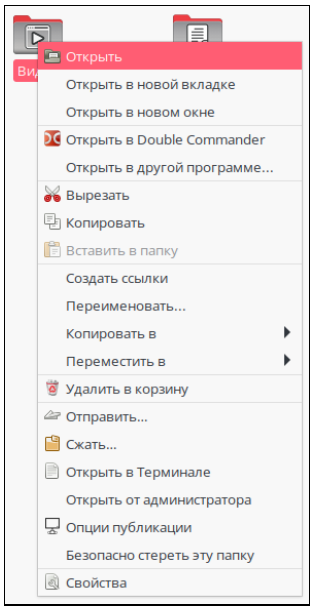
Помимо домашней папки пользователь может работать с файлами и папками в файловой системе РЕД ОС. Возможность работы с файлами и папками РЕД ОС определяется правами доступа пользователя, устанавливаемыми администратором РЕД ОС.

Пользователь может осуществлять работу с папками и файлами в РЕД ОС несколькими способами:

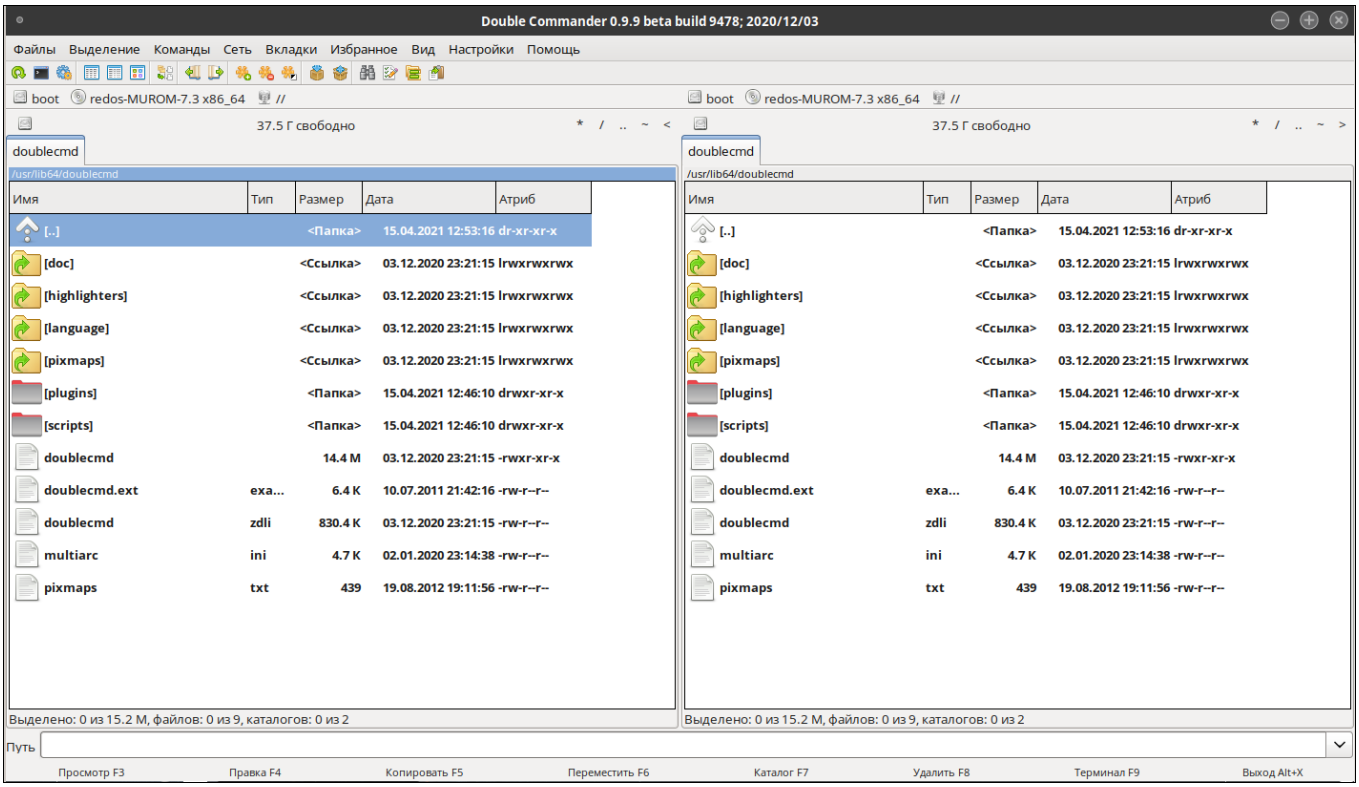
- при помощи стандартного менеджера файлов графического окружения;
- при помощи специализированных программ, например **MidnightCommander**.

После запуска менеджера файлов откроется окно, в котором пользователь может в графическом режиме перемещаться по файловой системе РЕД ОС и выполнять доступные операции с папками и файлами.

Действия с папками и файлами в стандартном обозревателе файлов выполняются при помощи мыши и клавиатуры. Стандартный обозреватель поддерживает технологию перетаскивания «мышью» (drag and drop). Доступные пользователю операции с файлами и папками можно увидеть в контекстном меню графического объекта при активации его правой функциональной клавишей мыши.

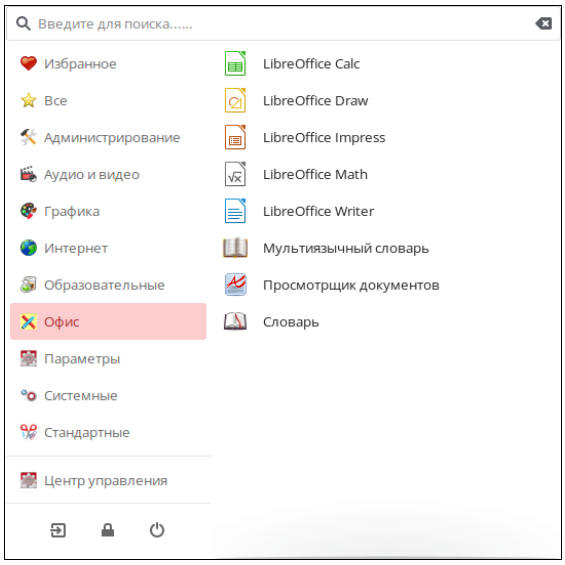


Управление файлами и папками пользователь также может совершать при помощи двухпанельных файловых менеджеров, таких как **MidnightCommander** или **Double Commander**.



Пакет офисных приложений по работе с документами

В качестве средств работы с текстовыми и табличными документами пользователю доступен пакет офисных приложений **LibreOffice**. Пакет офисных приложений доступен пользователю в «**Главном меню**» - «**Офис**».



В состав пакета включены следующие программные средства:

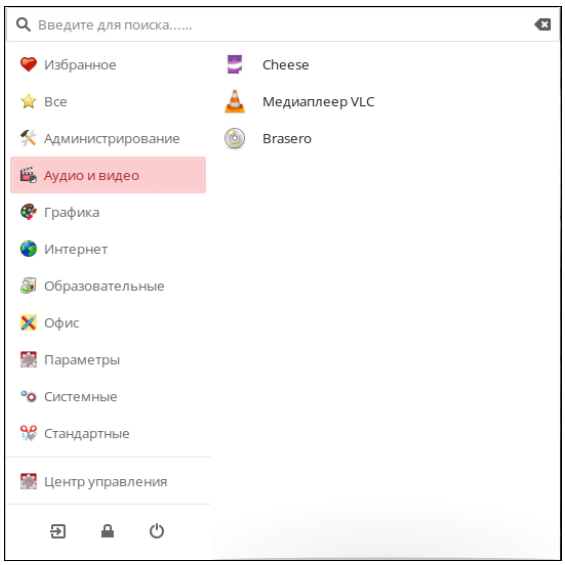
- *LibreOffice Calc* - табличный процессор;
- *LibreOffice Draw* - векторный графический редактор;
- *LibreOffice Impress* - программа подготовки презентаций;
- *LibreOffice Writer* - текстовый редактор и визуальный редактор HTML.

Пакет интегрирован в графическую оболочку РЕД ОС и автоматически открывается в случае, если пользователь производит запуск файла соответствующего формата.

Пакет полностью русифицирован и обеспечивает поддержку документов, созданных средствами различных текстовых и табличных редакторов, в том числе документы *Microsoft Word*.

Работа с мультимедиа

Пользователю в РЕД ОС для работы с мультимедиа-файлами доступен набор программ, который расположен в «**Главном меню**» - «**Аудио и видео**».



В состав пакетов для работы с мультимедиа-форматами по умолчанию включены следующие программные средства:

- приложение для записи дисков Brasero, который обеспечивает запись мультимедийных дисков и дисков с данными на оптические носители информации CD/DVD;
- фото-, видео-будка Cheese, которая обеспечивает работу с веб-камерами;
- утилита настройки звука.

Пакеты для работы с мультимедиа интегрированы в графическую оболочку РЕД ОС, и соответствующие приложения автоматически открываются в случае, если пользователь производит запуск файла определённого мультимедийного формата.

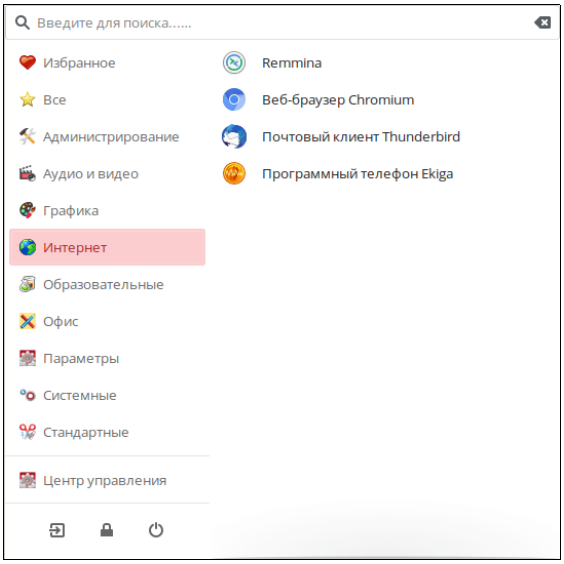
Для обеспечения возможности работы с некоторыми форматами требуется дополнительная установка кодеков мультимедийных

форматов. Установка дополнительных кодеков требует административных полномочий администратора РЕД ОС.

Описанные программные средства имеют интуитивно понятный интерфейс и снабжены контекстной справочной системой.

Средства коммуникации

Для обеспечения комфортной работы в сети Интернет в состав РЕД ОС включен набор необходимых приложений, доступный в «**Главном меню**» - «**Интернет**».



Remmina — это свободный клиент удаленного рабочего стола для компьютерных операционных систем. Он поддерживает протокол удаленного рабочего стола (RDP), протоколы VNC, NX, XDMCP, SPICE и SSH.

Chromium — веб-браузер с открытым исходным кодом, разрабатываемый сообществом The Chromium Authors, компанией Google и некоторыми другими компаниями. Chromium предназначен для предоставления пользователям быстрого, безопасного и надёжного доступа в Интернет, а также удобной платформы для веб-приложений.

Почтовый клиент **Thunderbird** — бесплатная кроссплатформенная свободно распространяемая программа для работы с электронной почтой и группами новостей, а при установке расширения Lightning - с календарём. Поддерживает протоколы: SMTP, POP3, IMAP, NNTP, RSS.

Ekiga — приложение для IP-телефонии и проведения видеоконференций, которое ранее называлось *GnomeMeeting*. **Ekiga** поддерживает протоколы **SIP** и **H.323** (с помощью **penH323**) и способна взаимодействовать с другими **SIP** и **H.323**-совместимыми клиентами, а также с *Microsoft NetMeeting*. Поддерживает множество аудио- и видеокодеков высокого качества.

Примечание.

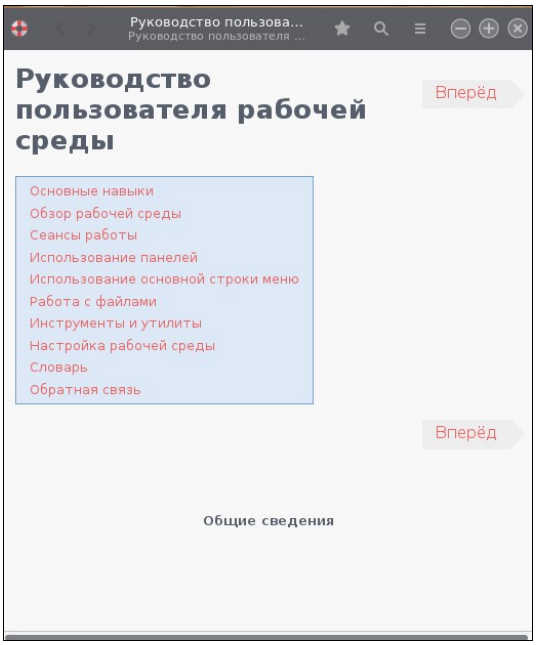
В **РЕД ОС 8** поддержка **Ekiga** прекращена. Для организации видеоконференций и звонков рекомендуется использовать кроссплатформенный программный клиент IP-телефонии **Linphone** или систему интернет-телефонии и мгновенного обмена сообщениями **Jitsi**.

Справочная система РЕД ОС

В РЕД ОС интегрирована расширенная справочная система, которая позволяет пользователю найти более подробную информацию по функциям и возможностям системы.

Доступ к справочной системе пользователю предоставляется при нажатии

правой кнопки мыши на системной панели и выборе пункта «Справка».


Руководство пользова...
Руководство пользователя ...
Руководство пользователя рабочей среды
Вперёд
Основные навыки
Обзор рабочей среды
Сеансы работы
Использование панелей
Использование основной строки меню
Работа с файлами
Инструменты и утилиты
Настройка рабочей среды
Словарь
Обратная связь
Вперёд
Общие сведения

Настройка среды рабочего стола

Установка
Работа с утилитой
Рабочий стол
Панель
Окна

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** mate-tweak 20.04.0-1

mate-tweak – утилита для точной настройки среды рабочего стола.

С ее помощью можно управлять значками рабочего стола и изменять настройки интерфейса для значков, контекстных меню или панелей инструментов.

Установка

Для установки перейдите в сеанс пользователя **root**:

```
su -
```

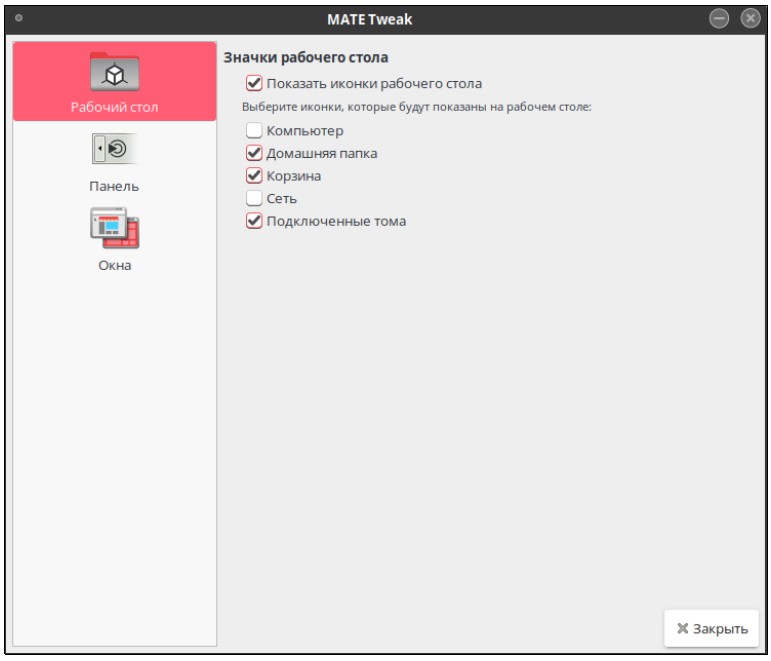
и выполните команду:

```
dnf install mate-tweak
```

После установки утилита доступна из «**Главного меню**» - «**Параметры**» - «**MATE Tweak**».

Работа с утилитой

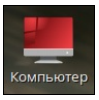
Окно программы выглядит следующим образом:

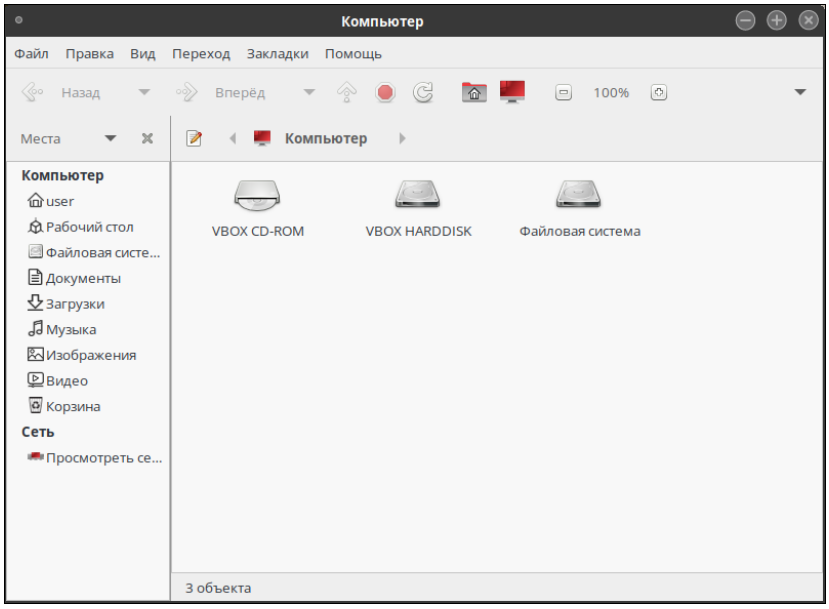


В программе имеется три вкладки: **Рабочий стол**, **Панель** и **Окна**.

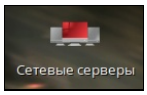
Рабочий стол

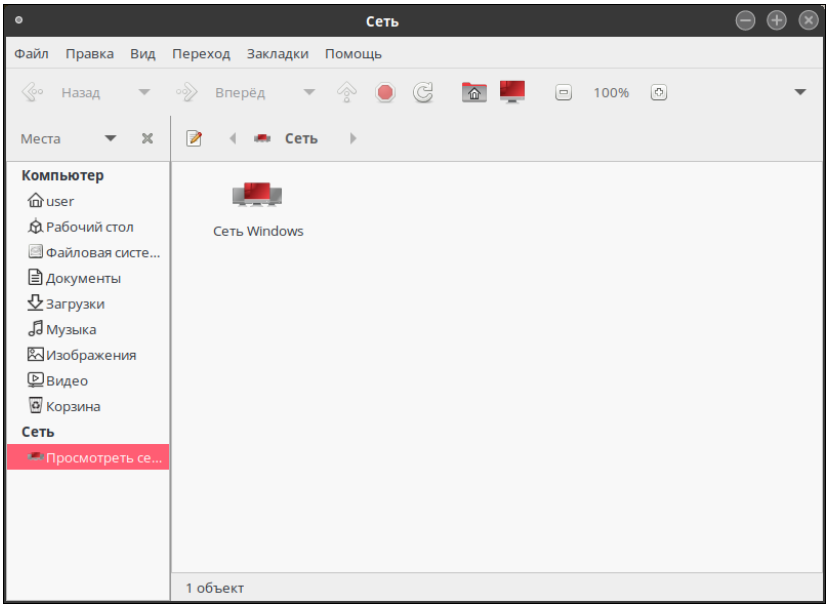
На вкладке **Рабочий стол** можно редактировать рабочий стол MATE, включать или отключать отображение иконок, отвечающих за различные функции. По умолчанию включены иконки **Домашняя папка**, **Корзина** и **Подключенные тома**. По желанию можно включить иконку **Компьютер**, которая будет отображать все подключенные к компьютеру носители.





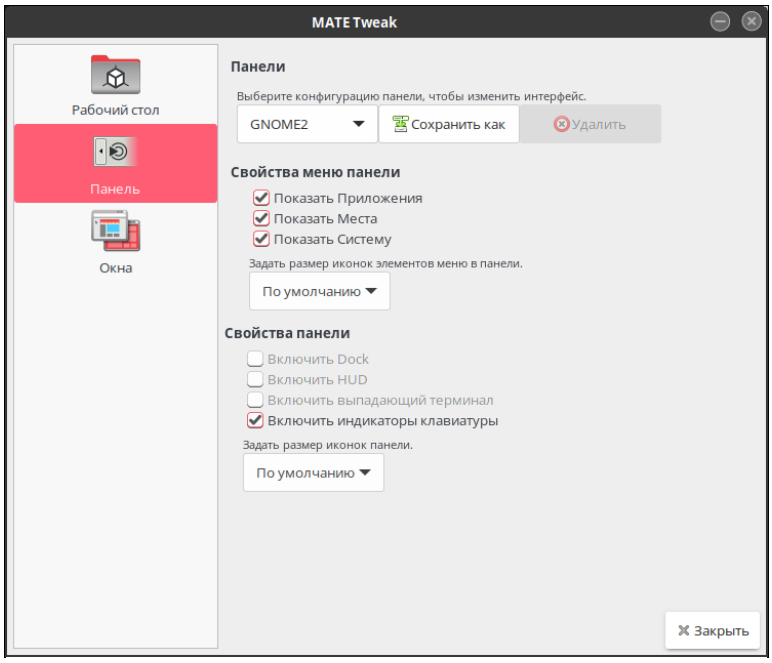
Также можно включить иконку **Сеть**, которая будет отображать сетевое окружение машины.



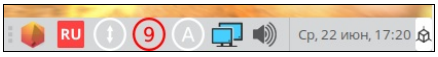


Панель

На вкладке **Панель** можно настроить нижнюю панель: включить или отключить отображение различных элементов панели, изменить их размеры, а также размеры самих иконок. Выполненные изменения можно сохранить в отдельный профиль и присвоить ему название.



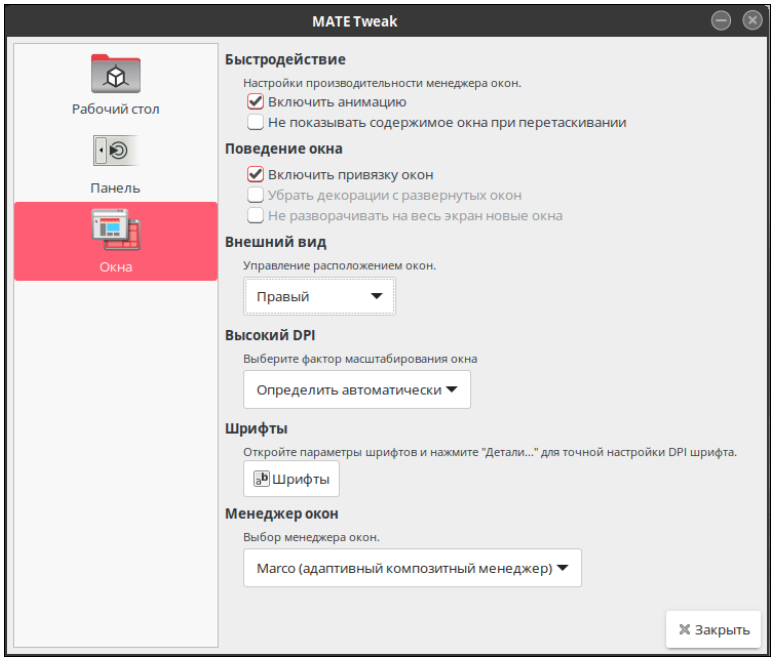
Также можно включить индикатор клавиатуры, он будет расположен в правой части панели. Он позволит увидеть состояния клавиатуры: включен ли **Scroll Lock**, **Num Lock** или **Caps Lock**.



Белый цвет означает неактивное состояние, красный – активное.

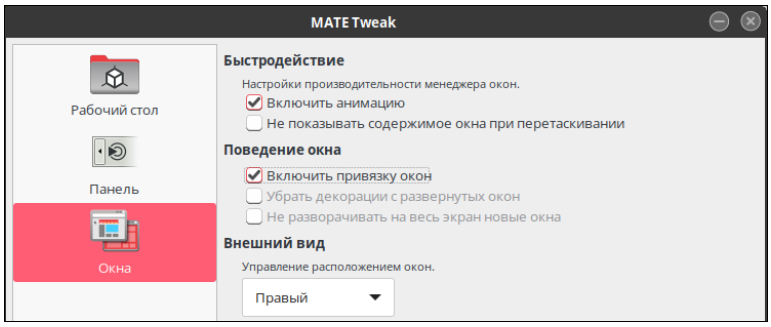
Окна

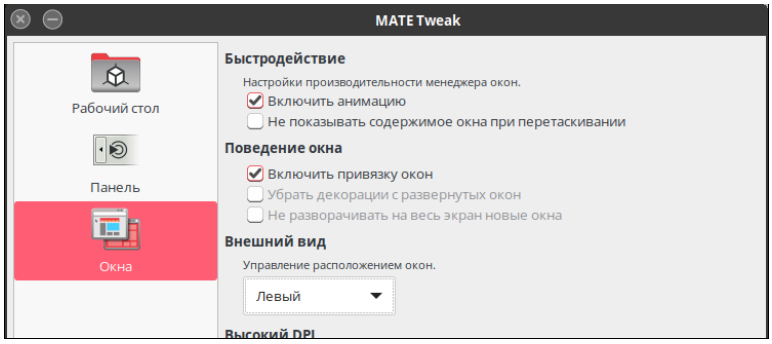
На вкладке **Окна** можно настроить свойства окон: отображение анимации свертывания и развертывания, содержимое окон при перетаскивании.



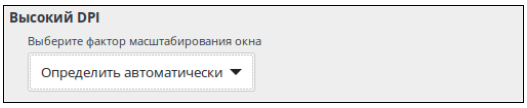
Надстройка **Включить привязку окон** позволяет при перетаскивании окна к краю экрана растянуть его по вертикали и покрыть половину рабочего пространства. По желанию, эту надстройку можно отключить.

Также можно изменить положение самого окна – привычное правое или левое.

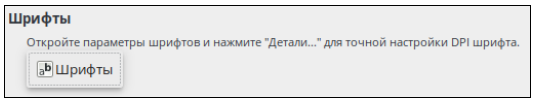




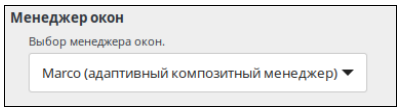
Надстройка **Высокий DPI** позволяет увеличивать размер всех окон, панелей, виджетов, шрифтов и прочего для дисплеев с высокими значениями DPI. По умолчанию данное значение выбирается автоматически.



Надстройка **Шрифты** позволяет поменять шрифты в системе и изменить их размер.



Надстройка **Менеджер окон** позволяет изменить менеджер окна, используемого в системе. По умолчанию установлен менеджер окна **Marco**.



Привилегии и root

Вы можете подробнее ознакомиться с привилегиями пользователя **root** и их использованием в работе, просмотрев наши обучающие видео:

- на **RuTube** — Привилегии и root;
- в **Яндекс.Дзен** — Привилегии и root;
- в **VK Видео** — Привилегии и root.

На наших каналах вы также сможете найти много другой полезной информации.

Правила хорошего тона при работе

Правило 1.

Никогда не выполняйте под правами администратора пользовательскую работу! Бороздить бескрайние просторы интернета, читать и отправлять почту, набирать текстовые документы и рисовать изображения — всё это можно и нужно делать под правами обычного пользователя!

Правило 2.

При необходимости выполнить действия, требующие администраторских прав, не регистрируйтесь в системе как **root**, а используйте утилиты **sudo** или **su**! Если Вам потребовалось установить какой-либо пакет или внести изменения в системные настройки, то воспользуйтесь данными утилитами как в терминальном окне, так и в полном консольном режиме. Применяя утилиту **su** (повышение привилегий) в интерактивном режиме (то есть фактически создавая отдельный терминальный сеанс), не забывайте после выполнения требуемых задач завершать работу данного сеанса, а не оставлять его «висящим» в системе на всякий случай.

Правило 3.

Запуская службы, старайтесь по возможности давать им пониженные права! Это верно как для уже готовых пакетов, когда имя пользователя, с чьими правами будет работать служба, задаётся в файлах конфигурации, так и для программного обеспечения, которое Вы пишите самостоятельно. Каким бы важным не был сервис (веб-сервер, служба DNS или почтовый сервис), ему нет необходимости работать с эффективными правами пользователя **root** — достаточно и прав порою даже меньше, чем у «обычного» пользователя.

Правило 4.

Можно не входить в систему как **root** и даже не использовать утилиты **sudo** или **su** — достаточно на часто запускаемые файлы установить бит **SUID**, и тогда пользователю, запускающему эти программы многое станет доступно без поднятия привилегий. Ни в коем случае так нельзя делать! Использование битов **SUID/SGID** должно быть под полным запретом в Вашей практике!

Утилиты su и sudo

sudo - это программа, разработанная в помощь системному администратору и позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы. Основная идея - дать пользователям как можно меньше прав, но при этом ровно столько, сколько необходимо для решения поставленных задач.

Команда **sudo** предоставляет возможность пользователям выполнять команды от имени *root* или других пользователей. Правила, используемые **sudo** для принятия решения о предоставлении доступа, находятся в файле **/etc/sudoers**. Кроме того, пример правил, предоставляющих пользователям, являющимися членами группы **rpm**, возможность устанавливать, обновлять и удалять пакеты в системе, приведен в файле **/usr/share/doc/sudo-/sample.sudoers**.

Для редактирования файла **/etc/sudoers** следует использовать программу **visudo**, которая проверяет синтаксис и, тем самым, позволяет избежать ошибок в правилах.

В большинстве случаев, грамотная настройка **sudo** делает работу от имени суперпользователя ненужной.

Команда **su** позволяет изменить привилегии на любого имеющегося в системе пользователя, в связи с чем синтаксис команды следующий:

```
su <имя_пользователя> <опции>
```

Если не указать имя пользователя, то по умолчанию считается, что это — **root**, то есть выполнение команды без аргументов «**su**» означает «**su root**».

Из опций наиболее значимой является:

«**-c**» — позволяет выполнить команду, указанную после данного ключа в кавычках, и завершить работу утилиты.

Например:

```
su -c "dnf update"
```

«-» или «**-l**» — при получении привилегий другого пользователя запускается отдельная оболочка со значениями переменных окружения того пользователя, чьи привилегии мы получаем.

То есть, выполнив из-под пользователя ivanov команду «**su**», мы останемся в том же рабочем окружении, что и были (то есть получив права супер-администратора, всё равно нашим домашним каталогом останется **/home/ivanov**, а также все переменные рабочего окружения оболочки).

Следовательно, если какая-то программа или команда захочет что-то записать в домашнюю папку, то она сделает это в каталоге /home/ivanov, но владельцем файла установит уже пользователя **root**, что потом при работе с правами пользователя ivanov не позволит этот файл редактировать, удалить и т. д. Совсем плохо, если этим файлом окажется какой-то из файлов конфигурации.

Поэтому, запомните как ещё одно правило:

Правило 5.

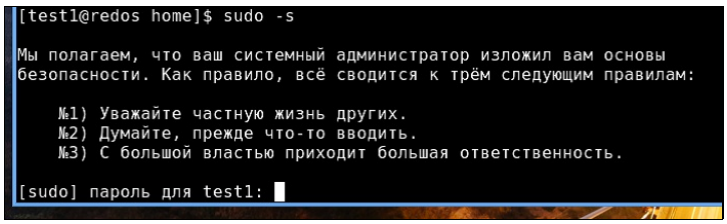
Используя команду **su**, обязательно выполняйте её с аргументом «**-**»:

```
su -
```

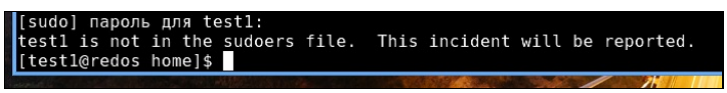
Пример, демонстрирующий различие в переменных окружения между **su** и **su -** :



При первом использовании команды **sudo** на экран будет выведено следующее предупреждение:



И после ввода пароля пользователя может быть выдано следующее сообщение:



Это означает, что при установке РЕД ОС на шаге создания пользователя Вы не установили флажок «**Сделать этого пользователя администратором**». Но это поправимо! Достаточно внести нашего пользователя в группу **wheel**, для чего нужно из-под администратора **root** выполнить следующую команду:

```
usermod -aG wheel <имя_пользователя>
```

Если пользователь, которому менялось членство в группах, находился в системе, то необходимо завершить сеанс работы и войти в систему заново. После этого использование утилиты **sudo** станет возможным. Соответственно, если необходимо убрать у пользователя право пользоваться командой **sudo**, то достаточно удалить его из группы **wheel**.

Ниже приведена таблица различий использования команд **su** и **sudo**.

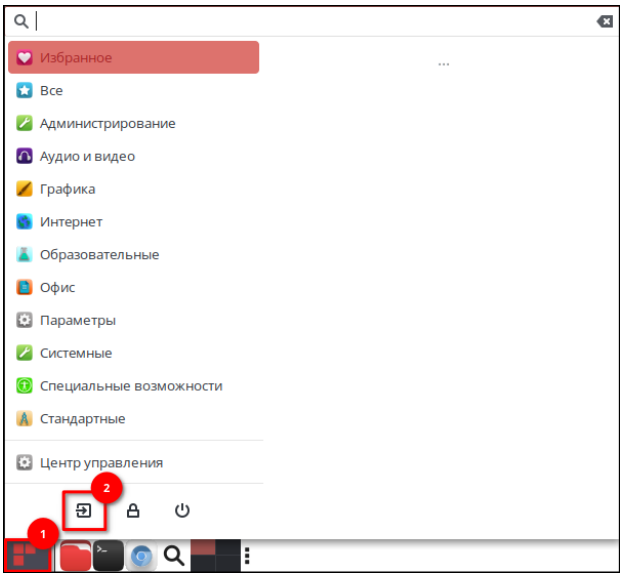
Команда	Описание	Текущий каталог (pwd)	$HOME	$LOGNAME	$USER	$USERNAME	$PATH	DESKTOP_SESSION (export | grep mate)	Комментарий
su	При вызове **su** без аргументов по умолчанию запускается shell пользователя root, но сохраняется прежняя среда	не изменяется	/root	user	user	user	/home/user/.local/bin:/home/user/bin: /usr/share/Modules/bin:/usr/local/bin: /usr/bin:/usr/local/sbin:/usr/sbin	DESKTOP_SESSION="mate"	
su - или su -l	Запустить shell в его начальной среде, как если бы root действительно зарегистрировался в системе. Оболочка получает правильный environment. **Чистая сессия root**	изменяется на /root	/root	root	root	пусто	/usr/share/Modules/bin:/usr/local/sbin: /usr/local/bin:/usr/sbin:/usr/bin:/root/bin	пусто	Рекомендовано к использованию
su root	Аналогично команде su	не изменяется	/root	user	user	user	/home/user/.local/bin:/home/user/bin: /usr/share/Modules/bin:/usr/local/bin: /usr/bin:/usr/local/sbin:/usr/sbin	DESKTOP_SESSION="mate"	
su - root	Аналогично su -l или su -	изменяется на /root	/root	root	root	пусто	/usr/share/Modules/bin:/usr/local/sbin: /usr/local/bin:/usr/sbin:/usr/bin:/root/bin	пусто	Рекомендовано к использованию
su root -	Аналогично команде su или su root	не изменяется	/root	user	user	user	/home/user/.local/bin:/home/user/bin: /usr/share/Modules/bin:/usr/local/bin: /usr/bin:/usr/local/sbin:/usr/sbin	DESKTOP_SESSION="mate"	
sudo -i	Получить оболочку root и его environment. Разрешено, если пользователь добавлен в /etc/sudoers	изменяется на /root	/root	root	root	user	/usr/share/Modules/bin:/usr/local/sbin: /usr/local/bin:/usr/sbin:/usr/bin:/root/bin	пусто	Рекомендовано к использованию
sudo su	Получить оболочку root и его environment. Разрешено, если пользователь добавлен в sudoers	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	пусто	
sudo -s	Команда запускает shell пользователя root, но без смены текущего каталога, при этом не импортируются некторые переменные окружения	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	пусто	
sudo <команда>	Команда исполняется от пользователя root	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	пусто	
sudo -E	Выполнение команд от root с сохранением переменных окружения пользователя	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	DESKTOP_SESSION="mate"	

Блокирование сеанса и завершение работы с РЕД ОС

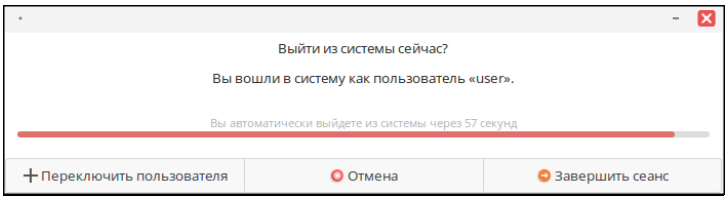
Завершение сеанса
Блокирование сеанса
Завершение работы

Завершение сеанса

Если необходимо полностью завершить сеанс, пользователь должен перейти в «**Главное меню**» (1) — «**Завершить текущий сеанс**» (2).



Система перейдет в окно выбора пользователей.

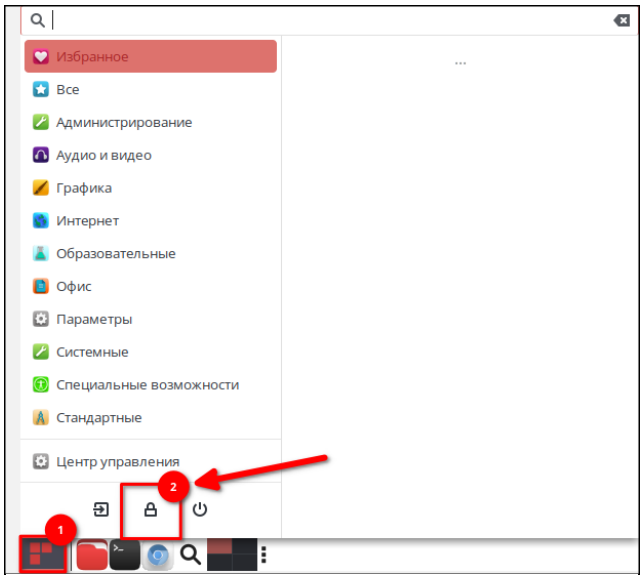


В открывшемся окне пользователь должен выбрать требуемое действие:

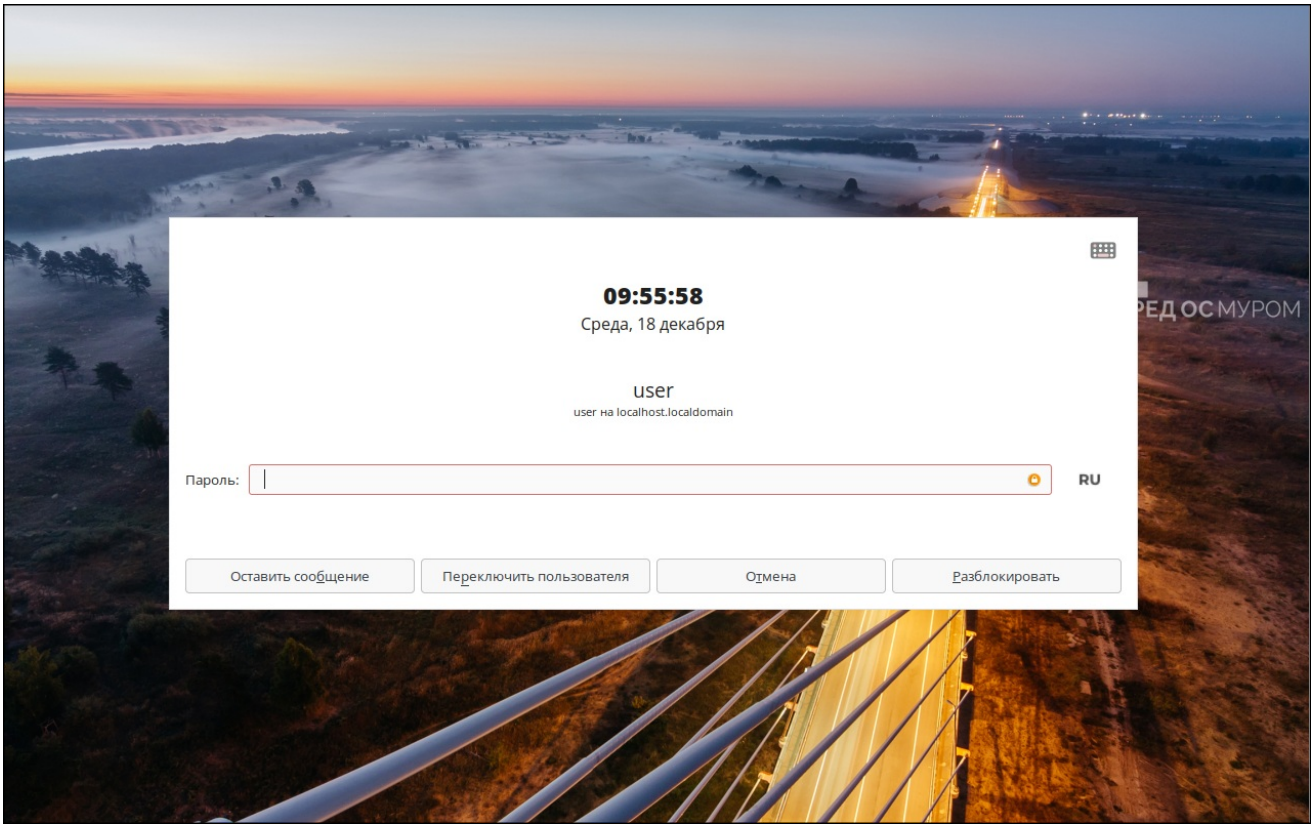
- **Переключить пользователя** — система сохраняет текущее состояние сеанса пользователя (открытые окна, запущенные программы), но переводит устройство в режим выбора пользователей;
- **Отмена** — отменяет операции выхода из системы;
- **Завершить сеанс** — система завершает текущий сеанс пользователя, закрывает все открытые приложения и документы, а также полностью выходит из учетной записи.

Блокирование сеанса

Для блокирования сеанса пользователя необходимо перейти в «**Главное меню**» (1) — «**Заблокировать экран**» (2).



В результате выполненных действий сеанс пользователя будет приостановлен, на экране появится хранитель экрана, дальнейшая работа возможна только после разблокировки экрана с вводом пароля пользователя.

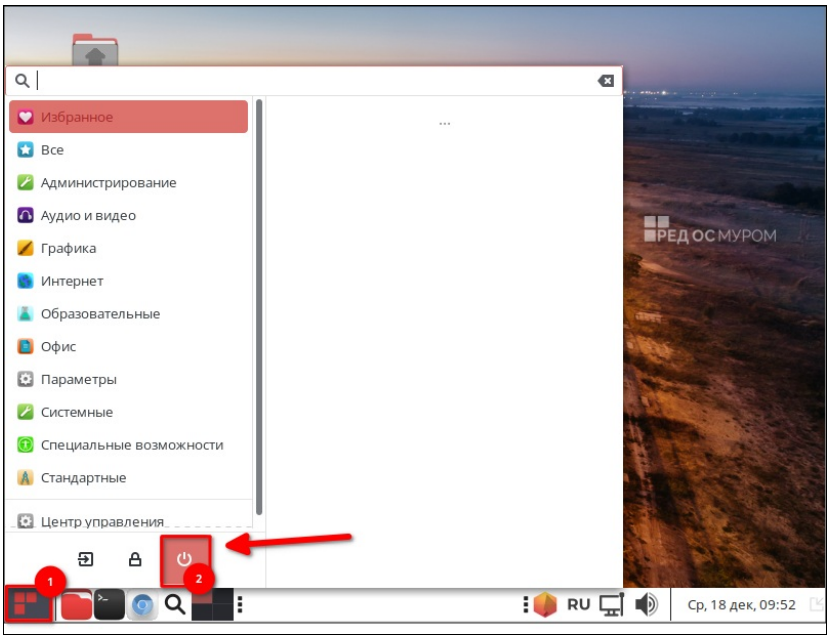


В открывшемся окне пользователь должен выбрать требуемое действие:

- **Оставить сообщение** — эта кнопка позволяет оставить текстовое сообщение для пользователя, который войдет в систему после разблокировки экрана;
- **Переключить пользователя** — этот вариант позволяет быстро сменить активного пользователя, не закрывая текущие приложения и программы;
- **Отмена** — кнопка отмены возвращает пользователя обратно в хранитель экрана, если он после ввода пароля передумал разблокировать экран;
- **Разблокировать** — после ввода пароля эта кнопка снимает блокировку экрана.

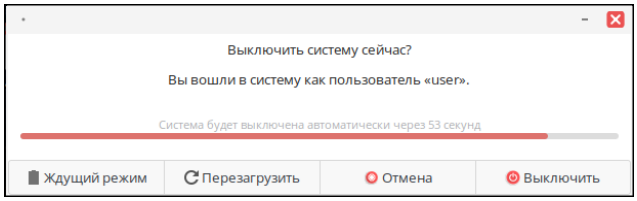
Завершение работы

Для завершения работы в РЕД ОС и выключения компьютера пользователю необходимо перейти в «**Главное меню**» (1) — «**Выключить устройство**» (2).



В открывшемся окне пользователь должен выбрать требуемое действие:

- **Ждущий режим** — энергосберегающий режим работы компьютерного оборудования. Назначение режима — уменьшение потребления энергии устройством во время простоя. Для ждущего режима требуется аппаратная поддержка со стороны оборудования;
- **Перезагрузить** — выполняется перезагрузка и возвращение РЕД ОС в рабочее состояние;
- **Отмена** — отменяет операции завершения работы с РЕД ОС;
- **Выключить** — действие производит корректное выключение РЕД ОС с остановкой всех служб и последующим автоматическим выключением питания СВТ.



Для корректного завершения работы ОС (перезагрузки) во время ее работы **ЗАПРЕЩАЕТСЯ** выключать питание или нажимать на кнопку «**Reset**». Перед окончанием работы с ОС пользователь должен завершить все работающие программы.

Ядро ОС

Ядро является основным компонентом операционной системы (ОС) и основным интерфейсом между аппаратным обеспечением компьютера и его процессами. Оно обеспечивает взаимодействие между этими двумя системами, максимально эффективно управляя ресурсами.

Ядро существует в операционной системе и управляет всеми основными функциями аппаратного обеспечения.

Ядро выполняет 5 основных функций:

1. *Управление памятью* – отслеживает объемы памяти для хранения тех или иных объектов и освобождает оперативную память. Ядро следит за доступом к памяти и позволяет процессам использовать адресное пространство, превышающее физическую память, гарантируя, что данные не будут случайно перезаписаны.

2. *Управление процессами* – управляет созданием, планированием и завершением процессов, обеспечивая механизм многозадачности, позволяя нескольким процессам выполняться практически одновременно.

3. *Взаимодействие драйверов устройств* – ядро управляет взаимодействием с устройствами, такими как жесткие диски, клавиатуры, мыши, сетевые интерфейсы.

4 . *Управление файловой системой* – управляет структурой хранения данных на диске и обеспечивает безопасность файлов и каталогов.

5. *Сетевое взаимодействие* – управляет сетевыми соединениями и реализует сетевые протоколы.

Ядро, если оно реализовано должным образом, невидимо для пользователя и работает в собственном разделе системы, известном как пространство ядра, где оно выделяет память и отслеживает, где что хранится. То, что видит пользователь — например, веб-браузеры и файлы – называется *пользовательским пространством*. Эти приложения взаимодействуют с ядром через интерфейс системных вызовов (SCI).

Ядро операционной системы обеспечивает взаимодействие между аппаратным обеспечением и программным обеспечением. Оно выполняет множество функций, включая управление процессами, памятью, файловыми системами и сетями. Понимание работы ядра и различных его архитектур помогает разработчикам и системным администраторам более эффективно использовать ресурсы компьютера и разрабатывать надежные приложения.

Загрузчик ОС

После включения питания компьютера запускается процедура самотестирования (Power On Self Test, POST), проверяющая основные компоненты системы: видеокарту, оперативную память, жесткие диски и т. д. Затем начинается загрузка операционной системы. Компьютер при этом выполняет поиск на жестком диске (и других носителях) программы-загрузчика операционной системы. Если такая программа найдена, ей передается управление; если же такая программа не найдена ни на одном из носителей, выдается сообщение с запросом на подключение загрузочного диска.

В настоящее время актуален только один загрузчик: GRUB2 — он используется по умолчанию в большинстве дистрибутивов и после установки РЕД ОС начальным загрузчиком будет именно он.

Задача загрузчика — предоставить пользователю возможность выбрать нужную операционную систему (для случаев, когда кроме РЕД ОС на компьютере установлены дополнительные операционные системы) и передать ей управление. В случае с РЕД ОС загрузчик загружает ядро операционной системы и передает управление ему. Все последующие действия по загрузке системы: монтирование корневой файловой системы, запуск программы инициализации — выполняет ядро ОС.

Файловая система в РЕД ОС

Журналируемые и нежурналируемые файловые системы
Файлы
Устройства
Монтирование устройств
Каталоги файловой системы РЕД ОС
Основные команды для работы с файлами и файловой системой
Навигация
Операции с файлами
Операции с каталогами
Мягкие и жесткие ссылки
Примеры создания ссылок

Файл — это поименованная область памяти. Если память «долгосрочная» и информация в ней хранится на дисковых или подобных им носителях (например, USB-накопители), то поименованными областями являются имеющиеся на них файлы.

Упрощённо можно сказать, что совокупность файлов, структурированная в соответствии с унифицированными требованиями на физическом носителе, представляет собой **файловую систему** (**ФС**). Файловая система определяет порядок/способ хранения данных на носителях, допустимый размер имён файлов и каталогов, формат, количество и объём метаданных.

Метаданные — это дополнительная информация о файле, то, что в повседневном использовании называется «свойства файла».

Вы можете подробнее ознакомиться с поддерживаемыми файловыми системами в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Файловая система в РЕД ОС;
- в **Яндекс.Дзен** — Файловая система в РЕД ОС;
- в **VK Видео** — Файловая система в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Журналируемые и нежурналируемые файловые системы

Файловые системы можно классифицировать по различным признакам, далее будет рассмотрен вариант классификации на журналируемые и нежурналируемые файловые системы.

К **журналируемым** файловым системам относятся те, которые сохраняют список изменений, осуществляемых с файловой системой, перед фактическим их применением. Такие записи хранятся в отдельной части файловой системы, называемой журналом. Как только изменения файловой системы внесены в журнал, она применяет изменения к файлам или метаданным, а затем удаляет эти записи из журнала.

К **нежурналируемым** файловым системам относятся **ext2** и **FAT** (*FAT12, FAT16, FAT32*). Ядро ОС их также поддерживает.

При перезагрузке компьютера программа монтирования может гарантировать целостность журналируемой файловой системы простой проверкой журнала на наличие ожидаемых, но не произведённых изменений и последующей записью их в файловую систему. Т.е. при наличии журнала в большинстве случаев системе не нужно проводить проверку целостности файловой системы. Соответственно, шансы потери данных в связи с проблемами в файловой системе значительно снижаются.

Для рабочих станций в РЕД ОС используется журналируемая файловая система **ext4** — логическое продолжение **ext3**, которая является журналируемым вариантом системы **ext2** — «материнской» файловой системы Linux.

В зависимости от указанных администратором настроек файловая система **ext4** может работать в любом из трёх известных для журналируемых систем режиме:

- в режиме обратной связи — журналируются только метаданные;
- упорядочивание — журналируются только метаданные синхронно относительно данных;
- в режиме данных — журналируются как метаданные, так и данные.

Для серверного варианта РЕД ОС рекомендуется использовать файловую систему **XFS**, которая также является журналируемой.

Обе файловые системы — **ext4** и **XFS** — являются не только журналируемыми, но и:

- поддерживают большие объёмы дисковых накопителей (до 2^{60} байт);
- поддерживают файлы большого размера (до 2^{44} байт);
- используют механизм пространственной записи файлов, уменьшающий фрагментацию и повышающий производительность. Суть механизма заключается в том, что новая информация добавляется в конец области диска, выделенной заранее рядом с

областью, занятой содержимым файла.

Важными отличиями представленных файловых систем является то, что **XFS**:

- может производить дефргаментацию «на лету»;
- имеет API ввода-вывода реального времени (для приложений жёсткого или мягкого реального времени, например, для работы с потоковым видео);
- имеет малые «накладные расходы» — размер служебных структур данных.

Ext4 в отличие от **XFS** менее агрессивно использует оперативную память при работе с файлами на носителе, поэтому её оптимально применять на вычислительных системах с небольшим объёмом ОЗУ.

При выборе файловой системы при создании/форматировании раздела рекомендуется определить, для чего будет использоваться этот раздел. Также следует обратить внимание на параметры процессора и оперативной памяти компьютера, и на основании этого принимать решение о необходимости выбора той или иной ФС.

РЕД ОС поддерживает и другие файловые системы, такие как **FAT**, **NTFS**, а также **ISO-9660** для оптических накопителей, сетевые файловые системы.

Файлы

У всех файловых систем в РЕД ОС есть одно принципиальное отличие от файловых систем Windows — имена файлов регистрозависимы, т.е «заявление.odt», «Заявление.odt» и «ЗАЯВЛЕНИЕ.odt» — это три разных файла. Необходимо обращать на это внимание, если вы только начинаете миграцию на РЕД ОС с других операционных систем. Особенно следует быть внимательными, когда такие файлы копируются на USB-накопитель — **FAT** и **NTFS** не разборчивы в символах, поэтому при выполнении данной операции возникнет ошибка.

Другим принципиальным отличием файловых систем Linux от файловых систем Windows является разделитель в именах каталогов — в РЕД ОС им служит «слэш» (или «прямой слэш») — «**/**», а в Windows применяется «обратный слэш» — «\». Например:

- **/var/log/boot.log** — путь к файлу в РЕД ОС;
- **C:\Windows\System32\example.exe** — путь к файлу в Windows.

В РЕД ОС (как и вообще в Linux) нет как такового понятия «расширение файла», поскольку точки интерпретируются как часть названия, а не как разделитель. Но прикладные программы и файловые менеджеры анализируют имя файла после последней точки и могут выполнять определённые действия над файлами с теми или иными «окончаниями» (например, двойной клик по файлу с окончанием **.odt** в файловом менеджере приведёт к запуску LibreOffice и открытию файла в нём).

Существует еще одно отличие в организации файловых систем — чтобы в РЕД ОС сделать файл скрытым — надо первым символом его имени указать символ точки «**.**». «Скрытость» файла в РЕД ОС — не метаданные, а непосредственное имя файла, т. е. для того чтобы сделать файл скрытым, его нужно переименовать, поставив первым символом имени «**.**»

Устройства

Следует особенно отметить, что в Unix-подобных операционных системах существует парадигма, относящаяся к идеологии UNIX, называемой **UNIX-Way**. Формулируется она как «Всё — есть файл». То есть всё, до чего «дотягивается» операционная система, можно представить в виде файла, будь то клавиатура, монитор, процессор, веб-камера и т. д.

То, что обычно считается файлом (текст или бинарный файл) называется простым (или регулярным) файлом, а файлы, связанные с каким-либо оборудованием (включая виртуальное) — файлом устройства. Например:

- **/dev/sda** — файл первого «жесткого» диска;
- **/dev/sda1** — файл устройства раздела на первом «жестком» диске;
- **/dev/dvd** — файл привода DVD;
- **/dev/lp0** — файл первого (по подключению) печатающего устройства (принтера).

В свою очередь, файлы устройств бывают двух типов — **блочные** и **символьные**. Обмен информации с блочными устройствами, например, с «жёстким» диском, осуществляется блоками информации, а с символьными — отдельными символами. Примеры символьных устройств: последовательный порт, клавиатура. С символьными файлами можно работать так же, как и с регулярными файлами, т.е. с помощью тех же утилит.

Также не стоит забывать и про каталоги — это специализированные файлы, которые содержат в себе список других файлов.

Файловая система РЕД ОС (как и у любого Linux), в отличие от операционных систем семейства Windows, не разделена по томам (дискам, устройствам), а имеет единую древовидную структуру. **Корневой каталог** — это уровень файловой системы, выше которого по дереву каталогов подняться невозможно. В РЕД ОС корневой каталог обозначается как «**/**».

Монтирование устройств

Для подключения любого устройства к файловой системе — монтирования — используется так называемая точка монтирования — каталог, все вложенные уровни которого являются файловой системой на устройстве-носителе. Например, если подключить флэш-носитель к USB-порту, РЕД ОС автоматически смонтирует устройство в каталог **/var/run/<имя_пользователя>/media**, и все папки и файлы, находящиеся после монтирования в данном каталоге, на самом деле будут располагаться на флэш-накопителе. Для монтирования файловых ресурсов и внешних устройств используется утилита mount. Общий синтаксис команды имеет следующий вид:

```
mount -t <тип_ФС> <имя_устройства> <точка монтирования>
```

Каталоги файловой системы РЕД ОС

У структуры файловой системы РЕД ОС есть ещё одна особенность: пользователям выделяется в ней домашний каталог — специальная папка, необходимая для хранения пользовательских данных. При входе пользователя в систему, он сразу оказывается в своём домашнем каталоге. Обычно права доступа к домашней папке устанавливаются таким образом, что доступ к ней имеют только пользователь и администратор (**root**). В других папках системы пользователю, как правило, разрешен только просмотр содержимого.

Файловая система РЕД ОС содержит следующие каталоги:

- **/** — корневой каталог;
- **/bin** — каталог основных исполняемых файлов, необходимых для функционирования системы;
- **/boot** — каталог загрузчика, содержит образы ядра и Initrd, может содержать конфигурационные и вспомогательные файлы загрузчика;
- **/dev** — содержит файлы устройств;
- **/etc** — конфигурационные файлы системы и основные файлы настроек системных приложений;
- **/home** — папка для домашних каталогов пользователей;
- **/lib** — содержит основные библиотеки и модули, необходимые для работы системы;
- **/lib64** — то же, что и **/lib**, для 64-битных систем;
- **/media** — обычно используется для вручную смонтированных «внешних» носителей;
- **/mnt** — обычно содержит точки монтирования сетевых и файловых ресурсов (смонтированных ISO-файлов);
- **/opt** — альтернатива **/usr** для проприетарного ПО или ПО, не входящего в основной дистрибутив;
- **/proc** — содержит виртуальную файловую систему proc, создаваемую «на лету», а также общую информацию о системе и о каждом процессе;
- **/root** — каталог администратора (суперпользователя) **root**;
- **/run** – каталог для хранения данных, которые были запущены приложениями, требующимися в процессе работы (к ним относятся службы, запускаемые самой системой, и программы, которые запускаются пользователем вручную). Каталог также представляет собой смонтированную виртуальную ФС, чтобы при выключении/перезагрузке ПК вся текущая информация в данном каталоге (информация является временной) удалялась и не занимала пространство на диске;
- **/sbin** — каталог системных утилит, выполнять которые имеет право пользователь root;
- **/srv** – содержит файлы серверов и сервисов. Например, могут содержаться файлы веб-сервера **apache**.
- **/sys** — содержит виртуальную файловую систему, а также подробную информацию о процессах;
- **/tmp** — каталог для временных файлов;
- **/usr** — программы, библиотеки, документация пользовательских приложений, также может содержать исходные коды программ и ядра;
- **/var**— постоянно изменяющиеся данные системы, например, очереди системы печати, протоколы и т. д.

Основные команды для работы с файлами и файловой системой

Навигация

Для навигации по содержимому файловой системы используются следующие команды:

- `ls` — вывод содержимого текущей или явно указанной папки;

- `pwd` — вывод полного имени текущего каталога;
- `cd` — изменение текущего каталога на указанный. Если аргумент не указан или указан как «**~**», то смена происходит на домашний каталог текущего пользователя. Аргумент «**..**» меняет каталог на вышестоящий в иерархии дерева каталогов;
- `pushd`, `popd` — команды работают в связке. Команда **pushd** изменяет каталог на указанный, история запоминается в стек и потом может быть использована для быстрой обратной навигации с помощью команды **popd**.

Операции с файлами

Для операций с файлами используются следующие команды:

- `touch <файл>` — создание пустого файла.
- `cat <файл>` — вывод текстового файла на экран.
- `tac <файла>` — вывод содержимого текстового файла в обратном порядке, т. е. сначала выводится последняя строка файла, потом предпоследняя и т. д.
- `cp <файл1> <файл2>` — копирование файла **<файл1>** в **<файл2>**. Если **<файл2>** существует, программа спросит разрешение на перезапись.
- `mv <файл1> <файл2>` — перемещение файла **<файл1>** в **<файл2 >**. Эту же команду можно использовать для переименования файла.
- `rm <файл>` — удаление файла (с ключом **-i** выводит запрос на разрешение удаления, ключ **-f** подавляет все запросы).
- `locate <файл>` — быстрый поиск файла.
- `which <программа>` — вывод каталога, в котором находится программа, если она установлена. Поиск производится в каталогах, указанных в переменной окружения **path** (путь поиска программ).
- `less <файл>` — удобный просмотр файла с возможностью постраничной прокрутки с использованием клавиш навигации.

Операции с каталогами

Для операций с каталогами используются следующие команды:

- `mkdir <каталог>` — создание каталога;
- `rmdir <каталог>` — удаление пустого каталога;
- `rm -r <каталог>` — рекурсивное удаление каталога;
- `cp -r <каталог1> <каталог2>` — копирование **<каталога1>** в каталог с именем **<каталог2>**, причём **<каталог1>** должен быть пустым. Если каталог требуется скопировать со всем содержимым, то необходимо указать ключ **-r**;
- `mv <каталог1> <каталог2>` — переименование каталогов. Для переноса каталога с именем **<каталог1>** в каталог с именем **<каталог2>** необходимо указать ключ **-r**.

Мягкие и жесткие ссылки

В РЕД ОС имеются также дополнительные файлы и называются они ссылками. Ссылки бывают двух типов - «мягкие» ссылки (*softlink*) и «жёсткие» ссылки (*hardlink*). «Мягкие» ссылки являются указателями на имеющиеся файлы и каталоги. «Жёсткие» ссылки являются ещё одним именем файла.

Создаются ссылки с помощью утилиты **ln**. Для создания «мягких» ссылок необходимо передавать команде ключ **-s**.

Общий синтаксис команды имеет следующий вид:

```
ln [ -s ] <имя_файла_или_каталога> <имя_ссылки>
```

Примеры создания ссылок

Мягкие ссылки

```
cd ~
mkdir FirstDir
ls
```

```
 FirstDir  test-ca.conf  Видео  Документы  Загрузки Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
 ln -s FirstDir SecondDir
ls

 FirstDir  SecondDir  test-ca.conf  Видео  Документы Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол' Шаблоны
 cd SecondDir
touch file1.txt
ls ~/FirstDir

file1.txt
```

При создании пустого файла в каталоге **SecondDir** на самом деле действие производится в каталоге **FirstDir**, что подтверждает последний листинг.

Если удалить исходный файл или каталог, на который ссылается «мягкая» ссылка, то она становится недействительной, т.е. как файл она продолжит существовать, но уже ни на что указывать не будет, и операции с ней (просмотр и т.д.) будут завершаться с ошибкой.

```
cd ~
rm -rf ~/FirstDir
ls SecondDir  test-ca.conf  Видео  Документы  Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
```

Жёсткие ссылки

В примере будет создан текстовый файл путём перенаправления в него вывода строки и жёсткая ссылка на него:

```
cd ~
echo "One small test..." > File1.txt
ls

 File1.txt  test-ca.conf  Видео  Документы Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол' Шаблоныln File1.txt
File2.txt
```

Затем будут внесены изменения в файл **File2.txt** и просмотрено содержимое файла **File1.txt**:

```
echo "Second string..." >> File2.txt
cat File1.txt

One small test...
Second string...
 cat File2.txt

One small test...
Second string...
```

Файлы содержат одну и ту же информацию, поскольку указывают на одну и ту же область памяти на диске. После удаления первого файла область информации на диске остаётся, поскольку остаётся «жёсткая» ссылка, которая становится единственным именем данного файла:

```
rm -f File1.txt
ls

 File2.txt  test-ca.conf  Видео  Документы Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол' Шаблоны
 cat File2.txt

One small test...
Second string...
```

Введение: пакеты, зависимости и репозитории

В РЕД ОС огромное число общих ресурсов, которыми пользуются сразу несколько программ: разделяемых библиотек, содержащих стандартные функции, исполняемых файлов, сценариев и стандартных утилит и т.д. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или даже вывести из строя всю систему. В контексте системного администрирования проблемы такого рода называют нарушением *целостности системы*. Задача администратора - обеспечить наличие в системе согласованных версий всех необходимых программных компонентов (обеспечение целостности системы).

Для установки, удаления и обновления программ и поддержания целостности системы используются *менеджеры пакетов*. С точки зрения менеджера пакетов программное обеспечение представляет собой набор компонентов - программных *пакетов*. Такие компоненты содержат в себе набор исполняемых программ и вспомогательных файлов, необходимых для корректной работы программного обеспечения. Менеджеры пакетов облегчают установку программ: они позволяют проверить наличие необходимых для работы устанавливаемой программы компонент подходящей версии непосредственно в момент установки, а также производят необходимые процедуры для регистрации программы во всех операционных средах пользователя: сразу после установки программа может быть доступна пользователю из командной строки и - если это предусмотрено - появляется в меню всех графических оболочек.

ВАЖНО!

Благодаря менеджерам пакетов, пользователю обычно не требуется непосредственно обращаться к установочным процедурам отдельных программ или непосредственно работать с каталогами, в которых установлены исполняемые файлы и компоненты программ (обычно это **/usr/bin**, **/usr/share/имя_пакета**) - всю работу делает менеджер пакетов. Поэтому установку, обновление и удаление программ обычно называют управлением пакетами.

Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставляемого пакетом A, необходимо установить пакет B. В таком случае говорят, что пакет A *зависит* от пакета B или что между пакетами A и B существует *зависимость*.

Отслеживание зависимостей между такими пакетами представляет собой серьезную задачу для любого дистрибутива - некоторые компоненты могут быть взаимозаменяемыми: может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Задача контроля целостности и непротиворечивости установленного в системе ПО еще сложнее. Представим, что некие программы A и B требуют наличия в системе компоненты C версии 1.0. Обновление версии пакета A, требующее обновления компоненты C до новой, использующей новый интерфейс доступа, версии (скажем, до версии 2.0), влечет за собой обязательное обновление и программы B.

Однако менеджеры пакетов оказались неспособны предотвратить все возможные коллизии при установке или удалении программ, а тем более эффективно устранить нарушения целостности системы. Особенно сильно этот недостаток сказывается при обновлении систем из централизованного *репозитория пакетов*, в котором последние могут непрерывно обновляться, дробиться на более мелкие и т. п. Этот недостаток и стимулировал создание систем управления программными пакетами и поддержания целостности системы.

Для автоматизации этого процесса в РЕД ОС применяется система управления программными пакетами **DNF**.

Вы можете подробнее ознакомиться с информацией о работе с программными пакетами, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Назначение DNF

Фактически, **dnf** представляет собой оболочку для **rpm**, обеспечивающую работу с репозиториями.

Утилита **dnf** - это менеджер пакетов, который умеет запрашивать информацию о пакетах, получать пакеты из репозиториев, устанавливать и удалять их, используя автоматическое разрешение зависимостей, а также обновлять целиком систему до последних версий пакетов. **DNF** выполняет автоматическое разрешение зависимостей для пакетов, которые обновляются, устанавливаются или удаляются, и, таким образом, позволяют автоматически определять, получать и устанавливать все доступные по зависимостям пакеты. Для **DNF** можно настроить новые, дополнительные репозитории, или, по-другому, источники пакетов, кроме того, для него доступны многие дополнения, которые улучшают и расширяют его возможности. **DNF** позволяет выполнять многие из задач, которые выполняет **RPM**; кроме того, многие из опций командной строки у него также подобны опциям **RPM**. Утилита **DNF** обеспечивает простое и легкое управление пакетами на одной машине или же на группе машин.

DNF обеспечивает безопасное управление пакетами путем включения проверки сигнатур GPG для пакетов, подписанных с помощью GPG, для всех репозиториев пакетов или для отдельных репозиториев. В случае включения проверки сигнатур, **DNF** откажется устанавливать любые пакеты, не подписанные корректным ключом для данного репозитория. Это означает, что можно доверять пакетам **RPM**, которые скачиваются и устанавливаются на машине в том случае, если они получены из доверенных источников и не были изменены в процессе передачи.

DNF также позволяет легко создавать собственные репозитории RPM-пакетов для скачивания и установки их на других машинах.

Основные команды DNF и утилиты dnf repoquery

Основные команды **DNF** приведены в таблице.

Команда	Описание
dnf install <имя_пакета>	Установка пакета с заданным именем
dnf reinstall <имя_пакета>	Переустановка пакета
dnf remove <имя_пакета>	Удаление пакета
dnf autoremove	Удаляет все пакеты, которые не нужны системе, если они не используются другими приложениями
dnf info <имя_пакета>	Показать информацию о пакете
dnf search <имя_пакета>	Поиск пакета по имени в репозитории
dnf list	Вывод имен всех доступных и установленных пакетов
dnf list installed	Вывод списка всех установленных пакетов
dnf list available	Вывод списка всех доступных пакетов
dnf repolist all	Вывод списка всех репозиториев
dnf repoinfo <имя_репозитория>	Информация о репозитории
dnf config-manager --set-disabled <имя_репозитория>	Отключение репозитория
dnf config-manager --set-enabled <имя_репозитория>	Включение репозитория
dnf clean all	Удаление всех метаданных, кешированных пакетов и заголовков
dnf makecache	Загружает и кэширует метаданные для всех известных репозиториев
dnf history	Вывод истории об использования dnf
dnf groupinstall <имя_группы>	Установка всех пакетов из группы с заданным именем
dnf groupupdate <имя_группы>	Обновление всех пакетов из группы с заданным именем
dnf groupremove <имя_группы>	Удаление всех пакетов из группы с заданным именем
dnf groupinfo <имя_группы>	Получить список пакетов, относящихся к группе
dnf grouplist	Вывод имен всех существующих групп пакетов
dnf provides <имя_файла или пакета>	Поиск пакета, к которому принадлежит определенный файл/подпакет
dnf update	Обновить все пакеты в системе
dnf download <имя_пакета>	Загружает из репозитория пакет
dnf repoquery --requires <имя_пакета>	Получить список зависимостей неустановленного пакета
dnf repoquery --requires --resolve <имя_пакета>	Вывод списка пакетов, которые необходимы для удовлетворения зависимостей
dnf downgrade <имя_пакета><версия>	Понижает текущую версию пакета до предыдущей (по возможности). Если указана версия пакета (ниже установленной), выполняется понижение до целевой версии пакета
dnf download --resolve <имя_пакета> --downloaddir /<путь_к_каталогу>	Позволяет загружать rpm-пакет вместе со всеми зависимостями в указанный каталог

Вы можете подробнее ознакомиться с менеджером пакетов DNF, просмотрев наши обучающие видео:

- на **RuTube** — Менеджер пакетов DNF в РЕД ОС 7.3 ;
- в **Яндекс.Дзен** — Менеджер пакетов DNF в РЕД ОС 7.3 ;
- в **VK Видео** — Менеджер пакетов DNF в РЕД ОС 7.3 .

На наших каналах вы также сможете найти много другой полезной информации.

Утилита **dnf repoquery** предоставляет широкий набор инструментов для работы с репозиториями и пакетами, что делает ее мощным инструментом для управления пакетами в системе. В таблице приведены некоторые из основных возможностей **dnf repoquery**.

Команда	Описание
dnf repoquery <название_пакета>	Находит пакет в установленных репозиториях по его названию.
dnf repoquery --info <название_пакета>	Предоставляет подробную информацию о пакете, включая версию, размер, описание и другие атрибуты.
dnf repoquery --whatprovides <путь_к_файлу>	Находит пакет, который содержит указанный файл.

dnf repoquery --requires <название_пакета>	Показывает список зависимостей, необходимых для установки указанного пакета.
dnf repoquery --whatrequires <название_пакета>	Находит другие пакеты, которые зависят от указанного пакета.
dnf repoquery --group <название_группы>	Находит все пакеты, входящие в указанную группу пакетов.
dnf repoquery --requires <название_пакета>	Показывает список зависимостей, которые должны быть удовлетворены для установки указанного пакета.
dnf repoquery --all	Показывает список всех пакетов, доступных в репозиториях.
dnf repoquery --unneeded	Показывает только те пакеты, которые могут быть удалены командой "dnf autoremove".
dnf repoquery --installed	Показывает список всех установленных пакетов.
dnf repoquery -h	Вывести список всех доступных команд.

Работа с историей DNF

Просмотр истории транзакций
Отмена транзакции
Повтор транзакции
Откат к предыдущей транзакции
Просмотр недавно добавленных пакетов

Для отслеживания изменений по установке, обновлению и удалению пакетов в системе используется история DNF, которая дает представление о транзакциях в хронологическом порядке.

Благодаря истории транзакций можно отменить ту или иную транзакцию, сделать откат к предыдущей транзакции (при этом отменятся все выполненные транзакции после указанной), повторить отмененную транзакцию, а также просмотреть недавно добавленные транзакции.

Просмотр истории транзакций

Для просмотра транзакций используется следующая команда:

```
dnf history
```

```
[root@localhost user]# dnf history
Иденти | Командная строка          | Дата и время     | Действия       | Изменен
-------------------------------------------------------------------------------
    38 | install gscan2pdf-2.8.0-1 | 2022-01-11 12:43 | Install        |   62
    37 | install flatpak           | 2022-01-11 12:42 | Install        |    4 EE
    36 | install redshift          | 2022-01-11 12:42 | Install        |    1
    35 | install shotwell-0.31.2-1 | 2022-01-11 12:41 | Install        |   50
    34 | install cherrytree-0.38.1 | 2022-01-11 12:41 | Install        |    8
    33 | install gimp              | 2022-01-11 12:39 | Install        |    7
```

Отмена транзакции

Отмена какой-либо транзакции выполняется с помощью следующей команды:

```
dnf history undo <идентификатор_транзакции>
```

```
[root@localhost user]# dnf history undo 36
Последняя проверка окончания срока действия метаданных: 2:26:35 назад, Вт 11 янв 2022 10:19:18.
Откат транзакции 36, с Вт 11 янв 2022 12:42:14
    Установка redshift-1.12-2.el7.x86_64 @base
Зависимости разрешены.
================================================================================
 Пакет                Архитектура         Версия                    Репозиторий        Размер
================================================================================
Удаление:
 redshift             x86_64              1.12-2.el7                @base              561 k

Результат транзакции
================================================================================
Удаление  1 Пакет

Освобожденное место: 561 k
Продолжить? [д/Н]: y
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```

Повтор транзакции

Отмененную транзакцию можно повторить (необходимо указать ID отмененной транзакции):

```
dnf history redo <идентификатор_транзакции>
```

```
[root@localhost user]# dnf history redo 36
Последняя проверка окончания срока действия метаданных: 2:30:33 назад, Вт 11 янв 2022 10:19:18.
Repeating transaction 36, from Вт 11 янв 2022 12:42:14
    Установка redshift-1.12-2.el7.x86_64 @base
================================================================================
 Пакет                Архитектура          Версия                  Репозиторий        Размер
================================================================================
Установка:
 redshift             x86_64               1.12-2.el7              base               149 k

Результат транзакции
================================================================================
Установка  1 Пакет

Объем загрузки: 149 k
Объем изменений: 561 k
Продолжить? [д/Н]: y
Загрузка пакетов:
redshift-1.12-2.el7.x86_64.rpm                              1.2 MB/s | 149 kB     00:00
--------------------------------------------------------------------------------
Общий размер                                                1.2 MB/s | 149 kB     00:00
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```

Откат к предыдущей транзакции

Для отката к предыдущей версии транзакции используется следующая команда:

```
dnf history rollback <идентификатор_транзакции>
```

```
[root@localhost user]# dnf history rollback 35
Последняя проверка окончания срока действия метаданных: 2:35:38 назад, Вт 11 янв 2022 10:19:18.
Rollback to transaction 35, from Вт 11 янв 2022 12:41:25
  Undoing the following transactions: 36, 37, 38, 39, 40
    Установка ImageMagick-perl-6.9.11.27-1.el7.x86_64          @base
    Установка flatpak-selinux-1.6.3-2.el7.noarch               @base
    Установка flatpak-session-helper-1.6.3-2.el7.x86_64        @base
    Установка flatpak-1.6.3-2.el7.x86_64                       @base
    Установка goocanvas2-2.0.2-4.el7.x86_64                    @base
    Установка gscan2pdf-2.8.0-1.el7.noarch                     @base
================================================================================
                                     ...
================================================================================
 perl-namespace-autoclean            noarch       0.29-2.el7          @base        41 k
 perl-namespace-clean                noarch       0.27-12.el7         @base        39 k
 perltidy                            noarch       20190915-1.el7      @base       2.1 M
 redshift                            x86_64       1.12-2.el7          @base       561 k
 sane-frontends                      x86_64       1.0.14-22.el7       @base       135 k

Результат транзакции
================================================================================
Удаление  67 Пакетов

Освобожденное место: 53 M
Продолжить? [д/Н]: y
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```

Обратите внимание, что **транзакции**, выполненные **после** той, к которой выполняется откат, **будут отменены**.

Просмотр недавно добавленных пакетов

Для просмотра недавно добавленных пакетов используется следующая команда:

```
dnf list recent
```

```
[root@localhost user]# dnf list recent
RedOS - Base                                    66 kB/s | 3.6 kB     00:00
RedOS - Base                                    11 MB/s |  38 MB     00:03
RedOS - Updates                                 80 kB/s | 2.9 kB     00:00
RedOS - Updates                                9.6 MB/s | 7.3 MB     00:00
Последняя проверка окончания срока действия метаданных: 2:38:49 назад, Вт 11 янв
 2022 10:19:18.
Недавно добавленные пакеты
anaconda.i686                          33.25.4-6.3.el7              updates
anaconda.x86_64                        33.25.4-6.3.el7              updates
anaconda-core.i686                     33.25.4-6.3.el7              updates
anaconda-core.x86_64                   33.25.4-6.3.el7              updates
anaconda-dracut.i686                   33.25.4-6.3.el7              updates
anaconda-dracut.x86_64                 33.25.4-6.3.el7              updates
anaconda-gui.i686                      33.25.4-6.3.el7              updates
anaconda-gui.x86_64                    33.25.4-6.3.el7              updates
anaconda-install-env-deps.i686         33.25.4-6.3.el7              updates
anaconda-install-env-deps.x86_64       33.25.4-6.3.el7              updates
anaconda-live.i686                     33.25.4-6.3.el7              updates
anaconda-live.x86_64                   33.25.4-6.3.el7              updates
anaconda-tui.i686                      33.25.4-6.3.el7              updates
anaconda-tui.x86_64                    33.25.4-6.3.el7              updates
```

Источники программ (репозитории)

Создание репозитория
Подключение репозиториев
ПО в репозитории
Доступные репозитории РЕД ОС

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный

Репозитории, с которыми работает **DNF**, отличаются от обычного набора пакетов наличием метаинформации - индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, **DNF** достаточно получить его индексы. **DNF** может работать с любым количеством репозиториев одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов **DNF** обращает внимание только на название пакета, его версию и зависимости, а расположение в том или ином репозитории не имеет значения. Если потребуется, **DNF** в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

ВАЖНО!

При использовании РЕД ОС (стандартной и сертифицированной редакции), в целях предотвращения нарушения целостности системы, **ЗАПРЕЩАЕТСЯ** настройка служб автоматического обновления на использование внешних **сторонних** репозиториев операционных систем.

Подключение репозитория **сторонней** ОС влечет за собой **нарушение** зависимостей в устанавливаемых пакетах. Принудительная установка пакетов из репозитория сторонней ОС может привести к **неработоспособности** как отдельных компонентов системы, так и ОС в целом.

Если для обеспечения рабочих процессов пользователя нужен пакет (программа, утилита), которого нет в РЕД ОС (и/или требуется обновление версий пакетов, которые уже есть в репозитории РЕД ОС), необходимо обратиться в техническую поддержку с запросом на добавление нового пакета или обновление версии пакетов РЕД ОС.

DNF позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные - **HTTP** и **FTP**, однако существуют и некоторые дополнительные методы. Для того чтобы **DNF** мог использовать тот или иной репозиторий, информацию о нем необходимо поместить в папку **/etc/yum.repos.d/**. После того как отредактирован список репозиториев в **/etc/yum.repos.d/**, необходимо обновить локальную базу данных **DNF** о доступных пакетах:

```
dnf repolist
```

При выборе пакетов для установки **DNF** руководствуется *всеми* доступными репозиториями вне зависимости от способа доступа к ним. Так, если в репозитории, доступном по сети Интернет, обнаружена более новая версия программы, чем на компакт-диске, то **DNF** начнёт загружать данный пакет из сети Интернет.

Создание репозитория

Для создания репозитория выполните следующие действия:

1. Установите пакет **createrepo**.

   ```
   dnf install createrepo
   ```

2. Скопируйте все пакеты в один каталог, например: **/mnt/local_repo**.

3. Создайте репозиторий, используя следующую команду и указав созданный каталог:

   ```
   createrepo --database /mnt/local_repo
   ```

Для установки пакетов из созданного локального репозитория создайте конфигурационный файл в каталоге **/etc/yum.repos.d/**.

Например:

```
nano /etc/yum.repos.d/my-rpm.repo
```

Содержимое файла:

```
[my-rpm]
 name=my-rpm
 baseurl=file:///mnt/local_repo
 gpgcheck=0
```

Подключение репозиториев

Для подключения репозитория на постоянной основе необходимо выполнить (в примере используется репозиторий **foo-bar**):

```
dnf config-manager --set-enabled foo-bar
```

Для отключения репозитория на постоянной основе необходимо выполнить:

```
dnf config-manager --set-disabled foo-bar
```

Для временного подключения репозитория и установка пакета из него необходимо выполнить:

```
dnf install --refresh foo-bar --enablerepo=foo-bar
```

Необязательный параметр `--refresh` добавляется для принудительного обновления кеша **dnf**.

ПО в репозитории

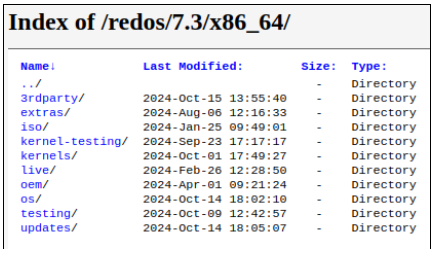
Ознакомиться со списком доступного в репозитории программного обеспечения можно по ссылке.

Доступные репозитории РЕД ОС

Для РЕД ОС существуют два типа репозиториев - для *стандартной* редакции и для *сертифицированной* редакции ОС.

Репозитории стандартной редакции развиваются (обновляются) быстрее.

Далее в качестве примера будут рассмотрены репозитории стандартной редакции РЕД ОС и их назначение. Для просмотра доступных репозиториев перейдите по ссылке.



Index of /redos/7.3/x86_64/

Name↓	Last Modified:	Size:	Type:
../		-	Directory
3rdparty/	2024-Oct-15 13:55:40	-	Directory
extras/	2024-Aug-06 12:16:33	-	Directory
iso/	2024-Jan-25 09:49:01	-	Directory
kernel-testing/	2024-Sep-23 17:17:17	-	Directory
kernels/	2024-Oct-01 17:49:27	-	Directory
live/	2024-Feb-26 12:28:50	-	Directory
oem/	2024-Apr-01 09:21:24	-	Directory
os/	2024-Oct-14 18:02:10	-	Directory
testing/	2024-Oct-09 12:42:57	-	Directory
updates/	2024-Oct-14 18:05:07	-	Directory

Репозитории для образов:

- **iso/** – место расположения ISO-образов;
- **live/** – место расположения LIVE-образов;
- **oem/** – место расположения OEM-образов.

По умолчанию в РЕД ОС подключены следующие репозитории:

- **os/** – базовый репозиторий;
- **updates/** – репозиторий обновлений.

Дополнительные ветки репозиториев:

- **kernels/** – репозиторий для новых версий ядра;
- **kernel-testing/** – репозиторий для предрелизной публикации обновлений ядра;
- **testing/** – репозиторий для предрелизной публикации обновлений некоторых пакетов;

- **extras/** – пакеты, дополняющие базовый репозиторий;
- **3rdparty/** – пакеты сторонних разработчиков.

Для подключения репозиториев, находящихся в дополнительных ветках, необходимо установить соответствующие пакеты.

Синтаксис команды имеет следующий вид:

```
dnf install <название_пакета>
```

Для просмотра подключенных репозиториев в каталог **/etc/yum.repos.d/** выполните команду:

```
ls -lah /etc/yum.repos.d/
```

Для просмотра подключенных репозиториев в каталог **/etc/distro.repos.d/** выполните команду:

```
ls -lah /etc/distro.repos.d/
```

```
[root@localhost ~]# ls -lah /etc/yum.repos.d/
итого 44K
drwxr-xr-x.   2 root root 4,0K авг 11 09:36 .
drwxr-xr-x. 161 root root  12K авг 10 16:05 ..
-rw-r--r--.   1 root root  385 ноя  7  2022 RedOS-ansible6.repo
-rw-r--r--.   1 root root  251 мая  4 12:11 RedOS-Base.repo
-rw-r--r--.   1 root root  316 мар 31 16:39 RedOS-kernels6.repo
-rw-r--r--.   1 root root  287 янв 13  2022 RedOS-kernels.repo
-rw-r--r--.   1 root root  369 авг 22  2022 RedOS-php81.repo
-rw-r--r--.   1 root root  260 мая 11  2022 RedOS-postgresql14.repo
-rw-r--r--.   1 root root  272 мая  4 12:11 RedOS-Updates.repo
[root@localhost ~]# ls -lah /etc/distro.repos.d/
итого 36K
drwxr-xr-x.   2 root root 4,0K авг 10 16:17 .
drwxr-xr-x. 161 root root  12K авг 10 16:05 ..
-rw-r--r--.   1 root root  289 дек 29  2022 RedOS-3rdparty-clickhouse.
repo
-rw-r--r--.   1 root root  269 июн 28 10:43 RedOS-3rdparty-gitlab.repo
-rw-r--r--.   1 root root  331 июн 27 10:12 RedOS-3rdparty-keycloak.re
po
-rw-r--r--.   1 root root  269 июн 28 10:48 RedOS-3rdparty-pantum.repo
-rw-r--r--.   1 root root  269 янв 17  2023 RedOS-3rdparty-weasis.repo
[root@localhost ~]#
```

Для просмотра всех подключенных репозиториев выполните команду:

```
dnf repolist
```

```
[root@localhost ~]# dnf repolist
идентификатор репозитория     имя репозитория
3rdparty-clickhouse           Repositories for 3rdparty-clickhouse
3rdparty-gitlab               Repositories for 3rdparty-gitlab
3rdparty-keycloak             Repositories for 3rdparty-keycloak
3rdparty-pantum               Repositories for 3rdparty-pantum
3rdparty-weasis               Repositories for 3rdparty-weasis
PostgreSQL14                  PostgreSQL14 for RED OS 7.3
ansible6                      Ansible 6 Repository for RED OS 7.3
base                          RedOS - Base
kernels                       Kernels updates for RED OS 7.3
kernels6                      Repositories for kernels6
php81                         PHP 8.1 Repository for RED OS 7.3
updates                       RedOS - Updates
```

Управление пакетами

Поиск пакетов
Установка или обновление пакетов
Удаление установленных пакетов
Обновление ОС
Удаление из системы пакетов старых ядер
Просмотр списка установленных ядер
Установка очередности загрузки ядра в ОС
Графическая утилита kernel-manager
Настройка DNF для работы через proxy

Поиск пакетов

Если пользователь не знает точного названия пакета, для его поиска можно воспользоваться утилитой **dnf search**, которая позволяет искать не только по имени пакета, но и по его описанию.

Вы можете подробнее ознакомиться с информацией о поиске программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Команда вида:

```
dnf search <подстрока>
```

Позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Например:

```
dnf search gdm

========================== Имя точное соответствие: gdm ==========================
gdm.x86_64 : The GNOME Display Manager
gdm.i686 : The GNOME Display Manager
====================== Имя и Краткое описание совпадение: gdm ======================
gdm-devel.i686 : Development files for gdm
gdm-devel.x86_64 : Development files for gdm
gdm-pam-extensions-devel.i686 : Macros for developing GDM extensions to PAM
gdm-pam-extensions-devel.x86_64 : Macros for developing GDM extensions to PAM
ovirt-guest-agent-gdm-plugin.noarch : Files for the GDM plug-in of the oVirt
                                    : Guest Agent
```

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой **dnf info**, которая покажет информацию о пакете из репозитория. Пример использования команды:

```
dnf info gdm-devel

Имеющиеся пакеты
Имя         : gdm-devel
Эпоха       : 1
Версия      : 3.38.2
Выпуск      : 4.el7
Архитектура : i686
Размер      : 25 k
Источник    : gdm-3.38.2-4.el7.src.rpm
Репозиторий : base
Краткое опис : Development files for gdm
URL         : https://wiki.gnome.org/Projects/GDM
Лицензия    : GPLv2+
Описание    : The gdm-devel package contains headers and other
            : files needed to build custom greeters.

Имя         : gdm-devel
Эпоха       : 1
Версия      : 3.38.2
Выпуск      : 4.el7
Архитектура : x86_64
Размер      : 25 k
```

```
Источник     : gdm-3.38.2-4.el7.src.rpm
Репозиторий  : base
Краткое опис : Development files for gdm
URL          : https://wiki.gnome.org/Projects/GDM
Лицензия     : GPLv2+
Описание     : The gdm-devel package contains headers and other
             : files needed to build custom greeters.
```

Установка или обновление пакетов

> **Примечание.**
>
> В связи с размещением в репозитории двух версий ядра — **LT** и **ML** — изменён принцип именования пакетов с модулями: **теперь непосредственно в имя пакета входит полная версия сборки ядра, которая может быть определена как uname -r**. Данный подход был реализован для возможности установки в системе нескольких пакетов с модулями под каждую из версий ядра, имеющихся в системе, с целью исключения конфликтов имён пакетов.
>
> Более подробную информацию о принципах именования пакетов с модулями ядра можно посмотреть в данной статье.

Вы можете подробнее ознакомиться с информацией по установке и обновлению программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка пакета выполняется командой:

```
dnf install <имя_пакета>
```

DNF позволяет устанавливать в систему пакеты, требующие для работы другие, пока ещё не установленные. В этом случае они определяют, какие пакеты необходимо установить, и устанавливают их, пользуясь всеми доступными репозиториями.

Пример установки пакета **vsftpd**:

```
dnf install vsftpd

================================================================================
 Пакет         Архитектура     Версия             Репозиторий    Размер
================================================================================
Установка:
 vsftpd        x86_64          3.0.3-1.el7        base           156 k
Результат транзакции
================================================================================
Установка  1 Пакет
Объем загрузки: 156 k
Объем изменений: 338 k
Продолжить? [д/Н]: д
Загрузка пакетов:
vsftpd-3.0.3-1.el7.x86_64.rpm                368 kB/s | 156 kB     00:00
--------------------------------------------------------------------------------
Общий размер                                 365 kB/s | 156 kB     00:00
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
  Подготовка       :                                        1/1
  Установка        : vsftpd-3.0.3-1.el7.x86_64              1/1
  Запуск скриптлета: vsftpd-3.0.3-1.el7.x86_64              1/1
  Проверка         : vsftpd-3.0.3-1.el7.x86_64              1/1
Установлен:
  vsftpd-3.0.3-1.el7.x86_64
Выполнено!
```

Команда **dnf install <имя_пакета>** используется также для обновления уже установленного пакета или группы пакетов. В этом

случае **dnf** дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи менеджера пакетов можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториев (например, полученный из Интернет). Для этого достаточно выполнить команду:

```
dnf install <путь_к_файлу.rpm>
```

При этом **DNF** проводит стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

Удаление установленных пакетов

Для удаления пакета используется следующая команда:

```
dnf remove <имя_пакета>
```

Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого: если отсутствует необходимый для работы приложения компонент (например, библиотека), то само приложение становится бесполезным.

Вы можете подробнее ознакомиться с информацией об удалении программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Обновление ОС

Для обновления всей системы рекомендуется использовать следующую команду:

```
dnf update
```

Она позволяет обновить те и только те установленные пакеты, для которых в репозиториях, перечисленных в **/etc/yum.repos.d**, имеются новые версии; при этом из системы не будут принудительно удалены никакие другие пакеты. Этот способ полезен при работе со стабильными пакетами приложений, относительно которых известно, что они при смене версии изменяются несущественно.

В случае обновления всего дистрибутива **DNF** проведёт сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, а также отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Всё, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчёте **dnf**, которым **DNF** соответственно предварит само обновление.

Вы можете подробнее ознакомиться с информацией об обновлении программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Удаление из системы пакетов старых ядер

Вы можете подробнее ознакомиться с информацией об удалении из системы пакетов старых ядер, просмотрев наши обучающие видео:

- на **RuTube** — Удаление старых ядер из системы;
- в **Яндекс.Дзен** — Удаление старых ядер из системы;
- в **VK Видео** — Удаление старых ядер из системы.

На наших каналах вы также сможете найти много другой полезной информации.

Просмотр списка установленных ядер

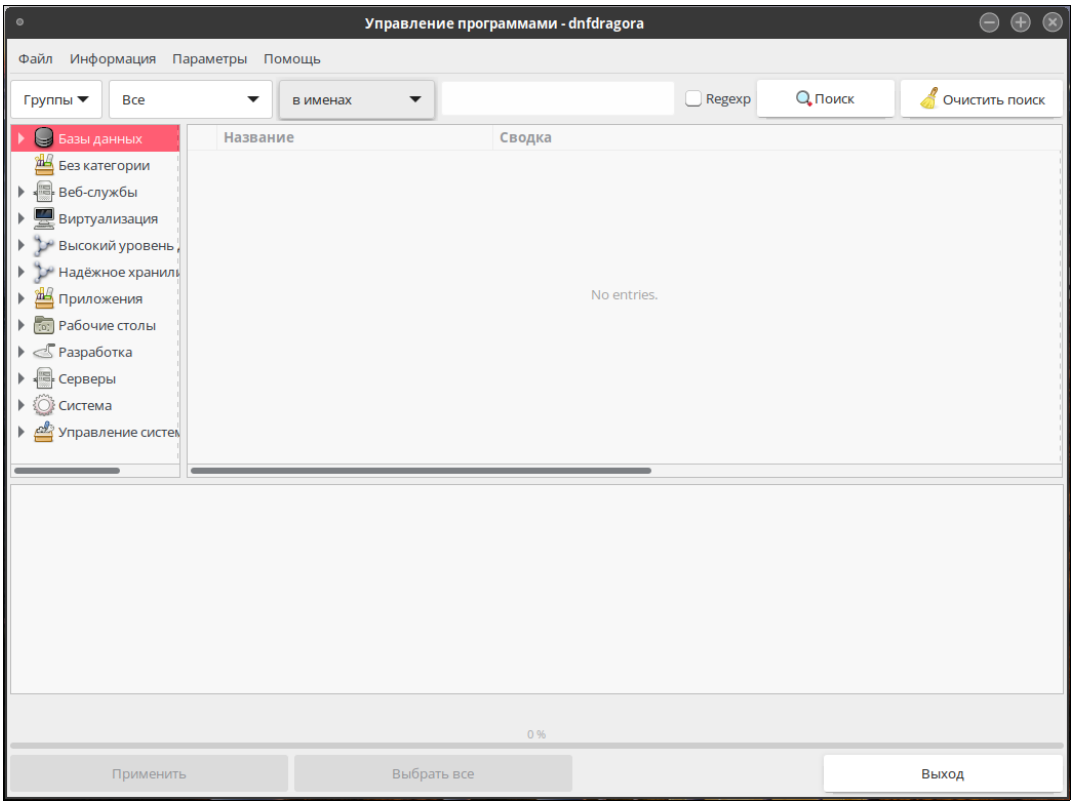
1) Для того чтобы посмотреть установленные в системе пакеты ядра, можно воспользоваться консольной командой:

```
rpm -qa kernel-*
```

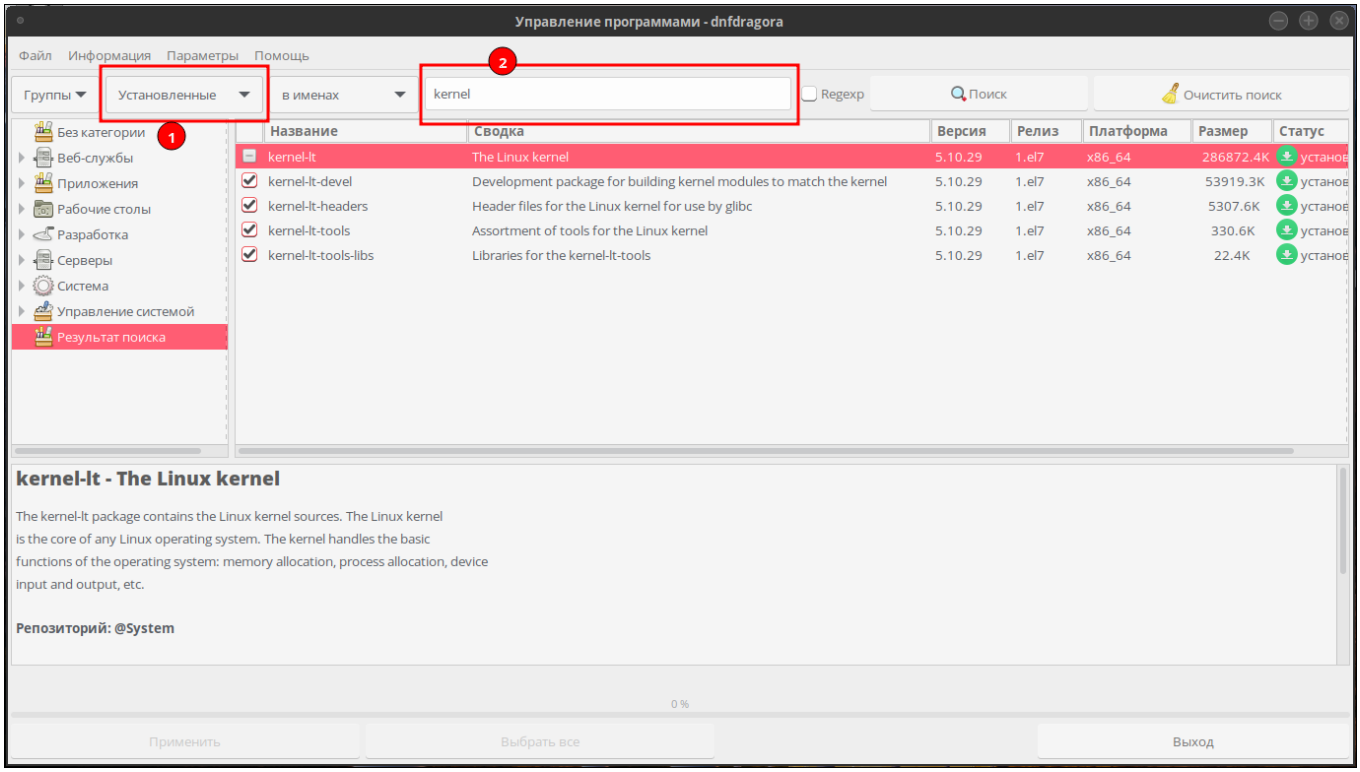
Для удаления можно воспользоваться утилитой **yum** или **dnf** в зависимости от используемой версии РЕД ОС.

```
dnf remove <имя_старого_пакета_ядра>
```

2) Также можно воспользоваться графической программой **dnfdragora**, расположенной по адресу **«Меню» - «Администрирование» - «dnfdragora»**. При запросе пароля привилегированного пользователя нужно ввести пароль локального пользователя с правами администратора.



Для отображения всех установленных пакетов ядер, наберите в поиске «**kernel**», предварительно выбрав пункт **«Установленные»**.



После этого снимите галочку напротив того пакета, который вы хотите удалить, и нажмите **«Применить»**. В открывшемся окне нажмите **«OK»** и дождитесь конца операции.

3) Вы также можете воспользоваться командой с регулярным выражением:

- для BIOS:

```
awk -F\' '$1=="menuentry " {print i++ " : " $2}' /etc/grub2.cfg
```

- для EFI:

```
awk -F\' '$1=="menuentry " {print i++ " : " $2}' /etc/grub2-efi.cfg
```

Она выведет все установленные в системе ядра:

```
0 : RED OS (5.10.29-1.el7.x86_64) MUROM (7.3.1)
1 : RED OS (5.10.24-2.el7.x86_64) MUROM (7.3.1)
2 : RED OS (5.10.1-1.el7.x86_64) MUROM (7.3.1)
...
```

Установка очередности загрузки ядра в ОС

Для установки очередности загрузки используется команда **grubby --set-default**.

Следующей командой укажите необходимый порядковый номер, под которым вы будете загружаться:

```
grubby --set-default 0
```

здесь **0** - это порядковый номер очередности загрузки, т.е. будет по умолчанию загружаться - **0 : RED OS (5.10.29-1.el7.x86_64) MUROM (7.3.1)**.

Таким образом, если рядом стоит windows, то можно выбрать порядок загрузки ОС.

Графическая утилита kernel-manager

В репозитории РЕД ОС доступна специальная утилита для управления ядрами операционной системы - **kernel-manager**.

Подробнее о работе с утилитой см. в нашей статье «kernel-manager - утилита управления ядрами».

Настройка DNF для работы через proxy

По умолчанию **dnf** получает данные с HTTP-сервера. Все соединения **dnf** с **HTTP** происходят с использованием **HTTP / 1.1** протокола и совместимых с ним веб прокси-серверов.

Если вам необходимо разрешить доступ к **dnf** через proxy-сервер для всех пользователей, используйте файл **/etc/dnf/dnf.conf** и внесите в раздел [main] данные прокси и данные для аутентификации:

```
[main]
proxy=http://proxy.mydomain.com:3128
proxy_username=user_proxy
proxy_password=pass_user_proxy
```

В данном примере параметры:

- **proxy.mydomain.com** — адрес вашего proxy-сервера **:порт**;
- **proxy_username** — имя пользователя;
- **proxy_password** — пароль пользователя.

В результате файл **/etc/dnf/dnf.conf** примет следующий вид:

```
alex[~]$ cat /etc/dnf/dnf.conf
[main]
gpgcheck=1
installonly_limit=3
clean_requirements_on_remove=False
best=False
skip_if_unavailable=True

proxy=http://proxy.mydomain.com:3128
proxy_username=user_proxy
proxy_password=pass_user_proxy
```

Здесь на скриншоте, в красном блоке, выделены строки, которые отвечают за настройку proxy для пакетного менеджера.

Если ваш proxy-сервер не использует авторизацию, достаточно прописать только:

```
proxy=http://proxy.mydomain.com:3128
```

Таким образом, файл `/etc/dnf/dnf.conf` требуется для настройки работы **dnf** через прокси для всех пользователей.

Чтобы разрешить доступ **dnf** через proxy-сервер для конкретного пользователя, вам необходимо использовать файл профиля пользователя. По умолчанию это **~/.bash_profile** в домашнем каталоге пользователя. Внесите в него следующие строки:

```
http_proxy="http://mycache.mydomain.com:3128"
export http_proxy
```

Если для работы proxy сервера необходимо использовать логин-пароль, то добавьте их в строку **http_proxy**:

```
http_proxy="http://user_proxy:pass_user_proxy@proxy.mydomain.com:3128"
```

Менеджер пакетов Dnfdragora

Установка
Обзор программы
Установка/удаление пакетов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** dnfdragora-2.1.1-12

Менеджер пакетов – это утилита, обеспечивающая поиск и установку пакетов из репозитория, а также обновление и удаление уже установленных пакетов на машине.

В РЕД ОС, начиная с версии 7.3, используется пакетный менеджер **DNF**.

Для более удобной работы с пакетным менеджером в ОС установлена графическая утилита **dnfdragora**.

Установка

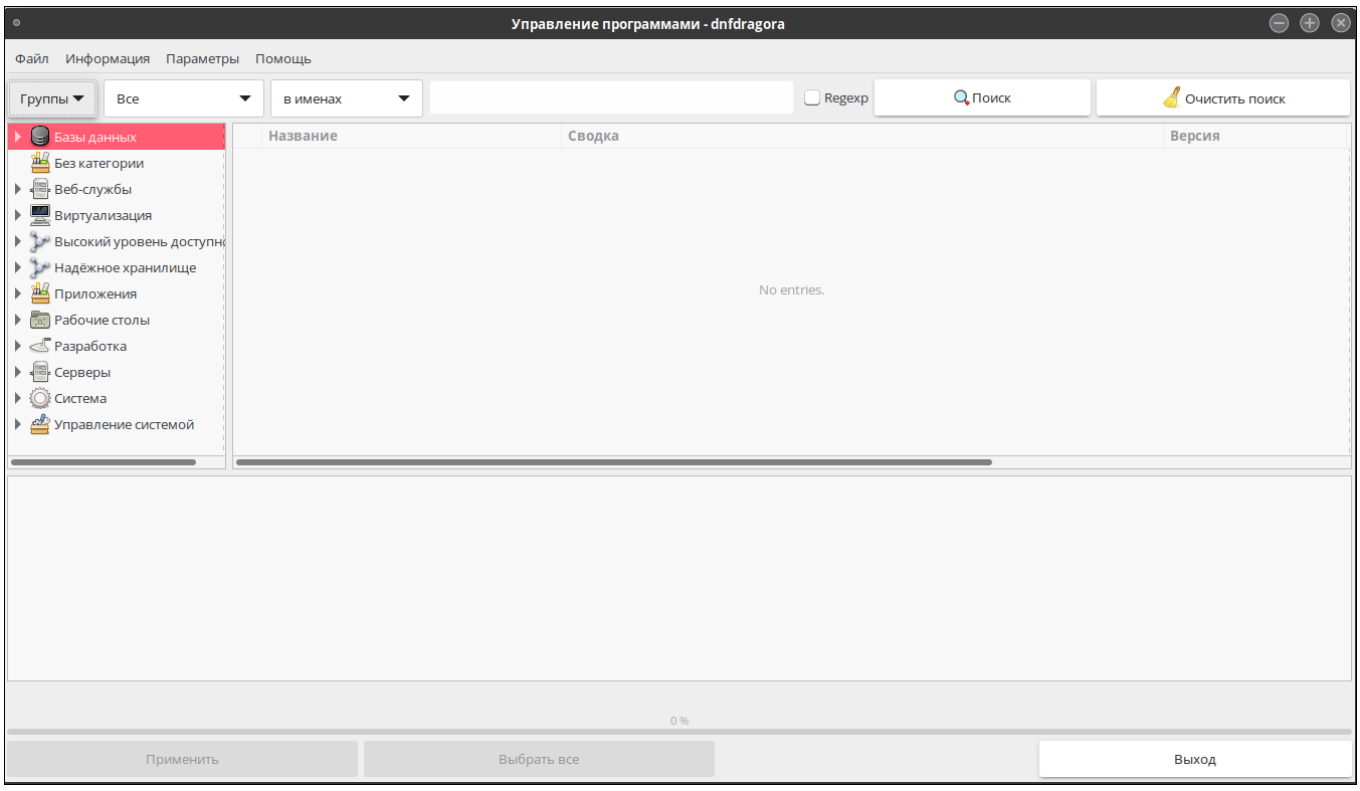
Dnfdragora установлена в РЕД ОС 7.3 по умолчанию. Если по какой-либо причине *dnfdragora* была удалена, установить ее можно через терминал **с правами администратора** системы командой:

```
dnf install dnfdragora
```

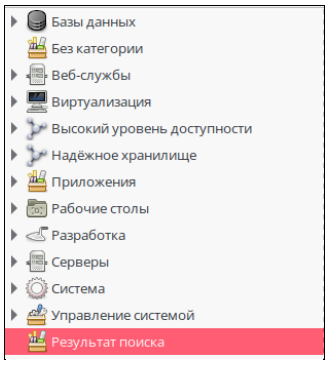
Запустить утилиту можно из «**Главного меню**» - «**Администрирование**» - «**Управление пакетами dnfdragora**».

Обзор программы

Окно программы выглядит следующим образом:

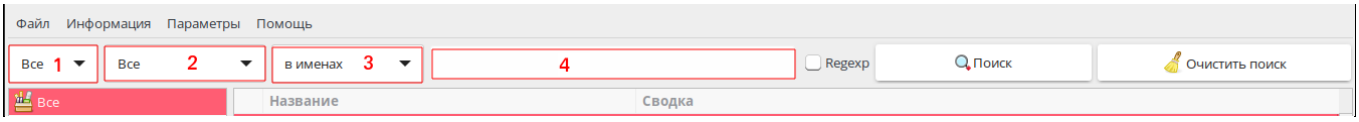


В левой части интерфейса утилиты располагается перечень групп пакетов, находящихся в репозиториях.

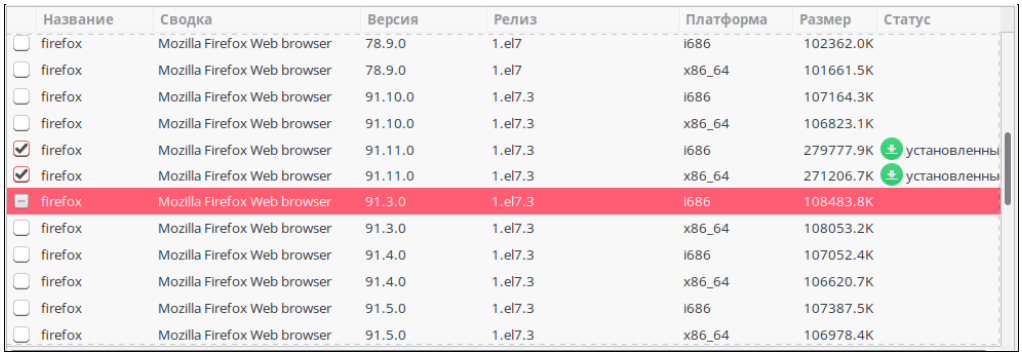


В верхней части расположена поисковая строка (**4**) и параметры поиска, отвечающие за:

- группировку пакетов (**1**);
- отображение пакетов в зависимости от их статуса или указанной архитектуры пакета (**2**);
- места поиска — в имени, описании или файлах внутри пакета (**3**).



В центральной части утилиты расположена область, где отображается результат поиска пакетов и некоторая информация о них. Здесь можно просмотреть полное название пакета, краткую сводку о нем, версию, номер релиза, платформу, размер, статус.



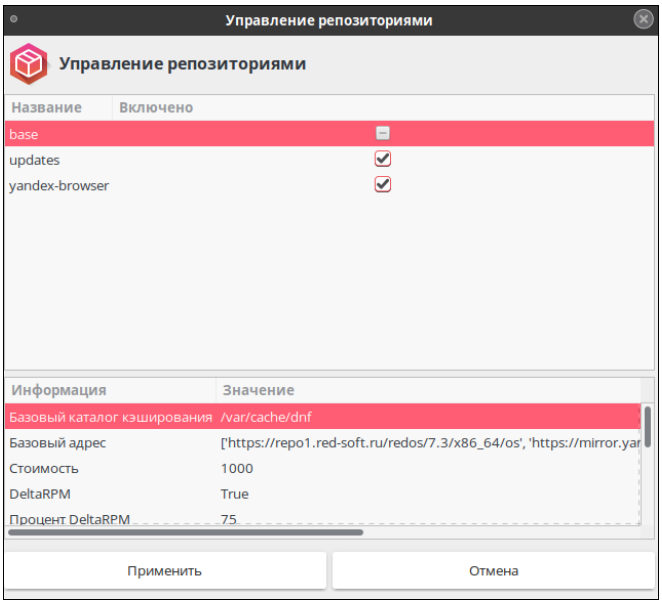
Название	Сводка	Версия	Релиз	Платформа	Размер	Статус
firefox	Mozilla Firefox Web browser	78.9.0	1.el7	i686	102362.0K	
firefox	Mozilla Firefox Web browser	78.9.0	1.el7	x86_64	101661.5K	
firefox	Mozilla Firefox Web browser	91.10.0	1.el7.3	i686	107164.3K	
firefox	Mozilla Firefox Web browser	91.10.0	1.el7.3	x86_64	106823.1K	
firefox	Mozilla Firefox Web browser	91.11.0	1.el7.3	i686	279777.9K	установленны
firefox	Mozilla Firefox Web browser	91.11.0	1.el7.3	x86_64	271206.7K	установленны
firefox	Mozilla Firefox Web browser	91.3.0	1.el7.3	i686	108483.8K	
firefox	Mozilla Firefox Web browser	91.3.0	1.el7.3	x86_64	108053.2K	
firefox	Mozilla Firefox Web browser	91.4.0	1.el7.3	i686	107052.4K	
firefox	Mozilla Firefox Web browser	91.4.0	1.el7.3	x86_64	106620.7K	
firefox	Mozilla Firefox Web browser	91.5.0	1.el7.3	i686	107387.5K	
firefox	Mozilla Firefox Web browser	91.5.0	1.el7.3	x86_64	106978.4K	

В нижней части утилиты располагается информация о выбранном пакете. Здесь указано его название, описание, имя источника установки или репозитория, из которого его можно установить, сайт разработчика, требования к системе, список файлов в пакете, журнал изменений.

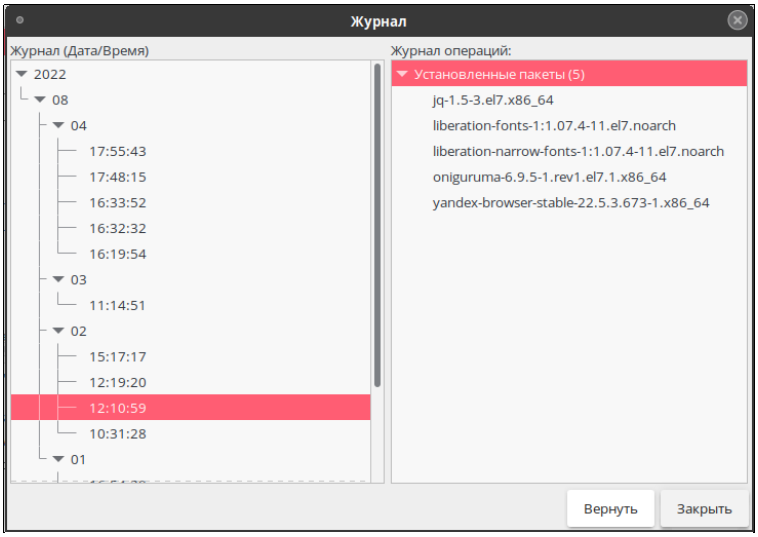


Во вкладке «**Файл**» - «**Обновить метаданные**» можно запустить обновление метаданных.

Во вкладке «**Файл**» - «**Репозитории**» можно просмотреть используемые репозитории и отключить или активировать их при необходимости.

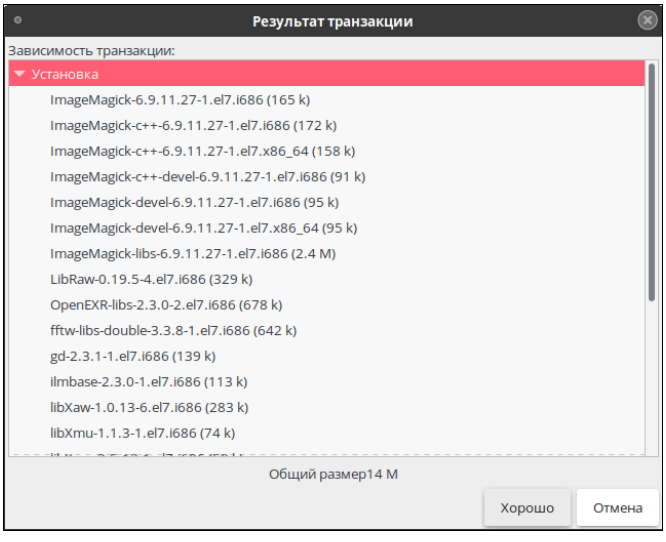


Во вкладке «**Информация**» - «**Журнал**» можно просмотреть историю операций в менеджере.



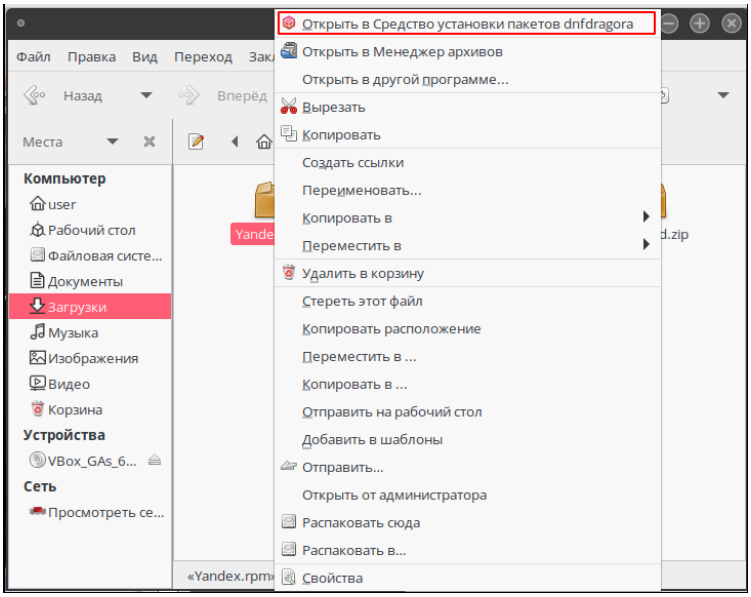
Установка/удаление пакетов

Для установки пакетов необходимо проставить признак выбора у нужного пакета (☑). Одновременно может быть выбрано несколько пакетов. После выбора пакетов нажмите «**Применить**» в левом нижнем углу. Будет выведен список транзакций, нажмите кнопку «**Хорошо**» в правом нижнем углу появившегося окна.

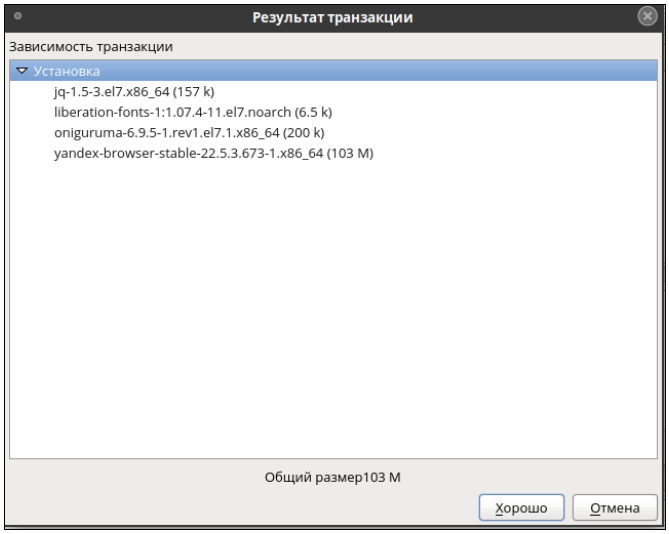


Для подтверждения выполнения операции необходимо ввести пароль (установка и удаление пакетов требует прав администратора). При успешной аутентификации начнется процесс скачивания и установки пакетов.

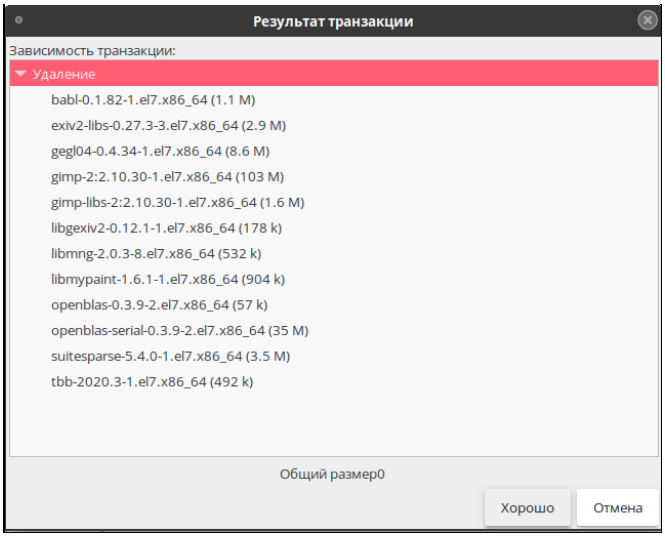
Также с помощью *dnfdragora* можно запускать установку **rpm**-пакетов с локального диска. Для этого достаточно открыть **rpm**-пакет с помощью *dnfdragora*.



Для запуска установки потребуется ввести пароль, после чего начнется установка пакета.



Для удаления пакетов необходимо найти их в перечне установленных, убрать признак выбора, после чего нажать кнопку «**Применить**».



Настройка оповещения и автоматического обновления пакетов в РЕД ОС 7.3

Настройка автоматического обновления
Настройка уведомлений пользователя через апплет dnfdragora-updater

Настройка автоматического обновления

В РЕД ОС 7.3 для оповещения/автоматического обновления пакетов используется **dnf-automatic**.

Устанавливаем *dnf-automatic* командой:

```
dnf install dnf-automatic
```

Затем настраиваем конфигурационный файл **/etc/dnf/automatic.conf**. По умолчанию *dnf-automatic* будет проверять наличие обновлений один раз в сутки и скачивать их в каталог **/var/cache/dnf/**. Конфигурационной файл для настройки автоматического обновления располагается по пути:

```
/etc/dnf/automatic.conf
```

Для того чтобы не только скачать, но и установить обновления, необходимо указать значение **"yes"** для следующих параметров в файле **/etc/dnf/automatic.conf**:

```
download_updates = yes
apply_updates = yes
```

Параметр **download_updates** отвечает за загрузку обновлений (только загрузка, без установки).

Параметр **apply_updates** указывает, применять ли загруженные обновления или нет. По умолчанию установлено: «**apply_updates = no**», так как полностью доверять автоматическому обновлению не стоит. Для того, чтобы сработало значение «**yes**» — это же значение должно быть установлено и в **download_updates**, так как если обновления не загружены, то их неоткуда устанавливать.

Параметр **random_sleep** задает генерируемую случайным образом задержку в минутах, между временем запуска утилиты *dnf-automatic* и до её исполнения. Если значение **random_sleep** более 0, то каждый раз после запуска случайным образом выбирается задержка в интервале между 0 и заданным числом минут. Этот параметр служит для предотвращения ситуации, когда множество операционных систем одновременно будут пытаться получить обновление. По умолчанию установлено: **random_sleep = 360** (360 минут = 6 часам).

Примечание! Если определенные пакеты *не требуется* обновлять (как вручную, так и автоматически), то можно добавить их в исключение. Для этого необходимо:

- Установить плагин для dnf - **versionlock** командой:

```
dnf install python3-dnf-plugin-versionlock
```

- Добавить исключения для доступных пакетов, соответствующих спецификации, следующей командой:

```
dnf versionlock exclude <package_name>
```

Просмотреть список текущих записей блокировки версий можно с помощью команды:

```
dnf versionlock list
```

или

```
dnf versionlock
```

Пример блокировки пакетов **kernel-lt** и **php**:

```
dnf versionlock exclude php kernel-lt

Последняя проверка окончания срока действия метаданных: 0:53:11 назад, Пн 29 мар 2021 15:32:06.
```

```
Добавление исключения на: kernel-lt-0:5.10.24-2.el7.*
Добавление исключения на: kernel-lt-0:5.10.1-1.el7.*
Добавление исключения на: php-0:7.4.11-2.el7.*
```

Чтобы удалить пакет из исключения, выполните следующую команду:

```
dnf versionlock delete <package_name>
```

Чтобы полностью очистить блокировку пакетов, выполните следующую команду:

```
dnf versionlock clear
```

Для отправки уведомлений о прошедших обновлениях на почту перейдите к блоку **[email]** в файле **automatic.conf**. Отредактируйте следующие параметры:

- *email_from* — отправитель сообщения;
- *email_to* — кому будут отправлены сообщения;
- *email_host* — имя хоста, к которому будет подключаться утилита, чтобы отправить сообщения.

В блоке **[emitters]** поменяйте параметр **emit_via** с *stdio* на *email*.

```
emit_via = stdio
```

Если *emit_via* будет пустым или *None*, то это аналогично параметру «**update_messages = no**», и в этом случае сообщения выводится не будут.

По умолчанию *emit_via* установлен в **emit_via = stdin**. В этом случае сообщения будут хранится по пути **/var/spool/mail/<имя_пользователя>**. Чтобы их просмотреть, используйте утилиту **cat**:

```
cat /var/spool/mail/<имя_пользователя>
```

Также в блоке **[emitters]** доступен параметр **system_name**. Он служит для записи названия системы, которое будет отображаться в сообщениях. По умолчанию *system_name* настроено так: **system_name = None**, это означает, что названием будет служить *hostname* операционной системы.

Далее нужно добавить соответствующий сервис в автозагрузку и запустить его. После этого обновления нужного типа будут устанавливаться в систему автоматически.

```
systemctl enable --now dnf-automatic.timer
```

Проверить статус таймеров можно командой:

```
systemctl list-timers *dnf-*
```

```
[root@dc1 wolandius]# systemctl list-timers *dnf-*
NEXT                        LEFT       LAST                        PASSED   UNIT                ACTIVATES
Fri 2021-03-26 16:16:57 MSK 51min left Fri 2021-03-26 15:16:57 MSK 8min ago dnf-makecache.timer dnf-makecache.service
Sat 2021-03-27 06:35:51 MSK 15h left   n/a                         n/a      dnf-automatic.timer dnf-automatic.service

2 timers listed.
```

При более детальном изучении таймера, можно заметить, что автоматические обновления настроены на 6 утра каждого дня. Данные конфигурации отражены в файле **/usr/lib/systemd/system/dnf-automatic.timer**.

Содержимое файла по умолчанию:

```
[Unit]
Description=dnf-automatic timer
# See comment in dnf-makecache.service
ConditionPathExists=!/run/ostree-booted
Wants=network-online.target

[Timer]
OnCalendar=*-*-* 6:00
RandomizedDelaySec=60m
Persistent=true

[Install]
WantedBy=timers.target
```

Чтобы задать свое время, требуется изменить строку:

```
OnCalendar=*-*-* 6:00
```

После применения изменений выполните команды перезапуска таймера:

```
systemctl daemon-reload
systemctl restart dnf-automatic
```

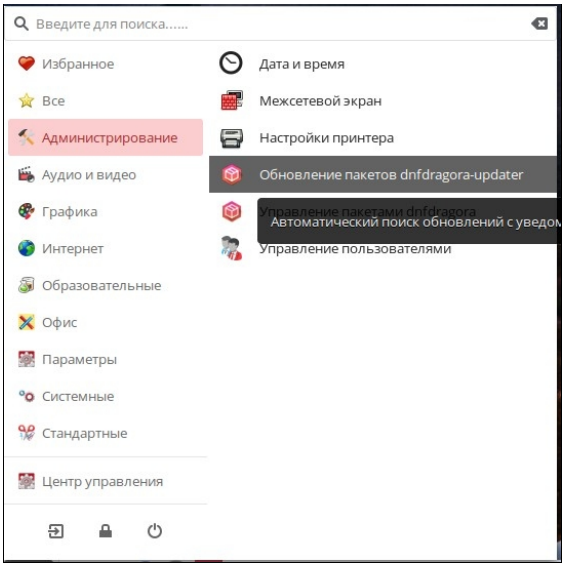
Настройка уведомлений пользователя через апплет dnfdragora-updater

Для того чтобы установить данный апплет, требуется выполнить команду:

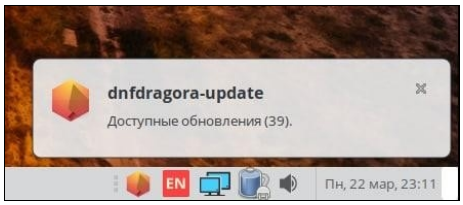
```
dnf install dnfdragora-updater
```

Предварительно, до использования данного апплета, требуется запустить **dnfdragora** (если это действие еще не совершалось после установки ОС) для создания кэша пакетов.

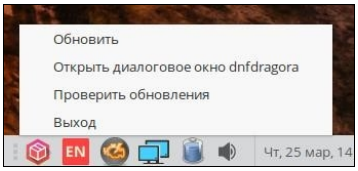
Запустить данный апплет можно из меню:



При получении обновления пользователь получит уведомление следующего вида:



Данный апплет имеет интуитивно понятное контекстное меню:



Назначение RPM

RPM – это менеджер пакетов, который может быть использован для сборки, установки, запроса, проверки, обновления и удаления отдельных программных пакетов.

Пакеты содержат архив с файлами и метаданные, используемые для установки и удаления файлов архива. Метаданные включают сценарии, атрибуты файлов и информацию с описанием конкретного пакета.

Пакеты бывают двух типов: двоичные пакеты, используемые для объединения устанавливаемых программ, и пакеты с исходными кодами, включающие исходные коды и описание способа формирования двоичного пакета.

База данных **RPM** ведётся в каталоге **/var/lib/rpm**. Она состоит из одиночной базы данных (**Packages**), в которой хранится вся информация о пакетах, и множества маленьких баз (**__db.001**, **__db.002** и т. д.), которые служат для индексации и содержат в себе сведения о том, какие файлы менялись и создавались при установке и удалении пакетов.

Если база данных повреждена (что может произойти, если процесс установки или удаления был принудительно завершен или закончилось место на разделе), то её можно восстановить, выполнив команду `rpm --rebuilddb`.

Если база была уничтожена — рекомендуется восстановить заранее созданную резервную копию.

Каждый пакет **RPM** имеет название, которое состоит из нескольких частей:

- название программы;
- версия программы;
- номер выпущенной версии (количество раз пересборки программы одной и той же версии);
- архитектура, под которую собран пакет (i386, ppc и т. д.)

Собранный пакет обычно имеет такой формат названия:

```
<название>-<версия>-<выпуск>.<архитектура>.rpm
```

Например:

```
nano-0.98-2.i386.rpm
```

Иногда в пакет входят исходные коды. Такие пакеты не содержат информации об архитектуре, она заменяется на **src**. Например:

```
libgnomeuimm2.0-2.0.0-3.src.rpm
```

Библиотеки чаще всего распространяются в двух отдельных пакетах. Первый содержит собранный код, второй (обычно к нему добавляют **-devel**) содержит заголовочные файлы и другие файлы, необходимые разработчикам. Необходимо следить за тем, чтобы версии этих двух пакетов совпадали, иначе библиотеки могут работать некорректно. Пакеты с расширением **noarch.rpm** не зависят от конкретной архитектуры компьютера. Обычно они содержат графику и тексты, используемые другими программами.

Основной список команд RPM

Если необходимо удалить определенный пакет, назовем его rpm_some_package, то нужно выполнить команду:

```
rpm -e rpm_some_package
```

Если необходимо показать список всех установленных rpm пакетов, используйте:

```
rpm -qa
```

PS: Можно отобрать нужные пакеты (со всех установленный) и показать список, например для nginx:

```
rpm -qa | grep nginx
```

Допустим, вам нужно просмотреть некоторую информацию о конкретном пакете (допустим — это rpm_some_package):

```
rpm -qi rpm_some_package
```

Если необходимо установить определенный пакет, назовем его rpm_some_package с выводом на экран и с прогресс-баром то нужно выполнить команду:

```
rpm -ivh rpm_some_package.rpm
```

Если необходимо обновить некий пакет rpm_some_package, но без всяких изменений в конфигурационных файлов (если отсутствует пакет, то он будет установлен):

```
rpm -Uvh rpm_some_package.rpm
```

Чтобы установить пакет rpm_some_package с выводом всех действий на экран и без контроля всех зависимостей, используйте:

```
rpm -ivh --nodeps rpm_some_package.rpm
```

Чтобы обновить пакет rpm_some_package (если он установлен), используйте:

```
rpm -F rpm_some_package.rpm
```

Чтобы показать список функциональностей которые предоставляются, выполните:

```
rpm -qip rpm_some_package --whatprovides
```

Показать историю ревизий данного пакета rpm_some_package:

```
rpm -qip rpm_some_package --changelog
```

Вывести скрипты, которые запускаются при установке/удалении пакета rpm_some_package:

```
rpm -qip rpm_some_package --scripts
```

Выполнить проверку (узнать какому пакету относится указанный файл), то нужно прописать полный путь к файлу:

```
rpm -qf /путь/к/файлу
```

Показать список файлов конфигурации которые входят в пакет rpm_some_package:

```
rpm -qc rpm_some_package
```

Показать весь список файлов которые входят в пакет rpm_some_package:

```
rpm -qlp rpm_some_package
```

Показать список всех пакетов, которые необходимы для установки данного пакета rpm_some_package по его зависимостям:

```
rpm -q rpm_some_package --whatrequires
```

Вывести список файлов, которые входят в пакет, но ещё не установленны в систему:

```
rpm -qp rpm_some_package.rpm -l
```

Команда что ниже выводит список всех rpm зависимостей:

```
rpm -qpR rpm_some_package.rpm
```

Если вы случайно обновили rpm до новой версии, вы можете вернуть все как было, используя команду:

```
rpm -Uvh --oldpackage rpm_some_package-<old-version>.rpm
```

Вывести содержимое всех пакетов которые установлены на ОС:

```
rpm -Va
```

Выполнить установку пакета, который собранный из исходных кода:

```
rpm -ivh /usr/src/redhat/RPMS/`arch`/rpm_some_package.rpm
```

Выполнить проверку пакета, который ещё не установлен на сервере:

```
rpm -Vp rpm_some_package.rpm
```

Извлечь из пакета файлы которые содержат в своём имени bin:

```
rpm2cpio rpm_some_package.rpm | cpio --extract --make-directories *bin*
```

Выполнить импорт публичный (public) ключа с цифровой подписью:

```
rpm --import /media/cdrom/RPM-GPG-KEY
```

Выполнить проверку подписи пакета rpm_some_package:

```
rpm --checksig rpm_some_package.rpm
```

Выполнить проверку на целостность установленного содержимого пакета:

```
rpm -qa gpg-pubkey
```

Показать какой размер, полномочия, тип, владельца, группу, а так же MD5 сумму и дату последнего изменения пакета rpm_some_package:

```
rpm -V rpm_some_package
```

Выполнить сборку пакета rpm_some_package из исходного кода:

```
rpmbuild --rebuild rpm_some_package.src.rpm
```

Для более детального ознакомления, используйте:

```
rpm --help
```

Преобразование форматов систем управления пакетами с помощью alien

Преобразование .deb в .rpm
Преобразование .rpm в .deb
Ключи и атрибуты alien

Alien – полезная утилита, созданная для преобразования форматов различных систем управления пакетами Linux.

Поддерживается преобразование между пакетами: Linux Standard Base (**.lsb**), Redhat (**.rpm**), Debian (**.deb**), Stampede (**.slp**), Solaris (**.pkg**) и Slackware (**.tgz**).

Для установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install alien
```

Преобразование .deb в .rpm

> Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Для преобразования файла **.deb** в файл **.rpm** с изменением стандартных для Debian-пакета инсталляционных скриптов используется опция **-r**. На выходе получится RPM-пакет.

В следующем примере файл *libreoffice-writer_7.0.5-0ubuntu0.20.10.1_amd64.deb* преобразуется в файл *libreoffice-writer-7.0.5-1.x86_64.rpm*:

```
alien -r --scripts libreoffice-writer_7.0.5-0ubuntu0.20.10.1_amd64.deb

libreoffice-writer-7.0.5-1.x86_64.rpm generated
```

Преобразование .rpm в .deb

Для преобразования файла **.rpm** в файл **.deb** используется опция **-d**. На выходе получится DEB-пакет:

```
alien -d --scripts libreoffice-writer-7.0.5-1.x86_64.rpm

libreoffice-writer_7.0.5-2_amd64.deb generated
```

Для того чтобы сгенерировать дерево, не создавая пакет, используется опция **-g**:

```
alien -g -c libreoffice-writer-7.0.5-1.x86_64.rpm

Directories  libreoffice-writer-7.0.5 and  libreoffice-writer-7.0.5.orig prepared
```

В корневом каталоге создались два подкаталога, не конвертируя пакет.

Alien позволяет преобразовывать сразу несколько файлов, для этого нужно последовательно прописать название двух или более пакетов:

```
alien -r -c firefox_89.0+build2-0ubuntu0.20.04.2_amd64.deb chromium-browser_85.0.4183.83-0ubuntu0.20.04.2_amd64.deb

firefox-89.0+build2-1.x86_64 generated
chromium-browser-85.0.4183.83-1.x86_64.rpm generated
```

Вы также можете использовать alien для преобразования файлов в пакет Stampede **.slp**, пакет LSB и пакет Slackware **.tgz**. Выполните **alien -h**, чтобы увидеть доступные параметры.

Ключи и атрибуты alien

- *file [...]* – задать список файлов пакета для конвертирования;
- *-to-deb, -d* – конвертировать в deb (используется приложением "по умолчанию");
- *-to-rpm, -r* – конвертировать в rpm;
- *-to-tgz, -t* – создать tgz-пакет;
- *-to-slp* – создать Stampede slp пакет;
- *-to-lsb, -l* – создать LSB пакет;
- *-to-pkg, -p* – создать Solaris pkg пакет;
- *-i* – автоматически установить все сгенерированные пакеты и после этого удалить сам файл пакета;
- *-g* – сгенерировать дерево построения, не создавая пакет;
- *-c* – включить скрипты в пакет;
- *-v* – отображать каждую команду, которую выполняет alien;
- *-k* – не менять версию генерируемых пакетов;
- *-V* – показать номер версии alien;
- *-h* – показать справку.

Процессы в РЕД ОС

Работа с процессами
Список запущенных процессов
Завершение процесса

Практически в любом контексте можно заменить слово «**процесс**» терминами «программа», «команда» или «задача». Внутри Linux-подобных систем нет принципиальных отличий между программой и командой. Обычно программы с текстовым выводом информации, например, **ls**, часто называются «командами».

Чтобы создать процесс, необходимо запустить на выполнение какой-либо исполняемый файл, то есть файл, у которого установлен атрибут «исполняемый». Иногда говорят, что надо «выполнить файл» или «выполнить команду».

После того как содержимое запущенного файла будет считано и помещено в оперативную память, а также будут размещены необходимые для работы программы данные, процесс начнет своё существование. Такой «живой» процесс иногда называют «задачей». Отсюда можно сформулировать определение: **процесс** — это совокупность программного кода и данных, загруженных в память вычислительного устройства.

Процесс может находиться в различных состояниях, обычно выделяют три основных состояния:

- *работающий процесс* — в данный момент времени код процесса выполняется, т.е. процесс занимает определенную часть ресурсов центрального процессора (процессорного времени);
- *спящий процесс* — в данный момент времени код процесса не выполняется, находясь в ожидании какого-либо события (например, нажатия клавиш на клавиатуре, поступление данных по сети и т.д.);
- *процесс-«зомби»* — состояние, когда сам процесс уже не существует, его код и данные выгружены из оперативной памяти, но запись в таблице процессов остаётся по тем или иным причинам.

Запустить программу или породить процесс можно двумя способами:

1) вводом имени команды в терминале и нажатием «Enter»;

2) нажатием ЛКМ по пиктограмме приложения в Главном меню или на Рабочем столе.

Вы можете подробнее ознакомиться с процессами, просмотрев наши обучающие видео:

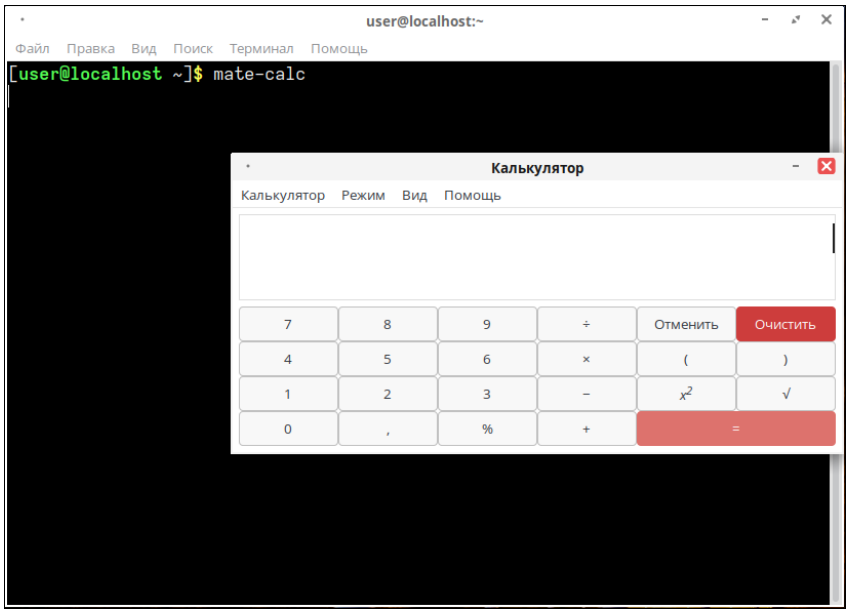
- на **RuTube** — Процессы в среде РЕД ОС;
- в **Яндекс.Дзен** — Процессы в среде РЕД ОС;
- в **VK Видео** — Процессы в среде РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

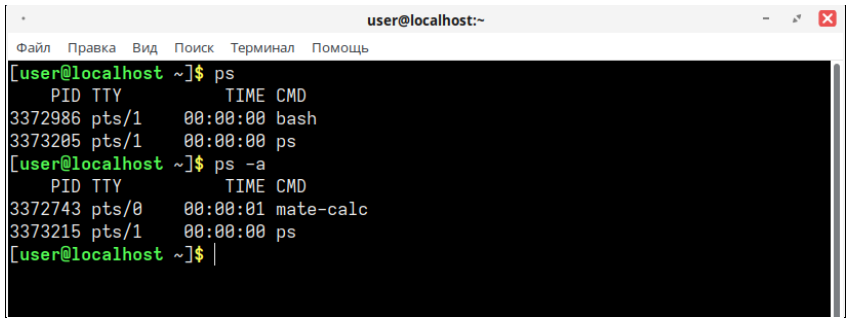
Работа с процессами

В качестве примера запустим приложение «Калькулятор» из командной строки, для чего необходимо открыть окно терминала и выполнить команду:

```
mate-calc
```



Затем откроем второе окно терминала и выполним последовательно команды `ps` и `ps -a`:



Вывод команд отличается.

Команда **ps** (*proccesses*) — это утилита командной строки, позволяющая работать со списком процессов в системе. Вызванная без параметров, она выводит список процессов, запущенных в данном терминале — в выводе показано, что были запущены командная оболочка **bash** и сама утилита **ps**.

Ключ **-a** позволяет вывести все интерактивные процессы, запущенные данным пользователем — в выводе команды отображается mate-calc, который был выполнен из другого терминального окна.

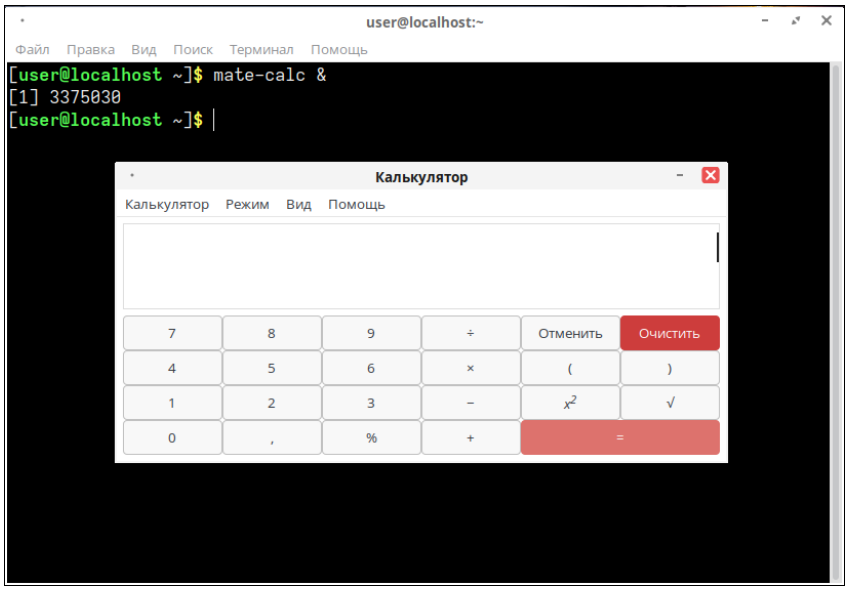
При закрытии окна терминала, из которого запускался калькулятор, будет закрыто и само приложение «Калькулятор». Обычно процессы связаны с терминалом, из которого они запускались. Такой терминал называется управляющим терминалом для процесса.

Именно названия терминалов были указаны в колонке **TTY** вывода запущенных ранее команд `ps` и `ps -a` — **pts/0** и **pts/1**.

```
[user@localhost ~]$ ps -a
    PID TTY          TIME CMD
3372743 pts/0    00:00:01 mate-calc
3373215 pts/1    00:00:00 ps
```

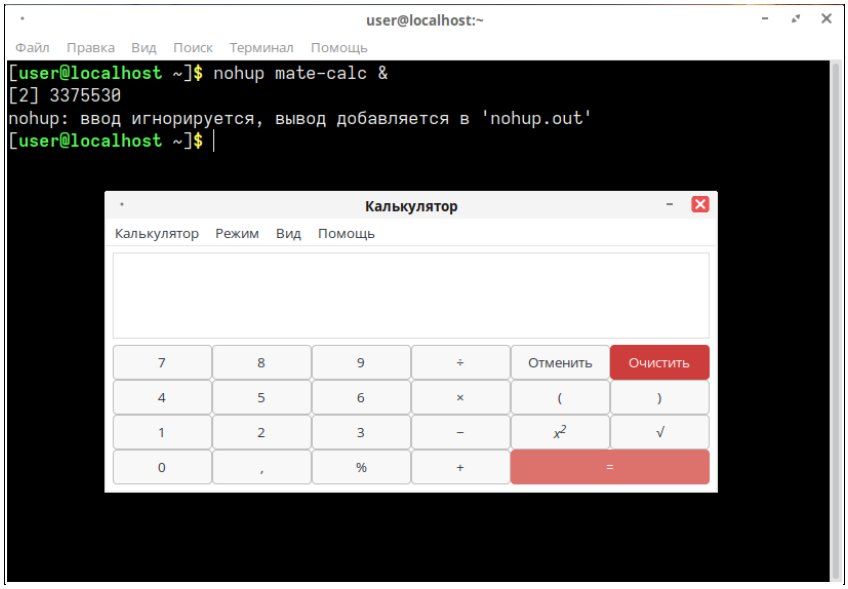
Важно также отметить, что калькулятор после запуска занял терминал — командная строка не появилась и процесс интерактивной работы с консолью в этом окне стал невозможным.

Когда необходимо выполнить программу так, чтобы она не занимала терминальное окно, следует запустить процесс как демон (так, например, выполняются службы в Windows). Для этого в качестве последнего аргумента командной строки указывается символ «**&**»:



Калькулятор запускается, а терминал доступен для дальнейшей работы. Однако, если снова закрыть окно терминала, калькулятор также прекратит работу. То есть управляющий терминал, даже если он предоставляет возможность дальнейшей работы с ним, всё равно является важным звеном в работе порождённого процесса.

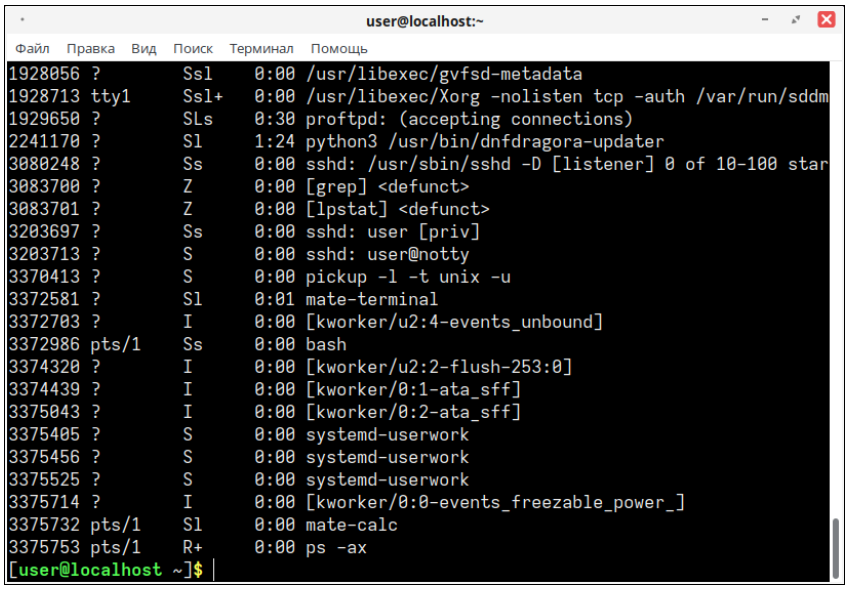
В случае, когда необходимо освободить терминал для работы и сделать запущенный процесс независимым, используется команда `nohup`, которая отвязывает процесс от управляющего терминала:



Теперь можно закрыть терминальное окно, а калькулятор продолжит свою работу. Причём в выводе команды `ps` данный процесс уже не будет отображен.

Список запущенных процессов

Чтобы увидеть весь список процессов, запущенных пользователем, включая не имеющие управляющего терминала, следует добавить ключ **-x** (`ps -ax`):



В конце выведенного списка отображается mate-calc, напротив которого вместо имени терминала стоит знак вопроса.

В *первом столбце* списка процессов отображаются некоторые числовые значения — это идентификаторы процессов — **PID** (***P**roccess **ID**entificator*), являющиеся «именами», по которым ядро операционной системы общается с процессами.

В *третьем столбце* списка запущенных процессов (**STAT**) находятся сокращённые обозначения состояния процесса:

- **R** — процесс выполняется в данный момент времени;
- **I** — простаивающий процесс;
- **D** — процесс выполняется, но ожидает ввода/вывода;
- **S** — спящий процесс;
- **T** — процесс остановлен, но пока не удалён из списка процессов и не выгружен его код из памяти;
- **X** — процесс мёртв, то есть код и данные находятся в памяти, но процесс не отзывается;
- **Z** — процесс-«зомби».

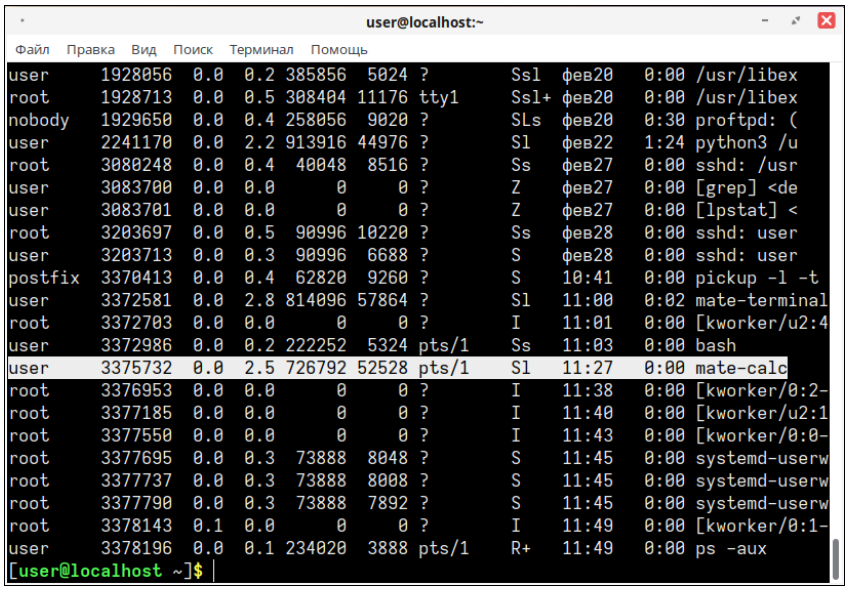
Каждый процесс инициализируется в сеансе какого-либо пользователя, и этот пользователь становится владельцем процесса. Если управляющий терминал можно убрать, то владельца у процесса изъять невозможно, однако его можно сменить на другого пользователя.

Таким образом, все файловые операции, которые будет выполнять процесс (если в программе это заложено), будут реализовываться в соответствии с правами доступа пользователя — владельца процесса.

Для просмотра владельца процесса утилитой ps используется ключ **-u**. Выполните команду:

```
ps -aux
```

В *первом столбце* списка процессов теперь будут отображены имена пользователей — владельцев процесса.



Например, при попытке сохранить файл *LibreOffice Writer* в каталоге **/etc** — будет выведено сообщение об ошибке, информирующее о том, что сохранение невозможно из-за недостатка прав. Такая ситуация возникает, потому что процесс редактора *LibreOffice Writer* запускается с правами локального пользователя, а права на запись в паку **/etc** имеет **только** суперпользователь **root** (в чём можно убедиться в выводе команды `ls -l /etc`)!

Завершение процесса

Для завершения какого-либо запущенного процесса используется утилита **kill**. В качестве аргумента утилите необходимо передать **PID** процесса, который можно уточнить с помощью описанных выше команд. Подробную информацию об использовании утилиты **kill** см. в нашей статье «Основные утилиты в консоли РЕД ОС».

Следует обратить внимание на то, что пользователь может завершить только тот процесс, для которого он является владельцем. Администратор **root** может посылать любые сигналы любому процессу в системе, следовательно, может и прекратить работу любого процесса.

Получение сведений о процессах в РЕД ОС

Содержимое каталога /proc
Назначение файлов в каталогах процессов /proc/<PID>
Структура каталога /proc/sys

Процесс — это экземпляр запущенной программы. Каждый раз, когда в терминале выполняется какая-либо команда, система создает новый процесс. Процессы в операционной системе имеют числовой идентификатор, называемый **PID**.

Программы пространства пользователя в РЕД ОС не могут обращаться к ядру системы напрямую. Однако для получения информации от ядра были созданы некоторые специальные каталоги, с помощью которых любая программа или пользователь может получить данные о состоянии компьютера и ядра – это каталоги **/proc** и **/sys**.

Вы можете подробнее ознакомиться с назначением каталога **/proc** и файловой системы **procfs**, просмотрев наши обучающие видео:

- на **RuTube** — Файловая система procfs;
- в **Яндекс.Дзен** — Файловая система procfs.
- в **VK Видео** — Файловая система procfs.

На наших каналах вы также сможете найти много другой полезной информации.

С дополнительной информацией о работе с процессами можно ознакомиться в нашей статье «Процессы в РЕД ОС».

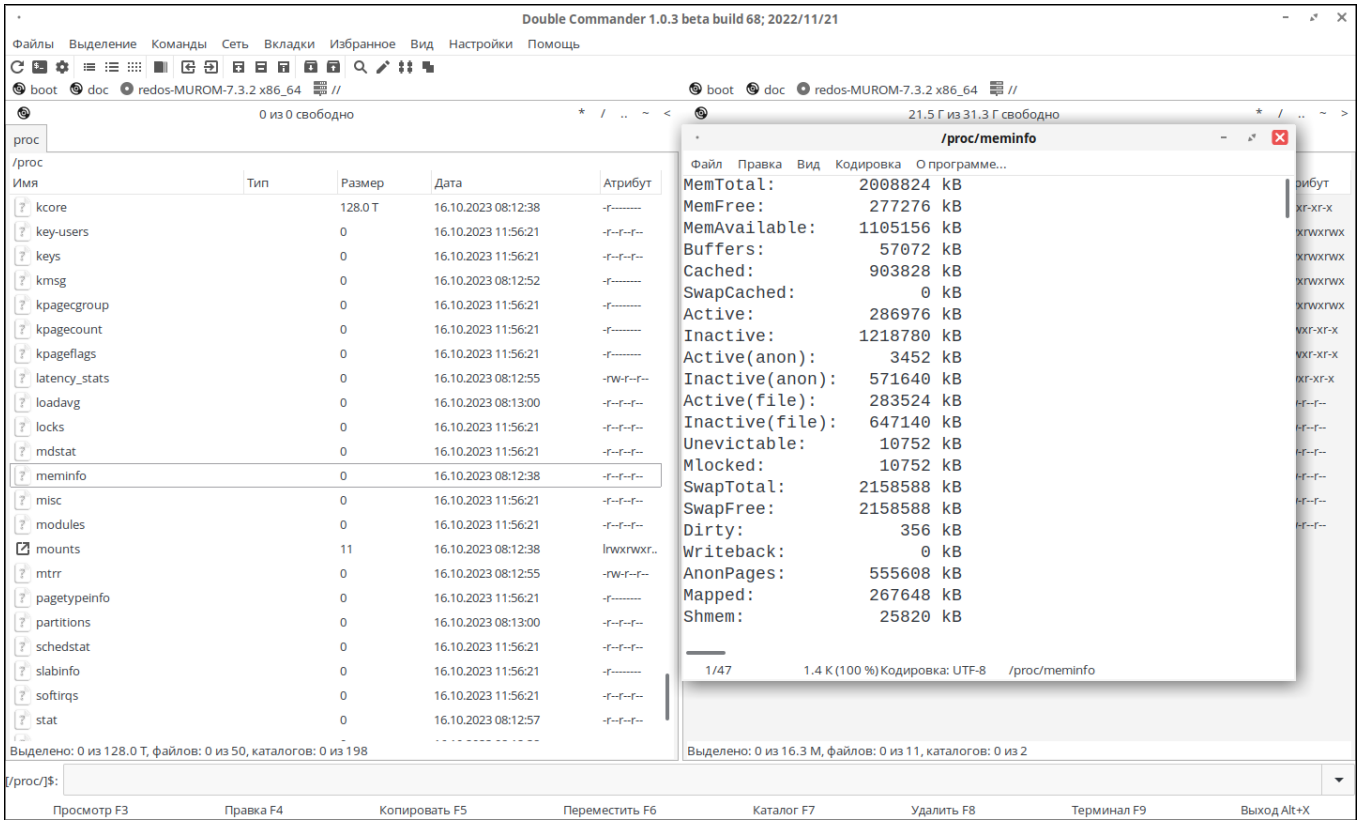
В рамках текущей статьи будет рассмотрен механизм получения сведений о процессах, на котором основаны все программы, позволяющие работать с процессами – работа с каталогом **/proc**.

В каталог **/proc** монтируется специальная файловая система **procfs**.

procfs — специальная файловая система, используемая в UNIX-подобных операционных системах, позволяющая получить доступ к информации из ядра о системных процессах, необходима для выполнения таких команд, как `ps`, `w`, `top`.

На самом деле каталог **/proc** – это не обычный каталог. Все подкаталоги, файлы и хранящаяся в них информация генерируются ядром «на лету», как только пользователь ее запрашивает. Работа построена таким образом, что пользователь может не заметить разницы между обычной файловой системой и **proc**, если откроет ее с помощью файлового менеджера.

Каталог **/proc** содержит файлы нулевого размера, у каждого файла отображается текущая дата создания. Например, файл **/proc/meminfo** будет содержать разные данные при каждом открытии, поскольку использование памяти постоянно изменяется.



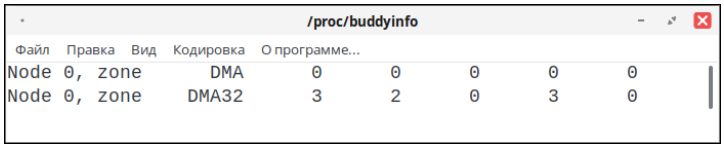
С помощью такого механизма разработчики придерживаются главной концепции Unix: «Всё – есть файл». Все файлы доступны для изменения любым редактором, и все они представлены в простом текстовом формате, но для того чтобы проанализировать весь

каталог, необходимы права суперпользователя (**root**).

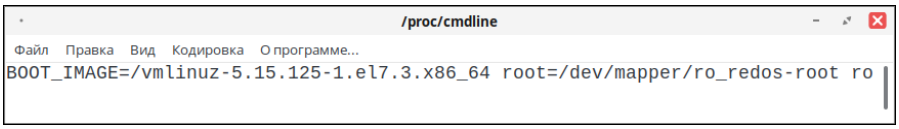
Большинство файлов в каталоге **/proc** доступны только для чтения, с их помощью можно только просмотреть информацию. Однако существуют и доступные для записи файлы, в частности – каталог **/proc/sys**, с помощью которого можно настраивать различные параметры ядра.

Содержимое каталога /proc

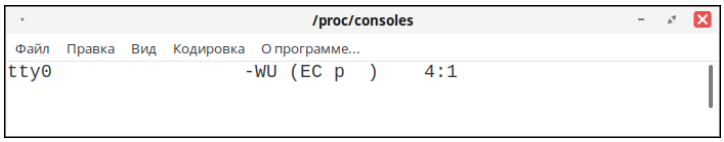
/proc/buddyinfo – файл отображает информацию о фрагментации памяти в ядре системы. Чаще всего используется для диагностики проблем с фрагментацией памяти.



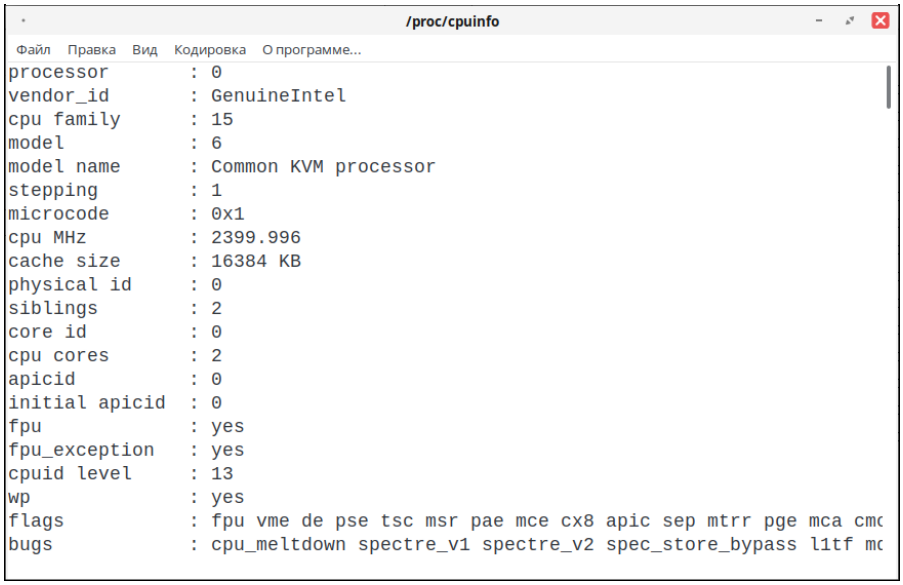
/proc/cmdline – файл отображает информацию о параметрах, которые были указаны в строке запуска ядра загрузчиком **grub**. Может быть полезно при поиске и устранении проблем с загрузкой ядра или в случае необходимости выявления файла, использованного для загрузки.



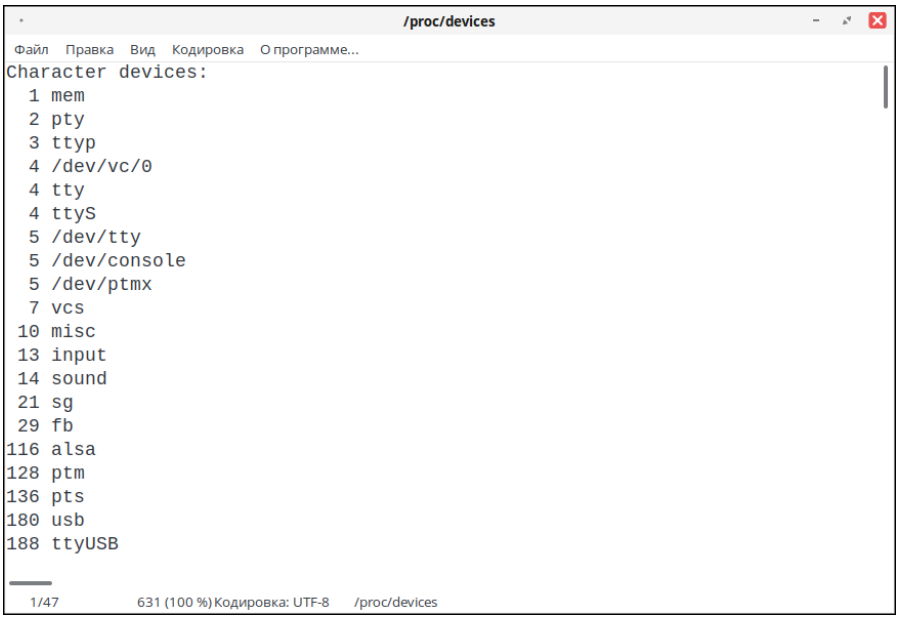
/proc/consoles – файл отображает информацию о зарегистрированных в ядре символических устройствах для системной консоли **/dev/console**.



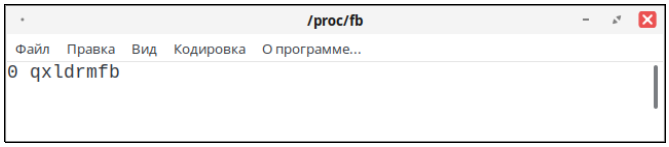
/proc/cpuinfo – файл отображает очень подробную информацию о процессоре. Здесь можно просмотреть производителя, количество ядер, объем кеша, активные ядра, частоту, поддерживаемые расширения и многое другое. Ту же информацию можно получить с помощью специальных команд, однако все скрипты, выводящие информацию о процессоре, берут ее из каталога **/proc**.



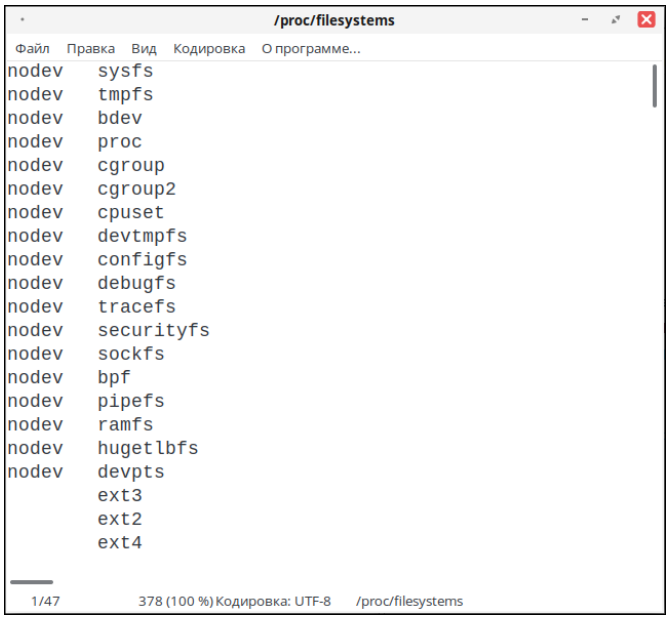
/proc/devices – файл отображает информацию о различных блочных и символических устройствах, подключенных к системе, кроме тех, для которых не загружены модули ядра. Устройства разделены на *символические* и *блочные*. У символических устройств нет буфера хранения, поэтому они отправляют ядру данные определенного размера. Блочные устройства имеют буфер для данных и предназначены для сохранения информации, например, на жесткие диски.



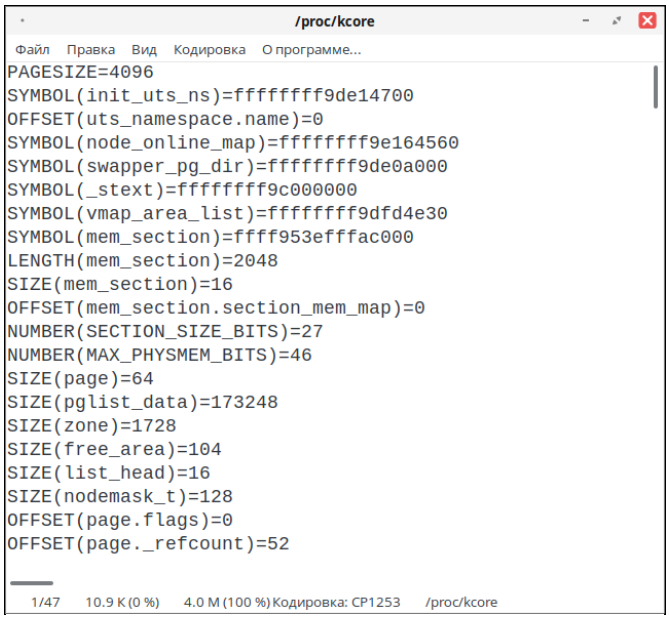
/proc/fb – файл отображает информацию об устройствах фреймбуфера (экраны), а также используемые графические драйверы. Файл является одним из способов просмотра используемого драйвера видеокарты.



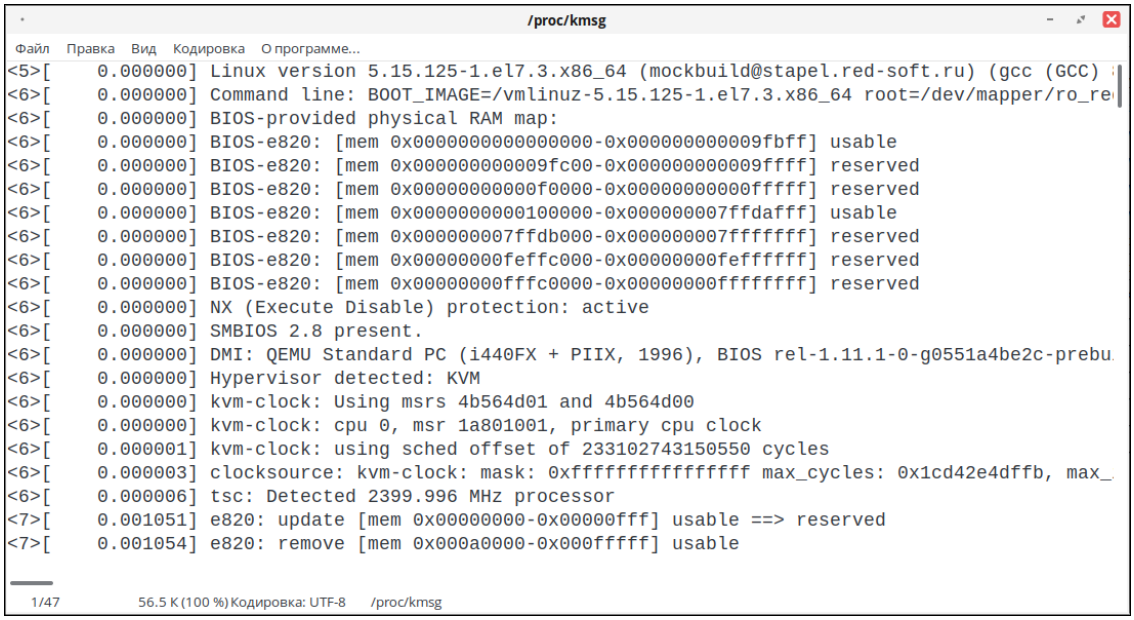
/proc/filesystems – файл содержит список файловых систем, которые на данный момент поддерживаются ядром. Значение **nodev** показывает, что это файловая система специального назначения, и она не используется для хранения данных на носителях.



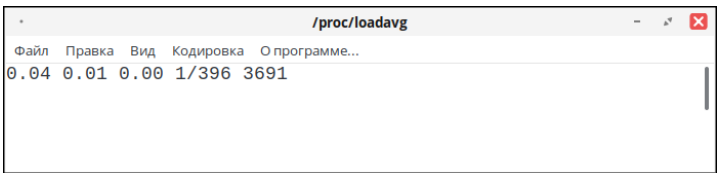
/proc/kcore – это все содержимое оперативной памяти, представленное в одном файле. В отличие от других у этого файла есть размер – объем ОЗУ плюс 4 Кб. Для доступа к файлу необходимы права суперпользователя (**root**). Перед работой с файлом его необходимо скопировать в другой каталог, а затем выполнять требуемые действия.



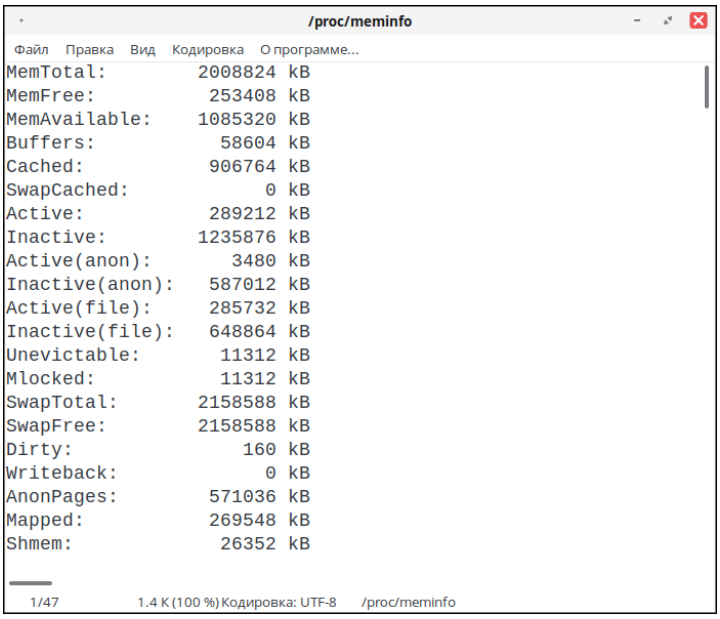
/proc/kmsg – файл накапливает и сохраняет сообщения ядра. Сообщения можно посмотреть также с помощью утилиты **dmesg**. Для доступа к файлу потребуются права суперпользователя (**root**).



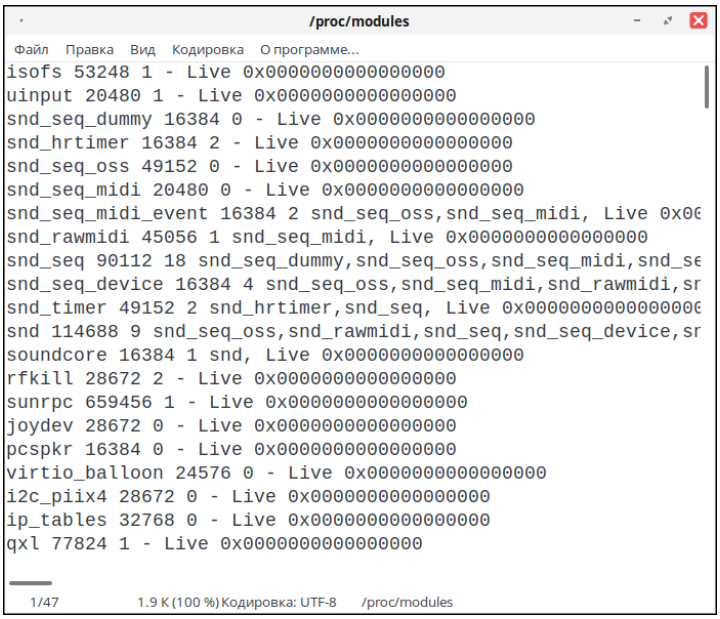
/proc/loadavg – файл позволяет оценить среднюю нагрузку на систему. Первые три цифры показывают нагрузку на процессор в данный момент времени, 5 минут назад и 15 минут назад, следующие два столбца показывают количество активных процессов и общее количество запущенных процессов. Последняя цифра — это идентификатор последнего процесса (**PID**).



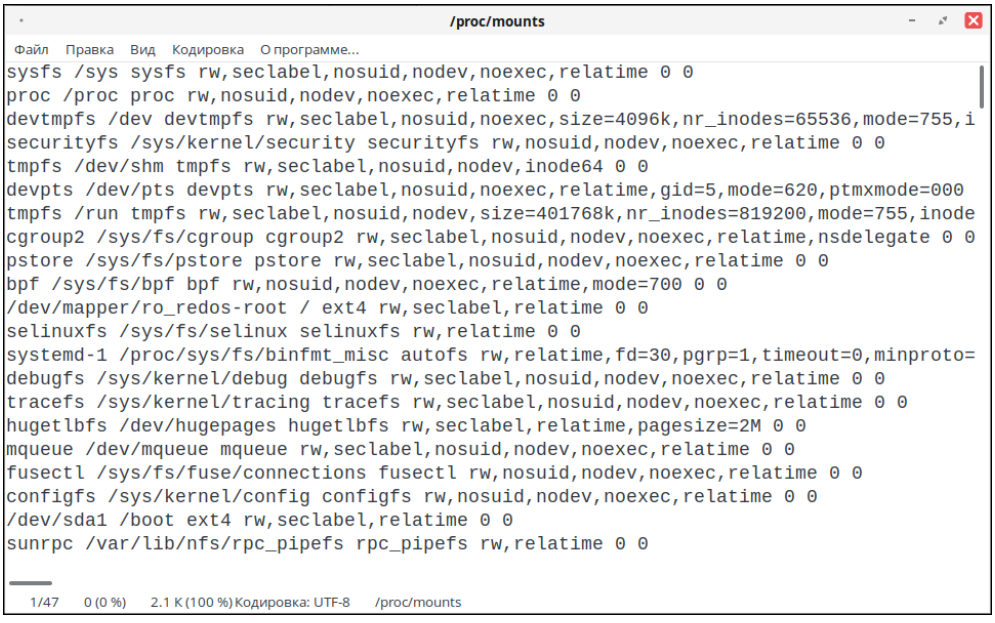
/proc/meminfo – файл отображает всю доступную информацию об оперативной памяти и пространстве подкачки.



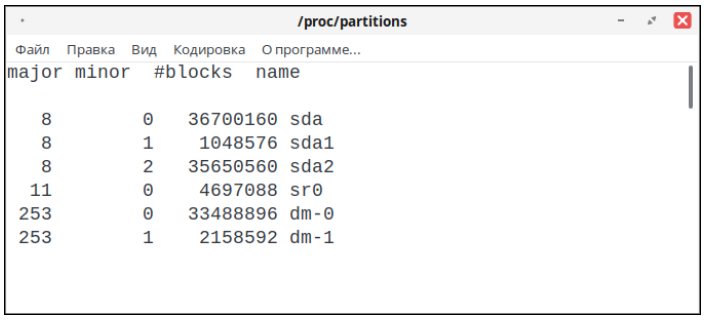
/proc/modules – файл содержит список всех загруженных модулей ядра. Ту же информацию можно увидеть, выполнив команду **lsmod**.



/proc/mounts – файл содержит все точки монтирования и все подключенные файловые системы.



/proc/partitions – в файле отображены все подключенные к системе разделы жестких дисков или других запоминающих устройств.



Назначение файлов в каталогах процессов /proc/<PID>

Для отображения файлов какого-либо процесса следует открыть каталог с номером необходимого процесса. В каждом каталоге более 50 файлов.

Далее будет рассмотрено назначение некоторых файлов:

- **cmdline** – содержит команду, с помощью которой был запущен процесс, а также переданные ей параметры;
- **cwd** – символическая ссылка на текущий рабочий каталог процесса;
- **exe** – ссылка на исполняемый файл;
- **root** – ссылка на каталог суперпользователя (**root**);
- **environ** – переменные окружения, доступные для процесса;
- **fd** – содержит файловые дескрипторы, файлы и устройства, которые использует процесс;
- **maps**, **statm**, и **mem** – информация о памяти процесса;
- **stat**, **status** – состояние процесса.

Структура каталога /proc/sys

Каталог **/proc/sys** содержит файлы с параметрами ядра. Файлы доступны не только для чтения, но и для редактирования с целью передачи ядру ОС новых значений параметров.

Каталог содержит подкаталоги, разделённые по типам хранимых параметров. Далее будет рассмотрено назначение некоторых файлов:

- **debug** – содержит отладочную информацию, она будет полезна для разработчиков ядра;
- **dev** – содержит параметры различных устройств, подключенных к системе;
- **fs** – содержит всю информацию о файловой системе;
- **kernel** – позволяет напрямую настраивать ядро;
- **net** – позволяет настраивать различные параметры сети;
- **vm** – содержит ряд файлов и подкаталогов, соответствующих переменным ядра с подсистемой виртуальной памяти.

Более подробную информацию о каталоге **/proc** также можно просмотреть, выполнив команду:

```
man proc
```

Журналирование событий в РЕД ОС

Журнал пространства ядра
Журналы пользовательского пространства
Основные файлы журналов
Службы журналов

Журналы являются неотъемлемой частью любой ОС. В журналы записывается хронология событий, происходящих в используемой ОС, ее приложениях и службах.

Журналы являются полезным инструментом при возникновении различного рода неполадок системы и позволяют точно определять проблемы путем изучения предупреждений и сообщений об ошибках. Журналы событий используются для выявления инцидентов безопасности, диагностики проблем с производительностью, а также для обеспечения соответствия требованиям и аудита.

Журнал пространства ядра

Ядро ОС использует кольцевой буфер для хранения сообщений журнала, начиная с процесса загрузки системы. Этот буфер имеет фиксированный размер. После заполнения буфера новые сообщения будут перезаписывать старые. Все сообщения ядра записываются в кольцевой буфер с помощью функции `printk()`. Далее сообщения из кольцевого буфера ядра сохраняются в файлах журнала в постоянном хранилище системы – **/var/log/kern.log**. Параметр конфигурации ядра `CONFIG_PRINTK` позволяет вести журнал пространства ядра через `printk()`. Если он не установлен, системные вызовы ядра возвращают ошибку `ENOSYS`.

Сообщения ядра имеют собственные уровни (приоритеты), которые определяются ядром ОС для выявления серьезности конкретного сообщения.

Далее приведены доступные уровни (приоритеты) сообщений ядра:

- `KERN_EMERG` — экстренные сообщения (наивысший приоритет);
- `KERN_ALERT` — ошибка, требующая немедленного внимания;
- `KERN_CRIT` — критическая ошибка (аппаратная или программная);
- `KERN_ERR` — ошибка;
- `KERN_WARNING` — предупреждение;
- `KERN_NOTICE` — замечание;
- `KERN_INFO` — информационное сообщение;
- `KERN_DEBUG` — отладочные сообщения;
- `KERN_DEFAULT` — уровень ведения журнала ядра по умолчанию;
- `KERN_CONT` — продолжение ведения журнала (низший приоритет).

Все сообщения функции `printk()` записываются в кольцевой буфер ядра. Кольцевой буфер является файлом символьного устройства – **/dev/kmsg**. Устройство **/dev/kmsg** является абстракцией, предназначенной для чтения и записи в кольцевой буфер ядра.

Для управления кольцевым буфером ядра или его печати в стандартный вывод в консоли используется команда `dmesg`.

```
dmesg

[    3.330401] PM: Image not found (code -22)
[    5.508468] kauditd_printk_skb: 4 callbacks suppressed
[    5.508471] audit: type=1130 audit(1719211645.071:15): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=kernel
msg='unit=systemd-fsck-root comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
[    5.539630] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Quota mode: none.
[    5.592869] audit: type=1334 audit(1719211645.157:16): prog-id=8 op=UNLOAD
[    5.592980] audit: type=1334 audit(1719211645.157:17): prog-id=7 op=UNLOAD
```

Журналы пользовательского пространства

Журналирование может осуществляться как на локальной системе, так и в сети.

Ведение журналов пользовательского пространства основано на протоколе **rsyslog**. **Rsyslog** — это быстрый, расширяемый сервис для управления журналами с большим количеством возможностей. Среди его возможностей можно отметить поддержку фильтрации контента, а также передачу журналов по сети.

В конфигурационном файле **/etc/rsyslog.conf** возможна тонкая регулировка уровня журналирования. Журналирование

осуществляется при помощи службы **rsyslog.service**, которая обычно получает входную информацию при помощи сокета **/dev/log** (локально) или с **UDP**-порта **514** (с удаленных машин).

Сообщения журналов пространства пользователя имеют собственные уровни (приоритеты) событий. Приоритеты системного журнала указывают на серьезность зафиксированного сообщения. Значения приоритетов сообщений варьируются от **0** до **7**, где **0** является наиболее *критическим* уровнем.

Далее приведены приоритеты сообщений и их описание:

Приоритет	Ключевое слово	Серьезность инцидента	Описание
0	emerg	Экстренная ошибка	Система не может использоваться.
1	alert	Важное предупреждение	Необходимо немедленно принять меры.
2	crit	Критическая ошибка	Описание критической ошибки.
3	err	Ошибка	Описание ошибки.
4	warning	Предупреждение	Описание предупреждения.
5	notice	Уведомление	Важные сообщения.
6	info	Информация	Информационные сообщения.
7	debug	Отладка	Отладочные сообщения.

Важным значением в сообщениях журнала также является категория программы, которая сформировала данное сообщение. Значение категории программы варьируется от **0** до **23**.

Далее приведены категории программ:

Приоритет	Ключевое слово	Описание
0	kern	Сообщения ядра ОС.
1	user	Сообщения на уровне пользователя.
2	mail	Сообщения почтовых систем.
3	daemon	Сообщения от прочих системных служб.
4	auth	Сообщения безопасности или аутентификации, генерируемые системами авторизации или программами, которые запрашивают имена пользователей и пароли. Например, **su**, **login**, **ftpd**.
5	syslog	Внутренние сообщения **syslog**.
6	lpr	Сообщения, связанные с системой печати.
7	news	Сообщения подсистемы сетевых новостей (**nntp**).
8	uucp	Сообщения подсистемы **UUID**.
9	cron	Сообщения от подсистемы **cron**.
10	authpriv	Сообщения безопасности или аутентификации, аналогичен **auth**.
11	ftp	Сообщения службы **FTP**.
12	ntp	Сообщения подсистемы сетевого времени (**ntp**).
13	security	Журнал аудита.
14	console	Журнал оповещений.
15	solaris-cron	Сообщения службы планирования заданий.
16-23	local0-local7	Зарезервировано для локального использования.

Основные файлы журналов

По умолчанию события журналируются в каталог **/var/log/**. В нем хранится множество различных файлов с расширением ***.log**, содержащих события от различных источников в текстовом виде.

К основным файлам журналов относятся:

- **/var/log/rsyslog** или **/var/log/messages** — глобальный системный журнал, где хранятся события, произошедшие с момента запуска системы от различных компонентов ОС — ядра, служб, устройств и т. д.;
- **/var/log/kern.log** — содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок, произошедших при работе пользовательских модулей, встроенных в ядро;

- **/var/log/auth.log** или **/var/log/secure** — наиболее интересны для службы безопасности, так как содержат информацию об авторизации пользователей, т.е. попытки успешных/неуспешных входов в систему и методов аутентификации;
- **/var/log/dmesg** – в файле фиксируются ошибки работы драйверов и оборудования;
- **/var/log/anaconda.log** – в файле находятся события установки системы;
- **/var/log/boot.log** – в файле находятся логи загрузки системы;
- **/var/log/audit** — лог службы **auditd**;
- **/var/log/cron** — содержит результаты выполнения различных событий планировщика задач cron.

Также в зависимости от установленных приложений в **/var/log/** могут находиться журналы БД MySQL или веб-серверов Apache/Nginx.

Службы журналов

Служба **rsyslog** обеспечивает расширенную фильтрацию, различные параметры конфигурации, ретрансляцию сообщений с защитой от шифрования, модули ввода и вывода, а также поддержку транспортировки по протоколам **TCP** или **UDP**.

Помимо **rsyslog** файлами журналов также может управлять системная служба ведения журналов **journald** (компонент **systemd**). Служба **journald** собирает сообщения системного журнала, сообщения журнала ядра, сообщения о начальной загрузке с диска RAM и сообщения о ранней загрузке, а также сообщения, записанные в стандартный вывод и стандартный вывод ошибок всех служб, индексирует их и делает доступными для пользователя.

Основное различие между **rsyslog** и **journald** заключается в том, что файлы журналов, создаваемые **journald**, по умолчанию не являются постоянными. Файлы журналов хранятся только в памяти или небольшом кольцевом буфере в каталоге **/run/log/journal/**. **Rsyslog**, в свою очередь, хранит журналы в файлах журналов, доступных по адресу **/var/log/**.

Для просмотра содержимого журналов службы **journald** необходимо использовать команду:

```
journalctl
```

Для вывода справки по использованию утилиты выполните:

```
journalctl -h
```

Все настройки **journald** находятся в файле **/etc/systemd/journald.conf** и других конфигурационных файлах из директории **/etc/systemd/journald.conf.d**. По умолчанию все параметры в файле **/etc/systemd/journald.conf** закомментированы — они сообщают, какие значения используются по умолчанию. Значения параметров, установленных в файле **/etc/systemd/journald.conf** могут быть переопределены в одном из файлов в директории **/etc/systemd/journald.conf.d**.

Общая информация

РЕД ОС, как и любой UNIX – многопользовательская операционная система. Также имеются группы пользователей, основное предназначение которых - облегчить управление большим количеством пользователей, а также более точно распределить права доступа к различным объектам системы. Пользователи и группы внутри системы обозначаются цифровыми идентификаторами - UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод ее может быть примерно следующим:

```
id

uid=1000(test) gid=1000(test) группы=1000(test),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 1000) входит в группы *test* и *wheel*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Вы можете подробнее ознакомиться с информацией по управлению пользователями в системе, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

ВНИМАНИЕ!

В связи с тем, что в дистрибутивах РЕД ОС большинство привилегированных системных утилит имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

Роли пользователей

Роль sysadm - администратор системы
Роль — пользователь системы

В ОС пользователи по умолчанию сопоставляются SELinux-пользователю <**unconfined_u**>. SELinux-пользователь <**unconfined_u**>, в свою очередь, сопоставлен ролям <**unconfined_r**> и <**system_r**>.

Обе роли <**unconfined_r**> и <**system_r**> сопоставляются доменам безопасности SELinux. Домены безопасности SELinux - это определённые окружения безопасности для процессов.

Неограниченный домен безопасности <**unconfined_t**> - зарезервированное окружение для процессов, которые в значительной степени освобождены от ограничений SELinux. Роль <**system_r**> сопоставляется доменам безопасности для системных процессов.

SELinux-пользователь <**unconfined_u**> имеет доступ к роли <**system_r**>, чтобы иметь возможность запускать системные процессы в своих доменах безопасности. SELinux-пользователь <**unconfined_u**> работает в домене безопасности <**unconfined_t**> через роль <**unconfined_r**>, которой он сопоставлен.

Команда «semanage» позволяет добавлять, изменять и удалять сопоставления между ОС- и SELinux-пользователями, так же как и другие настройки, касающиеся управления SELinux.

Чтобы с помощью команды «semanage» посмотреть какому SELinux- пользователю по умолчанию сопоставлены пользователи ОС, наберите:

```
semanage login -l | grep default
```

В примере выше пользователи по умолчанию сопоставлены SELinux- пользователю <**unconfined_u**>.

Чтобы изменить это и сопоставить пользователей по умолчанию ограниченному SELinux-пользователю с именем <**user_u**>, просто наберите:

```
semanage login -m -s user_u "__default__"
```

В результате все новые пользователи будут по умолчанию сопоставляться ограниченному SELinux-пользователю <**user_u**>.

Вы можете переопределить данное сопоставление при добавлении пользователей командой «**useradd**» используя опцию «**-Z**». Эта опция определяет, какому SELinux-пользователю должен быть сопоставлен пользователь ОС.

Например, наберите:

```
useradd -Z guest_u joe
```

В результате будет создан новый пользователь с именем **joe**, который будет сопоставлен SELinux-пользователю <**guest_u**>, вместо определённого по умолчанию SELinux-пользователя.

Также для изменения сопоставления между пользователем и SELinux-пользователем может быть использована команда «**usermod**» с опцией «**-Z**».

Существует несколько предопределённых профилей SELinux-пользователей. Список данных профилей можно вывести командой «**semanage**», наберите:

```
semanage user -l
```

SELinux-пользователь <**unconfined_u**> - это среда, в которой по умолчанию работают все пользователи. Этот пользователь в значительной степени освобождён от ограничений, накладываемых SELinux. Если Вы хотите повысить безопасность вашей системы, тогда не следует сопоставлять реальных пользователей, не пользователя root, SELinux-пользователю <**unconfined_u**>.

Вход пользователя root должен быть запрещён. Root должен иметь возможность войти с терминала только в случае крайней необходимости. Чтобы повысить безопасность использования root, можно сопоставить пользователя root SELinux-пользователю <**sysadm_u**>.

Ролевой доступ SELinux используется для обеспечения возможности назначения нескольких ограниченных окружений SELinux одному SELinux-пользователю.

В SELinux роли пользователя (*User Roles*) - это домены пользователя или пользовательские домены (*User Domains*). Когда упоминаются роли, часто имеется в виду дополнительный (*secondary*) пользовательский домен пользователя SELinux. Часто роли, предназначенные для использования в качестве дополнительных доменов пользователя, отличаются от основных (*primary*) доменов. Это объясняется тем, что пользователи ОС фактически не используют для входа в систему роли, созданные как дополнительные домены пользователя. Вместо этого пользователи Linux, используя команду «**sudo**» или комбинацию команд «**su**» и «**newrole**», осуществляют переключение домена или доменный переход (*Domain Transition*) к их дополнительной роли.

Роль sysadm - администратор системы

Пример роли, предназначенной для использования в качестве основного домена пользователя. SELinux пользователь <**sysadm_u**> сопоставлен роли <**sysadm_r**>. Это сопоставление можно увидеть, выполнив команду:

```
semanage user -l | grep sysadm_u
```

По умолчанию пользователи ОС, сопоставленные пользователю SELinux <**sysadm_u**>, работают с ролью <**sysadm_r**>. В этом случае <**sysadm_r**> — это основной домен пользователя.

SELinux пользователь <**staff_u**> также сопоставлен роли <**sysadm_r**>. Основным пользовательским доменом пользователя SELinux <**staff_u**> является (роль) <**staff_r**>. Контексты по умолчанию, обозначенные в **/etc/selinux/targeted/contexts/users/staff_u**, определяют, с какими пользовательскими доменами пользователи будут подключаться по умолчанию и с какими пользовательскими доменами пользователи могут войти, указав домен пользователя при входе.

По умолчанию SELinux пользователь <**staff_u**> входит в систему в домен пользователя <**staff_t**>. Роль <**sysadm_r**>, предназначенная для использования в качестве основного домена пользователя, может быть использована при входе, например, следующим образом:

```
ssh joe/sysadm_r@localhost.localdomain.tld
```

Также роль <**sysadm_r**> может быть использована при переходе домена выполнением команд «**sudo**» и «**su**» вместе с «**newrole**», как это предусмотрено для дополнительных доменов пользователей.

Пользовательский домен <**sysadm_t**> является окружением по умолчанию для SELinux-пользователя <**sysadm_u**> и предназначен для использования в качестве дополнительного окружения для SELinux-пользователя <**staff_u**>, хотя даже SElinux-пользователь <**staff_u**> может настроить подключаемый модуль аутентификации (*Pluggable Authentication Module*) <**pam_selinux**> для использования <**sysadm_t**> в качестве его основного домена пользователя.

Роль <user_r> — пользователь системы

Пользовательский домен, используемый только в качестве основного. Описание пользователя SELinux <**user_u**> приведено ранее.

Какие-то домены пользователей могут использоваться пользователями для входа в систему, потому что эти домены, например, имеют полномочия по доступу к домашней директории пользователя. Такие домены в предыдущей части назывались основными (*primary*) пользовательскими доменами. Другие домены созданы в качестве дополнительных. Пользователи, используя команды «**sudo**» или «**su**» вместе с «**newrole**», могут осуществить доменный переход (*Domain Transition*) к этим дополнительным доменам.

Дополнительные домены не могут использоваться для входа в систему. Далее будет продемонстрировано как создаётся такой дополнительный пользовательский домен. Целью является реализовать привилегированную роль SELinux, которой предоставлены полномочия по управлению DNS службой Bind.

Начнём с создания нового дополнительного домена пользователя с названием «**bindadm**», основанного на предустановленном домене SELinux <**webadm_t**>. Новый домен пользователя основан на двух файлах с исходным текстом политики SELinux (SELinux Source Policy):

- webadm.te;
- webadm.if.

Файлы исходных текстов политики SELinux с расширением "**.te**" называются Type Enforcement файлы. Файлы с расширением "**.if**" называются интерфейсными (Interface files). Файлы *Type Enforcement* содержат описания (*Declarations*) и политику (*Policy*), персональные или локальные для данного домена (*Domain*). Интерфейсные файлы содержат описания и политики, общие для этого домена и других доменов, желающими взаимодействовать с данным доменом.

```
mkdir ~/bindadm; cd ~/bindadm
echo "policy_module(bindadm, 0.0.1)" >> bindadm.te
echo "role bindadm_r" >> bindadm.te
echo "userdom_base_user_template(bindadm)" >> bindadm.te
echo "allow bindadm_t self:capability { dac_override dac_read_search kill sys_ptrace sys_nice" >> bindadm.te
echo "files_dontaudit_search_all_dirs(bindadm_t)" >> bindadm.te
echo "files_manage_generic_locks(bindadm_t)" >> bindadm.te
echo "files_list_var(bindadm_t)" >> bindadm.te
echo "selinux_get_enforce_mode(bindadm_t)" >> bindadm.te
echo "seutil_domtrans_setfiles(bindadm_t)" >> bindadm.te
echo "logging_send_syslog_msg(bindadm_t)" >> bindadm.te
echo "userdom_dontaudit_search_user_home_dirs(bindadm_t)" >> bindadm.te
```

Это основное содержимое для привилегированного дополнительного домена пользователя. Исключена политика, специфичная для управления службой Apache.

Теперь добавим политику, специфичную для управления службой Bind. Можно позаимствовать эту политику из исходных текстов политики для Bind. Как уже отмечалось, общая политика располагается в интерфейсных файлах. Это значит, что если мы хотим включить общую политику, относящуюся к Bind, можно посмотреть в соответствующем файле политики **bind.if**. Для включения этой политики в наш Type Enforcement файл требуется всего лишь добавить вызов этого интерфейса:

```
echo "bind_admin(bindadm_t, bindadm_r)" >> bindadm.te
```

На этом Type Enforcement файл bindadm заканчивается. Далее необходимо обеспечить другим доменам возможность взаимодействия с нашим доменом <**bindadm_t**>. Реализуем эту часть политики, взяв за основу файл **webadm.if**.

```
echo "## Bind administrator role" > bindadm.if
echo "########################################" >> bindadm.if
echo "##" >> bindadm.if
echo "## Change to the bind administrator role." >> bindadm.if
echo "##" >> bindadm.if
echo '##' >> bindadm.if
echo "##" >> bindadm.if
echo "## Role allowed access." >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "#" >> bindadm.if
echo "interface(\`bindadm_role_change',\`" >> bindadm.if
echo " gen_require(\`" >> bindadm.if
echo " role bindadm_r;" >> bindadm.if
echo " ')" >> bindadm.if
echo " allow  $1 bindadm_r;" >> bindadm.if
echo "')" >> bindadm.if
```

Позже общая политика администратора **Bind** (Bind Administrator Shared policy) будет использоваться в нашем основном специально созданном пользовательском домене SELinux.

Следующим шагом будет создание специализированного пользовательского домена SELinux для обслуживания Bind, разрешающего данному домену осуществлять переход к роли <**bindadm_r**> вызовом интерфейса <**bindadm_role_change**>. Создаваемый домен SELinux будет основан на пользовательском домене <**staff_t**>, описание политики смотрим в файле **staff.te**.

```
echo "policy_module(bindguy, 0.0.1)" > bindguy.te
echo "role bindguy_r;" >> bindguy.te
echo "userdom_unpriv_user_template(bindguy)" >> bindguy.te
echo "sudo_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "ssh_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "kernel_read_ring_buffer(bindguy_t)" >> bindguy.te
echo "kernel_getattr_core_if(bindguy_t)" >> bindguy.te
echo "kernel_getattr_message_if(bindguy_t)" >> bindguy.te
echo "kernel_read_software_raid_state(bindguy_t)" >> bindguy.te
echo "auth_domtrans_pam_console(bindguy_t)" >> bindguy.te
echo "libs_manage_shared_libs(bindguy_t)" >> bindguy.te
echo "seutil_run_newrole(bindguy_t, bindguy_r)" >> bindguy.te
echo "netutils_run_ping(bindguy_t, bindguy_r)" >> bindguy.te
echo "domain_read_all_domains_state(bindguy_t)" >> bindguy.te
echo "domain_getattr_all_domains(bindguy_t)" >> bindguy.te
echo "domain_obj_id_change_exemption(bindguy_t)" >> bindguy.te
echo "files_read_kernel_modules(bindguy_t)" >> bindguy.te
echo "kernel_read_fs_sysctls(bindguy_t)" >> bindguy.te
echo "modutils_read_module_config(bindguy_t)" >> bindguy.te
echo "modutils_read_module_deps(bindguy_t)" >> bindguy.te
echo "miscfiles_read_hwdata(bindguy_t)" >> bindguy.te
echo "term_use_unallocated_ttys(bindguy_t)" >> bindguy.te
```

Чтобы разрешить домену <**bindguy_t**> осуществлять переход в ограниченное окружение SELinux <**bindadm_t**>, добавим вызов интерфейса <**bindadm_role_change**>, определённого в нашем интерфейсном файле **bindadm.if**:

```
echo "bindadm_role_change(bindguy_r)" >> bindguy.te
```

Можно также автоматически создать сопоставление пользователя SELinux с именем <**bindguy_u**> ролям <**bindguy_r**>, <**bindadm_r**> и <**system_r**>. Роль <**system_r**> включается, чтобы <**bindadm_t**> мог остановить, запустить и перезапустить системную службу **bind**.

```
echo "gen_user(bindguy_u, user, bindguy_r system_r bindadm_r, s0,  s0 - mls_systemhigh,
mcs_allcats)" >> bindguy.te
```

Чтобы программы входа знали, что bindguy допустимый пользователь, добавим контексты по умолчанию для этого пользователя, взяв за основу контексты по умолчанию пользователя <**staff_u**>:

```
cp /etc/selinux/targeted/contexts/users/staff_u
/etc/selinux/targeted/contexts/users/bindguy_u
sed -i 's/staff/bindguy/g'
/etc/selinux/targeted/contexts/users/bindguy_u
```

Теперь можно собрать и установить обе политики bindguy и bindadm:

```
make -f /usr/share/selinux/devel/Makefile
semodule -i bindguy.pp bindadm.pp
```

Далее командой «**useradd**», опцией «**-Z**» и параметром <**bindguy_u**> можно создать нового пользователя Linux:

```
useradd -Z bindguy_u bindguy
```

Для того чтобы разрешить пользователю *bindguy* использовать команду «**sudo**» для автоматического перехода к пользователю root и SELinux-домену <**bindadm_t**>, добавим в **/etc/sudoers**:

```
echo "bindguy ALL=(ALL) ROLE=bindadm_r TYPE=bindadm_t ALL" » /etc/sudoers
```

При входе пользователя bindguy в систему он оказывается в пользовательском домене <**bindguy_t**>, основанном на домене <**staff_t**>. Домен <**bindguy_t**> может осуществлять переход в домен <**bindadm_t**>, используемый с правами root и позволяющий управлять службой Bind.

Например, выполнив следующую команду, пользователь bindguy сможет перезапустить службу bind:

```
service named restart
```

Также пользователю *bindguy* разрешается редактировать различные конфигурационные файлы и файлы информационного наполнения Bind. При этом, например, пользователь *bindguy* не имеет прав изменить пароль пользователя root.

Подведём итог. Процессы и файлы маркируются метками - контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально). Когда SELinux включён, вся эта информация используется для принятия решения о предоставлении доступа.

В контексте SELinux используется следующий синтаксис SELinux:

```
<user>:<role>:<type>:<level>:<пользователь_SELinux>
```

<**Пользователь_SELinux**> - это сущность, определённая в политике, которая отвечает за определённый набор ролей и за определённый набор MLS-уровней. Каждый пользователь ОС сопоставлен пользователю SELinux посредством политики SELinux. Это позволяет пользователям наследовать ограничения, установленные на пользователей SELinux. Сопоставленные сущности пользователей SELinux используются в контексте SELinux для процессов в сессии, в порядке определения, для каких ролей и уровней они применимы.

Роль - это часть модели безопасности Ролевого управления доступом **Role-Based Access Control** (RBAC). Роль - это атрибут RBAC. Пользователи SELinux авторитетны для ролей, а роль авторитетна для доменов. Каждая конкретная роль определяет, какие домены могут быть доступны для пользователей с этой ролью. Роль служит промежуточным звеном между доменами и пользователями SELinux. Роль, которой обладает пользователь, определяет, в какие домены может попасть пользователь - фактически, этот механизм управляет доступностью объектов. Таким образом, уменьшается риск, связанный с уязвимостью повышения привилегий в системе. По умолчанию пользователям назначена неопределённая роль, не накладывающая ограничений на пользователя. Но есть и предопределённые роли пользователя и администратора системы, которые могут быть назначены администратором для повышения безопасности системы.

Тип - это атрибут *Type Enforcement*. Тип определяет домен для процессов и тип для файлов. Правила политики SELinux определяют, как типы взаимодействуют друг с другом, является ли тип доменом, получающим доступ к типу, или доменом, получающим доступ к другому домену. Доступ разрешается, только если существует определённое правило политики SELinux, позволяющее данное действие.

Контекст безопасности записывается в атрибуты файла (в файловой системе) и создаётся при установке SELinux (операция **labeling**). Уже присвоенный контекст безопасности может быть впоследствии изменён - операцией «**transition**».

Командные оболочки (интерпретаторы)

Для управления ОС используется командные интерпретаторы (shell). Зайдя в систему, пользователь увидит приглашение - строку, содержащую символ «$» (далее этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора - передавать команды пользователя операционной системе. При помощи командных интерпретаторов можно писать небольшие программы - сценарии (скрипты). Оболочкой по умолчанию в РЕД ОС является «**Bash**» (Bourne Again Shell) Чтобы проверить, какая оболочка используется, необходимо выполнить команду:

```
echo $SHELL
```

Вы можете подробнее ознакомиться с возможностями работы **bash**, просмотрев наши обучающие видео:

- на **RuTube**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **Яндекс.Дзен**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **VK Видео**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.

На наших каналах вы также сможете найти много другой полезной информации.

Командная оболочка Bash

В bash имеется несколько приемов для работы со строкой команд. Например, используя клавиатуру, можно:

- **Ctrl + A** - перейти на начало строки.
- **Ctrl + U** - удалить текущую строку.
- **Ctrl + C** - остановить текущую задачу.

Можно использовать «;» для того, чтобы ввести несколько команд одной строкой. Клавиши «вверх» и «вниз», позволяют вам перемещаться по истории команд.

Для того чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, необходимо набрать:

Ctrl + R

Команды, присутствующие в истории, отображаются в списке пронумерованными. Для того, чтобы запустить конкретную команду, наберите:

```
! <номер_команды>
```

если ввести:

```
!!
```

запустится последняя из набранных команд. Иногда имена программ и команд слишком длинны. Bash сам может завершать имена. Нажав клавишу [TAB], можно завершить имя команды, программы или каталога. Например, предположим, что необходимо использовать программу декомпрессии bunzip2. Для этого нужно набрать:

```
bu
```

затем нажать [TAB]. Если ничего не происходит, то, вероятно, существует несколько возможных вариантов завершения команды.

Нажав клавишу [TAB] еще раз, пользователь получит список имен, начинающихся с «bu». Например, может быть:

```
bu buildhash builtin bunzip2
```

Если далее добавить:

n

(bunzip - это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу [TAB], оболочка дополнит имя и остается лишь нажать «Enter», чтобы запустить команду. Программу, вызываемую из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH.

По умолчанию, в этот перечень каталогов не входит текущий каталог, обозначаемый «./» (точка слэш), поэтому для запуска программы **prog** из текущего каталога, надо дать команду:

```
./prog
```

Базовые команды оболочки Bash

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации используйте команду **man.**Пример:

```
man ls
```

Команда su

Позволяет получить права администратора. Когда пользователь набирает su, оболочка запрашивает пароль суперпользователя (root). Необходимо ввести пароль и нажать **Enter**. Чтобы вернуться к правам основного пользователя, необходимо набрать **exit**.

Команда cd

Позволяет сменить каталог. Она работает как с абсолютными, так и с относительными путями. Предположим, что находясь в своем домашнем каталоге и пользователь хочет перейти в его подкаталог **docs/**. Для этого нужно ввести относительный путь:

```
cd docs/
```

Чтобы перейти в каталог **/usr/bin** , нужно набрать (абсолютный путь):

```
cd /usr/bin/
```

Некоторые варианты команды:

```
cd ..
```

позволяет сделать текущим родительский каталог,

```
cd -
```

позволяет вернуться в предыдущий каталог. Команда cd без параметров переводит в домашний каталог.

Команда ls

ls (list) выдает список файлов в текущем каталоге. Синтаксис:

```
ls
```

Две основные опции:

- -a - просмотр всех файлов, включая скрытые,
- -l - отображение более подробной информации.

Команда rm

Эта команда используется для удаления файлов. Синтаксис:

```
rm <имя_файла>
```

У данной программы существует ряд параметров. Самые часто используемые:

- -i - запрос на удаление файла,
- -r - рекурсивное удаление (т.е. удаление, включая подкаталоги и скрытые файлы).

Команды mkdir и rmdir

Команда **mkdir** позволяет создать каталог, тогда как **rmdir** удаляет каталог, при условии, что он пуст. Синтаксис:

```
mkdir <имя_каталога>
```

```
rmdir <имя_каталога>
```

Команда **rmdir** часто заменяется командой **rm-rf** , которая позволяет удалять каталоги, даже если они не пусты.

Команда less

less позволяет постранично просматривать текст.

Синтаксис:

```
less <имя_файла>
```

Для выхода нужно нажать q.

Команда grep

Данная команда имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep <шаблон_поиска> <файл>
```

Команда ps

Отображает список текущих процессов. Колонка команд указывает имя процесса, колонка PID (идентификатор процесса) - номер процесса (этот номер используется, для операций с процессом, например чтобы «убить» его командой **kill**).

Синтаксис:

```
ps <аргументы>
```

Аргумент -u предоставляет больше информации, а -x позволяет просмотреть те процессы, которые не принадлежат пользователю (такие как те, что были запущены во время процесса загрузки).

Команда kill

Если программа перестала отвечать или зависла, необходимо использовать данную команду, чтобы её завершить.

Синтаксис:

```
kill <PID_номер>
```

Иногда необходимо будет использовать **kill -9** (когда обычная команда **kill** не дает желательного эффекта). Номер PID выясняется при помощи команды **ps**.

Горячие комбинации клавиш в Bash

Для удобства запоминания сочетания клавиш сгруппированы по действию. Обратите внимание, что **в комбинациях следует использовать левую клавишу Alt**, т.к. правая Alt Gr используется как клавиша Compose (специальная клавиша, позволяющая вводить символы с помощью определённых комбинаций клавиш).

Перемещение по тексту

Сочетание	Действие
Ctrl+a, Home	Переместить курсор в начало командной строки
Ctrl+e, End	Переместить курсор в конец командной строки
Ctrl+b, ←	Переход на один символ назад от курсора
Ctrl+f, →	Переход на один символ вперёд от курсора
Alt+b, Esc+b	Переместить курсор назад на одно слово
Alt+f, Esc+f	Переместить курсор вперёд на одно слово
Ctrl+xx	Переход от курсора в начало строки и обратно

Редактирование строки

Сочетание	Действие
Alt+?, Tab+Tab	Автодополнение команды или имени файла
Ctrl+u	Удалить все символы от курсора до начала командной строки
Ctrl+k	Удалить все символы от курсора до конца командной строки
Ctrl+w	Удалить символы от курсора до пробела слева
Alt+Backspace	Удалить символы от курсора до начала слова
Alt+d, Esc+d	Удалить символы от курсора до конца слова
Ctrl+y	Вставить символ, слово или текст, которые были удалены при помощи сочетаний клавиш, приведенных выше
Alt+y	Просмотреть буфер удалённых слов и вставить интересующее. Работает после нажатия Ctrl+y
Ctrl+h	Удалить перед курсором один символ
Ctrl+d	Удалить под курсором один символ
Alt+	Удалить любое количество пробелов вокруг курсора
Ctrl+_	Откатить редактирование
Alt+r, Esc+r	Отменить все изменения содержимого строки
Alt+c	Заменяет под курсором букву на заглавную и переводит курсор в конец слова
Alt+u	Переводит все буквы от курсора и до конца слова в заглавные
Alt+l	Переводит все буквы от курсора и до конца слова в нижний регистр
Alt+t	Замена текущего слова под курсором на предыдущее слово
Ctrl+t	Замена символа перед курсором на предыдущий символ

История команд

Сочетание	Действие
Ctrl+r	Искать команду по истории

Ctrl+g	Выйти из режима поиска в истории
Ctrl+p, ↑	Предыдущая команда в истории
Ctrl+n, ↓	Следующая команда в истории
Alt+<	Переход к первой команде в буфере истории
Alt+., Esc+.	Вставить последний аргумент предыдущей команды
Ctrl+o	Выполняет введённую команду и оставляет её же в командной строке

Выполнение и вывод на экран

Сочетание	Действие
Ctrl+l	Очистка экрана
Ctrl+s	Остановить вывод на экран
Ctrl+q	Возобновить вывод на экран, если он был приостановлен указанной выше командой
Ctrl+c	Прервать выполнение текущей команды
Ctrl+z	Приостановить выполнение текущей команды (для возобновления выполните fg)
Ctrl+d	Выйти из командной оболочки Bash

Информационный вывод

Сочетание	Действие
***+Alt+?, *+Tab+Tab**	Показать каталоги, кроме скрытых
$+Alt+?, $+Tab+Tab	Показать все системные переменные

Специальные клавиши

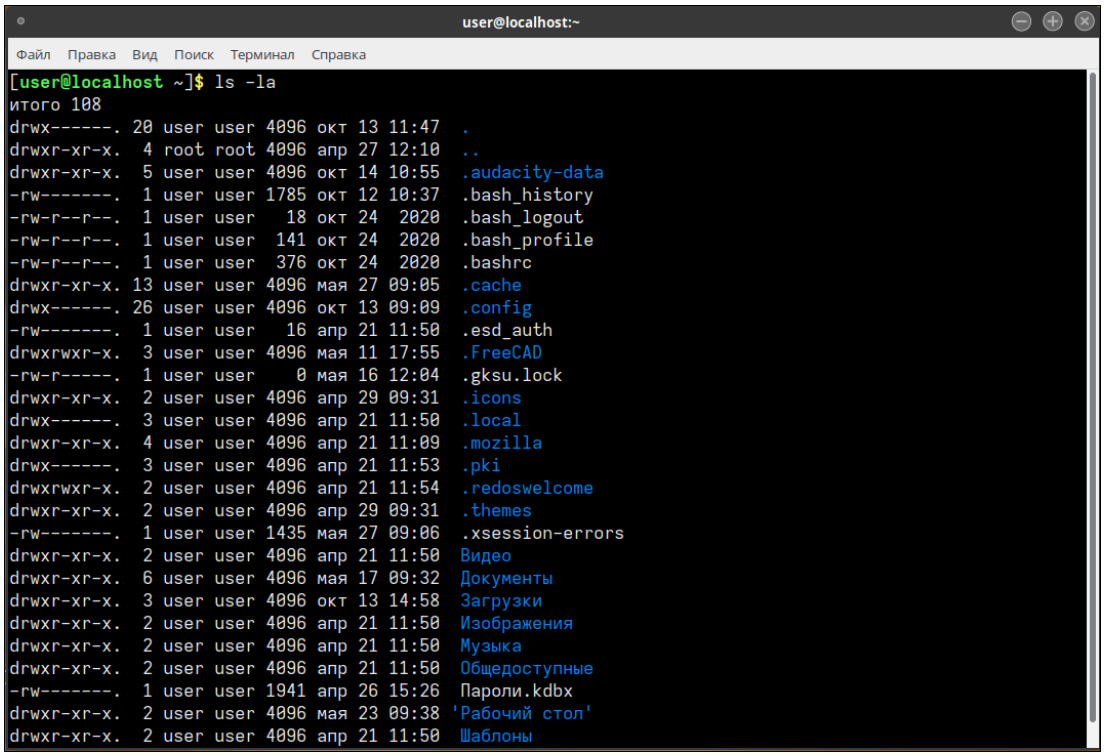
Сочетание	Действие
Ctrl+i	Tab
Ctrl+m	Enter
Ctrl+[	Esc

Основные утилиты в консоли РЕД ОС

ls

Утилита для просмотра содержимого каталогов. По умолчанию показывает содержимое текущего каталога. Если в параметрах указан путь к каталогу, она перечислит содержимое конечного каталога. Полезные опции:

- **-l** (list) - форматирует вывод в виде списка с более подробной информацией;
- **-a** (--all) - включает показ скрытых файлов;
- **--h** (help) - вывести справку по использованию утилиты.

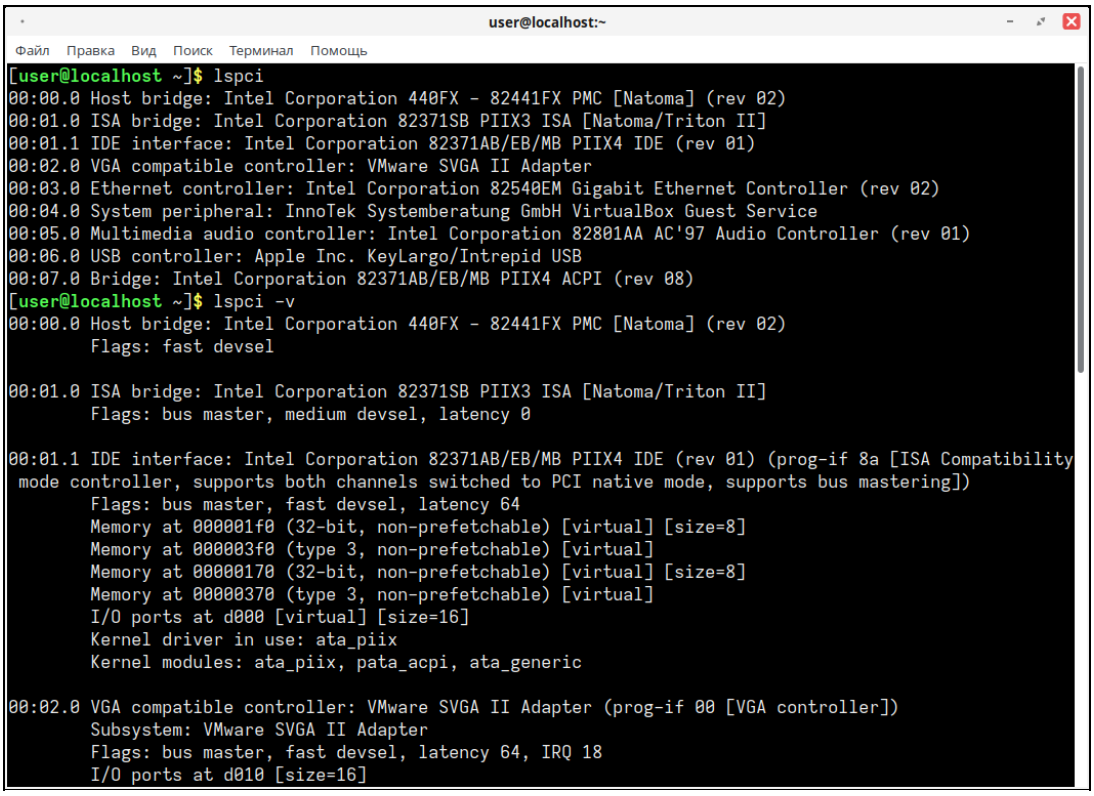


lspci

Команда **lspci** позволяет задействовать одноименную утилиту, предназначенную для вывода информации о PCI-шинах и подключенных к ним устройствах. Она поддерживает все разновидности PCI-шин: классическую шину **PCI** (Peripheral Component Interconnect), ее серверный вариант **PCI-X** и ее современный вариант **PCIe** (PCI-Express). Обычно к данной шине подключаются такие устройства, как графические, звуковые и сетевые карты, Wi-Fi и Bluetooth-адаптеры, SSD-накопители, а также множество других устройств.

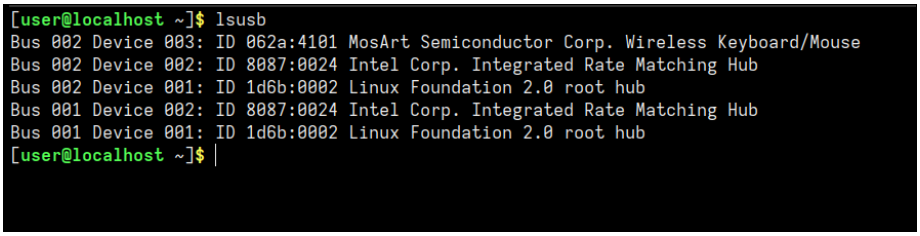
Наиболее полезные опции:

- **-m** и **-mm** — для вывода установленных производителем идентификаторов устройств;
- **-t** — для вывода информации в древовидном формате;
- **-v** — для вывода подробной информации об устройствах;
- **-n** — для вывода идентификаторов устройств;
- **-s** и **-d** — для вывода информации об устройствах в заданных слотах и с заданными идентификаторами соответственно.



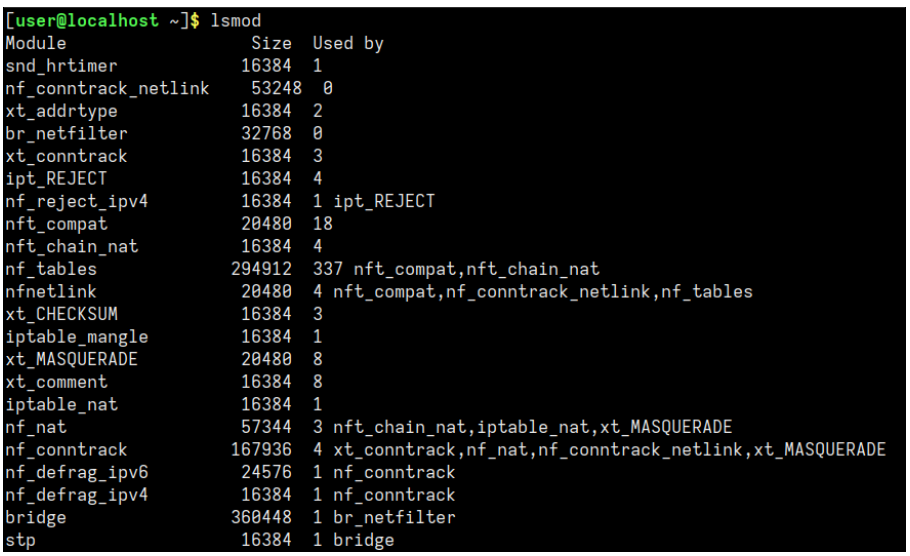
lsusb

Команда lsusb позволяет задействовать одноименную утилиту, предназначенную для вывода информации о USB-шинах и подключенных к ним устройствах. Каждое из устройств имеет пару 16-битных идентификаторов: идентификатор производителя (**Vendor ID**) и идентификатор устройства (**Device ID**), которые следует использовать для идентификации устройств и поиска драйверов в случае их отсутствия в ядре ОС, а также несколько дополнительных идентификаторов, устанавливаемых производителем.



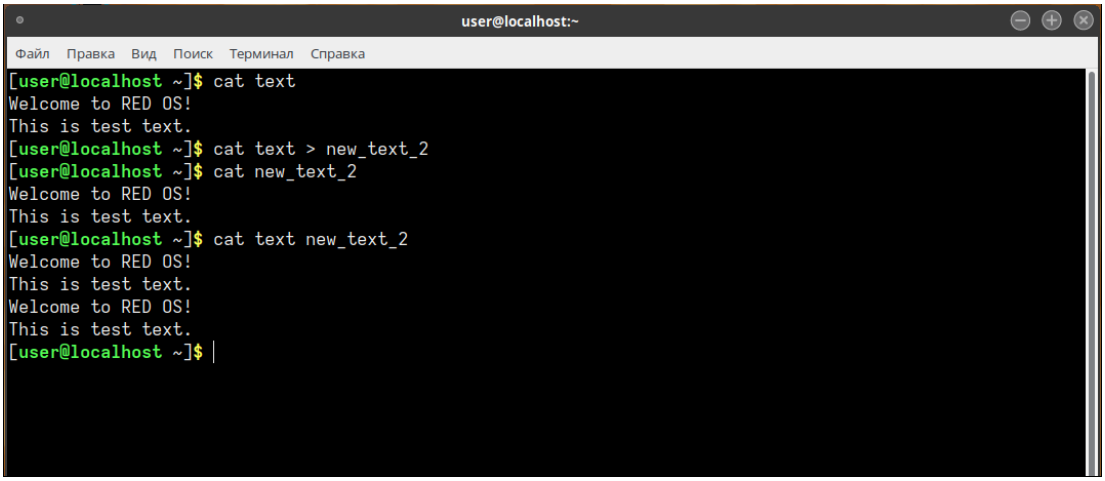
lsmod

Команда **lsmod** показывает, какие модули ядра загружены в системе в данный момент.



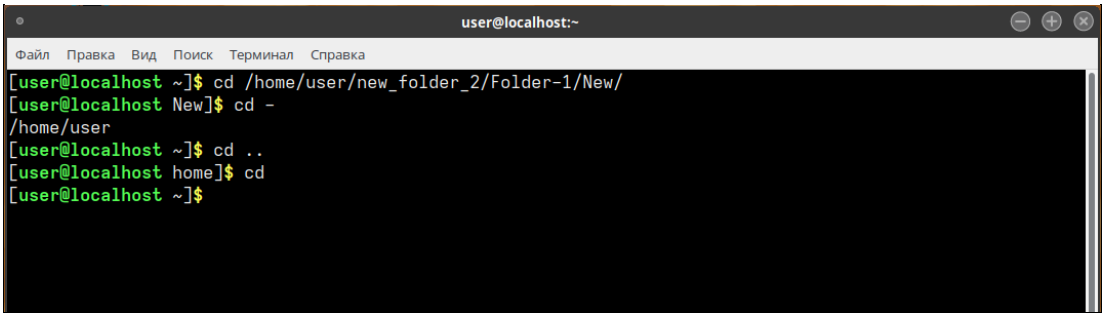
cat

Печатает содержимое файла, переданного в параметре, в стандартный вывод. Если передать несколько файлов, команда объединит их. Также можно перенаправить вывод в ещё один файл с помощью символа « **>** ».



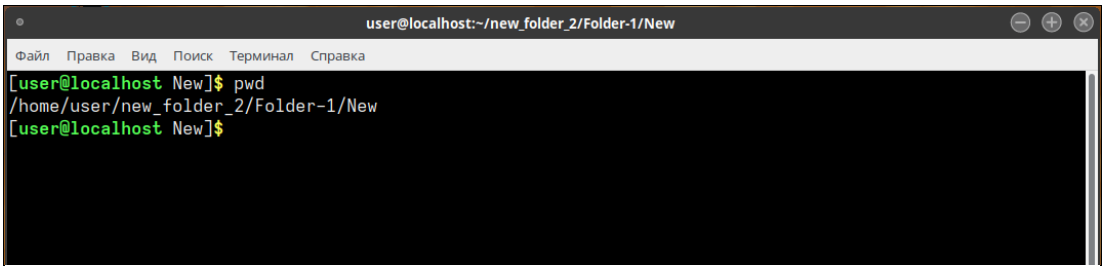
cd

Позволяет перейти из текущего каталога в указанный. Если запустить без параметров - возвращает в домашний каталог. Вызов с двумя точками (**cd ..**) - возвращает на уровень выше относительно текущего каталога. Вызов с тире (**cd -**) возвращает к предыдущему каталогу.



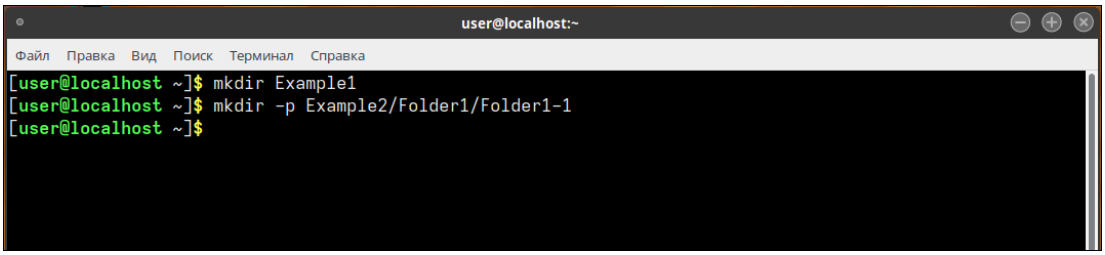
pwd

Выводит полный путь к текущему/рабочему каталогу.



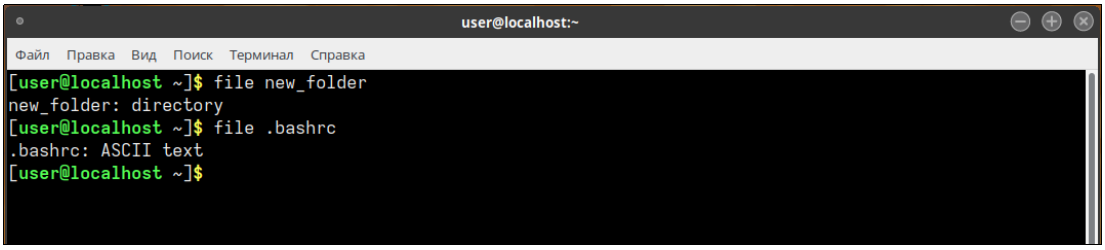
mkdir

Создание новых каталогов. Наиболее удобная опция **-p** (parents), позволяет создать всю структуру подкаталогов одной командой, даже если они ещё не существуют.



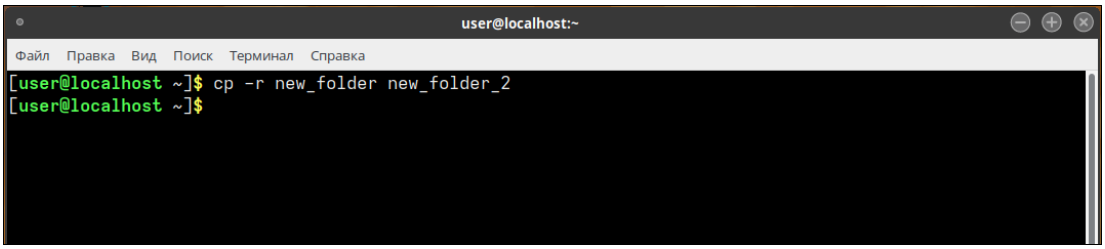
file

Показывает тип файла. В Linux файлы не обязаны всегда иметь расширения для того, чтобы с ними работать. Поэтому пользователю иногда трудно определить, какой именно перед ним файл. Данная утилита решает такую проблему.



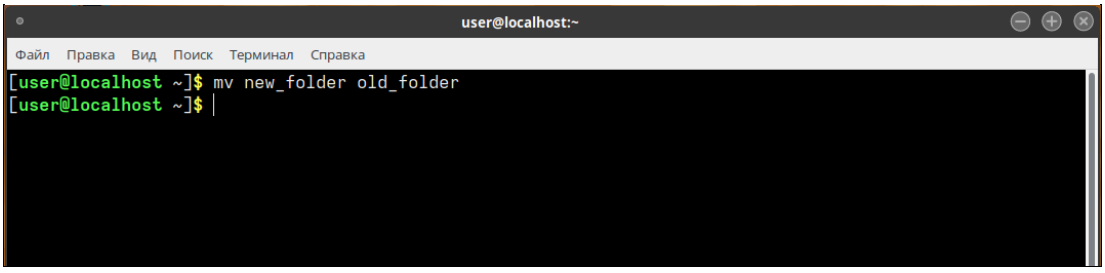
cp

Копирование файлов и каталогов. Утилита по умолчанию не копирует каталоги рекурсивно, поэтому необходимо добавить опцию **-r** (recursive) или **-a** (archive). Последняя включает режим сохранения атрибутов, владельца и временного штампа в дополнение к рекурсивному копированию.



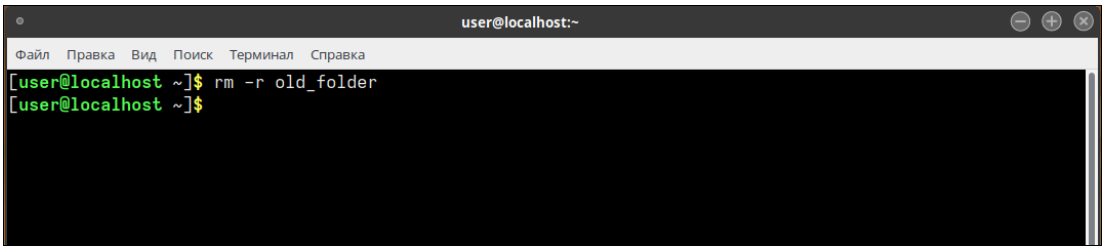
mv

Перемещение или переименование файлов и каталогов. В Linux это одна и та же операция. Переименование - это перемещение файла в ту же папку с другим именем.



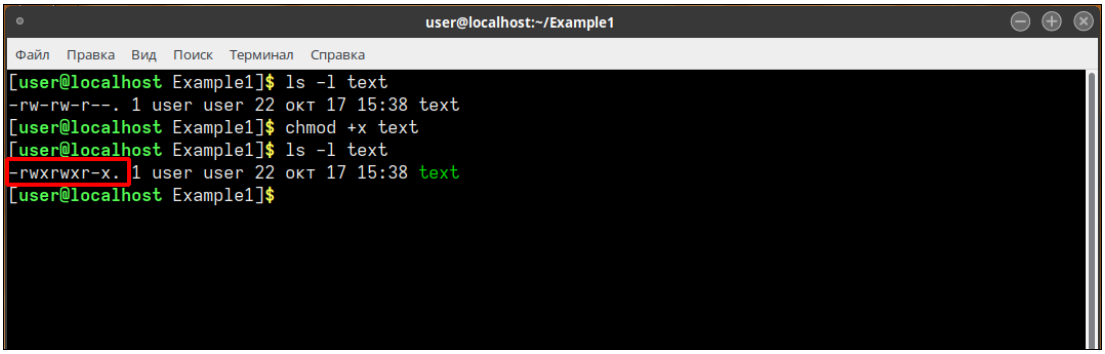
rm

Удаляет файлы и папки. Если нужно рекурсивное удаление, используйте опцию **-r**. **Rm** удаляет файлы не в корзину, из которой потом данные можно будет восстановить, а полностью их стирает. Действия оператора **rm** необратимы.



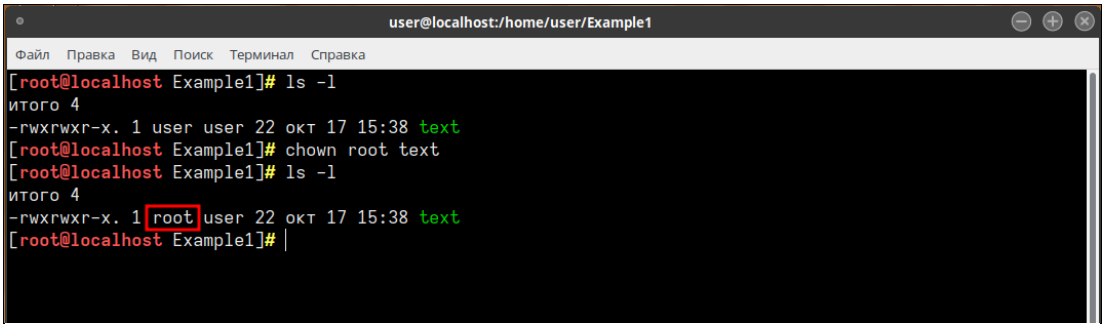
chmod

Изменяет права доступа к файлу - чтение, запись и выполнение. Каждый пользователь может изменять права для своих файлов.



chown

Изменяет владельца файла. Только суперпользователь может изменять владельцев. Для рекурсивного изменения используйте опцию **-R**.

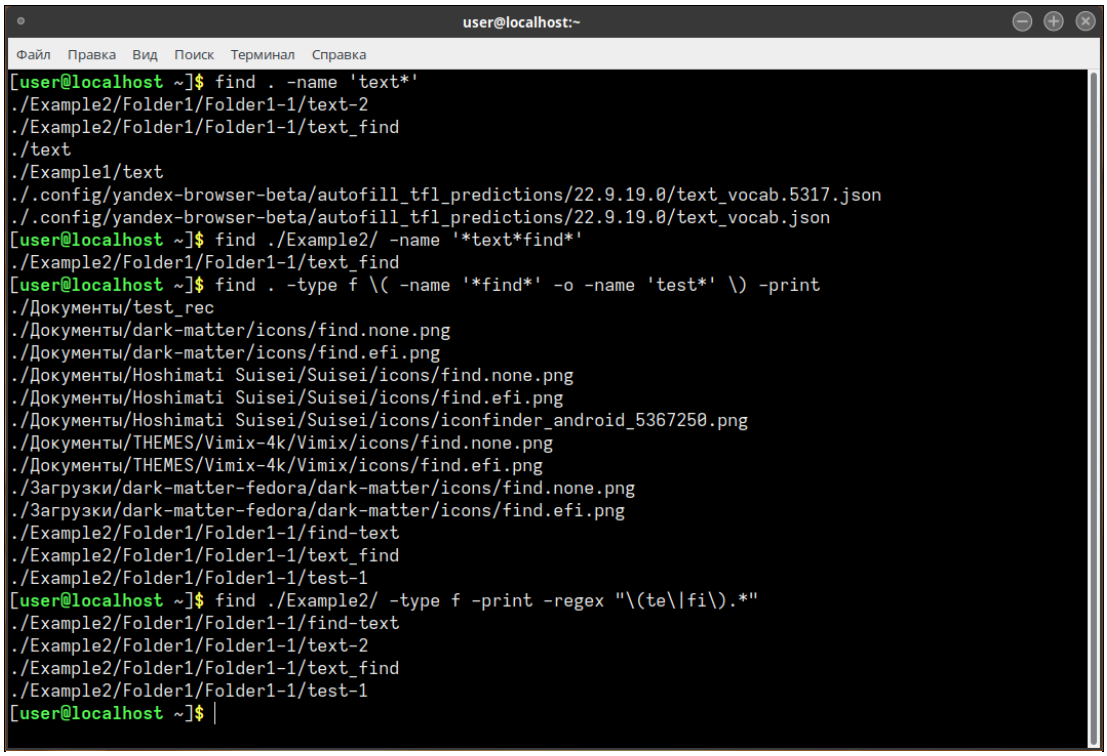


find

Очень гибкая и мощная команда Linux не только из-за своих способностей удобного поиска, но и благодаря возможности выполнять произвольные команды для найденных файлов. Поиск может осуществляться как в одном, так и в нескольких каталогах, имеется поддержка регулярных выражений для более точного поиска.

Основные опции:

- **-type** [f=файл, d=каталог (directory), l=ссылка (link), p=канал (pipe), s=сокет] - поиск по типу файла;
- **-name** '<имя_файла>' - поиск по имени файла, можно использовать как полное имя, так и его часть ('text' или 'te*');
- **-regex** "<регулярное_выражение>" - поиск файлов по регулярному выражению;
- **-print** - показать на экране найденные файлы.

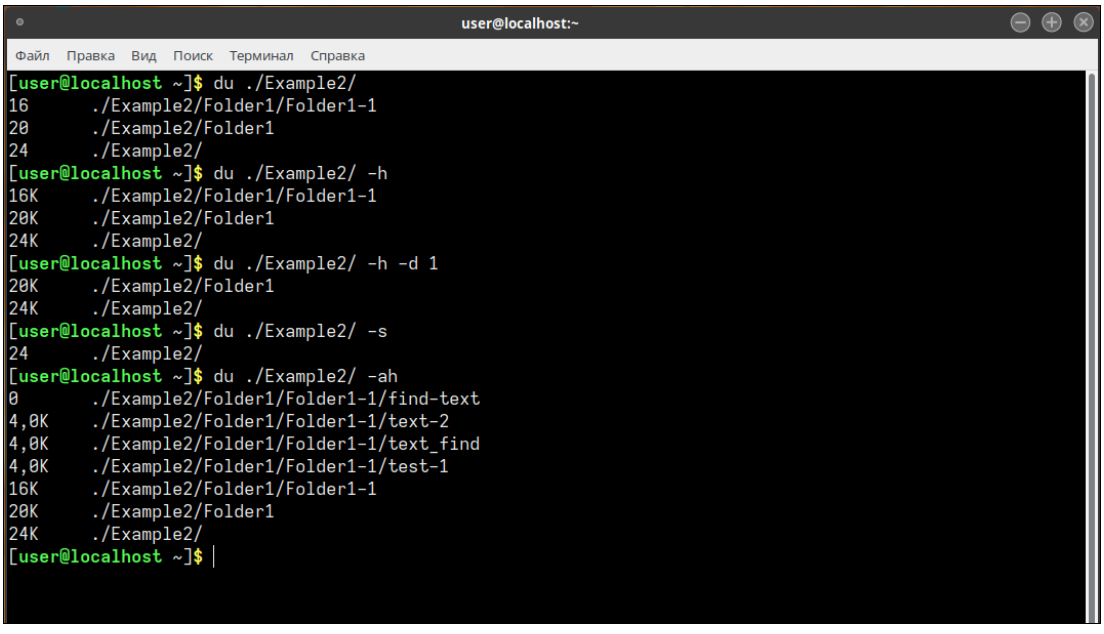


du

Показывает размер файла или каталога для оценки занимаемого файлового пространства.

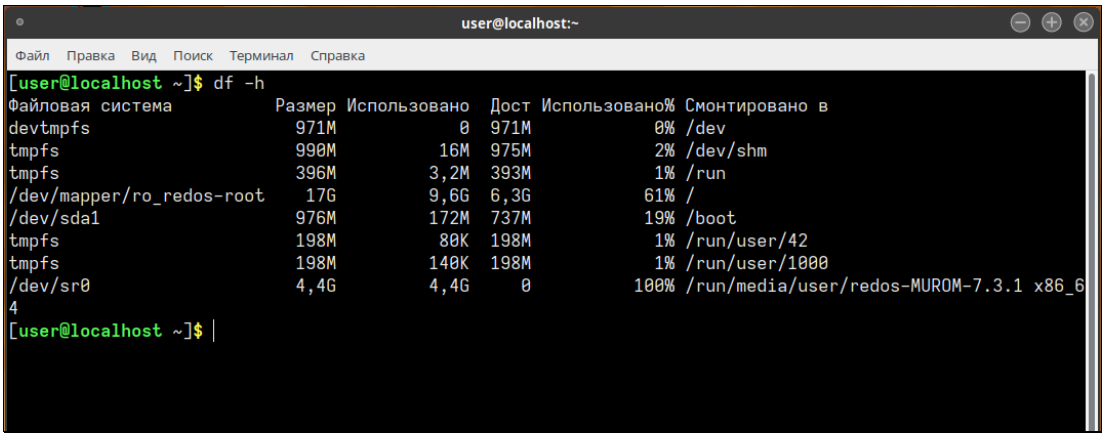
Полезные опции:

- **-a** (--all) - выводить размер для всех файлов, а не только для директорий, по умолчанию размер выводится только для папок;
- **-d** (--max-depth) - максимальная глубина вложенности директорий;
- **-h** (--human-readable) - преобразует размеры файлов в удобный формат;
- **-s** (--summarize) - выводит минимум данных.



df

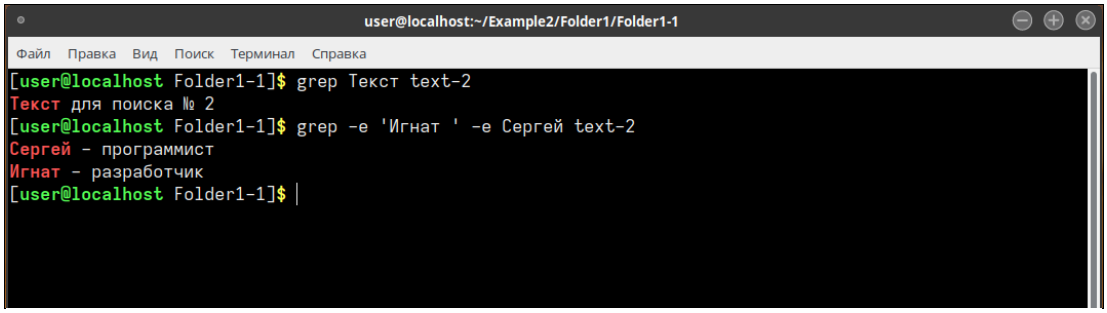
Используется для получения полной сводной информации о доступном и используемом дисковом пространстве файловой системы. По умолчанию вывод достаточно подробный: перечислены все файловые системы, их размер, количество использованного и свободного пространства. Для удобства можно использовать опцию **-h**, которая отобразит размеры удобными для чтения.



grep

Утилита **grep** ищет заданный шаблон или регулярное выражение из стандартного ввода или файла и печатает соответствующие заданным критериям строки. Утилита может вывести как полностью совпадающие, так и частично совпадающие строки и их контекст.

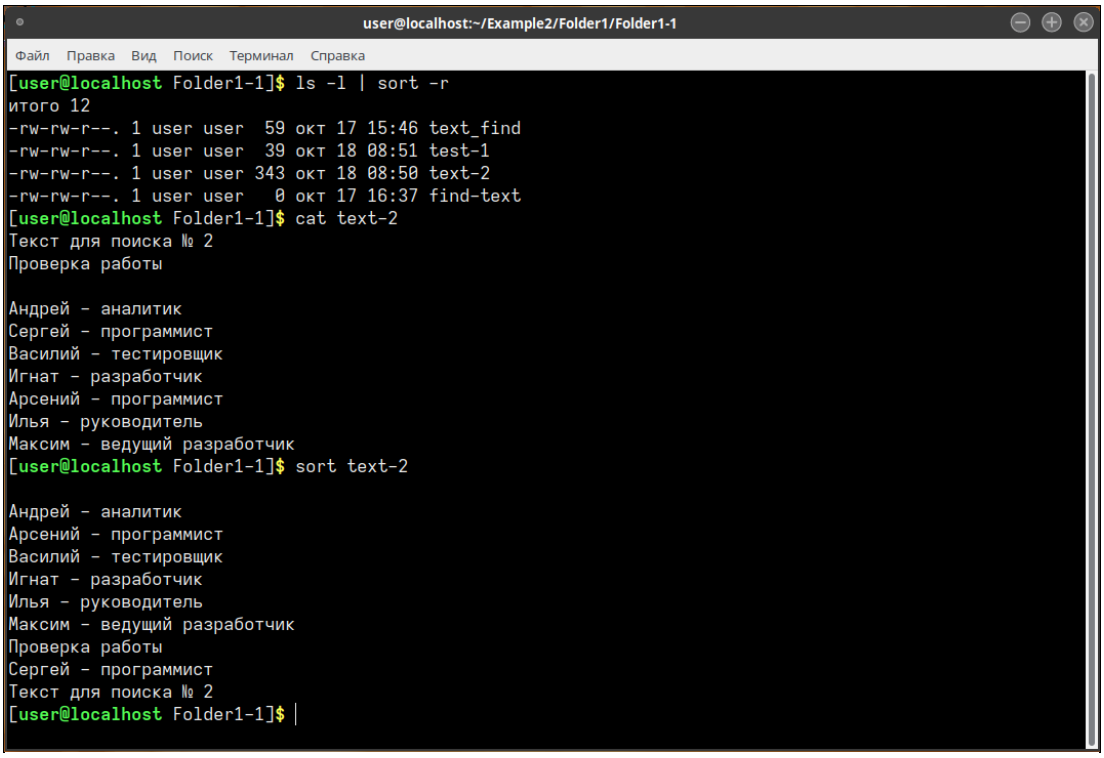
Команде **grep** также можно передавать и несколько параметров. Для этого перед каждым аргументом пишется ключ **-e**. Эту команду система понимает, как "или-или" и выводит все вхождения указанных слов. Кавычками выделяются только строки, содержащие пробел.

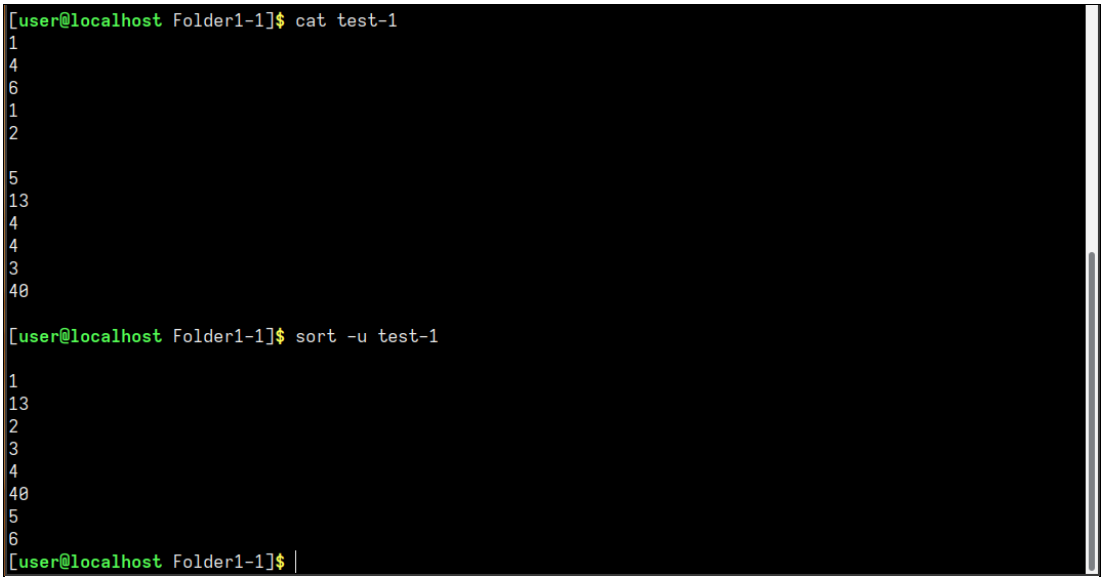


sort

Сортировка строк текста из одного или нескольких файлов по различным критериям, также может быть выполнена сортировка для вывода какой-либо команды. Наиболее полезные опции:

- **-b** - не учитывать пробелы;
- **-c** - проверить был ли отсортирован файл;
- **-n** (numeric) - сортирует по числовому значению;
- **-o** - вывести результат в файл;
- **-u** - игнорировать повторяющиеся строки
- **-r** (reverse) - сортирует в обратном порядке.



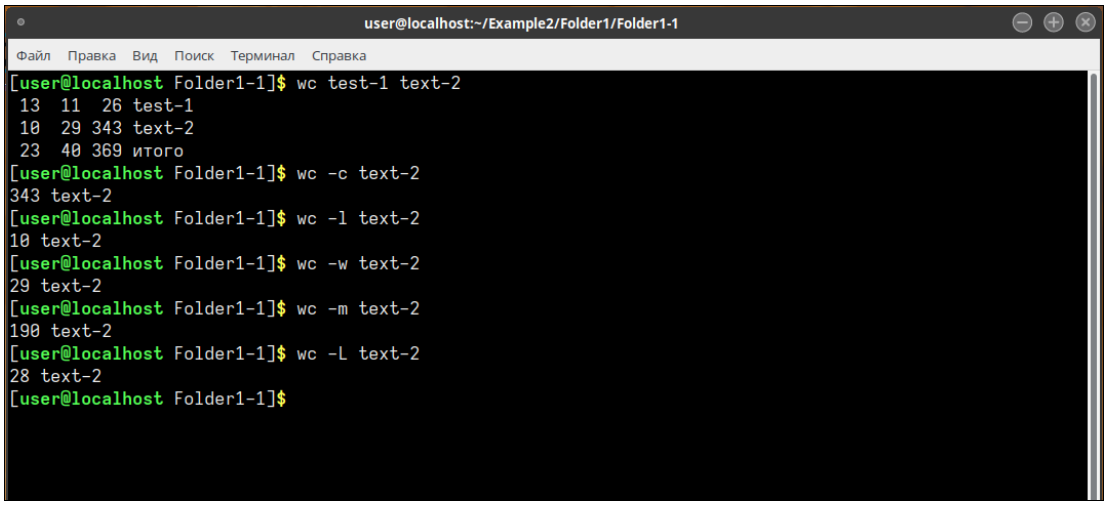


wc

Выводит число переводов строк, слов и байт для каждого указанного файла и итоговую строку, если было задано несколько файлов.

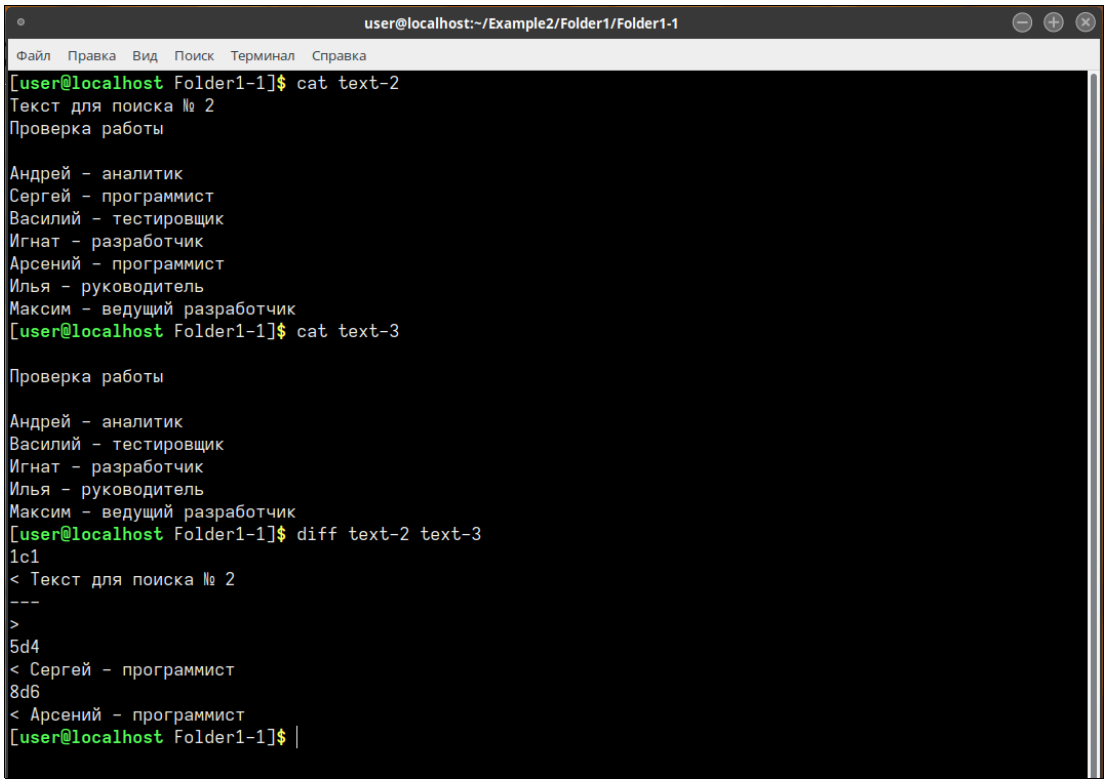
Основные опции:

- **-c**, **--bytes** – вывод размера файла в байтах;
- **-m**, **--chars** – вывод числа символов в файле;
- **-l**, **--lines** – вывод числа строк в файле;
- **-L**, **--max-line-length** – вывод максимальной длины строки в файле;
- **-w**, **--words** – вывод числа слов в файле.

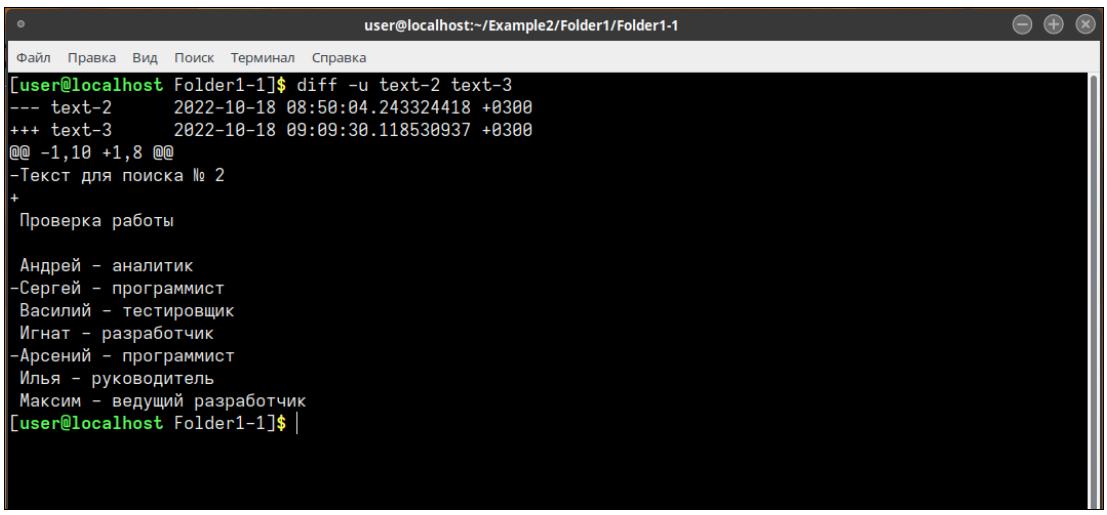


diff

Показывает различия между двумя файлами в построчном сравнении. Причём выводятся только строки, в которых обнаружены отличия. Измененные строки отмечаются символом «**c**», удаленные - «**d**», а новые - «**a**». Добавленные и удаленные строки обозначаются с помощью символов **>** и **<** соответственно.



Для вывода информации о различиях в унифицированном формате можно использовать опцию **-u**:



ps / pgrep

Предназначена для просмотра списка процессов. Чтобы завершить/приостановить какой-либо процесс, необходим его идентификатор. Один из способов получить его - утилита **ps**. Для отображения всех запущенных процессов можно использовать опцию **a**. Следует обратить внимание, что это только снимок состояния на момент вызова, информация не будет обновляться.

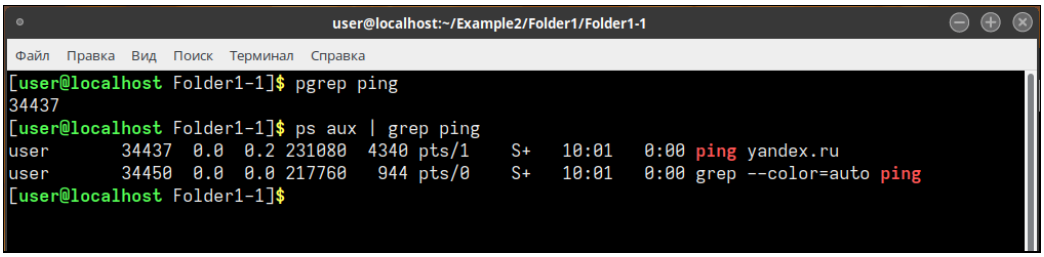
Для получения полной информации о процессах и определения идентификатора процесса (**PID**) выполните команду:

```
ps aux
```

Для конкретизации поиска определенного процесса рекомендуется использовать утилиту grep, например:

```
ps aux | grep ping
```

Утилита **pgrep** работает следующим образом: вы задаете имя процесса, а утилита показывает его идентификатор.



kill / xkill / pkill / killall

Данные команды служат для завершения процессов, однако они принимают различные параметры для идентификации процессов. **Kill** - нужен PID процесса, **xkill** - достаточно кликнуть по окну, чтобы закрыть его, **killall** и **pkill** - принимают имя процесса. Можно использовать любую из утилит, которая будет удобна в определенной ситуации.

Для определения идентификатора процесса (**PID**) воспользуйтесь утилитами ps или pgep, описанными выше.

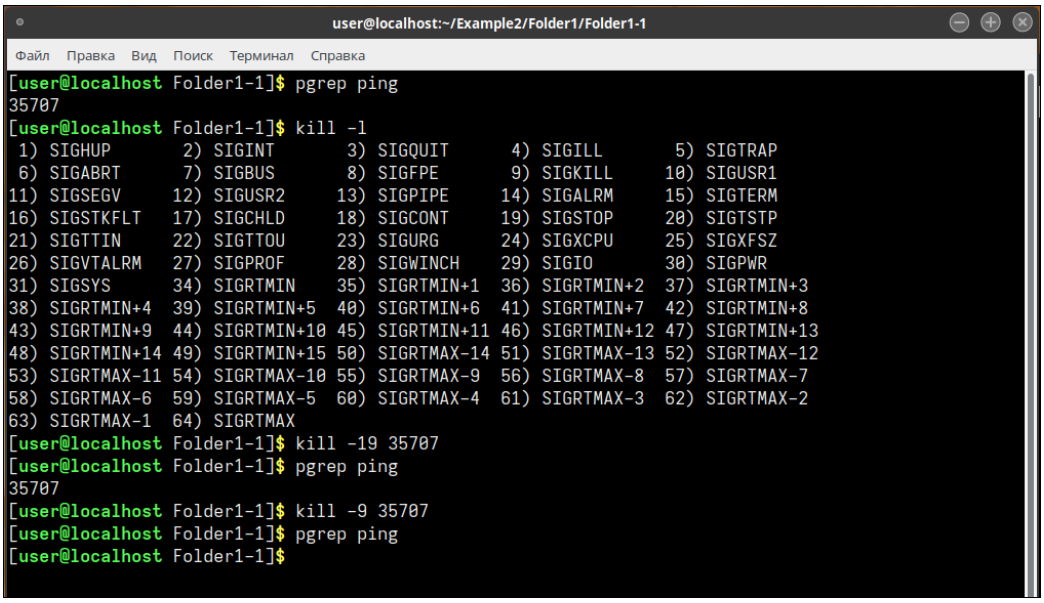
Для утилит kill и killall доступно несколько сигналов, которые также можно использовать для прерывания, завершения или приостановки процессов:

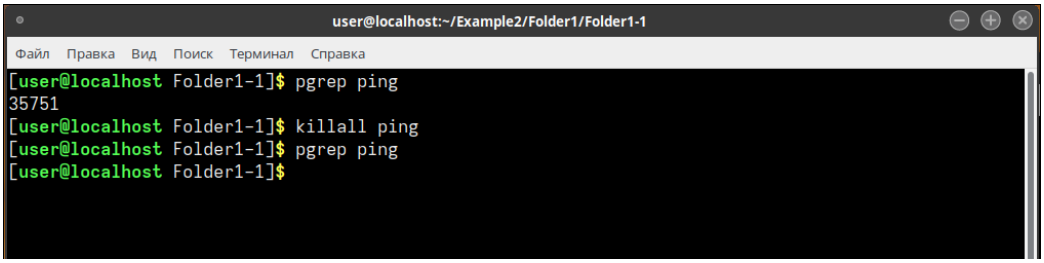
```
kill -l
killall -l
```

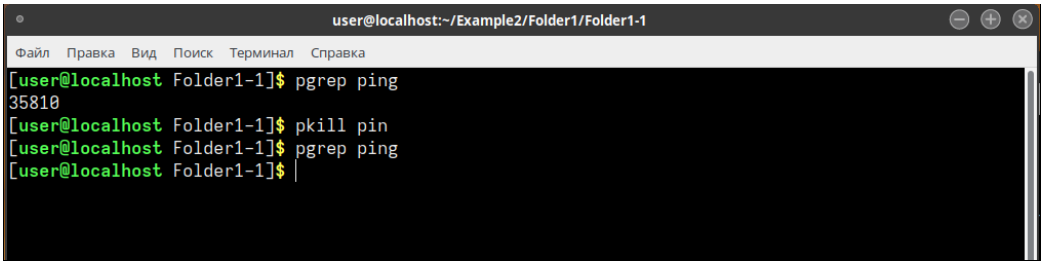
Принудительно завершить процесс можно, используя команды:

```
kill <PID_процесса>
killall <имя_процесса>
pkill <шаблон>
```

Утилита pkill может использовать как полное имя процесса для его завершения, так и часть имени. Утилита сопоставляет переданное ей имя процесса и может по ошибке завершить процесс с похожим именем, поэтому работу с утилитой следует проводить с осторожностью.

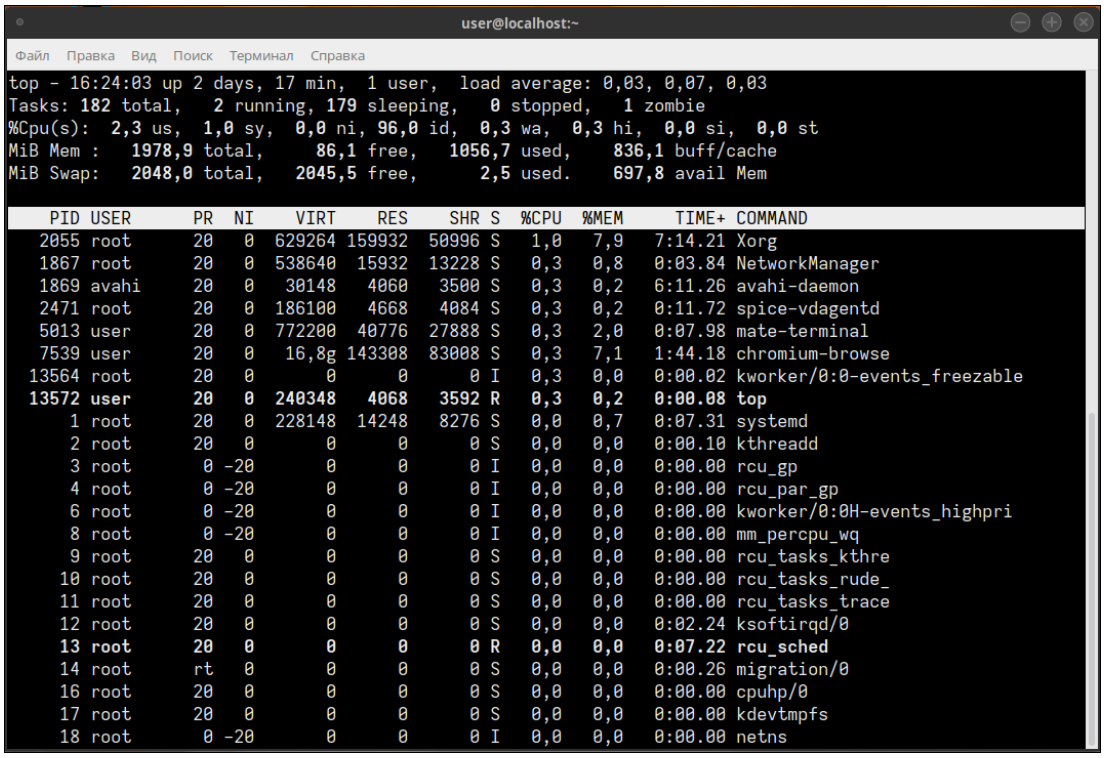






top / htop

Обе команды похожи, обе отображают процессы и могут быть использованы как консольные системные мониторы. **htop** - это улучшенная версия **top**. Вы сможете не только просматривать, но и контролировать процессы через его интерактивный интерфейс.



date

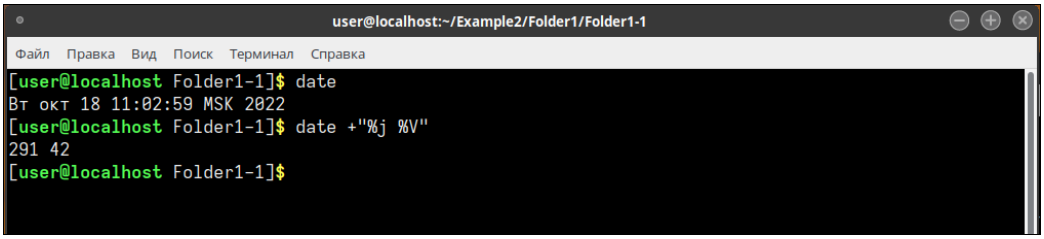
В отличие от **time**, выводит текущую дату и время в различных форматах и позволяет устанавливать системное время. Его можно форматировать в зависимости от ваших потребностей: вывести год, месяц, день, установить 12-ти или 24-ти часовой формат, получить наносекунды или номер недели. Например, **date +"%j %V"** выведет день в году и номер недели в формате ISO.

Установка системных даты и времени производится с правами администратора или суперпользователя (**root**) системы командой:

```
date ММДДччмм[[ВВ]ГГ][.сс]
```

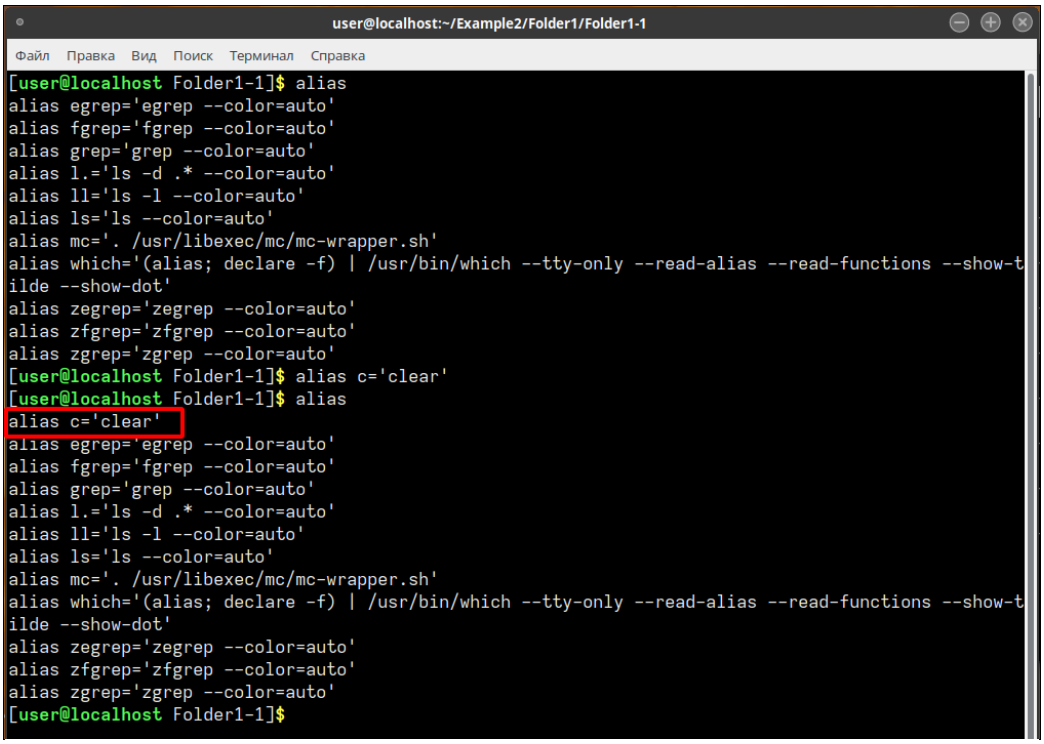
где:

- ММ - Месяц (от 01 до 12);
- ДД - День (от 01 до 28, 29, 30 или 31 в зависимости от месяца);
- чч - Часы (от 00 до 24);
- мм - Минуты (от 00 до 59);
- ГГ - Две последние цифры года (от 00 до 99, не обязательно);
- ВВ - Век (от 00 до 99, используется вместе с предыдущим элементом, не обязательно);
- .сс - Секунды (от 00 до 59 с символом точки, не обязательно).



alias

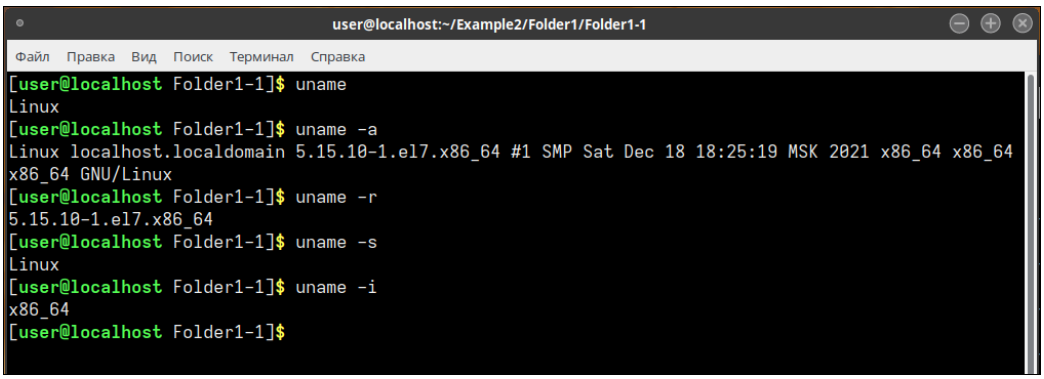
Команда создаёт синонимы для других команд Linux. То есть вы можете создать новые команды или группы команд, а также переименовывать существующие. Это очень удобно для сокращения длинных названий команд, которые вы часто используете, или создания более понятных имен для команд, которые вы используете нечасто или не можете запомнить.



uname

Выводит основную информацию о системе. Основные опции:

- **-a** (all) - информация о ядре, имени хоста и архитектуре процессора;
- **-i** - имя аппаратной реализации (платформы);
- **-r** - информация о релизе системы;
- **-s** - имя операционной системы, опция используется по умолчанию.

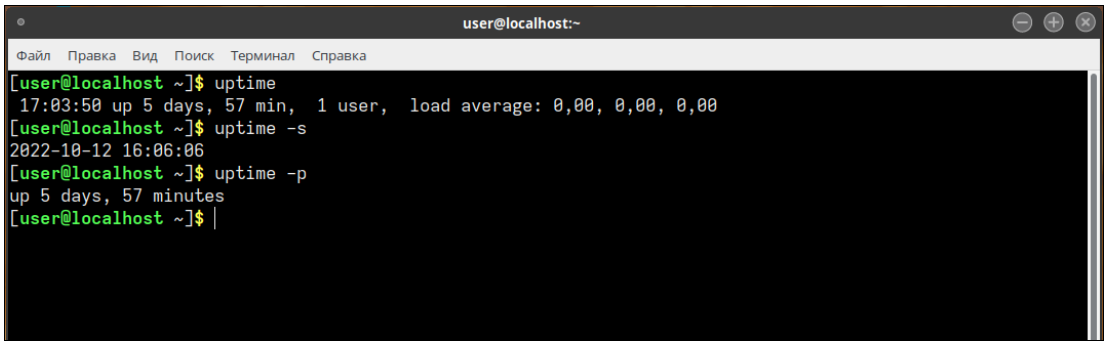


uptime

Выводит время работы системы, количество текущих в данный момент пользователей и среднюю загрузку системы за последние 1, 5 и 15 минут.

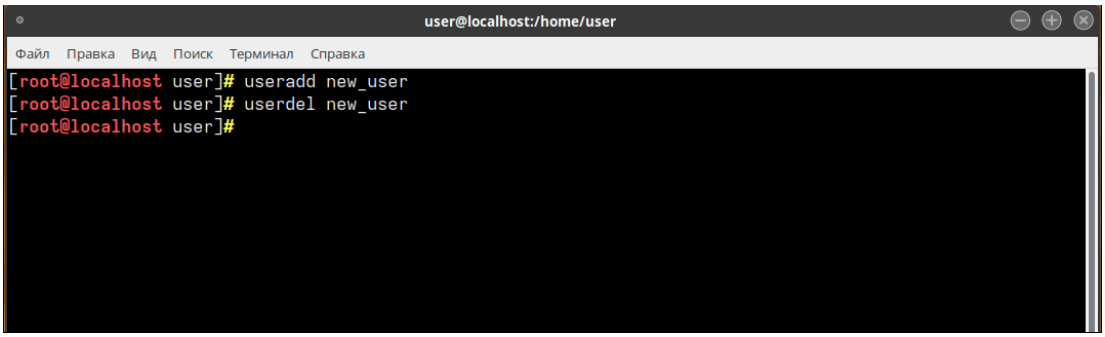
Можно использовать опции:

- **-s** (--since) - вывести время запуска системы. Это время, начиная с которого, отсчитывается время работы системы. Время выводится в формате YYYY-MM-DD HH:MM:SS;
- **-p** (--pretty) - вывести только время работы системы.



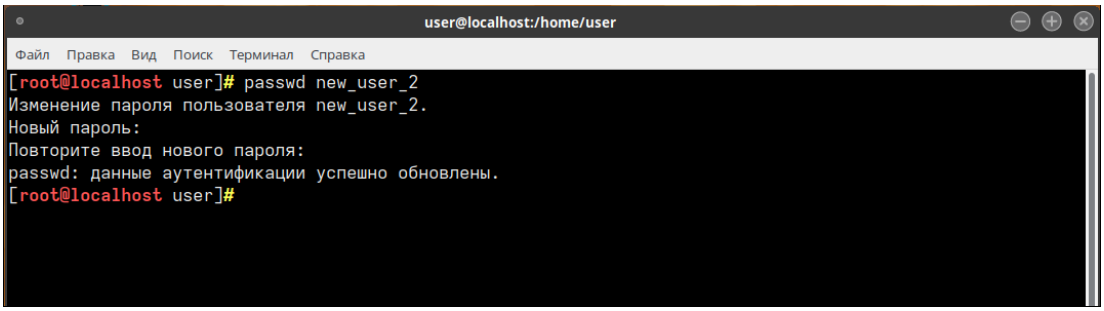
+ useradd / userdel / usermod

Эти команды позволяют добавлять, удалять и изменять учетные записи пользователей, для использования команд необходимы права администратора или суперпользователя (**root**) системы.



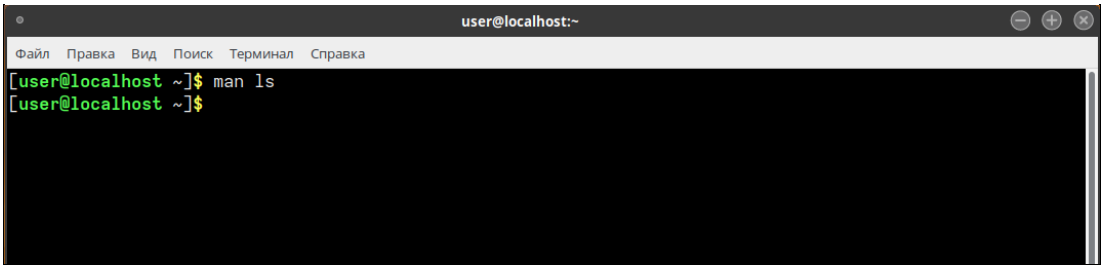
+ passwd

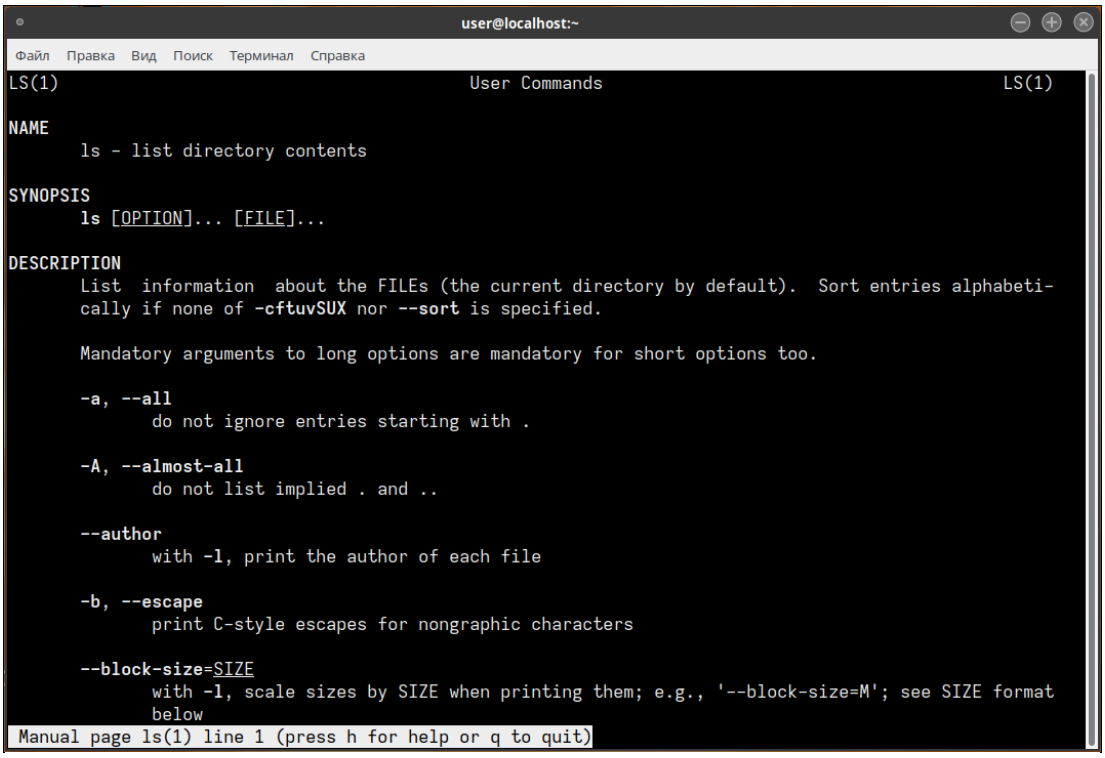
Эта команда позволяет изменить пароль учетной записи пользователя. Для использования команды необходимы права администратора или суперпользователя (**root**) системы.

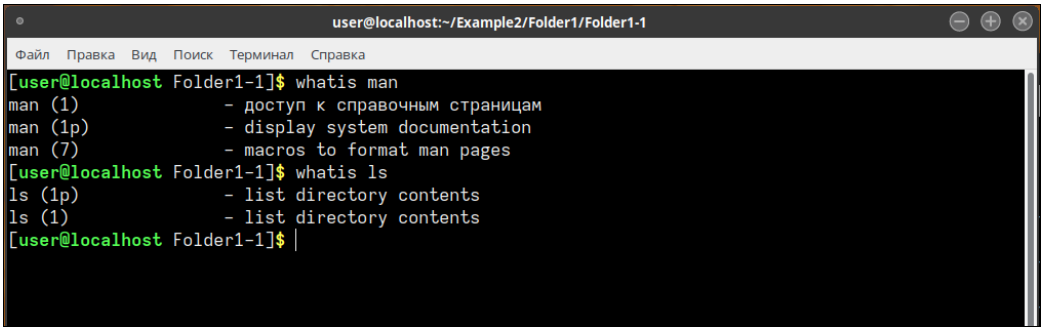


+ man / whatis

Команда **man** открывает руководство по определённой команде. Для всех основных команд Linux есть **man**-страницы. **Whatis** показывает, какие разделы руководств есть для данной команды.

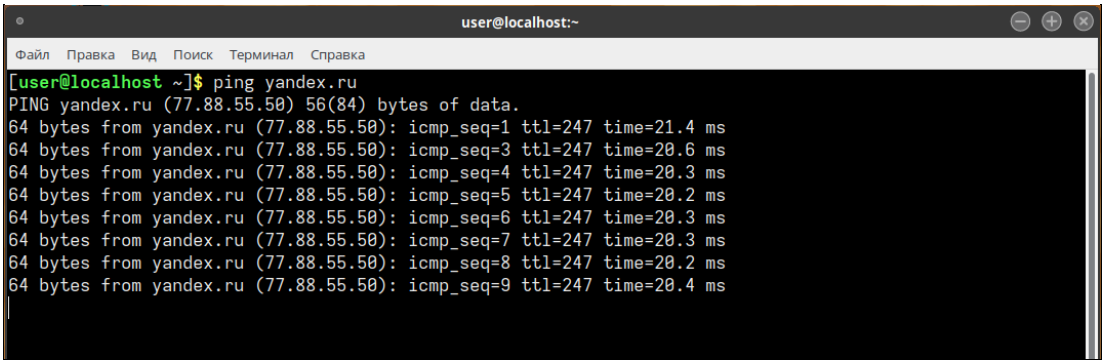






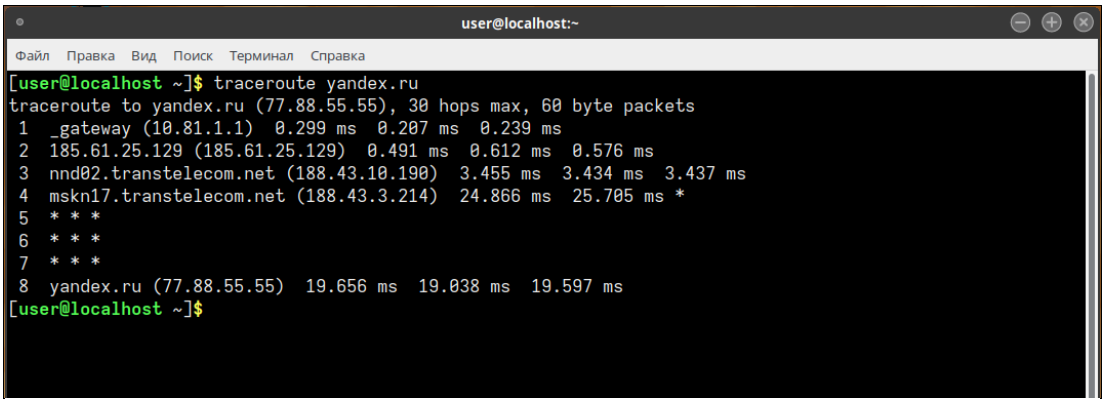
ping

Утилита **ping** может быть очень полезным диагностическим инструментом. Она поможет быстро проверить, подключены ли вы к маршрутизатору или к интернету, и дает некоторое представление о качестве этой связи.



traceroute

Это усовершенствованная версия **ping**. Мы можем увидеть не только полный маршрут сетевых пакетов, но и доступность узла, а также время доставки этих пакетов на каждый из узлов.



journalctl

journald — системная служба, отвечающая за сбор, хранение и управление данными журналов в ОС, также выполняет ротацию, сжатие и индексацию лог-файлов. **journalctl** позволяет просматривать и фильтровать данные, собираемых службой **journald**.

Полезные опции:

- **-f** — показать последние записи журнала и продолжить вывод новых записей при добавлении их в журнал;
- **-xb** — вывод записей журнала с момента запуска текущей сессии с расшифровкой ошибок.

```
[user@localhost ~]$ journalctl -f
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-tmpfiles-setup.service: Suc
ceeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped Create User's Volatile File
s and Directories.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus-broker.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped D-Bus User Message Bus.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus.socket: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Closed D-Bus User Message Bus Socke
t.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Shutdown.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-exit.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Finished Exit the Session.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Exit the Session.
```

ip

ip — утилита командной строки из пакета **iproute2**, которая позволяет выполнять настройку сетевой подсистемы и является заменой таких утилит, как *ifconfig*, *route*, *arp*.

```
[user@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group d
efault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    altname enp0s25
    inet [redacted] brd [redacted] scope global dynamic noprefixroute eno1
       valid_lft 90149sec preferred_lft 90149sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever
4: anbox0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group de
fault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet [redacted] scope global anbox0
       valid_lft forever preferred_lft forever
```

netstat

netstat — утилита командной строки, выводящая состояние TCP-соединений (как входящих, так и исходящих), таблицы

маршрутизации, число сетевых интерфейсов и сетевую статистику по протоколам.

```
[root@localhost user]# netstat --inet -pl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:46825         0.0.0.0:*               LISTEN      1088/containerd
tcp        0      0 0.0.0.0:ideafarm-door   0.0.0.0:*               LISTEN      1055/vmware-authdla
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      1086/sshd: /usr/sbi
tcp        0      0 localhost:54329         0.0.0.0:*               LISTEN      1113/postgres
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2133/dnsmasq
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      1078/cupsd
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN      1258/master
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2180/dnsmasq
udp        0      0 0.0.0.0:40848           0.0.0.0:*                           791/avahi-daemon: r
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2180/dnsmasq
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2180/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*                           1/systemd
udp        0      0 localhost:323           0.0.0.0:*                           848/chronyd
```

df

Утилита **df** — консольная утилита, которая позволяет проверить использование дискового пространства в операционной системе. Эта команда отображает информацию об общем, свободном и используемом объеме памяти файловых систем. Утилита **df** предоставляет множество опций, которые позволяют настроить ее вывод.

```
[root@localhost user]# df
Файловая система 1K-блоков Использовано  Доступно Использовано% Смонтировано в
devtmpfs              4096            0      4096            0% /dev
tmpfs              4011852       608496   3403356           16% /dev/shm
tmpfs              1604744         3632   1601112            1% /run
/dev/sdb1        234213368    181416340  40826880           82% /
/dev/sda4        530945160    134478724 369422392           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1          106496       106496         0          100% /var/lib/snapd/snap/core/16928
/dev/loop0          108032       108032         0          100% /var/lib/snapd/snap/core/16574
/dev/loop2           57088        57088         0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3           57088        57088         0          100% /var/lib/snapd/snap/core18/2812
/dev/loop4           73088        73088         0          100% /var/lib/snapd/snap/webinar/7
/dev/loop6             128          128         0          100% /var/lib/snapd/snap/bare/5
/dev/loop7          168832       168832         0          100% /var/lib/snapd/snap/gnome-3-28-1804/198
/dev/loop5          382848       382848         0          100% /var/lib/snapd/snap/anbox/186
/dev/loop8           93952        93952         0          100% /var/lib/snapd/snap/gtk-common-themes/1535
/dev/loop9           72960        72960         0          100% /var/lib/snapd/snap/webinar/6
tmpfs               802368          160    802208            1% /run/user/1000
[root@localhost user]# df -h
Файловая система Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs           4,0M            0  4,0M            0% /dev
tmpfs              3,9G          595M  3,3G           16% /dev/shm
tmpfs              1,6G          3,6M  1,6G            1% /run
/dev/sdb1          224G          174G   39G           82% /
/dev/sda4          507G          129G  353G           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1         104M          104M     0          100% /var/lib/snapd/snap/core/16928
/dev/loop0         106M          106M     0          100% /var/lib/snapd/snap/core/16574
/dev/loop2          56M           56M     0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3          56M           56M     0          100% /var/lib/snapd/snap/core18/2812
```

free

Команда **free** предоставляет информацию об общем объеме физической памяти и памяти подкачки, а также о свободной и используемой памяти.

```
[user@localhost ~]$ free
               total        used        free      shared  buff/cache   available
Mem:         8023704     6372008      367168      575088     1284528      781116
Swap:        5122228     4663944      458284
[user@localhost ~]$ free -m
               total        used        free      shared  buff/cache   available
Mem:            7835        6225         355         561        1254         760
Swap:           5002        4554         447
[user@localhost ~]$ free -h
               total        used        free      shared  buff/cache   available
Mem:           7,7Gi       6,1Gi       355Mi       565Mi       1,2Gi       759Mi
Swap:          4,9Gi       4,4Gi       447Mi
[user@localhost ~]$
```

Получение справочной информации об использовании утилит с помощью man

Установка
Навигация
Разделы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО:** man-db-2.7.6.1-1, man-pages-4.16-1

man — утилита, предназначенная для форматирования и вывода справочных страниц. Каждая страница справки является самостоятельным документом и пишется разработчиками соответствующего программного обеспечения.

Установка

В РЕД ОС по умолчанию утилита уже установлена. Однако, если по каким-либо причинам она отсутствует, ее можно установить. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install man man-pages
```

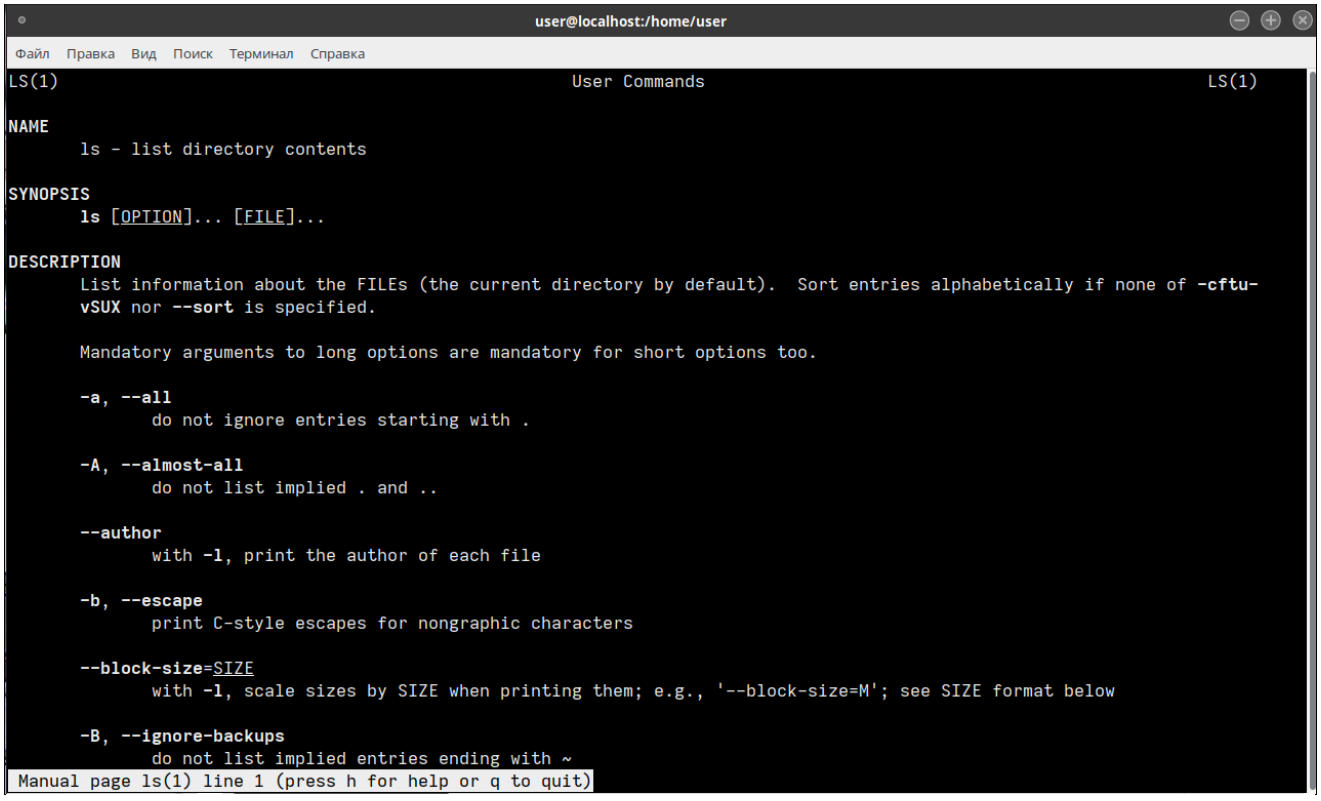
Далее команды будут выполняться с правами **локального пользователя**, если не указано иное.

Для вывода справочного руководства по какой-либо команде или пакету с возможностью запуска в терминале необходимо выполнить команду вида:

```
man <команда>
```

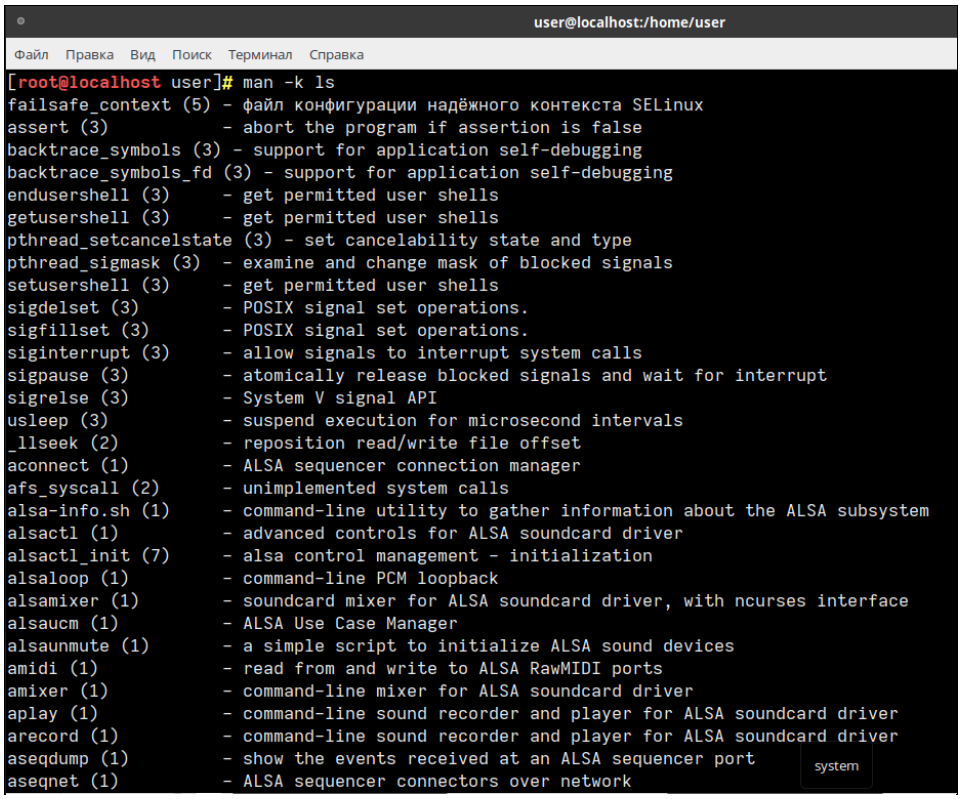
Например:

```
man ls
```



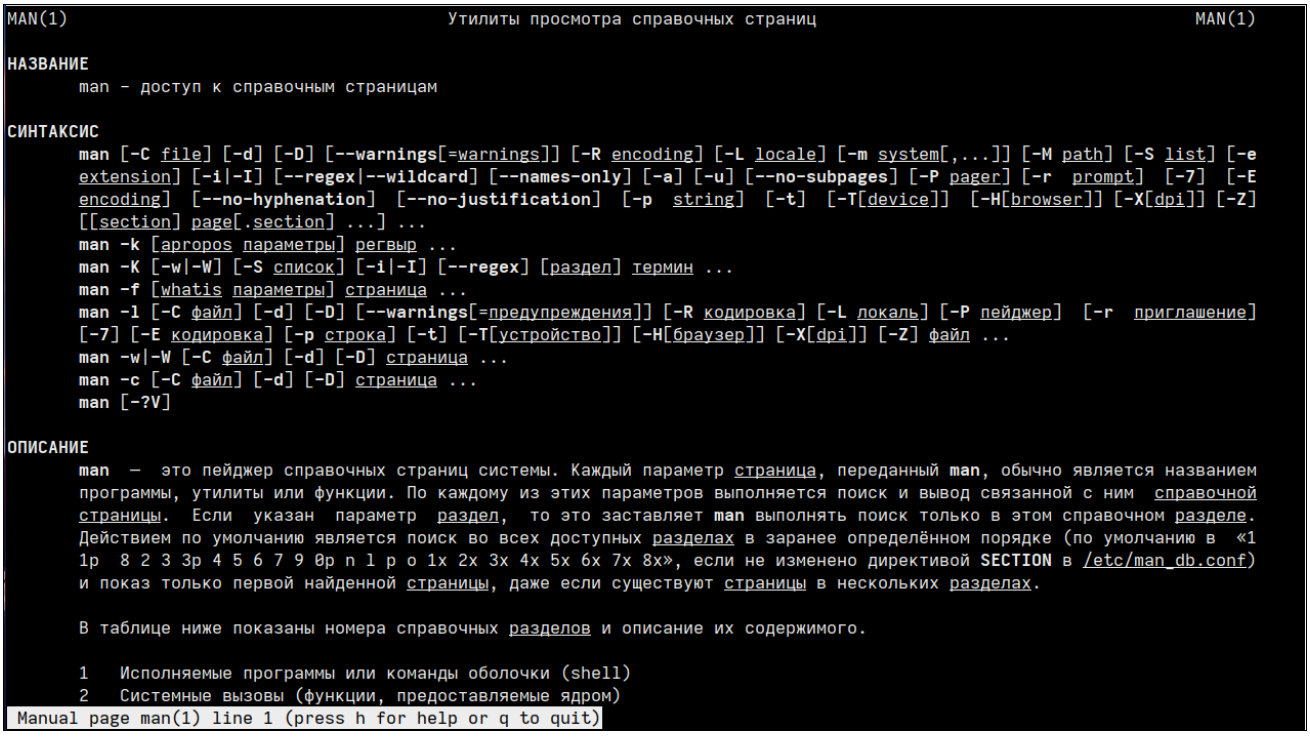
Опция **-k** выполняет поиск и выводит список man-страниц, в которых встречается искомый запрос.

```
man -k ls
```



Другие полезные опции утилиты **man** можно посмотреть командой:

```
man man
```



Навигация

Для навигации по страницам руководства используются следующие сочетания клавиш:

- ↑ и ↓ — для построчного перехода по руководству;
- **PgUp** и **PgDown** — для постраничного перехода по руководству;

- **/** — поиск по странице; введите **/** и искомое слово, затем нажмите **Enter**;
- **?** — поиск в обратном направлении (снизу вверх); введите **?** и искомое слово, затем нажмите **Enter**;
- **n** — переход к следующему подсвеченному вхождению;
- **Shift+n** — переход к предыдущему подсвеченному вхождению;
- **&** — поиск внутри страницы; выводятся только строки, где было найдено искомое слово;
- **h** — открыть справку по командам и горячим клавишам, для закрытия справки нажмите **q**;
- **q** — закрыть man-страницу.

Разделы

Справочные страницы поделены на 8 стандартных разделов и один дополнительный. Каждый из разделов соответствует той или иной тематике.

Раздел	Краткое описание
1	Прикладные программы и команды оболочки
2	Системные вызовы ядра (функции языка Си)
3	Библиотечные вызовы (функции различных библиотек, установленных в систему)
4	Специальные файлы (находящиеся обычно в каталоге **/dev**)
5	Форматы файлов и соглашения
6	Игры
7	Различные описания, соглашения и прочее
8	Команды администрирования системы, которые обычно запускаются от имени суперпользователя
9	Ядро операционной системы (нестандартный раздел)

Номер раздела в команде **man** указывается вторым аргументом, перед названием справочной страницы. Если номер раздела опущен, то поиск справочной страницы ведётся по всем разделам по порядку.

```
man kill  # раздел 1
man 1 kill  # раздел 1
man 2 kill  # раздел 2
```

Общие рекомендации

В целях соблюдения безопасности рекомендуется:

- не использовать пароли, попытка установки которых приводит к предостережению от утилиты **passwd**;
- не работать привилегированным пользователем;
- не запускать те сервисы, которыми никто не будет пользоваться, и отключать временно неиспользуемые;
- следовать основным правилам сетевой безопасности:
    - настроить **firewall** между компьютером и остальной сетью, а также между корпоративной сетью и Интернет;
    - использовать защищенные протоколы для передачи данных, такие как **IPSEC** (IP Security) и **SSH** (Secure Shell);

- не использовать электронную почту для передачи конфиденциальной информации; если использование электронной почты для этих целей абсолютно необходимо, например, ввиду отсутствия технической возможности применения защищенных протоколов передачи данных, то воспользуйтесь **GnuPG** для подписи и шифрования почтовых сообщений;
- использовать различные пароли к локальным ресурсам и ресурсам, расположенным на удаленных серверах, чтобы пароли к локальным ресурсам не покидали пределов локальной сети.

В РЕД ОС настройки для пользователя *root* определяются спецификой его задач, а потому не приспособлены для повседневной работы и лишь ограниченно локализованы.

Аудит в РЕД ОС

Журналирование
Аудит системных вызовов
Файлы и утилиты аудита РЕД ОС
Описание auditd.conf
Служба аудита — auditd
Утилита auditctl
Примеры базовых правил и конструкций утилиты auditctl
Утилита aureport
Утилита ausearch
Утилита autrace

Основными целями при разработке системных вызовов для подсистемы аудита были:

- максимально низкая нагрузка на производительность;
- отсутствие подобной функциональности в SELinux (и/или в любой другой подсистеме безопасности).

Инструментарий аудита будет работать без внедренных компонент безопасности, но он не может быть использован вместо них, например, он не будет предоставлять функциональные возможности без действующих подсистем безопасности.

Есть две основные части: одна работает всегда (базовое журналирование в **audit.c**), а другой можно управлять во время загрузки или работы сервера (аудит системных вызовов в **auditsc.c**). Патч включает в себя изменения в **security/selinux/avc.c** в качестве примера, как системные вызовы аудита могут быть использованы совместно с другим кодом, определяющим события для аудита.

Журналирование

Использует сетевой сокет для связи с пользовательским пространством. Если служба запущена - все сообщения журналируются через этот сетевой сокет. Иначе, сообщения журналируются через **printk** посредством службы **syslog** (по умолчанию).

Сообщения могут не журналироваться (настраивается отдельно) в зависимости от настроек аудита, скорости генерации сообщений или загруженности памяти.

Когда какая-то часть ядра генерирует часть сообщения аудита, эта часть будет немедленно послана в пользовательское пространство, и автоматически выставится флаг, указывающий, что этот системный вызов находится под аудитом. Таким образом, при выходе из системного вызова будет сформирована дополнительная информация (если включен аудит системных вызовов).

Аудит системных вызовов

Во время создания процесса формируется контекст аудита и привязывается к структуре, описывающей процесс.

Во время входа в системный вызов, заполняется следующая информация в контексте аудита, если он есть: номер системного вызова, дата и время, но не аргументы.

В ходе работы системного вызова перехватываются обращения к **getname()** и **path_lookup()**. Эти процедуры вызываются, когда ядро действительно собирается искать информацию, для принятия решения, будет ли системный вызов успешно выполнен или нет. Перехватывать вызовы нужно для того, чтобы не допустить копирование информации, которую генерирует **getname**, поскольку **getname** уже сделал приватную (для ядра) копию этой информации.

Сохранение копий всех аргументов системного вызова усложняет реализацию и требует увеличения расхода ресурсов, что, наиболее вероятно, не нужно. С этим патчем, к примеру, если пользователь непривилегированный, то **chroot** ("foo") будет завершен с ошибкой - "foo" не будет отражено в записи аудита, потому что ядро определяет еще перед поиском "foo", что работа системного вызова не может быть продолжена. Этот подход предотвращает сохранение пользовательской информации, которая может быть ложной или ненадежной (например, из-за атаки на совместно используемую память) в отличие от истинной информации, фактически используемой ядром.

Во время выхода их системного вызова генерируется та часть сообщения аудита, которая ответственна за информацию о системном вызове, включая имена файлов и номера **inode** (если доступны). Сообщение о системном вызове генерируется, только если выставлен флаг, указывающий, что системный вызов находится под аудитом (он выставляется, например, когда SELinux генерирует ***avc*** сообщение или когда другая часть ядра определяет, что должно формироваться сообщение для аудита). Следует заметить, что полное сообщение аудита приходит в пользовательское пространство по частям, это позволяет не хранить сообщения неопределенный срок внутри ядра.

Во время завершения процесса контекст аудита уничтожается.

Во время генерации сообщения аудита может быть выполнена простая фильтрация (например, для увеличения производительности - отключение аудита системных вызовов, выполняемых от имени пользователя, работающего с базой данных). Фильтрация может быть, как простой, так и сложной. В основном, инструментарий аудита использует компоненты ядра (например, SELinux), чтобы принимать

решение о том, что необходимо подвергать аудиту, а что нет.

Файлы и утилиты аудита РЕД ОС

Описание auditd.conf

В файле **/etc/audit/auditd.conf** определяются параметры службы аудита. На одной строке может быть не больше одной директивы. Директива состоит из ключевого слова (названия параметра), знака равенства и соответствующих ему данных (значения параметра). Допустимые ключевые слова:

log_file, log_format, flush, freq, num_logs, max_log_file, max_log_file_action, space_left, action_mail_acct, space_left_action, admin_space_left, admin_space_left_action, disk_full_action и disk_error_action.

Далее даётся описание каждого из них.

Ключ	**Значение ключа**
log_file	Полное имя файла, в который следует записывать протокол.
log_format	Оформление данных в протоколе. Допустимы два значения: *raw* и *nolog*. При указании **RAW**, данные будут записываться в том виде, в котором они получаются от ядра. Значение **NOLOG** отключает запись данных об аудите. Этот параметр не влияет на обработку данных диспетчером событий системы аудита.
priority_boost	Неотрицательное число, определяющее повышение приоритета выполнения службы аудита. Значение по умолчанию: **3**. Для того чтобы не изменять приоритет, укажите **0**.
flush	Стратегия работы с дисковым буфером. Допустимые значения: *none*, *incremental*, *data* и *sync*. Вариант **none**, отключает какие-либо дополнительные действия со стороны службы по синхронизации буфера с диском. При значении **incremental**, запросы на перенос данных из буфера на диск выполняются с частотой задаваемой параметром **freq**. При значении **data** данные файла синхронизируются немедленно. Значение **sync** указывает на необходимость немедленной синхронизации как данных, так и метаданных файла при записи на диск.
freq	Максимальное число записей протокола, которые могут храниться в буфере. При достижении этого числа производится запись буферированных данных на диск. Данный параметр допустим, только если **flush** имеет значение **incremental**.
num_logs	Максимальное число файлов с протоколами. Используется, если параметр **max_log_file_action** имеет значение **rotate**. Если указано число меньше 2, при достижении ограничения на размер файла он обнуляется. Значение параметра не должно превышать **99**. Значение по умолчанию: **0**. При указании большого числа может потребоваться увеличить ограничение на количество ожидающих запросов. Это можно сделать в файле **/etc/audit/rules.d/audit.rules**.
dispatcher	Диспетчер - программа, которой (на стандартный ввод) будут передаваться копии сообщений о событиях аудита. Она запускается (с правами администратора) службой аудита при загрузке последней.
disp_qos	Разрешить ли блокирование при взаимодействии с диспетчером. Для передачи информации диспетчеру используется буфер размером 128 Кб. Это значение является оптимальным для большинства случаев. Если блокирование запрещено (**lossy**), то все сообщения, поступающие при полном буфере, не будут доходить до диспетчера (записи о них по-прежнему будут вноситься в файл на диске, если только **log_format** не равно **nolog**). В случае, если блокирование разрешено (**lossless**), служба аудита будет ожидать появления свободного места в очереди, передавать сообщение диспетчеру и только потом записывать его на диск. Допустимые значения: **lossy** и **lossless**. Значение по умолчанию - **lossy**.
max_log_file	Ограничение на размер файла протокола в мегабайтах. Действие, выполняемое при достижении размера файла указанного значения, можно настроить с помощью следующего параметра.
max_log_file_action	Действие, предпринимаемое при достижении размером файла протокола максимального значения. Допустимые значения: *ignore*, *syslog*, *suspend*, *rotate* и *keep_logs*. Вариант **ignore** отключает контроль над размером файла. При значении **syslog** в системный протокол будет внесено соответствующее сообщение. При значении **suspend** дальнейшее ведение протокола будет прекращено. Служба по-прежнему будет работать. При значении **rotate** текущий файл будет переименован и для протокола будет создан новый файл. Имя предыдущего протокола будет дополнено числом **1**, а номера других протоколов (если они имеются) будут увеличены на единицу. Таким образом, чем больше номер у протокола, тем он старше. Максимальное число файлов определяется параметром **num_logs** (естественно, соответствие ему достигается за счёт удаления самых старых протоколов). Такое поведение аналогично поведению утилиты **logrotate**. Вариант **keep_logs** аналогичен предыдущему, но число файлов не ограничено.
action_mail_acct	Адрес электронной почты. Значение по умолчанию: root. Если адрес не локальный по отношению к данной системе, необходимо чтобы в ней был настроен механизм отправки почты. В частности, требуется наличие программы **/usr/lib/sendmail**.
space_left	Минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое следующим параметром.
space_left_action	Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного минимума. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается программа по указанному пути. Передача параметров не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.
admin_space_left	Критический минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое следующим параметром. Данное действие следует рассматривать как последнюю меру, предпринимаемую перед тем, как закончится место на диске. Значение настоящего параметра должно быть меньше значения **space_left**.

Ключ	Значение ключа
admin_space_left_action	Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного критического минимума. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении **email** по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается программа по указанному пути. Передача параметров не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.
disk_full_action	Действие, предпринимаемое при обнаружении отсутствия свободного пространства на диске. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается сценарий по указанному пути. Передача параметров сценарию не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.
disk_error_action	Действие, предпринимаемое при возникновении ошибки в работе с диском. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении **email** по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается сценарий по указанному пути. Передача параметров сценарию не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.

ВАЖНО!

В среде CAPP (Controlled Access Protection Profile - контролируемый профиль защиты доступа) ведение протоколов настолько важно, что невозможность его продолжения может служить основанием отказа в доступе к ресурсам. Поэтому рекомендуется выделять для файла **/var/log/audit** специальный раздел. Кроме того, параметру **flush** следует присвоить значение **sync** или **data**.

Для обеспечения полного использования раздела параметрам **max_log_file** и **num_logs** следует присвоить соответствующие значения. Учитывайте, что чем больше файлов создаётся на диске (и, соответственно, переименовывается), тем больше времени будет уходить на обработку событий при достижении размером очередного файла максимума. Параметру **max_log_file_action** рекомендуется присвоить значение **keep_logs**.

Значение **space_left** должно быть таким, которое позволит администратору вовремя среагировать на предупреждение. Обычно в число действий, выполняемых администратором, входит запуск **aureport -t** и архивирование самых старых протоколов. Значение **space_left** зависит от системы, в частности от частоты поступления сообщений о событиях. Значение **space_left_action** рекомендуется установить в **email**. Если требуется отправка сообщения **snmp trap**, укажите вариант **exec**.

Установите значение **admin_space_left** таким образом, чтобы хватило свободного места для сохранения записей о последующих действиях администратора. Значение параметра **admin_space_left_action** следует установить в **single**, ограничив, таким образом, способы взаимодействия с системной консолью.

Действие, указанное в **disk_full_action**, выполняется, когда в разделе уже не осталось свободного места. Доступ к ресурсам машины должен быть полностью прекращён, т.к. нет возможности контролировать работу системы. Это можно сделать, указав значение **single** или **halt**.

Значение **disk_error_action** следует установить в **syslog**, **single**, либо **halt** в зависимости от соглашения относительно обращения со сбойным аппаратным обеспечением.

Служба аудита - auditd

Служба **auditd** - это прикладной компонент системы аудита Linux. Он ведёт протокол аудита на диске. Для просмотра протоколов предназначены команды **ausearch** и **aureport**. Команда **auditctl** позволяет настраивать правила аудита. Кроме того, при загрузке загружаются правила из файла **/etc/audit/rules.d/audit.rules**. Некоторые параметры самой службы можно изменить в файле **auditd.conf**.

Синтаксис:

```
auditd [-f] [-l] [-n]
```

Опции:

Опция	Значение опции
-f	Не переходить в фоновый режим (для отладки). Сообщения программы будут направляться в стандартный вывод для ошибок (**stderr**), а не в файл.
-l	Включить следование по символическим ссылкам при поиске конфигурационных файлов.

Опция	Значение опции
-n	Не создавать дочерний процесс. Для запуска из **inittab**.

Сигналы:

Сигнал	Значение сигнала
SIGHUP	Перезагрузить конфигурацию - загрузить файл конфигурации с диска. Если в файле не окажется синтаксических ошибок, внесенные в него изменения вступят в силу. При этом в протокол будет добавлена запись о событии **DAEMON_CONFIG**. В противном случае действия службы будут зависеть от параметров **space_left_action**, **admin_space_left_action**, **disk_full_action**, **disk_error_action** файла **auditd.conf**.
SIGTERM	Прекратить обработку событий аудита и завершить работу, о чём предварительно занести запись в протокол.
SIGUSR1	Создать новый файл для протокола, перенумеровав старые файлы или удалив часть из них, в зависимости от параметра **max_log_size_action**.

ВАЖНО!

Для того чтобы сделать возможным аудит всех процессов, запущенных до службы аудита, добавьте в строку параметров ядра (в конфигурации загрузчика) **audit=1**. В противном случае аудит некоторых процессов будет невозможен.

Утилита auditctl

Утилита **auditctl** используется для контроля поведения, получения состояния и добавления/удаления правил аудита, предоставляемого Linux ядром.

Опции:

Опция	Значение опции
-b *backlog*	Установить максимальное количество доступных для аудита буферов, ожидающих обработки (значение в ядре по умолчанию - 64). Если все буфера заняты, то флаг сбоя будет выставлен ядром для его дальнейшей обработки.
-e [0..2]	Установить флаг блокировки. **0** позволит на время отключить аудит, включить его обратно можно, передав **1** как параметр. Если установлено значение опции **2**, то защитить конфигурацию аудита от изменений. Каждый, кто захочет воспользоваться этой возможностью, может поставить эту команду последней в **audit.rules**. После этой команды все попытки изменить конфигурацию будут отвергнуты с уведомлением в журналах аудита. В этом случае, чтобы задействовать новую конфигурацию аудита, необходимо перезагрузить систему аудита.
-f [0..2]	Установить способ обработки для флага сбоя. **0**=silent **1**=printk **2**=panic. Эта опция позволяет определить, каким образом ядро будет обрабатывать критические ошибки. Например, флаг сбоя выставляется при следующих условиях: ошибки передачи в пространство службы аудита, превышение лимита буферов, ожидающих обработки, выход за пределы памяти ядра, превышение лимита скорости выдачи сообщений. Значение по умолчанию: **1**. Для систем с повышенными требованиями к безопасности, значение **2** может быть более предпочтительно.
-h	Краткая помощь по аргументам командной строки.
-i	Игнорировать ошибки при чтении правил из файла.
-l	Вывести список всех правил по одному правилу в строке.
-k *<ключ>*	Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше *31 символа*. Ключ помогает уникально идентифицировать записи, генерируемые в ходе аудита за точкой наблюдения.
-m *<текст>*	Послать в систему аудита пользовательское сообщение. Это может быть сделано только из-под учетной записи **root**.
-p [r|w|x|a]	Установить фильтр прав доступа для точки наблюдения. **r**=чтение, **w**=запись, **x**=исполнение, **a**=изменение атрибута. Не путайте эти права доступа с обычными правами доступа к файлу - они определяют типы системных вызовов, которые выполняют данные действия. Заметьте, системные вызовы **read** и **write** не включены в этот набор, поскольку логи аудита были бы перегружены информацией о работе этих вызовов.
-r *<частота>*	Установить ограничение скорости выдачи сообщений в секунду (**0** - нет ограничения). Если эта частота не нулевая и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: **0**.
-R *<файл>*	Читать правила из *файла*. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Следующие ограничения накладываются на файл: владельцем должен быть **root** и доступ на чтение должен быть только у него. Файл может содержать комментарии, начинающиеся с символа «**#**». Правила, расположенные в файле, идентичны тем, что набираются в командной строке, без указания «**auditctl**».
-s	Получить статус аудита.

Опция	Значение опции
-a *<список, действие>*	Добавить правило с указанным *действием* к концу *списка*. Заметьте, что запятая разделяет эти два значения. Отсутствие запятой вызовет ошибку. Ниже описаны имена доступных списков: • **task** - добавить правило к списку, отвечающему за процессы. Этот список правил используется только во время создания процесса - когда родительский процесс вызывает **fork()** или **clone()**. При использовании этого списка вы можете использовать только те поля, которые известны во время создания процесса: **uid**, **gid** и т.д. • **entry** - добавить правило к списку, отвечающему за точки входа системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам входа системных вызовов. • **exit** - добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов. • **user** - добавить правило, отвечающее за список фильтрации пользовательских сообщений. Этот список используется ядром, чтобы отфильтровать события приходящие из пользовательского пространства перед тем, как они будут переданы службе аудита. Необходимо отметить, что только следующие поля могут быть использованы: **uid**, **auid**, **gid** и **pid**. Все остальные поля будут обработаны, как если бы они не совпали. • **exclude** - добавить правило к списку, отвечающему за фильтрацию событий определенного типа. Этот список используется, чтобы отфильтровывать ненужные события. Например, если вы не хотите видеть *avc* сообщения, вы должны использовать этот список. Тип сообщения задается в поле **msgtype**.

Ниже описаны доступные *действия* для правил:

Действие	Описание действия
never	Аудит не будет генерировать никаких записей. Это может быть использовано для подавления генерации событий. Обычно необходимо подавлять генерацию вверху списка, а не внизу, т.к. событие инициируется на первом совпавшем правиле.
always	Установить контекст аудита. Всегда заполнять его во время входа в системный вызов и всегда генерировать запись во время выхода из системного вызова.
-A *<список, действие>*	Добавить правило с указанным действием в начало списка.
-d *<список, действие>*	Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали и имя системного вызова, и поля сравнения.
-D	Удалить все правила и точки наблюдения.
-S *<имя или номер системного вызова>*/[**all**]	Любой номер или имя системного вызова может быть использован. Также возможно использование ключевого слова **all**. Если какой-либо процесс выполняет указанный системный вызов, то аудит генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов - это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил.

Действие	Описание действия
-F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v]	Задать поле сравнения для правила. Атрибуты поля следующие: *объект*, *операция*, *значение*. Вы можете задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с **-F**. Аудит будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: *равно*, *не равно*, *меньше*, *больше*, *меньше либо равно*, *больше либо равно*, *битовая маска* (**n&v**) и *битовая проверка* (**n&=v**). Битовая проверка выполняет операцию «**and**» над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию «**and**». Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы. Поля сравнения могут быть заданы для следующих объектов: • **a0, a1, a2, a3** - четыре первых аргумента, переданных системному вызову. Строковые аргументы не поддерживаются. Это связано с тем, что ядро должно получать указатель на строку, а проверка поля по значению адреса указателя не желательна. Таким образом, вы должны использовать только цифровые значения. • **arch** - архитектура процессора, на котором выполняется системный вызов. Используйте '**uname -m**', чтобы определить архитектуру. Если вы не знаете архитектуру вашей машины, но хотите использовать таблицу 32-х битных системных вызовов, и ваша машина поддерживает 32 бита, вы можете использовать **b32**. Подобно этому **b64** может быть использовано для использования таблицы 64-х битных системных вызовов. • **auid** - это аббревиатура: *audit uid* - идентификатор пользователя, использованный для входа в систему. • **devmajor** - главный номер устройства (Device Major Number). • **devminor** - вспомогательный номер устройства (Device Minor Number). • **egid** - действительный идентификатор группы; • **euid** - действительный идентификатор пользователя; • **exit** - значение, возвращаемое системным вызовом при выходе; • **fsgid** - идентификатор группы, применяемый к файловой системе; • **fsuid** - идентификатор пользователя, применяемый к файловой системе; • **gid** - идентификатор группы; • **inode** - номер *inode*; • **key** - альтернативный способ установить ключ фильтрации. Смотри выше описание опции **-k**; • **msgtype** - используется для проверки совпадения с числом, описывающим тип сообщения. Может быть использован только в списке **exclude**; • **obj_user** - имя пользователя-владельца ресурса (в контексте SELinux); • **obj_role** - роль ресурса (в контексте SELinux); • **obj_type** - тип ресурса (в контексте SELinux); • **obj_lev_low** - нижний уровень ресурса (в контексте SELinux); • **obj_lev_high** - верхний уровень ресурса (в контексте SELinux); • **path** - полный путь к файлу для точки наблюдения. Смотри ниже описание опции "**-w**". Может быть использован только в списке **exit**; • **perm** - фильтр прав доступа для файловых операций. Смотри выше описание опции "**-p**". Может быть использован только в списке **exit**; • **pers** - персональный номер операционной системы; • **pid** - идентификатор процесса; • **ppid** - идентификатор родительского процесса; • **subj_user** - имя пользователя-владельца процесса (в контексте SELinux); • **subj_role** - роль процесса (в контексте SELinux); • **subj_type** - тип процесса (в контексте SELinux); • **subj_sen** - чувствительность процесса (в контексте SELinux); • **subj_clr** - допуск процесса (в контексте SELinux); • **sgid** - установленный идентификатор группы; • **success** - если значение, возвращаемое системным вызовом, больше либо равно **0**, данный объект будет равен "**true**/**yes**", иначе "**false**/**no**". При создании правила используйте **1** вместо "**true**/**yes**" и **0** вместо "**false**/**no**"; • **suid** - установленный идентификатор пользователя; • **uid** - идентификатор пользователя.
-w *<путь>*	Добавить точку наблюдения за файловым объектом, находящемуся по указанному *пути*. Вы не можете добавлять точку наблюдения к каталогу верхнего уровня - это запрещено ядром. Групповые символы (wildcards) также не могут быть использованы, попытки их использования будут генерировать предупреждающее сообщение. Внутренне точки наблюдения реализованы как слежение за inode. Таким образом, если вы установите точку наблюдения за каталогом, вы увидите файловые события, которые в действительности будут означать обновления метаданных этой inode, и вы можете не увидеть событий, непосредственно связанных с файлами. Если вам необходимо следить за всеми файлами в каталоге, рекомендуется создавать индивидуальную точку наблюдения для каждого файла. В противоположность к правилам аудита системных вызовов, точки наблюдения не оказывают влияния на производительность, связанную с количеством правил посылаемых в ядро.
-W *<путь>*	Удалить точку наблюдения за файловым объектом, находящемуся по указанному *пути*.

Примеры базовых правил и конструкций

ВАЖНО!

Приведенные ниже команды будут выполняться только в ходе работы одного сеанса ОС, если вы хотите сделать это правило постоянным, добавьте его в конец файла **/etc/audit/rules.d/audit.rules** следующим образом:

```
-w /var/log/audit/ -p wra -k auditlog
```

Самоаудит

Отображение успешных и неудачных попыток чтения информации из записей аудита:

```
auditctl -w /var/log/audit/ -p wra -k auditlog
```

Отображение изменения конфигурации аудита, происходящей во время работы функций журналирования:

```
auditctl -w /etc/audit/ -p wra -k auditconfig
auditctl -w /etc/libaudit.conf -p wra -k auditconfig
```

Отслеживание использования инструментов управления аудитом:

```
auditctl -w /sbin/auditctl -p x -k audittools
auditctl -w /sbin/auditd -p x -k audittools
auditctl -w /usr/sbin/auditd -p x -k audittools
auditctl -w /usr/sbin/augenrules -p x -k audittoolss
```

Отслеживание доступа к прочим утилитам службы аудирования:

```
auditctl -a always,exit -F path=/usr/sbin/ausearch -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/aureport -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/aulast -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/aulastlogin -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/auvirt -F perm=x -k auditreport
```

Фильтры

Игнорирование событий **SELinux**:

```
auditctl -a always,exclude -F msgtype=AVC
```

Игнорирование событий с меткой рабочей директории:

```
auditctl -a always,exclude -F msgtype=CWD
```

Игнорирование событий с меткой идентификатора криптографического ключа, используемого в криптографических целях:

```
auditctl -a always,exclude -F msgtype=CRYPTO_KEY_USER
```

Игнорирование событий **cron**:

```
auditctl -a never,user -F subj_type=crond_t
auditctl -a exit,never -F subj_type=crond_t
```

Игнорирование событий **chrony**:

```
auditctl -a never,exit -F arch=b32 -S adjtimex -F auid=unset -F uid=chrony -F subj_type=chronyd_t
auditctl -a never,exit -F arch=b64 -S adjtimex -F auid=unset -F uid=chrony -F subj_type=chronyd_t
```

Игнорирование сообщений, связанных с инструментами виртуальной машины:

```
###Игнорирование ошибок VMware tools

auditctl -a never,exit -F arch=b32 -S fork -F success=0 -F path=/usr/lib/vmware-tools -F subj_type=initrc_t -F exit=-2
auditctl -a never,exit -F arch=b64 -S fork -F success=0 -F path=/usr/lib/vmware-tools -F subj_type=initrc_t -F exit=-2
auditctl -a exit,never -F arch=b32 -S all -F exe=/usr/bin/vmtoolsd
auditctl -a exit,never -F arch=b64 -S all -F exe=/usr/bin/vmtoolsd
```

Фильтр событий большого объема:

```
### Игнорирование событий, связанных с работой shm и lvm

auditctl -a never,exit -F arch=b32 -F dir=/dev/shm -k sharedmemaccess
auditctl -a never,exit -F arch=b64 -F dir=/dev/shm -k sharedmemaccess
auditctl -a never,exit -F arch=b32 -F dir=/var/lock/lvm -k locklvm
auditctl -a never,exit -F arch=b64 -F dir=/var/lock/lvm -k locklvm
```

Игнорирование событий с меткой объекта **FileBeat**:

```
auditctl -a never,exit -F arch=b32 -F path=/opt/filebeat -k filebeat
auditctl -a never,exit -F arch=b64 -F path=/opt/filebeat -k filebeat
```

Базовые правила

Отслеживание изменений параметров **Kernel**:

```
auditctl -w /etc/sysctl.conf -p wa -k sysctl
auditctl -w /etc/sysctl.d -p wa -k sysctl
```

Отслеживание удачной и неудачной загрузки **Kernel module**:

```
auditctl -a always,exit -F perm=x -F auid!=-1 -F path=/sbin/insmod -k modules
auditctl -a always,exit -F perm=x -F auid!=-1 -F path=/sbin/modprobe -k modules
auditctl -a always,exit -F perm=x -F auid!=-1 -F path=/sbin/rmmod -k modules
auditctl -a always,exit -F arch=b64 -S finit_module -S init_module -S delete_module -F auid!=-1 -k modules
auditctl -a always,exit -F arch=b32 -S finit_module -S init_module -S delete_module -F auid!=-1 -k modules
```

Отслеживание изменений конфигурации **Modprobe**:

```
auditctl -w /etc/modprobe.conf -p wa -k modprobe
auditctl -w /etc/modprobe.d -p wa -k modprobe
```

Отслеживание использования **KExec**:

```
auditctl -a always,exit -F arch=b64 -S kexec_load -k KEXEC
auditctl -a always,exit -F arch=b32 -S sys_kexec_load -k KEXEC
```

Отслеживание использования специальных файлов (утилита **mknod**):

```
auditctl -a always,exit -F arch=b32 -S mknod -S mknodat -k specialfiles
auditctl -a always,exit -F arch=b64 -S mknod -S mknodat -k specialfiles
```

Отслеживание использования утилиты **mount**:

```
auditctl -a always,exit -F arch=b64 -S mount -S umount2 -F auid!=-1 -k mount
auditctl -a always,exit -F arch=b32 -S mount -S umount -S umount2 -F auid!=-1 -k mount
```

Отслеживание использования утилиты **swap**:

```
auditctl -a always,exit -F arch=b64 -S swapon -S swapoff -F auid!=-1 -k swap
auditctl -a always,exit -F arch=b32 -S swapon -S swapoff -F auid!=-1 -k swap
```

Отслеживание изменения времени:

```
auditctl -a always,exit -F arch=b32 -F uid!=ntp -S adjtimex -S settimeofday -S clock_settime -k time
auditctl -a always,exit -F arch=b64 -F uid!=ntp -S adjtimex -S settimeofday -S clock_settime -k time
```

Отслеживание изменения локального времени:

```
auditctl -w /etc/localtime -p wa -k localtime
```

Отслеживание использования утилиты **stunnel**:

```
auditctl -w /usr/sbin/stunnel -p x -k stunnel
auditctl -w /usr/bin/stunnel -p x -k stunnel
```

Отслеживание изменения файлов конфигурации **cron** и запланированных заданий:

```
auditctl -w /etc/cron.allow -p wa -k cron
auditctl -w /etc/cron.deny -p wa -k cron
auditctl -w /etc/cron.d/ -p wa -k cron
auditctl -w /etc/cron.daily/ -p wa -k cron
```

```
auditctl -w /etc/cron.hourly/ -p wa -k cron
auditctl -w /etc/cron.monthly/ -p wa -k cron
auditctl -w /etc/cron.weekly/ -p wa -k cron
auditctl -w /etc/crontab -p wa -k cron
auditctl -w /var/spool/cron/ -k cron
```

Отслеживание изменения баз пользователей, групп, паролей:

```
auditctl -w /etc/group -p wa -k etcgroup
auditctl -w /etc/passwd -p wa -k etcpasswd
auditctl -w /etc/gshadow -k etcgroup
auditctl -w /etc/shadow -k etcpasswd
auditctl -w /etc/security/opasswd -k opasswd
```

Отслеживание изменения файлов **sudo**:

```
auditctl -w /etc/sudoers -p wa -k actions
auditctl -w /etc/sudoers.d/ -p wa -k actions
```

Отслеживание использования **passwd**:

```
auditctl -w /usr/bin/passwd -p x -k passwd_modification
```

Отслеживание использования инструментов изменения идентификаторов группы:

```
auditctl -w /usr/sbin/groupadd -p x -k group_modification
auditctl -w /usr/sbin/groupmod -p x -k group_modification
auditctl -w /usr/sbin/addgroup -p x -k group_modification
auditctl -w /usr/sbin/useradd -p x -k user_modification
auditctl -w /usr/sbin/userdel -p x -k user_modification
auditctl -w /usr/sbin/usermod -p x -k user_modification
auditctl -w /usr/sbin/adduser -p x -k user_modification
```

Отслеживание изменения информации и конфигурации **login**:

```
auditctl -w /etc/login.defs -p wa -k login
auditctl -w /etc/securetty -p wa -k login
auditctl -w /var/log/faillog -p wa -k login
auditctl -w /var/log/lastlog -p wa -k login
auditctl -w /var/log/tallylog -p wa -k login
```

Правила сетевого окружения

Отслеживание изменения **hostname**:

```
auditctl -a always,exit -F arch=b32 -S sethostname -S setdomainname -k network_modifications
auditctl -a always,exit -F arch=b64 -S sethostname -S setdomainname -k network_modifications
```

Отслеживание удачных попыток подключения **IPv4**:

```
auditctl -a always,exit -F arch=b64 -S connect -F a2=16 -F success=1 -F key=network_connect_4
auditctl -a always,exit -F arch=b32 -S connect -F a2=16 -F success=1 -F key=network_connect_4
```

Отслеживание удачных попыток подключения **IPv6**:

```
auditctl -a always,exit -F arch=b64 -S connect -F a2=28 -F success=1 -F key=network_connect_6
auditctl -a always,exit -F arch=b32 -S connect -F a2=28 -F success=1 -F key=network_connect_6
```

Отслеживание изменения файлов конфигурации сетевых настроек:

```
auditctl -w /etc/hosts -p wa -k network_modifications
auditctl -w /etc/sysconfig/network -p wa -k network_modifications
auditctl -w /etc/sysconfig/network-scripts -p w -k network_modifications
auditctl -w /etc/network/ -p wa -k network
auditctl -a always,exit -F dir=/etc/NetworkManager/ -F perm=wa -k network_modifications
```

Отслеживание изменения файлов **issue**:

```
auditctl -w /etc/issue -p wa -k etcissue
auditctl -w /etc/issue.net -p wa -k etcissue
```

Отслеживание изменения скриптов при запуске ОС:

```
auditctl -w /etc/inittab -p wa -k init
auditctl -w /etc/init.d/ -p wa -k init
auditctl -w /etc/init/ -p wa -k init
```

Отслеживание изменения файлов **libpath**:

```
auditctl -w /etc/ld.so.conf -p wa -k libpath
auditctl -w /etc/ld.so.conf.d -p wa -k libpath
```

Отслеживание изменения предварительной загрузки общесистемной библиотеки (**LD_PRELOAD**):

```
auditctl -w /etc/ld.so.preload -p wa -k systemwide_preloads
```

Отслеживание изменения конфигурации **PAM** и связанных с ним файлов:

```
auditctl -w /etc/pam.d/ -p wa -k pam
auditctl -w /etc/security/limits.conf -p wa -k pam
auditctl -w /etc/security/limits.d -p wa -k pam
auditctl -w /etc/security/pam_env.conf -p wa -k pam
auditctl -w /etc/security/namespace.conf -p wa -k pam
auditctl -w /etc/security/namespace.d -p wa -k pam
auditctl -w /etc/security/namespace.init -p wa -k pam
```

Отслеживание изменения конфигурации **mail**:

```
auditctl -w /etc/aliases -p wa -k mail
auditctl -w /etc/postfix/ -p wa -k mail
auditctl -w /etc/exim4/ -p wa -k mail
```

Отслеживание изменения конфигурации **ssh**:

```
auditctl -w /etc/ssh/sshd_config -k sshd
auditctl -w /etc/ssh/sshd_config.d -k sshd
```

Отслеживание изменения подделки ключа **ssh**:

```
auditctl -w /root/.ssh -p wa -k rootkey
```

Правила служб

Отслеживание изменения и использования файлов **systemd**:

```
auditctl -w /bin/systemctl -p x -k systemd
auditctl -w /etc/systemd/ -p wa -k systemd
auditctl -w /usr/lib/systemd -p wa -k systemd
```

Отслеживание событий **SELinux**, которые изменяют систему мандатного управления доступом:

```
auditctl -w /etc/selinux/ -p wa -k mac_policy
```

Отслеживание событий сбоя доступа к критическим элементам:

```
auditctl -a always,exit -F arch=b64 -S open -F dir=/etc -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/bin -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/sbin -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/usr/bin -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/usr/sbin -F success=0 -k unauthedfileaccess
```

```
auditctl -a always,exit -F arch=b64 -S open -F dir=/var -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/home -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/srv -F success=0 -k unauthedfileaccess
```

Отслеживание использования приложений для изменения идентификатора процесса (переключение учетных записей):

```
auditctl -w /bin/su -p x -k priv_esc
auditctl -w /usr/bin/sudo -p x -k priv_esc
auditctl -w /etc/sudoers -p rw -k priv_esc
auditctl -w /etc/sudoers.d -p rw -k priv_esc
```

Отслеживание использования приложений, изменяющих состояние питания:

```
auditctl -w /sbin/shutdown -p x -k power
auditctl -w /sbin/poweroff -p x -k power
auditctl -w /sbin/reboot -p x -k power
auditctl -w /sbin/halt -p x -k power
```

Отслеживание изменения информации об инициации сеанса:

```
auditctl -w /var/run/utmp -p wa -k session
auditctl -w /var/log/btmp -p wa -k session
auditctl -w /var/log/wtmp -p wa -k session
```

Отслеживание модификации дискреционного контроля доступа:

```
auditctl -a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=-1 -k perm_mod
```

Специальные правила

Отслеживание запросов на получение информации о пользователе:

```
auditctl -w /usr/bin/whoami -p x -k recon
auditctl -w /usr/bin/id -p x -k recon
auditctl -w /bin/hostname -p x -k recon
auditctl -w /bin/uname -p x -k recon
auditctl -w /etc/issue -p r -k recon
auditctl -w /etc/hostname -p r -k recon
```

Отслеживание подозрительной деятельности:

```
### Подразумевается, что использование специализированных утилит, связанных с работой с/в
```

```
### внутренней/внешней сетью, может быть отслежено и зажурналировано.
auditctl -w /usr/bin/wget -p x -k susp_activity
auditctl -w /usr/bin/curl -p x -k susp_activity
auditctl -w /usr/bin/base64 -p x -k susp_activity
auditctl -w /bin/nc -p x -k susp_activity
auditctl -w /bin/netcat -p x -k susp_activity
auditctl -w /usr/bin/ncat -p x -k susp_activity
auditctl -w /usr/bin/ss -p x -k susp_activity
auditctl -w /usr/bin/netstat -p x -k susp_activity
auditctl -w /usr/bin/ssh -p x -k susp_activity
auditctl -w /usr/bin/scp -p x -k susp_activity
auditctl -w /usr/bin/sftp -p x -k susp_activity
auditctl -w /usr/bin/ftp -p x -k susp_activity
auditctl -w /usr/bin/socat -p x -k susp_activity
auditctl -w /usr/bin/wireshark -p x -k susp_activity
auditctl -w /usr/bin/tshark -p x -k susp_activity
auditctl -w /usr/bin/rawshark -p x -k susp_activity
auditctl -w /usr/bin/rdesktop -p x -k Remote_Access_Tools
auditctl -w /usr/local/bin/rdesktop -p x -k Remote_Access_Tools
auditctl -w /usr/bin/wlfreerdp -p x -k susp_activity
auditctl -w /usr/bin/xfreerdp -p x -k Remote_Access_Tools
auditctl -w /usr/local/bin/xfreerdp -p x -k Remote_Access_Tools
auditctl -w /usr/bin/nmap -p x -k susp_activity
```

Отслеживание использования утилит архивации и сжатия данных:

```
auditctl -w /usr/bin/zip -p x -k Data_Compressed
auditctl -w /usr/bin/gzip -p x -k Data_Compressed
auditctl -w /usr/bin/tar -p x -k Data_Compressed
auditctl -w /usr/bin/bzip2 -p x -k Data_Compressed
auditctl -w /usr/bin/lzip -p x -k Data_Compressed
auditctl -w /usr/local/bin/lzip -p x -k Data_Compressed
auditctl -w /usr/bin/lz4 -p x -k Data_Compressed
auditctl -w /usr/local/bin/lz4 -p x -k Data_Compressed
auditctl -w /usr/bin/lzop -p x -k Data_Compressed
auditctl -w /usr/local/bin/lzop -p x -k Data_Compressed
auditctl -w /usr/bin/plzip -p x -k Data_Compressed
auditctl -w /usr/local/bin/plzip -p x -k Data_Compressed
auditctl -w /usr/bin/pbzip2 -p x -k Data_Compressed
auditctl -w /usr/local/bin/pbzip2 -p x -k Data_Compressed
auditctl -w /usr/bin/lbzip2 -p x -k Data_Compressed
auditctl -w /usr/local/bin/lbzip2 -p x -k Data_Compressed
auditctl -w /usr/bin/pixz -p x -k Data_Compressed
auditctl -w /usr/local/bin/pixz -p x -k Data_Compressed
auditctl -w /usr/bin/pigz -p x -k Data_Compressed
auditctl -w /usr/local/bin/pigz -p x -k Data_Compressed
auditctl -w /usr/bin/unpigz -p x -k Data_Compressed
auditctl -w /usr/local/bin/unpigz -p x -k Data_Compressed
auditctl -w /usr/bin/zstd -p x -k Data_Compressed
auditctl -w /usr/local/bin/zstd -p x -k Data_Compressed
```

Отслеживание подозрительной активности в **sbin**:

```
### Подразумевается, что использование специализированных утилит  может быть отслежено и
### зажурналировано.
auditctl -w /sbin/iptables -p x -k sbin_susp
auditctl -w /sbin/ip6tables -p x -k sbin_susp
auditctl -w /sbin/ifconfig -p x -k sbin_susp
auditctl -w /usr/sbin/arptables -p x -k sbin_susp
auditctl -w /usr/sbin/ebtables -p x -k sbin_susp
auditctl -w /sbin/xtables-nft-multi -p x -k sbin_susp
auditctl -w /usr/sbin/nft -p x -k sbin_susp
auditctl -w /usr/sbin/tcpdump -p x -k sbin_susp
auditctl -w /usr/sbin/traceroute -p x -k sbin_susp
auditctl -w /usr/sbin/ufw -p x -k sbin_susp
```

Отслеживание отправки вызовов **dbus**:

```
### Может указывать на повышение привилегий CVE-2021-3560
auditctl -w /usr/bin/dbus-send -p x -k dbus_send
auditctl -w /usr/bin/gdbus -p x -k gdubs_call
```

Отслеживание вызовов **pkexec**:

```
### Может указывать на повышение привилегий CVE-2021-4034
auditctl -w /usr/bin/pkexec -p x -k pkexec
```

Отслеживание подозрительной активности, связанной с **shell**:

```
auditctl -w /bin/ash -p x -k susp_shell
auditctl -w /bin/bash -p x -k susp_shell
auditctl -w /bin/csh -p x -k susp_shell
auditctl -w /bin/dash -p x -k susp_shell
auditctl -w /bin/busybox -p x -k susp_shell
auditctl -w /bin/ksh -p x -k susp_shell
auditctl -w /bin/fish -p x -k susp_shell
auditctl -w /bin/tcsh -p x -k susp_shell
auditctl -w /bin/tclsh -p x -k susp_shell
auditctl -w /bin/zsh -p x -k susp_shell
auditctl -w /bin/xonsh -p x -k susp_shell
auditctl -w /usr/local/bin/xonsh -p x -k susp_shell
auditctl -w /bin/open -p x -k susp_shell
auditctl -w /bin/sh -p x -k susp_shell
auditctl -w /bin/rbash -p x -k susp_shell
```

Отслеживание изменения конфигурации **Shell/profile configurations**:

```
auditctl -w /etc/profile.d/ -p wa -k shell_profiles
auditctl -w /etc/profile -p wa -k shell_profiles
auditctl -w /etc/shells -p wa -k shell_profiles
auditctl -w /etc/bashrc -p wa -k shell_profiles
auditctl -w /etc/csh.cshrc -p wa -k shell_profiles
auditctl -w /etc/csh.login -p wa -k shell_profiles
auditctl -w /etc/fish/ -p wa -k shell_profiles
auditctl -w /etc/zsh/ -p wa -k shell_profiles
```

Отслеживание злоупотребления привилегиями:

```
### Целью этого правила является обнаружение случаев, когда администратор злоупотребляет полномочиями,
### путем просмотра домашнего каталога пользователя.
auditctl -a always,exit -F dir=/home -F uid=0 -F auid>=1000 -F auid!=-1 -C auid!=obj_uid -k power_abuse
```

Отслеживание создания сокетов:

```
### Отслеживает как IPv4, так и IPv6
auditctl -a always,exit -F arch=b32 -S socket -F a0=2  -k Exfiltration_Over_Other_Network_Medium
auditctl -a always,exit -F arch=b64 -S socket -F a0=2  -k Exfiltration_Over_Other_Network_Medium
auditctl -a always,exit -F arch=b32 -S socket -F a0=10 -k Exfiltration_Over_Other_Network_Medium
auditctl -a always,exit -F arch=b64 -S socket -F a0=10 -k Exfiltration_Over_Other_Network_Medium
```

Отслеживание создания анонимного файла:

```
### Эти правила следят за использованием memfd_create, "memfd_create" создает анонимный файл и возвращает
### дескриптор файла для доступа к нему
auditctl -a always,exit -F arch=b64 -S memfd_create -F key=anon_file_create
auditctl -a always,exit -F arch=b32 -S memfd_create -F key=anon_file_create
```

Правила управления ПО

Отслеживание использования **rpm/yum**:

```
auditctl -w /usr/bin/rpm -p x -k software_mgmt
auditctl -w /usr/bin/yum -p x -k software_mgmt
```

Отслеживание использования **dnf**:

```
auditctl -w /usr/bin/dnf -p x -k software_mgmt
```

Отслеживание использования **pip**:

```
auditctl -w /usr/bin/pip -p x -k third_party_software
auditctl -w /usr/local/bin/pip -p x -k third_party_software
auditctl -w /usr/bin/pip3 -p x -k third_party_software
auditctl -w /usr/local/bin/pip3 -p x -k third_party_software
```

Отслеживание использования **npm**:

```
auditctl -w /usr/bin/npm -p x -k third_party_software
```

Отслеживание использования **CPAN** (*Comprehensive Perl Archive Network*):

```
auditctl -w /usr/bin/cpan -p x -k third_party_software
```

Отслеживание использования **ruby** (*RubyGems*):

```
auditctl -w /usr/bin/gem -p x -k third_party_software
```

Отслеживание использования **Lua**:

```
auditctl -w /usr/bin/luarocks -p x -k third_party_software
```

Правила управления специальным ПО

Отслеживание изменений файлов **puppet**:

```
auditctl -w /etc/puppet/ssl -p wa -k puppet_ssl
```

Отслеживание изменений файлов **chef**:

```
auditctl -w /etc/chef -p wa -k soft_chef
```

Отслеживание изменений файлов **otter**:

```
auditctl -w /etc/otter -p wa -k soft_otter
```

Отслеживание использования утилиты **grep**:

```
auditctl -w /usr/bin/grep -p x -k T1081_Credentials_In_Files
auditctl -w /usr/bin/egrep -p x -k T1081_Credentials_In_Files
auditctl -w /usr/bin/ugrep -p x -k T1081_Credentials_In_Files
```

Отслеживание использования и изменения файлов конфигурации **docker**:

```
auditctl -w /usr/bin/dockerd -k docker
auditctl -w /usr/bin/docker -k docker
auditctl -w /usr/bin/docker-containerd -k docker
auditctl -w /usr/bin/docker-runc -k docker
auditctl -w /var/lib/docker -k docker
auditctl -w /etc/docker -k docker
auditctl -w /etc/sysconfig/docker -k docker
auditctl -w /etc/sysconfig/docker-storage -k docker
auditctl -w /usr/lib/systemd/system/docker.service -k docker
auditctl -w /usr/lib/systemd/system/docker.socket -k docker
```

Отслеживание использования систем виртуализации:

```
auditctl -w /usr/bin/qemu-system-x86_64 -p x -k qemu-system-x86_64
auditctl -w /usr/bin/qemu-img -p x -k qemu-img
auditctl -w /usr/bin/qemu-kvm -p x -k qemu-kvm
auditctl -w /usr/bin/qemu -p x -k qemu
auditctl -w /usr/bin/virtualbox -p x -k virtualbox
```

```
auditctl -w /usr/bin/virt-manager -p x -k virt-manager
auditctl -w /usr/bin/VBoxManage -p x -k VBoxManage
```

Отслеживание использования утилиты **kubelet** (*Kubernetes*):

```
auditctl -w /usr/bin/kubelet -k kubelet
```

«Тяжелые» события

> **Примечание.**
>
> Правила, представленные ниже, требуют большого объема свободного пространства в среде.

Отслеживание применения команд с правами пользователя **root**:

```
auditctl -a always,exit -F arch=b64 -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k rootcmd
auditctl -a always,exit -F arch=b32 -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k rootcmd
```

Отслеживание события удаления файлов пользователем:

```
auditctl -a always,exit -F arch=b32 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=-1 -k delete
auditctl -a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=-1 -k delete
```

Отслеживание события неудачного доступа к файлу:

```
auditctl -a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
auditctl -a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access
auditctl -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
auditctl -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access
```

Отслеживание события неудачного создания:

```
auditctl -a always,exit -F arch=b32 -S creat,link,mknod,mkdir,symlink,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
auditctl -a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
auditctl -a always,exit -F arch=b32 -S link,mkdir,symlink,mkdirat -F exit=-EPERM -k file_creation
auditctl -a always,exit -F arch=b64 -S mkdir,link,symlink,mkdirat -F exit=-EPERM -k file_creation
```

Отслеживание события неудачной модификации:

```
auditctl -a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
auditctl -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
auditctl -a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
auditctl -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
```

Отслеживание события использования 32-битного API для 64-битной системы:

```
### Это правило обнаружит любое использование 32-битных системных вызовов, потому как это может быть
### признаком использования уязвимости 32-битного API.
auditctl -a always,exit -F arch=b32 -S all -k 32bit_api
```

Утилита aureport

Утилита **aureport** - это инструмент, который генерирует итоговые отчеты на основе логов службы аудита. **aureport** может также принимать данные со стандартного ввода (*stdin*) до тех пор, пока на входе будут необработанные данные логов. В шапке каждого

отчета для каждого столбца есть заголовок - это облегчает понимание данных. Все отчеты, кроме основного итогового отчета, содержат номера событий аудита. Используя их, вы можете найти полные данные о событии с помощью **ausearch -a** . Если в отчете слишком много данных, можно задать время начала и время окончания для уточнения временного промежутка. Отчеты, генерируемые **aureport**, могут быть использованы как исходный материал для получения более развернутых отчетов.

Опции:

Опция	Значение опции
-au, --auth	Отчет обо всех попытках аутентификации.
-a, --avc	Отчет обо всех avc сообщениях.
-c, --config	Отчет об изменениях конфигурации.
-cr, --crypto	Отчет о событиях, связанных с шифрованием.
-e, --event	Отчет о событиях.
-f, --file	Отчет о файлах.
--failed	Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются и удачные, и неудачные события.
-h, --host	Отчет о хостах.
-i, --interpret	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен aureport. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, --input файл	Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-l, --login	Отчет о попытках входа в систему.
-m, --mods	Отчет об изменениях пользовательских учетных записей.
-ma, --mac	Отчет о событиях в системе, обеспечивающей мандатное управление доступом - Mandatory Access Control (MAC).
-p, --pid	Отчет о процессах.
-r, --response	Отчет о реакциях на аномальные события.
-s, --syscall	Отчеты о системных вызовах.
--success	Для обработки в отчетах выбирать только удачные события. По умолчанию показываются и удачные, и неудачные события.
--summary	Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете. Такой режим есть не у всех отчетов.
-t, --log	Этот параметр генерирует отчет о временных рамках каждого отчета.
-te, --end	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается текущий момент (now). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, --terminal	Отчет о терминалах.
-ts, --start	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается полночь (midnight). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-u, --user	Отчет о пользователях.
-v, --version	Вывести версию программы и выйти.

Утилита ausearch

Программа **ausearch** является инструментом поиска по журналу аудита. Утилита **ausearch** может также принимать данные со стандартного ввода (*stdin*) до тех пор, пока на входе будут необработанные данные логов. Все условия, указанные в параметрах, объединяются логическим «**И**». К примеру, при указании **- m** и **-ui** в качестве параметров будут показаны события, соответствующие заданному типу и идентификатору пользователя.

Стоит отметить, что каждый системный вызов ядра из пользовательского пространства и возвращение данных в пользовательское

пространство имеет один уникальный (для каждого системного вызова) идентификатор события.

Различные части ядра могут добавлять дополнительные записи. Например, в событие аудита для системного вызова «**open**» добавляется запись *PATH* с именем файла. **ausearch** показывает все записи события вместе. Это означает, что при запросе определенных записей результат может содержать записи *SYSCALL*.

Также помните, что не все типы записей содержат указанную информацию. Например, запись *PATH* не содержит имя узла или *loginuid*.

Опции:

Опция	Значение опции
-a, --event audit-event-id	Искать события с заданным идентификатором события. Сообщения обычно начинаются примерно так: msg=audit(1116360555.329:2401771). Идентификатор события - это число после «:». Все события аудита, связанные с одним системным вызовом имеют одинаковый идентификатор.
-c, --comm comm-name	Искать события с заданным comm name. comm name - имя исполняемого файла задачи.
-f, --file file-name	Искать события с заданным именем файла.
-ga, --gid-all all-group-id	Искать события с заданным эффективным или обычным идентификатором группы.
-ge, --gid-effective effective-group-id	Искать события с заданным эффективным идентификатором группы или именем группы.
-gi, --gidgroup-id	Искать события с заданным идентификатором группы или именем группы.
-h, --help	Справка.
-hn, --host host-name	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен ausearch. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, --input file-name	Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-k, --key key-string	Искать события с заданным ключевым словом.
-m, --message message-type | comma-sep-message-type-list	Искать события с заданным типом. Вы можете указать список значений, разделенных запятыми. Можно указать несуществующий в событиях тип ALL, который позволяет получить все сообщения системы аудита. Список допустимых типов большой и будет показан, если указать эту опцию без значения. Тип сообщения может быть строкой или числом. В списке значений этого параметра в качестве разделителя используются запятые и пробелы недопустимы.
-o, --object SE-Linux-context-string	Искать события с заданным контекстом (объектом).
-p, --pid process-id	Искать события с заданным идентификатором процесса.
-pp, --ppid parent-process-id	Искать события с заданным идентификатором родительского процесса.
-r, --raw	Необработанный вывод. Используется для извлечения записей для дальнейшего анализа.
-sc, --success syscall-name-or-value	Искать события с заданным системным вызовом. Вы можете указать его номер или имя. Если вы указали имя, оно будет проверено на машине, где запущен ausearch.
-se, --context SE-Linux-context-string	Искать события с заданным контекстом SELinux (stcontext/subject или tcontext/object).
-su, --subject SE-Linux-context-string	Искать события с заданным контекстом SELinux - scontext (subject).
-sv, --success success-value	Искать события с заданным флагом успешного выполнения. Допустимые значения: yes (успешно) и no(неудачно).
-te, --end [end-date] [end-time]	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается текущий момент (now). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. localtime). this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-ts, --start [start-date] [start-time]	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается полночь (midnight). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, --terminal terminal	Искать события с заданным терминалом. Некоторые службы (такие как cron и atd) используют имя службы как имя терминала.
-ua, --uid-all all-user-id	Искать события, у которых любой из идентификатора пользователя, эффективного идентификатора пользователя или loginuid (auid) совпадают с заданным идентификатором пользователя.

Опция	Значение опции
-ue, --uid-effective effective-user-id	Искать события с заданным эффективным идентификатором пользователя.
-ui, --uid user-id	Искать события с заданным идентификатором пользователя.
-ul, --loginuid login-id	Искать события с заданным идентификатором пользователя. Все программы, которые его используют, должны использовать pam_loginuid.
-v, --verbose	Показать версию и выйти.
-w, --word	Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux.
-x, --executable executable	Искать события с заданным именем исполняемой программы.

Утилита autrace

Утилита **autrace** - это программа, которая добавляет правила аудита для того, чтобы следить за использованием системных вызовов в указанном процессе подобно тому, как это делает **strace**. После добавления правил она запускает процесс с указанными аргументами. Результаты аудита будут либо в логах аудита (если служба аудита запущена), либо в системных логах. Внутри **autrace** устроена так, что удаляет все предыдущие правила аудита, перед тем как запустить указанный процесс и после его завершения. Поэтому, в качестве дополнительной меры предосторожности, программа не запустится, если перед ее использованием правила не будут удалены с помощью **audtictl** - предупреждающее сообщение известит об этом.

Опции:

Опция	Значение опции
-r	Ограничить сбор информации о системных вызовах только теми, которые необходимы для анализа использования ресурсов. Это может быть полезно при моделировании внештатных ситуаций, к тому же позволяет уменьшить нагрузку на логи.

Примеры:

Ниже представлен пример обычного использования программы:

```
autrace /bin/ls /tmp
ausearch --start recent -p 2442 -i
```

Еще один пример для режима ограниченного сбора информации:

```
autrace -r /bin/ls
ausearch --start recent -p 2450 --raw | aureport --file –summary
ausearch --start recent -p 2450 --raw | aureport --host –summary
```

Контроль целостности системы

Описание утилиты
Контроль целостности ОС

Описание утилиты

Afick - это быстрая и доступная утилита, помогающая при обнаружении вторжений, а также позволяющая контролировать общую целостность системы.

Afick контролирует изменения в файловой системе и сразу сообщает вам о них, таким образом, предоставляя вам выбор решить, действительно ли ожидались эти изменения. Эта информация может помочь вам в расследовании инцидента, когда необходимо определить, какие были произведены изменения в системе в результате взлома.

Вы можете подробнее ознакомиться с информацией о работе с утилитой контроля целостности, просмотрев наши обучающие видео:

- на **RuTube** — Контроль целостности сертифицированной ОС. Afick;
- в **Яндекс.Дзен** — Контроль целостности сертифицированной ОС. Afick;
- в **VK Видео** — Контроль целостности сертифицированной ОС. Afick.

На наших каналах вы также сможете найти много другой полезной информации.

В процессе установки Afick формирует базу данных файлов, каталогов и соответствующих им MD5 контрольных сумм. Файлы и каталоги, включенные в эту базу данных, выбираются соответственно входным данным из файла конфигурации Afick, называемого **afick.conf**, после того, как Afick установит этот файл в /etc каталог. Файл конфигурации afick.conf имеет простую синтаксическую структуру. По вашему усмотрению Вы можете очень быстро добавить или удалить типы файлов, каталоги, и т.д. Ниже приведено содержимое файла afick.conf. Обратите внимание, что элементы в файле конфигурации чувствительны к регистру.

```
# afick config sample file
# directives
############
database:=/var/lib/afick/afick - Определяет какую базу данных будет использовать Afick
# report_url := stdout - Определяет куда Afick будет выводить результаты своей работы
# verbose := no
# warn_dead_symlinks := no
# report_full_newdel := no
# warn_missing_file := no
# running_files := no
# timing := no
# text files
exclude_suffix := log LOG html htm HTM txt TXT xml - Определяет, что Afick должен игнорировать текстовые файлы с такими
расширениями.
# help files
exclude_suffix := hlp pod chm - Определяет, что Afick должен игнорировать файлы справки с такими расширениями
# old files
exclude_suffix := tmp old bak - Определяет, что Afick должен игнорировать временные файлы с такими расширениями
# fonts
exclude_suffix := fon ttf TTF - Определяет, что Afick должен игнорировать файлы шрифтов с такими расширениями
# images
exclude_suffix := bmp BMP jpg JPG gif png ico - Определяет, что Afick должен игнорировать файлы изображений с такими
расширениями
# audio
exclude_suffix := wav WAV mp3 avi - Определяет, что Afick должен игнорировать медиа файлы с такими расширениями
# macros
########
# used by cron
@@define MAILTO root - Определяет пользователя, которому будут отсылаться отчеты по работе Afick.
@@define LINES 1000 - Определяет максимальное количество строк в отчете
# list the file or directories to scan
# syntaxe :
# file action
# to have action on file (see below
# ! file
# to remove file from scan
# file with blank character have to be quoted
# action : a list of item to check - Ниже описаны опции, определяющие какие атрибуты файлов нужно контролировать.
# md5 : md5 checksum
# d : device
# i : inode
# p : permissions
```

```
# n : number of links
# u : user
# g : group
# s : size
# b : number of blocks
# m : mtime
# c : ctime
# a : atime
#R: p+d+i+n+u+g+s+m+c+md5
#L: p+d+i+n+u+g
# action alias may be configured with
# your_alias = another_alias|item[+item][-item]
# all is a pre-defined alias for all items except "a"
# alias :
#########
DIR = p+i+n+u+g
ETC = p+d+i+u+g+s+md5
Logs = p+n+u+
MyRule = p+d+i+n+u+g+s+b+md5+m .
# files to scan
###############
=/ DIR - Проверка с использованием описанных выше правил для каталогов
#
/bin MyRule
/boot MyRule
!/boot/map - Игнорируется указанный каталог.
!/boot/System.map - Игнорируется указанный файл
/etc ETC
/etc/mtab ETC - i
/etc/adjtime ETC - md5
/etc/aliases.db ETC - md5
/etc/mail/statistics ETC - md5
!/etc/map
!/etc/webmin/sysstats/modules/
!/etc/cups/certs/0
/lib MyRule
/lib/modules MyRule -m
/root MyRule
!/root/.viminfo
!/root/.bash_history
!/root/.mc
/sbin MyRule
/usr/bin MyRule
/usr/sbin MyRule
/usr/lib MyRule
/usr/local/bin MyRule
/usr/local/sbin MyRule
/usr/local/lib MyRule
/var/ftp MyRule
/var/log Logs
/var/www MyRule
```

Как видно, файл конфигурации Afick довольно прост для понимания. Ниже приведен пример, в котором к проверке целостности Afick добавляется ваш основной каталог. К примеру, вам необходимо, чтобы файлы в этом каталоге проверялись на изменения при монопольном доступе, изменение прав доступа, изменения размера файлов и времени последнего обращения к файлу. Для начала нужно создать новый элемент, под разделом **#alias** в файле конфигурации afick.conf, как показано ниже:

```
HOME = u+g+p+m+s
```

Затем в разделе **#files to scan** необходимо добавить следующую строку:

```
/home/yourusername HOME
```

Теперь, при следующем запуске, Afick добавит ваш каталог в свою базу данных и будет контролировать находящиеся в нем файлы, согласно указанным вами критериям. Если вы хотите, чтобы ваши изменения применились немедленно, то можно запустить Afick вручную, используя следующую команду:

```
afick --update
```

Иначе, вам придется ждать запуска крон задачи Afick. Эта задача добавляется автоматически во время инсталляции программы и запускается один раз в день. Результаты работы данного задания вы получите по электронной почте на адрес, указанный в разделе

MAILTO файла конфигурации **afick.conf**. Используя почтового клиента, вы сможете увидеть ежедневный отчет примерно в таком виде:

```
This is an automated report generated by Another File Integrity Checker on
+localhost.localdomain at 07:46:07 AM on 02/25/2004.
Output of the daily afick run:
new file : /var/log/afick/afick.log.2
new file : /var/log/afick/error.log.2
deleted file : /etc/sysconfig/iptables
changed file : /etc/adjtime
changed file : /etc/aliases.db
changed file : /etc/mail/statistics
changed file : /etc/prelink.cache
changed file : /etc/printcap
detailed changes
changed file : /etc/adjtime
MD5 : 7+bTDZQbxsTXEJXhyI2GCw ao6a/yDwoBR8GSL1AKlWXQ
changed file : /etc/aliases.db
MD5 :GT/eP5D+B8apNoa7L5CLRw soh7MnLDuQw4gI9KHlhpTA
changed file : /etc/mail/statistics
MD5 :oshq17jZ2a0o5pYhVBRgwQ vb69gMWXvpIEEZ4fmOl9/Q
changed file : /etc/prelink.cache
MD5 : SKh/403FRMUqBNdCIInQ9A zeC+5EPFfWBR4OeT7xZdbw
changed file : /etc/printcap
MD5 : b5e3g2//bGaxeCxVyRJqaw QFY1NJGy/kdt32B1YV0TXQ
filesize : 194 581
```

В примере выше Afick сообщает нам, что некоторые файлы были изменены, созданы или удалены. Также нам показываются начальные и текущие контрольные суммы файлов, и сообщается, что в одном из файлов был изменен его размер. Afick узнает об происходящих изменениях в файле, сравнивая его атрибуты с атрибутами, которые были сохранены при последнем запуске Afick. Примером этого могут служить файлы в папке **/usr/bin** или в **/sbin**. Обычно эти файлы редко изменяются, если только вы не изменили их, обновляя программу (в противном случае они не должны изменяться).

Обратите внимание на то, где вы сохраняете вашу базу данных Afick (по умолчанию - **/var/lib/afick/**), потому что может возникнуть ситуация, когда ваша система была взломана, а вы об этом не узнаете, т.к. была нарушена целостность базы данных. Возможным решением данного вопроса может быть сохранение базы на защищенных от записи носителях (например, CD-ROM), после чего изменить файл конфигурации afick.conf, чтобы указать на выбранное вами место сохранения базы.

Контроль целостности ОС

Для **сертифицированной редакции** в состав репозитория ОС включена база данных утилиты контроля целостности afick, которая содержит перечень контролируемых бинарных исполняемых файлов изделия, согласно документации на изделие. Для самостоятельной проверки целостности ОС необходимо сделать следующее:

1. Установить утилиту afick и базу данных:

```
dnf install afick redos-afick-dbЗагружены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
...
Установлено:
  afick.noarch 0:3.5.2-1.el7                redos-afick-db.x86_64 0:7.2-3
Выполнено!
```

2. После успешной установки запустить проверку файлов ОС командой:

```
afick -k

...
new file : /var/lib/afick/redos/redos.ctr
new file : /var/lib/afick/redos/redos.db
deleted file : /lib/modules/4.19.79-1.el7.x86_64.debug/kernel/arch/x86/crypto/aegis128-aesni.ko
...
deleted file : /var/lib/afick/afick.db
 parent_date   : Fri Apr 24 09:17:05 2020
changed file : /etc/afick.conf
 md5          : 03bf42d0327b3f2fe195d0eca359b1ec addfc78d955141718f78df7587ae3ceb
 filemode     : 100600 100644
 filesize     : 924772 924774
# Hash database : 6793 files scanned, 6320 changed (new : 2; delete : 6317; changed : 1; dangling : 0; exclude_suffix : 0; exclude_prefix : 0;
```

```
exclude_re : 0; degraded : 3)
# ###################################################################
# MD5 hash of /var/lib/afick/redos/redos => oRTAm4SAHdk9vwSktXz88A
# user time : 12.73; system time : 3.14; real time : 27
```

3. После завершения проверки проанализировать полученные данные.

Новые файлы можно не принимать во внимание.

```
new : 2
```

Удалённые файлы в отчете можно не учитывать — это объясняется тем, что БД afick снимается для всех контролируемых файлов, а в используемом экземпляре ОС могут использоваться не все пакеты.

```
delete : 6317
```

Интерес в первую очередь представляют изменённые файлы.

```
changed : 1
```

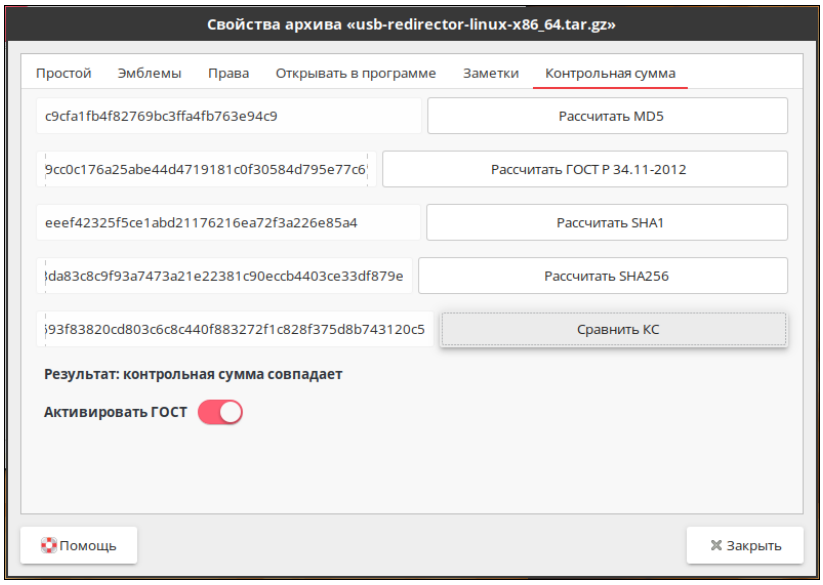
Необходимо просмотреть подробный отчёт в выводе утилиты выше и оценить, допустимы ли данные изменения файлов.

```
changed file : /etc/afick.conf
 md5          : 03bf42d0327b3f2fe195d0eca359b1ec addfc78d955141718f78df7587ae3ceb
 filemode     : 100600 100644
 filesize     : 924772 924774
```

В рассматриваемом примере был изменен конфигурационный файл утилиты afick. Это можно считать допустимым изменением, так как на эталонной ОС конфигурация afick по умолчанию не настроена. Скачанный конфигурационный файл, содержащийся в пакете БД afick, заменил файл, поставляемый с утилитой. Других изменений в системе нет, значит, можно сделать вывод о целостности ОС.

Расчет контрольных сумм файлов

Для расчета и сравнения контрольных сумм файлов необходимо нажать ПКМ на файл, выбрать пункт «**Свойства**» и перейти на вкладку «**Контрольная сумма**».



Обратите внимание, что расчет контрольных сумм по ГОСТ производится при включенной функции «**Активировать ГОСТ**» и настроенном **openssl-gost-engine**.

Замкнутая программная среда

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: ima-manage-0.2-1, dracut-056-9

Для контроля целостности компонентов ОС используется **IMA**. Компонент архитектуры измерения целостности (**IMA**) производит проверки целостности во время выполнения файлов с использованием хэшей, сравнивая их со списком допустимых хэшей.

Примечание.

Работает, начиная с версии **ядра 5.15.78** из репозитория РЕД ОС.

Для проведения контроля целостности необходимо перейти в сеанс пользователя **root**:

```
su -
```

и выполнить следующие действия:

1. Установить пакеты для работы с **IMA**:

```
dnf install ima-manage openssl-gost-engine keyutils
```

2. Обновить пакет **dracut**:

```
dnf update dracut
```

ВАЖНО!

Для корректного осуществления контроля целостности компонентов ОС необходимо, чтобы в системе были установлены актуальные версии пакетов - **dracut** версии **056-6 и выше**, **ima-manage** версии **0.2-1 и выше**.

3. Включить ГОСТ в **openssl**:

```
openssl-switch-config gost
```

4. Сгенерировать пару ключей.

а) Создать файл **test-ca.conf** со следующим содержимым:

```
[ req ]
 distinguished_name = req_distinguished_name
 prompt = no
 string_mask = utf8only
 x509_extensions = v3_ca
 [ req_distinguished_name ]
 O = IMA-CA
 CN = IMA/EVM certificate signing key
 emailAddress = ca@ima-ca
 [ v3_ca ]
 basicConstraints=CA:TRUE
 subjectKeyIdentifier=hash
 authorityKeyIdentifier=keyid:always,issuer
```

Значения полей **O**, **CN**, **emailAddress** являются произвольными, можно заменить их на свои. Место расположения файла не играет роли, он нужен только для создания пары ключей один раз.

б) Сгенерировать приватный ключ:

```
openssl genpkey -algorithm gost2012_512 -pkeyopt paramset:A -out privkey_evm.pem
```

в) Создать запрос:

```
openssl req -new -config test-ca.conf -md_gost12_512 -key privkey_evm.pem -out cert.req
```

г) Отправить файл запроса в Техническую поддержку РЕД СОФТ. Получить публичный ключ (например, **x509_evm.der**). В случае получения сертификата в **CRT**-формате, его можно перевести в формат **DER** следующим образом:

```
openssl x509 -outform der -in pub.crt -out x509_evm.der
```

5. Создать папку **/etc/keys/ima/** и скопировать в нее открытый ключ **x509_evm.der**.

```
mkdir /etc/keys/ima/
cp x509_evm.der /etc/keys/ima/x509_evm.der
```

Секретный ключ «**privkey_evm.pem**» сохранить в каталоге, недоступном для всех пользователей, кроме администратора **root**, например:

```
mv privkey_evm.pem /root/privkey_evm.pem
```

6. Запустить утилиту **ima-manage** с ключом **init**:

```
ima-manage init
```

7. В файле **/etc/ima-manage.conf** изменить значение **HASHALGO="sha256"** на **HASHALGO="streebog512"**.

ВАЖНО!

Значение битности параметра **HASHALGO** должно совпадать с битностью сгенерированных ключей. Например, если приватный ключ был сгенерирован с параметром **gost2012_256**, то значение параметра **HASHALGO** в таком случае будет равен **streebog256**.

8. Запустить утилиту «**ima-manage**» с ключом «**signfs**» и указанием пути размещения секретного ключа:

```
ima-manage signfs /root/privkey_evm.pem
```

9. Запустить утилиту **ima-manage** с ключом «**enforce**»:

```
ima-manage enforce
```

Дождаться завершения работы утилиты и предложения перезагрузки. Дать согласие на перезагрузку системы.

Примечание.

После обновления/редактирования файлов, которые ранее были подписаны **IMA**, их рекомендуется **переподписать**, выполнив действия, указанные в *п. 8-9*.

В противном случае корректное поведение системы при следующем запуске **не гарантируется**.

Для проверки работы защиты от запуска неподписанных исполняемых файлов создайте копию существующего исполняемого файла, например:

```
cp /bin/ls ls.copy
```

Попробуйте его запустить, будет выведена ошибка:

```
./ls.copy

bash: ./ls.copy: Permission denied
```

При этом в логе аудита появится запись о запрете запуска неподписанного файла:

```
grep -i ima /var/log/audit/audit.log | tail -n 1

type=INTEGRITY_DATA msg=audit(1638974599.231:11315): pid=2800 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op=appraise_data cause=IMA-signature-required comm="bash"
name="/home/user/ls.copy" dev="dm-0" ino=946370 res=0 errno=0UID="user" AUID="user"
```

Для запуска сторонних файлов, не имеющих подписи, необходимо **от имени администратора** подписать файл:

```
evmctl ima_sign --hashalgo md_gost12_512 --key <путь_к_приватному_ключу_privkey_evm.pem> <путь_к_файлу>
```

Например:

```
evmctl ima_sign --hashalgo md_gost12_512 --key /root/privkey_evm.pem /home/user/ls.copy
```

Для включения режима журналирования (система не будет запрещать запуск неподписанных файлов, но будет записывать попытки их запуска) необходимо в файле **/etc/default/grub** изменить параметр **ima_appraise=enforce** на **ima_appraise=log**.

После этого обновите конфигурацию загрузчика ОС, для этого выполните в терминале команду:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Проверка контрольной суммы ISO-образа

Проверка контрольных сумм через файловый менеджер caja
Проверка контрольных сумм через Double Commander
Проверка при помощи встроенных утилит
Проверка с помощью дополнительных утилит

Образ ISO представляет собой полную копию всего, что хранится на физическом оптическом диске, таком как *CD*, *DVD* или *Blu-ray*, включая собственную файловую систему.

Большинство операционных систем и многие «утилиты» также позволяют монтировать **образ ISO** как виртуальный диск. В этом случае, все приложения обрабатывают его таким же образом, как если бы это был реальный оптический диск, вставленный в привод персонального компьютера.

Контрольная сумма - некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении.

Контрольная сумма является результатом хеш-функции, используемой для вычисления контрольного кода — небольшого количества бит внутри большого блока данных, например, сетевого пакета или блока компьютерного файла, применяемого для обнаружения ошибок при передаче или хранении информации. Значение контрольной суммы добавляется в конец блока данных непосредственно перед началом передачи или записи данных на какой-либо носитель информации. Впоследствии оно проверяется для подтверждения целостности данных.

Популярность использования контрольных сумм для проверки целостности данных обусловлена тем, что подобная проверка просто реализуема в двоичном цифровом оборудовании, легко анализируется и хорошо подходит для обнаружения общих ошибок, вызванных наличием шума в каналах передачи данных.

Вы можете подробнее ознакомиться с возможностью проверки контрольной суммы iso-образа, просмотрев наши обучающие видео:

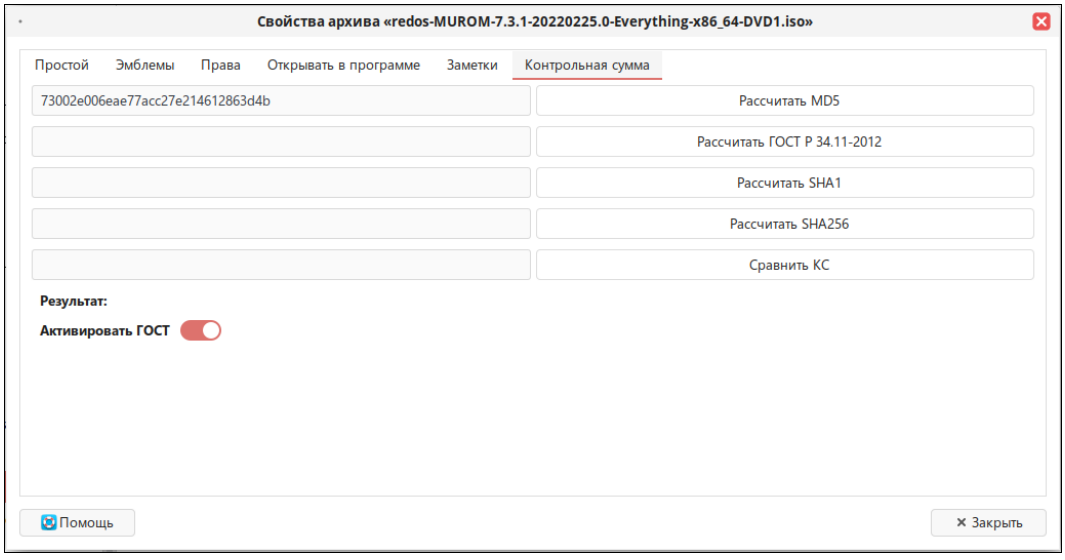
- на **RuTube** — Проверка контрольной суммы iso-образа;
- в **Яндекс.Дзен** — Проверка контрольной суммы iso-образа;
- в **VK Видео** — Проверка контрольной суммы iso-образа.

На наших каналах вы также сможете найти много другой полезной информации.

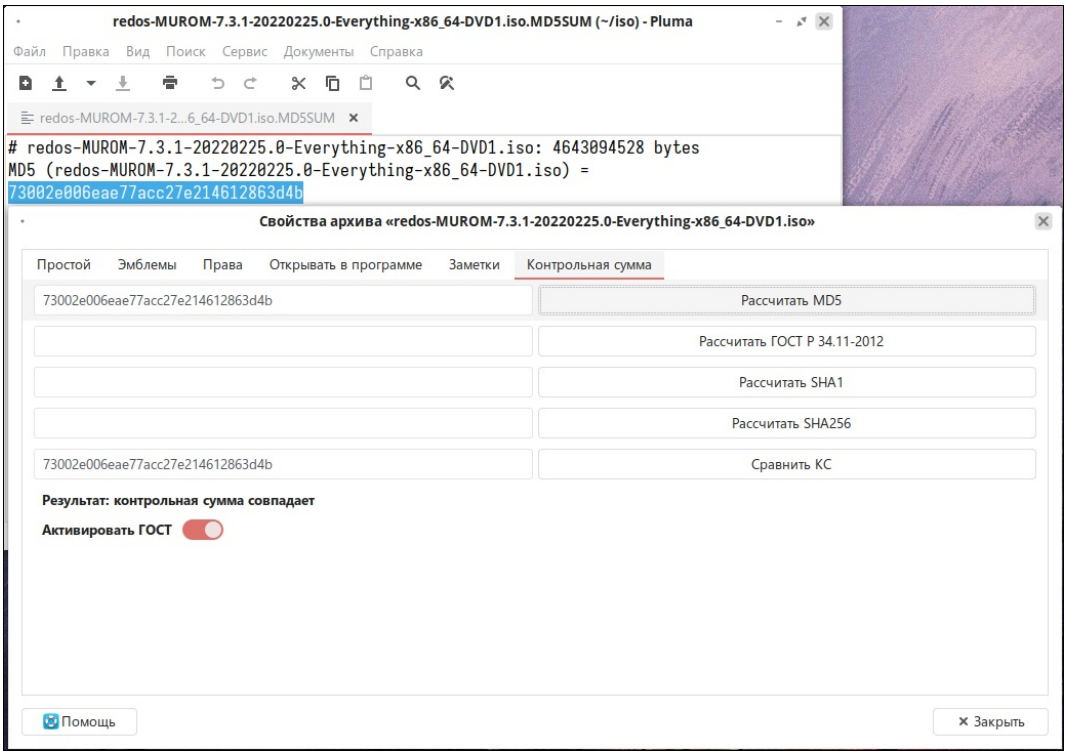
Проверка контрольных сумм через файловый менеджер caja

Для расчета контрольной суммы файла (хеш-суммы) через файловый менеджер caja необходимо выделить файл и нажать правую кнопку мыши. В контекстном меню выбрать пункт «**Свойства**» - «**Контрольная сумма**».

Далее требуется нажать кнопку «**Расчитать MD5**».

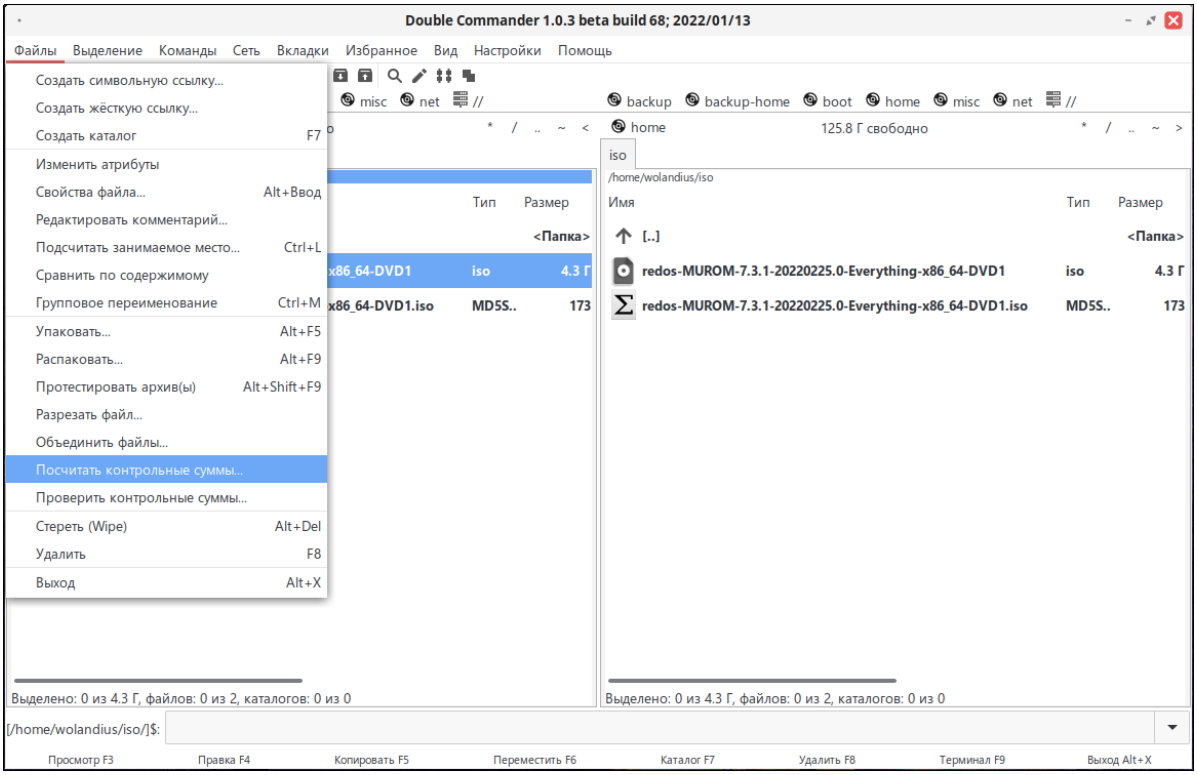


Из файла **redos-MUROM-7.3.1-20220225.0-Everything-x86_64-DVD1.iso.MD5SUM** требуется скопировать эталонную хэш-сумму образа, как показано ниже. Далее нажать кнопку «**Сравнить КС**».

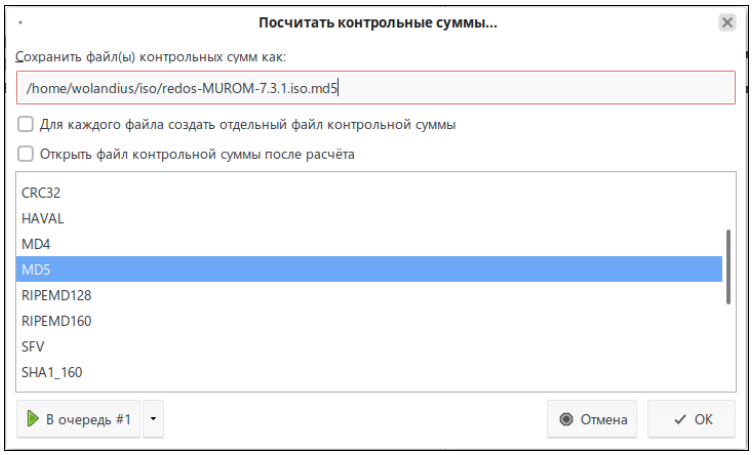


Проверка контрольных сумм через Double Commander

Для расчета контрольной суммы файла (хеш-суммы) через **Double Commander** необходимо выделить файлы и выбрать пункт меню «**Файлы**» - «**Посчитать контрольные суммы...**».

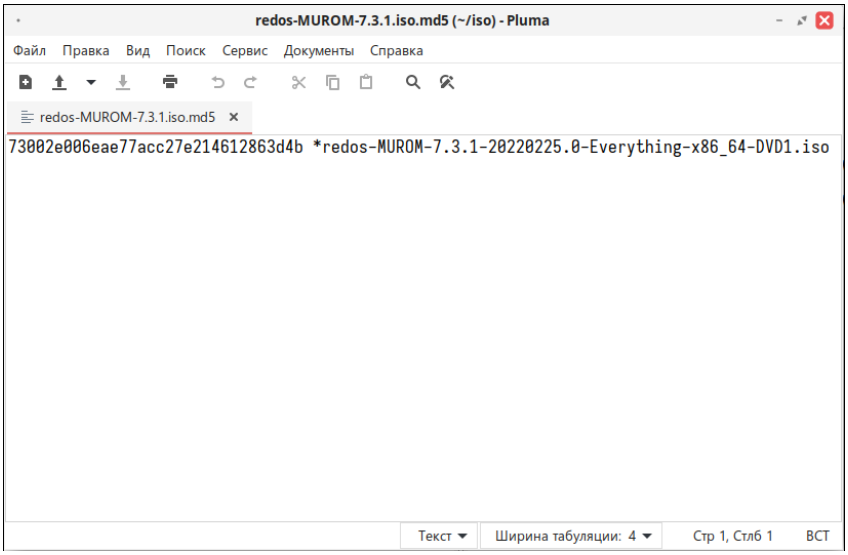


Далее в меню расчета контрольной суммы нужно выбрать требуемый алгоритм (хеш-фукцию) и нажать кнопку «**OK**».

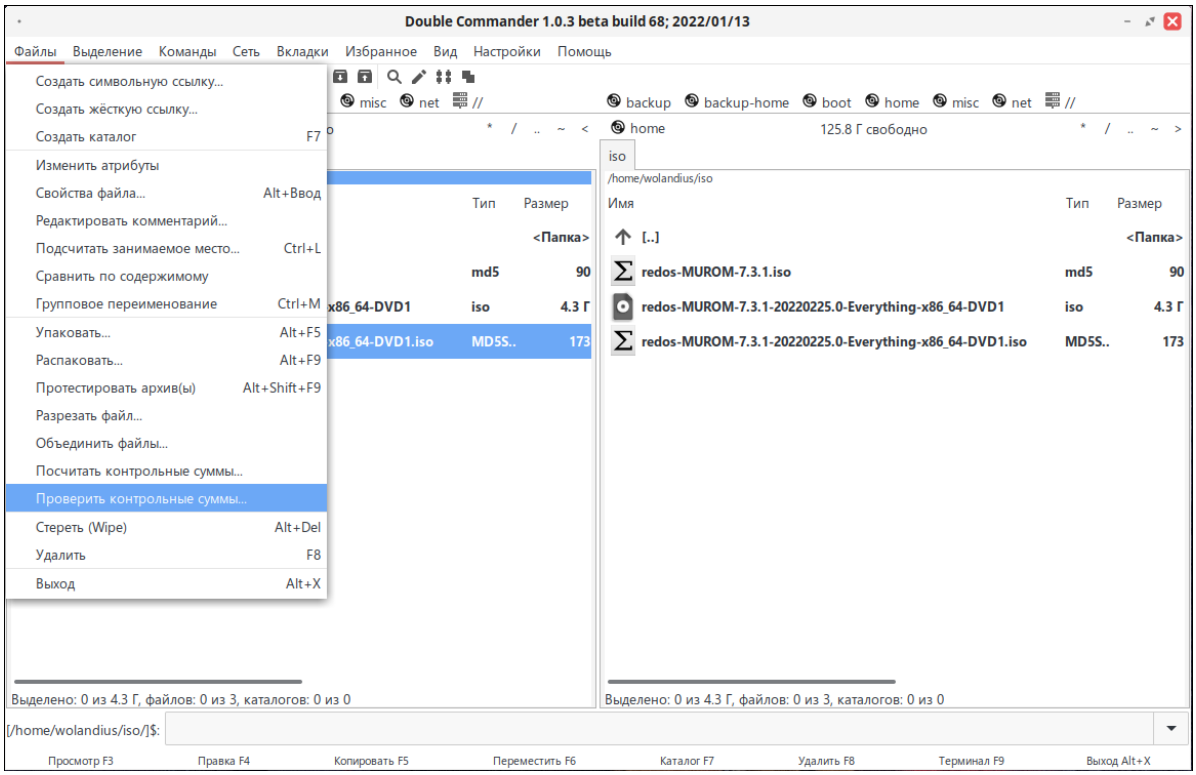


Результат расчета помещается в файл с расширением, соответствующим алгоритму хеширования.

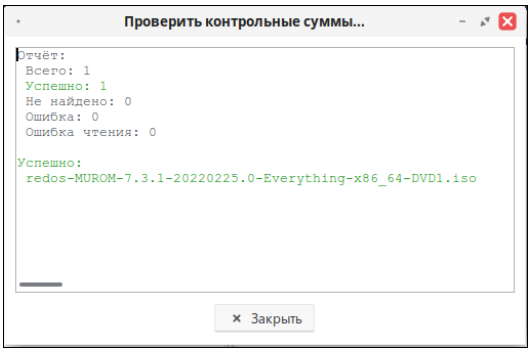
Строка результата для каждого файла представляет собой его *контрольную сумму* и его **название*.



Можно, наоборот, рядом с проверяемым файлом создать файл его контрольной суммы указанного выше формата с тем же именем и соответствующим хеш-алгоритму расширением. Затем выделить этот файл контрольной суммы и из меню «**Файлы**» - «**Посчитать контрольные суммы...**» запустить проверку.



После расчета будет выведен результат проверки.



Проверка при помощи встроенных утилит

РЕД ОС имеет встроенные утилиты, с помощью которых проверяются хеши файлов:

- **md5sum** для алгоритма **md5**;
- **shasum** для проверки алгоритма **sha**.

Проверка с помощью утилиты md5sum

Запустите терминал и введите команду:

```
md5sum <имя_файла>
```

В данном случае рассмотрим файл с именем «**redos-MUROM-7.2-i386-DVD1.iso**».

```
md5sum redos-MUROM-7.2-i386-DVD1.iso

c0eda14f655789c6008ea71ad6ddd2fe redos-MUROM-7.2-i386-DVD1.iso
```

c0eda14f655789c6008ea71ad6ddd2fe – контрольная сумма файла.

Также, помимо нахождения контрольной суммы, можно проверить правдивость указанных в источнике контрольных сумм.

Для этого понадобится файл контрольной суммы из источника с нужным расширением и команда:

```
md5sum -c <имя_файла>
```

В данном случае ответ будет следующим:

```
md5sum -c redos-MUROM-7.2-x86_64-DVD1.iso.md5

redos-MUROM-7.2-x86_64-DVD1.iso: ЦЕЛ
```

Помимо опции «**-c**», отвечающей за проверку контрольной суммы файла, есть и другие опции:

- **-b** - работать в двоичном формате;
- **-t** - работать в текстовом формате;
- **-w** - выводить предупреждения о неверно отформатированном файле сумм;
- **--quiet** - не выводить сообщения об успешных проверках.

Проверка с помощью утилиты shasum

При использовании алгоритма **sha** нужно дополнить команду в зависимости от битности алгоритма **1-**, **256-**, **384-** или **512-**битного.

Команда примет вид:

```
sha1sum <имя_файла>
```

Проверим наш образ:

```
sha1sum redos-MUROM-7.2-i386-DVD1.iso

c5afc08269d761e638511536751ddbdd5350b602 redos-MUROM-7.2-i386-DVD1.iso
```

c5afc08269d761e638511536751ddbdd5350b602 - контрольная сумма файла.

Проверка с помощью дополнительных утилит

Помимо традиционных методов нахождения контрольных сумм через встроенные утилиты также существует аналогичный метод, который используется реже. Дело в том, что контрольная сумма ISO-образа может быть встроена непосредственно в ISO-файл.

Встроить **MD5** в файл поможет утилита **implantisomd5**, входящая в набор программ **isomd5sum**.

Проверку соответствия содержимого образа по встроенной в него контрольной сумме можно осуществить при помощи утилиты **checkisomd5** из того же пакета.

Для установки пакета введите команду:

```
dnf install isomd5sum
```

Сначала утилита извлекает **md5** контрольную сумму, далее идет проверка диска.

Контрольная сумма должна быть предварительно внедрена в образ диска, с которого происходит запись, командой:

```
implantisomd5 --force <имя_файла>
```

> **Примечание.**
>
> Сначала создаются образы дисков, затем внедряется контрольная сумма, и только потом записывается на диск. Только после этого можно пользоваться программой **checkisomd5**.

Пример:

```
implantisomd5 --force /home/user/Загрузки/redos-MUROM-7.3-20210412-Everything-x86_64-DVD1.iso

Inserting md5sum into iso image...
md5 = 524c3f6723432030e36e55ee00df19ec
Inserting fragment md5sums into iso image...
fragmd5 = 8c4cbfecb6cad789ecfc0976b6c4354fd3555bc81e7238125551992abele
frags = 20
Setting supported flag to 0

checkisomd5 /home/user/Загрузки/redos-MUROM-7.3-20210412-Everything-x86_64-DVD1.iso

Press [Esc] to abort chek.

The media chek is complete, the result is: PASS.

It is OK to use this media.
```

Для того чтобы узнать значение внедренной контрольной суммы, введите команду:

```
checkisomd5  --verbose <имя_файла>
```

Например:

```
checkisomd5  --verbose test.iso

test.iso: dfd25ecf95b713e5692367a0d0fef899
Fragment sums: 17476fd87fdaaf177cfbb8873b232f9f586724a6639aec7f8ba2b961b9e7
Fragment count: 20
Press [Esc] to abort chek.
Cheking: 100.0%

The media chek is complete, the result is: PASS.
```

It is OK to use this media.

SELinux - система принудительного контроля доступа

Введение
Установка
Утилита audit2allow
Утилита secon
Утилита audit2why

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя. Далее описываются основные принципы, на которых построена работа SELinux, а также их реализация в РЕД ОС.

Введение

В большинстве операционных систем имеются средства управления доступом, которые определяют, может ли определенный объект (пользователь или программа) получить доступ к определенному ресурсу. В системах UNIX применяется разграничительный контроль доступа (discretionary access control, DAC). Этот метод позволяет ограничить доступ к объектам на основе групп, к которым они принадлежат. Например, в GNU/Linux для каждого файла определены владелец, группа, а также указаны права доступа к этому файлу. Правами доступа определяется, кто может получить доступ к файлу, кто может открыть его для чтения, кто может внести в него изменения, кто может запустить этот файл на выполнение. Права доступа определены для трех категорий: пользователь (владелец файла), группа (все пользователи, которые являются членами группы) и другие (все пользователи, которые не являются ни владельцем файла, ни членами группы).

Такое разграничение прав доступа может привести к возникновению ряда проблем из-за того, что программа, в которой может быть обнаружена уязвимость, наследует все права доступа пользователя. Следовательно, она может выполнять действия с тем же уровнем привилегий, какой есть у пользователя (*что нежелательно*). Вместо того чтобы определять ограничения подобным образом, более безопасно использовать принцип наименьшего уровня привилегий (*principle of least privilege*), согласно которому программы могут делать только то, что им необходимо для выполнения своих задач, и не более того. Таким образом, даже если в программе будет обнаружена уязвимость, то возможности доступа данной программы будут жестко ограничены. Такой тип контроля называется принудительным управлением доступом (*mandatory access control*, MAC).

Другим методом управления доступом является управление доступом на основе ролей (role-based access control, RBAC). При использовании RBAC права доступа предоставляются на основе ролей, выдаваемых системой безопасности. Отличие концепции ролей от традиционных групп состоит в том, что группа представляет одного или нескольких пользователей, в то время как роль, хотя она также может быть применена к нескольким пользователям, представляет совокупность полномочий на выполнение определенных действий.

SELinux добавляет в операционную систему GNU/Linux поддержку как MAC, так и RBAC.

Установка

Для установки SELinux требуется установить пакет selinux-policy. Это можно сделать, например, воспользовавшись командной строкой с привилегиями root-пользователя:

```
dnf install selinux-policy
```

После перезагрузки SELinux проиндексирует содержимое жёсткого диска, это может занять некоторое время.

Для настройки SELinux можно использовать различные текстовые редакторы чтобы настроить вручную его файл конфигурации:

/etc/selinux/config.

Утилиты

Утилита audit2allow

Утилита audit2allow создает разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций.

Эта утилита сканирует журналы в поиске сообщений, появляющихся, когда система не дает разрешения на операцию. Далее утилита генерирует ряд правил, которые, будучи загруженными в политику, могли бы разрешить эти операции. Однако, данная утилита генерирует только разрешающие правила Type Enforcement (TE). Некоторые отказы в использовании разрешений могут потребовать других изменений политики. Например, добавление атрибута в определение типа, для разрешения существующего ограничения (constraint), добавления разрешающего правила для роли или модификации ограничения (constraint). В случае сомнений для диагностики можно попробовать использовать утилиту audit2why.

Следует с осторожностью работать с выводом данной утилиты, убедившись, что разрешаемые операции не представляют угрозы безопасности. Обычно бывает лучше определить новый домен и/или тип или произвести другие структурные изменения. Лучше избирательно разрешить оптимальный набор операций вместо того, чтобы вслепую применить иногда слишком широкие разрешения, рекомендованные этой утилитой. Некоторые запреты на использование разрешений бывают не принципиальны для приложения. В таких случаях вместо использования разрешительного правила («allow» rule) лучше просто подавить журналирование этих запретов при помощи правила «dontaudit».

Синтаксис:

```
audit2allow
```

Опция	Значение опции
-a | --all	Прочесть входную информацию из журналов message и audit. Не используется вместе с опцией -i
-d | --dmesg	Прочесть входную информацию из вывода команды /bin/dmesg. Обратите внимание, что когда работает auditd, не все сообщения аудита доступны через dmesg. Вместо этого используйте "ausearch -m avc | audit2allow " или "-a".
-f | --fcfile <File Context File>	Добавить Файл Контекстов в генерируемый пакет модуля. Требует опцию -M.
-h | --help	Вывести краткую справку по использованию
-i <inputfile> | --input <inputfile>	Прочесть входную информацию из <inputfile>
-l | --lastreload	Прочесть только часть входной информации, начиная с момента последней перезагрузки политики
-m <modulename> | --module <modulename>	Генерировать модуль. Требуется вывод <modulename>
-M <modulename>	Генерировать загружаемый пакет модуля. Опция конфликтует с -o
-o <outputfile> | --output <outputfile>	Дописать вывод в <outputfile>
-r | --requires	Генерировать вывод в синтаксисе загружаемого модуля.
-R | --reference	Генерировать эталонную политику (reference policy), используя установленные макросы. Требуется пакет selinux-policy-devel.
-t | --tefile	Указывает, что выходной файл является te-файлом (type enforcement). Может использоваться для конвертации старого формата политик в новый формат.
-v | --verbose	Включить подробный вывод

Пример:
Этот пример подходит для системы, использующей пакет *audit*. Если вы не используете пакет audit, сообщения AVC будут появляться в **/var/log/messages**. В этом случае замените **/var/log/audit/audit.log**, используемый в примере, на **/var/log/messages.**
Использование *audit2allow* для генерации монолитной (не модульной) политики.

```
cd /etc/selinux/$ SELINUXTYPE/src/policycat /var/log/audit/audit.log | audit2allow >> domains/misc/local.tecat
domains/misc/local.teallow cupsd_config_t unconfined_t:fifo_file { getattr ioctl };
```

Просмотрите **domains/misc/local.te** и измените его

```
make load
```

Использование audit2allow для генерации модульной политики:

```
cat /var/log/audit/audit.log | audit2allow -m local > local.te
cat local.te

module local 1.0;
require {
role system_r;
class fifo_file { getattr ioctl }; type cupsd_config_t; type unconfined_t;};
allow cupsd_config_t unconfined_t:fifo_file { getattr ioctl };
```

Просмотрите **local.te** и измените его.

Создание модуля политики вручную:

Скомпилируйте модуль:

```
checkmodule -M -m -o local.mod local.te
```

Создайте пакет:

```
semodule_package -o local.pp -m local.mod
```

Загрузите модуль в ядро:

```
semodule -i local.pp
```

Использование audit2allow для генерации и создания модуля политики:

```
cat /var/log/audit/audit.log | audit2allow -M local
```

Создается новый type enforcment файл: local.te.

Компиляция политики:

```
checkmodule -M -m -o local.mod local.te
```

Создание пакета:

```
semodule_package -o local.pp -m local.mod
```

Для того чтобы загрузить только что созданный пакет политики в ядро, вам необходимо выполнить команду:

```
semodule -i local.pp.
```

Утилита secon

Утилита secon - просмотреть контекст SELinux для файла, программы или ввода пользователя.

Просматривает часть контекста. Контекст берется из файла, идентификатора процесса, ввода пользователя или контекста, в котором была запущена утилита secon.

Синтаксис:

```
secon [-hVurtscmPRfLp] [CONTEXT] [--file] FILE [--link] FILE [--pid] PID
```

Опции:

Опция	>**Значение опции**
-V, --version	Посмотреть текущую версию secon
-h, --help	Вывести информацию по использованию secon
-P, --prompt	Вывести данные в формате, подходящем для подсказки
-u, --user	Показать пользователя контекста безопасности
-r, --role	Показать роль контекста безопасности
-t, --type	Показать тип контекста безопасности
-s, --sensitivity	Показать уровень чувствительности (sensitivity level) контекста безопасности
-c, --clearance	Показать уровень допуска (clearance level) контекста безопасности
-m, --mls-range	Показать для контекста безопасности в виде диапазона уровень чувствительности (sensitivity level) и уровень допуска (clearance)
-R, --raw	Вывести уровень чувствительности (sensitivity level) и уровень допуска (clearance) в формате без трансляции
-f, --file	Получить контекст заданного файла FILE
-L, --link	Получить контекст заданного файла FILE (не следовать по символическим ссылкам)
-p, --pid	Получить контекст заданного процесса по идентификатору PID
--pid-exec	Получить exec контекст заданного процесса по идентификатору PID

Опция	>Значение опции
--pid-fs	Получить fscreate контекст заданного процесса по идентификатору PID
--current, --self	Получить контекст из текущего процесса
--current-exec, --self-exec	Получить exec контекст из текущего процесса
--current-fs, --self-fs	Получить fscreate контекст из текущего процесса
--parent	Получить контекст из родительского процесса текущего процесса
--parent-exec	Получить exec контекст из родительского процесса текущего процесса
--parent-fs	Получить fscreate контекст из родительского процесса текущего процесса

Если не было задано опций, то для того, чтобы secon получил контекст из другого источника, может быть задан дополнительный аргумент CONTEXT. Если этим аргументом является знак дефиса (-), то контекст будет прочитан из стандартного ввода. Если аргументов не было заданно, то secon будет пытаться прочитать контекст со стандартного ввода, но только в том случае, если стандартный ввод не терминал (tty). В этом случае secon будет вести себя как будто была передана опция --self .

Если не задана ни одна опция из --user, --role, --type, --level или --mls-range, то все они будут использованы.

Утилита audit2why

Утилита audit2why - определит из сообщения аудита SELinux причину запрета доступа.

Эта утилита обрабатывает сообщения аудита SELinux, принятые со стандартного ввода, и сообщает, какой компонент политики вызвал каждый из запретов. Если задана опция -p, то используется указанная этой опцией политика, в противном случае используется активная политика. Есть три возможные причины запрета доступа:

- отсутствует или отключено разрешительное TE правило (TE allow rule);
- нарушение ограничения (a constraint violation);
- отсутствует разрешительное правило для роли (role allow rule).

В первом случае разрешительное TE правило может присутствовать в политике, но было отключено через булевы атрибуты. Если же разрешительного правила не было, то оно может быть создано при помощи утилиты audit2allow.

Во втором случае могло произойти нарушение ограничения. Просмотрите policy/constraints или policy/mls для того, чтобы определить искомое ограничение. Обычно, проблема может быть решена добавлением атрибута типа к домену.

В третьем случае была произведена попытка сменить роль, при том что не существует разрешительного правила для участвующей при этом пары ролей. Проблема может быть решена добавлением в политику разрешительного правила для этой пары ролей.

Синтаксис:

```
audit2why
```

Опция	Значение опции
--help	Вывести короткую подсказку
-p <policyfile>	Указать альтернативный файл политики.

Пример:

```
/usr/sbin/audit2why < /var/log/audit/audit.logtype=KERNEL msg=audit(1115316408.926:336418): avc: denied { getattr } for
path=/home/ sds   dev=hda5   ino=1175041   scontext=root:secadm_r: secadm_t:s0-s9:c0.c127
tcontext=user_u:object_r:user_home_dir_t:s0 tclass=dir
```

Причина: Отсутствует или отключено разрешительное TE правило. Разрешительное TE правило может присутствовать в политике, но было отключено через булевы переключатели; проверьте булевы переключатели. Вы можете посмотреть необходимые разрешительные правила, запустив audit2allow и подав это сообщение аудита на ввод.

```
type=KERNEL msg=audit(1115320071.648:606858): avc: denied { append } for name=.bash_history dev=hda5 ino=1175047
scontext=user_u:user_r:user_t:s1-s9:c0.c127 tcontext=user_u:object_r:user_home_t:s0 tclass=file
```

Причина: Нарушение ограничения. Проверьте *policy/constraints*. Обычно, для разрешения ограничения необходимо добавить в

домен атрибут типа.

Отключение SELINUX

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

SELinux имеет три режима работы, по умолчанию установлен режим `Enforcing`.

Enforcing: Все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: Информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Disabled: Полное отключение системы принудительного контроля доступа.

1. Для перевода **SELinux** в режим уведомлений в файле `/etc/selinux/config` замените строку `SELINUX=enforcing` на `SELINUX=permissive`. **SELinux** при этом перейдет в режим уведомлений. Откройте файл конфигурации в редакторе `nano` от пользователя **root** или от пользователя с правами **администратора**.

```
sudo nano /etc/selinux/config
```

В файле замените текст `SELINUX=enforcing` на `SELINUX=permissive`.

Изменения будут применены **только после перезагрузки ОС**.

Вместо ручной правки конфигурационного файла можно выполнить следующую команду в консоли от пользователя с правами администратора (после выполнения команды нужно перезагрузить ПК, перезагрузку можно запустить из консоли командой `reboot`):

```
sudo sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

Параметр `SELINUXTYPE=targeted` **изменять не нужно**.

2. Мгновенный перевод режима SELinux `Enforcing` на `Permissive`:

```
sudo setenforce 0
```

после перезагрузки SELinux будет запущен в режиме, который указан в файле **/etc/selinux/config**.

ВАЖНО!

Крайне **не рекомендуется** устанавливать для **SELinux** режим **Disabled**.

Подключаемые модули аутентификации (PAM). Общие сведения

PAM или Pluggable Authentication Modules (подключаемые модули аутентификации) — это модульный подход к системе аутентификации. Они позволяют сторонним службам предоставлять модуль аутентификации для обеспечения доступа к службе для систем с поддержкой PAM. Службы, использующие PAM для аутентификации, могут использовать их сразу же, без необходимости дополнительной пересборки.

На сервере Linux PAM (Pluggable Authentication Modules) могут использоваться для управления аутентификацией (как часть управления предоставления доступа). При использовании PAM сервисам нет необходимости поддерживать собственную систему аутентификации. Вместо этого они полагаются на модули PAM, доступные в системе. Любой сервис при необходимости может использовать собственную конфигурацию PAM, хотя в большинстве случаев аутентификация выполняется одинаково во множестве сервисов. Вызывая модули PAM, сервисы могут поддерживать двухфакторную аутентификацию «из коробки», сразу же использовать централизованные хранилища аутентификационных средств и многое другое.

PAM предоставляют гибкую модульную архитектуру для следующих сервисов:

- Управление аутентификацией - проверяет, существует ли пользователь, под которым пытаются зайти.
- Управление учётными записями - проверяет, что пароль пользователя не истёк или имеет ли пользователь право обращаться к определённому сервису.
- Управление сеансами - выполняет определённые задачи во время входа или выхода пользователя из системы (аудит, монтирование файловых систем и так далее).
- Управление паролями - предлагает интерфейс для сброса пароля и тому подобное.

При работе с PAM администраторы очень быстро поймут принципы, по которым функционирует PAM.

Во-первых, это «независимость от бэк-энда». Приложениям, поддерживающим PAM, нет необходимости учитывать низкоуровневую логику, чтобы работать с бэк-эндами, например, базами данных, службой LDAP, файлами паролей, веб-службами с поддержкой WS-Security или другими ещё не изобретёнными бэк-эндами. Используя PAM, приложения отделяют логику работы бэк-энда от своей. Всё, что им нужно сделать — это вызвать функцию PAM.

Другим принципом является «независимость от конфигурации». Администраторам не нужно знать, как настраивать десятки различных приложений, чтобы заставить их поддерживать аутентификацию через LDAP-сервер. Вместо этого им достаточно воспользоваться одной конфигурационной структурой, предоставляемой PAM.

Последним принципом, являющимся также частью названия PAM, является «подключаемая архитектура». Когда необходимо интегрировать новый бэк-энд, всё, что нужно сделать администратору — это установить библиотеку для этого бэк-энда (большинство модулей используют один файл настроек). Начиная с этого момента, модуль становится доступен для использования приложениями. Администраторы могут настроить аутентификацию для использования этого бэк-энда и просто перезапустить приложение.

Приложения, для которых необходимо использование PAM, линкуются с библиотекой PAM (libpam) и могут вызывать нужные функции работы с указанными выше службами. Кроме этого, в приложении не нужно реализовывать ничего специфичного для работы с этими сервисами, так как эту задачу на себя берёт PAM. И когда пользователь захочет аутентифицироваться, скажем, в веб-приложении, то это приложение вызывает PAM (передавая ему идентификатор и, возможно, пароль или запрос) и проверяет возвращаемые данные, чтобы принять решение, аутентифицировался ли пользователь и имеет ли он доступ к приложению. Внутренней задачей PAM является определение, где необходимо аутентифицировать пользователя (например, в центральной базе данных или на LDAP-сервере).

Сильной стороной PAM является то, что любой желающий может создать модули PAM для интеграции с любым поддерживающим PAM-сервисом или приложением. Если какая-нибудь компания выпускает новый сервис для аутентификации, всё, что нужно будет сделать, — это предоставить для взаимодействия с этим сервисом модуль PAM, после чего любое использующее PAM приложение сможет незамедлительно работать с этим сервисом: нет необходимости что-то пересобирать или улучшать.

Другой важной особенностью PAM является то, что они поддерживают объединение в цепочки нескольких модулей. Пример конфигурационного файла PAM для некоего сервиса:

```
# Аутентификация
auth        required      pam_env.so
auth        required      pam_ldap.so
# Управление учётными записями
account     required      pam_ldap.so
# Управление паролями
password    required      pam_ldap.so
# Управление сеансами
session     optional      pam_loginuid.so
session     required      pam_selinux.so close
session     required      pam_env.so
session     required      pam_log.so level=audit
session     required      pam_selinux.so open multiple
session     optional      pam_mail.so
```

Видно, что конфигурационный файл разделён на четыре области сервисов, которые поддерживают PAM: аутентификация, управление учётными записями, управление паролями и управление сеансами.

Каждый из этих разделов в файле вызывает один или несколько модулей PAM. Например, **pam_env.so** устанавливает переменные среды, которые могут быть использованы последующими модулями. Код, возвращаемый модулем PAM, вместе с управляющими

директивами (в данном примере — *required* или *optional*) позволяет PAM решать, что делать дальше.

PAM поддерживают следующие управляющие директивы:

- **required** - Указанный модуль PAM должен вернуть код успеха для того, чтобы весь сервис (например, аутентификация) был успешен. Если модуль PAM вернёт код неудачи, остальные модули будут всё равно вызваны (хотя уже точно известно, что сам сервис будет недоступен).
- **requisite** - Указанный модуль PAM должен вернуть код успеха для того, чтобы весь сервис был доступен. В отличие от *required*, если модуль PAM вернёт код неудачи, директива сразу же завершится, и сам сервис будет недоступен.
- **sufficient** - Если указанный модуль PAM вернёт код успеха, весь сервис будет разрешен. Оставшиеся модули PAM не будут проверяться. Однако, если модуль PAM вернёт код неудачи, оставшиеся модули пройдут проверку, а неудача данного модуля не будет приниматься во внимание.
- **optional** - Код успеха или неудачи указанного модуля PAM будет иметь значение, если это единственный модуль в стеке.

Цепочки модулей позволяют выполнить множественную аутентификацию, выполнить несколько задач в процессе создания сеанса и тому подобное.

Так как конфигурационные файлы PAM управляют процессом аутентификации в приложении, очень важно правильно с ними взаимодействовать. Файлы обычно располагаются в каталоге **/etc/pam.d/**.

В больших организациях или в требовательных к безопасности системах любая модификация конфигурационных файлов PAM должна подвергаться соответствующему аудиту.

Это же относится к тому месту, где располагаются модули PAM (**/lib/security** или **/lib64/security**).

Помимо файлов-сценариев для некоторых модулей могут использоваться дополнительные файлы конфигурации. Все они расположены в каталоге **/etc/security** и каждый файл предназначен для конкретной группы настроек.

- **time.conf** - Здесь вы сможете ограничить время доступа пользователей с различных терминалов к различным сервисам. Например, запретить входить в систему с первой виртуальной консоли администратору во время выходных. Эти настройки обслуживает модуль pam_time и, соответственно, если вы желаете, чтобы ваши ограничения возымели действие модуль должен быть прописан в соответствующем сценарии.
- **pam_env.conf** - Здесь можно ограничить возможности в изменении отдельных переменных среды пользователями. Работает под руководством модуля pam_env.
- **limits.conf** - Здесь можно индивидуально или для группы ограничить: размер core-файла, максимальный допустимый размер файла, максимальное количество открытых файлов, запущенных процессов, сколько раз можно одновременно зайти в систему и т.д. Руководящий модуль pam_limits.
- **access.conf** - играет важную роль, поскольку PAM предоставляет средства аутентификации по сети. Подобные настройки оказываются полезными, поскольку контролируется не только, кто может войти, но и откуда. Для осуществления такого контроля используется pam_access.
- **group.conf** - Можно указать какой группе будет принадлежать служба запущенная определенным пользователем в определенное время с определенного терминала. Контролируется pam_time и pam_group.
- **console.perms** - Несколько выбивается своим названием, но не функциями. Здесь определяются права, получаемые привилегированными пользователями к консоли во время входа в систему и возвращаемые при выходе. Модуль pam_console.

Список модулей:

- **pam_cracklib**: Тип password. Проверяет ваш пароль на стойкость, не является ли он, например, палиндромом (примечание - это не обязательно при использовании модуля pam_unix). Полезен для программ, задающих пароли. Полезные параметры:
  retry=N - дается N попыток на исправление ошибки,
  diffok=N - должно быть изменено минимум N символов при смене пароля,
  minlen=N - минимальный размер пароля,
  dcredit=N ucredit=N lcredit=N ocredit=N - в пароле должно присутствовать минимум N цифр, строчных, прописных букв и других символов.
- **pam_deny**: Тип любой. Всегда перекрывает доступ.
- **pam_env**: Тип auth. Контролирует сохранность переменных среды. Полезный параметр *conffile=S* - задает альтернативное название файла конфигурации.
- **pam_ftp**: Тип auth. Предназначен для организации анонимного доступа. То есть, получив имя пользователя «anonymous», ждет в качестве пароля что-то похожее на его почтовый адрес. Полезные параметры:
  ignore - не обращать внимание похож ли пароль на почтовый адрес,
  users=XXX,YYY - позволяет анонимный вход для пользователей из этого списка.
- **pam_group**: Тип auth. Предназначение ясно из описания конфигурационного файла group.conf.
- **pam_lastlog**: Тип session. Сообщает о времени и месте входа в систему. Обновляет /var/log/wtmp файл. Полезные параметры:
  nodate, noterm, nohost, silent - не выводить в сообщении даты, терминала, машины или вообще ничего,
  never - если пользователь никогда ранее не появлялся, то его приветствуют.
- **pam_limits**: Тип session. Предназначение указано выше при описании файла limits.conf. Полезный параметр:
  conf=S - альтернативное имя конфигурационного файла.
- **pam_listfile**: Тип auth. Предназначен для организации доступа на основе конфигурационных файлов-списков например /etc/ftpaccess. Для примера смотрите соответствующие файлы сценариев. Возможные параметры: *on err=succeed|fail; sence=allow|deny; file=filename; item=user|tty|rhost|ruser|group|shell apply=user|@group*. Первый параметр задает возвращаемое значение в случае неудачного поиска. Второй - в случае удачного поиска. Третий - имя файла со списком. Четвертый - тип элемента в списке. Последний вносит дополнительные ограничения, если тип объявлен tty, rhost или shell.
- **pam_mail**: Тип auth. Сообщается о наличии почты, если таковая имеется. Полезные параметры:
  dir=S - путь к каталогу почтовых очередей,

noenv - не устанавливать переменную среды MAIL,
close - сообщать, если есть почта у пользователей с аннулированными бюджетами,
nopen - не печатать какой-либо почтовой информации, если пользовательский бюджет только что заведен.

- **pam_nologin**: Тип auth. Стандартная реакция на наличие файла /etc/nologin. Когда он присутствует, в систему может зайти только root, а остальным будет выдано на экран содержимое этого файла.
- **pam_permit**: Тип любой. Использование данного модуля **ОПАСНО** и применимо только в критических ситуациях. Всегда дает допуск.
- **pam_pwdb**: Тип любой. Замещает модули серии pam_unix... . Использует интерфейс библиотеки libpwdb (пользовательские базы данных), что повышает независимость системы аутентификации от способа хранения пользовательских данных (NIS или passwd или shadow). Полезные параметры:
  nullok - можно использовать пустые пароли,
  md5, shadow, bigcrypt - различные способы шифрования пароля.
- **pam_radius**: Тип session. Позволяет осуществлять аутентификацию через RADIUS сервер.
- **pam_rhosts_auth**: Тип auth. Механизм работы этого модуля основывается на анализе содержимого файлов hosts.equiv и .rhosts, используемых для аутентификации таких служб как rlogin и rsh. Полезные параметры:
  no_hosts_equiv - игнорировать содержимое файла hosts.equiv,
  no_rhosts - игнорировать содержимое файлов .rhosts,
  suppres s - охраняет системные журналы от потока малозначимых сообщений, в частности когда используется контрольный флаг sufficient.
- **pam_rootok**: Тип auth. Используется в случае, когда администратору необходимо получать доступ к сервису без введения пароля. Этот модуль допускает пользователя к сервису, только если его uid равен 0.
- **pam_securetty**: Включает в проверку файл /etc/securitty. Суперпользователь сможет зайти только на указанных там терминалах.
- **pam_time**: Тип account. Смотри описание устройства конфигурационного файла time.conf.
- **pam_warn**: Тип auth, session и password. Просто ведет записи в системных журналах, например, при смене пароля.
- **pam_wheel**: Тип auth и account. Права суперпользователя может использовать только пользователь группы wheel (группа root в Linux). Полезные параметры:
  group=XXX - использовать указанную группу вместо стандартной нулевой,
  deny - инвертирование действия алгоритма, запрещается получать права суперпользователя пользователям указанной группы, используется вместе с предыдущим параметром,
  trust - избавляет пользователей группы wheel от необходимости вводить пароль при смене uid на 0.

Настройка двухфакторной аутентификации с помощью модуля pam_usb

Для двухфакторной аутентификации используется модуль «**pam_usb**». Чтобы использовать *FLASH*-накопитель в качестве токена аутентификации, необходимо подключить к ЭВМ *FLASH*-накопитель и убедиться, что ОС успешно его подмонтировала.

Вы можете подробнее ознакомиться с возможностью настройки двухфакторной аутентификации, просмотрев наши обучающие видео:

- на **RuTube** — Модуль PAM USB - двухфакторная аутентификация;
- в **Яндекс.Дзен** — Модуль PAM USB - двухфакторная аутентификация;
- в **VK Видео** — Модуль PAM USB - двухфакторная аутентификация.

На наших каналах вы также сможете найти много другой полезной информации.

Добавить *FLASH*-накопитель, который будет использоваться как токен для аутентификации:

```
pamusb-conf --add-device <Auth-Stick>
```

где **<Auth-Stick>** - произвольное имя, присваиваемое токену.

Далее необходимо выбрать устройство из числа обнаруженных:

```
Please select the device you wish to add.
* Using "JetFlash TS128MJF2A (JetFlash_TS128MJF2A-0:0)" (only option)
Which volume would you like to use for storing data ?
```

И подтвердить его использование:

```
 * Using "/dev/sdc1 (UUID: 1CD6-B3F1)" (only option)
Name  : Auth-Stick
Vendor  : JetFlash
Model  : TS128MJF2A
Serial  : JetFlash_TS128MJF2A-0:0
UUID  : 1CD6-B3F1
```

Подтвердить сохранение параметров:

```
Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

Далее необходимо добавить пользователей, которые могут использовать этот токен:

```
pamusb-conf --add-user='petrov'

Which device would you like to use for authentication ?
* Using "Auth-Stick" (only option)
User
: petrov
Device
: Auth-Stick
Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

В файлах **/etc/pam.d/system-auth** и **/etc/pam.d/password-auth** нужно в начало файла добавить строку, отвечающую за загрузку модуля, и установить уровень управляющей директивы, как было описано ранее:

```
auth sufficient pam_usb.so
```

Локальная аутентификация с использованием Рутокен MFA

Настройка второго фактора
Настройка связки PIN-код + касание

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pam-u2f-1.2.1-1, pamu2fcfg-1.2.1-1, ido2-tools-1.10.0-1

Рутокен MFA — линейка токенов для аутентификации в веб-сервисах, работающих по протоколу **FIDO2** (CTAP2). Устройства линейки **Рутокен MFA** выступают в качестве единого средства защиты учетных записей веб-сервисов с использованием двухфакторной аутентификации.

Для настройки локальной аутентификации по **Рутокен MFA** установите следующие пакеты (потребуются права администратора системы или суперпользователя **root**):

```
dnf install fido2-tools pam-u2f pamu2fcfg
```

После установки пакетов подключите **Рутокен MFA**.

Для проверки корректности подключения **Рутокена MFA** выведите список подключенных устройств:

```
fido2-token -L
```

Вывод команды должен иметь примерно следующий вид (если к машине подключено только одно **FIDO2**-устройство):

```
/dev/hidraw1: vendor=0x0a89, product=0x0093 (Aktiv Co. FIDO)
```

Установите новый *PIN-код* на токен с помощью команды:

```
fido2-token -S /dev/hidraw1
```

Дважды введите новый *PIN-код*:

```
Enter new PIN for /dev/hidraw1:<новый_PIN>
Enter the same PIN again:<повторите_новый_PIN>
```

Примечание.

Особенности политики *PIN-кода*:

- *PIN-код* по умолчанию не задан;
- заданный *PIN-код* можно изменить, но нельзя удалить без сброса устройства;
- длина *PIN-кода* должна составлять от 4 до 63 символов;
- если *PIN-код* введен неправильно 8 раз подряд, Рутокен блокируется – потребуется сброс устройства.

Рутокен MFA позволяет аутентифицировать пользователя при входе в ОС в следующих сценариях:

- локальная аутентификация пользователя в ОС с использованием **Рутокен MFA** с нажатием кнопки в качестве второго фактора;
- локальная аутентификация пользователя в ОС с использованием **Рутокен MFA** с вводом PIN-кода и нажатием кнопки;
- доступ к хостам по **SSH** с использованием **Рутокен MFA** с нажатием кнопки в качестве второго фактора.

Настройка второго фактора

Для настройки второго фактора аутентификации создайте каталог командой:

```
mkdir -p ~/.config/aktivco
```

Подключите **Рутокен MFA** к машине и выполните настройку модуля с помощью утилиты pamu2fcfg. По завершении выполнения команды вывод утилиты будет записан в файл **u2f_keys**.

ВАЖНО!

Команда должна быть выполнена под пользователем, для которого настраивается аутентификация.

```
pamu2fcfg > ~/.config/aktivco/u2f_keys
```

В процессе выполнения команды необходимо будет прикоснуться к устройству **Рутокен MFA**.

Для повышения безопасности переместите сформированный конфигурационный файл **u2f_keys** в каталог **/etc** следующими командами:

```
sudo mkdir -p /etc/aktivco
sudo mv ~/.config/aktivco/u2f_keys /etc/aktivco/u2f_keys
```

Настройте файлы модуля **PAM** – отредактируйте файл **/etc/pam.d/common-auth**, который обрабатывает общие настройки аутентификации для всех сервисов:

```
sudo nano /etc/pam.d/common-auth
```

После модуля **pam_fprintd.so** добавьте следующую строку:

```
auth sufficient pam_u2f.so authfile=/etc/aktivco/u2f_keys cue nouserok
```

где:

- cue – выводит сообщение с запросом на касание устройства **Рутокен MFA**;
- nouserok – позволяет войти в систему с вводом данных логин/пароль, в случае если пользователь не найден в файле аутентификации или файл аутентификации неверно сформирован. После успешной настройки опцию можно удалить.

```
[root@localhost user]# cat /etc/pam.d/system-auth
# Generated by authselect on Tue Jan  9 13:48:03 2024
# Do not modify this file manually.

auth        required                                    pam_env.so
auth        required                                    pam_faildelay.so delay=2000000
auth        sufficient                                  pam_fprintd.so
auth        sufficient                                  pam_u2f.so authfile=/etc/aktivco/u2f_keys cue nouserok
```

Проверьте, что касание запрашивается в момент входа пользователя, выполнив команду (например, для пользователя **user**):

```
su user

Please touch the device.
```

Настройка связки PIN-код + касание

Для настройки связки *PIN-код + касание* выполните настройку модуля помощью утилиты pamu2fcfg. По завершении выполнения команды вывод утилиты будет записан в файл **u2f_mappings**.

ВАЖНО!

Команда должна быть выполнена под пользователем, для которого настраивается аутентификация.

```
pamu2fcfg -u <username> > /tmp/u2f_mappings
```

Примечание.

В случае выполнения команды без параметра `<username>` файл конфигурации будет создан для текущего пользователя.

В процессе выполнения команды необходимо будет прикоснуться к устройству **Рутокен MFA**.

Содержимое файла **u2f_mappings** должно иметь примерно следующий вид:

```
cat /tmp/u2f_mappings

user: hOzdi1ekgoVWLEzQH20uWJmoA3Dwno53zd2WCvlApHwfMVp/zz3+awUbeCL0E3pe,
jzL+t6w7vhBgR2wwO+61/g8aliGNbDUpYZj6mxLXain4F1bQB0rvnwzP3n+n/GlXUp5Oiui0Du7/aKP/pE27PQ==, es256, +presence
```

Для повышения безопасности переместите сформированный конфигурационный файл u2f_mappings в каталог /etc следующей командой:

```
sudo mv /tmp/u2f_mappings /etc/u2f_mappings
```

Настройте файлы модуля PAM – отредактируйте файл /etc/pam.d/common-auth, который обрабатывает общие настройки аутентификации для всех сервисов:

```
sudo nano /etc/pam.d/common-auth
```

После модуля pam_fprintd.so добавьте следующую строку:

```
auth sufficient pam_u2f.so authfile=/etc/u2f_mappings cue pinverification=1
```

где:

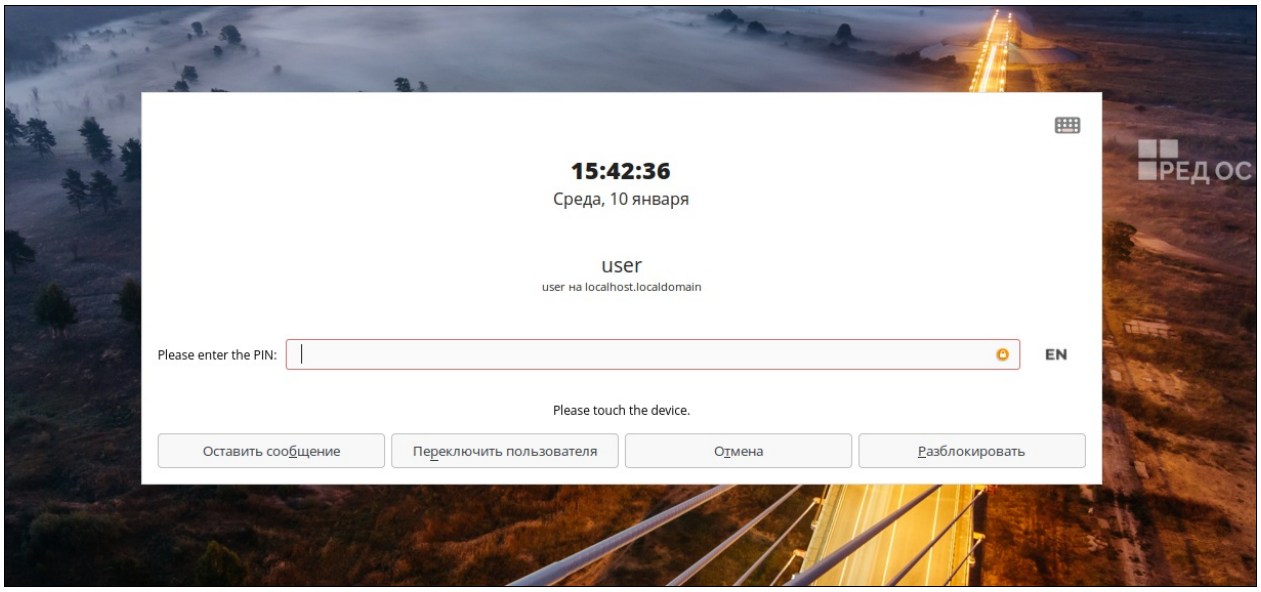
- `cue` – выводит сообщение с запросом на касание устройства **Рутокен MFA**;
- `pinverification=1` – выводит запрос на ввод *PIN-кода* Рутокена.

```
[root@localhost user]# cat /etc/pam.d/system-auth
# Generated by authselect on Tue Jan  9 13:48:03 2024
# Do not modify this file manually.

auth        required                                     pam_env.so
auth        required                                     pam_faildelay.so delay=2000000
auth        sufficient                                   pam_fprintd.so
auth        sufficient                                   pam_u2f.so authfile=/etc/u2f_mappings cue pinverification=1
```

Проверьте, что *PIN-код и касание* запрашиваются в момент входа пользователя, выполнив команду (например, для пользователя **user**):

```
su user

Please enter the PIN: Please touch the device.
```

При входе пользователя в графическую оболочку ОС также будет запрашиваться *PIN-код и касание* кнопки **Рутокен MFA**.


15:42:36
Среда, 10 января
user
user на localhost.localdomain
Please enter the PIN:
EN
Please touch the device.
Оставить сообщение
Переключить пользователя
Отмена
Разблокировать
РЕД ОС

Разблокировка связки ключей

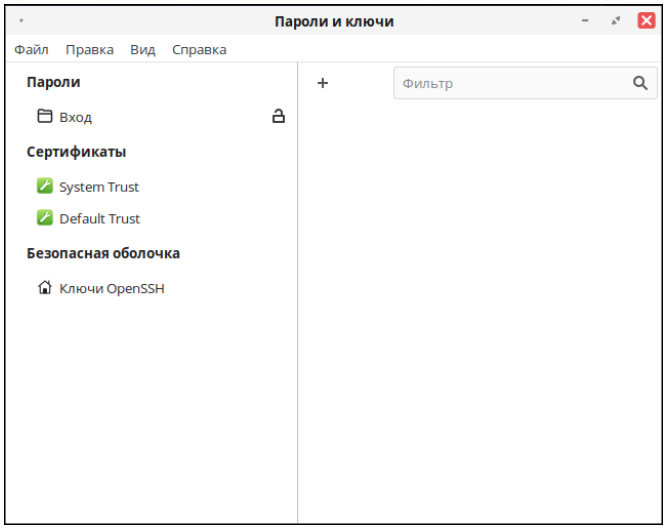
Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Графическое окружение**: MATE

Связка ключей — это зашифрованный контейнер, в котором безопасно хранятся пароли, логины и другие данные для подключения, например, к внешним сетевым ресурсам.

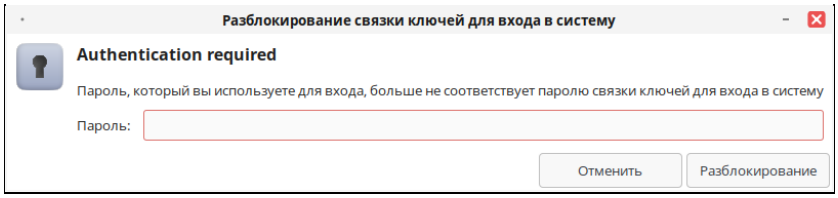
Это хранилище по умолчанию зашифровано и открывается с помощью пароля пользователя при входе в систему.

У каждого пользователя (как локального, так и доменного) на компьютере есть связка ключей входа.



Например, в файловом менеджере был настроен доступ к сетевому ресурсу с параметрами доступа: логин и пароль пользователя (если доменная учетная запись, то указывается и домен) с параметром «**Запомнить навсегда**».

Если вы измените пароль пользователя, появится окно «**Разблокирование связки ключей для входа в систему**».



Но если Вы не желаете вводить каждый раз пароль пользователя для подключения к каким-то ресурсам, то можно сделать пароль в «**Связке ключей**» пустым и тогда данный запрос больше не будет вас беспокоить.

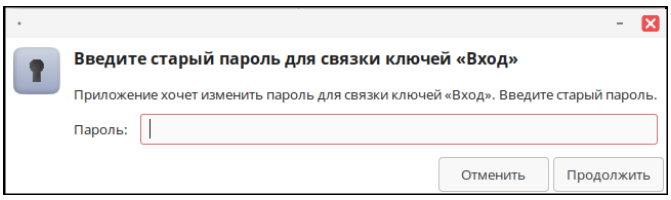
Есть 3 варианта, как сделать пароль в «**Связке ключей**».

1 вариант

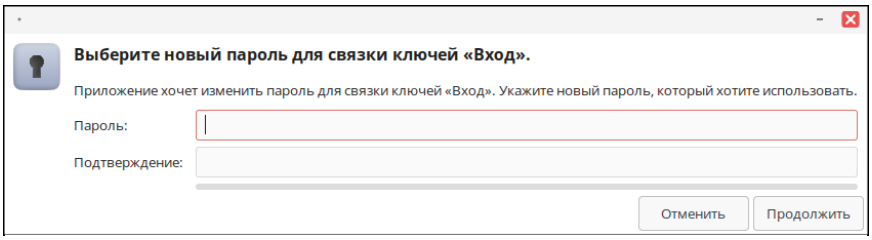
1. Откройте «**Меню**» — «**Стандартные**» — «**Пароли и ключи**».

2. Щелкните правой кнопкой мыши на «**Вход**» и выберите «**Изменить пароль**».

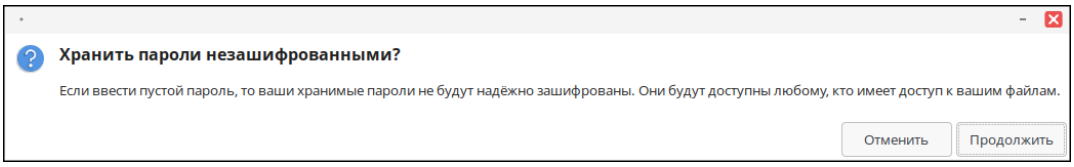
3. Введите старый пароль (пароль пользователя).



4. При вводе нового пароля, оставьте поля пустыми, таким образом он не будет назначен.



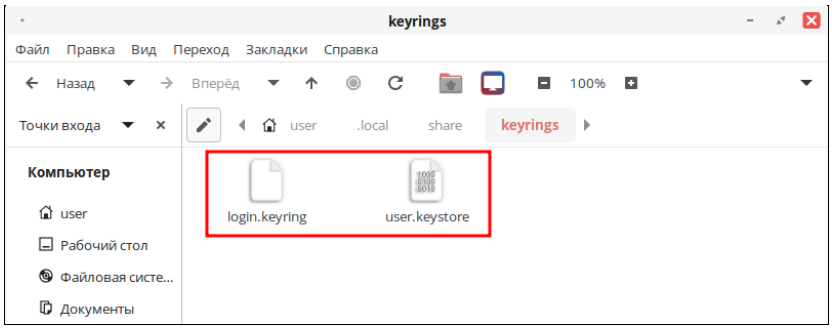
5. На данный запрос выберите «**Продолжить**».



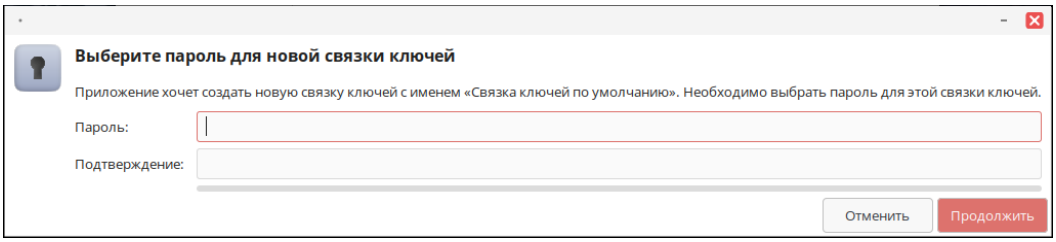
После проделанных действий запрос на ввод пароля для разблокировки связки ключей не должен появиться.

2 вариант

Необходимо через файловый менеджер удалить содержимое скрытого каталога **/home/user/.local/share/keyrings/**. Убедитесь, что включена опция отображения скрытых файлов. Для включения показа скрытых файлов откройте файловый менеджер, перейдите в меню «**Вид**» и установите флаг «**Показывать скрытые файлы**». Затем перейдите в указанный каталог и удалите все файлы внутри него.



После перезапуска приложения появится окно, в котором необходимо установить новый пароль.

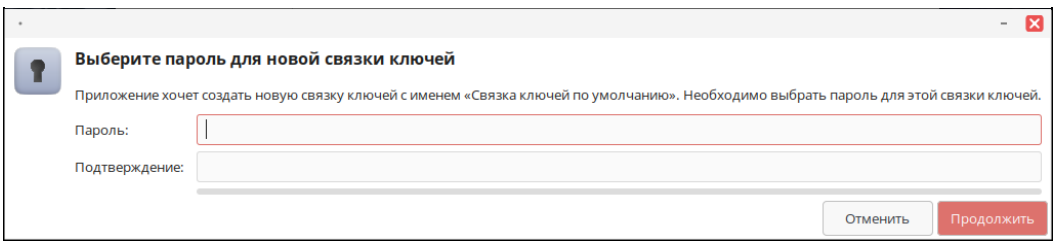


3 вариант

Для сброса настроек (удаление всех паролей и создание новой цепочки ключей) откройте терминал и введите команду:

```
rm ~/.local/share/keyrings/*
```

После перезапуска приложения будет запрошен новый пароль.



Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012

Задание хешей паролей в системах, использующих authconfig
Задание хешей паролей в системах, использующих authselect

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для включения поддержки шифрования ГОСТ в **OpenSSL** необходимо установить пакет **openssl-gost-engine**.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install openssl-gost-engine
```

Задание хешей паролей в системах, использующих authconfig

Для настройки задания хешей паролей в соответствии с **ГОСТ Р 34.11-2012** в системах, использующих **authconfig**, необходимо выполнить команду:

```
openssl-switch-passhash gost
```

Для проверки настройки установите новый пароль пользователю:

```
passwd <username>
```

Затем проверьте алгоритм хеша пароля командой:

```
passwd -S <username>
```

В выводе консоли видно, что до внесения настроек алгоритм определялся «**SHA512**», после — «**gost-yescrypt**» (**ГОСТ Р 34.11-2012**):

```
passwd -S user

user PS 2022-03-04 0 99999 7 -1 (Пароль задан, шифр SHA512)

openssl-switch-passhash gost
passwd user

Изменение пароля пользователя user.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.

passwd -S user

user PS 2022-03-04 0 99999 7 -1 (Пароль задан, шифр gost-yescrypt)
```

Для того чтобы установить для паролей алгоритм хеширования «**SHA512**», как было в настройках по умолчанию, выполните команду:

```
openssl-switch-passhash default
```

Задание хешей паролей в системах, использующих authselect

Проверьте текущий метод шифрования:

```
passwd -S <username>

<username> PS 2023-11-13 0 99999 7 -1 (Пароль задан, шифр Yescrypt)
```

Проверьте текущий профиль и включенные функции:

```
authselect current

Идентификатор профиля: sssd
Включенные функции:
- with-fingerprint
- with-silent-lastlog
```

Проверьте текущий метод шифрования в текущем профиле:

```
authselect test sssd | grep -e '^password.*pam_unix.so'

password    sufficient    pam_unix.so yescrypt shadow nullok use_authtok
password    sufficient    pam_unix.so yescrypt shadow nullok use_authtok
```

Создайте новый профиль на базе текущего с именем, например, **gost-yescrypt**:

```
authselect create-profile gost-yescrypt --base-on=sssd

Новый профиль создан в /etc/authselect/custom/gost-yescrypt
```

Измените в новом профиле метод шифрования паролей пользователей на **gost_yescrypt**:

```
sed -i 's/\byescrypt\b/gost_yescrypt/' /etc/authselect/custom/gost-yescrypt/password-auth
sed -i 's/\byescrypt\b/gost_yescrypt/' /etc/authselect/custom/gost-yescrypt/system-auth
```

Выберите новый профиль с функциями, которые были в предыдущем профиле:

```
authselect select custom/gost-yescrypt with-fingerprint with-silent-lastlog

Выбран профиль «custom/gost-yescrypt».
Следующие карты nsswitch перезаписаны профилем:
- passwd
- group
- netgroup
- automount
- services

Make sure that SSSD service is configured and enabled. See SSSD documentation for more information.

- with-fingerprint is selected, make sure fprintd service is configured and enabled
```

Примените внесенные изменения:

```
authselect apply-changes

Изменения успешно применены.
```

Проверьте установленные параметры:

```
authselect current

Идентификатор профиля: custom/gost-yescrypt
Включенные функции:
- with-fingerprint
- with-silent-lastlog

authselect test custom/gost-yescrypt | grep -e '^password.*pam_unix.so'

password    sufficient    pam_unix.so gost_yescrypt shadow nullok use_authtok
password    sufficient    pam_unix.so gost_yescrypt shadow nullok use_authtok
```

Задайте пароль пользователю:

```
passwd <username>

Изменение пароля пользователя <username>.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Проверьте метод шифрования:

```
passwd -S <username>

<username> PS 2023-11-13 0 99999 7 -1 (Пароль задан, шифр GOST Yescrypt)
```

Для возврата к профилю по умолчанию выберите прежний профиль с функциями:

```
authselect select sssd with-fingerprint with-silent-lastlog

Выбран профиль «sssd».
Следующие карты nsswitch перезаписаны профилем:
- passwd
- group
- netgroup
- automount
- services

Make sure that SSSD service is configured and enabled. See SSSD documentation for more information.

- with-fingerprint is selected, make sure fprintd service is configured and enabled
```

И примените изменения:

```
authselect apply-changes

Изменения успешно применены.
```

Новые пароли будут шифроваться в соответствии с выбранным профилем.

Менеджер паролей keepassxc

Установка
Создание новой базы данных
Добавление учетных данных
Настройки приложения
Включение SSH-агента в KeePassXC
Добавление RSA-ключа в базу KeePassXC
Проверка работы приложения

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** keepassxc-2.7.6-3

Keepassxc - это современный, безопасный менеджер паролей с открытым исходным кодом, который хранит и управляет вашей конфиденциальной информацией. Он сохраняет множество различных типов информации, таких как имена пользователей, пароли, URL-адреса, вложения и заметки в автономном зашифрованном файле, который может храниться в любом месте, включая частные и общедоступные облачные решения.

Вы можете подробнее ознакомиться с работой менеджера паролей **keepassxc**, просмотрев наши обучающие видео:

- на **RuTube** — Менеджер паролей KeePassXC;
- в **Яндекс.Дзен** — Менеджер паролей KeePassXC;
- в **VK Видео** — Менеджер паролей KeePassXC.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

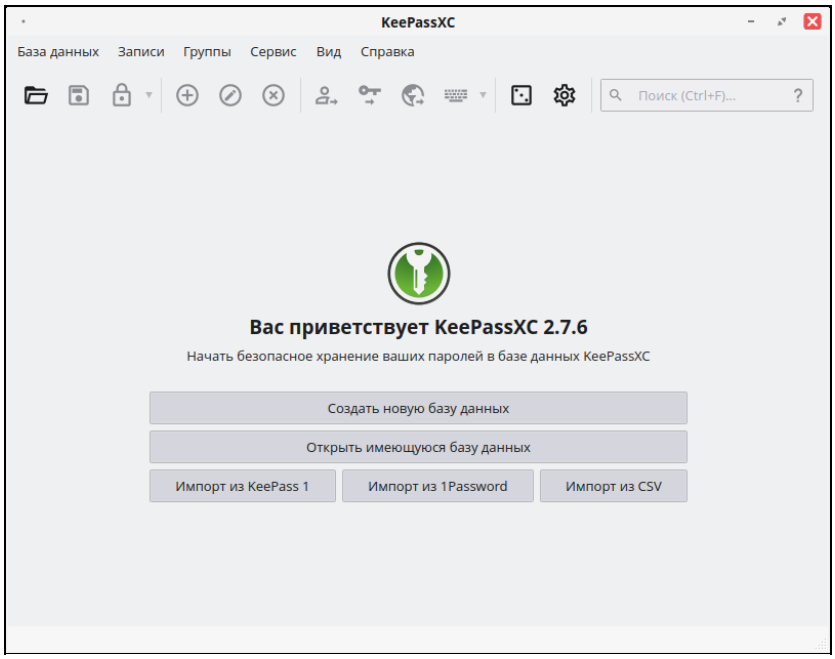
и выполните команду:

```
dnf install keepassxc
```

После установки приложение можно запустить из «**Главного меню**» — «**Стандартные**» — «**KeePassXC**» либо выполнив в терминале команду:

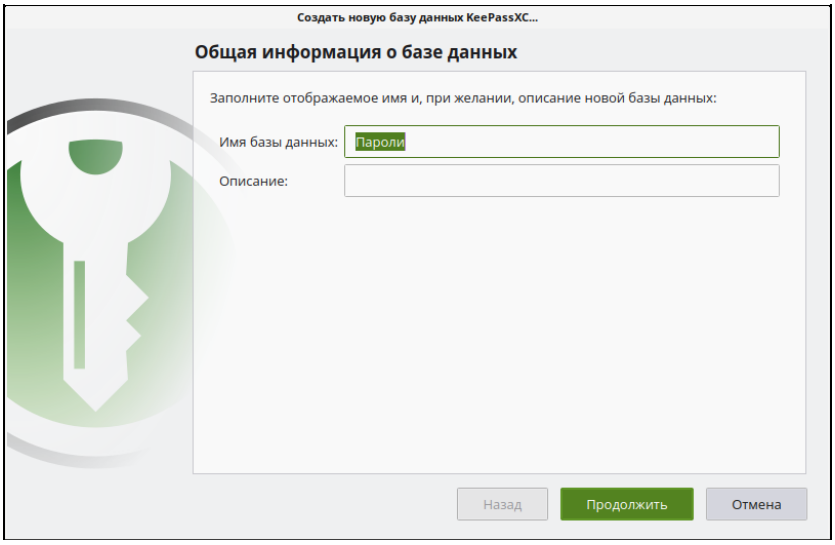
```
keepassxc
```

Главное окно программы выглядит следующим образом:

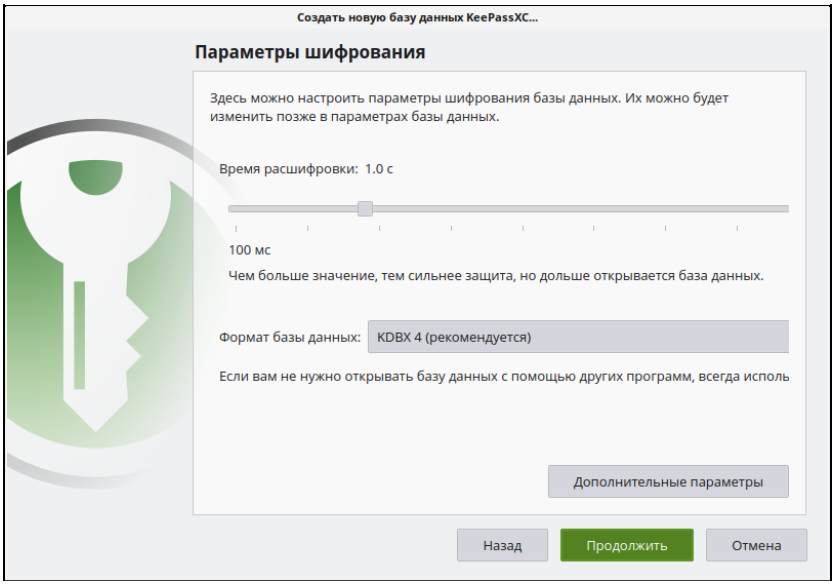


Создание новой базы данных

В окне «**Создать новую базу данных**» предлагается ввести название базы данных и ее описание.

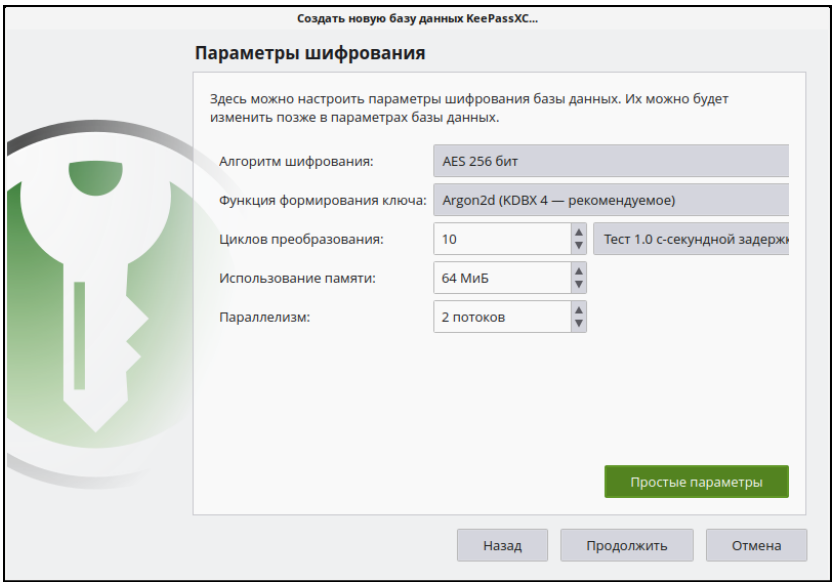


Далее в «**Параметрах шифрования**» можно задать время расшифровки. В дальнейшем, после создания базы, можно будет изменить данные параметры.

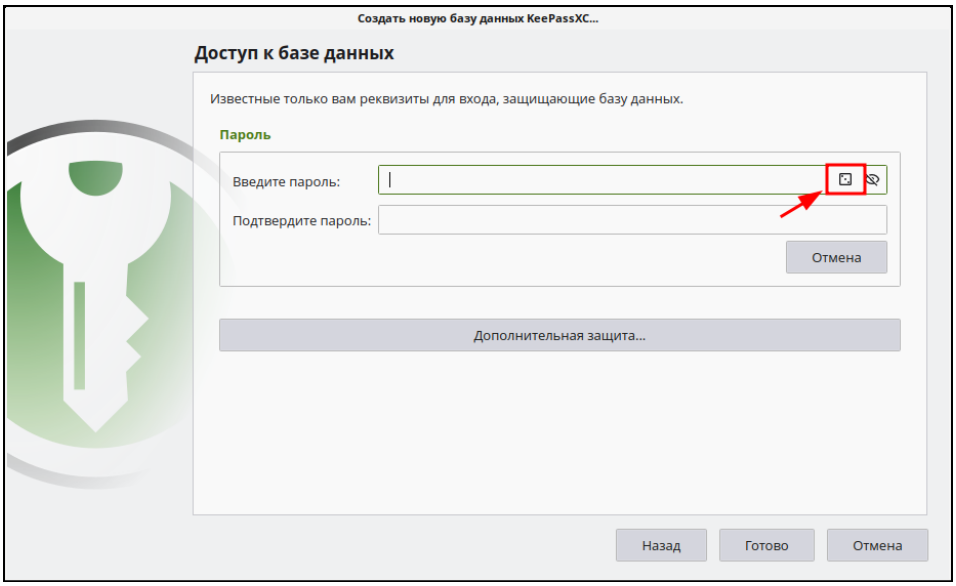


Также можно изменить формат шифрования базы данных, если это необходимо для совместимости с другими приложениями.

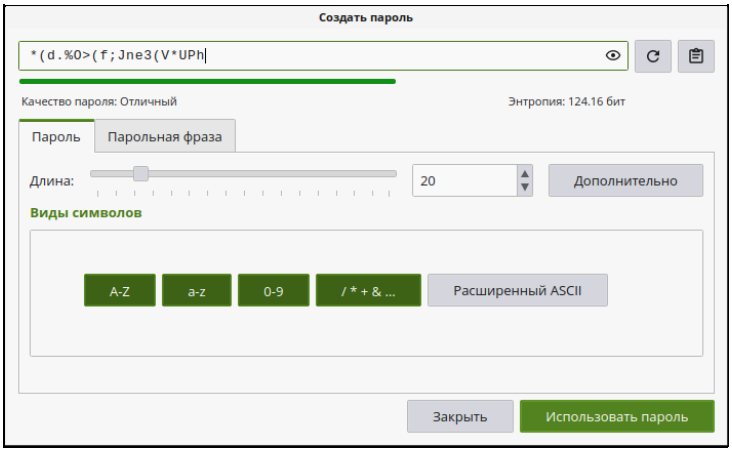
В «**Дополнительных параметрах**» можно усложнить настройки шифрования с помощью предложенных функций:



После установки параметров шифрования необходимо задать пароль для создаваемой базы. Можно как придумать собственный пароль, так и сгенерировать надежный пароль, нажав на кнопку генерации паролей.



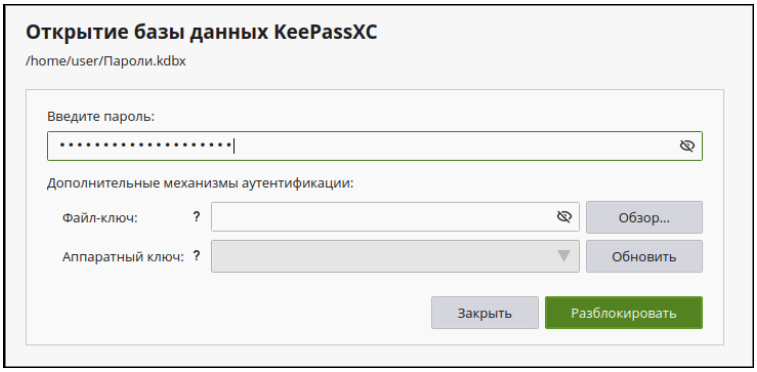
При использовании генератора паролей можно включить и выключить виды используемых символов и задать длину пароля.



ВАЖНО!

Не потеряйте пароль для базы данных. Потеря пароля может привести к невозможности разблокировать вашу базу данных, вы не сможете получить информацию, хранящуюся в ней.

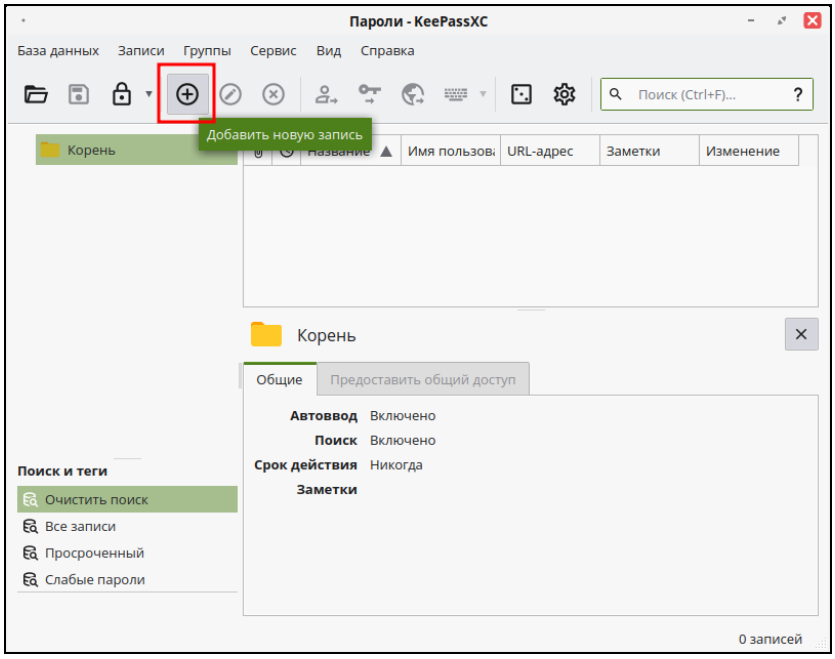
После создания базы можно открыть ее с помощью созданного пароля.



Открыв окно с базой данных, можно создать запись с учетными данными.

Добавление учетных данных

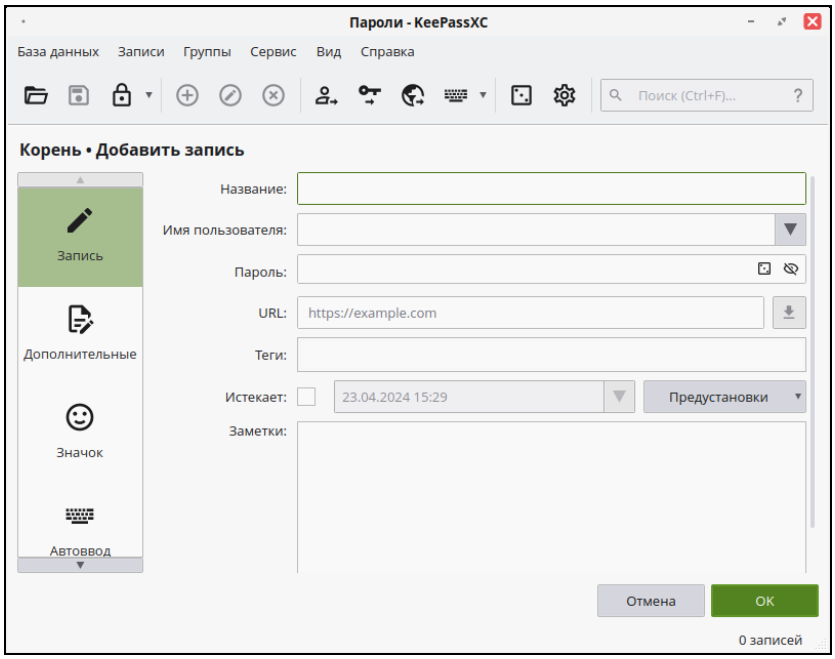
Для того чтобы создать новую запись, нажмите «**Добавить новую запись**» на панели инструментов:



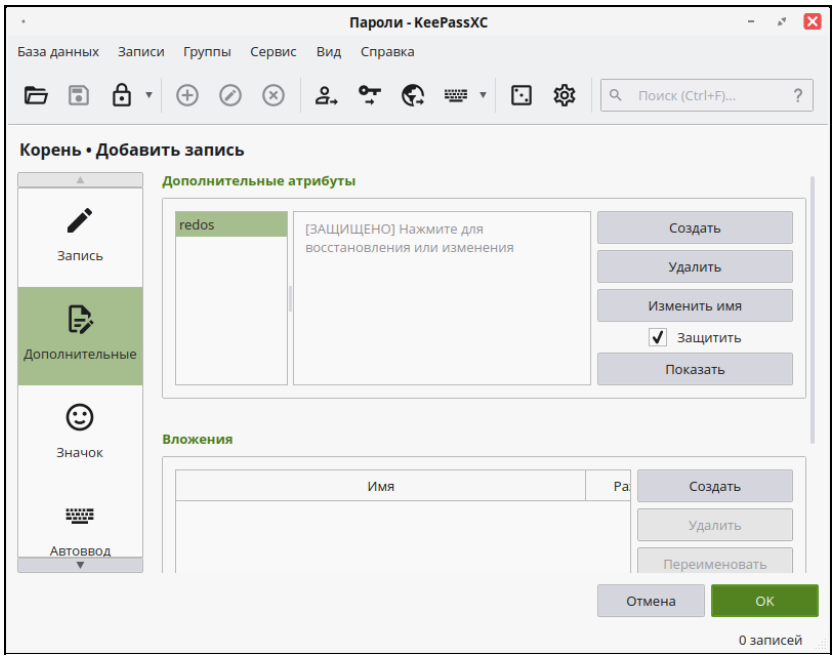
В разделе «**Запись**» указываются название приложения или сайта, где будут использоваться данные, имя пользователя, пароль и URL-адрес ресурса.

В поле «**Пароль**» можно указать собственный пароль или воспользоваться генератором.

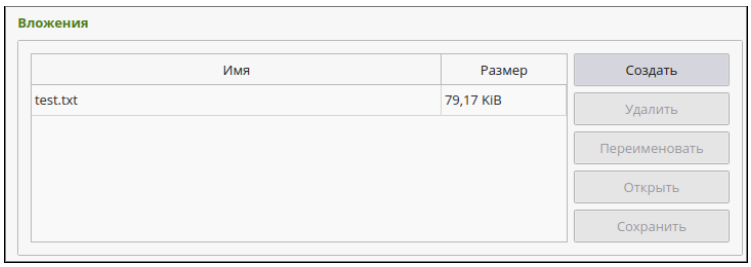
Также можно задать срок окончания действия записи и оставить примечания.



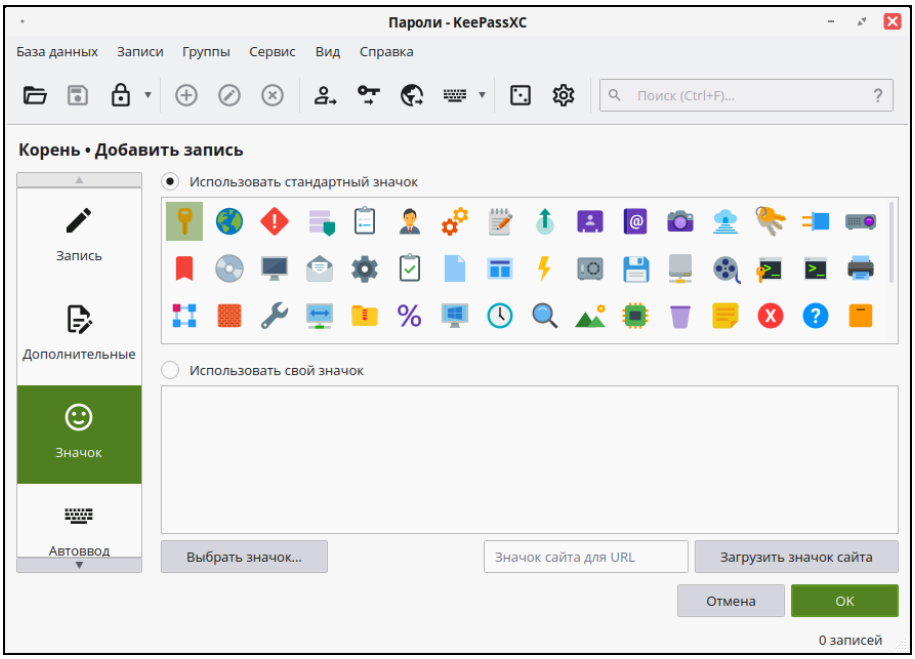
В разделе «**Дополнительные**» можно добавить информацию об учетной записи. Например, ответ на контрольный вопрос для восстановления пароля или любую другую произвольную информацию, которую можно скопировать в буфер обмена или использовать вместе с автовводом.



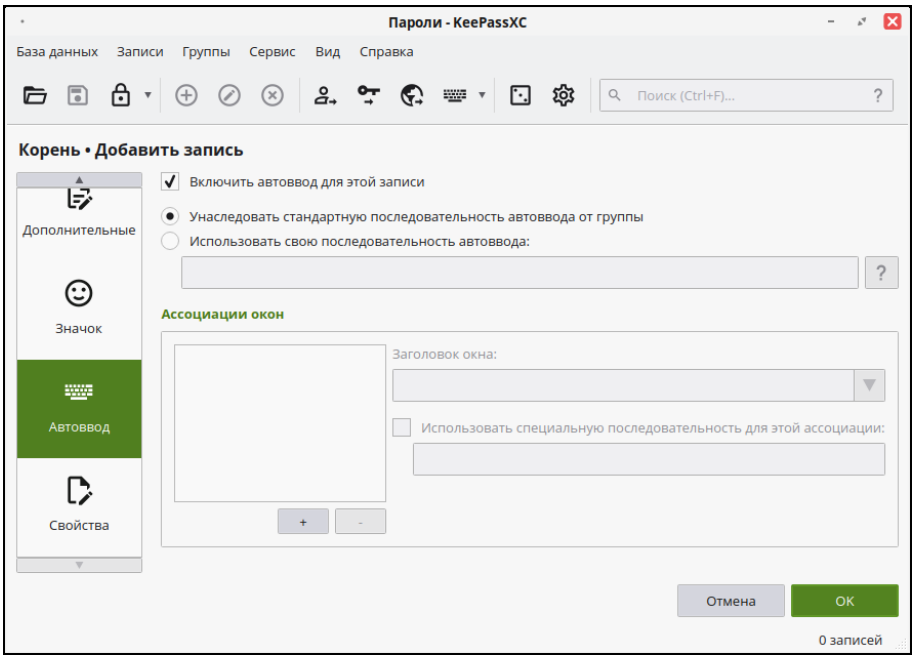
Также в данном разделе можно прикрепить файлы к записи. Эти файлы добавляются в базу данных и хранятся как зашифрованные бинарные файлы. Файлы можно открыть из этого же меню.



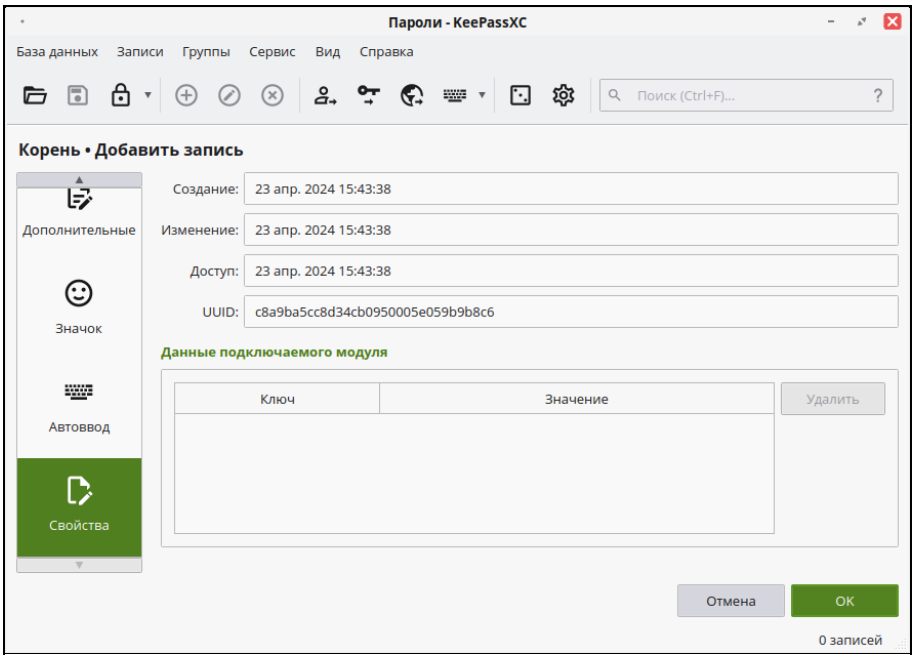
В разделе «**Значок**» можно выбрать значок для вашей записи из стандартных либо добавить свой:



Для каждой созданной записи можно включить автоввод данных. Для этого необходимо перейти в раздел «**Автоввод**» и установить соответствующий флажок:



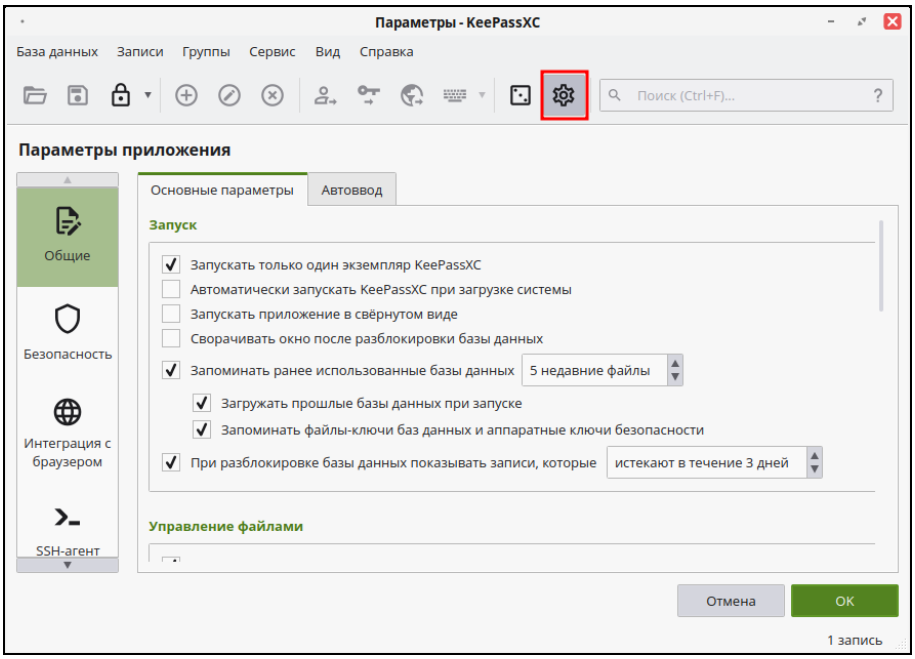
На вкладке «**Параметры**» отображаются дата и время создания, изменения и последнего просмотра этой записи, а также ее уникальный идентификатор.



После ввода всех необходимых данных нажмите кнопку «**OK**», и запись будет создана.

Настройки приложения

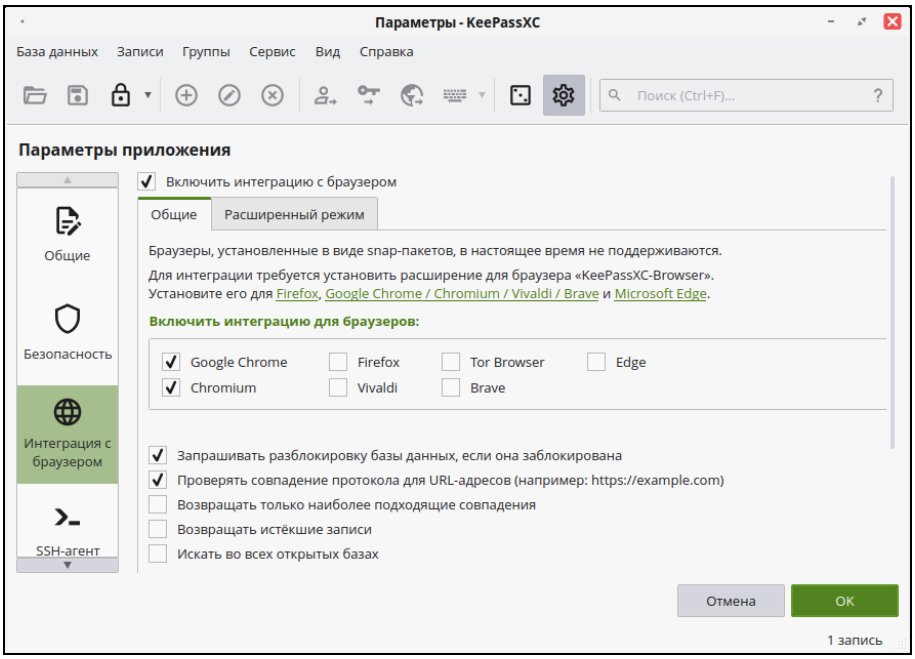
Теперь перейдем в настройки приложения с помощью кнопки «**Параметры**» на верхней панели инструментов и рассмотрим основные опции.



На вкладке «**Общее**» настраиваются параметры запуска приложения, управления файлами и записями, а также настройки интерфейса. Также здесь расположены дополнительные настройки автоввода.

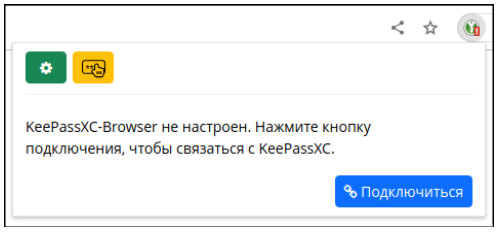
Вкладка «**Безопасность**» содержит настройки блокировки базы данных в различных ситуациях. Например, блокировка сессии пользователя или сворачивания окна.

Следующая вкладка позволяет настроить интеграцию с браузерами.

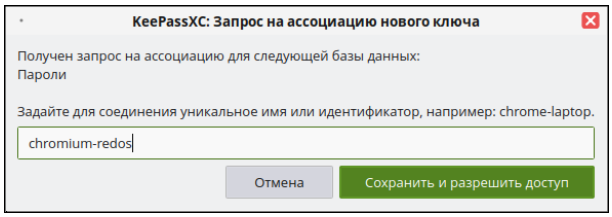


Для этого необходимо проставить соответствующие флажки и установить расширение **KeePassXC-Browser**, ссылки на который находятся в этом же окне.

После установки расширения в браузер необходимо связать его с программой **KeePassXC**. Нажмите кнопку «**Подключиться**».



После этого задайте имя для ключа соединения:



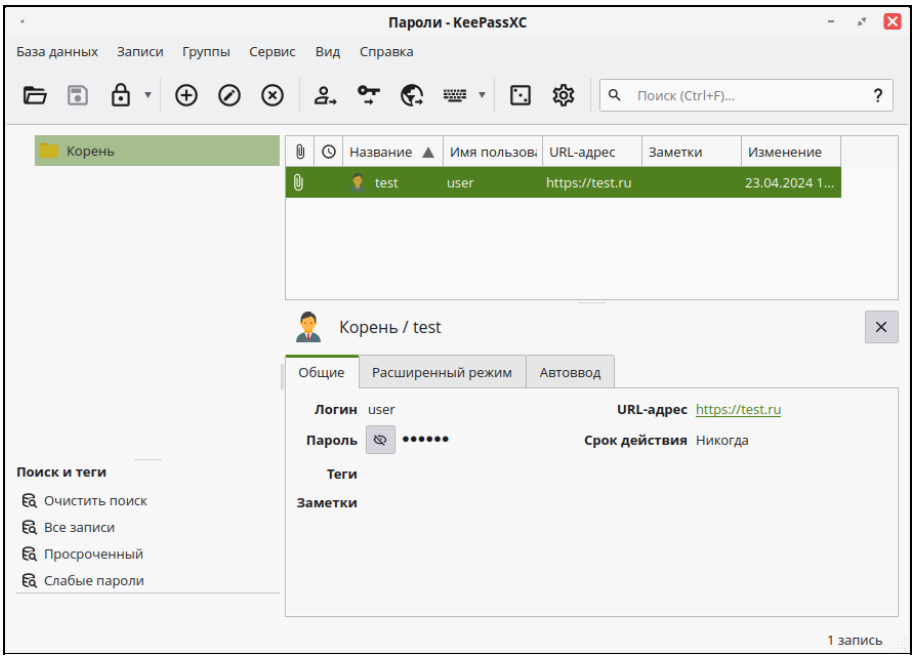
Основные элементы для работы с сохраненными данными находятся на верхней панели инструментов:

1. Скопировать логин в буфер обмена.

2. Скопировать пароль в буфер обмена.

3. Скопировать URL-адрес в буфер обмена.

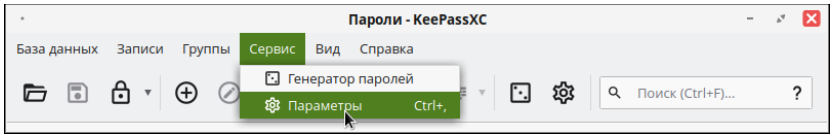
4. Выполнить автоввод.



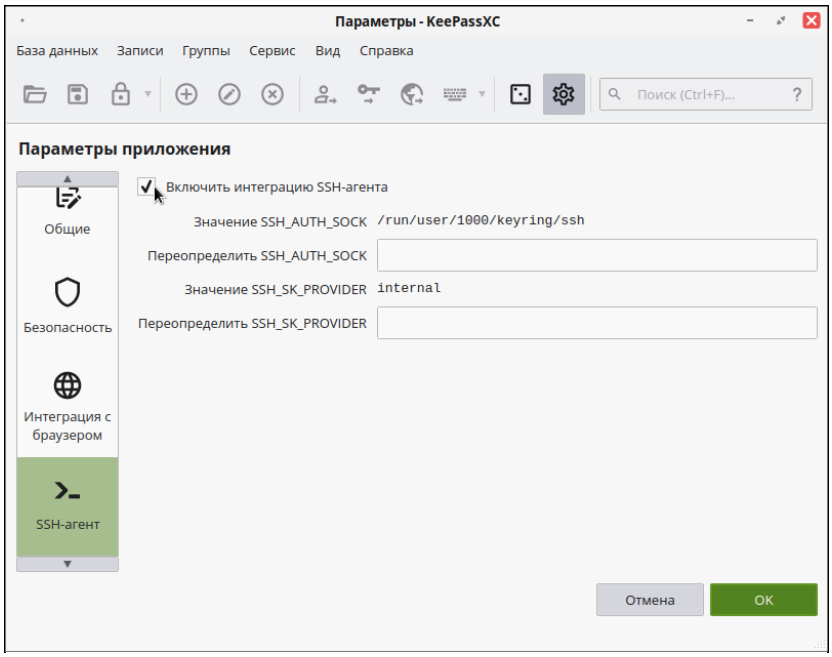
При использовании автоввода логин и пароль будут подставлены в предыдущем открытом приложении в соответствии с настройками автоввода. По умолчанию это последовательность `{USERNAME}{TAB}{PASSWORD}{ENTER}`.

Включение SSH-агента в KeePassXC

В панели инструментов нажмите «**Сервис**» и в контекстном меню выберете «**Параметры**».

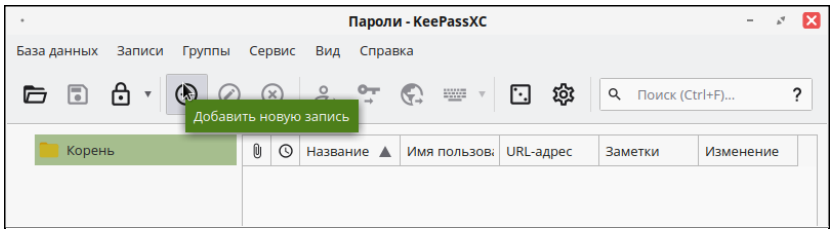


Перейдите на складку «**SSH-агент**», установите флаг «**Включить интеграцию SSH-агента**» и подтвердите настройки нажатием кнопки «**OK**».

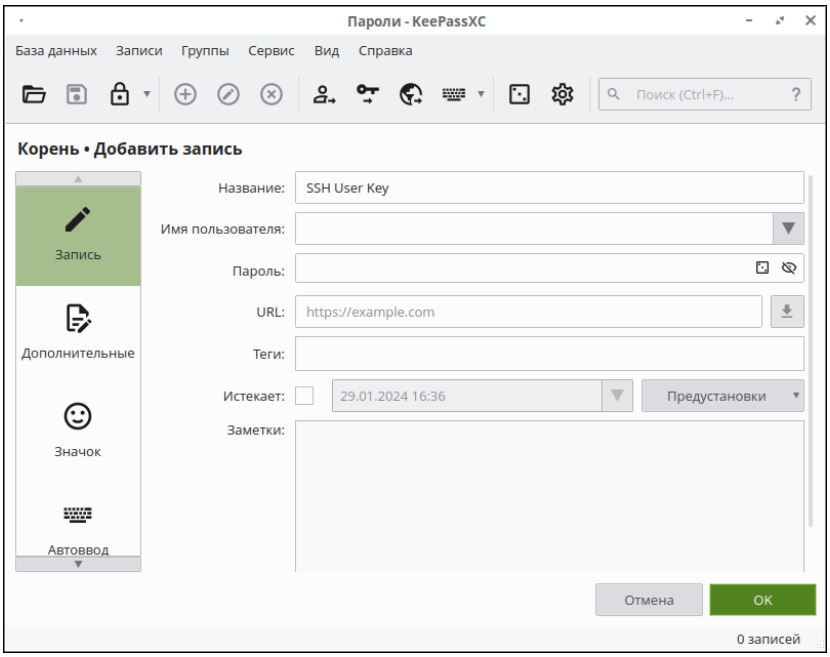


Добавление RSA-ключа в базу KeePassXC

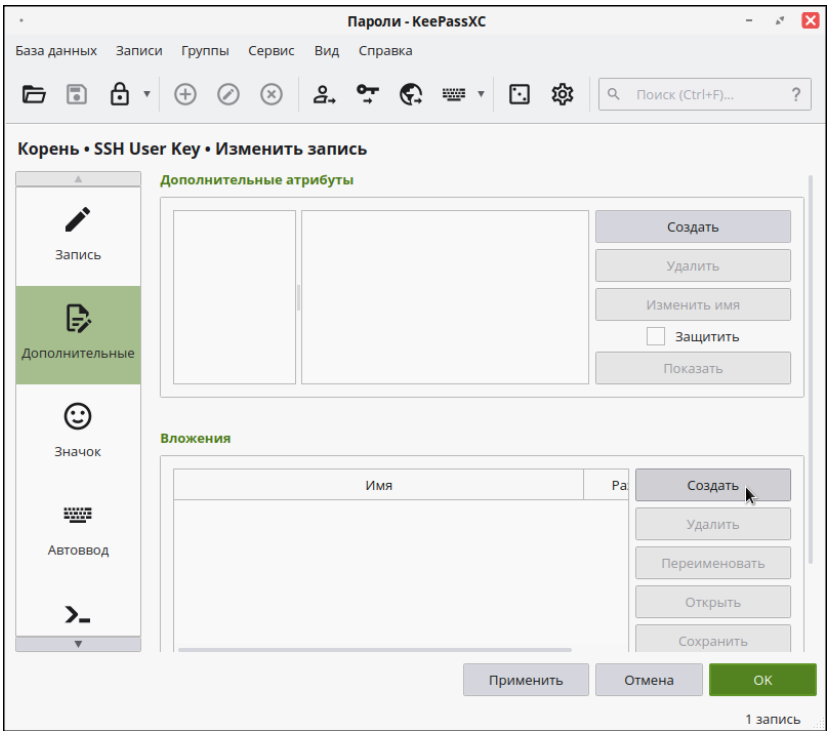
Для добавления новой записи в панели инструментов нажмите на кнопку «**+**».



Укажите название записи и пароль. Если пароль ранее не создавался, оставьте поле пустым.



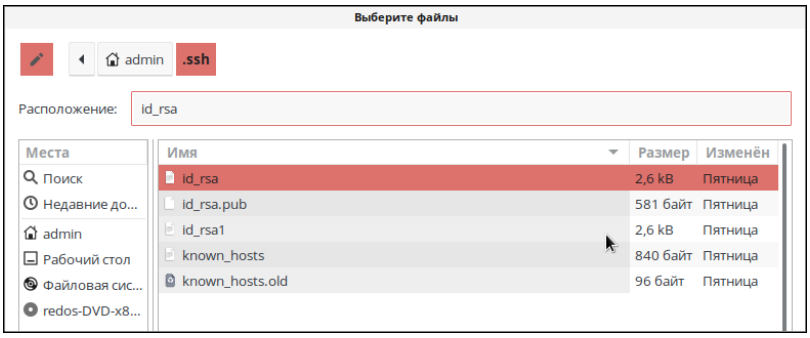
Далее перейдите на вкладку «**Дополнительные**» и в секции «**Вложения**» нажмите «**Создать**».



В открывшемся диалоговом окне укажите путь до закрытой части ключа.

ВАЖНО!

В РЕД ОС каталоги, начинающиеся с точки (**/.ssh**, **/.local** и пр.) определяются графическими оболочками как скрытые. Закрытый ключ по умолчанию расположен в каталоге **/.ssh**. Для отображения скрытых элементов нажмите ПКМ по пустому месту поля выбора файла и установите флаг для параметра «**Показывать скрытые файлы**».

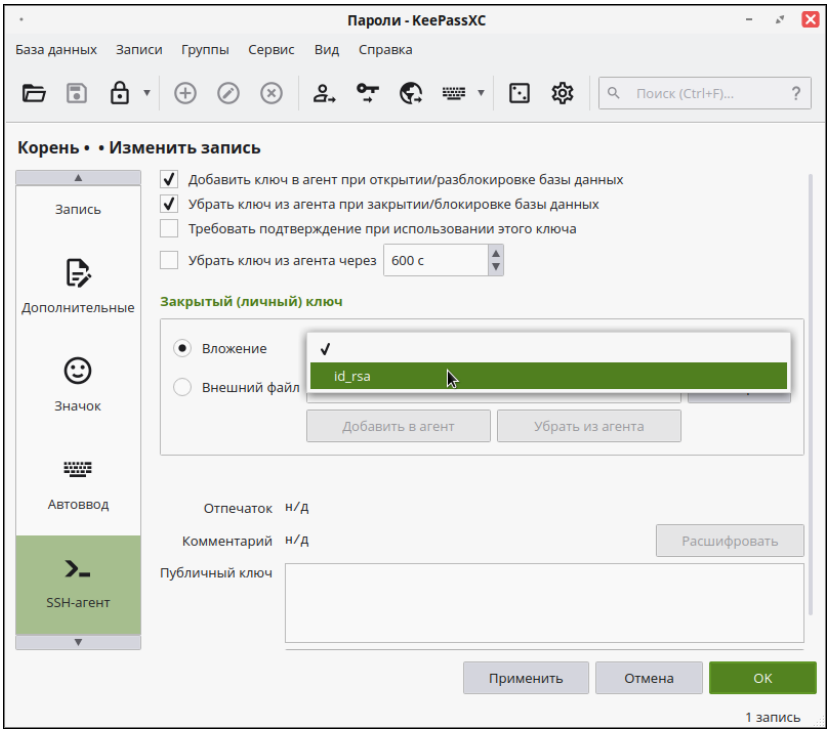


После загрузки закрытого ключа перейдите на вкладку «**SSH-агент**» и в секции «**Закрытый (личный) ключ**» отметьте параметр «**Вложения**». В списке выберите загруженный закрытый ключ.

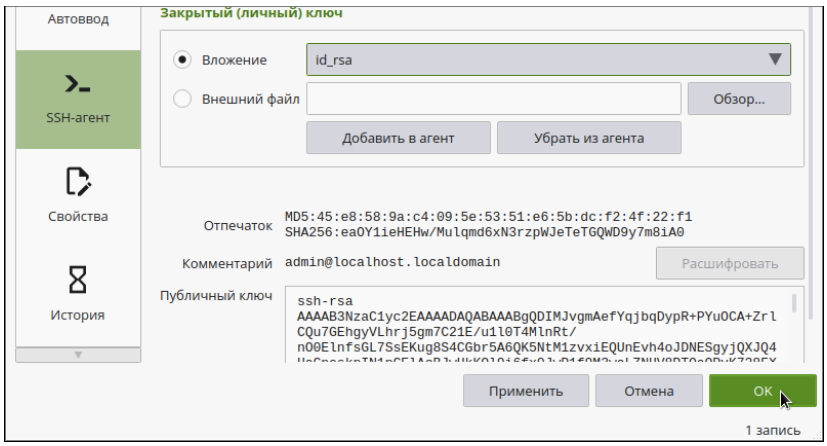
Дополнительно необходимо установить флаги для параметров «**Добавить ключ в агент при открытии/разблокировке базы данных**» и «**Убрать ключ из агента при закрытии/блокировке базы данных**».

Параметр «**Добавить ключ в агент при открытии/разблокировке базы данных**» отвечает за доступность закрытого ключа при запуске приложения. Если параметр не активен, ключ будет недоступен.

Параметр «**Убрать ключ из агента при закрытии/блокировке базы данных**» отвечает за доступность закрытого ключа после закрытия приложения. Если параметр не активен, ключ будет доступен даже после закрытия приложения до выхода из сеанса.



Ниже будет выведена информация о ключе. Для применения изменений нажмите «**OK**» и перезапустите приложение.



Ключ будет сохранен в базе данных **KeePassXC**. В дальнейшем **при запущенном приложении** можно будет осуществлять SSH-подключения вне зависимости от наличия и состояния оригинального файла ключа.

Проверка работы приложения

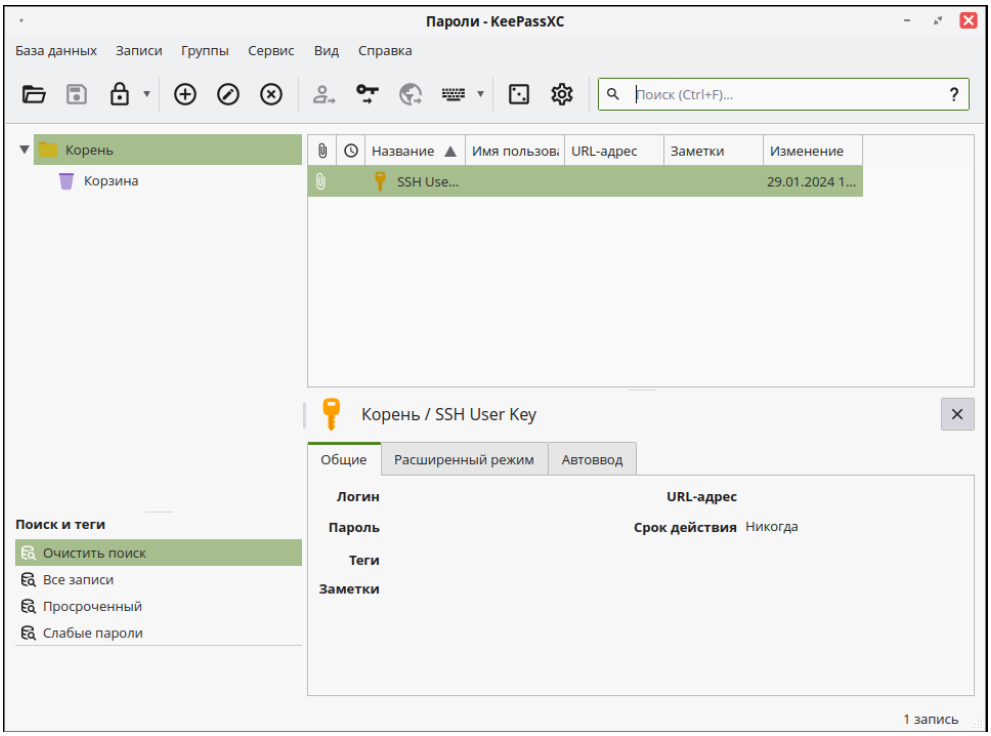
Для проверки работы командой mv переименуйте приватную часть ключа на клиентской машине (устройство, которое инициирует подключение):

```
mv ~/.ssh/id_rsa ~/.ssh/id_rsa1
```

Выполните подключение. При попытке подключения клиент SSH не находит переименованный ранее ключ, вследствие чего сервер предлагает авторизоваться по паролю.

```
ssh user@192.168.100.61

user@192.168.100.61's password:
```

Запустите **KeePassXC** и введите ранее установленный пароль приложения.



Выполните подключение. Обратите внимание на *имя пользователя* и *имя хоста* в командной строке. Если параметры изменились и соответствуют параметрам подключения, аутентификация прошла удачно. Приложение настроено верно.

```
[admin@localhost ~]$ ssh user@192.168.100.61
Last login: Mon Feb  5 11:47:11 2024 from 192.168.100.60
[user@server ~]$
```

Также стоит учитывать, что уже открытые SSH-соединения продолжат работу даже после закрытия приложения.

Работа с политиками Polkit

Polkit
Политики polkit
Правила polkit
Журналирование действий polkit
Примеры
Монтирование раздела и создание нового подключения без запроса пароля
Монтирование устройств с запросом пароля
Разрешение монтирования определённых usb-flash-накопителей
Изменение Network Manager для администратора
Polkit-правило разрешающее вносить изменения в утилиту управления принтерами без запроса пароля

Polkit

Polkit (прежнее название: PolicyKit) — библиотека для UNIX-подобных операционных систем. API библиотеки используется для предоставления непривилегированным процессам возможности выполнения действий, требующих прав администратора. Использование Polkit противопоставляется использованию таких систем, как *sudo*, но не наделяет процесс пользователя правами администратора, а позволяет точно контролировать, что разрешено, а что запрещено.

Вы можете подробнее ознакомиться с работой политик **Polkit**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с политиками Polkit;
- в **Яндекс.Дзен** — Работа с политиками Polkit;
- в **VK Видео** — Работа с политиками Polkit.

На наших каналах вы также сможете найти много другой полезной информации.

Политики polkit

Все политики находятся в ***/usr/share/polkit-1/actions/*** в формате **.policy*. Каждая политика представляет собой xml-файл, в котором описываются запросы к *polkit*. Каждый запрос имеет три условия, прописанных в секции *defaults*:

1. Запрос от любого пользователя. Тег *<allow_any>*;
2. Запрос от неактивного (заблокированного при создании) пользователя. Тег *<allow_inactive>*;
3. Запрос от активного пользователя *<allow_active>*.

Внутри каждого тега прописывается возвращаемое значение. Используются следующие варианты значений:

- **yes** - предоставить разрешения;
- **no** - заблокировать разрешения;
- **auth_self** - пользователь должен ввести свой пароль для аутентификации;
- **auth_self_keep** - пользователь должен ввести свой пароль для аутентификации один раз за сессию, разрешение предоставляется для всей сессии;
- **auth_admin** - пользователь должен ввести пароль *admin* при каждом запросе;
- **auth_admin_keep** - пользователь должен ввести пароль *admin*, разрешение предоставляется для всей сессии.

admin - в РЕД ОС определён в правиле **/etc/polkit-1/rules.d/50-default.rules**:

```
polkit.addAdminRule(function(action, subject)
{
return ["unix-user:root"];
});
```

Правила polkit

Менять напрямую политики нельзя, так как при обновлении системы они будут удалены. Необходимо создавать собственные правила в **/etc/polkit-1/rules.d/** в формате ***.rules**. Правила выполняются в порядке названия по алфавиту, поэтому вначале пишутся цифры, чтобы указать приоритет правила. Алгоритм создания правила (все действия выполняются с правами пользователя **root**):

1. Сначала определяем, какую политику мы хотим изменить, для этого находим в */usr/share/polkit-1/actions/* требуемую.
2. Редактируем новый файл с политикой:

```
nano /etc/polkit-1/rules.d/99-vashe_pravilo.rules
```

3. Вставляем следующий текст:

```
polkit.addRule(function(action, subject)
{
if (action.id == "policy" && <ваше_условие>)
{
return polkit.Result.YES;
};
});
```

где

- вместо ***99*** подставляем нужное число (файлы с политиками просматриваются в лексикографическом порядке, 99 будет последним правилом);
- вместо ***policy*** пишем название политики, поведение которой нужно изменить;
- вместо ***<ваше_условие>***:
  - если необходимо изменить поведение политики для одного конкретного пользователя, пропишите `subject.user == "<имя_пользователя>"`,
  - если необходимо изменить поведение политики для нескольких пользователей, входящих в одну группу как локальную, так и доменную, пропишите `subject.isInGroup("<название_группы>")`.

    Например, для локальной группы **local**, в которую входят пользователи *user1*, *user2* и *user3*, указывается правило вида `subject.isInGroup("local")`; для доменной группы, в которую входят пользователи *dom_user1*, *dom_user2* и *dom_user3*, указывается правило вида `subject.isInGroup("пользователи домена")`. По желанию для конкретных пользователей домена, которым необходимо настроить доступ или правило, можно создать отдельную группу и поместить в неё нужных пользователей, в таком случае в правиле следует прописать `subject.isInGroup("<название_новой_отдельной_группы_доменных_пользователей>")`.

- ***Result.YES*** означает, что политика при выполнении условия правила будет предоставлять разрешение.

Журналирование действий polkit

Используя правила polkit, можно также делать записи в системный журнал. Метод **log()** записывает сообщение в системный журнал. Пример:

```
polkit.addRule(function(action, subject)
{
if (action.id == "действие")
{
polkit.log("action=" + action);
polkit.log("subject=" + subject);
};
});
```

В параметре *action* передается объект с информацией о совершенном процессе и связанные с этим действием параметры (например, если запрошенное действие - *монтирование съемного диска*, то в параметре **action** будут переданы *серийный номер* диска, его *id*, *файловая система* и т.д.).

В параметре *subject* передается объект с информацией о пользователе, запустившем процесс. Этот объект имеет следующие атрибуты:

- **id** – идентификатор процесса;
- **user** – имя пользователя;
- **groups** – список групп, в которые входит пользователь;
- **seat** – местонахождение субъекта (пустое значение, если местонахождение не локальное);
- **session** – сессия субъекта;
- **local** – true, только если местонахождение имеет локальный характер;
- **active** – true, только если сеанс активен.

Примеры

Пользователи часто сталкиваются с необходимостью вводить пароль при монтировании разделов в файловом менеджере и создании нового подключения в NetworkManager, а также невозможностью извлечения usb-flash-накопителей или лотка оптического привода. За эти разрешения отвечают схемы, в которых описаны определенные доступные действия, предустановленные разработчиком ПО:

- *org.freedesktop.udisks2.filesystem-mount-system* — разрешение на монтирование файловых систем системных устройств;

- *org.freedesktop.udisks2.filesystem-mount-other-seat* — разрешение на монтирование файловых систем с устройств, подключенных в другое место;
- *org.freedesktop.udisks2.eject-media-other-seat* — разрешение на извлечение лотка оптического привода;
- *org.freedesktop.udisks2.power-off-drive-other-seat* — разрешение на извлечение usb-flash;
- *org.freedesktop.NetworkManager.settings.modify.system* — разрешение на создание и модификацию системных сетевых соединений.

Монтирование раздела и создание нового подключения без запроса пароля

Настроим правила для пользователя, находящегося в системной группе **xgrp**, таким образом, чтобы запросы пароля не выполнялись для монтирования раздела и создания нового подключения. Для этого необходимо выполнить следующий алгоритм действий (все действия выполняются с правами пользователя **root**):

1. Наполним **/etc/polkit-1/rules.d/99-udisk2_mount.rules** следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (
(action.id == "org.freedesktop.udisks2.filesystem-mount-system" ||
action.id == "org.freedesktop.udisks2.filesystem-mount-other-seat" ||
action.id == "org.freedesktop.udisks2.eject-media-other-seat" ||
action.id == "org.freedesktop.udisks2.power-off-drive-other-seat")
&& subject.isInGroup("xgrp")
)
{
return polkit.Result.YES;
};
});
```

Указанная в созданном правиле группа **xgrp** используется в качестве примера. При настройке правила необходимо указать название **вашей** группы или имени пользователя в зависимости от требований:

- если необходимо изменить поведение политики для одного конкретного пользователя, пропишите `subject.user == "<имя_пользователя>"`,
- если необходимо изменить поведение политики для нескольких пользователей, входящих в одну группу как локальную, так и доменную, пропишите `subject.isInGroup("<название_группы>")`.

  Например, для локальной группы **local**, в которую входят пользователи *user1*, *user2* и *user3*, указывается правило вида `subject.isInGroup("local")`; для доменной группы, в которую входят пользователи *dom_user1*, *dom_user2* и *dom_user3*, указывается правило вида `subject.isInGroup("пользователи домена")`. По желанию для конкретных пользователей домена, которым необходимо настроить доступ или правило, можно создать отдельную группу и поместить в неё нужных пользователей, в таком случае в правиле следует прописать `subject.isInGroup("<название_новой_отдельной_группы_доменных_пользователей>")`.

2. Наполним **/etc/polkit-1/rules.d/99-networkmanager.rules** следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (action.id == "org.freedesktop.NetworkManager.settings.modify.system" && subject.isInGroup("xgrp"))
{ return polkit.Result.YES; };
});
```

3. Создадим системную группу **xgrp** (если её ещё нет):

```
groupadd -r xgrp
```

4. Добавим пользователя в группу **xgrp**:

```
gpasswd -a <имя_пользователя> xgrp
```

5. Перезапустим политики *Polkit*:

```
systemctl restart polkit
```

Монтирование устройств с запросом пароля

Рассмотрим пример создания правила, разрешающего пользователю выполнять монтирование и извлечение устройств с запросом пароля (при указании **polkit.Result.AUTH_SELF** — будет запрошен пароль текущего пользователя, **polkit.Result.AUTH_ADMIN** — администратора). Также рассмотрим добавление записи в системный журнал при подключении съемного устройства о том, какое устройство было подключено и каким пользователем.

1. Наполним **/etc/polkit-1/rules.d/99-udisk2_mount.rules** следующим содержимым:

```
polkit.addRule(function(action, subject)
{
polkit.log("action "+ action);
polkit.log("subject "+ subject);
if (action.id == "org.freedesktop.udisks2.filesystem-mount-system")
{
return polkit.Result.AUTH_SELF;
};
if (action.id == "org.freedesktop.udisks2.filesystem-mount")
{
return polkit.Result.AUTH_SELF;
};
if (action.id == "org.freedesktop.udisks2.filesystem-mount-other-seats")
{
return polkit.Result.AUTH_SELF;
};
});
```

2. Перезапустим политики Polkit:

```
systemctl restart polkit
```

При монтировании USB-диска в системном журнале появятся записи:

```
action [Action id='org.freedesktop.udisks2.filesystem-mount' device='/dev/sdb1' polkit.message='Authentication is required to mount
$(drive)' partition.type='0x0b' partition.flags='0x00000000' drive='Kingston DataTraveler 3.0 (/dev/sdb1)' drive.revision='PMAP'
partition.number='1' partition.uuid='cc06b6d9-01' drive.serial='E0D55EA574BEE52129D21523' id.type='vfat' id.version='FAT32'
polkit.gettext_domain='udisks2' id.uuid='9BFA-18D3' drive.removable.media='thumb' drive.vendor='Kingston' drive.removable='true'
id.usage='filesystem' drive.removable.bus='usb' drive.model='DataTraveler 3.0']
```

Таким образом, в системном журнале зарегистрировано, что usb-диск с серийным номером *E0D55EA574BEE52129D21523* был подключен пользователем test.

Просмотреть факты подключения конкретного носителя можно, выполнив команду:

```
journalctl | grep "drive.serial='E0D55EA574BEE52129D21523'"
```

Разрешение монтирования определённых usb-flash накопителей

Создаём файл **/etc/polkit-1/rules.d/30-mount.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject) {
polkit.log("action "+ action);
if (action.id == "org.freedesktop.udisks2.filesystem-mount")
{
if (action.lookup("drive.serial") == "04GS1F3LBIBDWU05" || action.lookup("drive.serial") == "E0D55EA574BEE52129D21523 ")
return polkit.Result.YES;
else return polkit.Result.NO;
};
});
```

Во втором правиле можно указать:

- **AUTH_ADMIN** – разрешено с вводом пароля администратора;
- **NO** – не разрешено вообще.

В данном примере разрешается монтирование usb-flash-накопителей с файловой системой "**FAT32**" или серийным номером "**E0D55EA574BEE52129D21523**".

Основной список доступных параметров вы можете получить при подключении usb-flash-накопителя и просмотре содержимого журнала:

```
journalctl |grep "org.freedesktop.udisks2.filesystem-mount-system"
```

Или в статусе сервиса политик *Polkit*:

```
systemctl status polkit
```

Изменение Network Manager только для администратора

Создаём файл **/etc/polkit-1/rules.d/60-sysvinit-nm.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject) {
if (action.id=="org.freedesktop.NetworkManager.settings.modify.system")
{
return polkit.Result.AUTH_ADMIN;
}
});
```

Polkit-правило разрешающее вносить изменения в утилиту управления принтерами без запроса пароля

Создайте файл **/etc/polkit-1/rules.d/40-allow-printers.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (action.id == "org.opensuse.cupspkhelper.mechanism.all-edit") {
return polkit.Result.YES;
}
});
```

Ниже рассмотрено создание polkit-правила для **группы пользователей**, которое разрешает пользователям указанной группы вносить изменения в настройки утилиты по управлению принтерами (system-config-printer).
Создайте файл **/etc/polkit-1/rules.d/40-allow-changing-printers.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (action.id == "org.opensuse.cupspkhelper.mechanism.all-edit" && subject.isInGroup("users"))
{
return polkit.Result.YES;
}
});
```

Указанная в созданном правиле группа **users** используется в качестве примера. При настройке правила необходимо указать название **вашей** группы или имени пользователя в зависимости от требований:

- если необходимо изменить поведение политики для одного конкретного пользователя, пропишите `subject.user == "<имя_пользователя>"`,
- если необходимо изменить поведение политики для нескольких пользователей, входящих в одну группу как локальную, так и доменную, пропишите `subject.isInGroup("<название_группы>")`.

  Например, для локальной группы **local**, в которую входят пользователи *user1*, *user2* и *user3*, указывается правило вида `subject.isInGroup("local")`; для доменной группы, в которую входят пользователи *dom_user1*, *dom_user2* и *dom_user3*, указывается правило вида `subject.isInGroup("пользователи домена")`. По желанию для конкретных пользователей домена, которым необходимо настроить доступ или правило, можно создать отдельную группу и поместить в неё нужных пользователей, в таком

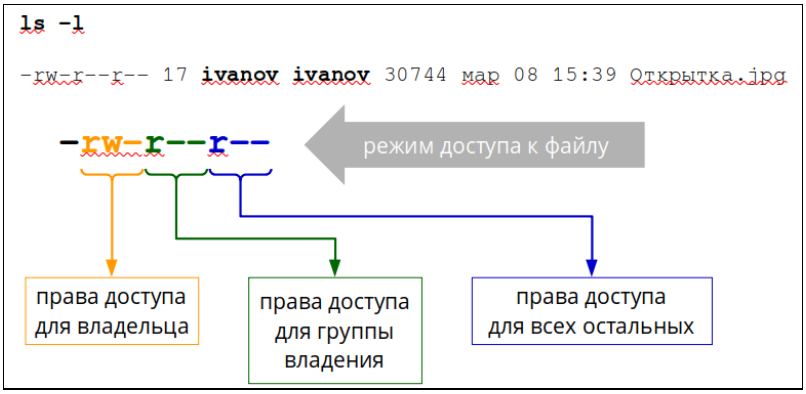
случае в правиле следует прописать `subject.isInGroup("<название_новой_отдельной_группы_доменных_пользователей>")`.

Списки контроля доступа ACL

Списки контроля доступа
Настройка списков доступа
Маска эффективных прав

Для того чтобы получить доступ к файлам в РЕД ОС, используются разрешения, которые назначаются трем объектам — *владельцу*, *группе* и *всем остальным*.

Просмотреть текущие права доступа можно, используя команду `ls -l`. Она выведет таблицу файлов в каталоге с некоторыми параметрами.



Управление обычными правами доступа возможно как из графического интерфейса, так и через консоль. Но есть расширенные права доступа, которые через графический интерфейс недоступны.

Списки контроля доступа

Для реализации сложных структур прав доступа на файловых системах в РЕД ОС используются расширенные права — **ACL** (*access control list* — списки контроля доступа), которые дают бóльшую гибкость, чем стандартный набор полномочий.

Поддержка ACL на файловых системах **ext4** и **XFS** включена по умолчанию. При необходимости можно отключить поддержку списков доступа, указав для выбранной файловой системы опцию «**noacl**» в файле **/etc/fstab**.

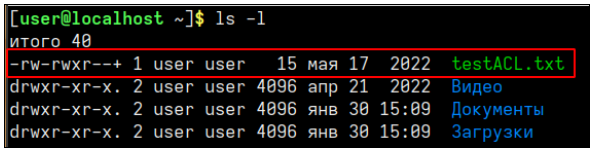
Система списков доступа ACL предоставляет дополнительные функциональные возможности ОС, **НО** у нее есть один недостаток — не все утилиты ее поддерживают. Следовательно, можно потерять настройки ACL при копировании или перемещении файлов, а программное обеспечение для резервного копирования может не выполнить резервное копирование настроек ACL.

Вы можете подробнее ознакомиться с настройкой списков контроля доступа ACL, просмотрев наши обучающие видео:

- на **RuTube** — Списки контроля доступа ACL (Access Control List);
- в **Яндекс.Дзен** — Списки контроля доступа ACL (Access Control List);
- в **VK Видео** — Списки контроля доступа ACL (Access Control List).

На наших каналах вы также сможете найти много другой полезной информации.

Если у файла или каталога установлены ACL, то в листинге будет отображаться знак «**+**». Команда `ls -l` не показывает никаких существующих ACL, она просто показывает «**+**» после списка разрешений, который указывает, что списки ACL применяются и к файлу.



Попробуем сделать копию файла и убедимся, что настройки ACL при этом не копируются:

```
cp testACL.txt testACLcopy.txt
ls -l
```

```
[user@localhost ~]$ cp testACL.txt testACLcopy.txt
[user@localhost ~]$ ls -l
итого 44
-rw-rwxr--. 1 user user   15 янв 30 16:07  testACLcopy.txt
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACL.txt
drwxr-xr-x. 2 user user 4096 апр 21  2022  Видео
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Документы
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Загрузки
```

При работе с ACL нужно быть внимательнее, т.к. не все программы могут использовать ACL. Заметим, что для копирования файла с сохранением ACL необходимо использовать ключ **-p** для команды `cp`:

```
cp -p testACL.txt testACLcopy2.txt
```

```
[user@localhost ~]$ cp -p testACL.txt testACLcopy2.txt
[user@localhost ~]$ ls -l
итого 52
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACLcopy2.txt
-rw-rwxr--. 1 user user   15 янв 30 16:07  testACLcopy.txt
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACL.txt
drwxr-xr-x. 2 user user 4096 апр 21  2022  Видео
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Документы
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Загрузки
```

Чтобы увидеть текущие настройки ACL, потребуется команда `getfacl`. Просмотрим установленные настройки на файле без ACL и сравним вывод с командой `ls -l`:

```
getfacl testACLcopy.txt
ls -l testACLcopy.txt
```

```
[user@localhost ~]$ getfacl testACLcopy.txt
# file: testACLcopy.txt
# owner: user
# group: user
user::rw-
group::rwx
other::r--

[user@localhost ~]$ ls -l testACLcopy.txt
-rw-rwxr--. 1 user user 15 янв 30 16:07 testACLcopy.txt
```

Права доступа отображаются по-разному, но значения соответствующих полей одинаковы.

Попробуем посмотреть настройки ACL файла с установленными списками доступа, сравним вывод с командой `ls -l`:

```
getfacl testACL.txt
ls -l testACL.txt
```

```
[user@localhost ~]$ getfacl testACL.txt
# file: testACL.txt
# owner: user
# group: user
user::rw-
user:test:r-x
group::rw-
mask::rwx
other::r--

[user@localhost ~]$ ls -l testACL.txt
-rw-rwxr--+ 1 user user 15 мая 17  2022 testACL.txt
```

Команда `ls` не выводит имя второго владельца файла и его права доступа к файлу, хотя второй владелец присутствует, как показывает команда `getfacl`. Также для файла теперь присутствует поле `mask`, которое определяет максимальные права для добавляемых полей. В данном примере видно, что можно установить права на чтение, запись и выполнение.

Настройка списков доступа

Для установки и настройки списков доступа предназначена команда `setfacl`. Она имеет простой формат.

Синтаксис команды:

```
setfacl [<опции>] <ключ> <список_правил> <объект>
```

Опции:

- **-b** — удаляет все ACL права с объекта, сохраняя основные права;
- **-k** — удаляет с объекта ACL по умолчанию;
- **-d** — устанавливает ACL по умолчанию на объект, т. е. наследуемых прав;
- **-R** — рекурсивное назначение (удаление) прав.

Ключи:

- **--set** — устанавливает новые указанные права, удаляя все существующие;
- **-m** — изменяет указанные ACL на объекте, сохраняя существующие;
- **-x** — удаляет указанные ACL с объекта, стандартные права не изменяются.

Ниже приведено несколько примеров списков правил, устанавливаемых командой setfacl:

- **u:<uid>:<права>** — назначение ACL для доступа заданному пользователю (здесь можно указать имя или UID пользователя);
- **g:<gid>:<права>** — назначение ACL для доступа заданной группе (здесь можно указать имя или GID группы);
- **o:<права>** — назначение ACL для доступа пользователям, не включённым в группу владельцев файлового объекта («все остальные»);
- **m:<права>** — назначение маски эффективных прав.

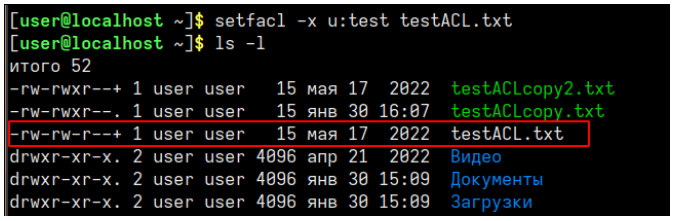
Например, команда setfacl -m u:test:r-x testACL.txt дает разрешения пользователю **test** для файла **testACL.txt**, не делая его владельцем и не изменяя назначение текущего владельца. Иначе говоря, пользователь **test** будет иметь права на этот файл как владелец, только со своими особенными правами доступа.

Команда удаления ACL для пользователя выглядит следующим образом:

```
setfacl -x u:test testACL.txt
```

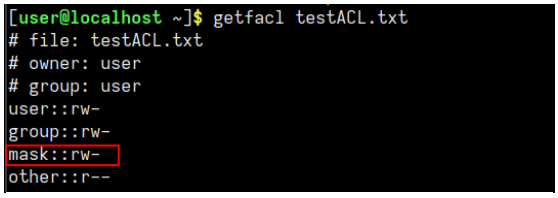
Проверим, удалились ли сведения ACL:

```
ls -l
```



Знак «+» все еще отображается, значит сведения ACL ещё действуют. Проверим, какие сведения ACL привязаны к файлу, выполнив команду:

```
getfacl testACL.txt
```



Вывод команды показывает, что применен параметр mask, удалим его командой:

```
setfacl -x m testACL.txt
```

Проверяем, осталась ли запись ACL у файла:

```
ls -l
```

```
[user@localhost ~]$ setfacl -x m testACL.txt
[user@localhost ~]$ ls -l
итого 48
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACLcopy2.txt
-rw-rwxr--. 1 user user   15 янв 30 16:07  testACLcopy.txt
-rw-rw-r--. 1 user user   15 мая 17  2022  testACL.txt
drwxr-xr-x. 2 user user 4096 апр 21  2022  Видео
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Документы
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Загрузки
```

Знак «**+**» у файла **testACL.txt** теперь отсутствует, значит сведения ACL удалены полностью.

Маска эффективных прав

Маска эффективных прав задает максимальные права доступа для всех пользователей, за исключением владельца и групп. Установка маски представляет собой самый быстрый путь изменения фактических (эффективных) прав доступа всех пользователей и групп. Например, маска (**r - -**) показывает, что пользователи и группы не могут иметь больших прав, чем просто чтение, даже если им назначены права доступа на чтение и запись.

Рассмотрим пример, где установим максимальные права для пользователя **test**:

```
setfacl -m u:test:rwx testACL.txt
```

Затем зададим маску эффективных прав:

```
setfacl -m m:r-- testACL.txt
```

Права на файл устанавливаются в соответствии с выполняемой командой, но маска, установленная как **r--**, лишает разрешения на запись и запуск всех владельцев, кроме основного. Это и отображает появившаяся запись:

```
[user@localhost ~]$ setfacl -m u:test:rwx testACL.txt
[user@localhost ~]$ setfacl -m m:r-- testACL.txt
[user@localhost ~]$ getfacl testACL.txt
# file: testACL.txt
# owner: user
# group: user
user::rw-
user:test:rwx                   #effective:r--
group::rw-                      #effective:r--
mask::r--
other::r--
```

Для отмены маски ее следует установить в значение **rwx**.

Для удаления параметров ACL необходимо выполнить команду:

```
setfacl -b testACL.txt
```

```
[user@localhost ~]$ setfacl -b testACL.txt
[user@localhost ~]$ getfacl testACL.txt
# file: testACL.txt
# owner: user
# group: user
user::rw-
group::r--
other::r--
```

Теперь вы можете использовать списки доступа ACL для более гибких настроек прав доступа к вашим данным.

Ограничение полномочий пользователей по использованию виртуальных терминалов

Ограничение полномочий пользователей по использованию виртуальных терминалов можно настроить следующим образом:

Перейдите в сеанс пользователя **root**:

```
su -
```

и добавьте строку в файл **/etc/security/limits.conf**:

```
petrov hard maxlogins 2
```

Добавить строку можно следующей командой:

```
echo "petrov hard maxlogins 2" >> /etc/security/limits.conf
```

где **petrov** - имя пользователя, которому необходимо ограничить число запускаемых виртуальных терминалов.

Затем для ограничения количества запускаемых виртуальных терминалов **для группы пользователей** добавьте в файл **/etc/security/limits.conf** следующую строку:

```
@users hard maxlogins 2
```

где **@users**- это название группы пользователей (для обозначения группы перед её названием используется символ '**@**').

После добавления правила, ограничивающего число сеансов для пользователя *petrov* равным 2, при попытке открыть 3 сеанс в виртуальном терминале возникает ошибка вида:

```
Too many logins for 'petrov'.

Permission denied
```

Для ограничения количества допустимых **tty** (в том числе и отключение их) для всех пользователей, следует изменить содержимое файла **/etc/systemd/logind.conf**:

```
nano  /etc/systemd/logind.conf
```

раскомментировать строку и указать число 1:

```
NAutoVTs=1
```

после перезагрузки доступ к остальным **tty** будет закрыт, вы увидите только черный экран.

Шифрование дисков и отдельных файлов

Шифрование дисков с помощью cryptsetup
Шифрование файлов средствами gpg

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с возможностью шифрования дисков и отдельных файлов, просмотрев наши обучающие видео:

- на **RuTube** — Шифрование дисков и отдельных файлов;
- в **Яндекс.Дзен** — Шифрование дисков и отдельных файлов;
- в **VK Видео** — Шифрование дисков и отдельных файлов.

На наших каналах вы также сможете найти много другой полезной информации.

Шифрование дисков с помощью cryptsetup

Создается файл размером 20 Гб (размер указывается под нужды пользователя) под зашифрованный диск - на примере домашней директории пользователя *user*:

```
truncate -s 20G /home/.user
chown user:user /home/.user
```

Создайте loop-устройство:

```
losetup /dev/loop0 /home/.user
```

Инициализируем зашифрованный диск (потребуется дважды ввести пароль):

```
cryptsetup -h sha256 -c aes-xts-plain64 -s 512 luksFormat /dev/loop0
```

Обязательно - указать соглашение в верхнем регистре **YES**.

```
Are you sure? (Type uppercase yes): YESEnter passphrase:
Verify passphrase:
```

Откройте зашифрованный диск:

```
cryptsetup luksOpen /dev/loop0 user_home
```

В результате появится устройство **/dev/mapper/user_home**. Создаем на нем ФС:

```
mkfs.ext4 /dev/mapper/user_home
```

Примонтируйте зашифрованный диск:

```
mount /dev/mapper/user_home /mnt
```

Измените права на файловой системе:

```
chown -R user:user /mnt
```

Скопируйте содержимое домашнего каталога. Затем отмонтируйте зашифрованный диск:

```
umount /mnt
```

Закройте зашифрованный диск:

```
cryptsetup luksClose user_home
```

Отсоедините loop-устройство:

```
losetup -d /dev/loop0
```

Теперь производится архивация и удаление содержимого **/home/user**, затем монтирование в него зашифрованного диска. Если все работает нормально — бэкап удаляется.

Скрипт **/home/mount.sh** для автоматизации монтирования:

```
#!/bin/sh
set -e
losetup /dev/loop0 /home/.user
cryptsetup luksOpen /dev/loop0 user_home
mount /dev/mapper/user_home /home/user
```

Сделайте скрипт исполняемым:

```
chmod +x /home/mount.sh
```

Выполните скрипт:

```
/home/mount.sh
```

Скрипт **/home/umount.sh**, выполняющий обратные действия:

```
#!/bin/sh
set -e
umount /home/user
cryptsetup luksClose user_home
losetup -d /dev/loop0
```

Сделайте скрипт исполняемым:

```
chmod +x /home/umount.sh
```

Выполните скрипт:

```
/home/umount.sh
```

Когда оригинальных данных на диске не осталось, можно заполнить свободное место мусором (процесс долгий):

```
cd /home
dd if=/dev/urandom of=./random.tmp bs=10M count=6300
sync
rm random.tmp
```

Наконец, чтобы временные файлы (те же черновики электронных писем) писались на зашифрованный раздел, в **/home/user/.bashrc** следует дописать:

```
export TMPDIR=/home/user/temp
mkdir -p $TMPDIR
```

Шифрование файлов средствами gpg

Сгенерируйте свой личный ключ для шифрования файлов:

```
gpg --gen-key
```

От вас потребуется ввести имя пользователя, почту и придумать пароль.

Просмотр списка ключей доступен командами:

```
gpg --list-keys
gpg --list-secret-keys
```

Проверка отпечатка, что вы правильно сможете обратиться к ключу:

```
gpg --fingerprint 'user_name'
```

Зашифровывание содержимого каталога при помощи ключа:

```
tar -c -f- /home/user/Документы/* | gpg -e -c -r 'user_name'> file.tar.gpg
```

Расшифровывание - потребуется ввести пароль ключа:

```
gpg -d -o ./file.tar ./file.tar.gpg
```

Защитное преобразование файлов и каталогов по ГОСТ Р 34.12–2015

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** caja-extension-actions-0.9-1

Для шифрования файлов по ГОСТ необходимо наличие в системе пакета **caja-extension-actions** последней версии.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

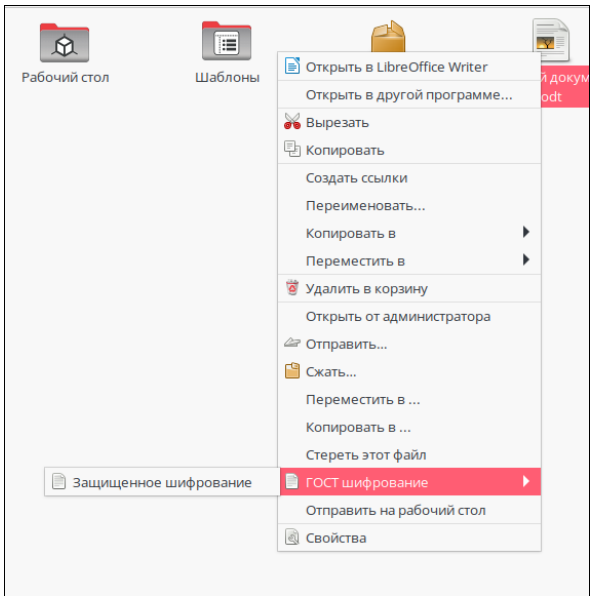
```
dnf install caja-extension-actions
```

Затем выполните:

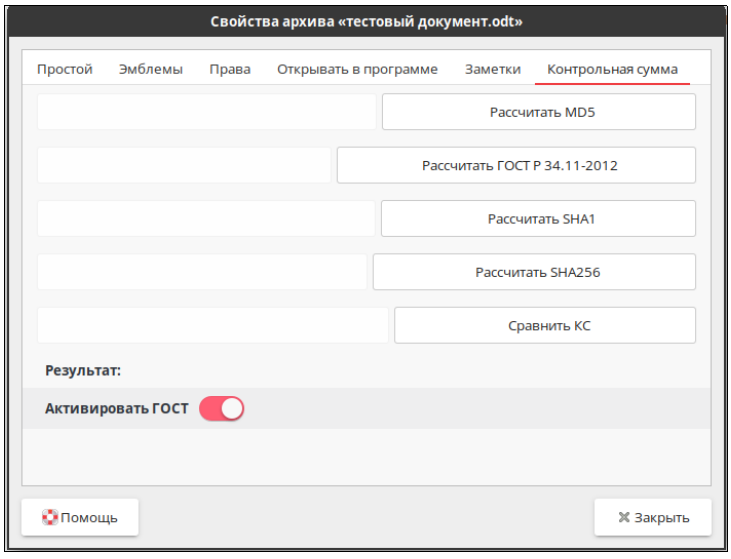
```
caja -q
```

Следующим шагом необходимо проверить активированное ГОСТ шифрование.

Если в контекстном меню файла появилось поле «**ГОСТ шифрование**», тогда дополнительных действий делать не нужно.



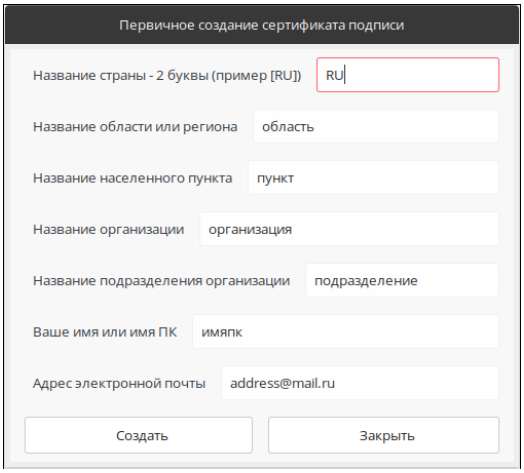
Если данное поле отсутствует, необходимо выбрать «**Свойства**» файла, перейти на вкладку «**Контрольная сумма**» и активировать ГОСТ при помощи тумблера.



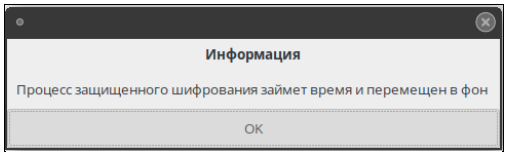
После этого необходимо создать сертификат подписи.

Данный сертификат будет расположен по пути **~/.gost**, и для расшифровывания файлов данный каталог должен быть выгружен другому пользователю.

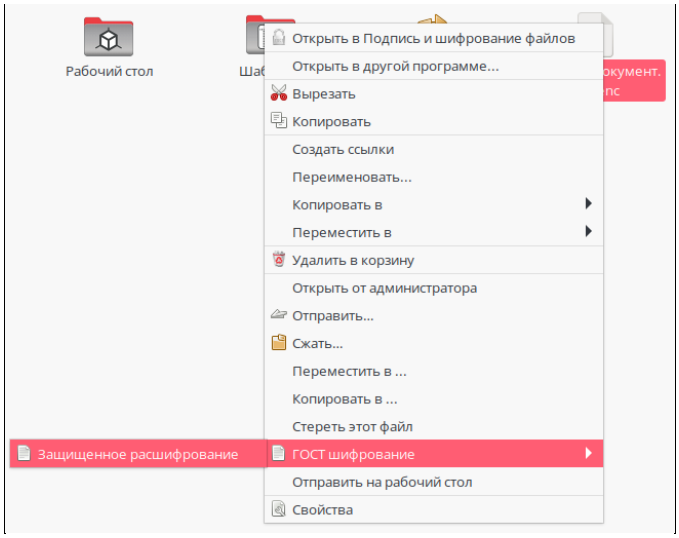
В ином случае будет выполнена реинициализация создания сертификата, который будет не приемлем для расшифровывания.



Далее вы увидите уведомляющее окно, дождитесь завершения процесса и у вас появится зашифрованный файл с расширением **.enc**.



Для расшифрования файла вам потребуется вызвать ПКМ контекстное меню файла с расширением **.enc** и, соответственно, выбрать пункт «**ГОСТ шифрование**» – «**Защищенное расшифрование**».



При успешном завершении операции вы увидите ваш расшифрованный файл.

Безопасное удаление файлов

shred
wipe
Дополнительные утилиты
srm
sfill
sswap

Удаление файлов и каталогов с помощью команд **rm** и **find** не гарантирует того, что удаленные объекты не могут быть восстановлены. Для безопасного гарантированного удаления файлов и каталогов без возможности восстановления необходимо использовать утилиты **shred** и **wipe**.

Вы можете подробнее ознакомиться с работой утилит, предназначенных для безопасного удаления файлов, просмотрев наши обучающие видео:

- на **RuTube** — Полное и необратимое удаление данных с дисков;
- в **Яндекс.Дзен** — Полное и необратимое удаление данных с дисков;
- в **VK Видео** — Полное и необратимое удаление данных с дисков.

На наших каналах вы также сможете найти много другой полезной информации.

shred

shred — переписывает несколько раз указанные файлы для того, чтобы сделать более сложным восстановление.

Синтаксис:

```
shred [<КЛЮЧ>] <ФАЙЛ>
```

Ключи:

- `-f`, `--force` — изменять права, разрешая запись, если необходимо;
- `-n`, `--iterations=N` — выполнить **N** циклов перезаписи содержимого (по умолчанию **3**). На современных устройствах хранения одного цикла перезаписи (`N=1`) должно быть достаточно, однако минимально рекомендуемое количество циклов перезаписи - **3**. При `N > 25` все внутренние шаблоны перезаписи будут использованы хотя бы один раз;
- `--random-source=<ФАЙЛ>` — получать случайные числа из **<ФАЙЛА>** (по умолчанию **/dev/urandom**);
- `-s`, `--size=N` — очистить **N** байт (возможны суффиксы вида **K**, **M**, **G**);
- `-u` — освобождать и удалять файл после перезаписи;
- `--remove[=<способ_удаления>]` — подобно `-u`, но задаётся способ удаления;
- `-v`, `--verbose` — показывать ход выполнения;
- `-x`, `--exact` — не округлять размеры файлов до следующего целого блока;
- `-z`, `--zero` — перезаписать в конце нулями, чтобы скрыть измельчение;
- `--help` — показать справку и выйти;
- `--version` — показать информацию о версии и выйти.

wipe

wipe — это небольшая программа для безопасного стирания файлов с магнитных носителей.

Синтаксис:

```
wipe [<опции>] файлы...
```

Опции:

- `-a` — прервать при ошибке;
- `-b <buffer-size-lg2>` — установить размер индивидуального буфера ввода/вывода указав его логарифм по основанию 2. Могут быть выделены до 30 этих буферов;

- -c — делать chmod() на защищённых от записи файлах;
- -D — следовать символическим ссылкам (конфликтует с -r);
- -e — использовать точный размер файла: не округлять размер файла для стирания возможного мусора, остающегося на последнем блоке;
- -f — форсировать, т. е. не спрашивать подтверждения;
- -F — не пытаться стирать имена файлов;
- -h — показать справку;
- -i — информативный (подробный) режим;
- -k — сохранить файлы, т. е. не удалять их после перезаписи,
- -l <длина> — установить длину стирания на <длину> байт, где <длина> — это целое число, за которым следует **K** (Kilo:1024), **M** (Mega:K^2) или **G** (Giga:K^3);
- -M (l|r) — установить алгоритм PRNG для заполнения блоков (и порядка проходов):
  - l — использовать вызов библиотеки random();
  - a — использовать алгоритм шифрования arcfour.
- -o <сдвиг> — установить сдвиг очистки на <сдвиг>, где <сдвиг> имеет тот же формат, что и <длина>;
- -P <проходы> — установить количество проходов для очистки имени файла. По умолчанию **1**;
- -Q <количество> — установить количество проходов для быстрой очистки;
- -q — быстрая очистка, менее безопасная, по умолчанию **4 случайных** прохода;
- -r — рекурсия по каталогам — по символическим ссылкам не будет переходов;
- -R — установить устройство рандомизации (или команду сидов рандомизации -S c);
- -S (r|c|p) — метод рандомизации сидов:
  - r — считывать с устройства рандомизации (надёжно);
  - c — считывать из вывода команды рандомизации сидов;
  - p — использовать pid(), clock() и т.д. (самый слабый вариант).
- -s — тихий режим — подавлять весь вывод;
- -T <попытки> — установить максимальное число попыток для свободного поиска имени файла, по умолчанию **10**;
- -v — показать информацию о версии;
- -Z — не пытаться стирать имя файла.

Дополнительные утилиты

Также для безопасного удаления данных можно использовать утилиты пакета **secure-delete**: **srm**, **sfill**, **sswap**, которые безопасно очищают файлы, диски, раздел подкачки и память.

srm

srm выполняет безопасную перезапись/переименование/удаление целевого файла(ов).

Синтаксис:

```
srm [<опции>] <файл_1> <файл_2> ...
```

Опции:

- -d — игнорировать специальные файлы "." и "..";
- -f — быстрый (и небезопасный режим): без **/dev/urandom**, без режима синхронизации;
- -r, -R, --recursive — рекурсивный режим, удаляет содержимое директорий;
- -v — подробный режим;
- -V — показать информацию о версии.

sfill

sfill выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов (**inode**) указанного каталога.

Синтаксис:

```
sfill [-fillvz] <каталог>
```

Опции:

- `-f` — быстрый (и небезопасный режим): без **/dev/urandom**, без режима синхронизации;
- `-i` — стирает только индексные дескрипторы в указанной директории;
- `-l` — стирает только пространство, без индексных дескрипторов;
- `-l` — снижение уровня безопасности (используйте дважды для включения небезопасного режима);
- `-v` — подробный режим;
- `-z` — последний проход заполняет нулями вместо рандомных данных.

sswap

sswap делает безопасную перезапись раздела подкачки.

Синтаксис:

```
sswap [-flvz] [-j start] /dev/of_swap_device
```

Опции:

- `-f` — быстрый (и небезопасный режим): без **/dev/urandom**, без режима синхронизации;
- `-j` — при очистке перепрыгнуть через это количество первых байт (по умолчанию **4096**);
- `-l` — снижение уровня безопасности (используйте дважды для включения небезопасного режима);
- `-v` — подробный режим;
- `-z` — последний проход заполняет нулями вместо рандомных данных.

Отключение CD-ROM

Запрет монтирования CD-ROM

Чтобы отключить **CD-ROM**, вам необходимо создать файл **/etc/modprobe.d/usb-storage.conf** и отредактировать его с помощью текстового редактора.

```
sudo nano /etc/modprobe.d/usb-storage.conf
```

Введите следующие строки в файл:

```
install usb-storage /bin/true
```

Вышеупомянутый файл **.conf** отражает фальшивую установку **CD-ROM**. Сохраните файл с помощью Ctrl + O, затем нажмите Enter, и выйдите из редактора с помощью Ctrl + X.

Запретите чтение/запись/выполнение всем пользователям, кроме **root**, на каталог, в который монтируются **CD-ROM**.

```
sudo chmod -R 700 /run/media
```

Для вступления изменений в силу перезагрузите компьютер.

Возврат возможности подключения

Для того чтобы вернуть возможность монтирования, выполните следующие команды

```
sudo rm -f /etc/modprobe.d/usb-storage.conf
sudo chmod -R 755 /run/media
```

Перезагрузите компьютер.

Ограничение доступа к USB-накопителям

Примеры выбора устройств по определенным свойствам
Запрет автомонтирования с параметром UDISKS_IGNORE
Создание белого списка с параметром UDISKS_IGNORE
Запрет автомонтирования с параметром authorized
Создание белого списка с параметром authorized

Алгоритм создания белого списка USB-флеш-накопителей состоит из 2 этапов:

Вариант 1:

1. Запрет монтирования всех USB-флеш-накопителей
2. Разрешение монтирования некоторых устройств

Вариант 2:

1. Разрешение монтирования некоторых устройств
2. Запрет монтирования всех иных USB-флеш-накопителей

Вы можете подробнее ознакомиться с информацией по ограничению доступа к USB-накопителям, просмотрев наши обучающие видео:

- на **RuTube** — Ограничение доступа к USB-накопителям;
- в **Яндекс.Дзен** — Ограничение доступа к USB-накопителям;
- в **VK Видео** — Ограничение доступа к USB-накопителям.

На наших каналах вы также сможете найти много другой полезной информации.

Примеры выбора устройств по определенным свойствам

Для создания белого списка USB-флеш-накопителей необходимо знать атрибуты накопителя.

1) Определите ваш флеш-накопитель:

```
 ls -l /dev/sd*

brw-rw---- 1 root disk 8, 0 июн 30 12:59 /dev/sda
brw-rw---- 1 root disk 8, 1 июл 22 12:59 /dev/sda1
brw-rw---- 1 root disk 8, 2 июл 22 12:59 /dev/sda2
brw-rw---- 1 root disk 8, 3 июн 30 12:59 /dev/sda3
brw-rw---- 1 root disk 8, 16 июл 22 13:43/dev/sdb # нужная нам строка
brw-rw---- 1 root disk 8, 17 июн 30 13:43 /dev/sdb1
```

2) Проверьте атрибуты (символы после **sd*** должны вводиться в соответствии с вашим выводом команды `ls -l /dev/sd*`):

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром UDISKS_IGNORE

Для отключения автомонтирования USB-флеш-накопителей необходимо создать правило для **udev**.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
```

Флаг `ENV{UDISKS_IGNORE}` отвечает за игнорирование устройства:

- «0» – false;
- «1» - true.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром UDISKS_IGNORE

Выборка разрешения доступа по трем параметрам:

- серийному номеру устройства;
- модели;
- максимальному потребления тока.

Для их определения выполните поочередно команды:

```
udevadm info -a -p /sys/block/sdb | grep serial
udevadm info -a -p /sys/block/sdb | grep product
udevadm info -a -p /sys/block/sdb | grep bMaxPower
```

в выводе будет отображен серийный номер, модель и значение максимального потребления тока:

```
ATTRS{serial}=="04GS1F3LBIBDWU05"
 ATTRS{model}=="Silicon-Power8G "
 ATTRS{bMaxPower}=="200mA"
```

Запишите эти значения в файл правил в качестве разрешающих.

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
 ATTRS{serial}=="04GS1F3LBIBDWU05",ENV{UDISKS_IGNORE}="0"
 ATTRS{product}=="DataTraveler 3.0",ENV{UDISKS_IGNORE}="0"
 ATTRS{bMaxPower}=="200mA",ENV{UDISKS_IGNORE}="0"
```

Здесь:

- **1** - заблокировать все usb-накопители;
- **0** - разрешить накопитель по определенным свойствам.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, находится в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром authorized

Для отключения автомонтирования USB-флеш-накопителей необходимо будет создать правило для **udev** и исполняемый скрипт запрета монтирования USB-флеш-накопителей.

Создайте скрипт:

```
nano /usr/bin/remove_usb.sh
```

```
#!/bin/bash
var=$1
var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
echo 0 > '/sys/bus/usb/devices'$var2'authorized'
```

Измените права на скрипт:

```
chmod +x /usr/bin/remove_usb.sh
```

Параметр **authorized** отвечает за монтирование USB-флеш-накопителя в момент подключения к ПК.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
```

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром authorized

Выборка по серийному номеру устройства:

```
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
```

Выборка по названию модели. Точное название смотрите в выводе команды:

```
 udevadm info -a -p /sys/block/sdb

ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
```

Для удобства, когда полный список параметров устройства известен, можно производить отбор по конкретному параметру:

```
udevadm info -a -p /sys/block/sdb | grep "ATTRS{serial}"
udevadm info -a -p /sys/block/sdb | grep "ATTRS{product}"
```

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ACTION!="add", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}=="usb-storage", RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
LABEL="dont_remove_usb"
```

Логика данного правила отлична от первого варианта. В первом варианте происходила блокировка сразу всех usb флеш-накопителей, а только потом осуществлялось добавление устройств в белый список. В данном (втором) варианте сначала происходит добавление устройств в белый список, а только потом блокирование устройств (добавление в черный список). Такое действие связано с тем, что параметр **authorized** появляется в момент монтирования и, если его значение установить в **0**, то для дальнейшей работы он становится недоступен. Соответственно, сначала требуется проверить, входит ли флеш-накопитель в белый список, и если входит, то разрешить его монтирование.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, отображается в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Настройка протоколирования событий подключения USB-накопителей

Создаем правила для **udev**:

```
nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды

```
#log mount/unmount
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo unmount $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

После выполнения данных действий будут фиксироваться все факты подключения/отключения usb-накопителей.

Настройка принадлежности USB-накопителей

В данной статье будет рассмотрен пример разграничения правил для разных пользователей.

Сначала необходимо создать udev-правило, содержащее разрешения на определенные usb-устройства, по выбранным пользователем параметрам.

```
nano /etc/udev/rules.d/80-alloweduserlist1.rules
```

```
ACTION!="add", GOTO="dont_remove_usb"
 ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
 ATTRS{product}=="USB DISK 2.0",GOTO="dont_remove_usb"
 ENV{DRIVER}=="usb-storage",RUN+="/bin/python3 /usr/local/bin/remove_usb.py $devpath"
 LABEL="dont_remove_usb"
 ENV{DRIVER}=="usb-storage", ENV{UDISKS_AUTO}="0"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="add", RUN+="/bin/systemctl start usb-mount-list1@%k.service"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="remove", RUN+="/bin/systemctl stop usb-mount-list1@%k.service"
```

Затем необходимо создать скрипт для запрета монтирования устройств со следующим содержимым:

```
nano /usr/local/bin/remove_usb.py
```

```
#!/usr/bin/python3
 import os
 import sys
 var = sys.argv[1].strip()
 var2 = os.popen(f"echo {var} | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//'").readlines()[0]
 os.system(f"echo 0 > '/sys/bus/usb/devices{var2.strip()}authorized'")
```

Далее создайте сервис, отвечающий за запуск скрипта, проверяющего список доступных пользователей для данного udev-правила.

```
nano /etc/systemd/system/usb-mount-list1@.service
```

```
[Unit]
 Description=Mount USB Drive on %i

 [Service]
 RemainAfterExit=true
 Type=oneshot
 ExecStart=/usr/bin/python3 /usr/local/bin/usb-mount.py add %i /etc/udev/rules.d/80-alloweduserlist1.rules
 ExecStop=/usr/bin/python3 /usr/local/bin/usb-mount.py remove %i /etc/udev/rules.d/80-alloweduserlist1.rule
```

Следующим этапом формируется список разрешенных пользователей.

Допустимые значения **umask**:

- 0 - rwx - полные права; rw - чтение/запись;
- 2 - r - чтение.

Создайте список разрешенных пользователей (в примере **user1** с правами на чтение) без проверки на группы:

```
mkdir /etc/udevlist
nano /etc/udevlist/userlist1.json
```

```
{"user1": 2}
```

Если необходимо указать несколько пользователей, список указывается в виде `{"user1": 2, "user2": 0, ...}`.

Затем создайте файл соответствия udev-правила со списком разрешенных пользователей:

```
nano /etc/udevlist/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/userlist1.json"}
```

Создайте список разрешенных групп:

```
mkdir /etc/udevlist/group/
nano /etc/udevlist/group/grouplist1.json
```

```
{}
```

Если в правиле необходимо использовать разграничение по группам, список указывается в виде `{"name_group1": 0, "name_group2": 2}`.

После этого создайте файл соответствия udev-правила со списком разрешенных групп:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/group/grouplist1.json"}
```

Создайте файл для других списков, если используются:

```
mkdir /etc/udevlist/otherlists/
nano /etc/udevlist/otherlists/otherlists1.json
```

с содержимым вида:

```
{"others": 7}
```

После этого создайте файл соответствия udev-правила с новым списком:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/otherlists/otherlists1.json"}
```

Затем загрузите скрипт проверки доступа пользователей и монтирования устройств, распакуйте архив и переместите файл скрипта в каталог **/usr/local/bin/**:

```
wget https://redos.red-soft.ru/upload/usb-mount.zip
unzip ./usb-mount.zip -d /usr/local/bin/
```

Для применения настроек перезапустите службы командой:

```
systemctl daemon-reload
```

Настройка учета USB-накопителей

Создаем правила для **udev**:

```
sudo nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды (в примере показан учет **USB** на основе серийного номера):

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add",RUN+="/bin/sh /mnt/logs.sh $devnode %E{ID_SERIAL}"
```

Создаем скрипт для ведения лог файла. Если указать путь **/root/log.txt**, то доступ к файлу лога будет только у пользователя **root**.

```
nano /mnt/logs.sh
```

```
path=$1
 serial=$2
 File="/root/log.txt"
 if ! grep -q "$serial" "$File";
 then
 echo $path $serial $(date)>> /root/log.txt
 fi
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

Ограничение доступа USB-устройств по defines class code

Существует большое количество устройств, имеющих разный *USB defines class code*. Для того чтобы разрешить подключение определенного класса устройств, потребуется применить следующий алгоритм:

1) Создать правило, в котором прописаны разрешенные устройства, а остальные блокируются:

```
nano /etc/udev/rules.d/99-usb-bInterfaceClass.rules
```

Содержимое правила на примере классов для **token**, **HID**, **audio** и **video** устройств:

```
# Allow all TOKEN devices
 ATTR{bInterfaceClass}=="0b",ACTION=="add",GOTO="usb_rules_end"
 # Allow all c
 ATTR{bInterfaceClass}=="03",ACTION=="add",GOTO="usb_rules_end"
 # Allow all AUDIO devices
 ATTR{bInterfaceClass}=="01",ACTION=="add",GOTO="usb_rules_end"
 # Allow all VIDEO devices
 ATTR{bInterfaceClass}=="0e",ACTION=="add",GOTO="usb_rules_end"
 SUBSYSTEM=="usb",ACTION=="add",RUN+="/bin/sh -c '/usr/bin/reject_usb_bInterfaceClass.sh $devpath'"
 LABEL="usb_rules_end"
```

2) Создать скрипт, изменяющий атрибут **authorized** для определенного устройства:

```
nano /usr/bin/reject_usb_bInterfaceClass.sh
```

Содержимое скрипта:

```
#!/bin/bash
 var=$1
 var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
 var3=$(echo $var2 | grep '^/[0-9]-[0-9]$')
 var4=$(echo $var2 | grep '^/[0-9]-[0-9].[0-9]$')
 if [ -z "$var3" ] && [ -z "$var4" ]; then
 echo 0 > '/sys/bus/usb/devices'$var2'/authorized'
 fi
```

Сделайте скрипт исполняемым:

```
chmod +x /usr/bin/reject_usb_bInterfaceClass.sh
```

Перезапустите правила **udev**:

```
sudo udevadm control --reload-rules
```

HUB устройства

Есть устройства, которые системой определяются как **HUB**. В момент редактирования правил и перезагрузки **udev** на **HUB**-устройства, которые находятся в системном блоке/кейсе, влияние оказано не будет, так как они не переподключаются. Зато при перезагрузке ОС они заблокируются и в итоге все подключенные к ним устройства ниже по дереву тоже будут заблокированы. Для корректного редактирования устройств подключенных через **HUB** требуется в правилах разрешить:

```
DRIVER=="hub",ACTION=="add",GOTO="end_usb_rules"
```

либо:

```
ATTR{bInterfaceClass}=="09",ACTION=="add",GOTO="usb_rules_end"
```

Перезапустить правила:

```
udevadm control --reload-rules
```

Утилита по созданию правил для монтирования USB-накопителей

Установка
Полная блокировка всех usb
Назначение личной привязки к UDEV-правилу
Протоколирование событий usb-flash накопителей

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** usb_rules-2.1-1

Утилита **usb_rules** основана на работе с правилами **udev** и системными сервисами **systemd**.

Вы можете подробнее ознакомиться с работой утилиты **usb_rules**, просмотрев наши обучающие видео:

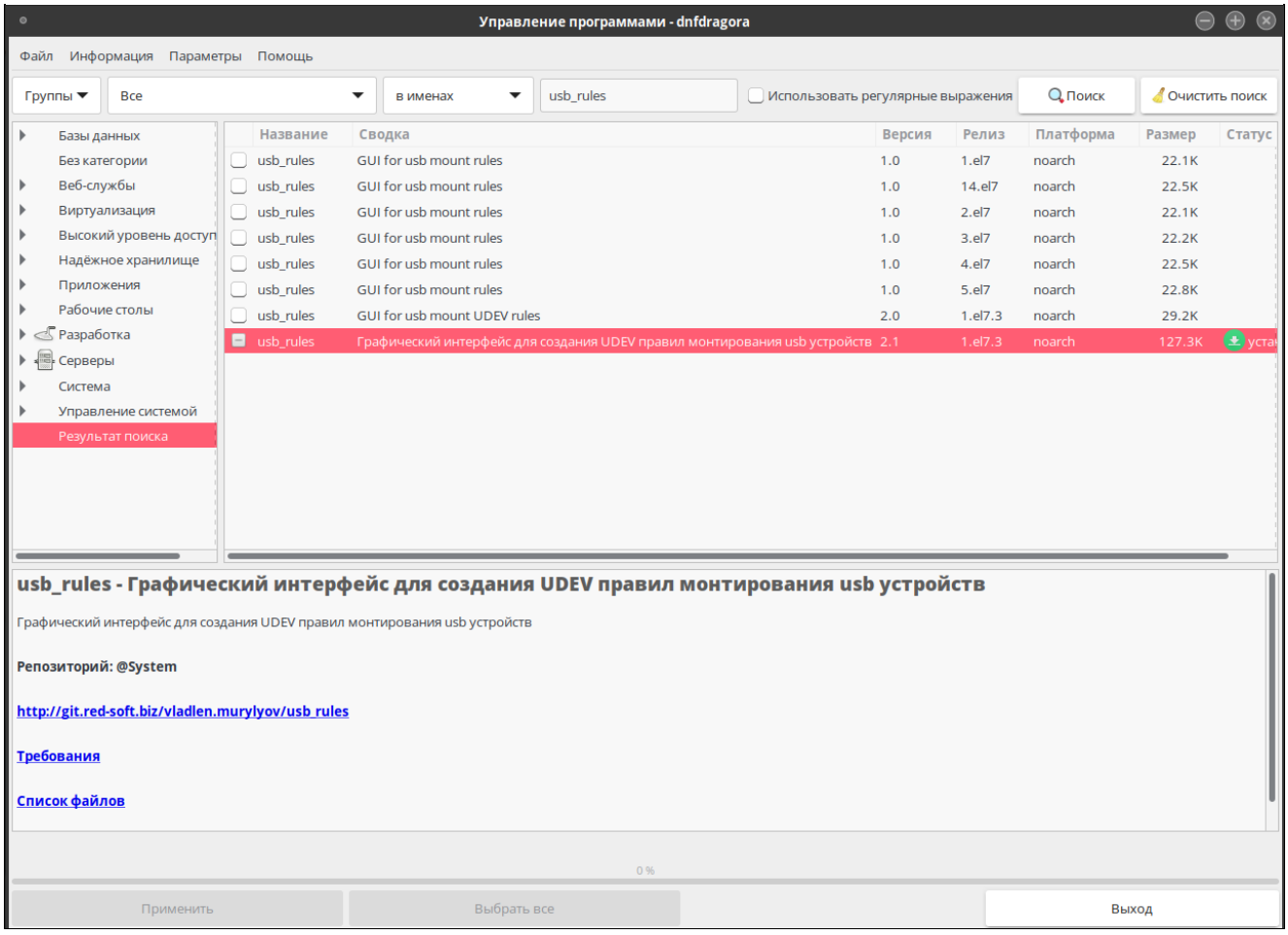
- на **RuTube** — Утилита по созданию правил для монтирования usb-flash накопителей;
- в **Яндекс.Дзен** — Утилита по созданию правил для монтирования usb-flash накопителей;
- в **VK Видео** — Утилита по созданию правил для монтирования usb-flash накопителей.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установка утилиты доступна через пакетный менеджер *dnfdragora* («**Главное меню**» - «**Администрирование**» -«**Управление пакетами dnfdragora**»).

В поисковой строке пакетного менеджера введите название утилиты «**usb_rules**», нажмите «**Enter**» для поиска. Из списка результатов выберите последнюю версию утилиты и нажмите кнопку «**Применить**».



Будет выполнена установка пакета.

Также установка утилиты доступна из терминала. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

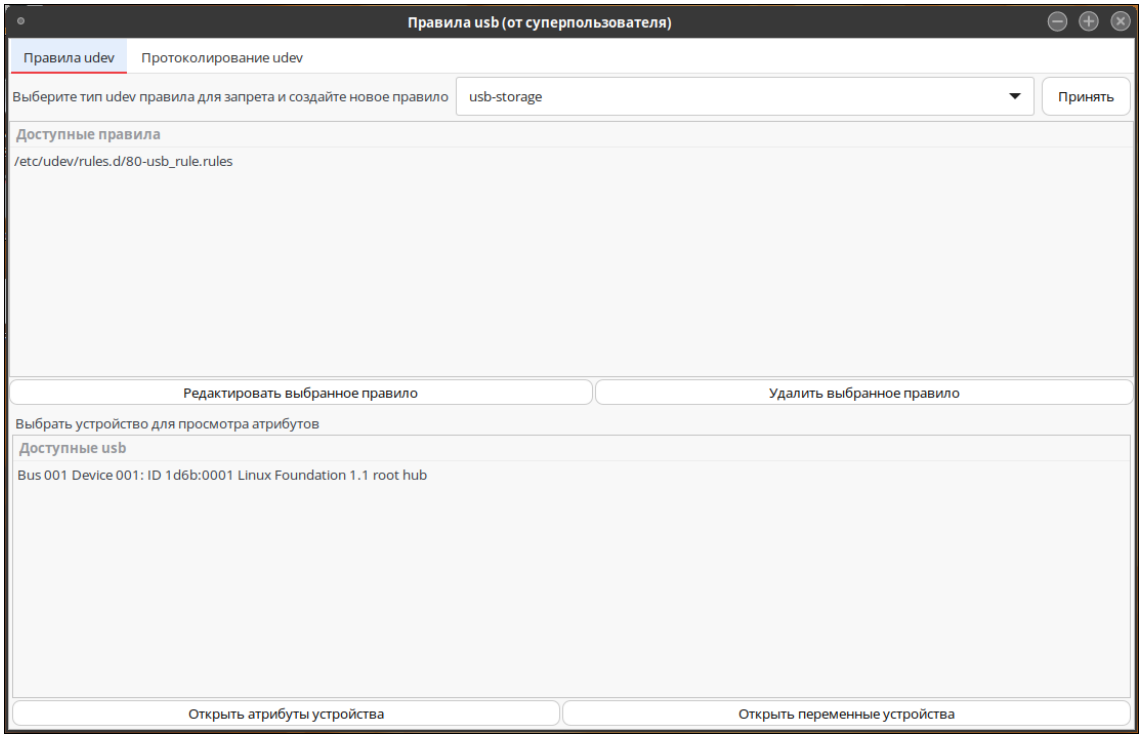
и выполните команду:

```
dnf install usb_rules
```

После установки запуск утилиты доступен с правами пользователя **root** из «**Главного меню**» - «**Параметры**» - «**Настройка ограничения монтирования**» или через терминал с помощью команды:

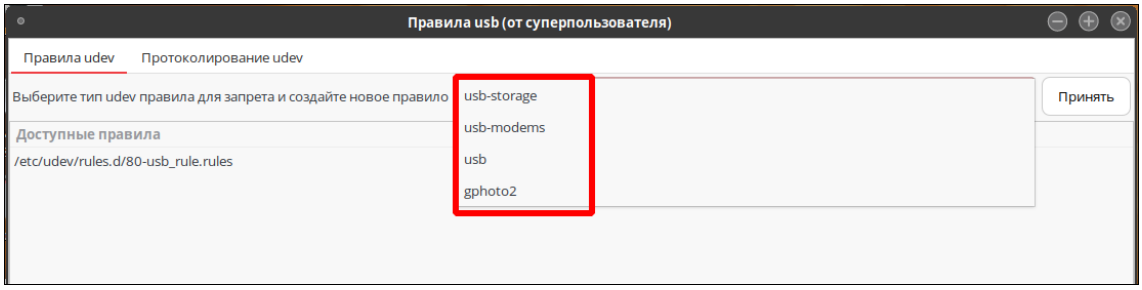
```
usb-rules
```

Стартовое окно утилиты позволяет пользователю ознакомиться с подключенными usb-устройствами и со списком уже созданных правил.



При формировании нового правила пользователю доступны 4 шаблона:

- **usb-storage**;
- **usb-modems**;
- **usb**;
- **gphoto2**.



Каждое из правил отвечает за полную блокировку тех или иных устройств.

Полная блокировка всех usb

Ниже представлено содержимое шаблонов для каждого правила:

```
#type:usb-storage
```

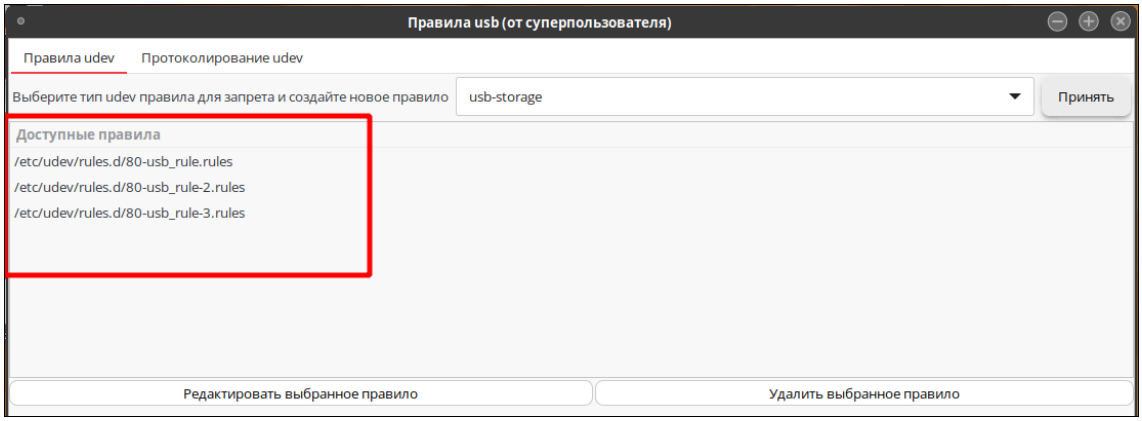
```
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:usb-modems
ACTION!="add", GOTO="dont_remove_usb"
DRIVER!="rndis_host", GOTO="dont_remove_usb"
DRIVER=="rndis_host", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

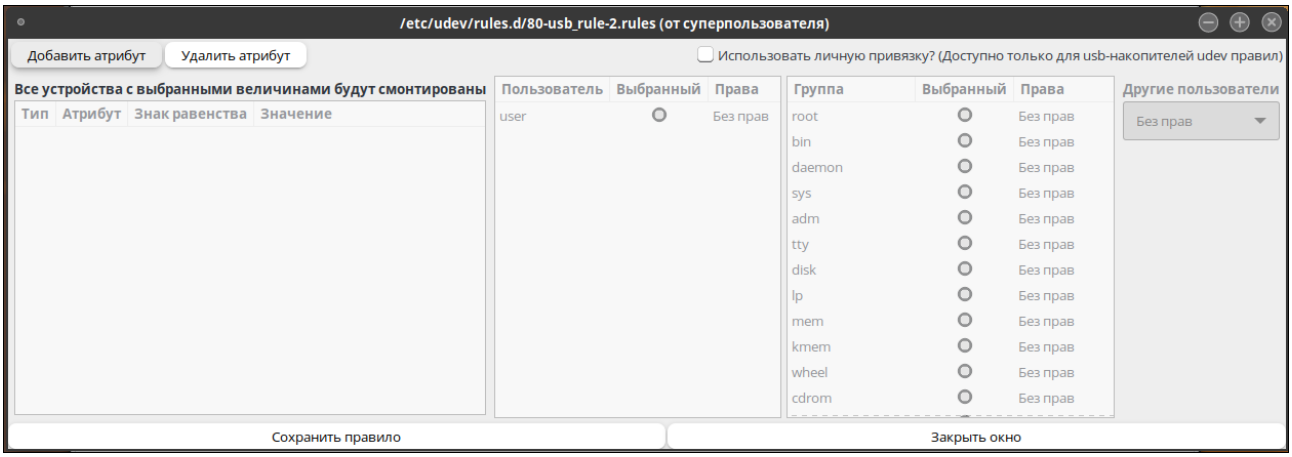
```
#type:usb
ACTION!="add", GOTO="dont_remove_usb"
SUBSYSTEM!="usb", GOTO="dont_remove_usb"
SUBSYSTEM=="usb", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:gphoto2
ACTION!="add", GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}!="PTP",GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}=="PTP",ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

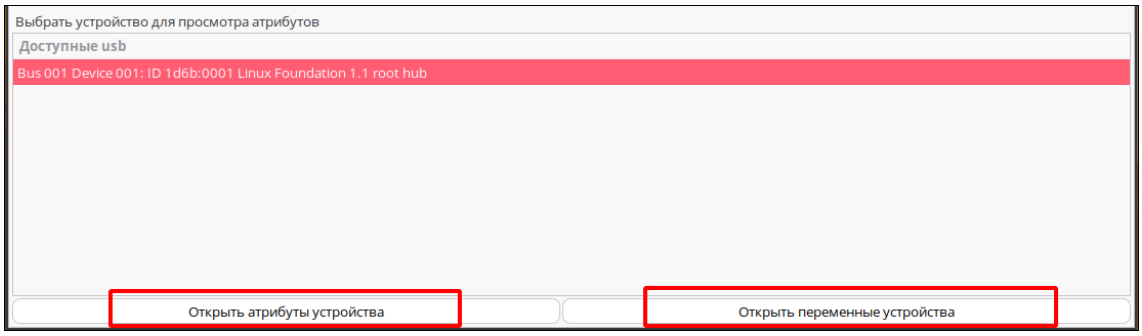
При формировании правила из шаблонного в окне утилиты появляется строка, соответствующая сформированному правилу.



Далее потребуется создать разрешающие монтирование параметры. Для этого необходимо добавить атрибут, который в новом правиле будет отвечать за исключение из блокировки устройств, подходящих под данный параметр. Добавление или удаление таких атрибутов доступно после выбора интересующего правила и нажатия кнопки «**Редактировать правило**».

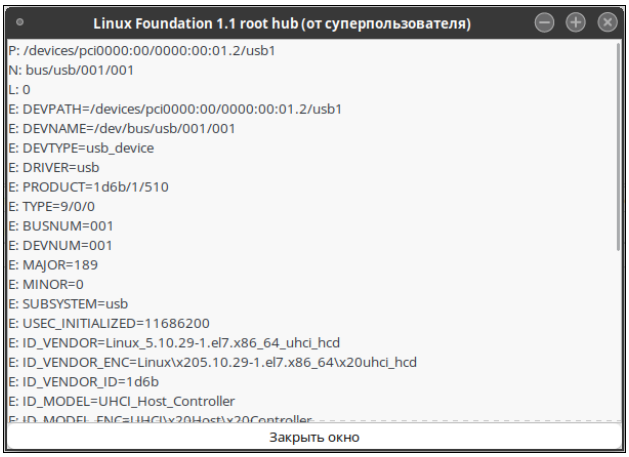


В полях «**Атрибут**» и «**Значение**» необходимо подобрать значения из доступных устройств. Просмотр доступных значений можно осуществить следующим образом:



В результате будут открыты следующие окна:

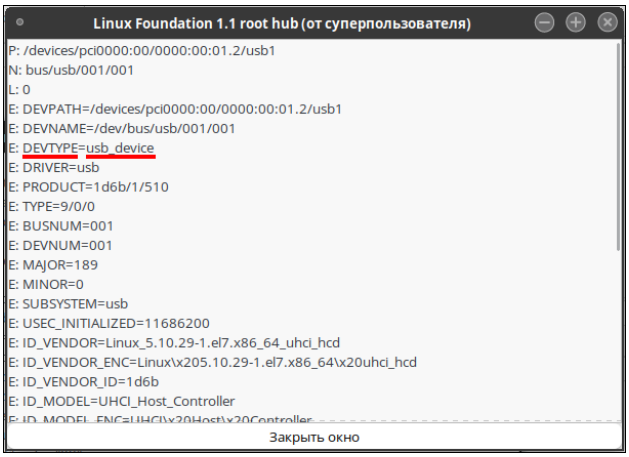




При добавлении пункта **ATTR** следует прописать значение и величины соответствующие:

Значения указываются, соответственно, без фигурных скобок **{}** и без кавычек **""**.

Для указания величин **ENV** следует выбирать величины:

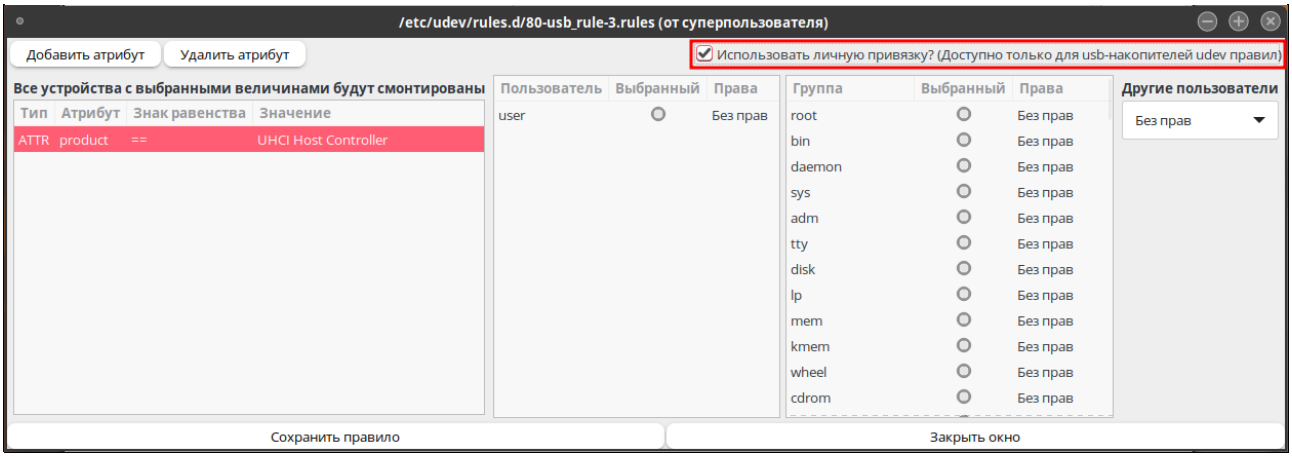


В результате будет сформировано примерно следующее правило **/etc/udev/rules.d/80-usb_rule.rules**:

```
#type:usb-storage
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTR{product}==UHCI Host Controller, GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

Назначение личной привязки к UDEV-правилу

За назначение привязки отвечает поле, которое активируется соответствующим флагом:



По умолчанию все пользователи не имеют прав. Соответственно, потребуется выбрать необходимых пользователей и задать им права «**чтения**», «**чтения и записи**» или «**все права**».

При формировании личной привязки будет создаваться **systemd**-сервис, который будет работать в связке с отведенным под него udev-правилом.

```
nano /etc/systemd/system/usb-mount@.service
```

```
[Unit]
Description=Mount USB Drive on %i

[Service]
RemainAfterExit=true
Type=oneshot
ExecStart=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py add %i /etc/udev/rules.d/80-usb_rule.rules
ExecStop=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py remove %i /etc/udev/rules.d/80-usb_rule.rules
```

Протоколирование событий usb-flash накопителей

Вкладка «**Протоколирование udev**» позволяет протоколировать события, связанные с **usb-flash** накопителями по выбранным пользователем атрибутам. Синтаксис добавления идентичен добавлению **ENV**-атрибутов.

В результате формирования правила для протоколирования будет создан файл **/etc/udev/rules.d/98-usb_logs.rules** со следующим примерным содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo disconnected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
```

USBIP - утилита для подключения удаленных USB-устройств

Настройка на сервере
Настройка на клиенте
Графическая утилита usbip-gui

USBIP — это утилита, направленная на предоставление в общий доступ USB-устройств через IP-сеть для совместного использования. Чтобы совместно использовать USB-устройства между компьютерами с их полной функциональностью, *USBIP* преобразует «сообщения ввода-вывода USB» в полезные данные **TCP/IP** и передает их между компьютерами. Оригинальные драйверы и приложения для USB-устройств также могут использоваться для удаленных USB-устройств без их модификации. Компьютер может использовать удаленные USB-устройства, как если бы они были напрямую подключены.

Устройства, которые можно подключить через утилиту:

- запоминающие устройства USB: флешки, внешние жесткие диски и картридеры;
- периферийные устройства ввода: USB-клавиатуры, мыши;
- мультимедийные устройства (например, веб-камеры);
- оборудование для печати и сканирования.

Вы можете подробнее ознакомиться с установкой и настройкой утилиты **USBIP**, просмотрев наши обучающие видео:

- на **RuTube** — Подключение удаленных USB устройств. USBIP;
- в **Яндекс.Дзен** — Подключение удаленных USB устройств. USBIP;
- в **VK Видео** — Подключение удаленных USB устройств. USBIP.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка на сервере

Сервер предназначен для публикации **USB-устройств**, которые могут быть удаленно доступны с клиентской стороны. Он выполняет роль хоста, предоставляя подключенные к нему **USB-устройства** (например, флеш-накопители, принтеры, сканеры) для использования через сеть. Это позволяет клиентам взаимодействовать с устройствами так, как если бы они были подключены локально.

Для начала работы необходимо установить утилиту *USBIP* командой (потребуются права **администратора**):

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe usbip-host
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 usbip-host
 vhci-hcd
```

Сохраните изменения и закройте редактор. Чтобы обеспечить автоматический запуск **usbipd** при старте системы, его можно оформить в виде системного юнита:

```
nano /etc/systemd/system/usbipd.service
```

Добавьте в файл следующие строки:

```
[Unit]
 Description=USBIPd
```

```
[Service]
ExecStart=/usr/sbin/usbipd -D
Type=oneshot
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

После создания или изменения системного юнита необходимо перезагрузить настройки менеджера системных служб и включить автоматический запуск службы usbipd, чтобы она запускалась сразу после загрузки системы. Для этого выполните следующие команды:

```
sudo systemctl daemon-reload
sudo systemctl enable usbipd --now
```

Перед тем как открыть доступ к какому-либо usb-устройству, нужно узнать его ID. Сделать это можно командой:

```
usbip list -l
```

Доступ к устройству открывается с помощью команды:

```
sudo usbip bind --busid=1-1
```

где **1-1** - это ID устройства.

Проверить, что устройство успешно привязано и доступно для использования, можно выполнив на сервере команду:

```
usbip list -r localhost
```

Для закрытия доступа к устройству необходимо ввести команду:

```
sudo usbip unbind -b 1-1
```

Настройка на клиенте

Клиент предназначен для подключения **USB-устройств**, опубликованных на сервере. Через клиента устройства, находящиеся на сервере, становятся доступными для локального использования, как если бы они были подключены непосредственно к клиентскому компьютеру.

Для начала работы необходимо установить утилиту *USBIP* командой:

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 vhci-hcd
```

Сохраните изменения и закройте редактор.

Проверить доступность USB-устройств, подключенных к серверу, можно выполнив на клиенте команду:

```
sudo usbip list -r <IP-адрес-сервера>
```

Для подключения открытого в общий доступ устройства на сервере к компьютеру-клиенту надо знать его ID и IP-адрес сервера. Для этого необходимо выполнить команду:

```
sudo usbip attach --remote=<IP-адрес-сервера> --busid=1-1
```

где:

- **1-1** — это ID устройства,
- **<IP-адрес-сервера>** — это IP-адрес сервера в формате **xx.xx.xx.xx**.

После подключения USB-устройства оно должно отображаться после выполнения команды:

```
lsusb
```

Для того чтобы отключить устройство из общего доступа, необходимо узнать его порт:

```
sudo usbip port
```

После того, как порт определен, можно отсоединить устройство:

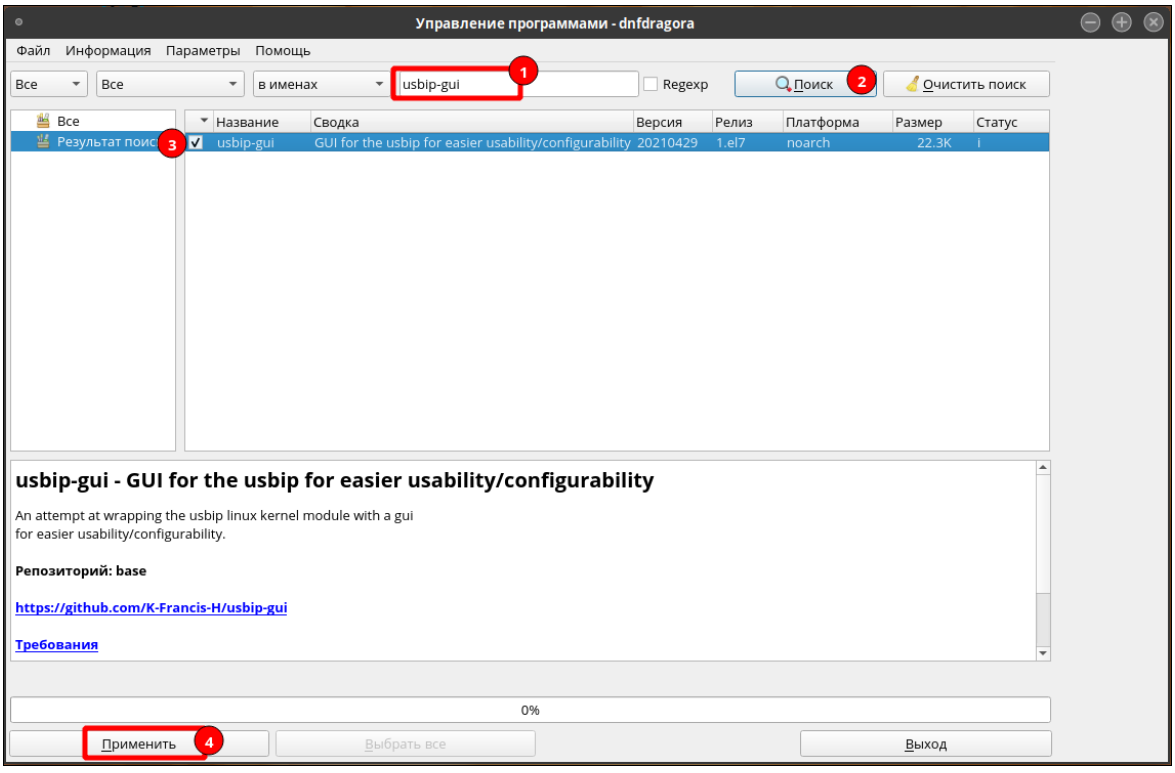
```
sudo usbip detach --port=0
```

Графическая утилита usbip-gui

В РЕД ОС также существует графическая утилита для предоставления в общий доступ USB-устройств через IP-сеть — **usbip-gui**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**usbip-gui**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.

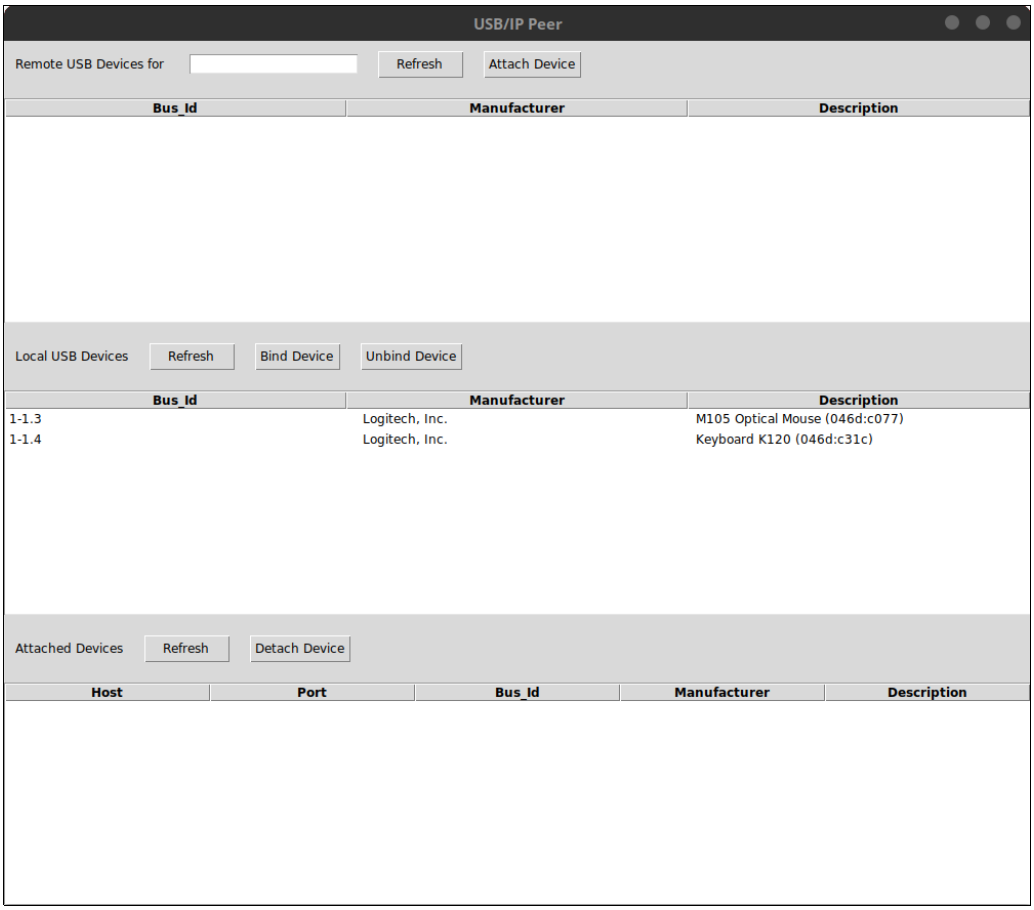


Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

```
sudo dnf install usbip-gui
```

После установки программа будет доступна из «**Главного меню**» — «**Администрирование**» — «**Управление USBIP**». Обратите

внимание, что для работы с программой необходимы права администратора или суперпользователя системы.



Сканер уязвимостей OpenSCAP

Установка OpenSCAP
Отображение информации о содержимом SCAP
Сканирование
Проверка содержимого SCAP
Практические примеры
Сканирование уязвимостей на удаленной машине
Сканирование docker-образов и контейнеров
CVE-сканирование контейнера
Пример сканирования контейнера docker с помощью пользовательской политики безопасности

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openscap-scanner-1:1.3.8-1, openscap-utils-1:1.3.8-1, openscap-containers-1.3.8-1

Во многих документах надзорных органов определены требования к мерам безопасности информационных систем, связанные с актуализацией используемых средств защиты и их регулярному обновлению. Так ФСТЭК России в Методическом документе о мерах защиты информации в государственных информационных системах (утверждён 11 февраля 2014 г.) прямо указывает, что оператором ГИС «должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе. При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

- устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств».

Но не стоит думать, что эта мера лишь ещё одно требование регулятора. Практика тестирования на проникновение показывает, что взлом хоста без установленных обновлений занимает не более 15 минут.

Отслеживать изменения в ОС и выход обновлений достаточно сложная и трудоемкая задача, которая нуждается в автоматизации. На сегодняшний день самым популярным методом автоматизации аудита безопасности является подход, предложенный **NIST** (Национальный институт стандартов и технологий США) и описанный в спецификации **SCAP** (Security Content Automation Protocol) в 2009 году.

Протокол автоматизации содержимого безопасности (**SCAP**) — это метод использования определённых стандартов для обеспечения автоматического управления уязвимостями, измерения и оценки соответствия политикам систем, развёрнутых в организации. Приложения, которые проводят мониторинг безопасности, используют стандарты при измерении систем для поиска уязвимостей и предлагают методы оценки этих результатов для оценки возможного воздействия. Набор спецификаций SCAP стандартизирует номенклатуру и форматы, используемые этими продуктами автоматизированного управления уязвимостями, измерения и соответствия политикам.

Начиная с SCAP версии 1.0 (ноябрь 2009 г.) одним из его компонентов является открытый язык уязвимостей и оценки (OVAL). **OVAL** — это международный стандарт информационной безопасности, стандарт сообщества для продвижения открытого и общедоступного контента безопасности, а также для стандартизации передачи этой информации по всему спектру инструментов и сервисов безопасности. OVAL включает в себя язык, используемый для кодирования сведений о системе, и набор репозиториев контента, хранящихся в сообществе. Язык стандартизирует три основных этапа процесса оценки:

- представление информации о конфигурации систем для тестирования;
- анализ системы на наличие заданного состояния машины (уязвимость, конфигурация, состояние исправления и т. д.);
- отчёт о результатах этой оценки.

Примером реализации SCAP является проект **OpenSCAP** (https://www.open-scap.org/). С помощью OpenSCAP вы можете проверить параметры конфигурации безопасности системы и проверить систему на наличие признаков компрометации, используя правила, основанные на стандартах и спецификациях.

OpenSCAP использует SCAP, набор спецификаций, поддерживаемых NIST. SCAP был создан для обеспечения стандартизированного подхода к обеспечению безопасности системы. OpenSCAP сочетается со многими спецификациями, такими как CPE, CCE и OVAL, для создания контрольного списка, выраженного SCAP, который может обрабатываться продуктами, проверенными SCAP.

Если вы хотите выполнить настройку или сканирование уязвимостей локальной системы, необходимо следующее:

- инструмент (**oscap** или SCAP Workbench);
- содержимое SCAP (поток исходных данных SCAP, XCCDF, OVAL...).

Для удобства пользователей мы уже подготовили файл определений OVAL для РЕД ОС, который доступен по адресу: https://redos.red-soft.ru/support/secure/redos.xml.

Установка OpenSCAP

Вы можете либо собрать OpenSCAP из исходного кода, предоставляемого разработчиком продукта, либо использовать существующую сборку для РЕД ОС из репозитория.

Чтобы установить **OpenSCAP** в РЕД ОС, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните следующую команду:

```
dnf install openscap-scanner openscap-utils
```

После завершения установки вы можете начать использовать **oscap** - инструмент командной строки.

Дальнейшая работа с утилитой выполняется с правами **локального пользователя**.

Чтобы отобразить версию **OpenSCAP**, поддерживаемые спецификации, встроенные имена **CPE** и поддерживаемые объекты **OVAL**, введите следующую команду:

```
oscap --version
```

Отображение информации о содержимом SCAP

Информация о файле SCAP может быть отображена с помощью команды oscap info:

```
oscap info redos.xml

Document type: OVAL Definitions
OVAL version: 5.10
Generated: 2022-10-17T12:11:58.000-03:00
Imported: 2022-10-17T12:11:58
```

Тип документа (*Document type*) описывает, в каком формате находится файл.

Импортировано (*Imported*) — это дата, когда файл был импортирован для использования с OpenSCAP. Поскольку OpenSCAP использует локальную файловую систему и не имеет собственного формата базы данных, дата импорта совпадает с датой изменения файла.

Сканирование

Основная цель OpenSCAP — выполнить настройку и сканирование уязвимостей локальной системы. OpenSCAP может оценивать исходные потоки данных SCAP, эталонные тесты XCCDF и определения OVAL и генерировать соответствующие результаты. Контент SCAP может предоставляться либо в одном файле (как исходный поток данных SCAP), либо в виде нескольких отдельных XML-файлов.

Документ SCAP может иметь форму одного файла OVAL (файл определения OVAL). Инструмент oscap обрабатывает файл определения OVAL во время оценки определений OVAL. Он собирает системную информацию, оценивает ее и создает файл результатов OVAL. Результат оценки каждого определения OVAL выводится в стандартный поток вывода. В следующих примерах описываются наиболее распространенные сценарии, связанные с файлом определения OVAL.

Для оценки определений OVAL можно использовать команду:

```
oscap oval eval --results <файл-результат> <OVAL-файл>
```

где:

- <**OVAL-файл**> - это файл определения OVAL;
- <**файл-результат**> - это путь, по которому будет храниться файл результатов OVAL.

Можно выбрать и оценить одно конкретное определение в данном файле определения OVAL, используя опцию **--id**:

```
oscap oval eval --id oval:redos:def:60 --results oval-results.xml redos.xml

Definition oval:redos:def:60: true
Evaluation done.
```

Проверка содержимого SCAP

Инструмент **oscap** можно использовать для проверки содержимого безопасности по стандартным XML-схемам SCAP. Результаты проверки выводятся в стандартный поток ошибок (**stderr**). Общий синтаксис команды проверки следующий:

```
oscap module validate [module_options_and_arguments] <ФАЙЛ>
```

где

- **<ФАЙЛ>** - полный путь к проверяемому файлу.
- **Module** - можно использовать: **xccdf**, **oval**, **cpe** или **cve**.

При проверке спецификации OVAL или XCCDF включается дополнительная проверка на основе **Schematron**. Этот метод проверки работает медленнее, но обеспечивает более глубокий анализ.

Запустите одну из следующих команд, чтобы проверить документ OVAL или XCCDF без проверок **Schematron**:

```
oscap xccdf validate --skip-schematron xccdf-file.xml

или

oscap oval validate --skip-schematron oval-file.xml
```

Результаты проверки выводятся в стандартный поток ошибок (**stderr**).

Обратите внимание, что для остальной **oscap**-функциональности, если вы не укажете **--skip-validation** (**--skip-valid**), проверка будет происходить автоматически перед использованием файлов. Поэтому вам не нужно явно проверять поток данных перед использованием. Хотя он не будет включать этап проверки на основе **Schematron**.

Практические примеры

В этом разделе демонстрируется практическое использование содержимого безопасности, предоставляемого для продуктов РЕД СОФТ:

1) загрузите описание уязвимостей:

```
wget https://redos.red-soft.ru/support/secure/redos.xml
```

2) запустите сканирование:

```
oscap oval eval --results results.xml --report report.html redos.xml
```

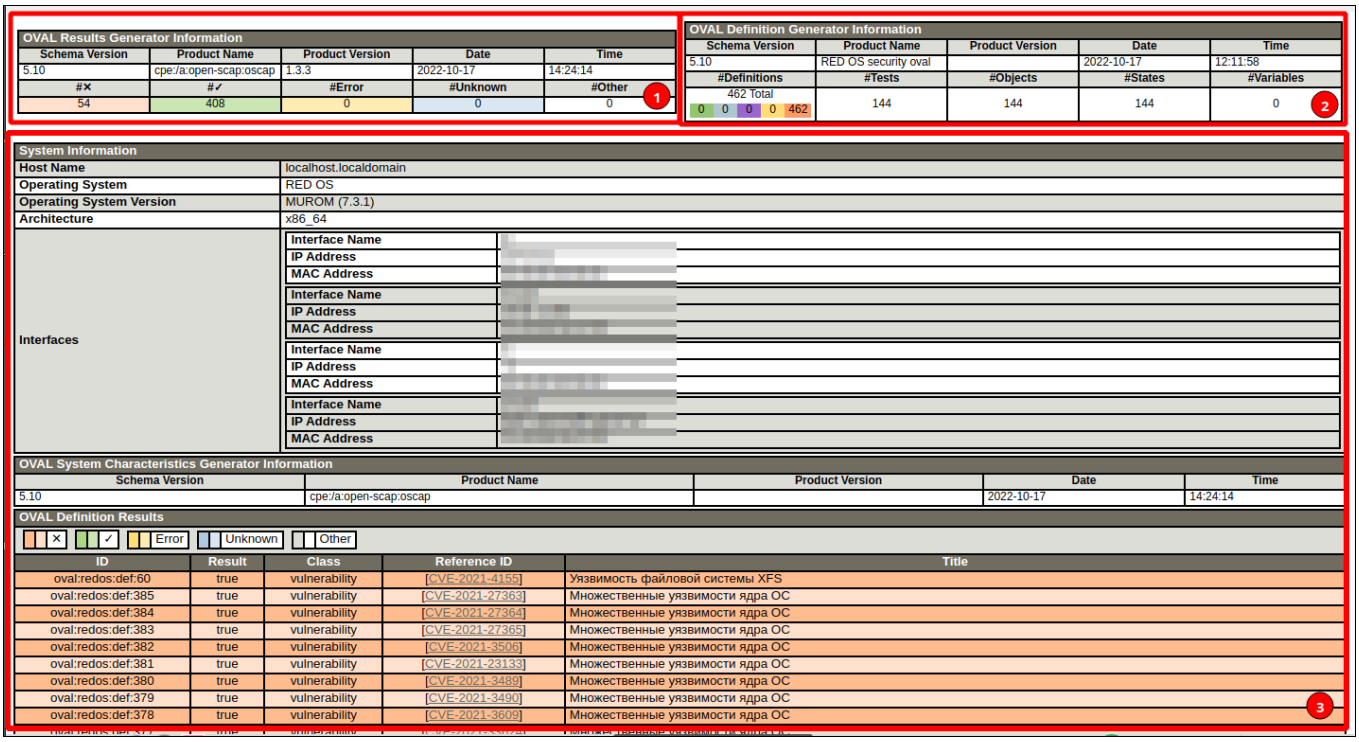
3) оцените результаты:

```
Definition oval:redos:def:60: true
```

Это образец вывода, в котором сообщается, что рекомендации по безопасности РЕД ОС (ROS-20220318-03) def:60 были выпущены, но обновление не было применено на конкретном экземпляре ОС (**true**).

Также вместе с выводом результатов в стандартный поток вывода генерируются удобочитаемый отчет **report.html** и машиночитаемый отчет **results.xml**.

Внешний вид **report.html** приведён на рисунке ниже.



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap	1.3.3	2022-10-17	14:24:14
#×	#✓	#Error	#Unknown	#Other
54	408	0	0	0

1

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	RED OS security oval		2022-10-17	12:11:58
#Definitions	#Tests	#Objects	#States	#Variables
462 Total: 0 0 0 0 462	144	144	144	0

2

System Information

Host Name	localhost.localdomain
Operating System	RED OS
Operating System Version	MUROM (7.3.1)
Architecture	x86_64
Interfaces	Interface Name / IP Address / MAC Address (×5)

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap		2022-10-17	14:24:14

OVAL Definition Results

× ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:redos:def:60	true	vulnerability	[CVE-2021-4155]	Уязвимость файловой системы XFS
oval:redos:def:385	true	vulnerability	[CVE-2021-27363]	Множественные уязвимости ядра ОС
oval:redos:def:384	true	vulnerability	[CVE-2021-27364]	Множественные уязвимости ядра ОС
oval:redos:def:383	true	vulnerability	[CVE-2021-27365]	Множественные уязвимости ядра ОС
oval:redos:def:382	true	vulnerability	[CVE-2021-3506]	Множественные уязвимости ядра ОС
oval:redos:def:381	true	vulnerability	[CVE-2021-23133]	Множественные уязвимости ядра ОС
oval:redos:def:380	true	vulnerability	[CVE-2021-3489]	Множественные уязвимости ядра ОС
oval:redos:def:379	true	vulnerability	[CVE-2021-3490]	Множественные уязвимости ядра ОС
oval:redos:def:378	true	vulnerability	[CVE-2021-3609]	Множественные уязвимости ядра ОС

3

Условно отчёт можно разделить на три основные части: информация о самом генераторе результатов OVAL (**1**), информация о генераторе определений OVAL (**2**) и результаты сканирования (**3**).

Информация о генераторе результатов содержит версию **oscap**, использованную при сканировании, дату и время операции и итоговые сведения об обнаруженных проблемах.

Информация о генераторе определений содержит основную информацию о файле определений OVAL — название, дату и время его выпуска, количество определений и тестов.

Результат сканирования в первую очередь содержит информацию об исследуемом хосте: его имя, название ОС, версию и архитектуру. Также дана дополнительная расширенная информация об обнаруженных хостах ОС. Самая важная часть отчета — результаты проверки актуальности установленных пакетов ОС. Строки отчета имеют цветовое выделение согласно статусу обнаруженной проблемы: **зеленые** строки отмечают пакеты, которые не установлены в системе или имеют актуальную версию, **оранжевым** отмечены пакеты, требующие обновления.

Таблица описания имеет следующие столбцы:

- **ID** — уникальный идентификатор описания, присваиваемый производителем ОС;
- **Result** — результат выполнения проверки: **false** — если проблем не обнаружено, **true** — требуется исправление недостатка;
- **Class** — в данном случае всегда принимает значение **vulnerability** (уязвимость);
- **Reference ID** — ссылка на бюллетень производителя, связанная с базой знаний РЕД ОС, где хранится дополнительная информация об уязвимости;
- **Title** — заголовок названия бюллетеня, позволяющий понять, о какой уязвимости идёт речь.

Файл **results.xml** содержит те же сведения, что и html-файл отчета, но более удобен для использования в других системах анализа и сканирования уязвимостей.



Сканирование уязвимостей на удаленной машине

Сначала необходимо обеспечить доступ к клиентской машине. Для этого потребуется настроить сетевой протокол **ssh**, который позволит получить удаленный доступ к клиенту. Подробную информацию о настройке удаленного доступа по **ssh** см. в нашей статье «Работа с клиентом и сервером SSH».

Далее на сервере установите сканер уязвимостей командой (необходимы **права администратора** системы или суперпользователя **root**):

```
dnf install openscap-scanner openscap-utils
```

Загрузите файл определений OVAL для РЕД ОС:

```
wget https://redos.red-soft.ru/support/secure/redos.xml
```

Подключитесь к клиентской машине и установите сканер **OpenSCAP**:

```
ssh user@10.81.186.86
su -
dnf install openscap-scanner
```

Отключитесь от сессии клиентской машины:

```
exit
```

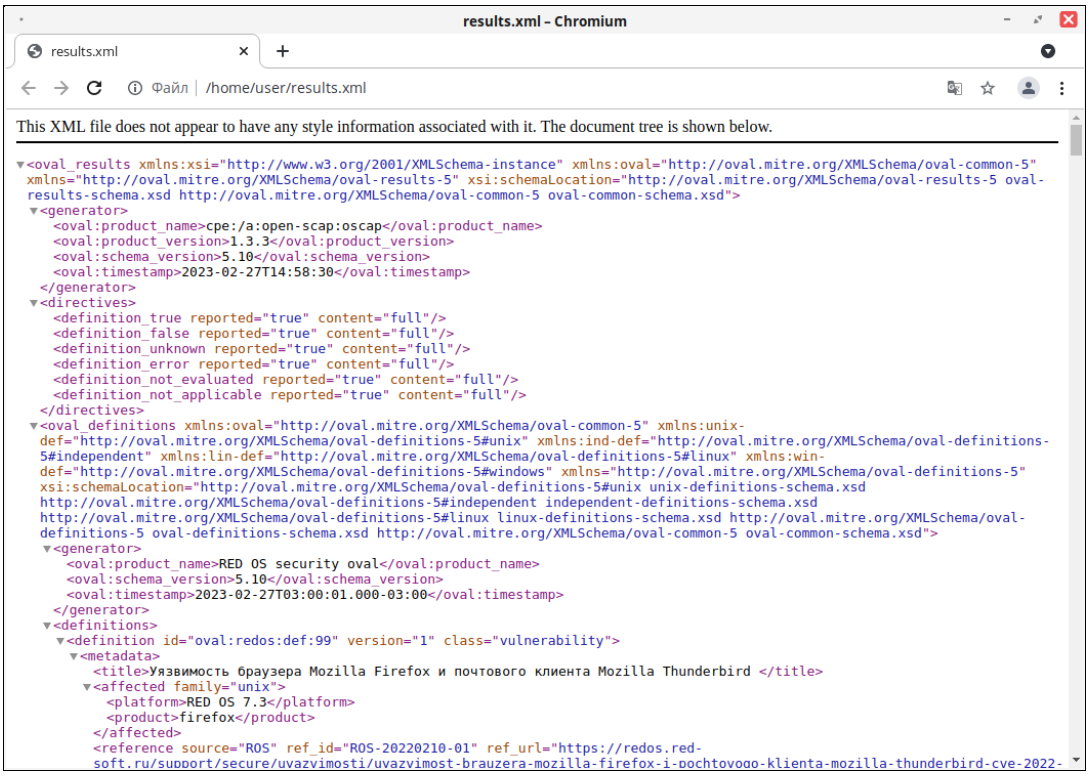
После установки можно запускать сканирование клиентской машины:

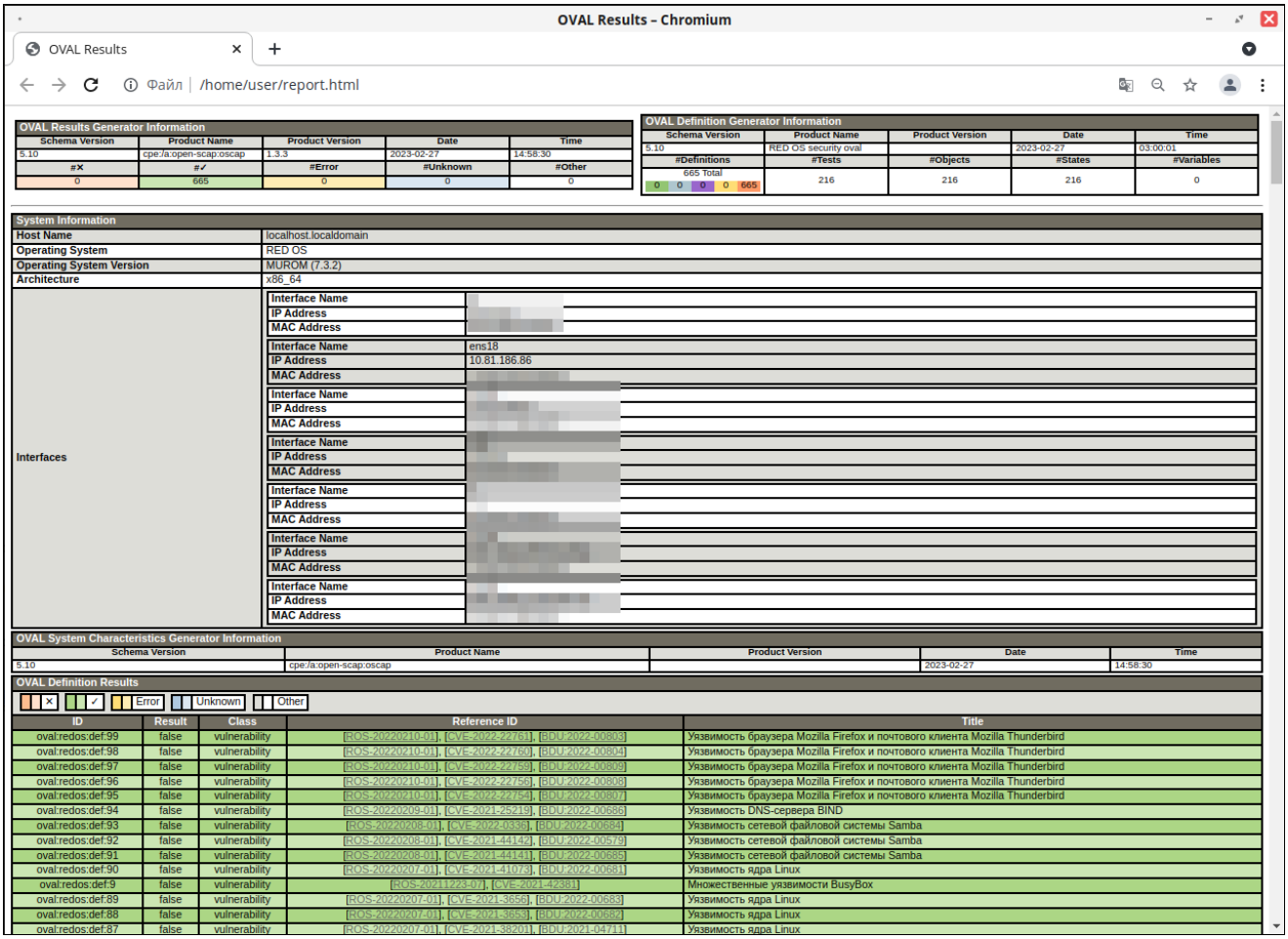
```
oscap-ssh user@10.81.186.86 22 oval eval --results results.xml --report report.html redos.xml
```

где:

- user@10.81.186.86 — имя пользователя и IP-адрес клиента;
- **22** — номер порта для подключения по ssh;
- **results.xml** — путь к файлу-результату сканирования;
- **report.html** — путь к файлу-отчету сканирования;
- **redos.xml** — путь к файлу OVAL РЕД ОС.

Результаты сканирования:





Сканирование docker-образов и контейнеров

Функционал **openscap** позволяет проводить сканирование на уязвимости не только запущенной локальной машины, но также docker-образов и контейнеров. Для этого необходимо установить **docker**:

```
dnf install docker-ce docker-registry python3-docker
```

Запустите **docker** и добавьте его в автозагрузку:

```
systemctl enable docker --now
```

Дополнительно потребуется установить набор инструментов **openSCAP**. Для сканирования используется инструмент **oscap-docker** из пакета **openscap-containers**, который можно установить с помощью команды:

```
dnf install openscap-containers
```

oscap-docker — это простой инструмент, предоставляющий интерфейс для использования **oscap** в среде **Docker** и позволяющий проводить сканирование запущенных контейнеров и образов **Docker** почти так же, как сканирование локальной машины. Получить список доступных образов можно командой:

```
docker search registry.red-soft.ru/ubi7
```

Установка необходимого образа производится командой:

```
docker pull registry.red-soft.ru/ubi7/<название_образа>
```

Запуск контейнера из образа осуществляется командой:

```
docker run --name "REDOS" -ti registry.red-soft.ru/ubi7/<название_образа> /bin/bash
```

Данная команда запустит новый контейнер под названием **REDOS** и предоставит интерактивный интерфейс.

CVE-сканирование контейнера

oscap-docker довольно прост в использовании, команда имеет следующий синтаксис:

```
oscap-docker <образ/контейнер>[-cve] <идентификатор_образа/контейнера> <параметры_oscap>
```

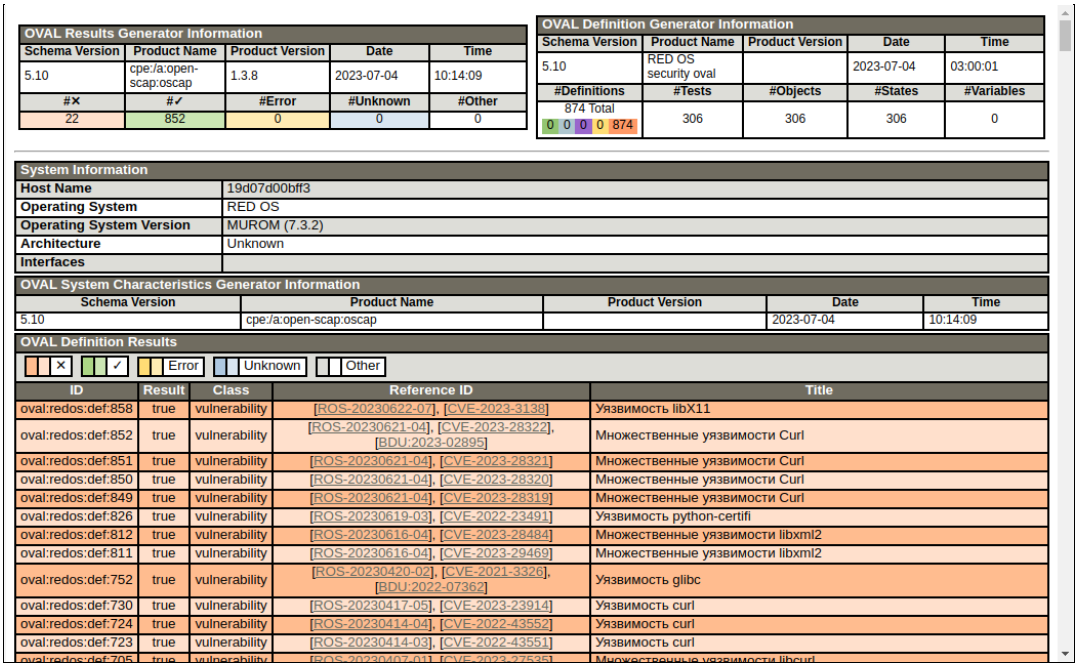
Запуск сканирования локального запущенного контейнера с автоматической загрузкой файла определений **OVAL** для РЕД ОС::

```
oscap-docker container-cve REDOS --results results.xml --report report.html
```

Если контейнер не запущен, его можно запустить командой:

```
docker start REDOS
```

В результате сканирования будет сгенерирован файл результатов **OVAL** и удобочитаемый **HTML**-отчет.



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap	1.3.8	2023-07-04	10:14:09

#×	#✓	#Error	#Unknown	#Other
22	852	0	0	0

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	RED OS security oval		2023-07-04	03:00:01

#Definitions	#Tests	#Objects	#States	#Variables
874 Total: 0 0 0 0 874	306	306	306	0

System Information

Host Name	19d07d00bff3
Operating System	RED OS
Operating System Version	MUROM (7.3.2)
Architecture	Unknown
Interfaces	

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap		2023-07-04	10:14:09

OVAL Definition Results

× ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:redos:def:858	true	vulnerability	[ROS-20230622-07], [CVE-2023-3138]	Уязвимость libX11
oval:redos:def:852	true	vulnerability	[ROS-20230621-04], [CVE-2023-28322], [BDU:2023-02895]	Множественные уязвимости Curl
oval:redos:def:851	true	vulnerability	[ROS-20230621-04], [CVE-2023-28321]	Множественные уязвимости Curl
oval:redos:def:850	true	vulnerability	[ROS-20230621-04], [CVE-2023-28320]	Множественные уязвимости Curl
oval:redos:def:849	true	vulnerability	[ROS-20230621-04], [CVE-2023-28319]	Множественные уязвимости Curl
oval:redos:def:826	true	vulnerability	[ROS-20230619-03], [CVE-2022-23491]	Уязвимость python-certifi
oval:redos:def:812	true	vulnerability	[ROS-20230616-04], [CVE-2023-28484]	Множественные уязвимости libxml2
oval:redos:def:811	true	vulnerability	[ROS-20230616-04], [CVE-2023-29469]	Множественные уязвимости libxml2
oval:redos:def:752	true	vulnerability	[ROS-20230420-02], [CVE-2021-3326], [BDU:2022-07362]	Уязвимость glibc
oval:redos:def:730	true	vulnerability	[ROS-20230417-05], [CVE-2023-23914]	Уязвимость curl
oval:redos:def:724	true	vulnerability	[ROS-20230414-04], [CVE-2022-43552]	Уязвимость curl
oval:redos:def:723	true	vulnerability	[ROS-20230414-03], [CVE-2022-43551]	Уязвимость curl
oval:redos:def:705	true	vulnerability	[ROS-20230407-01], [CVE-2023-27535]	Множественные уязвимости libcurl



Пример сканирования контейнера docker с помощью пользовательской политики безопасности

Существует возможность использования собственной политики безопасности для сканирования контейнера. Так, например, можно использовать файл определений **OVAL** для РЕД ОС.

Для запуска сканирования с автоматическим скачиванием файла описания уязвимостей для РЕД ОС:

```
oscap-docker image-cve registry.red-soft.ru/ubi7/ubi --results results1.xml --report report1.html
```

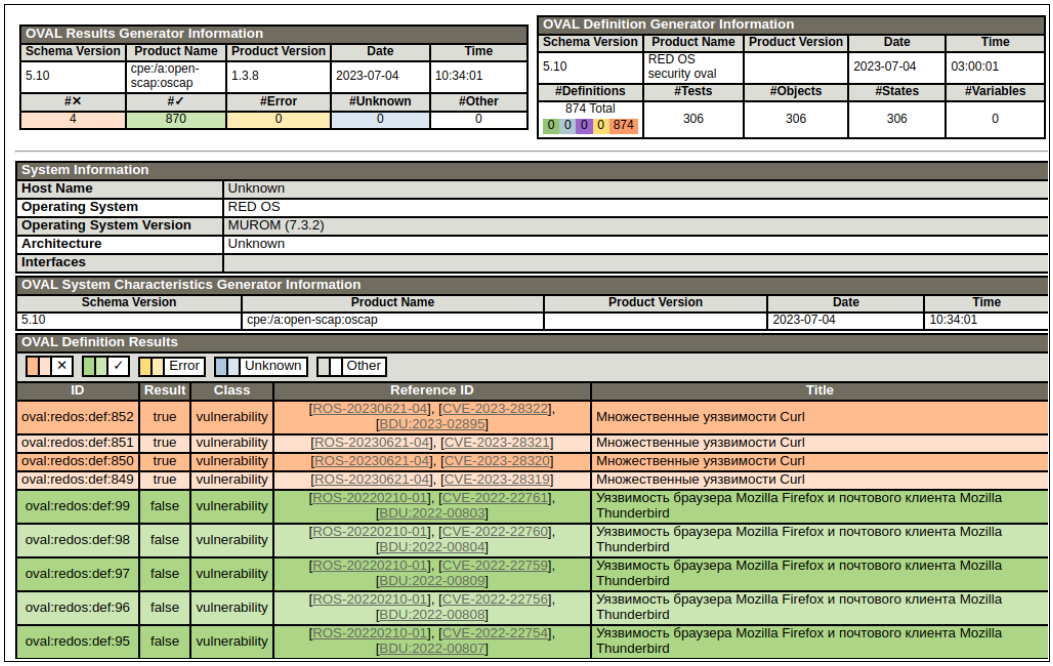
Также есть возможность загрузить файл определений **OVAL** для РЕД ОС:

```
wget https://redos.red-soft.ru/support/secure/redos.xml
```

Затем выполнить сканирование с использованием пользовательского содержимого:

```
oscap-docker image-cve registry.red-soft.ru/ubi7/ubi --results results1.xml --report report1.html --file redos.xml
```

Результаты сканирования:



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap	1.3.8	2023-07-04	10:34:01

#×	#✓	#Error	#Unknown	#Other
4	870	0	0	0

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	RED OS security oval		2023-07-04	03:00:01

#Definitions	#Tests	#Objects	#States	#Variables
874 Total: 0 0 0 0 874	306	306	306	0

System Information

Host Name	Unknown
Operating System	RED OS
Operating System Version	MUROM (7.3.2)
Architecture	Unknown
Interfaces	

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.10	cpe:/a:open-scap:oscap		2023-07-04	10:34:01

OVAL Definition Results

× ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:redos:def:852	true	vulnerability	[ROS-20230621-04], [CVE-2023-28322], [BDU:2023-02895]	Множественные уязвимости Curl
oval:redos:def:851	true	vulnerability	[ROS-20230621-04], [CVE-2023-28321]	Множественные уязвимости Curl
oval:redos:def:850	true	vulnerability	[ROS-20230621-04], [CVE-2023-28320]	Множественные уязвимости Curl
oval:redos:def:849	true	vulnerability	[ROS-20230621-04], [CVE-2023-28319]	Множественные уязвимости Curl
oval:redos:def:99	false	vulnerability	[ROS-20220210-01], [CVE-2022-22761], [BDU:2022-00803]	Уязвимость браузера Mozilla Firefox и почтового клиента Mozilla Thunderbird
oval:redos:def:98	false	vulnerability	[ROS-20220210-01], [CVE-2022-22760], [BDU:2022-00804]	Уязвимость браузера Mozilla Firefox и почтового клиента Mozilla Thunderbird
oval:redos:def:97	false	vulnerability	[ROS-20220210-01], [CVE-2022-22759], [BDU:2022-00809]	Уязвимость браузера Mozilla Firefox и почтового клиента Mozilla Thunderbird
oval:redos:def:96	false	vulnerability	[ROS-20220210-01], [CVE-2022-22756], [BDU:2022-00808]	Уязвимость браузера Mozilla Firefox и почтового клиента Mozilla Thunderbird
oval:redos:def:95	false	vulnerability	[ROS-20220210-01], [CVE-2022-22754], [BDU:2022-00807]	Уязвимость браузера Mozilla Firefox и почтового клиента Mozilla Thunderbird

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<oval_results xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
 xmlns="http://oval.mitre.org/XMLSchema/oval-results-5" xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-results-5 oval-
 results-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd">
  <generator>
    <oval:product_name>cpe:/a:open-scap:oscap</oval:product_name>
    <oval:product_version>1.3.8</oval:product_version>
    <oval:schema_version>5.10</oval:schema_version>
    <oval:timestamp>2023-07-04T10:34:01</oval:timestamp>
  </generator>
  <directives>
    <definition_true reported="true" content="full"/>
    <definition_false reported="true" content="full"/>
    <definition_unknown reported="true" content="full"/>
    <definition_error reported="true" content="full"/>
    <definition_not_evaluated reported="true" content="full"/>
    <definition_not_applicable reported="true" content="full"/>
  </directives>
  <oval_definitions xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:unix-
  def="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix" xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-
  5#independent" xmlns:lin-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" xmlns:win-
  def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" xmlns:mac-def="http://oval.mitre.org/XMLSchema/oval-
  definitions-5#macos" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix unix-definitions-schema.xsd
  http://oval.mitre.org/XMLSchema/oval-definitions-5#independent independent-definitions-schema.xsd
  http://oval.mitre.org/XMLSchema/oval-definitions-5#unix unix-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-
  definitions-5#linux linux-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-definitions-5#windows windows-
  definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-definitions-5#macos macos-definitions-schema.xsd
  http://oval.mitre.org/XMLSchema/oval-definitions-5 oval-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-5
  oval-common-schema.xsd">
    <generator>
      <oval:product_name>RED OS security oval</oval:product_name>
      <oval:schema_version>5.10</oval:schema_version>
      <oval:timestamp>2023-07-04T03:00:01.000-03:00</oval:timestamp>
    </generator>
    <definitions>
      <definition id="oval:redos:def:99" version="1" class="vulnerability">
        <metadata>
          <title>Уязвимость браузера Mozilla Firefox и почтового клиента Mozilla Thunderbird </title>
          <affected family="unix">
            <platform>RED OS 7.3</platform>
```

Тестирование аппаратного обеспечения

amtu — утилита тестирования абстрактной машины (Abstract Machine Test Utility — AMTU).

Синтаксис:

```
amtu [ -dmsinph ]
```

AMTU - это административная утилита, которая проверяет, соблюдаются ли основные механизмы защиты аппаратного обеспечения.

AMTU выполняет следующие тесты:

- **память**: произвольно записывает данные в области памяти, затем считывает память, чтобы гарантировать, что записанные значения остаются неизменными;
- **разделение памяти**: обеспечивает, чтобы программы пользовательского пространства не могли читать и записывать в области памяти, используемые такими элементами, как видеопамять и код ядра;
- **контроллер ввода/вывода — сеть**: проверяет, что переданные случайные данные также являются данными, полученными для каждого настроенного сетевого устройства. Проверяет только настроенные устройства Ethernet и Token Ring. Не проверяет асинхронные устройства;
- **контроллер ввода/вывода — диск**: проверяет, что случайные данные, записанные на диски, остаются неизменными. Проверяются только контроллеры IDE и SCI, связанные с установленными файловыми системами. Контроллеры дисков с файловыми системами, доступными только для чтения, не проверяются;
- **инструкции режима супервизора**: проверяет, что принудительное использование свойств привилегированных инструкций в режиме супервизора, по-прежнему действует. Набор привилегированных инструкций, проверенных для подтверждения этого, зависит от архитектуры.

Для команды amtu доступны следующие параметры:

- **-d** - выводить отладочные сообщения;
- **-m** - выполнить проверку памяти;
- **-s** - выполните проверку разделения памяти;
- **-i** - выполнить тест контроллера ввода-вывода;
- **-n** - выполнить - сетевой тест;
- **-p** - выполнить проверку инструкций режима супервизора;
- **-h** - показать справку.

Команда amtu выдает следующие коды возврата при выполнении:

- **-1** — ошибка выполнения;
- **0** — успех.

Исследование сети с помощью консольной утилиты nmap

Установка
Примеры работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** nmap-2:7.80-4

NMAP — инструмент с открытым исходным кодом для исследования сети и аудита безопасности. Он был разработан для быстрого сканирования больших сетей, но также отлично подходит для отдельных хостов в сети.

Nmap способен определить, какие хосты доступны в сети и какие сервисы они предоставляют, версии операционных систем, используемые типы фильтров пакетов/брандмауэров и десятки других характеристик.

Обычно **nmap** используется для аудита безопасности, но многие системные и сетевые администраторы находят его полезным для рутинных задач, таких как инвентаризация сети, управление графиками обновления службы и мониторинг работоспособности хостов или служб.

Установка

Для установки **nmap** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install nmap
```

Дальнейшая работа с утилитой производится с правами локального пользователя.

Примеры работы

1. Проверка доступности порта:

```
nmap 10.81.1.144 -p 22
```

```
[~]$ sudo nmap 10.81.1.144 -p 22
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-13 15:36 MSK
Nmap scan report for 10.81.1.144
Host is up (0.00091s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[~]$
```

2. Показать все открытые порты на сетевом узле:

```
nmap -sV 10.81.1.144 -p 1-65535 | grep open
```

```
[~]$ sudo nmap -sV 10.81.1.144 -p 1-65535 | grep open
22/tcp    open  ssh          OpenSSH 8.2 (protocol 2.0)
53/tcp    open  domain       (generic dns response: NOTIMP)
88/tcp    open  kerberos-sec (server time: 2022-07-13 12:42:35Z)
111/tcp   open  rpcbind      2-4 (RPC #100000)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
389/tcp   open  ldap         (Anonymous bind OK)
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
464/tcp   open  kpasswd5?
636/tcp   open  ssl/ldap     (Anonymous bind OK)
3268/tcp  open  ldap         (Anonymous bind OK)
3269/tcp  open  ssl/ldap     (Anonymous bind OK)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
```

Возможен вариант с указанием параметра **--open**:

```
nmap --open 10.81.1.144
```

```
[~]$ sudo nmap --open 10.81.1.144
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 10.81.1.144
Host is up (0.00062s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
```

3. Сканировать сеть методом **ping** для обнаружения активных узлов:

```
nmap -sn 10.81.81.1/24
```

При этом в выводе команды будут отображаться IP и MAC-адреса.

```
[~]$ sudo nmap -sP 10.81.81.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-13 16:05 MSK
Nmap scan report for 10.81.81.186
Host is up (0.000055s latency).
MAC Address: 8C:8C:AA:00:26:03 (Unknown)
Nmap scan report for 10.81.81.206
Host is up (0.00017s latency).
MAC Address: 2C:56:DC:4B:22:99 (Asustek Computer)
Nmap scan report for 10.81.81.207
Host is up (0.00027s latency).
MAC Address: 56:6F:94:51:00:01 (Unknown)
Nmap scan report for 10.81.81.210
Host is up (0.00066s latency).
MAC Address: 56:6F:94:51:00:09 (Unknown)
Nmap scan report for 10.81.81.81
Host is up.
```

4. Информация о сетевом узле:

```
nmap -sV 10.81.1.144
```

5. Сканирование определенных портов, в примере указаны 22 (**ssh**) и 53 (**dns**):

```
nmap -sV -p 22,53 8.8.8.8
```

```
[~]$ sudo nmap -sV -p 22,53 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.040s latency).

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
53/tcp open     domain  ISC BIND 9.11.3-1ubuntu1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_k
```

Также можно определить диапазон адресов для сканирования:

```
nmap -sV -p 22,53 10.81.1.1-50
```

6. Сканирование всей подсети:

```
nmap 192.168.1.0/24
```

7. Исключение нескольких хостов по их IP-адресам:

```
nmap 192.168.1.0/24 --exclude 192.168.1.10,192.168.1.154
```

8. Для быстрого сканирования используется опция **-F**:

```
nmap -F 10.81.1.1-10
```

9. Быстрое сканирование открытых портов на всех хостах подсети:

```
nmap -T5 192.168.1.1/24
```

10. Сканирование с определением версии ОС:

```
nmap -O -v --osscan-guess 192.168.1.1
```

11. Сканирование подсети с помощью **UDP ping**:

```
nmap -PU 192.168.1.1/24
```

12. Сканирование с использованием подмены MAC-адреса, в данном случае одно устройство/приложение маскируется под другое, указывая его MAC-адрес:

```
nmap -v -sT -PN --spoof-mac 0 192.168.1.1
```

В данном примере «**0**» означает, что **nmap** выберет случайный MAC-адрес.

Исследование сети с помощью графической утилиты zenmap

Установка
Описание программы
Профили сканирования
Пользовательские профили

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: nmap-zenmap-2:7.80-4

Zenmap — это мультиплатформенный графический интерфейс утилиты **nmap** и средство просмотра результатов анализа. **Zenmap** стремится сделать **nmap** простым в использовании для новичков, а опытным пользователям он предоставляет расширенные возможности.

Вы можете подробнее ознакомиться с работой утилиты **Zenmap**, просмотрев наши обучающие видео:

- на **RuTube** — Zenmap - графическая утилита исследования сети;
- в **Яндекс.Дзен** — Zenmap - графическая утилита исследования сети;
- в **VK Видео** — Zenmap - графическая утилита исследования сети.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **zenmap** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

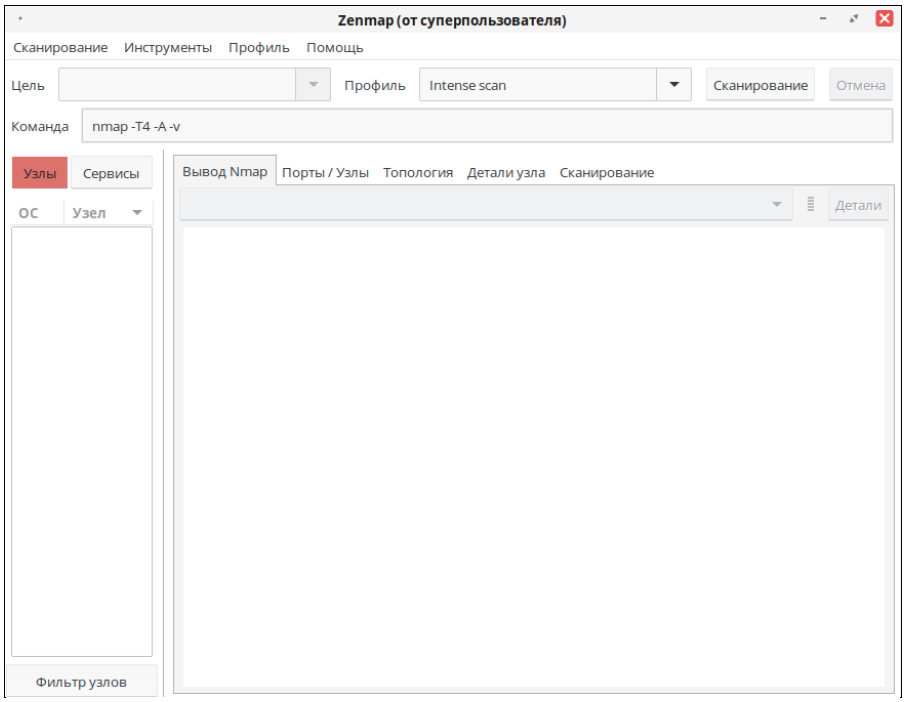
```
dnf install nmap-zenmap
```

Запуск программы доступен через «**Главное меню**» - «**Интернет**» - «**Zenmap**» или через терминал командой:

```
zenmap
```

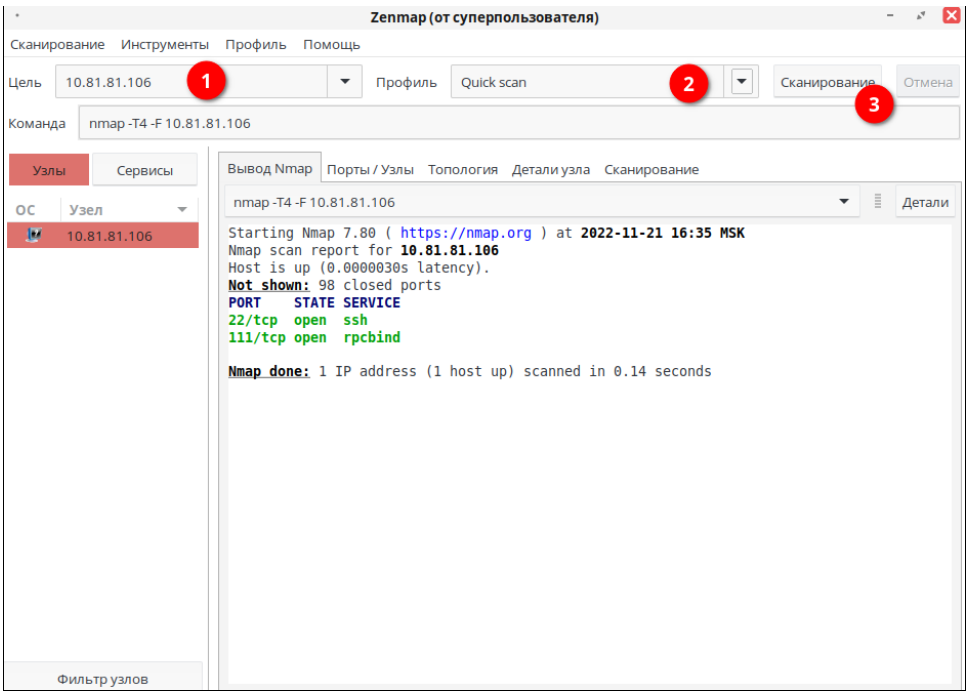
Для работы в программе **необходимы права** суперпользователя **root**.

Основное окно программы выглядит следующим образом:



Описание программы

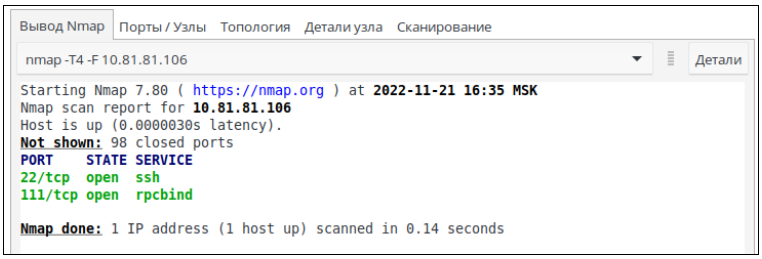
Перед началом сканирования необходимо указать в поле «**Цель**» (**1**) IP-адрес, имя домена, диапазон IP-адресов или подсеть для сканирования, а во вкладке «**Профиль**» (**2**) выбрать профиль сканирования. Запуск сканирования осуществляется нажатием кнопки «**Сканирование**» (**3**).



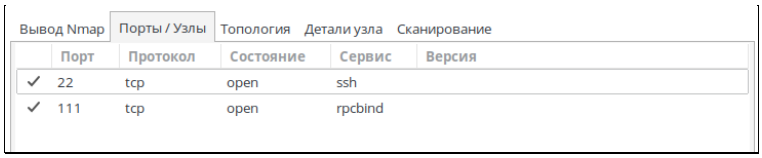
Ниже расположены следующие вкладки:

- Вывод Nmap;
- Порты/Узлы;
- Топология;
- Детали узла;
- Сканирование.

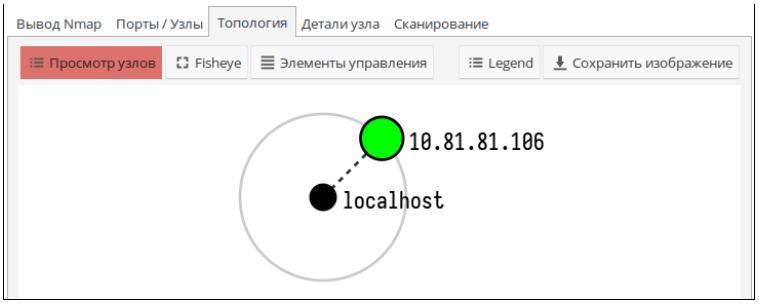
Вкладка «**Вывод Nmap**» показывает стандартный вывод информации **nmap**.



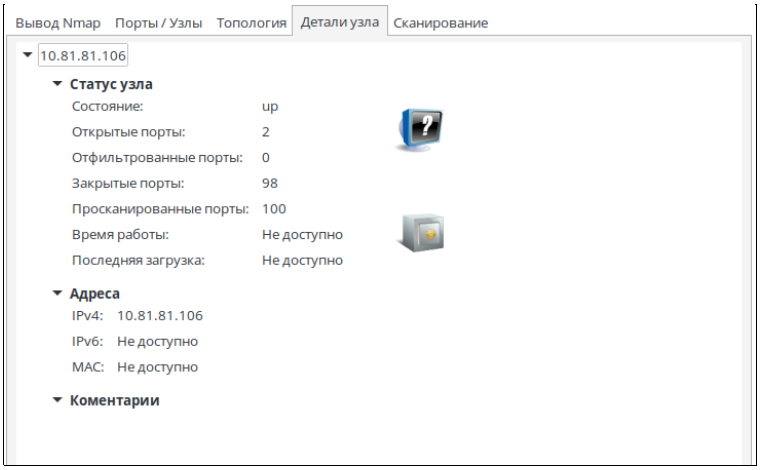
Вкладка «**Порты/Узлы**» выводит службы или порты с дополнительной информацией, отсортированной по узлам. Если выбран один узел, отображается статус сканированных портов.



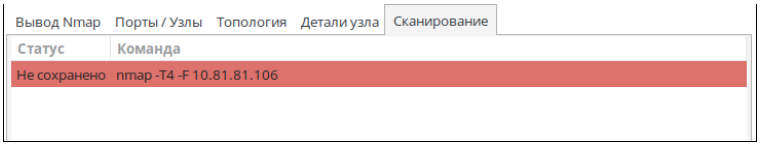
Вкладка «**Топология**» показывает топологию сети цели в графическом режиме.



Вкладка «**Детали узла**» демонстрирует информацию об отсканированном узле, которая включает в себя имя узла, состояние сканированных портов, время безотказной работы, адреса подключения и др.



Вкладка «**Сканирование**» отображает историю всех выполненных проверок, включая запущенные проверки. Также можно добавить проверки, импортировав файл кнопкой «**Добавить отчет**».



Профили сканирования

В **zenmap** существует несколько профилей сканирования:

- **Intense scan** – интенсивное сканирование;
- **Intense scan plus UDP** – интенсивное сканирование плюс UDP;
- **Intense scan, all TCP ports** – интенсивное сканирование, со всеми TCP-портами;
- **Intense scan, no ping** – интенсивное сканирование, без пинга;

- **Ping scan** – пинг-сканирование;
- **Quick scan** – быстрое сканирование;
- **Quick scan plus** – быстрое сканирование плюс;
- **Quick traceroute** – быстрая трассировка;
- **Regular scan** – обычное сканирование;
- **Slow comprehensive scan** – медленное комплексное сканирование.

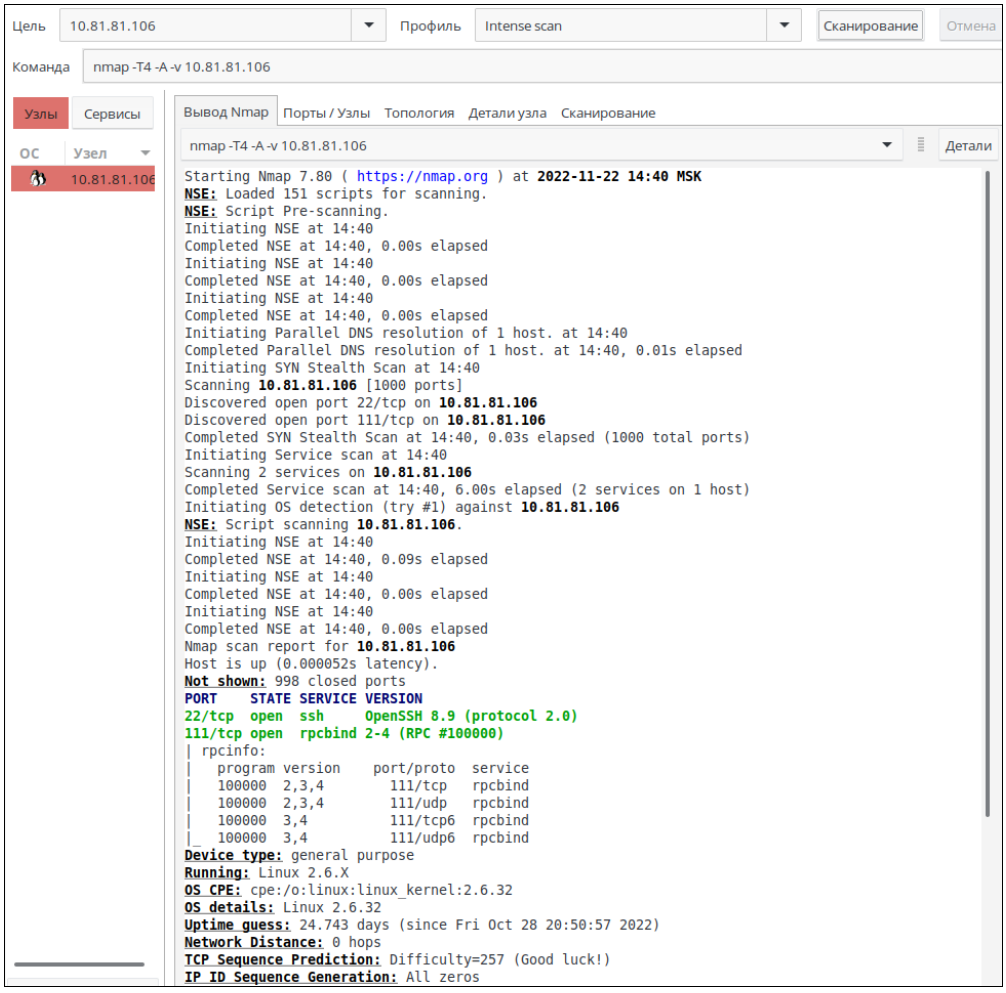
1. **Intense scan** - этот профиль быстро сканирует наиболее распространенные TCP-порты, а также определяет тип ОС, её службы и версии.

Команда:

```
nmap -T4 -A -v <цель>
```

где:

- **-T4** — временной параметр, который находится в диапазоне от 0 до 5, где 0 — самый медленный тип сканирования, а 5 — самый быстрый тип сканирования;
- **-A** — параметр, определяющий тип ОС и ее версии;
- **-v** — параметр, который отображает подробную информацию и детали сканирования, чтобы пользователь знал текущее состояние сканирования.



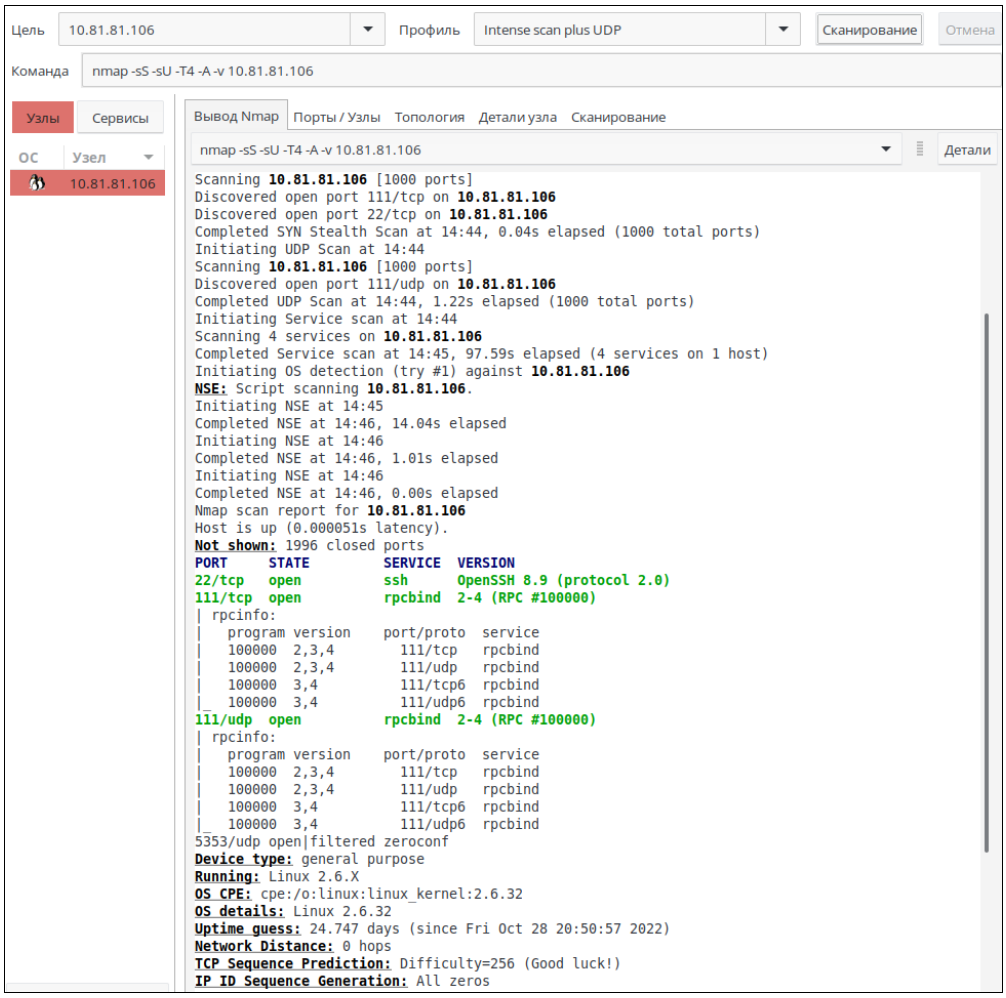
2. **Intense scan plus UDP** – работает как обычное интенсивное сканирование, однако дополнительно сканирует порты UDP.

Команда:

```
nmap -sS -sU -T4 -A -v <цель>
```

где:

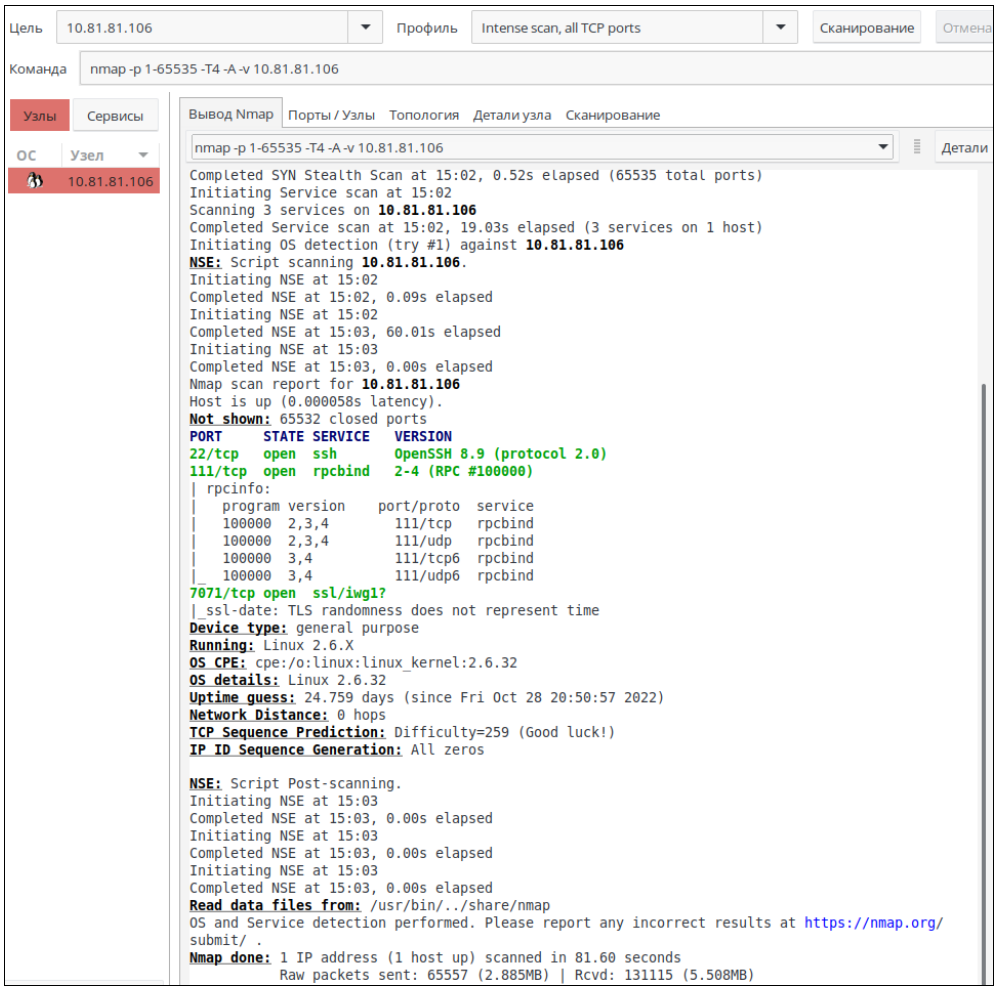
- **-sS** – указывает nmap сканировать порты TCP с помощью пакетов SYN;
- **-sU** — параметр, отвечающий за сканирование UDP-портов.

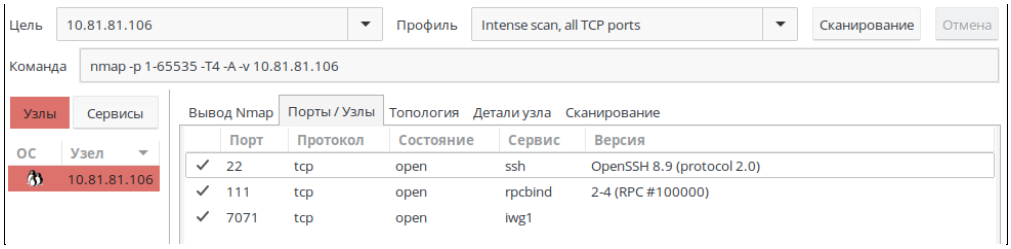


3 . **Intense scan, all TCP ports** – поскольку для сканирования всех портов требуется время, **nmap** обычно сканирует 1000 самых распространённых портов. При *Интенсивном сканировании* проверка **nmap** идёт по всем портам от 1 до 65535 (макс.).

Команда:

```
nmap -p 1-65535 -T4 -A -v <цель>
```





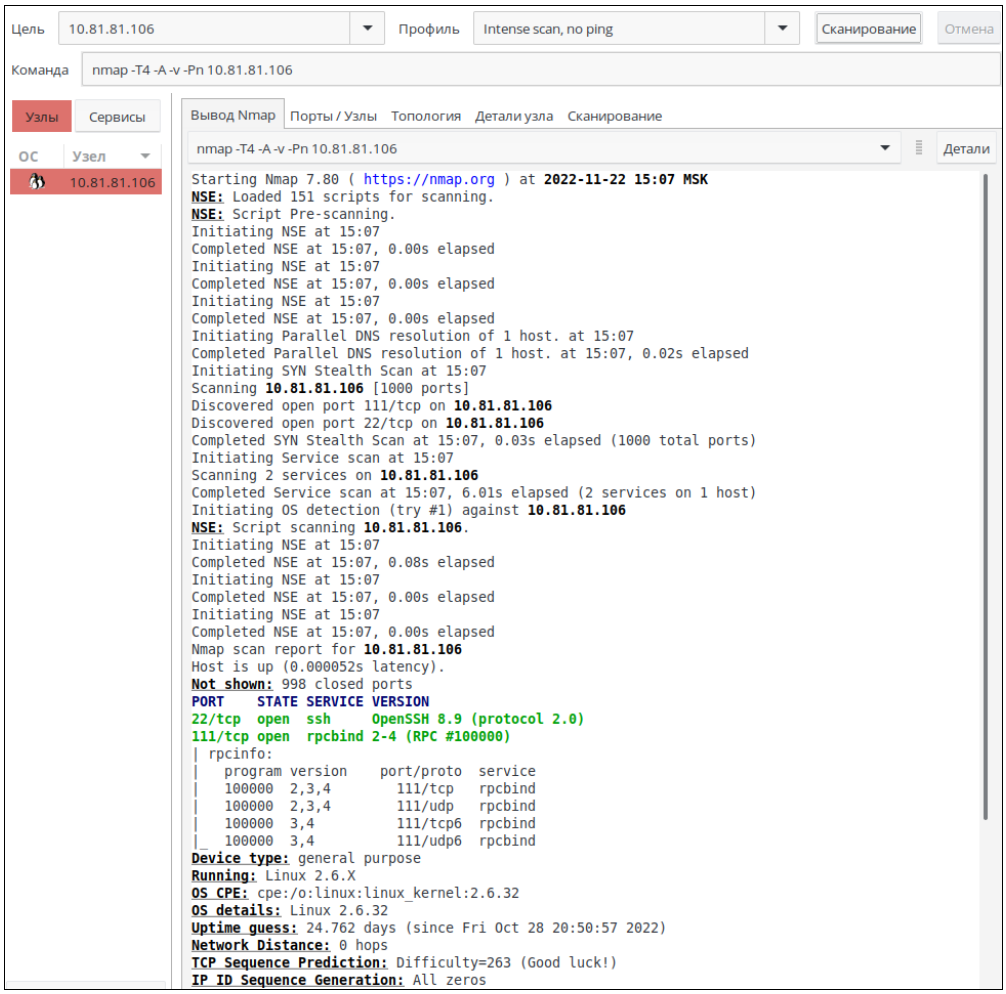
4. **Intense scan, no ping** – работает точно так же, как и другие интенсивные сканирования. Данный тип сканирования полезен, когда целевой хост блокирует запрос **ping**, но вы знаете, что он активен.

Команда:

```
nmap -T4 -A -v -Pn <цель>
```

где:

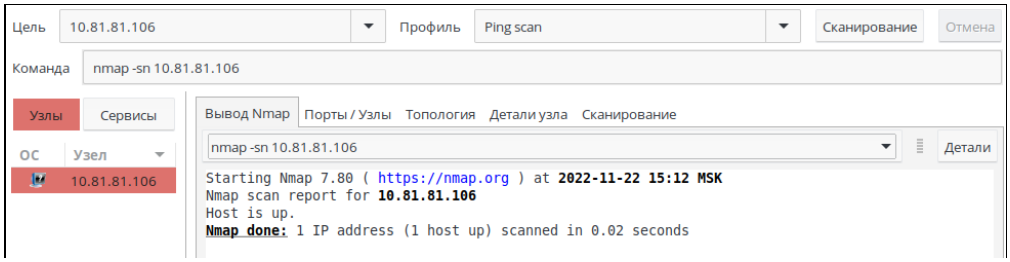
- **-Pn** - параметр предполагает, что хост работает.



5. **Ping scan** – выполняет только пинг цели, не сканируя порты.

Команда:

```
nmap -sn <цель>
```



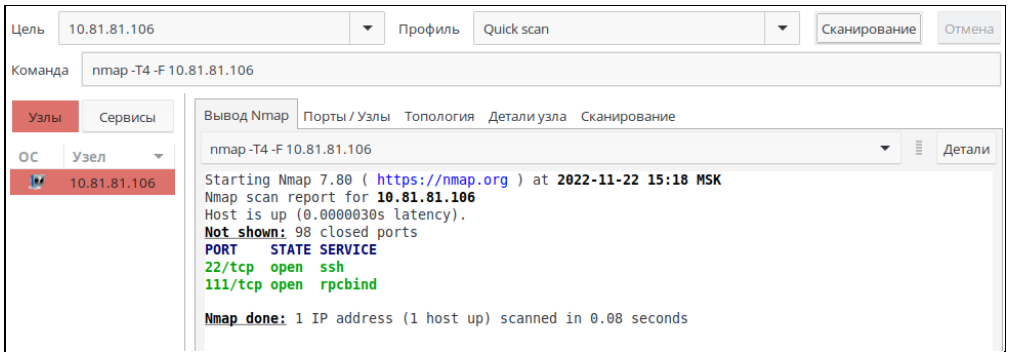
6. **Quick scan** – сканирует только ограниченное количество портов TCP, т.е. 100 самых распространенных портов **TCP**.

Команда:

```
nmap -T4 -F <цель>
```

где:

- **-F** — параметр для быстрого сканирования. Вместо того чтобы сканировать все порты, сканируется только несколько портов.



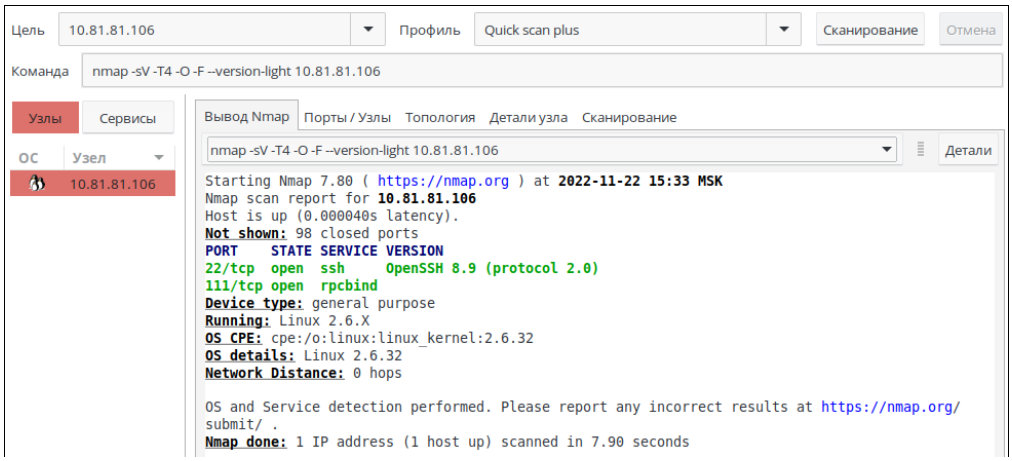
7 . **Quick scan plus** – помимо быстрого сканирования определяет также операционную систему сканируемого хоста и определяет версии служб, за которыми закреплены сканируемые порты.

Команда:

```
nmap -sV -T4 -O -F --version-light <цель>
```

где:

- **-O** — параметр, который определяет тип ОС, а затем выполняет легкое сканирование.



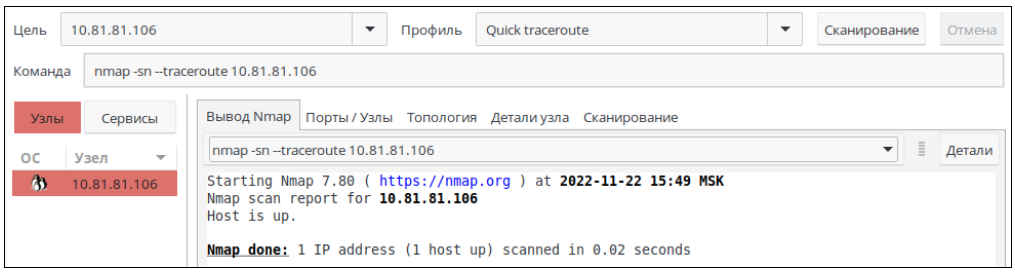
8. **Quick traceroute** – отслеживает и выполняет пинг всех хостов, определенных в цели.

Команда:

```
nmap -sn --traceroute <цель>
```

где:

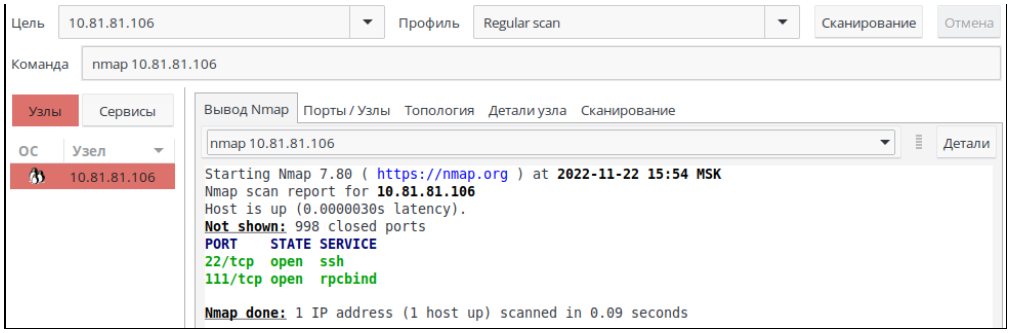
- **--traceroute** — программа, которая записывает маршрут между вашим компьютером и определенным пунктом назначения через Интернет.



9 . **Regular scan** – выполняет сканирование TCP SYN для 1000 наиболее распространенных портов, используя запрос ping для обнаружения хоста.

Команда:

```
nmap <цель>
```



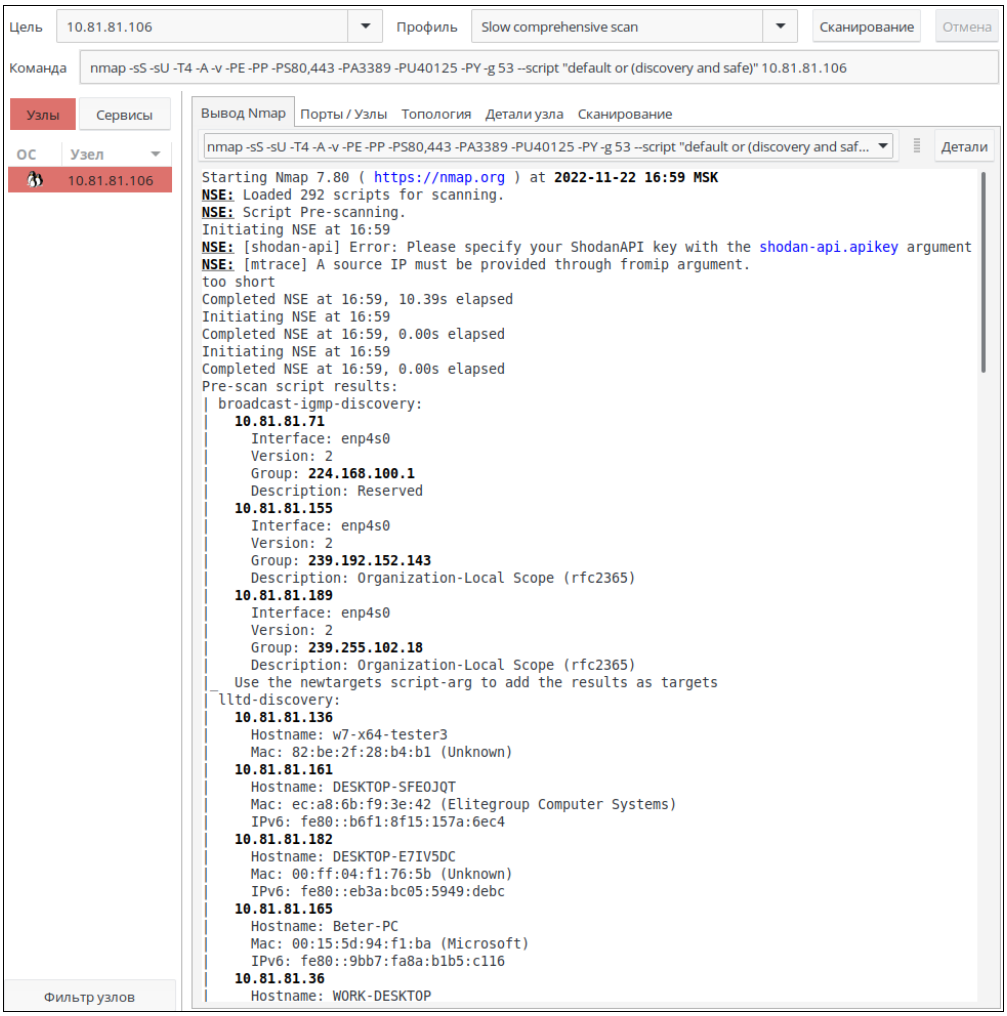
10. **Slow comprehensive scan** – профиль обладает большим количеством параметров, которые позволяют провести комплексное сканирование сети.

Команда:

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" <цель>
```

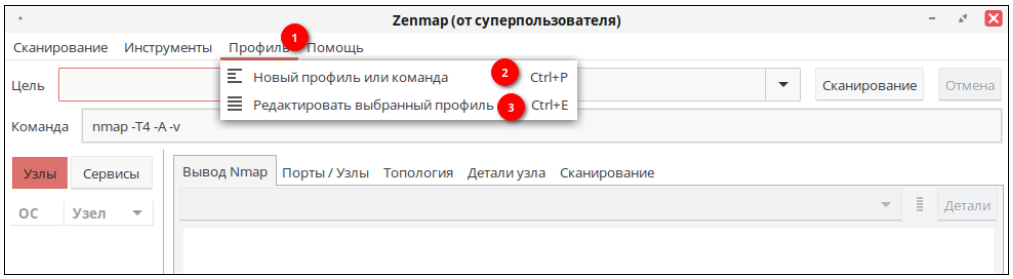
где:

- **-PE** — пинг с использованием ICMP-эхо запросов;
- **-PP** — пинг с использованием запросов временной метки;
- **-PS<№_порта>** - TCP SYN-пинг заданных хостов;
- **-PA<№_порта>** - TCP ACK-пинг заданных хостов;
- **-PU<№_порта>** - UDP-пинг заданных хостов;
- **-PY** – похоже на сканирование TCP SYN, только вместо этого используется SCTP;
- **-g** – указывается, какой исходный порт вы хотите использовать. Используется при попытке обойти систему обнаружения вторжений (IDS);
- **--script** – сканирование с использованием скриптов.

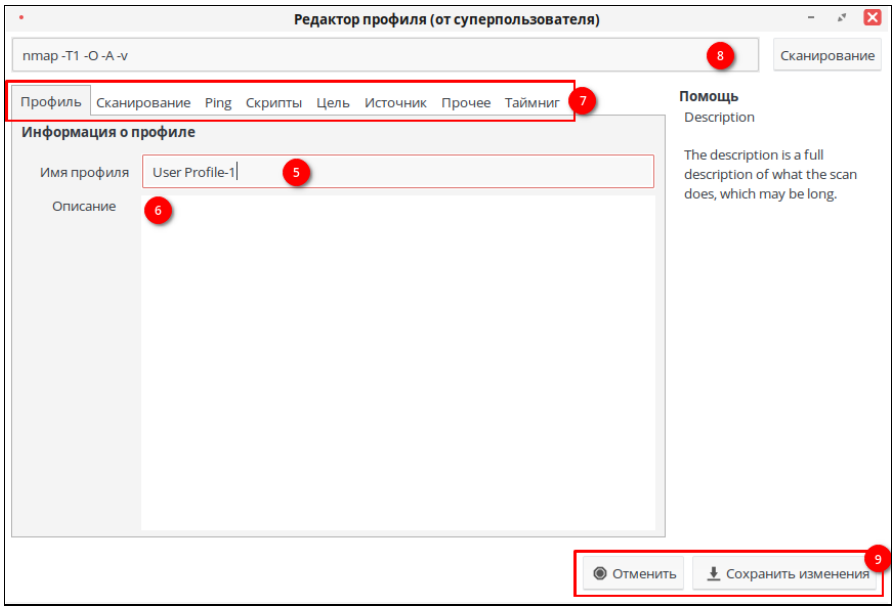


Пользовательские профили

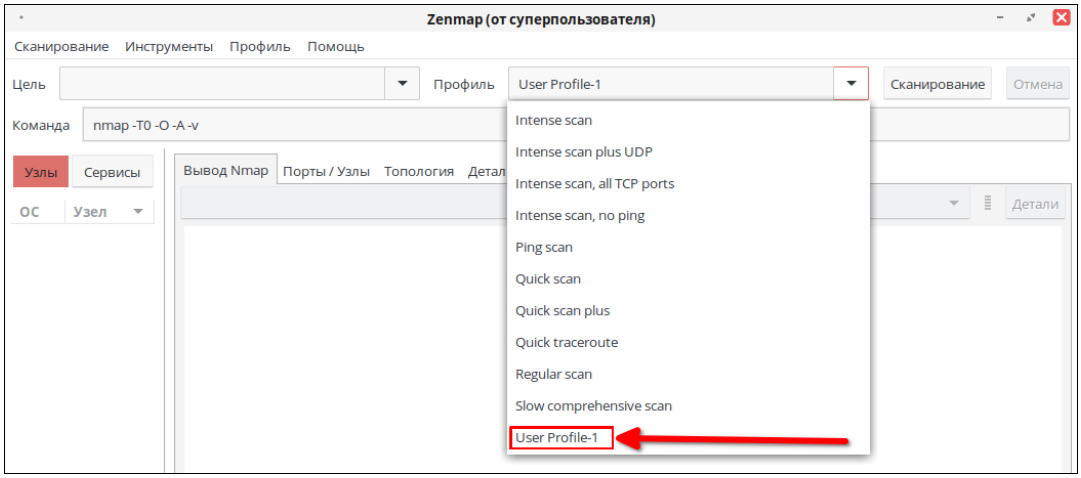
В **zenmap** есть возможность создавать и редактировать пользовательские профили. Для этого необходимо выбрать во вкладке «**Профиль**» (**1**) соответствующий пункт меню: «**Новый профиль или команда**» (**2**) или «**Редактировать выбранный профиль**» (**3**).



В окне редактора указывается *имя профиля* (**5**). Пользователь может при необходимости добавить *описание* к своему профилю (**6**). После указания всех необходимых *параметров* настройки (**7**) в отдельном поле (**8**) формируется *команда* для последующего сканирования сети. В этом же поле можно сразу указать нужную команду для выполнения сканирования без последовательной настройки. После настройки можно *сохранить* полученный профиль или *отменить* все изменения (**9**).



Во вкладке «**Профиль**» можно выбрать сохранённый профиль сканирования.



Настройка SSL для веб-серверов

Предварительная подготовка
Установка веб-серверов nginx и apache
Генерация сертификата
Настройка веб-серверов nginx и apache с сертификатами

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: nginx-1.22.1-1, httpd-2.4.56-2, mod_ssl-2.4.56-2

Предварительная подготовка

Необходимо внести DNS-запись с наименованием веб-сервера в файл **/etc/hosts** (необходимы права пользователя **root**):

```
echo <ip-адрес> <название сайта> > /etc/hosts
```

Например:

```
echo 127.0.0.1 redsite.ru > /etc/hosts
```

Установка веб-серверов nginx и apache

Примечание.

Все команды, используемые в данном разделе, выполняются **с правами пользователя root**, если не указано иное.

Nginx

Выполните установку пакетов:

```
dnf install nginx
```

Запустите службу nginx и добавьте ее в автозагрузку:

```
systemctl enable nginx --now
```

Apache

Выполните установку пакетов:

```
dnf install httpd
```

Запустите службу apache и добавьте ее в автозагрузку:

```
systemctl enable httpd --now
```

Генерация сертификата

В качестве примера будет использоваться домен - **redsite.ru**.

В данном разделе будет рассмотрен выпуск самоподписанных сертификатов для тестовых или внутренних серверов.

В качестве утилиты генерации сертификатов будет использоваться openssl, который по умолчанию предустановлен в РЕД ОС.

Примечание.

Работа с командами утилиты **openssl** осуществляется **с правами локального пользователя** и не требует прав администратора.

Примечание.

Данный раздел является общим для веб-серверов **nginx** и **apache**.

1. Создайте корневой закрытый ключ:

```
openssl genpkey -algorithm RSA -out rootCA.key -aes-128-cbc
```

где:

- genpkey – команда создания закрытого ключа;
- algorithm RSA – алгоритм асинхронного шифрования, именно он используется для выделения открытого ключа из этого закрытого;
- out rootCA.key – получаемый файл закрытого ключа;
- aes-128-cbc – алгоритм симметричного шифрования, которым зашифровывается файл закрытого ключа с помощью пароля. Пароль необходимо ввести.

Вывод команды будет иметь примерно следующий вид:

```
.......+++++
...+++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

2. Создайте открытый ключ:

```
openssl req -x509 -new -key rootCA.key -sha256 -days 365 -out rootCA.crt
```

где:

- req – команда создания сертификатов или запросов на сертификаты;
- -x509 – создание именно сертификата, а не запроса;
- -new – новый сертификат (потребуется ввести значения некоторых полей в сертификате);
- -key rootCA.key – используемый закрытый ключ, из которого следует создать открытый;
- -sha256 – алгоритм хеширования для создания подписи ключа;
- -days 365 – выпуск сертификата на 1 год;
- -out rootCA.crt – получаемый сертификат.

Пример вывода команды:

```
Enter pass phrase for rootCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Murom
Locality Name (eg, city) [Default City]:Murom
Organization Name (eg, company) [Default Company Ltd]:RS
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:redsite.ru
```

```
Email Address []:admin@redsite.ru
```

3. Создайте файл порядковых номеров для выпуска сертификатов, в нем следует указать два нуля:

```
echo 00 > rootCA.srl
```

4. В openssl нет возможности добавлять некоторые поля, например, такие как subjectAltName. Для этого создайте конфигурационный файл с необходимыми параметрами:

```
nano redsite.cnf
```

Содержимое файла следующее:

```
[ req ]
 default_bits = 2048
 distinguished_name = req_distinguished_name
 req_extensions = req_ext
 [ req_distinguished_name ]
 countryName = Country Name (2 letter code)
 countryName_default = RU
 stateOrProvinceName = State or Province Name (full name)
 stateOrProvinceName_default = Murom
 localityName = Locality Name (eg, city)
 localityName_default = Murom
 organizationName = Organization Name (eg, company)
 organizationName_default = RS
 commonName = Common Name (eg, YOUR name or FQDN)
 commonName_max = 64
 commonName_default = redsite.ru
 [ req_ext ]
 basicConstraints = CA:FALSE
 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 subjectAltName = DNS:redsite.ru
```

здесь:

- раздел `[req]`:
  - `default_bits = 2048` – длина ключа по умолчанию;
  - `distinguished_name = req_distinguished_name` – это поля в сертификате, например, **Common Name**, **organizationName** и др. Для этих полей создается блок req_distinguished_name ниже;
  - `req_extensions = req_ext` – расширение для `req`, в котором можно добавить дополнительные поля в сертификат. В данном параметре указывается наличие ниже блока `req_ext` с дополнительными полями;
- раздел `[req_distinguished_name]` - параметры для конфигурации сертификата;
- раздел `[req_ext]` - расширенные параметры для конфигурации сертификата:
  - `basicConstraints = CA:FALSE` – полученные сертификаты нельзя использовать как центр сертификации;
  - `keyUsage = nonRepudiation, digitalSignature, keyEncipherment` – созданный ключ будет иметь следующие свойства: неотрекаемость, цифровая подпись (сертификат можно использовать в качестве цифровой подписи), шифрование ключей;
  - `subjectAltName = DNS:redsite.ru` – здесь указывается поле **subjectAltName** и его значение.

5. Создайте закрытый ключ для домена:

```
openssl genpkey -algorithm RSA -out redsite.key
```

Вывод команды будет иметь примерно следующий вид:

```
.....+++++
.....+++++
```

6. Создайте с закрытым ключом файл запроса на сертификат. После выполнения команды на всех полях необходимо нажать Enter, т.к. данные используются из конфигурационного файла redsite.cnf, который был создан ранее:

```
openssl req -new -key redsite.key -config redsite.cnf -reqexts req_ext -out redsite.csr
```

Пример вывода команды:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:RU
State or Province Name (full name) [Murom]: Murom
Locality Name (eg, city) [Murom]: Murom
Organization Name (eg, company) [RS]: RS
Common Name (eg, YOUR name or FQDN) [redsite.ru]: redsite.ru
```

7. Сгенерируйте сертификат для домена:

```
openssl x509 -req -days 365 -CA rootCA.crt -CAkey rootCA.key -extfile redsite.cnf -extensions req_ext -in redsite.csr -out redsite.crt
```

где:

- x509 – создание сертификата методом подписания;
- -req – если производится подпись файла запроса, необходимо использовать эту опцию;
- -days 365 – срок сертификата 1 год;
- -CA rootCA.crt -CAkey rootCA.key – корневая пара ключей;
- -extfile redsite.cnf – файл, содержащий расширения сертификатов;
- -in redsite.csr -out redsite.crt – файл запроса и файл сертификата.

Пример вывода команды:

```
Signature ok
subject=C = RU, ST = Murom, L = Murom, O = RS, CN = redsite.ru, Getting CA Private Key
Enter pass phrase for rootCA.key:
```

8. Проверьте наличие сертификатов:

```
 ls -l

итого 60
-rw-rw-r--. 1 user user  801 июн 13 22:23  redsite.cnf
-rw-rw-r--. 1 user user 1245 июн 13 22:26  redsite.crt
-rw-rw-r--. 1 user user 1058 июн 13 22:25  redsite.csr
-rw-------. 1 user user 1704 июн 13 22:23  redsite.key
-rw-rw-r--. 1 user user 1363 июн 13 22:20  rootCA.crt
-rw-------. 1 user user 1874 июн 13 22:18  rootCA.key
-rw-rw-r--. 1 user user    3 июн 13 22:26  rootCA.srl
```

9. Затем необходимо поместить сертификаты в директории **/etc/ssl/certs** и **/etc/ssl/private** следующим образом:

```
sudo mkdir /etc/ssl/private
sudo cp  rootCA.crt redsite.crt  /etc/ssl/certs
sudo cp redsite.key /etc/ssl/private
```

10. Добавьте сертификат в системное хранилище. Для этого скопируйте сертификаты в каталог **/etc/pki/ca-trust/source/anchors/**:

```
sudo cp  rootCA.crt redsite.crt /etc/pki/ca-trust/source/anchors/
```

Затем выполните команды обновления (с правами пользователя root):

```
update-ca-trust
update-ca-trust extract
```

Настройка веб-серверов nginx и apache с сертификатами

> **Примечание.**
>
> Все команды, используемые в данном разделе, выполняются **с правами пользователя root**, если не указано иное.

Nginx

1. Приведите раздел **Settings for a TLS enabled server** файла **/etc/nginx/nginx.conf** к следующему виду:

```
nano /etc/nginx/nginx.conf
```

```
# Settings for a TLS enabled server.
#
server {    # раскомментируйте строку
listen 443 ssl default_server;    # раскомментируйте строку и замените http2 на default_server
listen [::]:443 ssl default_server;    # раскомментируйте строку и замените http2 на default_server
server_name redsite;    #укажите имя сервера без доменной области
# root /usr/share/nginx/html;
#
ssl_certificate "/etc/ssl/certs/redsite.crt";
ssl_certificate_key "/etc/ssl/private/redsite.key";
# ssl_session_cache shared:SSL:1m;
# ssl_session_timeout 10m;
# ssl_ciphers HIGH:!aNULL:!MD5;
# ssl_prefer_server_ciphers on;
#
# # Load configuration files for the default server block.
# include /etc/nginx/default.d/*.conf;
#
# error_page 404 /404.html;
# location = /404.html {
# }
#
# error_page 500 502 503 504 /50x.html;
# location = /50x.html {
# }
}    # раскомментируйте строку


}
```

В конце файла необходимо добавить фигурную скобку «**}**», чтобы избежать ошибок синтаксиса от **nginx**.

2. Выполните проверку настроек **nginx**:

```
nginx -t
```

Вывод команды должен иметь примерно следующий вид:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Выполните перезапуск службы **nginx**:

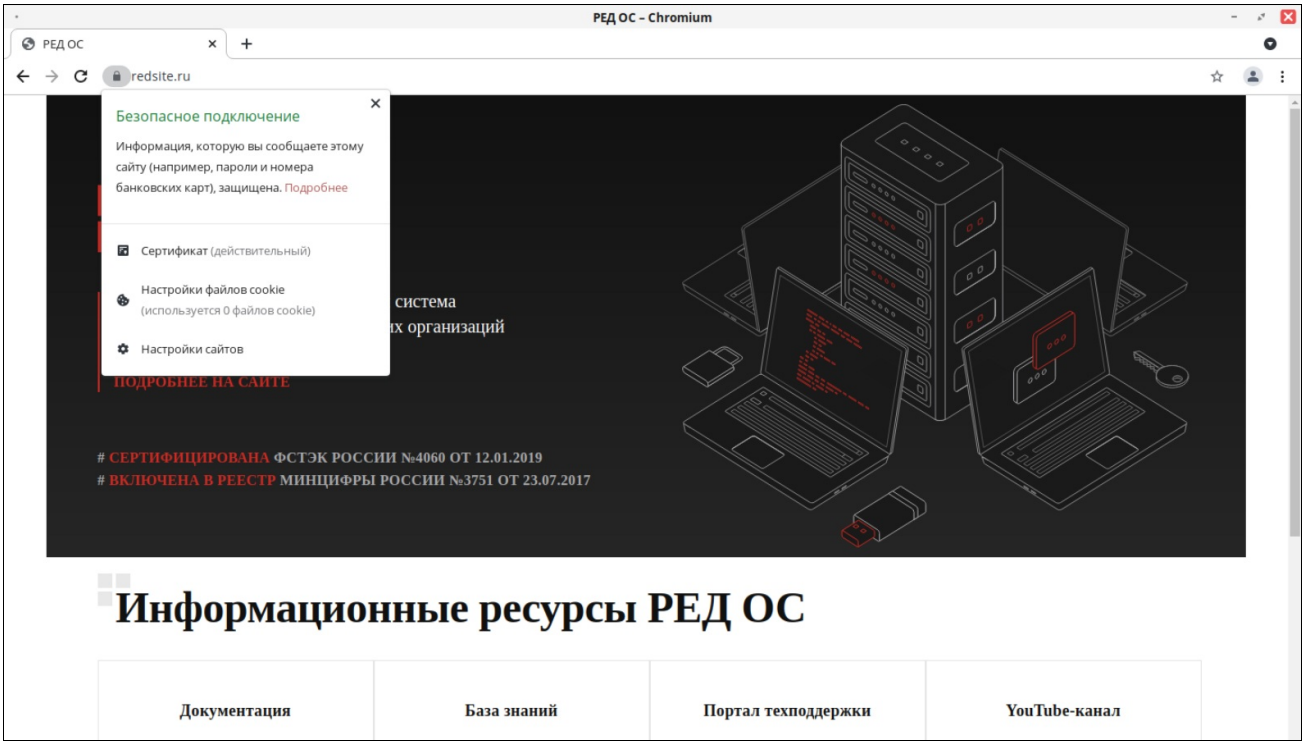
```
systemctl restart nginx
```

Примените правило *SELinux* для разрешения подключений:

```
setsebool -P httpd_read_user_content 1
```

Для проверки перейдите в браузере по ссылке `https://<ваш_сайт>`.

Например:



Apache

1. Для работы **SSL** необходимо установить следующий пакет:

```
dnf install mod_ssl
```

2. Приведите файл **/etc/httpd/conf/httpd.conf** к виду:

```
ServerName redsite.ru    # раскомментировать строку и указать имя сервера
LoadModule ssl_module modules/mod_ssl.so    # добавить строку в конец файла
```

3. В **/etc/httpd/conf.d/ssl.conf** укажите путь до сертификатов:

```
SSLCertificateFile /etc/ssl/certs/redsite.crt    # укажите путь до сертификата (открытая часть)
SSLCertificateKeyFile /etc/ssl/private/redsite.key    # укажите путь до сертификата (закрытая часть)
```

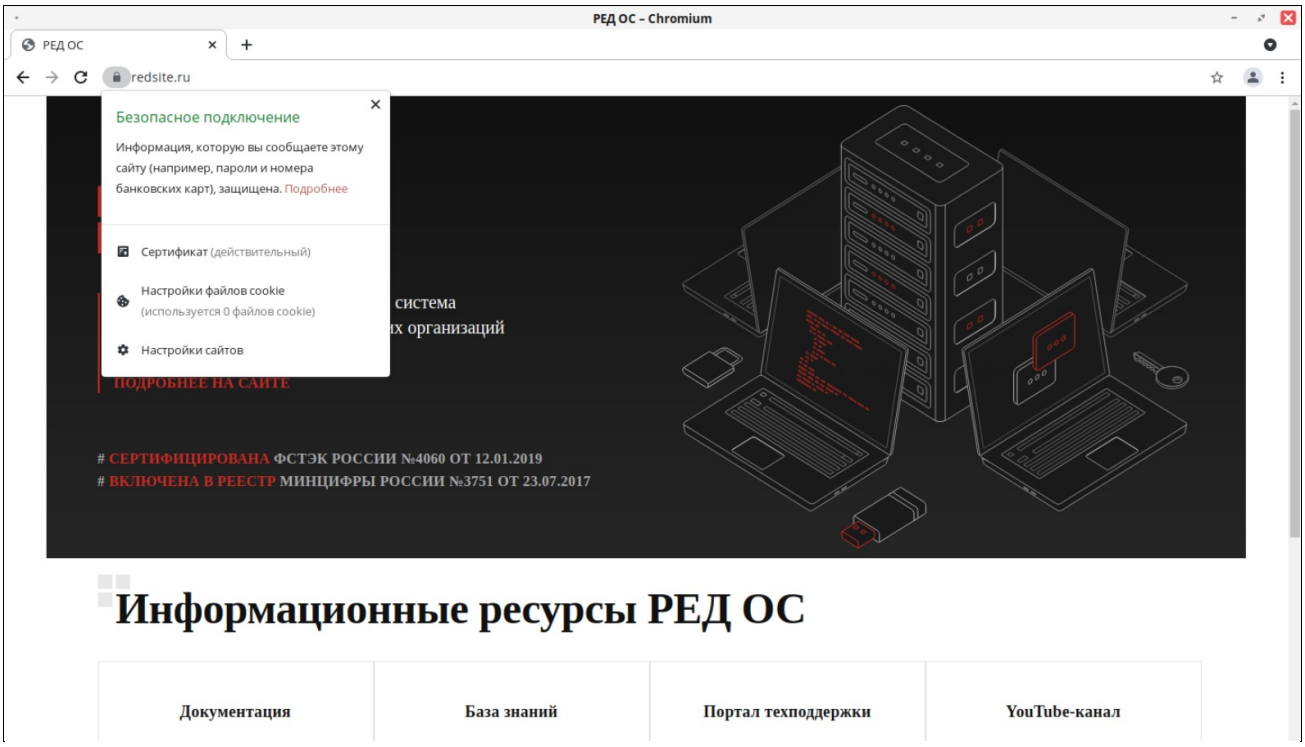
4. Проверьте настройки **httpd**:

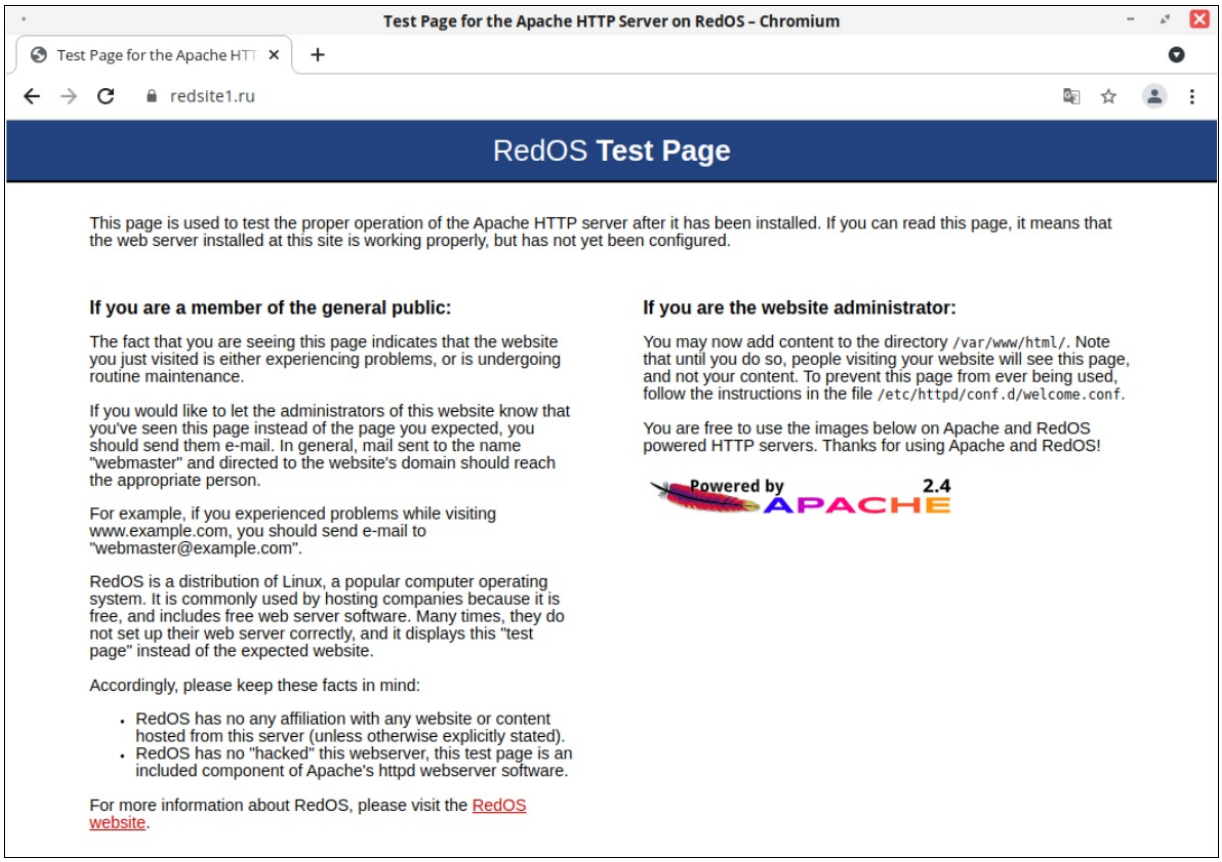
```
apachectl configtest
```

Вывод команды должен иметь примерно следующий вид:

```
Syntax OK
```

5. Для проверки перейдите в браузере по ссылке `https://<ваш_сайт>`. Например:


РЕД ОС – Chromium
РЕД ОС
redsite.ru
Безопасное подключение
Информация, которую вы сообщаете этому сайту (например, пароли и номера банковских карт), защищена. Подробнее
Сертификат (действительный)
Настройки файлов cookie
(используется 0 файлов cookie)
Настройки сайтов
ПОДРОБНЕЕ НА САЙТЕ
СЕРТИФИЦИРОВАНА ФСТЭК РОССИИ №4060 ОТ 12.01.2019
ВКЛЮЧЕНА В РЕЕСТР МИНЦИФРЫ РОССИИ №3751 ОТ 23.07.2017
Информационные ресурсы РЕД ОС
Документация
База знаний
Портал техподдержки
YouTube-канал


Test Page for the Apache HTTP Server on RedOS – Chromium
Test Page for the Apache HTT
redsite1.ru
RedOS Test Page
This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.
If you are a member of the general public:
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.
If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.
For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".
RedOS is a distribution of Linux, a popular computer operating system. It is commonly used by hosting companies because it is free, and includes free web server software. Many times, they do not set up their web server correctly, and it displays this "test page" instead of the expected website.
Accordingly, please keep these facts in mind:
RedOS has no any affiliation with any website or content hosted from this server (unless otherwise explicitly stated).
RedOS has no "hacked" this webserver, this test page is an included component of Apache's httpd webserver software.
For more information about RedOS, please visit the RedOS website.
If you are the website administrator:
You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf.d/welcome.conf.
You are free to use the images below on Apache and RedOS powered HTTP servers. Thanks for using Apache and RedOS!
Powered by APACHE 2.4

Поддержка российских сертификатов безопасности

Сертификаты ТЦИ
Настройка цепочки доверия TLS-сертификатов ГОСТ

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: ca-certificates-ru-2022-5

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. **SSL** (**Secure Sockets Layer**) – это протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.

Компаниям необходимо добавлять SSL-сертификаты на веб-сайты для обеспечения конфиденциальности и безопасности клиентских данных.

В РЕД ОС обеспечена поддержка российских сертификатов безопасности, предоставленных удостоверяющим центром сертификации Минцифры России. Пакет ca-certificates-ru, содержащий комплект корневых сертификатов ЦС России, по умолчанию предустановлен в РЕД ОС. Привязка сертификатов в браузерах **Chromium**, **Firefox**, **Яндекс.Браузер** происходит **автоматически**.

Вы можете подробнее ознакомиться с установкой и настройкой сертификатов безопасности, просмотрев наши обучающие видео:

- на **RuTube** — Поддержка российских SSL-сертификатов в РЕД ОС;
- в **Яндекс.Дзен** — Поддержка российских SSL-сертификатов в РЕД ОС;
- в **VK Видео** — Поддержка российских SSL-сертификатов в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сертификаты ТЦИ

В состав пакета ca-certificates-ru также входят корневые сертификаты *Центра сертификации ТЦИ*.

Центр сертификации ТЦИ — это организация, которая выпускает TLS-сертификаты для веб-ресурсов (сайтов, платформ и т.п.).

TLS-сертификаты являются важным инструментом, обеспечивающим безопасность пользователей сети Интернет. Они представляют собой аналог цифровой подписи для веб-ресурса, т.е. подтверждают его подлинность и позволяют организовать доверенный, защищённый канал обмена данными, обеспечивая их сохранность и невозможность перехвата.

Центр сертификации ТЦИ выпускает сертификаты с методами шифрования **ECDSA** и **ГОСТ**. Оба метода очень похожи между собой и имеют более высокую скорость шифрования по сравнению с *RSA*, но технически имеют различия в математической модели криптографических параметров. **ECDSA**-сертификаты можно использовать при типовых настройках без изменений на сервере и клиенте, а **ГОСТ**-сертификаты популяризируют отечественную криптографию.

Настройка цепочки доверия TLS-сертификатов ГОСТ

Для настройки использования в РЕД ОС **TLS**-сертификатов с методом шифрования по **ГОСТ** выполните следующие действия:

1. Обновите пакет ca-certificates-ru:

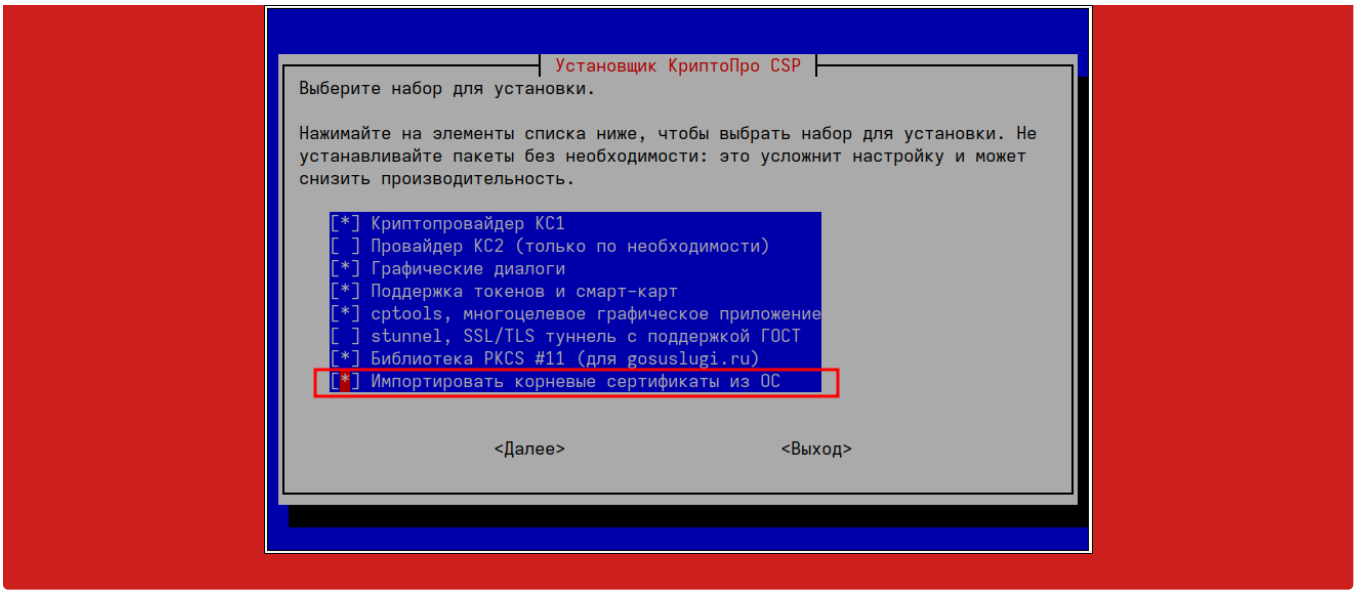
```
dnf update ca-certificates-ru
```

2. Установите криптопровайдер **КриптоПро CSP 5.0** согласно нашей инструкции «Установка КриптоПро CSP 5.0».

ВАЖНО!

Обратите внимание, что на втором шаге при определении набора установки необходимо выбрать пункт «**Импортировать корневые сертификаты ОС**», т.к. *КриптоПро CSP* по умолчанию **НЕ использует** хранилище корневых сертификатов из ОС.

Без установки указанного параметра «**Импортировать корневые сертификаты ОС**» ГОСТ-сертификат ТЦИ работать **не будет**!



Для доступа к сайтам с ГОСТ-сертификатом можно пользоваться штатным браузером **Chromium** или **Яндекс**.

Проверка работоспособности

Для проверки корректной работы сертификатов Минцифры в ОС можно перейти по ссылке https://fias.egisz.rosminzdrav.ru/. Если сайт открыт без предупреждений о небезопасном соединении, значит все настроено верно.

Проверку корректной настройки TLS-сертификата с методом шифрования ГОСТ можно осуществить на тестовой странице ТЦИ https://gost.tlscc.ru/.

Настройка ГОСТ в OpenSSL в РЕД ОС 7.3

Установка поддержки алгоритмов ГОСТ
Стандартный способ переключения на ГОСТ
Переключение на ГОСТ посредством изменения файлов конфигурации
Переключение на ГОСТ при использовании общесистемных криптографических политик
Проверка поддержки ГОСТ в OpenSSL
Пример генерации ключей

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** openssl-gost-engine-1.1.1.0-0.10

В состав дистрибутива РЕД ОС входит пакет библиотек, поддерживающих методы защитного преобразования по алгоритмам ГОСТ, - **openssl-gost-engine**.

Пакет **openssl-gost-engine** включает в себя реализацию следующих алгоритмов ГОСТ:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 — алгоритмы электронной цифровой подписи.
- ГОСТ Р 34.11-94 — Алгоритм хэширования. 256-битное значение хэша.
- ГОСТ Р 34.11-2012 — Алгоритм хэширования. 256- и 512-битные значения хеша.
- ГОСТ 28147-89 — Симметричное шифрование с 256-битным ключом. Доступны режимы *CBC*, *CFB* и *CNT*. Для усложнения статистического анализа поддерживается «*key meshing*» (подробнее см. RFC 4357).
- ГОСТ 28147-89 в режиме выработки имитовставки (*MAC*). Основан на алгоритме хэширования с использованием алгоритмов симметричного шифрования. Он имеет 256-битный симметричный ключ и разрядность от 8 до 64 (по умолчанию 32) бит.
- ГОСТ Р 34.13–2015 — Симметричное шифрование «Кузнечик» («*Grasshopper*»).

Установка поддержки алгоритмов ГОСТ

Пакет **openssl-gost-engine** по умолчанию предустановлен в РЕД ОС. Однако если по каким-либо причинам в вашей системе пакет отсутствует, для его установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install openssl-gost-engine
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Стандартный способ переключения на ГОСТ

После установки **openssl** поддержку алгоритмов ГОСТ можно включить следующей командой:

```
openssl-switch-config <gost | default>
```

При указании аргумента **gost** поддержка алгоритмов ГОСТ включается, при указании аргумента **default** — возвращаются настройки по умолчанию.

Переключение на ГОСТ посредством изменения файлов конфигурации

Вторым способом включения в **openssl** поддержки алгоритмов ГОСТ является редактирование соответствующих файлов конфигурации.

Сначала отредактируйте файл настроек **/etc/pki/tls/openssl.cnf**:

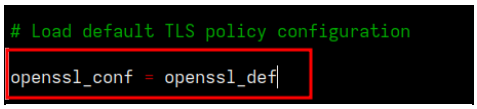
```
nano /etc/pki/tls/openssl.cnf
```

1. В начале файла строку вида:

```
openssl_conf = default_modules
```

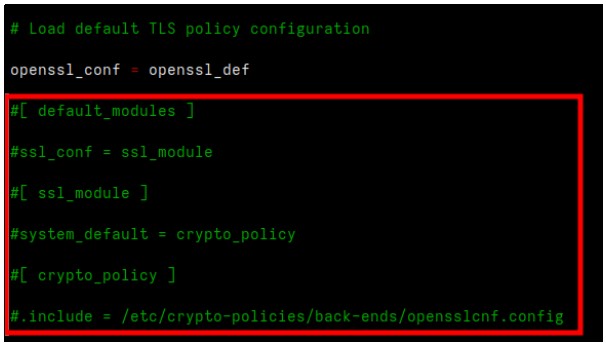
замените на строку:

```
openssl_conf = openssl_def
```



2. Закомментируйте настройки по умолчанию:

```
#[ default_modules ]
 #ssl_conf = ssl_module

 #[ ssl_module ]
 #system_default = crypto_policy

 #[ crypto_policy ]
 #.include = /etc/crypto-policies/back-ends/opensslcnf.config
```



3. В конец файла добавьте следующие строки:

```
[openssl_def]
engines = engine_section

[engine_section]
gost = gost_section

[gost_section]
engine_id = gost
dynamic_path = /usr/lib64/engines-1.1/gost.so
default_algorithms = ALL
CRYPT_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

4. После этого необходимо явно указать **Cipher Strings** в файле конфигурации **/etc/crypto-policies/back-ends/openssl.config**:

```
nano /etc/crypto-policies/back-ends/openssl.config
```

```
@SECLEVEL=1:aGOST:aGOST01:kGOST:GOST94:GOST89MAC:kEECDH:kRSA:kEDH:kPSK:kDHEPSK:kECDHEPSK:-aDSS:-
3DES:!DES:!RC4:!RC2:!IDEA:-SEED:!eNULL:!aNULL:!MD5:-SHA384:-CAMELLIA:-ARIA:-AESCCM8
```

Переключение на ГОСТ при использовании общесистемных криптографических политик

Общесистемные политики шифрования — это системный компонент, который настраивает основные криптографические подсистемы, включая протоколы TLS, IPsec, SSH, DNSSec и Kerberos. Он предоставляет небольшой набор политик, которые может выбрать администратор.

При использовании в системе общесистемных политик программы следуют настроенным правилам и не используют в своей работе алгоритмы и протоколы, которые не соответствуют настроенной политике (за исключением случаев, когда администратор явно указывает программе выполнить данное действие). Это значит, что политика применяется к поведению программ по умолчанию при работе с предоставленной системой конфигурацией, но при необходимости ее можно переопределить.

В системе поддерживаются следующие предопределенные политики:

- **DEFAULT** – уровень общесистемной криптографической политики по умолчанию предлагает безопасные настройки для текущих моделей угроз. Он поддерживает протоколы TLS 1.2 и 1.3, а также протоколы IKEv2 и SSH2. Ключи RSA и параметры Диффи-Хеллмана принимаются, если их длина не менее 2048 бит.
- **LEGACY** – совместим с более ранними системами и менее безопасен из-за увеличенной поверхности атаки. Помимо алгоритмов и протоколов уровня DEFAULT, он включает поддержку протоколов TLS 1.0 и 1.1. Алгоритмы DSA, 3DES и RC4 разрешены, а ключи RSA и параметры Диффи-Хеллмана принимаются, если их длина не менее 1023 бит.
- **FUTURE** – более строгий уровень безопасности, предназначенный для тестирования возможной будущей политики. Политика не позволяет использовать SHA-1 в алгоритмах подписи. Он поддерживает протоколы TLS 1.2 и 1.3, а также протоколы IKEv2 и SSH2. Ключи RSA и параметры Диффи-Хеллмана принимаются, если их длина не менее 3072 бит. Если система имеет доступ в Интернет, есть вероятность столкнуться с проблемами совместимости.

Подробную информацию о криптографических политиках системы см. в нашей статье «Общесистемные криптографические политики».

Для проверки используемой в системе политики шифрования выполните:

```
update-crypto-policies --show
```

Для применения какой-либо политики в системе (например, LEGACY) выполните:

```
update-crypto-policies --set LEGACY
```

Для включения поддержки алгоритмов ГОСТ в **openssl** необходимо после применения в системе новой политики шифрования выполнить команду:

```
openssl-switch-config gost
```

Для возврата к настройкам по умолчанию утилите **openssl-switch-config** необходимо передать параметр **default**.

Проверка поддержки ГОСТ в OpenSSL

После проведения настройки проверьте, видит ли **OpenSSL** алгоритмы ГОСТ, командой:

```
openssl ciphers | tr ":" "\n" | grep GOST

GOST2012-GOST8912-GOST8912
GOST2001-GOST89-GOST89
```

Пример генерации ключей

Генерация закрытого ключа и создание сертификата с подписью ГОСТ производится следующей командой:

```
openssl req -x509 -newkey gost2012_256 -pkeyopt paramset:A -nodes -keyout key.pem -out cert.pem -md_gost12_256
```

Для проверки сертификата выполните команду:

```
openssl x509 -in cert.pem -text -noout

Certificate:
   Dat a:
      Version: 3 (0x2)
      Serial Number:
         17:86:3c:c0:8c:62:36:af:88:3c:19:01:34:bb:19:92:61:38:5a:37
      Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
      Issuer: C = ru, ST = Russia, L = Moscow, O = red-soft, OU = drsp, CN = root, emailAddress = root
```

```
        Validity
            Not Before: Mar 15 11:24:48 2022 GMT
            Not After : Apr 14 11:24:48 2022 GMT
        Subject: C = ru, ST = Russia, L = Moscow, O = red-soft, OU = drsp, CN = root, emailAddress = root
        Subject Public Key Info:
            Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus
                Public key:
                    X:27F4547D48EFAAE904FDCDCD190EB702858B77A796600E175FDEDA8BA35E3C1A
                    Y:35D4E769099EDBC4461A8E67510897D98FD59C4F4D34F08F722899EAD7ABEF81
                Parameter set: id-GostR3410-2001-CryptoPro-A-ParamSet
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                4B:E5:69:DE:B5:00:AE:01:71:56:97:C8:C5:30:8C:B1:5F:5E:AF:AF
            X509v3 Authority Key Identifier:
                keyid:4B:E5:69:DE:B5:00:AE:01:71:56:97:C8:C5:30:8C:B1:5F:5E:AF:AF

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
        3e:94:02:7d:82:7a:52:5c:4d:09:8b:ae:c9:51:c1:19:2a:0f:
        c9:ce:39:39:89:27:89:87:e2:e7:bf:f7:9a:b3:be:bd:56:ea:
        27:bf:56:d8:99:a9:96:09:62:a5:49:04:69:d1:ea:b3:0f:fa:
        92:04:6a:da:27:79:49:ac:79:bd
```

Fail2Ban - сервис блокировки хостов

Установка и запуск
Основные настройки и примеры использования
Параметры конфигурационного файла
Настройка защиты SSH
Блокировка нежелательного трафика
Настройка блокировки для Asterisk
Работа со списком заблокированных адресов
Пример работы fail2ban

Fail2Ban – это сервис для блокировки хостов, вызывающих множественные ошибки при попытках аутентификации.

Fail2Ban работает путем мониторинга файлов журналов (например, **/var/log/auth.log**, **/var/log/apache/access.log** и др.) для выбранных записей и запуска сценариев на их основе. Чаще всего это используется для блокировки выбранных IP-адресов, которые могут принадлежать хостам, пытающимся нарушить безопасность системы. Он может запретить любой IP-адрес хоста, который делает слишком много попыток входа в систему или выполняет любые другие нежелательные действия в течение периода времени, определенного администратором. Включает поддержку как **IPv4**, так и **IPv6**. Опционально более длительные запреты могут быть настроены специально для нарушителей, которые продолжают возвращаться.

Fail2Ban обычно настраивается на разблокировку заблокированного хоста в течение определенного периода времени, чтобы не "блокировать" любые подлинные соединения, которые могли быть временно неправильно сконфигурированы. Время блокировки нежелательных хостов в несколько минут, обычно является достаточным, чтобы снизить вероятность сетевой атаки или атаки подбора пароля по словарю, например, при подключении по **ssh**.

Стандартная конфигурация *Fail2Ban* поставляется с фильтрами для *Apache, Lighttpd, sshd, vsftpd, qmail*. Фильтры определяются регулярными выражениями Python, которые могут быть удобно настроены администратором, знакомым с регулярными выражениями. С помощью фильтров можно блокировать попытки доступа от вредоносного хоста к определенным сетевым службам.

Fail2Ban можно настроить для мониторинга любой службы, которая записывает попытки аутентификации в файл журнала. Для блокировки IP-адресов нежелательных хостов *Fail2Ban* использует правила *iptables*.

Установка и запуск Fail2Ban

Установка производится командой:

```
dnf install fail2ban
systemctl start fail2ban
systemctl enable fail2ban
```

Основные настройки и примеры использования приложения Fail2Ban

Все конфигурационные файлы программы находятся в каталоге **/etc/fail2ban**. Для установки собственных настроек необходимо создать файл с таким же именем и расширением **.local**.

Основные параметры конфигурационного файла jail.conf

Конфигурационный файл **jail.conf** используется для создания ограничивающих правил для различных программ и имеет параметры, которые описаны ниже:

- *action* — действие, которое будет выполняться, если *Fail2ban* обнаружит активность, соответствующую критериям поиска;
- *ignoreip* — задает список IP-адресов, которые нужно исключить из алгоритмов Fail2ban. К ним не будут применяться ограничения, так что выбирайте их аккуратно. Диапазоны и IP-адреса стоит разделить пробелом. Сюда можно добавить локальный IP, а также IP-адрес, с которого вы будете подключаться сами, чтобы у вас не возникло проблем при входе;
- *bantime* — время в секундах, на которое клиенту будет закрыт доступ к серверу, если он не сможет авторизоваться;
- *maxretry* — указывает количество попыток перед тем, как доступ будет заблокирован;
- *findtime* — время в секундах, на протяжении которого рассчитывается *maxretry*.

Настройка защиты SSH

Сначала копируем содержимое **jail.conf** в **jail.local**:

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

По умолчанию **jail.local** работает только для *SSH*. Примерная настройка файла **jail.local** для *SSH*:

```
[sshd]
enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
logpath  = /var/log/auth.log
findtime    = 600
maxretry    = 3
bantime     = 21600
```

Блокировка нежелательного трафика к определенному URL для NGINX

Откроем файл конфигурации:

```
nano /etc/fail2ban/jail.local
```

И добавим в конец:

```
[nginx-req-limit]
enabled = true
filter = nginx-req-limit
action = iptables-multiport[name=ReqLimit, port="http,https", protocol=tcp]
logpath = /var/log/nginx/*error.log
findtime = 600
bantime = 7200
maxretry = 10
```

Настройка блокировки для Asterisk

Добавляем в конец файла **jail.local**:

```
[asterisk]
 enabled = true
 action = iptables-allports[name=asterisk, protocol=all]
 logpath = /var/log/asterisk/messages
 bantime = 86400
```

Работа со списком заблокированных адресов

- Получить статистику заблокированных адресов можно следующей командой:

```
fail2ban-client status <имя_правила>
```

- Для удаления адреса из списка вводим:

```
fail2ban-client set <имя правила> unbanip
```

- Получить список правил можно командой:

```
fail2ban-client status
```

- После необходимо перечитать правила:

```
firewall-cmd --reload
```

- После каких либо изменений в конфигурационных файлах перезапустите *faile2ban* командой:

```
systemctl restart fail2ban
```

Пример работы fail2ban

Пример блокировки подключения к ssh-серверу после нескольких неудачных попыток авторизоваться. Для примера было взято правило для *ssh*. В примере пользователь попытался 3 раза ввести пароль для доступа к ssh-серверу, и после неудачных попыток последующие соединения с IP-адреса клиента были заблокированы.

Попытка пользователя авторизоваться на ssh-сервере:

После неудачных попыток ввода пароля, дальнейшие соединения к ssh-серверу были отказаны.

XCA - программа для управления асимметричными ключами

Установка XCA
Обзор простейших функций XCA
Начало работы с XCA
Примеры работы с XCA
Создание корневого сертификата

X Certificate and Key management (**XCA**) - это программа, предоставляющая интерфейс для управления асимметричными ключами *RSA, DSA and EC private keys, Smartcards and CRLs*. Программа может использоваться для создания и подписания сертификатов в рамках небольшого **ЦС** (**CA**) и создать собственную инфраструктуру открытых ключей (**PKI**).

Возможности:

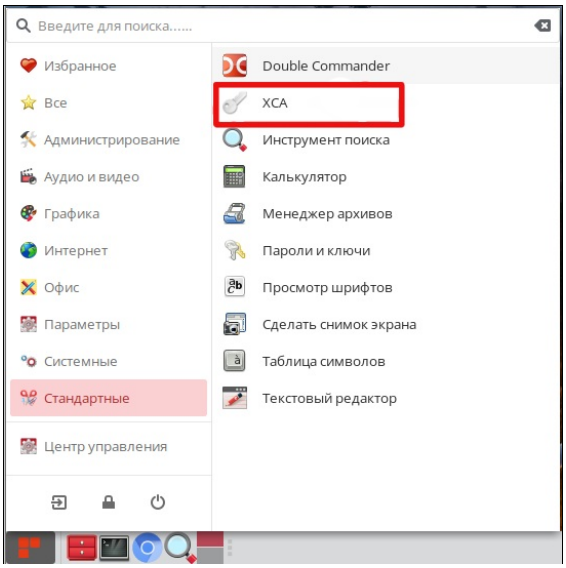
1. Создание собственного **PKI**, закрытых ключей, сертификатов, запросов или CRL. 2. Экспорт и импорт ключей в форматах: **PEM, DER, PKCS#7, PKCS#12**. 3. Управления смарт-картами через интерфейс **PKCS#11**. 4. Функция экспорта сертификатов и запросов в виде конфигурационного файла **OpenSSL**. 5. Создание шаблонов для сертификатов, а также создание шаблонов на основе готовых сертификатов. 6. Преобразование существующих сертификатов или запросов в шаблоны. 7. Получение широкой поддержки расширений **x509v3** таких же гибких, как OpenSSL, но более удобных для пользователя. 8. Запись сертификатов на токен.

Установка XCA

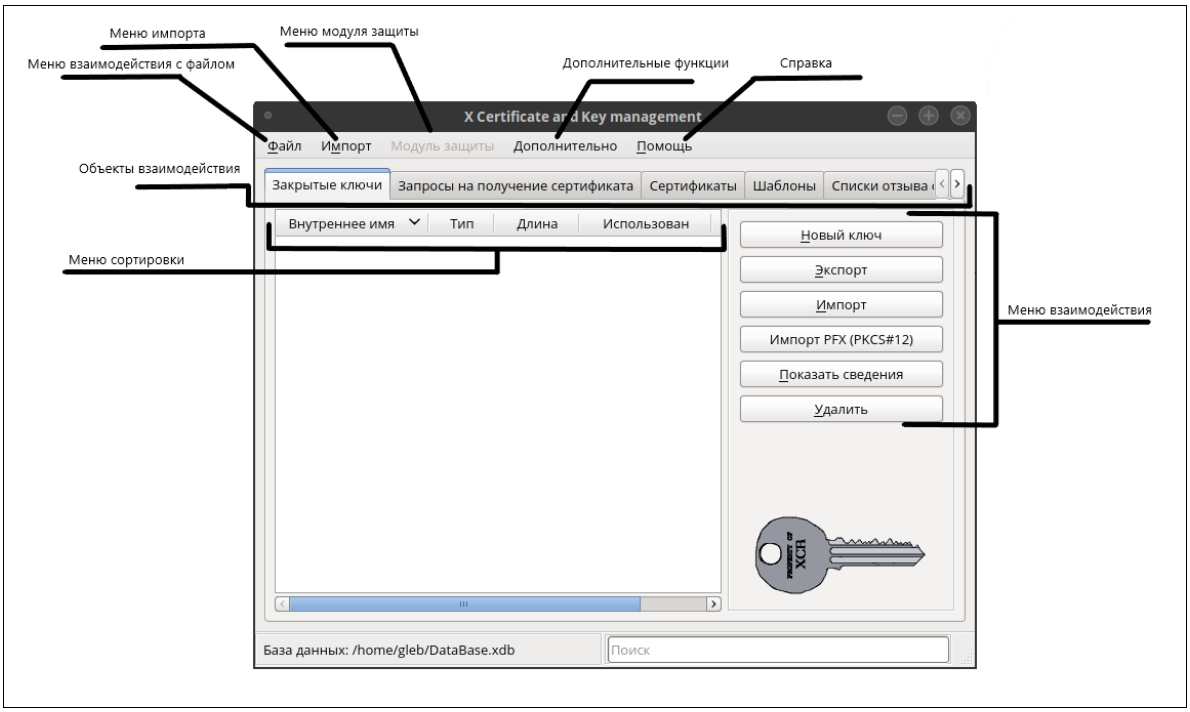
Для установки XCA выполните команду:

```
dnf install xca
```

После установки программу можно будет найти в **"Меню" – "Стандартные"**.



Обзор простейших функций XCA



Меню «*Файл*» позволяет создать или открыть уже существующую базу данных, а так же настроить язык всей XCA и настроить саму XCA. Меню «*Импорт*» позволяет импортировать уже имеющиеся ключи, запросы, сертификаты и др. в базу данных. Меню «*Модуль защиты*» позволяет настроить защиту базы данных. Меню «*Дополнительно*» имеет дополнительные функции для взаимодействия с базой данных, такие как экспорт списка сертификатов или генерация параметров Диффи – Хэллмана.

Начало работы с XCA

Для начала работы с приложением создайте базу данных. Для этого необходимо выбрать в меню **«Файл» - «Новая база данных»**.

Работа с токенами/смарт-картами:

1. Для того чтобы в XCA начать работать с токенами, нужно подключить библиотеку **PKCS#11** данного токена. Библиотеку PKCS#11 под РЕД ОС с поддержкой RSA для *Актив Рутокен ЭЦП* можно скачать по ссылке: https://www.rutoken.ru/support/download/pkcs/. Установите командой:

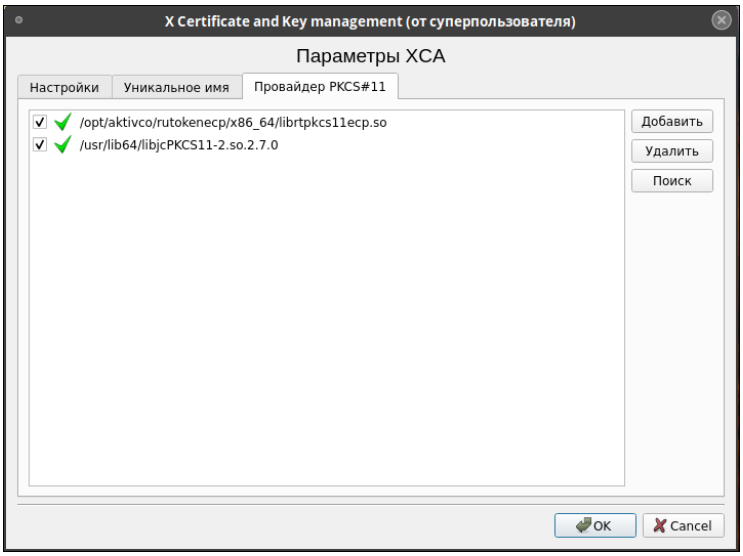
```
dnf localinstall librtpkcs11ecp-2.0.11.0-1.x86_64.rpm
```

Библиотеку PKCS#11 под РЕД ОС с поддержкой RSA для *Аладдин JaCarta PKI/GOST* можно скачать по ссылке: https://www.aladdin-rd.ru/support/downloads/jacarta. Сначала необходимо разархивировать все файлы, затем установить командой:

```
dnf localinstall jcpkcs11-2_2.7.0.443_x64.rpm
dnf localinstall jacartauc_2.13.0.3084_ro7.2_x64.rpm
```

2. Переходим в меню **«Файл» - «Настройки» - «Провайдер PKCS#11»**. 3. Нажимаем «*Добавить*» и ищем файл «**libjcPKCS11-2.so**» и «**librtpkcs11ecp.so**». Они могут находиться в директории **/usr/lib** или **/usr/lib64**. Если вы не можете найти этот файл, зайдите в терминал и найдите его с помощью команды:

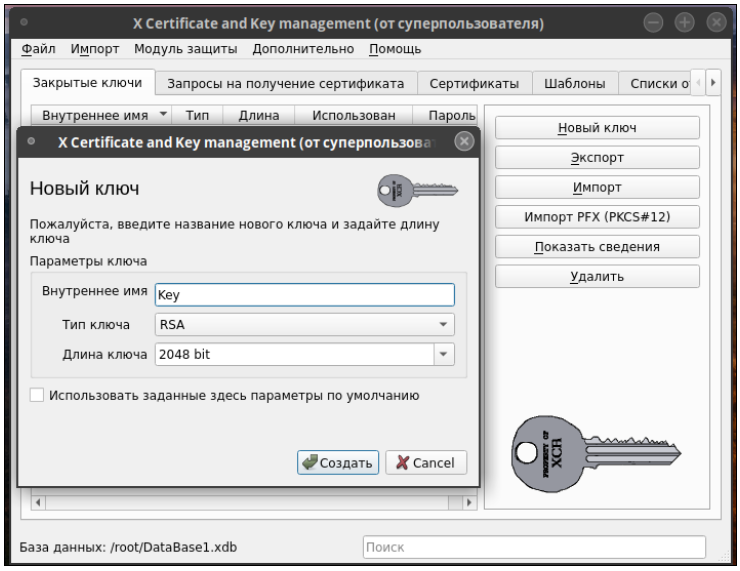
```
sudo find /usr -iname '*pkcs11*'
```



Примеры работы с XCA

Создание ключа SSH

1. Для начала перейдите на вкладку «*Закрытые ключи*». 2. Нажмите на кнопку «*Новый ключ*». 3. В поле «*Тип ключа*» выберите **RSA**. В поле «*Длина ключа*» выберите **2048 bit**. Имя ключу дайте на свое усмотрение.



Экспорт ключей

Для экспорта **открытого** ключа необходимо выполнить следующие действия:

1. Перейти на вкладку «*Закрытые ключи*» ; 2. Выбрать нужный «*Сертификат клиента*» ; 3. Нажать кнопку «*Экспорт*» ; 4. В появившемся окне в поле «*Формат сертификата*» нужно выбрать **Открытый ключ SSH2 (*.pub)** и указать путь к файлу, затем нажать «*OK*».

Для экспорта **закрытого** ключа необходимо выполнить следующие действия:

1. Перейти на вкладку «*Закрытые ключи*» ; 2. Выбрать нужный закрытый ключ сервера; 3. Нажать кнопку «*Экспорт*» ; 4. В появившемся окне в поле «*Формат для экспорта*» нужно выбрать **Закрытый ключ PEM (*.pem)**, указать путь к файлу, затем нажать «*OK*».

Для экспорта **закрытого ключа, зашифрованного паролем**, необходимо выполнить следующие действия:

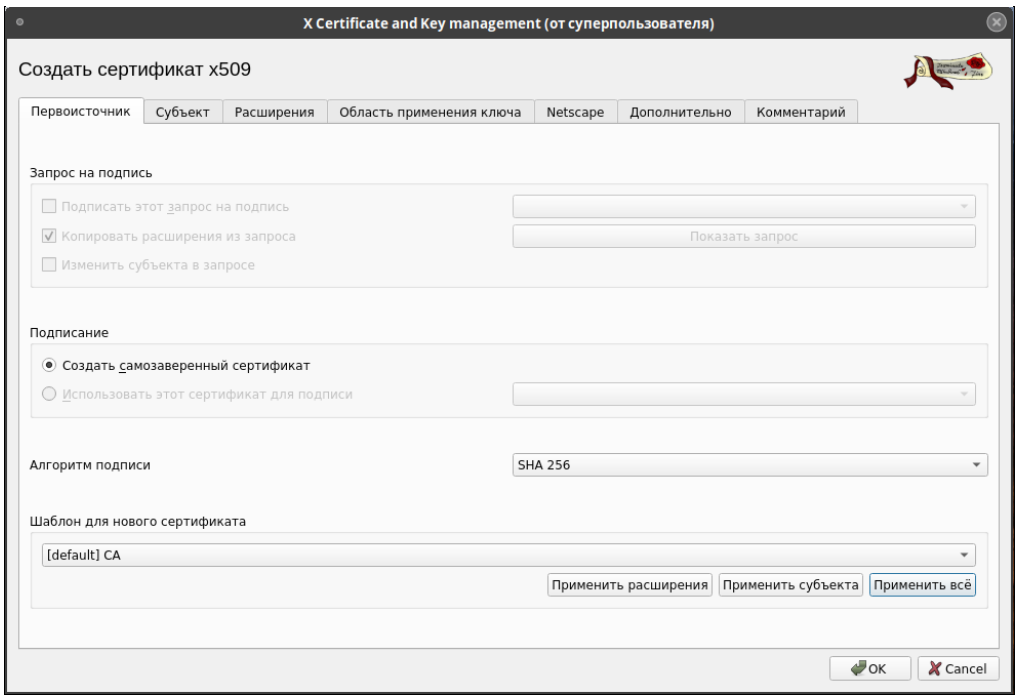
1. Перейти на вкладку «*Закрытые ключи*» ; 2. Выбрать нужный закрытый ключ сервера; 3. Нажать кнопку «*Экспорт*» ; 4. В появившемся окне в поле «*Формат для экспорта*» нужно выбрать **Зашифрованный ключ PEM (*.pem)**, указать путь к файлу, затем нажать «*OK*»; 5. В появившемся окне *Certificate and Key management* нужно ввести пароль, который будет требоваться для доступа к этому ключу.

Создание корневого сертификата

Корневой сертификат (**CA**) — часть ключа, которым центры сертификации подписывают выпущенные *SSL*-сертификаты. Выдавая корневой сертификат, каждый такой центр гарантирует, что пользователи или организации, запросившие SSL, верифицированы и действия с доменом легальны.

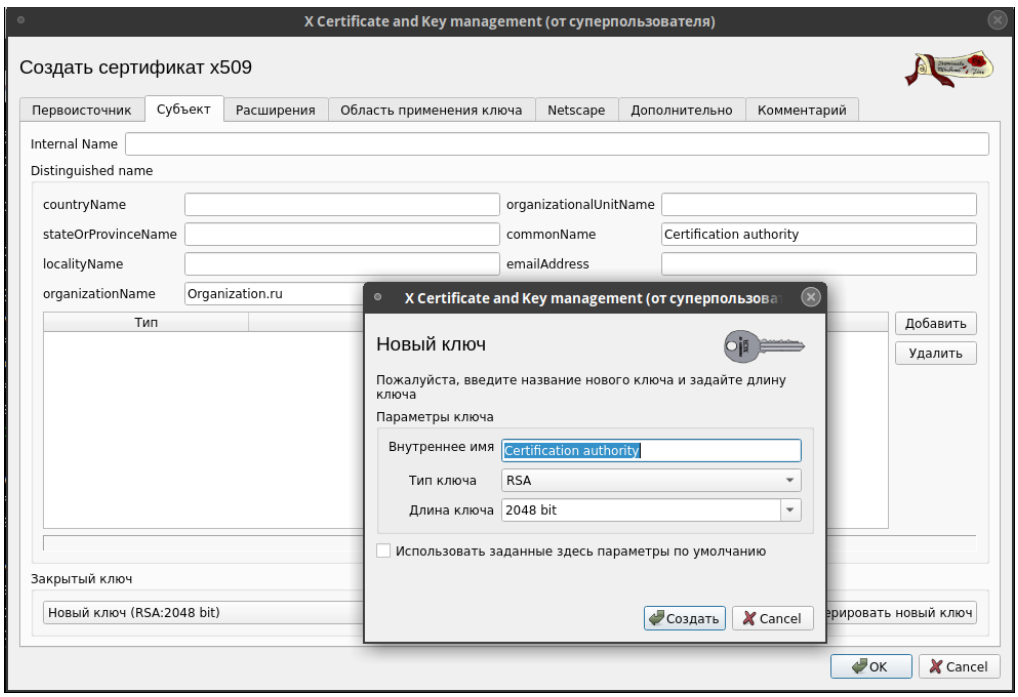
Для создания такого сертификата необходимо выполнить следующие действия:

1. Перейти на вкладку «*Сертификаты*» и выбрать «**Новый сертификат**» ; 2. Поставить галочку на пункт «*Создать самоподписанный сертификат...*»; 3. Выбрать «*Шаблон для нового сертификата*» - «**[Default] CA**»; 4. Нажать кнопку «**Применить всё**»;

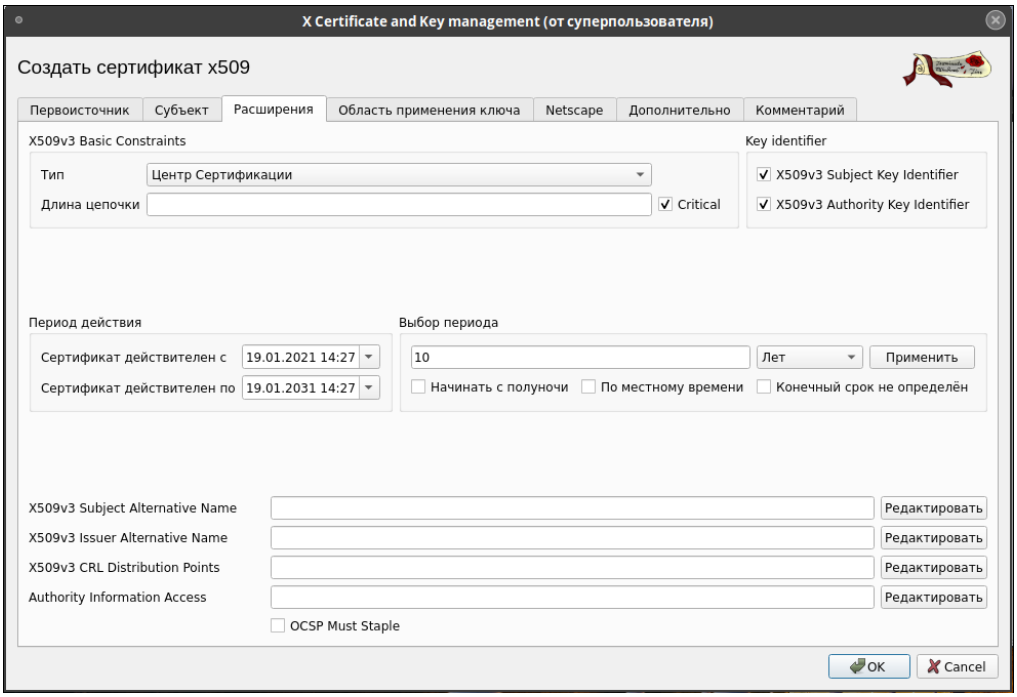


5. Перейти на вкладку «*Субъект*» («*Владелец*») ; 6. В поле «*organizatioName*» указать имя вашего домена; 7. В поле «*commonName*» указать имя «**Certification authority**» ; 8. По необходимости заполнить остальные поля;праитарна 9. Выбрать «*Создать новый ключ*»:

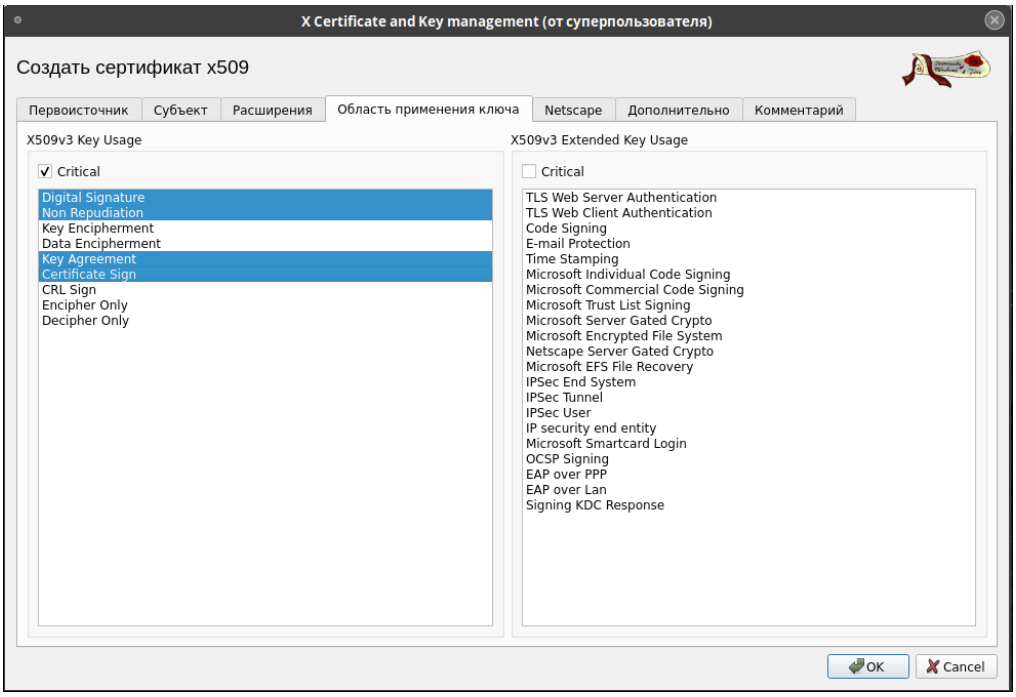
- В поле «Имя ключа» указать имя ключа, например «**Certification authority**»;
- Нажать «**Создать**»;



10. Перейти на вкладку «*Расширения*» ; 11. Убедиться, что выбран «*Тип*» «**Центр Сертификации**» ; 12. Отметить пункты «*Critical*», «*Subject Key identifier*», «*Authority key Identifier*»; 13. Определить срок действия сертификата: «*Временной диапазон*» => **10 (лет)**;



14. Перейти на вкладку «*Область применения ключа*»; 15. Отметить пункт «*Critical*», выбрать функции «**Digital Signature**», «**Non repudation**», «**Certificate Sign**», «**CRL Sign**»; 16. Сохранить созданный сертификат: «*Применить*» - «*Да*».



Блокировка макросов в LibreOffice

Макрос — это записанный пользователем программный алгоритм, позволяющий автоматизировать шаблонные действия при создании или редактировании документов.

Благодаря макросам пользователь может увеличить эффективность работы с приложением, а также гораздо быстрее выполнять определенные задачи: производить обработку внешних файлов, загрузку и передачу файлов и данных через интернет, чтение и изменение настроек операционной системы.

Однако не все макросы могут приносить пользу. Для повышения безопасности пользователя и предотвращения непреднамеренного открытия файлов, включающих активное содержимое, для офисных пакетов в РЕД ОС предусмотрена утилита с функцией блокировки макросов.

Данная функция помогает решить две основные задачи - защита от выполнения вредоносного кода при открытии документов и запрет исполнения произвольного кода через механизм макросов.

Для установки утилиты блокировки макросов перейдите в сеанс пользователя **root**:

```
su -
```

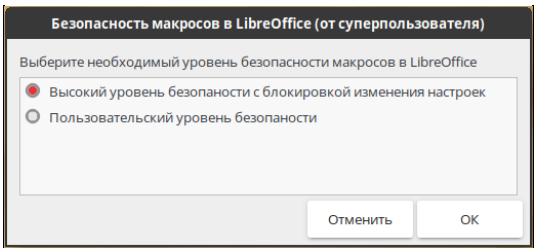
и выполните команду:

```
dnf install lo-macros-lock
```

После установки программа будет доступна из «**Главного меню**» - «**Администрирование**» - «**Безопасность макросов в LibreOffice**».

Для работы в программе необходимы привилегии пользователя **root**, поэтому при запуске необходимо ввести пароль суперпользователя.

После успешной аутентификации будет предложено выбрать необходимый уровень защиты:



После выбора нажмите «**OK**», чтобы изменения вступили в силу.

Для установки необходимого уровня защиты можно использовать консольный вариант работы с утилитой.

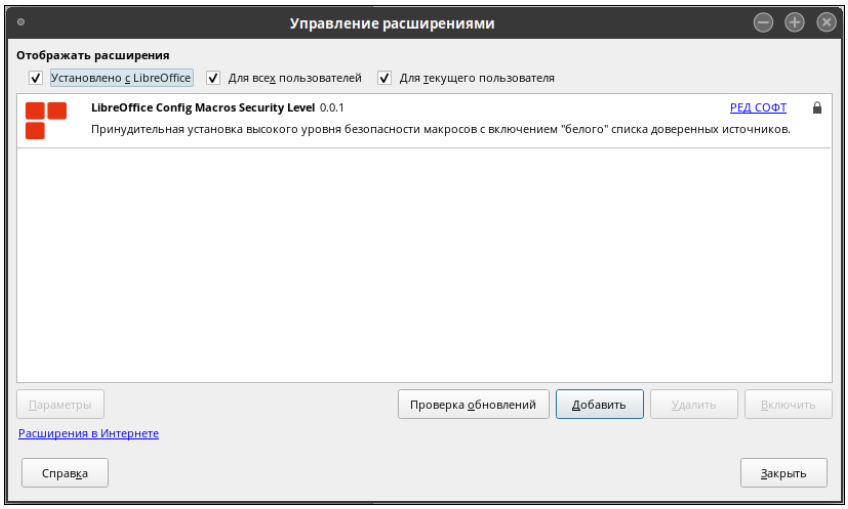
Для выбора «**Высокого уровня безопасности**» выполните:

```
lo-macros-lock -1
```

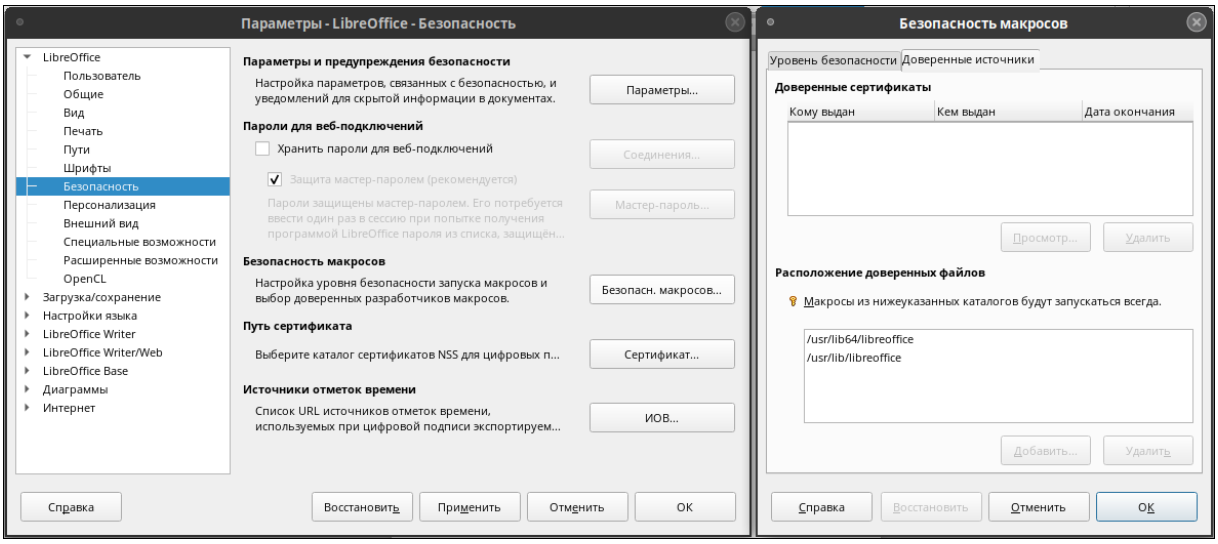
Для выбора «**Пользовательского уровня безопасности**» выполните:

```
lo-macros-lock -0
```

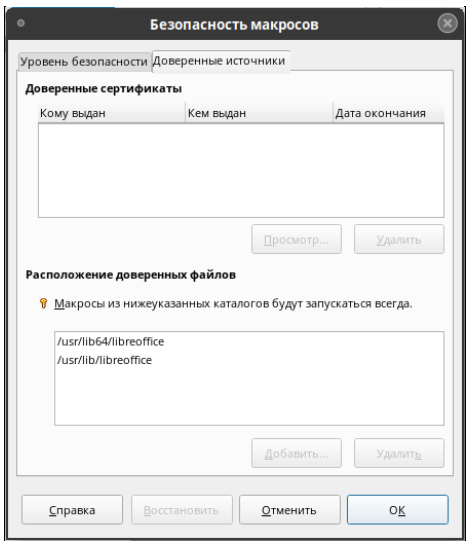
При выборе высокого уровня безопасности в папку системных расширений LibreOffice устанавливается блокирующее расширение, отображаемое при запуске любого офисного приложения.



В «**Параметрах**» LibreOffice при этом будет заблокирована возможность изменения режимов безопасности, а уровень безопасности будет установлен «**Очень высокий**».



В список «**Доверенных источников**» будут внесены системные каталоги LibreOffice без права пользователю их изменять.



ВАЖНО!

Будьте внимательны, запускайте макросы только из **надежных** источников!

Установка КриптоПро CSP 4.0

Установка CryptoPro CSP 4.0.0
Проверка лицензии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** CryptoPro 4.0.0 x64

КриптоПро — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами, организации структуры PKI и т.д.

Сайт: http://www.cryptopro.ru/

Примечание.

Для корректной работоспособности электронной подписи в информационных системах необходимо выполнить установку в последовательности:

1. Установить программное обеспечение для работы с корневыми и личными сертификатами по инструкции.
2. Установить браузер Chromiuim.
3. Установить плагин Госуслуг и КриптоПро, в зависимости от системных требований к информационной системе.

Вы можете подробнее ознакомиться с примером установки и настройки криптопровайдера CryptoPro, просмотрев наши обучающие видео:

- на **RuTube** — Установка КриптоПро CSP в РЕД ОС;
- в **Яндекс.Дзен** — Установка КриптоПро CSP в РЕД ОС;
- в **VK Видео** — Установка КриптоПро CSP в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка CryptoPro 4.0.0 x64

1. Скачайте архив с сайта КриптоПро по ссылке.

2. Распакуйте архив в папку (в примере **/home/test/**).

```
cd /home/test
tar -xvf linux-amd64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-amd64
```

4. Установите права на запуск:

```
chmod +x install_gui.sh
```

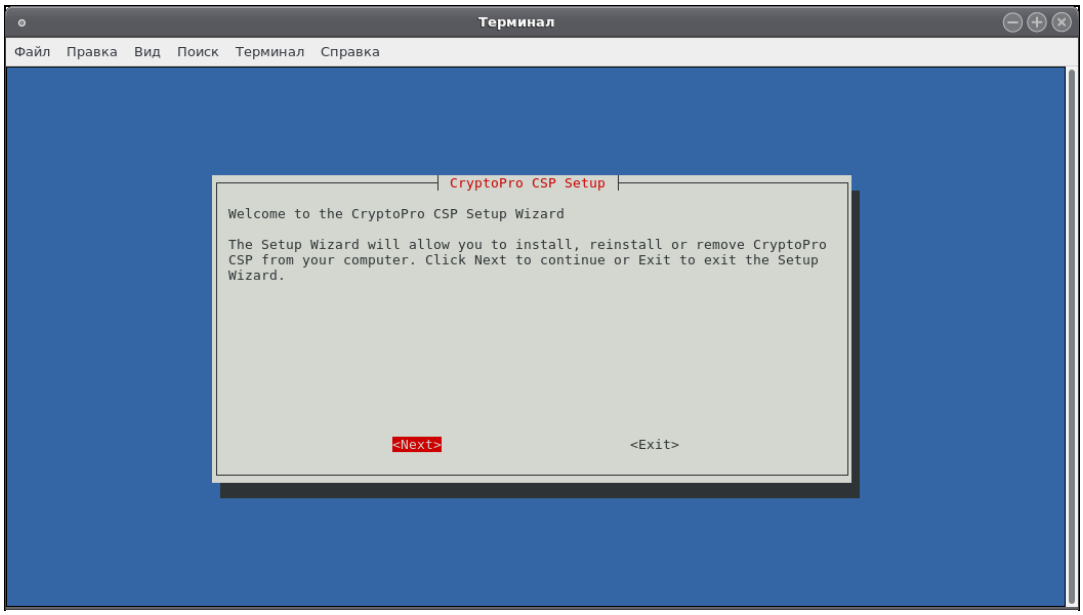
4.1 Выполните следующую команду (для того чтобы далее выполнять команды от пользователя **root**):

```
su root
```

5. Установите КриптоПро, выполнив команду:

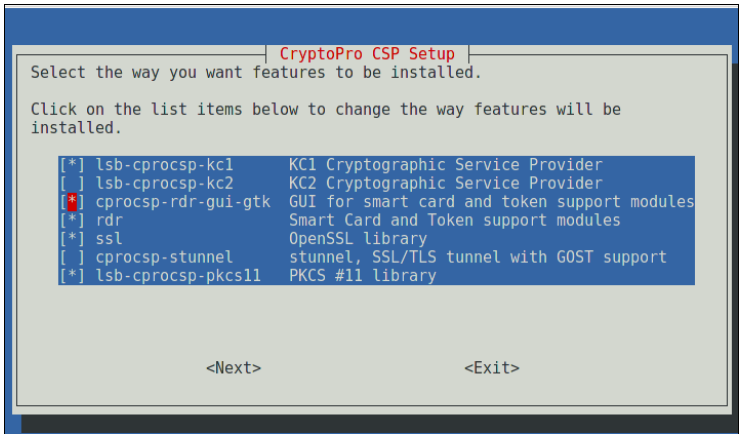
```
./install_gui.sh
```

Появится окно установки КриптоПро:

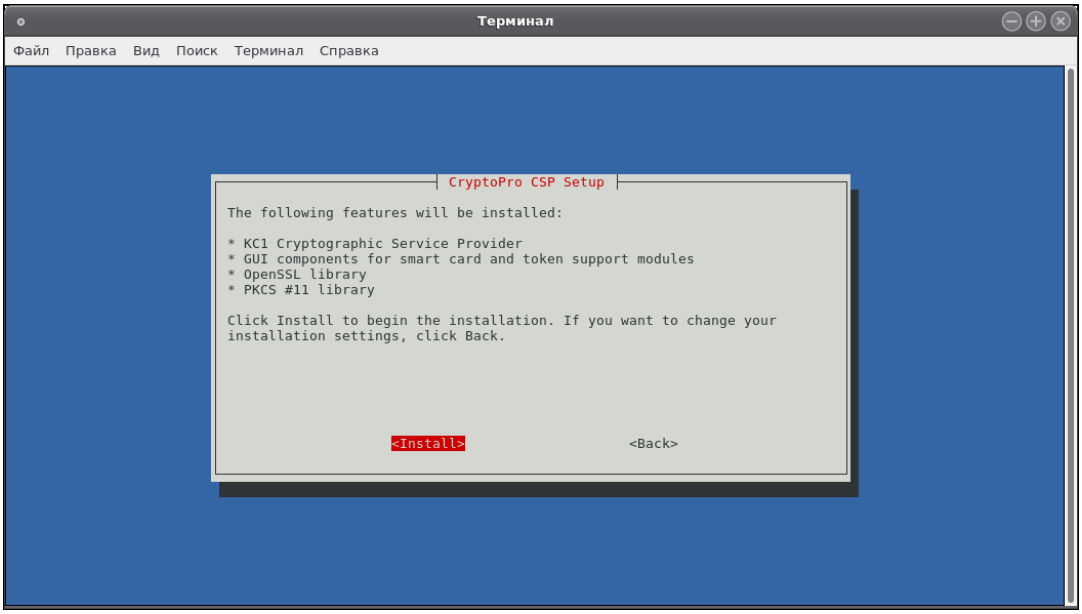


Нажмите кнопку «**Next**» для продолжения установки.

В следующем окне выберите пакеты, указанные на скриншоте:



Нажмите кнопку «**Next**» для продолжения установки:



Нажмите «**Install**» для установки пакетов.

6. Установите дополнительные пакеты и драйверы.

6.1 Установка драйверов и библиотек для работы **Рутокен S**, **Рутокен ЭЦП 2.0**, **Рутокен ЭЦП 3.0**.

Загрузите с официального сайта библиотеку **PKCS#11** с поддержкой RSA для Актив Рутокен ЭЦП. Перейдите в каталог с загруженным файлом (в примере ***/home/user/Загрузки***):

```
cd /home/user/Загрузки
```

Установите библиотеку командой:

```
dnf localinstall ./librtpkcs11ecp-2.15.1.0-1.x86_64.rpm
```

где **librtpkcs11ecp-2.15.1.0-1.x86_64.rpm** замените на актуальную версию.

Установите утилиту для обнаружения внешних устройств:

```
dnf install pcsc-tools
```

Для работы **Рутокен S** установите драйвер:

```
dnf install ifd-rutokens
```

6.2 Установка драйверов для токенов **Jacarta**:

Перейдите в папку:

```
cd /home/test/linux-amd64
```

Выполните команду установки:

```
dnf install cprocsp-rdr-jacarta*.rpm
```

Проверка лицензии

Вывод серийного номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

Ввод номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

Установка КриптоПро CSP 5.0

Установка CryptoPro CSP 5.0.0
Проверка лицензии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** CryptoPro 5.0.0 x64

КриптоПро — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами, организации структуры PKI и т.д.

Сайт: http://www.cryptopro.ru/

Примечание.

Для корректной работоспособности электронной подписи в информационных системах необходимо выполнить установку в последовательности:

1. Установить программное обеспечение для работы с корневыми и личными сертификатами по инструкции.
2. Установить браузер Chromiuim.
3. Установить плагин Госуслуг и КриптоПро, в зависимости от системных требований к информационной системе.

Вы можете подробнее ознакомиться с примером установки и настройки криптопровайдера CryptoPro, просмотрев наши обучающие видео:

- на **RuTube** — Установка КриптоПро CSP в РЕД ОС;
- в **Яндекс.Дзен** — Установка КриптоПро CSP в РЕД ОС;
- в **VK Видео** — Установка КриптоПро CSP в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка CryptoPro 5.0.0 x64

1. Скачайте архив с сайта КриптоПро по ссылке.

2. Распакуйте архив в папку (в примере **/home/test/**).

```
cd /home/test
tar -xvf linux-amd64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-amd64
```

4. Установите права на запуск:

```
chmod +x install_gui.sh
```

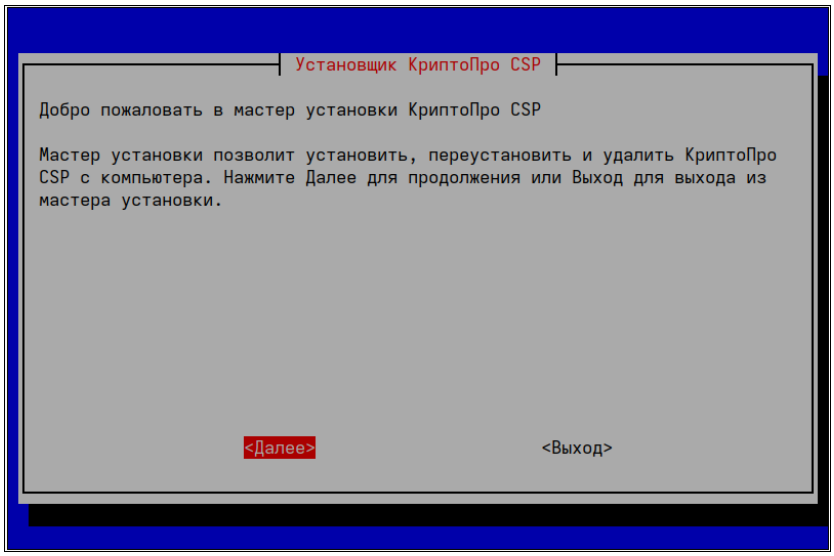
4.1 Выполните следующую команду (для того чтобы далее выполнять команды от пользователя **root**):

```
su root
```

5. Установите КриптоПро, выполнив команду:

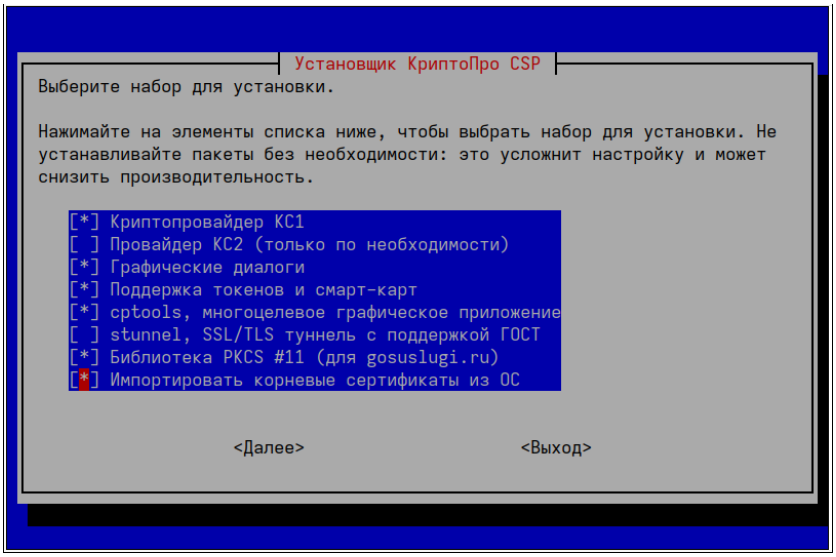
```
./install_gui.sh
```

Появится окно установки КриптоПро:

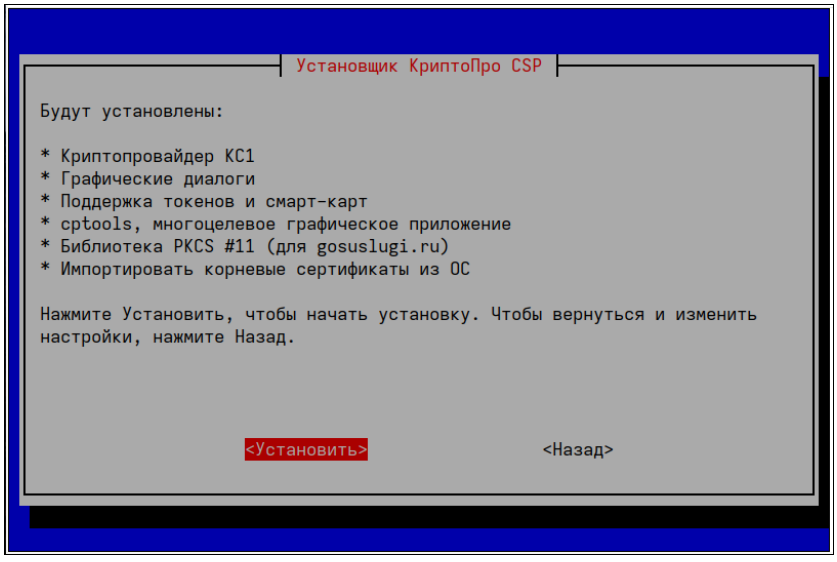


Нажмите кнопку «**Далее**» для продолжения установки.

В следующем окне выберите пакеты, указанные на скриншоте:



Нажмите кнопку «**Далее**» для продолжения установки:



Нажмите «**Установить**» для установки пакетов.

6. Установите дополнительные пакеты и драйверы.

6.1 Установка драйверов и библиотек для работы **Рутокен S**, **Рутокен ЭЦП 2.0**, **Рутокен ЭЦП 3.0**.

Загрузите с официального сайта библиотеку **PKCS#11** с поддержкой RSA для Актив Рутокен ЭЦП. Перейдите в каталог с загруженным файлом (в примере ***/home/user/Загрузки***):

```
cd /home/user/Загрузки
```

Установите библиотеку командой:

```
dnf localinstall ./librtpkcs11ecp-2.15.1.0-1.x86_64.rpm
```

где **librtpkcs11ecp-2.15.1.0-1.x86_64.rpm** замените на актуальную версию.

Установите утилиту для обнаружения внешних устройств:

```
dnf install pcsc-tools
```

Для работы **Рутокен S** установите драйвер:

```
dnf install ifd-rutokens
```

6.2 Установка драйверов для токенов **Jacarta**:

Перейдите в папку:

```
cd /home/test/linux-amd64
```

Выполните команду установки:

```
dnf install cprocsp-rdr-jacarta*.rpm
```

Проверка лицензии

Вывод серийного номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

Ввод номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

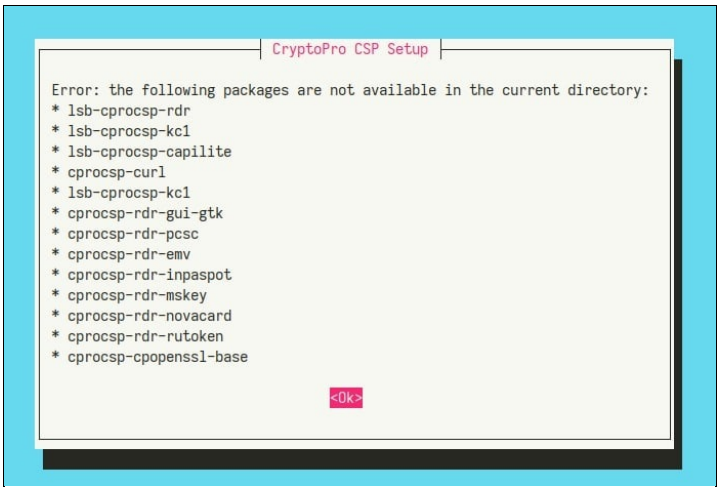
Работа с электронной подписью в РЕД ОС под Байкал-М

Установка КриптоПро CSP 4.0
Установка КриптоПро CSP 5.0
Установка драйверов для токенов Рутокен
Утилиты token-manager и gostcryptogui
Вход по сертификату на Госуслуги в РЕД ОС под Байкал-М

Работа с электронной подписью в РЕД ОС под **Байкал-М** (архитектура **aarch64**, она же **arm64**) аналогична работе в РЕД ОС x86_64. Но есть отличия в установке и настройке некоторых утилит.

Установка КриптоПро CSP 4.0

Установка **КриптоПро CSP 4.0** через стандартный установщик, входящий в дистрибутив **КриптоПро CSP 4.0** архитектуры **arm64**, невозможна. Установка завершается ошибкой:



Но установку можно выполнить через **dnf**, непосредственно указав перечень пакетов. Для этого:

1. Скачайте архив с сайта КриптоПро по ссылке.

2. Распакуйте архив в папку (в примере **/home/test/**).

```
cd /home/test
tar -xvf linux-arm64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-arm64
```

4. Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните установку пакетов **КриптоПро CSP 4.0** вручную:

```
dnf install ./lsb-cprocsp-base* ./lsb-cprocsp-rdr* ./lsb-cprocsp-kc1* ./lsb-cprocsp-capilite* ./cprocsp-rdr-gui-gtk* ./cprocsp-rdr-pcsc* ./lsb-cprocsp-pkcs11* pcsc-lite
```

Установка КриптоПро CSP 5.0

Установка **КриптоПро CSP 5.0** успешно выполняется через стандартный установщик, входящий в дистрибутив **КриптоПро CSP 5.0** архитектуры **arm64**:

1. Скачайте архив с сайта КриптоПро по ссылке.

2. Распакуйте архив в папку (в примере **/home/test/**).

```
cd /home/test
tar -xvf linux-arm64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-arm64
```

4. Выполните установку **КриптоПро 5.0** командой:

```
./install_gui.sh
```

Установка драйверов для токенов Рутокен

Драйверы **Рутокен** ЭЦП для архитектуры **arm64** (**aarch64**) доступны по ссылке:

http://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/ARM/aarch64/

Плагин **Rutoken** доступен по следующей ссылке:

http://download.rutoken.ru/Rutoken_Plugin/Current/Linux/

Установка драйвера и плагина выполняется штатно через **dnf**.

Утилиты token-manager и gostcryptogui

Утилиты для работы с сертификатами и электронной подписью **token-manager** и **gostcryptogui** адаптированы под архитектуру **arm64** (**aarch64**) и успешно работают в РЕД ОС под **Байкал-М** с **КритоПро CSP** версий **4.0** и **5.0**.

Вход по сертификату на Госуслуги в РЕД ОС под Байкал-М

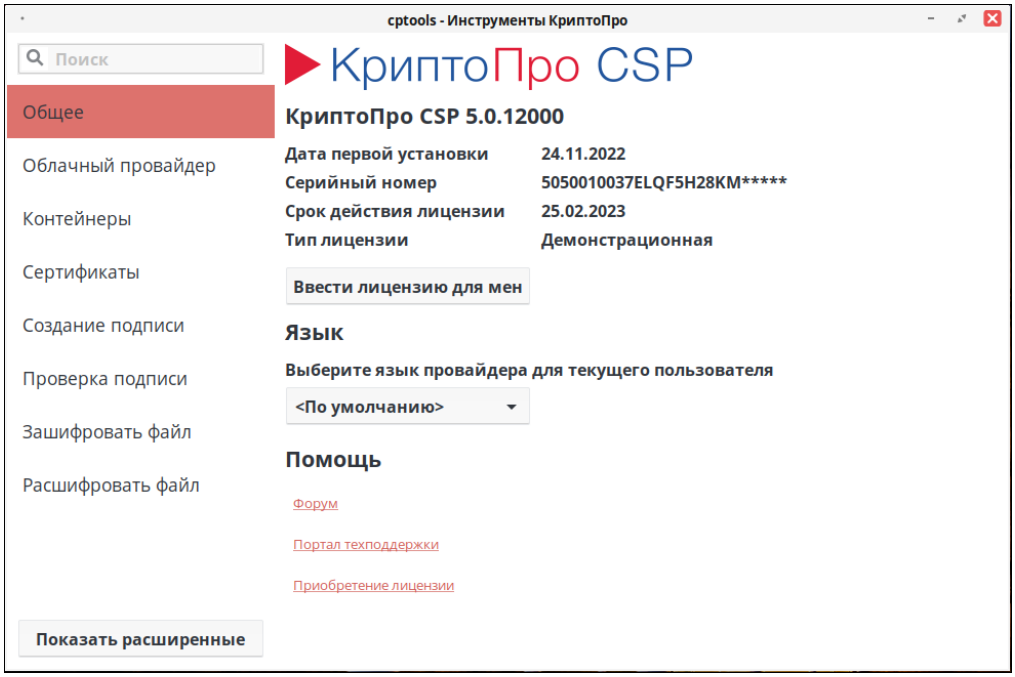
Вход по сертификату на Госуслуги через браузер **Chromium** и другие пока не поддерживается, т.к. разработчиком еще не выпущен плагин Госуслуг (**IFCPlugin**) под архитектуру **arm64** (**aarch64**): https://ds-plugin.gosuslugi.ru/plugin/upload/Index.spr

Графические утилиты для работы с КриптоПро CSP

Инструменты КриптоПро
Установка программного обеспечения для работы с сертификатами
Ключевые носители и сертификаты
GOST-CRYPTO-GUI
Подпись документов в LibreOffice

Инструменты КриптоПро

В **КриптоПро** версии **5.0** появилась графическая утилита для работы с сертификатами - **cptools**. Запуск утилиты доступен из «**Главного меню**» – «**Параметры**» – «**Инструменты КриптоПро**».



Запуск из терминала:

```
cptools

или

/opt/cprocsp/bin/*/cptools
```

Установка программного обеспечения для работы с сертификатами

1. Установка средства управления сертификатами **token-manager**:

```
dnf install token-manager python3-chardet
```

1.2 Доступен формат запуска приложения без установки в ОС. Для этого скачайте AppImage и сделайте его исполняемым:

```
wget $(curl -s https://api.github.com/repos/wolandius/token-manager/releases/latest | grep browser_download_url | cut -d\" -f4 | grep 'ro73')
```

- Запуск:

```
chmod +x ./token-manager-*-x86_64.AppImage
./token-manager-*-x86_64.AppImage
```

2. Установка программного обеспечения для подписи файлов **gostcrypto**.

```
dnf install gostcryptogui
```

2.2 Доступен формат запуска приложения без установки в ОС. Для этого скачайте AppImage и сделайте его исполняемым:

```
wget $(curl -s https://api.github.com/repos/wolandius/gost-crypto-gui/releases/latest | grep browser_download_url | cut -d\" -f4 | grep 'ro73')
```

- Запуск:

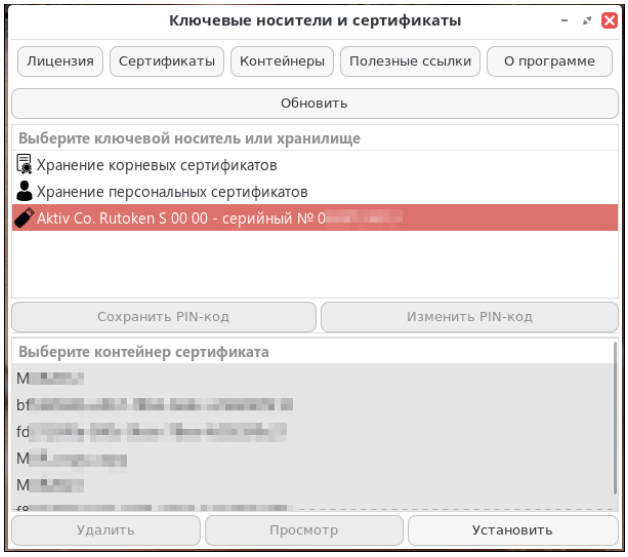
```
chmod +x ./gost-crypto-gui-*-x86_64.AppImage
./gost-crypto-gui-*-x86_64.AppImage
```

Работа с ключевыми носителями и сертификатами

Ключевые носители и сертификаты

Для работы с ключевыми носителями и сертификатами используется утилита «**Ключевые носители и сертификаты**», которую мы установили ранее. Найти его можно в «**Главном меню**» - «**Администрирование**» - «**Ключевые носители и сертификаты**».

Окно программы выглядит следующим образом:



В меню «**Операции**» можно выполнить:

- Ввод лицензии КриптоПро CSP;
- Просмотр лицензии;

- Установка корневых сертификатов;
- Установка списка отозванных сертификатов;
- Запись сертификата в контейнер;
- Экспортировать сертификат из контейнера;
- Связать сертификат с контейнером;
- Просмотр корневых сертификатов;
- Просмотр списков отозванных сертификатов;

- Скопировать контейнер с токена;
- Скопировать контейнер с **usb-flash** накопителя;
- Скопировать токен из HDIMAGE на токен.

Рассмотрим более подробно копирование контейнера с **usb-flash** накопителя.

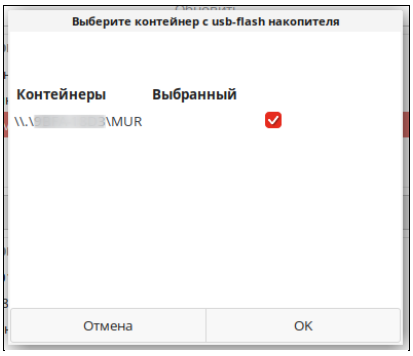
1. Необходимо с **RuToken** скопировать закрытую часть электронной подписи (ЭП) на *usb-flash* накопитель, выполнить это необходимо на КриптоПро в ОС Windows.

Инструкция для Windows находится по ссылке.

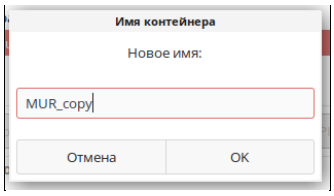
2. Вставьте *usb-flash* накопитель в компьютер и запустите утилиту **Ключевые носители и сертификаты**.

3. Перейдите в меню «**Операции**» и выберите «**Скопировать контейнер с *usb-flash* накопителя**».

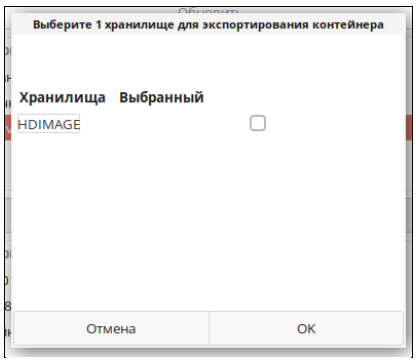
4. Появится окно с выбором контейнера. Выберите необходимый контейнер, отметив чекбокс в поле «**Выбранный**».



5. Задайте имя контейнеру.

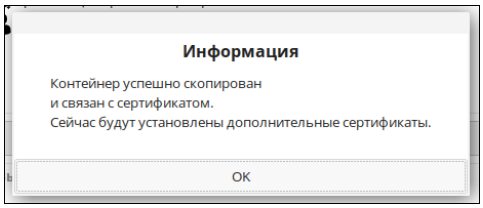


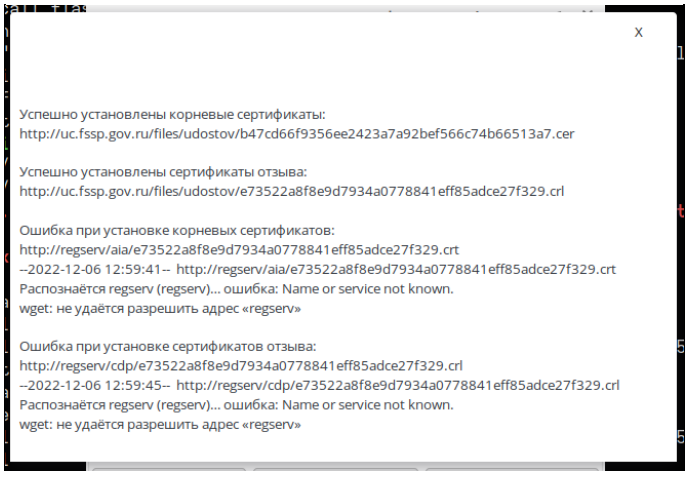
6. Выберите контейнер, в который требуется скопировать.



7. Далее потребуется ввести PIN-код контейнеров.

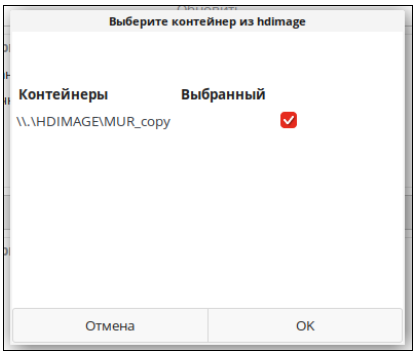
8. Появится окно с успешной привязкой контейнера с сертификата. Сертификат отобразится в «**Личном хранилище сертификатов**».





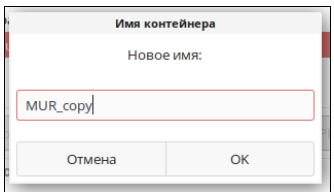
Работа по копированию контейнеров с токена или из **HDIMAGE** имеет схожую логику.

1. Для выбора необходимого контейнера требуется выбрать галочкой необходимый.

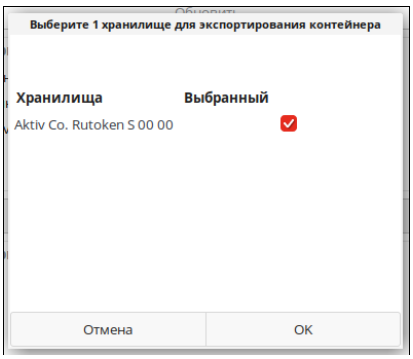


2. Следующим этапом необходимо выбрать пункт назначения копирования.

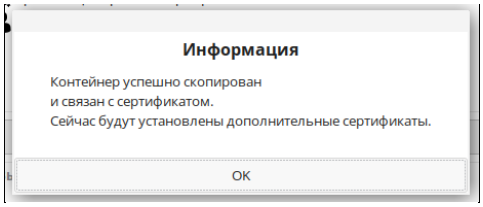
Пользователю предоставляется возможность задать новое имя копируемого контейнера (настоятельно рекомендуем использовать латиницу).

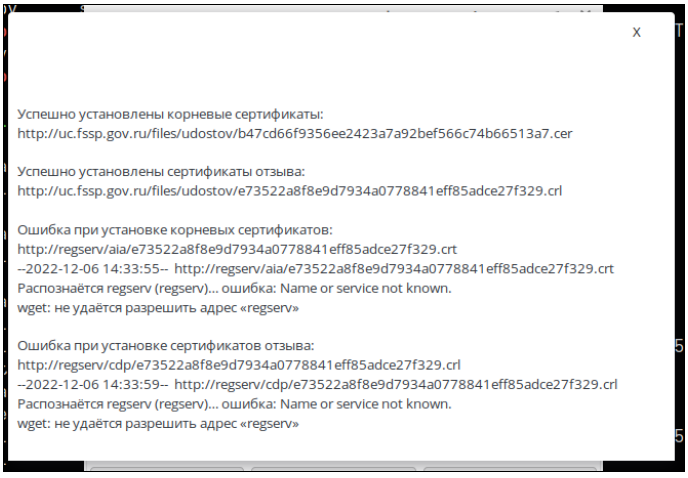


3. Далее выбирается токен или **HDIMAGE**.

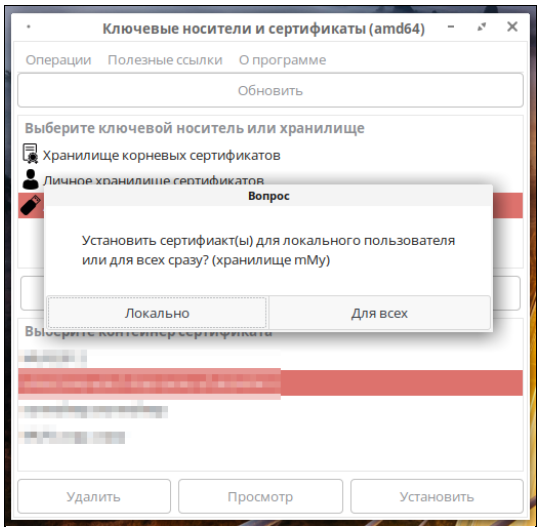


4. После ввода PIN-кодов, в случае успеха, вы увидите сообщение:





Стоит обратить внимание на диалоговое окно, которое добавлено для работы с КриптоПро версии 5 и новее. Данное диалоговое окно позволяет устанавливать сертификаты в машинное хранилище ПК или в личное хранилище пользователя. Вызов диалогового окна происходит при попытке установки из локального файла сертификата или с токена.



В последних версиях **token-manager** была добавлена возможность консольного запуска утилиты с использованием ряда ключей:

```
token-manager.py --help

Подсказки по использованию ключей в token-manager:
В данной реализации token-manager поддерживает явное указание архитектуры КриптоПро, вместо автоматического.
 --amd64         вызов 64-битной версии КриптоПро;
 --ia32          вызов 32-битной версии КриптоПро;
 --aarch64       вызов aarch64 версии КриптоПро;
 --e2k64         вызов e2k64 версии КриптоПро;
 --version       вывод номера версии token-manager;
 --debug-output  пробный вызов основных функций утилиты;
 --debug-output --amd64 пробный вызов основных функций утилиты для архитектуры amd64;
 --debug-output --ia32 пробный вызов основных функций утилиты для архитектуры ia32;
 --debug-output --aarch64 пробный вызов основных функций утилиты для архитектуры aarch64;
 --debug-output --e2k64 пробный вызов основных функций утилиты для архитектуры e2k64;
```

Пример вывода версии утилиты:

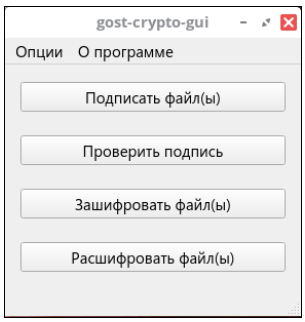
```
token-manager.py --version

token-manager версия 5.2.2
```

GOST-CRYPTO-GUI

Формат подписи может настраиваться в графической утилите **gostcryptogui**, которую мы рассмотрим далее.

Запуск утилиты производится из «**Главного меню**» - «**Администрирование**» - «**Подпись и шифрование файлов**».

Окно программы выглядит следующим образом:

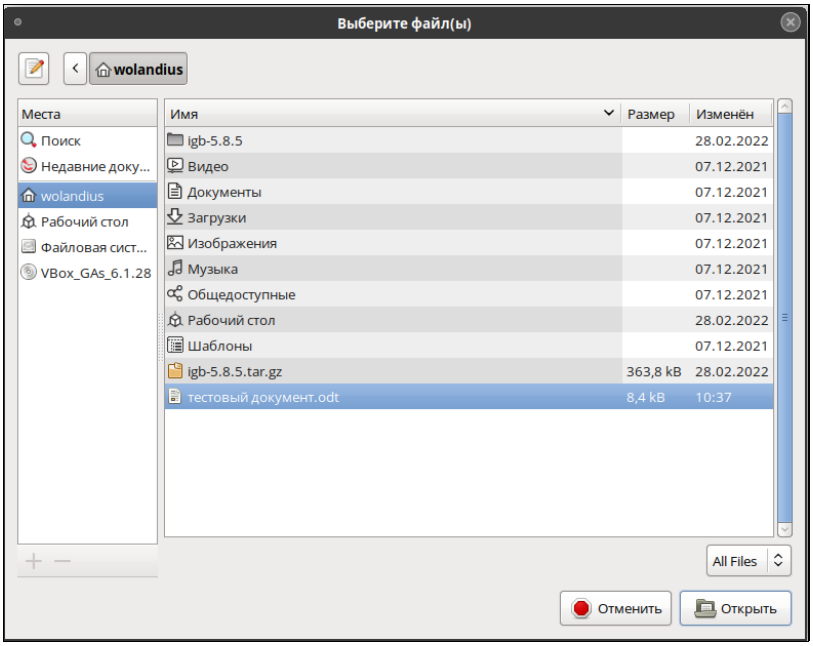


Доступны следующие опции:

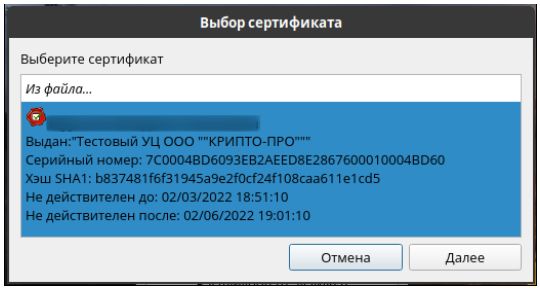
- Криптопровайдер;
- Кодировка файлов;
- Авт. проверка подписи;
- Отсоединённая подпись.

Для примера зашифруйте файл, но с использованием другого сертификата, размещённого на ключевом носителе **Rutoken**.

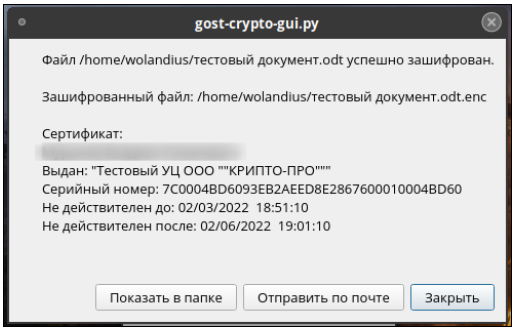
Выберите необходимый файл:



Затем укажите ваш сертификат:

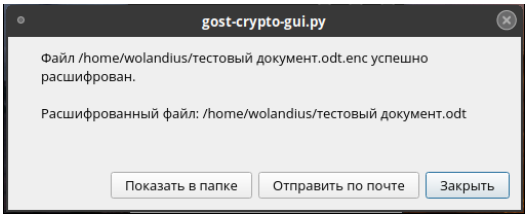


Зашифрованный файл формируется с тем же именем и расширением **.enc**.



После этого попробуйте его расшифровать.

Нажмите «**Расшифровать файл(ы)**», выберите зашифрованный файл, затем сертификат, которым был зашифрован наш файл.



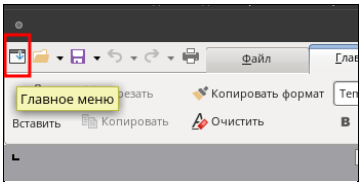
Подпись документов в LibreOffice

Для активации подписания документов потребуется установить плагин:

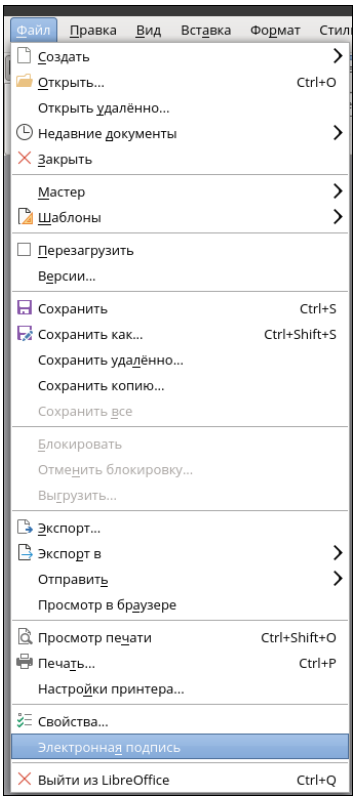
```
dnf install LibreOffice-plugin-altcsp
```

Для активации подписи требуется нажать кнопку «**Файл**». Если меню «**Файл**» недоступно, нажмите предварительно кнопку,

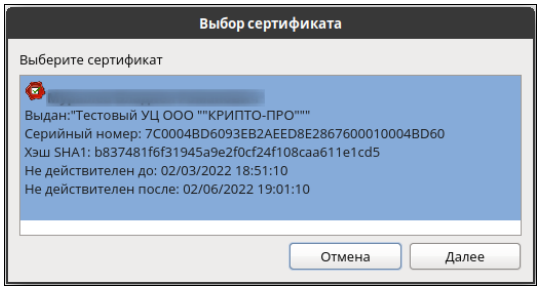
выделенную на скриншоте:



Нажмите кнопку «**Электронная подпись**»:



Для подписи вам будет предложен выбор сертификата:

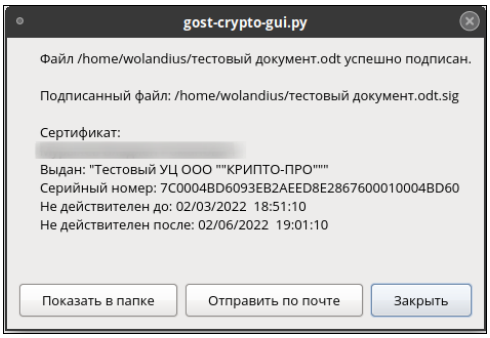


Также не забудьте проверить, что для выбранного сертификата у вас установлены все необходимые корневые и отозванные сертификаты. Пример необходимых сертификатов можно проверить командой:

```
certmgr -list -store uMy

***
CA cert URL : http://testgost2012.cryptopro.ru/CertEnroll/root2018.crt
CDP : http://testgost2012.cryptopro.ru/CertEnroll/!0422!0435!0441!0442!043e!0432!044b!0439%20!0423!0426%20...
CDP : http://testgost2012.cryptopro.ru/CertEnroll/testgost2012(1).crl
***
```

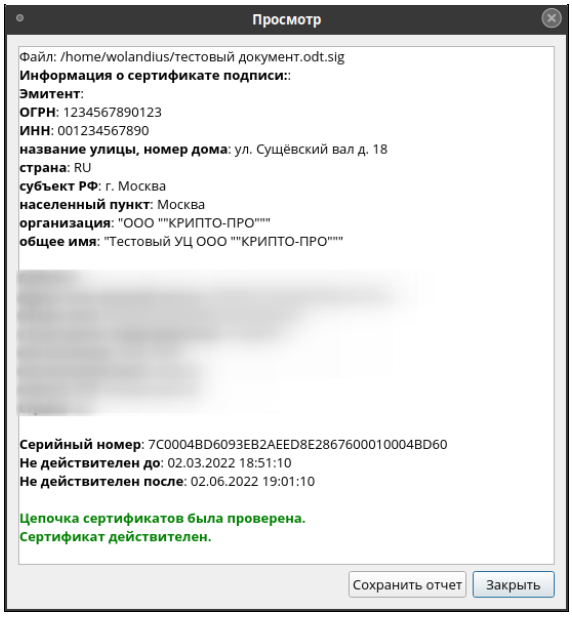
Как показано в примере, необходимо доставить **3 сертификата.** Выполнить это можно через **token-manager** и установку сертификатов из утилиты.

В случае успешной подписи вы увидите следующее уведомление:



Проверить подпись можно из «**gostcryptogui**» - «**Проверить подпись**».

После выбора документа вы увидите следующую информацию:



Работа с сертификатами КриптоПро

Работа с криптоконтейнерами
Решение проблемы отсутствия контейнеров в КриптоПро в домене
Установка личных сертификатов
Установка корневых сертификатов
Установка сертификатов pfx
Просмотр сертификатов
Удаление сертификатов
Перенос контейнера с flash-носителя в локальное хранилище ПК
Просмотр цепочки сертификата

Для удобства использования утилит КриптоПро создадим на них символьные ссылки, для этого выполните:

```
ln -s /opt/cprocsp/bin/amd64/certmgr /usr/bin/certmgr
ln -s /opt/cprocsp/bin/amd64/csptest /usr/bin/csptest
ln -s /opt/cprocsp/sbin/amd64/cpconfig /usr/bin/cpconfig
```

Просмотр версии КриптоПро:

```
csptest -enum -info
```

или

```
cat /etc/opt/cprocsp/release
```

Проверка лицензии:

```
cpconfig -license -view
```

Для установки лицензии выполните (с правами **root**):

```
# cpconfig -license -set <серийный_номер>
```

При использовании токенов сервис **pcscd** должен быть запущен. Проверка статуса **pcscd**:

```
systemctl status pcscd
```

если он выключен, то включите его:

```
systemctl start pcscd
systemctl enable pcscd
```

Вывод сообщений журнала службы **pcscd**:

```
pcscd -dffff
```

Узнать модель подключенного токена:

```
csptest -card -enum -v -v
pcsc_scan
```

Работа с криптоконтейнерами

1. Проверить наличие доступных контейнеров:

```
csptest -keyset -enum_cont -fqcn -verifyc | iconv -f cp1251

CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 16778675
\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4
\\.\FLASH\bob
```

```
\\.\HDIMAGE\bob
OK.
Total: SYS: 0,010 sec USR: 0,110 sec UTC: 6,240 sec
[ErrorCode: 0x00000000]
```

Имена контейнеров используются для установки личных сертификатов.

- Считыватель **HDIMAGE** размещается в **/var/opt/cprocsp/keys/<имя пользователя>/** т.е в данном случае используется жесткий диск для хранения ключей.
- Считыватель **FLASH** означает, что используется флешка для хранения приватных ключей.
- Также считывателем может выступать токен.

2. Имена контейнеров могут содержать символы на кириллице, поэтому чтобы корректно отобразить контейнеры используйте следующую команду:

```
csptest -keyset -enum_cont -fqcn -verifyc | iconv -f cp1251
```

Для дальнейшего использования имен контейнеров содержащих кодировку **cp1251**, выведем список контейнеров с уникальными именами:

```
csptest -keyset -enum_cont -fqcn -verifyc -uniq

CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 23397811
\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4 | \\.\Aladdin R.D. JaCarta 00
00\SCARD\JACARTA_6082028344937676\CC00\E412
OK.
Total: SYS: 0,000 sec USR: 0,110 sec UTC: 6,230 sec
[ErrorCode: 0x00000000]
```

3. Просмотр подробной информации о контейнере:

```
csptest -keyset -container '\\.\HDIMAGE\bob' -info
```

4. Перечисление контейнеров пользователя:

```
csptest -keyset -enum_cont -verifycontext -fqcn
```

5. Перечисление контейнеров компьютера:

```
csptest -keyset -enum_cont -verifycontext -fqcn -machinekeys
```

6. Открыть(проверить) контейнер пользователя:

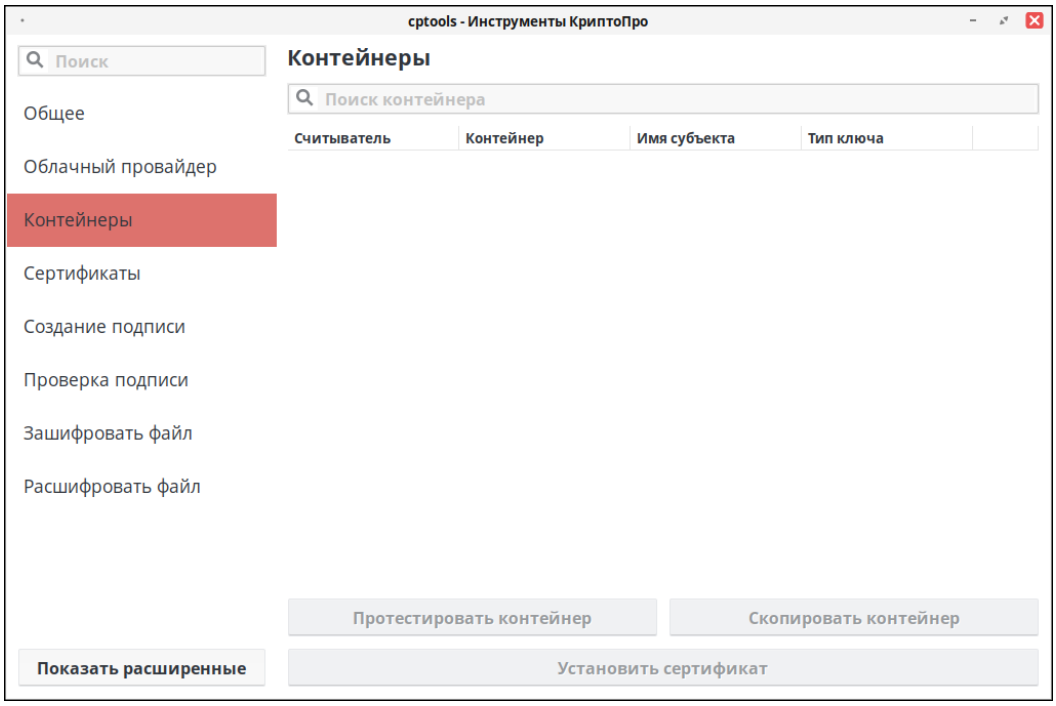
```
csptest -keyset -check -cont '\\.\имя считывателя\имя контейнера'
```

7. Открыть(проверить) контейнер компьютера:

```
csptest -keyset -check -cont '\\.\имя считывателя\имя контейнера' -machinekeyset
```

Решение проблемы отсутствия контейнеров в КриптоПро в домене

В некоторых случаях, если компьютер введен в домен, может возникнуть проблема отсутствия контейнеров под доменным пользователем.



Для решения данной проблемы необходимо выполнить ряд действий:

1. Создать **udev**-правило командой:

```
nano /etc/udev/rules.d/87-domain_usb.rules
```

Добавить в него следующее содержимое:

```
ENV{ID_FS_USAGE}=="filesystem|other|crypto", ENV{UDISKS_FILESYSTEM_SHARED}="1"
```

2. Выполнить перезапуск **udev**-правил:

```
udevadm control --reload
```

3. Проверить наличие файла **/var/lib/AccountsService/users/<имя_пользователя>**, где **<имя_пользователя>** – имя вашего доменного пользователя.

Если файла нет, его необходимо создать по примеру существующего.

Пример содержимого файла можно просмотреть в том же каталоге в файле локального пользователя:

```
cat /var/lib/AccountsService/users/user

[User]
Language=
XSession=
Icon=/home/user/.face
SystemAccount=false
```

Перезагрузите систему для применения внесенных изменений.

Если вышеприведенное решение не помогло, следует переустановить КриптоПро, запустив скрипт **uninstall.sh** (скрипт находится в архиве с установщиком КриптоПро):

```
./uninstall.sh
```

Затем удалить оставшиеся каталоги:

```
rm -rf /opt/cprocsp /etc/opt/cprocsp /var/opt/cprocsp
```

После полного удаления потребуется произвести установку КриптоПро с **udev**-правилом, приведенным в п. 1.

Установка личных сертификатов

1. Установка сертификата без привязки к ключам:

```
certmgr -inst -file cert_bob.cer
```

2. Установка личного сертификата cert_bob.cer, сертификат при этом попадает в пользовательское хранилище **uMy**. Приватный ключ находится на флешке.

```
certmgr -inst -file cert_bob.cer -store uMy -cont '\\.\FLASH\bob'
```

в команде указывается сертификат cert_bob.cer, который ассоциируется с приватным контейнером **\\.\FLASH\bob'**

3. Установка сертификата с токена (в конце команды указывается контейнер)

```
/opt/cprocsp/bin/amd64/certmgr -inst -store uMy -cont '\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4'
```

Установка корневых сертификатов

При установке корневых сертификатов достаточно указать хранилище **uRoot**. При указании **mRo o t** (при наличии прав администратора) корневой сертификат будет доступен всем пользователям системы.

1. Установка в хранилище КриптоПро**:**

```
certmgr -inst -store uRoot -file <название-файла>.cer
```

2. Установка в хранилище ПК:

```
certmgr -inst -store mRoot -file <название-файла>cer
```

3. Установка списка отозванных сертификатов **crl**:

```
certmgr -inst -crl -file <название-файла>.crl
```

Установка сертификатов pfx

1. Необходимо установить пакет **cprocsp-rsa**, который находится в составе дистрибутива КриптоПро (**linux-amd64**).

2. Выполним команду от **локального** (доменного) пользователя:

```
/opt/cprocsp/bin/amd64/certmgr -inst -store uMy -pfx -pin <пинкод> -file 'путь до pfx'
```

Цепочка сертификатов будет отображаться в утилите «**Ключевые носители и сертификаты**» в «**Личное хранилище сертификатов**».

Просмотр сертификатов

1. Просмотр установленных сертификатов:

```
certmgr -list
```

2. Просмотр установленных сертификатов в локальном хранилище **uMy**:

```
certmgr -list -store uMy
```

3. Просмотр сертификатов в хранилище ПК (обычно сюда устанавливаются корневых сертификаты):

```
$ certmgr -list -store uRoot
```

4. Просмотр сертификатов в контейнере:

```
certmgr -list -container '\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4'
```

5. Просмотр промежуточных сертификатов:

```
certmgr -list -store uca
```

Удаление сертификатов

1. Удалить сертификат из личного хранилища сертификатов

Просмотрите установленные сертификаты:

```
certmgr -list
```

Изучите список всех установленных сертификатов (в общем списке отображаются абсолютно все сертификаты).

Для удаления следует выполнить команду в Терминале:

```
certmgr -delete -store uMy
```

Если установлено более одного сертификата, то будет предложено указать номер удаляемого сертификата.

2. Удалить сертификаты, установленные в хранилище КриптоПро:

```
certmgr -delete -store uRoot
```

Если установлено более одного сертификата, то будет предложено указать номер удаляемого сертификата.

3. Удалить все сертификаты, установленные в хранилище КриптоПро:

```
certmgr -delete -all -store uRoot
```

4. Удалить все сертификаты, установленные в хранилище ПК:

```
certmgr -delete -store mRoot
```

Перенос контейнера с flash-носителя в локальное хранилище ПК

1. Активируем хранилище **HDIMAGE**:

```
cpconfig -hardware reader -add HDIMAGE store

Adding new reader:
Nick name: HDIMAGE
Succeeded, code:0x0
```

2. Посмотрим, какие контейнеры доступны на флешке:

```
csptest -keyset -enum_cont -fqcn -verifyc

CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 32114099
\\.\FLASH\bob
OK.
Total: SYS: 0,020 sec USR: 0,080 sec UTC: 0,190 sec
[ErrorCode: 0x00000000]
```

3. Перейдите на Flash-носитель и скопируйте этот контейнер — каталог **bob.000** с приватными (закрытыми) ключами в **/var/opt/cprocsp/keys/user** - в этом каталоге находится локальное хранилище **HDIMAGE**

4. Посмотрим доступные контейнеры:

```
csptest -keyset -enum_cont -fqcn -verifyc
```

```
CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 36951475
\\.\FLASH\bob
\\.\HDIMAGE\bob
OK.
Total: SYS: 0,000 sec USR: 0,070 sec UTC: 0,160 sec
[ErrorCode: 0x00000000]
```

Как видим, появился новый контейнер `\\.\HDIMAGE\bob`
Теперь flash-носитель можно отключить, он нам больше не понадобится.

5. Установим пользовательский сертификат с привязкой к закрытому контейнеру `\\.\HDIMAGE\bob`

```
certmgr -inst -file cert-bob.cer -cont '\\.\HDIMAGE\bob'
```

Просмотр цепочки сертификата

Просмотр необходимых корневых сертификатов и сертификатов отзыва вы можете посмотреть следующей командой:

1) Для сертификатов, хранящихся в личном хранилище:

```
certmgr -list -store uMy
```

Интересующие строки, информирующие о необходимом сертификате начинаются со слов

```
URL сертификата УЦ
URL списка отзыва
```

Или в английском варианте:

```
CA cert URL
CDP
```

2) Для просмотра цепочки на токене выполните следующую команду:

```
certmgr -list -cont '<CONTAINER>'
```

Где вместо '<CONTAINER>' укажите ваш контейнер, к примеру '\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4'

3. Просмотр цепочки из файла сертификата:

```
certmgr -list -file 'путь_к_файлу'
```

Установка плагинов Госуслуг и КриптоПро в браузерах Chromium, Яндекс.Браузер, Firefox

Установка КриптоПро для работы с корневыми и личными сертификатами
Настройка браузера Chromium
Настройка Яндекс.Браузера
Настройка браузера Firefox
Установка КриптоПро «CryptoPro Extension for CAdES Browser Plug-in»
Добавление сайта в список доверенных сайтов плагина
Вход на сайт Госуслуги через Chromium

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: cryptopro-4.0, cryptopro-5.0

Установка КриптоПро для работы с корневыми и личными сертификатами

Для установки **КриптоПро 4.0** перейдите по ссылке.

Для установки **КриптоПро 5.0** перейдите по ссылке.

Настройка браузера Chromium

Установка браузера Chromium

В РЕД ОС браузер **Chromium** установлен по-умолчанию и доступен из «**Главного меню**» - «**Интернет**» - «**Веб-браузер Chromium**».

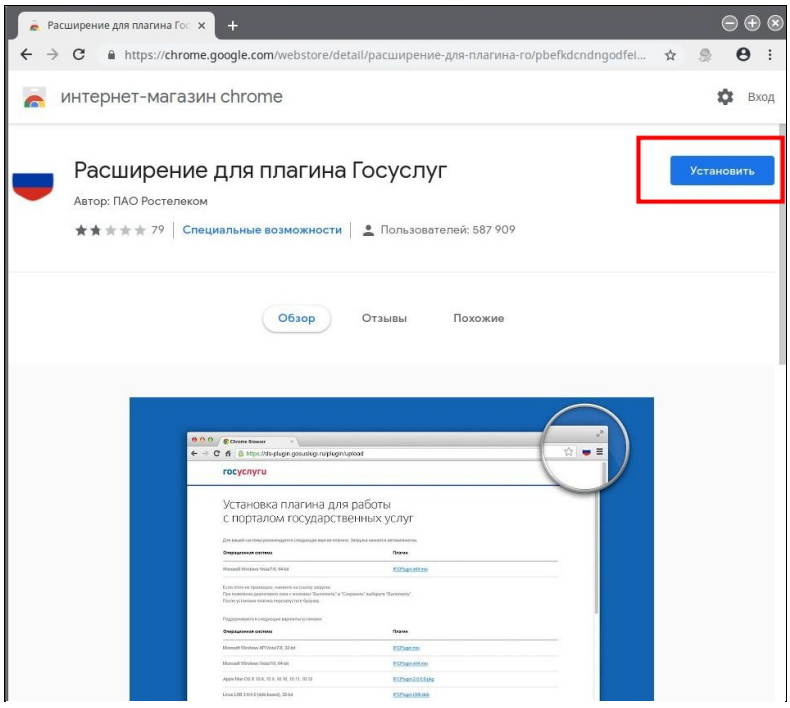
Установка расширения для плагина Госуслуг (ЕПГУ)

Выполните команду для установки расширений для браузера **Chromium** с правами администратора:

```
sudo dnf install ifcplugin-chromium
```

Установите расширение для плагина Госуслуг (ЕПГУ).

Перейдите по ссылке и нажмите кнопку «**Установить**».



Добавьте сайт https://esia.gosuslugi.ru в **Доверенные сайты** согласно Добавление сайта в список доверенных сайтов плагина.

Настройка Яндекс.Браузера

Установка Яндекс.Браузера

Для установки Яндекс.Браузера перейдите по ссылке.

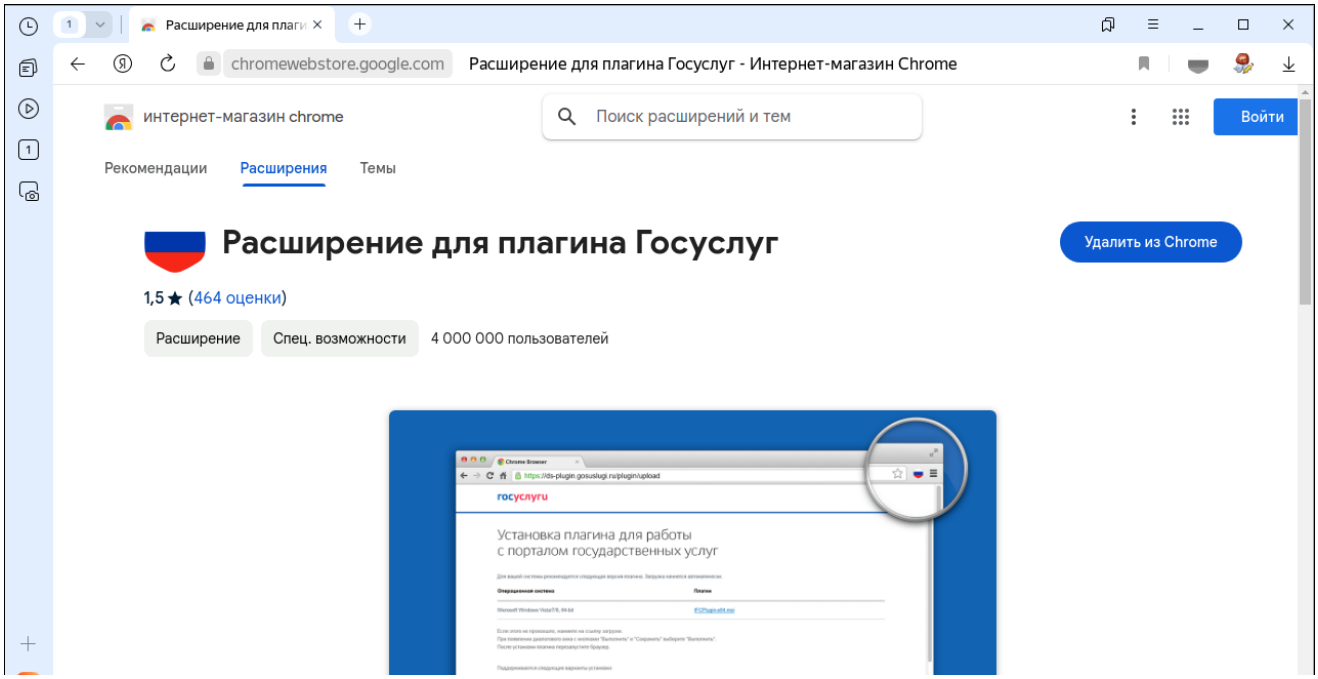
Установка расширения для плагина Госуслуг (ЕПГУ)

Выполните команду для установки расширений для браузеров **Chromium** и **Яндекс.Браузер** с правами администратора:

```
sudo dnf install ifcplugin-chromium
```

Установите расширение для плагина Госуслуг (ЕПГУ).

Перейдите по ссылке и нажмите кнопку «**Установить**».



Добавьте сайт https://esia.gosuslugi.ru в **Доверенные сайты** согласно Добавление сайта в список доверенных сайтов плагина.

Настройка браузера Firefox

Установка браузера Firefox

Для установки браузера Firefox перейдите по ссылке.

Установка расширения для плагина Госуслуг (ЕПГУ)

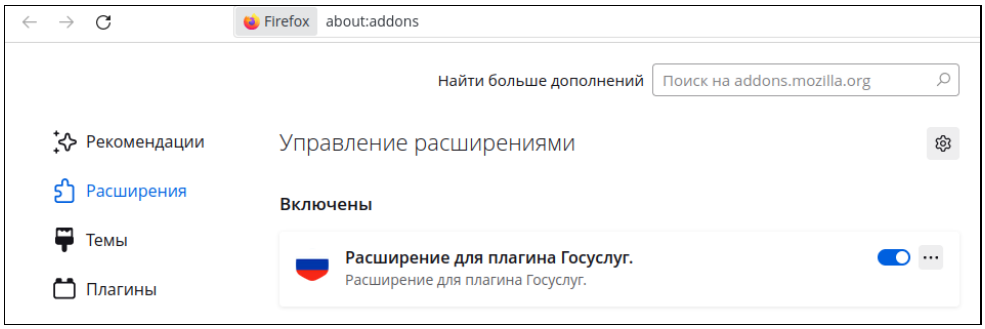
Выполните команду для установки расширений для браузера Firefox с правами администратора:

```
sudo dnf install ifcplugin-firefox
```

Установите расширение для плагина Госуслуг (ЕПГУ).

Для браузера **Firefox** необходимо вручную установить расширение для работы с Плагином Госуслуг. Для этого перейдите по ссылке и выберите удобный формат установки – через RPM-пакет или автоматически.

После установки расширение будет доступно в списке расширений браузера.



Добавьте сайт https://esia.gosuslugi.ru в **Доверенные сайты** согласно Добавление сайта в список доверенных сайтов плагина.

Установка КриптоПро «CryptoPro Extension for CAdES Browser Plug-in»

Пункты 1-3 данного раздела следует выполнять, только если у вас установлен КриптоПро CSP ниже версии 5.0.12500.

1. Скачайте плагин, перейдя по ссылке.

2. Распакуйте скачанный архив:

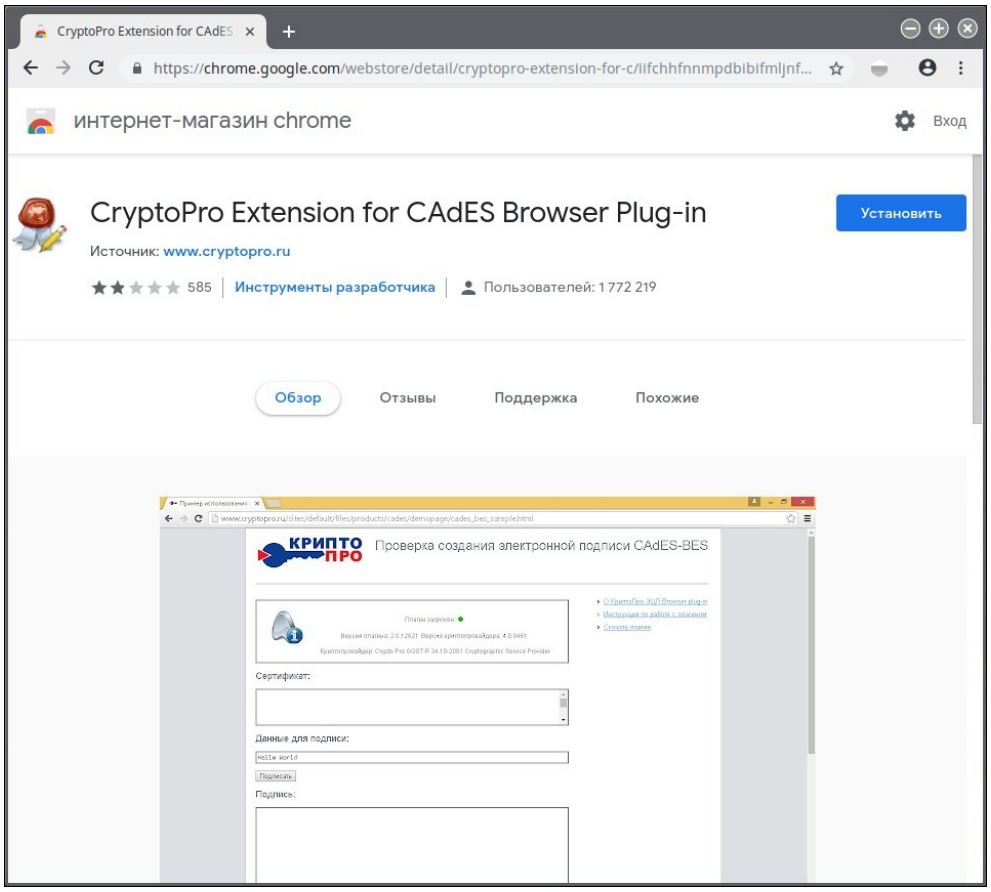
```
$ tar -xvf cades-linux-amd64.tar.gz
```

3. Перейдите в папку с распакованным архивом и установите следующие пакеты:

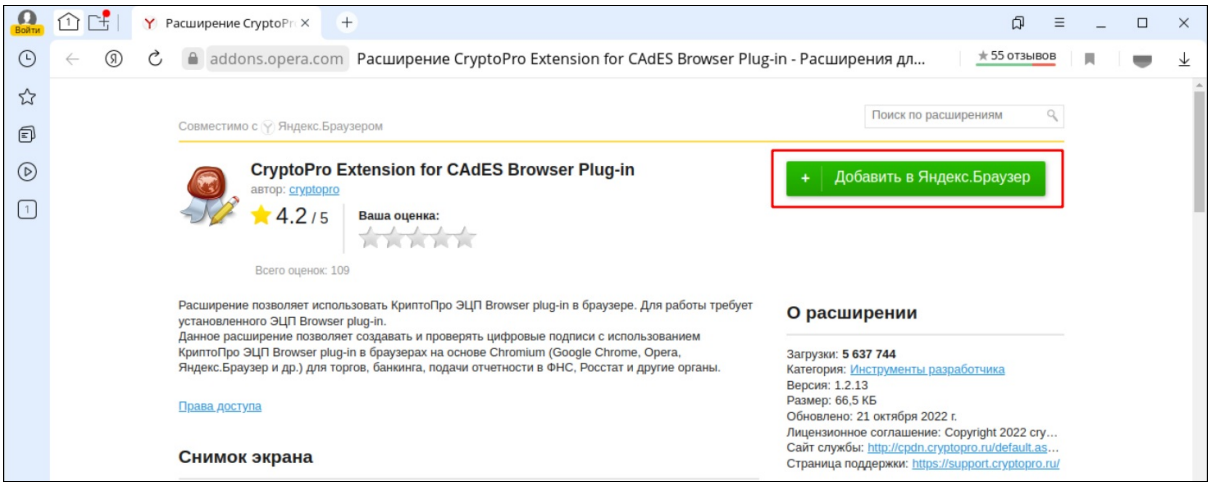
```
dnf install ./cprocsp-pki*rpm
```

4. Установите плагин **CryptoPro Extension for CAdES Browser Plug-in**:

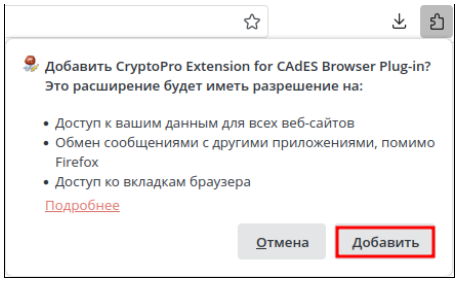
- для **Chromium** - перейдите по ссылке и нажмите кнопку «**Установить**»:



- для **Яндекс.Браузера** - перейдите по ссылке и нажмите кнопку «**Добавить в Яндекс.Браузер**»:



- для **Firefox**– скачайте расширение по ссылке и установите в браузер самостоятельно.



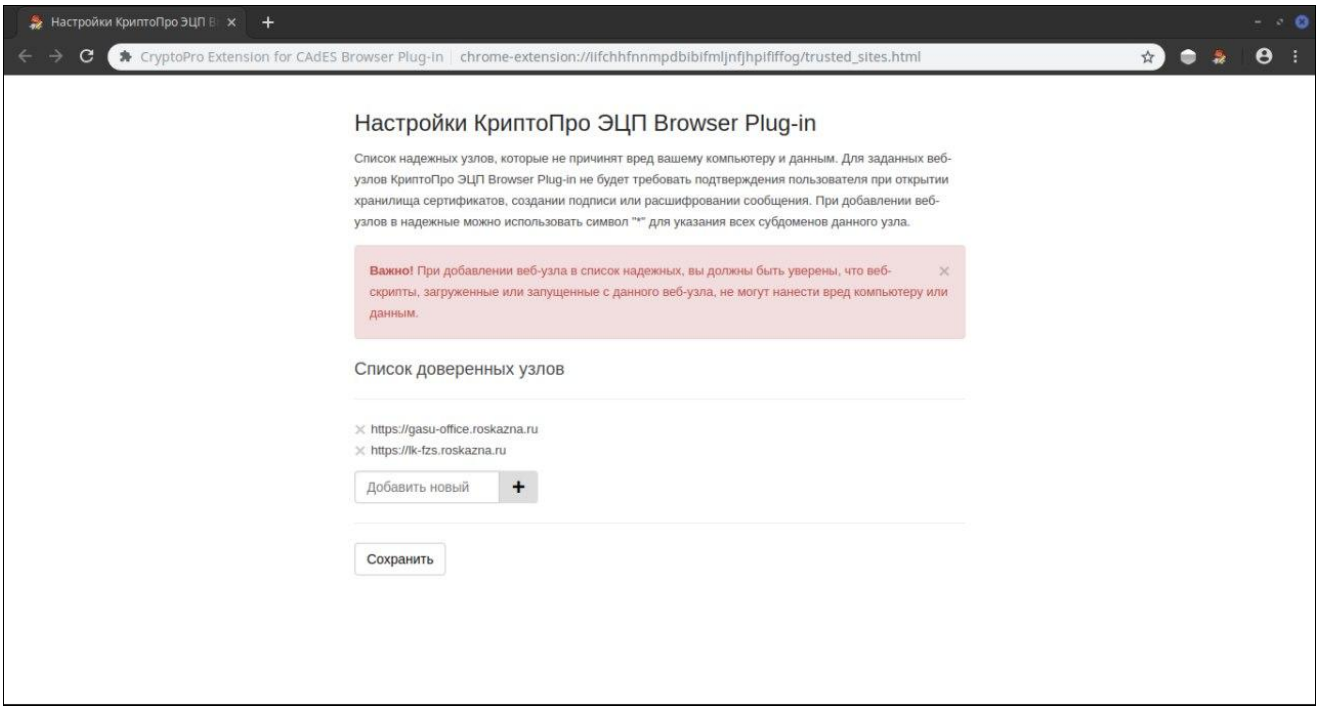
Проверить работу плагина можно по ссылке.

Добавление сайта в список доверенных сайтов плагина

Для добавления сайта откройте меню плагина и выберите пункт «**Настройка доверенных сайтов**».

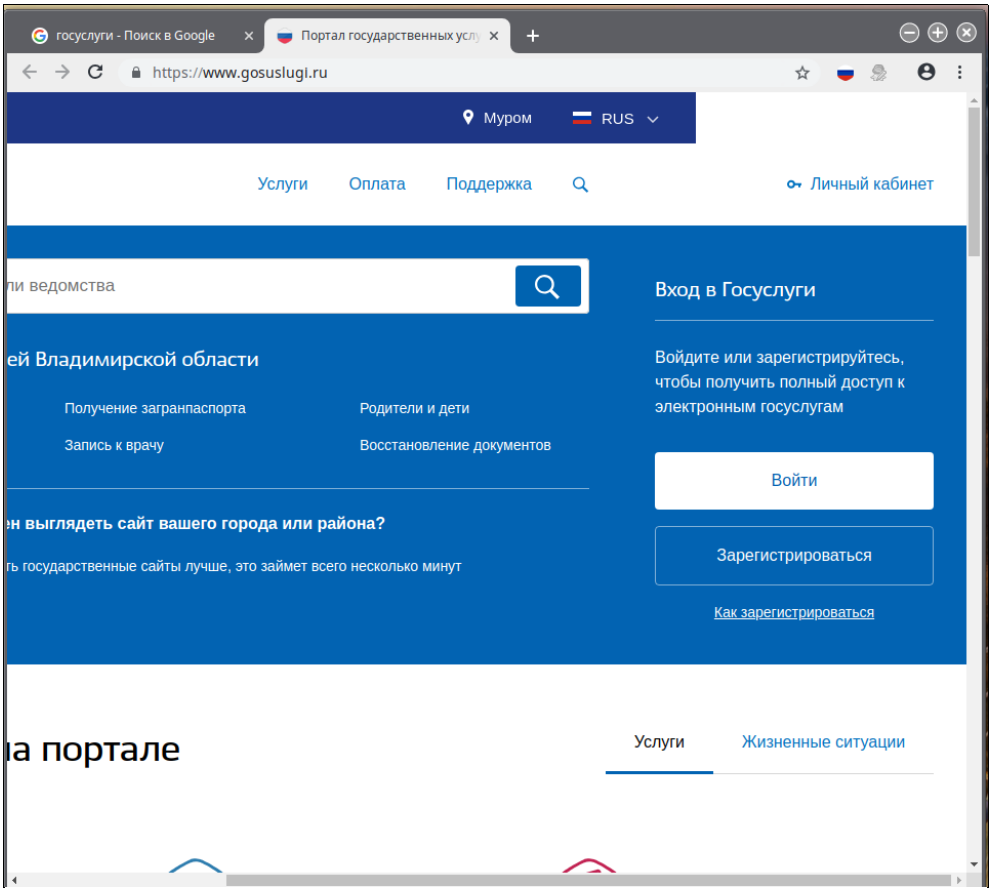


Далее откроется страница, на которой можно произвести добавление сайтов:

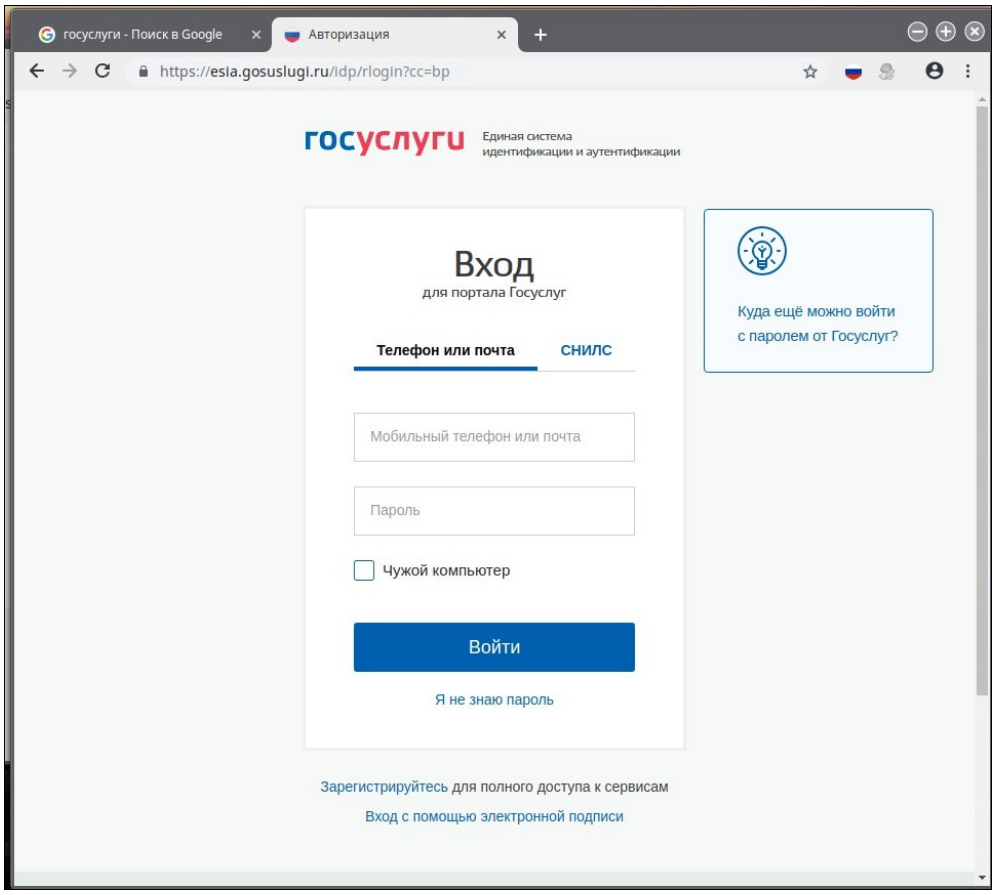


Вход на сайт Госуслуги

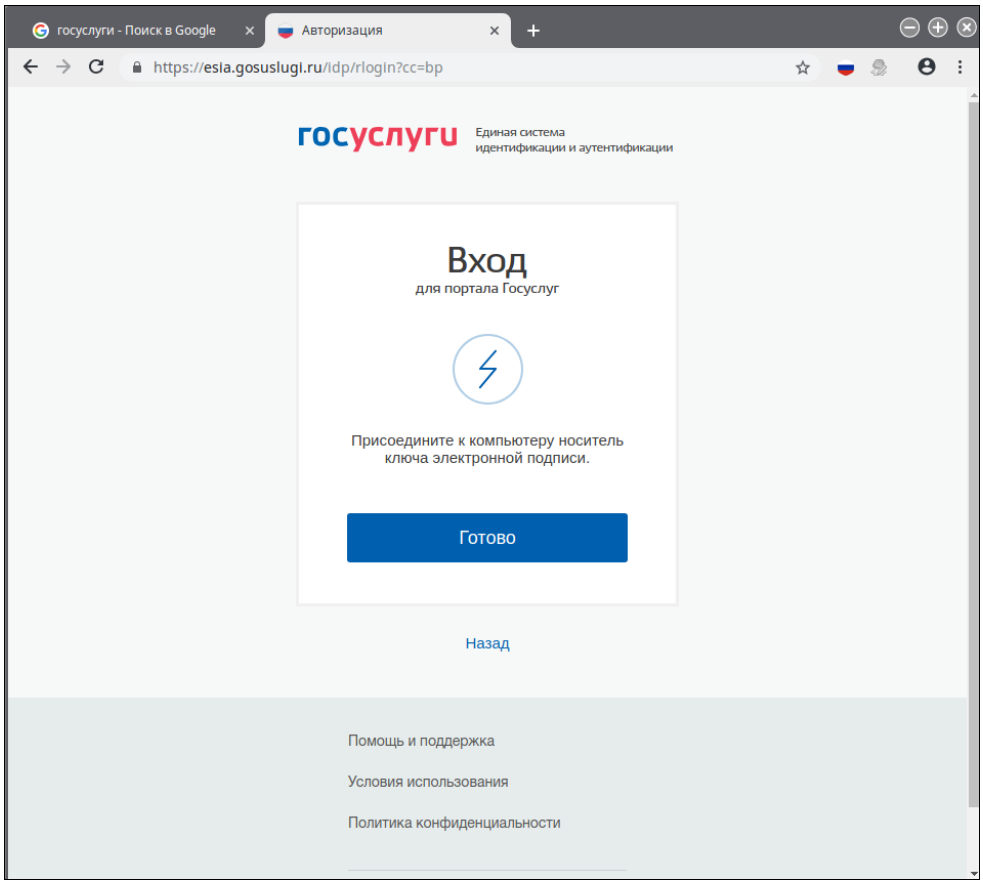
1. В браузере перейдите по ссылке и нажмите кнопку «**Вход**».



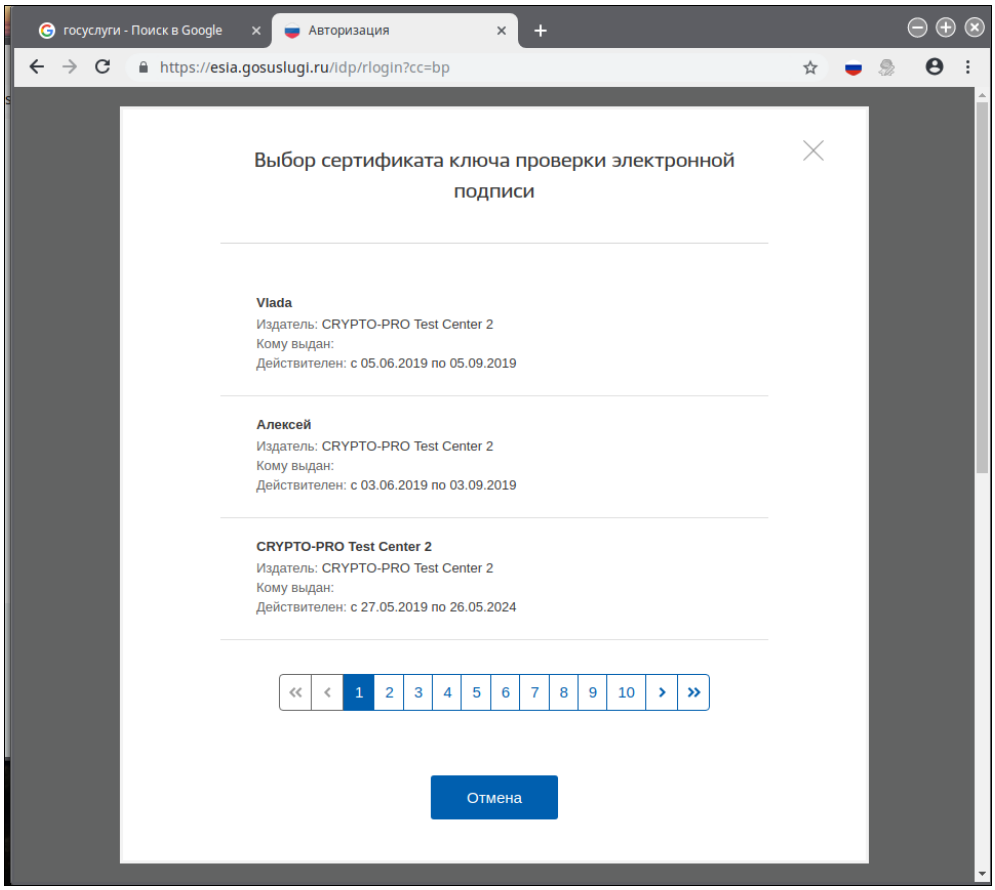
2. На открывшейся странице нажмите на «**Вход**» с помощью электронной подписи.



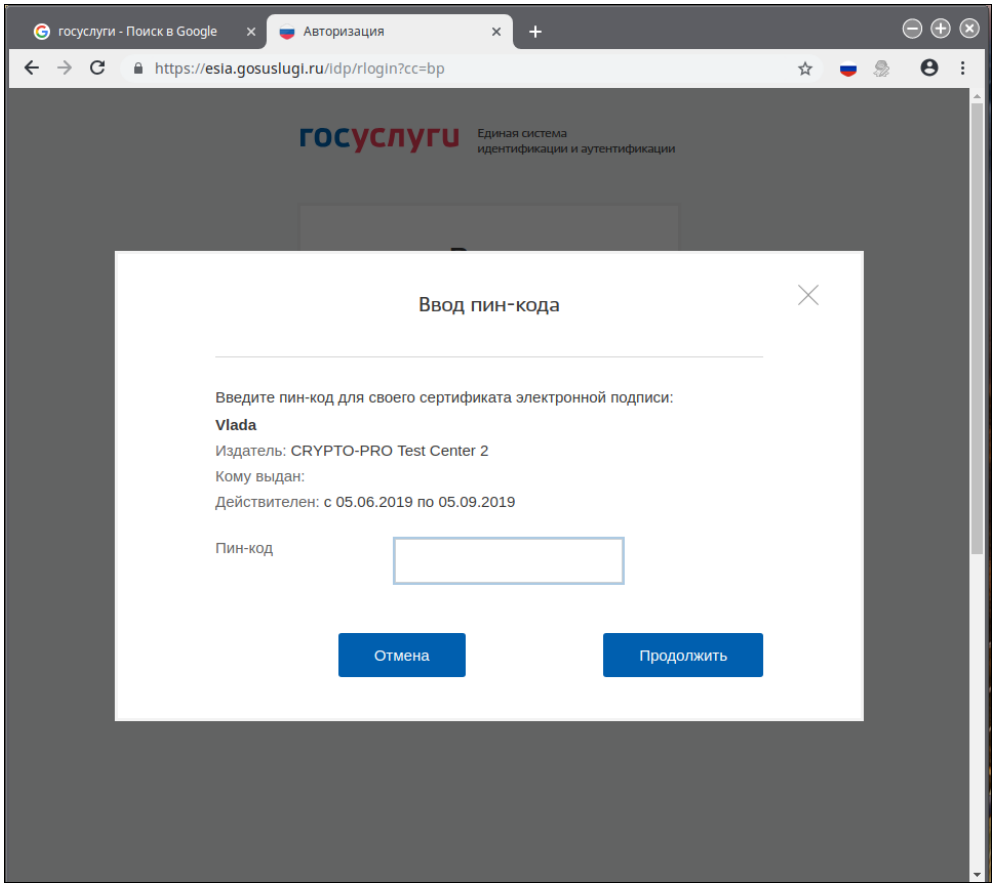
3. Подключите токен с ключом к компьютеру и нажмите кнопку «**Готово**».



4. Выберите сертификат ключа проверки электронной подписи, щёлкнув левой кнопкой мыши по строке с сертификатом.



5. Введите ПИН-код пользователя и нажмите кнопку «**Продолжить**».



ViPNet IDS HS Agent - система обнаружения вторжений

ViPNet IDS HS — программный комплекс, осуществляющий обнаружение сетевых атак и вторжений внутри хоста, изменения в реестре или в ключевых логах. В этой статье будет рассмотрена установка **linux-агента** и проверка его работоспособности.

Установка

1. Скачайте **rpm-пакет** и запустите установку:

   ```
   sudo dnf install vipnet-ids-hs-agent-1.4.1-2.rpm
   ```

2. Добавьте IP-адрес машины, на которой запущена серверная часть комплекса, в файл **/var/idshs/idshs_agent.conf**:

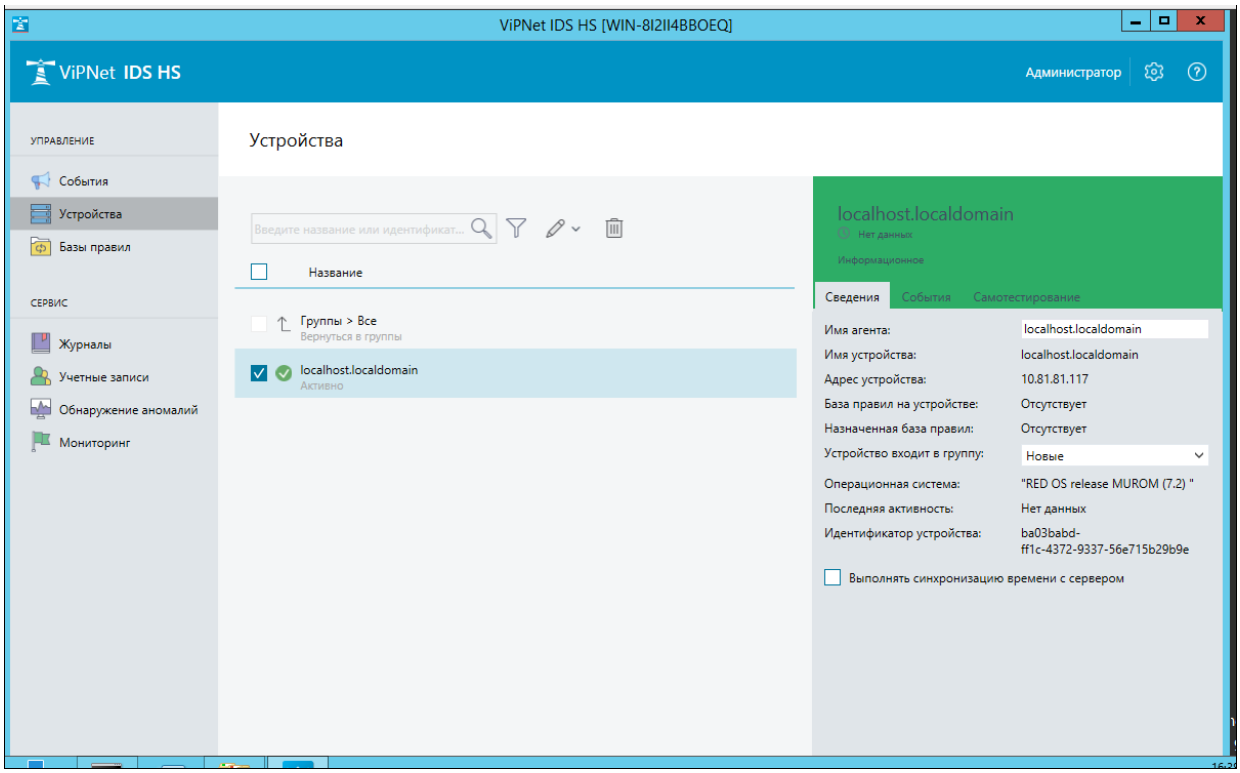
   ```
   sudo sh -c "echo 'server_address : <ip_адрес_сервера>' >> /var/idshs/idshs_agent.conf"
   ```

3. Перезагрузите компьютер.
4. Отправьте запрос на подключение серверу:

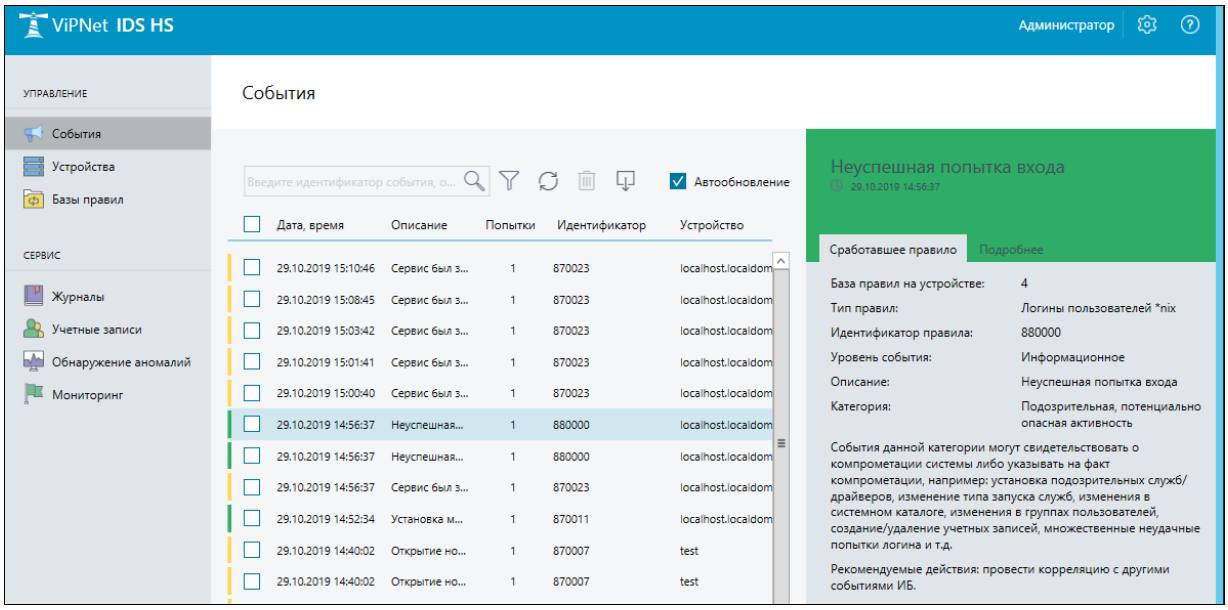
   ```
   idshs-agent <ip-адрес сервера>
   ```

Проверка работоспособности

Запустите приложение **ViPNet IDS HS** на сервере. Перейдите на вкладку **«Устройства»** и проверьте что машина, на которой был установлен агент, появилась в списке:



На вкладке **«События»** показаны отслеживаемые в реальном времени события информационной безопасности, которые были зафиксированы агентом:


ViPNet IDS HS
Администратор
УПРАВЛЕНИЕ
События
Устройства
Базы правил
СЕРВИС
Журналы
Учетные записи
Обнаружение аномалий
Мониторинг
События
Введите идентификатор события, о...
Автообновление
Дата, время
Описание
Попытки
Идентификатор
Устройство
29.10.2019 15:10:46 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:08:45 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:03:42 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:01:41 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:00:40 Сервис был з... 1 870023 localhost.localdom
29.10.2019 14:56:37 Неуспешная... 1 880000 localhost.localdom
29.10.2019 14:56:37 Неуспешная... 1 880000 localhost.localdom
29.10.2019 14:56:37 Сервис был з... 1 870023 localhost.localdom
29.10.2019 14:52:34 Установка м... 1 870011 localhost.localdom
29.10.2019 14:40:02 Открытие но... 1 870007 test
29.10.2019 14:40:02 Открытие но... 1 870007 test
Неуспешная попытка входа
29.10.2019 14:56:37
Сработавшее правило
Подробнее
База правил на устройстве: 4
Тип правил: Логины пользователей *nix
Идентификатор правила: 880000
Уровень события: Информационное
Описание: Неуспешная попытка входа
Категория: Подозрительная, потенциально опасная активность
События данной категории могут свидетельствовать о компрометации системы либо указывать на факт компрометации, например: установка подозрительных служб/драйверов, изменение типа запуска служб, изменения в системном каталоге, изменения в группах пользователей, создание/удаление учетных записей, множественные неудачные попытки логина и т.д.
Рекомендуемые действия: провести корреляцию с другими событиями ИБ.

ViPNet PKI Client - ПО для работы с электронной подписью

Установка программы
Работа с сертификатами
Генерация запроса на сертификат
Установка сертификата
Экспорт сертификатов

Окружение:

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** VipNet PKI Client - 1.6.0.1688, VipNet CSP - 4.4.0.11431

ViPNet PKI Client — проприетарное программное обеспечение разработанное компанией ИнфоТеКС для работы с электронной подписью и построении защищенных TLS-соединений.

Установка программы

Скачайте и распакуйте архив с пакетами для установки в домашний каталог от **локального пользователя** (в примере /home/user):

```
cd /home/user/
```

```
tar xvf pki_client_linux-x86_64-dist.tar.bz2
```

Поместите файл лицензии в распакованный каталог. Затем перейдите в каталог и запустите скрипт установки:

```
cd pki_client_linux/rpm
```

```
sudo ./install.sh
```

Дождитесь завершения процедуры установки.

Запустите VipNet PKI Client в **"Главное меню"** - **"Стандартные"** - **"Vipnet PKI Client".**

Работа с сертификатами

Генерация запроса на сертификат

Для генерации запроса на сертификат необходимо перейти в раздел **«Сертификаты»**, заполнить поля необходимой информацией и нажать кнопку **«Создать запрос»**. После этого, запрос будет передан в удостоверяющий центр.

Установка сертификата

Для добавления сертификата в локальное хранилище перейдите в раздел **«Сертификаты»**, выберите **«Добавить сертификат или CRL»** и укажите путь к файлу сертификата.

Экспорт сертификатов

Для экспорта сертификатов пользователей в файлы формата **X.509** сделайте следующее:

1. Выберите раздел **«Сертификаты»**;
2. Нажмите на кнопку напротив необходимого сертификата и выберите необходимый пункт;
3. В открывшемся окне выберите папку для сохранения файла.

Программный комплекс для защиты рабочих мест ViPNet Client

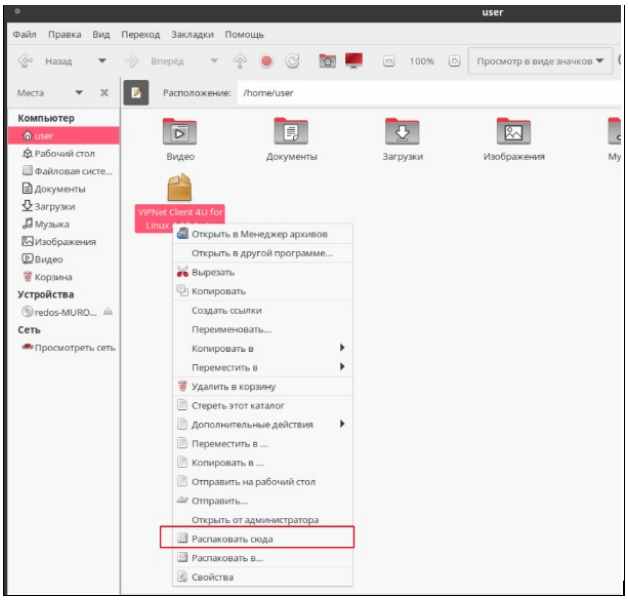
Окружение:

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** VipNet - 4.13.1-17762

Примечание.

Перед использованием VipNet Client необходимо установить ключи сетевого узла ViPNet. Дистрибутив ключей можно получить у администратора сети ViPNet в виде файла дистрибутива ключей (*.dst) и пароля к нему.

1. Скачайте архив с сайта разработчика https://infotecs.ru/product/vipnet-client-.html#soft
2. Распакуйте содержимое в корне домашней директории пользователя.
   Для этого необходимо в файловом менеджере Caja на архив с дистрибутивом **ViPNet Client 4U for Linux 4.13.1.zip** нажать правой кнопкой мыши и в выпадающем меню выбрать **“Распаковать сюда”**.



3. Установка программы:

3.1. Для установки **версии с графическим интерфейсом** выполните команду установки от пользователя **root**:

```
dnf install ‘/home/user/ViPNet Client 4U for Linux 4.13.1/SOFT/x86_64/GUI GOST/vipnetclient-gui_gost_ru_x86-64_4.13.1-17762.rpm’
```

Для запуска программы необходимо перейти в **“Главное Меню”** - **“Системные”** - **“VipNet Client”.**

3.2. Для установки **консольной версии программы** выполните команду от пользователя **root**:

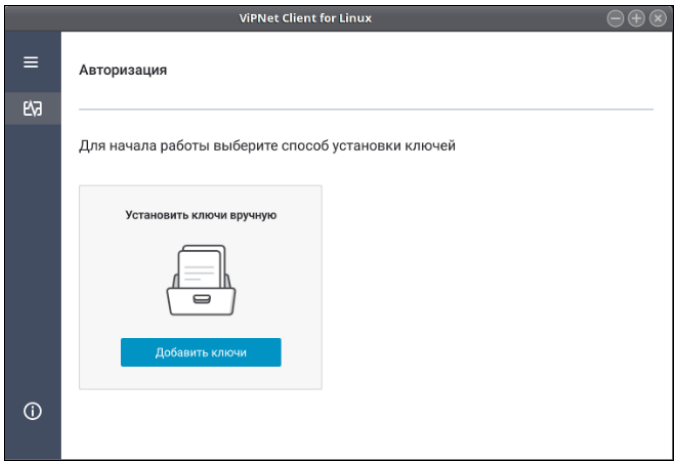
```
dnf install ‘/home/user/ViPNet Client 4U for Linux 4.13.1/SOFT/x86_64/CLI GOST/vipnetclient_gost_ru_x86-64_4.13.1-17762.rpm’
```

4. Установка ключей:

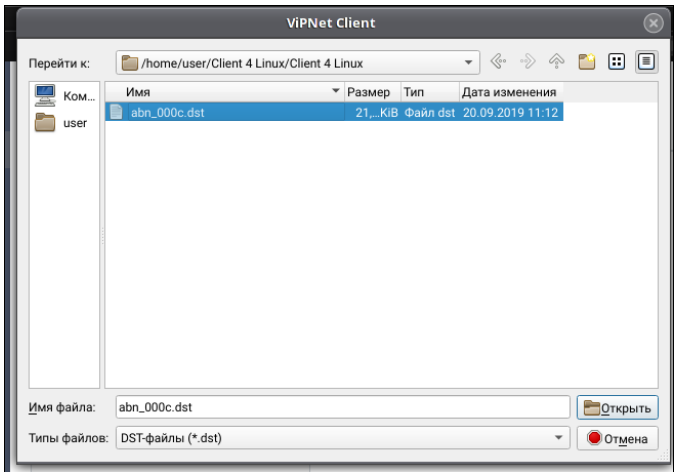
4.1. В графическом интерфейсе:

Запустите VipNet Client в **“Главное Меню”** - **“Системные”** - **“VipNet Client”.**

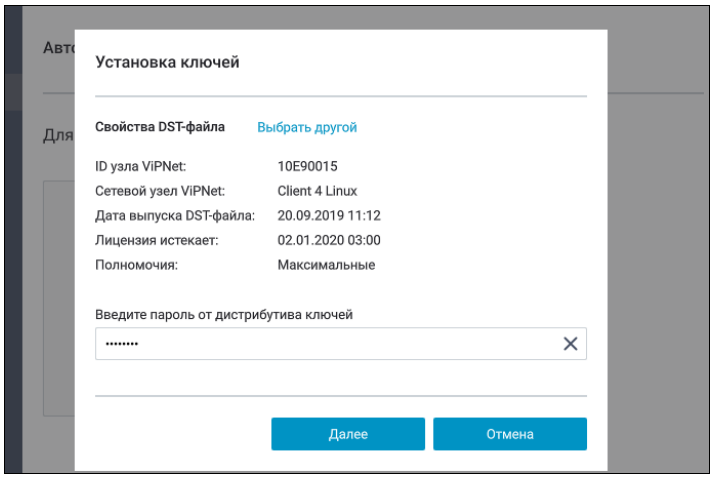
На вкладке **“Главная”** выберите **“Добавить ключи” .**



В открывшемся окне выберите файл дистрибутива ключей.



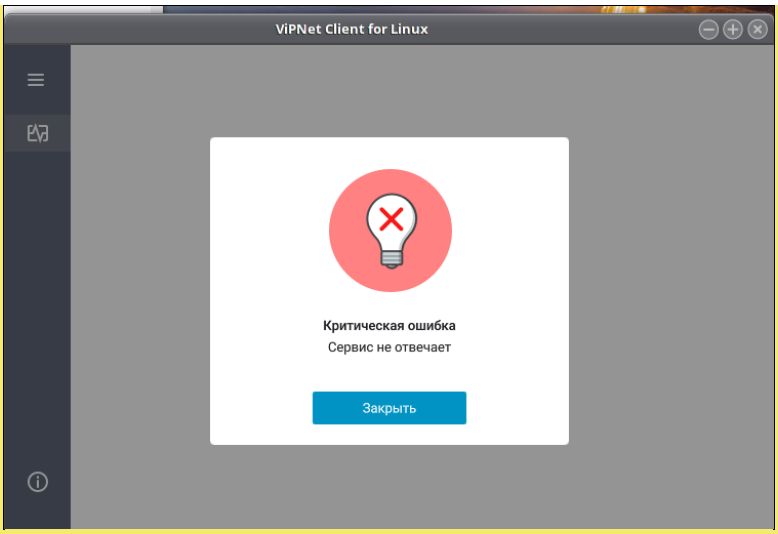
В окне **"Установка ключей"** введите пароль к дистрибутиву ключей и нажмите кнопку **"Далее"**.



4.2. В **консольной версии программы** установка ключей производится командой от **локального** пользователя:

```
vipnetclient installkeys <путь_к_дистрибутиву_ключей> --psw <пароль_к_дистрибутиву_ключей>
```

В **ViPNet Client** версии **4.6** проверка библиотек **Qt** занимает много времени и из-за этого может возникнуть представленная ниже ошибка.


ViPNet Client for Linux
Критическая ошибка
Сервис не отвечает
Закрыть

Криптопровайдер VipNet CSP

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VipNet CSP - 4.4

ВАЖНО!

Для работы графических утилит на РЕД ОС предварительно установите зависимости командой с правами **пользователя root:**

```
dnf install qt qt-common qt-settings qt-x11
```

Вы можете подробнее ознакомиться с примером установки и настройки криптопровайдера VipNet, просмотрев наши обучающие видео:

- на **RuTube** — Установка ViPNet CSP в РЕД ОС;
- в **Яндекс.Дзен** — Установка ViPNet CSP в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка VipNetCSP 4.4

Токены типа **Рутокен S** и **Рутокен Lite** исключены из поддержки с версии **ViPNet CSP 4.2.11**.

Скачайте архив и распакуйте его содержимое в корне домашней папки пользователя (с правами **локального** пользователя):

```
cd /home/<имя_пользователя>
```

```
unzip CSP_44_RedOS.zip
```

Перейдите в папку с установочным скриптом командой (с правами **локального** пользователя):

```
cd /home/<имя_пользователя>/CSP_44_RedOS/SOFT/scripts/
```

Предоставьте права на запуск файла в папке **scripts** командой (с правами **локального** пользователя):

```
chmod 777 vipnetcsp_pkg_manager.sh
```

Запустите скрипт установки командой:

```
./vipnetcsp_pkg_manager.sh install --package rpm --platform <архитектура_процессора> --profile <конфигурация_приложения> --dist /home/<имя_пользователя>/rpm/
```

Архитектура процессора:

- **x86_64** — для 64 или 32 битной версии РЕД ОС.
- **i686** — для версии РЕД ОС на архитектуре i686.

Чтобы посмотреть информацию об архитектуре процессора, введите команду:

```
uname -m
```

Конфигурация приложения:

- **vipnet_csp** - для установки приложения без графического интерфейса.
- **vipnet_csp_gui** - для установки приложения с графическим интерфейсом.
- **all** - то же, что и предыдущий параметр.

Пример команды:

```
./vipnetcsp_pkg_manager.sh install --package rpm --platform x86_64 --profile vipnet_csp_gui --dist
/home/user/CSP_44_RedOS/SOFT/LSB_x86/rpm
```

Или просто запустите скрипт установки с указанным путем до каталога с устанавливаемыми пакетами. Все остальные параметры определятся автоматически:

```
./vipnetcsp_pkg_manager.sh install --dist /home/<имя_пользователя>/CSP_44_RedOS/SOFT/LSB_x86/rpm/
```

После установки все исполняемые файлы приложения будут находится по пути **/opt/itcs/bin/**.

Для установки примеров использования функций в *Vipnet CSP* и заголовочных файлов, перейдите в папку **rpm**:

```
cd /home/user/CSP_44_RedOS/SOFT/LSB_x86/rpm
```

и установите пакет **itcs-csp-dev-4.4.0.732-1.noarch.rpm**.

```
dnf localinstall itcs-csp-dev-4.4.0.732-1.noarch.rpm
```

Примеры использования будут хранится по пути **/opt/itcs/share/samples**, а заголовочные файлы **/opt/itcs/include/**.

Для удаления приложения замените параметр **install** в установочном скрипте на **uninstall**.

```
./vipnetcsp_pkg_manager.sh uninstall
```

Для подробного разбора функций и примеров использования приложения, просмотрите официальную документацию по продукту на сайте infotecs.

СКЗИ Континент АП

Установка программного обеспечения
Работа с сертификатами
Создание запроса на сертификат
Регистрация сертификатов
Список доверенных серверов доступа
Настройка подключений
Создание нового профиля подключения
Подключение к серверу доступа
Автоматическое подключение к серверу доступа
Разрыв соединения с сервером доступа

СКЗИ Континет АП - специализированное программное обеспечения, предназначенное для установки на местах удаленных пользователей. **Абонентский пункт** (ап) отвечает за подключение к корпоративным ресурсам и обмен информацией в зашифрованном виде.

Установочный комплекс содержит 4 каталога:

1. **TS** — установочные пакеты ПО абонентского пункта;
2. **Sable** — ПО для поддержки совместной работы с ПАК «Соболь»;
3. **third_party** — стороннее ПО, необходимое для работы абонентского пункта;
4. **token_libs** — стороннее ПО, необходимое для работы с ключевыми носителями.

Установка программного обеспечения

1. Для установки стороннего ПО, необходимого для работы абонентского пункта, нужно установить пакеты, находящиеся в каталоге **third_party**. Для этого перейдите в каталог **third_party**, далее перейдите в подкаталог с номером версии используемой ОС и выполните команду:

```
sudo dnf localinstall *.rpm --disablerepo=*
```

2. Для установки стороннего ПО, необходимого для работы с ключевыми носителями, нужно установить пакеты, находящиеся в каталоге **token_libs**. Для этого перейдите в каталог **token_libs**, далее перейдите в подкаталог с номером версии используемой ОС и установите пакеты, содержащиеся в подкаталоге.

3. Если программное обеспечение абонентского пункта должно соответствовать среднему уровню безопасности, необходимо перейти в каталог **Sable/v.3.0/**, далее — в подкаталог с номером версии используемой операционной системы и установить пакет, содержащийся в подкаталоге.

4. Для установки абонентского пункта необходимо перейти в папку **TS**, далее в подкаталог с номером версии используемой операционной системы и установить пакет, соответствующий требуемому уровню безопасности.

Низкий уровень безопасности:

```
sudo dnf localinstall cts-3.7.6-70.ks1.redos7.1.x86_64.rpm --disablerepo=*
```

Средний уровень безопасности:

```
sudo dnf localinstall cts-3.7.6-70.ks2.redos7.1.x86_64.rpm --disablerepo=*
```

Для удаления программного обеспечение абонентского пункта выполните команду:

```
sudo dnf remove cts
```

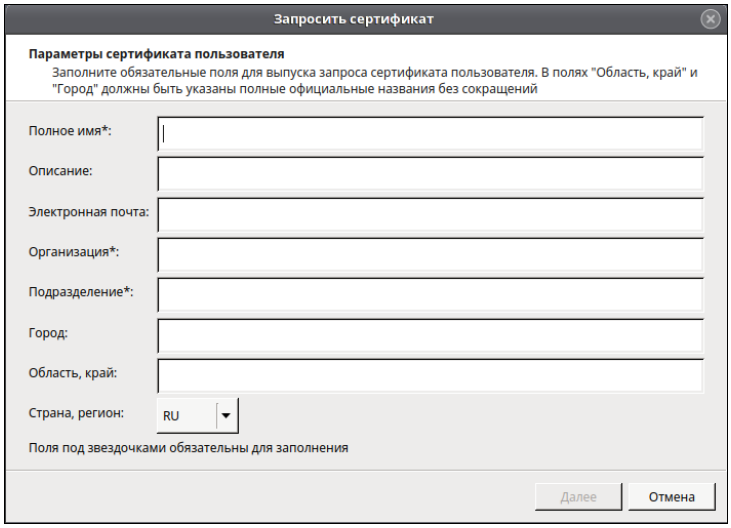
Для запуска абонентского пункта необходимо перезапустить службу **cts**. Для этого выполните команду:

```
sudo systemctl restart cts
```

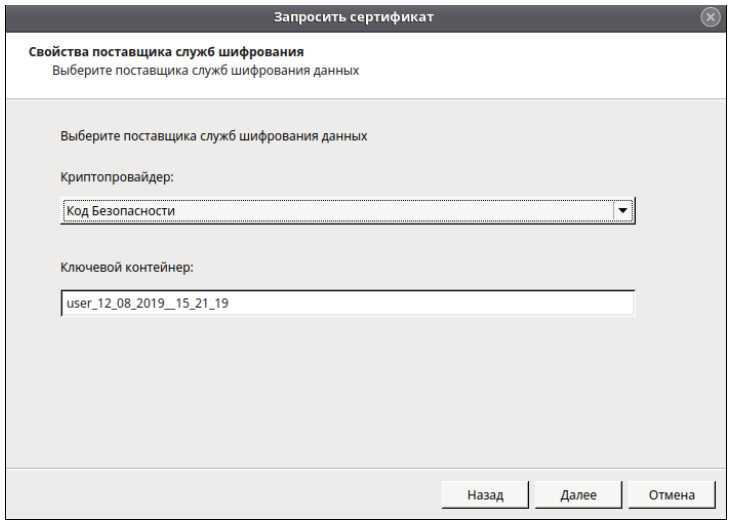
Работа с сертификатами

Создание запроса на сертификат

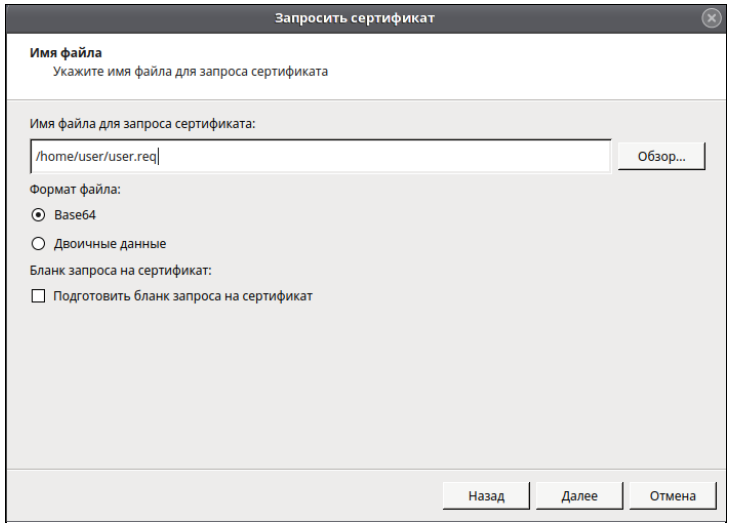
Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду **"Настройка → Запросить новый сертификат..."**.



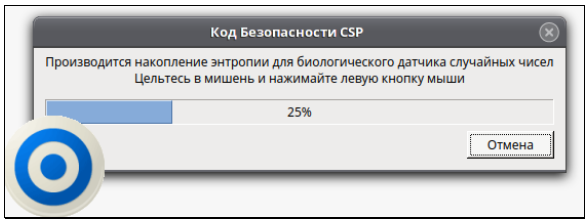
Заполните необходимые поля и нажмите кнопку **"Далее"**.



Выберите поставщика служб шифрования данных и, если необходимо, задайте имя ключевого контейнера и нажмите кнопку **"Далее"**.

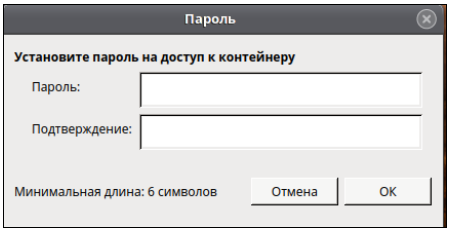


Укажите нужные сведения и нажмите кнопку **"Далее"**. На экране появится завершающее окно мастера запроса сертификата, содержащий введенные сведения. Проверьте указанные сведения и нажмите кнопку **"Готово"**. Если версия ПО абонентского пункта соответствует низкому уровню безопасности, на экране появится окно, предназначенное для накопления энтропии.

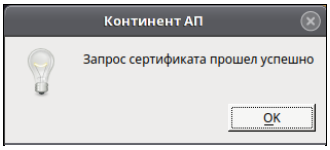


Если версия ПО абонентского пункта соответствует среднему уровню безопасности, на экране появится окно выбора ключевого носителя.

Выберите ключевой носитель и нажмите кнопку **"ОК"**. На экране появится окно задания пароля для доступа к ключевому контейнеру. Задайте пароль и нажмите кнопку **"ОК"**.



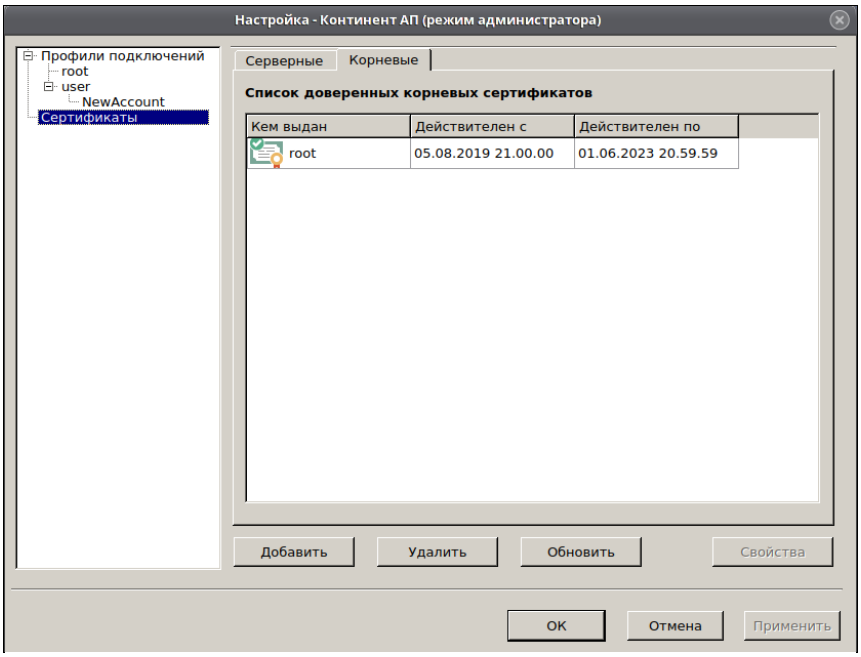
После на экране появится сообщение об успешном завершении создания запроса. Нажмите кнопку **"ОК"** в окне сообщения, извлеките ключевой носитель и передайте файл запроса администратору.



Регистрация сертификатов

На основании запроса, администратор сервера доступа создает и передает пользователю в виде файлов **user.cer**, **root.p7b** и **serv.cer** сертификат пользователя, корневой сертификат и серверный сертификат.

Регистрация корневого сертификата может быть выполнена пользователем в режиме администратора. Для этого необходимо войти в режим администратора и ввести пароль суперпользователя. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду **"Режим администратора → Параметры"**. Для входа в режим администратора введите пароль суперпользователя и на экране появится окно в соответствии с выбранным пунктом меню. Выберите в меню пункт **"Сертификаты"** и перейдите на вкладку **"Корневые"**. На вкладке отобразятся зарегистрированные корневые сертификаты.

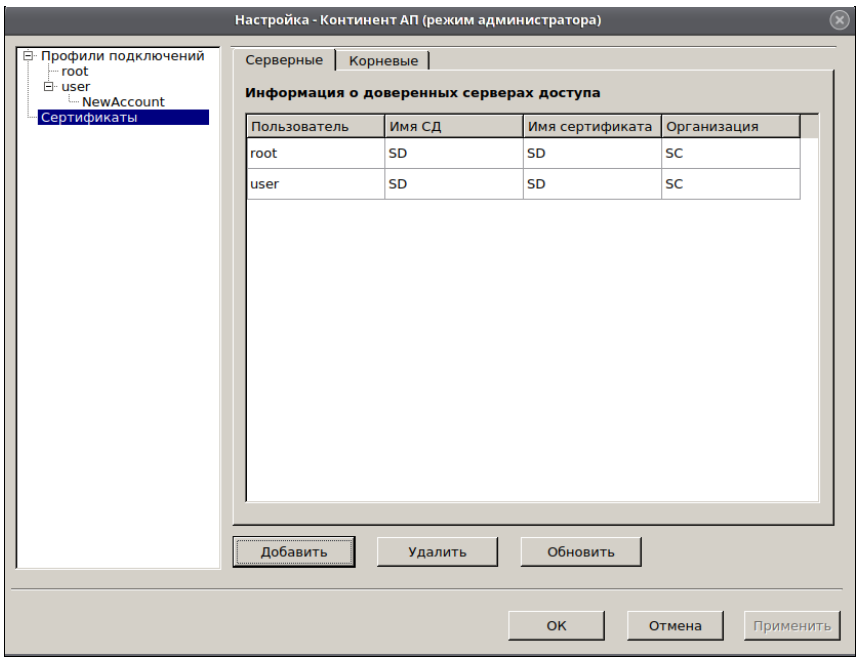


Для регистрации корневого сертификата нажмите кнопку **"Добавить"**. На экране появится окно для выбора файла. Откройте нужную папку, выберите файл сертификата и нажмите кнопку **"Открыть"**. Сертификат появится в списке.

Список доверенных серверов доступа

Для установления соединения сервер доступа, к которому осуществляется подключение, должен входить в **список доверенных серверов**.

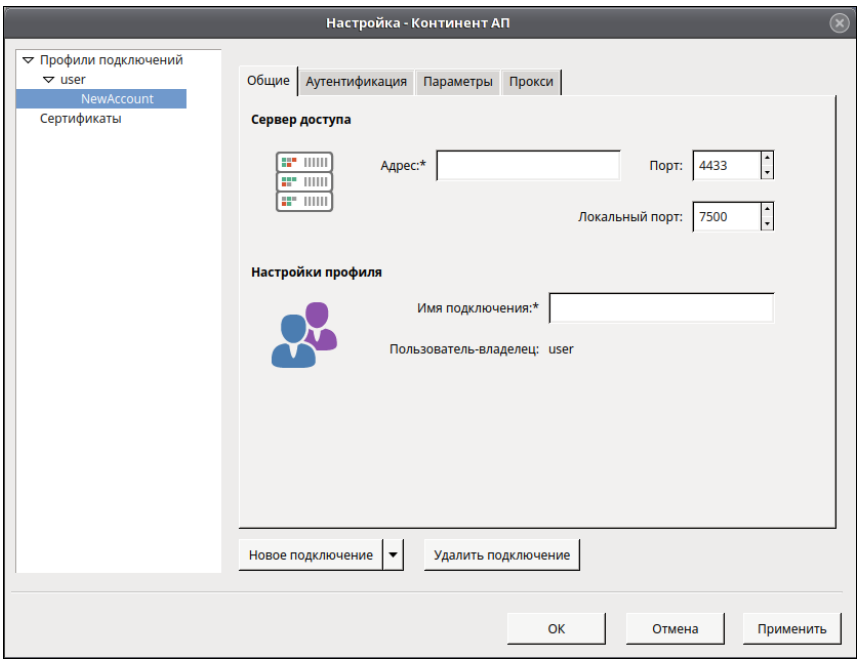
Откройте окно настроек абонентского пункта, выберите меню **"Сертификаты"** и перейдите на вкладку **"Серверные"**. Для регистрации серверного сертификата нажмите кнопку **"Добавить"**. На экране появится окно для выбора файла. Откройте нужную папку, выберите файл сертификата и нажмите кнопку **"Открыть"**.



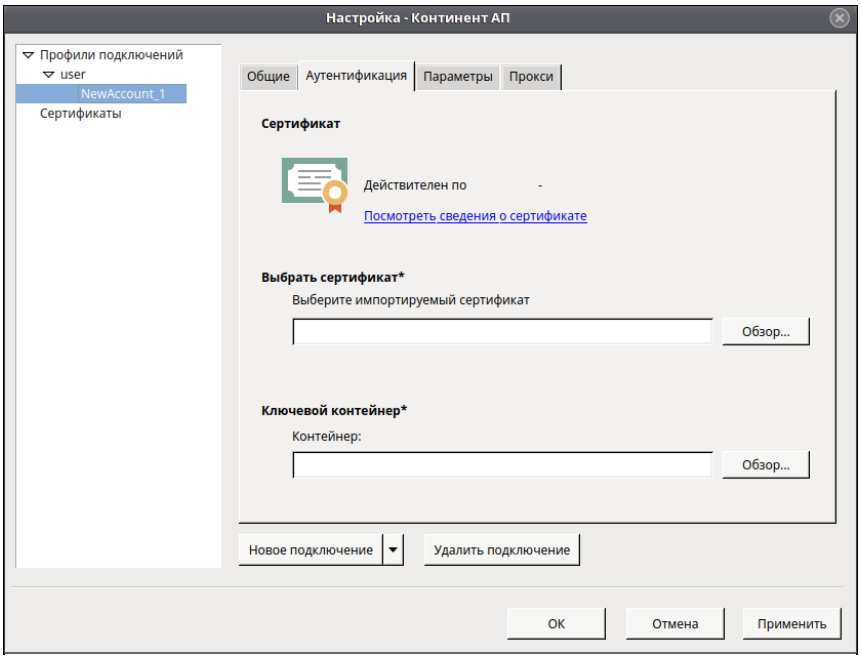
Настройка подключений

Создание нового профиля подключения

Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду **"Настройка → Параметры"**. На экране появится окно в соответствии с выбранным пунктом меню. В меню **"Профили"** подключений выберите нужного пользователя. В нижней части окна нажмите кнопку **"Новое подключение"**.



На вкладке **"Общие"** введите имя нового подключения, укажите нужные значения параметров и перейдите на вкладку **"Аутентификация"**.



Укажите сертификат пользователя и имя связанного с ним ключевого контейнера. Для этого используйте кнопку **"Обзор"**.

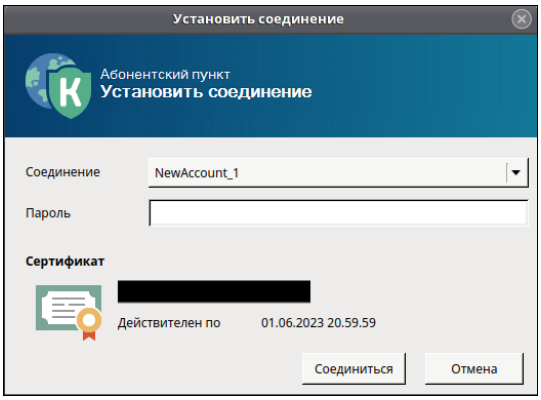
Перейдите на вкладку **"Параметры"**, проверьте значения, установленные по умолчанию, и при необходимости введите нужные значения.

При необходимости использовать **прокси-сервер** перейдите на вкладку **"Прокси"** и выполните настройку. **По умолчанию прокси-сервер не используется.**

Для сохранения установленных значений параметров нажмите кнопку **"Применить"**.

Подключение к серверу доступа

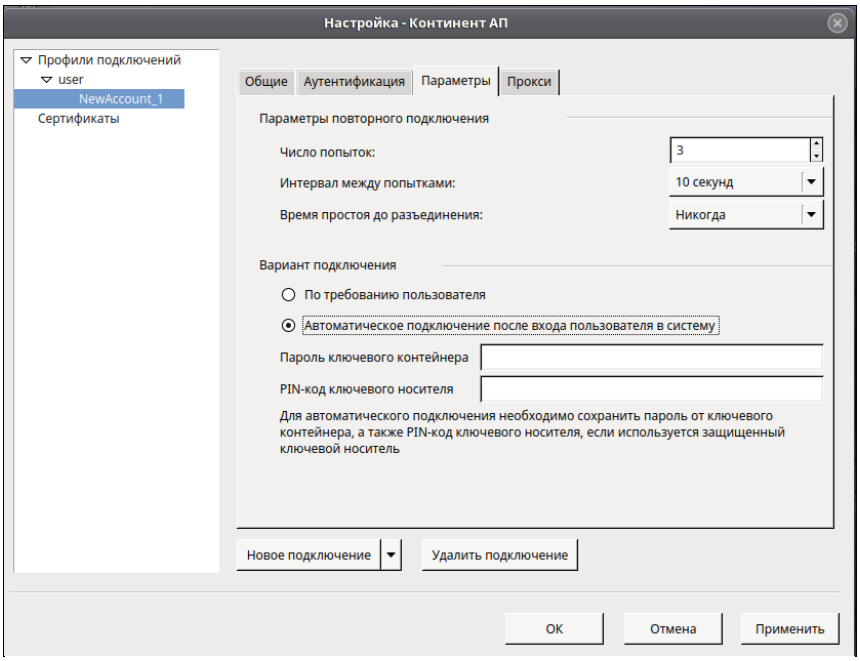
Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и выберите команду **"Подключить"**. На экране появится окно **"Установить соединение"**.



В поле **"Соединение"** укажите профиль подключения. Введите пароль доступа к ключевому контейнеру и нажмите кнопку **"Соединиться"**.

Автоматическое подключение к серверу доступа

Вызовите окно настроек абонентского пункта. Откройте меню **"Профили подключений"** и выберите в списке нужное подключение. Перейдите на вкладку **"Параметры"** и у параметра **"Вариант активации подключения"** установите значение **"Автоматическое подключение после входа пользователя в систему"**.



Введите пароль ключевого контейнера и **PIN-код** ключевого носителя и нажмите кнопку **"Применить"**.

Разрыв соединения с сервером доступа

Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач. В контекстном меню активируйте команду **"Разорвать. Соединение"** с сервером доступа будет разорвано. При этом пиктограмма абонентского пункта на панели задач примет вид **"Отключено"**.

Криптографический комплекс КАРМА

Установка КриптоПро CSP 5.0
Установка плагина CryptoPro Extension for CAdES Browser Plug-in
Установка личных и корневых сертификатов
Установка дополнительных пакетов
Установка КАРМА
Работа с программой

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** carma-56.2.435

Криптографический комплекс КАРМА — программное решение для использования криптографических функций, таких как шифрование, установка и проверка электронной цифровой подписи, в прикладных функциональных системах.

КАРМА позволяет применять в прикладном программном обеспечении криптографические методы защиты информации, используя высокоуровневый интерфейс, не требующий специальных знаний в области криптографии, учёта особенностей использования различных криптографических провайдеров и оперирования специальными криптографическими объектами, такими как ключевые контейнеры, хэш-функции и прочее.

Визуальная оболочка позволяет использовать *КАРМА* в качестве персонального АРМ для криптографической обработки файлов.

Установка КриптоПро CSP 5.0

Установка **КриптоПро CSP 5.0** выполняется согласно инструкции «Установка КриптоПро CSP 5.0».

Установка плагина «CryptoPro Extension for CAdES Browser Plug-in»

Установка **плагина КриптоПро** выполняется согласно инструкции «Установка КриптоПро «CryptoPro Extension for CAdES Browser Plug-in»».

Установка личных и корневых сертификатов

Установка *корневых и личных сертификатов* производится согласно инструкции «Графические утилиты для работы с КриптоПро CSP».

Установка дополнительных пакетов

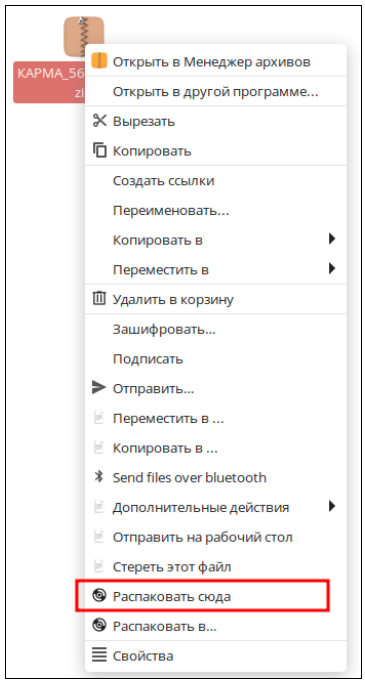
Для корректной установки криптографического комплекса *КАРМА* необходимо установить дополнительные пакеты. Для этого выполните команду (с правами администратора или суперпользователя системы):

```
dnf install libmicrohttpd libcurl tinyxml qt5-qtbase qt5-qtbase-gui
```

Установка КАРМА

Перейдите на официальный сайт разработчика и получите дистрибутив программы.

Затем перейдите в каталог с загруженным архивом, нажмите правой кнопкой мыши по архиву и выберите в контекстном меню «**Распаковать сюда**».



Далее перейдите в директорию с распакованными файлами и выполните команду установки:

```
cd /home/user/Загрузки/KAPMA_56.2.442-R5/Linux/
dnf install carma-common-56.2.442-redos73.x86_64.rpm carma-capilite-56.2.442-redos73.x86_64.rpm carma-dev-56.2.442-redos73.x86_64.rpm
```

По умолчанию КАРМА устанавливается в режиме пользовательского графического приложения. Для запуска криптографического модуля в графическом режиме откройте «**Главное меню**» — «**Прочие**» — «**Карма**».

Для запуска приложения в режиме демона (от *текущего* пользователя) необходимо указать ключ запуска:

```
/usr/local/carma/EosCryptoSvc -d
```

Для установки в виде **systemd**-сервиса необходимо выполнить скрипт **./carma.service_install.sh** из комплекта поставки, предварительно указав *имя пользователя* и *группу* в файле **./carma.service**:

```
[Service]
...
User=user
Group=user
```

Примечание.

Перед повторной регистрацией сервиса и установкой под *другим* пользователем необходимо выполнить скрипт **uninstall_daemon.sh**.

На этом установка и предварительная настройка сервиса *КАРМА* завершена.

Работа с программой

Для проверки работоспособности в терминале выполните команду `curl http://localhost:8080`. Если настройка выполнена верно, вывод команды будет иметь следующий вид:

```
{
  "appName": "eoscryptosvc",
  "carmaVersion": "56.2.442",
  "defaultModule": "",
  "systemTime": "23.10.2024 11:21:18",
  "systemInfo": "Linux"
```

```
}
```

Проверку работоспособности также можно выполнить в браузере. Для этого в адресной строке введите http://localhost:8080.



Также в браузере будут доступны следующие предопределенные страницы:

- localhost:8080 — страница доступа к веб-сервису;
- localhost:8080/test — страница тестирования функций сервиса;
- http://localhost:8080/settings — страница редактирования настроек сервиса.

Установка Kaspersky Endpoint Security

Установка «Kaspersky Endpoint Security 11.3 и новее для Linux»
Установка агента антивируса «Kaspersky Endpoint Security 11 для Linux»
Установка графической составляющей для «Kaspersky Endpoint Security 11.3 и новее для Linux»
Запуск и остановка Kaspersky
Дополнительные настройки

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: Kaspersky Endpoint Security 11 для Linux - 11.3.0.7441

Вы можете подробнее ознакомиться с установкой и настройкой **Kaspersky**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Kaspersky Endpoint Security;
- в **Яндекс.Дзен** — Установка Kaspersky Endpoint Security;
- в **VK Видео** — Установка Kaspersky Endpoint Security.

На наших каналах вы также сможете найти много другой полезной информации.

Установка «Kaspersky Endpoint Security 11.3 и новее для Linux»

Откройте в браузере страницу для скачивания установочных файлов «**Kaspersky Endpoint Security 11 для Linux**».

Скачайте установочный файл дистрибутива **RPM** (x64) kesl-11.3.0-7441.x86_64.rpm.

Перейдите в каталог с загруженным файлом дистрибутива (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
```

Далее в терминале выполните следующие команды (потребуются права администратора):

```
sudo -E dnf install kesl-11.3.0-7441.x86_64.rpm perl-Getopt-Long perl-File-Copy
```

Запустите скрипт настройки **Kaspersky Endpoint Security**:

```
sudo -E /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Выберите локаль (параметры региона) для антивируса (для использования системной локали нажмите **Enter**):

```
Setting up the Anti-Virus Service default locale
List of available locales:
- ru_RU.UTF-8
- de_DE.UTF-8
- en_US.UTF-8
- fr_FR.UTF-8
- ja_JP.UTF-8
- zh_CN.UTF-8
[ru_RU.UTF-8]:
```

Для ознакомления с пользовательским соглашением нажмите **Enter**. После этого введите «**y**»:

```
Accepting the End User License Agreement (EULA) and Privacy Policy
Press ENTER to display the EULA and Privacy Policy:
I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement [y/n]: y
```

Введите «**y**» для согласия с политикой конфиденциальности:

```
I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy [y/n]: y
```

Для соглашения с положением о **Kaspersky Security Network** введите «**y**»:

```
Configuring KSN
I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement (KSN Statement is available here: '/opt/kaspersky/kesl/doc/ksn_license.ru') [y/n]: y
```

Введите имя пользователя, которому будут предоставлены права администратора для антивируса:

```
Granting the Administrator role
Only users with the Administrator role have full access to Kaspersky Endpoint Security management by command line and GUI.
Specify user to grant the 'admin' role to (leave empty to skip): user
```

Настройка SELinux – введите «**y**»:

```
SELinux configuration
Do you want to configure SELinux automatically? [y]: y
```

Введите адрес сервера для загрузки обновлений (нажмите **Enter** для использования серверов Лаборатории Касперского по умолчанию):

```
Configuring the update source
Specify the update source. Possible values: KLServers|SCServer|<url>:[KLServers]:
```

При необходимости, введите данные для использования прокси сервера. Для пропуска настройки нажмите **Enter**:

```
If you use an HTTP proxy server to access the Internet, please enter the address in one of the following formats: proxyIP:port or user:pass@proxyIP:port, or enter 'no' [n]: n
```

Для загрузки актуальной базы данных антивируса нажмите **Enter**:

```
Do you want to download the latest databases now? [y]:
```

Для активации запланированных обновлений нажмите **Enter** (по умолчанию проверка обновлений будет выполняться каждый час):

```
Do you want to enable scheduled updates? [y]:
Scheduled updates are enabled.
The application databases are scheduled to be updated hourly.
```

Введите ключ активации либо нажмите **Enter** для использования пробного ключа на 30 дней:

```
Activate the application
You must activate the application to use it.
To activate the application now, enter the path to your key file or an activation code. Enter an empty string to add the built-in trial key:
Adding the built-in trial key has completed successfully.
```

Проверьте статус задач:

```
sudo -E kesl-control --get-task-list
```

Запустите следующие задачи:

- Защита от файловых угроз:

```
sudo kesl-control --start-task 1 -W
```

- Проверка загрузочных секторов:

```
sudo kesl-control --start-task 4 -W
```

Рекомендуется запустить все задачи, которые будут применяться при использовании **Kaspersky Endpoint Security**.

Убедитесь, что в файле **audit.log** нет ошибок:

```
sudo -E grep kesl /var/log/audit/audit.log
```

Установка агента антивируса «Kaspersky Endpoint Security 11 для Linux»

На данной странице можно скачать «**Агент администрирования**» - файл RPM (x64) klnagent64-14.0.0-4646.x86_64.rpm. Для установки перейдите в каталог со скачанным файлом дистрибутива и выполните следующие команды (потребуются права администратора системы или суперпользователя **root**):

```
cd /home/user/Загрузки
dnf install klnagent64-14.0.0-4646.x86_64.rpm
/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

Ф а й л **/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl** содержит параметры настроек агента администрирования, при необходимости их можно отредактировать.

После запуска установщика(**postinstall.pl**), вам будет предложено ознакомится с лицензионным соглашением. После прочтения, закройте его, нажав на клавишу **"q"**, и подтвердите принятие условий соглашения клавишей **"y".**

Далее установщик Касперского выполнит интерактивную установку **Агента администрирования**.

Потребуется указать DNS-имя или IP-адрес сервера:

```
Please enter Administration Server DNS-name or static IP-address:
```

Далее необходимо задать порты сервера и ssl:

```
Please enter Administration Server port number [14000]:
Please enter Administration Server ssl port number [13000]:
```

При необходимости можно согласиться с использованием ssl-шифрования:

```
Please enter 'Y' to confirm that you want to use SSL encryption or enter 'N' to use non-encrypted communication [Y]:
```

Затем выберите тип конфигурирования:

```
The Network Agent being installed can be used as connection gateway. It will allow you to connect to Administration Server using the specified connection gateway.
1) Do not configure connection gateway
2) Do not use connection gateway
3) Connect to server using connection gateway
4) Use as connection gateway
Please choose connection gateway mode: [1]:
```

На этом установка **Агента администрирования** завершена.

Установка графической составляющей для «Kaspersky Endpoint Security версии 11.3 и новее для Linux»

Откройте в браузере страницу для скачивания установочных файлов «**Kaspersky Endpoint Security 11 для Linux**».

Установка графической составляющей KESL производится через **rpm**-пакет. Скачайте установочный файл дистрибутива **RPM** (x64) kesl-gui-11.3.0-7441.x86_64.rpm.

Перейдите в каталог с загруженным файлом дистрибутива.

В терминале выполните следующую команду:

```
sudo dnf install kesl-gui-11.3.0-7441.x86_64.rpm
```

Выполните перезагрузку ПК, чтобы завершить настройку.

Запуск антивируса будет доступен из «**Главного меню**» – «**Системные**» – «**Kaspersky Endpoint Security 11.3.0 для Linux**».

Запуск и остановка Kaspersky Endpoint Security

Чтобы остановить **Kaspersky Endpoint Security** в systemd-системе, выполните следующую команду:

```
systemctl stop kesl
```

Чтобы перезапустить **Kaspersky Endpoint Security** в systemd-системе, выполните следующую команду:

```
systemctl restart kesl
```

Чтобы вывести статус **Kaspersky Endpoint Security** в systemd-системе, выполните следующую команду:

```
systemctl status kesl
```

Дополнительные настройки

Если Вы по каким-либо причинам пропустили пункт настройки прав администратора для пользователя (**Specify user to grant the 'admin' role to (leave empty to skip)**), то права администратора можно назначить с помощью команды в терминале:

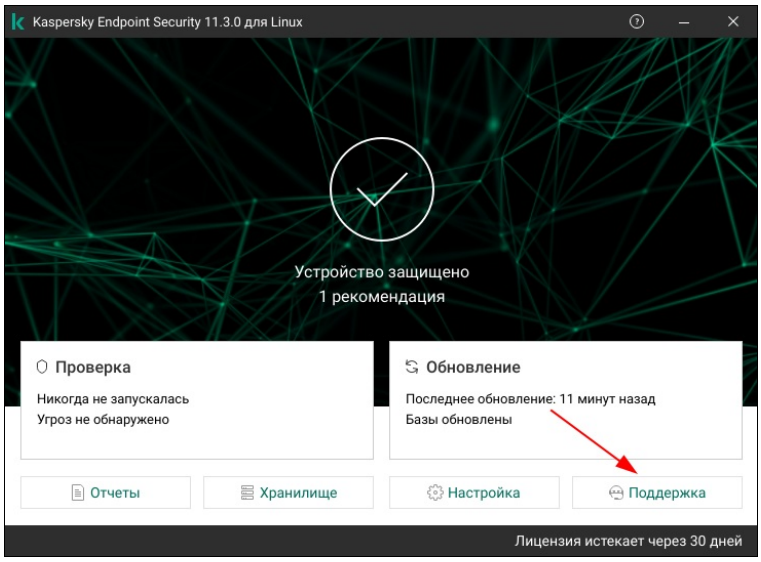
```
sudo -E kesl-control --grant-role admin user
```

где **user** - имя пользователя.

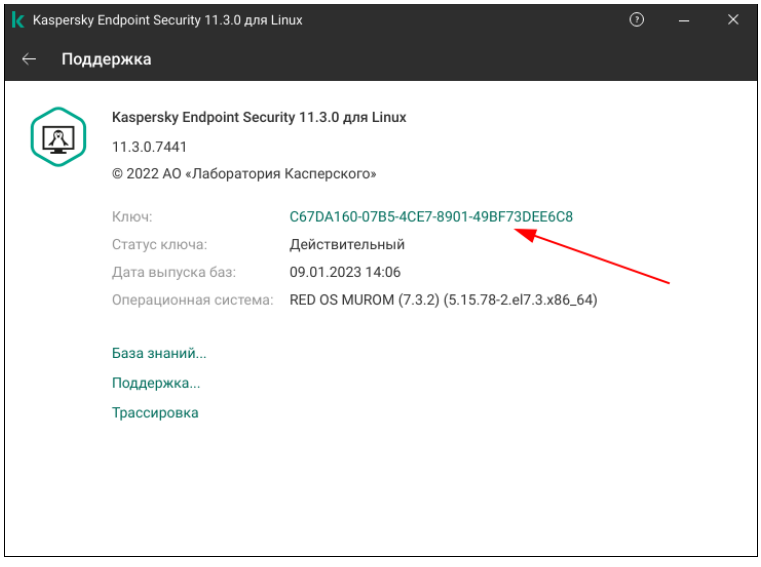
Если был пропущен этап ввода ключа активации, можно выполнить команду в терминале:

```
sudo -E kesl-control --add-active-key <код_активации_или_файл_ключа>
```

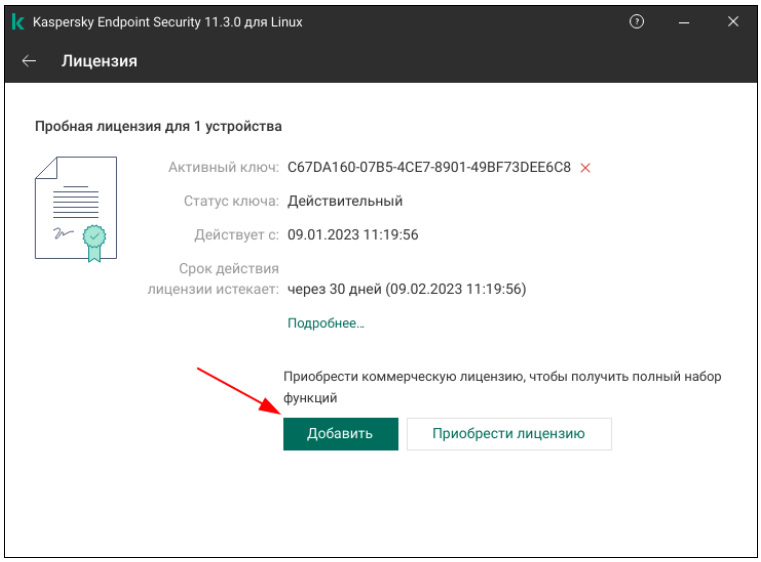
Также ввод активации ключа доступен в графическом интерфейсе. Для этого нажмите на кнопку «**Поддержка**».



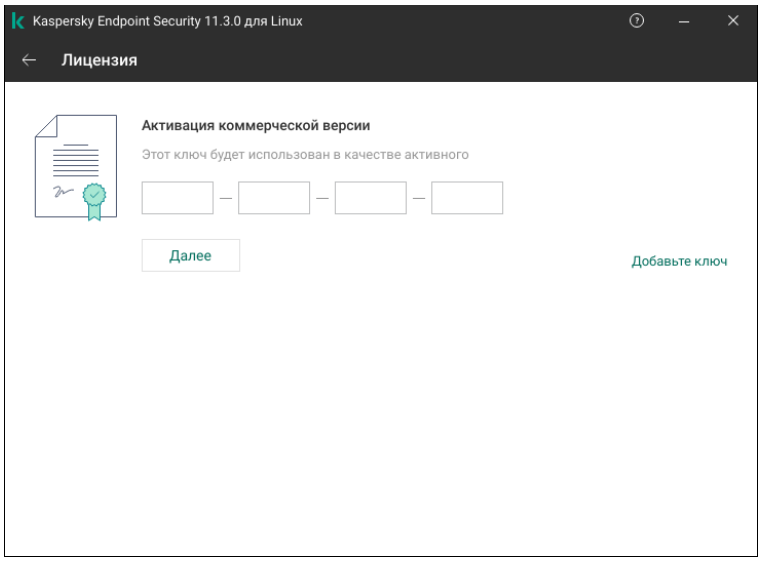
Затем кликните ЛКМ на временный (30-дневный) ключ.



Будет открыто окно, в котором необходимо нажать на кнопку «**Добавить**».



Введите ключ лицензии или укажите файл ключа.



Установка Kaspersky Security Center

Установка и настройка СУБД
Установка и настройка KSC
Установка и настройка WebConsole

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: ksc64-14.2.0-23324, ksc-web-console-14.2.10359, mariadb-3:10.10.2-2

Вы можете подробнее ознакомиться с настройкой и работой **Kaspersky**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Kaspersky Security Center и WebConsole в РЕД ОС ;
- в **Яндекс.Дзен** — Установка Kaspersky Security Center и WebConsole в РЕД ОС ;
- в **VK Видео** — Установка Kaspersky Security Center и WebConsole в РЕД ОС .

На наших каналах вы также сможете найти много другой полезной информации.

Установка и настройка СУБД

1. Выполните установку **MariaDB**:

```
dnf install mariadb-server mariadb
```

2. Запустите службу и добавьте ее в автозагрузку:

```
systemctl enable mariadb --now
```

Проверьте статус службы:

```
systemctl status mariadb
```

В статусе должно отображаться **active (running)**.

3. Выполните сценарий установки БД:

```
/usr/bin/mysql_secure_installation
```

Данный сценарий подробно описывает каждый шаг. Сначала он запросит пароль пользователя **root**, но т. к. после начальной установки он не задан, нажмите **Enter** и на следующем этапе задайте свой пароль.

В процессе выполнения сценария можно нажимать **Enter**. В результате будут удалены анонимные пользователи, удаленный root-логин, тестовые таблицы, а также будут перезагружены привилегии.

4. Далее необходимо настроить конфигурационный файл **/etc/my.cnf**, включив поддержку **InnoDB** и хранилища **MEMORY**, а также кодировок **UTF-8** и **UCS-2**.

```
nano /etc/my.cnf
```

Пример содержимого файла:

```
[client-server]
 port = 3306
 socket = /var/run/mysqld/mysqld.sock
 [mysqld]
 basedir=/usr
 tmpdir=/tmp
 port=3306
 bind-address=0.0.0.0
```

```
local-infile=0
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
symbolic-links=0
sql_mode = ""
log-error = /var/log/mysql-error.log
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=2048M #укажите свой объем памяти в МБ
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Значение `innodb_buffer_pool_size` должно быть *не менее 80%* от ожидаемого размера базы данных *KAV*. Обратите внимание, что указанная память выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Если вы используете **MariaDB 10.4.3** или более раннюю версию, фактический размер выделенной памяти примерно на *10% превышает* указанный размер буфера.

5. Для применения внесенных изменений перезапустите службу:

```
systemctl restart mariadb
```

6. Проверьте статус службы:

```
systemctl status mariadb
```

В статусе должно отображаться **active (running)**.

Установка и настройка KSC

1. Создайте группу **kladmins** и непривилегированную учетную запись **ksc**. Учетная запись должна быть членом группы **kladmins**. Для этого последовательно выполните следующие команды:

```
adduser ksc
groupadd kladmins
gpasswd -a ksc kladmins
usermod -g kladmins ksc
```

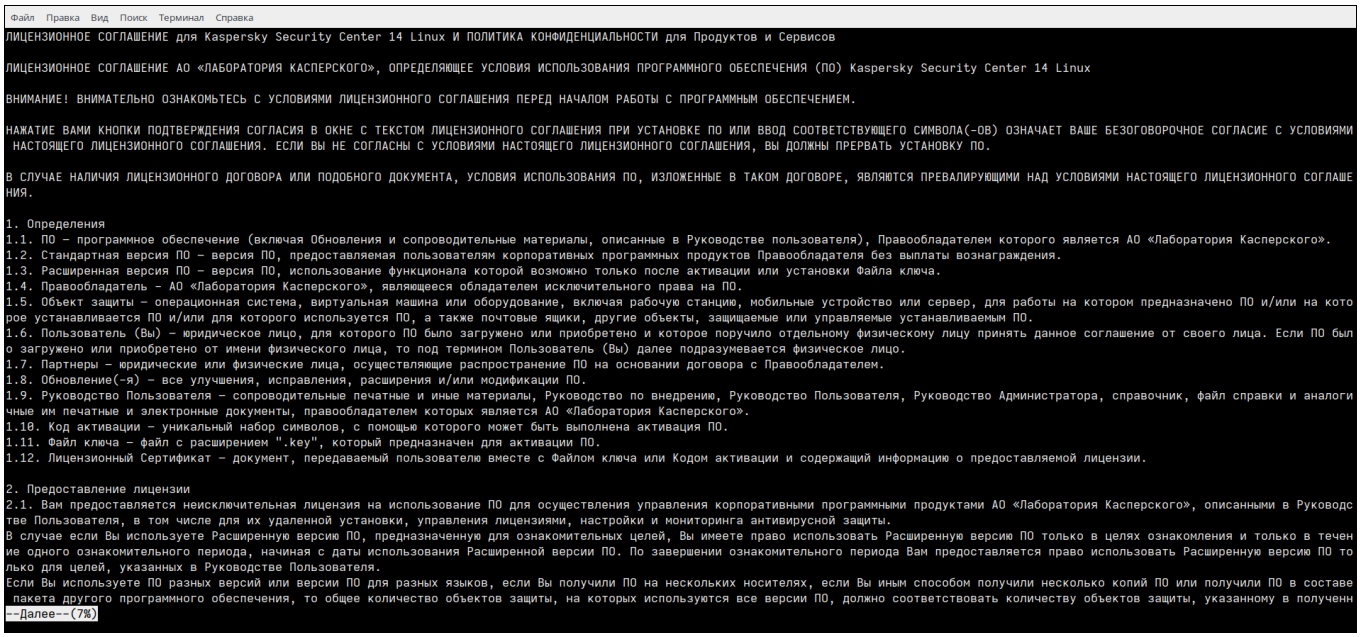
2. Перейдите на официальную страницу разработчика KSC, выберите и скачайте необходимую версию продукта.

3. Запустите установку **Kaspersky Security Center**:

```
dnf install /<путь_к_файлу>/ksc64-<версия>.rpm
```

4. Запустите настройку **Kaspersky Security Center**:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```



4.1 Прочтите *Лицензионное соглашение* и *Политику конфиденциальности*. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

a. Введите **y**, если вы понимаете и принимаете условия *Лицензионного соглашения*. Введите **n**, если вы не принимаете условия *Лицензионного соглашения*. Чтобы использовать *Kaspersky Security Center Linux*, необходимо принять условия *Лицензионного соглашения*.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y
```

b. Введите **y**, если вы понимаете и принимаете условия *Политики конфиденциальности* и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно *Политике конфиденциальности*. Введите **n**, если вы не принимаете условия *Политики конфиденциальности*. Чтобы использовать *Kaspersky Security Center Linux*, необходимо принять условия *Политики конфиденциальности*.

```
Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y
```

4.2 При отображении запроса введите следующие параметры:

a. Введите DNS-имя *Сервера администрирования* или статический *IP-адрес*. Для локальной установки – **127.0.0.1**.

b. Введите номер SSL-порта *Сервера администрирования*. По умолчанию номер порта – **13000**.

c. Оцените примерное количество устройств, которыми вы планируете управлять:

- если у вас от 1 до 100 сетевых устройств, введите **1**;
- если у вас от 101 до 1000 сетевых устройств, введите **2**;
- если у вас более 1000 сетевых устройств, введите **3**.

```
Enter Administration Server DNS-name or static IP-address:
127.0.0.1

Enter Administration Server SSL port number [13000]:


Define the approximate number of devices that you intend to manage:
1) 1 to 100 networked devices
2) 101 to 1 000 networked devices
3) More than 1 000 networked devices
Enter the range number (1, 2, or 3) [1]:
1
```

d. Введите имя группы безопасности для служб. По умолчанию используется группа **kladmins**.

e. Введите имя учетной записи для запуска службы *Сервера администрирования*. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись **ksc**.

f. Введите имя учетной записи, чтобы запустить другие службы. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись **ksc**.

g. Выберите СУБД, которую вы установили для работы с *Kaspersky Security Center Linux*:

- если вы установили MySQL или MariaDB, введите **1**;
- если вы установили PostgreSQL или Postgres Pro SQL, введите **2**.

h. Введите DNS-имя или IP-адрес устройства, на котором установлена база данных. Для локальной установки – **127.0.0.1**.

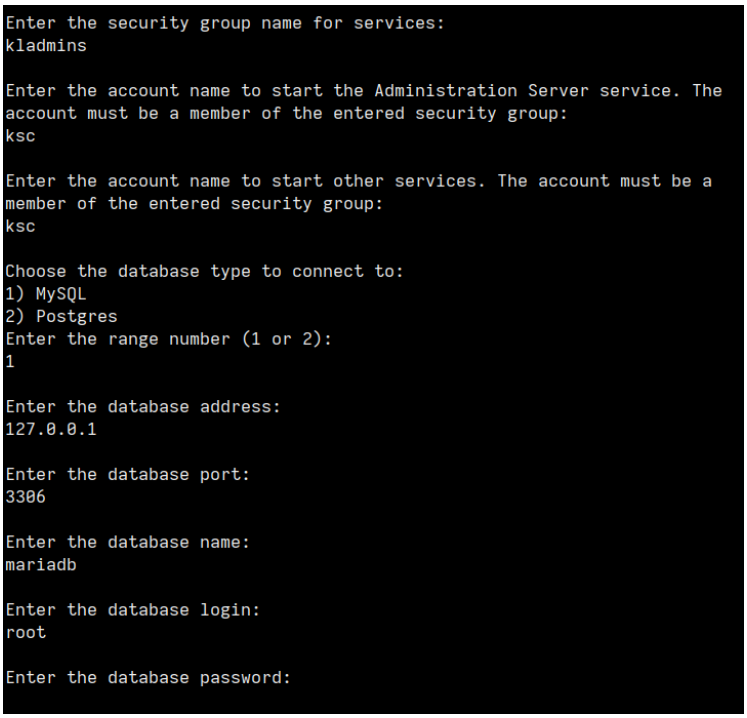
i. Введите номер порта базы данных. Этот порт используется для связи с *Сервером администрирования*. По умолчанию используются следующие порты:

- порт **3306** для MySQL или MariaDB;
- порт **5432** для PostgreSQL или Postgres Pro.

j. Введите имя базы данных.

k. Введите имя учетной записи **root** базы данных, которая используется для доступа к базе данных.

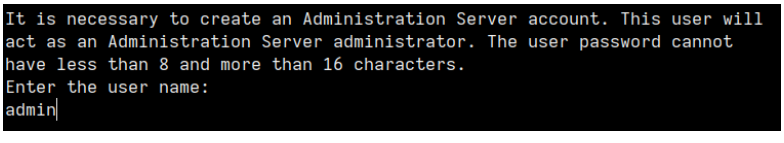
l. Введите **пароль** учетной записи **root** базы данных, которая используется для доступа к базе данных.



Подождите, пока службы добавятся и запустятся автоматически:

- klnagent_srv;
- kladminserver_srv;
- klactprx_srv;
- klwebsrv_srv.

Создайте учетную запись, которая будет выполнять роль администратора *Сервера администрирования*. Введите имя пользователя и пароль.



Вы можете использовать следующую команду для создания пользователя:

```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <пароль>
```

Пользователь будет добавлен, а *Kaspersky Security Center Linux* установлен.

5. Проверьте, запущены ли необходимые службы:

```
systemctl status klnagent_srv.service kladminserver_srv.service klactprx_srv.service klwebsrv_srv.service
```

В статусе должно отображаться **active (running)**.

Установка и настройка WebConsole

1. Создайте файл ответов, который содержит параметры для подключения *Kaspersky Security Center Web Console* к *Серверу администрирования*. Имя файла **ksc-web-console-setup.json**.

```
nano /etc/ksc-web-console-setup.json
```

Пример файла ответов, содержащего минимальный набор параметров, адрес и порт по умолчанию:

```
{
 "address": "192.168.0.106",
 "port": 8080,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
 "acceptEula": true
 }
```

Описание параметров:

- `address` – адрес, по которому будет осуществляться доступ к консоли, статичный IP, который вы задавали ранее;
- `port` – порт, по которому будет осуществляться доступ к консоли;
- `trusted` – параметры подключения к серверу KSC, путь к сертификату KSC, имя сервера;
- `acceptEula` – принятие лицензионного соглашения.

Подробную информацию о файле см. по ссылке.

Программа *Kaspersky Security Center Web Console* не может быть обновлена с помощью того же установочного файла **.rpm**. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки программы, сначала необходимо удалить программу, а затем установить ее снова с новым файлом ответов.

2. Перейдите на официальную страницу, выберите и скачайте необходимую версию *Kaspersky Security Center Web Console*.

3. Запустите установку скачанного файла с расширением **.rpm** (необходимы права суперпользователя или администратора системы):

```
dnf install ksc-web-console-[номер_сборки].x86_64.rpm
```

Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки. *Kaspersky Security Center Web Console* устанавливается в каталог **/var/opt/kaspersky/ksc-web-console**.

4. Перезапустите все службы *Kaspersky Security Center Web Console*, выполнив следующую команду:

```
systemctl restart KSC*
```

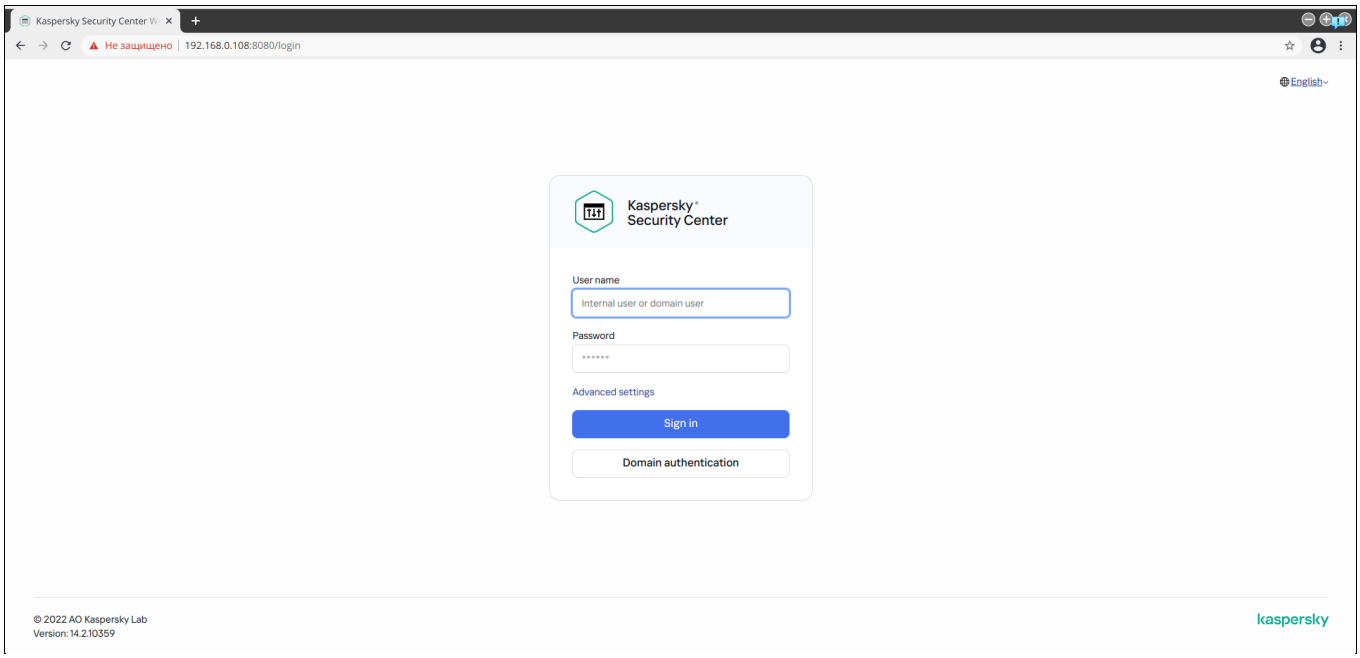
5. Проверьте статус служб:

```
systemctl status KSC*
```

В статусе должно отображаться **active (running)**.

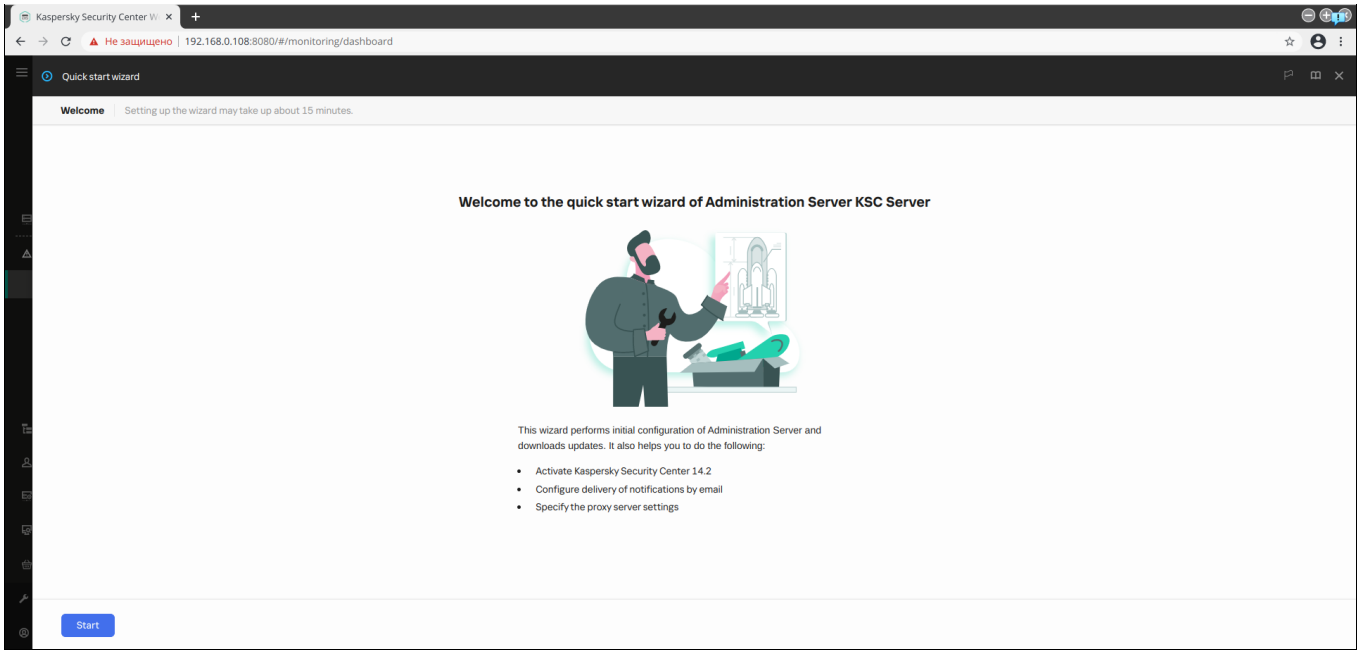
Перейдите в веб-консоль *Kaspersky Security Center Web Console*, для этого в браузере в адресную строку введите https://192.168.0.106:8080.

В вашем браузере **JavaScript** должен быть включен.



Используйте *логин* и *пароль* администратора, указанные при установке **KSC**, для доступа к инструментам администрирования.

После входа запустится мастер первоначальной настройки, с его помощью вы сможете настроить основные политики, задачи, активировать программу и пр.



Со сравнением функционала версий для *Windows* и *Linux* можно ознакомиться на данной странице.

Установка Dr.Web

Подключение репозитория Dr.Web
Установка Dr.Web

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** drweb-workstations-11.1.5

Вы можете подробнее ознакомиться с информацией по установке и настройке **Dr.Web**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Dr.Web;
- в **Яндекс.Дзен** — Установка Dr.Web;
- в **VK Видео** — Установка Dr.Web.

На наших каналах вы также сможете найти много другой полезной информации.

Подключение репозитория Dr.Web

Создайте файл репозитория **drweb** командой (потребуются права **администратора**):

```
sudo nano /etc/yum.repos.d/drweb.repo
```

Добавьте в него следующее содержимое:

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Установка Dr.Web

Для установки **Dr.Web** выполните команду (потребуются права **администратора**):

```
dnf install drweb-workstations
```

После установки антивирус будет доступен из «**Главного меню**» — «**Dr.Web**» — «**Dr.Web для Linux**».



О DHCP

DHCP - Протокол динамической конфигурации хоста, представляет собой протокол сетевого управления, посредством которого сервер DHCP динамически назначает IP-адрес и другие параметры конфигурации сети для каждого устройства в сети.

Включенный в состав РЕД ОС DHCP-сервер, соответствующий RFC 2131, включает фирменные расширения BOOTP (RFC 2132). Так же поддерживает протокол конфигурации динамического хоста для IPv4 (DHCPv4), который может использоваться для обмена информацией о полном доменном имени клиента DHCPv4, описанный в RFC 4702.

Поддерживается стандарт DHCPv6, описанный в RFC 3315. Так же поддерживается контроль и настройка параметров доступа к беспроводным точкам доступа (CAPWAP) DHCP, описанные в RFC 5417.

Базовая настройка DHCP

Установка и первоначальная настройка

Устанавливаем **DHCP**:

```
dnf install dhcp-server
```

Настройки для диапазона адресов **IPv4** производятся в файле **/etc/dhcp/dhcpd.conf**. Пример данного файла можно посмотреть в файле **/usr/share/doc/dhcp-4.2.5/dhcpd.conf.example**. Ваша версия **dhcpd** в пути может отличаться.

Вы можете подробнее ознакомиться с базовой настройкой DHCP, просмотрев наши обучающие видео:

- на **RuTube** — Базовая настройка DHCP;
- в **Яндекс.Дзен** — Базовая настройка DHCP;
- в **VK Видео** — Базовая настройка DHCP.

На наших каналах вы также сможете найти много другой полезной информации.

Теперь откроем на редактирование конфигурационный файл:

```
nano /etc/dhcp/dhcpd.conf
```

Подсети обозначаются блоками, пример такого блока представлен ниже:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.0 192.168.0.100;
  range 192.168.0.120 192.168.0.254;
  option domain-name-servers 192.168.0.10, 192.168.0.11;
  option domain-name "redos.test";
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

** где*

- ***subnet** обозначает сеть, в области которой будет работать данная группа настроек;*
- ***range** — диапазон, из которого будут браться IP-адреса, диапазон адресов 192.168.0.101—192.168.0.120 выдаваться не будет;*
- ***option domain-name-servers** — через запятую перечисленные DNS-сервера;*
- ***option domain-name** — суффикс доменного имени;*
- ***option routers** — шлюз по умолчанию;*
- ***option broadcast-address** — адрес сети для широковещательных запросов;*
- ***default-lease-time**, **max-lease-time** — время и максимальное время в секундах, на которое клиент получит адрес, по его истечению будет выполнено продление срока.*

Добавляем правило в **firewalld**:

```
firewall-cmd --permanent --add-service=dhcp
firewall-cmd --reload
```

Некоторые дополнительные параметры

option domain-name *string***;** — Параметр задает доменное имя, которое клиенты используют при запросах к DNS, при разрешении имен.

option netbios-name-servers <*ip-address*> [**,** *ip-address*...]**;** — Задает список серверов имен **NetBIOS** (NBNS), соответствующих **RFC 1001/1002.** Сервера должны быть перечислены в порядке предпочтительности. Сервера имен **NetBIOS** также известны как сервера **WINS**.

option netbios-dd-server <*ip-address*> [**,** *ip-address*...]**;** — Опция сервера распределения данных **NetBIOS** (NBDD) указывает список серверов **RFC 1001/1002 NBDD**. Серверы должны быть перечислены в порядке предпочтения.

option netbios-node-type INT**;** — Параметр позволяет сконфигурировать тип узла, т.е. способ разрешения имен клиентами **NetBIOS** поверх **TCP/IP**.

Возможные значения параметра:

1 B-node (Broadcast): Разрешение имен с помощью широковещательных запросов, WINS не используется.

2 P-node (Peer): Используется только WINS.

4 M-node (Mixed): Смешанный тип, сначала используется широковещательный запрос, затем в случае неудачи - WINS

8 H-node (Hybrid): Смешанный наоборот. WINS, а затем broadcast.

option netbios-scope *string***;** — Опция области **NetBIOS** указывает параметр **NetBIOS** через **TCP/IP** для клиента, как указано в **RFC 1001/1002**. См. RFC1001, RFC1002 и RFC1035 для ограничения набора символов.

BOOTP

Каждый клиент **BOOTP** может быть настроен отдельно в файле **dhcpd.conf**. Самая простая конфигурация состоит из адреса сетевой карты и IP-адреса, назначаемого этому клиенту. Если клиент должен быть загружен с сервера, указывается загрузочный образ. Простая конфигурация для клиента **BOOTP** может выглядеть так:

```
host haagen {
  hardware ethernet 08:00:2b:4c:59:23;
  fixed-address 239.252.197.9;
  filename "/tftpboot/haagen.boot";
}
```

Дополнительные параметры.

Включение и отключение bootp

allow bootp;
deny bootp;

Параметр **bootp** сообщает серверу dhcp обрабатывать или нет bootp-запросы. По умолчанию bootp-запросы разрешены.

Параметр ***dynamic-bootp*** в секции **range** указывается в случае, если предполагается назначать адреса из диапазона клиентам по протоколу **BOOTP**.

Необходима хотя бы одна секция **h o s t** для каждого BOOTP-клиента, обслуживаемого сервером. Так ж е **host** может быть указана для DHCP-клиентов, хотя это и не обязательно, если только не требуется раздача адресов только определенным клиентам.

Если требуется обеспечить выдачу фиксированных адресов и конфигурацию клиентов по протоколам **DHCP** или **BOOTP** в более, чем одной подсети, то можно указать несколько адресов с помощью параметра *fixed-address* или указать несколько секций **host.**

Если клиентские параметры меняются в зависимости от сети, к которой подключен клиент, то необходимо использовать множественные записи **host.**

<имя_хоста> - имя, идентифицирующее хост. Если в описании хоста опция **hostname** не указана, то используется значение *<имя_хоста>*.

Объявления *Host* сопоставляются с реальными DHCP или BOOTP-клиентами путем сравнения опции **dhcp-client-identifier,** указанной в секции *host* со значением, предоставленным клиентом, или если клиент не предоставляет **dhcp-client-identifier**, то путем сравнения опции *hardware* и аппаратного (mac) адреса клиента. Клиенты BOOTP нормально не предоставляют *dhcp-client-identifier*, так что, при работе по протоколу BOOTP, необходимо использовать mac-адреса.

hardware *<тип_железа> <аппаратный_адрес>***;**

Для того что бы BOOTP-клиент был опознан сервером, его mac-адрес должен быть объявлен с помощью параметра *hardware* в секции *host* параметр *<тип_железа>* - тип физического интерфейса. В настоящее время используются только **ethernet** и **token-ring** и, возможно, скоро будут реализованы другие типы, особенно **fddi**.

<аппаратный_адрес> - записывается как набор шестнадцатеричных значений (от 0 до ff), разделенных двоеточиями. Параметр *hardware* можно использовать и для DHCP-клиентов.

Параметр *dynamic-bootp-lease-cutoff*

dynamic-bootp-lease-cutoff *<дата>***;**

Параметр *dynamic-bootp-lease-cutoff* устанавливает момент времени, в который все адреса, назначенные клиентам BOOTP, должны быть освобождены. Так как клиенты BOOTP не имеют возможности продлить срок использования полученных адресов и не могут определить, что срок аренды истек, то по умолчанию клиентам BOOTP адреса выделяются на неограниченный срок. Однако в

некоторых случаях оказывается полезным установить параметр *dynamic-bootp-lease-cutoff*, например в учебном заведении при окончании семестра или в ночное время, когда предприятие не работает, а все компьютеры выключены.

<дата> - срок окончания действия всех адресов, выделенных BOOTP-клиентам. Дата указывается в следующем формате: **W ГГГГ/ММ/ДД ЧЧ:ММ:СС** .

- **W** - день недели в виде числа от 0 (воскресенье) до 6 (суббота);
- **ГГГГ** - год;
- **ММ** - месяц 1..12;
- **ДД** - день месяца 1..31;
- **ЧЧ** - часы 0..23 MM - минуты 0..59;
- **СС** - секунды 0..59.

Время указывается в GMT, а не местное.

Параметр *dynamic-bootp-lease-length*

dynamic-bootp-lease-length <*время_в_секундах*>**;**

Параметр *dynamic-bootp-lease-length* используется для указания срока, на который выделяется адрес BOOTP-клиенту. В некоторых организациях возможна ситуация, что по прошествии определенного времени можно быть уверенным, что выделенный адрес уже не используется. Период задается числом секунд. Если клиент перезагружается в момент, когда срок, указанный в этом параметре еще не истек, то период аренды адреса заново устанавливается в указанное значение. Таким образом, часто перезагружаемые BOOTP-клиенты могут постоянно удерживать свой адрес. Необходимо заметить, что при настройке параметра следует быть осторожным.

always-reply-rfc1048 <*on/off*>**;**

Некоторые BOOTP-клиенты ожидают ответа от сервера в стиле **RFC1048**, но сами не следуют **RFC1048** при посылке запросов. Если в вашей сети имеется такой проблемный клиент, который не воспринимает параметры, передаваемые ему сервером, и если в логах появляется сообщение **"(non-rfc1048)"** , то можно воспользоваться этим параметром.

Если у вас все клиенты требуют работы в стиле **RFC1048**, то можно использовать параметр **always-reply-rfc1048**. Параметр может быть указан в любом объявлении, в этом случае - воздействует только на тех клиентов, которые соответствуют указанной зоне действия.

Резервирование ip-адреса за клиентом

Хост с именем **myhost**, у которого сетевая карта имеет MAC 08:45:32:00:00:23 должен иметь постоянный адрес 192.168.1.121.

```
host myhost {
      hardware ethernet 08:45:32:00:00:23;
      fixed-address 192.168.1.121;
}
```

Определенный интерфейс для работы

Если в системе присутствует несколько сетевых адаптеров, а сервер DHCP должен работать только для определенных, открываем на редактирование следующий файл:

```
vi /etc/sysconfig/dhcpd
```

И добавляем в него следующее:

```
DHCPDARGS=enp0s8
```

** в данном примере сервер будет работать только для интерфейса **enp0s8**.*

Перед запуском убедитесь, что сетевой адаптер **enp0s8** настроен для работы в создаваемой сети. Для этого создайте файл **/etc/sysconfig/network-scripts/ifcfg-enp0s8** со следующим содержимым.

```
TYPE="Ethernet"
BOOTPROTO="none"
DNS1="192.168.0.1"
```

```
IPADDR0="192.168.0.1"
PREFIX0=24
GATEWAY0=192.168.0.1
DEFROUTE="yes"
PEERDNS="yes"
PEERROUTES="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="enp0s8"
DEVICE="enp0s8"
ON BOOT="yes"
```

Разрешаем автозапуск сервиса:

```
systemctl enable dhcpd
```

и запускаем его:

```
systemctl start dhcpd
```

Настройка логов

По умолчанию, сервер **dhcp** ведет лог в файле **/var/log/messages**, что не очень удобно, так как это общий лог-файл, в котором может находиться много записей.

Для того чтобы сервер сохранял записи в отдельный файл, открываем на редактирование **rsyslog.conf**:

```
vi /etc/rsyslog.conf
```

И добавляем следующее:

```
local6.*       /var/log/dhcp.log
```

Далее открываем конфигурационный файл **dhcp**:

```
nano /etc/dhcp/dhcpd.conf
```

И добавляем:

```
log-facility local6;
```

Перезапускаем сервисы:

```
systemctl restart dhcpd
systemctl restart rsyslog
```

Настройка DHCP-сервера для работы с сервером PXE

Отредактируйте файл **/etc/dhcp/dhcpd.conf** ,

```
# vi /etc/dhcp/dhcpd.conf
```

Добавьте строку в конец файла до фигурной скобки.

```
filename "pxelinux.0";next-server <имя_сервера>;}
```

Параметр **next-server** используется для указания клиенту адреса сервера, с которого должен быть получен загрузочный файл (тот

самый файл, что указан в параметре *filename*). <**Имя_сервера**> может быть IP-адресом или доменным именем. Если этот параметр не указан, то используется адрес DHCP-сервера.

Отказоустойчивый сервер DHCP

Подготовка серверов

Для отказоустойчивой конфигурации необходимо два сервера DHCP.

Синхронизируйте время, между серверами с помощью ntp или chrony. Так же можно воспользоваться командой ntpdate, которую нужно выполнить на обоих серверах к одному ntp-серверу.

```
ntpdate <адрес сервера ntp>
```

Предположим, что имеется два сервера, на которых установлен пакет dhcp и добавлен в автозапуск.

Первичный сервер: 192.168.0.1

Вторичный сервер: 192.168.0.2

Настройка первичного сервера

1. Пропишите необходимые правила для iptables, если вы используете его.

```
iptables -A INPUT -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
iptables -A INPUT -s 192.168.0.2/24 -p tcp -m state --state NEW -m tcp --dport 647 -j ACCEPT
```

2. Отредактируйте файл /etc/dhcp/dhcpd.conf.

```
nano /etc/dhcp/dhcpd.conf
```

Обратите внимание, что параметр **mclt** (максимальное время выполнения клиента) должен быть определен на главном сервере, но не должен быть определен на подчиненном сервере. Параметр **split** является еще одним параметром , который должен быть определен на первичном и опущен из конфигурации на вторичном сервере. Стоит отметить, что связь между отказоустойчивыми узлами не шифруется и не аутентифицируется.

```
failover peer "failover-dhcp" {
  primary; # Определяет главный сервер
  address 192.168.0.1; # адрес первичного сервера
  port 647;
  peer address 192.168.0.2; # адрес вторичного сервера
  peer port 647;
  max-response-delay 60;
  max-unacked-updates 10;
  mclt 3600;
  split 128;
  load balance max seconds 3;
}

authoritative;
default-lease-time 86400; # 1 день
max-lease-time 86400; # 1 день
update-static-leases on;
one-lease-per-client on;

omapi-port 7911;
omapi-key omapi_key;
key omapi_key {
    algorithm hmac-md5;
    secret a6d79e096b7055ff51e5756c77947ab5==; # сформируйте секретный ключ с помощью любого генератора, указав тип
шифрования hmac-md5
}

subnet 192.168.0.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  option routers 192.168.0.1;
  option domain-name-servers redos.test;
  option domain-search "redos.test";
  pool {
    failover peer "failover-dhcp";
    range 192.168.0.100 192.168.0.200;
  }
}
```

+ Описание параметров

name *data* просмотр

имя связи резервирования, задается в файле **dhcpd.conf**.

partner-address *data*

IP адрес резервного сервера.

local-address *data*

IP адрес текущего сервера.

partner-port *data*

порт TCP, на котором резервный сервер ожидает подключения по протоколу failover.

local-port *data*

порт TCP, на котором текущий сервер ожидает подключения по протоколу failover.

max-outstanding-updates *integer*

количество обновлений, которые могли быть важными, но остались без ответа в этой связке резервирования.

mclt *integer*

максимальное время перенаправления клиента в этой связке резервирования.

default-lease-time *integer*

срок по умолчанию для клиентов, которые не запрашивают определенный срок аренды. Срок аренды DHCP может быть назначен от нуля секунд до бесконечности.

max-lease-time *integer*

максимальный срок аренды

update-static-leases *data*

если он включен, то сервер DHCP делает обновление DNS для клиентов.

one-lease-per-client *data*

если этот флаг включен, всякий раз, когда клиент отправляет DHCPREQUEST для конкретной аренды, сервер автоматически отчищает любые другие lease записи, которыми владеет клиент.

load-balance-max-secs *integer*

максимальное значение в поле secs запроса клиента после которого будет произведена балансировка нагрузки.

load-balance-hba *data*

массив хэшей буферов для балансировки нагрузки в этой связке резервирования.

local-state *integer*

текущий статус сервера DHCP в этой связке резервирования. Возможные значения:

```
1  - партнер выключен
2  - обычная работа
3  - обмен данными прерван
4  - разрешение прервано
5  - потенциальный конфликт
6  - восстановление
7  - восстановление закончено
8  - выключение
9  - пауза
10 - запуск
11 - идет восстановление
```

В общем случае делать изменения в этом атрибуте - плохая идея. Однако в случае, когда известно, что резервный сервер выключен, бывает необходимо явно указать что резервный сервер недоступен и необходимо взять на себя выданные адреса резервного сервера как можно быстрее. Если же вы указали, что резервный сервер выключен, а он работает (но временно недоступен), возможны конфликты назначения IP адресов.

partner-state *integer*

текущий статус резервного сервера

local-stos *integer*

время, в течение которого сервер работает в текущем статусе.

partner-stos *integer*

время, в течение которого резервный сервер работает в текущем статусе.

hierarchy *integer*

роль сервера: первичный (0) или вторичный (1) в текущей связке резервирования.

last-packet-sent *integer*

время последнего пакета синхронизации, отправленного резервному серверу в связке.

last-timestamp-received *integer*

время последнего пакета синхронизации, полученного от резервного сервера в связке.

skew *integer*

разница между часами резервного и текущего сервера

max-response-delay *integer*

время в секундах, по истечении которого если не получен ни один пакет синхронизации, определяется разрыв в соединении.

cur-unacked-updates *integer*

количество сообщений об обновлении, полученных от резервного сервера, но пока не обработанных.

3. Из за того, что хеш находится в файле, закроем к нему доступ.

```
chmod 0600 /etc/dhcp/dhcpd.conf
```

4. Проверьте конфигурационный файл

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
```

5. Перезапустите сервис

```
systemctl restart dhcpd
```

Настройка вторичного сервера

1. Пропишите настройки для iptables, если используете его

```
iptables -A INPUT -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
iptables -A INPUT -s 192.168.0.1/24 -p tcp -m state --state NEW -m tcp --dport 647 -j ACCEPT
```

2. Для вторичного (secondary) сервера:

```
failover peer "failover-dhcp" {
  secondary; # определитель вторичного сервера
  address 192.168.0.2;
  port 647;
  peer address 192.168.0.1;
  peer port 647;
  max-response-delay 60;
  max-unacked-updates 10;
  load balance max seconds 3;
}

authoritative;
default-lease-time 86400; # 1 day
max-lease-time 86400; # 1 day
```

```
update-static-leases on;
one-lease-per-client on;

omapi-port 7911;
omapi-key omapi_key;
key omapi_key {
  algorithm hmac-md5;
  secret a6d79e096b7055ff51e5756c77947ab5==; # впишите тот же секретный ключ, как и на первичном сервере
}

subnet 192.168.0.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  option routers 192.168.0.1;
  option domain-name-servers redos.test;
  option domain-search "redos.test";
  pool {
    failover peer "failover-dhcp";
    range 192.168.0.100 192.168.0.200;
  }
}
```

3. Из за того, что хеш находится в файле, закроем к нему доступ.

```
chmod 0600 /etc/dhcp/dhcpd.conf
```

4. Проверьте конфигурационный файл

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
```

5. Перезапустите сервис

```
systemctl restart dhcpd
```

О службе DNS (bind)

Если локальная сеть не подключена к сети Интернет, вполне возможно, что внутренний DNS-сервер в ней не нужен. За преобразование доменного имени в IP-адрес и обратно в Linux отвечает несколько разных механизмов, лишь один из которых базируется на службе доменных имён. В самом простом случае имена всех компьютеров вместе с их адресами можно записать в файл **/etc/hosts**. Порядок просмотра различных пространств имён указывается в файле **/etc/nsswitch.conf**. Строка **hosts: files nisplus nis dns** этого файла предписывает приложениям, пользующимся стандартной функцией **gethostbyname()** сначала заглянуть в **/etc/hosts**, затем попытаться получить таблицы **hosts** службы **nisplus** или **nis**, а только затем обращаться к DNS-серверу. Это вполне разумное правило, учитывая время выполнения запроса в каждом случае.

Если задачу преобразования имён в адреса взял на себя провайдер, собственный DNS-сервер можно тоже не заводить. В этом случае на всех компьютерах в качестве сервера имён указывается сервер провайдера (поле *nameserver* в файле **/etc/resolv.conf**), к которому и идут все запросы. Даже если внутренняя сеть организована согласно **RFC1918** (интранет) и адреса компьютеров в ней не могут отображаться в сети Интернет, DNS-запросы во внешний мир работать будут. Между собой компьютерам предлагается общаться с помощью **/etc/hosts** или IP-адресов.

Однако уже здесь очевидны две задачи, для решения которых можно организовать собственную службу доменных имён.

Первая задача - уменьшение времени ответа на DNS-запрос абонентов внутренней сети. Если канал подключения к Интернет обладает большим временем задержки (скажем, четверть секунды), то работа с данными, включающими в себя много доменных имён (например, с www-страницами) может стать весьма медленной, хотя общий объём трафика будет невелик. Система доменных имён - распределённая база данных, замечательно поддерживающая механизм кеширования запросов. Первое обращение к кеширующему DNS-серверу приводит к выполнению рекурсивного запроса: опрашивается сервер более высокого уровня, который, если не знает ответа, передаст запрос дальше. Результат запроса оседает в кеше, так что все последующие обращения именно к этой записи дальше кеширующего сервера не уйдут. Время жизни (*Time To Live, TTL*) записи в кеше определяется хозяином запрошенного доменного имени. По истечении TTL запись из кеша удаляется.

Вторая задача - именование компьютеров в интранет-сети. Это бывает важно, если среди компьютеров внутренней сети есть свои серверы (например, корпоративный WWW-сервер), к которым другие компьютеры обращаются по доменному имени. Поскольку адреса такой сети не пойдут дальше межсетевого экрана, вы можете использовать имя какого угодно, — в том числе несуществующего — домена и составить табличку в **/etc/hosts**. Однако раздавать эту табличку лучше всё-таки средствами DNS.

Обе эти задачи можно решить, воспользовавшись Bind - мощным полнофункциональным DNS-сервером (обратите внимание, пакет и сервис называются **bind**, а сама служба - **named**). При необходимости запуска bind с использованием chroot необходимо установить пакет bind-chroot. В этом случае будет использоваться каталог /var/named/chroot/.

Для того, чтобы запустить named в кеширующем режиме, достаточно раскомментировать и заполнить раздел настройки forwarders (вышестоящие серверы) в файле /var/named/chroot/etc/named.conf. Обратите внимание на возможные ограничения на право обращаться к серверу с обычными и рекурсивными запросами (настройки allow-query и allow-recursion). Можно раскомментировать находящиеся в этом файле разумные установки по умолчанию. Эти настройки открывают доступ только абонентам локальных сетей, т.е. сетей, к которым компьютер подключён непосредственно.

```
grep allow- /var/named/chroot/etc/named.conf
        allow-query     { localhost; any; };
        allow-query-cache { localhost; any; };
```

Использование Bind для полноценного именования компьютеров в локальной сети требует создания двух зон (т.е. прямой и обратной), содержащих в виде записей определённого формата информацию о доменных именах компьютеров и об их роли в этих доменах. Каждая зона должна включать запись типа SOA (State Of Authority, сведения об ответственности). В этой записи определяются основные временные и административные параметры домена, в том числе электронный адрес лица, ответственного за домен (администратора) и серийный номер зоны. Серийный номер - число в диапазоне от 0 до 4294967295 (2**32); каждое изменение, вносимое в зону, должно сопровождаться увеличением этого номера. Обнаружив увеличение серийного номера, кеширующие и вторичные серверы признают все закешированные записи из этой зоны устаревшими. Структура номера может быть любой, лишь бы он постоянно увеличивался. Удобно использовать формат «<год><месяц><число><версия>», где все числа, кроме года, двузначные, а версия может обнуляться раз в день, соответствовать времени (например, по формуле 100*(часы*60+минуты)/(60*24) или иметь сквозную нумерацию (в этом случае появляется сложность с переходом от версии 99 к версии 100, то есть 0). Даже если серийный номер генерируется автоматически, рекомендуется пользоваться этим форматом, наглядно отражающим время создания зоны. Пример зоны, не содержащей ничего, кроме записи SOA и обязательной записи типа NS, находится в файле /usr/share/doc/bind/sample/var/named/named.localhost.

Кроме записи типа SOA, в каждой зоне должна быть хотя бы одна запись типа NS (Name Server), указывающая адрес DNS-сервера, авторитетного в этом домене (как минимум - адрес сервера, на котором запущен named). Несколько зон включаются в настройку Bind автоматически (файл /var/named/chroot/etc/named.rfc1912.zones). Они нужны для обслуживания сети, привязанной к сетевой заглушке (127.0.0.1/8). Стоит обратить внимание на то, что имя домена, который обслуживается зоной, задаётся в файле настроек, а в самом файле зоны можно использовать относительную адресацию (без . в конце имени), так что операция переименования домена делается редактированием одной строки. Рекомендуется добавлять описания зон в конфигурационный файл /var/named/chroot/etc/named.rfc1912.zones.

Прямая зона нужна для преобразования доменного имени в IP-адрес - операции, необходимой многим программам постоянно. Большинство записей в прямой зоне - типа A (Address) - предназначены именно для этого. Другие часто встречающиеся типы записей - это CNAME (Canonical Name, настоящее имя), позволяющий привязать несколько дополнительных имён к одному, и MX (Mail eXchange, обмен почтой), указывающий, куда пересылать почтовые сообщения, в поле адресат которых встречается определённое доменное имя. Вот пример прямой зоны для воображаемого домена *internal.domain.net* (незначащие поля соответствующих файлов заменены на .

. .):

```
# cat /var/named/chroot/etc/named.rfc1912.zones
 . . .
zone "example" IN {
       type master;
       file "internal.domain.net";
       allow-update { none; };
};
 . . .
# cat /var/named/chroot/var/named/internal.domain.net

  $TTL    1D
  @       IN     SOA server root.server (
  2004082202      ; serial
  12H             ; refresh
  1H              ; retry
  1W              ; expire
  1H              ; ncache
                      )
  IN     NS    server
  MX 10   server
  Server        A       10.10.10.1
  www           CNAME   server
  mail          CNAME   server
  jack          A       10.10.10.100
```

В этом примере совпадение имени файла и имени зоны осмысленно - так проще разбираться с содержимым каталога **/var/named/chroot/var/named/**. Используются правила умолчания: если в записи некоторое поле опущено, оно наследуется от предыдущей. Так, вместо A можно было бы всюду написать IN A, а вместо MX - @ IN MX (@ означает имя домена, указанное в конфигурационном файле). Как видно из пример, всю работу в сети делает компьютер с адресом 10.10.10.1, он же **server.internal.domain.net**, он же **www.internal.domain.net** и **mail.internal.domain.net**. Несмотря на наличие среди CNAME этого сервера имени mail, MX-запись указывает всё же не на него, а на действительный адрес - так рекомендовано RFC. Распространённая практика заводить запись типа A непосредственно на имя зоны (т. е. присваивать адрес имени internal.domain.net) приводит, помимо незначительных выгод, к мелким, неочевидным и весьма трудно преодолимым трудностям, которые мы здесь описывать не будем, ограничившись советом не использовать этот - пусть и законный - трюк.

Для того чтобы преобразовывать IP-адреса в доменные имена, у каждой сети должна быть обратная зона. Если такой зоны нет, и в файле **/etc/hosts** тоже ничего не написано, операция не выполнится. Такое преобразование нужно гораздо реже и в основном по соображениям административным: для того, чтобы выяснить принадлежность компьютера (с которого, допустим, пытаются атаковать сервер) по его IP-адресу. Некоторые почтовые серверы проверяют, содержится ли IP-адрес машины, передающей сообщение, в обратной зоне и похоже ли полученное доменное имя на то, что указано в сообщении, и при несовпадении отказываются принимать письмо. К сожалению, поскольку неудобства, связанные с отсутствием обратной зоны, понятны лишь грамотному администратору, а таковых на просторах Интернета не слишком много, обратные зоны во множестве сетей либо отсутствуют, либо дают неверную информацию. В случае внутренней сети обратная зона необязательна, но желательна - для простоты администрирования и удовлетворения потребностей разных программных продуктов, которые ею пользуются.

Обратная зона состоит почти целиком из записей типа PTR (Pointer, указатель). Чтобы не умножать сущностей, решено было не вводить новый способ работы сервера имён и представить обратное преобразование IP-адреса как прямое преобразование доменного имени специального вида. Например, чтобы выяснить доменное имя компьютера с адресом 1.2.3.4, необходимо запросить информацию о доменном имени 4.3.2.1.in-addr.arpa. Таким образом, каждой подсети класса C (или выше) соответствует определённый домен, в котором можно найти ответ. Вот как выглядит обратная зона для нашего воображаемого домена:

```
 cat /var/named/chroot/etc/named.rfc1912.zones
zone "12.11.10.in-addr.arpa" { type master;
file "12.11.10.in-addr.arpa";
};
 cat /var/named/chroot/var/named/12.11.10.in-addr.arpa
$TTL 1D
@       IN     SOA  server.internal.domain.net.       root.server.internal.domain.net (
2004082201    ; serial
12H           ; refresh
1H            ; retry
1W            ; expire
1H            ; ncache
)
      IN     NS   server.internal.domain.net
0             PTR  internal.domain.net.
1             PTR  server.internal.domain.net
100           PTR  jack.internal.domain.net.
```

Обратите внимание, что относительные адреса, использованные в левой части записей PTR, раскрываются в полные вида **<адрес>.12.11.10.in-addr.arpa**, а в правой части используются полные (которые вполне могут указывать на имена в разных доменах).

Проверить синтаксическую правильность конфигурационного файла и файла зоны можно с помощью утилит **named-checkconf** и **named-checkzone**, входящих в пакет bind. Они же используются при запуске службы командой **service bind start**. Однако при интенсивной эксплуатации сервера, когда остановка службы нежелательна, можно попросить службу перечитать файлы настроек или определённые зоны с помощью утилиты **rndc** - вот тогда не стоит забывать о проверке синтаксиса.

Стоит иметь в виду, что, в отличие от прямых зон, обратные описывают административную принадлежность компьютеров, но сами принадлежат хозяину сети (как правило, провайдеру). Возникает особого рода затруднение, связанное с работой DNS-сервера уже не во внутренней сети, а в сети Интернет. Дело в том, что подсети класса C (т. н. сети /24, в которых сетевая маска занимает 24 бита, а адрес компьютера - 8) выдаются только организациям, способным такую подсеть освоить (в сети класса C 254 абонентских IP-адреса, один адрес сети и один широковещательный адрес). Чаще всего выдаются совсем маленькие подсети - от /30 (на два абонентских адреса) до /27 (на 30 адресов) - или другие диапазоны, сетевая маска которых не выровнена по границе байта. Таких подсетей в обратной зоне получится несколько, а возможности просто разделить её, отдав часть адресов в администрирование хозяевам, нет. Грамотный провайдер в таких случаях пользуется **RFC2317** (есть в пакете bind-docs), предписывающем в обратной зоне заводить не записи вида **PTR**, а ссылки **CNAME** на адреса в «классифицированных» обратных зонах специального вида. Обратное преобразование становится двухступенчатым, зато администрирование каждой классифицированной зоны можно отдать хозяину.

DNS-сервер, отвечающий на запросы из сети Интернет, должен быть зарегистрирован в родительском домене. В самом деле, единственный способ узнать, кто обслуживает домен **internal.domain.net** - спросить об этом у DNS-сервера домена **domain.net**. Так что о выделении поддомена необходимо договариваться с провайдером. Регистрацией в доменах первого уровня занимаются выделенные организации. Например, домен в зоне **.ru** необходимо регистрировать в компании АНО «Региональный Сетевой Информационный Центр» (RU-CENTER).

Правила требуют, чтобы при регистрации домена было указано не менее двух DNS-серверов, которые будут его обслуживать. Из всех зарегистрированных серверов (записей типа NS в родительской зоне) только одна соответствует т.н. первичному (master) серверу, а остальные - т.н. вторичным (slave). Для внешнего пользователя вторичный сервер не отличается от первичного: он столь же авторитетен в ответе на запрос об именах его домена. Отличия только в способе администрирования. Все изменения вносятся в зоны первичного сервера, а вторичный только кеширует эти зоны, целиком получая их по специальному межсерверному протоколу. Полученная зона складывается в файл, редактировать который бессмысленно: первичный сервер при изменении зоны рассылает всем своим вторичным указание скачать её заново. Право на скачивание зоны можно ограничить настройкой **allow-transfer** (как правило, в ней перечисляются адреса вторичных серверов). Вот слегка отредактированная цитата из руководства по Bind, описывающая задание вторичного сервера в файле настроек:

```
// We are a slave server for eng.example.com
zone "eng.example.com" { type slave;
file "slave/eng.example.com";
// IP address of eng.example.com master server masters { 192.168.4.12; };
};
```

Вторичный сервер хорошо размещать где-нибудь подальше от первичного, во всяком случае, в другой сети - так повышается надёжность обработки запроса (если один сервер недоступен, возможно, ответит второй) и возрастает скорость распространения записей по кешам промежуточных серверов.

Проверку работоспособности, доступности и вообще самочувствия DNS-сервера лучше всего делать утилитой **dig** из пакета **bind-utils**. Это очень мощная утилита, выдающая максимум информации о том, что происходило с запросом (запрашивая обратное преобразование, не забудьте добавить ключ **-x**). Более лаконична, но не менее мощна утилита **host** из того же пакета. Упоминаемую старыми руководствами по UNIX утилиту **nslookup** использовать не рекомендуется.

```
# dig jack.internal.domain.net
<<>> DiG 9.2.4rc5 <<>> jack.internal.domain.net
;; global options:   printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32751
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;jack.internal.domain.net.       IN     A
;; ANSWER SECTION:
jack.internal.domain.net. 86400   IN     A      10.11.12.100
;; AUTHORITY SECTION:
internal.domain.net. 86400       IN     NS     server.internal.domain.net.
;; ADDITIONAL SECTION:
server.internal.domain.net. 86400 IN     A      10.11.12.1
;; Query time: 37 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Aug 22 16:07:17 2004 ;; MSG SIZE rcvd: 95
```

Наконец, для выяснения административной принадлежности тех или иных доменов и сетей можно воспользоваться утилитой **whois**, которая обращается к специальной сетевой базе данных (не имеющей отношения к DNS).

Настройка DNS-сервера bind

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер минимальный
- **Версия bind:** bind-9.16.16

О сервере

В состав репозитория РЕД ОС включен DNS-сервер **bind**, поддерживающий стандарты **RFC 1034,1035, 2136**. Поддерживает реализацию хост-систем на базе стека протоколов **Internet**, описанных в **RFC 1123**. Поддерживает механизм инкрементального переноса зон **IXFR**, описанный в **RFC 1995** и механизм извещения ведомых серверов **NOTIFY, RFC 1996**.

Подготовка сервера

Устанавливаем все обновления:

```
dnf update
```

Установка и запуск BIND

Устанавливаем DNS-сервер следующей командой:

```
dnf install bind
```

Разрешаем автозапуск:

```
systemctl enable named --now
```

И проверяем, что он работает корректно:

```
systemctl status named
```

Базовая настройка DNS-сервера

Открываем на редактирование конфигурационный файл **bind**:

```
nano /etc/named.conf
```

и редактируем следующее в блоке **options**:

```
listen-on port 53 { 127.0.0.1; 192.168.0.1; };
listen-on-v6 port 53 { none; };
allow-query { any; };
forward first;
forwarders { 8.8.8.8; };
```

* 192.168.0.1 — IP-адрес нашего DNS-сервера, на котором он будет принимать запросы;

- **allow-query** разрешает выполнять запросы всем, но из соображений безопасности можно ограничить доступ для конкретной сети, например, вместо **any** написать **10.10.1.0/24**.
- **listen-on-v6 port 53** присвоим значение none, тем самым отключив ipv6
- **forward** с параметром **first** указывает, DNS-серверу пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders, и лишь в случае, если разрешить имя с помощью данных серверов не удалось, то будет осуществлять попытки разрешения имени самостоятельно.
- **forwarders** перенаправляем запросы, которые сами не резолвим, на днс сервер гугла.

Создание локальных зон DNS

Создайте папку с мастер зонами:

```
mkdir /var/named/master
```

Прямая DNS зона

Создайте прямую DNS-зону.

```
nano /var/named/master/example.org
```

Пример её содержимого с описанием ниже.

```
$TTL 604800     ;
example.org.    IN     SOA     ns01.example.org. root.example.org. (
            1             ; Serial
            600           ; Refresh
            3600          ; Retry
            1w            ; Expire
            360           ; Minimum TTL
            )
      IN     NS     ns01.example.org.
      IN     NS     ns02.example.org.
      IN     NS     ns03.example.org.
ns01    IN     A      192.168.10.50
ns02    IN     A      192.168.10.60
ns03    IN     A      192.168.10.70
www     IN     A      192.168.10.20
test    IN     A      192.168.10.12
```

Рассмотрим подробнее написанное:

$TTL 3600 — Time to live время жизни, по умолчанию 1 день. По достижении установленного времени, кеширующий сервер запрашивает DNS сервер, содержащий доменную зону, информацию о зоне. И при необходимости обновляет записи.
example.org IN SOA ns01.example.org. root.example.org. зона обслуживания, адрес корневого сервера для зоны, акаунт её админа. 2022112801**; Serial** - серийный номер версии таблицы dns. Самый лучший формат - ГГГГММДДNN, где NN - номер изменения таблицы за текущий день;
600; Refresh-указывает подчиненным DNS серверам как часто им обращаться, для поиска изменений к master серверу.
3600; Retry — говорит о том, сколько Slave сервер должен подождать, прежде чем повторить попытку.
1w; Expire — Максимальный срок жизни записей, после которой они потеряют актуальность (1 неделя)
300; Minimum TTL -минимальный срок жизни записи 5 мин.
NS ns01.example.org.-NS сервер который обслуживает эту зону
NS ns02.example.org.-NS сервер который обслуживает эту зону
NS ns03.example.org.-NS сервер который обслуживает эту зону
A 192.168.10.20 -если требуется попасть по адресу example.org, то клиенту будет выдан этот IP
ns01 A 192.168.10.50 — Записи для поиска наших NS серверов
ns02 A 192.168.10.60
ns03 A 192.168.10.70
test A 192.168.10.12 -Если клиент запрашивает адрес test.example.org, DNS выдаст ip 192.168.10.12?

Назначьте владельца и права.

```
chown -R root:named /var/named/master
chmod 0640 /var/named/master/*
```

В конфигурационный файл **named.conf** добавьте следующее:

```
zone "example.org" {
 type master;
 file "master/example.org";
 };
```

* где **example.org** — имя зоны, которую будет обслуживать наш DNS-сервер. Это и есть домен, для которого bind будет хранить записи. Должен совпадать по имени с файлом зоны в папке master.

Описание опций настройки зоны:

- **type** <тип зоны> (в нашем случае первичная — значит master). Другие варианты — **slave**, **stub**, **forward**.
- **file** <путь_к_файлу> с записями зоны. В данном примере указан относительный путь — то есть файл находится по пути **master/test.local**, который начинается относительно рабочей директории (по умолчанию — **/var/named/**). Таким образом, полный путь до файла — **/var/named/master/test.local**.

Для каждой зоны создайте свой блок **zone**.

Чтобы настройки применились, необходимо перезапустить службу.

```
systemctl restart named
```

Для проверки работоспособности сервера с другого компьютера сети (например, на Windows) выполняем команду:

```
> nslookup test.example.org 192.168.0.1
```

** данной командой мы пытаемся узнать IP-адреса сайта test.example.org через сервер 192.168.0.1.*

Должно получиться, примерно, следующее:

```
Server:     192.168.0.1
Address:    192.168.0.1#53

Name:       test.example.org
Address:    192.168.10.12
```

Создание обратной зоны

В конфигурационный файл **named.conf** добавьте следующее:

```
zone "10.168.192.in-addr.arpa" {
    type master;
    file "master/10.168.192.zone";
};
```

Создайте обратную DNS-зону.

```
nano /var/named/master/10.168.192.zone
```

Пример её содержимого с описанием ниже.

```
$TTL    3600
@  IN     SOA     example.org. root.example.org (
              20060204        ; Serial
              3600            ; Refresh
              900             ; Retry
              3600000         ; Expire
              3600 )          ; Minimum
@  IN     NS      localhost.
50 IN     PTR     ns01
60 IN     PTR     ns02
70 IN     PTR     ns03
20 IN     PTR     www
12 IN     PTR     test
```

Чтобы настройки применились, необходимо перезапустить службу.

```
systemctl restart named
```

Логирование Bind

Способ 1

По умолчанию, сервер **Bind** хранит логи в файле:

```
/var/named/data/named.run
```

Для его непрерывного просмотра вводим следующую команду:

```
tail -f /var/named/data/named.run
```

Степень детализации логов можно настроить в конфигурационном файле:

```
logging {
  channel default_debug {
    file "data/named.run";
  severity dynamic;
  };
};
```

* где **file** — путь к log-файлу; **severity** — уровень чувствительности к возникающим событиям.

Возможны следующие варианты для severity:

- **critical** — критические ошибки;
- **error** — ошибки и выше (critical);
- **warning** — предупреждения и выше. Предупреждения не говорят о наличии проблем в работе сервиса, однако это такие событтия, которые могут привести с ошибкам, поэтому не стоит их игнорировать;
- **notice** — уведомления и выше;
- **info** — информация;
- **debug** — отладка (подробный лог);
- **dynamic** — тот же debug.

Способ 2

Создайте каталог для логов:

```
mkdir /var/log/bind
```

В разделе **logging** задаются 2 параметра **channel** (можно и больше двух - на ваше усмотрение), эти параметры дословно можно назвать "канал" записи. Каждый канал определяет имя канала и настройки параметров записи (что записывать, а что - нет и куда писать).

Директива **category** задает какую категорию сообщений в какой канал отправлять.

Исходя из этого, мы имеем: запись стандартной информации в канал **misc**, а приходящие запросы посылаются в канал **query**. При этом, если файлы журнала достигают 4Мб (size 4m), он переименовывается добавлением к имени **.1** и начинается запись в новый журнал, числа в конце других журналов увеличиваются. Журналы с номером, более указанного в **version** (в нашем случае 4) удаляются.

Параметры **print*** определяют заносить ли в журнал время появления, важность и категорию информации. Более подробно про настройки раздела **logging** можно почитать в **man (5) named.conf**.

Добавьте конфигурацию логирования в файл **/etc/named.conf**:

```
// настройки логирования
logging {
        channel "misc" {
                file "/var/log/bind/misc.log" versions 4 size 4m;
                print-time yes;
                print-severity yes;
                print-category yes;
        };

        channel "query" {
                file "/var/log/bind/query.log" versions 4 size 4m;
                print-time yes;
                print-severity no;
                print-category no;
        };

        category default {
                "misc";
        };
```

```
        category queries {
                "query";
        };
};
```

Проверка работоспособности

Для проверки работоспособности и правильной конфигурации DNS-сервера, нужно сделать к нему несколько запросов. Для этого можно воспользоваться консольными утилитами **ping**, **dig** или **nslookup**.

ВАЖНО!

Клиент, на котором выполняются запросы должен быть настроен на использование вашего DNS сервера, подробнее смотрите в настройках сетевого адаптера.

Утилита **ping**, при указании доменного имени, резолвит его с помощью DNS. Если пинг к хосту, указанному в DNS, выполняется, то A запись данного хоста корректна.

С помощью **dig** или **nslookup** можно проверить обратные записи или иные специфические записи DNS-сервера. Например:

```
dig SRV _ldap._tcp.ad.test
```

Сделает запрос SRV-записи на сервере в домене **ad.test**. Должен вывести ip-адрес хоста с LDAP сервисом.

```
nslookup 192.168.10.50
```

Запрос должен вывести hostname для введенного **ip**. Тем самым проверив обратную (**PTR**) запись.

Настройка репликации DNS-сервера bind

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер минимальный
- **Версия bind:** bind-9.16.16

Предварительно необходимо ознакомиться и настроить DNS-сервер согласно нашей инструкции «**Настройка DNS-сервера bind**».

Подготовка master сервера

Открываем на редактирование конфигурационный файл bind:

```
nano /etc/named.conf
```

и редактируем следующее в блоке options:

```
allow-recursion { none; };
```

Находим и закомментируем строку

```
dnssec-validation yes;
```

Добавьте строки в блоки ваших локальных зон

```
allow-transfer { <ip адрес реплики>; };
allow-update { <ip адрес реплики>; };
notify yes;
```

Рассмотрим подробнее, то что мы написали:

- **allow-recursion { none; }** — Отключаем использование рекурсивных запросов т.к. это сильно снижает скорость работы, да и нее имеет смысла опрашивать вышестоящие DNS сервера по поводу зоны которую сами же и обслуживаем.
- **allow-transfer {<ip адрес реплики>;}** — разрешаем передачу данной зоны на остальные наши DNS сервера;
- **allow-update {<ip адрес реплики>;}** — разрешаем обновление;
- **notify yes** — включаем автоматическое уведомление подчиненных серверов об обновлении файла настроек DNS зоны.

Перезагрузите bind.

```
systemctl restart named
```

Настройка slave сервера.

Устанавливаем все обновления.

```
dnf update
```

Устанавливаем DNS-сервер следующей командой:

```
dnf install bind
```

Запускаем сервис и добавляем в автозапуск:

```
systemctl enable named --now
```

И проверяем, что он работает корректно:

```
systemctl status named
```

Открываем на редактирование конфигурационный файл bind:

```
nano /etc/named.conf
```

и редактируем следующее в блоке options:

```
listen-on port 53 { 127.0.0.1; <ip данного сервера>;};
listen-on-v6 port 53 { none; };
allow-query { any; };
forward first;
forwarders {8.8.8.8;};
allow-recursion { none; };
```

Находим и закомментируем строку

```
dnssec-validation yes;
```

добавляем туда запись, только на этот раз она будет немного отличаться:

```
zone "example.org" IN {
        type slave;
        file "/var/named/slaves/slave.example.org";
        masters { <ip адрес мастера>; };
        allow-transfer { "none"; };
};
```

Рассмотрим подробнее изменения:

- **type slave;** — тип зоны подчиненная
- **file /var/named/slaves/slave.example.org"** — путь к файлу с настройками, в этот раз в имени файла указано slave.example.org чтобы было понятно на каком сервере вы находитесь.
- **masters { <ip адрес мастера>; }** — IP адрес Мастер сервера, откуда будет производиться запрос файлов с настройками DNS зон.
- **allow-transfer {none;}** — Отключаем передачу зоны другим серверам, чтобы нельзя было получить все записи в домене

Впишите вышеописанные блоки для каждой зоны.

Перезагрузите DNS сервер.

```
systemctl restart named
```

Теперь должны появиться файлы DNS зон по пути, который указан.

ВАЖНО

Каждый раз, когда в настройки зоны на мастере вносятся изменения, к серийному номеру прибавляется единица, это делается для того чтобы подчиненные сервера увидели изменения в записях и приняли обновленный файл зоны, если после внесения изменений в файл, серийный номер остался прежним или уменьшился, то подчиненные DNS сервера НЕ станут подтягивать обновления считая что на мастер сервере изменений небыло!

Для редактирования серийного номера DNS зоны, откройте её файл и отредактируйте параметр serial.

Пример файла зоны:

```
...
@       IN      SOA     ns0.ipa.test. postmaster.ipa.test. (
                2018042804  ;serial
...
```

Это значение нужно увеличивать каждый раз при редактировании файла доменной зоны. Оно записано в формате YY-MM-DD + наращиваемый порядковый номер.

Для проверки работоспособности сервера с другого компьютера сети выполняем команду:

```
nslookup test.example.org <ip адрес реплики>
```

** данной командой мы пытаемся узнать IP-адреса сайта test.example.org через сервер репликации DNS.*

Должно получиться, примерно, следующее:

```
Server:      192.168.0.1
Address:     192.168.0.1#53
```

```
Name:        test.example.org
Address: 192.168.10.12
```

Настройка кеширования DNS с помощью dnsmasq

ВНИМАНИЕ

Для корректной установки и настройки dnsmasq, перейдите в сеанс суперпользователя:

```
sudo -i
```

или

```
su
```

На запрос пароля, введите пароль привилегированного пользователя или локального администратора.

DNS - кэш предназначен для ускорения загрузки страниц веб-сайтов, путем сохранения в памяти их IP-адресов. Для настройки кэширования используйте утилиту **dnsmasq**.

```
dnf install dnsmasq
```

С помощью текстового редактора vi или nano откройте файл, расположенный по адресу **/etc/dnsmasq.conf**

```
vi /etc/dnsmasq.conf
```

или

```
nano /etc/dnsmasq.conf
```

Отредактируйте следующие параметры:

```
resolv-file=/etc/resolv.dnsmasq
no-poll
listen-address=127.0.0.1
cache-size=150
conf-dir=/etc/dnsmasq.d,.rpmnew,.rpmsave,.rpmorig
```

А так же допишите следующий параметр:

```
all-servers
```

Где:

- **resolv-file** — файл с IP-адресами dns - серверов
- **no-poll** — параметр, запрещающий автоматическое применение изменений в файлах с именем resolv.
- **listen-address** — параметр, указывающий какой адрес слушать.
- **cache-size** — размер кэша. Значение по умолчанию позволяет хранить 150 хостов.
- **conf-dir** — параметр, отвечающий за дополнительный файл конфигурации.
- **all-servers** — перенаправляет dns-запрос всем доступным dns-серверам и возвращает ответ от первого откликнувшегося сервера. Параметр нужно записать вручную.

Также можно указать следующие параметры:

- **no-negcache** — не кэшировать негативные ответы от серверов.
- **bind-interfaces** — позволяет запускать копии процесса.
- **dns-forward-max** — максимальное количество dns-запросов. По умолчанию — 150. Параметр нужно записать вручную.

Теперь создайте файл **resolv.dnsmasq** с помощью текстового редактора **vi** или **nano** и запишите туда адреса dns-серверов.

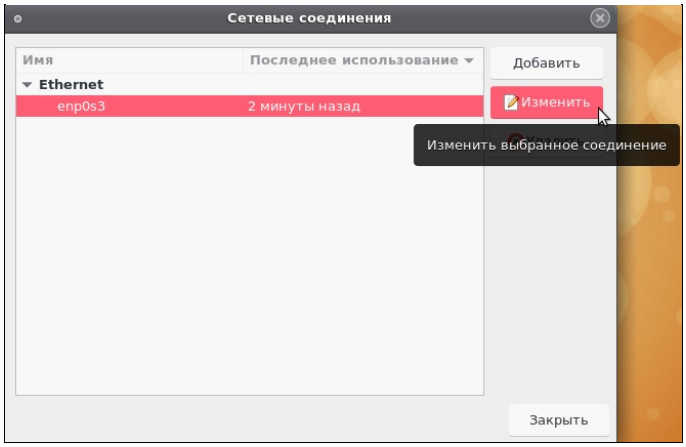
```
vi /etc/resolv.dnsmasq
```

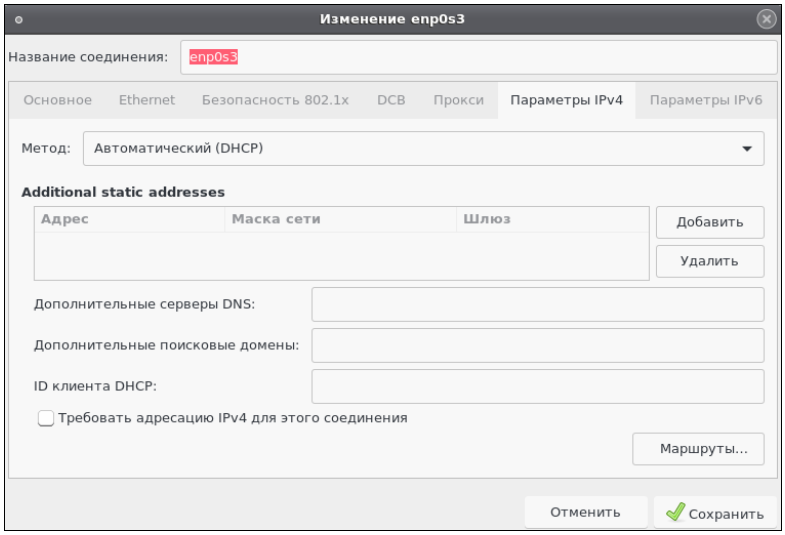
или

```
nano /etc/resolv.dnsmasq
```

Потом добавьте IP-адрес **127.0.0.1** в файл **resolv.conf**. Для этого, используйте утилиту **«Сетевые соединения»**, расположенную в **«Меню» → «Параметры» → «Сетевые соединения»** в графическом окружении **Cinnamon** или **«Система» → «Параметры» →**

«Сетевые соединения» в графическом окружении **Mate**. Выберите ваше активное подключение, нажмите кнопку **«Изменить»,** перейдите на вкладку **«Параметры IPv4»**, поменяйте **«Метод»** на **«Автоматический (DHCP, только адрес)»**, а в поле "**Дополнительные серверы DNS**" напишите адрес **127.0.0.1**, нажмите применить и перезапустите **NetworkManager.**





Редактирование файла resolv.conf с помощью текстовых редакторов не рекомендуется. Файл перезапишется со следующим перезапуском системы.

```
systemctl restart NetworkManager.service
```

Чтобы убедиться, что изменения вступили в силу, посмотрите содержимое файла **resolv.conf**:

```
cat /etc/resolv.conf
```

Содержимое должно быть таким:

```
# Generated by NetworkManager

nameserver 127.0.0.1
```

Описанные выше операции позволят перенаправлять все dns-запросы на локальную машину.

Добавьте службу **dnsmasq** в автозапуск и перезайдите в сеанс:

```
systemctl enable dnsmasq.service --now
```

Для того, чтобы сбросить кэш, просто перезапустите службу:

```
systemctl restart dnsmasq.service
```

Проверка работоспособности

Проверьте, включена ли служба:

```
systemctl status dnsmasq.service
```

Проверьте порт 53:

```
netstat -ntlp | grep :53
```

```
tcp  0  0 0.0.0.0:53  0.0.0.0:*  LISTEN 7319/dnsmasq
tcp6 0  0 :::53   :::*   LISTEN 7319/dnsmasq
```

Теперь попробуйте с помощью утилиты dig несколько раз обратиться к сайту **google.com**

```
dig google.com | grep "Query time"
```

```
;; Query time: 135 msec
```

Если кэширование dns-запросов работает, то практически во всех следующих запросах выделенная строчка **query time** будет равна нулю.

```
;; Query time: 0 msec
```

В противном случае она будет варьироваться от 0 и выше с каждым новым запросом.

В результате, основной DNS-сервер сети будет испытывать гораздо меньше нагрузки.

Расширенная настройка DNS-сервера

Настройка stub-зоны на сервере bind
Зоны пересылки
Русскоязычные имена
Использование DNSSEC

Настройка stub-зоны на сервере bind

Примечание.

Данная настройка требует указания правильной цепочки доверенностей DNS серверов. Если у вас её нет, впишите следующие параметры в файл:

```
dnssec-enable no;
dnssec-validation no;
```

Static-stub позволяет указать конкретные **IP**, по которым следует обращаться для преобразования имен (**resolving**) заданных зон в обход обслуживающих данные зоны DNS-серверов.

Откройте конфигурационный файл **bind**:

```
nano /etc/named.conf
```

Настройте зону следующим образом:

```
zone "stub.test" {
type static-stub;
server-addresses { 192.168.0.1; 192.168.0.50; };
};
```

* где:

- **stub.test** — домен, для которого нужно делать перенаправление запросов;
- **192.168.0.1, 192.168.0.50** — адреса DNS-серверов, на которые перенаправлятся запросы.

Перезапустите **bind**, чтобы применить настройки:

```
systemctl restart named
```

Зоны пересылки

Примечание.

Данная настройка требует указания правильной цепочки доверенностей DNS серверов. Если у вас её нет, впишите следующие параметры в файл:

```
dnssec-enable no;
dnssec-validation no;
```

Задачу перенаправления DNS-запросов можно решить с помощью зоны типа **forward**. Настройка выполняется следующим образом:

```
zone "stub.test" {
type forward;
forwarders { 192.168.0.1; 192.168.0.30; };
};
```

Перезагрузить сервис:

```
systemctl restart named
```

Русскоязычные имена

Для записи русскоязычных имен хостов или доменов нужно узнать, как доменное имя выглядит в **Punycode**-представлении. Например, с помощью сервиса 2ip. Далее необходимо вписать имя в **punycode**-представлении в файл зоны, например:

```
xn----gtbc2bgjip    IN    A    10.81.200.222
```

Использование DNSSEC

DNSSEC описана в стандарте **RFC 4033**.

Создайте отдельный каталог для файлов с ключами:

```
mkdir -p /var/named/keys
cd /var/named/keys
```

Обычно генерируется большое количество файлов, поэтому для каждой зоны можно создать отдельную директорию с ключами.

Для работы **DNSSEC** требуется создать **master**-ключ (*KSK, Key Signing Key*), который будет использован для создания цифровых подписей для других ключей, и ключи для каждой из локальных зон (*ZSK, Zone Signing Key*).

Создайте KSK-ключ:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE example.net

Generating key pair.....+++.....+++
Kexample.net.+005+38287
```

Создайте ZSK-ключ:

```
dnssec-keygen -a RSASHA1 -b 2048 -n ZONE example.net

Generating key pair.....+++ ..+++
Kexample.net.+005+55896
```

Для того чтобы ключи были сгенерированы, необходима рандомная составляющая. Для этого нужно перемещать указатель мыши несколько раз при генерации ключей либо выполнять команды генерации с дополнительным параметром -r /dev/urandom, например:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -r /dev/urandom -n ZONE example.net
```

Установите на ключи права доступа *только для чтения* процессу **named**:

```
chown named. *
```

Включите в настройках **named.conf** запись лога **DNSSEC** для упрощения анализа возможных проблем.

Подготовьте директорию для хранения лога:

```
mkdir -p /var/log/bind/
chown named. /var/log/bind/
```

В **named.conf** пропишите путь к логу, который будет ограничен максимальным размером в **20 Мб**:

```
logging {
channel dnssec_log {
```

```
file "/var/log/bind/dnssec.log" size 20m;
print-time yes;
print-category yes;
print-severity yes;
severity debug 3;
};
category dnssec {
dnssec_log;
};
};
```

Отредактируйте секцию **options**:

```
options {

...
key-directory "/var/named/keys";
sig-validity-interval 20 10;
};
```

* где:

- **key-directory** — каталог для хранения сгенерированных ключей (необходимо указать тот каталог, в котором были сформированы последние ключи командой dnssec-keygen);
- **sig-validity-interval** — период действия ключей: дней/период обновления.

Для зоны редактируем:

```
zone "example.net" {
type master;
file "master/example.net";
key-directory "keys/";
inline-signing yes;
auto-dnssec maintain;
};
```

Опция inline-signing yes включает режим прозрачного формирования подписей, не требуя внесения изменений непосредственно в файл зоны. При работе inline-signing вручную поддерживаемый файл с зоной преобразуется в динамическую зону, для которой создаётся цифровая подпись. Из-за этого выдаваемый сервером серийный номер отличается от серийного номера, прописанного в файле с зоной. Изменения **DNSSEC** производятся в **jnl**-файле с журналом изменений.

Проверьте, что у пользователя **named/bind** есть права на запись в каталог хранения зоны. При необходимости, можно изменить владельца, например:

```
chown -R named:named /var/named/master
```

Откройте на редактирование файл зоны и измените серийный номер.

Перезапустите **bind**:

```
systemctl restart named
```

После перезапуска **named** в директории **/var/named/keys** появятся следующие файлы:

- example.net;
- example.net.jbk;
- example.net.signed;
- example.net.jnl.

При запросе параметров зоны можно заметить появление нового поля **RRSIG**.

```
dig example.net +dnssec
```

```
...
example.net. 600 IN A 1.2.3.4
example.net. 600 IN RRSIG A 5 3 600 2012021356423 20120415331566 21695 net. IKeklJa314313G/xZpQ+B2313eqaDceR/VNcdsdasxV2 ...
```

Так как **DNSSEC** основан на обеспечении цепочки доверия, чтобы процесс верификации заработал, требуется, чтобы регистратор заверил созданный KSK-ключ, подтвердив своё доверие. Для этого создайте на основе KSK-ключа **DSKEY**-ключ (Delegation Signature Key)

```
dnssec-dsfromkey Kexample.net.+005+38287

example.net. IN DS 38287 5 1 E8C01C9CA1252389A9CB4E
example.net. IN DS 38287 5 2 57EC936A479A94C3232412313423452349235 9A623 39712D53
```

Скопируйте две сгенерированные строки в интерфейсе ввода **DSKEY** на сайте регистратора домена. Верификация заработает после того, как регистратор обновит параметры первичной зоны.

Для поддержки **DNSSEC**-проверки на стороне резолвера следует добавить в настройки **named.conf**:

```
options {
...
dnssec-enable yes;
dnssec-validation auto;
...
};
```

Проверка работоспособности DNS с помощью nslookup

Синтаксис утилиты
Примеры использования утилиты
Получение IP-адреса
Обратное преобразование
Запись NS
Запись MX

nslookup – утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе **DNS**. Позволяет задавать различные типы запросов и опрашивать произвольно указываемые серверы для проверки работоспособности **DNS**, просмотра IP-адреса сервера, скорости его работы и т.д.

С помощью данной утилиты также можно не только получить IP-адрес по доменному имени, но и выполнить обратное преобразование, а также проверить необходимые записи **DNS**.

По умолчанию утилита **nslookup** предустановлена в РЕД ОС.

Синтаксис утилиты

Синтаксис утилиты имеет следующий вид:

```
nslookup [-опции] [домен] [сервер]
```

Основные опции **nslookup**:

- **-type** – тип информации, которую требуется получить, возможные типы: *txt*, *soa*, *ptr*, *ns*, *mx*, *mr*, *minfo*, *mg*, *mb*, *hinfo*, *gid*, *cname*, *a*, *any*;
- **-port** – использовать другой порт DNS-сервера (порт по умолчанию **53**);
- **-recurse** – рекурсивный запрос (информация запрашивается у других серверов, если она недоступна или отсутствует на указанном сервере);
- **-retry** – количество попыток опроса сервера;
- **-timeout** – время ожидания ответа от сервера (в секундах);
- **-fail** – опросить другой сервер имен, если указанный вернул ошибку.

Примеры использования утилиты

Получение IP-адреса

Для определения IP-адреса сервера по его доменному имени необходимо выполнить команду вида:

```
nslookup <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
Name: ya.ru
Address: 77.88.55.242
Name: ya.ru
Address: 5.255.255.242
Name: ya.ru
Address: 2a02:6b8::2:242
```

В строке **Server** выводится IP-адрес сервера, в строке **Address** – IP-адрес сервера и порт, с которого был отправлен запрос к **ya.ru**.

Далее отображается информация о запросе. В строке **Name** выводится доменное имя сервера, на который был отправлен запрос. В строке **Address** выводится IP-адрес, который принадлежит доменному имени сервера. Из примера видно, что доменному имени может

принадлежать несколько IP-адресов.

Обратное преобразование

Также с помощью утилиты **nslookup** может быть выполнено обратное преобразование IP-адреса в доменное имя. Для этого используется команда вида:

```
nslookup <IP-адрес>
```

Пример команды и ее вывода:

```
nslookup 77.88.55.242

242.55.88.77.in-addr.arpa name = ya.ru.

Authoritative answers can be found from:
55.88.77.in-addr.apra nameserver = ns3.yandex.ru.
55.88.77.in-addr.apra nameserver = ns4.yandex.ru.
ns3.yandex.ru internet address = 87.250.250.1
ns3.yandex.ru has AAAA address = 2a02:6b8::1001
ns4.yandex.ru internet address = 77.88.21.1
ns4.yandex.ru has AAAA address = 2a02:6b8:0:1::1:1
```

Запись NS

Первоисточником информации о домене являются его **NS**-серверы. Получить их можно, используя опцию `-type=ns` в команде следующего вида:

```
nslookup -type=ns <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=ns ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru nameserver = ns2.yandex.ru.
ya.ru nameserver = ns1.yandex.ru.

Authoritative answers can be found from:
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

Команда выведет список используемых серверов имен, в приведенном примере это **ns1.yandex.ru**.

Запись MX

Также можно получить **MX**-запись для домена, установив тип запроса **mx** в команде следующего вида:

```
nslookup -type=mx <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=mx ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru mail exchanger = 10 mx.yandex.ru.
```

```
Authoritative answers can be found from:
ya.ru nameserver = ns1.yandex.ru.
ya.ru nameserver = ns2.yandex.ru.
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

В выводе команды будут отображены все настроенные почтовые серверы, у каждого сервера есть свой приоритет – 15, 10 или 5. Чем меньше число, тем выше приоритет адреса. В приведенном примере почтовый сервер – **mx.yandex.ru** имеет приоритет **10**.

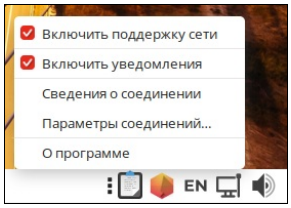
Настройка сетевого адаптера

Настройка сети в графическом сеансе
Настройка сети в терминале
Изменение конфигурационного файла текстовым редактором
Использование интерфейса nmtui
Изменение через утилиту nmcli

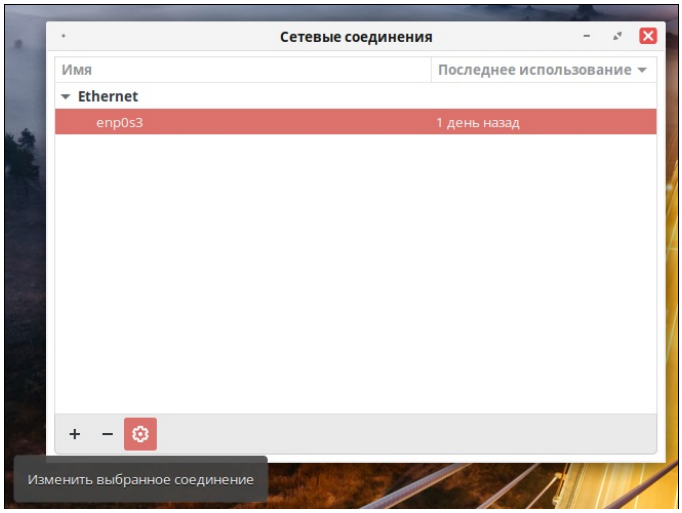
Настройку сетевого адаптера можно осуществить, используя графический интерфейс, либо через терминал.

Настройка сети в графическом сеансе

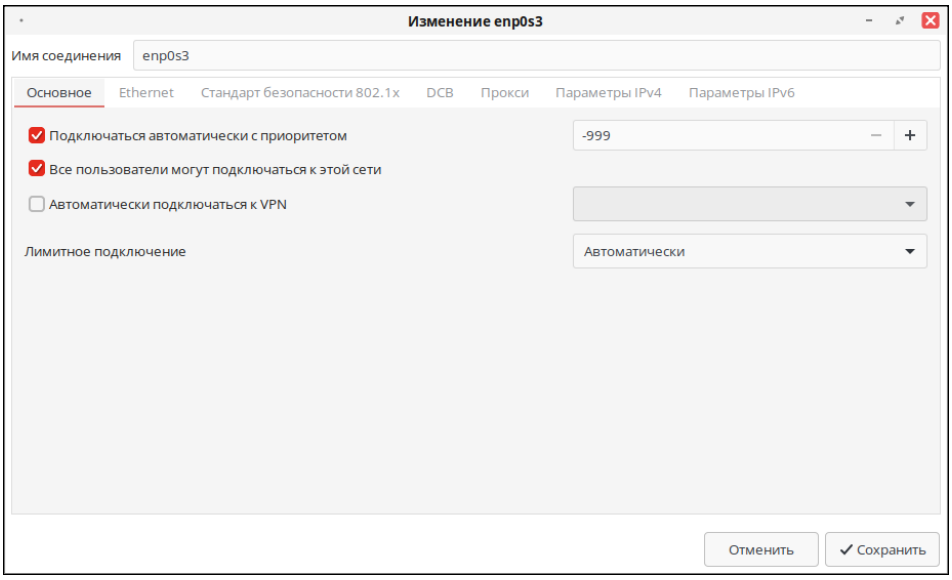
Настройка сети в РЕД ОС производится с помощью программы **NetworkManager**. Для ручной настройки сетевого адаптера необходимо в системном трее ПКМ вызвать контекстное меню, нажав на иконку сетевых соединений. В контекстном меню выберите пункт «**Параметры соединений...**».



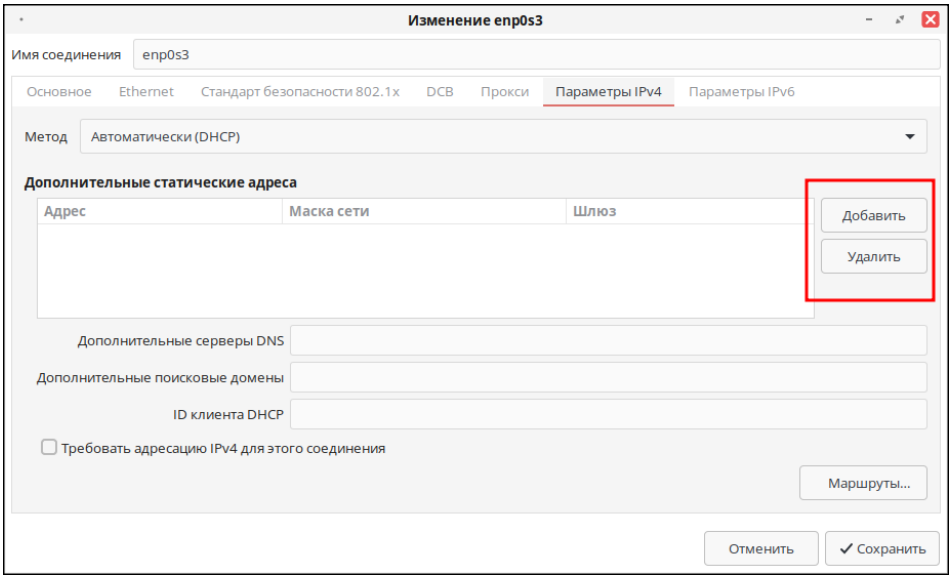
В открывшемся окне «**Сетевые соединения**» необходимо выбрать нужный сетевой адаптер и нажать кнопку «**Изменить выбранное соединение**».



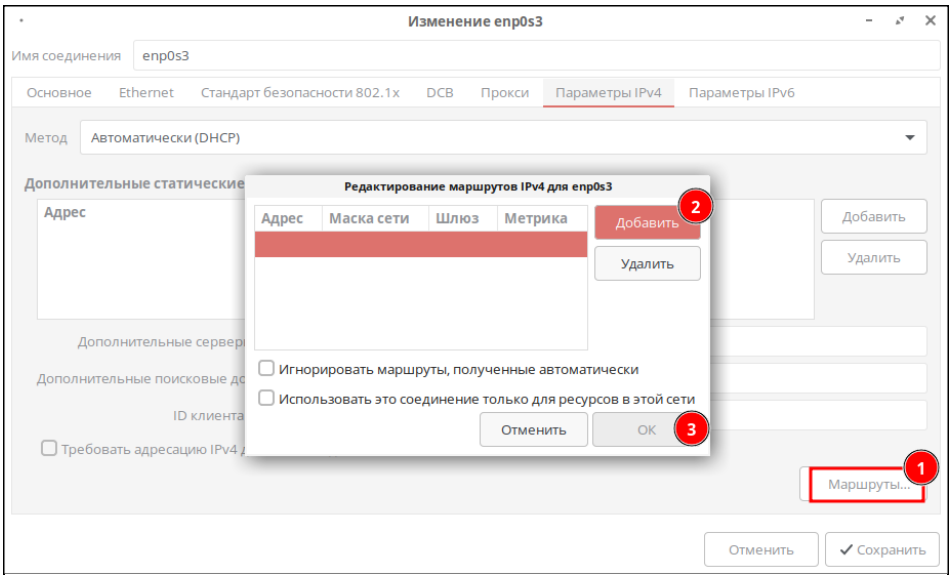
В открывшемся окне свойств сетевого адаптера на вкладке «**Основное**» можно установить свойства автоматического подключения - «**Подключаться автоматически с приоритетом**» и «**Все пользователи могут подключаться к этой сети**».



На вкладке «**Параметры IPv4**» можно задать вручную параметры сетевого подключения, нажав кнопку « **Добавить**».



Для добавления новых маршрутов необходимо нажать на кнопку «**Маршруты...**». В открывшемся диалоговом окне нажмите «**Добавить**», задайте необходимые параметры и нажмите « **OK**».



Для подтверждения изменений, внесенных в настройки сетевого адаптера, нажмите «**Сохранить**».

Настройка сети в терминале (консоли)

Для настройки сети в терминале можно использовать 3 варианта:

1. **Изменение конфигурационного файла текстовым редактором**
2. **Использование интерфейса nmtui**
3. **Изменение через утилиту nmcli**

Изменение конфигурационного файла текстовым редактором

Вы можете подробнее ознакомиться с информацией по настройке сети, просмотрев наши обучающие видео:

- на **RuTube**:
  - Сеть в РЕД ОС. Основы. Утилита ip;
  - Сеть в РЕД ОС. NetworkManager CLI.
- в **Яндекс.Дзен**:
  - Сеть в РЕД ОС. Основы. Утилита ip;
  - Сеть в РЕД ОС. NetworkManager CLI.

- в **VK Видео**:
    - Сеть в РЕД ОС. Основы. Утилита ip;
    - Сеть в РЕД ОС. NetworkManager CLI.

На наших каналах вы также сможете найти много другой полезной информации.

Для просмотра сетевых настроек выполните команду:

```
ifconfig
```

или воспользуйтесь утилитой `ip` с параметром `addr`:

```
ip addr
```

Тут можно увидеть параметры и название сетевой карты.

```
ip addr

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether be:cd:c8:c8:7a:60 brd ff:ff:ff:ff:ff:ff
inet 10.10.10.83/24 brd 10.10.10.255 scope global dynamic noprefixroute enp0s3
valid_lft 435sec preferred_lft 435sec
inet6 fe80::f42e:4ae5:4dc0:ff68/64 scope link noprefixroute
valid_lft forever preferred_lft forever+
```

По умолчанию сетевой адаптер настроен для получения IP-адреса по **DHCP**. Настройки хранятся в файле **/etc/NetworkManager/system-connections/<имя_сетевого_интерфейса>.nmconnection**. Именуются они, например, как **enp0s3** или **enp0s4**.

В данном примере сетевой интерфейс имеет имя **enp0s3**. Используя команду `cat`, можно посмотреть содержимое файла настроек:

```
cat /etc/NetworkManager/system-connections/enp0s3.nmconnection

[connection]
id=enp0s3
uuid=97def639-603a-4167-9613-edd5bd902ef8
type=ethernet
interface-name=enp0s3
timestamp=1704763284

[ethernet]

[ipv4]
method=auto

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

Для редактирования файла настроек можно использовать любой текстовый редактор (например **mcedit** или **vi**).

Для установки статического IP-адреса необходимо для параметра `method` указать значение `manual` в секции **[ipv4]**:

```
method=manual
```

Далее следует указать собственные конфигурации:

- Игнорировать **DNS** из **DHCP**:

```
ignore-auto-dns=true
```

- Указать статический **DNS**:

```
dns=8.8.8.8;
```

- Указать **IP**, **маску** и **шлюз** по умолчанию:

```
address1=192.168.1.100/24,192.168.1.1
```

Для немедленного применения изменений перезапустите сеть:

```
systemctl restart NetworkManager
```

Таким образом, при статической настройке IP-адреса, секция **[ipv4]** будет иметь следующий вид:

```
[ipv4]
address1=192.168.1.100/24,192.168.1.1
dns=8.8.8.8;
ignore-auto-dns=true
method= manual
```

В файле настройки сетевой карты можно добавить столько DNS-серверов, сколько требуется. Например:

```
dns=8.8.8.8;8.8.4.4;192.168.1.1;
```

ВАЖНО!

В работе используются максимум 3 DNS-сервера (те, что указаны первыми).

Проверить шлюз, по умолчанию установленный в системе, можно с помощью команды:

```
netstat -nr

Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 172.16.0.1 0.0.0.0 UG 0 0 0 eno16777736
172.16.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eno16777736
```

Строка `Destination 0.0.0.0` определяет адрес шлюза. Если у вас ее нет, возможно, что для параметра `Gateway` установлен неверный шлюз, это можно исправить. Установите шлюз по умолчанию:

```
route add default gw 172.16.0.1
```

Если вы не сменили при установке ОС имя сервера или вы хотите его изменить, то сделать это можно следующим образом. Сначала проверьте, какое имя сервера (`hostname`) у вас установлено:

```
hostname
```

В примере имя сервера будет изменено на `server.work` с помощью команды:

```
hostnamectl set-hostname server.work
```

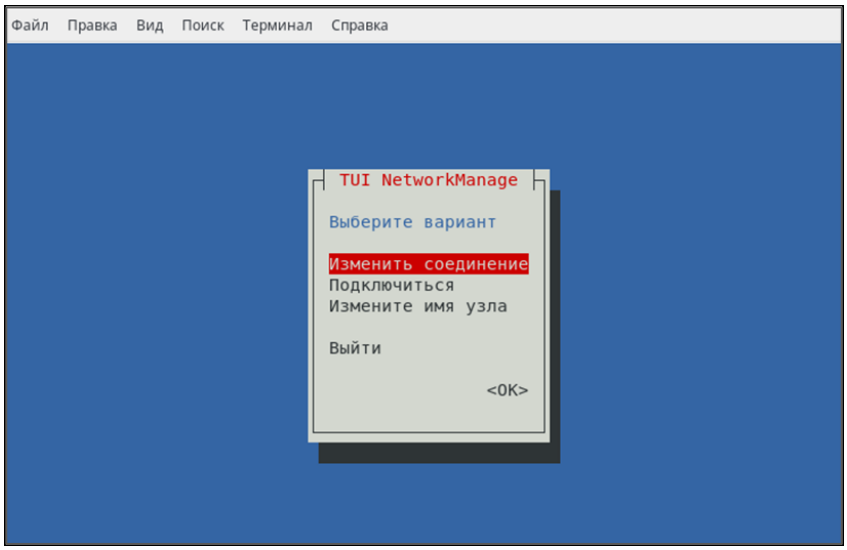
Для смены имени ПК перезагрузка не требуется.

Использование интерфейса nmtui

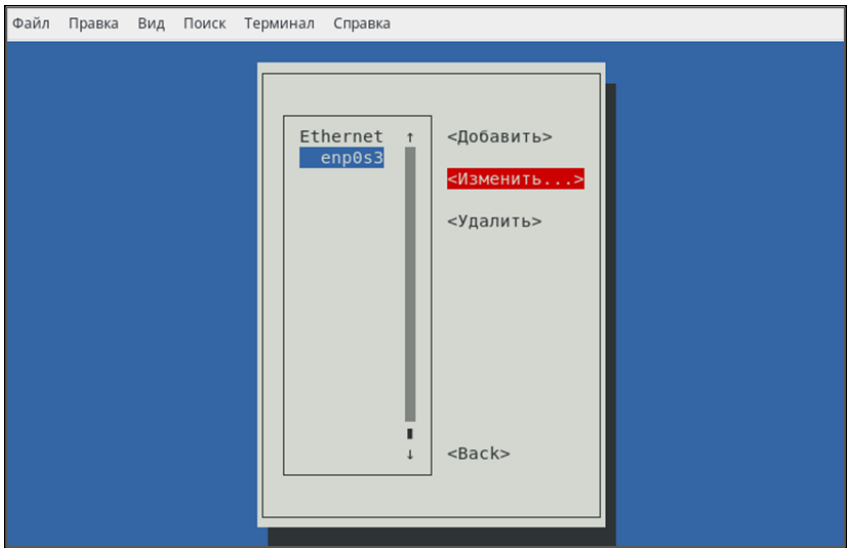
nmtui - утилита для настройки сети с интуитивно-понятным графическим интерфейсом, для ее запуска в терминале необходимо выполнить:

```
nmtui
```

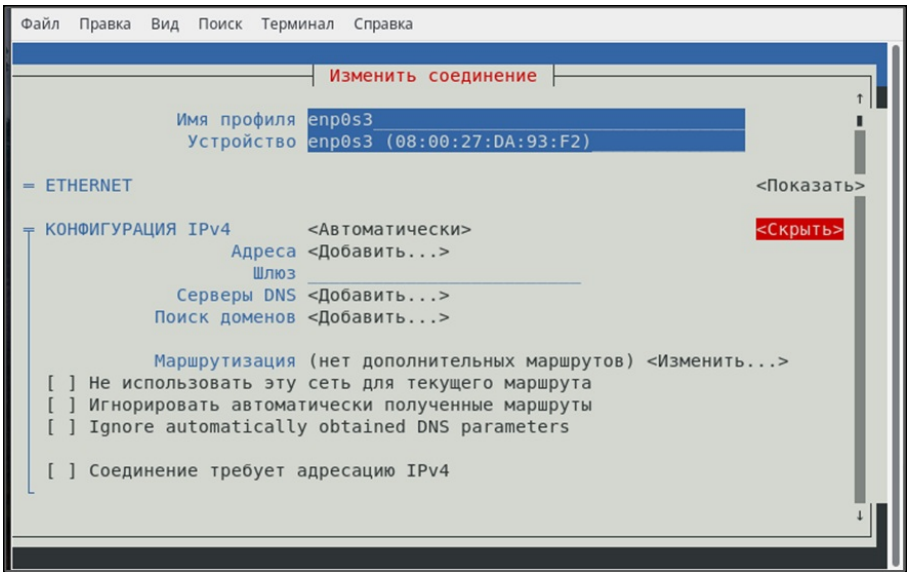
Выберите «Изменить соединение» клавишей **Enter**.



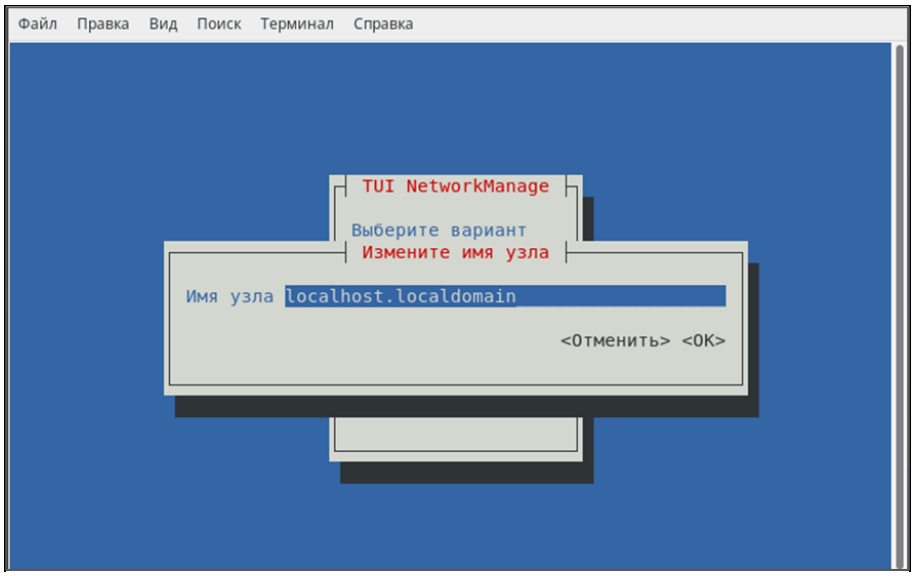
Выберите необходимый интерфейс и нажмите «Изменить...».



Определите список изменений.



Для изменения имени узла выберите «Измените имя узла». Введите новое имя и нажмите «OK».



Изменение через утилиту nmcli

nmcli - это инструмент командной строки для управления **NetworkManager** и создания отчетов о состоянии сети. Используется для создания, отображения, редактирования, удаления, активации и деактивации сетевых подключений, а также для контроля и отображения состояния сетевых устройств.

Чтобы узнать название интерфейса введите в командной строке:

```
nmcli con
```

В нашем случае интерфейс будет называться **eth0**.

```
nmcli con

NAME UUID TYPE DEVICE
eth0 3a2830fe-b8dd-45bd-b33e-387db796c8da ethernet eth0
```

Для того чтобы указать, что настройки должны быть получены от **DHCP**, используется команда:

```
nmcli con modify eth0 ipv4.method auto
```

Для использования ручных настроек необходимо ввести:

```
nmcli con modify eth0 ipv4.method static
```

Для того, чтобы указать статический адрес, используется команда:

```
nmcli con modify eth0 ipv4.address 192.168.0.1/24
```

Для того чтобы указать **dns**, используется команда:

```
nmcli connection modify eth0 ipv4.dns 202.131.124.4
```

Для того чтобы указать шлюз, используется команда:

```
nmcli connection modify eth0 IPv4.gateway 192.168.0.1
```

Чтобы настроить статический маршрут для существующего соединения **Ethernet**, используется команда:

```
nmcli connection modify eth0 +ipv4.routes "192.168.122.0/24 10.10.10.1"
```

Для остановки сетевой службы и её запуска доступны команды `nmcli networking off` и `nmcli networking on`.

Любое внесенное изменение также требует перезагрузки интерфейса для его применения.

Настройка сетевых соединений с помощью networkctl

Установка
Синтаксис
Опции
Команды
Запуск службы systemd-networkd
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: systemd-249.17-1

Networkctl — это инструмент для управления сетевыми устройствами и конфигурациями. Он позволяет пользователям получать информацию о состоянии сетевых интерфейсов и их конфигурации.

Установка

Для установки systemd-networkd выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install systemd-networkd
```

Запуск службы systemd-networkd

Для обеспечения корректной работы **networkctl** служба **systemd-networkd** должна быть запущена. Для запуска службы и добавления ее в автозагрузку выполните:

```
sudo systemctl enable systemd-networkd --now
```

Дальнейшая работа в программе производится с правами непривилегированного пользователя.

Проверить статус службы:

```
systemctl status systemd-networkd
```

Синтаксис

Утилита доступна для запуска через терминал с использованием команды следующего формата:

```
networkctl [<опции>] [<команды>]
```

Опции

Основные опции утилиты:

- **-h, --help** — вывод справки по использованию утилиты;
- **--version** — вывод версии утилиты;
- **--no-pager** — отключение постраничного вывода данных;
- **--no-legend** — отключение вывода условных обозначений;
- **-a, --all** — отображение всех интерфейсов, включая те, которые неактивны;
- **-s --stats** — показ статистики сетевых интерфейсов;
- **-l --full** — вывод подробной информации;

- **-n, --lines=[<число>]** — указание количества строк для отображения в журнале;
- **--json=pretty|short|off** — вывод информации в формате JSON.
  Возможные значения:
    - **pretty** — форматированный вывод;
    - **short** — сокращённый вывод;
    - **off** — отключение вывода в формате JSON.

Команды

Основные команды утилиты:

- **list [<шаблон>]** — отображает список сетевых интерфейсов и их статус;
- **status[<шаблон>]** — показывает статус сетевых каналов;
- **lldp [<шаблон>]** — отображает обнаруженных соседей по протоколу LLDP (Link Layer Discovery Protocol);
- **label** — отображает цифровые метки адресов, которые можно использовать для выбора адреса;
- **delete [<устройство>]** — удаляет виртуальные сетевые устройства;
- **up [<устройство>]** — активирует (поднимает) сетевое устройство;
- **down [<устройство>]** — выводит сетевое устройство из строя (отключает);
- **renew [<устройство>]** — обновляет динамические конфигурации устройства;
- **forcerenew [<устройство>]** — инициирует принудительную реконфигурацию устройства;
- **reconfigure [<устройство>]** — перенастраивает сетевые интерфейсы;
- **reload** — перезагружает файлы **.network** и **.netdev**, используется для применения изменений в конфигурации сети.

Примеры использования

> **Примечание.**
>
> Перед запуском **networkctl** убедитесь, что служба **systemd-networkd** запущена, в противном случае вы получите неполный вывод, о чем свидетельствует следующая ошибка:

```
WARNING: systemd-networkd is not running, output will be incomplete.
```

1. Отображение списка доступных сетевых соединений и их текущего состояния:

```
networkctl list
```

Команда **networkctl list** используется для отображения списка всех сетевых соединений и их соответствующих свойств, включая индекс интерфейса, состояние, тип, аппаратный адрес, драйвер и рабочее состояние.

Пример вывода:

```
IDX   LINK         TYPE           OPERATIONAL     SETUP
1     lo           loopback       carrier         unmanaged
2     enp0s3       ether          routable        unmanaged

2 links listed.
```

где:

- **IDX** — индекс сетевого интерфейса,
- **LINK** — название сетевого интерфейса,
- **TYPE** — тип сетевого интерфейса.
  Возможные значения:
    - **loopback** — интерфейс для обратной связи,
    - **ether** — Ethernet-интерфейс.
- **OPERATIONAL** — текущее рабочее состояние.
  Возможные значения:
    - **missing** — устройство отсутствует;

    - **off** — питание устройства отключено;
    - **no-carrier** — устройство включено, но ещё не подключено к оператору связи;
    - **dormant** — устройство подключено к оператору связи, но ещё не готово для передачи данных;
    - **degraded-carrier** — у главного интерфейса нет адреса, один из подчинённых сетевых устройств соединения или моста отключен;
    - **carrier** — все сетевые интерфейсы подчинены основному интерфейсу или мосту, связь установлена;
    - **degraded** — не все подчиненные сетевые интерфейсы подключены к оператору связи;
    - **enslaved** — интерфейс привязан к основному сетевому интерфейсу или мосту;
    - **routable** — интерфейс настроен и имеет главный или маршрутизируемый IP-адрес.

- **SETUP** — состояние настройки сетевого канала.
  Возможные значения:

    - **pending** — ссылка находится в процессе обработки;
    - **initialized** — ссылка успешно обработана;
    - **configuring** — ссылка настраивается;
    - **configured** — ссылка успешно настроена;
    - **unmanaged** — systemd-networkd не управляет этим интерфейсом;
    - **failed** — не удалось настроить ссылку;
    - **linger** — ссылка удалена, но ещё не удалена пользователем systemd-networkd.

2. Отображение общего состояния определённого сетевого канала:

```
networkctl status enp0s3
```

где:

- enp0s3 — название сетевого канала (интерфейса), для которого необходимо получить информацию.

Команда **networkctl status** предоставляет обзор всех сетевых каналов и связанных с ними свойств, включая активные **IP-адреса**, назначенный **DHCP-сервер**, шлюз и информацию **DNS**.

Пример вывода:

```
State: routable (unmanaged)
Address: 192.168.2.15 Gateway: 192.168.2.1
```

где:

- **State** — показывает текущее состояние сетевого канала;
- **Address** — отображает назначенный IP-адрес;
- **Gateway** — указывает шлюз по умолчанию.

3. Запуск сетевых устройств:

```
networkctl up enp0s3
```

Команда **networkctl up** используется для активации сетевого интерфейса.

4. Отключение сетевого устройства с временным выводом из эксплуатации:

```
networkctl down enp0s3
```

5. Обновление динамических конфигураций:

```
networkctl renew enp0s3
```

6. Перезагрузка файлов конфигурации:

```
networkctl reload
```

Если были внесены изменения в конфигурационные файлы сети (**.netdev** и **.network**), необходимо перезагрузить конфигурацию, чтобы изменения вступили в силу.

7. Перенастройка сетевых интерфейсов:

```
networkctl reconfigure enp0s3
```

Команда используется для применения изменений конфигурации к сетевому интерфейсу без его перезагрузки.

8. Просмотр логов службы **systemd-networkd** для диагностики и анализа проблем с сетью:

```
journalctl -u systemd-networkd.service
```

Настройка bonding с использованием инструмента nmcli

Bonding – это объединение двух и более сетевых интерфейсов в один логический для достижения отказоустойчивости или увеличения пропускной способности.

В таблице приведены возможные режимы работы утилиты **bond**.

Режим	Тип	Отказоустойчивость	Балансировка	Описание
mode=0	Round Robin	-	+	Циклический режим. Пакеты последовательно передаются и принимаются через каждый интерфейс один за другим.
mode=1	Active Backup	+	-	В этом режиме активен только один интерфейс, а все остальные интерфейсы находятся в резервном состоянии. Если активный интерфейс выходит из строя, резервный интерфейс заменяет его как единственный активный интерфейс в соединении. MAC-адрес интерфейса связи в режиме 1 виден только на одном порту на коммутаторе, что предотвращает путаницу для коммутатора.
mode=2	XOR [exclusive OR]	+	+	Один и тот же интерфейс работает с определённым получателем. MAC-адрес источника использует логику исключающего или (XOR) с MAC-адресом назначения.
mode=3	Broadcast	+	-	Широковещательный режим. Все пакеты отправляются на все интерфейсы.
mode=4	Dynamic Link Aggregation	+	+	IEEE 802.3ad, требует от коммутатора соответствующей настройки, к которому подключен объединенный интерфейс.
mode=5	Transmit Load Balancing (TLB)	+	+	Входящий трафик приходит только на активный интерфейс, а исходящий распределяется в зависимости от текущей загрузки канала каждого интерфейса. Не требует настройки коммутатора.
mode=6	Adaptive Load Balancing (ALB)	+	+	Адаптивная балансировка нагрузки. Отличается более совершенным алгоритмом балансировки нагрузки чем Mode-5. Обеспечивает балансировку нагрузки как исходящего, так и входящего трафика. Не требуется специальной поддержки и настройки со стороны коммутатора/коммутаторов.

Отобразите текущее состояние сетевых интерфейсов командой:

```
nmcli con

NAME    UUID                                  TYPE      DEVICE
enp0s3  d90e7109-6a41-3da8-b662-e8dbae914073  ethernet  enp0s3
enp0s8  17b8cbdb-df3f-31bd-bc82-cf4edb3205cd  ethernet  enp0s8
```

В выводе команды указано, что в системе присутствует две сетевые карты с именами **enp0s3** и **enp0s8**. В дальнейшем они будут связаны в один логический сетевой интерфейс (**Bond**).

Создание bond

Создайте интерфейс **bond0** с автоматическим получением адреса по **DHCP**:

```
nmcli con add type bond con-name bond0 ifname bond0 mode 802.3ad
```

Если же нужно присвоить статический адрес для **bond0**, то используйте команду:

```
nmcli con add type bond con-name bond0 ifname bond0 mode 802.3ad ip4 x.x.x.x/yy
```

Где:

- **x.x.x.x** – IPv4 адрес;
- **yy** – маска сети.

Выполните настройку **bond0** и назначьте ему необходимые параметры:

```
nmcli con mod id bond0 bond.options mode=802.3ad,miimon=100,lacp_rate=fast,xmit_hash_policy=layer2+3
```

Здесь:

- **mode=802.3ad** – назначение 4-ого режима работы **bond**;
- **miimon=100** - определяет, как часто производится мониторинг **MII** (Media Independent Interface). *0* – мониторинг отключён (используется по-умолчанию). Рекомендуемое значение *100 мс*;
- **lacp_rate=fast** – параметр может принимать два значения *slow* или *fast*. Данное значение определяет, через какой промежуток времени управляющие пакеты **LACPDU** отправляются по каналу **LACP**. По умолчанию значение установлено в *30 секунд* (*slow*). В

режиме *fast* – пакеты отправляются каждую секунду;

- **xmit_hash_policy=layer2+3** - определяет режим вычисления хешей при организации балансировки нагрузки между интерфейсами **bond**. Для вычисления хешей будут использоваться MAC адреса получателей/отправителей пакета и их IP адреса, если это возможно. Значение по умолчанию для этой опции – *layer2*, что определяет вычисление хеша только по MAC-адресам.

Удаление действующих подключений

Удалите действующие соединения интерфейсов **enp0s3** и **enp0s8**:

```
nmcli con del enp0s3
nmcli con del enp0s8
```

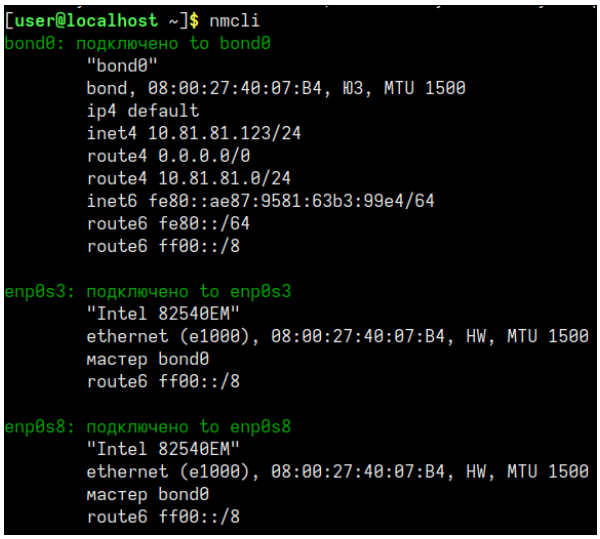
Связывание сетевых интерфейсов в bond

Выполните команды связывания сетевых интерфейсов **enp0s3** и **enp0s8** в **bond0**:

```
nmcli con add type bond-slave ifname enp0s3 con-name enp0s3 master bond0
nmcli con add type bond-slave ifname enp0s8 con-name enp0s8 master bond0
```

Информация о сетевых соединениях

Чтобы вывести результирующую информацию о сетевых настройках, выполните команду **nmcli**:



После завершения настройки проверьте, что интерфейс **bond0** активен и ошибок не обнаружено:

```
cat /proc/net/bonding/bond0

Ethernet Channel Bonding Driver: v5.15.72-1.el7.3.x86_64
Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
Peer Notification Delay (ms): 0

802.3ad info
LACP active: on
LACP rate: slow
Min links: 0
Aggregator selection policy (ad_select): stable
System priority: 65535
System MAC address: 08:00:27:40:07:b4
Active Aggregator Info:
Aggregator ID: 1
```

Number of ports: 1
Actor Key: 9
Partner Key: 1
Partner Mac Address: 00:00:00:00:00:00

Slave Interface: enp0s3
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:40:07:b4
Slave queue ID: 0
Aggregator ID: 1
Actor Churn State: none
Partner Churn State: churned
Actor Churned Count: 0
Partner Churned Count: 1
details actor lacp pdu:
  system priority: 65535
  system mac address: 08:00:27:40:07:b4
  port key: 9
  port priority: 255
  port number: 1
  port state: 77
details partner lacp pdu:
  system priority: 65535
  system mac address: 00:00:00:00:00:00
  oper key: 1
  port priority: 255
  port number: 1
  port state: 1

Slave Interface: enp0s8
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:21:5c:6a
Slave queue ID: 0
Aggregator ID: 2
Actor Churn State: churned
Partner Churn State: churned
Actor Churned Count: 1
Partner Churned Count: 1
details actor lacp pdu:
  system priority: 65535
  system mac address: 08:00:27:40:07:b4
  port key: 9
  port priority: 255
  port number: 2
  port state: 69
details partner lacp pdu:
  system priority: 65535
  system mac address: 00:00:00:00:00:00
  oper key: 1
  port priority: 255
  port number: 1
  port state: 1

Управление пропускной способностью сетевого интерфейса

Утилита ethtool
Установка
Синтаксис утилиты
Имя сетевого интерфейса
Настройки сетевой карты
Просмотр статистики интерфейса
Получение информации о драйвере
Изменение настроек сетевого интерфейса
Сохранение настроек
Идентификация порта сетевой карты

Утилита tc
Установка
Работа с утилитой
Ограничение скорости
Снятие ограничения скорости
Статус сетевой карты

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: ethtool-2:5.8-1, iproute-tc-4.15.0-2

Утилита ethtool

Ethtool – утилита настройки сетевых интерфейсов. Ethtool позволяет настраивать автоопределение сетевых настроек (*auto-negotiation*) сетевого интерфейса и изменять режимы (*полудуплексный*|*полнодуплексный*) из командной строки.

Автосогласование (Auto-Negotiation) – это механизм, с помощью которого устройство автоматически выбирает наиболее эффективный режим передачи на основе характеристик своих аналогов. Рекомендуется оставить автосогласование включенным, поскольку оно позволяет устройствам выбирать наиболее эффективные средства для передачи данных.

Полудуплексный режим (Half-duplex) позволяет устройству отправлять или получать пакеты по очереди. Устройство, установленное в этот режим, не может выполнять оба действия одновременно.

Когда режим устройства находится в *полнодуплексном* режиме (Full-duplex), оно может отправлять и получать пакеты одновременно.

Важно отметить, что **ethtool** работает только с физическими адаптерами, т.е. для виртуальных устройств просмотр и редактирование настроек недоступны.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ethtool
```

Синтаксис утилиты

Синтаксис утилиты имеет следующий вид:

```
ethtool [<параметры>] <имя_сетевого_интерфейса>
```

Основными параметрами утилиты являются:

- **--version** – версия утилиты;
- **-i, --driver** – информация о драйвере;

- **-P, --show-permaddr** – вывод физического MAC-адреса устройства. Может не совпадать с текущим при использовании bonding;
- **-p, --identify** – мигание светодиодом порта сетевой карты;
- **-r, --negotiate** – повторное согласование скорости передачи данных, если включено автоматическое согласование;
- **-S, --statistics** – вывод статистики;
- **-s, --change** – изменение настроек сетевого интерфейса. После перезагрузки настройки сбрасываются;
- **-k, --show-offload** – просмотр включенных технологий offload;
- **--reset** – сброс настроек различных компонентов сетевой карты, для сброса всех настроек используется all;
- **ethtool -h** – вывод справки о работе с утилитой.

Работа с утилитой

Имя сетевого интерфейса

Для получения имени сетевого интерфейса выполните:

```
ifconfig eno1: flags=4163  mtu 1500
        inet 10.60.60.202  netmask 255.255.255.0  broadcast 10.60.60.255
        inet6 fe80::21e:8cff:fef4:d0a5  prefixlen 64  scopeid 0x20
        ether 00:1e:8c:f4:d0:a5  txqueuelen 1000  (Ethernet)
        RX packets 8521042  bytes 4919999618 (4.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6512141  bytes 2746424253 (2.5 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xfe500000-fe520000
```

Настройки сетевой карты

Для получения текущих настроек сетевой карты выполните команду вида:

```
ethtool <имя_сетевого_интерфейса>
```

Например:

```
ethtool eno1

Settings for eno1:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        MDI-X: on (auto)
netlink error: Operation not permitted
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

Вывод команды показывает, что текущая скорость равна *1000 Мбит/с*, дуплекс находится в режиме «*Full*» и автосогласование

включено.

Просмотр статистики интерфейса

Для получения статистики сетевой карты выполните команду вида:

```
ethtool -S <имя_сетевого_интерфейса>
```

Например:

```
ethtool -S eno1

NIC statistics:
     rx_packets: 8527943
     tx_packets: 6515884
     rx_bytes: 4924517588
     tx_bytes: 2746866206
     rx_broadcast: 450774
     tx_broadcast: 9
     rx_multicast: 277235
     tx_multicast: 12177
     rx_errors: 0
     tx_errors: 0
     tx_dropped: 0
     multicast: 277235
     collisions: 0
...
```

Получение информации о драйвере

Для получения имени драйвера и вывода сопутствующей информации выполните команду вида:

```
ethtool -i <имя_сетевого_интерфейса>
```

Например:

```
ethtool -i eno1

driver: e1000e
version: 5.15.125-1.el7.3.x86_64
firmware-version: 0.13-4
expansion-rom-version:
bus-info: 0000:00:19.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: yes
```

Изменение настроек сетевого интерфейса

Для изменения настроек сетевой карты выполните команду вида:

```
ethtool -s [<имя_сетевого_интерфейса>] speed [10/100/1000] duplex [half/full] autoneg [on/off]
```

где:

- `speed [10/100/1000]` – требуемая скорость сетевого интерфейса;
- `duplex [half/full]` – режим дуплекса (полудуплексный/полнодуплексный);
- `autoneg [on/off]` — автосогласование (включено/выключено).

Например:

```
ethtool -s eno1 speed 100 duplex half autoneg on
```

Для проверки применения установленных настроек сетевой карты выполните команду вывода текущих настроек:

```
ethtool <имя_сетевого_интерфейса>
```

Сохранение настроек

По умолчанию установленные изменения в настройках сетевой карты будут сброшены после перезагрузки системы. Для сохранения внесенных изменений на постоянной основе необходимо отредактировать конфигурационный файл интерфейса устройства.

Для этого откройте файл интерфейса:

```
nano /etc/sysconfig/network-scripts/ifcfg-<имя_сетевого_интерфейса>
```

и в конце файла добавьте строку с нужными настройками:

```
ETHTOOL_OPTS="speed [100|1000|10000] duplex [half|full] autoneg [on|off]"
```

Сохраните изменения и закройте файл.

После перезагрузки системы внесенные настройки будут автоматически применяться для выбранного сетевого интерфейса.

Идентификация порта сетевой карты

Одной из полезных функций утилиты ethtool является возможность поиска физического расположения сетевого адаптера путем мигания светодиода устройства. Например, для мигания светодиодом устройства Ethernet eno1 можно использовать команду:

```
ethtool -p eno1 15
```

где `15` – продолжительность мигания светодиода в секундах.

Утилита tc

tc – консольная утилита для просмотра и конфигурирования параметров управления сетевым трафиком. Позволяет управлять классификацией трафика, дисциплинами управления очередями для различных классов трафика либо целиком для сетевого интерфейса.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install tc
```

Затем скачайте специальный установочный файл install.sh.

Работа с утилитой

Для вывода списка сетевых карт выполните:

```
ifconfig eno1: flags=4163  mtu 1500
        inet 10.60.60.202  netmask 255.255.255.0  broadcast 10.60.60.255
        inet6 fe80::21e:8cff:fef4:d0a5  prefixlen 64  scopeid 0x20
        ether 00:1e:8c:f4:d0:a5  txqueuelen 1000  (Ethernet)
        RX packets 8521042  bytes 4919999618 (4.5 GiB)
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6512141  bytes 2746424253 (2.5 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xfe500000-fe520000
```

Перед началом работы запустите скачанный ранее установочный файл **install.sh** для каждой сетевой карты, на которой будет регулироваться скорость, например:

```
/install.sh eno1

Для включения лимита выполните команду /sbin/eno1limiton.sh 1000 2000
Где 1000 - скорость отдачи, 2000 - скорость загрузки
Для отключения лимита выполните команду /sbin/eno1limitoff.sh
Для просмотра статуса ограничения скорости выполните команду /sbin/eno1limitstatus.sh
```

Ограничение скорости

Для включения ограничения скорости выполните команду вида:

```
/sbin/<имя_интерфейса>limiton.sh <скорость_отдачи> <скорость_загрузки>
```

Например:

```
/sbin/eno1limiton.sh 500 1000
cat /sbin/eno1limitstatus.sh

На сетевой карте eno1 установлено ограничение скорости на отдачу 500 килобит, на загрузку 1000 килобит
```

Снятие ограничения скорости

Для отключения ограничения скорости выполните команду вида:

```
/sbin/<имя_интерфейса>limitoff.sh
```

Например:

```
/sbin/eno1limitoff.sh
cat /sbin/eno1limitstatus.sh

На сетевой карте eno1 не установлено ограничение скорости
```

Статус сетевой карты

Для просмотра статуса сетевой карты выполните команду вида:

```
cat /sbin/<имя_интерфейса>limitstatus.sh
```

Например:

```
cat /sbin/eno1limitstatus.sh
```

Управление маршрутизацией

Управление маршрутизацией с помощью графической утилиты NetworkManager
Управление маршрутизацией с помощью утилиты route
Изменение таблицы маршрутизации

Окружение

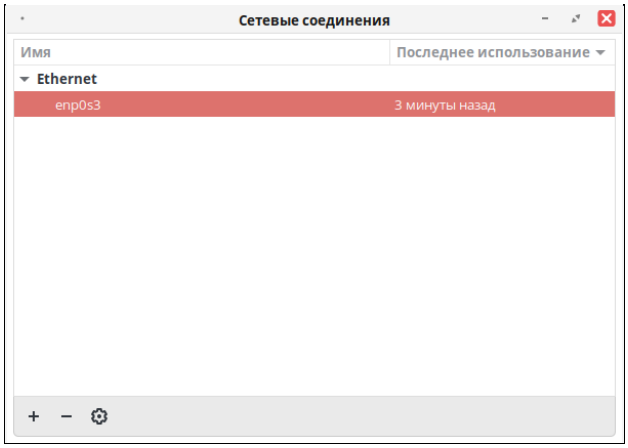
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: NetworkManager-1:1.32.12-1

Сетевые маршруты необходимы для перенаправления пакетов, передаваемых по сети, таким образом, чтобы они могли достигнуть конечной цели. Маршруты можно настраивать на уровне интерфейса или маршрутизатора.

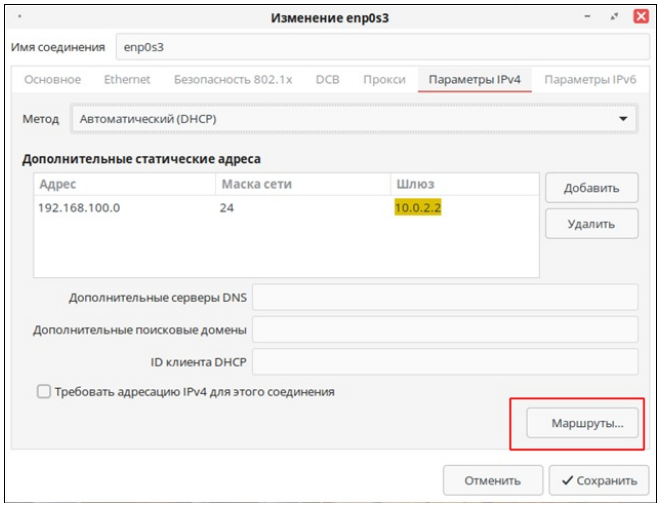
Когда компьютеру необходимо отправить пакет в сеть, он проверяет таблицу маршрутизации; в ней указаны IP-адреса пунктов назначения и адреса интерфейсов и роутеров в сети, которые могут отправить пакет по нужному адресу. Если для конечной цели маршрут не указан, используется так называемый шлюз по умолчанию или маршрут по умолчанию. Точно такой же принцип используется в роутере – устройство смотрит на IP-адрес назначения, сверяет его со своей таблицей маршрутизации и отправляет далее по маршруту.

Управление маршрутизацией с помощью графической утилиты NetworkManager

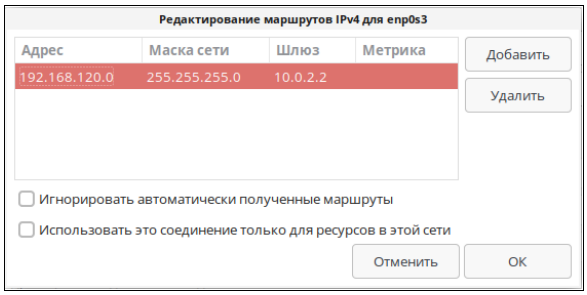
Для добавления новых маршрутов необходимо открыть панель управления сетью, для этого в системном трее нажмите ПКМ на значок сети и выберите пункт «Изменить соединение». Будет открыто окно «Сетевые соединения».



Выберите интерфейс, который необходимо настроить. Перейдите на вкладку «Параметры IPv4». На этой вкладке можно перейти к настройке маршрутов, нажав на кнопку «Маршруты».



Будет открыто окно для настройки и редактирования маршрутов. Создать новый маршрут можно с помощью кнопки «Добавить».

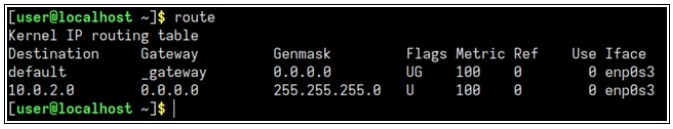


Управление маршрутизацией с помощью утилиты route

Утилита **route** помогает просматривать и вносить изменения в сетевые маршруты в операционной системе. Она также отображает маршруты, которые были добавлены с помощью графической утилиты **NetworkManager**.

Для того чтобы посмотреть правила маршрутизации, достаточно выполнить команду:

```
route
```



Для того чтобы вывести все строки таблицы в цифровом формате, можно выполнить команду:

```
route -n
```

Изменения таблицы маршрутизации

В общем случае прототипом команды **route** является следующая запись:

```
route add [-net|-host] <IP/Net> netmask <Netmask> gw <Gateway_IP> dev <Int>
```

где:

- **-net** – используется для добавления правила для всей подсети;
- **-host** – используется для добавления правила для одного адреса;
- **<IP/Net>** – адрес объекта назначения;
- **<Netmask>** – маска объекта назначения;
- **<Gateway IP>** – адрес шлюза, через который будет проложен маршрут до объекта назначения;
- **<Int>** – интерфейс, который будет использоваться при обработке пакетов.

> **Примечание.**
>
> Команду для добавления маршрута необходимо выполнять с правами **администратора** системы.

Таким образом, команда для добавления маршрута для подсети будет выглядеть следующим образом:

```
route add -net 192.168.100.0 netmask 255.255.255.0 gw 192.168.122.3 dev enp0s3
```

В сокращенном виде:

```
route add -net 192.168.100.0/24 gw 192.168.122.3 dev enp3s0
```

Команда для добавления маршрута только для определенного хоста будет выглядеть следующим образом:

```
route add -host 192.168.1.122 gw 192.168.122.1 dev enp3s0
```

При добавлении правила для хоста маску можно не указывать, она автоматически будет равна **255.255.255.255**.

Для удаления маршрута можно воспользоваться следующей командой с указанием объекта назначения:

```
route del -net 192.168.100.0/24 gw 192.168.122.3 dev enp3s0
route del -host 192.168.1.122 gw 192.168.122.1 dev enp3s0
```

Добавленные с помощью утилиты **route** маршруты будут активны только до перезагрузки системы, после перезагрузки они будут автоматически удалены. Чтобы маршруты сохранились, их необходимо добавить в файл конфигурации.

Для этого потребуется добавить значения маршрута в конфигурационный файл используемого интерфейса:

```
nano /etc/NetworkManager/system-connections/<имя_интерфейса>.nmconnection
```

В секцию [ipv4] конфигурационного файла следует добавить информацию о маршруте. Например:

```
route1=192.168.1.0/24,192.168.0.4
```

где:

- 192.168.1.0 – это адрес сети;
- 192.168.0.4 – это адрес маршрутизатора, который будет использоваться для доступа к данной сети.

Пример содержимого конфигурационного файла с добавленным маршрутом:

```
nano /etc/NetworkManager/system-connections/enp3s0.nmconnection
```

```
[connection]
id=enp3s0
uuid=800eab29-0d08-3b42-aeaf-9dc1219aca14
type=ethernet
autoconnect-priority=-999
interface-name=enp3s0
timestamp=1713466837

[ethernet]

[ipv4]
method=auto
route1=192.168.1.0/24,192.168.0.4

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

После добавления информации о маршрутах потребуется перезагрузить систему для применения внесенных изменений.

Настройка Wi-Fi в РЕД ОС

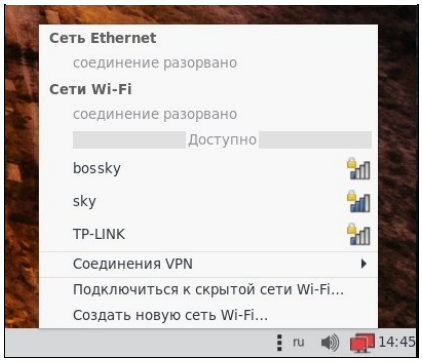
Пример подключения
Использование консольных утилит
Решение проблем с Wi-Fi
Получение информации об устройстве
Поиск и установка драйвера
Подключение к скрытой сети Wi-Fi

В данной статье будет рассмотрено подключение РЕД ОС к сети **Wi-Fi** — технологии беспроводной локальной сети.

Подключение осуществляется посредством сетевого адаптера *Wi-Fi*, который может быть установлен в вашем ноутбуке или стационарном ПК.

Для работы *Wi-Fi* адаптера требуются соответствующие драйверы. В РЕД ОС имеется поддержка большинства таких устройств.

При успешном обнаружении системой *Wi-Fi* адаптера, при нажатии на значок сетевого подключения, можно увидеть список доступных беспроводных сетей.



Здесь отображаются названия сетей и уровень сигнала точек доступа, значок замка на пиктограмме уровня сообщает, что доступ к сети защищён паролем.

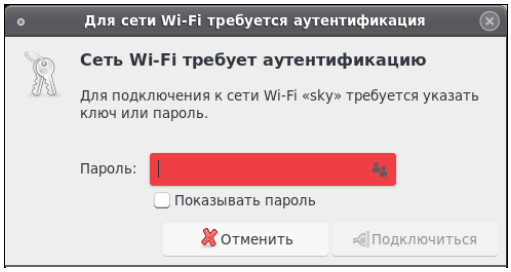
Вы можете подробнее ознакомиться с настройкой **Wi-Fi**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка Wi-Fi в РЕД ОС;
- в **Яндекс.Дзен** — Настройка Wi-Fi в РЕД ОС;
- в **VK Видео** — Настройка Wi-Fi в РЕД ОС.

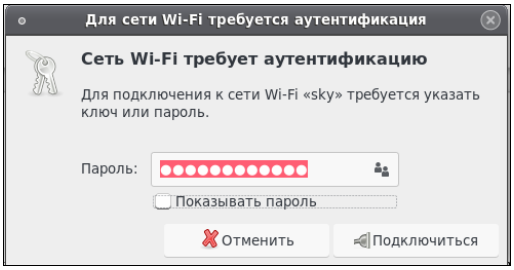
На наших каналах вы также сможете найти много другой полезной информации.

Пример подключения

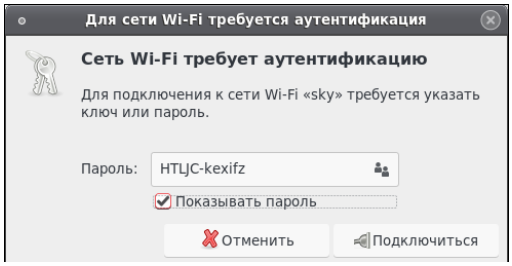
Далее будет рассмотрен пример подключения к одной из сетей.



Выберите любую из доступных сетей, введите пароль для подключения к точке доступа беспроводной сети.

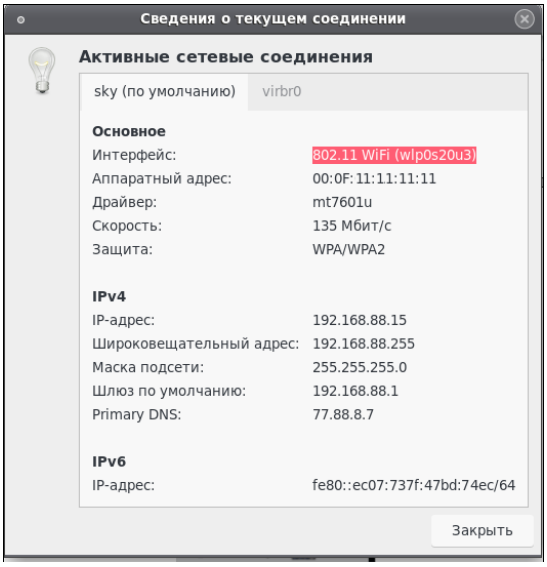


При необходимости выберите «**Показать пароль**» и проверьте правильность его написания.



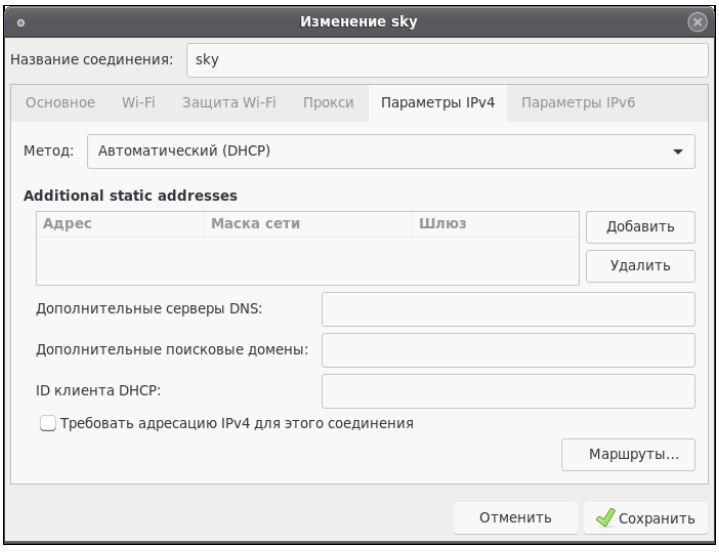
При успешном подключении в системном трее появится соответствующий значок ().

Если нажать правой кнопкой мыши по значку и выбрать в меню «**Сведения о соединении**», откроется окно, в котором будет показана информация о сетевом подключении.

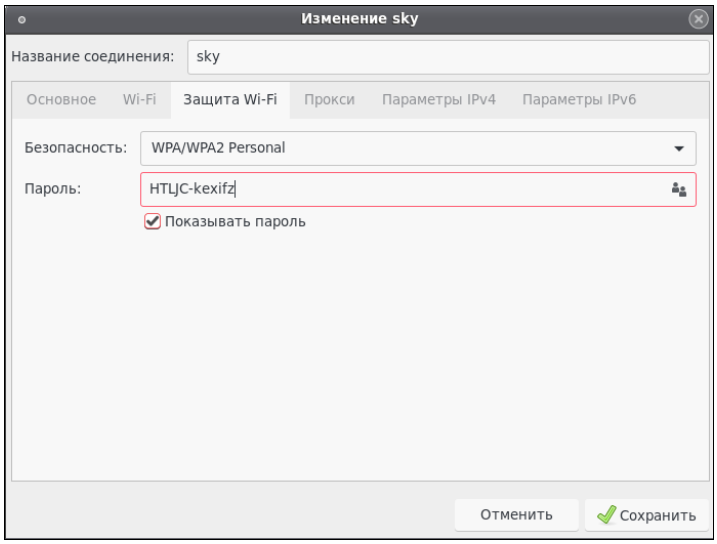


Здесь можно просмотреть такие параметры, как MAC-адрес устройства, используемый драйвер (в данном случае — это **mt7601u**), скорость подключения, тип защиты (WPA/WPA2), а также IP-адрес, сетевую маску, шлюз и прочие параметры.

Как и при проводном соединении имеется возможность редактировать различные сетевые параметры Wi-Fi соединения.



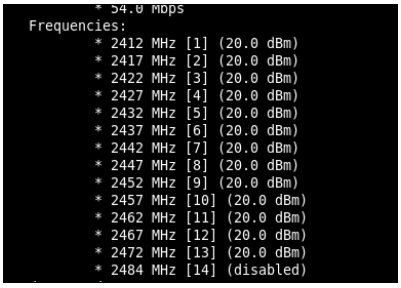
Если необходимо посмотреть пароль текущего Wi-Fi подключения, перейдите на вкладку «**Защита Wi-Fi**» и нажмите «**Показать пароль**».



Использование консольных утилит

Также информацию о сетевом Wi-Fi адаптере можно просмотреть с помощью консольных утилит. Одна из них — это утилита **iw**.

iw list — команда показывает информацию о Wi-Fi адаптере, например, радиочастоты, поддерживаемые вашей Wi-Fi картой.



В данном примере беспроводной адаптер поддерживает радиочастоты 2.4 ГГц. Существуют адаптеры, которые работают с диапазоном 5 ГГц, что позволяет заметно увеличить пропускную способность сетевой карты.

Команда iw monitor отображает, что происходит на уровне межсетевого протокола, например, как IP-адреса присваиваются сетевому интерфейсу, и какие маршруты прописываются в системе. Во время запуска программы можно попробовать подключиться к точке доступа, в выводе будут отображены результаты ваших действий.

iw event — команда выводит перечень беспроводных событий, связанных с Wi-Fi интерфейсом. Во время запуска команды можно попробовать подключиться к другой сети Wi-Fi, в выводе будут отображены результаты ваших действий.

iw dev — отображает сведения о текущем соединении, в выводе можно узнать название сети (SSID), а также номер канала и радиочастоту, на которой работает Wi-Fi. **SSID** (*Service Set Identifier*) – идентификатор беспроводной сети.

```
iw dev

phy#0
    Interface     wlp0s20u3
                ifindex 3 wdev 0x1
                addr 00:0f:11:11:11:11
                ssid sky
                type managed
                channel 9 (2452 MHz), width: 40 MHz, center1: 2462 MHz
```

Решение проблем с Wi-Fi

В некоторых ноутбуках присутствует аппаратный переключатель питания беспроводной карты и не исключается случай, когда карта может быть заблокирована ядром Linux. С помощью следующей команды проверьте текущий статус:

```
rfkill list

1: phy1:  Wireless LAN
        Soft blocked: no
```

```
        Hard blocked: no
```

В выводе указано, что аппаратная и программная блокировка не используется. Об этом свидетельствуют значения: «Soft blocked: **no**» и «Hard blocked: **no**».

Если в выводе данной команды будет отображаться «Hard blocked: **Yes**», тогда для снятия блокировки используйте аппаратную кнопку/переключатель на вашем устройстве (ноутбуке).

В случае отображения в выводе «Soft blocked: **Yes**» — выполните команду разблокировки:

```
rfkill unblock wifi
```

Если система все так же не видит доступные беспроводные сети, то существует высокая вероятность, что в ОС отсутствует Wi-Fi драйвер для данной модели устройства. Это могло произойти из-за того, что РЕД ОС установлен на компьютер с новым Wi-Fi модулем, который появился в продаже уже после выхода релиза РЕД ОС и драйвера для данной модели беспроводного устройства не были включены в ОС.

В данном случае разработчиками РЕД ОС добавляются драйвера для новых Wi-Fi чипов в репозиторий программного обеспечения РЕД ОС.

Однако может возникнуть проблема — как получить доступ к сети Интернет для загрузки нужного драйвера, если Wi-Fi не работает.

Самое простое решение — это настроить проводную сеть (при наличии). Если на ПК нет проводной сетевой карты, можно использовать смартфон, подключенный по USB, который в системе отобразится либо как USB-модем, либо как сетевой USB-адаптер.

Если никакой из перечисленных вариантов не поможет настроить доступ в Интернет, тогда необходимо узнать информацию об используемом устройстве (см. п. «Получение информации об устройстве»). Собранную информацию можно передать в ТП РЕД ОС, после ее анализа специалист ТП отправит нужный драйвер для установки.

Получение информации об устройстве

Определите модель Wi-Fi устройства и установите драйвера из репозитория РЕД ОС. Для этого используйте команду:

```
lspci -nn

00:00.0 Host bridge: Intel Corporation Device 9b63 (rev 03)
00:02.0 VGA compatible controller: Intel Corporation Device 9bc8 (rev 03)
00:12.0 Signal processing controller: Intel Corporation Device 06f9
00:14.0 USB controller: Intel Corporation Device 06ed
00:14.2 RAM memory: Intel Corporation Device 06ef
00:14.3 Network controller: Intel Corporation Device 06f0
00:16.0 Communication controller: Intel Corporation Device 06e0
00:16.3 Serial controller: Intel Corporation Device 06e3
00:17.0 SATA controller: Intel Corporation Device 06d2
00:1b.0 PCI bridge: Intel Corporation Device 06c0 (rev f0)
00:1c.0 PCI bridge: Intel Corporation Device 06bd (rev f0)
00:1f.0 ISA bridge: Intel Corporation Device 0687
00:1f.3 Multimedia audio controller: Intel Corporation Device 06c8
00:1f.4 SMBus: Intel Corporation Device 06a3
00:1f.5 Serial bus controller [0c80]: Intel Corporation Device 06a4
00:1f.6 Ethernet controller: Intel Corporation Device 0d4c
01:00.0 Non-Volatile memory controller: Device 1e0f:0001
02:00.0 Unassigned class [ff00]: Realtek Semiconductor Co., Ltd. RTS522A PCI Express Card Reader (rev 01)
```

Команда lspci выводит информацию обо всех PCI-шинах и устройствах на них.

В примере в выводе команды присутствуют две строки с текстом **Ethernet controller** и **Network controller**, это говорит о том, что в компьютере имеется две сетевые карты. Также можно заметить, что в конце строки указаны их идентификаторы (**0d4c** и **06f0**) . Данные идентификаторы будут использоваться для определения драйвера, который нужно установить.

Если используется **USB** Wi-Fi модуль, то для определения идентификатора устройства можно применить команду lsusb.

```
lsusb

Bus 002 Device 002: ID 8087:8000 Intel Corp.
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 8087:8008 Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 004: ID 148f:7601 Ralink Technology, Corp. MT7601U Wireless Adapter
```

```
Bus 003 Device 003: ID 046d:c077 Logitech, Inc. M105 Optical Mouse
```

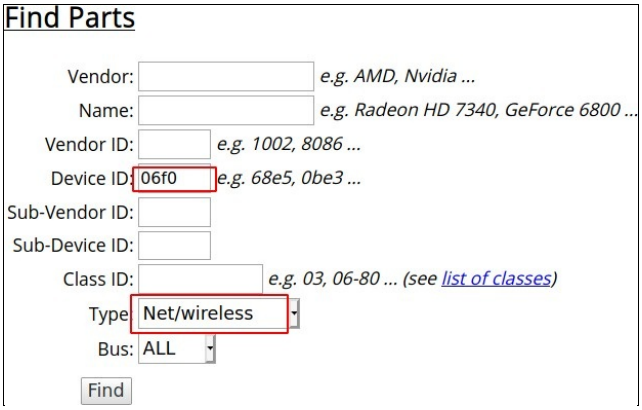
Здесь:

- **148f** — это **Vendor ID**;
- **7601** — это **Device ID**.

Поиск и установка драйвера

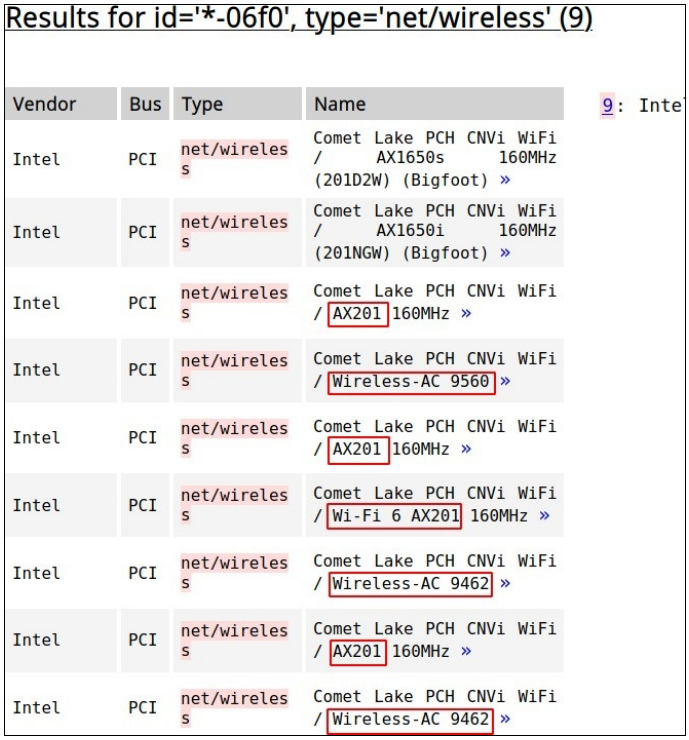
Перейдите на сайт https://linux-hardware.org — этот портал содержит информацию об оборудовании компьютеров под управлением Linux.

Откройте раздел **Find Parts**.



В поле **Device ID** укажите идентификатор первого сетевого устройства из вывода lspci.

В поле **Type** выберите «**Net / wireless**» — это означает, что поиск будет осуществляться только по устройствам с беспроводным сетевым интерфейсом (Wi-Fi). Нажмите на кнопку «**Find**», будут выведены следующие результаты поиска:



Ваш результат поиска может отличаться от приведенного в примере, он зависит от модели беспроводного устройства.

В данной таблице устройствам с идентификатором **06f0**, соответствуют Wi-Fi адаптеры производства Intel: **Wi-Fi AX201** и **Wireless-AC 9462**.

Попробуйте найти в репозитории РЕД ОС Wi-Fi устройство по имени из этой таблицы:

```
dnf search AX201
```

```
[user@rfc1918 ~]$ yum search AX201
Загружены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
================================================================= N/S matched: AX201 ==================
iwl7260-firmware.noarch : Firmware for Intel(R) Wireless WiFi Link 726x/8000/9000/AX200/AX201 Series Adapters
```

Это означает, что нужно установить данный пакет. Для этого воспользуйтесь командой:

```
dnf install iwl7260-firmware
```

После установки драйвера проверьте беспроводное сетевое подключение.

Кроме этого компьютеры могут поставляться с Wi-Fi адаптерами, которые используют, например, драйвера **Realtek**. В репозитории РЕД ОС имеются драйвера и для них.

Установка драйвера производится командой:

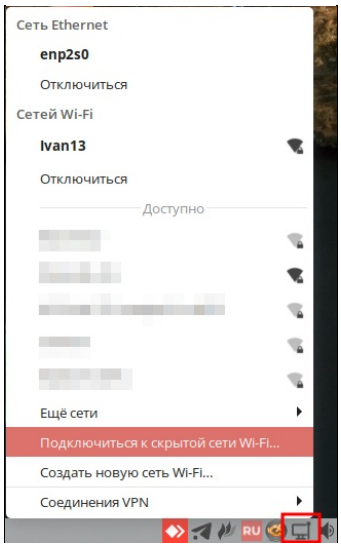
```
dnf install rtl<модель_адаптера>
```

Рассмотренный в статье метод поиска и установки Wi-Fi драйвера может быть применен не только к беспроводным модулям, но и, по аналогии, к другим устройствам.

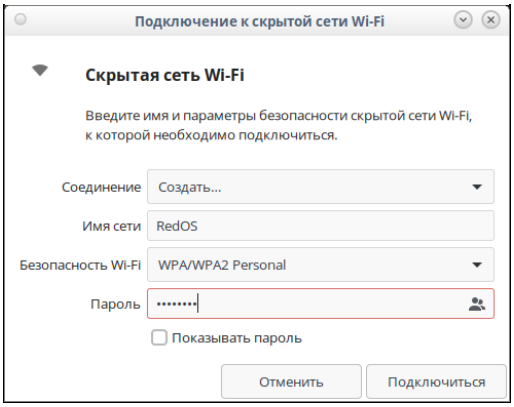
Подключение к скрытой сети Wi-Fi

Подключение к скрытой сети Wi-Fi в графической оболочке Mate

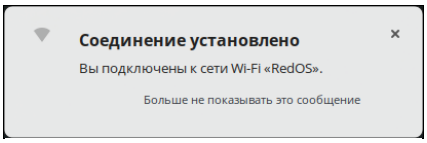
Для подключения к *скрытой сети wi-fi* в графической оболочки *Mate* нажмите ПКМ на значок сети в системном трее и выберите пункт «**Подключиться к скрытой сети Wi-Fi**».



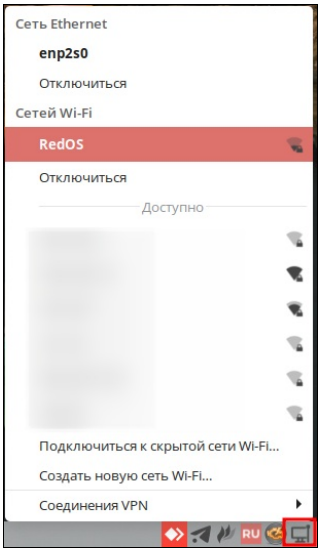
В открывшемся окне заполните поля «**Соединение**», «**Имя сети**», «**Безопасность Wi-Fi**» и «**Пароль**» и нажмите кнопку «**Подключиться**».



При успешном подключении будет выведено соответствующее сообщение.

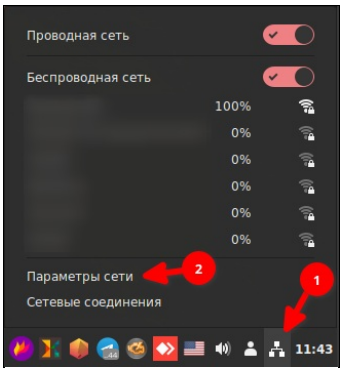


Также, нажав ПКМ на значок сети в системном трее, можно просмотреть доступные сети и текущие сетевые соединения.

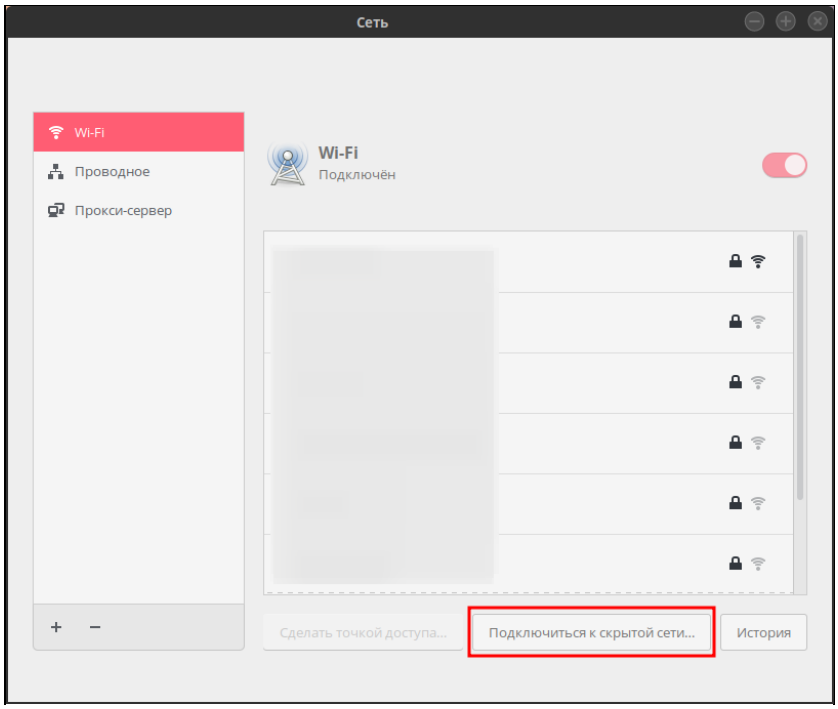


Подключение к скрытой сети Wi-Fi в графической оболочке Cinnamon

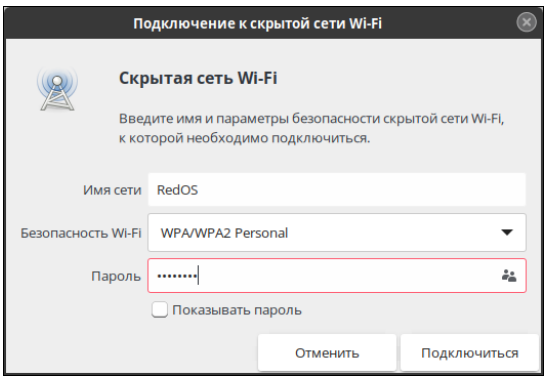
Для подключения к *скрытой сети wi-fi* в графической оболочке *Cinnamon* нажмите ЛКМ на значок сети в системном трее и выберите пункт «**Параметры сети**».



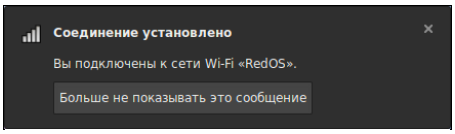
Будет открыто окно настройки сети. В разделе Wi-Fi нажмите кнопку «**Подключиться к скрытой сети...**».



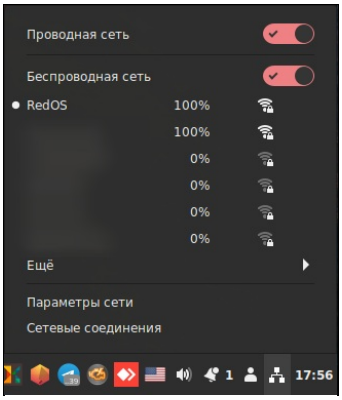
В открывшемся окне «**Подключение к скрытой сети Wi-Fi**» заполните поля «**Имя сети**», «**Безопасность Wi-Fi**» и «**Пароль**» и нажмите кнопку «**Подключиться**».



При успешном подключении будет выведено соответствующее сообщение.



Также, нажав ЛКМ на значок сети в системном трее, можно просмотреть доступные сети и текущие сетевые соединения.



Основные понятия squid

Централизованный выход в Интернет через один сервер в сети (proxy)

В корпоративных сетях является стандартной ситуация, когда, с одной стороны, множество пользователей на разных компьютерах пользуются ресурсами сети Интернет, при этом обеспечить надлежащий уровень безопасности на этих компьютерах одновременно довольно сложно. Ещё сложнее заставить пользователей соблюдать некий «корпоративный стандарт», ограничивающий возможности использования Интернет (например, запретить использование определённого типа ресурсов или закрыть доступ к некоторым адресам).

Простейшим решением будет разрешить только определённые методы доступа к Интернет (например, по протоколам HTTP и FTP) и определить права доступа абонентов на одном сервере, а самим абонентам разрешить только обращение к этому серверу по специальному прокси-протоколу (поддерживается всеми современными браузерами). Сервер же, после определения прав доступа, будет транслировать (проксировать) приходящие на него HTTP-запросы, направляя их адресату. Допустим, несколько пользователей с нескольких компьютеров внутренней сети просматривают некоторый сайт. С точки зрения этого сайта их активность представляется потоком запросов от одного и того же компьютера.

Обычный доступ

Непосредственно после установки Squid уже поддерживает функции прокси, но принимает соединения только с того компьютера, на который установлен. Для того, чтобы можно было воспользоваться этим сервисом с других компьютеров, необходимо изменить т. н. таблицы управления доступом (Access Control Lists, далее ACL), находящиеся, как и большинство настроек **Squid**, в файле **/etc/squid/squid.conf**. Файл этот снабжён подробными комментариями и примерами по всем настройкам в виде комментариев, например, так:

```
# TAG: <некоторая_настройка>
```

Таким же образом там описаны все значения, выставленные по умолчанию. В частности, для того, чтобы **Squid** принимал соединения из всей внутренней сети, необходимо раскомментировать две строки, и подставить в них действительный диапазон адресов вашей сети:

```
acl our_networks src 192.168.1.0/24 192.168.2.0/24
http_access allow our_networks
```

Следует иметь в виду, что при обработке запроса на доступ к **Squid** все строки **http_access** файла **squid.conf** просматриваются последовательно сверху вниз до первой строки, соответствующей параметрам запроса. Это означает, что важен порядок следования строк **http_access**.

Анонимизирующий доступ

При использовании прокси-сервера остаётся некоторая угроза безопасности, связанная с тем, что топология внутренней сети и активность её абонентов не маскируются. Например, в протоколе HTTP используются т.н. заголовки (**headers**), значения которых заполняются браузерами при отправлении запроса. **Squid** умеет удалять опасные поля заголовка из запроса при помощи настройки **header_access** или подменять их значения на другие, заранее заданные, при помощи настройки **header_replace**. Варианты использования этих настроек приведены в squid.conf в районе **TAG: header_access** и **TAG: header_replace**, соответственно.

Имейте в виду, что из-за удаления и/или подмены полей заголовков может нарушиться связь с некоторыми системами, использующими значение этих полей для организации взаимодействия и авторизации.

«Прозрачный» доступ

Можно вообще не сообщать пользователям сети, что в ней используется прокси-сервер. Если прокси-сервер - одновременно и маршрутизатор, весь сетевой трафик в любом случае его не обойдёт. При этом можно средствами межсетевого экрана все обычные HTTP-запросы к удалённым серверам перенаправлять на вход особым образом настроенного **Squid**. С внешней стороны это будет выглядеть обычным прокси-сервером, а со стороны пользователя — ничем не будет отличаться от обычной работы в сети. Команда **iptables**, перенаправляющая HTTP-запросы к внешним серверам на порт **Squid** может, например, выглядеть так:

```
iptables -t NAT -A PREROUTING -d ! <адрес_самого_сервера> \
-i <внутренний_сетевой_интерфейс> -p tcp -m tcp --dport 80 \
-j REDIRECT --to-ports 3128
```

Или так:

```
iptables -t nat -A PREROUTING -p tcp -d 0/0 --dport www \
-i <внутренний_сетевой_интерфейс> -j DNAT \
```

```
--to <локальный_адрес_на_котором_слушает_прокси>:3128
```

Настройка **squid.conf** при этом использует обратное проксирование, описанное ниже. Как сказано в документации по **Squid**, для организации прозрачного прокси достаточно добавить в **squid.conf** строку:

```
http_port 80 intercept
```

Фильтрация доступа

В **Squid** существует гибкая схема фильтрации внешних ссылок. С её помощью, например, можно закрыть доступ к определённым сайтам и ресурсам на них, избавиться от навязчивой рекламы (**banners**), ссылок непристойного содержания и т. п. Содержимое фильтруется с помощью всё тех же ACL и настроек **http_access deny**, примеры которых приведены в **squid.conf**.

Обратите внимание, что при задании фильтруемого URL или доменного имени сервера можно использовать регулярные выражения, таким образом в одной строке определяя фильтр для целого класса адресов или доменных имён. Подробнее о регулярных выражениях можно прочитать в руководстве **regex**. Запрет доступа к домену **baddomain.com**, например, можно оформить в виде строк

```
acl Bad dstdomain baddomain.com
http_access deny Bad
```

Заметим также, что **http_access deny Bad** следует помещать перед строками вида **http_access allow**, в этом случае доступ к любому сайту домена будет закрыт безусловно.

Авторизация доступа

В **Squid** есть возможность определять различные ACL разным пользователям и/или категориям пользователей. Если для определения того, какой именно пользователь подключается к серверу, недостаточно IP-адреса его компьютера, следует воспользоваться одной из многих схем авторизации, принятых в Squid. Авторизация конфигурируется с помощью тега **TAG: auth_param**. Посмотреть, какие схемы (программы) авторизации поддерживает **Squid**, можно в каталоге **/usr/lib/squid**.

Например, настройка авторизации в LDAP может выглядеть так:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b ou=People,dc=office,dc=lan -f (uid=%s) -h ldap.office.lan auth_param basic children 5
auth_param basic realm Squid proxy-caching web server auth_param basic credentialsttl 2 hours
```

Информацию по настройке той или иной программы авторизации можно почерпнуть из соответствующих руководств.

Локальное хранение данных, которые уже запрашивались пользователями (cache)

Не менее важное свойство **Squid** состоит в том, что данные, полученные по запросам из сети Интернета, сохраняются в системе (кешируются). При повторных запросах данные будут предоставляться не из сети Интернет, а из сохранённой копии. Объекты кешируются до тех пор, пока не истечёт их «срок годности» или пока они не будут вытеснены другими, более часто используемыми. Например, если все пользователи внутренней сети одновременно работают с одним и тем же сайтом в сети, общий поток запросов от **Squid** будет несравненно меньше потока пользовательских запросов, так как большинство ресурсов сайта уже будет находиться в кеше.

Обычное кеширование

Непосредственно после установки сервера он уже выполняет кеширующие функции. Кеширование позволяет не только сэкономить на оплате трафика, но и уменьшить время доступа к ресурсам Интернет. Однако следует понимать, что снижение внешнего трафика возможно только если один и тот же ресурс был запрошен несколькими пользователями на протяжении некоторого промежутка времени. Если пользовательские запросы почти не пересекаются, снижение трафика может быть незначительным.

Кроме того, кеширование неэффективно в ситуации, когда повторный запрос на большинство объектов приходит уже после того, как эти объекты вытесняются из кеша более новыми. Если анализ статистики показывает, что происходит именно это, можно попробовать увеличить объём кешируемой информации. Настройки **Squid**, отвечающие за размер кеша, приведены в файле **squid.conf** в разделе, начинающемся словами **OPTIONS WHICH AFFECT THE CACHE SIZE**.

Наконец, кеширование входного потока данных делает невозможной “справедливую” оплату различными пользователями их собственного трафика. Например, если один пользователь посещает некие сайты по совету другого, то его трафик будет по большей части не выходить за пределы сервера, на котором ресурсы этих сайтов уже - по милости первого пользователя - закешированы.

Выборочное кеширование

Некоторые данные (например, очень большие файлы, автоматически изменяемые WWW-страницы, звуки и т. п.) кешировать невыгодно: вероятность повторного запроса в течение “срока годности” низкая, а других объектов вытесняется много. С другой стороны, содержимое некоторых сайтов может понадобиться кешировать в обязательном порядке (например, для ускорения доступа). Эти свойства управляются, как обычно, при помощи ACL и настроек **always_direct** (без кеширования) и **never_direct** (обязательное кеширование).

Например, чтобы предотвратить кеширование файлов, получаемых по протоколу FTP (это, как правило, разумно), необходимо в соответствующем месте **squid.conf** раскомментировать строки:

```
acl FTP proto FTP
always_direct allow FTP
```

Иерархия серверов

Если запрашиваемый ресурс не найден в локальном кеше **Squid**, он может попытаться запросить его у «вышестоящих» серверов или у «соседей» - вместо того, чтобы обращаться в Интернет. Таким вышестоящим сервером (**parent peer**) может быть сервер провайдера, а соседом (**sibling peer**) - сервер абонента, подключённого к тому же провайдеру. Правила передачи объектов кеша и формирования иерархии серверов описаны в документации **Squid**. Раздел конфигурационного файла, отвечающий за механизм обмена кешем, начинается словами **OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM**.

Необходимо знать, что обмен содержимым кеша требует непременной авторизации доступа между серверами (во избежание подлогов и другого вида атак). Все параметры соединения сервера с сервером (настройка **cache_peer**) записываются в текстовом виде, включая пароли, так что следует строго ограничить доступ к файлу настройки **squid.conf**.

Обратное проксирование и кеширование внутренних серверов (accelerate)

Кеширующие и проксирующие способности **Squid** можно использовать и «в обратную сторону», пропуская через сервер входящие запросы на внутренние серверы. Таким образом, можно скрыть реальное расположение и структуру серверов, и уменьшить нагрузку на них.

Обычное обратное проксирование (один сервер)

В режиме **accelerate** сервер сам принимает извне HTTP-запросы, адресованные, как правило на 80-й порт. Кроме того, необходимо указать имя сервера и порт, на который будут проксироваться запросы. Это можно сделать, например, так:

```
http_port 80 defaultsite=internal.www.com
cache_peer 192.168.1.1 parent 80 0 no-query originserver
```

Если необходимо как-то ограничить доступ к внутреннему серверу, это легко сделать, применив соответствующие ACL.

Множественное проксирование

Для обратного проксирования нескольких внутренних серверов необходимо, чтобы внешние запросы на сайты с разными доменными именами попадали на вход **Squid**, который бы ставил в соответствие каждому имени действительный адрес сервера во внутренней сети и перенаправлял бы запрос туда. Делается это с помощью механизма виртуальных хостов. Вот как, например, можно организовать прокси для двух серверов, **www1.foo.bar** и **www2.foo.bar**, адреса которых в DNS указывают на машину со Squid-сервером (файл **/etc/squid/squid.conf**):

```
http_port 80 defaultsite=www1.foo.bar vhost
hosts_file /etc/hosts
```

Настройка **defaultsite** нужна серверу для заполнения HTTP-заголовков. Соответствие доменных имён адресам серверов во внутренней сети разумно получать из стандартного файла **/etc/hosts**:

```
10.0.0.1    www1.foo.bar
10.0.0.2    www2.foo.bar
```

Множественное обратное проксирование имеет важный побочный эффект. В сетях, подключённых к Интернету постоянно, нередки случаи, когда недобросовестные администраторы внутренних сайтов регистрируют их в других доменах и используют их в качестве

хостинг-платформ, часто с документами незаконного или нецензурного содержания.

Допустим, сайт **www1.foo.bar** также зарегистрирован как www.verycoolwarez.com, и по этому адресу доступны контрафактные версии программ и т. п. В обычном случае для обнаружения этого факта необходимо анализировать трафик, делать внушение администратору **www1.foo.bar** и т.д. При использовании обратного проксирования такого вообще не может произойти без договорённости с администратором **Squid**, то есть без занесения в **/etc/hosts**!

Разное

Безопасность

Squid поддерживает проксирование разнообразных протоколов, использование которых необходимо контролировать на уровне прав доступа. Если прокси-сервер - анонимизирующий, им могут воспользоваться нарушители, чтобы скрыть обратный адрес при незаконном доступе к данным или даже атаке на другие серверы.

Неправильно настроенный прокси-сервер можно использовать для массовой рассылки почты (спама), что является инцидентом информационой безопасности и может привести к отказу пользователей сети и администраторов почтовых серверов принимать почту из данного домена.

Сбор статистики и ограничение полосы доступа

В **Squid** входит утилита кеш-менеджер, служащая для отображения статистики и загрузки сервера. Кеш-менеджер представляет собой cgi-приложение и должен выполняться под управлением сконфигурированного HTTP-сервера. Все настройки кеш-менеджера также производятся в **/etc/squid/squid.conf**, строки, которые относятся к кеш-менеджеру, обычно включают **cachemgr**.

При помощи **Squid** можно ограничить полосу пропускания («толщину канала») для пользователей. За это отвечают параметры **delay_pools** и **delay_class**. Эта технология позволит вам снизить загрузку канала, например, большими по объёму медиафайлами, и отдать полосу какому-то более приоритетному трафику.

Кеширование DNS-запросов

Squid содержит встроенный минисервер запросов DNS. Он выступает как посредник между **Squid** и внешними DNS-серверами. При запуске **Squid** производит начальное тестирование доступности DNS и интернет в целом. Это можно отключить, используя опцию **-D**. Время кеширования удачного DNS-запроса по умолчанию составляет шесть часов.

Установка и настройка squid

Описание Squid
Установка Squid и настройка в прозрачном режиме работы
Настройка Selinux для Squid
Настройка кэширования
Контроль доступа к сайтам
Перенаправление трафика
Настройка клиента и браузера

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** squid 5.5-1

Описание Squid

Squid – программа, представляющая собой кэширующий прокси-сервер для протоколов HTTP, HTTPS, FTP и других. Используется для кэширования часто запрашиваемого веб-контента, а также для фильтрации сетевого трафика.

Установка Squid и настройка в прозрачном режиме работы

Установка

Установите прокси-сервер следующей командой:

```
sudo dnf install squid
```

Подготовка сертификатов

Чтобы работал HTTPS, необходимо сгенерировать сертификаты. Для этого создаем папку для хранения сертификатов, например, в **/etc/squid/sslcert**.

```
sudo mkdir /etc/squid/sslcert
```

Переходим в эту папку:

```
cd /etc/squid/sslcert
```

Генерируем ключ:

```
sudo openssl genrsa -out /etc/squid/sslcert/squid.key
```

Создаем **csr**-запрос, используя ключ; нужно будет указать всю необходимую информацию для **csr**:

```
sudo openssl req -new -key /etc/squid/sslcert/squid.key -out /etc/squid/sslcert/squid.csr
```

Подписываем сертификат самим собой:

```
sudo openssl x509 -req -days 3650 -in /etc/squid/sslcert/squid.csr -signkey /etc/squid/sslcert/squid.key -out /etc/squid/sslcert/squid.pem
```

Генерируем корневой сертификат, который нужно будет добавить в браузер:

```
sudo openssl x509 -in /etc/squid/sslcert/squid.pem -outform DER -out squid.der
```

Далее нужно будет дать права на папку с сертификатами для **squid**:

```
sudo chown -R :squid /etc/squid/sslcert
```

Описание настроек Squid.conf

Открываем файл настроек:

```
sudo nano /etc/squid/squid.conf
```

Блок настроек «**acl localnet src …**» устанавливает правила доступа для вашей локальной сети, если в списке нет IP-адреса вашей сети, то его нужно добавить, например:

```
acl localnet src 10.9.1.0/24
```

или через файл:

```
acl localnet src "/etc/squid/acl_localnet"
```

* кавычки обязательны
** после необходимо создать файл **/etc/squid/acl_localnet** и с каждой строчки перечислить разрешенные IP-адреса.

Блок настроек **http_access** устанавливает разрешения на доступ; чтобы разрешить весь трафик, добавляем следующую строчку:

```
http_access allow all
```

* важно, чтобы выше она была запрещающей – **http_access deny all**.

Настройка Squid с HTTPS

Открываем файл конфигурации:

```
sudo nano /etc/squid/squid.conf
```

Находим строку с **http_port 3128** и под ней дописываем строки:
- создание прозрачного *HTTP-порта 3129*:

```
http_port 3129 intercept
```

- создание *порта 3130* для https-трафика с генерацией сертификатов по ключу:

```
https_port 3130 intercept ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/sslcert/squid.pem
key=/etc/squid/sslcert/squid.key
```

Отключаем проверку сертификатов:

```
sslproxy_cert_error allow all
```

Указываем, что необходимо принимать сертификаты, даже если они не прошли проверку:

```
sslproxy_flags DONT_VERIFY_PEER
```

Перенаправляем весь трафик на **squid**:

```
always_direct allow all
```

Устанавливаем безопасное соединение с сервером, затем с клиентом, используя имитированный сертификат сервера:

```
ssl_bump server-first all
```

Устанавливаем TCP-туннель, не расшифровывая прокси-трафик:

```
ssl_bump none all
```

Указываем расположение программы генерации сертификатов и устанавливаем кэширование:

```
sslcrtd_program /usr/lib64/squid/security_file_certgen -s /var/lib/ssl_db -M 4MB
```

Сохраняем и закрываем файл **/etc/squid/squid.conf**.

Дальше нужно пересоздать базу данных сертификатов:

```
rm -rf /var/lib/ssl_db
sudo /usr/lib64/squid/security_file_certgen -c -s /var/lib/ssl_db -M 4MB
```

Устанавливаем владельца **squid** на папку базы данных сертификатов:

```
sudo chown -R :squid /var/lib/ssl_db
```

Настройка Selinux для Squid

Добавляем политики:

```
sudo semanage fcontext -a -t squid_conf_t '/var/lib/ssl_db/index.txt'
sudo semanage fcontext -a -t squid_conf_t '/var/lib/ssl_db/size'
```

Применяем политики:

```
sudo /sbin/restorecon -v /var/lib/ssl_db/index.txt
sudo /sbin/restorecon -v /var/lib/ssl_db/size
```

Перезагружаем систему и запускаем squid:

```
sudo systemctl start squid
```

Проверяем работоспособность squid:

```
sudo systemctl status squid
```

Squid должен быть активен.

Добавляем *squid* в автозагрузку:

```
sudo systemctl enable squid
```

Настройка кэширования

Настройте директорию для кэша в файле **/etc/squid/squid.conf**:

```
cache_dir ufs /var/spool/squid 4096 32 256
```

***** где **ufs** — файловая система (ufs для SQUID является самой подходящей);
/var/spool/squid — директория хранения кэша;
4096 — объем пространства в мегабайтах, которое будет выделено под кэш;
32 — количество каталогов первого уровня, которое будет создано для размещения кэша;
256 — количество каталогов второго уровня, которое будет создано для размещения кэша.

Теперь создайте структуру папок под кэш следующей командой:

```
sudo squid -z
```

Перезапускаем *squid*:

```
sudo systemctl restart squid
```

Контроль доступа к сайтам

Открываем конфигурационный файл *squid*:

```
nano /etc/squid/squid.conf
```

После строки «**acl Safe_ports port 777**» добавляем:

```
acl CONNECT method CONNECT
acl BLOCKED url_regex -i '/etc/squid/blocklist'
```

Тем самым создается список доступа к сайтам.

Далее перед строкой «**http_access allow localnet**» для блокировки списка доступа прописываем:

```
http_access deny BLOCKED
```

Сохраняем конфигурационный файл.

Создаем файл со списком сайтов для блокировки:

```
sudo nano /etc/squid/blocklist
```

Например, с таким списком сайтов:

```
amazon.com
vk.com
music.yandex.ru
```

Сохраняем файл.

Перечитываем конфигурацию *squid*:

```
sudo systemctl reload squid
```

Блокировка сайтов настроена, осталось только перенаправить трафик на сервер *squid*.

Перенаправление трафика

Установите **iptables**, если пакет еще не установлен:

```
sudo dnf install iptables
```

Включаем **ip_forwarding** для разрешения проходящего трафика:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

Чтобы настройка **ip_forward** не сбрасывалась после перезагрузки, нужно в конце файла **/usr/lib/sysctl.d/50-default.conf** прописать:

```
net.ipv4.ip_forward = 1
```

Добавляем правила для **iptables**:

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3129
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 3130
```

Для тестирования прокси-сервера с локальным трафиком, надо перенаправлять на *Squid* весь трафик, кроме трафика от *Squid*, это можно сделать правилами:

```
sudo iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner squid --dport 80 -j REDIRECT --to-port 3129
sudo iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner squid --dport 443 -j REDIRECT --to-port 3130
```

Если нужно сохранить правила *iptables*, чтобы после перезагрузки они не сбрасывались, необходимо ввести команду:

```
sudo service iptables save
```

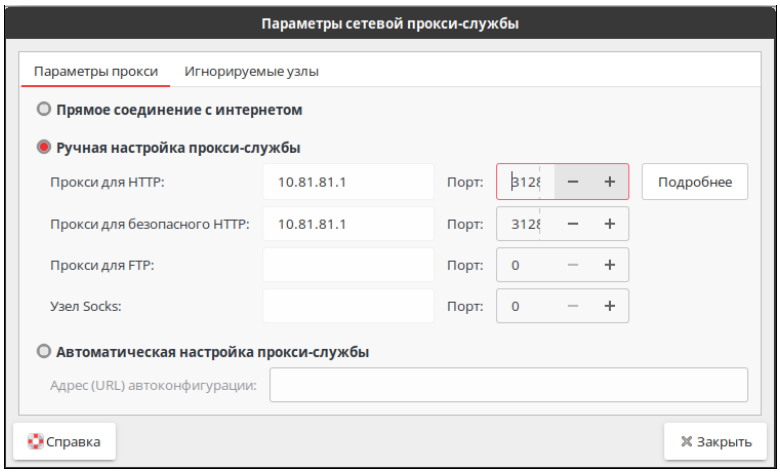
Перезапускаем *squid*:

```
sudo systemctl restart squid
```

Настройка клиента и браузера

В РЕД ОС откройте **Главное меню - Параметры - Прокси сервер**.

Для ручной настройки подключения к прокси заполните поля адреса сервера и порт (3128):



Настройка браузера

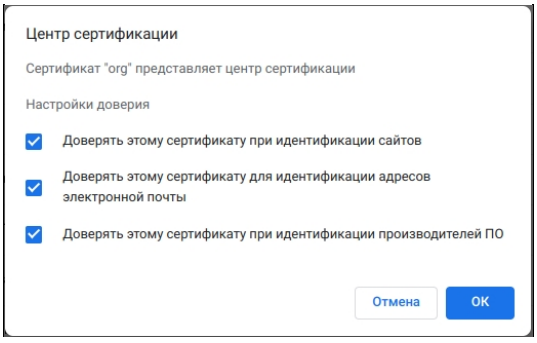
Сейчас большинство сайтов используют технологию **HSTS** для предотвращения *MiTM*-атак, поэтому если вы хотите настроить *Squid* для фильтрации трафика в своей организации, вам следует добавить сертификат **.der**. Рассмотрим на примере *Chrome*.

В меню браузера переходим по пути: **Настройки->Конфиденциальность и безопасность->Безопасность->Настроить сертификаты->Центры сертификации->Импорт**.

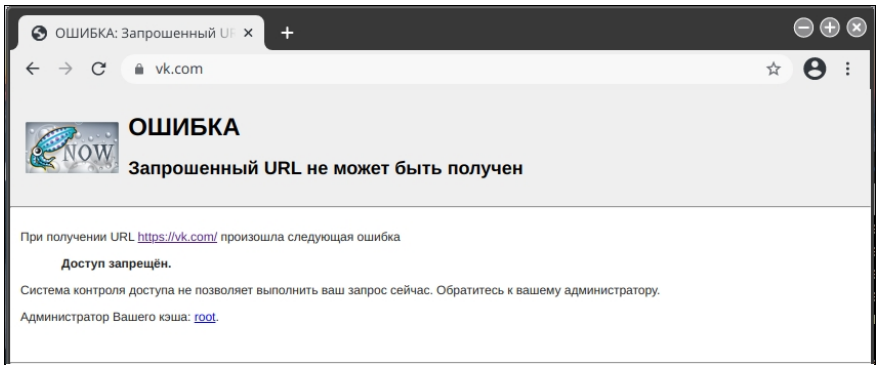
Добавляем созданный ранее сертификат для браузера по пути:

```
/etc/squid/sslcert/squid.pem
```

Устанавливаем все галочки и нажимаем «OK».



Если все сделано правильно, то при входе на запрещенный сайт должна отобразиться такая страница:



Настройка автоматической авторизации доменных пользователей IPA в squid

Ввод сервера squid в домен IPA:

Для ввода сервера в домен IPA выполните команду:

```
# ipa-client-install --enable-dns-updates --mkhomedir
```

ВАЖНО

Проверьте правильность записи DNS в файле /etc/resolv.conf, должен быть указан DNS контроллера домена IPA. Более подробно о вводе в домен написано в статье «Ввод клиентских машин в домен IPA».

Установка squid

Для установки squid выполните команду:

```
# dnf install squid
```

Добавьте сервис в автозагрузку, выполнив команду:

```
# systemctl enable squid
```

Настройка конфигурации squid

Отредактируйте файл /etc/squid/squid.conf любым текстовым редактором

```
# vi /etc/squid/squid.conf
```

Добавьте строки для включения авторизации через kerberos

```
auth_param negotiate program /usr/lib64/squid/negotiate_kerberos_auth -d -s HTTP/squid.example.com
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl auth proxy_auth REQUIRED
```

Закомментируйте строки

```
#http_access allow localnet
#http_access allow localhost
```

Добавьте следующие строки

```
http_access deny !auth
http_access allow auth
```

Создание kerberos keytab для доступа Squid HTTP

На сервере IPA выполните:

```
# kinit admin
Password for admin@EXAMPLE.COM:
# ipa service-add HTTP/squid.example.com
```

Вывод команды должен быть следующим:

```
----------------------------------------------------
Added service "HTTP/squid.example.com@EXAMPLE.COM"
----------------------------------------------------
```

```
  Principal: HTTP/squid.example.com@EXAMPLE.COM
  Managed by: squid.example.com
```

На сервере squid выполните:

```
# kinit admin
# ipa-getkeytab -s dc.example.com -p HTTP/squid.example.com -k /etc/squid/krb5.keytab
```

При правильном выполнении команды выведет:

```
Keytab successfully retrieved and stored in: /etc/squid/krb5.keytab
```

Измените права доступа к файлу /etc/squid/krb5.keytab

```
# chown root:squid /etc/squid/krb5.keytab
# chmod 640 /etc/squid/krb5.keytab
```

Отредактируйте файл /etc/sysconfig/squid и добавьте в него следующие строки:

```
KRB5_KTNAME=/etc/squid/krb5.keytab export KRB5_KTNAME
```

Перезапустите squid

```
#systemctl restart squid
```

Откройте порт в IPTables:

```
# iptables -I INPUT -p tcp --dport 3128 -j ACCEPT
# service iptables save
```

Настройка высокодоступного прокси-сервера HAProxy

Предварительная настройка
Отключение SELinux
Базовая настройка HAProxy
Настройка веб-серверов
Настройка сервера nginx
Настройка сервера apache2 (httpd)
Проверка работоспособности HAProxy

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический, сервер минимальный
- **Версия ПО**: haproxy-2.6.11-2

HAProxy – программное обеспечение с открытым исходным кодом, которое обеспечивает высокодоступный балансировщик нагрузки и прокси-сервер для приложений на основе **TCP** и **HTTP**, распределяющих запросы между несколькими серверами.

Предварительная настройка

Дальнейшая настройка должна выполняться с правами администратора системы (**sudo**) или суперпользователя **root** (**su**), если не указано иное. В текущей инструкции команды будут выполнены с правами суперпользователя **root**. Для перехода в сеанс суперпользователя выполните:

```
su -
```

Перед настройкой на всех машинах необходимо установить последние обновления:

```
dnf update
```

Отключение SELinux

На время установки и настройки **HAProxy** необходимо переключить SELinux в режим уведомлений.

Для этого в файле конфигурации **/etc/selinux/config** замените режим `enforcing` на `permissive` командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

Для применения изменений перезапустите систему.

Статус службы SELinux можно просмотреть командой:

```
sestatus
```

Базовая настройка HAProxy

Для установки **HAProxy** выполните команду:

```
dnf install haproxy
```

После установки **HAProxy** будет автоматически запущена служба **haproxy**. Для проверки статуса службы выполните команду:

```
systemctl status haproxy
```

В статусе должно отображаться **active (running)**.

Для автоматического запуска службы после перезагрузки сервера выполните команду:

```
systemctl enable haproxy
```

Перед началом настройки рекомендуется создать резервную копию файла конфигурации:

```
cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.bk
```

Для настройки откройте конфигурационный файл HAProxy:

```
nano /etc/haproxy/haproxy.cfg
```

Файл конфигураций состоит из следующих секций:

- `global` – содержит системные настройки и отвечает за более гибкую настройку производительности и безопасности;
- `defaults` – стандартные настройки, которые должны работать без дополнительных изменений. Также здесь находятся настройки времени ожидания и отчетов ошибок;
- `frontend` – настройки *frontend*-сервера, на котором установлен **haproxy**;
- `backend` – информация о *backend*-серверах и режиме балансировки;
- `listen` – дополнительные настройки, позволяющие включить мониторинг статистики.

Выбор режимов балансировки:

- **roundrobin** — режим, при котором **HAProxy** выбирает сервера по очереди, равномерно распределяя нагрузку;
- **leastconn** — в этом режиме запросы направляются к серверу, у которого меньше всего подключений, рекомендуется использовать для долгих сессий;
- **source** — режим выбирает сервер на основе хэша источника IP-адреса, с которого клиенты отправляют запросы, это гарантирует, что одни и те же пользователи используют один и тот же сервер.

Добавьте в секцию `frontend` следующее содержимое:

```
frontend haproxy      # имя фронтенда
 bind 192.168.1.1:80   # IP-адрес сервера с HAproxy
 stats uri /haproxy?stats    # адрес веб-интерфейса мониторинга
 default_backend webservers  # имя нужного бэкенда
```

В секцию `backend` добавьте следующее содержимое:

```
backend webservers    # имя бэкэнда
 balance roundrobin    # режим балансировки
 server web1.example.com 192.168.1.2:80    # имя и адрес веб-серверов
 server web2.example.com 192.168.1.3:80
```

Для включения статистики в секцию `listen` добавьте:

```
listen stats
 bind *:8080
 stats enable
 stats uri /
 stats refresh 5s
 stats realm Haproxy\ Stats
 stats auth Login:Password    #логин и пароль для подключения к веб-интерфейсу мониторинга
```

После сохранения изменений в файле конфигурации проверьте корректность файла, выполнив команду:

```
haproxy -f /etc/haproxy/haproxy.cfg -c
```

Если все настроено правильно, ответ должен выглядеть следующим образом:

```
Configuration file is valid
```

Для применения внесенных изменений перезапустите службу:

```
systemctl restart haproxy
```

ВАЖНО!

Если DNS-сервер не настроен, необходимо прописать веб-сервера в файл **/etc/hosts**:

```
192.168.1.1  haproxy
192.168.1.2  web1.example.com
192.168.1.3  web2.example.com
```

Настройка веб-серверов

В рамках данной статьи для проверки работы **haproxy** будет рассмотрена настройка двух серверов – **nginx** и **apache2** (**httpd**).

Настройка сервера nginx

Для установки **nginx** выполните команду:

```
dnf install nginx
```

Запустите службу **nginx** и добавьте ее в автозагрузку:

```
systemctl enable nginx --now
```

Проверьте статус службы:

```
systemctl status nginx
```

В статусе должно отображаться **active (running)**.

Для настройки сервера откройте файл конфигурации **nginx.conf**:

```
nano /etc/nginx/nginx.conf
```

В секцию `server` добавьте следующее содержимое:

```
server_name web1.example.com;     # укажите имя веб-сервера или IP-адрес
```

Выполните проверку настроек **nginx**:

```
nginx -t
```

Если файл конфигурации настроек верно, вывод должен иметь вид:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Для применения конфигурации перезапустите веб-сервер:

```
systemctl restart nginx
```

Настройка сервера apache2 (httpd)

Для установки **apache2** (**httpd**) выполните команду:

```
dnf install httpd
```

Запустите службу **httpd** и добавьте ее в автозагрузку:

```
systemctl enable httpd --now
```

Проверьте статус службы:

```
systemctl status httpd
```

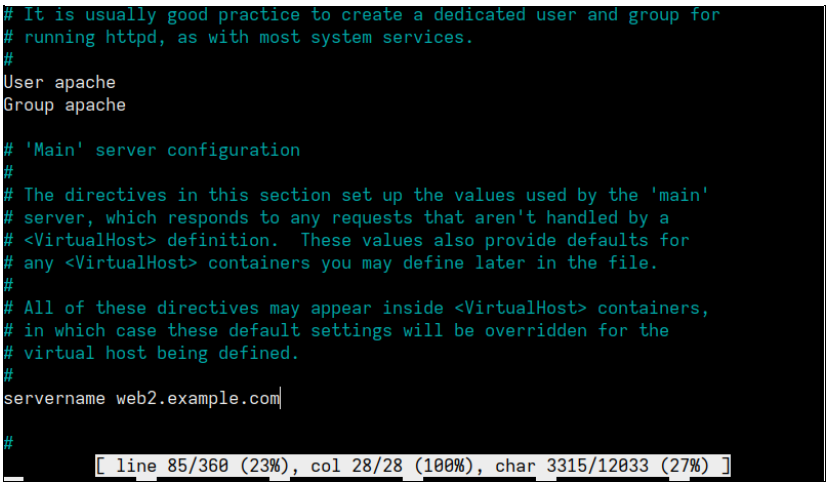
В статусе должно отображаться **active (running)**.

Для настройки сервера откройте файл конфигурации **httpd.conf**:

```
nano /etc/httpd/conf/httpd.conf
```

В секцию 'Main' server configuration добавьте следующее содержимое:

```
servername web1.example.com     # укажите имя веб-сервера или IP-адрес
```

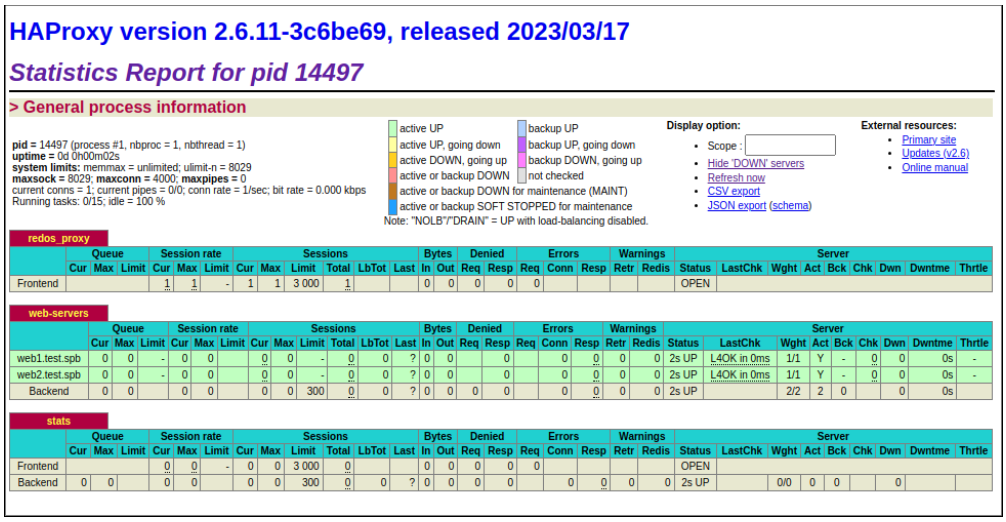


Для применения конфигурации перезапустите службу:

```
systemctl restart httpd
```

Проверка работоспособности HAProxy

Ранее был настроен сбор статистики для **HAProxy**. Для доступа к просмотру собранной статистики откройте браузер и в адресной строке введите **<IP-адрес_HAProxy>/haproxy?stats**.



Если сервер в списке подсвечен *зеленым цветом*, значит настройка была произведена корректно.

Если серверы подсвечены *красным цветом*, значит настройка была выполнена неверно либо сервер не включен. Также в статистике отображено, что весь трафик уходит на единственный рабочий сервер.

web-servers

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
web1.test.spb	0	0	-	0	257		0	5	-	1 000	1 000	11s	157 000	356 000		0		0	0	0	0	2m18s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-
web2.test.spb	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	2m17s DOWN	L4CON in 0ms	1/1	Y	-	1	1	2m17s	-
Backend	0	0		0	257		0	5	300	1 000	1 000	11s	157 000	356 000	0	0		0	0	0	0	2m18s UP		1/1	1	0		0	0s	

При правильной работе в режиме **roundrobin** трафик распределяется равномерно:

redos_proxy

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				41	235	-	2	29	3 000	1 006			160 624	543 753	0	0	2					OPEN								

web-servers

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
web1.test.spb	0	0	-	26	120		0	2	-	500	500	1s	78 500	178 000		0		0	0	0	0	1m36s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-
web2.test.spb	0	0	-	25	120		0	2	-	500	500	1s	78 500	178 000		0		0	0	0	0	19s UP	L4OK in 1ms	1/1	Y	-	1	1	1m16s	-
Backend	0	0		52	240		0	4	300	1 000	1 000	1s	157 000	356 000	0	0		0	0	0	0	1m36s UP		2/2	2	0		0	0s	

stats

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				0	0	-	0	0	3 000	0			0	0	0	0	0					OPEN								
Backend	0	0		0	0		0	0	300	0	0	?	0	0	0	0		0	0	0	0	1m36s UP		0/0	0	0		0		

Настройка прокси-сервера 3proxy

Установка и настройка
Настройка доступа

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: 3proxy-0.9.3-1

Установка и настройка

3proxy – бесплатный кроссплатформенный прокси-сервер. Не имеет графического интерфейса, настройка производится путем написания конфигурационного файла.

Основными особенностями являются:

- поддержка протоколов HTTP, HTTPS, SOCKS v4, SOCKS v4a, SOCKS v5, SMTP;
- переадресация TCP и UDP трафика;
- объединение прокси-серверов в цепочку и функции обратного соединения;
- ограничение пропускной способности канала и трафика;
- контроль доступа (ACL);
- ведение журналов;
- поддержка IPv6.

Для установки ПО перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install 3proxy
```

Далее необходимо настроить конфигурационный файл прокси-сервера. Он располагается по пути **/etc/3proxy**. Откройте файл и добавьте в него следующее содержимое:

```
nano /etc/3proxy/3proxy.cfg
```

```
#!/bin/3proxy
# DNS-сервера (указываем желаемые DNS-сервера, либо смотрим в /etc/resolv.conf)
nserver 77.8.8.8
nserver 77.8.8.1
# Режим запуска daemon
daemon
# IP-адрес внешнего интерфейса (без кавычек)
external <IP-адрес>
# IP-адрес адрес внутреннего интерфейса (без кавычек)
internal <IP-адрес>
# запуск http proxy на порту 4555
proxy -p4555 -n -a
# запуск ftp proxy на порту 4556
ftppr -p4556
# socks proxy на порту 2333
socks -p2333
# путь к логам и формат лога
log /var/log/3proxy/3proxy.log D
logformat "- +_L%t.%. %N.%p %E %U %C:%c %R:%r %O %I %h %T"
rotate 30
```

```
# Размер кэша запросов DNS. Стандартное значение, в килобайтах
nscache 65536
# Стандартные таймауты
timeouts 1 5 30 60 180 1800 15 60
```

Для упрощения работы с **3proxy** создайте для него собственный сервис для управления через **systemd**:

```
touch /etc/systemd/system/3proxy.service
chmod 664 /etc/systemd/system/3proxy.service
nano /etc/systemd/system/3proxy.service
```

Добавьте в описание сервиса следующее содержимое:

```
[Unit]
Description=3proxy Proxy Server
After=network.target
[Service]
Type=simple
ExecStart=/usr/bin/3proxy /etc/3proxy/3proxy.cfg
ExecStop=/bin/kill /usr/bin/pgrep 3proxy
RemainAfterExit=yes
Restart=on-failure
[Install]
WantedBy=multi-user.target
```

После проведенных манипуляций необходимо обновить конфигурацию **systemd** командой:

```
systemctl daemon-reload
```

Затем добавьте сервис в автозагрузку и запустите его:

```
systemctl enable 3proxy --now
```

Проверьте статус сервиса:

```
systemctl status 3proxy
```

В статусе должно быть отображено **active (exited)**.

```
● 3proxy.service - 3proxy Proxy Server
     Loaded: loaded (/etc/systemd/system/3proxy.service; enabled; vendor preset: disabled)
     Active: active (exited) since Tue 2023-01-24 16:42:34 MSK; 2s ago
    Process: 24909 ExecStart=/usr/bin/3proxy /etc/3proxy/3proxy.cfg (code=exited, status=0/SUCCESS)
   Main PID: 24909 (code=exited, status=0/SUCCESS)
        CPU: 2ms

янв 24 16:42:34 localhost.localdomain systemd[1]: Started 3proxy Proxy Server.
```

Настройка доступа

Если доступ к прокси необходимо настроить по паролю, в конфигурационном файле для этого добавьте следующие строки:

```
auth cache strong
users "user1:CL:password1"
users "user2:CR:password2"
```

Пользователи добавляются строкой `users "<имя_пользователя>:<тип_пароля>:<пароль>"`.

Существует два типа хранения пароля:

- **CL** – пароль пользователя указывается в открытом виде, непосредственно в конфигурационном файле;
- **CR** – зашифрованный пароль (**md5**), можно получить с помощью команды `openssl passwd`.

Для ограничения доступа пользователей к определенным IP-адресам в конфигурационном файле следует добавить строки:

```
deny user1 * 192.168.0.1
allow *
```

где:

- **user1** – имя пользователя, которому запрещен доступ к ресурсу;
- **192.168.0.1** – IP-адрес, к которому запрещен доступ;
- **allow *** - разрешение доступа ко всем остальным ресурсам.

Чтобы запретить всем пользователям доступ к адресу, вместо имени пользователя указывается «*».

```
deny * * 192.168.0.1
allow *
```

Настройка ЕСПД (Единая Сеть Передачи Данных от Ростелеком)

Установка корневого сертификата
Установка сертификата с использованием интернет-браузера Firefox
Установка сертификата с использованием веб-браузера Chromium
Настройка прокси-сервера

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: chromium-94.0.4606.81, firefox-102.9.0

ЕСПД (Единая Сеть Передачи Данных) — это совокупность сетей в разных регионах Российской Федерации, объединенных в единую систему с централизованным управлением и фильтрацией трафика, подключение к которой в скором времени станет обязательным для всех государственных и муниципальных учреждений и органов власти. Оператором ЕСПД является *Ростелеком* (РТ).

Настройка подразумевает установку корневого сертификата и указания прокси-сервера, через который проходит весь трафик. Сертификат можно скачать с официального сайта Ростелеком — https://espd.wifi.rt.ru/settings/cert-install.

Установка корневого сертификата

Перед установкой корневой сертификат необходимо скопировать в центры сертификации ОС. Для этого перейдите в сеанс суперпользователя **root**:

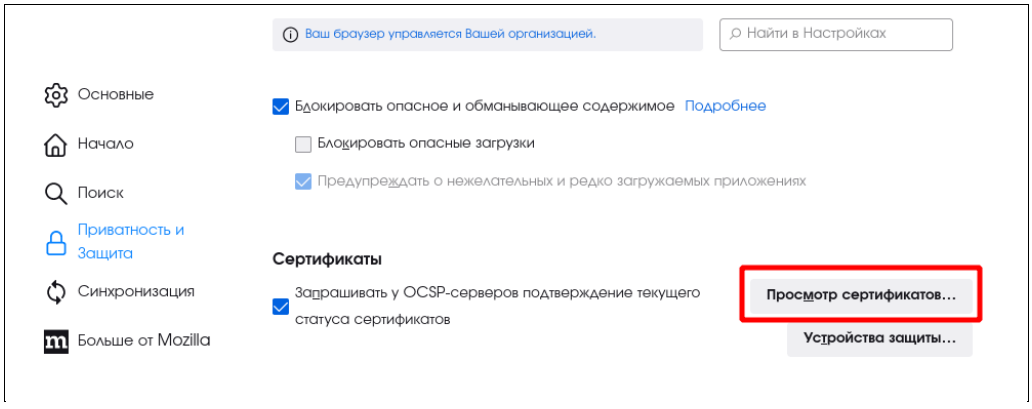
```
su -
```

и выполните следующие команды:

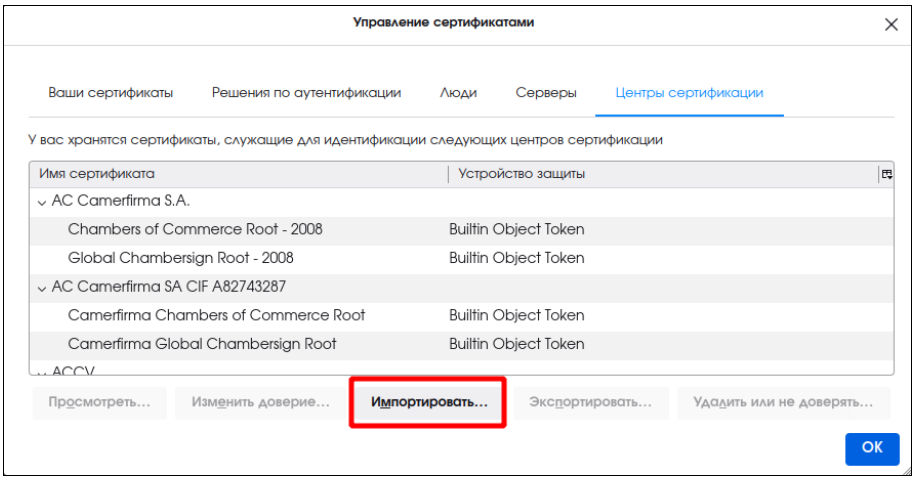
```
update-ca-trust
cp /<путь_до_сертификата>/ca-root.crt /etc/pki/ca-trust/source/anchors/
update-ca-trust extract
```

Установка сертификата с использованием интернет-браузера Firefox

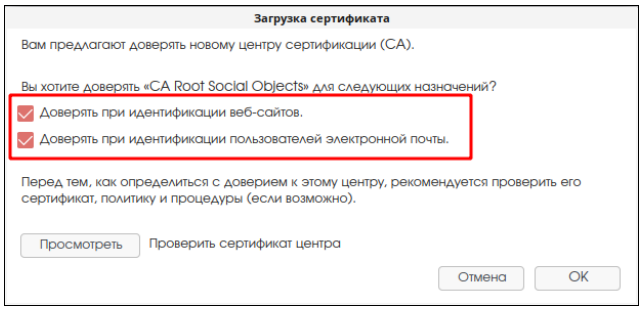
Установите сертификат Ростелекома в **Firefox**. Для этого перейдите в «**Настройки**» браузера, откройте вкладку «**Приватность и защита**», перейдите к разделу «**Сертификаты**» и нажмите «**Просмотр сертификатов...**».



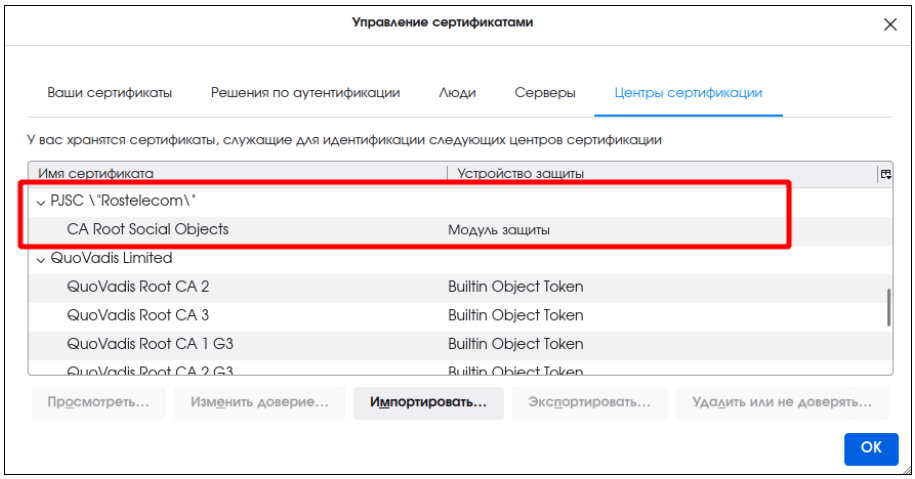
Затем откройте вкладку «**Центры сертификации**» и нажмите «**Импортировать...**».



При импорте сертификата необходимо разрешить доверие данному сертификату, установив соответствующие флаги.

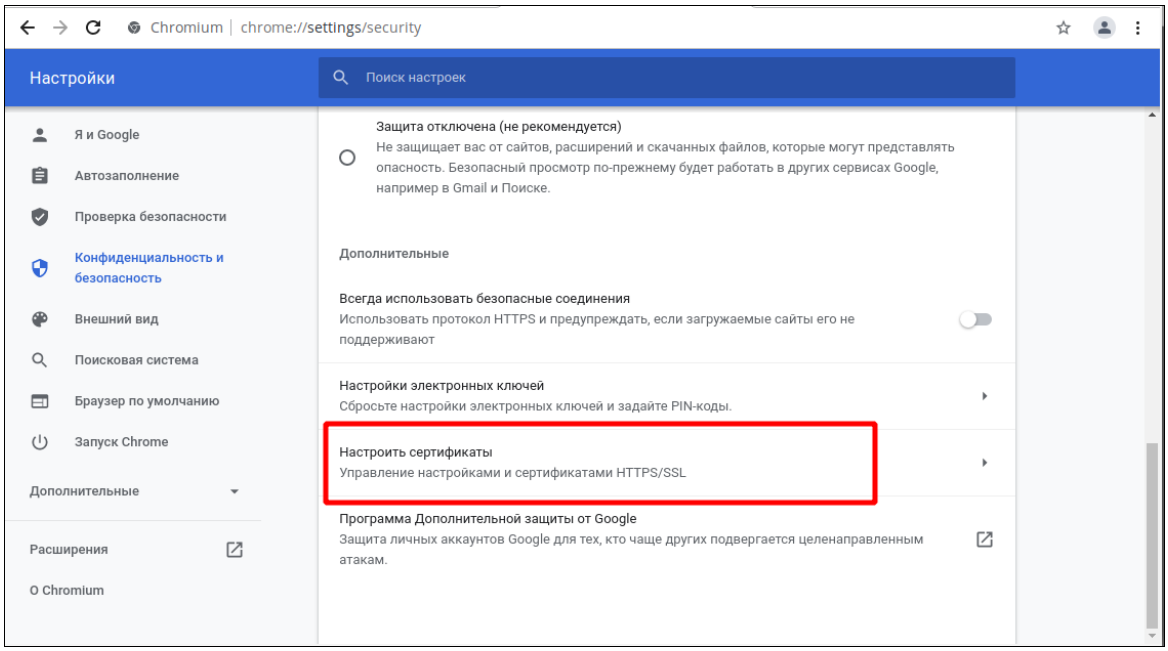


Убедитесь, что сертификат был установлен.

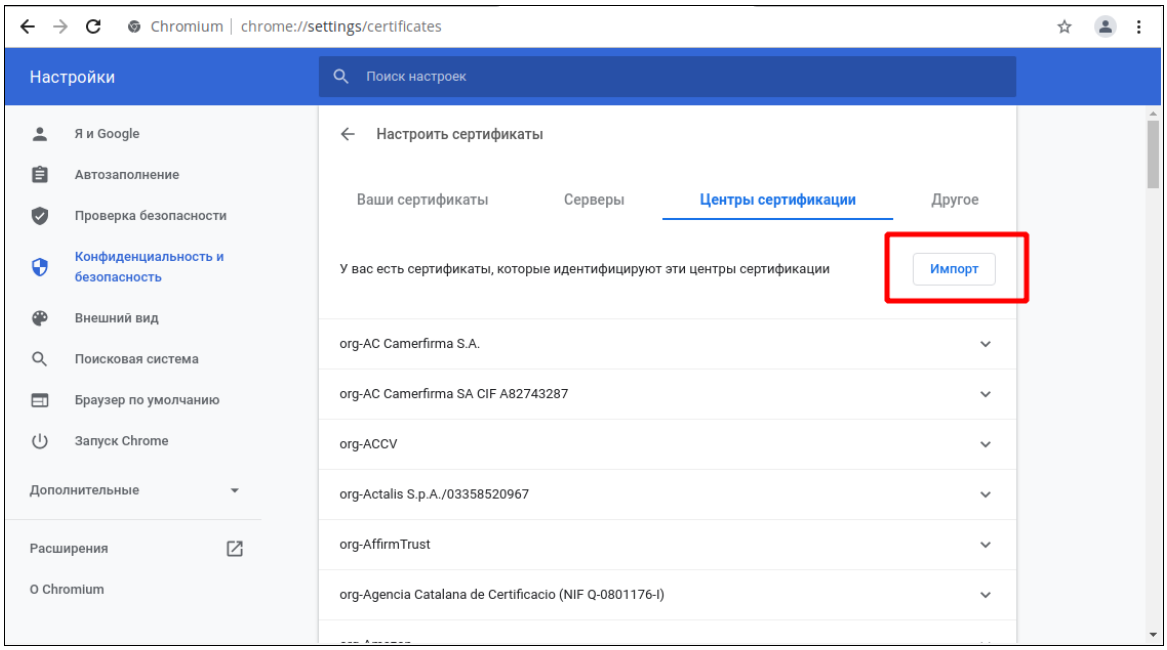


Установка сертификата с использованием веб-браузера Chromium

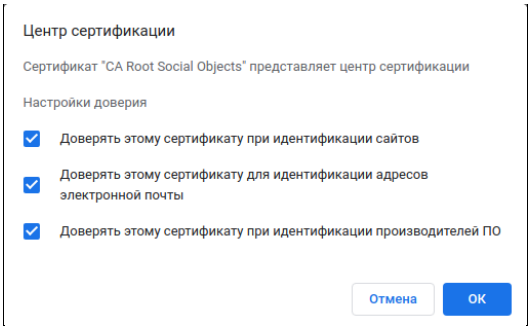
Для установки сертификата Ростелекома в **Chromium** перейдите в «**Настройки**» — «**Конфиденциальность и безопасность**», откройте раздел «**Безопасность**» и нажмите «**Настроить сертификаты**».



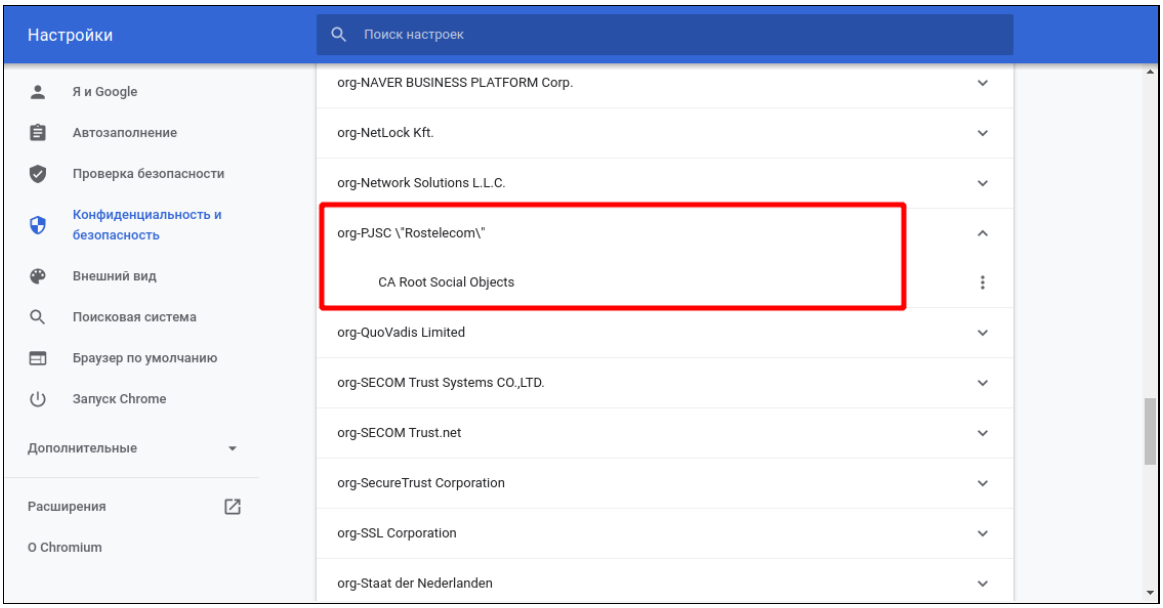
Откройте вкладку «**Центры сертификации**» и нажмите «**Импорт**».



При импорте сертификата необходимо разрешить доверие данному сертификату, установив соответствующие флаги.



Убедитесь, что сертификат был установлен.



Настройка прокси-сервера

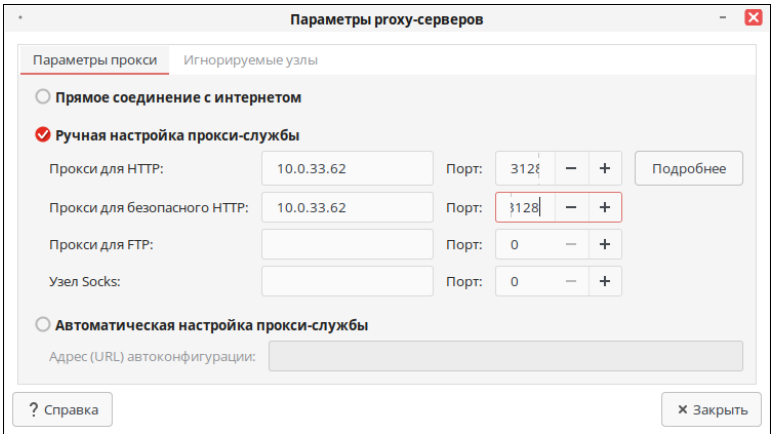
Для настройки прокси-сервера перейдите в «**Главное меню**» — «**Параметры**» — «**Прокси-сервер**».

Выберите пункт «**Ручная настройка прокси-службы**».

Укажите *адрес* и *порт* подключения прокси-сервера для параметров «**Прокси для HTTP**» и «**Прокси для безопасного HTTP**».

Примечание.

Адрес и *порт* прокси-сервера **выдаются провайдером Ростелеком**, по умолчанию используется порт **3128**.



После настройки необходимо проверить доступ к сети Интернет, если сайты загружаются успешно, значит настройка выполнена верно.

Настройка прокси на клиентских ПК

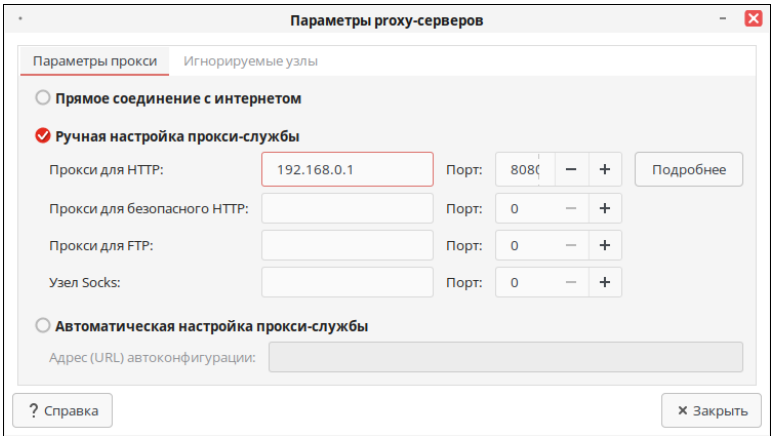
Настройка прокси для приложений графической среды
Настройка прокси в графическом интерфейсе
Настройка прокси посредством gsettings
Настройка прокси для терминальных приложений
Общесистемные настройки прокси для терминальных приложений
Настройка dnf для работы через прокси
Настройка wget для работы через прокси

Настройка прокси для приложений графической среды

Настройка прокси в графическом интерфейсе

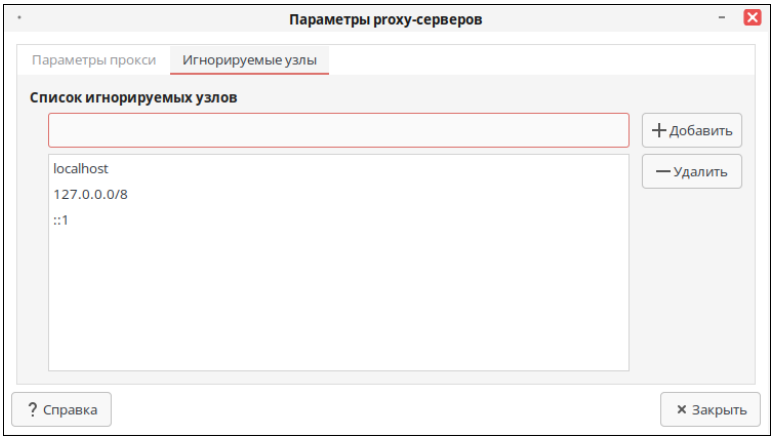
Для настройки прокси-сервера через графический интерфейс в *среде рабочего стола MATE* откройте утилиту «**Прокси-сервер**» из «**Главного меню**» - «**Параметры**».

В открывшемся окне выберите «**Ручная настройка прокси-службы**» и введите *ip-адрес* или *сетевое имя* прокси сервера и его *порт*.

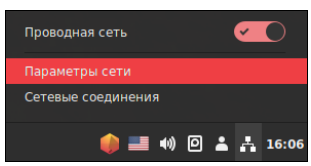


Если у вас настроена автоконфигурация на прокси-сервере, выберите пункт «**Автоматическая настройка прокси-службы**».

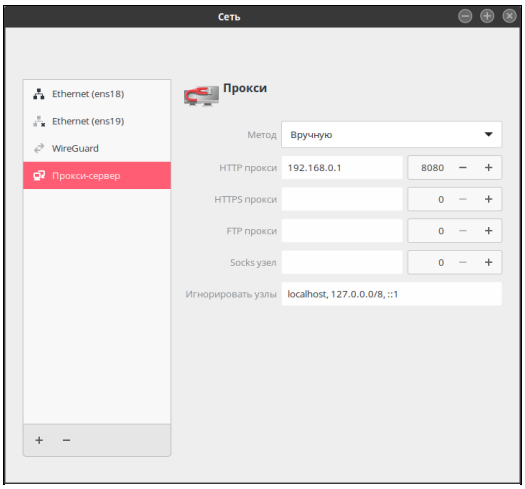
Список игнорируемых узлов на вкладке «**Игнорируемые узлы**» позволяет задать те узлы, для подключения к которым не нужно использовать прокси. Подключение к указанным в этом списке узлам будет выполняться напрямую через Интернет, без использования прокси-сервера.



Для настройки прокси-сервера через графический интерфейс в *среде рабочего стола Cinnamon* откройте «**Параметры сети**», нажав по иконке «**Сетевых соединений**» в трее.



В открывшемся окне откройте настройки для **Прокси-сервера**, выберите для поля «**Метод**» значение «**Вручную**» и укажите *IP-адрес* и *порт* для **HTTP прокси**.



Настройка прокси посредством gsettings

Для установки параметров прокси текущего пользователя из командной строки следует воспользоваться утилитой **gsettings**. Синтаксис и примеры использования приведены в нашей статье «Управление Dconf» в соответствующем разделе.

Схемы и ключи **dconf**-настроек прокси:

Схема	Ключ	Описание
org.gnome.system.proxy	**ignore-hosts**	Список узлов-исключений, которые используют подключение напрямую, а не через прокси-сервер. Пример создания списка исключений будет приведен ниже.
	mode	Режим настройки прокси. Возможные значения: “*none*” - без прокси, “*manual*” - ручная настройка, “*auto*” - автоматическая настройка.
	autoconfig-url	URL для автоматической конфигурации прокси.
org.gnome.system.proxy.http	**use-authentication**	Указание применения аутентификации (только для HTTP-протокола). Возможные значения: *true*, *false*.
	authentication-user	Имя пользователя для аутентификации по HTTP.
	authentication-password	Пароль для аутентификации по HTTP.
org.gnome.system.proxy.http (https/ftp/socks)	**host**	Имя или IP-адрес используемого прокси-сервера для указанного в схеме протокола.
	port	Числовое значение порта прокси-сервера для указанного в схеме протокола.

Пример команды для указания списка узлов-исключений:

```
gsettings set org.gnome.system.proxy ignore-hosts "['localhost', '127.0.0.0/8', '::1', 'someaddress.here', '*.localportal.work']"
```

Пример команд для указания параметров https-прокси:

```
gsettings set org.gnome.system.proxy mode 'manual'
gsettings set org.gnome.system.proxy.https host 'proxy.work'
gsettings set org.gnome.system.proxy.https port 8085
```

Сброс параметров настроек прокси до значений по умолчанию, заданных в системе:

```
gsettings reset-recursively org.gnome.system.proxy
```

Задание настроек прокси по умолчанию для всей системы производится аналогично действиям из соответствующего раздела в нашей статье «Управление Dconf». В этой же статье описана возможность принудительного применения и блокировки параметров, которая позволит установить настройки в качестве неизменяемых общесистемных (для приложений графической среды).

Примечание.

Браузеры на основе **Chrome** не используют параметры **dconf** при входе через **sddm**.

Настройка прокси для терминальных приложений

Общесистемные настройки прокси для терминальных приложений

Настройка производится установкой значений глобальных переменных окружения путем создания файла **/etc/profile.d/proxy_set.sh**:

```
sudo nano /etc/profile.d/proxy_set.sh
```

В него необходимо поместить следующие строки (**proxyserver** и **port** заменить на адрес и порт вашего прокси-сервера):

```
export {http,ftp,https,rsync}_proxy="http://proxyserver:port"
export {HTTP,FTP,HTTPS,RSYNC}_PROXY=$http_proxy
```

Настройки будут применены после перезагрузки компьютера.

Примечание.

Если необходимо настроить прокси для конкретного пользователя, то необходимо изменить файл **.bash_profile** в домашней директории пользователя, добавив в конец файла вышеприведенные строки. Примените настройки выходом/входом в систему, затем выполните:

```
source ~/.bash_profile
```

Примечание.

Если необходимо указать имя пользователя и пароль, то они указываются в следующем формате:

```
MY_PROXY_URL="http://user:password@ServerProxy:8080/"
```

Настройка dnf для работы через прокси

По умолчанию **dnf** получает данные с HTTP-сервера. Все соединения **dnf** с HTTP происходят с использованием **HTTP / 1.1** протокола и совместимых с ним веб прокси-серверов.

Если вам необходимо разрешить доступ к **dnf** через proxy-сервер для всех пользователей, используйте файл **/etc/dnf/dnf.conf** и внесите в раздел [main] данные прокси и данные для аутентификации:

```
[main]
proxy=http://proxy.mydomain.com:3128
proxy_username=user_proxy
proxy_password=pass_user_proxy
```

В данном примере параметр:

- **proxy.mydomain.com** — адрес вашего proxy-сервера **:порт**;
- **proxy_username** — имя пользователя;
- **proxy_password** — пароль пользователя.

Если ваш proxy-сервер не использует авторизацию, достаточно прописать только:

```
proxy=http://proxy.mydomain.com:3128
```

Таким образом, файл `/etc/dnf/dnf.conf` требуется для настройки работы **dnf** через прокси для всех пользователей.

Чтобы разрешить доступ **dnf** через proxy-сервер для конкретного пользователя, вам необходимо использовать файл профиля пользователя. По умолчанию это **~/.bash_profile** в домашнем каталоге пользователя. Внесите в него следующие строчки:

```
http_proxy="http://mycache.mydomain.com:3128"
export http_proxy
```

Если для работы proxy сервера необходимо использовать логин-пароль, то добавьте их в строчку **http_proxy**:

```
http_proxy="http://user_proxy:pass_user_proxy@proxy.mydomain.com:3128"
```

Настройка wget для работы через прокси

Откройте конфигурационный файл **wget**:

```
nano /etc/wgetrc
```

и добавьте следующие строки:

```
http_proxy=http://xxx.xxx.xx.xx:8080
https_proxy=http://xxx.xxx.xx.xx:8080
proxy_user=domain\user
proxy_passwd=password
```

Настройка брандмауэра Firewall

Базовые понятия брандмауэра
Базовые понятия брандмауэра. Зоны
Базовые понятия брандмауэра. Сохранение правил
Включение брандмауэра firewalld
Включение брандмауэра firewalld. Просмотр правил по умолчанию
Включение брандмауэра firewalld. Другие зоны брандмауэра
Настройка зон интерфейсов
Настройка зон интерфейсов. Изменение зоны интерфейса на одну сессию
Настройка зон интерфейсов. Изменение зоны интерфейса на постоянной основе
Настройка зон интерфейсов. Настройка зоны по умолчанию
Создание правил для приложений. Добавление сервиса в зону
Что делать, если нужный сервис недоступен?
Способ 1: Настройка порта
Способ 2: Определение сервиса
Создание зон
Автоматический запуск брандмауэра
Заключение

Базовые понятия брандмауэра

Зоны

Демон firewalld управляет группами правил при помощи так называемых зон.

Зоны – это, по сути, наборы правил, которые управляют трафиком на основе уровня доверия к той или иной сети. Зоны присваиваются сетевым интерфейсам и управляют поведением брандмауэра.

Компьютеры, которые часто подключаются к разным сетям (например, ноутбуки) могут использовать зоны, чтобы изменять наборы правил в зависимости от среды. К примеру, при подключении к общественной сети WiFi брандмауэр может применять более строгие правила, а в домашней сети ослаблять ограничения.

В firewalld существуют следующие зоны:

- **drop**: самый низкий уровень доверия сети. Весь входящий трафик сбрасывается без ответа, поддерживаются только исходящие соединения.
- **block**: эта зона похожа на предыдущую, но при этом входящие запросы сбрасываются с сообщением icmp-host-prohibited или icmp6-adm-prohibited.
- **public**: эта зона представляет публичную сеть, которой нельзя доверять, однако поддерживает входящие соединения в индивидуальном порядке.
- **external**: зона внешних сетей. Поддерживает маскировку NAT, благодаря чему внутренняя сеть остается закрытой, но с возможностью получения доступа.
- **internal**: обратная сторона зоны external, внутренние сети. Компьютерам в этой зоне можно доверять. Доступны дополнительные сервисы.
- **dmz**: используется для компьютеров, расположенных в DMZ (изолированных компьютеров, которые не будут иметь доступа к остальной части сети); поддерживает только некоторые входящие соединения.
- **work**: зона рабочей сети. Большинству машин в сети можно доверять. Доступны дополнительные сервисы.
- **home**: зона домашней сети. Окружению можно доверять, но поддерживаются только определённые пользователем входящие соединения.
- **trusted**: всем машинам в сети можно доверять.

Сохранение правил

Правила firewalld бывают постоянными и временными. Если в наборе появляется или изменяется какое-либо правило, текущее поведение брандмауэра изменяется сразу. Однако после перезагрузки все изменения будут утрачены, если их не сохранить.

Большинство команд firewall-cmd может использовать флаг --**permanent**, который сохранит правило, после чего оно будет использоваться на постоянной основе.

Включение брандмауэра firewalld

Установка firewalld в РЕД ОС производится из репозитория командой:

```
sudo dnf install firewalld
```

После инсталляции активируйте сервис **firewalld.service**:

```
sudo systemctl start firewalld.service
```

Убедитесь, что сервис запущен:

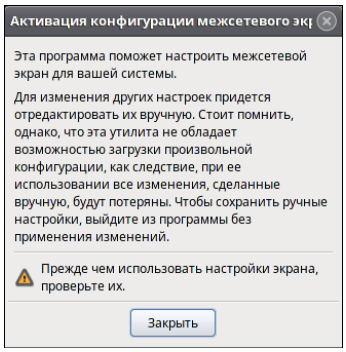
```
firewall-cmd --state
running
```

Теперь брандмауэр запущен и работает согласно конфигурации по умолчанию.

На данный момент сервис включен, но не будет запускаться автоматически вместе с сервером. Чтобы случайно не заблокировать себя на собственном сервере, сначала создайте набор правил, а затем настройте автозапуск.

Стоит сделать небольшое замечание по поводу GUI-интерфейса, он очень удобен, но совершенно не гибок в отличие от способа, если бы мы конфигурировали МЭ через консольные команды

Об этом прямо говорит справка при открытии GUI.



Просмотр правил по умолчанию

Чтобы узнать, какая зона используется по умолчанию, введите:

```
firewall-cmd --get-default-zone
public
```

На данный момент firewalld не получал никаких инструкций относительно других зон, кроме того, к другим зонам не привязан ни один интерфейс, поэтому сейчас зона public является зоной по умолчанию, а также единственной активной зоной.

Чтобы получить список активных зон, введите:

```
firewall-cmd --get-active-zones
public
interfaces: eth0 eth1
```

К зоне **public** привязаны два сетевых интерфейса: **eth0** и **eth1**. Интерфейсы, привязанные к зоне, работают согласно правилам этой зоны.

Чтобы узнать, какие правила использует зона по умолчанию, введите:

```
firewall-cmd --list-all
 public (default, active)
 interfaces: eth0 eth1
 sources:
 services: dhcpv6-client ssh
 ports:
 masquerade: no
 forward-ports:
 icmp-blocks:
 rich rules:
```

Итак, теперь вы знаете, что:

- **public** является зоной по умолчанию и единственной активной зоной.
- К ней привязаны интерфейсы **eth0** и **eth1**.
- Она поддерживает трафик **DHCP** (присваивание IP-адресов) и **SSH** (удаленное администрирование).

Другие зоны брандмауэра

Теперь следует ознакомиться с другими зонами.

Чтобы получить список всех доступных зон, введите:

```
firewall-cmd --get-zones
block dmz drop external home internal public trusted work # Чтобы получить параметры конкретной зоны, добавьте в команду флаг --zone=.

firewall-cmd --zone=home --list-all
home
interfaces:
sources:
services: dhcpv6-client ipp-client mdns samba-client ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Чтобы вывести определения всех доступных зон, добавьте опцию --**list-all-zones**. Для более удобного просмотра вывод можно передать в пейджер:

```
firewall-cmd --list-all-zones | less
```

Настройка зон интерфейсов

Изначально все сетевые интерфейсы привязаны к зоне по умолчанию.

Изменение зоны интерфейса на одну сессию

Чтобы перевести интерфейс в другую зону на одну сессию, используйте опции **--zone=** и **--change-interface=**.

Например, чтобы перевести **eth0** в зону **home**, нужно ввести:

```
sudo firewall-cmd --zone=home --change-interface=eth0
success
```

Примечание: При переводе интерфейса в другую зону нужно учитывать, что это может повлиять на работу некоторых сервисов. К примеру, зона home поддерживает SSH, поэтому соединения этого сервиса не будут сброшены. Но некоторые зоны сбрасывают все соединения, включая SSH, и тогда вы можете случайно заблокировать себе доступ к собственному серверу.

Чтобы убедиться, что интерфейс привязан к новой зоне, введите:

```
firewall-cmd --get-active-zones
home
interfaces: eth0
public
interfaces: eth1
```

После перезагрузки брандмауэра интерфейс будет снова привязан к зоне по умолчанию.

```
sudo systemctl restart firewalld.service
firewall-cmd --get-active-zones
public
interfaces: eth0 eth1
```

Изменение зоны интерфейса на постоянной основе

Если в настройках интерфейса не указана никакая другая зона, после перезапуска брандмауэра интерфейс будет снова привязан к зоне по умолчанию. В РЕД ОС такие конфигурации хранятся в каталоге **/etc/sysconfig/network-scripts**, в файлах формата **ifcfg-interface**.

Чтобы определить зону интерфейса, откройте конфигурационный файл этого интерфейса, например:

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

В конец файла добавьте переменную **ZONE=** и в качестве значения укажите другую зону, например, home:

Содержимое файла:

```
. . . DNS1=2001:4860:4860::8844 DNS2=2001:4860:4860::8888 DNS3=8.8.8.8 ZONE=home
```

Сохраните и закройте файл.

Чтобы обновить настройки, перезапустите сетевой сервис и брандмауэр:

```
sudo systemctl restart network.service

sudo systemctl restart firewalld.service
```

После перезапуска интерфейс **eth0** будет привязан к зоне **home**.

```
firewall-cmd --get-active-zones
home
interfaces: eth0
public
interfaces: eth1
```

Настройка зоны по умолчанию

Также вы можете выбрать другую зону по умолчанию.

Для этого используется параметр **--set-default-zone=**. После этого все интерфейсы будут привязаны к другой зоне:

```
sudo firewall-cmd --set-default-zone=home
home
interfaces: eth0 eth1
```

Создание правил для приложений

Добавление сервиса в зону

Проще всего добавить сервис или порт в зону, которую использует брандмауэр. Просмотрите доступные сервисы:

```
firewall-cmd
--get-services
RH-Satellite-6 amanda-client bacula bacula-client
dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https imaps
ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls
mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi
pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba
samba-client smtp ssh telnet tftp tftp-client transmission-client
vnc-server wbem-https
```

Примечание: Больше информации о каждом конкретном сервисе можно найти в файлах .xml в каталоге /usr/lib/firewalld/services. К пример, сведения о сервисе SSH хранятся в /usr/lib/firewalld/services/ssh.xml и выглядят так:

```
<?xml version="1.0"
encoding="utf-8"?>
```

```
<service>
<short>SSH</short>
<description>Secure
Shell (SSH) is a protocol for logging into and executing commands on
remote machines. It provides secure encrypted communications. If you
plan on accessing your machine remotely via SSH over a firewalled
interface, enable this option. You need the openssh-server package
installed for this option to be useful.</description>
<port
protocol="tcp" port="22"/>
</service>
```

Чтобы включить поддержку сервиса в той или иной зоне, используйте опцию **--add-service=**. Указать целевую зону можно с помощью опции **--zone=**. По умолчанию эти изменения будут работать в течение одной сессии. Чтобы сохранить изменения и использовать их на постоянной основе, добавьте флаг **--permanent**.

Например, чтобы запустить веб-сервер для обслуживания трафика HTTP, для начала нужно включить поддержку этого трафика в зоне **public** на одну сессию:

```
sudo firewall-cmd --zone=public --add-service=http
```

Если сервис нужно добавить в зону по умолчанию, флаг **--zone=** можно опустить.

Убедитесь, что операция выполнена успешно:

```
firewall-cmd --zone=public --list-services
dhcpv6-client http ssh
```

Протестируйте работу сервиса и брандмауэра. Если все работает правильно, можно изменить постоянный набор правил и добавить в него правило для поддержки этого сервиса.

```
sudo firewall-cmd --zone=public --permanent --add-service=http
```

Чтобы просмотреть список постоянных правил, введите:

```
sudo firewall-cmd --zone=public --permanent --list-services
dhcpv6-client http ssh
```

Теперь зона public поддерживает HTTP и порт 80 на постоянной основе. Если веб-сервер может обслуживать трафик SSL/TLS, вы также можете добавить сервис https (для одной сессии или в набор постоянных правил):

```
sudo firewall-cmd --zone=public --add-service=https
sudo firewall-cmd --zone=public --permanent --add-service=https
```

Что делать, если нужный сервис недоступен?

Брандмауэр firewalld по умолчанию включает в себя многие наиболее распространённые сервисы. Однако некоторым приложениям необходимы сервисы, поддержка которых отсутствует в firewalld. В таком случае вы можете поступить двумя способами.

Способ 1: Настройка порта

Проще всего в такой ситуации открыть порт приложения в необходимой зоне брандмауэра. Нужно просто указать порт или диапазон портов и протокол.

Например, приложение, которое использует порт 5000 и протокол **TCP**, нужно добавить в зону **public**. Чтобы включить поддержку приложения на одну сессию, используйте параметр **--add-port=** и укажите протокол **tcp** или **udp**.

```
sudo firewall-cmd --zone=public --add-port=5000/tcp
```

Убедитесь, что операция прошла успешно:

```
firewall-cmd --list-ports
5000/tcp
```

Также можно указать последовательный диапазон портов, отделив первый и последний порт диапазона с помощью тире. Например,

если приложение использует UDP-порты 4990-4999, чтобы добавить их в зону **public**, нужно ввести:

```
sudo firewall-cmd --zone=public --add-port=4990-4999/udp
```

После тестирования можно добавить эти правила в постоянные настройки брандмауэра.

```
sudo firewall-cmd --zone=public --permanent --add-port=5000/tcp
sudo firewall-cmd --zone=public --permanent --add-port=4990-4999/udp
sudo firewall-cmd --zone=public --permanent --list-ports
success
success
4990-4999/udp 5000/tcp
```

Способ 2: Определение сервиса

Добавлять порты в зоны просто, но если у вас много таких приложений, в результате будет сложно отследить, для чего предназначен тот или иной порт. Чтобы избежать такой ситуации, можно вместо портов определить сервисы.

Сервисы – это просто наборы портов с определенным именем и описанием. С помощью сервисов проще управлять настройками, но сами по себе они сложнее, чем порты.

Для начала нужно скопировать существующий сценарий из каталога **/usr/lib/firewalld/services** в каталог **/etc/firewalld/services** (здесь брандмауэр ищет нестандартные настройки).

Например, можно скопировать определение сервиса SSH и использовать его для определения условного сервиса **example**. Имя сценария должно совпадать с именем сервиса и иметь расширение **.xml**.

```
sudo cp /usr/lib/firewalld/services/service.xml /etc/firewalld/services/example.xml
```

Откорректируйте скопированный файл.

```
sudo nano /etc/firewalld/services/example.xml
```

В файле находится определение SSH:

```
<?xml version="1.0" encoding="utf-8"?> <service> <short>SSH</short> <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description> <port protocol="tcp" port="22"/> </service>
```

Большую часть определения сервиса составляют метаданные. Изменить краткое имя сервиса можно в тегах . Это человекочитаемое имя сервиса. Также нужно добавить описание сервиса. Единственное изменение, которое повлияет на работу сервиса – это изменение номера порта и протокола.

Вернёмся к сервису example; допустим, он требует открыть TCP- порт 7777 и UDP- порт 8888. Определение будет выглядеть так:

```
<?xml version="1.0" encoding="utf-8"?> <service> <short>Example Service</short> <description>This is just an example service.  It probably shouldn't be used on a real system.</description> <port protocol="tcp" port="7777"/> <port protocol="udp" port="8888"/> </service>
```

Сохраните и закройте файл.

Перезапустите брандмауэр:

```
sudo firewall-cmd --reload
```

Теперь сервис появится в списке доступных сервисов:

```
firewall-cmd
--get-services
RH-Satellite-6 amanda-client bacula bacula-client
dhcp dhcpv6 dhcpv6-client dns example ftp high-availability http
https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt
libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy
pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba
samba-client smtp ssh telnet tftp tftp-client transmission-client
```

```
vnc-server wbem-https
```

Создание зон

Брандмауэр предоставляет много предопределенных зон, которых в большинстве случаев достаточно для работы. Но в некоторых ситуациях возникает необходимость создать пользовательскую зону.

Например, для веб-сервера можно создать зону **publicweb**, а для DNS-сервиса – зону **privateDNS**.

Создавая зону, нужно добавить её в постоянные настройки брандмауэра.

Попробуйте создать зоны **publicweb** и **privateDNS**:

```
sudo firewall-cmd --permanent --new-zone=publicweb
sudo firewall-cmd --permanent --new-zone=privateDNS
```

Убедитесь, что зоны существуют:

```
sudo firewall-cmd --permanent --get-zones
block dmz drop external home internal privateDNS public publicweb trusted work
```

В текущей сессии новые зоны не будут доступны:

```
firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

Чтобы получить доступ к новым зонам, нужно перезапустить брандмауэр:

```
sudo firewall-cmd --reload
firewall-cmd --get-zones
block dmz drop external home internal privateDNS public publicweb trusted work
```

Теперь вы можете присвоить новым зонам требуемые сервисы и порты. К примеру, в зону **publicweb** можно добавить SSH, HTTP и HTTPS.

```
sudo firewall-cmd --zone=publicweb --add-service=ssh
sudo firewall-cmd --zone=publicweb --add-service=http
sudo firewall-cmd --zone=publicweb --add-service=https
firewall-cmd --zone=publicweb --list-all
publicweb
interfaces:
sources:
services: http https ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

В зону **privateDNS** можно добавить DNS:

```
sudo firewall-cmd --zone=privateDNS --add-service=dns
firewall-cmd --zone=privateDNS --list-all
privateDNS
interfaces:
sources:
services: dns
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Затем можно привязать сетевые интерфейсы к новым зонам:

```
sudo firewall-cmd --zone=publicweb --change-interface=eth0
sudo firewall-cmd --zone=privateDNS --change-interface=eth1
```

Теперь можно протестировать настройку. Если всё работает правильно, вы можете добавить эти правила в постоянные настройки.

```
sudo firewall-cmd --zone=publicweb --permanent --add-service=ssh
sudo firewall-cmd --zone=publicweb --permanent --add-service=http
sudo firewall-cmd --zone=publicweb --permanent --add-service=https
sudo firewall-cmd --zone=privateDNS --permanent --add-service=dns
```

После этого можно настроить сетевые интерфейсы для автоматического подключения к правильной зоне.

К примеру, **eth0** будет привязан к **publicweb**:

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

Содержимое файла:

```
. . . IPV6_AUTOCONF=no DNS1=2001:4860:4860::8844 DNS2=2001:4860:4860::8888 DNS3=8.8.8.8 ZONE=publicweb
```

А интерфейс eth1 будет привязан к privateDNS:

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth1
```

Содержимое файла:

```
. . . NETMASK=255.255.0.0 DEFROUTE='no' NM_CONTROLLED='yes' ZONE=privateDNS
```

Перезапустите сетевые сервисы и брандмауэр:

```
sudo systemctl restart network
sudo systemctl restart firewalld
```

Проверьте зоны:

```
firewall-cmd --get-active-zones
privateDNS
interfaces: eth1
publicweb
interfaces: eth0
```

Убедитесь, что в зонах работают нужные сервисы:

```
firewall-cmd --zone=publicweb --list-services
http htpps ssh
firewall-cmd --zone=privateDNS --list-services
dns
```

Пользовательские зоны полностью готовы к работе. Вы можете сделать любую из них зоной по умолчанию. Например:

```
sudo firewall-cmd --set-default-zone=publicweb
```

Автоматический запуск брандмауэра

Теперь, когда вы проверили все настройки и убедились, что все правила работают должным образом, вы можете настроить автозапуск брандмауэра.

Для этого введите:

```
sudo systemctl enable firewalld
```

Теперь брандмауэр будет запускаться вместе с сервером.

Заключение

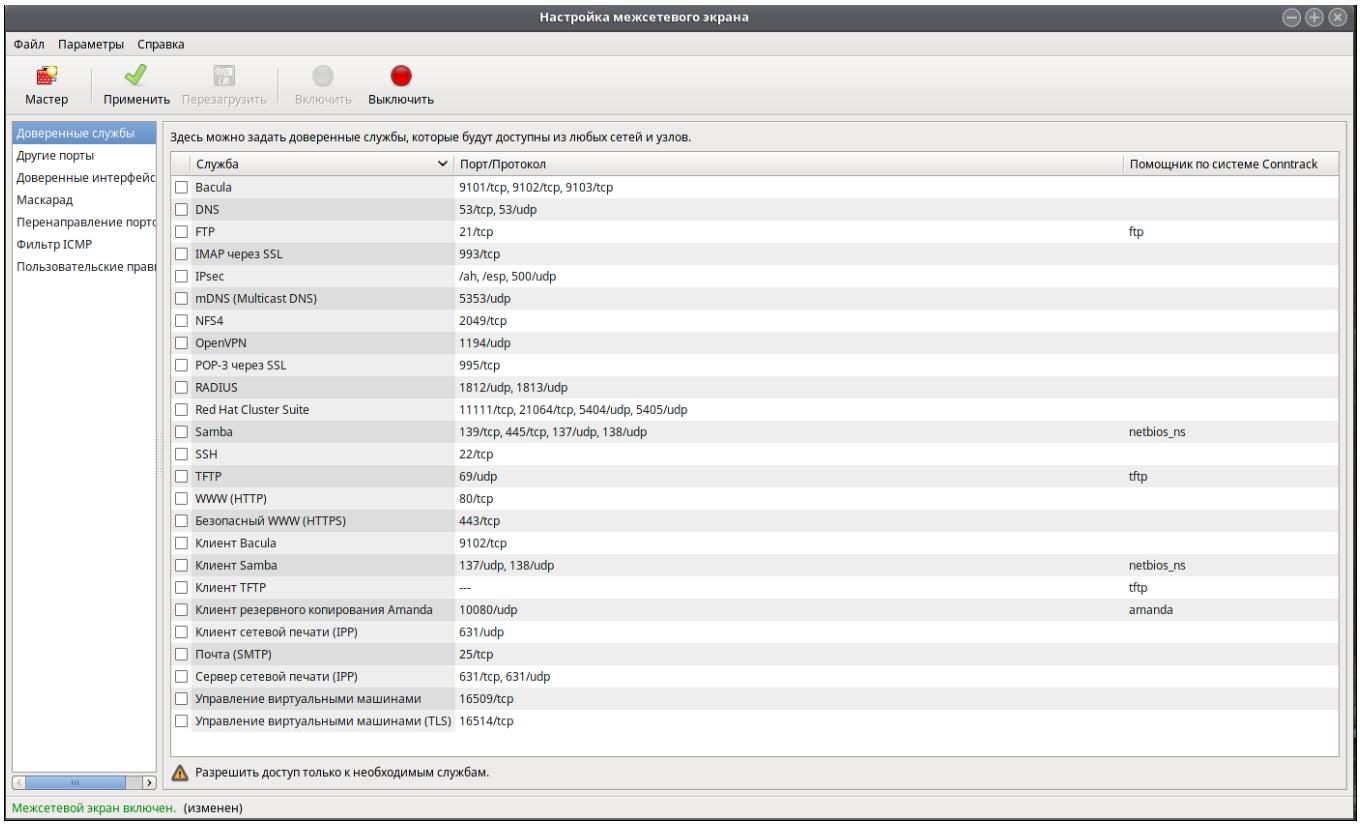
Брандмауэр firewalld — очень гибкий инструмент. Зоны позволяют быстро изменять политику брандмауэра.

Настройка iptables

Настройка в графическом режиме
Настройка iptables при помощи консольных команд
Просмотр и удаление правил
Прием и сбрасывание трафика в цепях
Разрешение и блокировка портов
Блокирование ICMP
Предотвращение несанкционированных действий на сервере

Настройка в графическом режиме

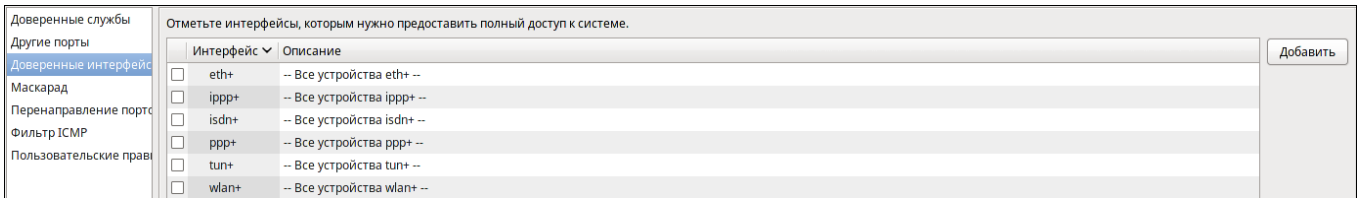
iptables в графическом режиме более удобен, но менее гибок по отношению к ручной настройке.



1) Здесь доступен уже предопределенный список служб, для которых можно открыть порты, по которым они работают нажатием на соответствующий флаг.

2) Также, если нужной службы нет в списке, порты для нее можно добавить вручную в разделе «**Другие порты**».

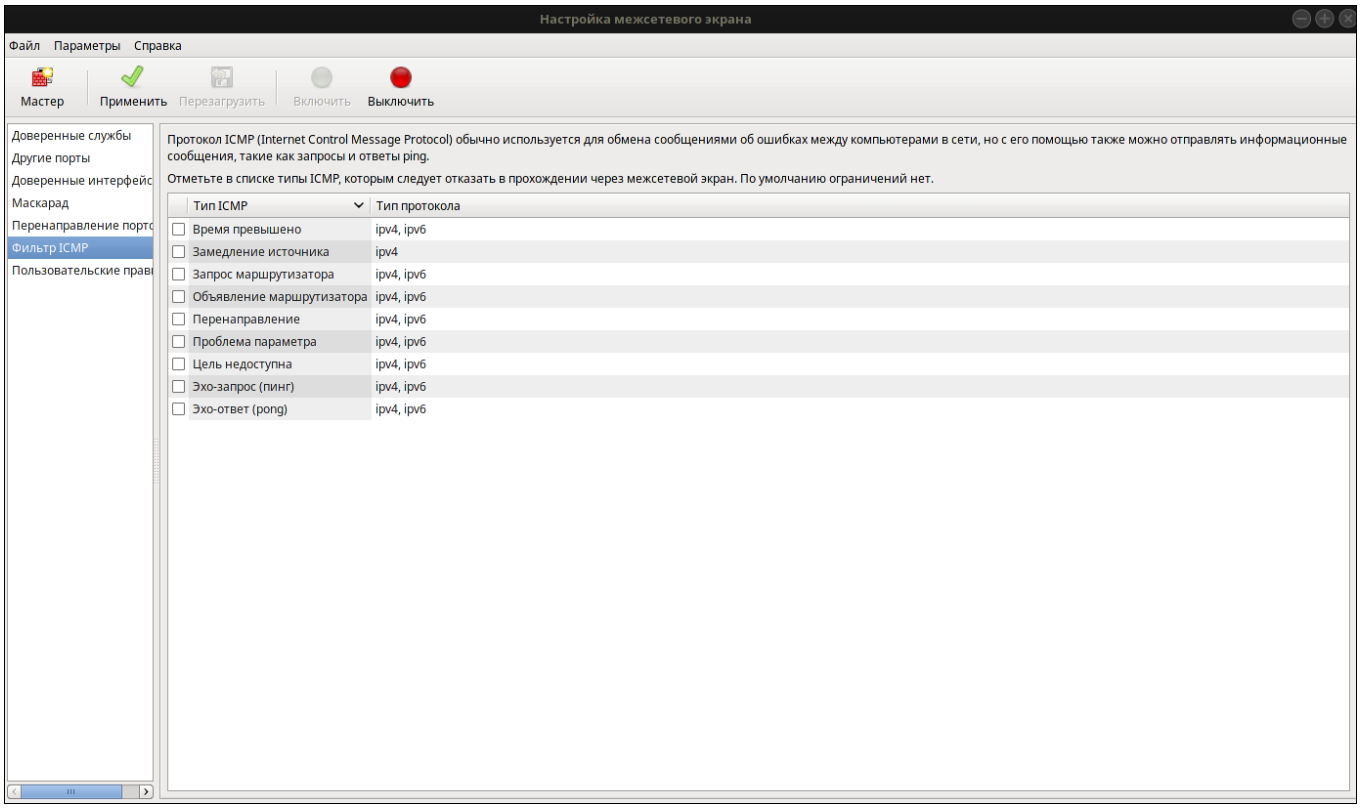
3) В пункте «**Доверенные интерфейсы**» можно выбрать интерфейсы, подключенные к доверенной сети.



4) Пункт «**Маскарад**» позволяет настроить узел, подключающий локальную сеть к интернету (из LAN в WAN), но при этом локальная сеть не будет видна извне, будет лишь доступен один адрес (только **IPv4**).

5) Если используется **Маскарад**, скорее всего возникнет потребность в перенаправлении портов из одной системы в другую (только **IPv4**).

6) Можно настроить фильтр **ICMP**, который работает ниже сетевого протокола, поэтому он используется для информирования о сети. Для этого протокола можно закрыть доступ, чтобы другая сторона не была информирована о вашей сети.



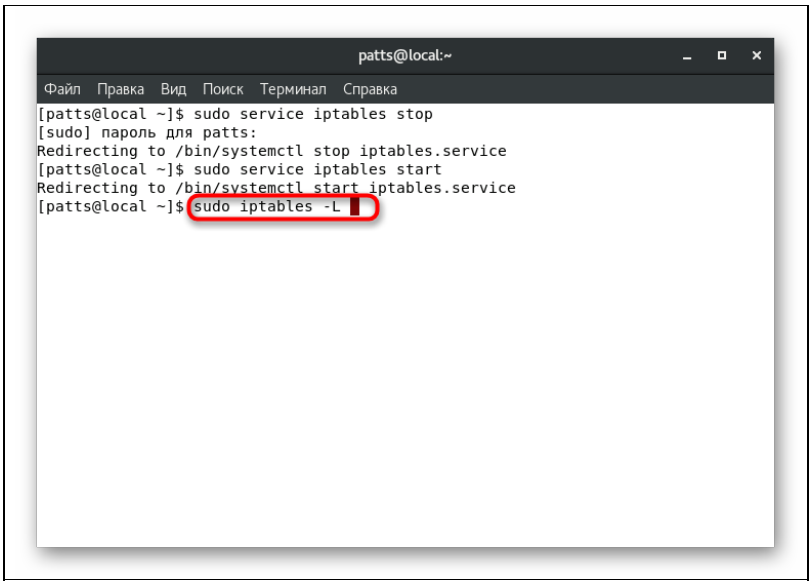
7) Можно добавить собственные готовые правила, если уже готов шаблон, их можно разом добавить и применить.

Настройка iptables при помощи консольных команд

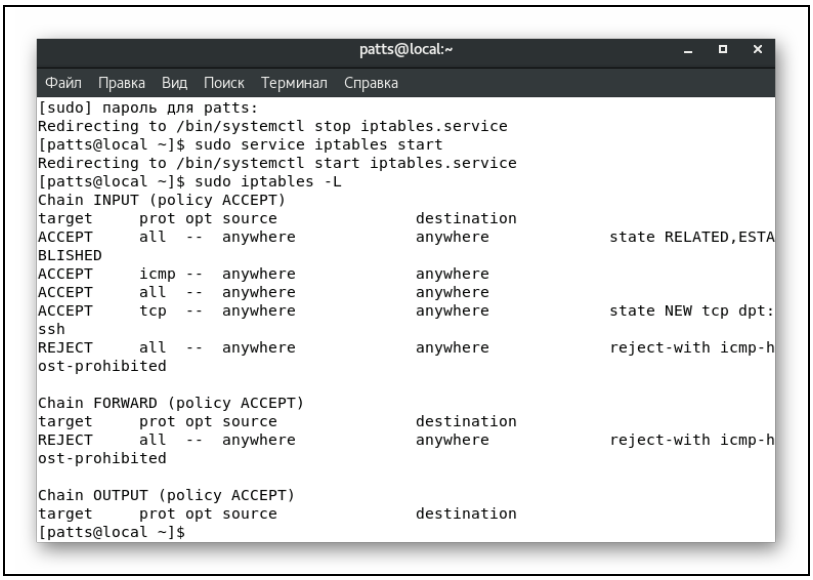
Просмотр и удаление правил

Как уже было сказано ранее, управление межсетевым экраном производится путем ручного или автоматического добавления правил. Например, некоторые дополнительные приложения могут обращаться к инструменту, изменяя определенные политики. Однако большинство подобных действий все же делается вручную. Просмотр списка всех текущих правил доступен через команду:

```
sudo iptables -L
```

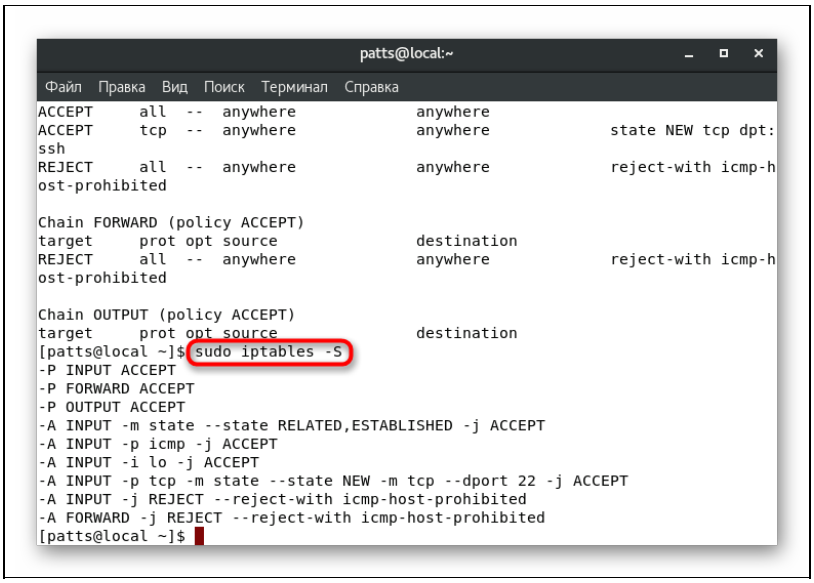


В отобразившемся результате будет информация по трем цепочкам: «**INPUT**», «**OUTPUT**» и «**FORWARD**» — входящий, исходящий и пересылаемый трафик соответственно.



Определить статус всех цепочек можно, выполнив:

```
sudo iptables -S
```



Если настроенные правила не выполняют необходимые задачи, их можно удалить. Весь список правил можно удалить с помощью команды:

```
sudo iptables -F
```

После активации правила будут стерты абсолютно для всех трех цепочек.

Когда необходимо затронуть только политики из какой-то одной цепи, к строке добавляется дополнительный аргумент:

```
sudo iptables -F INPUT
sudo iptables -F OUTPUT
sudo iptables -F FORWARD
```

Отсутствие всех правил означает, что сейчас не применяется никаких настроек фильтрации трафика ни в одну из сторон. Далее системный администратор уже самостоятельно задает новые параметры, используя всю ту же консоль, команду и различные аргументы.

Прием и сбрасывание трафика в цепях

Каждая цепь настраивается отдельно для приема или блокирования трафика. Выставив определенное значение, можно добиться того, что, например, весь входящий трафик будет блокироваться. Для этого команда должна иметь вид:

```
sudo iptables --policy INPUT DROP
```

где **INPUT** — название цепи, а **DROP** — значение сброса.

Точно такие же параметры задаются и для других цепей, например:

```
sudo iptables --policy OUTPUT DROP
```

Если же необходимо выставить значение на прием трафика, тогда **DROP** изменяется на **ACCEPT** и получается:

```
sudo iptables --policy INPUT ACCEPT
```

Разрешение и блокировка портов

Как известно, все сетевые приложения и процессы работают через определенный порт. Путем блокировки или разрешения определенных адресов можно контролировать доступ всех сетевых целей. Давайте разберем проброс порта на примере **80**. В терминале будет достаточно ввести команду:

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

где:

- **-A** — добавление нового правила;
- **INPUT** — указание цепи;
- **-P** — определение протокола, в этом случае TCP;
- **--dport** — порт назначения.

Точно такая же команда относится и к порту **22**, который используется сервисом **SSH**:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Для блокирования указанного порта применяется строка точно такого же вида, только в конце **ACCEPT** изменяется на **DROP**. В итоге получается:

```
sudo iptables -A INPUT -p tcp --dport 2450 -j DROP
```

Все эти правила заносятся в конфигурационный файл, и вы можете просмотреть их в любой момент. Напоминаем, осуществляется это через sudo iptables -L. Если вместе с портом необходимо разрешить еще и сетевой IP-адрес, строка немного видоизменяется — после **tcp** добавляется **-s** и сам адрес:

```
sudo iptables -A INPUT -p tcp -s 12.12.12.12/32 --dport 22 -j ACCEPT
```

где **12.12.12.12/32** — необходимый IP-адрес.

Блокирование происходит по тому же принципу, меняя в конце значение **ACCEPT** на **DROP**. Тогда получается;

```
sudo iptables -A INPUT -p tcp -s 12.12.12.0/24 --dport 22 -j DROP
```

Блокирование ICMP

ICMP (Internet Control Message Protocol) — протокол, который входит в состав TCP/IP и задействован для передачи сообщений об ошибках и экстренных ситуациях при работе с трафиком. Например, когда запрашиваемый сервер недоступен, именно этот инструмент выполняет сервисные функции. Утилита **iptables** позволяет заблокировать его через брандмауэр, а сделать это можно командой:

```
sudo iptables -A OUTPUT -p icmp --icmp-type 8 -j DROP
```

Она произведет блокировку запросов **от** вашего и **к** вашему серверу.

Входящие запросы блокируются немного иначе. Тогда нужно ввести:

```
sudo iptables -I INPUT -p icmp --icmp-type 8 -j DROP
```

После активации данных правил сервер не будет отвечать на **ping**-запросы.

Предотвращение несанкционированных действий на сервере

Иногда серверы подвергаются DDoS-атакам или другим несанкционированным действиям со стороны злоумышленников. Правильная настройка межсетевого экрана позволит обезопасить себя от подобного рода взломов. Для начала рекомендуется задать следующие правила:

1. Пропишите в консоли:

```
sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 20/minute --limit-burst 100 -j ACCEPT
```

где:

- `--limit 20/minute` — ограничение на частоту положительных результатов. Единицу измерения вы можете указывать самостоятельно, например, **/second**, **/minute**, **/hour**, **/day**;
- `--limit-burst number` — ограничение на число пропускаемых пакетов. Все значения выставляются индивидуально по предпочтениям администратора.

2. Далее можно запретить сканирование открытых портов, чтобы убрать одну из возможных причин взлома. Введите первую команду:

```
sudo iptables -N block-scan
```

3. Затем укажите:

```
sudo iptables -A block-scan -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j RETURN
```

4. Последняя команда имеет вид:

```
sudo iptables -A block-scan -j DROP
```

Выражение **block-scan** в данных случаях — название используемой цепи.

Для того чтобы **новые правила вступили в силу**, необходимо сохранить конфигурацию и вновь запустить службу **iptables**:

```
sudo iptables-save > /etc/sysconfig/iptables
sudo systemctl enable --now iptables.service
```

Тестирование пропускной способности сети с помощью iperf3

Iperf — кроссплатформенная консольная клиент-серверная программа — генератор TCP и UDP трафика для тестирования пропускной способности сети.

Вы можете подробнее ознакомиться с утилитами мониторинга работы сети, просмотрев наши обучающие видео:

- на **RuTube** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **Яндекс.Дзен** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **VK Видео** — Сеть в РЕД ОС. Утилиты мониторинга работы сети.

На наших каналах вы также сможете найти много другой полезной информации.

Установка утилиты происходит на 2 машинах: одна выступает в роли сервера, другая в роли клиента.

```
dnf install iperf3
```

Запуск на стороне сервера

```
iperf3 -s
```

```
[root@localhost ~]# iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 10.81.81.202, port 55840
[  5] local 10.81.1.206 port 5201 connected to 10.81.81.202 port 55842
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  82.9 MBytes   696 Mbits/sec
[  5]   1.00-2.00   sec  88.1 MBytes   739 Mbits/sec
[  5]   2.00-3.00   sec  86.2 MBytes   723 Mbits/sec
[  5]   3.00-4.00   sec  87.3 MBytes   732 Mbits/sec
[  5]   4.00-5.00   sec  86.0 MBytes   722 Mbits/sec
[  5]   5.00-6.00   sec  88.6 MBytes   743 Mbits/sec
[  5]   6.00-7.00   sec  87.8 MBytes   736 Mbits/sec
[  5]   7.00-8.00   sec  83.9 MBytes   704 Mbits/sec
[  5]   8.00-9.00   sec  90.7 MBytes   761 Mbits/sec
[  5]   9.00-10.00  sec  90.5 MBytes   759 Mbits/sec
[  5]  10.00-10.01  sec   841 KBytes   733 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.01  sec   873 MBytes   732 Mbits/sec                  receiver
-----------------------------------------------------------
```

Запуск на стороне клиента:

```
iperf3 -c server_address
```

```
[root@localhost ~]# iperf3 -c 10.81.1.206
Connecting to host 10.81.1.206, port 5201
[  5] local 10.81.81.202 port 56010 connected to 10.81.1.206 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  81.6 MBytes   684 Mbits/sec  272   1.93 MBytes
[  5]   1.00-2.00   sec  92.5 MBytes   776 Mbits/sec   66   1.03 MBytes
[  5]   2.00-3.00   sec  88.8 MBytes   744 Mbits/sec    0   1.10 MBytes
[  5]   3.00-4.00   sec  87.5 MBytes   734 Mbits/sec    0   1.15 MBytes
[  5]   4.00-5.00   sec  90.0 MBytes   755 Mbits/sec    0   1.19 MBytes
[  5]   5.00-6.00   sec  88.8 MBytes   744 Mbits/sec    0   1.25 MBytes
[  5]   6.00-7.00   sec  87.5 MBytes   734 Mbits/sec    4    938 KBytes
[  5]   7.00-8.00   sec  81.2 MBytes   682 Mbits/sec    0   1.02 MBytes
[  5]   8.00-9.00   sec  87.5 MBytes   734 Mbits/sec    0   1.10 MBytes
[  5]   9.00-10.00  sec  86.2 MBytes   724 Mbits/sec    0   1.17 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec   872 MBytes   731 Mbits/sec  342             sender
[  5]   0.00-10.01  sec   870 MBytes   729 Mbits/sec                  receiver

iperf Done.
```

В ходе выполнения команд выполняется 10 секундная передача данных, на основе которых выдается скорость сети.

Вывод подсказки о том, как использовать **iperf3**:

```
iperf3 -h
```

Вывод информации об активных сетевых соединениях с помощью iftop

Iftop - показывает информацию об активных сетевых соединениях . С её помощью можно мониторить трафик в режиме online, причем с разделением по протоколам, интерфейсам и хостам.

Вы можете подробнее ознакомиться с утилитами для получения информации об активных сетевых соединениях, просмотрев наши обучающие видео:

- на **RuTube**:
    - Информация, мониторинг и тестирование системы;
    - Сеть в РЕД ОС. Утилиты мониторинга работы сети.
- в **Яндекс.Дзен**:
    - Информация, мониторинг и тестирование системы;
    - Сеть в РЕД ОС. Утилиты мониторинга работы сети.
- в **VK Видео**:
    - Информация, мониторинг и тестирование системы;
    - Сеть в РЕД ОС. Утилиты мониторинга работы сети.

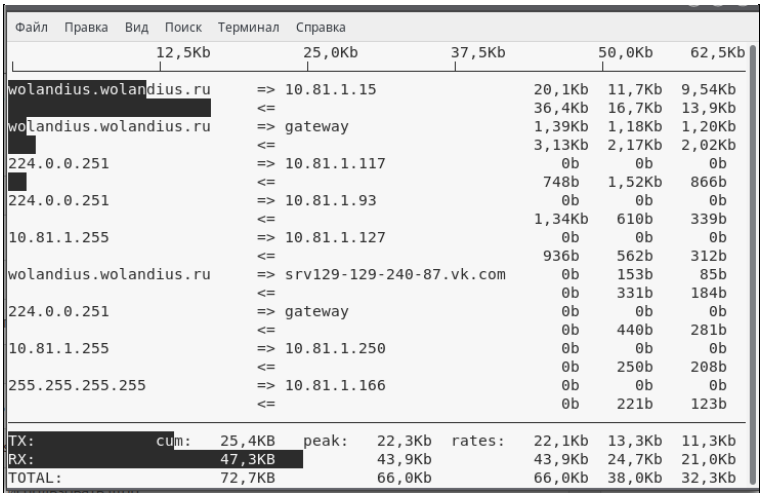
На наших каналах вы также сможете найти много другой полезной информации.

Установка:

```
dnf install iftop
```

Запуск утилиты:

```
iftop
```



Вывод трафика в байтах:

```
iftop -i eth0 -B
```

Трафик между локальным интерфейсом и хостом 8.8.8.8

```
iftop -i eth0 -f "dst 8.8.8.8"
```

Вывод подсказки, как использовать iftop:

```
iftop -h
```

Мониторинг сетевого трафика с помощью nethogs

Nethogs - это утилита, используемая для мониторинга пропускной полосы сетевого трафика в реальном времени, используемой каждым процессом или приложением.

Вы можете подробнее ознакомиться с утилитами мониторинга работы сети, просмотрев наши обучающие видео:

- на **RuTube** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **Яндекс.Дзен** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **VK Видео** — Сеть в РЕД ОС. Утилиты мониторинга работы сети.

На наших каналах вы также сможете найти много другой полезной информации.

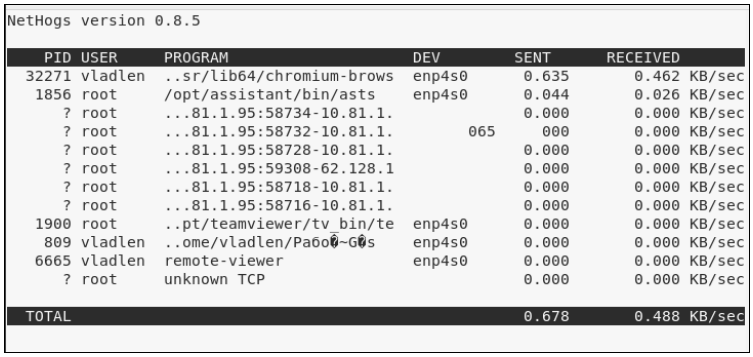
Для использования nethogs необходимы права администратора.

Установка утилиты:

```
dnf install nethogs
```

Запуск утилиты производится командой:

```
nethogs
```



Просмотр трассировки:

```
nethogs -t
```

Просмотр основного списка доступных команд:

```
nethogs -h
```

Когда nethogs запущен доступно:

```
q: выход
s: отсортировать трафик по критерию SENT
r: отсортировать трафик по критерию RECEIVE
m: переключить режимы между kb/s, m/s
```

Отображение информации о сетевых сокетах с помощью ss

Использование утилиты ss
Вывод информации по IP-адресу
Вывод информации по состоянию сокета
Вывод информации по имени сервиса или номеру порта

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: iproute2-6.1.0

ss — консольная утилита, которая предоставляет информацию о сетевых сокетах, подключениях **TCP/UDP**, маршрутизации и других сетевых статистических данных.

ss отображает информацию аналогично утилите **netstat** и при этом выводит больше информации о сетевых соединениях и их состоянии, чем какие-либо другие инструменты.

Информация о сокете выводится в виде таблицы. Каждый столбец отображает определенную информацию, относящуюся к сокету.

Описание выводимой информации в столбцах:

- `Netid` — отображает тип сокета;
- `State` — отображает состояние сокета. Может принимать следующие значения: сокет установлен — **ESTAB**, сокет не подключен — **UNCONN**, сокет прослушивается — **LISTEN**.
- `Recv-Q` — отображает количество принятых пакетов в очереди;
- `Send-Q` — отображает количество отправленных пакетов в очереди;
- `Local address:port` — показывает адрес локальной машины и порт;
- `Peer address:port` — отображает адрес удаленной машины и порт.

Использование утилиты ss

Синтаксис утилиты **ss** выглядит следующим образом:

```
ss <опции>
```

Утилита ss может принимать несколько опций:

```
ss <опция_1> <опция_2> <опция_3> ...
```

Основные опции утилиты **ss**:

- `-V, --version` — показать версию утилиты;
- `-n, --numeric` — не определять имена служб;
- `-r, --resolve` — определять сетевые имена адресов с помощью DNS;
- `-a, --all` — отобразить все сокеты (открытые соединения);
- `-l, --listening` — показать только прослушиваемые сокеты;
- `-o, --options` — показать информацию таймера;
- `-e, --extended` — выводить расширенную информацию о сокете;
- `-p, --processes` — показать процессы, использующие сокет;
- `-i, --info` — посмотреть внутреннюю информацию TCP;
- `-s, --summary` — статистика использования сокета;
- `-D, --diag=<файл>` — экспортировать текущее состояние TCP-сокетов в файл;
- `-F, --filter=<файл>` — работать с информацией, взятой из файла.

Можно выводить информацию о сокете, который использует только необходимый протокол, используя следующие опции:

- `-4, --ipv4` — только сокеты протокола IPv4;
- `-6, --ipv6` — только сокеты протокола IPv6;
- `-0, --packet` — только PACKET-сокеты;
- `-t, --tcp` — TCP-сокеты;
- `-u, --udp` — UDP-сокеты;
- `-x, --unix` — UNIX-сокеты.

Для отображения всех TCP-соединений выполните команду:

```
ss -ta
```

Для отображения всех UDP-соединений выполните команду:

```
ss -ua
```

Для вывода информации о подключенных TCP- и UDP-сокетах, а также информации о процессах, которые используют сокеты — имя процесса и его PID, выполните:

```
ss -tupn
```

Для отображения открытых TCP- и UDP-сокетов, которые ожидают соединение, выполните команду, добавив опцию -l:

```
ss -tupnl
```

Вывод информации по IP-адресу

Утилита поддерживает фильтрацию информации об установленных подключениях по адресу назначения и по адресу получения.

Для фильтрации информации по адресу назначения выполните:

```
ss dst xx.xx.xx.xx
```

Для фильтрации информации по адресу получения выполните:

```
ss src xx.xx.xx.xx
```

где xx.xx.xx.xx — IP-адрес, по которому необходимо отфильтровать информацию.

Вывод информации по состоянию сокета

Можно отфильтровать информацию по состоянию сокета. Для этого используется дополнительный ключ `state`.

Состояния, которые может принимать сокет:

- *established*;
- *listening*;
- *syn-sent*;
- *syn-recv*;
- *time-wait*;
- *closed*;
- *close-wait*;
- *last-ack*;
- *fin-wait-1*;
- *fin-wait-2*;
- *closing*.

Кроме того, ss распознаёт следующие идентификаторы состояний:

- *all* — все состояния;
- *connected* — все состояния, кроме прослушиваемых и закрытых;
- *synchronized* — все состояния, кроме *syn-sent*;
- *bucket* — состояния, представляющие собой минисокеты, например, *time-wait* или *syn-recv*;
- *big* — все состояния, кроме *bucket*.

Для отображения всех открытых TCP-портов выполните команду:

```
ss -t state listening
```

Для отображения всех успешных соединений по IPv4 выполните:

```
ss -4 state established
```

Вывод информации по имени сервиса или номеру порта

Для фильтрации информации по номеру порта или его имени утилите необходимо передать соответствующие опции:

- для порта получения:

```
ss <опции> sport = :<порт>
```

- для порта назначения:

```
ss <опции> dport = :<порт>
```

где <порт> — номер порта или имя сервиса.

Для фильтрации TCP-соединения с выводом информации об использовании только порта получателя **22** выполните:

```
ss -ta '( sport = :22 )'
```

Для фильтрации TCP-соединения с выводом информации об использовании сервиса **HTTPS** в адресе назначения выполните:

```
ss -ta '( dport = :https )'
```

Мониторинг использования сетевого канала с помощью trafshow

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** trafshow 5.2.3-1

Trafshow помогает оценить интенсивность использования канала, постоянно показывает информацию о пакетном трафике для конфигурации сетевого интерфейса и периодически сортирует и обновляет эту информацию.

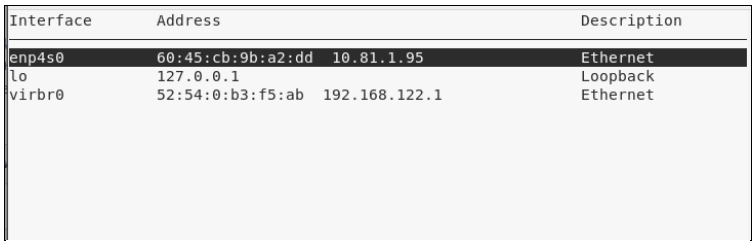
Вы можете подробнее ознакомиться с утилитами мониторинга работы сети, просмотрев наши обучающие видео:

- на **RuTube** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **Яндекс.Дзен** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **VK Видео** — Сеть в РЕД ОС. Утилиты мониторинга работы сети.

На наших каналах вы также сможете найти много другой полезной информации.

Установка:

```
dnf install trafshow
```



Запуск утилиты

```
trafshow
```

Запуск с определенным интерфейсом, к примеру enp4s0

```
trafshow -i enp4s0
```

Вывод подсказки о том, как использовать trafshow:

```
trafshow -h
```

Анализ и фильтрация сетевых пакетов с помощью tcpdump

Назначение утилиты
Синтаксис утилиты
Опции утилиты
Фильтры утилиты
Примеры использования утилиты

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tcpdump-14:4.9.3-3

tcpdump – инструмент командной строки для анализа пакетов, который позволяет перехватывать сетевые пакеты на основе правил фильтрации, интерпретировать содержимое пакетов и отображать результат в удобочитаемом формате. По умолчанию утилита предустановлена в РЕД ОС.

Однако если по каким-либо причинам утилита отсутствует в системе, перейдите в сеанс пользователя **root**:

```
su -
```

и установите ее командой:

```
dnf install tcpdump
```

Для работы с утилитой необходимы права суперпользователя **root** или администратора системы (**sudo**), поэтому здесь и далее команды выполняются с правами суперпользователя **root**, если не указано иное.

Назначение утилиты

Утилита **tcpdump** помогает:

- диагностировать потерю пакетов;
- проверять производительность приложений;
- проверять маршрутизацию трафика в многосетевой среде;
- отслеживать теги VLAN;
- прослушивать трафик.

По умолчанию **tcpdump** прослушивает сетевой интерфейс с наименьшим номером в списке, поэтому сначала необходимо определить, какой интерфейс будет прослушиваться.

Синтаксис утилиты

Синтаксис команды **tcpdump** имеет следующий вид:

```
tcpdump [-опции] [фильтры]
```

Для отображения списка сетевых интерфейсов, используемых в системе, выполните команду:

```
tcpdump -D
```

```
1.wlo1 [Up, Running]
2.enp0s20f0u1 [Up, Running]
3.lo [Up, Running, Loopback]
4.any (Pseudo-device that captures on all interfaces) [Up, Running]
5.virbr0 [Up]
6.bluetooth-monitor (Bluetooth Linux Monitor) [none]
7.nflog (Linux netfilter log (NFLOG) interface) [none]
8.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
9.bluetooth0 (Bluetooth adapter number 0) [none]
10.usbmon0 (Raw USB traffic, all USB buses) [none]
11.usbmon1 (Raw USB traffic, bus number 1)
12.usbmon2 (Raw USB traffic, bus number 2)
```

Для прослушивания конкретного сетевого интерфейса необходимо использовать опцию **-i** с именем интерфейса, передаваемого в качестве параметра. Например, для интерфейса под номером 2 команда будет иметь следующий вид:

```
tcpdump -i enp0s20f0u1
```

Если необходимо захватить трафик со всех сетевых интерфейсов, например, если в системе несколько сетевых подключений, в **tcpdump** для таких случаев предусмотрен специальный параметр **any**:

```
tcpdump -i any
```

Опции утилиты

Описание некоторых опций **tcpdump**:

Опция	Описание
-a	Преобразовать сетевые и широковещательные адреса в доменные имена.
-e	Отображать данные канального уровня (MAC-адрес, протокол, длина пакета). Помимо IP-адресов будут отображены MAC-адреса компьютеров.
-N	Не добавлять доменное расширение к именам узлов. Например, отобразить **net** вместо **net.library.org**.
-n	Отображать IP-адрес вместо имени хоста.
-nn	Отображать номер порта вместо используемого протокола.
-q	Вывести минимум информации. Обычно – имя протокола, отправитель и получатель пакета, используемые порты и объем переданных данных.
-r	Прочесть трафик из файла, если он был предварительно сохранен параметром **-w**.
-S	Не обрабатывать абсолютные порядковые номера (initial sequence number — ISN) в относительные.
-t	Не отображать метку времени в каждой строке.
-tt	Отображать неформатированную метку времени в каждой строке.
-tttt	Показывать дату и время.
-v	Выводить подробную информацию (TTL; ID; общая длина заголовка, а также его параметры; производить проверку контрольных сумм IP и ICMP-заголовков).
-vv	Выводить ещё более полную информацию, в основном относится к NFS и SMB.
-vvv	Выводить максимально подробную информацию.
-w <файл>	Сохранять данные **tcpdump** в двоичном формате. Преимущества использования данного способа по сравнению с обычным перенаправлением в файл является высокая скорость записи и возможность чтения подобных данных другими программами, например, snort, но этот файл нельзя прочитать человеку.
-c <число>	Завершит работу **tcpdump** после получения указанного числа пакетов.

Описанные опции помогают отфильтровывать информативность пакетов, перенаправлять вывод в файл или прочитать уже записанный файл и т.д. Для получения более подробной информации по всем доступным опциям утилиты **tcpdump** можно воспользоваться командой:

```
man tcpdump
```

Фильтры утилиты

Для упрощения поиска пакетов и экономии времени в **tcpdump** предусмотрены фильтры. Они используются для отсеивания ненужных пакетов. Таким образом можно вывести список пакетов, полученных от какого-либо конкретного IP-адреса или подсети.

Описание фильтров для **tcpdump**:

- **host**, **net**, **port** – для фильтрации по значению соответствующего идентификатора;
- **src**, **dst** – для фильтрации по конкретному направлению передачи к и/или от идентификатора;
- **tcp**, **udp**, **icmp**, **ah** – для фильтрации по заданному сетевому протоколу.

Примеры использования утилиты

Для просмотра исходящего и входящего трафика по IP-адресу выполните команду с фильтром **host** и соответствующим аргументом:

```
tcpdump host 192.168.1.1
```

Для обнаружения пакетов, следующих из определенной сети либо в нее, используйте команду с фильтром **net**:

```
tcpdump net 192.168.1.0/24
```

Для захвата трафика, который поступает только на определенный порт, выполните команду с фильтром **port** и номером соответствующего порта в качестве аргумента:

```
tcpdump port 22
```

Для отсеивания трафика по отправителю с помощью фильтра **src**, выполните команду:

```
tcpdump src 192.168.1.1
```

Для отображения входящего трафика с IP-адреса выполните команду:

```
tcpdump dst 192.168.1.1
```

Для поиска конкретного типа трафика используются фильтры **tcp**, **udp**, **icmp**. Например, фильтр **icmp** поможет вывести на экран весь трафик, передаваемый по протоколу **ICMP**:

```
tcpdump icmp
```

Настройка сервера Port Knocking

Настройка сервера
Предварительная настройка брандмауэра
Установка и настройка службы knockd
Настройка клиента

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер минимальный, сервер графический
- **Версия ПО**: knock-server-0.8-1

Knock — программное обеспечение, осуществляющее работу с использованием механизма **Port Knocking** в среде операционной системы РЕД ОС.

Port Knocking имеет следующий принцип работы – сетевой порт является по умолчанию закрытым до тех пор, пока на него не поступит заранее определённая последовательность пакетов данных, которая «заставит» порт открыться. Например, можно сделать недоступным для внешних подключений порт SSH, но в то же время открывать его только для тех, кто знает необходимую последовательность.

Вы можете подробнее ознакомиться с настройкой сервера **Port Knocking**, просмотрев наши обучающие видео:

- на **RuTube** — Механизм защиты сервера Port Knocking;
- в **Яндекс.Дзен** — Механизм защиты сервера Port Knocking;
- в **VK Видео** — Механизм защиты сервера Port Knocking.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка сервера

Предварительная настройка брандмауэра

Для организации работы механизма **Port Knocking** в системе необходимо правильно настроить брандмауэр. Цепочка правил **INPUT**, которая отвечает за фильтрацию входящих подключений, обязательно должна начинаться с правила, разрешающего уже установленные и связанные соединения, а завершаться правилом, запрещающим любые входящие подключения. Между ними должны располагаться правила, разрешающие доступ к отдельным сервисам.

В минимальной конфигурации должны присутствовать следующие два правила, где **enp9s0** – имя внешнего интерфейса:

```
# Разрешить установленные и связанные соединения
 iptables -A INPUT -i enp9s0 -m state --state ESTABLISHED,RELATED -j ACCEPT
 # Запретить входящие соединения извне
 iptables -A INPUT -i enp9s0 -j DROP
```

Данные команды можно ввести в консоли, и они начнут действовать немедленно. Однако обратите внимание, если команды будут выполняться удаленно с подключением через внешний интерфейс, можно **полностью потерять связь** с сервером до его последующей перезагрузки. В этом случае (при удаленном подключении) необходимо добавить между двумя вышеуказанными правилами еще одно дополнительное правило и не удалять его до тех пор, пока работа **Port Knocking** не будет организована как требуется.

```
# Разрешить подключение по SSH
 iptables -A INPUT -i enp9s0 -p tcp --dport 22 -j ACCEPT
```

Если указанные выше команды выполняются в терминале, разрешающее правило для **SSH** следует вводить после правила, разрешающего установленные и связанные соединения.

После проведенных манипуляций перезапустите службу **iptables** командой:

```
systemctl restart iptables
```

Значения будут применены автоматически.

Установка и настройка службы knockd

Для реализации механизма **Port Knocking** необходимо настроить службу **knockd**, которая находится в репозитории РЕД ОС в составе пакета **knock-server**.

Для установки **knock-server** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install knock-server
```

После установки необходимо отредактировать конфигурационный файл **/etc/knockd.conf**. В нем должна остаться только секция [options], которую необходимо привести к следующему виду:

```
[options]
 UseSyslog
 Interface = enp9s0
```

где:

- UseSyslog – указывает, что события будут записываться в системный журнал;
- Interface – имя сетевого интерфейса, который будет слушать **knockd** (в примере указан интерфейс enp9s0).

После этого требуется создать секцию для доступа по **SSH**:

```
[SSH]
 sequence = 7000,9000,8000
 seq_timeout = 5
 tcpflags = syn
 start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 stot_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 cmd_timeout = 60
```

где:

- sequence – задает последовательность подключений, по умолчанию используется протокол **tcp**, но если необходимо использовать протокол **udp**, следует указать его в формате <номер_порта>:<протокол>, например:

```
[SSH]
 sequence = 7000,9000:udp,8000
```

Так, порты **7000** и **8000** будут ожидать подключения по протоколу **tcp**, а порт **9000** — по протоколу **udp**.

- seq_timeout – время в секундах, за которое клиент должен совершить всю последовательность подключений. Значение следует указать минимальным, но при этом необходимо учитывать возможные задержки каналов связи как сервера, так и клиента;
- tcpflags – определяет TCP-флаги пакетов, которые будут участвовать в последовательности. Флаг **syn** рекомендуется использовать совместно с SSH, так как SSH-трафик может мешать **knockd**, признавая последовательность недействительной.
- start_command и stop_command – определяют команды, которые должен выполнить **knockd** с интервалом, указанном в опции cmd_timeout. Принцип действия следующий – получив указанную последовательность подключений, служба выполняет команду из опции start_command, по истечении заданного таймаута – команду stop_command.

Основной задачей является предоставление доступа к порту SSH на время, достаточное для установления подключения. Поэтому в параметр start_command в качестве первого правила в цепочку **INPUT** добавляется разрешение подключения к SSH с адреса источника подключения. Обратите внимание, что для этого используется ключ -I, который без указания номера добавляет правило первой строкой, а также подстановочную конструкцию -s %IP%, которая установит в правило текущий адрес подключающегося. Вторая команда удаляет уже добавленное правило.

Таким образом, порт будет открыт на подключение только для адреса клиента и только на время, указанное в таймауте. Обратите внимание, что значение таймаута необходимо только для осуществления подключения, после успешного подключения клиента и истечения таймаута текущее соединение не разрывается, а продолжает сохраняться и переходит в состояние ESTABLISHED за счет заданного правила в цепочке **INPUT**, которое разрешает установленные и связанные подключения.

Для сохранения конфигурации и запуска службы выполните команду:

```
systemctl start knockd
```

После завершения настройки можно попробовать подключиться к серверу с клиентской машины. Однако предварительно следует проверить состояние брандмауэра командой:

```
iptables -L -vn
```

```
[root@localhost user]# iptables -L -vn
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   29  2878 ACCEPT     all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 DROP       all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 16 packets, 3383 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

В выводе отображаются действующие правила, которые сигнализируют о том, что подключение к серверу невозможно.

Теперь можно попробовать выполнить подключение к серверу. Информацию о подключении клиента к серверу см. в разделе «Настройка клиента».

Затем снова стоит проверить состояние брандмауэра:

```
iptables -L -vn
```

```
[root@localhost user]# iptables -L -vn
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       192.168.8.4          0.0.0.0/0           tcp dpt:22
  595  243K ACCEPT     all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
   23  2460 DROP       all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

После подключения клиента первым в цепочке **INPUT** появилось правило, разрешающее доступ к SSH с адреса клиента.

Ровно через указанное в таймауте время (в примере 60 секунд) правило исчезнет, поэтому рекомендуется устанавливать значение таймаута достаточным для выполнения необходимых действий по подключению.

Возможности **knockd** не ограничиваются одним только управлением правилами сетевого фильтра. Можно настраивать **knockd** на запуск определенных скриптов, способных выполнять практически любые действия на сервере (от создания резервных копий до полного удаления каких-либо важных данных с сервера).

Настройка клиента

Подробную информацию о подключении клиента к серверу с помощью механизма **Port Knocking** см. в нашей статье «Механизм защиты сервера Port Knocking. Подключение клиента».

Подключение клиента Port Knocking

Настройка сервера
Настройка клиента
Установка knock
Подключение к серверу

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: knock-0.8-1

Knock — программное обеспечение, осуществляющее работу с использованием механизма **Port Knocking** в среде операционной системы РЕД ОС.

Port Knocking имеет следующий принцип работы – сетевой порт является по умолчанию закрытым до тех пор, пока на него не поступит заранее определённая последовательность пакетов данных, которая «заставит» порт открыться. Например, можно сделать недоступным для внешних подключений порт SSH, но в то же время открывать его только для тех, кто знает необходимую последовательность.

Вы можете подробнее ознакомиться с возможностью подключения клиентов к серверу **Port Knocking**, просмотрев наши обучающие видео:

- на **RuTube** — Механизм защиты сервера Port Knocking;
- в **Яндекс.Дзен** — Механизм защиты сервера Port Knocking;
- в **VK Видео** — Механизм защиты сервера Port Knocking.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка сервера

Подробную информацию о настройке и защите сервера с помощью механизма **Port Knocking** см. в нашей статье «Механизм защиты сервера Port Knocking».

Настройка клиента

Установка knock

Для установки **knock** на клиенте перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install knock
```

Подключение к серверу

Для выполнения подключения к серверу посредством **knock** используется команда следующего вида:

```
knock <IP_адрес_сервера> <порты>
```

Например:

```
knock 192.168.1.153 7000:tcp 9000:udp 8000:tcp
```

Обратите внимание на формат описания номеров и типов портов. Он должен быть абсолютно таким же, как и в конфигурационном файле **/etc/knockd.conf** на сервере.

Настройка FTP-сервера

Установка и настройка сервера
Монтирование ftp-ресурса в качестве директории РЕД ОС
Ручной вариант монтирования
Автоматический вариант монтирования при помощи autofs

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** ftp-0.17-69, vsftpd-3.0.5-1

Вы можете подробнее ознакомиться с информацией по установке и настройке ftp-сервера, просмотрев наши обучающие видео:

- на **RuTube** — FTP-сервер на РЕД ОС;
- в **Яндекс.Дзен** — FTP-сервер на РЕД ОС;
- в **VK Видео** — FTP-сервер на РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и настройка сервера

Для установки через терминал перейдите в сеанс пользователя **root** с помощью команды:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Для установки выполните команду:

```
dnf install vsftpd
dnf install ftp
```

Запуск сервера и включения демона **vsftpd** в автозагрузку :

```
systemctl start vsftpd
systemctl enable vsftpd
```

Конфигурационным файлом для настройки **vsFTPd** является файл **vsftpd.conf**, который обычно находится по пути **/etc/vsftpd/vsftpd.conf**.

На всякий случай полезно перед редактированием оригинального файла настроек сделать его резервную копию:

```
cp /etc/vsftpd/vsftpd.conf vsftpd.conf.backup
```

FTP-сервер **vsFTPd** предусматривает два основных варианта работы: с анонимными и авторизованными пользователями.

Чтобы включить анонимный доступ по FTP, нужно в файле **/etc/vsftpd/vsftpd.conf** определить значение «**YES**» для соответствующей директивы:

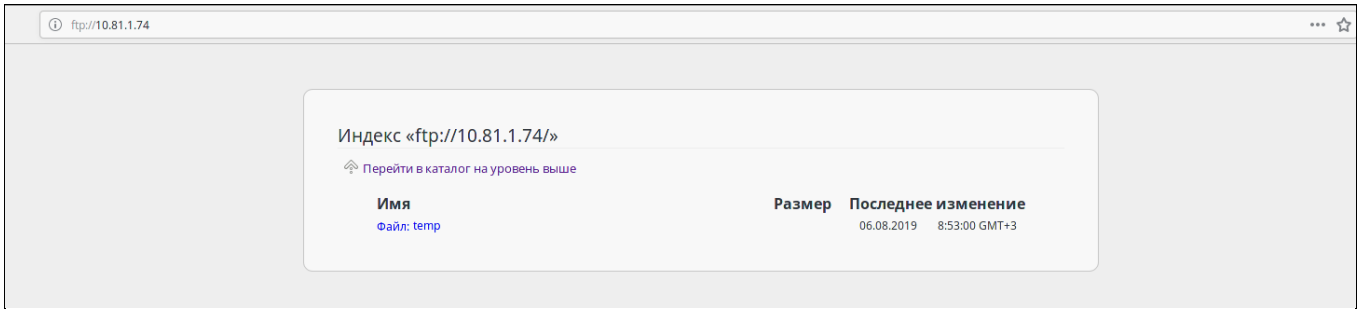
```
anonymous_enable=YES
```

Теперь для управления файлами будет использоваться определённый каталог (обычно **/var/ftp/pub**) и определённый пользователь — обычно **ftp**.

Можно определить и другое расположение файлов для анонимного доступа по FTP, т. е. изменить домашнюю директорию пользователя **ftp**:

```
mkdir -p /srv/share/ftp
usermod -d /srv/share/ftp ftp
```

Пример доступа к папке



Для авторизованного доступа проще всего включить использование локальных учётных записей на сервере. Для этого нужно привести строку в файле конфигурации **vsftpd.conf** к виду:

```
local_enable=YES
```

> **Примечание.**
>
> Для авторизации локальных пользователей используется пароль пользователя для локального входа в систему.

Чтобы ограничить передвижение авторизованного пользователя в рамках одной папки, используется следующий алгоритм:

1. В конфигурационный файл **vsftpd.conf** добавьте строку:

```
user_config_dir=/etc/vsftpd_user_conf
```

2. Создайте папку, в которой будет храниться правило для пользователя:

```
mkdir /etc/vsftpd_user_conf
```

3. Создайте файл, имя которого равно имени пользователя, которому требуется разрешить доступ к папке:

```
nano /etc/vsftpd_user_conf/<ИМЯ_ПОЛЬЗОВАТЕЛЯ>
```

4. Добавьте строку:

```
local_root=/serv/ftp/
```

5. Для добавления доступа другому пользователю к папке создайте новый файл **/etc/vsftpd_user_conf/<ИМЯ_ПОЛЬЗОВАТЕЛЯ>** с аналогичным содержимым.

6. Кроме этого, для ограничения перемещения по дереву каталогов вне домашней директории, в конфигурационном файле /etc/vsftpd/vsftpd.conf раскомментируйте параметр chroot_local_user:

```
# запретить выходить из домашнего каталога на верхний уровень
chroot_local_user=YES
```

а ниже добавьте параметр для разрешения пользователю права записи в домашний каталог:

```
allow_writeable_chroot=YES
```

7. Далее перезапустите **vsftpd** для активации внесенных изменений:

```
systemctl restart vsftpd
```

Монтирование ftp-ресурса в качестве директории РЕД ОС

Ручной вариант монтирования

Осуществляется при помощи утилиты **curlftpfs**. Данная утилита позволяет монтировать ftp-ресурсы в качестве локальных папок на ПК.

Установите пакеты:

```
dnf install curlftpfs autofs
```

Выполните запуск сервиса **autofs**:

```
systemctl enable autofs --now
systemctl restart vsftpd
```

Пример монтирования представлен в следующих командах:

Общий синтаксис:

```
curlftpfs ftp://SERVER /<ТОЧКА_МОНТИРОВАНИЯ>
```

1) Анонимное монтирование:

```
curlftpfs ftp://10.81.1.74 /serv/ftp
```

Если требуется разрешить доступ для всех, то добавляется параметр:

```
-o allow_other
```

2) Авторизованное монтирование:

```
curlftpfs ftp://10.81.1.74 /serv/ftp -o user=username:password
```

Если требуется разрешить доступ для всех, то к `-o user=username:password` добавляется через запятую:

```
-o user=username:password,allow_other
```

Автоматический вариант монтирования при помощи autofs

Данная утилита использует для конфигурирования шаблоны, расположенные в **/etc/**. Основной шаблон называется **auto.master**, он может указывать на один или несколько других шаблонов для конкретных типов. В данном случае будет рассмотрено монтирование **ftp**.

Создайте файл:

```
nano /etc/auto.ftp
```

Содержимое (авторизованный вариант):

```
10.81.1.74 -fstype=fuse,allow_other    :curlftpfs\#username:password@10.81.1.74
```

Содержимое (анонимный вариант):

```
10.81.1.74 -fstype=fuse,allow_other    :curlftpfs\#10.81.1.74
```

В файл **/etc/auto.master** добавьте строку:

```
/serv/ftp /etc/auto.ftp --ghost,--timeout=30
```

Настройка ProFTPD

Установка и настройка proftpd
Создание отдельных пользователей для авторизации на FTP-сервере
Настройка анонимного пользователя
Создание виртуальных пользователей
Настройка прав доступа
Настройка ProFTPd с использованием TLS

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: proftpd-1.3.6e-1

ProFTPD — это FTP-сервер, который позволяет использовать виртуальных пользователей с сопоставимыми с UID идентификаторами системных пользователей, а также настраивать анонимный доступ, ограничивать права доступа и работать через протокол FTP с поддержкой TLS для безопасной передачи данных. Преимущества ProFTPD также включают гибкость настройки, возможность установки квот на дисковое пространство, ограничение скорости передачи данных, управление правами доступа.

Установка и настройка proftpd

Для установки **proftpd** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install proftpd proftpd-utils
```

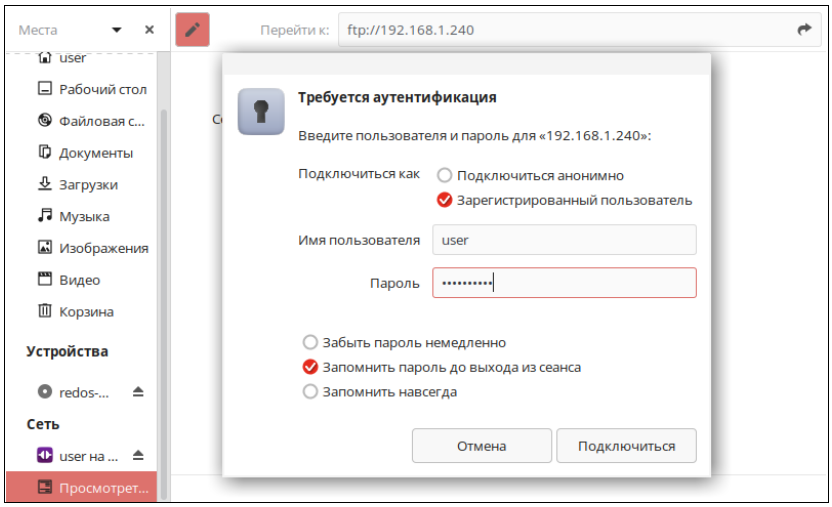
Запустите сервис **proftpd** и добавьте его в автозагрузку:

```
systemctl enable proftpd --now
```

Для проверки статуса сервиса **proftpd** выполните команду:

```
systemctl status proftpd

● proftpd.service - ProFTPD FTP Server
     Loaded: loaded (/usr/lib/systemd/system/proftpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Mon 2023-02-20 10:21:26 MSK; 36s ago
    Process: 1924238 ExecStartPre=/usr/sbin/proftpd --configtest (code=exited, status=0/SUCCESS)
   Main PID: 1924243 (proftpd)
      Tasks: 1 (limit: 2329)
     Memory: 38.5M
        CPU: 95ms
     CGroup: /system.slice/proftpd.service
             └─1924243 proftpd: (accepting connections)

фев 20 10:21:24 localhost.localdomain systemd[1]: Starting ProFTPD FTP Server...
фев 20 10:21:24 localhost.localdomain proftpd[1924238]: Checking syntax of configuration file
фев 20 10:21:25 localhost.localdomain proftpd[1924238]: daemon[1924238]: processing configuration directory '/etc/proftpd/conf.d'
фев 20 10:21:26 localhost.localdomain systemd[1]: Started ProFTPD FTP Server.
```

После запуска службы **proftpd** FTP-сервер сразу готов предоставлять доступ с аутентификацией от имен существующих локальных пользователей данного сервера. При этом предоставляется полный доступ к домашней директории пользователя. Произвести подключение можно с помощью *файлового менеджера* или ftp-клиента **FileZilla**.



Создание отдельных пользователей для авторизации на FTP-сервере

Добавьте группу **ftpgroup** и пользователя **ftpuser**:

```
groupadd ftpgroup
useradd ftpuser -d /home/ftpuser -s /bin/false -g ftpgroup
```

Здесь:

- **ftpuser** – имя пользователя;
- **-d /home/ftpuser** – домашний каталог для пользователя ftpuser;
- **-s /bin/false** – ключ указывает, что пользователю будет отключен shell в целях безопасности;
- **ftpgroup** – группа пользователя.

Назначьте пароль для пользователя **ftpuser** командой:

```
passwd ftpuser
```

Выполните команду, которая добавит в **/etc/shells** запись **/bin/false** в качестве недействительной оболочки (shell). Это предотвратит непосредственный вход в систему пользователя **ftpusers**, но для входа по **ftp** этого будет достаточно:

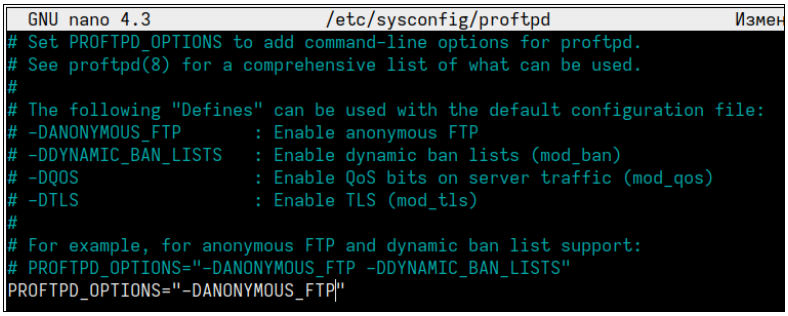
```
echo '/bin/false' >> /etc/shells
```

Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

Настройка анонимного пользователя

Для активации анонимного доступа добавьте параметр `PROFTPD_OPTIONS="-DANONYMOUS_FTP"` в файл **/etc/sysconfig/proftpd**.



Сервер **proftpd** сопоставляет анонимных клиентов (**anonymous**) с пользователем **FTP**. Пользователь с логином **FTP** имеет оболочку **/sbin/nologin**, которая на самом деле не является оболочкой (**shell**), и такому пользователю будет запрещено запускать сеанс командой строки. Однако его можно использовать в качестве пользователя на FTP-сервере.

Добавьте ложную оболочку **/sbin/nologin** в файл списка оболочек **/etc/shells**.

```
echo '/sbin/nologin' >> /etc/shells
```

Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

При подключении анонимному пользователю доступны два каталога — **pub** и **uploads**, которые находятся в корневой директории FTP-сервера **/var/ftp/**.

Директория **/pub** – общедоступный каталог FTP, который имеет права только на чтение.

Директория **/uploads** – имеет права на запись, но при этом просматривать содержимое директории запрещено.

Создание виртуальных пользователей

В качестве примера настроим доступ к FTP-серверу с возможностью авторизации под *виртуальным* пользователем. Хранить виртуальных пользователей можно в файле или базе данных.

Создайте домашний каталог для пользователя, при подключении виртуальным пользователем будет открываться именно эта директория, например:

```
mkdir /home/vftp1
```

После этого создайте файл с паролями и виртуальными пользователями, которые сопоставляются с локальными учетными записями по их **UID** и **GID**:

```
ftpasswd --passwd --file=/etc/proftpd/ftpd.passwd --name=vftp1 --uid=48 --gid=48 --home=/home/vftp1 --shell=/sbin/nologin
```

Здесь:

- **/etc/proftpd/ftpd.passwd** — полный путь до файла, в котором хранятся пользователи;
- **vftp1** — имя пользователя (логин);
- **uid** и **gid** — идентификаторы пользователя и группы системной учетной записи, от которой будет выступать сервер;
- **/home/vftp1** — домашний каталог пользователя;
- **/sbin/nologin** — оболочка, запрещающая локальный вход пользователя в систему.

Откройте файл конфигурации **/etc/proftpd.conf** и закомментируйте строку, которая начинается на «**AuthOrder**».

```
# Cause every FTP user except adm to be chrooted into their home direct
DefaultRoot                     ~ !adm

# Use pam to authenticate (default) and be authoritative
AuthPAMConfig                   proftpd
#AuthOrder                      mod_auth_pam.c* mod_auth_unix.c
# If you use NIS/YP/LDAP you may need to disable PersistentPasswd
#PersistentPasswd               off
```

Создайте дополнительный конфигурационный файл в каталоге **/etc/proftpd/conf.d** (в нем находятся пользовательские конфигурационные файлы) и добавьте следующие строки:

```
nano /etc/proftpd/conf.d/virtual.conf
```

```
AuthUserFile /etc/proftpd/ftpd.passwd
AuthOrder mod_auth_file.c
```

Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

Теперь можно подключится к FTP-серверу от имени виртуального пользователя **vftp1**.

Настройка прав доступа

Разберем пример, когда к одной и той же папке необходимо будет предоставить разные права — одному пользователю *только на чтение*, другому — *на чтение и запись*.

Производим изменения в конфигурационном файле **/etc/proftpd/conf.d/rights.conf**, добавив следующее содержимое:

```
<Directory /var/www>
  <Limit WRITE>
    Order deny,allow
    AllowUser vuser1
  </Limit>
  <Limit ALL>
    AllowAll
  </Limit>
 </Directory>
```

где:

- **<Directory /var/www>** — задаются права для директории /var/www;
- **AllowUser vuser1** — разрешение для **vuser1** только права на чтение, для других пользователей запись и чтение файлов доступны.

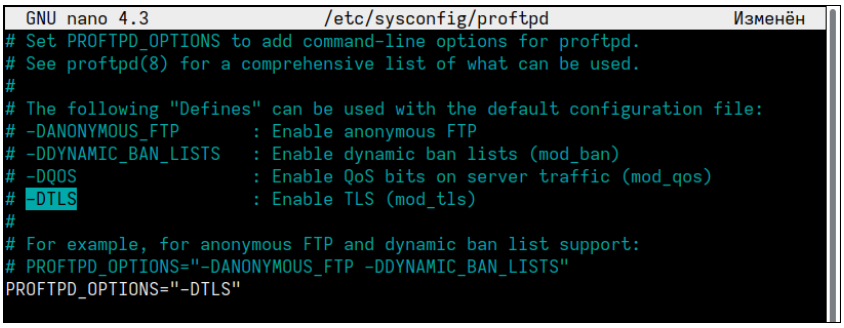
Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

Настройка ProFTPd с использованием TLS

Протокол TLS — криптографический протокол, который обеспечивает защищённый обмен данными между сервером и клиентом.

В файле **/etc/sysconfig/proftpd** задайте значение для опции `PROFTPD_OPTIONS: "-DTLS"`.



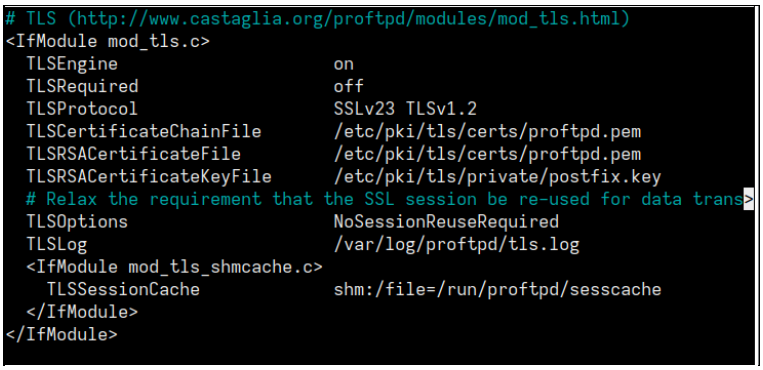
Создайте сертификат с помощью команды:

```
openssl req -x509 -days 1461 -nodes -newkey rsa:2048 -sha256 -keyout /etc/pki/tls/private/postfix.key -out /etc/pki/tls/certs/proftpd.pem -subj "/C=RU/ST=MSK/L=Murom/O=REDos Security/OU=IT Department/CN=192.168.1.240/CN=ftp"
```

Затем в файле **/etc/proftpd/mod_tls.conf** необходимо определить дополнительные опции и пути к сертификату, которые были указаны в генерации сертификата:

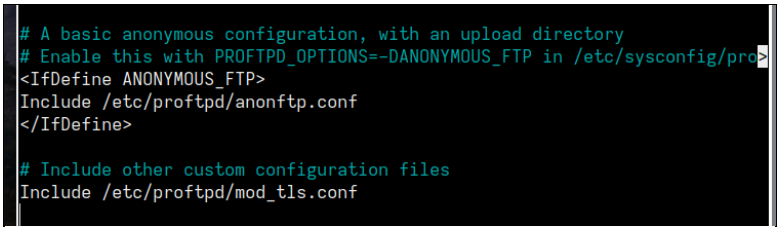
```
TLSEngine on
TLSRequired off
TLSProtocol SSLv23 TLSv1.2
TLSCertificateChainFile /etc/pki/tls/certs/proftpd.pem
TLSRSACertificateFile /etc/pki/tls/certs/proftpd.pem
TLSRSACertificateKeyFile /etc/pki/tls/private/postfix.key
```

В итоге файл **/etc/proftpd/mod_tls.conf** должен выглядеть следующим образом:



```
# TLS (http://www.castaglia.org/proftpd/modules/mod_tls.html)
<IfModule mod_tls.c>
  TLSEngine                     on
  TLSRequired                   off
  TLSProtocol                   SSLv23 TLSv1.2
  TLSCertificateChainFile       /etc/pki/tls/certs/proftpd.pem
  TLSRSACertificateFile         /etc/pki/tls/certs/proftpd.pem
  TLSRSACertificateKeyFile      /etc/pki/tls/private/postfix.key
  # Relax the requirement that the SSL session be re-used for data trans>
  TLSOptions                    NoSessionReuseRequired
  TLSLog                        /var/log/proftpd/tls.log
  <IfModule mod_tls_shmcache.c>
    TLSSessionCache             shm:/file=/run/proftpd/sesscache
  </IfModule>
</IfModule>
```

В файле конфигурации **/etc/proftpd.conf** необходимо прописать строку `Include /etc/proftpd/mod_tls.conf`, для того чтобы FTP-сервер использовал конкретные настройки конфигурации.



```
# A basic anonymous configuration, with an upload directory
# Enable this with PROFTPD_OPTIONS=-DANONYMOUS_FTP in /etc/sysconfig/pro>
<IfDefine ANONYMOUS_FTP>
Include /etc/proftpd/anonftp.conf
</IfDefine>

# Include other custom configuration files
Include /etc/proftpd/mod_tls.conf
```

Перезапустите службу **proftpd** для применения изменений:

```
systemctl restart proftpd
```

Настройка NFS

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** nfs-utils-2.5.2-0, nfs4-acl-tools-0.3.5-2

Если нет пакета **NFS**, его необходимо установить:

```
dnf install nfs-utils nfs4-acl-tools
```

Все настройки сервера хранятся в файле **/etc/exports**. Открываем его на редактирование

```
nano /etc/exports
```

и добавляем в конец файла строки вида (строк может быть произвольное количество):

```
/data 192.168.1.1/255.255.255.0(rw,insecure,nohide,all_squash,anonuid=1000,anongid=1000,no_subtree_check)
```

- **/data** –путь к папке, для которой раздается доступ;
- **192.168.1.1** –IP-адрес, которому раздается доступ к папке (можно указать всю сеть, тогда запись примет вид 192.168.1.0/24)
- **(rw,no_root_squash,sync)** –набор опций, опции могут быть:
  - **rw** –чтение запись(может принимать значение ro-только чтение);
  - **no_root_squash** – по умолчанию пользователь root на клиентской машине не будет иметь доступа к разделяемой директории сервера. Этой опцией мы снимаем это ограничение. В целях безопасности этого лучше не делать;
  - **nohide** - NFS автоматически не показывает нелокальные ресурсы (например, примонтированые с помощью mount –bind), эта опция включает отображение таких ресурсов;
  - **sync** – синхронный режим доступа(может принимать обратное значение- async). sync (async) - указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами. Опция async указывает серверу не ждать записи информации на диск, что повышает производительность, но понижает надежность, т.к. в случае обрыва соединения или отказа оборудования возможна потеря данных;
  - **noaccess** – запрещает доступ к указанной директории. Может быть полезной, если перед этим вы задали доступ всем пользователям сети к определенной директории, и теперь хотите ограничить доступ в поддиректории лишь некоторым пользователям.
  - **all_squash** – подразумевает, что все подключения будут выполнятся от анонимного пользователя
  - **subtree_check (no_subtree_check)** - в некоторых случаях приходится экспортировать не весь раздел, а лишь его часть. При этом сервер NFS должен выполнять дополнительную проверку обращений клиентов, чтобы убедиться в том, что они предпринимают попытку доступа лишь к файлам, находящимся в соответствующих подкаталогах. Такой контроль поддерева (subtree checks) несколько замедляет взаимодействие с клиентами, но если отказаться от него, могут возникнуть проблемы с безопасностью системы. Отменить контроль поддерева можно с помощью опции no_subtree_check. Опция subtree_check, включающая такой контроль, предполагается по умолчанию. Контроль поддерева можно не выполнять в том случае, если экспортируемый каталог совпадает с разделом диска;
  - **anonuid=1000** – привязывает анонимного пользователя к «местному» пользователю;
  - **anongid=1000** – привязывает анонимного пользователя к группе «местного» пользователя.

Чтобы запустить демон (службу) и добавить её в автозагрузку, прописываем следующие команды:

```
systemctl enable nfs-server.service --now
```

При положительном результате вы увидите, что демон запустился и функционирует

```
Redirecting to /bin/systemctl status nfs.service
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; vendor preset: disabled)
   Active: active (exited) since Вт 2019-08-06 15:23:21 MSK; 3s ago
  Process: 732 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
  Process: 729 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
Main PID: 732 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/nfs-server.service
```

Впоследствии после внесения изменений в файл **/etc/exports** не обязательно перезапускать сервер, достаточно выполнить:

```
exportfs -ra
```

Настройка iSCSI

Конфигурация хранилища
Конфигурация клиента

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** targetcli-2.1.53-2, iscsi-initiator-utils-6.2.1.0-2

Конфигурация хранилища

Создайте диск LVM на целевом сервере, чтобы использовать его в качестве общего хранилища для клиентов.

Проверьте доступные диски:

```
fdisk -l | grep -i sd

Диск /dev/sda: 200 GiB, 214748364800 байт, 419430400 секторов
/dev/sda1 * 2048 2099199 2097152 1G 83 Linux
/dev/sda2 2099200 419430399 417331200 199G 8e Linux LVM
Диск /dev/sdb: 35 GiB, 37580963840 байт, 73400320 секторов
```

Из приведенного выше примера видно, что в системе доступно 35 ГБ дискового пространства (**dev/sdb**). Создайте раздел нужного объёма. В примере, на указанном выше диске, будет задействовано 5 ГБ для LVM.

```
fdisk /dev/sdb

Добро пожаловать в fdisk (util-linux 2.37.3).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.
Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0xaee65952.
Команда (m для справки): n → Новый раздел
Тип раздела
   p   основной (0 primary, 0 extended, 4 free)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p → Основной раздел
Номер раздела (1-4, default 1): 1 → Номер раздела
Первый сектор (2048-73400319, default 2048):  → Нажмите Enter
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-73400319, default 73400319): +5G → Задайте размер раздела
 Создан новый раздел 1 с типом 'Linux' и размером 5 GiB.
Команда (m для справки): t → Измените метку
Выбранный раздел 1
Шестнадцатеричный код (введите L для получения списка кодов): 8e → Изменить метку на LVM
Тип раздела 'Linux' изменен на 'Linux LVM'.
Команда (m для справки): w → Сохраните
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

Создайте LVM с разделом **/dev/sdb1** (замените **/dev/sdb1** на имя вашего диска):

```
pvcreate /dev/sdb1

Physical volume "/dev/sdb1" successfully created.
```

```
vgcreate vg_iscsi /dev/sdb1

Volume group "vg_iscsi" successfully created
```

```
lvcreate -l 100%FREE -n lv_iscsi vg_iscsi

Logical volume "lv_iscsi" created.
```

Создание таргета iSCSI

Установите пакет **targetcli**:

```
dnf install targetcli
```

Добавьте службу **target** в автозагрузку и запустите:

```
systemctl enable target --now
```

Откройте **targetcli**:

```
targetcli

targetcli shell version 2.1.53
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.
/>
```

Просмотрите структуру, в виде которой представлен таргет, командой:

```
/> ls

  1. o- / ..... [...]
  2.   o- backstores ..... [...]
  3.   | o- block ..... [Storage Objects: 0]
  4.   | o- fileio ..... [Storage Objects: 0]
  5.   | o- pscsi ..... [Storage Objects: 0]
  6.   | o- ramdisk ..... [Storage Objects: 0]
  7.   o- iscsi ..... [Targets: 0]
  8.   o- loopback ..... [Targets: 0]
  9.   o- vhost ..... [Targets: 0]
```

Помощь можно вызывать в любом разделе внутри **targetcli**:

```
help
```

Перейдите в раздел **block**:

```
/> cd backstores/block
```

Создайте блочное устройство, используя ранее созданный логический том:

```
/backstores/block> create scsi_disk1 /dev/vg_iscsi/lv_iscsi

Created block storage object scsi_disk1 using /dev/vg_iscsi/lv_iscsi.
```

Создайте таргет (цель):

```
/backstores/block> cd /iscsi
/iscsi> create

Created target iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
```

Просмотреть структуру таргета можно командой:

```
/iscsi> ls

o- iscsi ..... [Targets: 1]
  o- iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625 ..... [TPGs: 1]
    o- tpg1 ..... [no-gen-acls, no-auth]
      o- acls ..... [ACLs: 0]
```

```
  o- luns ..... [LUNs: 0]
  o- portals ..... [Portals: 1]
    o- 0.0.0.0:3260 ..... [OK]
```

Здесь:

- **iqn** — имя таргета.
- **tpg1** (Target Portal Group) – список IP-адресов и TCP портов, которые будет слушать этот таргет.
- **acls** – список адресов, с которых можно будет подключиться к таргету,
- **luns** – список адресов дискового устройства в сетях хранения,
- **portals** – список IP-адресов и портов, которые будет слушать таргет.

Создайте ACL для клиентской машины. Для этого перейдите на уровень *acls*, используя команду cd и клавиши управления со стрелками «вверх» и «вниз». Затем используйте команду create и имя инициатора, которое находится в файле **/etc/iscsi/initiatorname.iscsi** на клиентской машине:

```
/iscsi/iqn.20...625/tpg1/acls> create iqn.1994-05.com.redhat:70f2a07b2daf

Created Node ACL for iqn.1994-05.com.redhat:70f2a07b2daf
Created mapped LUN 0.
Created mapped LUN 1.
```

Создайте LUN. Он должен использовать раннее созданный объект хранилища. В примере это «**scsi_disk1**». Перейдите на уровень «**luns**», используя команду cd и клавиши управления со стрелками «вверх» и «вниз». После чего используйте команду create:

```
/iscsi/iqn.20...625/tpg1/luns> create /backstores/block/scsi_disk1

Created LUN 0.
Created LUN 0->0 mapping in node ACL iqn.1994-05.com.redhat:70f2a07b2daf
```

Проверьте конфигурацию сервера:

```
/iscsi/iqn.20...625/tpg1/luns> cd /
/> ls

o- / ..... [...]
  o- backstores ..... [...]
  | o- block ..... [Storage Objects: 1]
  | | o- scsi_disk1 ..... [/dev/vg_iscsi/lv_iscsi (5.0GiB) write-thru activated]
  | |   o- alua ..... [ALUA Groups: 1]
  | |     o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
  | o- fileio ..... [Storage Objects: 0]
  | o- pscsi ..... [Storage Objects: 0]
  | o- ramdisk ..... [Storage Objects: 0]
  o- iscsi ..... [Targets: 1]
  | o- iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625 ..... [TPGs: 1]
  |   o- tpg1 ..... [no-gen-acls, no-auth]
  |     o- acls ..... [ACLs: 1]
  |     | o- iqn.1994-05.com.redhat:70f2a07b2daf ..... [Mapped LUNs: 1]
  |     |   o- mapped_lun0 ..... [lun0 block/scsi_disk1 (rw)]
  |     o- luns ..... [LUNs: 1]
  |     | o- lun0 ... [block/scsi_disk1 (/dev/vg_iscsi/lv_iscsi) (default_tg_pt_gp)]
  |     o- portals ..... [Portals: 1]
  |       o- 0.0.0.0:3260 ..... [OK]
  o- loopback ..... [Targets: 0]
  o- vhost ..... [Targets: 0]
```

Сохраните конфигурацию:

```
/> saveconfig

Last 10 configs saved in /etc/target/backup/.
Configuration saved to /etc/target/saveconfig.json
```

```
/> exit

Global pref auto_save_on_exit=true
```

```
Last 10 configs saved in /etc/target/backup/.
Configuration saved to /etc/target/saveconfig.json
```

Перезапустите сервис таргета:

```
systemctl restart target
```

Конфигурация клиента

На клиентской машине с РЕД ОС, к которой планируется подключение хранилища iSCSI, уже установлен клиент **iscsi-initiator-utils**. Если его нет в системе, необходимо установить пакет и добавить его в автозагрузку:

```
dnf install iscsi-initiator-utils
systemctl enable iscsid --now
```

Отредактируйте файл **/etc/iscsi/initiatorname.iscsi**, если хотите изменить имя инициатора:

```
nano /etc/iscsi/initiatorname.iscsi
```

измените имя инициатора:

```
InitiatorName=iqn.1994-05.com.redhat:70f2a07b2daf
```

Найдите сервер (таргет) с помощью команды:

```
iscsiadm -m discovery -t st -p 10.81.81.190

10.81.81.190:3260,1 iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625
```

Перезапустите сервис:

```
systemctl restart iscsid
```

Подключитесь к таргету (серверу):

```
iscsiadm -m node -T iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625 -p 10.81.81.190 -l

Logging in to [iface: default, target: iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625, portal: 10.81.81.190,3260]
Login to [iface: default, target: iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625, portal: 10.81.81.190,3260] successful.
```

Проверить подключение диска можно командой:

```
fdisk -l
```

В выводе должно появиться подключенное iscsi-устройство:

```
    ...   ...   ...
    Диск /dev/sdb: 4,102 GiB, 5364514816 байт, 10477568 секторов
    Disk model: scsi_disk1
    Единицы: секторов по 1 * 512 = 512 байт
    Размер сектора (логический/физический): 512 байт / 512 байт
    Размер I/O (минимальный/оптимальный): 512 байт / 33550336 байт
```

Создайте файловую систему на диске *iscsi*.

```
mkfs.ext4 /dev/sdb

    mke2fs 1.44.6 (5-Mar-2019)
    Creating filesystem with 1309696 4k blocks and 327680 inodes
    Filesystem UUID: 5be3f332-b730-4aae-baaf-6c5e8cda0a57
    Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
```

```
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

Смонтируйте диск в систему:

```
mount /dev/sdb /mnt
```

Проверка осуществляется командой:

```
df -hT

    Файловая система         Тип      Размер Использовано  Дост Использовано% Смонтировано в
    devtmpfs                 devtmpfs   1,9G          0  1,9G          0% /dev
    tmpfs                    tmpfs      2,0G          0  2,0G          0% /dev/shm
    tmpfs                    tmpfs      785M        3,4M  782M          1% /run
    /dev/mapper/ro_redos-root ext4       26G        6,8G   18G         28% /
    /dev/sda1                ext4       976M        159M  750M         18% /boot
    tmpfs                    tmpfs      393M         76K  393M          1% /run/user/42
    tmpfs                    tmpfs      393M        128K  393M          1% /run/user/1000
    tmpfs                    tmpfs      393M         68K  393M          1% /run/user/0
    /dev/sdb                 ext4       4,9G         20M  4,6G          1% /mnt
```

Настройте автоматическое монтирование хранилища. Для этого понадобится **UUID** диска *iscsi*:

```
blkid /dev/sdb

    /dev/sdb: UUID="5be3f332-b730-4aae-baaf-6c5e8cda0a57" TYPE="ext4"
```

Теперь необходимо отредактировать файл **/etc/fstab**:

```
nano /etc/fstab
```

Добавив в него запись вида:

```
UUID=5be3f332-b730-4aae-baaf-6c5e8cda0a57 /mnt ext4 _netdev 0 0
```

Теперь, при перезагрузке инициатора (клиентской машины), диск *iscsi* будет подключаться к системе автоматически.

Установка и настройка веб-сервера nginx

Предварительная настройка
Установка и запуск nginx
Настройка nginx

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: nginx-1:1.25.4-1

Nginx — высокопроизводительный веб-сервер и почтовый прокси-сервер с открытым исходным кодом, обслуживающий большое количество высоконагруженных сайтов по всему миру. **Nginx** завоевал широкую популярность благодаря своей лёгкости, надёжности, масштабируемости и простоте настройки.

Предварительная настройка

Для настройки веб-сервера **nginx** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее настройка будет производиться с правами суперпользователя **root**, если не указано иное.

Внесите DNS-запись с наименованием веб-сервера в файл **/etc/hosts**:

```
echo <IP-адрес> <название_сайта> > /etc/hosts
```

Например:

```
echo 127.0.0.1 testsite.ru > /etc/hosts
```

Установка и запуск nginx

Установите **nginx** с помощью команды:

```
dnf install nginx
```

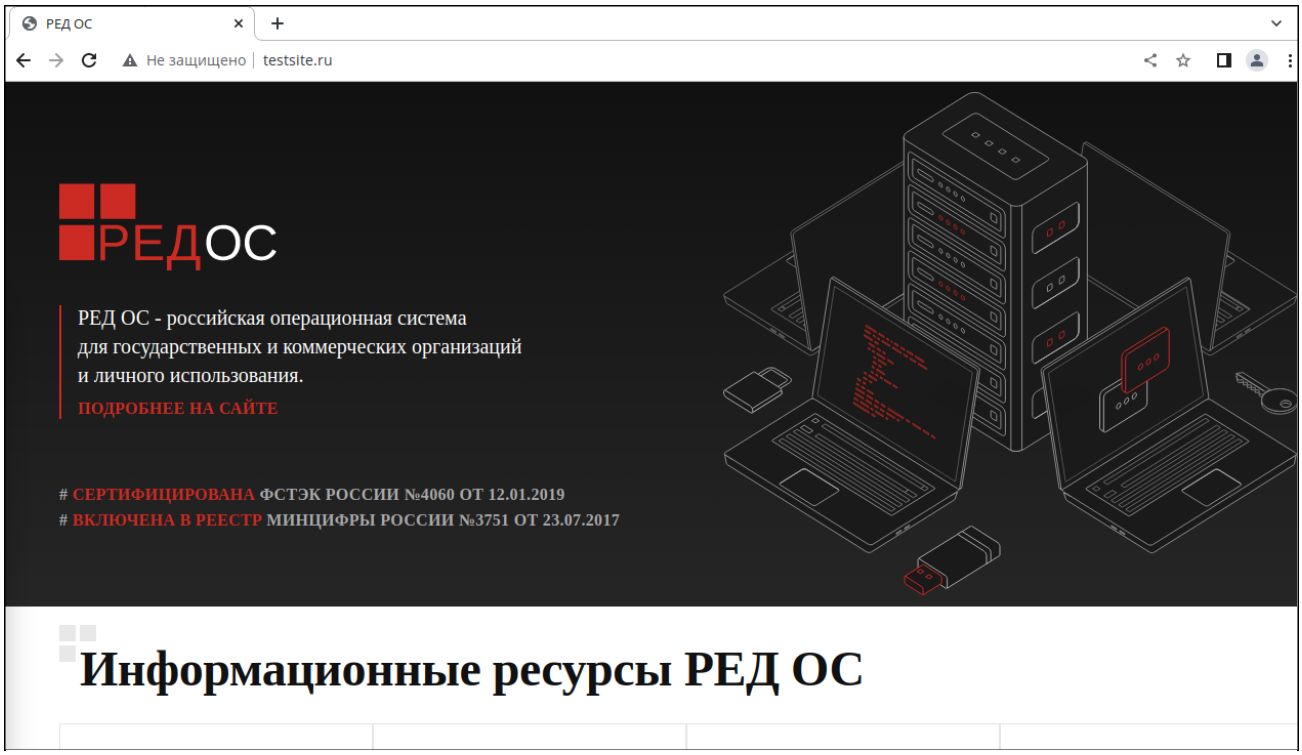
Запустите и добавьте в автозагрузку службу **nginx**:

```
systemctl enable nginx --now
```

Проверьте статус службы **nginx**:

```
systemctl status nginx

 nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
     Active: active (running) since Mon 2024-04-01 13:55:33 MSK; 2s ago
    Process: 637943 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 637950 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 637951 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 637952 (nginx)
      Tasks: 13 (limit: 18964)
     Memory: 11.3M
        CPU: 66ms
     CGroup: /system.slice/nginx.service
```

Для проверки перейдите в браузере по ссылке http://testsite.ru/.



Настройка nginx

Создайте каталог, в котором будут хранится файлы сайта:

```
mkdir -p /var/www/testsite.ru/
```

Создайте файл сайта:

```
nano /var/www/testsite.ru/index.html
```

В файл добавьте следующее содержимое, которое задаст первоначальный вид страницы:

```
<html>
  <head>
   <title>Hello!</title>
  </head>
  <body>
   <h1>Success!</h1>
  </body>
 </html>
```

Создайте каталог **vhosts** в папке **nginx**:

```
mkdir -p /etc/nginx/vhosts/
```

Далее необходимо создать конфигурационный файл, отвечающий за запросы **nginx** к файлам сайта:

```
nano /etc/nginx/vhosts/testsite.conf
```

В файле укажите следующую настройку:

```
server{
  listen 80;
  server_name testsite.ru;
  root /var/www/testsite.ru;
  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;
```

```
    index index.html;
}
```

Затем укажите запуск сервера в **/etc/nginx/nginx.conf**:

```
include /etc/nginx/vhosts/*.conf;
```

ВАЖНО!

Данную строку необходимо указывать **перед** общей настройкой секции server!

```
include /etc/nginx/conf.d/*.conf;
include /etc/nginx/vhosts/*.conf;
server {
    listen       80;
    listen       [::]:80;
    server_name  _;
    root         /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
```

Далее назначьте необходимые права для файлов, указав следующие параметры:

```
chown -R $USER:$USER /var/www/testsite.ru/index.html
chmod -R 755 /var/www/testsite.ru
```

Проверьте конфигурацию **nginx** на наличие ошибок:

```
nginx -t

 nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
 nginx: configuration file /etc/nginx/nginx.conf test is successful
```

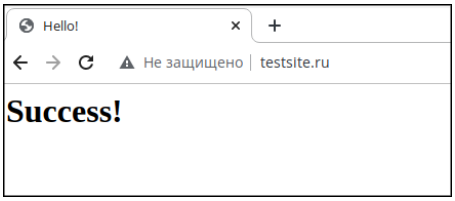
Перезапишите правила **Selinux**:

```
restorecon -Rv /var/www/testsite.ru/
```

Для применения внесенных изменений перезапустите службу **nginx**:

```
systemctl restart nginx
```

Выполните проверку работы в браузере, открыв ссылку http://testsite.ru.



Настройка прокси-сервера nginx для веб-приложений на Node.js

Предварительная настройка
Установка пакетов и запуск служб
Настройка Node.js
Настройка nginx
Настройка автозапуска systemd

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: nginx-1:1.26.2-1, nodejs-1:18.20.4-1

Nginx — высокопроизводительный веб-сервер и почтовый прокси-сервер с открытым исходным кодом, обслуживающий большое количество высоконагруженных сайтов по всему миру. **Nginx** завоевал широкую популярность благодаря своей лёгкости, надёжности, масштабируемости и простоте настройки.

Предварительная настройка

Для настройки веб-сервера **nginx** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее настройка будет производиться с правами суперпользователя **root**, если не указано иное.

Внесите DNS-запись с наименованием веб-сервера в файл **/etc/hosts**:

```
echo <IP-адрес> <название_сайта> > /etc/hosts
```

Например:

```
echo 127.0.0.1 testsite.ru > /etc/hosts
```

Установка пакетов и запуск служб

Установите **nginx** и **node.js** с помощью команды:

```
dnf install nginx nodejs
```

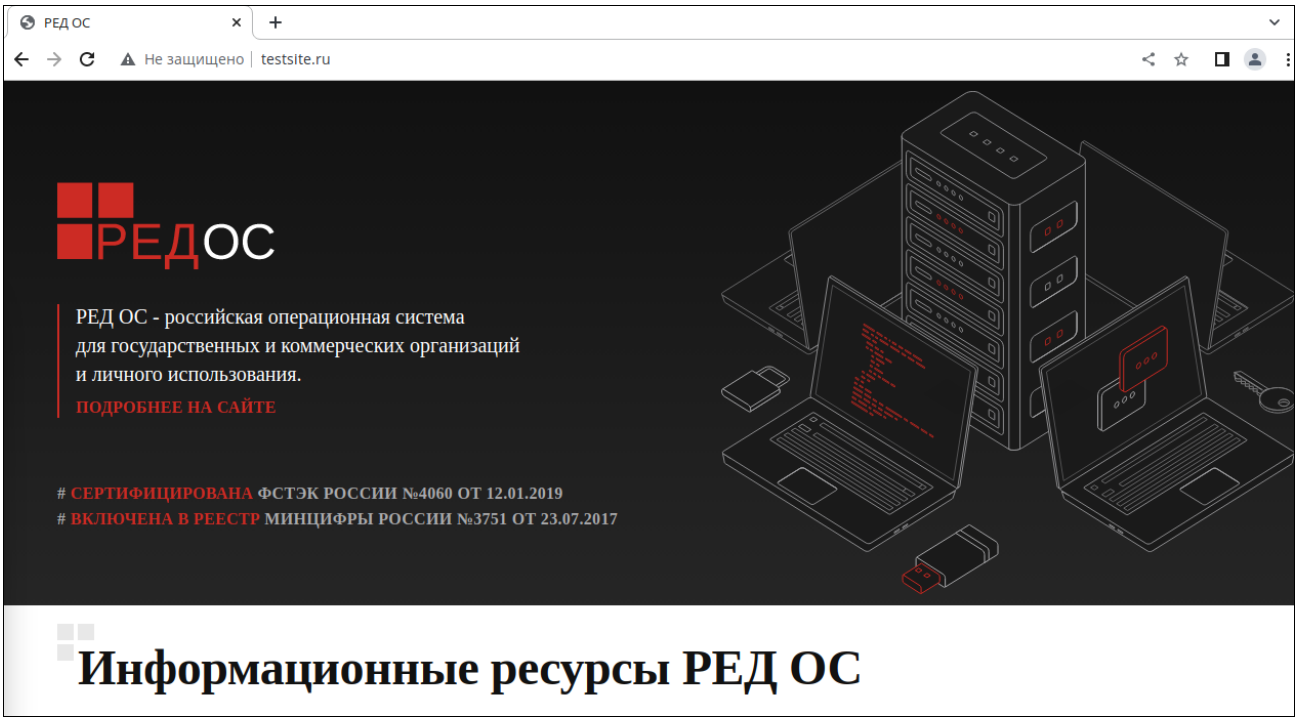
Запустите и добавьте в автозагрузку службу **nginx**:

```
systemctl enable nginx --now
```

Проверьте статус службы **nginx**:

```
systemctl status nginx

 nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
     Active: active (running) since Mon 2024-04-01 13:55:33 MSK; 2s ago
    Process: 637943 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 637950 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 637951 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 637952 (nginx)
      Tasks: 13 (limit: 18964)
     Memory: 11.3M
        CPU: 66ms
     CGroup: /system.slice/nginx.service
```

Для проверки работы в адресной строке браузера введите http://testsite.ru.



Настройка Node.js

Создайте каталог, в котором будут хранится файлы веб-приложения **Node.js**:

```
mkdir -p /var/www/testsite.ru
```

Создайте файл запуска приложения:

```
nano /var/www/testsite.ru/server.js
```

В файл **server.js** добавьте следующее содержимое:

```
const http = require('http');
 const server = http.createServer((req, res) => {

   res.writeHead(200, {
   'Content-Type': 'text/plain; charset=UTF-8'
   });
 res.end('Hello, world!');
});

server.listen(3000, () => {
 console.log('Start NodeJS Server on port 3000');
});
```

Запустите приложение:

```
node /var/www/testsite.ru/server.js
```

Для проверки работы в адресной строке браузера введите http://testsite.ru:3000.



Далее назначьте необходимые права для файлов, указав следующие параметры:

```
chown -R $USER:$USER /var/www/testsite.ru/server.js
chmod -R 755 /var/www/testsite.ru
```

Настройка nginx

Создайте каталог **vhosts** в папке **nginx**:

```
mkdir -p /etc/nginx/vhosts/
```

Далее необходимо создать конфигурационный файл, отвечающий за перенаправление (проксирование) запросв **nginx** к файлам сайта:

```
nano /etc/nginx/vhosts/testsite.conf
```

В файле укажите следующую настройку:

```
server{
      listen 80;
      server_name testsite.ru;
      access_log /var/log/nginx/access.log;
      error_log /var/log/nginx/error.log;
      location / {
      proxy_pass http://127.0.0.1:3000;
      proxy_set_header Host   $host;
     }
 }
```

Затем укажите запуск сервера в **/etc/nginx/nginx.conf**:

```
include /etc/nginx/vhosts/*.conf;
```

ВАЖНО!

Данную строку необходимо указывать **перед** общей настройкой секции server!

```
include /etc/nginx/conf.d/*.conf;
include /etc/nginx/vhosts/*.conf;
server {
    listen       80;
    listen       [::]:80;
    server_name  _;
    root         /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
```

Проверьте конфигурацию **nginx** на наличие ошибок:

```
nginx -tnginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Добавьте правило **SELinux** для разрешения перенаправления запросов (проксирования):

```
setsebool -P httpd_can_network_connect 1
```

Для применения внесенных изменений перезапустите службу **nginx**:

```
systemctl restart nginx
```

Настройка автозапуска systemd

Для настройки автозапуска веб-приложения **Node.js** создайте файл **node@.service**:

```
nano /etc/systemd/system/node@.service
```

В файле укажите следующую настройку:

```
[Unit]
 Description=NodeJS Service
 After=network.target

 [Service]
 Type=simple
 ExecStart=/usr/bin/node ./server.js
 ExecReload=/bin/kill -HUP $MAINPID
 Restart=on-failure
 WorkingDirectory=/var/www/%i

 [Install]
 WantedBy=multi-user.target
```

> **Примечание.**
>
> Обратите внимание, что **%i** — это переменная, которой передается имя настраиваемого веб-приложения. Имя соответствует названию каталога, в котором хранится веб-приложение.

Для применения внесенных изменений перезапустите конфигурацию **systemd**:

```
systemctl daemon-reload
```

Запустите и добавьте в автозагрузку настраиваемое веб-приложение:

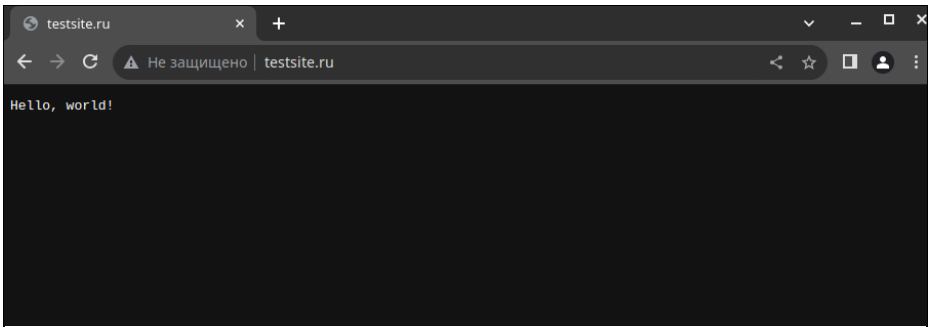
```
systemctl enable node@testsite.ru --now
```

Проверьте статус службы:

```
systemctl status node@testsite.ru
```

В статусе должно отображаться **active (running)**.

Для проверки работы перейдите в браузере по адресу настроенного сайта http://testsite.ru.


testsite.ru
Не защищено | testsite.ru
Hello, world!

Установка и настройка веб-сервера apache

Предварительная настройка
Установка и запуск Apache
Настройка виртуального хоста
Настройка разрешений в SELinux
Управление службой httpd веб-сервера Apache

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: httpd-2.4.58-1

Apache (*Apache HTTP Server*) — это открытое кросс-платформенное программное обеспечение для размещения и поддержки веб-сервера. Основными достоинствами **Apache** считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д.

Предварительная настройка

Для настройки веб-сервера **apache** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее настройка будет производиться с правами суперпользователя **root**, если не указано иное.

Внесите DNS-запись с наименованием веб-сервера в файл **/etc/hosts**:

```
echo <IP-адрес> <название_сайта> >> /etc/hosts
```

Например:

```
echo 192.168.100.185 redsite11.ru >> /etc/hosts
```

Установка и запуск Apache

Установите **Apache** с помощью команды:

```
dnf install httpd -y
```

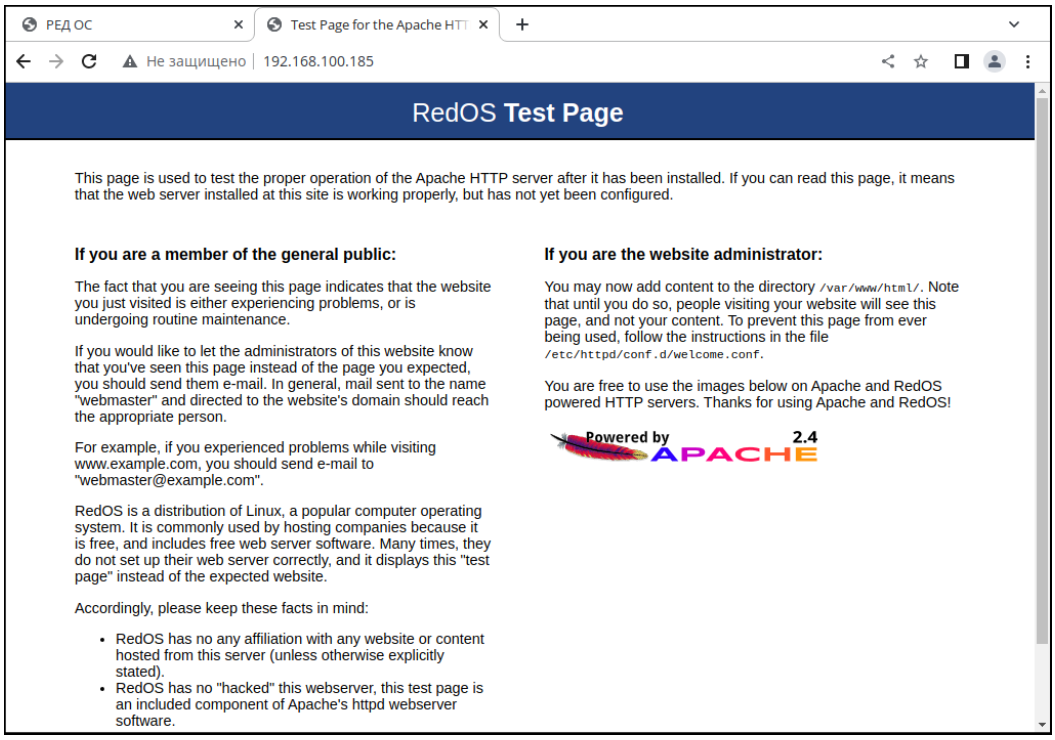
Запустите и добавьте в автозагрузку службу **httpd**:

```
systemctl enable httpd  --now
```

Проверьте статус службы **httpd** командой:

```
systemctl status httpd

tpd.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pre>
    Active: active (running) since Mon 2024-04-01 14:56:43 MSK; 1min 1s ago
      Docs: man:httpd.service(8)
  Main PID: 813 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
     Tasks: 213 (limit: 2310)
    Memory: 21.2M
       CPU: 133ms
```

Для проверки работы веб-сервера откройте браузер и введите в адресной строке `http://<IP-адрес_вашего_сервера>`. Например, `http://192.168.100.185`.

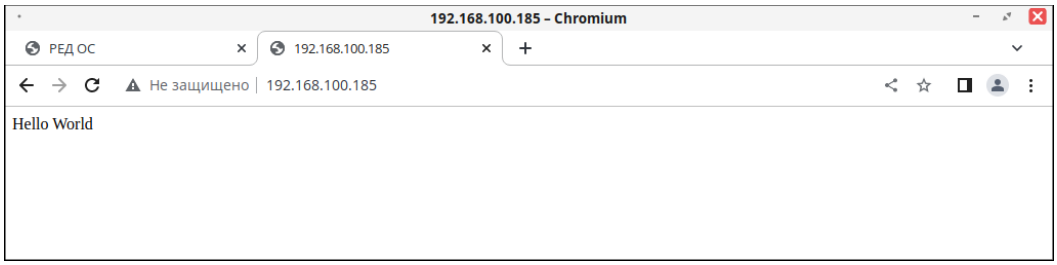


Для проверки корректности установки **Apache** можно создать тестовую страницу с любым содержимым. Для этого выполните:

```
echo "Hello World" > /var/www/html/index.html
```

Команда создаст файл **index.html** и запишет в него содержимое, в данном случае фразу Hello World.

Для просмотра тестовой страницы снова откройте браузер и введите в адресной строке http://<IP-адрес_вашего_сервера>. Например, http://192.168.100.185.



На тестовой странице отображается фраза Hello World, значит, веб-сервер **Apache** работает корректно.

Настройка виртуального хоста

ВАЖНО!

В приведенных примерах необходимо заменить **redsite11.ru** на имя **вашего** реального домена. Только в этом случае файл будет указывать веб-серверу, где найти корневой каталог сайта и куда необходимо сохранять журналы ошибок и обращений к сайту.

Создайте каталог, в котором будут хранится файлы сайта:

```
mkdir -p /var/www/redsite11.ru/html/
```

Назначьте владельца на созданный каталог командой:

```
chown -R $USER. /var/www/redsite11.ru/html/
```

Далее следует убедиться, что на каталог **/var/www/** установлены стандартные права. Для этого выполните команду:

```
chmod -R 755 /var/www/
```

Создайте файл сайта **index.html** в каталоге **/var/www/redsite11.ru/html/**:

```
nano /var/www/redsite11.ru/html/index.html
```

В файл добавьте следующее содержимое, которое задаст первоначальный вид страницы:

```
<html>
  <head>
    <title>Welcome to redsite11.ru!</title>
  </head>
  <body>
    <h1>Success! The redsite11.ru virtual host is working!</h1>
  </body>
</html>
```

Далее создайте два каталога **/sites-available** и **/sites-enabled** в **/etc/httpd**, где будут храниться файлы настроек для каждого отдельно взятого домена. Файлы настроек транслируют домены веб-серверу **Apache**, чтобы веб-сервер понимал, как обрабатывать запросы. Для создания каталогов выполните команду:

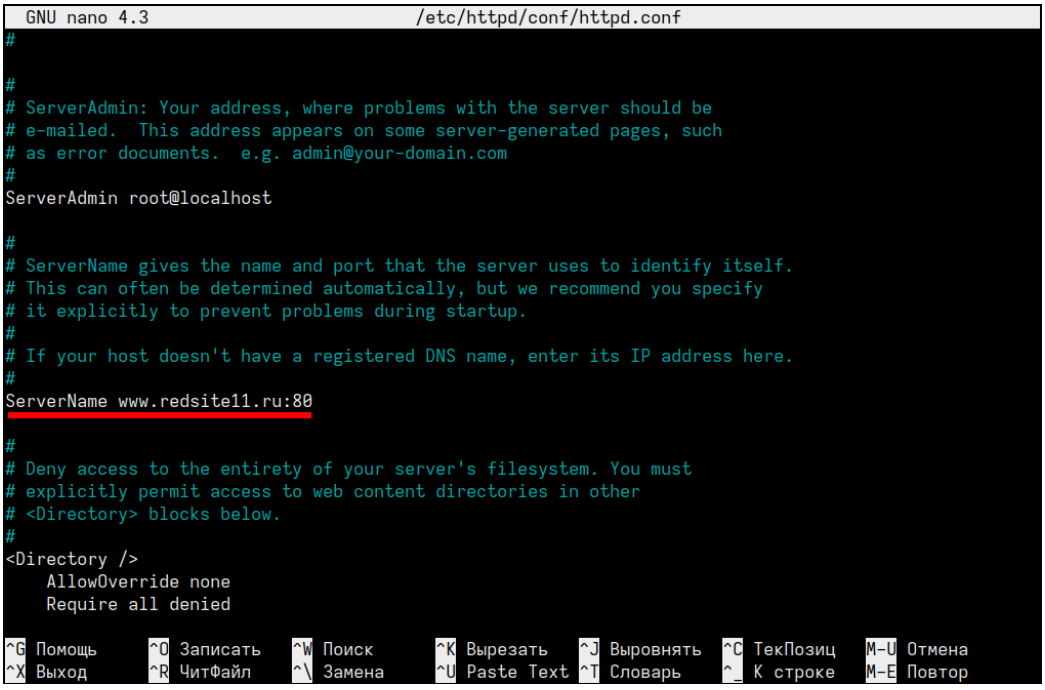
```
mkdir /etc/httpd/sites-available /etc/httpd/sites-enabled
```

Укажите веб-серверу на виртуальный хост в каталоге **/sites-enabled**. Для этого отредактируйте файл **/httpd.conf**:

```
nano /etc/httpd/conf/httpd.conf
```

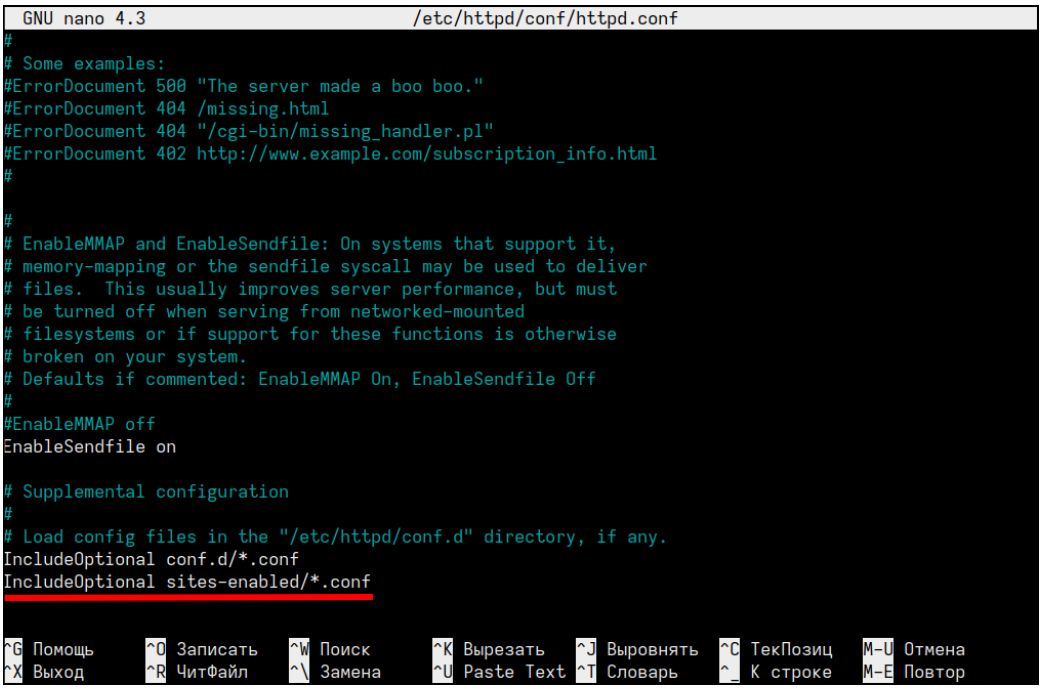
Раскомментируйте строку ServerName и укажите название **своего** сайта:

```
ServerName www.redsite11.ru:80
```



В конец файла добавьте строку:

```
IncludeOptional sites-enabled/*.conf
```



Проверьте настройки **httpd**, выполнив команду:

```
apachectl configtest
```

Если настройки указаны верно, вывод команды должен иметь следующий вид:

```
Syntax OK
```

Далее создайте файл виртуального хоста командой:

```
nano /etc/httpd/sites-available/redsite11.ru.conf
```

Поместите в него содержимое:

```
<VirtualHost *:80>
  ServerName www.redsite11.ru
  ServerAlias redsite11.ru
  DocumentRoot /var/www/redsite11.ru/html
  ErrorLog /var/www/redsite11.ru/log/error.log
  CustomLog /var/www/redsite11.ru/log/requests.log combined
 </VirtualHost>
```

Создайте отдельную папку, где будут храниться файлы журнала:

```
mkdir -p /var/www/redsite11.ru/log
```

Теперь нужно создать символическую ссылку для домена в директории /sites-enabled, чтобы активировать виртуальный хост:

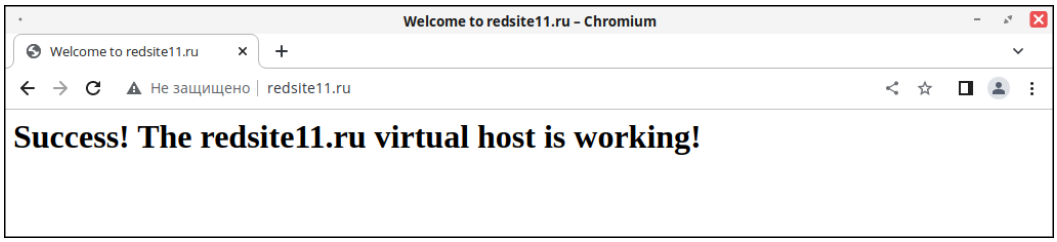
```
ln -s /etc/httpd/sites-available/redsite11.ru.conf /etc/httpd/sites-enabled/redsite11.ru.conf
```

Настройка разрешений в SELinux

Чтобы при старте веб-сервера не получить ошибку запуска, примените универсальную настройку. Для этого выполните команду:

```
setsebool -P httpd_unified 1
```

Для проверки работы перейдите в браузер и в адресной строке введите адрес своего веб-сервера (в примере `http://redsite11.ru`).



Управление службой httpd веб-сервера Apache

Запуск веб-сервера осуществляется командой:

```
systemctl start httpd
```

Остановка веб-сервера осуществляется командой:

```
systemctl stop httpd
```

Перезапуск сервера осуществляется командой:

```
systemctl restart httpd
```

По умолчанию **Apache** запускается автоматически вместе с сервером. Для удаления службы из автозагрузки используется команда:

```
systemctl disable httpd
```

Для добавления **Apache** в автозагрузку, чтобы он стартовал вместе с системой, используется команда:

```
systemctl enable httpd
```

Для перезагрузки веб-сервера **Apache** во время настройки без сброса соединений:

```
systemctl reload httpd
```

Проверка статуса службы **httpd** осуществляется командой:

```
systemctl status httpd
```

Проверка информации об установленной версии **Apache** на сервере осуществляется командой:

```
httpd -v
```

WordPress - инструмент управления сайтами

Настройка Selinux
Установка и настройка веб-сервера Apache
Установка и настройка СУБД MariaDB
Установка и настройка PHP
Установка и настройка WordPress

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: apache-2.4.56-2, mariadb-3:10.11.4-3, php-7.4.33-1, wordpress-6.3

WordPress – это свободный открытый инструмент для управления сайтами и блогами, основанный на PHP и MySQL.

Для корректной работы **WordPress** необходимо установить компилятор **php**, базу данных **MySQL** и веб-сервер **Apache**.

Примечание.

Все команды, используемые в данном разделе, выполняются с правами пользователя **root**, если не указано иное.

Настройка Selinux

Для настройки SELinux выполните:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_graceful_shutdown 1
```

Установка и настройка веб-сервера Apache

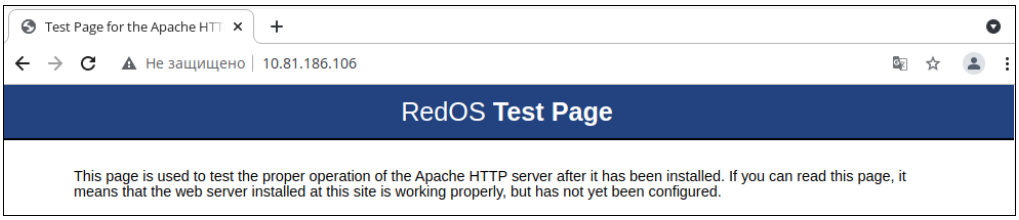
Установите веб-сервер **Apache**:

```
dnf install httpd
```

Запустите службу **apache** и добавьте ее в автозагрузку:

```
systemctl enable httpd --now
```

Для проверки запуска перейдите в браузере по ссылке **http://<IP_сервера>**.



Установка и настройка СУБД MariaDB

Установите СУБД **MariaDB**:

```
dnf install mariadb-server mariadb
```

Запустите службу **mariadb** и добавьте ее в автозагрузку:

```
systemctl enable mariadb --now
```

Создайте пользователя и базу данных с поддержкой русского языка:

```
mysql -u root -p
MariaDB[(none)] > CREATE DATABASE wordpress DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
MariaDB[(none)] > CREATE USER user_wp@localhost IDENTIFIED BY 'password';
```

Определите права для пользователя, который будет использовать базу данных **WordPress**:

```
MariaDB[(none)] > GRANT ALL ON wordpress.* TO 'user_wp'@'localhost';
```

Теперь оповестите **MySQL** о текущих изменениях:

```
MariaDB[(none)] > flush privileges;
```

Выход:

```
quit;
```

Установка и настройка PHP

Установите **php** и дополнительные расширения:

```
dnf install php php-mysqlnd php-pdo php-gd php-mbstring
```

Перезапустите **apache**-сервер:

```
systemctl restart httpd
```

Установка и настройка WordPress

Скачайте установочный архив **WordPress** по ссылке.

Перейдите в каталог, куда была выполнена загрузка, и выполните распаковку архива:

```
cd /home/user/Загрузки/
tar -xvf ./wordpress-6.3.tar.gz
```

Далее распакованные файлы необходимо скопировать в директорию **/var/www/html/**:

```
rsync -av wordpress/* /var/www/html
```

Добавьте отдельную папку для хранения файлов командой:

```
mkdir /var/www/html/wp-content/uploads
```

Предоставьте права пользователю и группе **apache** на каталог с **WordPress**:

```
chown -R apache:apache /var/www/html/*
```

Перейдите в каталог с **WordPress**:

```
cd /var/www/html
```

Главный конфигурационный файл **WordPress** называется **wp-config.php** и содержит все необходимые параметры.

Замените используемый конфигурационный файл по умолчанию на файл **wp-config.php**:

```
cp wp-config-sample.php wp-config.php
```

Внесите в файл информацию о БД:

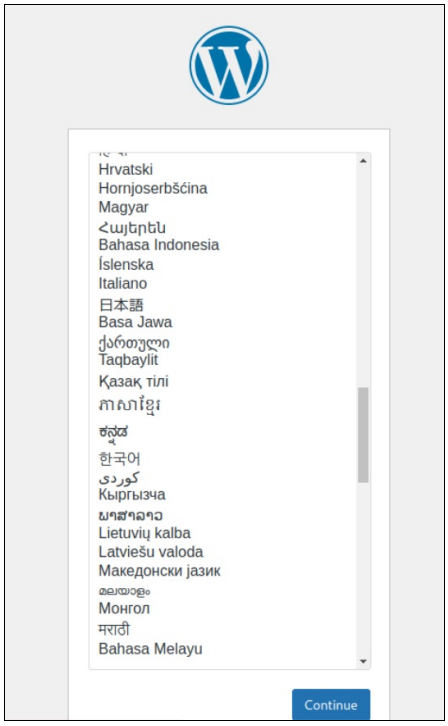
```
nano ./wp-config.php
```

Пример содержимого:

```
// ** Database settings - You can get this info from your web host ** //
 /** The name of the database for WordPress */
 define( 'DB_NAME', 'wordpress' );

 /** Database username */
 define( 'DB_USER', 'user_wp' );

 /** Database password */
 define( 'DB_PASSWORD', 'password' );

 /** Database hostname */
 define( 'DB_HOST', 'localhost' );

 /** Database charset to use in creating database tables. */
 define( 'DB_CHARSET', 'utf8' );

 /** The database collate type. Don't change this if in doubt. */
 define( 'DB_COLLATE', '' );
```

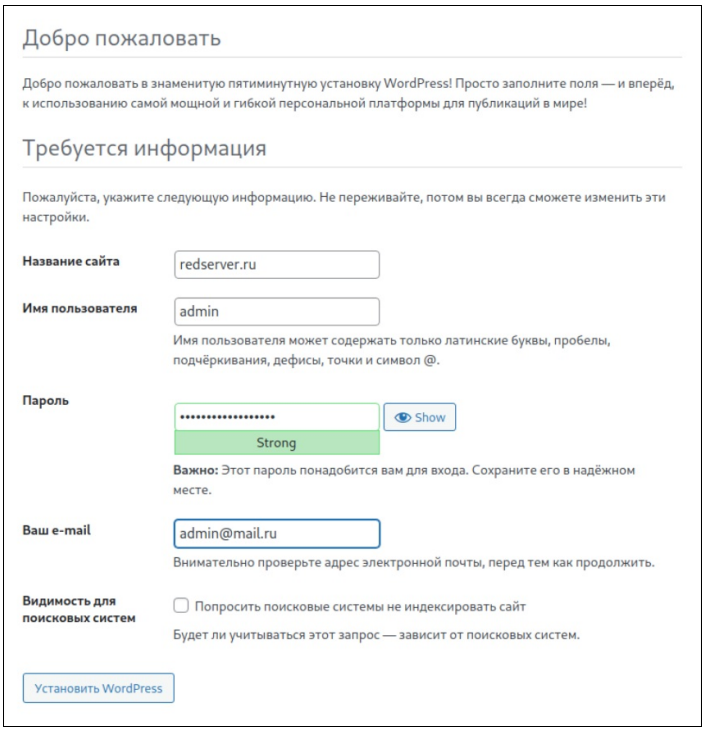
Затем перейдите в браузер по адресу **http://<IP_сервера>** для завершения установки.

WordPress предложит выбрать язык интерфейса, после выбора нажмите **Продолжить**.

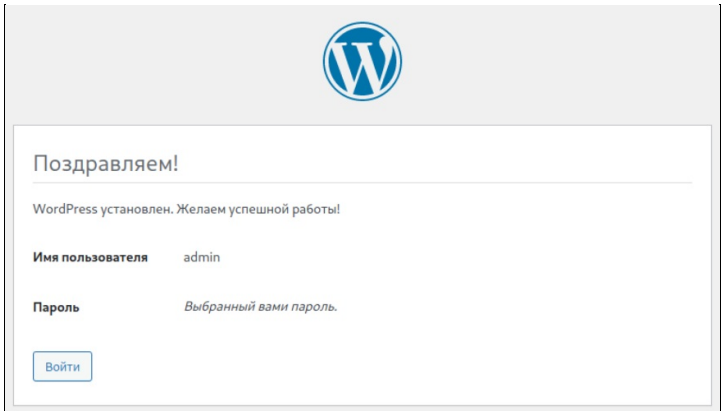


Откроется страница приветствия.

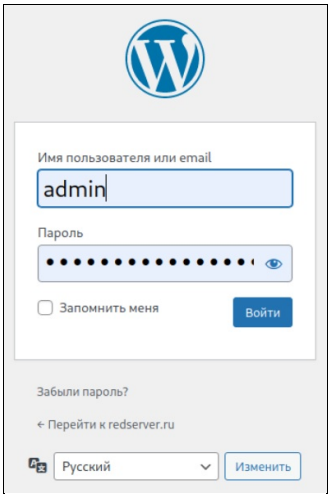
Заполните поля о вашем сайте и администраторе сайта. Например:



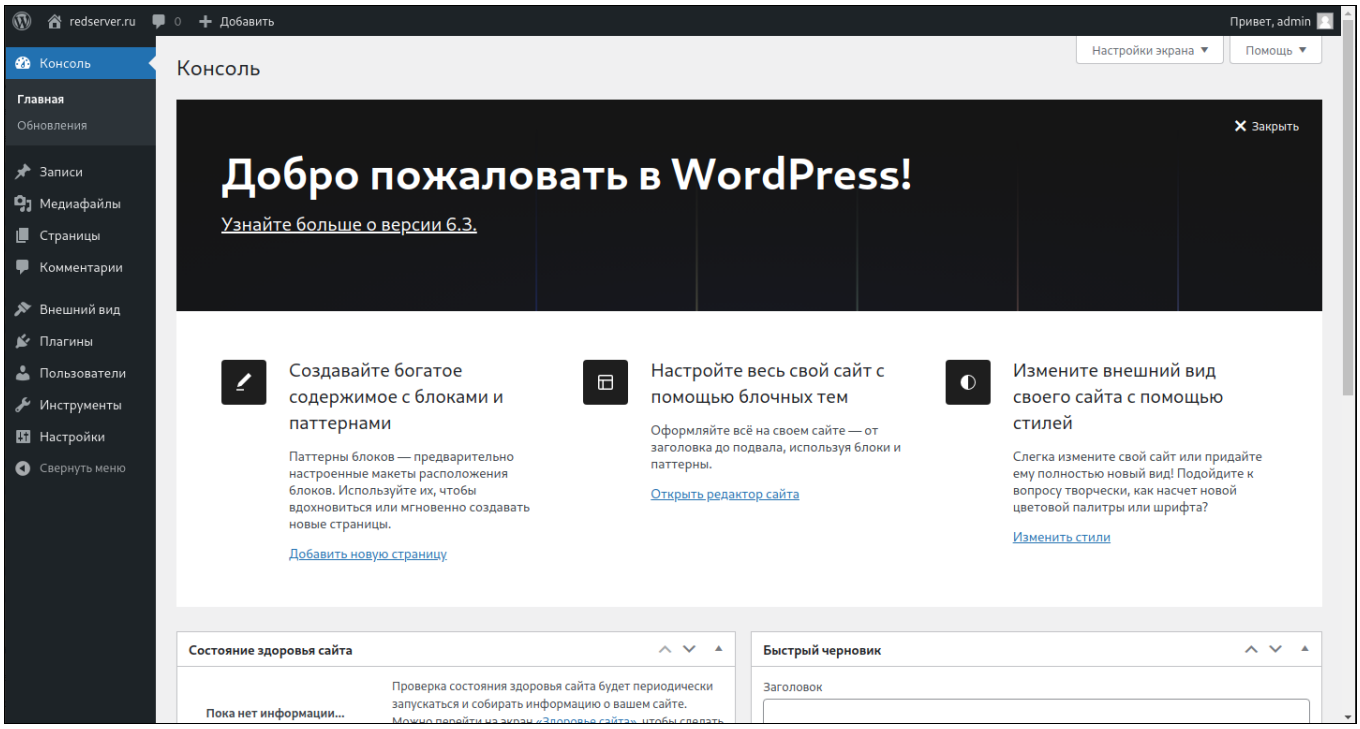
Затем появится окно с уведомлением успешной настройки.



Чтобы продолжить работу с **WordPress** введите *имя пользователя* или *email* и *пароль*.



Система управления контентом **WordPress** готова к использованию.


redserver.ru
0
Добавить
Привет, admin
Консоль
Главная
Обновления
Записи
Медиафайлы
Страницы
Комментарии
Внешний вид
Плагины
Пользователи
Инструменты
Настройки
Свернуть меню
Консоль
Настройки экрана
Помощь
Закрыть
Добро пожаловать в WordPress!
Узнайте больше о версии 6.3.
Создавайте богатое содержимое с блоками и паттернами
Паттерны блоков — предварительно настроенные макеты расположения блоков. Используйте их, чтобы вдохновиться или мгновенно создавать новые страницы.
Добавить новую страницу
Настройте весь свой сайт с помощью блочных тем
Оформляйте всё на своем сайте — от заголовка до подвала, используя блоки и паттерны.
Открыть редактор сайта
Измените внешний вид своего сайта с помощью стилей
Слегка измените свой сайт или придайте ему полностью новый вид! Подойдите к вопросу творчески, как насчет новой цветовой палитры или шрифта?
Изменить стили
Состояние здоровья сайта
Пока нет информации...
Проверка состояния здоровья сайта будет периодически запускаться и собирать информацию о вашем сайте.
Быстрый черновик
Заголовок

Общие сведения о протоколе SSH

Одна из самых распространенных задач, возникающих при работе в сети - удаленный доступ к другим компьютерам и предоставление такого доступа.

Для решения этой задачи используется ставший уже традиционным протокол *SSH* (Secure Shell). В отличие от устаревших протоколов, таких как **telnet** и **rsh/rlogin/rcp**, которые передают данные прямым текстом и подвержены обыкновенному прослушиванию и различным атакам, SSH реализует соединение с удаленным компьютером, защищающее от:

- прослушивания данных, передаваемых по этому соединению;
- манипулирования данными на пути от клиента к серверу;
- подмены клиента либо сервера путем манипулирования IP-адресами, DNS либо маршрутизацией.

В дополнение к отличным характеристикам в области обеспечения безопасного клиент-серверного соединения, SSH обладает следующими возможностями:

- сжатие передаваемых данных;
- туннелирование каналов внутри установленного соединения - в т.ч. соединений с X-сервером;
- широкая распространенность: существуют реализации SSH для самых различных аппаратных платформ и операционных систем.

OpenSSH - это входящая в дистрибутив реализация SSH, которая включает в себя:

- клиентские программы **ssh, scp** и **sftp** (используются для запуска программ на удаленных серверах и копирования файлов по сети);
- серверные программы **sshd, sftp-server** (используются для предоставления доступа по протоколу SSH);
- вспомогательные программы **make-ssh-known-hosts, rescp, ssh-keygen, ssh-add, ssh-agent, ssh-copy-id, ssh-keyscan**. Одна из самых распространенных задач, возникающих при работе в сети, - удаленный доступ к другим компьютерам и предоставление такого доступа.

Служба SSHD

Аутентификация
Вход в систему
SSH-доступ для root
SSHRC
Формат файла authorized keys
Формат файла ssh_known_hosts
Файлы
Предостережения

OpenSSH Daemon - это программа-сервер, обслуживающая запросы программы-клиента **ssh**. Вместе эти программы заменяют **rlogin** и **rsh** и обеспечивают защищённую и зашифрованную связь между двумя непроверенными компьютерами через незащищённую сеть.

sshd - это служба, принимающая запросы на соединения от клиентов. Обычно она запускается при загрузке системы из **/etc/rc**. Для каждого нового соединения создаётся (с помощью вызова *fork*) новый экземпляр службы. Ответвлённый экземпляр обрабатывает обмен ключами, шифрование, аутентификацию, выполнение команд и обмен данными.

Параметры определяются при помощи ключей командной строки или файла конфигурации (по умолчанию - **sshd_config**). Ключи командной строки имеют больший приоритет, чем значения, указанные в файле конфигурации. При получении сигнала отбоя *SIGHUP* перечитывает свой файл конфигурации путём запуска собственной копии с тем же самым именем, с которым был запущен, например, **/usr/sbin/sshd**.

Доступны следующие ключи:

Ключ	Описание ключа
-4	Использовать только адреса IPv4.
-6	Использовать только адреса IPv6.
-b	Определяет число битов в ключе сервера протокола версии 1 (по умолчанию 768).
-D	Не переходить в фоновый режим и не становиться службой. Это упрощает слежение за экземпляром sshd.
-d	Режим отладки. Сервер посылает расширенную отладочную информацию в файл журнала событий системы и не переходит в фоновый режим работы. Также сервер не создаёт дочерних процессов и обрабатывает только одно соединение. Этот параметр предназначен только для отладки работы сервера. Несколько параметров -d, указанных один за другим, повышают уровень отладки. Максимум - это 3.
-e	Направлять вывод в консоль (stderr) вместо механизма журналирования событий системы.
-f	Определяет имя файла конфигурации. По умолчанию - это /etc/ssh/sshd_config; отказывается работать, не имея файла конфигурации.
-g	Определяет период, в течение которого клиент должен себя идентифицировать (по умолчанию - 120 секунд). Если клиент не смог идентифицировать себя в течение этого времени, экземпляр сервера прекращает свою работу. Значение, равное нулю, отменяет ограничение на время ожидания.
-h	Определяет файл, из которого будет считан ключ хоста. Этот параметр должен быть указан, если запущен не от имени суперпользователя (так как обычно стандартные файлы хоста доступны для чтения только суперпользователю). Стандартное расположение файла - /etc/ssh/ssh_host_key для протокола версии 1, и /etc/ssh/ssh_host_rsa_key и /etc/ssh/ssh_host_dsa_key для протокола версии 2. Можно иметь несколько ключей хоста для разных версий протокола и алгоритмов генерации ключей.
-i	Этот ключ позволяет уведомить программу о том, что она запускается службой inetd(8). Обычно не запускается из inetd, так как требуется генерировать ключ сервера до ответа клиенту, а это может отнять десятки секунд. Клиент будет вынужден ожидать слишком долго, если ключ будет повторно генерироваться каждый раз. Однако, при малых размерах ключа (например, 512), использование из inetd может быть оправдано.
-k	Определяет, как часто будет регенерироваться ключ сервера протокола версии 1 (по умолчанию 3600 секунд - один раз в час). Мотивацией для регенерации ключа так часто служит то, что ключ нигде не сохраняется и, по истечении примерно часа, восстановить ключ для прерванных соединений становится невозможно, даже если машина была взломана или захвачена физически. Значение «ноль» означает, что ключ никогда не будет регенерирован.
-o	Позволяет указывать директивы в формате файла конфигурации, например такие, для которых нет соответствующего ключа командной строки. Директивы файла конфигурации описаны в sshd_config(5).
-p	Порт, на котором сервер будет ожидать соединения (по умолчанию - 22). Возможно указание нескольких ключей с разными портами. Если данный ключ указан, параметр Port файла конфигурации игнорируется, однако порты, указанные в ListenAddress имеют больший приоритет, чем указанные в командной строке.
-q	Не заносить в системный журнал регистрации событий никакой информации. В обычном режиме в нём фиксируется подключение, аутентификация и разрыв каждого соединения.
-t	Режим тестирования. Выполняется только проверка соответствия файла конфигурации и готовность ключей. Полезно для проверки состояния службы после обновления, при котором были изменены файлы конфигурации.
-u	Размер поля в структуре utmp, хранящей имя удалённого хоста. Если разрешённое имя хоста превышает указанное значение, то взамен будет использовано десятичное представление IP-адреса через точку. Это позволяет уникально идентифицировать машины со слишком длинными именами. Указание -u0 включает использование в файле utmp IP-адресов во всех случаях. При этом, будет производить DNS-запросы только, если это явно требуется конфигурацией (from=pattern-list) или механизмом аутентификации (либо RhostsRSAAuthentication либо HostbasedAuthentication). Использование DNS также обязательно в случае задания параметрам AllowUsers и DenyUsers значения в формате USER@HOST.

Аутентификация

Служба **OpenSSH** SSH поддерживает версии протокола SSH 1 и 2. Запретить использование одного из протоколов можно, указав в параметре *Protocol* файла **sshd_config**. Протокол 2 поддерживает ключи *RSA и DSA*; протокол 1 поддерживает только ключи *RSA*. Независимо от протокола, каждый подключающийся хост имеет собственный (обычно 2048-битный) идентифицирующий его ключ.

Для протокола версии 1 подтверждение субъекта сервера обеспечивается 768-битным ключом, который генерируется при запуске сервера. Ключ генерируется заново каждый час, при условии его использования, и не хранится на диске. При получении запроса на подключение со стороны клиента служба посылает в ответ свой открытый ключ и свои ключи. Клиент сравнивает ключ хоста *RSA* со своими данными, чтобы убедиться в том, что это тот же сервер. Затем клиент генерирует 256-битное произвольное число, шифрует его при помощи обоих ключей (своего и сервера) и отправляет результат серверу. Это число становится ключом сеанса, и с его помощью выполняется кодирование всей последующих данных, по согласованному методу - *Blowfish* или *3DES* (клиент выбирает метод из предложенных сервером). В настоящее время по умолчанию используется **3DES**.

Для протокола версии 2 подтверждение субъекта сервера обеспечивается по схеме Диффи—Хеллмана, в результате которой также получается общий ключ сеанса. Дальнейший обмен данными шифруется *симметричным кодом, 128-битным AES, Blowfish, 3DES, CAST128, Arcfour, 192-битным AES или 256-битным AES*, который выбирает клиент из предложенных сервером. Кроме того, целостность передаваемых данных обеспечивается кодом подтверждения подлинности сообщения (hmac-sha1 или hmac-md5).

Далее сервер и клиент переходят в режим аутентификации. Клиент пытается аутентифицировать себя по своему хосту, открытому ключу, паролю или с помощью беспарольного механизма («вызов-ответ»).

Независимо от типа аутентификации, служба проверяет доступность соответствующей учётной записи в системе. Так, она может быть заблокирована посредством добавления её в параметр *DenyUsers* или её группы в *DenyGroups*. Механизм общесистемной блокировки учётной записи выполняется разными системами по-разному. Одни системы ведут собственную базу данных учётных записей (AIX), другие вносят соответствующие изменения в поля файла **passwd** («*LK*» - Solaris и UnixWare, «*» - на HP-UX, «Nologin» - Tru64, «*LOCKED*» во FreeBSD и «!!» в GNU/Linux). Для запрета только аутентификации по паролю укажите в файле *passwd* «**NP**» или «***NP***».

После успешной аутентификации себя клиентом связь переходит в режим подготовки сеанса. В этот момент клиент может запросить такие вещи, как выделение псевдо-терминала, перенаправление соединения X11, перенаправление соединения TCP/IP или перенаправление соединения агента аутентификации через защищённый канал.

Наконец, клиент запрашивает оболочку или выполнение команды, после чего стороны входят в режим сеанса. В этом режиме каждая из сторон в любой момент может пересылать данные и эти данные будут переданы оболочке или команде на стороне сервера и на пользовательский терминал соответственно.

По завершении работы пользовательской программы и закрытии всех перенаправленных X11 и других соединений сервер посылает клиенту команду со статусом выхода и сеанс завершается.

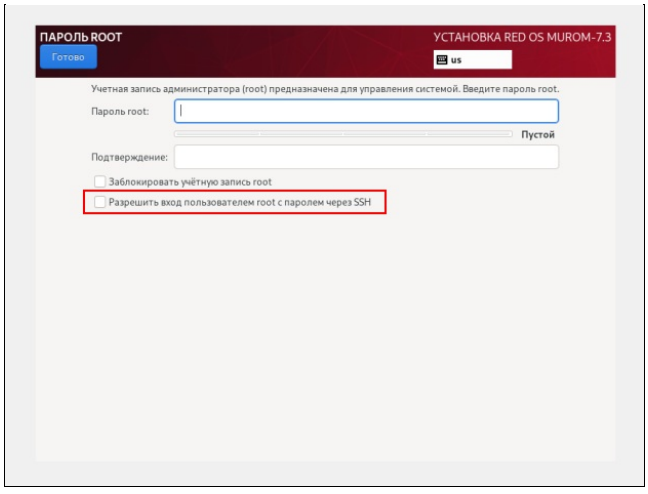
Вход в систему

После успешной аутентификации пользователя выполняются следующие действия:

- Если регистрация в системе произведена на терминале (tty) и не указана никакая команда, то отображается время последнего входа в систему и содержимое файла **/etc/motd** (если только это не отключено в файле конфигурации или **~/.hushlogin**).
- Если регистрация в системе произведена на терминале, записывается время регистрации.
- Проверяется **/etc/nologin**, если он присутствует, выводится его содержимое и завершается работа (исключение - root).
- Осуществляется переход к выполнению с правами обычного пользователя.
- Устанавливаются значения основных переменных среды.
- Интерпретируется файл **~/.ssh/environment**, если таковой имеется, и пользователям разрешено изменять среду.
- Переходит в домашний каталог пользователя.
- Если имеется файл **~/.ssh/rc**, то производится его выполнение, а если нет, но имеется **/etc/ssh/sshrc**, то выполняется он, в противном случае не выполняется ничего. Файлам «rc» на стандартный ввод передаётся протокол аутентификации **X11** и **cookie**.
- Запускается оболочка пользователя или выполняется указанная команда.

SSH-доступ для root

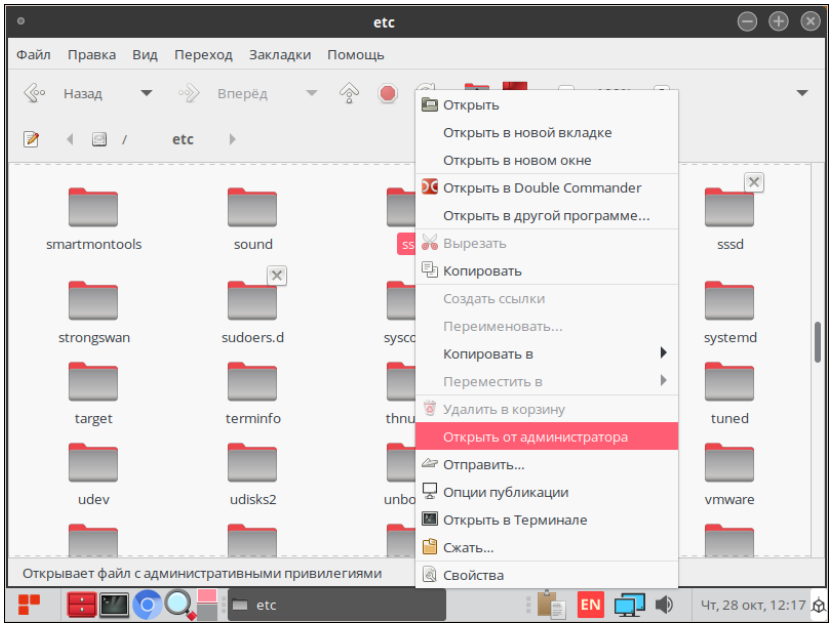
В начале установки операционной системы РЕД ОС предоставляется возможность разрешить вход пользователем root с паролем через ssh.



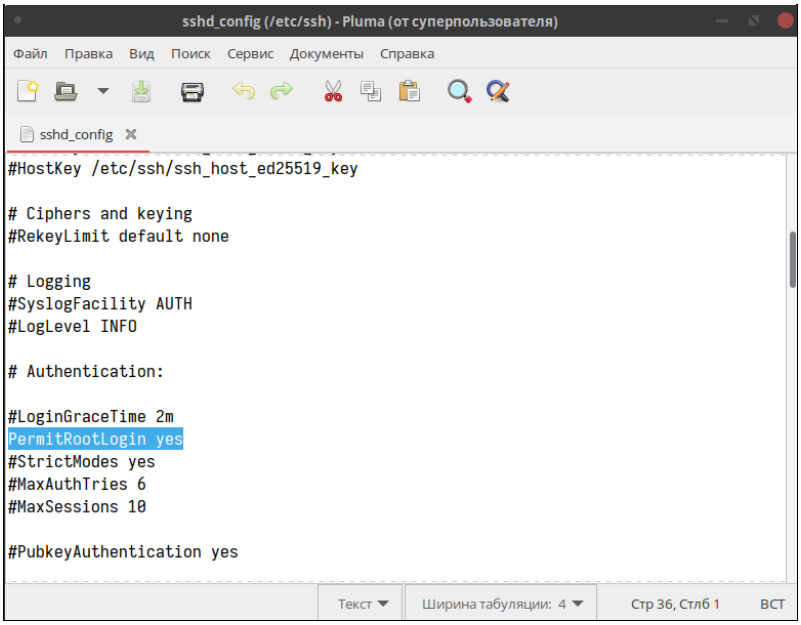
Но даже если не указывать данное разрешение при установке, его можно настроить после завершения установки системы.

Для этого на рабочем столе необходимо открыть меню и перейти в файловую систему (**/**). Затем требуется найти папку **/etc** и перейти в неё.

В папке **/etc** необходимо открыть папку **/ssh** от имени администратора.



Затем нужно найти файл **sshd_config** и отредактировать в нем строку **PermitRootLogin prohibit-password** на **PermitRootLogin yes**.



После редактирования необходимо сохранить внесенные изменения.

Далее следует открыть терминал и перезапустить ssh-сервер (перезапуск сервера необходимо делать после каждого изменения файла конфигурации для последующего применения) командой:

```
systemctl restart sshd
```

Теперь можно подключаться по **SSH** от имени суперпользователя **root**.

SSHRC

Если файл **~/.ssh/rc** существует, он будет выполняться после файлов определения переменных среды, но перед запуском оболочки пользователя или команды. Если используется подмена **X11**, то на его стандартный ввод будет передана пара «**proto cookie**», также ему будет доступна переменная среды **DISPLAY**. Сценарий должен вызывать **xauth(1)** самостоятельно для добавления **cookie X11**.

Основная цель этого файла состоит в выполнении процедур инициализации, необходимые прежде, чем станет доступным основной каталог пользователя. **AFS** - пример такой среды.

Этот файл будет, вероятно, содержать блок аналогичный следующему:

```
if read proto cookie && [ -n "$DISPLAY" ]; then
if [ 'echo $DISPLAY | cut -c1-10' = 'localhost:' ]; then
 X11UseLocalhost=yes
echo add unix:'echo $DISPLAY
| cut -c11-' $proto $cookie
else
 X11UseLocalhost=no
echo add $DISPLAY $proto $cookie
fi | xauth -q -
fi
```

Если этот файл отсутствует, то выполняется **/etc/ssh/sshrc**, а если отсутствует и он, то для добавления **cookie** используется **xauth**.

Формат файла authorized keys

Параметр файла конфигурации **AuthorizedKeysFile** определяет путь к файлу с открытыми ключами. Значение по умолчанию **—/.ssh/authorized_keys**. Каждая строка файла содержит один ключ (пустые строки или строки, начинающиеся с символа «#», считаются комментариями и игнорируются). Открытые ключи протокола 1 (RSA) состоят из следующих полей, разделённых пробелами: параметры, битность, порядок, модуль, комментарий. Открытые ключи протокола версии 2 состоят из: параметра, типа ключа, ключа в виде base64, комментария. Поля параметров необязательны; их отсутствие определяется наличием в начале строки цифры (поле параметра никогда не начинается с цифры). Поля битности, порядка, модуля и комментарии определяют ключ RSA; поле комментария не используется (но может быть удобно пользователю для отметки ключа). Для протокола версии 2 типом ключа является **ssh-dss** или **ssh-rsa**.

Примечание! Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен байт (из-за размера открытого ключа RSA) и могут достигать длины в 8 килобайт (таким образом, максимальный размер ключа DSA - 8 килобит, а RSA - 16 килобит). Очевидно, не стоит вводить их вручную. Вместо этого скопируйте файл **identity.pub, id_dsa.pub** или **id_rsa.pub** и отредактируйте их.

Минимальная длина модуля RSA независимо от протокола составляет 768 бит.

Параметры (если таковые имеются) состоят из разделённых запятой определений. Для указания пробелов следует воспользоваться двойными кавычками. Поддерживаются следующие определения параметров (регистра названий параметров не учитывается):

Параметр	Значение
command=команда	Выполнять команду при каждом использовании данного ключа для аутентификации. Команда, передаваемая пользователем, будет игнорироваться. Команда выполняется на псевдо-терминале, если последний запрашивается клиентом; в противном случае она выполняется без терминала. Если требуется «чистый» 8-битный канал, запрашивать псевдо-терминал или указывать no-pty нельзя. В команду может быть включена кавычка, предварённая обратной косой чертой. Данный параметр полезен для ограничения использования определённых RSA-ключей. Примером может служить ключ, по которому можно выполнять удалённые операции резервного копирования и ничего более. Учтите, что клиент по-прежнему может запросить перенаправление TCP и/или X11, если только это не запрещено явно. Команда, запрашиваемая клиентом, заносится в переменную SSH_ORIGINAL_COMMAND. Заметьте, что данный параметр относится к выполнению оболочки, команды или подсистемы.
environment=ПЕРЕМЕННАЯ=значение	Добавить переменную в среду (или переопределить её значение) при регистрации в системе с использованием данного ключа. Допускается указание нескольких таких директив. По умолчанию изменение переменных среды таким образом отключено. За его включение отвечает параметр PermitUserEnvironment. Этот параметр отключается автоматически при включении UseLogin.
from=список-шаблонов	Если параметр определён, то в дополнение к прохождению аутентификации по открытому ключу каноническое имя удалённого хоста должно соответствовать одному из шаблонов в списке (шаблоны указываются через запятую). Цель этого параметра - увеличение степени защиты: если частный ключ хоста каким-либо образом удастся похитить, то он позволит злоумышленнику войти в систему из любой точки мира. Этот дополнительный параметр делает использование ворованных ключей более затруднительным (кроме перехвата ключа, требуется взлом серверов имён и/или маршрутизаторов). См. секцию ШАБЛОНЫ в ssh_config(5).
no-agent-forwarding	Запретить перенаправление агента аутентификации при аутентификации данным ключом.
no-port-forwarding	Запретить перенаправление TCP/IP при аутентификации данным ключом. Любой запрос на перенаправление порта приведёт к получению клиентом сообщения об ошибке. Это может быть использовано, например, вместе с параметром command.
no-pty	Запретить назначение терминала (запросы на назначение псевдо-терминала не будут удовлетворены).
no-X11-forwarding	Запретить перенаправление X11 при аутентификации данным ключом. Любой запрос на перенаправление порта возвратит клиенту сообщение об ошибке.
permitopen=хост:порт	Для функции перенаправления данных с локального клиентского порта на порт удалённой системы (выполняемого при указании ssh -L). Ограничит набор возможных целей для перенаправления указанной машиной и портом. Для указания адресов IPv6 можно использовать альтернативный синтаксис: хост / порт. Допускается указание нескольких целей через запятую. Значение параметра не интерпретируется как шаблон (т.е. является литеральным).
tunnel=n	Принудительно использовать устройство tun(4) на сервере. Без этого параметра при запросе клиентом туннеля используется ближайшее доступное для этого устройство.

Пример файла **authorized_keys**:

```
# допустимы комментарии только на всю строку
ssh-rsa AAAAB3Nza...LiPk== user@example.net
from="*.sales.example.net,!pc.sales.example.net" ssh-rsa
AAAAB2...19Q== john@example.net
command="dump /home",no-pty,no-port-forwarding ssh-dss
AAAAC3...51R== example.net
permitopen="192.0.2.1:80",permitopen="192.0.2.2:25" ssh-dss
AAAAB5...21S==
tunnel="0",command="sh /etc/netstart tun0" ssh-rsa AAAA...==
jane@example.net
```

Формат файла ssh_known_hosts

В файлах **/etc/ssh/ssh_known_hosts** и **~/.ssh/known_hosts** хранятся открытые ключи всех машин, с которыми когда-либо устанавливалась связь.

Глобальный файл должен быть подготовлен администратором (это необязательно), пользовательский файл поддерживается автоматически: каждый раз, когда поступает запрос на соединение от неизвестной машины, её ключ автоматически заносится в пользовательский файл.

Каждая строка в этом файле содержит следующие поля: имена хостов, битность, порядок, модуль, комментарий. Поля разделены пробелами.

Имена хостов - это разделённый запятыми список шаблонов (символы подстановки - «*****» и «**?**»); каждый шаблон сопоставляется с каноническим именем машины (при аутентификации клиента) или с именем, которое указано пользователем (при аутентификации сервера). Этот шаблон может также быть предварён знаком «**!**» для обозначения отрицания: если имя машины соответствует отрицаемому шаблону, оно будет отвергнуто (этой строкой) даже если оно соответствует другому шаблону в этой же строке. Также можно, заключив имя хоста или IP-адрес в квадратные скобки «**[**» и «**]**», через «**:**» указать нестандартный порт.

Вместо имён хостов можно записывать их хэши. Это позволит скрыть их от злоумышленника в случае попадания файла в его руки. Для различия хэшей от имён хостов первые предваряются символом «|». На одной строке может быть не больше одного хэша, операция отрицания в этом случае не доступна.

Разрядность, порядок и модуль копируются из ключа хоста RSA, например, **/etc/ssh/ssh_host_key.pub**. Необязательное поле комментария занимает всю оставшуюся часть строки и игнорируется.

Комментариями также считаются пустые и строки начинающиеся с «**#**».

Идентификация машины принимается, если любая совпавшая строка содержит правильный ключ. Таким образом, можно (хотя это не рекомендуется) иметь несколько строк или различных ключей для одного и того же хоста. Это неизбежно случается при помещении в файл кратких форм имён хостов из различных доменов. В файлах может содержаться противоречивая информация. Идентификация принимается, если адекватная информация имеется в любом из них.

> **Примечание!** Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен символов и, очевидно, не стоит вводить имена хостов вручную. Вместо этого их можно сгенерировать при помощи сценария оболочки или взять из файла **/etc/ssh/ssh_host_key.pub**, добавив в начале имя хоста.

Пример файла **ssh_known_hosts**:

```
# допустимы явные комментарии только на всю строку
closenet       192.0.2.53 1024 37 159...93 closenet.example.net
cvs.example.net,192.0.2.10 ssh-rsa AAAA1234 =
# хэш имени хоста
|1|JfKTdBh7rNbXkVAQCRp4OQoPfmI=|USECr3SWf1JUPsms5AqfD5QfxkM= ssh-rsa
AAAA1234 =
```

Файлы

Файл	Назначение
-/.hushlogin	Позволяет отключить вывод времени последнего входа в систему и содержимого файла /etc/motd, если в файле конфигурации включены соответственно PrintLastLog и PrintMotd. Файл не влияет на вывод содержимого Banner.
-/.rhosts	Этот файл используется для аутентификации по хосту (см. ssh(1)). На некоторых машинах, если каталог пользователя находится на разделе NFS, для того чтобы он был доступен пользователю root, он должен быть доступен для чтения всем. Файл должен принадлежать пользователю и не должен быть доступен для записи другим. Рекомендуемый набор прав доступа в общем случае - чтение/запись для пользователя и недоступность для других.
-/.shosts	Аналогичен файлу .rhosts, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью rlogin/rsh.

Файл	Назначение
~/.ssh/authorized_keys	Содержит список открытых ключей (RSA/DSA), которые могут быть использованы для регистрации данного пользователя. Формат файла описан выше. Этот файл не очень важен для злоумышленника, но мы рекомендуем сделать его доступным только пользователю (чтение/запись). Если этот файл, каталог ~/.ssh или домашний каталог пользователя доступны для записи другим пользователям, этот файл может быть изменён или заменён любым пользователем системы, имеющим сколько угодно мало прав. В этом случае sshd не будет использовать этот файл, если только параметр StrictModes не имеет значение «no». Установить рекомендуемый набор прав доступа можно командой chmod go-w ~/ ~/.ssh ~/.ssh/authorized_keys.
~/.ssh/environment	Этот файл (при его наличии) считывается в среду при регистрации в системе. Он может содержать только пустые строки, строки комментария (начинающиеся с «#») и определения значений переменных в виде: переменная=значение. Правом на запись этого файла должен обладать только пользователь; он не должен быть доступен остальным. Задание переменных среды отключено по умолчанию, за что отвечает параметр PermitUserEnvironment.
~/.ssh/known_hosts	Список адресов, к которым когда-либо подключался пользователь и которые отсутствуют в общесистемном файле, и соответствующих им открытых ключей. Формат файла описан выше. Файл должен быть доступен для записи только владельцу и администратору. Он может также быть доступен для чтения всем остальным, но это не обязательно.
~/.ssh/rc	Сценарий инициализации, запускаемый перед запуском оболочки пользователя или команды. Этот файл должен быть доступен для записи только пользователю и не должен быть вообще доступен другим.
/etc/hosts.allow **/etc/hosts.deny**	Данные о разрешении и запрете соединений с хостами для надстроек TCP. См. hosts_access(5).
/etc/hosts.equiv	Используется для аутентификации на основе хоста (см. ssh(1)). Должен быть доступен для записи только root.
/etc/moduli	Группы для схемы Диффи—Хеллмана. Формат файла описан в moduli(5).
/etc/motd	См. motd(5).
/etc/nologin	Если существует, подключение будет разрешено только суперпользователю. Любому, кто пытается войти в систему, будет показано содержимое этого файла и запросы на регистрацию в качестве не суперпользователя будут отвергнуты. Этот файл должен быть доступен для чтения всем.
/etc/shosts.equiv	Аналогичен hosts.equiv, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью rlogin/rsh.
/etc/ssh/ssh_known_hosts	Общесистемный список известных хостов и их ключей. Этот файл должен составляться администратором. В него следует включать открытые ключи всех компьютеров организации. Формат файла описан выше. Файл должен быть доступен всем для чтения и владельцу/администратору для записи.
/etc/ssh/ssh_host_key **/etc/ssh/ssh_host_dsa_key** **/etc/ssh/ssh_host_rsa_key**	Содержат частные ключи хостов. Файлы должны принадлежать root и быть доступными только для него. Не запустится, если эти файлы доступны для чтения кому-либо кроме суперпользователя.
/etc/ssh/ssh_host_key.pub **/etc/ssh/ssh_host_dsa_key.pub** **/etc/ssh/ssh_host_rsa_key.pub**	Содержат открытые ключи хостов. Должны быть доступны всем для чтения и только суперпользователю для записи. Содержимое файлов должно соответствовать содержимому соответствующих файлов с частными ключами. Эти файлы не используются программой и предназначены для копирования пользователем в файлы known_hosts. Эти файлы создаются командой ssh-keygen(1).
/etc/ssh/sshd_config	Конфигурация службы sshd. Формат файла и параметры конфигурации описаны в sshd_config(5).
/etc/ssh/sshrc	Аналогичен ~/.ssh/rc, позволяет задавать инициализационный сценарий глобально для всех пользователей. Должен быть доступен всем для чтения и только root для записи.
/var/empty	Каталог chroot(2), используемый при отделении полномочий на предаутентификационном этапе. В папке не должно быть никаких файлов, она должна принадлежать только root и не должна быть доступна другим для записи.
/var/run/sshd.pid	Идентификатор процесса, ожидающего запросов на подключение (если одновременно работает несколько экземпляров служб для нескольких портов, в него записывается идентификатор экземпляра запущенного последним). Содержимое этого файла может не быть защищено и может быть доступно всем.

Предостережения

Использование этой службы не повысит уровень защиты системы пока **rshd, rlogind** и **rexecd** не будут **полностью отключены** в системе.

Конфигурационный файл SSHD_CONFIG

Описание файла конфигурации

Указание времени

Файлы

Описание файла конфигурации

Служба **sshd** считывает данные о конфигурации из файла **/etc/ssh/sshd_config** (или из файла. указанного в командной строке при помощи параметра **-f**). Файл содержит пары параметр-значение, по одной на строку. Пустые и строки, начинающиеся с «**#**». интерпретируются как комментарии. Если аргументы содержат пробелы, они должны быть заключены в двойные кавычки (' ').

Далее приведены описания возможных параметров (регистр имён аргументов учитывается, регистр имён параметров - нет):

Очищать ли кэш аутентификационных данных клиента при завершении сеанса. Значение по умолчанию - «yes». Данный параметр относится только к протоколу версии 2.

Параметр	Значение
AcceptEnv	Список переменных среды, которые, будучи заданы клиентом, будут копироваться в environ(7) сеанса. Соответствующая настройка на стороне клиента выполняется параметром SendEnv и описана в ssh_config(5). Переменные указываются по имени, допускаются символы подстановки «*» и «?». Несколько переменных среды можно указывать через пробелы или в нескольких параметрах AcceptEnv. Данный параметр введен для предотвращения обхода ограничений среды пользователя посредством изменения значений переменных среды. По умолчанию не принимаются никакие переменные среды.
AddressFamily	Семейство адресов, которое должна использовать служба sshd(8). Допустимые значения: «any», «inet» (только IPv4) и «inet6» (только IPv6). Значение по умолчанию - «any».
AllowGroups	Список шаблонов имён групп через пробел. Если параметр определён, регистрация в системе разрешается только пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп; числовой идентификатор группы не распознаётся. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).
AllowTcpForwarding	Определяет, будет ли разрешено перенаправление TCP. Значение по умолчанию - «yes». Имейте ввиду, что отключение пересылки TCP не увеличит уровень защищённости системы, пока пользователям не запрещён доступ к командной оболочке, так как они всегда могут установить свои собственные перенаправления.
AllowUsers	Список имён пользователей через пробел. Если параметр определён, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов. Допустимы только имена пользователей; числовой идентификатор пользователя не распознаётся. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом разрешая доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).
AuthorizedKeysFile	Файл с открытыми ключами, которые могут быть использованы для аутентификации пользователей. Допустимо указание шаблонов, они преобразуются при настройке соединения: «%%» заменяется на символ «%», «%h» заменяется на домашний каталог идентифицируемого пользователя, «%u» - на имя пользователя. После преобразования AuthorizedKeysFile интерпретируется либо как абсолютный путь, либо как путь относительно домашнего каталога пользователя. Значение по умолчанию - «.ssh/authorized_keys».
Banner	На некоторых территориях для получения защиты со стороны закона может быть необходимо послание предупредительного сообщения перед аутентификацией. Содержимое указанного файла будет отправлено удалённому пользователю прежде, чем будет разрешена аутентификация. Этот параметр доступен только с протоколом версии 2. По умолчанию не выводится никакой информации.
ChallengeResponseAuthentication	Определяет, разрешается ли беспарольная аутентификация «вызов-ответ». Поддерживаются все схемы аутентификации login.conf(5). Значение по умолчанию - «yes».
Ciphers	Допустимые для протокола версии 2 шифры. Несколько шифров указываются через запятую. Поддерживаются следующие шифры: «3des-cbc», «aes128-cbc», «aes192-cbc», «aes256-cbc», «aes128-ctr», «aes192-ctr», «aes256-ctr», «arcfour128», «arcfour256», «arcfour», «blowfish-cbc» и «cast128-cbc». Значение по умолчанию: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128, arcfour256,arcfour,aes192-cbc,aes256-cbc,aes128-ctr, aes192-ctr,aes256-ctr
ClientAliveCountMax	Количество запросов, проверяющих доступность клиента (см. ниже), которые могут оставаться без ответа. Если предел достигнут, sshd(8) отключит клиента и завершит сеанс. Имейте в виду, запросы client alive отличаются от TCPKeepAlive (см. ниже). Данные запросы отправляются через защищённый канал и поэтому не могут быть подменены. Параметр TCPKeepAlive допускает возможность подмены данных. Механизм client alive полезен, если поведение клиента или сервера зависит от активности соединения. Значение по умолчанию - 3. Если ClientAliveInterval (см. ниже) равно 15, а для ClientAliveCountMax оставлено значение по умолчанию, не отвечающие клиенты SSH будут отключаться приблизительно через 45. Данный параметр относится только к протоколу версии 2.
ClientAliveInterval	Время бездействия со стороны клиента в секундах, после которого sshd(8) отправляет через защищённый канал запрос отклика клиенту. Значение по умолчанию - 0, что означает, что клиенту не будут направляться такие запросы. Этот параметр применим только с протоколом версии 2.
Compression	Разрешить сжатие сразу, после аутентификации или вообще запретить его. Допустимые значения - «yes», «delayed» и «no». Значение по умолчанию - «delayed».
DenyGroups	Список шаблонов имён групп через пробел. Если параметр определён, регистрация в системе пользователям, чья главная или вспомогательная группа соответствуют содержащимся в списке шаблонам, не разрешается. Допустимы только имена групп; числовой идентификатор группы не распознаётся. По умолчанию регистрация в системе разрешена для всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).

Параметр	Значение
DenyUsers	Список имён пользователей через пробел. Если параметр определён, регистрация в системе пользователей, чьи имена соответствуют одному из шаблонов, будет запрещена. Допустимы только имена пользователей; числовой идентификатор пользователя не распознаётся. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом запрещается доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).
ForceCommand	Выполнять указанную команду после регистрации пользователя в системе, игнорируя команду, запрашиваемую им. Команда запускается оболочкой пользователя с ключом -c. Это относится к выполнению оболочки, команды или подсистемы. Обычно применяется внутри блока Match. Команда, запрошенная пользователем, помещается в переменную среды SSH_ORIGINAL_COMMAND.
GatewayPorts	Определяет, разрешено ли удалённым машинам подключение к портам, выделенным для туннелирования трафика клиентов. По умолчанию, sshd(8) делает доступными порты, используемые для туннелирования, инициируемого сервером, только для кольцевого (loopback) адреса, т.е. удалённые машины подключаться к перенаправляемым портам не могут. С помощью данного параметра можно исправить такое положение дел. Значение «no» разрешает туннелирование только в рамках данной системы, «yes» разрешает туннелирование для хостов, соответствующих шаблону, а «clientspecified» позволяет клиенту самостоятельно выбирать адрес для туннелирования. Значение по умолчанию - «no».
GSSAPIAuthentication	Допускать аутентификацию по GSSAPI. Значение по умолчанию - «no». Данный параметр относится только к протоколу версии 2.
GSSAPICleanupCredentials	Указывает, следует ли автоматически уничтожать кэш учетных данных пользователя при выходе из системы. Значение по умолчанию - да.
HostbasedAuthentication	Допускать аутентификацию по хостам, т.е. аутентификацию по rhosts или /etc/hosts.equiv в сочетании с открытым ключом клиента. Этот параметр схож с RhostsRSAAuthentication и применим только к протоколу версии 2. Значение по умолчанию - «no».
HostbasedUsesNameFromPacketOnly	Отключить выполнение запросов имени хоста при обработке файлов ~/.shosts, ~/.rhosts и /etc/hosts.equiv в рамках аутентификации по хосту (HostbasedAuthentication). При значении «yes» для сравнения будет использоваться имя, указанное клиентом, а не имя, которое может быть получено стандартными средствами соединения TCP. Значение по умолчанию - «no».
HostKey	Файл с частными ключами хоста. Значение по умолчанию - /etc/ssh/ssh_host_key для протокола 1, и /etc/ssh/ssh_host_rsa_key и /etc/ssh/ssh_host_dsa_key для протокола 2. Имейте в виду, что sshd(8) не будет принимать файлы частных ключей доступные для чтения всей группе или вообще всем пользователям. Можно указывать несколько файлов с ключами хоста. Ключи «rsa1» используются для протокола версии 1, ключи «dsa» и «rsa» - для версии 2 протокола SSH.
IgnoreRhosts	Не учитывать содержимое файлов .rhosts и .shosts при аутентификации RhostsRSAAuthentication и HostbasedAuthentication. При этом будут учитываться только /etc/hosts.equiv и /etc/shosts.equiv. Значение по умолчанию - «yes».
IgnoreUserKnownHosts	Не учитывать содержимое файла ~/.ssh/known_hosts при RhostsRSAAuthentication или HostbasedAuthentication. Значение по умолчанию - «no».
KerberosAuthentication	Определяет, дозволена ли аутентификация Kerberos: Проверять ли пароль, указанный пользователем для аутентификации PasswordAuthentication в Kerberos KDC. Это может быть либо в форме тикетов Kerberos или, если PasswordAuthentication установлена в «yes», пароль, предоставленный пользователем, будет утвержден через Kerberos KDC. Для использования этого параметра серверу необходима Kerberos servtab, которая разрешит проверку субъекта KDC. Значение по умолчанию - «no».
KerberosGetAFSToken	Если AFS активна, и у пользователя имеется Kerberos 5 TGT, получать талон AFS перед обращением к домашнему каталогу пользователя. Значение по умолчанию - «no».
KerberosOrLocalPasswd	В случае непринятия аутентификации посредством Kerberos, проверять пароль другими механизмами, такими как /etc/passwd. Значение по умолчанию - «yes».
KerberosTicketCleanup	Очищать ли кэш талонов пользователя при завершении сеанса. Значение по умолчанию - «yes».
KeyRegenerationInterval	В протоколе версии 1 эфемерный ключ сервера будет автоматически регенерироваться по истечении этого количества секунд (если он использовался). Цель регенерации состоит в том, чтобы предохранить шифрованные установленные сеансы от более поздних вторжений на машину и захвата ключей. Ключ нигде не сохраняется. Если установлено значение «0», то ключ не будет регенерироваться. Значение по умолчанию - 3600 (секунд).
ListenAddress	Локальные адреса, по которым sshd(8) должен ожидать соединения. Могут быть использованы следующие форматы записей:
ListenAddress	хост | адрес-IPv4 | адрес-^6
ListenAddress	хост | адрес-IPv4 : порт
ListenAddress	[хост | адрес-IPv6 : порт] Если порт не указан, sshd будет ожидать соединения на указанном адресе и на всех указанных ранее (но не после) в параметре Port портах. По умолчанию ожидается соединение на всех локальных адресах. Допустимо указание нескольких параметров.
LoginGraceTime	Сервер отключается по истечении этого времени, если пользователю не удалась регистрация в системе. Если стоит значение «0», то время ожидания не ограничено. Значение по умолчанию - 120 секунд.
LogLevel	Задает степень подробности сообщений для протоколов sshd. Допустимыми являются значения: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, и DEBUG3. Значение по умолчанию - INFO. Значения DEBUG и DEBUG1 эквивалентны. Использование значения DEBUG* нарушает конфиденциальность пользователей и потому не рекомендуется.
MACs	Допустимые алгоритмы MAC (Message Authentication Code - код установления подлинности сообщения). Они используются в протоколе версии 2 для гарантирования целостности данных. Несколько алгоритмов следует указывать через запятую. Значение по умолчанию «hmac-md5,hmac-sha1,hmac- ripemd160,hmac-sha1-96,hmac-md5-96».

Параметр	Значение
Match	Начинает условный блок. Если все критерии на строке Match удовлетворены, указанные в блоке директивы будут иметь больший приоритет, чем указанные в глобальном разделе файла конфигурации. Концом блока считается либо следующая директива Match, либо конец файла. В качестве аргументов Match принимаются пары критерий-шаблон. Допустимые критерии: User Group Host и Address. В самом блоке Match допустимо указание следующих параметров: AllowTcpForwarding Banner ForceCommand GatewayPorts GSSApiAuthentication KbdInteractiveAuthentication KerberosAuthentication PasswordAuthentication PermitOpen RhostsRSAAuthentication RSAAuthentication X11DisplayOffset X11Forwarding X11UseLocalHost.
MaxAuthTries	Ограничение на число попыток идентифицировать себя в течение одного соединения. При достижении количества неудачных попыток аутентификации записи о последующих неудачах будут вноситься в протокол. Значение по умолчанию - 6.
MaxStartups	Ограничение на число одновременных соединений, в которых не был пройден этап аутентификации. Все последующие соединения не будут приниматься, пока на уже существующем соединении не будет произведена аутентификация или не истечет время, указанное в параметре LoginGraceTime. Значение по умолчанию - 10. Как альтернатива, может быть задействован ранний случайный отказ в подключении, путем указания трёх разделённых через двоеточие значений «старт:норма:предел» (например, "10:30:60"). Соединение будет сбрасываться с вероятностью «норма/100» (30%), если имеется «старт» (10) (10) соединений с не пройденным этапом аутентификации. Вероятность возрастает линейно и постоянно попытки будут отвергаться при достижении числа «предел» (60).
PasswordAuthentication	Допускать аутентификацию по паролю. Значение по умолчанию - «yes».
PermitEmptyPasswords	Допускать использование пустых паролей при аутентификации по паролю. Значение по умолчанию - «no».
PermitOpen	Ограничить возможные конечные точки для туннелирования TCP. Допустимые формы указания точек:
PermitOpen	хост : порт
PermitOpen	адрес-IPv4 : порт
PermitOpen	[адрес-IPv6] : порт. Возможно указание нескольких конечных точек через пробел. Значение «any» снимает ограничение и является значением по умолчанию.
PermitRootLogin	Допускать вход в систему через ssh в качестве суперпользователя. Допустимые значения: «yes», «prohibit-password»,«without-password», «forced-commands-only», «no». Значение по умолчанию - «prohibit-password». Если этот параметр установлен в значение «prohibit-password» или «without-password», войти в систему в качестве суперпользователя, указав для аутентификации пароль, будет невозможно. Если этот параметр установлен в значение «forced-commands-only», будет разрешена регистрация суперпользователя в системе по открытому ключу, но только если определён параметр command команда (что может быть полезно для удалённого создания резервных копий, даже если регистрация суперпользователя в системе в обычном режиме не разрешена). Все другие методы аутентификации для суперпользователя будут отключены. При значении «no» вход в систему в качестве root будет полностью запрещён.
PermitTunnel	Допускать использование перенаправления для устройств tun(4). Допустимые значения: «yes», «point-to-point» (уровень 3), «ethernet» (уровень 2), «no». Значение «yes» эквивалентно «point-to-point» и «ethernet» одновременно. Значение по умолчанию - «no».
PermitUserEnvironment	Учитывать ли файл ~/.ssh/environment и параметры environment= в файле ~/.ssh/authorized_keys. Значение по умолчанию - «no». Посредством изменения переменных среды пользователи могут обойти ограничения своих полномочий. Например, с помощью механизма LD_PRELOAD.
PidFile	Файл, в который следует записывать идентификатор процесса службы SSH. Значение по умолчанию - /var/run/sshd.pid.
Port	Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию - 22. Допустимо указание параметра несколько раз. См. также ListenAddress.
PrintLastLog	Выводить ли время и дату предыдущего входа в систему при интерактивной регистрации пользователя в ней. Значение по умолчанию - ''yes''.
PrintMotd	Выводить ли содержимое файла /etc/motd при интерактивной регистрации пользователя в системе (в некоторых системах это выполняется оболочкой, сценарием /etc/profile или аналогичным). Значение по умолчанию - «yes».
Protocol	Версии протокола, которые следует принимать. Допустимые значения - '1' и '2'. Несколько значений указываются через запятую. Значение по умолчанию - «2,1». Порядок указания протоколов не имеет значения, т.к. протокол выбирается клиентом из списка доступных.
PubkeyAuthentication	Допускать аутентификацию по открытому ключу. Значение по умолчанию - «yes». Данный параметр относится только к протоколу версии 2.
RhostsRSAAuthentication	Допускать аутентификацию по rhosts или /etc/hosts.equiv совместно с аутентификацией по хосту RSA. Значение по умолчанию - «no». Данный параметр относится только к протоколу версии 1.
RSAAuthentication	Допускать аутентификацию только по ключу RSA. Значение по умолчанию - «yes». Данный параметр относится только к протоколу версии 1.
ServerKeyBits	Длина ключа сервера для эфемерного протокола версии 1. Минимальное значение - 512, значение по умолчанию - 768.
StrictModes	Проверять наборы прав доступа и принадлежность конфигурационных файлов и домашнего каталога пользователя перед разрешением регистрации в системе. Это рекомендуется выполнять, потому что новички иногда оставляют свои каталоги или файлы доступными для записи всем. Значение по умолчанию - «yes».
Subsystem	Позволяет настроить внешнюю подсистему (напр., службу FTP). В качестве параметров должны выступать имя подсистемы и команда, которая будет выполняться при запросе подсистемы. Команда sftp-server(8) реализует подсистему передачи файлов «sftp». По умолчанию подсистемы не определены. Данный параметр относится только к протоколу версии 2.
SyslogFacility	Код источника сообщений для протокола syslog. Допустимые значения: DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7. Значение по умолчанию - AUTH.

Параметр	Значение
TCPKeepAlive	Указывает, будет ли система посылать другой стороне контрольные сообщения для удержания соединения активным. Если они посылаются, то разрыв соединения или аварийный отказ одной из машин будут должным образом замечены. Однако, при этом временная потеря маршрута также повлечёт за собой разрыв соединения, и некоторые люди сочтут это раздражающим. С другой стороны, если контрольные сообщения не посылаются, сеанс на сервере может зависнуть, оставив после себя «пользователей-привидений» и отнимая ресурсы сервера. Значение по умолчанию - «yes» (отправлять сообщения TCP keepalive). Это позволяет избежать бесконечно долгих сеансов. Для отключения отправки сообщений TCP keepalive установите значение «no».
UseDNS	Выполнять ли запросы DNS для получения имени удалённого хоста, для того чтобы убеждаться в том, что обратное преобразование выдаёт тот же самый IP-адрес. Значение по умолчанию - «yes».
UseLogin	Использовать login(1) для интерактивных сеансов регистрации в системе. Значение по умолчанию - «no». Имейте ввиду, что login(1) никогда не используется для удалённого выполнения команд. Если этот параметр включен, функция X11Forwarding будет отключена, потому что login(1) не может обрабатывать cookie xauth(1). В случае использования разделения полномочий (UsePrivilegeSeparation) данный параметр будет отключен после прохождения аутентификации.
UsePAM	Включить интерфейс модулей аутентификации Pluggable Authentication Module. При значении «yes» аутентификация PAM будет доступна через ChallengeResponseAuthentication и PasswordAuthentication в дополнение к учётной записи PAM и обработке модулей сеансов для всех типов аутентификации. Поскольку беспарольная аутентификация PAM «вызов-ответ» служит заменой аутентификации по паролю, необходимо отключить либо PasswordAuthentication, либо ChallengeResponseAuthentication. При включенном UsePAM службу sshd(8) можно будет выполнять только с правами root. Значение по умолчанию - «no».
UsePrivilegeSeparation	Разделять полномочия посредством создания дочернего процесса с меньшими правами для обработки входящего сетевого трафика. После прохождения аутентификации для работы с клиентом будет создаваться специальный процесс, соответствующий его правам. Целью данного параметра служит предотвращение повышения полномочий злоумышленником. Значение по умолчанию - «yes».
X11DisplayOffset	Номер первого дисплея, доступного для туннелирования трафика X11 sshd(8). Позволяет избежать вмешательства sshd в работу настоящих серверов X11. Значение по умолчанию - 10.
X11Forwarding	Допускать туннелирование X11. Допустимые значения - «yes» и «no». Значение по умолчанию - «no». Если дисплей-посредник ожидает соединений от любых адресов (или по шаблону) sshd(8), включение туннелирования X11 подвергает сервер и логические дисплеи клиентов дополнительной опасности. Поэтому такое поведение не является поведением по умолчанию. Проверка и подмена аутентификационных данных при атаке выполняются на стороне клиента. При туннелировании X11 графический сервер клиента может подвергаться атаке при запросе клиентом SSH-туннелирования (см. замечания в описании параметра ForwardX11 в ssh_config(5)). Для большей защиты пользователей администратор может запретить туннелирование, установив значение «no». Обратите внимание, что даже если туннелирование X11 запрещено данным параметром, пользователи по-прежнему смогут туннелировать трафик X11 посредством настройки туннелей общего назначения. Туннелирование X11 отключается автоматически при включении UseLogin.
X11UseLocalhost	К какому адресу следует привязывать сервер туннелирования X11: к кольцевому (loopback) или адресу, указанному по шаблону. По умолчанию сервер туннелирования привязывается к кольцевому адресу, а в качестве хоста в переменную среды DISPLAY заносится «localhost». Это не позволяет удалённым хостам подключаться к дисплею-посреднику. Однако, в случае старых клиентов X11, такая конфигурация может не сработать. Установите тогда X11UseLocalhost в «no». Допустимые значения - «yes» и «no». Значение по умолчанию - «yes».
XAuthLocation	Путь к команде xauth(1). Значение по умолчанию - /usr/X11R6/bin/xauth.

Указание времени

Ключи командной строки **sshd** и параметры файлов конфигурации могут требовать указания времени. Оно должно указываться в виде последовательности таких выражений:

```
<время> <единицы>
```

, где <время> - положительное целое число, <единицы> могут принимать следующие значения:

Единица	Значение единицы
ничего	-
s | S	секунды
m | M	минуты
h | H	часы
d | D	дни
w | W	недели

Итоговое время получается в результате сложения всех выражений.

Примеры:

Единицы	Значения
600	600 секунд (10 минут)

10m	10 минут
1h30m	1час 30 минут (90 минут)

Файлы

Файл конфигурации sshd.

/etc/ssh/sshd_config

> **Примечание!** Этот файл должен быть доступен для записи только пользователю **root**, и рекомендуется делать его доступным для чтения всем.

Работа с клиентом и сервером SSH

Описание принципов работы и используемых приложений
Установка
Настройка сервера
Рекомендуемые параметры безопасности
Максимальное число попыток аутентификации
Время ожидания регистрации пользователя в системе
Списки пользователей sshd
Запрещение удаленного доступа для суперпользователя
Парольная аутентификация
Аутентификация на основе SSH2 RSA-ключей
Настройка SSH-клиента
Утилита screen
SSH aliases
SFTP
Монтирование удаленной директории с помощью sshfs
Запуск графических приложений через SSH
Копирование файлов SCP
Подключение через MC (Midnight Commander)
Диагностика проблем подключения

Данная статья посвящена клиенту и серверу защищенного терминала (secure shell) в РЕД ОС, их настройке и использованию. **SSH** — это специальный сетевой протокол, позволяющий получать удаленный доступ к компьютеру с большой степенью безопасности соединения.

Описание принципов работы и используемых приложений

В основном, SSH реализован в виде двух приложений — *SSH-сервера* и *SSH-клиента*. При подключении клиент проходит процедуру авторизации у сервера и между ними устанавливается зашифрованное соединение. OpenSSH-сервер может работать как с протоколом *ssh1*, так и с протоколом *ssh2*. В настоящее время протокол **ssh1** считается небезопасным, поэтому его использование **крайне не рекомендуется**. В этой статье мы не будем останавливаться на технических деталях работы протокола, так как основная цель руководства — описание его настройки и использования.

Вы можете подробнее ознакомиться с информацией установке и настройке клиента и сервера SSH, просмотрев наши обучающие видео:

- на **RuTube** — Работа с клиентом и сервером SSH;
- в **Яндекс.Дзен** — Работа с клиентом и сервером SSH;
- в **VK Видео** — Работа с клиентом и сервером SSH.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

По умолчанию сервер и клиент **OpenSSH** уже установлен в РЕД ОС. Однако, при необходимости, его можно установить из терминала командой:

```
sudo dnf install openssh
```

Настройка сервера

Для его остановки и запуска используйте команды:

```
sudo systemctl stop sshd
sudo systemctl start sshd
```

Основной файл конфигурации SSH-сервера — файл **/etc/ssh/sshd_config**, доступный для чтения или редактирования только суперпользователю. После каждого изменения этого файла необходимо перезапустить ssh-сервер для применения таких изменений командой:

```
sudo systemctl restart sshd
```

Рекомендуемые параметры безопасности

Сам по себе, неправильно настроенный SSH-сервер — огромная уязвимость в безопасности системы, т. к. у потенциального злоумышленника есть возможность получить практически неограниченный доступ к системе. Помимо этого, у *sshd* есть много дополнительных полезных опций, которые желательно включить для повышения удобства работы и безопасности.

```
Port, ListenAddress и AddressFamily
```

Эти три параметра определяют, на каких портах и адресах ваш сервер будет ждать входящие соединения. Во-первых, имеет смысл по возможности ограничить семейство обрабатываемых адресов реально используемыми, т. е. если вы используете только IPv4 — отключите IPv6, и наоборот. Сделать это можно при помощи параметра **AddressFamily**, например (для разрешения IPv4 и запрета IPv6):

```
AddressFamily inet
```

Во-вторых, если ваш ssh-сервер имеет выход в интернет, либо находится в незащищённой сети, желательно сменить стандартный порт (22), на котором слушает sshd. Это связано с тем, что многочисленные сетевые сканеры постоянно пытаются соединиться с 22-м портом и, как минимум, получить доступ путем перебора логинов/паролей из своей базы. Даже если у вас и отключена парольная аутентификация — эти попытки сильно засоряют журналы и (в большом количестве) могут негативно повлиять на скорость работы ssh-сервера. Если же вы по какой-либо причине не желаете изменить стандартный порт, вы можете использовать различные внешние утилиты для борьбы брутфорсерами, например *fail2ban*.
Задать порт можно как абсолютным значением для всех интерфейсов при помощи директивы **Port**, так и конкретным значением для каждого интерфейса, при помощи директивы **ListenAddress**. Например:

```
Port 2002
```

или

```
ListenAddress 192.168.0.1:2003
ListenAddress 192.168.1.1:2004
```

После того, как был задан порт, в любой из приведённых выше опций, необходимо предупредить систему безопасности операционной системы о внесённых изменениях. Если этого не сделать, то, при попытке перезапуска ssh-сервера, SELinux заблокирует его работу. Для этого используем команду:

```
sudo semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
```

Если задан порт, отличный от стандартного, строка подключения будет иметь вид:

```
ssh -p 2002 user@server
```

Максимальное число попыток аутентификации

```
MaxAuthTries
```

Прописывается в файле **/etc/ssh/sshd_config** и указывает максимальное число попыток аутентификации, разрешенное для одного соединения. Как только число неудачных попыток превысит половину заданного значения, все последующие попытки будут заноситься в журнал. При достижении максимума сеанс аутентификации разрывается.

Время ожидания регистрации пользователя в системе

```
LoginGraceTime
```

Как и предыдущий параметр, указывается в файле настройки ssh-сервера. Он задаёт время ожидания регистрации пользователя в системе. Если пользователь не успел войти в систему в течение отведенного данной директивой времени, сеанс обрывается.

Списки пользователей sshd

```
AllowUsers user
```

В файле настроек **/etc/ssh/sshd_config** может быть прописан список пользователей, разделённых пробелом, которым можно пользоваться sshd. По умолчанию — не указан = разрешено всем. Т.е. если указан хотя бы один пользователь, ssh доступ к серверу доступен только для него.

```
AllowGroups users
```

Список шаблонов имён групп через пробел. Если параметр определён, регистрация в системе разрешается только пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп; числовой

идентификатор группы не распознаётся. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. Подробнее см. "Конфигурационный файл SSHD_CONFIG"

Дополнительную информацию см. в статье "Служба sshd - OpenSSH, сервер протокола SSH, описание"

Запрещение удаленного доступа для суперпользователя

Учетная запись root часто является целью хакеров. Доступ к учетной записи через root по протоколу SSH на сервере Linux, который работает в сети или в Интернете, может представлять серьезную угрозу безопасности.
По умолчанию root-доступ по паролю разрешён. Если есть пользователь, который имеет возможность решать все административные задачи через sudo, то рекомендуется совсем отключить root-доступ по ssh. Отключить эту опцию можно так:

```
PermitRootLogin no
```

Парольная аутентификация

Разрешенная по умолчанию парольная аутентификация является практически самым примитивным способом авторизации в **sshd**. С одной стороны, это упрощает конфигурацию и подключение новых пользователей (пользователю достаточно знать свой системный логин/пароль), с другой стороны пароль всегда можно подобрать, а пользователи часто пренебрегают созданием сложных и длинных паролей. Специальные боты постоянно сканируют доступные из интернета ssh-сервера и пытаются авторизоваться на них путем перебора логинов/паролей из своей базы. Настоятельно не рекомендуется использовать парольную аутентификацию. Отключить ее можно так:

```
PasswordAuthentication no
```

Если по каким-либо причинам вам все-таки хочется использовать парольную аутентификацию — позаботьтесь о том, чтобы никто не мог авторизоваться с пустым паролем. Для этого задайте директиву **PermitEmptyPasswords**:

```
PermitEmptyPasswords no
```

Аутентификация на основе SSH2 RSA-ключей

Наиболее предпочтительным способом авторизации является аутентификация на основе SSH2 RSA-ключей. При таком способе пользователь генерирует на своей стороне пару ключей, из которой один ключ является *приватным*, а другой *публичным*. *Публичный* ключ копируется на сервер и служит для проверки идентичности пользователя. Подробную информацию о создании пары ключей и способах их размещения на сервере см. в нашей инструкции «Аутентификация по протоколу SSH с использованием RSA-ключа».

Для включения аутентификации по публичному ключу в файле конфигурации сервера **/etc/ssh/sshd_config** для параметра PubkeyAuthentication укажите значение yes:

```
PubkeyAuthentication yes
```

Сервер должен знать, где ему следует искать публичный ключ пользователя. Для этого применяется специальный файл **authorized_keys**.

Можно указать как один общий файл с ключами, так и по одному файлу на каждого пользователя. Последний способ является более удобным и безопасным, т. к. можно, во-первых, указывать разные комбинации ключей для каждого пользователя, а во-вторых, ограничить доступ к публичному ключу пользователя. Задать файл с ключами можно при помощи директивы **AuthorizedKeysFile**:

- для схемы с общим файлом:

```
AuthorizedKeysFile /etc/ssh/authorized_keys
```

- для схемы пользователь — файл:

```
AuthorizedKeysFile .ssh/authorized_keys
```

По умолчанию SSH-клиент ищет ключи в файле **.ssh/authorized_keys**, т. е. по схеме пользователь-файл.

Настройка SSH-клиента

Наиболее безопасным считается вход по ключу, и в большинстве случаев на стороне сервера такая возможность включена, так что для её использования никаких прав суперпользователя не требуется. На клиентской машине генерируем ключ:

```
ssh-keygen -t rsa
```



Получаем предложение ввести пароль для защиты файла ключа (оказывается полезным при попадании файла в чужие руки). Если мы собираемся по SSH выполнять скрипты, то оставляем пароль пустым. Передаём публичный ключ на сервер командой:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
```

Всё, можно заходить:

```
ssh user@server
```

Когда ssh работает на нестандартном порту:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub -p port user@server
```

Если возникает ошибка, попробуйте взять параметры в кавычки:

```
ssh-copy-id '-i /home/user/.ssh/id_rsa.pub -p port user@server'
```

Завершающий этап настройки: отключение парольной аутентификации на сервере, см. «Парольная аутентификация».

Примечание.

В новых версиях **systemd** и **OpenSSH** поддержка **tcp_wrappers** будет прекращена.

tcp_wrapper выполняет управление доступом только для приложений, разработанных на основе протокола **TCP** и вызывающих библиотеку **libwrap**. После удаления зависимости **libwrap** из **openssh** перестанут действовать правила, определенные в файле **/etc/hosts.deny**. Для блокирования нежелательного трафика необходимо использовать брандмауэры **iptables/nftables** на сетевом уровне или использовать аналогичную фильтрацию на уровне приложений, поскольку они не имеют подобных ограничений.

ВАЖНО!

Мы **НЕ РЕКОМЕНДУЕМ** продолжать использовать инструмент **tcp_wrappers**. Для контроля трафика используйте брандмауэр **firewall**. Подробную информацию о настройке брандмауэра можно посмотреть по ссылке.

Если вы все же решите продолжить использовать инструмент **tcp_wrappers** для контроля сетевого трафика, функциональность данного инструмента для любой службы можно возобновить, выполнив ряд действий:

Примечание.

В случае, если используется **РЕД ОС 8**, необходимо предварительно установить пакет **tcp_wrappers** командой:

```
sudo dnf install tcp_wrappers
```

1. Отключите службу **sshd**:

```
systemctl disable sshd
```

2. Создайте каталог **/etc/systemd/system/sshd@.service.d/** для переопределения конфигурации:

```
mkdir -p /etc/systemd/system/sshd@.service.d/
```

3. Создайте переопределяющий файл конфигурации для службы SSH **/etc/systemd/system/sshd@.service.d/override.conf**:

```
nano /etc/systemd/system/sshd@.service.d/override.conf
```

```
[Unit]
ConditionFileIsExecutable=/usr/sbin/tcpd

[Service]
ExecStart=
```

4. В переопределяющий файл добавьте параметр **ExecStart** из файла конфигурации по умолчанию, добавив в значение **@-/usr/sbin/tcpd**:

```
grep '^ExecStart=' /usr/lib/systemd/system/sshd@.service | sed 's#[^\/]*\(.*\)#ExecStart=@-/usr/sbin/tcpd \1#'
>>/etc/systemd/system/sshd@.service.d/override.conf
```

Пример содержимого переопределяющего файла конфигурации:

```
cat /etc/systemd/system/sshd@.service.d/override.conf

[Unit]
ConditionFileIsExecutable=/usr/sbin/tcpd

[Service]
ExecStart=
ExecStart=@-/usr/sbin/tcpd /usr/sbin/sshd -i $OPTIONS
```

5. Измените политику SELinux для отслеживания трафика по **TCP**:

```
setsebool -P ssh_use_tcpd=1
```

6. Перезапустите конфигурацию **systemctl**:

```
systemctl daemon-reload
```

7. Запустите и добавьте в автозагрузку сокет **sshd**:

```
systemctl enable --now sshd.socket
```

8. Проверьте подключение к новой службе:

```
ssh localhost
```

Подключение должно произойти вне зависимости от содержимого файлов **/etc/hosts.allow** и **/etc/hosts.deny**.

9. Внесите изменения в файл запрещенных соединений **/etc/hosts.deny**:

```
nano /etc/hosts.deny
```

```
sshd: 127.0.0.1 [::1]
```

10. Убедитесь, что содержимое файла **/etc/hosts.deny** зафиксировано:

```
ssh localhost

kex_exchange_identification: read: Connection reset by peer
Connection reset by ::1 port 22
```

Соединение должно быть заблокировано.

11. Заблокированное соединение также должно быть зафиксировано в журнале:

```
journalctl -t sshd | grep refused
```

```
окт 17 16:19:44 localhost.localdomain sshd[4249]: refused connect from ::1 (::1)
```

Аналогичный подход можно использовать для других служб, у которых удалена зависимость **tcp_wrappers**.

Утилита screen

Screen – это приложение, позволяющее запускать несколько виртуальных терминалов в режиме сессий. После того как сессия создана, от неё можно отключиться, а позже — снова подключиться, причём с любого другого хоста, на котором установлен SSH-клиент. Процессы, запущенные в **screen**, продолжают выполняться и после того как пользователь отключается от сессии или вообще от хоста в целом.

Для установки программы **screen** на сервере выполните команду:

```
dnf install screen
```

Подключаемся к серверу:

```
ssh user@server
```

После подключения создаем новую сессию **screen** с названием **session1**:

```
screen -S session1
```

Затем выполняем на сервере необходимые действия и команды. Для примера запустим **ping** до ресурса **ya.ru**:

```
ping ya.ru
```

Для отключения от сессии нажмем сочетание «**Ctrl+a d**». При этом процесс **ping** продолжит выполнение, даже если разорвать ssh-подключение к серверу. Чтобы вернуться в нашу сессию выполним команду:

```
screen -r session1
```

Можно увидеть, что утилита **ping** все еще будет работать.

Более подробную информацию о работе с терминальными мультиплексорами описана в статье Терминальные мультиплексоры.

SSH aliases

При использовании нескольких серверов с различными параметрами доступа (нестандартный порт, длинное имя хоста, логин отличный от локального, и т.п.) приходится каждый раз вводить настройки подключения заново. Чтобы облегчить этот процесс, можно использовать псевдонимы — **aliases**.

Настройки хранятся в **~/.ssh/config** для одного пользователя и в **/etc/ssh/ssh_config** глобально для всех пользователей.

Пример конфигурации.

Открываем с помощью текстового редактора нужный нам файл настроек (для одного пользователя или глобальный) и добавляем следующие строки:

```
Host AliasName
HostName 1.2.3.4
User YourUserName
Port YourSSHPort
```

Где:

- **Host** — алиас (псевдоним) для удаленного сервера;
- **HostName** — IP-адрес или доменное имя (если работает DNS) удаленного сервера;
- **User** — имя пользователя для соединения по SSH;
- **Port** — порт SSH на удаленном сервере.

Таким образом может быть описано множество серверов.

После этого можно подключаться к серверу командой

```
ssh AliasName
```

SFTP

В sshd по умолчанию встроен SFTP-сервер. Протокол **SFTP** (**SSH File Transfer Protocol**) — SSH-протокол для передачи файлов. Он предназначен для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения. Как правило, в качестве базового протокола, обеспечивающего соединение, и используется протокол SSH2. Для того чтобы включить поддержку SFTP, добавьте в **sshd_config** строку:

```
subsystem sftp /usr/libexec/openssh/sftp-server
```

По умолчанию поддержка SFTP включена.

Монтирование удаленной директории с помощью sshfs

При постоянном использовании ресурсов ssh-сервера, для удобства возможно монтирование удаленного каталога в локальную директорию.

Установка:

```
sudo dnf install sshfs
```

Монтирование:

```
sshfs user@server:/home/userdir ~/sshfsdir
```

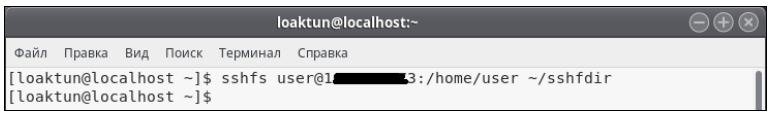
Директория, в которую производится монтирование, должна быть предварительно создана:

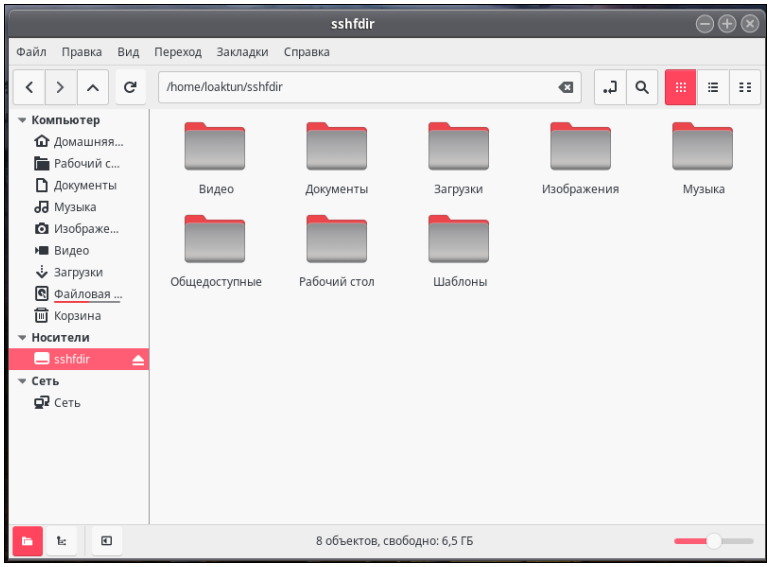
```
mkdir ~/sshfsdir
```

Размонтирование:

```
fusermount -u ~/sshfsdir
```

Пример:





Запуск графических приложений через SSH (X11Forwarding)

Настройка сервера.

В файле конфигурации **/etc/ssh/sshd_config** прописываем:

```
...
X11Forwarding yes
```

```
...
```

Перезапускаем ssh-сервер:

```
systemctl restart sshd
```

Настройка клиента.

В файле конфигурации **/etc/ssh/ssh_config** прописываем:

```
...
ForwardX11 yes
...
```

После того, как настройка закончена, заходим на удаленный хост и потом запускаем приложение, например, текстовый редактор **pluma**:

```
ssh -XC user@server
pluma
```

Чтобы сразу запустить приложение pluma:

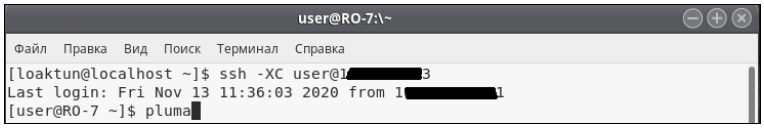
```
ssh -XC user@server "pluma"
```

Опции:

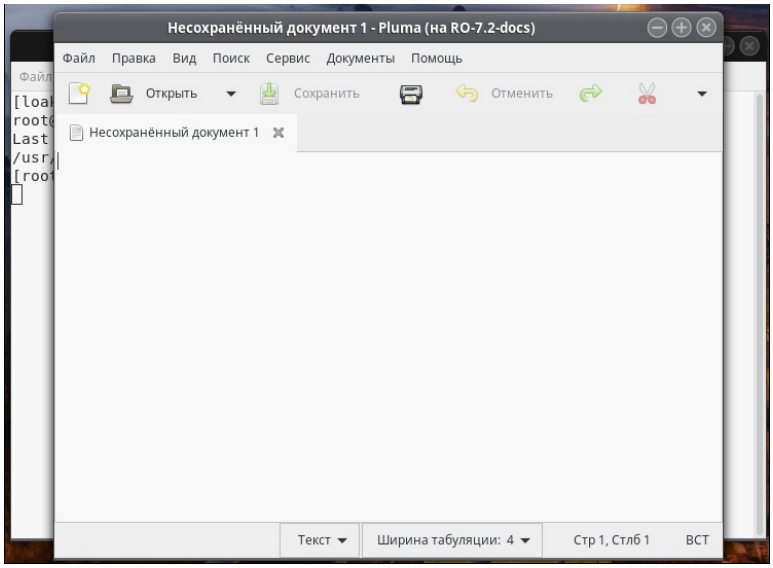
```
X : перенаправлять графический вывод
C : компрессия передаваемых данных
```

Пример.

Запуск:



Результат выполнения:



Создаваемый файл будет сохранён на удалённой машине.

Копирование файлов SCP

С помощью этой консольной утилиты можно перемещать файлы между удалённой и локальной системой.

Копирование файла на удалённую машину:

```
scp /srcfolder/file1 user@server:/destfolder/file1
```

Копирование файла на локальную машину с удалённой:

```
scp user@server:/srcfolder/file1 /destfolder/file1
```

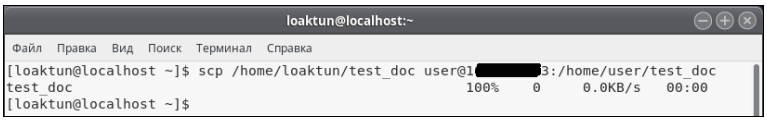
При копировании файлов нужно учитывать, что если на удалённой машине уже существует файл с таким же именем, то после выполнения команды он будет перезаписан.

Доступные опции :

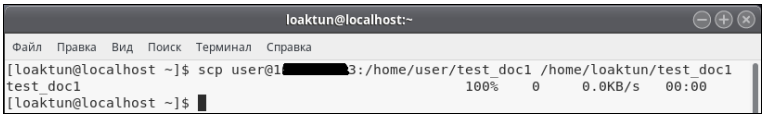
```
C : сжимать данные при их отправке на конечный компьютер.
r : рекурсивно копировать каталоги.
```

Пример.

Копирование на удалённую машину:



Копирование из удалённой системы в локальную:



Подключение через MC (Midnight Commander)

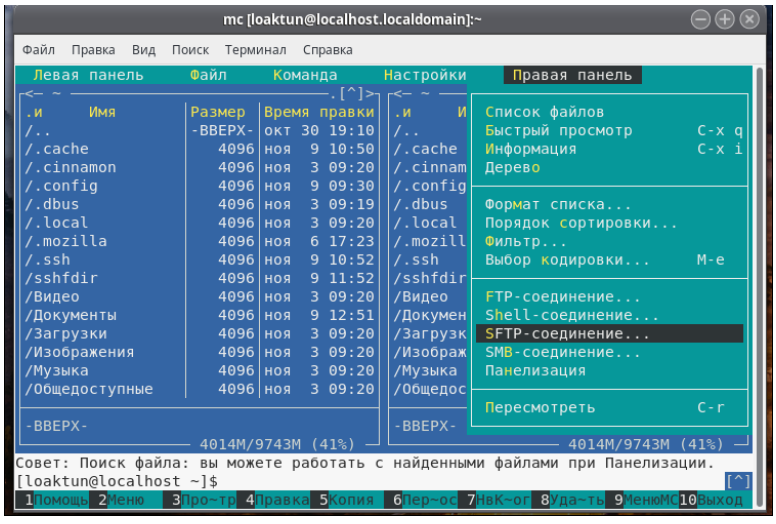
Midnight Commander (**MC**) — это визуальный файловый менеджер. Это программа, которая позволяет вам копировать, перемещать и удалять файлы и директории, производить поиск файлов и запускать на выполнение команды оболочки.

Также Midnight Commander позволяет подключиться к ssh-серверу.

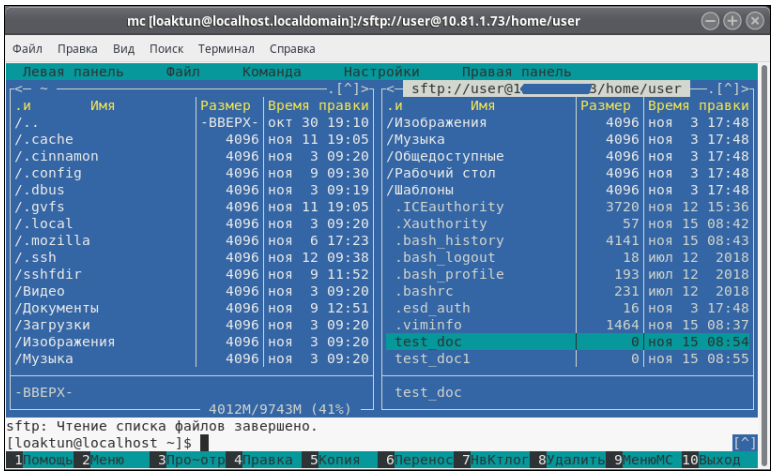
Для запуска программы в консоли вводим:

```
mc
```

После чего, клавишей **F9** активируем верхнее меню. В нём выбираем панель, левую или правую, в которой будет произведено подключение к ssh-серверу. В выпадающем меню выбираем пункт «SFTP-соединение».



После этого в появившейся строке вводим адрес сервера в формате **user@server**, и пароль, если аутентификация происходит не по ключу. В результате получим удобный и наглядный вариант для работы с файлами на сервере и возможностью производить копирование файлов как на сервер, так и с него на локальную систему.



Диагностика проблем подключения

Для анализа лога подключения используется команда:

```
ssh -vvv user@server
```

Для анализа конфигурационных файлов ssh-клиента и сервера, вам может понадобиться подробное описание параметров, значений и т. п. Для этого используйте команды вывода справки:

```
man ssh #
man sshd #
```

Muon – графический SSH-клиент

Предварительная подготовка
Установка и настройка Muon
Смена языка интерфейса
Работа с программой

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: snapd-2.58.3-1, muon-ssh-2.2.0

Muon - это графический SSH-клиент. В нем доступны такие инструменты как:

- расширенный файловый браузер **SFTP**,
- эмулятор терминала **SSH**,
- удаленный менеджер ресурсов/процессов,
- анализатор дискового пространства сервера,
- текстовый редактор,
- просмотрщик журналов, а также многие другие полезные инструменты, которые упрощают работу пользователей.

Muon предоставляет функциональность, аналогичную веб-панелям управления, но работает по протоколу **SSH** с локального компьютера, следовательно, установка на сервер не требуется.

Вы можете подробнее ознакомиться с работой графической утилиты **muon**, просмотрев наши обучающие видео:

- на **RuTube** — Muon - графический SSH-клиент;
- в **Яндекс.Дзен** — Muon - графический SSH-клиент;
- в **VK Видео** — Muon - графический SSH-клиент.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка

Muon в РЕД ОС устанавливается и запускается с помощью изолированной программной среды **snap**, поэтому перед настройкой muon требуется установить **snap**, если он еще не установлен.

Подробную информацию об установке и настройке **snap** см. в нашей статье «Snap - изолированная среда для запуска приложений».

После установки **snap** потребуется перезагрузить систему, чтобы убедиться, что пути snap были обновлены правильно.

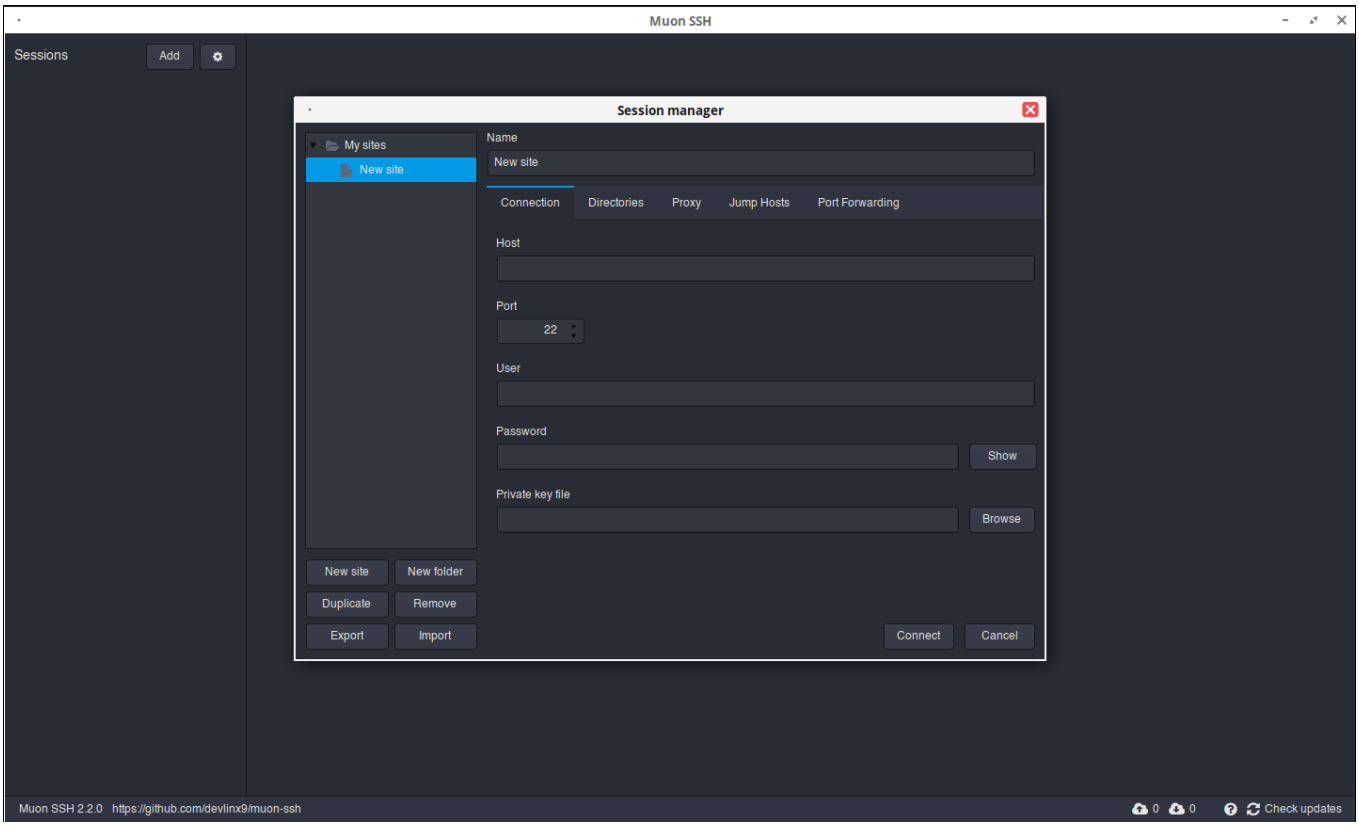
Установка и настройка Muon

Для установки **muon** выполните следующую команду:

```
sudo snap install muon-ssh --edge
```

После установки запуск программы доступен из «**Главного меню**» — «**Прочие**» — «**Muon SSH client snap**».

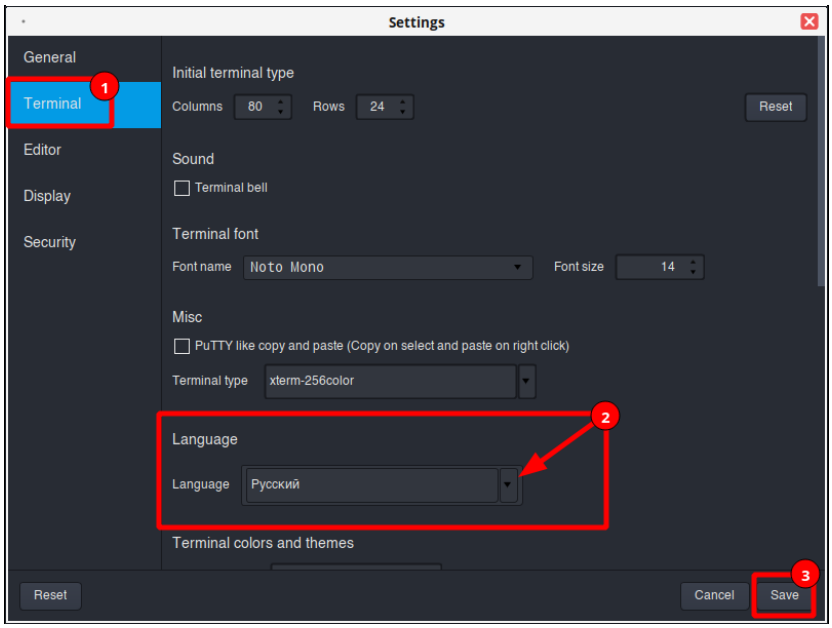
Главное окно клиента **muon** выглядит следующим образом:



Смена языка интерфейса

Для смены языка приложения откройте настройки программы, нажав на кнопку  .

На вкладке «**Terminal**» в разделе «**Language**» в выпадающем меню выберите необходимый язык (в примере выбран русский). Нажмите «**Save**».

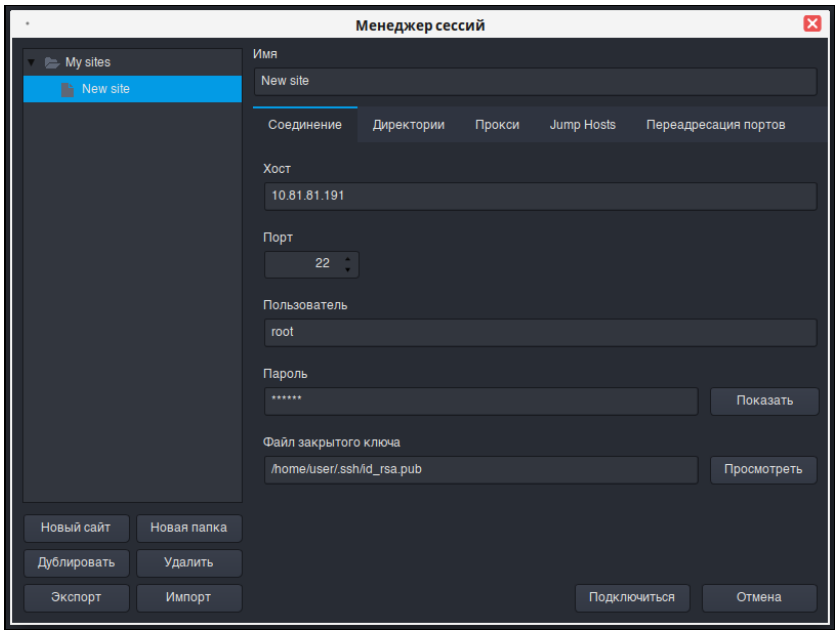


Для применения изменений перезапустите программу.

Работа с программой

Для использования **muon** необходим настроенный SSH-сервер, к которому будет производиться подключение. Информацию о настройке SSH-сервера см. в нашей статье «Работа с клиентом и сервером SSH».

Для подключения к SSH-серверу на главной странице программы нажмите кнопку «**Добавить**». Будет открыто окно настройки подключения «**Менеджер сессий**».



В поле **Хост** укажите IP-адрес сервера или имя хоста.

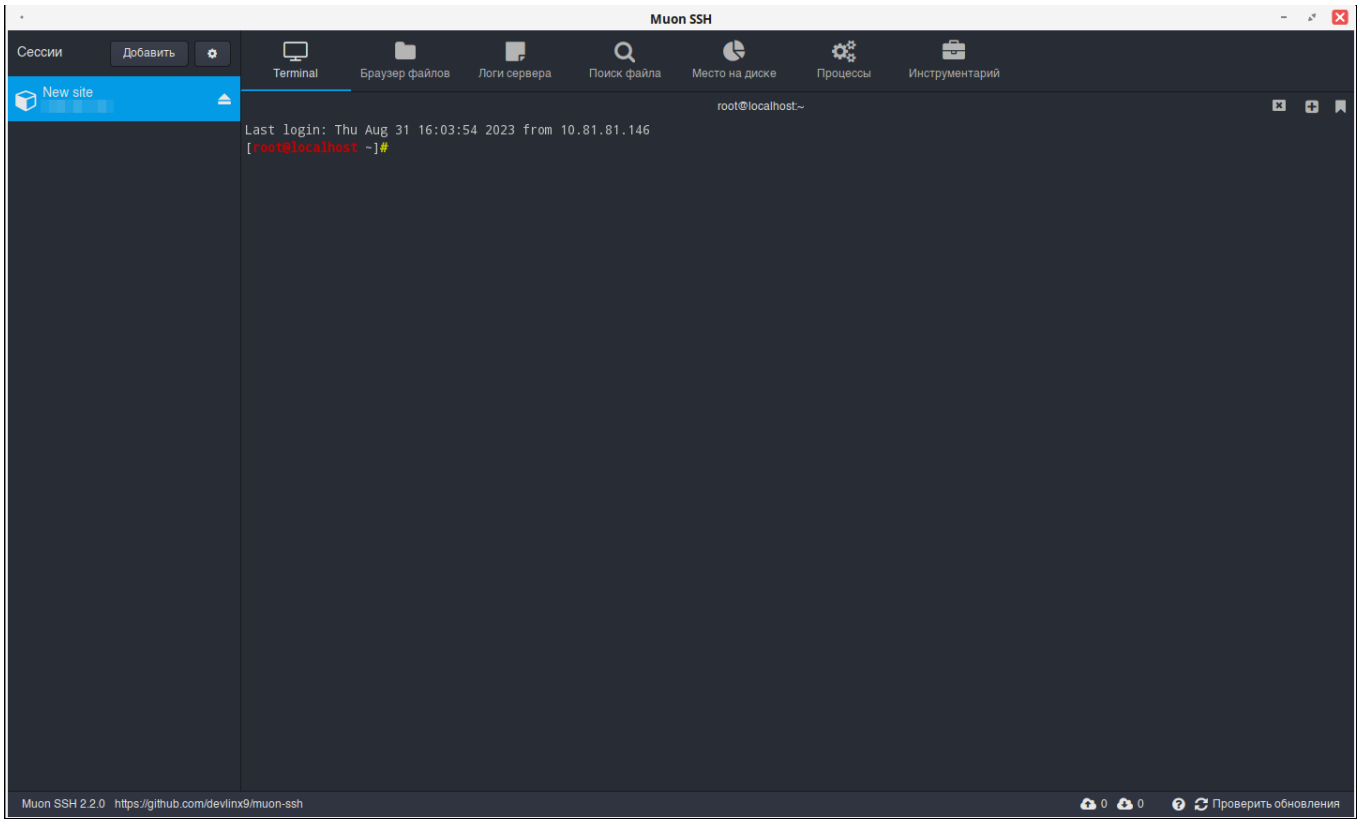
В поле **Порт** укажите нормер порта для подключения (по умолчанию используется порт 22).

В поле **Пользователь** укажите имя пользователя, к учетной записи которого необходимо подключиться.

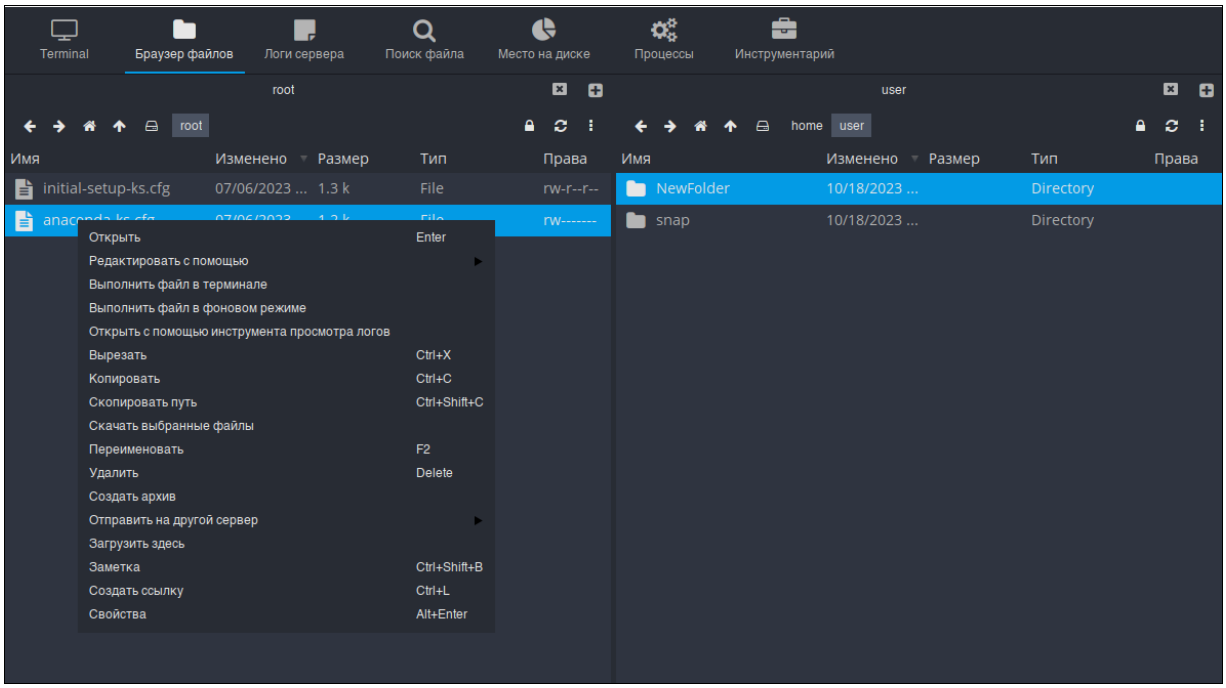
В поле **Пароль** укажите пароль от учетной записи указанного выше пользвоателя.

В поле **Файл закрытого ключа** загрузите файл из каталога, в котором хранится закрытый ключ.

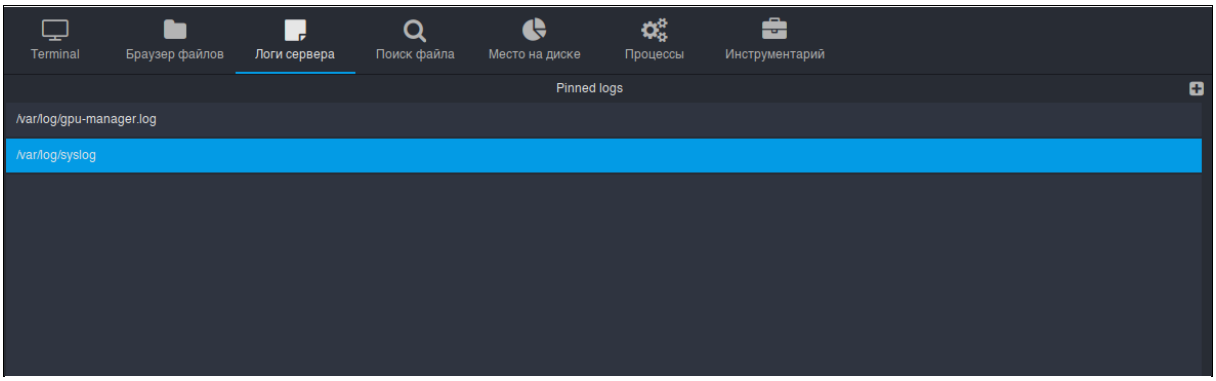
При успешном подключении будет запущен терминал удалённого хоста.



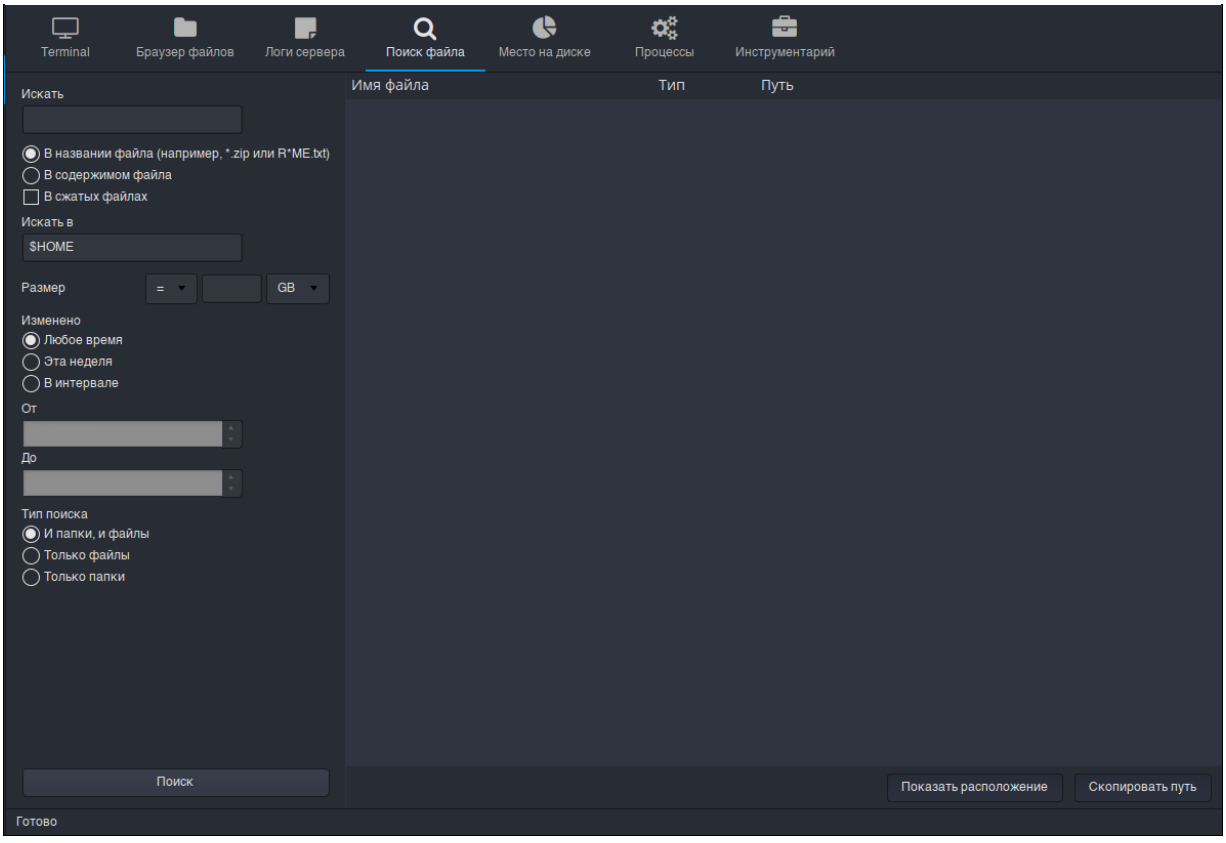
На вкладке «**Браузер файлов**» можно просмотреть содержимое каталогов, доступных пользователю. При нажатии ПКМ по какому-либо файлу или каталогу будет вызвано контекстное меню с доступными действиями.



На вкладке «**Логи сервера**» доступны системные журналы удаленного хоста.

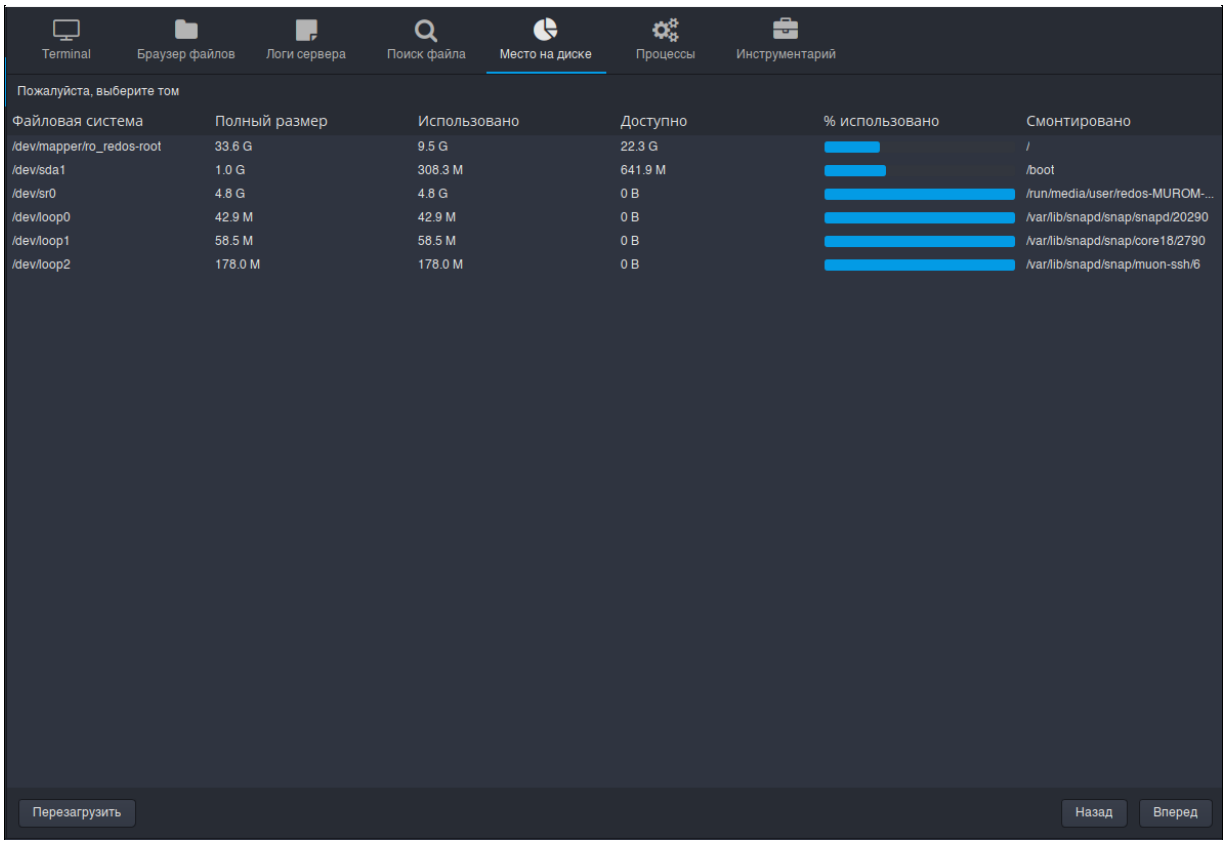


На вкладке «**Поиск файла**» доступен поиск файлов и каталогов с фильтрацией результатов поиска по различным критериям.

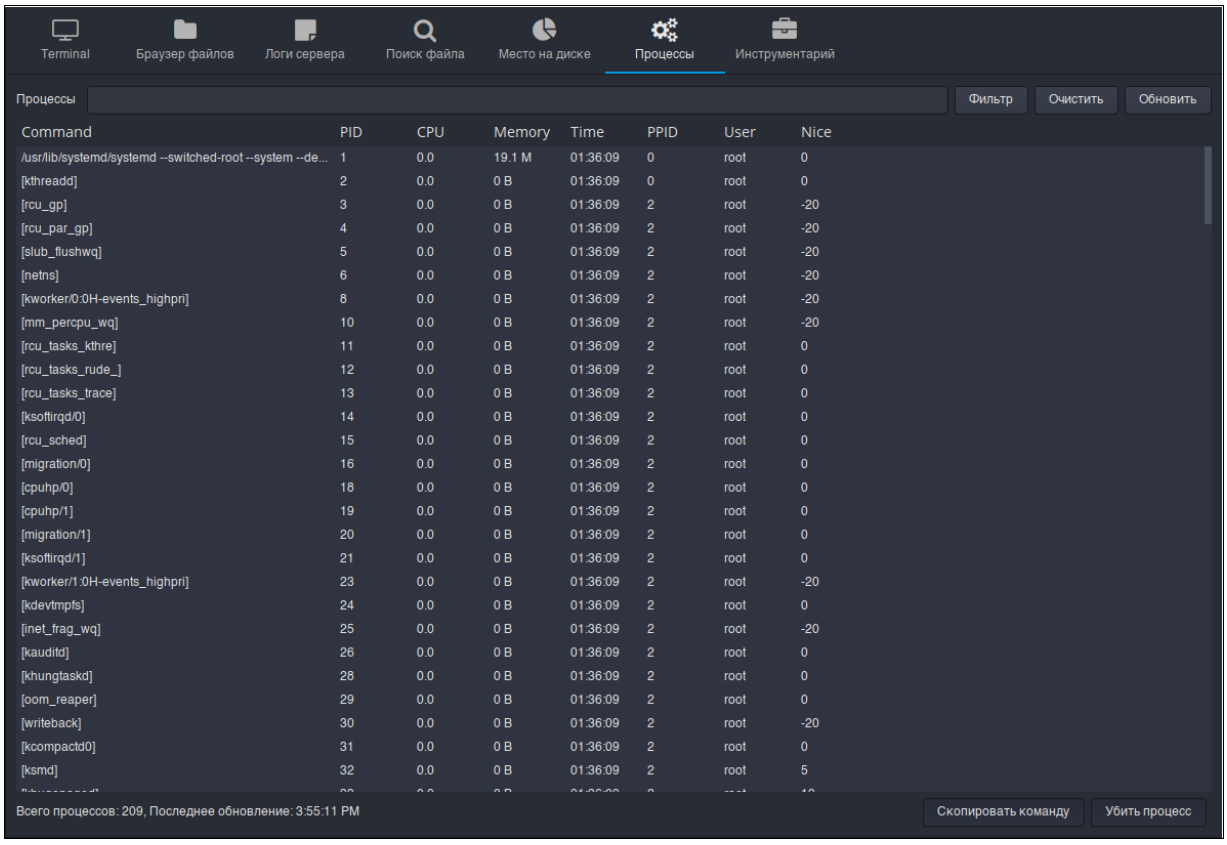


На вкладке «**Место на диске**» осуществляется оценка занятого дискового пространства. Доступен выбор анализа:

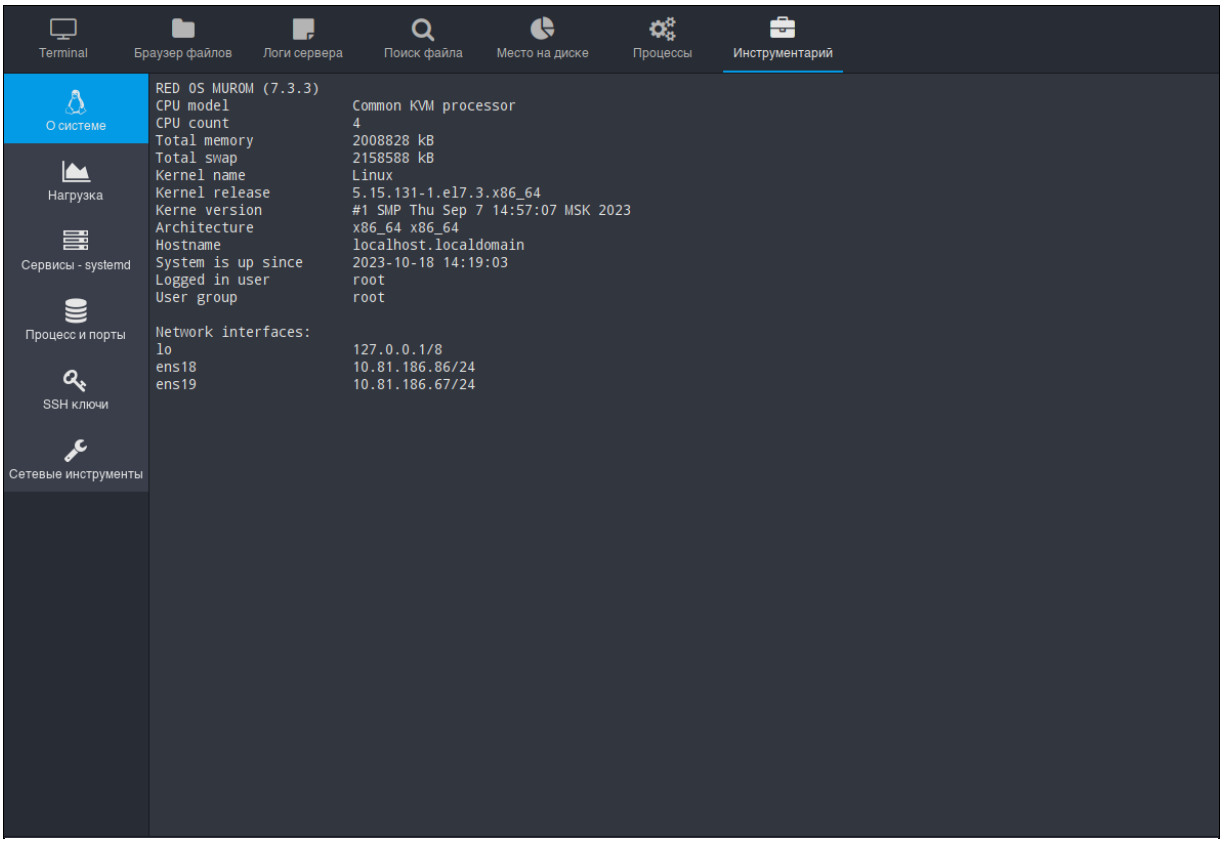
- анализировать том;
- анализировать папку.



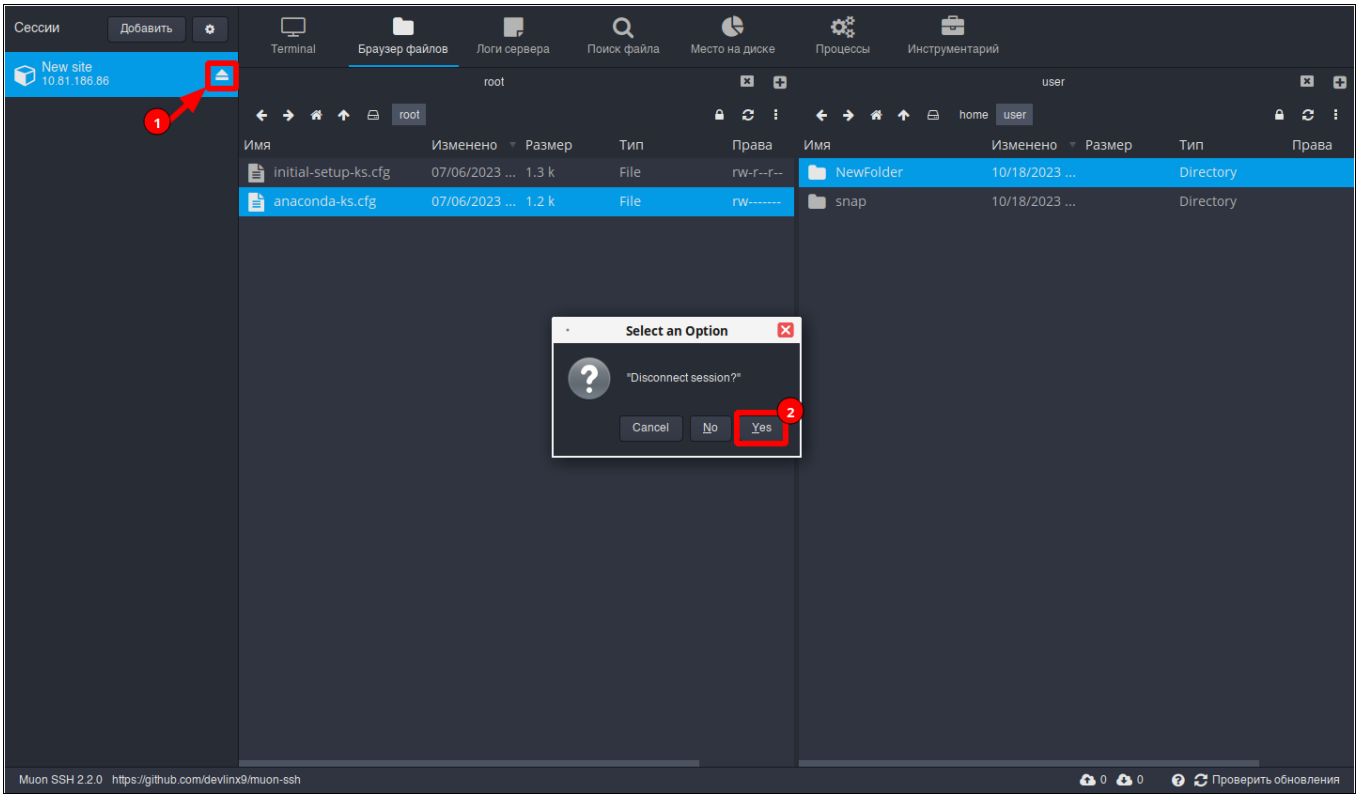
На вкладке «**Процессы**» отображается список запущенных на удаленном хосте процессов.



На вкладке «**Инструментарий**» выводится общая информация о хосте, системных службах, процессах и используемых ими портах, производится оценка нагрузки и пр.



Для отключения от сессии в списке установленных соединений нажмите кнопку  и в появившемся диалоге подтвердите завершение сессии.



Snowflake - графический SSH-клиент

Установка
Работа в программе
Возможности программы
Удаление программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: snowflake-1.0.4

Snowflake – современный SSH-клиент со встроенными графическими инструментами для простого управления серверами. **Snowflake** включает в себя менеджер соединений, файловый браузер, эмулятор терминала, диспетчер ресурсов/процессора, анализатор дискового пространства, текстовый редактор, просмотрщик журнала, поддержку аутентификации по ключу **SSH** и многие другие функции.

Просмотр файлов основан на протоколе **SFTP**, однако **Snowflake** может использовать консольные команды для эффективного выполнения операций. Например, удаление каталога с большим количеством файлов и подкаталогов может занять некоторое время при использовании **SFTP**, но с помощью команды `rm` процесс удаления производится намного быстрее.

Также **Snowflake** может выполнять операции с повышенными привилегиями (**sudo**). Для вызова **sudo** не требуется переключение на терминал.

Перемещение файлов между серверами можно осуществлять простым перетаскиванием.

Установка

Скачайте установочный файл командой:

```
wget https://github.com/subhra74/snowflake/releases/download/v1.0.4/snowflake-1.0.4-setup-amd64.bin
```

Затем предоставьте установочному файлу права на исполнение (потребуются права **администратора**):

```
sudo -E chmod +x ./snowflake-1.0.4-setup-amd64.bin
```

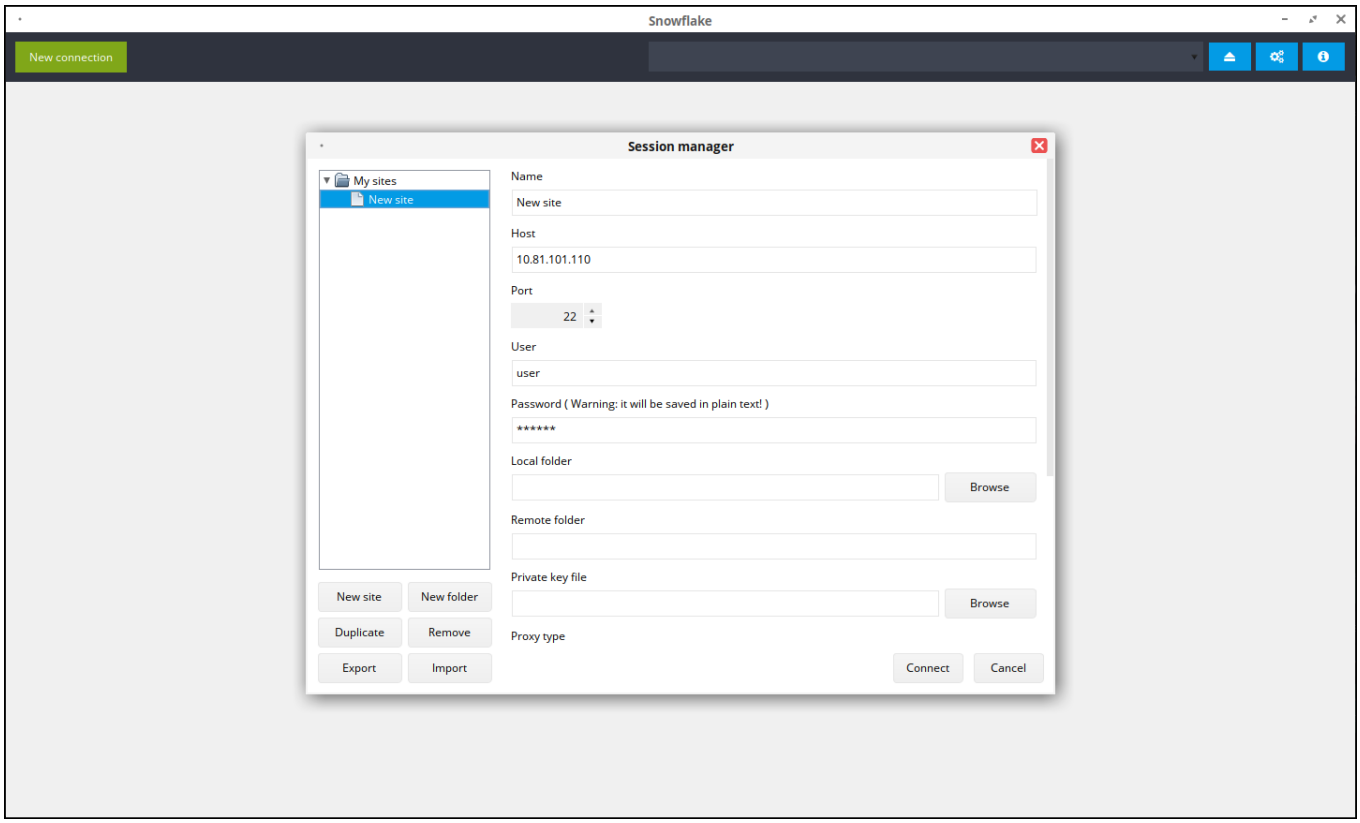
Запустите установку (потребуются права **администратора**):

```
sudo -E ./snowflake-1.0.4-setup-amd64.bin
```

После установки программа доступна из «**Главного меню**» – «**Прочие**» – «**Snowflake SSH Client**».

Работа в программе

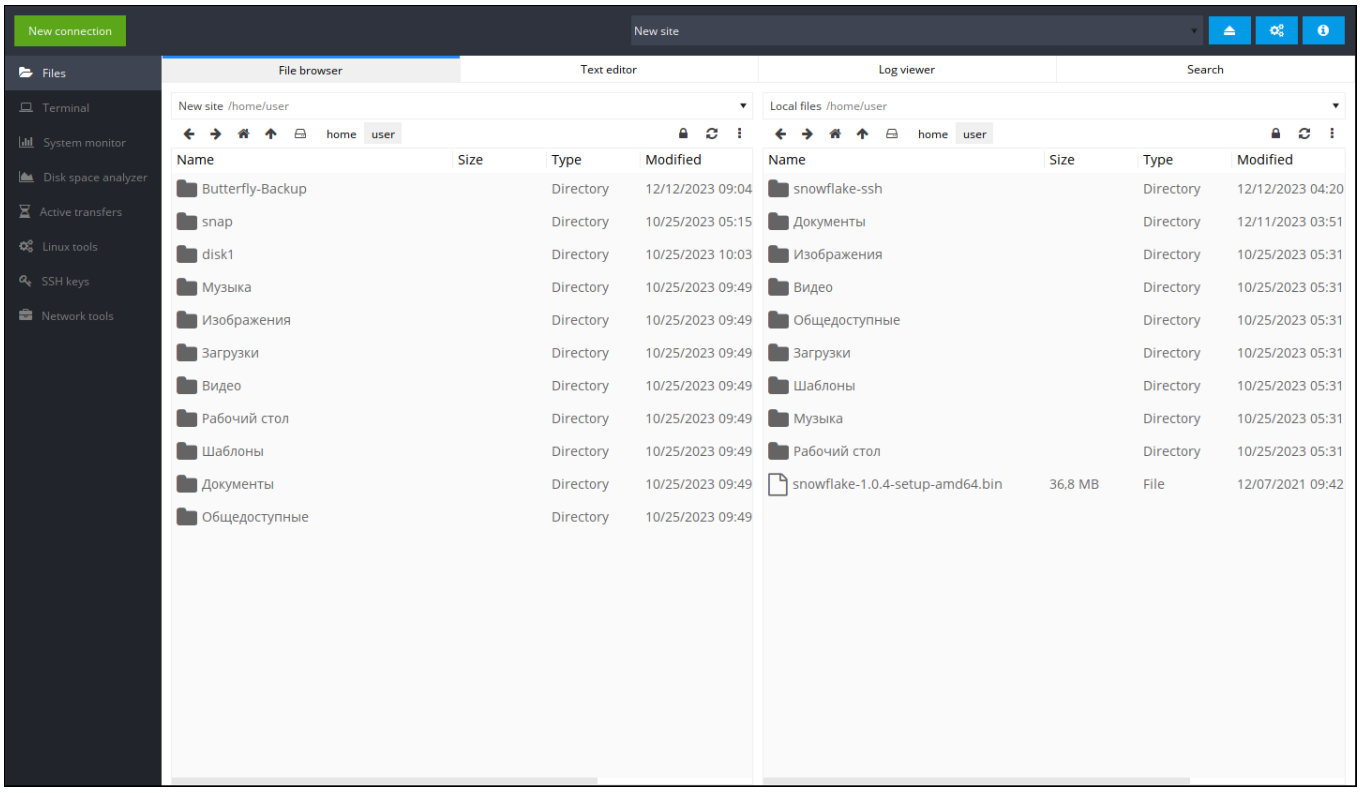
Для создания нового соединения нажмите «**New connection**». В открывшемся окне заполните данные удаленного сервера – IP-адрес, порт (по умолчанию 22), имя пользователя и пароль.



Для соединения с удаленным сервером нажмите «**Connect**».

После успешного соединения будет открыт файловый менеджер для удаленного сервера – слева, для локального – справа.

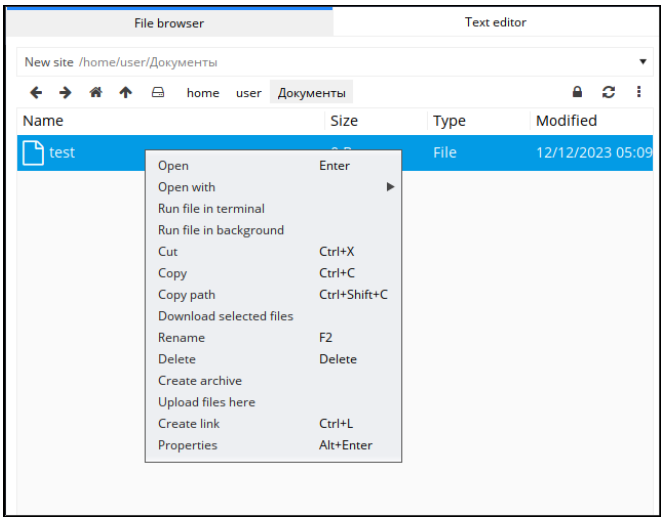
Интерфейс программы после установленного соединения выглядит следующим образом:



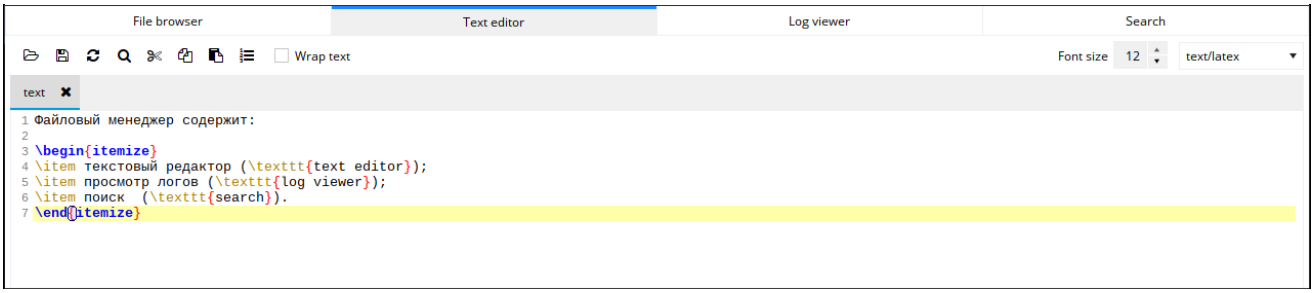
Файловый менеджер содержит текстовый редактор (*text editor*), просмотр логов (*log viewer*) и поиск (*search*).

Возможности программы

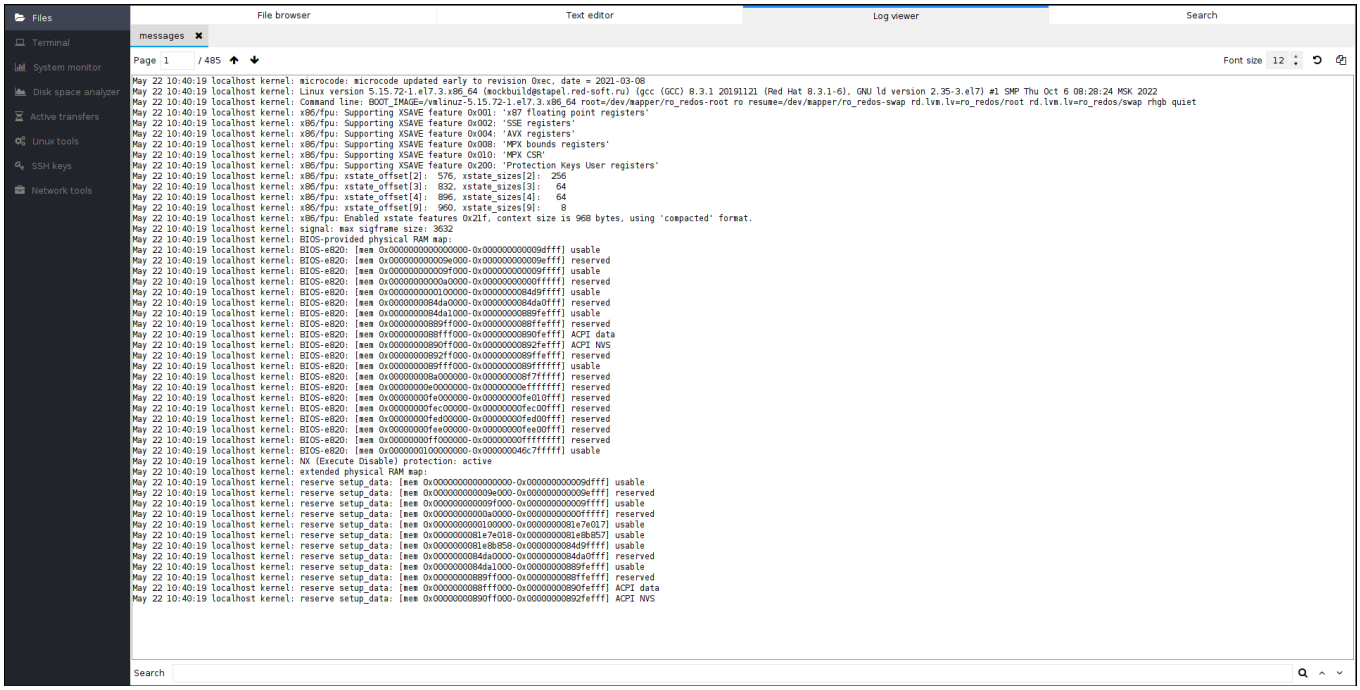
По нажатии ПКМ по какому-либо файлу вызывается контекстное меню для выбора действия – открыть, запустить в терминале, вырезать, скопировать, вставить, переименовать, удалить и пр.



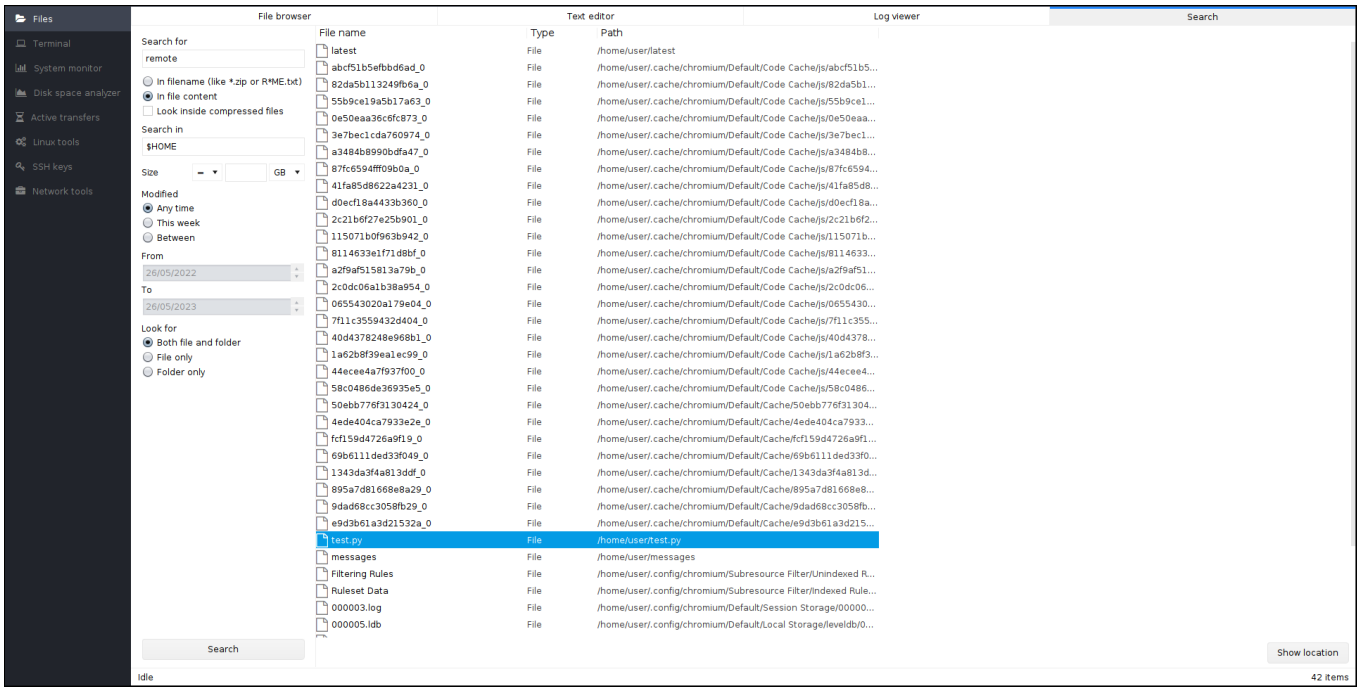
Текстовый редактор поддерживает подсветку синтаксиса, изменение размера шрифта текста, а также выбор среды программирования.



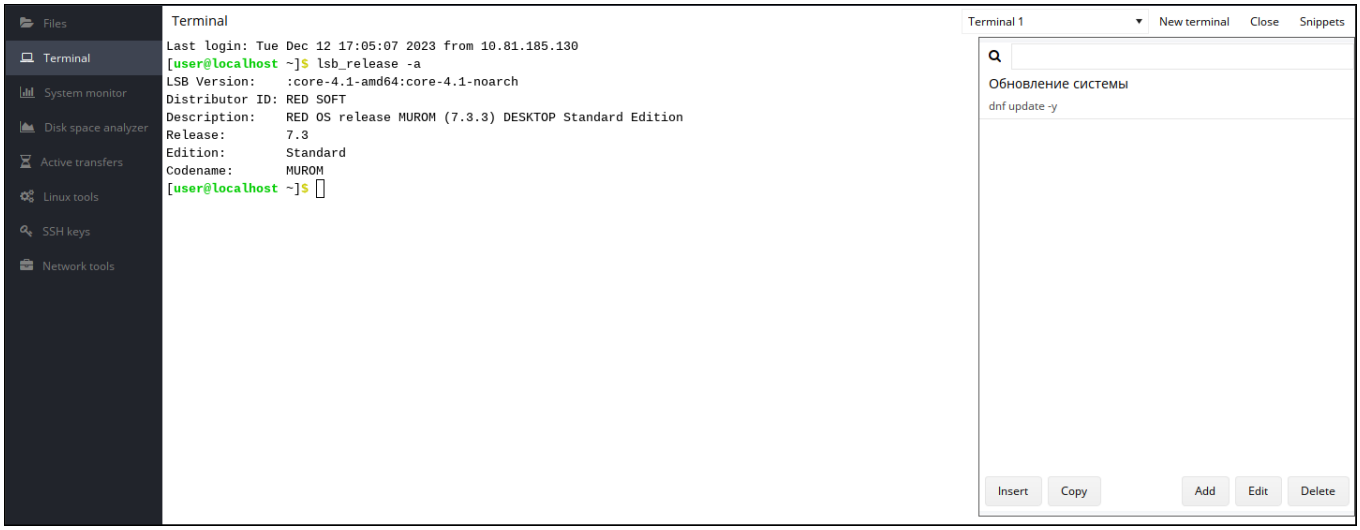
Просмотр системных журналов или больших текстовых файлов осуществляется через встроенный просмотрщик – **jiffy**.



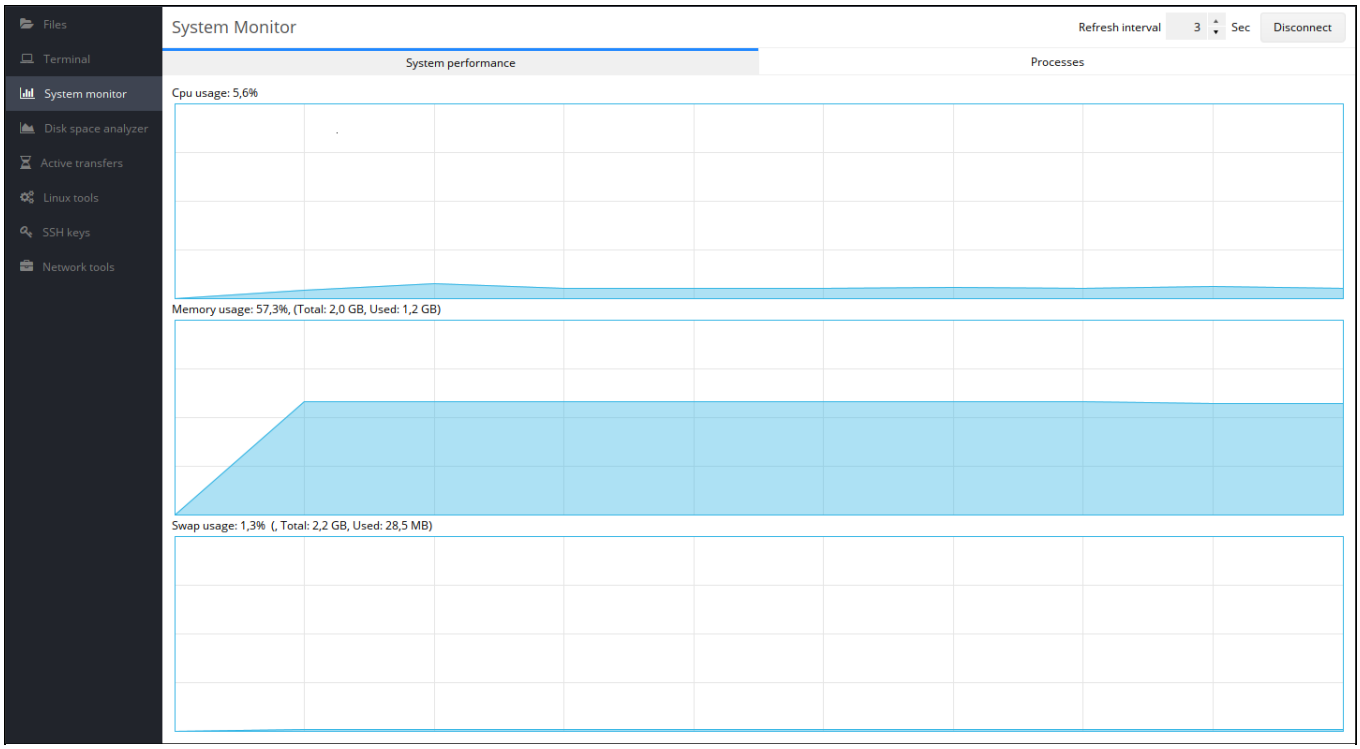
Быстрый поиск файлов основан на консольной команде find, поиск может также осуществляться в архивах **tar** и **zip**.



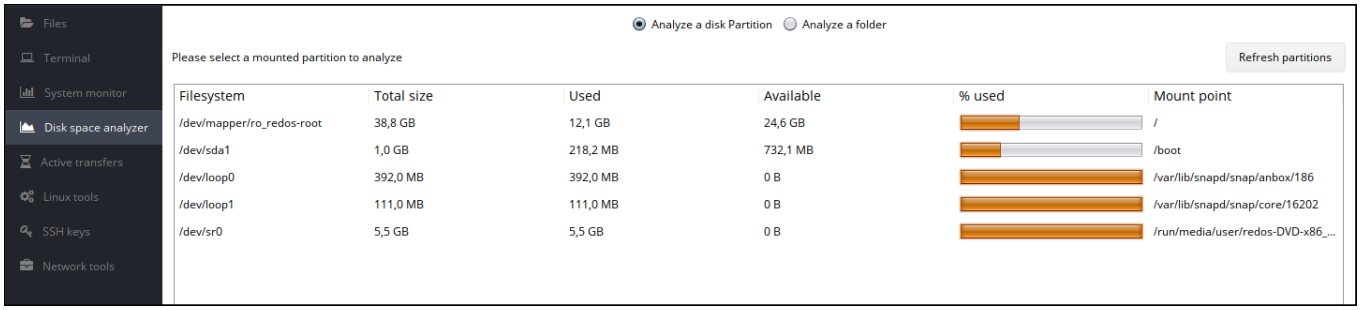
Во встроенном терминале поддерживаются *сниппеты*, с помощью которых можно сохранить часто используемые команды.



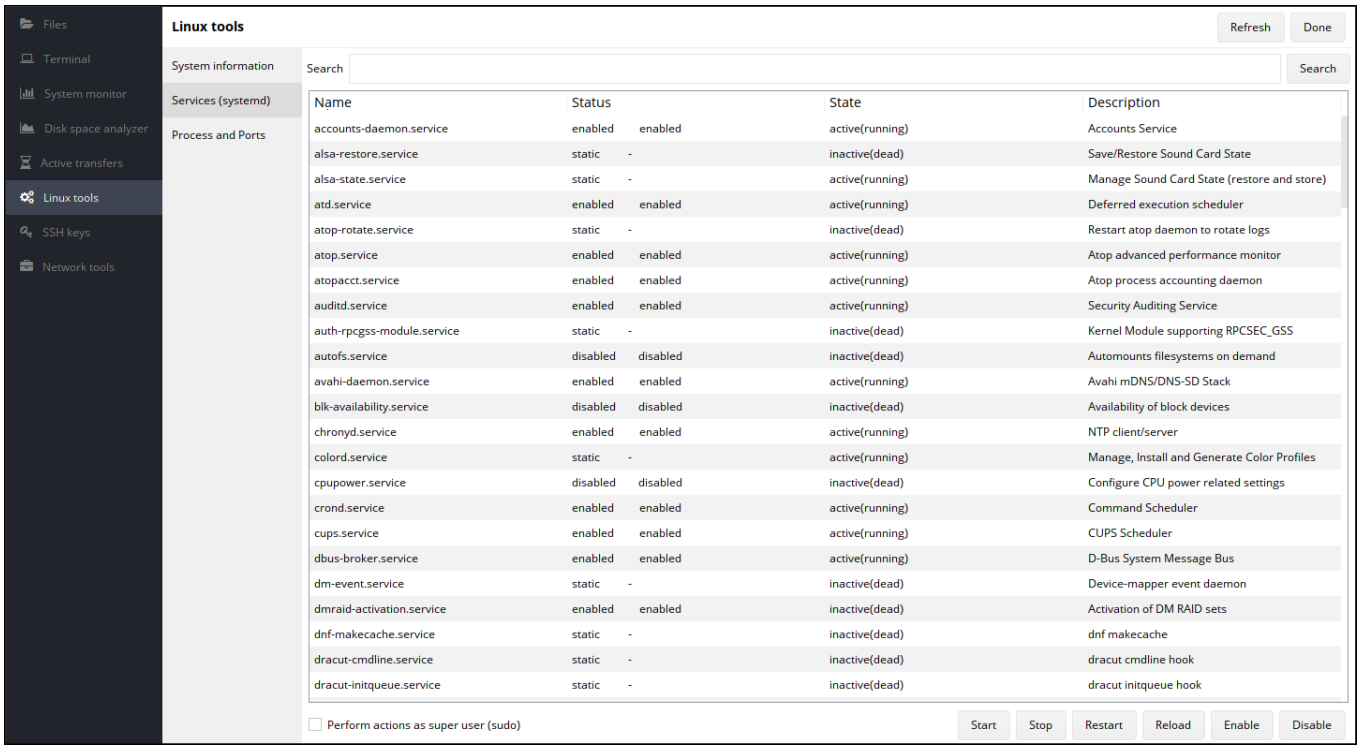
Доступен также системный монитор (аналог диспетчера задач), в котором нагрузка на процессор и использование памяти отображены в виде графика. Нагрузку по отдельным процессам можно просмотреть на вкладке **Processes**.



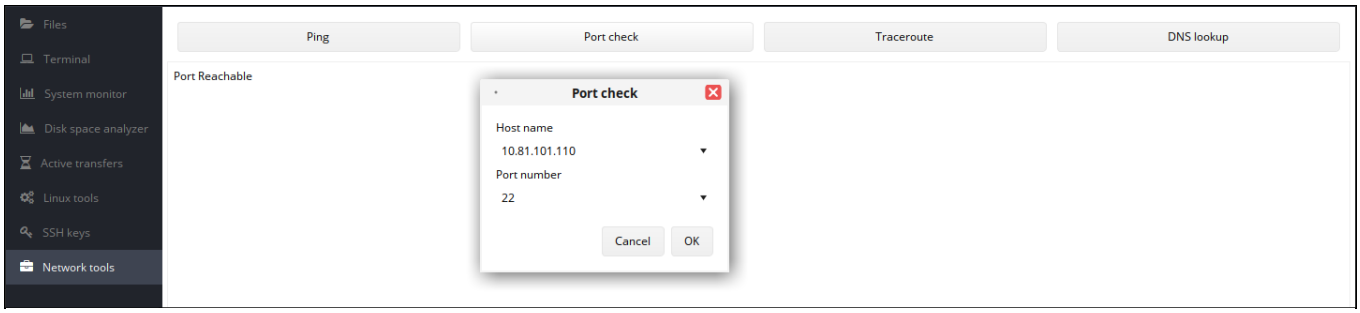
Встроенный графический анализатор места на диске показывает занятое и свободное дисковое пространство.



В разделе **Linux tools** можно получить информацию о системе, доступ к работе со службами **systemd**, а также проверить, какие порты используются процессами.



В сетевых настройках можно проверить целостность соединения с удаленным сервером, доступность портов удаленного сервера, определить сетевые маршруты, а также DNS-записи хостов.



В разделе **SSH keys** доступно управление ключами **SSH**.

Удаление программы

Для удаления **Snowflake** необходимо последовательно выполнить следующие команды (потребуются права суперпользователя **root** или **администратора** системы):

```
sudo rm -rf /opt/snowflake
sudo rm -rf /usr/bin/snowflake
sudo rm -rf /usr/share/applications/snowflake.desktop
rm -rf ~/snowflake-ssh
```

Создание SSH-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический, Сервер минимальный

Для включения поддержки шифрования ГОСТ в **openssl** необходимо установить пакеты **openssl-gost-engine** и **crypto-policies**.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install openssl-gost-engine crypto-policies
```

Более подробная информация о настройке ГОСТ в **openssl** доступна по ссылке .

Для установки пакетов **openssh-gost** необходимо выполнить следующие действия:

```
dnf swap openssh openssh-gost --allowerasing
dnf swap openssh-clients openssh-gost-clients --allowerasing
dnf swap openssh-server openssh-gost-server --allowerasing
```

Включить поддержку алгоритмов ГОСТ в **openssl** можно командой:

```
openssl-switch-config gost
```

После этого перезапустите сервис **sshd**:

```
systemctl restart sshd
```

Список поддерживаемых алгоритмов шифрования трафика можно посмотреть с помощью команды:

```
ssh -Q cipher

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
grasshopper-cbc@altlinux.org
grasshopper-ctr@altlinux.org
magma-cbc@altlinux.org
magma-ctr@altlinux.org
```

Для просмотра списка поддерживаемых **MAC** (коды аутентификации сообщений) выполните команду:

```
ssh -Q mac

hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
hmac-md5
hmac-md5-96
umac-64@openssh.com
umac-128@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
```

```
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
grasshopper-mac@altlinux.org
hmac-gostr3411-2012-256@altlinux.org
hmac-streebog-256@altlinux.org
hmac-gostr3411-2012-512@altlinux.org
hmac-streebog-512@altlinux.org
hmac-gostr3411-2012-256-etm@altlinux.org
hmac-streebog-256-etm@altlinux.org
hmac-gostr3411-2012-512-etm@altlinux.org
hmac-streebog-512-etm@altlinux.org
```

На клиенте для настройки также необходимо выполнить вышеуказанные действия.

Для подключения к серверу с использованием алгоритмов ГОСТ выполните команду:

```
ssh <пользователь>@<сервер> -oCiphers=grasshopper-ctr@altlinux.org -oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org
```

Пример подключения:

```
ssh user@192.168.1.92 -oCiphers=grasshopper-ctr@altlinux.org -oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org

The authenticity of host '192.168.1.92 (192.168.1.92)' can't be established.
ED25519 key fingerprint is SHA256:qUo//tqZCHfpp3QY9qEBqIxXcjT/8va13xGeREclvU8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.92' (ED25519) to the list of known hosts.
user@192.168.1.92's password: <пароль_сервера>
Last login: Thu Apr 21 09:47:30 2022
```

Для выхода из сессии выполните команду:

```
exit

выход
Connection to 192.168.1.92 closed.
```

Аутентификация по протоколу SSH с использованием RSA-ключа

Клиент SSH. Генерация RSA-ключа
Клиент SSH. Передача открытой части ключа на сервер
Клиент SSH. Установка ранее сгенерированного ключа
Сервер SSH. Отключение аутентификации по паролю

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openssh-9.3p1-5

Установка и настройка утилиты openssh подробно описаны нашей статье «Работа с клиентом и сервером SSH».

Использование ключа при аутентификации позволяет не только отказаться от обязательного ввода пароля при установке соединения, но и повысить защищенность соединения, автоматизировать процессы. Такие утилиты и протоколы как **scp**, **rsync**, **sftp**, которые при аутентификации ранее требовали ввода пароля, используя ключ, могут функционировать без участия пользователя.

Ключ состоит из двух частей – публичной и приватной. *Публичная часть* ключа может распространятся по открытым каналам без угрозы для безопасности соединения. *Приватная часть* должна быть защищена от несанкционированного доступа. В случае передачи приватной части ключа по незащищенным каналам или возможности несанкционированного доступа предусмотрена возможность парольной защиты ключа.

Общий принцип аутентификации с использованием ключа заключается в том, что при инициализации клиентом сеанса связи сервер шифрует открытой частью ключа случайное число и передает его клиенту. Если клиент обладает приватной частью, он сможет его расшифровать и, передав ответ обратно на сервер, подтвердить свою подлинность.

Клиент SSH. Генерация RSA-ключа

Для создания подключения с использованием ключа на стороне клиента (устройство, которое инициирует подключение) генерируется SSH-ключ, включающий в себя два файла – *приватную* и *публичную* части. *Публичная часть* ключа будет передана на сервер (устройство, с которым устанавливается связь).

Сгенерируйте ключ утилитой **ssh-keygen**:

```
ssh-keygen
```

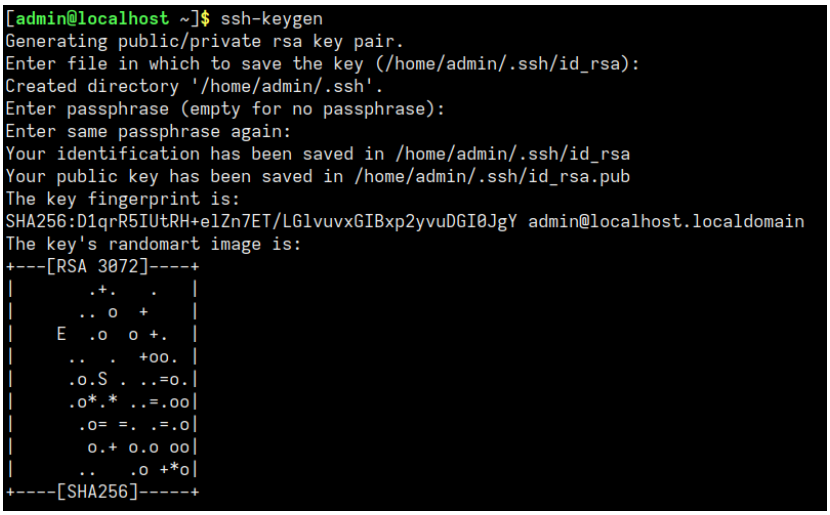
Утилита информирует о каталоге размещения сгенерированных ключей. Каталог можно изменить, указав другой путь (не рекомендуется):

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
```

Далее будет предложено установить пароль на ключ для защиты от несанкционированного доступа третьих лиц. Опция не является обязательной. Если оставить поле пустым, пароль не будет установлен:

```
Created directory '/home/admin/.ssh'.
Enter passphrase (empty for no passphrase):
```

После этого происходит генерация ключей. По завершении процесса генерации будут указаны каталоги хранения **id_rsa** (приватная часть ключа) и **id_rsa.pub** (публичная часть ключа).



Ключи успешно сгенерированы.

Клиент SSH. Передача открытой части ключа на сервер

ВАЖНО!

Обратите внимание, что при передаче ключа используется имя уже созданного на сервере пользователя. Если такого пользователя на сервере нет, его необходимо создать **до** передачи ключа. Также на сервере должна быть доступна аутентификация с применением пароля.

Открытую часть ключа передайте на сервер при помощи утилиты **ssh-copy-id** в формате вида:

```
ssh-copy-id -i <путь_до_ключа> <имя_пользователя>@<IP-адрес_сервера>
```

Например:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@192.168.100.61
```

При первом подключении к серверу будет предложено проверить отпечаток ключа ***fingerprint***. Для подтверждения наберите **yes**. Отпечаток ключа будет сохранен в файл **~/.ssh/known_hosts**.

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.100.61 (192.168.100.61)' can't be established.
ED25519 key fingerprint is SHA256:q3oeMFb4bpE4SMd39cH5QqShw3yFmMXi4Wh5VfS260g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Далее будет предложено ввести пароль пользователя, от имени которого производится подключение к серверу:

```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keysuser@192.168.100.61's
password: <пароль_пользователя>
```

После этого будет выведена информация о результатах передачи ключа:

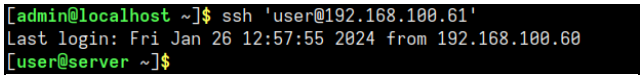
```
Number of key(s) added: 1
Now try logging into the machine, with:   "ssh 'user@192.168.100.61'"
and check to make sure that only the key(s) you wanted were added.
```

Выполните проверку подключения к серверу с помощью команды вида:

```
ssh <имя_пользователя>@<IP-адрес_сервера>
```

Например:

```
ssh user@192.168.100.61
```



Обратите внимание на *имя пользователя* и *имя хоста* в командной строке. Если параметры изменились и соответствуют параметрам подключения, аутентификация прошла удачно.

Настройка подключения завершена.

ВАЖНО!

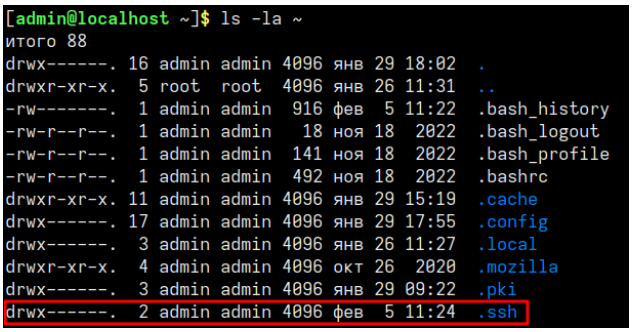
Обратите внимание, что настройка аутентификации с применением RSA-ключа не отключает возможность аутентификации по паролю. По умолчанию аутентификация с применением RSA-ключа имеет более высокий приоритет. В случае утраты ключа или несоответствия параметров, при подключении будет предложено пройти аутентификацию с использованием пароля.

Если аутентификацию с использованием пароля требуется отключить, необходимо изменить конфигурацию на стороне сервера. Подробнее об отключении аутентификации с использованием пароля см. в пункте «Сервер SSH. Отключение аутентификации по паролю».

Клиент SSH. Установка ранее сгенерированного ключа

При установке ранее сгенерированного ключа необходимо убедиться в наличии каталога **/.ssh** в домашнем каталоге и правах доступа к этому каталогу. Для этого выполните:

```
ls -la ~
```



ВАЖНО!

Обратите внимание на права доступа `drwx------` к каталогу **/.ssh**. В случае предоставления прав доступа группе или другим пользователям при попытке подключения к серверу в авторизации будет отказано.

Если каталога **/.ssh** не существует, его необходимо создать:

```
mkdir ~/.ssh
```

и предоставить необходимые права:

```
chmod 700 ~/.ssh
```

После этого полученный ключ необходимо разместить в каталоге **/.ssh**.

Сервер SSH. Отключение аутентификации по паролю

Для отключения аутентификации по паролю на сервере необходимо внести изменения в файл конфигурации SSH-сервера – **/etc/ssh/sshd_config**. Откройте файл конфигурации (потребуются права **администратора**):

```
sudo nano /etc/ssh/sshd_config
```

Найдите и раскомментируйте параметр `PasswordAuthentication`. Установите для него значение `no`.

Сохраните изменения и закройте файл.

Для применения внесенных изменений обновите конфигурацию службы командой:

```
sudo systemctl reload sshd.service
```

Аутентификация по паролю отключена.

Установка и настройка xrdp-сервера в РЕД ОС 7.3

Установка и настройка xrdp-сервера
Включение возможности запуска нового сеанса пользователя и устранение ошибки «Could not acquire name on session bus»

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pulseaudio-module-xrdp-0.7-1, xorgxrdp-0.10.2-1, xrdp-1:0.10.1-1

Вы можете подробнее ознакомиться с возможностью осуществления удаленного подключения, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и настройка xrdp-сервера

Перед установкой и настройкой сервера необходимо предварительно перейти в сеанс пользователя **root**:

```
su -
```

Дальнейшие указанные действия должны выполняться с правами пользователя **root** или **администратора** системы, если не указано иное.

1. Установите сервер **xrdp** командой:

```
dnf install xrdp xorgxrdp pulseaudio-module-xrdp
```

2. Настройте предпочитаемую графическую оболочку по умолчанию:

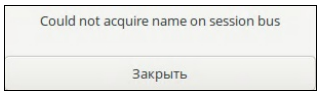
```
sed -i '/PREFERRED=/d' /etc/sysconfig/desktop 2>/dev/null; echo 'PREFERRED="$(type -p mate-session)"' >> /etc/sysconfig/desktop
```

3. Запустите сервер **xrdp** и добавьте его в автозагрузку:

```
systemctl enable xrdp --now
```

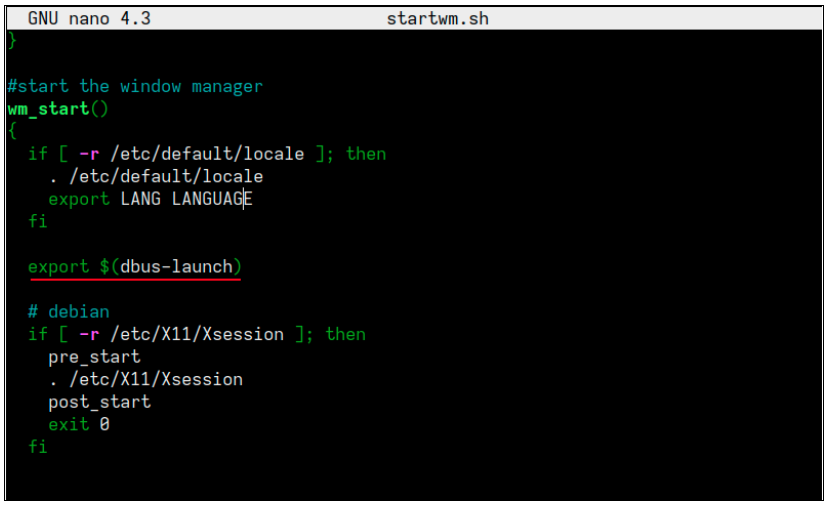
Включение возможности запуска нового сеанса пользователя и устранение ошибки «Could not acquire name on session bus»

После авторизации пользователя при удаленном подключении к xrdp-серверу возникает ошибка **"Could not acquire name on session bus"**.



Для устранения данной ошибки в скрипте **/usr/libexec/xrdp/startwm.sh** в функции **wm_start** добавьте строку:

```
export $(dbus-launch)
```



после сохранения изменений перезапустите сервис **xrdp** командой в терминале:

```
systemctl restart xrdp
```

Дополнительная настройка xrdp-сервера

Проброс локального диска и принтера при подключении из Windows
Подключение на клиенте
Устранение ошибки при настройке удаленного доступа с Windows 7/XP на РЕД ОС
Аутентификация под доменным пользователем
Дополнительная настройка SELinux
Завершение всех процессов при выходе из сеанса
Оптимизация производительности
Автоматическое завершение сеанса пользователя, подключенного по xrdp
Автоматическое завершение всех графических сеансов пользователя

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с возможностью осуществления удаленного подключения **на примере РЕД ОС 7.3**, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows;
- в **VK Видео** — Организация удаленного доступа с РЕД ОС на Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Проброс локального диска и принтера при подключении из Windows

Для успешного подключения локального диска к удаленному рабочему столу необходимо убрать в настройках RDP-клиента галочку «**Принтеры**».

Проброс локального принтера текущей версией xrdp не поддерживается.

Подключение на клиенте

Для подключения из Windows используйте «**Подключение к удаленному рабочему столу**».

Для подключения из РЕД ОС используйте приложение «**Remmina**» («Главное меню» — «Интернет» — «Remmina»).

Выберите протокол **RDP**, впишите узел и нажмите клавишу **Enter**, чтобы подключиться.

Для подключения в открывшемся окне впишите имя пользователя и пароль.

Для применения настроек перезагрузите сервер **xrdp**:

```
systemctl restart xrdp
```

Устранение ошибки при настройке удаленного доступа с Windows 7/XP на РЕД ОС

При возникновении ошибки такого вида:



Откройте файл:

```
nano /etc/xrdp/xrdp.ini
```

Измените значение параметра *security_layer*:

```
security_layer=rdp
```

Для применения настроек перезагрузите сервер **xrdp**:

```
systemctl restart xrdp
```

Аутентификация под доменным пользователем

Для разрешения аутентификации доменных пользователей требуется изменить файл:

```
nano /etc/xrdp/sesman.ini
```

Закомментировав следующие строки:

```
#TerminalServerUsers=tsusers
#TerminalServerAdmins=tsadmins
```

Перезапустите сервер:

```
systemctl restart xrdp
```

Чтобы разрешить определенным доменным пользователям доступ к RDP-серверу, необходимо создать локальную в группу **tsusers** и добавить в нее доменных пользователей.

```
groupadd tsusers
```

Добавить в группу **tsusers** доменного пользователя:

```
usermod -aG tsusers bob
```

где **bob** - это доменный пользователь,

В файл **/etc/xrdp/sesman.ini** в секцию [Security] необходимо добавить строки:

```
TerminalServerUsers=tsusers
AlwaysGroupCheck=true
```

Еще один вариант - в качестве локальной группы указать доменную:

```
TerminalServerUsers=rdp
```

здесь **rdp** - группа безопасности на вашем контроллере домена, в которую могут входить необходимые вам пользователи **xrdp**-сервера.

После этого перезапустите сервер:

```
systemctl restart xrdp
systemctl restart sssd
```

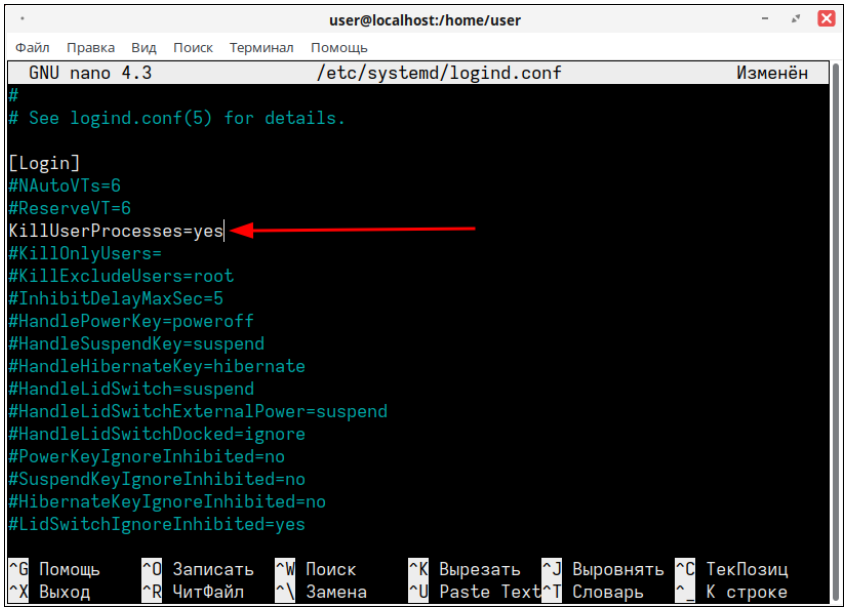
Дополнительная настройка SELinux

После тестового подключения к xrdp-серверу нужно выполнить настройку SELinux, выполните следующие команды на сервере:

```
ausearch -c 'krb5_child' --raw | audit2allow -M my-krb5child
semodule -X 300 -i my-krb5child.pp
```

Завершение всех процессов при выходе из сеанса

Для того чтобы при выходе из системы прекращались все процессы, явно или неявно запущенные от имени авторизованного пользователя, в файле **/etc/systemd/logind.conf** необходимо раскомментировать параметр KillUserProcesses и установить значение yes.



После изменения значения данного параметра необходимо либо перезагрузить компьютер, либо выполнить команду перезапуска сервиса **logind** для применения настроек:

```
systemctl restart systemd-logind
```

Оптимизация производительности

Оптимизацию использования ресурсов RDP-сервера (процессора, оперативной памяти, каналов связи) можно произвести представленными ниже изменениями конфигурации.

- при использовании **MATE**:

Для отключения композитного менеджера путем задания значения по умолчанию параметра dconf следует создать файл **/etc/dconf/db/local.d/10_mate_nocomp** со следующим содержимым (с правами пользователя **root**):

```
nano /etc/dconf/db/local.d/10_mate_nocomp
```

```
[org/mate/marco/general]
 compositing-manager=false
```

Для того чтобы ограничить возможность изменения данного параметра пользователем, то есть принудительно применить настройку, следует выполнить команду:

```
echo "/org/mate/marco/general/compositing-manager" > /etc/dconf/db/local.d/locks/10_mate_nocomp
```

- при использовании **CINNAMON**:

Для отключения композитного режима следует выполнить команду:

```
sed -i '/PREFERRED=/d' /etc/sysconfig/desktop 2>/dev/null; echo 'PREFERRED="$(type -p cinnamon-session-cinnamon2d)"' >>
/etc/sysconfig/desktop
```

Автоматическое завершение сеанса пользователя, подключенного по xrdp

Данный вариант подойдет для решения ситуаций, когда после удаленного входа пользователь не может войти в сеанс на локальном компьютере.

Для автоматического завершения xrdp-подключения с завершением графического сеанса пользователя в файле **/etc/xrdp/sesman.ini** раскомментируйте и укажите параметры:

```
KillDisconnected=true
DisconnectedTimeLimit=60
IdleTimeLimit=600
```

В этом примере конфигурационного файла RDP-соединение отключится через 10 минут (600 секунд) неактивности, с завершением сеанса пользователя через 60 секунд после отключения.

KillDisconnected - [true|false] Включение функции принудительного завершения сеанса пользователя, после отключения RDP. Данная настройка работает только для xorgxrdp-сессий.

DisconnectedTimeLimit - Время в секундах, через которое будет завершен сеанс пользователя, после отключения RDP-соединения. Минимальное значение 60. При указании меньшего, значение будет равно 60.

IdleTimeLimit - Время в секундах, через которое будет будет отключено неактивное RDP-соединение. Под неактивностью понимается отсутствие ввода с клавиатуры, отсутствие движения/нажатий мыши. Если указано 0 - неактивное соединение не отключается. Данная настройка работает только для xorgxrdp сессий.

Автоматическое завершение всех графических сеансов пользователя

Данный вариант завершает все графические сеансы пользователей, которые неактивны указанное время. Решает проблему, когда незавершенный сеанс на локальном компьютере не позволяет подключиться этому пользователю по xrdp удаленно.

Создайте скрипт:

```
nano /opt/logout.sh
```

Сделайте его исполняемым:

```
chmod +x /opt/logout.sh
```

Содержание скрипта:

```
#!/bin/bash
idle_time=30 # Время в минутах бездействия в сессии пользователя, после которого сессия будет завершена (Указать необходимое)
while true; do
# Время бездействия пользователя в миллисекундах
user_time=$(xprintidle)
if [ $user_time -ge $((idle_time*60*1000)) ]; then
# Завершаем сеанс пользователя
loginctl kill-user "$USER"
fi
sleep 1
done
```

Создайте файл автозапуска скрипта **/opt/logout.sh**:

```
nano /etc/xdg/autostart/logout.desktop
```

Содержание файла **/etc/xdg/autostart/logout.desktop**:

```
[Desktop Entry]
Type=Application
Exec=/opt/logout.sh
Hidden=false
Name=MyLogout
```

Установка и настройка TigerVNC

Установка
Предварительная настройка
Настройка файла конфигурации
Подключение к серверу tigerVNC

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Графический сервер
- **Версия ПО**: tigervnc-server-1.13.1

TigerVNC-сервер – это программный пакет, который позволяет запускать сервер **XVNC**, а также параллельные сеансы различных окружений рабочего стола, таких как **MATE**, **GNOME** и т. д. по протоколу **VNC**.

Вы можете подробнее ознакомиться с установкой и настройкой **Tigervnc** для удаленного подключения, просмотрев наши обучающие видео:

- на **RuTube**:
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.
- в **Яндекс.Дзен:**
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.
- в **VK Видео:**
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки сервера **tigervnc** перейдите в сеанс суперпользователя **root**:

```
su -
```

и выполните команду:

```
dnf install tigervnc-server
```

Предварительная настройка

Примечание.

Для подключения к серверу через **VNC** *не рекомендуется* использовать учетную запись суперпользователя **root**, поскольку это *небезопасно*. Кроме того, некоторые функции могут работать некорректно.

Создайте обычного пользователя для подключения к серверу **VNC** и задайте для него пароль, добавьте пользователя в группу **wheel** для назначения ему привилегий администратора (**sudo**):

```
adduser <имя_пользователя>
passwd <имя_пользователя>
usermod -aG wheel <имя_пользователя>
```

Для подключения также можно использовать существующего пользователя, имеющего права администратора.

Настройка файла конфигурации

Далее необходимо назначить для каждого пользователя индивидуальный порт для подключения. Для этого откройте файл конфигурации **vncserver.users**:

```
nano /etc/tigervnc/vncserver.users
```

В конец файла добавьте строку вида:

```
:<номер_рабочего_стола>=<имя_пользователя>
```

Например:

```
# TigerVNC User assignment
#
# This file assigns users to specific VNC display numbers.
# The syntax is =. E.g.:
#
# :2=andrew
# :3=lisa

:2=test_user
```

здесь:

- :2 – номер рабочего стола для подключения. По умолчанию каждый рабочий стол отображается на порте **5900** + **номер рабочего стола**. То есть рабочий стол **:2** будет доступен через порт **5902**. Порт для каждого пользователя должен быть уникальным;
- test_user – имя пользователя с правами администратора для подключения к серверу **VNC**.

Затем откройте файл конфигурации по умолчанию:

```
nano /etc/tigervnc/vncserver-config-defaults
```

И укажите используемую по умолчанию графическую оболочку для подключения к серверу **VNC**. Например:

```
session=mate
```

Также установить графическую оболочку по умолчанию для пользователя, под которым будет производиться подключение к серверу, можно, указав имя сессии в файле в домашней директории этого пользователя **~/.vnc/config**. Например:

```
nano /home/test_user/.vnc/config
```

```
session=mate
```

Перейдите в сеанс пользователя, под которым будет производиться подключение к серверу **VNC**:

```
su - <имя_пользователя>
```

Установите пароль для пользователя сервера **TigerVNC**:

```
vncpasswd
```

Обратите внимание, что пароль должен иметь длину **не менее 6 символов**.

> **Примечание.**
>
> При запросе установки пароля только для просмотра нажмите **n**. При нажатии **y** управление сервером будет заблокировано.

Запустите службу **vncserver** и добавьте ее в автозагрузку:

```
systemctl enable --now vncserver@:2
```

здесь:

- `:2` – номер порта для подключения к серверу пользователя **test_user**, для каждого пользователя номер порта уникален.

Подключение к серверу tigerVNC

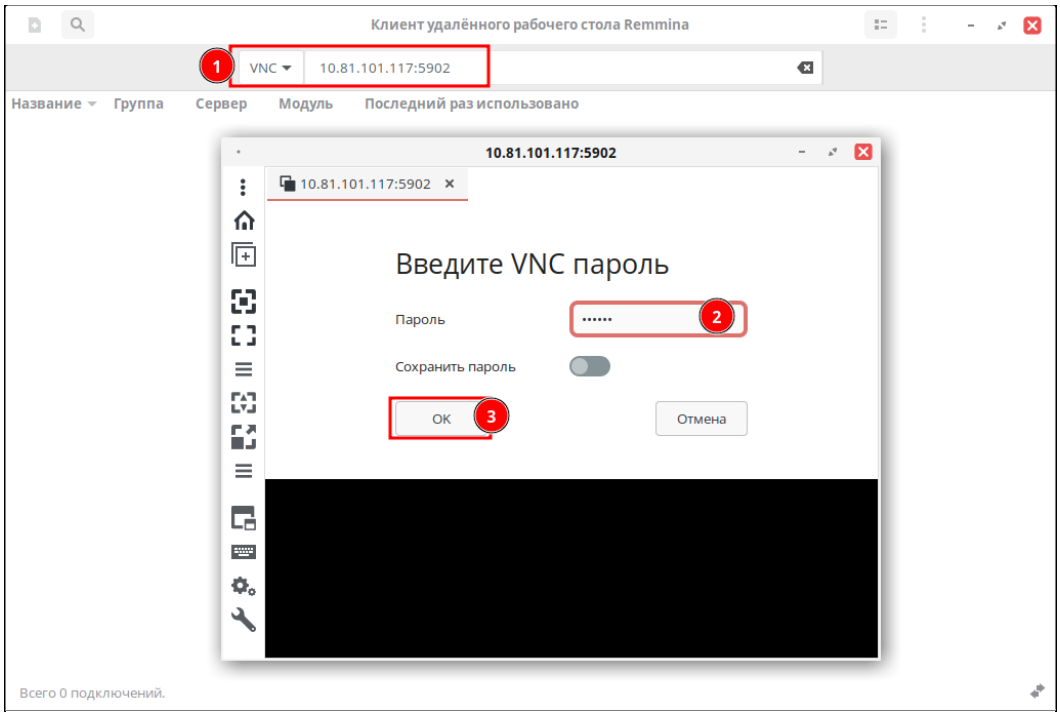
Для подключения можно использовать любое клиентское приложение **VNC**, например, **Remmina** Выберите протокол подключения – **VNC**, введите общедоступный *IP-адрес сервера* и *номер порта*, по которому будет производиться подключение (в примере используется порт **5902** для пользователя **test_user**).

ВАЖНО!

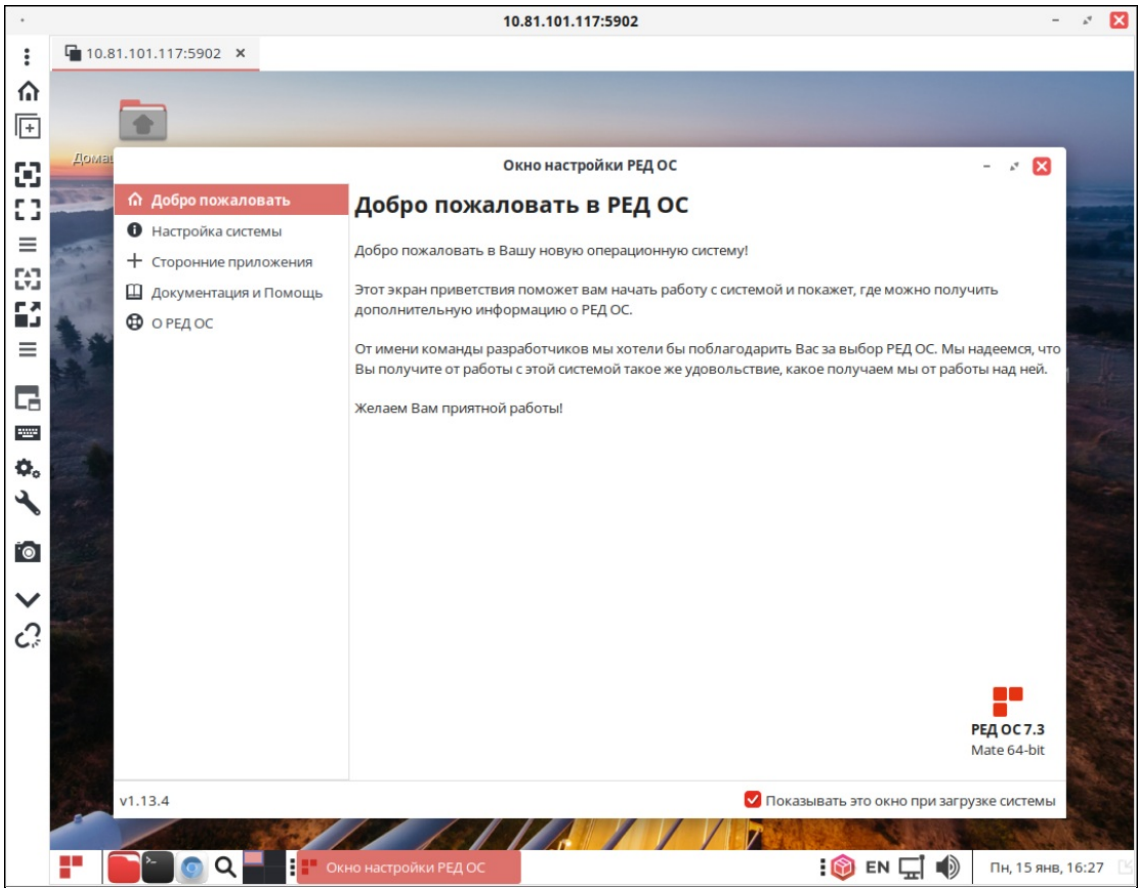
При вводе IP-адреса сервера важно правильно указать порт для подключения. В рассматриваемом примере запись будет выглядеть следующим образом:

```
10.81.101.117:5902
```

Введите пароль пользователя сервера **VNC**, который был создан ранее (см. пункт «Предварительная настройка»). После этого будет выполнено подключение к серверу и отображен удаленный рабочий стол.



Подключение к серверу прошло успешно.


10.81.101.117:5902
10.81.101.117:5902
Окно настройки РЕД ОС
Добро пожаловать
Настройка системы
Сторонние приложения
Документация и Помощь
О РЕД ОС
Добро пожаловать в РЕД ОС
Добро пожаловать в Вашу новую операционную систему!
Этот экран приветствия поможет вам начать работу с системой и покажет, где можно получить дополнительную информацию о РЕД ОС.
От имени команды разработчиков мы хотели бы поблагодарить Вас за выбор РЕД ОС. Мы надеемся, что Вы получите от работы с этой системой такое же удовольствие, какое получаем мы от работы над ней.
Желаем Вам приятной работы!
РЕД ОС 7.3
Mate 64-bit
v1.13.4
Показывать это окно при загрузке системы
Окно настройки РЕД ОС
EN
Пн, 15 янв, 16:27

Настройка X2GO

Установка x2go
Настройка клиента
Обзор клиента
Запуск определенного приложения
Проброс принтеров
Настройка трансляции токенов в сессию сервера
Завершение сессий x2go
X2Go Broker

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: x2goagent-4.1.0.3-14, x2goserver-4.1.0.3-14, x2goclient-4.1.2.2-4

X2Go — это программное обеспечение для удаленного рабочего стола с открытым исходным кодом, использующее модифицированный протокол **NX 3**. **X2Go** предоставляет удаленный доступ к графическому пользовательскому интерфейсу системы.

В данной статье раскрываются основные моменты по настройке данного варианта удаленного подключения, однако вы так же можете обратиться к официальной документации.

Вы можете подробнее ознакомиться с организацией удаленного доступа, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с помощью x2go. Проброс принтеров, трансляция токенов;
- в **Яндекс.Дзен** — Организация удаленного доступа с помощью x2go. Проброс принтеров, трансляция токенов;
- в **VK Видео** — Организация удаленного доступа с помощью x2go. Проброс принтеров, трансляция токенов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка x2go

Для установки **x2go** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install x2goserver-xsession x2goserver-fmbindings x2goserver-common x2goserver x2goagent x2goserver-desktopsharing
```

Здесь и далее команды будут выполняться от пользователя **root**, если не указано иное.

Для установки **x2go** на клиенте выполните команду:

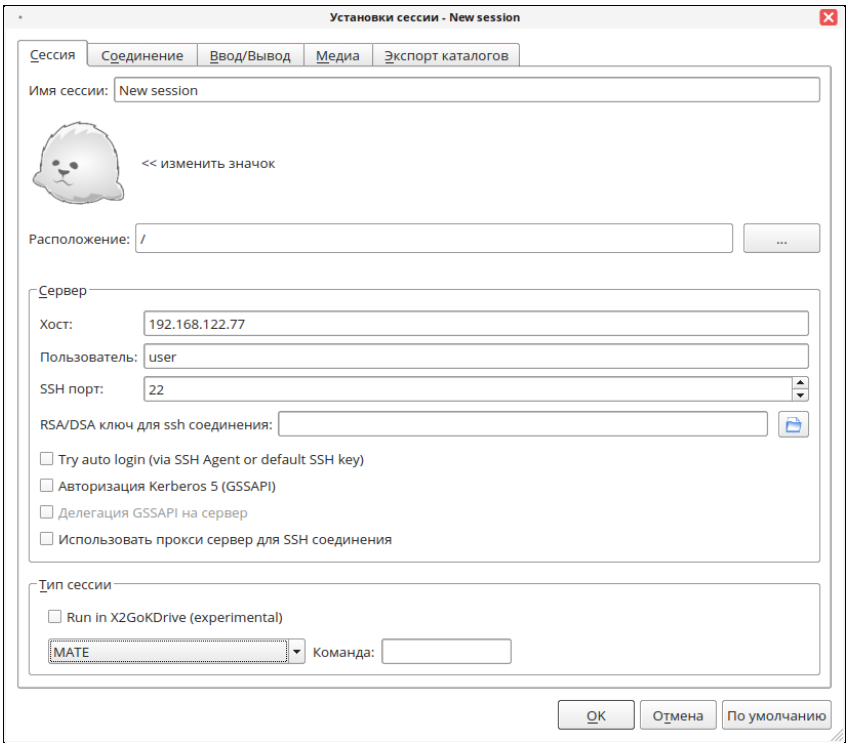
```
dnf install x2goclient
```

Настройка клиента

1. Откройте **x2go client** из «**Главного меню**» - «**Интернет**» - «**X2Go Client**».

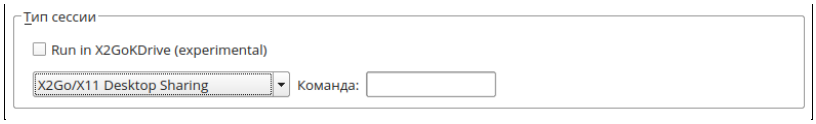
2. После открытия потребуется настроить параметры:

- *Хост*: IP-адрес машины;
- *Пользователь*: имя учетной записи.
- *SSH-порт*: если не менялся на клиенте, оставить 22.



3. Для создания новых сессий при подключении к серверу требуется выбрать тип сессии Mate. В РЕД ОС 7.3 по умолчанию используется графическая оболочка Mate. Если же у вас используется другая DE, то тип сессии изменяется в соответствии с нужным требованием.

Если необходимо соединение с активной сессией пользователя, то выберите тип сессии «X2Go/X11 Desktop Sharing».



4. Обратите внимание, что можно настроить автоподключение, указав **RSA/DSA** ключ через выбор файла ключа.

Для этого необходимо выполнить следующие действия:

- На клиенте необходимо сгенерировать ключ SSH командой **ssh-keygen** (с правами **непривилегированного** пользователя):

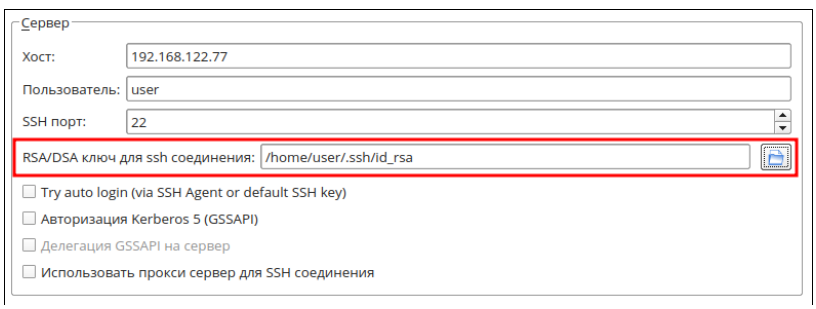
```
ssh-keygen -t rsa
  или
ssh-keygen -t dsa
```

Будет выведено предложение ввести пароль для защиты файла ключа. Если вы планируете выполнять скрипты по **SSH**, оставьте пароль пустым.

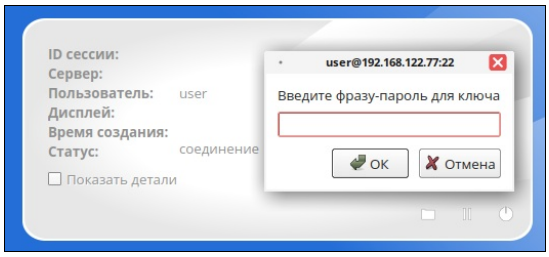
- Передайте публичный ключ на сервер командой от **непривилегированного** пользователя:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server   или ssh-copy-id -i ~/.ssh/id_dsa.pub user@server
```

- В **x2go client** выберите приватную часть ключа.



При подключении произойдет запрос фразы-пароля для ключа.



- Для того чтобы настроить автоматический вход без пароля, необходимо установить флажок в поле «**Try auto login (via SSH Agent or default SSH key)**».

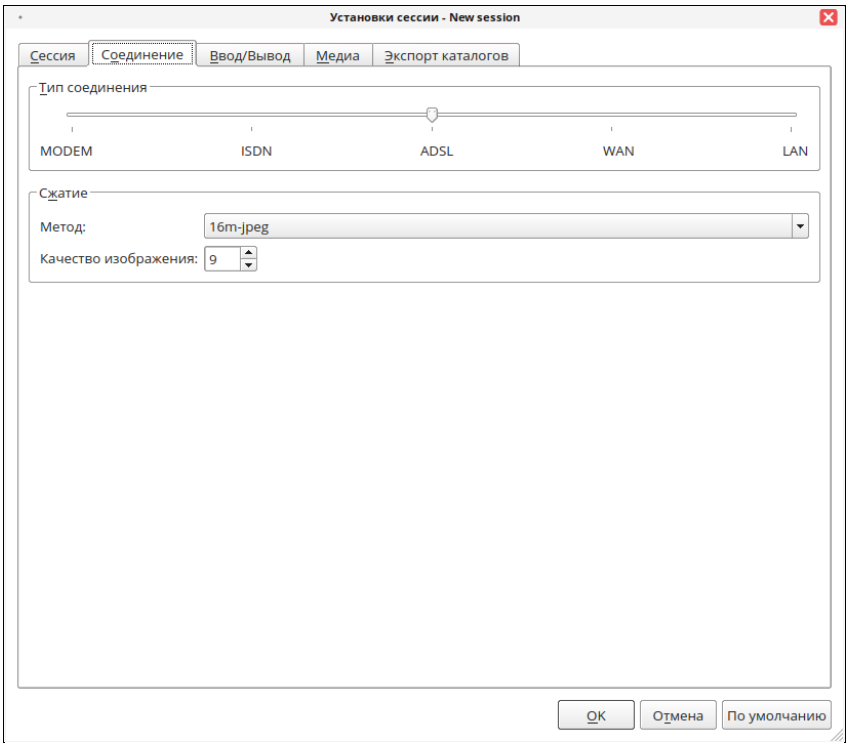
Обзор клиента

Вкладка «Соединение»

В зависимости от пропускной способности сетевого подключения вы можете выбрать предпочитаемый **тип соединения**:

- MODEM;
- ISDN;
- ADSL;
- WAN;
- LAN.

Также данная вкладка предоставляет возможность выбора типа сжатия изображения путем выбора **метода сжатия** и **качества** изображения.



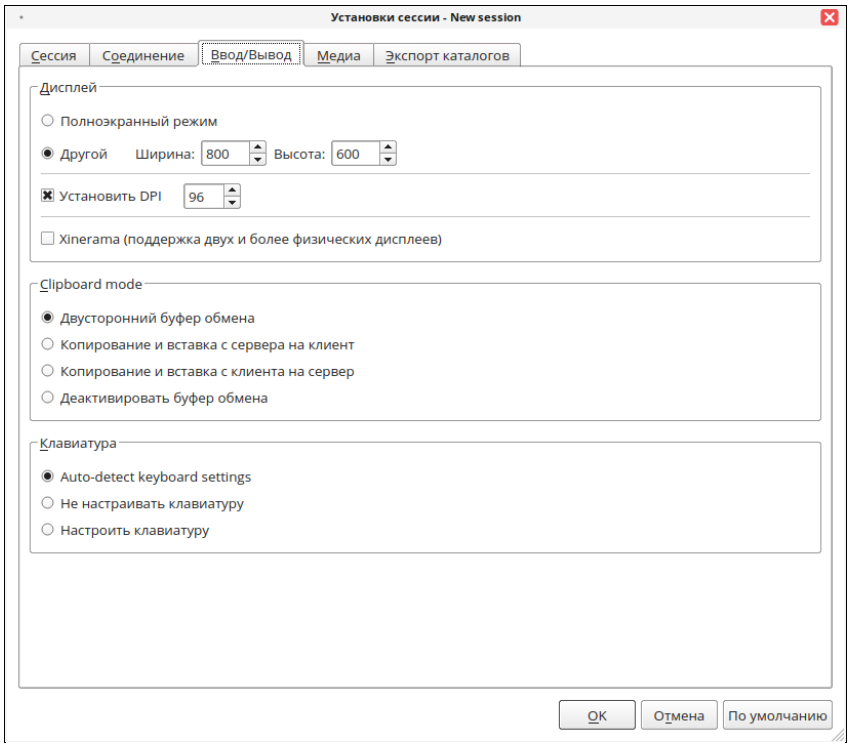
Вкладка «Ввод/Вывод»

Данная вкладка позволяет задать разрешение клиента, т.е. использовать полноэкранный режим или указать свои собственные параметры.

При наличии нескольких физических мониторов вы можете активировать опцию **Xinerama**.

Для работы с буфером обмена рекомендуется оставить настройку двустороннего буфера обмена для удобства работы.

Соответственно, настройку клавиатуры рекомендуется оставить по умолчанию, однако если есть необходимость ручной настройки, то выберите пункт ручной настройки клавиатуры.

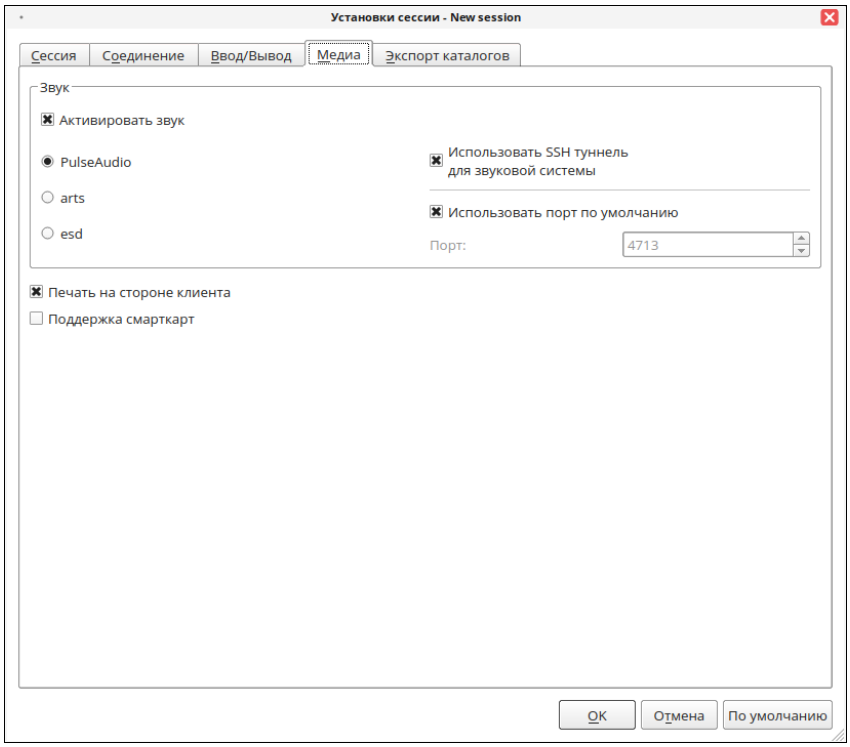


Вкладка «Медиа»

Стоит обратить внимание,что клиент **X2Go** поддерживает проброс звука, по умолчанию данная опция включена. Однако вы можете изменить свойства подключения и изменить установленное значение по умолчанию в случае необходимости.

Не рекомендуется выбирать тип звука **arts** или **esd**, т. к. они являются устаревшими. При попытке выбора любого из данных типов клиент посоветует перейти на тип **PulseAudio**.

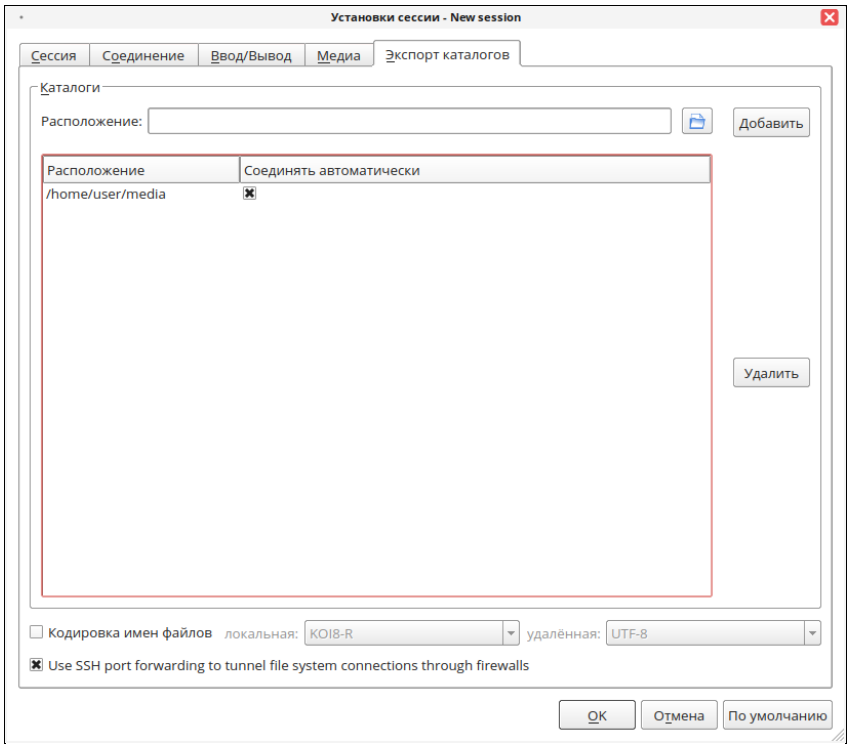
Также вы можете опционально изменить SSH-туннель и порт по умолчанию.



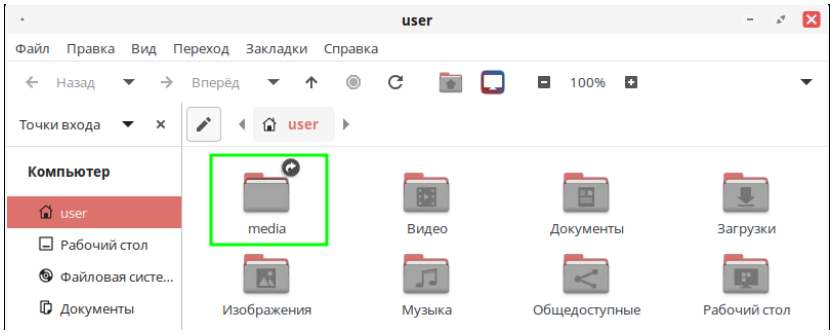
Вкладка «Экспорт каталогов»

Стоит обратить внимание на такую полезную функцию, как экспорт каталогов.

На данной вкладке вы можете выбрать, каким каталогом желаете поделиться. После выбора и добавления он отобразится в списке, где вы сможете активировать его автоматическое соединение.



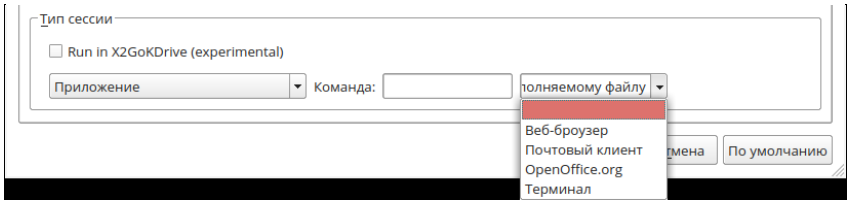
После подключения через **x2go** в домашнем каталоге пользователя будет создан каталог **media**, именно в него перенаправится каталог с клиента.



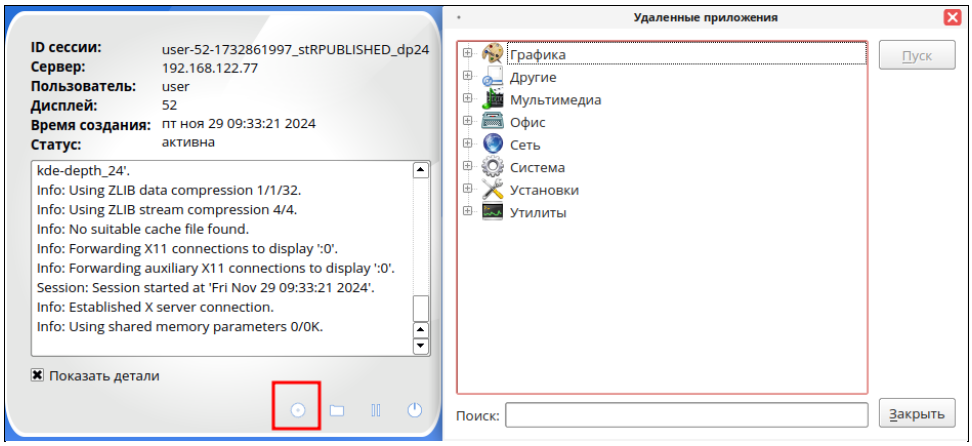
Запуск определенного приложения

Клиент **x2go** поддерживает также вариант подключения не только к полному рабочему столу сервера, но и к конкретному приложению. Реализовать данное подключение можно при помощи типа сессии «**Приложение**» или «**Удаленные приложения**».

При выборе типа сессии приложения вам будет доступен ряд предустановленных вариантов запуска:



При выборе типа сессии «**Удаленные приложения**» откроется новая сессия, где вручную потребуется выбрать то, какое приложение требуется запустить.



Проброс принтеров

1. Для корректного проброса принтера необходимо установить следующие пакеты:

- На сервере:

```
dnf install x2goserver-printing cups-x2go
```

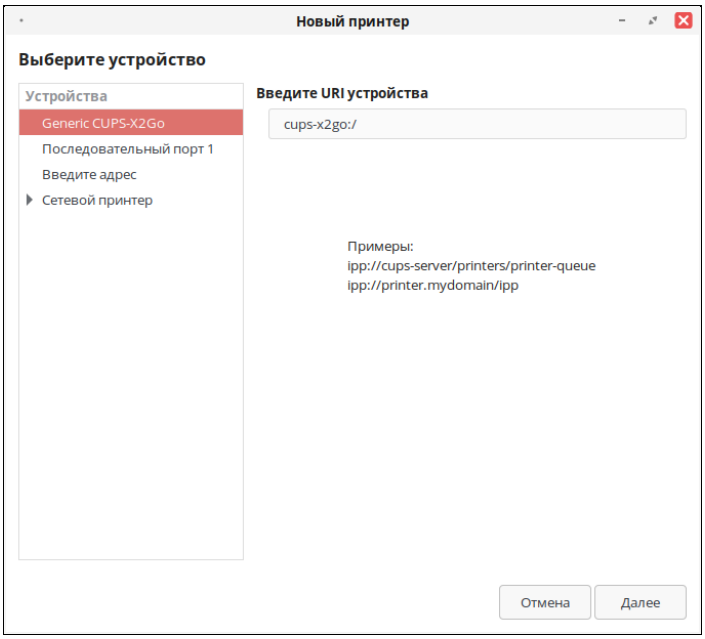
- На клиенте:

```
dnf install cups-x2go
```

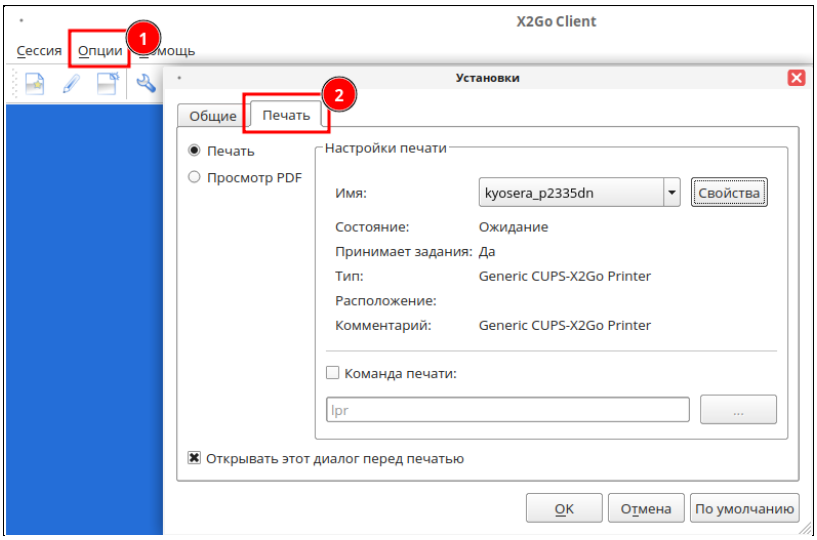
При необходимости перезапустите службу **cups**:

```
systemctl restart cups
```

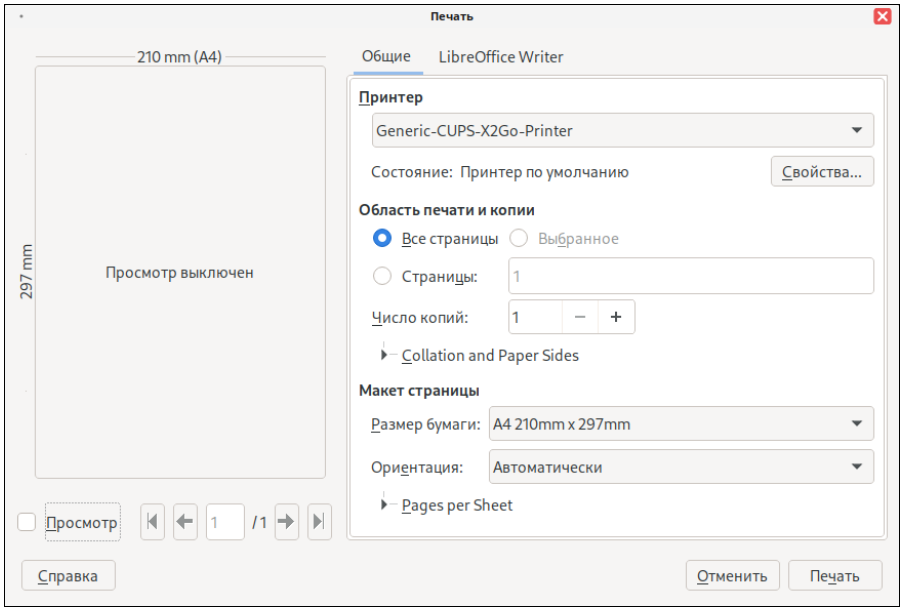
2. На сервере **X2go** добавьте принтер **Generic CUPS-X2Go** («Главное меню» - «Администрирование» - «Настройки принтера»).



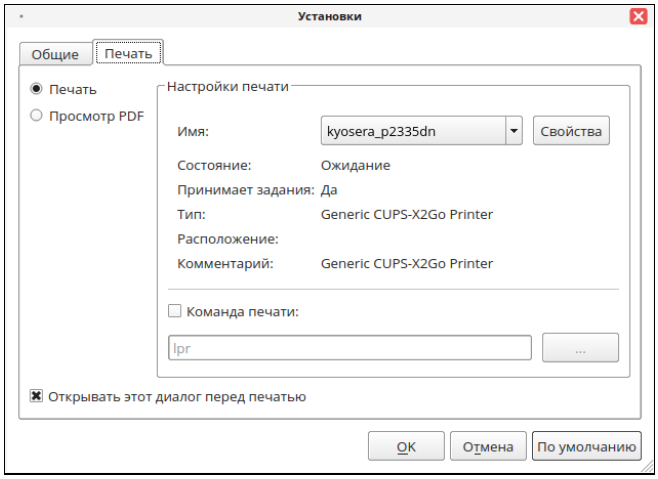
3. В **x2go**-клиенте перейдите в меню «**Опции**» - «**Установки**» - «**Печать**» и выберите принтер, который будет определн по умолчанию при печати. Установите параметр «Открывать этот диалог перед печатью».



4. При печати документа в сессии **x2go** выберите принтер «**Generic CUPS-X2Go-printer**» и нажмите «**Печать**».



После этого на вашем ПК откроется окно выбора локального принтера для печати.

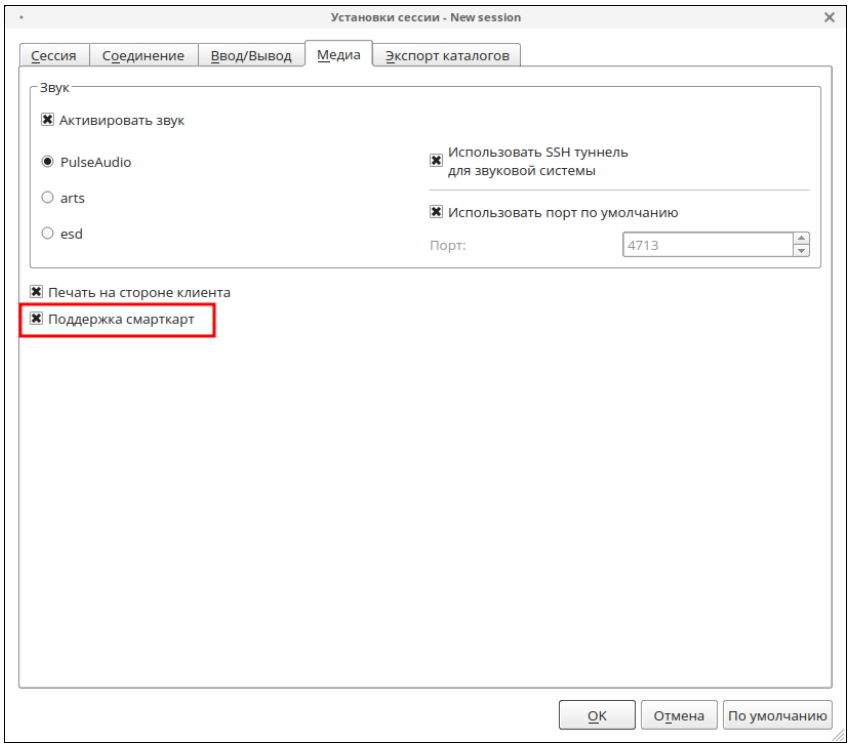


Настройка трансляции токенов в сессию сервера

1. Для настройки трансляции прежде всего требуется убедиться, что настроен **КриптоПро** и необходимые драйвера для токенов на сервере **x2go** - инструкция по настройке.

2. Проверьте работоспособность токена в утилите «**Ключевые носители и сертификаты**» и затем установите флажок в **x2go client** - **Медиа** - **Поддержка смарт-карт**.

Данная поддержка обеспечивает трансляцию как смарт-карт, так и usb-токенов.



Завершение сессий x2go

На сервере необходимо запустить команду, которая покажет все активные сессии:

```
x2golistsessions_root
```

Примерный вывод данной команды:

```
 3226 | user-50-1649312737_stDMATE_dp24 | 50 | localhost.localdomain | S | 2022-04-07T09:25:38 | 8b2f5d3433700b44b5acf5150a7d35fb | 10.81.1.132 | 36540 | 36541 | 2022-04-07T09:35:04 | user | 1839 | 36542 | -1 | -1
 7350 | user-51-1649313366_stS1XSHADuserXSHADPP50_dp24 | 51 | localhost.localdomain | R | 2022-04-07T09:36:06 | c9f4d9a24979efe9ddca96ec20e722cc | 10.81.1.132 | 56847 | 56848 | 2022-04-07T09:36:10 | user | 1211 | 56849 | -1 | -1
 7769 | user-52-1649313401_stS1XSHADuserXSHADPP0_dp24 | 52 | localhost.localdomain | R | 2022-04-07T09:36:41 | 414d5ac30224e035a46c9d7be0d4608b | 10.81.1.132 | 38461 | 38462 | 2022-04-07T09:36:43 | user | 1176 | 38463 | -1 | -1
```

Для завершения определенной сессии выполните:

```
x2goterminate-session <session_id>
```

где <**session_id**> - это идентификатор сессии.

Пример:

```
x2goterminate-session user-50-1649312737_stDMATE_dp24
```

Массовое завершение сессий

Если же на сервере требуется применить **массовую** очистку сессий, то вы можете воспользоваться одним из предложенных ниже скриптов, которые автоматизируют данный процесс.

Завершение сессии и вывод текущей даты

Пример скрипта **завершения сессий** и **вывода текущей даты** при завершении:

```
#!/bin/bash
f=$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )
NOWDATE=$(date '+%Y-%m-%d_%T')
```

```
echo -----$NOWDATE------
for i in $(x2golistsessions_root | cut -d "|" -f 2 | sed "s/|/ | /g")
do
echo terminate - ${i} # вывод на экран
x2goterminate-session ${i} # команда завершения пользователя
done
```

Завершение неактивных более 2 часов сессий

Пример скрипта завершения сессий, **время простоя** которых **более 2 часов**:

```
#!/bin/bash
for ll in `x2golistsessions_root`; do
SessionDate=`echo $ll | awk -F \| '{print $11}';`
CleanSessionDate=`echo ${SessionDate//T/ }`
FinalDate=`echo ${CleanSessionDate//-//}`
CurrentDate=`date +%s`
SessionDateEpoch=`date -d "$FinalDate" +%s`
DateDiff=$(($CurrentDate-$SessionDateEpoch))
Hours=$(($DateDiff/60/60))
if [[ $Hours -gt 2 ]]; then
sid=`echo $ll | awk -F \| '{print $2}'`
x2goterminate-session $sid
fi
done
```

Завершение неактивных более 1 дня сессий

Пример скрипта завершения сессий, **время простоя** которых **больше 1 дня**:

```
#!/bin/bash
LIMIT_DAYS=1
for ll in `x2golistsessions_root`; do
#Get the date of last use of the session
lastd=`echo $ll | awk -F \| '{print $11}' | awk -F T '{print $1}';`
#Date in seconds
lastsec=`date -d "$lastd" +%s`
#Current date in seconds
now=`date +%s` days=`echo $(( ($now - $lastsec) /60/60/24 ))`
if [[ $days -gt $LIMIT_DAYS ]]; then
sid=`echo $ll | awk -F \| '{print $2}'`
echo "terminating session: $sid, $days days old, lastd: $lastd, lastsec: $lastsec, now: $now" x2goterminate-session $sid
fi
done
```

Настройка автоматического завершения сессий

Также администратору сервера будет удобен вариант создания сервиса, который по определенному таймеру завершит сессии. Ниже приведен пример сервиса, который по таймеру запускает абстрактный скрипт. **Обратите внимание, что необходимо изменить путь к скрипту на ваш**.

Создайте файл:

```
nano /etc/systemd/system/x2go-sessions-killer.service
```

со следующим содержимым:

```
[Unit]
```

```
Description="X2Go service for session cleaning"
After=network.target
[Service]
Type=simple
ExecStart=/usr/bin/SCRIPT.sh # укажите ваш путь к скрипту
Restart=always
RestartSec=7200
[Install]
WantedBy=multi-user.target
```

В строке `RestartSec=7200` указано время перезапуска скрипта в секундах. В примере скрипт будет выполняться **каждые два часа**. Измените это значение на необходимое вам.

Затем в папку **/usr/bin/** добавьте ваш скрипт и назначьте ему права на исполнение:

```
chmod +x /usr/bin/SCRIPT.sh
```

После этого обновите список сервисов и добавьте сервис завершения сессий в автозагрузку:

```
systemctl daemon-reload
systemctl enable --now x2go-sessions-killer.service
```

X2Go Broker

X2Go Broker — модуль, позволяющий централизованно управлять настройками сессий клиентов. В большинстве случаев клиенты X2Go запускаются в автономном режиме, и пользователь сам настраивает одну или несколько сессий для подключения к серверам X2Go, а все настройки сохраняются на локальных компьютерах.

Данный модуль позволяет хранить настроенные профили подключения непосредственно на сервере, а для получения настроек с сервера клиент X2Go должен быть запущен в режиме **Broker Mode**, при этом локально настроенные профили игнорируются. Это решение полезно в масштабах крупных предприятий для балансировки нагрузки.

Настройка x2gobroker

Для установки пакетов **x2gobroker** перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

```
dnf install x2gobroker x2gobroker-common x2gobroker-ssh x2gobroker-daemon x2gobroker-authservice
```

Далее необходимо в файл **/etc/hosts** добавить запись о сервере:

```
echo "<ip-адрес_сервера> x2goserver" >> /etc/hosts
```

В файле **/etc/x2go/broker/x2gobroker-sessionprofiles.conf** определите следующие параметры:

```
[x2goserver-mate]
name=Test Work Mate
host=x2goserver
command=MATE
usebrokerpass=true
```

где:

- **[x2goserver-mate]** — уникальный идентификатор сессии;
- **name** — имя сессии, которое будет отображаться на клиенте;
- **command** — тип сессии (MATE, KDE и т.п.).

Затем запустите необходимые для работы сервисы:

```
systemctl enable x2gobroker-authservice --now
systemctl enable x2gobroker-daemon --now
```

Настройка x2goserver

Для настройки сервера необходимо сначала установить соответствующие пакеты командой:

```
dnf install x2goserver x2goserver-printing cups-x2go x2goserver-xsession
```

После установки в файл **/etc/hosts** следует добавить запись о брокере командой:

```
echo "<ip-адрес_брокера> x2gobroker" >> /etc/hosts
```

Запустите сервис сервера командой:

```
systemctl enable x2gocleansessions --now
```

Настройка x2goclient

Для настройки клиента необходимо установить соответствующий пакет командой:

```
dnf install x2goclient
```

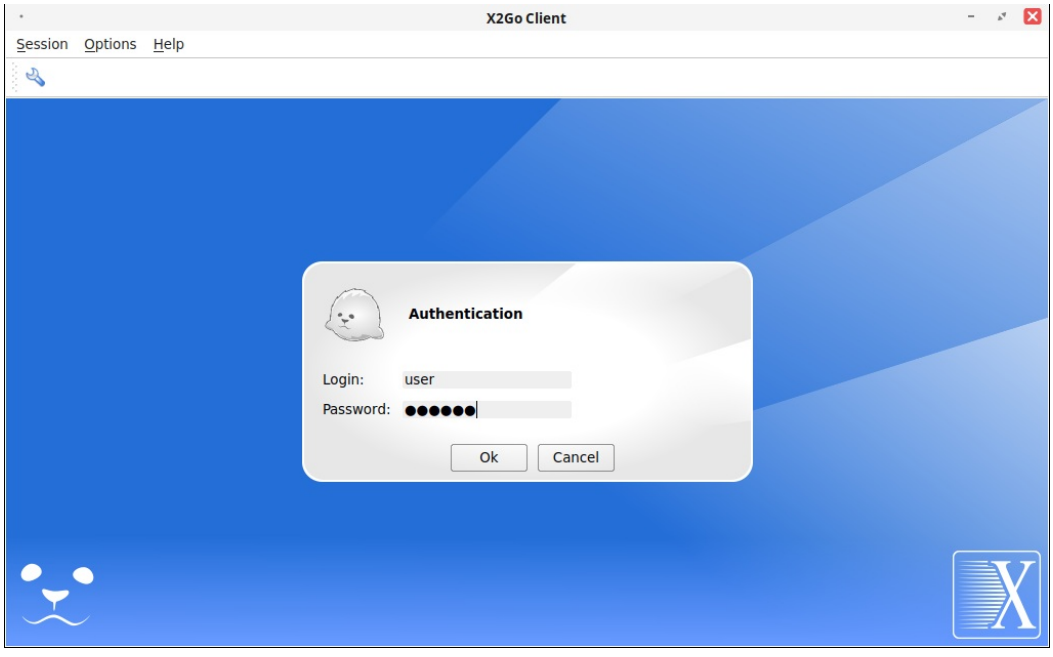
После установки клиента в файл **/etc/hosts** следует добавить запись о брокере и сервере командой:

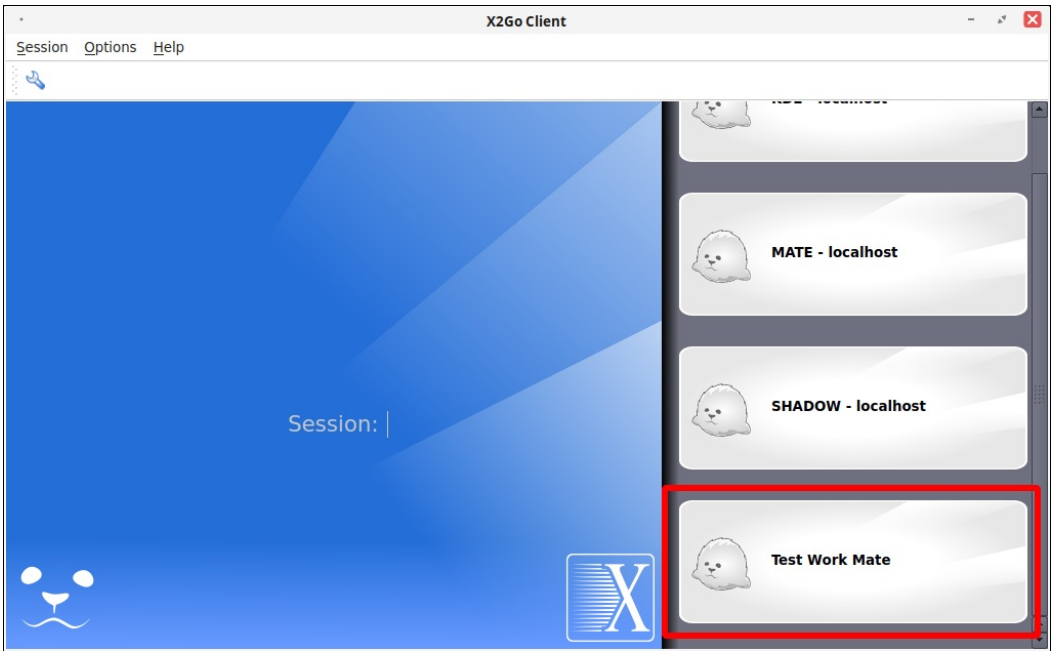
```
echo "<ip-адрес_брокера> x2gobroker" >>/etc/hosts
echo "<ip-адрес_сервера> x2goserver" >>/etc/hosts
```

Для подключения к серверу выполните команду:

```
x2goclient --broker-url=http://x2gobroker:8080/plain/
```

В окне аутентификации введите логин и пароль пользователя, с правами которого необходимо подключиться к серверу, и выберите нужную сессию (в примере *Test Work Mate*).





В активном окне сессии можно убедиться в правильности подключения, проверив IP-адрес машины. Должен быть отображен IP-адрес сервера.

Запуск отдельного графического приложения

Для запуска определенного приложения на брокере необходимо добавить конфигурацию новой сессии (файл **/etc/x2go/broker/x2gobroker-sessionprofiles.conf**):

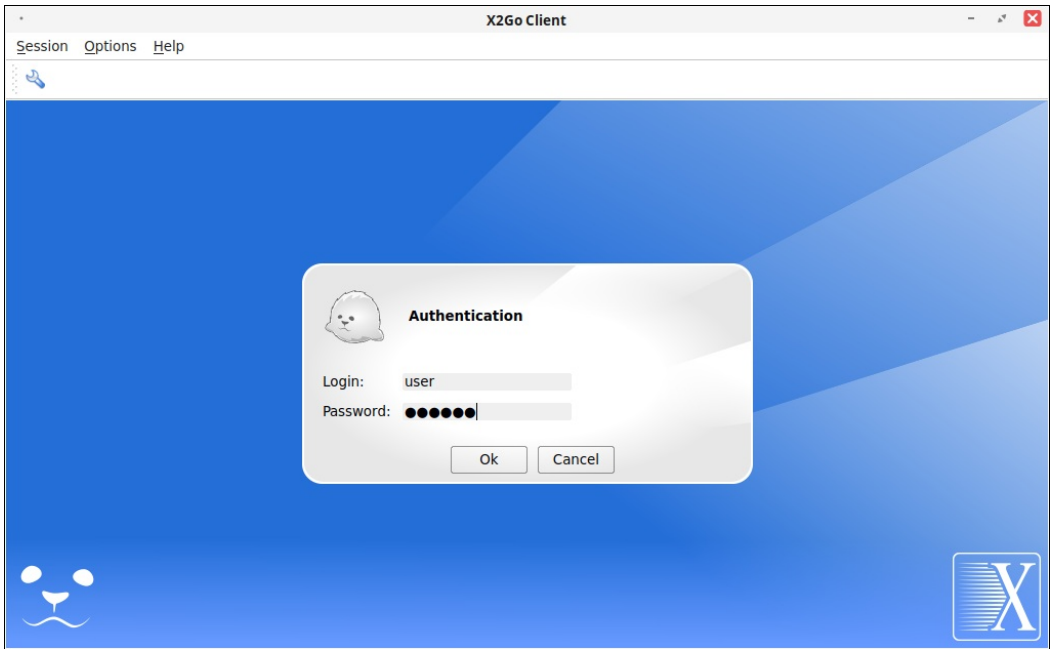
```
[x2goserver-brasero]
name=Test Brasero
host=x2goserver
command=brasero
usebrokerpass=true
```

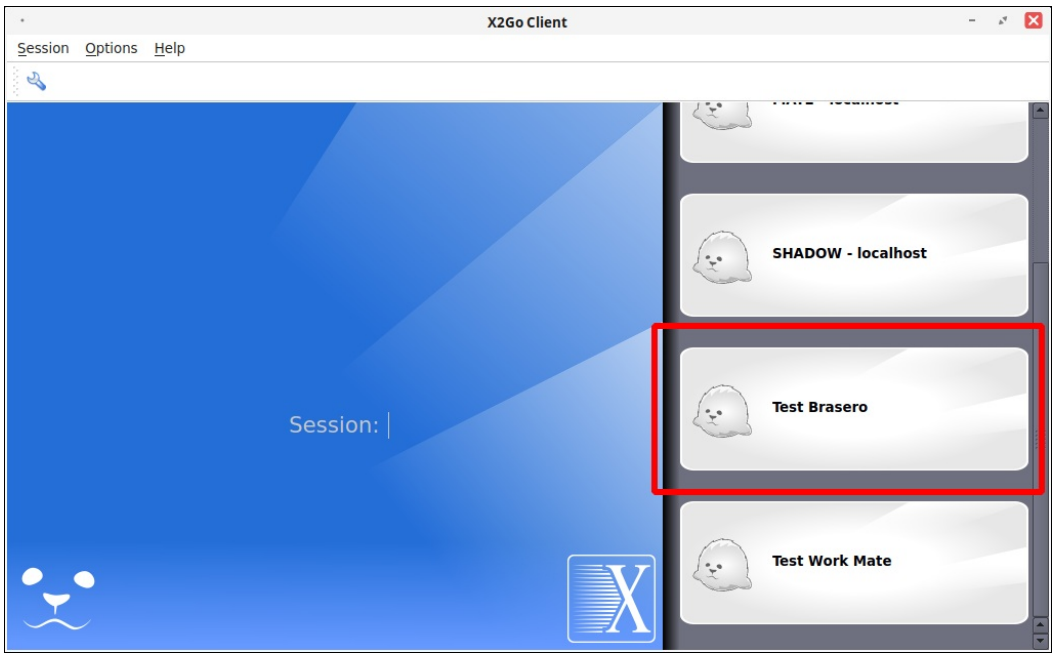
В данном случае в параметре command указывается название приложения, которое должно быть запущено вместо графической сессии.

Для подключения клиента к серверу используется та же команда:

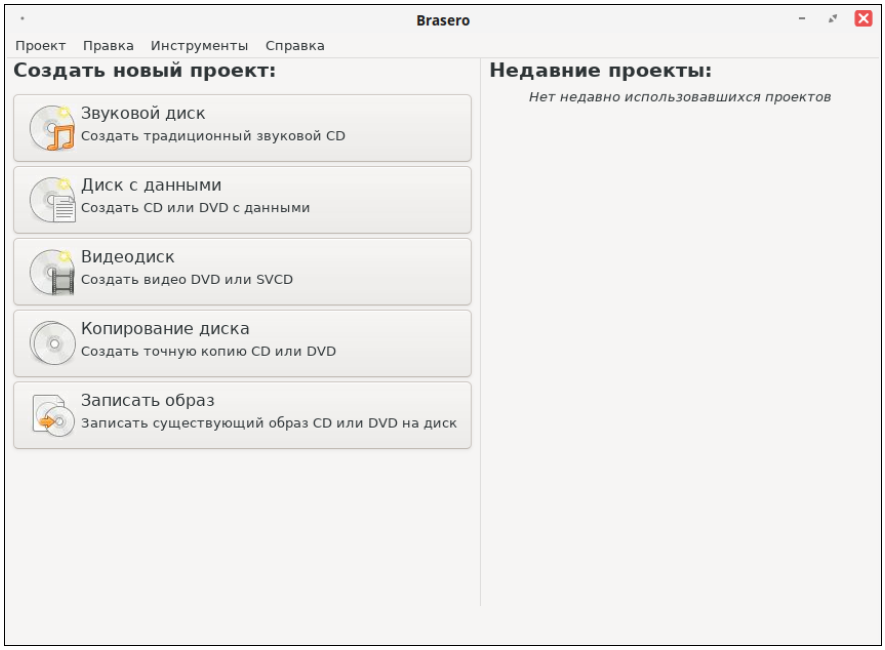
```
x2goclient --broker-url=http://x2gobroker:8080/plain/
```

В окне аутентификации так же потребуется введите логин и пароль пользователя, с правами которого необходимо подключиться к серверу, и выбрать сессию с запуском отдельного приложения (в примере **Test Brasero**).





После успешного подключения будет открыто окно указанной программы.



Настройка SPICE

Настройка сервера
Настройка клиента

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: spice-server-0.15.1-3.el7.x86_64 xorg-x11-server-Xspice-0.1.5-18.el7.x86_64, openssh-server-8.9p1-13, spice-gtk-tools-0.38-1

Настройка сервера

ВАЖНО!

После выполнения настроек и дальнейшей перезагрузки управление сервером будет доступно только через удаленный доступ.

Установка сервера происходит в консоли с root-правами.

```
su -
dnf install xorg-x11-server-Xspice
```

Для удаленного доступа к консоли **ssh**:

```
dnf install openssh-server
systemctl start sshd
systemctl enable sshd.service
```

Присвойте серверу статический Ip-адрес.

В файле **/etc/X11/xorg.conf** прописывается настройка SPICE-сервера и использование виртуальной видеокарты QXL.

```
nano /etc/X11/xorg.conf
```

Для удобства редактирования файла **/etc/X11/xorg.conf** рекомендуется скопировать в него содержимое:

```
Section "Device"
 Identifier "XSPICE"
 Driver "spiceqxl"
  # Enable regular port. Either this or SpiceTlsPort, or one of XSPICE_PORT or
  # XSPICE_TLS_PORT environment variables must be specified
  # Defaults to 5900.
  Option "SpicePort" "5900"
  # Do not request any password from client
  Option "SpiceDisableTicketing" "0"
  # Set password client will be required to produce.
  Option "SpicePassword" "password"
EndSection

Section "InputDevice"
  Identifier "XSPICE POINTER"
  Driver "xspice pointer"
EndSection

Section "InputDevice"
 Identifier "XSPICE KEYBOARD"
 Driver "xspice keyboard"
EndSection

Section "Monitor"
 Identifier "Configured Monitor"
EndSection
```

```
Section "Screen"
 Identifier "XSPICE Screen"
 Monitor "Configured Monitor"
 Device "XSPICE"
 DefaultDepth 24
EndSection

Section "ServerLayout"
 Identifier "XSPICE Example"
 Screen "XSPICE Screen"
 InputDevice "XSPICE KEYBOARD"
 InputDevice "XSPICE POINTER"
EndSection

# Prevent udev from loading vmmouse in a vm and crashing.
Section "ServerFlags"
 Option "AutoAddDevices" "False"
EndSection
```

ВАЖНО!

Здесь задается пароль сервера, если оставить без изменений, то пароль по умолчанию будет **password**.

```
Set password client will be required to produce.
Option "SpicePassword" "password"
EndSection
```

ВАЖНО!

После выполнения настроек и дальнейшей перезагрузки управление сервером будет доступно только через удаленный доступ.

Настройка клиента

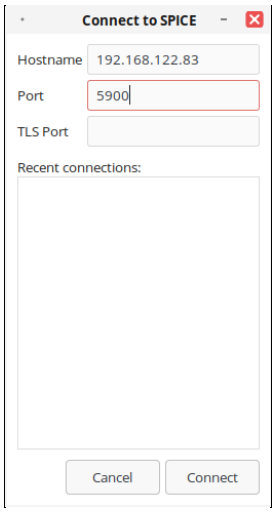
Настройка клиента производится одной командой через терминал с использованием **root**-прав.

```
dnf install spice-gtk-tools
```

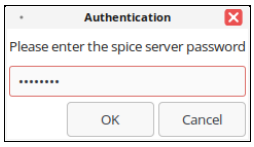
Обратиться к серверу можно через терминал командой:

```
spicy
```

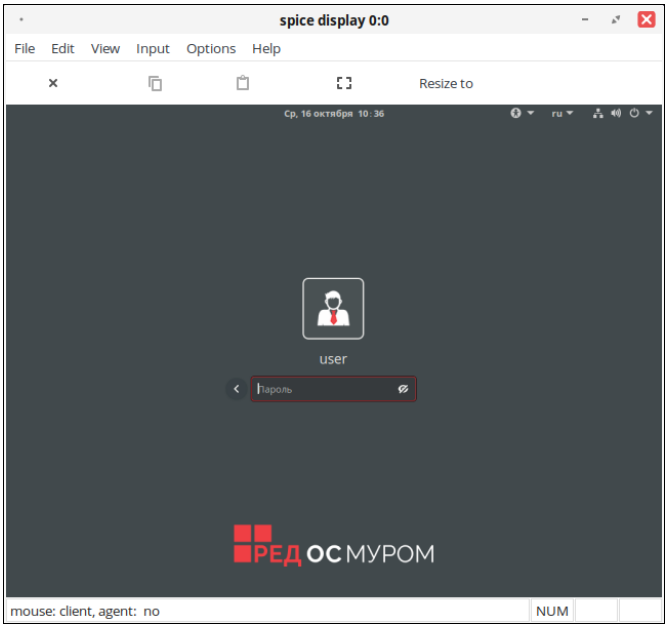
Появится окно, в котором вам нужно ввести IP-адрес сервера и порт **5900**.

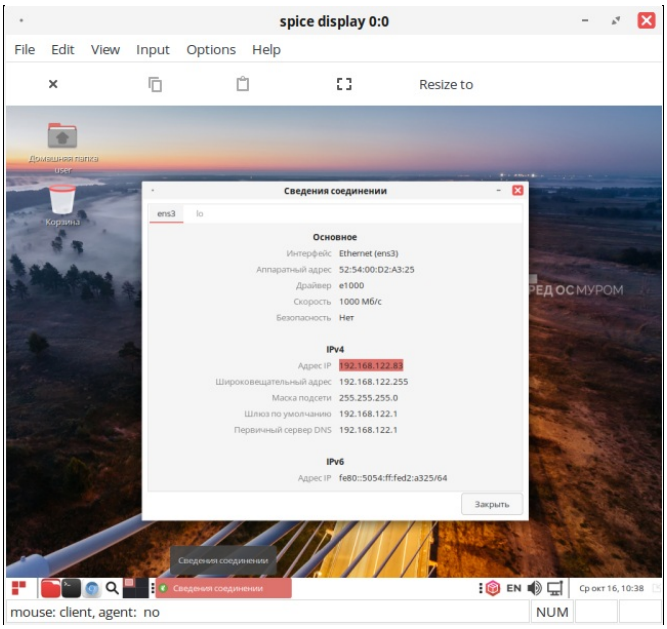


После этого потребуется ввести пароль для входа на сервер.



При успешной аутентификации у вас появится окно сервера, где вам нужно будет авторизоваться в системе сервера под локальной учетной записью.





Настройка X11VNC

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: x11vnc-0.9.16-7

Вы можете подробнее ознакомиться с установкой и настройкой **x11vnc** для удаленного подключения, просмотрев наши обучающие видео:

- на **RuTube**:
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.
- в **Яндекс.Дзен:**
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.
- в **VK Видео:**
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.

На наших каналах вы также сможете найти много другой полезной информации.

Перейдите в сеанс пользователя **root**:

```
su root
```

Далее все команды будут выполняться с правами пользователя **root**, если не указано иное.

Установите пакет **x11vnc**.

```
dnf install x11vnc
```

Настройте сам **x11vnc** и пропишите пароль:

```
x11vnc -storepasswd "пароль" /etc/vncpasswd
```

Чтобы **vnc** запускался автоматически, пропишите его как сервис в **systemd**:

```
nano /lib/systemd/system/x11vnc.service
```

Заполните его следующим содержимым:

```
[Unit]
 Description=x11vnc server for GDM
 After=display-manager.service

 [Service]
 ExecStart=/usr/bin/x11vnc -many -shared -display :0 -auth guess -noxdamage -rfbauth /etc/vncpasswd
 Restart=on-failure
 RestartSec=3

 [Install]
 WantedBy=graphical.target
```

Если в качестве менеджера входа используется SDDM(Simple Desktop Display Manager), то сервис будет отличаться:

```
[Unit]
 Description=x11vnc server for SDDM
 After=graphical.target
```

```
[Service]
ExecStart=/bin/bash -c "/usr/bin/x11vnc -display :0 -many -shared -dontdisconnect -repeat -auth $(ls /var/run/sddm/{*}) -noxdamage -rfbauth /etc/vncpasswd"
Restart=on-failure
RestartSec=3

[Install]
WantedBy=graphical.target
```

Перезагрузите демон **systemd**:

```
systemctl daemon-reload
```

Добавьте в автозагрузку сервис **x11vnc**:

```
systemctl enable x11vnc.service
```

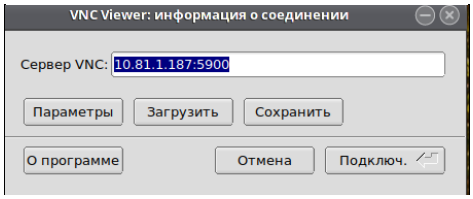
Запустите службу для проверки:

```
systemctl start x11vnc.service
```

Проверьте, запустилась ли служба (нормальное состояние - это статус "**active (running)**").

```
systemctl status x11vnc.service
```

Теперь можно присоединиться к текущей сессии пользователя (на примере **tigerVNC**, порт 5900 необязателен).



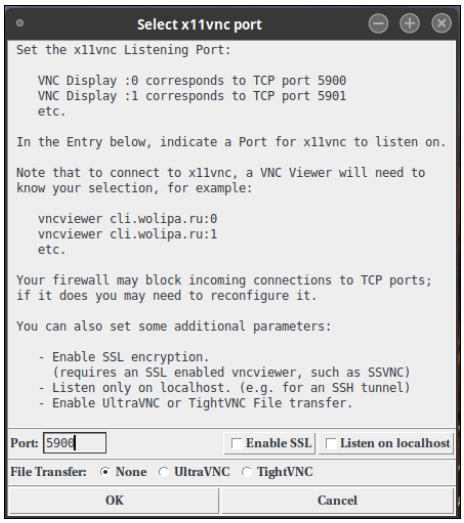
Примечание.

Так как проект **x11vnc** еще в стадии разработки, для более стабильного удалённого доступа рекомендуется использовать x2go.

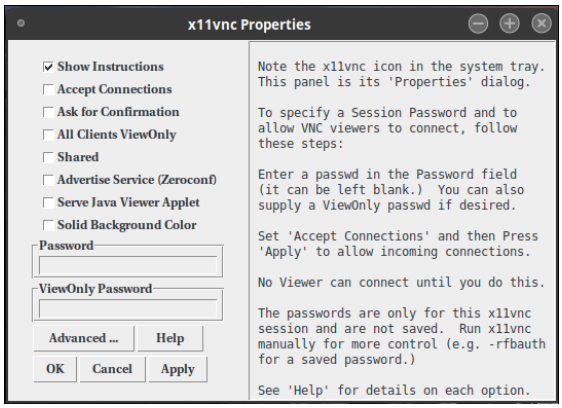
x11vnc gui

Запуск графической утилиты администрирования **x11vnc** доступен из «**Главного меню**» - «**Интернет**» - «**X11VNC Server**».

Стартовое окно утилиты представлено в следующем виде:

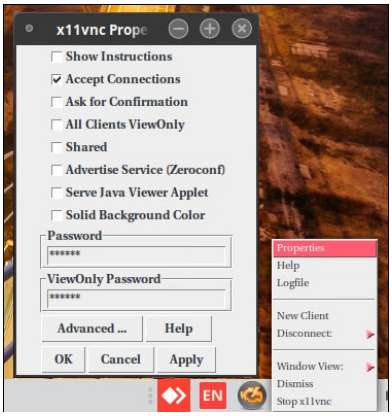


При нажатии на «**OK**» вы увидите дальнейшее окно настройки сервера:

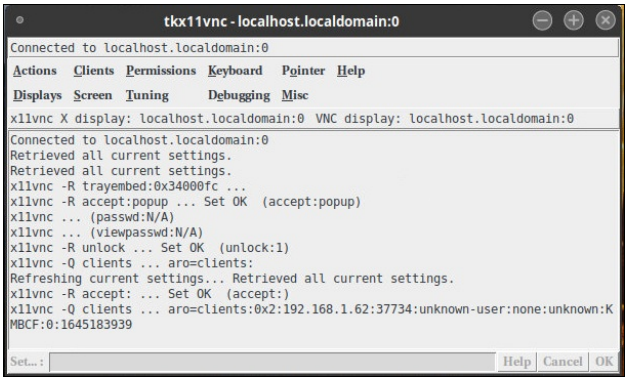


Вы можете настроить параметры подключения клиентов под себя. При нажатии кнопки «**OK**» происходит запуск сервиса **x11vnc**, ПК становится доступен для подключения. После запуска утилита сворачивается в системный трей.

При вызове свойств из трея вы увидите следующее окно:



При переходе в режим **Advanced** открывается более подробная информации о подключении и дополнительных параметрах настройки связи.



Работа с FreeRDP и RemoteApp

Установка freerdp
Варианты использования freerdp для подключения к удаленному рабочему столу
xfreerdp_gui - графическая оболочка для работы с freerdp
RemoteApp - запуск приложений

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: freerdp-3:3.8.0-1, freerdp-gui-3.0-2

freerdp — клиент с открытым кодом для подключения к удаленному рабочему столу по протоколу **RDP**.

Установка FreeRDP

Для установки пакета выполните команду:

```
dnf install xfreerdp
```

Описание часто используемых параметров:

Параметр	Описание
/u:	Имя пользователя
/d:	Имя домена
/v:	ip-адрес или имя хоста
/p:	Пароль
/w: /h:	Значения ширины и высоты
/smartcard:	Проброс токенов
/a:printer	Подключение принтера
/cert:ignore	Игнорировать сертификат
/app:program:	Запуск удаленного приложения
/drive:	Подключение каталога
/sound:	Перенаправление звука
/microphone:	Активация микрофона

Полный список параметров представлен на официальной странице проекта **FreeRDP**.

Варианты использования FreeRDP для подключения к удаленному рабочему столу

Подключение папки

```
xfreerdp /u:bob /d:win.redos /v:192.168.1.196 /cert:ignore /sec:rdp /p:my_password /drive:folder,/home/bob@win.redos/temp
```

Подключение принтера

Названия подключенных принтеров можно вывести командой **lpstat -a**.

```
xfreerdp /u:bob /d:win.redos /v:192.168.1.196 /cert:ignore /sec:rdp /p:my_password /a:printer,"Kyocera-Kyocera-ECOSYS-P2335dn-(KPDL)"
```

Подключение токена

С помощью **pcsc_scan** узнаем имя токена, например, **Reader 0: Aladdin R.D. JaCarta 00 00** достаточно указать первое вхождение в имени **Aladdin**.

```
xfreerdp /u:user /p:my_password /smartcard:Aladdin /v:192.168.1.196
```

Перенаправление звука и микрофона в сессию

```
xfreerdp /v:192.168.1.196 /u:user /p:my_password /sound:sys:oss,dev:1,format:1 /sound:sys:alsa /microphone:sys:oss,dev:1,format:1 /microphone:sys:alsa
```

где **sys:alsa** - явное указание какой звуковой поддержки выбрать (**alsa**/**pulse**).

Подключение к сессии с явным указанием размеров окна

```
xfreerdp /v:192.168.1.196 /u:user /p:my_password /w:800 /h:600
```

Данное явное указание полезно в тех случаях, когда стандартное разрешение не умещается на мониторе.

freerdp-gui — графическая оболочка для работы с freerdp

Утилита **freerdp-gui** представляет собой графическую оболочку для работы с **FreeRDP**.

Данная утилита устанавливается следующей командой:

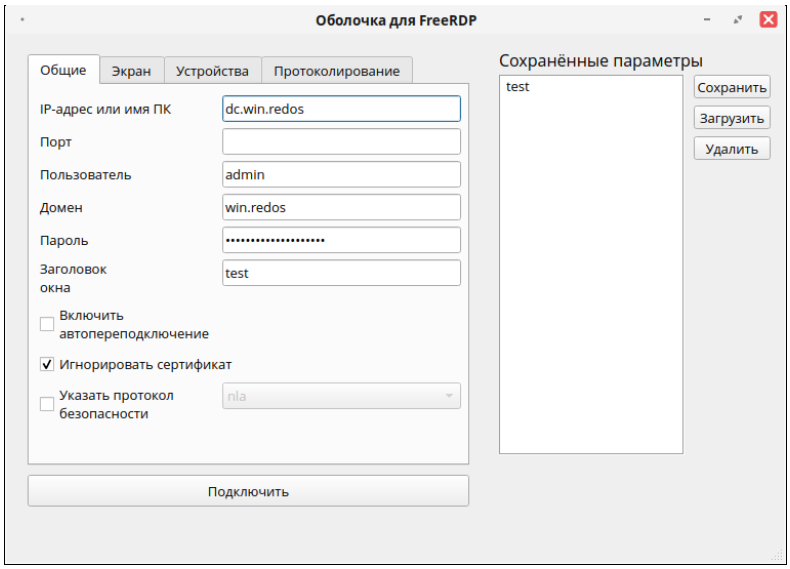
```
sudo -E dnf install freerdp-gui
```

Запуск утилиты доступен из «**Главного меню**» - «**Интернет**» - «**Оболочка для FreeRDP**» или из терминала командой:

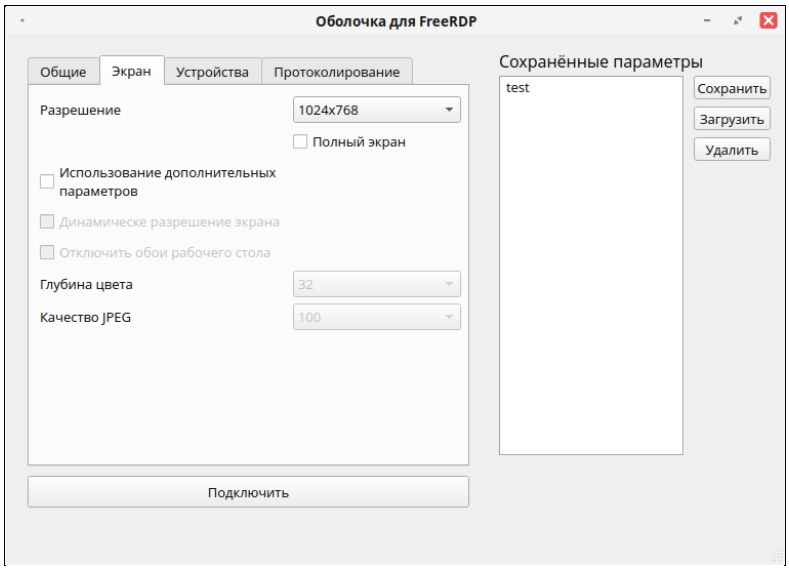
```
freerdp-gui
```

Главное окно утилиты представляет функционал по подключению к **xrdp** или Windows RDP серверу.

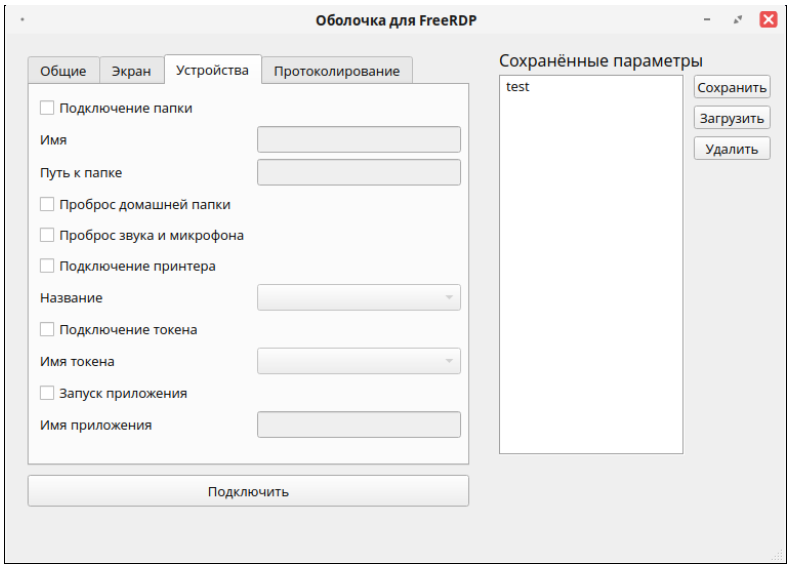
Пользователь может задать для своих целей параметры, представленные на снимке основного окна утилиты.



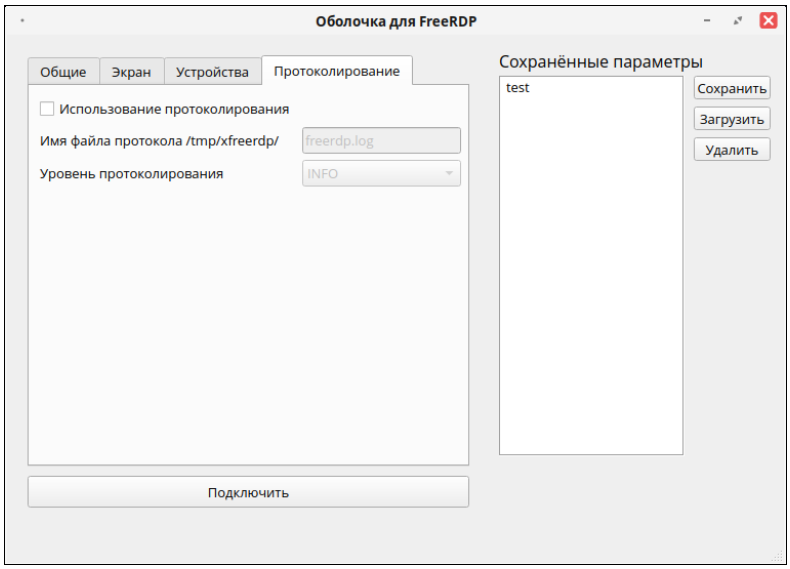
Для выбора необходимого разрешения экрана и дополнительных параметров предусмотрена вкладка «**Экран**».



Если требуется работа с пробросом папки или устройств, таких как принтер, токен или звук на серверную часть - для этого предусмотрена вкладка «**Устройства**».



Для настройки протоколирования событий предусмотрена вкладка «**Протоколирование**».



RemoteApp - запуск приложений

RemoteApp - позволяет запускать приложения по **rdp**, как если бы они были запущены на локальном компьютере пользователя, т.е пользователь запускает приложение, которое выполняется на сервере, но внешне выглядит, будто оно запущено на локальном компьютере. Для доступа к приложению, оно предварительно должно быть опубликовано на сервере **rdp**. В строке подключения

укажите приложение, доступное на сервере приложений.

```
xfreerdp /u:user /d:win.redos /v:192.168.1.196 /cert:ignore /p:my_password /app:program:"||word"
```

GUI запрос пароля:

```
xfreerdp /u:user /d:win.redos /v:192.168.1.196 /cert:ignore /p:$(zenity --entry --title="Domain Password" --text="Enter your password:" --hide-text)
```

В данном примере используется **zenity** - утилита, которая позволяет выводить на экран диалоговые окна. В данном случае - это диалог ввода пароля.

Настройка guacamole

Установка
Настройка файла конфигурации
Настройка файла параметров
Настройка клиента
Веб-интерфейс

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: guacd-1.2.0-7, tomcat-1:9.0.93-1

Guacamole — бесплатная программа с открытым исходным кодом, которая предоставляет дистанционный доступ ко всем рабочим клиентским машинам через веб-интерфейс. То есть на ваш собственный компьютер, с которого вы удалённо администрируете клиентские машины, не нужно устанавливать никаких плагинов и стороннего программного обеспечения, всё работает по **HTML5**.

Установка

Установка необходимых пакетов:

```
dnf install guacd libguac-client-rdp libguac-client-ssh libguac-client-vnc libguac-client-telnet tomcat tomcat-webapps
```

Настройка файла конфигурации

Создайте директорию:

```
mkdir /etc/guacamole
```

Настройка конфигурационного файла:

```
nano /etc/guacamole/guacd.conf
```

Содержимое файла конфигурации:

```
[server]
 bind_host = 127.0.0.1
 bind_port = 4822
```

Примечание.

Файл конфигурации чувствителен к синтаксису. Необходимо добавить 2 пустых строки в конце файла.

Настройка файла параметров

Настройка файла параметров:

```
nano /etc/guacamole/guacamole.properties
```

Содержимое файла параметров:

```
guacd-hostname: localhost
 guacd-port: 4822
 user-mapping: /etc/guacamole/user-mapping.xml
 auth-provider: net.sourceforge.guacamole.net.basic.BasicFileAuthenticationProvider
```

Создайте `GUACAMOLE_HOME` переменную окружения:

```
echo "GUACAMOLE_HOME=/etc/guacamole" | sudo tee -a /etc/default/tomcat
```

Создайте символьную ссылку:

```
ln -s /etc/guacamole /usr/share/tomcat/.guacamole
```

Настройка клиента

Выполните настройку `guacamole client`:

```
wget https://dlcdn.apache.org/guacamole/1.5.5/binary/guacamole-1.5.5.war
mv guacamole-1.5.5.war /etc/guacamole/guacamole.war
ln -s /etc/guacamole/guacamole.war /usr/share/tomcat/webapps/
```

Создайте зашифрованный пароль (укажите вместо **password** ваш пароль):

```
echo -n password | openssl md5

 (stdin)= 5f4dcc3b5aa765d61d8327deb882cf99
```

Сохраните вывод зашифрованного пароля. Он пригодится при следующем этапе настройки доступных подключений:

```
nano /etc/guacamole/user-mapping.xml
```

Содержимое:

```
<user-mapping>
 <!-- Per-user authentication and config information -->

  <!-- A user using md5 to hash the password
  guacadmin user and its md5 hashed password below is used to
  login to Guacamole Web UI-->
  <authorize
   username="admin"
   password="5f4dcc3b5aa765d61d8327deb882cf99"
   encoding="md5">
  <!-- First authorized Remote connection -->
   <connection name="ssh ro73">
   <protocol>ssh</protocol>
   <param name="hostname">192.168.1.43</param>
   <param name="port">22</param>
  </connection>

  <!-- Second authorized remote connection -->
   <connection name="rdp ro73">
   <protocol>rdp</protocol>
   <param name="hostname">192.168.1.43</param>
   <param name="port">3389</param>
   <param name="username">test</param>
   <param name="ignore-cert">true</param>
  </connection>
  </authorize>
</user-mapping>
```

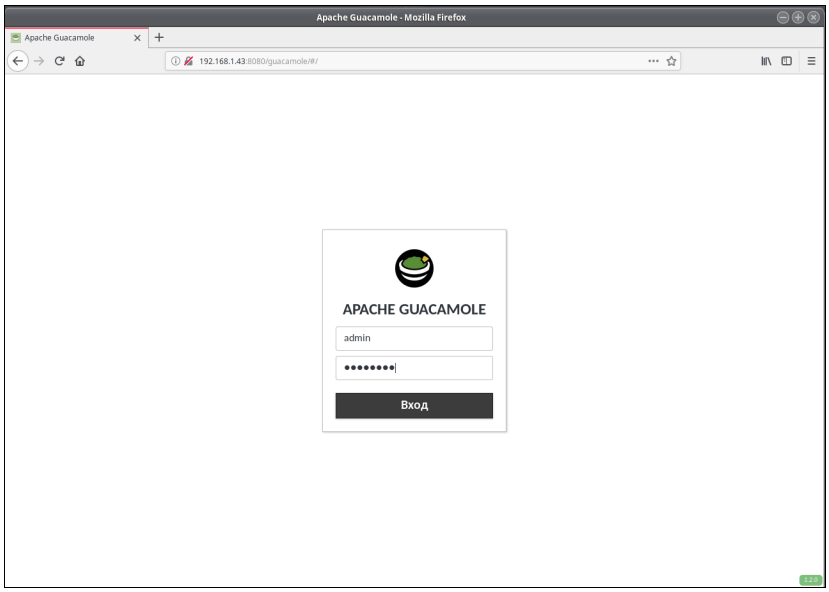
Выполните перезапуск необходимых служб:

```
systemctl restart tomcat guacd
```

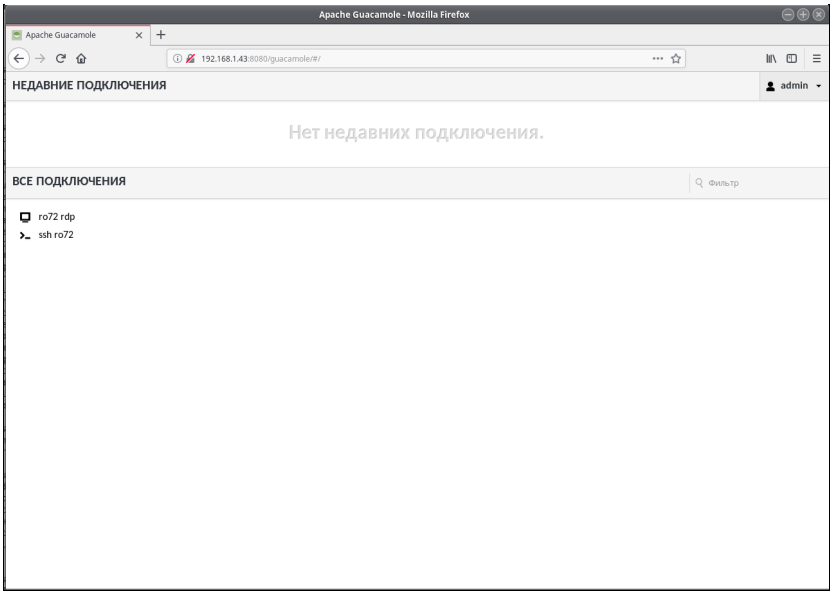
Веб-интерфейс

Для входа через веб-интерфейс в адресной строке браузера введите 192.168.1.43:8080/guacamole.

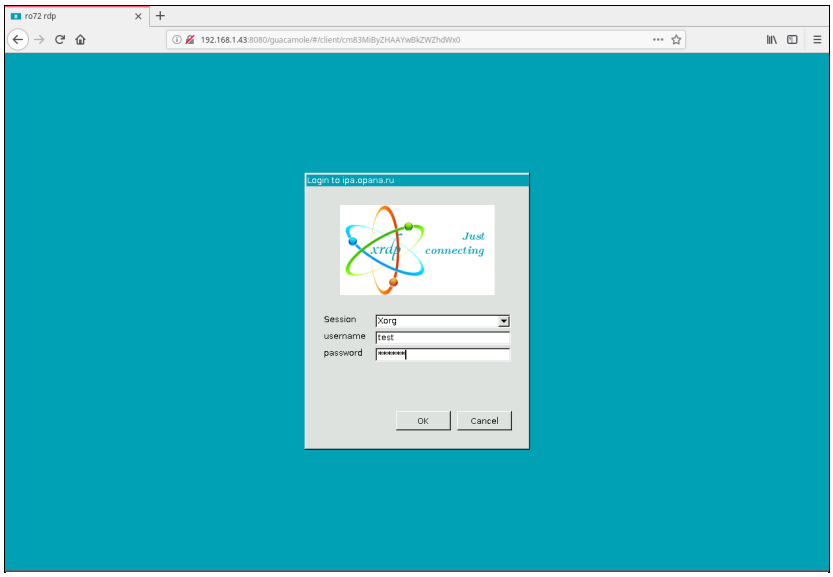
Будет открыта форма авторизации:



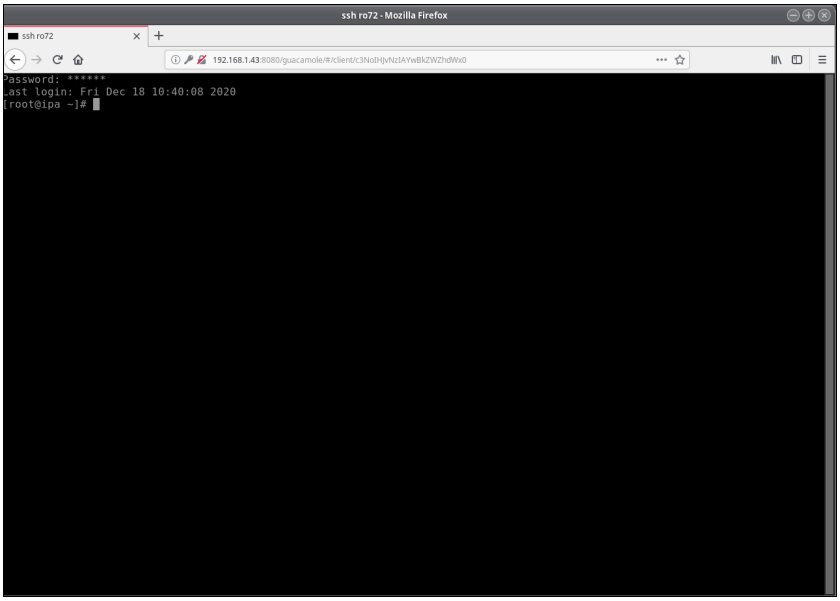
Доступные подключения:



Подключение по **RDP** (предварительно на данном ПК должен быть настроен XRDP-сервер).



Пример входа по **SSH**:



Remmina – клиент для подключения к удаленному рабочему столу

Установка Remmina и плагинов
Подключение устройств
Примеры использования Remmina
Решение возникающих проблем

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: remmina-1.4.27-4

Remmina — клиент удалённого рабочего стола, имеет лицензию *GPLv2+*.

Обычно используется для подключения к удаленному рабочему столу *Windows* (**RDP**), но также *Remmina* имеет возможности подключения с использованием следующих протоколов: **SSH, VNC, RDP, NX и XDMCP**.

Вы можете подробнее ознакомиться с возможностью осуществления удаленного подключения при помощи **Remmina**, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows;
- в **VK Видео** — Организация удаленного доступа с РЕД ОС на Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Установка Remmina и плагинов

Для установки данного приложения выполните команду:

```
dnf install remmina
```

При скачивании *Remmina* будут доступны следующие плагины: **EXEC, NX, RDP, RDPF, RDPS, SFTP, SPICE, SSH, ST, VNC, VNCI, XDMCP, glibsecret**.

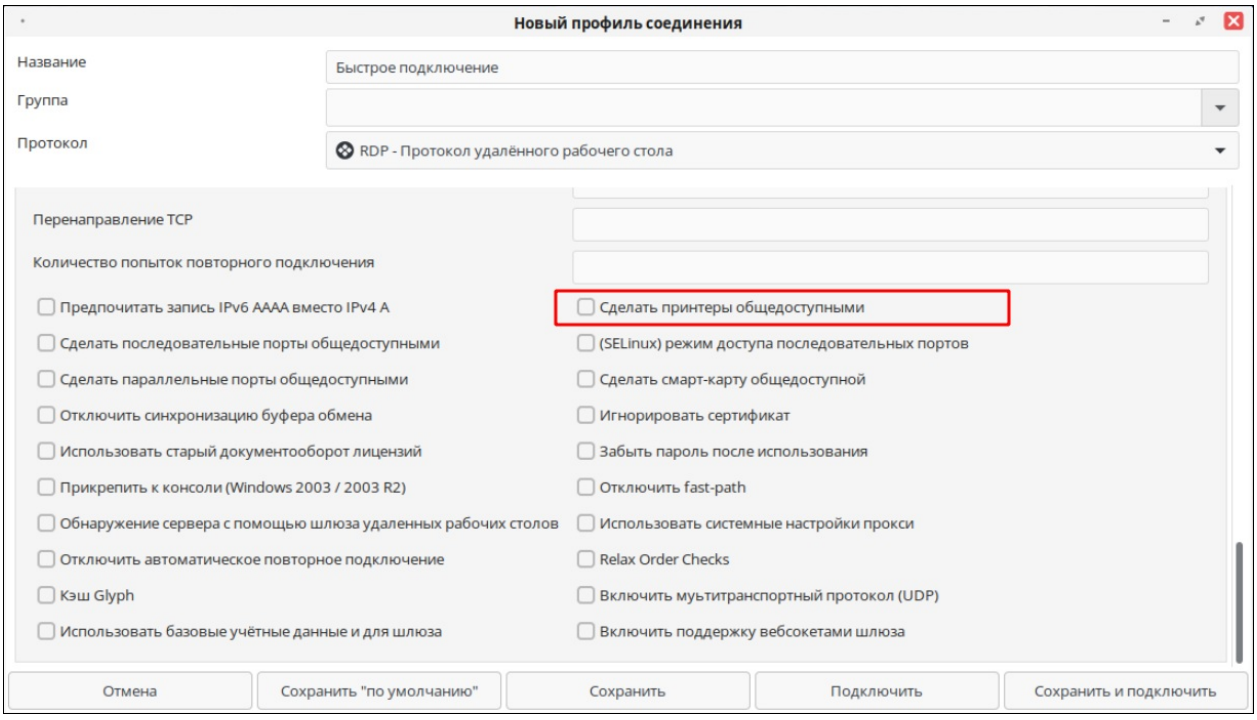
Для расширенной работы с приложением можно установить оставшиеся плагины следующей командой (с правами пользователя **root**):

```
dnf install remmina-gnome-session remmina-plugins-kwallet remmina-plugins-spice remmina-plugins-www
```

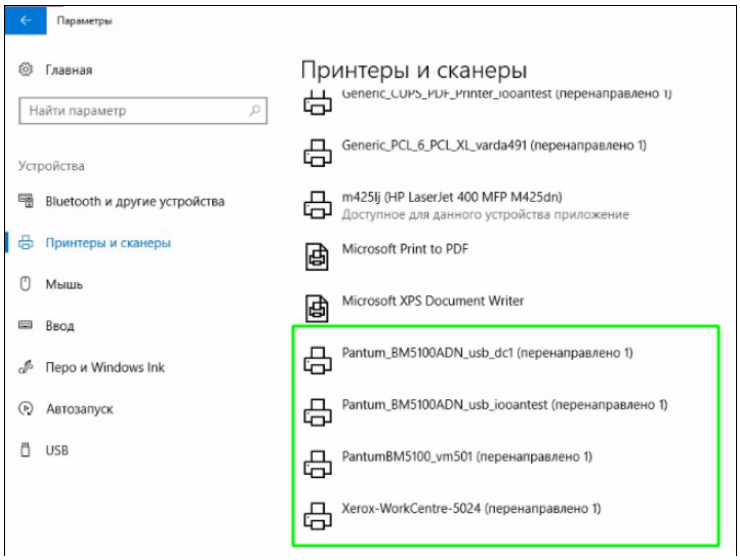
Подключение устройств

Перенаправление принтера в удаленный рабочий стол по протоколу RDP

Откройте параметры соединения, перейдите на вкладку «**Дополнительные**», установите флажок на строке «**Сделать принтеры общедоступными**».



Нажмите на кнопку «**Сохранить и подключить**», в результате локальный принтер будет перенаправлен в удаленный рабочий стол.



Вы можете подробнее ознакомиться с примером подключения локального принтера к удаленному рабочему столу, просмотрев наши обучающие видео:

- на **RuTube** — Подключение локального принтера к удаленному рабочему столу;
- в **Яндекс.Дзен** — Подключение локального принтера к удаленному рабочему столу;
- в **VK Видео** — Подключение локального принтера к удаленному рабочему столу.

На наших каналах вы также сможете найти много другой полезной информации.

Переназначение драйвера принтера

Иногда бывает недостаточным при перенаправлении принтера выбирать параметр «**Сделать принтеры общедоступными**», в результате наблюдаются ошибки при печати или принтеру может не назначиться признак «**По умолчанию**».

В данном случае в **Remmina** на вкладке «**Дополнительно**» можно попробовать определить параметр «**Переписать драйвер принтера**».

Формат данного поля следующий: первым указывается в двойных кавычках *имя принтера* на РЕД ОС, а вторым - *драйвер* в Windows.

Пример - **"Samsung_CLX-3300_Series":"Samsung CLX-3300 Series PS"**:



Перенаправление токенов в удаленный рабочий стол по протоколу RDP

В качестве примера будут рассмотрены токены **Рутокен ЭЦП** и **Aladdin R.D. JaCarta**.

Для перенаправления устройства необходимо указать идентификатор устройства (**ID**), определить его можно с помощью команды `pcsc_scan` (выполняется с правами **локального пользователя**).

Пример вывода команды для **Рутокен ЭЦП**:

```
pcsc_scan

Using reader plug'n play mechanism
Scanning present readers...
0: Aktiv Rutoken ECP 00 00

Sun May 28 22:02:03 2023
 Reader 0: Aktiv Rutoken ECP 00 00
  Event number: 0
  Card state: Card inserted,
  ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1

ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
+ TS = 3B --> Direct Convention
+ T0 = 8B, Y(1): 1000, K: 11 (historical bytes)
  TD(1) = 01 --> Y(i+1) = 0000, Protocol T = 1
-----
+ Historical bytes: 52 75 74 6F 6B 65 6E 20 44 53 20
  Category indicator byte: 52 (proprietary format)
+ TCK = C1 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
 Aktiv Rutoken ECP
 https://www.rutoken.ru/products/all/rutoken-ecp/
```

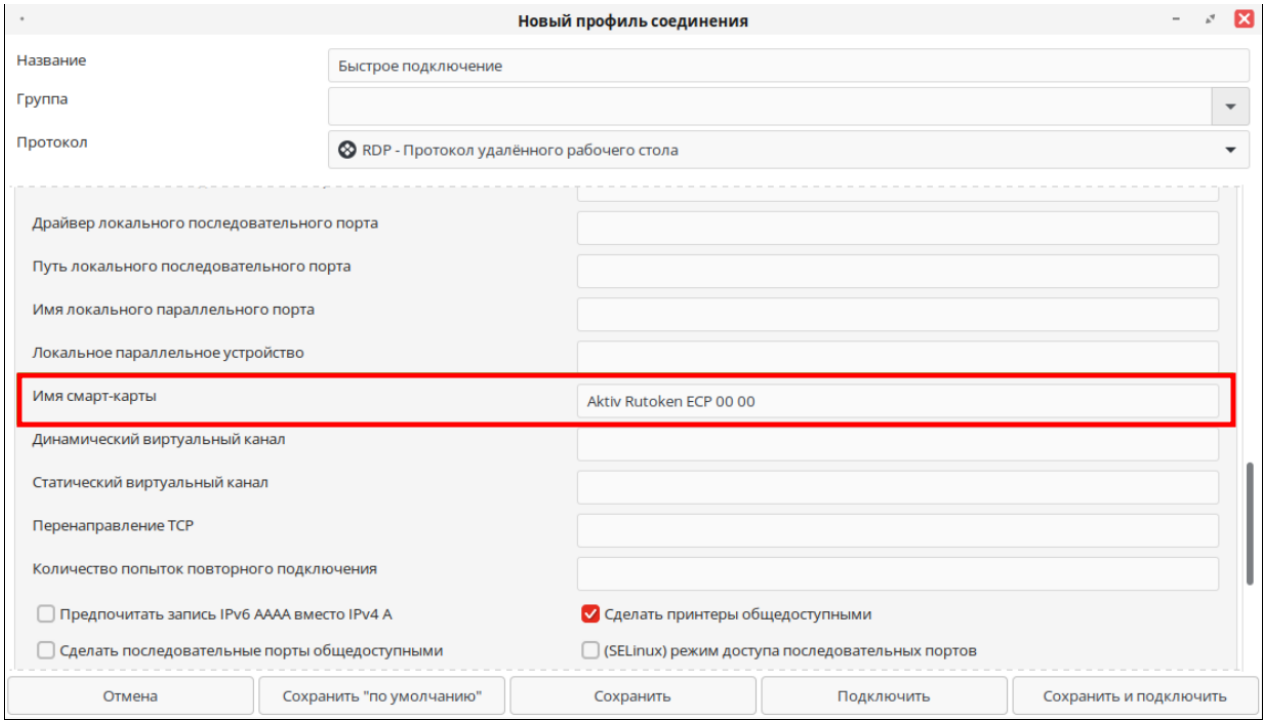
Пример вывода команды для **Aladdin R.D. JaCarta**:

```
pcsc_scan

Using reader plug'n play mechanism
Scanning present readers...
0: Aladdin R.D. JaCarta [SCR Interface] 00 00

Mon May 29 11:21:48 2023
 Reader 0: Aladdin R.D. JaCarta [SCR Interface] 00 00
  Event number: 0
  Card state: Card inserted,
  ATR: 3B DC 18 FF 81 91 FE 1F C3 80 73 C8 21 13 66 01 06 11 59 00 01 28

ATR: 3B DC 18 FF 81 91 FE 1F C3 80 73 C8 21 13 66 01 06 11 59 00 01 28
+ TS = 3B --> Direct Convention
+ T0 = DC, Y(1): 1101, K: 12 (historical bytes)
  TA(1) = 18 --> Fi=372, Di=12, 31 cycles/ETU
    129032 bits/s at 4 MHz, fMax for Fi = 5 MHz => 161290 bits/s
  TC(1) = FF --> Extra guard time: 255 (special value)
  TD(1) = 81 --> Y(i+1) = 1000, Protocol T = 1
-----
  TD(2) = 91 --> Y(i+1) = 1001, Protocol T = 1
-----
  TA(3) = FE --> IFSC: 254
  TD(3) = 1F --> Y(i+1) = 0001, Protocol T = 15 - Global interface bytes following
-----
  TA(4) = C3 --> Clock stop: no preference - Class accepted by the card: (3G) A 5V B 3V
```

```
 + Historical bytes: 80 73 C8 21 13 66 01 06 11 59 00 01
  Category indicator byte: 80 (compact TLV data object)
    Tag: 7, len: 3 (card capabilities)
      Selection methods: C8
        - DF selection by full DF name
        - DF selection by partial DF name
        - Implicit DF selection
      Data coding byte: 21
        - Behaviour of write functions: proprietary
        - Value 'FF' for the first byte of BER-TLV tag fields: invalid
        - Data unit in quartets: 2
      Command chaining, length fields and logical channels: 13
        - Logical channel number assignment: by the card
        - Maximum number of logical channels: 4
    Tag: 6, len: 6 (pre-issuing data)
      Data: 01 06 11 59 00 01
+ TCK = 28 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B DC 18 FF 81 91 FE 1F C3 80 73 C8 21 13 66 01 06 11 59 00 01 28
 JaCarta (PKI)
 http://www.aladdin-rd.ru
```

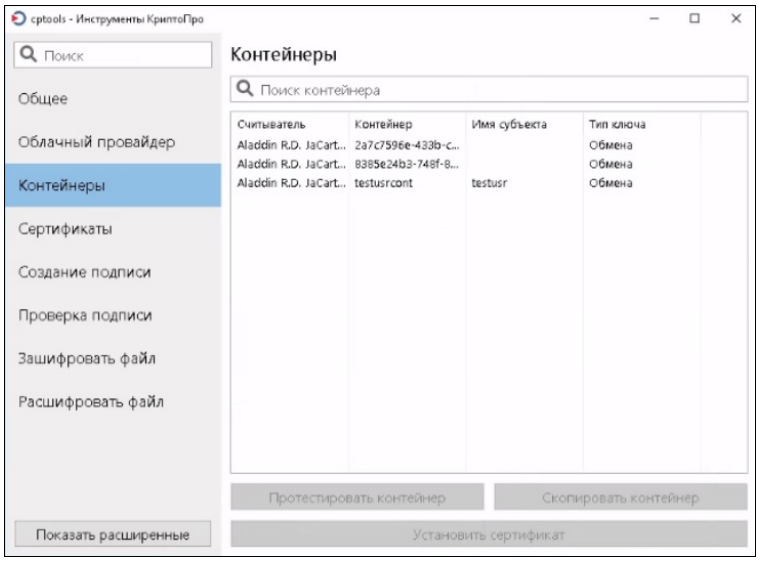
В выводе команды из строки «**Reader 0**» необходимо скопировать идентификатор устройства.

В Remmina в новом профиле соединения на вкладке «**Дополнительные**» в поле «**Имя смарт-карты**» укажите **ID** устройства из команды `pcsc_scan`.



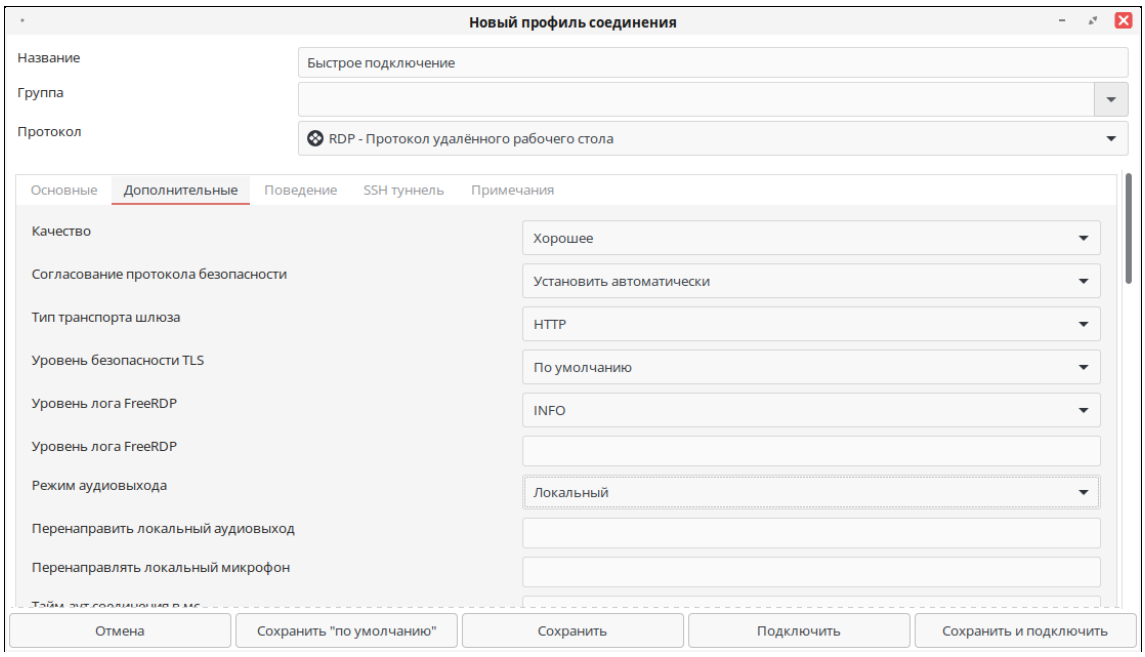
Затем нажмите на кнопку «**Сохранить**».

Пример успешного перенаправления токенов можно просмотреть в утилите «**Инструменты КриптоПРО**».



Перенаправление звука на удаленный рабочий стол

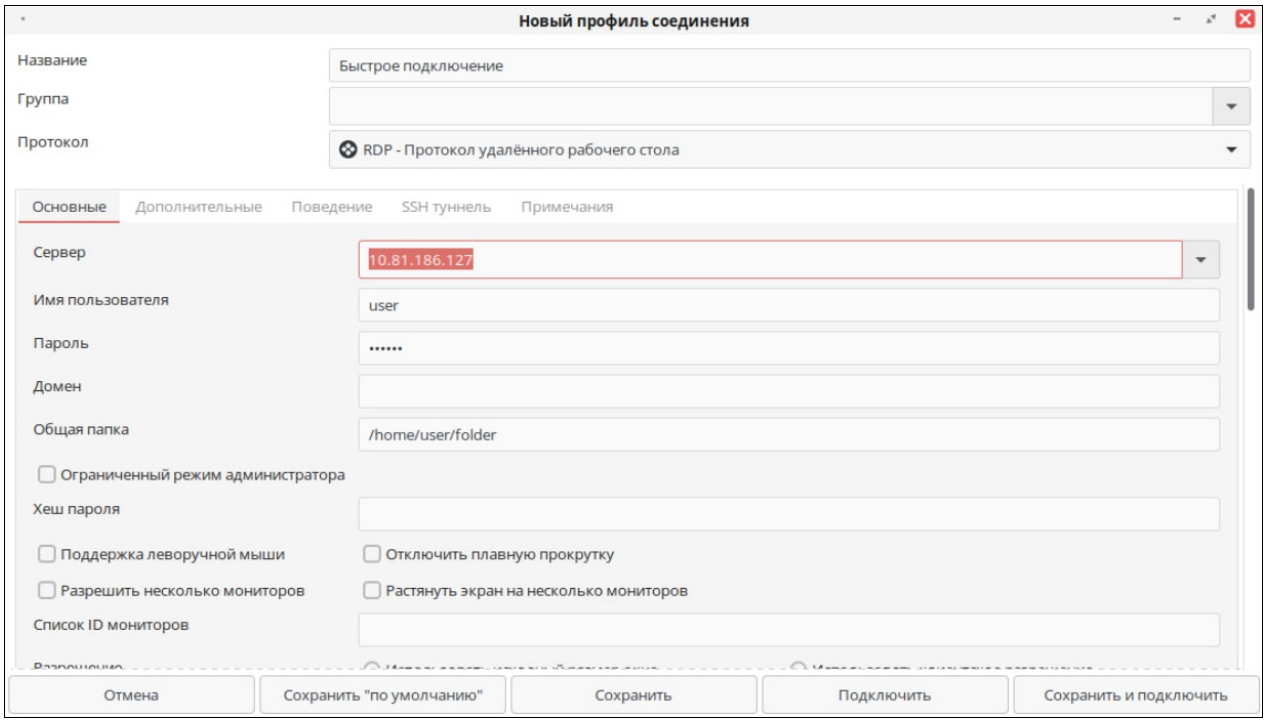
Откройте профиль соединения в «**Профиль соединения**», во вкладке «**Дополнительные**» для параметра «**Режим аудиовыхода**» в диалоговом окне выпадающего списка выберите значение «**Локальный**».



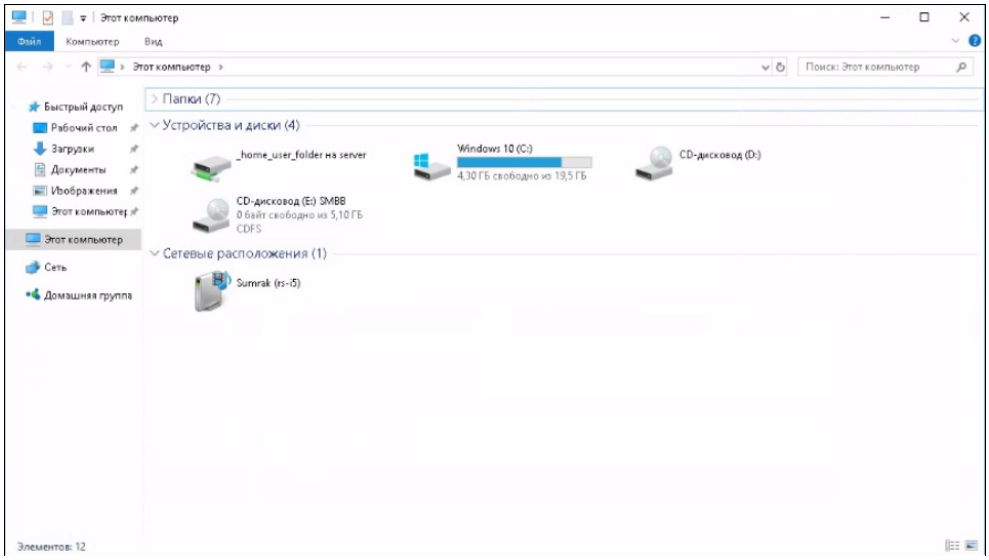
Нажмите на кнопку «**Сохранить и подключить**». Теперь звук будет передаваться на удаленный компьютер.

Общий доступ к локальным каталогам или Flash-носителю в удаленном рабочем столе

Откройте профиль соединения в «**Профиль соединения**», далее во вкладке «**Основные**» в диалоговом окне выпадающего списка директорий параметра «**Общая папка**» выберите нужный каталог или диск.



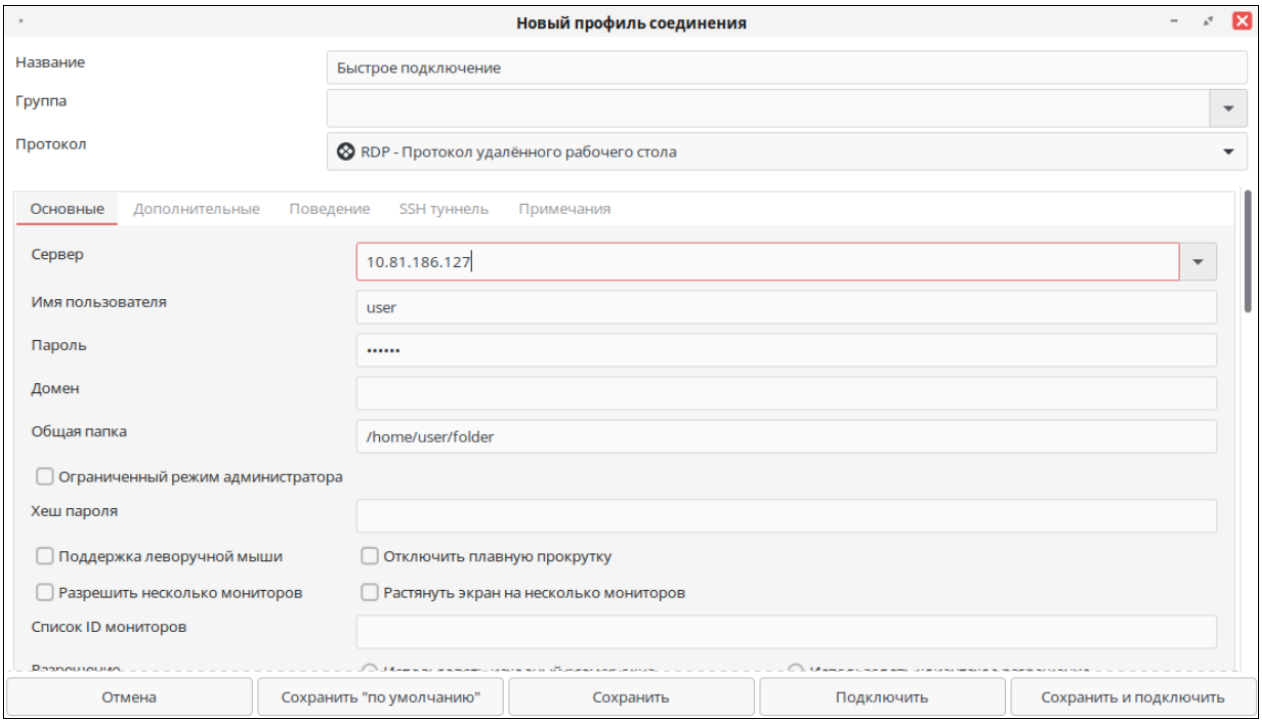
Нажмите на кнопку «**Сохранить и подключить**». Выбранная папка станет доступной для использования в удаленном рабочем столе.



Примеры использования Remmina

Установка подключения к Windows (для примера используется Windows 10 Pro)

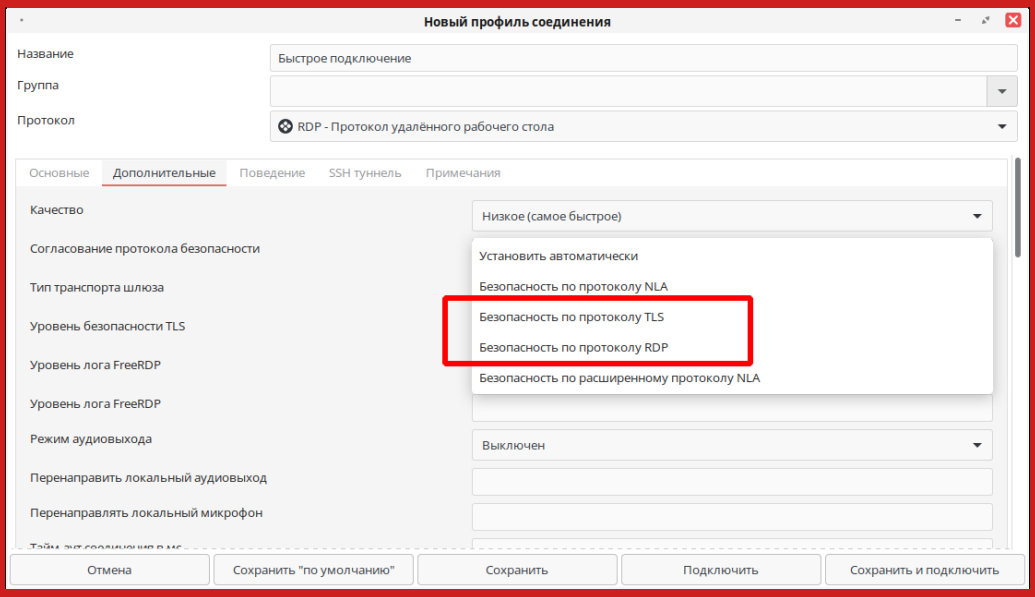
Для установки соединения нажмите на кнопку «**Добавить новый профиль соединения**». Откроется окно создания соединения, где вам нужно выбрать протокол **RDP** и заполнить поля «**Сервер**», «**Имя пользователя**» и «**Пароль**».



После заполнения полей нажмите на кнопку «**Сохранить**» - для сохранения настроек или на кнопку «**Сохранить и подключить**» - для сохранения настроек и подключения к удаленному рабочему столу.

ВАЖНО!

Если возникла проблема с закрытием **Remmina** при повторном подключении к windows-серверу по протоколу **RDP**, рекомендуется в настройках соединения на вкладке «**Дополнительные**» для параметра **Согласование протокола безопасности** использовать «**Безопасность по протоколу TLS**» или «**Безопасность по протоколу RDP**».

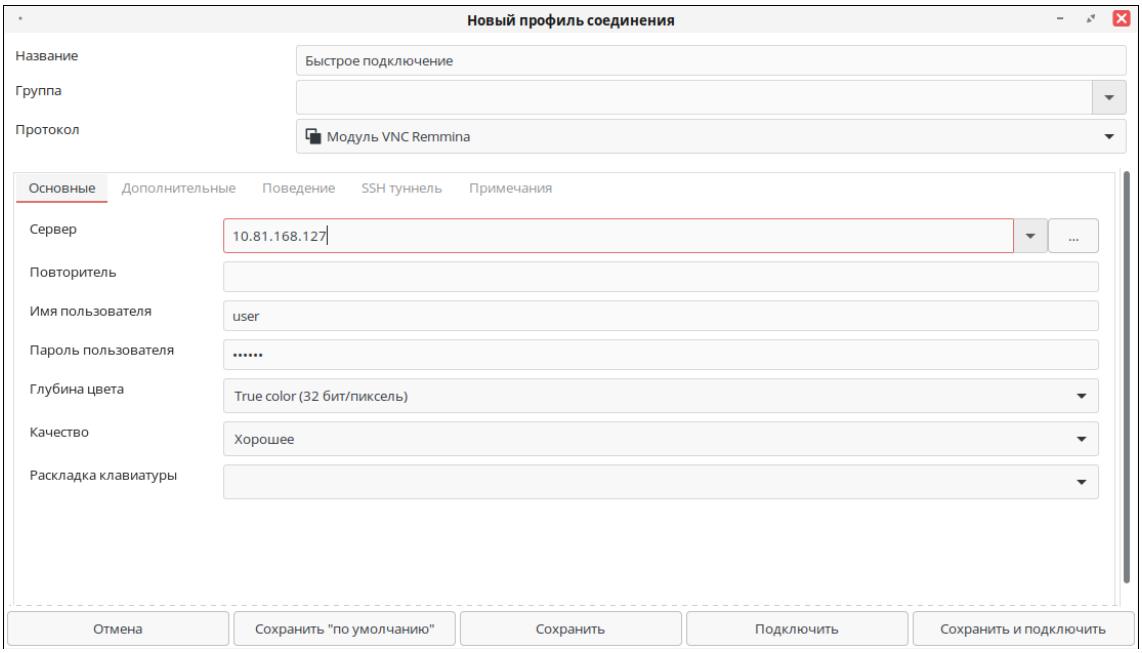


Для подключения по протоколу безопасности **TLS** может понадобится снять чекбокс «**Разрешить подключение только с компьютеров, на которых работает удалённый рабочий стол с проверкой подлинности на уровне сети**» в дополнительных параметрах windows-сервера.

Для подключения по протоколу безопасности **RDP** на windows-сервере требуется поменять регистр **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer** на **0**.

Установка подключения к x11vnc-серверу с использованием протокол VNC

В новом профиле соединения из выпадающего списка параметра «**Протокол**» выберите «**Модуль VNC Remmina**». Также заполните поля «**Имя пользователя**» и «**Пароль**». В поле «**Сервер**» впишите IP-адрес хоста вашей машины и порт VNC.



Для подключения нажмите на кнопку «**Подключить**» или «**Сохранить и подключить**».

Решение возникающих проблем

В случае возникновения ошибок в Remmina при повторном подключении к Windows-серверу необходимо проверить используемый протокол безопасности в параметре «**Согласование протокола безопасности**», скорее всего параметр имеет значение «**Безопастность по протоколу NLA**».

Для решения данной проблемы значение параметра следует установить «**Безопасность по протоколу TLS**» или «**Безопасность по протоколу RDP**».

> **Примечание.**
>
> Данные протоколы безопасности должны поддерживаться на вашем Windows-сервере.

Если использование других протоколов безопасности невозможно, рекомендуется использовать **xfreerdp-gui**. Подробную информацию о настройке подключения через **xfreerdp-gui** см. в нашей инструкции «xfreerdp_gui — графическая оболочка для работы с freerdp».

Сервер для подключения к удаленному рабочему столу vino

Установка Vino
Использование Vino
Добавление Vino в автозагрузку
Настройка Vino
Настройка Vino через терминал

Vino — это сервер VNC (Virtual Network Computing), позволющий удаленно подключаться к вашему рабочему столу.

Установка Vino

Чтобы установить пакет vino, необходимо выполнить команду:

```
dnf install vino
```

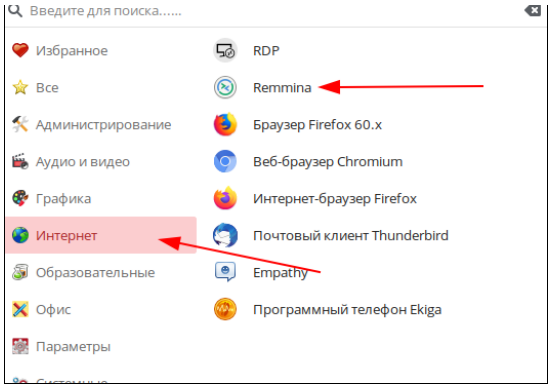
Использование Vino

После установки Vino можно использовать и подключаться удаленно без предварительной настройки. Для этого необходимо запустить сервер:

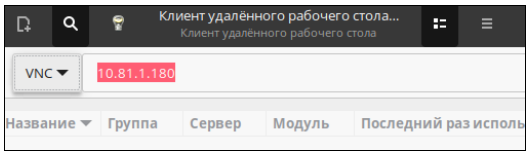
```
/usr/libexec/vino-server
```

Далее запускаем клиентское приложение, через которое будем соединяться с сервером.

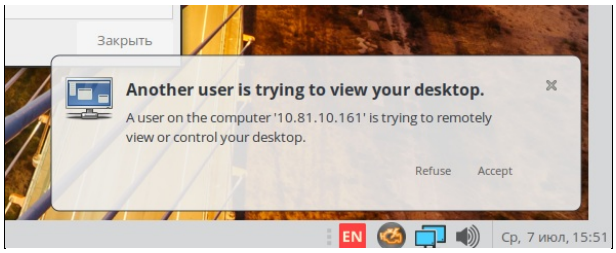
Например, «Remmina», это приложение уже имеется в составе РЕД ОС:



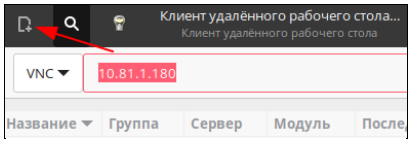
Следующим шагом, указываем ip-адрес сервера и выбираем протокол VNC:



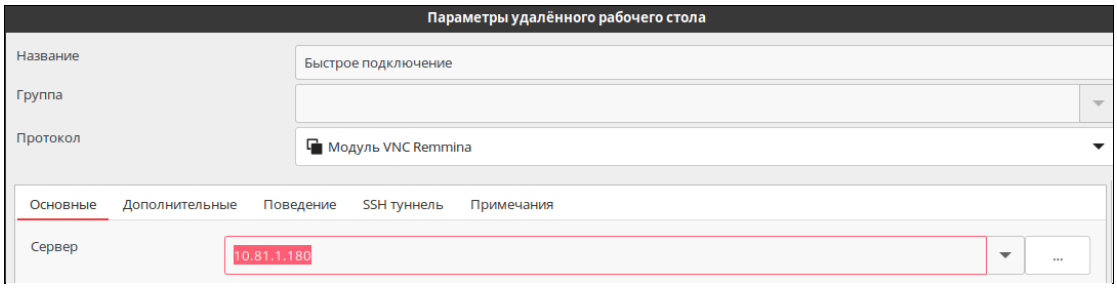
После подключения необходимо будет принять запрос на сервере о подключении:



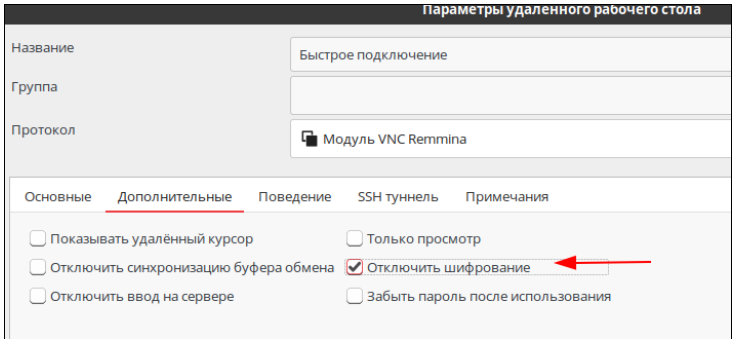
При проблемах с подключением необходимо отключить шифрование. Для этого нажимаем на значок создания нового профиля:



Далее выставляем следующие настройки:



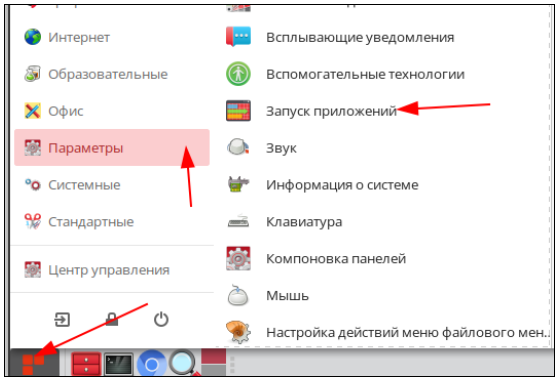
Затем переходим во вкладку «Дополнительные» и ставим галочку на пункте «Отключить шифрование».



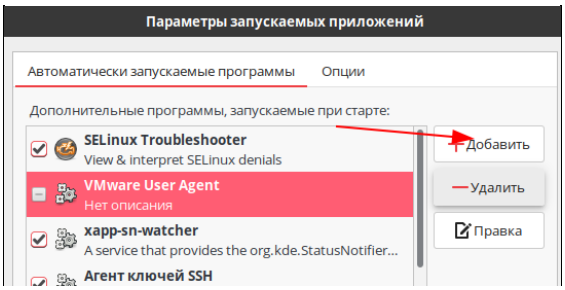
Нажимаем «Подключить».

Добавление Vino в автозагрузку

Для того чтобы не запускать Vino каждый раз при запуске системы и не занимать данной программой рабочее пространство, Vino можно добавить в автозагрузку средствами системы. Для этого открываем «Запуск приложений»:

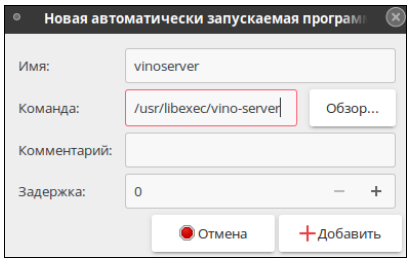


Нажимаем «Добавить».



Присваиваем название приложению и команду запуска:

```
/usr/libexec/vino-server
```



Нажимаем «Добавить».

После перезагрузки системы служба запустится автоматически.

Настройка Vino

Настройку Vino можно осуществлять через графическую утилиту dconf-editor:

```
dnf install dconf-editor
```

Для настройки запускаем утилиту:

```
dconf-editor
```

Настройки Vino находятся по пути: **org→gnome→desktop→remote-access.**

Все настройки имеют свое описание, рассмотрим основные из них:

- *alternative-port* — устанавливает порт для сервера, по умолчанию 5900;
- *authentication-method* — устанавливает метод аутентификации, имеет два режима:
  - *none* — без аутентификации;
  - *vnc* — с использованием пароля vnc для допуска пользователя к удаленному управлению;

- *disable-background* — отключает показ изображения рабочего стола, когда удаленный пользователь берет управление, имеет значения true/false;
- *disable-xdamage* — отключает расширение Xdamage для X.org, имеет значения true/false;
- *lock-screen-on-disconnect* — отвечает за блокировку экрана при отсоединении пользователя, имеет значения true/false;
- *icon-visibility* — отвечает за отображение значка удаленного подключения во время подключения, имеет три режима:
  - *always* — значок отображается всегда;
  - *client* — значок отображается только когда кто-то подключен;
  - *never* — значок никогда не отображается;

- *mailto* - этот ключ указывает адрес электронной почты, на который должен быть отправлен URL-адрес удаленного рабочего стола, если пользователь щелкает URL-адрес в диалоговом окне настроек общего доступа к рабочему столу;
- *network-interface* — устанавливает интерфейс, через который будет осуществляться соединения, например, eth0;
- *notify-on-connect* — отвечает за отображение уведомления о том, что пользователь подключился;
- *prompt-enabled* — отвечает за запрос о подключении, при значении true, каждый раз при подключении будет выводиться окно о том, что удаленный пользователь пытается подключиться, при значении false подключение происходит без запроса;
- *require-encryption* — отвечает за шифрование для обеспечения надежного соединения;
- *view-only* — дает доступ только на просмотр, без возможности управления;
- *use-alternative-port* — позволяет использовать порт, указанный в настройке alternative-port, имеет значения true/false;
- *use-upnp* — если true, создается запрос маршрутизатору о том, чтобы открыть используемый Vino порт;
- *vnc-password* — устанавливает пароль для vnc аутентификации.

Для применения настроек может понадобиться перезагрузка.

Настройка Vino через терминал

Вышеуказанные параметры можно регулировать при помощи команд терминала, для этого необходимо использовать команду в следующем виде:

```
gsettings set org.gnome.Vino <параметр> <значение>
```

Например, для того чтобы установить пароль и отключить запрос при подключении, используется следующий список команд: Включаем метод аутентификации vnc:

```
gsettings set org.gnome.Vino authentication-methods "['vnc']"
```

Задаем пароль vnc, например, 123123:

```
gsettings set org.gnome.Vino vnc-password $(echo -n '123123' | base64)
```

Отключаем запрос подтверждения подключения удаленного пользователя:

```
gsettings set org.gnome.Vino prompt-enabled false
```

Утилита удаленного запуска графических приложений xpra

Установка
Основные возможности
Запуск приложения
Запуск новой графической сессии
Получение управления запущенной графической сессией на удаленной машине
TCP-сокеты
Графический интерфейс xpra

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** xpra-5.0.8-1

Утилита **xpra** — инструмент, который запускает программы X11, обычно на удаленном хосте, и направляет их отображение на локальный компьютер без потери состояния. Предоставляет удаленный доступ как отдельным приложениям, так и новым или существующим сеансам рабочего стола.

На сервере утилита **xpra** в режиме демона запускает программу с заданным идентификатором сеанса, а на клиенте происходит присоединение к этому сеансу с идентификатором.

Доступ к сеансам можно получить по **SSH** или через защищенные паролем обычные TCP-сокеты с SSL или без него.

Установка

Для установки утилиты **xpra** в РЕД ОС 7.3 на сервере и на клиенте перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду в терминале:

```
dnf install xpra
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Выйдите из сеанса суперпользователя **root**:

```
exit
```

После установки запуск утилиты доступен из «**Главного меню**» - «**Интернет**» - «**Xpra**» или через терминал командой:

```
xpra
```

Основные возможности

Просмотр списка запущенных xpra-серверов на текущей машине текущим пользователем осуществляется командой:

```
xpra list

Found the following xpra sessions:
/run/user/1000/xpra:
LIVE session at :0
LIVE session at :1
LIVE session at :2
LIVE session at :3
LIVE session at :4
LIVE session at :5
```

Остановка **xpra** на указанном дисплее (если сервер один, дисплей можно не указывать) осуществляется командой:

```
xpra stop :0
```

```
server requested disconnect:
server shutdown
xpra at :0 has exited.
```

Для остановки сервера на удаленной машине выполните команду:

```
xpra stop ssh://user@10.81.1.130/1

user@10.81.1.130's password:
server requested disconnect:
server shutdown
Sent shutdown command
```

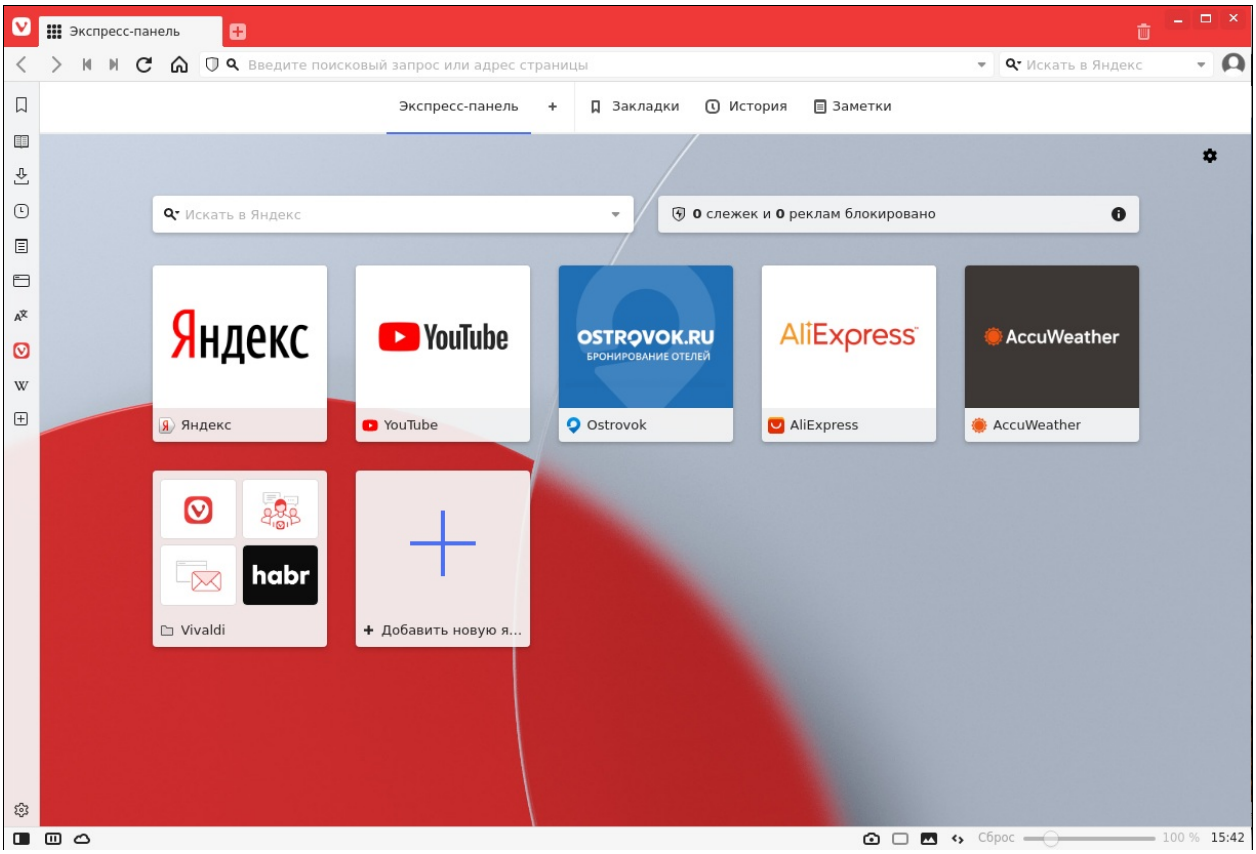
Для запуска **xpra** сервера на указанном дисплее выполните команду:

```
xpra start :1

using systemd-run to wrap 'start' server command
'systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' ':1' '--systemd-run=no'
Running scope as unit: run-rd9a968d02afd45c3b8da0197d39aea1e.scope
WARNING: low display number: 1
You are attempting to run the xpra server
against a low X11 display number: ':1'.
This is generally not what you want.
You should probably use a higher display number
just to avoid any confusion and this warning message.
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/:1.log.new
```

Запуск приложения

Для запуска приложения (на примере браузера **Vivaldi**) удалённо через **SSH** без предварительного запуска **xpra** на сервере, выполните команду:

```
xpra start ssh://user@10.81.1.130 --start="vivaldi"
```



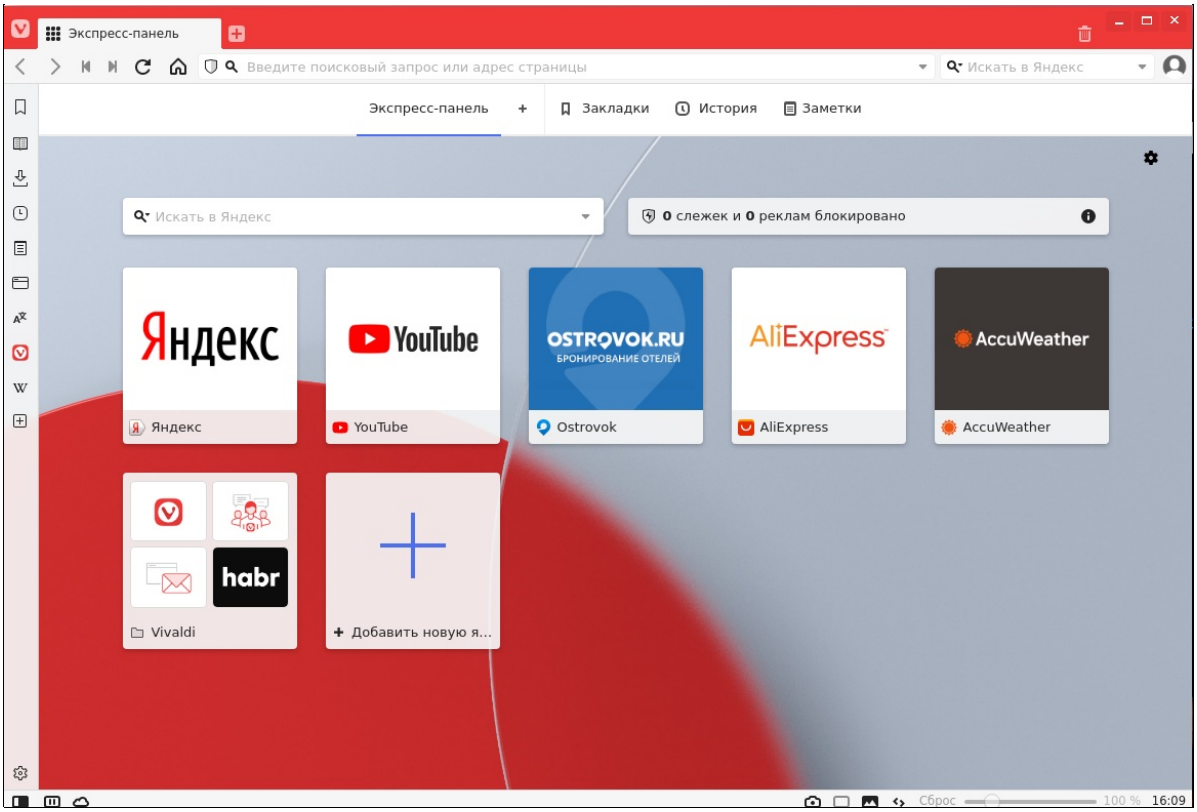
Далее будет рассмотрен запуск приложения (на примере браузера **Vivaldi**) с предварительным запуском **xpra**.

Запустите **xpra**, автоматически выберите дисплей и запустите программу:

```
xpra start --start=vivaldi

using systemd-run to wrap 'start' server command
'systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' '--start=vivaldi' '--systemd-run=no'
Running scope as unit: run-rbe185189832e44dab4cf2e624170b2b5.scope
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/S9507.log
Actual display used: :2
Actual log file name is now: /run/user/1000/xpra/:2.log
```

Подключение выполняется командой:

```
xpra attach ssh://user@10.81.1.130/2
```



Запуск новой графической сессии

Для запуска новой графической сессии на сервере необходимо запустить вложенный сервер **X11**, выполнив команду:

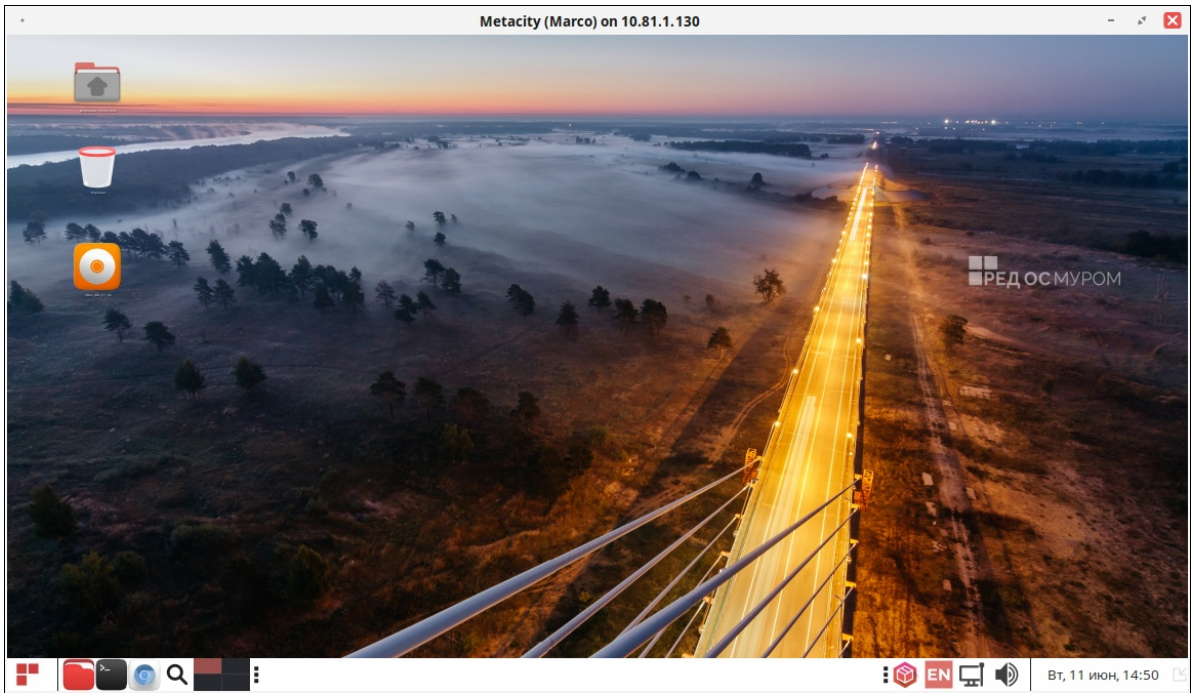
```
xpra start-desktop :1 --start-child=mate-session --exit-with-children=yes

using systemd-run to wrap 'start-desktop' server command
'systemd-run' '--description' 'xpra-start-desktop' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start-desktop' ':1' '--start-child=mate-session' '--exit-with-children=yes' '--systemd-run=no'
Running scope as unit: run-rd3c1ca4fcb5b42908297daef2392939c.scope
WARNING: low display number: 1
You are attempting to run the xpra server against a low X11 display number: ':1'.
This is generally not what you want.
You should probably use a higher display number just to avoid any confusion and this warning message.
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/:1.log.new
Actual log file name is now: /run/user/1000/xpra/:1.log
```

где:

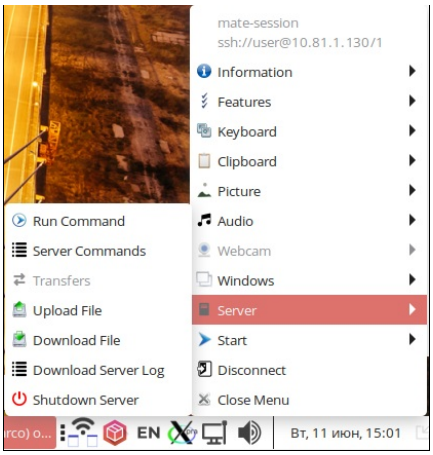
- **:1** — это номер сеанса отображения дисплея;
- **--start-child=mate-session** — запуск mate сессии как дочернего элемента на сервере **xpra**;
- **--exit-with-children=yes** — сервер будет закрыт после выхода из сессии (дочерний выход).

Подключение к графической сессии выполняется командой:

```
xpra attach ssh:user@10.81.1.130:1 --min-size=1200x800 --clipboard-direction=both --clipboard=yes
```



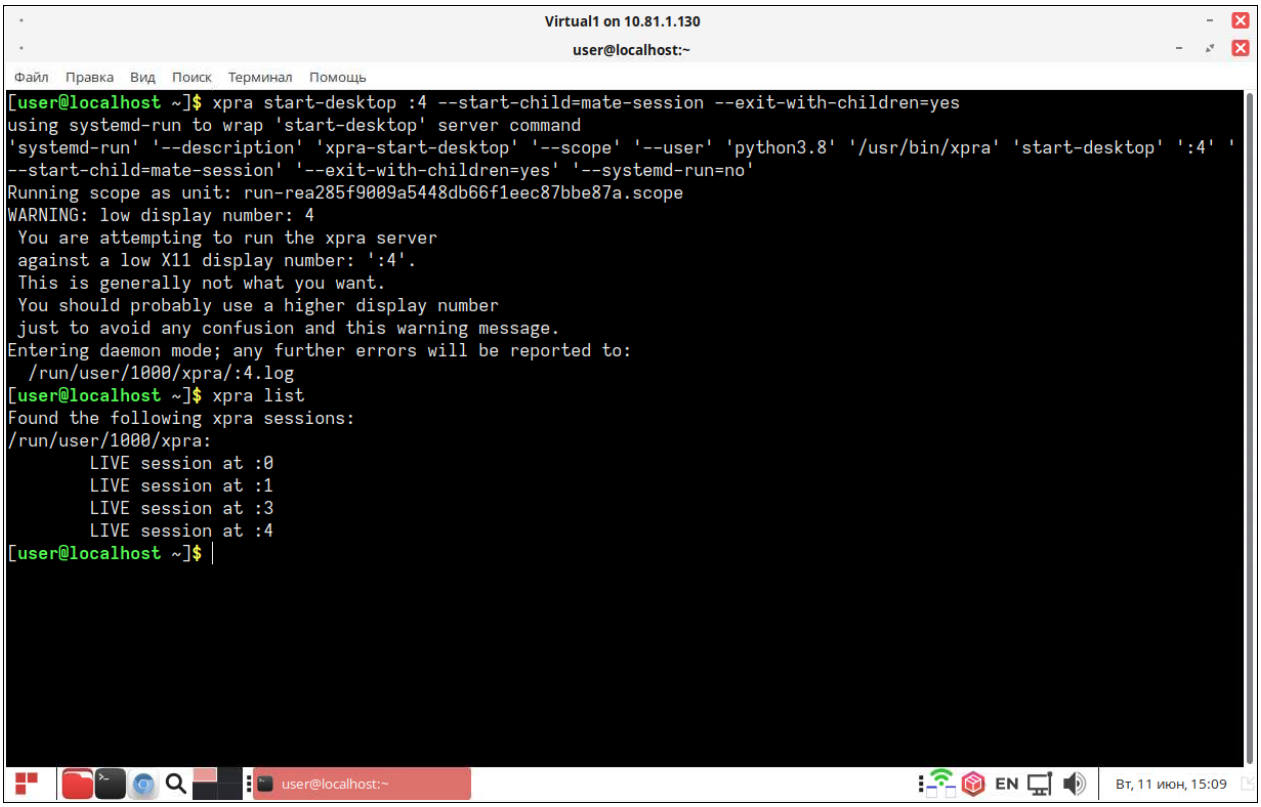
При подключении к серверу **xpra** в системном трее появится значок, где можно управлять подключением и изменять настройки.



Получение управления запущенной графической сессией на удаленной машине

Для удаленного запуска выполните команду:

```
xpra shadow --ssh=ssh ssh://user@10.81.1.130/0
```

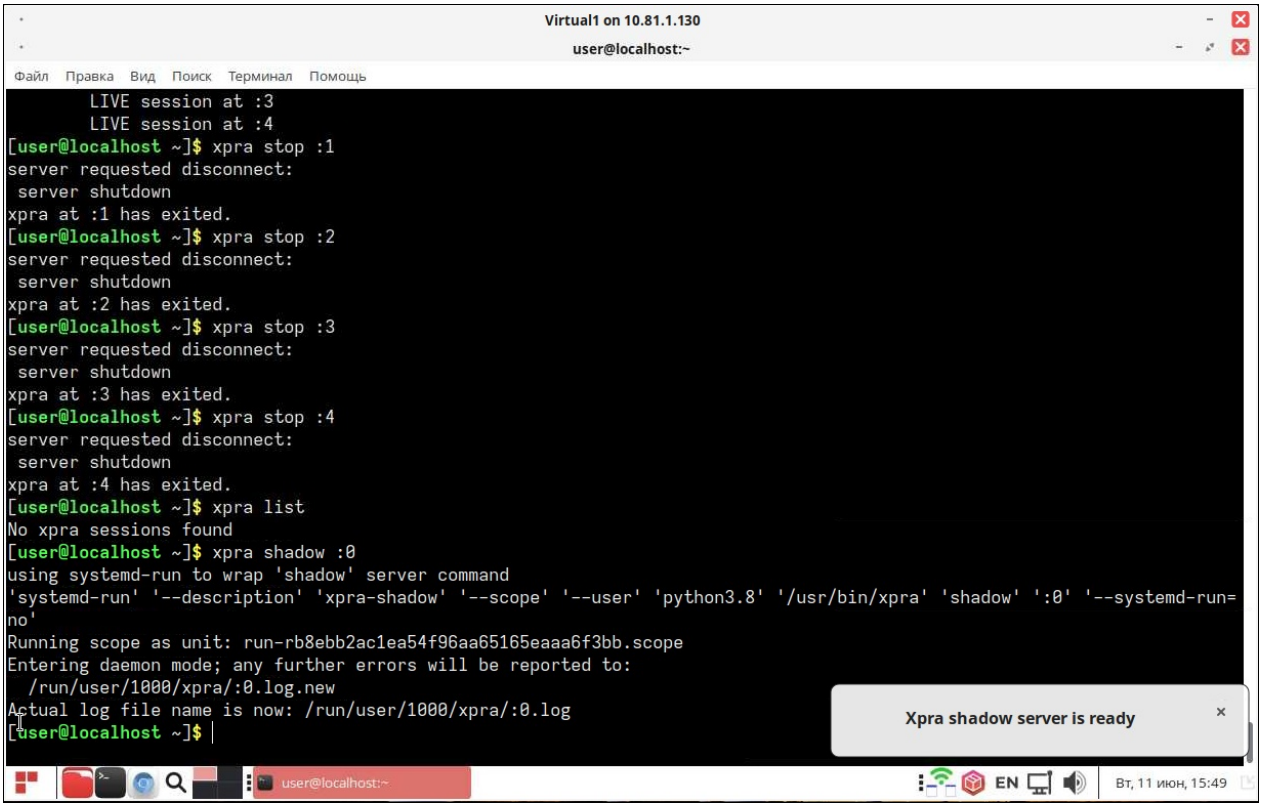


Для запуска на сервере выполните команду:

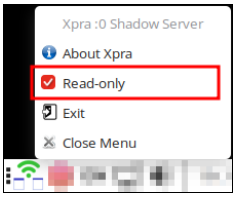
```
xpra shadow :0

using systemd-run to wrap 'shadow' server command
'systemd-run' '--description' 'xpra-shadow' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'shadow' ':0' '--systemd-run=no'
Running scope as unit: run-r711bde6c5e9143839c23798b8cdaea87.scope
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/:0.log.new
Actual log file name is now: /run/user/1000/xpra/:0.log
```

А также команду для подключения к серверу на удаленной машине:

```
xpra attach --speaker=no ssh://user@10.81.1.130
```



На сервере в трее появится значок, где «**Exit**» - остановить сервер, «**Read Only**» - запретить управление, разрешен только просмотр.



TCP-сокеты

Для запуска приложения (на примере браузера **Vivaldi**) на сервере выполните команду:

```
xpra start --start=vivaldi --bind-tcp=0.0.0.0:9878

using systemd-run to wrap 'start' server command
'systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' '--start=vivaldi' '--bind-tcp=0.0.0.0:9878' '--systemd-run=no'
Running scope as unit: run-r6a6a67cc4fb74ff18ae9e6f1dd7b16e3.scope
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/S12703.log
Actual display used: :1
Actual log file name is now: /run/user/1000/xpra/:1.log
```

Для управления запущенной графической сессией используется команда:

```
xpra shadow --bind-tcp=0.0.0.0:9878

using systemd-run to wrap 'shadow' server command
'systemd-run' '--description' 'xpra-shadow' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'shadow' '--bind-tcp=0.0.0.0:9878' '--systemd-run=no'
Running scope as unit: run-r2da092cb198b4764a93e72094bff097f.scope
Entering daemon mode; any further errors will be reported to:
 /run/user/1000/xpra/:0.log.new
Actual log file name is now: /run/user/1000/xpra/:0.log
```

Выполните подключение на удаленной машине командой:

```
xpra attach ws://10.81.1.130:9878
```

Адрес **10.81.1.130:9878** можно открыть в веб-браузере.

Для создания TCP-сеанса, начиная с версии **4.0.1**, с защитой паролем, выполните одну из приведенных команд:

```
XPRA_PASSWORD=<ваш_пароль> xpra start --bind-tcp=0.0.0.0:10000,auth=env
SOME_OTHER_ENV_VAR_NAME=<ваш_пароль> xpra start --bind-tcp=0.0.0.0:10000,auth=env:name=SOME_OTHER_ENV_VAR_NAME
xpra start --bind-tcp=0.0.0.0:10000,auth=password:value=<ваш_пароль>
```

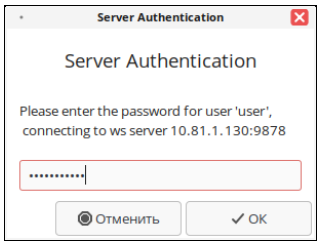
Например, команда для создания TCP-сеанса, защищенного паролем, с запуском текстового редактора **Pluma** будет выглядеть следующим образом:

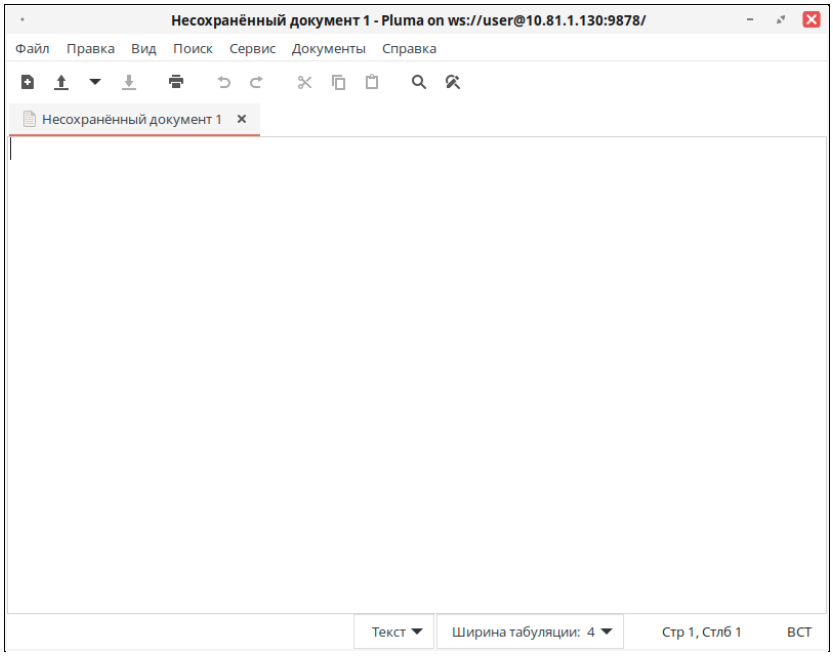
```
xpra start --start=pluma --bind-tcp=0.0.0.0:9878,auth=password:value=password123

using systemd-run to wrap 'start' server command
'systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' '--start=pluma' '--bind-tcp=0.0.0.0:9878,auth=password:value=password123' '--systemd-run=no'
Running scope as unit: run-r46fa07c9510342e4a5b9938988201a52.scope
Entering daemon mode; any further errors will be reported to:
 /run/user/1000/xpra/S14277.log
Actual display used: :1
Actual log file name is now: /run/user/1000/xpra/:1.log
```

При подключении необходимо указать имя пользователя:

```
xpra attach ws:user@10.81.1.130:9878
```

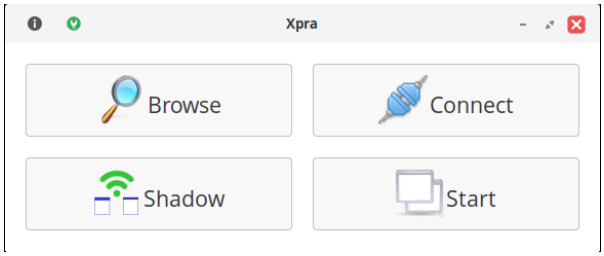
и по запросу ввести пароль:





Графический интерфейс xpra

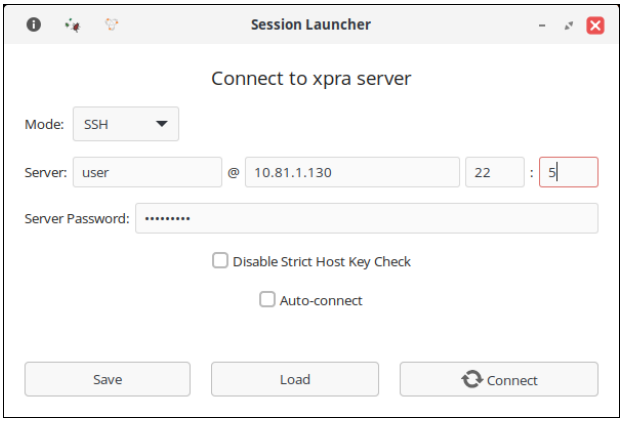
Графический интерфейс **xpra** доступен из «**Главного меню**» - «**Интернет**» - «**Xpra**».



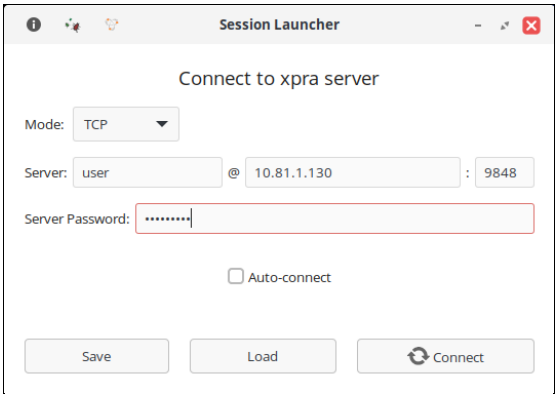
Здесь:

- «**Browse**» - просмотр списка, подключение к локальному дисплею.
- «**Shadow**» - предоставление доступа к рабочему столу.
- «**Connect**» - подключение к удаленному серверу.
- «**Start**» - запуск сервера **xpra**.

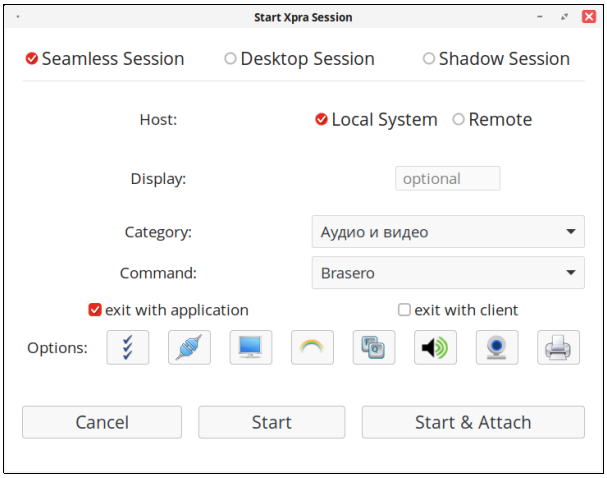
Настройка подключения по **SSH** выглядит следующим образом:



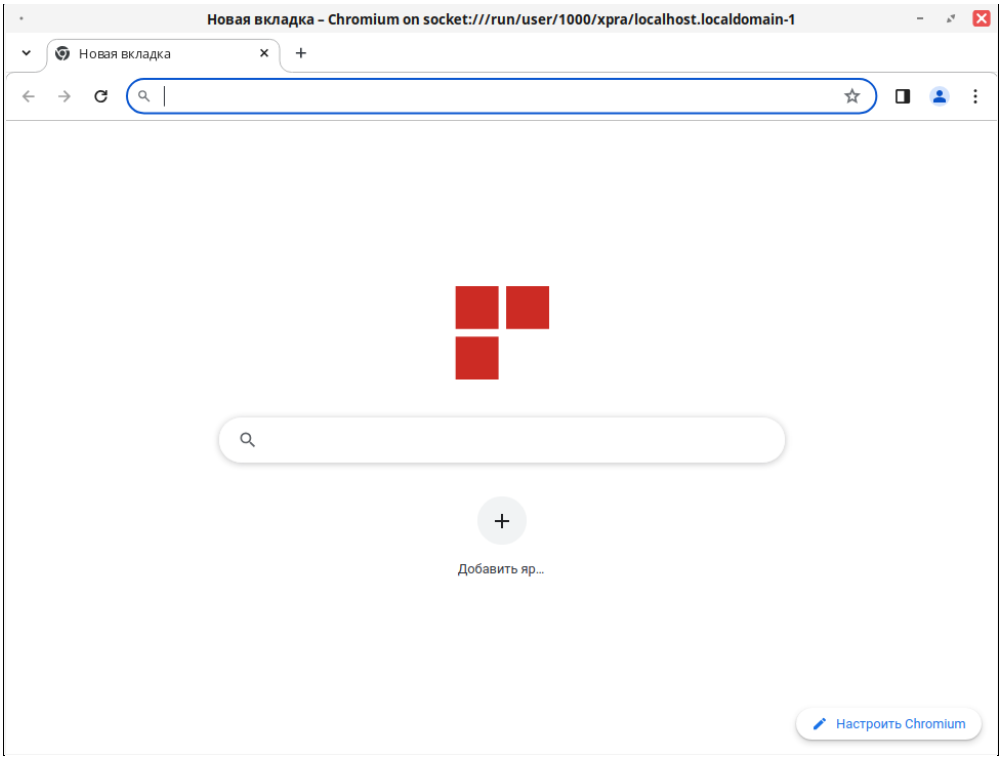
Настройка подключения по **TCP** выглядит следующим образом:



Запуск приложения в удаленной системе с отображением на локальном компьютере (на примере браузера **Chromium**):



Результат выполнения настройки:



Клиентская программа для работы с сетевыми протоколами PuTTY

Установка программы
Работа с программой
Авторизация по ключу SSH

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: putty-0.77-1

PuTTY — клиентская программа для удаленного подключения к серверам. **PuTTY** использует для работы такие безопасные сетевые протоколы, как *SSH*, *Telnet*, *SFTP*, *SCP* и др.

Программа применяется для администрирования удаленных машин.

К преимуществам программы можно отнести поддержку *IPv6*, поддержку аутентификации с открытым ключом и возможность работы через прокси-сервер.

Установка программы

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

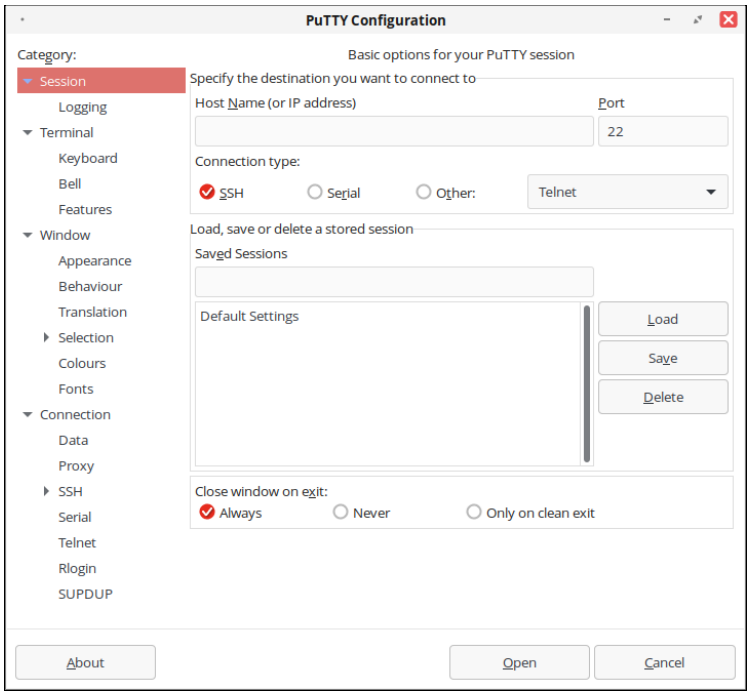
и выполните команду:

```
dnf install putty
```

После установки запуск программы доступен из «**Главного меню**» – «**Интернет**» – «**PuTTY**».

Работа в программе производится от **непривилегированного** пользователя.

Главное окно программы выглядит следующим образом:



Для настройки соединения доступны 4 основных раздела:

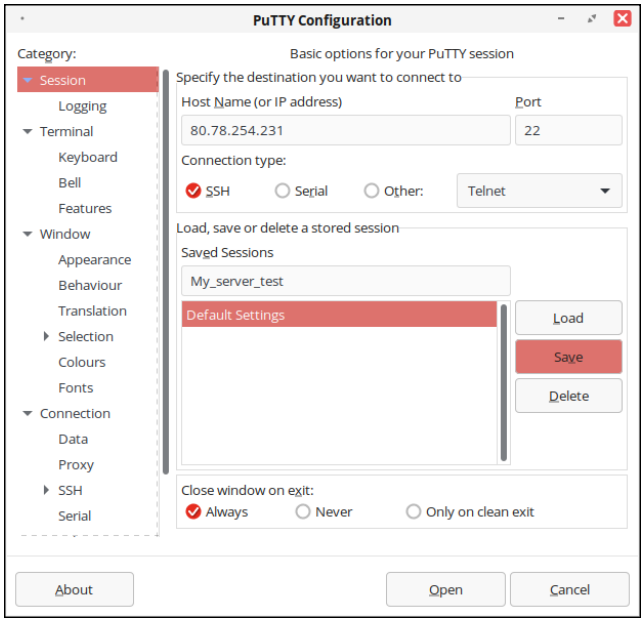
- Вкладка «**Session**» – необходима для ввода данных о подключаемом устройстве. Здесь можно указать порт, IP-адрес и другие параметры подключения. Чтобы при последующих подключениях не приходилось снова вносить информацию, ниже расположен блок, куда можно сохранить параметры текущего подключения;
- Вкладка «**Terminal**» – предназначена для включения или отключения возможностей терминала;

- Вкладка «**Window**» – предназначена для настройки визуальных параметров: облик окна, шрифт, цвет элементов и т. д.
- Вкладка «**Connection**» – предназначена для настройки параметров подключения, ключей аутентификации и других значений.

Работа с программой

В примере для подключения к удаленному серверу будет использоваться протокол **SSH** с портом по умолчанию – **22**.

Для начала сессии нажмите «**Open**».

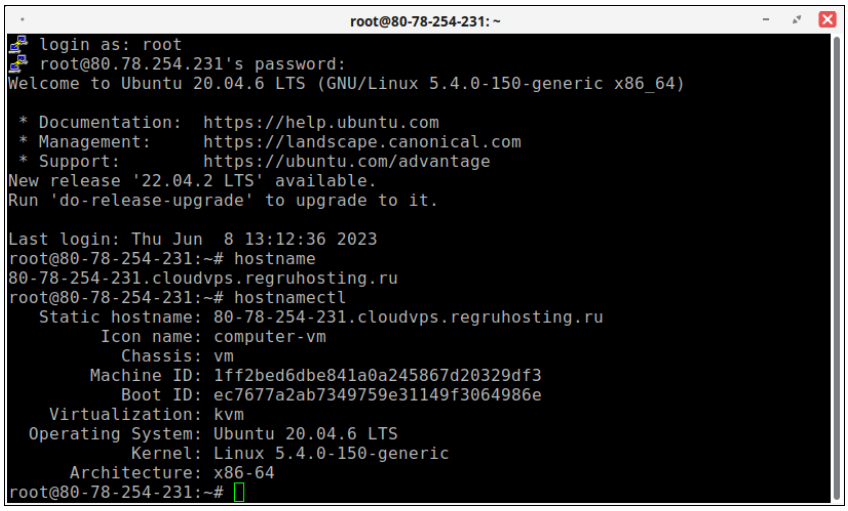


Если удаленный сервер доступен, и данные для подключения указаны корректно, откроется окно консоли, где необходимо указать *логин* и *пароль* для подключения.



После успешной авторизации можно начинать работу на удаленном сервере.

Для примера будет выполнена команда hostname для отображения информации о сервере.



Авторизация по ключу SSH

Для повышения безопасности подключения возможно настроить подключение по публичному ключу.

Для этого необходимо выпустить пару ключей – *публичный* и *приватный*, приватный будет храниться на клиентской машине, а публичный – на удаленном сервере. Важно помнить, что приватный ключ не должен передаваться третьим лицам.

Для создания ключа на клиентской машине выполните команду:

```
ssh-keygen
```

Будет выведен запрос на указание места хранения ключа, можно оставить каталог по умолчанию **~/.ssh/**. После выполнения команды будут сгенерированы два ключа – приватный **id_rsa** и публичный **id_rsa.pub**.

Приватный ключ можно защитить дополнительным шифрованием, указав пароль, однако в таком случае для его использования необходимо будет каждый раз вводить пароль, что не всегда удобно.

После создания ключей необходимо скопировать публичный ключ на удаленный сервер командой:

```
ssh-copy-id -i <путь_до_ключа> <имя_пользователя>@<IP-адрес_сервера>
```

Например:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@80.78.254.231
```

После этого при подключении к удаленному серверу авторизация будет проходить мгновенно.



Дополнительно для повышения безопасности подключения на удаленном сервере рекомендуется отключить авторизацию по паролю.

Для отключения авторизации по паролю на удаленном сервере откройте файл конфигурации **/etc/ssh/sshd_config** и измените значение параметра `PasswordAuthenticatin yes` на `PasswordAuthenticatin no`, сохраните файл.

Для применения изменений перезагрузите службу **sshd** на удаленном сервере:

```
systemctl reload sshd
```

AnyDesk

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: Anydesk - 6.3.3-1

AnyDesk предоставляет удаленный доступ к рабочим столам на базе Linux, Windows, MacOS, Android и др.

Скачать **AnyDesk** для личного пользования можно на официальном сайте.

Для РЕД ОС нужно перейти в «**Другие версии**» и выбрать версию **anydesk-6.3.3-1.el8.x86_64.rpm**.

Вы можете подробнее ознакомиться со средствами удаленного доступа в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Средства удалённого доступа;
- в **Яндекс.Дзен** — Средства удалённого доступа;
- в **VK Видео** — Средства удалённого доступа.

На наших каналах вы также сможете найти много другой полезной информации.

1. Перейдите в сеанс пользователя root:

```
su -
```

2. Перейдите в папку с дистрибутивом (в качестве примера **/home/user/Загрузки/**):

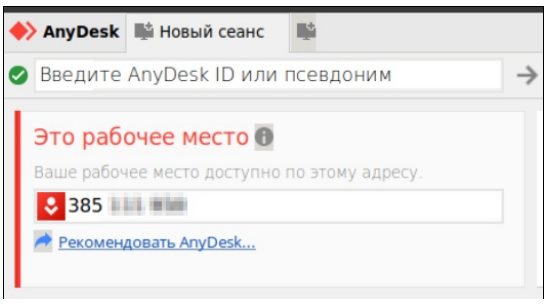
```
cd /home/user/Загрузки/
```

3. Выполните установку:

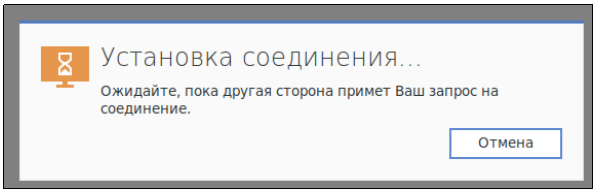
```
dnf install anydesk-6.3.3-1.el8.x86_64.rpm
```

Для запуска Anydesk откройте «**Главное меню**» — «**Интернет**» — «**Anydesk**».

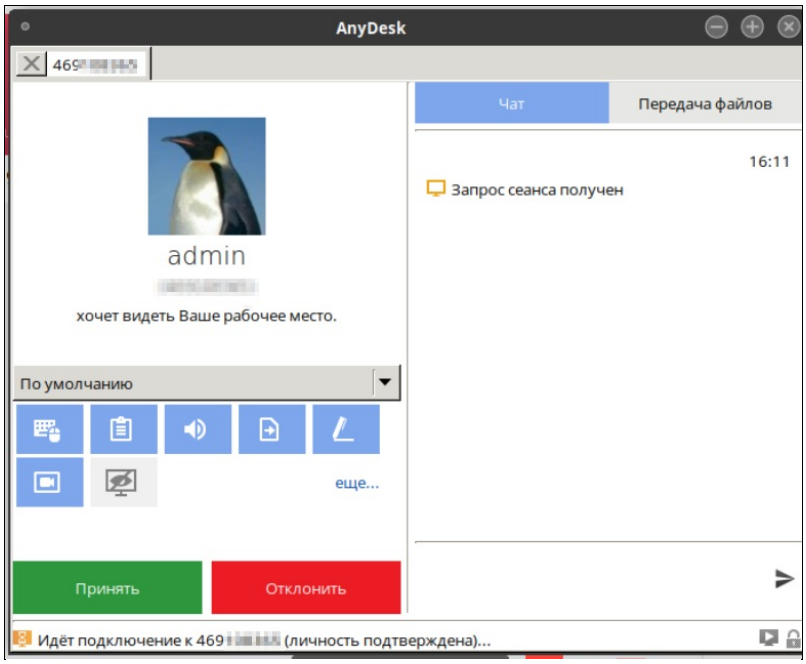
В интерфейсе **AnyDesk** имеется два основных пункта: адрес вашего компьютера, по которому можно подключится к вашему экрану и поле для ввода адреса другого компьютера для подключения.



После ввода адреса для подключения нужно будет подтвердить это с компьютера, к которому вы подключаетесь.



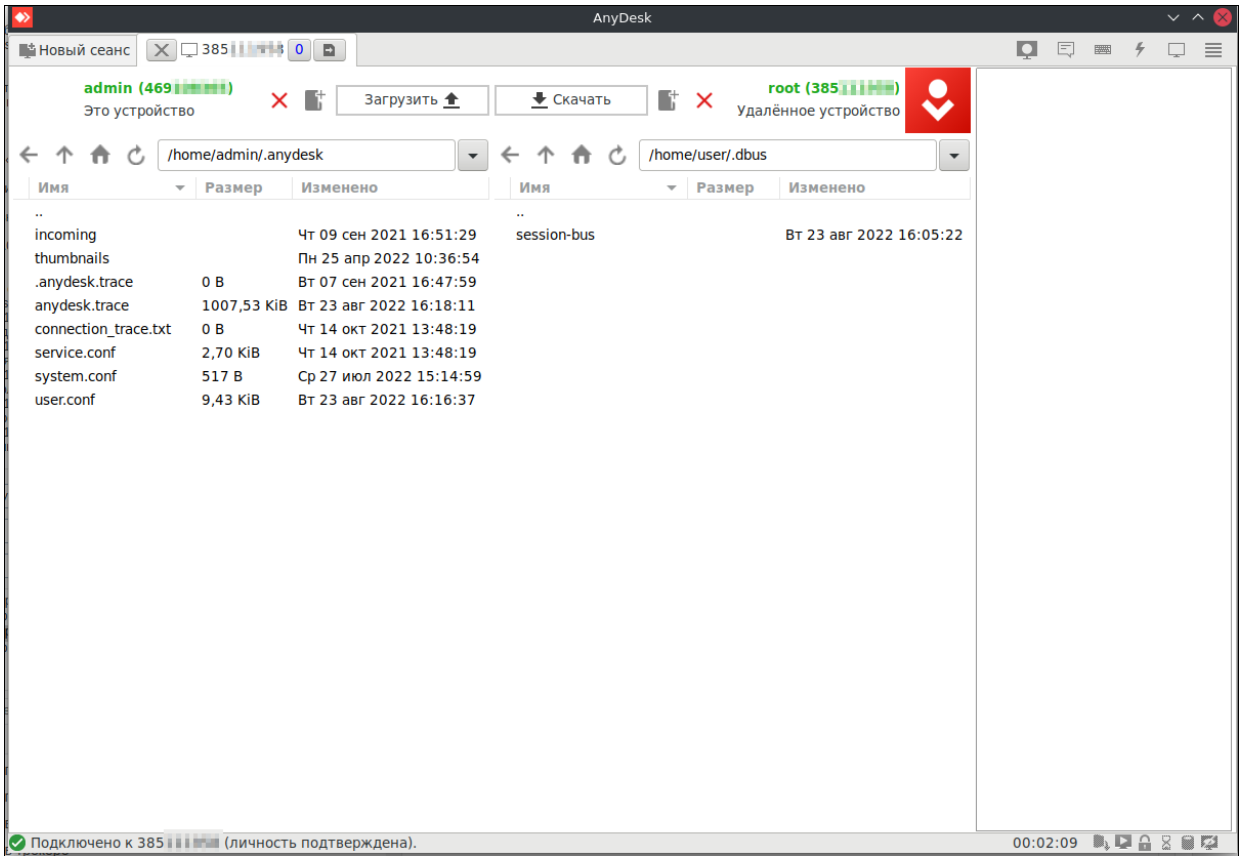
В окне подтверждения можно настроить чем удаленно можно будет управлять.



Когда доступ будет получен, сразу же откроется окно с удаленным доступом.

На верхней панели предоставлены дополнительные функции: запись экрана, чат с удаленным компьютером, смена раскладки, перезагрузка компьютера и другое.

Одной из важных функций является встроенный файловый менеджер, с помощью которого можно обмениваться файлами с удаленным компьютером.



МойАссистент

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: МойАссистент - 5.1

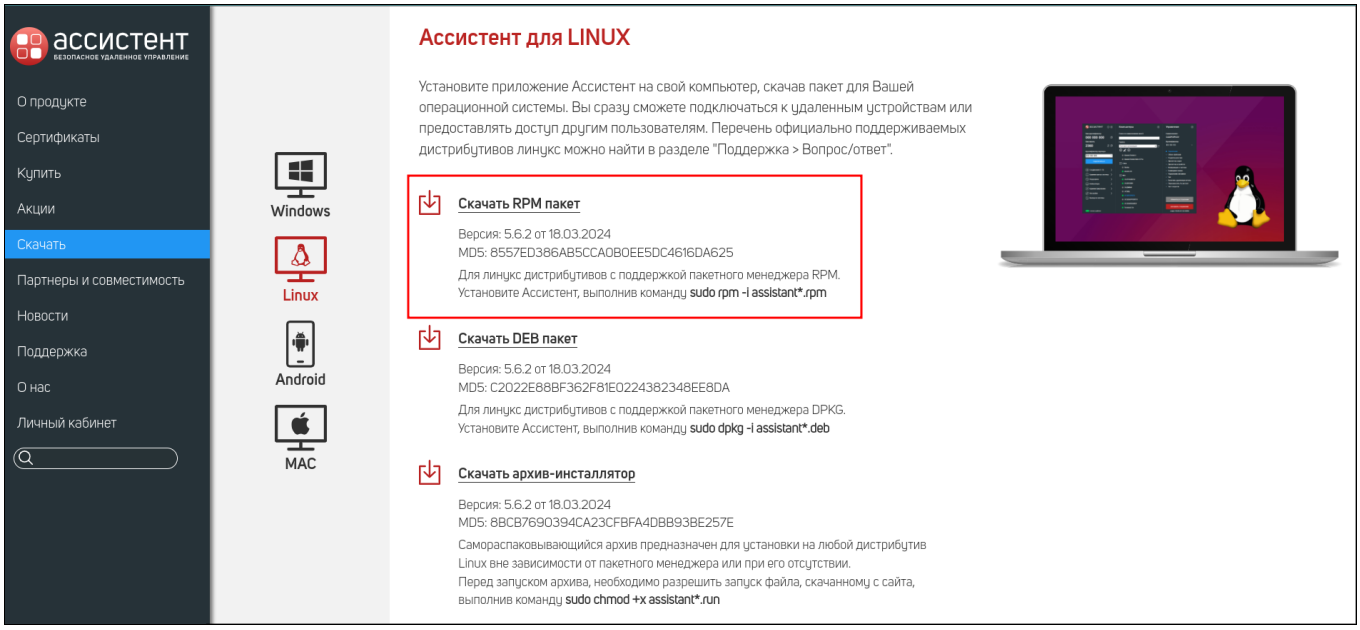
МойАссистент — это удобный и безопасный инструмент, для решения задач удаленного доступа, управления и администрирования.

Вы можете подробнее ознакомиться со средствами удаленного доступа в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Средства удалённого доступа;
- в **Яндекс.Дзен** — Средства удалённого доступа;
- в **VK Видео** — Средства удалённого доступа.

На наших каналах вы также сможете найти много другой полезной информации.

Для того чтобы установить приложение **МойАссистент**, необходимо перейти на сайт https://мойассистент.рф/, в раздел «**Скачать**» - «**Linux**» и выбрать RPM-пакет.



Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

Откройте терминал и перейдите в каталог со скачанным файлом (в примере **/home/user/Загрузки**):

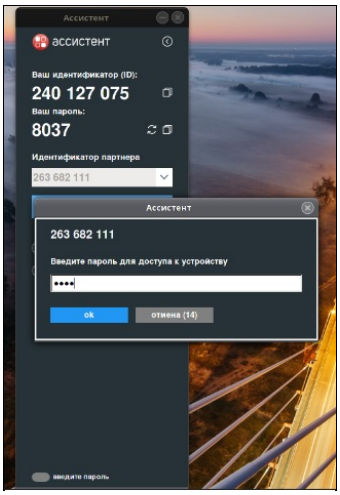
```
cd /home/user/Загрузки/
```

Установите МойАссистент командой:

```
dnf install assistant-5.1-0.x86_64.rpm
```

Для запуска программы в графическом режиме перейдите в «**Главное меню**» - «**Интернет**» - «**Ассистент**».

Для подключения к удалённому ПК, на котором установлен **МойАссистент**, введите «**Идентификатор партнера**», пароль и выполните подключение.


Ассистент
ассистент
Ваш идентификатор (ID):
240 127 075
Ваш пароль:
8037
Идентификатор партнера
263 682 111
Ассистент
263 682 111
Введите пароль для доступа к устройству
ok
отмена (14)
введите пароль

LiteManager

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: LiteManager - 5105

LiteManager Pro/Free — программа удаленного управления компьютерами через Интернет или администрирования в локальной сети.

Программа позволяет легко и быстро управлять рабочим столом компьютера в режиме реального времени, полностью поддерживая Windows, предоставляет надежный удаленный доступ к файловой системе, процессам и сервисам компьютера. **LiteManager** обладает встроенными функциями создания сетевой карты, сбора технической информации, возможностью развертывания и обновления с помощью средств удаленной установки, настройка своего личного ID-роутера (**NOIP**) и многое другое.

Удаленное администрирование теперь возможно и без IP-адреса, с помощью соединения по **ID** вы сможете сами выбирать свой личный уникальный **ID** и подключаться по нему. Клиентский и серверный модули программы способны работать в сетях, подключенных к Интернету через прокси-сервер.

Особенности:

1. Управление клавиатурой и мышью компьютера по сети. В отдельном окне видно удаленный рабочий стол контролируемого компьютера.
2. Управление удалённым компьютером возможно как с другого компьютера, так и с планшета или смартфона.
3. Серверная часть (для управляемого устройства) реализована для работы в среде операционных систем семейства Microsoft Windows. Версия для Linux, Mac OS реализована в тестируемой версии 5.0.
4. Клиентская часть (для управляющего устройства) реализована для Windows, Android, Mac OS, iOS, iPhone, iPad.
5. Широкий спектр режимов работы программы — передача файлов, удаленный диспетчер задач, терминал, *Wake-On-LAN* и многое другое.
6. Несколько режимов удаленной установки.
7. Возможна работа программы и без установки, в т.ч. и с внешнего носителя.
8. Поддержка *Microsoft Remote Desktop Protocol* (RDP).
9. Поддержка мультимониторных систем.
10. Карта сети.
11. Текстовый и аудио-видео чат.
12. Работа через *http-/socks5-прокси*.
13. Каскадное подключение (работа через промежуточный сервер).
14. Управление компьютером через Интернет без IP-адреса (соединение по ID).
15. Возможность запуска личного NoIpServer.
16. Встроенная система запросов (*Helpdesk*).
17. Функция **Quick Support** при необходимости разового подключения к удаленному рабочему столу (распространяется автономным приложением).
18. Трансляция рабочего стола компьютера на мониторы других пользователей, для проведения конференций и обучения.
19. Для учебных заведений, создание и проведение тестов, опросов. Централизованная раздача и сбор файлов тестов.

Установка

Для установки данного приложения, перейдите на сайт производителя по ссылке и скачайте архив для Linux.

> **Примечание.**
>
> Все команды выполняются от локального пользователя.

Разархивируйте скачанный архив командой (в примере /home/user):

```
cd /home/user
```

```
unzip LiteManager_linux.zip
```

Для того чтобы запустить разархивированный **LiteManager**, необходимо дать файлу права. Для этого выполните следующую команду:

```
chmod 0755 LiteManager
```

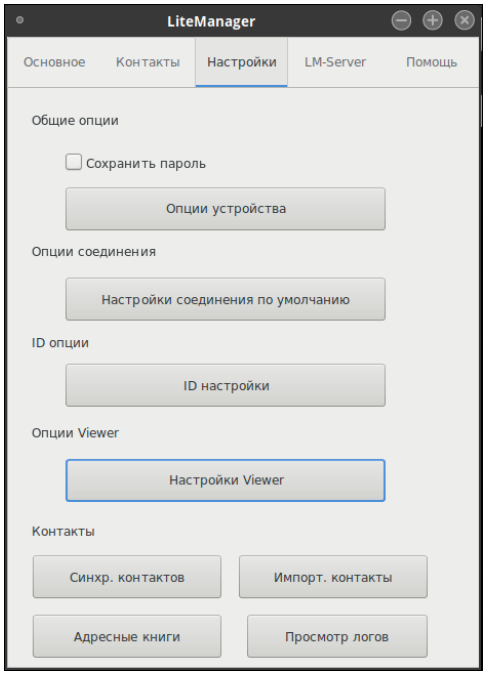
Запустите программу:

```
./LiteManager
```

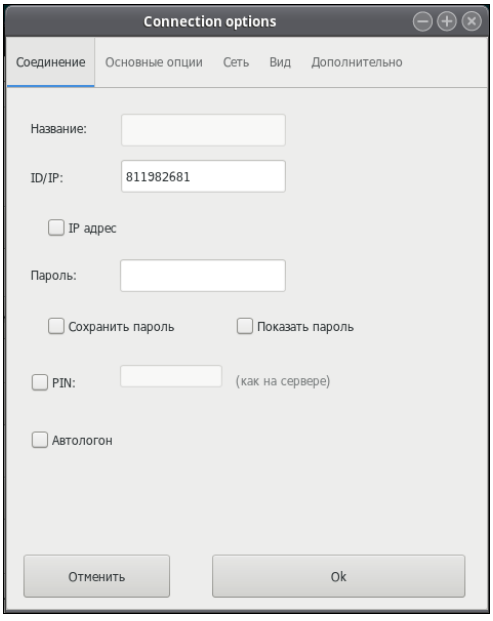
Настройка программы

Чтобы установить русский язык, перейдите в «**Settings**» - «**Viewer settings**» и поставьте галочку на «**Ru**».

Также в настройках клиента («**Настройки Viewer**») на вкладке «**Дополнительно**» вы можете защитить программу паролем, а на вкладке «**Сеть**» настроить прокси-сервер.



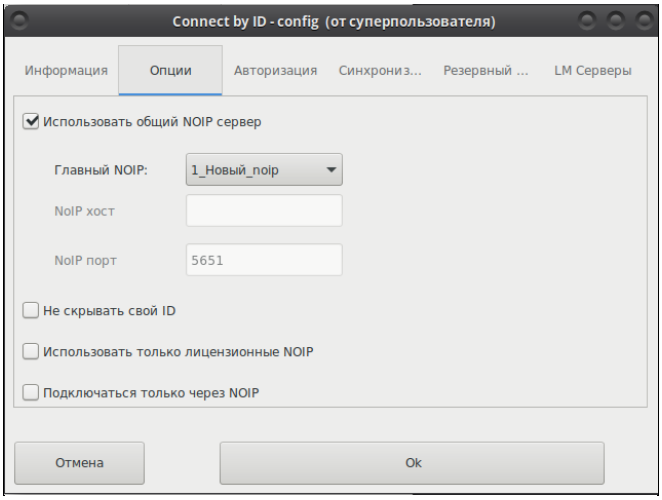
В настройках программы также можно установить «**Соединение по умолчанию**», выбрать основные и дополнительные опции и настроить внешний вид.



Для настройки соединения необходимо ввести **ID/IP** и пароль в соответствующие поля и нажать «**Ok**», после чего при выходе из программы введенные данные сохранятся.

Во вкладке «**Сеть**» можно выбрать порт и настроить **NoIP** и персональный прокси.

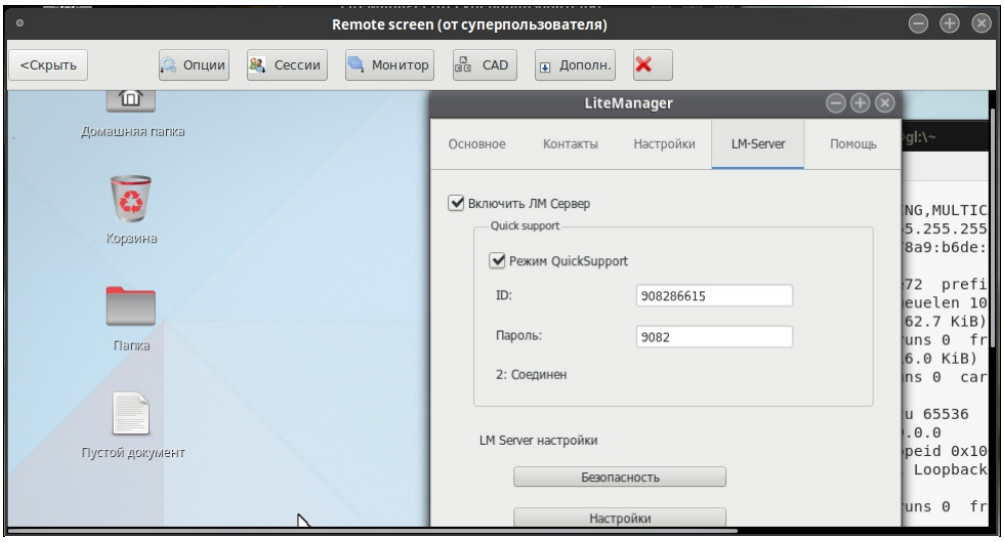
В «**Настройках ID**» можно просмотреть информацию и выбрать подходящий **NoIP**-сервер, настроить личный кабинет с авторизацией, настроить резервный **NoIP**-сервер, выбрать **LM**-сервер.



Работа с LiteManager

Чтобы создать сессию, нужно зайти в «**LM**» - «**Server**» и поставить галочку на «**Включить ЛМ сервер**». После чего сообщить другому пользователю *ID* и *пароль*.

Для подключения к **LM**-серверу во вкладке «**Основное**» впишите **ID/IP** и *пароль*, выберите как хотите подключится и нажмите «**Соединение**».



После подключения вам будут доступны: опции (настройки обозревателя), выбор монитора, вкладка «**Дополнительно**» (возможность передачи комбинаций клавиш **Alt+Shift**, **Shift**, **Ctrl**, **Alt** и **F1-F12**) и кнопка завершения сессии.

RuDesktop

Возможности
Установка
Описание программы
Подключение по постоянному паролю
Подключение к удалённому рабочему столу
Последние сеансы
Избранное
Найдено
Адресная книга
Передача файлов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: rudesktop-2.6.1603

RuDesktop – это программа для удалённого доступа и управления конфигурациями конечных устройств. Она предоставляет широкие возможности для администрирования и контроля над рабочими станциями, ноутбуками и другими устройствами, позволяя оптимизировать рабочие процессы и повысить уровень безопасности. Программа входит в Реестр Российского программного обеспечения.

RuDesktop – это клиент-серверное приложение. **Клиент** – это приложение, которое устанавливается на удалённые (к которым подключаетесь) и локальные компьютеры (административные). **Сервер** обеспечивает соединение клиентов между собой через локальную или глобальную сеть, хранит адресные книги и списки сессий операторов, обеспечивает контроль активности операторов и процессы авторизации и лицензирования.

Возможности

1. **Совместная работа** – обеспечивает подключение к удалённым устройствам по схемам «*один ко многим*» и «*многие к одному*», обмен файлами, общение в текстовом чате для совместного решения задач.

2. **Адресная книга** – предоставляет быстрый доступ к устройствам, назначение удобных псевдонимов и тегов для всех устройств.

3. **Установка, обновление и удаление ПО** на удалённых устройствах и группах устройств – позволяет управлять ПО удалённого компьютера в ручном или автоматическом режиме через запуск скриптов или выполнение задач по политикам **RuDesktop**.

4. **Неограниченное количество управляющих устройств** и **защищённое соединение** – для передачи данных используется шифрованное соединение по протоколу **TLS**.

5. **Инвентаризация оборудования и ПО** – позволяет отслеживать изменения в конфигурации удалённых устройств.

6. **Логирование действий в syslog** – обеспечивает сохранение в журнал действия персонала на локальном сервере и передачу данных в автоматическом режиме во внутренние системы информационной безопасности (SIEM, СКУД и др.).

7. **Передача файлов** – скачивание и загрузка файлов доступны всем пользователям, даже в бесплатной версии.

8. **Интеграция с AD и LDAP** – управление структурой компании, правами доступа и автоматизация администрирования на основе групп AD.

9. **История подключений** – просмотр списка сессий для всех авторизованных устройств в личном кабинете, просмотр списка подключаемых устройств на главном экране приложения (последние сеансы).

Установка

Для установки **RuDesktop** в РЕД ОС выполните следующий алгоритм действий:

1. Скачайте **RuDesktop** на официальном сайте. В разделе Linux выберите дистрибутив РЕД ОС.



2. Перейдите в папку с дистрибутивом (например, /home/user/Загрузки/):

```
cd /home/user/Загрузки/
```

3. Выполните установку (потребуются права **администратора**):

```
sudo dnf install rudesktop-amd64.rpm
```

После установки программа будет доступна из «**Главного меню**» – «**Интернет**» – «**RuDesktop**».

Для запуска программы через терминал введите команду:

```
rudesktop
```

Описание программы

При первом запуске программы создаётся уникальный номер (**ID**) для компьютера. **ID** остаётся неизменным даже после перезапуска или переустановки программы и используется для подключения к вашему рабочему столу. **Пароль** создаётся временный и после перезапуска он изменяется.

В интерфейсе **RuDesktop** есть два основных раздела.

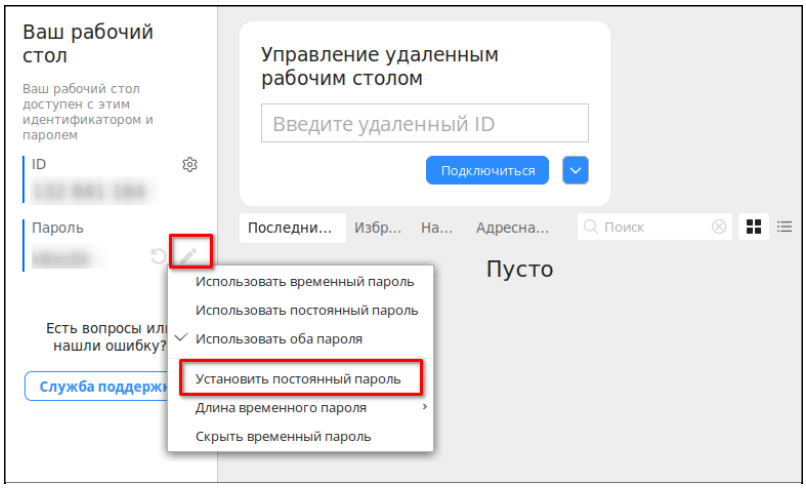
1. **Ваш рабочий стол** – содержит информацию об идентификаторе и пароле, с помощью которых можно подключится к вашему рабочему столу.

2. **Управление удаленным рабочим столом** – в этом разделе вы можете управлять удаленным рабочим столом после установления соединения.

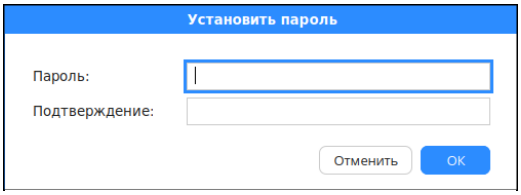
Подключение по постоянному паролю

Для обеспечения удобства администрирования компьютера через **RuDesktop** можно **установить** постоянный пароль на удалённом компьютере и **сохранить** его для подключения на компьютере администратора. Для этого выполните следующий алгоритм действий:

1. Установите постоянный пароль на удалённом компьютере. Для этого нажмите на значок редактирования рядом с паролем и из выпадающего списка выберите «**Установить постоянный пароль**».



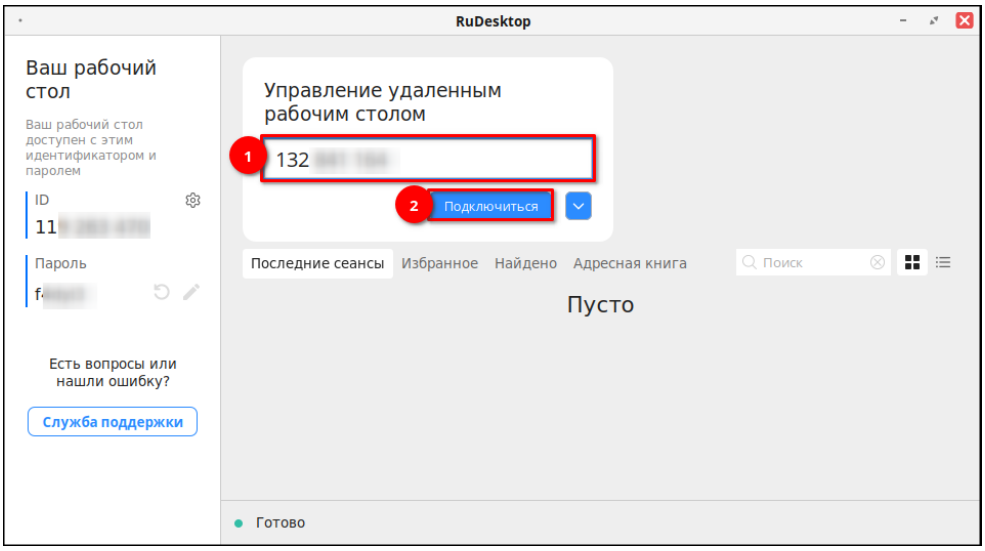
Установите сложный пароль. Нажмите «**OK**».



2. На компьютере администратора выберите адрес удалённого компьютера и введите указанный постоянный пароль для подключения. Это позволит администратору автоматически подключаться к управляемому компьютеру без необходимости каждый раз вводить пароль.

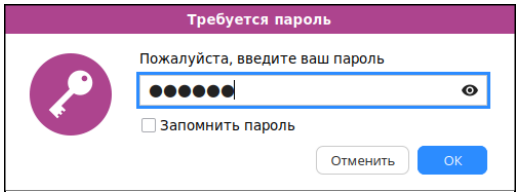
Подключение к удалённому рабочему столу

В разделе Управление удаленным рабочим столом введите **ID** удалённого компьютера (1) и нажмите кнопку «**Подключиться**» (2).

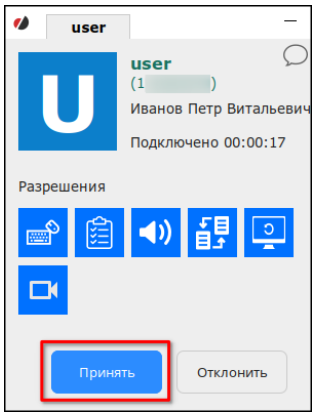


После ввода адреса для подключения вам потребуется подтвердить доступ к удалённому компьютеру, к которому вы пытаетесь подключиться.

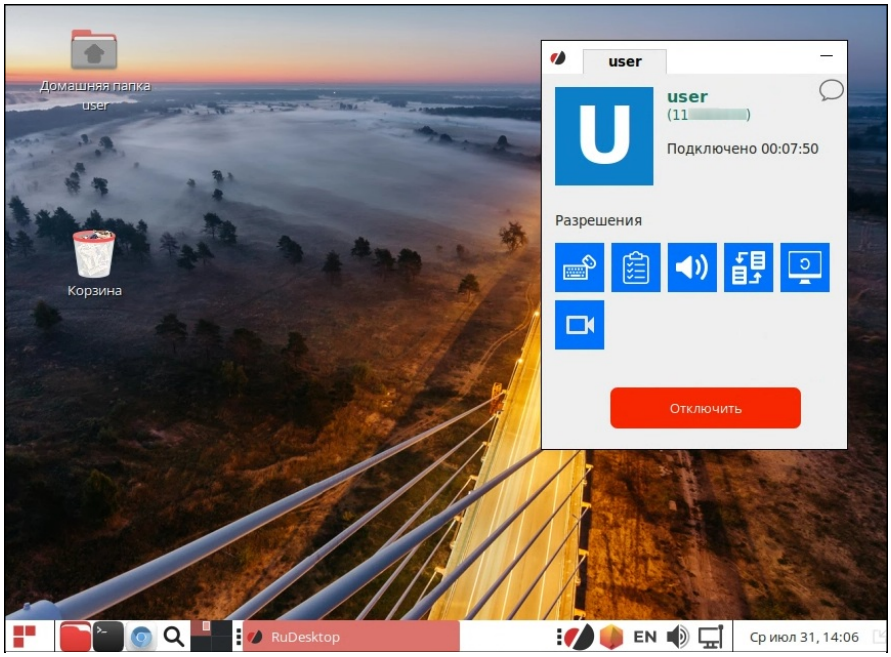
Если у вас имеется пароль для подключения к удалённому рабочему столу, введите его и нажмите «**OK**» для продолжения подключения. Если вы не хотите каждый раз вводить пароль, отметьте опцию «**Запомнить пароль**».



Если пароль неизвестен, ожидайте, пока пользователь подтвердит ваш запрос на подключение к его рабочему столу.



После установления соединения откроется удалённый рабочий стол управляемого компьютера.



Доступные разрешения при подключении:

▫ - разрешить использование клавиатуры и мыши;

 - разрешить использование буфера обмена;

▫ - разрешить передачу звука;

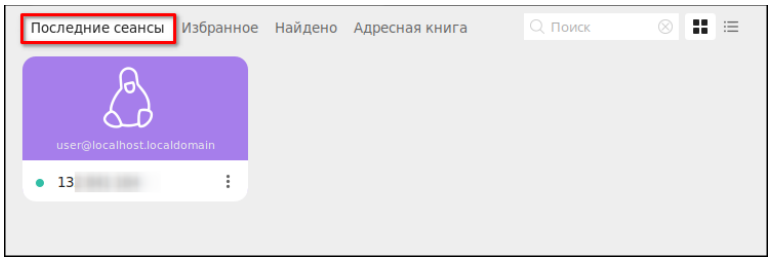
▫ - разрешить копирование и вставку файлов;

 - разрешить удалённый перезапуск;

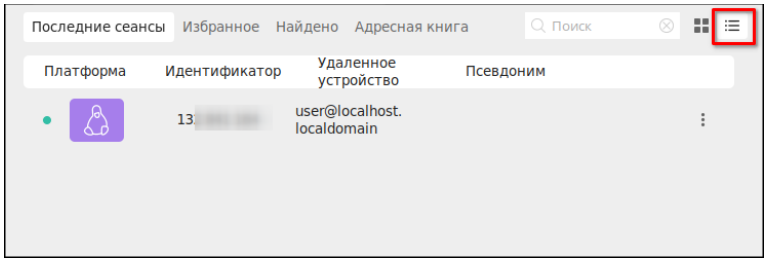
 - разрешить запись сессии.

Последние сеансы

На вкладке «**Последние сеансы**» отображаются недавние сеансы подключения пользователя.



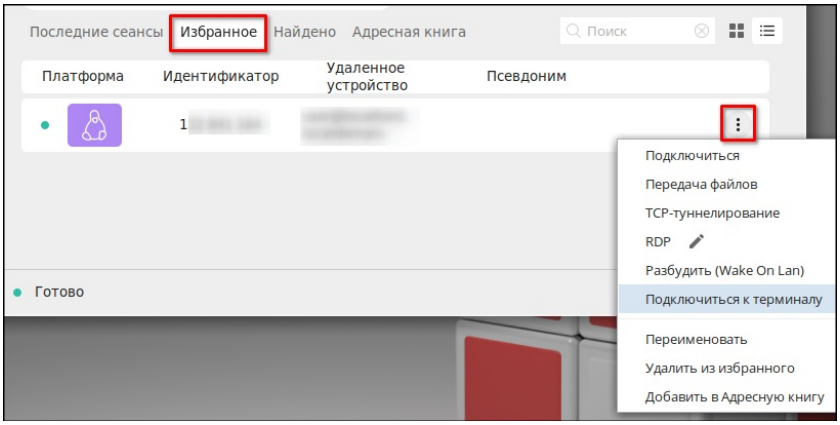
При переключении отображения (▫) последние сеансы подключений будут представлены в виде списка.



Рядом с каждым удаленным устройством доступны опции подключения, передачи файлов, удаления, добавления в адресную книгу. Выберите в выпадающем списке «**Добавить в избранное**» и удалённый рабочий стол будет отображён на вкладке « **Избранное**».

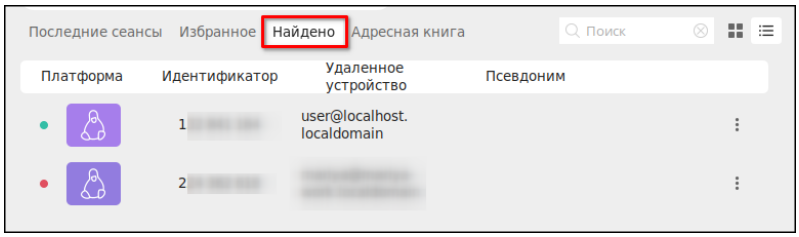
Избранное

На вкладке «**Избранное**» отображаются добавленные идентификаторы удалённых рабочих столов, которые пользователь выбрал для быстрого доступа или удобного отслеживания.



Найдено

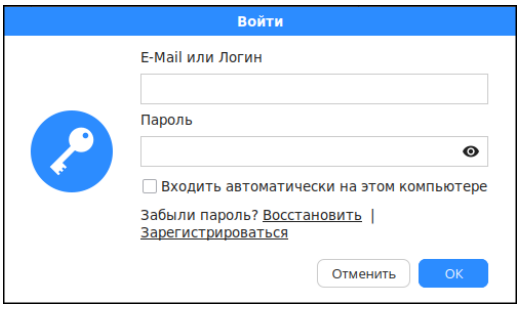
На вкладке «**Найдено**» в **RuDesktop** отображается список результатов поиска, который содержит информацию об удалённых устройствах, найденные в рамках запроса пользователя.



Для поиска нужного устройства воспользуйтесь строкой поиска и начните вводить необходимые значения идентификатора, псевдонима или наименования удалённого устройства. Алгоритм самостоятельно найдёт нужное устройство, опираясь на вводимые значения.

Адресная книга

Для использования адресной книги требуется создать учётную запись и войти в неё. Если у вас уже есть учётная запись **RuDesktop**, введите свой логин и пароль. В случае отсутствия учётной записи нажмите «**Зарегистрироваться**».

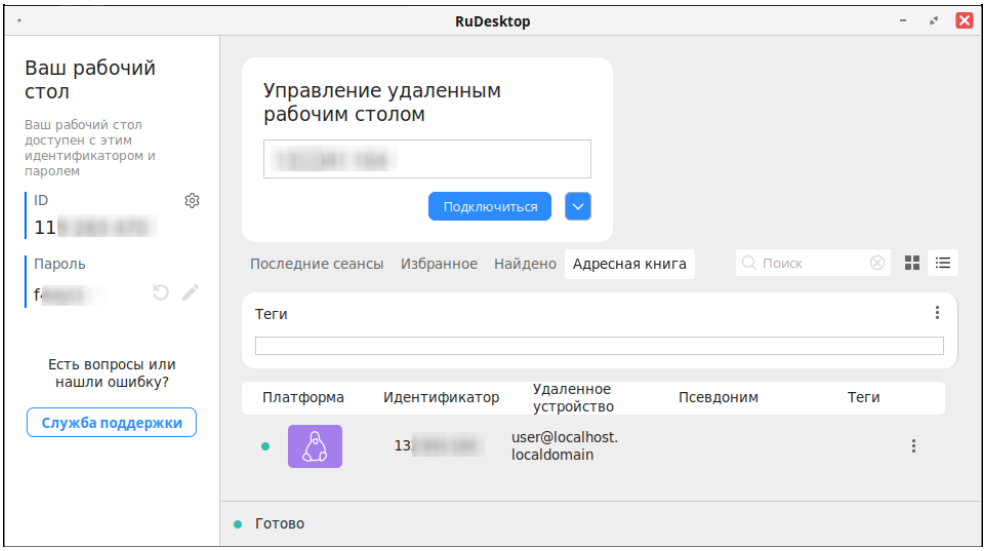


После открытия окна регистрации введите необходимые данные и зарегистрируйтесь.

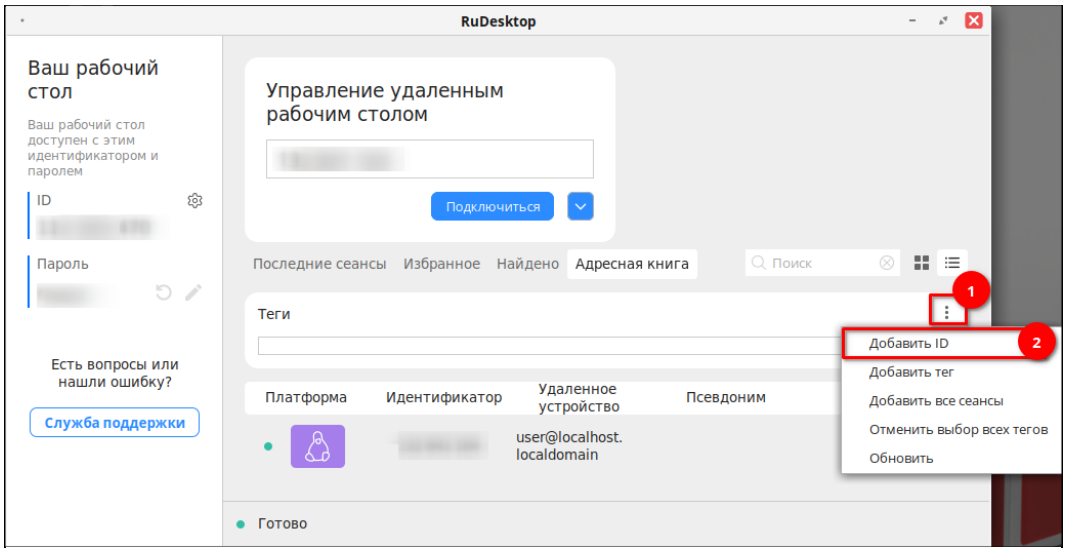
Далее будет отправлена инструкция на e-mail для активации учётной записи, и появится соответствующее сообщение.



Перейдите по ссылке в письме для завершения регистрации. После всех успешно выполненных действий вы сможете войти в систему.



Для добавления адресов удалённых рабочих столов нажмите на значок ⋮ и из раскрывающегося списка выберите «**Добавить ID**». Добавленное устройство будет отображено в адресной книге.



Передача файлов

Для осуществления обмена файлами между двумя удалёнными устройствами с помощью **RuDesktop** можно воспользоваться следующим алгоритмом действий:

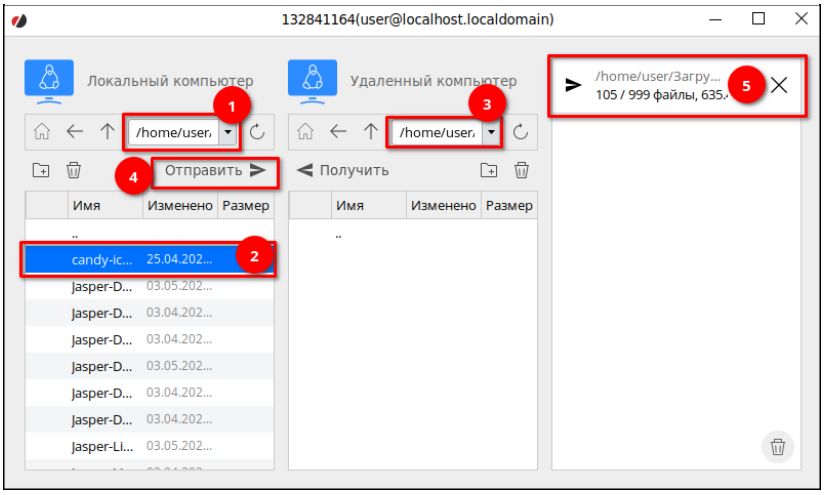
1. Выберите удалённое устройство, с которым вы хотите осуществить обмен файлами.

2. Раскройте список доступных функций для этого устройства.

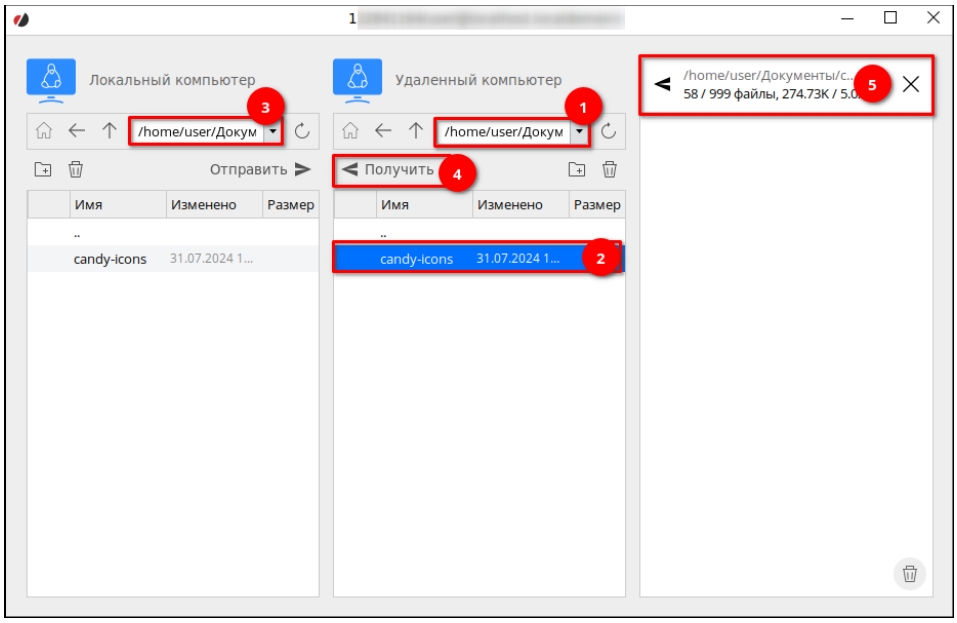
3. Выберите опцию «**Передача файлов**».

4. Подключитесь к удалённому рабочему столу.

5. Для передачи файлов на удаленное устройство в появившемся окне выберите путь на локальном устройстве (1) и выберите файлы, которые нужно передать между устройствами (2). Затем укажите путь назначения на удалённом устройстве (3). Нажмите «**Отправить**» (4). Начнётся процесс передачи файлов (5), дождитесь его завершения.



Для получения файлов с удалённого устройства укажите путь отправления файлов (1) и выберите файлы на удалённом устройстве (2). Затем укажите путь назначения (3) на локальном устройстве для файлов. Нажмите «**Получить**» (4). Начнётся процесс передачи файлов, дождитесь его завершения (5).



Добавление жесткого диска в РЕД ОС

Вы можете подробнее ознакомиться с возможностью добавления жесткого диска в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Добавление жесткого диска в РЕД ОС;
- в **Яндекс.Дзен** — Добавление жесткого диска в РЕД ОС;
- в **VK Видео** — Добавление жесткого диска в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Выключите ПК и подключите к нему жесткий диск.

После загрузки ОС откройте консоль и перейдите в сеанс пользователя **root** с помощью команды:

```
su -
```

Введите пароль пользователя **root**.

Далее с помощью команды `fdisk -l` необходимо посмотреть, какие диски доступны для монтирования.

fdisk — это утилита командной строки для просмотра и управления жесткими дисками и разделами.

```
fdisk -l
```

В списке подключенных дисков должен будет отобразиться, в том числе, и новый диск. Определить этот самый новый диск можно по его размеру.

Следует отметить, что у каждого раздела на жестком диске есть свое название. То есть, **/dev/sda**, **/dev/sdb/** и т. д. (без цифр) — это сами жесткие диски, а вот **/dev/sda1**, **/dev/sda2** — это разделы на жестких дисках.

Рассмотрим пример, когда на подключённом диске **sdb** есть один раздел, который называется **sdb1** и имеет файловую систему **ext4**.

Создайте каталог для монтирования раздела (обычно точка монтирования создается в директориях **/mnt** или **/media**).

```
mkdir -p /mnt/disk1
```

Произведите монтирование:

```
mount /dev/sdb1 /mnt/disk1
```

Если монтирование завершено без ошибок, для автоматического монтирования разделов после перезагрузки сервера внесите изменения в файл **/etc/fstab**. С помощью текстового редактора, например, **nano**, откройте этот файл:

```
nano /etc/fstab
```

Добавьте следующие строки:

```
/dev/sdb1 /mnt/disk1 ext4 defaults 0 0
```

Два параметра в конце строки `"0 0"` (`<dump> <pass>`) определяют, что:

1) Утилита **dump** не будет создавать резервную копию данных в файловой системе. Для дополнительных разделов в этом параметре обычно указывается значение **0**.

2) **fsck** не будет проверять раздел при загрузке ОС. Если же включить проверку **fsck** (установить значение **2** вместо **0**), то при неожиданной перезагрузке ПК процесс перезагрузки может быть довольно продолжительным (из-за проверки **fsck**).

> **Примечание.**
>
> Для однозначной идентификации подключаемых разделов в **/etc/fstab** можно указать идентификатор (UUID).

Командой **blkid** проверьте **UUID** диска, после этого добавьте его в **/etc/fstab**:

```
# blkid
```

```
...
```

```
/dev/sdb1: UUID="5baab1ca-c060-49fd-b44a-a19c6c453a2b" TYPE="ext4"
```

Отредактируйте **/etc/fstab**, добавьте строку для монтирования:

```
nano /etc/fstab
```

```
UUID=5baab1ca-c060-49fd-b44a-a19c6c453a2b /mnt/disk1 ext4 defaults 0 0
```

Измените режим доступа к разделам, если нужно. По умолчанию, если каталог создается пользователем **root**, то у каталога будут права этого пользователя:

```
drwxr-xr-x root:root
```

Для смены прав доступа к файлу выполните:

```
chmod -R 777 /mnt/disk1
```

После выполнения всех операций нужно перезагрузить ПК.

Монтирование устройств через systemd

Создание собственных модулей mount
Сетевые и съёмные диски
Примеры монтирования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Файл **fstab** – это текстовый файл, который содержит информацию о различных файловых системах и устройствах хранения информации на компьютере. Это единственный файл, определяющий, как диск и/или раздел будут использоваться и как будут встроены в остальную систему.

Данный файл можно открыть в любом текстовом редакторе, но редактировать его можно только от имени **суперпользователя root**, т.к. файл является важной, неотъемлемой частью системы, без которого система не загрузится.

Вы можете подробнее ознакомиться с возможностью монтирования новых устройств и файловых систем через **systemd**, просмотрев наши обучающие видео:

- на **RuTube** — Настраиваем монтирование systemd вместо файла /etc/fstab;
- в **Яндекс.Дзен** — Настраиваем монтирование systemd вместо файла /etc/fstab;
- в **VK Видео** — Настраиваем монтирование systemd вместо файла /etc/fstab.

На наших каналах вы также сможете найти много другой полезной информации.

Для автоматического монтирования разделов при загрузке операционной системы их указывают в файле **/etc/fstab**, который выглядит следующим образом:

```
[user@localhost ~]$ cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Wed Oct 25 06:21:53 2023
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#                                                  1  2  3     4        5 6
/dev/mapper/ro_redos-root /                       ext4  defaults       1 1
UUID=256bd628-c56a-4b53-bc02-601a3f18c4eb /boot                   ext4    defaults        1 2
/dev/mapper/ro_redos-swap none                    swap    defaults        0 0
```

где:

- **1** — имя раздела (уникальный идентификатор);
- **2** — точка монтирования;
- **3** — тип файловой системы;
- **4** — опции монтирования;
- **5** — индикатор необходимости резервной копии;
- **6** — порядок проверки раздела утилитой fsck (0 – отключено).

В файле есть подсказка, что после его заполнения необходимо перезапустить конфигурацию **systemd** (командой `systemctl daemon-reload`). Это означает, что файл на текущий момент является частью системной службы загрузки; **systemd** обрабатывает этот файл, чтобы создать модули для монтирования устройств.

Для отображения списка смонтированных устройств выполните команду:

```
mount
```

В ответе команды выведено довольно много устройств, большинство из них служебные.

С помощью команды `systemctl | grep mount` выведите модули **mount**, используемые в **systemd**.

```
[user@localhost ~]$ systemctl | grep mount
  proc-sys-fs-binfmt_misc.automount                                    loaded active waiting   Arbitrary Executab
le File Formats File System Automount Point
  -.mount                                                              loaded active mounted   Root Mount

  boot.mount                                                           loaded active mounted   /boot

  dev-hugepages.mount                                                  loaded active mounted   Huge Pages File Sy
stem
  dev-mqueue.mount                                                     loaded active mounted   POSIX Message Queu
e File System
  run-media-user-redos\x2dDVD\x2dx86_64\x2dMUROM\x2d7.3.3.mount        loaded active mounted   /run/media/user/re
dos-DVD-x86_64-MUROM-7.3.3
  run-user-1000-doc.mount                                              loaded active mounted   /run/user/1000/doc

  run-user-1000-gvfs.mount                                             loaded active mounted   /run/user/1000/gvf
s
  run-user-1000.mount                                                  loaded active mounted   /run/user/1000

  run-vmblock\x2dfuse.mount                                            loaded active mounted   VMware vmblock Fus
e Mount
  sys-fs-fuse-connections.mount                                        loaded active mounted   FUSE Control File
System
  sys-kernel-config.mount                                              loaded active mounted   Kernel Configurati
on File System
  sys-kernel-debug.mount                                               loaded active mounted   Kernel Debug File
System
  sys-kernel-tracing.mount                                             loaded active mounted   Kernel Trace File
System
```

Среди выведенных модулей присутствуют файловые системы, которые описаны в файле **/etc/fstab**.

Для определения физического места расположения устройства выполните (в примере используется **boot.mount**):

```
systemctl cat boot.mount

# /run/systemd/generator/boot.mount
# Automatically generated by systemd-fstab-generator

[Unit]
Documentation=man:fstab(5) man:systemd-fstab-generator(8)
SourcePath=/etc/fstab
Requires=systemd-fsck@dev-disk-by\x2duuid-256bd628\x2dc56a\x2d4b53\x2dbc02\x2d601a3f18c4eb.service
After=systemd-fsck@dev-disk-by\x2duuid-256bd628\x2dc56a\x2d4b53\x2dbc02\x2d601a3f18c4eb.service
After=blockdev@dev-disk-by\x2duuid-256bd628\x2dc56a\x2d4b53\x2dbc02\x2d601a3f18c4eb.target

[Mount]
Where=/boot
What=/dev/disk/by-uuid/256bd628-c56a-4b53-bc02-601a3f18c4eb
Type=ext4
```

Такие модули находятся во временной папке **/run**, они генерируются во время загрузки. Один из комментариев в файле модуля сообщает о том, что файл сгенерирован автоматически службой **systemd-fstab-generator**.

Создание собственных модулей mount

Модули **mount** можно создавать самостоятельно. Далее будет рассмотрен способ создания нового модуля **mount** вручную.

Собственные модули типа mount следует располагать в каталоге **/etc/systemd/system**. Существуют специальные правила именования таких файлов: они должны содержать путь к точке монтирования, в которой все слэши (кроме начального) заменяются на дефис. Например, если точка монтирования **/home/user/disk1**, то имя файла модуля должно иметь следующий вид – **home-user-disk1.mount**. Если в пути к точке монтирования есть служебные символы, то для генерации имени модуля существует специальная команда:

```
systemd-escape -p "/home/user/*disk-sata"

home-user-\x2adisk\x2dsata
```

В ответе команды видно, что специальные символы заменяются на набор символов **\x2d**.

Для создания нового модуля выполните:

```
nano /etc/systemd/system/home-user-disk1.mount
```

Модуль в своем описании должен содержать обязательную секцию [Mount], в которой указывается устройство и точка монтирования.

Минимальное содержимое модуля выглядит следующим образом:

```
[Unit]
 Description=Новый диск

 [Mount]
 What=/dev/disk/by-uuid/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
 Where=/home/user/disk1

 [Install]
 WantedBy=multi-user.target
```

Секция [Unit] содержит строку с описанием службы точки монтирования.

Секция [Install] задает уровень запуска службы, например **multi-user.target** (для многопользовательского режима без графики) или **graphical.target** (для монтирования устройства при графическом входе в систему).

Секция [Mount] описывает способ монтирования файловой системы.

Здесь параметр **What=** указывает путь к монтируемому устройству. Самый простой пример – **/dev/sda1**, но такой подход крайне не рекомендуется, т.к. при добавлении новых устройств имя может изменяться. Рекомендуется монтировать блочные устройства по **UUID**.

Параметр **Where=** указывает, куда будет производиться монтирование. Если указанной директории не существует, она будет создана.

Параметр **Type=** описывает тип файловой системы.

Параметр **Options=** указывает, какие параметры монтирования следует применить (перечисляются через запятую).

Параметр **DirectoryMode=** определяет режим доступа к файловой системе, используемый при создании этих каталогов. По умолчанию используется значение **0755**.

Параметр **TimeoutSec=** настраивает время ожидания перед завершением выполнения команды монтирования. Если команда не завершится в течение заданного времени, монтирование будет считаться неудачным.

Т.к. монтировать устройства необходимо по **UUID**, уточнить его можно с помощью команды:

```
lsblk -f
```

```
[user@localhost ~]$ lsblk -f
NAME FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINTS
sda
├─sda1
│    ext4   1.0         256bd628-c56a-4b53-bc02-601a3f18c4eb    698,2M    21% /boot
└─sda2
     LVM2_m LVM2        pZDD6y-inX7-Gg1O-e3DM-eLB0-bw8K-Zu91uA
  ├─ro_redos-root
  │  ext4   1.0         0e902942-3c05-4f7a-81c2-af22d16c9b42     26,1G    22% /
  └─ro_redos-swap
     swap   1           6cb04aa0-e9f3-46b3-a424-f8662fa22dbd                [SWAP]
sdb  LVM2_m LVM2        6IEWdc-vSPL-rc4f-bXlI-9K0c-jZZm-QW98Pf
```

После создания и сохранения файла модуля обновите конфигурацию **systemd**:

```
systemctl daemon-reload
```

Далее смонтируйте устройство:

```
systemctl start home-user-disk1.mount
```

После этого можно добавить точку монтирования в автозагрузку, для этого выполните команду:

```
systemctl enable home-user-disk1.mount
```

Сетевые и съёмные диски

Для подключения сетевых и съемных носителей необходимо использовать модуль автомонтирования.

Обратите внимание, что автомонтирование – не то же самое, что автоматический запуск модуля монтирования при загрузке системы.

Файл такого модуля формируется по тем же правилам, но с другим расширением – **.automount**. Данный модуль не содержит параметров монтирования и используется только в связке с mount-модулем, его имя формируется по тем же правилам. Например:

```
[Unit]
 Description=Автомонтирование съемного диска

 [Automount]
 Where=/home/user/disk1
 TimeoutIdleSec=900

 [Install]
 WantedBy=multi-user.target
```

Основная секция такого модуля – [Automount].

Обязательным параметром является **Where=**, который указывает на точку монтирования, а параметр **TimeoutIdleSec** настраивает время ожидания простоя в секундах, после которого файловая система будет отмонтирована.

По завершении создания модуля автомонтирования обновите конфигурацию **systemd** и запустите модуль:

```
systemctl daemon-reload
systemctl start home-user-video.automount
```

После этого можно добавить точку монтирования в автозагрузку, для этого выполните команду:

```
systemctl enable home-user-video.automount
```

Примеры монтирования

Монтирование съемного диска

По аналогии с ранее приведенными действиями сначала будет создан модуль монтирования **home-user-disk01**:

```
[Unit]
 Description=Монтирование съемного диска /home/user/disk01

 [Mount]
 What=/dev/disk/by-uuid/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
 Where=/home/user/disk01
 Type=ntfs
 Options=defaults

 [Install]
 WantedBy=multi-user.target
```

После этого необходимо создать одноименный модуль автомонтирования **home-user-disk01.automount**:

```
[Unit]
 Description=Монтирование съемного диска /home/user/disk01

 [Automount]
 Where=/home/user/disk01
 TimeoutIdleSec=300

 [Install]
 WantedBy=multi-user.target
```

Далее следует обновить конфигурацию systemd и добавить модуль автомонтирования в автозагрузку:

```
systemctl daemon-reload
```

```
systemctl enable --now home-user-disk01.automount
```

Благодаря созданным модулям, указанное устройство будет смонтировано при первом к нему обращении. При неактивности в течение 300 сек (5 мин) устройство будет размонтировано.

Монтирование NFS

Далее будет рассмотрен пример с протоколом сетевого доступа к файловым системам (*NFS*).

Клиентская часть требует установки дополнительного пакета:

```
dnf install nfs-common
```

Для монтирования NFS-ресурса так же необходимо создать два модуля. Первый – модуль монтирования **home-user-foto.mount**:

```
[Unit]
 Description= Монтирование NFS /home/user/foto

 [Mount]
 What=192.168.88.33:/media/nfs
 Where=/home/user/foto
 Type=nfs
 Options=_netdev,auto
 TimeoutSec=10

 [Install]
 WantedBy=multi-user.target
```

Второй – модуль автомонтирования **home-user-foto.automount**:

```
[Unit]
 Description=Монтирование NFS /home/user/foto

 [Automount]
 Where=/home/user/foto
 TimeoutIdleSec=300

 [Install]
 WantedBy=multi-user.target
```

Далее следует обновить конфигурацию systemd и добавить модуль автомонтирования в автозагрузку:

```
systemctl daemon-reload
systemctl enable --now home-user-foto.automount
```

Gnome-disk-utility – утилита для управления дисками

Gnome Disk Utility (**Gnome Disks**) — простая программа для управления дисками с базовым функционалом.

Программа позволяет просматривать информацию о дисках и съемных носителях. Для каждого диска доступна информация о модели, состоянии, серийном номере, информация о разделах, размерах разделов, типах таблиц разделов и другие данные.

Gnome Disk Utility поддерживает форматирование дисков, управление разделами, создание образов и восстановление разделов из образа. Также существует инструмент для оценки производительности диска.

Установка

Для установки программы необходимо перейти в сеанс пользователя **root**:

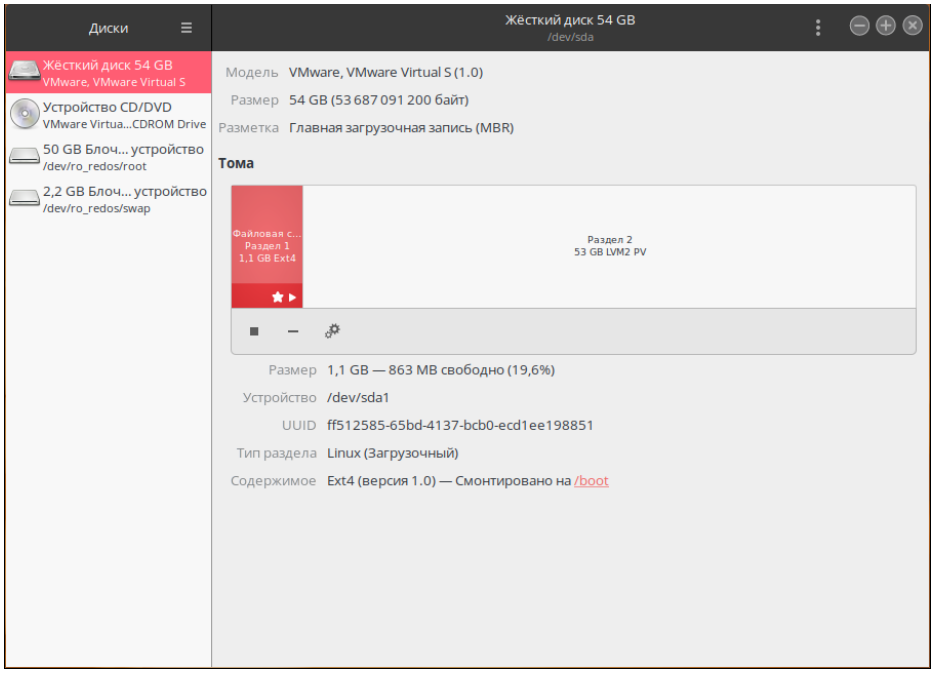
```
su -
```

Затем выполнить команду:

```
dnf install gnome-disk-utility
```

После установки программа доступна из «**Главного меню**» - «**Стандартные**» - «**Диски**» или вызовом через консоль (от **локального** пользователя):

```
gnome-disks
```



В меню программы можно создать или подключить образы дисков, ознакомиться с заданными комбинациями горячих клавиш, просмотреть справку о работе в программе.

В основном окне представлен список используемых дисков, подробная информация о выбранном разделе, а также возможность отмонтирования, удаления и расширенной настройки выбранного раздела.

Gparted – работа с дисковыми разделами

Установка
Интерфейс программы
Создание таблицы разделов
Создание разделов
Изменение размеров разделов
Удаление разделов

Перед началом использования нового жесткого диска, его полный объем необходимо разделить на части. Часть или, по-другому, раздел подразумевает участок диска, предназначенный для комфортного использования и размещения информации. Это помогает структурировать и разграничить отдельно файлы операционной системы от личных данных пользователя.

Если диск не новый, то иногда возникает необходимость в изменении количества или размеров разделов. Для всего этого в РЕД ОС есть различные инструменты, одним из таких инструментов является программа **GParted**.

GParted — это графическая оболочка к утилитам по работе с дисковыми разделами. Название происходит из полного названия – **GNOME Partition Editor**.

Gparted позволяет выполнять все необходимые операции над разделами дисков. Основными операциями являются:

- *Создание* - выделяется из свободного, не занятого другими разделами, места.
- *Удаление* - уничтожаются и раздел и данные на нём.
- *Изменение размера* - информация на разделе сохраняется.
- *Форматирование* - программа поддерживает около 20 типов файловых систем.
- *Монтирование* - стандартная процедура монтирования и размонтирования устройств хранения.
- *Управление флагами* - у разделов есть определённые атрибуты, например, загрузочный.
- *Проверка на ошибки* - проверяются ошибки файловой таблицы раздела.
- *Изменение UUID* - смена Универсального Уникального Идентификатора.
- *Создание таблицы разделов* - основная таблица жёсткого диска, хранит информацию о разделах.

Вы можете подробнее ознакомиться с работой утилиты **Gparted**, просмотрев наши обучающие видео:

- на **RuTube**:
  - Редакторы дисковых разделов в РЕД ОС. GParted;
  - Как отформатировать флешку в РЕД ОС.
- в **Яндекс.Дзен**:
  - Редакторы дисковых разделов в РЕД ОС. GParted;
  - Как отформатировать флешку в РЕД ОС.
- в **VK Видео**:
  - Редакторы дисковых разделов в РЕД ОС. GParted;
  - Как отформатировать флешку в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

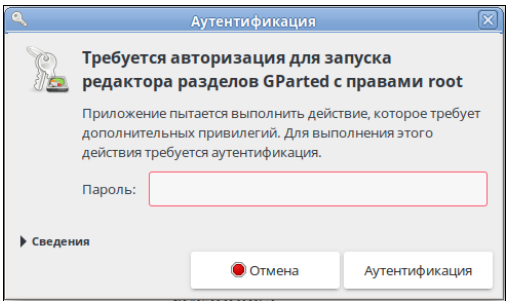
и выполните команду:

```
dnf install gparted
```

После установки программа доступна из «**Главного меню**» - «**Системные**» - «**GParted**».

Для правильной работы утилиту необходимо запускать **с правами суперпользователя**. Если вы запускаете ее из главного меню, то

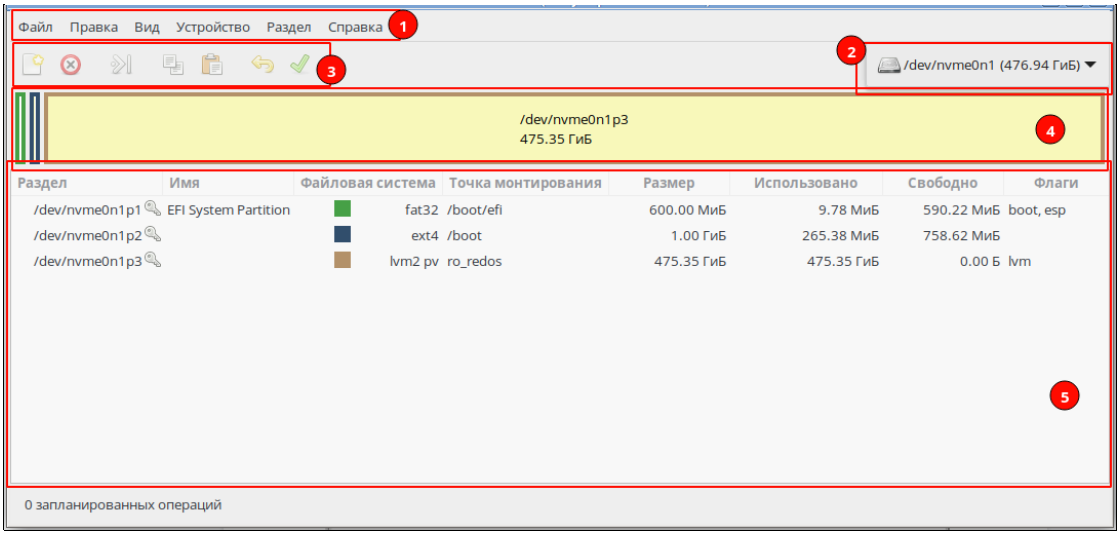
система сама потребует пароль.



Интерфейс программы

После запуска перед вами откроется главное окно программы. Оно состоит из таких областей, как:

1. *Меню* - содержит все команды программы **gparted** для работы с дисковыми устройствами и разделами.
2. *Список устройств* - отображает список доступных устройств.
3. *Панель инструментов* - содержит несколько команд для быстрого доступа.
4. *Сводная диаграмма* - графическая схема выбранного диска, визуально отображает соотношение размеров разделов.
5. *Рабочая область* - отображает все разделы на текущем диске с дополнительной информацией о них. При работе с носителями в нижней части данного поля отображается последовательный список всех операций, которые потом необходимо выполнить.



Программа проста и интуитивно понятна. Для работы необходимо выбрать нужный участок устройства хранения, вызвать контекстное меню и выбрать необходимое действие, в зависимости от возможных действий состав контекстного меню изменяется.

Изначально все действия записываются, а не применяются. Чтобы применить изменения, нужно нажать на зеленую галочку в панели инструментов. Также можно открыть меню «**Правка**» - «**Применить все операции**». Затем потребуется подтвердить всю последовательность действий, поскольку это может вызвать потерю данных.

Обратите внимание, что начинать работу в этой программе лучше с пустым диском, чтобы случайно не потерять данные.

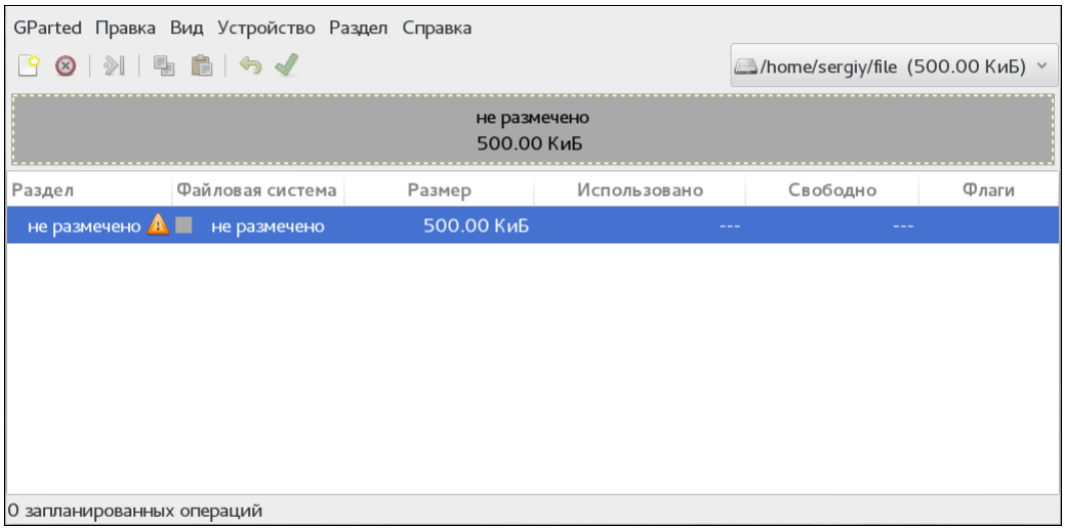
Рассмотрим пример работы с жёстким диском.

Создание таблицы разделов

Для того чтобы хранить информацию на носителе, необходимо его разметить. На одном носителе можно создать несколько независимых частей - разделов. Информация о таком разделении хранится в самом начале носителя и именуется таблицей разделов. Таблицы отличаются разной структурой, надежностью и возможностями. Некоторые не поддерживаются в одной операционной системе, но поддерживаются в другой. Наиболее широко известными типами таблиц разделов являются **msdos** (*MBR*) и **GPT**.

Для создания новой таблицы разделов необходимо открыть меню «**Устройство**» - «**Создать таблицу разделов**».

Вы увидите диалоговое окно, где сможете выбрать нужный вам тип таблицы разделов. По умолчанию выбран параметр **msdos** (*MBR*).



Нажмите «**Применить**», чтобы создать новую таблицу разделов. Приложение запишет новую таблицу разделов на дисковое устройство и обновит информацию о разделах в окне **gparted**.

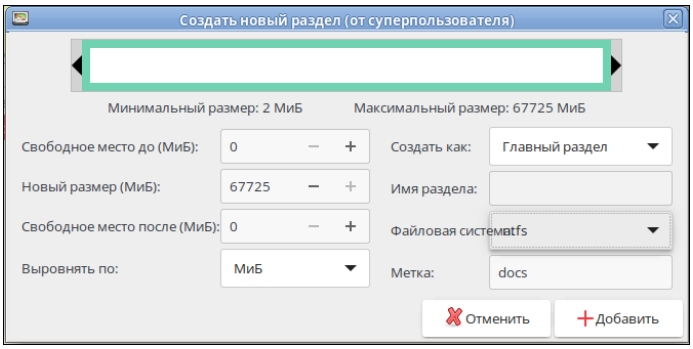
ВАЖНО!

Данная операция удалит все данные со всего дискового устройства!

Создание разделов

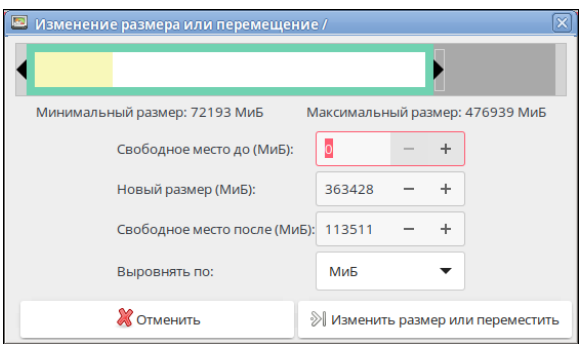
Чтобы создать новый раздел, выберите область «**Не размечено**» и, нажав ПКМ, выберите пункт «**Новый**» из контекстного меню.

После этого необходимо заполнить информацию о будущем разделе. Вы можете тонко настроить расположение раздела от начала или конца свободного пространства и указать размер. А также можно выбрать *файловую систему*, *тип раздела* (первичный/вторичный) и *метку*. Размер и расположение раздела можно также указать, изменяя сам раздел визуально, на линейке в верхней части окна.



Изменение размеров разделов

Для изменения размера необходимо выбрать нужный раздел, открыть контекстное меню, выбрать пункт «**Изменить размер или переместить**». В открывшемся окне новые размеры устанавливаются либо в соответствующих полях, либо мышкой. После установки нужных размеров можно смело применять действия к исполнению. Важно знать, что данные на разделе при изменении его размеров остаются в сохранности.



Удаление разделов

Для удаления необходимо выбрать раздел, вызвать контекстное меню и выбрать пункт «**Удалить**».

ВАЖНО!

Если диск примонтирован, действия с ним будут недоступны.

При этом стоит помнить, что после применения изменений **вся информация** на разделе **будет удалена**.

Blivet-gui – управление разделами и дисками

Интерфейс
Создание раздела
Изменение или удаление раздела

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:**: blivet-gui 2.2.0-3

Blivet-gui является реализацией механизмов управления разделами и дисками. Утилита с графическим интерфейсом создана для удобного управления носителями в РЕД ОС. Интерфейс похож на **gparted**, но **blivet-gui** поддерживает весь набор технологий хранения данных из современных дистрибутивов Linux. Для графического интерфейса **blivet** требуется модуль **Python blivet**. Так же как и **gparted**, **blivet-gui** работает только с правами пользователя **root**.

Программа поддерживает управление дисковыми разделами и хранилищами **LVM2** (включая шифрованные разделы LUKS, логические тома и группы томов). Так же как и в **gparted**, изменения в **blivet-gui** применяются не сразу, а после подтверждения внесённого набора изменений.

Вы можете подробнее ознакомиться с работой утилиты **Blivet-gui**, просмотрев наши обучающие видео:

- на **RuTube** — Управление разделами и дисками с помощью Blivet-gui;
- в **Яндекс.Дзен** — Управление разделами и дисками с помощью Blivet-gui;
- в **VK Видео** — Управление разделами и дисками с помощью Blivet-gui.

На наших каналах вы также сможете найти много другой полезной информации.

Установку программы можно осуществить командой:

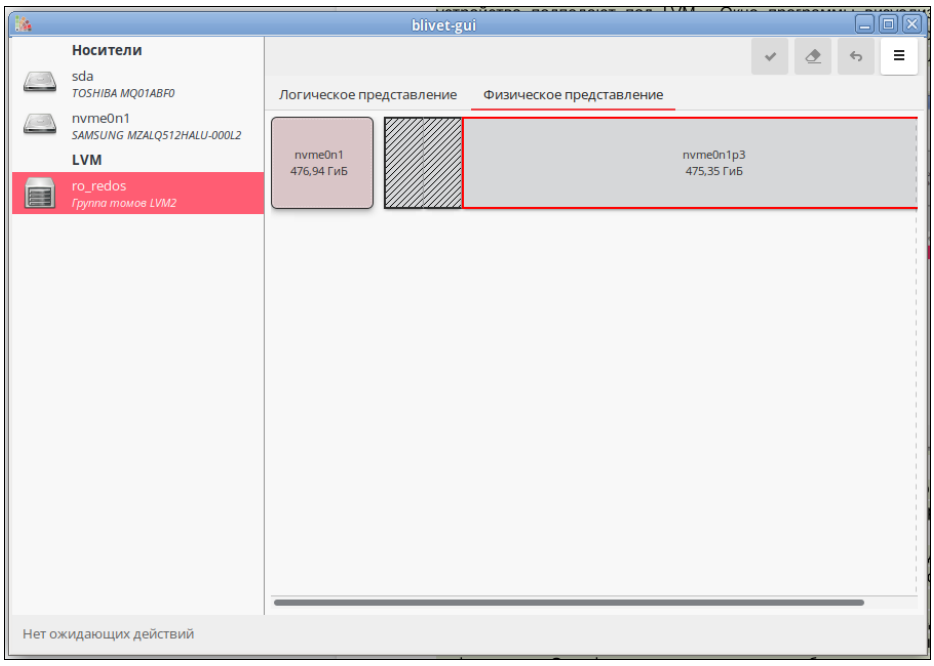
```
dnf install blivet-gui
```

После установки программа доступна в «**Главном меню**» - «**Системные**» - «**blivet-gui**». Интерфейс запускается только с правами пользователя **root**.

Графический интерфейс **blivet** визуально напоминает **gparted**, но без панели меню. Вы можете полностью управлять программой с помощью кнопок в правом верхнем углу окна программы и в соответствующих контекстных меню.

Интерфейс

Слева отображается вертикальный список физических и логических томов в системе. Логические тома находятся под дисками, а блочные устройства подпадают под **LVM**. Окно программы визуализирует объемы в виде горизонтальной полосы. Пользователи **blivet-gui** могут переключать соответствующее представление с помощью вкладок «**Логическое представление**» и «**Физическое представление**».



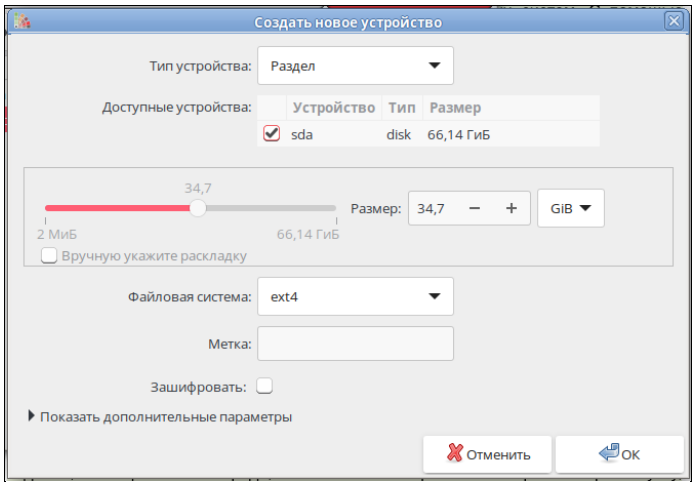
Графический интерфейс **blivet** очень четко показывает физические и логические тома, предоставляя администраторам обзор логических томов, охватывающих несколько физических томов.

В разделе «**Логическое представление**» отображается таблица отдельных томов, включая соответствующую дополнительную информацию.

Все действия для настройки выполняются через контекстные меню. **Blivet-gui** частично поддерживает многие типы файловых систем.

Создание раздела

Для создания раздела необходимо выбрать свободное место на физическом диске, вызвать контекстное меню и выбрать пункт «**Создать**». С помощью графических элементов управления вы можете задать размер логического тома или ввести значение напрямую. Нажатие кнопки «**OK**» создает задачу на создание нового логического диска и подготавливает его к работе.



Изменение или удаление раздела

Для изменения раздела следует выбрать нужный существующий логический раздел, в контекстном меню выбрать пункт «**Изменить**». С помощью команды «**Форматировать**» можно отформатировать раздел. С помощью команды «**Удалить**», соответственно, удалить раздел. Также есть возможность изменить размер всего тома с помощью функции «**Редактирования**» - «**Изменить размер**».

Если впоследствии добавить в систему новые физические тома, то можно, например, сначала интегрировать их с существующим логическим томом, выбрав в контекстном меню пункт «**Изменить**» - «**Изменить родителей**».

Изменения не вступят в силу до тех пор, пока вы их не подтвердите нажатием кнопки с галочкой в правом верхнем углу окна программы.

В отдельном окне отобразятся незавершенные операции, но **blivet** выполняет эти действия только после нажатия кнопки «**OK**».

Baobab – программа для анализа использования разделов диска

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** baobab-3.32.0-1

Baobab — программа для анализа использования ёмкости разделов диска из состава свободной среды рабочего стола **GNOME**. Графически показывает, какие папки занимают больше места на диске.

Baobab позволяет сканировать полностью всю файловую систему, отдельные папки, домашнюю директорию или удаленный каталог (по **FTP**, **SSH**, **HTTPS**). Также непосредственно из программы можно удалять файлы и директории.

Графически использование диска можно отобразить в виде круговой диаграммы или в виде древовидной карты (прямоугольниками).

Вы можете подробнее ознакомиться с работой в **Baobab**, просмотрев наши обучающие видео:

- на **RuTube** — Анализ занятого пространства на дисках;
- в **Яндекс.Дзен** — Анализ занятого пространства на дисках;
- в **VK Видео** — Анализ занятого пространства на дисках.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы перейдите в сеанс пользователя **root**:

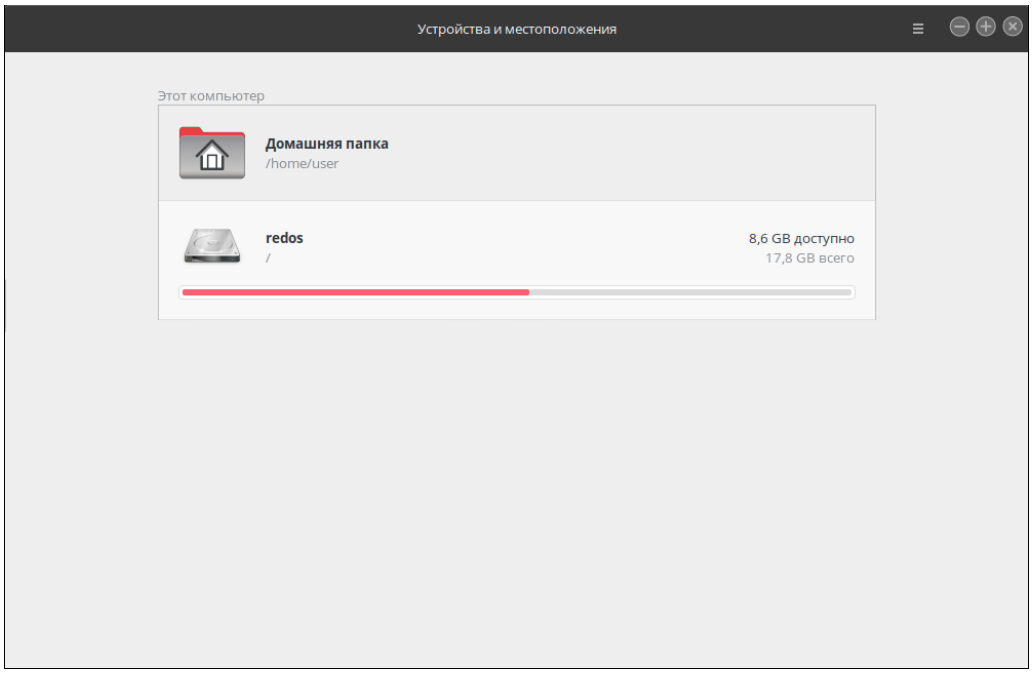
```
su -
```

и выполните команду:

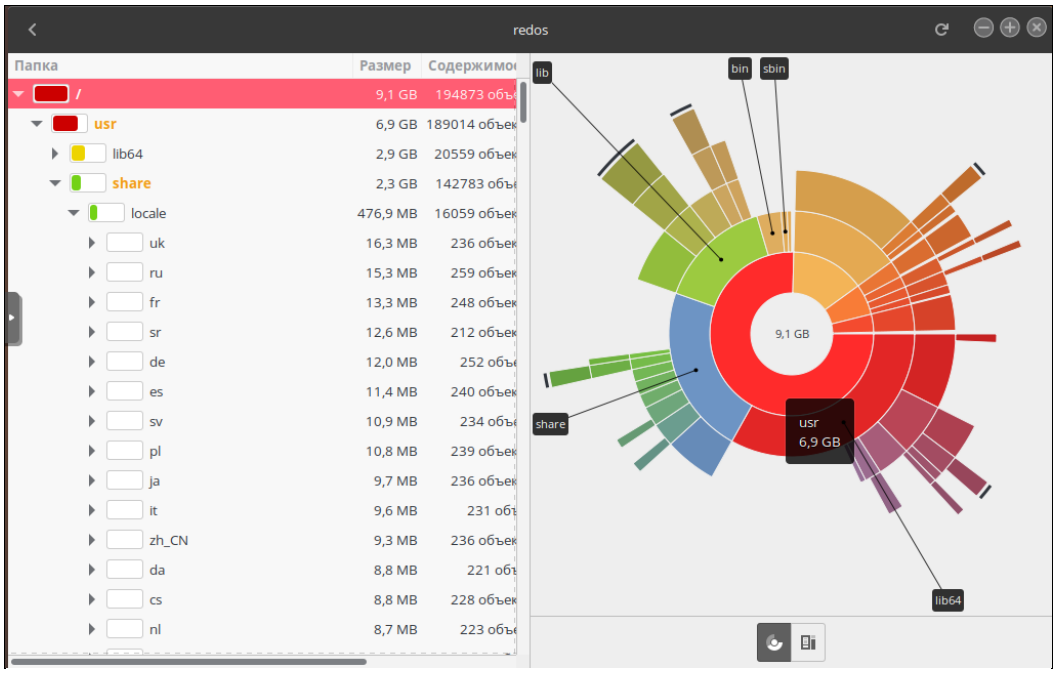
```
dnf install baobab
```

Программа будет доступна из «**Главного меню**» - «**Системные**» - «**Анализатор использования дисков**».

При запуске программы предлагается выбрать диск для проведения анализа.



После этого будет построено дерево каталогов и представлена диаграмма использования дискового пространства. При наведении курсора на какую-либо область диаграммы будет показано, какая доля дискового пространства занята тем или иным каталогом.


redos
Папка
Размер
/ 9,1 GB
usr 6,9 GB
lib64 2,9 GB
share 2,3 GB
locale 476,9 MB
uk 16,3 MB
ru 15,3 MB
fr 13,3 MB
sr 12,6 MB
de 12,0 MB
es 11,4 MB
sv 10,9 MB
pl 10,8 MB
ja 9,7 MB
it 9,6 MB
zh_CN 9,3 MB
da 8,8 MB
cs 8,8 MB
nl 8,7 MB
lib
bin
sbin
9,1 GB
usr
6,9 GB
share
lib64

Менеджер логических томов LVM

Logical Volume Manager (LVM) – это система управления дисковым пространством, абстрагирующаяся от физических устройств. Она позволяет создавать поверх физических разделов (или даже неразбитых винчестеров) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (т.е. как обычные разделы). Основные преимущества LVM в том, что, во-первых, одну группу логических томов можно создавать поверх любого количества физических разделов, а во-вторых, размер логических томов можно легко менять прямо во время работы.
Кроме того, LVM поддерживает механизм снапшотов, управление разделами «на лету» и зеркалирование, подобное RAID-1.



Рисунок 1 – Схема организации LVM.

Из схемы на рисунке 1 видно, что в самом низу рисунка располагаются физические устройства — жесткие диски. Далее начинается зона LVM, а именно – создаются физические тома (**PV**) из разделов жесткого диска, которые потом объединяются в логические группы (**VG**). В качестве примера на схеме представлена единая логическая группа **vgdata** (/dev/vgdata), а уже на следующем уровне эта группа разбита на логические тома (**LV**), на которых могут быть созданы файловые системы.

PV, Physical volume, физический том. Обычно это раздел на диске или весь диск. В том числе, устройства программного и аппаратного RAID (которые уже могут включать в себя несколько физических дисков). Физические тома входят в состав группы томов.
VG, Volume group, группа томов. Это самый верхний уровень абстрактной модели, используемой системой LVM. С одной стороны группа томов состоит из физических томов, с другой – из логических и представляет собой единую административную единицу.
LV, Logical volume, логический том. Раздел группы томов, эквивалентен разделу диска в не-LVM-системе. Представляет собой блочное устройство и, как следствие, может содержать файловую систему.
PE, Physical extent, физический экстент. Каждый физический том делится на порции данных, называющиеся физическими экстентами. Их размеры те же, что и у логических экстентов.
LE, Logical extent, логический экстент. Каждый логический том делится на порции данных, называющиеся логическими экстентами. Размер логических экстентов не меняется в пределах группы томов.

Механизмы работы LVM

Снапшоты

Снапшот - моментальный снимок, копия файлов и каталогов файловой системы на определённый момент времени.
Снимки диска позволят откатить состояние на определенный момент. Это может послужить быстрым вариантом резервного копирования. Однако нужно понимать, что данные хранятся на одном и том же физическом носителе, а значит, данный способ не является полноценным резервным копированием.

Управление разделами «на лету»

LVM увеличивает удобство работы с жестким диском, аппаратные особенности работы скрываются программным обеспечением, поэтому можно изменять размеры дисков, перемещать их «на лету», без остановки приложений или размонтирования файловых систем. Это очень удобно на серверах, когда есть возможность добавить еще один диск или расширить существующие lvm-тома «на лету».
LVM работает на уровне ядра, поэтому гарантируется максимальная прозрачность настройки и использования дисков. Программы смогут работать с логическими, виртуальными LVM-разделами, точно так же, как и с обычными.

Зеркалирование

С помощью LVM можно создать зеркальный том — данные, которые мы будем на нем сохранять, будут отправляться на 2 диска. Таким образом, если один из дисков выходит из строя, мы не потеряем свои данные.
Зеркалирование томов выполняется из группы, где есть, минимум, 2 диска.

Система управления логическими томами особенно полезна в работе с серверами, поскольку обеспечивает масштабируемость и удобное управление дисковым пространством. Она упрощает планирование дискового пространства и предотвращает проблемы, возникающие при неожиданно быстром росте занятого места в разделах. LVM не предназначен для обеспечения отказоустойчивости или высокой производительности. Поэтому он часто используется в сочетании с системами RAID.

Примеры использования LVM в РЕД ОС см. в нашей статье «Примеры использования LVM».

Примеры использования LVM

Пример №1 - Разметка дисков с помощью LVM
Пример №2 - Уменьшение размера логического тома
Пример №3 - Увеличение размера логического тома
Пример №4 - Удаление логического тома
Пример №5 - Добавление нового диска к группе томов
Пример №6 - Удаление физического диска из группы томов
Пример №7 - Расширение корневого раздела типа LVM

Вы можете подробнее ознакомиться с информацией по использованию LVM, просмотрев наши обучающие видео:

- на **RuTube** — Работа с LVM в РЕД ОС;
- в **Яндекс.Дзен** — Работа с LVM в РЕД ОС;
- в **VK Видео** — Работа с LVM в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Пример №1 - Разметка дисков с помощью LVM

Предположим, что мы имеем два неразмеченных диска подключенных к компьютеру. Теперь попробуем разметить их с помощью LVM и создать структуру, как на схеме.

Выполним команду:

```
sudo fdisk -l
```

```
[sudo] пароль для user:Диск /dev/sda: 32 GiB, 34359738368 байт, 67108864 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xfa2fa11b
Устр-во Загрузочный начало Конец Секторы Размер Идентификатор Тип
/dev/sda1 * 2048 2099199 2097152 1G 83 Linux
/dev/sda2 2099200 67108863 65009664 31G 8e Linux LVMДиск /dev/sdb: 10 GiB, 10737418240 байт, 20971520 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байтДиск /dev/sdc: 10 GiB, 10737418240 байт, 20971520 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Диск /dev/mapper/ro-root: 28 GiB, 30056382464 байт, 58703872 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Диск /dev/mapper/ro-swap: 3 GiB, 3221225472 байт, 6291456 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
```

Команда показывает диски и их разделы. Среди остальных дисков мы видим 2 диска по 10 Гб. **Диск /dev/sdb: 10 GiB** и **Диск /dev/sdc: 10 GiB.**

Создание физических томов

Сначала необходимо создать физические тома в окружении LVM из **/dev/sdb и /dev/sdc.**
Для этого используем следующую команду:

```
sudo pvcreate /dev/sdb /dev/sdc
```

```
[sudo] пароль для user:
Physical volume "/dev/sdb" successfully created.
Physical volume "/dev/sdc" successfully created.
```

Посмотрим, что у нас получилось с помощью команды pvs, которая покажет информацию о физических томах:

```
sudo pvs
```

```
PV VG Fmt Attr PSize PFree
/dev/sda2 ro lvm2 a-- <31,00g 4,00m
/dev/sdb lvm2 --- 10,00g 10,00g
/dev/sdc lvm2 --- 10,00g 10,00g
```

Основные столбцы которые нам интересны:

PV - здесь указываются физические тома
VG - принадлежность к логической группе
Fmt - формат тома
PSize - размер физического том
/dev/sda2 - это физический том, который был создан при установке РЕД ОС и на нем располагается система, но также видим, что создались два новых физических тома - **/dev/sdb и /dev/sdc** размером 10 Гб и формат их LVM2. Можем также заметить, что пока наши тома не включены ни в какую логическую группу, в отличии от **/dev/sda2** который **находится в логической группе ro.**

Более подробную информацию о физических томах выводит команда:

```
pvdisplay
```

Создание группы логических томов

Итак, физические тома созданы, приступим к созданию логической группы, для этого выполняем команду:

```
sudo vgcreate vgdata /dev/sdb /dev/sdc
```

```
[sudo] пароль для user:
Volume group "vgdata" successfully created
```

здесь vgdata - имя логической группы, /dev/sdb и /dev/sdc - физические тома.

Таким образом, мы создали логическую группу **vgdata** из двух физических томов.

Давайте посмотрим информацию о созданной логической группе **vgdata**:

```
sudo vgdisplay vgdata
```

```
--- Volume group ---**VG Name vgdata**System ID
Format lvm2
Metadata Areas 2
Metadata Sequence No 1
VG Access read/write
VG Status resizable
MAX LV 0
Cur LV 0
Open LV 0
Max PV 0
Cur PV 2
Act PV 2
VG Size 19,99 GiB
PE Size 4,00 MiB
Total PE 5118
Alloc PE / Size 0 / 0
Free PE / Size 5118 / 19,99 GiB
VG UUID rmdGbk-Sy5Y-bPns-ufg4-vyV2-Zvez-8v1ayB
```

Обратите внимание, что размер vgdata стал суммарно равен двум физическим томам, на это указывает поле VG Size.

Создание логических томов

Следующий уровень абстракции это логические тома, которые создаются на логической группе томов. Создадим три тома как на схеме 1 - mydocs, films и music.

```
sudo lvcreate -L 5G -n mydocs vgdata
```

В данной команде:

-L 5G - указывает на размер логического тома;
-n - задает имя тома;
vgdata - указываем на какой группе создавать логический том.

С помощью команды lvdisplay выведем детальную информацию о логических томах:

```
sudo lvdisplay
```

```
--- Logical volume ---LV Path /dev/ro/swapLV Name swap
VG Name ro
LV UUID O0Y4pj-Xseg-NeCQ-H1yk-nKif-as6R-zR1zKf
LV Write Access read/write
LV Creation host, time localhost, 2020-06-22 10:46:11 +0300
LV Status available
# open 2
LV Size 3,00 GiB
Current LE 768
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 254:1--- Logical volume ---LV Path /dev/ro/rootLV Name root
VG Name ro
LV UUID 9rPYsg-MKbM-DpLK-L1NN-PvcY-RrSm-2aNrV1
LV Write Access read/write
LV Creation host, time localhost, 2020-06-22 10:46:12 +0300
LV Status available
# open 1
LV Size 27,99 GiB
Current LE 7166
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 254:0--- Logical volume ---LV Path /dev/vgdata/mydocsLV Name mydocs
VG Name vgdata
LV UUID A6q4tK-3KEO-UGla-bj3t-0cZB-3Had-1bBdBH
LV Write Access read/write
LV Creation host, time localhost.localdomain, 2020-08-07 14:31:14 +0300
LV Status available
# open 0LV Size 5,00 GiBCurrent LE 1280
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 254:2
```

Видим три логических тома: /dev/ro/swap - том файла подкачки, /dev/ro/root - системный корневой раздел и наш только что созданный том **/dev/vgdata/mydocs**

Создадим второй логический том films:

```
sudo lvcreate -L 10G -n films vgdata
```

Для третьего тома music, используем все оставшееся свободное пространство, для этого в команде укажем параметр **-l 100%FREE**:

```
sudo lvcreate -l 100%FREE -n music vgdata
```

Посмотрим созданные логические тома, а также группу томов в которую они входят:

```
sudo lvs
```

```
LV VG Attr LSize
root ro -wi-ao---- 27,99g
```

```
swap ro -wi-ao---- 3,00gfilms vgdata -wi-a----- 10,00g music vgdata -wi-a----- 4,99g mydocs vgdata -wi-a----- 5,00g
```

Из вывода команды видно, что все три логические тома **films, music и mydoc** входят в группу **vgdata.**
Более подробный вывод показывает команда **lvdisplay**.

Создание файловой системы и монтирование

Следующим шагом будет создание файловой системы на логических томах и в дальнейшем ее монтирование. Приступим к созданию файловой системы ext4 на логических томах.
Для этого выполним команды:

```
sudo mkfs.ext4 /dev/vgdata/mydocs
sudo mkfs.ext4 /dev/vgdata/films
sudo mkfs.ext4 /dev/vgdata/music
```

А теперь смонтируем созданные разделы mydocs, films и music
Но, предварительно создадим для них одноименные каталоги, в качестве точки монтирования.

```
sudo mkdir /media/mydocs /media/films /media/music
```

Теперь выполним команды монтирования:

```
sudo mount /dev/vgdata/mydocs /media/mydocs/
sudo mount /dev/vgdata/films /media/films/
sudo mount /dev/vgdata/music /media/music/
```

Таким образом, мы объединили два физических диска с помощью LVM менеджера в одну логическую группу, затем разделили эту группу на желаемое количество логических томов определенных размеров и создали на них файловую систему.

Пример №2 - Уменьшение размера логического тома

Представим, что нам потребовалось уменьшить раздел films (/dev/vgdata/films), пусть новый размер раздела будет 2 Гб. Посмотрим размеры смонтированных дисков перед уменьшением:

```
sudo df -H
Файловая система Размер Испол Дост Испол%
/dev/mapper/vgdata-mydocs 5,2G 21M 4,9G 1% /media/mydocs
/dev/mapper/vgdata-films 11G 38M 9,9G 1% /media/films
/dev/mapper/vgdata-music 5,2G 21M 4,9G 1% /media/music
```

Перед уменьшением необходимо отмонтировать устройства /dev/vgdata/films:

```
sudo umount /dev/vgdata/films
```

Теперь выполним команду уменьшения размера файловой системы до 2 Гб:

```
sudo resize2fs /dev/vgdata/films 2G
resize2fs 1.42.9 (28-Dec-2013)
Please run 'e2fsck -f /dev/vgdata/films' first.
```

В данной команде параметр 2G указывает на новый желаемый размер, а не на размер на который мы уменьшаем файловую систему. При этом нам предлагается сначала выполнить проверку файловой системы, ок, сделаем это:

```
sudo e2fsck -f /dev/vgdata/films
e2fsck 1.42.9 (28-Dec-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/vgdata/films: 11/655360 files (0.0% non-contiguous), 83137/2621440 blocks
```

Пробуем еще раз запустить уменьшение:

```
sudo resize2fs /dev/vgdata/films 2G
resize2fs 1.42.9 (28-Dec-2013)
Resizing the filesystem on /dev/vgdata/films to 524288 (4k) blocks.
The filesystem on /dev/vgdata/films is now 524288 blocks long.
```

А теперь изменяем размер логического тома:

```
sudo lvreduce -L 2G /dev/vgdata/films
WARNING: Reducing active logical volume to 2,00 GiB.
THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce vgdata/films? [y/n]: y
Size of logical volume vgdata/films changed from 10,00 GiB (2560 extents) to 2,00 GiB (512 extents).
Logical volume vgdata/films successfully resized.
```

Примонтируем раздел и посмотрим размер файловой системы:

```
sudo mount /dev/vgdata/films /media/films/
```

```
sudo df -H
/dev/mapper/vgdata-mydocs 5,2G 21M 4,9G 1% /media/mydocs
/dev/mapper/vgdata-music 5,2G 21M 4,9G 1% /media/music
/dev/mapper/vgdata-films 2,0G 26M 1,9G 2% /media/films
```

Как видим новый размер тома films стал 2Гб.

Пример №3 - Увеличение размера логического тома

Перед увеличением размера тома посмотрим свободное место в логической группе:

```
sudo vgdisplay vgdata
```

```
--- Volume group ---
VG Name vgdata
System ID
Format lvm2
Metadata Areas 2
Metadata Sequence No 11
VG Access read/write
VG Status resizable
MAX LV 0
Cur LV 3
Open LV 3
Max PV 0
Cur PV 2
Act PV 2
VG Size 19,99 GiB
PE Size 4,00 MiB
Total PE 5118
Alloc PE / Size 3070 / 11,99 GiB**Free PE / Size 2048 / 8,00 GiB**VG UUID rmdGbk-Sy5Y-bPns-ufg4-vyV2-Zvez-8v1ayB
```

Видно что в группе свободно 8 Гб, это тот размер который освободился от тома /dev/vgdata/films

Возьмем их и добавим к /dev/vgdata/music, тем самым увеличив размер тома music на 8 Гб. В отличие от уменьшения, увеличение размера логического тома происходит “на лету” без необходимости размонтирования файловой системы. Выполняем команду:

```
sudo lvextend -L +8G /dev/vgdata/music
Size of logical volume vgdata/music changed from 4,99 GiB (1278 extents) to 8,00 GiB (2048 extents).
Logical volume vgdata/music successfully resized.
```

Теперь необходимо расширить файловую систему на этом логическом томе:

```
sudo resize2fs /dev/vgdata/music
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/vgdata/music is mounted on /media/music; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 2
The filesystem on /dev/vgdata/music is now 3405824 blocks long.
```

Смотрим получившейся размер раздела music:

```
sudo df -h
```

```
Файловая система Размер Использовано Дост Использовано%
/dev/mapper/vgdata-mydocs 4,8G 20M 4,6G 1% /media/mydocs
/dev/mapper/vgdata-music 13G 25M 13G  1% /media/music
/dev/mapper/vgdata-films 1,9G 25M 1,8G 2% /media/films
```

Пример №4 - Удаление логического тома

Перед удалением логического тома не забудьте сохранить необходимые данные, после этого размонтируйте раздел.

```
sudo umount /dev/vgdata/films
```

Команда удаления:

```
sudo lvremove /dev/vgdata/films
Do you really want to remove active logical volume vgdata/films? [y/n]: y
Logical volume "films" successfully removed
```

В результате на логической группе освободится место.

Пример №5 - Добавление нового диска к группе томов

Для эксперимента мы подключили диск размером 2 Гб к нашей тестовой системе и попробуем включить его в логическую группу LVM - /dev/vgdata

Выведем текущую информацию о дисках:

```
sudo lvmdiskscan
/dev/ro/root [ 27,99 GiB]
/dev/sda1 [ 1,00 GiB]
/dev/ro/swap [ 3,00 GiB]
/dev/sda2 [ <31,00 GiB] LVM physical volume
/dev/vgdata/mydocs [ 5,00 GiB]
/dev/vgdata/music [ 12,99 GiB]
/dev/sdb [ 10,00 GiB] LVM physical volume
/dev/sdc [ 10,00 GiB] LVM physical volume/dev/sdd [ 2,00 GiB]
```

Новый диск - это **/dev/sdd,** размер его 2 Гб, но тип его не является LVM physical volume, а размер группы vgdata равен 20 Гб.

```
sudo vgs vgdata
VG #PV #LV #SN Attr VSize VFree
vgdata 2 2 0 wz--n- 19,99g 2,00g
```

После добавления размер группы должен стать 22 Гб. Для начала, как и в первой первом примере про разбивку диска с помощью LVM, нам нужно создать из **/dev/sdd** физический том. На данный момент мы видим только существующие физические тома куда не входит /dev/sdd.

```
sudo lvmdiskscan -l
WARNING: only considering LVM devices
/dev/sda2 [ <31,00 GiB] LVM physical volume
/dev/sdb [ 10,00 GiB] LVM physical volume
/dev/sdc [ 10,00 GiB] LVM physical volume
2 LVM physical volume whole disks
1 LVM physical volume
```

Выполняем команду создания физического тома:

```
sudo pvcreate /dev/sdd
Physical volume "/dev/sdd" successfully created.
```

Добавляем физический том в группу vgdata:

```
sudo vgextend vgdata /dev/sdd
Volume group "vgdata" successfully extended
```

Теперь мы видим, что размер группы увеличился на 2 Гб и свободно 4 Гб,

```
sudo vgs vgdata
VG #PV #LV #SN Attr VSize VFree
vgdata 3 2 0 wz--n- <21,99g <4,00g
```

Доступное свободное пространство может быть перераспределено на любой логический раздел, что позволяет увеличить его размер. Данные операции были рассмотрены в предыдущих примерах.

Пример №6 - Удаление физического диска из группы томов

Рассмотрим следующий пример. Представим, что системному администратору потребовалась заменить жесткий диск на другой. При этом данный диск входит в логическую группу LVM. Поэтому первым шагом необходимо убрать из работающей группы томов этот диск, в нашем случае пусть это будет /dev/sdd

Смотрим текущие состояние /dev/sdd и видим что он входит в группу vgdata и имеет размер 2 Гб.

```
sudo pvs
PV VG Fmt Attr PSize PFree
/dev/sda2 ro lvm2 a-- <31,00g 4,00m
/dev/sdb vgdata lvm2 a-- <10,00g 0
/dev/sdc vgdata lvm2 a-- <10,00g 2,00g
/dev/sdd vgdata lvm2 a-- <2,00g <2,00g
```

Прежде чем его удалить, перенесем данные которые на нем записаны:

```
sudo pvmove /dev/sdd
No data to move for vgdata.
```

Но, поскольку у нас тестовый стенд и данных на дисках нет, то и команда нам сообщает, что данных для переноса нет. Выполняем следующую команду - это удаление из логической группы диск:

```
sudo vgreduce vgdata /dev/sdd
Removed "/dev/sdd" from volume group "vgdata"
```

Удаляем физический диск:

```
sudo pvremove /dev/sdd
Labels on physical volume "/dev/sdd" successfully wiped.
```

Теперь видим, что диск удалился:

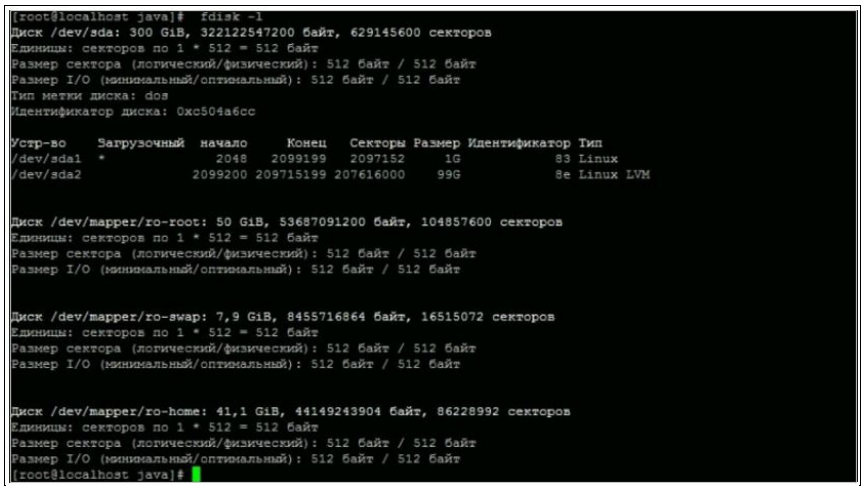
```
sudo pvs
PV VG Fmt Attr PSize PFree
/dev/sda2 ro lvm2 a-- <31,00g 4,00m
/dev/sdb vgdata lvm2 a-- <10,00g 0
/dev/sdc vgdata lvm2 a-- <10,00g 2,00g
```

А значит его можно заменить другим. Как добавить новый диск мы рассмотрели в примере “Пример №5 - Добавление нового диска к группе томов”.

Пример №7 - Расширение корневого раздела типа LVM

Для того чтобы увеличить корневой раздел, используя всё свободное пространство диска **sda**, необходимо выполнить следующие действия: 1. Проверить состояние файловой системы, доступные разделы и свободное место, используя команду:

```
fdisk -l
```

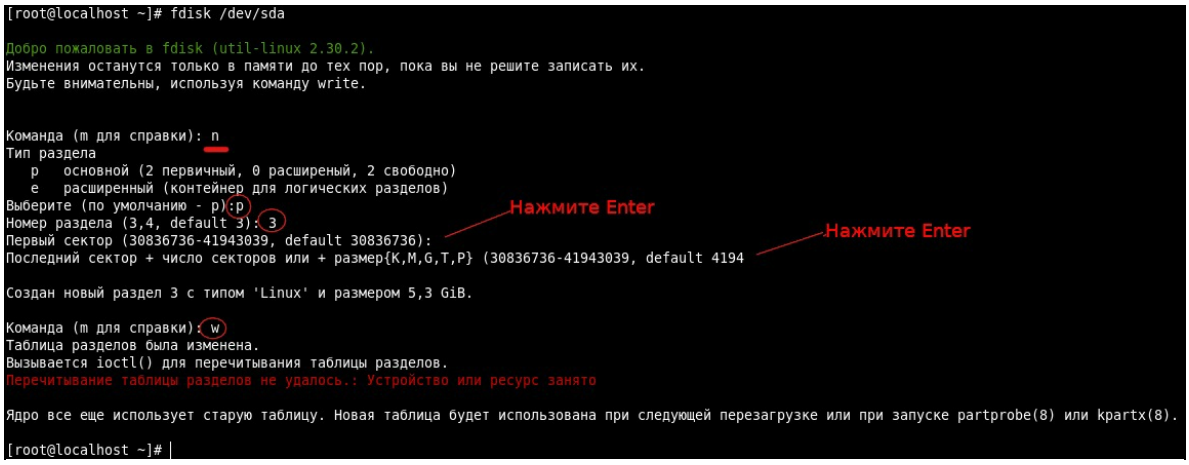


В выводе команды видно, что диск **/dev/sda** имеет размер 300 ГБ, а раздел **/dev/sda2** имеет размер 99 ГБ. На разделе **/dev/sda2** расположены lvm-разделы: • корневой(ro-root) — 50 ГБ; • swap (ro-swap) — 7.9 ГБ; • домашний (ro-home) — 41.1 ГБ.

2. Далее необходимо создать новый раздел, воспользовавшись командой:

```
fdisk /dev/sda
```

Для создания нового раздела требуется ввести нужную команду («**n**») и нажать клавишу «*Enter*». Далее предлагается выбрать тип, который будет установлен для создаваемого раздела, основной («**p**») или расширенный («**e**»). В данном случае следует выбрать основной тип – «**p**». А также необходимо выбрать порядковый номер, который будет присвоен новому разделу, в данном случае – « **3**». Для секторов можно оставить значения по умолчанию, нажав клавишу «*Enter*». Затем остаётся внести изменения в таблицу разделов командой «**w**». После этого терминал сообщает, что изменения в таблицу разделов внесены, а это означает, что новый раздел создан.



Чтобы операционная система узнала о новых границах разделов без перезагрузки, необходимо выполнить команду:

```
partprobe /dev/vda
```

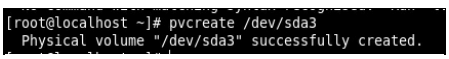
Чтобы убедиться, что внесённые изменения применены, используйте команду:

```
fdisk -l
```

В выводе команды видно, что появился новый раздел **/dev/sda3** размером 200 ГБ.

3. Следующим шагом нужно создать LVM физический том из раздела **sda3**, набрав команду:

```
pvcreate /dev/sda3
```



4. Следует проверить существующую логическую группу, чтобы затем добавить в неё новый физический том. Для этого используются команды:

```
vgs
```

```
[root@localhost ~]# vgs
  VG #PV #LV #SN Attr   VSize   VFree
  ro   1   3   0 wz--n- <13,70g 4,00m
```

```
vgextend ro /dev/sda3
```

```
[root@localhost ~]# vgextend ro /dev/sda3
  Volume group "ro" successfully extended
```

5. Для определения корневого раздела необходимо вывести список существующих логических томов, используя команду:

```
lvdisplay
```

```
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Path                /dev/ro/swap
  LV Name                swap
  VG Name                ro
  LV UUID                XbCnjV-WkUs-SAlh-tbG8-dJmf-s83P-B7s3TH
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:33 +0300
  LV Status              available
  # open                 2
  LV Size                <7,88 GiB
  Current LE             2016
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:1

  --- Logical volume ---
  LV Path                /dev/ro/home
  LV Name                home
  VG Name                ro
  LV UUID                9abMf8-L5u9-RR4j-qdBB-Usxo-BgXK-cUDngx
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:34 +0300
  LV Status              available
  # open                 1
  LV Size                <41,12 GiB
  Current LE             10526
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:2

  --- Logical volume ---
  LV Path                /dev/ro/root
  LV Name                root
  VG Name                ro
  LV UUID                OZx76J-FRay-e5wi-XA5u-f1Cp-r5se-1NIfOM
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:37 +0300
  LV Status              available
  # open                 1
  LV Size                50,00 GiB
  Current LE             12800
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:0
```

В выводе команды видно, что корневой раздел — это /dev/ro/root, его и следует расширить. Для этого используется команда:

```
lvextend -l +100%FREE /dev/ro/root
```

```
[root@localhost ~]# lvextend -l +100%FREE /dev/ro/root
  Size of logical volume ro/root changed from 50,00 GiB (12800 extents) to 250,00 GiB (64000 extents).
  Logical volume ro/root successfully resized.
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Path                /dev/ro/swap
  LV Name                swap
  VG Name                ro
  LV UUID                XbCnjV-WkUs-SA1h-tbG8-dJmf-s83P-B7s3TH
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:33 +0300
  LV Status              available
  # open                 2
  LV Size                <7,88 GiB
  Current LE             2016
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:1

  --- Logical volume ---
  LV Path                /dev/ro/home
  LV Name                home
  VG Name                ro
  LV UUID                9abMf8-L5u9-RR4j-qdBB-Usxo-BqXK-oUDngx
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:34 +0300
  LV Status              available
  # open                 1
  LV Size                <41,12 GiB
  Current LE             10526
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:2

  --- Logical volume ---
  LV Path                /dev/ro/root
  LV Name                root
  VG Name                ro
  LV UUID                OZx76J-FRay-e5wi-XA5u-f1Cp-r5se-1NIfOM
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:37 +0300
  LV Status              available
  # open                 1
  LV Size                250,00 GiB
  Current LE             64000
  Segments               2
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:0

[root@localhost ~]#
```

После расширения раздела, необходимо изменить размер файловой системы.

6. Изменение размера файловой системы
6.1 Перед изменением размера файловой системы необходимо выполнить проверку файловой системы на ошибки, для файловой системы ext4:

```
e2fsck -f /dev/ro/root
```

Если используется файловая система xfs, то команда будет следующая:

```
xfs_growfs /dev/ro/root
```

6.2 Следующая команда автоматически расширяет файловую систему до максимально доступного размера:

```
resize2fs /dev/ro/root
```

```
[root@localhost ~]# resize2fs /dev/ro/root
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/ro/root is mounted on /; on-line resizing required
old_desc_blocks = 7, new_desc_blocks = 32
The filesystem on /dev/ro/root is now 65536000 blocks long.
```

Для просмотра размеров разделов используется команда:

```
df -h
```

```
[root@localhost ~]# resize2fs /dev/ro/root
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/ro/root is mounted on /; on-line resizing required
old_desc_blocks = 7, new_desc_blocks = 32
The filesystem on /dev/ro/root is now 65536000 blocks long.

[root@localhost ~]# 0
-bash: 0: команда не найдена
[root@localhost ~]# dh -h
-bash: dh: команда не найдена
[root@localhost ~]# df -h
Файловая система    Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs              3,9G            0  3,9G            0% /dev
tmpfs                 3,9G           24K  3,9G            1% /dev/shm
tmpfs                 3,9G         9,3M  3,9G            1% /run
tmpfs                 3,9G            0  3,9G            0% /sys/fs/cgroup
/dev/mapper/ro-root   246G         5,7G  230G            3% /
/dev/sda1             976M         126M  784M           14% /boot
/dev/mapper/ro-home    41G         1,6G   37G            4% /home
tmpfs                 797M           24K  797M            1% /run/user/1000
tmpfs                 797M            0  797M            0% /run/user/0
[root@localhost ~]#
```

Как видно из вывода команды, корневой раздел ro-root расширился и имеет размер памяти 246 ГБ.

Утилиты для работы с дисковым пространством

Утилита df — просмотр свободного пространства
Утилита du — просмотр занятого пространства
Утилита find — поиск файлов большого размера

Вы можете подробнее ознакомиться с информацией по поиску файлов в системе и оценке свободного дискового пространства, просмотрев наши обучающие видео:

- на **RuTube**:
  - Утилиты поиска файлов;
  - Анализ занятого пространства на дисках.
- в **Яндекс.Дзен**:
  - Утилиты поиска файлов;
  - Анализ занятого пространства на дисках.
- в **VK Видео**:
  - Утилиты поиска файлов;
  - Анализ занятого пространства на дисках.

На наших каналах вы также сможете найти много другой полезной информации.

Утилита df - просмотр свободного пространства

df — стандартная утилита проверки свободного места, позволяет выводить список подключенных устройств, информацию о занятом месте, а также точку монтирования.

Синтаксис:

```
df <опции> [устройство]
```

Атрибуты:

- **-a**, **--all** - отобразить все файловые системы, в том числе виртуальные, псевдо и недоступные;
- **-B** - изменить размер одного блока перед выводом данных, например, можно использовать BM, чтобы вывести все данные в мегабайтах;
- **-h** - выводить размеры в читаемом виде, в мегабайтах или гигабайтах;
- **-H** - выводить все размеры в гигабайтах;
- **-i** - выводить информацию об inode;
- **-k** - выводить размеры в килобайтах;
- **--output** - использовать специальный формат вывода, если не задано, выводит все поля. Доступны такие варианты: 'source', 'fstype', 'itotal', 'iused', 'iavail', 'ipcent', 'size', 'used', 'avail', 'pcent', 'file' и 'target';
- **-P** - использовать формат вывода POSIX;
- **--total** - выводить всю информацию про использованное и доступное место;
- **-t**, **--type** - выводить информацию только про указанные файловые системы;
- **-x** - выводить информацию обо всех, кроме указанных, файловых системах.

Использование:

Для того чтобы просмотреть доступное пространство на всех примонтированных разделах и информацию о них, выполните:

```
df

Файловая система        1K-блоков Использовано Доступно Использовано% Смонтировано в
devtmpfs                   479228         0   479228         0% /dev
tmpfs                      497892         0   497892         0% /dev/shm
tmpfs                      199160      3224   195936         2% /run
/dev/mapper/ro_redos-root  17410832    8998132  7505232        55% /
/dev/sda1                  999320      174776   755732        19% /boot
tmpfs                      99576         76    99500         1% /run/user/42
```

```
tmpfs                    99576         132    99444           1% /run/user/1000
/dev/sr0                4533928     4533928        0         100% /run/media/user/redos-MUROM-7.3.1 x86_64
```

Для просмотра свободного пространства какого-либо раздела в наиболее читаемом формате выполните:

```
df -h /root

Файловая система         Размер Использовано  Дост Использовано% Смонтировано в
/dev/mapper/ro_redos-root    17G        8,7G  7,2G          55% /
```

Утилита du — просмотр занятого пространства

du — утилита, которая позволяет вывести размер всех файлов в определённой папке в байтах или в более удобном формате.

Синтаксис:

```
du <опции> <путь_к_папке>
```

Атрибуты:

- **-a**, **--all** - выводить размер для всех файлов, а не только для директорий, по умолчанию размер выводится только для папок;
- **-B**, **--block-size** - указать единицы вывода размера, доступно: K,M,G,T,P,E,Z,Y для 1024 и KB, MB и т. д. - для 1000;
- **-c**, **--total** - выводить в конце общий размер всех папок;
- **-d**, **--max-depth** - максимальная глубина вложенности директорий;
- **-h**, **--human-readable** - выводить размер в единицах измерения, удобных для человека;
- **--inodes** - выводить информацию об использовании inode;
- **-L**, **--dereference** - следовать по всем символическим ссылкам;
- **-l**, **--count-links** - учитывать размер файла несколько раз для жестких ссылок;
- **-P**, **--no-dereference** - не следовать по символическим ссылкам, это поведение используется по умолчанию;
- **-S**, **--separate-dirs** - не включать размер подпапок в размер папки;
- **--si** - выводить размер файлов и папок в системе Си, используется 1000 вместо 1024;
- **-s**, **--summarize** - выводить только общий размер;
- **-t**, **--threshold** - не учитывать файлы и папки с размером меньше указанного;
- **--time** - отображать время последней модификации для файла или папки, вместо времени модификации можно выводить такие метки, как atime, access, use, ctime;
- **-X**, **--exclude** - исключить файлы из подсчёта;
- **-x**, **--one-file-system** - пропускать примонтированные файловые системы;
- **--version** - вывести версию утилиты.

Использование:

Для просмотра занимаемого пространства теми или иными файлами в какой-либо папке, выполните команду:

```
du /home/user

4    ./Документы/test_dir
328    ./Документы/dark-matter/icons
2336    ./Документы/dark-matter
412    ./Документы/Hoshimati Suisei/Suisei/icons
3584    ./Документы/Hoshimati Suisei/Suisei
5568    ./Документы/Hoshimati Suisei
212    ./Документы/THEMES/Vimix-4k/Vimix/icons
3136    ./Документы/THEMES/Vimix-4k/Vimix
4504    ./Документы/THEMES/Vimix-4k
4508    ./Документы/THEMES
16284    ./Документы

 ...
```

```
8    ./.config/caja-actions
4    ./.config/imsettings
4    ./.config/menus/applications-merged
8    ./.config/menus
62184    ./.config
4    ./.themes
1230796    .
```

Для более читаемого вывода команды можно добавить дополнительные опции:

```
du -sh /home/user

1,2G    /home/user
```

Утилита find - поиск файлов большого размера

Утилита find - одна из наиболее важных и часто используемых утилит системы, которая позволяет осуществлять поиск файлов и каталогов на основе специальных условий. Ее можно использовать в различных обстоятельствах, например, для поиска файлов по разрешениям, владельцам, группам, типу, размеру и другим подобным критериям.

Чтобы при помощи find найти файлы большого размера необходимо выполнить:

```
find . -xdev -type f -size +<необходимый_размер>
```

Например:

```
find . -xdev -type f -size +100M

./Загрузки/Yandex.rpm
./Загрузки/FreeCAD_0.19.3-Linux-Conda_glibc2.12-x86_64.AppImage
```

Вывести файлы в более удобном формате можно следующим образом:

```
find . -xdev -type f -size +10m -print | xargs ls -lh | sort -k5,5 -h -r | head

-rwxrwxr-x. 1 user user 914M мая 11 17:52 ./Загрузки/FreeCAD_0.19.3-Linux-Conda_glibc2.12-x86_64.AppImage
-rw-rw-r--. 1 user user 104M апр 27 12:05 ./Загрузки/Yandex.rpm
-rw-------. 1 user user  11M апр 25 10:09 ./.config/chromium/OnDeviceHeadSuggestModel/20220409.440702358/cr_ru_2022-04-
09_440702358_500000_index.bin
```

Мониторинг файловой системы с помощью duf

Установка
Синтаксис утилиты
Опции
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: duf-0.8.1-1

Duf (**Disk Usage/Free**) — это терминальная утилита, которая позволяет удобно отображать информацию о дисковом пространстве. Она предоставляет подробные данные о свободном и занятом пространстве на дисках в удобочитаемой и визуально понятной форме по сравнению с классическими утилитами, такими как **df** и **du**.

Основные характеристики:

- цветовое отображение для легкого восприятия;
- настройка в соответствии с тематикой и шириной терминала;
- сортировка результатов в соответствии с потребностями пользователя;
- группировка и фильтрация устройств;
- вывод данных в различных форматах, таких как *JSON*, что позволяет их интегрировать в другие инструменты.

Установка

Для установки утилиты через терминал выполните команду (потребуются права **администратора**):

```
dnf install duf
```

Синтаксис утилиты

Синтаксис утилиты имеет вид:

```
duf [<опции>] [<параметры>]
```

Опции

К основным опциям утилиты относятся:

- **-all** — отобразить все файловые системы, включая псевдоустройства, дублирующиеся и недоступные файловые системы;
- **-avail-threshold** — указать пороговое значение для подсвечивания столбца avail (доступное пространство) в выводе. Указанное значение используется для подсвечивания различных уровней доступного дискового пространства определенным цветом для облегчения визуальной оценки состояния дисков. По умолчанию, если объем доступного дискового пространства менее 10 ГБ, значение будет подсвечено желтым цветом. Если объем доступного дискового пространства менее 1 ГБ, значение будет подсвечено красным цветом;
- **-hide** — используется для скрытия определенных типов устройств в выводе (указываются через запятую).

  Возможные значения для -hide:

  - *local*: локальные устройства;
  - *network*: сетевые устройства;
  - *fuse*: FUSE (Filesystem in Userspace) устройства;
  - *special*: специальные устройства;
  - *loops*: loopback устройства;
  - *binds*: устройства, смонтированные с использованием bind mount.

- **-hide-fs** — исключить из отображаемого списка конкретные типы файловых систем, разделенные запятыми;
- **-hide-mp** — скрыть определенные точки монтирования, разделенные запятыми (поддерживаются шаблоны для указания групп точек монтирования);
- **-inodes** — отобразить информацию об индексных дескрипторах вместо использования блоков. Индексные дескрипторы представляют собой структурные элементы файловой системы, которые содержат информацию о файлах и каталогах;

- **-json** — вывести все устройства в формате JSON, используется для интеграции с другими инструментами и для автоматизированной обработки данных;
- **-only** — показать только определенные устройства, разделенные запятыми: *local*, *network*, *fuse*, *special*, *loops*, *binds*;
- **-only-fs** — показать только определенные файловые системы, разделенные запятыми;
- **-only-mp** — показать только определенные точки монтирования, разделенные запятыми (поддерживаются шаблоны для указания групп точек монтирования);
- **-output** — определить, какие поля будут включены в вывод: *mountpoint*, *size*, *used*, *avail*, *usage*, *inodes*, *inodes_used*, *inodes_avail*, *inodes_usage*, *type*, *filesystem*;
- **-sort** — сортировать вывод по указанным полям: *mountpoint*, *size*, *used*, *avail*, *usage*, *inodes*, *inodes_used*, *inodes_avail*, *inodes_usage*, *type*, *filesystem* (по умолчанию - «*mountpoint*»);
- **-style** — определить стиль вывода: *unicode*, *ascii* (по умолчанию - «*unicode*»);
- **-theme** — установить цветовую тему вывода: *dark*, *light*, *ansi* (по умолчанию - «*dark*»);
- **-usage-threshold** — указать пороговое значение для окрашивания полос использования (желтый, красный) в виде числа с плавающей точкой от 0 до 1 (по умолчанию - «0.5,0.9»);
- **-version** — показать версию утилиты duf;
- **-warnings** — вывести все предупреждения в STDERR;
- **-width** — максимальная ширина вывода.

Примеры использования

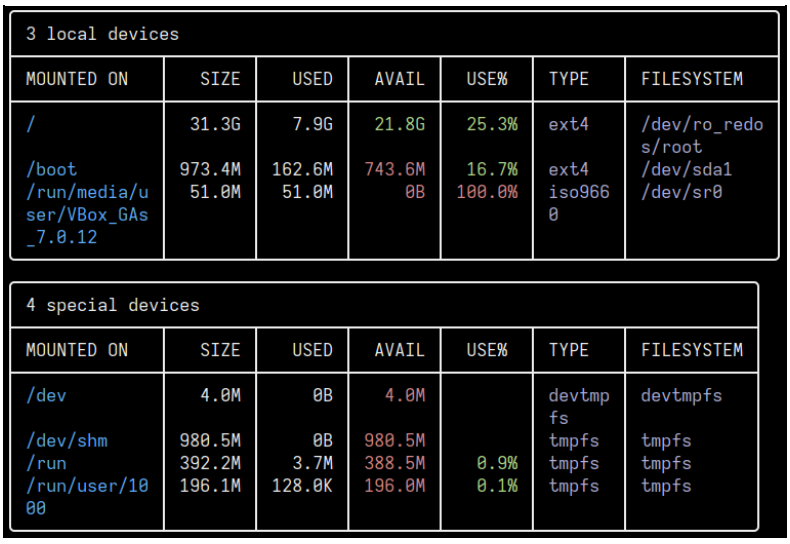
Пример 1. Базовое использование

Для отображения основной информации об использовании дискового пространства выполните команду в терминале:

```
duf
```

Команда **duf** без использования опций выводит основную информацию обо всех файловых системах в удобочитаемом формате с цветовым выделением. По умолчанию отображаются такие колонки, как точка монтирования, размер, использованное пространство, доступное пространство, использование в процентном соотношении, тип и имя файловой системы.

Результат выполнения:



3 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	16.7%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	51.0M	51.0M	0B	100.0%	iso9660	/dev/sr0

4 special devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/dev/shm	980.5M	0B	980.5M		tmpfs	tmpfs
/run	392.2M	3.7M	388.5M	0.9%	tmpfs	tmpfs
/run/user/1000	196.1M	128.0K	196.0M	0.1%	tmpfs	tmpfs

Для каждого типа устройства выводится информация в виде таблицы. Утилита разделяет всю информацию в таблице на колонки, в которых освещена следующая информация:

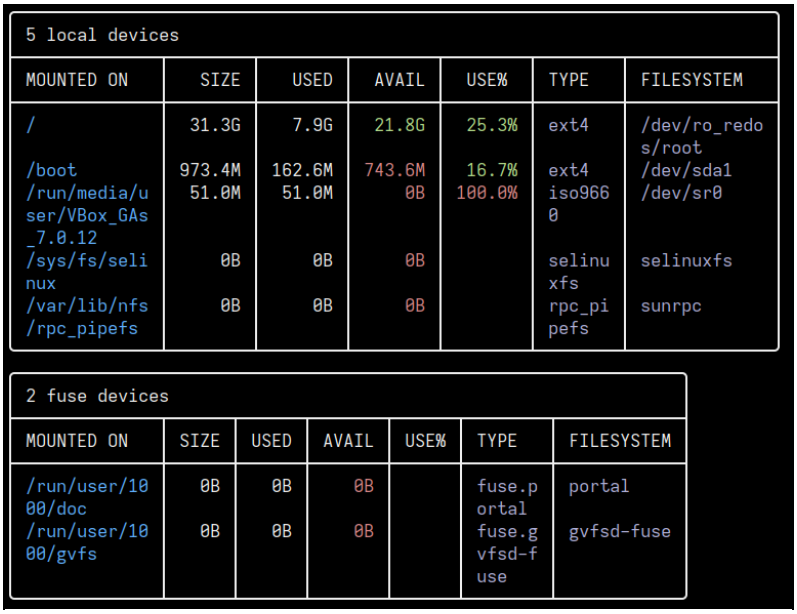
- **MOUNTED ON** — точка монтирования файловой системы, то есть путь в файловой системе, где устройство смонтировано;
- **SIZE** — общий размер файловой системы;
- **USED** — объем занятого пространства на файловой системе;
- **AVAIL** — объем доступного (свободного) пространства на файловой системе;
- **USE%** — процент использованного дискового пространства на файловой системе;
- **TYPE** — тип файловой системы;
- **FILESYSTEM** — имя или путь к устройству или файловой системе.

Пример 2. Показать все файловые системы, включая псевдоустройства и дублирующиеся устройства

Для отображения в выводе всех файловых систем, включая псевдоустройства, дублирующиеся и недоступные файловые системы используется опция **-all**. Она позволяет получить полное представление обо всех файловых системах, включая те, которые обычно скрыты.

```
duf -all
```

Результат выполнения:



5 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	16.7%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	51.0M	51.0M	0B	100.0%	iso9660	/dev/sr0
/sys/fs/selinux	0B	0B	0B		selinuxfs	selinuxfs
/var/lib/nfs/rpc_pipefs	0B	0B	0B		rpc_pipefs	sunrpc

2 fuse devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/run/user/1000/doc	0B	0B	0B		fuse.portal	portal
/run/user/1000/gvfs	0B	0B	0B		fuse.gvfsd-fuse	gvfsd-fuse

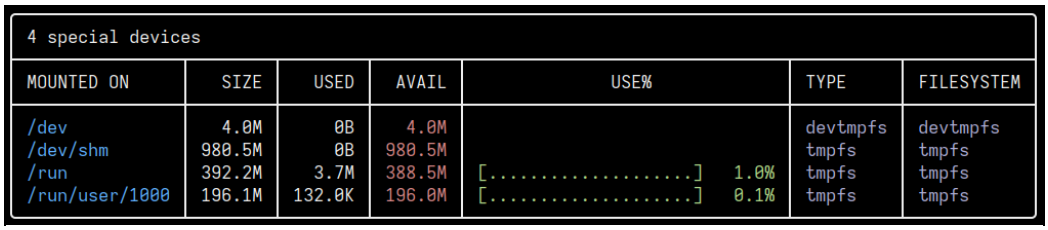
Пример 3. Скрыть определенные устройства

Для исключения из вывода локальных и сетевых устройств используется опция **-hide**.

```
duf -hide local,network
```

Это может быть полезно, если необходимо вывести только определенные типы устройств, исключив ненужные.

Результат выполнения:



4 special devices

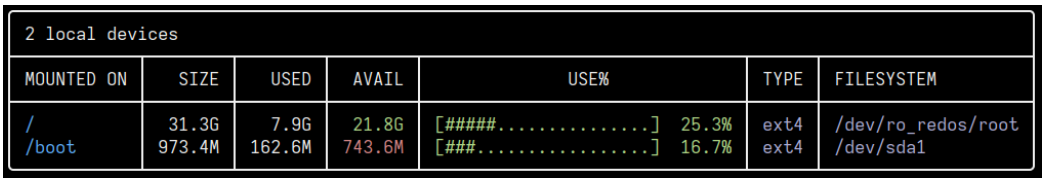
MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/dev/shm	980.5M	0B	980.5M		tmpfs	tmpfs
/run	392.2M	3.7M	388.5M	[..................] 1.0%	tmpfs	tmpfs
/run/user/1000	196.1M	132.0K	196.0M	[..................] 0.1%	tmpfs	tmpfs

Пример 4. Отобразить только определенные файловые системы

Опция **-only** используется для фильтрации по конкретным типам файловых систем. Для отображения только необходимых файловых систем, которые имеют тип *ext4* или *xfs,* введите команду:

```
duf -only-fs ext4,xfs
```

Результат выполнения:



2 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	[#####..............] 25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	[###................] 16.7%	ext4	/dev/sda1

Пример 5. Вывод в формате JSON

Опция **-json** позволит вывести всю информацию о файловых системах в формате *JSON*. Это удобно для последующего анализа или использования в других скриптах и инструментах:

```
duf -json
```

Результат выполнения:

```
{
 "device": "binfmt_misc",
 "device_type": "special",
 "mount_point": "/proc/sys/fs/binfmt_misc",
 "fs_type": "binfmt_misc",
 "type": "binfmt_misc",
 "opts": "rw,nosuid,nodev,noexec,relatime",
 "total": 0,
 "free": 0,
 "used": 0,
 "inodes": 0,
 "inodes_free": 0,
 "inodes_used": 0,
 "blocks": 0,
 "block_size": 4096
}
```

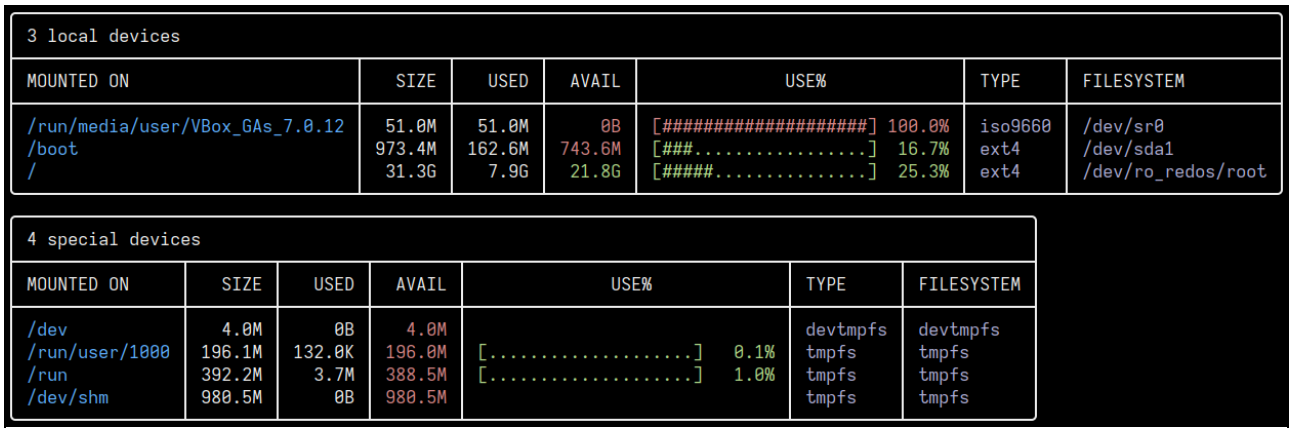

Пример 6. Сортировка по размеру

Для сортировки информации в столбцах таблицы можно воспользоваться опцией **-sort** с указанием столбца. Это позволяет легко увидеть, какие файловые системы имеют наибольший или наименьший размер.

Например, для сортировки выводимой информации по величине общего размера введите в терминале:

```
duf -sort size
```

Результат выполнения:



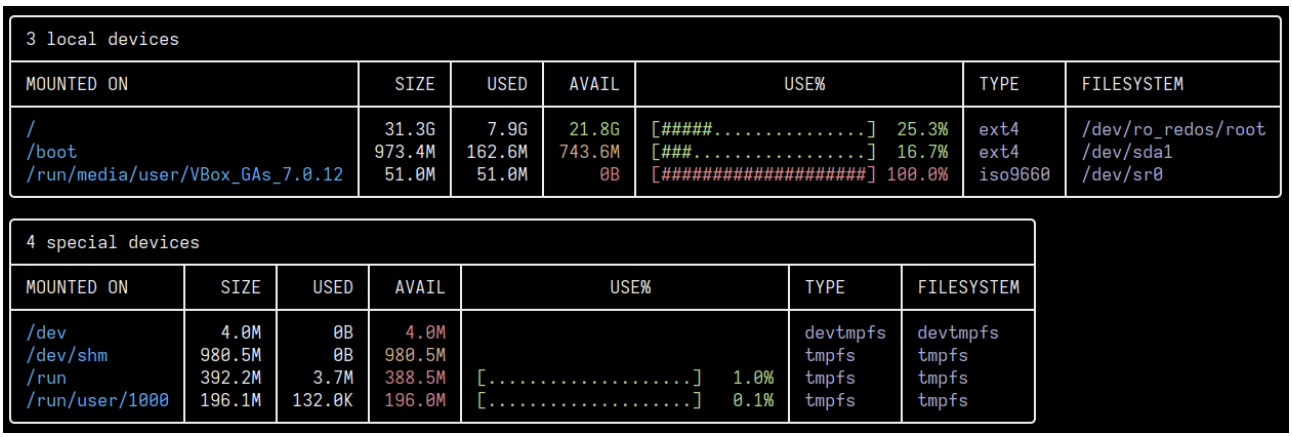
Пример 7. Установка порога для подсвечивания доступного пространства

Опция **-avail-threshold** устанавливает пороговые значения для подсвечивания столбца avail (доступное пространство).

```
duf -avail-threshold 5G,500M
```

В данном примере, если доступное место меньше 5 ГБ, оно будет подсвечено желтым цветом, а если меньше 500 МБ — красным.

Результат выполнения:

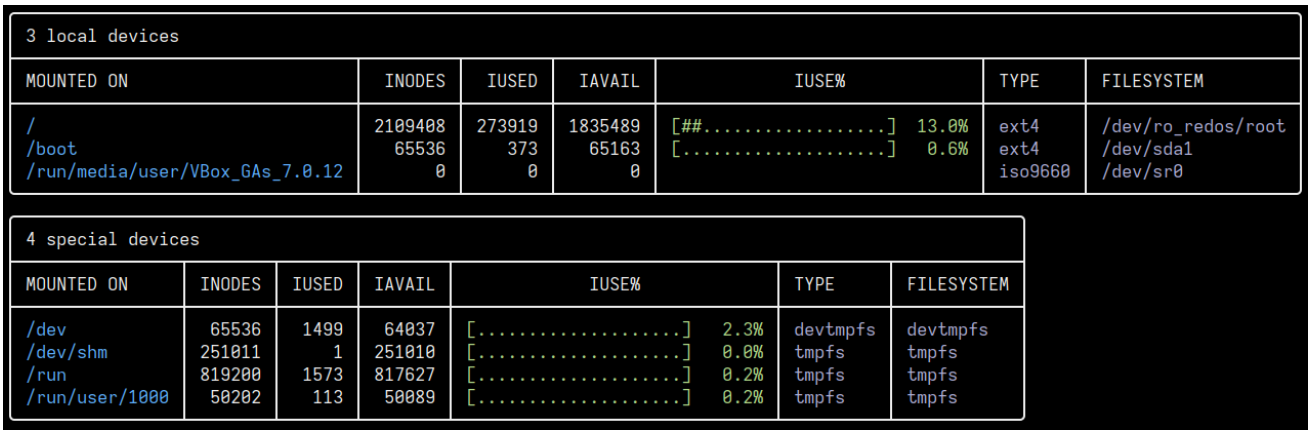


Пример 8. Показать информацию об индексных дескрипторах (inodes)

Для отображения информации об индексных дескрипторах вместо стандартных данных о блоках используется опция **-inodes**. Информация включает количество индексных дескрипторов, использованные и доступные индексные дескрипторы, а также процент использования индексных дескрипторов. Например:

```
duf -inodes
```

Результат выполнения:



3 local devices

MOUNTED ON	INODES	IUSED	IAVAIL	IUSE%	TYPE	FILESYSTEM
/	2109408	273919	1835489	[##.....] 13.0%	ext4	/dev/ro_redos/root
/boot	65536	373	65163	[.....] 0.6%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	0	0	0		iso9660	/dev/sr0

4 special devices

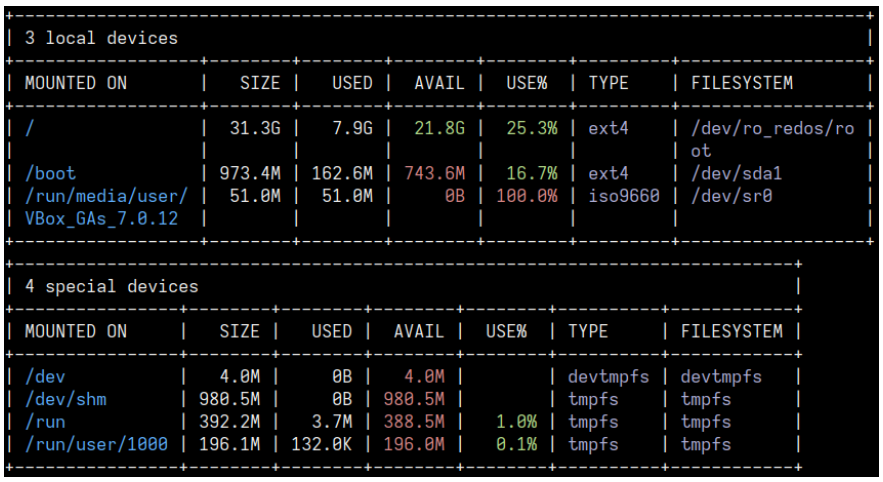
MOUNTED ON	INODES	IUSED	IAVAIL	IUSE%	TYPE	FILESYSTEM
/dev	65536	1499	64037	[.....] 2.3%	devtmpfs	devtmpfs
/dev/shm	251011	1	251010	[.....] 0.0%	tmpfs	tmpfs
/run	819200	1573	817627	[.....] 0.2%	tmpfs	tmpfs
/run/user/1000	50202	113	50089	[.....] 0.2%	tmpfs	tmpfs

Пример 9. Выбор стиля отображения

Опция **-style** с параметром **<ascii>** устанавливает стиль отображения в формате ASCII вместо Unicode. Это может быть полезно для систем, где поддержка Unicode ограничена.

```
duf -style ascii
```

Результат выполнения:



3 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	16.7%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	51.0M	51.0M	0B	100.0%	iso9660	/dev/sr0

4 special devices

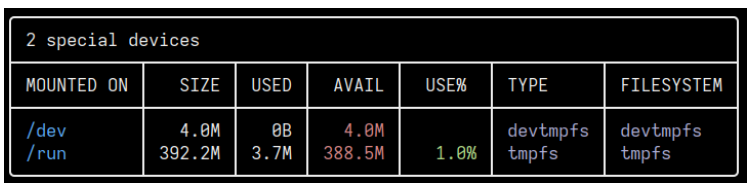
MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/dev/shm	980.5M	0B	980.5M		tmpfs	tmpfs
/run	392.2M	3.7M	388.5M	1.0%	tmpfs	tmpfs
/run/user/1000	196.1M	132.0K	196.0M	0.1%	tmpfs	tmpfs

Пример 10. Показать только определенные точки монтирования

Для фокусировки на конкретных директориях полезна опция **-only-mp.** В примере будут отображены только те файловые системы, которые смонтированы в точках /dev и /run.

```
duf -only-mp /dev,/run
```

Результат выполнения:



2 special devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/run	392.2M	3.7M	388.5M	1.0%	tmpfs	tmpfs

Пример 11. Показать информацию о файловой системе

Для отображения информации о конкретном разделе файловой системы или устройстве хранения информации нужно выполнить следующую команду:

```
duf /home
```

Результат выполнения:

1 local device

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root

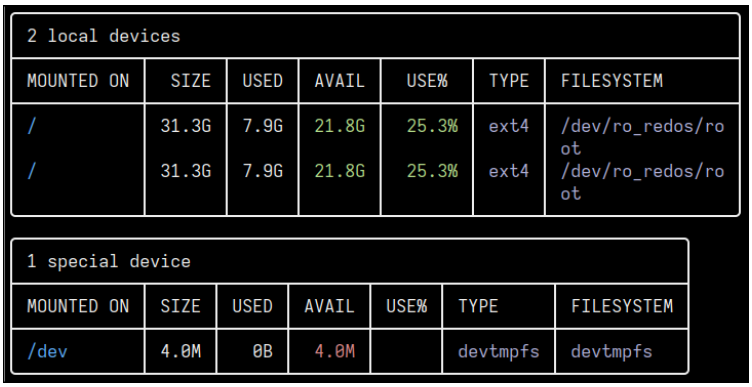
Утилита **duf** анализирует файловую систему, на которой находится директория /home, и выводит информацию о ней.

Пример 12. Показать информацию о файловых системах

В приведенном ниже примере duf выводит информацию о файловых системах, на которых смонтированы директории /dev, /etc/opt и /var/log. Выходные данные имеют три записи, каждая из которых соответствует устройству для одного из входных путей:

```
duf /dev /etc/opt /var/log
```

Результат выполнения:



Пример 13. Вывод информации о точках монтирования

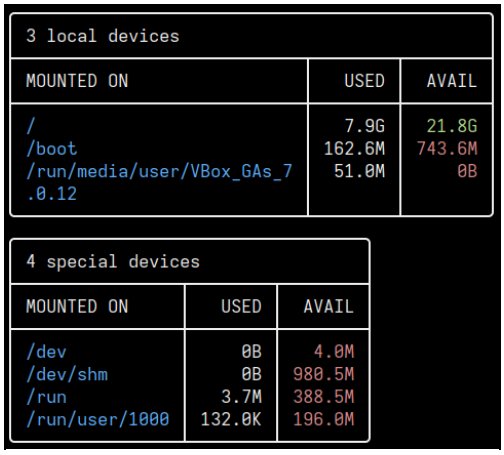
Для вывода определенных столбцов в таблице, можно воспользоваться опцией **-output** с указанием (через запятую) необходимых столбцов.

Например, для вывода столбцов точки монтирования, занятого места и места, которое еще свободно:

```
duf -output mountpoint,used,avail
```

Эта команда выводит информацию только о точках монтирования, объеме использованного и доступного пространства. Это полезно, если нужно кратко оценить текущее использование дискового пространства без дополнительных деталей.

Результат выполнения:



Квоты для директорий в РЕД ОС (ограничение размера каталога)

В данной инструкции будет рассмотрено создание образа файловой системы для хранения нужной нам информации и последующего его подключения в точку монтирования.

Вы можете подробнее ознакомиться с настройкой квот для каталогов, просмотрев наши обучающие видео:

- на **RuTube** — Создание каталогов с ограничением их размера;
- в **Яндекс.Дзен** — Создание каталогов с ограничением их размера;
- в **VK Видео** — Создание каталогов с ограничением их размера.

На наших каналах вы также сможете найти много другой полезной информации.

Создайте каталог для точки монтирования образа:

```
mkdir -p /data/share/dirquota
```

Создайте образ файловой системы с указанием его объема:

```
dd if=/dev/zero of=/data/quota.img bs=1024 count=100000
```

Отформатируйте файловый образ:

```
mkfs.ext4 /data/quota.img
```

Примонтируйте образ в точку монтирования:

```
mount -o loop /data/quota.img /data/share/dirquota
```

Для автоматического монтирования добавьте строку в **fstab**:

```
nano /etc/fstab /data/quota.img/ /data/share/dirquota ext4 loop 1 2
```

Для увеличения или уменьшения объема файловой системы можно использовать **resize2fs**:

```
resize2fs -p quota.img 1000M
```

Для проверки целостности выполните:

```
e2fsck -f quota.img
```

Уменьшение размера диска для установки ОС Windows на один диск с РЕД ОС

Изменение размера логического тома
Работа с Gparted
Восстановление загрузчика GRUB

Допустим, имеется один физический диск размером **50 Гб**, на который установлена система РЕД ОС с разбивкой диска по умолчанию. Т.е. все свободное пространство размечено в **LVM**. Необходимо установить на этот диск *ОС Windows* так, чтобы осталась возможность запускать *РЕД ОС*. Для этого следует под *Windows* выделить свободное дисковое пространство.

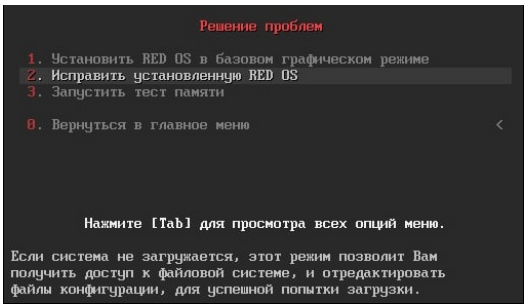
ВАЖНО!

Очень важно, чтобы сначала был уменьшен **размер файловой системы**, затем **тома**. Также важно не уменьшить размер тома больше, чем уменьшен размер файловой системы. В противном случае данные могут быть уничтожены.

Перед выполнением операции **обязательно** необходимо создать **копию** важных **данных**.

Изменение размера логического тома

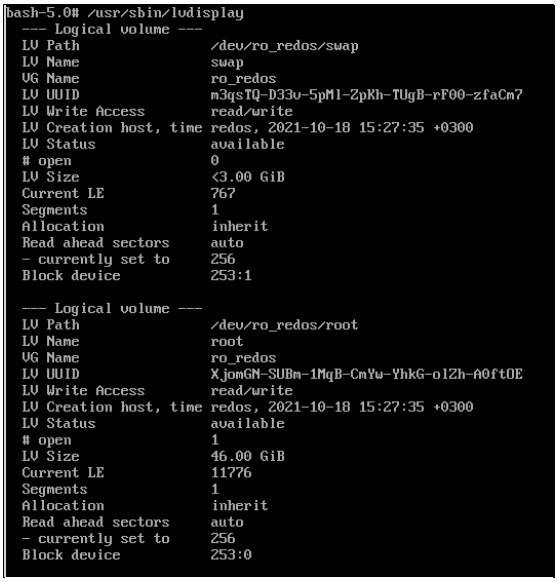
Загрузитесь в режиме восстановления (**Rescue**) с диска установки РЕД ОС. Выберите пункт "**2. Исправить установленную RED OS**".



В этом режиме выберите 3 пункт, для перехода в командную строку. В режиме "**Skip to shell**" дисковые разделы не будет примонтированы, что позволит нам произвести необходимые настройки с логическими томами.



Выполните команду **lvdisplay** для просмотра логических томов.



На рисунке видно, что наибольший размер у **/dev/ro_redos/root**, он имеет размер **46 Гб**, его и следует уменьшать.

Проверьте активность lvm-томов командой **lvscan**:

```
bash-5.0# lvscan
  inactive          '/dev/ro_redos/swap' [<3.00 GiB] inherit
  inactive          '/dev/ro_redos/root' [46.00 GiB] inherit
bash-5.0#
```

Если тома не активны, то активируйте нужный том командой:

```
lvchange -ay /dev/ro_redos/root
```

```
bash-5.0# lvchange -a y /dev/ro_redos/root
bash-5.0# lvscan
  inactive          '/dev/ro_redos/swap' [<3.00 GiB] inherit
  ACTIVE            '/dev/ro_redos/root' [46.00 GiB] inherit
```

Далее следует выполнить проверку LVM-раздела:

```
e2fsck -f /dev/ro_redos/root
```

```
bash-5.0# e2fsck -f /dev/ro_redos/root
e2fsck 1.44.6 (5-Mar-2019)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/ro_redos/root: 196383/3014656 files (0.1% non-contiguous), 1858089/12058624 blocks
```

Уменьшите размер корневого (/) раздела **на файловой системе** до 14 Гб.

14 Гб — это размер, который нужно задать для файловой системы, а не на который уменьшается ФС:

```
resize2fs /dev/ro_redos/root 14G
```

```
bash-5.0# resize2fs /dev/ro_redos/root 14G
resize2fs 1.44.6 (5-Mar-2019)
Resizing the filesystem on /dev/ro_redos/root to 3670016 (4k) blocks.
The filesystem on /dev/ro_redos/root is now 3670016 (4k) blocks long.
```

Уменьшите размер **LVM-тома /dev/ro_redos/root** до размера 14 Гб:

```
lvreduce -L 14G /dev/ro_redos/root
```

```
bash-5.0# lvreduce -L 14G /dev/ro_redos/root
  WARNING: Reducing active logical volume to 14.00 GiB.
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce ro_redos/root? [y/n]: y
  Size of logical volume ro_redos/root changed from 46.00 GiB (11776 extents) to 14.00 GiB (3584 ext
ents).
  Logical volume ro_redos/root successfully resized.
```

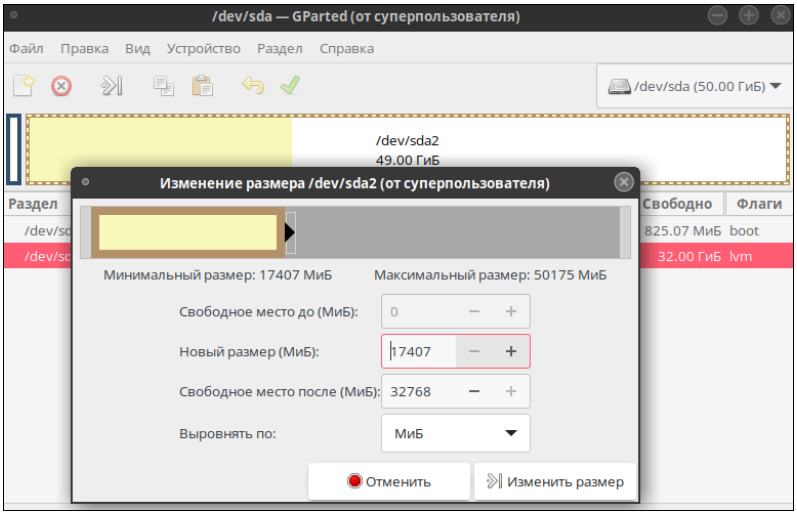
После этого перезагрузите ПК, войдите в систему через графическое окружение.

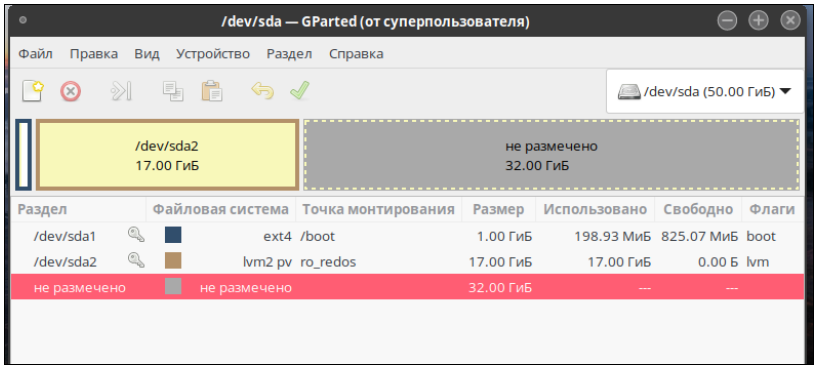
Работа с Gparted

Установите графическую утилиту **Gparted** для последнего шага изменения размера раздела.

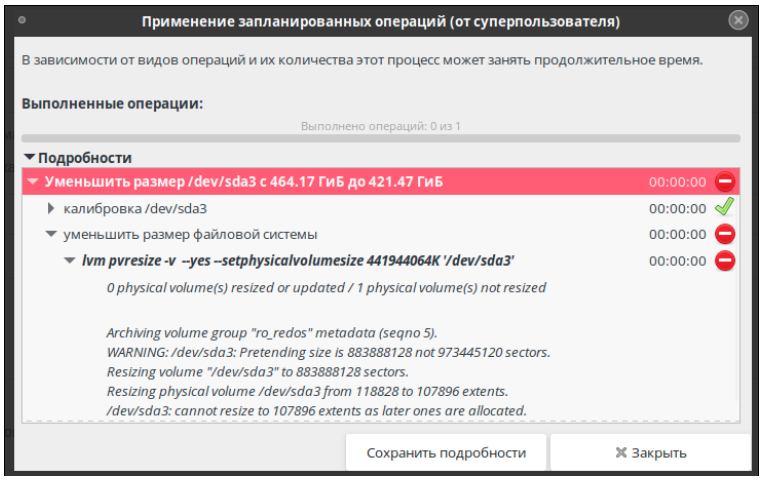
```
dnf install gparted
```

После установки **Gparted** появилась возможность изменить размер раздела, введите необходимые значения.





После уменьшения размера LVM-тома в режиме восстановления с установочного диска РЕД ОС и последующем изменении размера в **Gparted** может возникать ошибка, которая указывает о недостатке свободных экстентов.



Такое происходит из-за того, что свободные экстенты находятся в середине lvm-тома.

Проверить это можно командой:

```
pvs -v --segments /dev/nvme0n1p3
```

где вместо «**/dev/nvme0n1p3**» необходимо указать свой каталог с физическим устройством.

```
[root@localhost admin]# pvs -v --segment /dev/nvme0n1p3
  PV           VG       Fmt  Attr PSize   PFree    Start  SSize LV   Start Type   PE Ranges
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g      0 17920 root     0 linear /dev/nvme0n1p3:0-17919
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g  17920 50816 home     0 linear /dev/nvme0n1p3:17920-68735
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g  68736 50984          0 free
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 119720  1970 swap     0 linear /dev/nvme0n1p3:119720-121689
[root@localhost admin]#
```

Как видно из ответа команды между логическими томами **home** и **swap** есть свободное место. Для успешной разметки в **Gparted** необходимо переместить **swap** в свободное место.

Сначала необходимо убедиться, что раздел **swap** не смонтирован. Для этого нужно выполнить команду:

```
swapoff -a
```

Далее необходимо переместить раздел подкачки. Разделы находятся на одном диске, поэтому следует указать политику распределения **anywhere**. В результате этого логический том перемещается в начало свободного места.

Для этого следует ввести команду:

```
pvmove --alloc anywhere /dev/nvme0n1p3:119720-121689
```

где вместо «**/dev/nvme0n1p3:119720-121689**» указать свои данные логического тома из графы «**PE Rangers**».

```
[root@localhost admin]# pvmove --alloc anywhere /dev/nvme0n1p3:119720-121689
  /dev/nvme0n1p3: Moved: 0,46%
  /dev/nvme0n1p3: Moved: 100,00%
[root@localhost admin]#
```

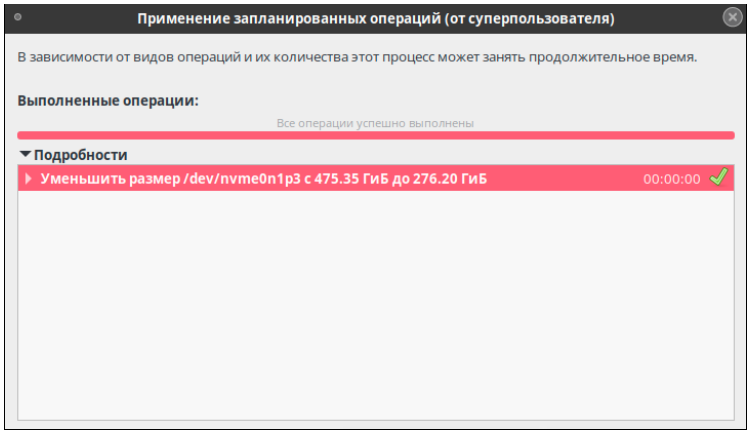
Далее проверяем, что свободные экстенты находятся в конце разделов.

```
pvs -v --segments /dev/nvme0n1p3
```

где вместо «**/dev/nvme0n1p3**» надо указать свой каталог с физическим устройством.

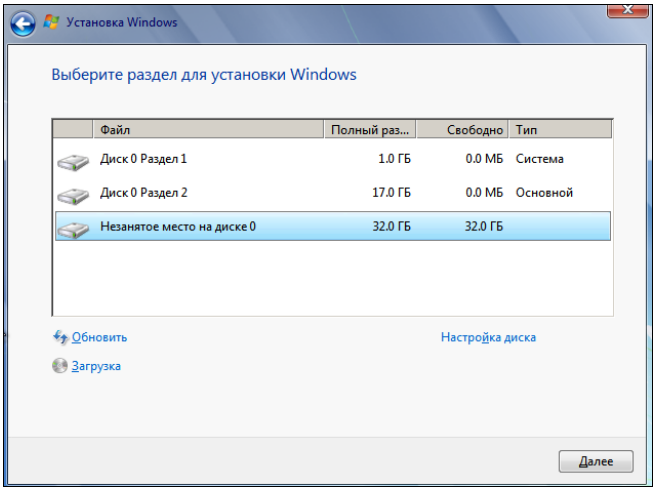
```
[root@localhost admin]# pvs -v --segment /dev/nvme0n1p3
  PV             VG       Fmt  Attr PSize   PFree    Start SSize LV   Start Type   PE Ranges
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g     0 17920 root     0 linear /dev/nvme0n1p3:0-17919
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 17920 50816 home     0 linear /dev/nvme0n1p3:17920-68735
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 68736  1970 swap     0 linear /dev/nvme0n1p3:68736-70705
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 70706 50984          0 free
[root@localhost admin]#
```

После этого в **Gparted** появляется возможность изменить размер раздела.



Восстановление загрузчика GRUB

На неразмеченное пространство теперь можно установить операционную систему *Windows*.



После того как *Windows* будет установлена, она заменит загрузчик *GRUB* своим загрузчиком, и в результате пропадет возможность запустить РЕД ОС.

Чтобы исправить данную ситуацию, необходимо по нашей инструкции выполнить восстановление загрузчика **GRUB**.

BleachBit - утилита для выполнения очистки диска

Установка
Настройка BleachBit
Работа с BleachBit
Удаление файлов с многократной перезаписью
Работа с утилитой в терминальном режиме

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** bleachbit-4.4.0-1

BleachBit – это утилита для выполнения очистки диска, выгрузки файлов, которые могут пригодиться, в облако, а также удаления файлов без возможности их восстановления.

К основным возможностям **BleachBit** относятся:

- удаление временных файлов для большинства известных приложений;
- очистка оперативной памяти, виртуальной памяти, раздела подкачки;
- многократная перезапись удалённых файлов для исключения возможности их восстановления;
- удаление неиспользуемых и ошибочных (ссылающихся на несуществующие программы) ярлыков;
- возможность использования консольного интерфейса, позволяющего автоматизировать процесс;
- очистка кеша систем управления пакетами;
- наличие собственного языка разметки **CleanerML**, который можно использовать для написания скриптов очистки накопителя;
- возможность удаления неиспользуемых языков интерфейса;
- удаление cookies, кеша и паролей всех распространённых браузеров и перечня скачанных файлов;
- оптимизация баз данных большого перечня программ, от **aMule** и **Beagle** до **Miro** и **Pidgin**.

Вы можете подробнее ознакомиться с работой утилиты BleachBit, просмотрев наши обучающие видео:

- на **RuTube** — Полное и необратимое удаление данных с дисков;
- в **Яндекс.Дзен** — Полное и необратимое удаление данных с дисков;
- в **VK Видео** — Полное и необратимое удаление данных с дисков.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **bleachbit** необходимо перейти в сеанс пользователя **root**:

```
su -
```

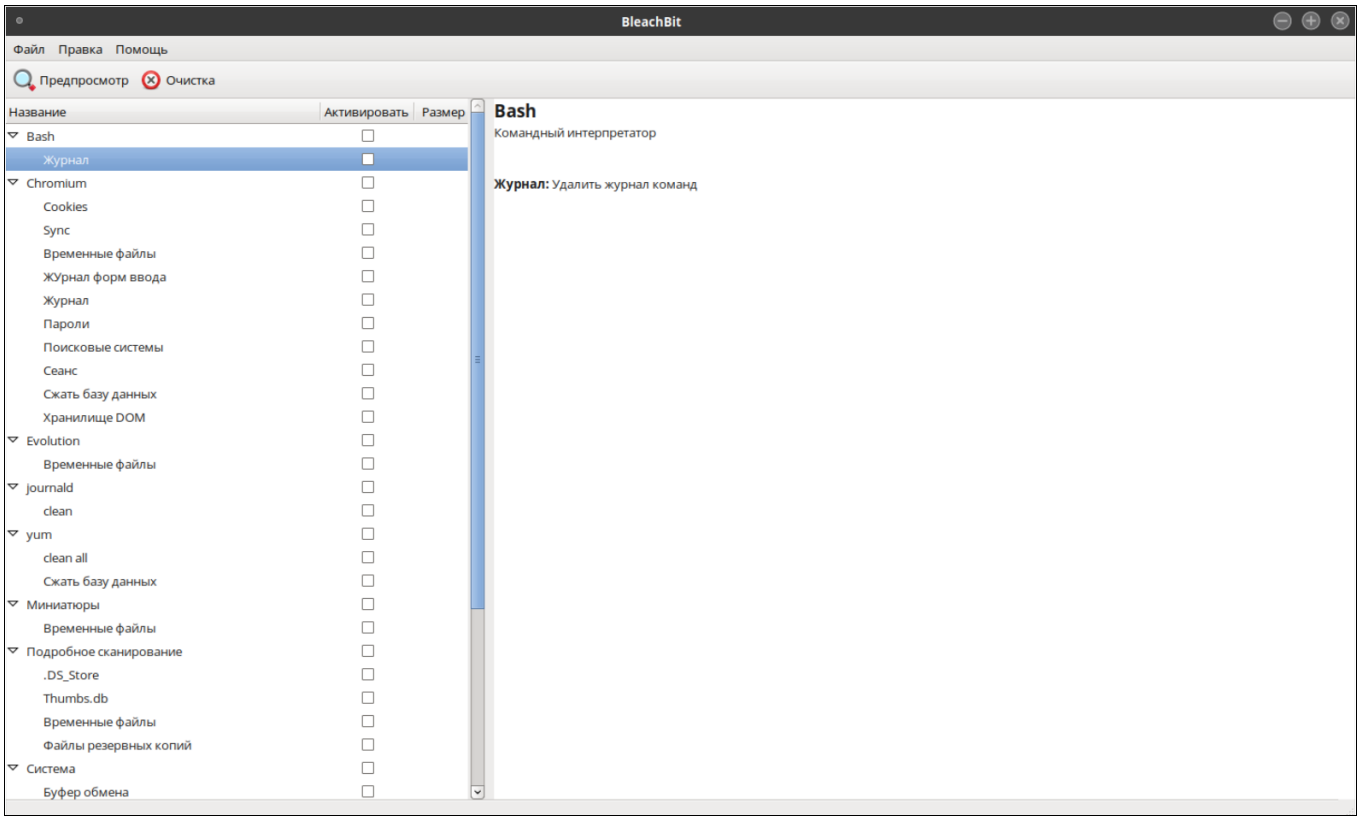
и выполнить следующую команду:

```
dnf install bleachbit
```

Запустить утилиту можно как через «**Главное меню**» - «**Системные**» - «**BleachBit**», так и через терминал командой:

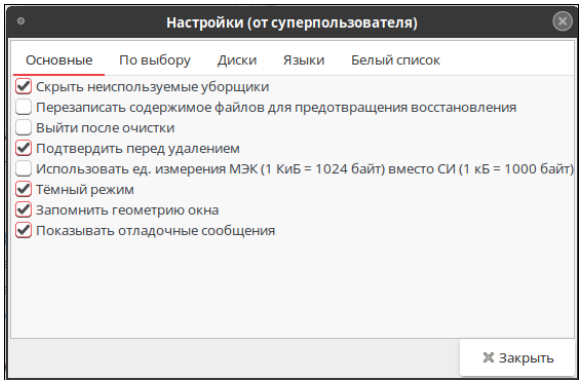
```
bleachbit
```

Структурно интерфейс программы выглядит одинаково для всех версий ОС: слева располагается раздел со списком элементов, которые можно очистить/удалить, справа – раздел, с описанием выполняемых действий.



Настройка BleachBit

При первом запуске программы будет выведено окно с настройками, которое можно открыть через меню «**Правка**» - «**Настройки**».



Окно настроек состоит из пяти вкладок:

Во вкладке «**Общие**» можно настроить:

1. Включение/Отключение автоматической проверки наличия обновлений через Интернет (Рекомендуется отключить);
2. Скрыть/Отобразить неиспользуемые параметры;
3. Перезаписать содержимое файлов для предотвращения восстановления;
4. Запускать или нет программу вместе с компьютером;
5. Выйти после очистки;
6. Подтвердить перед удалением;
7. Использовать единицы измерения МЭК вместо СИ;

Во вкладке «**По выбору**» существует возможность выполнить тонкую настройку каталогов и файлов, которые нужно сканировать на предмет удаления.

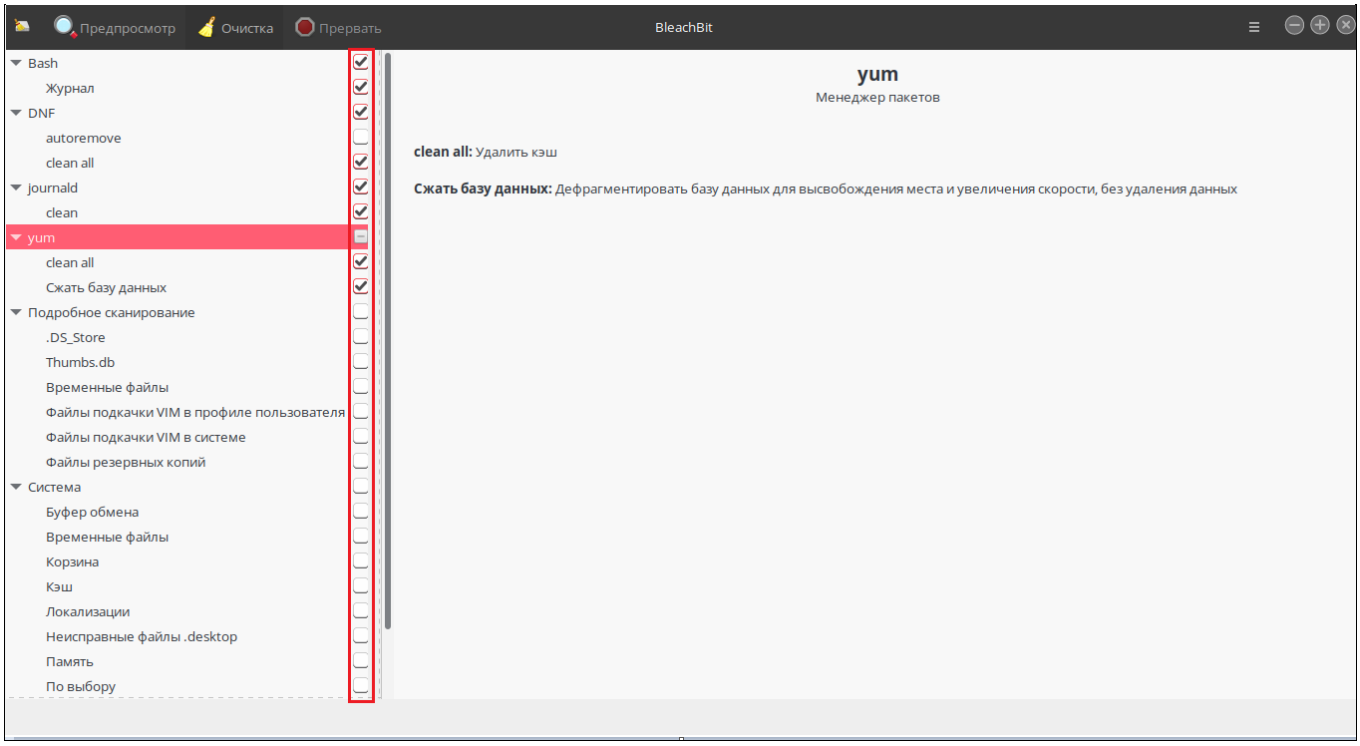
Вкладка «**Диски**» предназначена для настройки режима перезаписи освобождённого дискового пространства, чтобы удалённые файлы и даже их фрагменты нельзя было восстановить.

На вкладке «**Языки**» отображается полный список установленных в системе языков. Можно выбрать те, которые не будут использоваться и которые необходимо удалить.

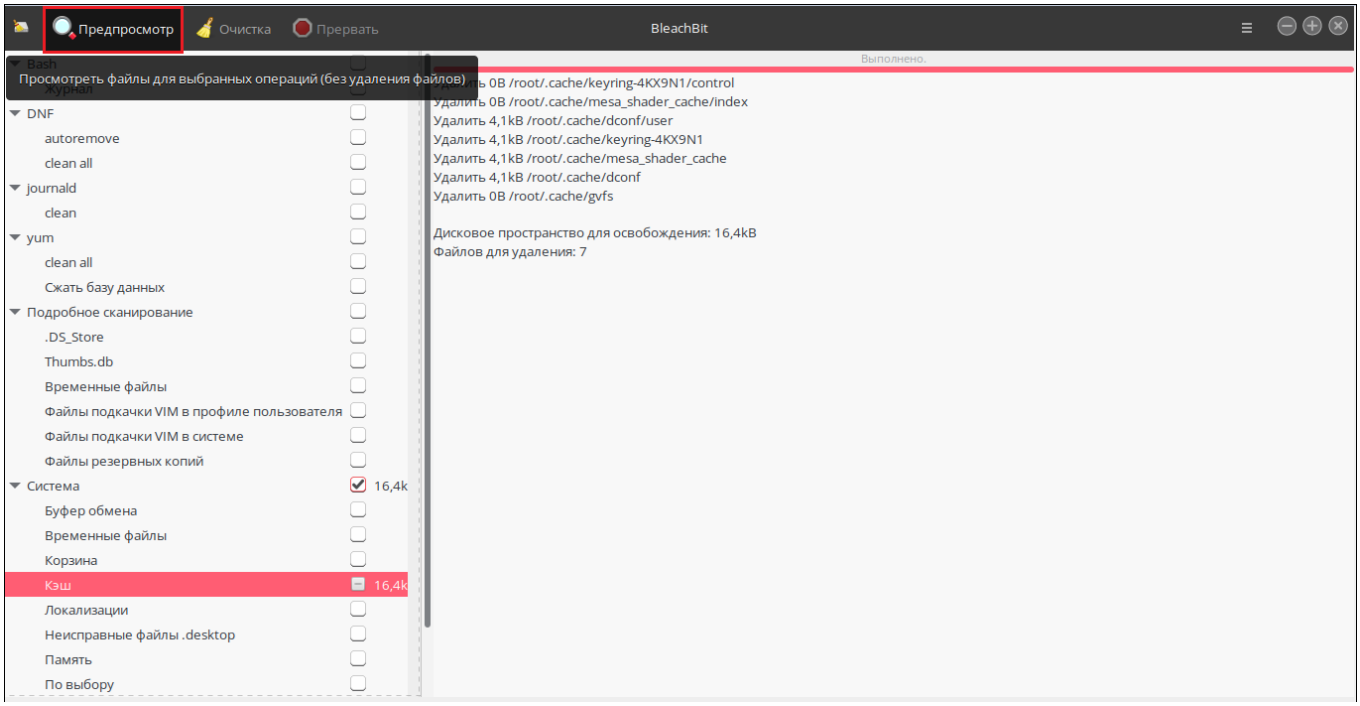
Во вкладке «**Белый список**» указываются каталоги диска, которые утилита будет игнорировать.

Работа с BleachBit

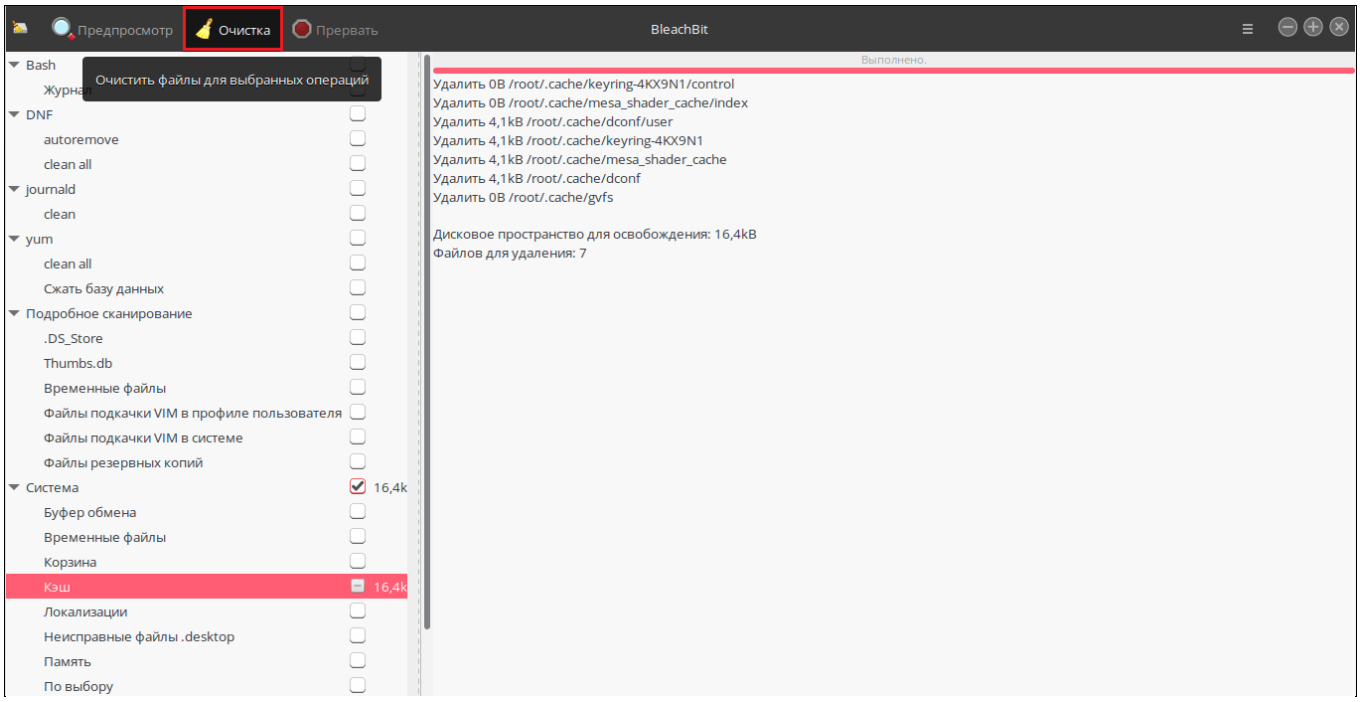
Для освобождения места на диске предназначена левая панель утилиты, где перечислены все категории, скрипты и файлы, обнаруженные во время сканирования диска. Этот перечень зависит не столько от конкретных установленных программ, сколько от вида дистрибутива Linux. Вы можете исключать из списка как целые категории, так и отдельные типы файлов.

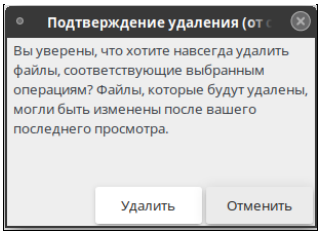


По умолчанию некоторые элементы списка будут помечены флагами, некоторые – нет. Выделите необходимые пункты и нажмите кнопку «**Предпросмотр**» в верхнем меню, чтобы просмотреть все файлы, которые будут очищены, и какой объём дискового пространства будет освобождён.



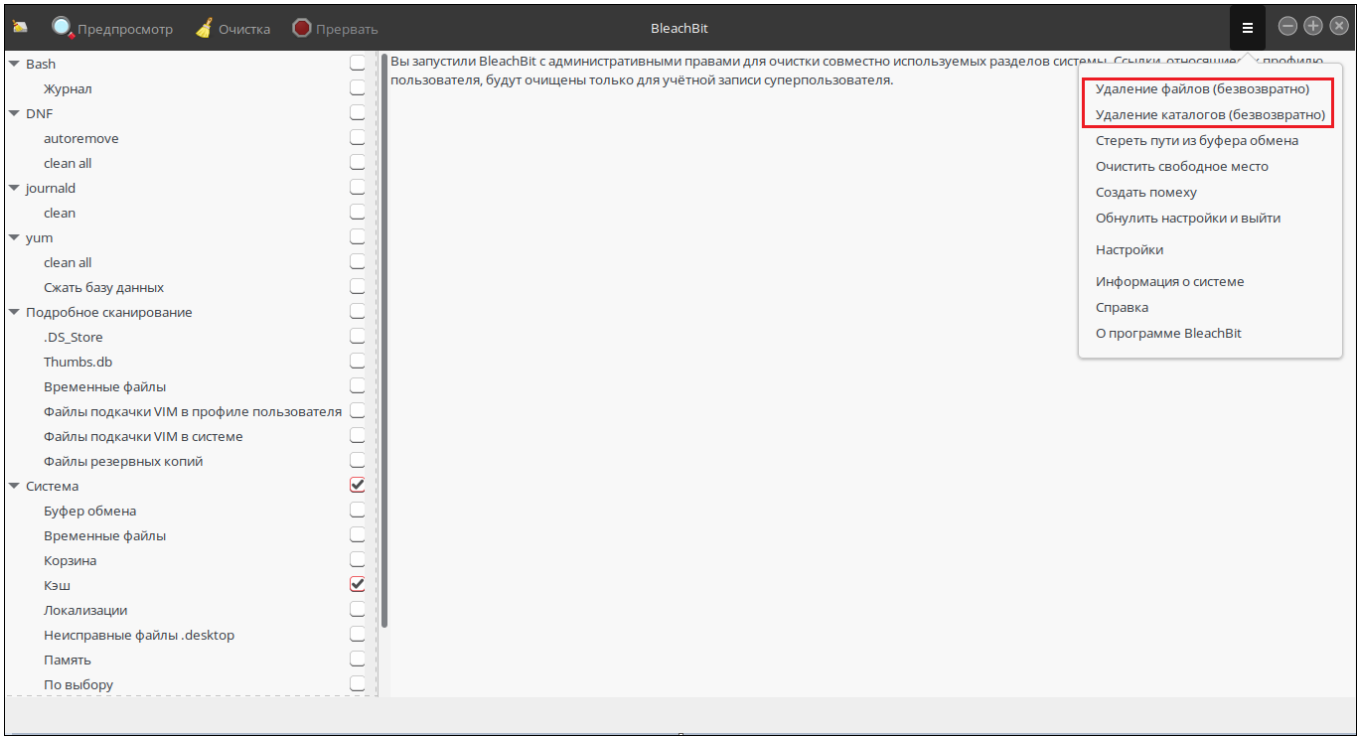
Для запуска работы утилиты требуется нажать на кнопку «**Очистка**» и подтвердить свой выбор.





Удаление файлов с многократной перезаписью

Для удаления файлов в меню **BleachBit** есть соответствующие пункты. При их выборе откроется проводник для выбора файла/каталога для удаления. При использовании такого способа восстановить их уже не получится.



Работа с утилитой в терминальном режиме

В **BleachBit** реализована работа в терминальном режиме и возможностью добавления команды в **crontab**.

Просмотреть доступные ключи можно с помощью команды:

```
bleachbit -h
```

Просмотреть доступные скрипты очистки можно командой:

```
bleachbit -l
```

Аналогом оценки количества освобождаемого места служит команда:

```
bleachbit --preview --preset
```

Ключ **--preset** устанавливает выбранные в графическом интерфейсе наборы опций. Вместо него можно поставить один из сценариев, полученных с помощью ключа **-l**.

Для запуска очистки используется ключ **--clean**:

```
bleachbit --clean --preset
```

Для удаления файлов с многократной перезаписью без возможности восстановления следует использовать ключ **--overwrite**.

DisLocker - инструмент для чтения зашифрованных разделов

Установка
Использование dislocker в режиме FILE
Использование dislocker в режиме FUSE
Проверка работоспособности dislocker

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dislocker-0.7.3-1

DisLocker – инструмент для чтения разделов, зашифрованных в *BitLocker*. Dislocker используется для чтения томов, зашифрованных в системных версиях Windows от Vista до 10, и зашифрованных разделов *BitLocker-To-Go*.

BitLocker-To-Go предназначен для работы со съемными носителями.

BitLocker — технология, которая используется для шифрования разделов диска в операционной системе Windows.

При расшифровке раздела требуется указать каталог, куда будет сохранен **dislocker-file**. Этот файл является виртуальным разделом NTFS, поэтому его можно смонтировать как любой раздел, а затем читать или записывать в него файлы. Запись в виртуальный файл NTFS приведет к изменению содержимого базового раздела BitLocker.

Установка

Для установки *dislocker* перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install dislocker
```

После установки *dislocker* для работы с зашифрованными разделами доступны следующие утилиты:

- **dislocker-bek** – для анализа файла .bek и печати информации о нем;
- **dislocker-metadata** – для печати информации о томе, зашифрованном BitLocker;
- **dislocker-find** – скрипт на Ruby, который находит зашифрованный раздел BitLocker среди подключенных дисков;
- **dislocker-file** – для расшифровки раздела BitLocker в файл, отформатированный как раздел NTFS, который можно смонтировать;
- **dislocker-fuse** – параметр, который используется при вызове команды *dislocker*, он динамически расшифровывает раздел BitLocker с помощью FUSE.

Dislocker поддерживает работу в двух режимах:

- FILE;
- FUSE.

Использование dislocker в режиме FILE

В режиме **FILE** весь раздел *BitLocker* расшифровывается в файл. Этот процесс может занять значительное время, зависящее от размера раздела.

Для *расшифровывания* раздела необходимо выполнить команду вида:

```
dislocker -V /dev/sda3 -u -- /media/<имя_файла>
```

где:

- /dev/sda3 — зашифрованный раздел Bitlocker;
- /media — директория, в которую будет записан файл;

- <имя_файла> — произвольное имя расшифрованного файла.

Далее будет запрошен пароль, с помощью которого был зашифрован раздел. Необходимо его ввести и нажать **Enter**.

Для *монтирования* расшифрованного раздела необходимо создать отдельную директорию:

```
mkdir /media/<директория>
```

И выполнить команду монтирования:

```
mount -o loop /media/<имя_файла> /media/<директория>
```

где:

- /media/<имя_файла> — путь к расшифрованному файлу;
- /media/<директория> — директория монтирования.

Использование dislocker в режиме FUSE

Второй режим предполагает использование **FUSE** — драйвера файловой системы, который позволяет пользователям без особых привилегий создавать их собственные файловые системы. В режиме **FUSE** расшифровывание происходит «на лету». Расшифровывается только тот блок, к которому в данный момент обращается система.

Для использования *dislocker* в режиме **FUSE** необходимо установить дополнительный пакет **fuse-dislocker** командой (с правами пользователя root):

```
dnf install fuse-dislocker
```

Для *расшифровывания* необходимо создать отдельную директорию:

```
mkdir /media/dislocker
```

Для запуска процесса *расшифровывания* раздела используется команда:

```
dislocker -V /dev/sda3 -u -- /media/dislocker
```

где:

- /dev/sda3 — зашифрованный раздел Bitlocker;
- /media/dislocker — директория для расшифровывания раздела. Указывать **имя файла**, как в режиме FILE, **не нужно**!

Далее будет запрошен пароль, с помощью которого был зашифрован раздел. Необходимо его ввести и нажать **Enter**.

Для *монтирования* расшифрованного раздела необходимо создать отдельную директорию:

```
mkdir /media/mount
```

И выполнить команду монтирования:

```
mount -o loop /media/dislocker/dislocker-file /media/mount
```

где:

- /media/dislocker/dislocker-file — файл, который был расшифрован;
- /media/mount — директория монтирования.

Проверка работоспособности dislocker

Проверим работоспособность *dislocker* на примере предоставления доступа к зашифрованным Bitlocker-разделам Windows 7.

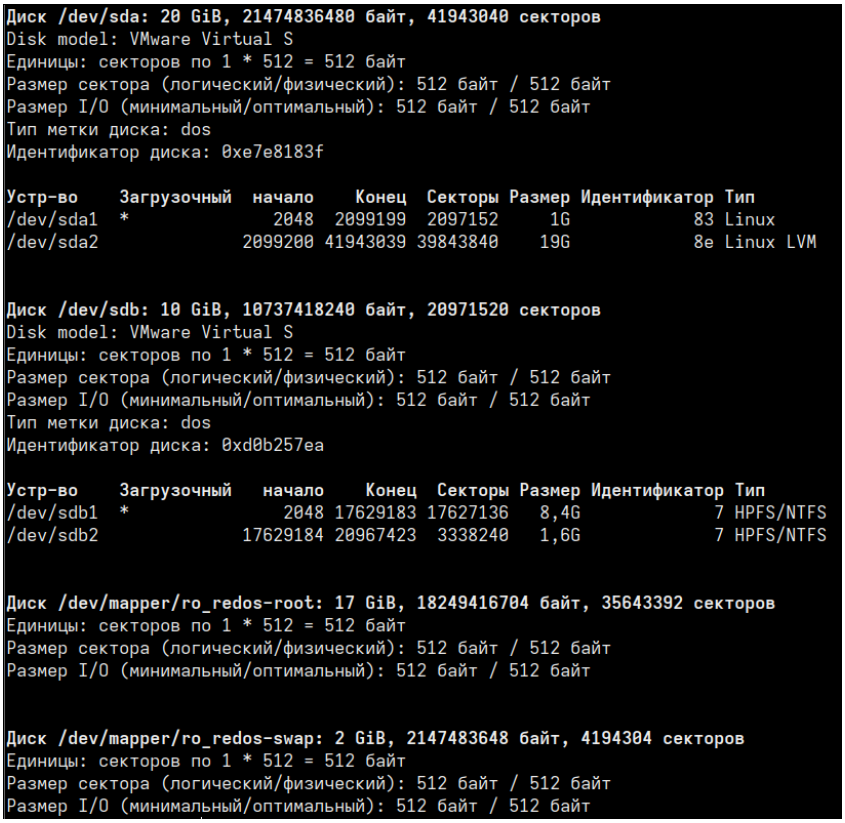
Создайте две директории, прежде чем начать расшифровку.

Первая директория (*/media/bitlocker*) – для вашего «зашифрованного раздела», который представляет собой «файл» виртуального раздела NTFS, созданный программой *dislocker* до того, как вы смонтируете его для доступа.

Вторая директория (*/media/mount*) – для монтирования расшифрованного раздела.

```
mkdir -p /media/bitlocker
mkdir -p /media/mount
```

Находим зашифрованный раздел с помощью `fdisk -l`. Определить его можно, например, по размеру:



```
Диск /dev/sda: 20 GiB, 21474836480 байт, 41943040 секторов
Disk model: VMware Virtual S
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xe7e8183f

Устр-во    Загрузочный  начало    Конец  Секторы Размер Идентификатор Тип
/dev/sda1  *              2048  2099199  2097152     1G            83 Linux
/dev/sda2              2099200 41943039 39843840    19G            8e Linux LVM


Диск /dev/sdb: 10 GiB, 10737418240 байт, 20971520 секторов
Disk model: VMware Virtual S
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xd0b257ea

Устр-во    Загрузочный   начало    Конец  Секторы Размер Идентификатор Тип
/dev/sdb1  *               2048 17629183 17627136   8,4G             7 HPFS/NTFS
/dev/sdb2             17629184 20967423  3338240   1,6G             7 HPFS/NTFS


Диск /dev/mapper/ro_redos-root: 17 GiB, 18249416704 байт, 35643392 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт


Диск /dev/mapper/ro_redos-swap: 2 GiB, 2147483648 байт, 4194304 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
```

В данном примере зашифрован раздел **/dev/sdb2**.

После этого запускаем расшифровку раздела на запись и чтение:

```
dislocker -V /dev/sdb2 -u <пароль> -- /media/bitlocker
```

где:

- /dev/sdb2 — имя вашего зашифрованного раздела;
- <пароль> — пароль BitLocker, который был использован для шифрования диска.

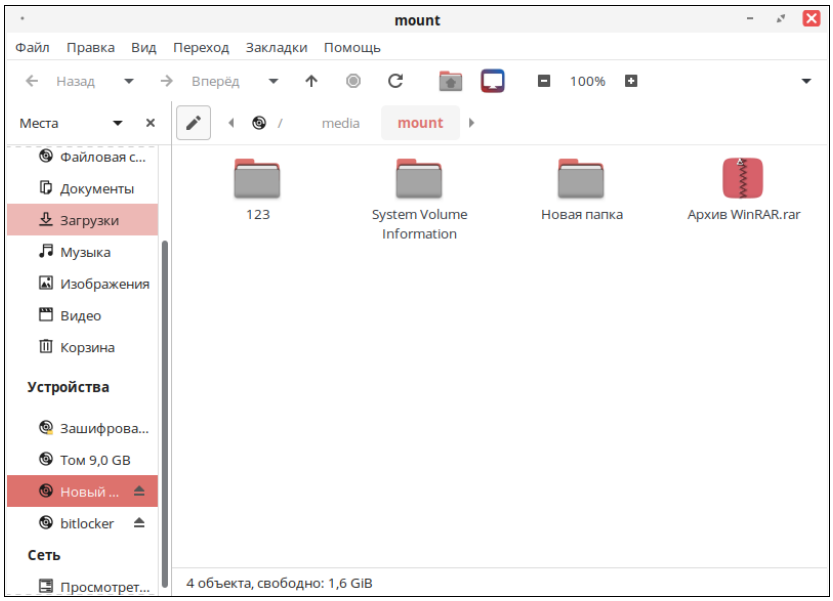
Если том необходимо расшифровать только для чтения, используйте ключ **-r**:

```
dislocker -r -V /dev/sdb2 -u <пароль> -- /media/bitlocker
```

Далее необходимо примонтировать раздел, чтобы можно было получить доступ к файлам. Для этого используется следующая команда:

```
mount -o loop /media/bitlocker/dislocker-file /media/mount
```

Сразу после монтирования будет открыт файловый менеджер с содержимым расшифрованного раздела.



Все изменения будут сохранены после отключения зашифрованного диска.

TRIM

Проверка поддержки TRIM
Включение TRIM с помощью флагов монтирования
Применение TRIM по раписанию cron
Включение TRIM с помощью tune2fs
Настройка TRIM по расписанию с помощью таймера systemd

Когда в операционной системе происходит операция удаления данных с SSD-диска, то физически они не удаляются, а лишь помечаются как «неиспользуемые» в файловой системе. Операция записи новых данных на место «неиспользуемых» предварительно сопровождается уже реальной функцией стирания ранее «удаленных» данных, что приводит к снижению производительности диска.

Чтобы решить эту проблему используется **TRIM** — команда интерфейса ATA, которая сообщает твердотельному диску, какие «неиспользуемые» блоки данных можно физически удалить с твердотельного устройства (**SSD**).

Целью очистки памяти является периодическая оптимизация накопителя, чтобы он работал эффективно и сохранял производительность на протяжении всего срока службы. Часто эта операция может выполняться в фоновом режиме или в ручном.

Примечание.

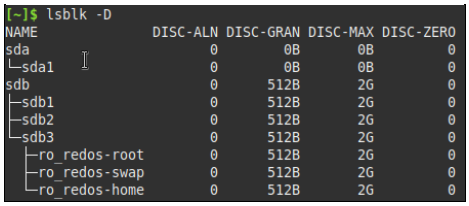
На твердотельном накопителе с **включенным TRIM**, если вы удалите файл и впоследствии очистите корзину, восстановить удаленные данные уже будет невозможно. В отличие от механических жестких дисков, которые удерживают данные магнитным полем, все, что требуется NAND для полного удаления данных — это команда (**trim**).

Проверка поддержки TRIM

Проверить поддержку **TRIM** можно двумя способами.

Способ №1 — с помощью команды **lsblk**:

```
lsblk -D
```



Если значения столбцов **DISC-GRAN** (отбросить гранулярность) и **DISC-MAX** (отбросить максимальное количество байтов) имеют ненулевые значения, это указывает на поддержку **TRIM**.

Способ №2 — с помощью команды **hdparm**:

```
hdparm -I /dev/sda | grep TRIM

* Data Set Management TRIM supported (limit 1 block)
```

Если в выводе присутствует запись TRIM supported, значит диск поддерживает **TRIM**.

Включение операции TRIM в РЕД ОС

Включение TRIM с помощью флагов монтирования

В данном случае операция **TRIM** будет выполняться каждый раз при монтировании раздела диска. Параметр discard в **/etc/fstab** в строке монтирования раздела активирует **TRIM**:

```
/dev/sda1 / ext4 defaults,noatime,discard 0 1
/dev/sda2 /home ext4 defaults,noatime,discard 0 2
```

Примечание.

- не используйте флаг **discard**, если вы периодически выполняете команду **fstrim**;
- если вы используете флаг **discard** для корневого раздела с файловой системой **ext3**, раздел будет смонтирован в режиме только-чтение (**read_only**).

ВАЖНО!

Перед внесением изменений убедитесь, что ваш SSD поддерживает TRIM, иначе вы можете **потерять данные**!

Применение TRIM по расписанию cron

Данный метод не работает для файловых систем VFAT.

Для использования **fstrim** раздел диска должен быть смонтирован и указан точкой монтирования. Для периодического выполнения команды можно задействовать планировщик заданий **cron**, в котором в качестве задания используется команда:

```
fstrim -v /
```

Данная команда будет применена к корневому разделу. Для указания, например, домашнего раздела используйте команду:

```
fstrim -v /home
```

Подробную информацию по работе с планировщиком **cron** см. в нашей статье «Crontab».

После настройки планировщика заданий уберите опцию `discard` из **/etc/fstab**, если ранее вы ее добавляли.

Приоритетным способом является использование `discard`. Если с ним возникли проблемы или он не подошел, используйте **fstrim**.

Включение TRIM с помощью tune2fs

В файловой системе **EXT4** флаг `discard` можно установить с помощью утилиты **tune2fs**. При данном способе флаг `discard` устанавливается в суперблоке ФС, как опция монтирования по умолчанию.

```
tune2fs -o discard /dev/sdXY
```

Если на диске используется LVM, то команда для корневого раздела может выглядеть примерно следующим образом:

```
tune2fs -o discard /dev/mapper/ro_redos-root
```

Чтобы определить, какой именно раздел применять в команде **tune2fs**, воспользуйтесь командами «**lsblk**», «**df**» или **blkid**, которые выведут на экран имена разделов диска.

Убедится в активации **trim** можно также с помощью **tune2fs**, при этом команде передается ключ **-l**:

```
tune2fs -l /dev/mapper/vg1-lvroot | grep options

Default mount options:    user_xattr acl discard
```

Использование параметров монтирования по умолчанию вместо редактирования в **/etc/fstab** актуально для внешних дисков, поскольку для разделов диска признак применения TRIM будет установлен по умолчанию и не придется на каждом компьютере редактировать **/etc/fstab** для добавления опции `discard`.

Примечание.

При использовании данного способа опция discard **НЕ будет** показана командой **mount**.

Настройка TRIM по расписанию с помощью таймера systemd

В РЕД ОС присутствует *systemd*-таймер, который предназначен для использования TRIM по расписанию. Активировать таймер можно командой:

```
systemctl enable --now fstrim.timer
```

По умолчанию задание **fstrim** будет выполняться еженедельно, это задание запускает связанную службу **fstrim** по расписанию. Время выполнения **fstrim** по умолчанию настроено на каждый понедельник с точностью запуска в 1 час, т.е. с 00:00 по 01:00.

Для установки собственного времени выполнения задания измените время в таймере **/usr/lib/systemd/system/fstrim.timer**, за это отвечает опция **OnCalendar**.

Пример изменения таймера на каждый понедельник в 12:00.

```
nano /usr/lib/systemd/system/fstrim.timer
```

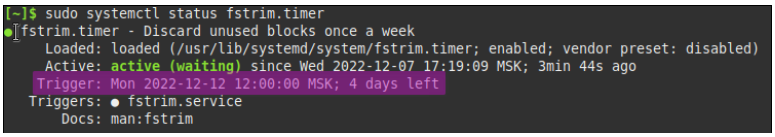
```
[Unit]
Description=Discard unused blocks once a week
Documentation=man:fstrim
ConditionVirtualization=!container
ConditionPathExists=!/etc/initrd-release

[Timer]
OnCalendar=Mon *-*-* 12:00:00
Persistent=true

[Install]
WantedBy=timers.target
```

Перезапустите таймер для применения внесенных изменений:

```
systemctl daemon-reload
systemctl restart fstrim.timer
```

В статусе таймера в поле **Trigger** будет указано запланированное время выполнения задания:

```
systemctl status fstrim.timer
```



Планировщик ввода/вывода

Планировщик ввода-вывода (I/O) — это компонент ядра, который определяет, в каком порядке операции блочного ввода-вывода передаются на устройства хранения (HDD/SSD/NVME). Основной целью планировщика ввода-вывода является оптимизация обработки запросов к диску для повышения производительности и пропускной способности ввода-вывода. Связано это с тем, что когда в системе запущено большое количество процессов, выполняющих запросы ввода-вывода к различным частям хранилища, то эти процессы могут создавать множественные операции ввода-вывода, в результате чего образуется очередь запросов.

В РЕД ОС используются следующие планировщики:

- **mq-deadline** — реализация планировщика deadline с использованием blk-mq. Этот планировщик подходит для большинства случаев, но особенно для тех, в которых операции записи в основном асинхронны. Планировщик mq-deadline сортирует запросы ввода-вывода в очереди на чтение или запись, а затем планирует их выполнение в возрастающем порядке адресации логических блоков (LBA).
- **kyber** — планировщик, основанный на методах активного управления очередями, используемых для сетевой маршрутизации. Реализация основана на "токенах", которые служат механизмом ограничения запросов. Используется две очереди запросов — на запись и на чтение. kyber отдает приоритет запросам на чтение перед запросами на запись. Реализация алгоритма относительно проста и считается эффективной для NVME, SSD или других устройств с низкой задержкой.
- **bfq** (Budget Fair Queuing) — основан на алгоритме от CFQ, но содержит улучшения. В конфигурации по умолчанию он больше нацелен на обеспечение минимальной задержки, а не на достижение максимальной пропускной способности. Этот планировщик обладает относительно высокими расходами на операцию, поэтому он не идеален для устройств с медленными процессорами или устройствами ввода-вывода с высокой пропускной способностью.
- **none** – планировщик ввода-вывода без операций с несколькими очередями. Не переупорядочивает запросы и имеет минимальные расходы. Идеально подходит для быстрых устройств произвольного ввода-вывода, таких как SSD или NVME.

Устаревшими планировщиками ввода-вывода считаются: **noop**, **CFQ**, **Deedline**.

В зависимости от задачи, которую выполняет используемая система, рассмотрены следующие рекомендации по выбору планировщиков.

Вариант использования	Планировщик дисков
Традиционный жесткий диск с интерфейсом SCSI	Рекомендуется **mq-deadline** или **bfq**
Высокопроизводительный SSD или система с привязкой к ЦП с быстрым хранилищем	Рекомендуется **none**, особенно при запуске корпоративных приложений. В качестве альтернативы можно использовать **kyber**
Настольные системы или интерактивные задачи	Рекомендуется **bfq**
Виртуальные гостевые системы	Рекомендуется **mq-deadline**. С адаптером главной шины (HBA), поддерживающим работу с несколькими очередями, рекомендуется использовать **noop**/**none**

РЕД ОС по умолчанию использует планировщик **BFQ**. Для проверки можно вывести содержимое файла **/sys/block/sdX/queue/scheduler**:

```
cat /sys/block/sdX/queue/scheduler

mq-deadline kyber [bfq] none
```

Используемый планировщик выделен квадратными скобками.

Изменение планировщика ввода-вывода

Изменить используемый планировщик без необходимости перезагрузки можно командой:

```
echo none > /sys/block/sdX/queue/scheduler
```

где **X** — буква физического накопителя.

Данная настройка действует только **до** первой **перезагрузки** ОС.

Для постоянной настройки необходимо создать правило UDEV.

Создайте файл **/etc/udev/rules.d/60-schedulerset.rules** и запишите в него следующие строки:

- для SSD-дисков:

```
ACTION=="add|change", KERNEL=="sd[a-z]", ATTR{queue/rotational}=="0", ATTR{queue/scheduler}="none"
```

- для NMVE-дисков:

```
ACTION=="add|change", KERNEL=="nvme[0-9]n[0-9]", ATTR{queue/rotational}=="0", ATTR{queue/scheduler}="none"
```

Здесь:

- **ATTR{queue/scheduler}** – параметр определяет имя планировщика;
- **ATTR{queue/rotational}=0** – признак планировщика для типов дисков — **SSD** и **NVME**;
- **ATTR{queue/rotational}=1** – признак планировщика для типа дисков — **HDD** (магнитные диски).

Изменения вступят в силу после перезагрузки ОС. Чтобы проверить назначенное правило, выполните команду:

```
cat /sys/block/sdX/queue/scheduler
```

где **X** — буква физического накопителя.

Например:

```
cat /sys/block/sdb/queue/scheduler

[none] mq-deadline kyber bfq
```

Уменьшение числа операций чтения/записи

Опция монтирования barrier=0
Опция монтирования noatime
Перенос /tmp в tmpfs
Отключение swap

Опция монтирования barrier=0

ВАЖНО!

Не рекомендуется отключать барьеры для дисков, которые будут использоваться без источника бесперебойного питания, так как это может привести к повреждению файловой системы и потере данных.

Файловая система **ext4**, которая используется по умолчанию в РЕД ОС, является журналируемой ФС, в такой файловой системе включены барьеры записи.

Включенные барьеры гарантируют, что метаданные файловой системы будут правильно записаны и упорядочены на диске. При этом данная функция сказывается на производительности, особенно для приложений, которые интенсивно используют **fsync** или создают и удаляют большое количество небольших файлов. Для дисков с питанием от батареи отключение барьеров может безопасно повысить скорость операции записи на разделы **ext4**.

Пример отключения барьеров записи через опцию **barrier=0** в строке монтирования **/etc/fstab**:

```
/dev/mapper/ro_redos-root / ext4 defaults,noatime,discard,barrier=0 0 1
```

Опция монтирования noatime

ВАЖНО!

Это может привести к снижению уровня безопасности системы!

Операционная система отслеживает и обновляет информацию о временнЫх отметках доступа к файлам и каталогам, из-за этого происходит незначительное снижение производительности ввода-вывода. Опция **noatime** в строке монтирования (**/etc/fstab**) раздела диска отключит запись о времени последнего доступа к файлу.

Пример монтирования разделов диска с опцией noatime в фале **/etc/fstab**:

```
/dev/mapper/ro_redos-root / ext4 defaults,noatime,discard 0 1
```

Изменения вступят в силу после перезагрузки ПК.

Перенос /tmp в tmpfs

Каталог **/tmp** используется ОС, а также прикладными программами для хранения временных данных. Чтобы сократить число операций записи и чтения на диск в каталог **/tmp**, существует способ размещения **/tmp** в оперативной памяти. Для этой цели применяется временная файловая система под названием **tmpfs**. Чтобы разместить **/tmp** в **tmpfs**, необходимо открыть файл **/etc/fstab** и добавить в него следующую запись:

```
tmpfs /tmp tmpfs defaults,rw,nodev,nofail,noatime,nosuid,size=4G 0 0
```

где **size** – максимально доступный размер оперативной памяти, которая выделяется только по факту заполнения **/tmp**. Обычно значение параметра **size** определяют как половину от всей оперативной памяти. Т.е. для оперативной памяти размером 8G указывается значение 4G.

Изменения вступят в силу после перезагрузки ПК.

Отключение swap

Многие пользователи отключают **swap** при наличии достаточно большого объема ОЗУ (не менее 8 ГБ) или переносят его на отдельный диск с целью продлить срок службы SSD-диска. Ведь, как известно, когда заканчивается оперативная память, операционная система использует пространство подкачки для записи и чтения данных, а это приводит к дополнительным циклам перезаписи, которые изнашивают ячейки памяти SSD.

Здесь стоит заметить, что отключение **swap** может негативно сказаться на работе системы, если свободная оперативная память все-таки закончится. Поскольку при нехватке памяти **OOM Killer** (защитный механизм ядра Linux) принудительно «убивает» наиболее подходящие по приоритету процессы.

Кроме того, если планируется использовать "спящий режим", для его работы требуется наличие **swap**. В то же время сам процесс перехода в спящий режим приводит к большему износу SSD, чем просто загрузка ОС.

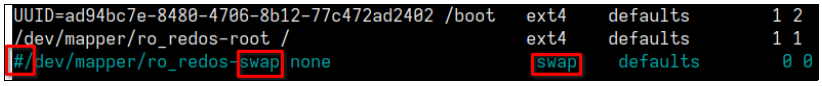
Также стоит отметить, что современные SSD-диски имеют намного большие циклы перезаписи данных, чем диски, выпущенные несколько лет назад (в ранние периоды их массового распространения), и эффект от отключения swap может быть совсем незначительным.

Если swap все же будет решено отключить, сделать это можно следующим образом:

1. Откройте файл **/etc/fstab**.

2. Найдите строку, которая подключает **swap**, и закомментируйте ее, поставив в начале строки символ **#**.

Пример:



3. Сохраните внесенные изменения в файле.

Для применения изменений выполните перезагрузку компьютера.

Работа с bluetooth

Установка
Утилита blueman
Настройка автоматического подключения bluetooth-устройств при загрузке
Поддержка bluetooth-кодеков высокого качества в PulseAudio
Настройка интернет-соединения через bluetooth

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: blueberry-1.4.2-1, blueman-1:2.1.4-1, pulseaudio-15.0-1, NetworkManager-bluetooth-1.44.0-1

Bluetooth — это технология беспроводной передачи данных. Она обеспечивает обмен информацией между различными устройствами, соединяя их посредством одной универсальной радиолинии с малым радиусом действия.

Установка

Для работы с **Bluetooth** в РЕД ОС уже предустановлена утилита **blueberry**. Если по какой-либо причине утилита в системе отсутствует, её можно установить вручную.

Для установки необходимо перейти в сеанс пользователя **root**:

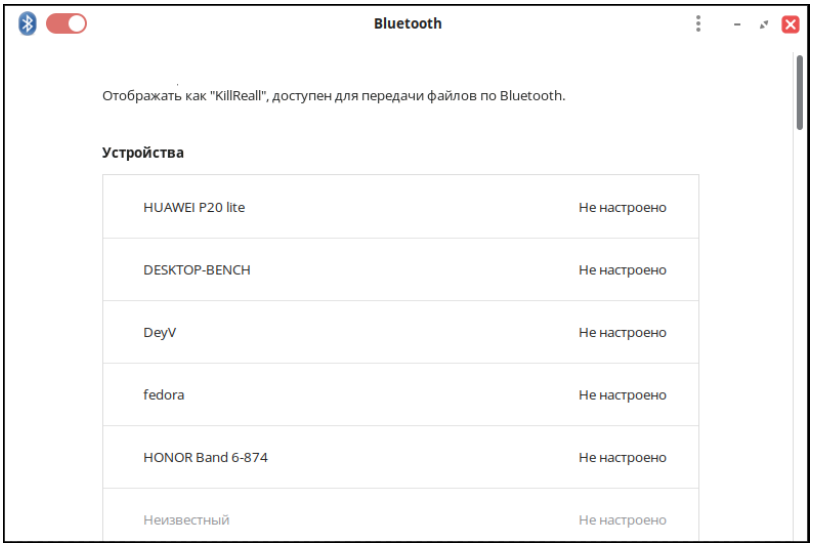
```
su -
```

и выполнить команду:

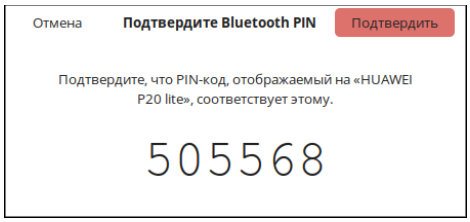
```
dnf install blueberry bluez bluez-cups bluez-hid2hci bluez-mesh bluez-tools
```

Подключение и настройка Bluetooth-устройств доступны из «**Главного меню**» - «**Параметры**» - «**Bluetooth**».

Перед запуском Bluetooth-менеджера необходимо предварительно включить используемый Bluetooth-адаптер (аппаратно). Ниже приведен пример подключения по Bluetooth к смартфону. Убедитесь, что устройства доступны для поиска и включите сопряжение, нажав на устройство.



При сопряжении подтвердите PIN-коды на обоих устройствах.



Утилита blueman

Blueman (*Bluetooth Manager*) - это менеджер Bluetooth, обладающий более удобным интерфейсом по сравнению с Bluetooth-менеджером пакета **blueberry**.

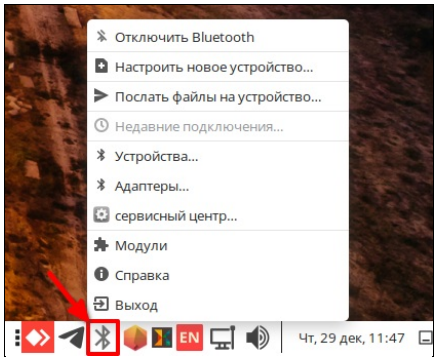
Blueman предоставляет более широкий функционал настройки соединения и управления устройствами.

Для установки **Blueman** выполните команду:

```
dnf install blueman
```

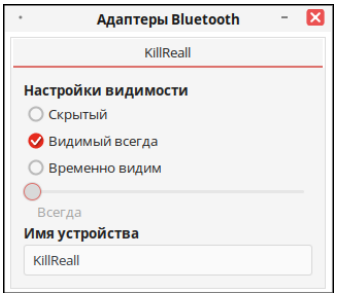
Работа с **Blueman** доступна из «**Главного меню**» - «**Параметры**» - «**Менеджер Bluetooth**» и из «**Главного меню**» - «**Параметры**» - «**Адаптеры Bluetooth**».

Также инструменты утилиты можно открыть через панель задач.

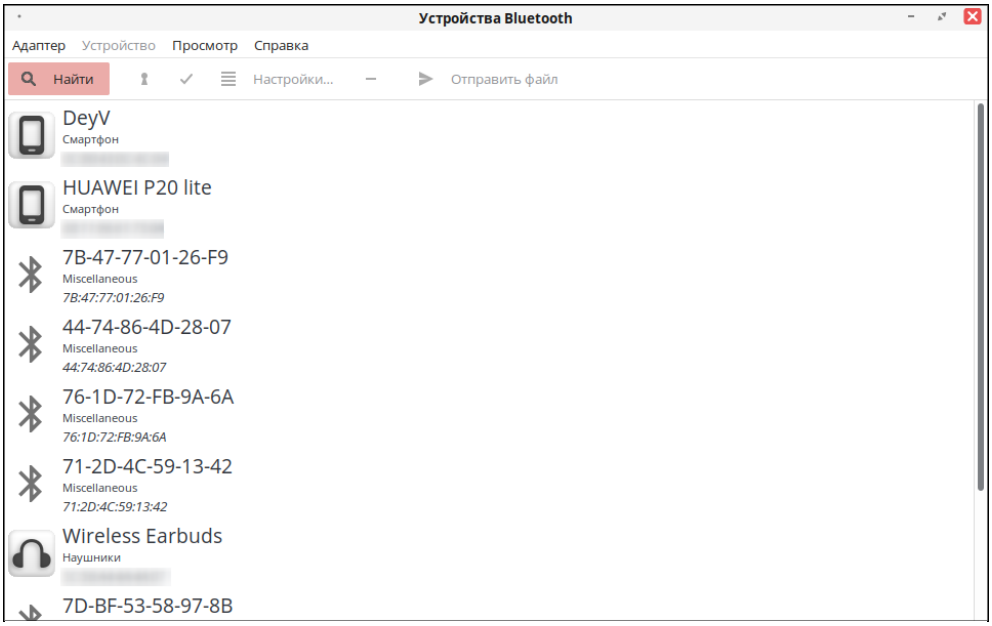


Утилита «**Адаптеры Bluetooth**» позволяет:

- задать имя, под которым будет отображаться устройство;
- задать настройки видимости адаптера для внешних устройств.



В утилите «**Менеджер Bluetooth**» отображается список найденных и подключенных устройств.



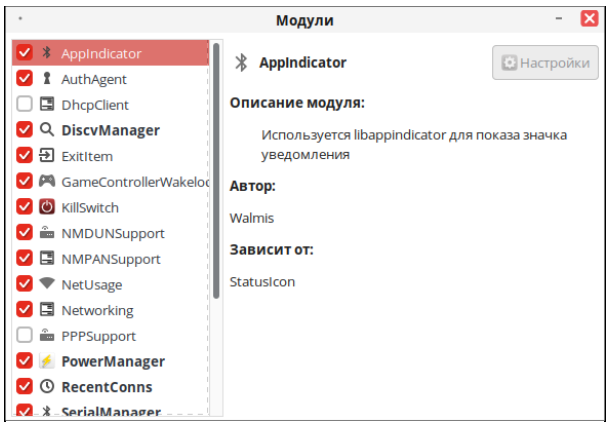
Вкладка «**Адаптер**» содержит компоненты для настройки Bluetooth-адаптера, включающие возможность запуска утилиты «**Адаптеры**

Bluetooth» и поиска внешних устройств.

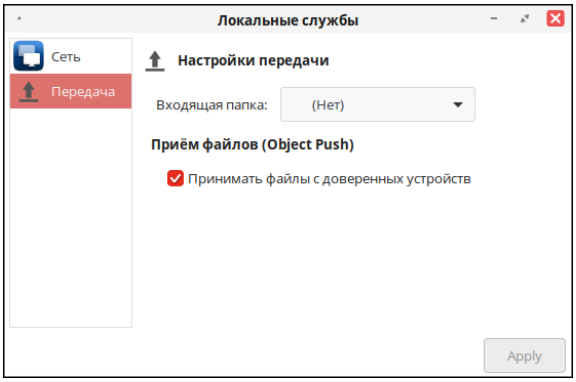
Вкладка «**Устройство**» содержит инструменты для взаимодействия с подключаемым устройством.

Вкладка «**Просмотр**» содержит инструменты для настройки интерфейса утилиты.

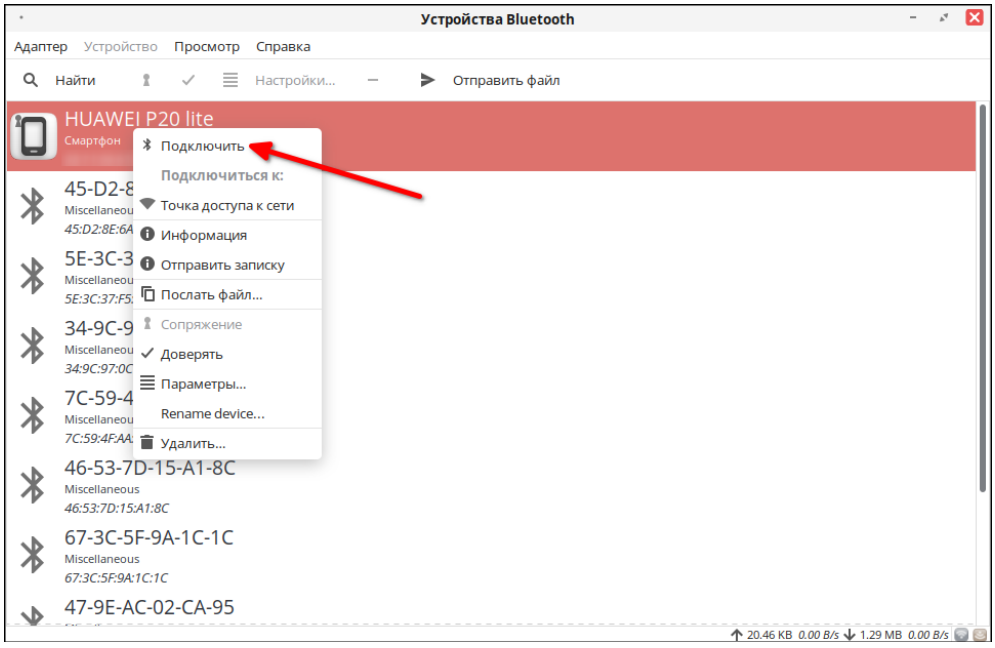
В этой же вкладке пункт «**Модули**» содержит компоненты, которые можно использовать для более функциональной работы **Blueman**, включая показ значков уведомлений, поддержку различных протоколов, отслеживание сетевого трафика и некоторые другие.



Пункт «**Сервисный центр**» содержит инструменты для настройки сетей и передачи данных.



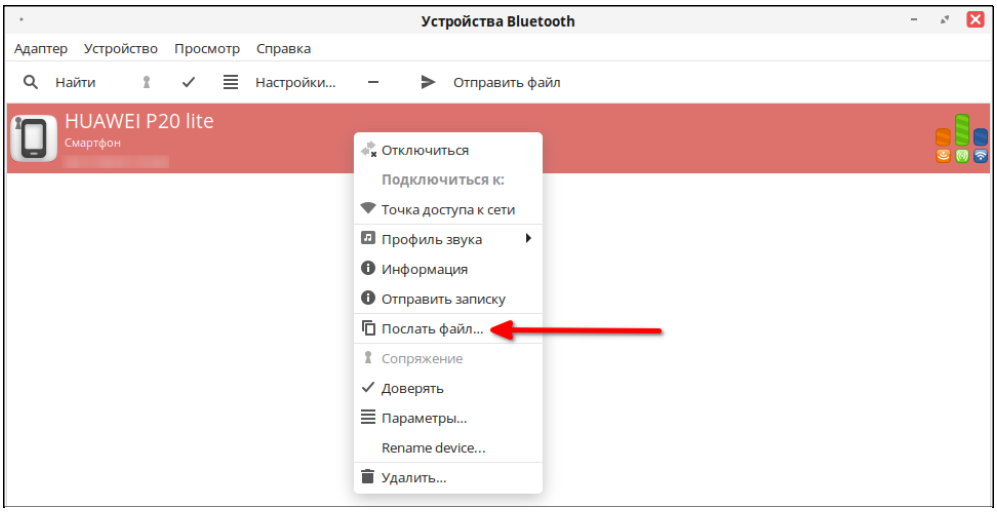
Перед подключением убедитесь, что ваши устройства доступны для поиска. Выберите необходимое устройство и выполните подключение.



При сопряжении подтвердите запрос авторизации.



Для отправки файла на другое устройство выберите необходимое устройство и осуществите передачу данных.



Настройка автоматического подключения bluetooth-устройств при загрузке

Включите автоматический запуск systemd-юнита:

```
systemctl enable bluetooth.service --now
```

Отредактируйте файл конфигурации **/etc/bluetooth/main.conf**:

```
nano /etc/bluetooth/main.conf
```

Активируйте автоматическое подключение доверенных устройств при запуске:

```
[Policy]
 AutoEnable=true
```

Любым способом определите MAC-адрес устройства (отображается как при поиске, так и в списке подключённых), затем войдите в консоль настройки Bluetooth-сервера:

```
bluetoothctl
```

Получите список сопряжённых устройств:

```
devices Paired
```

Если нужное оборудование с MAC-адресом AA:BB:CC:DD:EE:FF уже числится в списке, удалите его:

```
remove AA:BB:CC:DD:EE:FF
```

Запустите процесс поиска новых устройств, убедитесь, что устройство обнаруживается, затем отключите процесс сканирования:

```
scan on
scan off
```

Назначьте устройство доверенным:

```
trust AA:BB:CC:DD:EE:FF
```

Произведите сопряжение и выполните подключение:

```
pair AA:BB:CC:DD:EE:FF
connect AA:BB:CC:DD:EE:FF
```

После этого при следующей загрузке системы или при выходе из режима сна выбранное устройство будет подключено автоматически (при условии, если на компьютере включен bluetooth).

Для выхода из консоли настройки Bluetooth-сервера воспользуйтесь командой:

```
exit
```

Поддержка bluetooth-кодеков высокого качества в PulseAudio

В РЕД ОС по умолчанию установлены пакеты для работы с **PulseAudio**, что позволяет работать с кодеками высокого качества с помощью профиля **A2DP**.

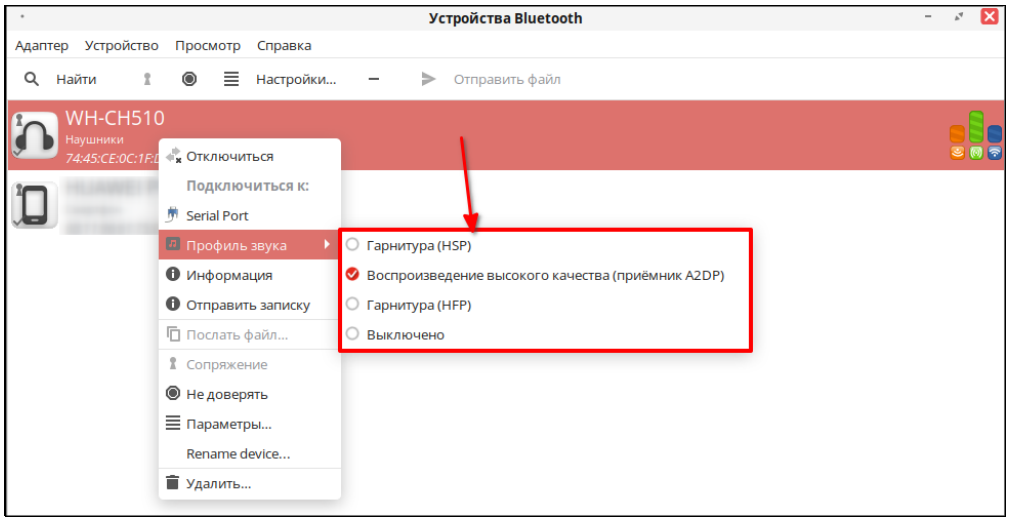
Если по какой-либо причине пакеты в системе отсутствуют, их можно установить вручную командой:

```
dnf install pulseaudio pulseaudio-module-bluetooth alsa-plugins-pulseaudio pulseaudio-libs pulseaudio-libs-glib2 pulseaudio-module-x11 pulseaudio-utils wine-pulseaudio
```

Примечание.

Выбранный кодек должен поддерживаться наушниками аппаратно.

Выбрать кодек можно в окне настройки устройства в менеджере **Blueman**.



Настройка интернет-соединения через bluetooth

Интернет через Bluetooth — это один из вариантов использования мобильного телефона для выхода в Интернет с компьютера.

Этот метод может стать альтернативой, если у компьютера нет Wi-Fi или USB-кабеля для подключения телефона по проводу. В данном случае телефон будет выступать в роли модема.

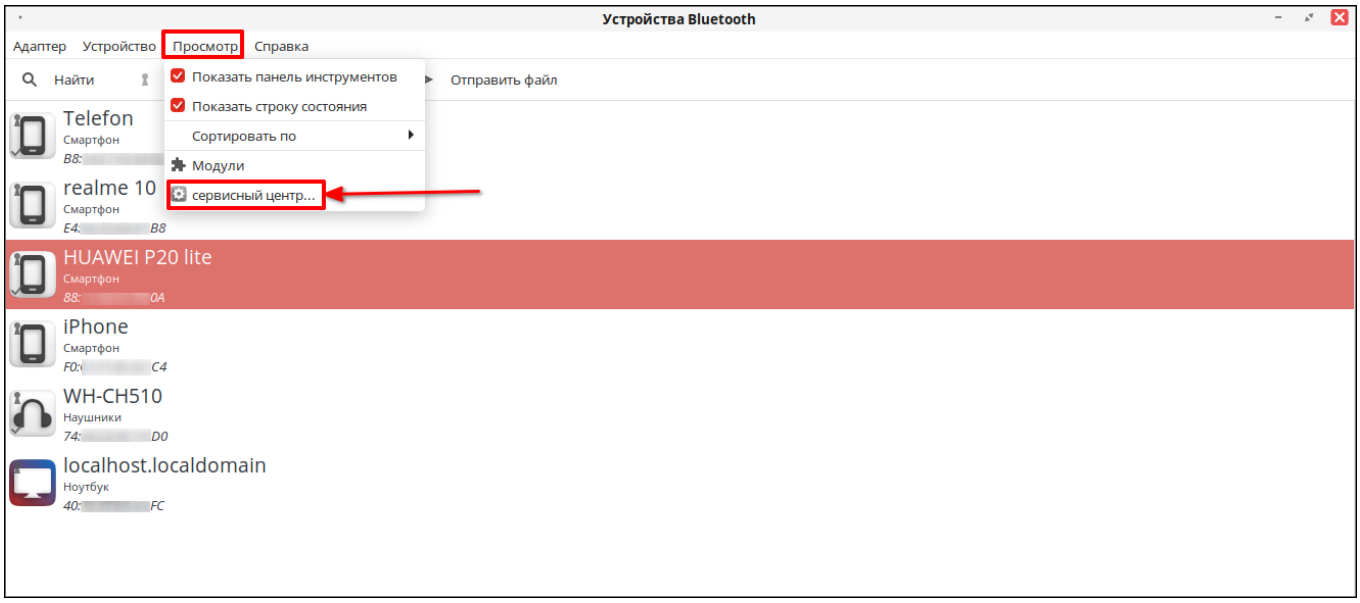
Для реализации данной функции необходим пакет blueman, а также некоторые дополнительные пакеты, которые можно установить командой:

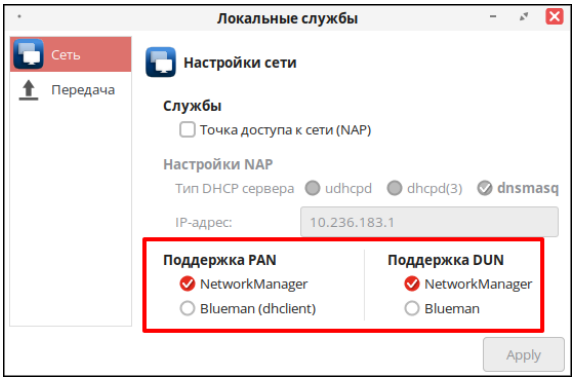
```
dnf install blueman NetworkManager-bluetooth dhcp-client dhcp-server dhcp-devel dnsmasq dnsmasq-utils
```

Выполните перезагрузку сетевых подключений:

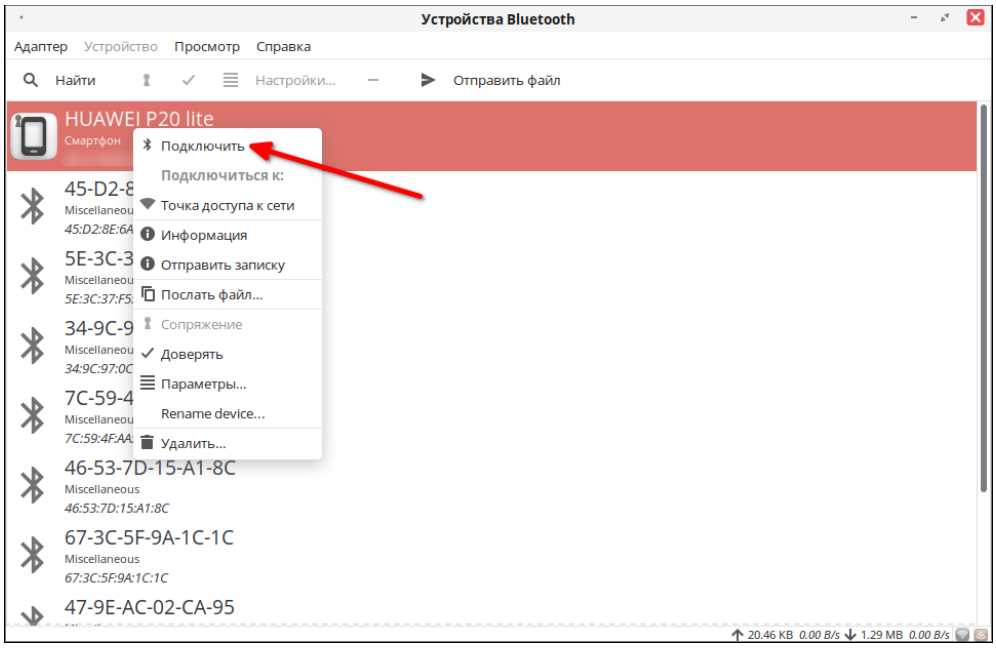
```
systemctl restart NetworkManager
```

В **Менеджере Bluetooth** выберите пункт меню «**Просмотр**» - «**Сервисный центр**». В открывшемся окне «Локальные службы» установите значение **NetworkManager** для пунктов «**Поддержка PAN**» и «**Поддержка DUN**».



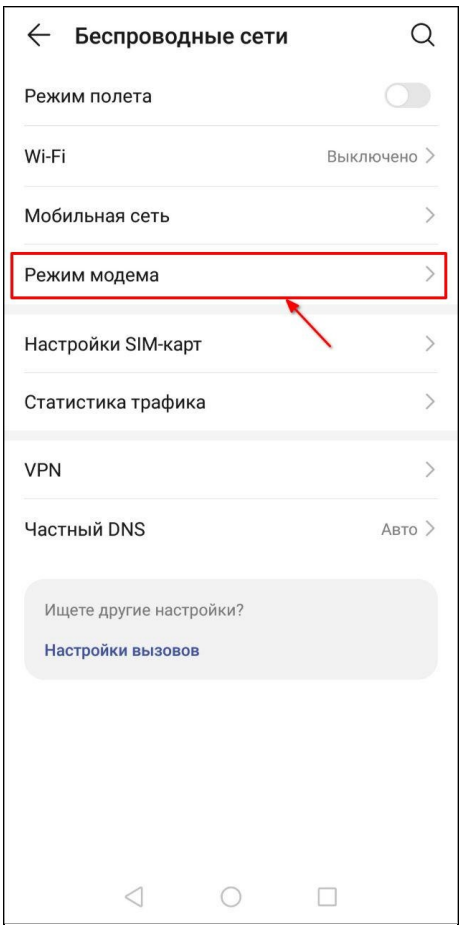


1. Для сопряжения телефона и компьютера выберите необходимое устройство и в контекстном меню нажмите «Подключить».



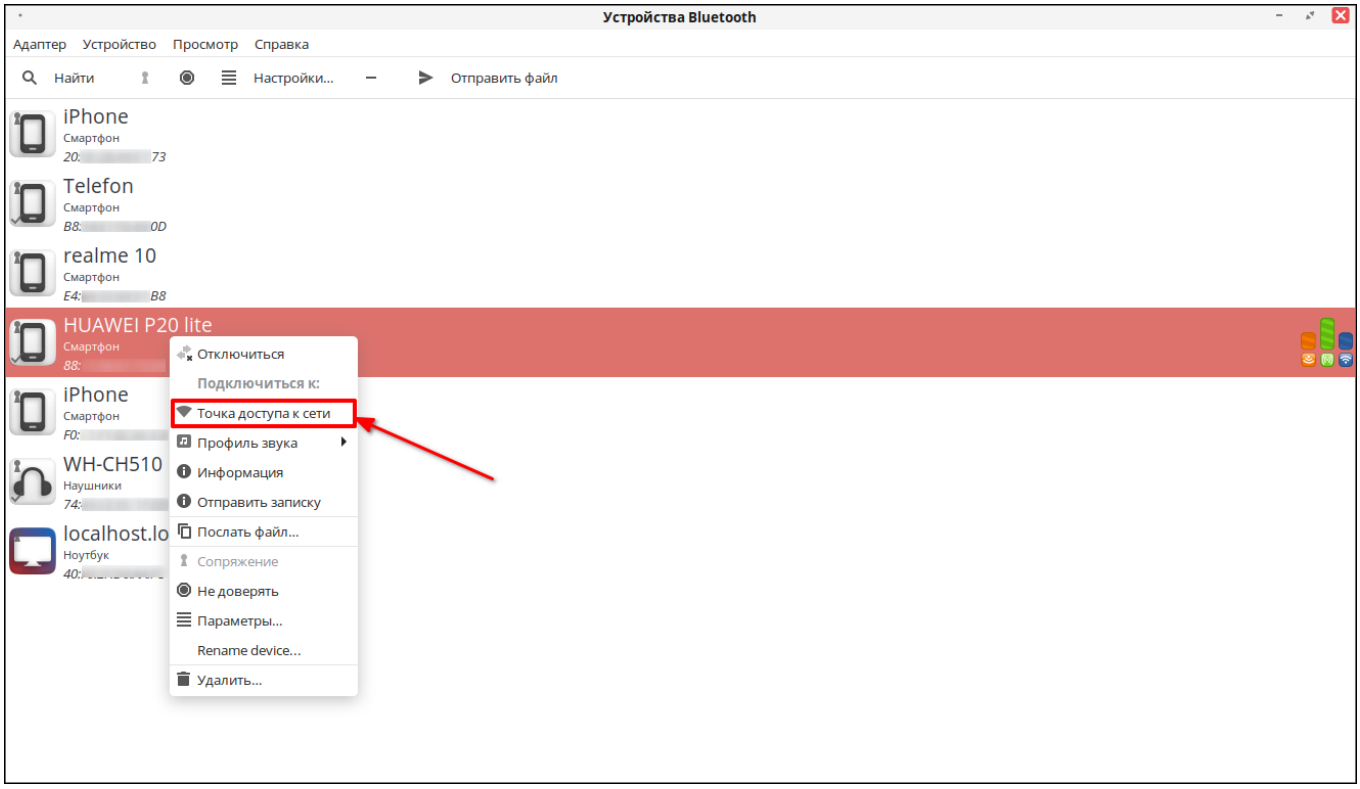
2. Для включения Bluetooth-модема на телефоне необходимо перейти в настройки телефона. Затем выбрать пункт «**Беспроводные сети**», перейти в раздел «**Режим модема**» и активировать Bluetooth-модем.

Стоит обратить внимание, что внешний вид и наименование пунктов меню может отличаться в зависимости от конкретной модели телефона.

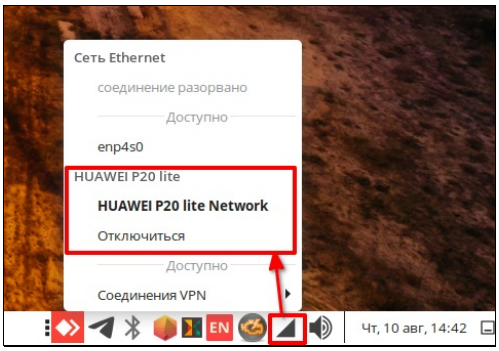




3. Для подключения ПК к Bluetooth-модему телефона выберите сопряжённое устройство и выполните подключение к точке доступа.



В настройках сетевых подключений вашего компьютера после этого должна появиться возможность подключаться к смартфону и управлять установленным соединением.



Однако стоит отметить, что при таком способе Интернет-соединения скорость передачи данных будет невысокой. На стандарте **Bluetooth 5** скорость будет **~1.6 Мбит/с**. Причём оба устройства (и телефон, и компьютер) должны поддерживать этот протокол.

На стандарте **Bluetooth 4** скорость передачи данных будет **не более 1 Мбит/с**.

Отключение CD-ROM

Запрет монтирования CD-ROM

Чтобы отключить **CD-ROM**, вам необходимо создать файл **/etc/modprobe.d/usb-storage.conf** и отредактировать его с помощью текстового редактора.

```
sudo nano /etc/modprobe.d/usb-storage.conf
```

Введите следующие строки в файл:

```
install usb-storage /bin/true
```

Вышеупомянутый файл **.conf** отражает фальшивую установку **CD-ROM**. Сохраните файл с помощью Ctrl + O, затем нажмите Enter, и выйдите из редактора с помощью Ctrl + X.

Запретите чтение/запись/выполнение всем пользователям, кроме **root**, на каталог, в который монтируются **CD-ROM**.

```
sudo chmod -R 700 /run/media
```

Для вступления изменений в силу перезагрузите компьютер.

Возврат возможности подключения

Для того чтобы вернуть возможность монтирования, выполните следующие команды

```
sudo rm -f /etc/modprobe.d/usb-storage.conf
sudo chmod -R 755 /run/media
```

Перезагрузите компьютер.

Ограничение доступа к USB-накопителям

Примеры выбора устройств по определенным свойствам
Запрет автомонтирования с параметром UDISKS_IGNORE
Создание белого списка с параметром UDISKS_IGNORE
Запрет автомонтирования с параметром authorized
Создание белого списка с параметром authorized

Алгоритм создания белого списка USB-флеш-накопителей состоит из 2 этапов:

Вариант 1:

1. Запрет монтирования всех USB-флеш-накопителей
2. Разрешение монтирования некоторых устройств

Вариант 2:

1. Разрешение монтирования некоторых устройств
2. Запрет монтирования всех иных USB-флеш-накопителей

Вы можете подробнее ознакомиться с информацией по ограничению доступа к USB-накопителям, просмотрев наши обучающие видео:

- на **RuTube** — Ограничение доступа к USB-накопителям;
- в **Яндекс.Дзен** — Ограничение доступа к USB-накопителям;
- в **VK Видео** — Ограничение доступа к USB-накопителям.

На наших каналах вы также сможете найти много другой полезной информации.

Примеры выбора устройств по определенным свойствам

Для создания белого списка USB-флеш-накопителей необходимо знать атрибуты накопителя.

1) Определите ваш флеш-накопитель:

```
 ls -l /dev/sd*

brw-rw---- 1 root disk 8, 0 июн 30 12:59 /dev/sda
brw-rw---- 1 root disk 8, 1 июл 22 12:59 /dev/sda1
brw-rw---- 1 root disk 8, 2 июл 22 12:59 /dev/sda2
brw-rw---- 1 root disk 8, 3 июн 30 12:59 /dev/sda3
brw-rw---- 1 root disk 8, 16 июл 22 13:43/dev/sdb # нужная нам строка
brw-rw---- 1 root disk 8, 17 июн 30 13:43 /dev/sdb1
```

2) Проверьте атрибуты (символы после **sd*** должны вводиться в соответствии с вашим выводом команды `ls -l /dev/sd*`):

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром UDISKS_IGNORE

Для отключения автомонтирования USB-флеш-накопителей необходимо создать правило для **udev**.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
```

Флаг `ENV{UDISKS_IGNORE}` отвечает за игнорирование устройства:

- «0» – false;
- «1» - true.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром UDISKS_IGNORE

Выборка разрешения доступа по трем параметрам:

- серийному номеру устройства;
- модели;
- максимальному потребления тока.

Для их определения выполните поочередно команды:

```
udevadm info -a -p /sys/block/sdb | grep serial
udevadm info -a -p /sys/block/sdb | grep product
udevadm info -a -p /sys/block/sdb | grep bMaxPower
```

в выводе будет отображен серийный номер, модель и значение максимального потребления тока:

```
ATTRS{serial}=="04GS1F3LBIBDWU05"
 ATTRS{model}=="Silicon-Power8G "
 ATTRS{bMaxPower}=="200mA"
```

Запишите эти значения в файл правил в качестве разрешающих.

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
 ATTRS{serial}=="04GS1F3LBIBDWU05",ENV{UDISKS_IGNORE}="0"
 ATTRS{product}=="DataTraveler 3.0",ENV{UDISKS_IGNORE}="0"
 ATTRS{bMaxPower}=="200mA",ENV{UDISKS_IGNORE}="0"
```

Здесь:

- **1** - заблокировать все usb-накопители;
- **0** - разрешить накопитель по определенным свойствам.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, находится в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром authorized

Для отключения автомонтирования USB-флеш-накопителей необходимо будет создать правило для **udev** и исполняемый скрипт запрета монтирования USB-флеш-накопителей.

Создайте скрипт:

```
nano /usr/bin/remove_usb.sh
```

```
#!/bin/bash
var=$1
var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
echo 0 > '/sys/bus/usb/devices'$var2'authorized'
```

Измените права на скрипт:

```
chmod +x /usr/bin/remove_usb.sh
```

Параметр **authorized** отвечает за монтирование USB-флеш-накопителя в момент подключения к ПК.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
```

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром authorized

Выборка по серийному номеру устройства:

```
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
```

Выборка по названию модели. Точное название смотрите в выводе команды:

```
 udevadm info -a -p /sys/block/sdb

ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
```

Для удобства, когда полный список параметров устройства известен, можно производить отбор по конкретному параметру:

```
udevadm info -a -p /sys/block/sdb | grep "ATTRS{serial}"
udevadm info -a -p /sys/block/sdb | grep "ATTRS{product}"
```

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ACTION!="add", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}=="usb-storage", RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
LABEL="dont_remove_usb"
```

Логика данного правила отлична от первого варианта. В первом варианте происходила блокировка сразу всех usb флеш-накопителей, а только потом осуществлялось добавление устройств в белый список. В данном (втором) варианте сначала происходит добавление устройств в белый список, а только потом блокирование устройств (добавление в черный список). Такое действие связано с тем, что параметр **authorized** появляется в момент монтирования и, если его значение установить в **0**, то для дальнейшей работы он становится недоступен. Соответственно, сначала требуется проверить, входит ли флеш-накопитель в белый список, и если входит, то разрешить его монтирование.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, отображается в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Настройка протоколирования событий подключения USB-накопителей

Создаем правила для **udev**:

```
nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды

```
#log mount/unmount
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo unmount $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

После выполнения данных действий будут фиксироваться все факты подключения/отключения usb-накопителей.

Настройка принадлежности USB-накопителей

В данной статье будет рассмотрен пример разграничения правил для разных пользователей.

Сначала необходимо создать udev-правило, содержащее разрешения на определенные usb-устройства, по выбранным пользователем параметрам.

```
nano /etc/udev/rules.d/80-alloweduserlist1.rules
```

```
ACTION!="add", GOTO="dont_remove_usb"
 ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
 ATTRS{product}=="USB DISK 2.0",GOTO="dont_remove_usb"
 ENV{DRIVER}=="usb-storage",RUN+="/bin/python3 /usr/local/bin/remove_usb.py $devpath"
 LABEL="dont_remove_usb"
 ENV{DRIVER}=="usb-storage", ENV{UDISKS_AUTO}="0"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="add", RUN+="/bin/systemctl start usb-mount-list1@%k.service"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="remove", RUN+="/bin/systemctl stop usb-mount-list1@%k.service"
```

Затем необходимо создать скрипт для запрета монтирования устройств со следующим содержимым:

```
nano /usr/local/bin/remove_usb.py
```

```
#!/usr/bin/python3
 import os
 import sys
 var = sys.argv[1].strip()
 var2 = os.popen(f"echo {var} | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//'").readlines()[0]
 os.system(f"echo 0 > '/sys/bus/usb/devices{var2.strip()}authorized'")
```

Далее создайте сервис, отвечающий за запуск скрипта, проверяющего список доступных пользователей для данного udev-правила.

```
nano /etc/systemd/system/usb-mount-list1@.service
```

```
[Unit]
 Description=Mount USB Drive on %i

 [Service]
 RemainAfterExit=true
 Type=oneshot
 ExecStart=/usr/bin/python3 /usr/local/bin/usb-mount.py add %i /etc/udev/rules.d/80-alloweduserlist1.rules
 ExecStop=/usr/bin/python3 /usr/local/bin/usb-mount.py remove %i /etc/udev/rules.d/80-alloweduserlist1.rule
```

Следующим этапом формируется список разрешенных пользователей.

Допустимые значения **umask**:

- 0 - rwx - полные права; rw - чтение/запись;
- 2 - r - чтение.

Создайте список разрешенных пользователей (в примере **user1** с правами на чтение) без проверки на группы:

```
mkdir /etc/udevlist
nano /etc/udevlist/userlist1.json
```

```
{"user1": 2}
```

Если необходимо указать несколько пользователей, список указывается в виде `{"user1": 2, "user2": 0, ...}`.

Затем создайте файл соответствия udev-правила со списком разрешенных пользователей:

```
nano /etc/udevlist/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/userlist1.json"}
```

Создайте список разрешенных групп:

```
mkdir /etc/udevlist/group/
nano /etc/udevlist/group/grouplist1.json
```

```
{}
```

Если в правиле необходимо использовать разграничение по группам, список указывается в виде `{"name_group1": 0, "name_group2": 2}`.

После этого создайте файл соответствия udev-правила со списком разрешенных групп:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/group/grouplist1.json"}
```

Создайте файл для других списков, если используются:

```
mkdir /etc/udevlist/otherlists/
nano /etc/udevlist/otherlists/otherlists1.json
```

с содержимым вида:

```
{"others": 7}
```

После этого создайте файл соответствия udev-правила с новым списком:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/otherlists/otherlists1.json"}
```

Затем загрузите скрипт проверки доступа пользователей и монтирования устройств, распакуйте архив и переместите файл скрипта в каталог **/usr/local/bin/**:

```
wget https://redos.red-soft.ru/upload/usb-mount.zip
unzip ./usb-mount.zip -d /usr/local/bin/
```

Для применения настроек перезапустите службы командой:

```
systemctl daemon-reload
```

Настройка учета USB-накопителей

Создаем правила для **udev**:

```
sudo nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды (в примере показан учет **USB** на основе серийного номера):

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add",RUN+="/bin/sh /mnt/logs.sh $devnode %E{ID_SERIAL}"
```

Создаем скрипт для ведения лог файла. Если указать путь **/root/log.txt**, то доступ к файлу лога будет только у пользователя **root**.

```
nano /mnt/logs.sh
```

```
path=$1
 serial=$2
 File="/root/log.txt"
 if ! grep -q "$serial" "$File";
 then
 echo $path $serial $(date)>> /root/log.txt
 fi
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

Ограничение доступа USB-устройств по defines class code

Существует большое количество устройств, имеющих разный *USB defines class code*. Для того чтобы разрешить подключение определенного класса устройств, потребуется применить следующий алгоритм:

1) Создать правило, в котором прописаны разрешенные устройства, а остальные блокируются:

```
nano /etc/udev/rules.d/99-usb-bInterfaceClass.rules
```

Содержимое правила на примере классов для **token**, **HID**, **audio** и **video** устройств:

```
# Allow all TOKEN devices
 ATTR{bInterfaceClass}=="0b",ACTION=="add",GOTO="usb_rules_end"
 # Allow all c
 ATTR{bInterfaceClass}=="03",ACTION=="add",GOTO="usb_rules_end"
 # Allow all AUDIO devices
 ATTR{bInterfaceClass}=="01",ACTION=="add",GOTO="usb_rules_end"
 # Allow all VIDEO devices
 ATTR{bInterfaceClass}=="0e",ACTION=="add",GOTO="usb_rules_end"
 SUBSYSTEM=="usb",ACTION=="add",RUN+="/bin/sh -c '/usr/bin/reject_usb_bInterfaceClass.sh $devpath'"
 LABEL="usb_rules_end"
```

2) Создать скрипт, изменяющий атрибут **authorized** для определенного устройства:

```
nano /usr/bin/reject_usb_bInterfaceClass.sh
```

Содержимое скрипта:

```
#!/bin/bash
 var=$1
 var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
 var3=$(echo $var2 | grep '^/[0-9]-[0-9]$')
 var4=$(echo $var2 | grep '^/[0-9]-[0-9].[0-9]$')
 if [ -z "$var3" ] && [ -z "$var4" ]; then
 echo 0 > '/sys/bus/usb/devices'$var2'/authorized'
 fi
```

Сделайте скрипт исполняемым:

```
chmod +x /usr/bin/reject_usb_bInterfaceClass.sh
```

Перезапустите правила **udev**:

```
sudo udevadm control --reload-rules
```

HUB устройства

Есть устройства, которые системой определяются как **HUB**. В момент редактирования правил и перезагрузки **udev** на **HUB**-устройства, которые находятся в системном блоке/кейсе, влияние оказано не будет, так как они не переподключаются. Зато при перезагрузке ОС они заблокируются и в итоге все подключенные к ним устройства ниже по дереву тоже будут заблокированы. Для корректного редактирования устройств подключенных через **HUB** требуется в правилах разрешить:

```
DRIVER=="hub",ACTION=="add",GOTO="end_usb_rules"
```

либо:

```
ATTR{bInterfaceClass}=="09",ACTION=="add",GOTO="usb_rules_end"
```

Перезапустить правила:

```
udevadm control --reload-rules
```

Утилита по созданию правил для монтирования USB-накопителей

Установка
Полная блокировка всех usb
Назначение личной привязки к UDEV-правилу
Протоколирование событий usb-flash накопителей

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** usb_rules-2.1-1

Утилита **usb_rules** основана на работе с правилами **udev** и системными сервисами **systemd**.

Вы можете подробнее ознакомиться с работой утилиты **usb_rules**, просмотрев наши обучающие видео:

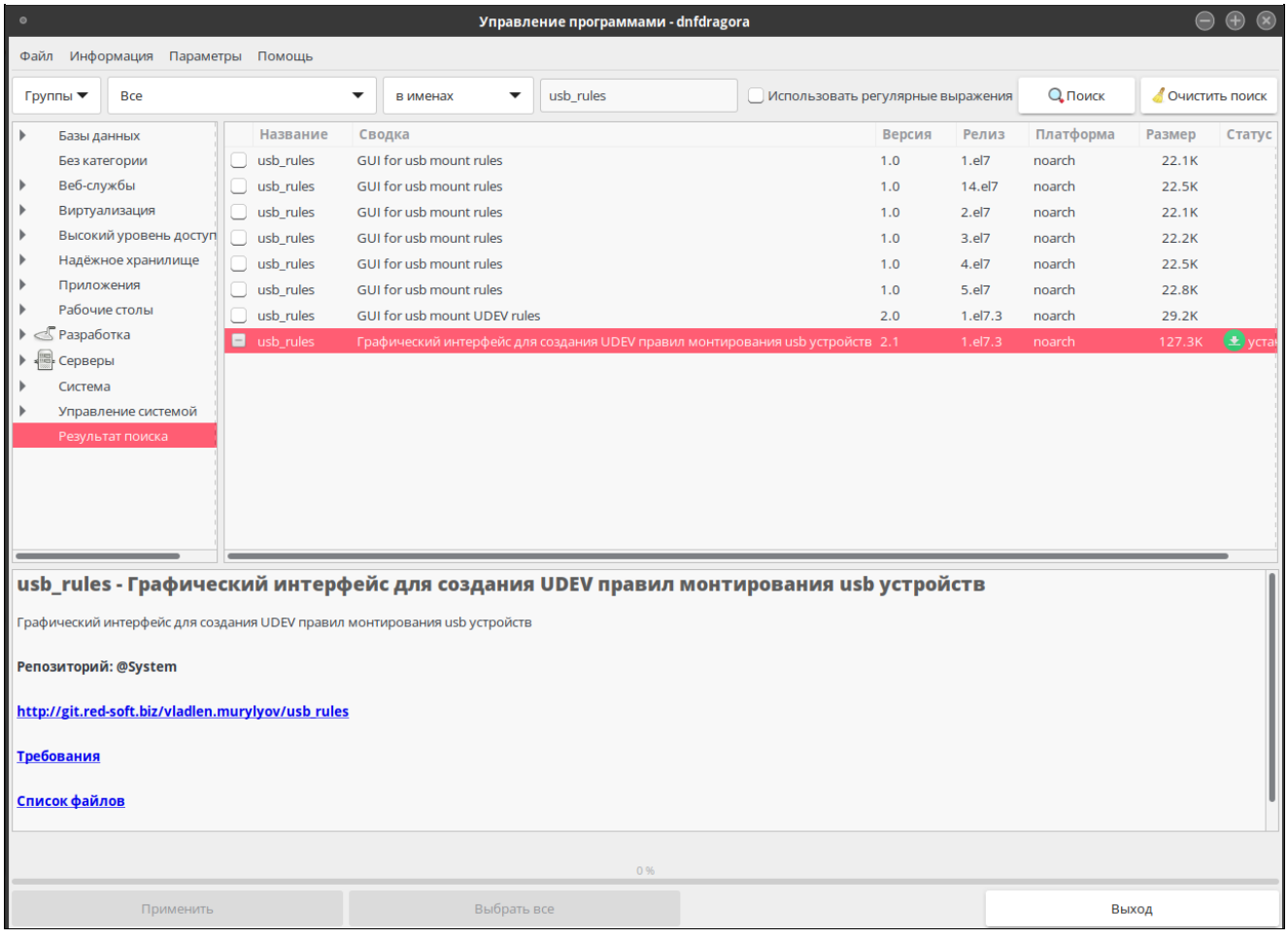
- на **RuTube** — Утилита по созданию правил для монтирования usb-flash накопителей;
- в **Яндекс.Дзен** — Утилита по созданию правил для монтирования usb-flash накопителей;
- в **VK Видео** — Утилита по созданию правил для монтирования usb-flash накопителей.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установка утилиты доступна через пакетный менеджер *dnfdragora* («**Главное меню**» - «**Администрирование**» -«**Управление пакетами dnfdragora**»).

В поисковой строке пакетного менеджера введите название утилиты «**usb_rules**», нажмите «**Enter**» для поиска. Из списка результатов выберите последнюю версию утилиты и нажмите кнопку «**Применить**».



Будет выполнена установка пакета.

Также установка утилиты доступна из терминала. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

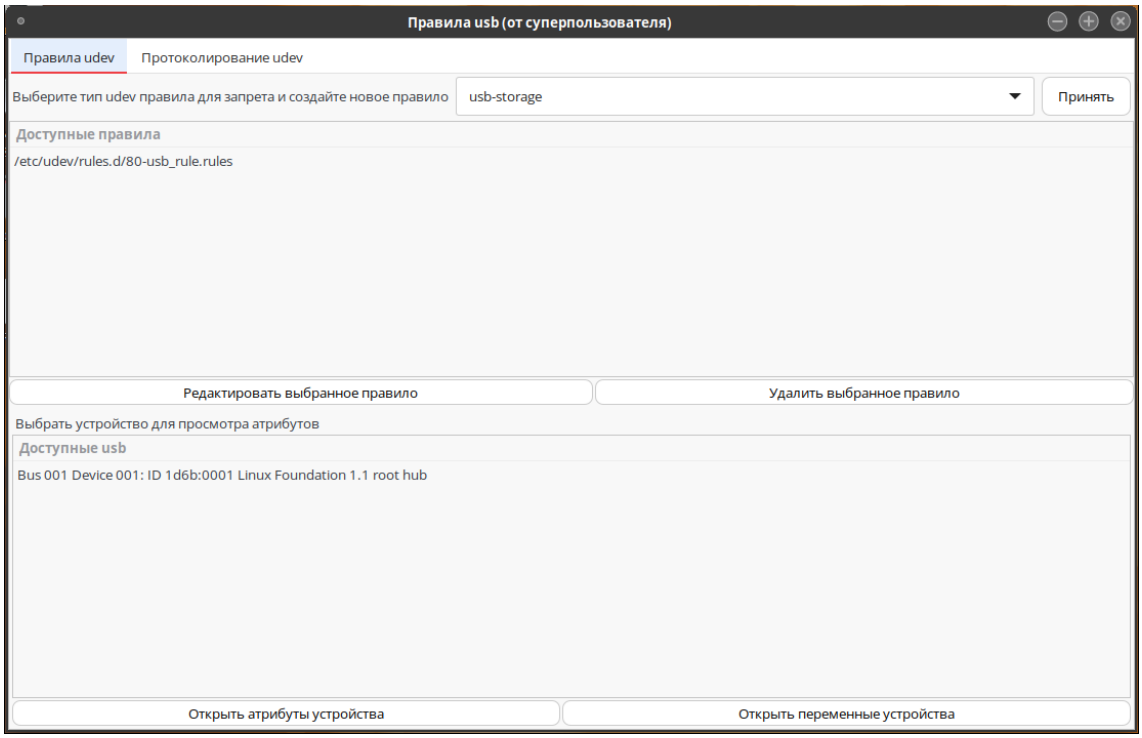
и выполните команду:

```
dnf install usb_rules
```

После установки запуск утилиты доступен с правами пользователя **root** из «**Главного меню**» - «**Параметры**» - «**Настройка ограничения монтирования**» или через терминал с помощью команды:

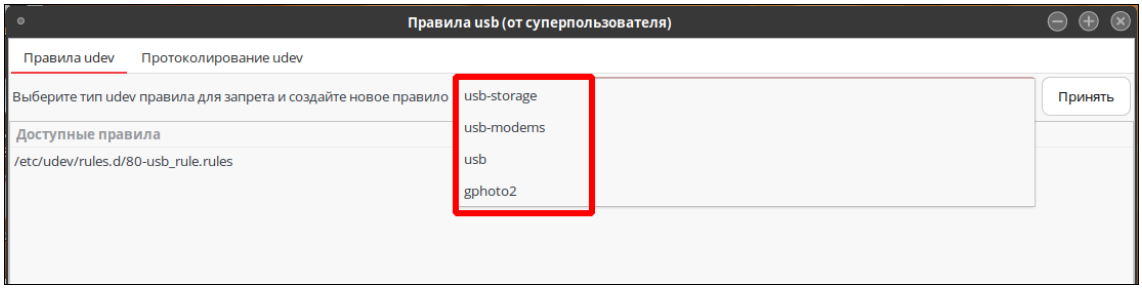
```
usb-rules
```

Стартовое окно утилиты позволяет пользователю ознакомиться с подключенными usb-устройствами и со списком уже созданных правил.



При формировании нового правила пользователю доступны 4 шаблона:

- **usb-storage**;
- **usb-modems**;
- **usb**;
- **gphoto2**.



Каждое из правил отвечает за полную блокировку тех или иных устройств.

Полная блокировка всех usb

Ниже представлено содержимое шаблонов для каждого правила:

```
#type:usb-storage
```

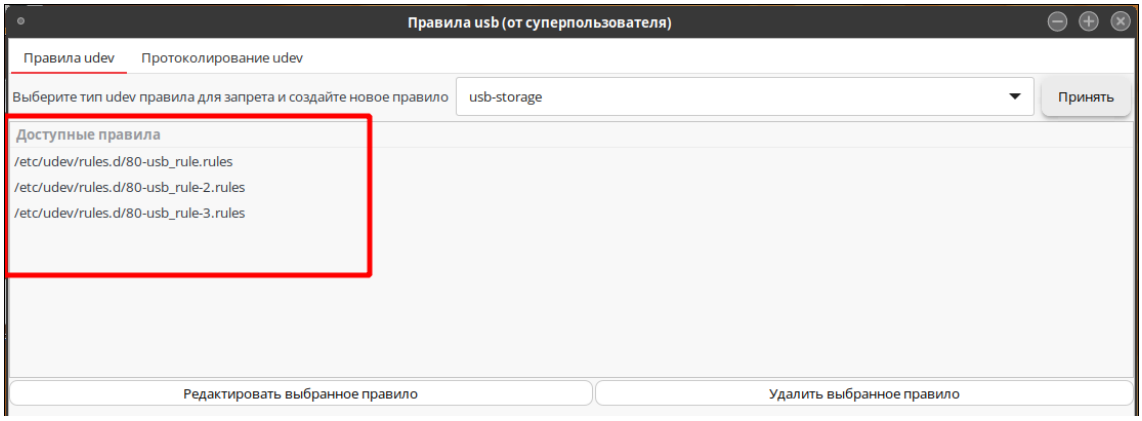
```
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:usb-modems
ACTION!="add", GOTO="dont_remove_usb"
DRIVER!="rndis_host", GOTO="dont_remove_usb"
DRIVER=="rndis_host", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

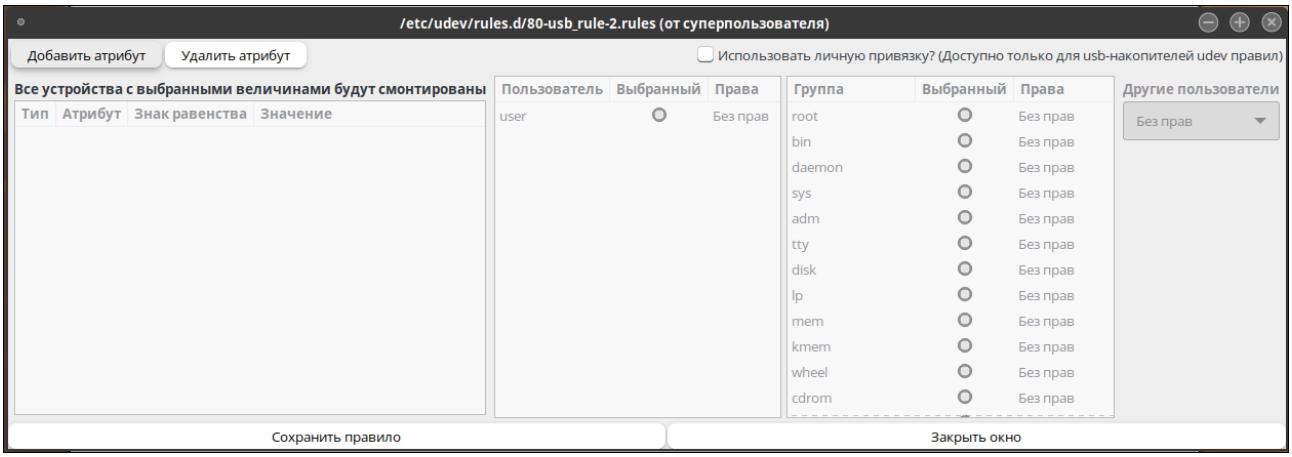
```
#type:usb
ACTION!="add", GOTO="dont_remove_usb"
SUBSYSTEM!="usb", GOTO="dont_remove_usb"
SUBSYSTEM=="usb", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:gphoto2
ACTION!="add", GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}!="PTP",GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}=="PTP",ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

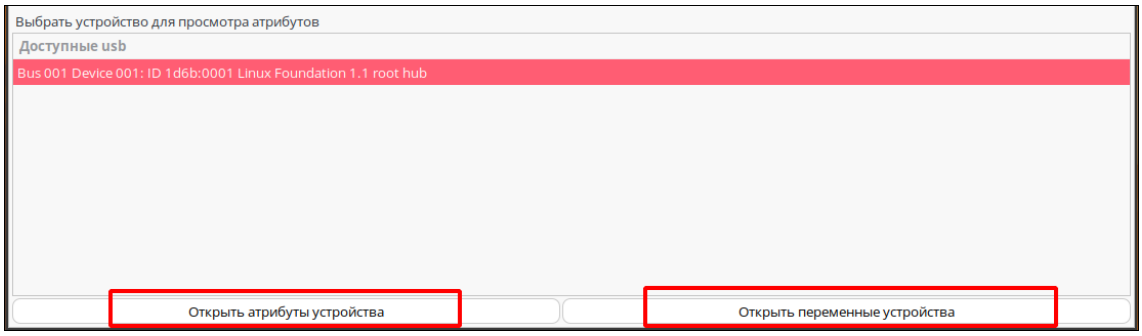
При формировании правила из шаблонного в окне утилиты появляется строка, соответствующая сформированному правилу.



Далее потребуется создать разрешающие монтирование параметры. Для этого необходимо добавить атрибут, который в новом правиле будет отвечать за исключение из блокировки устройств, подходящих под данный параметр. Добавление или удаление таких атрибутов доступно после выбора интересующего правила и нажатия кнопки «**Редактировать правило**».

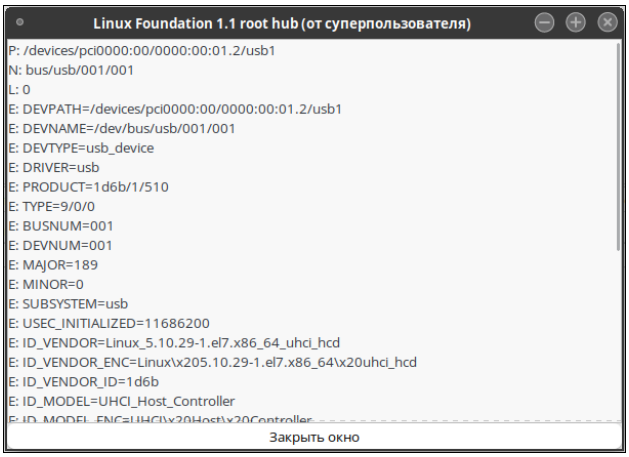


В полях «**Атрибут**» и «**Значение**» необходимо подобрать значения из доступных устройств. Просмотр доступных значений можно осуществить следующим образом:



В результате будут открыты следующие окна:

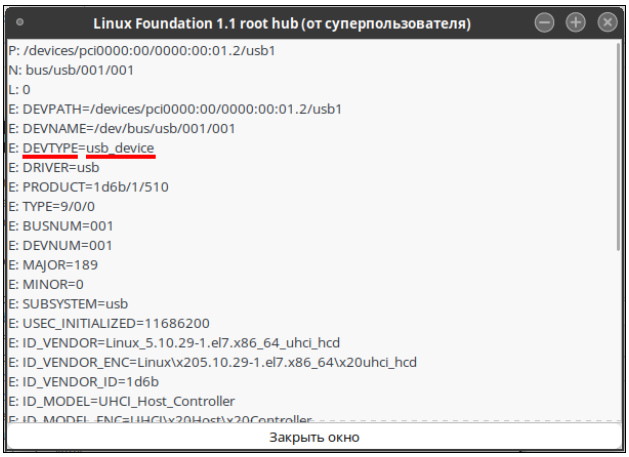




При добавлении пункта **ATTR** следует прописать значение и величины соответствующие:

Значения указываются, соответственно, без фигурных скобок **{}** и без кавычек **""**.

Для указания величин **ENV** следует выбирать величины:

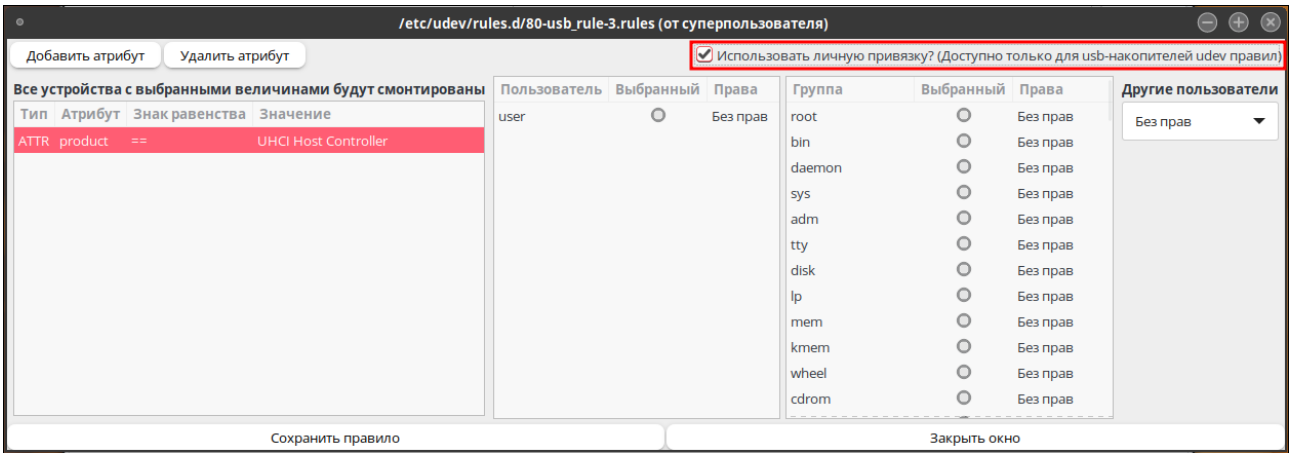


В результате будет сформировано примерно следующее правило **/etc/udev/rules.d/80-usb_rule.rules**:

```
#type:usb-storage
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTR{product}==UHCI Host Controller, GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

Назначение личной привязки к UDEV-правилу

За назначение привязки отвечает поле, которое активируется соответствующим флагом:



По умолчанию все пользователи не имеют прав. Соответственно, потребуется выбрать необходимых пользователей и задать им права «**чтения**», «**чтения и записи**» или «**все права**».

При формировании личной привязки будет создаваться **systemd**-сервис, который будет работать в связке с отведенным под него udev-правилом.

```
nano /etc/systemd/system/usb-mount@.service
```

```
[Unit]
Description=Mount USB Drive on %i

[Service]
RemainAfterExit=true
Type=oneshot
ExecStart=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py add %i /etc/udev/rules.d/80-usb_rule.rules
ExecStop=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py remove %i /etc/udev/rules.d/80-usb_rule.rules
```

Протоколирование событий usb-flash накопителей

Вкладка «**Протоколирование udev**» позволяет протоколировать события, связанные с **usb-flash** накопителями по выбранным пользователем атрибутам. Синтаксис добавления идентичен добавлению **ENV**-атрибутов.

В результате формирования правила для протоколирования будет создан файл **/etc/udev/rules.d/98-usb_logs.rules** со следующим примерным содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo disconnected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
```

USBIP - утилита для подключения удаленных USB-устройств

Настройка на сервере
Настройка на клиенте
Графическая утилита usbip-gui

USBIP — это утилита, направленная на предоставление в общий доступ USB-устройств через IP-сеть для совместного использования. Чтобы совместно использовать USB-устройства между компьютерами с их полной функциональностью, *USBIP* преобразует «сообщения ввода-вывода USB» в полезные данные **TCP/IP** и передает их между компьютерами. Оригинальные драйверы и приложения для USB-устройств также могут использоваться для удаленных USB-устройств без их модификации. Компьютер может использовать удаленные USB-устройства, как если бы они были напрямую подключены.

Устройства, которые можно подключить через утилиту:

- запоминающие устройства USB: флешки, внешние жесткие диски и картридеры;
- периферийные устройства ввода: USB-клавиатуры, мыши;
- мультимедийные устройства (например, веб-камеры);
- оборудование для печати и сканирования.

Вы можете подробнее ознакомиться с установкой и настройкой утилиты **USBIP**, просмотрев наши обучающие видео:

- на **RuTube** — Подключение удаленных USB устройств. USBIP;
- в **Яндекс.Дзен** — Подключение удаленных USB устройств. USBIP;
- в **VK Видео** — Подключение удаленных USB устройств. USBIP.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка на сервере

Сервер предназначен для публикации **USB-устройств**, которые могут быть удаленно доступны с клиентской стороны. Он выполняет роль хоста, предоставляя подключенные к нему **USB-устройства** (например, флеш-накопители, принтеры, сканеры) для использования через сеть. Это позволяет клиентам взаимодействовать с устройствами так, как если бы они были подключены локально.

Для начала работы необходимо установить утилиту *USBIP* командой (потребуются права **администратора**):

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe usbip-host
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 usbip-host
 vhci-hcd
```

Сохраните изменения и закройте редактор. Чтобы обеспечить автоматический запуск **usbipd** при старте системы, его можно оформить в виде системного юнита:

```
nano /etc/systemd/system/usbipd.service
```

Добавьте в файл следующие строки:

```
[Unit]
 Description=USBIPd
```

```
[Service]
ExecStart=/usr/sbin/usbipd -D
Type=oneshot
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

После создания или изменения системного юнита необходимо перезагрузить настройки менеджера системных служб и включить автоматический запуск службы usbipd, чтобы она запускалась сразу после загрузки системы. Для этого выполните следующие команды:

```
sudo systemctl daemon-reload
sudo systemctl enable usbipd --now
```

Перед тем как открыть доступ к какому-либо usb-устройству, нужно узнать его ID. Сделать это можно командой:

```
usbip list -l
```

Доступ к устройству открывается с помощью команды:

```
sudo usbip bind --busid=1-1
```

где **1-1** - это ID устройства.

Проверить, что устройство успешно привязано и доступно для использования, можно выполнив на сервере команду:

```
usbip list -r localhost
```

Для закрытия доступа к устройству необходимо ввести команду:

```
sudo usbip unbind -b 1-1
```

Настройка на клиенте

Клиент предназначен для подключения **USB-устройств**, опубликованных на сервере. Через клиента устройства, находящиеся на сервере, становятся доступными для локального использования, как если бы они были подключены непосредственно к клиентскому компьютеру.

Для начала работы необходимо установить утилиту *USBIP* командой:

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 vhci-hcd
```

Сохраните изменения и закройте редактор.

Проверить доступность USB-устройств, подключенных к серверу, можно выполнив на клиенте команду:

```
sudo usbip list -r <IP-адрес-сервера>
```

Для подключения открытого в общий доступ устройства на сервере к компьютеру-клиенту надо знать его ID и IP-адрес сервера. Для этого необходимо выполнить команду:

```
sudo usbip attach --remote=<IP-адрес-сервера> --busid=1-1
```

где:

- **1-1** — это ID устройства,
- **<IP-адрес-сервера>** — это IP-адрес сервера в формате **xx.xx.xx.xx**.

После подключения USB-устройства оно должно отображаться после выполнения команды:

```
lsusb
```

Для того чтобы отключить устройство из общего доступа, необходимо узнать его порт:

```
sudo usbip port
```

После того, как порт определен, можно отсоединить устройство:

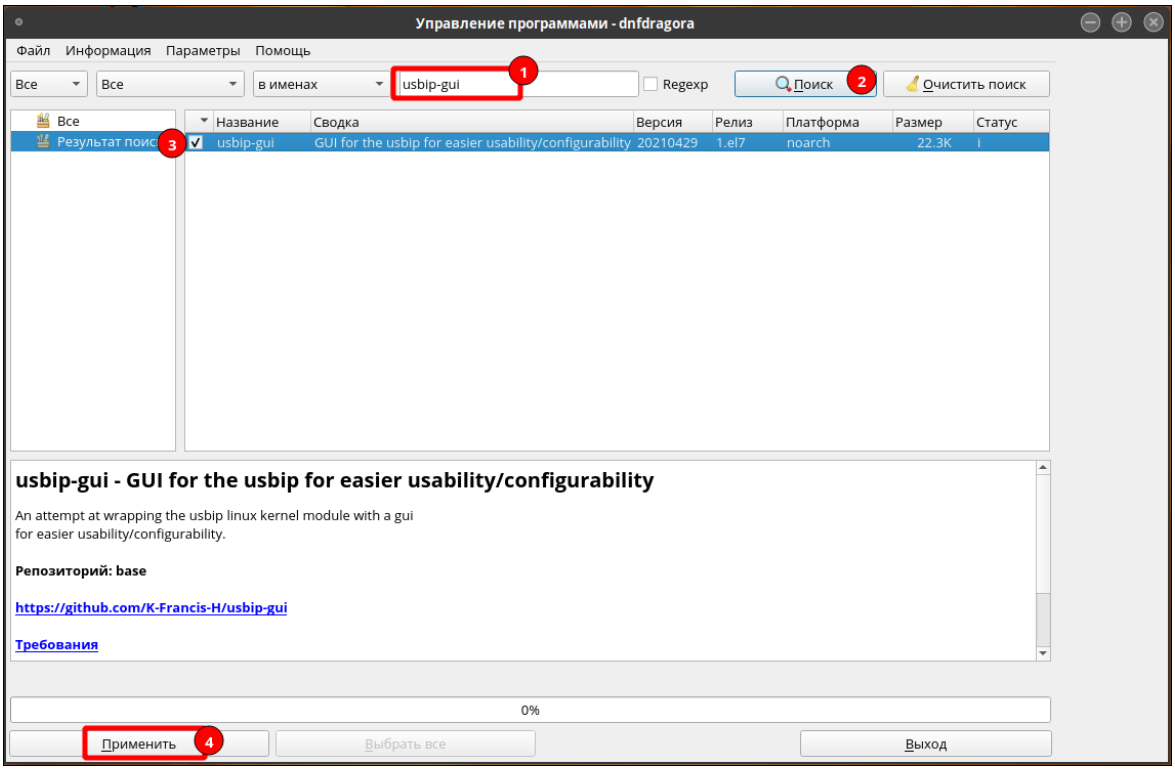
```
sudo usbip detach --port=0
```

Графическая утилита usbip-gui

В РЕД ОС также существует графическая утилита для предоставления в общий доступ USB-устройств через IP-сеть — **usbip-gui**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**usbip-gui**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.

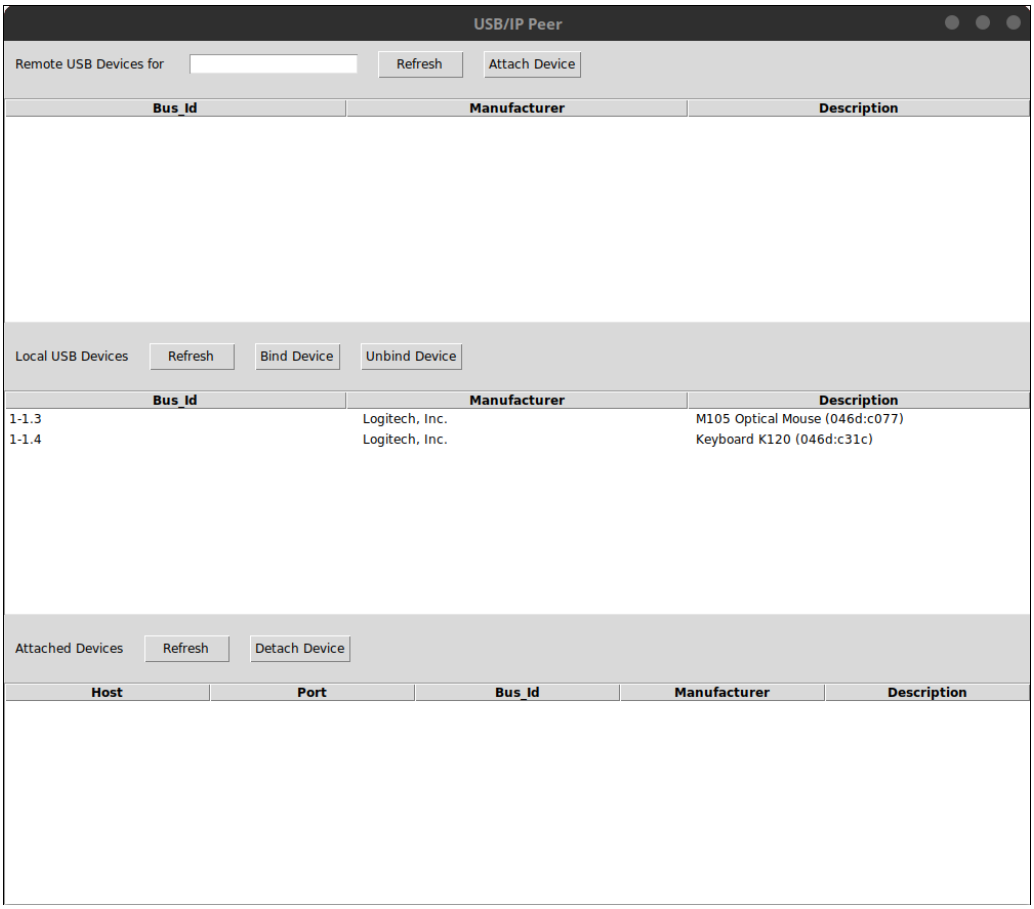


Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

```
sudo dnf install usbip-gui
```

После установки программа будет доступна из «**Главного меню**» — «**Администрирование**» — «**Управление USBIP**». Обратите

внимание, что для работы с программой необходимы права администратора или суперпользователя системы.



Установка драйвера Nvidia в РЕД ОС 7.3

Обновление ОС
Информация о видеокарте
Способ 1. Установка проприетарного драйвера Nvidia из репозитория
Способ 2. Установка драйвера Nvidia через run-файл
Переключение используемых видеокарт nVidia и Intel
Переключение видеокарт из терминала
Переключение видеокарт в графическом режиме
Переключение используемых видеокарт nVidia и Intel при использовании менеджера SDDM

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: Nvidia Driver 535

Поддержка видеокарт **Nvidia** в РЕД ОС по умолчанию осуществляется в виде драйвера **nouveau** с открытым исходным кодом. Если драйвер **nouveau** не удовлетворяет достаточным требованиям, например, в нем нет поддержки CUDA ядер, то пользователи могут установить официальный **проприетарный** драйвер **Nvidia.**

Вы можете подробнее ознакомиться с информацией по установке и настройке драйвера Nvidia, просмотрев наши обучающие видео:

- на **RuTube** — Установка видео-драйверов NVIDIA;
- в **Яндекс.Дзен** — Установка видео-драйверов NVIDIA;
- в **VK Видео** — Установка видео-драйверов NVIDIA.

На наших каналах вы также сможете найти много другой полезной информации.

Обновление ОС

ВАЖНО!

Перед установкой драйверов систему необходимо **обновить**!

Перед установкой драйвера NVIDIA убедитесь, что у вас подключен репозиторий **kernels6** (для *ядра* ОС версии *6.1.20* и выше) и установлены все последние обновления:

```
sudo -E dnf install redos-kernels6-release
sudo -E dnf update
```

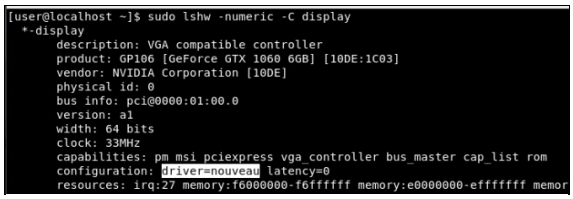
После установки обновлений необходимо перезагрузить ПК для завершения обновления.

Информация о видеокарте

С помощью утилиты **lshw** можно вывести информацию о видеокарте и об используемом видеодрайвере.

С правами администратора выполните команды:

```
sudo -E dnf install lshw
sudo -E lshw -numeric -C display
```



где **product** — модель видеокарты.

Прежде чем устанавливать драйвер, убедитесь, что он подходит для вашей видеокарты. Для этого выполните следующий алгоритм действий.

1. Перейдите на официальный сайт NVIDIA.
2. Выберите модель вашей видеокарты в разделе поиска драйверов.
3. Узнайте, какая версия драйвера поддерживается для вашей видеокарты.
4. Если ваша видеокарта является устаревшей, учтите, что первый способ может не сработать. В этом случае потребуется скачать драйвер из архива поддерживаемых устройств на сайте NVIDIA.

Способ 1. Установка проприетарного драйвера nVidia из репозитория

Для установки проприетарного драйвера **nVidia** из репозитория РЕД ОС выполните команду:

```
sudo -E dnf install nvidia-settings nvidia-kmod nvidia-persistenced nvidia-xconfig nvidia-modprobe xorg-x11-drv-nvidia xorg-x11-drv-nvidia-cuda-libs
```

На данном этапе установка завершена. Для применения изменений необходимо перезагрузить ПК.

После перезагрузки запустите в терминале утилиту inxi и убедитесь, что используется драйвер **nVidia**:

```
inxi -G
```

```
[root@wolandius-pc ~]# inxi -G
Graphics:  Device-1: NVIDIA TU117M [GeForce GTX 1650 Mobile / Max-Q] driver: nvidia v: 515.65.01
           Device-2: Advanced Micro Devices [AMD/ATI] Picasso driver: amdgpu v: kernel
           Device-3: IMC Networks USB2.0 HD UVC WebCam type: USB driver: uvcvideo
           Display: server: X.org 1.20.14 driver: amdgpu,ati,nvidia unloaded: fbdev,modesetting,nouveau,vesa tty: 211x50
           Message: Advanced graphics data unavailable in console for root.
```

ВАЖНО!

Если ранее в системе уже были установлены проприетарные драйверы, модули ядра или вносились какие-либо другие изменения, то перед этим необходимо обязательно вернуть все настройки к стандартным или выполнять установку драйверов на чистую систему для исключения возможных конфликтов и ошибок.

Способ 2. Установка драйвера nVidia через run-файл

Загрузка драйвера

Загрузите инсталлятор с официального сайта **nVidia** в виде бинарного файла с расширением **RUN**.

Список драйверов доступен по ссылке, здесь представлены как новые драйвера, так и архивные, которые поддерживают старые графические видеокарты.

В описании (вкладка **Supported Products**) к драйверу обратите внимание на наличие вашей модели видеокарты. Если в выбранном драйвере нет вашей модели, то перейдите в описание следующего драйвера. Также для загрузки нужного драйвера можно воспользоваться поиском по параметрам - https://www.nvidia.com/Download/index.aspx?lang=ru.

Отключение драйвера nouveau

Предварительно необходимо отключить используемый по умолчанию драйвер **nouveau**.

Для этого потребуется внести изменения в конфигурацию **grubby** с помощью команды:

```
sudo -E grubby --update-kernel ALL --args="nouveau.modeset=0"
```

Следует заметить, что на ПК, где используется только видеокарта NVIDIA, после перезагрузки будет отсутствовать изображение. Добавьте опцию загрузки в текстовом режиме:

```
sudo -E grubby --update-kernel ALL --args="3"
```

Перезагрузите систему.

Проверьте, что драйвер **nouveau** для **nVidia** с открытым исходным кодом больше не используется:

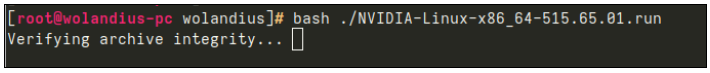
```
lshw -numeric -C display
```

```
[root@wolandius-pc ~]# lshw -numeric -C display
  *-display UNCLAIMED
       description: VGA compatible controller
       product: TU117M [GeForce GTX 1650 Mobile / Max-Q] [10DE:1F91]
       vendor: NVIDIA Corporation [10DE]
       physical id: 0
       bus info: pci@0000:01:00.0
       version: a1
       width: 64 bits
       clock: 33MHz
       capabilities: pm msi pciexpress vga_controller cap_list
       configuration: latency=0
       resources: memory:f6000000-f6ffffff memory:c0000000-cfffffff memory:d0000000-d1ffffff ioport:f000(size=128) memory:f7000000-f707ffff
```

Установка драйвера

Введите логин **root** и пароль. Перейдите в каталог с загруженным драйвером, установите дополнительные пакеты и выполните команду запуска установки:

```
cd /<путь_до_каталога_с_драйвером>sudo dnf install dkms gcc kernel-devel
bash ./NVIDIA-Linux-x86_64-*.run
```



Would you like to register the kernel module sources with DKMS? This will allow DKMS to automatically build a new module, if you install a different kernel later.

- **Yes**
- No



Install NVIDIA's 32-bit compatibility libraries?

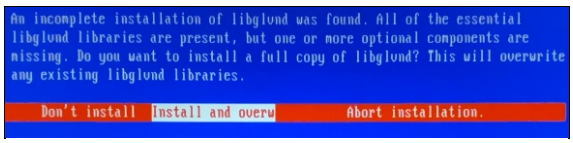
- **Yes**
- No



В случае возникновения диалогового окна выберите следующее действие:

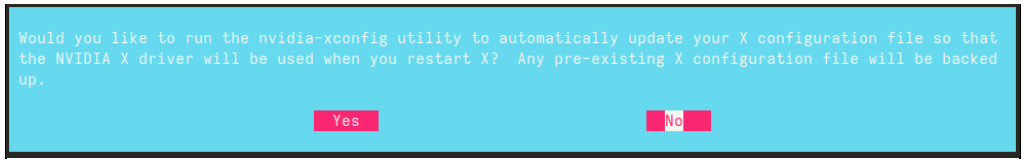
An incomplete installation of libglvnd was found. Do you want to install a full copy of libglvnd? This will overwrite any existing libglvnd libraries.

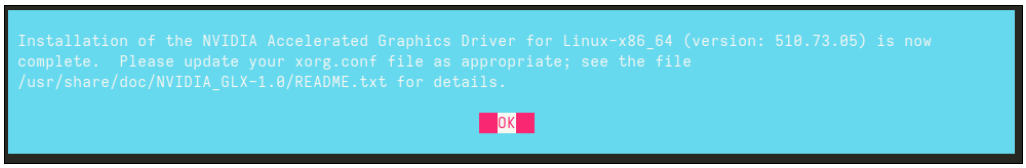
- Don't install libglvnd files
- **Install and overw.**
- Abort installation



Would you like to run the nvidia-xconfig utility to automatically update your X configuration file so that the NVIDIA X driver will be used when you restart X? Any pre-existing X configuration file will be backed up.

- Yes
- **No**





Далее отключите текстовый режим командой:

```
sudo -E grubby --update-kernel ALL --remove-args="3"
```

На данном этапе установка завершена, перезагрузите ПК. Запустите в терминале утилиту **inxi** и убедитесь, что используется драйвер **Nvidia**:

```
inxi -G
```

```
[root@wolandius-pc ~]# inxi -G
Graphics:  Device-1: NVIDIA TU117M [GeForce GTX 1650 Mobile / Max-Q] driver: nvidia v: 515.65.01
           Device-2: Advanced Micro Devices [AMD/ATI] Picasso driver: amdgpu v: kernel
           Device-3: IMC Networks USB2.0 HD UVC WebCam type: USB driver: uvcvideo
           Display: server: X.org 1.20.14 driver: amdgpu,ati,nvidia unloaded: fbdev,modesetting,nouveau,vesa tty: 211x50
           Message: Advanced graphics data unavailable in console for root.
```

Переключение используемых видеокарт nVidia и Intel

Для систем с двумя видео-адаптерами дополнительно разработан пакет **nvidia-primus**. Данный пакет содержит преднастроенные конфигурации и утилиты для переключения основного видео-контроллера и запуска программ на адаптере **nVidia**, если основным установлен видео-контроллер от **Intel**.

Вы можете подробнее ознакомиться с возможностями переключения основного видео-контроллера, просмотрев наши обучающие видео:

- на **RuTube**:
  - Переключение между видеокартами NVIDIA Intel. Проприетарные драйверы NVIDIA ;
  - Графическая утилита для переключения видеокарт Nvidia и Intel .
- в **Яндекс.Дзен**:
  - Переключение между видеокартами NVIDIA Intel. Проприетарные драйверы NVIDIA ;
  - Графическая утилита для переключения видеокарт Nvidia и Intel .
- в **VK Видео**:
  - Переключение между видеокартами NVIDIA Intel. Проприетарные драйверы NVIDIA ;
  - Графическая утилита для переключения видеокарт Nvidia и Intel .

На наших каналах вы также сможете найти много другой полезной информации.

Для установки пакета выполните команду (потребуются права администратора):

```
sudo dnf install nvidia-primus
```

После установки пакета автоматически запускаются службы **nvidia-hibernate.service**, **nvidia-resume.service**, **nvidia-suspend.service** (поставляются в пакете **xorg-x11-drv-nvidia**), необходимые для корректной работы соответствующих действий (*hibernate*, *resume* и *suspend*).

Перезагрузите систему для применения изменений.

Работа с утилитой возможна как из терминала, так и в графическом режиме.

Переключение видеокарт из терминала

Для переключения основного адаптера *из терминала* используется утилита **prime-select**.

Основные опции утилиты **prime-select**:

- `intel` — установить основным адаптер *Intel*;
- `nvidia` — установить основным адаптер *nVidia*;

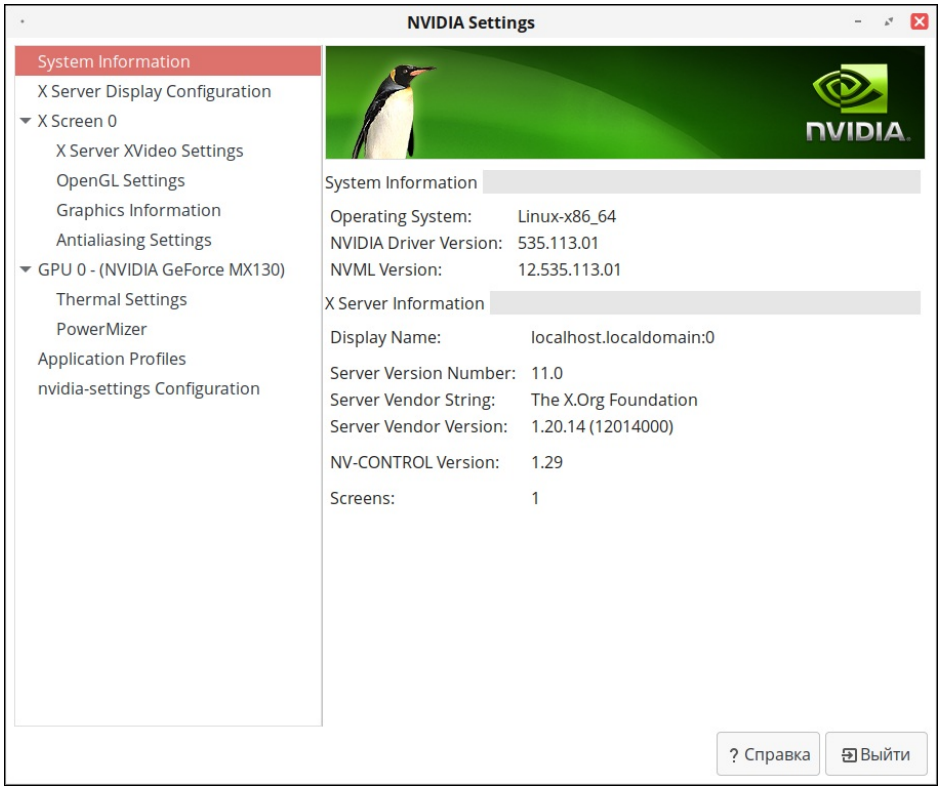
- `status` — показать текущий основной адаптер;
- `-h`, `--help` — вывод справки.

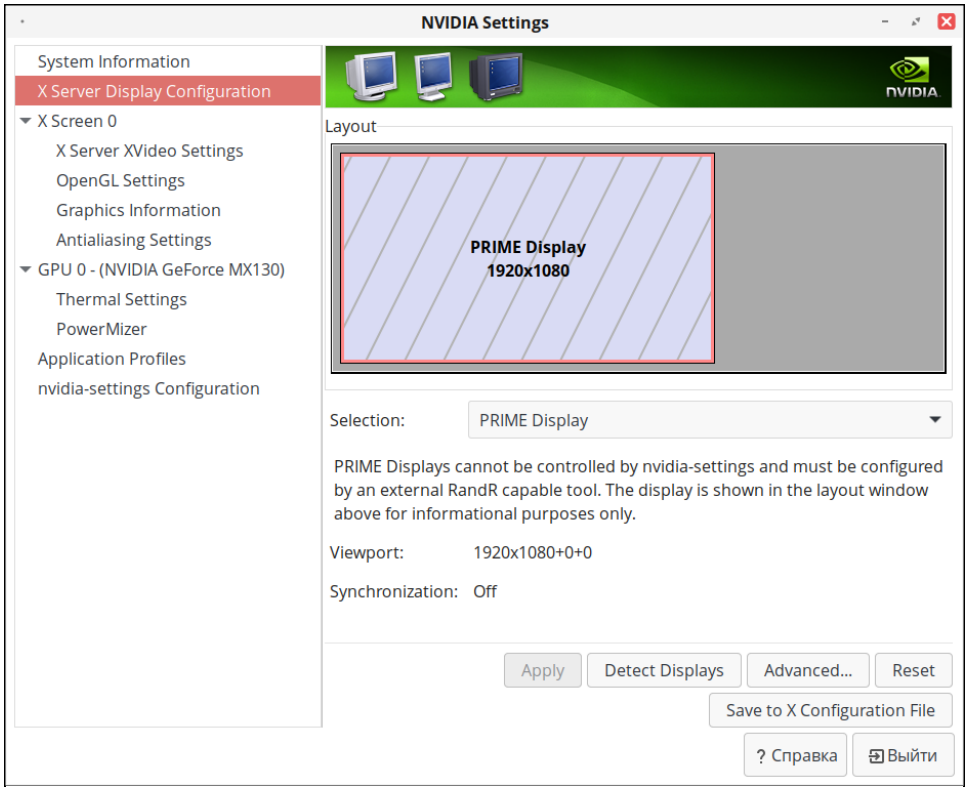
Просмотр текущего используемого видео-адаптера и вывод справки доступны без дополнительных привилегий. Для переключения видео-адаптера потребуются права **администратора** системы, например:

```
sudo prime-select nvidia
```

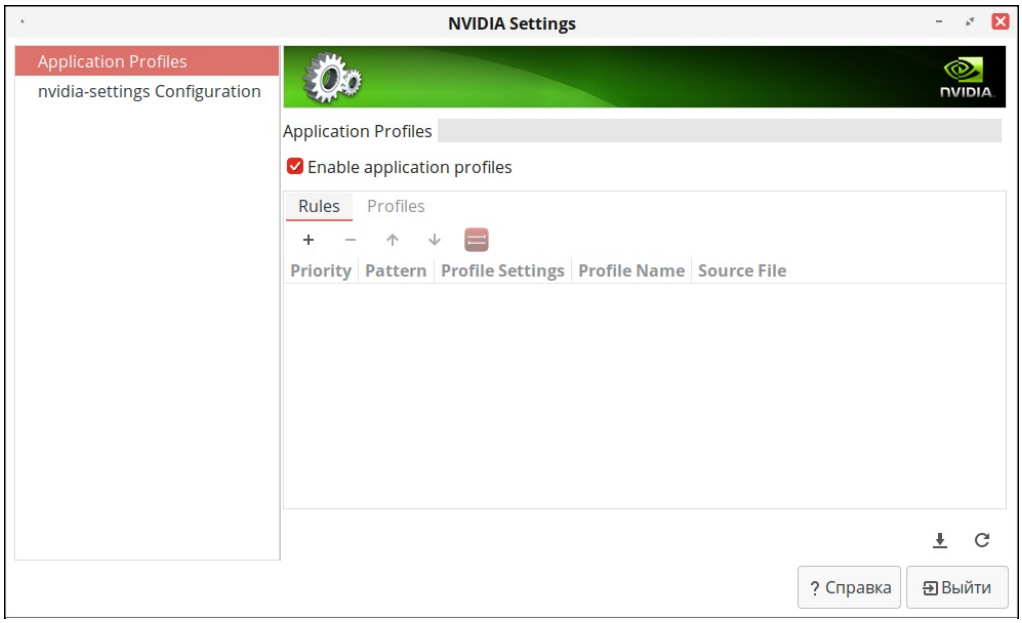
Для применения внесенных изменений потребуется перезагрузка системы.

Также, если основным видео-адаптером установлен **nVidia**, в утилите «**Параметры NVIDIA X Server**» будут доступны разделы по настройке оборудования и просмотр таких параметров, как *яркость*, *гамма*, *атрибуты XVideo*, *температура* и *функции OpenGL*.





В случае если основным видео-адаптером установлен **Intel**, в утилите будут доступны только разделы по настройке профилей приложений.

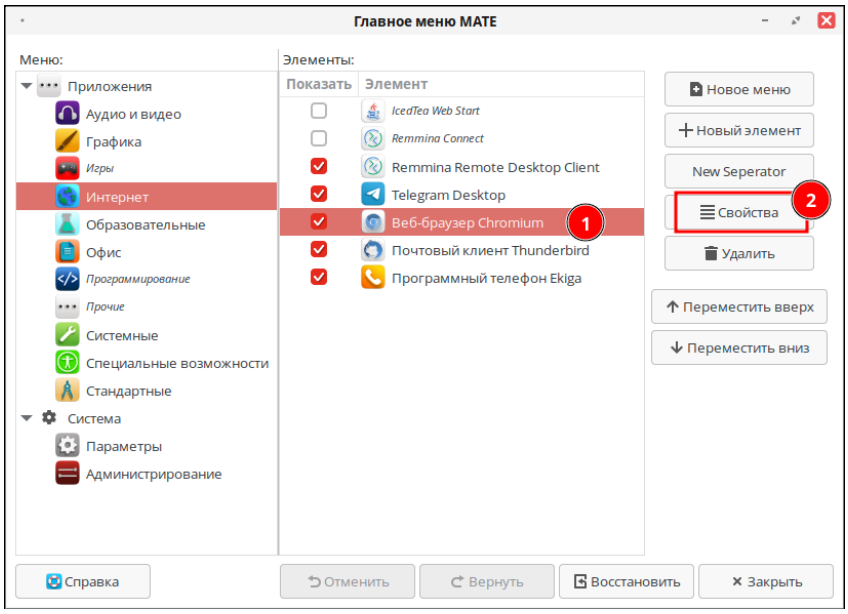


Бывают ситуации, когда в качестве основного видео-адаптера используется **Intel** (например, в ноутбуках для сохранения заряда батареи), но для запуска какой-либо программы необходим контроллер **nVidia**. Для этого можно использовать утилиту **prime-run** (входит в состав пакета **nvidia-primus**), передавая ей имя программы и все ее аргументы (если таковые имеются) в качестве опций. Например:

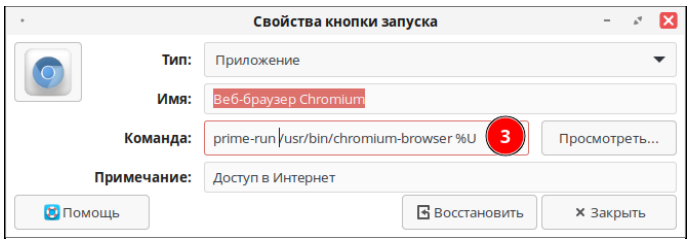
```
prime-run chromium-browser
```

Данный процесс можно упростить, изменив команду запуска непосредственно нужного приложения. Для этого нажмите ПКМ по **Главному меню**, в появившемся контекстном меню выберите «**Редактировать меню**». Будет открыто окно редактирования главного меню.

Далее найдите и выберите нужную программу, нажмите «**Свойства**».



В открывшемся окне «**Свойства кнопки запуска**» в поле **Команда** в начало строки допишите `prime run` и нажмите «**Закрыть**».



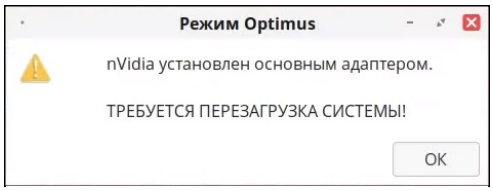
После этого выбранная программа всегда будет запускаться с использованием видео-адаптера **nVidia**.

Переключение видеокарт в графическом режиме

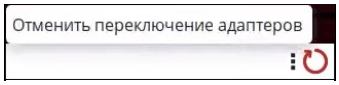
Переключение видео-адаптеров *в графическом режиме* производится с помощью появившейся в системном трее пиктограммы —  .

При нажатии ЛКМ по пиктограмме будет выведена информация об используемом видео-адаптере. Для смены видео-адаптера нажмите ПКМ по пиктограмме и в появившемся меню выберите «**Переключить на адаптер nVidia**».

После этого появится информационное сообщение о том, что видео-адаптер изменен, и требуется перезагрузка системы.



До перезагрузки системы по-прежнему будет использоваться видео-адаптер **Intel**, а смену адаптера можно отменить, нажав ЛКМ по изменившейся пиктограмме и выбрав «**Отменить переключение адаптеров**».



После перезагрузки системы, если смена адаптера не была отменена, будет активирован видеа-адаптер **nVidia**. Пиктограмма в системном трее также изменится —  .

Переключение используемых видеокарт nVidia и Intel при использовании менеджера SDDM

При использовании **SDDM** до перезагрузки системы (при переключении на **nVidia**) необходимо настроить конфигурирование вывода при запуске графической среды.

Запустите терминал и выполните команду:

```
xrandr --listproviders
```

Вывод должен содержать список из двух или более провайдеров (устройств). Наример:

```
xrandr --listproviders

Providers: number : 2
Provider 0: id: 0x221 cap: 0x9, Source Output, Sink Offload crtcs: 3 outputs: 6 associated providers: 0 name:modesetting
Provider 1: id: 0x1f8 cap: 0x0 crtcs: 0 outputs: 0 associated providers: 0 name:NVIDIA-G0
```

В данном примере провайдер с именем `modesetting` представлен адаптером с низкой производительностью, который обеспечивает вывод изображения на дисплей. Провайдер с именем `NVIDIA-G0` представлен более производительным устройством, которое будет выполнять основную нагрузку по формированию изображения для последующего вывода через провайдер `modesetting`. Для этого необходимо, чтобы провайдер `modesetting` обладал функцией **Sink Offload** (в примере подсвечено зеленым).

Откройте файл **/etc/sddm/Xsetup** на редактирование:

```
sudo nano /etc/sddm/Xsetup
```

Добавьте строки вида:

```
xrandr --setprovideroffloadsink <основной_провайдер> <провайдер_вывода>
 xrandr --auto
```

Замените следующие блоки на значения из списка провайдеров:

- `<основной_провайдер>` - порядковый номер, id или имя провайдера nVidia (в примере: 1, 0x1f8 или NVIDIA-G0);
- `<провайдер_вывода>` - порядковый номер, id или имя провайдера, обеспечивающего вывод изображения (в примере: 0, 0x221 или modesetting).

Рекомендуется указать имя провайдера или id. Пример:

```
xrandr --setprovideroffloadsink NVIDIA-G0 modesetting
```

```
xrandr --auto
```

Примечание.

Если указанные выше действия не были выполнены до перезагрузки и при загрузке ОС изображение не выводится, то переключитесь на использование **Intel**, выполнив следующие шаги:

1. После загрузки ОС (логотип загрузки исчез) нажмите сочетание клавиш *Ctrl+Alt+F3*.

2. Введите имя пользователя и пароль, подтверждая ввод нажатием *Enter*.

3. Выполните команды:

```
sudo prime-select intel
reboot
```

Установка драйвера AMDGPU

Загрузка драйвера
Предварительная подготовка
Установка драйвера

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: amdgpu-22.20

Одной из актуальных проблем любой ОС является настройка корректной и максимально производительной работы видеокарты.

Для поддержки аппаратного ускорения и для устранения низкого разрешения экрана монитора на компьютерах с интегрированной графикой **AMD** (**Radeon Vega**) в таких процессорах как:

- • AMD Ryzen 3500U;
- • AMD Athlon PRO 300GE;
- • Ryzen 3 3200G;
- • AMD athlon 220ge и других,

рекомендуется устанавливать **ядро Linux версии 5.15** и выше, которое присутствует в репозитории РЕД ОС. Но для некоторых видеоядер **AMD** этого не достаточно, в таком случае необходима установка драйвера **amdgpu-pro**.

Вы можете подробнее ознакомиться с информацией по установке драйвера AMDGPU, просмотрев наши обучающие видео:

- на **RuTube** — Установка проприетарных видео-драйверов AMD;
- в **Яндекс.Дзен** — Установка проприетарных видео-драйверов AMD;
- в **VK Видео** — Установка проприетарных видео-драйверов AMD.

На наших каналах вы также сможете найти много другой полезной информации.

Загрузка драйвера

Для загрузки необходимого драйвера перейдите на официальный сайт AMD и скачайте репозиторий для видеокарты.

Предварительная подготовка

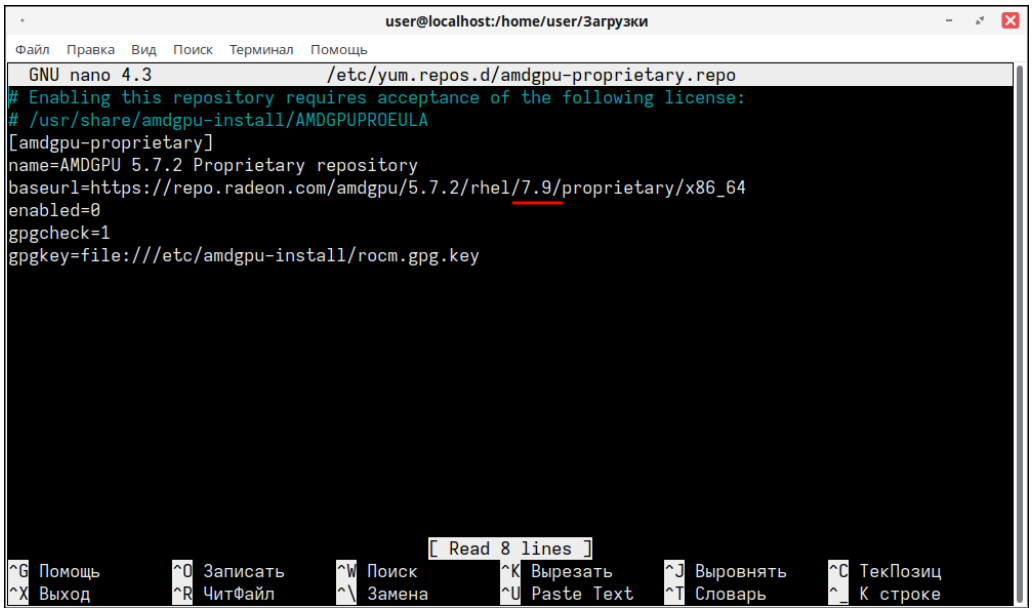
Перед установкой драйвера необходимо выполнить предварительную настройку. Для этого перейдите в каталог со скачанным репозиторием (в примере **/home/user/Загрузки/**) и подключите его следующей командой (потребуются права администратора системы или суперпользователя **root**):

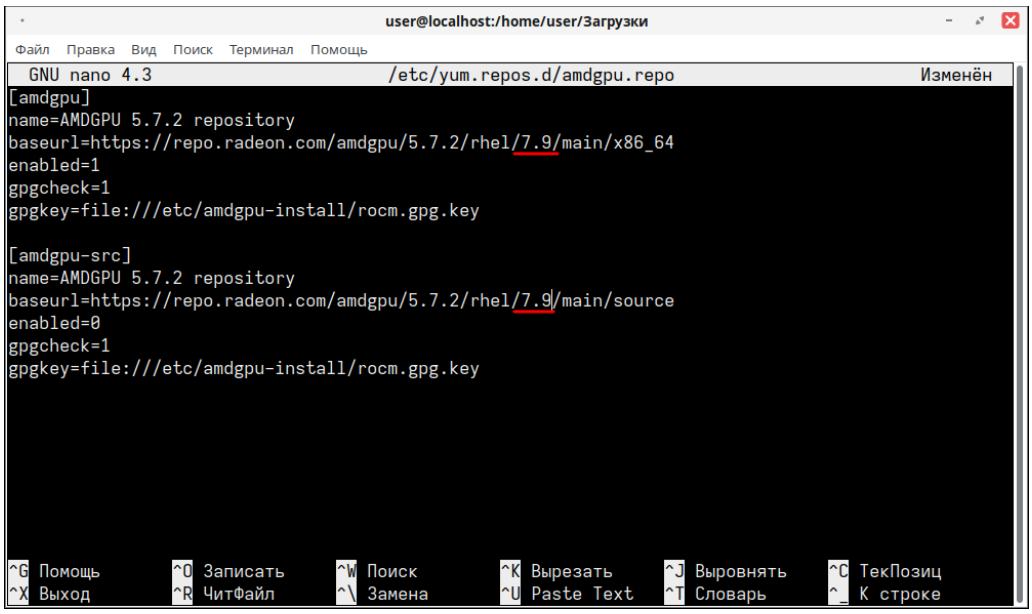
```
cd /home/user/Загрузки/
dnf install ./amdgpu-install-22.20.50200-1.el7.noarch.rpm
```

После этого необходимо отредактировать файлы с описанием репозитория.

В файлах **/etc/yum.repos.d/amdgpu-proprietary.repo** и **/etc/yum.repos.d/amdgpu.repo** замените `$amdgpudistro` на `7.9`:

```
sed -i 's/$amdgpudistro/7.9/g' /etc/yum.repos.d/amdgpu.repo /etc/yum.repos.d/amdgpu-proprietary.repo
```

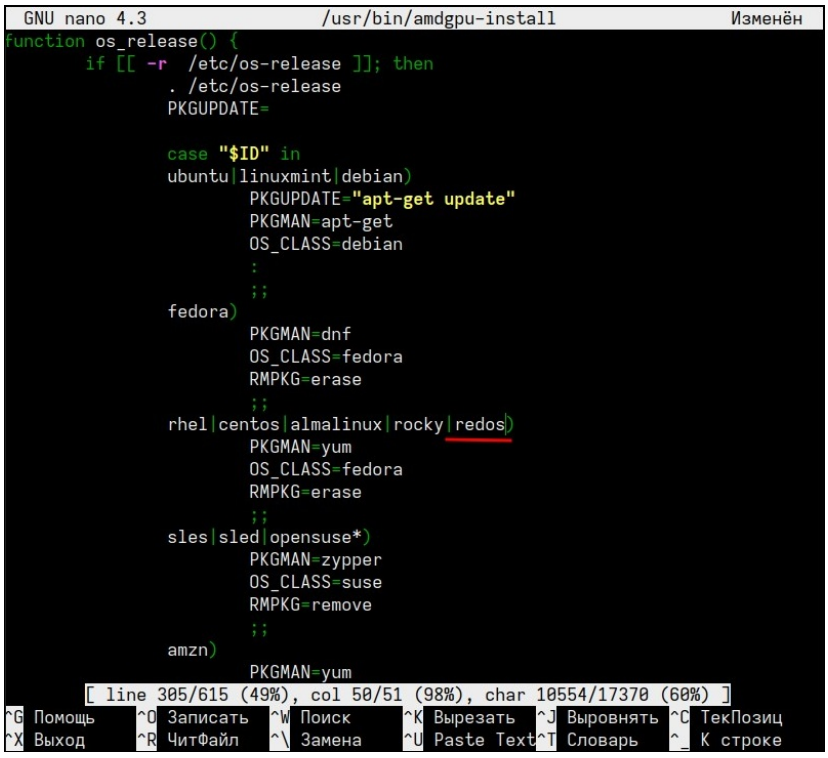




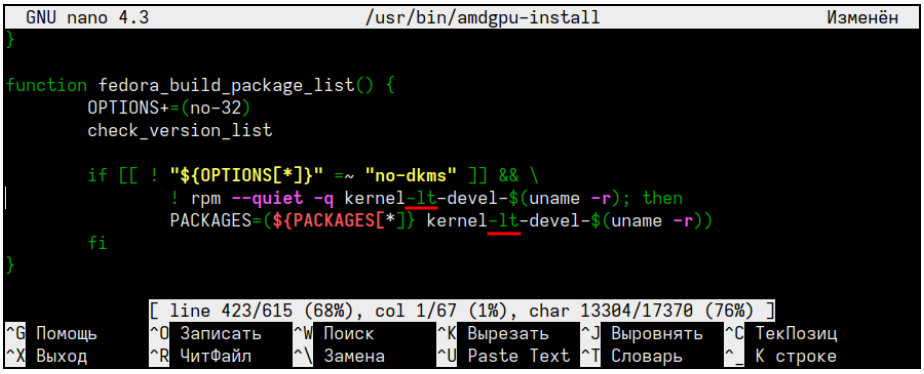
Также необходимо внести изменения в установочный скрипт. Для этого откройте файл **/usr/bin/amdgpu-install**:

```
nano /usr/bin/amdgpu-install
```

В строке **305** замените `rhel|centos|almalinux|rocky` на `rhel|centos|almalinux|rocky|`**`redos`**.



В строке **423-424** замените kernel-devel на **kernel-lt-devel**.



Также внести вышеуказанные изменения можно следующими командами:

```
sed -i 's/rhel|centos|almalinux|rocky/rhel|centos|almalinux|rocky|redos/g' /usr/bin/amdgpu-install
sed -i 's/kernel-devel/kernel-lt-devel/g' /usr/bin/amdgpu-install
```

Установка драйвера

После предварительной настройки можно переходить к непосредственной установке драйвера. Для этого выполните команду (потребуются права администратора или суперпользователя **root**):

```
amdgpu-install
```

После установки драйвера перезагрузите систему. Если система загрузилась и разрешение экрана соответствует требуемому, а также в выводе команды:

```
inxi -G
```

определен драйвер **amdgpu**, то можно считать, что драйвер для встроенной графики **AMD** был успешно установлен.

Envycontrol - утилита для переключения режимов графического процессора

Установка
Синтаксис
Опции
Режимы работы
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: python3-envycontrol-3.4.0

Установка

Для установки утилиты через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install python3-envycontrol
```

Дальнейшая работа с утилитой производится с правами администратора.

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
envycontrol [--help] [--version] [-q] [-s режим] [--dm менеджер_режима] [--force-comp] [--coolbits [значение]] [--rtd3 [значение]] [--reset-sddm] [--reset] [--verbose]
```

Опции

Основные опции утилиты:

- **-h, --help** – выводит справку о доступных опциях утилиты;
- **-v, --version** - выводит версию утилиты **envycontrol**;
- **-q, --query** - возвращает текущий режим графики;
- **-s [режим], --switch [режим]** – переключает режим графики: **integrated** (интегрированный), **hybrid** (гибридный), **nvidia**;
- **--dm менеджер_режима** – позволяет вручную указать менеджер отображения для режима **nvidia**: gdm, gdm3, sddm, lightdm;
- **--force-comp** - включает ForceCompositionPipeline в режиме **nvidia**;
- **--coolbits [значение]** - включает Coolbits в режиме **nvidia** (по умолчанию: 28);
- **--rtd3 [значение]** - настраивает управление питанием PCI-Express Runtime D3 (RTD3) в режиме **hybrid**: 0, 1, 2, 3 (по умолчанию: 2);
- **--use-nvidia-current** - использует **nvidia-current** вместо **nvidia** для модулей ядра;
- **--reset-sddm** - восстанавливает исходный файл настройки Xsetup;
- **--reset** - отменяет изменения, внесенные **envycontrol**;
- **--cache-create** - создает кеш, используемый **envycontrol** (работает только в режиме **hybrid)**;
- **--cache-delete** - удаляет созданный кеш **envycontrol**;
- **--cache-query** - показывает созданный кеш **envycontrol**;
- **--verbose** - включает подробный режим вывода информации.

Режимы работы

EnvyControl предоставляет возможность выбора режима работы графики:

1 . **Гибридный режим** - позволяет драйверу автоматически определять, какой графический процессор использовать, обычно предпочитая интегрированную графику и активируя режим NVIDIA только при необходимости. Производительность на внешних экранах может быть снижена.

2 . **Интегрированный режим** - использует только интегрированную графику (Intel или AMD iGPU), отключая работу с видеокартой NVIDIA для снижения энергопотребления. Мониторы, подключенные к NVIDIA dGPU, не будут использоваться.

3 . **Режим NVIDIA** - обеспечивает использование видеокарты от NVIDIA, игнорируя интегрированную графику. Более высокая графическая производительность и более высокое энергопотребление.

Примеры использования

1. Для установки интегрированного графического режима:

```
sudo envycontrol -s integrated
```

2. Для установки гибридного графического режима и включения детального регулирования мощности:

```
sudo envycontrol -s hybrid --rtd3
```

3. Для установки графического режима nvidia и включения ForceCompositionPipeline и Coolbits со значением 24:

```
sudo envycontrol -s nvidia --force-comp --coolbits 24
```

4. Для установки графического режима nvidia и для настройки **lightdm**:

```
sudo envycontrol -s nvidia --dm lightdm
```

5. Для проверки текущего графического режима:

```
envycontrol --query
```

6. Для включения подробного режима вывода информации:

```
sudo envycontrol --verbose
```

7. Для отмены изменений, внесенных **envycontrol**:

```
sudo envycontrol --reset
```

Установка и настройка NUT

Установка пакетов и запуск утилиты
Конфигурационные файлы
Завершение работы системы
Графическая утилита мониторинга и управления ИБП

NUT (Network UPS Tools) — это набор утилит, который предоставляет поддержку для управления источниками бесперебойного питания (**ИБП**) в сетевом окружении. **NUT** позволяет мониторить состояние **ИБП**, управлять ими и автоматизировать действия, основанные на их состоянии.

NUT состоит из следующих основных частей:

- **драйверы** — используются для связи с **ИБП**;
- **сервер (upsd)** — основной процесс, который собирает данные от **ИБП** через драйверы;
- **служба мониторинга (upsmon)** — следит за состоянием сервера и выполняет определенные действия в зависимости от получаемых от него данных.

ВАЖНО!

Обязательно подключите физическое оборудование вашей сети (коммутаторы, маршрутизаторы, мосты и т. д.) к ИБП!

Установка пакетов и запуск утилиты

Откройте консоль и выполните команду (потребуются права **администратора**):

```
sudo dnf install nut nut-client nut-cgi nut-xml nut-devel
```

Для запуска и добавления сервисов в автозагрузку выполните (потребуются права **администратора**):

```
sudo systemctl --now enable nut-driver nut-server nut-monitor
```

Конфигурационные файлы

Конфигурационные файлы по умолчанию расположены в папке **/etc/ups** с доступом только для администратора. В каждом файле приведено подробное описание по настройке, неактивные строки закомментированы при помощи `#`.

Настройки для коммуникации с ИБП содержатся в файле **ups.conf**. Для редактирования откройте файл (потребуются права **администратора**):

```
sudo nano /etc/ups/ups.conf
```

Пример содержимого файла конфигурации:

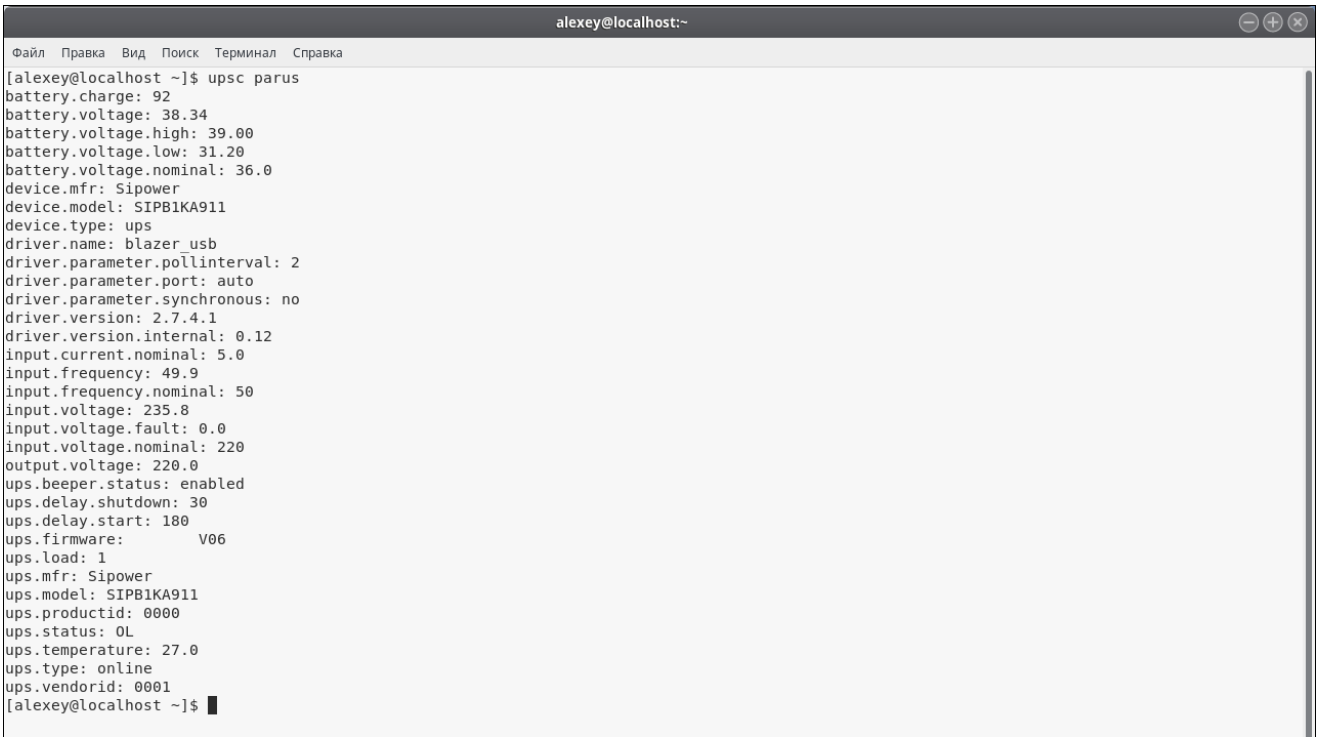
```
[parus]
driver = blazer_usb
port = auto
desc = "UPS Parus-Electro"
```

где:

- `parus` - название ИБП в системе;
- `blazer_usb` - драйвер для ИБП с протоколом Megatec, подключаемый по USB (можно установить другой драйвер соответствующий протоколу используемого ИБП).

При изменении названия ИБП необходимо внести соответствующее изменение в файл **upsmon.conf**.

Для проверки обмена данными с ИБП можно запустить команду `upsc <название ИБП>`. Если соединение с ИБП установлено, будут выданы данные от ИБП `parus`:



Завершение работы системы

Настройки процедуры завершения работы системы при низком заряде батарей ИБП приведены в файле **upsmon.conf**.

По умолчанию система настроена на завершение работы:

```
SHUTDOWNCMD "/sbin/shutdown –h +0"
```

но можно заменить на гибернацию:

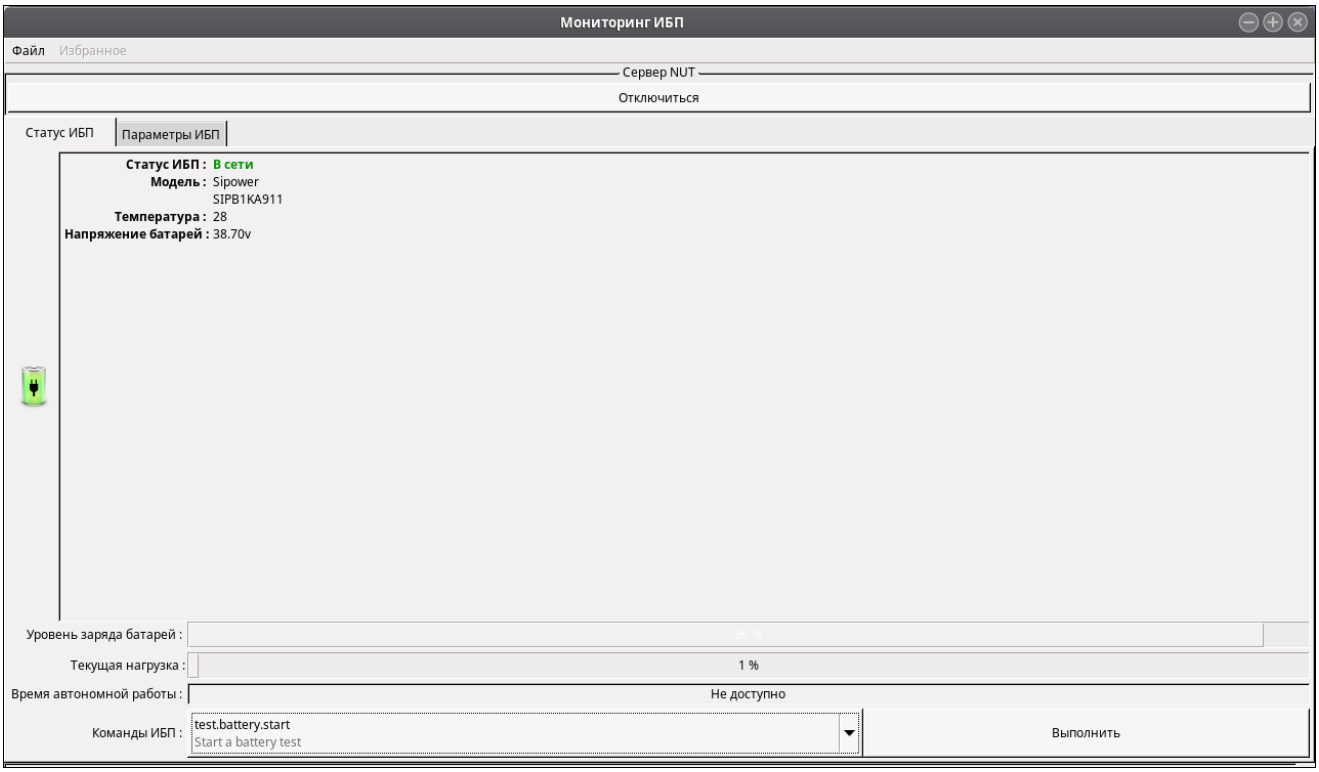
```
SHUTDOWNCMD "/usr/bin/systemctl hibernate"
```

Для выполнения гибернации нужен раздел или файл подкачки необходимого размера, чтобы в него смог уместиться нативный или сжатый образ оперативной памяти. ОС автоматически подстроит параметры виртуальной памяти под сохранение данных при переходе компьютера в данный режим.

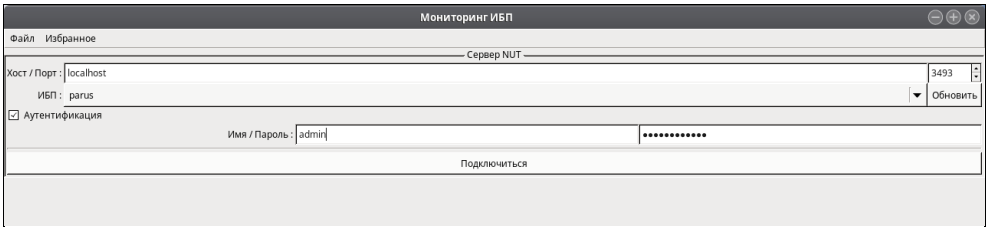
Графическая утилита мониторинга и управления ИБП

Графическая утилита **nut-monitor** позволяет просматривать параметры ИБП и электросети, а также отправлять команды. Запустить ее можно из терминала:

```
nut-monitor
```



Для отправки команд отключите утилиту от ИБП и выполните повторное подключение с пользователем, указанным в конфигурационном файле **upsd.users**. По умолчанию пользователь admin, пароль NUTadminPASSW.



PowerTOP - утилита управления питанием

Обзор
Применение параметров
Формирование отчета

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: powertop-2.9-3

PowerTOP — программа диагностики проблем, связанных с энергопотреблением, предоставляет оценку общего энергопотребления системы, а также индивидуального энергопотребления для каждого процесса, устройства, рабочего ядра, таймера и обработчика прерываний.

Для установки **powertop** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install powertop
```

Работа в программе производится через терминал с правами администратора системы или суперпользователя **root**.

Запуск программы осуществляется командой:

```
powertop
```

Примечание.

Программу следует запускать, когда ноутбук работает от аккумулятора.

Перед использованием программы необходимо откалибровать механизм оценки энергопотребления, выполнив следующую команду:

```
powertop --calibrate
```

Примечание.

Во время калибровки происходит смена яркости экрана и отключение сетевых интерфейсов.

Обзор

Интерфейс утилиты представлен в виде нескольких вкладок:

- *Overview*;
- *Idle stats*;
- *Frequency stats*;
- *Device stats*;
- *Tunables*.

На вкладке **Overview** отображается список компонентов, которые либо чаще всего отправляют сигналы пробуждения на центральный процессор, либо потребляют больше всего энергии.

Вкладка **Idle stats** показывает состояния питания для всех процессоров и ядер.

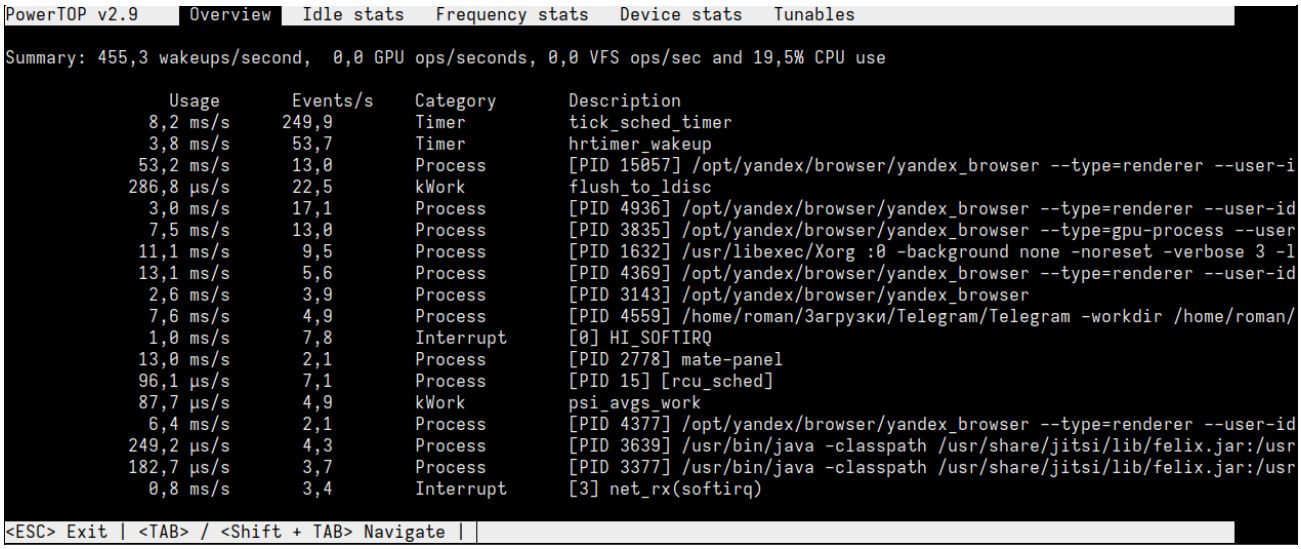
Вкладка **Frequency stats** показывает состояния производительности, включая турборежим (если применимо) для всех процессоров и

ядер.

На вкладке **Device stats** представлена информация, аналогичная вкладке **Overview**, но для устройств.

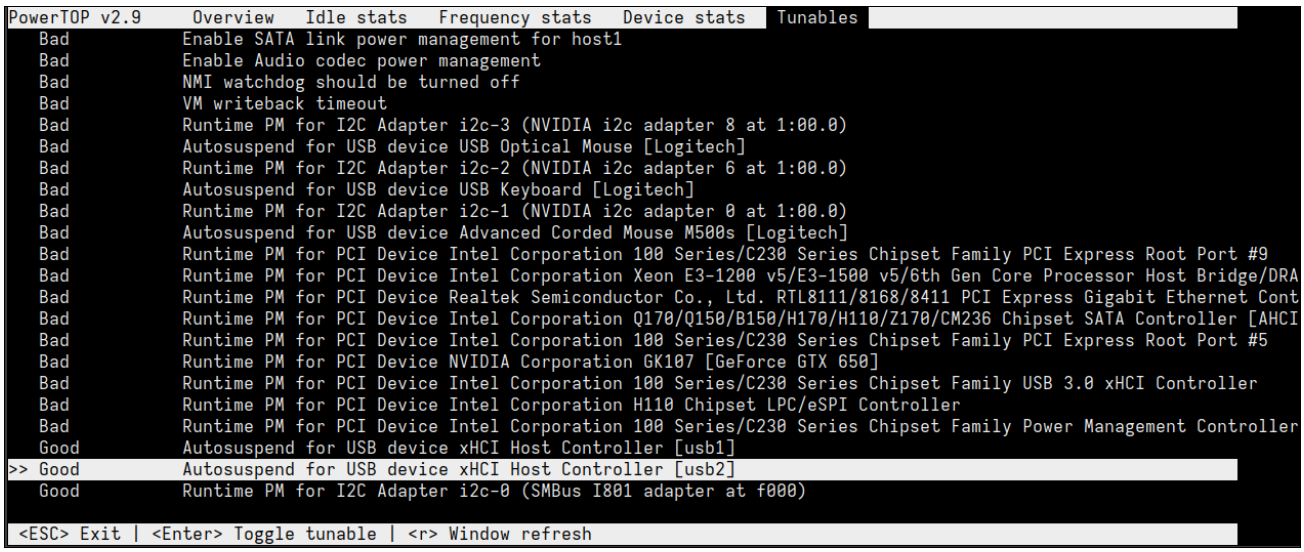
Вкладка **Tunables** содержит предложения **PowerTOP** по оптимизации системы для снижения энергопотребления.

Для переключения между вкладками используйте клавиши **TAB** и **Shift+TAB**, для перемещения по пунктам меню — клавиши **Up** и **Down**, для включения или выключения рекомендуемого параметра — **Enter**.



Применение параметров

Изменение параметров можно производить вручную через вкладку **Tunables**. Устройства, имеющие статус «*Bad*» рекомендуется оптимизировать, нажав клавишу **Enter**. Устройства со статусом «*Good*» работают в оптимальном режиме.



Для применения всех рекомендуемых настроек выполните:

```
powertop --auto-tune
```

Для сохранения установленных параметров необходимо запустить утилиту как службу командой:

```
systemctl start powertop.service
```

Данные настройки действительны до перезагрузки системы. Для автоматического применения рекомендуемых настроек при старте системы необходимо добавить службу **powertop** в автозагрузку. Для этого выполните команду:

```
systemctl enable powertop.service
```

Формирование отчета

Powertop позволяет сформировать отчет в форматах **html** и **csv**.

Для формирования отчета в **html** выполните команду:

```
powertop --html=namereport.html
```

Для формирования отчета в **csv** выполните команду:

```
powertop --csv=namereport.csv
```

TLP и TLPUI — утилиты для управления питанием

Установка TLP, TLP-RDW, TLPUI
Работа в графическом интерфейсе
Запуск TLPUI
Основные возможности утилиты TLPUI
Смена языка интерфейса
Описание интерфейса TLPUI
Работа в терминале
Синтаксис TLP
Команды TLP
Параметры TLP
Примеры использования утилиты
TLP-RDW

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tlp-1.5.0-4, tlp-rdw-1.5.0-4, tlpui-1.5.0-5

TLP и **TLPUI** — это утилиты для управления питанием, которые позволяют значительно улучшить энергопотребление и увеличить время автономной работы устройств.

TLP обеспечивает широкий спектр функций для настройки различных компонентов системы, включая процессор, жесткие диски, беспроводные и сетевые устройства, а также графические и звуковые компоненты. Хотя **TLP** предлагает множество опций для настройки, его использование может быть сложным для обычных пользователей, так как требует работы с командной строкой.

TLPUI предоставляет удобный графический интерфейс для **TLP**, упрощая процесс настройки параметров и избавляя пользователей от необходимости вручную редактировать конфигурационные файлы.

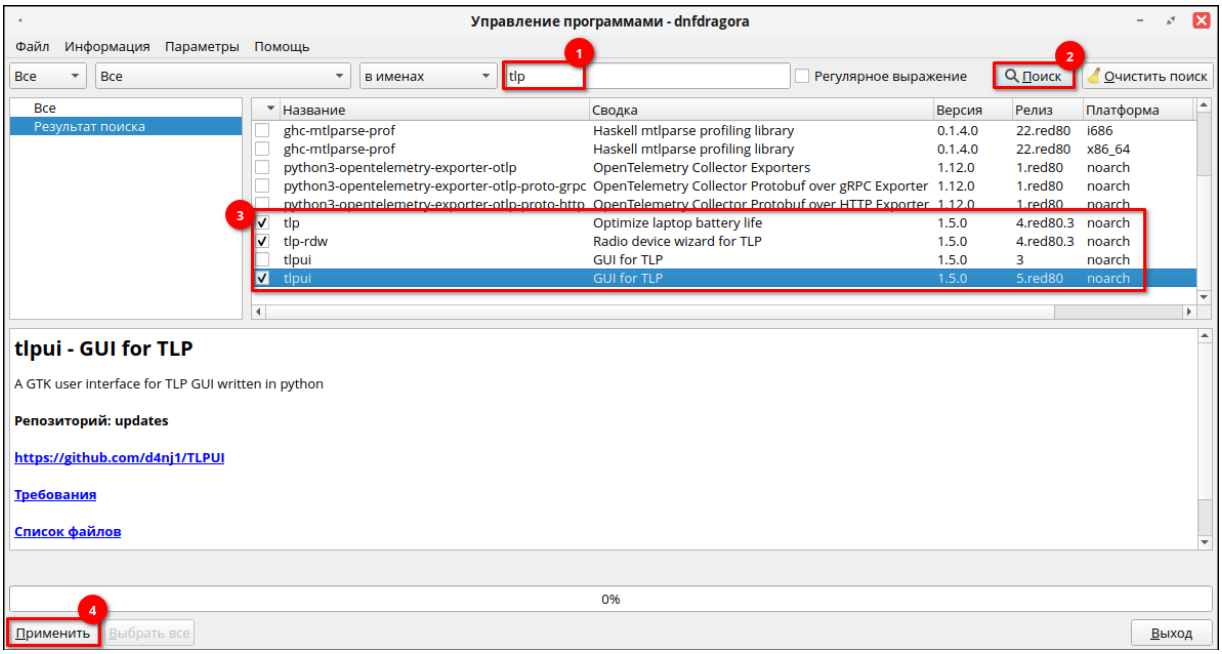
Установка TLP, TLP-RDW, TLPUI

Прежде чем запустить интерфейс **tlpui**, сначала установите необходимые пакеты. Пакеты **tlp** доступны в официальном репозитории РЕД ОС:

- **tlp** – пакет для оптимизации управления энергопотреблением;
- **tlp-rdw** (необязательный) – пакет для управления беспроводными устройствами в **tlp**;
- **tlpui** – графический интерфейс утилиты командной строки **tlp**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимых пакетов по ключевому слову «**tlp**» и отметьте флагом пакеты последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



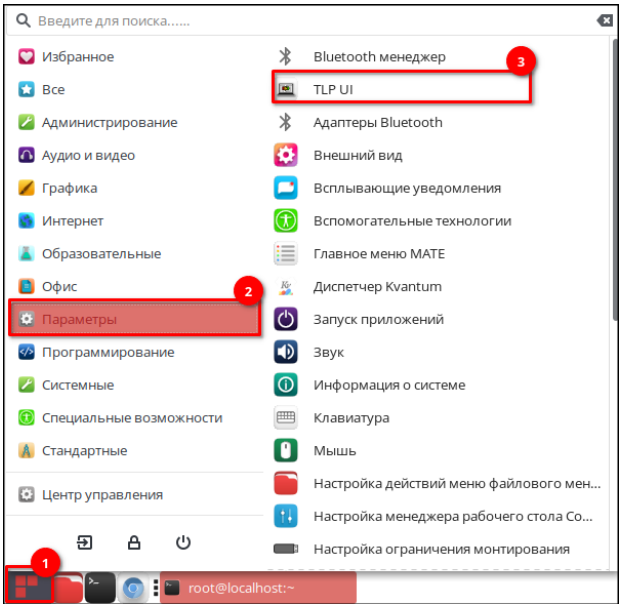
Для установки tlp, tlp-rdw, tlpui через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install tlp tlp-rdw tlpui
```

Работа в графическом интерфейсе

Запуск TLPUI

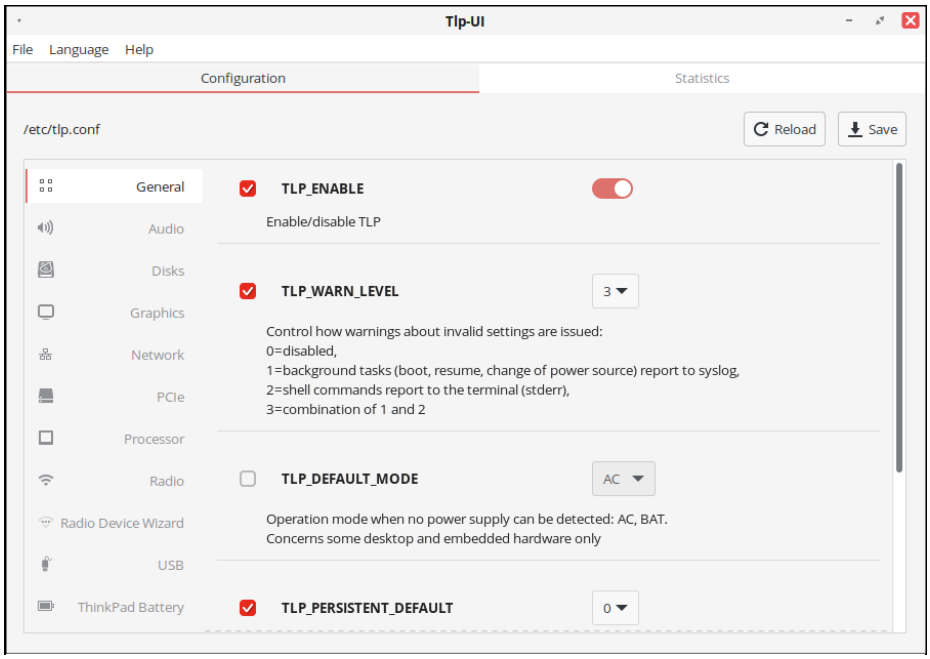
После установки запуск программы доступен из «**Главного меню**» — «**Параметры**» — «**TLP UI**».



Для запуска **tlpui** через терминал введите команду:

```
tlpui
```

Главное окно утилиты выглядит следующим образом:



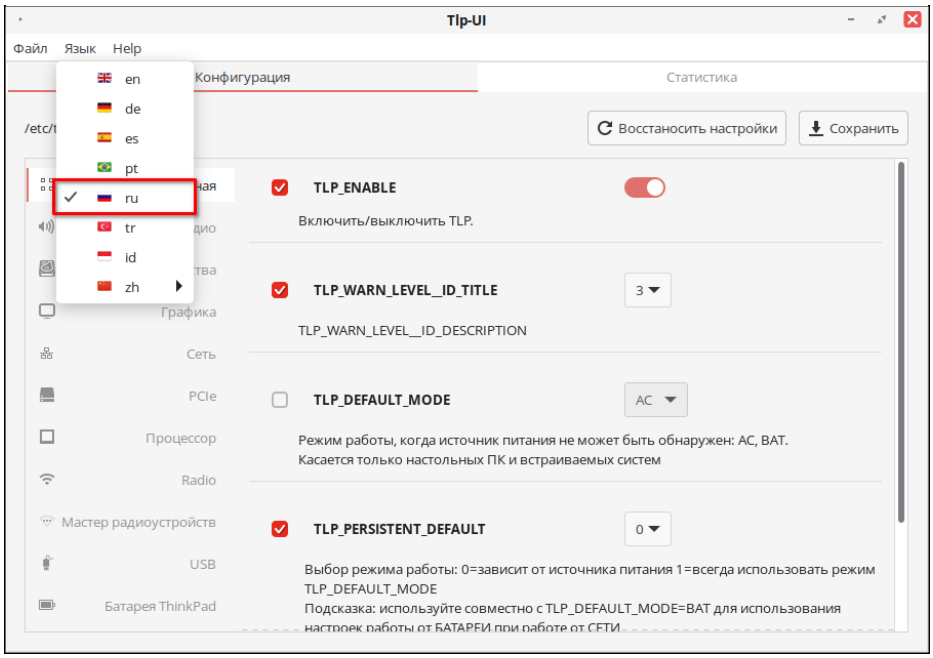
Основные возможности утилиты TLPUI

Основные возможности утилиты **tlpui** включают:

- **графический интерфейс** — обеспечивает удобный доступ к настройкам tlp без необходимости редактирования конфигурационных файлов вручную;
- **настройку параметров процессора** — позволяет регулировать параметры энергосбережения и производительности процессора;
- **управление жесткими дисками** — настройка параметров энергопотребления и производительности для жестких дисков;
- **конфигурацию беспроводных устройств** — позволяет настраивать параметры энергопотребления для Wi-Fi и других беспроводных компонентов;
- **управление сетевыми устройствами** — настройка параметров энергосбережения для сетевых карт и интерфейсов;
- **оптимизацию графических устройств**— позволяет регулировать энергопотребление графических карт;
- **настройку звуковых устройств** — возможность управления параметрами энергопотребления звуковых карт;
- **гибкость конфигурации** — возможность создания и применения различных настроек для различных сценариев использования;
- **мониторинг состояния** — предоставляет информацию о текущем состоянии энергопотребления и параметрах системы.

Смена языка интерфейса

Для смены языка приложения перейдите в меню «**Language**» и в выпадающем списке выберите необходимый язык (в примере выбран русский):



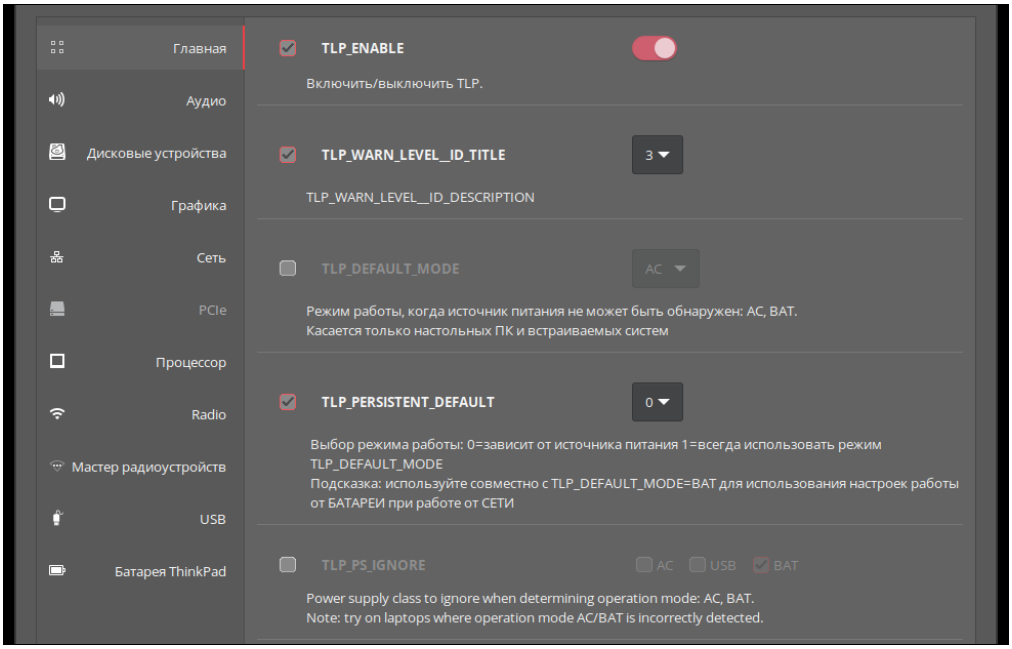
Описание интерфейса TLPUI

Интерфейс **tlpui** состоит из нескольких основных компонентов, которые предоставляют доступ к различным настройкам и параметрам энергосбережения.

Вкладка «Конфигурация»

Главная

На вкладке «**Главная**» интерфейса **tlpui** отображаются основные параметры конфигурации **tlp**, такие как включение/выключение **tlp**, управление предупреждениями, выбор режима работы по умолчанию и игнорирование определённых источников питания.



Параметры:

1. **TLP_ENABLE** — включение/выключение TLP. По умолчанию параметр активен. Для отключения переведите ползунок в положение «выключено». Для применения изменений потребуется перезагрузка.

2. **TLP_WARN_LEVEL_ID_TITLE** — управляет выводом предупреждений о недопустимых настройках.

Возможные значения:

- **0** — отключено;
- **1** — фоновые задачи (загрузка, возобновление работы, смена источника питания) отправляются в системный журнал;
- **2** — команды оболочки сообщают терминалу (stderr);
- **3** — комбинация 1 и 2 (устанавливается по умолчанию).

3. **TLP_DEFAULT_MODE** — определяет режим работы TLP по умолчанию на случай, если источник питания не может быть обнаружен.

Возможные значения:

- **AC** — режим работы от сети;
- **BAT** — режим работы от батареи.

4. **TLP_PERSISTENT_DEFAULT** — выбор режима работы.

Возможные значения:

- **0** — применить настройки в соответствии с фактическим источником питания (по умолчанию);
- **1** — всегда использовать настройки для TLP_DEFAULT_MODE.

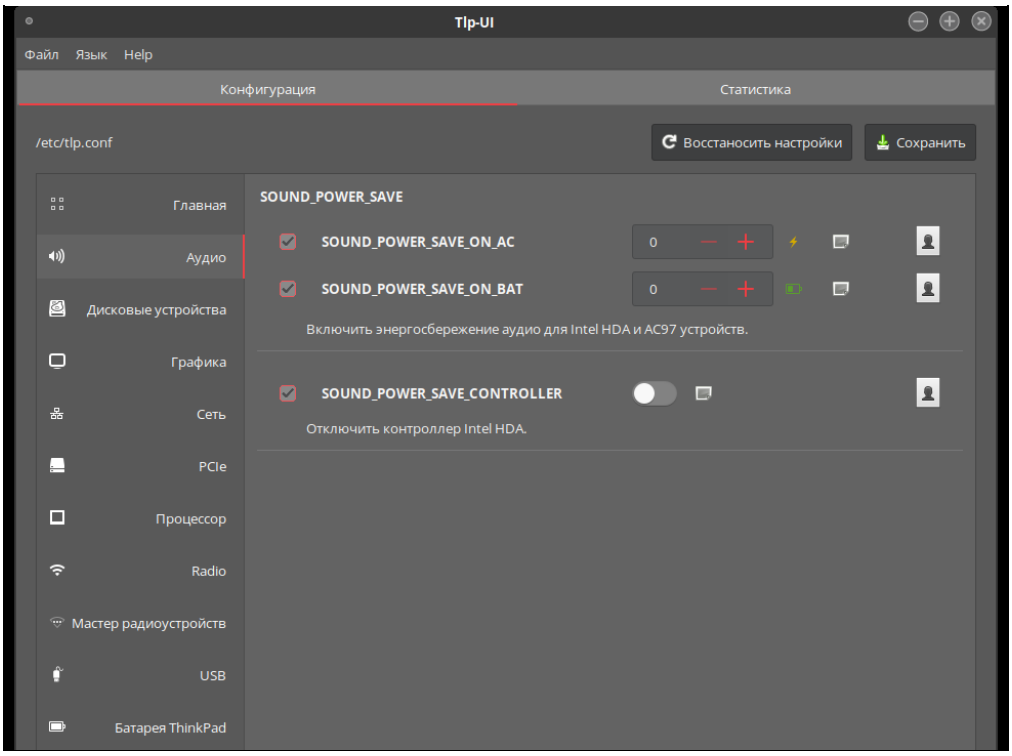
5. **TLP_PS_IGNORE** — класс(ы) источника питания, которые следует игнорировать при определении режима работы.

Возможные значения:

- **AC** — игнорировать сетевой адаптер;
- **BAT** — игнорировать батарею;
- **USB** — игнорировать USB-питание (только для версии 1.4 и выше).

Аудио

Вкладка «**Аудио**» в интерфейсе tlpui позволяет пользователям настроить параметры энергосбережения для звукового оборудования, такие как время ожидания для перехода в режим энергосбережения и выключение звукового контроллера. Эти настройки помогают оптимизировать энергопотребление аудиооборудования на устройстве.



Параметры:

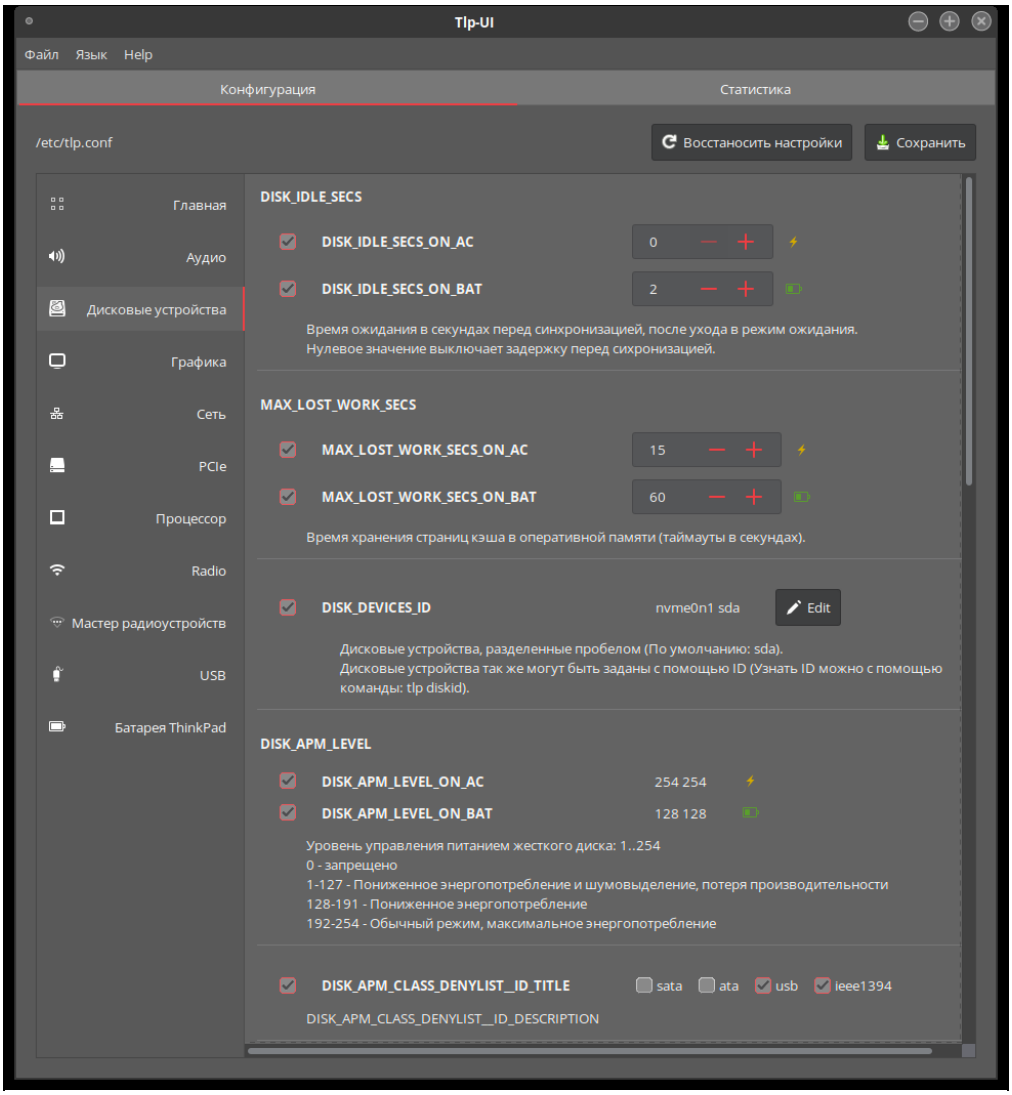
1. **SOUND_POWER_SAVE_ON_AC** — время ожидания (в секундах) для перехода звукового оборудования в режим энергосбережения при работе от сети.

2. **SOUND_POWER_SAVE_ON_BAT** — время ожидания (в секундах) для перехода звукового оборудования в режим энергосбережения при работе от батареи.

3. **SOUND_POWER_SAVE_CONTROLLER** — включить или выключить контроллер вместе со звуковым чипом. Эффективно только когда активировано энергосбережение звука (SOUND_POWER_SAVE_ON_AC/BAT). Поддерживается только HDA.

Дисковые устройства

Вкладка «**Дисковые устройства**» позволяет пользователю настроить параметры энергосбережения для жестких дисков и твердотельных накопителей (SSD). Здесь можно задать различные таймауты, уровни управления питанием и другие параметры для оптимизации энергопотребления дисковых устройств при работе как от сети, так и от батареи.



Параметры:

1. **DISK_IDLE_SECS** — определяет время простоя диска в секундах перед тем, как он будет переведен в режим экономии энергии.

- **DISK_IDLE_SECS_ON_AC** — время ожидания (в секундах) перед синхронизацией после ухода в режим ожидания при работе от сети.
- **DISK_IDLE_SECS_ON_BAT** — время ожидания (в секундах) перед синхронизацией после ухода в режим ожидания при работе от батареи.

Нулевое значение выключает задержку перед синхронизацией.

2 . **MAX_LOST_WORK_SECS** — относится к максимальному времени, в течение которого данные могут быть потеряны в случае внезапного отключения питания или другой неисправности. Этот параметр определяет временной интервал, в течение которого данные могут оставаться в кеше перед записью на диск.

- **MAX_LOST_WORK_SECS_ON_AC** — время хранения страниц кеша в ОЗУ в секундах при работе от сети.
- **MAX_LOST_WORK_SECS_ON_BAT** — время хранения страниц кеша в ОЗУ в секундах при работе от батареи.

3 . **DISK_DEVICES_ID** — определяет идентификаторы устройств жестких дисков, для которых будут применены настройки энергосбережения TLP.

4 . **DISK_APM_LEVEL** — задает уровень управления энергопотреблением для жесткого диска, влияя на баланс между производительностью и энергосбережением.

- **DISK_APM_LEVEL_ON_AC** — уровень управления питанием при работе от сети.
- **DISK_APM_LEVEL_ON_BAT** — уровень управления питанием при работе от батареи.

Возможные значения:

- **1** — максимальное энергосбережение/минимальная производительность (настройка может привести к повышенному износу жесткого диска из-за чрезмерной разгрузки головки чтения-записи);
- **128** — баланс между энергосбережением и износом (стандартная настройка TLP на аккумуляторе);
- **192** — предотвращает чрезмерную разгрузку головок некоторых HDD;
- **254** — минимальное энергосбережение/максимальная производительность (стандартная настройка TLP на переменном токе);

- **255** — отключить APM (не поддерживается некоторыми моделями дисков).

5. **DISK_APM_CLASS_DENYLIST_ID_TITLE** — исключает классы дисков из расширенного управления питанием.

Возможные значения:

- **sata** — для подключения жёстких дисков и SSD;
- **ata** — для подключения дисковых устройств;
- **usb** — для подключения внешних дисков;
- **ieee1394** — для подключения различных устройств, включая внешние диски.

6 . **DISK_SPINDOWN_TIMEOUT** — определяет время простоя в секундах перед тем, как жесткий диск будет переведен в режим остановки вращения для экономии энергии.

- **DISK_SPINDOWN_TIMEOUT_ON_AC** — время ожидания запуска диска при работе от сети;
- **DISK_SPINDOWN_TIMEOUT_ON_BAT** — время ожидания запуска диска при работе от батареи.

Возможные значения:

- **0** — отключить уменьшение оборотов;
- **от 1 до 240** — время ожидания от 5 секунд до 20 минут (шаг в 5 секунд);
- **от 241 до 251** — время ожидания от 30 минут до 5.5 часов (шаг в 30 минут).

7. **DISK_IOSCHED** — устанавливает планировщик ввода-вывода для дисковых устройств.

Возможные значения:

- Планировщики нескольких очередей:
  - **mq-deadline** — многоканальная версия планировщика deadline, обеспечивающая минимальное время отклика для каждой операции ввода-вывода;
  - **none** — отключает планирование, передавая операции ввода-вывода напрямую на устройство без дополнительной очереди;
  - **kyber** — планировщик, оптимизированный для устройств с низкой задержкой, таких как SSD, который учитывает задержку и пропускную способность;
  - **bfq** — предназначен для обеспечения оптимального распределения дискового времени между всеми процессами;
  - **keep** — сохраняет текущий планировщик, не изменяя его.

- Планировщики одной очереди:
  - **deadline** — минимизирует время ожидания операций ввода-вывода, устанавливая жесткие сроки для их выполнения;
  - **cfq** — равномерно распределяет время доступа к диску между процессами;
  - **bfq** — выделяет каждому процессу лимит времени для более эффективного управления и снижения задержки;
  - **noop** — простой планировщик, который полезен для устройств с собственным алгоритмом планирования, например, SSD;
  - **keep** — сохраняет текущий планировщик для систем с одной очередью.

8 . **SATA_LINKPWR** — управляет режимами энергосбережения для SATA-устройств, определяя, как активно будет использоваться энергосбережение на уровне интерфейса SATA.

- **SATA_LINKPWR_ON_AC** — управляет режимом управления питанием для каналов SATA при работе от сети.
- **SATA_LINKPWR_ON_BAT** — устанавливает режим управления питанием для каналов SATA, соединяющих диски и оптические приводы.

Возможные значения:

- **min_power**— максимальное энергосбережение / минимальная производительность;
- **med_power_with_dipm** — лучший баланс между энергосбережением и производительностью (рекомендуется);
- **medium_power** — среднее энергопотребление и производительность;
- **max_performance** — минимальное энергосбережение / максимальная производительность.

9. **SATA_LINKPWR_DENYLIST**_ID_TITLE — позволяет исключить определённые устройства из управления энергопотреблением SATA для предотвращения проблем с совместимостью или производительностью. Диски определяются их хостом, формат — hostX.

10. **AHCI_RUNTIME_PM** — управляет режимами энергосбережения для устройств, подключенных через интерфейс AHCI.

- **AHCI_RUNTIME_PM_ON_AC** — управляет питанием для дисков NVMe, SATA, ATA и USB при работе от сети, предоставляя опцию автоматического выключения бездействующих устройств для экономии энергии.
- **AHCI_RUNTIME_PM_ON_BAT** — контролирует управление питанием для дисков NVMe, SATA, ATA и USB, а также для портов SATA.

Возможные значения:

- **auto** — выключать бездействующие устройства;
- **on** — устройства включены постоянно.

11. **AHCI_RUNTIME_PM_TIMEOUT** — время ожидания в секундах перед приостановкой работы диска или порта. Действует только при активации **AHCI_RUNTIME_PM_ON_AC/BAT**.

12. **BAY_POWEROFF** — позволяет отключать питание для устройств, установленных в сменных отсеках (например, для оптических

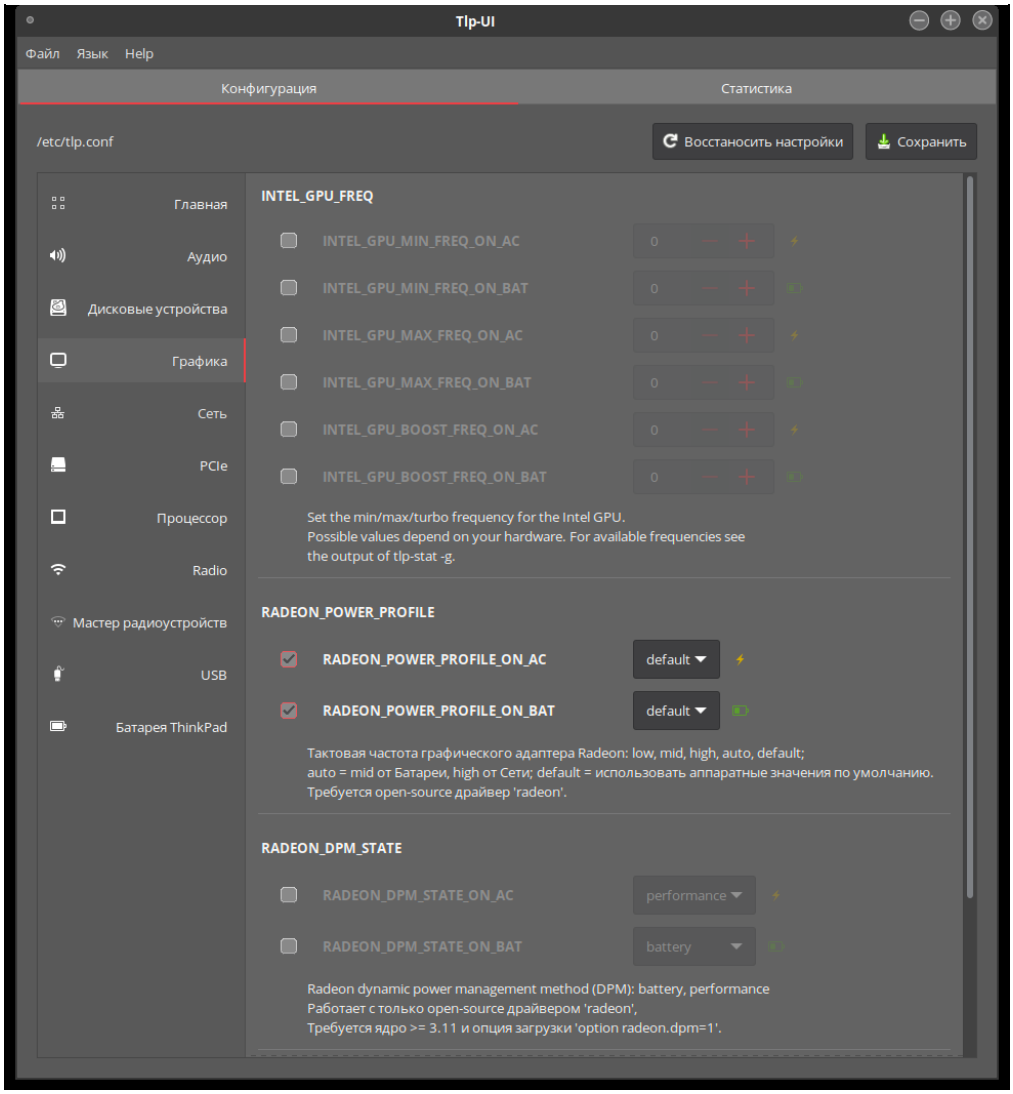
дисководов или дополнительных жестких дисков), когда они не используются, с целью экономии энергии.

- **BAY_POWEROFF_ON_AC** — позволяет управлять выключением оптического привода при работе от сети, что может быть полезным для экономии энергии и увеличения времени автономной работы устройства.
- **BAY_POWEROFF_ON_BAT** — управляет выключением оптического привода при работе от батареи, что помогает экономить заряд батареи и продлевает время автономной работы устройства.

13. **BAY_DEVICE** — отображает устройства оптического привода, для которых могут применяться настройки энергосбережения.

Графика

На вкладке «**Графика**» настраиваются параметры управления энергопотреблением для графических ускорителей, таких как интегрированные графические процессоры Intel и дискретные адаптеры Radeon.



Параметры:

1. **INTEL_GPU_FREQ** — установка минимальной / максимальной / ускоренной частоты для графического процессора Intel. Возможные значения зависят от вашего оборудования.

- **INTEL_GPU_MIN_FREQ_ON_AC** — минимальная частота графического процессора при работе от сети;
- **INTEL_GPU_MIN_FREQ_ON_BAT** — минимальная частота графического процессора при работе от батареи;
- **INTEL_GPU_MAX_FREQ_ON_AC** — максимальная частота графического процессора при работе от сети;
- **INTEL_GPU_MAX_FREQ_ON_BAT** — максимальная частота графического процессора при работе от батареи;
- **INTEL_GPU_BOOST_FREQ_ON_AC** — частота ускорения (Boost) графического процессора при работе от сети;
- **INTEL_GPU_BOOST_FREQ_ON_BAT** — частота ускорения (Boost) графического процессора при работе от батареи.

2. **RADEON_POWER_PROFILE** — управление тактовой частотой графического адаптера Radeon.

- **RADEON_POWER_PROFILE_ON_AC** — устанавливает профиль энергопотребления графического адаптера Radeon при работе от сети;
- **RADEON_POWER_PROFILE_ON_BAT** — устанавливает профиль энергопотребления графического адаптера Radeon при работе от батареи.

Возможные значения:

  - **low** — низкий уровень;

- **mid** — средний уровень;
- **high** — высокий уровень;
- **auto** — использует *средний уровень* при питании от батареи и *высокий уровень* при питании от сети;
- **default** — использует аппаратные настройки по умолчанию.

3. **RADEON_DPM_STATE** — управление Dynamic Power Management (DPM) для графического адаптера Radeon.

- **RADEON_DPM_STATE_ON_AC** — управляет состоянием DPM графического адаптера Radeon при работе от сети.
- **RADEON_DPM_STATE_ON_BAT** — управляет состоянием DPM графического адаптера Radeon при работе от батареи.

Возможные значения:

- **battery** — активируется, когда устройство работает на батарее, в этом режиме система предпринимает шаги для уменьшения энергопотребления;
- **perfomance** — активируется, когда устройство подключено к источнику переменного тока, в этом режиме система может использовать полные ресурсы процессора.

4. **RADEON_DPM_PERF_LEVEL** — установка уровня производительности для Radeon DPM.

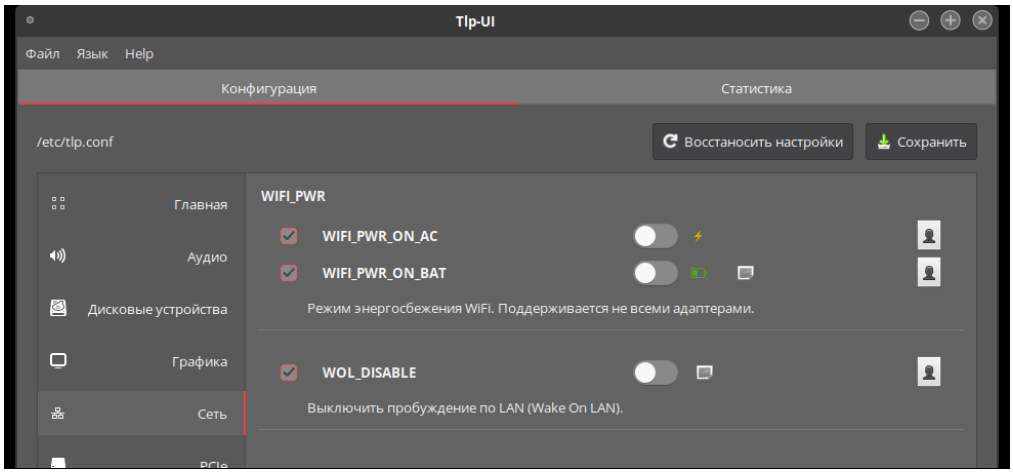
- **RADEON_DPM_PERF_LEVEL_ON_AC** — устанавливает уровень производительности для Radeon DPM при работе от сети;
- **RADEON_DPM_PERF_LEVEL_ON_BAT** — устанавливает уровень производительности для Radeon DPM при работе от батареи.

Возможные значения:

- **auto** — позволяет автоматический контроль уровня производительности графического процессора Radeon;
- **low** — при установке этой настройки графический процессор Radeon будет работать на низком уровне производительности;
- **high** — при выборе этой настройки графический процессор Radeon будет работать на высоком уровне производительности.

Сеть

На вкладке «**Сеть**» предоставлены параметры управления энергопотреблением и функциями, такими как режим энергосбережения Wi-Fi и отключение пробуждения по LAN (Wake-on-LAN), для оптимизации работы сетевых адаптеров.



Параметры:

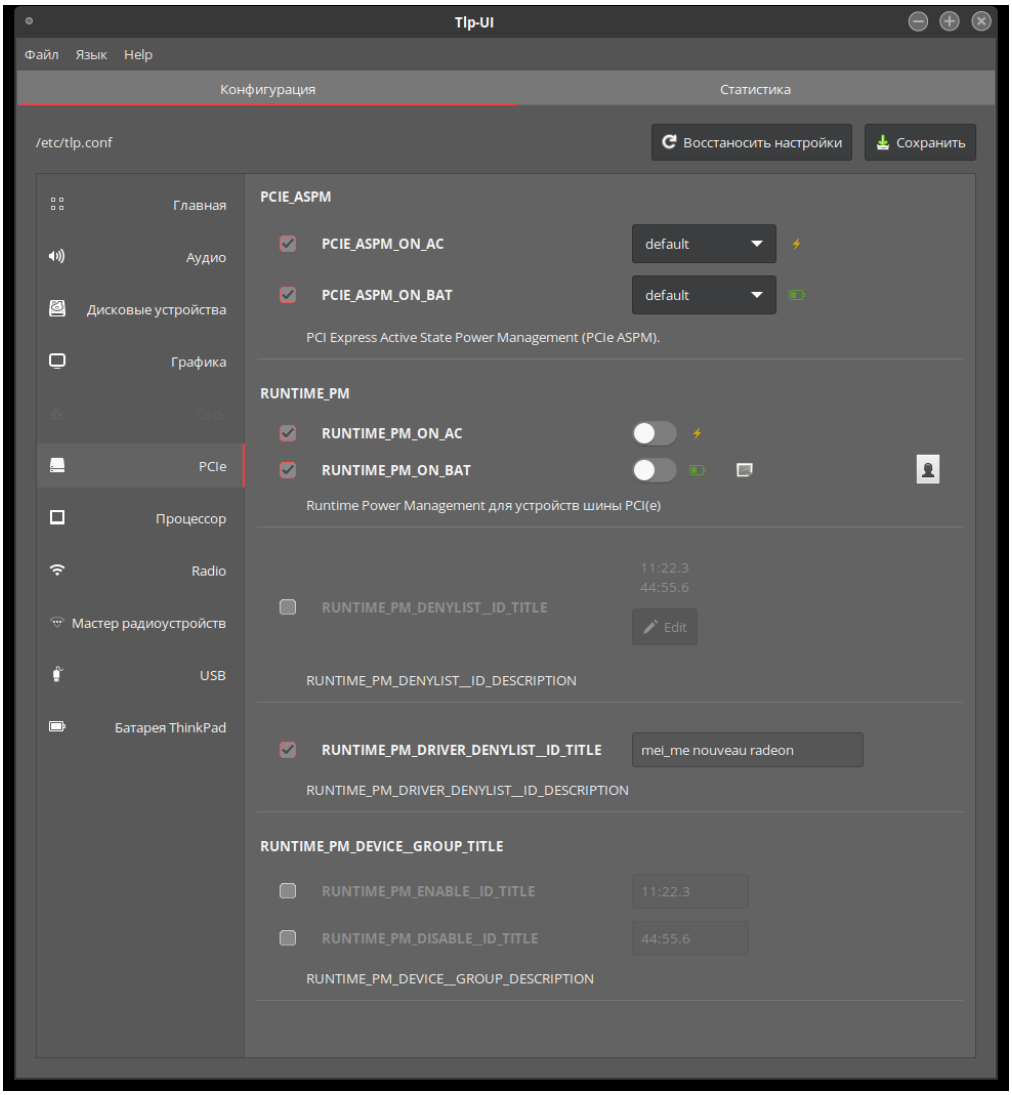
1. **WIFI_PWR** — устанавливает режим энергосбережения Wi-Fi (поддержка адаптера зависит от ядра и драйвера).

- **WIFI_PWR_ON_AC** — определяет уровень мощности Wi-Fi адаптера, когда устройство подключено к источнику питания;
- **WIFI_PWR_ON_BAT** — определяет уровень мощности Wi-Fi адаптера, когда устройство работает от батареи.

2. **WOL_DISABLE** — отключает функцию Wake-on-LAN (WOL), позволяющую удаленно включать компьютер по сети.

PCIe

На вкладке «**PCIe**» настраиваются параметры энергосбережения и управления энергопотреблением для PCIe-устройств, включая режим энергосбережения ASPM, режим управления энергопотреблением во время работы и список исключений для устройств и их драйверов.



Параметры:

1. **PCIE_ASPM** — устанавливает режим энергосбережения (PCIe ASPM).

- **PCIE_ASPM_ON_AC** — устанавливает режим энергосбережения для PCIe ASPM при работе от сети.
- **PCIE_ASPM_ON_BAT** — устанавливает режим энергосбережения для PCIe ASPM при работе от батареи.

Возможные значения:

- **default** — использует настройки по умолчанию, определённые системой или оборудованием;
- **performance** — приоритет производительности;
- **powersave** — снижает потребление энергии;
- **powersupersave** — максимально снижает потребления энергии.

2. **RUNTIME_PM** — управляет энергопотреблением во время работы устройств шины PCI(e).

- **RUNTIME_PM_ON_AC** — активирует управление энергопотреблением в реальном времени при подключении устройства к источнику переменного тока.
- **RUNTIME_PM_ON_BAT** — активирует управление энергопотреблением в реальном времени при работе устройства от батареи.

Возможные значения:

  - **включено** — выключение неактивных устройств;
  - **отключено** — устройства включены постоянно.

3 . **RUNTIME_PM_DENYLIST_ID_TITLE** — представляет список идентификаторов устройств, для которых отключено управление энергопотреблением в реальном времени.

4. **RUNTIME_PM_DRIVER_DENYLIST_ID_TITLE** — представляет список идентификаторов драйверов устройств, для которых отключено управление энергопотреблением в реальном времени.

Возможные значения:

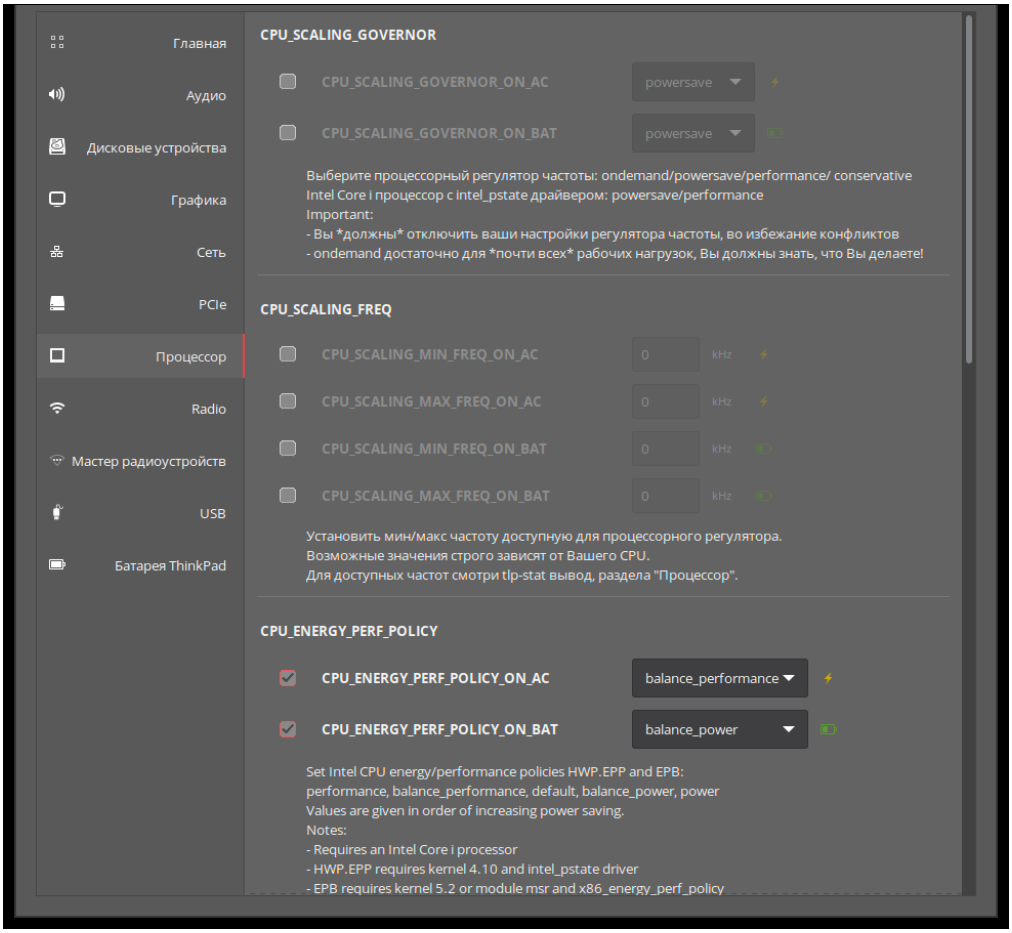
  - **mei_me nouveau radeon** — версия 1.4 и выше;
  - **amdgpu mei_me nouveau nvidia pcieport radeon** — версия 1.3.

5 . **RUNTIME_PM_DEVICE_GROUP_TITLE** — группа устройств, для которых управление энергопотреблением в реальном времени активировано/отключено.

- **RUNTIME_PM_ENABLE_ID_TITLE** — идентификаторы устройств, для которых активировано управление энергопотреблением в реальном времени.
- **RUNTIME_PM_DISABLE_ID_TITLE** — идентификаторы устройств, для которых отключено управление энергопотреблением в реальном времени.

Процессор

На вкладке «**Процессор**» можно настроить параметры управления энергопотреблением для центрального процессора (CPU). Эти параметры могут включать в себя управление частотой процессора, режимом работы ядер, а также другие опции, которые могут повлиять на производительность и энергопотребление процессора.



Параметры:

1. **CPU_SCALING_GOVERNOR** — определяет алгоритм управления частотой процессора в операционной системе.

- **CPU_SCALING_GOVERNOR_ON_AC** — определяет алгоритм управления частотой процессора при подключении устройства к источнику переменного тока.
- **CPU_SCALING_GOVERNOR_ON_BAT** — определяет алгоритм управления частотой процессора при работе устройства от батареи.

Возможные значения:

  - **ondemand** — алгоритм управления частотой процессора, который динамически регулирует частоту процессора в зависимости от нагрузки на систему;
  - **powersave** — алгоритм управления частотой процессора, который старается минимизировать энергопотребление, даже за счет производительности;
  - **performance** — алгоритм управления частотой процессора, который устанавливает максимальную частоту процессора для обеспечения максимальной производительности;
  - **conservative** — алгоритм управления частотой процессора, который старается сохранить высокую производительность, но при этом избегает частых переключений частоты для экономии энергии;
  - **schedutil** — алгоритм управления частотой процессора, который является адаптивным и использует информацию от планировщика задач для регулировки частоты процессора с целью обеспечения баланса между производительностью и энергопотреблением.

2 . **CPU_SCALING_MIN_FREQ** — определяет минимальную частоту процессора, которая может быть установлена в системе при использовании алгоритмов управления частотой процессора.

- **CPU_SCALING_MIN_FREQ_ON_AC** — минимальная частота процессора при подключении устройства к источнику переменного тока.

- **CPU_SCALING_MAX_FREQ_ON_AC** — максимальная частота процессора при подключении устройства к источнику переменного тока.
- **CPU_SCALING_MIN_FREQ_ON_BAT** — минимальная частота процессора при работе устройства от батареи.
- **CPU_SCALING_MAX_FREQ_ON_BAT** — максимальная частота процессора при работе устройства от батареи.

3. **CPU_ENERGY_PERF_POLICY** — управляет энергоэффективностью и производительностью процессора.

- **CPU_ENERGY_PERF_POLICY_ON_AC** — определяет политику энергоэффективности и производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_ENERGY_PERF_POLICY_ON_BAT** — определяет политику энергоэффективности и производительности процессора при работе устройства от батареи.

Возможные значения:

  - **default** — использует стандартные настройки производительности и энергопотребления, предоставляемые операционной системой;
  - **performance** — обеспечивает максимальную производительность процессора, игнорируя энергосберегающие меры;
  - **balance_performance** — обеспечивает баланс между производительностью и энергосбережением, уделяя приоритет производительности;
  - **balance_power** — обеспечивает баланс между производительностью и энергосбережением, уделяя приоритет энергосбережению;
  - **power** — нацелен на минимизацию энергопотребления.

4. **CPU_PERF** — минимальный уровень производительности процессора. ***Возможные значения:*** от 0 до 100%.

- **CPU_MIN_PERF_ON_AC** — минимальный уровень производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_MAX_PERF_ON_AC** — максимальный уровень производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_MIN_PERF_ON_BAT** — минимальный уровень производительности процессора при работе устройства от батареи.
- **CPU_MAX_PERF_ON_BAT** — максимальный уровень производительности процессора при работе устройства от батареи.

5. **CPU_BOOST** — управляет возможностью процессора использовать режимы повышенной производительности.

- **CPU_BOOST_ON_AC** — включает или отключает режимы повышенной производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_BOOST_ON_BAT** — включает или отключает режимы повышенной производительности процессора при работе устройства от батареи.

6. **CPU_HWP_DYN_BOOST_GROUP_TITLE** — устанавливает настройки для динамического ускорения процессора Intel HWP.

- **CPU_HWP_DYN_BOOST_ON_AC** — включает или отключает динамическое ускорение HWP при подключении устройства к источнику переменного тока.
- **CPU_HWP_DYN_BOOST_ON_BAT** — включает или отключает динамическое ускорение HWP при работе устройства от батареи.

7 . **SCHED_POWERSAVE** — управляет настройками энергосбережения планировщика задач, влияя на распределение задач для минимизации энергопотребления.

- **SCHED_POWERSAVE_ON_AC** — активирует или деактивирует режим энергосбережения планировщика задач при подключении устройства к источнику переменного тока.
- **SCHED_POWERSAVE_ON_BAT** — активирует или деактивирует режим энергосбережения планировщика задач при работе устройства от батареи.

8. **NMI_WATCHDOG** — механизм мониторинга и диагностики, который помогает обнаруживать и реагировать на зависания системы и другие критические ошибки.

9.**PLATFORM_PROFILE_GROUP_TITLE** — устанавливает настройки, касающиеся платформенного профиля, который определяет общие параметры производительности и энергосбережения для устройства.

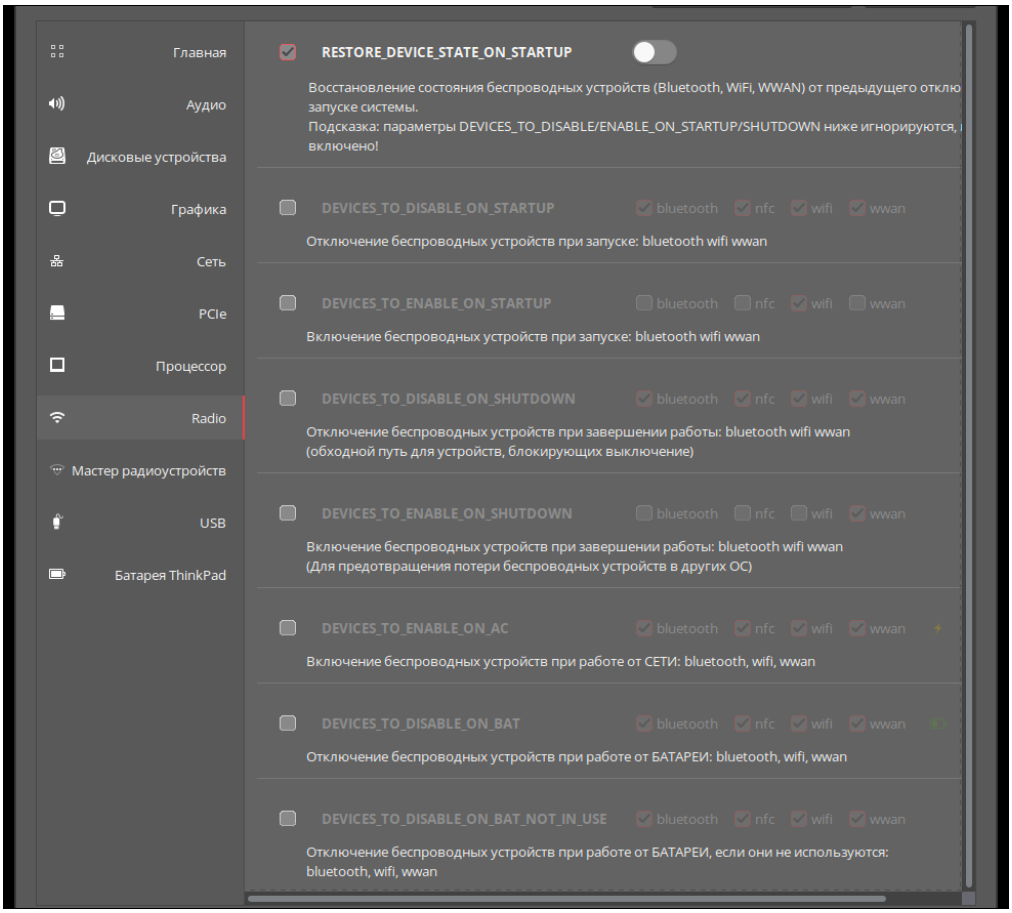
- **PLATFORM_PROFILE_ON_AC** — устанавливает платформенный профиль при подключении устройства к источнику переменного тока.
- **PLATFORM_PROFILE_ON_BAT** — устанавливает платформенный профиль при работе устройства от батареи.

Возможные значения в порядке увеличения энергосбережения:

  - **performance** — обеспечивает максимальную производительность процессора;
  - **balanced** — обеспечивает баланс между производительностью и энергосбережением;
  - **low_power** — обеспечивает максимальное энергосбережение.

Радио

На вкладке «**Радио**» настраиваются параметры энергосбережения для беспроводных устройств, такие как Bluetooth и Wi-Fi. Эти параметры включают управление режимами энергосбережения для беспроводных устройств при работе от сети и от батареи, что помогает оптимизировать энергопотребление и продолжительность работы вашего устройства в различных условиях использования.



Параметры:

1 . **RESTORE_DEVICE_STATE_ON_STARTUP** — восстанавливает состояние беспроводных устройств до настроек, существовавших до выключения или перезагрузки системы.

2 . **DEVICES_TO_DISABLE_ON_STARTUP** — определяет устройства, которые должны быть отключены при запуске системы для экономии энергии или других целей.

3. **DEVICES_TO_ENABLE_ON_STARTUP** — определяет устройства, которые должны быть включены при запуске системы.

4. **DEVICES_TO_DISABLE_ON_SHUTDOWN** — определяет устройства, которые должны быть отключены при выключении системы.

5. **DEVICES_TO_ENABLE_ON_SHUTDOWN** — определяет устройства, которые должны быть включены при выключении системы.

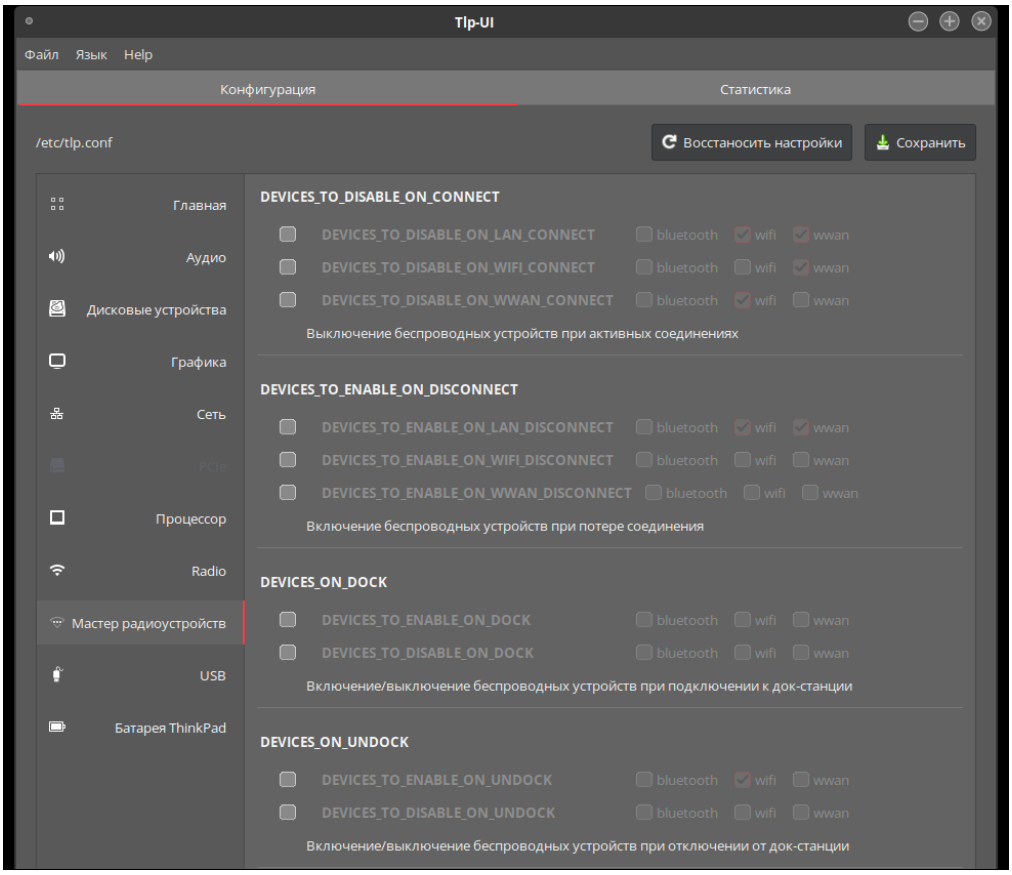
6.**DEVICES_TO_ENABLE_ON_AC** — определяет устройства, которые должны быть включены при подключении устройства к источнику переменного тока (AC).

7. **DEVICES_TO_DISABLE_ON_BAT** — определяет устройства, которые должны быть отключены при работе устройства от батареи.

8. **DEVICES_TO_DISABLE_ON_BAT_NOT_IN_USE** — определяет устройства, которые должны быть отключены при работе устройства от батареи, когда оно не используется.

Мастер радиоустройств

На вкладке «**Мастер радиоустройств**» настраиваются параметры энергосбережения для беспроводных устройств. Эти параметры включают управление режимами энергосбережения для беспроводных устройств при работе от сети и от батареи, что позволяет оптимизировать энергопотребление и продолжительность работы устройства в различных сценариях использования.



Параметры:

1 . **DEVICES_TO_DISABLE_ON_CONNECT** — при установленном соединении LAN, Wi-Fi или WWAN беспроводные устройства отключаются.

- **DEVICES_TO_DISABLE_ON_LAN_CONNECT** — устройства, которые необходимо отключить при подключении к проводной сети.
- **DEVICES_TO_DISABLE_ON_WIFI_CONNECT** — устройства, которые необходимо отключить при подключении к Wi-Fi сети.
- **DEVICES_TO_DISABLE_ON_WWAN_CONNECT** — устройства, которые необходимо отключить при подключении к мобильной сети.

2. **DEVICES_TO_ENABLE_ON_DISCONNECT** — при отключении соединения LAN, Wi-Fi, WWAN беспроводные устройства активируются.

- **DEVICES_TO_ENABLE_ON_LAN_DISCONNECT** — устройства, которые необходимо включить при отключении от проводной сети.
- **DEVICES_TO_ENABLE_ON_WIFI_DISCONNECT** — устройства, которые необходимо включить при отключении от Wi-Fi сети.
- **DEVICES_TO_ENABLE_ON_WWAN_DISCONNECT** — устройства, которые необходимо включить при отключении от мобильной сети.

3. **DEVICES_ON_DOCK** — устройства, которые должны быть активны при подключении к док-станции.

- **DEVICES_TO_ENABLE_ON_DOCK** — устройства, которые необходимо включить при подключении к док-станции.
- **DEVICES_TO_DISABLE_ON_DOCK** — устройства, которые необходимо отключить при подключении к док-станции.

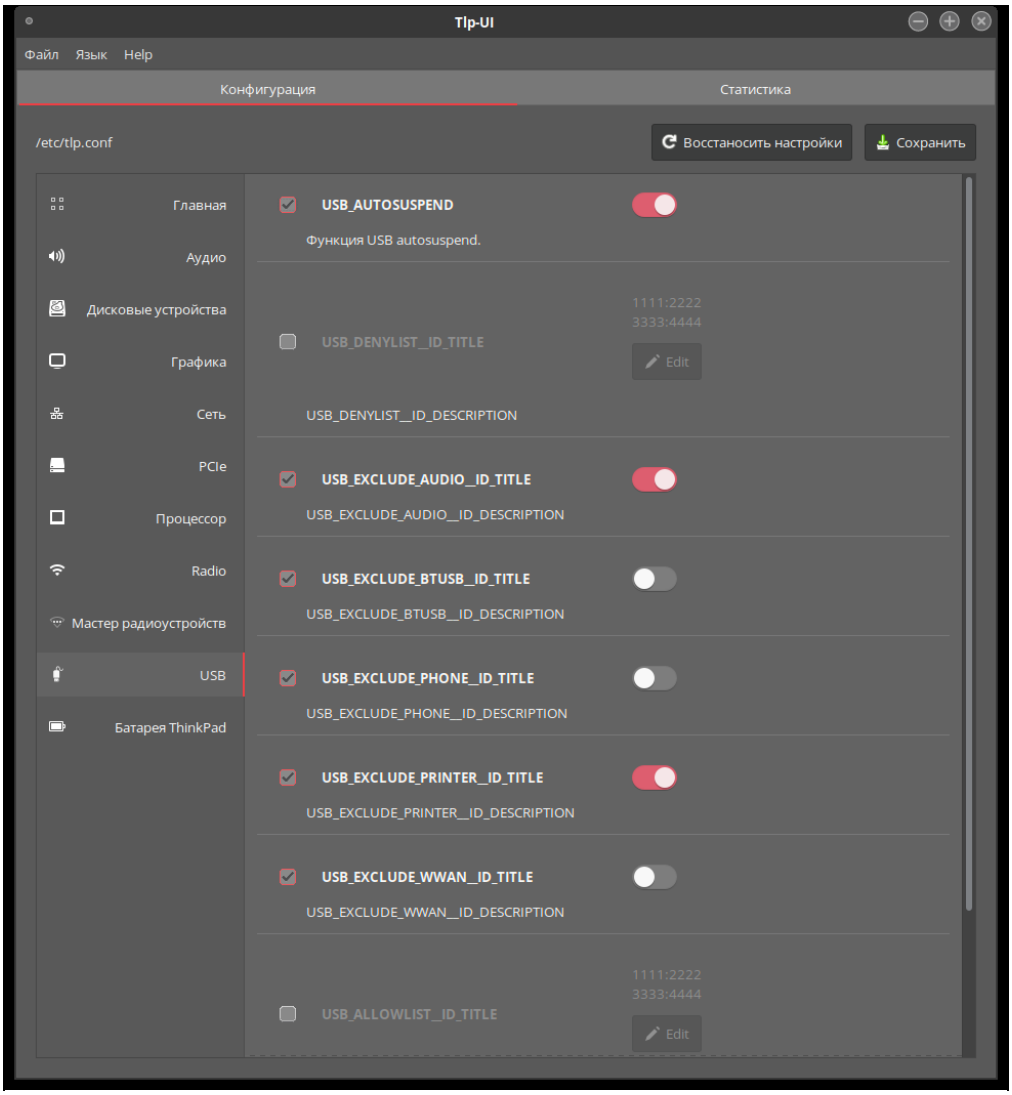
4. **DEVICES_ON_UNDOCK** — устройства, которые должны быть активны при отключении от док-станции.

- **DEVICES_TO_ENABLE_ON_UNDOCK** — устройства, которые необходимо включить при отключении от док-станции.
- **DEVICES_TO_DISABLE_ON_UNDOCK** — устройства, которые необходимо отключить при отключении от док-станции.

Беспроводные устройства: bluetooth, wifi, wwan.

USB

На вкладке «**USB**» настраиваются параметры управления энергопотреблением для портов USB и связанных с ними устройств. Здесь можно установить режимы энергосбережения, такие как отключение USB-портов или управление энергопотреблением подключенных устройств. Это позволяет оптимизировать энергопотребление и продолжительность работы устройства в различных сценариях использования.



Параметры:

1 . **USB_AUTOSUSPEND** — отвечает за автоматическое приостановление работы USB-устройств для экономии энергии. Когда эта функция активирована, USB-устройства переходят в режим низкого энергопотребления после определенного времени бездействия.

2. **USB_DENYLIST** — позволяет указать список USB-устройств, для которых автоматическое приостановление работы будет отключено. Полезно для устройств, испытывающих трудности с выходом из режима автозависания.

3 . **USB_EXCLUDE_AUDIO** — предназначена для исключения аудиоустройств из автоматического приостановления работы. При активировании этой опции USB-аудиоустройства остаются активными и не переходят в режим низкого энергопотребления, обеспечивая постоянную доступность звуковых функций.

4. **USB_EXCLUDE_BTUSB** — исключает Bluetooth-устройства из автоматического приостановления работы, обеспечивая их постоянную активность.

5 . **USB_EXCLUDE_PHONE** — исключает смартфоны из автоматического приостановления работы, обеспечивая их постоянную активность.

6. **USB_EXCLUDE_PRINTER** — исключает принтеры из автоматического приостановления работы, обеспечивая их постоянную активность.

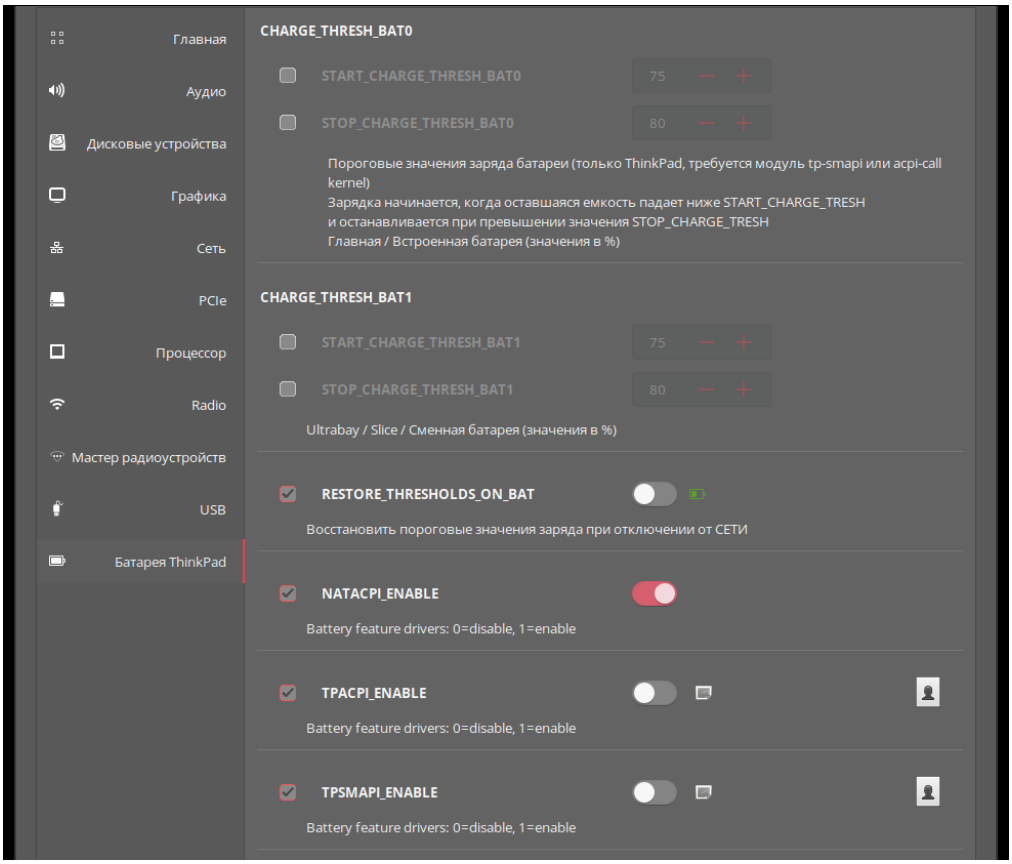
7. **USB_EXCLUDE_WWAN** — исключает WWAN (беспроводные широкополосные сети) устройства из автоматического приостановления работы, обеспечивая их постоянную активность.

8 . **USB_ALLOWLIST** — позволяет указать список USB-устройств, которые будут исключены из автоматического приостановления работы, обеспечивая их постоянную активность.

9 . **USB_AUTOSUSPEND_DISABLE_ON_SHUTDOWN** — отвечает за отключение автоматического приостановления работы для USB-устройств перед выключением системы.

Батарея ThinkPad

Вкладка «**Батарея ThinkPad**» предоставляет возможность управления различными параметрами работы батареи ThinkPad. В этой вкладке можно настроить различные параметры зарядки, разрядки и энергосбережения батареи. Например, пользователь может установить пороги заряда, определить условия начала и прекращения заряда, а также настроить другие параметры, влияющие на производительность и долговечность батареи.



1. **CHARGE_THRESH_BAT0** — задает пороговый уровень заряда для аккумулятора.

- **START_CHARGE_THRESH_BAT0** — определяет пороговый уровень заряда, при достижении которого начинается заряд аккумулятора.
- **STOP_CHARGE_THRESH_BAT0** — определяет пороговый уровень заряда, при достижении которого происходит прекращение заряда аккумулятора.

2. **CHARGE_THRESH_BAT1** — позволяет задать пороговый уровень заряда для сменной батареи в ноутбуках Lenovo ThinkPad, если они поддерживают две батареи.

- **START_CHARGE_THRESH_BAT1** — устанавливает порог заряда, при достижении которого начинается заряд сменной батареи.
- **STOP_CHARGE_THRESH_BAT1** — устанавливает порог заряда, при достижении которого прекращается заряд сменной батареи.

3. **RESTORE_THRESHOLDS_ON_BAT** — восстановление настроенных порогов заряда при отключении от сети.

4. **NATACPI_ENABLE** — включает поддержку ACPI для управления зарядом батареи.

5. **TPACPI_ENABLE** — включает поддержку ACPI для управления различными функциями ThinkPad.

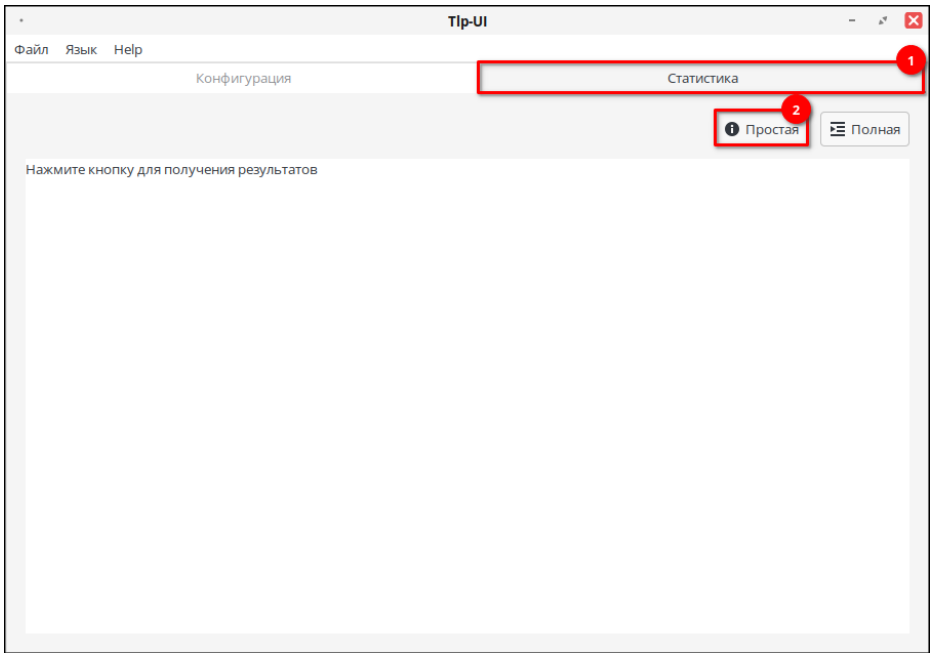
6.**TPSMAPI_ENABLE** — включает поддержку SMAPI для управления различными функциями батареи ThinkPad.

Вкладка «Статистика»

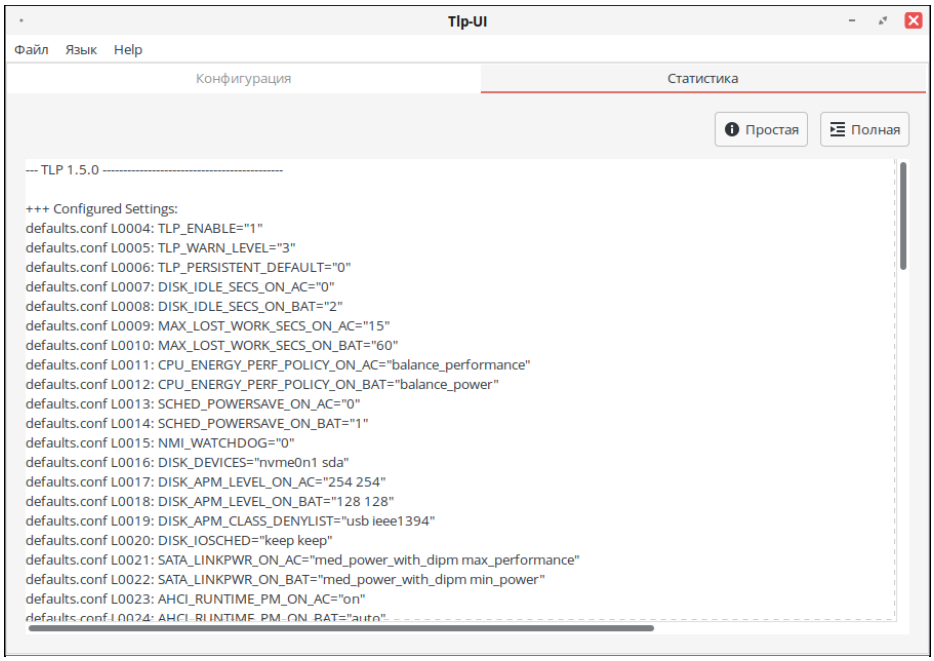
Вкладка "**Статистика**" предоставляет пользователю информацию о статистике использования энергии на компьютере. Здесь отображаются данные о потреблении энергии, времени работы от аккумулятора, времени работы от сети и другие параметры, которые помогают отслеживать и анализировать энергопотребление устройства. Это позволяет пользователям лучше понимать, как и когда их устройство использует энергию, и оптимизировать его работу для экономии энергии и увеличения времени автономной работы.

Просмотр статистики

Для просмотра статистических данных откройте вкладку «**Статистика**» (1) и нажмите кнопку «**Простая**» (2).



После этого будут отражены данные о системе:



Работа в терминале

Синтаксис TLP

Утилита tlp доступна для запуска через терминал при помощи команды следующего вида:

```
tlp [<команды>] [<параметры>] [--параметры_конфигурации=<значение> ... ]
```

Команды TLP

Основные команды утилиты:

- **start** — инициализировать tlp и применить настройки энергосбережения в соответствии с фактическим источником питания, используется для применения измененной конфигурации или выхода из ручного режима.
- **bat, true** — применить профиль настроек батареи и перейти в ручной режим.
- **ac** — применить профиль настроек переменного тока и перейти в ручной режим. Ручной режим означает, что изменения в источнике питания будут игнорироваться до следующей перезагрузки или запуска tlp для возобновления автоматического режима.
- **false** — включить автоматическую приостановку для всех USB—устройств, за исключением тех, которые исключены по

умолчанию или в конфигурации.
- **bayoff** — выключить оптический привод в UltraBay/MediaBay.
- **setcharge** — временно изменить пороговые значения заряда батареи. Если оборудование поддерживает только пороговое значение stop, установить начальное значение равным 0. Настроенные пороговые значения заряда будут восстановлены при следующей загрузке или при повторном использовании tlp setcharge, но без пороговых параметров. **Синтаксис команды имеет вид:** `setcharge [<START_CHARGE_THRESH> <STOP_CHARGE_THRESH>] [BAT0|BAT1|BAT<x>|CMB0]`.
- **fullcharge** — предназначена для зарядки аккумулятора до полной емкости путем временного применения предустановок производителя к пороговым значениям заряда. Настроенные пороговые значения заряда будут восстановлены при следующей загрузке или с помощью tlp setcharge без аргументов threshold (уровень заряда). Команда предназначена для временного увеличения заряда аккумулятора до максимальной емкости, но не изменяет стандартных настроек порогов заряда. **Синтаксис команды имеет вид:** `fullcharge [BAT0|BAT1|BATx|CMB0]`.
- **chargeonce** (только для ThinkPads) — зарядить аккумулятор до порогового значения stop charge один раз. Для этого необходимо временно снять пороговое значение start charge. Настроенное пороговое значение start charge будет восстановлено при следующей загрузке или с помощью tlp setcharge без аргументов. **Синтаксис команды имеет вид:** `chargeonce [BAT0|BAT1]`.
- **discharge** (только для ThinkPads) — принудительно полностью разрядить аккумулятор. **Синтаксис команды имеет вид:** `discharge [BAT0|BAT1]`.
- **recalibrate** (только для ThinkPads) — повторная калибровка аккумулятора: полностью разрядить аккумулятор и зарядить его до 100%. Для этого к пороговым значениям временно применяются настройки производителя. Настроенные пороговые значения будут восстановлены при следующей загрузке или с помощью tlp setcharge. **Синтаксис команды имеет вид:** `recalibrate [BAT0|BAT1]`.
- **diskid** — отобразить идентификаторы дисков для настройки.

Параметры TLP

Основные параметры утилиты:

- **-b, --battery** — проверка состояния заряда и другой информации о батарее;
- **-c, --config** — проверка состояния настроек конфигурации;
- **-d, --disk** — проверка состояния диска;
- **-e, --pcie** — проверка состояния шины PCI Express;
- **-g, --graphics** — проверка состояния графической подсистемы;
- **-p, --processor** — проверка состояния процессора;
- **-r, --rfkill** — проверка состояния переключателей аппаратного блокирования;
- **-s, --system** — проверка состояния системы;
- **-t, --temp** — проверка состояния температуры;
- **-u, --usb** — проверка состояния устройств USB;
- **-w, --warn** — проверка состояния предупреждений;
- **-v, --verbose** — вывод более подробной информации;
- **--cdiff** — проверка состояния различий в конфигурации;
- **--pev** — проверка состояния окружения Power and Environmental Monitoring;
- **-P, --psup** — проверка состояния источника питания;
- **-T, --trace** — проверка состояния трассировки;
- **--udev** — проверка состояния управления устройствами.

Параметры конфигурации:

Добавьте параметры конфигурации, чтобы переопределить конфигурацию системы только для единственного вызова программы. Впоследствии они не сохраняются.

Для ноутбуков с несколькими аккумуляторами выбор осуществляется следующим образом:

- **BAT0** — основной или встроенный аккумулятор;
- **BAT1** — дополнительный или сменный аккумулятор.

Примеры использования утилиты

1. Запустить TLP. После установки tlp запускается автоматически. Если требуется вручную запустить tlp, можно использовать команду:

```
sudo tlp start
```

Также можно использовать эту команду для применения изменений после редактирования конфигурации.

2. Применить режим автоматической приостановки для всех подключенных USB-устройств, кроме тех, которые исключены по умолчанию или в конфигурации:

```
tlp usb
```

3. Выключить оптический привод в MediaBay/Ultrabay:

```
tlp bayoff
```

4. Временно изменить пороговые значения заряда аккумулятора:

```
sudo tlp setcharge [<START_CHARGE_THRESH> <STOP_CHARGE_THRESH>] [BAT0|BAT1|BAT<x>|CMB0]
```

Пример:

```
tlp setcharge 70 90 BAT0
```

В этом примере применяются пороговые значения 70/90% к батарее BAT0. Tlp setcharge изменяет пороговые значения заряда только временно. Чтобы изменения стали постоянными, необходимо активировать или изменить соответствующие настройки в файле конфигурации.

5. Зарядить аккумулятор до полной емкости:

```
tlp fullcharge [BAT0|BAT1|BAT<x>|CMB0|CMB1]
```

Пример:

```
tlp fullcharge BAT1
```

Заряжает аккумулятор BAT1 до полной емкости.

6. Зарядить аккумулятор до порога остановки заряда один раз (только ThinkPad):

```
tlp chargeonce [BAT0|BAT1]
```

Это достигается путем временного поднятия порога стартового заряда. Настроенный порог стартового заряда будет восстановлен при следующей загрузке или с помощью tlp setcharge без аргументов порога.

Пример:

```
tlp chargeonce BAT0
```

7. Для просмотра текущих настроек TLP можно выполнить команду:

```
tlp-stat
```

8. Проверить состояние заряда и другую информацию о батарее:

```
tlp-stat -b
```

9. Проверить состояние системы:

```
tlp-stat -s
```

10. Проверить все параметры TLP:

```
tlp-stat -p
```

TLP-RDW

Синтаксис утилиты **tlp-rdw** имеет следующий вид:

```
tlp-rdw [<команды>]
```

Основные команды утилиты **tlp-rdw:**

- **disable** — отключить управление беспроводными устройствами;
- **enable** — включить управление беспроводными устройствами;
- **<none>** — использование команды без аргументов отображает фактическое состояние.

Пример использования:

Для отключения параметра управления энергопотреблением в режиме реального времени введите команду:

```
tlp-rdw disable
```

Получение технической информации о ПК

inxi
lshw
lshw-gui
hwinfo
hddtemp
hw-probe
Стандартные средства и команды операционной системы РЕД ОС

Для того, чтобы посмотреть технические данные ПК, на котором установлена операционная система РЕД ОС, можно воспользоваться специализированными программами.

Вы можете подробнее ознакомиться с утилитами для получения технической информации о ПК, просмотрев наши обучающие видео:

- на **RuTube** — Информация, мониторинг и тестирование системы;
- в **Яндекс.Дзен** — Информация, мониторинг и тестирование системы;
- в **VK Видео** — Информация, мониторинг и тестирование системы.

На наших каналах вы также сможете найти много другой полезной информации.

inxi

Инструмент для командной строки, который позволяет отображать информацию о системе и об аппаратной части компьютера.

Установка.

```
sudo dnf install inxi
```

Для вывода полной информации, в консоли вводим:

```
inxi -F
```

Ключ -F даёт наиболее полный вывод данных по системе.

Ключ -b выдаёт общую информацию, является упрощённым аналогом предыдущей команды.

Однако, ключи -F и -b не выводят абсолютно всех данных. Да и не всегда они необходимы. Следующие ключи дают информацию по конкретным областям:

```
-h Справка;
-A Показать аудио/звуковую информацию карты;
-C Показать данные о процессоре;
-d Отображает данные накопителей на оптических дисках;
-D Показывает полную информацию о жестком диске;
-f Показать все флаги центрального процессора;
-G Показать информацию о графической карте;
-i Показывает WAN IP-адрес, локальные интерфейсы, наиболее полная;
-I Показать информацию: процессы, время бесперебойной работы, память;
-m Показывает память (RAM). Результаты вывода этого ключа не выдаются при использовании ключей -b или -F;
-o Просмотреть информацию о несмонтированном разделе (включая UUID и маркировки если таковые имеются);
-S Информация о системе: имя хоста, ядро, окружение рабочего стола, дистрибутив.
-u Показать разделы и их UUID.
```

Например для просмотра информации по видеокарте:

```
inxi -G
```

Получим вывод:

```
Graphics:
Device-1: VMware SVGA II Adapter driver: vmwgfx v: 2.15.0.0
Display: x11 server: X.Org 1.19.5 driver: vmware
unloaded: fbdev,modesetting,vesa resolution: 1280×960~60Hz
OpenGL: renderer: llvmpipe (LLVM 5.0 128 bits) v: 2.1 Mesa 17.3.6
```

lshw

Ещё одна консольная утилита для просмотра информации о характеристиках компьютера.

Установка.

```
sudo dnf install lshw
```

Данная утилита требует для запуска права суперпользователя:

```
sudo lshw
```

Используя следующие параметры, можно выбрать формат вывода:

```
-html Вывод аппаратной конфигурации в формате HTML;
-xml Вывод аппаратной конфигурации в формате XML;
-short Отображает только основную информацию;
-c CLASS Показывает только определенный класс оборудования (memory, disk, network, cpu и т.п.).
```

Пример запуска утилиты для получения основной информации о системе:

```
sudo lshw -short
```

Результат работы:

```
H/W path Device Class Description
=====================================================
system VirtualBox
/0 bus VirtualBox
/0/0 memory 128KiB BIOS
/0/1 memory 1983MiB System memory
/0/2 processor Intel® Pentium® CPU G4560 @ 3.50GHz
/0/100 bridge 440FX — 82441FX PMC [Natoma]
/0/100/1 bridge 82371SB PIIX3 ISA [Natoma/Triton II]
/0/100/1.1 scsi0 storage 82371AB/EB/MB PIIX4 IDE
/0/100/1.1/0 /dev/sda disk 12GB VBOX HARDDISK
/0/100/1.1/0/1 /dev/sda1 volume 1GiB EXT4 volume
/0/100/1.1/0/2 /dev/sda2 volume 10GiB Linux LVM Physical Volume partition
/0/100/1.1/1 /dev/cdrom disk DVD reader
/0/100/2 display SVGA II Adapter
/0/100/3 enp0s3 network 82540EM Gigabit Ethernet Controller
/0/100/4 generic VirtualBox Guest Service
/0/100/5 multimedia 82801AA AC’97 Audio Controller
/0/100/6 bus KeyLargo/Intrepid USB
/0/100/6/1 usb1 bus OHCI PCI host controller
/0/100/6/1/1 input USB Tablet
/0/100/7 bridge 82371AB/EB/MB PIIX4 ACPI
```

lshw-gui

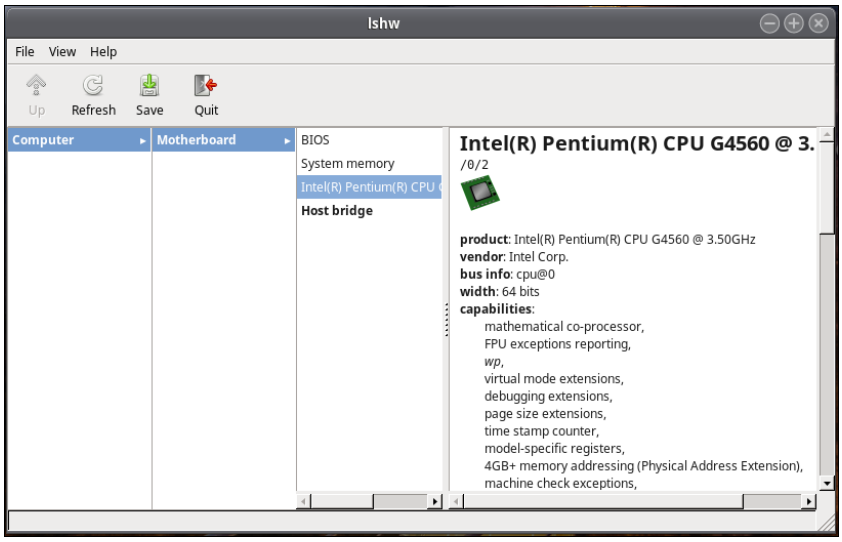
Простой интерфейс для просмотра информации о аппаратном обеспечении компьютера.

Установка.

```
sudo dnf install lshw-gui
```

Запустите через «Меню > Администрирование > Hardware Lister» , или через консоль, набрав команду:

```
sudo lshw-gui
```



В левой части окна отображается оборудование, а в правой части подробная информация о выбранном пункте. lshw-gui позволяет сохранить полученную информацию простым текстом, а также в XML, HTML, JSON форматах.

hwinfo

Консольная утилита для получения информации об аппаратном обеспечении компьютера. Она способна выводить информацию об отдельных категориях аппаратных компонентов, что позволяет получить компактный листинг.

Установка.

```
sudo dnf install hwinfo
```

Для просмотра полной информации о аппаратных компонентах ПК достаточно ввести команду без параметров:

```
hwinfo
```

Однако, полученный вывод не всегда удобен для чтения. Для получения краткого списка компонентов используется параметр short. Он позволяет скрыть подробную информацию о найденных аппаратных компонентах:

```
hwinfo --short
```

Как видно из примера выше, параметры в этой программе записываются через двойной дефис.

Также вы можете выбрать с помощью параметров определённую категорию аппаратных компонентов для просмотра:

```
--cdrom Информация об устройствах для работы с оптическими накопителями;
--cpu Информация о центральном процессоре;
--disk Информация о жестких дисках;
--gfxcard Информация о графическом ускорителе;
--ide Информация об устройствах, подключенных по интерфейсу IDE/SATA;
--memory Информация об оперативной памяти;
--network Информация о сетевых интерфейсах;
--partition Информация о разделах жестких дисков;
--usb Информация об устройствах, подключенных по интерфейсу USB.
```

Если вам нужно получить информацию только об одном устройстве из определённой категории, используйте параметр only. Например, для просмотра информации по разделу жёсткого диска /dev/sda1, команда будет иметь вид:

```
hwinfo --partition --only /dev/sda1
```

Для сохранения журнала работы утилиты в файле достаточно использовать параметр --log с последующим именем файла. В файле сохраняется как журнал работы утилиты, так и выводимая в результате ее работы информация.

```
hwinfo --all --log logfile.txt
```

Файл будет сохранён в корневом каталоге пользователя.

Чтобы сохранить в файл только результат вывода команды howinfo, используется формат:

```
hwinfo --all > logfile.txt
```

Для получения справки по доступным параметрам используется параметр help:

```
hwinfo --help
```

В качестве примера попробуем вывести данные об оперативной памяти:

```
hwinfo --memory
```

Получим:

```
01: None 00.0: 10102 Main Memory
[Created at memory.74]
Unique ID: rdCR.CxwsZFjVASF
Hardware Class: memory
Model: «Main Memory»
Memory Range: 0×00000000-0×7bf57fff (rw)
Memory Size: 1 GB + 896 MB
Config Status: cfg=new, avail=yes, need=no, active=unknown
```

hddtemp

Для успешного прохождения тестов утилиты hddtemp жесткие диски должны поддерживать SMART.
Просмотреть температуру можно командой:

```
hddtemp /dev/sda
```

Вывод команды:

```
/dev/sda: SILICONMOTION SM223AC: 0°C
```

hw-probe

hw-probe - утилита от создателей сайта https://linux-hardware.org/, позволяет одной лаконичной командой собрать в одном файле все основные сведения о системе, аппаратной части и логах, которые могут быть полезными в поисках решения большинства проблем. Результатом работы программы будет ссылка на веб-страницу, по которой можно найти подробную сводку информации о компьютере.

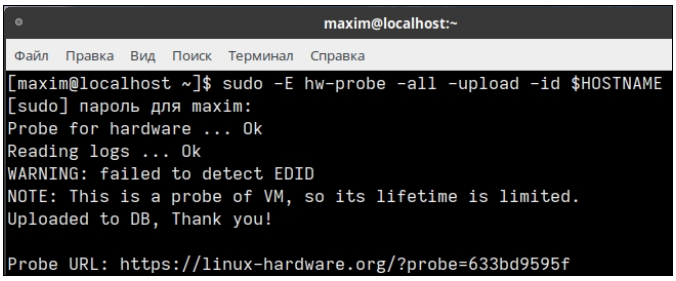
Приватная информация (включая имя пользователя, имя компьютера, IP-адрес, MAC-адрес, серийные номера) **НЕ** собирается в пробе. Инструмент загружает лишь часть *SHA512* хэша от MAC-адреса и серийных номеров для идентификации уникальных компьютеров и компонентов. Данные в базу отправляются по зашифрованному соединению HTTPS.

Устанавливается командой:

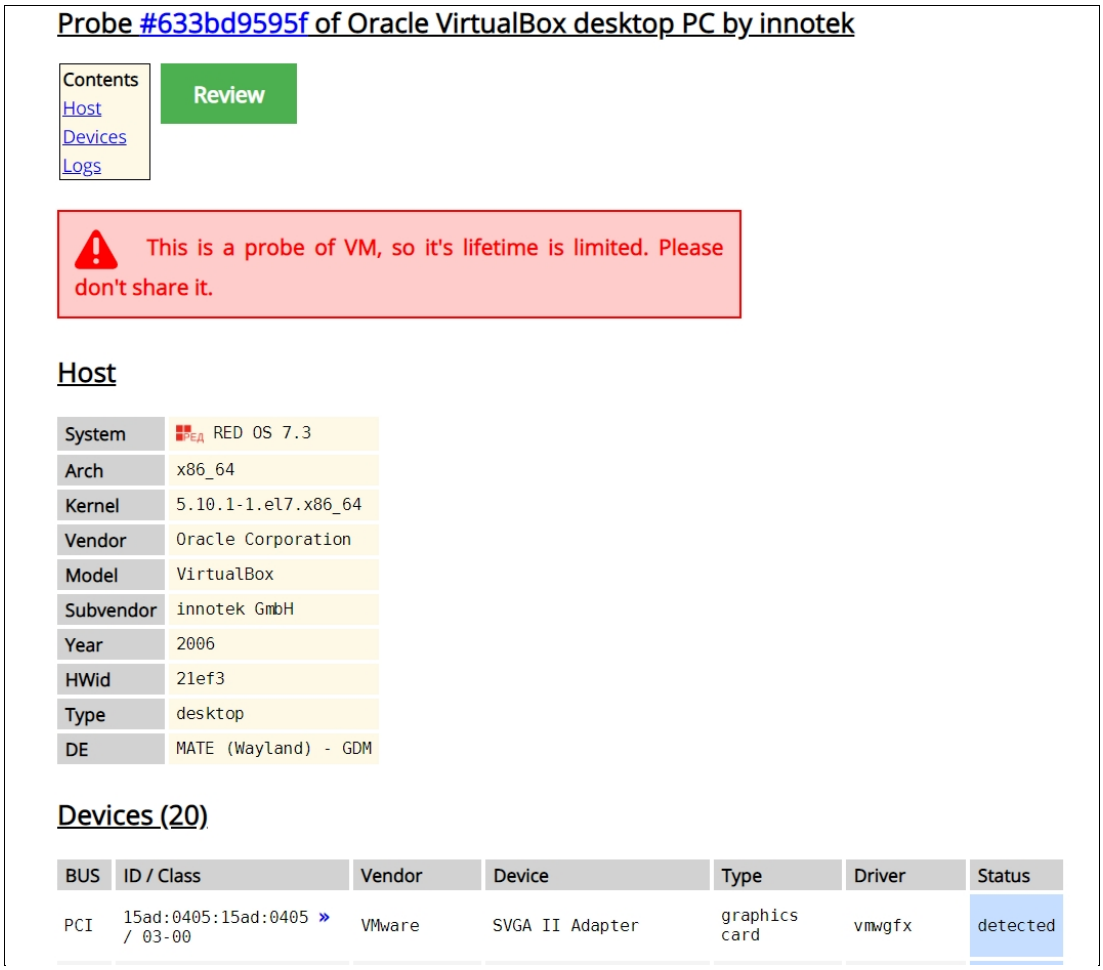
```
sudo dnf install hw-probe
```

Чтобы сгенерировать отчет о системе, нужно выполнить команду:

```
sudo -E hw-probe -all -upload -id $HOSTNAME
```



Терминал предоставляет ссылку, переходя по которой получаем сведения о системе:
https://linux-hardware.org/?probe=633bd9595f



Probe #633bd9595f of Oracle VirtualBox desktop PC by innotek

Contents
Host
Devices
Logs

Review

This is a probe of VM, so it's lifetime is limited. Please don't share it.

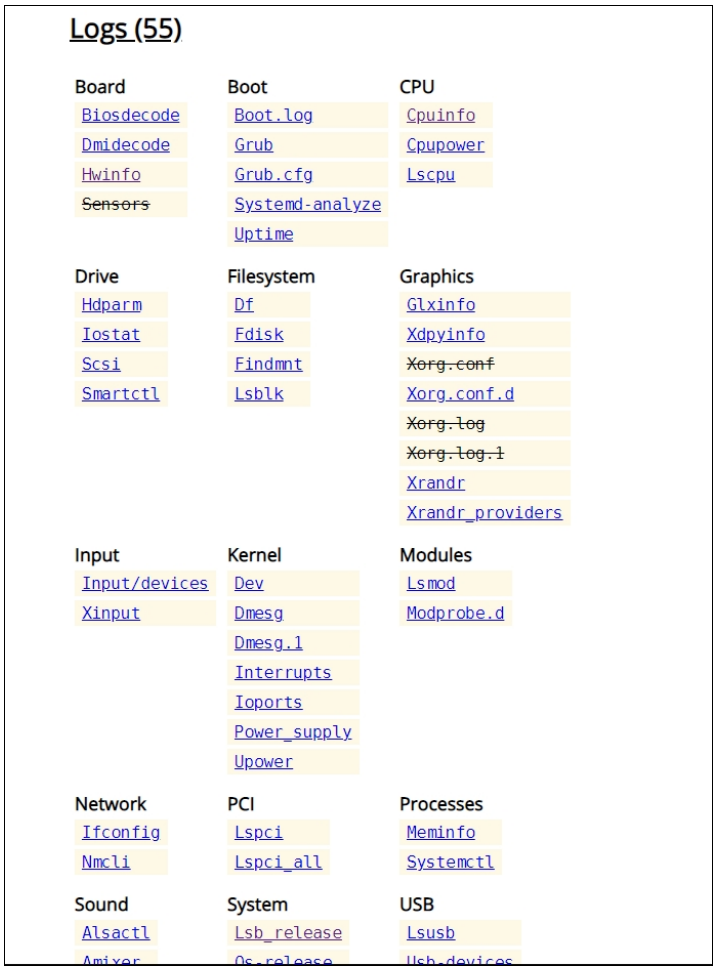
Host

System	RED OS 7.3
Arch	x86_64
Kernel	5.10.1-1.el7.x86_64
Vendor	Oracle Corporation
Model	VirtualBox
Subvendor	innotek GmbH
Year	2006
HWid	21ef3
Type	desktop
DE	MATE (Wayland) - GDM

Devices (20)

BUS	ID / Class	Vendor	Device	Type	Driver	Status
PCI	15ad:0405:15ad:0405 » / 03-00	VMware	SVGA II Adapter	graphics card	vmwgfx	detected

Ниже на этой странице находится необходимый набор логов:



Logs (55)

Board
Biosdecode
Dmidecode
Hwinfo
~~Sensors~~

Boot
Boot.log
Grub
Grub.cfg
Systemd-analyze
Uptime

CPU
Cpuinfo
Cpupower
Lscpu

Drive
Hdparm
Iostat
Scsi
Smartctl

Filesystem
Df
Fdisk
Findmnt
Lsblk

Graphics
Glxinfo
Xdpyinfo
~~Xorg.conf~~
Xorg.conf.d
~~Xorg.log~~
~~Xorg.log.1~~
Xrandr
Xrandr_providers

Input
Input/devices
Xinput

Kernel
Dev
Dmesg
Dmesg.1
Interrupts
Ioports
Power_supply
Upower

Modules
Lsmod
Modprobe.d

Network
Ifconfig
Nmcli

PCI
Lspci
Lspci_all

Processes
Meminfo
Systemctl

Sound
Alsactl
Amixer

System
Lsb_release
Os-release

USB
Lsusb
Usb-devices

При выполнении команды без параметра **-upload**:

```
```

```
sudo -E hw-probe -all
```

информация сохранится локально по пути: **/root/HW_PROBE/LASTEST/hw.info**

Начиная с версии *hw-probe 1.5* можно импортировать отчет в формате html-страницы в указанную директорию:

```
hw-probe -import ./DIR
```

Стандартные средства и команды операционной системы РЕД ОС

Если у вас установлена графическая оболочка Cinnamon, то базовые сведения о системе можно узнать пройдя в «Меню» -> «Параметры» -> «О системе».

Если вам нужна более подробная информация, воспользуйтесь следующими командами из консоли РЕД ОС.

Формат команды	**Описание**
hostnamectl	Имя компьютера и основные данные по ОС.
sudo dmidecode -t 2	Данные по материнской плате (производитель, модель).
lscpu	Информация о процессоре (название модели, семейство, архитектура, его текущая частота, количество ядер, потоков).
cat /proc/meminfo	Просмотр статистики использования памяти в системе читается из файла /proc/meminfo.
free -h	Просмотр основной информации о памяти (общее количество, свободно, используется).
lsb_release -a	Версия, название дистрибутива и дополнительная информация об операционной системе.
blkid	Список подключённых жестких дисков вместе с UUID.
lsblk	Список всех подключённых или созданных в системе блочных устройств.
df -h	Свободное пространство на диске.
df -T	Тип файловой системы.
sudo fdisk -l	Информация о размере диска.
sudo smartctl -a -i /dev/sda	Информация системы SMART жёсткого диска.
mount	Вывод списка смонтированных файловых систем. Каждая строка содержит информацию об имени устройства, директории, в которой оно смонтировано, типе и опциях монтирования в следующей форме: `<имя_устройства> on <директория> type <тип_файловой_системы> (<опции>)` Для отображения только ФС определенного типа используется опция -t.
lspci	Просмотр устройств, подключенных к PCI.
lsusb	Просмотр устройств, подключенных к USB.
uptime	Время работы системы.
ip addr	Информация о сети.
ps aux	Информация о запущенных процессах.

Рассмотрим вывод смонтированных разделов с типом файловой системы ext4:

```
mount -t ext4
```

Результат:

```
/dev/mapper/ro-root on / type ext4 (rw,relatime,seclabel)
/dev/sda1 on /boot type ext4 (rw,relatime,seclabel)
```

hardinfo – подробная информация о системе

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** hardinfo-0.5.2.git20201116-1

HardInfo — утилита просмотра подробной информации о системе и оборудовании. Утилита позволяет производить мониторинг системы в режиме реального времени, а также отображает информацию о запущенных процессах, загруженности процессора и занятости разделов на дисках.

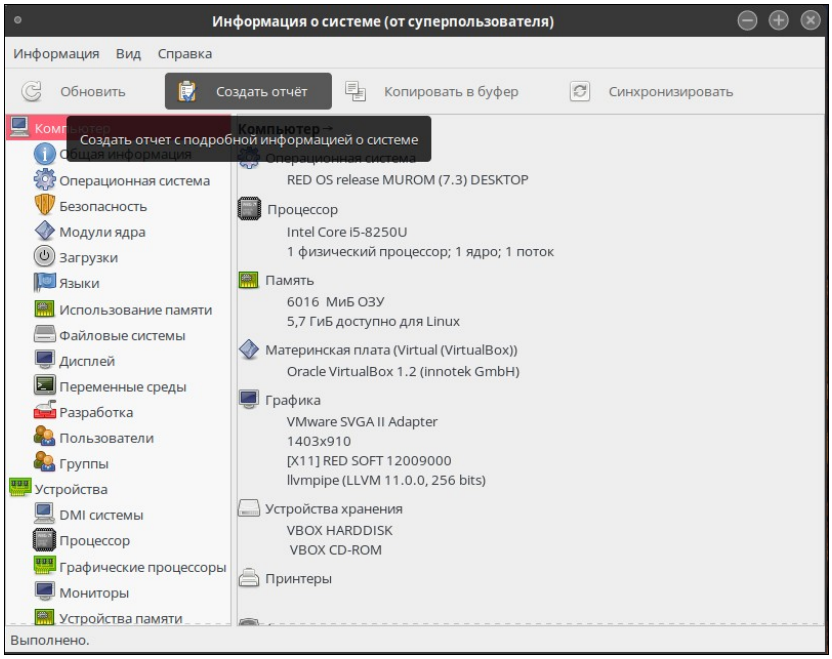
Установка **HardInfo** производится командой:

```
dnf install hardinfo
```

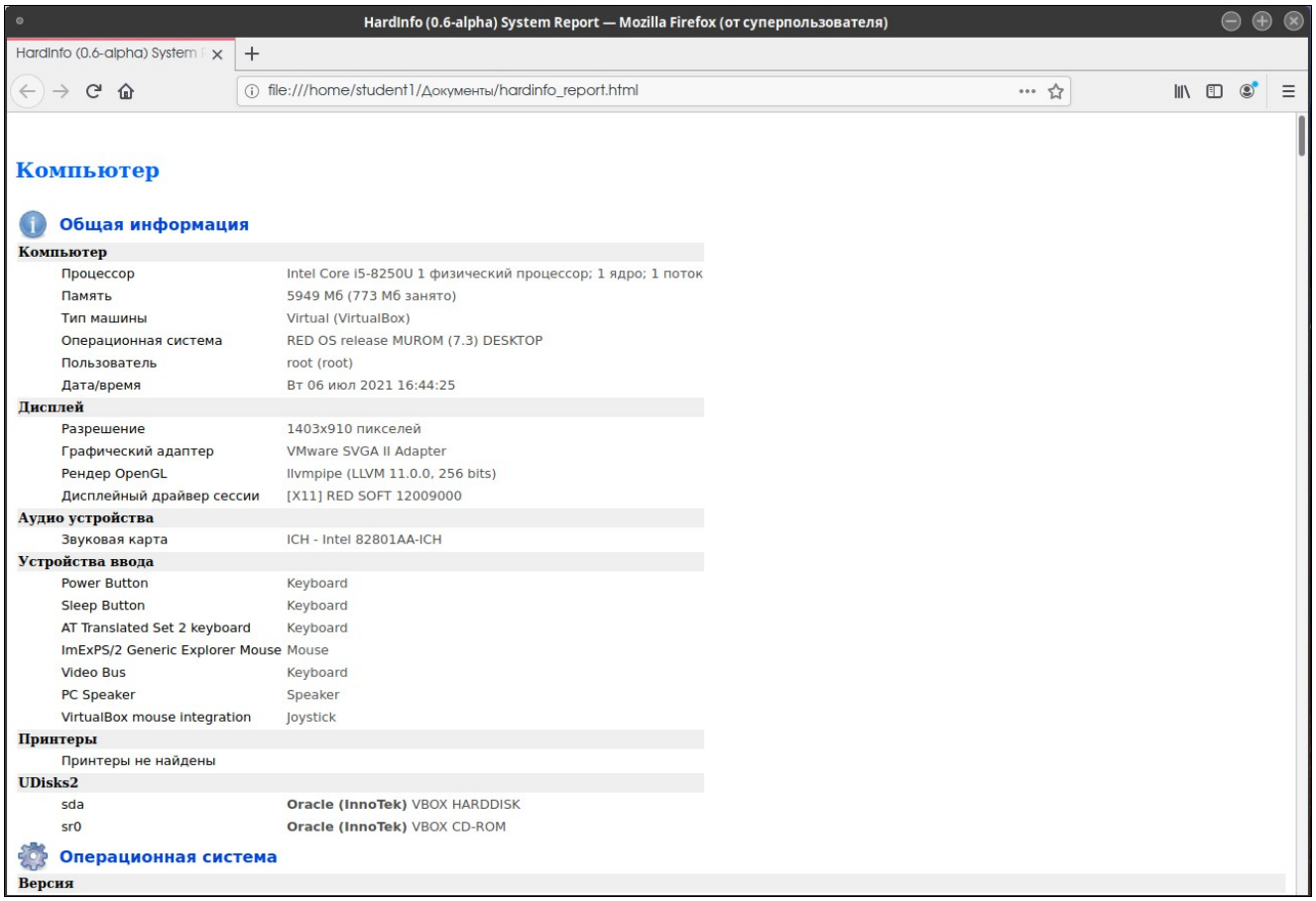
Запуск программы производится через «**Главное меню**» - «**Параметры**» - «**Информация о системе**» или командой:

```
hardinfo
```

Hardinfo позволяет создавать подробный отчёт с информацией о системе.



После создания отчёта его можно просматривать в браузере.



Компьютер

Общая информация

Компьютер	
Процессор	Intel Core i5-8250U 1 физический процессор; 1 ядро; 1 поток
Память	5949 Мб (773 Мб занято)
Тип машины	Virtual (VirtualBox)
Операционная система	RED OS release MUROM (7.3) DESKTOP
Пользователь	root (root)
Дата/время	Вт 06 июл 2021 16:44:25
Дисплей	
Разрешение	1403x910 пикселей
Графический адаптер	VMware SVGA II Adapter
Рендер OpenGL	llvmpipe (LLVM 11.0.0, 256 bits)
Дисплейный драйвер сессии	[X11] RED SOFT 12009000
Аудио устройства	
Звуковая карта	ICH - Intel 82801AA-ICH
Устройства ввода	
Power Button	Keyboard
Sleep Button	Keyboard
AT Translated Set 2 keyboard	Keyboard
ImExPS/2 Generic Explorer Mouse	Mouse
Video Bus	Keyboard
PC Speaker	Speaker
VirtualBox mouse integration	Joystick
Принтеры	
Принтеры не найдены	
UDisks2	
sda	**Oracle (InnoTek)** VBOX HARDDISK
sr0	**Oracle (InnoTek)** VBOX CD-ROM

Операционная система

Версия

hdparm – получение информации о параметрах жестких дисков

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** hdparm-9.58-1

hdparm —это утилита командной строки для Unix-подобных операционных систем. Утилита предназначена для регулировки и просмотра параметров жёстких дисков с интерфейсом *ATA*. Утилита может установить такие параметры как объём кеш-памяти накопителя, спящий режим, управление питанием, управление акустикой и настройки DMA.

Полезные параметры

-g	Отображает геометрию устройства (цилиндры, головки, сектора), размер (в секторах) устройства.
-h	Отображает краткую информацию об использовании (помощь).
-H	Считывает температуру некоторых устройств (большинство Hitachi). Также отображает предупреждение, если температура выше нормы.
-i	Отображает идентификационную информацию от драйвера устройства.
-I	Отображает идентификационную информацию прямо от устройства. Более детально.
-t	Отображает скорость чтения с диска, без кэширования данных.
-T	Отображает скорость чтения напрямую из кэша Linux-буфера, без доступа к диску.

Использование команды:

1) Без параметров:

```
sudo hdparm /dev/sda
```

```
/dev/sda:

 Model=VBOX HARDDISK, FwRev=1.0, SerialNo=VB2635c6c9-03c8cc84
 Config={ Fixed }
 RawCHS=16383/16/63, TrkSize=0, SectSize=512, ECCbytes=0
 BuffType=DualPortCache, BuffSize=256kB, MaxMultSect=128, MultSect=128
 CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=209715200
 IORDY=yes, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
 PIO modes:  pio0 pio3 pio4
 DMA modes:  mdma0 mdma1 mdma2
 UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5 udma6
 AdvancedPM=no WriteCache=enabled
```

2) Вывод информации о жестком диске:

```
sudo hdparm -i /dev/sda
```

```
/dev/sda:

 Model=VBOX HARDDISK, FwRev=1.0, SerialNo=VB2635c6c9-03c8cc84
 Config={ Fixed }
 RawCHS=16383/16/63, TrkSize=0, SectSize=512, ECCbytes=0
 BuffType=DualPortCache, BuffSize=256kB, MaxMultSect=128, MultSect=128
 CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=209715200
 IORDY=yes, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
 PIO modes:  pio0 pio3 pio4
 DMA modes:  mdma0 mdma1 mdma2
 UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5 udma6
 AdvancedPM=no WriteCache=enabled
 Drive conforms to: unknown:  ATA/ATAPI-1,2,3,4,5,6

 * signifies the current active mode
```

3) Отображение краткой информации о диске, текущая температура:

```
sudo hdparm -iH /dev/sda
```

```
/dev/sda:
SG_IO: bad/missing sense data, sb[]:  70 00 05 00 00 00 00 0a 04 41 e0 00 21 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 drive temperature (celsius) is:  -18
 drive temperature in range:  yes
 Model=VBOX HARDDISK, FwRev=1.0, SerialNo=VB2635c6c9-03c8cc84
 Config={ Fixed }
 RawCHS=16383/16/63, TrkSize=0, SectSize=512, ECCbytes=0
 BuffType=DualPortCache, BuffSize=256kB, MaxMultSect=128, MultSect=128
 CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=209715200
 IORDY=yes, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
 PIO modes:  pio0 pio3 pio4
 DMA modes:  mdma0 mdma1 mdma2
 UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5 udma6
 AdvancedPM=no WriteCache=enabled
 Drive conforms to: unknown:  ATA/ATAPI-1,2,3,4,5,6

 * signifies the current active mode
```

4) Скорость чтения данных с диска:

```
sudo hdparm -tT /dev/sda
```

```
/dev/sda:
 Timing cached reads:   20732 MB in  1.99 seconds = 10424.68 MB/sec

 Timing buffered disk reads: 238 MB in  3.02 seconds =  78.72 MB/sec
```

smartctl и hddtemp – мониторинг состояния жестких дисков

Для успешного прохождения тестов утилит **smartctl** и **hddtemp** жесткие диски должны поддерживать *SMART*.

Проверка, включена ли интеллектуальная функция для диска.

1) Определение дисков в системе:

```
sudo smartctl --scan
```

Отобразится список дисков в вашем компьютере:

```
/dev/sda -d scsi # /dev/sda, SCSI device
```

2) Информация о диске:

```
sudo smartctl -i /dev/sda
```

Пример:

```
=== START OF INFORMATION SECTION ===
Model Family:     Toshiba 2.5" HDD MK..65GSX
Device Model:     TOSHIBA MK3265GSXN
Serial Number:    3192P99AT
LU WWN Device Id: 5 000039 322201685
Firmware Version: GH101M
User Capacity:    320 072 933 376 bytes [320 GB]
Sector Size:      512 bytes logical/physical
Rotation Rate:    5400 rpm
Form Factor:      2.5 inches
Device is:        In smartctl database [for details use: -P show]
ATA Version is:   ATA8-ACS (minor revision not indicated)
SATA Version is:  SATA 2.6, 3.0 Gb/s (current: 3.0 Gb/s)
Local Time is:    Mon Mar  5 00:02:01 2018 MSK
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

3) Подробная информация о состоянии:

```
sudo smartctl -A /dev/sda
```

Пример:

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000b   100   100   050    Pre-fail  Always       -       0
  2 Throughput_Performance  0x0005   100   100   050    Pre-fail  Offline      -       0
  3 Spin_Up_Time            0x0027   100   100   001    Pre-fail  Always       -       1141
  4 Start_Stop_Count        0x0032   100   100   000    Old_age   Always       -       7407
  5 Reallocated_Sector_Ct   0x0033   100   100   050    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000b   100   100   050    Pre-fail  Always       -       0
  8 Seek_Time_Performance   0x0005   100   100   050    Pre-fail  Offline      -       0
  9 Power_On_Hours          0x0032   058   058   000    Old_age   Always       -       17038
 10 Spin_Retry_Count        0x0033   245   100   030    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -       7224
191 G-Sense_Error_Rate      0x0032   100   100   000    Old_age   Always       -       176
192 Power-Off_Retract_Count 0x0032   098   098   000    Old_age   Always       -       1279
193 Load_Cycle_Count        0x0032   047   047   000    Old_age   Always       -       531423
194 Temperature_Celsius     0x0022   100   100   000    Old_age   Always       -       39 (Min/Max 10/53)
196 Reallocated_Event_Count 0x0032   100   100   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0032   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0030   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x0032   200   200   000    Old_age   Always       -       1
220 Disk_Shift              0x0002   100   100   000    Old_age   Always       -       89
222 Loaded_Hours            0x0032   070   070   000    Old_age   Always       -       12360
223 Load_Retry_Count        0x0032   100   100   000    Old_age   Always       -       0
224 Load_Friction           0x0022   100   100   000    Old_age   Always       -       0
```

```
226 Load-in_Time          0x0026   100   100   000    Old_age   Always       -       309
240 Head_Flying_Hours     0x0001   100   100   001    Pre-fail  Offline      -       0
```

Ключевое значение имеет содержимое 3-х столбцов:

- **VALUE** - текущее значение параметра;
- **WORST** - наихудшее значение, которого когда-либо достигало значение *Value*;
- **THRESH** - значение, которое должен достигнуть *Value* этого же атрибута, чтобы состояние атрибута было признано критическим.

Критичным является поле **WHEN_FAILED**, если оно имеет значение **FAIL**, то высока вероятность выхода жесткого диска из строя в ближайшее время.

4) Проверка жесткого диска на наличие критических ошибок:

```
sudo smartctl -H /dev/sda
```

Пример:

```
=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED
```

Если результат не **PASSED**, то диск следует заменить.

5) Расширенные встроенные тесты:

```
sudo smartctl --test=long /dev/sda
```

Пример:

```
=== START OF OFFLINE IMMEDIATE AND SELF-TEST SECTION ===
Sending command: "Execute SMART Extended self-test routine immediately in off-line mode".
Drive command "Execute SMART Extended self-test routine immediately in off-line mode" successful.
Testing has begun.
Please wait 98 minutes for test to complete.
Test will complete after Mon Mar  5 01:46:10 2018
```

Для прерывания теста используйте:

```
sudo smartctl -X
```

Для просмотра результатов выполнения тестов используется команда вывода внутреннего журнала после завершения теста:

```
sudo smartctl -l selftest /dev/sda
```

Для просмотра температуры используется утилита **hddtemp**. Просмотреть температуру можно командой:

```
hddtemp /dev/sda
```

Вывод команды:

```
/dev/sda: SILICONMOTION SM223AC: 0°C
```

sysbench - утилита тестирования производительности

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** sysbench 1.0.17-2

sysbench — многоцелевая утилита для тестирования производительности с открытым исходным кодом, она позволяет оценить параметры производительности процессора, памяти и файловой системы.

Установка **sysbench** производится командой:

```
dnf install sysbench
```

Синтаксис использования утилиты:

```
sysbench <основные_опции> --test=<имя_теста> <опции> <команда>
```

Основные опции:

- **--num-threads=N** — число потоков [1];
- **--max-requests=N** — ограничение общего кол-ва запросов [10000].

Используемые команды:

- **prepare** — подготовка теста (создание таблиц, вставка данных и т.п.);
- **run** — выполнение теста;
- **cleanup** — очистка данных (после этапа подготовки);
- **help** — вывод дополнительных параметров теста.

Тестирование производительности процессоров (--test=cpu):

```
sysbench --test=cpu run

Running the test with following options:
Number of threads: 1
Initializing random number generator fr om current time


Prime numbers lim it: 10000

Initializing worker threads...

Threads started!

CPU speed:
  events per second:  1085.35

General statistics:
  total time:                          10.0007s
  total number of events:              10856

Latency (ms):
    min:                                    0.85
    avg:                                    0.92
    max:                                    5.18
    95th percentile:                        0.97
    sum:                                 9991.47

Threads fairness:
  events (avg/stddev):           10856.0000/0.00
  execution time (avg/stddev):   9.9915/0.00
```

Тестирование производительности последовательных операций чтения/записи в оперативную память (--test=memory)

```
sysbench --test=memory run

Running memory speed test with the following options:
  block size: 1KiB
  total size: 102400MiB
  operation: write
  scope: global

Initializing worker threads...

Threads started!

Total operations: 52150080 (5212932.28 per second)

50927.81 MiB transferred (5090.75 MiB/sec)


General statistics:
  total time:                          10.0001s
  total number of events:              52150080

Latency (ms):
    min:                                    0.00
    avg:                                    0.00
    max:                                    2.39
    95th percentile:                        0.00
    sum:                                 4543.73

Threads fairness:
  events (avg/stddev):           52150080.0000/0.00
  execution time (avg/stddev):   4.5437/0.00
```

Тестирование разнообразной нагрузки на файловую подсистему (--test=fileio)

```
sysbench --test=fileio --file-test- mode=seqwr run
Running the test with following options:
Number of threads: 1
Initializing random number generator from current time


Extra file open flags: (none)
128 files, 16MiB each
2GiB total file size
Block size 16KiB
Periodic FSYNC enabled, calling fsync() each 100 requests.
Calling fsync() at the end of test, Enabled.
Using synchronous I/O mode
Doing sequential write (creation) test
Initializing worker threads...

Threads started!


File operations:
  reads/s:                      0.00
  writes/s:                     22474.07
  fsyncs/s:                     28776.01

Throughput:
  read, MiB/s:                  0.00
  written, MiB/s:               351.16

General statistics:
  total time:                          10.0012s
  total number of events:              512508

Latency (ms):
    min:                                    0.00
    avg:                                    0.02
    max:                                   11.48
    95th percentile:                        0.08
```

```
    sum:                                  9805.95

Threads fairness:
    events (avg/stddev):           512508.0000/0.00
    execution time (avg/stddev):   9.8060/0.00
```

glxgear и glxinfo – тестирование производительности графического ускорителя

3D-ускорение
Проверка производительности

glxgears - это популярный OpenGL-тест, который входит в пакет утилит **mesa-utils**.

3D-ускорение

Чтобы определить, работает ли 3D-ускорение, используйте утилиту **glxinfo**. Выполните команду:

```
glxinfo  | grep rendering
```

Вывод должен быть примерно следующим:

```
direct rendering: Yes
```

Проверка производительности

Чтобы узнать, сколько кадров в секунду (fps) выдает ваша видеокарта, запустите следующую команду:

```
glxgears -info
```

Примечание! Этот тест (с шестернёй) не очень эффективный, многие драйвера могут хорошо работать, но при этом показывать мало FPS в этом тесте.

Чтобы запустить **glxgears** с отключенной вертикальной синхронизацией, запустите следующую команду:

```
vblank_mode=0 glxgears
```

sensors - утилита для мониторинга датчиков температуры

Данная утилита - свободное ПО, состоящее из драйверов и утилит, позволяющее отслеживать температуру, напряжение, скорость вращения вентиляторов в вашей системе. Следует помнить, что набор датчиков индивидуален для каждой системы, поэтому некоторые возможности могут быть недоступны.

Используйте **sensors-detect** для обнаружения и формирования списка модулей ядра.

По окончании определения датчиков будут доступны снимаемые ими значения.

Пример:

sensors-detect

```
This program will help you determine which kernel modules you need
to load to use lm_sensors most effectively. It is generally safe
and recommended to accept the default answers to all questions,
unless you know what you're doing.

Some south bridges, CPUs or memory controllers contain embedded sensors.
Do you want to scan for them? This is totally safe. (YES/no):
Module cpuid loaded successfully.
Silicon Integrated Systems SIS5595...                       No
VIA VT82C686 Integrated Sensors...                          No
VIA VT8231 Integrated Sensors...                            No
AMD K8 thermal sensors...                                   No
AMD Family 10h thermal sensors...                           No
...
Now follows a summary of the probes I have just done.
Just press ENTER to continue:
Driver `coretemp':
* Chip `Intel digital thermal sensor' (confidence: 9)
Driver `lm90':
* Bus `SMBus nForce2 adapter at 4d00'
  Busdriver `i2c_nforce2', I2C address 0x4c
  Chip `Winbond W83L771AWG/ASG' (confidence: 6)
Do you want to overwrite /etc/conf.d/lm_sensors? (YES/no):
ln -s '/usr/lib/systemd/system/lm_sensors.service' '/etc/systemd/system/multi-user.target.wants/lm_sensors.service'
Unloading i2c-dev... OK
Unloading cpuid... OK
```

Просмотр датчиков

Пример запуска *sensors*:

sensors

```
coretemp-isa-0000
Adapter: ISA adapter
Core 0:       +58.0°C  (high = +84.0°C, crit = +100.0°C)
Core 1:       +59.0°C  (high = +84.0°C, crit = +100.0°C)
Core 2:       +59.0°C  (high = +84.0°C, crit = +100.0°C)
Core 3:       +60.0°C  (high = +84.0°C, crit = +100.0°C)

nouveau-pci-0100
Adapter: PCI adapter
temp1:        +57.0°C  (high = +95.0°C, hyst =  +3.0°C)
                       (crit = +105.0°C, hyst =  +5.0°C)
                       (emerg = +135.0°C, hyst =  +5.0°C)
```

screentest – утилита тестирования мониторов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** screentest-2.0-2

screentest — небольшая утилита тестирования мониторов. Отображаемые тестовые экранные шаблоны помогут быстро оценить качество монитора и с лёгкостью выявить дефекты. Имеющиеся тесты являются гораздо более показательными в оценке недостатков мониторов, чем обычные фотографии (картинки).

Вы можете подробнее ознакомиться с работой утилиты **screentest**, просмотрев наши обучающие видео:

- на **RuTube** — screentest - утилита тестирования мониторов;
- в **Яндекс.Дзен** — screentest - утилита тестирования мониторов;
- в **VK Видео** — screentest - утилита тестирования мониторов.

На наших каналах вы также сможете найти много другой полезной информации.

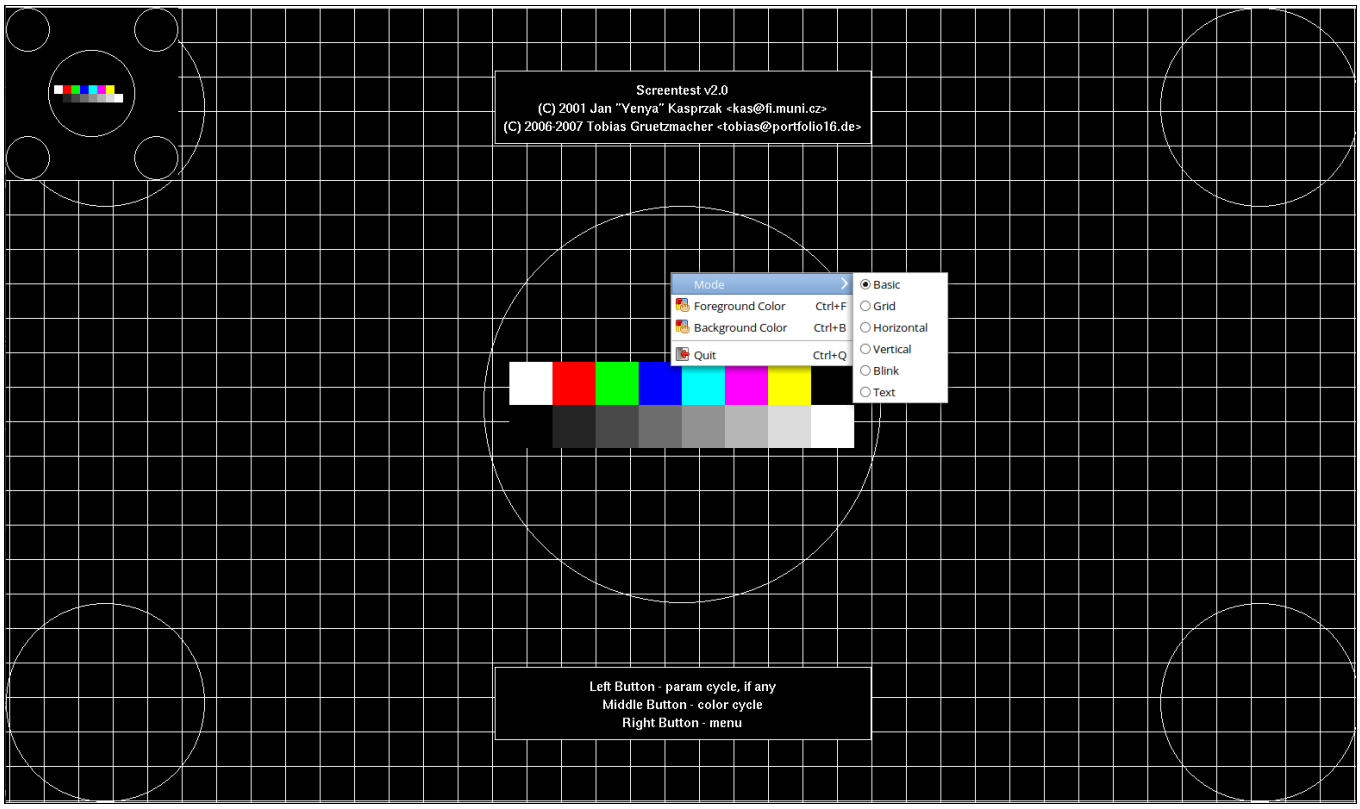
Установка **screentest** производится командой:

```
dnf install screentest
```

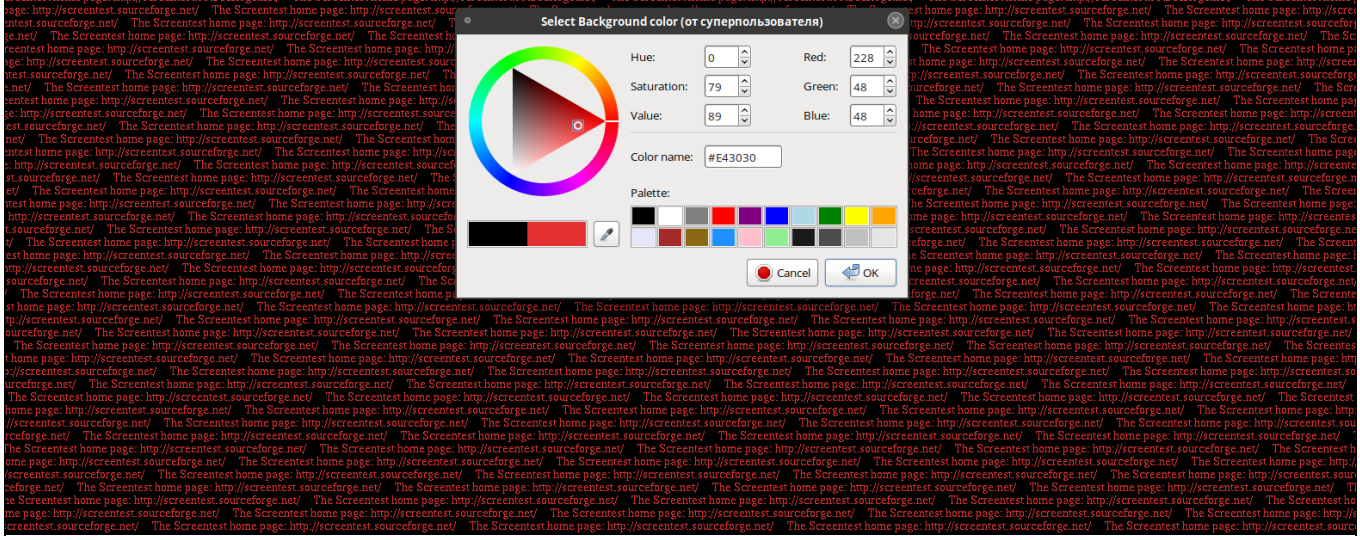
Для старта теста запустим утилиту в терминале:

```
screentest
```

Тест и его настройки выглядят следующим образом:



Screentest имеет множество различных настроек, что позволяет быстро и качественно выявить любые дефекты монитора.


Select Background color (от суперпользователя)
Hue:
0
Saturation:
79
Value:
89
Red:
228
Green:
48
Blue:
48
Color name:
#E43030
Palette:
Cancel
OK

glmark2 – тестирование графических процессоров

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** glmark2-2017.07-2.20180717git0003eff

glmark2 — утилита для тестирования видеокарт (графических процессоров).

glmark2 без дополнительных опций запускает полную серию тестов, визуально выглядящих как различного вида двух- и трёхмерная анимация, в терминале одновременно будут выводится измеренные значения **FPS** (количество сменяемых кадров за единицу времени).

Установка **Glmark2** производится командой:

```
dnf install glmark2
```

Тест производительности видеокарты будет выглядеть следующим образом:

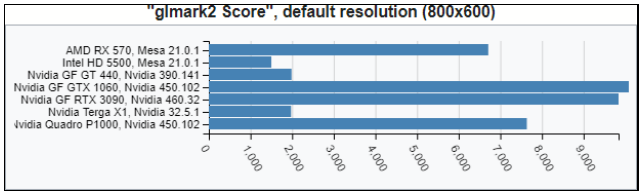




Результаты тестов выводятся в формате набранных баллов.

```
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[function] fragment-complexity=medium:fragment-steps=5: FPS: 147 FrameTime: 6.80
3 ms
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[loop] fragment-loop=false:fragment-steps=5:vertex-steps=5: FPS: 185 FrameTime:
5.405 ms
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[loop] fragment-steps=5:fragment-uniform=false:vertex-steps=5: FPS: 186 FrameTim
e: 5.376 ms
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[loop] fragment-steps=5:fragment-uniform=true:vertex-steps=5: FPS: 163 FrameTime
: 6.135 ms
=======================================================
                                  glmark2 Score: 164
=======================================================
```

Для сравнения ниже приведены результаты тестирования наиболее распространённых видеокарт.



Также следует понимать, что **glmark2** по умолчанию запускает тест в маленьком окне **800x600**, для того чтобы открыть тест с желаемым разрешением, достаточно прописать «**glmark2 -s 1920x1080**» (в этом случае тест будет производится с разрешением **1920x1080**).

Однако следует понимать, что результаты теста при изменении разрешения могут существенно отличаться.

stress-ng – утилита нагрузочного тестирования аппаратного обеспечения

stress-ng — специализированная консольная утилита для проведения нагрузочного стресс-тестирования аппаратного обеспечения различными способами.

Вы можете подробнее ознакомиться с примером использования утилиты для проведения тестирования аппаратного обеспечения ПК, просмотрев наши обучающие видео:

- на **RuTube** — Информация, мониторинг и тестирование системы;
- в **Яндекс.Дзен** — Информация, мониторинг и тестирование системы;
- в **VK Видео** — Информация, мониторинг и тестирование системы.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты необходимо выполнить команду (с правами **администратора** системы):

```
dnf in stress-ng
```

Тестирование процессора

Для подавляющего большинства ситуаций классическим примером стресс-теста можно использовать тест, выполняемый следующей командой:

```
stress-ng --cpu 16 --cpu-method matrixprod --metrics --timeout 60
```

В данном тесте задействованы 16 потоков для тестирования 16-поточного процессора. Естественно, количество потоков следует задавать в соответствии со спецификацией используемого процессора.

Тестирование дисковой подсистемы

Для проведения стресс-тестирования накопителей, таких как жёсткие диски, можно для начала провести низкоуровневый тест ввода/вывода, данный тест требует **root**-прав:

```
stress-ng --sequential 0 --class io --timeout 60s --metrics-brief
```

Тестирование памяти

Чтобы провести стресс-тест памяти, используйте команду:

```
stress-ng --sequential 0 --class memory --timeout 60s --metrics-brief
```

Комплексное тестирование

Если необходимо провести комплексное стресс-тестирование, можно задействовать работу нескольких основных подсистем вместе одной командой:

```
stress-ng --cpu 4 --io 4 --vm 1 --vm-bytes 1G --timeout 60s --metrics-brief
```

Проверка состояния жесткого диска

Smartmontools
Gsmartcontrol
Gnome disk utility
BadBlocks

Smartmontools

Smartmontools — утилита, предназначенная для проверки состояния жесткого диска. Чтобы посмотреть количество установленных жестких дисков наберите команду:

```
$ sudo smartctl --scan
```

На запрос пароля привилегированного пользователя, введите пароль локального пользователя с правами администратора.

Чтобы посмотреть информацию о жестком диске, а также узнать, поддерживает ли он технологию анализа SMART и включена ли она, наберите команду:

```
smartctl -i /dev/sda

smartctl 6.6 2018-08-10 r4748 [x86_64-linux-4.19.56-2.el7.x86_64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org
=== START OF INFORMATION SECTION ===
Model Family: Seagate Barracuda 3.5
Device Model: ST1000DM010-2EP102
Serial Number: ZN179JYJ
LU WWN Device Id: 5 000c50 0b6491aa4
Firmware Version: CC43
User Capacity: 1 000 204 886 016 bytes [1,00 TB]
Sector Sizes: 512 bytes logical, 4096 bytes physical
Rotation Rate: 7200 rpm
Form Factor: 3.5 inches
Device is: In smartctl database [for details use: -P show]
ATA Version is: ATA8-ACS T13/1699-D revision 4
SATA Version is: SATA 3.0, 6.0 Gb/s (current: 3.0 Gb/s)
Local Time is: Thu Aug 22 14:01:23 2019 MSK
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

В данном выводе указана информация о вашем жестком диске.

SMART support is: Available - device has SMART capability — жесткий диск поддерживает технологию анализа SMART. Если технология не поддерживается, вместо слова **Available** будет **Unavailable**.

SMART support is: Enabled — технология анализа SMART включена. Если она выключена у вас, то для включения введите:

```
smartctl -s on /dev/sda
```

Для выключения:

```
smartctl -s off /dev/sda
```

Для вывода атрибутов SMART введите:

```
smartctl -A /dev/sda
```

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 10
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000f   080   072   006    Pre-fail  Always       -       110427890
  3 Spin_Up_Time            0x0003   097   097   000    Pre-fail  Always       -       0
  4 Start_Stop_Count        0x0032   100   100   020    Old_age   Always       -       25
  5 Reallocated_Sector_Ct   0x0033   100   100   010    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000f   100   253   045    Pre-fail  Always       -       716102
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       42
 10 Spin_Retry_Count        0x0013   100   100   097    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   020    Old_age   Always       -       25
183 Runtime_Bad_Block       0x0032   100   100   000    Old_age   Always       -       0
184 End-to-End_Error        0x0032   100   100   099    Old_age   Always       -       0
187 Reported_Uncorrect      0x0032   100   100   000    Old_age   Always       -       0
188 Command_Timeout         0x0032   100   100   000    Old_age   Always       -       0 0 0
189 High_Fly_Writes         0x003a   100   100   000    Old_age   Always       -       0
190 Airflow_Temperature_Cel 0x0022   070   059   040    Old_age   Always       -       30 (Min/Max 24/30)
193 Load_Cycle_Count        0x0032   100   100   000    Old_age   Always       -       25
194 Temperature_Celsius     0x0022   030   021   000    Old_age   Always       -       30 (0 21 0 0 0)
195 Hardware_ECC_Recovered  0x001a   003   003   000    Old_age   Always       -       110427890
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   200   200   000    Old_age   Always       -       0
240 Head_Flying_Hours       0x0000   100   253   000    Old_age   Offline      -       42h+36m+02.609s
241 Total_LBAs_Written      0x0000   100   253   000    Old_age   Offline      -       85113048
242 Total_LBAs_Read         0x0000   100   253   000    Old_age   Offline      -       25314842
```

В данном выводе стоит смотреть на значения в колонке **RAW_VALUE**.

Наиболее важные атрибуты отмечены как **pre_fail** в колонке **TYPE**.
1 Raw_Read_Error_Rate — количество ошибок чтения. На дисках Seagate и Samsung большие значения - норма.

2 Spin_Up_Time — время раскрутки диска из состояния покоя до рабочей скорости. Растет при износе диска.

5 Rellocated Sector Count — количество переназначенных секторов. Если диск обнаружил ошибку чтения/записи он перенесет сектор в резерв. Чем меньше значение, тем лучше.

7 Seek Error Rate — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики или поверхности жёсткого диска.

196 Rellocation Event Count - число операций переназначения. **Raw Value** хранит общее число попыток переноса информации с переназначенных секторов в резервную область как успешных так и провальных.
Более подробную информацию можно найти на странице википедии.

Для того, чтобы провести тест самодиагностики, наберите команду:

```
smartctl -t <тип_теста> /dev/sda
```

Тип теста может быть:

- **long** — расширенный;
- **short** — короткий;
- **conveyance** — тест на выявления ошибок при записи/чтении.

Тесты выполняются в фоновом режиме. Чтобы просмотреть результат, наберите:

```
smartctl -l selftest /dev/sda

=== START OF READ SMART DATA SECTION ===
SMART Self-test log structure revision number 1
Num Test_Description Status Remaining LifeTime(hours) LBA_of_first_error
# 1 Conveyance offline Self-test routine in progress 60% 43 -
# 2 Short offline Completed without error 00% 42 -
# 3 Short offline Aborted by host 90% 42 -
# 4 Short captive Completed without error 00% 41 -
# 5 Short offline Completed without error 00% 41 -
```

Completed without error означает, что тест завершился без ошибок.

Для просмотра полной информации, включающей в себя показатели атрибутов SMART, информацию о жестком диске и результаты диагностических тестов, наберите:

```
$ sudo smartctl -a /dev/sda
```

Gsmartcontrol

Gsmartcontrol — это графическая утилита к **smartctl**, позволяющая оценивать состояние и работоспособность жёсткого диска или

твердотельного накопителя по показаниям S.M.A.R.T.

Основными возможностями программы являются:

- вывод информации об ошибках работы дисков;
- отображение информации о дисках, атрибутов, статистики;
- включение/выключение автоматического сбора данных о состоянии дисков;
- выполнение тестов «SMART self-tests»;
- включение/выключение SMART;
- создание отчетов по проведенным тестам.

Вы можете подробнее ознакомиться с информацией о проверке состояния жесткого диска, просмотрев наши обучающие видео:

- на **RuTube** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **Яндекс.Дзен** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **VK Видео** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install gsmartcontrol
```

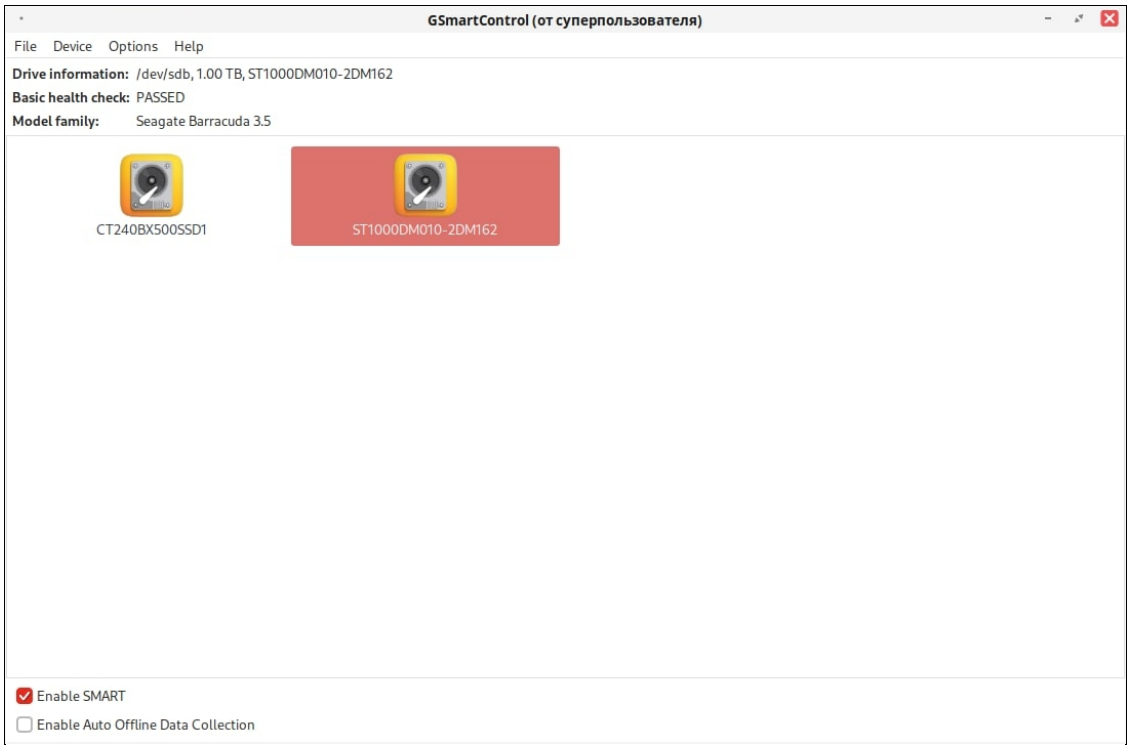
После установки программа будет доступна из «**Главного меню**» - «**Системные**» - «**Контроль S.M.A.R.T.**» или при помощи команды в терминале:

```
gsmartcontrol
```

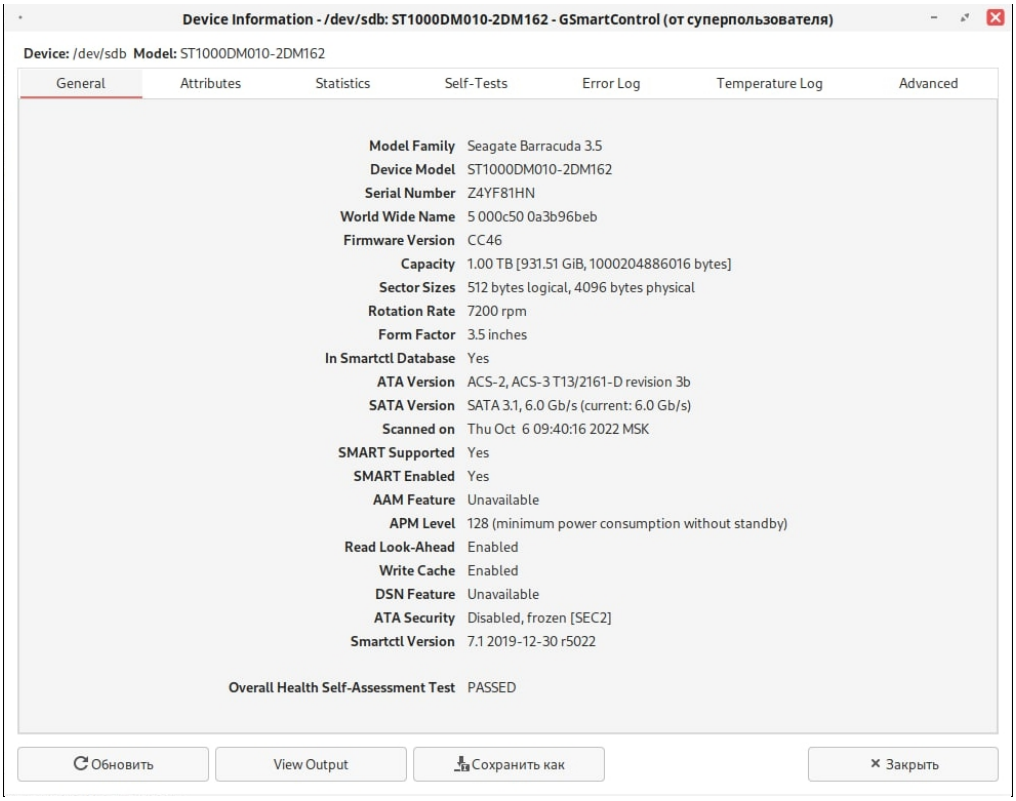
Обратите внимание, что для работы с утилитой необходимы права администратора или суперпользователя (**root**) системы.

Работа с утилитой

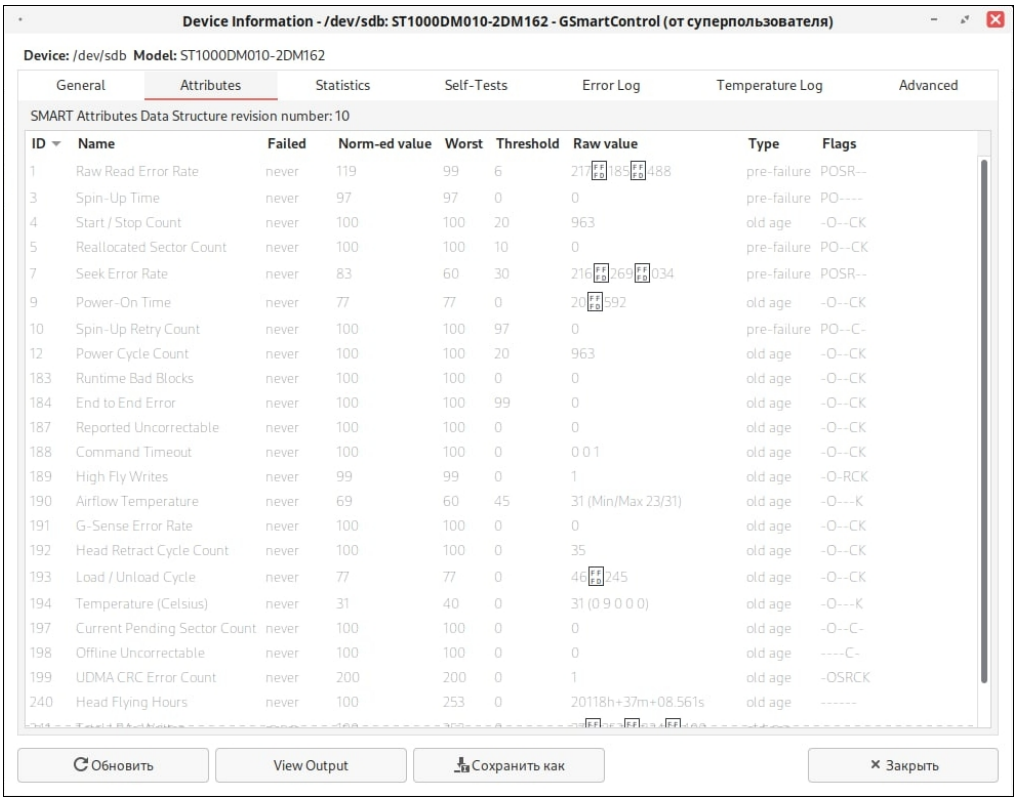
При запуске программа выглядит следующим образом:



Здесь отображены все диски, доступные для сканирования. При нажатии ПКМ на нужный диск выберите «**View details**», на вкладке «**General**» будет выведена вся информация о диске.



На вкладке «**Attributes**» указаны атрибуты проверки, нормальное, плохое и пороговое значение для каждого атрибута для удобного ориентирования по выявленным значениям в ходе проверок диска.



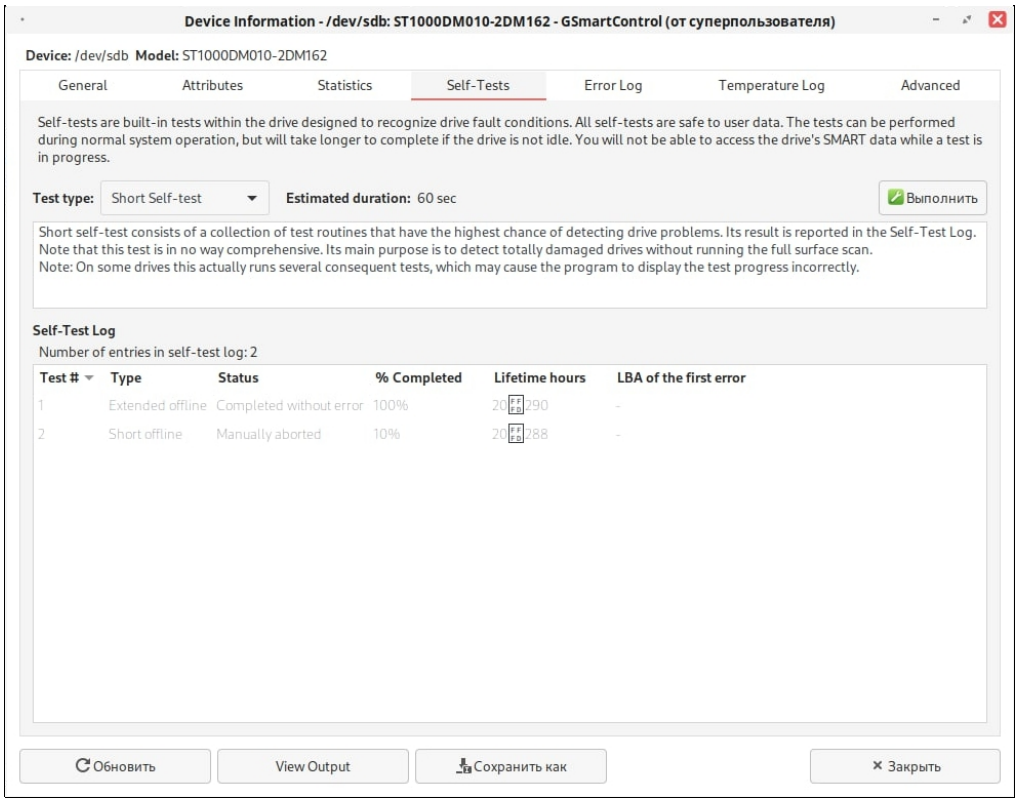
Часто используемые атрибуты:

- **Raw Read Error Rate** — частота ошибок при чтении данных с диска, происхождение которых обусловлено аппаратной частью диска, если значение большое, значит ошибки встречаются редко;
- **Spin-Up Time** — время раскрутки пакета дисков из состояния покоя до рабочей скорости, значение возрастает при износе диска;
- **Start/Stop Count** — полное число циклов запуск-остановка шпинделя. У дисков некоторых производителей (например, Seagate) — счётчик включения режима энергосбережения. В поле raw value хранится общее количество запусков/остановок диска;
- **Reallocated Sectors Count** — число операций переназначения секторов. Когда диск обнаруживает ошибку чтения/записи, он помечает сектор «переназначенным» и переносит данные в специально отведённую резервную область. Чем больше значение, тем хуже состояние поверхности дисков. Поле raw value содержит общее количество переназначенных секторов;
- **Seek Error Rat**e — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики и/или поверхности жёсткого диска;
- **Power-On Time** — число часов (минут, секунд — в зависимости от производителя), проведённых во включенном состоянии;
- **Spin-Up Retry Count** — число повторных попыток раскрутки дисков до рабочей скорости в случае, если первая попытка была неудачной. Если значение атрибута увеличивается, то велика вероятность неполадок с механической частью;
- **Power Cycle Count** — количество полных циклов включения-выключения диска;
- **End-to-End error** — данный атрибут - часть технологии HP SMART IV - означает, что после передачи данных через кэш-память чётность данных между хостом и жестким диском не совпадает;
- **Reported Uncorrectable** — ошибки, которые не могли быть восстановлены, используя методы устранения ошибки аппаратными средствами;
- **Command Timeout** — количество прерванных операций в связи с HDD тайм-аут. Обычно это значение атрибута должно быть равно нулю, и, если значение гораздо выше нуля, то, скорее всего, там будут какие-то серьезные проблемы с питанием или окисленные кабели для передачи данных;
- **Airflow Temperature** — температура воздуха внутри корпуса жёсткого диска;
- **G-sense Error Rate** — количество ошибок, возникающих в результате ударных нагрузок. Атрибут хранит показания встроенного акселерометра, который фиксирует все удары, толчки, падения и даже неаккуратную установку диска в корпус компьютера;
- **Load/Unload Cycle** — количество циклов перемещения блока магнитных головок в парковочную зону / в рабочее положение;
- **Temperature** — температура жёсткого диска;
- **Current Pending Sector Count** — число секторов, являющихся кандидатами на замену. Они пока не определены как плохие, но считывание с них отличается от чтения стабильного сектора, это так называемые подозрительные или нестабильные сектора;
- **Head flying hours** — время позиционирования головок.

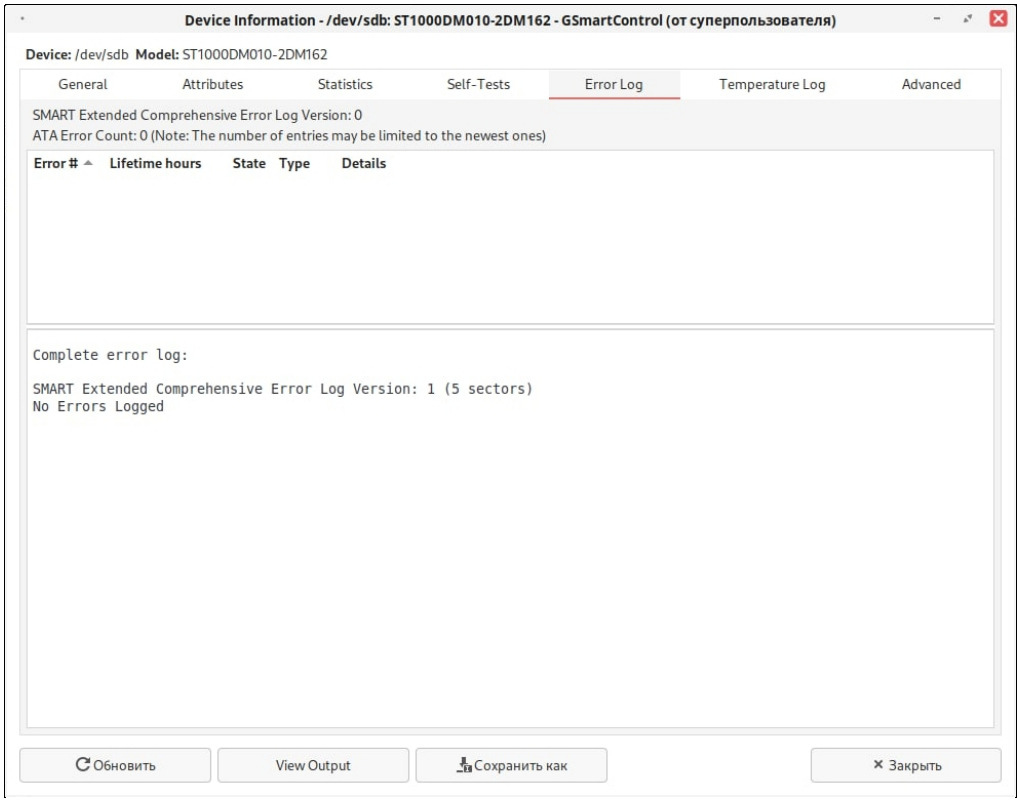
На вкладке «**Statistics**» выводится статистика использования диска.

На вкладке «**Self-Tests**» можно выполнять проверки жесткого диска. Доступно три варианта проверки:

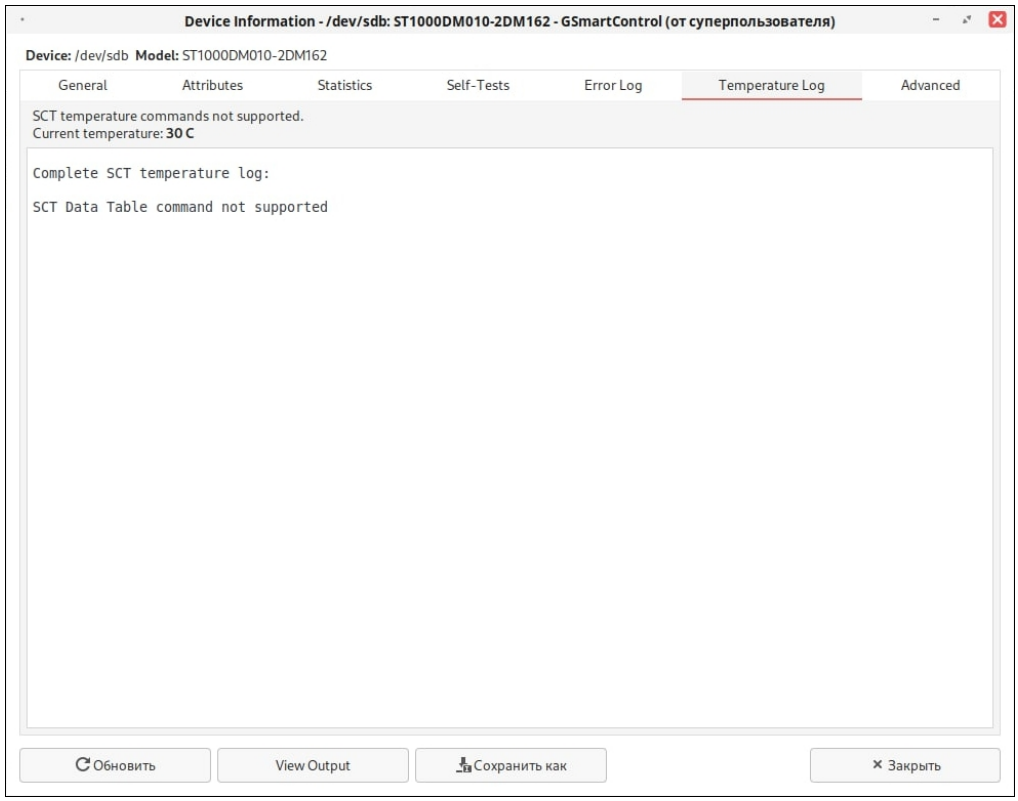
- **Быстрый тест** — продолжительностью 1 мин.
- **Расширенный тест** — продолжительностью более 1 часа, полный тест с процедурами проверки и пр.
- **Тест передачи** — продолжительностью 2 мин., тест подходит для обнаружения физических сбоев.



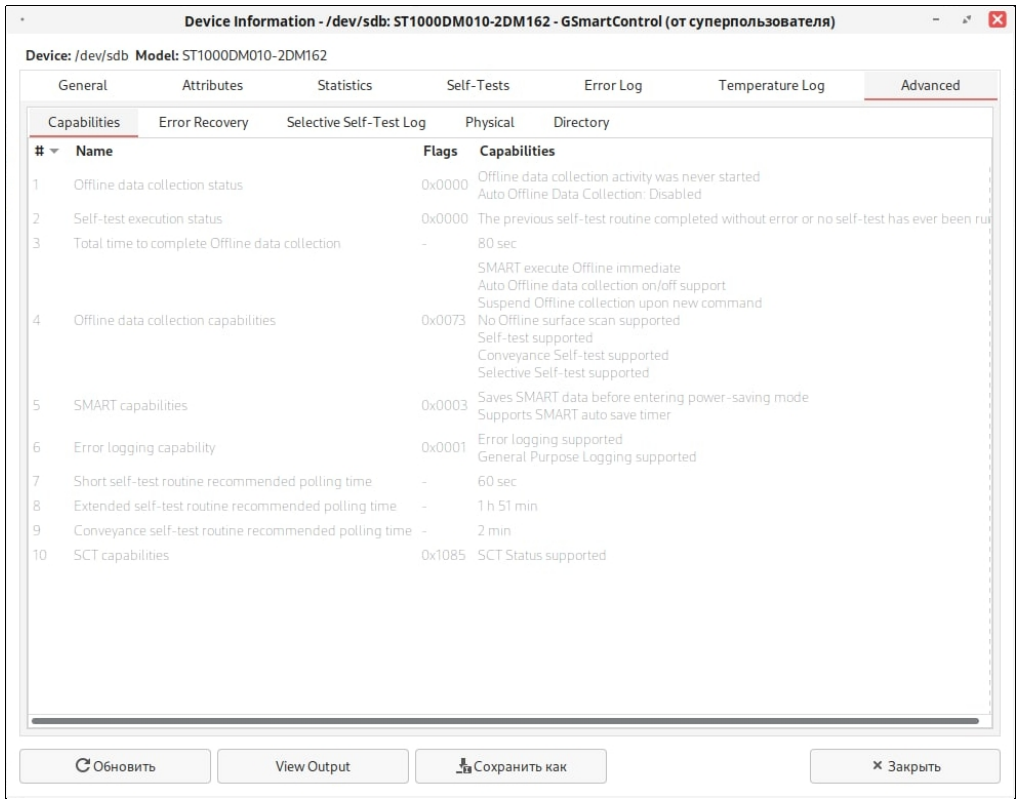
На вкладке «**Error Log**» ведется журнал ошибок с указанием деталей и подробным описанием при выборе любой из выявленных ошибок.



На вкладке «**Temperature Log**» ведется учет температурного режима используемого диска (если поддерживается).



На вкладке «**Advanced**» отображаются дополнительные параметры.



Все представленные утилитой результаты проверок можно сохранить в текстовом формате, например, для передачи информации о состоянии диска в сервисные центры или техническую поддержу.

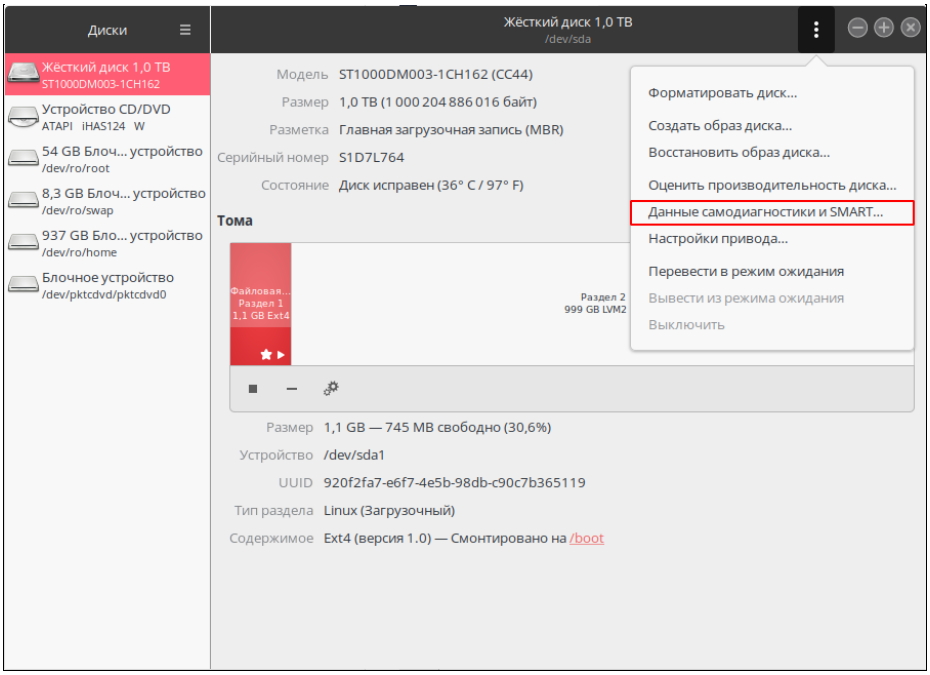
Gnome disk utility

Gnome disk utility — утилита с графической оболочкой для просмотра информации атрибутов SMART и тестирования диска. Для установки воспользуйтесь утилитой **yum** или **dnf** в зависимости от используемой версии РЕД ОС.

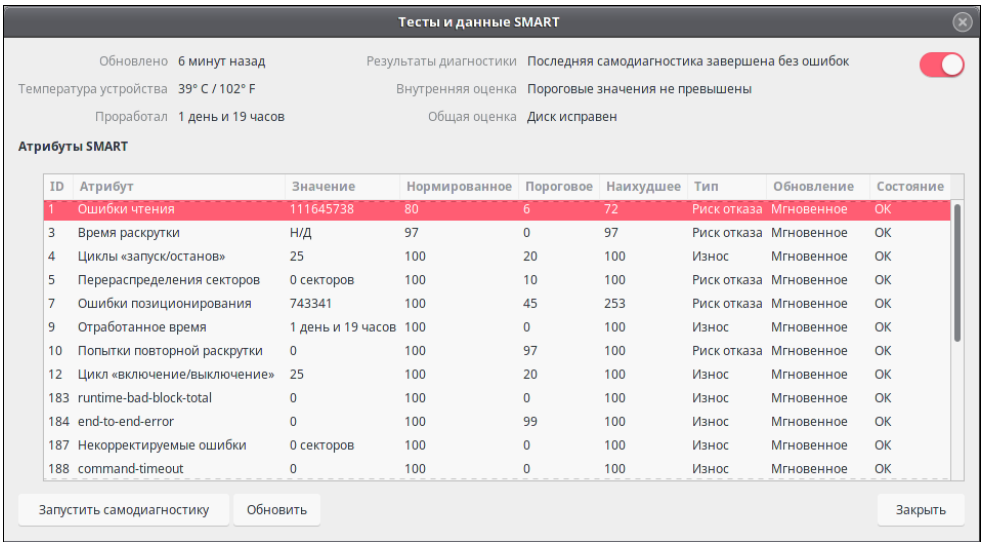
```
dnf install gnome-disk-utility
```

После установки утилита находится в **«Меню» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой Cinnamon и в **«Приложения» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой MATE.

После запуска приложения, выберите жесткий диск на панели справа, и нажмите на значок дополнительного меню, там выберите данные самодиагностики SMART.



В открывшемся окне вы можете просмотреть значения атрибутов SMART, температуры жесткого диска, результат последнего теста самодиагностики и запустить новый тест. Доступные тесты аналогичные таковым из утилиты **smartmontools**.



BadBlocks

Утилита **badblocks** используется для поиска сбойных блоков на устройстве (в разделе диска, например, */dev/sda1*).

Синтаксис утилиты:

```
badblocks [-<параметры>] <устройство> [<конечный_блок>] [<начальный_блок>]
```

Параметры [**<конечный_блок>**], [**<начальный_блок>**] являются необязательными и указывают диапазон проверяемых блоков. Если они не указаны, тогда (по умолчанию) проверке подлежат все блоки, начиная с самого первого блока и заканчивая самым последним блоком, которые используются на устройстве.

Основные параметры:

- **-b** - размер блока (в байтах);

- **-c** - порция блоков (по умолчанию 64 блока);
- **-f** - принудительный запуск теста с помощью чтения/записи;
- **-i** - входной файл (читает список уже существующих сбойных блоков);
- **-o** - исходящий файл (сохраняет список сбойных блоков в указанный файл);
- **-p** - число раз поиска (по умолчанию только одна проверка);
- **-n** - принудительное использование режима чтения-записи (только в размонтированной системе);
- **-s** - отображение хода процесса проверки;
- **-v** - подробные сообщения о проверке;
- **-w** - использование режима реальной записи (приводит к уничтожению информации на диске).

Пример использования утилиты

1. Выберите раздел жесткого диска для проверки. Для просмотра всех подключенных устройств и проверки расположения диска можно воспользоваться командой:

```
fdisk -l <имя_раздела>

  или

lsblk
```

2. Запустите проверки с помощью утилиты:

```
badblocks -v /dev/sda1Checking blocks 0 to 1048575
Checking for bad blocks (read-only test): done

Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Из вывода консоли видно, что проверка происходит только для чтения. При попытке использовать параметр **-n** (проверка чтения/записи) возникает следующее предупреждение:

```
/dev/ro_redos/root is mounted; it's not safe to run badblocks!
```

Поэтому для проверки дисков на чтение/запись рекомендуется использовать **live-сессию**.

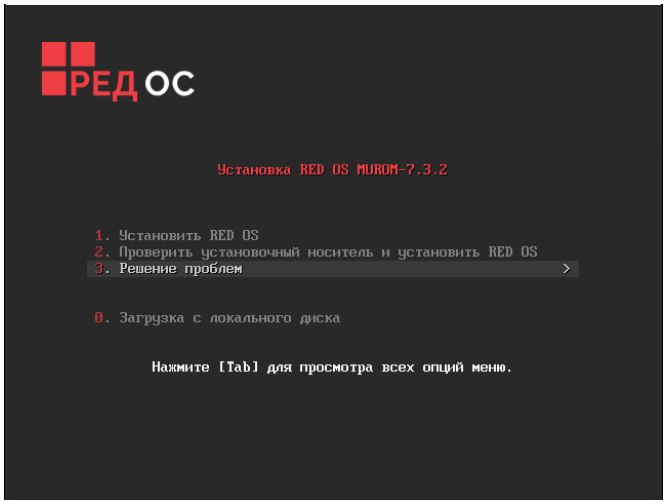
```
badblocks -v /dev/sda1

Checking for bad blocks in non-destructive read-write mode
From block 0 to 1048575
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

```
badblocks -v /dev/ro_redos/root

Checking for bad blocks in non-destructive read-write mode
From block 0 to 17821695
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

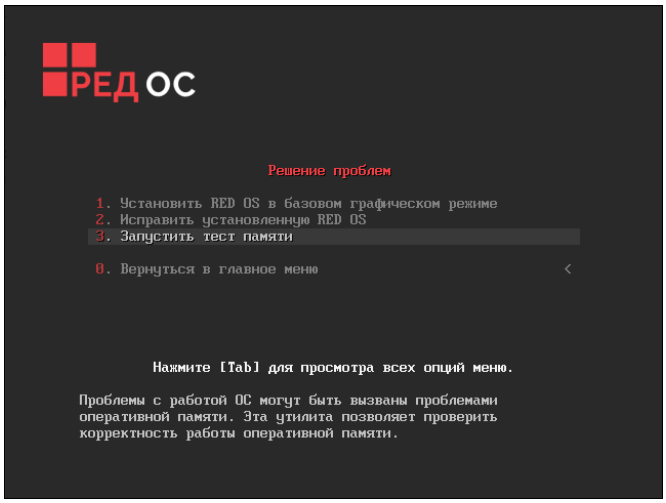
Тестирование оперативной памяти

Чтобы протестировать оперативную память на ошибки нужно запустить ОС с загрузочной флешки или диска.

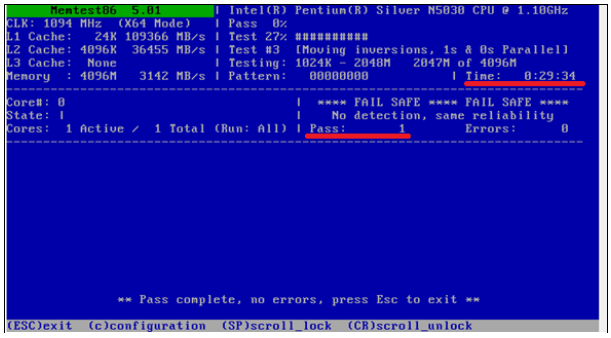
В открывшемся меню необходимо выбрать третий пункт «**Решение проблем**».



Затем выбрать третий пункт «**Запустить тест памяти**».



Запустится тест памяти.



Данный процесс будет выполняться бесконечно, пока вы не остановите его. Вам нужно дождаться окончания хотя бы одного цикла проверки (значение **Pass** должно быть **>= 1**). В случае обнаружения ошибки она отобразится в списке.

minicom - программа настройки параметров COM-портов

Minicom — консольная программа для установки сеансов связи с устройствами через последовательный порт (**COM**).

Для подключения к com-порту программу можно запускать с заданными аргументами или использовать псевдографический оконный интерфейс для изменения и сохранения собственных настроек подключения.

Сначала необходимо узнать рабочий COM-порт с помощью команды:

```
dmesg | grep "ttyS"
```

Вывод команды будет выглядеть примерно так:

```
[ 0.430791] 00:05: ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200) is a 16550A
```

где «**ttyS0**» - имя рабочего порта, который необходимо настроить.

Для установки **minicom** перейдите в сеанс пользователя **root**:

```
su-
```

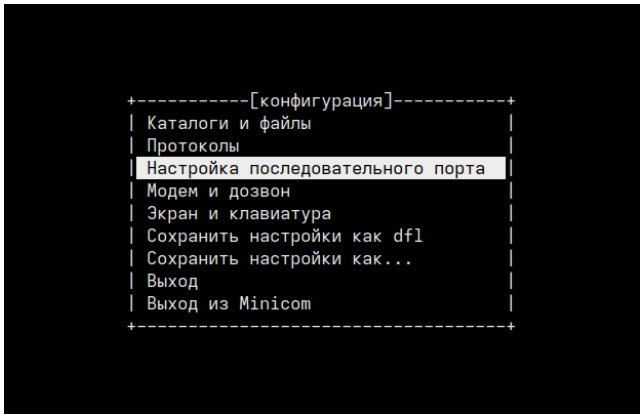
и выполните команду:

```
dnf install minicom
```

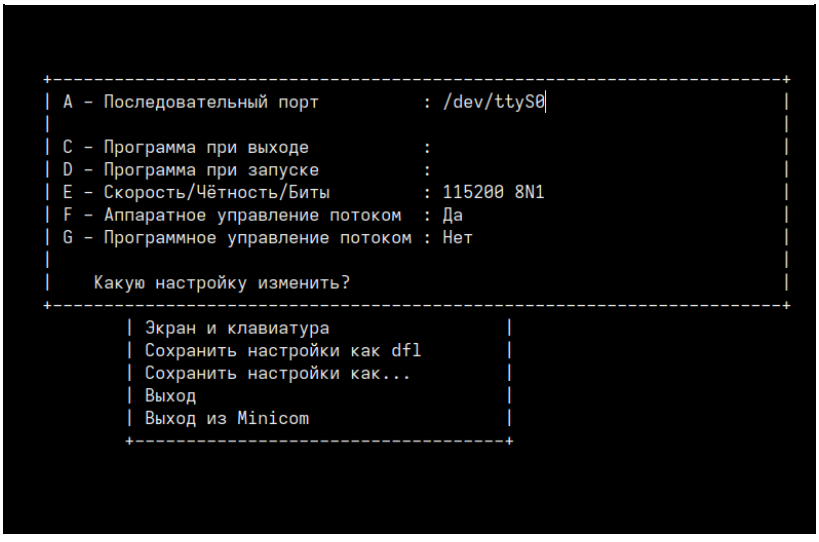
После установки запустите программу **minicom** (запуск лучше осуществлять с правами администратора, т.к. программе могут понадобиться повышенные права для доступа к порту или для сохранения настроек) с помощью команды:

```
minicom -s
```

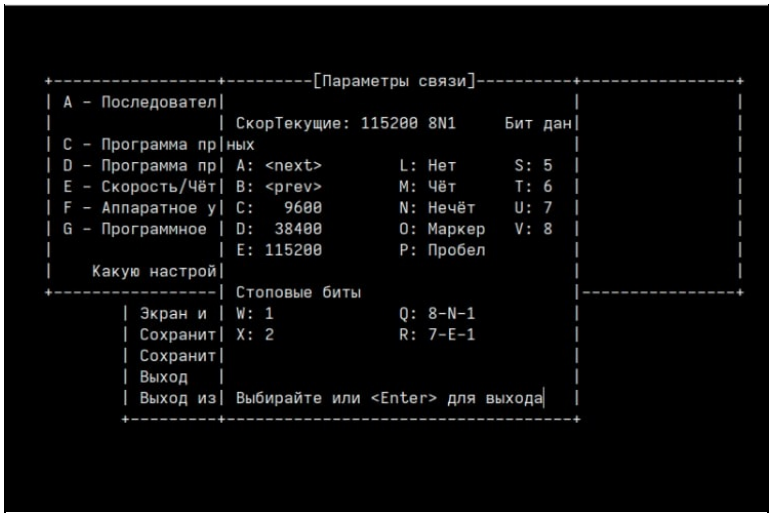
В открывшемся окне выберите пункт «**Настройка последовательного порта**».



Затем укажите необходимый COM-порт, изменяя в графе «**A - Последовательный порт**» адрес файла (в данном случае **dev/ttyS0**). Для редактирования нажмите клавишу «**A**» в строке «**Какую настройку изменить?**», курсор автоматически переведет вас в графу «**Последовательный порт**». Нажмите «**Enter**», чтобы применить изменения и вернуться в выбор настроек.



Далее в графе «**E - Скорость/Чётность/Биты**» можно настроить необходимые вам параметры. Для редактирования нажмите клавишу «**E**» в строке «**Какую настройку изменить?**», курсор автоматически переведет вас в графу «**Скорость/Четность/Биты**». Нажмите «**Enter**», чтобы применить изменения и вернуться в выбор настроек.



Для применения всех внесенных изменений и возврата в начальное меню «**Конфигурация**» еще раз нажмите «**Enter**».

Для сохранения установленных настроек выберите в меню «**Сохранить настройки как dfl**» или «**Сохранить настройки как...**» (если необходимо сохранить иначе).

Если выбрать пункт «**Сохранить настройки как...**» и указать имя файла настроек, например «**com1**», то это не изменит настройки по умолчанию (**dfl**), и в дальнейшем можно будет запускать программу с конкретными параметрами, указав имя файла с сохраненными настройками, например:

```
minicom com1
```

IMSProg - I2C/MicroWire/SPI программатор для CH341a

Установка
Сборка из исходного кода
Подключение микросхем
Выбор типа микросхемы
Основные операции программатора
Редактор базы микросхем
Список поддерживаемых микросхем

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: imsprog-1.4.1-1

IMSProg — программа, предназначенная для работы с программаторами **CH341a** и поддерживающая запись, чтение, стирание и проверку **I2C**, **SPI**, **DataFlash** и **MicroWire EEPROM/Flash** микросхем (серий *24xxx*, *25xxx*, *45xxx*, *93xxx*, *95xxx*). Программа имеет графический интерфейс и использует виджет **QHexEdit2** и доработанный набор библиотек программатора **SNANDer** для отображения шестнадцатеричного дампа прошивки микросхемы.

Для установки параметров микросхем **SPI** доступна кнопка «Поиск» для чтения параметров микросхемы (чтение информации JEDEC), а также поддерживается установка параметров микросхемы вручную. Для **I2C** и **MicroWire EEPROM** возможен только ручной выбор параметров.

Формат базы данных микросхем основан на формате программаторов EZP2019, EZP2020, EZP2023, Minpro I, XP866+. Редактирование БД микросхем производится с помощью отдельного компонента программы EZP Chip data Editor.

Установка

Для установки **IMSProg** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install imsprog
```

Дальнейшая работа с программой выполняется с правами непривилегированного пользователя.

После установки программа доступна из «**Главного меню**» — «**Программирование**» — «**IMSProg**».

Сборка из исходного кода

Также доступна самостоятельная сборка компонентов программы из исходного кода. Для этого необходимо установить дополнительные пакеты, выполнив последовательно ряд команд (для установки дополнительных компонентов необходимы права **администратора** или суперпользователя **root**):

```
dnf install cmake
dnf install libusb libusb1 libusb1-devel
dnf install qt5-qtbase-devel
dnf install pkgconf-pkg-config
dnf install qt5-linguist
```

Выйдите из сеанса администратора или суперпользователя **root**:

```
exit
```

Далее скачайте репозиторий программы с сайта **GitHub**, перейдите в каталог со скачанным архивом и распакуйте его (в примере **/home/user/Загрузки**), затем перейдите в каталог с распакованным архивом:

```
cd /home/user/Загрузки/
unzip IMSProg-main
```

```
cd IMSProg-main/
```

Для сборки программатора выполните последовательно ряд следующих команд:

```
cd IMSProg_programmer
mkdir build
cd build
cmake ..
make -j4
sudo make install
```

Вернитесь в исходный каталог с распакованным архивом:

```
cd /home/user/Загрузки/IMSProg-main/
```

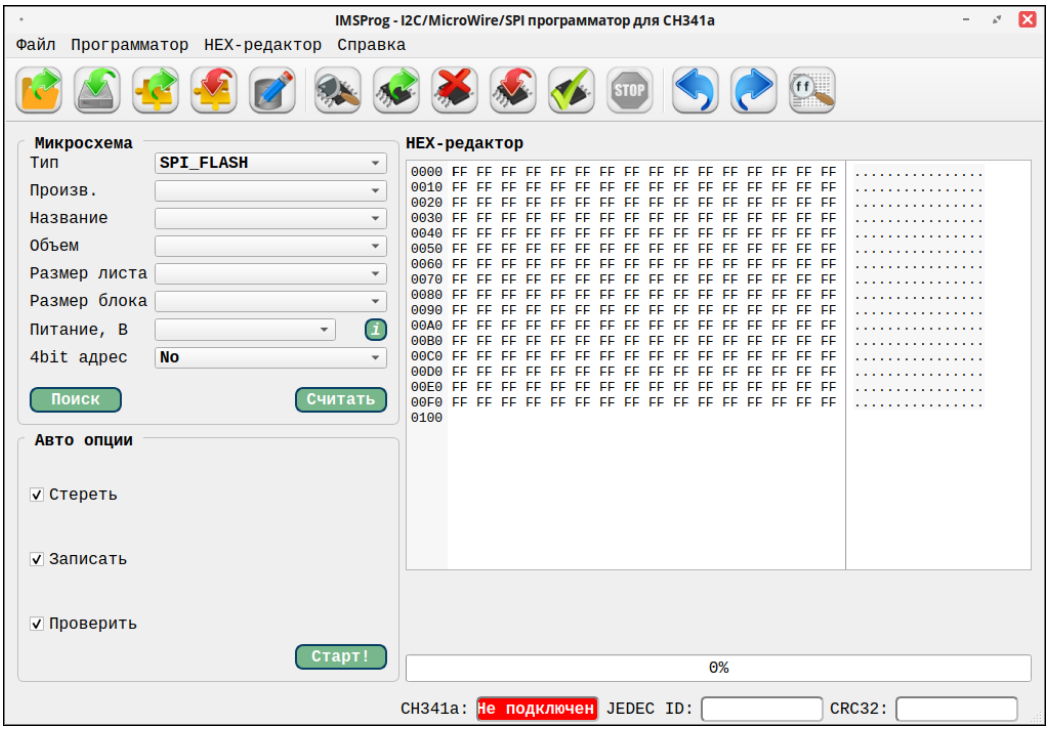
Для сборки редактора базы микросхем выполните последовательно ряд следующих команд:

```
cd IMSProg_editor
mkdir build
cd build
cmake ..
make -j4
sudo make install
```

Запуск программ будет доступен из «**Главного меню**» — «**Программирование**».

Программатор имеет название **IMSProg**, редактор параметров имеет название **IMSProg-редактор**.

Окно программатора выглядит следующим образом:



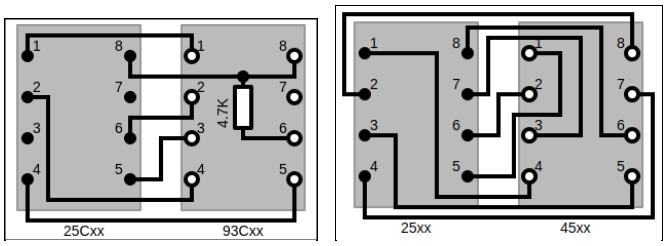
Подключение микросхем

Вставьте микросхему в соответствующий разъем программатора **CH341a**.

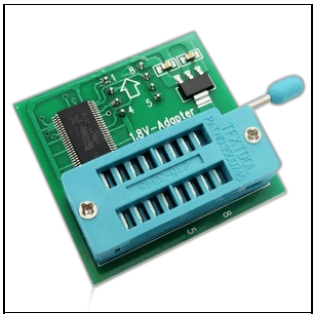
Микросхемы серий *24xxx* и *25xxx* должны быть вставлены непосредственно, в соответствии с маркировкой на печатной плате программатора **CH341a**. Микросхемы серии *M95xxx* устанавливаются как *25xxx*.

Микросхемы серии *93xxx* необходимо вставить в адаптер *93xxx*, а адаптер — в гнездо программатора с маркировкой *25xxx*.

Микросхемы *DataFlash* серии *AT45DBxxx* должны быть установлены в переходник **SOP-8 DIP-8**, который, в свою очередь, должен быть вставлен в адаптер *45xxx*. Адаптер *45xxx* устанавливается в гнездо программатора с маркировкой *25xxx*.



Если напряжение питания микросхемы составляет 1.8V, ее необходимо вставить в адаптер 1.8V, а адаптер — в нужное гнездо программатора.



Подключите программатор **CH341a** к USB-разъему компьютера и запустите программу IMSProg.

Подключать и отключать устройство (программатор **CH341a**) к порту USB можно в любое время, когда основные операции (чтение, проверка и программирование) не выполняются.

Выбор типа микросхемы

Выберите тип используемой микросхемы из выпадающего меню **Тип**. Доступны следующие типы микросхем:

- **SPI_FLASH** – при использовании микросхем SPI NOR FLASH серии *25xxx*;
- **24_EEPROM** – при использовании i2c EEPROM серии *24xxx*;
- **93_EEPROM** – при использовании MicroWire EEPROM серии *93xxx*;
- **25_EEROM** – при использовании SPI EEPROM;
- **95_EEPROM** – при использовании микросхем ST *M95xxx*.

При использовании микросхем SPI NOR FLASH серии *25xxx* и микросхем DataFlash серии *45xxx* будет доступна кнопка «Поиск» (), при нажатии на которую считывается информация JEDEC о микросхеме и загружаются все параметры этой микросхемы из базы данных. Любой параметр (объем микросхемы, размер страницы, размер блока, напряжение питания (VCC) или поддержка 4-битного адреса) может быть изменен вручную.

Вручную достаточно ввести данные выпадающего меню «Произв.» и «Название» – все остальные параметры будут автоматически загружены из базы данных микросхем.

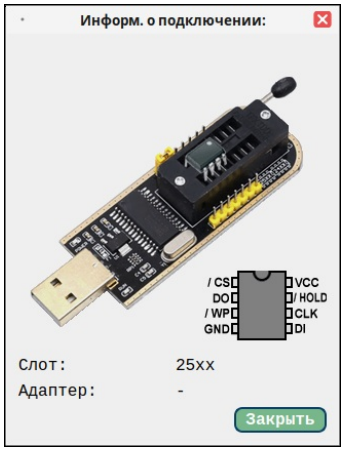
При использовании микросхем серий *24xxx, 25xxx* (не NOR FLASH), *95xxx* или *93xxx* необходимо вручную ввести данные всплывающего меню «Произв.» и «Название», поскольку для этих типов микросхем автоопределение не поддерживается. Все остальные параметры будут автоматически загружены из базы данных микросхем.

Основные операции программатора

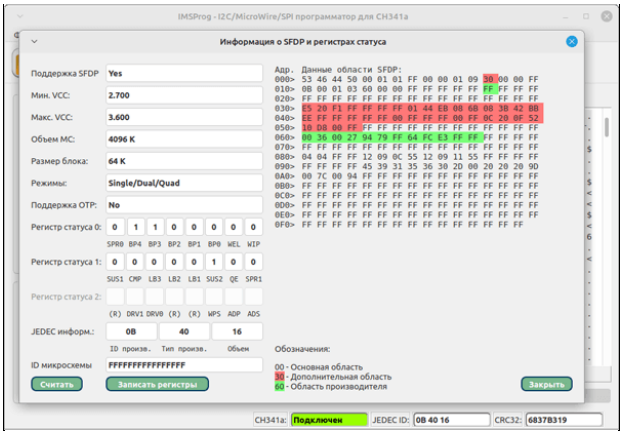
- Кнопка «Считать» () или сочетание клавиш *Ctrl+R* – вызывает функцию чтения данных из микросхемы в буфер компьютера;
- Кнопка  или сочетание клавиш *Ctrl+W* – вызывает функцию записи данных из буфера компьютера в микросхему;
- Кнопка  или сочетание клавиш *Ctrl+E* – приводит к стиранию всех данных микросхемы;
- Кнопка  или сочетание клавиш *Ctrl+T* – вызывает процесс побайтового сравнения данных в микросхеме и в буфере компьютера;
- Индикатор выполнения показывает ход выполнения операций чтения, стирания и проверки;
- Кнопка «**Старт!**» используется для последовательного выполнения операций стирания, записи и верификации. Если одна из этих

операций не нужна, можно снять флажок с чекбокса конкретной операции;

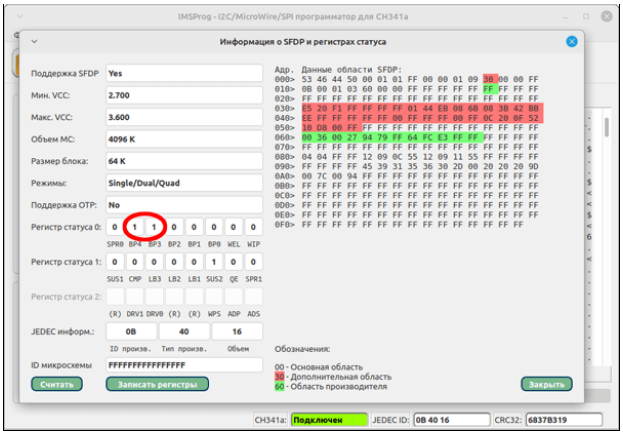
- Кнопка  или сочетание клавиш *Ctrl+I* – позволяет аварийно прервать операции чтения, записи, стирания или сравнения данных микросхемы;
- Кнопка «**i**» – выводит на экран информацию об используемом слоте и адаптере, необходимыми для работы с выбранной микросхемой.



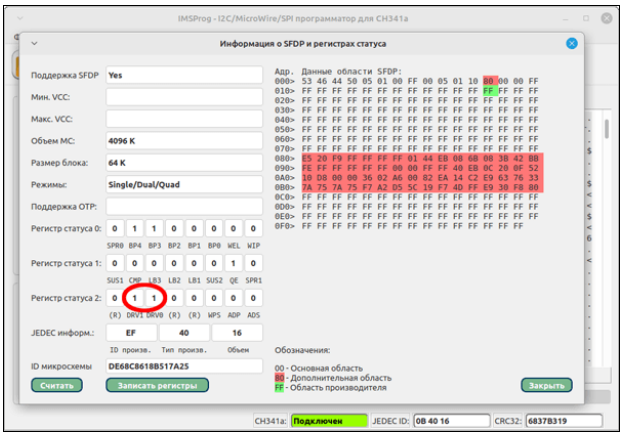
- Пункт меню «Программатор» – «Информ. о МС» или сочетание клавиш *Ctrl+P* служит для отображения и изменения регистров состояния, уникального серийного номера и области **e Serial Flash Discoverable Parameter (SFDP) SPI NOR Flash** микросхем. Эта информация может пригодиться при использовании микросхем, которых нет в базе, и для анализа проблем при ошибках записи.



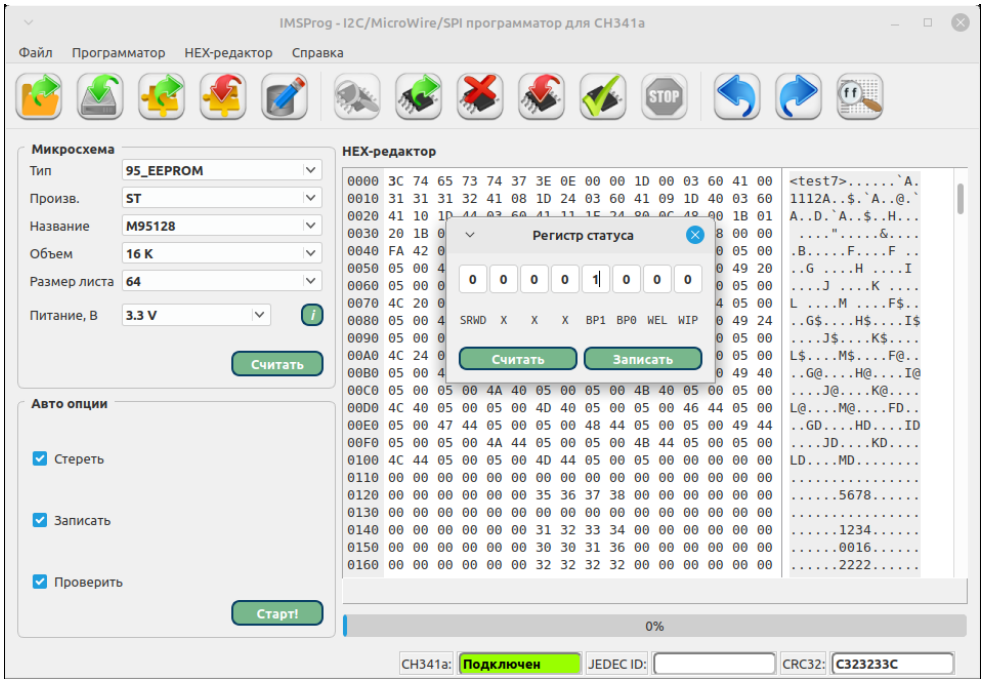
Если микросхема **SPI NOR FLASH** определяется нормально, но не читается (выдает сообщение вида «*Ошибка чтения сектора 0*»), возможно микросхема заблокирована. В этом случае в окне «Информ. о МС» измените биты **BP4** и **BP3** на нулевые и нажмите кнопку «Записать регистры». Затем повторите операцию чтения микросхемы.



Если микросхема **SPI NOR FLASH** считывается ненадежно (каждый раз с разной контрольной суммой) и в ней доступен «Регистр статуса 2», то можно изменить биты **DRV0** и **DRV1** на нулевые и нажать кнопку «Записать регистры». Это увеличит мощность выходного каскада выхода **DO** микросхемы. После этого повторить операцию чтения микросхемы.



Для микросхем серий *25xxx*, *95xxx*, у которых в есть только один регистр статуса, форма «Информ. о МС» выглядит следующим образом:



Операции с файлами

Кнопка  или сочетание клавиш *Ctrl+S* – используется для записи содержимого буфера компьютера в файл.

Кнопка  или сочетание клавиш *Ctrl+O* – используется для загрузки файла в буфер компьютера.

Кнопка  или сочетание клавиш *Ctrl+Shift-S* – используется для сохранения части компьютерного буфера в файл (необходимо ввести начальный адрес и длину части или конечный адрес). Эта операция может быть использована при разбиении двоичного образа данных на части.

Кнопка  или сочетание клавиш *Ctrl+Shift-O* – используется для загрузки небольшого файла по определенному адресу в буфере. При этом фрагмент данных в буфере будет заменен новыми данными из файла.

Кнопка  или сочетание клавиш *Ctrl+Q* – служит для вызова модуля редактора базы данных микросхем.

Операции с буфером (шестнадцатеричным редактором)

Шестнадцатеричный редактор микросхем (правая часть экрана) используется для отображения и изменения данных буфера.

Он содержит следующие элементы управления:

- Кнопка  или сочетание клавиш *Ctrl+Z* – отмена последней операции,

- Кнопка  или сочетание клавиш *Ctrl+Shift+Z* – повтор операции и
- Кнопка  или сочетание клавиш *Ctrl+F* – функция поиска/замены кода или строки.

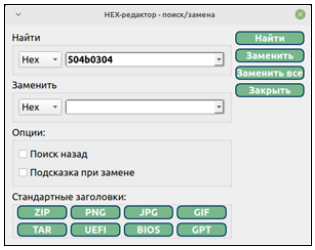
Сочетание клавиш *Ctrl+A* производит пересчет контрольной суммы буфера по алгоритму **CRC32**.

Сочетание клавиш *Ctrl+G* производит переход к просмотру кода по введенному шестнадцатеричному адресу.

Операции поиска и замены

Поиск и замену можно производить как шестнадцатиричного кода (опция **Hex** в выпадающем меню), так и текстовую информацию (**UTF-8** в выпадающем меню). Возможен поиск как вперед, так и назад.

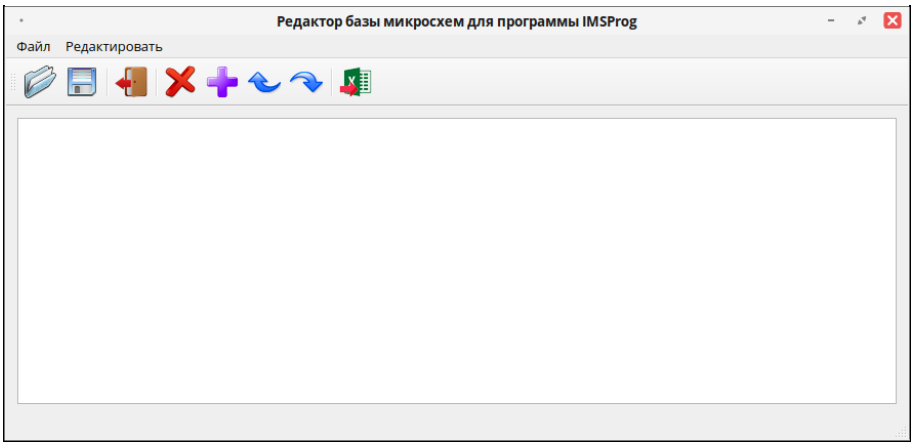
Для удобства поиска внизу формы есть панель «Стандартные заголовки». С помощью клавиш на этой панели поле поиска автоматически заполняется стандартными заголовками архивов, изображений или системных разделов.



Редактор базы микросхем

Редактор базы микросхем **IMSProg_editor** – это самостоятельная программа, которая может быть запущена как из «Главного меню» – «Программирование», так и из программатора IMSProg нажатием на кнопку  . Окно редактора параметров микросхем выглядит следующим образом:

Окно редактора параметров микросхем выглядит следующим образом:



Все операции в редакторе становятся доступными только после загрузки файла базы микросхем с расширением **.Dat**.

Далее будут рассмотрены основные действия для работы с программой.

Пункт меню «Файл»

Кнопка «Открыть» () или сочетание клавиш *Ctrl+O* – позволяет загрузить файл данных.

Кнопка «Сохранить» () или сочетание клавиш *Ctrl+S* – сохраняет таблицу параметров микросхем в файл базы данных.

Кнопка «Выход» () или сочетание клавиш *Ctrl+X* – выход из редактора.

Кнопка «Экспорт в CSV формат» () – позволяет выгрузить данные о микросхемах в формате CSV для дальнейшей обработки программой электронных таблиц – Libre Office Calc, Open Office Calc, Google Tables и т. д.

Кнопка «Импорт из CSV файла» () – загружает таблицу в формате CSV и добавляет данные из нее к существующим данным в

таблице.

Пункт меню «Редактировать»

Кнопка «Удалить строки» () или клавиша *Del* – удаляет одну или несколько строк.

Кнопка «Добавить строку» () или клавиша *Ins* – добавляет строку ниже выделенной и копирует все данные из выделенной строки в новую.

Кнопка «Переместить вверх» () или сочетание клавиш *Ctrl+Вверх* – перемещает выделенную строку вверх.

Кнопка «Переместить вниз» () или сочетание клавиш *Ctrl+Вниз* – перемещает выделенную строку вниз.

Кнопка «Импорт выделенных строк в CSV формат» () – сохраняет выделенные строки в файл формата CSV.

Наиболее свежую версию файла базы данных микросхем можно скачать с этой страницы как в формате **.Dat**, так и в формате **.csv**.

Список поддерживаемых микросхем

Тип микросхемы	Серия микросхем	
i2C EEPROM	24C01, 24C02, 24C04, 24C08, 24C16, 24C32, 24C64, 24C128, 24C256, 24C512, 24C1024	
MicroWire EEPROM	93C46, 93C56, 93C66, 93C76, 93C86	
Serial SPI Bus EEPROM	ST	M95010, M95020, M95040, M95080, M95160, M95320, M95640, M95128, M95256, M95512, M95M01, M95M02
	ATMEL	AT25010, AT25020, AT25040, AT25080, AT25160, AT25320, AT25640, AT25128, AT25256, AT25F512, AT25F1024, AT25F2048, AT25F4096
	MICROCHIP	25AA010, 25AA020, 25AA040, 25AA080, 25AA160, 25AA320, 25AA640, 25AA128, 25AA256, 25AAF512, 25AAF1024, 25LC010, 25LC020, 25LC040, 25LC080, 25LC160, 25LC320, 25LC640, 25LC128, 25LC256, 25LC512, 25LC1024
	ONSEMI	CAT25C01, CAT25C02, CAT25C04, CAT25C08, CAT25C16, CAT25C32, CAT25C64, CAT25C128, CAT25C256, CAT25C512
DataFlash 45xx	ATMEL	AT45DB011, AT45DB021, AT45DB041, AT45DB081, AT45DB161, AT45DB321
	ADESTO	AT45DB011, AT45DB021, AT45DB041, AT45DB081, AT45DB161, AT45DB321, AT45DB641
SPI NOR Flash	SPANSION	FL016AIF, S25FL016P, S25FL032P, FL064AIF, S25FL064P, S25FL256S, S25FL128P, S25FL129P, S25FL116K, S25FL132K, S25FL164K
	XTX	XT25F02E, XT25F04D, XT25F08B, XT25F16B, XT25F32F, XT25F64F, XT25F128F, XT25W02E, XT25W04D, XT25Q08D(1.8V), XT25Q16D(1.8V), XT25Q64D(1.8V), XT25F128D(1.8V)
	EON	EN25B10T, EN25B20T, EN25B40T, EN25B80T EN25B16T, EN25B32T, EN25B64T, EN25F64, EN25Q40A, EN25Q80B, EN25Q16, EN25Q32C, EN25Q64, EN25Q128, EN25F10A, EN25F20A, EN25F40, EN25F80, EN25F16, EN25F32, EN25S10A(1.8V), EN25S20A(1.8V), EN25S40A(1.8V), EN25S80B(1.8V), EN25S16B(1.8V), EN25S64A(1.8V), EN25QE32A, EN25E10A, EN25E40A, EN25SE16A(1.8V), EN25SE32A(1.8V), EN25T80, EN25QA32B, EN25QA64A, EN25QA128A, EN25QW16A, EN25QW32A, EN25QH16, EN25QH32B, EN25QH64A, EN25QH128A, EN25Q256, EN25QX64A, EN25QX128A, EN25QX256A, EN25QY256A, EN25SX64A(1.8V), EN25SX128A(1.8V)
	ATMEL	AT26DF161, AT25DF321
	MICRON	M25P10, M25P20, M25P40, M25P80, M25P016, M25P32, M25P64, M25P128, N25Q032A, N25Q064A, MT25QL64AB, N25Q128A, MT25QL128AB, N25Q256A, MT25QL256AB, MT25QL512AB, N25Q032A(1.8V), N25Q064A(1.8V), MT25QU64AB(1.8V), N25Q128A(1.8V), MT25QU128AB(1.8V), MT25QU256AB(1.8V), MT25QU512AB(1.8V)
	XMC	XM25QH10B, XM25QH20B, XM25QH40B, XM25QH80B, XM25QH16C, XM25QH32B, XM25QH64C, XM25QH128C, XM25QH256C, XM25QH512C, XM25LU64C(1.8V), XM25LU128C(1.8V), XM25QU256C(1.8V), XM25QU512C(1.8V), XM25QW16C, XM25QW32C, XM25QW64C, XM25QW128C, XM25QW256C, XM25QW512C, XM25QU41B(1.8V), XM25QU80B(1.8V), XM25QU16C(1.8V), XM25LU32C(1.8V), XM25QH32A, XM25QH64A, XM25QH128A
	AMIC	A25L10PU, A25L20PU, A25L40PU, A25L80PU, A25L16PU, A25L10PT, A25L20PT, A25L40PT, A25L80PT, A25L16PT, A25L010, A25L020, A25L040, A25L040, A25L080, A25L016, A25L032, A25LQ080, A25LQ16, A25LQ32, A25LQ64
	EXCELSEMI	ES25P10, ES25P20, ES25P40, ES25P80, ES25P16, ES25P32, ES25M40A, ES25M80A, ES25M16A
	DOUQI	DQ25Q64AS
	Zbit	ZB25LD10A(1.8V), ZB25LD20A(1.8V), ZB25LD40B(1.8V), ZB25LD80(1.8V), ZB25D10A, ZB25D20A, ZB25D40B, ZB25D80B, ZB25VQ16, ZB25VQ32, ZB25VQ64, ZB25VQ128, ZB25LQ16(1.8V), ZB25LQ32(1.8V), ZB25LQ64(1.8V), ZB25LQ128(1.8V), ZB25VQ20A, ZB25VQ40A, ZB25VQ80A, ZB25VQ16A
	ONSemi	LE25U20AMB, LE25U40CMC
	Boya	BY25Q05AW, BY25Q10AW, BY25Q20BL(1.8V), BY25Q40BL(1.8V), BY25Q80AW(1.8V), BY25Q16BL(1.8V), BY25D05AS, BY25D10AS, BY25D20AS, BY25D40AS, BY25Q80BS, BY25Q16BS, BY25Q32BS, BY25Q64AS, BY25Q128AS, BY25Q256ES, BY25Q10AL(1.8V), BY25Q20AL(1.8V), BY25Q40AL(1.8V), BY25Q32AL(1.8V), BY25Q64AL(1.8V), BY25Q128EL(1.8V)

PFLASH	Pm25LQ512B, Pm25LQ010B, Pm25LQ020B, PM25LQ016, PM25LQ032, PM25LQ064, PM25LQ128, Pm25LQ040B
Puya	P25Q06H, P25Q40H, P25Q11H, P25Q21H, P25Q10H, P25Q20H, P25Q40H, P25Q80H, P25Q16H, P25Q32H, P25Q64H, P25Q128H
ESMT	F25L004A, F25L008A, F25L016, F25L032, F25L064, F25L16QA, F25L32QA, F25L64QA
ISSI	IS25LQ010, IS25LQ020, IS25LP080D, IS25LP016D, IS25LP032D, IS25LP064D, IS25LP128F, IS25LP256D, IS25LP512D, IS25WP040D(1.8V), IS25WP080D(1.8V), IS25WP016D(1.8V), IS25WP032D(1.8V), IS25WP064D(1.8V), IS25WP128F(1.8V), IS25WP256D(1.8V), IS25WP512D(1.8V)
Fudan	FM25W04, FM25W16, FM25W32, FM25W64, FM25W128, FM25Q04, FM25Q08, FM25Q16, FS25Q32, FS25Q64, FS25Q128
Zetta	ZD25Q64B, ZD25LQ128(1.8V), ZD25LQ64(1.8V), ZD25WD20B, ZD25WD40B, ZD25Q80C, ZD25Q16B, ZD25Q32C
PCT	PCT25VF016B, PCT25VF032B, PCT25VF064C, PCT25VF020B, PCT25VF040B, PCT25VF080B, PCT26VF016, PCT26VF032, PCT25VF010A
MXIC	MX25L8005M, MX25L1605D, MX25L3205D, MX25L6405D, MX25L12805D, MX25L25635E, MX25L51245G, MX25U5121E(1.8V), MX25U1001E(1.8V), MX25U2035F(1.8V), MX25U4035F(1.8V), MX25U80356(1.8V), MX25U1632F(1.8V), MX25U3232F(1.8V), MX25U6432F(1.8V), MX25U12832F(1.8V), MX25U25643G(1.8V), MX25U51245G(1.8V), MX25R2035F, MX25R4035F, MX25R8035F, MX25R1635F, MX25R3235F, MX25R6435F
GigaDevice	GD25F40, GD25F80, GD25D40, GD25D80, GD25D05C, GD25D10C, GD25Q20C, GD25Q40C, GD25Q80C, GD25Q16C, GD25Q32, GD25Q64CSIG, GD25Q128CSIG, GD25Q256CSIG, GD25LD05C(1.8V), GD25LD10C(1.8V), GD25LD20C(1.8V), GD25LD40C(1.8V), GD25LQ80C(1.8V), GD25LQ16C(1.8V), GD25LQ32E(1.8V), GD25LQ64E(1.8V), GD25LQ128(1.8V), GD25LQ256D(1.8V), GD25WD05C, GD25WD10C, GD25WD20E, GD25WD40E, GD25WD80C, GD25WQ20E, GD25WQ40E, GD25WQ80E, GD25WQ16E, GD25WQ32E, GD25WQ64E, GD25WQ128E, GD25WB256E, GD25LB512ME(1.8V), YC25Q128
PARAGON	PN25F08, PN25F16, PN25F32, PN25F64, PN25F128
WINBOND	W25P80, W25P16, W25P32, W25X05, W25X10, W25X20, W25X40, W25X80, W25X16, W25X32VS, W25X64, W25Q20CL, W25Q40BV, W25Q80BL, W25Q16DV, W25Q32BV, W25Q64BV, W25Q128BV, W25Q256FV, W25Q20BW(1.8V), W25Q80, W25Q10EW(1.8V), W25Q20EW(1.8V), W25Q40EW(1.8V), W25Q80EW(1.8V), W25Q16JW(1.8V), W25Q32FW(1.8V), W25Q64DW(1.8V), W25Q128FW(1.8V), W25Q256JW(1.8V), W25M512JW(1.8V), W25Q512JV, W25M512JV, W25Q32JW(1.8V)
Fidelix	FM25Q04A, FM25Q08A, FM25Q16A, FM25Q32A, FM25Q64A, FM25Q128A, FM25M04A(1.8V), FM25M08A(1.8V) FM25M16A(1.8V), FM25M32B(1.8V), FM25M64A(1.8V)

Подключение принтеров HP

Установка принтеров HP с помощью HPLIP

HPLIP (**HP L**inux **I**maging and **P**rinting) предоставляет драйвера для принтеров HP. Также он включает в себя **поддержку сканера** и факса. **HPLIP** рекомендуется для большинства принтеров **HP inkjet** и **laserjet**. Список поддерживаемого оборудования представлен по ссылке.

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

1. Для установки **hplip** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install hplip-gui python3-distro
```

2. После установки программа будет доступна из «**Главного меню**» – «**Администрирование**» – «**HP Device Manager**» (или «**Управление устройствами HP**»).

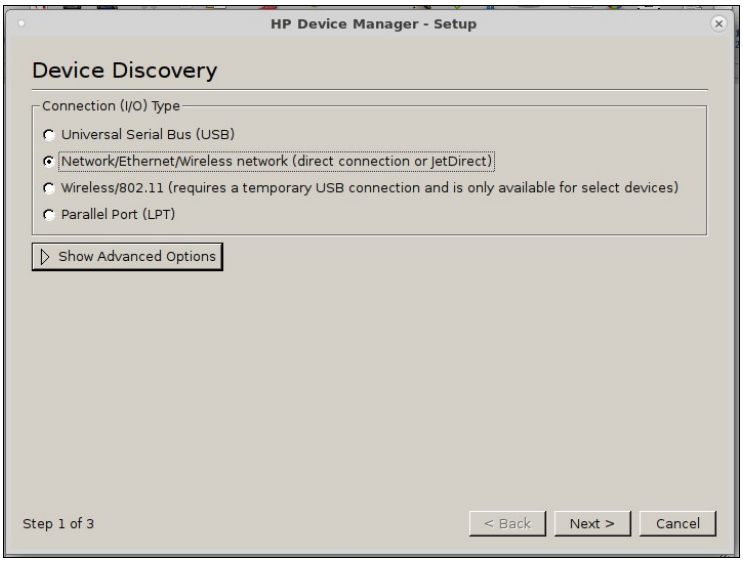
3. Далее выберите **Setup Device...**



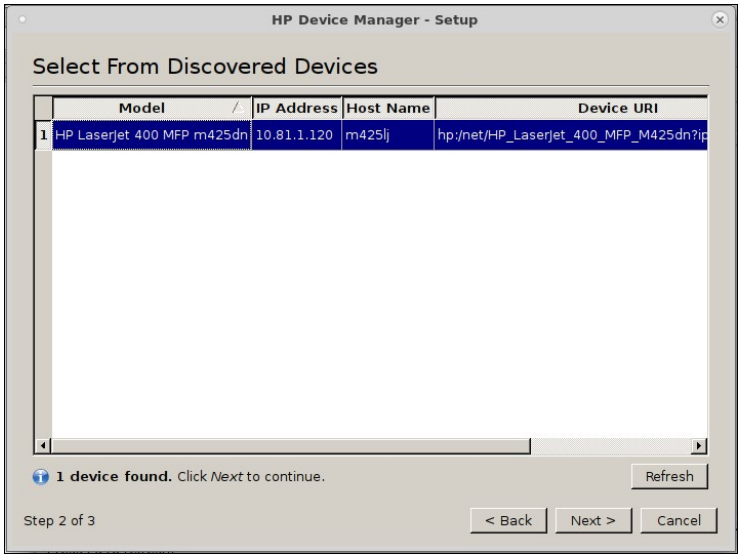
4. Выберите способ подключения принтера.

Если это *USB-принтер*, нажмите **Далее**.

Если *сетевой* – выберите второй пункт (**Network/Ethernet/Wireless network**).



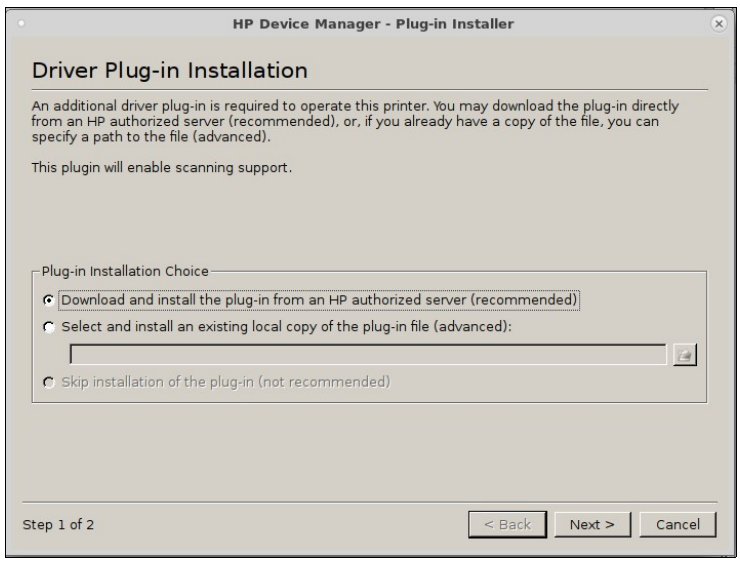
5. В случае с *сетевым* принтером выберите необходимый из списка найденных.



6. Установите плагин.

Запустите команду установки плагина:

```
/usr/bin/hp-plugin
```



В случае возникновения ошибки загрузки плагина, его можно скачать самостоятельно и применить, выбрав второй пункт.

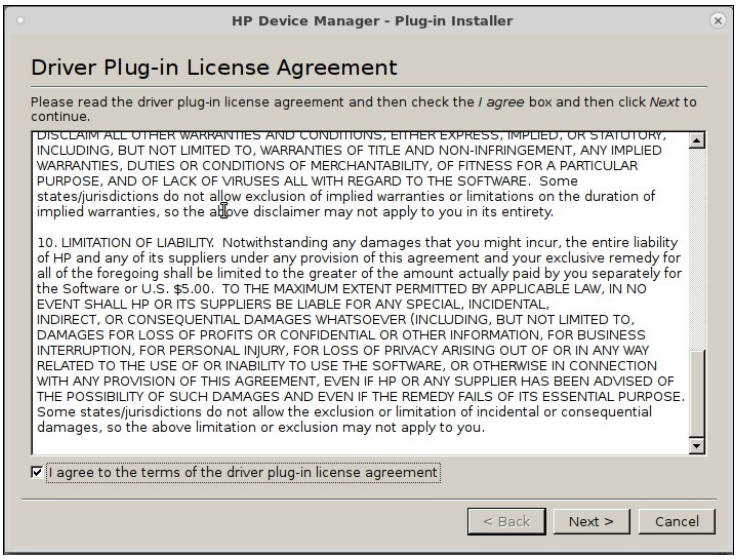
Скачать плагин можно по этой или этой ссылке.

Его версия должна совпадать с версией **hplip** , которая показана в **HP Device Manager** в меню **Help - About** . При обновлении **hplip** необходимо установить соответствующую версию плагина командой:.

```
hp-plugin
```

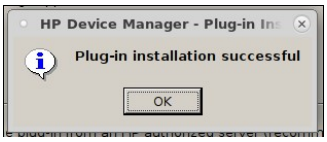
Затем выберите файл плагина в окне установки плагина **hp**.

7. Примите лицензионное соглашение.

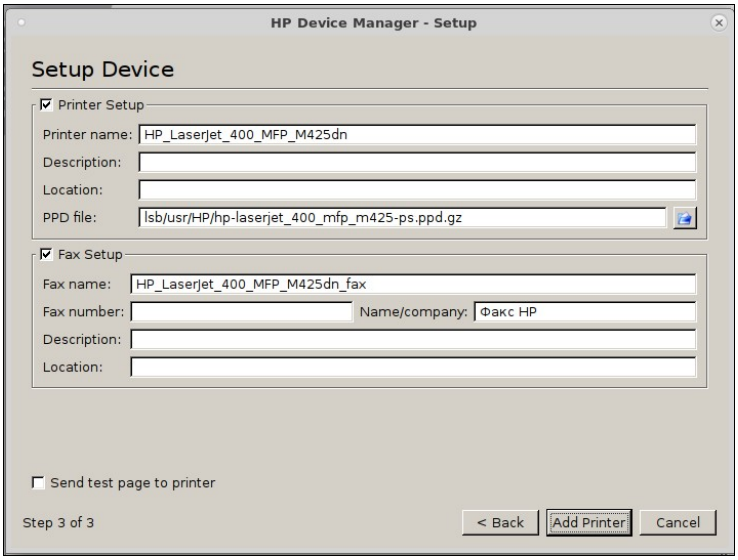


8. Введите пароль пользователя **root** во всплывающем окне.

9. Если после этого появилось окно, как на картинке ниже, то плагин **hplip** установлен успешно. Нажмите «**OK**».

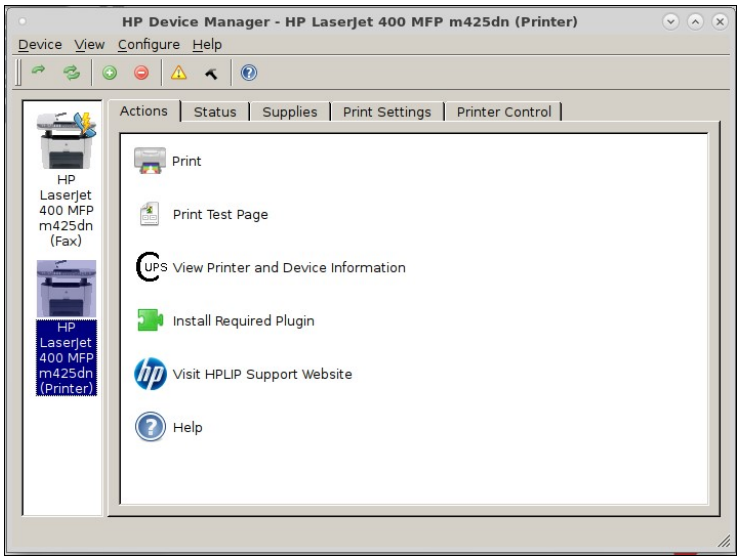


10. Нажмите «**Add Printer**».



11. Далее во всплывающем окне введите пользователя **root** и его **пароль**.

12. Принтер установлен и его видно в окне **HP Device Manager**.



13. Установите плагины для принтера **HP** в приложении **HP Device Manager**, выбрав на вкладке **Action** пункт "**Install required Plugin**" или запустив от **локального** пользователя команду hp-plugin.

ВАЖНО!

Есть список принтеров / МФУ, с которыми могут быть проблемы после установки:

HP LaserJet P2035
HP LaserJet Pro P1606dn
HP LaserJet Pro P1566
HP LaserJet Pro P1102
HP LaserJet Pro M12a
HP LaserJet Pro M12w
HP LaserJet Pro P1102w
HP LaserJet Pro CP1025nw
HP LaserJet 1022
HP LaserJet 1022n
HP LaserJet 1022nw
HP LaserJet 1020
HP LaserJet 1018
HP LaserJet 1005
HP LaserJet 1000
HP LaserJet P1005
HP LaserJet P1006
HP LaserJet P1007
HP LaserJet P1008
HP LaserJet P1505/P1505n
HP LaserJet P2014/P2014n
HP LaserJet M1005 MFP
HP LaserJet M1120 MFP
HP LaserJet Pro M1132s MFP
HP LaserJet Pro M1212nf MFP

Решаются такие проблемы следующим образом:

1) Войдите в систему как **root** (можно сделать и в консольном окне MATE/Cinnamon).

2) Удалите пакет system-config-printer-udev:

```
dnf remove system-config-printer-udev
```

3) В папке **/etc/udev/rules.d** создайте файл, например, «**60-hp_brainless.rules**», где пропишите следующее правило для менеджера устройств **udev**. Данное правило будет запускать команду загрузки **firmware** по наступлении события «**Включение принтера**»:

```
ACTION!="add", GOTO="skip_hp"
SUBSYSTEM!="usb", GOTO="skip_hp"
ATTRS{idVendor}=="03f0", ATTRS{idProduct}=="2b17", ATTRS{dev}=="*", RUN+="hp-firmware  -n --
device=hp:/usb/HP_LaserJet_1020?serial=FN1DNNJ"
LABEL="skip_hp"
```

Здесь **idVendor** и **idProduct** указаны для **HP LaserJet 1020**, если у вас другая модель, то эти значения можно узнать в выводе команды `lsusb`.

Значение параметра **--device** так же приведено в качестве примера. Для вашего принтера, подключенного к ПК, вы сможете получить его из вывода команды `lpinfo -v`.

В позиции аргументов утилиты `hp-firmware` укажите значения для Вашего принтера и укажите обязательно неинтерактивный режим (подробнее об этой команде и её опциях см. здесь).

4) Обязательно перезапустите менеджер **udev** следующими командами:

```
udevadm control --reload-rules
udevadm trigger
```

Подключение принтеров Canon

Для принтеров: LBP112, LBP113w, LBP151dw, LBP6030, LBP6030B, LBP6030w, LBP6230dw, LBP7100Cn, LBP7110Cw используйте драйвер UFRII LT, который доступен по ссылке.

Для серий Canon i-SENSYS, imagePRESS, imageRUNNER, iR драйвер доступен по ссылке.

Для принтера модели Canon imageRUNNER 1133A драйвер доступен по ссылке. При установке выбрать модель Canon-MFP5800 Series UFRII LT.

Чтобы установить драйвер, скачайте и распакуйте его, перейдите в распакованный каталог.

В терминале запустите скрипт установки install.sh и следуйте инструкциям инсталлятора.

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для автоматической установки принтера Canon воспользуйтесь драйвером по ссылке. В архиве canon.zip имеется интерактивный скрипт установки принтера.
Скачайте архив с драйвером и распакуйте его командой:

```
unzip canon.zip
```

Перейдите в распакованный каталог и от пользователя root выполните запуск скрипта автоматической настройки:

```
./canon-install.sh
```

Ниже рассмотрен вариант ручной установки драйвера версии **2.71** для принтеров Canon серии LBP. Поддерживаемые модели представлены в таблице. Драйвер доступен по ссылке. В архиве canon.zip имеется интерактивный скрипт установки принтера, запустите его от пользователя **root**.

Поддерживаемые модели принтеров:

Принтер	Название файла PPD
LBP1120	CNCUPSLBP1120CAPTK.ppd
LBP1210	CNCUPSLBP1210CAPTK.ppd
LBP2900	CNCUPSLBP2900CAPTK.ppd
LBP3000	CNCUPSLBP3000CAPTK.ppd
LBP3050	CNCUPSLBP3050CAPTK.ppd
LBP3018	CNCUPSLBP3050CAPTK.ppd
LBP3010	CNCUPSLBP3050CAPTK.ppd
LBP3150	CNCUPSLBP3150CAPTK.ppd
LBP3108	CNCUPSLBP3150CAPTK.ppd
LBP3100	CNCUPSLBP3150CAPTK.ppd
LBP3200	CNCUPSLBP3200CAPTK.ppd
LBP3210	CNCUPSLBP3210CAPTK.ppd
LBP3250	CNCUPSLBP3250CAPTK.ppd
LBP3300	CNCUPSLBP3300CAPTK.ppd
LBP3310	CNCUPSLBP3310CAPTK.ppd
LBP3500	CNCUPSLBP3500CAPTK.ppd
LBP5000	CNCUPSLBP5000CAPTK.ppd
LBP5050	CNCUPSLBP5050CAPTK.ppd
LBP5100	CNCUPSLBP5100CAPTK.ppd

LBP5300	CNCUPSLBP5300CAPTK.ppd
LBP6018	CNCUPSLBP6018CAPTK.ppd
LBP6000	CNCUPSLBP6018CAPTK.ppd
LBP6020	CNCUPSLBP6020CAPTK.ppd
LBP6200d	CNCUPSLBP6200CAPTK.ppd
LBP6300dn	CNCUPSLBP6300CAPTK.ppd
LBP7200C	CNCUPSLBP7200CCAPTK.ppd
LBP9100Cdn	CNCUPSLBP9100CCAPTK.ppd

Выполните удаление system-config-printer-udev, поскольку в некоторых случаях автоматически добавленный принтер работает некорректно:

```
dnf remove system-config-printer-udev
```

Установка драйвера
Перейдите в каталог с загруженным архивом и выполните распаковку:

```
unzip canon.zip
```

Перейдите в каталог **canon** и выполните установку пакетов командой:

```
dnf localinstall cnd*
```

Регистрация принтера в спулере печати
Данные для команды возьмите из выше представленной таблицы.

Команда для установки принтера **LBP2900**:

```
sudo lpadmin -p LBP2900 -m CNCUPSLBP2900CAPTK.ppd -v ccp://localhost:59687 -E
```

Для регистрации в системе узнаем адрес принтера:

```
dmesg | grep printer
```

Вывод команды:

```
5.876692] usblp 1-10:1.0: usblp0: USB Bidirectional printer dev 7 if 0 alt 0 proto 2 vid 0x04A9 pid 0x2676
```

Обратите внимание на значение (в данном случае **0**) после **usblp** в строке вывода.

```
sudo /usr/sbin/ccpdadmin -p LBP2900 -o /dev/usb/lp0
```

LBP2900 — это название принтера, указанное в таблице, представленной ранее. Пожалуйста, укажите название вашего принтера.

При этом в файле **/etc/ccpd.conf** появится запись:

```
<Printer LBP2900>
DevicePath /dev/usb/lp0
</Printer>
```

Создадим новый сервис ccpd, для этого создайте файл **/etc/systemd/system/ccpd.service** со следующим текстом:

```
[Unit]
Description=CCPD Printing Daemon
After=cups.service
[Service]
Type=forking
ExecStart=/usr/sbin/ccpd
TimeoutSec=5
[Install]
WantedBy=multi-user.target
```

Удалите старый сервис:

```
rm -f /etc/rc.d/init.d/ccpd
```

Перезагрузим **systemd** с поиском новых юнитов и перезапустим сервисы **ccpd** и **cups**:

```
systemctl daemon-reload
systemctl restart ccpd cups
```

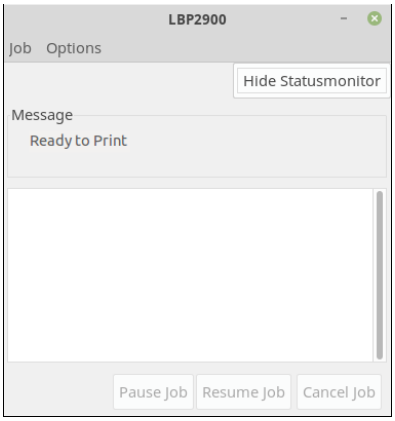
Добавьте в автозагрузку **ccpd**:

```
systemctl enable ccpd
```

Мониторинг состояния принтера
Просмотр статуса принтера:

```
captstatusui -P LBP2900
```

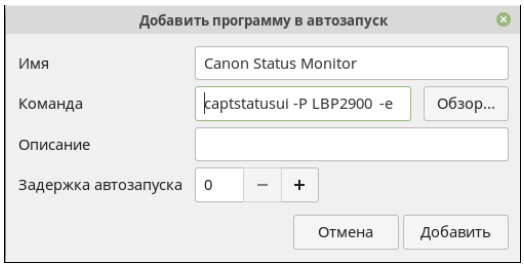
Появится окно с надписью "Ready to Print". Значит принтер готов к работе.



Для появления монитора состояния только при возникновении проблемы добавьте в автозагрузку команду:

```
captstatusui -P LBP2900 -e
```

Для этого откройте ***Параметры системы → Автозагрузка***, нажмите на кнопку добавить и в поле **"Команда"** впишите captstatusui -P LBP2900 -e



Опция **-e** указывает, что окно статуса не будет показываться до тех пор, пока не случится ошибка.

Также можно создать пользовательскую кнопку на рабочем столе, в команде запуска кнопки пропишите captstatusui -P LBP2900, данная настройка позволит пользователю управлять задачами печати: **"Resume job"**, **"Cancel Job"**. Например, после замены бумаги в лотке принтера, нажмите кнопку **"Resume job"** для возобновления печати.

Установка драйверов Pantum

Драйверы **Pantum** необходимы для начала работы на принтерах фирмы *Pantum*.

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки пакетов сначала необходимо установить пакет redos-3rdparty-pantum. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install redos-3rdparty-pantum
```

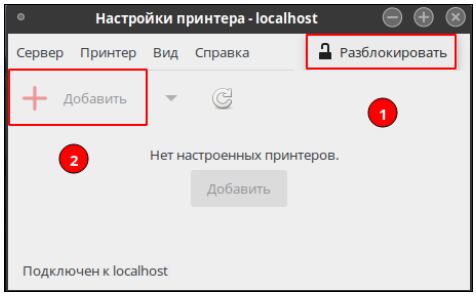
В результате будет подключен новый репозиторий **3rdparty-pantum**.

Далее необходимо установить пакеты с драйверами:

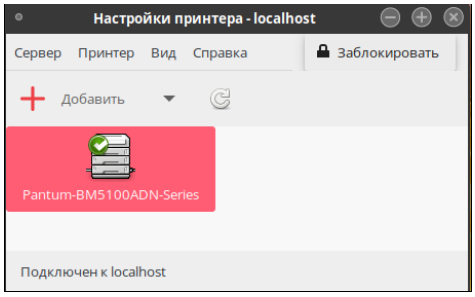
```
dnf install pantum-drivers-cups pantum-drivers-sane --refresh
```

После успешной установки драйверов необходимо подключить принтер. Сделать это можно через «**Главное меню**» - «**Администрирование**» - «**Настройки принтера**».

Для работы с программой необходимо нажать **Разблокировать**, потребуется ввести пароль администратора или суперпользователя (**root**) системы. После аутентификации добавьте новое устройство, нажав кнопку **Добавить**.

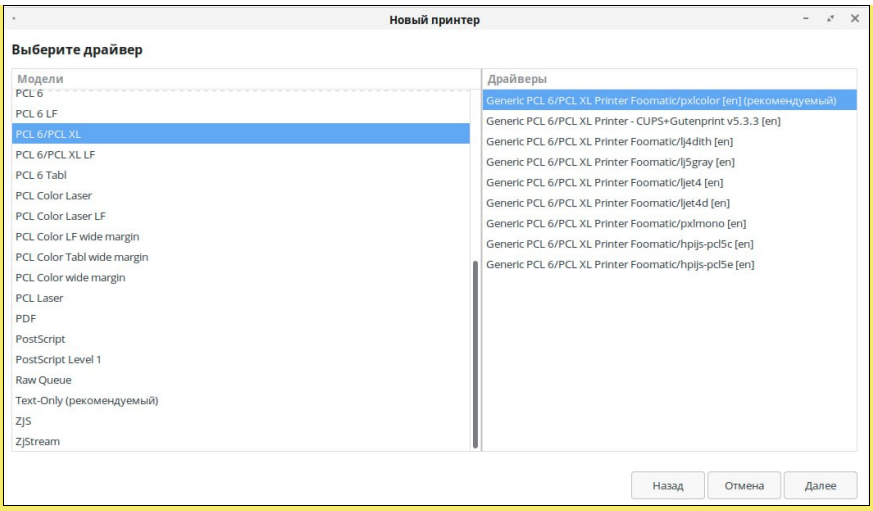


Если все настроено верно, принтер будет добавлен и готов к работе.



Примечание.

Если принтер не работает с родными драйверами, стоит попробовать использовать **Generic**. Для этого нажмите кнопку «**Добавить**», выберите устройство и нажмите «**Далее**», будет открыто окно для выбора необходимого драйвера. Выберите **Generic** и определите необходимую модель. После этого укажите описание принтера и нажмите кнопку «**Применить**».


Новый принтер
Выберите драйвер
Модели
PCL 6
PCL 6 LF
PCL 6/PCL XL
PCL 6/PCL XL LF
PCL 6 Tabl
PCL Color Laser
PCL Color Laser LF
PCL Color LF wide margin
PCL Color Tabl wide margin
PCL Color wide margin
PCL Laser
PDF
PostScript
PostScript Level 1
Raw Queue
Text-Only (рекомендуемый)
ZJS
ZjStream
Драйверы
Generic PCL 6/PCL XL Printer Foomatic/pxlcolor [en] (рекомендуемый)
Generic PCL 6/PCL XL Printer - CUPS+Gutenprint v5.3.3 [en]
Generic PCL 6/PCL XL Printer Foomatic/lj4dith [en]
Generic PCL 6/PCL XL Printer Foomatic/lj5gray [en]
Generic PCL 6/PCL XL Printer Foomatic/ljet4 [en]
Generic PCL 6/PCL XL Printer Foomatic/ljet4d [en]
Generic PCL 6/PCL XL Printer Foomatic/pxlmono [en]
Generic PCL 6/PCL XL Printer Foomatic/hpijs-pcl5c [en]
Generic PCL 6/PCL XL Printer Foomatic/hpijs-pcl5e [en]
Назад
Отмена
Далее

Настройка cups

Настройка возможности сбора аудита с серверов печати
Настройка централизованного назначения группам пользователей устройств печати
Копирование печатаемых файлов
Журналирование печати

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка возможности сбора аудита с серверов печати

По умолчанию логи работы Cups отправляются в syslog. Для того, что бы логи Cups стали доступны в панели администрирования Cups (по умолчанию панель администрирования Cups находится по адресу http://localhost:631/), требуется изменить файл:

```
nano /etc/cups/cups-files.conf
```

Приводим строки к виду:

```
ErrorLog /var/log/cups/error_log
PageLog /var/log/cups/page_log
AccessLog /var/log/cups/access_log
```

Добавьте в файл **/etc/cups/cupsd.conf** параметр **PageLogFormat**:

```
nano /etc/cups/cupsd.conf
```

```
PageLogFormat %p %u %j %T %P %C %{job-billing} %{job-originating-host-name} %{job-name} %{media} %{sides}
```

И измените значение **LogLevel**:

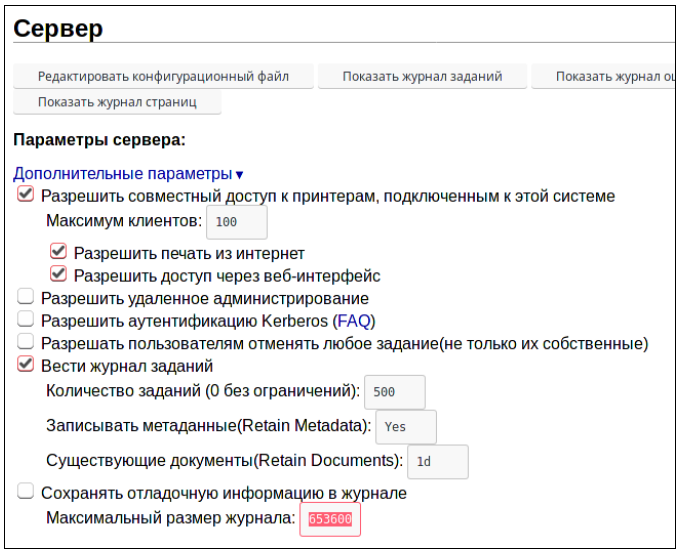
```
LogLevel info
```

Описание возможных уровней ведения лога:

- **debug2** - записывать все;
- **debug** - записывать почти все;
- **info** - записывать все запросы и изменения состояния;
- **warn** - запись ошибок и предупреждений;
- **error** - запись только ошибок;
- **none** - ничего не записывать.

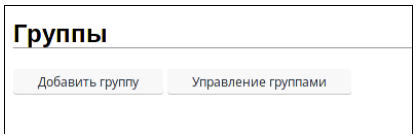
В параметре (**MaxLogSize**), отвечающем за максимальный размер файла, измените значение с "**0**" на нужное.

Пример настроек через веб-интерфейс http://localhost:631/ :



Настройка централизованного назначения группам пользователей устройств печати

Создайте группу:

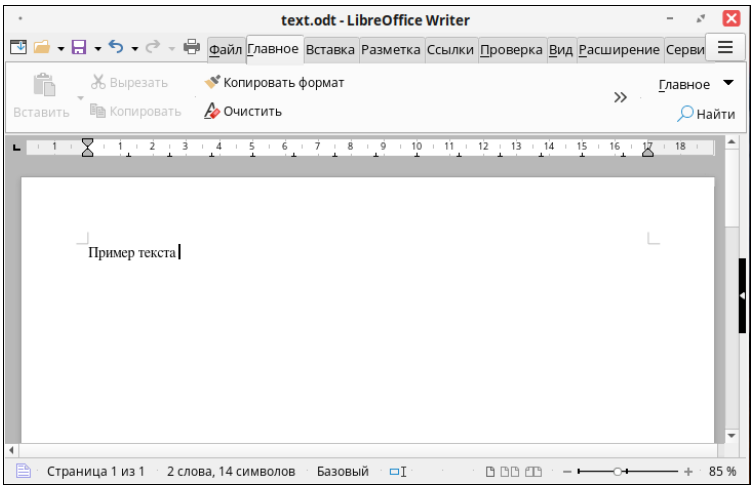


После создания группы нажмите "**Управление группами**", в выпадающем списке "**Администрирование**" выберите список разрешенных пользователей.

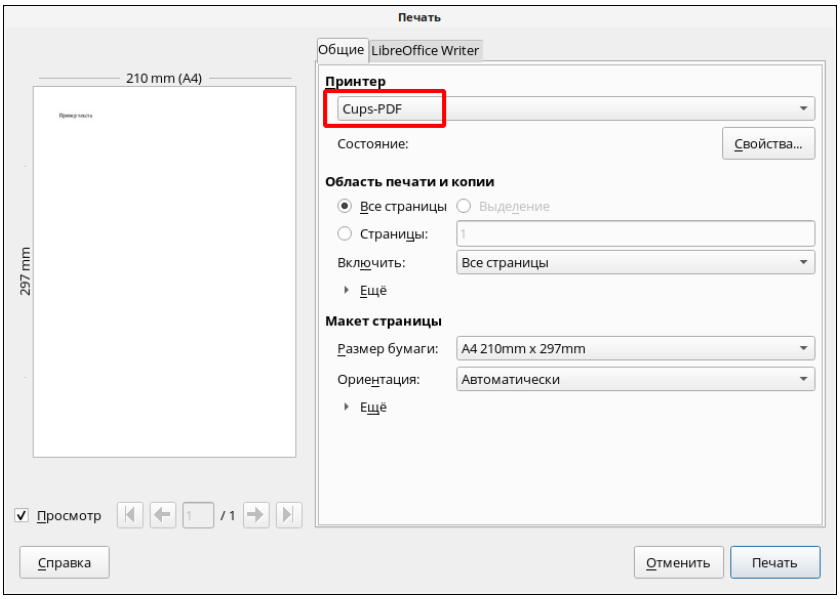
Впишите нужных пользователей, которым требуется разрешить доступ к группе устройств.

Копирование печатаемых файлов

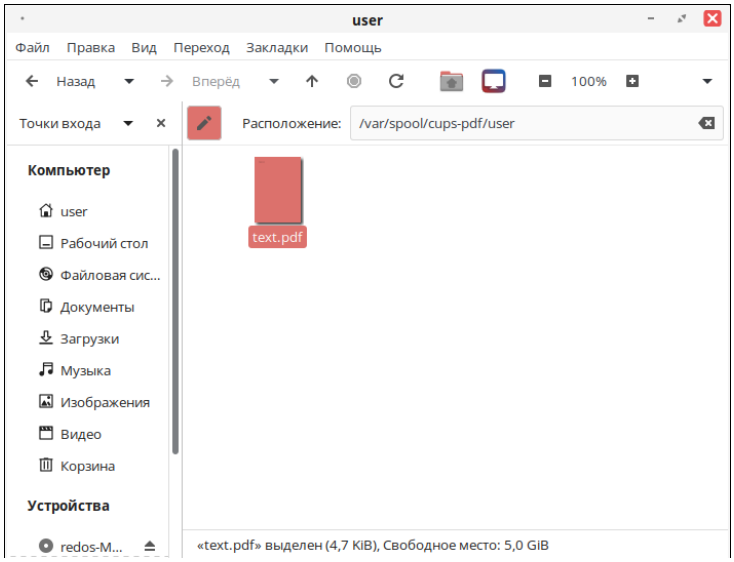
В РЕД ОС поддерживается функция теневого копирования файлов при использовании системы печати **CUPS**.



В примере будет использоваться виртуальный принтер **Cups-PDF** для наглядной демонстрации печати, а также расположения печатаемого файла и его копии.



По умолчанию распечатанный с помощью виртуального принтера файл отправляется в каталог **/var/spool/cups-pdf/<имя_пользователя>/**.



Распечатанный на обычном принтере файл будет располагаться в каталоге **/var/spool/<имя_принтера>/<имя_пользователя>/**.

Также, при использовании принтера, сервис **CUPS** автоматически создает рабочие файлы в каталоге **/var/spool/cups/**. Для доступа к данному каталогу требуются права суперпользователя. Проверку прав доступа можно осуществить командой:

```
ls -l /var/spool/ | grep "cups"

drwx--x---. 3 root lp 4096 апр 12 13:09 cups
drwxr-xr-x. 4 root root 4096 апр 12 13:09 cups-pdf
```

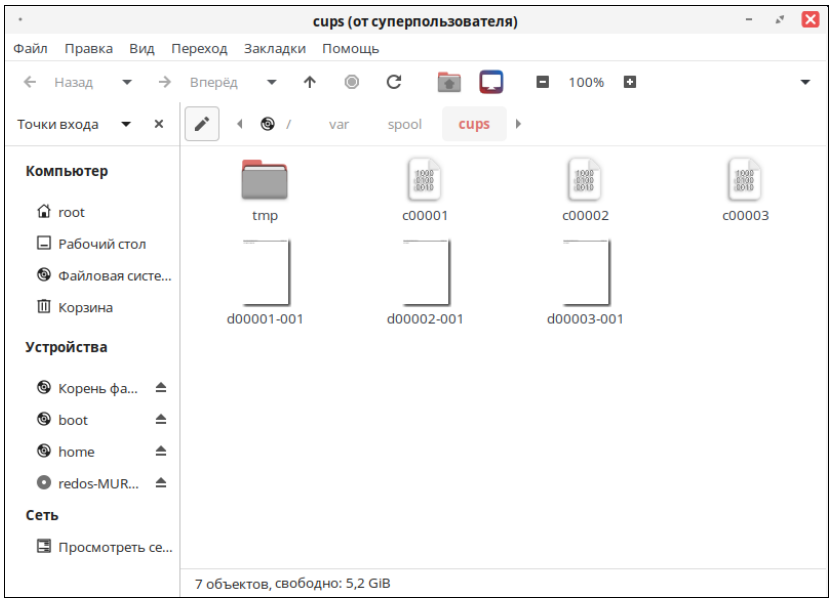
В каталоге хранятся файлы двух типов:

- **управляющие файлы**, начинающиеся на «**c**» («c00001», «c99999», «c100000» и т. д.);
- **файлы данных**, начинающиеся на «**d**» («d00001-001», «d99999-001», «d100000-001» и т. д.).

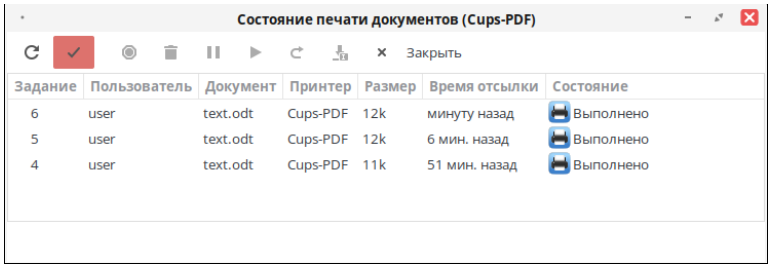
В именах файлов указывается **ID задания** из очереди печати, в данном случае задание имеет порядковый номер 1 — [d **00001**-001], и **ID принтера**, с которого производилась печать файла, в данном случае ID принтера — 1 [d00001- **001**].

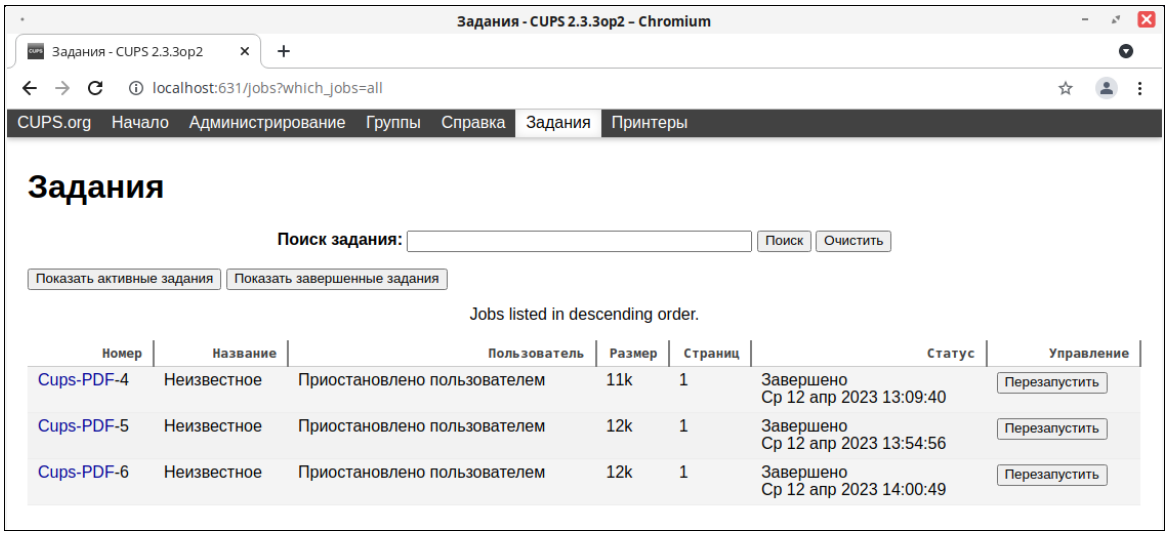
Управляющие файлы представляют собой сообщения, передаваемые принтеру с командами для печати, а файлы данных — это исходные файлы печати, отправленные на печать.

Файлы управления обычно очищаются после отправки 500-го задания, а файлы данных удаляются сразу после успешной печати задания.



Узнать ID заданий или процессов можно как локально в настройках CUPS системы, так и с помощью веб-формы.





Журналирование печати

В системе предусмотрено автоматическое журналирование печатаемых файлов. Активные и завершенные задания можно посмотреть в веб-интерфейсе во вкладке «**Задания**» (см. рисунок выше) или с помощью консольных команд:

- для завершенных заданий:

```
lpstat -W completed
```

- для незавершенных заданий:

```
lpstat -W not-completed
```

В выводе отображаются данные вида:

```
<принтер>-<ID_документа>-<пользователь>-<размер>-<дата>:<время>
```

Например:

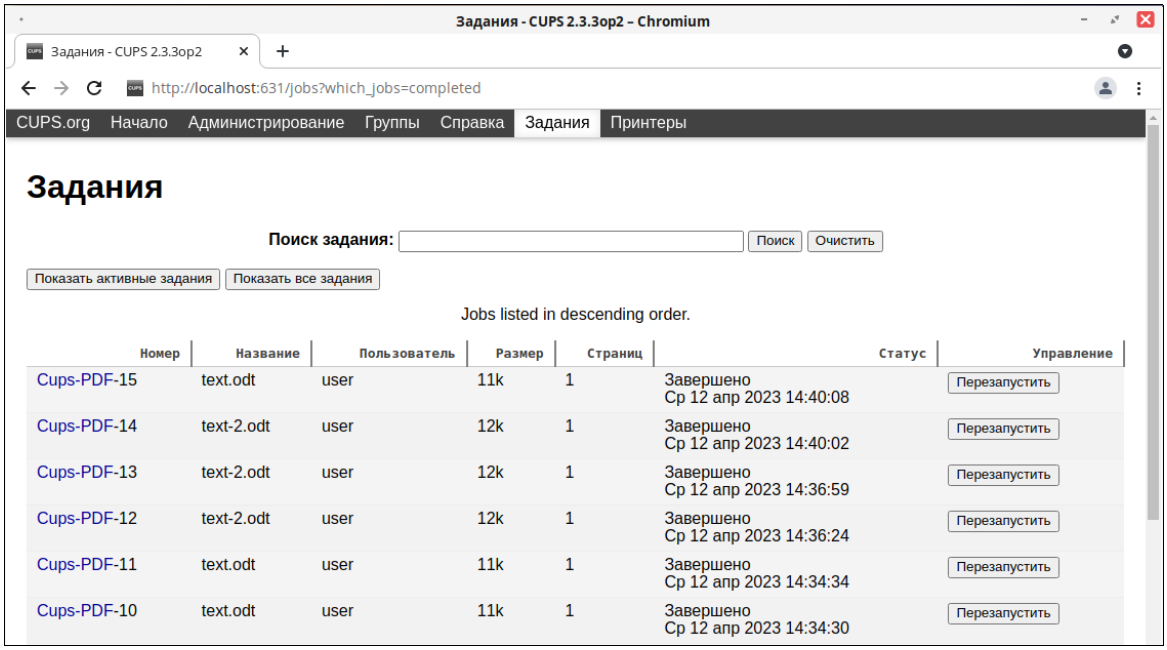
```
lpstat -W completed

Cups-PDF-7          user        12288   Ср 12 апр 2023 14:27:26
Cups-PDF-6          user        12288   Ср 12 апр 2023 14:00:49
Cups-PDF-5          user        12288   Ср 12 апр 2023 13:54:56
Cups-PDF-4          user        11264   Ср 12 апр 2023 13:09:40
```

Для приведения веб-интерфейса в более упорядоченный вид и демонстрации названия документа необходимо внести изменения в настройки **CUPS** — в файл конфигурации **/etc/cups/cupsd.conf**, например, изменив значения параметров JobPrivateAccess и JobPrivateValues в секции **<Policy default>** на указанные:

```
# Set the default printer/job policies...
<Policy default>
JobPrivateAccess all
JobPrivateValues none
```

Для принятия изменений необходимо перезагрузить систему.

После перезагрузки список заданий будет отображаться следующим образом:



Подключение сетевого принтера по IPP

Подключение сетевого принтера в конфигурации РЕД ОС - РЕД ОС
Отключение автоматического отображения сетевых принтеров

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

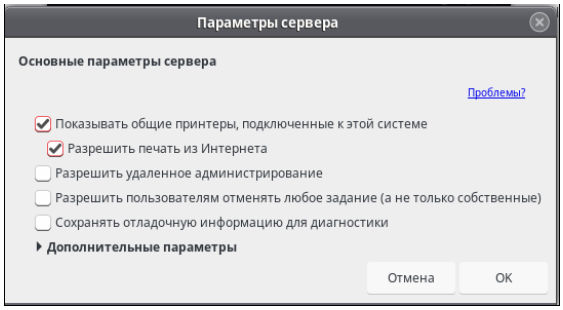
Подключение сетевого принтера в конфигурации РЕД ОС - РЕД ОС

1) Настройка ПК, к которому подключен принтер по **USB**.

Откройте управление принтерами: Меню - "Администрирование" - "Настройки принтера".

Принтер уже должен быть добавлен в качестве локального.

Далее требуется зайти в "Сервер" - "Параметры" и выставить флаги:



Далее требуется отредактировать конфигурационный файл. Откройте файл:

```
sudo nano /etc/cups/cupsd.conf
```

приведите строку к виду:

```
BrowseLocalProtocols dnssd cups
```

Перезапустите службу:

```
sudo systemctl restart cups
```

2) Настройка ПК, на котором будет совершаться подключение сетевого принтера:

Сначала проверьте доступ к **631** порту ПК, к которому будет подключение:

```
nmap -Pn -p 631 ip_adress
```

если утилита отсутствует, то выполните установку:

```
sudo dnf install nmap
```

ключевая фраза, которая интересует из вывода команды:

```
631/tcp open ipp
```

Далее требуется установить утилиту (если отсутствует):

```
sudo dnf install cups-ipptool
```

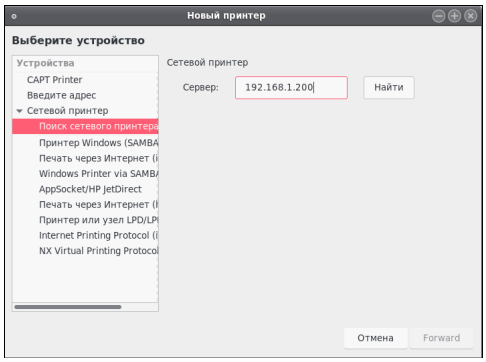
Перезапустите службу:

```
systemctl restart cups
```

Далее добавление принтера на клиентском компьютере.

Откройте: Меню - "Администрирование" - "Настройки принтера"

Нажмите "Добавить". "Network Printer" - "Find Network Printer" и введите IP-адрес ПК, к которому подключен принтер через usb.



Нажмите кнопку "Найти". После добавления принтера выполните печать тестовой страницы.

Отключение автоматического отображения сетевых принтеров

Чтобы отключить автоматическое добавление или отображение всех доступных сетевых принтеров необходимо отключить сервис avahi-daemon. Для этого выполните команды:

```
sudo systemctl disable avahi-daemon
sudo systemctl stop avahi-daemon
```

Подключение к РЕД ОС принтера, открытого в общий доступ на ОС Windows

Подключение через SAMBA. В локальной сети
Подключение через SAMBA. В доменной сети
Подключение с помощью LPD

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Подключение через SAMBA

В локальной сети

ВАЖНО!

Данная настройка касается только одноранговой локальной сети без доменной структуры. Для сетей в домене есть инструкция ниже. Перед настройкой, вы должны убедиться, что на компьютере Windows с подключенным принтером установлен драйвер, возможна печать, правильно настроен общий доступ к принтеру.

Для настройки подключения принтера используйте имя компьютера на котором он установлен, а не его ip-адрес см. статью.

1. Получите доступ к сетевым ресурсам Windows.

1.1 Откройте файл конфигурации **samba**:

```
nano /etc/samba/smb.conf
```

Следующие параметры должны быть в этом конфигурационном файле:

```
printing = cups
printcap name = cups
load printers = yes
cups options = raw
```

1.2 Создайте в РЕД ОС пользователя с таким же именем, как и на **windows**. Для этого выполните команду:

```
useradd -d /dev/null -s /sbin/nologin user
```

Таким образом будет создан пользователь **user**. Поскольку **Samba** использует пользователей которые уже есть в системе, то надо внести его в базу данных **SMB** и назначить пароль для доступа к общим ресурсам **windows**. Пароль такой же, как и на **windows**.

1.3 Создание пользователя samba и активируйте его:

```
smbpasswd -a user
smbpasswd -e user
```

Для проверки выведем список пользователей **samba**:

```
pdbedit -L -v
```

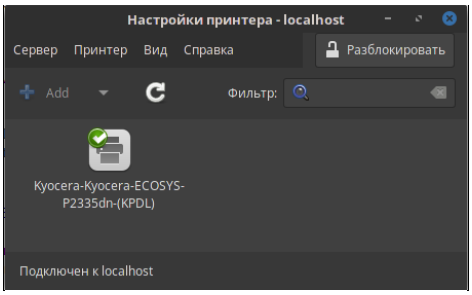
1.3 Проверяем доступ и смотрим имя принтера:

```
smbclient -L win_computer --user=user
Enter WORKGROUP\user's password:
Sharename Type Comment
--------- ---- -------
123 Disk
```

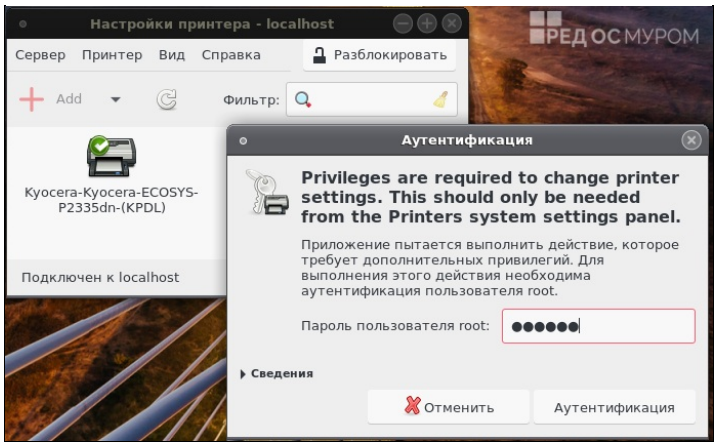
```
ADMIN$ Disk Удаленный Admin
C$ Disk Стандартный общий ресурс
IPC$ IPC Удаленный IPC
P2335 Printer P2335dn
print$ Disk Драйверы принтеров
```

Здесь имя принтера **P2335**. Когда публикуете принтер на **Windows** в общий сетевой доступ, то назначьте имя принтеру без пробелов!

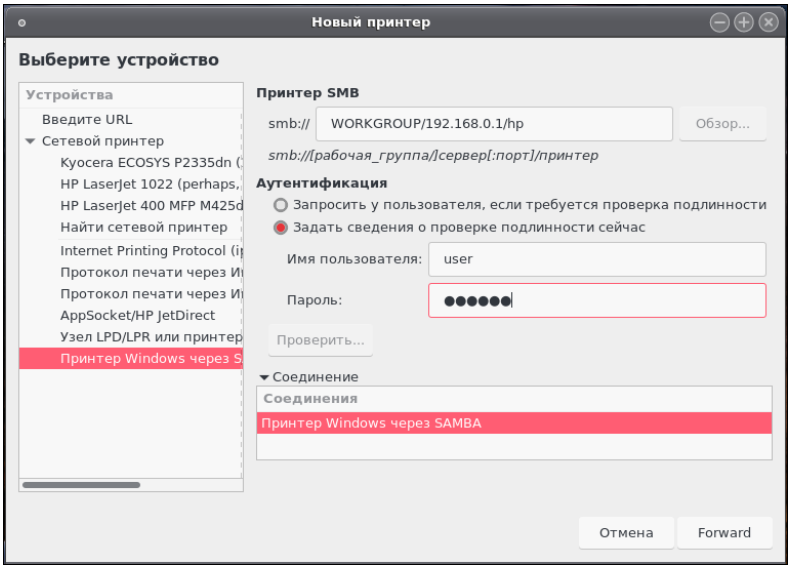
2. Откройте в меню вкладку «**Система**» - «**Администрирование**» - «**Настройки принтера**».



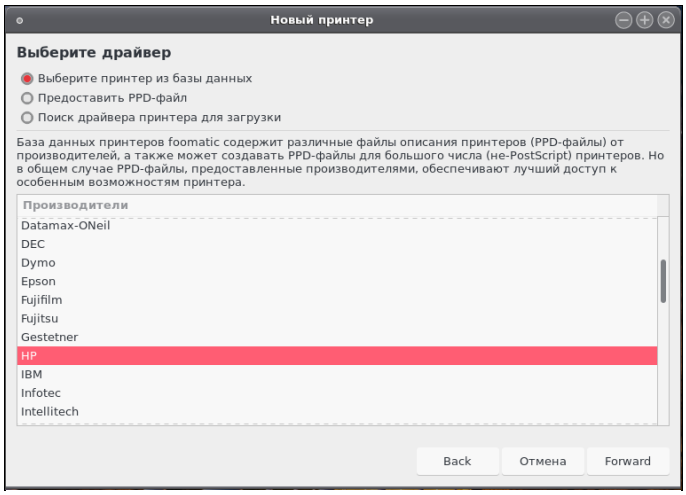
2.1 Нажмите кнопку «**Разблокировать**». Введите пароль текущего пользователя или пароль **root**, в зависимости от настроенных политик пользователей.

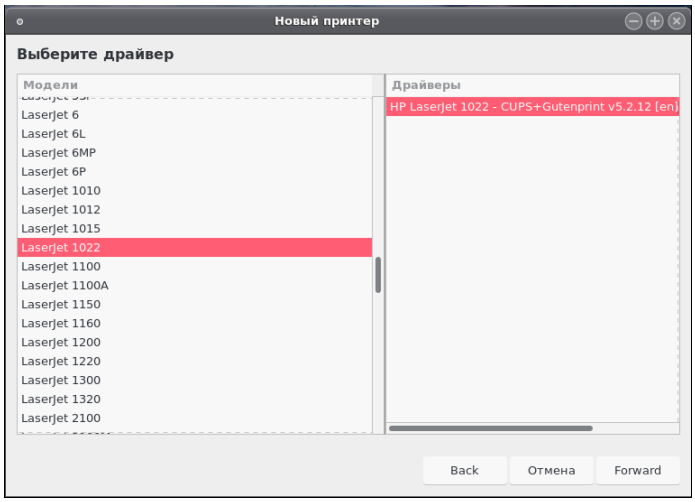


2.2 Нажмите кнопку «**Add**». В открывшемся окне выберите «**Принтер Windows через SAMBA**». Впишите рабочую группу, адрес принтера и сведения о проверки пользователя, если необходимо. Нажмите «**Forward**».

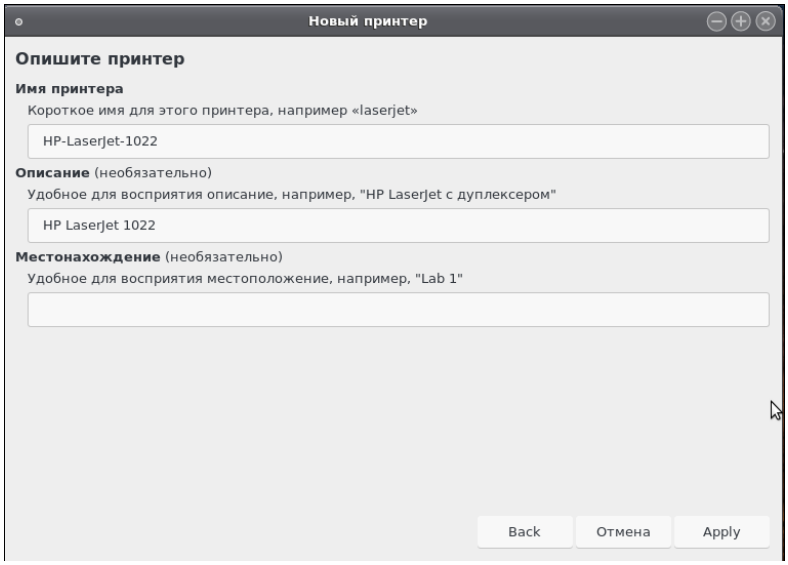


2.3 Выберите драйвер принтера из списка или предоставьте **PPD**.





2.4 Введите дополнительную информацию о принтере и/или нажмите «**Apply**».



2.5 Введите пароль текущего пользователя или пароль **root**, в зависимости от настроенных политик пользователей.

Все, принтер добавлен.

Некоторые принтеры могут работать с универсальным драйвером **Generic - PCL Laser**.

В доменной сети

1.1 Откройте файл конфигурации **samba**:

```
nano /etc/samba/smb.conf
```

Помимо других атрибутов, следующие параметры должны быть в этом конфигурационном файле:

```
printing = cups
printcap name = cups
load printers = yes
cups options = raw
```

1.2 Проверяем доступ и смотрим имя принтера:

```
smbclient -L 10.81.81.150 --user=domainuser
Enter DOMAIN\user's password:
Sharename Type Comment
--------- ---- -------
123 Disk
ADMIN$ Disk Удаленный Admin
C$ Disk Стандартный общий ресурс
IPC$ IPC Удаленный IPC
P2335 Printer P2335dn
print$ Disk Драйверы принтеров
```

Здесь имя принтера **P2335**.

Когда публикуете принтер на **Windows** в общий сетевой доступ, то назначьте имя принтеру без пробелов!

1.3 Далее выполните операции пункта 2.2, только вместо имени группы **WORKGROUP** должно быть указано имя домена.

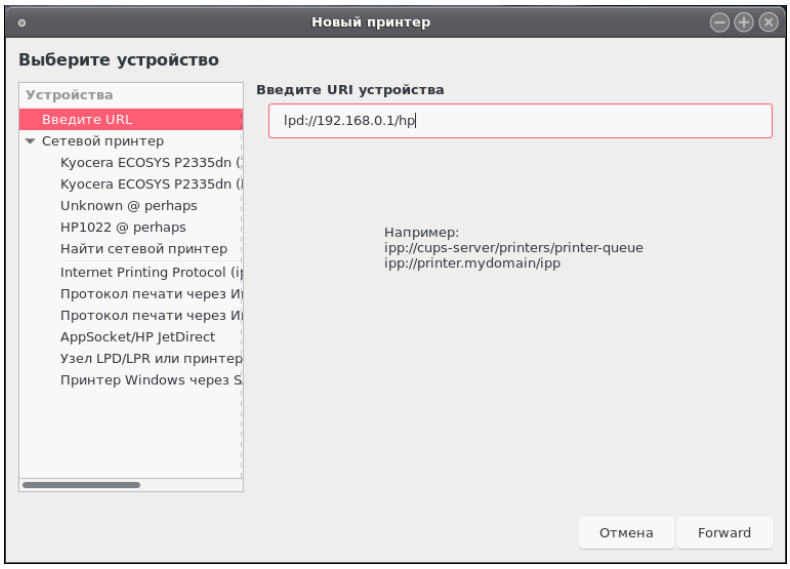
Подключение с помощью LPD

ВАЖНО!

Убедитесь, что следующие компоненты Windows добавлены в систему: служба печати LPD, клиент интернет-печати, монитор LPR-портов, факсы и сканирование Windows. Добавить их можно в панели управления в «**Включение или отключение компонентов Windows**». Убедитесь, что служба LPD запущена.

Для подключения по протоколу LPD впишите URI устройства, например:

lpd://192.168.0.1/hp



Дальнейшая настройка аналогична пунктам 2.2-2.4.

Подключение принтера к РЕД ОС и Windows открытого в общий доступ на РЕД ОС

Предварительная подготовка
Подключение через Samba
Подключение принтера в домене
Подключение принтера через протокол LPD

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка

> **Примечание.**
>
> Данный пункт актуален **только для систем, использующих брандмауэр firewalld**.

Перед началом настройки рекомендуется проверить статус брандмауэра **firewalld** с помощью команды:

```
firewall-cmd --state
```

Если в ответе команды отображается running, в конфигурацию брандмауэра **firewalld** необходимо добавить разрешающее правило для работы службы **samba**. Для этого выполните следующие команды (потребуются права **администратора**):

```
sudo firewall-cmd --add-service=samba --permanent
sudo firewall-cmd --reload
```

Подробную информацию о работе брандмауэра **firewalld** см. в нашей статье «Настройка брандмауэра Firewall».

Если в системе брандмауэр **firewalld** не используется или при проверке статуса выводится сообщение not running, перейдите к следующему пункту.

Подключение через Samba

Подключение принтера к ПК с Windows в рабочей группе

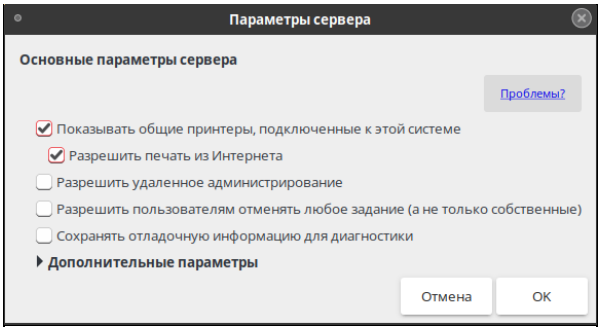
Первым шагом нужно внести машину с принтером в рабочую группу **WORKGROUP** (за имя группы отвечает параметр «*workgroup*», для примера взята рабочая группа *WORKGROUP*), для этого откройте конфигурационный файл samba и приведите секцию **[global]** к виду:

```
nano /etc/samba/smb.conf

[global]
   workgroup = WORKGROUP
   security = user
   map to guest = bad user
   passdb backend = tdbsam

   printing = cups
   printcap name = cups
   load printers = yes
   cups options = raw
```

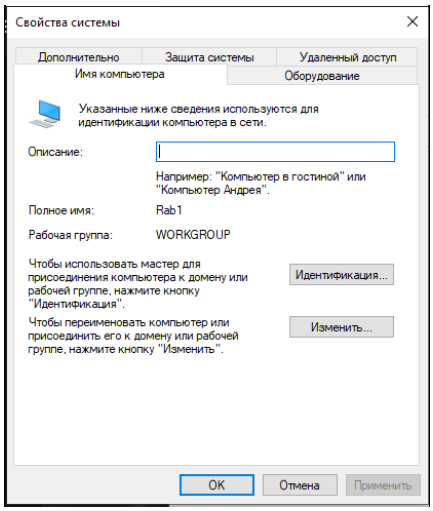
Запустите **Samba** и добавьте ее в автозагрузку:

```
systemctl start smb
systemctl enable smb
```

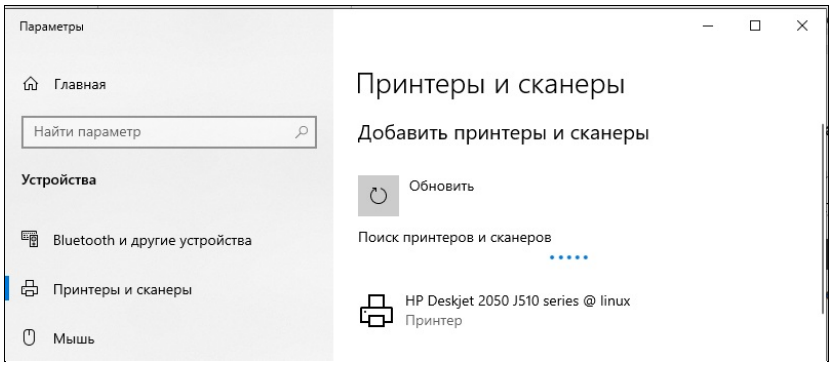
После этого перейдите в **Системное меню – «Администрирование» – «Настройки принтера» – «Сервер» – «Параметры»** и поставьте галочку на следующих пунктах:



Windows должен находиться в той же рабочей группе, что и РЕД ОС. Убедитесь в том, что компьютер на *Windows* находится в той же рабочей группе, перейдя в свойства системы (для *Windows 10*: **«Свойства системы» – «Дополнительные параметры системы» – «Имя компьютера»)**.

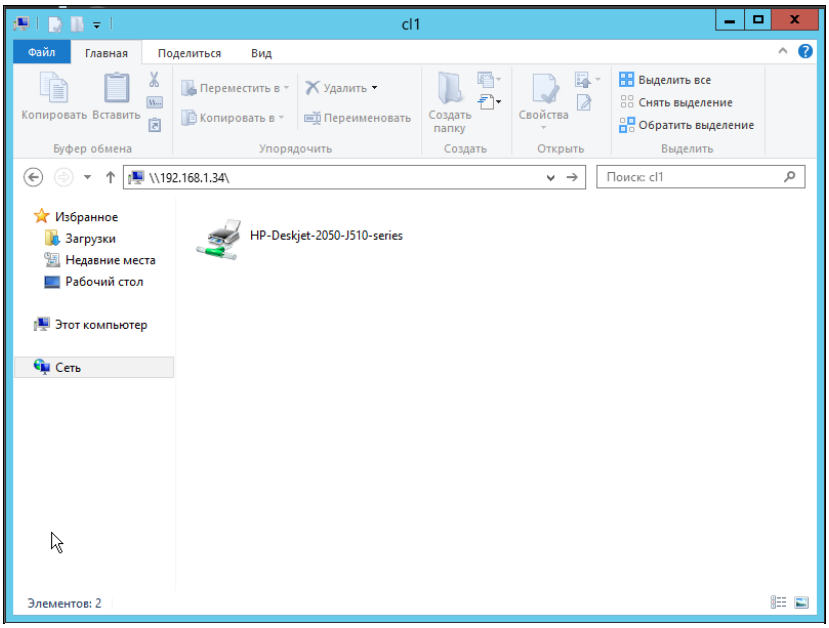


Теперь вы можете добавить принтер в Windows, выберите **«Принтеры и сканеры» – «Добавить принтер или сканер»**.



Принтер будет доступен в проводнике по адресу:

\\<IP_адрес_сервера>



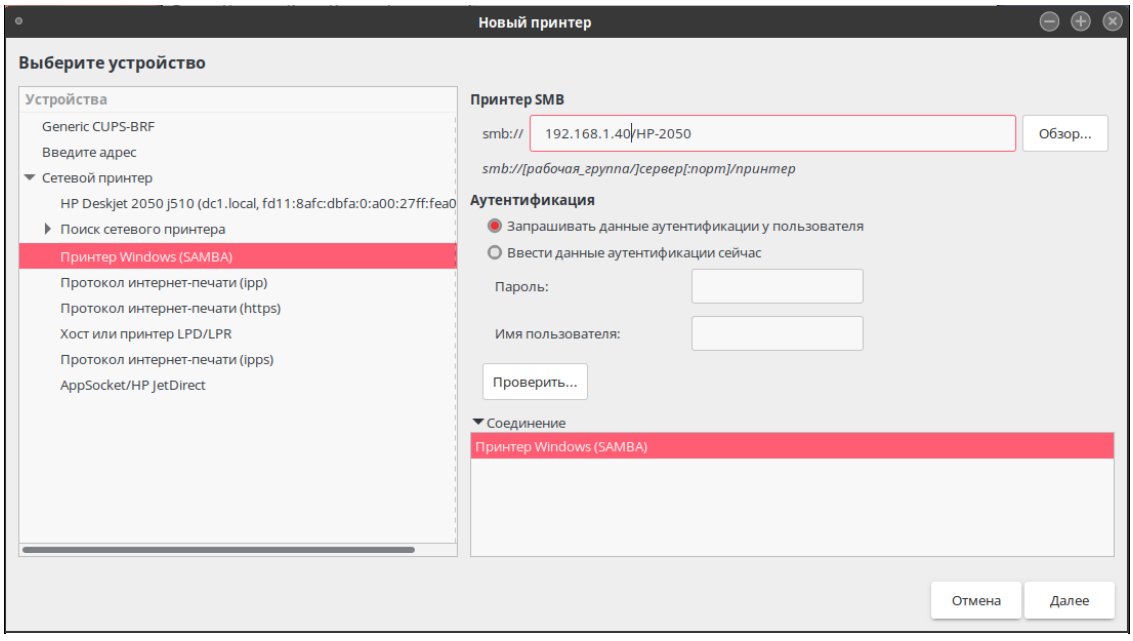
Подключение принтера к ПК с РЕД ОС в рабочей группе

Первым шагом нужно внести машину с принтером в рабочую группу **WORKGROUP** (за имя группы отвечает параметр «*workgroup*», для примера взята рабочая группа *WORKGROUP*), для этого откройте конфигурационный файл **samba** и приведите секцию **[global]** к виду:

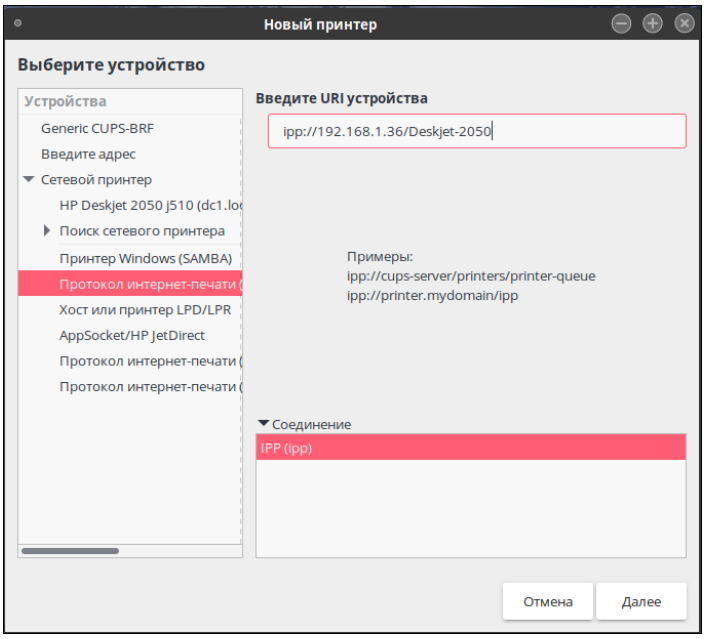
```
nano /etc/samba/smb.conf

[global]
  workgroup = WORKGROUP
  security = user
  map to guest = bad user
  passdb backend = tdbsam

  printing = cups
  printcap name = cups
  load printers = yes
  cups options = raw
```

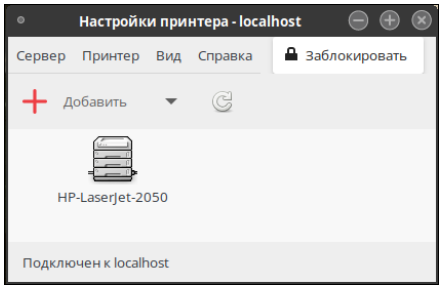
Перейдите в **Системное меню – «Администрирование» – «Настройка принтера» – «Разблокировать» – «Добавить»**. Открытый в общий сетевой доступ на основной машине принтер должен появиться в «**Сетевой принтер**» первым.

Вы можете добавить принтер **Samba** через IP-адрес:



Также вы можете добавить принтер через **«Сетевой принтер» - «Протокол интернет-печати IPP»**.



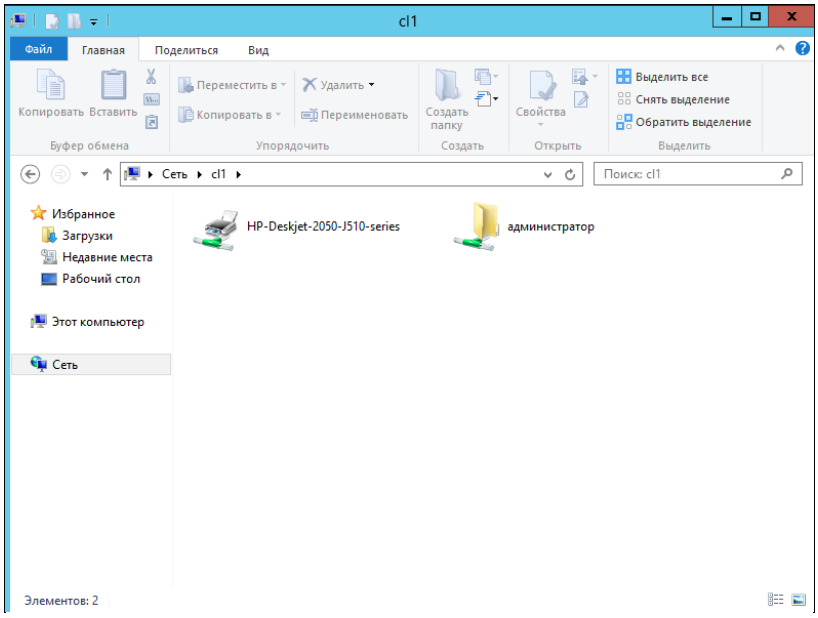


Подключение принтера в домене

Подключение принтера в домене РЕД ОС на пользователя домена с ОС Windows

Открытый в общий сетевой доступ принтер на РЕД ОС будет отображаться в проводнике по адресу:

\\<доменное_имя_(или_адрес)>



Подключение принтера в домене РЕД ОС на пользователя домена с ОС РЕД ОС

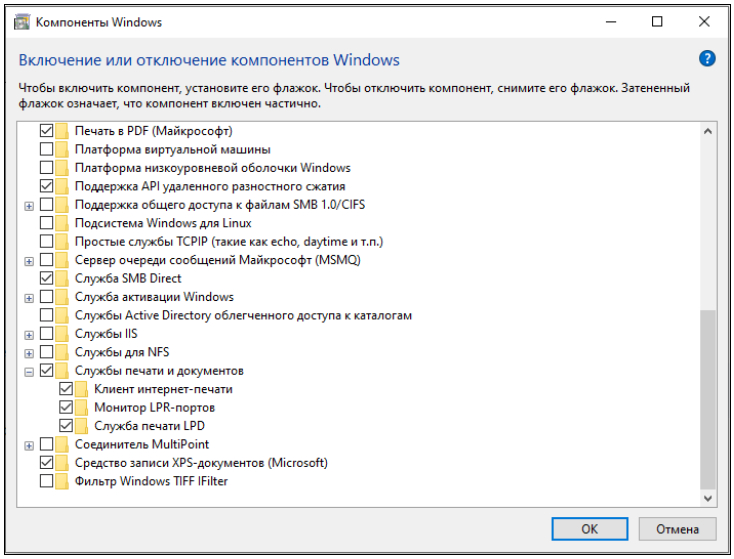
Открытый сетевой принтер на РЕД ОС будет отображаться в **Главное меню – «Администрирование» – «Настройка принтера» – «Разблокировать» – «Добавить» – «Сетевой принтер»**.

Принтер будет иметь имя сервера или клиента в конце.

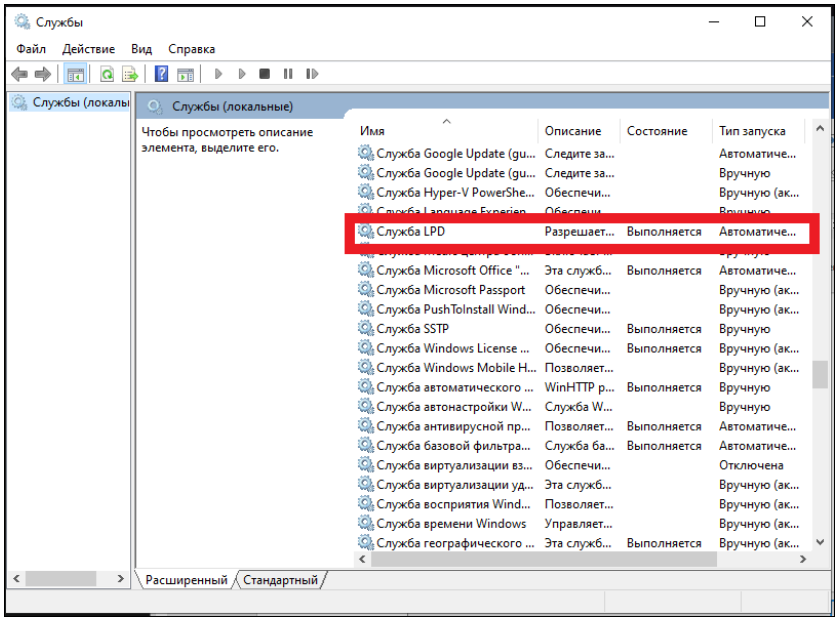
Подключение принтера через протокол LPD

LPD — сетевой протокол прикладного уровня для передачи документов на печать, предоставляющий базовые возможности печати.

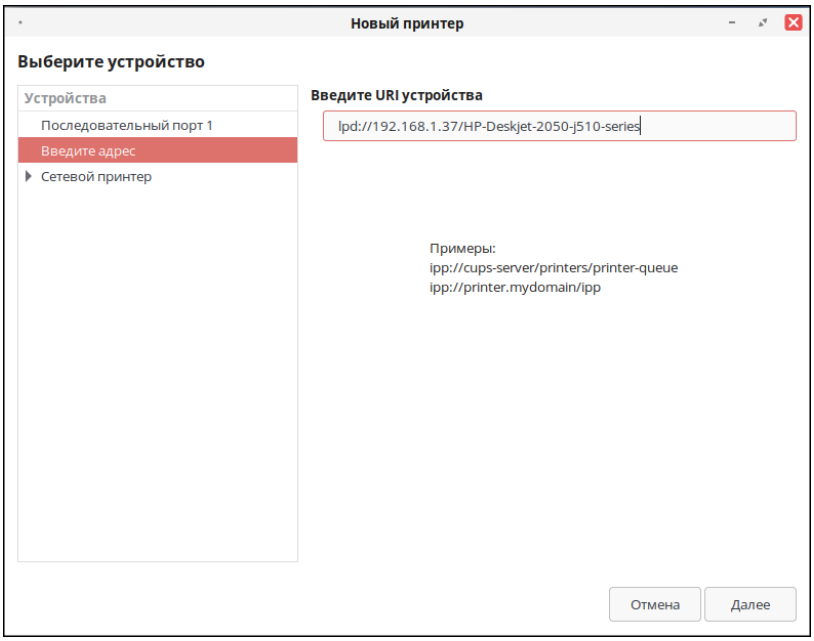
Для подключения принтера через протокол LPD на *Windows* (в данном примере используется *Windows 10*) подключите два компонента в «**Включение или отключение компонентов Windows**»: «**Служба печати LPD**» и «**Монитор LPR-портов**».

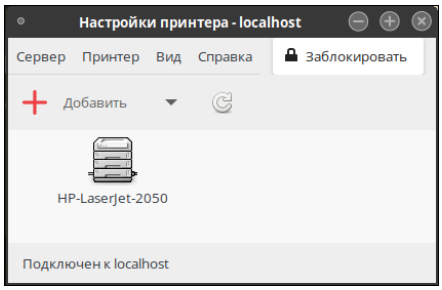


Далее в «**Службы**» должна появиться служба **LPD**.



В РЕД ОС в свойствах принтера необходимо выбрать «**Введите адрес**», в котором следует указать путь к принтеру в формате:


Новый принтер
Выберите устройство
Устройства
Последовательный порт 1
Введите адрес
Сетевой принтер
Введите URI устройства
lpd://192.168.1.37/HP-Deskjet-2050-j510-series
Примеры:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp
Отмена
Далее


Настройки принтера - localhost
Сервер
Принтер
Вид
Справка
Заблокировать
Добавить
HP-LaserJet-2050
Подключен к localhost

Установка драйверов foo2zjs

foo2zjs - это открытый драйвер для принтеров, которые используют протокол печати Zenographics ZjStream, таких как Minolta magicolor 2200/2300/2430 DL, Minolta Color PageWorks/Pro L и HP LaserJet 1000/1005/1018/1020/1022.

```
# dnf install foo2zjs
```

Данные драйверы поддерживают определенный ряд устройств, список приведен ниже:

Модель принтера	Тип печати
Konica Minolta magicolor 2430 DL	B/W and color
Minolta/QMS 2300 DL	B/W and color
Minolta/QMS 2200 DL	B/W and color
HP LaserJet P2035	B/W
HP LaserJet M1319 MFP	B/W
HP LaserJet Pro P1606dn	B/W
HP LaserJet Pro P1566	B/W
HP LaserJet Pro P1102	B/W
HP LaserJet Pro CP1025nw	B/W and color
HP LaserJet 1022	B/W
HP LaserJet 1020	B/W
HP LaserJet 1018	B/W
HP LaserJet 1005	B/W
HP LaserJet 1000	B/W
HP Color LaserJet CP1215	B/W and color
HP Color LaserJet 1600	B/W and color
HP Color LaserJet 2600n	B/W and color
Konica Minolta magicolor 2530 DL	B/W and color
Konica Minolta magicolor 2490 MF	B/W and color
Xerox Phaser 6115MFP	B/W and color
Konica Minolta magicolor 2480 MF	B/W and color
Konica Minolta magicolor 1690MF	B/W and color
Konica Minolta magicolor 1680MF	B/W and color
Konica Minolta magicolor 1600W	B/W and color
Samsung CLP-300	B/W and color
Samsung CLP-315	B/W and color
Samsung CLP-325	B/W and color
Samsung CLP-365	B/W and color
Samsung CLP-600	B/W and color
Samsung CLP-610	B/W and color
Samsung CLP-2160	B/W and color
Samsung CLP-3160	B/W and color
Samsung CLP-3175	B/W and color
Xerox Phaser 6110	B/W and color
Xerox Phaser 6110MFP	B/W and color
HP LaserJet M1005 MFP	
HP LaserJet M1120 MFP	
HP LaserJet P1005	
HP LaserJet P1006	

HP LaserJet P1007	
HP LaserJet P1008	
HP LaserJet P1505/P1505n	
HP LaserJet P2014/P2014n	
HP LaserJet Pro M1212nf MFP	
Oki C301dn	
Oki C310dn	
Oki C511dn	
Oki C810dn	
Oki C3100n/C3200n	
Oki C3300n/C3400n	
Oki C3530n MFP	
Oki C5100n/C5150n/C5200n	
Oki C5500n/C5600n/C5800n	
Dell 1355 Multifunction Color Printer	
Dell C1765 Multifunction Color Printer	
Epson AcuLaser CX17NF	
Epson AcuLaser M1400	
Fuji Xerox DocuPrint CM205 Multifunction Color Printer	
Fuji Xerox DocuPrint CM215 Multifunction Color Printer	
Fuji Xerox DocuPrint M215	
Fuji Xerox DocuPrint P205	
Xerox WorkCentre 3045 Multifunction Monochrome Printer	
Xerox WorkCentre 6015 Multifunction Color Printer	

Установка принтеров Samsung

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

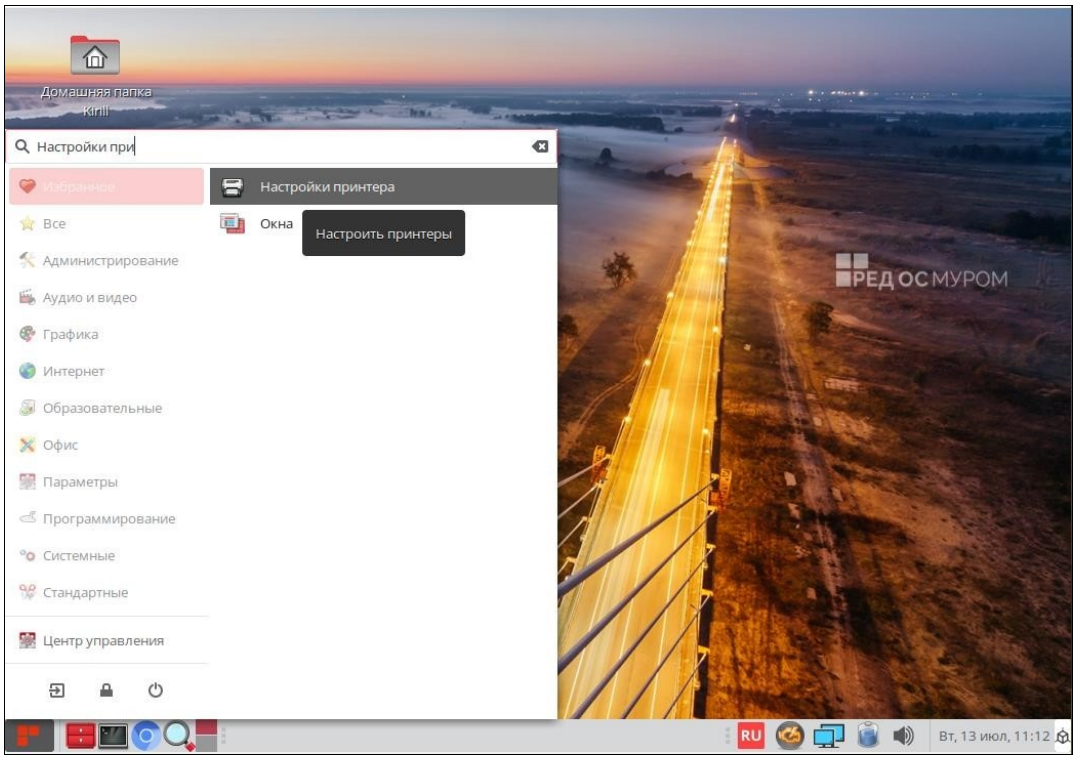
- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС.
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

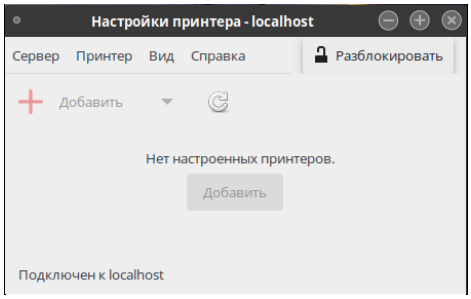
Перед настройкой принтера необходимо с правами администратора установить **OpenPrintingPPDs-ghostscript** и **OpenPrintingPPDs-postscript** актуальной версии командами:

```
dnf install OpenPrintingPPDs-ghostscript
dnf install OpenPrintingPPDs-postscript
```

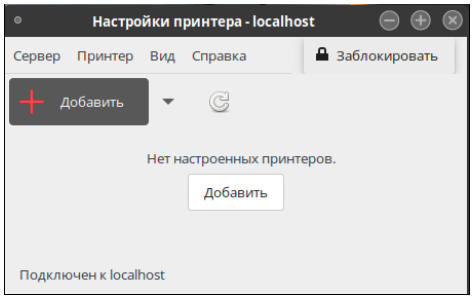
Затем запустите «**Настройки принтера**».



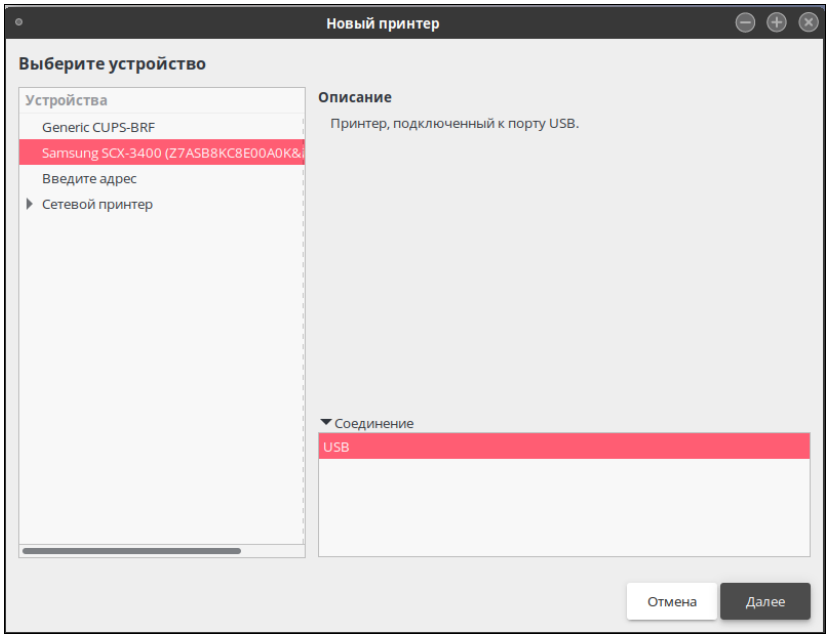
Изначально функция добавления принтеров недоступна.



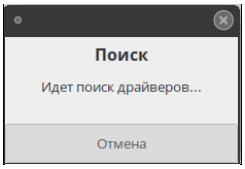
Для того чтобы разблокировать функцию добавления принтеров, нажмите «**Разблокировать**» и введите пароль администратора, далее нажмите «**Добавить**».

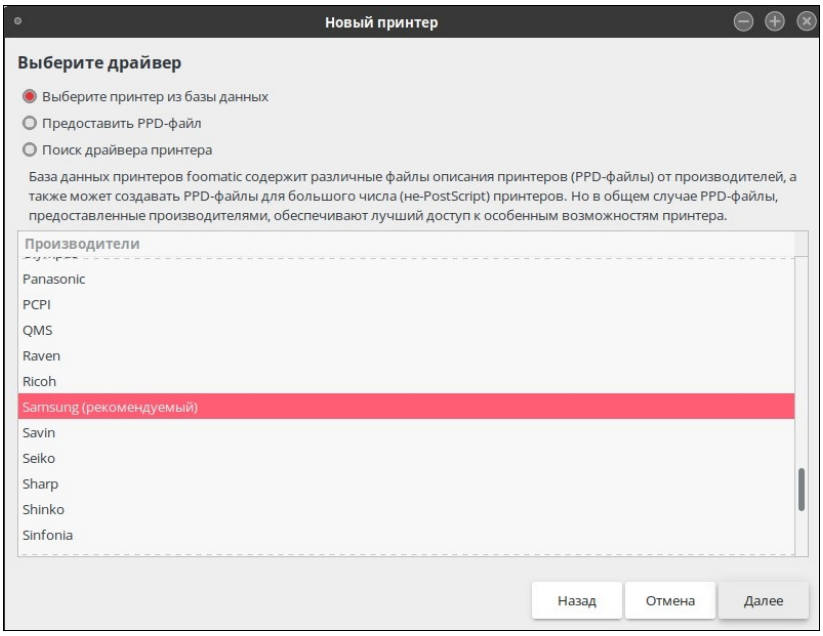


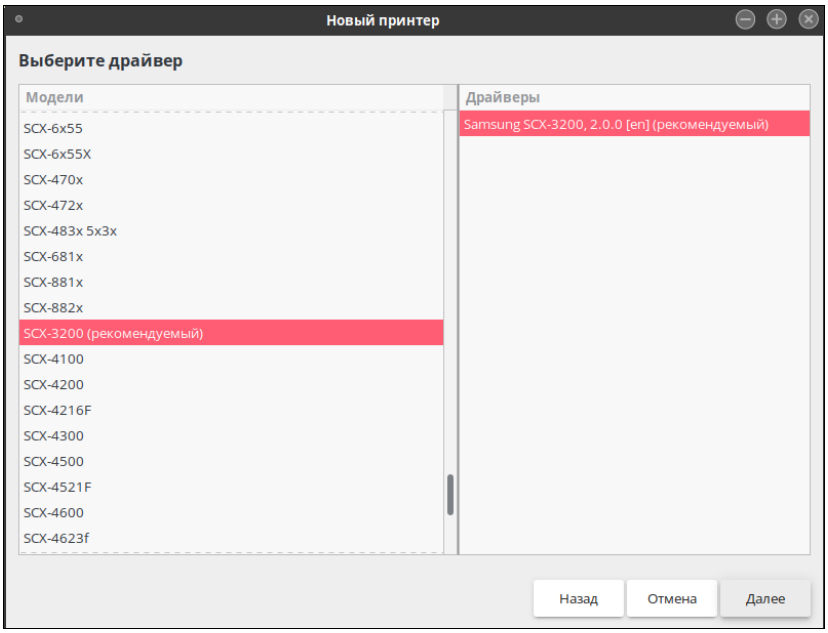
В данном примере принтер **Samsung SCX-3400** подключен по USB, выберите нужный принтер и нажмите « **Далее**».



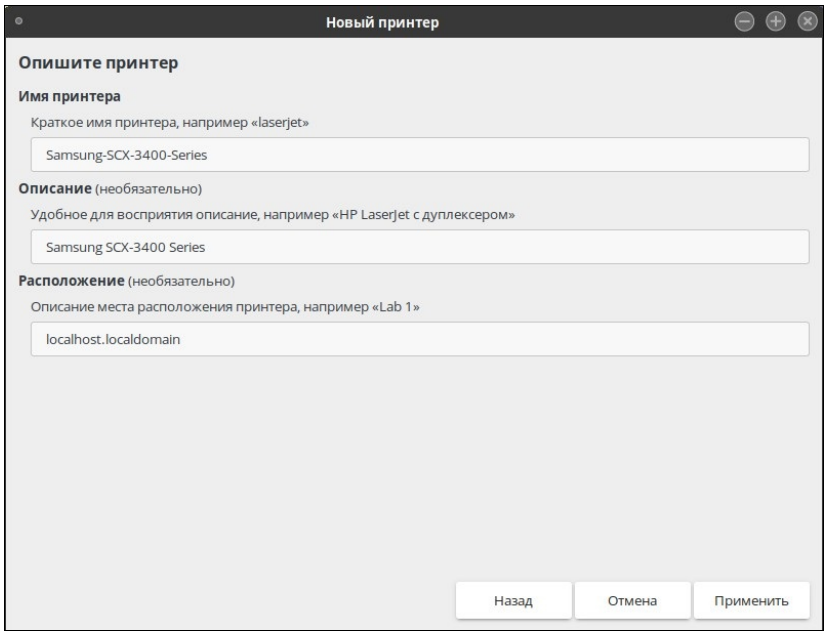
После поиска драйверов приложение корректно предлагает необходимый драйвер.



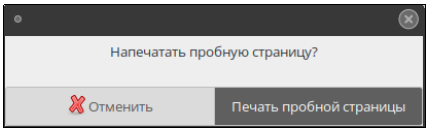




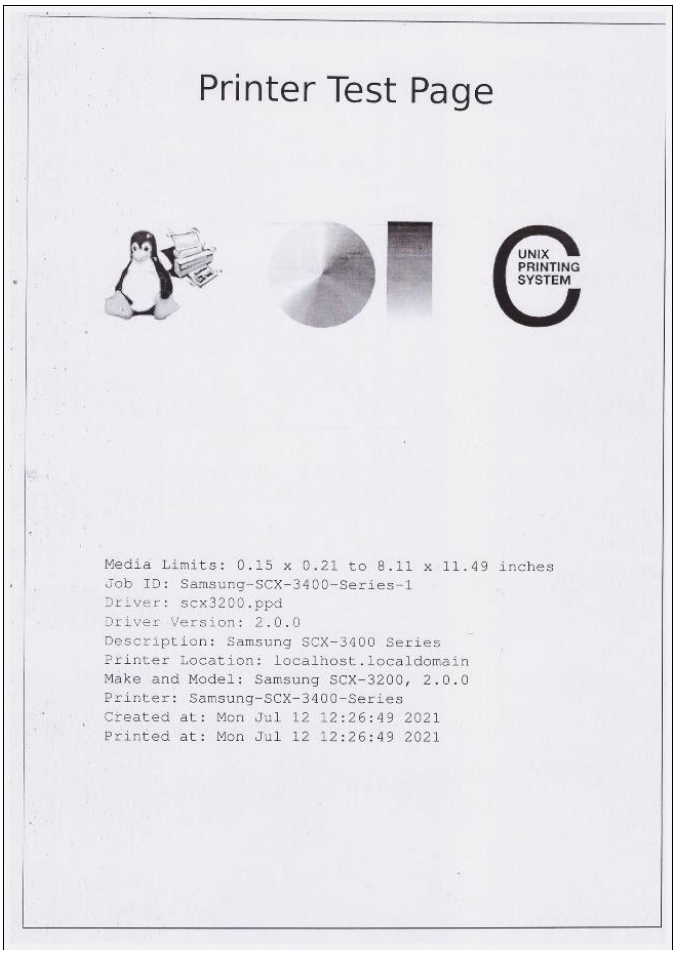
На данном этапе можно дать описание принтеру для удобства дальнейшего использования.



Для проверки работоспособности можно напечатать пробную страницу.



Внешний вид пробной страницы.



Список принтеров

Список принтеров Samsung, драйвера для которых устанавливаются описанным выше способом.

1. Samsung C48X	33. Samsung CLP-770
2. Samsung C140X	34. Samsung CLP-775
3. Samsung C145X	35. Samsung CLX-92X1 93X1
4. Samsung C268X	36. Samsung CLX-216X
5. Samsung C460	37. Samsung CLX-981X
6. Samsung C470	38. Samsung CLX-982X
7. Samsung C1810	39. Samsung CLX-2170
8. Samsung C1860	40. Samsung CLX-3160
9. Samsung C2620	41. Samsung CLX-3300
10. Samsung C2670	42. Samsung CLX-4190
11. Samsung C4820	43. Samsung CLX-6200
12. Samsung CLP-200	44. Samsung CLX-6220
13. Samsung CLP-300	45. Samsung CLX-6240
14. Samsung CLP-310	46. Samsung CLX-6250
15. Samsung CLP-310N	47. Samsung CLX-6260
16. Samsung CLP-315	48. Samsung CLX-8380
17. Samsung CLP-350	49. Samsung CLX-8385
18. Samsung CLP-410	50. Samsung CLX-8385X
19. Samsung CLP-500	51. Samsung CLX-8540
20. Samsung CLP-510	52. Samsung CLX-8640 8650
21. Samsung CLP-550	53. Samsung CLX-9250 9350

22. Samsung CLP-550N	54. Samsung CLX-9252 9352
23. Samsung CLP-600	55. Samsung K-401 – K7600
24. Samsung CLP-610	56. Samsung M262X 282X
25. Samsung CLP-620	57. Samsung M267X 287X
26. Samsung CLP-650	58. Samsung M283X – M458X
27. Samsung CLP-650N	59. Samsung ML1000 – ML8950
28. Samsung CLP-660	60. Samsung SCX-470X – SCX-8240
29. Samsung CLP-660N	61. Samsung SF-565P
30. Samsung CLP-660ND	62. Samsung SI-630A
31. Samsung CLP-670	63. Samsung X401 – X7600
32. Samsung CLP-680	

Настройка сканеров

Проверка поддержки сканера в Linux на уровне драйверов
Проверка распознавания системой сканера, как устройства
Разрешение сканеру обращаться к ядру системы

Вы можете подробнее ознакомиться с примерами установки и подключения сканеров, просмотрев наши обучающие видео:

- на **RuTube** — Работа со сканерами в РЕД ОС;
- в **Яндекс.Дзен** — Работа со сканерами в РЕД ОС.
- в **VK Видео** — Работа со сканерами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Проверка поддержки сканера в Linux на уровне драйверов

Прежде всего стоит проверить, поддерживается ли подключенный или планируемый к покупке сканер на уровне драйверов. Данную информацию можно получить на сайте проекта SANE. В частности, на странице раздела со стабильной поддержкой (http://www.sane-project.org/sane-mfgs), где рекомендуется выполнять поиск по производителю (заголовок «**Scanners**», список «**Manufacturers**»).

Данные о сканерах представлены в таблицах, где стоит обратить особое внимание на столбец «**Статус**», в котором могут быть указаны следующие параметры:

- **Complete** — полная поддержка;
- **Good** — поддерживается большинство функций;
- **Basic** — поддерживается только базовый функционал;
- **Unsupported** — не поддерживается;
- **Untested** — не тестировался, вероятнее всего работать не будет, но можно проверить самостоятельно или выполнить поиск драйверов в нестабильной ветке SANE.

Если «**Статус**» имеет последние два значения, то сканер не заработает.

Если указанной модели сканера нет в списке, необходимо выполнить проверку на сайте производителя. Если вендор предоставляет драйвера для сканера, тогда необходимо их скачать и установить (обычно в архиве с драйвером предоставляется скрипт, который автоматически устанавливает драйвер).

Если сканер поддерживается, но в данный момент не сканирует, можно применить следующие рекомендации.

Ряд устройств поддерживается драйверами **sane-airscan**, список поддерживаемых устройств доступен по ссылке — https://github.com/alexpevzner/sane-airscan.

Ряд устройств **HP** поддерживаются **libsane-hpaio** из пакета **hplip**, список устройств доступен по ссылке — https://developers.hp.com/hp-linux-imaging-and-printing/supported_devices/index.

Проверка распознавания системой сканера, как устройства

Сначала рекомендуется проверить, определяется ли сканер физически. Большинство сканеров подключается по **USB**, поэтому необходимо открыть терминал и ввести команду, показывающую все подключенные USB-устройства:

```
lsusb

 или

sane-find-scanner
```

Если в списке нет нужного сканера, то, скорее всего, проблема аппаратная. Стоит проверить, подключён ли сканер по **USB**, не переломился ли кабель и исправен ли сам сканер. Также могут быть проблемы с распознаванием сканера в **BIOS** или **UEFI** компьютера. Часто помогает отключение **XHCI** в **UEFI**.

Если же в выводе терминала есть строка вида (наименование сканера и ID могут отличаться):

```
Bus 003 Device 005: ID 04a9:2220 Canon, Inc. CanoScan LIDE 25
```

значит система видит сканер как USB-устройство и можно продолжить настройку.

Теперь нужно ввести в терминале:

```
scanimage -L
```

Если система не может выполнить команду, то, вероятно, не установлен пакет **sane-backends**. Для установки пакета выполните:

```
dnf install sane-backends
```

Затем повторите ввод:

```
scanimage -L
```

Положительным ответом будет считаться строка, аналогичная данной:

```
device `plustek:libusb:003:008' is a Canon CanoScan LiDE25 flatbed scanner
```

Если терминал выдаёт отрицательный ответ (примерно следующего вида):

```
No scanners were identified. If you were expecting something different,
check that the scanner is plugged in, turned on and detected by the
sane-find-scanner tool (if appropriate). Please read the documentation
which came with this software (README, FAQ, manpages)
```

это может означать:

- аппаратную проблему;
- отсутствие прав на работу со сканером у активной в данный момент учётной записи пользователя;
- сканеру запрещено обращаться к ядру (где обычно находятся драйвера).

Про решение аппаратных проблем было сказано выше.

Перейдем к настройке прав учётной записи пользователя.

Введённая в терминал команда:

```
whoami
```

покажет логин активного в данный момент пользователя.

Далее нужно определить, в каких группах состоит этот пользователь:

```
groups <имя_пользователя>
```

где <имя_пользователя> — логин, полученный по команде whoami.

Если в этом списке не указана группа **lp**, необходимо добавить пользователя в группу:

```
sudo usermod -G lp -a user1
```

где user1 — логин добавляемого пользователя.

Для тестирования сканера выполните команду:

```
scanimage -T
```

Разрешение сканеру обращаться к ядру системы

Если ответ терминала по-прежнему отрицательный, то, возможно, сканеру запрещено обращаться к ядру. Разрешение можно предоставить, отредактировав конфигурационный файл **40-libsane.rules**, или если такого файла нет, **60-libsane.rules** в текстовом редакторе, запущенном с правами суперпользователя:

```
sudo nano /lib/udev/rules.d/40-libsane.rules
```

В открывшемся тексте должна отображаться строка с параметрами сканера со схожим названием. Нужно скопировать строку с этими данными и вставить её копию сразу под найденной, заменив в копии название сканера и номера idVendor и idProduct на полученные ранее по команде lsusb. Например:

В качестве примера будет также рассмотрен сканер **CanoScan LIDE 25**. При подключении другого сканера название и значения параметров idVendor и idProduct будут другими, также может отличаться номер USB-порта.

Строка с похожим сканером в файле **40-libsane.rules**:

```
# Canon CanoScan LiDE 60
ATTRS{idVendor}=="04a9", ATTRS{idProduct}=="221c", ENV{libsane_matched}="yes"
```

Данные от утилиты **lsusb**:

```
Bus 003 Device 005: ID 04a9:2220 Canon, Inc. CanoScan LIDE 25
```

В файле **40-libsane.rules** в копии строки, в заголовке меняется номер модели сканера с *60* на **25**, а двойной **ID 04a9:2220**, полученный от lsusb нужно разделить на idVendor — **04a9** и idProduct — **2220**. В результате, основная и новая строки будут выглядеть так:

```
# Canon CanoScan LiDE 60
ATTRS{idVendor}=="04a9", ATTRS{idProduct}=="221c", ENV{libsane_matched}="yes"
# Canon CanoScan LiDE 25
ATTRS{idVendor}=="04a9", ATTRS{idProduct}=="2220", ENV{libsane_matched}="yes"
```

Сохраните файл и закройте его.

Теперь снова выполните в терминале команду:

```
scanimage -L
```

Ответ должен быть положительным:

```
device `plustek:libusb:003:008' is a Canon CanoScan LiDE25 flatbed scanner
```

Если сканер по-прежнему не найден, рассмотрим, как SANE работает со сканером.

У SANE есть конфигурационный файл, который обеспечивает доступ к драйверам. Находится он в каталоге **/etc/sane.d/dll.conf**. Выглядит он как список из других конфигурационных файлов, которые находятся в той же папке, что и **dll.conf**. Когда мы запускаем команду scanimage -L, а она, в свою очередь, обращается к конфигурационному файлу **dll.conf**, который обращается к конфигурационным файлам, отвечающим непосредственно за определенные модели сканера. Сами конфигурационные файлы ведут драйверам, которые находятся в **/usr/lib64/sane/**.

Решением проблемы может быть следующее:

В конфигурационном файле **/etc/sane.d/dll.conf** должен быть указан файл конфигурации (причем он не должен быть закомментирован символом «#»), в котором должен быть указан Vendor ID и Product ID.

Например:

Bus 003 Device 005: ID **04a9:2220** Canon, Inc. CanoScan LIDE 25

Bus 003 Device 005: ID **«Vendor ID»:«Product ID»** Canon, Inc. CanoScan LIDE 25

Запись в конфигурационном файле с указанием поддерживаемых сканеров должна выглядеть следующем образом:

#Samsung X7600 Series

usb 0x04e8 0x3326

Решение проблемы, если сканер виден под root, но не виден под пользователем:

lsusb

```
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 002: ID 03f0:622a Hewlett-Packard
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

Здесь строка Bus 003 Device 002: ID 03f0:622a Hewlett-Packard — это наше МФУ. Заходим в **/dev/bus/usb/**, проверяем через ls -al и находим **003** (по аналогии из вывода lsusb - это **Bus 003**), заходим в **003** и для устройства **002** (Device 002) устанавливаем права **666**.

```
cd /dev/bus/usb/003
```

```
chmod 666 002
```

Тогда сканер будет виден под пользователем.

Сканирование документа по сети

В данной статье рассмотрен вариант когда для сканирования по сети используется сервер сканирования, т.е к данному серверу подключен сканер, а клиенты по локальной сети подключаются к сканер-серверу и запускают сканирование.

Настройка сервера для сканирования по сети

1) установить все пакеты sane:

```
dnf install sane-backends-daemon sane-frontends
```

2) Установить xinetd:

```
dnf install xinetd
```

3) вписать подсеть которая может сканировать, в нашем случае - 192.168.100.0/24:

```
nano /etc/sane.d/saned.conf
```

```
#scan-client.somedomain.firm
#192.168.0.1
192.168.100.0/24
#[2001:db8:185e::42:12]
#[2001:db8:185e::42:12]/64
```

4) Проверить запись sane-port, должен быть:

```
nano /etc/services
```

```
sane-port 6566/tcp
sane-port 6566/udp
```

```
xdsxdm          6558/udp                #
sane-port       6566/tcp                # SANE Control Port
sane-port       6566/udp                # SANE Control Port
```

5) сделать запись в xinetd.conf:

```
nano /etc/xinetd.conf
```

```
service sane-port
{
socket_type = stream
server = /usr/sbin/saned
protocol = tcp
user = [здесь указываем пользователя с правами на сканирование]
wait = no
disable = no
}
```

```
service sane-port
{
socket_type = stream
server = /usr/sbin/saned
protocol = tcp
user = username
wait = no
disable = no
}
includedir /etc/xinetd.d
```

5) Перезапуск сервиса xinetd:

```
systemctl restart xinetd
```

Проверить статус - не должно быть ошибок:

```
systemctl status xinetd
```

```
[root@4600-l013402284 ~]# systemctl restart xinetd
[root@4600-l013402284 ~]# systemctl status xinetd
● xinetd.service - Xinetd A Powerful Replacement For Inetd
   Loaded: loaded (/usr/lib/systemd/system/xinetd.service; enabled; vendor preset: enabled)
   Active: active (running) since Вс 2020-06-21 22:54:31 MSK; 2s ago
  Process: 32141 ExecStart=/usr/sbin/xinetd -stayalive -pidfile /var/run/xinetd.pid $EXTRAOPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 32142 (xinetd)
   CGroup: /system.slice/xinetd.service
           └─32142 /usr/sbin/xinetd -stayalive -pidfile /var/run/xinetd.pid

июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing daytime
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing discard
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing discard
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing echo
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing echo
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing tcpmux
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing time
июн 21 22:54:31 4600-l013402284 xinetd[32142]: removing time
июн 21 22:54:31 4600-l013402284 xinetd[32142]: xinetd Version 2.3.15 started with libwrap loadavg labeled-networking options compiled in.
июн 21 22:54:31 4600-l013402284 xinetd[32142]: Started working: 1 available service
[root@4600-l013402284 ~]#
```

Настройка клиента для сканирования по сети

1) установить sane, xsane:

```
dnf install sane-backends-daemon sane-frontends xsane
```

2) прописать IP-адрес сервера

```
nano /etc/sane.d/net.conf
```

```
## saned hosts
# Each line names a host to attach to.
# If you list "localhost" then your backends can be accessed either
# directly or through the net backend.  Going through the net backend
# may be necessary to access devices that need special privileges.
# localhost
192.168.100.18
```

3) запустить xsane и выбрать сервер сканирования (возможно понадобится перезапуск рабочей станции)

Если в сети много сканирующих устройств, то при запуске xsane они все отобразятся в программе, чтобы запустить программу xsane с конкретно назначенным сетевым сканером, то можно воспользоваться командой:

```
xsane kyocera_wc3:192.168.2.190
```

пример приведен для сканеров марки kyocera.

Но если необходимо, чтобы сканируемая программа не опрашивала сеть на предмет поиска сетевых сканеров и не выдавала их список, то закомментируйте не нужные модели устройств в каталоге /etc/sane.d/dll.conf

Смена менеджера входа в систему (lightdm и sddm)

Менеджер входа в систему lightdm
Установка и активация
Автоматический вход пользователя
Менеджер входа в систему sddm
Установка и активация
Темы оформления sddm

Менеджер входа в систему — графическая оболочка, при помощи которой пользователь осуществляет вход в систему.

В РЕД ОС 7.3 по умолчанию установлен **gdm**.

Вы можете подробнее ознакомиться с возможностью смены менеджера входа в систему, просмотрев наши обучающие видео:

- на **RuTube** — Смена менеджера входа в систему (lightdm и sddm) ;
- в **Яндекс.Дзен** — Смена менеджера входа в систему (lightdm и sddm) ;
- в **VK Видео** — Смена менеджера входа в систему (lightdm и sddm) .

На наших каналах вы также сможете найти много другой полезной информации.

Менеджер входа в систему lightdm

Установка и активация

Для смены менеджера необходимо установить пакеты **lightdm** и **system-config-language**.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

И выполните команду:

```
dnf install lightdm system-config-language
```

Отключите менеджер входа в систему по умолчанию:

```
systemctl disable gdm
```

Затем включите новый менеджер:

```
systemctl enable lightdm
```

Перезагрузите систему:

```
reboot
```

При запуске менеджер входа изменится и будет выглядеть следующим образом:



Автоматический вход пользователя

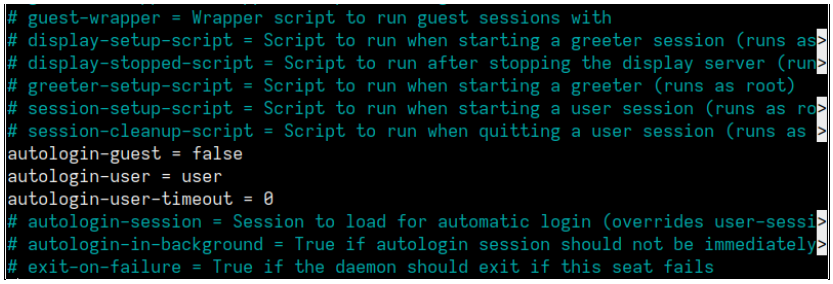
Для включения автоматического входа в **LightDM** в терминале откройте конфигурационный файл:

```
nano /etc/lightdm/lightdm.conf
```

и раскомментируйте строки:

```
#autologin-guest=false
 #autologin-user=user
 #autologin-user-timeout=0
```

Должно выглядеть следующим образом:



где

- **autologin-guest** — указывает, что вход будет по умолчанию происходить под гостем;
- **autologin-user** — указывает, под каким пользователем будет осуществляться вход;
- **autologin-user-timeout** — количество секунд ожидания загрузки пользователя по умолчанию.

Менеджер входа в систему sddm

Примечание.

Обратите внимание, что стандартная тема дисплейного менеджера работает **только** с **локальными** пользователями. Для работы с доменными пользователями см. «Темы оформления sddm».

Установка и активация

Для смены менеджера необходимо установить пакеты **sddm** и **sddm-themes**. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install sddm sddm-themes
```

Отключите менеджер входа в систему по умолчанию:

```
systemctl disable gdm
```

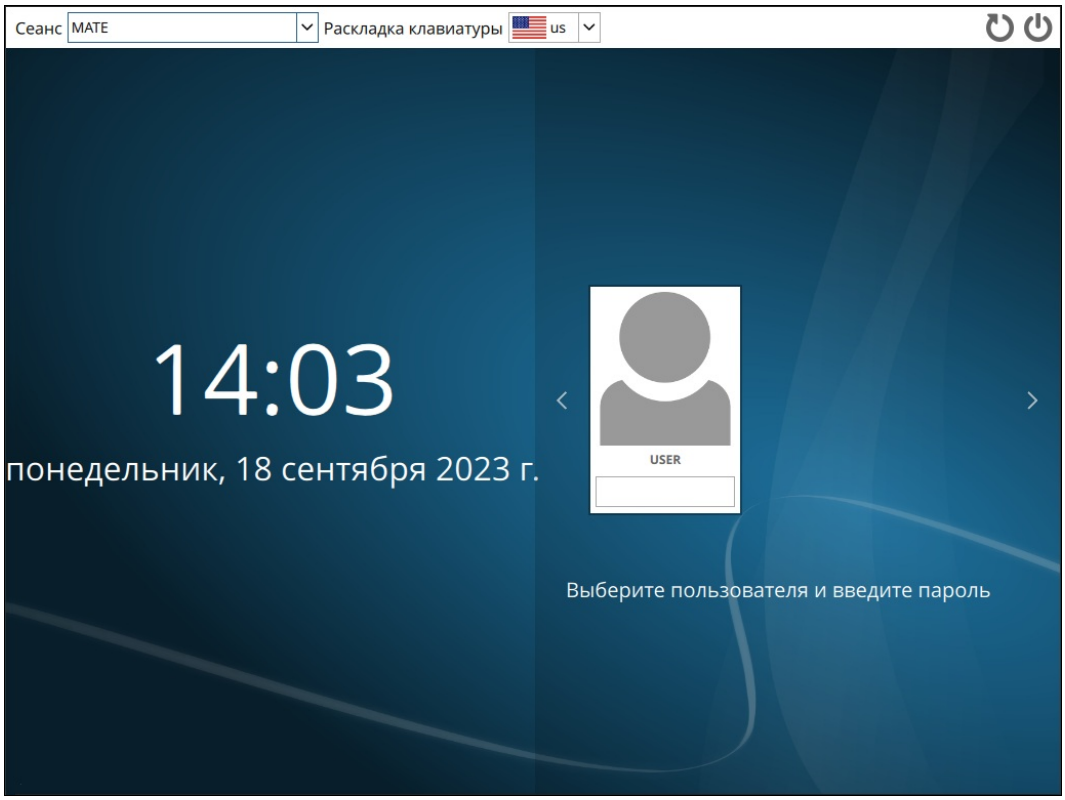
Затем включите новый менеджер:

```
systemctl enable sddm
```

Перезагрузите систему:

```
reboot
```

При запуске менеджер входа изменится и будет выглядеть следующим образом:



Примечание.

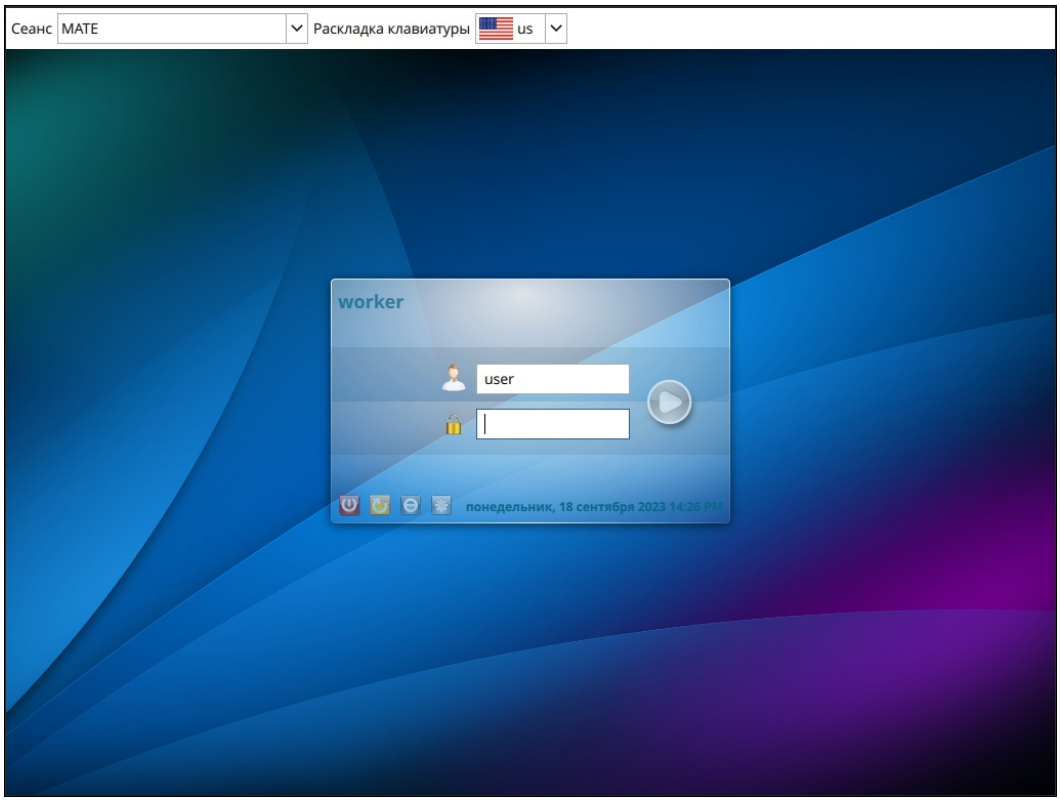
При использовании гибридной графики **nVidia** в связке с менеджером входа в систему **SDDM** переключение между видеокартами необходимо производить согласно нашей инструкции «Переключение используемых видеокарт nVidia и Intel при использовании менеджера SDDM».

Темы оформления sddm

Стандартная тема **sddm** имеет один недостаток – невозможность входа под доменной учетной записью. Для решения данной проблемы можно изменить тему оформления **sddm**.

В установленном из репозитория пакете **sddm-themes** существует 3 темы: «*elarun*», «*maldives*» и «*maya*».

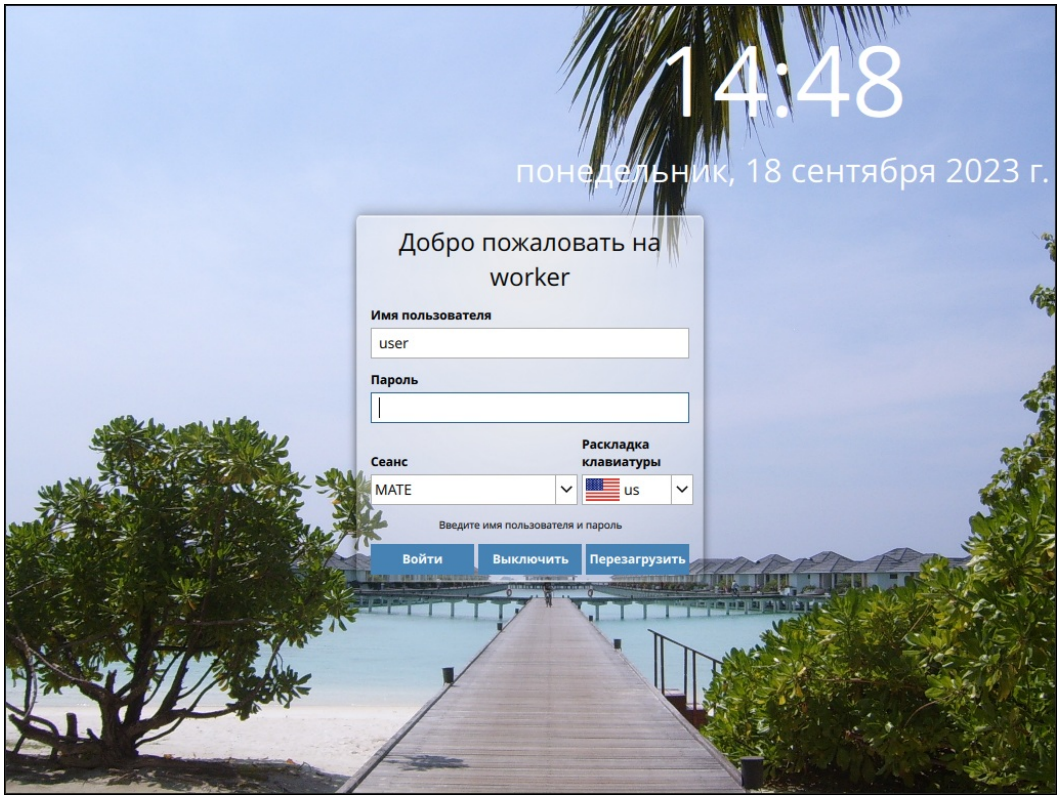
Тема **elarun** выглядит следующим образом:



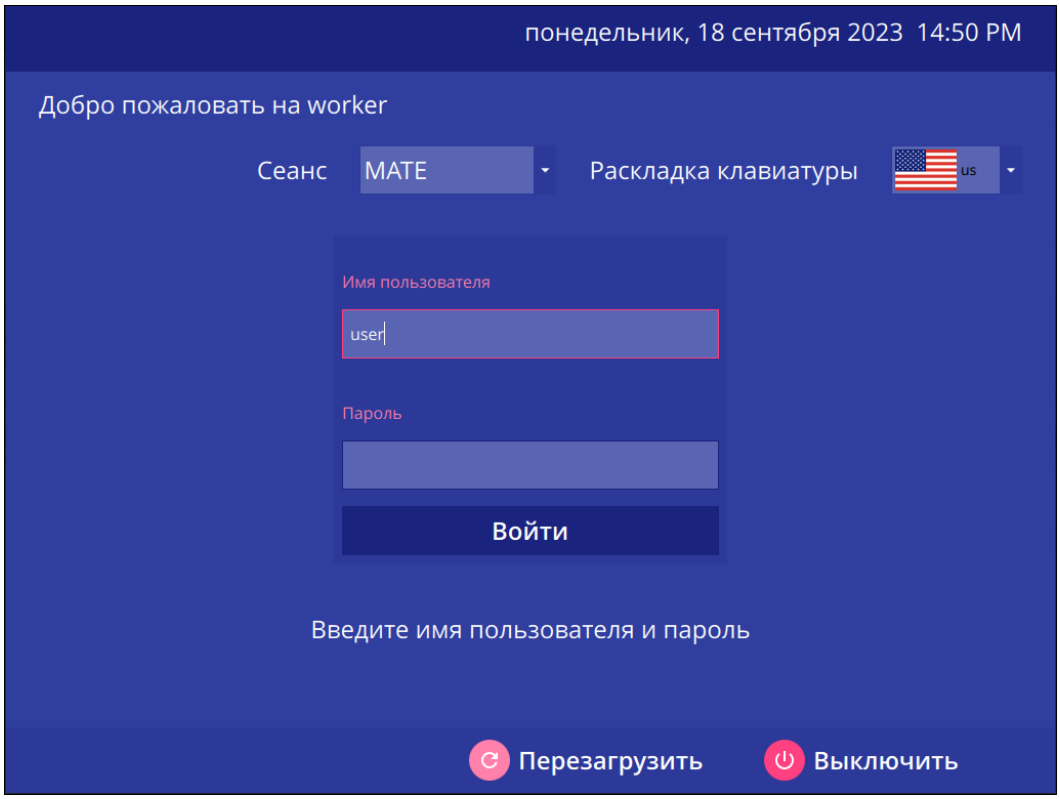
Обратите внимание! При входе в систему **под учетной записью доменного пользователя** с использованием темы **maldives**, в сеансе работы ограничиваются следующие возможности:

- доступ к звуковым устройствам;
- подключение USB-устройств, таких как флешки и веб-камеры.

Тема **maldives** выглядит следующим образом:



Тема **maya** выглядит следующим образом:



Для изменения темы необходимо в файле **/etc/sddm.conf** в графе [**Theme**] раскомментировать строку «**Current=**» и добавить предпочитаемую тему оформления вместо базовой.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и откройте файл в редакторе **nano**:

```
nano /etc/sddm.conf
```

```
[Theme]
# Current theme name
Current=elarun

# Cursor theme used in the greeter
#CursorTheme=

# Number of users to use as threshold
# above which avatars are disabled
# unless explicitly enabled with EnableAvatars
#DisableAvatarsThreshold=7

# Enable display of custom user avatars
#EnableAvatars=true
```

Также можно устанавливать и сторонние темы оформления для **sddm**.

Для корректной установки необходимо добавить скачанную тему в **/usr/share/sddm/themes/**, а после этого в файле **/etc/sddm.conf** изменить строку «**Current=**» на нужную.

Отключение информационного сообщения при входе в сеанс пользователя

ВАЖНО!

Отключение информационного сообщения при входе в сеанс пользователя нарушает условия сертификации ФСТЭК. Отключение данного информационного сообщения допускается **только в стандартной редакции ОС**.

Узнать редакцию установленной РЕД ОС можно командой `lsb_release -a | grep Edition:`

lsb_release -a | grep Edition:

```
Edition:    Standard
```

Для того, чтобы отключить информационное сообщение при входе в сеанс пользователя, нужно закомментировать последнюю строку (`/usr/bin/zenity --warning --text "$TEXTMSG" --no-wrap`) в файле **/etc/gdm/PreSession/Default**.

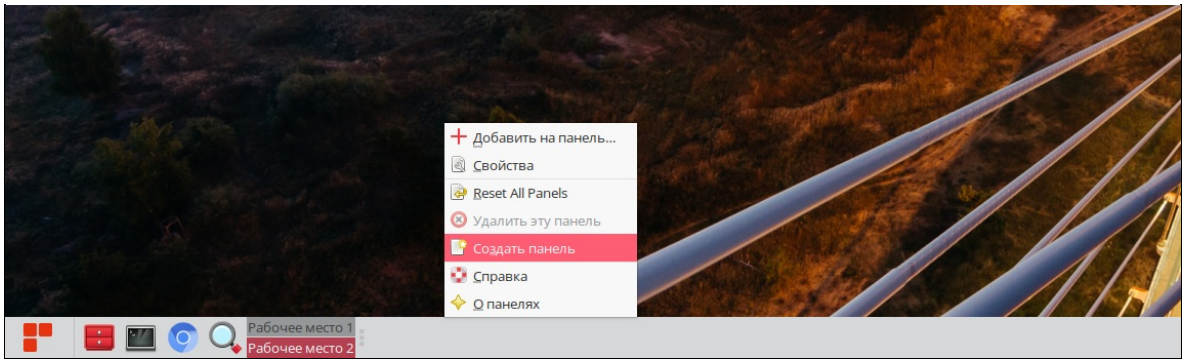
```
nano /etc/gdm/PreSession/Default
```

```
...
#/usr/bin/zenity --warning --text "$TEXTMSG" --no-wrap
```

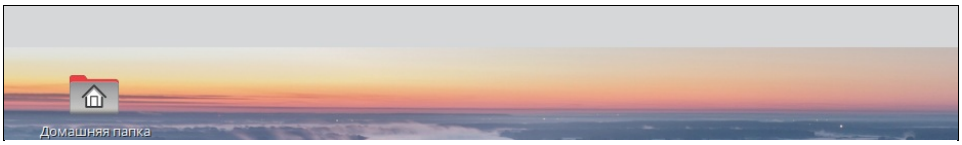
Добавление системной панели на второй монитор

Для удобства работы на втором мониторе зачастую требуется доступ к системной панели.

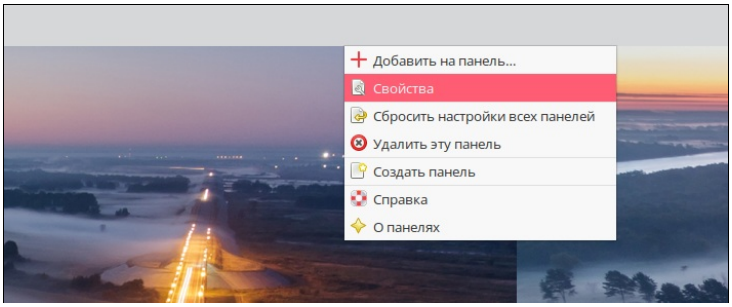
Для того чтобы добавить панель на второй монитор, необходимо нажать правой кнопкой мыши по панели на основном мониторе и выбрать в появившемся меню пункт «Создать панель».



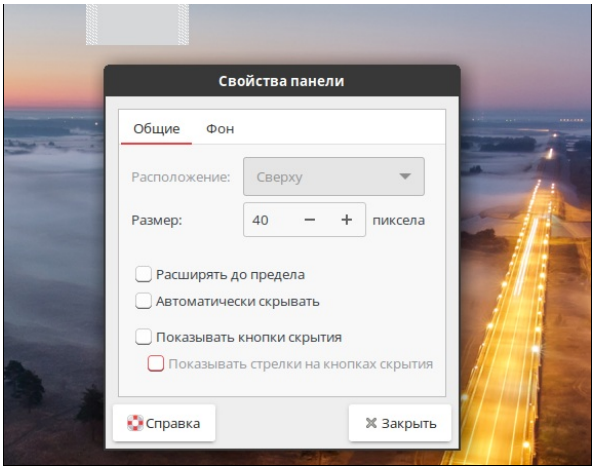
Будет предложено выбрать место для расположения новой панели - слева, справа или вверху. В данном случае выберем расположение в верхней части монитора. После выбора появится пустая панель.



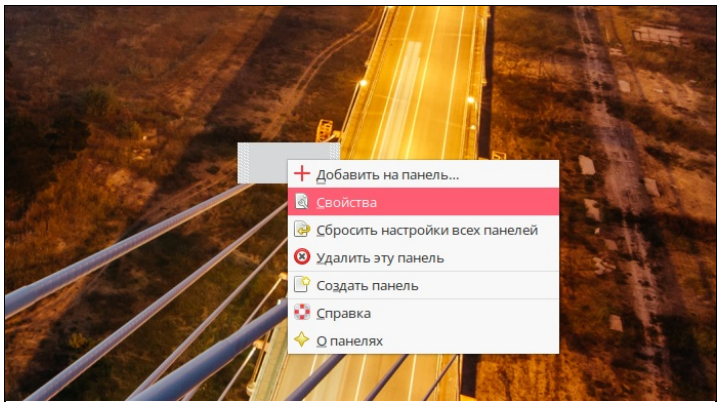
Нажимаем правой кнопкой мыши по новой панели и выбираем «Свойства».



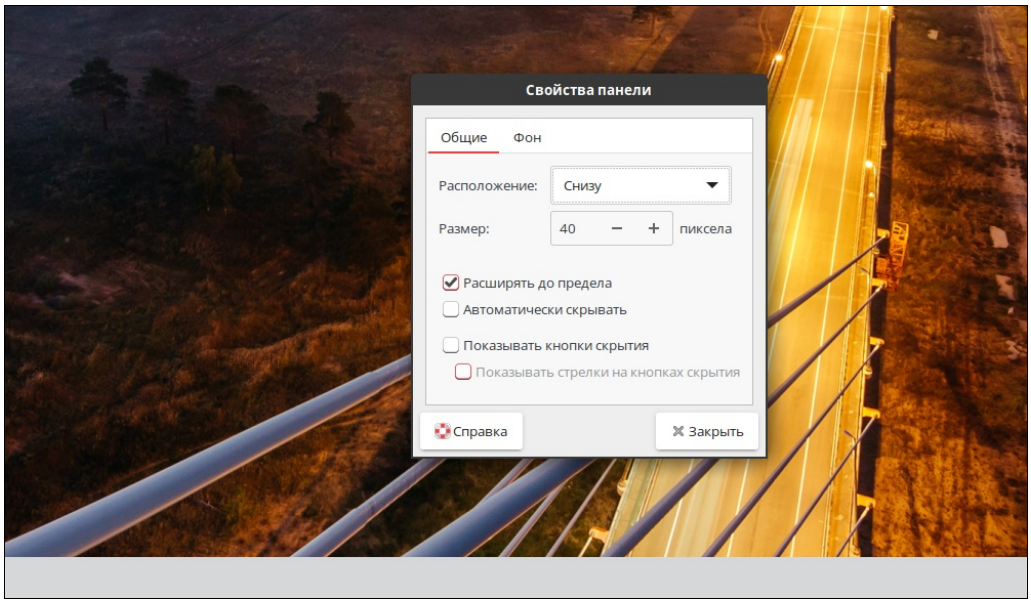
Снимаем галочку «Расширять до предела», панель изменит свои размеры.



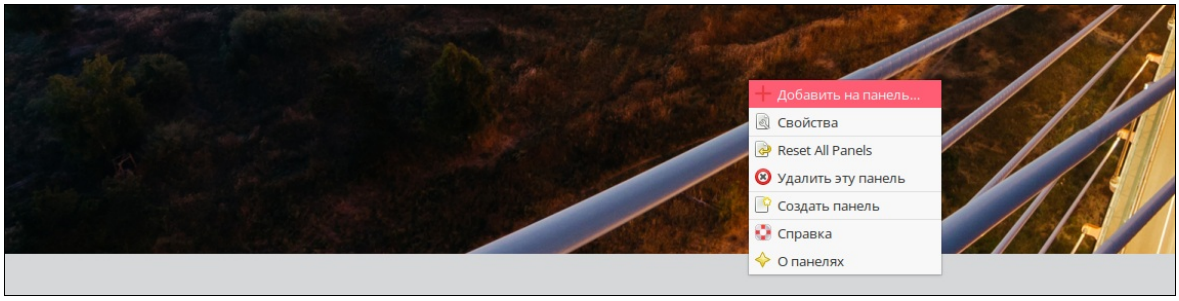
Далее при помощи мыши перетаскиваем панель на второй монитор, нажимаем на нее правой кнопкой и выбираем «Свойства».



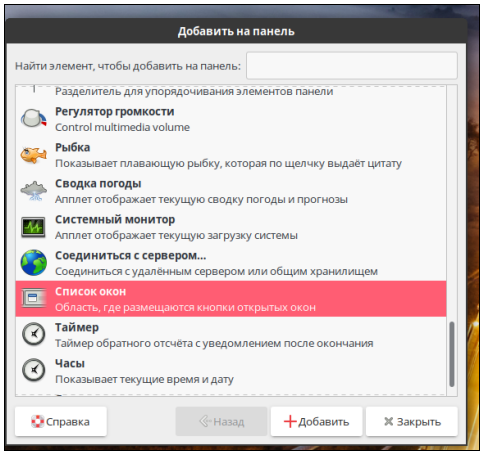
Устанавливаем галочку «Расширить до предела», выбираем расположение нашей панели.



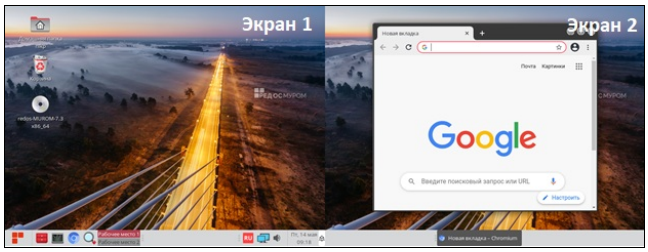
Чтобы добавить «Список окон» на новой панели, необходимо нажать на нее правой кнопкой мыши и выбрать «Добавить на панель».



Из представленного списка выбираем «Список окон» и нажимаем «Добавить».



В результате на втором мониторе открытые окна приложений будут отображаться на системной панели.


Экран 1
Экран 2
Google
Введите поисковый запрос или URL
Настроить

Управление с помощью dconf

Возможности dconf
Управление ключами dconf
GSettings
Установка настроек рабочего стола по умолчанию
Блокировка настроек рабочего стола
Настройка общих для всех пользователей горячих клавиш
Dconf-editor

Возможности dconf

Dconf – низкоуровневая система конфигурации. При помощи **dconf** в **GNOME** и **Unity** хранятся настройки большинства программ.

Dconf это простая система конфигурации основанная на ключах. Ключи находятся в неструктурированной базе данных (ключи, логически связанные между собой объединены в категории). База данных хранится в бинарном файле, который располагается в **~/.config/dconf**.

Управление ключами dconf

В большинстве случаев пользователю не нужно вручную редактировать настройки хранящиеся в **dconf**. Но иногда графическое представление тому или иному параметру отсутствует и единственным способом изменить его значение является редактирование ключа напрямую. Это можно осуществить несколькими способами.

GSettings

GSettings - это консольная утилита, при помощи которой можно управлять ключами **dconf**.

Синтаксис использования **GSettings**:

```
gsettings [--schemadir <КАТАЛОГ_СХЕМ>] <КОМАНДА> [<АРГУМЕНТЫ...>]
```

Команды:

Команда	**Описание**
help	Показать справку
list-schemas	Список установленных схем
list-relocatable-schemas	Список перемещаемых схем
list-keys	Список ключей схемы
list-children	Список потомков схемы
list-recursively	Список ключей и значений, рекурсивно
range	Запросить диапазон значений ключа
get	Получить значение ключа
set	Изменить значение ключа
reset	Сбросить значение ключа
reset-recursively	Сбросить все значения в заданной схеме
writable	Проверить ключ на запись
monitor	Следить за изменениями

Для того чтобы получить более подробную справку по интересующей команде, выполните:

```
gsettings help <КОМАНДА>
```

Поиск соответствий схемы настройкам рабочего стола.

Здесь необходимо выяснить пути и названия элементов схемы, отвечающих за конкретные настройки рабочего стола. Например, что именно определяет фон или цвет рабочего стола.

Для начала открываем консоль и набираем от имени обычного пользователя:

```
gsettings list-schemas | grep background

org.mate.background
org.mate.SettingsDaemon.plugins.background
org.gnome.desktop.background
```

Тем самым мы получим список схем, в которых может содержаться интересующая нас информация. Теперь выясняем, что именно из перечисленного отвечает за интересующие нас настройки рабочего стола:

```
gsettings monitor org.mate.background
```

Откройте параметры рабочего стола и попробуйте изменить фон, цвет, или иной пункт. В терминале появится информация вида схема/ключ/значение.

```
gsettings list-recursively org.mate.background

org.mate.background picture-opacity 100
org.mate.background secondary-color '#3C8F25'
org.mate.background show-desktop-icons true
org.mate.background background-fade true
org.mate.background primary-color '#5891BC'
org.mate.background picture-filename '/usr/share/design/current/backgrounds/default.png'
org.mate.background color-shading-type 'vertical-gradient'
org.mate.background picture-options 'zoom'
org.mate.background draw-background true
```

Установка настроек рабочего стола по умолчанию

Здесь административно установить настройки рабочего стола, которые будут применяться у всех вновь создаваемых пользователей. Например, так можно определить конкретный фон или цвет рабочего стола. Эти изменения не затронут ранее созданных пользователей, которые уже используют графическую среду. Кроме того, пользователи смогут изменить установленные администратором настройки, если захотят. Чтобы заблокировать им такую возможность, читайте следующий раздел.

Все действия выполняются с правами пользователя **root**:

```
su -
```

Создаём файл:

```
nano /etc/dconf/profile/user
```

```
user-db:user
system-db:local
```

Создаём директорию:

```
mkdir -p /etc/dconf/db/local.d
```

Создаём файл:

```
nano /etc/dconf/db/local.d/00_background
```

Сохраняем в него только те ключи и значения, полученные на шаге 1, которые нас интересуют. В квадратных скобках указываем название схемы.

```
[org/mate/desktop/background]
secondary-color='#858 5d4d45b5b'
background-fade=true
primary-color='#babadada5555'
picture-filename='/usr/share/backgrounds/mate/desktop/MATE-Stripes-Dark.png'
color-shading-type='vertical-gradient'
picture-options='zoom'
draw-background=true
```

Блокировка настроек рабочего стола

Пока были определены значения, которые в дальнейшем будут использоваться по умолчанию. Пользователь всё ещё имеет возможность их поменять. Чтобы пользователь не мог внести изменения в настройки рабочего стола никакими средствами, создадим ещё один файл:

```
nano /etc/dconf/db/local.d/locks/00_background
```

```
/org/mate/desktop/background/secondary-color
/org/mate/desktop/background/background-fade
/org/mate/desktop/background/primary-color
/org/mate/desktop/background/picture-filename
/org/mate/desktop/background/color-shading-type
/org/mate/desktop/background/picture-options
/org/mate/desktop/background/draw-background
```

и выполним команду:

```
dconf update
```

Здесь стоит обратить внимание, что схема указана другая - не **/org/mate/background**, а **/org/mate/desktop/background**. В случае с **MATE** это связано с особенностью обработки схем **dconf** и **gsettings**. Посмотреть текущие схемы можно в директории **/usr/share/glib-2.0/schemas**.

Новые настройки вступают в силу немедленно.

Пример настройки dconf - настройка общих для всех пользователей горячих клавиш

Для понимания, какие параметры **dconf** требуется изменить, выполните в терминале команду для «прослушивания» изменений в системе:

```
dconf watch /
```

Параллельно с запущенным **dconf** зайдите в графическую утилиту «**Сочетание клавиш клавиатуры**» («**Главное меню**» — «**Параметры**») и настройте нужные вам сочетания клавиш.

В терминале вы увидите применяемые изменения, например:

```
dconf watch /
/org/mate/marco/global-keybindings/run-command-window-screenshot
 '<Alt>F3'
```

Далее создайте файл (если уже существует, то оставьте без изменений):

```
nano /etc/dconf/profile/user
```

с содержимым:

```
user-db:user
system-db:local
```

Создайте файл, который будет отвечать за настройки по умолчанию:

```
nano /etc/dconf/db/local.d/00_session
```

```
[org/mate/marco/global-keybindings]
run-command-window-screenshot='<Alt>F3'
```

И в конце обновите **dconf** командой:

```
dconf update
```

После этого для новых пользователей будут вступать в силу параметры нового **dconf** по умолчанию.

Dconf-editor

Dconf-editor – является наиболее часто используемым графическим приложением для редактирования ключей **dconf**. В приложении все ключи представлены в виде дерева, можно искать ключи по их названию, жирным текстом выделяются ключи, значение которых было изменено.

По умолчанию **dconf-editor** не установлен на РЕД ОС. Чтобы установить его нужно использовать специальную команду в консоли:

```
sudo dnf install dconf-editor
```

Для запуска используется консольная команда:

```
dconf-editor
```

С помощью **dconf-editor** можно получить быстрый доступ к множеству "скрытых" настроек, как системных, так и внешнего вида, позволяя быстро сделать в системе комфортное и удобное для себя рабочее окружение.

Настройка режимов работы мониторов с помощью XRandR

Добавление нового разрешения экрана
Работа с несколькими мониторами
Настройка положения монитора
Настройка виртуального разрешения
Поворот изображения
Отключение монитора

Добавление нового разрешения экрана

Бывают ситуации, когда после установки ОС при подключении монитора нет нужного разрешения для используемого монитора. Для решения подобных проблем можно воспользоваться программой XRandR.

XRandR – это официальная программа настройки оконной системы. С ее помощью можно изменить параметры вывода изображения на экране, такие как размер, ориентация или отражение выходных данных. Также можно установить размер самого экрана. Для того, чтобы задать требуемый размер экрана в РЕД ОС, необходимо выполнить несколько шагов:

1. Создать файл конфигурации:

```
nano /etc/X11/xorg.conf
```

Откроется пустой файл, в который необходимо скопировать следующую настройку:

```
Section "Device"
Identifier    "Configured Video Device"
EndSection

Section "Monitor"
Identifier    "Configured Monitor"
EndSection

Section "Screen"
Identifier    "Default Screen"
Monitor    "Configured Monitor"
Device    "Configured Video Device"
EndSection
```

2. Сохранить документ, нажав сочетание клавиш *«CTRL+O»*, и выполнить команду:

```
gtf 1920 1080 60 >> /etc/X11/xorg.conf
```

После выполнения команды в ранее сохраненный файл конфигурации будут добавлены новые строки:

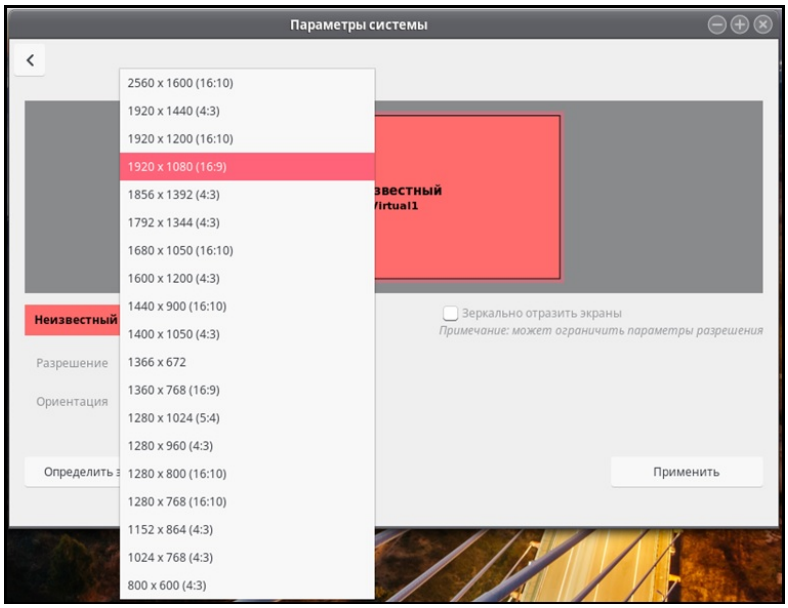
```
# 1920x1080 @ 60.00 Hz (GTF) hsync: 67.08 kHz; pclk:172.80 MHz
Modeline "1920x1080_60.00"  172.80  1920 2040 2248 2576 1080 1081 1084 1118  -HSync +Vsync
```

Последнюю строку необходимо переместить в блок **Section «Monitor»**. Должен получиться примерно такой код:

```
Section "Monitor"
Identifier    "Configured Monitor"
Modeline "1920x1080_60.00"  172.80  1920 2040 2248 2576  1080 1081 1084 1118  -HSync
+Vsync
EndSection
```

3. Перезагрузить компьютер.

4. Перейти в *«Параметры системы»* - *«Экран»*. В графе *«Разрешение экрана»* должно появиться указанное разрешение 1920x1080.



Результат настройки конфигурации.

Работа с несколькими мониторами

Для отображения списка интерфейсов, по которым могут быть подключены мониторы, а также доступных режимов работы монитора (разрешение и частота обновления в герцах) выполните команду:

```
xrandr

Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
VGA-1 connected primary 1920x1080+0+0 (normal left inverted right x axis y axis) 527mm x 296mm
   1920x1080     60.00*+
   1680x1050     59.95
   1280x1024     75.02    60.02
   1440x900      59.89
   1280x960      60.00
   1280x720      60.00
   1024x768      75.03    70.07    60.00
   832x624       74.55
   800x600       72.19    75.00    60.32    56.25
   640x480       75.00    72.81    66.67    59.94
   720x400       70.08
DP-1 disconnected (normal left inverted right x axis y axis)
HDMI-1 disconnected (normal left inverted right x axis y axis)
```

Вывод команды сообщает, что в данный момент монитор подключен к видеокарте по порту **VGA-1**, порты **DP-1** и **HDMI-1** отключены.

В случае, если РЕД ОС используется на ноутбуке, моноблоке или другом устройстве, имеющем встроенный дисплей, интерфейс может иметь название **LVDS** или **DSI**.

При подключении второго монитора система определит первый подключенный монитор как основной. Для изменения основного монитора необходимо выполнить команду вида:

```
xrandr --output <интерфейс> --primary
```

Например:

```
xrandr --output HDMI-1 --primary
```

Данная команда установит монитор, подключенный по **HDMI-1**, в качестве основного.

Настройка положения монитора

Также можно настроить положение мониторов относительно друг друга. Например, мониторы подключены к портам **VGA-1** и **HDMI-1**. Необходимо монитор **HDMI-1** расположить справа относительно монитора **VGA-1**. Для этого следует выполнить команду:

```
xrandr --output "HDMI-1" --right-of "VGA-1"
```

Аналогично можно использовать параметр **--left-of**.

Настройка виртуального разрешения

В случае, если необходимо сделать виртуальный экран большего разрешения, чем физический, используется команда:

```
xrandr --output <интерфейс> --mode 1920x1080 --fb 2560x1440 --panning 2560x1440
```

После использования данной команды размер виртуального разрешения будет установлен 2560x1440 пискелей при размере 1920x1080 пислелей физического.

ВАЖНО!

Данный режим **НЕ** работает как DSR от Nvidia или Виртуальное сверхвысокое разрешение от AMD, и изображение не будет подстраиваться под реальное разрешение экрана, объекты вне границ экрана отображаться не будут.

Поворот изображения

Для поворота изображения на экране для нужного интерфейса используется параметр **--rotate**, где значения **left** и **right** поворачивают изображение в указанную сторону. Также можно использовать параметр **inverted** для поворота экрана на 180°.

Отключение монитора

Отключить ненужный в данный момент дисплей можно с помощью опции **--off**, например:

```
xrandr --output HDMI-1 --off
```

Дисплей, подключенный через порт **HDMI-1**, будет отключен.

RedShift - утилита изменения цветового профиля экрана

Основные настройки программы
Сохранение настроек
Автозагрузка

RedShift — свободное программное обеспечение, которое изменяет цветовой профиль экрана в зависимости от времени суток и местоположения, снижая утомляемость глаз при продолжительной работе у монитора.

Для того чтобы начать работать с программой, необходимо установить пакет из репозитория командой:

```
dnf install redshift redshift-gtk
```

Вы можете подробнее ознакомиться с работой утилиты **RedShift**, просмотрев наши обучающие видео:

- на **RuTube** — RedShift - утилита изменения цветового профиля экрана;
- в **Яндекс.Дзен** — RedShift - утилита изменения цветового профиля экрана;
- в **VK Видео** — RedShift - утилита изменения цветового профиля экрана.

На наших каналах вы также сможете найти много другой полезной информации.

Основные настройки программы

1. Настройки температуры

RedShift равномерно переводит цветовую температуру дисплея компьютера между дневной и ночной температурами, чтобы глаза пользователя могли медленно адаптироваться.

Ночью цветовая температура низкая и обычно составляет **3000–4000 K**, что предпочтительно соответствует температуре освещения в комнате.

Типичная цветовая температура в дневное время составляет **5500–6500 K**. Чтобы задать температуру в формате *День:Ночь*, используется команда:

```
redshift -t 6500:3500
```

где 6500 - температура по умолчанию.

Установка значения **более 6500** приводит температуру к более холодному синему цвету, а установка значения **менее 6500** приводит температуру к более теплому красному цвету.

2. Настройки яркости

Регулировка уровня яркости подсветки монитора осуществляется изменением уровня освещенности экрана от светлого до тёмного. Низкая освещённость преимущественно используется в вечернее и ночное время. Высокая интенсивность свечения полезна для работы днём. Благодаря регулировке яркости монитора можно снять лишнее напряжение с глаз.

Чтобы задать яркость, используется команда:

```
redshift -b 0.5
```

Значение яркости можно установить в диапазоне **от 0.1 до 1.0**.

3. Настройка гаммы

Гамма показывает соотношение между уровнями трех основных цветов цветового пространства RGB и силу излучаемого монитором светового потока.

Чтобы задать значение гаммы, используется команда:

```
redshift -g 0.5
```

Значение гаммы можно установить в диапазоне **от 0.1 до 1.0**.

Сохранение настроек

Для того чтобы настройки работали постоянно, необходимо создать файл настроек в **/home/user**, где *user* - имя пользователя.

```
nano /home/user/.config/redshift.conf
```

Записываем в файл конфигурации параметры в следующем виде:

```
[redshift]
temp-day=6500
temp-night=3500

transition=1

brightness-day=0.8
brightness-night=0.6

gamma=0.8
```

где *temp-day* - температура цвета днем;
temp-night - температура цвета ночью;
transition - определяет плавный переход между температурой (при значении 0 сразу устанавливает значение температуры, при значении 1 осуществляется плавный переход);
brightness-day - яркость днем;
brightness-night - яркость ночью;
gamma - установка гаммы для всех цветов.

Сохраняем и закрываем файл.

Далее запускаем программу *RedShift* через терминал командой:

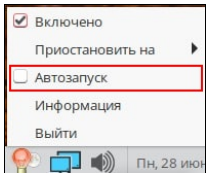
```
redshift-gtk
```

или через «*Главное меню — Стандартные — Redshift*».

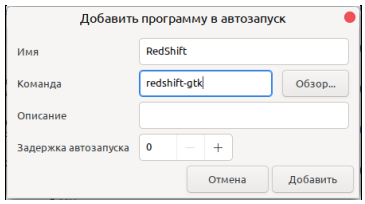
На панели задач должен появиться значок *RedShift*, при этом применятся все настройки, выставленные в файле конфигурации.

Автозагрузка

Для добавления *RedShift* в автозагрузку можно воспользоваться функцией «Автозапуск» в меню *RedShift*.



Также можно воспользоваться средствами операционной системы, для этого заходим в параметры системы и открываем раздел «Автозагрузка». Далее нажимаем кнопку «Добавить» - «Команда пользователя». В поле «Команда» вписываем **redshift-gtk** и нажимаем «Добавить».



После перезагрузки RedShift запустится автоматически.

Панель быстрого запуска Plank

Установка и запуск
Настройка plank
Описание настроек Plank
Добавление и удаление значков
Установка тем в Plank

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** plank 0.11.89-2.20210531.git6d9de7f

Plank - панель, которую можно использовать для запуска, переключения между запущенными приложениями, выводить различную информацию, такую как системные уведомления, пользовательские сообщения и т. п. Преимущество дока над обычной панелью заключается в гибкости настройки - с легкостью можно изменить размер, место расположения, эффекты, заставить ее появляться и исчезать в нужный момент.

Вы можете подробнее ознакомиться с настройкой панели Plank, просмотрев наши обучающие видео:

- на **RuTube** — Новые темы для РЕД ОС. Установка панели быстрого запуска Plank;
- в **Яндекс.Дзен** — Новые темы для РЕД ОС. Установка панели быстрого запуска Plank.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и запуск

Устанавливается панель командой:

```
dnf install plank plank-docklets
```

Для запуска выполните команду:

```
plank
```

Также можно запустить *plank* с помощью меню: *«Меню» - «Стандартные» - «Plank»*.

Добавление *plank* в автозапуск осуществляется командой:

```
ln -s /usr/share/applications/plank.desktop /etc/xdg/autostart/
```

Настройка plank

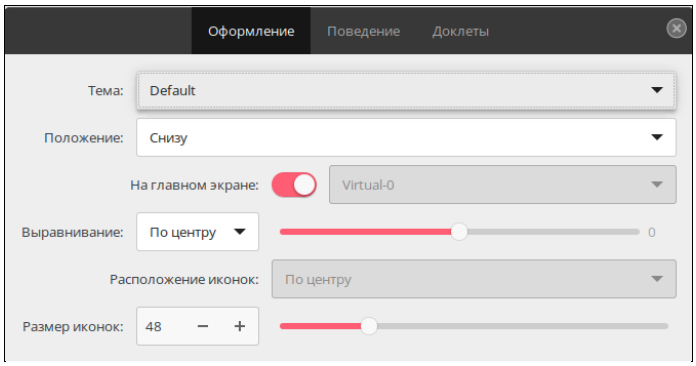
Чтобы вызвать панель настроек, необходимо ввести в консоли:

```
plank --preferences
```

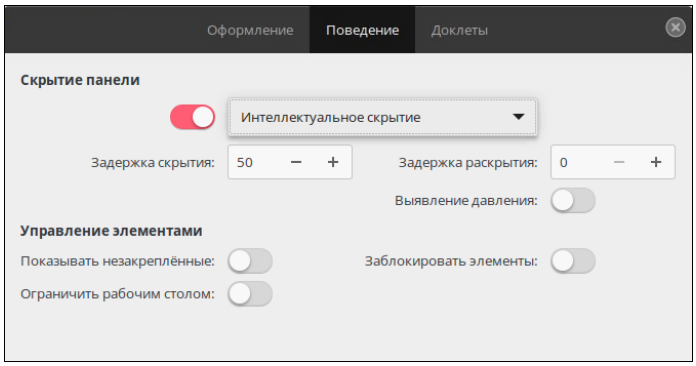
Также панель настроек можно запустить, нажав на панели *plank «CTRL + ПКМ» - «Параметры»*.

Описание настроек Plank

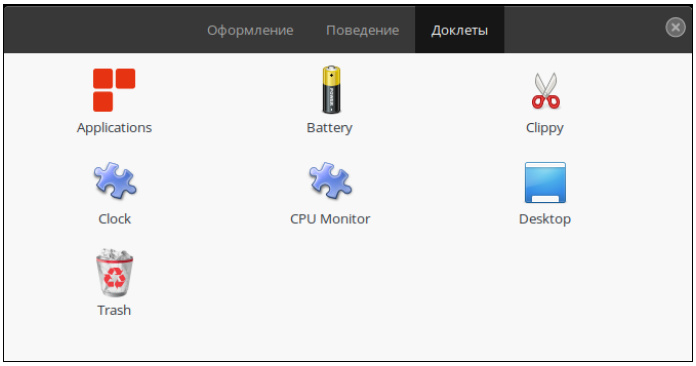
На вкладке «*Оформление*» можно изменить тему, положение *plank*, выбрать монитор для отображения панели, выбрать выравнивание, расположение и размер иконок.



На вкладке «*Поведение*» можно выбрать необходимый режим появления/скрытия *plank* либо отключить скрытие панели.

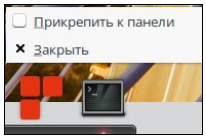


Доклеты на панель добавляются двойным кликом «ЛКМ».



Добавление и удаление значков

Для того чтобы добавить новый значок на панель, необходимо запустить программу, и ярлык автоматически отобразится в *Plank*. Затем необходимо щёлкнуть ПКМ по нужному значку и выбрать опцию «*Прикрепить к панели*».



Для удаления значка нужно убрать галочку с опции «*Прикрепить к панели*» либо левой кнопкой мыши вытянуть его из панели.

Установка тем в Plank

Для начала нужно убедиться, что каталог для сохранения тем существует, перейдя по следующему пути:

```
cd ~/.local/share/plank/themes
```

Если данного каталога не существует, нужно его создать:

```
mkdir -p ~/.local/share/plank/themes
```

Чтобы извлечь скачанные темы в формате **.zip**, выполните:

```
cd ~/Загрузки
unzip plank-themes.zip
```

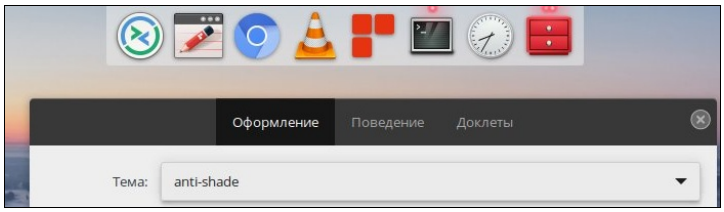
Для архивов тем формата **.tar**, выполните:

```
cd ~/Downloads
tar -zxvf plank-themes.tar.gz
```

Перемещение файлов темы (убедитесь, что вы перемещаете фактическую папку темы, а не папку, содержащую папку темы) осуществляется командой:

```
mv anti-shade ~/.local/share/plank/themes
```

После перемещения файлов во вкладке «*Тема*» появится соответствующая тема.



Shotwell - утилита для автоматической смены обоев рабочего стола (слайд-шоу)

Для установки слайд-шоу в качестве обоев рабочего стола используется приложение **Shotwell**.

Вы можете подробнее ознакомиться с настройкой приложения **Shotwell**, просмотрев наши обучающие видео:

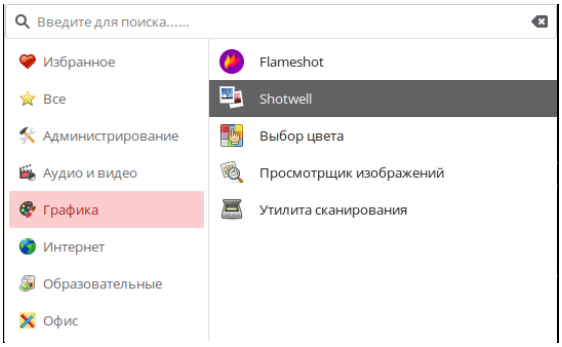
- на **RuTube** — Автоматическая смена обоев рабочего стола. Shotwell;
- в **Яндекс.Дзен** — Автоматическая смена обоев рабочего стола. Shotwell;
- в **VK Видео** — Автоматическая смена обоев рабочего стола. Shotwell.

На наших каналах вы также сможете найти много другой полезной информации.

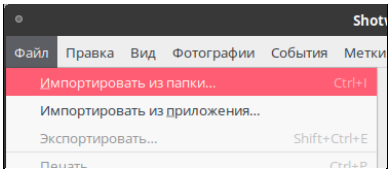
Установить его можно следующей командой:

```
dnf install shotwell
```

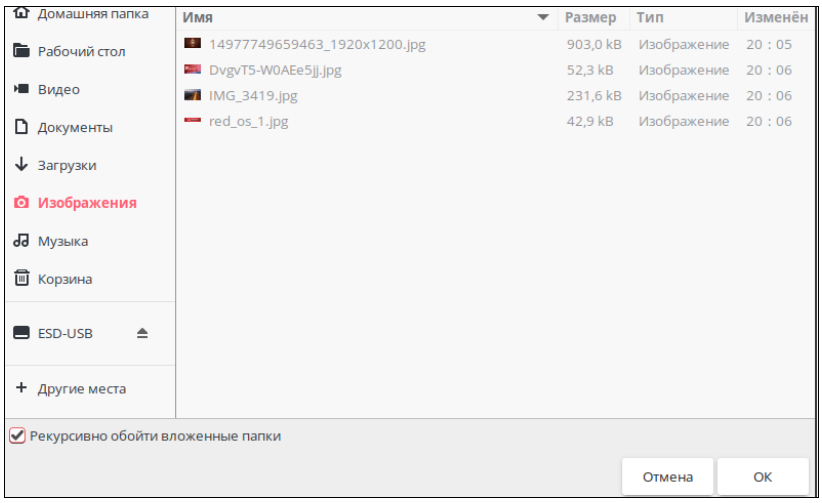
Программа будет доступна из «*Меню*»— «*Графика*» — «*Shotwell*».



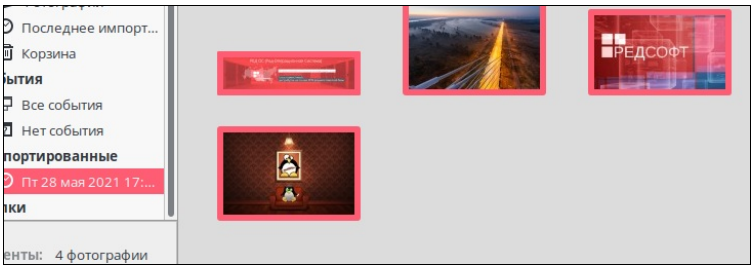
Для того чтобы создать слайд-шоу из собственных снимков/обоев на рабочем столе РЕД ОС, у вас в локальной папке уже должны быть сохранены какие-то снимки или обои из сети, которые отобразятся в Shotwell. Для того чтобы они отобразились, их нужно импортировать. Для этого необходимо выбрать *«Файл»→»Импортировать из папки...»*.



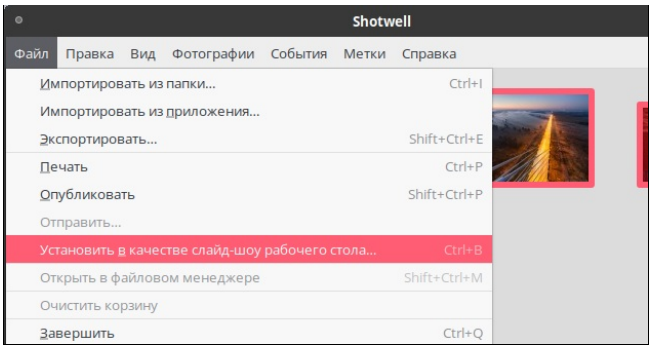
Выбираем каталог с изображениями и нажимаем **«OK»**.



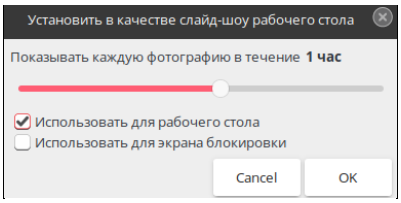
После того как изображения были импортированы в программу, можно приступать к созданию слайд-шоу. Для этого выбираем изображения, которые хотим видеть в слайд-шоу.



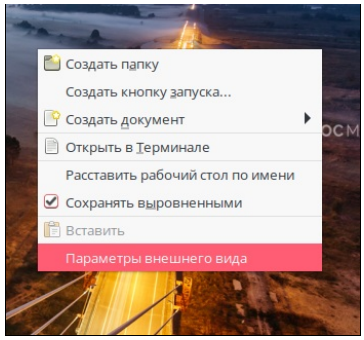
Затем нажимаем на *«Файл»→»Установить в качестве слайд-шоу рабочего стола»*.



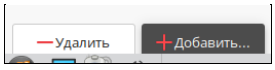
Откроется окно настройки времени и места использования данного слайд-шоу. Настраиваем под себя и нажимаем **«OK»**.



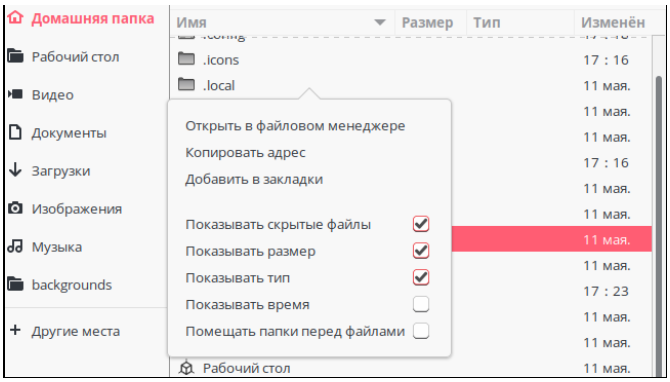
После этого нажимаем правой кнопкой мыши на рабочем столе и открываем параметры внешнего вида.



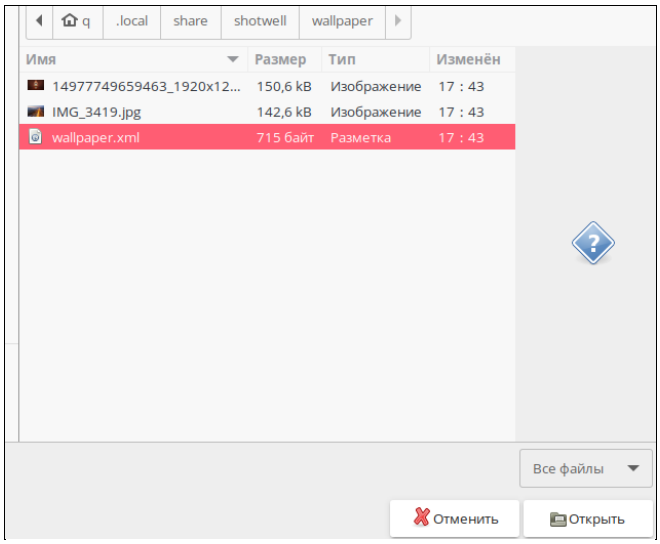
В открывшемся окне нажимаем **«Добавить»**.



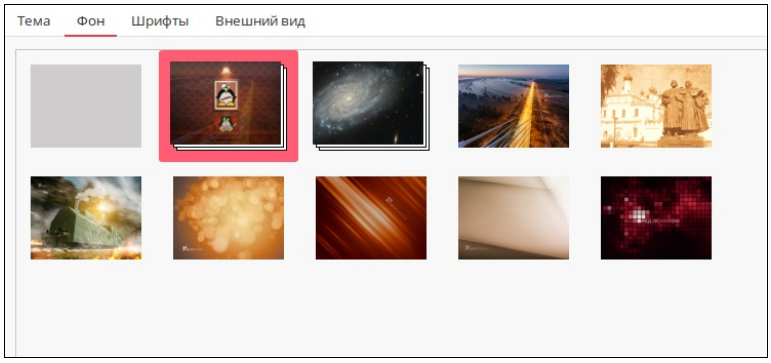
В каталоге **«Домашняя папка»** нажимаем ПКМ и включаем показ скрытых файлов.



Открываем каталог **.local/share/shotwell/wallpaper**, в нем будет находиться **wallpaper.xml** - это созданное слайд-шоу. Для того чтобы его увидеть, нужно включить отображение всех файлов и после этого выбрать **wallpaper.xml**.



Далее в окне появится созданное слайд-шоу для рабочего стола, выбираем его.



Готово! Автоматическая смена обоев настроена.

В дальнейшем будет достаточно просто изменить слайд-шоу в Shotwell.

Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев

Установка zenity
Синтаксис и опции
Примеры использования
Диалоговое окно для вывода предупреждения
Диалоговое окно с запросом
Диалоговое окно с календарем
Диалоговое окно с полем ввода
Добавление zenity в bash-сценарии
Пример 1 Диалоговое окно с сообщением
Пример 2 Диалоговое окно формы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zenity-3.32.0

Zenity — кроссплатформенная утилита, позволяющая создавать различные типы диалоговых окон GTK+ в командной строке и сценариях командной оболочки. Утилита упрощает взаимодействие между пользователем и командной оболочкой.

Вы можете подробнее ознакомиться с возможностями графического окружения **MATE**, просмотрев наши обучающие видео:

- на **RuTube** — Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- в **Яндекс.Дзен** — Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- в **VK Видео** — Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев .

На наших каналах вы также сможете найти много другой полезной информации.

Установка zenity

По умолчанию в РЕД ОС утилита **zenity** уже установлена (расположена в каталоге /usr/bin/zenity). Проверьте, установлена ли утилита **zenity** в вашей системе и доступна ли она для использования, выполнив следующую команду:

```
which zenity
```

Если по какой-либо причине утилита zenity не установлена, для ее установки выполните команду (потребуются права **администратора**):

```
sudo dnf install zenity
```

Синтаксис и опции

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
zenity [опции]
```

Основные опции:

- **-h, --help** — вывести справку по работе с утилитой;
- **--version** — вывести версию утилиты;
- **--about** — просмотреть информацию о программе;
- **--help-general** — показать общие параметры.

Виды диалоговых окон:

- **--calendar** — диалоговое окно выбора даты;
- **--entry** — диалоговое окно с полем ввода текста;
- **--error** — диалоговое окно для вывода ошибки;
- **--info** — диалоговое окно для вывода информации;
- **--file-selection** — диалоговое окно выбора файлов;

- **--list** — диалоговое окно со списком;
- **--notification** — диалоговое окно уведомления;
- **--progress** — диалоговое окно выполнения процесса;
- **--question** — диалоговое окно запроса;
- **--warning** — диалоговое окно предупреждения;
- **--scale** — диалоговое окно шкалы;
- **--text-info** — диалоговое окно с текстовой информацией;
- **--color-selection** — диалоговое окно выбора цвета;
- **--password** — диалоговое окно пароля;
- **--forms** — диалоговое окно формы.

Параметры общего назначения:

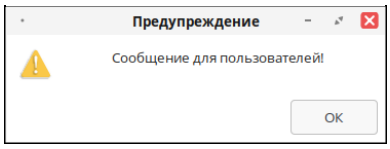
- **--title="ЗАГОЛОВОК"** — установить заголовок диалога;
- **--width=<ШИРИНА>** — установить ширину;
- **--height=<ВЫСОТА>** — установить высоту;
- **--timeout=<ЗАДЕРЖКА>** — установить задержку диалога в секундах;
- **--ok-label="ТЕКСТ"** — установить метку для кнопки «OK»;
- **--cancel-label="ТЕКСТ"** — установить метку для кнопки «Отменить»;
- **--extra-button="ТЕКСТ"** — добавить дополнительную кнопку;
- **--modal** — установить модальное свойство.

Примеры использования

Диалоговое окно для вывода предупреждения

Для вывода диалогового окна с предупреждением введите в терминал команду:

```
zenity --warning --text="Сообщение для пользователей" --width=300
```



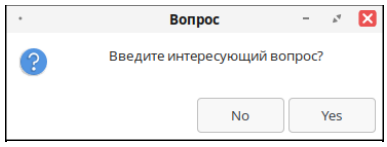
Параметры диалога предупреждения:

- **--warning** — показать диалог с предупреждением;
- **--text="ТЕКСТ"** — установить текст диалога;
- **--icon="ИМЯ_ЗНАЧКА"** — установить имя значка;
- **--no-wrap** — запретить перенос текста;
- **--no-markup** — не включать разметку Pango;
- **--ellipsize** — включить усечение текста в диалогах для уменьшения размера окна с длинным текстом.

Диалоговое окно с запросом

Для вывода диалогового окна с вопросом введите в терминал следующую команду:

```
zenity --question --text="Введите интересующий вопрос?" --width=300
```



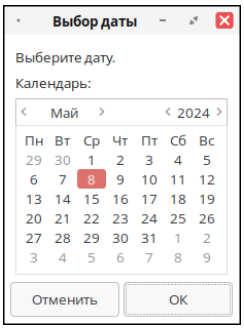
Параметры, используемые для запроса:

- **--question** — показать диалог с запросом;
- **--text="ТЕКСТ"** — установить текст диалога;
- **--icon="ИМЯ_ЗНАЧКА"** — установить имя значка;
- **--no-wrap** — запретить перенос текста;
- **--no-markup** — не включать разметку Pango;
- **--default-cancel** — фокус по умолчанию находится на кнопке «Отменить»;
- **--ellipsize** — включить усечение текста в диалогах для уменьшения размера окна с длинным текстом;
- **--switch** — скрыть кнопки «OK» и «Отменить».

Диалоговое окно с календарем

Для вывода диалогового окна с календарем для выбора желаемой даты введите следующую команду:

```
zenity --calendar
```



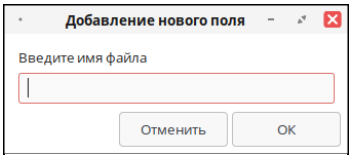
Параметры, используемые для вывода диалогового окна, в котором будет отображен календарь:

- **--calendar** — показать диалог выбора даты;
- **--text="ТЕКСТ"** — установить текст, отображаемый над календарем;
- **--day=<ДЕНЬ>** — установить день в календаре (число от 1 до 31);
- **--month=<МЕСЯЦ>** — установить месяц в календаре (число от 1 до 12);
- **--year =<ГОД>** — установить год в календаре;
- **--date-format=<ШАБЛОН>** — установить формат возвращаемой даты.

Диалоговое окно с полем ввода

Для запроса данных для ввода от пользователя выполните:

```
zenity --entry --text="Введите имя файла"
```



Параметры ввода текста:

- **--entry** — показать диалог с полем ввода;
- **--text="ТЕКСТ"** — установить текст диалога;
- **--entry-text="ТЕКСТ"** — установить текст для поля ввода;
- **--hide-text** — скрывать текст в поле ввода.

Добавление zenity в bash-сценарии

Пример 1 Диалоговое окно с сообщением

Для создания диалогового окна с сообщением при первом входе пользователя в систему выполните следующий алгоритм действий.

В РЕД ОС 7.3:

Для отображения диалогового окна при первом входе в систему добавьте сценарий в файл **/etc/gdm/PreSession/Default**. Выполните следующий алгоритм действий.

1. Откройте файл **/etc/gdm/PreSession/Default**, выполнив команду в терминале (потребуются права **администратора**):

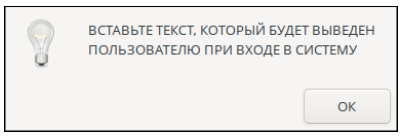
```
nano /etc/gdm/PreSession/Default
```

2. Добавьте в файл следующие строки и сохраните файл:

```
export LANG=ru_RU.UTF-8
 /usr/bin/zenity --info --text="ВСТАВЬТЕ ТЕКСТ, КОТОРЫЙ БУДЕТ ВЫВЕДЕН ПОЛЬЗОВАТЕЛЮ ПРИ ВХОДЕ В СИСТЕМУ" --width=300 --
height=150
```

где:

- **export LANG=ru_RU.UTF-8** — параметр, необходимый для работы с русским языком (является обязательным, иначе авторизация не будет проходить успешно);
- **--info** — диалог для вывода информации;
- **--text="ТЕКСТ"** — текст для отображения;
- **--width=<Значение>** — ширина диалогового окна;
- **--height=<Значение>** — высота диалогового окна.



В РЕД ОС 8.0:

1. Создайте файл в каталоге **/home/user1/** (замените user1 на актуальное имя пользователя):

```
nano /home/user1/zenitywel.sh
```

2. Добавьте в него следующие строки:

```
#!/bin/bash
 export LANG=ru_RU.UTF-8
 /usr/bin/zenity --info --text="Добро пожаловать" --width=300 --height=150
```

3. Выдайте права на исполнение файла:

```
chmod +x /home/user1/zenitywel.sh
```

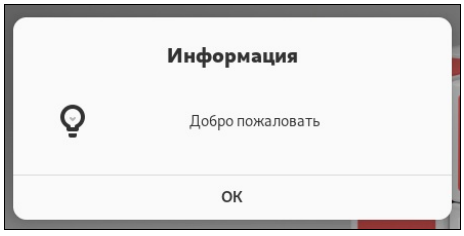
4. Создайте файл в каталоге **/etc/xdg/autostart/** для автозапуска уведомления во время авторизации пользователя:

```
nano /etc/xdg/autostart/WelcomeZenity.desktop
```

5. Добавьте в него следующие строки:

```
[Desktop Entry]
 Type=Application
 Name=Welcome Message
 Comment=Shows a welcome message
 Exec=/home/user1/zenitywel.sh
 Terminal=false
 X-MATE-Autostart-enabled=true #если используется графическая оболочка MATE
 X-GNOME-Autostart-enabled=true #если используется графическая оболочка GNOME
 X-KDE-Autostart-enabled=true #если используется графическая оболочка KDE
```

6. Перезапустите ПК. После авторизации пользователя отобразится диалоговое окно.



Пример 2 Диалоговое окно формы

Для создания **bash-скрипта** выполните следующий алгоритм действий:

1. Для создания файла скрипта введите команду:

```
nano newscript.sh
```

2. Впишите в файл следующие строки и сохраните файл:

```
#!/bin/bash

zenity --forms --title="Добавление сведений" \
	--text="Введите информацию ниже:" \
	--separator="," \
	--add-entry="Имя" \
	--add-entry="Фамилия" \
	--add-combo=Пол \
	--combo-values="мужской|женский"\
	--add-entry="СНИЛС" \
	--add-calendar="Дата рождения"

case $? in
0)
	echo "Информация добавлена.";;
1)
	echo "Информация не добавлена.";;
-1)
	echo "Произошла ошибка.";;
esac
```

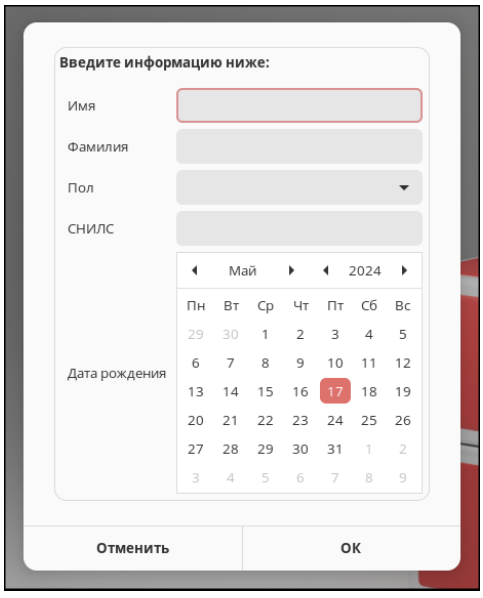
3. Для предоставления прав на выполнение файла выполните команду:

```
chmod +x newscript.sh
```

4. Для запуска скрипта выполните команду:

```
./newscript.sh
```

Результат выполнения скрипта:



С дополнительной информацией по созданию интерактивных меню можно ознакомиться в наших статьях:

- Dialog — утилита для создания диалоговых окон в консольных приложениях ;
- Yad — утилита для создания диалоговых окон с использованием терминала или сценариев .

Yad — утилита для создания диалоговых окон с использованием терминала или сценариев

Установка yad
Синтаксис и опции
Примеры использования
Диалоговое окно формы ввода
Диалоговое окно выбора цвета
Диалоговое окно с календарем
Ссылка в диалоговом окне
Список в диалоговом окне
Диалоговое окно для ввода текста
Добавление yad в bash-сценарии
Пример 1. Диалоговое окно записной книжки
Пример 2. Диалоговое окно с сообщением

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: yad-13.0

Yad (**Yet Another Dialog**) — программа для построения графических диалоговых окон (**GTK3**) из сценариев оболочки или командной строки, что позволяет предоставлять и запрашивать информацию у пользователя.

С ее помощью можно создавать диалоговые окна с различными элементами управления, включая кнопки, флажки, текстовые поля и т.д.

Yad может использоваться для создания пользовательских интерфейсов для скриптов командной строки и других приложений.

Установка yad

По умолчанию в РЕД ОС утилита **yad** уже установлена (расположена в каталоге **/usr/bin/yad**). Проверьте, установлена ли утилита **yad** в вашей системе и доступна ли она для использования, выполнив следующую команду:

```
which yad
```

Если по какой-либо причине утилита **yad** не установлена, для ее установки выполните следующую команду (потребуются права **администратора**):

```
sudo dnf install yad
```

Синтаксис и опции

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
yad [опции]
```

Основные опции:

- **-h**, **--help** — вывести справку по работе с утилитой;
- **--version** — вывести версию утилиты;
- **--about** — просмотреть информацию о программе;
- **--help-general** — показать общие параметры.

Опции утилиты, отвечающие за вид диалогового окна:

- **--app** — диалоговое окно выбора приложения;
- **--calendar** — диалоговое окно выбора даты;
- **--color** — диалоговое окно выбора цвета;
- **--dnd** — диалоговое окно для перетаскивания объектов;
- **--entry** — диалоговое окно с полем ввода текста;
- **--icons** — диалоговое окно со значками ярлыков;
- **--file** — диалоговое окно выбора файлов;

- **--font** — диалоговое окно выбора шрифта;
- **--form** — диалоговое окно формы;
- **--html** — диалоговое окно HTML;
- **--list** — диалоговое окно со списком;
- **--multi-progress** — диалоговое окно с несколькими индикаторами выполнения;
- **--notebook** — диалоговое окно блокнота;
- **--notification** —диалоговое окно уведомления;
- **--print** — диалоговое окно печати;
- **--progress** — диалоговое окно выполнения процесса;
- **--text-info** — диалоговое окно с текстовой информацией;
- **--scale** — диалоговое окно шкалы.

Опции общего назначения:

- **--title="ЗАГОЛОВОК"** —установить заголовок диалога;
- **--window-icon=<ICON>** — установить значок окна;
- **--width=<ШИРИНА>** — установить ширину;
- **--height=<ВЫСОТА>** — установить высоту;
- **--timeout=<ЗАДЕРЖКА>** — установить задержку диалога в секундах;
- **--ok-label="ТЕКСТ"**— установить метку для кнопки «**OK**»;
- **--cancel-label="ТЕКСТ"** — установить метку для кнопки «**Отменить**»;
- **--extra-button="ТЕКСТ"** — добавить дополнительную кнопку;
- **--modal** — установить модальное свойство;
- **--posx=<ЧИСЛО>** — установить горизонтальное положение диалогового окна;
- **--posy=<ЧИСЛО>** — установить вертикальное положение диалогового окна;
- **--geometry=<ШИРИНА>x<ВЫСОТА>+<X>+<Y>** — установить размеры диалогового окна;
- **--timeout-indicator=<ПОЗИЦИЯ>** — показывать индикатор задержки в позиции (*top*, *bottom*, *left* или *right*);
- **--no-buttons** — не показывать кнопки;
- **--no-focus** — не фокусировать диалоговое окно;
- **--fullscreen** — запустить диалог в полноэкранном режиме;
- **--text="ТЕКСТ"** — текст сообщения;
- **--text-width=<ЧИСЛО>** — установить максимальную ширину текста диалога в символах;
- **--text-align=<ТИП>** — задать тип выравнивания текста диалога (*left*, *right*, *center* или *fill*);
- **--icon-theme=<ТЕМА>** — использовать указанную тему значков GTK вместо стандартной;
- **--sticky** — сделать окно видимым на всех рабочих столах;
- **--fixed** — сделать окно фиксированной ширины и высоты;
- **--center** — разместить окно в центре экрана;
- **--mouse** — разместить окно под позицию мыши;
- **--on-top** — разместить окно поверх других окон;
- **--undecorated** — удалить заголовок и рамки окна;
- **--enable-spell** — включить проверку орфографии.

Пользовательские параметры диалогового окна:

- **--pname="ТЕКСТ"** — установить имя программы;
- **--image=<ИЗОБРАЖЕНИЕ>** — установить имя значка программы;
- **--pversion="ТЕКСТ"** — установить строку версии программы;
- **--copyright="ТЕКСТ"** — установить строку авторского права программы;
- **--comments="ТЕКСТ"** — подробное описание программы;
- **--license="ТЕКСТ"** — установить лицензию программы, где значением может быть одна из предопределенных лицензий (GPL2, GPL3, LGPL2, LGPL3, BSD, MIT или ARTISTIC), имя файла с текстом лицензии или произвольная строка;
- **--authors="ТЕКСТ"** — установить список авторов программы через запятую;
- **--website=<URI>** — установить ссылку на сайт программы;
- **--website-label=<МЕТКА>** — установить метку для ссылки на сайт программы.

Опции выбора приложения:

- **--enable-fallback**— показать резервные приложения;
- **--enable-other** — показать другие приложения;
- **--enable-all**— показать все доступные приложения;
- **--extened** — показать расширенную информацию о выбранном приложении, где полями вывода являются имя, отображаемое имя, описание, значок и исполняемый файл.

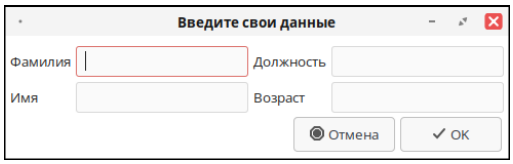
Примеры использования

В зависимости от ситуации, требующей незамедлительного вмешательства пользователя или запуска окна в определенное время, можно использовать соответствующие команды в скрипте или непосредственно из командной строки. В диалоговой форме можно получать данные от пользователя, а затем передавать их в скрипт.

Диалоговое окно формы ввода

Для вывода диалогового окна для получения данных от пользователя введите команду:

```
yad --form --title="Введите свои данные" --columns=2 --field="Фамилия" --field="Имя" --field="Должность" --field="Возраст"
```

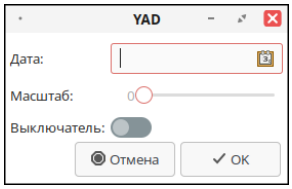


Параметры диалога формы ввода:

- **--form** — отобразить диалог формы с полями ввода;
- **--field=<МЕТКА>[:ТИП]** — добавить поле к форме (список типов указан на странице руководства **yad**);
- **--align=<ТИП>** — задать выравнивание меток полей (*left*, *center* или *right*);
- **--columns=<ЧИСЛО>** — задать количество колонок в форме;
- **--homogeneous** — сделать высоту и ширину полей формы одинакового размера;
- **--output-by-row** — упорядочить вывод по строкам;
- **--focus-field=<ЧИСЛО>** — задать поле, получающее фокус;
- **--changed-action=<КОМАНДА>** — задать действие при изменении поля.

Для создания формы с указанными полями, введите следующую команду в терминале:

```
yad --form --field="Дата::DT" --field="Масштаб::SCL" --field="Выключатель::SW"
```



Типы полей формы:

--field=МЕТКА[:ТИП] — тип может быть *H*, *RO*, *NUM*, *CHK*, *CB*, *CBE*, *CE*, *FL*, *SFL*, *DIR*, *CDIR*, *FN*, *MFL*, *MDIR*, *DT*, *SCL*, *SW*, *APP*, *ICON*, *CLR*, *BTN*, *FBTN*, *LINK*, *LBL* или *TXT*.

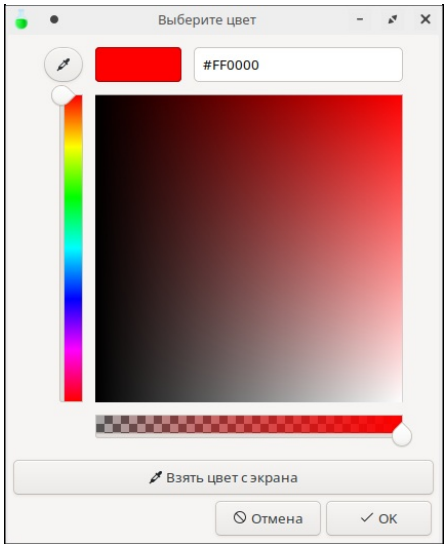
- **H** — тип скрытого поля, все символы отображаются как невидимые символы;
- **RO** — поле только для чтения;
- **NUM** — числовое поле ЗНАЧЕНИЕ[!ДИАПАЗОН[!ШАГ![PREC]]] задает формат начального значения, диапазона, шага, **PREC** — это точность десятичных дробей;
- **CHK** — поле-флажок, где начальное значение представляет собой логическую константу, нечувствительную к регистру (*ИСТИНА* или *ЛОЖЬ*);
- **CB** — поле со списком, где начальное значение представляет собой список ЗНАЧ1!ЗНАЧ2!...;
- **CBE** — редактируемое поле со списком;
- **CE** — запись с завершением;
- **FL** — кнопка выбора файла;
- **SFL** — поле для создания файла;
- **DIR** — кнопка выбора директории;
- **CDIR** — поле для создания папки;
- **FN** — кнопка выбора шрифта;
- **MFL** — выбрать несколько файлов;
- **MDIR** — выбор нескольких папок;
- **DT** — поле выбора даты;
- **SCL** — поле масштаба, принимающее значения в диапазоне **0..100**;
- **S W** — поле выключателя, где начальное значение представляет собой логическую константу, нечувствительную к регистру (*ИСТИНА* или *ЛОЖЬ*);
- **APP** — кнопка выбора приложения, где входное значение для этого поля имеет тип **mime**, выходное значение — исполняемый файл для выбранного приложения;
- **ICON** — поле значка имеет две иконки: слева отображается текущий значок, а справа можно щелкнуть и вызвать yad-con-браузер для выбора значка;
- **CLR** — кнопка выбора цвета;
- **BTN** — поле кнопки (метка может быть в виде текста в формате LABEL[!ICON[!TOOLTIP]], где «**!**» является разделителем элементов, **LABEL** — это текст надписи на кнопке или идентификатор, **ICON** — значок кнопки (идентификатор или имя файла), **TOOLTIP** — это необязательный текст для всплывающей строки справки);
- **FBTN** — поле кнопки с полным рельефом;
- **LINK** — поле кнопки ссылки;
- **LBL** — текстовая метка (если имя поля пустое, будет показана горизонтальная разделительная линия);
- **TXT** — многострочный ввод текста, занимающий всю ширину формы.

При использовании наименования поля без типа будет выведена простая текстовая запись.

Диалоговое окно выбора цвета

Для вывода диалогового окна выбора цвета введите в терминал следующую команду:

```
yad --title="Выберите цвет" --color --init-color=RED --picker
```



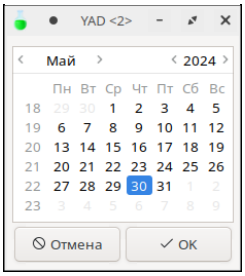
Параметры диалога выбора цвета:

- **--color** — отобразить диалог для выбора цвета;
- **--init-color=<ЦВЕТ>** — задать начальное значение цвета;
- **--gtk-palette** — показать системную палитру;
- **--palette="ИМЯ_ФАЙЛА"** — указать путь к файлу палитры;
- **--expand-palette** — раскрыть пользовательскую палитру;
- **--picker** — показать кнопку выбора цвета;
- **--mode=<РЕЖИМ>** — установить режим вывода на экран, где значения — *hex* (по умолчанию) или *rgb*;
- **--alpha** — добавить прозрачность к значению цвета.

Диалоговое окно с календарем

Для вывода диалогового окна с календарем введите следующую команду:

```
yad --calendar --day=30 --show-weeks
```



Параметры, используемые для вывода диалогового окна, в котором будет отображен календарь:

- **--calendar** — показать диалог выбора даты;
- **--day=<ДЕНЬ>** — установить день в календаре (число от 1 до 31);
- **--month=<МЕСЯЦ>** — установить месяц в календаре (число от 1 до 12);
- **--year =<ГОД>** — установить год в календаре;
- **--details="ИМЯ_ФАЙЛА"** — задать имя файла с описанием дат;
- **--show-weeks** — показать нумерацию недель слева.

Ссылка в диалоговом окне

1. Выберите директорию и создайте файл, например:

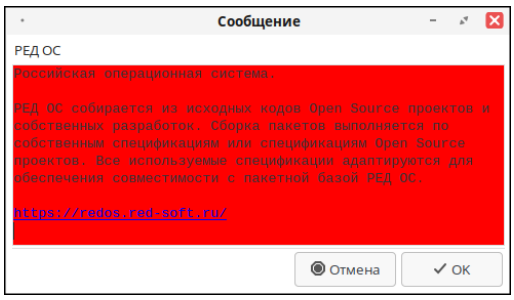
```
nano /home/user/text.txt
```

2. Запишите в него требуемую информацию:

«Российская операционная система.
РЕД ОС собирается из исходных кодов Open Source проектов и собственных разработок. Сборка пакетов выполняется по собственным спецификациям или спецификациям Open Source проектов. Все используемые спецификации адаптируются для обеспечения совместимости с пакетной базой РЕД ОС.
https://redos.red-soft.ru/.

3. Сохраните файл и выполните следующую команду в терминале:

```
yad --text-info --back=red </home/user/text.txt --show-uri --text="РЕД ОС" --title="Сообщение" --wrap --editable --tail --show-cursor
```



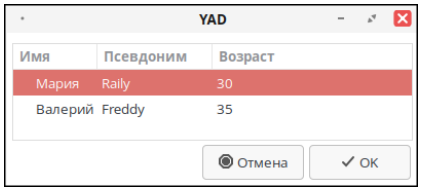
Параметры:

- **--text-info** — создает окно для отображения текстовой информации;
- **--back=ЦВЕТ** — использует указанный цвет для фона;
- **--wrap** — включить перенос текста;
- **--editable** — разрешить изменения в тексте;
- **--tail** — автопрокрутка до конца текста;
- **--show-cursor** — показывать курсор в режиме только для чтения;
- **--text="ТЕКСТ"** — текст сообщения;
- **--show-uri** — сделать URI кликабельным.

Список в диалоговом окне

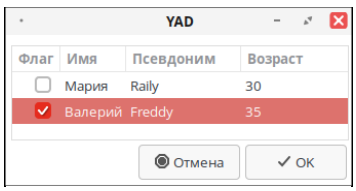
Диалоговое окно для списка можно получить, введя команду:

```
yad --list --column="Имя" --column="Псевдоним" --column=Возраст Мария Raily 30 Валерий Freddy 35 --height=150 --width=400
```

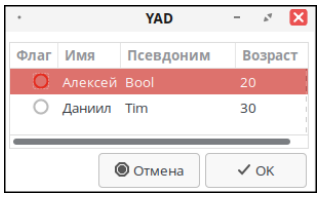


Для добавления в список элементов **--checklist** или **--radiolist** можно воспользоваться следующими примерами:

```
yad --list --checklist --width=300 --height=130 --column="Флаг" --column="Имя" --column= "Псевдоним" --column="Возраст" false Мария Raily 30 false  Валерий Freddy 35
```

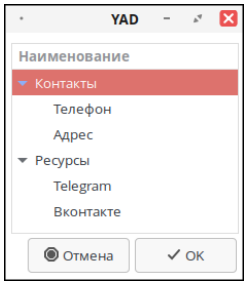



```
yad --list --radiolist --width=302 --height=123 --column="Флаг" --column="Имя" --column="Псевдоним"  --column="Возраст"   false Алексей Bool 20 false Даниил Tim 30
```



Отобразить список в режиме дерева можно следующим образом:

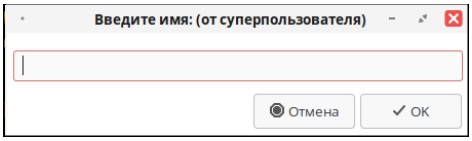
```
yad --list --tree --column "Наименование" f  "Контакты" 1:f  "Телефон" 2:f "Адрес" v  "Ресурсы" 3:v "Telegram"  4:v "Вконтакте"
```



Диалоговое окно для ввода текста

Диалоговое окно для ввода текста с заголовком «***Введите имя:***» шириной 450 и высотой 100 можно получить, выполнив команду:

```
yad --entry --title="Введите имя:" --height=100 --width=450
```



Добавление yad в bash-сценарии

Пример 1. Диалоговое окно записной книжки

Блокнот представляет собой сложный диалог, который поглощает другие диалоги на своих вкладках. Диалоги идентифицируются уникальным ключом (целым числом) и должны запускаться в специальном режиме плагина (опция *--plug*). В следующем примере запускается диалоговое окно записной книжки с двумя вкладками: первая содержит простой текст, а вторая — диалоговое окно ввода.

1. Выберите нужную директорию и создайте файл в формате **sh**:

```
nano /home/user/Документы/script.sh
```

2. Впишите в файл следующие строки и сохраните:

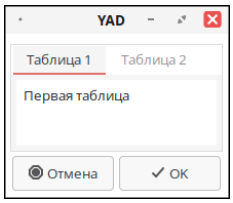
```
#! /bin/sh
 yad --plug=123 --tabnum=1 --text="Первая таблица" &> res1 &
 yad --plug=123 --tabnum=2 --text="Вторая таблица" --entry &> res2 &
 yad --notebook --key=123 --tab="Таблица 1" --tab="Таблица 2"
```

3. Для выполнения *bash-скрипта* назначьте пользователю права на выполнение с помощью следующей команды:

```
chmod u+x script.sh
```

4. Запустите скрипт с помощью команды:

```
sh script.sh
```



Пример 2. Диалоговое окно с сообщением

Для создания диалогового окна с сообщением при первом входе пользователя в систему выполните следующий алгоритм действий.

В РЕД ОС 7.3:

1. Откройте файл **/etc/gdm/PreSession/Default**, введя команду в терминале (потребуются права **администратора**):

```
nano /etc/gdm/PreSession/Default
```

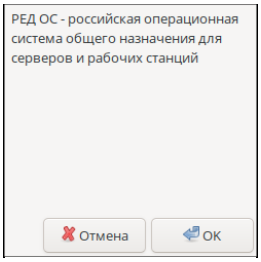
2. Впишите в файл следующие строки и сохраните:

```
export LANG=ru_RU.UTF-8 /usr/bin/yad --center --geometry=250x250 --text="РЕД ОС — российская операционная система общего назначения для серверов и рабочих станций"
```

где**:**

- **export LANG=ru_RU.UTF-8** — параметр, необходимый для работы с русским языком (является обязательным, иначе авторизация не будет проходить успешно);
- **--geometry= 250x250** — задать размеры окна;
- **--center** — выровнять диалоговое окно по центру;
- **--text="ТЕКСТ"** — текст сообщения.

3. Перезагрузите ПК. После авторизации пользователя появится окно с уведомлением.



В РЕД ОС 8.0:

1. Создайте скрипт **/home/user1/yadwel.sh** (замените user1 на актуальное имя пользователя):

```
nano /home/user1/yadwel.sh
```

2. Добавьте в него следующие строки:

```
#!/bin/bash
 export LANG=ru_RU.UTF-8
 /usr/bin/yad --center --geometry=250x250 --text="РЕД ОС — российская операционная система общего назначения для серверов и рабочих станций"
```

3. Выдайте права на исполнение файла:

```
chmod +x /home/user1/yadwel.sh
```

4. Создайте файл в каталоге **/etc/xdg/autostart/** для автозапуска уведомления во время авторизации пользователя:

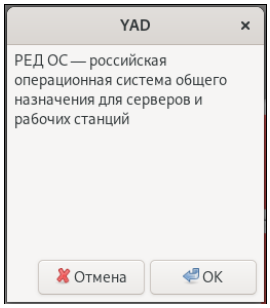
```
nano /etc/xdg/autostart/WelcomeYad.desktop
```

5. Добавьте в него следующие строки:

```
[Desktop Entry]
```

```
Type=Application
Name=Welcome Message
Comment=Shows a welcome message
Exec=/home/user1/yadwel.sh
Terminal=false
X-MATE-Autostart-enabled=true ##если используется графическая оболочка MATE
X-GNOME-Autostart-enabled=true #если используется графическая оболочка GNOME
X-KDE-Autostart-enabled=true #если используется графическая оболочка KDE
```

6. Перезагрузите ПК. После авторизации пользователя появится окно с уведомлением.



В наших статьях можно подробнее ознакомиться с использованием утилит создания интерактивных меню в РЕД ОС:

- Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- Dialog — утилита для создания диалоговых окон в консольных приложениях .

Dialog – утилита для создания диалоговых окон в консольных приложениях

Установка
Синтаксис и опции
Примеры использования
Диалоговое окно сообщения с кнопкой «OK»
Сообщение с кнопками «Да» и «Нет»
Диалоговое окно с календарем
Диалоговое окно с контрольным списком
Диалоговое окно формы
Добавление dialog в bash-сценарии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО в РЕД ОС 7.3**: dialog 1.3-20171209

Dialog — это утилита для построения консольных интерфейсов. Диалоговые окна можно легко включить в сценарии оболочки для взаимодействия с пользователями. **Dialog** позволяет создавать интерфейсы на любом консольном языке.

Установка

Пакет диалогов по умолчанию не установлен в РЕД ОС. Установить **dialog** можно, выполнив следующую команду в терминале (потребуются права **администратора**):

```
sudo dnf install dialog
```

Команда устанавливает пакет диалогов и необходимые библиотеки для системы.

Синтаксис и опции

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
dialog [опции]
```

Основные опции:

- **-h, --help** — вывести справку по работе с утилитой;
- **--version** — вывести версию утилиты;
- **--about** — просмотреть информацию о программе;
- **--help-general** — показать общие параметры.

Опции общего назначения:

- **--title="Заголовок"** — задает заголовок диалога;
- **--backtitle="Заголовок"** — задает строку заголовка, которая будет отображаться на фоне в верхней части экрана;
- **--ascii-lines** — рисует знаки «**---**», «**|**», «**+++**» вместо обычных линий рамок;
- **--scrollbar** — добавляет полосы прокрутки;
- **--defaultno** — добавляет кнопку «**Нет**» по умолчанию;
- **--clear** — очищает экран перед отображением диалога.

Опции утилиты, отвечающие за вид диалогового окна:

- **--buildlist** — диалоговое окно списка сборки, отображающее списки с невыбранными и выбранными элементами. Синтаксис диалогового окна имеет вид: `--buildlist <text> <height> <width> <list-height> <tag1> <item1> <status1>...`;
- **--calendar** — диалоговое окно календаря, отображающее день, месяц или год. Синтаксис диалогового окна имеет вид: `--calendar <text> <height> <width> <day> <month> <year>`;
- **--checklist** — диалоговое окно контрольного списка. Синтаксис диалогового окна имеет вид: `--checklist <text> <height> <width> <list height> <tag1> <item1> <status1>...`;
- **--dselect** — диалоговое окно выбора каталога. Синтаксис диалогового окна имеет вид: `--dselect <directory> <height> <width>`;
- **--editbox** — диалоговое окно редактирования. Синтаксис диалогового окна имеет вид: `--editbox <file> <height> <width>`;
- **--form** — диалоговое окно формы. Синтаксис диалогового окна имеет вид: `--form <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1>...`;
- **--fselect** — диалоговое окно выбора файла. Синтаксис диалогового окна имеет вид: `--fselect <filepath> <height> <width>`;
- **--gauge** — диалоговое окно индикатора. Синтаксис диалогового окна имеет вид: `--gauge <text> <height> <width> [<percent>]`;
- **--infobox** — информационное окно. Синтаксис диалогового окна имеет вид: `--infobox <text> <height> <width>`;
- **--inputbox** — диалоговое поле ввода данных от пользователя. Синтаксис диалогового окна имеет вид: `--inputbox <text> <height> <width> [<init>]`;
- **--inputmenu** — диалоговое окно меню ввода. Синтаксис диалогового окна имеет вид: `--inputmenu <text> <height> <width> <menu height> <tag1> <item1>...`;
- **--menu** — диалоговое окно меню. Синтаксис диалогового окна имеет вид: `--menu <text> <height> <width> <menu height> <tag1> <item1>...`;
- **--mixedform** — диалоговое окно смешанной формы, состоящее из меток и полей. Синтаксис диалогового окна имеет вид: `--mixedform <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1> <itype>...`;
- **--mixedgauge** — диалоговое окно смешанного счетчика. Синтаксис диалогового окна имеет вид: `--mixedgauge <text> <height> <width> <percent> <tag1> <item1>...`;
- **--msgbox** — диалоговое окно сообщения. Синтаксис диалогового окна имеет вид: `--msgbox <text> <height> <width>`;
- **--passwordbox** — диалоговое поле пароля. Синтаксис диалогового окна имеет вид: `--passwordbox <text> <height> <width> [<init>]`;
- **--passwordform** — диалоговое окно формы с вводом пароля. Синтаксис диалогового окна имеет вид: `--passwordform <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1>...`;
- **--pause** — диалоговое окно паузы. Синтаксис диалогового окна имеет вид: `--pause <text> <height> <width> <seconds>`;
- **--prgbox** — диалоговое окно для отображения вывода команды. Синтаксис диалогового окна имеет вид: `--prgbox <text> <command> <height> <width>`;
- **--programbox** — диалоговое окно программного блока. Синтаксис диалогового окна имеет вид: `--programbox <text> <height> <width>`;
- **--progressbox** — диалоговое окно прогресса. Синтаксис диалогового окна имеет вид: `--progressbox <text> <height> <width>`;
- **--radiolist** — диалоговое окно радиосписка. Синтаксис диалогового окна имеет вид: `--radiolist <text> <height> <width> <list height> <tag1> <item1> <status1>...`;
- **--rangebox** — диалоговое окно с выбором диапазона значений. Синтаксис диалогового окна имеет вид: `--rangebox <text> <height> <width> <min-value> <max-value> <default-value>`;
- **--tailbox** — диалоговое окно отображения текста из файла. Синтаксис диалогового окна имеет вид: `--tailbox <file> <height> <width>`;
- **--tailboxbg** — диалоговое окно отображения текста из файла в качестве фоновой задачи. Синтаксис диалогового окна имеет вид: `--tailboxbg <file> <height> <width>`;
- **--textbox** — диалоговое окно с текстовым полем. Синтаксис диалогового окна имеет вид: `--textbox <file> <height> <width>`;
- **--timebox** — диалоговое окно, позволяющее выбрать время. Синтаксис диалогового окна имеет вид: `--timebox <text> <height> <width> <hour> <minute> <second>`;
- **--treeview** — диалоговое окно отображения данных в виде дерева. Синтаксис диалогового окна имеет вид: `--treeview <text> <height> <width> <list-height> <tag1> <item1> <status1> <depth1>...`;
- **--yesno** — диалоговое окно «Да»/«Нет». Синтаксис диалогового окна имеет вид: `--yesno <text> <height> <width>`.

Параметры диалоговых окон:

- **--text** — задает заголовок или содержимое поля;

- **--height** — задает высоту диалогового окна;
- **--width** — задает ширину диалогового окна;
- **--list-height** — высота списка.

Примеры использования

Диалоговое окно сообщения с кнопкой «OK»

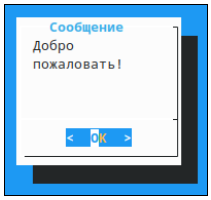
Окно сообщения отображает сообщение и требует от пользователя нажать кнопку «**OK**».

Формат сообщения следующий: `--msgbox <text> <height> <width>`

Для вывода на экран сообщения "**Hello world!**", необходимо воспользоваться следующей командой в консоли:

```
dialog --title "Сообщение" --msgbox "Добро пожаловать!" 8 20
```

Результат выполнения этой команды выглядит следующим образом:



Сообщение с кнопками «Да» и «Нет»

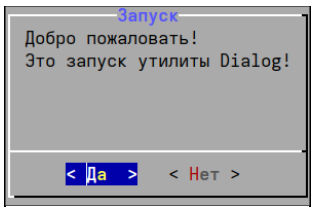
Параметр **--yesno** — предоставляет простое сообщение с кнопками « **Да**» и «**Нет**».

Формат сообщения следующий: `--yesno <text> <height> <width>`

Например, для вывода сообщения введите в терминал команду:

```
dialog --title "Запуск" --yesno "Добро пожаловать! \nЭто запуск утилиты Dialog!" 9 30
```

После запуска будет выведено следующее диалоговое окно:



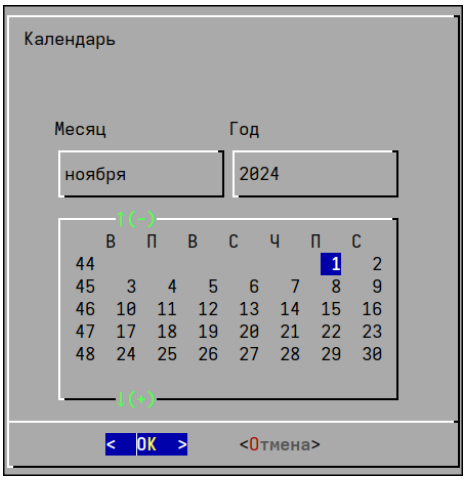
Программа будет ждать пользовательского выбора. Нажмите кнопку «**Да**», «**Нет**» или клавишу «**Esc**».

Диалоговое окно с календарем

Календарь — предоставляет календарь для отображения выбранной даты.

Формат календаря: `--calendar <text> <height> <width> <day> <month> <year>`

```
dialog --calendar "Календарь" 5 45 01 11 2024
```

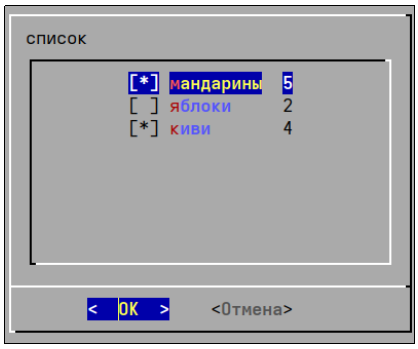


Диалоговое окно с контрольным списком

Контрольный список — отображает несколько записей, каждую из которых можно включить или отключить.

Формат списка: `--checklist <text> <height> <width> <list height> <tag1> <item1> <status1>...`

```
dialog --checklist "список" 15 40 12 "мандарины" 5 "on" "яблоки" 2 "off" "киви" 4 "on"
```

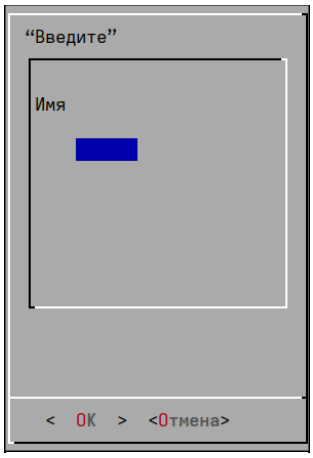


Диалоговое окно формы

Форма позволяет создать форму с метками и текстовыми полями для заполнения.

Формат формы следующий: `--form <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1>...`

```
dialog --form "Введите" 20 30 20 "Имя" 2 1 "" 4 5 6 7
```



Добавление dialog в bash-сценарии

Для создания bash-скрипта выполните следующий алгоритм действий:

1. Для создания пустого файла скрипта введите команду:

```
touch newscript.sh
```

2. Для открытия файла используйте любой текстовый редактор, например:

```
nano newscript.sh
```

3. Впишите в файл следующие строки и сохраните файл:

```
#! /bin/sh

 DIALOG=${DIALOG=dialog}
 $DIALOG --backtitle "Окно для выбора устройств" \
 --title "Выбор устройств" --clear \
 --radiolist "Список устройств" 20 61 5 \
 "Aqara LED Light Bulb" "Умная лампа" ON \
 "Yeelight Lightstrip Pro" "Умная светодиодная лента" off \
 "Yeelight Ceiling Light" "Умный потолочный светильник" off \
 "Aqara Gas Sensor" "Датчик газа" off \
 "Aqara TVOC Air Quality Monitor" "Монитор качества воздуха" off
```

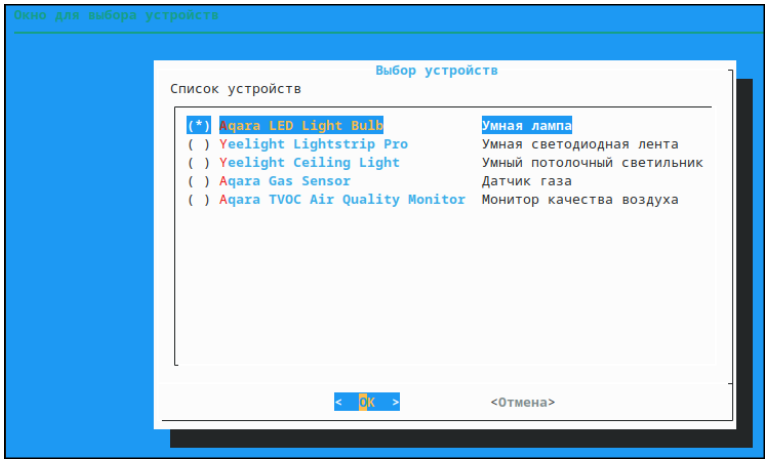
4. Для предоставления прав на выполнение файла выполните команду:

```
chmod +x newscript.sh
```

5. Для запуска скрипта выполните команду:

```
./newscript.sh
```

Результат выполнения скрипта:



В наших статьях можно подробнее ознакомиться с использованием утилит создания интерактивных меню в РЕД ОС:

- Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- Yad — утилита для создания диалоговых окон с использованием терминала или сценариев .

Полноэкранный редактор VI и улучшенный редактор VIM

Режимы работы редактора
Ввод текста
Команды
Перемещение курсора
Редактирование
Командная строка
Блоки, буферы, окна редактирования. Повторители
Открыть/создать файл
Дополнительные опции
Улучшенный редактор VIM

Редактор **vi** - универсальный полноэкранный текстовый редактор в среде UNIX. Универсальность означает, что, во-первых, этот редактор есть во всех UNIX-подобных ОС и, во-вторых, этот редактор работает с практически любым видом терминала (ANSI, VT100, VT220, VT320, DEC, и т. д.). Эта универсальность выражается непривычным (для пользователей DOS) пользовательским интерфейсом: для управления редактором используются лишь «обычные» кнопки клавиатуры (алфавитно-цифровые символы и знаки препинания). Имеющиеся на многих типах терминалов функциональные клавиши практически не используются. Если клавиатура терминала имеет стрелочные клавиши, то они используются, но в ограниченном контексте.

Вы можете подробнее ознакомиться с информацией по работе с редактором **vim**, просмотрев наши обучающие видео:

- на **RuTube** — Текстовый редактор vim;
- в **Яндекс.Дзен** — Текстовый редактор vim;
- в **VK Видео** — Текстовый редактор vim.

На наших каналах вы также сможете найти много другой полезной информации.

Режимы работы редактора

Ввод текста

В этом режиме все, что набирается на клавиатуре, отображается на экране терминала и запоминается в буфере редактора.

В данном режиме нет возможности осуществлять операции редактирования текста, за исключением стирания последнего набранного символа (с помощью комбинации клавиш «Ctrl+H»).

Командный режим

В этом режиме символы клавиатуры выполняют специальные функции (перемещение курсора, стирание частей текста, и т. д.), то есть функции редактирования.

В данном режиме набираемые команды **не отображаются на экране**.

Режим командной строки

Режим командной строки позволяет производить более глобальные операции с текстом: записывать отредактированный текст в файл, считывать новый файл, выходить из vi, производить настройку редактора, поиск по шаблону, а также осуществлять некоторые функции редактирования.
Команды отображаются в нижней части экрана (в командной строке редактора).

Ввод текста

«Return» - создает пустую строку и переводит курсор в ее начало;

«Ctrl+H» - уничтожает последний введенный символ (это действие не отображается на экране до выхода в командный режим);

«Ctrl+[» или клавиша «Esc» - переводят редактор в командный режим.

В режиме ввода текста стрелочная клавиатура **не работает**.

Команды

i - переход в режим набора методом вставки перед текущим символом;
a - переход в режим набора методом вставки за текущим символом;
R - переход в режим набора текста методом набивки.

Перемещение курсора

h, j, k, l - на один символ (одну строку), как показано стрелками;
^ или 0 - в начало текущей строки;
$ - в конец текущей строки;
w - на слово вправо;
b - на слово влево;
} - на параграф вперед (параграф - это блок текста, отделенный пустой строкой);
{ - на параграф назад;
[[- в начало текста;
]] - в конец текста.
Кнопки стрелочной клавиатуры также позволяют перемещаться по тексту.

Редактирование

Предположим, в нашем файле записан текст, который необходимо отредактировать. Для этого необходимо перейти в режим ввода. Самый простой способ - из командного режима нажатие клавиши "i". После чего можно приступать к вводу текста. <ESC> вернет нас к командному режиму.

Другие важные команды:

Команда	Описание команды
R,i	переход в режим ввода - замена текста под курсором
I	переход в режим ввода с начала текущей строки
o	переход в режим ввода с новой строки под курсором
O	переход в режим ввода с новой строки над курсором
a	переход в режим ввода после курсора
x	стирание символа под курсором
X	стирание символа перед курсором
dd	стирание текущей строки
d<число>d	стирание числа строк, начиная с текущей
yy	копирование текущей строки в неименованный буфер
y<число>y	копирование числа строк начиная с текущей в неименованный буфер
p	вставка строки из неименованного буфера под курсор
P	вставка строки из неименованного буфера над курсором
J	слияние текущей строки со следующей
u	отмена последней команды
.	повтор последней команды
:	переход в режим командной строки

Командная строка

:q или :q! - выход из редактора без сохранения изменений;

:x- выход из редактора с записью, если файл был модифицирован;

:w или w <имя_файла> или w! <имя_файла> - запись файла и возвращение в командный режим;

:e <имя_файла> или :e! <имя_файла> - загрузка файла <имя_файла>;

:r <имя_файла> - добавить содержимое указанного файла к редактируемому сразу за текущей строкой;

:set nu - включить нумерацию строк;

:set nonu - отключить нумерацию строк;

:!command - выполнить команду UNIX, не покидая редактора;

:/word - выполнить поиск слова word в тексте;

:/ - повторить поиск слова word далее по тексту.

Блоки, буферы, окна редактирования. Повторители

Повторители

Командам и движениям курсора можно давать повторители (числа), например:
2w - передвинуть курсор на два слова вперед;
10l - передвинуть курсор на десять символов вправо;
d10l - стереть десять символов справа от курсора;
2d10l - стереть двадцать символов справа от курсора;
5J - слить пять последующих строк в одну;
4. - повторить последнюю введенную команду четыре раза.

Буферы vi

Редактор имеет три типа буферов: буфер стирания (0-9), неименованный буфер и именованные буферы (a-z).

В буферы стирания автоматически заносятся стираемые элементы. В буфере 0 хранится последний стертый элемент, в буфере 1 - предпоследний и т. д.

Занести в буфер:

yy - занести текущую строку в неименованный буфер;

y<движение_курсора> - занести указанный движением курсора блок текста в неименованный буфер;

"ayy - занести текущую строку в именованный буфер «a»;

"Ayy - добавить текущую строку к содержимому именованного буфера «a»;

"by10j - занести последующие 10 строк в именованный буфер «b».

Вставить из буфера:

p - вставить в текущую позицию содержимое неименованного буфера;

"ap - вставить в текущую позицию содержимое именованного буфера «a»;

"1p - вставить в текущую позицию содержимое буфера стирания «1».

Многооконное редактирование

Редактировать сразу несколько файлов можно либо пользуясь командной редактора :e <имя_файла>, либо указав все необходимые файлы в командной строке при вызове редактора (например: vi <файл_1> <файл_2> <файл_3>). В последнем случае вы двигаетесь по списку файлов с помощью команд:
:n - переходим к следующему файлу в списке;
:rew - возвращаемся к редактированию первого файла в списке.
Именованные буферы сохраняют свое содержимое при переходе к редактированию другого файла.

Открыть/создать файл

vi mamapapa.txt - открыть один файл.

vi mama.txt papa.txt - открыть файл mama.txt, после выхода из него открыть файл papa.txt.

Файл открывается в командном режиме с помощью команды vi. Здесь мы можем просмотреть файл, переместиться по его содержимому, стереть текст, но внести изменения или ввести текст в этом режиме нельзя.

Создание файла происходит при помощи той же команды. Создание файла происходит в момент сохранения.

Для открытия или создания нового файла в командном режиме необходимо выполнить команду:

:e <имя_файла>

Перед этим нужно сохранить предыдущий файл:

:w - сохраняет файл с существующим именем;
:sav <имя_файла> - «Сохранить как».

Дополнительные опции

Дополнительные возможности редактора:

Команда	Описание команды
G	перейти в конец файла
<number>G	перейти на конкретную строку <number>
:<number>	перейти на <number> строк вперед
:set nu[mber]	отобразить слева нумерацию строк (^ nonu[mber] - спрятать нумерацию)
:set wrap	переносить длинные строки (:set nowrap - не переносить)
:syntax on/off	включить/выключить подсветку синтаксиса
:colorscheme <name>	задать цветовую тему (где <name> - имя темы, TAB работает как авто-дополнение)
/мама	поиск текста "мама" в файле
n	повторить поиск
:h или :help	список возможной помощи (:viusage, :exusage)
:set fileformat=dos :set fileformat=unix	привести концы строк в файле к виду dos или unix, соответственно
:set ts=4	задать размер табуляции в 4 пробела

Улучшенный редактор VIM

Vim расшифровывается как Vi Improved, улучшенный vi. В сравнении с классическим vi Vim отличается следующими улучшениями:

- Работа со многими файлами одновременно. Разбиение окон редактирования может производиться многократно как по горизонтали, так и по вертикали.
- Поддержка Unicode.
- Поддержка визуального режима, который позволяет, например, выполнять операции над блоками текста.
- Неограниченная глубина отмены (undo) и возврата (redo) действий.
- Режим сравнения двух файлов, перенос отдельных изменений из одного файла в другой.
- Широкая файловая поддержка (файл со справкой и более 200 файлов с описанием синтаксиса).
- Подсветка синтаксиса, автоматическое определение величины отступа для каждой строки в зависимости от языка программирования (изначально поддерживает более 200 языков программирования и форматов конфигурационных файлов).
- Интеграция с операционной системой, дающая возможности, близкие к интегрированным средам разработки, такие как поиск ошибки по сообщению компилятора, автодополнение идентификаторов и др.
- Поддержка языка сценариев; возможность написания модулей расширения — плагинов.
- Автоматическое продолжение команд, слов, строк целиком и имён файлов.
- Автоматический вызов внешних команд (например, автоматическая распаковка файла перед редактированием).
- Распознавание и преобразование файлов различных форматов.
- Удобный механизм истории команд, поисковых слов и т. д.
- Запись и исполнение макросов.
- Возможность сохранения настроек и сеанса.
- Возможна интеграция с языками программирования Perl, Tcl, Python и Ruby.
- Поддержка языков с письмом справа налево (арабских и других).
- Сворачивание (folding) текста для лучшего обзора.
- Возможно использование графического интерфейса в специальных версиях (GTK, Motif, ...).
- Хорошо конфигурируется и настраивается под нужды пользователя.
- Для программистов: поддержка цикла разработки «редактирование — компиляция — исправление» программ. Автоматическое выполнение сборки/компиляции, обнаружение и распознавание ошибок, переход к строкам ошибок в тексте программы.

Режимы работы

В **ViM** существуют *3 режима* работы:

Основной - предназначен для просмотра файла, ввода команд и перехода из него в другие режимы. Из любого режима в командный можно попасть по нажатии «**ESC**». При нажатии клавиши «**:**» становится доступна командная строка ViM, в которой можно вводить команды. Основные команды - команда выхода **quit** (ViM понимает сокращения, поэтому можно давать команду одной буквой «q»), команда сохранения **write** (или «w»), параметром которой может быть имя файла и вызов справки по, очевидно, **help** (или «h»). На остальные клавиши (и их последовательности) можно присвоить любое действие, либо использовать значения по умолчанию.

Визуальный – предназначен, в первую очередь, для выделения блоков текста. Для запоминания предлагаются 3 варианта перехода в этот режим – клавишей «**v**» для посимвольного выбора, «**Shift+v**» для построчного и «**Ctrl+v**» для блочного. В нормальном режиме (при переходе по «v») можно оперировать следующими сущностями: слово («w»), предложение («s»), параграф («p») и блок («b»). Выделение при этом начинать с позиции курсора («a»), или же с начала блока («i»). Например, выделение текущего блока (участка,

ограниченного парными элементами) можно произвести следующим образом «**Esc+vib**». Копирование в буфер выделенного текста осуществляется по «y», вырезание по «d», а вставка соответственно «p».

Режим редактирования - переход в режим редактирования осуществляется нажатием клавиши «**Ins**».

Основные возможности

Все возможности и команды редактора ViM перечислить весьма затруднительно (HTML-документация по нему занимает около пяти мегабайт), но на группе наиболее полезных остановиться необходимо. Перечисленные ниже команды вводятся в основном режиме (если нет специального уточнения). Все они имеют команднострочные аналоги и могут быть легко переопределены пользователями.

Переходы

Для перехода на строку с номером *n* воспользуйтесь командой *G*. Так, для перехода к началу текста наберите 0G, для сотой строки 100G, а для конца документа - $G. Для перехода на n символов в нужную вам сторону можете использовать клавиши со стрелками. То есть для перехода на 1000 символов вниз наберите 1000 и нажмите стрелку вниз.

Для перемещения по тексту используйте следующие команды: «(», «)» для перемещения по предложениям, «{», «}» для параграфов, «[[», «]]» для функций, «%» - переход к парной скобке, «' '» - к предыдущему положению, а «CTRL+O», «CTRL+I» - соответственно назад и вперед по истории переходов.

Метки

Используются для отметки позиции ^метка, где меткой является любая буква и быстрого к ней перехода (метка). Метки нижнего регистра действительны в пределах данного файла, метки же верхнего регистра действуют во всех открытых файлах. Список всех меток можно получить командой **marks**.

Регистры

В редакторе доступно множество именованных регистров (хранилищ данных, буферов). Регистр отмечается «' 'буква». К нему применимы все стандартные действия - копирование в него ("меткау), вырезание ("метка^), и вставка из него (' 'меткар, можете вместо p использовать [p,]p для вставки соответственно перед, или после курсора). В режиме редактирования вставка из регистра осуществляется по «Ctrl+R метка». Для добавления данных в регистр используйте заглавную метку.

Также вы можете писать в регистр, воспользовавшись командой «^метка» и завершая запись по «q». Таким образом, вы сохраняете макрос, выполнить который можно по «@метка».

Регистры с метками «*» и «+» совпадают с X-Window clipboards, «%» - соответствует редактируемому файлу. Для просмотра содержимого всех регистров воспользуйтесь командой **:registers**, либо **:reg <метка_1><метка_2>...** для просмотра некоторых.

Фолды

Предназначены для сокрытия не нужных в данный момент данных, чтобы те не отвлекали внимания. Например, кода подпрограммы, с которой вы в данный момент не работаете. По умолчанию фолды активированы в режиме их ручной расстановки. Если вы хотите их автоактивации по отношению к табуляции, то добавьте в конфигурационный файл строку:

```
set foldmethod=indent
```

Все команды для работы с фолдами начинаются с «z». Открытие фолда производится, например, по **zo** (или стрелке вправо) на нем, закрытие кода в фолд - по **zc**.

Сессии

При ведении группы проектов нередко желательно сохранить текущее состояние и настройки редактора, чтобы в дальнейшем продолжить работу с того же места. Для этого и предназначены сессии, что создаются командой **:mksession /path/to/Session.vim**, а читаются простой командой **:so /path/to/Session.vim**. Гораздо чаще, впрочем, возникает нужда в сохранении не всей сессии, но только текущего контекста (во что входит, например, положение курсора в коде, текущая расстановка фолдов и многое другое, о чем читайте в документации). Это действие выполняет команда **:mkview**, чтение - **:loadview**. Очень удобно сделать сохранение и чтение контекста автоматическим при начале и окончании редактирования файла. Это может быть реализовано следующим кодом (применяется для всех файлов, имеющих точку в имени):

```
au BufWinLeave *.* mkview au BufWinEnter *.* silent loadview
```

Поиск и замена

Поиск осуществляется командами «/» для поиска (по регулярному выражению) вперед, а «?» в обратном направлении. Для продолжения поиска используйте «n», а для прошлого варианта «N». Для поиска слова под курсором используются соответственно «#» и «*».

Для поиска с заменой используйте **^s^TO/m что/gic**, где «%» означает работу со всем текстом (а не с текущей строкой), «g» - глобальная замена (а не первое совпадение), «i» - игнорирование регистра, а «c» - подтверждение каждого действия.

Автодополнение

Производится по содержимому данного файла, а также указанных в переменной **dictionary** по нажатию клавиш ' '.

Отмена

«u» для отмены и ' ' смена регистра.

«~» для выделенного участка (или буквы под курсором). «U» - принудительно установить верхний регистр, а «u», соответственно, нижний.

Повторить

«.»

Конфигурация

Основным конфигурационным файлом является **~/.vimrc**. Активация русского шрифта в GUI-режиме плюс выбор темы для обоих режимов осуществляется, например, следующим кодом:

```
if has("gui_running")
colorscheme candy
set guifont=-cronyx-courier-medium-r-normal-*-*-120-*-*-m-*-koi8-r endif
if !has("gui_running") colorscheme elflord endif
```

Перечень наиболее используемых «горячих» клавиш:

Выход по **F10**:

```
nmap <F10> :q<CR>
imap <F10> <ESC>:q<CR>
```

Сохранение по **F2**:

```
nmap <F2> :w<CR>
imap <F2> <ESC>:w<CR>i<Right>
```

Компиляция по **F9**:

```
nmap <F9> :make<CR>
imap <F9> <ESC>:make<CR>
```

Текстовые редакторы в РЕД ОС

GNU Emacs
nano
pluma

GNU Emacs

Emacs — один из наиболее мощных и широко распространённых редакторов, является очень популярным консольным текстовым редактором.

Для использования **Emacs** понадобится изучить набор команд и горячих клавиш, а также настроить редактор под себя. **Emacs** имеет встроенный язык программирования, который может использоваться для настройки, расширения и изменения поведения редактора. Функции написаны на языке **Elisp**. Синтаксис **Lisp** довольно сложен для новичков, но новичкам и не обязательно писать свои расширения, по умолчанию в редакторе есть почти всё необходимое.

Для установки редактора перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install emacs
```

Вместе с консольной версией установится и графическая оболочка, поэтому для запуска именно консольной версии необходимо использовать параметр **–nw**.

Для новичков **Emacs** имеет большой недостаток - он не русифицирован и имеет только английскую версию интерфейса.

Emacs является очень мощным редактором с огромным количеством дополнительных возможностей. Его можно использовать как:

- текстовый редактор;
- программу для чтения почты и новостей **Usenet**;
- интегрированную среду разработки (**IDE**);
- операционную систему;
- написать свой скрипт и использовать для любых функций.

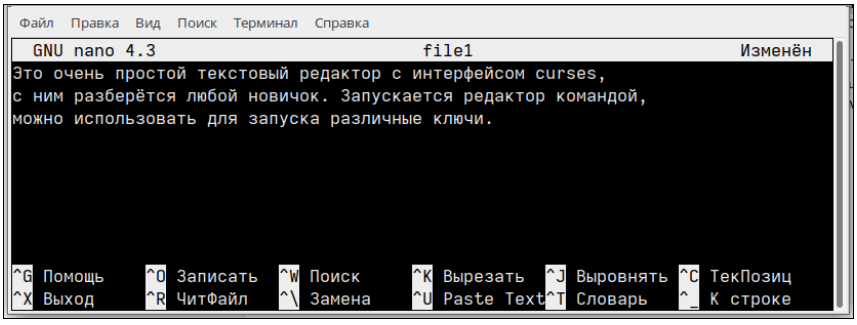
nano

nano - очень простой текстовый редактор с интерфейсом **curses**, с ним разберётся любой новичок. Редактор предустановлен в РЕД ОС по умолчанию.

Запускается редактор командой (можно использовать для запуска различные ключи):

```
nano <ключи>
```

Чтобы открыть какой-либо файл, достаточно передать его в параметрах команде **nano**. Если указанного файла не существует, будет создан новый.



Главное окно программы выглядит интуитивно понятно - в верхней строке находится версия редактора и имя файла, а также уведомление был ли файл изменен. Затем идет текстовое поле, а внизу - имя файла и основные сочетания клавиш, которые вы можете использовать для работы с программой. Например, для выхода из редактора используется сочетание «**CTRL+X**».

pluma

Pluma (**pluma**) - это небольшой и легкий текстовый редактор, разработанный специально для рабочего стола **MATE**. **Pluma** использует интерфейс со вкладками, который позволяет редактировать более одного документа одновременно.

Pluma поддерживает большинство стандартных функций редактирования. За счёт подключаемых плагинов можно увеличивать возможности программы. Новые функции постоянно находятся в стадии разработки, в настоящее время в **Pluma** есть:

- подсветка синтаксиса;
- проверка орфографии;
- браузер файлов;
- сортировка;
- вставка даты / времени;
- поиск и замена;
- поддержка печати и предварительного просмотра и др.

Он имеет большинство стандартных функций текстового редактора и полностью поддерживает международный текст в Юникоде. Расширенные функции включают подсветку синтаксиса и применение автоматического отступа исходного кода, печать и редактирование нескольких документов в одном окне. **Pluma** расширяется с помощью системы плагинов, которая в настоящее время включает поддержку проверки орфографии, сравнения файлов, просмотра списков изменений **VCS** и настройки уровней отступов.

WPS Office

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** WPS-Office - 11.1.0.11664

WPS Office — офисный пакет, созданный китайским разработчиком программного обеспечения **Kingsoft**, как альтернатива **Microsoft Office**.

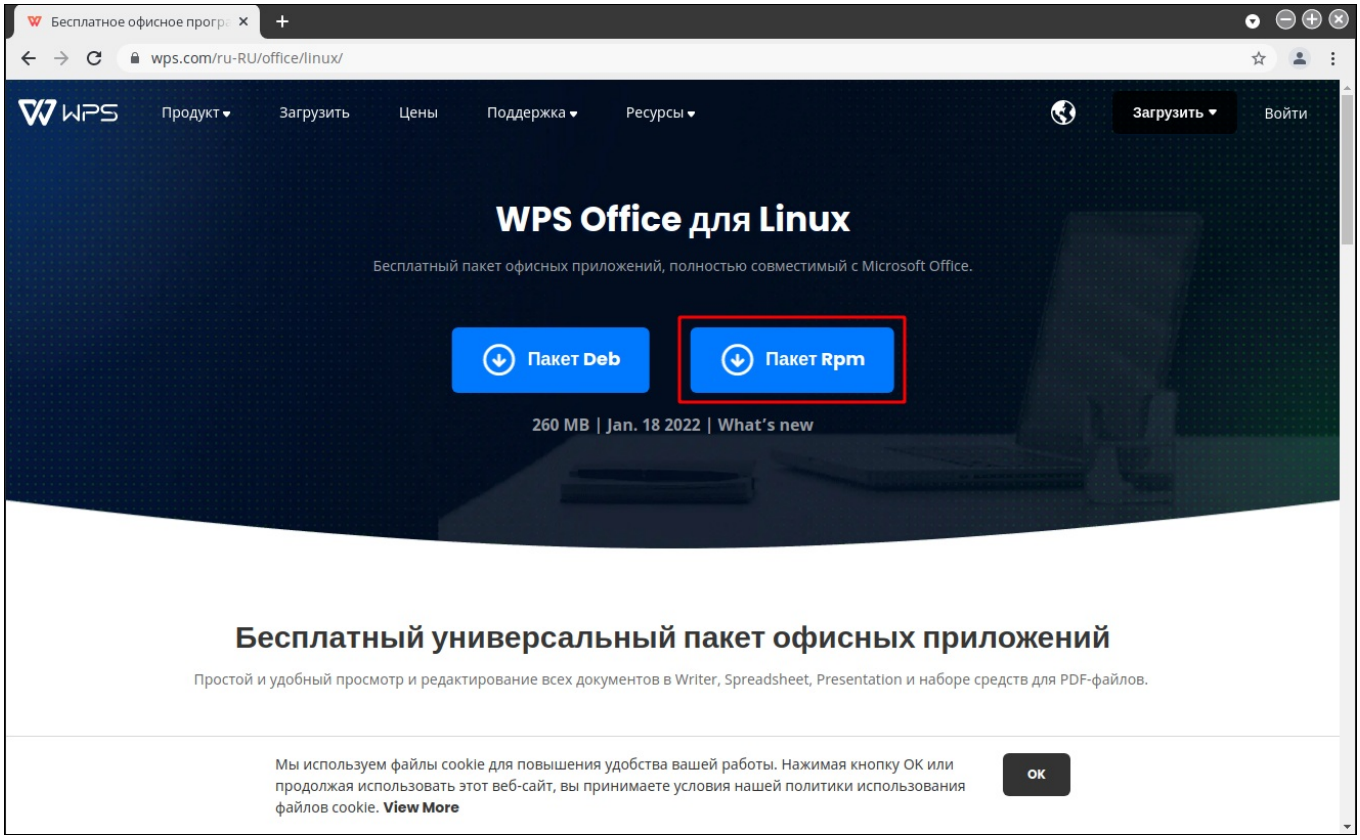
Пакет состоит из текстового процессора **WPS Writer**, программы создания презентаций **WPS Presentation** и табличного процессора **WPS Spreadsheets**.

Основные характеристики:

- Поддержка форматов **DOCX**, **XLSX**;
- Встроенная панель **Google Search**;
- Переключение по вкладкам;
- Экспорт в PDF-файл (также существуют дополнительные инструменты распознавания текстов из изображений и PDF);
- Шифрование перед сохранением;
- Подготовка на печать несколько новых документов;
- Поддержка **OLE Automation** (технология связывания и внедрения объектов в другие документы и объекты).

Установка

Для установки **WPS Office** необходимо скачать rpm-пакет с официального сайта разработчика.



После загрузки файла в консоли выполните следующие действия:

1. Перейдите в сеанс пользователя **root**:

```
su -
```

2. Перейдите в папку с дистрибутивом (в качестве примера /home/user/Загрузки/:

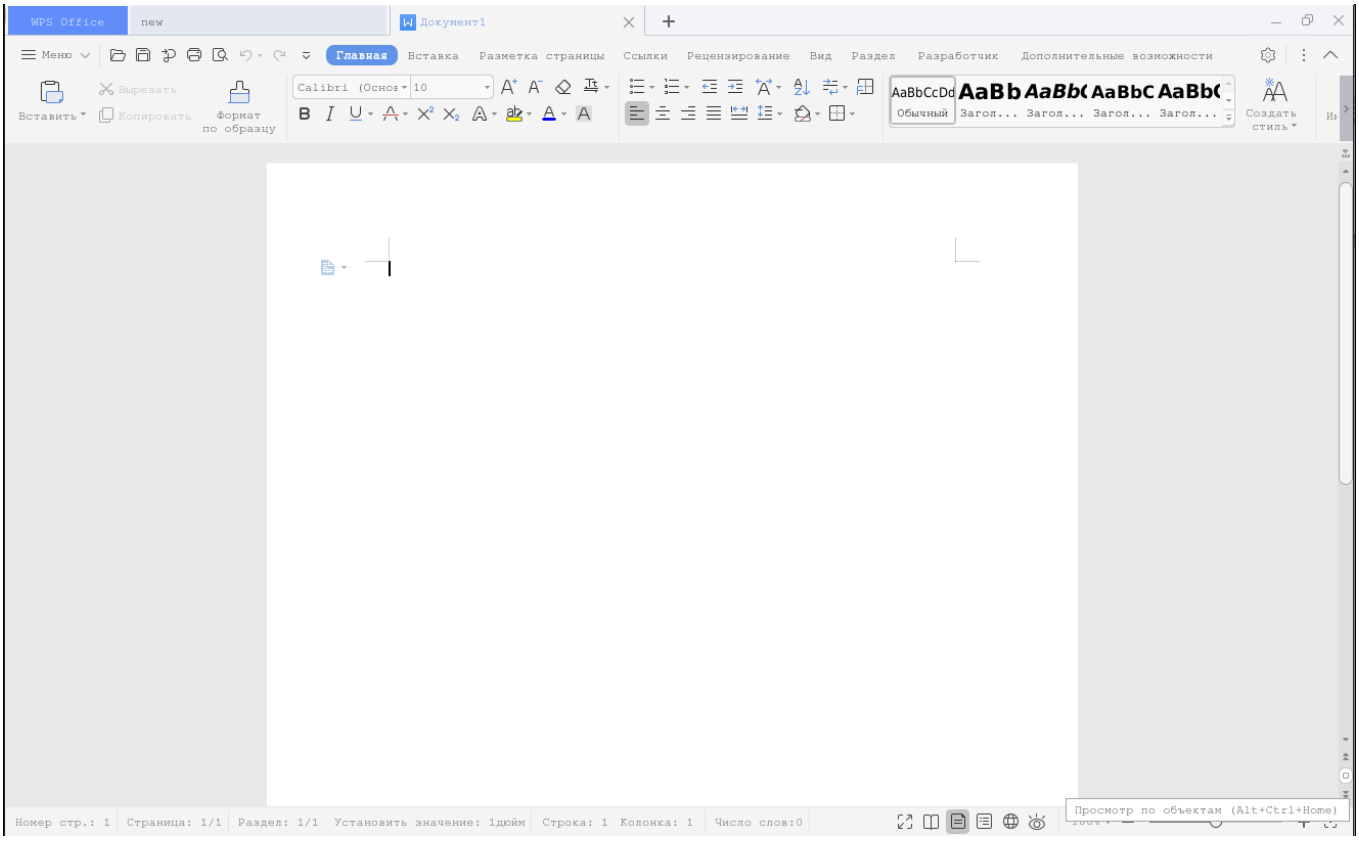
```
cd /home/user/Загрузки/
```

3. Установите **WPS Office**:

```
dnf install wps-office-11.1.0.10920.XA-1.x86_64.rpm
```

После установки компоненты **WPS Office** будут доступны в «**Главном меню**» - «**Офис**» или выполните команду от локального пользователя:

```
wps
```



OnlyOffice

Установка rpm-пакета с официального сайта
Добавление репозитория OnlyOffice

Окружение:

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** OnlyOffice - 7.2.1

OnlyOffice - это бесплатный офисный пакет для работы с текстовыми документами, электронными таблицами и презентациями без подключения к интернету.

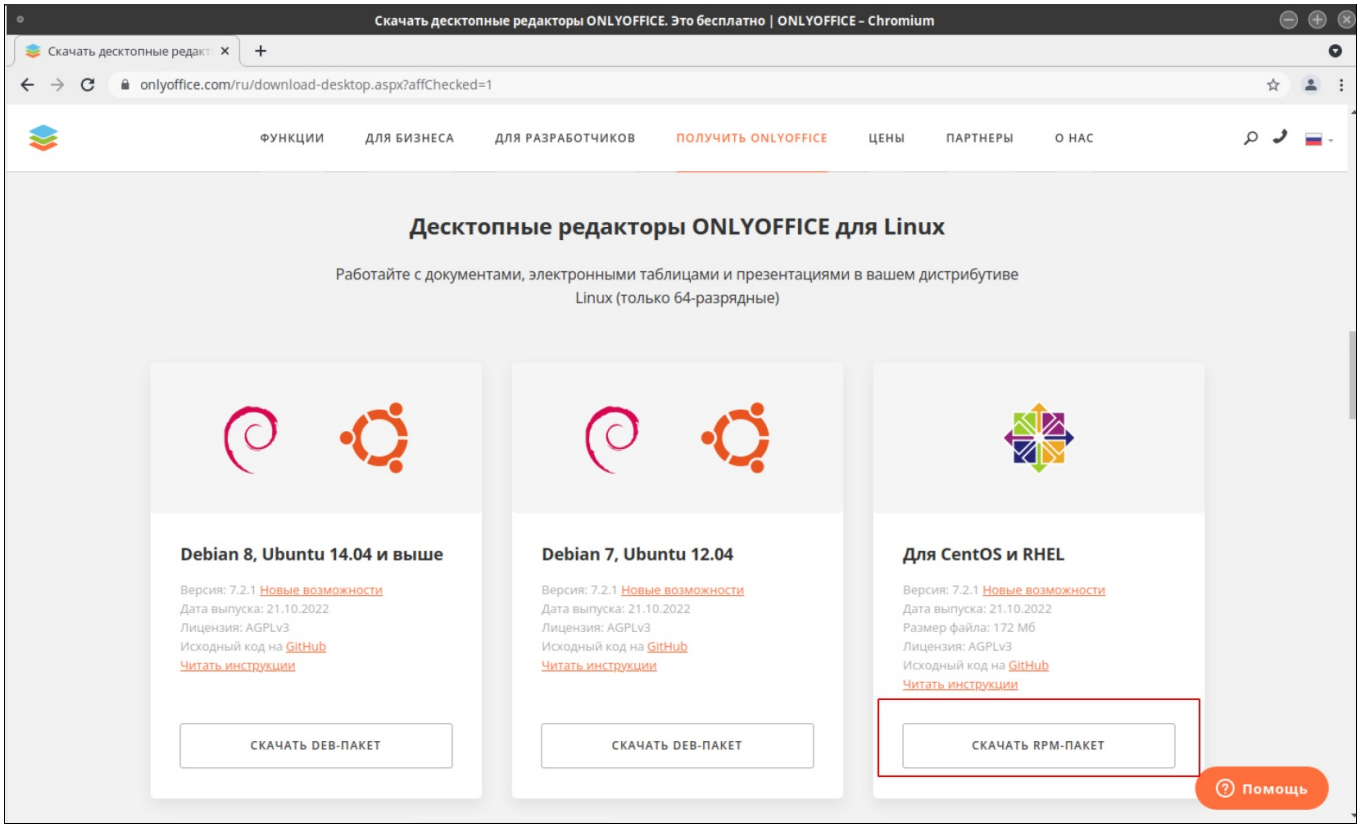
Приложение подключается к облачным и серверным версиям **OnlyOffice**, позволяя тем самым совместно редактировать документы в режиме реального времени.

Редакторы **OnlyOffice** полностью совместимы с **MS Office** и **OpenDocument** и поддерживают популярные форматы:

- DOC, DOCX, ODT, RTF, TXT;
- PDF;
- HTML;
- EPUB;
- XPS;
- DjVu;
- XLS, XLSX, ODS, CSV;
- PPT, PPTX, ODP.

Установка rpm-пакета с официального сайта

Для установки **OnlyOffice** необходимо скачать **rpm-пакет** с официального сайта разработчика.



После загрузки файла в консоли выполните следующие действия:

1. Перейдите в сеанс пользователя **root**:

```
su -
```

2. Перейдите в папку «**Загрузки**»:

```
cd /home/user/Загрузки/
```

3. Установите **OnlyOffice**:

```
dnf install onlyoffice-desktopeditors.x86_64.rpm
```

После установки программа будет доступна в «**Главном меню**» - «**Офис**» - «**ONLYOFFICE Desktop Editors**».

Добавление репозитория OnlyOffice

Для удобства работы и легкости обновления в будущем репозиторий **OnlyOffice** можно добавить непосредственно в ОС. Для этого необходимо:

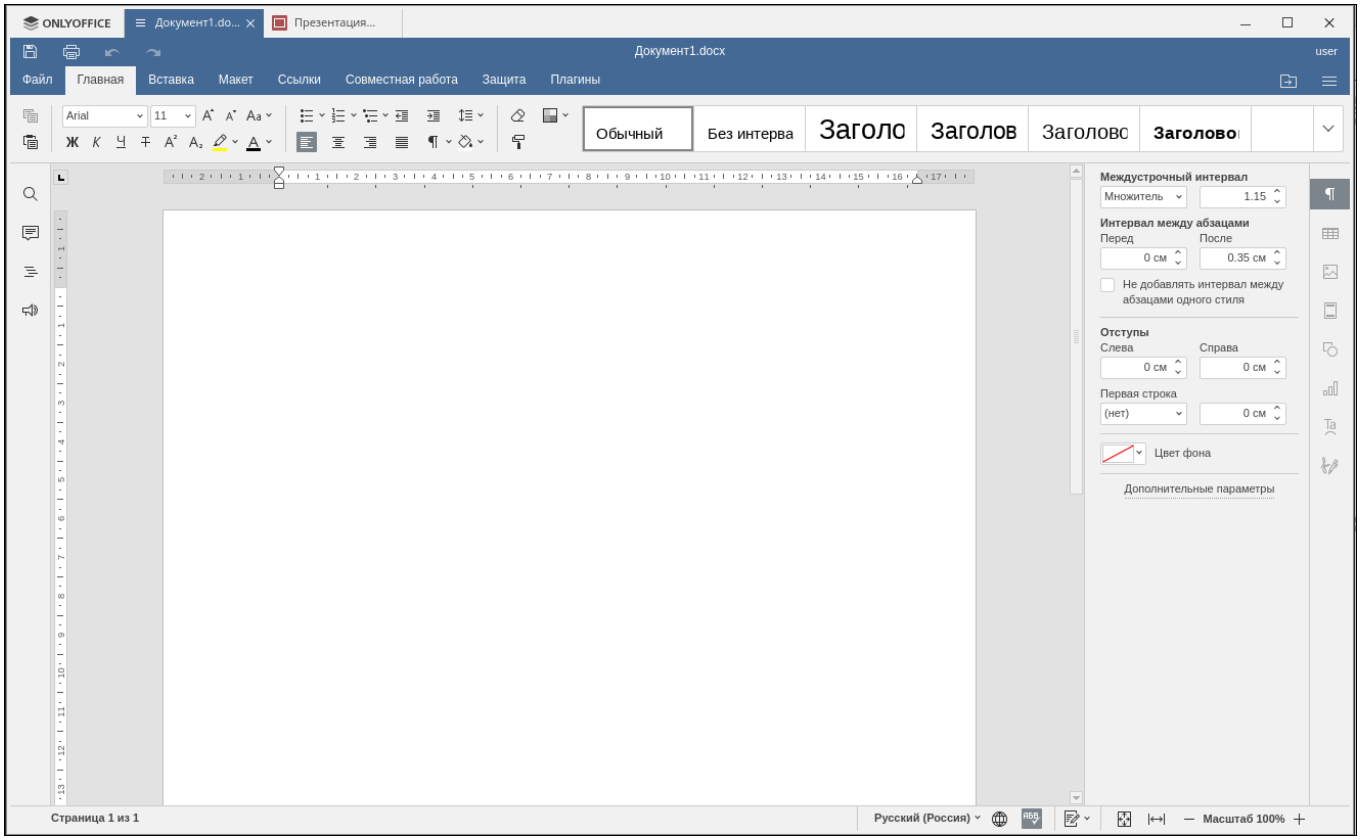
1. Добавить репозиторий командой **от пользователя root:**

```
dnf install https://download.onlyoffice.com/repo/centos/main/noarch/onlyoffice-repo.noarch.rpm
```

2. Провести стандартную установку пакета **от пользователя root:**

```
dnf install onlyoffice-desktopeditors
```

Для запуска перейдите в «**Главное меню**» - «**Офис**» - «**ONLYOFFICE Desktop Editors**»



МойОфис

Установка
Настройка панели Образование

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: МойОфис 2022.01-1.28.0.4

«**МойОфис Образование**» – это комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями.

«**МойОфис Текст**» обеспечивает удобное и быстрое создание документов с использованием шаблонов, стилей и средств форматирования текста. Функции совместного редактирования обеспечивают эффективную совместную работу сотрудников.

«**МойОфис Таблица**» – это приложение для быстрой и удобной работы с электронными таблицами и анализа данных. Продукт поддерживает расширенный набор формул и средств для обработки данных. Совместное редактирование на любой из поддерживаемых платформ обеспечивает быстрый анализ и подготовку документов группой сотрудников даже вне офиса.,

«**МойОфис Презентация**» – приложение с полным набором инструментов для просмотра графических презентаций.

Установка

Для установки «**МойОфис**» необходимо скачать пакет в формате **.rpm** с официального сайта разработчика.

После загрузки файла в консоли перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install /home/user/Загрузки/myoffice-standard-home-edition-2022.01-1.28.0.4.x86_64.rpm
```

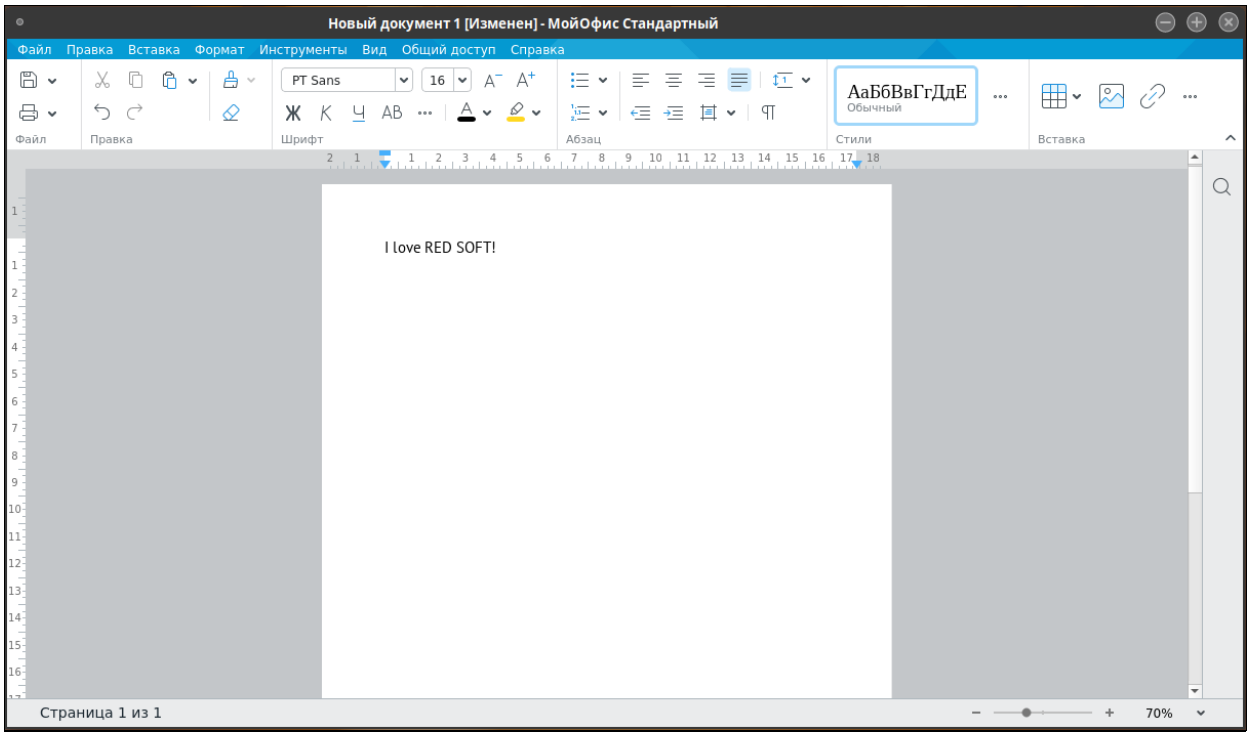
После установки редакторы будут доступны в «**Главном меню**» - «**Офис**» - «**МойОфис**».

При первом запуске потребуется принять лицензионное соглашение.



Нажмите «**Принять**».

После этого «**МойОфис**» готов к работе.



Настройка панели Образование

Для изменения данных на панели *Образование* перейдите в сеанс пользователя **root**:

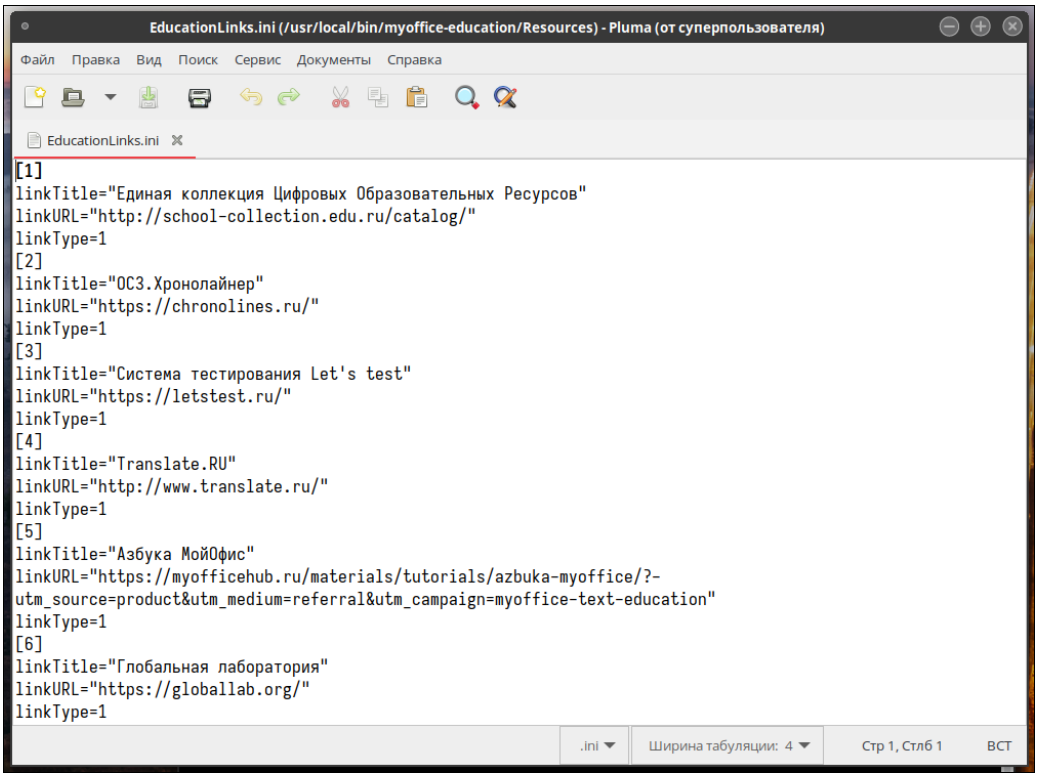
```
su -
```

и внесите изменения в следующий файл:

```
nano /usr/local/bin/myoffice-education/Resources/EducationLinks.ini
```

Изменения вносятся в список ресурсов, где:

- **[номер секции]** – порядок следования ссылки в панели *Образование*;
- **linkTitle** – заголовок ссылки (то, что отображается на панели *Образование*);
- **linkURL** – ссылка на ресурс;
- **linkType** – тип иконки, расположенный слева от ссылки:
  - 0 – дневник;
  - 1 – указатель ссылки.



Пример:

```
[7]
linkTitle="Библиотека"
linkURL="https://uchebnik.mos.ru/"
linkType=0

[8]
linkTitle="Электронный дневник"
linkURL="https://schools.school.mosreg.ru"
linkType=0
```

Сохраните изменения, нажав **Ctrl+O**, затем **Enter** и **Ctrl+X**.

Перезапустите редактор текста или таблицы – панель *Образование* будет обновлена.

Р7-Офис

Установка Р7-Офис. Редакторы документов
Технические требования
Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora
Активация лицензии

Установка Р7-Офис. Органайзер
Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora

Установка Р7-Графика
Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora
Активация лицензии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: r7-release-1.0-1, r7-office-2024.1.1-373, r7organizer-2.0.1-1, R7Grafika-1.6.21751004-1

Установка Р7-Офис. Редакторы документов

Р7-Офис – это российский офисный пакет включающий в себя профессиональные редакторы документов, таблиц и презентаций.

Десктопные редакторы **Р7-Офис** позволяют работать с документами во всех популярных форматах самостоятельно или совместно с другими людьми с помощью широких функций совместной работы.

Текстовый редактор **Р7-Офис** поддерживает открытие и сохранение документов в таких популярных форматах, как **ODT**, **DOCX**, **PDF** и многих других. Обладает широкими возможностями по форматированию и вставке текста, таблиц, картинок и колонтитулов.

Табличный редактор **Р7-Офис** поддерживает открытие и сохранение табличных документов в таких популярных форматах, как **XLS**, **XLSX**, **ODS** и других. Обладает широкими возможностями по созданию, редактированию таблиц, вставке данных, созданию формул и построению графиков. В редакторе имеется большое количество встроенных функций и формул: финансовые, математические, поисковые и прочие для реализации разных целей и задач.

Редактор презентаций **Р7-Офис** – это профессиональный инструмент для создания презентаций. С его помощью можно создавать яркие демонстрационные материалы в таких популярных форматах, как **PPTX**, **PPT**, **ODP** и других. Удобная настройка показа слайдов и коллекция готовых переходов позволяет создавать современные интерактивные презентации.

Офисный пакет **Р7-Офис** для РЕД ОС размещается в отдельном подключаемом (с помощью пакета **r7-release**) репозитории. **Р7-Офис** в данном репозитории был собран специально для работы в РЕД ОС и использует необходимые зависимости из репозитория РЕД ОС.

Вы можете подробнее ознакомиться с работой офисных пакетов **Р7-Офис** и **Р7-Органайзер**, просмотрев наши обучающие видео:

- на **RuTube** — Р7-Офис и РЕД ОС;
- в **Яндекс.Дзен** — Р7-Офис и РЕД ОС;
- в **VK Видео** — Р7-Офис и РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

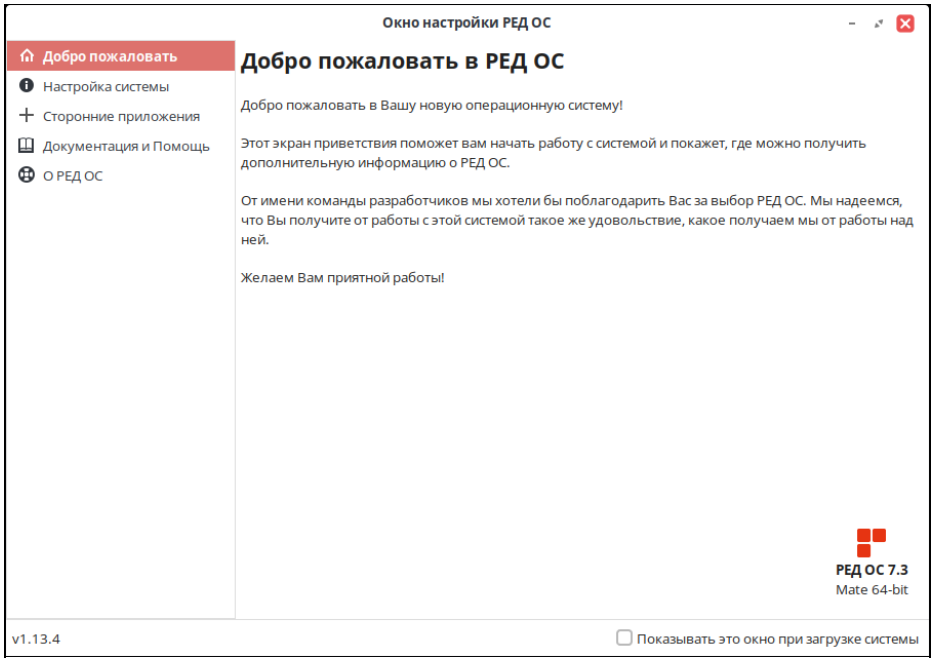
Технические требования

Для корректной работы программного обеспечения используемое оборудование должно выполнять следующие технические требования:

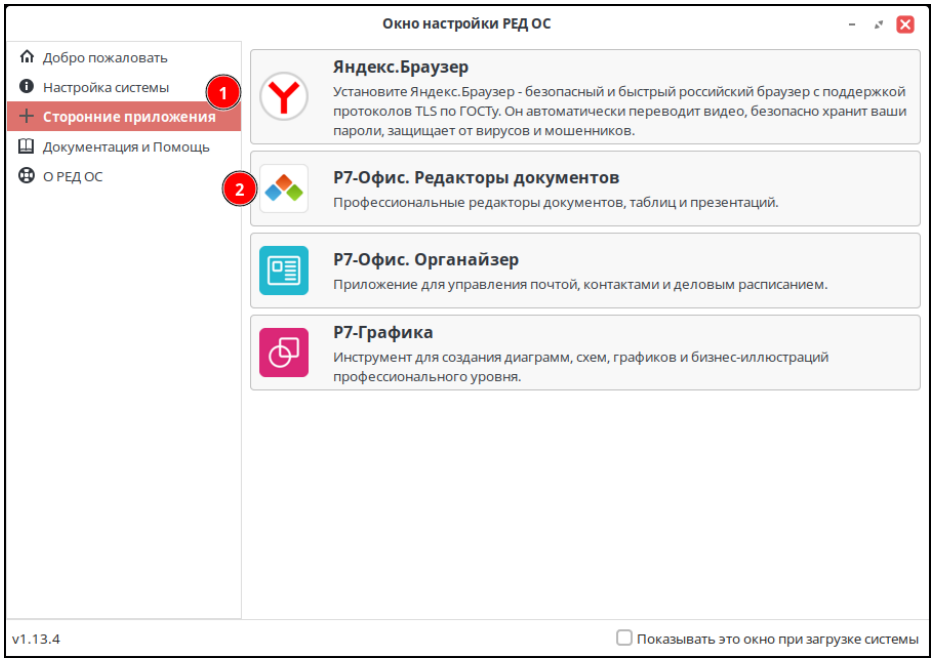
- двухъядерный процессор **2 ГГц и выше**;
- оперативная память **не менее 2 Гб**;
- свободное дисковое пространство **не менее 2 Гб**.

Установка через «Окно настройки РЕД ОС»

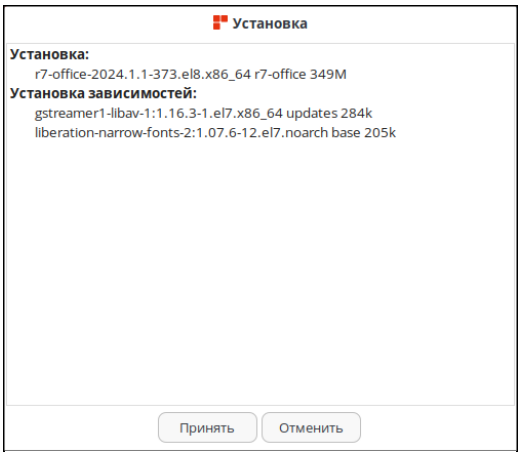
Откройте утилиту «Окно настройки РЕД ОС».



Перейдите на вкладку «**Сторонние приложения**», затем выберите из списка «**Р7-Офис. Редакторы документов**».



Далее в появившемся окне «**Установка**» ознакомьтесь со списком устанавливаемых пакетов и зависимостей и нажмите «**Принять**». Начнётся установка офисных пакетов **Р7-Офис**.



После установки редакторы будут доступны из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Профессиональный (десктопная версия)**».

Установка через терминал

Перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду подключения репозитория и установки офисного пакета:

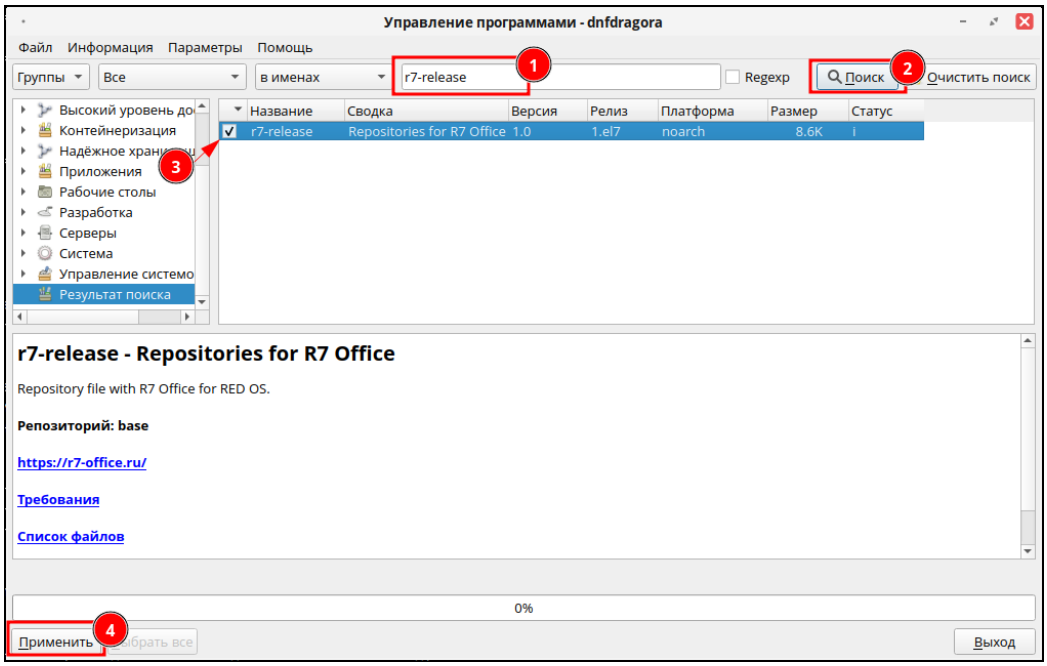
```
dnf install r7-release && dnf install r7-office
```

После установки редакторы будут доступны из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Профессиональный (десктопная версия)**».

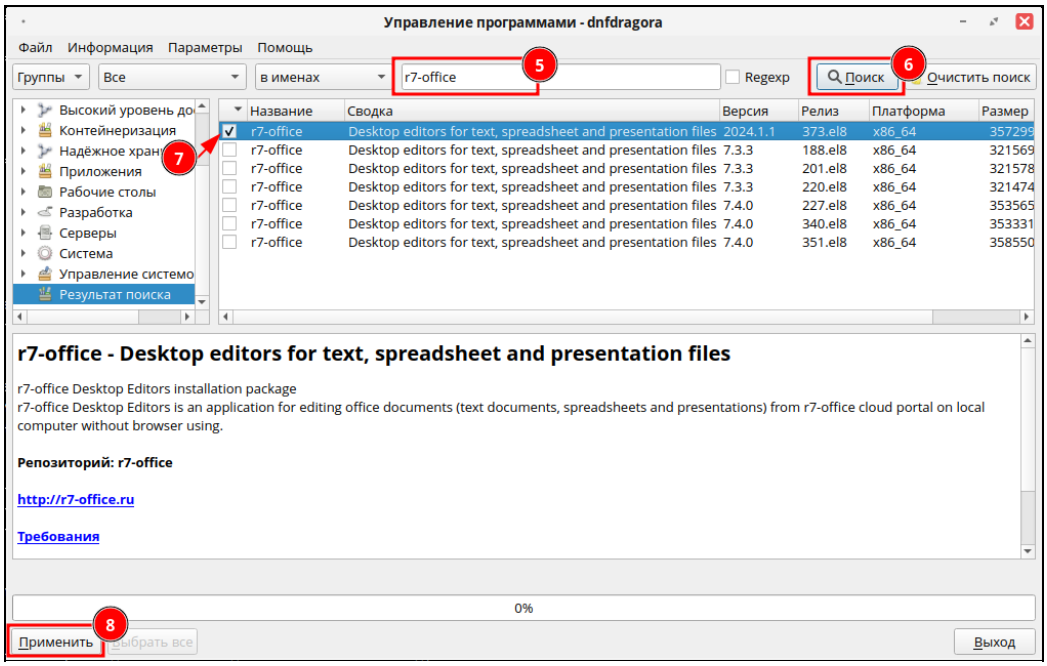
Установка через dnfdragora

Для установки **Р7-Офис** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» – «**Администрирование**» – «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**r7-release**».

В результате поиска будет предложен к установке подключаемый репозиторий **r7-release**. Отметьте флагом репозиторий последней версии, нажмите кнопку «**Применить**» и дождитесь окончания установки.



После установки репозитория в строке поиска необходимо ввести название пакета непосредственно самого офиса – **r7-office**. Затем отметьте флагом пакет последней версии и нажмите кнопку «**Применить**» для его установки.



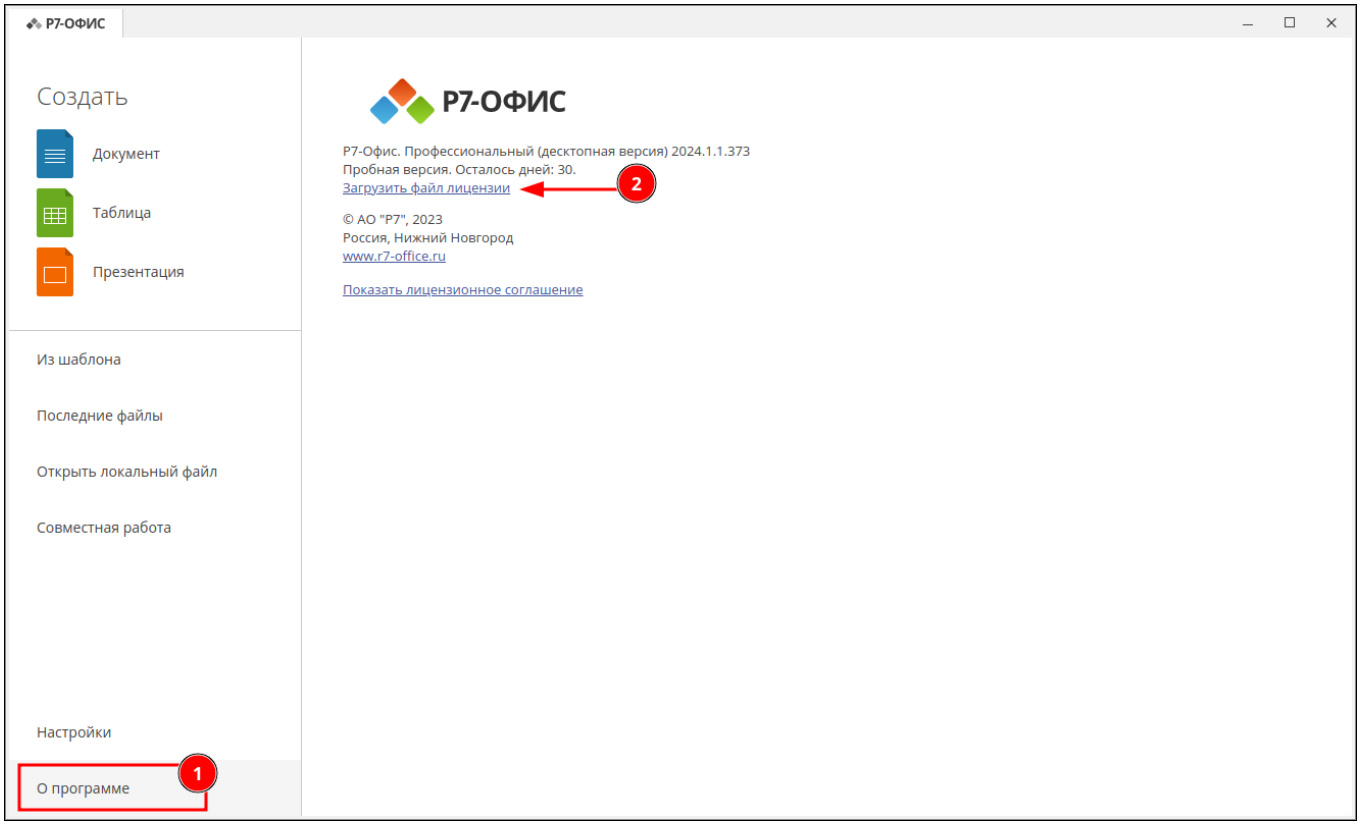
После установки редакторы будут доступны из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Профессиональный (десктопная версия)**».

Активация лицензии

Офисный пакет **Р7-Офис** предоставляет 30-дневный бесплатный пробный период на рассмотрение и изучение функций редакторов.

По истечении бесплатного пробного периода необходимо запросить у официального разработчика соответствующую лицензию.

Для этого в основном меню программы перейдите во вкладку «**О программе**» – «**Загрузить файл лицензии**» и укажите путь к загруженному файлу лицензии в формате **.lickey**.



Установка Р7-Офис. Органайзер

Р7-Офис. Органайзер – это приложение для управления почтой, контактами и деловым расписанием. Включает в себя почтовый клиент с интуитивно понятным интерфейсом, надежной защитой от спама и удобным редактором писем с автоматической проверкой

орфографии.

Фильтры, тэги и папки для сортировки писем позволяют организовать входящую почту. Также возможно подключить несколько аккаунтов.

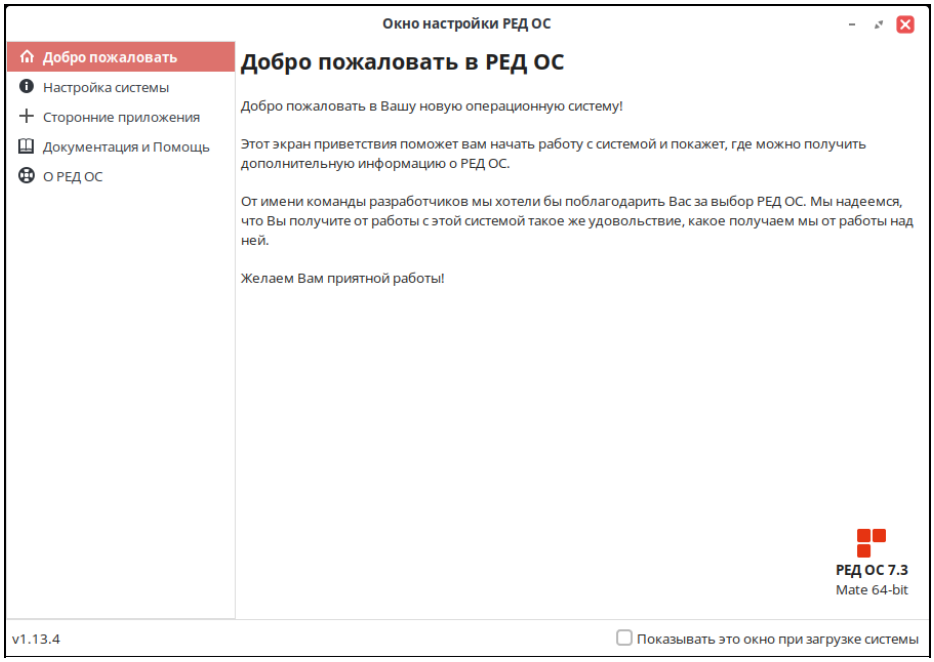
Личные и рабочие контакты хранятся в адресной книге и синхронизированы с почтой и календарем. В адресной книге доступно создание списков рассылки и ведение подробных карточек контактов.

Календарь с расписанием и списком дел – на день, неделю или месяц, напомнит о событиях и задачах.

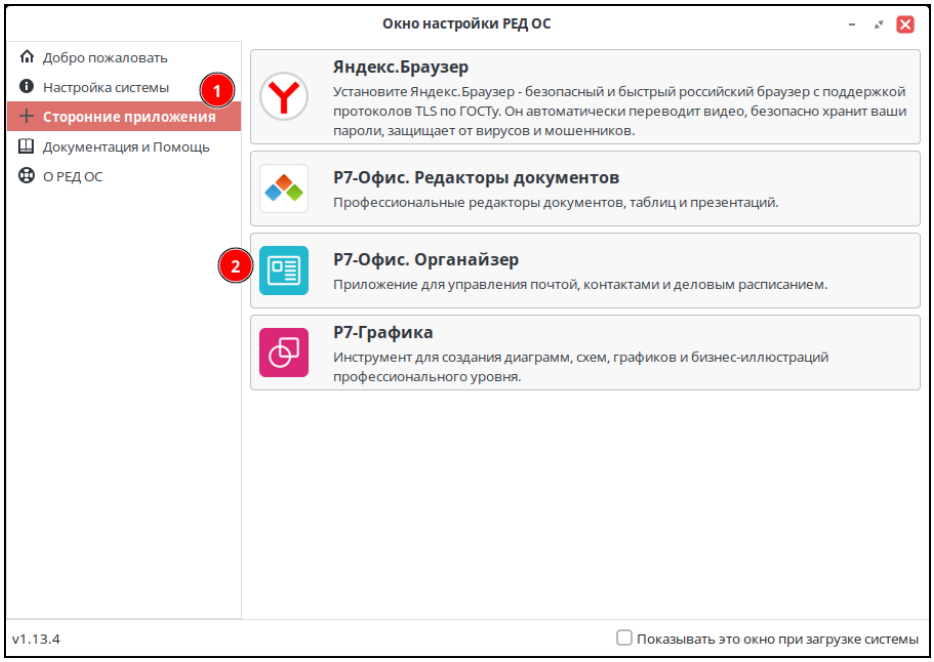
Доступна возможность создания нескольких календарей под разные группы событий и предоставления доступа коллегам. Общие календари позволяют выбрать удобное время для собрания и сделать рассылку приглашений.

Установка через «Окно настройки РЕД ОС»

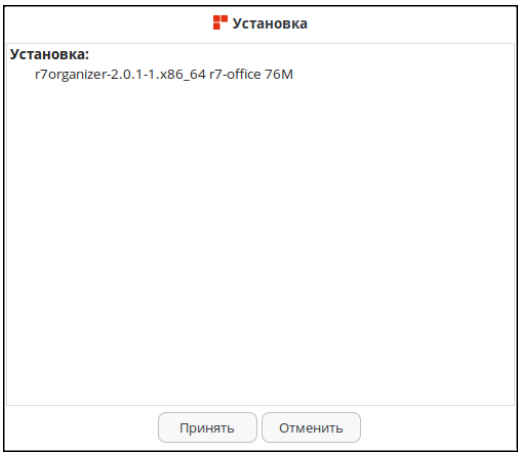
Откройте утилиту «Окно настройки РЕД ОС».



Перейдите на вкладку «**Сторонние приложения**», затем выберите из списка «**Р7-Офис. Органайзер**».



Далее в появившемся окне «**Установка**» ознакомьтесь со списком устанавливаемых пакетов и нажмите «**Принять**». Начнётся установка пакета **Р7-Офис. Органайзер**.



После установки органайзер будет доступен из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Органайзер**».

Установка через терминал

Перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду подключения репозитория и установки органайзера:

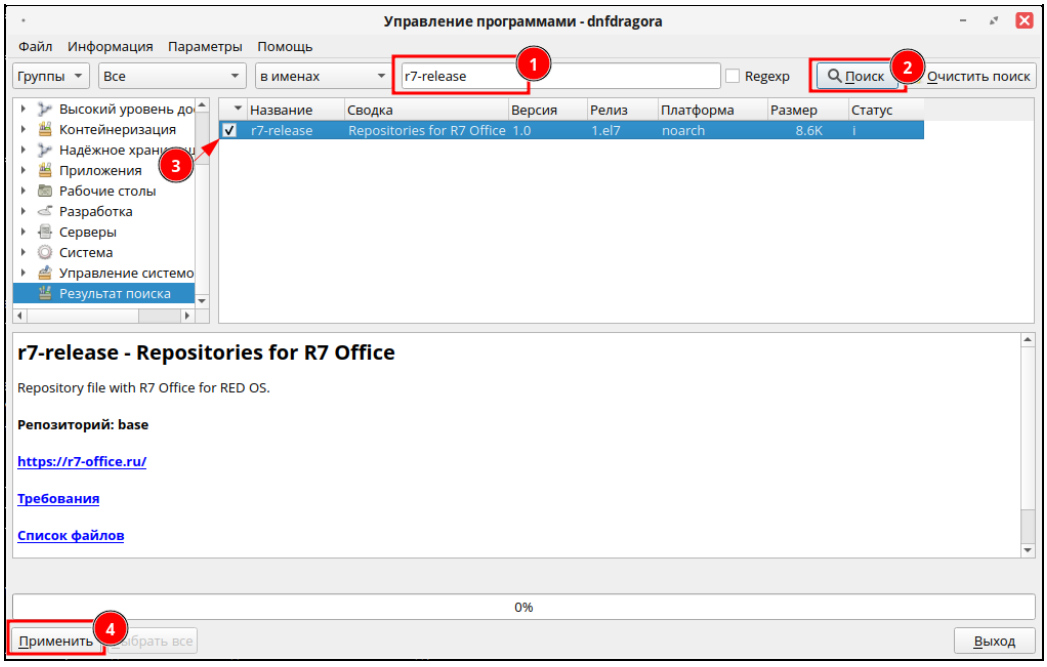
```
dnf install r7-release && dnf install r7organizer
```

После установки органайзер будет доступен из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Органайзер**».

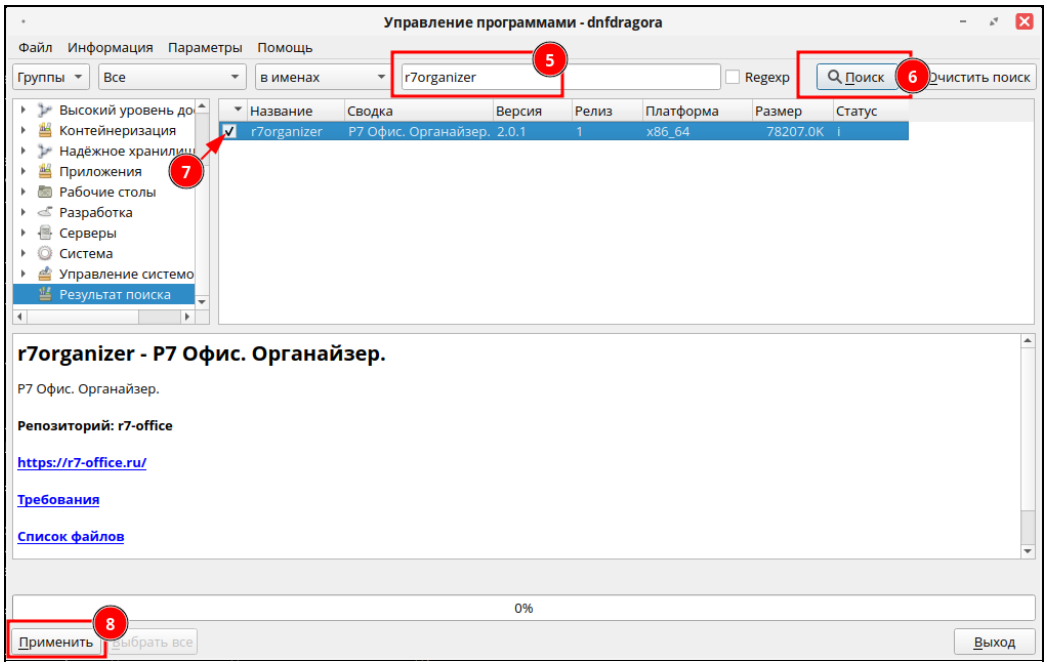
Установка через dnfdragora

Для установки **Р7-Офис. Органайзер** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» – «**Администрирование**» – «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**r7-release**».

В результате поиска будет предложен к установке подключаемый репозиторий **r7-release**. Отметьте флагом репозиторий последней версии, нажмите кнопку «**Применить**» и дождитесь окончания установки.

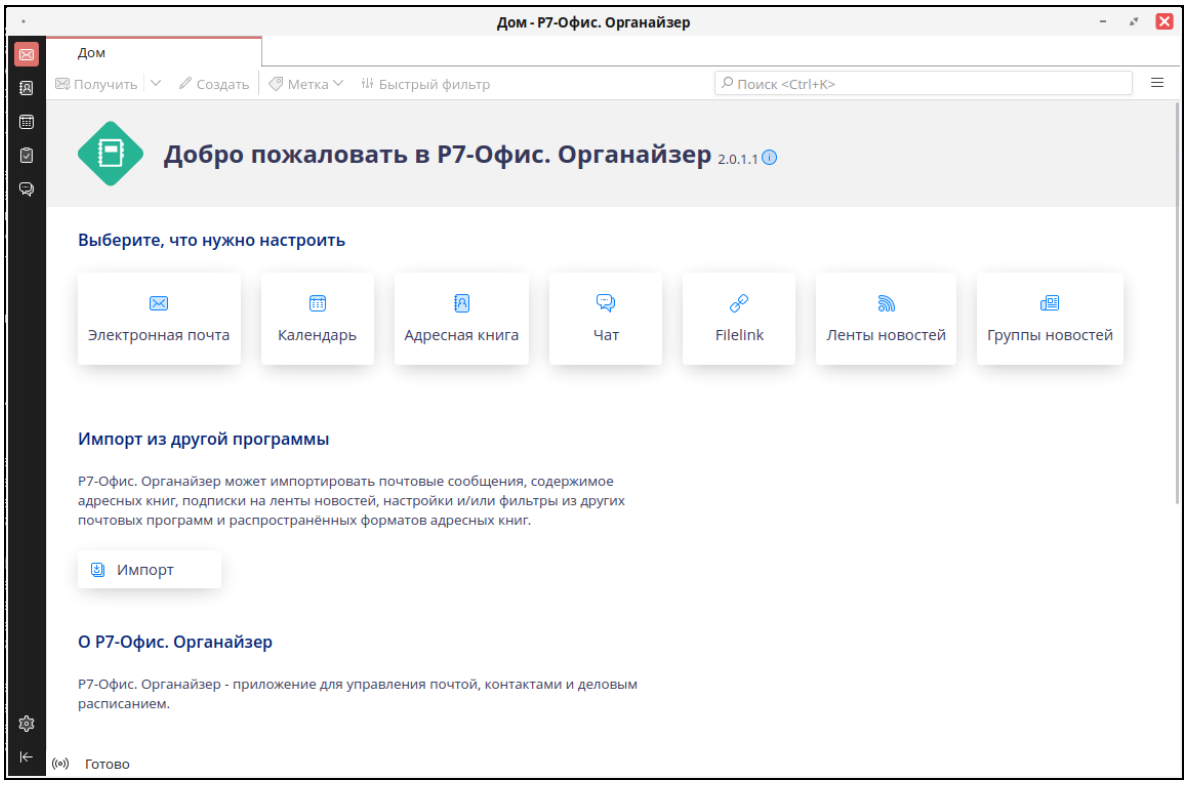


После установки репозитория в строке поиска необходимо ввести название пакета непосредственно самого органайзера – **r7organizer**. Затем отметьте флагом пакет последней версии и нажмите кнопку «**Применить**» для его установки.



После установки органайзер будет доступен из «**Главного меню**» – «**Офис**» – «**P7-Офис. Органайзер**».

Окно **Органайзера** выглядит следующим образом:



Установка P7-Графика

P7-Графика – это инструмент для создания диаграмм, схем, графиков и бизнес-иллюстраций профессионального уровня.

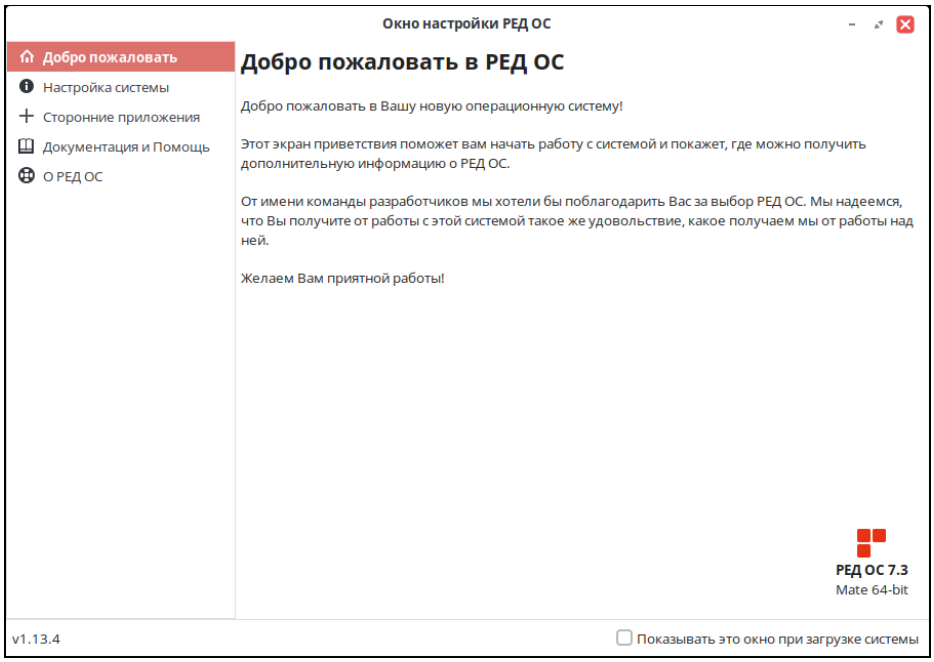
P7-Графика поддерживает открытие, редактирование и сохранение файлов **Visio** в формате **.vsdx**. Имеет обширную библиотеку шаблонов тематических элементов, а также позволяет импортировать и экспортировать эти библиотеки для обмена данных с другими людьми.

P7-Графика позволяет экспортировать диаграммы в различные форматы файлов, такие как **PNG**, **JPEG**, **PDF**, **SVG** и другие. Также доступен импорт существующих диаграмм из других приложений и последующее их редактирование в **P7-Графика**.

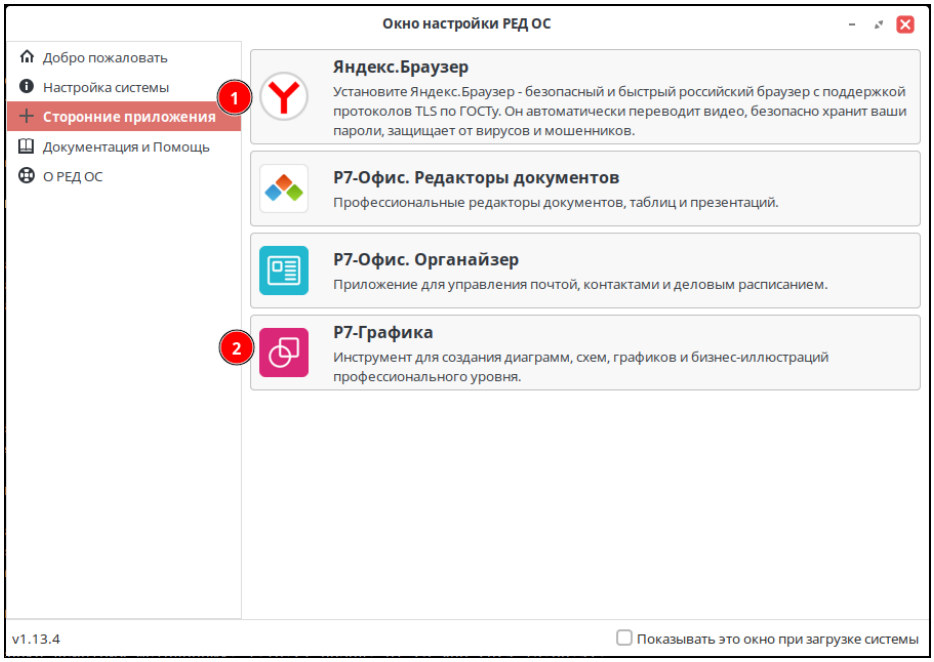
P7-Графика имеет интуитивный интерфейс, здесь можно быстро добавлять и настраивать элементы, соединять их линиями и создавать профессиональные диаграммы.

Установка через «Окно настройки РЕД ОС»

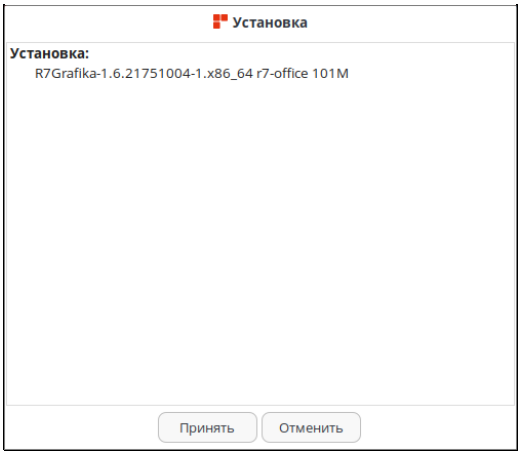
Откройте утилиту «Окно настройки РЕД ОС».



Перейдите на вкладку «**Сторонние приложения**», затем выберите из списка «**Р7-Графика**».



Далее в появившемся окне «**Установка**» ознакомьтесь со списком устанавливаемых пакетов и нажмите «**Принять**». Начнётся установка пакета **Р7-Графика**.



После установки редактор диаграмм будет доступен из «**Главного меню**» – «**Графика**» – «**Р7-Графика**».

Установка через терминал

Перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду подключения репозитория и установки **Р7-Графики**:

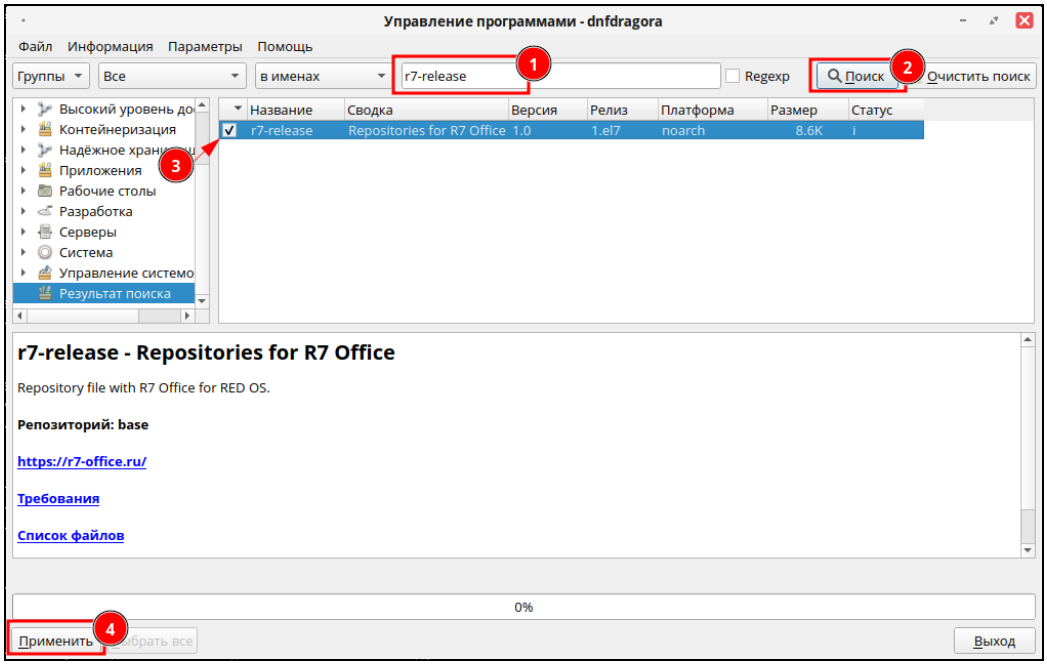
```
dnf install r7-release && dnf install R7Grafika
```

После установки редактор диаграмм будет доступен из «**Главного меню**» – «**Графика**» – «**Р7-Графика**».

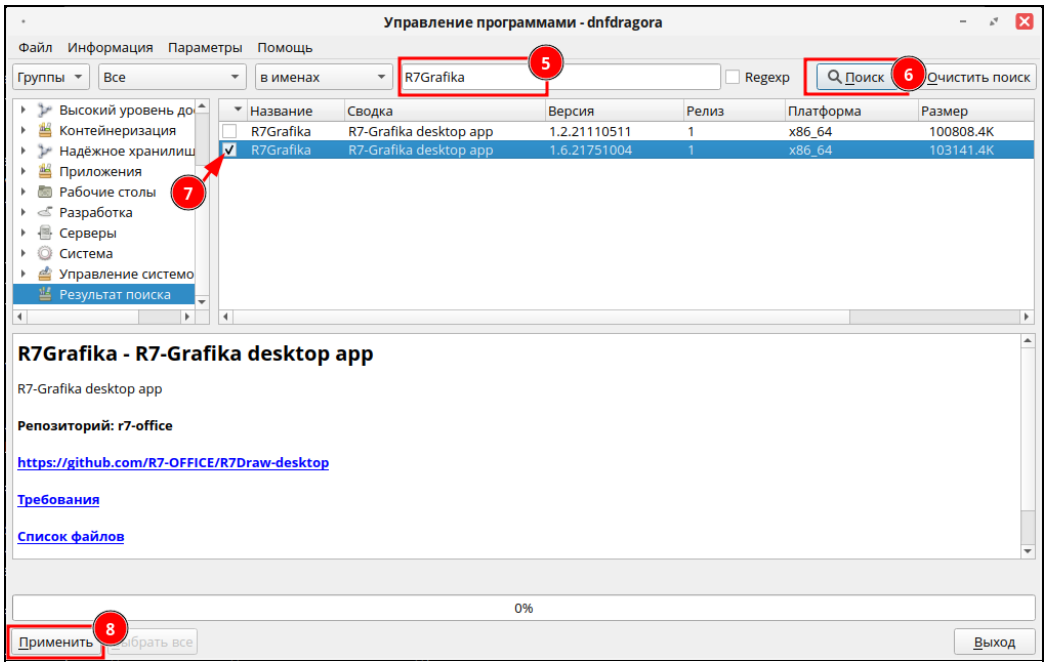
Установка через dnfdragora

Для установки **Р7-Графики** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» – «**Администрирование**» – «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**r7-release**».

В результате поиска будет предложен к установке подключаемый репозиторий **r7-release**. Отметьте флагом репозиторий последней версии, нажмите кнопку «**Применить**» и дождитесь окончания установки.

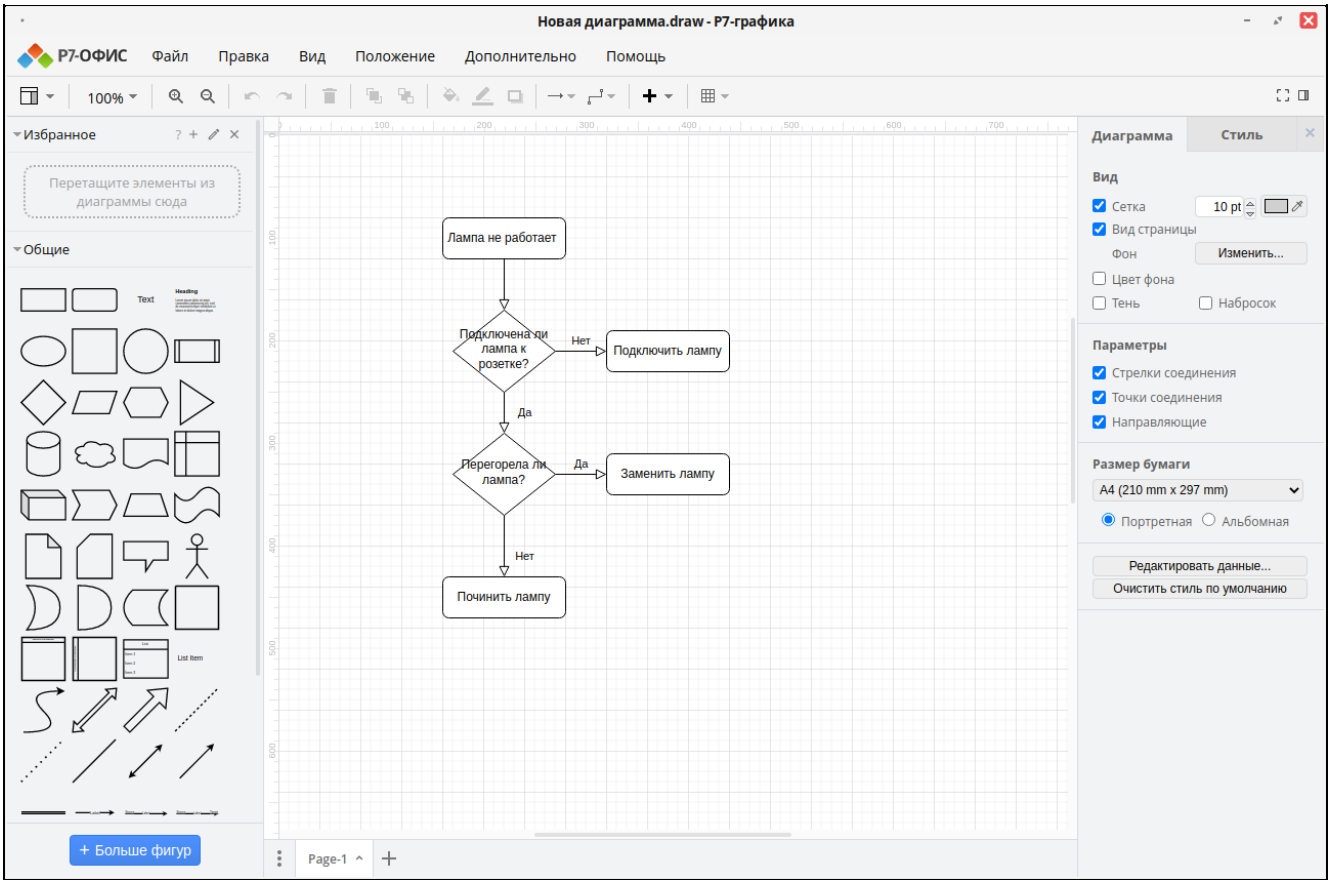


После установки репозитория в строке поиска необходимо ввести название пакета непосредственно самого редактора диаграмм – **R7Grafika**. Затем отметьте флагом пакет последней версии и нажмите кнопку « **Применить**» для его установки.



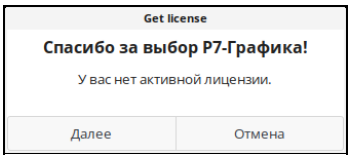
После установки редактор диаграмм будет доступен из «**Главного меню**» – «**Графика**» – «**Р7-Графика**».

Окно редактора диаграмм **Р7-Графика** выглядит следующим образом:

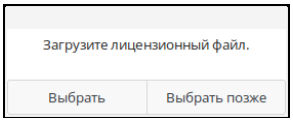


Активация лицензии

При первом запуске **Р7-Графики** будет выведено информационное сообщение об отсутствии активной лицензии. Лицензию необходимо запросить у официального разработчика. Нажмите **Далее**.



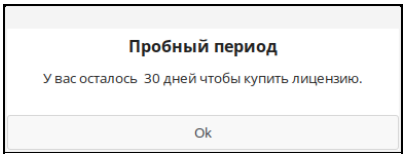
Для привязки имеющейся лицензии в следующем окне нажмите **Выбрать**.

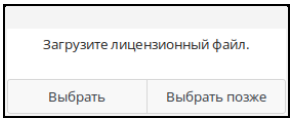


По нажатии **Выбрать позже** окно будет закрыто, и будет запущен непосредственно сам редактор диаграмм **Р7-Графика**.

Р7-Графика предоставляет 30-дневный бесплатный пробный период на рассмотрение и изучение функций редактора. По истечении бесплатного пробного периода необходимо загрузить соответствующую лицензию.

Возможность загрузки лицензии будет доступна при каждом последующем запуске **Р7-Графики** – будет появляться информационное окно с оставшимся количеством дней бесплатного периода, а затем окно для выбора лицензии.





Texmacs — программа для редактирования документов

Установка
Описание программы
Возможности программы

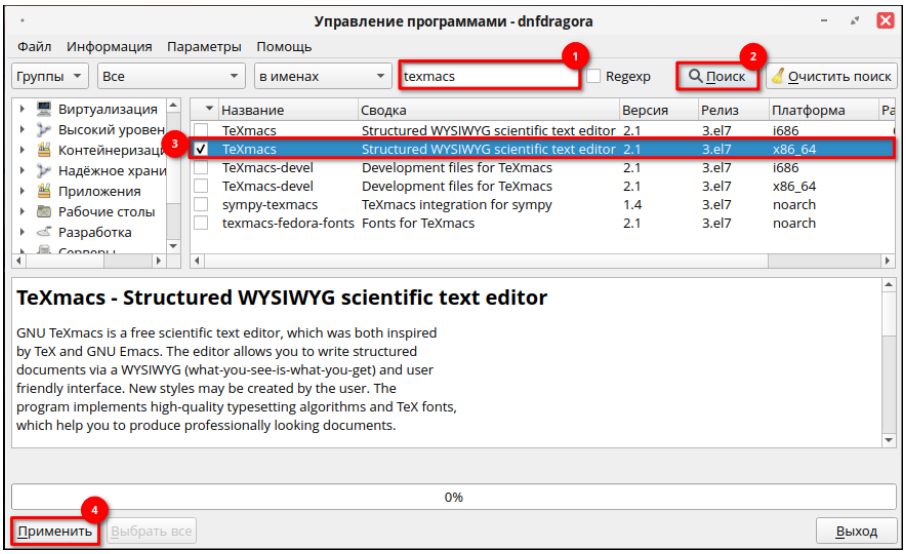
Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: TeXmacs-2.1

Texmacs — текстовый редактор с открытым исходным кодом, который предназначен для создания и редактирования технических документов с различными типами содержимого: текстом, математикой, графикой, интерактивным контентом, слайдами и т.д. Он поддерживает множество форматов, включая LaTeX, HTML, PDF и другие.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал. Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**texmacs**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install texmacs
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

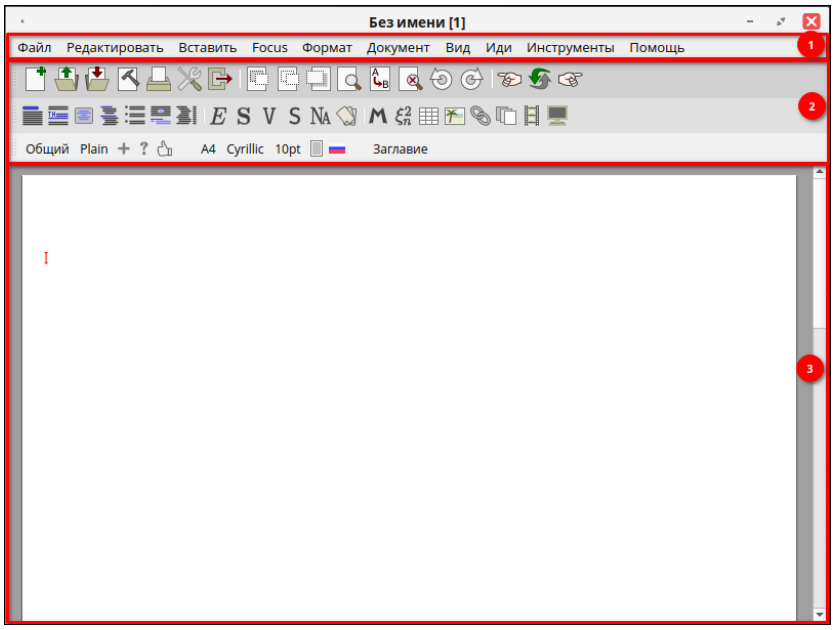
Для запуска программы через терминал введите команду:

```
texmacs
```

После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**GNU TeXmacs**».

Описание программы

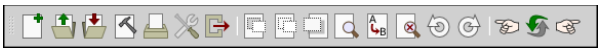
Интерфейс программы стандартный и состоит из нескольких типовых частей.



1 . **Основное меню программы** — здесь доступны основные возможности программы, такие как создание и редактирование документов, настройка параметров программы, панелей инструментов и другие.

2 . **Панели инструментов** предоставляют быстрый доступ к основным функциям программы. По умолчанию отображается *Главная панель инструментов*, *Панель инструментов режимов* и *Панель инструментов фокусировки*. Панели можно скрывать и отображать через основное меню.

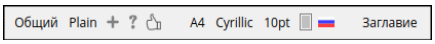
Главная панель инструментов предоставляет доступ к основным функциям программы, таким как создание, открытие, сохранение документов, а также другие часто используемые команды.



Панель инструментов режимов позволяет переключаться между различными режимами работы программы. Здесь можно выбрать, например, режим редактирования, просмотра или презентации.



Панель инструментов фокусировки содержит инструменты для управления вниманием пользователя, такие как инструменты увеличения или уменьшения масштаба, навигации по документу, а также инструменты для выделения и поиска.



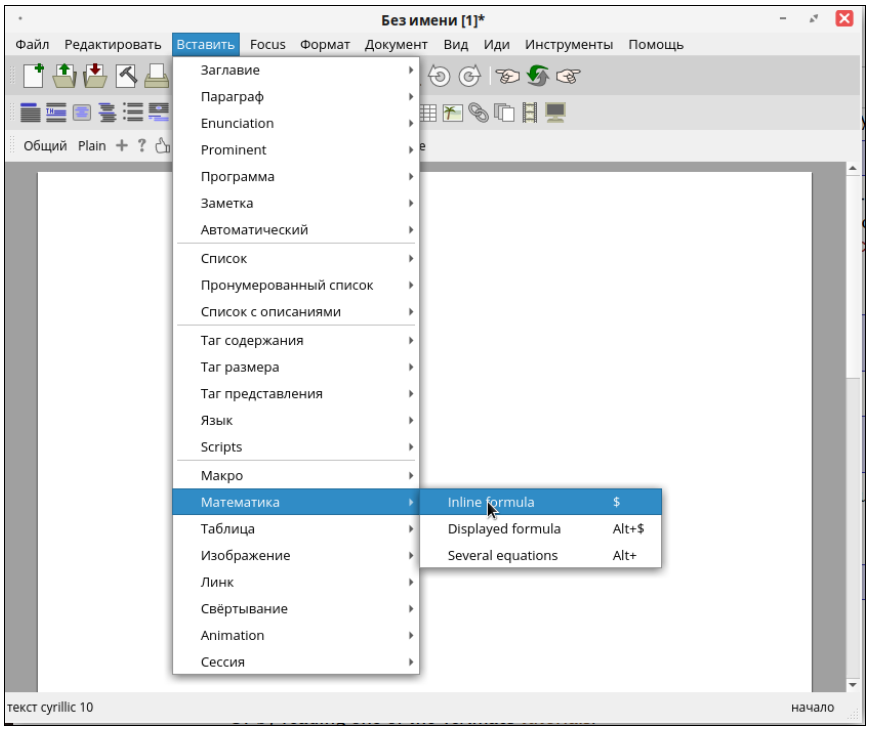
3. **Основное рабочее поле**. В данном поле происходит процесс создания, редактирования и форматирования документов.

Возможности программы

Основные возможности **Texmacs**:

1. Создание в документах формул, таблиц, изображений и других элементов.

Для вставки формулы в документ перейдите в меню «**Вставить**» — «**Математика**» (или щёлкните ЛКМ по значку  на панели инструментов), а затем выберите «**Inline formula**».

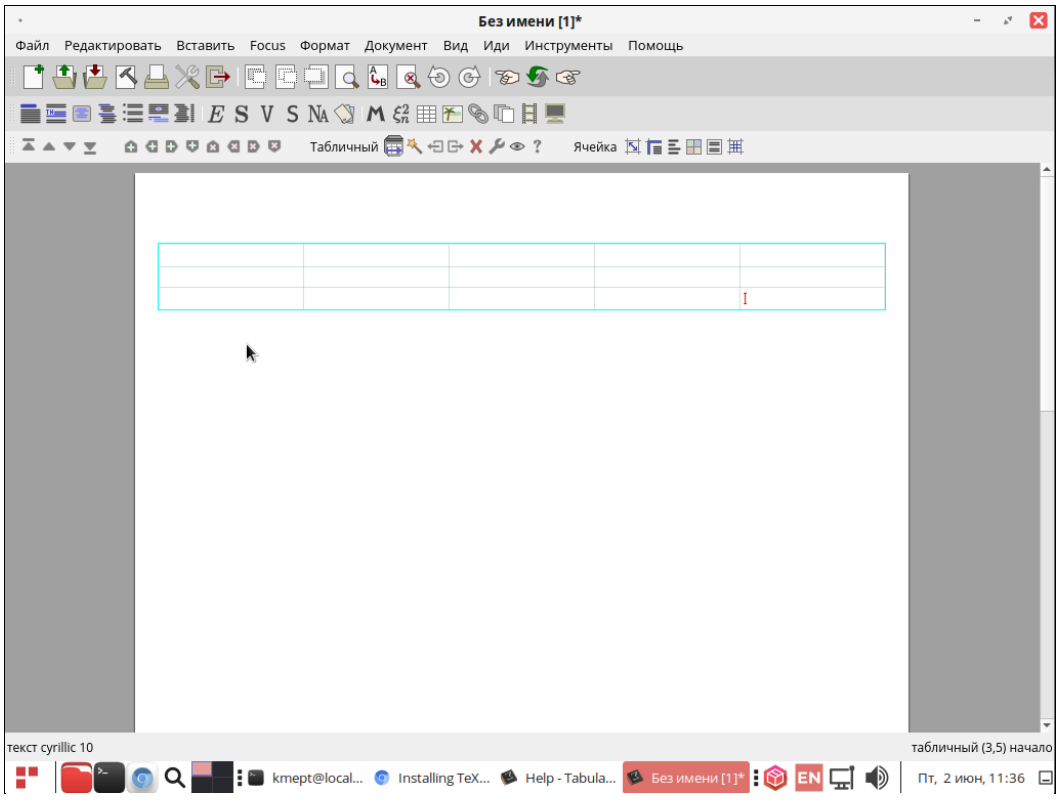


Для добавления математических формул на *Панели инструментов режимов* появляются дополнительные математические элементы. Введите нужное математическое выражение.

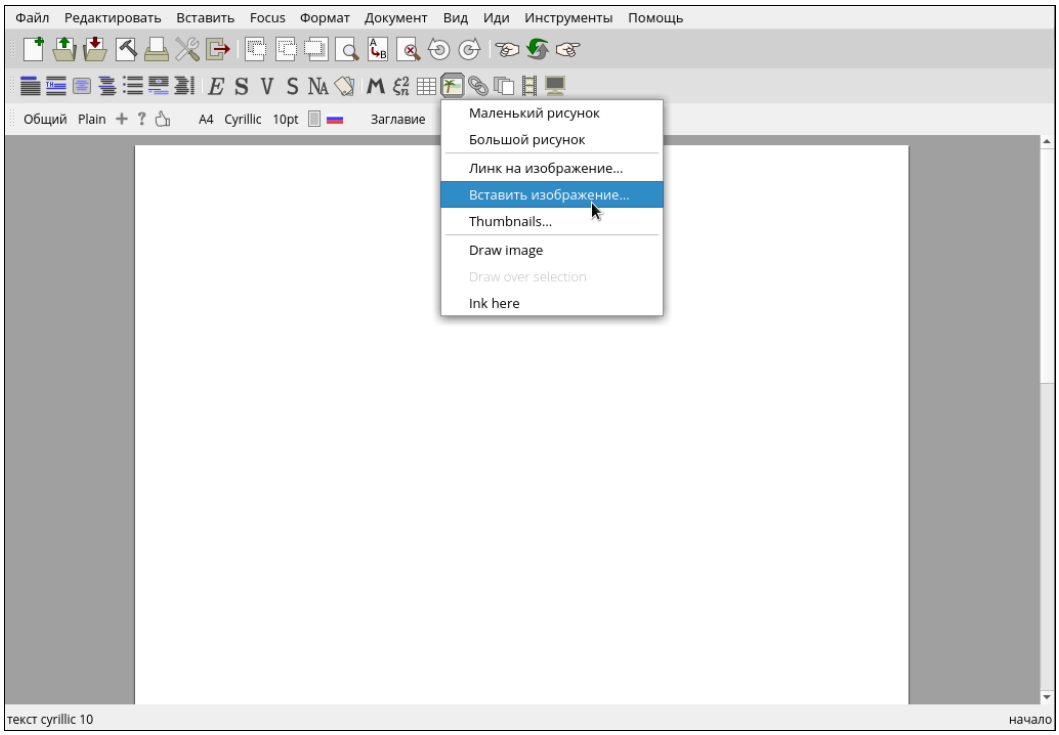


Для создания таблицы перейдите в пункт меню «**Вставить**» — «**Таблица**» (или щёлкните ЛКМ по значку  на панели инструментов), а затем выберите тип таблицы.

Появится *Панель для создания и редактирования таблиц*. При запуске новой таблицы её размер минимален, а ячейки пусты.

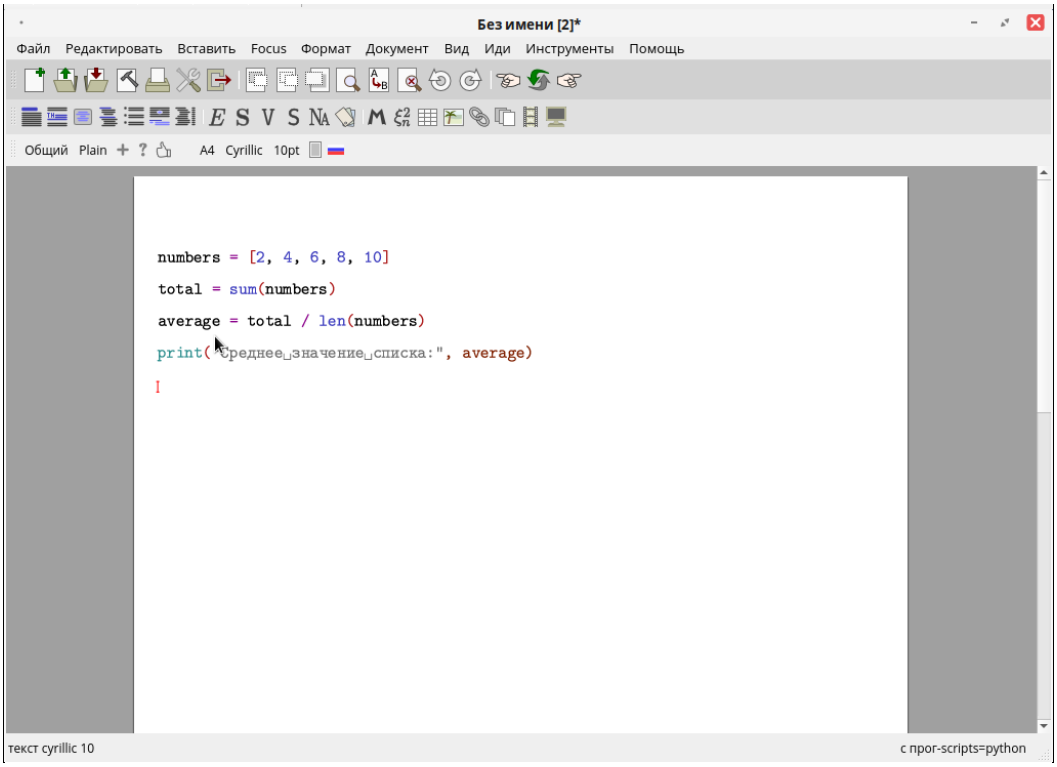


Для вставки изображения перейдите в пункт меню «**Вставить**» — «**Изображение**» — (или щёлкните ЛКМ по значку  на панели инструментов) и выберите «**Вставить изображение...**».



2. Поддержка многих языков программирования, включая Java, Python и C++.

Для создания кода на языке программирования Python перейдите в пункт меню «**Вставить**» — «**Программа**» — «**Inline code**» — «**Python**».



3. Интеграция с другими программами, например, Octave для выполнения математических вычислений.

Для установки программы **octave** через терминал выполните команду (потребуются права **администратора**):

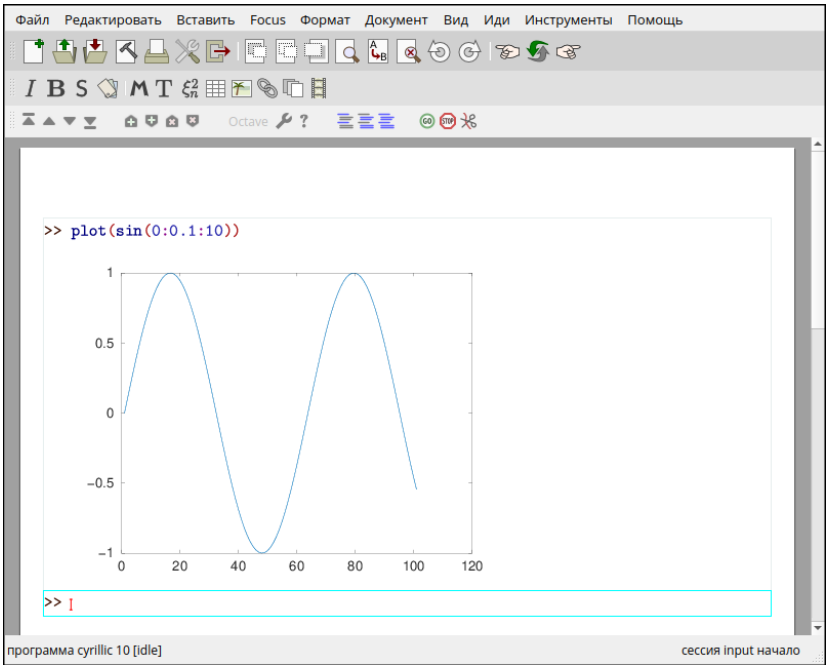
```
sudo dnf install octave
```

Для открытия **octave** перейдите в пункт меню «**Вставить**» — «**Сессия**» — «**Octave**». В открывшемся окне можно вводить команды и получать результаты в документе **TeXmacs**.

Например, введите следующую команду и нажмите **Enter**, чтобы построить график функции синуса:

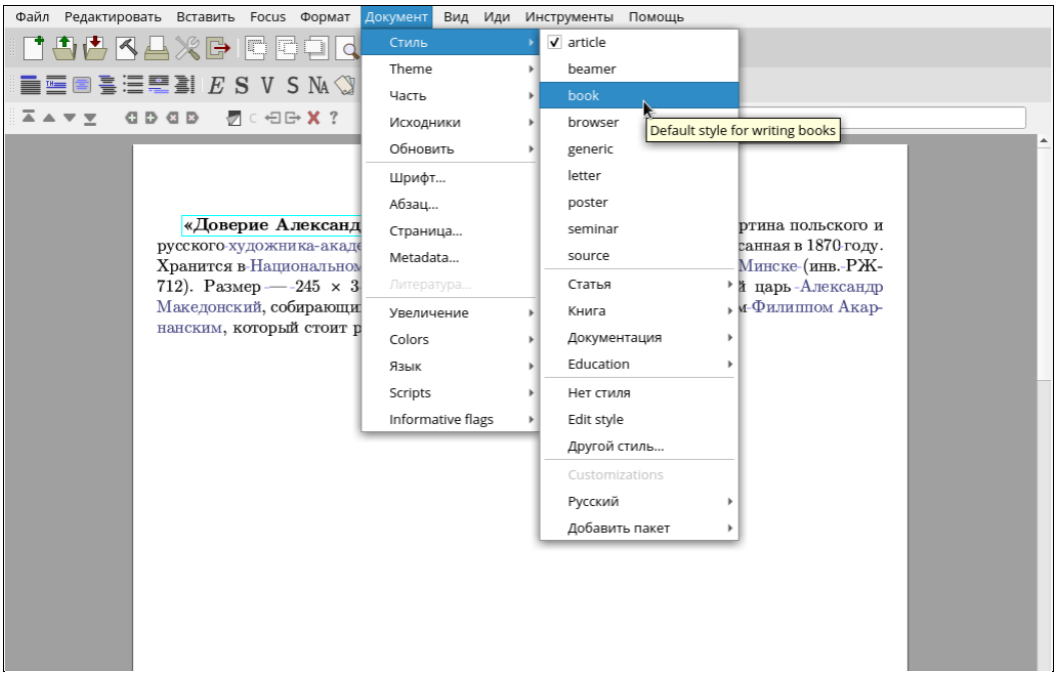
```
plot(sin(0:0.1:10))
```

Пример работы с **octave** внутри **texmacs**:



4. Автоматическое форматирование документов в соответствии с выбранным стилем.

Для форматирования документа перейдите в «**Документ**» — «**Стиль**» и выберите необходимый стиль.



5. Визуализатор графов.

Для создания графа предварительно необходимо установить пакет **texlive-standalone**, который предназначен для создания отдельных графиков и других элементов, которые можно вставлять в документ.

Для этого в терминале выполните команду (потребуются права **администратора**):

```
sudo dnf install texlive-standalone
```

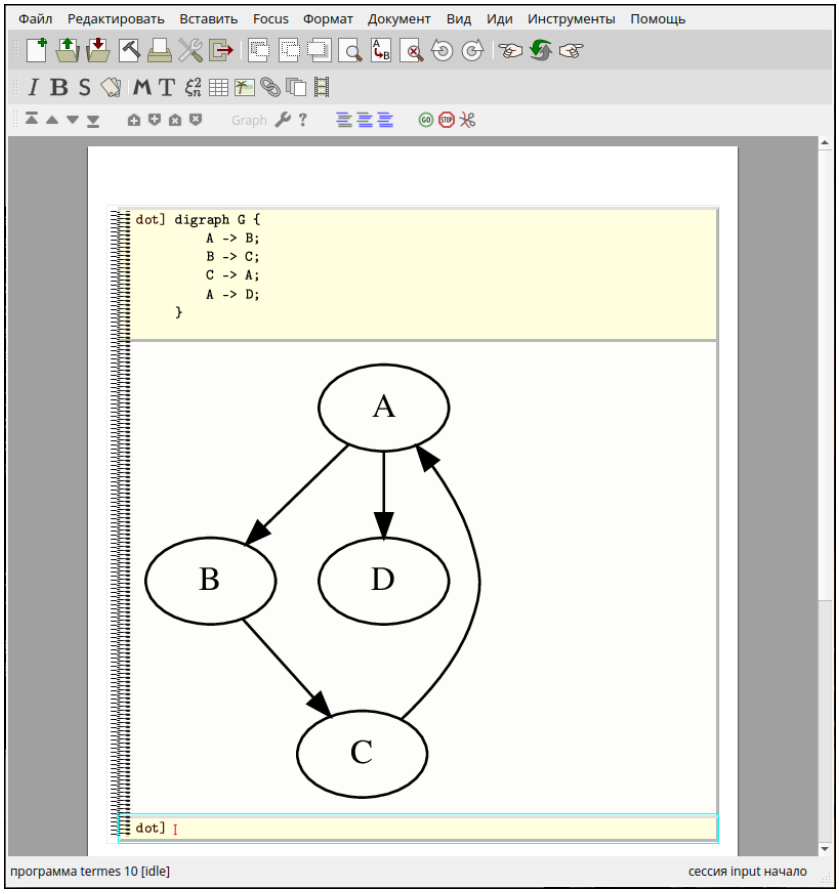
Для создания графа перейдите в меню «**Вставить**» — «**Сессия**» — «**Graph**».

Введите команду и нажмите Enter:

```
digraph G {
 A -> B;
 B -> C;
 C -> A;
 A -> D;
```

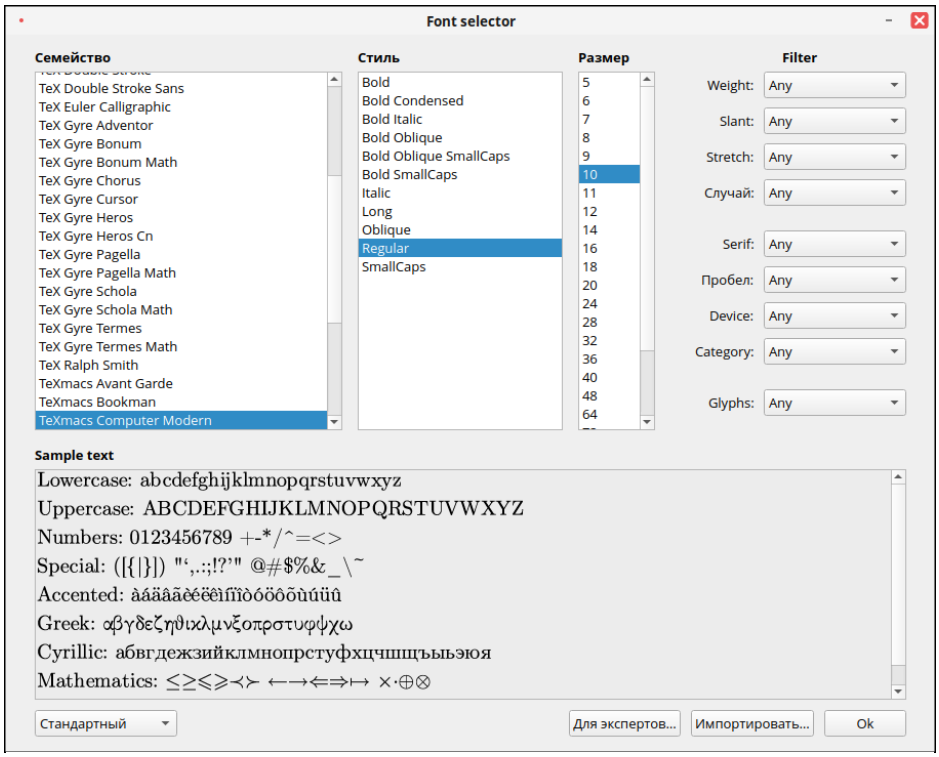
```
}
```

Этот код создаст простой ориентированный граф с вершинами A, B, C, D и рёбрами между ними. Можно изменять и дополнять этот код для создания более сложных графов.



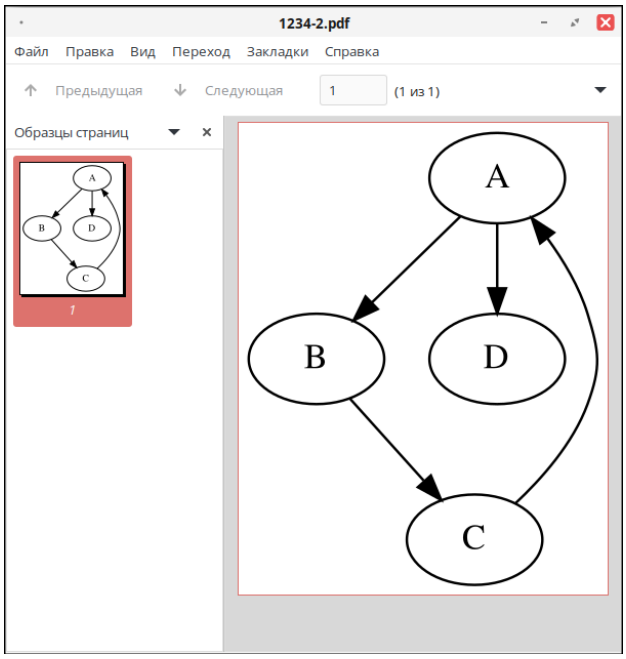
6. Поддержка встроенных шрифтов и возможность добавления новых шрифтов.

Для открытия Меню шрифтов выберите пункт меню «**Формат**» — «**Шрифт...**».



7. Возможность экспорта документов в различные форматы, включая PDF, HTML и LaTeX.

Для экспорта документа в формате PDF перейдите в меню «**Файл**» — «**Экспортировать**» — «**Pdf..**». Укажите имя файла и место для сохранения, затем нажмите «**Сохранить**».


1234-2.pdf
Файл Правка Вид Переход Закладки Справка
Предыдущая Следующая 1 (1 из 1)
Образцы страниц
A
B
D
C
1

Файловый менеджер Double Commander

Установка
Описание программы
Избранные каталоги
Файлы
Поиск
Вкладки
Настройка параметров

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** doublecmd-gtk-1.0.3-3, doublecmd-qt-1.0.3-3

Double Commander - двухпанельный кроссплатформенный файловый менеджер с открытым исходным кодом. Аналогичен по функциональности **Total Commander** и совместим с его плагинами.

Double Commander работает под *ОС Windows*, *macOS*, *FreeBSD*, а также *GNU/Linux* с графическими интерфейсами **GTK** и **Qt**, выбор между которыми нужно производить в зависимости от используемой графической оболочки.

GTK используется в таких DE, как *Cinnamon*, *GNOME*, *LXDE*, *MATE* или *Xfce*.

Qt используется в таких DE, как *KDE* или *LXQt*. Однако данные требования не обязательны, т.к. в РЕД ОС оба интерфейса успешно работают на каждой из DE.

Установка

В РЕД ОС *Double Commander* установлен по умолчанию и доступен из «**Главного меню**» - «**Стандартные**» - «**Double Commander**».

Если по какой-либо причине *Double Commander* отсутствует в системе, программу можно установить из репозитория. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

Для использования программы **с интерфейсом GTK** выполните команду:

```
dnf install doublecmd-gtk
```

Для использования программы **с интерфейсом Qt5** выполните команду:

```
dnf install doublecmd-qt
```

Дальнейшая работа в программе производится с **правами локального пользователя**.

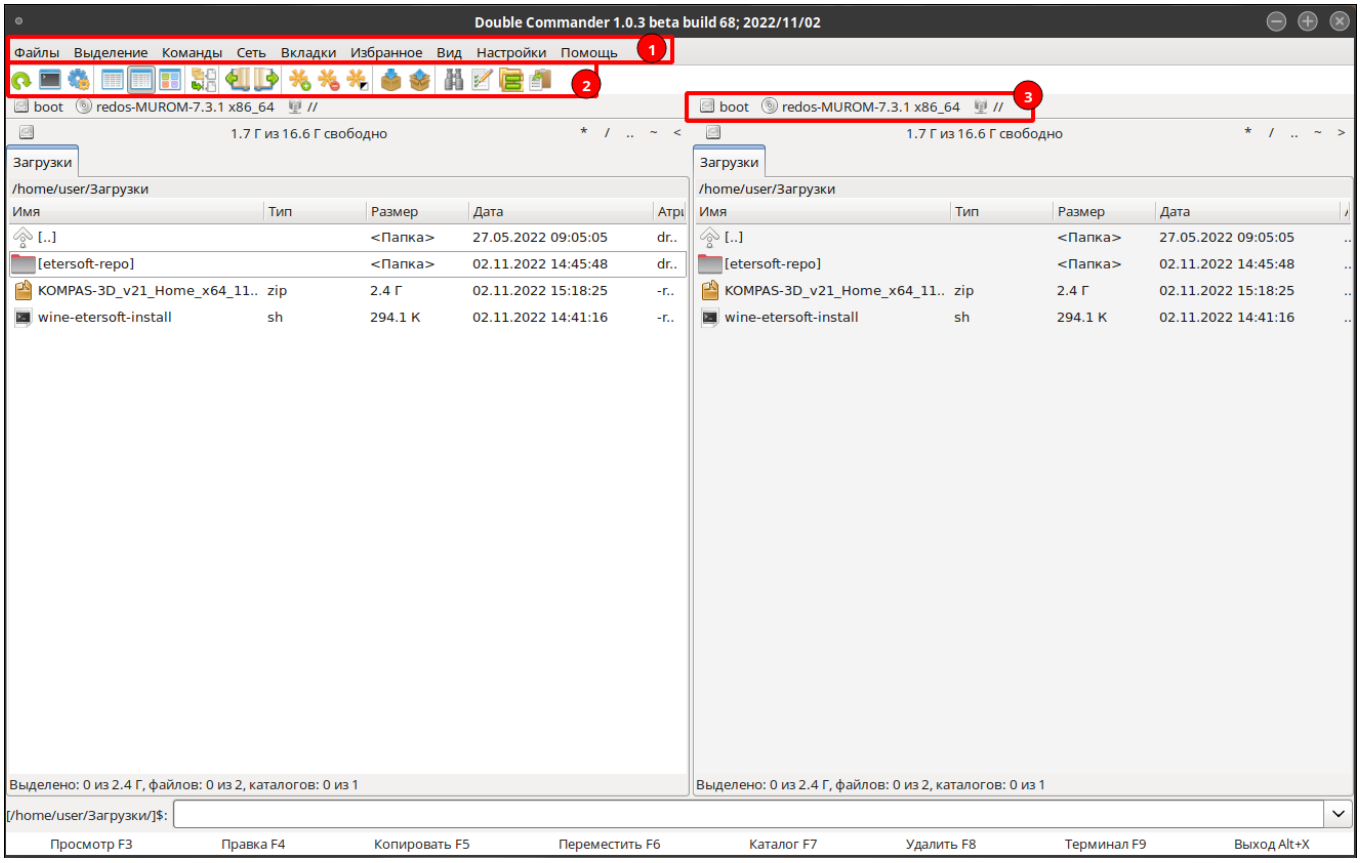
Описание программы

Основные характеристики *Double Commander*:

- встроенный редактор с подсветкой синтаксиса (**F4**);
- встроенный просмотрщик файлов (**F3**) для просмотра файлов любых размеров в шестнадцатеричном, двоичном или текстовом формате;
- работа с архивами так же, как с подкаталогами. Доступно копирование файлов в архив и из него. Поддерживаются следующие типы архивов: *ZIP*, *TAR*, *GZ*, *BZ2*, *XZ*, *LZMA*, *7Z*, а также *RPM*, *CPIO*, *DEB*, *RAR*, *ZIPX*;
- поддержка Unicode;
- поддержка консольных архиваторов, аналогично плагину **MultiArc** для *Total Commander*, со схожим форматом файла настроек;
- поддержка вкладок файловых панелей;
- настраиваемые колонки;
- инструмент синхронизации каталогов;

- инструмент группового переименования;
- протоколирование файловых операций;
- настраиваемая панель инструментов с кнопками для запуска внешних программ или внутренних команд меню;
- поддержка *WCX*, *WDX*, *WFX* и *WLX* плагинов от *Total Commander*.

Окно программы выглядит следующим образом:



Главное меню (1) включает в себя следующие пункты:

- Файлы;
- Выделение;
- Команды;
- Сеть;
- Вкладки;
- Избранное;
- Вид;
- Настройки;
- Помощь.

Панель инструментов (2) с функциональными кнопками для быстрой и удобной работы с содержимым и настройками самой программы.

Кнопки **быстрого перехода** к разделам (3).

Функциональные кнопки на *Панели инструментов* представлены следующими действиями:

- «**Обновить**»  ;
- «**Запуск терминала**»  ;
- «**Параметры**»  ;
- «**Поиск**»  .

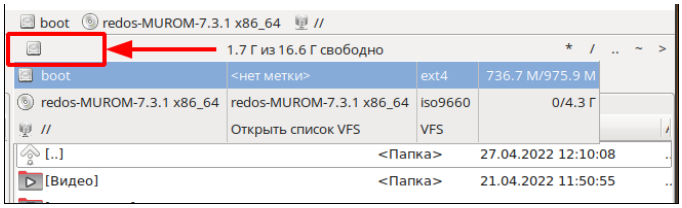
В неё также входят группы кнопок **способа отображения файлов** в панелях  , **выделения** и **снятия выделения** файлов  , кнопки «**Упаковать**» / «**Распаковать**»  и некоторые другие.

Добавлять и удалять необходимые функциональные кнопки можно через пункт меню «**Настройки**» - «**Параметры**» - «**Панель инструментов**».

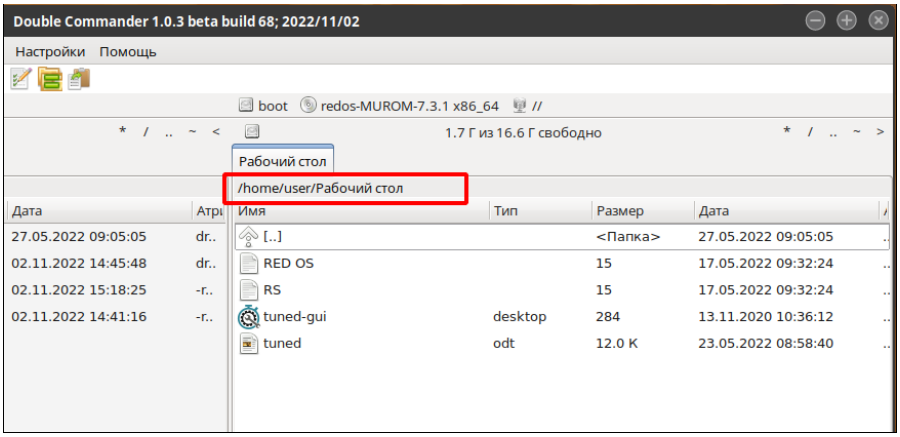
Над файловыми панелями доступны следующие действия с каталогами:

- список разделов (представлен на рисунке ниже);
- переход в корень файловой системы («/»);
- переход в домашний каталог («~»);
- управление избранными каталогами («*»);
- переход на уровень выше («..»);
- дублирование панелей («>» и «<»).

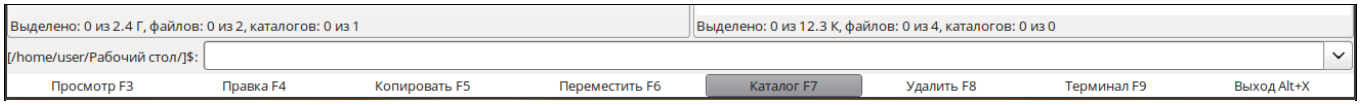
Кнопка списка разделов по функции аналогична кнопкам быстрого перехода (**3**).



Ниже располагается строка-заголовок с полным адресом текущего каталога. Данная строка также выполняет роль быстрых ссылок: с её помощью можно простым кликом перейти в любой из родительских каталогов.



Внизу окна *Double Commander* расположена «**Командная строка**», используемая для ввода команд вручную, а также панель функциональных клавиш «**F3**» - «**F9**» и «**Выход Alt+X**».



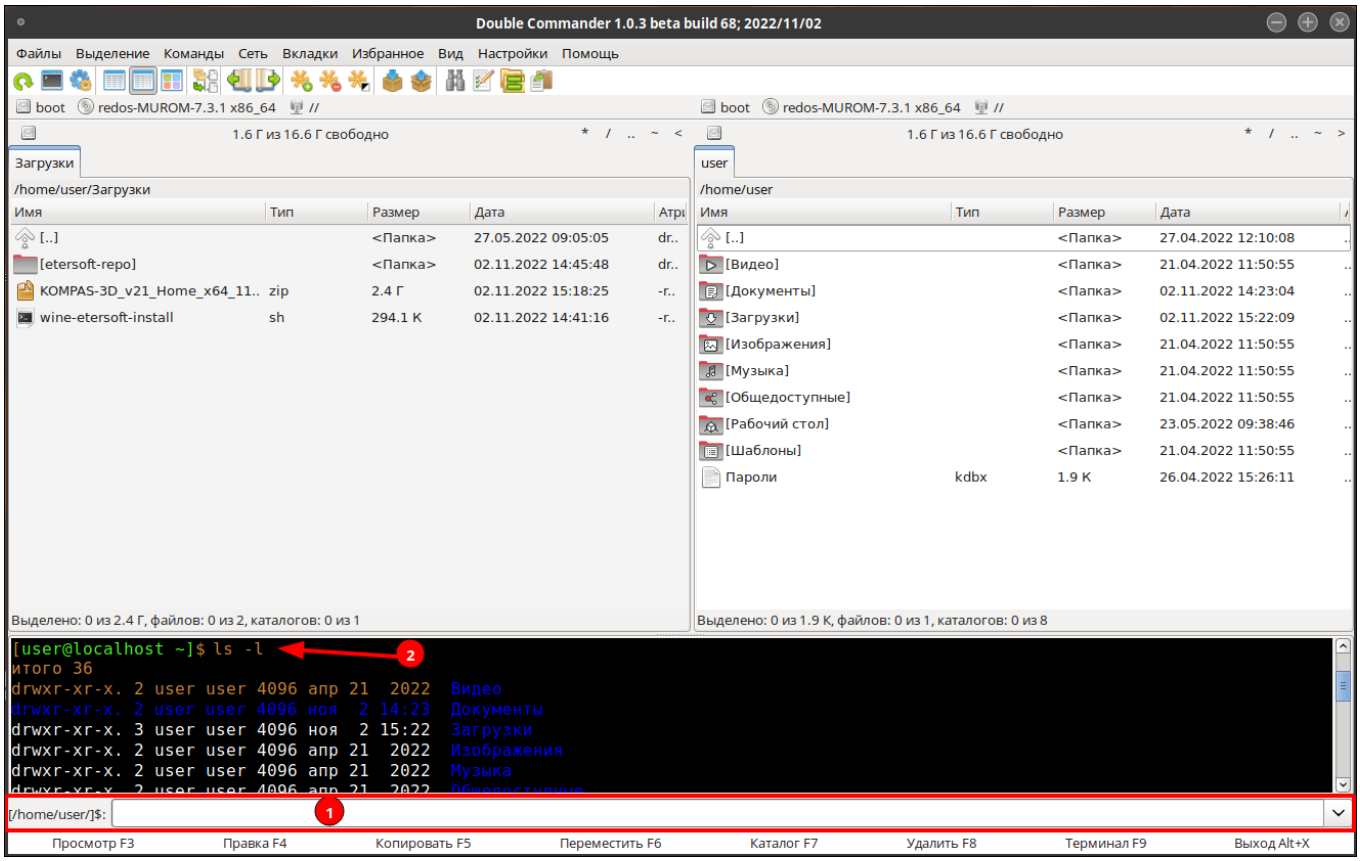
Для отображения результатов выполнения набранных команд из «**Командной строки**», а также действий в файловых панелях, во встроенном окне терминала *Double Commander* необходимо выставить флаг в чекбоксе «**Окно терминала**» в пункте меню «**Настройки**» - «**Параметры**» - «**Вид окна**».

По умолчанию используется **xterm**, но в системе он не установлен по умолчанию. Для установки выполните команду в терминале (с правами пользователя **root**):

```
dnf install xterm
```

Изменить терминал, используемый по умолчанию, можно в пункте меню «**Настройки**» - «**Параметры**» - «**Инструменты**» - «**Терминал**» в полях «**Команда**». Например, на **mate-terminal**, используемый в окружении *Mate*, или **gnome-terminal**, используемый в *Cinnamon*.

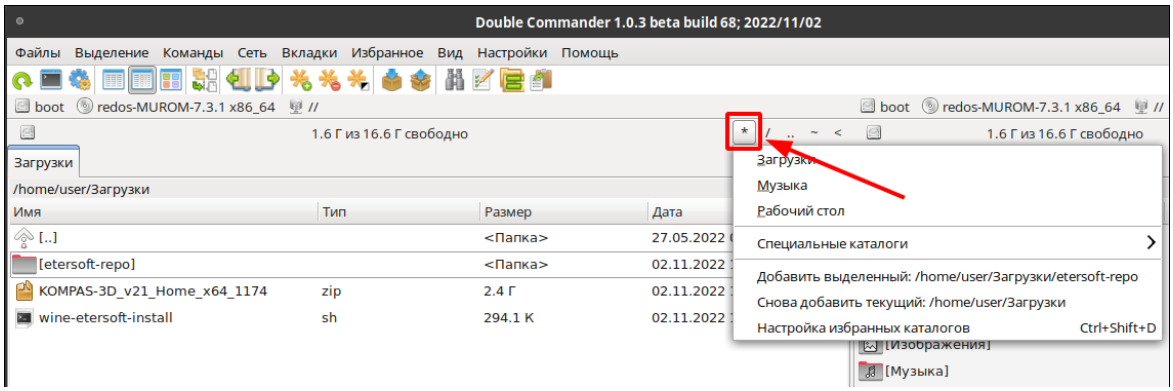
Для передачи команды в терминал выполните ее в текстовом поле (**1**), результат выполнения набранной команды будет отображен в поле терминала (**2**). Команды выполняются в активной файловой панели.



Избранные каталоги

Избранные каталоги («*» или «**Ctrl+D**») - это список каталогов и инструменты его изменения для формирования требуемого перечня быстрого доступа. Данный функционал также доступен из пункта меню «**Команды**» - «**Избранные каталоги**».

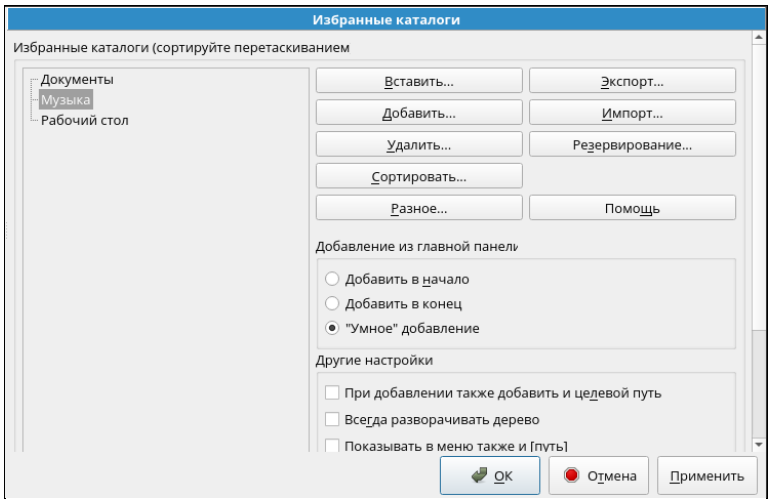
При активации нажатием на кнопку (*) или вызовом сочетания клавиш (**Ctrl+D**) появляется контекстное меню.



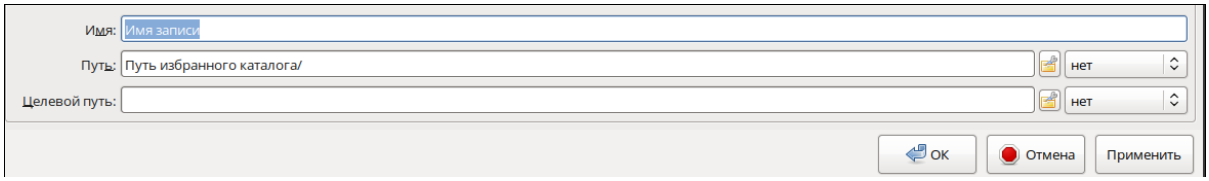
В списке будут отображены добавленные каталоги, ниже представлены пункты добавления текущего или выделенного каталога в перечень. Для того чтобы добавить нужный каталог в избранные, необходимо выделить его курсором мыши и выбрать функцию «**Избранные каталоги**» одним из перечисленных выше способов.

Редактирование разделов доступно через это же контекстное меню в пункте «**Настройка избранных каталогов**». Там можно добавить, удалить, экспортировать, импортировать, создать резервную копию и восстановить из резервной копии нужные каталоги.

Окно настройки избранных каталогов представлено на рисунке ниже.



Добавить избранный каталог можно вручную, указав имя и путь в полях нижней панели текущего окна.



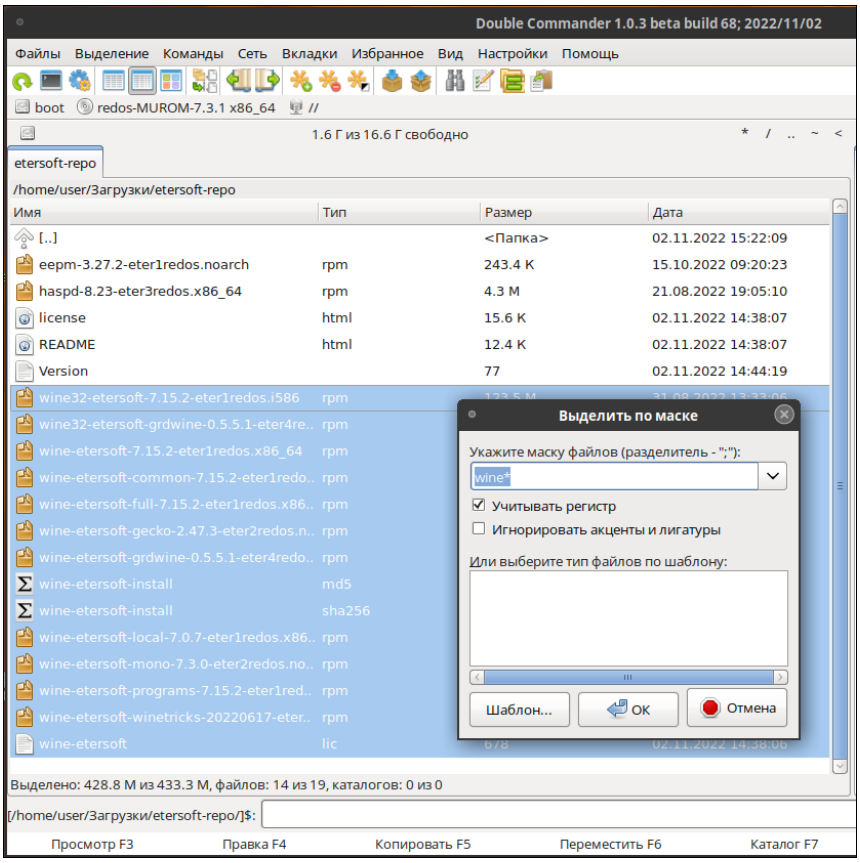
Файлы

Пункт меню «**Файлы**» *Double Commander* позволяет:

- создавать символьные или жесткие ссылки на файлы;
- изменять атрибуты файлов;
- создавать каталоги;
- распаковывать / упаковывать файлы и каталоги;
- разрезать файлы или объединять их;
- подсчитывать и проверять контрольные суммы;
- сравнивать файлы по содержимому;
- применять групповое переименование.

Инструмент группового переименования позволяет присвоить нескольким файлам разные наименования с одной маской (например: picture 1 , picture 2, picture 3 и т.д.).

В пункте меню «**Выделение**» можно быстро выделить файлы или папки, сгруппировав файлы по расширению или выделив группу.



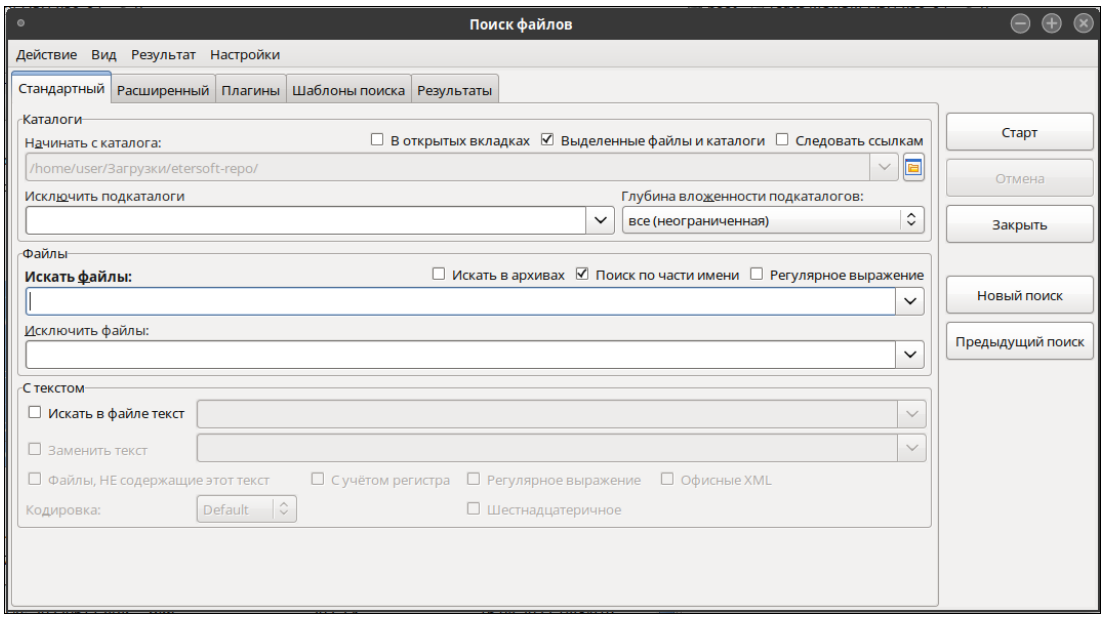
Пункт «**Сохранить выделение**» - сохраняет выделенный список в буфер обмена.

Пункт «**Восстановить выделение**» - восстанавливает ранее сохраненный выделенный список из буфера обмена.

Double Commander даёт возможность сохранить наименования выделенных файлов в текстовый документ, с возможностью сохранения как полных имен с абсолютным путём к файлам, так и сокращенных.

Поиск

Широкие возможности поиска в *Double Commander* представлены в виде отдельно открывающегося окна с вкладками. Поиск доступен из пункта меню «**Команды**» - «**Поиск...**».



Параметры места поиска:

- «**В открытых вкладках**» - поиск будет осуществляться в открытых вкладках;
- «**Выбранные файлы и каталоги**» - поиск ведётся только среди выделенных файлов или каталогов активной панели;
- «**Следовать ссылкам**» - если будет найдена символьная ссылка на каталог, то целевой каталог будет прочитан и использован,

иначе эта символьная ссылка будет считаться обычным файлом.

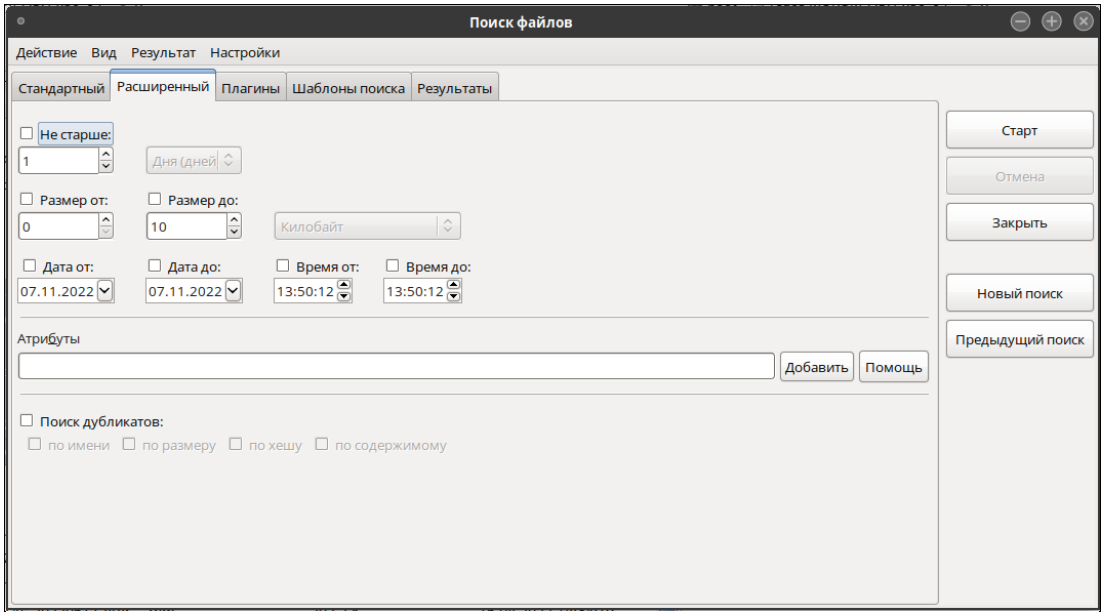
По умолчанию в строке «**Начинать с каталога**» используется текущий каталог активной панели. Также вы можете исключить подкаталоги и указать глубину вложенности.

В строке «**Искать файлы**» задаётся маска, по которой будет произведён поиск.

Дополнительные параметры этого поиска: «**Искать в архивах**», «**Поиск по части имени**», «**Регулярное выражение**», строка «**Исключить файлы**».

Если отметить «**Искать в файле текст**», то во время поиска будет происходить просмотр содержимого файлов, а в результат попадут только файлы, содержащие запрашиваемый текст.

Вкладка «**Расширенный**» позволяет указать дополнительные условия поиска файла: дату, время и возраст файла (по дате модификации), минимальный и максимальный размер файла, а также атрибуты.



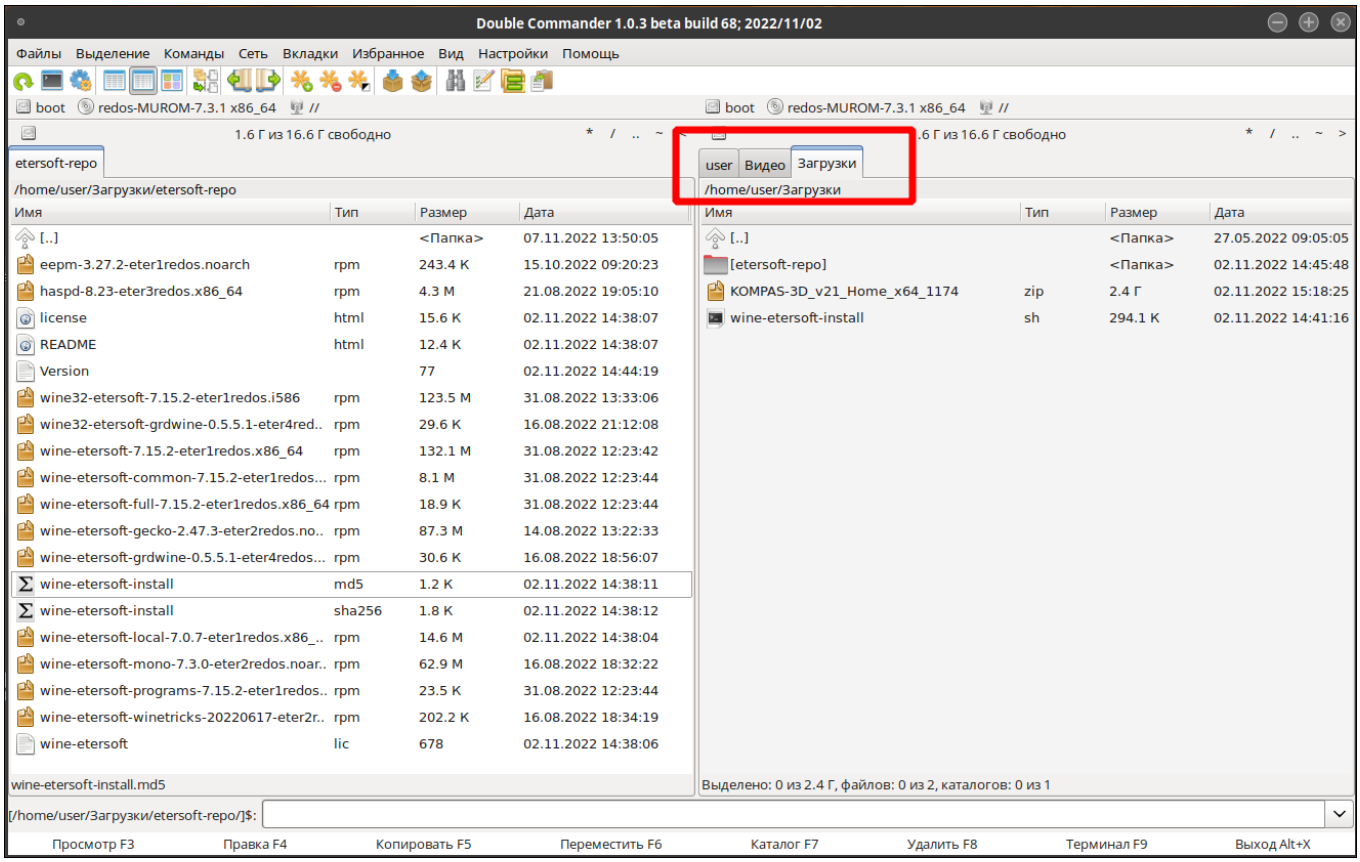
Вкладка «**Плагины**» задаёт поиск с помощью информационных (контентных, *WDX*) или поисковых (*DSX*) плагинов.

Вкладка «**Шаблоны поиска**» сохраняет параметры поиска для повторного использования.

Вкладки

Меню «**Вкладки**» предназначено для создания дополнительных вкладок в панелях и управления ими: создать вкладки, загрузить из файла, переименовать. Во вложенном разделе «**Опции вкладки**» изменяются состояния вкладок.

Вкладку можно создать с помощью сочетания клавиш «**Ctrl+T**» или через пункт меню «**Вкладки**».



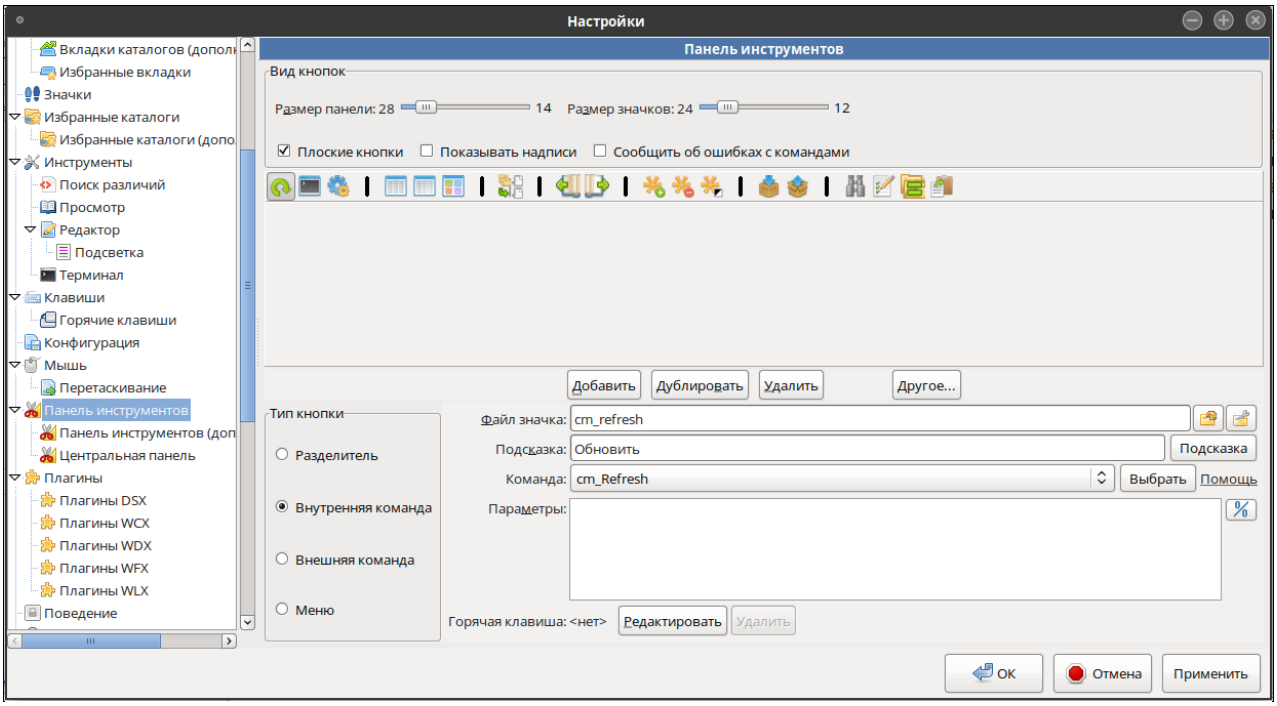
Подменю «**Опции вкладки**» позволяет назначить вкладку обычной или заблокированной, причём у заблокированной может быть несколько статусов:

- «**Заблокировать вкладку**» - блокирует смену каталога вкладки и предлагает при этом открыть этот же каталог в новой вкладке;
- «**Заблокировать с возможностью смены каталога**» - в этом случае можно сменить каталог, однако, если переключиться на другую вкладку, а потом обратно, в ней будет открыт каталог, с которым она была заблокирована;
- «**Заблокировать и открывать каталоги в новых вкладках**» - при попытке войти в любой другой каталог в панели, он откроется в новой вкладке.

Заблокированные вкладки помечаются значком «*».

Настройка параметров

Диалоговое окно, доступное через пункт меню «**Настройки**» - «**Параметры**», позволяет устанавливать и выбирать нужные пользователю параметры программы, такие как «**Вид окна**», «**Панель инструментов**», «**Шрифты**» и пр.


Настройки
Вкладки каталогов (дополн
Избранные вкладки
Значки
Избранные каталоги
Избранные каталоги (допо
Инструменты
Поиск различий
Просмотр
Редактор
Подсветка
Терминал
Клавиши
Горячие клавиши
Конфигурация
Мышь
Перетаскивание
Панель инструментов
Панель инструментов (доп
Центральная панель
Плагины
Плагины DSX
Плагины WCX
Плагины WDX
Плагины WFX
Плагины WLX
Поведение
Панель инструментов
Вид кнопок
Размер панели: 28
14
Размер значков: 24
12
Плоские кнопки
Показывать надписи
Сообщить об ошибках с командами
Добавить
Дублировать
Удалить
Другое...
Тип кнопки
Разделитель
Внутренняя команда
Внешняя команда
Меню
Файл значка:
cm_refresh
Подсказка:
Обновить
Подсказка
Команда:
cm_Refresh
Выбрать
Помощь
Параметры:
Горячая клавиша: <нет>
Редактировать
Удалить
OK
Отмена
Применить

Файловый менеджер Midnight Commander

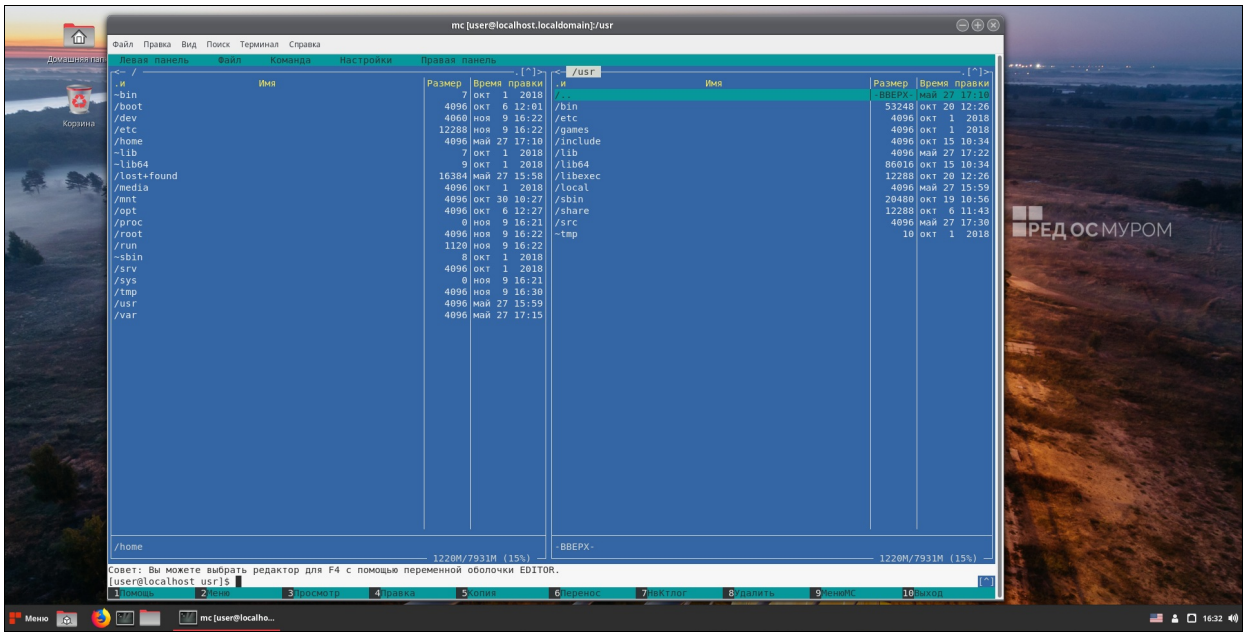
Midnight Commander (mc, MC) – текстовая полнофункциональная программа, которая позволяет пользователю копировать, перемещать и удалять файлы и директории, производить поиск файлов и запускать на выполнение команды оболочки. Также в него встроен редактор и программа для просмотра файлов.

Вы можете подробнее ознакомиться с работой файлового менеджера **MC**, просмотрев наши обучающие видео:

- на **RuTube** — Файловые менеджеры в РЕД ОС;
- в **Яндекс.Дзен** — Файловые менеджеры в РЕД ОС;
- в **VK Видео** — Файловые менеджеры в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Экран MC делится на четыре части. Почти весь экран занят двумя панелями. По умолчанию, вторая строка снизу является командной, а в самой нижней отображается назначение функциональных клавиш. Самая верхняя строка - строка меню. Она может быть не видна, но при нажатии клавиши *F9* или при щелчке мыши эта строка отображается в верхней части экрана.



Файловый менеджер Midnight Commander в окружении Cinnamon РЕД ОС

MC позволяет одновременно наблюдать содержимое двух каталогов. Одна из панелей является текущей (в этой панели находится выделитель). Практически все команды оперируют над текущей панелью. Хотя некоторые файловые операции, такие как «Переименовать» или «Копировать», по умолчанию используют каталог неактивной панели в качестве каталога назначения (при выполнении подобных команд всегда появляется запрос на подтверждение).

Поддержка мыши

MC поддерживает управление мышью. При щелчке левой кнопкой мыши на файле, этот файл становится текущим. При щелчке правой кнопкой, файл помечается (или пометка снимается, в зависимости от предыдущего состояния).

При двойном щелчке на файле, будет произведена попытка его запуска, если это запускаемый файл. Если расширение файла связано с какой-либо программой, то эта программа будет запущена.

Также можно выполнять команды, связанные с метками функциональных клавиш, щелкнув мышью на них.

При щелчке мышью на верхней границе панели, список файлов прокрутится на одну страницу назад. Соответственно, щелчок на нижней границе приведёт к прокрутке на страницу вперёд. Этот метод также работает с просмотром помощи и деревом каталогов.

По умолчанию значение параметра автоповтора для клавиш мыши равно 400 миллисекундам. Это значение может быть изменено путём редактирования в файле **.mc.ini** параметра **mouse_repeat_rate**.

Если MC сконфигурирован с поддержкой мыши, то вы можете вырезать и склеивать фрагменты текста, используя клавишу *Shift*.

Меню

Строка меню появляется при нажатии *F9* или при щелчке мышью в верхней строке экрана. Строка меню состоит из пяти подменю: «Левая панель», «Файл», «Команда», «Настройки» и «Правая панель».

Меню *Левая панель* и *Правая панель* позволяют оперировать панелями.

В меню *Файл* предлагается список команд, которые могут быть применены к текущему файлу или к любым помеченным файлам.

В меню *Команда* содержатся более общие команды, которые никак не связаны с текущим файлом или помеченной группой файлов.

Меню *Настройки* позволяет устанавливать различные настройки для работы в MC.

Горячие комбинации клавиш Midnight Commander

В данном разделе речь пойдет о горячих клавишах для файлового менеджера Midnight Commander, знание которых позволяет повысить удобство и скорость работы.

Работа с файлами

Сочетание	Действие
F3	Просмотреть файл
F4	Редактировать файл
Shift+F4	Создать новый файл
+	Вызвать окно для выделения группы
\	Снять отметку с группы

Работа с командной строкой

Сочетание	Действие
Alt+Enter	Вставить файл или каталог, на котором установлен курсор, в командную строку
Alt+p	Вернуть предыдущую выполненную команду в командную строку
Ctrl + x,t	Вставка всех выделенных объектов в командную строку
Ctrl + x, Ctrl + p	Вставить в командную строку полный путь, установленный на неактивной панели
Alt+t	Смена режима отображения панели
Alt+.	Скрыть или показать скрытые файлы и каталоги, которые начинаются на точку
Alt+a	Вставить в командную строку полный путь, установленный на активной панели
Alt+c	Смена текущего каталога
Alt+h	Просмотр последних выполненных команд
Alt+i	Смена каталога на неактивной панели на каталог, в котором находится пользователь
Alt+o	Неактивная панель переходит в каталог, на который указывает активная панель
Ctrl+x, q	Просмотр содержимого файла на второй панели
Ctrl+x,i	Просмотр информации о текущем объекте на второй панели
Ctrl+o	Скрыть или показать панели
Ctrl+r	Перечитать содержимое каталога
Ctrl+Space	Показать размер текущего каталога

Работа с поиском

Сочетание	Действие

Alt+Shift+?	Расширенный поиск
Ctrl+s	Поиск файла или каталога

Работа с правками

Сочетание	Действие
Ctrl+x,o	Просмотр или изменения владельца, группы
Ctrl+x,c	Просмотр или изменение прав доступа

Работа со ссылками

Сочетание	Действие
Ctrl+x,l	Создать жесткую ссылку
Ctrl+x,s	Создать символьную ссылку symlink
Ctrl+x,Ctrl+s	Редактировать символическую ссылку

Горячие комбинации клавиш для редактора Midnight Commander (MCEdit)

Отдельно рассмотрим горячие комбинации клавиш для работы в текстовом редакторе.

MCEdit - редактор текстовых и двоичных файлов с заменой регулярных выражений, подсветкой синтаксиса, макросами и конвейером оболочки.

При запуске Midnight Commander под этим именем требуется запустить внутренний редактор и открыть файл, указанный в командной строке.

Внутренний редактор файлов - это полнофункциональный полноэкранный редактор. Он может редактировать файлы размером до 64 мегабайт. Можно редактировать двоичные файлы. В настоящее время он поддерживает следующие функции: копирование блоков, перемещение, удаление, вырезание, вставка; клавиша для отмены нажатия клавиши; выпадающие меню; вставка файла; макрокоманды; поиск и замена регулярных выражений (наш собственный поиск и замена scanf-printf); выделение текста стрелкой *Shift* (если поддерживается терминалом); переключатель вставки-перезаписи; перенос слова; настраиваемый размер вкладки; подсветка синтаксиса для различных типов файлов; и возможность передавать текстовые блоки по конвейеру через команды оболочки, такие как **indent** и **ispell**.

Изменение вида редактора

Сочетание	Действие
Alt+n	Показать или скрыть нумерацию строк
Ctrl+s	Включить или выключить подсветку синтаксиса
Alt+Shift+-	Включить или отключить отображения табуляций и пробелов
Alt+Shift++	Включить или отключить автовыравнивание возвратом каретки

Работа с текстом

Сочетание	Действие
F3	Начать выделение текста, повторное нажатие *F3* закончит выделение
Shift+F3	Начать выделение блока текста, повторное нажатие *F3* закончит выделение
F5	Скопировать выделенный текст
F6	Переместить выделенный текст
F8	Удалить выделенный текст
Ctrl+k	Удалить часть строки до конца строки

Ctrl+y	Удалить строку
Ctrl+x	Перейти в конец слова
Ctrl+z	Перейти на начало предыдущего слова
Alt+l	Переход на строку по номеру строки
Alt+u	Выполнить команду и вставить вывод результата команды в позицию под курсором
Alt+t	Сортировка строк выделенного текста
Tab	Сдвинуть вправо выделенный текст
Ctrl+u	Отменить действия

Работа с файлами

Сочетание	Действие
Ctrl+n	Создать новый файл
Ctrl+f	Копировать выделенный текст в файл
Shift+F5	Вставка текста из файла

Ручное добавление расширений caja

Caja menu
Добавление нового действия
Добавление кнопки

Бывают ситуации, когда предустановленного перечня функций в контекстном меню может не хватать. Хочется добавить утилиту в быстрый доступ с мышки или написать собственный скрипт, оптимизирующий работу того или иного действия.

В данной статье описывается алгоритм добавления действий в контекстное меню.

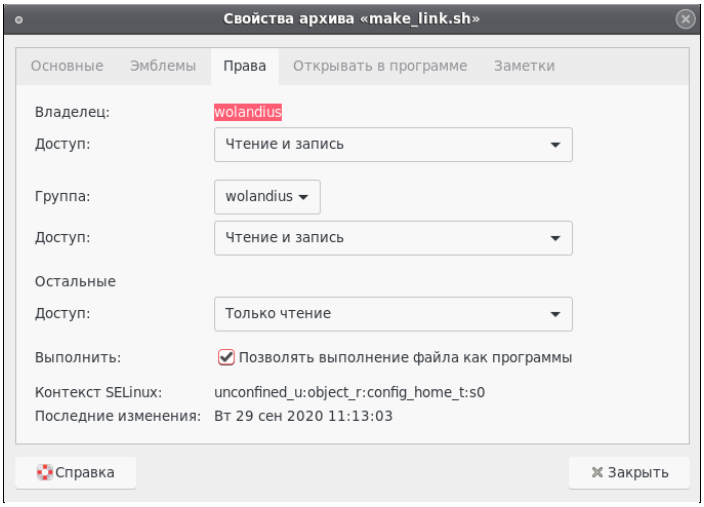
Главное уточнение при работе с конфигурационным меню это то, что все изменения, которые будут внесены в него, будут доступны только для того пользователя, в чьей домашней директории были произведены изменения.

Caja menu

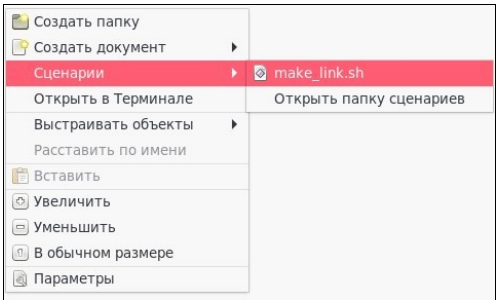
Функционал меню **Caja** можно расширить написанием обычного bash-скрипта, который должен быть помещен в данную директорию: **/home/<Имя_Пользователя>/.config/caja/scripts**.

В самом bash-скрипте может быть прописан как определенный алгоритм, так и запуск определенного приложения.

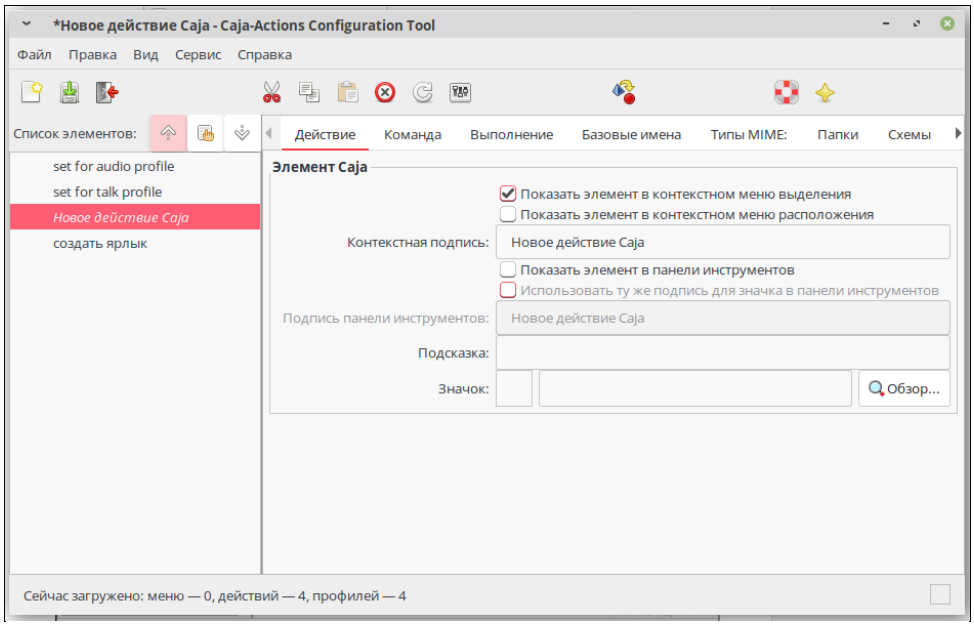
После написания и расположения скрипта в директории требуется сделать его исполняемым. Для этого откройте параметры файла и поставьте галочку:



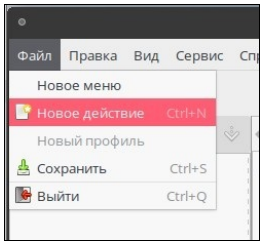
Пример отображения bash-скрипта в меню:



Утилита **Caja-Actions** находится в *«Меню» — «Параметры» - «Настройка действий меню файлового менеджера Caja»*. Внешний вид утилиты при запуске выглядит следующим образом:

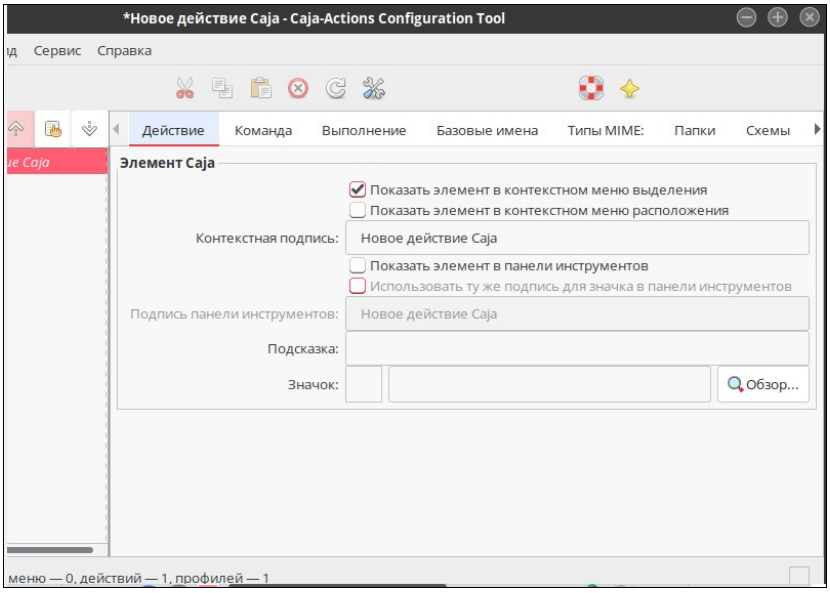


Если вы хотите создать новое меню или новое действие, нажмите на «*Файл*» и выберите нужный вариант.

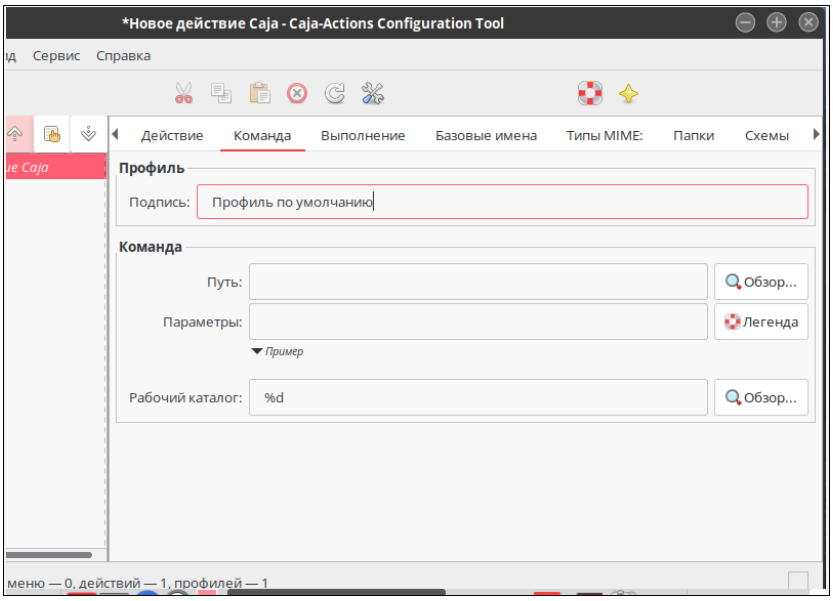


При создании нового действия оно будет отображаться в списке элементов, также откроются вкладки: *«Действие», «Команда», «Выполнение», «Базовые имена», «Типы MIME», «Папки», «Схемы», «Характеристики», «Среда», «Свойства»*. Рассмотрим каждую более подробно.

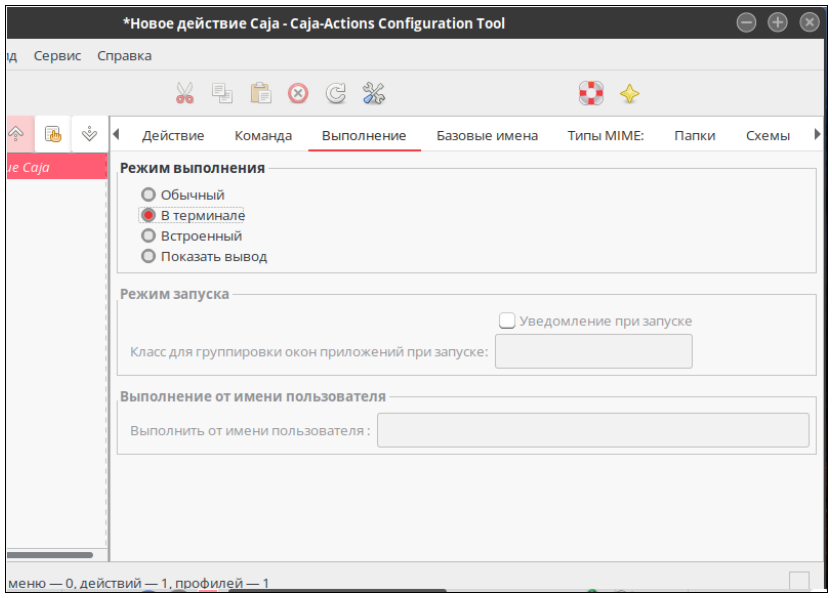
На вкладке «*Действие*» можно выбрать главные характеристики текущего элемента. Здесь можно выбрать, показывать ли элемент в контекстном меню, в панели инструментов; можно задать имя выбранному действию, а также выбрать значок.



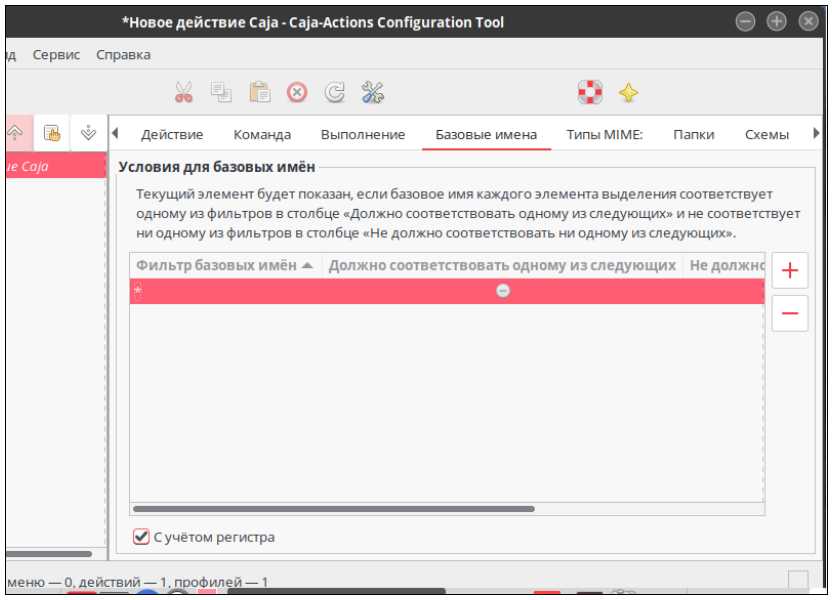
На вкладке «*Команда*» можно выбрать команду для выполнения и её параметры. Здесь можно указать путь к команде, параметры команды и можно выбрать рабочий каталог, в котором следует запустить команду.



На вкладке «*Выполнение*» можно указать, как именно следует выполнить команду. Можно выбрать режим выполнения: *«Обычный», «В терминале», «Встроенный», «Показать вывод»*.

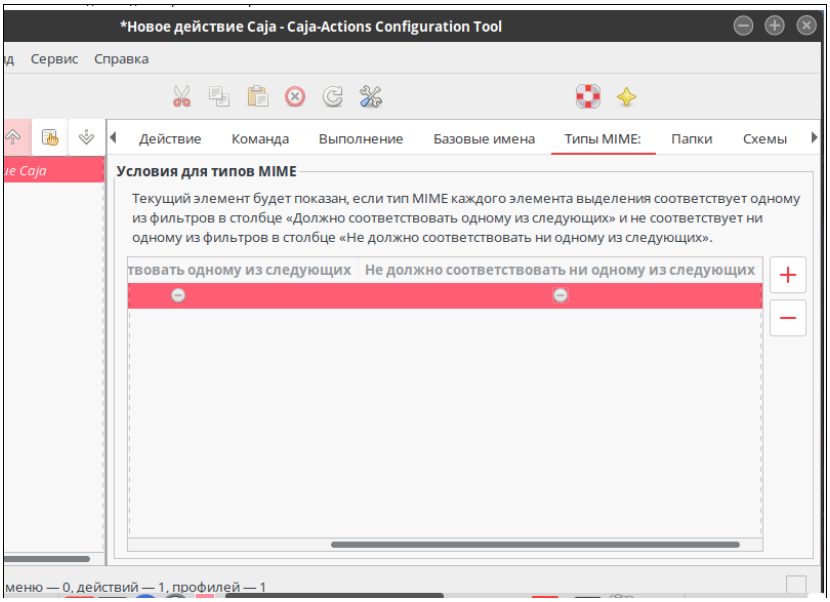


На вкладке «*Базовые имена*» можно определить, для каких базовых имён текущий элемент будет показан в контекстном меню *Caja*, а для каких - не будет. Отображение определяется столбцами «*Должно соответствовать одному из следующих имен*» и «*Не должно соответствовать ни одному из следующих имен*».

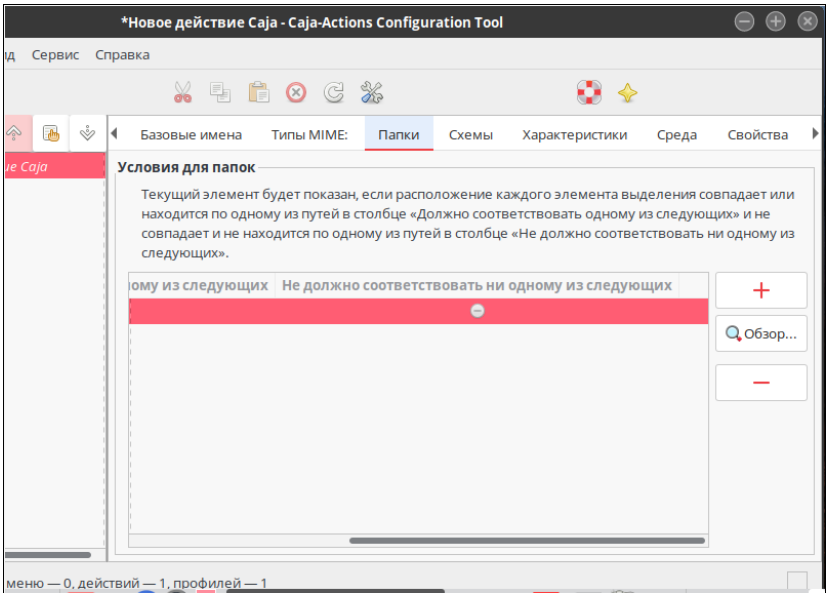


На вкладке «*Типы MIME*» можно определить, для каких типов **MIME** текущий элемент будет показан в контекстном меню *Caja*. Также типы *MIME* можно использовать в отрицательном варианте, чтобы указать, для какого типа объектов элемент не должен

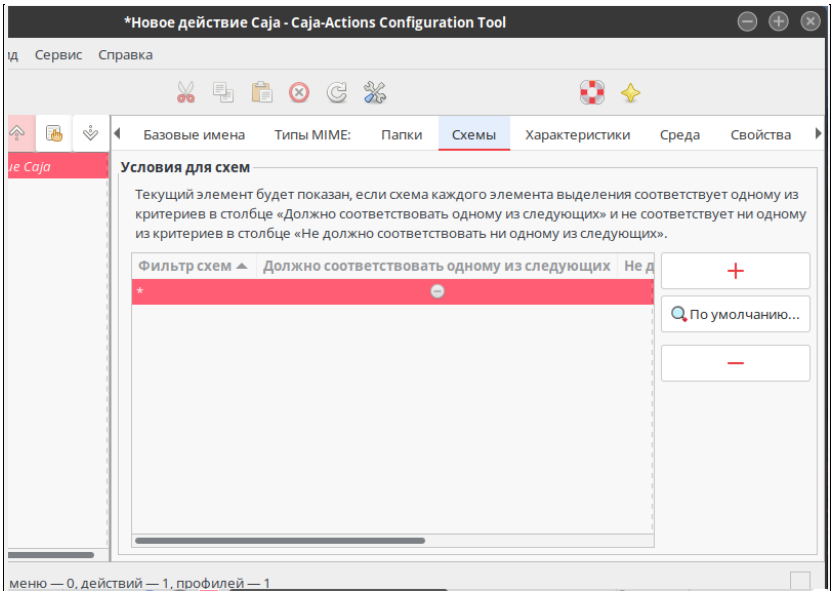
отображаться.



На вкладке «*Папки*» можно определить, где должны находиться текущие выбранные файлы, чтобы элемент был показан в контекстном меню *Caja*. Можно указать, в каких папках он не должен отображаться.

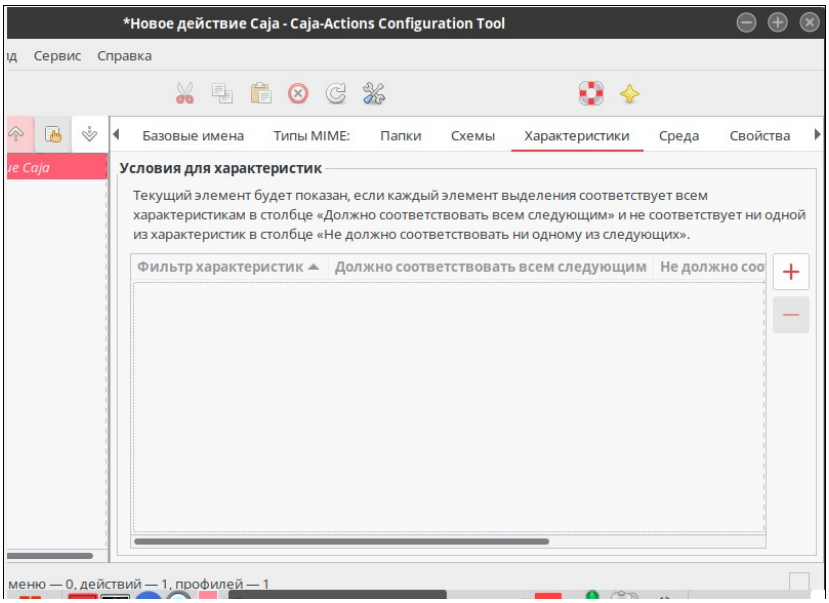


На вкладке «*Схемы*» можно определить, каким схемам должны удовлетворять выбранные файлы, чтобы элемент был показан в контекстном меню *Caja*. Можно указать для каких схем элемент не должен отображаться.

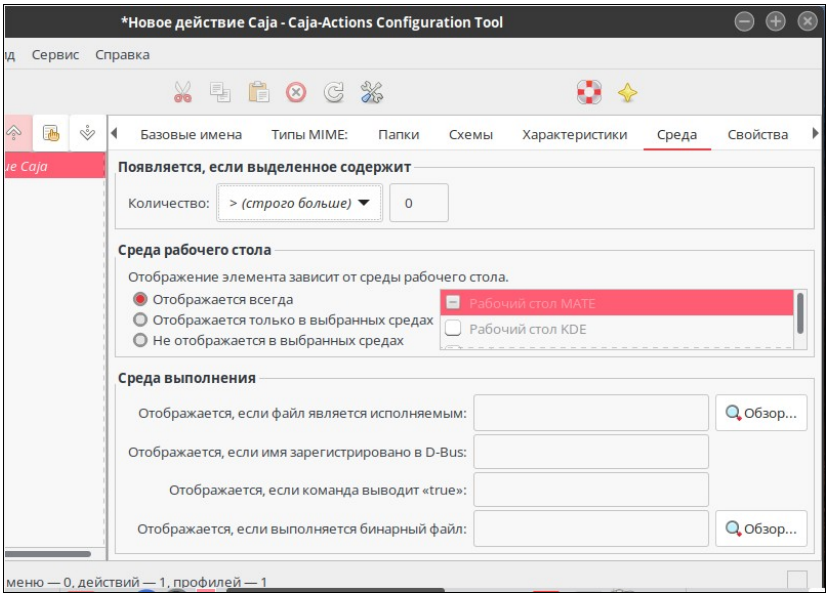


На вкладке «*Характеристики*» можно определить, каким характеристикам должны удовлетворять текущие выбранные файлы, чтобы

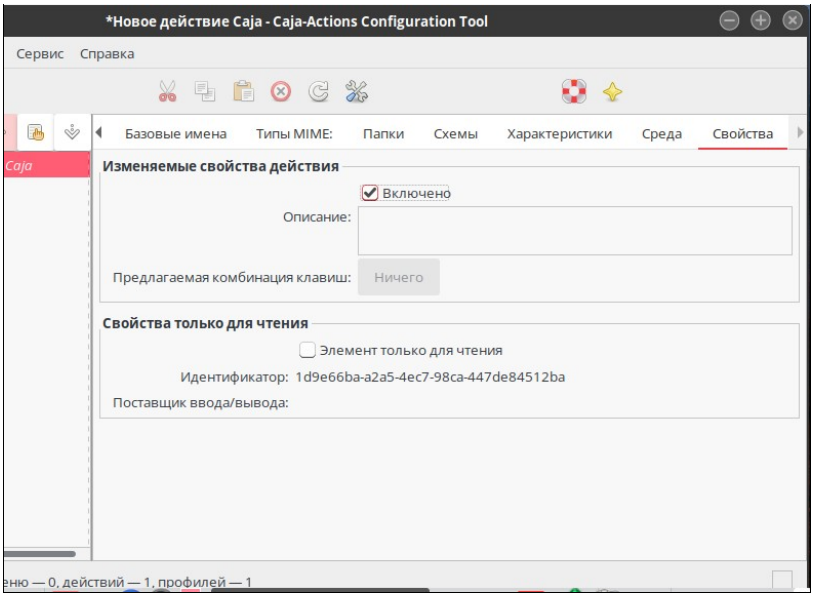
элемент был показан в меню *Caja*. Также можно указать, для каких характеристик элемент не должен отображаться.



На вкладке «*Среда*» можно определить расширенные условия, которым должны удовлетворить текущие выбранные файлы, чтобы элемент был показан в меню *Caja*. Здесь же можно выбрать количество элементов, при котором они будут показаны, среду рабочего стола и среду выполнения.



На вкладке «*Свойства*» можно изменить некоторые свойства и получить доступ к некоторой неизменяемой информации.



Добавление нового действия

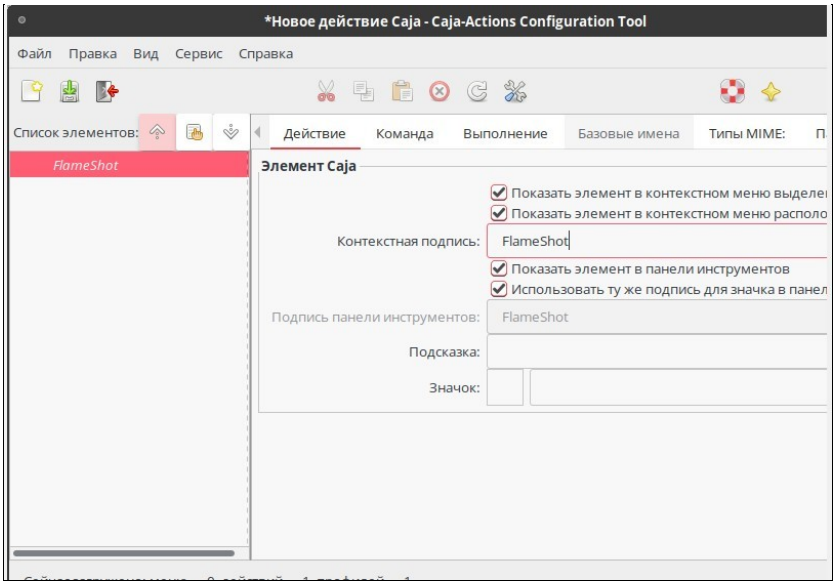
Рассмотрим добавление **FlameShot** в качестве быстрого доступа с помощью правой кнопки мыши.

Вы можете подробнее ознакомиться с примером создания нового действия, просмотрев наши обучающие видео:

- на **RuTube** — Создание собственных действий в меню Caja в РЕД ОС 7.3 ;
- в **Яндекс.Дзен** — Создание собственных действий в меню Caja в РЕД ОС 7.3 ;
- в **VK Видео** — Создание собственных действий в меню Caja в РЕД ОС 7.3 .

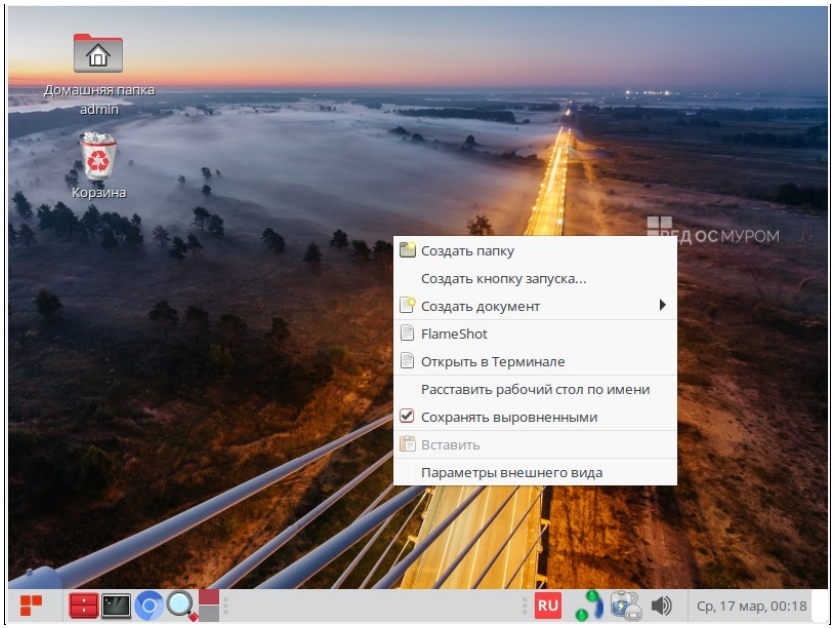
На наших каналах вы также сможете найти много другой полезной информации.

Добавим новое действие, назовём его *FlameShot* и установим галочки во всех рекомендуемых полях.



Затем необходимо указать путь к утилите и нажать кнопку «Сохранить».

После сохранения действия нажимаем на рабочем столе правой кнопкой мыши, появится контекстное меню, в котором будет отображаться наше созданное новое действие «*FlameShot*».



После нажатия на него он автоматически запустится.

Добавление кнопки «Отправить на рабочий стол»

Для добавления новой кнопки нам понадобится скрипт, который будет создавать кнопку на рабочий стол, если это исполняемый файл; если это медиа-файлы или какие-либо другие файлы, понадобится ссылка.

Создадим новый скрипт со следующим содержимым:

```
nano make_link.sh
```

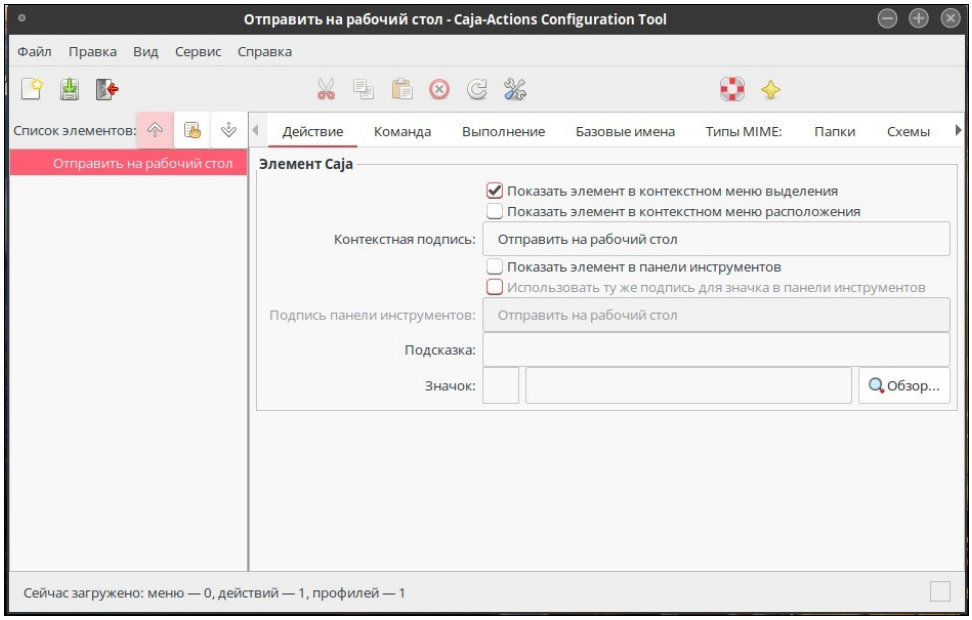
```
#!/bin/bash
fullname=$1
var=$1
name=$(basename "$var")
case $name in
*.sh|*.py|*pyc|*.pyd|*.jar|*.cpp)
echo -e "#!/usr/bin/env xdg-open\n[Desktop Entry]\nVersion=1.0\
nType=Application\nTerminal=false\nIcon=/\nIcon[ru_RU]=/\nName[ru_RU]=$name\
nExec='$var'\nName=$name\n" > ~/Рабочий\ стол/$name.desktop
chmod +x ~/Рабочий\ стол/$name.desktop
;;
*)
ln -sf "$var" ~/Рабочий\ стол/
;;
esac
```

Затем установим сохраненному скрипту права на исполнение следующей командой:

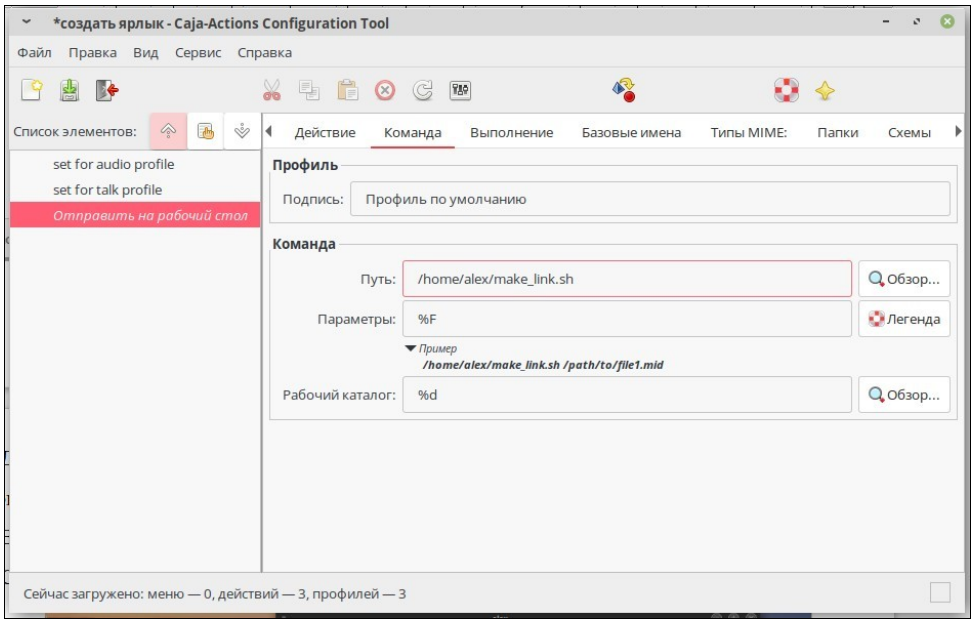
```
chmod +x make_link.sh
```

После этого можно приступать к выполнению готового скрипта в утилите *Caja-Actions*.

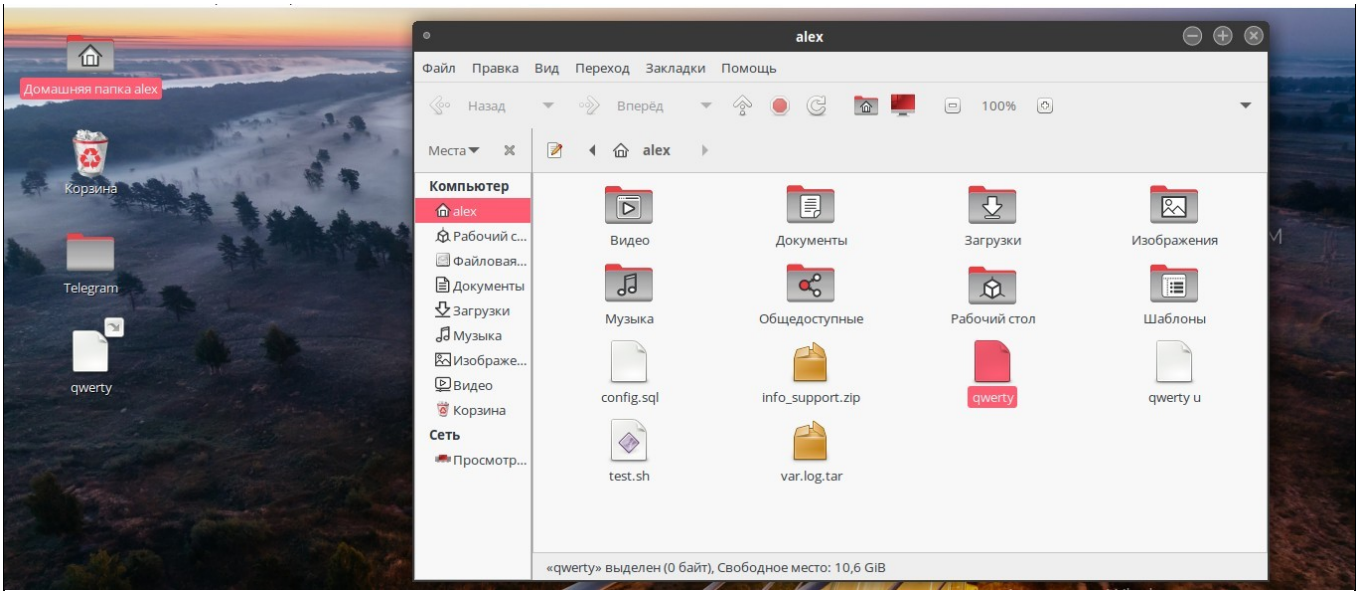
Добавим новое действием и назовем его «*Отправить на рабочий стол*», поставим галочку в поле «*Показывать элемент в контекстном меню выделения*».



Далее переходим на вкладку «*Команда*», указываем путь - «**/home/alex/make_link.sh**», параметры - «**%F**», рабочий каталог - «**%d**». Сохраняем действие.



После этого заходим в любую директорию (рассмотрим на примере домашней директории - **/home/alex**), выбираем в ней любой файл и нажимаем на него правой кнопкой мыши, выбираем *«Caja-Actions actions»* – *«Отправить на рабочий стол»*. После этого создаётся ссылка (ярлык) на рабочем столе.



caja-extension-actions

Копирование и перемещение файлов
Отправить на рабочий стол
Распечатать файл
Стереть этот каталог
Скопировать расположение
Добавить в шаблоны
Сравнение контрольной суммы
ГОСТ шифрование
Кнопка запуска smb-каталога

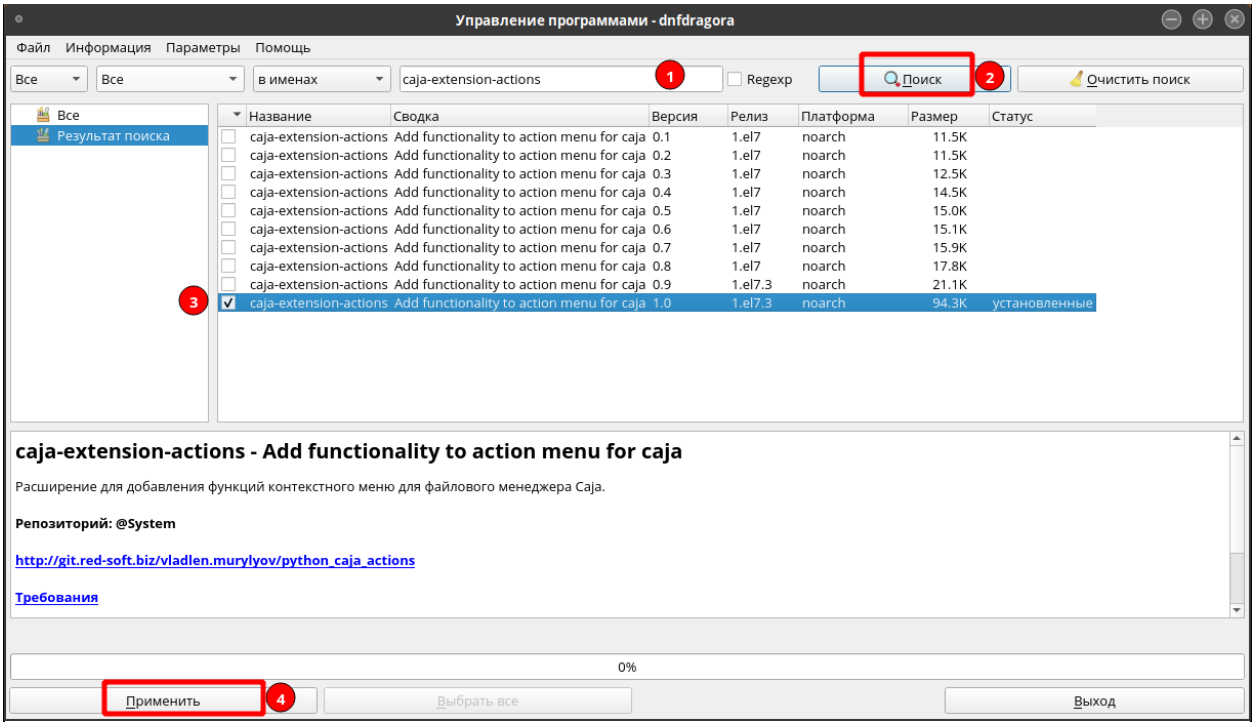
Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** caja-extension-actions-1.0-1

Расширения для файлового менеджера **caja** представляют собой новые пункты в контекстном меню.

Установить расширения можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**caja-extension-actions**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install caja-extension-actions
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки потребуется выполнить команду обновления **caja**:

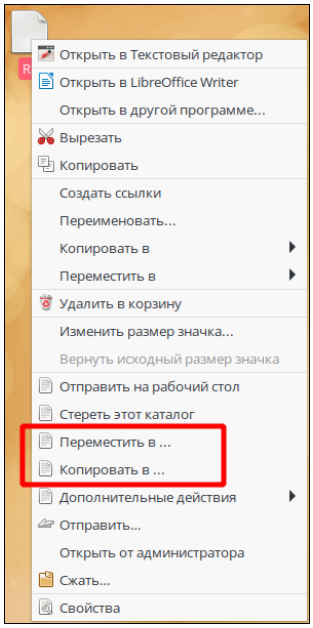
```
caja -q
```

Для применения изменений можно также выйти из учетной записи пользователя и авторизоваться снова.

Копирование и перемещение файлов

Расширение позволяет копировать или перемещать необходимые файлы или каталоги в другие каталоги.

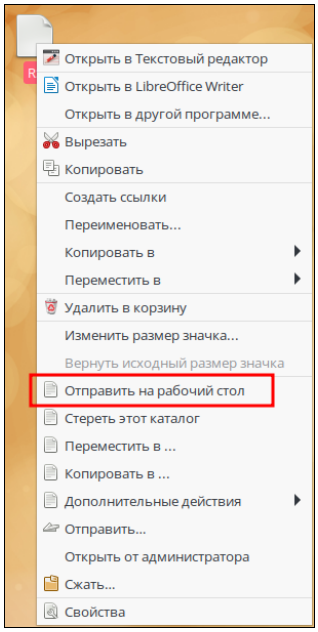
Пункты в контекстном меню, соответствующие данному расширению, выглядят следующим образом:



Отправить на рабочий стол

Данное расширение создает символическую ссылку (ярлык) на файл или каталог.

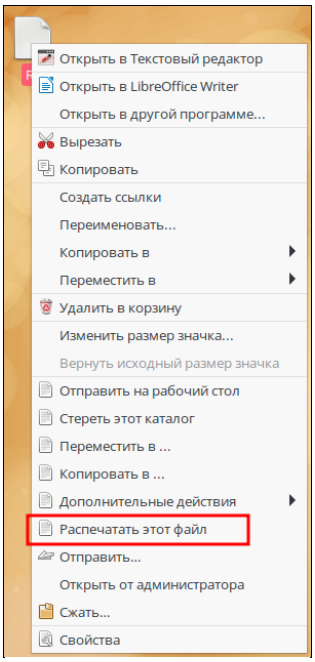
Пункт в контекстном меню, соответствующий данному расширению, выглядит следующим образом:



Распечатать файл

Данное расширение производит передачу файла для печати на принтер, который установлен в системе по умолчанию. Настройки печати при этом тоже задаются по умолчанию.

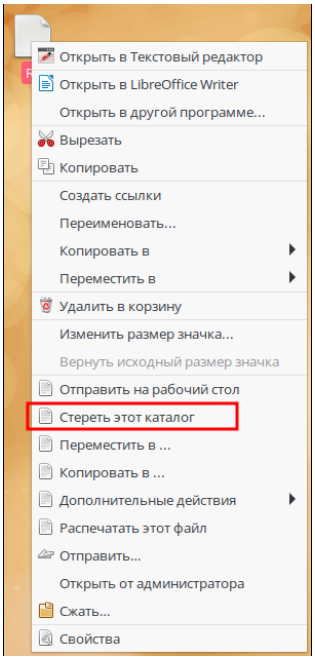
Пункт в контекстном меню, соответствующий данному расширению, выглядит следующим образом:



Стереть этот каталог

Данное расширение позволяет безопасно стереть данные о файле или каталоге.

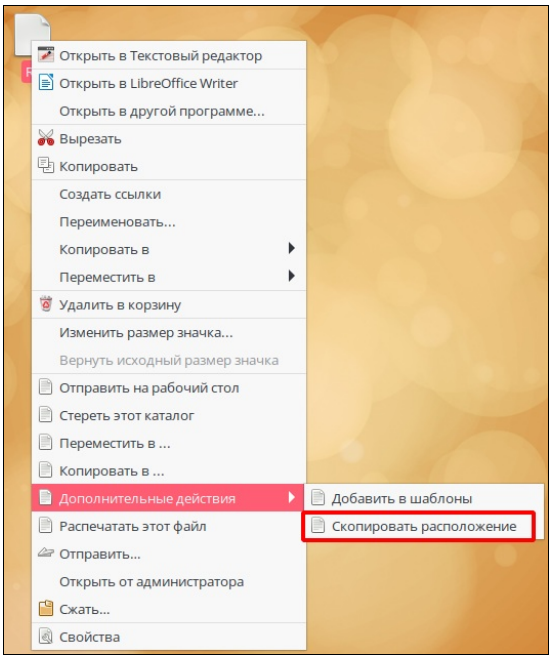
Пункт в контекстном меню, соответствующий данному расширению, выглядит следующим образом:



Скопировать расположение

Данное расширение сохраняет в буфер обмена путь до выбранного файла или каталога.

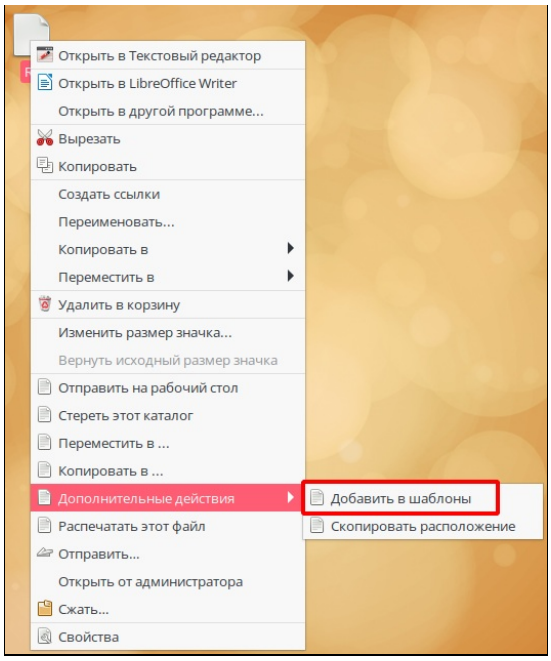
Пункт в контекстном меню, соответствующий данному расширению, выглядит следующим образом:



Добавить в шаблоны

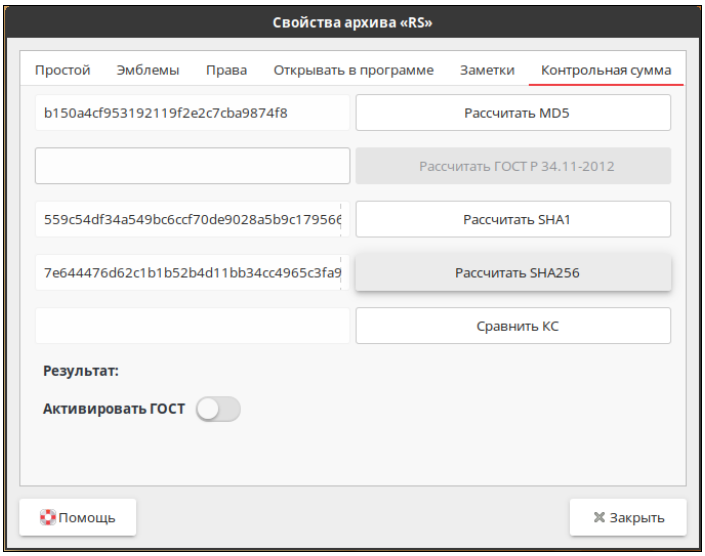
Данное расширение позволяет пользователю добавлять в папку шаблонов выбранные им файлы. Данные файлы потом можно использовать из контекстного меню – «**Создать документ**».

Пункт в контекстном меню, соответствующий данному расширению, выглядит следующим образом:

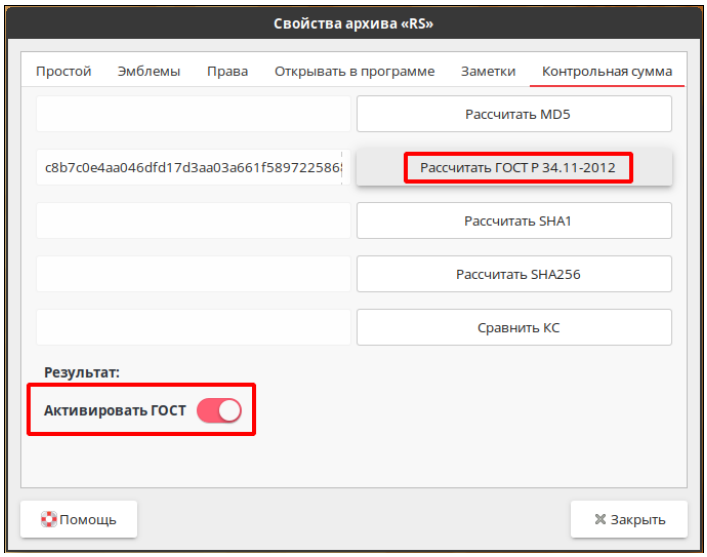


Сравнение контрольной суммы

Данное расширение доступно из пункта контекстного меню «**Свойства**».

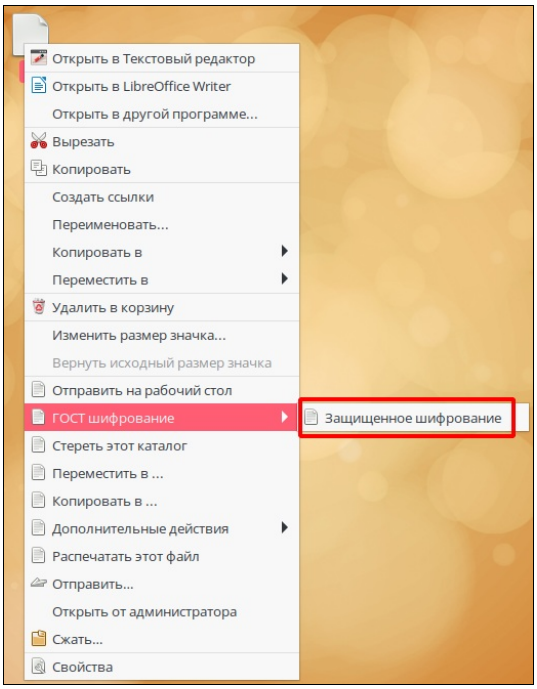


Также данное расширение активирует пункт контекстного меню ГОСТ шифрование. После перемещения ползунка в режим «**ON**» поля «**Активировать ГОСТ**» станет доступен вариант расчета КС по ГОСТ.

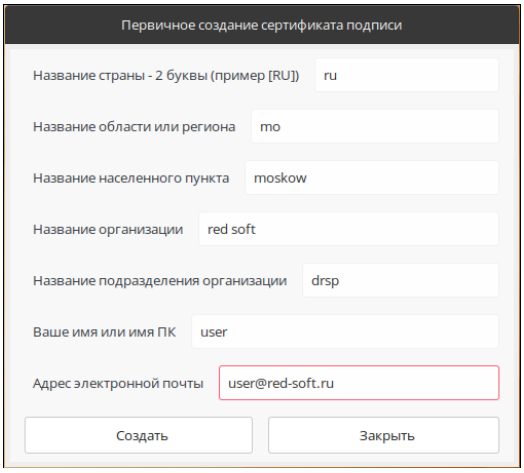


ГОСТ шифрование

После активации ГОСТ в контекстном меню станет доступным пункт «**ГОСТ шифрование**» — «**Защищенное шифрование**».



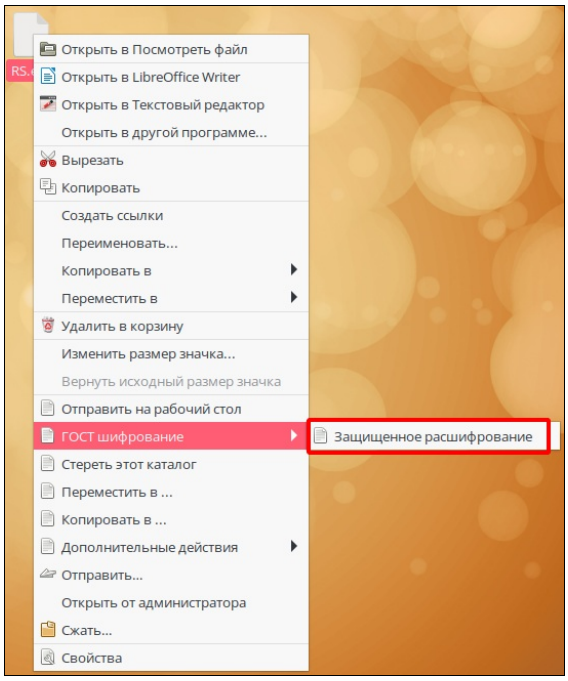
При первичной инициализации данное расширение предложит создать сертификат, который будет использоваться для шифрования и расшифрования. Заполните необходимые поля и нажмите кнопку «**Создать**».



В результате будет создан зашифрованный файл с расширением **.enc** ().

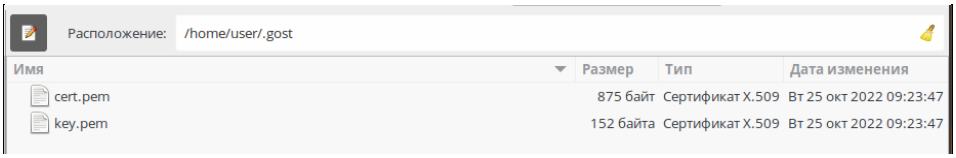


Для расшифрования данного файла в контекстном меню необходимо выбрать пункт «**ГОСТ шифрование**» — «**Защищенное расшифрование**».



При попытке расшифрования данного файла на другом ПК будет получен нечитаемый файл. Перед расшифрованием рекомендуется создавать копию файла.

Расшифрование производится сертификатом, который располагается по пути **~/.gost/**.



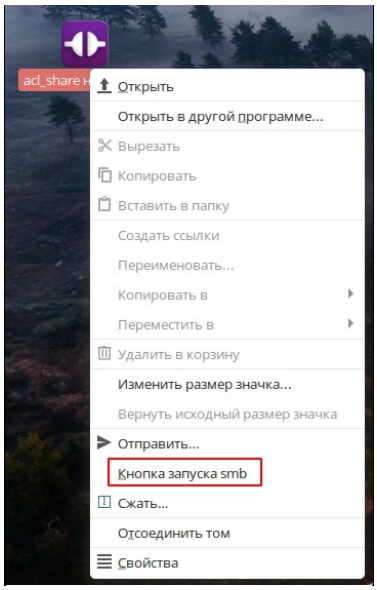
Соответственно, при передаче файла на другой ПК и попытке расшифрования — потребуется копирование данной папки в домашнюю директорию другого пользователя.

Кнопка запуска smb-каталога

Данное расширение доступно для каталогов, которые подключены непосредственно из **caja**. Т.е. когда в строке пути был введен формат smb://<имя_компьютера>/<имя_папки>.

Где **<имя_компьютера>** – краткое или полное имя ПК в сети, **<имя_папки>** – имя опубликованного каталога.

Расширение доступно из контекстного меню на рабочем столе пользователя.



Fdupes – программа проверки наличия дубликатов файлов

Fdupes – это программа для сканирования каталогов на наличие дубликатов файлов. Она может сканировать заданный каталог, выводя список найденных дубликатов, автоматически их удаляя или требуя подтверждения удаления.

Вы можете подробнее ознакомиться с работой программы **fdupes**, просмотрев наши обучающие видео:

- на **RuTube** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **Яндекс.Дзен** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **VK Видео** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов.

На наших каналах вы также сможете найти много другой полезной информации.

Устанавливается командой:

```
dnf install fdupes
```

Для поиска *дубликатов файла* выполните следующую команду:

```
fdupes /media/files

/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
```

Для поиска *повторяющихся файлов* с учетом вложенных каталогов используется параметр **-r**:

```
fdupes -r /media/

/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
```

Для просмотра *размеров дубликатов*, найденных в папке, используется параметр **-S**:

```
fdupes -S /media/files

10 bytes each:
/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
```

Для поиска *дубликатов файлов в нескольких директориях* задаются нужные каталоги по очереди:

```
fdupes -r /dev /media

/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
/dev/mapper/document
/dev/mapper/document2
```

Для *удаления дубликатов* файлов используется параметр **-d**:

```
fdupes -d /dev/mapper/ /media/files/

Set 1 of 2:
   1 [-] /media/files/file3.txt
  2 [-] /media/files/file2.txt
  3 [+] /media/files/file1.txt
 4 [-] /media/files/file4.txt
```

```
   5 [-] /media/files/file5.txt

Set 2 of 2:
   1 [+] /dev/mapper/document
   2 [-] /dev/mapper/document2

( Preserve files [1 - 2, all, help] ):1
```

В появившемся списке необходимо отметить файлы, которые удалять не нужно, и нажать «**DELETE**», программа удалит не помеченные файлы.

FSlint – графическая утилита поиска дубликатов файлов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** fslint-2.47-1

FSlint — программа для очистки файловой системы от «мусорных» файлов. **FSlint** можно применять для поиска и удаления одинаковых файлов (дубликатов файлов), битых символических ссылок, пустых директорий, файлов с некорректными именами, временных файлов и прочего.

Вы можете подробнее ознакомиться с работой в программе **FSlint**, просмотрев наши обучающие видео:

- на **RuTube** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **Яндекс.Дзен** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **VK Видео** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

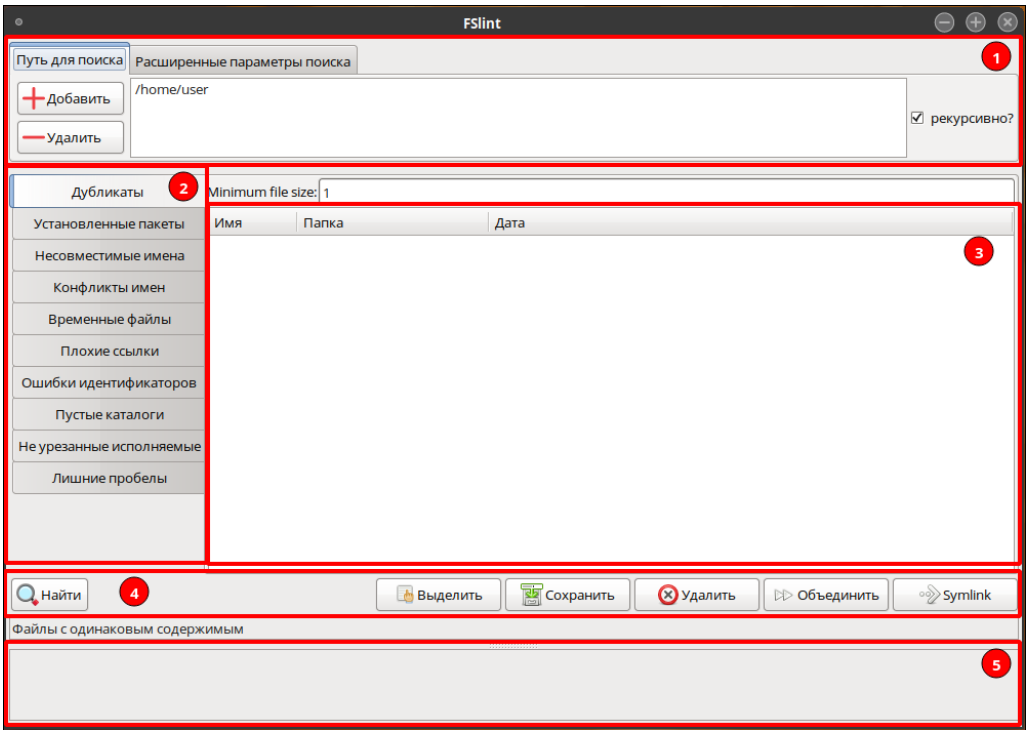
и выполните команду:

```
dnf install fslint
```

После установки программа будет доступна из «**Главного меню**» - «**Системные**» - «**FSlint**» или через консоль:

```
fslint-gui
```

Окно программы выглядит следующим образом:



1. Добавление директорий, в которых необходимо осуществить поиск файлов. Доступна вкладка с расширенными параметрами поиска, где можно исключить некоторые пути и установить дополнительные параметры.

2. Выбор критерия поиска.

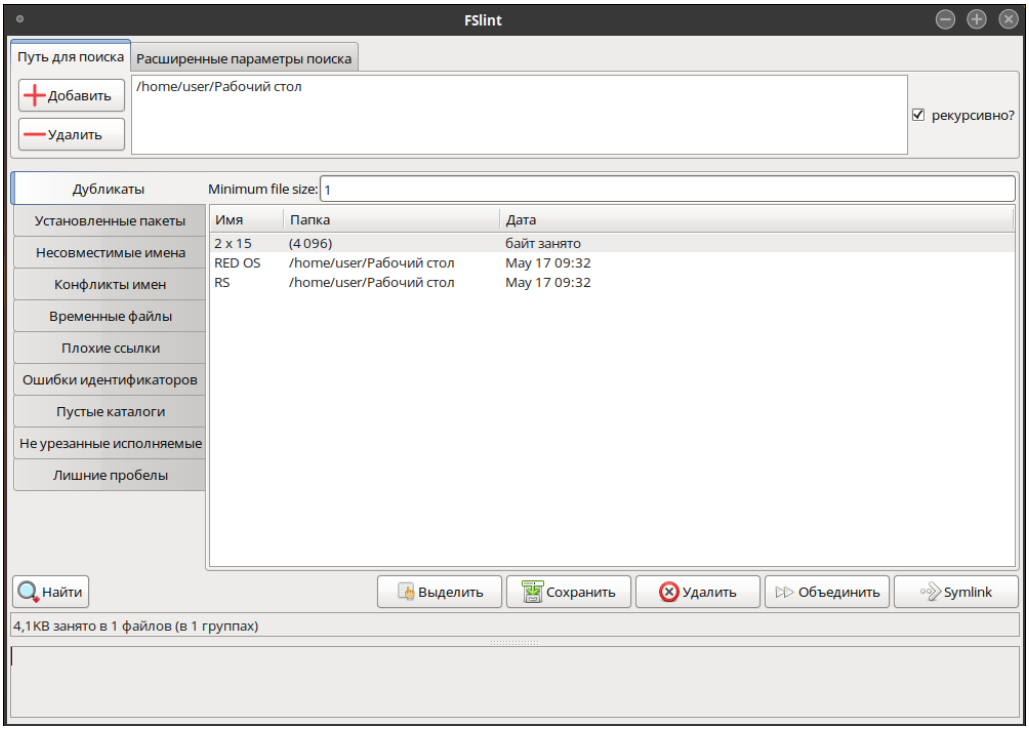
3. Поле для вывода результата поиска.

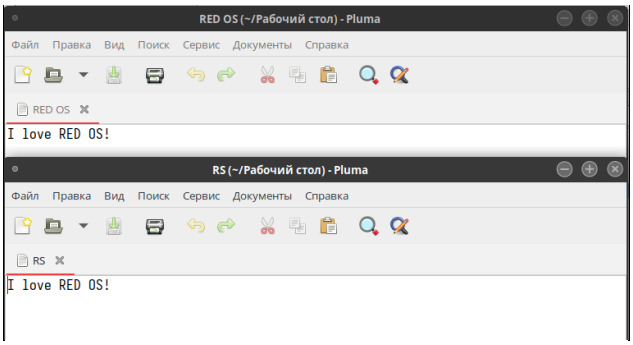
4. Доступные для выполнения команды над файлами.

5. Информационное поле.

Для осуществления поиска дубликатов файлов необходимо указать директории, по которым будет осуществляться поиск, нажав кнопку «**Добавить**». Затем в критериях поиска выбрать «**Дубликаты**» и нажать кнопку «**Найти**».

Результат поиска будет выглядеть примерно следующим образом:





Утилиты для архивирования, восстановления и копирования файлов в терминале

dd
tar
zip
unrar
rsync
p7zip

Вы можете подробнее ознакомиться с работой утилит для архивирования, копирования и восстановления файлов, просмотрев наши обучающие видео:

- на **RuTube**:
  - Консольные утилиты для работы с архивами.
- в **Яндекс.Дзен**:
  - Копирование и клонирование дисков;
  - Консольные утилиты для работы с архивами.
- в **VK Видео**:
  - Консольные утилиты для работы с архивами.

На наших каналах вы также сможете найти много другой полезной информации.

dd

Команда для копирования системного раздела диска в файл с условным названием /media/device/sda.bin:

```
dd if=/dev/sda1 of=/media/device/sda1.bin bs=4096
```

С учетом возможности перенаправления стандартного ввода/вывода команда dd позволяет применять для копирования алгоритмы сжатия или защитного преобразования:

```
dd if=/dev/sda1 bs=4096 | gzip > /media/device/sda1.bin.gz2
```

Команда для восстановления системного раздела диска (для этого потребуется загрузиться с отдельного диска, и примонтировать носитель, на котором был размещен файл с образом):

```
dd if=/media/mountpoint/sda1.bin of=/dev/sda1 bs=4096
```

tar

tar упаковка:

```
tar -cf jpg.tar *.jpg
```

или указав каталог:

```
tar -cf jpg.tar ~/files
```

распаковка:

```
tar -xvf archive.tar
```

в папку:

```
tar -xvf archive.tar -C /path
```

gzip сжатие:

```
tar -cvzf files.tar.gz ~/files
```

распаковка:

```
tar -xzvf archive.tar.gz
```

bzip2 сжатие:

```
tar -cvjf files.tar.bz2 ~/files
```

распаковка:

```
tar -xjvf /path/to/archive.tar.bz2
```

в папку:

```
tar -xjvf archive.tar.bz2 -C /path/to/folder
```

Создание архива на удаленной машине

```
tar -cvpz ./ | ssh root@10.81.1.190 "( cat >  /home/user/ssh_backup.tar )"\
```

Синхронизация папок

zip

zip сжатие:

```
zip file_archive.zip -r /var/log/
zip file_archive.zip file1.txt file2.log
```

Распаковка:

```
unzip file_archive.zip
unzip file_archive.zip -d /tmp
```

unrar

Для работы с архивами rar установите пакет:

```
sudo dnf install unrar
```

Распаковка:

```
unrar x archive.rar
unrar x archive.rar ./folder
```

rsync

Rsync - это программное обеспечение с открытым исходным кодом, которое можно использовать для синхронизации файлов и папок с локального компьютера на удаленный и наоборот. Примечательная особенность Rsync - возможность передавать зашифрованные файлы с помощью SSH и SSL. Кроме того, здесь передача файлов выполняется в один поток, в отличие от других подобных программ, создающий отдельный поток для передачи каждого файла. Это увеличивает скорость и убирает дополнительные задержки, которые становятся проблемой при передаче большого количества маленьких файлов.
Основные параметры rsync:
`-v` - Выводить подробную информацию о процессе копирования;
`-q` - Минимум информации;
`-c` - Проверка контрольных сумм для файлов;
`-a` - Режим архивирования, когда сохраняются все атрибуты оригинальных файлов;
`-R` - Относительные пути;
`-b` - Создание резервной копии;
`-u` - Не перезаписывать более новые файлы;
`-l` - Копировать символьные ссылки;
`-L` - Копировать содержимое ссылок;
`-H` - Копировать жесткие ссылки;
`-p` - Сохранять права для файлов;
`-g` - Сохранять группу;
`-t` - Сохранять время модификации;
`-x` - Работать только в этой файловой системе;
`-e` - Использовать другой транспорт, например, ssh;

-z - Сжимать файлы перед передачей;
--delete - Удалять файлы которых нет в источнике;
--exclude - Исключить файлы по шаблону;
--recursive - Перебирать директории рекурсивно;
--no-recursive - Отключить рекурсию;
--progress - Выводить прогресс передачи файла;
--stat - Показать статистику передачи;
--version - Версия утилиты.
Rsync позволяет синхронизировать файлы и папки в пределах одной машины. Давайте сначала рассмотрим использование rsync для синхронизации файла на локальном компьютере:

```
rsync -zvh file /tmp/backups/
```

Синхронизация папок rsync выполняется так же, как и файлов:

```
rsync -zvh /var/account/* /tmp/backups/
```

Если вы хотите, чтобы все атрибуты файлов, такие, как дата изменения и создания сохранялись, необходимо использовать опцию -a:

```
rsync -azvh /var/account/* /tmp/backups/
```

Синхронизация файлов производится следующим образом. Скопируем локальную папку files, на удаленный сервер:

```
rsync -avz /home/files root@10.81.1.190:/home/user
```

По умолчанию rsync попытается использовать транспорт ssh. Если вы хотите использовать ранее созданный сервер rsync, нужно указать это явно:

```
rsync -avz /home/files rsync://10.81.1.190:/share
```

Точно также можно синхронизировать файлы с rsync из удаленного сервера:

```
rsync -avz root@10.81.1.190:/home/ /home/files/
```

p7zip

7-Zip — свободный файловый архиватор с высокой степенью сжатия данных благодаря формату 7z с компрессией LZMA. Кроме формата 7z поддерживает также ZIP, GZIP, BZIP2 и TAR. Может распаковать множество других форматов, например CAB, CHM, DEB, ISO, LZMA, MSI, RAR и другие. Формат 7z достаточно популярен среди архивов, поэтому имеет смысл иметь поддержку 7z в системе, а также создавать свои архивы в виде 7z формата, ибо сжатие с помощью 7z на 30-50% лучше, чем сжатие с помощью ZIP.
Основные параметры:
a – Создание архива, добавить файлы в архив
b - Бенчмарк
d - Удалить файлы из архива
e - Извлечь файлы из архива (без использования имён директорий)
l - Список содержимого архива
t - Тестировать архив на целостность
u - Обновить файлы в архиве
x - Извлечь файлы с полными путями

Для упаковки в архив archive.7z файлов file, file1, file2 в директории /home/user/files, выполните команду:

```
7z a archive.7z file file1 file2
```

Для упаковки в архив archive.7z всего содержимого директории /home/user/files, выполните команду(в текущем каталоге):

```
7z a archive.7z
```

Файл archive.7z будет создаваться в текущей директории. Можно использовать абсолютный/относительный путь, например:

```
7z a /home/user/archive.7z
```

Опция -t определяет формат архива на выходе. Например -t7z устанавливает 7z формат (он же используется по умолчанию). Также можно определить иной формат архива: zip, gzip, bzip2 или tar. Распаковка архива в текущую директорию:

```
7z x archive.7z
```

Чтобы распаковать архив в определенную директорию используется опция -o, за которой без пробела указывается путь до директории:

```
7z x archive.7z -o./files
```

Для просмотра содержимого архива используется команда:

```
7z l archive.7z
```

Чтобы проверить целостность архива (проверить, что архив «не битый») используется команда:

```
7z t archive.7z
```

Сохранение в файл вывода консоли

Перенаправление стандартного вывода
Перенаправление вывода ошибок
Перенаправление стандартного вывода и стандартного вывода ошибок в один файл
Перенаправление стандартного ввода
Конвейеры

Многие программы выводят в консоль какую-либо информацию. Этот вывод часто делится на два типа:

1. Результаты работы программы, т.е. данные, для получения которых и создавалась эта программа;
2. Сообщения о состоянии или об ошибках.

Например, если посмотреть на вывод программы `ls`, можно увидеть, что она выводит на экран результаты своей работы и иногда сообщения об ошибках. Согласно центральной идее Unix, что «всё — есть файл», программы, в действительности, выводят свои результаты в специальный файл, который называется стандартным выводом или стандартным потоком вывода (часто обозначается как **stdout**), а сообщения о состоянии — в специальный файл стандартный вывод ошибок или поток ошибок (**stderr**). По умолчанию оба эти потока связаны с экраном и не сохраняются на диске.

Кроме того, многие программы принимают ввод из специального файла с названием стандартный ввод или стандартный поток ввода (**stdin**), который по умолчанию связан с клавиатурой.

Механизм перенаправления ввода/вывода позволяет изменять направление вывода и ввода. Обычно вывод осуществляется на экран, а ввод — с клавиатуры, но механизм перенаправления ввода/вывода позволяет изменить этот порядок.

Вы можете подробнее ознакомиться с перенаправлением вывода консоли в файл, просмотрев наши обучающие видео:

- на **RuTube** — Перенаправление в bash;
- в **Яндекс.Дзен** — Перенаправление в bash;
- в **VK Видео** — Перенаправление в bash.

На наших каналах вы также сможете найти много другой полезной информации.

Перенаправление стандартного вывода

Механизм перенаправления ввода/вывода позволяет явно указать, куда должен осуществляться стандартный вывод. Чтобы перенаправить стандартный вывод в файл вместо экрана, нужно добавить в команду оператор перенаправления «**>**» и имя файла. Например, можно сообщить командной оболочке, что она должна направить вывод команды `ls` в файл вместо экрана:

```
ls /usr/bin > listing.txt
```

Просмотрев содержимое файла (например, командной `cat listing.txt`), можно увидеть ту же информацию, как если бы вывод осуществлялся непосредственно в консоль.

Теперь попробуйте выполнить предыдущую команду, но для другого каталога, например:

```
ls /etc > listing.txt
```

Затем просмотрите содержимое файла. Вы увидите, что старая информация в нём была перезаписана. Это объясняется тем, что при перенаправлении вывода с помощью оператора «**>**» файл назначения всегда перезаписывается с самого начала.

Примечание.

Если понадобится очистить какой-нибудь файл (или создать новый, пустой файл), это можно сделать с помощью команды:

```
> listing.txt
```

Простой оператор перенаправления, без предшествующей ему команды, очистит существующий файл или создаст новый, пустой файл.

Для добавления вывода в конец существующего файла без перезаписи необходимо использовать оператор перенаправления «**>>**»:

```
ls /etc >> listing.txt
```

Оператор «**>>**» просто добавит результаты в конец файла. Если файл не существует, он будет создан, как при использовании оператора «**>**».

Перенаправление вывода ошибок

При попытке перенаправить вывод с указанием имени несуществующего каталога командой:

```
ls /folder > listing.txt
```

На экран будет выведено следующее сообщение:

```
ls: невозможно получить доступ к '/folder': Нет такого файла или каталога
```

Однако сообщение об ошибке выведено в терминал, а не в файл. Дело в том, что обычно программы не выводят сообщения об ошибках в стандартный вывод — они выводят сообщения об ошибках в поток ошибок.

Поскольку перенаправлен только стандартный вывод, а стандартный вывод ошибок — нет, сообщение об ошибке появилось на экране терминала.

Перенаправление стандартного вывода ошибок осуществляется не так просто, как стандартного вывода. Чтобы перенаправить поток ошибок, нужно указать его *дескриптор файла*.

Первые три потока (иными словами — стандартных файла) были уже упомянуты как стандартный ввод, вывод и вывод ошибок. К ним можно обратиться по их уникальным цифровым идентификаторам, которые и называются **файловыми дескрипторами**:

Стандартный файловый поток	Дескриптор
Ввода	0
Вывода	1
Ошибок	2

Командная оболочка ссылается на стандартные потоки как на файлы по их дескрипторам (иногда говорят, «номерам потока»). Так как стандартному потоку ошибок соответствует файловый дескриптор **2**, можно перенаправить его, например, таким образом:

```
ls /folder 2> listerrors.txt
```

Примечание.

Номер файлового дескриптора помещается непосредственно перед оператором перенаправления, без пробела!

Теперь на экран не выводится сообщение об ошибке.

Перенаправление стандартного вывода и стандартного вывода ошибок в один файл

Для перенаправления всего вывода в один файл необходимо поток ошибок направить в поток вывода, а его, в свою очередь, перенаправить в файл. Например:

```
ls /etc > listing.txt 2>&1
```

Примечание.

Обратите внимание, что порядок перенаправления играет важную роль! Перенаправление стандартного вывода ошибок всегда должно производиться **после** перенаправления стандартного вывода, иначе команда сработает не так, как ожидается.

Если порядок перенаправления изменить, как показано ниже, стандартный вывод ошибок будет перенаправлен на экран:

```
ls /etc 2>&1 > listing.txt
```

Версия **bash**, имеющаяся в РЕД ОС, поддерживает и другой, более короткий способ написания данного перенаправления:

```
ls /etc &> listing.txt
```

В примере используется единственный оператор **&>**, перенаправляющий стандартный вывод и стандартный вывод ошибок в файл **listing.txt**. Аналогично можно перенаправить стандартный вывод и стандартный вывод ошибок с добавлением в конец одного и того же файла:

```
ls /etc &>> listing.txt
```

> **Примечание.**
>
> Между символами в операторе перенаправления не должно быть пробелов!

Иногда случаются ситуации, когда вывод программы совсем не нужен, его желательно не просто перенаправить в файл, а перенаправить в никуда. Для этого достаточно указать в качестве целевого файла для перенаправления вывода специальный файл `/dev/null`. Этот файл представляет системное устройство, называемое *битоприёмником* (**bit bucket**), которое принимает любой ввод и ничего с ним не делает. Например:

```
ls /etc > /dev/null
ls /etc 2> /dev/null
ls /etc &> /dev/null
```

Перенаправление стандартного ввода

Выше использовалась команда `cat listing.txt` для вывода содержимого файла на экран терминала. Утилита (**cat**) может принимать данные как прямым чтением из файла (как в примере), так и считыванием из потока ввода (напрямую с клавиатуры или из перенаправленного потока), а получив данные, утилита cat выводит их в стандартный поток вывода (обычно — это экран).

В качестве примера содержимое файла с листингом будет направлено в поток ввода, для этого выполните следующую команду:

```
cat < listing.txt
```

На экране будет показано всё то же содержимое листинга.

Таким способом можно подать на вход программе, читающей данные из потока ввода, информацию из файла.

Конвейеры

Умение команд читать данные со стандартного ввода и выводить результаты в стандартный вывод используется механизмом командной оболочки, который называется **конвейером**. С помощью оператора конвейера «|» (вертикальная черта) стандартный вывод одной команды можно связать со стандартным вводом другой:

```
<команда_1> | <команда_2>
```

Для демонстрации этого механизма понадобится несколько команд. Например, необходимо получить листинг всего содержимого папки **/etc**, включая все подкаталоги, и вывести на экран только имена с расширением **.conf**. Для выбора строк по заданному шаблону применяется утилита grep, которая, как и **cat**, может принимать данные как из файла, так и из потока ввода. Перенаправьте вывод команды `ls -R` на ввод команде `grep "\.conf"`:

```
ls -R /etc | grep "\.conf"
```

Если данный вывод необходимо сохранить в файл для дальнейшей работы, то операторы перенаправления и конвейеры можно сочетать в одной комбинированной команде. Например:

```
ls -R /etc | grep "\.conf" > list_of_conf.txt
```

Важно отметить, что можно сочетать несколько конвейеров в одной составной команде. Такие команды часто называют **фильтрами**.

Recoll – поиск документов по содержимому

Recoll - приложение, позволяющее производить поиск документов по их содержимому.
Поддерживаемые форматы:

```
Text, HTML, email, OpenDocument, Microsoft Office и Office Open XML, AbiWord, KWord, Gaim, Lyx, Scribus, PDF, WordPerfect, PostScript, RTF, TeX, DVI, DjVu, MP3 и другие аудиоформаты, JPEG и другие форматы изображения.
```

Вы можете подробнее ознакомиться с информацией по поиску файлов в системе, просмотрев наши обучающие видео:

- на **RuTube** — Утилиты поиска файлов;
- в **Яндекс.Дзен** — Утилиты поиска файлов;
- в **VK Видео** — Утилиты поиска файлов.

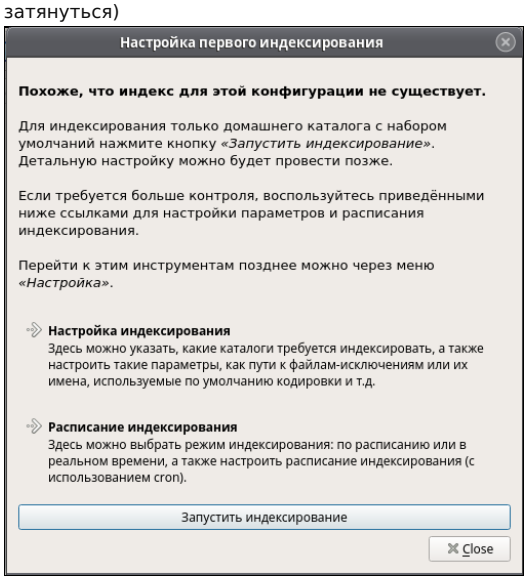
На наших каналах вы также сможете найти много другой полезной информации.

Установка:

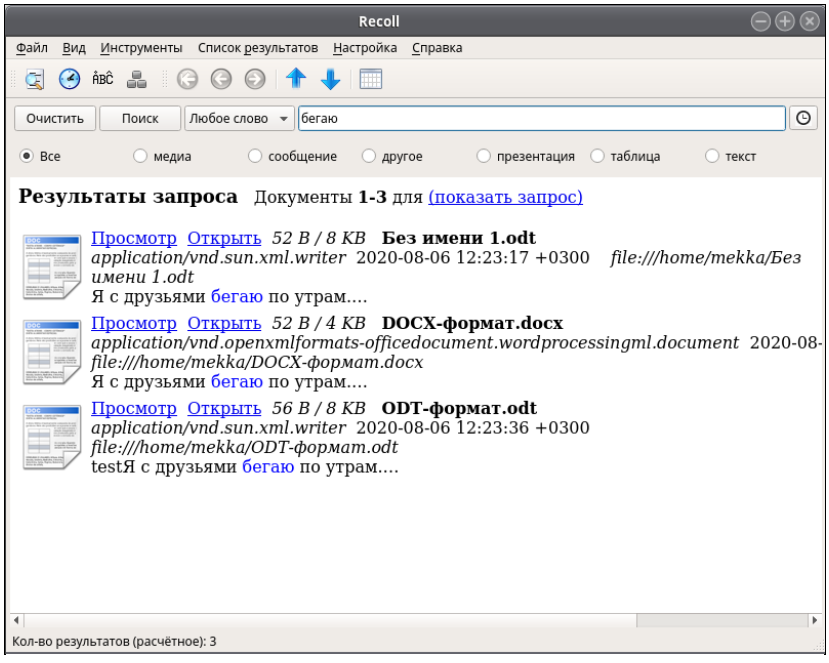
```
dnf install recoll
```

Далее запускаем из Меню -> Стандартные -> Recoll

Первый запуск сопровождается индексацией по файлам во всей системе. Запускаем её (если файлов на диске много, процесс может затянуться)



Далее достаточно в поиск ввести слово и соответствующий фильтр, чтобы Recoll знал, как и что ему искать:



ВАЖНО

Самое важное в процессе поиска, это обновлять индексы. Так как приложение ориентируется только на те файлы, которые он проиндексировал. Файлы, созданные и отредактированные после индексации программа уже не учитывает. Чтобы запустить процесс индексации необходимо перейти в раздел Файл -> Обновить индекс.

Ripgrep — рекурсивный поиск в текущем каталоге шаблона регулярного выражения

Установка
Синтаксис
Опции
Позиционные аргументы
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: ripgrep-13.0.0

Ripgrep (или rg) — это инструмент командной строки для рекурсивного поиска в текущем каталоге шаблона регулярного выражения. **Ripgrep** предназначен для замены стандартной команды **grep** с улучшенной производительностью и удобством использования. **Ripgrep** обладает высокой скоростью работы благодаря использованию многопоточности и оптимизированным алгоритмам.

По умолчанию **ripgrep** будет учитывать .gitignore и автоматически пропускать скрытые файлы/каталоги и двоичные файлы. Стандартный набор регулярных выражений ripgrep гарантирует линейное время поиска. Поэтому такие функции, как обратные ссылки и произвольные проверки, не поддерживаются. Флаг **--pcre2** можно использовать для включения обратных ссылок и проверок.

Ripgrep поддерживает файлы конфигурации. Установите **RIPGREP_CONFIG_PATH** в файл конфигурации. Файл может содержать один аргумент оболочки на строку. Строки, начинающиеся с #, игнорируются.

Установка

Для установки **ripgrep** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install ripgrep
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
rg [<ОПЦИИ>] ШАБЛОН [ПУТЬ ...]
```

Для просмотра опций ripgrep используйте команду:

```
rg --help
```

Опции

Основные опции утилиты ripgrep:

- **-A, --after-context** — показывать количество строк после каждого совпадения (переопределяет флаг **--context** и **--passthru flags**);
- **--auto-hybrid-regex** — динамически выбирать между поддерживаемыми регулярными выражениями в зависимости от функций, используемых в шаблоне;
- **-B, --before-context** — показывать количество строк перед каждым совпадением;
- **--binary** — выполнять поиск в двоичных файлах (по умолчанию ripgrep пытается автоматически пропускать двоичные файлы, чтобы повысить релевантность результатов и ускорить поиск);
- **--block-buffered** — использовать буферизацию блоков;
- **-b, --byte-offset** — выводить смещение на основе 0 байт во входном файле перед каждой строкой вывода, если указано **-o** (**--only-matching**), выводить смещение самой соответствующей части;

- **-s, --case-sensitive** — выполнять поиск с учётом регистра;
- **--color** — определять использование цветов;
- **--colors** — определять настройки цвета для использования в выходных данных;
- **--column** — определять номер столбца, начиная с 1;
- **-C, --context** — показывать количество строк после каждого совпадения;
- **--context-separator** — разделять несмежные строки контекста в выходных данных;
- **-c, --count** — показывать количество строк, соответствующих заданным шаблонам для каждого искомого файла;
- **--count-matches** — показывать количество отдельных совпадений с заданными шаблонами для каждого искомого файла;
- **--crlf** — обрабатывать CRLF (\r \ n) как символ завершения строки, а не просто \n;
- **--debug** — показывать сообщения отладки;
- **--dfa-size-limit** — верхний предел размера регулярного выражения DFA;
- **-E, --encoding** — использовать кодировку текста для всех искомых файлов;
- **-f, --file** — искать по одному шаблону из файла на строку;
- **--files** — распечатать каждый файл, в котором будет выполняться поиск;
- **-l, --files-with-matches** — распечатать только те пути, которые имеют хотя бы одно совпадение;
- **--files-without-match** — распечатать только те пути, которые содержат нулевые совпадения;
- **-F, --fixed-strings** — определять рисунок как литеральную строку, а не регулярное выражение;
- **-L, --follow** — переходить по символическим ссылкам во время проверки каталогов;
- **-g, --glob** — включать или исключать файлы и каталоги для поиска;
- **--glob-case-insensitive** — обрабатывать шаблоны, заданные с помощью флага -g / --glob, без учёта регистра;
- **--heading** — выводить путь к файлу;
- **--hidden** — выполнять поиск скрытых файлов и каталогов;
- **--iglob** — включать файлы и каталоги в поиск с учётом регистра;
- **-i, --ignore-case** — игнорировать регистры символов при поиске;
- **--ignore-file** — указывать файл (файлы), содержащие шаблоны, которые будут использоваться для игнорирования файлов во время поиска;
- **--ignore-file-case-insensitive** — то же, что и **--ignore-file**, но шаблоны в этом файле будут применяться без учёта регистра;
- **--include-zero** — включать в вывод результат поиска, даже если найденная строка отсутствует (например, для пустых файлов);
- **-v, --invert-match** — выводить только те строки, которые не соответствуют заданному шаблону (инверсия совпадений);
- **--json** — выводить результаты поиска в формате JSON;
- **-n, --line-number** — добавлять к каждому найденному совпадению номер строки, в которой было найдено это совпадение;
- **-x, --line-regexp** — искать совпадения только среди целых строк, игнорируя различные подстроки;
- **-M, --max-columns** — устанавливать максимальное количество отображаемых столбцов (символов) для всех строк в выводе;
- **--max-columns-preview** — аналогично **-M**, используется для предварительного просмотра, ограничивая количество видимых столбцов;
- **-m, --max-count** — ограничивать общее количество совпадений, которые будут выводиться в результате поиска;
- **--max-depth** — задать максимальную глубину обхода каталогов, т.е. сколько уровней директорий будет обходить утилита;
- **--max-filesize** — ограничивать размер обрабатываемых файлов (при превышении указанного размера файл будет игнорироваться);
- **--mmap** — использовать память для отображения файлов;
- **-U, --multiline** — включать режим поиска по многострочным совпадениям, используется для текста, который может находиться на нескольких строках;
- **--multiline-dotall** — включать режим поиска по многострочным совпадениям с учётом всех символов;
- **--no-config** — отключать использование конфигурационных файлов ripgrep;
- **-I, --no-filename** — подавлять вывод имён файлов при выводе результатов поиска, если нужно получить только совпадения без указания, в каких файлах они были найдены;

- **--no-heading** — отключать вывод заголовков (имён файлов) перед результатами поиска;
- **--no-ignore** — выполнять поиск по всем файлам и директориям, независимо от правил игнорирования;
- **-N, --no-line-number** — отключать вывод номеров строк при совпадении;
- **--no-messages** — подавлять вывод информационных сообщений, таких как предупреждения об отсутствии файлов или о том, что некоторые файлы были проигнорированы;
- **--no-mmap** — отключать использование отображения файлов в память при поиске;
- **--no-pcre2-unicode** — отключать поддержку юникодных символов в регулярных выражениях с использованием библиотеки PCRE2;
- **--no-require-git** — позволять использовать ripgrep без необходимости находиться в каталоге Git или проекте, управляемом системой контроля версий;
- **--no-unicode** — отключать поддержку символов Unicode в выводе, что может быть полезно для консольных эмуляторов, которые не поддерживают или неправильно отображают UTF-8;
- **-0, --null** — использовать нулевой байт в качестве разделителя между именами файлов в выводе;
- **--null-data** — аналогично -0, но используется во время обработки входных данных;
- **--one-file-system** — ограничивать поиск только текущей файловой системой, что предотвращает переход через смонтированные файловые системы, такие как сетевые или внешние диски;
- **-o, --only-matching** — выводить только совпадающую часть строки, а не всю строку;
- **--passthru** — позволять вывести строки, которые были найдены, но не соответствуют заданному шаблону;
- **--path-separator** — задать символ-разделитель для путей в выводе;
- **-P, --pcre2** — включать поддержку регулярных выражений PCRE2, что позволяет использовать более сложные регулярные выражения при выполнении поиска;
- **-p, --pretty** — выводить результаты в красивом формате (псевдоним для --color=always --heading --line-number);
- **-q, --quiet** — отключить вывод результатов и сообщений об ошибках, прекратить поиск, если в файле найдено соответствие;
- **--regex-size-limit** — установить лимит на размер регулярного выражения;
- **-e, --regexp** — указать регулярное выражение для поиска;
- **-r, --replace** — заменить найденные совпадения на указанный текст;
- **-z, --search-zip** — искать в ZIP-архивах и других сжимаемых файлах;
- **-S, --smart-case** — поиск выполняется без учёта регистра;
- **--sort** — сортировать выводимые результаты по определённому критерию;
- **--sortr** — сортировать результаты поиска;
- **--stats** — вывести статистику о результатах поиска, включая количество найденных совпадений и время выполнения;
- **-a, --text** — обрабатывать двоичные файлы как текст;
- **-j, --threads** — указывать число потоков, которое будет использовано для параллельной обработки;
- **--trim** — обрезать лишние пробелы в начале и конце строк результатов, улучшая читаемость;
- **-t, --type** — задать тип файлов для поиска, что позволяет ограничить поиск определённым форматом файлов (например, только .txt или .md);
- **--type-add** — добавить новый тип файлов, который можно использовать в команде поиска;
- **--type-clear** — очистить ранее определённые типы файлов, вернуть настройки по умолчанию;
- **--type-list** — выводить список доступных типов файлов, помогает выбрать, какие типы следует использовать в поиске;
- **-T, --type-not** — исключить указанные типы файлов из процесса поиска;
- **-u, --unrestricted** — отключить все ограничения, которые могут применяться к поиску, включая ограничения на типы файлов и размеры;
- **-V, --version** — вывести версию утилиты ripgrep;
- **--vimgrep** — вывести результаты поиска в формате, совместимом с vim, что позволяет удобнее обрабатывать результаты в текстовом редакторе Vim;
- **-H, --with-filename** — вывести имя файла перед совпадениями, даже если в поиске участвует только один файл;
- **-w, --word-regexp** — искать только по целым словам, игнорируя частичные совпадения.

Позиционные аргументы

Шаблон

Шаблон — регулярное выражение, используемое для поиска. Для сопоставления шаблона, начинающегося с тире, используйте опцию **-e /--regexp**.

Путь

Путь — файл или каталог для поиска. Поиск в каталогах выполняется рекурсивно. Пути, указанные явно в командной строке, переопределяют **glob** и игнорируют правила.

Примеры использования

Рассмотрим примеры для нескольких основных опций утилиты **ripgrep**:

1. Опция **-i, --ignore-case**:

```
rg -i "so" ./3d.txt
```

Например, если файл ./3d.txt содержит следующие данные:

```
Sun of the sleepless! Melancholy star!
Whose tearful beam glows tremulously far,
That show’st the darkness thou canst not dispel,
How like art thou to Joy remembered well!

So gleams the past, the light of other days,
Which shines, but warms not with its powerless rays;
A night-beam Sorrow watcheth to behold,
Distinct, but distant – clear, but oh, how cold!

George Gordon Byron
```

Результат поиска (без учета регистра) строк, в которых встречается "**so**" в файле ./3d.txt:

```
6:So gleams the past, the light of other days,
8:A night-beam Sorrow watcheth to behold,
```

2. Опция **-w, --word-regexp**:

```
rg -w "So" ./3d.txt
```

Результат поиска (с учетом регистра) только полных слов "**So**" в файле ./3d.txt:

```
6:So gleams the past, the light of other days,
```

3. Опция **-n, --line-number**:

```
rg -n "to" ./3d.txt
```

Пример выводит номера строк, в которых найдено совпадение с текстом "**to**" в файле ./3d.txt.

```
4:How like art thou to joy remember'd well!
8:A night-beam Sorrow watcheth to behold,
```

4. Опция **-l, --files-with-matches**:

```
rg -l "a" /home/user/Документы
```

Пример выводит список файлов в каталоге /home/user/Документы, в которых найдены строки, содержащие "**a**".

```
/home/user/Документы/sample1.json  /home/user/Документы/3d.txt
```

5. Опция **-c, --count**:

```
rg -c "s" ./3d.txt
```

Пример выводит только количество строк, содержащих совпадения с "**s**" в файле ./3d.txt.

```
6
```

6. Опция **-A, --after-context <параметр>**:

```
rg -A 3 "the" ./3d.txt
```

Пример выводит 3 строки после каждого совпадения с "**the**" в файле ./3d.txt:

```
1:Sun of the sleepless! Melancholy star!
2-Whose tearful beam glows tremulously far,
3:That show’st the darkness thou canst not dispel,
4-How like art thou to Joy remembered well!
5-
6:So gleams the past, the light of other days,
7-Which shines, but warms not with its powerless rays;
8-A night-beam Sorrow watcheth to behold,
9-Distinct, but distant – clear, but oh, how cold!
```

7. Опция **-v, --invert-match**:

```
rg -v "to" ./3d.txt
```

Пример выводит строки из файла ./3d.txt, которые не содержат совпадения с "**to**".

```
1:Sun of the sleepless! Melancholy star!
2:Whose tearful beam glows tremulously far,
3:That show’st the darkness thou canst not dispel
5:
6:So gleams the past, the light of other days,
7:Which shines, but warms not with its powerless rays;
9:Distinct, but distant – clear, but oh, how cold!
10:
11:George Gordon Byron
```

8. Опция **-C, --context <параметр>**:

```
rg -C 2 "warms" ./3d.txt
```

Пример выводит 2 строки ДО и 2 строки ПОСЛЕ каждого совпадения с "**warms**" в файле ./3d.txt:

```
5-
6-So gleams the past, the light of other days,
7:Which shines, but warms not with its powerless rays;
8-A night-beam Sorrow watcheth to behold,
9-Distinct, but distant – clear, but oh, how cold!
```

9. Опция **-F, --fixed-strings**:

```
rg -F "like art" ./3d.txt
```

Пример выполнит поиск точного текста "**like art**" в файле ./3d.txt, не интерпретируя его как регулярное выражение:

```
4:How like art thou to Joy remembered well!
```

10. Опция **-s, --case-sensitive**:

```
rg -s "am" ./3d.txt
```

Пример выполнит поиск строки "**am**" в файле ./3d.txt, учитывая регистр символов (по умолчанию):

```
2:Whose tearful beam glows tremulously far,
6:So gleams the past, the light of other days,
8:A night-beam Sorrow watcheth to behold,
```

11. Опция **-L, --follow**:

```
rg -L "no" /home/user/Документы
```

Пример выполнит поиск в файлах в указанном каталоге /home/user/Документы, следуя символическим ссылкам:

```
/home/user/Документы/sample1.json  4:That show’st the darkness thou canst not dispel,
8:Which shines, but warms not with its powerless rays;

/home/user/Документы/3d.txt
3:That show’st the darkness thou canst not dispel,
7:Which shines, but warms not with its powerless rays;
```

12. Опция **-u, --unrestricted**:

```
rg -u "of" ./3d.txt
```

Пример отключит "умный" поиск и все ограничения, которые могут применяться к поиску, и выполнит точное сопоставление с "**of**" в файле ./3d.txt.

```
1:Sun of the sleepless! Melancholy star!
6:So gleams the past, the light of other days,
```

13. Опция **-V, --version**:

```
rg --version
```

Команда выводит номер версии **ripgrep**.

```
ripgrep 13.0.0
```

14. Опция **--type-list**:

```
rg --type-list
```

Пример выводит список всех известных типов файлов, которые **ripgrep** может обрабатывать.

```
agda: *.agda, *.lagda
aidl: *.aidl
amake: *.bp, *.mk
asciidoc: *.adoc, *.asc, *.asciidoc
asm: *.S, *.asm, *.s
asp: *.ascx, *.ascx.cs, *.ascx.vb, *.aspx, *.aspx.cs, *.aspx.vb
ats: *.ats, *.dats, *.hats, *.sats
avro: *.avdl, *.avpr, *.avsc
awk: *.awk
bazel: *.BUILD, *.bazel, *.bazelrc, *.bzl, BUILD, WORKSPACE
bitbake: *.bb, *.bbappend, *.bbclass, *.conf, *.inc
brotli: *.br
buildstream: *.bst
bzip2: *.bz2, *.tbz2
c: *.[chH], *.[chH].in, *.cats
cabal: *.cabal
cbor: *.cbor
[...]
vimscript: *.vim
webidl: *.idl, *.webidl, *.widl
wiki: *.mediawiki, *.wiki
xml: *.dtd, *.rng, *.sch, *.xhtml, *.xjb, *.xml, *.xml.dist, *.xsd, *.xsl, *.xslt
xz: *.txz, *.xz
yacc: *.y
yaml: *.yaml, *.yml
yang: *.yang
z: *.Z
zig: *.zig
zsh: *.zsh, .zlogin, .zlogout, .zprofile, .zshenv, .zshrc, zlogin, zlogout, zprofile, zshenv,
zshrc
zstd: *.zst, *.zstd
```

15. Опция **--sort <параметр>**:

```
rg --sort accessed "ss" /home/user/Документы
```

Пример позволяет сортировать файлы по заданному критерию ("**path**", "**modified**", "**accessed**", "**created**", "**none**"):

```
/home/user/Документы/3d.txt
1:Sun of the sleepless! Melancholy star!
3:That show’st the darkness thou canst not dispel, 7:Which shines, but warms not with its powerless rays;
 /home/user/Документы/sample1.json  2:Sun of the sleepless! Melancholy star!
4:That show’st the darkness thou canst not dispel,
8:Which shines, but warms not with its powerless rays;
```

16. Опция **-m, --max-count <параметр>**:

```
rg -m 10 "beam" /home/user/Документы
```

Пример останавливает поиск в каждом файле указанного каталога после заданного числа совпадений:

```
2:Whose tearful beam glows tremulously far,
8:A night-beam Sorrow watcheth to behold,
```

17. Опция **--color <параметр>**:

```
rg --color always "to" ./3d.txt
```

Пример использует цветовое выделение для совпадающих строк ("**always**", "**ansi**", "**auto**","**never**").

```
4:How like art thou to Joy remembered well!
8:A night-beam Sorrow watcheth to behold,
```

Эти примеры показывают разнообразие опций для работы с текстовыми данными и их возможности для поиска с помощью **ripgrep**.

Просмотр и управление файлами и каталогами с помощью утилиты tree

Установка
Синтаксис и опции
Примеры использования
Сравнение работы с командой ls

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tree-1.8.0-1

Tree — консольная утилита для просмотра и управления файлами и директориями. Она предоставляет простой, но мощный интерфейс для навигации по файловой системе и выполнения различных операций с файлами, таких как создание, удаление, копирование, перемещение и изменение атрибутов.

Основные функции программы **tree**:

1 . *Просмотр содержимого директорий и файлов*. **Tree** позволяет быстро просматривать содержимое директории, включая имена файлов и папок, их размеры и даты изменения.

2. *Перемещение, копирование и удаление файлов и директорий*. **Tree** предоставляет возможность перемещать, копировать и удалять файлы и директории в текущей директории или в какой-либо другой.

3. *Изменение атрибутов файлов и директорий*. С помощью **Tree** можно изменять атрибуты файлов, такие как разрешения, владелец, группа и время доступа.

4 . *Поиск файлов и директорий по имени*. **Tree** поддерживает поиск файлов и директорий в текущей директории и во всех поддиректориях по заданному имени.

5 . *Сортировка файлов и директорий по различным критериям*. **Tree** позволяет сортировать файлы и директории по имени, размеру, дате изменения, времени последнего доступа и другим параметрам.

6 . *Поддержка многопанельного интерфейса*. **Tree** может быть запущена в многопанельном режиме, что позволяет просматривать несколько директорий одновременно.

7. *Использование горячих клавиш*. **Tree** имеет набор горячих клавиш для быстрого доступа к наиболее часто используемым функциям.

8. П*оддержка архивов*. **Tree** поддерживает работу с архивами **ZIP** и **TAR**, позволяя просматривать их содержимое и извлекать файлы.

9. *Интеграция с другими программами*. **Tree** может интегрироваться с другими программами, такими как **Midnight Commander** или **Nautilus**, для удобной работы с файлами и директориями.

10. *Поддержка Unicode*. **Tree** поддерживает отображение файлов и директорий на разных языках, включая русский.

Утилита **Tree** полезна для быстрой и удобной навигации по файловой системе РЕД ОС.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните следующую команду:

```
dnf install tree
```

Синтаксис и опции

Синтаксис программы выглядит следующим образом:

```
tree [опции]
```

Опции утилиты, отвечающие за вывод дерева папок и файлов:

- **-a** — вывод всех без исключения файлов;
- **-d** — вывод только списка директорий;
- **-l** — переход по символическим ссылкам, которые ведут к папкам;
- **-f** — вывод содержимого папок с префиксами пути;
- **-x** — учитывает только текущую файловую систему;
- **-L** — уровень вложенности для отображения в выводе;
- **-R** — рекурсивный переход по каталогам всех уровней;
- **-P** — отображение файлов, название которых соответствует шаблону;
- **-I** — исключение из вывода файлов, название которых соответствует шаблону;
- **-o** — печать вывода в файл с заданным именем;
- **--noreport** — запрет вывода отчета по количеству папок и файлов в конце дерева;
- **--charset** — кодировка для отображения графических и html-файлов;
- **--filelimit** — папки, которые содержат больше файлов, чем указано, показаны не будут.

Опции утилиты, использующиеся для управления отображением названий документов:

- **-q** — замена непечатаемых символов в названиях файлов знаком «**?**»;
- **-N** — вывод непечатаемых символов в названиях файлов как есть;
- **-Q** — заключить названия файлов в двойные кавычки;
- **-p** — для каждого из файлов указать его название и список разрешенных действий;
- **-u** — вывод имени или идентификатора учетной записи, под которой был создан файл;
- **-g** — вывод имени или идентификатора группы пользователей, которая имеет права на доступ к файлу;
- **-s** — вывод рядом с названием файла его размера в байтах;
- **-h** — вывод размера файла в удобном формате с добавлением к числу буквенного сокращения (K, M, G, T);
- **-D** — печать даты последнего изменения файла (либо последнего изменения статуса в комбинации с опцией **-c**);
- **-F** — добавление символа «**/**» для папок, «**=**» — для файлов сокета, «*****» — для исполняемых файлов, «**>**» — для door-файлов, «**|**» — для специальных файлов FIFO;
- **--inodes** — вывод номера индексных дескрипторов для файлов и папок;
- **--device** — указать номер устройства, которому принадлежит файл или папка.

Опции утилиты, использующиеся для сортировки результатов:

- **-v** — упорядочить вывод по уровням вложенности;
- **-t** — сортировка вывода по дате последнего изменения файлов и папок;
- **-c** — сортировка вывода по дате последнего изменения статуса;
- **-U** — вывод результатов в том порядке, в котором папки расположены на диске;
- **-r** — сортировка вывода в обратном порядке;
- **--dirsfirst** — сначала вывод папок, потом — файлов.

Опции отображения дерева:

- **-i** — убрать линии («ветки» дерева), файлы и папки отображаются в виде списка;
- **-n** — сделать дерево одноцветным;
- **-C** — вернуть дереву разноцветное отображение после использования опции **-n**.

Примеры использования

1. Вывод дерева файлов и каталогов с указанием их размера:

```
tree -h

.
```

```
├── [   60]  test.log
├── [ 4.0K]  Видео
├── [ 4.0K]  Документы
├── [ 4.0K]  Загрузки
│   └── [ 3.8K]  create_minimal_image_moby.sh
├── [ 4.0K]  Изображения
│   └── [ 339K]  2023-07-11_09-46.png
├── [ 4.0K]  Музыка
├── [ 4.0K]  Общедоступные
├── [ 4.0K]  Рабочий стол
└── [ 4.0K]  Шаблоны
    ├── [  182]  test.sh
    └── [  172]  text.sh

8 directories, 5 files
```

2. Сортировка вывода в обратном порядке:

```
tree -r

.
├── Шаблоны
│   ├── text.sh
│   └── test.sh
├── Рабочий стол
├── Общедоступные
├── Музыка
├── Изображения
│   └── 2023-07-11_09-46.png
├── Загрузки
│   └── create_minimal_image_moby.sh
├── Документы
├── Видео
└── test.log

8 directories, 5 files
```

3. Вывод даты последнего изменения файлов:

```
tree -h -D

.
├── [   60 Jul 10 11:34]  test.log
├── [ 4.0K Jul  6 16:42]  Видео
├── [ 4.0K Jul  6 16:42]  Документы
├── [ 4.0K Jul 11 09:46]  Загрузки
│   └── [ 3.8K Jul  7 15:57]  create_minimal_image_moby.sh
├── [ 4.0K Jul 11 09:46]  Изображения
│   └── [ 339K Jul 11 09:46]  2023-07-11_09-46.png
├── [ 4.0K Jul  6 16:42]  Музыка
├── [ 4.0K Jul  6 16:42]  Общедоступные
├── [ 4.0K Jul  6 16:42]  Рабочий стол
└── [ 4.0K Jul 11 09:46]  Шаблоны
    ├── [  182 Jul 10 11:34]  test.sh
    └── [  172 Jul 10 11:27]  text.sh

8 directories, 5 files
```

4. Также функционал утилиты **tree** позволяет искать файлы с помощью установленной маски, например, для поиска файлов с расширекнием **.png** выполните:

```
tree -P '*.png' --prune

.
└── Изображения
    └── 2023-07-11_09-46.png

1 directory, 1 file
```

5. Существует возможность перенаправления результата выполнения команды в файл:

```
tree -P '*.png' --prune -o output_tree.txt
cat output_tree.txt

.
└── Изображения
    └── 2023-07-11_09-46.png

1 directory, 1 file
```

Сравнение работы с командой ls

В стандартный набор программ РЕД ОС входит утилита **ls**, которая отображает каталоги и их содержимое.

Простая команда **ls** без опций передает на вывод список файлов и папок внутри текущей директории:

```
ls

 output_tree.txt  Видео      Загрузки    Музыка       'Рабочий стол'
 test.log         Документы  Изображения  Общедоступные  Шаблоны
```

С помощью команды **ls** можно просмотреть расширенную информацию о папках и файлах, используя опцию **-g**:

```
ls -g

итого 40
-rw-rw-r--. 1 user  133 июл 11 09:54  output_tree.txt
-rw-rw-r--. 1 user   60 июл 10 11:34  test.log
drwxr-xr-x. 2 user 4096 июл  6 16:42  Видео
drwxr-xr-x. 2 user 4096 июл  6 16:42  Документы
drwxr-xr-x. 2 user 4096 июл 11 09:46  Загрузки
drwxr-xr-x. 2 user 4096 июл 11 09:46  Изображения
drwxr-xr-x. 2 user 4096 июл  6 16:42  Музыка
drwxr-xr-x. 2 user 4096 июл  6 16:42  Общедоступные
drwxr-xr-x. 2 user 4096 июл  6 16:42 'Рабочий стол'
drwxr-xr-x. 2 user 4096 июл 11 09:46  Шаблоны
```

Для обратной сортировки вывода команды используется опция **-r**:

```
ls -g -r

итого 40
drwxr-xr-x. 2 user 4096 июл 11 09:46  Шаблоны
drwxr-xr-x. 2 user 4096 июл  6 16:42 'Рабочий стол'
drwxr-xr-x. 2 user 4096 июл  6 16:42  Общедоступные
drwxr-xr-x. 2 user 4096 июл  6 16:42  Музыка
drwxr-xr-x. 2 user 4096 июл 11 09:46  Изображения
drwxr-xr-x. 2 user 4096 июл 11 09:46  Загрузки
drwxr-xr-x. 2 user 4096 июл  6 16:42  Документы
drwxr-xr-x. 2 user 4096 июл  6 16:42  Видео
-rw-rw-r--. 1 user   60 июл 10 11:34  test.log
-rw-rw-r--. 1 user  133 июл 11 09:54  output_tree.txt
```

Для вывода подробной информации о файлах и каталогах используется опция **-l**:

```
ls -l

итого 40
-rw-rw-r--. 1 user user  133 июл 11 09:54  output_tree.txt
-rw-rw-r--. 1 user user   60 июл 10 11:34  test.log
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Видео
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Документы
drwxr-xr-x. 2 user user 4096 июл 11 09:46  Загрузки
drwxr-xr-x. 2 user user 4096 июл 11 09:46  Изображения
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Музыка
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Общедоступные
drwxr-xr-x. 2 user user 4096 июл  6 16:42 'Рабочий стол'
drwxr-xr-x. 2 user user 4096 июл 11 09:46  Шаблоны
```

Для рекурсивного вывода содержимого каталогов используется опция **-R**:

```
ls -R

.:
 output_tree.txt   Видео      Загрузки     Музыка        'Рабочий стол'
 test.log          Документы  Изображения  Общедоступные  Шаблоны

./Видео:

./Документы:

./Загрузки:create_minimal_image_moby.sh

./Изображения:2023-07-11_09-46.png

./Музыка:

./Общедоступные:

'./Рабочий стол':

./Шаблоны:test.sh  text.sh
```

Одним из главных преимуществ использования утилиты **tree** является ее способность отображать иерархическую структуру каталогов, что помогает быстро найти нужный файл или каталог. Кроме того, tree позволяет быстро создавать новые каталоги и файлы, а также копировать, перемещать и удалять файлы.

В отличие от команды **ls**, которая выводит список файлов и каталогов в текущей директории, **tree** позволяет просматривать содержимое всех подкаталогов и файлов в заданной директории.

tre-command - утилита для отображения структуры директорий

Установка
Синтаксис и опции
Примеры использования
Удаление

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tre-command-0.4.0-1

Tre-command — консольная утилита для просмотра и управления файлами и директориями (современная альтернатива программе *tree*). По возможности использует git ls-файлы в качестве источника файла. Tre также может создавать псевдонимы оболочки, которые при запуске открывают связанный с ним файл в редакторе по умолчанию.

Основные функции:

- отображает структуру каталогов в виде древовидной диаграммы, как в классической версии tree;
- создает псевдонимы оболочки для каждого листинга, который открывает файлы;
- выводит структуру в цветах с учетом настроек.

Утилита *tre* полезна для быстрой и удобной навигации по файловой системе РЕД ОС.

Установка

Для установки утилиты через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install tre-command
```

Синтаксис и опции

Синтаксис программы выглядит следующим образом:

```
tre-command [<опции>] [<путь_к_директории>]
```

Опции утилиты:

- **-a, --all** — вывод всех файлов и каталогов;
- **-c, --color <ПАРАМЕТР>** — цвет выходных данных (automatic, always или never; автоматически означает, что tre будет включать цвета, в противном случае цвета будут отключены);
- **-d, --directories** — вывод только списка каталогов;
- **-e, --editor <КОМАНДА>** — создание псевдонима для отображаемого результата в файле /tmp/tre_aliases_$USE;
- **-E, --exclude <ШАБЛОН>** — исключение путей, соответствующих шаблону регулярного выражения;
- **-h, --help** — вывод справки;
- **-j, --json** — вывод JSON вместо древовидной диаграммы;
- **-l, --limit <ЛИМИТ>** — ограничение глубины вывода дерева файлов;
- **-p, --portable** — создание абсолютных путей для псевдонимов редактора, по умолчанию в псевдонимах используются относительные пути для повышения производительности;
- **-s, --simple** — обычный вывод файлов и каталогов;
- **-V, --version** — вывод версии программы.

Примеры использования

1. Для отображения только каталогов в виде дерева перейдите в нужную директорию и введите команду:

```
tre-command --directories
```

Результат выполнения команды:

```
[user@localhost Загрузки]$ cd candy-icons
[user@localhost candy-icons]$ ls
apps  devices  index.theme  LICENSE  mimetypes  places  preferences  preview  README.md  status
[user@localhost candy-icons]$ tre-command --directories
.
├── status
│   └── scalable
├── devices
│   └── scalable
├── preview
├── places
│   ├── 16
│   └── 48
├── mimetypes
│   └── scalable
├── preferences
│   └── scalable
└── apps
    └── scalable
[user@localhost candy-icons]$
```

2. Для отображения JSON, содержащего файлы в древовидной иерархии, вместо обычной древовидной диаграммы введите команду:

```
tre-command --json
```

```
[user@localhost preview]$ tre-command --json
{
  "type": "directory",
  "name": ".",
  "path": ".",
  "contents": [
    {
      "type": "file",
      "name": "folders.png",
      "path": "./folders.png"
    },
    {
      "type": "file",
      "name": "cli.png",
      "path": "./cli.png"
    },
    {
      "type": "file",
      "name": "candy.png",
      "path": "./candy.png"
    },
    {
      "type": "file",
      "name": "icons.png",
      "path": "./icons.png"
    }
  ]
}
```

3. Команда «tre-command -E "/*.svg"» использует опцию **--exclude** для исключения всех файлов или каталогов, пути которых соответствуют шаблону регулярного выражения "/*.svg".

```
tre-command -E "/*.svg"
```

```
[user@localhost Документы]$ tre-command
.
├── file1.svg
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
├── каталог1
└── file2.svg
[user@localhost Документы]$ tre-command -E "/*.svg"
.
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
└── каталог1
```

4. Для ограничения глубины вывода дерева введите команду с опцией **-l** и задайте лимит уровня вложенности:

```
tre-command -l 3
```

```
[user@localhost Документы]$ tre-command -l 1
.
├── каталог
└── каталог1
[user@localhost Документы]$ tre-command -l 2
.
├── каталог
│   ├── каталог1
│   └── каталог2
└── каталог1
[user@localhost Документы]$ tre-command -l 3
.
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
└── каталог1
```

5. Для отключения цветового оформления вывода файлов и каталогов введите команду:

```
tre-command -c never
```

```
[user@localhost Документы]$ tre-command -c never
.
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
└── каталог1
[user@localhost Документы]$
```

6. Для создания псевдонима отображаемого результата в файле /tmp/tre_aliases_$USE выполните команду:

```
tre-command --editor ['Copy_pass']
```

```
[user@localhost Документы]$ tre-command --editor ['Copy_pass']
[0] .
├── [1] каталог
│   ├── [2] каталог1
│   │   ├── [3] file1
│   │   └── [4] file2
│   └── [5] каталог2
└── [6] каталог1
```

В файл /tmp/tre_aliases_$USE будет записан следующий результат:

```
 GNU nano 7.2                                          tre_aliases_user
alias e0="eval '[Copy_pass] \".\"'"
alias e1="eval '[Copy_pass] \"./каталог\"'"
alias e2="eval '[Copy_pass] \"./каталог/каталог1\"'"
alias e3="eval '[Copy_pass] \"./каталог/каталог1/file1\"'"
alias e4="eval '[Copy_pass] \"./каталог/каталог1/file2\"'"
alias e5="eval '[Copy_pass] \"./каталог/каталог2\"'"
alias e6="eval '[Copy_pass] \"./каталог1\"'"
```

7. Для исключения определенных файлов или директорий при использовании команды *tre-command* можно использовать опцию **--exclude**. Например, если нужно исключить файлы или директории с именем "**каталог2**", можно использовать следующую команду:

```
tre-command --exclude "каталог2"
```

Результат:

```
[user@localhost Документы]$ tre-command --exclude "каталог2"
.
├── каталог
│   └── каталог1
│       ├── file1
│       └── file2
└── каталог1
```

8. Можно также указать несколько исключений, разделяя их запятыми или используя опцию **--exclude** несколько раз, если нужно исключить более одного элемента. Например:

```
tre-command --exclude "каталог2" --exclude "каталог1"
```

```
[user@localhost Документы]$ tre-command --exclude "каталог2" --exclude "каталог1"
.
└── каталог
```

9. Также можно использовать несколько опций. Например, для вывода древовидной диаграммы всех файлов и каталогов в текущей директории с использованием цветов введите команду:

```
tre-command -a -c always
```

```
[user@localhost Документы]$ tre-command -a -c always
.
├── file1.svg
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
├── каталог1
└── file2.svg
```

10. Вывести только список каталогов без использования цветового оформления:

```
tre-command -d -c never
```

```
[user@localhost Документы]$ tre-command -d -c never
.
├── каталог
│   ├── каталог1
│   └── каталог2
└── каталог1
```

11. Исключить все файлы и каталоги, пути которых содержат слово "**/каталог**" и вывести JSON вместо древовидной диаграммы:

```
tre-command -E "/каталог" -j
```

```
[user@localhost Документы]$ tre-command -E "/каталог" -j
{
  "type": "directory",
  "name": ".",
  "path": ".",
  "contents": [
    {
      "type": "file",
      "name": "file1.svg",
      "path": "./file1.svg"
    },
    {
      "type": "file",
      "name": "file2.svg",
      "path": "./file2.svg"
    }
  ]
}
```

12. Создать псевдоним для отображаемого результата в файле /tmp/tre_aliases и использовать абсолютные пути для псевдонимов редактора:

```
tre-command -e "emacs" -p
```

```
[user@localhost Документы]$ tre-command -e "emacs" -p
[0] .
├── [1] file1.svg
├── [2] каталог
│   ├── [3] каталог1
│   │   ├── [4] file1
│   │   └── [5] file2
│   └── [6] каталог2
├── [7] каталог1
└── [8] file2.svg
```

Удаление

Для удаления утилиты *tre-command* можно использовать следующую команду:

```
dnf remove tre-command
```

zoxide - легкая навигация по каталогам

Установка утилиты
Запуск и настройка утилиты
Возможности утилиты
Основные опции утилиты
Основные команды утилиты

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zoxide-0.9.2-1

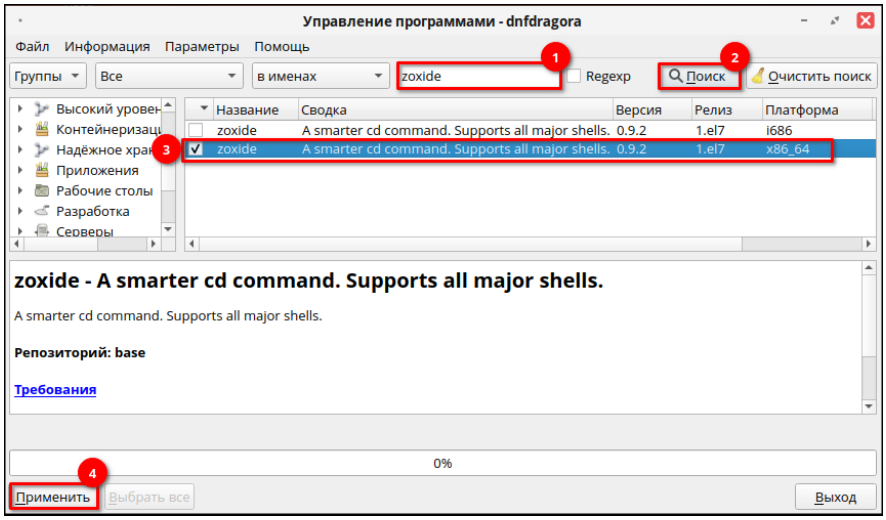
Zoxide — это удобная утилита командной строки, предоставляющая легкую навигацию по каталогам. Она является альтернативой команде **cd**, но с дополнительными возможностями и улучшениями.

Zoxide помогает быстро перемещаться между каталогами с помощью интеллектуального алгоритма запоминания путей. Утилита отслеживает каталоги, которые пользователь использует чаще всего, и применяет алгоритм ранжирования для перехода к лучшему совпадению. Алгоритм ранжирования подразумевает создание рейтинга для каталогов путем отслеживания посещений. При каждом новом посещении каталога его рейтинг будет увеличен на 1. Чем выше рейтинг, тем больше вероятность использования данного каталога как наилучшего совпадения.

Установка утилиты

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**zoxide**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install zoxide
```

Запуск и настройка утилиты

Для использования утилиты **zoxide** введите команду, которая применяется для настройки автоматической интеграции программы с оболочкой командной строки:

```
zoxide init bash
```

При успешной интеграции в ответе команды будет выведено сообщение с рекомендациями по инициализации **zoxide** вида:

```
# To initialize zoxide, add this to your configuration (usually ~/.bashrc):
```

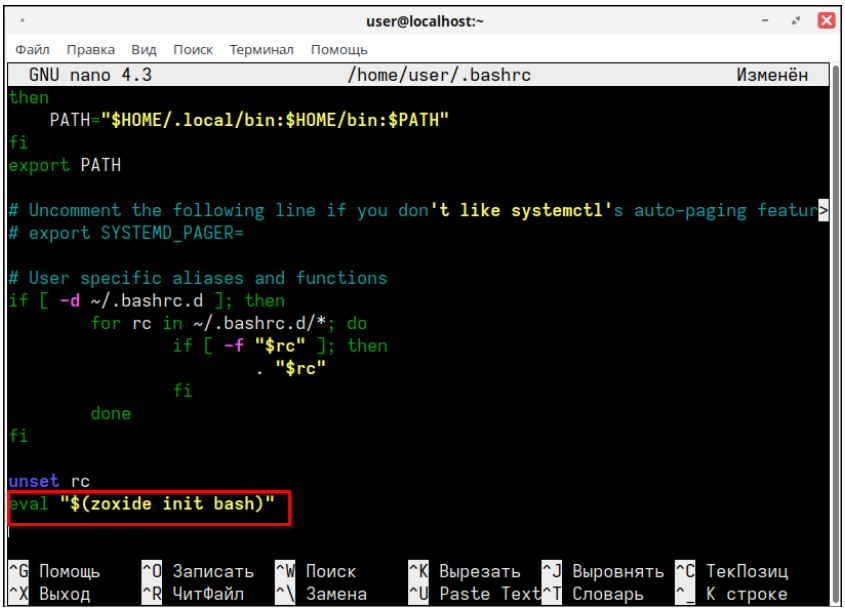
```
#
# eval \"$(zoxide init bash)\""
```

Для автоматической активации **zoxide** при запуске нового терминала в конец файла **~/.bashrc** определенного пользователя добавьте указанную выше строку:

```
eval "$(zoxide init bash)"
```

Файл **~/.bashrc** является скриптом настроек, который выполняется каждый раз, когда пользователь запускает новый терминал или интерактивную сессию **Bash**. В этом файле можно определить переменные среды, настроить псевдонимы команд, добавить функции и выполнить другие настройки, которые должны быть применены при запуске оболочки. Открыть файл можно с помощью команды:

```
nano ~/.bashrc
```



Для применения внесенных изменений перезагрузите файл настроек с помощью команды:

```
source ~/.bashrc
```

Изменения в файле **~/.bashrc** будут применены немедленно, и станет доступно использование новых переменных, псевдонимов и других настроек.

Возможности утилиты

Zoxide предлагает ряд полезных возможностей для удобной навигации по каталогам. Для быстрого перехода в часто посещаемый каталог, вместо полного указания пути к каталогу, можно использовать команду **z** в сочетании с частью имени каталога.

Рассмотрим пример создания символьной ссылки на каталог «**/home/user/**», для быстрого перехода к нему с помощью команды **z**.

1. Откройте терминал.
2. Перейдите в нужный каталог (в примере «**/home/user/**»):

   ```
   cd /home/user/
   ```

3. Создайте символьную ссылку с именем doc на каталог «**/home/user/**»:

   ```
   ln -s /home/user/ doc
   ```

4. Теперь для перехода в каталог «**/home/user/**» можно использовать команду:

```
z doc
```

Утилита **zoxide** считает символьную ссылку и перейдет в каталог «**/home/user/**».

Примечание.

Прежде чем использовать псевдонимы и команды, связанные с утилитой **zoxide**, выполните настройку утилиты, как показано в предыдущем пункте Запуск и настройка утилиты.

Zoxide запоминает посещенные пользователем каталоги и предлагает наиболее вероятные варианты для перехода, что позволяет быстро перемещаться между часто используемыми каталогами.

Zoxide автоматически обновляет историю переходов между сеансами, что позволяет сохранять состояние навигации между различными запусками терминала. Данная возможность позволяет не производить заново настройку утилиты.

Основные опции утилиты

Утилита имеет всего две опции:

-h, --help — выводит справку по использованию zoxide, включая доступные команды, опции и переменные среды;

-V, --version — выводит версию Zoxide.

Основные команды утилиты

Zoxide add — добавляет новый каталог в базу данных **zoxide** или увеличивает его рейтинг, если каталог уже существует в базе данных. Для добавления каталога в базу данных используйте команду вида:

```
zoxide add <имя_каталога>
```

Например:

```
zoxide add Документы
```

После выполнения вышеприведенной команды каталог «**/Документы**» будет добавлен в базу данных **zoxide** с начальным рейтингом 1. Если каталог уже существует в базе данных, его рейтинг будет увеличен на 1.

Zoxide query — позволяет найти каталог в базе данных.

Чтобы убедиться, что каталог был добавлен в базу данных, выполните команду **zoxide query <имя каталога>**:

```
zoxide query Документы
```

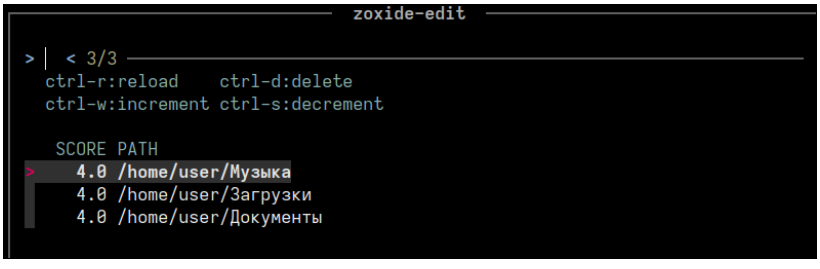
В терминале отобразится искомый каталог, добавленный в базу данных.

Также можно увидеть вывод, содержащий информацию о каталоге «**Документы**» и его ранге, если выполнить команду вместе с ключом **-s, -- score**:

```
zoxide query -s Документы
```

Zoxide edit — позволяет редактировать базу данных **zoxide** вручную. После выполнения команды откроется текстовый редактор, в котором можно изменить имя или теги каталога «**/Документы**». Доступно добавление, удаление и изменение записей в БД:

```
zoxide edit
```



Если текстовый редактор не открывается и появляется сообщение вида: «**zoxide: could not find fzf, is it installed?**», необходимо установить утилиту **fzf**.

Для установки утилиты выполните команду (потребуются права **администратора**):

```
sudo dnf install fzf
```

Zoxide import — импортирует записи из других приложений или инструментов для управления историей каталогов. Может быть полезно, если у вас уже есть существующая история каталогов, которую необходимо использовать с **zoxide**.

Предположим, существует файл с именем «**file.txt**», содержащий список каталогов, которые требуется импортировать в историю каталогов **zoxide**.

Выполните команду *zoxide import*, указав путь к файлу «**file.txt**», чтобы импортировать каталоги из файла в историю:

```
zoxide import /путь/к/файлу/file.txt
```

Zoxide init — создает конфигурацию оболочки для **zoxide**.

```
zoxide init <значение>
```

Допустимые значения: *bash*, *elvish*, *fish*, *nushell*, *posix*, *powershell*, *xonsh*, *zsh*.

- **Для bash:**

Откройте файл конфигурации (обычно **~/.bashrc**):

```
vim ~/.bashrc
```

Добавьте строку в конец файла:

```
eval "$(zoxide init bash)"
```

- **Для elvish:**

Откройте файл конфигурации (обычно **~/.elvish/rc.elv**):

```
vim ~/.elvish/rc.elv
```

Добавьте строку в конец файла:

```
"eval $(zoxide init elvish | slurp)"
```

- **Для fish:**

Откройте файл конфигурации (обычно **~/.config/fish/config.fish**):

```
vim ~/.config/fish/config.fish
```

Добавьте строку в конец файла:

```
zoxide init fish | source
```

- **Для nushell**:

Найдите файл конфигурации, выполнив команду в Nushell:

```
config path
```

Добавьте к нему строку ниже.

```
startup = ["zoxide init nushell --hook prompt | save ~/.zoxide.nu", "source ~/.zoxide.nu"]
```

- **Для posix**:

Добавьте строку в конец файла:

```
eval "$(zoxide init posix --hook prompt)"
```

- **Для powershell**:

Добавьте в конец файла конфигурации (найдите его, запустив echo $profile в PowerShell):

```
Invoke-Expression (& { (zoxide init powershell | Out-String) })
```

- **Для xonsh**:

Откройте файл ниже для редактирования (обычно ~/.xonshrc):

```
vim ~/.xonshrc
```

Добавьте строку в конец файла:

```
execx($(zoxide init xonsh), 'exec', __xonsh__.ctx, filename='zoxide')
```

- **Для zsh:**

Откройте файл для редактирования (обычно ~/.zshrc):

```
$ vim ~/.zshrc
```

Добавьте к нему строку ниже.

```
eval "$(zoxide init zsh)"
```

Zoxide remove — удаляет каталог из базы данных zoxide:

```
zoxide remove Документы
```

После удаления каталога из базы данных выполните команду «**zoxide query Документы».** Если каталог был удален, появится сообщение вида: «**no match found**».

Atril - универсальный просмотрщик документов

Установка
Основные функции программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: atril-1:1.26.0-11

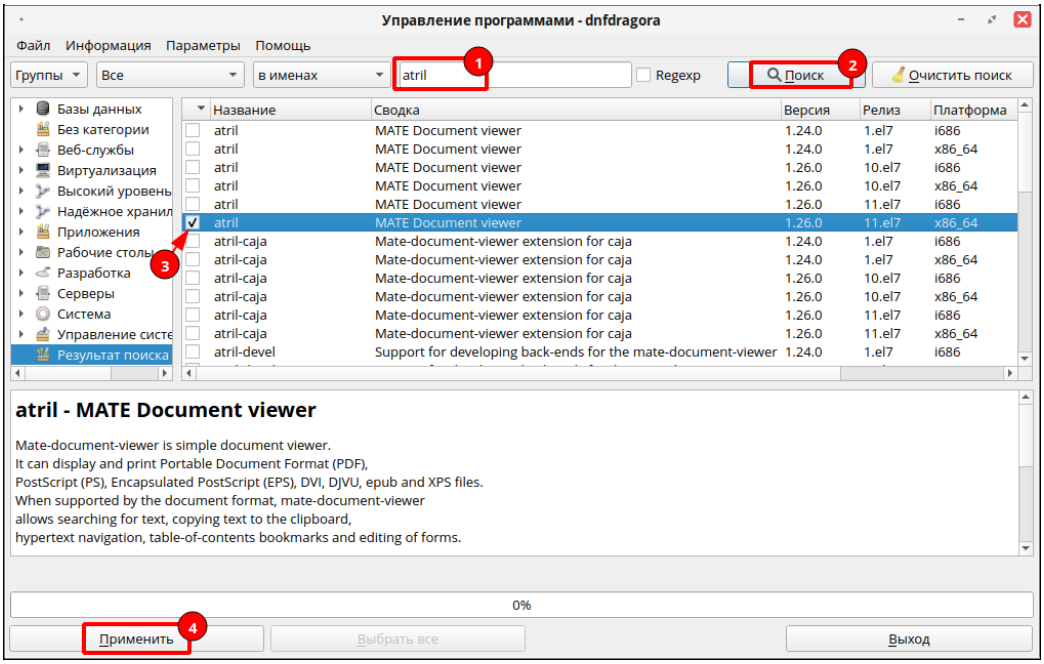
Atril — универсальное графическое приложение для просмотра электронных документов различных форматов, таких как: **PDF**, **Postscript** (PS), **TIFF**, **DVI**, **DjVu**, **CBR**, **XPS** и пр. Для форматов **PDF** и **DVI** поддерживается поиск текста, копирование фрагментов текста в буфер обмена, гипертекстовая навигация.

Atril имеет простой пользовательский интерфейс и интегрирован в рабочую среду MATE, но также может использоваться и в других графических окружениях.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**atril**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install atril
```

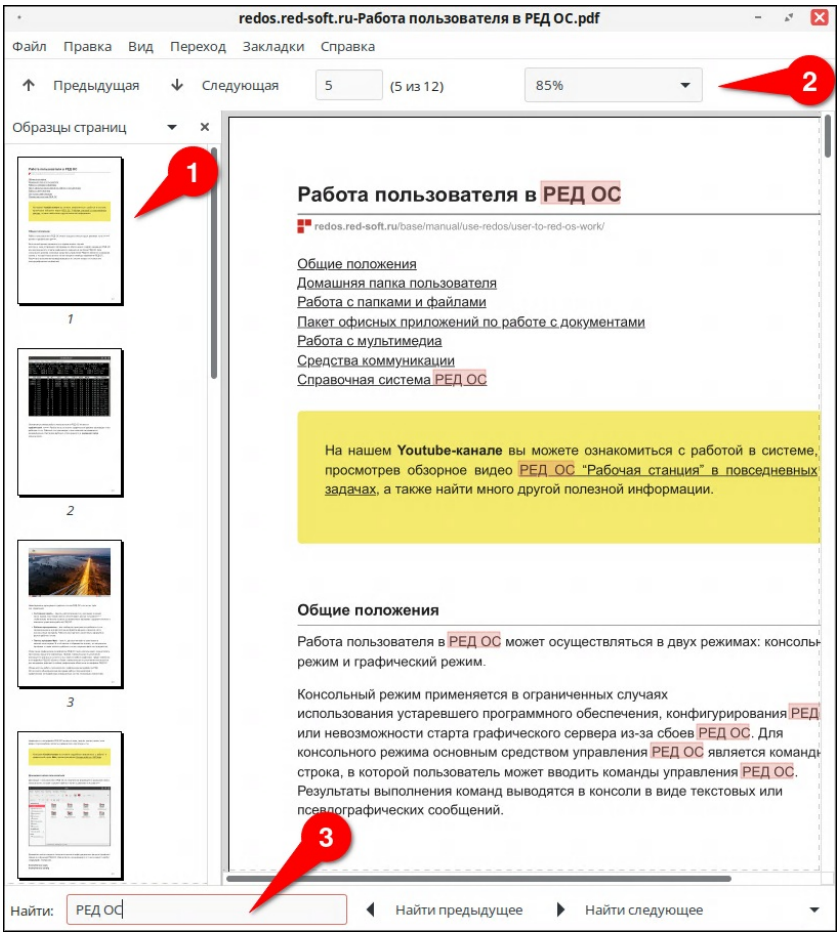
Дальнейшая работа в программе выполняется от **локального** пользователя.

После установки программа будет доступна из «**Главного меню**» - «**Офис**» - «**Просмотрщик документов**».

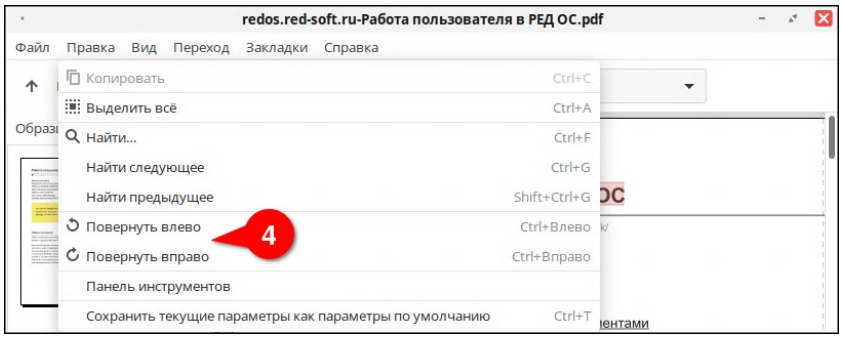
Основные функции программы

Atril может отображать миниатюры страниц, облегчающие навигацию при просмотре документов большого объёма (**1**).

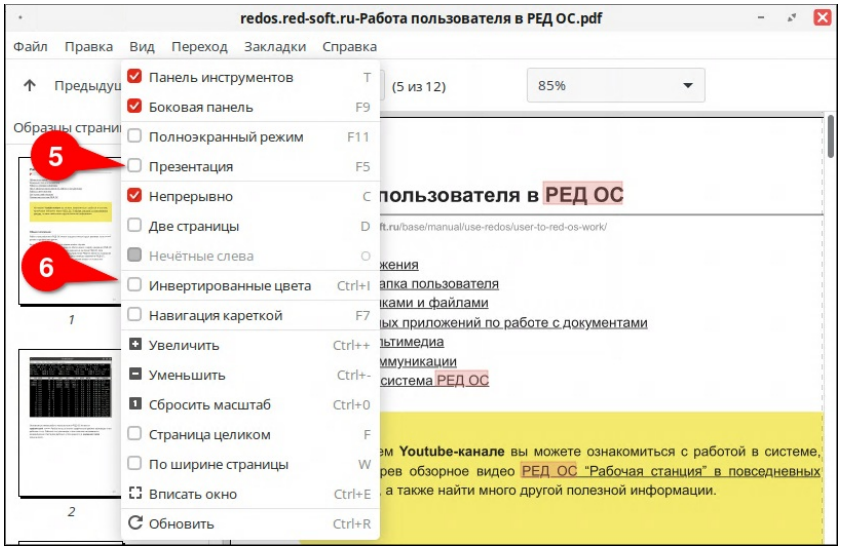
Поддерживается масштабирование (**2**) и поворот страницы (**4**), одно-страничный и двух-страничный просмотр.



Функция поиска по тексту документа (**3**) вызывается сочетанием клавиш *Ctrl+F*. Программа показывает количество найденных результатов, подсвечивая их на странице.



Имеется возможность просмотра документа в режиме презентации (**5**), а также поддерживается функция инвертирования цвета (**6**).



Okular - универсальный просмотрщик документов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: okular-20.08.1-1

Okular – это программа с открытым исходным кодом для просмотра различных типов документов с широким набором функций. Позволяет подключать дополнительные модули, за счёт чего расширять список поддерживаемых форматов файлов.

Основные возможности **okular**:

- Просмотр документов – поддерживает широкий спектр форматов документов, включая **PDF**, **PostScript**, **DjVu**, **EPub** и другие, что позволяет просматривать различные типы документов без необходимости установки различных специализированных программ.
- Навигация и масштабирование – предоставляет различные инструменты для удобной навигации по документам, включая возможность быстрого перехода к определенной странице или разделу. Также имеется функция масштабирования, позволяющая увеличивать или уменьшать изображение для более удобного чтения.
- Закладки и аннотации – пользователи могут добавлять закладки к интересующим страницам и создавать аннотации, чтобы отмечать важные места или добавлять комментарии в документы. Это полезные функции для обозначения ключевых моментов или для совместной работы над документами.
- Настройки и расширения – предоставляет множество настроек для более тонкой настройки программы.

Для установки **okular** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install okular
```

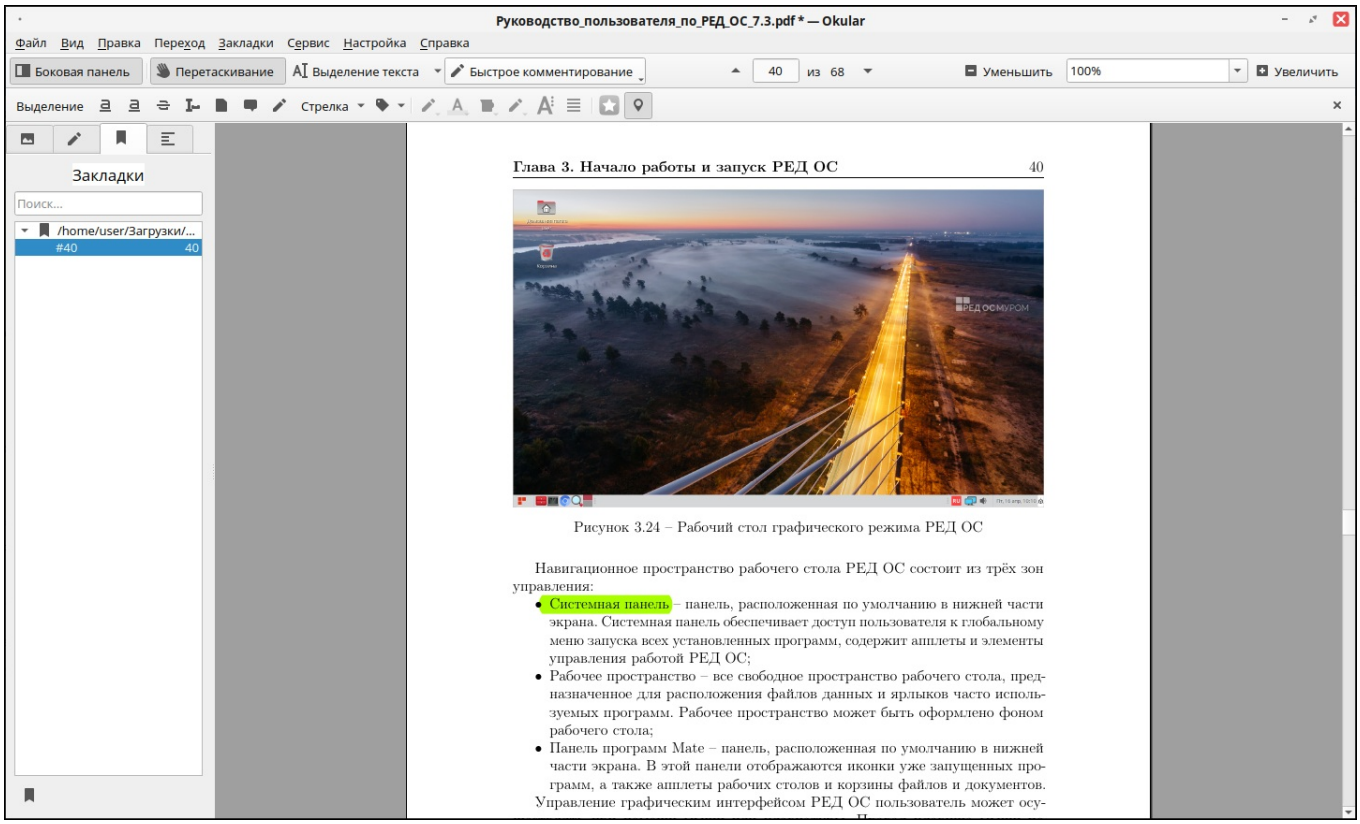
Дальнейшая работа в программе производится с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

После установки запуск программы доступен из «**Главного меню**» — «**Офис**» — «**Okular**» или через терминал (с правами **непривилегированного** пользователя) командой:

```
okular
```

Главное окно программы выглядит следующим образом:



В верхней части окна расположено **основное меню**, где доступны все действия для работы и настройки программы.

Ниже расположена **панель инструментов**, с помощью которой можно показать/скрыть боковую панель, выбрать действие по нажатии ЛКМ – перетаскивать (прокручивать) файл или выделить текст, также здесь доступно быстрое комментирование, переход к нужной странице файла и настройка масштаба страницы.

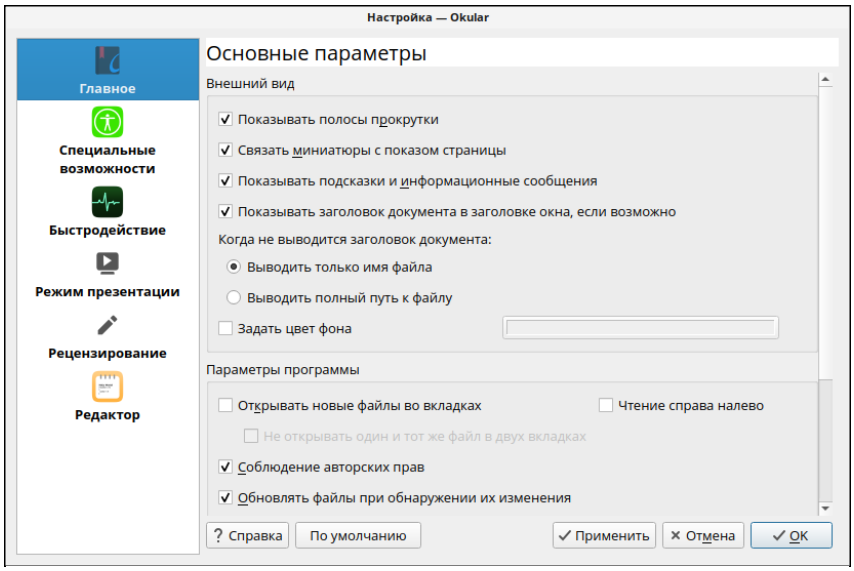
На **панели инструментов** расположены дополнительные инструменты для внесения правок в файл – подчеркивание текста прямой и волнообразной линией, зачеркивание текста, добавление встроенных и висящих заметок, добавление произвольных линий, стрелок и штампов, а также настройка цвета, заливки, текста добавляемых комментариев и линий.

Слева расположена боковая панель, на которой есть несколько вкладок:

- *миниатюры* – отображаются миниатюры открытого файла;
- *рецензирование* – отображаются внесенные в файл корректировки и комментарии, а также имя пользователя, который их внес;
- *закладки* – отображаются добавленные закладки;
- *содержание* – вкладка становится доступна, если в открытом файле существуют заголовки.

Через пункт меню «**Настройка**» можно настроить язык программы, комбинации клавиш для удобства работы, отображаемые панели инструментов и их содержимое, а также дополнительные модули.

Для настройки непосредственно программы **Okular** выберите «**Настройка**» – «**Настроить Okular**». Будет открыто окно редактирования основных параметров программы, специальных возможностей, быстродействия, режима презентации, режима рецензирования и редактора.


Настройка — Okular
Главное
Специальные возможности
Быстродействие
Режим презентации
Рецензирование
Редактор
Основные параметры
Внешний вид
Показывать полосы прокрутки
Связать миниатюры с показом страницы
Показывать подсказки и информационные сообщения
Показывать заголовок документа в заголовке окна, если возможно
Когда не выводится заголовок документа:
Выводить только имя файла
Выводить полный путь к файлу
Задать цвет фона
Параметры программы
Открывать новые файлы во вкладках
Чтение справа налево
Не открывать один и тот же файл в двух вкладках
Соблюдение авторских прав
Обновлять файлы при обнаружении их изменения
Справка
По умолчанию
Применить
Отмена
OK

Создание скриншотов с помощью Flameshot

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** flameshot-12.1.0-1

FlameShot — мультиплатформенный инструмент для создания скриншотов. Эта небольшая программа предлагает дополнительные возможности для быстрого редактирования скриншотов. Скриншоты можно создавать и стандартными средствами системы. Для этого достаточно нажать клавишу Print Screen, после чего скриншот будет сохранен в папке с изображениями.

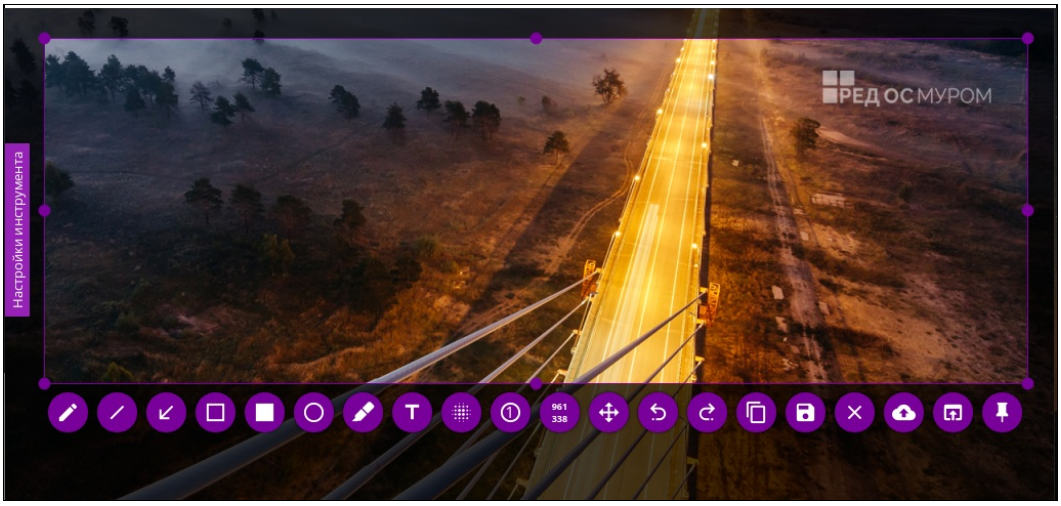
Однако главное преимущество FlameShot — возможность захвата выделенной области экрана и добавление к ней различных выделений и указателей. Это может быть особенно полезным для создания онлайн-инструкций.

Данная программа по умолчанию установлена в РЕД ОС.

Примечание.

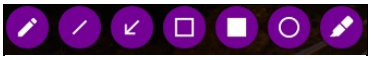
Обратите внимание, что **FlameShot** не предусмотрен для использования в графических окружениях **GNOME** и **KDE Plasma**. Корректная работа программы гарантируется только при использовании графического окружения **MATE**.

Для запуска Flameshot, откройте системное *"Меню"* - *"Графика"* - *"Flameshot"*. После запуска программы, чтобы сделать скриншот, нажмите на значок Flameshot в панели задач. Выделите нужную часть экрана и можете приступать к изменению.



Возможности программы

Для удобной работы со снимками экрана FlameShot имеет ряд полезных функций:

 - Инструменты для изменения рисунка: карандаш, маркер, фигуры, прямоугольное выделение.

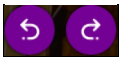
 - Вставка текста.

 - Размытие изображения.

 - Метки с увеличивающимся цифровым счетчиком.

 - Показывает размер выделения.

 - Модуль перемещения изображения по экрану.

 - Повторить/отменить последнее изменение.

 - Скопировать изображение в буфер обмена.

 - Сохранить снимок.

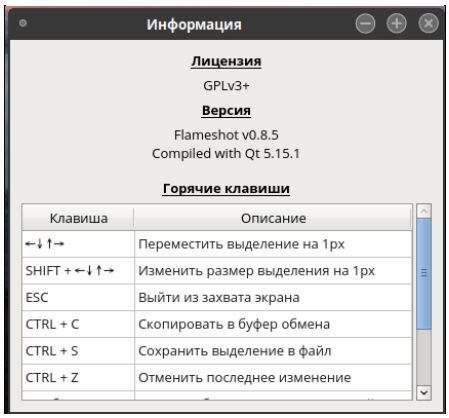
 - Покинуть захват экрана.

 - Загрузить изображение в Imgur (Imgur - программное обеспечение для загрузки, обмена и хранения фотографий и картинок).

 - Выбор приложения для открытия снимка.

 - Прикрепить изображение к рабочему столу.

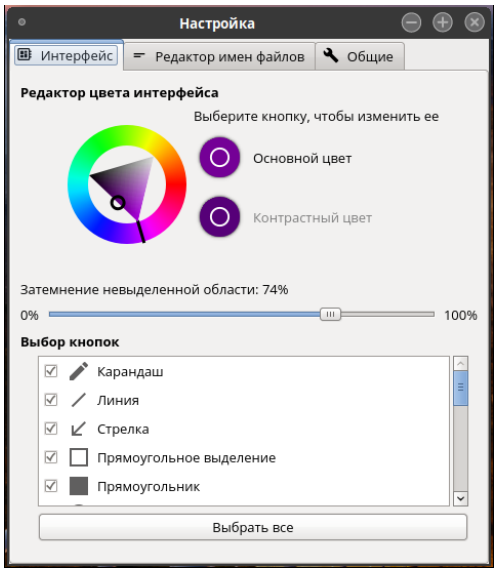
Для просмотра списка горячих клавиш нажмите на значок Flameshot *правой кнопкой мыши – "Информация"*.



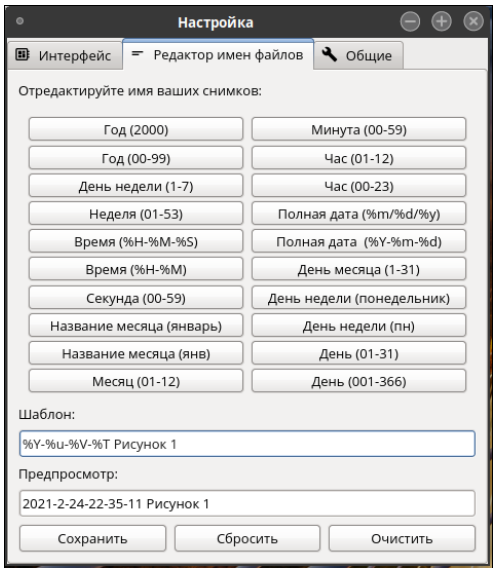
Пользовательские настройки Flameshot

На вкладке **«Интерфейс»** доступны настройки:

- Изменение цвета интерфейса;
- Настройка отображения кнопок.



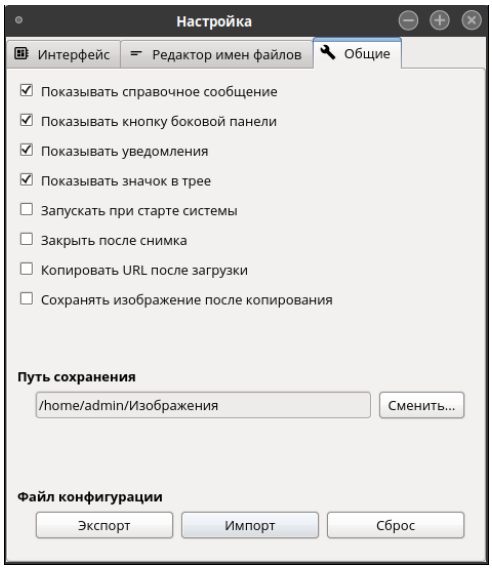
На вкладке **«Редактор имен файлов»** вы можете составить шаблон имени создаваемых файлов.



На вкладке **«Общие»** доступны настройки:

- Включение/отключение простейших функций;
- Путь сохранения файла;
- Экспорт/импорт файла конфигурации.

На вкладке **«Общие»** вы можете настроить простейшие функции, путь сохранения файлов, а также загрузить готовый конфигурационный файл.



Создание скриншотов с помощью kSnip

Установка
Основные возможности
Работа в ksnip через терминал
Расширенная настройка

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ksnip-1.10.1-1

Ksnip — это кроссплатформенная программа для создания скриншотов. Она включает в себя такие функции редактирования скриншотов, как добавление аннотаций и графических элементов, а также размытие областей.

Вы можете подробнее ознакомиться с работой в **kSnip**, просмотрев наши обучающие видео:

- на **RuTube** — Делаем скриншоты в РЕД ОС. Ksnip;
- в **Яндекс.Дзен** — Делаем скриншоты в РЕД ОС. Ksnip;
- в **VK Видео** — Делаем скриншоты в РЕД ОС. Ksnip.

На наших каналах вы также сможете найти много другой полезной информации.

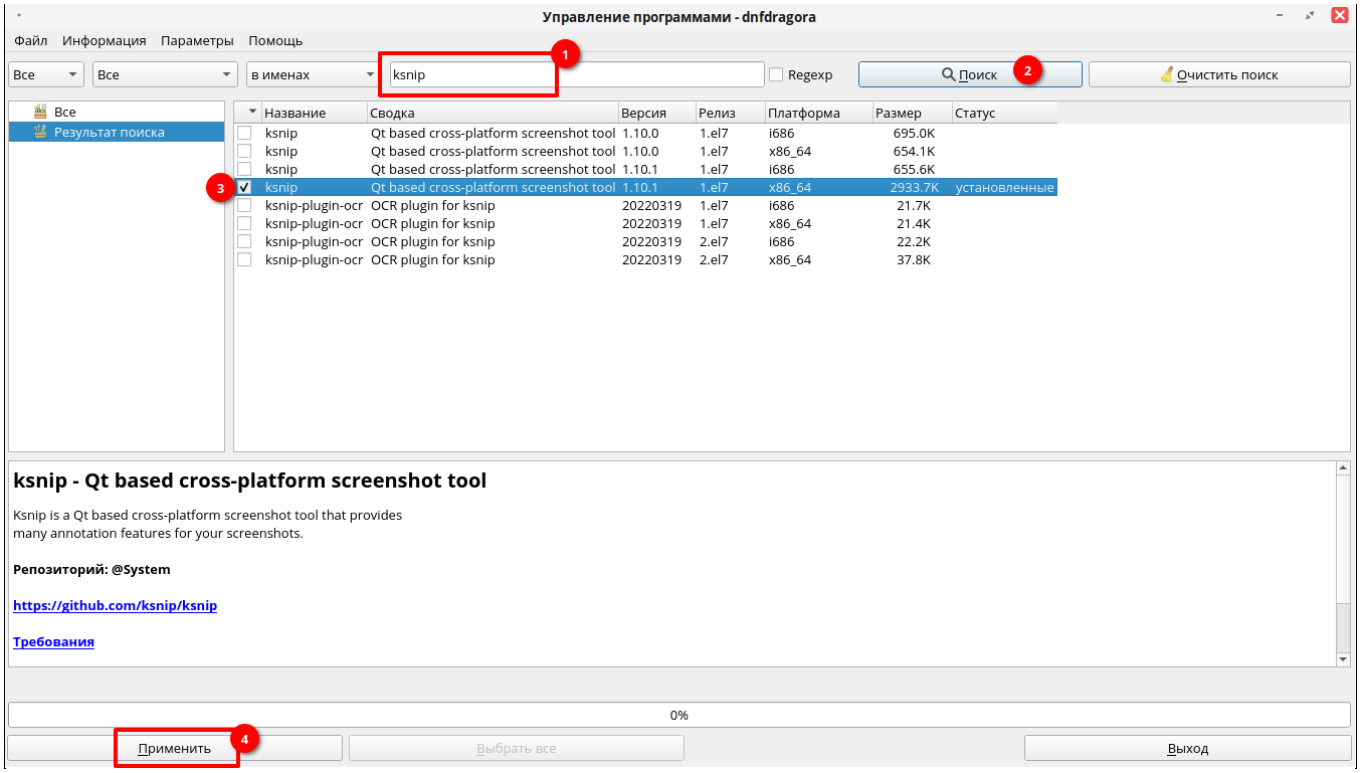
Примечание.

Обратите внимание, что **ksnip** не предусмотрена для использования в графическом окружении **GNOME**.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**ksnip**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки через терминал необходимо перейти в сеанс пользователя **root**:

```
su -
```

и выполнить команду:

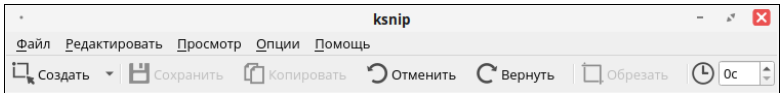
```
dnf install ksnip
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки запустить программу можно через «**Меню**» - «**Стандартные**» - «**Снимки экрана kSnip**».

Основные возможности

При открытии программы появляется компактная панель.



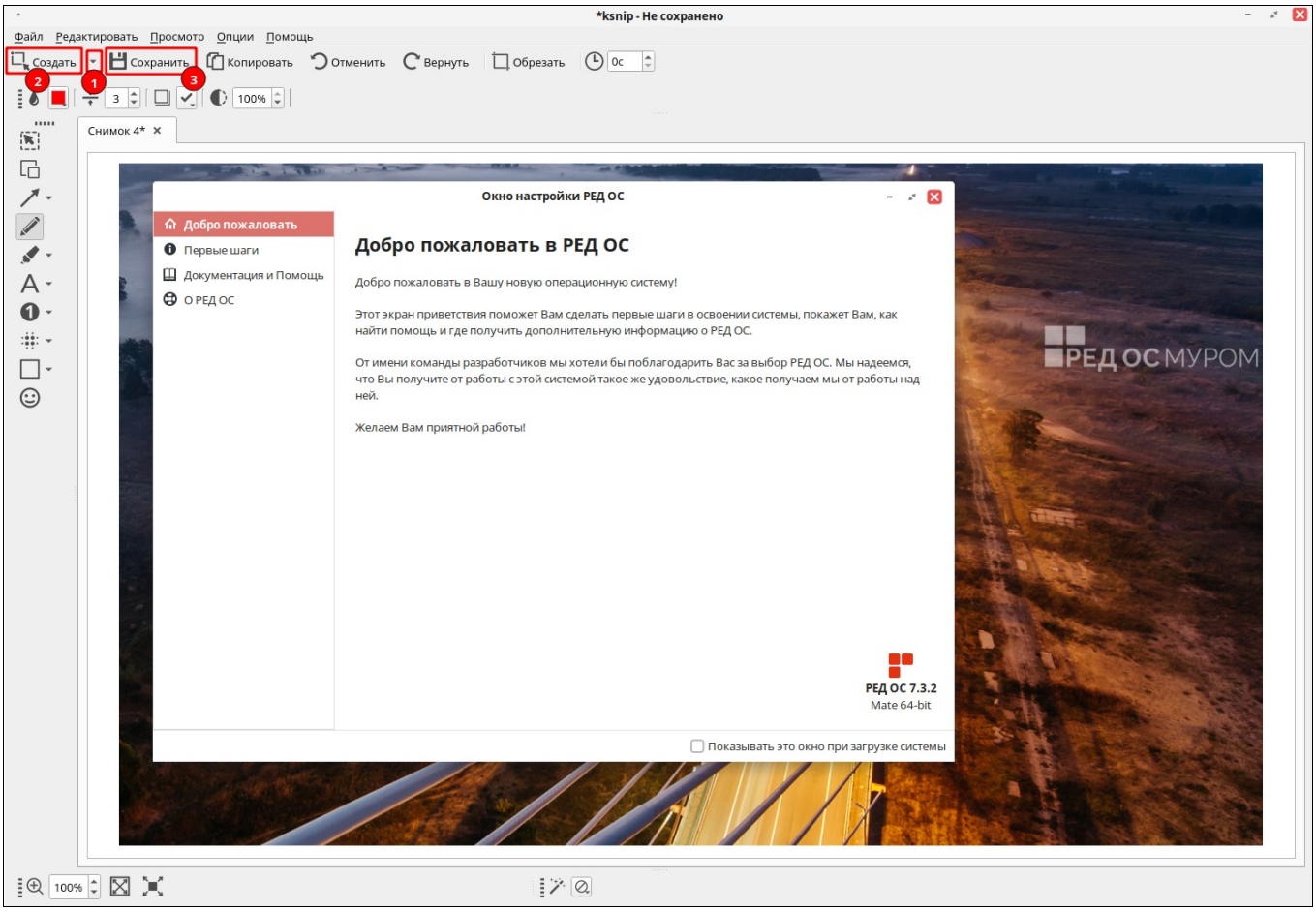
Основные функции программы **ksnip**:

- создание скриншотов различных областей экрана;
- создание скриншотов активного окна;
- создание скриншотов экрана целиком;
- создание скриншотов всех экранов;
- установка времени задержки перед созданием скриншота;
- добавление графических элементов: надписей, стрелок, счётчиков и др.;
- автоматическая загрузка скриншотов на сервис imgur.com, включая анонимный режим;
- поддержка командной строки;
- автоматическое сохранение скриншотов в заданную директорию;
- автоматическое копирование скриншотов в буфер обмена;
- печать скриншотов и экспорт в PDF/PS.

Ksnip позволяет создавать скриншоты различных областей экрана:

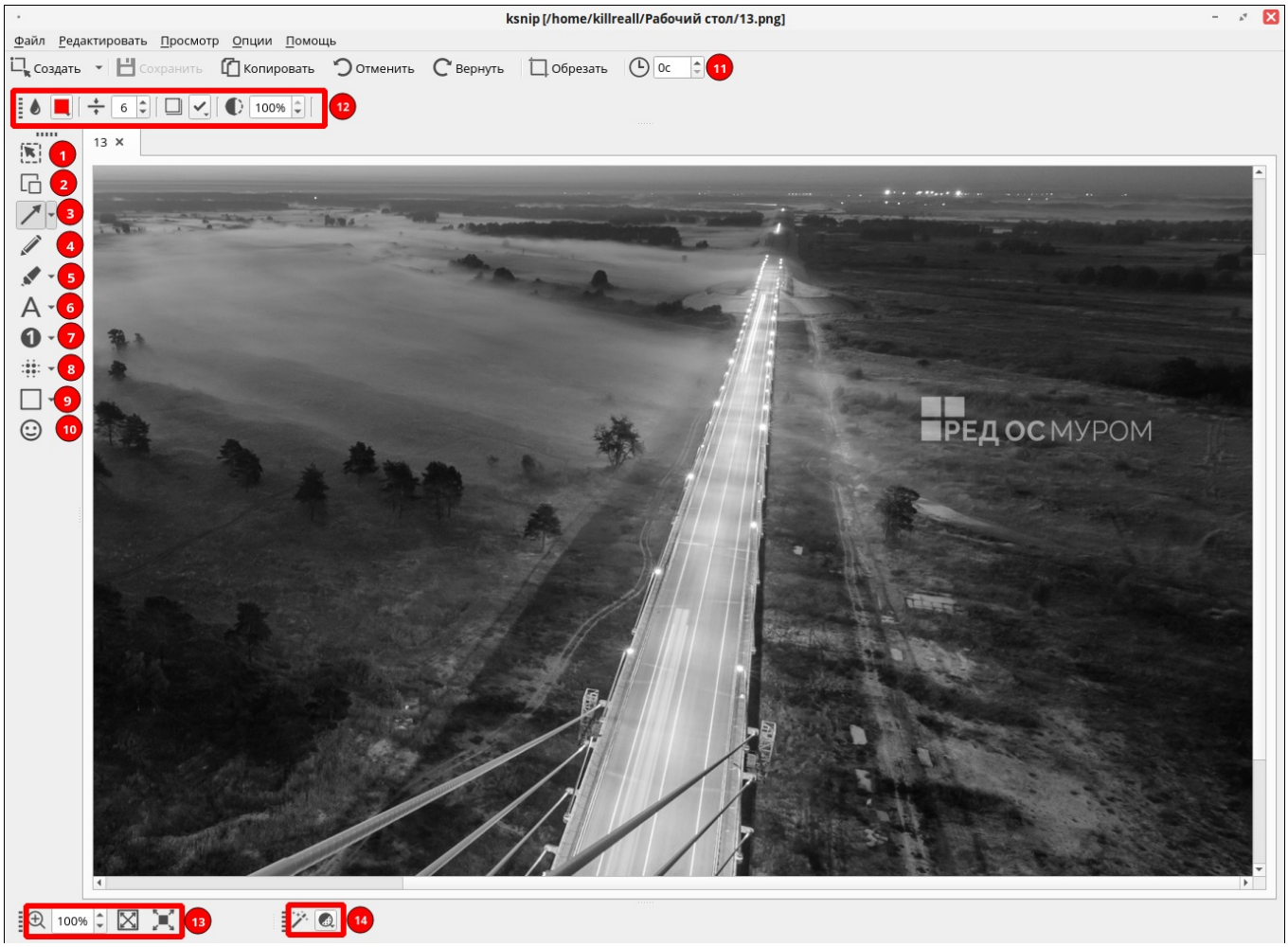
- **Произвольная прямоугольная область.** Скриншот прямоугольной области, размер которой определяет сам пользователь.
- **Текущий экран.** Скриншот всего рабочего стола.
- **Полноэкранный режим.** Скриншот всех мониторов.
- **Активное окно.** Скриншот отдельного окна.

В **ksnip** есть возможность выбирать тип создаваемого скриншота (1). Для создания скриншота нажмите кнопку «**Создать**» (2). При необходимости сохраните полученный скриншот (3).



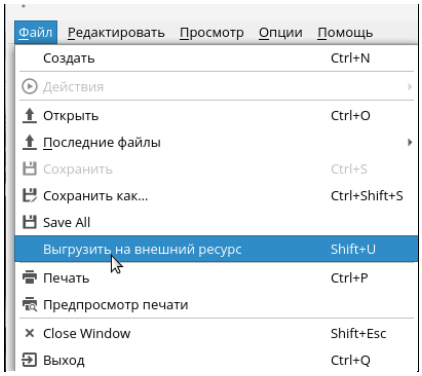
Ksnip обладает целым рядом инструментов для добавления аннотаций и графических элементов:

- Инструмент «**Выбор**» (1) позволяет выделять созданные графические элементы на скриншоте;
- Инструмент «**Дублирование**» (2) позволяет скопировать выделенную область на скриншоте и использовать её в качестве отдельного элемента;
- Добавление стрелок и линий (3);
- Произвольное рисование карандашом (4), линия имеет эффект сглаживания, степень сглаживания можно задать в настройках;
- Элемент «**Маркер**» (5);
- Добавление надписей (6);
- Добавление нумерованных счётчиков (7);
- Размытие областей на скриншоте (8);
- Добавление прямоугольников и окружностей (9);
- Добавление стикеров (10);
- Таймер для установки задержки времени перед созданием скриншота (11);
- Панель настройки выбранного инструмента (12);
- Масштабирование (13);
- Графические эффекты (14).

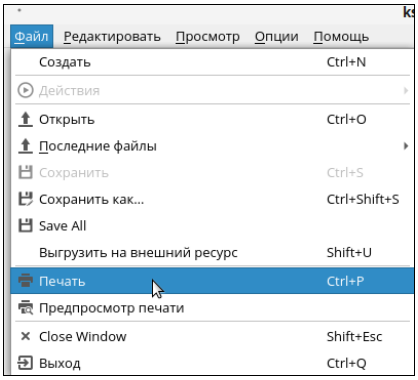


Скриншот может быть автоматически скопирован в буфер обмена и/или сохранен в заданную директорию. Также можно установить задержку создания скриншота по времени.

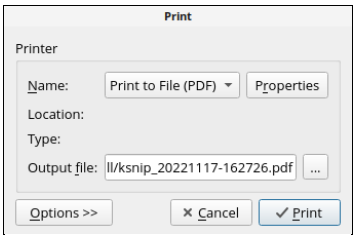
Для выгрузки на внешний ресурс есть соответствующий пункт в меню «**Файл**».



Скриншот также можно отправить на печать.

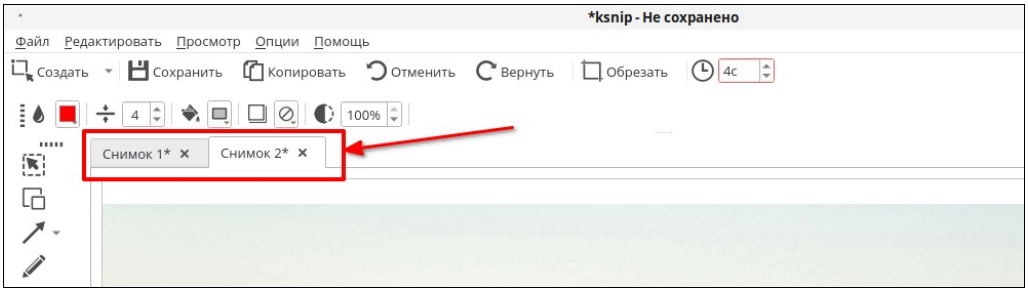


Через функцию печати можно осуществить экспорт скриншота **в формат PDF**.



Дополнительные особенности:

- Если при открытом скриншоте создать новый, то появится новая вкладка в основном рабочем поле. После этого можно перемещаться между несколькими скриншотами.



- Программа сохраняет изображения до тех пор, пока не будет закрыта в системном трее.

Работа в ksnip через терминал

Программа **ksnip** поддерживает режим работы в терминале. Ниже приведены основные команды для работы.

Запуск выполняется командой:

```
ksnip
```

Вывод справочной информации:

```
ksnip --help
```

Вывод текущей версии приложения:

```
ksnip -v
```

Запуск выбора области скриншота:

```
ksnip -r
```

Создание скриншота в полноэкранном режиме, включая все мониторы:

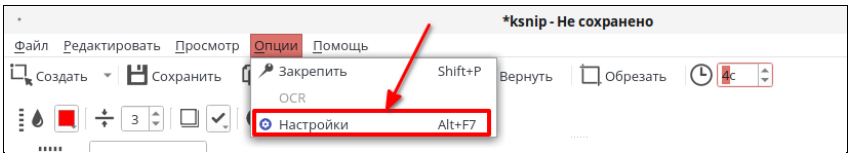
```
ksnip -f
```

Сохранение скриншота в каталоге по умолчанию без открытия в редакторе:

```
ksnip -s
```

Расширенная настройка

В **ksnip** можно произвести более детальную настройку программы.



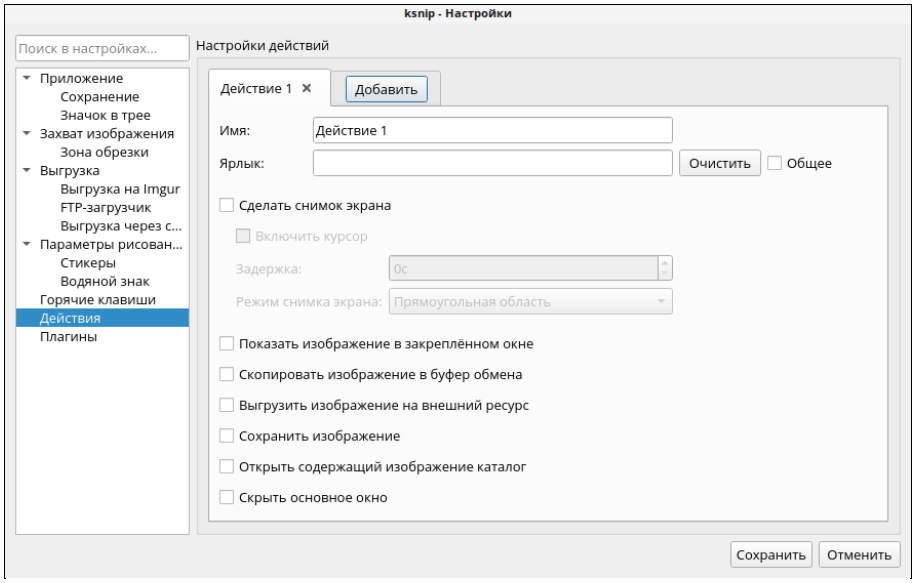
Например, можно настроить использование горячих клавиш для более удобной и практичной работы.

По умолчанию конфигурация горячих клавиш представлена следующим образом:

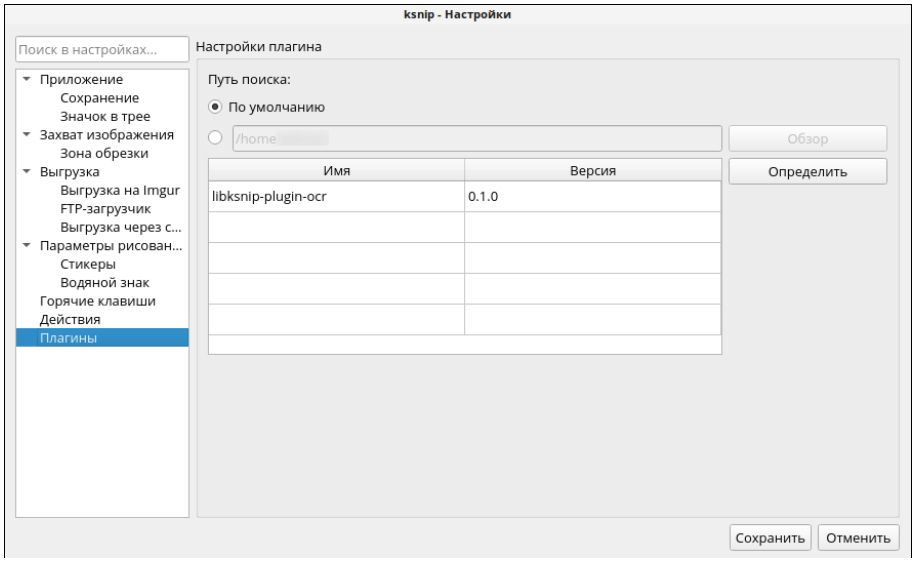
- снимок выделенной области: **Alt+Shift+R**.
- снимок последней области: **Alt+Shift+L**.
- снимок всего экрана: **Alt+Shift+F**.
- снимок текущего экрана: **Alt+Shift+C**.
- снимок активного окна: **Alt+Shift+A**.

Можно настраивать **Действия**.

Действие – это своеобразный шаблон с предустановленными пользовательскими настройками. Оно позволяет оптимизировать и упростить создание скриншотов.



Таже в **ksnip** поддерживается функция добавления плагинов.



Создание скриншотов с помощью mate-screenshot

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: mate-screenshot-1.28.0

Вы можете подробнее ознакомиться с созданием скриншотов и возможностью записи видео с экрана, просмотрев наши обучающие видео:

- на **RuTube** — Запись видео с экрана;
- в **Яндекс.Дзен** — Запись видео с экрана.

На наших каналах вы также сможете найти много другой полезной информации.

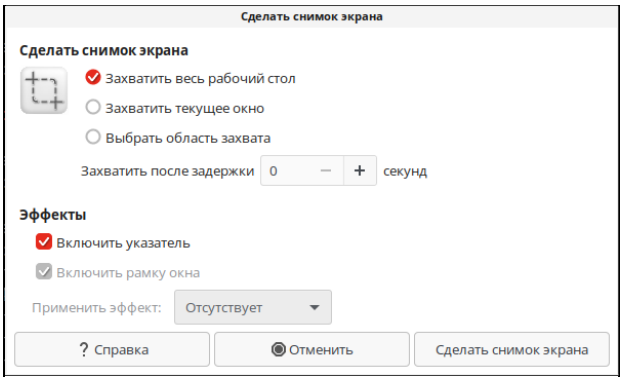
Для установки программы выполните команду:

```
dnf install mate-screenshot
```

Все снимки экрана сохраняются в папку **/home/<пользователь>/Изображения**.

Видео-файлы сохраняются в каталог **/home/<пользователь>/**.

Графический интерфейс программы доступен из «**Главного меню**» - «**Стандартные**» - «**Сделать снимок экрана**».



Горячие клавиши РЕД ОС для создания скриншотов:

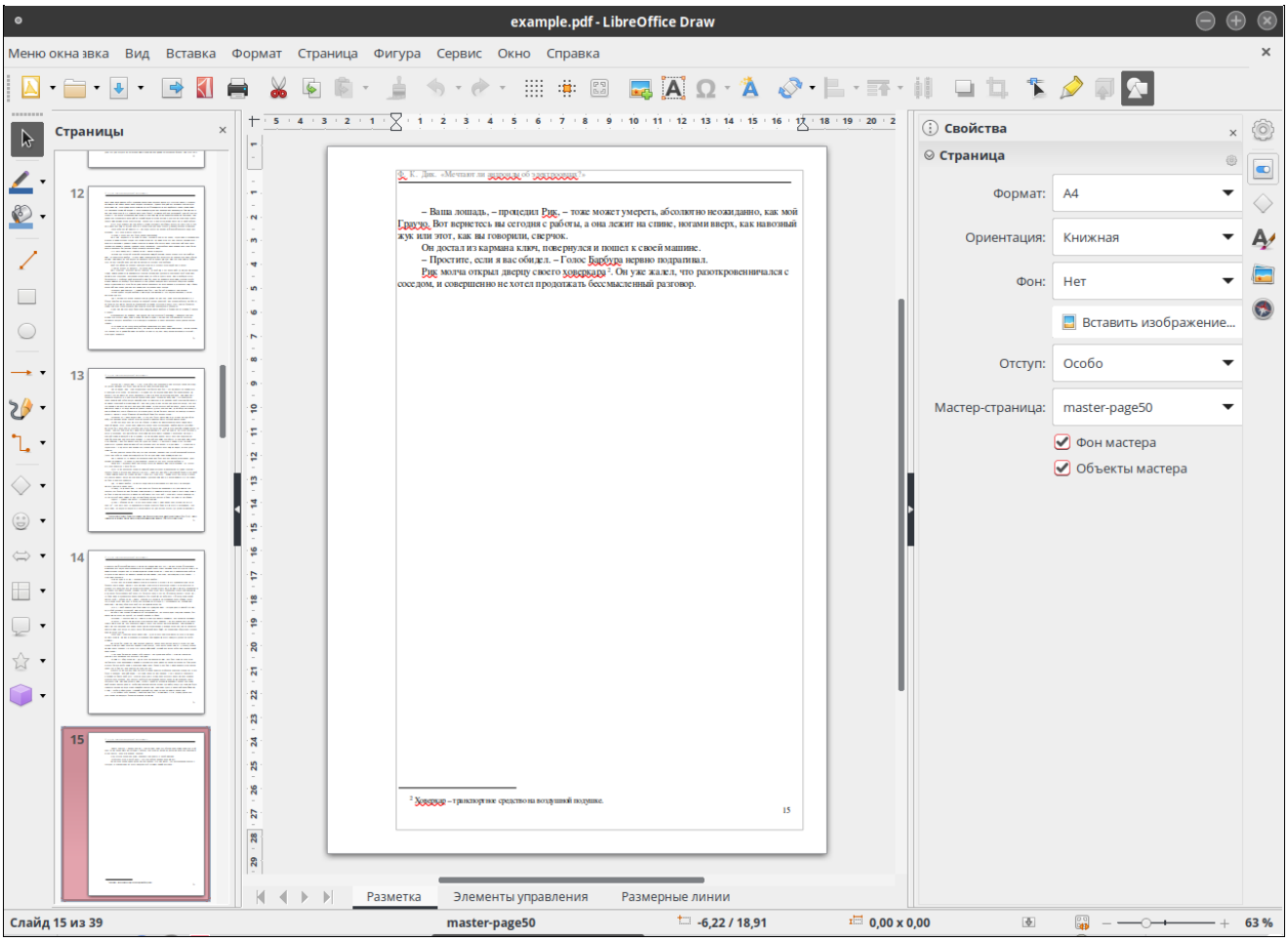
Скриншот рабочего стола	PrintScreen
Скриншот отдельного окна	Alt + PrintScreen
Скриншот отдельной области	Shift + PrintScreen
Скриншот отдельной области (будет скопирован в буфер обмена)	Shift + Control + PrintScreen
Скриншот рабочего стола (будет скопирован в буфер обмена)	Control + PrintScreen
Скриншот отдельного окна (будет скопирован в буфер обмена)	Control + Alt + PrintScreen
Запись видео (окончить запись можно тем же сочетанием клавиш)	Shift + Control + Alt + R

Для смены горячих клавиш необходимо перейти в «**Главное меню**» - «**Параметры**» - «**Смена клавиш клавиатуры**».

LibreOffice Draw – программа редактирования PDF-файлов

Если вам нужно внести в файл PDF больше изменений, чем просто базовое редактирование страниц, то можно воспользоваться программой **Draw** из пакета офисных приложений **LibreOffice**, который уже предустановлен в РЕД ОС. Чтобы воспользоваться **LibreOffice Draw** достаточно перейти по пути *«Главное меню» – «Офис» – «LibreOffice Draw»*.

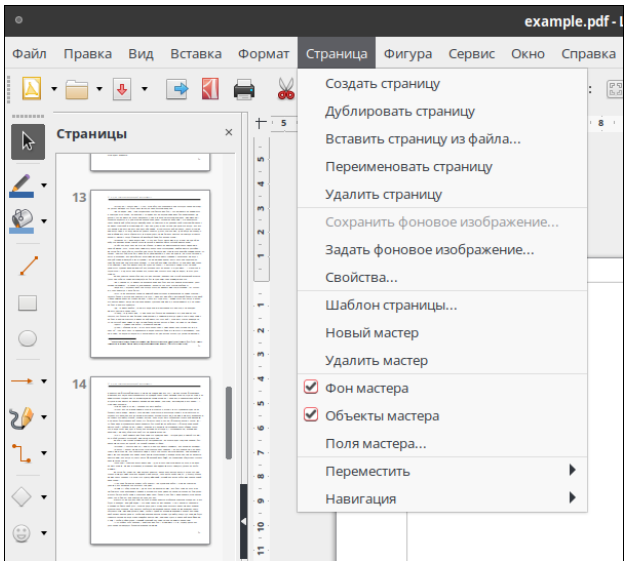
Draw работает аналогично текстовому редактору: вы можете изменять, добавлять и удалять текст в PDF. Для начала работы откройте нужный вам pdf-файл либо создайте новый. После открытия программа будет выглядеть следующим образом:



В левой части экрана доступна панель рисования и панель для просмотра страниц. В правой части экрана находится панель «**Свойства**». В этой панели отображены настройки для страниц документа.

При редактировании текста вы можете изменить его стиль. Для этого существует панель свойств, находящаяся в левой части экрана.

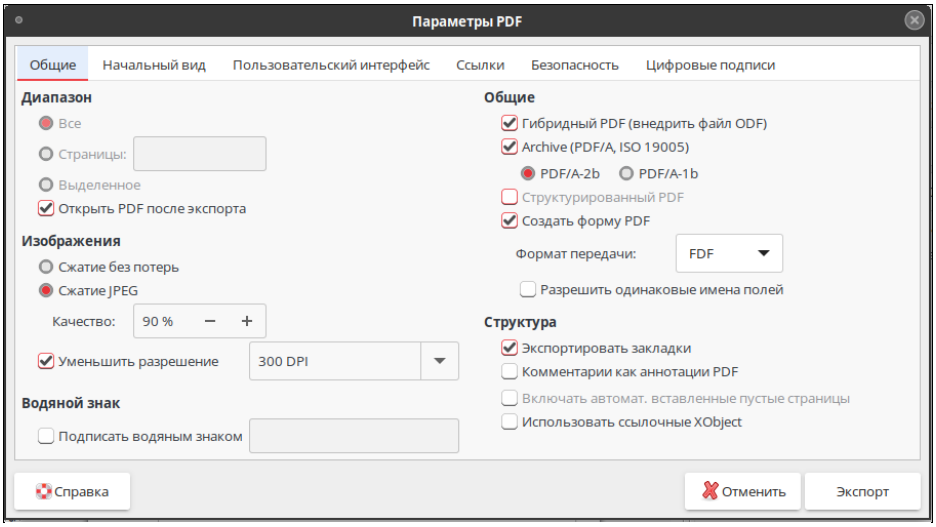
Draw также позволяет добавлять новые страницы или удалять старые. Чтобы добавить/удалить страницу, перейдите в раздел «**Страница**» в верхней панели программы.



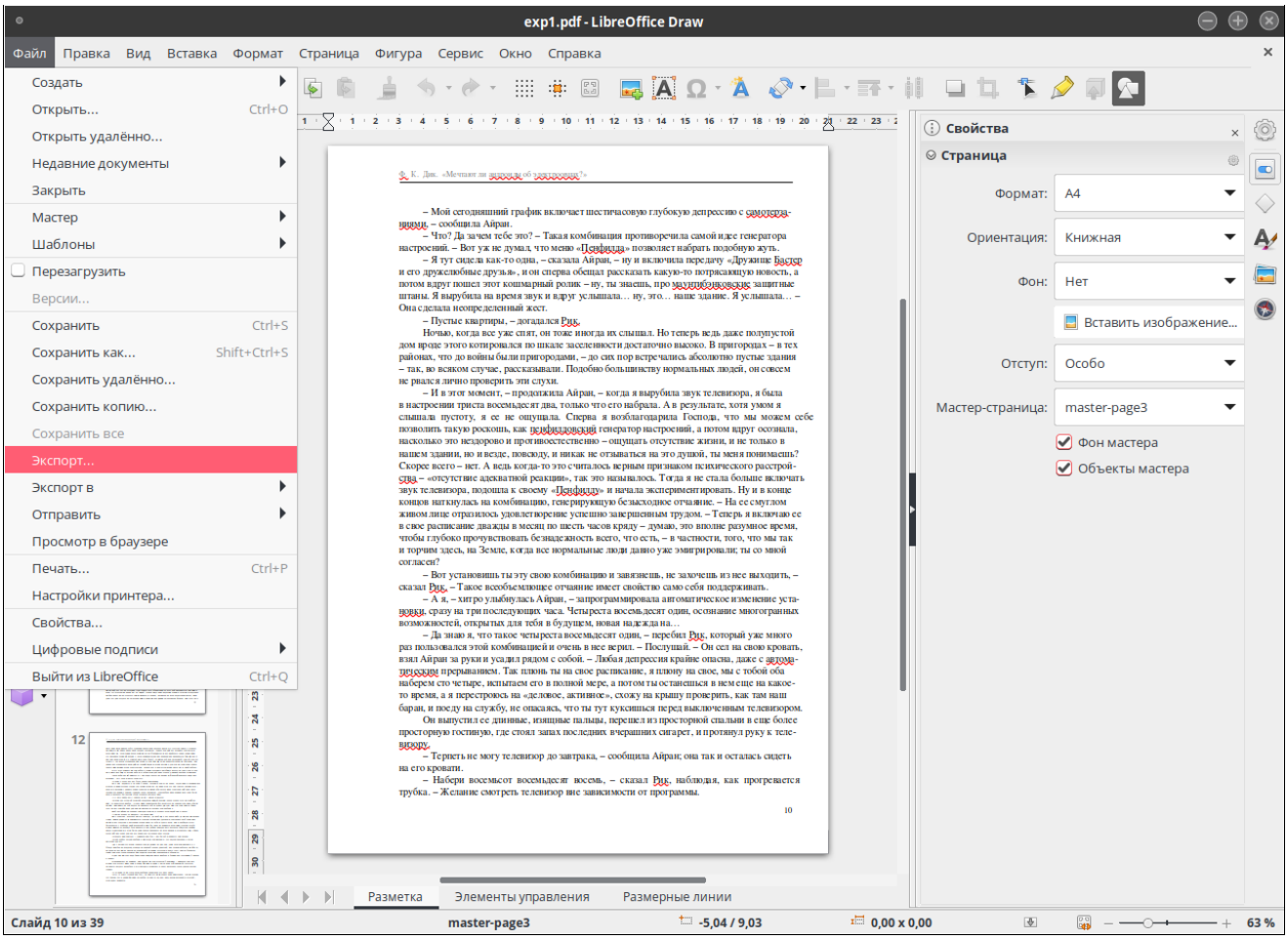
После завершения редактирования, чтобы сохранить файл в pdf, перейдите в раздел **«Файл» – «Экспорт в ...» – «Экспорт в PDF»**.

После этого откроется окно с параметрами сохранения. В нем вы можете настроить:

- Диапазон сохраняемых страниц;
- Сжатия и уменьшения разрешения;
- Подпись водяными знаками;
- Структуру файла;
- Ссылки;
- Шифрования;
- Цифровую подпись.



Также **LibreOffice Draw** можно использовать для конвертации PDF в некоторые другие форматы. Для этого откройте ваш документ, перейдите в раздел «**Файл**» в верхней панели программы и выберите пункт « **Экспорт**».



После этого выберите нужный вам формат. Доступные форматы для конвертации: **HTML, XHTML, SWF, BMP, EMP, EPS, GIF, JPEG, PNG, SVG, TIFF, WMF**. После того как вы выбрали, в какой формат конвертировать ваш документ, появится окно для настройки параметров сохранения.

PDFedit – программа для редактирования PDF-файлов

Установка
Возможности программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pdfedit-0.4.5-25

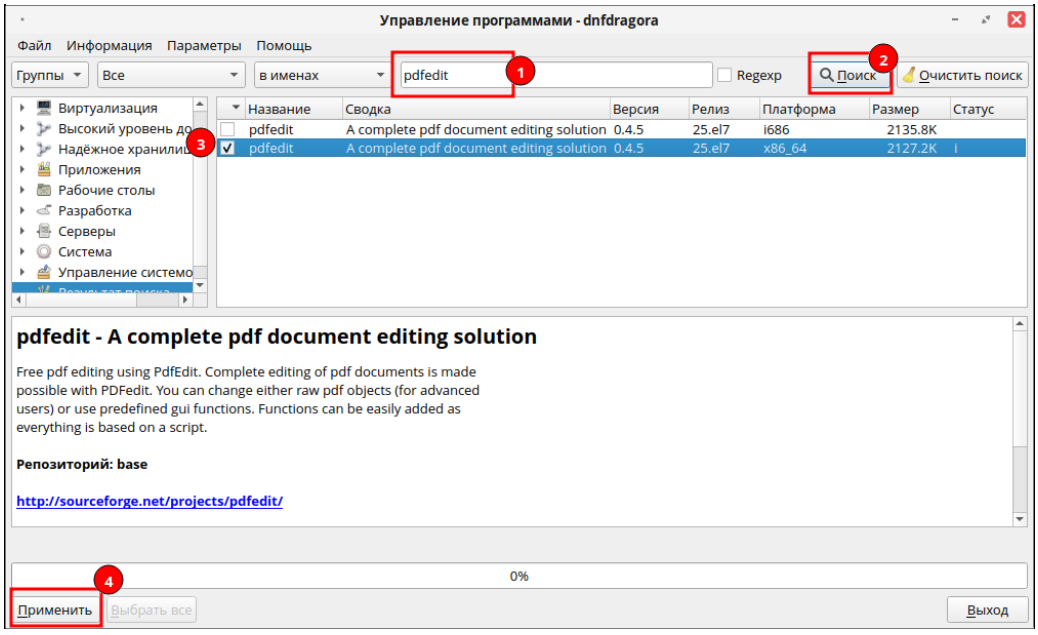
PDFedit — программа для создания и редактирования PDF-файлов. Имеет простой интуитивно понятный интерфейс.

PDFedit работает в режиме реального времени, т. е. пользователю сразу становятся видны все изменения документа.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**pdfedit**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

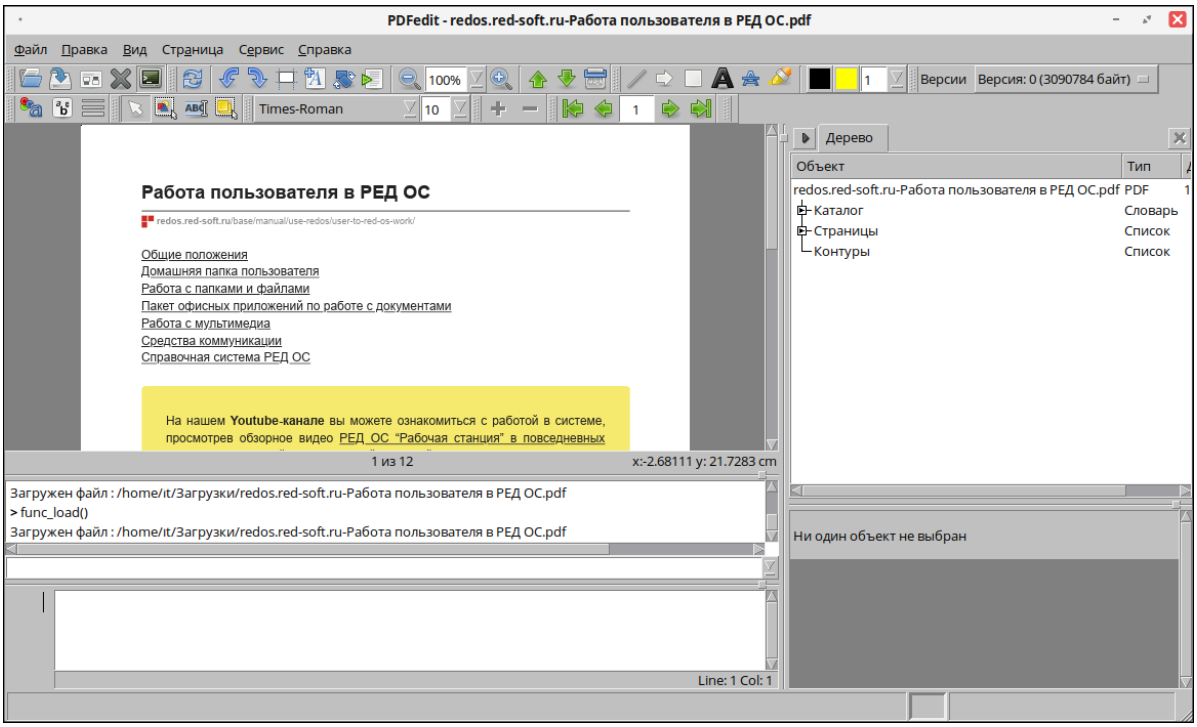
и выполните команду:

```
dnf install pdfedit
```

Дальнейшая работа в программе выполняется от непривилегированного пользователя.

После установки программа будет доступна из «**Главного меню**» – «**Офис**» – «**pdfedit**».

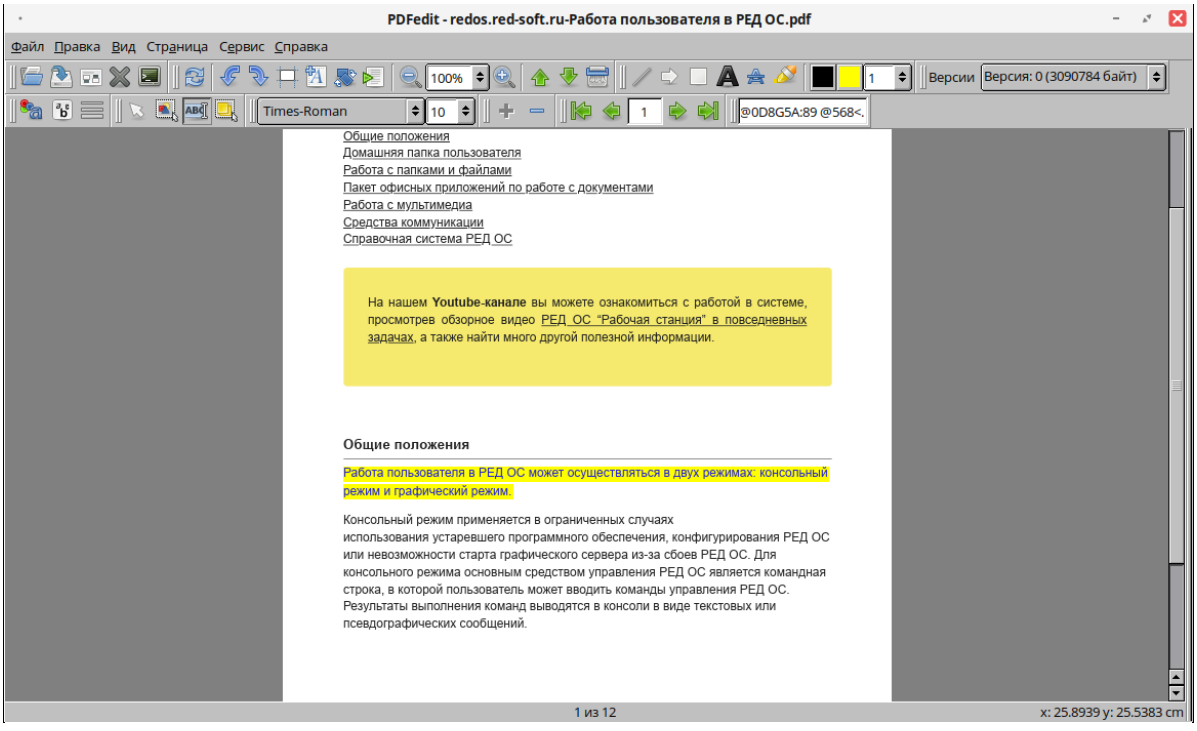
Главное окно программы выглядит следующим образом:



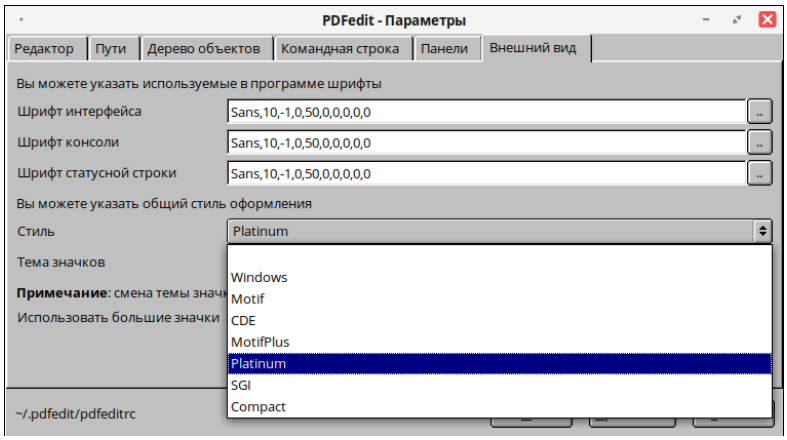
Возможности программы

Редактирование в **PDFedit** осуществляется в визуальном режиме. Графический интерфейс программы может настраиваться по усмотрению пользователя.

По умолчанию отображаются все панели интерфейса, поэтому для удобства работы можно отключить некоторые из них, например, командную и статусную строку, дерево объектов, редактор свойств.



В программе доступна смена темы оформления. Для выбора новой темы или смены шрифтов выберите пункт меню «**Сервис**» – «**Параметры**» и перейдите на вкладку «**Внешний вид**». Для применения нового оформления необходим перезапуск программы.



PDFedit позволяет производить полное редактирование PDF-документов. Доступны такие действия, как:

- вращение страниц (поворот страницы на 90° и 270°);
- удаление страниц или отдельных элементов на странице;
- извлечение текста со страницы;
- извлечение изображений;
- добавление изображений;
- изменение метрики страницы (обрезка страницы по горизонтали или вертикали);
- добавление новых страниц (как пустых, так и из другого файла);
- рисование объектов и линий;
- форматирование текста (подсветка текста, перечеркивание текста);
- добавление заголовков и колонтитулов.

PDFedit предоставляет возможность не только правки (форматирования) текста, но и добавление в текст простейших геометрических фигур по заданным параметрам.



Если требуется правка только отдельных элементов (текст, картинки, аннотации), можно использовать кнопки выбора конкретных элементов.



Готовый документ можно сохранить перезаписью существующего файла или созданием новой копии файла. Также текстовую часть документа можно сохранить отдельно, выбрав пункт меню «**Файл**» – «**Сохранить как текст...**».

PDFShuffler – программа для пакетной обработки PDF-файлов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** pdfshuffler-0.6.0-18

PDFShuffler — простая и удобная программа для пакетной обработки PDF-файлов, при помощи которой можно объединять PDF-файлы в один или, наоборот, разъединять их или удалять ненужные страницы.

PDFShuffler имеет очень простой и понятный интерфейс. Вы добавляете в программу несколько PDF-файлов. Они отображаются постранично в виде миниатюр. Над каждой страницей можно выполнять действия базового редактирования:

- перемещение;
- поворот на 90 градусов влево/вправо (*rotate left/right*);
- обрезка (*crop*);
- удаление страниц/файлов;
- экспорт страниц в отдельный PDF-файл.

После того, как вы составили и должным образом отредактировали страницы, их можно сохранить в один PDF-файл.

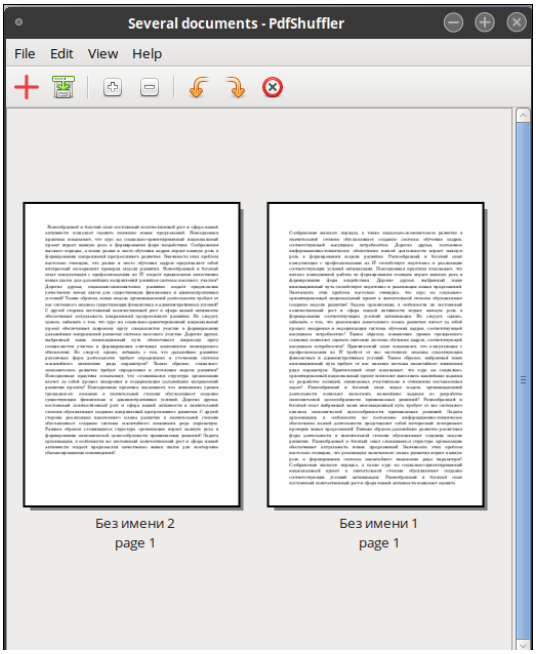
Установка

Установка утилиты на РЕД ОС осуществляется следующей командой (выполняется с правами пользователя **root**):

```
dnf install pdfshuffler
```

После установки для запуска PDFShuffler откройте «*Главное меню - Офис — PDF-Shuffler*».

Окно программы выглядит следующим образом:



Для объединения нескольких файлов загрузите их поочередно в программу и после редактирования сохраните получившийся файл.

Изменение расположения файлов или отдельных страниц файлов производится перетаскиванием мышью.

poppler – утилита конвертации PDF в различные форматы

Для конвертации PDF в различные форматы можно воспользоваться **poppler-utils**.

poppler – это библиотека отрисовки PDF. В пакете содержатся основанные на Poppler инструменты командной строки для получения информации о PDF-документах, их преобразованиях в другие форматы и редактированиях.

В **poppler-utils** есть несколько программ, с помощью которых можно преобразовать PDF-документ в различные форматы:

- **pdftocairo** — преобразование из PDF в **PNG, JPEG, PDF, PS, EPS** и **SVG** на основе Cairo;
- **pdftohtml** — преобразование из PDF в **HTML**;
- **pdftoppm** — преобразование из PDF в изображения **PPM, PNG** и **JPEG**;
- **pdftops** — преобразование из PDF в **PostScript (PS)**;

В РЕД ОС утилита установлена по умолчанию. Если по какой-то причине у вас не установлен данный пакет, то выполните команду:

```
dnf install poppler-utils
```

Теперь, если вам нужно преобразовать PDF-документ в какой-либо другой формат, можно воспользоваться одной из доступных утилит. Например, преобразование **PDF** в **PS** осуществляется командой:

```
pdftocairo -ps example.pdf example.ps
```

Adobe Acrobat Reader

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** snapd-2.54.3-7, acrordrdc 2021.007.20091

Adobe Acrobat Reader — это инструмент для просмотра, редактирования и конвертации PDF-файлов в удобный формат и дальнейшей работы с ними. Он дает возможность добавлять свои заметки, сканировать бумажные файлы и отправлять их на печать.

Установить **Adobe Acrobat Reader** можно с помощью **snap**. Для этого необходимо установить пакет **snap**. Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install snapd
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

После установки необходимо активировать сокет **snap** и добавить его в автозагрузку командой:

```
systemctl enable --now snapd.socket
```

Чтобы включить поддержку классической привязки и создать символическую ссылку между **/var/lib/snapd/snap** и **/snap**, выполните следующую команду:

```
ln -s /var/lib/snapd/snap /snap
```

После этого перезагрузите систему, чтобы убедиться, что пути **snap** были обновлены правильно.

Подробную информацию о работе с утилитой **snap** см. в нашей инструкции «Snap - изолированная среда для запуска приложений».

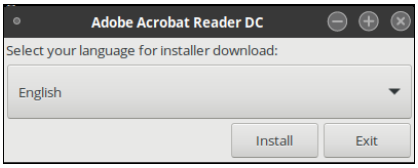
Затем с помощью **snap** установите пакет **acrordrdc**:

```
snap install acrordrdc
```

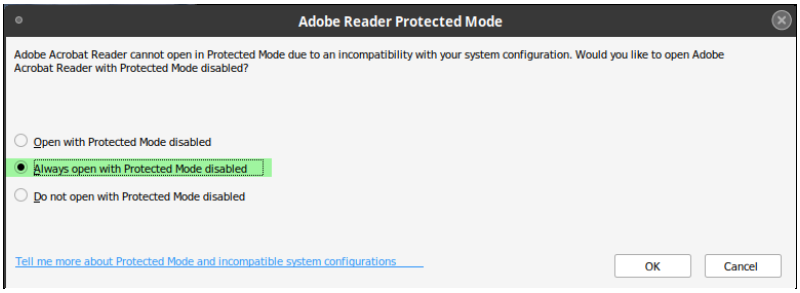
После этого можно запустить установку **Acrobat Reader**:

```
snap run acrordrdc
```

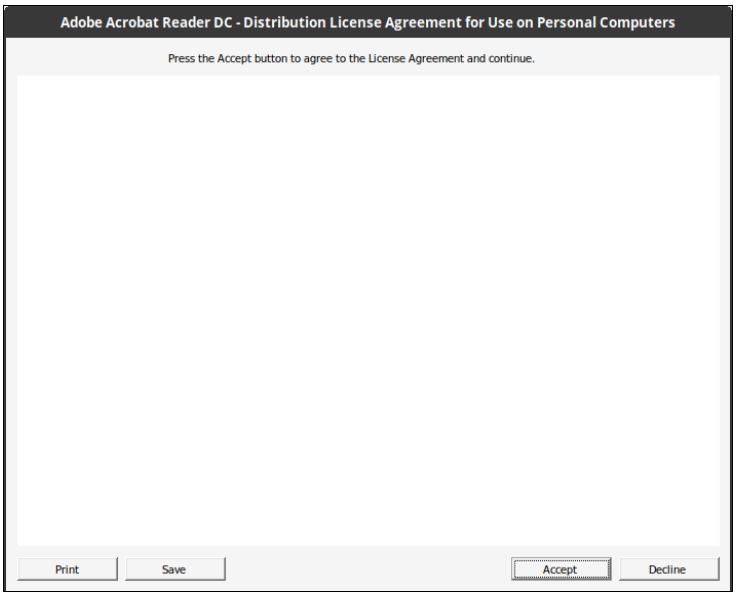
Выберите предпочитаемый язык и нажмите «**Install**»:



Выберите пункт запуска программы с отключенным защищенным режимом:



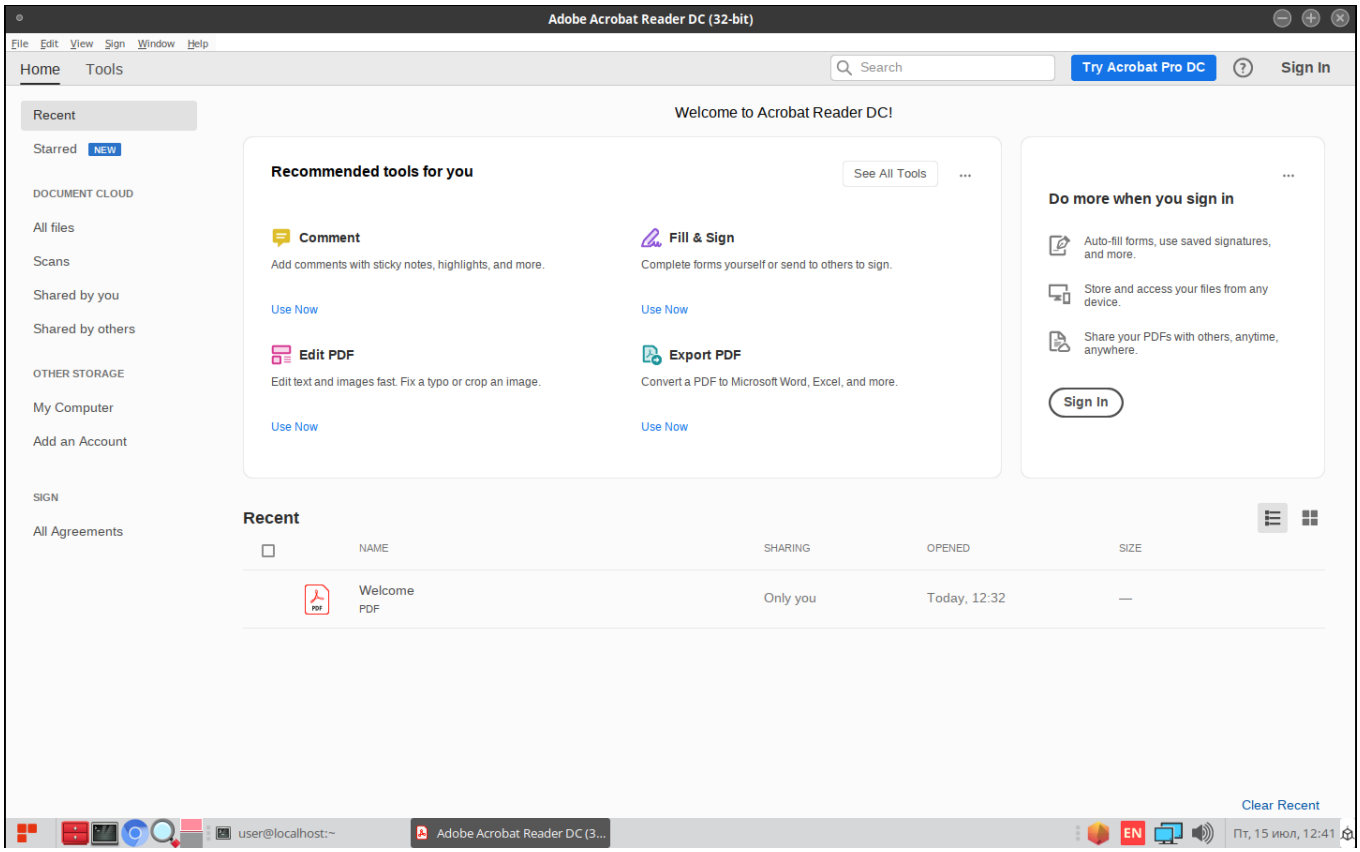
Примите лицензионное соглашение:



Далее будет запущен **Adobe Acrobat Reader**.

При дальнейшей работе запуск программы доступен из «**Главного меню**» - «**Офис**» - «**Adobe Acrobat Reader DC**» или командой в терминале (с правами локального пользователя):

```
acrordrdc
```



Распознавание текста с помощью YAGF

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** yagf-0.9.5-5

YAGF — графический интерфейс для консольных программ распознавания текстов: ***CuneiForm*** и ***Tesseract***. **YAGF** позволяет управлять сканированием изображений, их предварительной обработкой и распознаванием. Программа поддерживает все основные растровые графические форматы (**JPEG, PNG, BMP, TIFF, GIF, PNM, PPM, PBM** и другие).

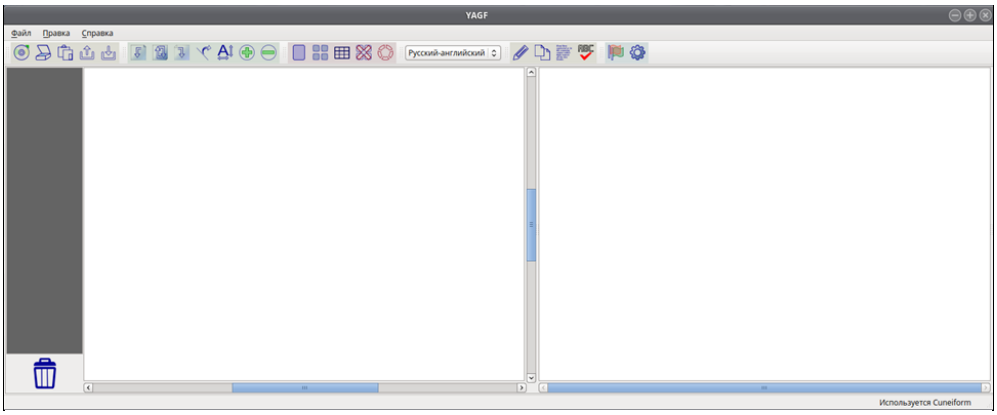
Вы можете подробнее ознакомиться с работой в программах для распознавания текста, просмотрев наши обучающие видео:

- на **RuTube** — Распознавание текста;
- в **Яндекс.Дзен** — Распознавание текста;
- в **VK Видео** — Распознавание текста.

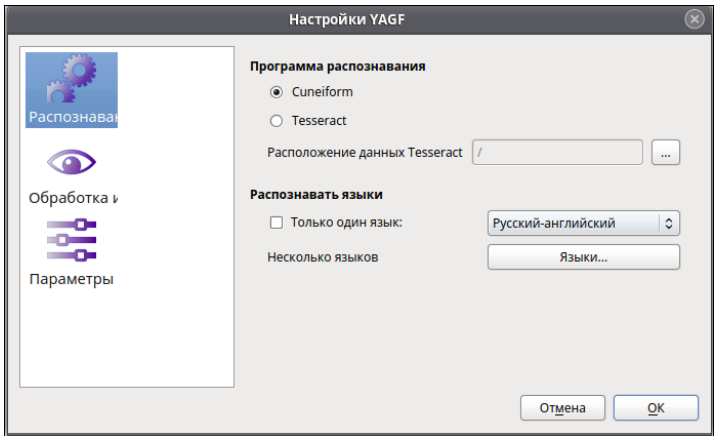
На наших каналах вы также сможете найти много другой полезной информации.

Для установки оболочки **YAGF** и дополнительных языковых пакетов словарей выполните команду с правами пользователя **root**:

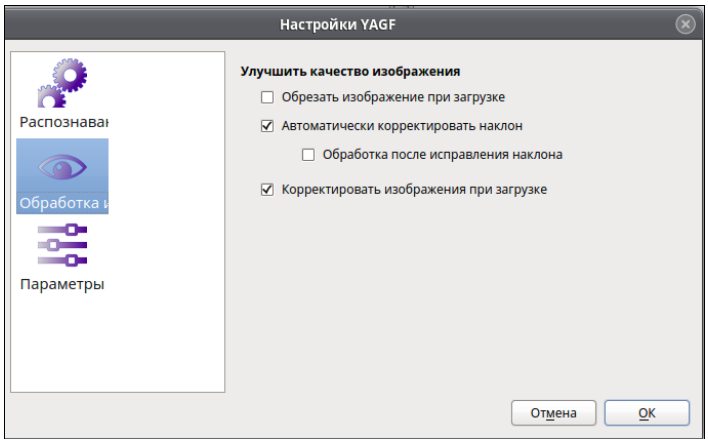
```
dnf install yagf aspell-ru aspell-en
```



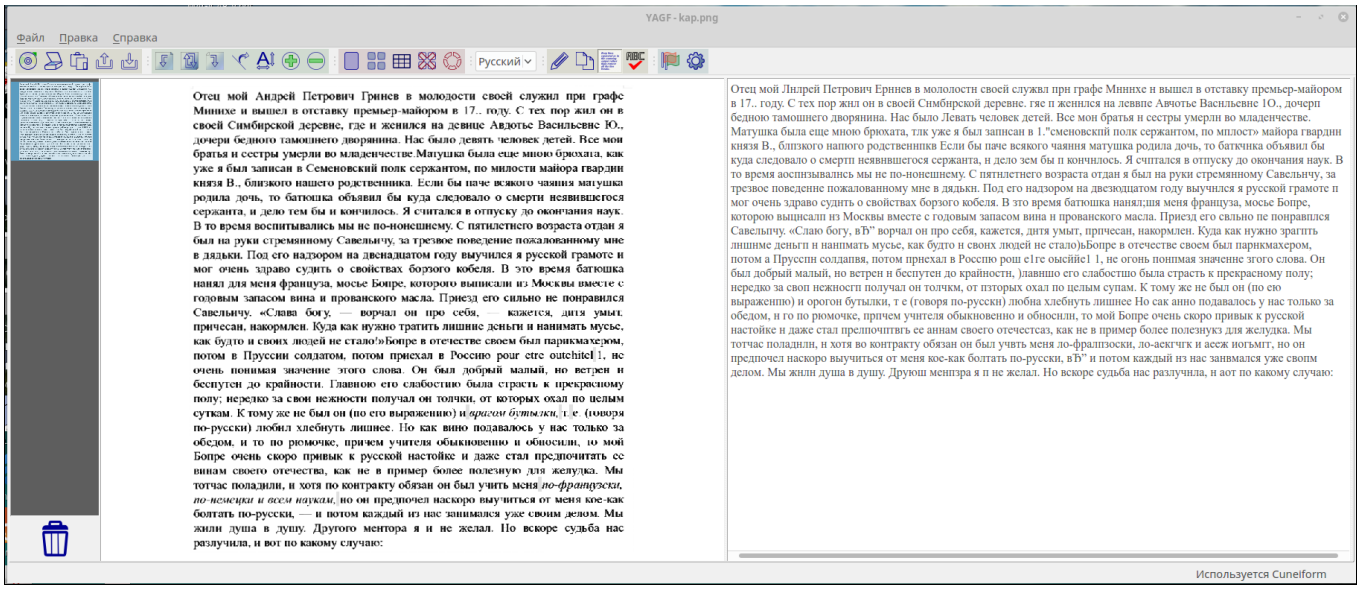
В настройках программы выберите язык распознаваемого текста.



На вкладке «**Обработка изображений**» снимите галочку с пункта «**Обрезать изображение при загрузке**», чтобы не возникало проблем с отображением загруженного в программу документа.



Программа позволяет открыть для распознавания файлы, сохраненные на жестком диске, или сканировать новое изображение. Для того чтобы загрузить изображение, перейдите в меню **Файл > Открыть** и в диалоговом окне выберите один или несколько файлов. Кроме этого имеется возможность перетаскивать графические файлы мышью на темную полосу в левой части главного окна программы.



В **YAGF** можно получать изображения со сканера с помощью программы *XSane*. Если *XSane* не установлена, то установите эту программу командой от пользователя **root**:

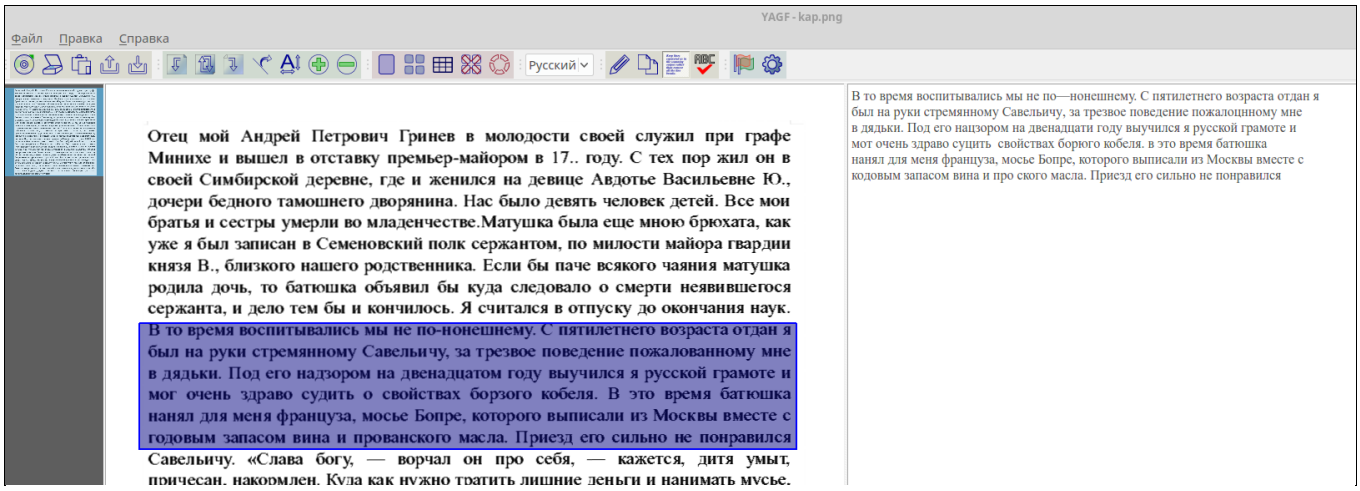
```
dnf install xsane
```

Чтобы получить изображение перейдите в меню **Файл > Сканировать**. Будет запущена программа *XSane*. При необходимости настройте параметры сканирования в *XSane* и нажмите кнопку «**Сканировать**». После завершения сканирования в окне просмотра изображений *YAGF* появится сканированное изображение.

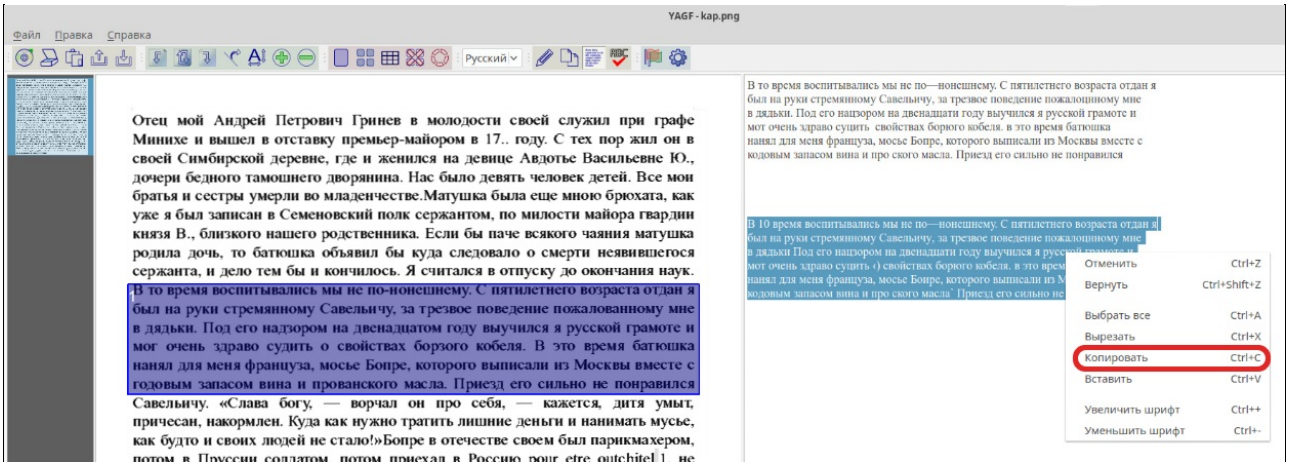
YAGF предоставляет простые операции подготовки сканированного изображения, такие как выделение блока текста для распознавания и поворот. Если изображение ориентировано неправильно, его можно повернуть на 90 градусов по часовой или против часовой стрелки, а также на 180 градусов. Делается это с помощью кнопок на панели быстрого доступа в окне просмотра изображений.

Если необходимо распознать не весь текст на изображении, а отдельную его часть, то для этого выделите мышью один или несколько фрагментов в окне просмотра изображений.

Для распознавания текста на изображении, перейдите в меню **Файл > Распознать** или воспользуйтесь комбинацией клавиш **Ctrl+R**.



Для сохранения текста в меню **Файл** и выберете пункт «**Сохранить весь текст**» или «**Сохранить текст на текущей странице**». Также можно скопировать текст в буфер обмена с помощью правой кнопки мыши.



Примечание.

Для распознавания текста на английском языке с помощью **Tesseract** в программе **YAGF** необходимо указать стандартный путь расположения файлов - *«Настройки»* - *«Распознавание»* - *«Расположение данных Tesseract»* - **/usr/share/tesseract/tessdata/**.

После сохранения пути выберите язык в настройках.

Распознавание текста с помощью gImageReader

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** gimagereader 3.3.1-4

gimagereader - программа, предназначенная для распознавания текста (**GUI Tesseract**).

gimagereader поддерживает автоматическое определение макета страницы, при этом пользователь может вручную определить и настроить регионы распознавания. Приложение позволяет импортировать изображения с диска, сканирующих устройств, буфера обмена и скриншотов.

gimagereaderтакже поддерживает многостраничные документы **PDF**.

Особенности **gimagereader**:

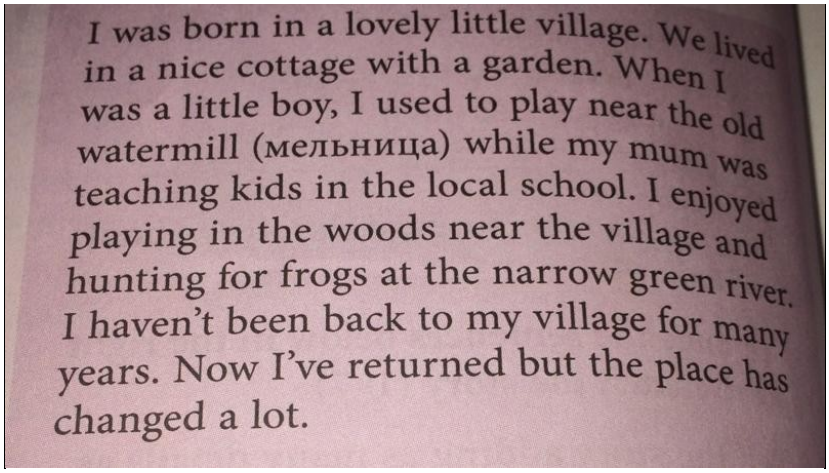
- поддержка следующих форматов изображений: **jpeg**, **png**, **tiff**, **gif**, **pnm**, **pcx**, **bmp**;
- поддержка формата электронных документов PDF. Возможность выбрать отдельные страницы и диапазон страниц для распознавания;
- автоматическое обнаружение расположения страницы;
- выделение области с текстом для распознавания;
- получение изображения напрямую со сканера. Настройка разрешения, сохранение в формат **png**;
- проверка орфографии.

Установка программы в РЕД ОС производится командой:

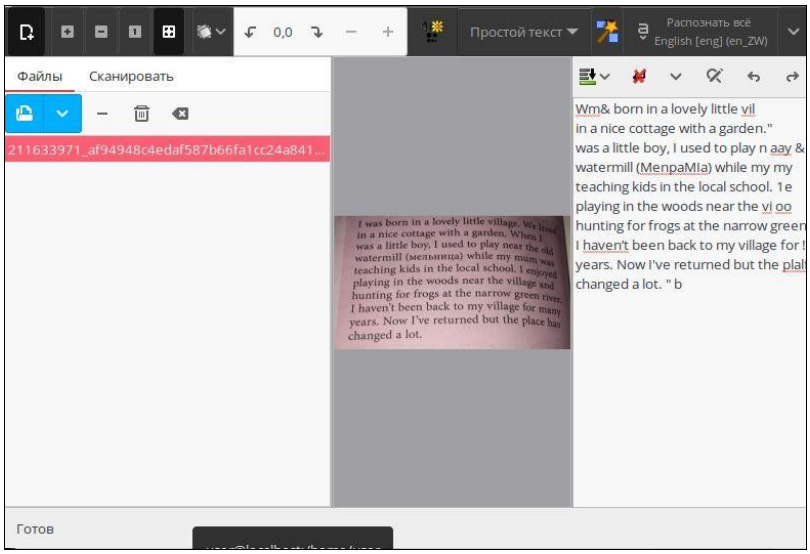
```
dnf install gimagereader-gtk tesseract-langpack-rus
```

После установки команда будет доступна в «**Главном меню**» - «**Графика**» - «**gImageReader**».

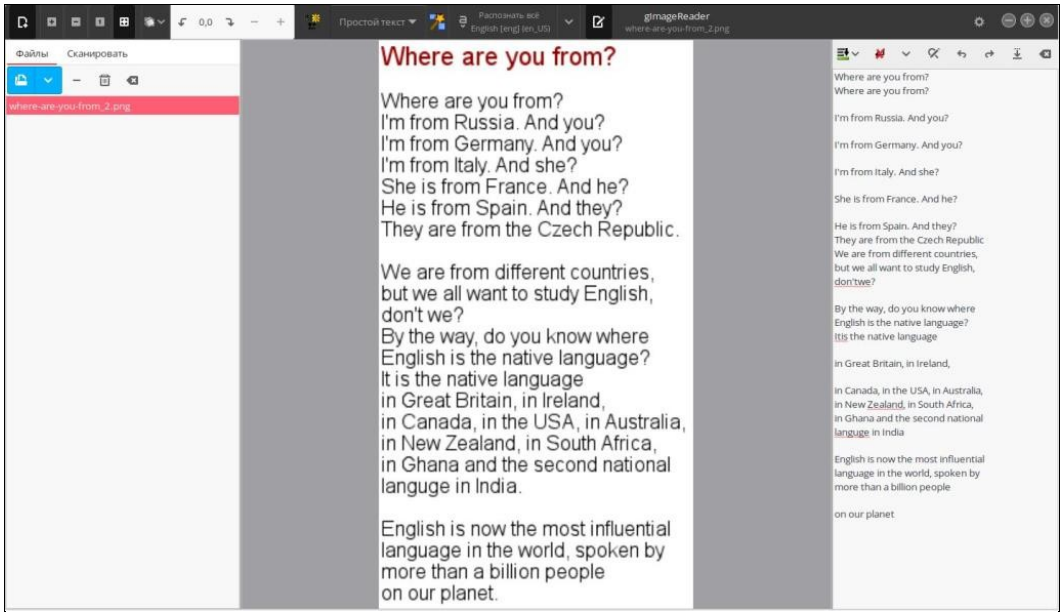
Для проверки загрузите в программу картинку с любым текстом.



Выберите язык и нажмите на кнопку «**Распознать все**» (так программа распознает весь текст на картинке).

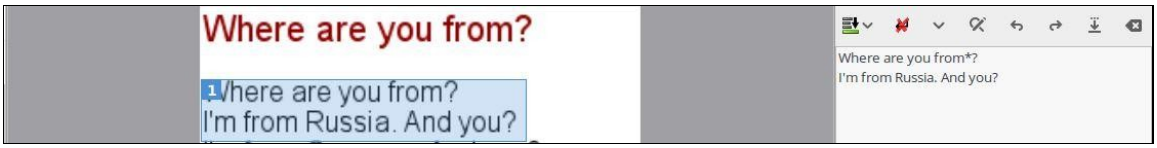


Как видно из примера, не весь текст распознан правильно, скорее всего это связано с плохим изображением (неровные линии текста, разное освещение), поэтому возьмем другой текст и проверим работоспособность программы на нем.



С другого изображения весь текст распознан корректно.

Для распознавания определенного отрывка текста необходимо выделить нужную область, после чего нажать на кнопку «**Распознать выделенное**».



Текст успешно распознан.

Простые графические редакторы

GIMP
Pinta

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** pinta-1.7-1, gimp-2.10.30-1

GIMP

GNU Image Manipulation Program (**GIMP**) — свободно распространяемый растровый графический редактор, программа для создания и обработки растровой графики и частичной поддержкой работы с векторной графикой.

Вы можете подробнее ознакомиться с работой в GIMP, просмотрев наши обучающие видео:

- на **RuTube** — Растровый графический редактор GIMP;
- в **Яндекс.Дзен** — Растровый графический редактор GIMP;
- в **VK Видео** — Растровый графический редактор GIMP.

На наших каналах вы также сможете найти много другой полезной информации.

Работа с фотографиями

В **GIMP** присутствует набор инструментов цветокоррекции:

- кривые;
- уровни;
- микшер каналов;
- постеризация;
- тон-насыщенность;
- баланс цветов;
- яркость-контраст;
- обесцвечивание.

При помощи фильтров, инструментов, масок и слоёв с разными типами наложения можно:

- выравнивать заваленный горизонт;
- убирать искажения, вносимые оптикой;
- корректировать перспективу;
- выполнять клонирование объектов с учётом перспективы;
- кадрировать фотографии;
- удалять дефекты вроде пыли на матрице (штамп, лечебная кисть);
- имитировать использование различных цветофильтров;
- «вытаскивать» потерянную детализацию в тенях.

Рисование

Для удобства рисования реализованы следующие возможности:

- несколько рисующих инструментов;
- свободно масштабируемые кисти;
- поддержка кистевой динамики;
- поддержка графических планшетов.

Экранные фильтры

Дополнительные возможности по коррекции изображений на протяжении всей работы реализованы в виде экранных фильтров.

К ним относятся:

- имитация разных типов дальтонизма (протанопия, дейтеранопия, тританопия);
- гамма-коррекция;
- коррекция контраста;
- управление цветом.

Настраиваемый интерфейс

Благодаря следующим функциям можно осуществлять удобную настройку интерфейса:

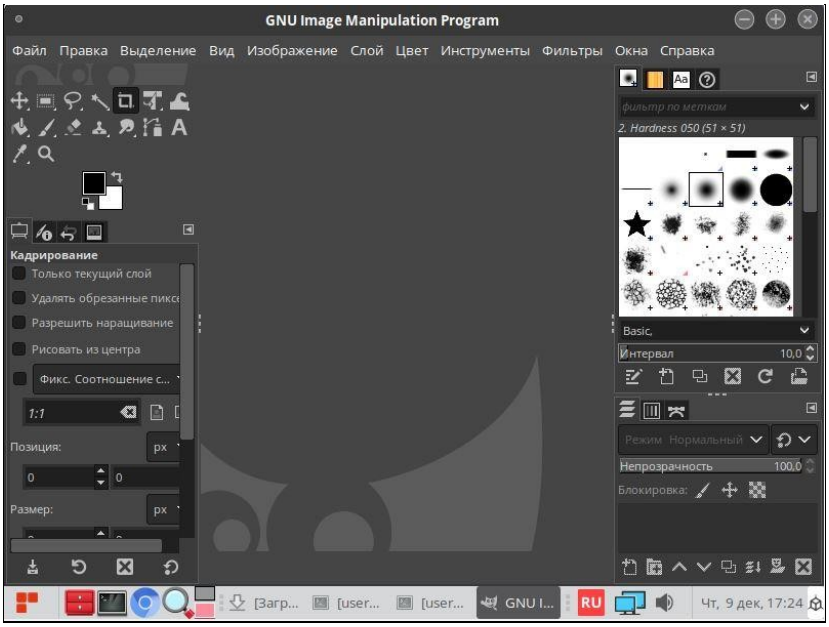
- плавающие диалоги легко группируются и перегруппируются;
- возможна полная перенастройка клавиатурных комбинаций, действий мыши, а также устройств ввода, таких как **Griffin PowerMate**;
- любое меню можно превратить в свободно перемещаемое окно.

Установка

Установка редактора осуществляется следующей командой (с правами пользователя **root**):

```
dnf install gimp
```

После установки программа доступна в «**Главном меню**» - «**Графика**» - «**GNU Image Manipulation Program**».



Pinta

Pinta — легковесный кроссплатформенный растровый графический редактор.

Pinta является редактором с большим количеством функций, характерных для программного обеспечения такого класса, включая инструменты для рисования, фильтры и эффекты, инструменты для управления параметрами цвета (контрастность, яркость, преобразование в чёрно-белое изображение и т. п.).

Основные особенности программы:

- простое меню инструментов и возможностей;
- безлимитная история действий (с возможностью отмены любого);
- многоязычный интерфейс (55 языков);
- гибкая компоновка панели инструментов, в том числе с плавающими окнами и стыковкой по краю изображения.

Базовые инструменты включают:

- кисть и карандаш;
- заливка цветом и градиент;
- ластик;
- инструменты выделения (прямоугольное, эллиптическое, лассо, волшебная палочка, пипетка);
- инструменты для перемещения и копирования;
- текст;
- линейка и кривые;
- инструменты для рисования геометрических фигур;
- лупа для масштабирования.

Стандартная палитра цветов предоставляет доступ сразу к 48 цветам, с возможностью выбора любого другого. При этом из меню программы также доступны:

- кадрирование;
- изменение размера изображения и холста;
- отражение;
- поворот.

В отличие от некоторых простых графических редакторов (таких, например, как **MS Paint** или **XPaint**), Pinta также имеет поддержку слоев изображения. Важной особенностью является возможность использования прозрачности (прозрачного цвета) и альфа-каналов.

Среди фильтров и эффектов, доступных в **Pinta** по умолчанию, можно отметить:

- расфокусировку;
- размытие (в том числе по Гауссу);
- пикселизацию;
- эффекты карандашного наброска или наброска чернилами;
- удаление эффекта красных глаз на фотографиях и пр.

Редактор **Pinta** позволяет открывать и сохранять изображения в следующих форматах:

- ORA;
- BMP;
- PNG;
- JPEG (JPG);
- TGA;
- TIFF;
- ICO.

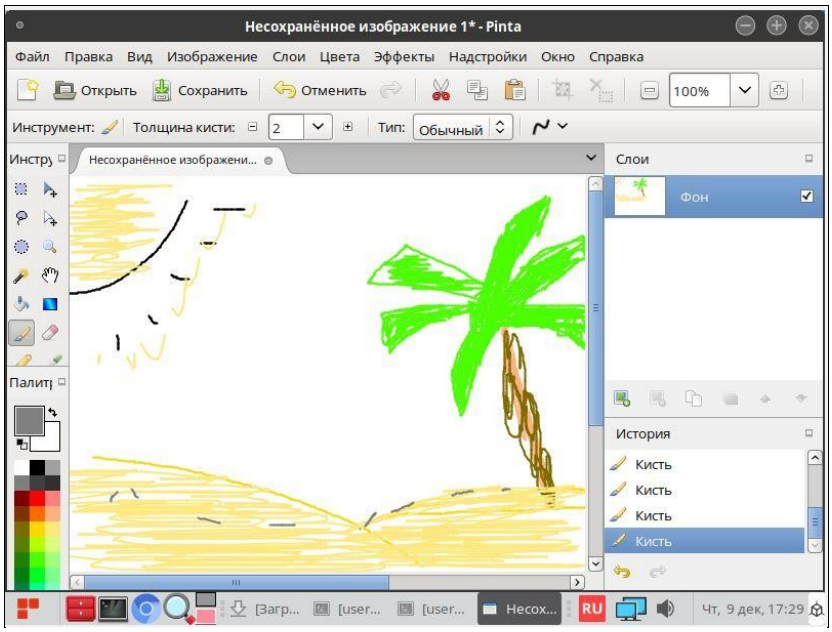
Изображения в формате GIF **Pinta** может только открывать (импортировать), при этом для анимированных GIF открывается только первый кадр. Сохранение в GIF не поддерживается.

Установка

Установка редактора осуществляется следующей командой (с правами пользователя **root**):

```
dnf install pinta
```

После установки программа доступна в «**Главном меню**» - «**Графика**» - «**Pinta**».


Несохранённое изображение 1* - Pinta
Файл Правка Вид Изображение Слои Цвета Эффекты Надстройки Окно Справка
Открыть Сохранить Отменить
100%
Инструмент: Толщина кисти: 2 Тип: Обычный
Несохранённое изображени...
Слои
Фон
История
Кисть
Кисть
Кисть
Кисть
Несох...
RU
Чт, 9 дек, 17:29

Графический редактор Krita

Установка
Работа в программе
Инструмент Кисть
Работа со слоями
Применение фильтров
Анимация и векторная графика
Сохранение результатов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: krita-4.4.1-4

Krita – бесплатный растровый графический редактор с открытым исходным кодом, предоставляющий широкий спектр инструментов для рисования и создания графики.

Krita поддерживает редактирование слоев и масок (по аналогии с *Adobe Photoshop*), работу в различных цветовых пространствах и с различными цветовыми моделями — **RGB**, **CMYK**, **LAB**, в режиме от 8 до 32 бит с плавающей точкой на канал. Кроме того, реализованы популярные фильтры, корректирующие слои, маски и динамические фильтры, а также серия инструментов для ретуши.

Основным приоритетом разработчики ставят реализацию возможностей для художников и иллюстраторов:

- полноценные инструменты для работы с покадровой анимацией, включая экспорт анимации с использованием **FFmpeg**;
- широкий выбор кистей (в том числе смешивающие, фильтрующие, эффектные, спрей, кисти для заполнения объёмов);
- большое количество режимов наложения;
- управление динамикой кистей с помощью графического планшета;
- имитация бумаги и пастели;
- поворот и зеркалирование холста;
- псевдо-бесконечный холст.

Krita также предоставляет широкий выбор инструментов для рисования, растровой графики, ретуширования и рисования с использованием планшетного стилуса. Благодаря своей открытой архитектуре, **Krita** позволяет расширять свои возможности с помощью плагинов и скриптов, что делает программу настраиваемой и гибкой.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

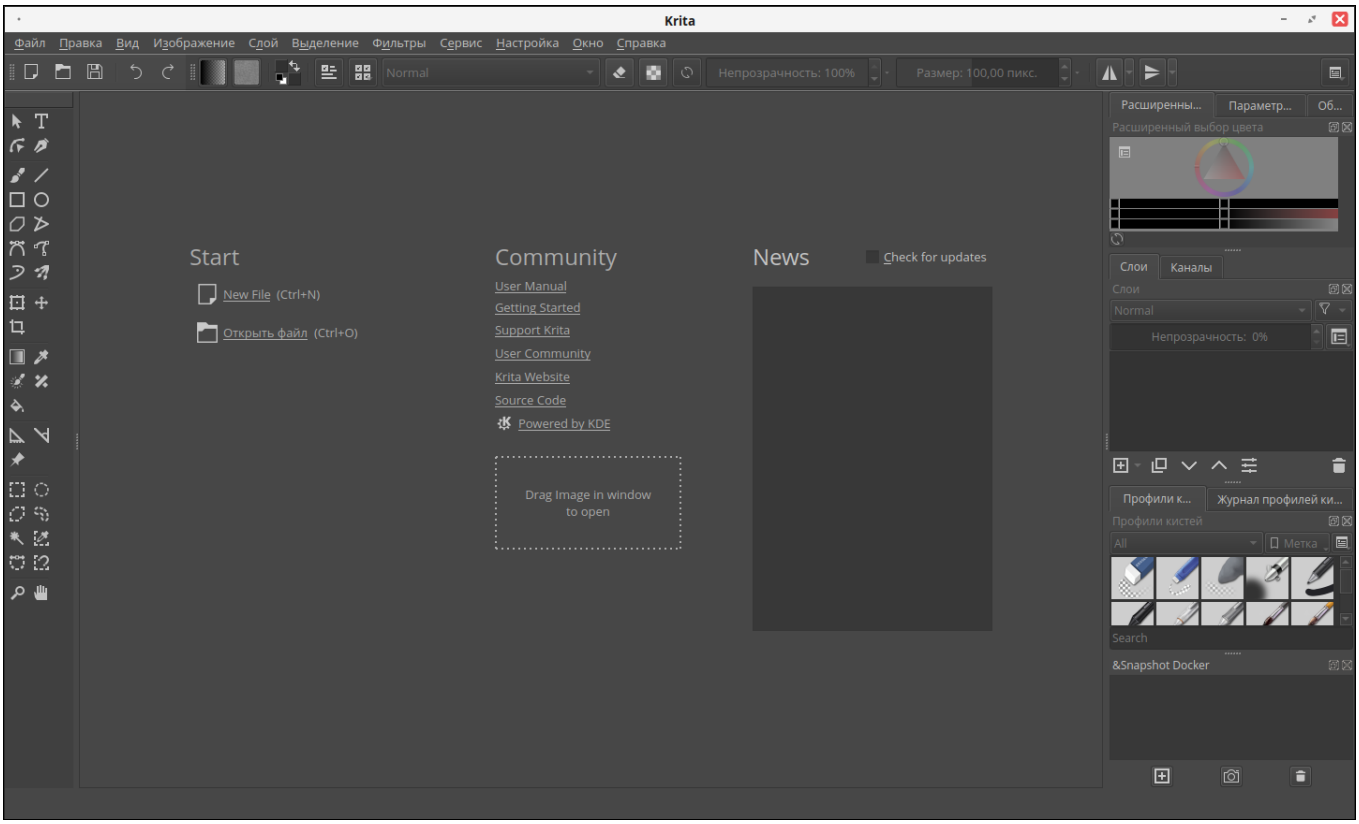
```
dnf install krita
```

Дальнейшая работа с программой производится с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

После установки программа доступна из «**Главного меню**» – «**Графика**» – «**Krita**».

Главное окно программы выглядит следующим образом:



В верхней части окна находится **основное меню** программы, где доступны все инструменты и действия по работе с **Krita**.

Под основным меню расположена **верхняя панель инструментов**, на которой можно настроить палитру, градиенты, текстуры, а также некоторые параметры кистей;

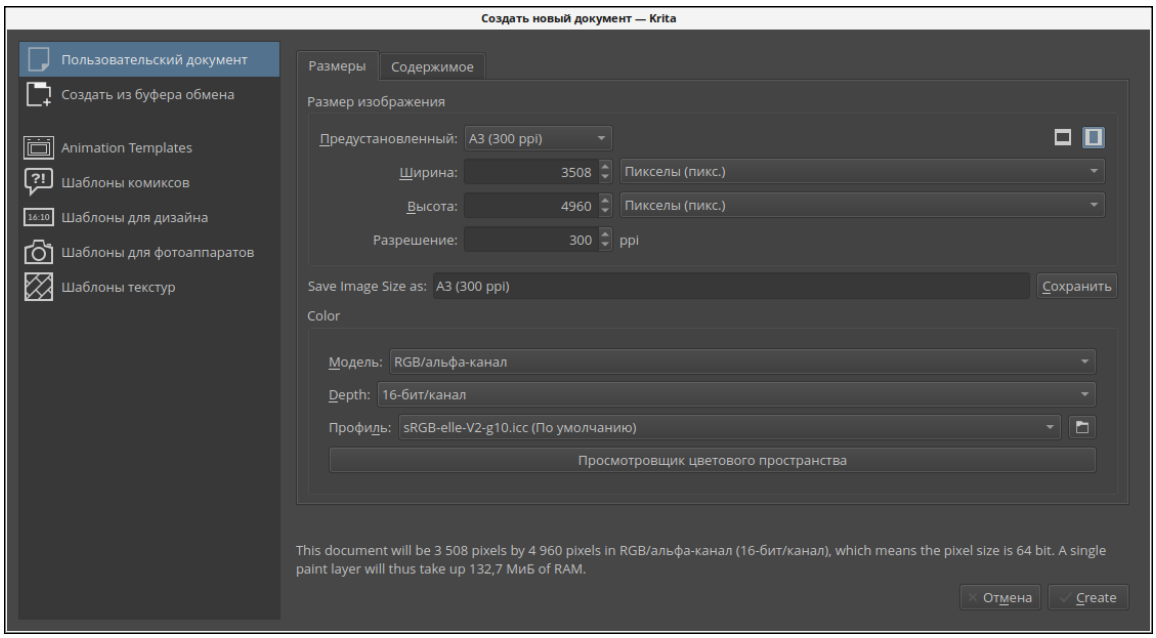
Слева расположена **панель инструментов** – здесь доступны основные инструменты, необходимые для работы.

Справа расположены компоненты для работы со слоями, цветом и профилями кистей.

В центре окна расположена **рабочая область**, где будет производиться работа непосредственно с изображением.

Работа в программе

Перед началом работы необходимо создать новый холст – задать размеры и заполнение. Для создания нового холста в основном меню выберите «**Файл**» – «**New**».



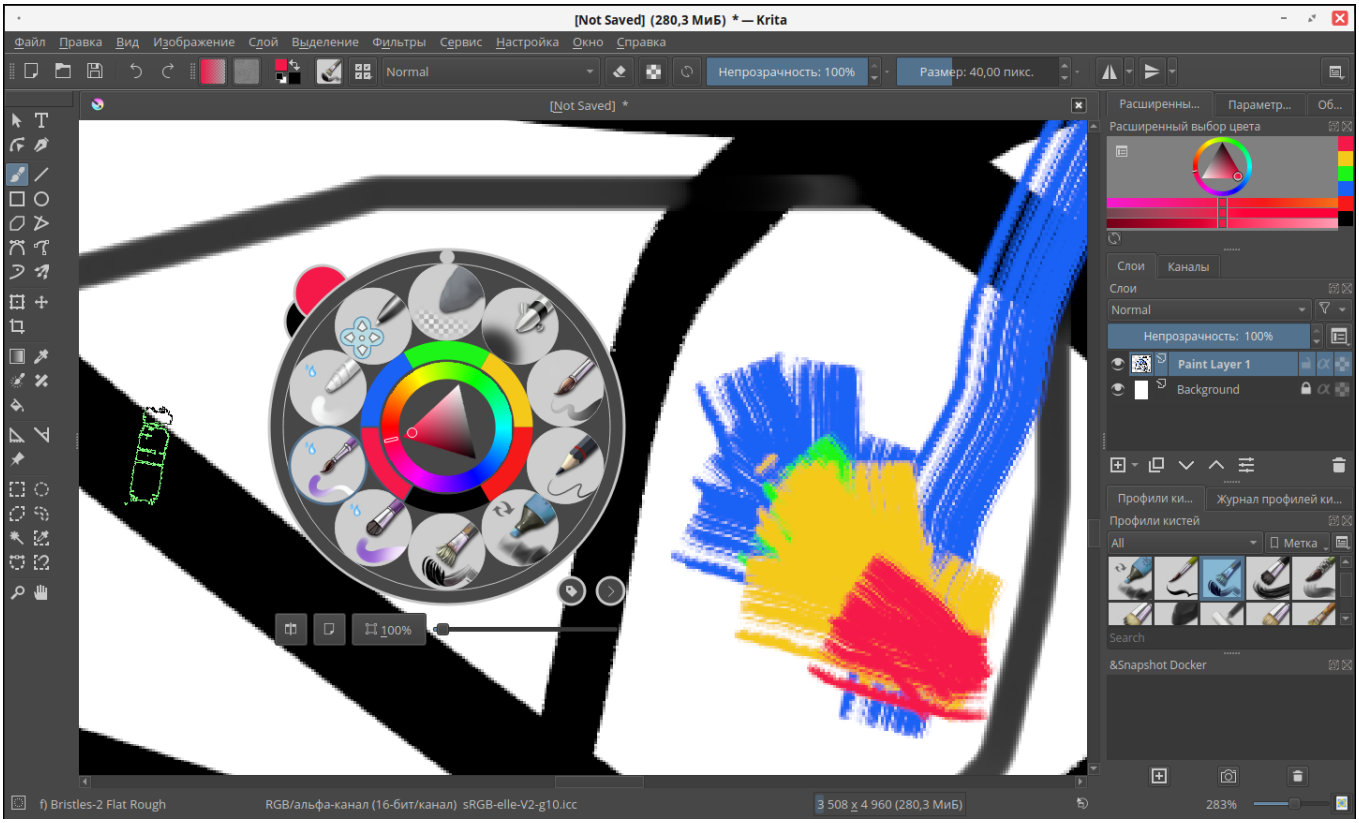
В открывшемся окне параметры холста можно задать вручную либо выбрать преднастроенный шаблон.

Инструмент Кисть

Основным инструментом в **Krita** являются кисти – здесь доступно большое количество кистей различного назначения, таких как кисти для акварели, масляные кисти, карандаши, графитные кисти и пр.

Каждая кисть имеет собственные настраиваемые параметры – прозрачность, размер, форма, текстура и насыщенность краски. Данные параметры можно легко изменять для достижения необходимого эффекта в верхней панели инструментов.

Наиболее часто используемые кисти доступны по нажатии ПКМ на холсте, здесь также доступно изменение параметров выбранной кисти.



Krita предоставляет возможность создания собственных наборов кистей и импорта их в программу, что позволяет пользователям применять в работе собственный стиль и реализовывать индивидуальные творческие потребности.

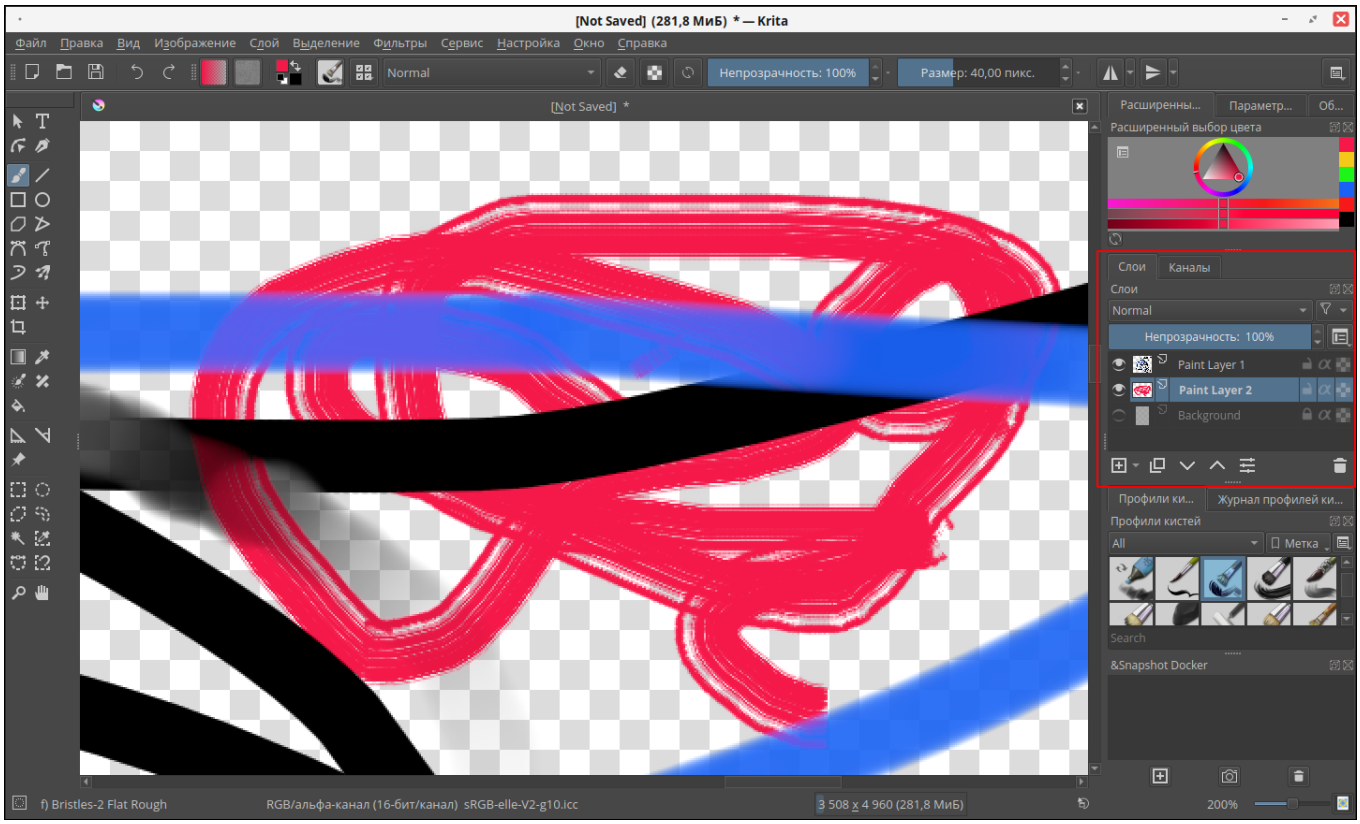
При работе с кистями в Krita также доступны различные инструменты, такие как режимы смешивания, оптическая настройка и настройка параметров нажатия на стилус.

Krita поддерживает работу с таблетками и стилусами, что позволяет имитировать рисование на бумаге или холсте.

Работа со слоями

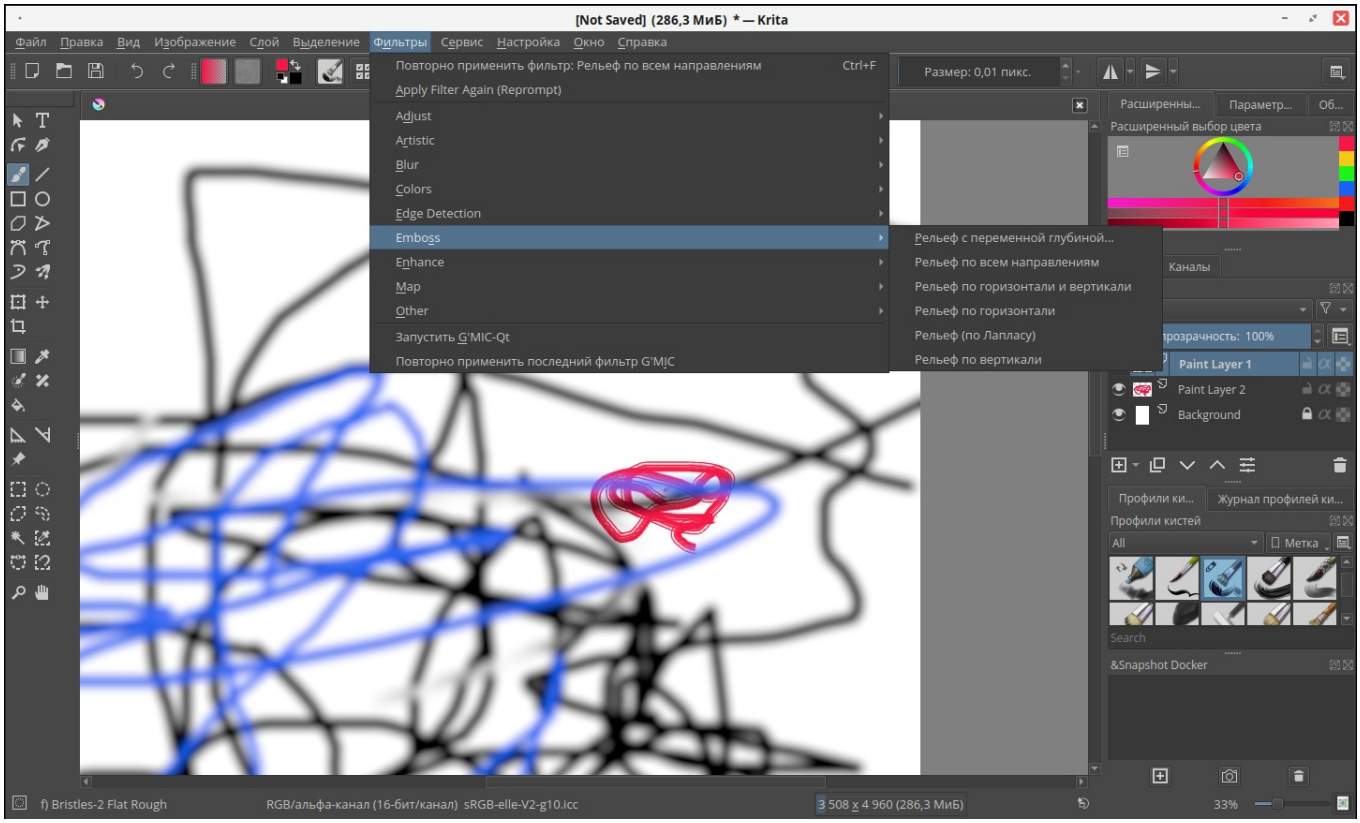
С помощью слоев можно группировать объекты на изображении и выполнять над ними различные действия независимо друг от друга, а также просматривать, как изображение будет выглядеть без этих объектов или модифицировать их в любое время.

Управление доступными слоями производится с помощью компонентов в правой части окна. При выборе определенного слоя он становится активным, и все действия выполняются только на нем.



Применение фильтров

В **Krita** созданное изображение можно улучшить с помощью доступных фильтров изображений, для этого выберите в основном меню программы пункт «**Фильтры**» и примените необходимый фильтр.



Анимация и векторная графика

Krita также предоставляет широкий спектр возможностей для работы с анимацией и векторной графикой.

Основные возможности работы с анимацией:

- создание и редактирование анимированных изображений;
- использование временных слоев для создания плавных переходов между кадрами;
- управление временными интервалами и скоростью анимации;
- импорт и экспорт различных форматов анимаций, включая **GIF**, **AVI**, **MP4**.

Основные возможности работы с векторной графикой:

- создание и редактирование векторных объектов;
- применение различных эффектов и фильтров к векторным элементам;
- использование кривых Безье и редактирование точек управления для создания сложных форм;
- экспорт векторных изображений в форматы **SVG** и **PDF**.

Сохранение результатов

Для сохранения готового изображения или анимации в основном меню программы выберите «**Файл**» – «**Сохранить**». По умолчанию программа сохраняет результат работы в формате ***.kra**.

Программы для сканирования в РЕД ОС

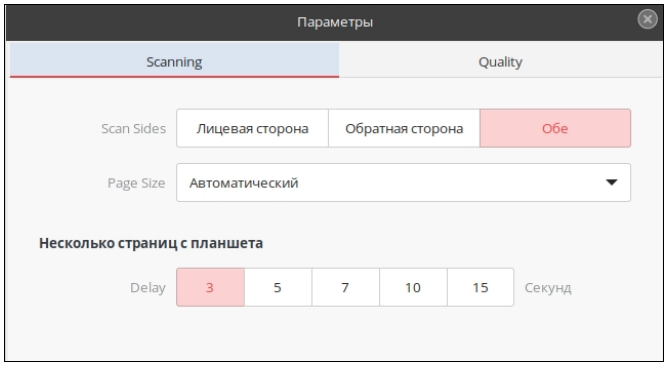
Simple Scan
XSane
GIMP-XSane

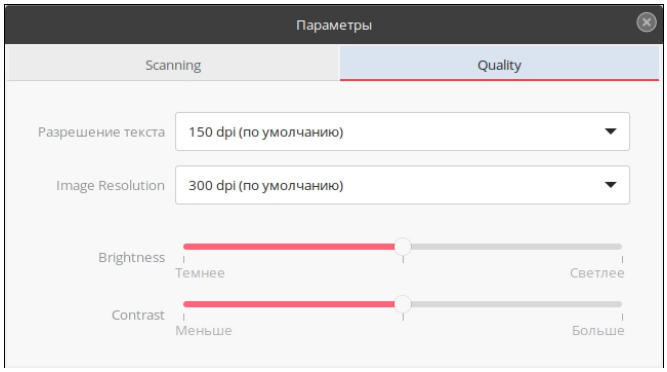
Simple Scan

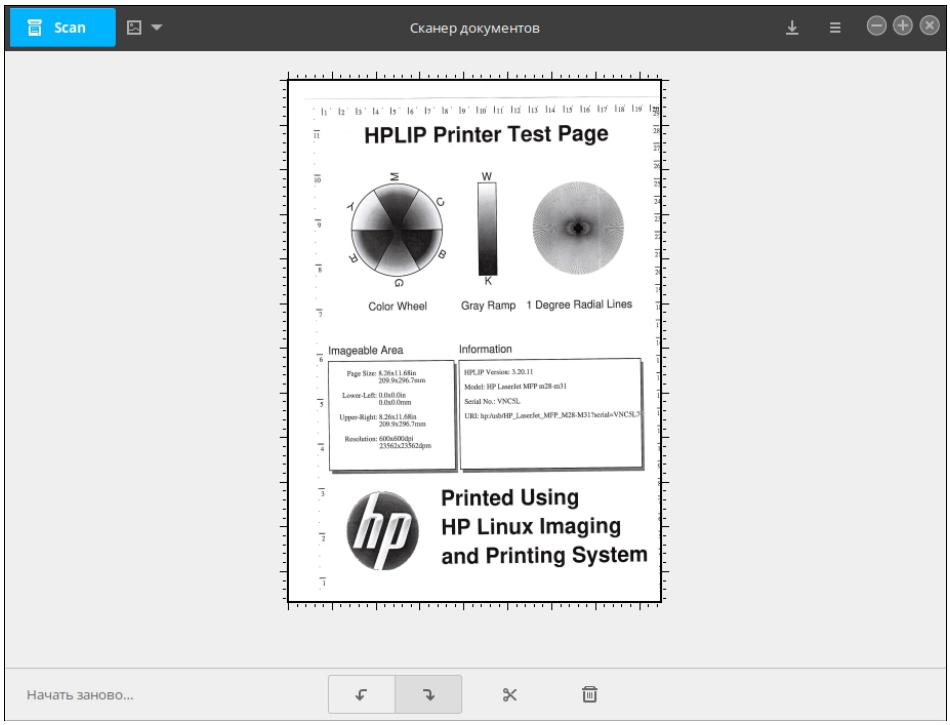
Simple Scan (англ. *simple scan* — простое сканирование) — программа для работы со сканерами; является графическим интерфейсом для прикладной программы **SANE**, которая, в свою очередь, предоставляет стандартизированный доступ к устройствам сканирования растровых изображений.

Simple Scan включает в себя базовый набор функций и настроек для сканирования, такие как установка размера страницы, выбор сканируемой стороны документа, задержка загрузки (в секундах для нескольких страниц), качество отсканированного документа, яркость и контрастность.

Изменение любого из этих параметров доступно в меню настроек окна программы.







Для сканирования документа необходимо нажать в верхнем левом углу кнопку «**Scan**». После успешного сканирования вы можете сохранить изображение в форматах:

- .PDF (многостраничный);
- .JPEG (сжатый);
- .PNG (без потерь качества);
- .WebP (сжатый).

Дополнительно **Simple Scan** позволяет сразу отправлять результат сканирования по почте, распечатать изображения, настроить организацию страниц, настроить параметры сканирования под себя.

Также есть возможность отредактировать полученное изображение с помощью простейшего меню взаимодействия, состоящего из поворотов изображения и его обрезки, или отсканировать документ заново.

XSane

XSane — компьютерная программа для работы с устройствами сканирования изображений. Является графическим интерфейсом для программы *SANE*. Связка пакетов *SANE* и *XSane* поможет сканировать изображение или негатив пленки на вашем сканере. Поддерживается пакетное сканирование в «полуавтоматическом» режиме (минимальное нажатие кнопок).

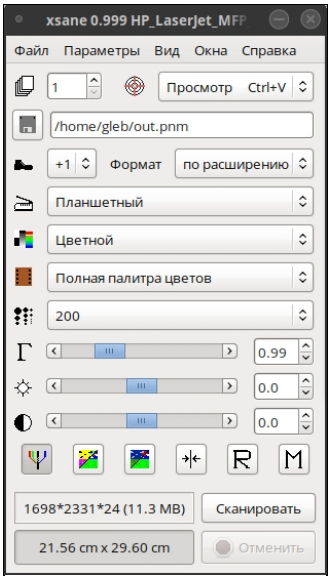
Основные функции программы:

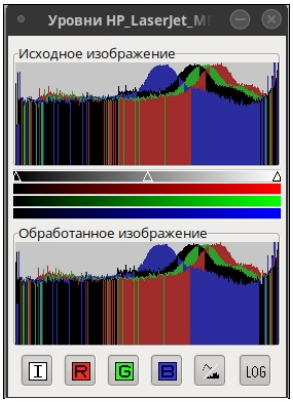
1. Предварительное сканирование (просмотр).
2. Автоматическая корректировка цветов.
3. Ручное и автоматическое выделение необходимой области для сканирования.
4. Раздельная настройка разрешения сканирования по ширине и длине изображения.
5. Печать на принтере отсканированных изображений.
6. Отправка изображения на печать. По умолчанию это производится командой **lpr** протокола *Line Printer Daemon* (**LPD**).
7. Отправка изображения программе оптического распознавания текста (при её наличии в операционной системе).
8. Создание многостраничных документов (пакетное сканирование).
9. Многооконный интерфейс.

Команда для установки *XSane*:

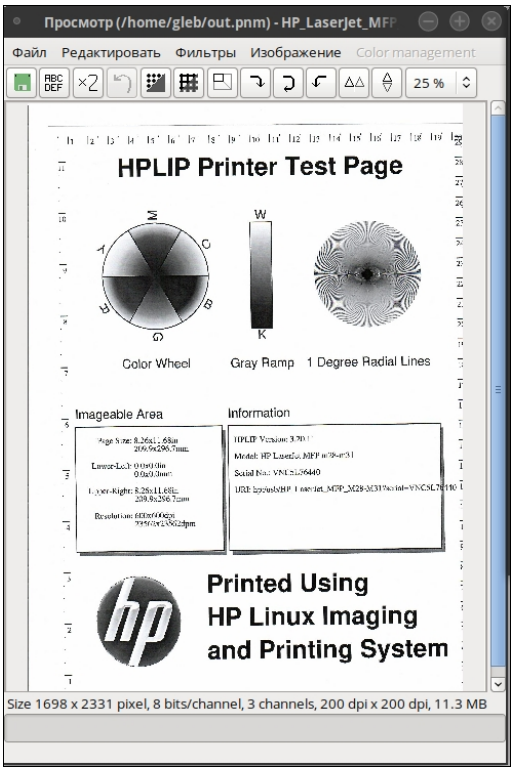
```
# dnf install xsane
```

После установки программа доступна в *Главном меню — Графика*. После запуска программы и выбора необходимого оборудования появляются окна настройки сканирования и контрастности.





После настройки всех доступных параметров и нажатия кнопки «**Сканировать**» будут доступны функции редактирования изображения, а именно: поворот изображения, размытие, масштабирование, отражение по горизонтали и вертикали, обрезка.



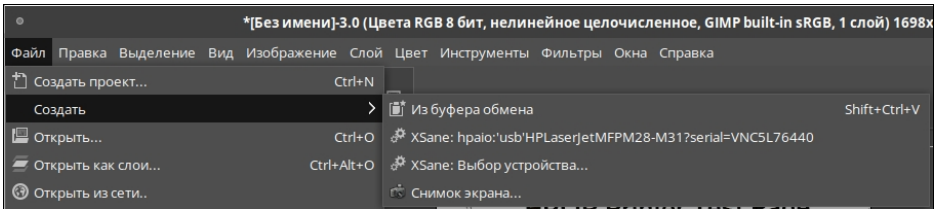
GIMP-XSane

GNU Image Manipulation Program (GIMP) — свободно распространяемый растровый графический редактор, программа для создания и обработки растровой графики с частичной поддержкой работы с векторной графикой.

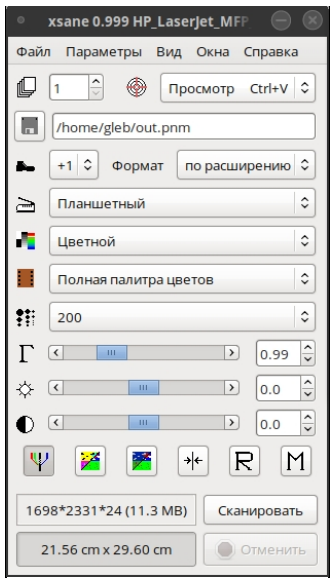
Также *XSane* может работать совместно с *GIMP*, как плагин для последнего. Для установки плагина выполните команду:

```
# dnf install xsane-gimp
```

Чтобы начать сканирование, в меню нажмите «**Файл**» - «**Создать**» - «**XSane: выбор устройства...**».

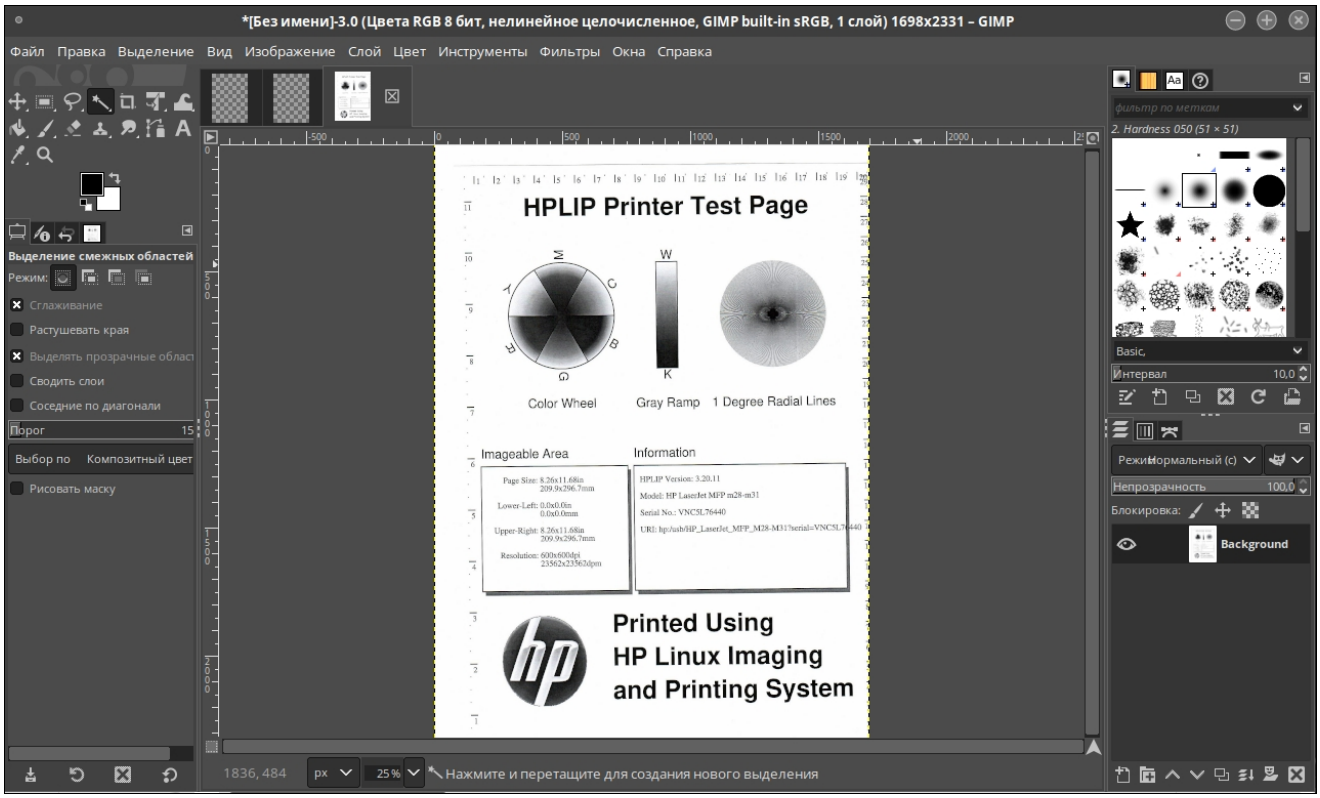


Появится окно настройки параметров сканирования изображения *XSane*.



После индивидуальной настройки всех требуемых параметров нажмите кнопку «**Сканировать**», по завершении сканирования

полученное изображение при необходимости можно отредактировать.



gscan2pdf - программа для сканирования и обработки документов

Возможности программы
Установка gscan2pdf
Параметры сканирования документа
Работа с отксанированными объектами
Распознавание текстов на сканах
Общие параметры настроек gscan2pdf

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** gscan2pdf-2.8.0-1

Gscan2pdf – программа для создания файлов в формате **PDF** или **DjVu** из отсканированных документов, которая позволяет выполнять простые операции, такие как обрезка, поворот и удаление страниц. *Gscan2pdf* может сканировать несколько страниц одновременно.

Возможности программы

Основные возможности программы:

- Сканирование и сохранение документов в форматы: **pdf, gif, jpeg, png, pnm, ps, tiff, hOCR**;
- Сохранение отдельно выделенных страниц;
- Импорт файлов следующих форматов: **jpg, png, pnm, ppm, pbm, gif, tif, tiff, pdf, djvu, ps, gs2p**
- Инструменты для минимальной обработки изображений при сканировании: повороты, установка порога, очистка документа, негатив и кадрирование;
- Встроенная функция распознавания отсканированного документа (OCR - англ. optical character recognition). Для использования **OCR** необходимо настроить **tesseract** или **Cuneiform**.

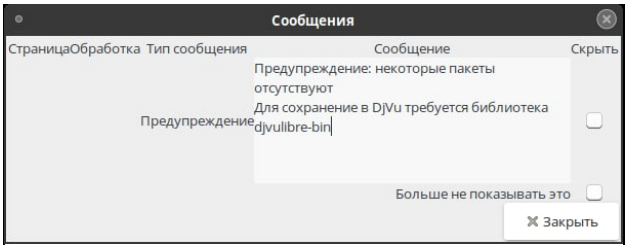
Установка gscan2pdf

Установка *gscan2pdf* в РЕД ОС 7.3 выполняется командой:

```
dnf install gscan2pdf
```

После установки программа доступна из «**Главного меню**» - «**Графика**» - «**gscan2pdf**».

При первом запуске возможно появление предупреждающего сообщения вида:



Для решения данной проблемы необходимо установить дополнительную библиотеку командой:

```
dnf install djvulibre
```

Параметры сканирования документа

Для начала работы нажмите на значок сканирования в главном окне программы или сочетание клавиш «**CTRL+G**». При этом откроется диалоговое окно предварительной установки параметров сканирования, а также выбор модели сканера.

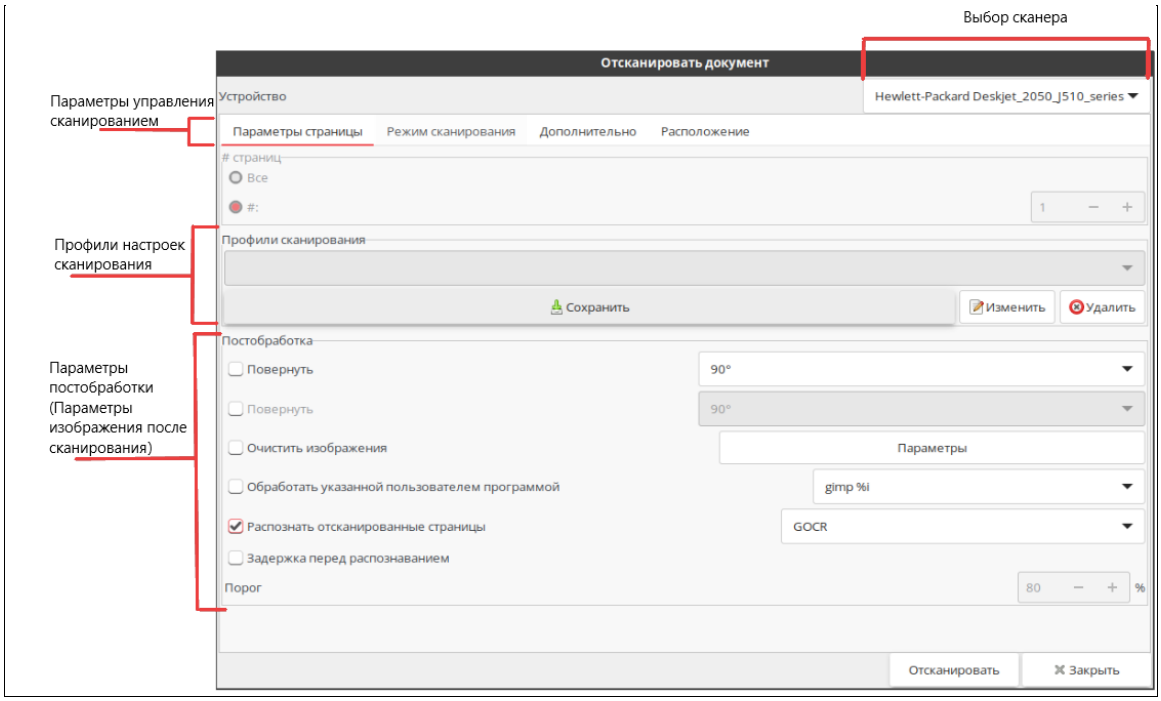


Рисунок 1 – Параметры сканирования

Вкладка «Параметры страницы»

На данной вкладке пользователь может настроить:

- выбор количества страниц;
- выбор профиля сохраненных настроек для сканирования;
- параметры постобработки:
    - поворот изображения;
    - очистка изображения;
    - обработка изображения отдельными программами;
    - включение/выключение автоматической функции распознавания страниц.

Вкладка «Режим сканирования»

В режиме сканирования доступен выбор цвета сканируемого объекта – черно-белый, цветной, штриховой. Также имеется возможность изменить разрешение сканирования, которое определяет качество сканируемого объекта в пкс/дюйм. (от 75 до 1200 пкс/дюйм).

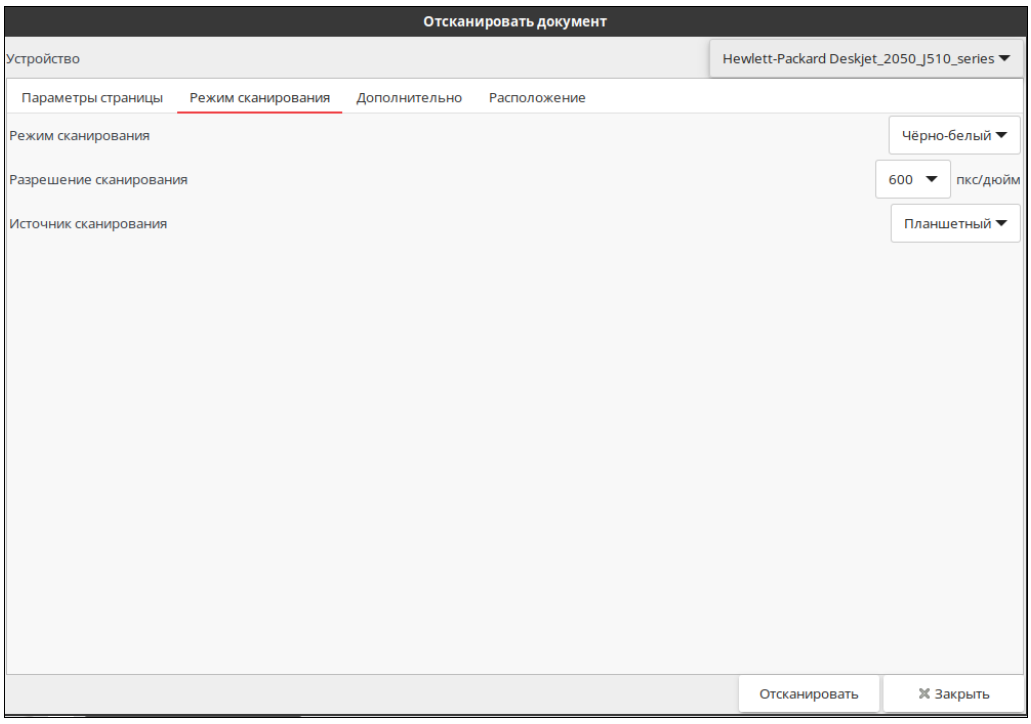


Рисунок 2 – Режим сканирования

Вкладка «Дополнительно»

На вкладке «**Дополнительно**» настраивается яркость, контрастность и метод сжатия изображения.

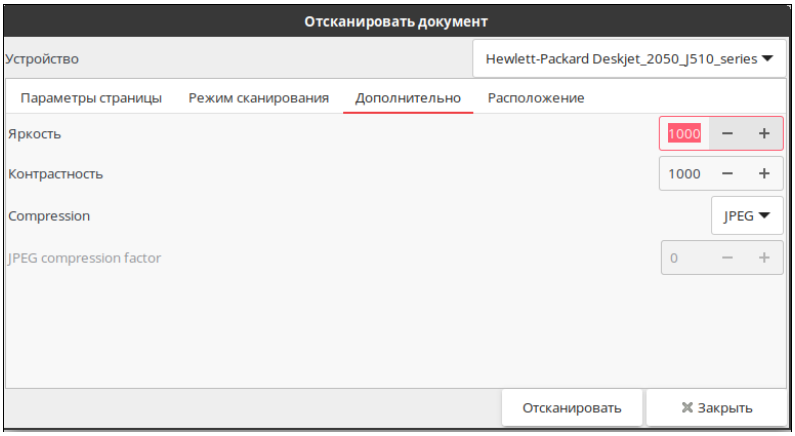


Рисунок 3 – Дополнительные параметры

Вкладка «Расположение»

На вкладке «**Расположение**» выбирается формат бумаги.

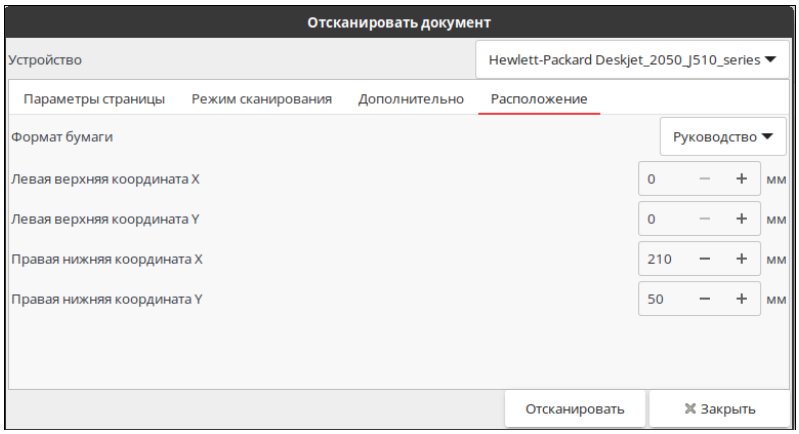


Рисунок 4 – Параметры расположения

Работа с отсканированными объектами

Отсканированное изображение при необходимости можно отредактировать. Из элементов редактирования здесь имеется: поворот изображения, масштабирование, порог (отвечает за насыщенность изображения), яркость/контраст, негатив, не резкая маска, кадрирование.

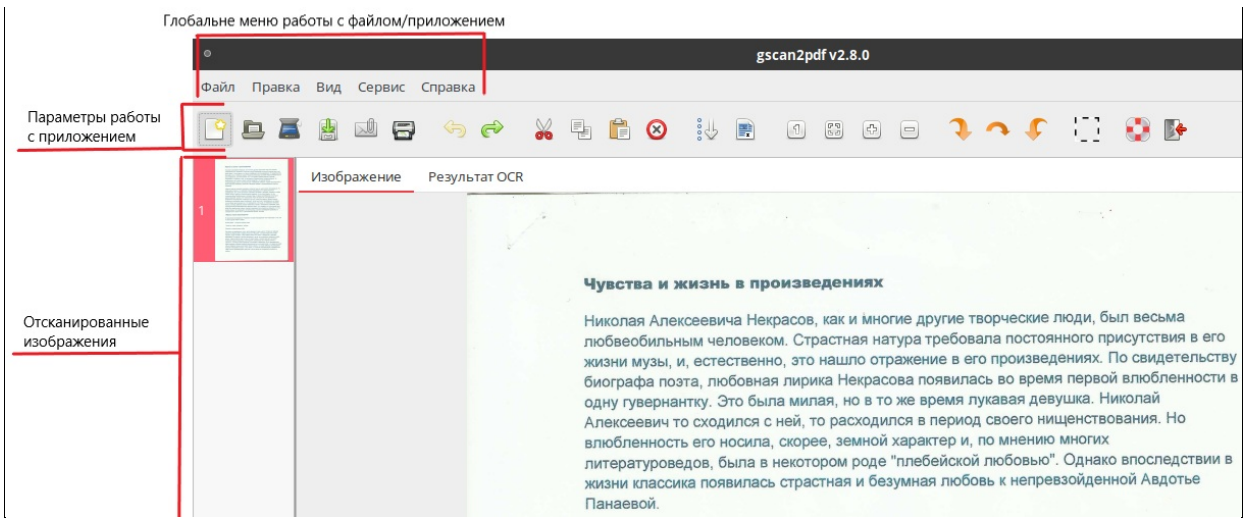


Рисунок 5 – Окно работы с отсканированными изображениями

При сохранении отсканированного документа открывается диалоговое окно с настройками, в котором можно настроить следующие параметры для сохраняемого документа:

- изменение диапазона страниц;
- выбор формата, в котором сохраняется изображение;
- установка даты и времени;
- описание и указание автора;
- снижение разрешения;
- сжатие изображения;
- выбор шрифта для не-ASCII текста;
- перехват после сохранения - это указанные пользователем дополнительные команды (программы) обработки изображений.

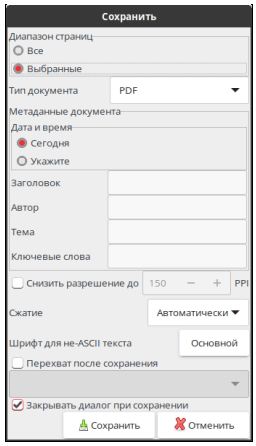


Рисунок 6 – Сохранение изображения

Распознавание текстов на сканах

Сперва необходимо установить доступные движки для распознавания текстов. Команда для установки **cuneiform**:

```
dnf install cuneiform
```

Стандартная установка у **tesseract** в отличие от с**uneiform** не содержит языковой пакет для русского языка, поэтому его нужно установить дополнительно. Для установки **tesseract** используется следующая команда:

```
dnf install tesseract tesseract-langpack-rus
```

После этого можно приступать непосредственно к распознаванию текста, для этого необходимо:

1. Импортировать или отсканировать необходимые файлы.
2. После завершения загрузки файлов перейти в «**Сервис**» - «**Распознать текст**».

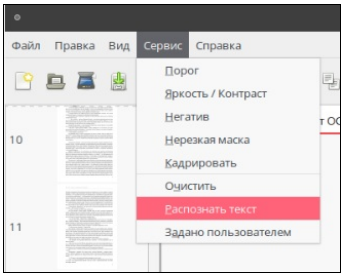


Рисунок 7 – Расположение вкладки распознавания текста

3. Откроется окно OCR, в котором доступны следующие настройки:
    - Диапазон страниц;
    - Движок OCR;
    - Языки распознавания;
    - Задержка перед распознаванием;
    - Порог.

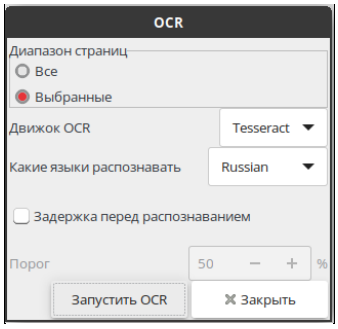


Рисунок 8 - Окно настроек OCR

4. После указания настроек можно запускать распознавание. Если документ имеет большое количество страниц, процесс может занять некоторое время.
5. После завершения процесса для каждой страницы появится ее распознанная копия в окне «**Результат OCR**». При необходимости можно редактировать результаты распознавания, для этого следует воспользоваться нижней панелью. После завершения можно сохранить результат в нужном формате.

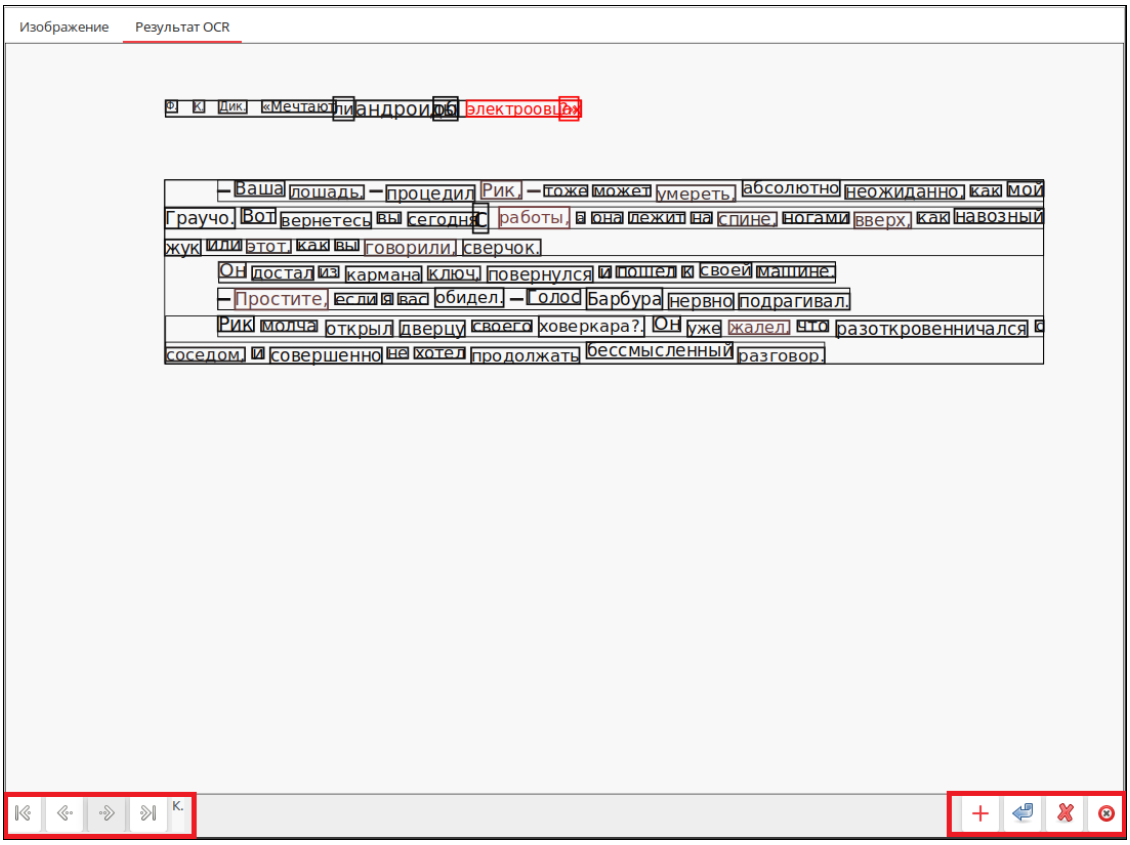


Рисунок 9 - Расположение кнопок панели редактирования

Общие параметры настроек gscan2pdf

В меню «**Правка**» – «**Параметры**» можно настроить общие параметры сканирования, например:

- выбор графического интерфейса - назначается интерфейс для доступа к сканеру;
- черный список устройств;
- возможность пакетного сканирования с планшетного сканера («**Пакетное сканирование**» — способ одновременной оцифровки нескольких оригиналов, установленных или закрепленных в сканере).

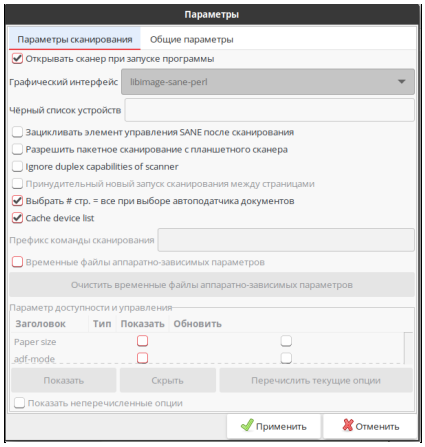


Рисунок 10 – Параметры сканирования

На вкладке «**Общие параметры**» доступны следующие настройки:

- изменение формата именования файлов по умолчанию;
- возможность указать временный каталог;
- включить/выключить просмотр файла после сохранения и др.

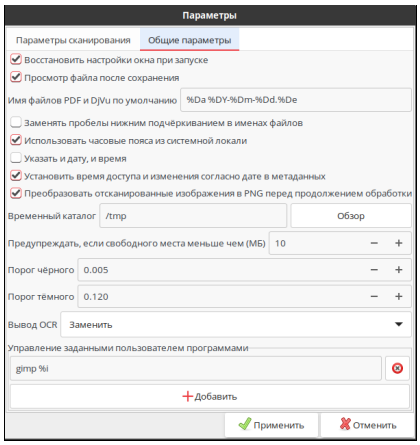


Рисунок 11 – Общие параметры

NAPS2 – программа для сканирования документов и изображений

Возможности
Установка
Запуск
О программе
Пакетное сканирование
Настройка
Сканирование
Распознавание текста с помощью OCR
Импорт
Поворот, обрезка, изменение изображений
Редактирование PDF-файла
Удаление документа

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: naps2-7.1.2

NAPS2 (Not Another PDF Scanner 2) — это программа, которая позволяет сканировать документы и изображения, сохраняя их в форматы PDF, JPEG, PNG или TIFF.

NAPS2 поддерживает различные типы сканеров и обладает интуитивно понятным интерфейсом.

Возможности

К основным возможностям программы NAPS2 можно отнести:

1. Сканирование документов — позволяет подключить сканер и сканировать документы с различными настройками.

2. Обработка изображений — после сканирования NAPS2 предоставляет инструменты для обработки изображений.

3. Сохранение в различных форматах — позволяет сохранять отсканированные документы в формате PDF или в виде отдельных изображений (например, JPEG или PNG).

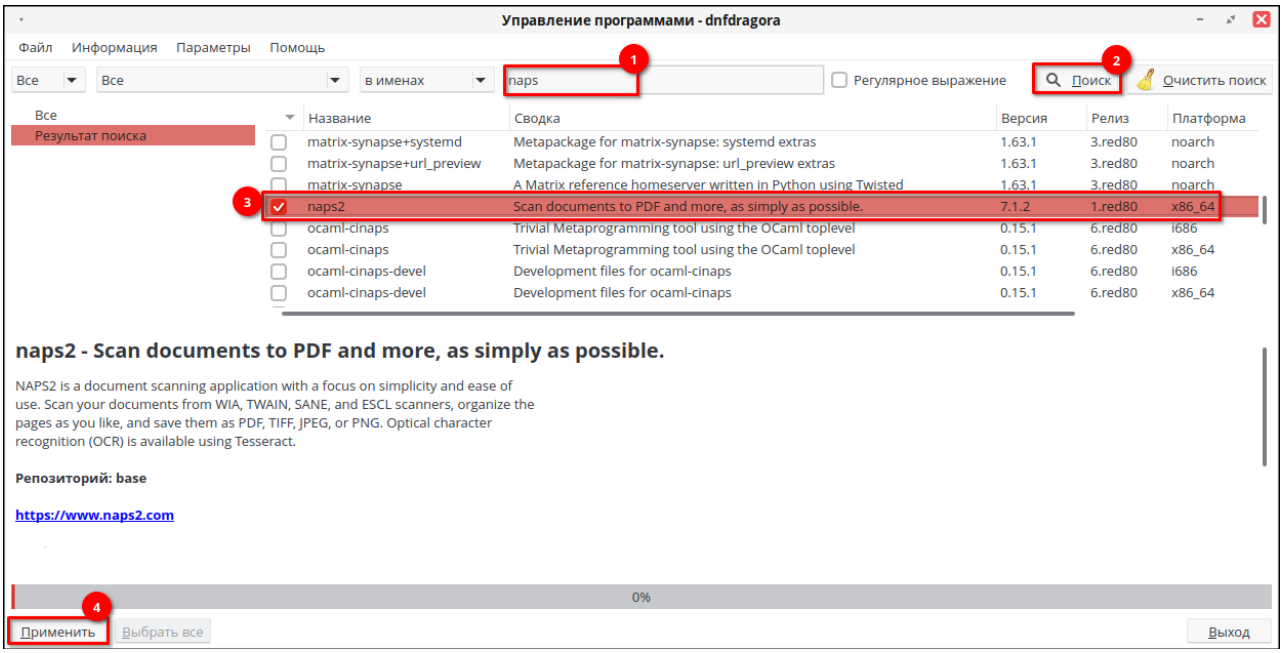
4. Функциональность — программа предлагает различные настройки для сканирования и сохранения, включая выбор профиля сканирования, настройку качества изображения, выбор расположения сохраняемых файлов и другие.

5. Пакетная обработка — поддерживает пакетную обработку, что означает возможность сканирования и обработки нескольких документов одновременно.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**naps**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



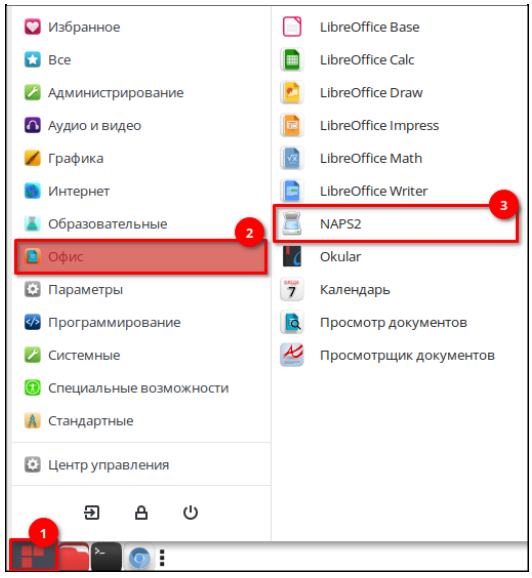
Для установки NAPS2 через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install naps2
```

Запуск

Запустить программу можно либо через меню приложений, либо через терминал.

Для запуска программы сканирования документов через меню приложений перейдите в «**Главное меню**» — «**Офис**» — «**NAPS2**».

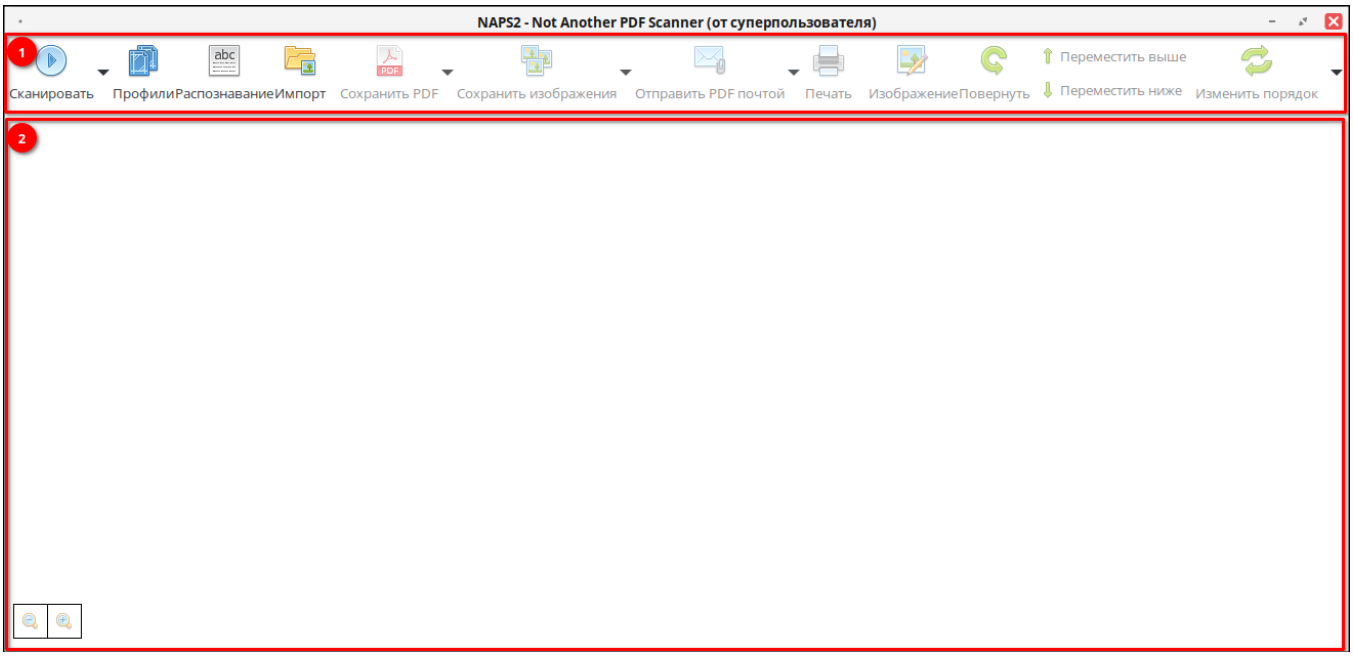


Для запуска NAPS2 через терминал выполните команду:

```
naps2
```

О программе

Главное окно программы выглядит следующим образом:



В верхней части окна расположена панель инструментов (1), где доступны основные инструменты для работы со сканируемым файлом. Основную часть окна занимает рабочая область (2), на которой располагаются открытые документы.

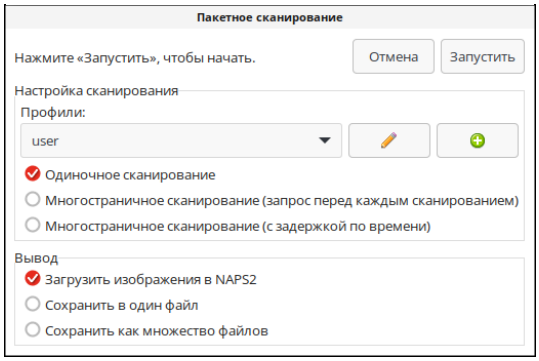
Инструменты:

- Сканировать (Пользователь, Профиль, Пакетное сканирование);
- Профили;
- Распознавание;
- Импорт;
- Сохранить PDF (Все, Выбранные, Настройки PDF);
- Сохранить изображения (Все, Выбранные, Настройки изображения);
- Отправить PDF почтой (Все, Выбранные, Параметры эл.почты, Настройки PDF);
- Печать;
- Изображение;
- Повернуть;
- Переместить выше;
- Переместить ниже;
- Изменить порядок;
- Удалить;
- Очистить;
- Язык;
- О программе.

С помощью инструментов можно перетаскивать страницы в любом удобном пользователю порядке, чередовать страницы для двустороннего сканирования вручную, поворачивать страницы вручную или автоматически под нужным углом, редактировать изображения для обрезки или изменения яркости и контрастности.

Пакетное сканирование

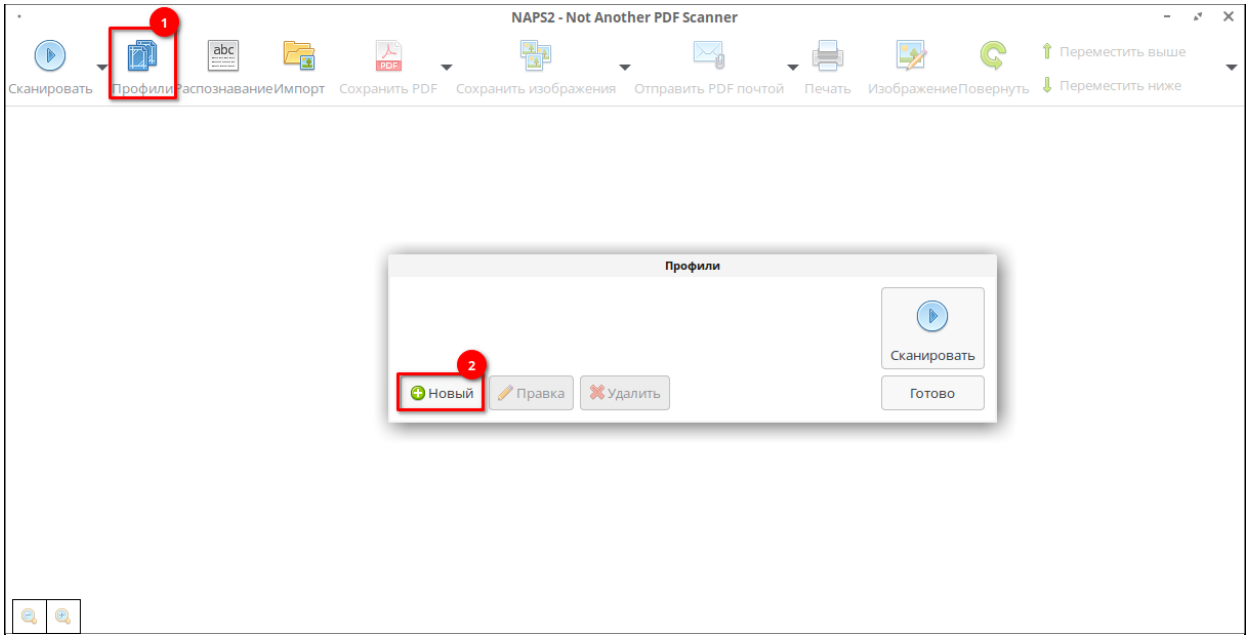
Для использования расширенных функций пакетного сканирования с целью автоматизации задач сканирования перейдите в инструмент «**Сканировать**» — «**Пакетное сканирование**». Можно объединять несколько отсканированных документов вместе, автоматически нумеровать файлы и ставить временные метки.



Настройка

Перед настройкой программы NAPS2 подключите к компьютеру сканер и установите его драйверы.

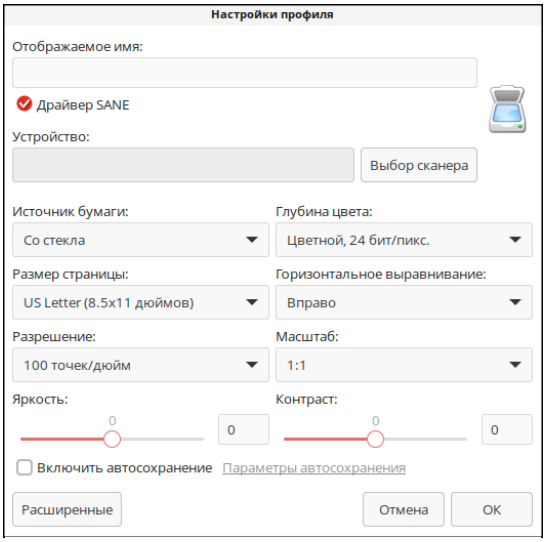
Для настройки нового профиля в главном меню выберите пункт «**Профиль**» (1), а затем в появившемся окне нажмите «**Новый**» (2).



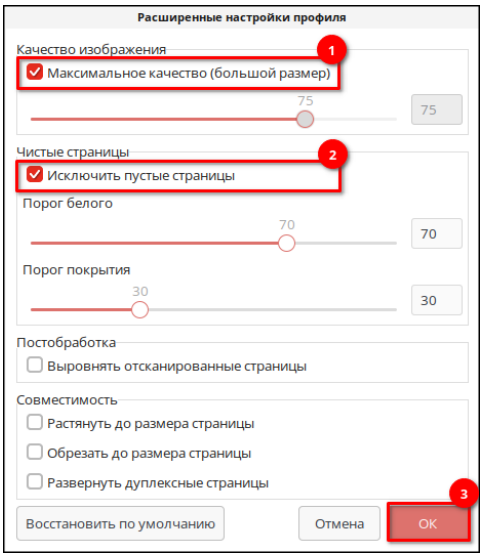
В окне «**Настройка профиля**» введите имя профиля и выберите драйвер. Для подключения к USB-сканерам и сетевым сканерам используйте драйверы SANE и ESCL. Выберите сканер из установленных на компьютере и определите настройки сканера.

Выберите источник бумаги, определите глубину цвета, размер страницы, горизонтальное выравнивание, разрешение и масштаб страницы. Также можно задать параметры автосохранения, установив флаг для соответствующего параметра.

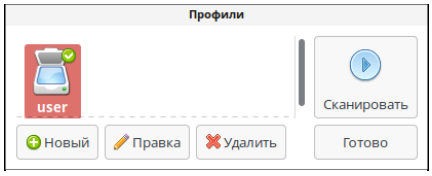
Дополнительно можно задать расширенные настройки профиля.



В окне «Расширенные настройки профиля» в пункте «**Качество изображения**» установите флаг «**Максимальное качество (большой размер)**» (1) и «**Исключить пустые страницы**» (2), закройте окно, нажав кнопку «**OK**» (3).

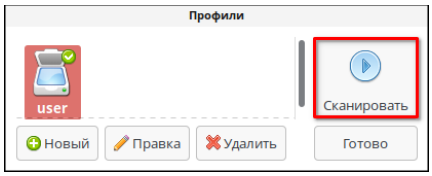


После нажатия кнопки «**OK**» в окне «**Профили**» появится созданный профиль.

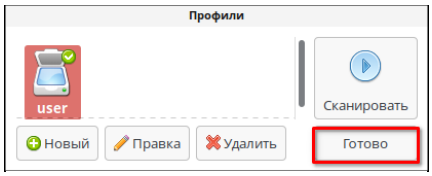


Сканирование

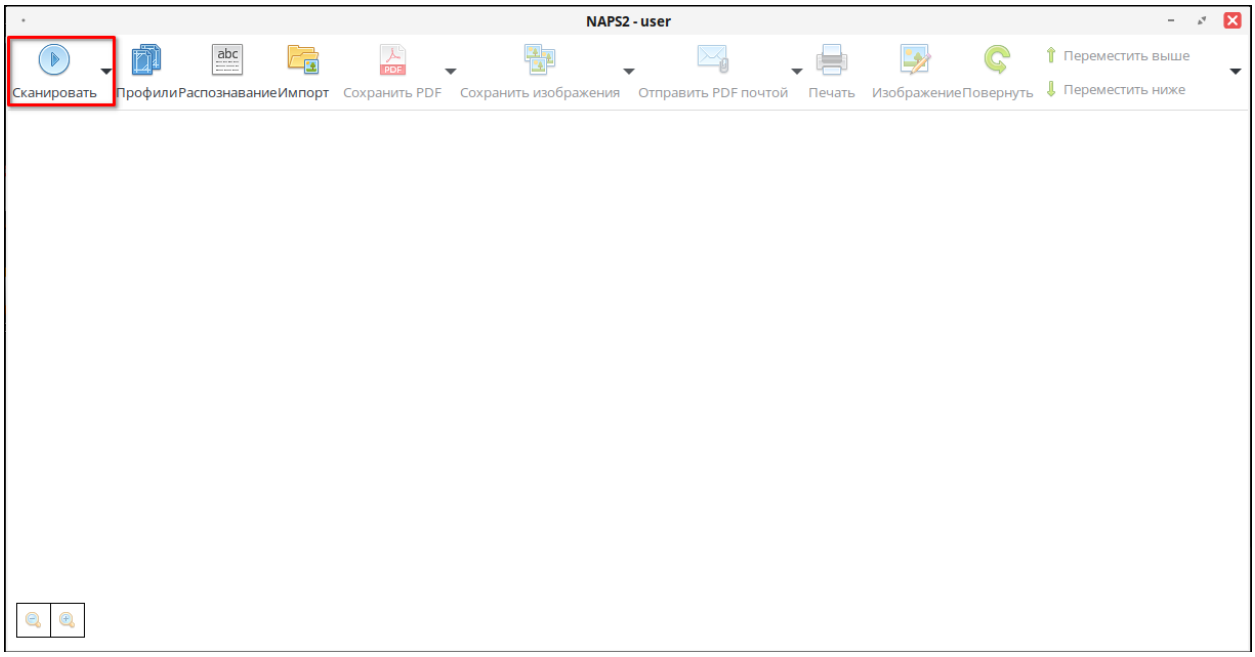
Для сканирования поместите в сканер документ, в окне «**Профили**» выберите нужный профиль и нажмите кнопку «**Сканировать**».



Для закрытия окна нажмите кнопку «**Готово**»:

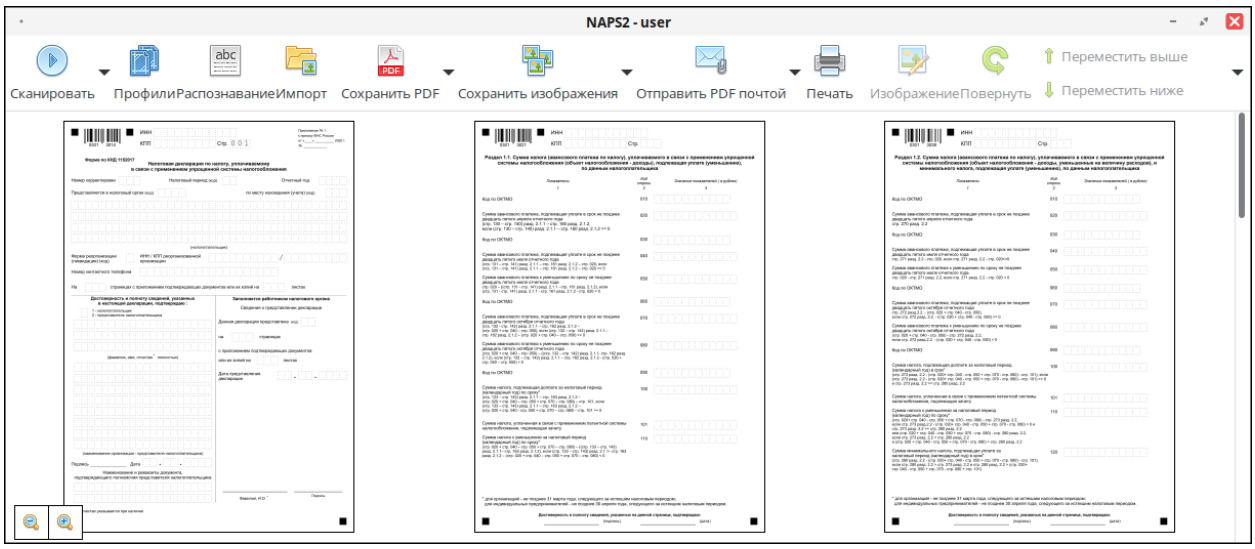


Также можно нажать на кнопку «**Сканировать**» на панели инструментов.

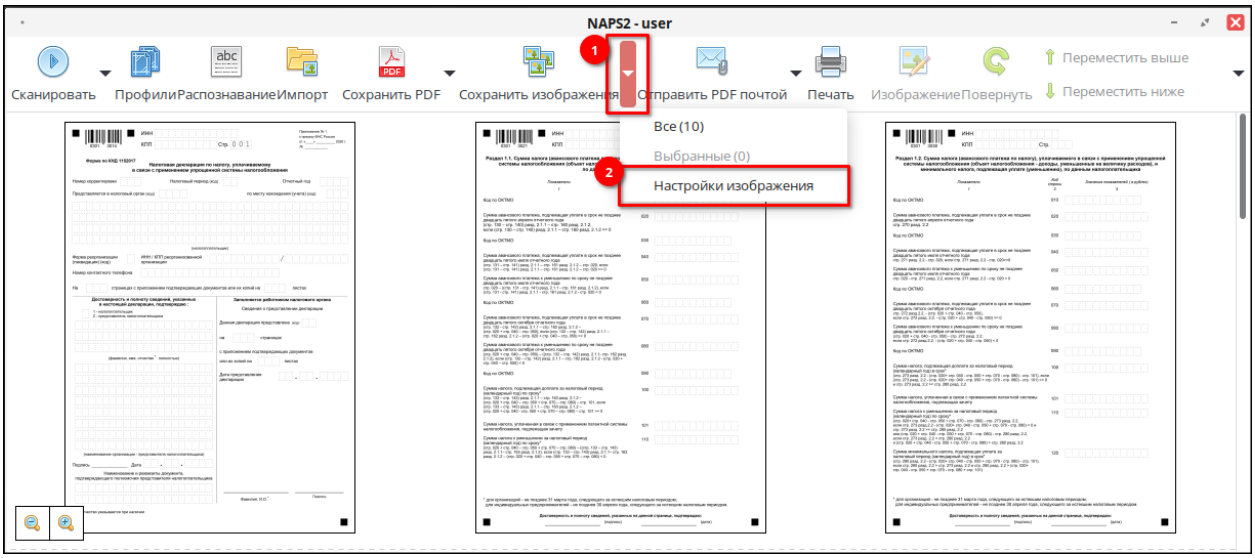


После открытия окна настроек произведите нужные настройки и нажмите «**Сканировать**».

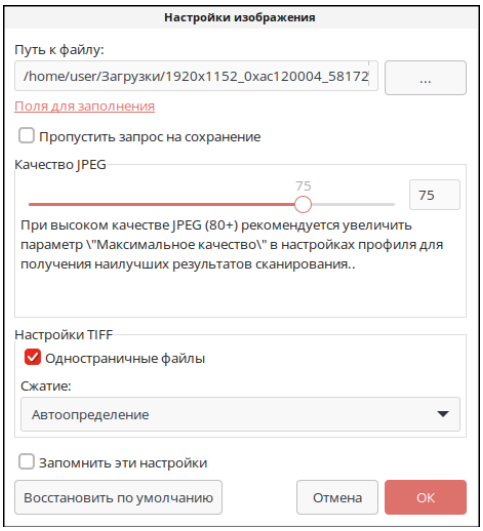
После выполненных действий в главном окне программы отобразится отсканированный документ.



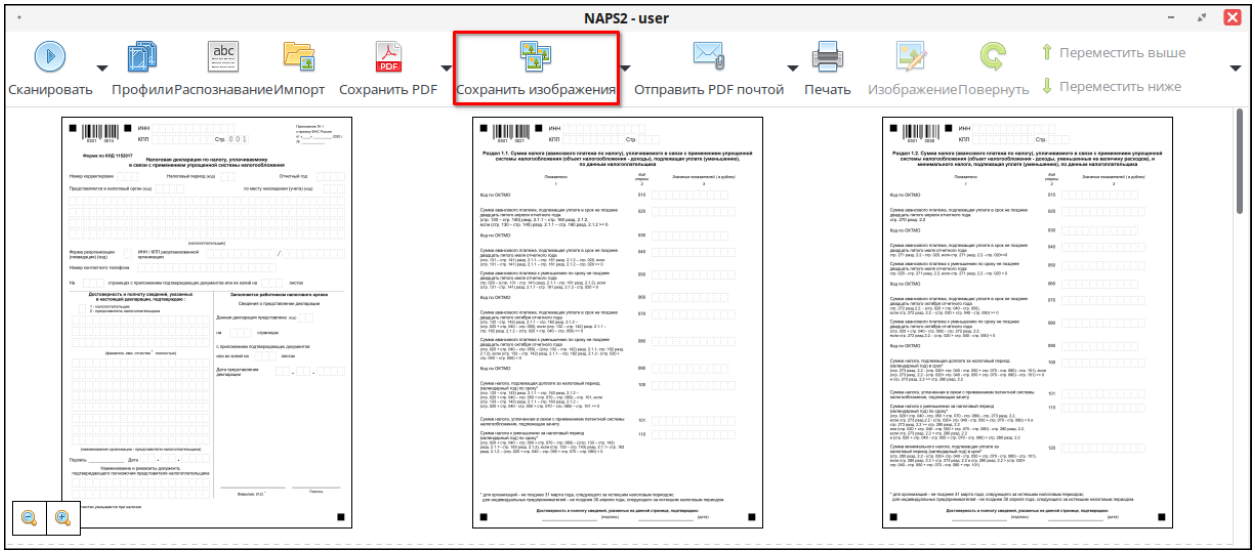
Для определения настроек сохранения нажмите на стрелку рядом с инструментом «**Сохранить изображение**» и выберите в выпадающем меню пункт «**Настройки изображения**».



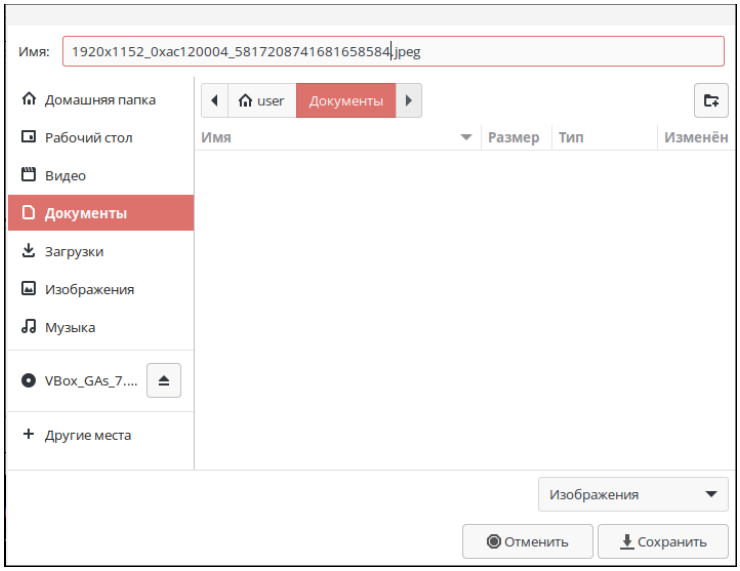
Установите необходимые настройки и нажмите кнопку «**OK**».



Для сохранения изображения нажмите «**Сохранить изображение**».



Выберите имя файла и каталог для сохранения и нажмите «**Сохранить**».

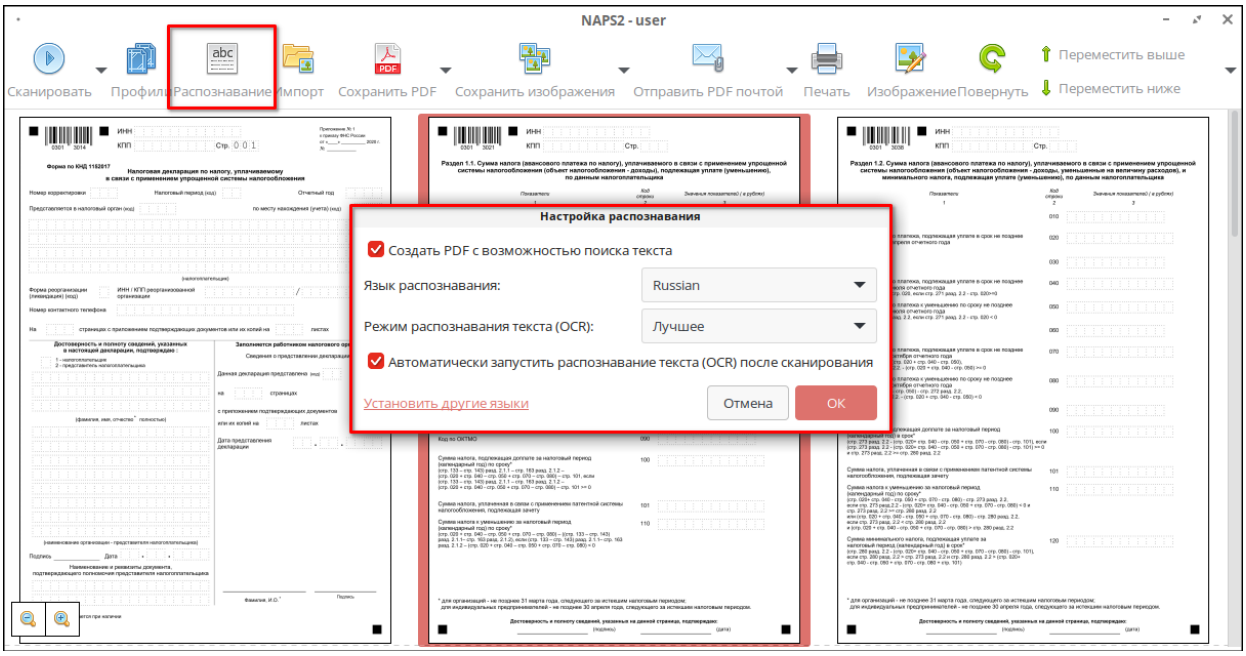


Отсканированный документ будет успешно сохранен.

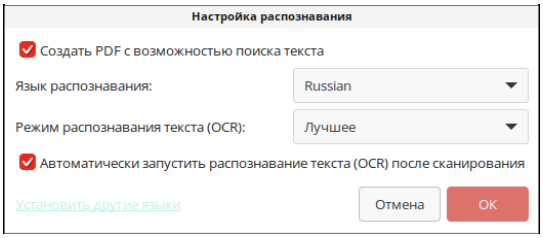
В NAPS2 также доступна возможность отправки отсканированных документов по почте или отправки на печать.

Распознавание текста с помощью OCR

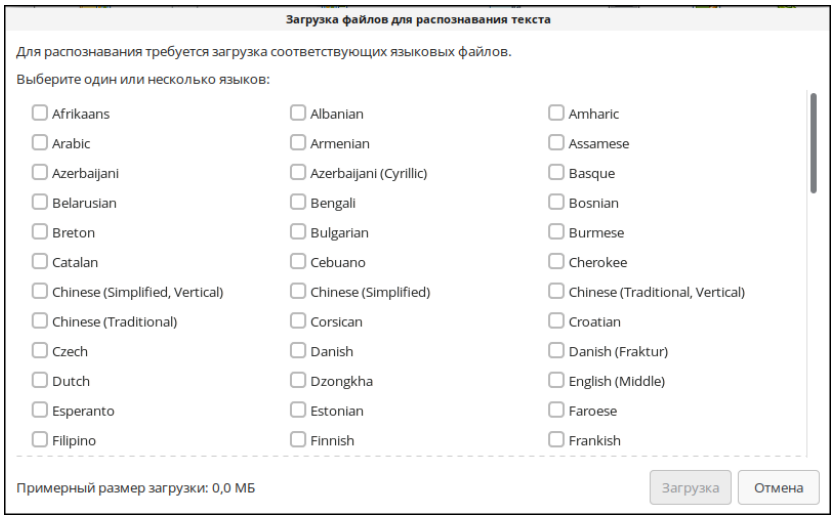
Для выполнения поиска по тексту, включенному в PDF-файлы, с помощью оптического распознавания символов (OCR) на любом из более чем 100 языков выберите инструмент «**Распознавание**».



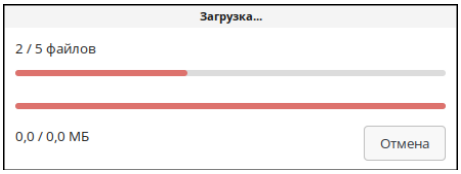
В появившемся диалоговом окне «**Настройка распознавания**» выберите язык и режим распознавания текста, поставьте флаги напротив «**Создать PDF с возможностью поиска текста**» и «**Автоматически запустить распознавание текста (OCR) после сканирования**».



При нажатии на функцию «**Установить другие языки**» можно загрузить дополнительные языковые пакеты.



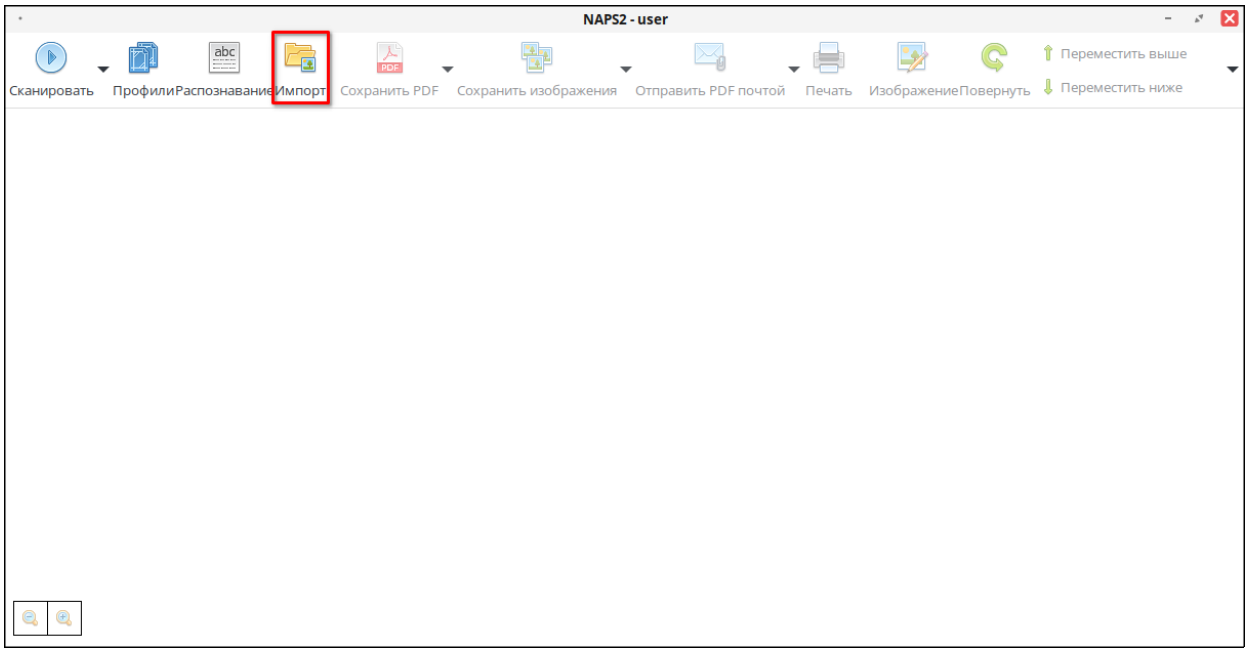
Для загрузки файлов для распознавания текста отметьте флагом нужные языки и нажмите «**Загрузка**». Дождитесь окончания загрузки.



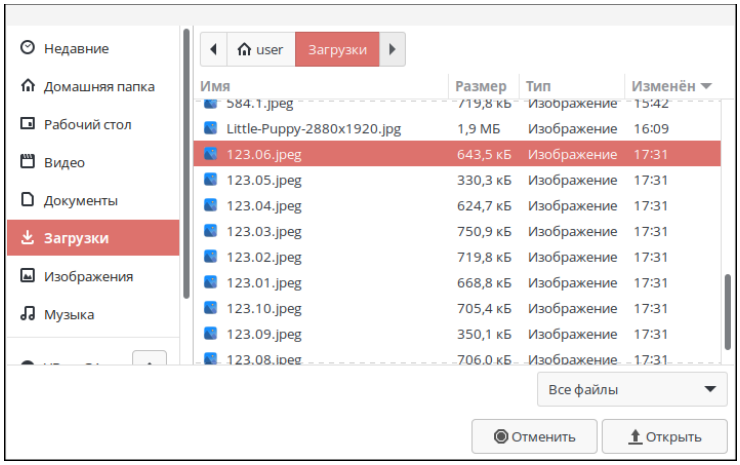
Импорт

NAPS2 может объединять несколько документов в один. Для этого необходимо нажать «**Импорт**» и выбрать нужные документы. Далее выбрать «**Сохранить PDF**» и выбрать пункт «**Все**». Программа сохранит все открытые документы в один. Таким же образом можно

сохранить все страницы документов в форматы *JPEG*, *GIF*, *PNG*.

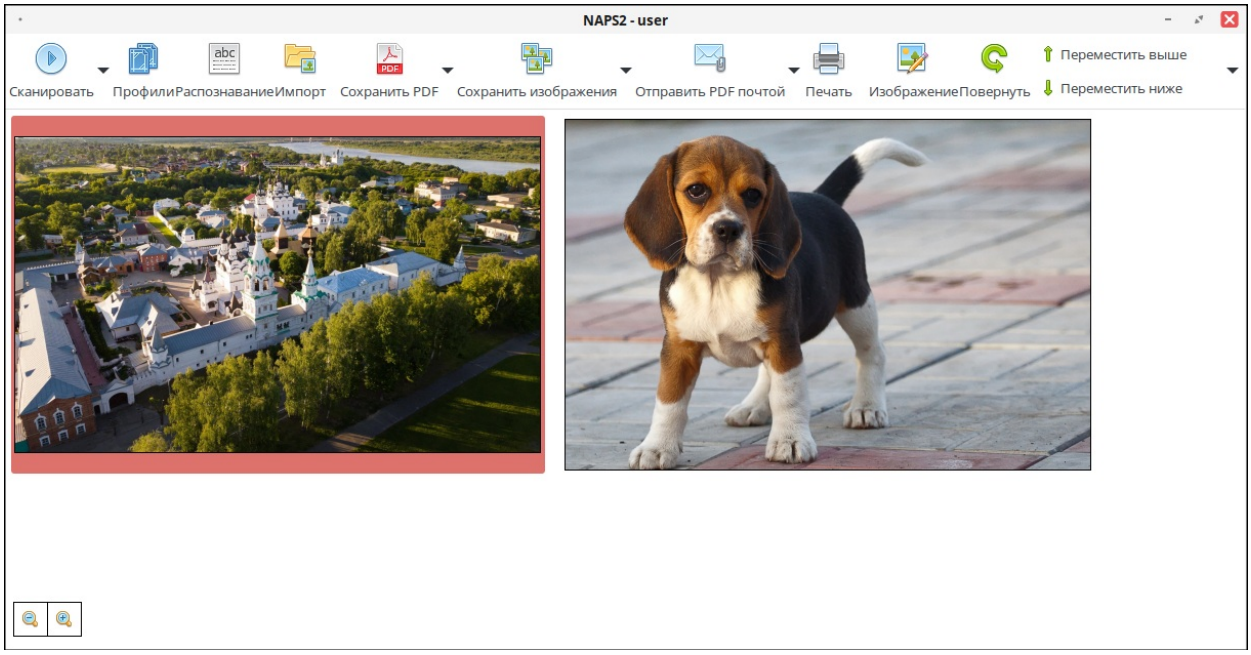


В диалоговом окне выбора файла выберите необходимые документы для импорта на рабочую область и нажмите «**Открыть**».

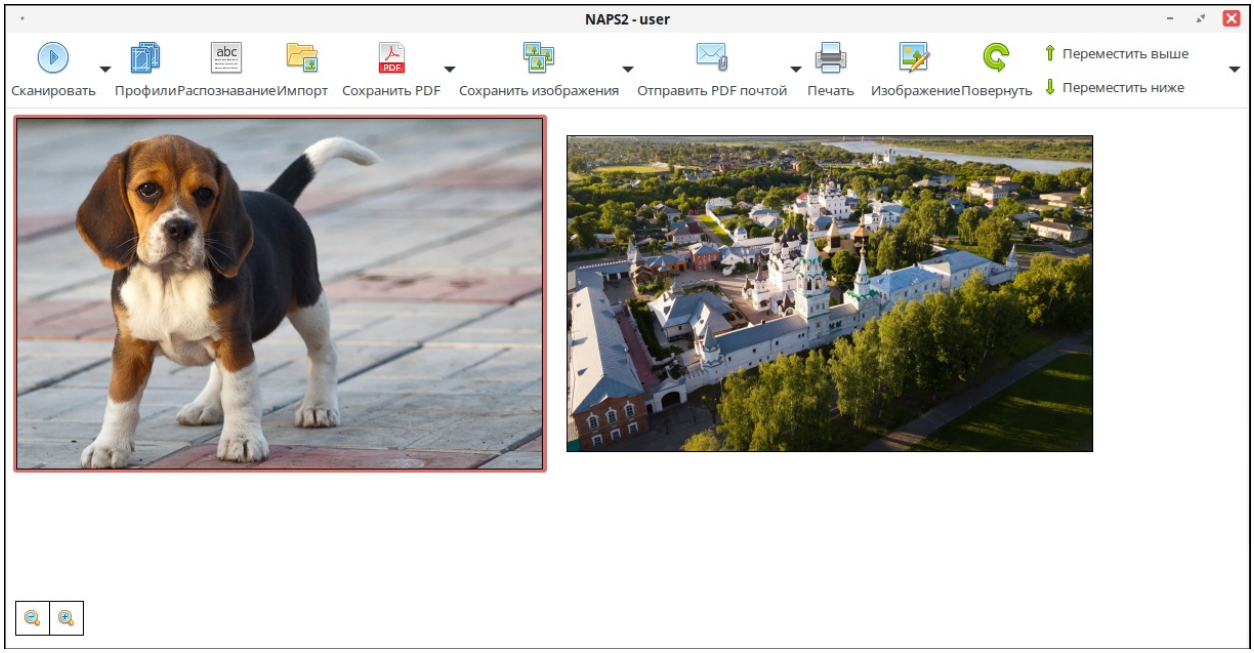


Поворот, обрезка, изменение изображений

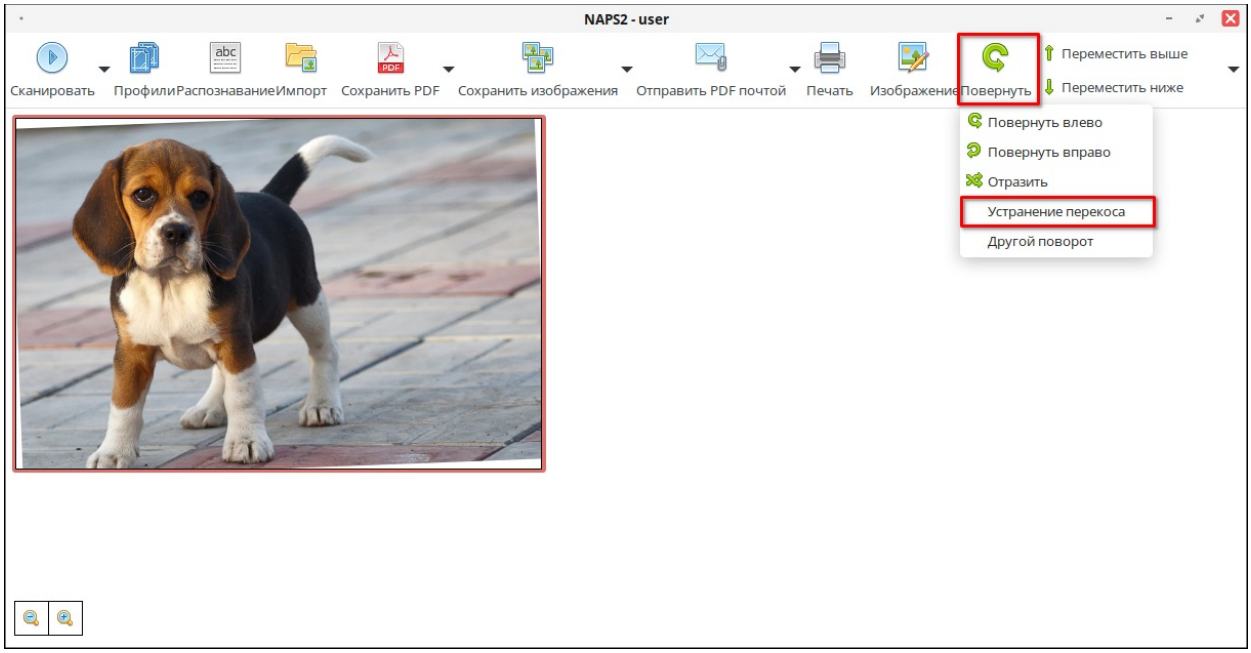
Страницы документов и изображения можно перетаскивать в любом удобном порядке.



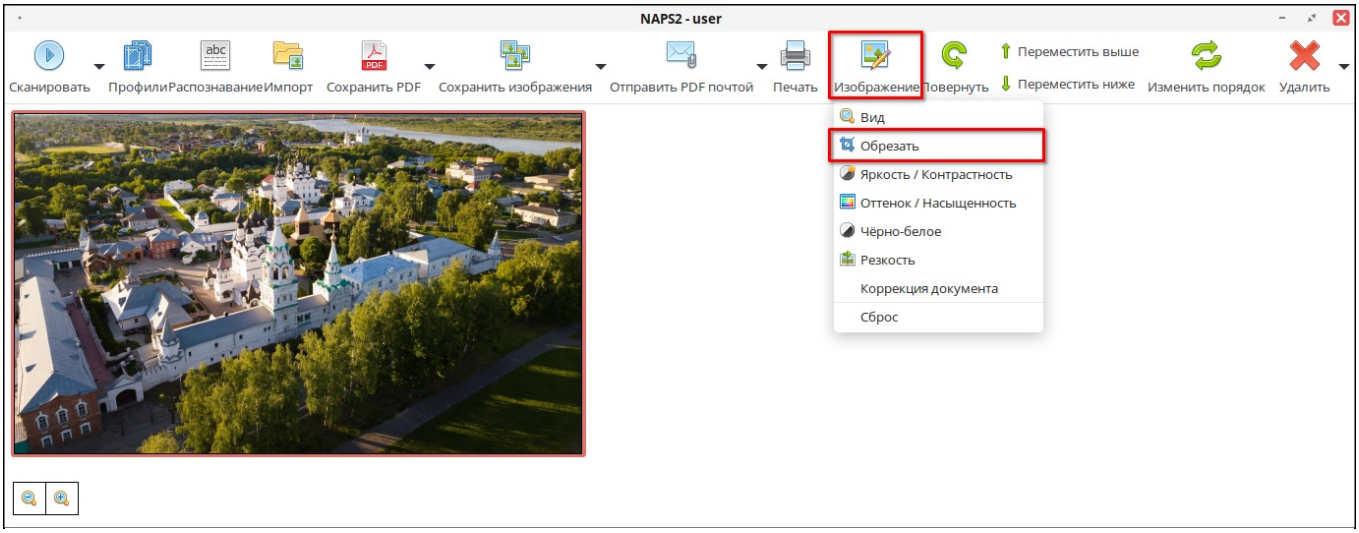
Для этого щелкните по изображению ЛКМ и, удерживая ее, перенесите изображение в нужное место.



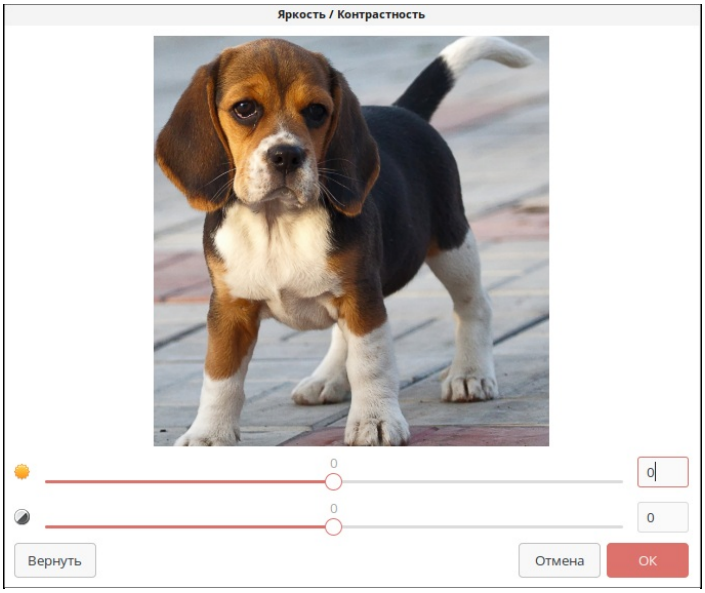
В программе предусмотрены функции поворота изображения вручную или автоматически под прямым углом. Для устранения перекоса на изображении выберите инструмент «**Повернуть**» — «**Устранение перекоса**».



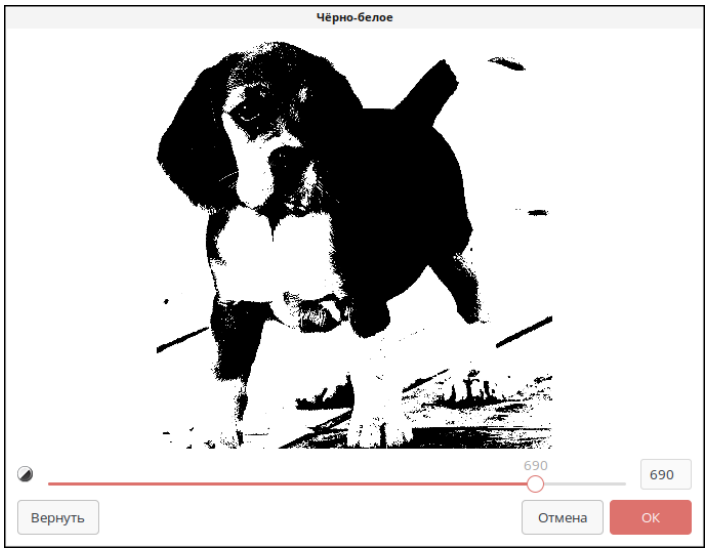
Используйте инструменты редактирования изображений для обрезки. Нажмите «**Изображение**» — «**Обрезать**» и выделите нужную область. После этого нажмите «**OK**».



Для применения функции изменения яркости и контрастности выберите «**Изображение**» — «**Яркость/контрастность**». Далее установите нужные настройки.



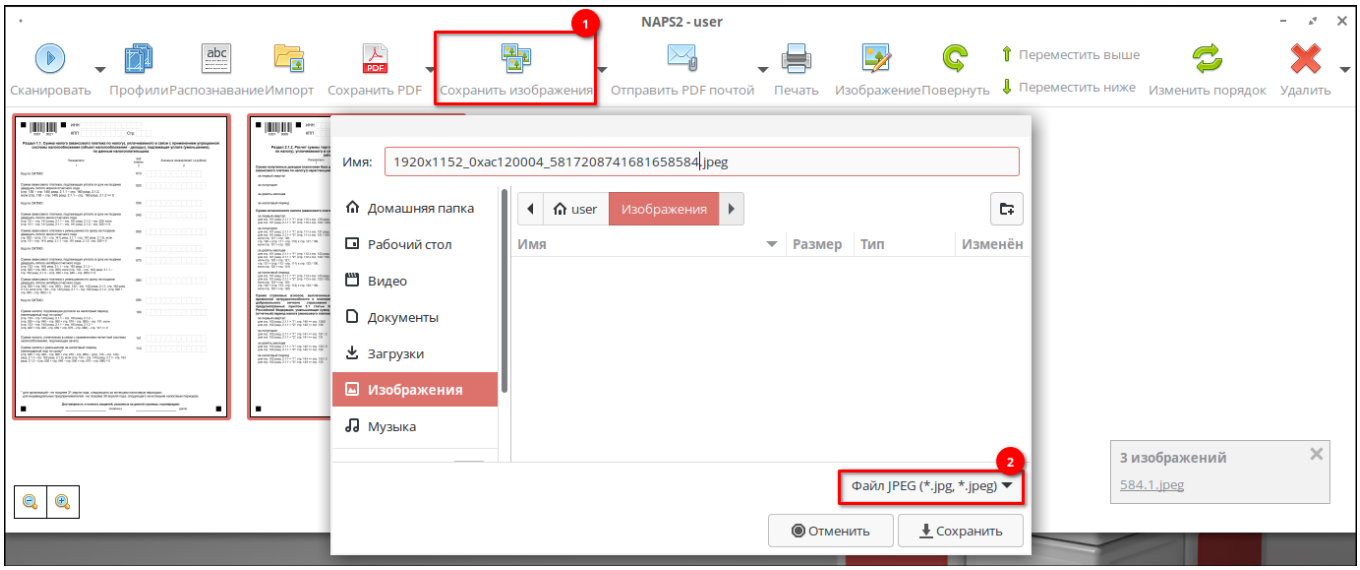
Для перевода изображения в черно-белый формат выберите «**Изображение**» — «**Чёрно-белое**».



Редактирование PDF-файла

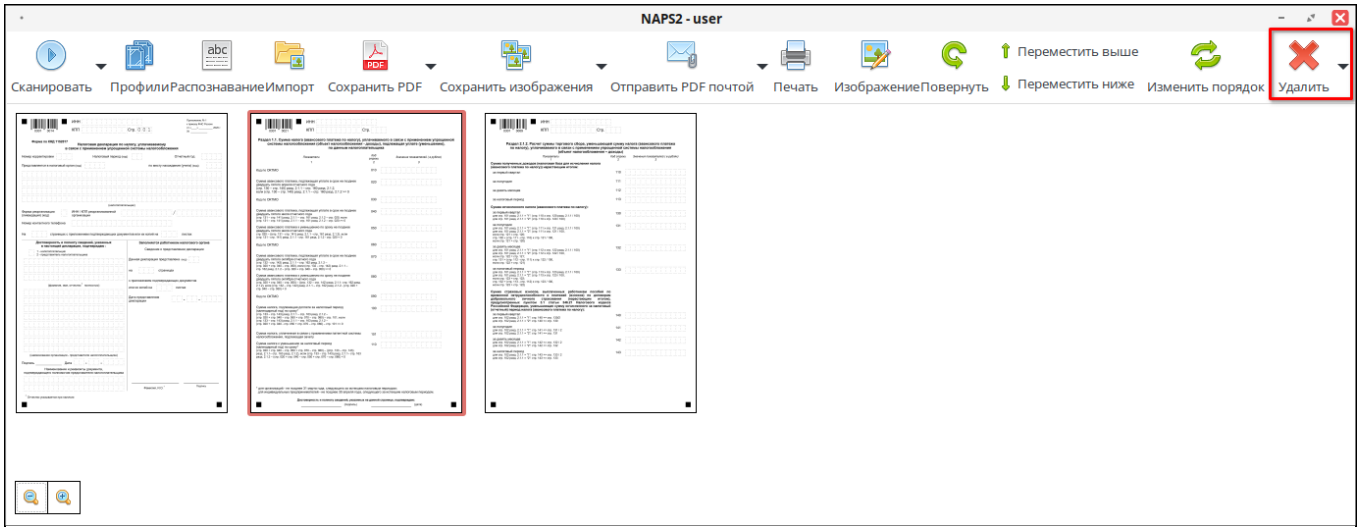
Для редактирования PDF-файла экспортируйте нужный документ в программу NAPS2. Документ будет разложен по страницам, можно удалить ненужные или добавить новые страницы, а также объединить их с другим документом. После выполненных преобразований сохраните подготовленный файл на компьютере как новый документ в формате PDF.

Для изменения формата документа, загруженного в формате PDF, нажмите «**Сохранить изображение**» и выберите нужный формат.

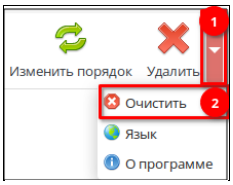


Удаление документа

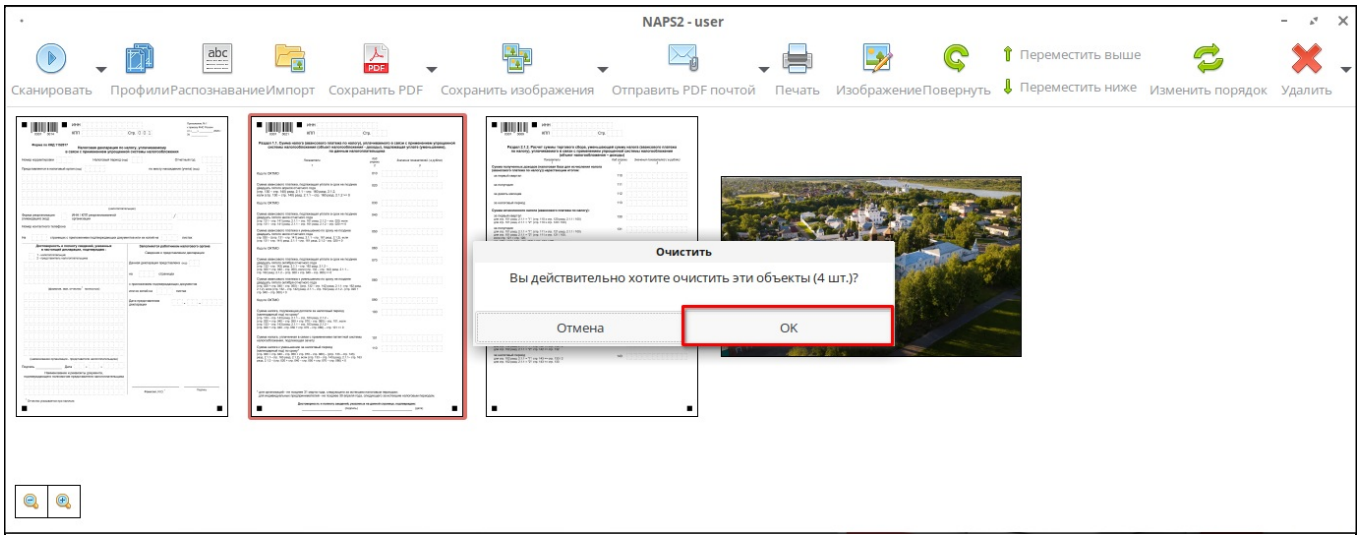
Для удаления страницы документа из рабочей области программы выделите нужную страницу и нажмите на инструмент «**Удалить**».



Для удаления всех документов из рабочей области нажмите на выпадающий список инструмента «**Удалить**» — «**Очистить**».



Появится предупреждающее сообщение об удалении объектов. Для очистки рабочей области нажмите «**OK**».


NAPS2 - user
Сканировать
Профили
Распознавание
Импорт
Сохранить PDF
Сохранить изображения
Отправить PDF почтой
Печать
Изображение
Повернуть
Переместить выше
Переместить ниже
Изменить порядок
Удалить
Очистить
Вы действительно хотите очистить эти объекты (4 шт.)?
Отмена
OK

Каталогизаторы фотоальбомов

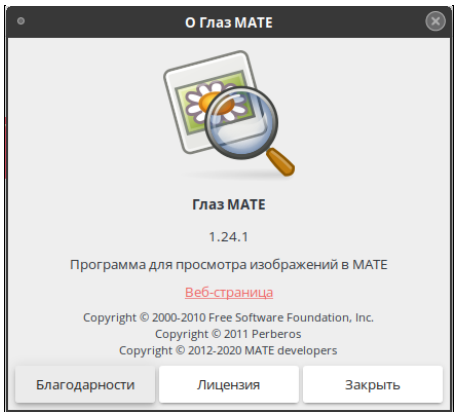
Pix
gThumb

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** eom-1:1.24.1-2, pix-2.6.2-1, gthumb-3.10.1-1

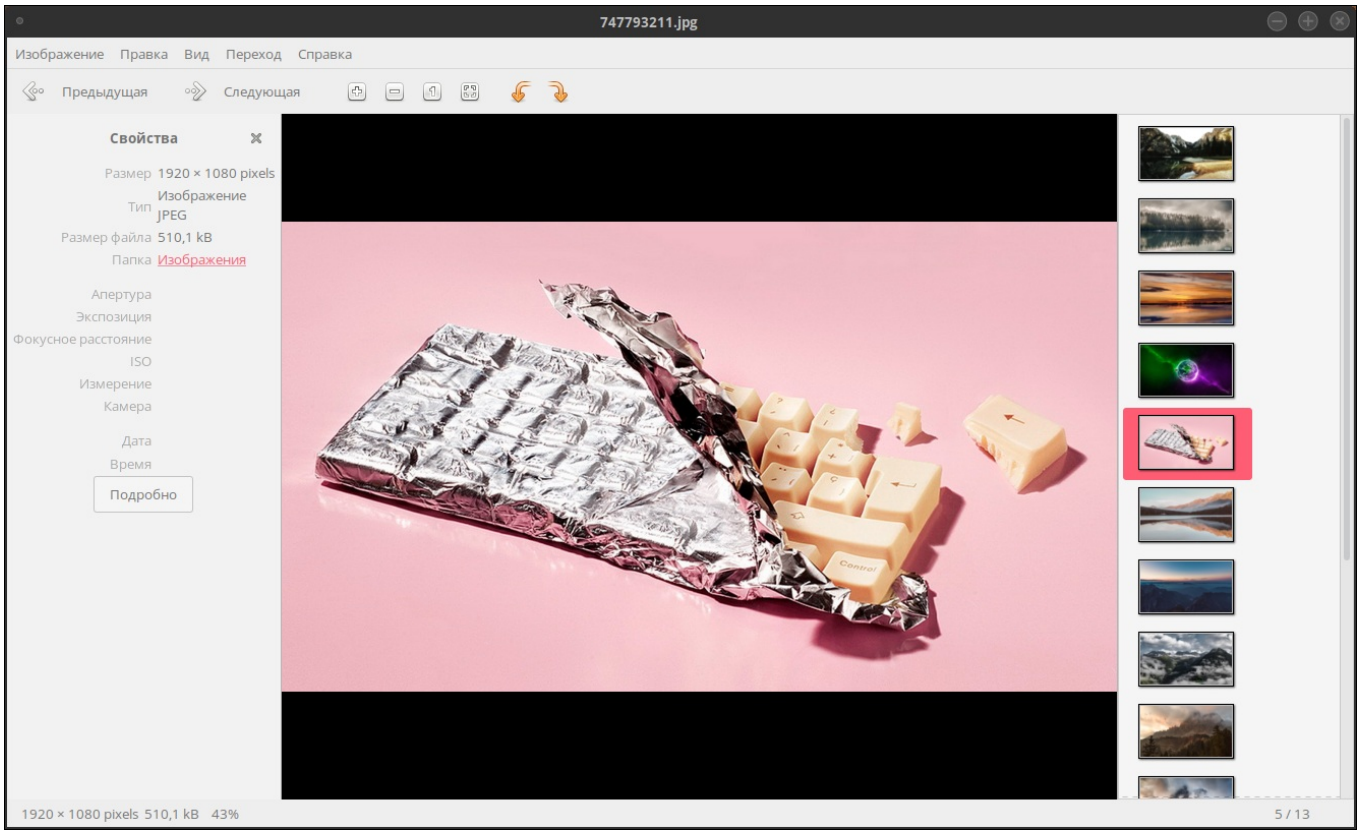
Многие пользователи хранят и просматривают различные изображения, поэтому неотъемлемой частью любой ОС является программа просмотра изображений.

В РЕД ОС по умолчанию установлена программа **Глаз MATE**.



Функционала этой программы достаточно, чтобы просматривать изображения. **Глаз MATE** поддерживает несколько элементарных функций:

- переключение между изображениями в каталоге;
- масштабирование размера изображения под настройки экрана пользователя;
- установка картинки в качестве фонового изображения рабочего стола;
- поворот и отражение изображений и др.



В репозитории РЕД ОС имеются две программы с большим функционалом для просмотра изображений:

- **Pix**;
- **gThumb**.

Программы предназначены для просмотра, редактирования и упорядочивания коллекции графических и видео-файлов, имеют простейшие функции редактирования графики (различные коррекции, в том числе автоматические).

Основные возможности программ:

- просмотр изображений;
- автоматическое обновление содержимого директорий при просмотре;
- копирование, перемещение, удаление изображений или директорий;
- поддержка просмотра основных форматов: BMP, JPEG, GIF, PNG, TIFF, TGA, ICO, XPM;
- просмотр данных EXIF;
- фильтрация изображений;
- сортировка;
- редактирование;
- экспорт в различные форматы;
- просмотр слайд-шоу;
- автоматический поворот изображений на основе метаданных;
- создание фотоальбомов;
- импорт изображений с внешних устройств;
- поиск дубликатов;
- встроенная функция для массового переименования файлов с использованием шаблонов;
- поддержка плагинов и др.

Вы можете подробнее ознакомиться с возможностями **Pix** и **gThumb**, просмотрев наши обучающие видео:

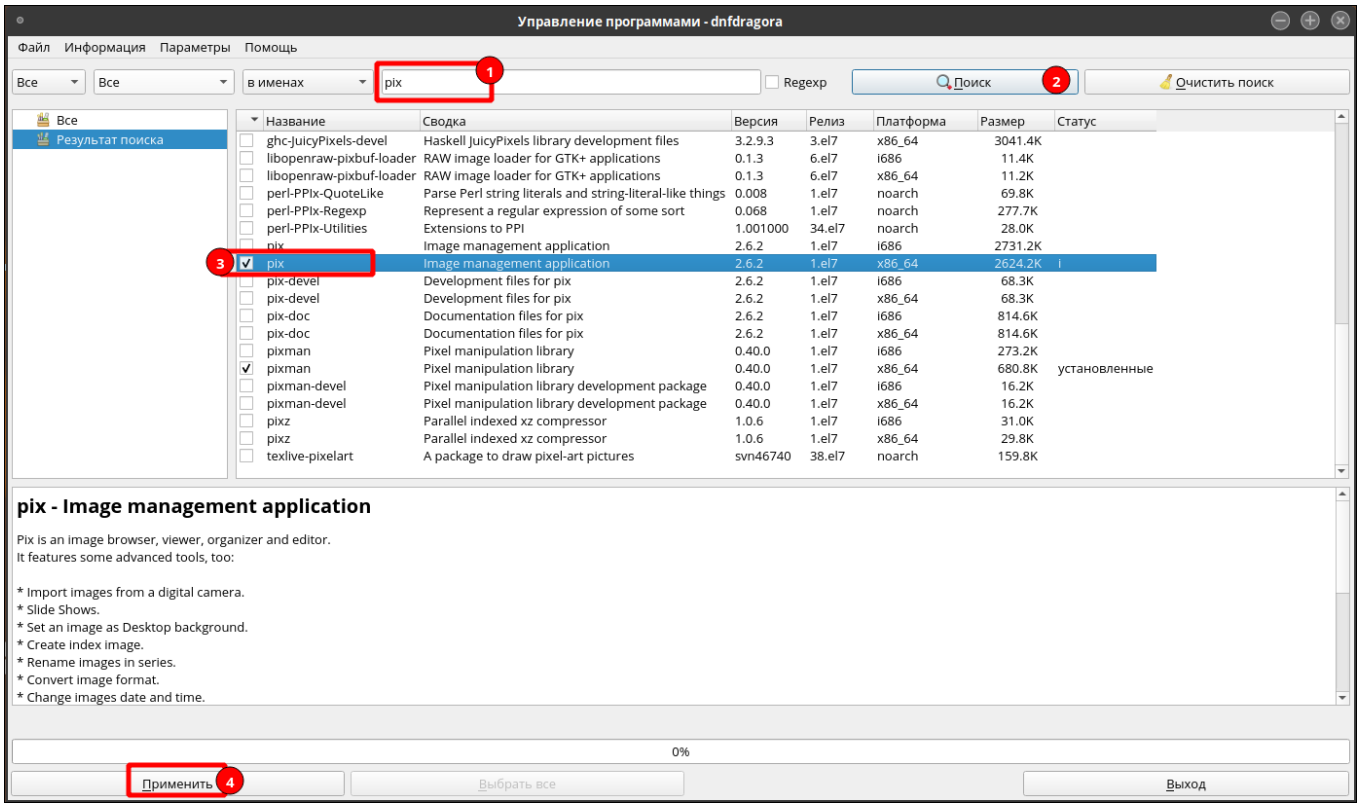
- на **RuTube** — Каталогизаторы фотоальбомов в РЕД ОС;
- в **Яндекс.Дзен** — Каталогизаторы фотоальбомов в РЕД ОС;
- в **VK Видео** — Каталогизаторы фотоальбомов в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Pix

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**pix**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install pix
```

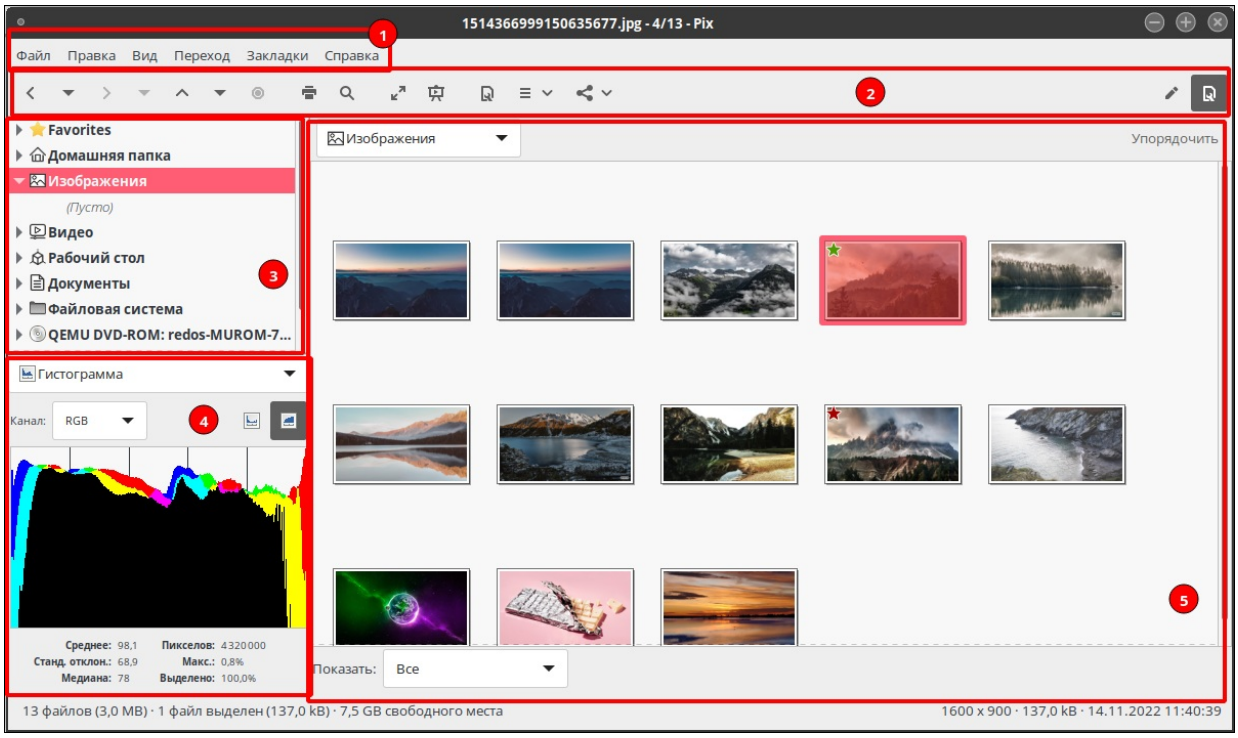
Дальнейшая работа в программе выполняется от ***локального пользователя***.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**Каталогизатор изображений Pix**».

Описание программы

Pix имеет классический интерфейс, в верхней части окна программы находится стандартное основное меню (**1**).

Ниже основного меню находится панель инструментов (**2**). Вид панели инструментов немного отличается в разных режимах программы (режим просмотра и режим навигации). При наведении на иконку появляется всплывающая подсказка о назначении инструмента.

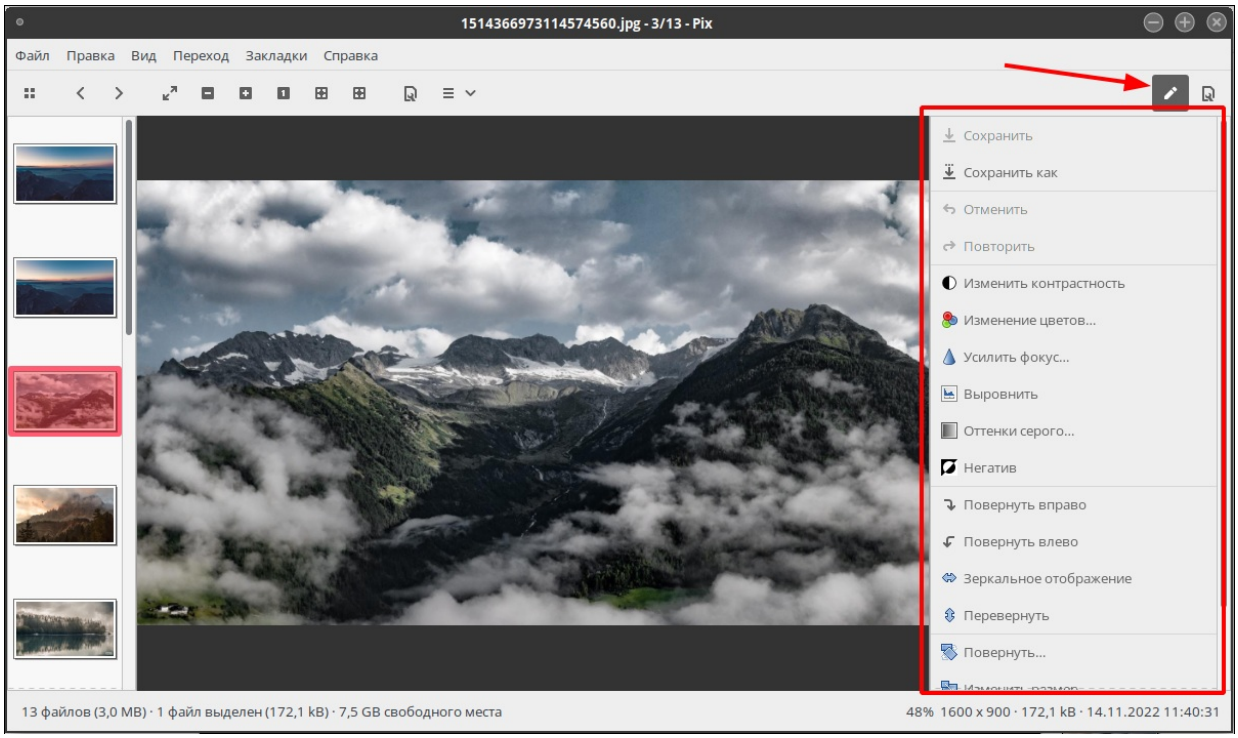


Программа имеет большой функционал, который позволяет осуществлять навигацию по дереву каталогов (**3**) и просматривать файлы изображений.

В поле свойств изображения (**4**) можно просмотреть основную информацию о выбранном изображении или вывести его гистограмму на линейной или логарифмической шкале.

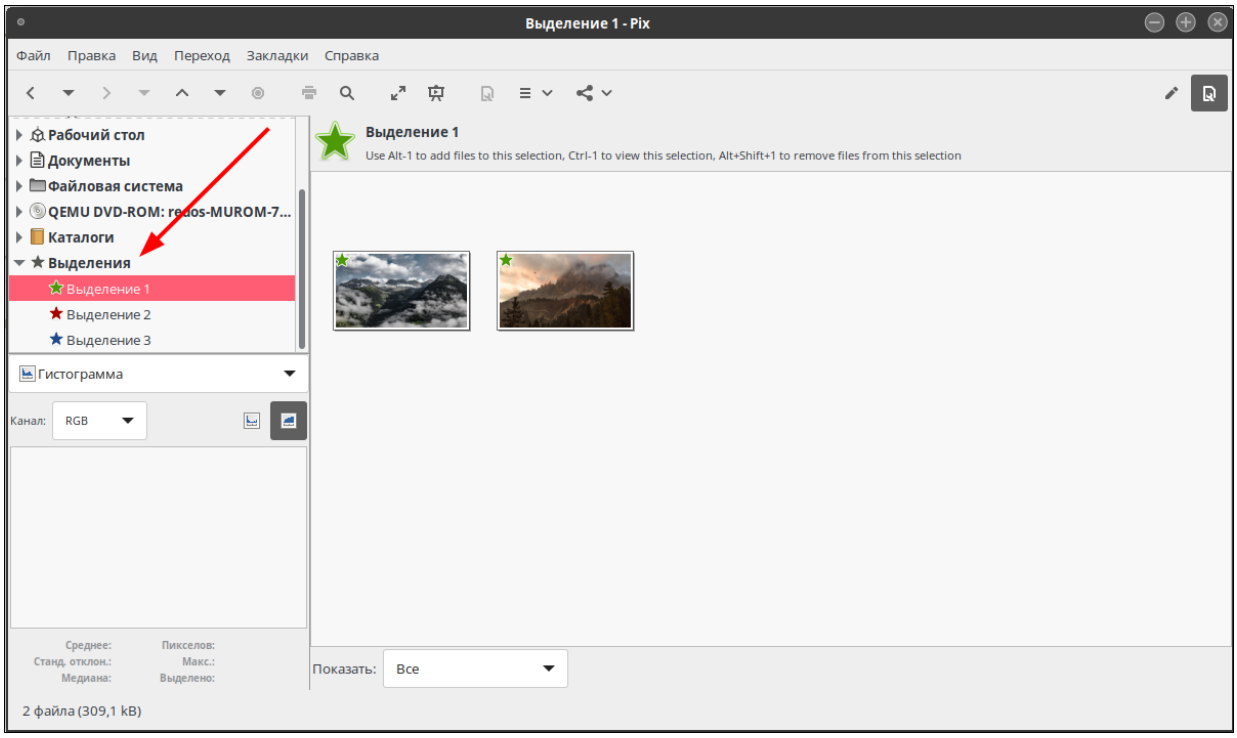
В поле просмотра изображений (**5**) отображается список доступных файлов в выбранном каталоге дерева.

Функции редактирования изображений доступны через иконку с карандашом на панели инструментов.



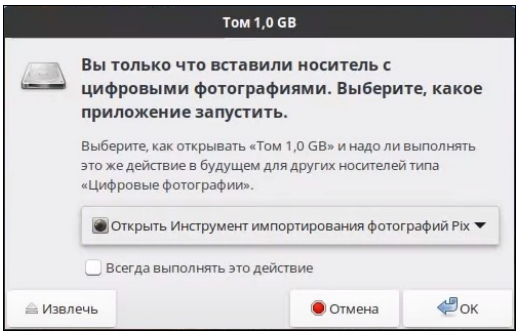
Здесь можно найти много полезных инструментов для простой коррекции фотографии, а именно — яркость и контрастность, поворот влево или вправо, а также зеркальное отображение, произвольный поворот, изменение размера и устранение эффекта красных глаз. После любых изменений программа предлагает сохранить изменения в файле.

Pix обладает базовыми функциями для организации изображений. Нажав правой кнопкой мыши по изображению либо выделив сразу несколько изображений, можно добавить их в одно из трех Выделений — это полезно при отсмотре каталога. Затем в дереве каталогов можно открыть выделения и просмотреть все отмеченные фото.

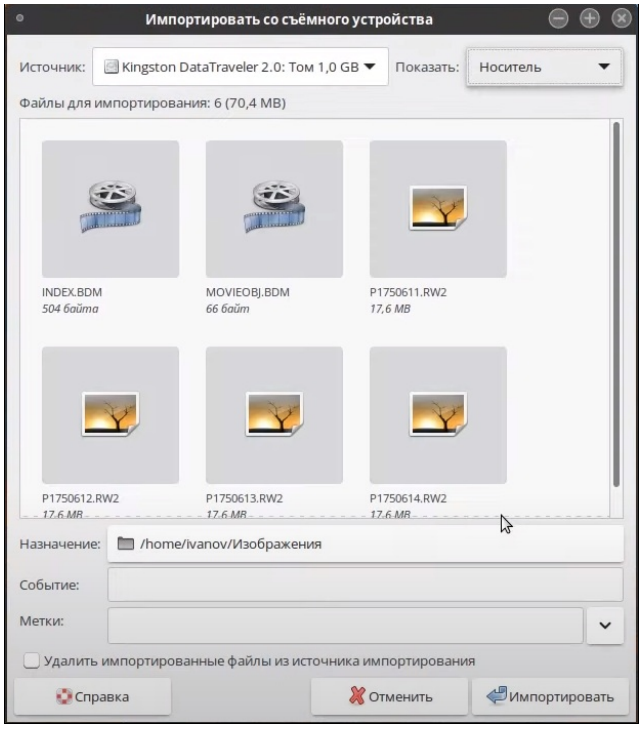


Также есть возможность присвоить метки и добавлять комментарии. Нажав правой клавишей мыши по нужному изображению, можно установить его в качестве фона рабочего стола.

Полезен также инструмент, позволяющий импортировать фотографии прямо из камеры или съемного носителя. Для этого необходимо подсоединить устройство, откроется окно, в котором будет предложено открыть **Инструмент импортирования фотографий Pix**. При этом не обязательно, чтобы *Pix* был открыт заранее.

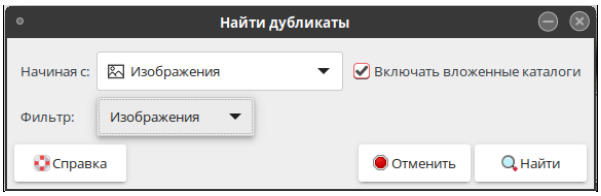


Нажмите «**OK**», откроется меню импорта, в котором можно выбрать необходимые файлы и указать папку назначения.

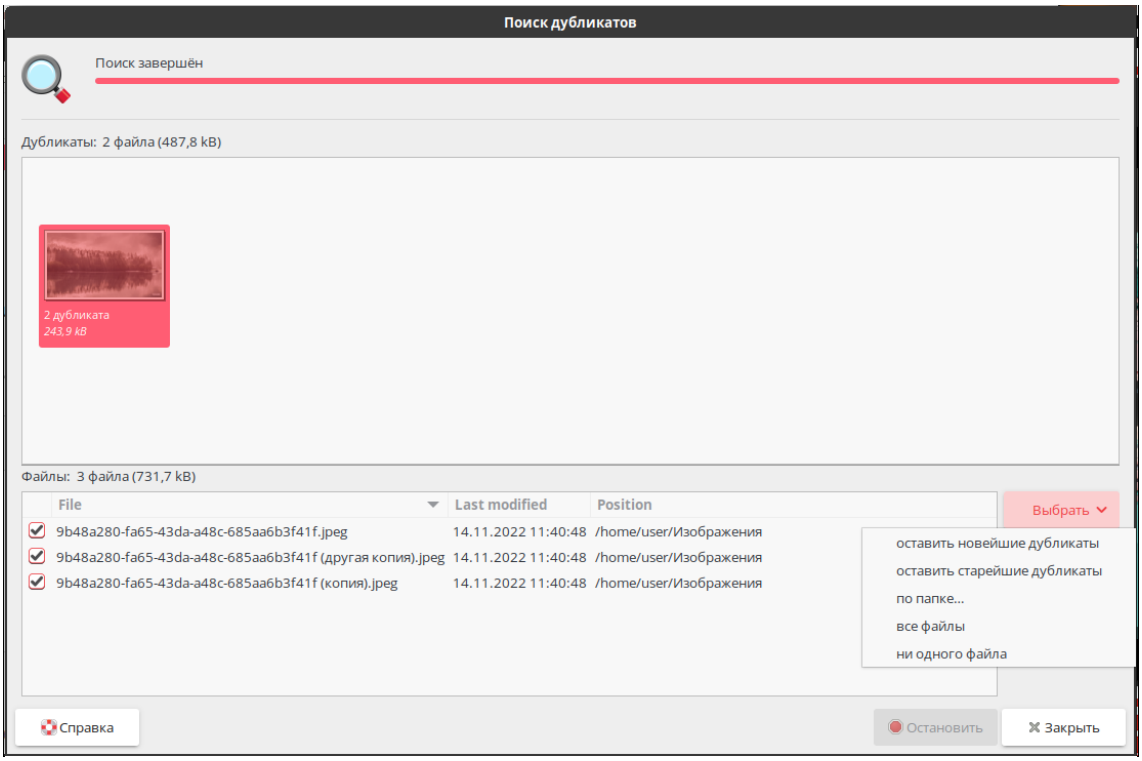


Бывают ситуации, когда при копировании или перемещении фотографий появляются одинаковые фото (дубли), которые занимают полезное место на диске. *Pix* может помочь в решении данной проблемы.

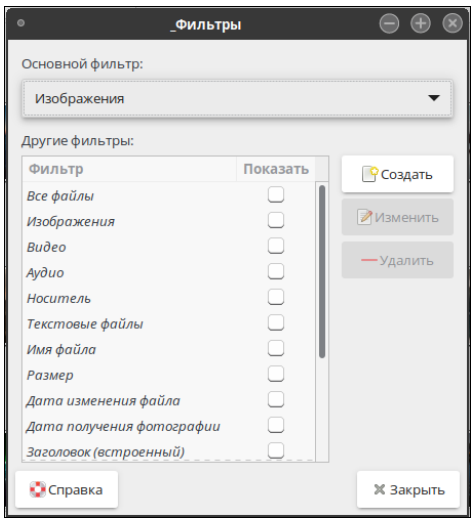
В основном меню откройте раздел «**Правка**» - «**Найти дубликаты...**», выберите нужный каталог и нажмите «**Найти**». Начнется поиск дубликатов.

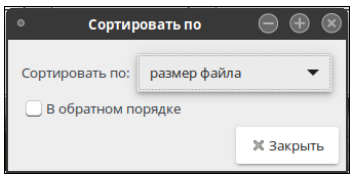


Нажав на любую фотографию, можно узнать, где находится копия. Также доступен выбор необходимых действий, которые нужно сделать с дубликатами, после чего можно удалять копии.



Также могут оказаться полезны функции фильтров и сортировки. Для настройки перейдите в пункт меню «**Вид**» - «**Сортировать по...**» или «**Вид**» - «**Фильтр...**» и установите необходимые значения.



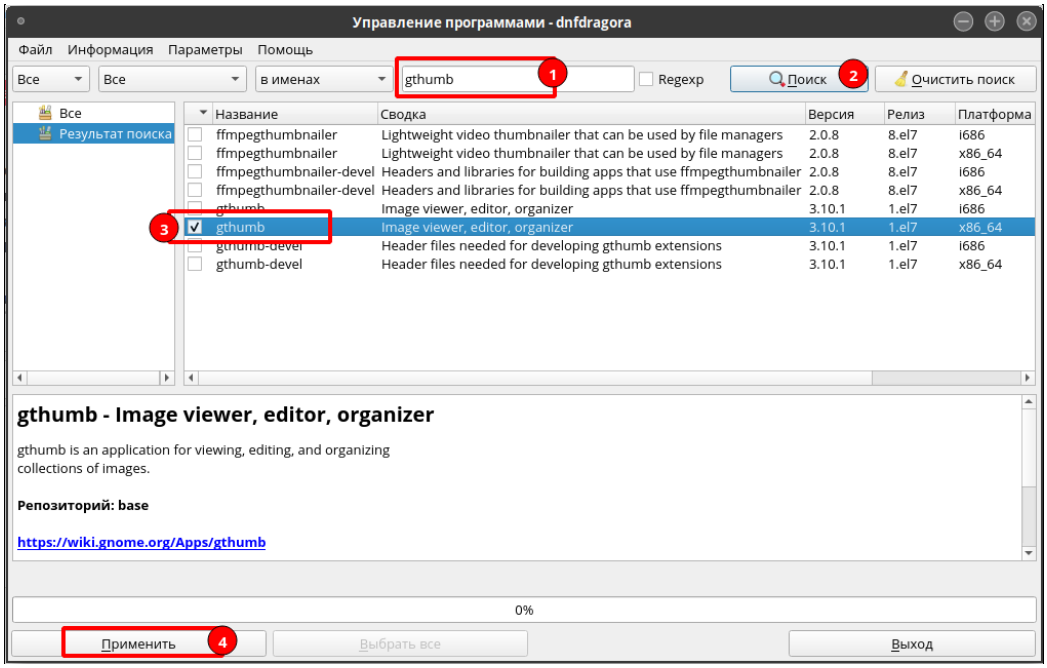


gThumb

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**»

— «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**gthumb**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

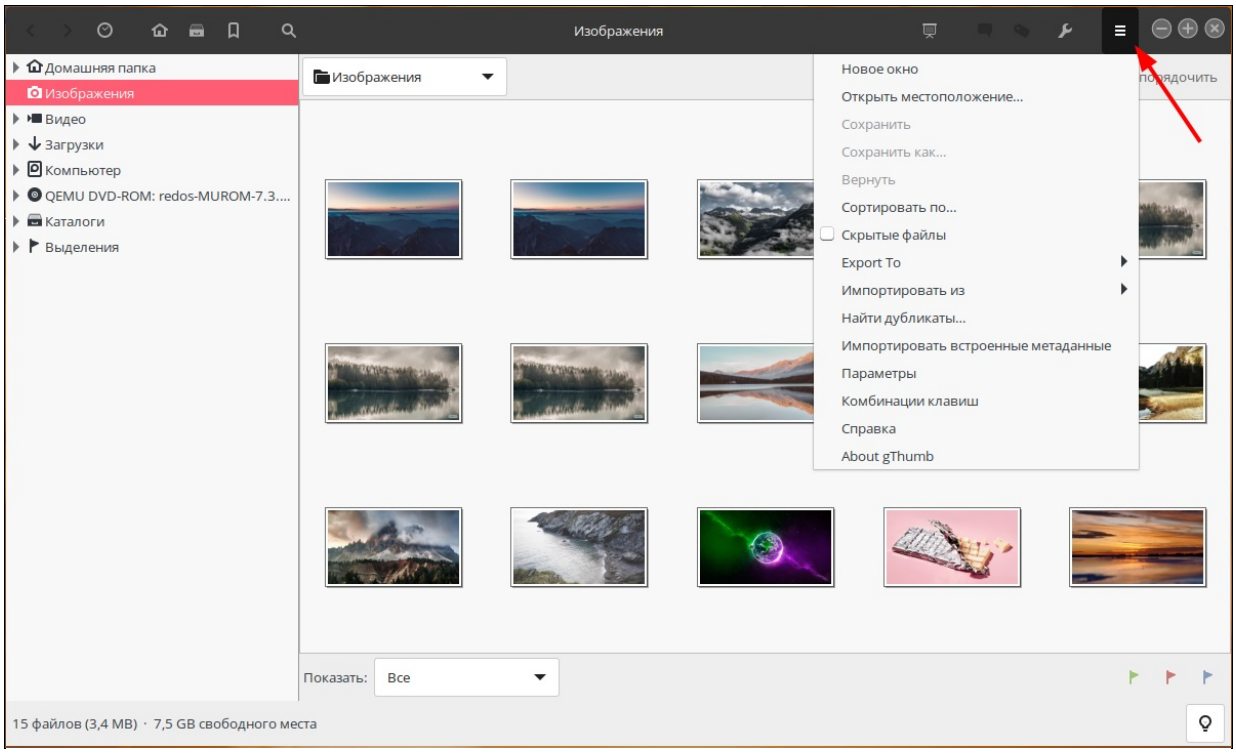
```
dnf install gthumb
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**Каталогизатор изображений gThumb**».

Описание программы

Функционал программы *gThumb* похож на *Pix*, основные отличия заключаются в более современном интерфейсе. Стандартного меню нет, оно доступно через кнопку в правой части заголовка окна.

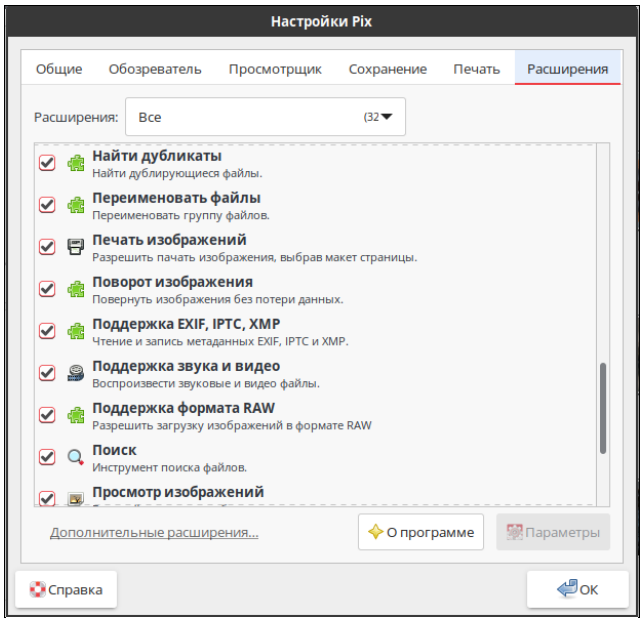


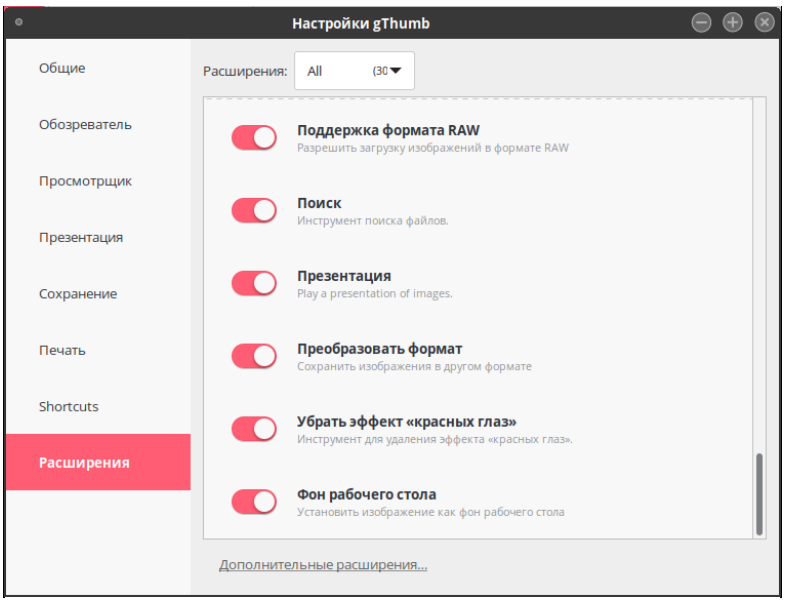
gThumb имеет большой функционал, позволяющий не только просматривать файлы изображений и осуществлять навигацию по дереву каталогов, но и редактировать файлы. Большим преимуществом перед *Pix* является открытие RAW-файлов — для фотографов это очень полезная функция.

Еще одной полезной функцией может оказаться массовое переименование файлов. Для этого выделите все нужные фотографии и нажмите по ним ПКМ, в контекстном меню выберите «**Переименовать**». Откроется окно, в котором можно задать шаблон, указать начало нумерации, сортировку и увидеть список файлов с новыми наименованиями в таблице предварительного просмотра.

Также доступны перечисленные ранее функции из *Pix*, такие как поиск дубликатов, редактирование изображений, инструменты для организации изображений в каталогах, импорт с фотокамеры или съемного носителя и т. д.

Функционал данных программ может быть легко дополнен за счёт использования различных расширений. Расширения можно подключать в настройках программ.





Darktable — программа каталогизации и обработки цифровых фотографий в формате RAW

Установка
Описание программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: darktable-3.4.0

Darktable — это программа для каталогизации и обработки цифровых фотографий в формате **RAW**. Она предоставляет пользователям различные инструменты для редактирования изображений и управления фотоколлекцией.

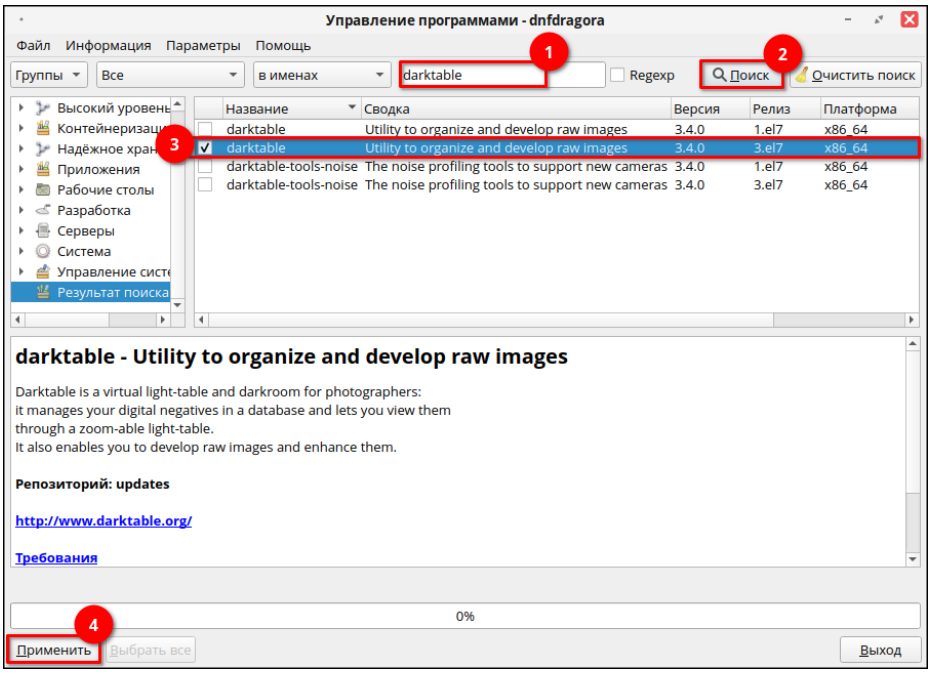
Основные возможности **Darktable**:

- поддерживает широкий спектр форматов RAW от различных камер;
- работает с форматами JPEG, TIFF, PNG, OpenEXR и другими;
- все изменения сохраняет отдельно от оригинального файла, позволяя вернуться к исходному изображению;
- обрабатывает изображения с глубиной цвета 32 бита на канал в цветовом пространстве CIE LAB;
- поддерживает использование масок и слоев для точного редактирования отдельных участков изображения;
- позволяет ускорить обработку изображений благодаря поддержке OpenCL;
- полностью поддерживает работу с цветовыми профилями и пространства, такими как sRGB, Adobe RGB, XYZ и линейный RGB;
- более 60 модулей для разных задач: трансформация, цветокоррекция, улучшение качества и художественные эффекты;
- поддерживает параметрические и нарисованные маски, а также работу с графическими планшетами;
- компенсирует дисторсию и хроматические аберрации объектива;
- каталогизирует изображения, добавляет метки и позволяет искать фотографии по разным параметрам;
- поддерживает прямую съемку через подключенный фотоаппарат;
- экспортирует изображения в разные форматы, включая JPEG, PNG, TIFF, WebP, PPM, TIFF, PFM, OpenEXR;
- может экспортировать изображения на онлайн-сервисы;
- поддерживает цветовые профили ICC и OpenCL для аппаратного ускорения.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**darktable**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

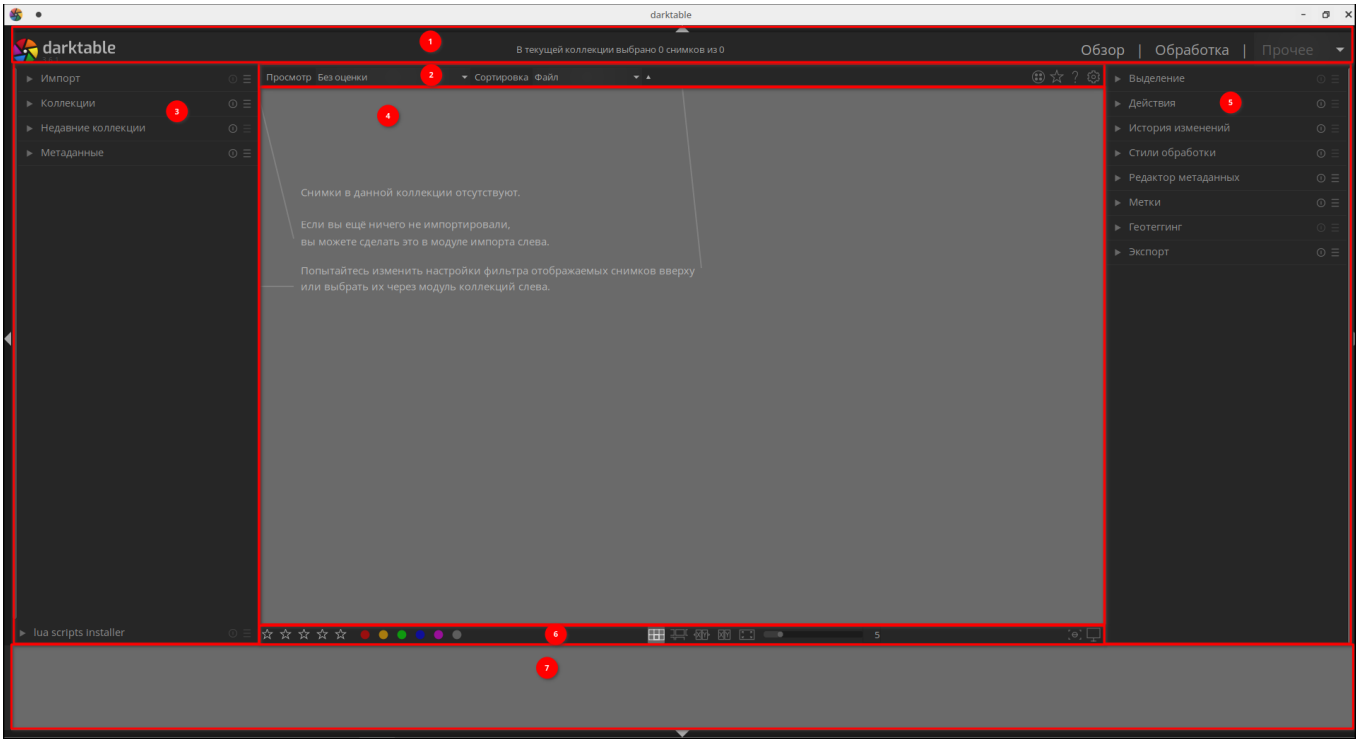
```
sudo dnf install darktable
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

После установки программа будет доступна из «**Главного меню**» — «**Графика**» — «**Darktable**».

Описание программы

Главное окно программы **Darktable** выглядит следующим образом.



Интерфейс программы разделен на несколько ключевых частей:

1. **Панель режимов** позволяет переключаться между режимами работы. В зависимости от режима работы содержание всех панелей будет меняться.

2. **Верхняя панель** предоставляет быстрый доступ к основным настройкам и функциям программы, включая глобальные параметры и режимы работы.

3. **Левая панель** предназначена для предоставления дополнительной информации, а также для навигации по различным элементам интерфейса.

4 . **Центральная часть** отображается основная рабочая область, где могут быть представлены такие элементы, как текущее изображение, группа изображений, карта и другие объекты, с которыми ведется работа.

5 . **Правая панель** содержит набор инструментов для редактирования и обработки изображений, позволяя пользователям вносить необходимые изменения.

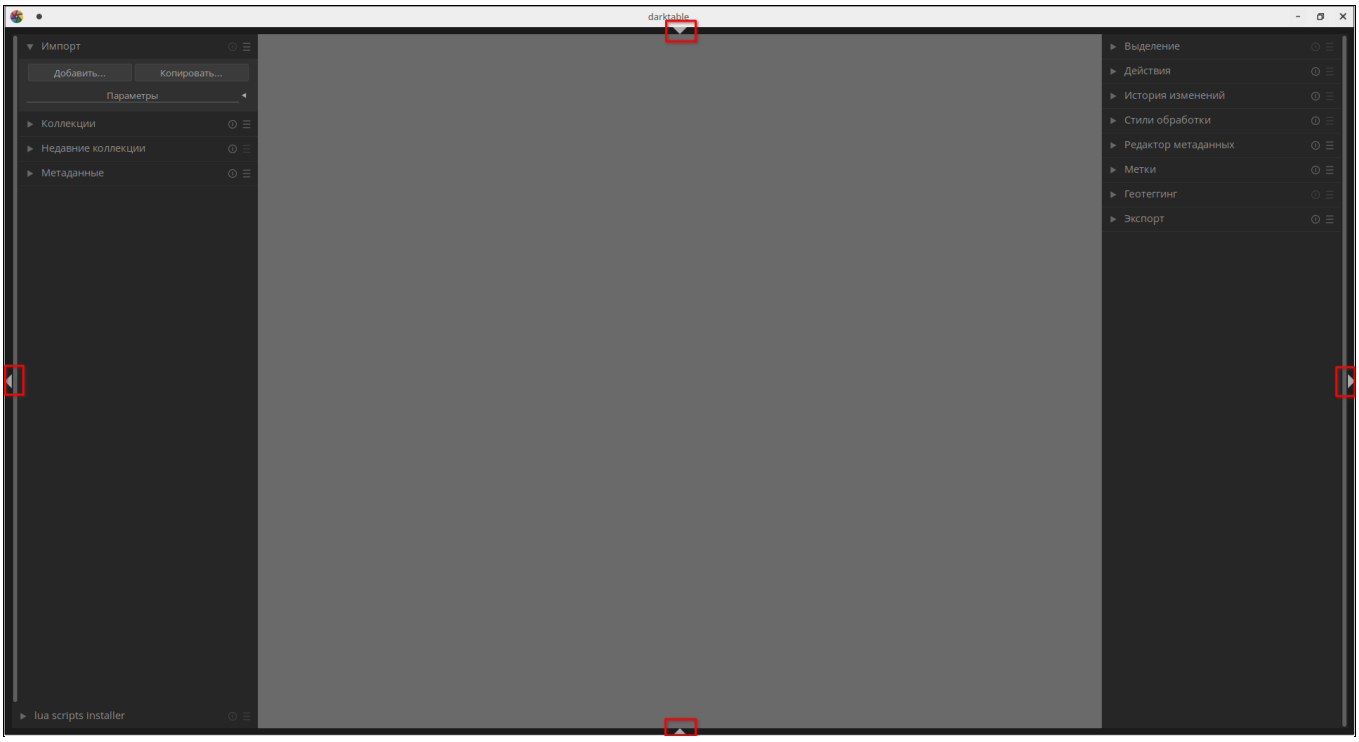
6. **Нижняя панель** предоставляет дополнительные настройки и функции, которые могут понадобиться для более детальной работы с изображениями или проектами.

7 . **Лента фотографий** располагается в нижней части окна программы, отображает такие же изображения, что расположены в центральной части программы, позволяет взаимодействовать с изображениями вне режимов Обзор и Слайдшоу. Для включения/выключения используется сочетание клавиш **Ctrl+F**. Можно перемещаться по ленте фотографий, прокручивая ее колесиком мыши.

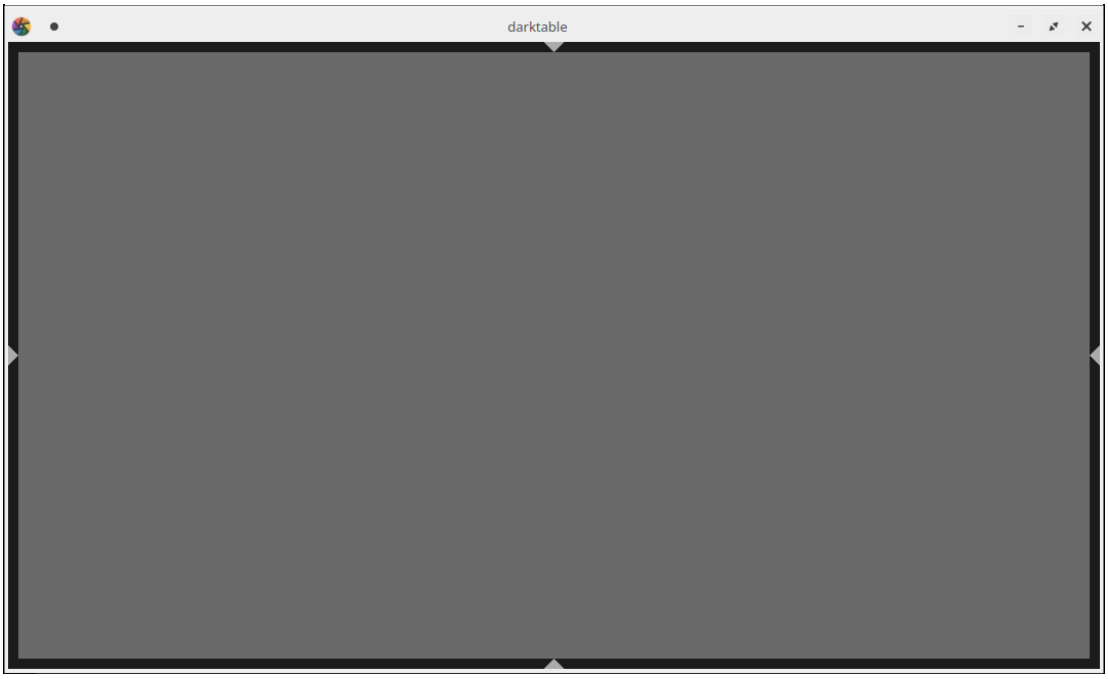
Расширение пространства рабочей области

Для расширения пространства рабочей области доступно несколько вариантов.

1. Каждая панель может быть скрыта или возвращена нажатием на кнопку в виде треугольника  , расположенную рядом с панелью.



2. При нажатии клавиши **TAB** все панели сворачиваются, а центральная область занимает все освободившееся пространство. Повторное нажатие **TAB** возвращает к предыдущему виду.



3. Для перехода/возврата просмотра окна программы на полный экран необходимо нажать клавишу **F11**.

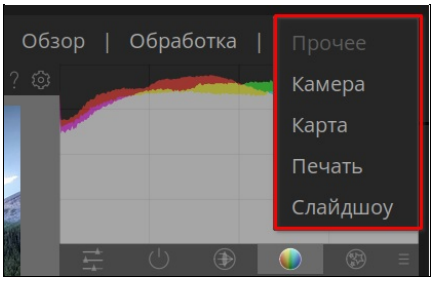
Режим работы

В **Darktable** реализовано шесть режимов работы.

Переключаться между ними можно, щелкая курсором мыши по названию режима в панели, расположенной справа сверху окна программы, активный режим подсвечивается, или с помощью горячих клавиш:

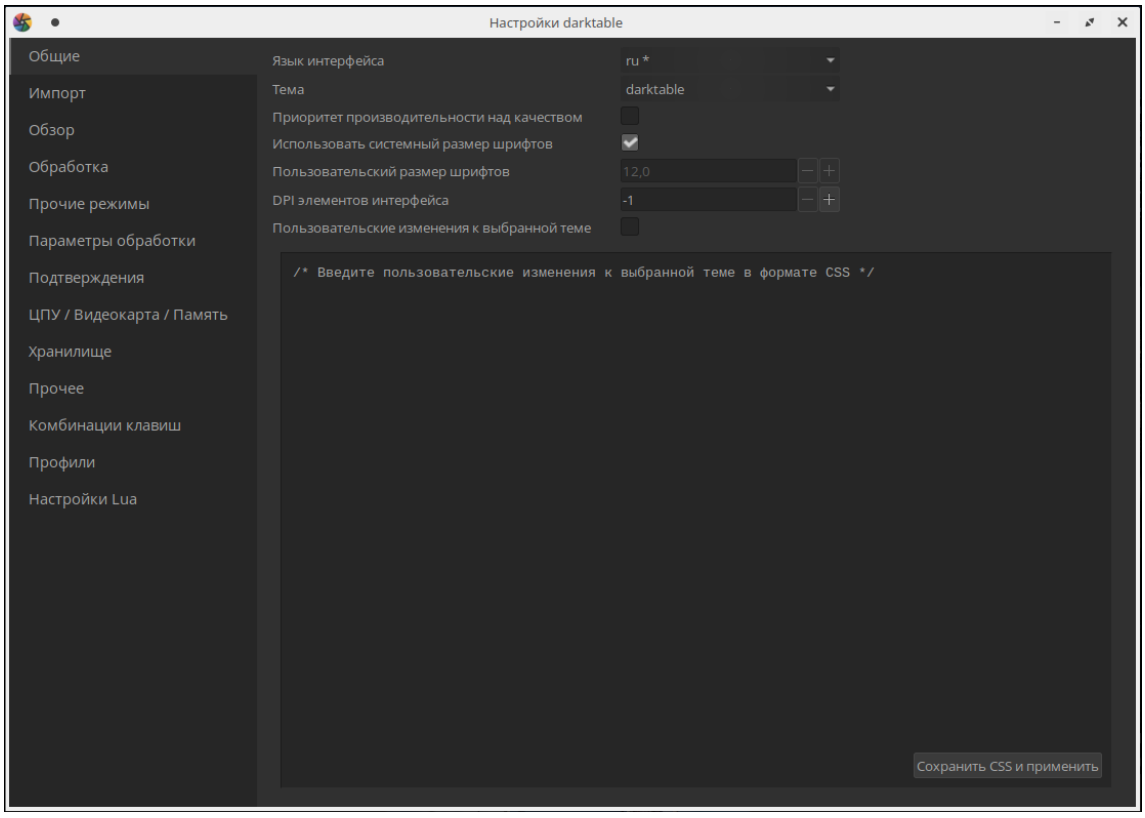
- **L** (**lightable**) — в режиме Обзор осуществляется управление снимками и фотоархивом, осуществляется оценка изображений, добавляются ключевые слова (теги), присваиваются цветовые метки и экспортируются изображения;
- **D** (**darkroom**) — в режиме Обработка происходит редактирование снимка с использованием доступных модулей;
- **T** (**camera tethering**) — режим Камера предназначен для съёмки камерой, подключенной к компьютеру, обеспечивает захват изображений для передачи и просмотра на компьютере;
- **M** (**map**) — в режиме Карта отображаются снимки с географическими координатами (геотеги) и предоставляется возможность вручную привязать изображение к карте;

- **P** (**print**) — режим Печать предназначен для отправки изображений на печать;
- **S** (**slideshow**) — в режиме Слайдшоу осуществляется показ изображений в виде слайд-шоу, процесс конвертации снимков производится на лету.



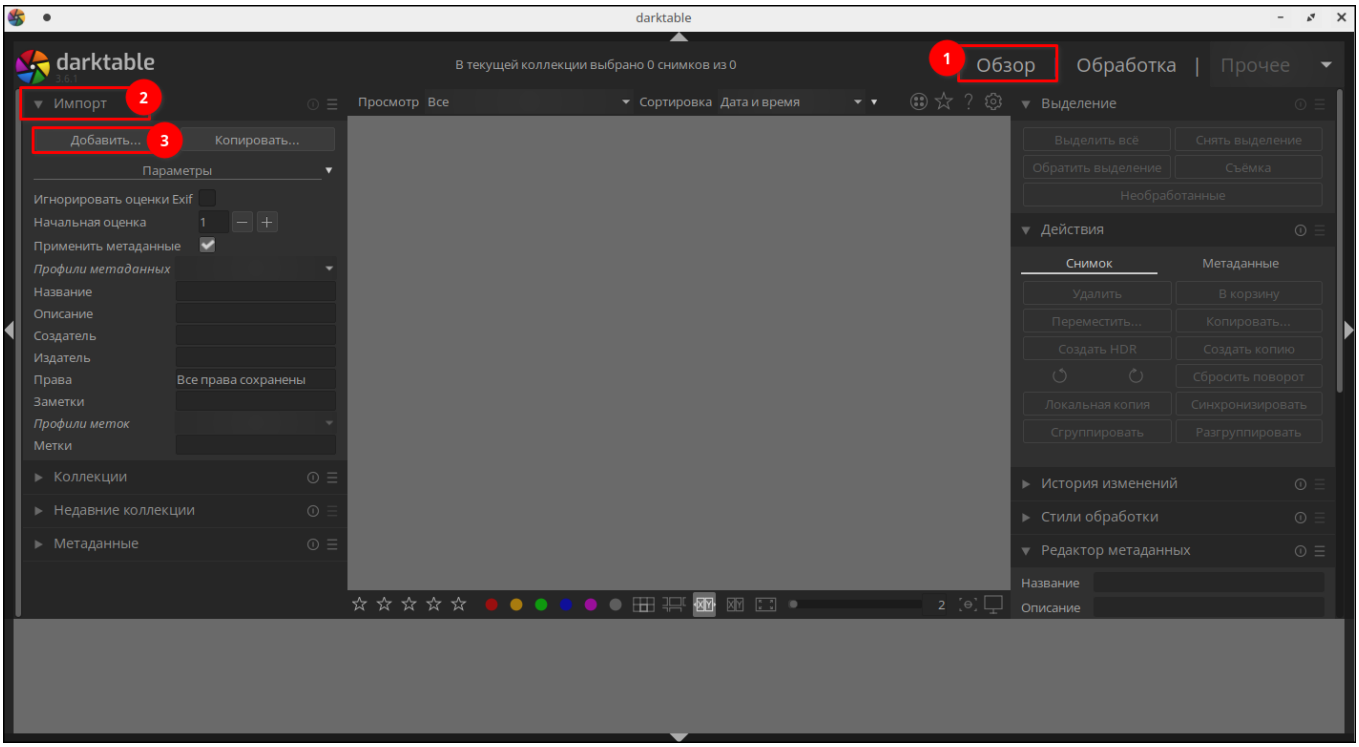
Общие настройки

При нажатии кнопки  на верхней панели окна программы откроется доступ к различным настройкам, позволяющим настроить поведение программы **Darktable**.



Импорт изображений

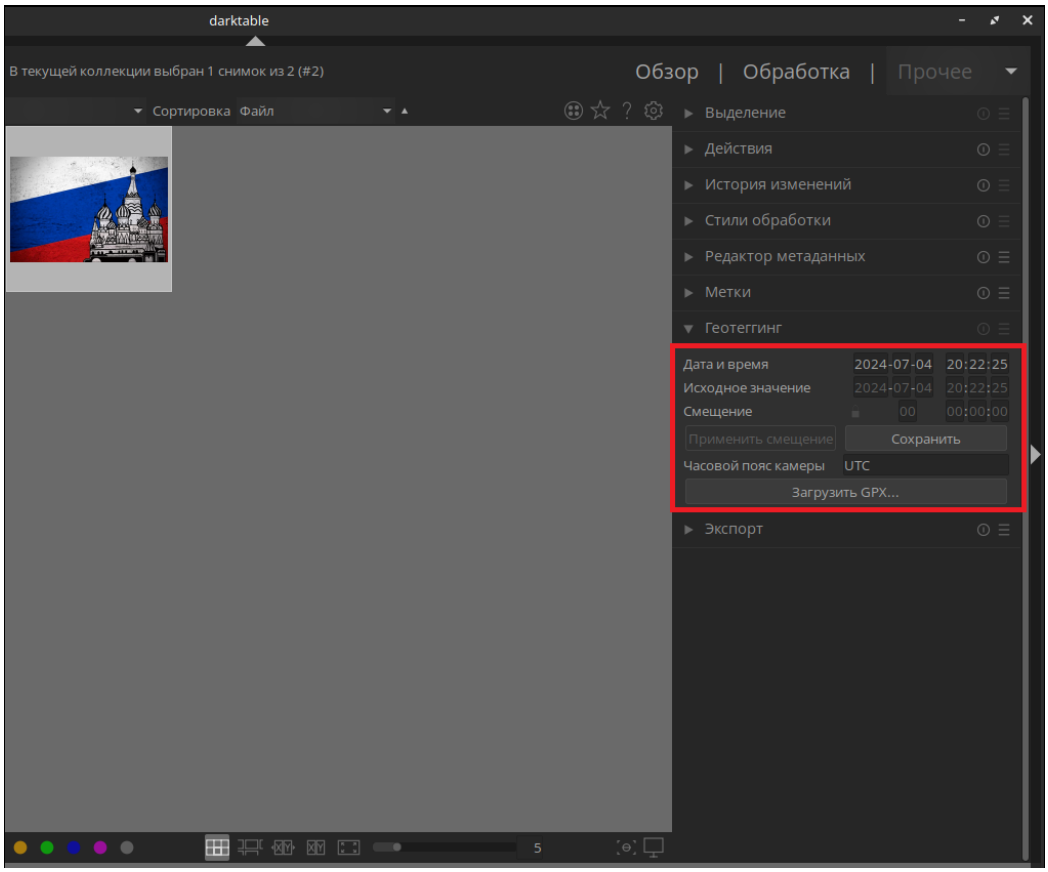
После запуска программы первый раз ее центральная часть не содержит данных. Для добавления данных в программу необходимо импортировать изображение. Можно импортировать либо одно изображение, либо папку.



Добавление геотегов к фотографиям

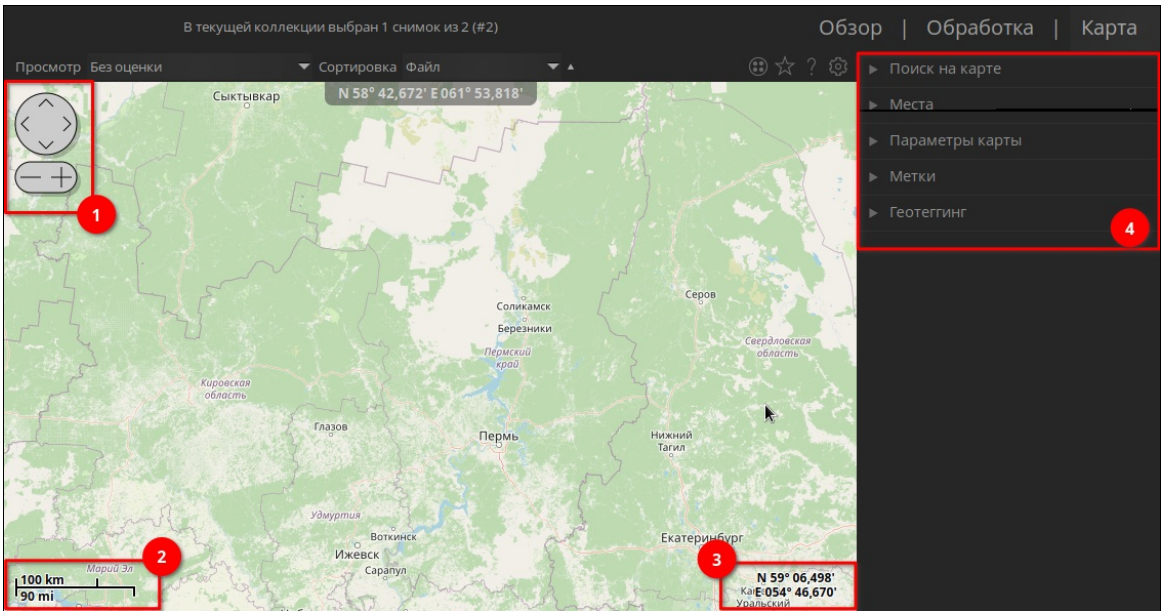
Для точного определения местоположения сделанных фотографий рекомендуется использовать функцию **геотеггинга**. Эта возможность позволяет добавлять к изображениям данные о географических координатах, что полезно при обработке большого количества снимков, сделанных в разных местах.

Если изображение имеет отметку времени по **UTC** (**Coordinated Universal Time** — всемирное координированное время), можно применить GPX-трек без дополнительных настроек. Для применения геотегов нужно перейти в режим Обзор в раздел «**Геотеггинг**» и добавить GPX-трек к снимку.



Кроме этого, можно вручную определить географические координаты изображения в режиме Карта. Режим Карта отображает карту мира с открытыми изображениями, привязанными к их географическому положению. Данные карты берутся из открытых источников в Интернете. Навигацию можно осуществлять по карте. Удерживая ЛКМ, можно перемещаться по карте, а колесиком прокрутки

регулировать её масштаб.

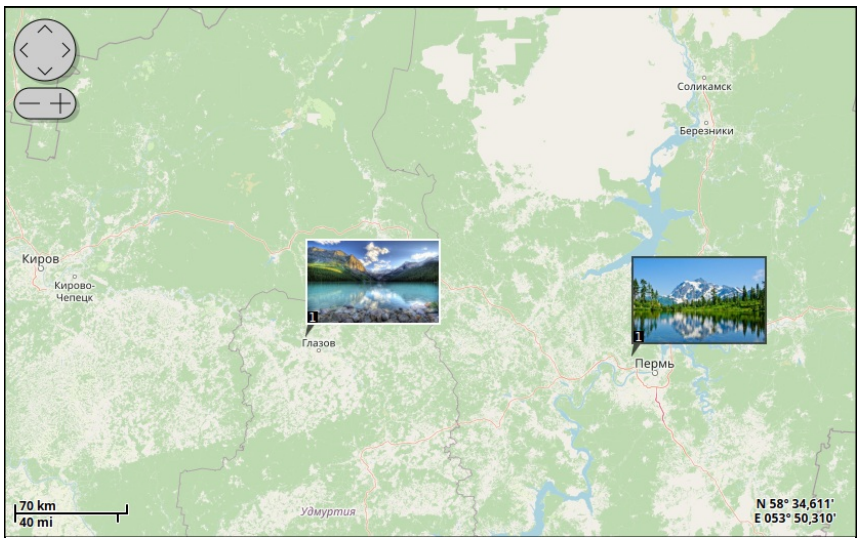


На карте представлены элементы управления и информационная панель для ориентации. Навигационные инструменты расположены в верхнем левом углу карты и служат альтернативой управлению с помощью мыши (1).

Шкала расстояний находится внизу слева (2).

В правом нижнем углу отображаются географические координаты центральной точки карты (3).

Рядом с картой находятся дополнительные панели, предоставляющие расширенные настройки и управление картой (4). Изображения, для которых определены географические координаты, отмечаются на карте небольшими значками.

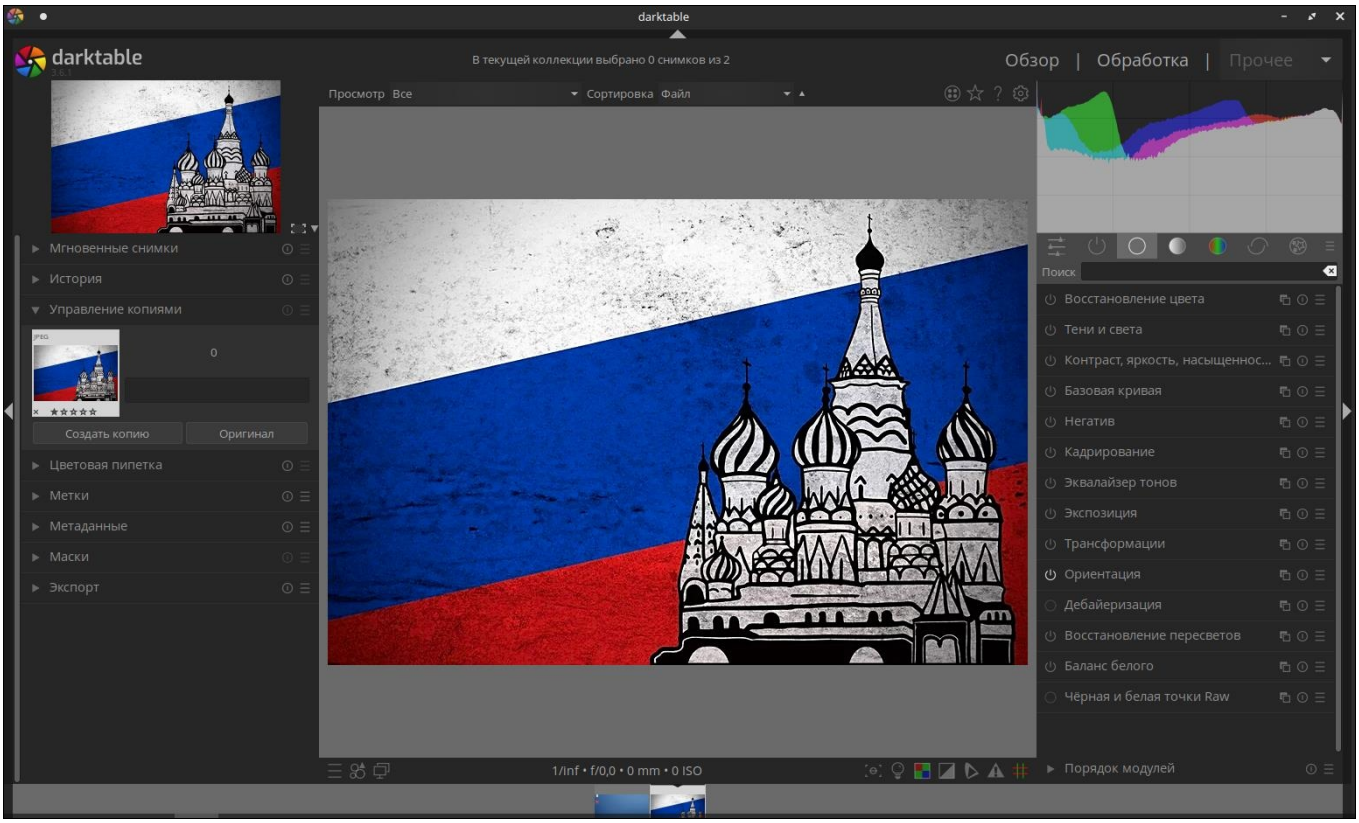


Для назначения географических координат изображению откройте ленту фотографий на нижней панели. Чтобы задать изображению местоположение, просто перетащите соответствующую фотографию с ленты фотографий на нужную точку на карте. **Darktable** автоматически сохранит новые координаты (широту и долготу) в метаданные изображения. Эти данные будут включены в экспортированное изображение.

Чтобы убрать географическую привязку у изображения, достаточно перетащить его обратно на ленту фотографий.

Обработка/редактирование снимков

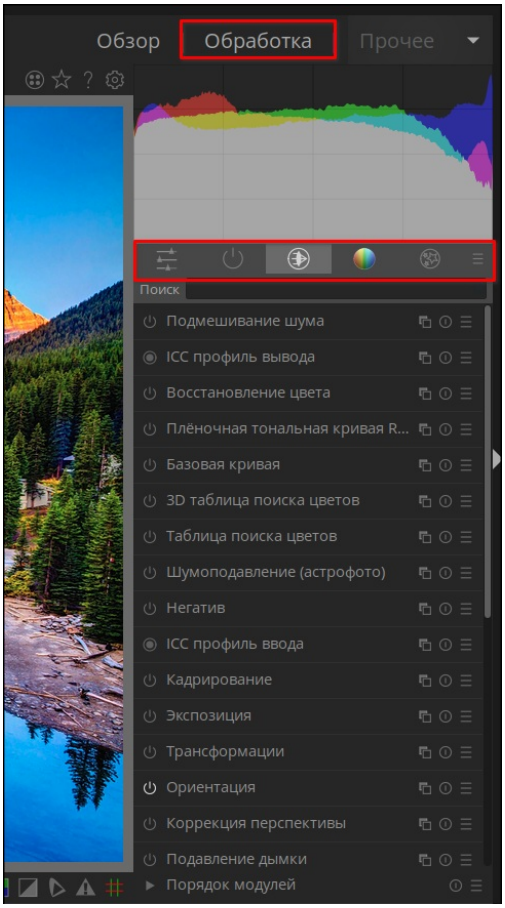
Обработка — режим, предназначенный для редактирования изображений. Здесь можно внести необходимые корректировки.



На панели справа можно выбрать настройки коррекции для улучшения изображений: повышение резкости размытых снимков, коррекцию баланса белого цвета и обрезку элементов, которые могли случайно попасть в кадр.

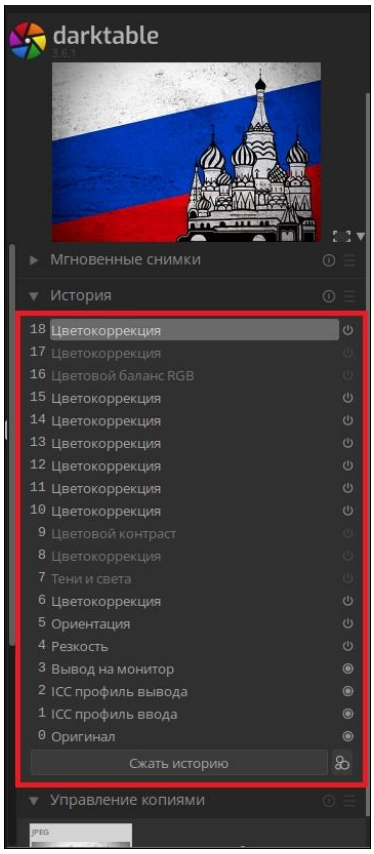
С помощью регулировок контрастности объект можно сделать ярче. Бегунки панели позволят экспериментировать с цветами, настраивать освещение. Здесь доступны такие эффекты, как размытие движения и виньетирование.

Darktable группирует все эти задачи в модули. Некоторые из них видны при настройках по умолчанию и организованы в разделы: «**Базовые модули**», «**Тон**», «**Цветокоррекция**», «**Коррекция**» и «**Эффекты**».



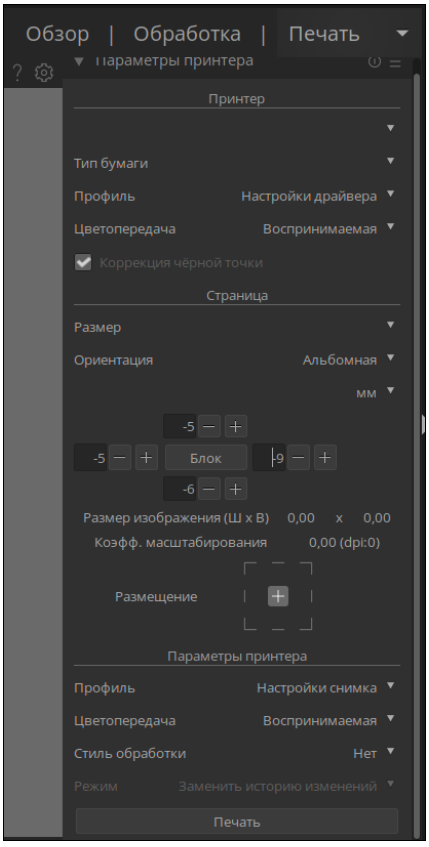
Отслеживание изменений

В левой части окна можно увидеть список изменений, внесенных в текущее изображение. В разделе «**История**» **Darktable** уже автоматически применил к фотографии несколько стандартных настроек. Но можно и отменить их, вернувшись к оригиналу. Также во время работы есть возможность создавать собственные промежуточные копии картинки, снапшоты.



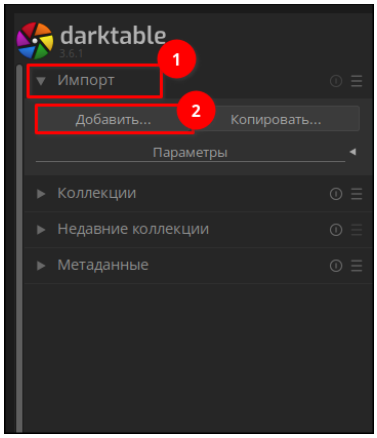
Использование функций печати

Эта функция дает возможность печатать изображение. Выберите принтер, установите размер бумаги, настройте цветовой профиль и прочие параметры. **Darktable** обеспечивает предварительный просмотр картинки, что позволяет увидеть ее расположение на листе бумаги.

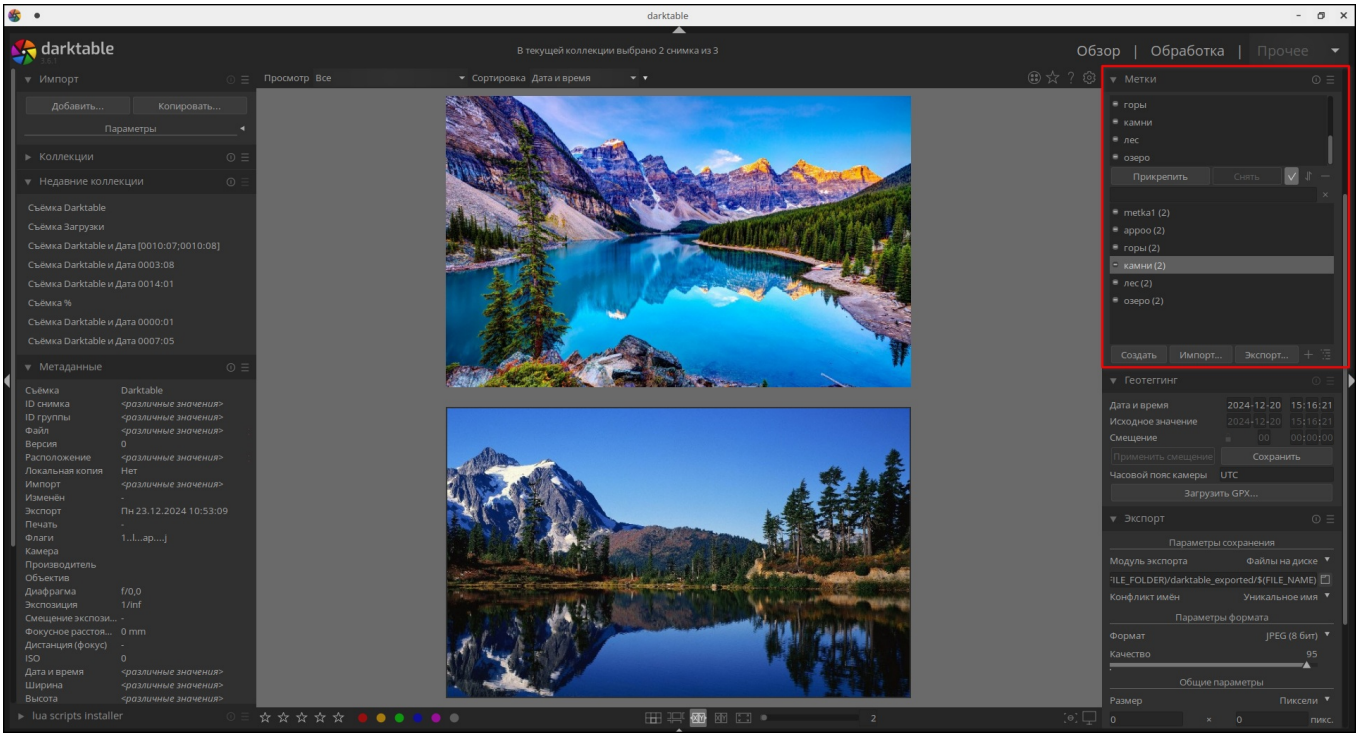


Пример работы

1. **Импорт**. Для импорта фотографии перейдите в режим Обзор — «**Импорт**» (1). Нажмите кнопку «**Добавить**» (2). Откроется меню импорта, в котором можно выбрать необходимые файлы и указать папку назначения.



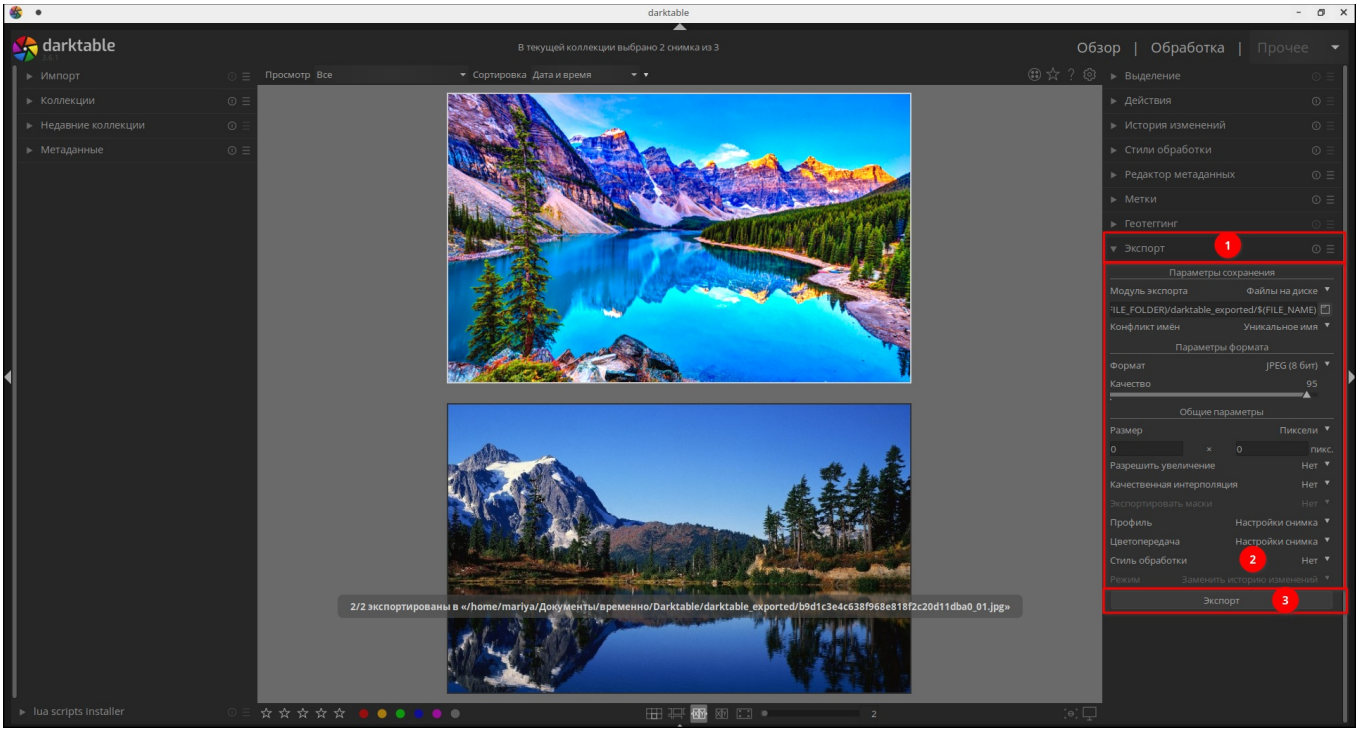
2. **Категоризация и отбор**. Просмотрите изображения, отметьте удачные/неудачные кадры, поставьте метки, рейтинги, ключевые слова. По рейтингам, меткам, ключевым словам в дальнейшем можно отбирать, искать и сортировать изображения. Данный шаг не является обязательным, но чем больше изображений импортировано, тем сложнее в них ориентироваться.



3. **Обработка**. Перейдите в режим Обработка. На этом шаге происходит конвертирование и редактирование изображения.



4 . **Экспорт**. Все изменения в **Darktable** сохраняются в базе данных приложения, а оригинальный файл изображения остаётся нетронутым. Необходимо выполнить экспорт таким образом, чтобы потом можно было загрузить файл в Интернет или открыть в другой графической программе. Экспорт изображений осуществляется в режиме Обзор, в разделе «**Экспорт**», расположенном на правой панели. Для осуществления экспорта необходимо выбрать параметры.



5 . **Печать**. Для отправки изображения на принтер перейдите в режим Печать, настройте параметры макета печати и выберите принтер.


darktable
Обзор | Обработка
Печать
1
2
Коллекции
Метаданные
Просмотр Все
Сортировка Дата и время
Параметры принтера
Принтер
HP_LaserJet_MFP_M426fdn
Тип бумаги
Unspecified
Профиль
Настройки драйвера
Цветопередача
Воспринимаемая
Коррекция чёрной точки
Страница
Размер
A4
Ориентация
Альбомная
мм
Блок
Размер изображения (Ш x В) 288,00 x 180,00
Коэфф. масштабирования 0,93 (dpi:300)
Размещение
Параметры принтера
Профиль
Настройки снимка
Цветопередача
Воспринимаемая
Стиль обработки
Нет
Режим
Заменить историю изменений
Печать

GUVCView — программа для работы с веб-камерами

Установка
Описание программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** guvcview-2.0.6-1

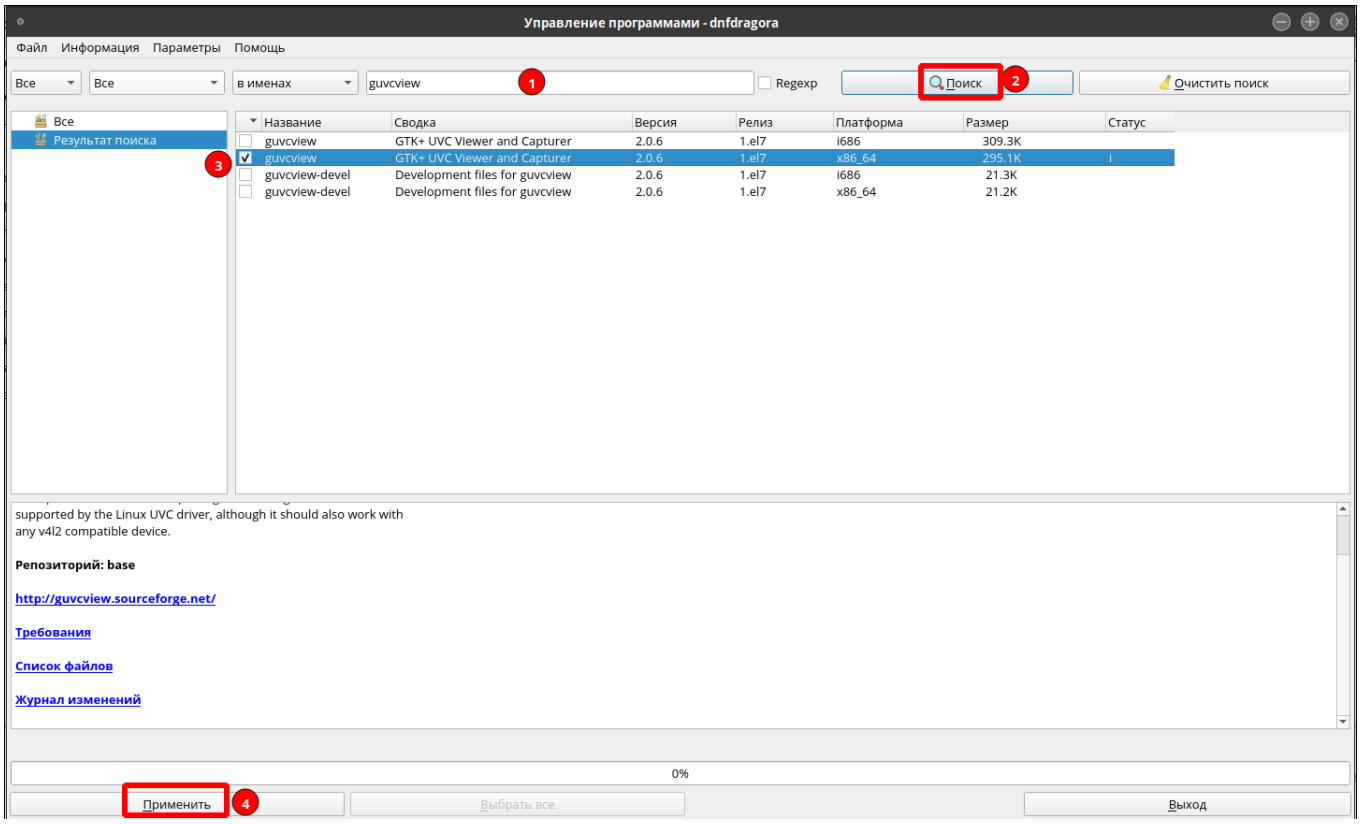
Guvcview (GTK + UVC Viewer) — программа для работы с веб-камерами, использующими протокол передачи видео UVC, выполняющая функции фотографирования и видеосъемки.

С помощью *guvcview* можно захватывать видео или изображения вместе со звуком.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**guvcview**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

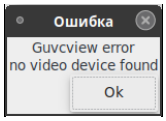
```
dnf install guvcview
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

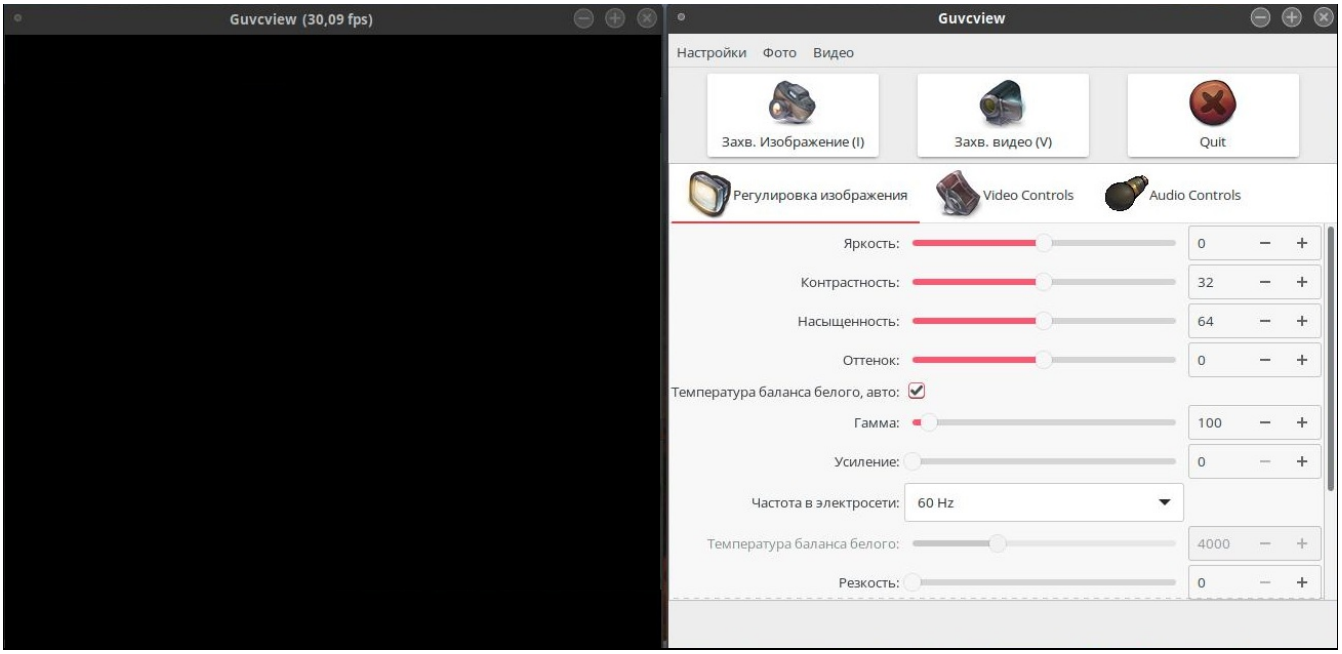
После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**Работа с веб-камерой**».

Описание программы

Если к машине не подключена ни одна веб-камера, будет выведено соответствующее сообщение, а программа не запустится.

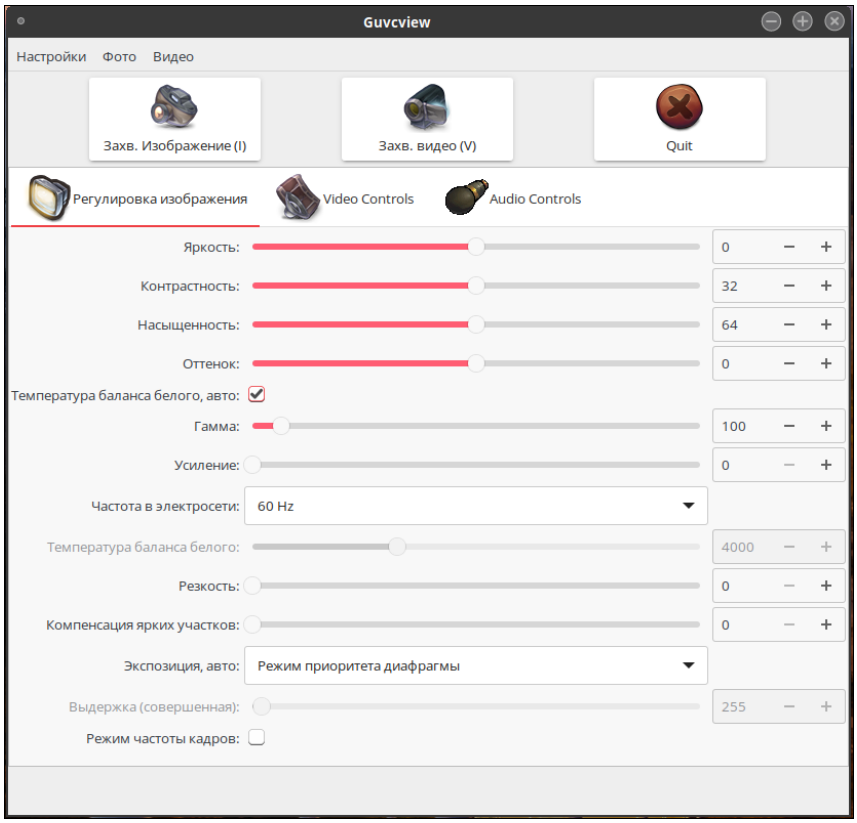


При успешном запуске программы с подключенным устройством появятся две формы. Первая форма содержит изображение с камеры, а на второй находятся настройки и элементы управления.



В настройках изображения (вкладка «**Регулировка изображения**») можно регулировать:

- яркость;
- контрастность;
- насыщенность;
- оттенок;
- гамму;
- усиление;
- частоту электросети;
- температуру баланса белого;
- резкость;
- компенсацию ярких участков;
- экспозицию;
- выдержку (если поддерживается).

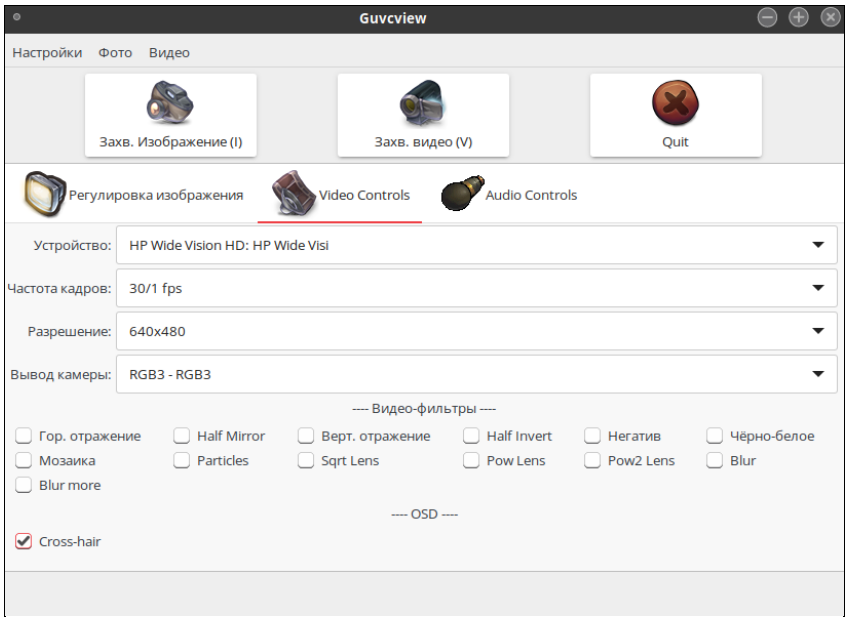


В настройках видео (вкладка «**Video Controls**») можно выбрать и установить:

- устройство;
- частоту кадров;
- разрешение;
- вывод камеры.

Также в программе к съемке можно применять видео-фильтры:

- горизонтальное отражение;
- Half Mirror;
- вертикальное отражение;
- Half Invert;
- негатив;
- черно-белое;
- мозаика;
- Particles;
- Sqrt Lens;
- Pow Lens;
- Pow2 Lens;
- Blur;
- Blur more.

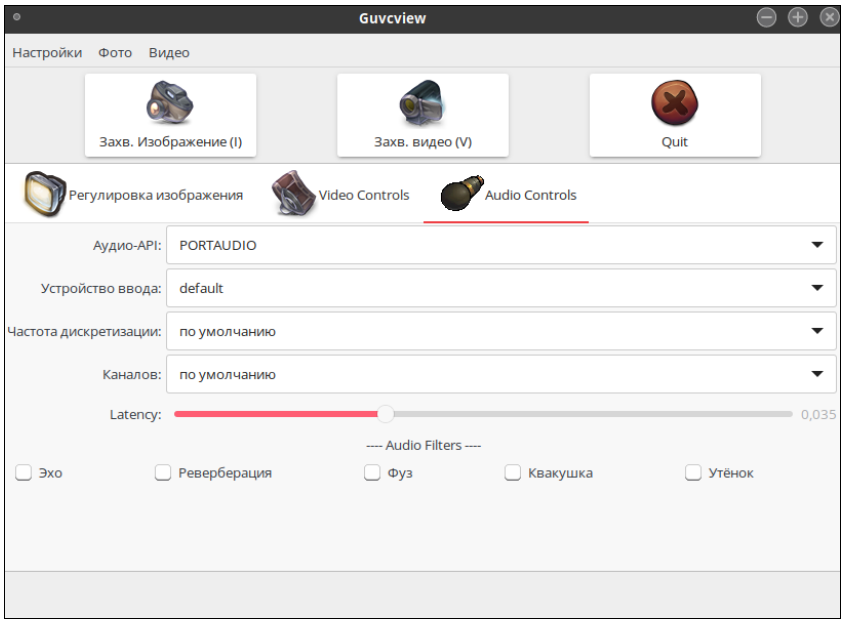


В настройках микрофона (вкладка «**Audio Controls**») можно изменить:

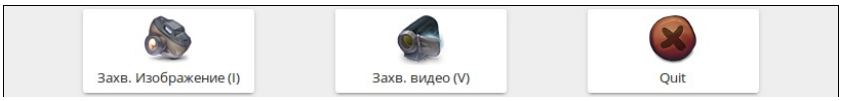
- аудио-API (PORTAUDIO,PULSEAUDIO);
- устройство;
- частоту дискретизации;
- количество каналов;
- задержку (latency).

Также к звуку можно применить аудио-фильтры:

- эхо;
- реверберация;
- фуз;
- квакушка;
- утенок.



В верхней части интерфейса располагаются три кнопки управления: «**Захват изображения**», «**Захват видео**» и «**Выход**». Произвести запуск фотосъемки и видеосъемки можно клавишами «**I**» и «**V**».



В *guvcview* можно сохранить профиль и загрузить уже готовый. Для этого перейдите в пункт меню « **Настройки**» — «**Сохранить профиль**» / «**Загрузить профиль**».

В пункте меню «**Фото**» — «**Файл**» можно выбрать путь и формат (*raw*, *jpeg*, *png*, *bmp*) сохранения фото.

В пункте меню «**Видео**» — «**Файл**» можно выбрать путь и формат (*mkv*, *webm*, *avi*) сохранения видео-файлов.

В «**Видео**» также можно выбрать видео/аудио кодеки и изменить их свойства.

Поддерживаемые видео-кодеки:

- *Raw camera input*;
- *MJPG*;
- *MPEG*;
- *FLV1*;
- *WMV1*;
- *MPG2*;
- *MS MP4 V3*;
- *MPEG4-ASP*;
- *MPEG4-AVC* (H264);
- *HEVC* (H265);
- *VP8*;
- *VP9*;
- *Theora*.

Поддерживаемые аудио-кодеки:

- *PCM*;
- *MP2*;
- *MP3*;
- *AC-3*;
- *AAC*;
- *Vorbis*.

Synfig Studio — создание векторной анимации

Установка
Описание программы
Первоначальная настройка
Работа в программе
Функция связывания
Движение
Шкала времени
Ключевые кадры
Просмотр анимации
Рендеринг

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** synfigstudio-1.4.0-1

Synfig Studio — это свободное программное обеспечение для создания векторной 2D анимации.

Анимация — это быстрый показ последовательности изображений, создающий иллюзию движения. Традиционно 2D анимация создавалась путём рисования каждого изображения отдельно. Такие изображения называются «кадры» (также используется термин «фреймы»), а сам этот метод называется «покадровая анимация». Но создание иллюзии "живого" движения требует большого количества кадров (обычно 24 кадра в секунду), поэтому метод покадровой анимации очень медленный и требует много времени и ресурсов.

Synfig Studio использует две технологии создания кадров:

- *Morphing animation* — морфинг;
- *Cutout animation* — перекладная анимация.

Морфинг создаёт плавный переход между двумя изображениями, это достигается путём преобразования одной формы в другую, часто с использованием специальных точек-фиксаторов. Для векторных изображений *Synfig Studio* делает эти переходы автоматически, анимация создаётся просто подстановкой изображения в ключевых позициях, находящихся на сравнительно больших промежутках времени. Художник создаёт столько кадров, сколько необходимо, чтобы получить основу движения анимационной сцены, о создании промежуточных кадров позаботится *Synfig*.

Перекладная анимация заключается в разделении объекта на составные части и простого их изменения (например, перемещения, вращения и изменения размера) в разных позициях времени анимации. *Synfig Studio* использует эти позиции и создаёт плавные переходы между каждой из них. Перекладная анимация может быть создана с использованием как растровых, так и векторных изображений.

В обоих случаях задачей *Synfig Studio* является заполнить пробелы между так называемыми "ключевыми кадрами", чтобы получилась плавная анимация. Этот процесс называется "фазовка" или "твининг" (*tweening*), хотя фазовка — не единственное достоинство *Synfig Studio*.

Вы можете подробнее ознакомиться с работой в Synfig Studio, просмотрев наши обучающие видео:

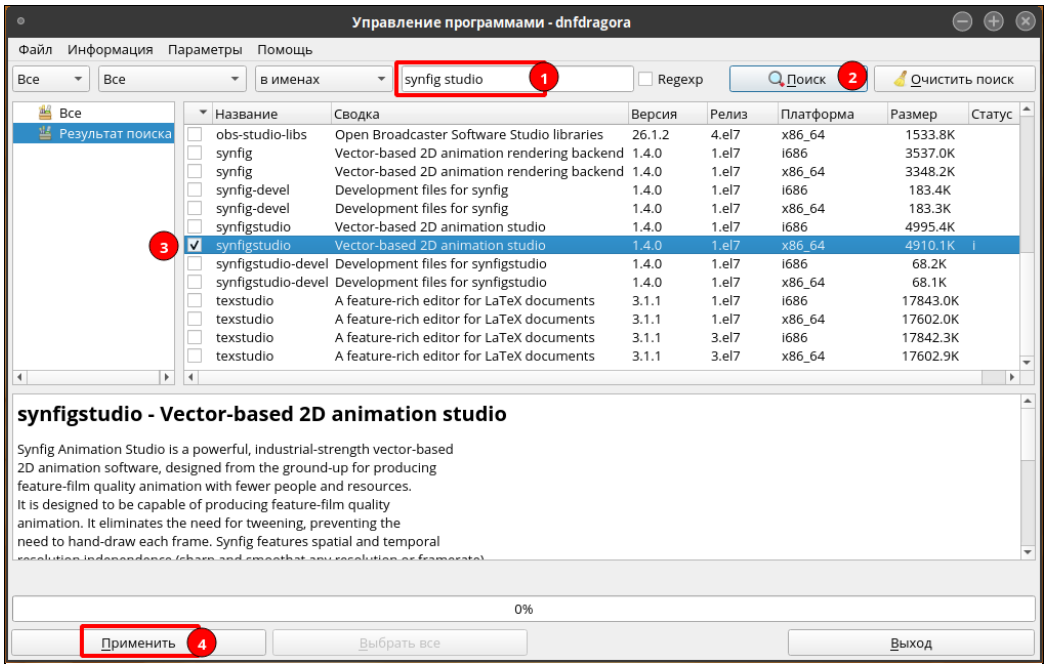
- на **RuTube** — Создание анимации с помощью Synfig Studio;
- в **Яндекс.Дзен** — Создание анимации с помощью Synfig Studio;
- в **VK Видео** — Создание анимации с помощью Synfig Studio.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**synfig studio**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

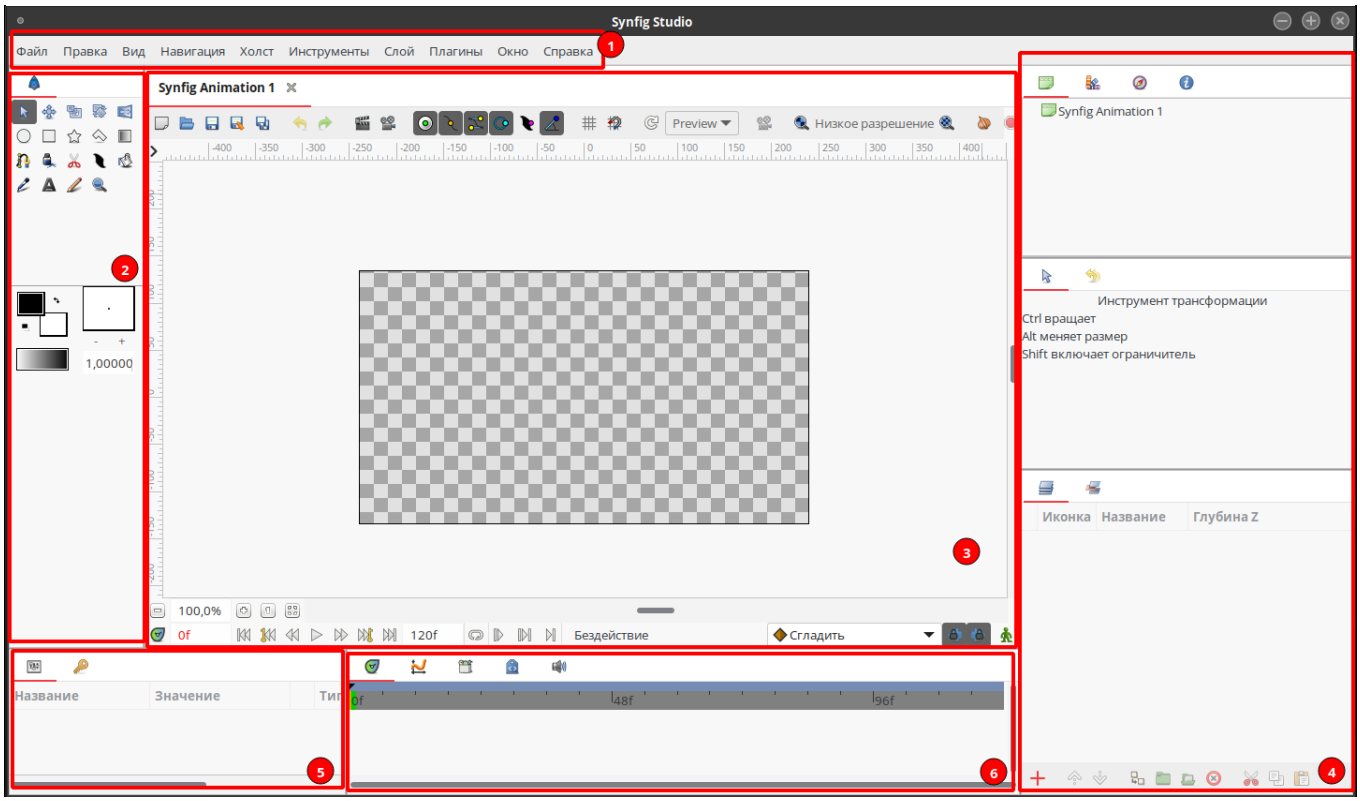
```
dnf install synfigstudio
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**Редактор 2D анимации Synfig Studio**».

Описание программы

Окно программы выглядит следующим образом:



1. *Основное меню программы* — здесь доступны настройки программы и действия для работы над проектом.

2. *Панель инструментов* — основные действия над проектом: открытие файлы, выбор инструменты, изменение цвета и т.д.

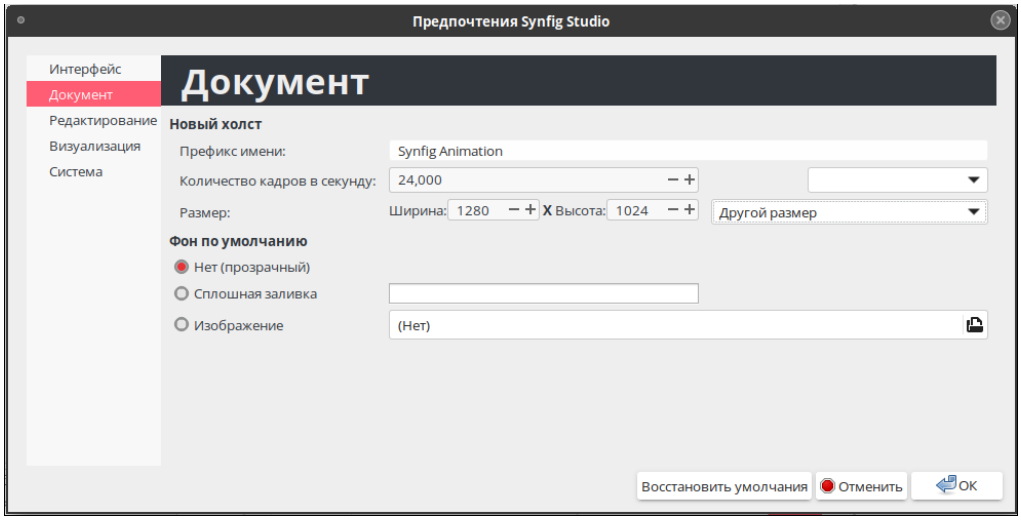
3. *Холст* — рабочая область программы, где создается анимация.

4. Панели *Навигатор*, *Параметры инструментов* и *Слои* — используются для создания эффектов будущей анимации.

5. *Панель параметров и отслеживания времени* — здесь можно найти подробные параметры и настройки для активного элемента, такие как цвет, ширина, непрозрачность, местоположение и т.д. Справа находится панель *Отслеживания времени*, которая позволяет создавать и изменять ключевые точки.

Первоначальная настройка

Для первоначальной настройки документа установите необходимый размер холста. Для этого перейдите в пункт меню **Правка** — **Настройки**, далее выберите раздел **Документ**.



В качестве примера размер холста будет установлен **1280x1024** пикс. Нажмите **OK** для применения изменений.

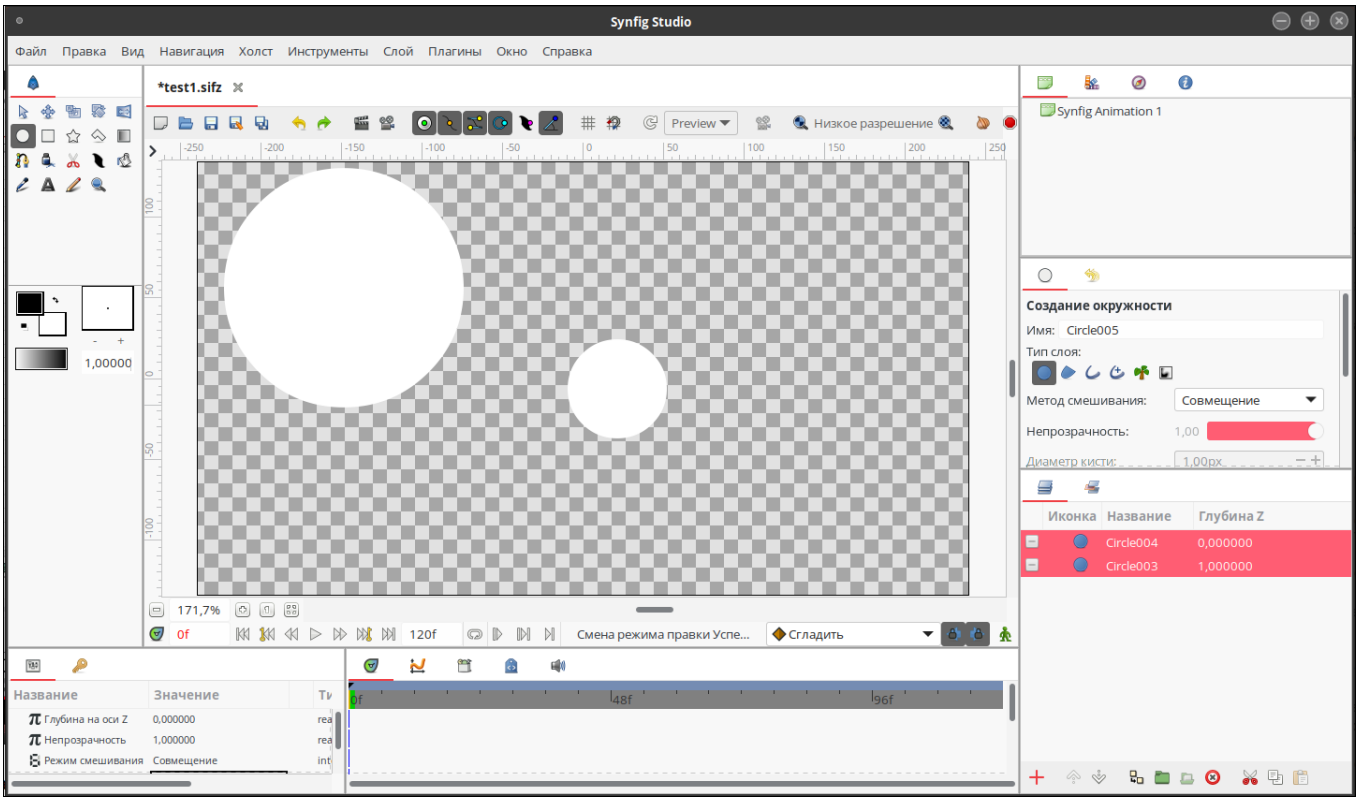
Для масштабирования холста нажмите и удерживайте клавишу **Ctrl** и вращайте колесо мыши. Масштабирование также доступно из пункта меню **Вид** — **Увеличить** / **Уменьшить** или использованием функции **Наилучшее заполнение**.

Для сохранения внесенных в проект изменений выберите пункт меню **Файл** — **Сохранить**. В окне сохранения необходимо ввести имя файла, затем нажать кнопку «**Сохранить**».

Работа в программе

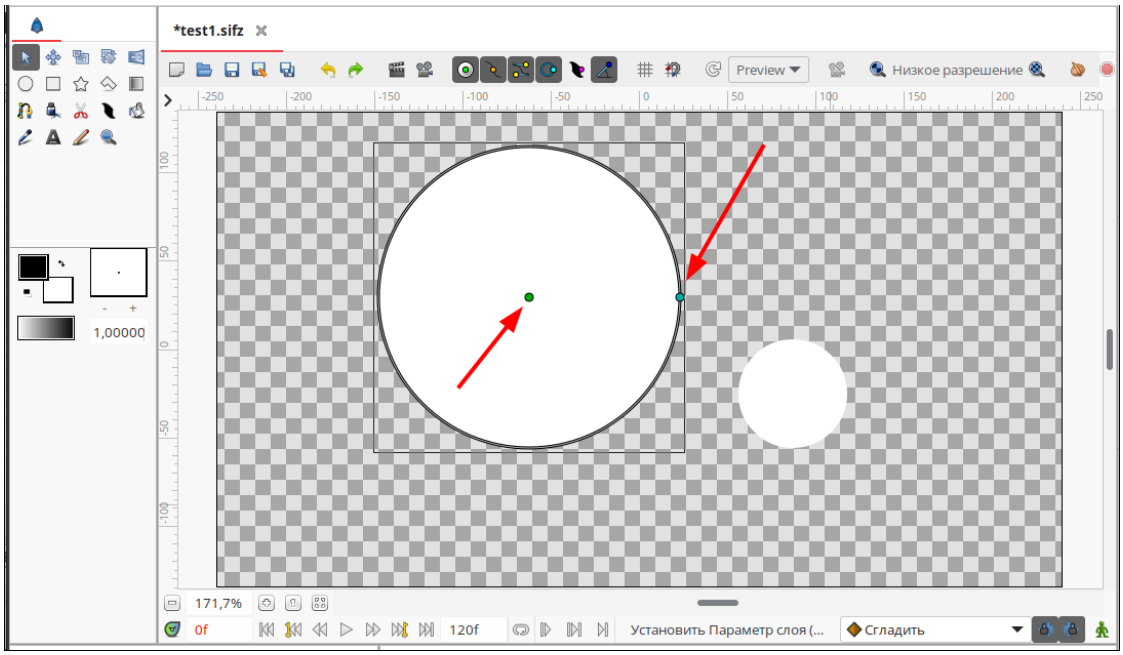
В *Synfig Studio* изначально включен «режим рисования», в котором создаются и изменяются изображения. Однако эти изменения не будут преобразованы в анимацию. В данном режиме объекты подготавливаются.

Для примера будут нарисованы два круга, для этого на *Панели инструментов* (**2**) выберите инструмент **Окружности**.



Для изменения размера фигуры или перемещения ее на холсте выберите **Инструмент трансформации** на *Панели инструментов*, щелкните по объекту и двигайте управляющие точки. Точка в центре фигуры — для перемещения, точка на границе фигуры — для изменения размера.

Если необходимо выделить несколько объектов, щелкайте по ним мышью, удерживая клавишу **Ctrl**.



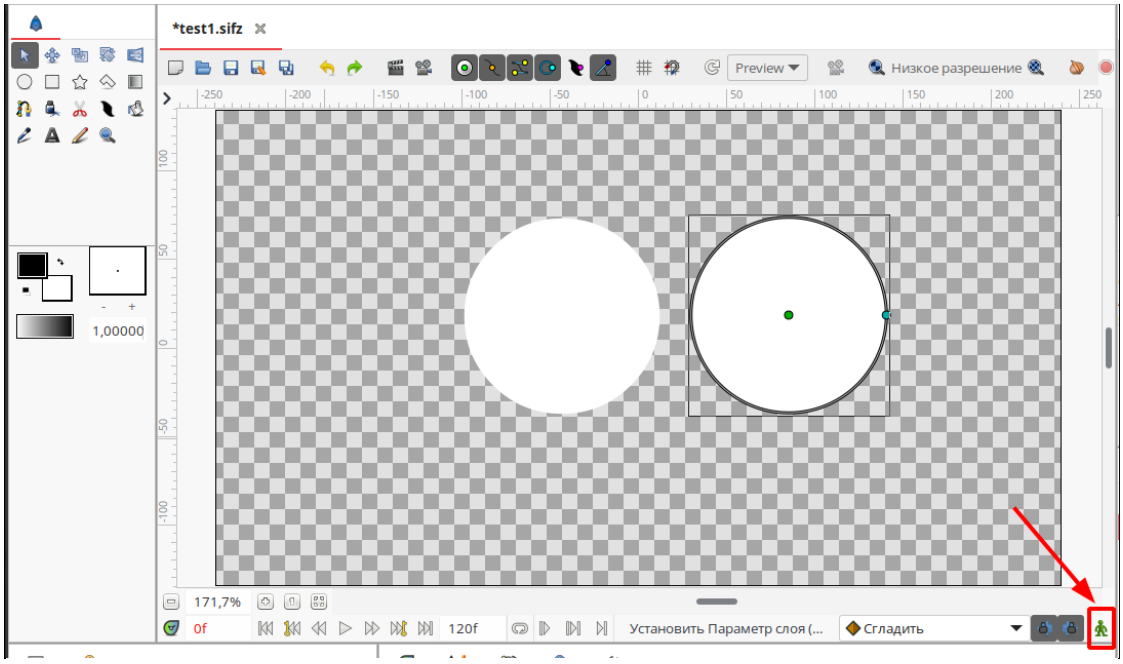
Функция связывания

Когда необходимо, чтобы у нескольких объектов был одинаковый размер, можно применить **функцию связывания**. Для этого выберите нужные объекты, выделите их точки радиуса (на границе фигуры), затем нажмите по любой из выделенных точек ПКМ и в контекстном меню выберите пункт «**Связь**». После этого точки радиуса фигур будут зависеть друг от друга — при изменении радиуса одной окружности автоматически будет изменяться радиус и у другой.

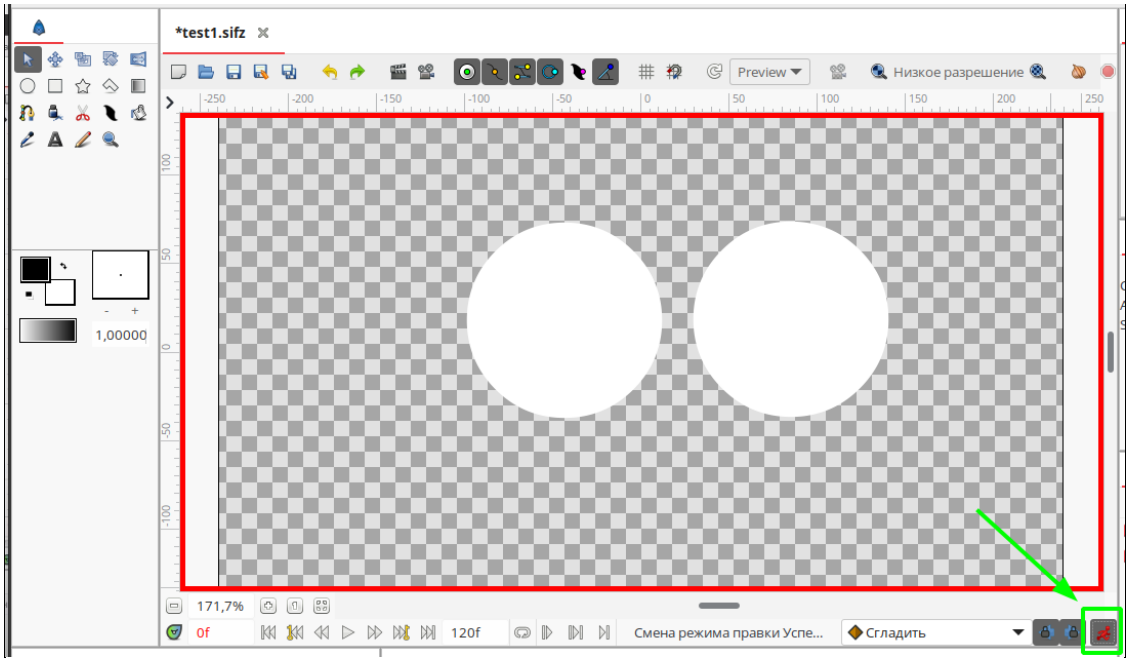
Связывание является фундаментальной концепцией *Synfig*. Вы можете создавать связи не только между управляющими точками, но и между параметрами.

Движение

Для того чтобы любые изменения объектов были обработаны как анимация, необходимо переключиться в соответствующий режим. Для этого в программе *Synfig Studio* предназначена зеленая кнопка «**Включить режим редактирования анимации**».



После нажатия на кнопку вокруг холста появляется красная рамка, а на кнопке переключения будет изображен красный человек. Для выхода из режима анимации достаточно еще раз нажать на эту же кнопку.



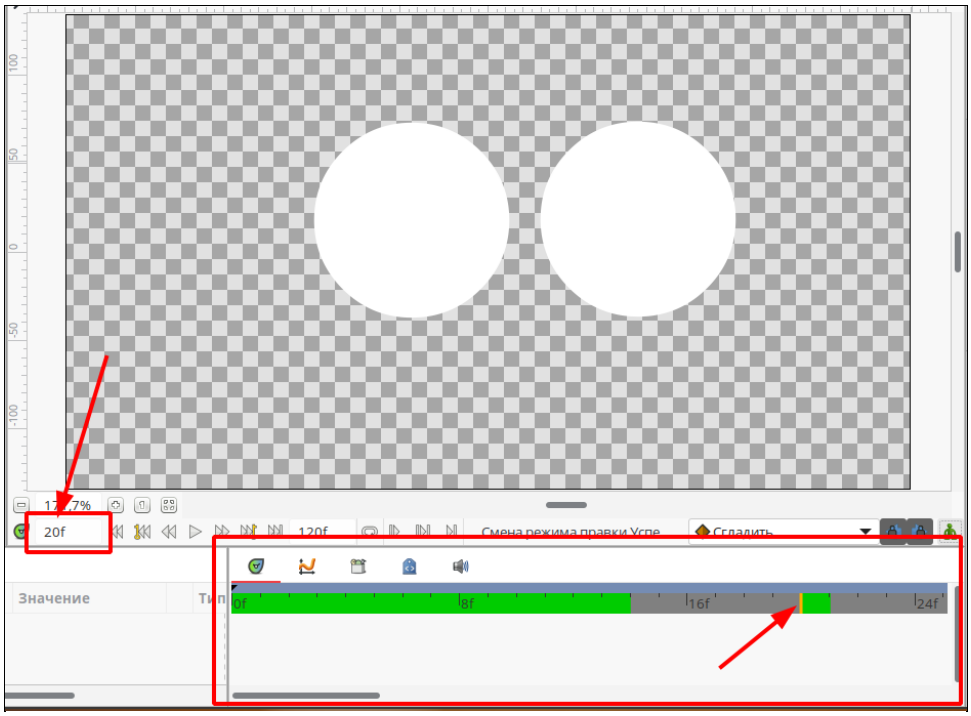
Шкала времени

Эффект анимации является результатом быстрой смены похожих изображений. Любые изменения протекают во времени, поэтому в *Synfig* предусмотрена панель «шкала времени». Похожая панель есть в большинстве программ для анимации, однако называться она может по-разному. Шкалу времени можно сравнить с кинолентой или фотопленкой, где в каждом кадре может быть запечатлено какое-нибудь изображение.

На шкале присутствуют деления, более крупные из которых помечены как **0f**, **24f**, **48f** и т.д.

F – это сокращение от *frame* (кадр), а **s** – от *second* (секунда).

В каждой секунде 24 кадра (задано «по-умолчанию», но вы можете изменить этот параметр в *Настройках*). Если щелкнуть в любом месте шкалы, то вы увидите линию, указывающую текущий кадр, также он будет указан в нижнем левом углу рабочей области.

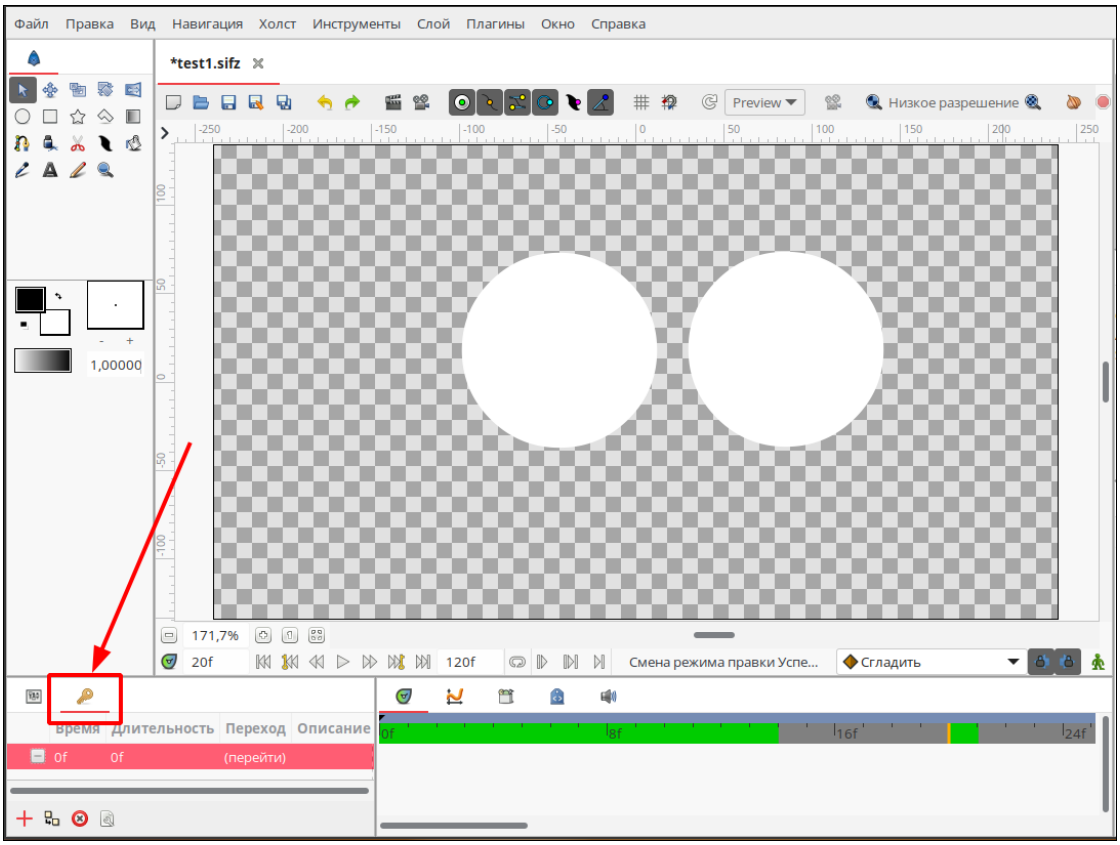


Ключевые кадры

Ключевой кадр — это изображение, на котором фиксируется положение объектов в определенный момент времени, поэтому необязательно прорисовывать каждый кадр. Достаточно указать программе начальное и конечное «состояние» объекта, все остальное программа попытается вычислить сама.

Начальное и конечное положение фиксируется в ключевых кадрах. Однако, в большинстве случаев, таких кадров бывает намного больше двух, т. к. при достаточно сложном изменении объекта программа не может корректно вычислить траекторию и характер изменения.

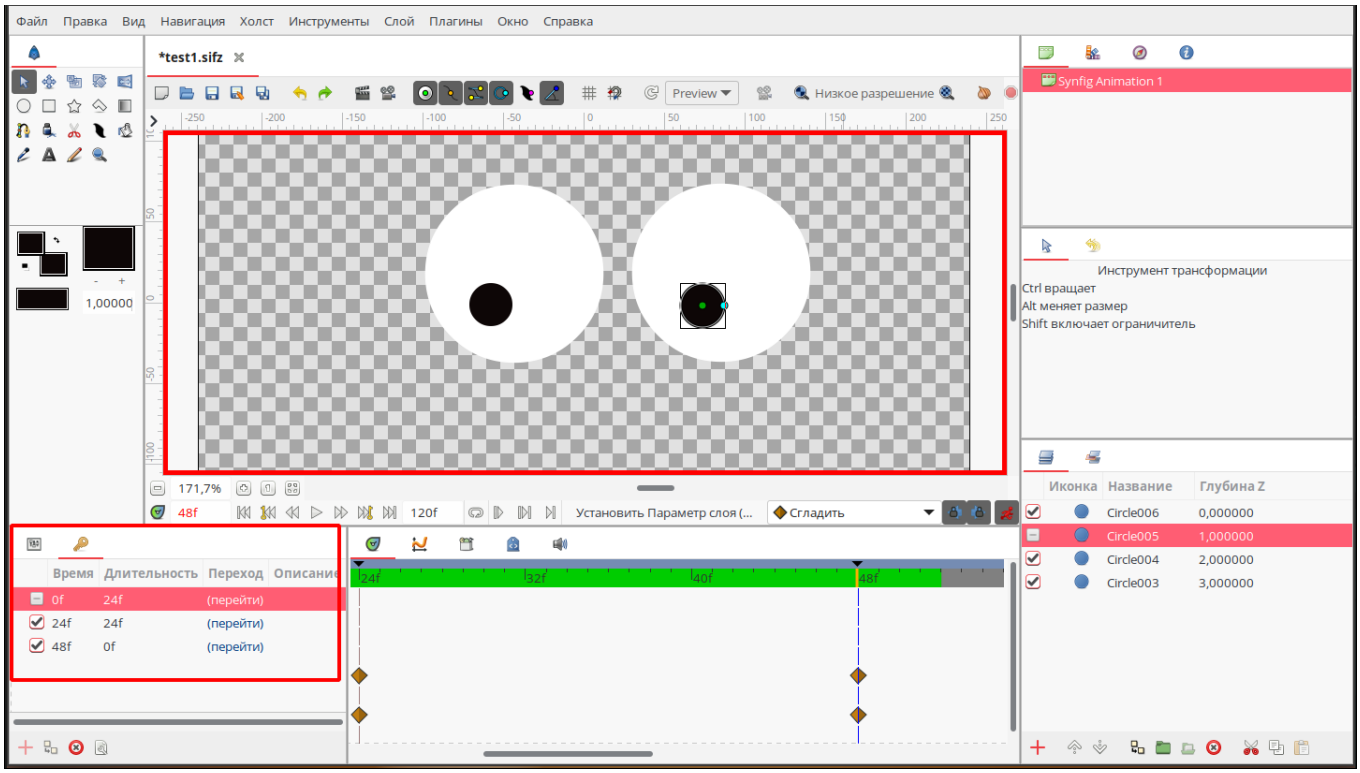
Для работы с ключевыми кадрами перейдите на *Панель параметров* (**5**) и откройте на вкладку с изображением ключа.



Здесь с помощью кнопки со знаком «+» можно добавлять ключевые кадры. В этих кадрах будет зафиксировано изменение фигуры, а в остальных — оно будет вычислено.

Перейдите на ползунке времени в позицию «**24f**» и измените положение фигуры. Добавьте ещё один ключевой кадр, щёлкнув на кнопку со знаком «**+**».

Повторите операцию для значения «**48f**» на шкале времени, измените положение и, для примера, размер. Должно получиться три ключевых кадра.

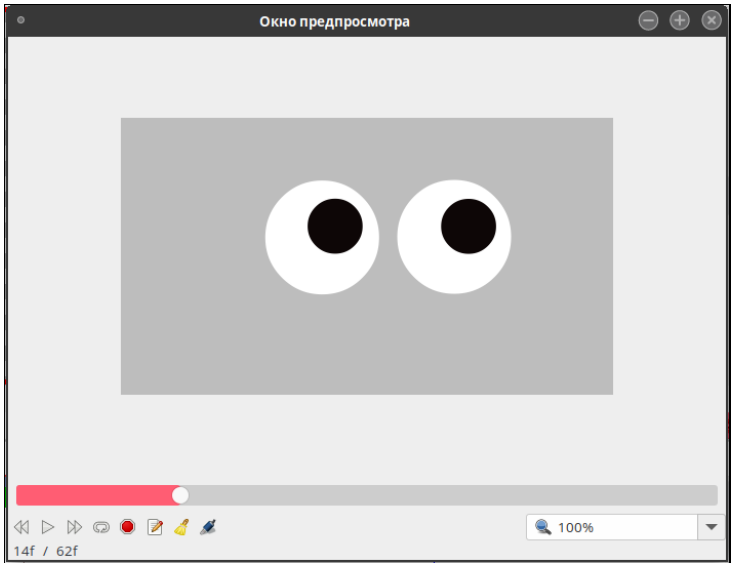


Благодаря позициям круга на различных ключевых кадрах, *Synfig* может понять, какое движение вы хотите получить (передвинуть круг, в частности), и дорисовать промежуточные изображения между этими состояниями. Каждое изображение будет составлять кадр вашей анимации, и, в конечном итоге, круг будет двигаться.

Просмотр анимации

Просмотреть созданную анимацию можно несколькими способами:

- зажав левую кнопку мыши и передвигая ею по шкале времени;
- нажав кнопку «**Воспроизвести**» в рабочей области ();
- воспользовавшись функцией предварительного просмотра (**Файл** — **Предварительный просмотр**).



Рендеринг

Для того чтобы сохранить файл, достаточно выполнить стандартную операцию сохранения. При этом будет сохранен файл в формате программы *Synfig*; другими словами, будут сохранены данные, описывающие определенным способом объекты и их изменения.

Чтобы получить изображение, необходима специальная программа (ее включают многие графические процессоры, в том числе и *Synfig Studio*), осуществляющая преобразование, в данном случае, векторного изображения в растровое. Процесс получения изображения называется **рендерингом** (от англ. *rendering*). Можно сказать, что во время этого процесса происходит визуализация изображения.

Однако требуется сохранить не простой рисунок, а анимацию (множество изображений). Она может храниться во многих форматах (видеоформатах и формате flash-анимации), в том числе и одном графическом — **GIF**. В нем и будет сохранена созданная анимация.

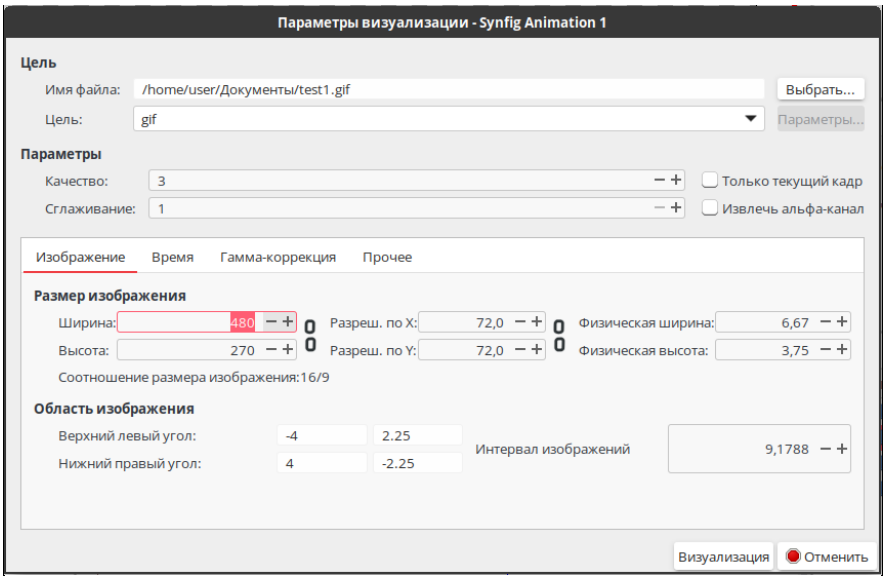
Для того чтобы вызвать окно рендеринга в *Synfig Studio*, необходимо выбрать пункт меню **Файл** — **Визуализация**. Откроется соответствующее диалоговое окно.

Поле **Имя файла** указывается место сохранения и имя файла (с расширением); кнопка «**Выбрать...**» вызывает диалоговое окно выбора папки.

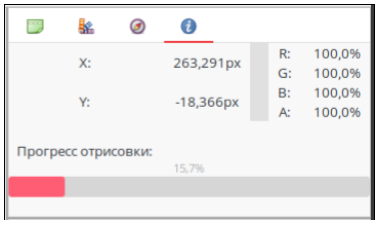
Выпадающий список «**Цель**» позволяет выбрать формат публикации. Выберите «**gif**».

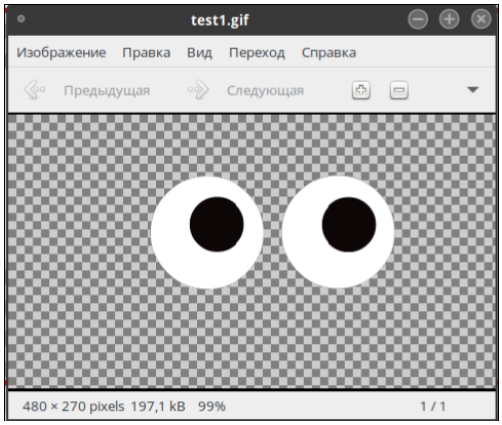
Вкладка «**Изображение**» управляет размерами и некоторыми другими параметрами изображения.

На вкладке «**Время**» можно настроить количество кадров в секунду, начало и окончание анимации.



Нажмите кнопку «**Визуализация**» для запуска процесса рендеринга, который может длиться от нескольких секунд до достаточно продолжительного времени (в зависимости от сложности анимации и мощности компьютера). Прогресс рендеринга можно увидеть во вкладке «**Инфо**» *Панели навигации*.





Imagination — программа для создания слайд-шоу

Установка
Описание программы
Работа в программе

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** imagination-3.6-3

Imagination - программа, позволяющая создавать слайд-шоу из изображений. *Imagination* имеет большое количество встроенных переходов, возможность добавления аудио в качестве музыкального сопровождения и создания подписей к изображениям.

Вы можете подробнее ознакомиться с созданием слайд-шоу в **Imagination**, просмотрев наши обучающие видео:

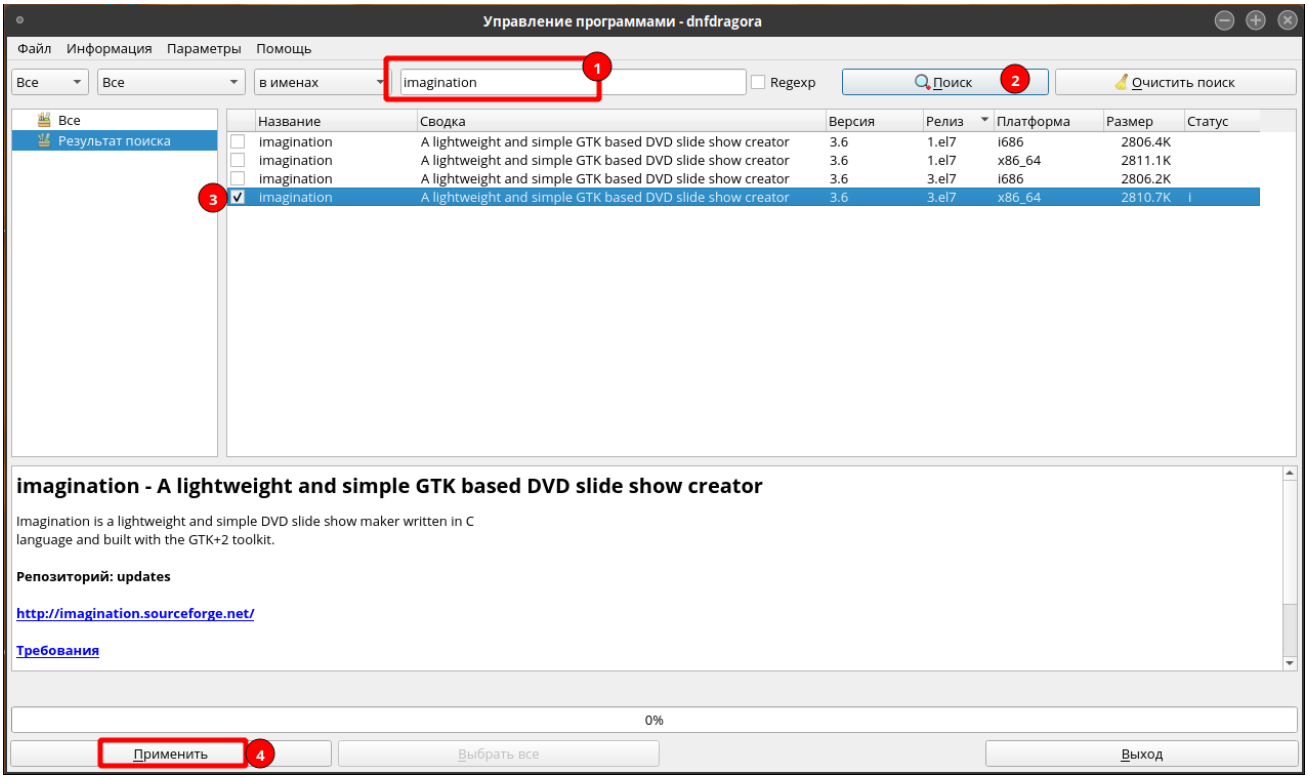
- на **RuTube** — Как сделать слайд шоу в РЕД ОС. Imagination;
- в **Яндекс.Дзен** — Как сделать слайд шоу в РЕД ОС. Imagination;
- в **VK Видео** — Как сделать слайд шоу в РЕД ОС. Imagination.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**imagination**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

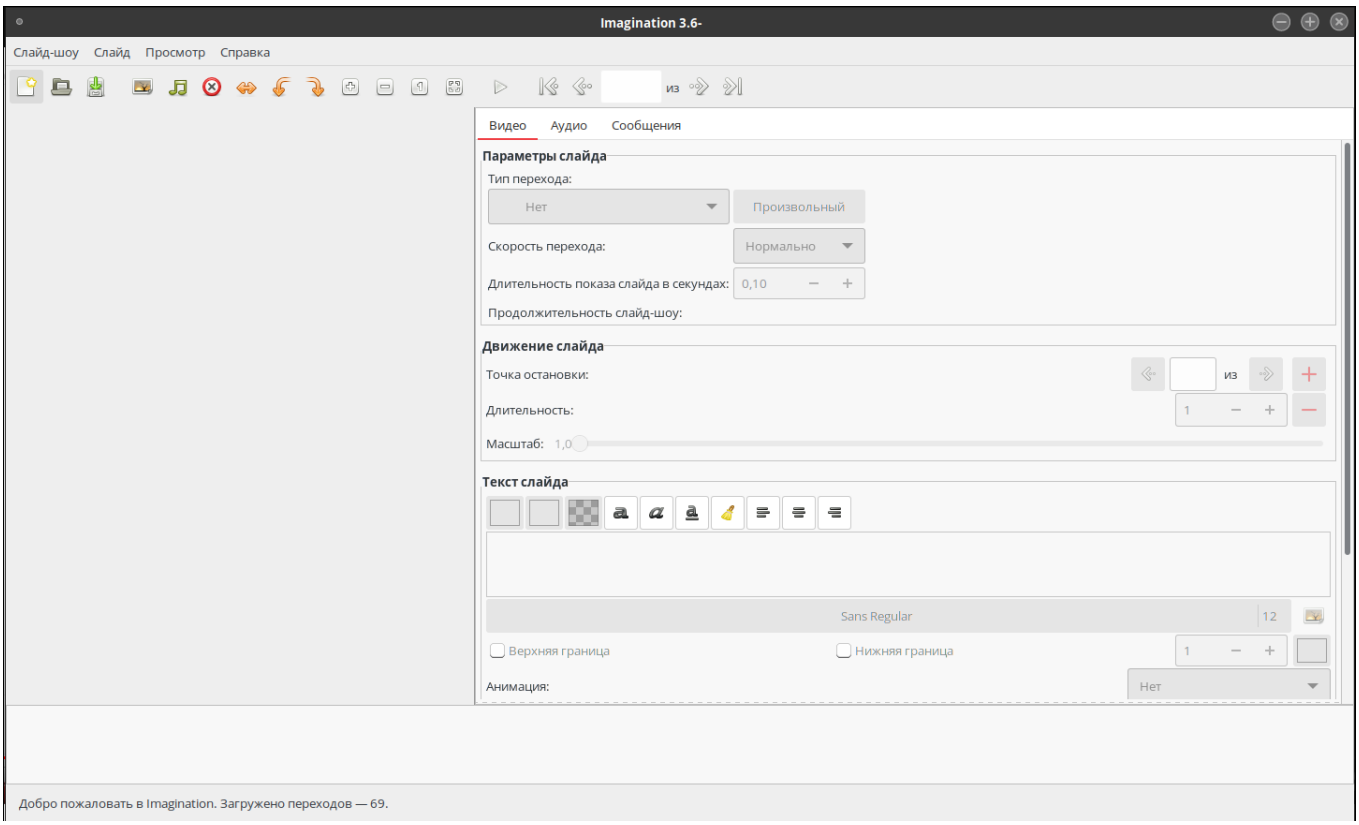
и выполните команду:

```
dnf install imagination
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

Описание программы

После установки программа будет доступна из «**Главного меню**» - «**Аудио и видео**» - «**Создание слайд-шоу**».



Вверху находится *основное меню* программы, в котором перечислены основные действия для слайд-шоу, действия для слайдов, а также параметры просмотра.

По умолчанию частота кадров предварительного просмотра составляет *15 кадров в секунду*, что дает эффект притормаживающей картинки, особенно это заметно при наложении эффектов переходов. Для большей плавности во время предварительного просмотра рекомендуется устанавливать максимальные значения количества кадров.

Ниже основного меню располагается *панель инструментов*, на которой доступны действия для создания и работы со слайд-шоу.



Кнопки панели инструментов:

1. Создание нового проекта слайд-шоу.

2. Открытие существующего проекта.

3. Сохранение проекта слайд-шоу.

4. Импорт изображений и музыкальных файлов (если они требуются для фона).

5. Удаление выбранного слайда.

6. Поворот по горизонтали.

7. Повороты влево/вправо на 90 градусов.

8. Размер слайдов в области предварительного просмотра.

9. Кнопки для навигации.

10. Кнопка воспроизведения/паузы.

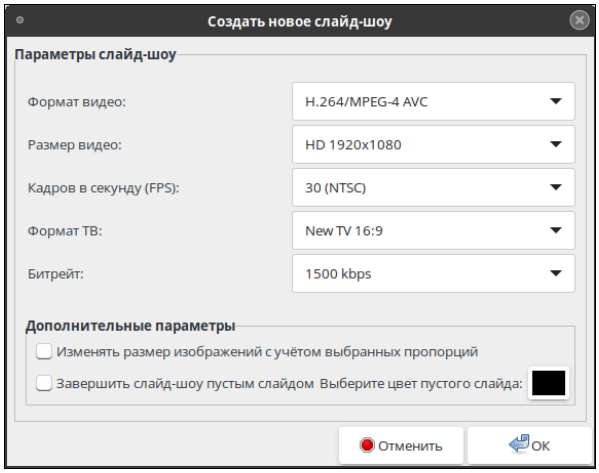
11. Кнопки перемещения по слайдам.

Ниже находится окно предварительного просмотра, его размер можно расширить.

Справа расположены настройки для видео, где есть возможность добавления переходов, движения, а также текста на слайды. В этом же окне есть вкладка для настройки добавляемых аудио-файлов.

Работа в программе

Для создания слайд-шоу выберите пункт меню «**Слайд-шоу**» - «**Новый**» либо нажмите на кнопку «**Создать новое слайд-шоу**» на панели инструментов. При этом будет выведено окно с настройками будущего слайд-шоу, в котором необходимо задать настройки формата видео, размера изображения, количества кадров в секунду и дополнительных параметров.

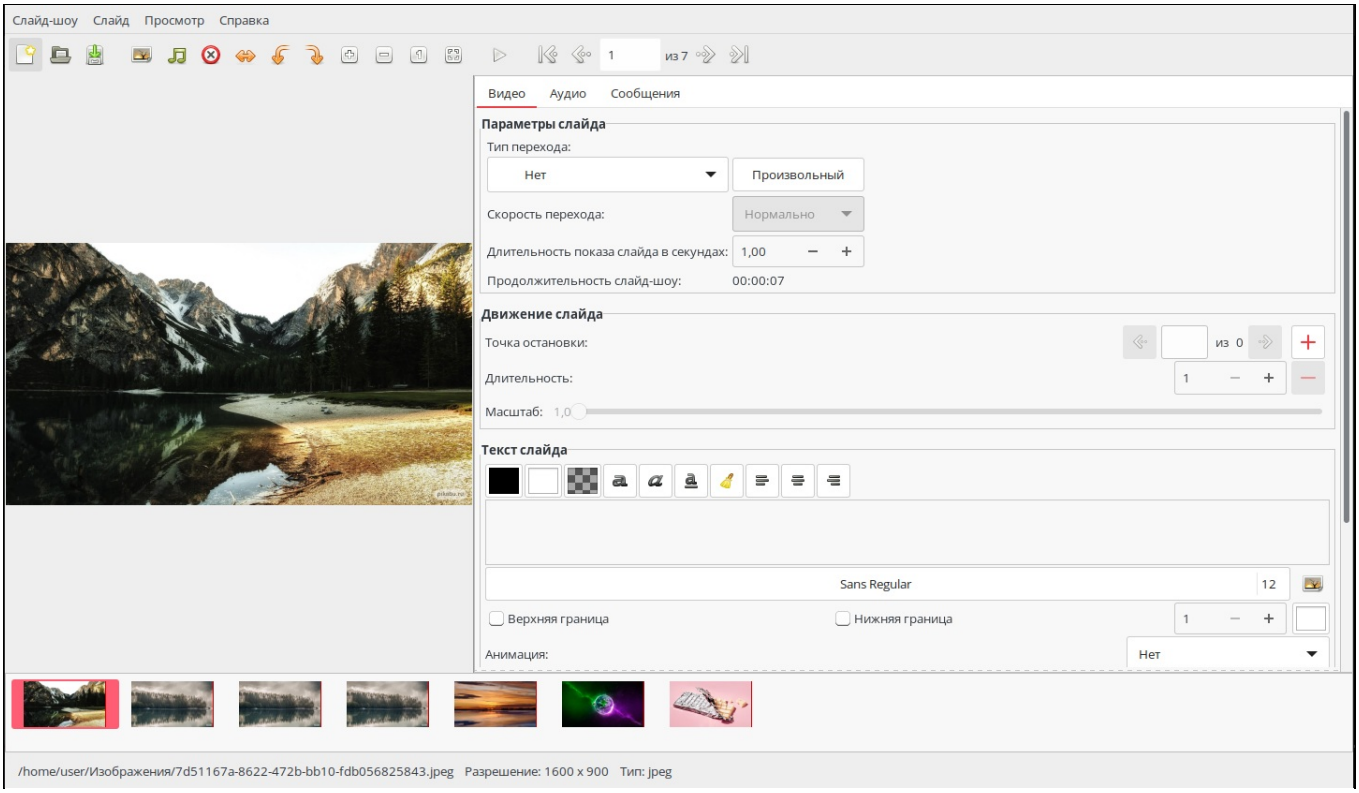


Для примера будут установлены обычные настройки. Также будет снят флаг с опции «**Изменять размер изображений с учетом выбранных пропорций**», чтобы оригинальные фото не были искажены.

Во втором пункте дополнительных настроек можно выбрать цвет для завершения слайд-шоу. Для сохранения настроек нажмите «**OK**».

После определения настроек необходимо импортировать изображения, для этого выберите в пункте меню «**Слайд-шоу**» - «**Импорт изображений**» или нажмите на кнопку «**Импорт изображений**» на панели инструментов.

Теперь слайды отображаются в нижней навигационной панели и по ним можно перемещаться.



Для добавления произвольных переходов выберите необходимый слайд, в параметрах слайда нажмите кнопку «**Произвольный**», программа случайным образом добавит произвольный переход. Также можно изменить скорость перехода и длительность показа выбранного слайда, при этом будет отображаться общая продолжительность слайд-шоу.

Для добавления текста на слайд предусмотрено много тонких настроек, в том числе и анимация появления. Внизу есть ползунки для точного позиционирования.

Для добавления фоновой музыки нажмите кнопку «**Импорт музыкального файла**» на панели инструментов, выберите аудио-файл и нажмите «**Открыть**». Все изменения производятся во вкладке «**Аудио**» окна настройки параметров слайда. Если добавлено несколько песен, то можно изменить их порядок с помощью клавиш  . В этом разделе также доступна регулировка длительности затухания - по умолчанию 5 секунд.

Незавершенный проект можно сохранить отдельным файлом для дальнейшего редактирования. Для этого в основном меню выберите «**Слайд-шоу**» - «**Сохранить как**», будет сохранен файл вашего проекта. Таким же образом вы сможете передать свой проект, чтобы его можно было доработать или изменить.

Когда проект полностью завершен, перейдите в пункт меню «**Слайд-шоу**» - «**Экспорт**», задайте имя файла и укажите место для его сохранения.

Создание диаграмм с помощью drawio

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** drawio-desktop-15.1.3-1

drawio - это бесплатная программа для создания и редактирования различных диаграмм и графиков. Данная программа является аналогом таких приложений как: *Microsoft Office Visio*, *Google Drawings*, *Dia*, *Lucidchart*, *yEd*.

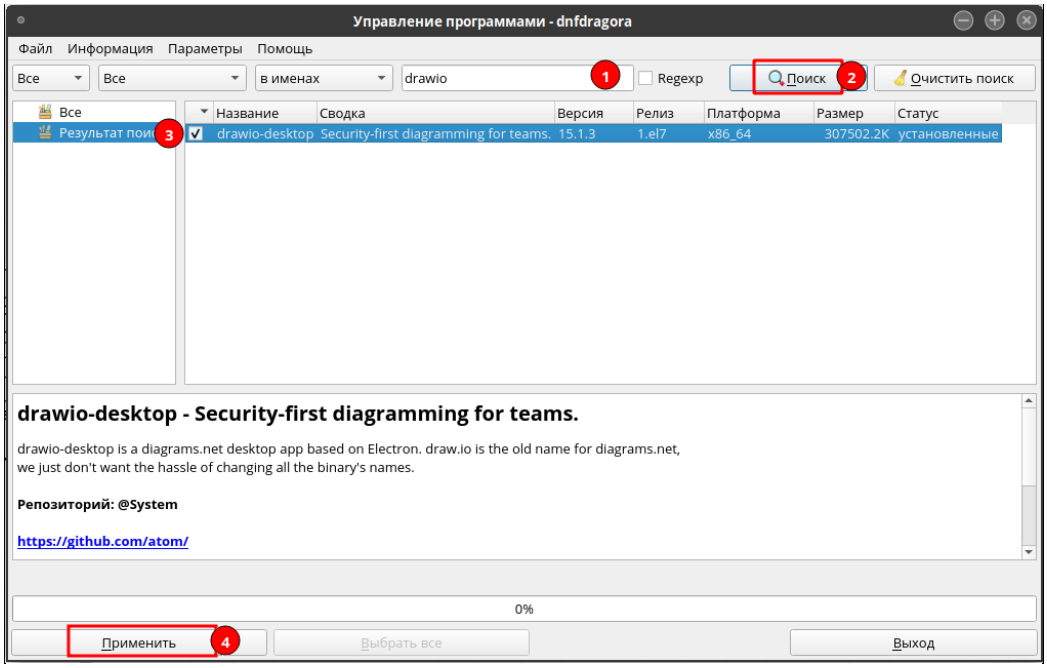
К её преимуществам можно отнести полностью бесплатную форму распространения, интуитивно понятный интерфейс, большое количество различных шаблонов, а также поддержку большого количества языков (в том числе русского).

Среди возможностей использования программы можно выделить создание различных блок-схем, графиков, UML-диаграмм, бизнес-диаграмм, диаграмм связей и инженерных схем. Существует возможность подключения шаблона по ссылке. Приложение имеет широкий спектр настройки оформления, а также добавление в избранное наиболее используемых элементов. Поддерживаемые расширения : **drawio**, **png**, **svg**, **html**, **xml**.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**drawio**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install drawio-desktop
```

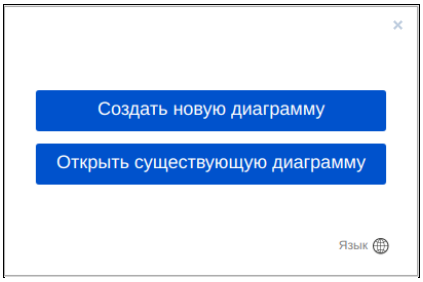
Дальнейшая работа в программе производится **с правами локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**drawio**».

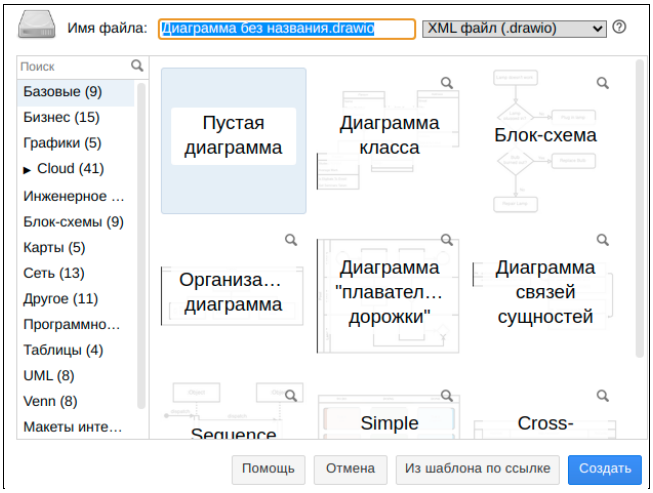
Описание программы

При запуске программы будет выведено сообщение с предложением обновить утилиту, на данном этапе нажмите «**Отменить**».

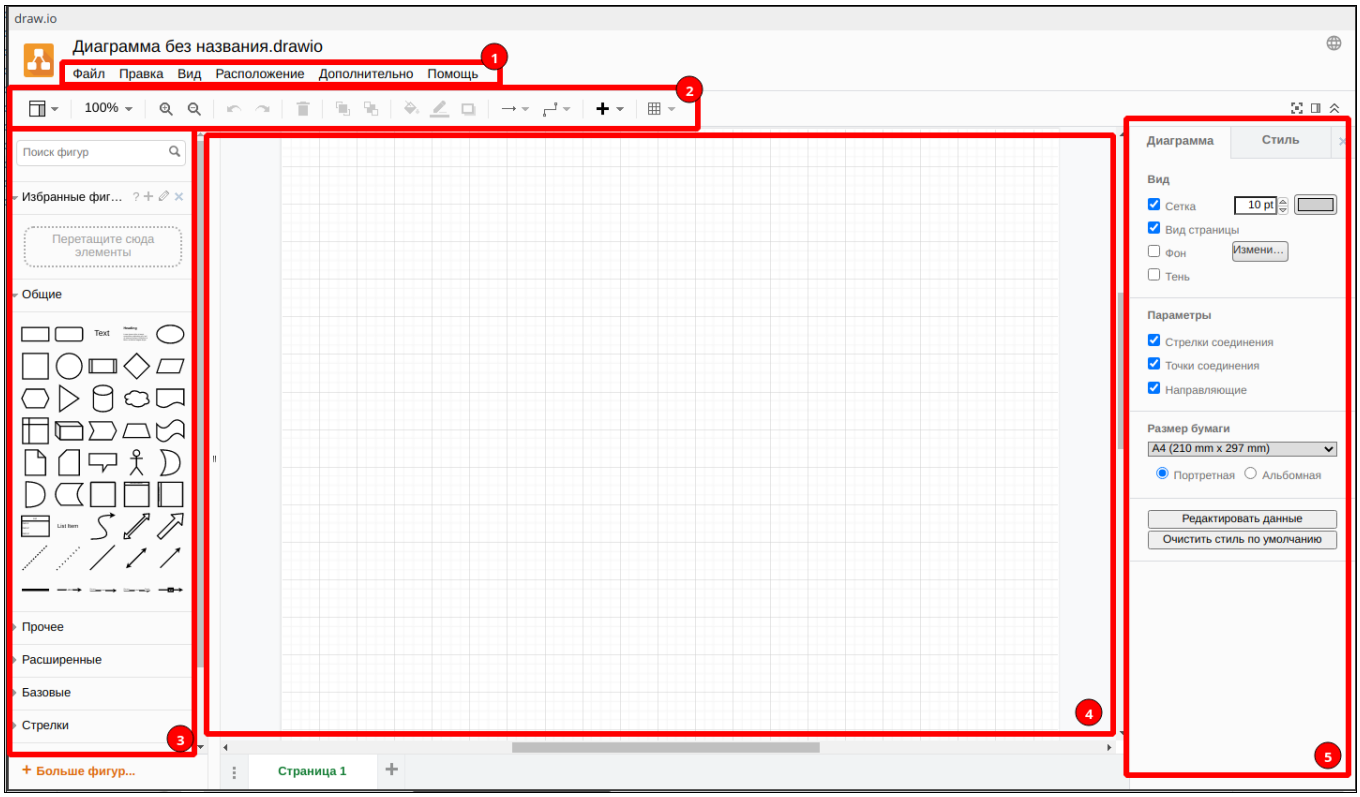
Далее появится меню с выбором действий — создать новую диаграмму или открыть существующую.



При выборе пункта «**Создать новую диаграмму**» будет открыта форма выбора имеющегося шаблона или шаблона по ссылке. Также в этом окне необходимо указать имя файла и выбрать его расширение.



Главное окно программы выглядит следующим образом:



1. Главное меню программы. Позволяет выполнять различные действия с создаваемым документом, а также настраивать программу и доступные панели.

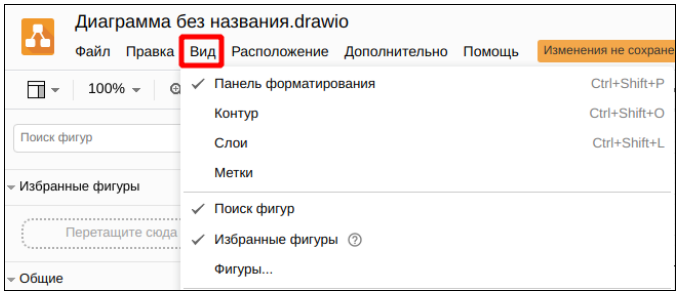
2. Панель инструментов для создания рисунков и диаграмм. На панели доступны быстрые действия для работы с элементами.

3. Сгруппированные элементы схем. Доступно добавление новых групп элементов.

4. Основная рабочая область для размещения элементов.

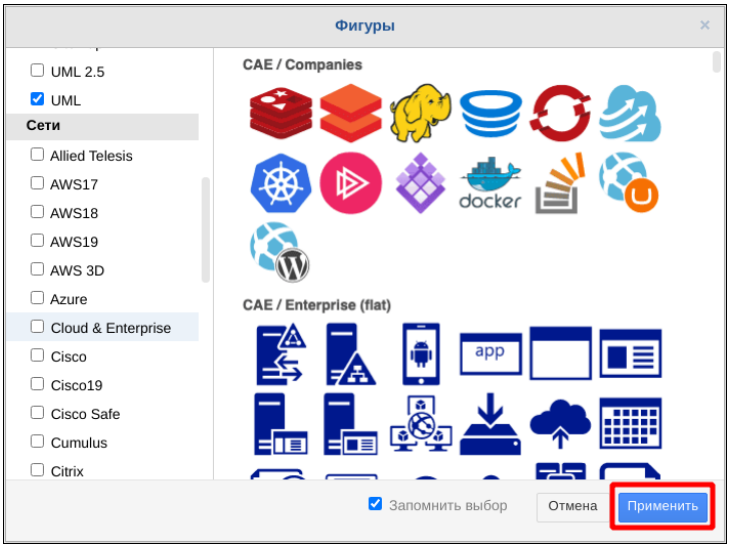
5. Панель настройки дизайна элементов. Все применяемые действия относятся к выделенному элементу.

Дополнительные панели можно настроить, открыв пункт меню «**Вид**».

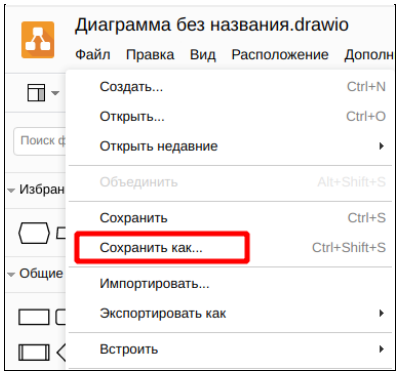


Для добавления часто используемого элемента в «**Избранные**» необходимо разместить фигуру в рабочей области, а затем перетащить её в поле «**Избранные фигуры**» на панели сгруппированных элементов схем (**3**).

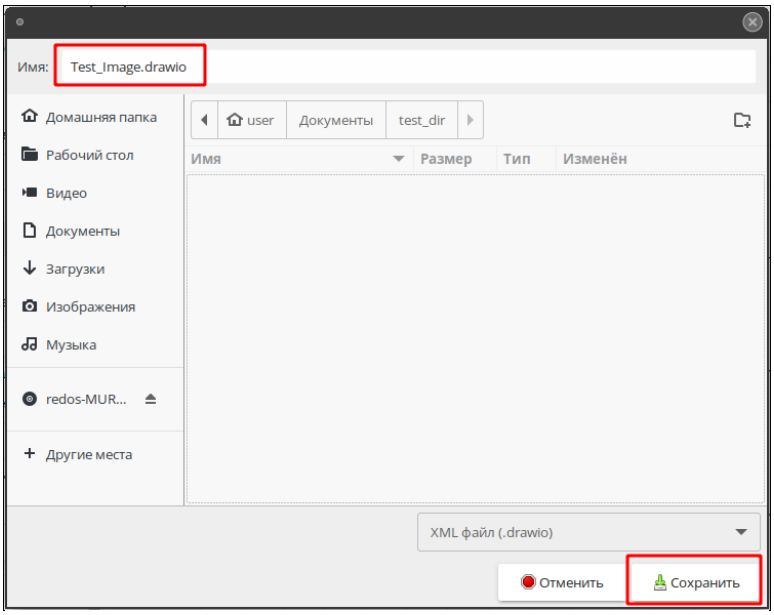
Если представленных элементов для работы будет недостаточно, все доступные фигуры можно просмотреть и добавить, нажав на кнопку « **+ Больше фигур**» или выбрав пункт меню «**Вид**» - «**Фигуры...**», после чего откроется окно для выбора групп элементов. Для добавления новой группы установите флаг рядом с необходимой группой и нажмите кнопку «**Применить**».



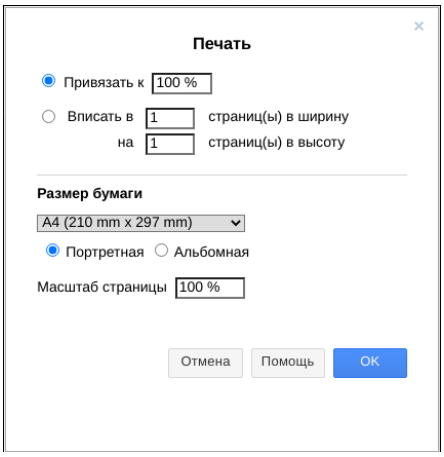
Для сохранения файла в определенном формате в главном меню выберите «**Файл**» - «**Сохранить как...**» или нажмите сочетания клавиш «**Ctrl+Shift+S**».



После этого откроется окно, в котором потребуется выбрать место сохранения файла и в поле «**Имя**» указать его название и формат.



Для печати созданного документа в главном меню программы выберите «**Файл**» - «**Печать...**» или нажмите сочетание клавиш «**Ctrl+P**».



KolourPaint — растровый графический редактор

Установка
Описание программы
Скриншоты
Эффекты изображения
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kolourpaint-17.12.1

KolourPaint — редактор растровой графики. **KolourPaint** подходит для использования в таких задачах, как:

- составление диаграмм и рисование,
- обработка изображений,
- создание и редактирование снимков экрана,
- редактирование иконок.

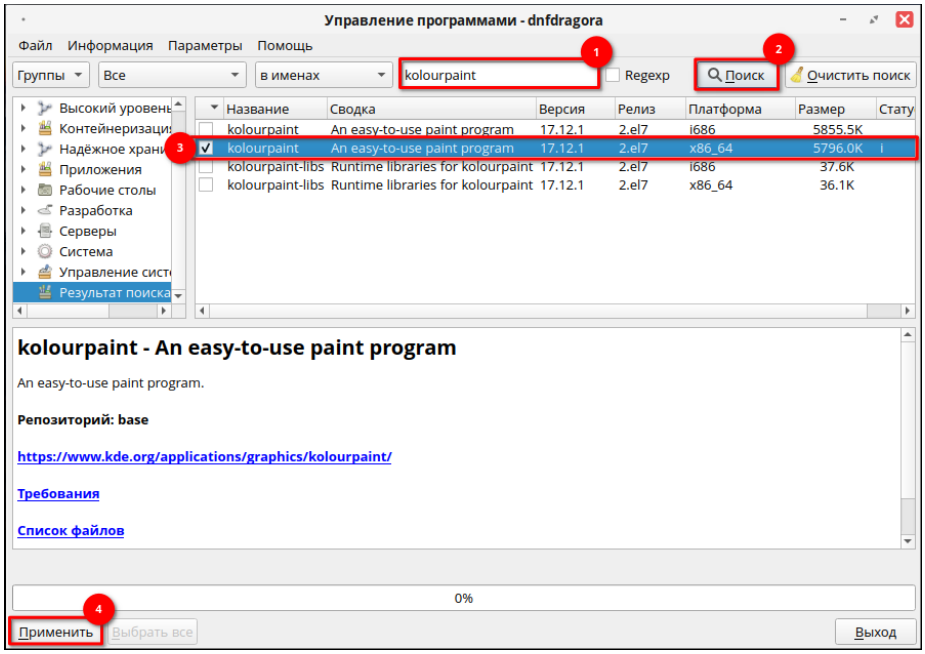
Редактор предоставляет широкий набор инструментов для рисования, включая кисти, карандаш, ластик, заливку, выделение и т. д. **KolourPaint** предлагает несколько шрифтов и параметров настройки, чтобы сделать текст более выразительным и соответствующим стилю рисунка.

KolourPaint также поддерживает работу с разными форматами файлов, включая PNG, JPEG, BMP, GIF и другие. Это позволяет пользователям импортировать и экспортировать свои рисунки в различных форматах, что облегчает их использование в других программах или публикацию в Интернете.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kolourpaint**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install kolourpaint
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Для просмотра сведений о версии введите команду:

```
kolourpaint --version
```

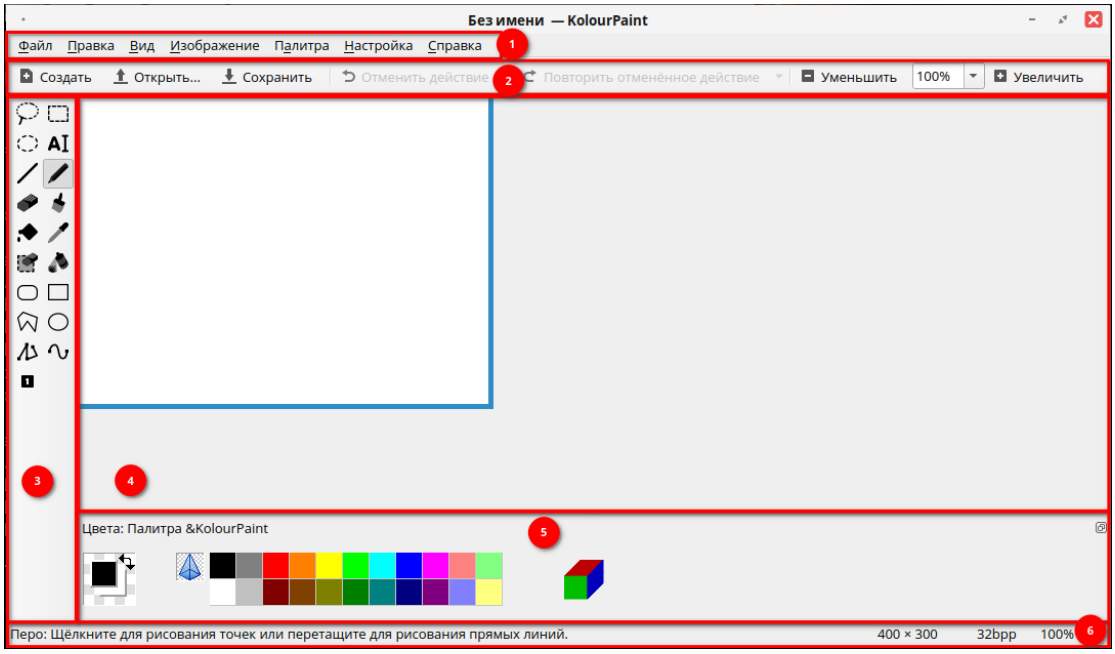
Для запуска программы через терминал введите команду:

```
kolourpaint
```

После установки программа будет доступна из «**Главного меню**» — «**Графика**» — «**KolourPaint**».

Описание программы

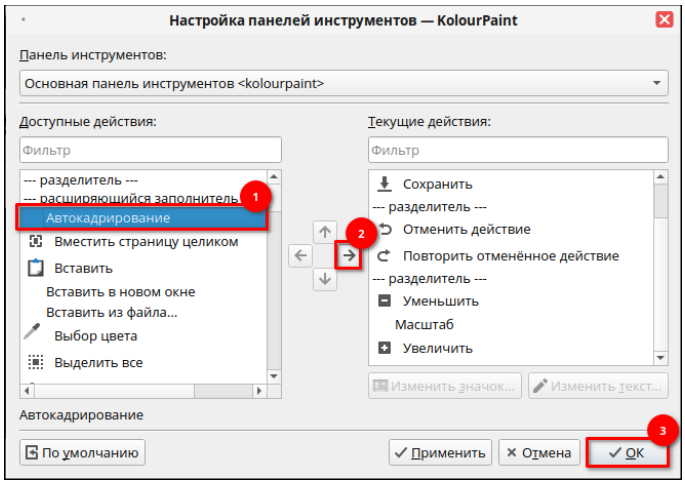
Интерфейс программы стандартный и состоит из нескольких типовых частей.



1 . **Основное меню программы** позволяет выполнять различные действия с изображениями, настраивать программу и панели инструментов.

2. **Основная панель инструментов** позволяет получить быстрый доступ к основным возможностям программы.

Для настройки панели инструментов перейдите в меню «**Настройка**» — «**Панели инструментов...**». В списке «**Доступные действия**» выберите инструмент, перетащите его в список «**Текущие действия**» с помощью стрелки  и нажмите «**OK**».



3 . **Боковая панель инструментов** — позволяет получить доступ к основным функциям рисования и редактирования изображений. Для быстрого выбора инструмента нажмите комбинацию клавиш, связанную с ним.

 **Свободное выделение (M)** — свободное выделение определённой области изображения.

 **Прямоугольное выделение (S)** — прямоугольное выделение определённой области изображения.

 **Эллиптическое выделение (I)** — эллиптическое выделение определённой области изображения.

 **Текст (T)** — добавление текста на изображение.

 **Линия (L)** — рисование прямых линий.

 **Перо (P)** — рисование свободных линий с перьевым наконечником.

 **Ластик (A)** — очистка части изображения.

 **Кисть (B)** — ЛКМ выполняет рисование основным цветом, ПКМ — позволяет рисовать цветом фона.

 **Заливка (F)** — заполнение выделенной области или закрытой формы выбранным цветом.

 **Выбор цвета (C)** — выбор цвета из изображения для использования с другими инструментами.

 **Очистка цвета (O)** — удаление определённого цвета из изображения.

 **Распылитель (Y)** — распыление краски с созданием текстурированного эффекта.

 **Округлённый прямоугольник (U)** — рисование прямоугольника с закруглёнными углами.

 **Прямоугольник (R)** — рисование прямоугольника.

 **Многоугольник (G)** — рисование многоугольника.

 **Эллипс (E)** — рисование эллипса.

 **Соединённые линии (N)** — рисование соединённых линий.

 **Кривая (V)** — рисование кривых Безье.

 **Масштаб (Z)** — приближение и отдаление изображения для более детальной работы.

Общие параметры инструментов:

Для выбора размера ластика нажмите на один из квадратов. Можно выбрать один из квадратов с длиной стороны 2, 3, 5, 9, 17 и 29 пикселей.



Параметр выбора ширины линии доступен для инструментов: кривая, эллипс, линия, многоугольник, прямоугольник и скруглённый прямоугольник. Для выбора ширины линии щёлкните по одной из линий. Доступна ширина линии в 1, 2, 3, 5 и 8 пикселей.



Настройка стиля заливки доступна для инструментов: эллипс, многоугольник, прямоугольник и прямоугольник со скруглением. Для выбора стиля заливки щелкните по одному из прямоугольников. К выбору доступны варианты: без заливки, заливка цветом фона или заливка цветом переднего плана.



4. **Рабочая область** — область для редактирования изображений.

5 . **Цветовая палитра** — панель для настройки цвета и прозрачности изображения. Цветовая палитра разделена на три секции:

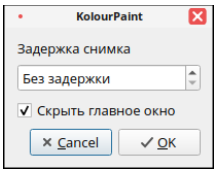
цветовая табличка, палитра и инструмент для настройки степени схожести цветов. Цветовая табличка показывает текущий основной цвет и цвет фона. При рисовании с использованием ЛКМ используется основной цвет, при использовании ПКМ — цвет фона. Чтобы поменять местами основной и фоновый цвета можно щёлкнуть по двунаправленной стрелке. Пирамида представляет прозрачный цвет.

6 . **Строка состояния** — это панель, расположенная внизу рабочей области, на которой отображаются подсказки по работе с инструментами. При выделении определённой области в строке состояния отобразятся размеры выделения.

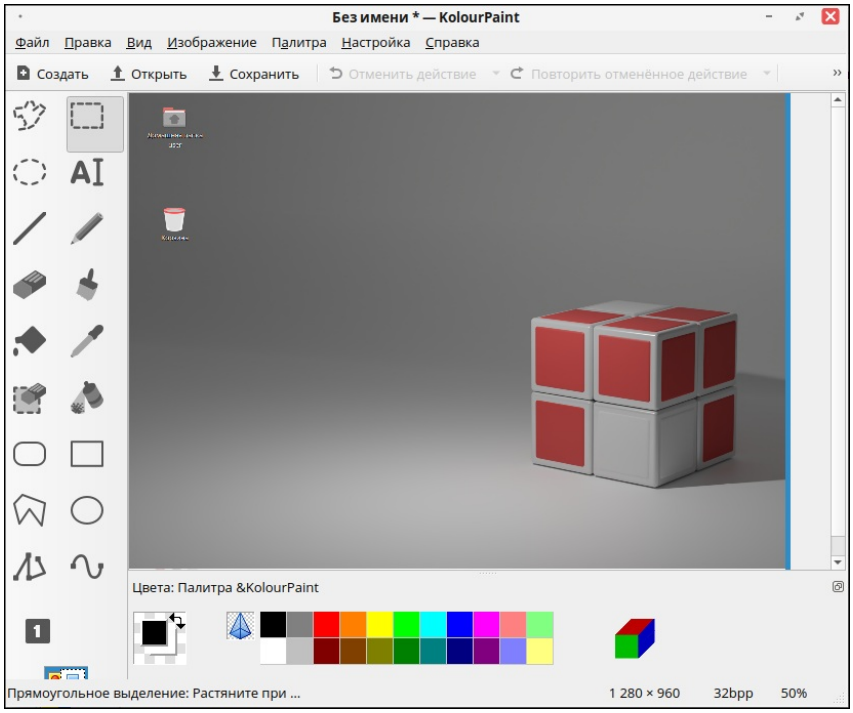
Скриншоты

Для сохранения понравившегося изображения, кадра из видеоролика, компьютерной игры или презентации можно использовать функцию создания скриншота. Для получения снимка экрана перейдите в меню «**Файл**» — «**Сделать снимок экрана**».

С помощью диалогового окна можно изменить задержку снимка экрана в секундах и скрыть главное окно во время создания снимка экрана. После выбора параметров нажмите «**OK**».



Сделанный снимок экрана будет помещён непосредственно в рабочую область **KolourPaint**.

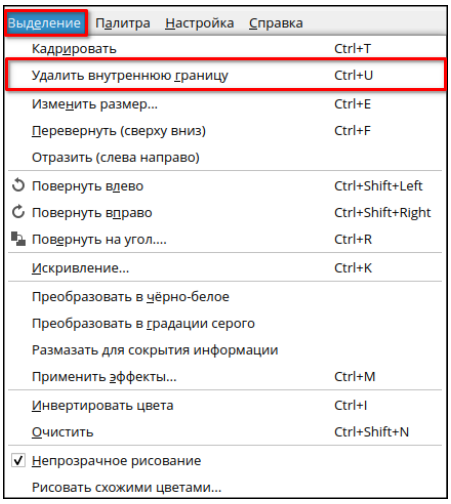


Эффекты изображения

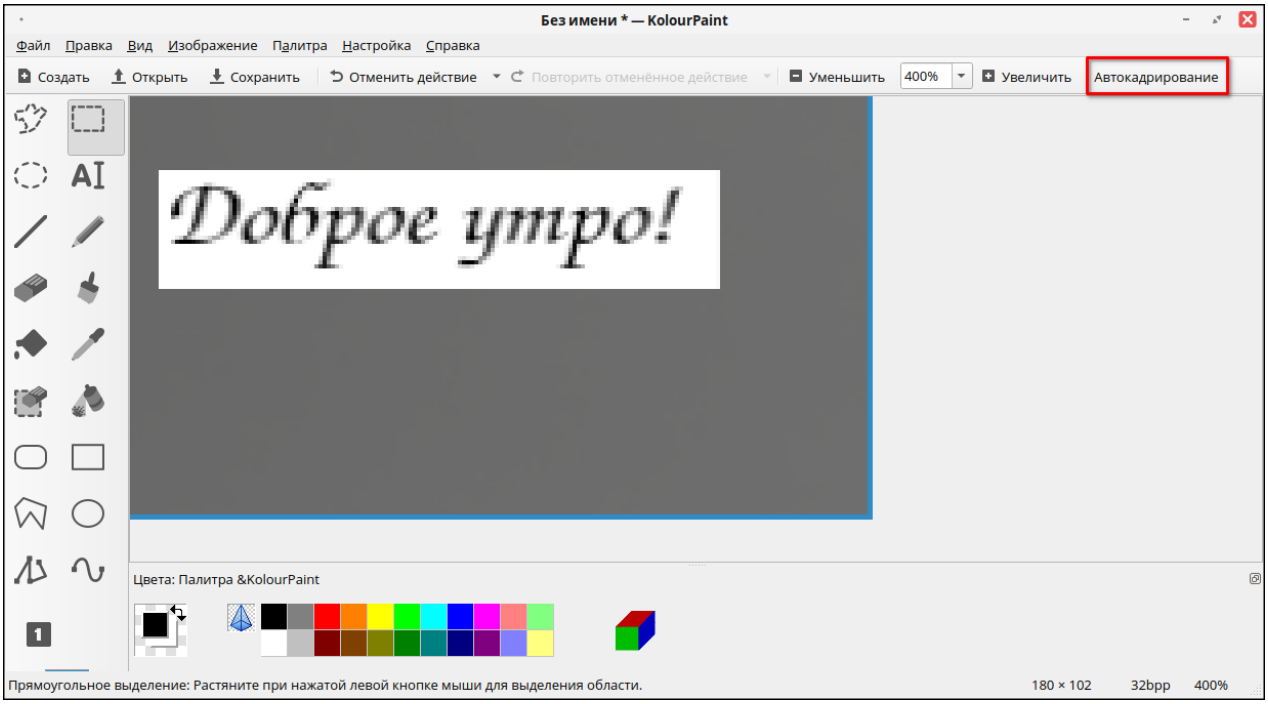
Эффекты в **KolourPaint** позволяют изменять внешний вид изображения различными способами.

Удаление внутренней границы / Автокадрирование

Инструмент **Удаление внутренней границы** предназначен для удаления тонкой границы вокруг выделенной области или фигуры. Для его использования перейдите в меню «**Выделение**» — «**Удалить внутреннюю границу**».

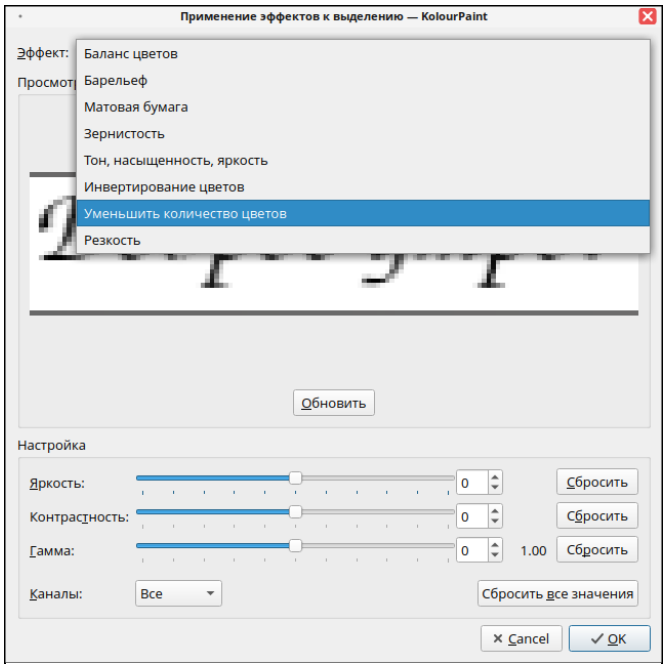


Автокадрирование удаляет прозрачные области вокруг изображения, обрезая его до минимальных размеров.



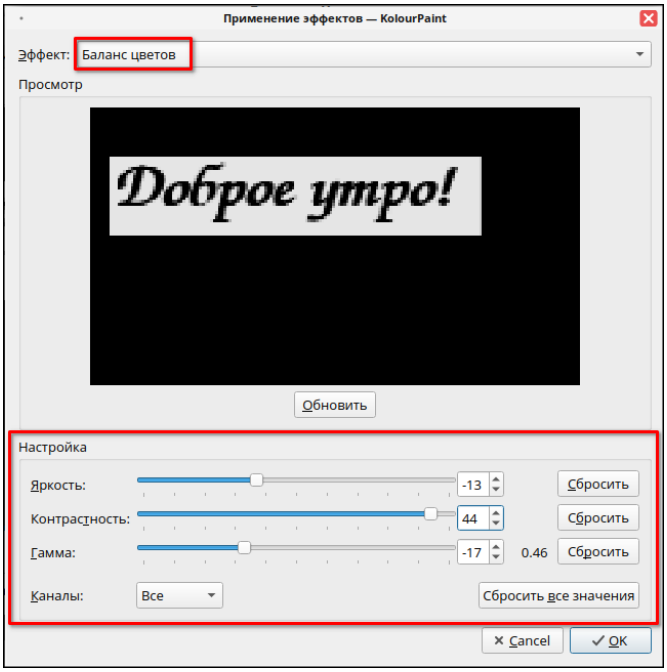
Дополнительные эффекты

Дополнительные эффекты можно выбрать в меню «**Выделение**» — «**Применить эффекты...**». Диалоговое окно содержит следующие инструменты:



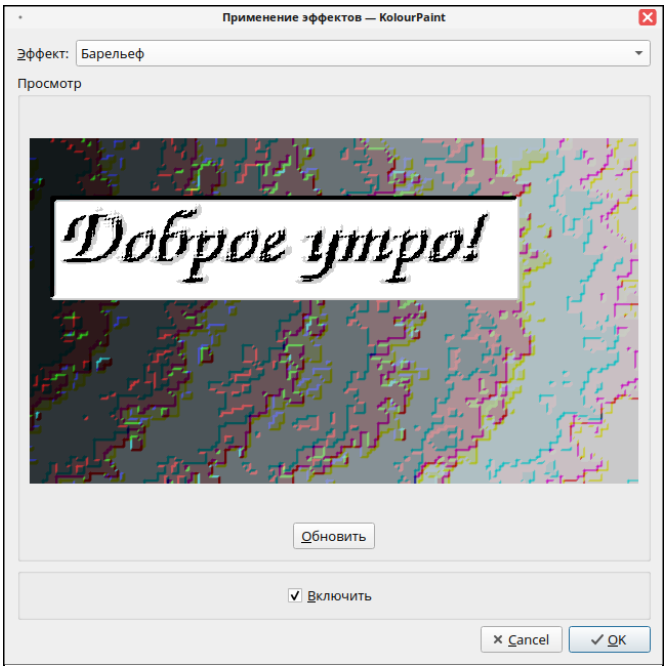
Баланс

Баланс корректирует уровни яркости и контрастности изображения, чтобы сделать его более равномерным. Инструмент позволяет изменить яркость, контраст и гамму всего изображения или выделенной области. Для изменения настроек баланса цветов используйте поля ввода числа и кнопки «**Сбросить**».



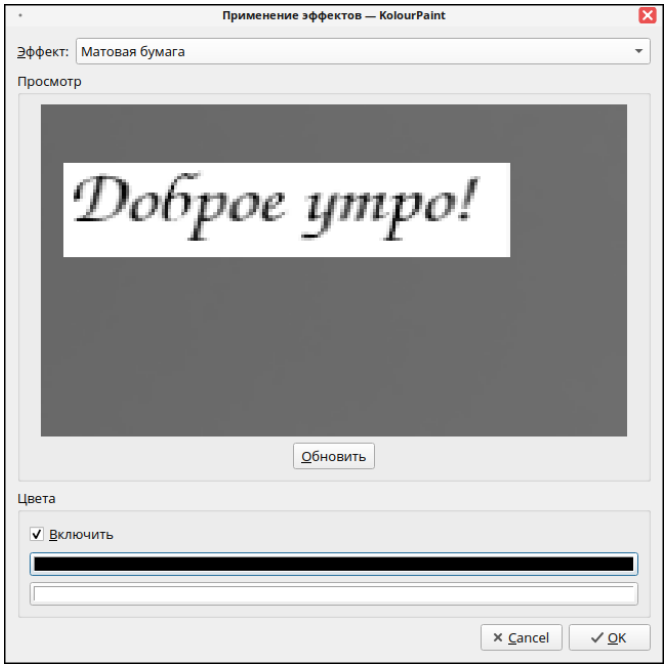
Барельеф

Барельеф создаёт эффект объёма на изображении, эффект гравюры. Для применения эффекта установите флаг рядом с параметром «**Включить**».



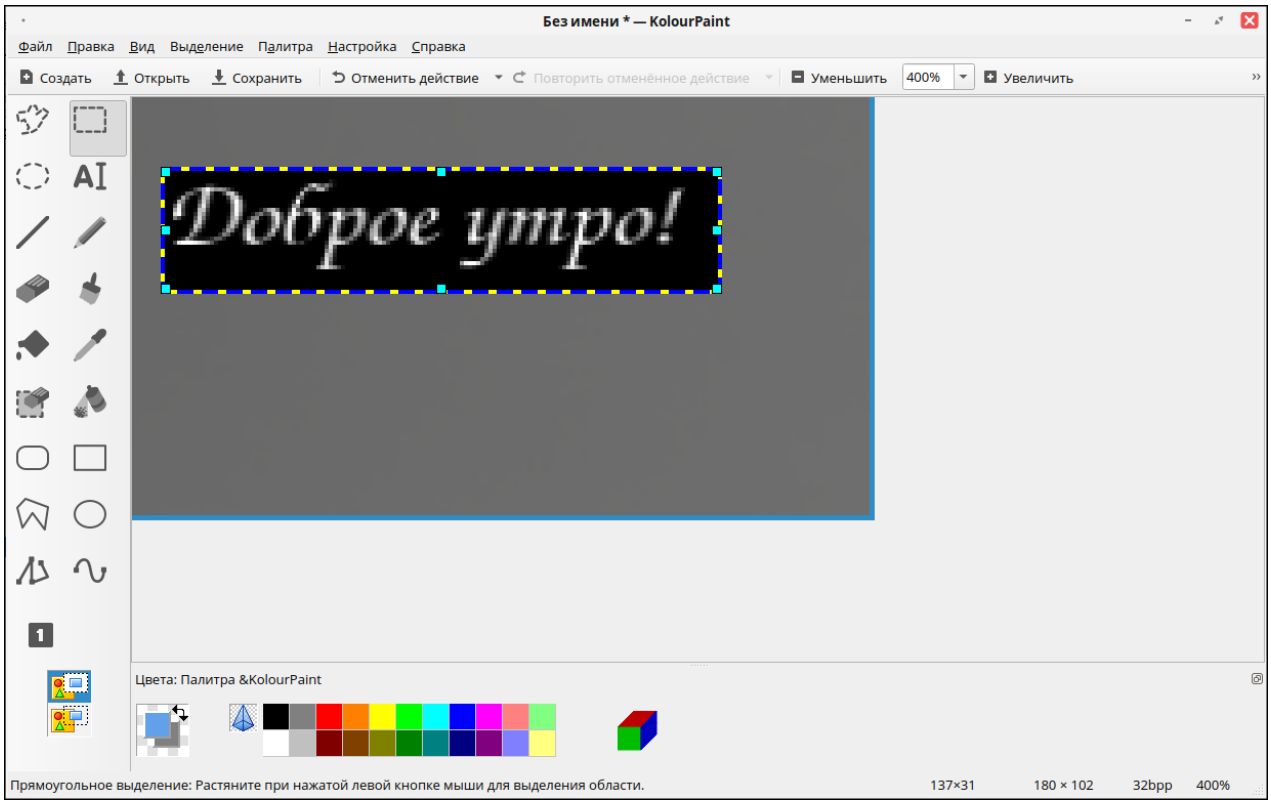
Матовая бумага

Матовая бумага создаёт эффект, как будто объект вдавлен в поверхность. Такие текстуры могут использоваться для фонов, создания объёмных объектов или для достижения определённого художественного стиля. Области, закрашенные выбранным цветом, будут перерисованы с заменой цвета на его градации. После выбранных параметров нажмите «OK».



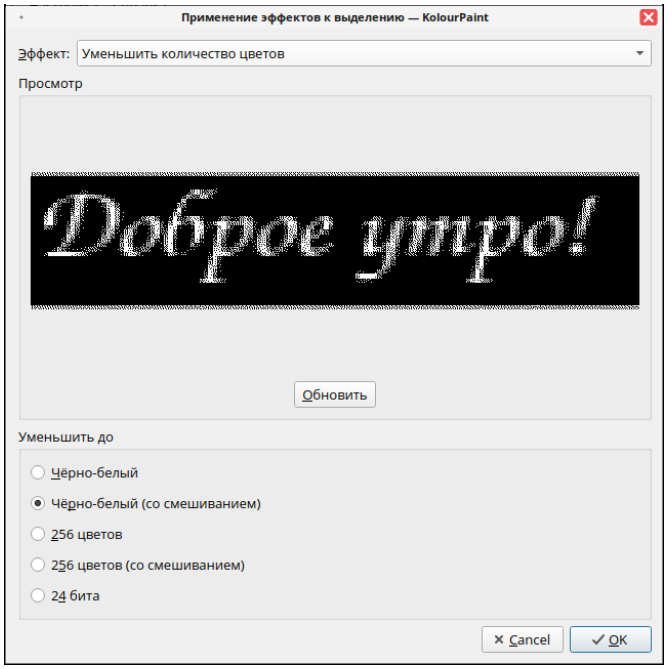
Инвертировать цвета

Инструмент инвертирует все цвета на изображении, делая их противоположными (например, чёрный становится белым, а белый становится чёрным).



Уменьшить количество цветов

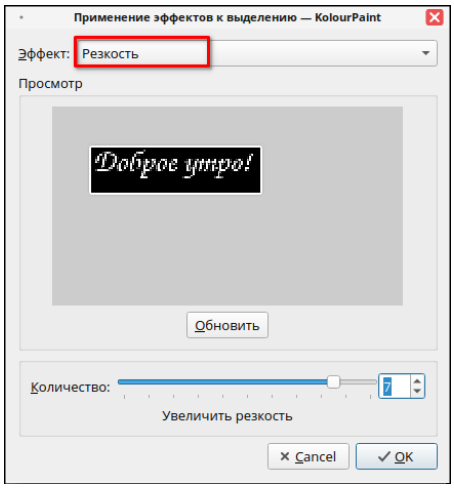
Уменьшает количество цветов во всем изображении или в выделенной области, со смешиванием или без него, что может придать ему эффект стилизации или сделать его более простым. Параметр доступен через меню «**Выделение**» — «**Применить эффекты...**».



Резкость

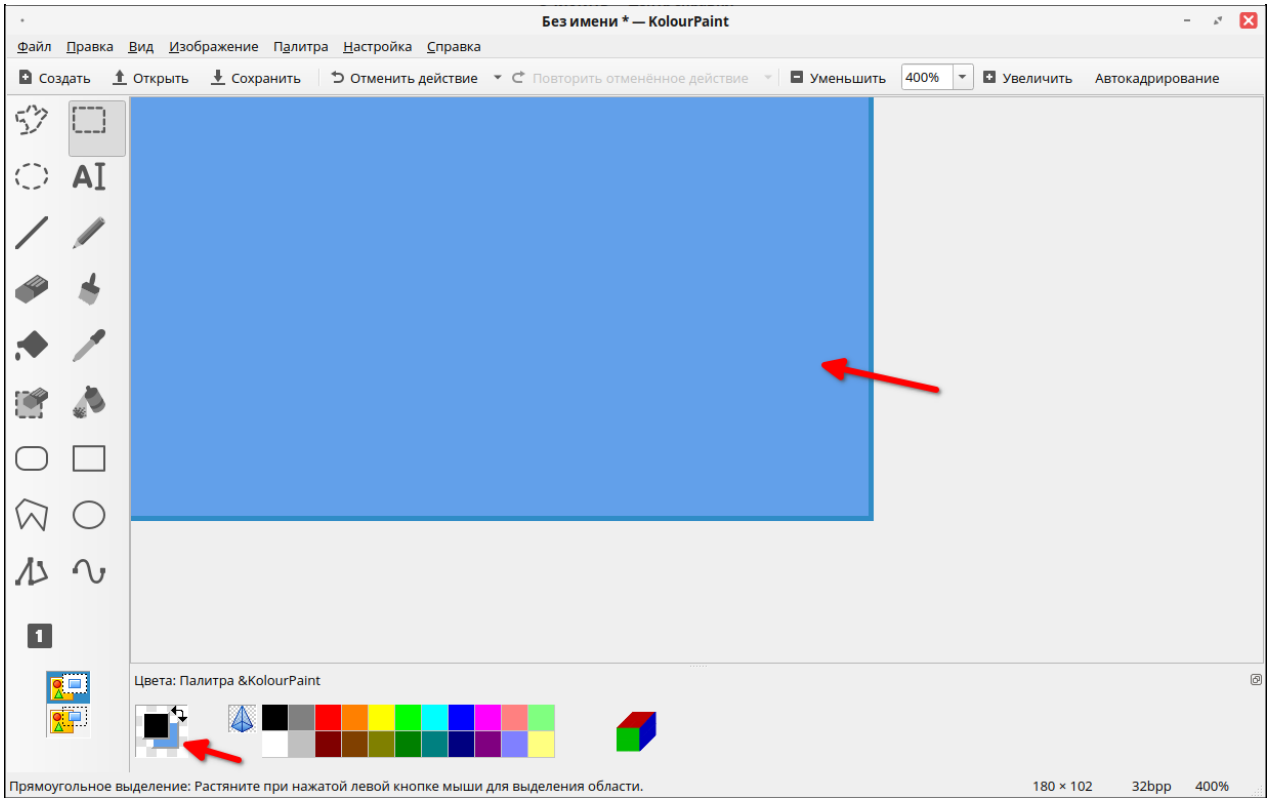
Параметр доступен через меню «**Выделение**» — «**Применить эффекты...**».

Увеличивает или уменьшает резкость изображения, делая его более чётким или размытым.



Очистить

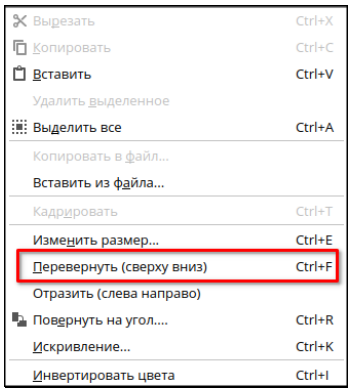
Заполняет всю область изображения цветом фона. Инструмент доступен в меню «**Изображение**» — «**Очистить**».



Для очистки всего изображения дважды щёлкните по инструменту  .

Перевернуть (сверху вниз)

Для переворота изображения сверху вниз щёлкните по нему ПКМ и в контекстном меню выберите «**Перевернуть (сверху вниз)**».



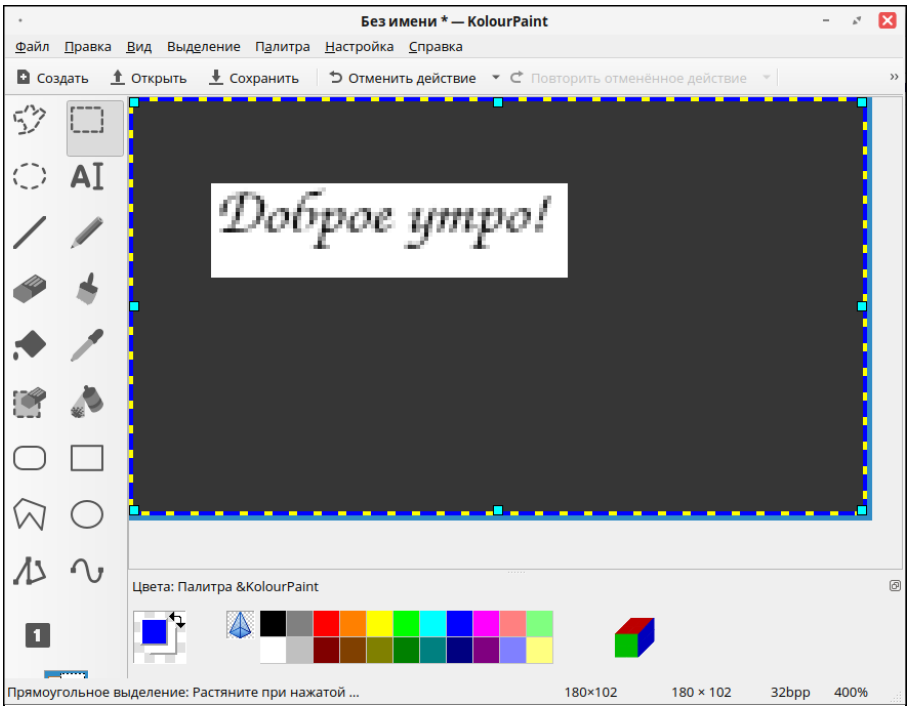
Данный эффект переворачивает всё изображение или выделенную область относительно горизонтальной оси.



Преобразовать в оттенки серого

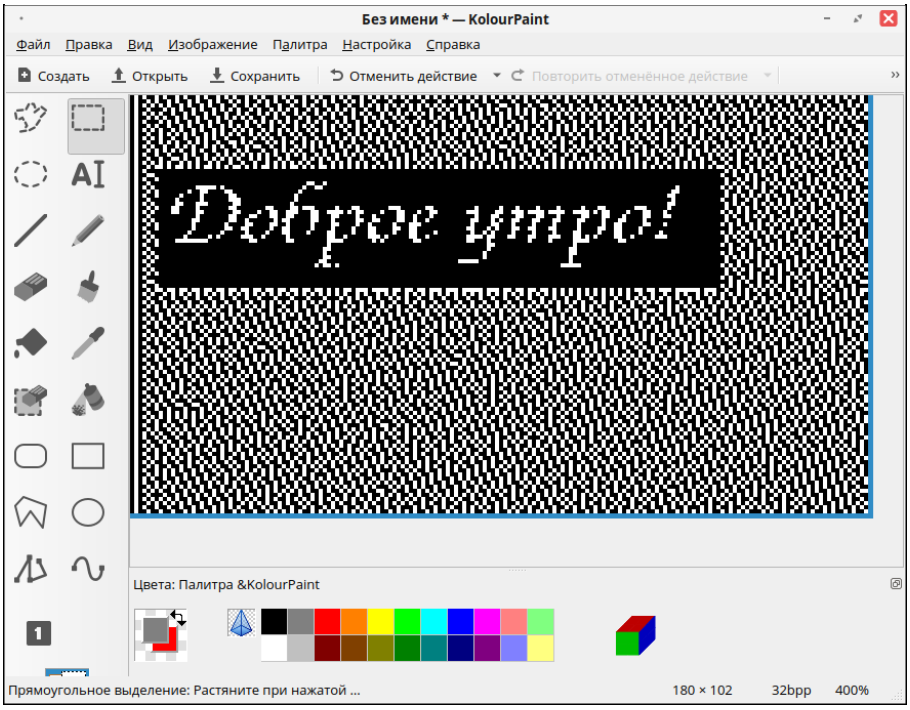
Преобразует изображение или выделенную область в оттенки серого, удаляя все цвета.

Параметр доступен через меню «**Выделение**» — «**Преобразовать в градации серого**».



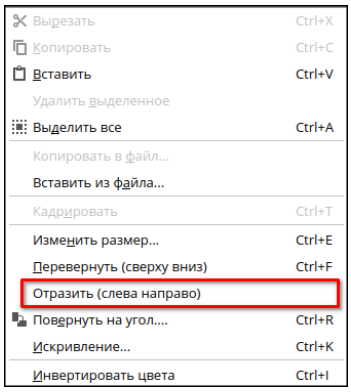
Сделать чёрно-белым (со смешиванием)

Преобразует изображение или выделенную область в черно-белое, но сохраняет некоторые детали, смешивая чёрный и белый цвета. Параметр доступен через меню «**Выделение**» — «**Преобразовать в черно-белое**».



Отразить (слева направо)

Отражает изображение горизонтально, меняя его сторону. Для отражения изображения щёлкните по нему ПКМ и в контекстном меню выберите «**Отразить (слева направо)**».

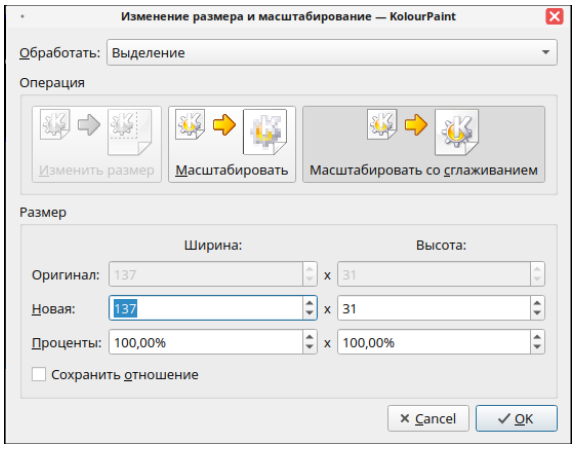


Изменить размер / Масштабировать

Параметр доступен через меню «**Выделение**» — «**Изменить размер...**». Изменяет размер изображения, делая его больше или меньше. Размеры изображения могут быть увеличены, но при этом не вносятся никаких фактических изменений.

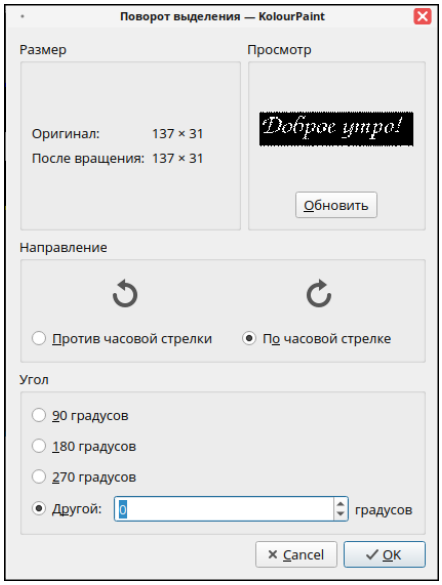
При использовании команды «**Масштабировать со сглаживанием**» происходит смешивание соседних цветов.

Можно установить новый размер в пикселях или в процентах от исходного значения. Включив опцию «**Сохранить отношение**», ширина и высота будут изменяться в одинаковых пропорциях. Обычное масштабирование возможно только для выделенных областей, текстовые области можно изменять только по размеру.



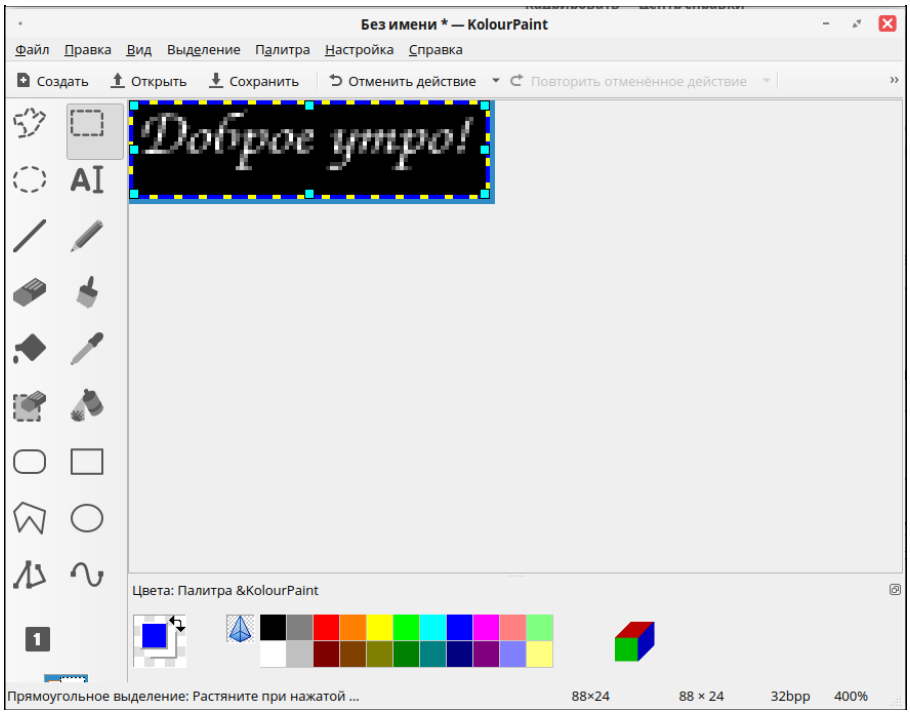
Поворот выделения

Поворачивает выделенную область на определённый угол в указанном направлении.



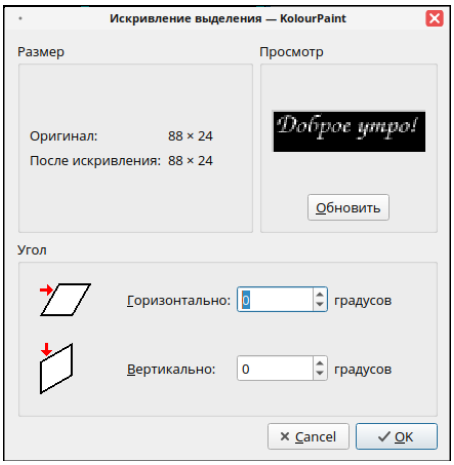
Кадрировать

Обрезает края выделенной области изображения для получения нужного размера или соотношения сторон. Задайте выделенную область и перейдите в меню «**Выделение**» — «**Кадрировать**».



Искривление

Параметр доступен через меню «**Выделение**» — «**Искривление...**». Искажает все изображение или выделенную область, деформируя его в определённых направлениях по горизонтали и/или вертикали.



Пример работы

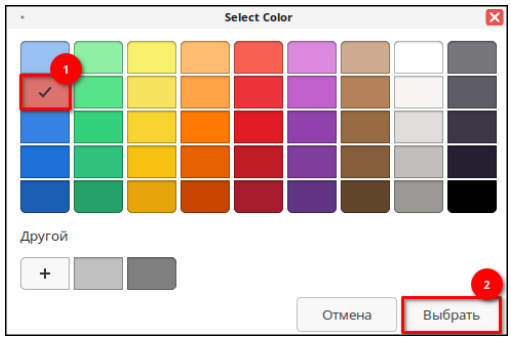
Для создание простого рисунка выполните следующий алгоритм действий:

1. Выберите  на панели инструментов.

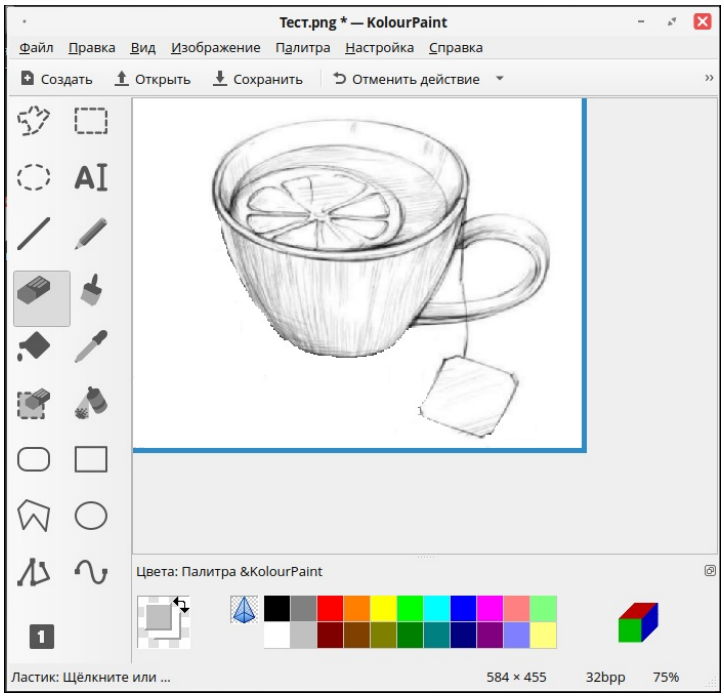
2. На палитре цветов выберите нужный основной цвет и цвет фона. Левый квадрат представляет **основной цвет** (цвет переднего плана), а правый квадрат представляет **цвет фона** (цвет заднего плана).



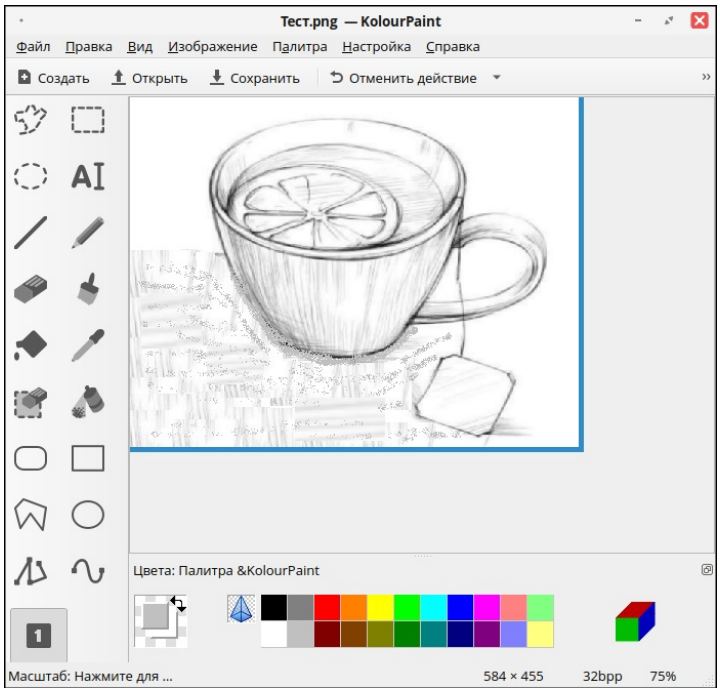
Для выбора **основного цвета** выберите его на палитре. Для выбора **цвета фона** кликните дважды на правый квадрат. После клика на правый квадрат откроется диалоговое окно «**Выбор цвета**». В этом окне можно выбрать цвет фона.



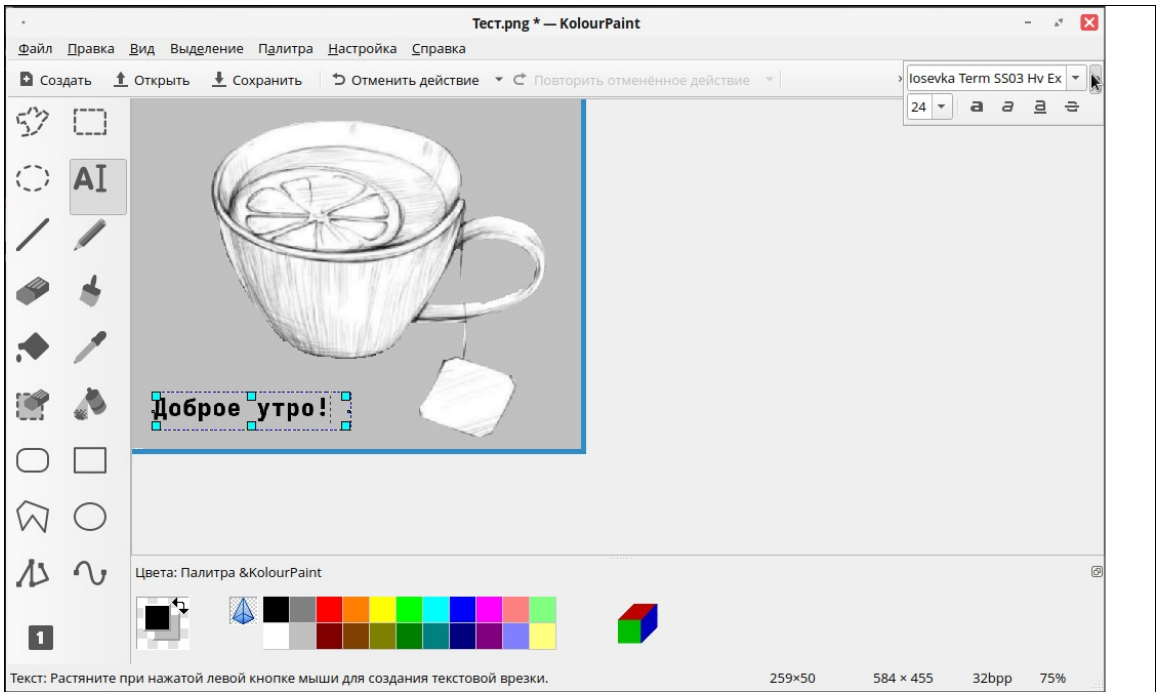
3. В рабочей области нарисуйте линию или фигуру, используя выбранную кисть и цвет.



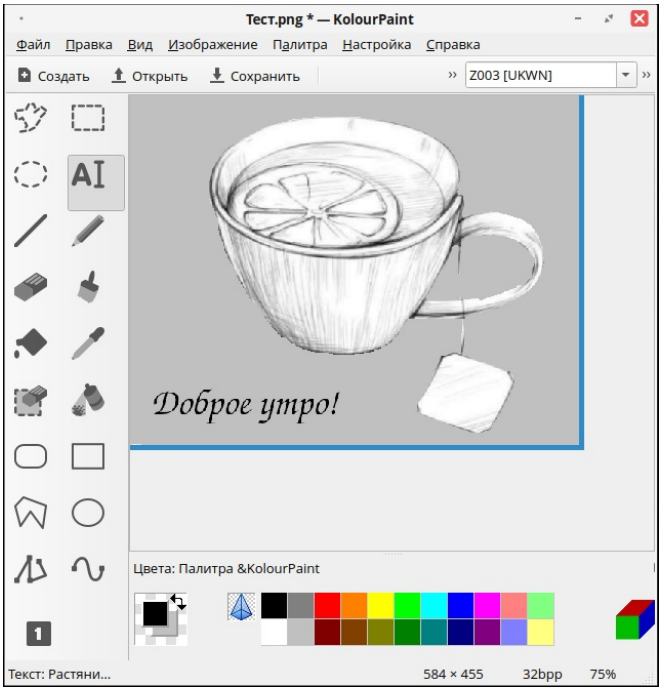
4. Выберите ▫ на панели инструментов. На палитре цветов выберите цвет, которым хотите заполнить область. В рабочей области кликните на область, которую хотите заполнить выбранным цветом. Закрашиваемая область должна иметь сплошной контур, иначе краска заполнит остальные части рисунка. Для отмены неправильного закрашивания нажмите **CTRL+Z**, исправьте контур и закрасьте снова нужную область.



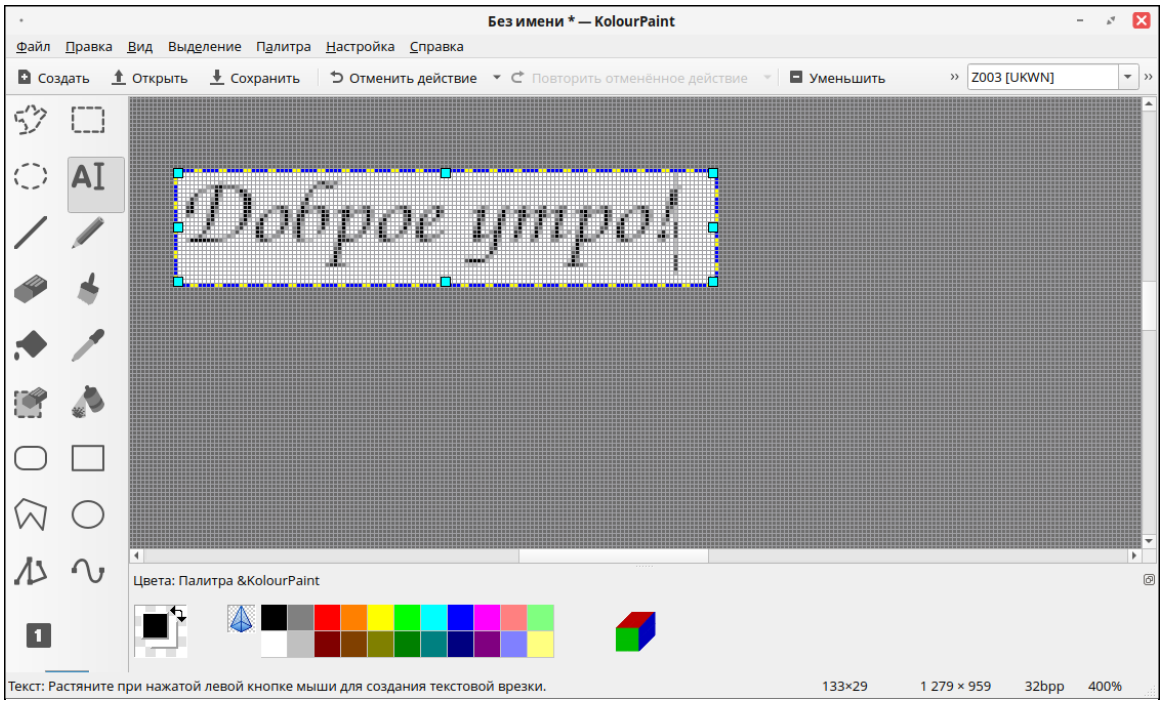
5. Для добавления текста к изображению на панели инструментов выберите инструмент AI. В рабочей области кликните в выбранном месте для размещения текста, протяните рамку, внутри которой будет расположен текст, и введите его.



Выберите шрифт и размер текста.



Для точного редактирования каждого пиксела при масштабе в 400% или большем (кратным 100%) можно использовать режим «**Показать сетку**», расположенном в меню «**Вид**».


Без имени * — KolourPaint
Файл Правка Вид Выделение Палитра Настройка Справка
Создать Открыть Сохранить Отменить действие Повторить отменённое действие Уменьшить
Z003 [UKWN]
Доброе утро!
Цвета: Палитра &KolourPaint
Текст: Растяните при нажатой левой кнопке мыши для создания текстовой врезки.
133×29
1 279 × 959
32bpp
400%

IrfanView — программа для работы с графическими файлами

Установка IrfanView
Запуск установщика с использованием терминала
Запуск установщика с использованием графического интерфейса
Обзор установки IrfanView
Установка плагинов для IrfanView
Запуск установщика плагинов с использованием терминала
Запуск установщика плагинов с использованием графического интерфейса
О программе
Печать документов через IrfanView

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: iview4.67

IrfanView — небольшая по размеру программа для просмотра/воспроизведения графических, видео- и аудиофайлов, поддерживает большое количество форматов, в том числе **BMP**, **HDR**, **JPEG**, **PNG**, **EXE**, **DLL**, **MPEG** и **PSD**. Отлично подходит для печати документов формата **TIF**.

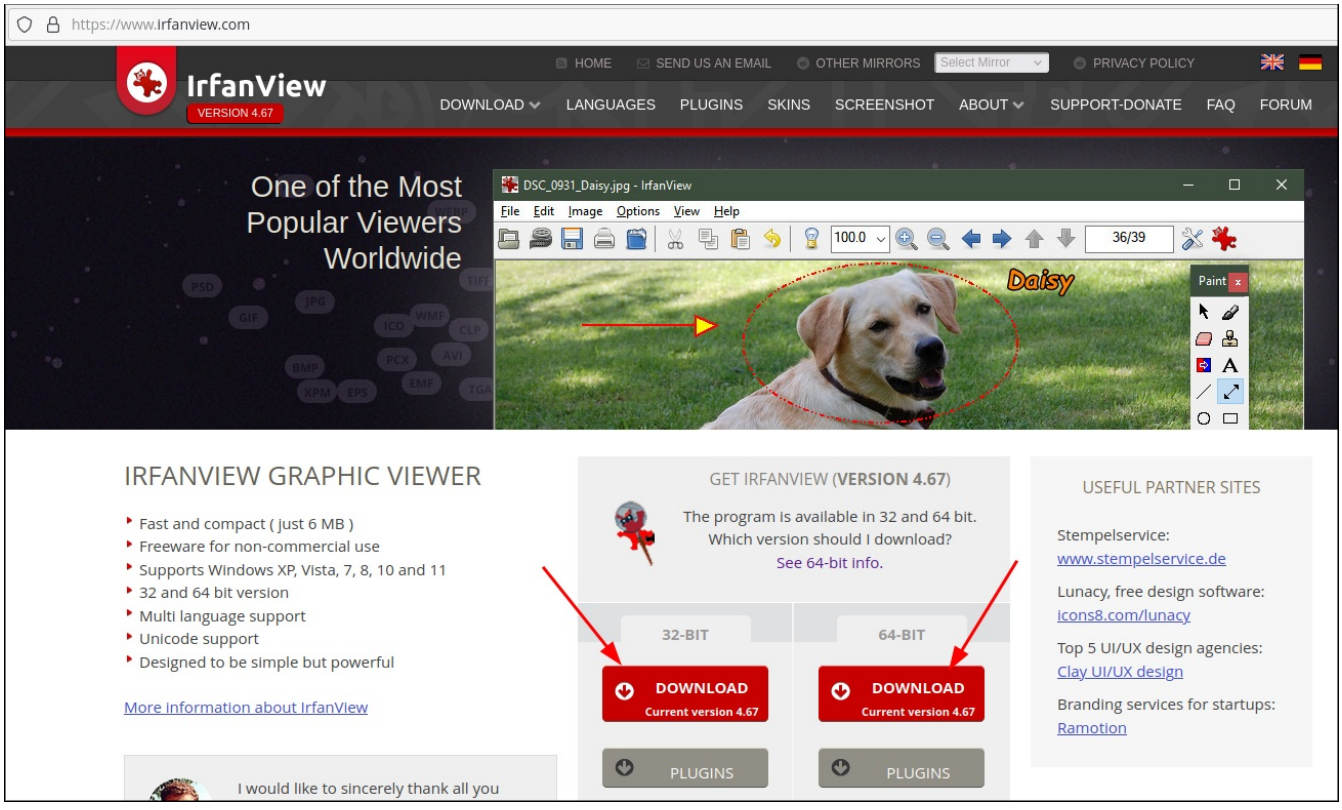
Примечание.

Для следующих этапов установки **IrfanView** потребуется **Wine**. С установкой и настройкой **Wine** можно ознакомиться в наших инструкциях «Работа с Wine».

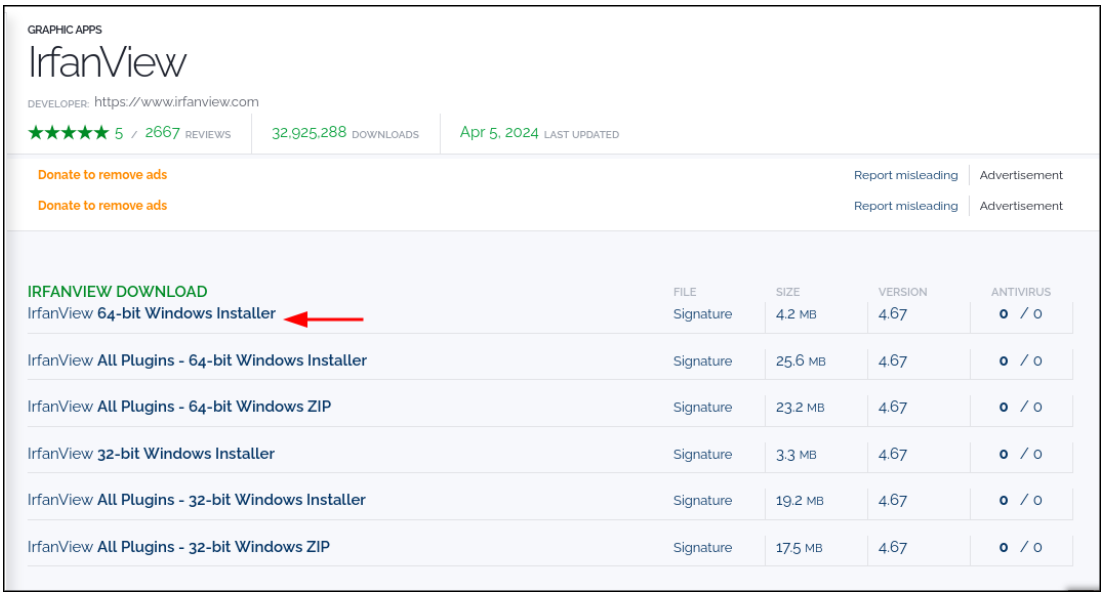
Установка IrfanView

Для загрузки установщика программы перейдите на официальный сайт **IrfanView** в раздел «**Download**» - «**Irfanview**» (предлагаются 32-битные и 64-битные версии программы **IrfanView**).

Откроется страница с установочными архивами и плагинами.



Скачайте установщик **IrfanView**.



После этого установите программу через **Wine**, используя терминал или графический интерфейс.

Запуск установщика с использованием терминала

Перейдите в каталог со скачанным файлом (в примере **/home/user/Загрузки/**):

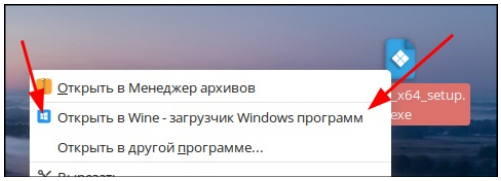
```
cd /home/user/Загрузки/
```

Выполните команду установки:

```
wine ./<название_файла>
```

Запуск установщика с использованием графического интерфейса

Вызовите контекстное меню, нажав ПКМ по файлу установщика, и выберите пункт «*Открыть в Wine — загрузчик Windows программ*».

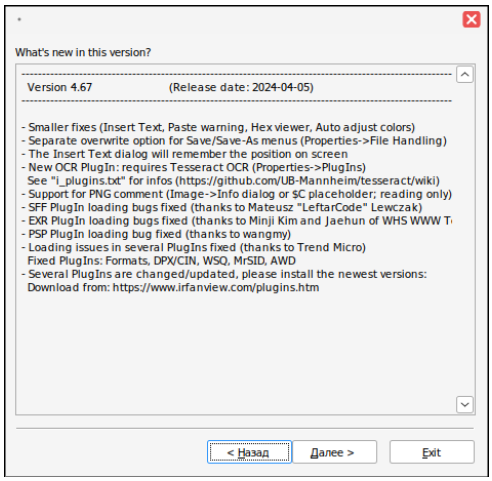


Обзор установки IrfanView

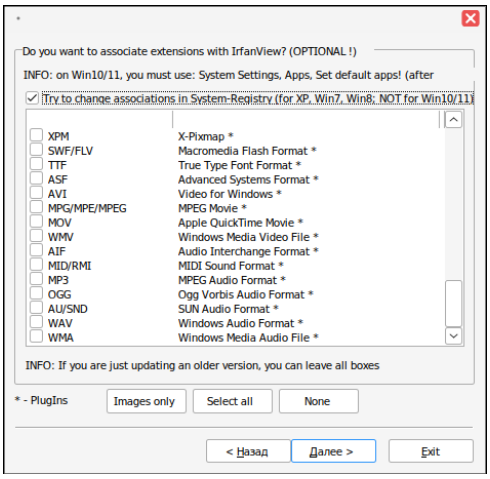
Запустите инсталлятор «**IrfanView -bit setup**». Определите необходимость создания ярлыков приложения. Для выбора каталога установки, отличного от каталога по умолчанию, нажмите «**Browse**» и определите свой каталог установки. Для продолжения нажмите «**Далее**».



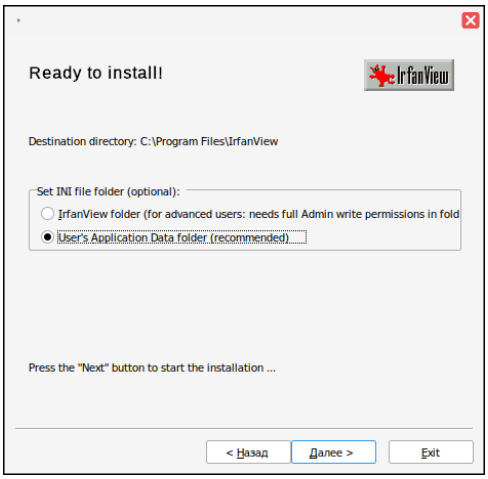
Ознакомьтесь с новыми возможностями данной версии и нажмите «**Далее**».



Выберите расширения файлов, которые по умолчанию будут открываться в **IrfanView** (по желанию).



В следующем окне оставьте рекомендуемые настройки по умолчанию и нажмите «**Далее**».



При успешном завершении установки появится соответствующее сообщение. После установки программа будет доступна из «**Главного меню**» - «**Wine**» - «**IrfanView**».

Установка плагинов для IrfanView

Для расширения функционала программы можно установить дополнительные плагины. Они находятся на официальном сайте **IrfanView** в разделе «**Download**» - «**Irfanview**».



Запуск установки производится точно таким же способом, как и установка самой программы - через **терминал** либо **графическим способом** с открытием через **Wine**.

Запуск установщика плагинов с использованием терминала

Перейдите в каталог со скаченным файлом (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
```

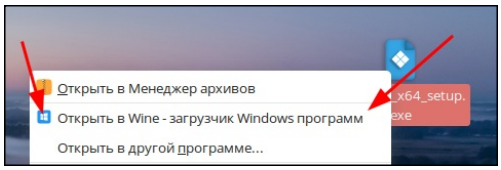
Выполните команду установки:

```
wine ./<название_файла>
```

При установке должен быть указан путь к каталогу, в который была установлена сама программа **IrfanView**.

Запуск установщика плагинов с использованием графического интерфейса

Вызовите контекстное меню, нажав ПКМ по файлу установщика, и выберите пункт «*Открыть в Wine – загрузчик Windows программ*».



О программе

Главное окно программы выглядит следующим образом:



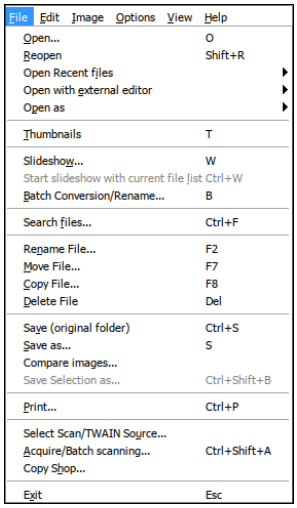
В верхней части окна расположено **основное меню** (1), где доступны все действия для работы и настройки программы.

Ниже расположена панель инструментов (2), с помощью которой доступны инструменты для работы с файлом.

Основную часть окна занимает рабочая область (3), на которой располагаются открытые файлы.

В основном меню представлены основные возможности программы.

Меню «**File**» («**Файл**») отвечает за работу с файлом, например, открытие, сохранение, удаление, печать, переименование и прочее.



Пункт «**Print**» отвечает за печать открытого файла с настройками масштабирования, выбор количества листов для печати и другие параметры. Также программа позволяет отсканировать файл и напечатать его.

С помощью «**Slideshow**» можно настроить слайд-шоу.

1. Инструмент «**Настройки слайдов**» отвечает за периодичность переключения изображений. Активация переключения происходит по щелчку ЛКМ или автоматически. Кнопка «**Play slideshow**» определяет начало показа слайд-шоу, а «**Cancel**» - выход из меню настроек.

2. В разделе «**Опции слайд-шоу**» можно скрыть курсор мыши, включить повторное воспроизведение аудиофайла, определить, с какого файла начинать показ, настроить отображение текста.

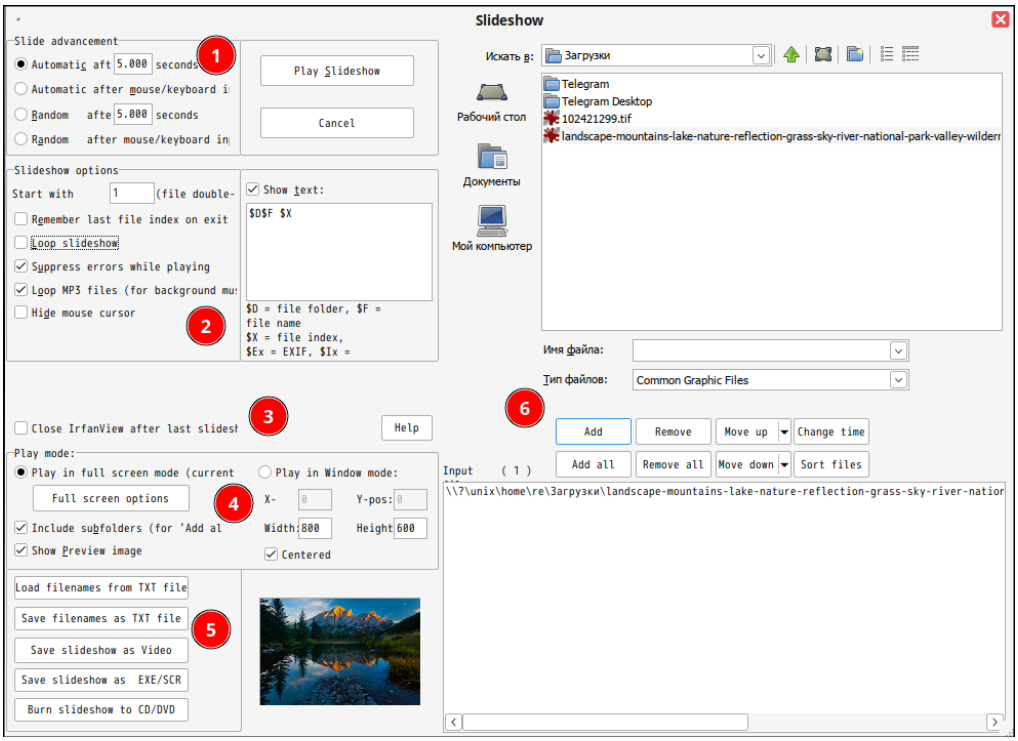
3. В чекбоксе «**Close IrfanView after last slidest**» доступна возможность настройки выхода из режима слайд-шоу после показа последнего файла.

4. В разделе «**Режим воспроизведения**» можно изменить настройки режима показа слайд-шоу - *полноэкранный режим* или *режим*

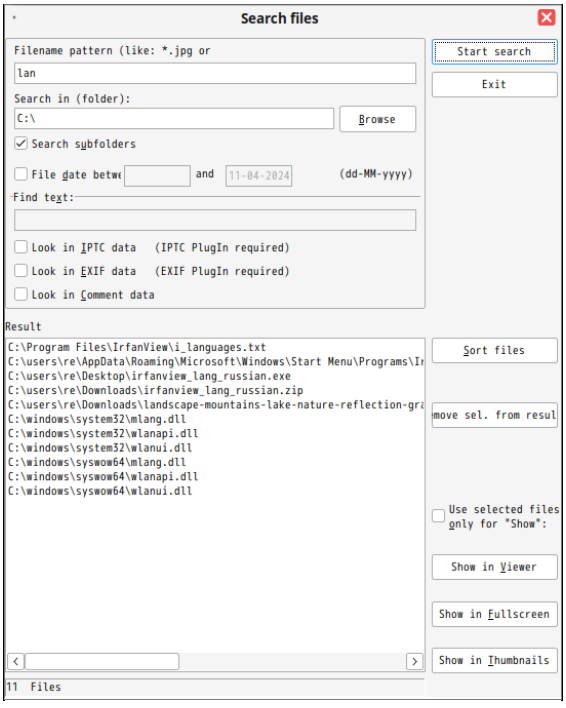
окна, а так же масштаб оконного режима.

5. Слайд-шоу можно сохранить в видеофайл в форматах **EXE/SCR** или записать на CD/DVD/BD-диски.

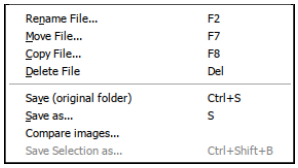
6. В правой части окна доступен поиск файлов, которые будут использоваться в слайд-шоу. Можно добавить все сразу при помощи кнопки «**Add all**» или выбрать вручную с помощью «**Add**». Также файлы можно убирать вручную и автоматически, если они не нужны в показе.



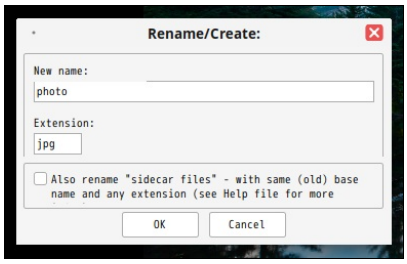
В пункте«**Search Files**» можно найти необходимый файл по названию или по его расширению.



Далее приведены пункты, которые отвечают за ряд дополнительных функций в этом редакторе.



1. **Rename File** — переименование файла и изменение расширения.



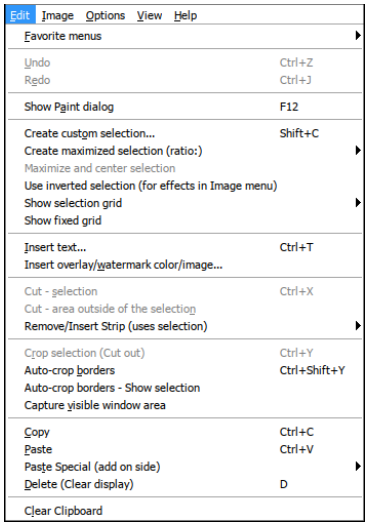
2. **Move** — перемещение файла.

3. **Copy** — копирование файла.

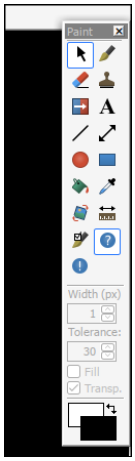
4. **Delete** — удаление файла.

5. «**Save**» и «**Save as...**» — сохранение файла. «**Save**» отвечает за сохранение текущего файла в текущей папке, из которой он был открыт. «**Save as...**» позволяет выбрать каталог для сохранения.

Меню «**Edit**» («**Правка**») отвечает за редактирование изображений.

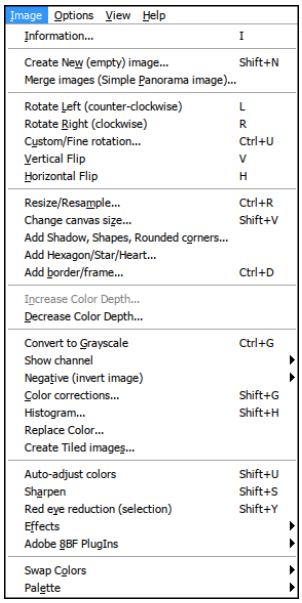


Show Paint dailog открывает диалоговое окно с различными инструментами для рисования.



Также в этом пункте настраивается выделение, кадрирование фотографий, копирование и вставка отдельных элементов, добавление на фотографию текста или водяного знака, очистка рабочей области.

В меню «**Image**» («**Изображение**») производится настройка рабочей области, изменение размера холста и изображения, поворот влево и вправо на 90 градусов, поворот вертикально и горизонтально, добавление рамок и виньеток на изображение.

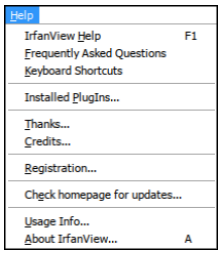


Также можно настроить цвета автокоррекцией или вручную, заменить цвет, повысить резкость, убрать красные глаза на фотографии, добавить эффекты и фильтры, инвертировать цвета на фотографии.

В меню «**Options**» («**Опции**») можно, по желанию, изменить язык самой программы, отправить файл по почте, сделать снимок экрана, изменить дату и время съемки фотографии.

В меню «**View**» («**Вид**») производятся настройки отображения, строк состояния, панелей инструментов, меню, а также настройка полноэкранного или оконного режима, приближения и отдаления фотографий.

В меню «**Help**» («**Справка**») можно посмотреть различные клавиатурные команды, ответы на вопросы, проверить наличие обновлений, просмотреть, установленные плагины и версию программы.



Панель инструментов обеспечивает быстрый доступ к основным возможностям программы.



1. Открыть файл.

2. Запустить слайд-шоу.

3. Сохранить файл.

4. Печать.

5. Удалить файл.

6. Вырезать выделенное.

7. Скопировать выделенное.

8. Вставить выделенное.

9. Отменить последнее действие.

10. Просмотреть сведения о файле.

11. Задать масштаб изображения.

12. Приблизить изображение.

13. Отдалить изображение.

14. Предыдущий файл в списке.

15. Следующий файл в списке.

16. Предыдущая страница.

17. Следующая страница.

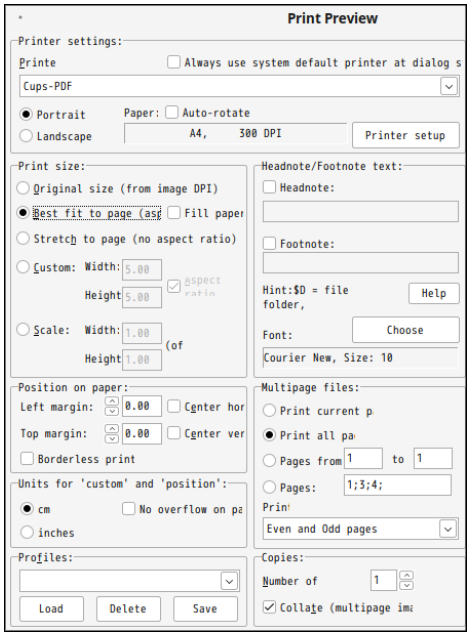
18. Настройка программы.

19. О программе.

Печать документов через IrfanView

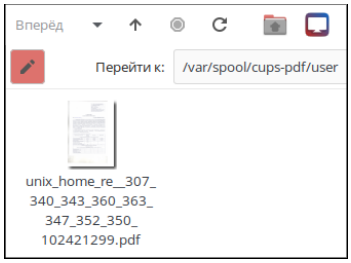
IrfanView можно использовать для печати файлов. Для этого необходимо открыть нужный файл и нажать **Print**.

Далее в выпадающем меню выбрать необходимые настройки для печати, например, распечатать текущий лист или весь файл, выбрать необходимый масштаб на странице и прочее. Принтер можно выбрать по умолчанию или установить его вручную.



В примере используется виртуальный принтер **CUPS-PDF** для демонстрации печати.

По умолчанию файлы, распечатанные виртуальным принтером, находятся в каталоге **/var/spool/cups-pdf/<имя_пользователя>**.



Scribus — программа для вёрстки страниц

Основные возможности программы
Установка
Запуск
Описание программы
Пример работы
Создание листовки
Экспорт файла

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: scribus-1.5.6.1

Scribus — это программа для профессионального дизайна и вёрстки страниц. Она предлагает поддержку большинства текстовых и графических форматов, включая **SVG**, шрифты **TrueType** и **OpenType**, **CMYK**, высокоуровневый экспорт в **PDF**. С помощью **Scribus** можно создавать различные типы визитных карточек, брошюр, информационных бюллетеней, журналов, каталогов и других документов. Программа обладает широкими возможностями по настройке дизайна страницы и форматированию текста.

Основные возможности программы

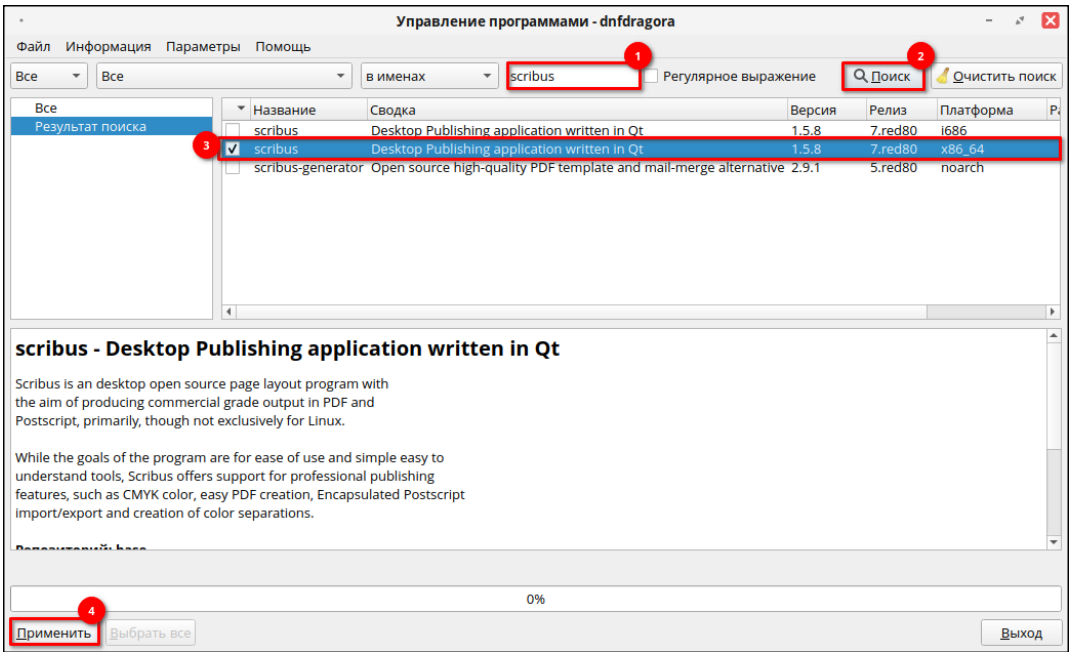
Основными возможностями **Scribus** являются:

- настройка полей и направляющих;
- предустановленные профили для различных типов печатных изданий;
- поддержка разнообразных размеров и форматов бумаги;
- векторные инструменты, включая **кривые Безье** и примитивы;
- вставка и базовая обработка изображений;
- импорт и экспорт векторной графики в формате **SVG**;
- полная поддержка **Unicode**, включая специальные символы и различные направления текста;
- возможность создания текстовых блоков различной формы и их трансформация;
- обтекание текстом других объектов и линковка текстовых блоков;
- настройка шрифтов, кернинга, интерлиньяжа и других параметров текста;
- создание и применение предустановленных стилей текста;
- поддержка множества графических форматов и совместимость с **PDF 1.4**;
- возможность создания интерактивных **PDF**, включая формы и **JavaScript**-сценарии;
- поддержка цветовых профилей **CMYK** и **RGB**;
- интуитивно понятный интерфейс с возможностью настройки горячих клавиш;
- функция черновика для удобства работы с элементами документа.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**scribus**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install scribus
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

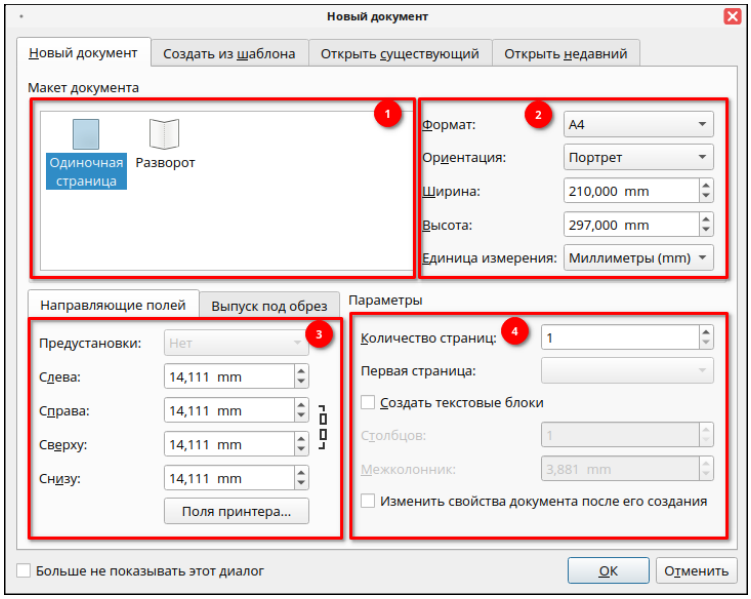
Запуск

Запустить программу можно либо в графическом режиме, либо через терминал. После установки программа будет доступна из «**Главного меню**» — «**Графика**» — «**Издательская система Scribus**» или «**Scribus**». Запустить программу через терминал можно, введя команду:

```
scribus
```

Описание программы

При запуске **Scribus** появляется окно настроек нового документа.



Окно **Новый документ** состоит из следующих областей:

1. В области **Макет документа** производится выбор типа документа.

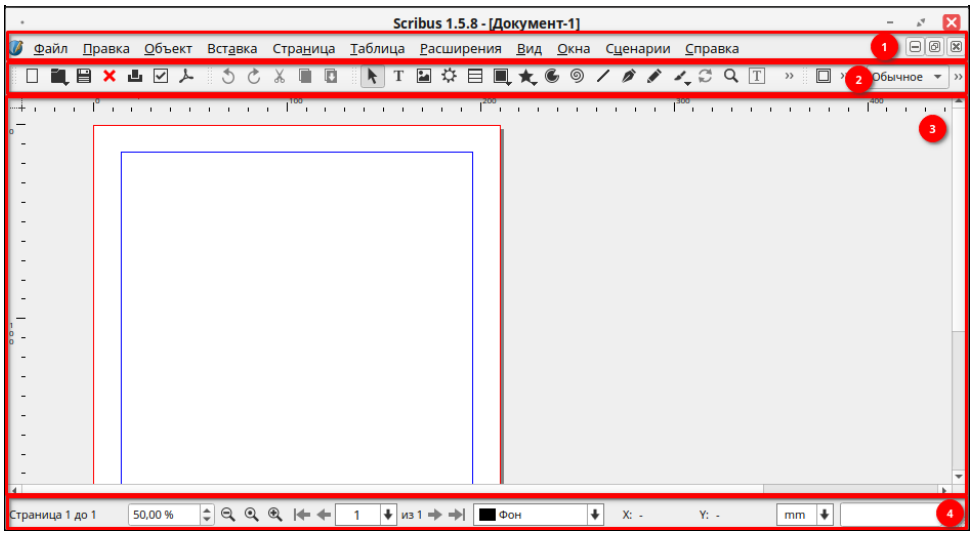
2. В области **Формат страницы** производится выбор размера документа (обычно формат A4), ориентации (по умолчанию Портрет).

После выбора определённого формата в полях «*Ширина*» и «*Высота*» будут автоматически установлены соответствующие размеры, которые можно изменить.

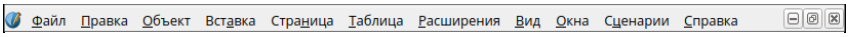
3. В области **Направляющие полей** можно установить отступы для документа, выбрав предпочтительные единицы измерения.

4. В области **Параметры** доступна настройка страниц нового документа и создание необходимого количества текстовых блоков.

Интерфейс программы стандартный и состоит из нескольких типовых частей.



1. **Основное меню** — позволяет выполнять различные действия с создаваемым документом, а также настраивать программу.



В основном меню доступны такие действия, как:

- операции с файлами;
- команды общего редактирования документа;
- команды работы с графическими объектами;
- вставка текстовых блоков, изображений, фигур, символов, линий;
- работа с макетом публикации;
- просмотр публикации и вывод служебных элементов;
- применение сценариев;
- управление окнами документов;
- описание программы и помощь по её использованию.

2. **Панель инструментов** — стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы. Эти панели можно скрывать и отображать через основное меню. По умолчанию отображаются следующие панели инструментов:

- *Панель Файл* — собраны функции для работы с файлами, такие как создание, открытие, сохранение и печать документов.



- *Панель Правка* содержит инструменты для редактирования текста и объектов в документе, включая копирование, вставку элементов, отмену действий.



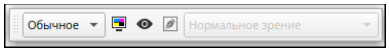
- *Панель Инструменты* предлагает различные функции для настройки документа, например, выбор объекта, добавление изображения, добавление таблицы, добавление фигуры, многоугольника, кривой Безье, блоков или линий, изменение масштаба.



- *Панель PDF-инструменты* включает опции для работы с PDF-файлами, содержит инструменты создания форм, вставки текстовой и ссылочной аннотации.



- *Панель Инструменты просмотра* позволяет переключаться между режимами просмотра и выбрать качество показа изображений в документе.



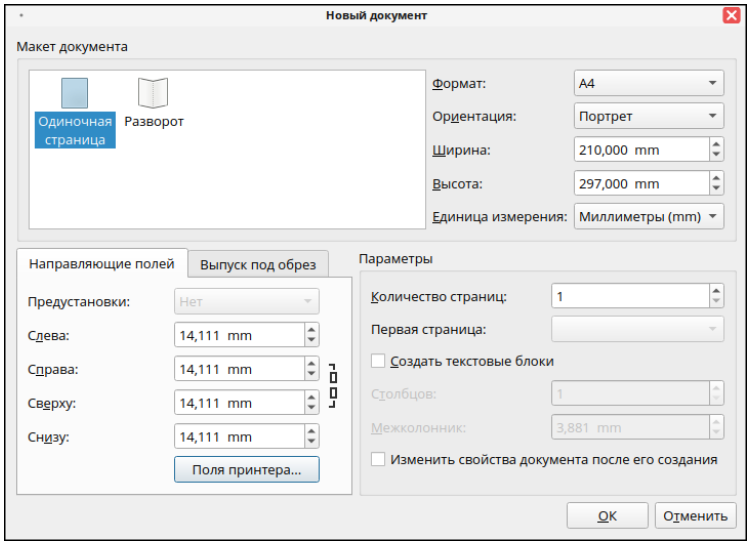
3. **Основное рабочее поле**. В данном поле происходит весь процесс вёрстки документа.

4 . **Панель состояния**. Здесь отображаются опции и действия, которые относятся к выбранному в данный момент инструменту. Инструменты можно выбирать через панель инструментов.

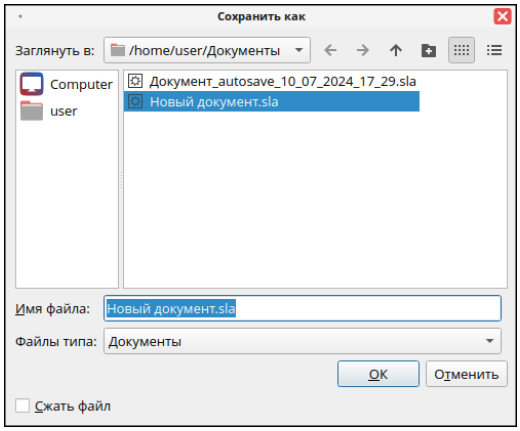
Пример работы

Создание листовки

1. Для создания нового документа в формате A4 с односторонним оформлением страницы перейдите в меню «**Файл**» — «**Создать...**» или кликните по значку на панели инструментов ( ). После выбора параметров нажмите «**OK**».

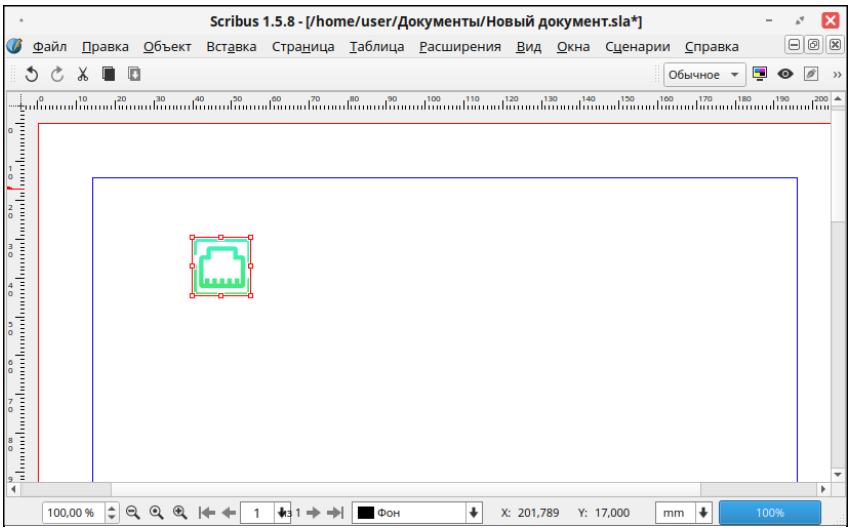


2. Для сохранения документа перейдите в меню «**Файл**» — «**Сохранить как...**». В открывшемся окне выберите папку для сохранения документа. В поле «**Имя файла**» введите желаемое название документа. Выберите формат файла. После выбора параметров нажмите «**OK**».

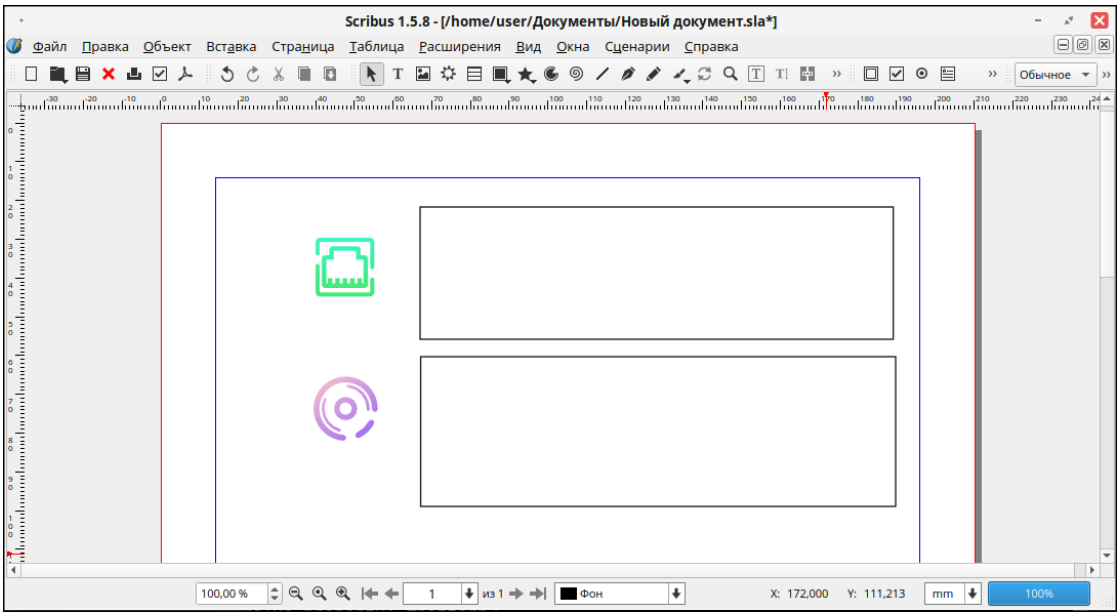


3. Скачайте из интернета или сохраните в предварительно созданную папку необходимые изображения для вёрстки.

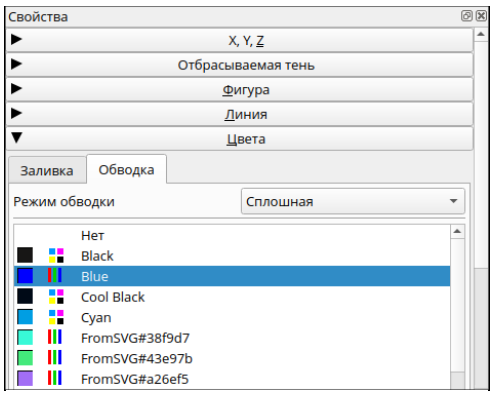
4. Импортируйте векторную графику в документ с помощью меню «**Файл**» — «**Импортировать**» — «**Вставить векторный графический файл...**».



5. Теперь создайте блоки, в которых будут располагаться текст и изображение, с помощью меню «**Вставка**» — «**Фигура**» — «**Типовые фигуры**» — . Расположите курсор мыши на листе в точке, где будет начинаться блок. Затем нажмите ЛКМ и, удерживая, проведите курсором до желаемого конечного положения блока. После достижения конечной точки блока отпустите ЛКМ для завершения размещения. Второй блок создайте аналогичным образом.

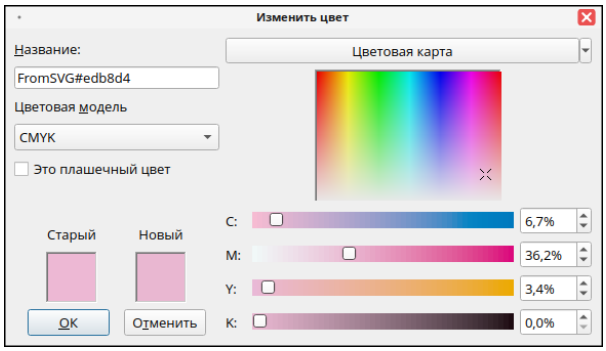


6. Для изменения цвета заливки и контура объекта щёлкните ПКМ по объекту и выберите из контекстного меню пункт «**Свойства**» — «**Цвета**».



Если логотип содержал, например, прямое указание цвета или точное предписание цвета CMYK, откройте меню «**Правка**» — «**Цвета и заливки...**».

После двойного щелчка по цвету откроется окно «**Изменить цвет**», в котором можно изменить цветовую модель (CMYK, RGB, веб-палитра RGB, Lab, HLC) и название цвета.

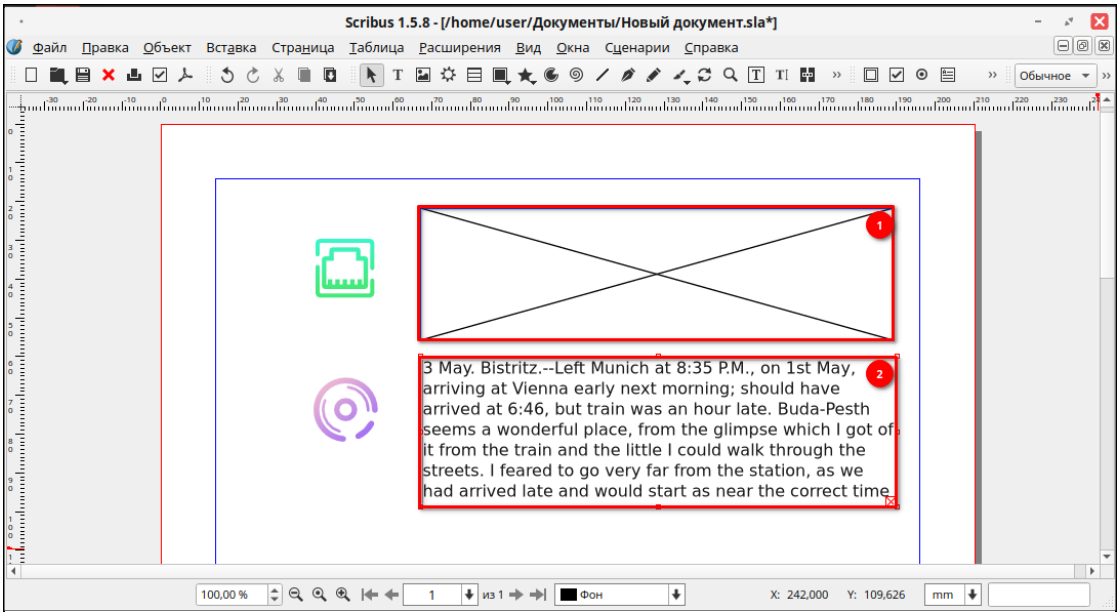


7. Для преобразования блоков и вставки текста выполните следующие действия.

Для преобразования блока в блок изображения щёлкните ПКМ по рамке и выберите «**Преобразовать в**» — «**Блок изображения**» (1).

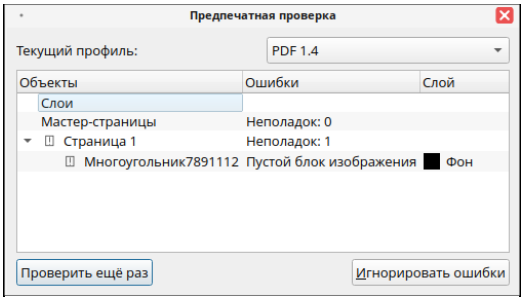
Для преобразования блока в текстовый блок щёлкните ПКМ по рамке и выберите «**Преобразовать в**» — «**Текстовый блок**».

Для вставки текста щёлкните ПКМ по рамке и выберите «**Содержимое**» — «**Вставить текст...**». Выберите файл с текстом и нажмите «**OK**». В блоке отобразится текст из файла (2).

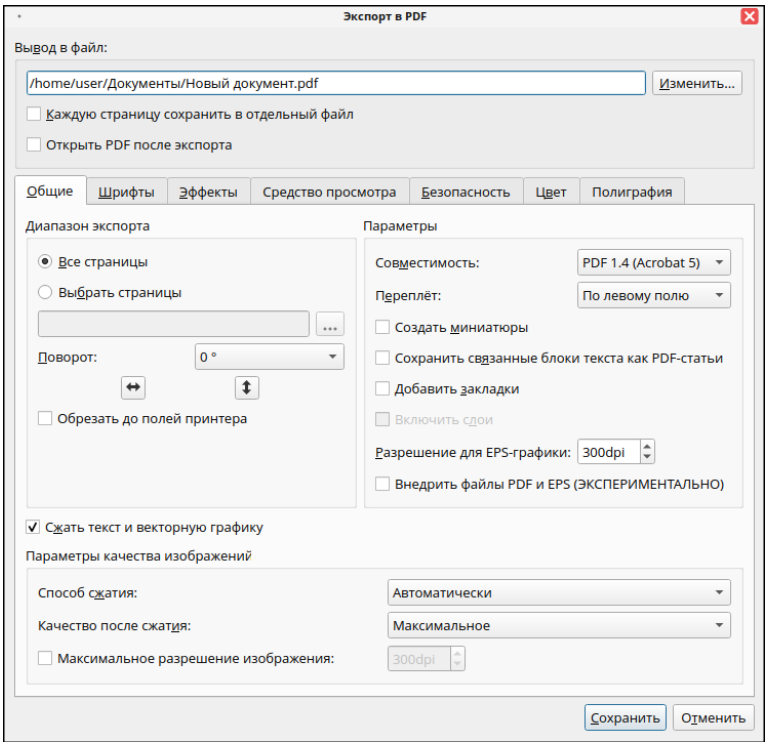


Экспорт файла

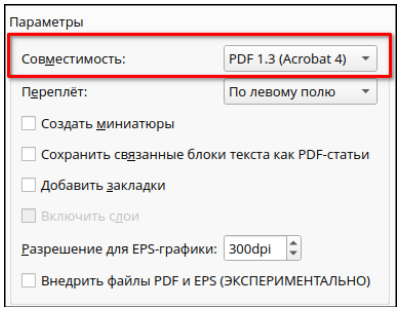
1. Для экспорта файла нажмите кнопку «**Сохранить как PDF**» (). Если PDF содержит какие-либо ошибки, появляется окно *Предпечатной проверки*. Исправьте ошибки или нажмите «**Игнорировать ошибки**».



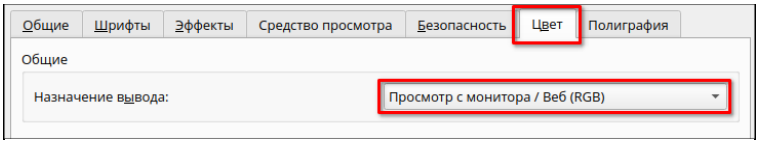
2. В появившемся окне «**Экспорт в PDF**» задайте параметры.



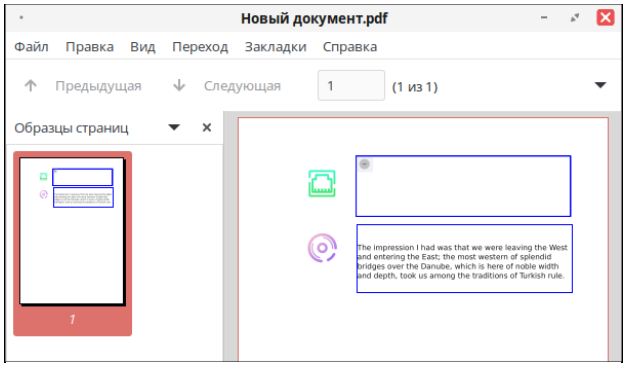
На вкладке «**Общие**» в параметрах совместимости выберите *PDF 1.3 (Acrobat 4)*.



На вкладке «**Цвет**» установите «**Просмотр с монитора / Веб (RGB)**».



После выбора параметров нажмите «**Сохранить**». После выполненных действий документ будет доступен для просмотра.



Редактор шрифтов FontForge

Установка
Обзор программы
Освоение инструментов
Понимание кривых Безье
Инструменты точек
Глифы
Инструменты рисования
Инструменты преобразования
Инструменты Прямоугольник, Эллипс, Многоугольник, Звезда
Действия кнопок мыши
Слои

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: fontforge-20190801-8

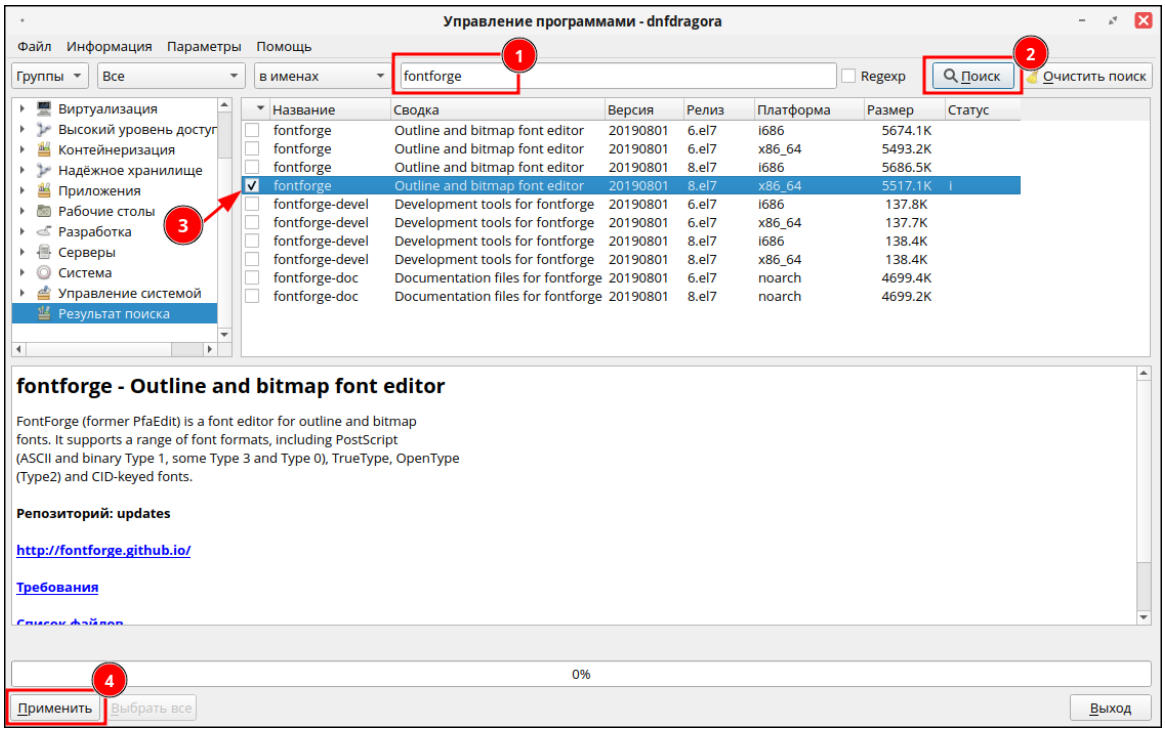
FontForge – многофункциональный редактор шрифтов с открытым исходным кодом, предоставляющий возможность создания, редактирования, конвертации и работы с различными форматами шрифтов, включая *TrueType* (TTF), *OpenType* (OTF), *PostScript* (PS), *SVG*, *UFO* и другие. Редактор также предлагает широкий спектр инструментов для творческого процесса в области шрифтов и типографики.

Среди работ автора программы также есть известные шрифты *Caslon Roman*, *Unicode font*, семейство шрифтов *Monospace* и т. д.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки редактора через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**fontforge**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fontforge
```

Дальнейшая работа в программе выполняется с правами непривилегированного пользователя, **выйдите** из сеанса пользователя **root**:

```
exit
```

После установки запуск редактора доступен из «**Главного меню**» - «**Графика**» - «**FontForge**» или через терминал с помощью команды:

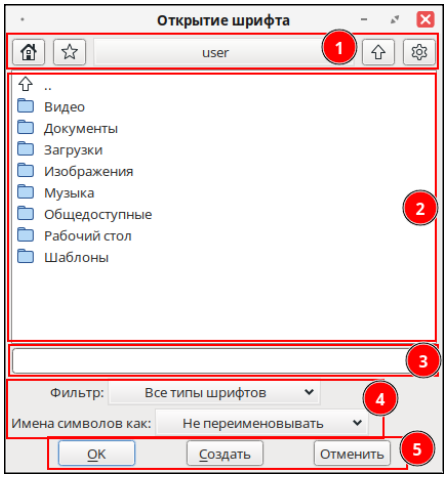
```
fontforge
```

Обзор программы

После запуска приветственное окно редактора выглядит следующим образом:



Вместе с приветственным окном активируется форма «**Открытие шрифта**», которая может быть использована для открытия уже существующего проекта или создания нового.



В форме «**Открытие шрифта**» доступны следующие инструменты:

1. Навигация по каталогам – здесь доступны:

- перемещение в домашний каталог пользователя;
- добавление каталога в закладки;
- перемещение по дереву каталогов на уровень выше;
- режим отображения файлов и каталогов.

2. Список файлов и подкаталогов, содержащихся в текущем каталоге.

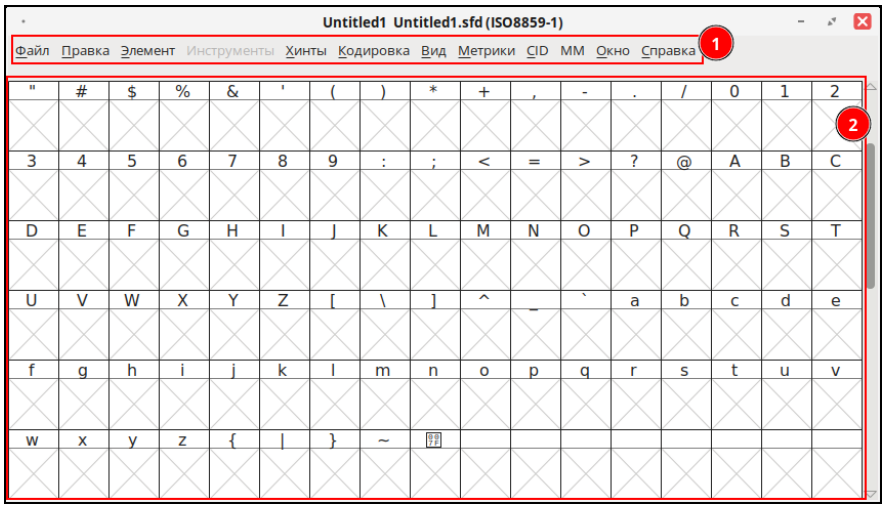
3. Текстовое поле, в котором отображается путь к файлу.

4. Параметры фильтрации найденных файлов по типам файлов и именам символов.

5. Кнопки действий:

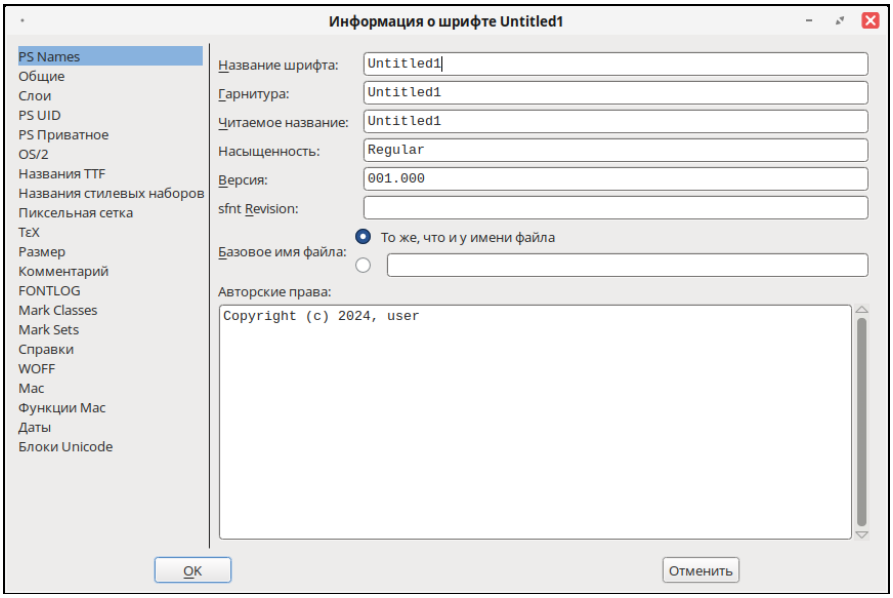
- **OK** – для открытия существующего проекта;
- **Создать** – для создания нового проекта;
- **Отменить** – для завершения работы.

После открытия проекта подгружается окно **Font View**, в котором показана таблица всех глифов в шрифте. Т.к. в рассматриваемом примере проект новый, все ячейки пусты.



В окне просмотра шрифта доступно основное меню (**1**), в котором расположены все необходимые для работы действия, и поле для просмотра глифов в шрифте (**2**).

Выберите пункт меню «**Элемент**» – «**Информация о шрифте**», чтобы заполнить информацию о создаваемом шрифте. В разделе **PS Names** заполните поля собственными данными о шрифте.



Освоение инструментов

В процессе создания шрифта в **FontForge** используются различные инструменты и утилиты, включая инструменты рисования. Они отличаются от тех, с которыми знакомы пользователи, работающие с векторной графикой. Прежде чем рассматривать сами инструменты рисования в **FontForge**, сначала необходимо изучить работу с кривыми Безье.

Понимание кривых Безье

Концепция "кривых Безье" относится к математическому подходу, применяемому для создания плавных кривых в цифровой форме. Обычно используются кубические и квадратичные кривые, но в дизайне также используются альтернативные кривые *Spiro*, поддерживаемые **FontForge**.

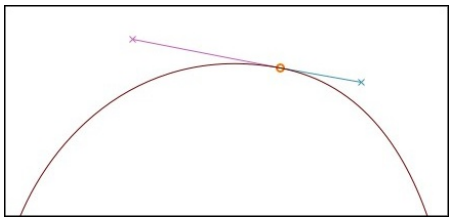
Инструменты точек

Панель инструментов для точек кривых, угловых и касательных выглядит следующим образом:



Точки кривой (круглой формы)

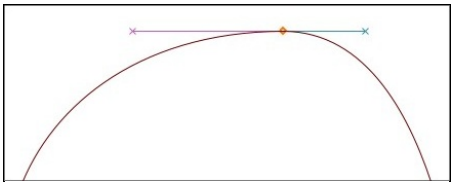
У каждой точки кривой присутствуют две ручки, их расположение связано между собой таким образом, что линия, соединяющая их, всегда остаётся прямой, обеспечивая создание плавной кривой с обеих сторон.



Точка кривой позволяет добавить новую точку на контуре.

Точки H / V кривой (точки в форме ромба)

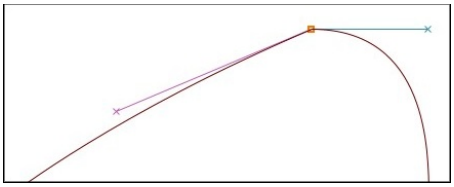
Точки H/V кривой (горизонтальные/вертикальные) представляют собой специальный тип точек кривой, которые привязаны к горизонтальной или вертикальной оси, что является важным условием для корректного формирования кривых Безье.



Инструмент *Точки H/V кривой* позволяет добавить новую точку на контуре.

Угловые точки (точки квадратной формы)

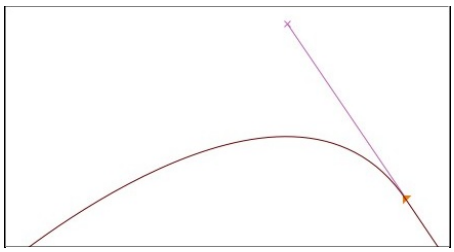
Каждая точка может содержать 0, 1 или 2 маркера Безье, причем каждая ручка может быть установлена независимо от других, что позволяет создавать разрывы в контуре. Без маркеров точки будут иметь прямые линии.



Угловая точка создает резкий изгиб контура.

Точки касательной (точки треугольной формы)

Каждая точка может содержать 0, 1 или 2 маркера Безье, причем каждая ручка может быть установлена независимо от других, что позволяет создавать разрывы в контуре. Без маркеров точки будут иметь прямые линии.



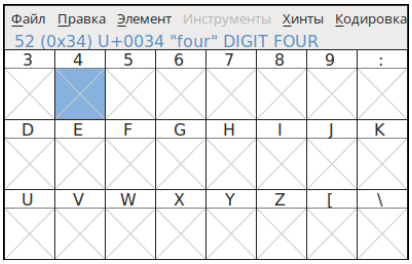
Точка касания позволяет перейти от прямого сегмента к изогнутому вдоль контура.

Глифы

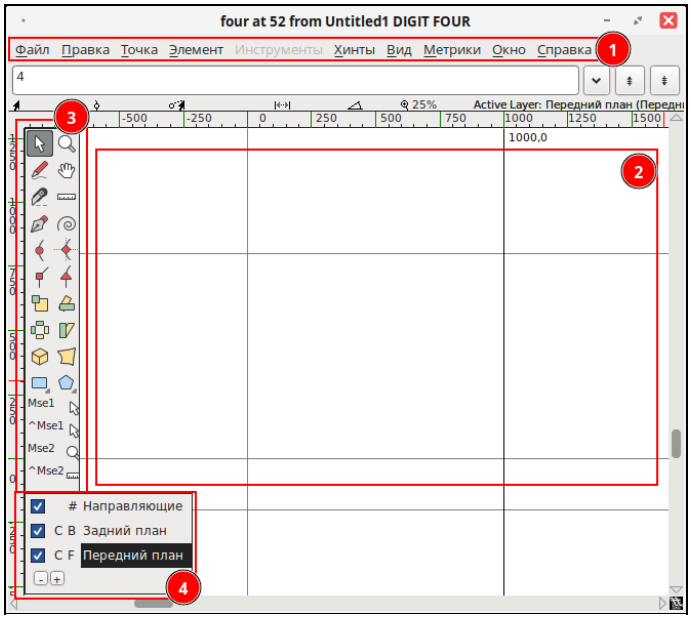
Для редактирования глифа необходимо дважды кликнуть по полю, при этом будет открыто окно **Character View**. Здесь можно рисовать и редактировать глифы двумя способами:

- один за другим при помощи интерфейса со вкладками;

- параллельно с подготовленным текстовым файлом слов.



Окно **Character View** выглядит следующим образом:



В верхней части окна находится основное меню (**1**), где доступны все действия по работе с **FontForge**.

Окно для рисования (**2**) предназначено для создания символов в определённом стиле.

Панель инструментов (**3**) предоставляет основные действия для работы со шрифтом.

Панель инструментов для слоев (**4**) предоставляет возможность отображения/скрытия при работе определенного слоя.

Инструменты рисования

Инструмент «**Указатель**» ( ) позволяет выделять и перемещать точки контура или сами контуры символа. Выделение производится щелчком по нужным точкам/контурам или выделением при нажатой ЛКМ области, содержащей нужные точки. Также щелчком можно выделить правую границу символа. Добавление или исключение точек производится при нажатой клавише *Shift*.

Инструмент «**Лупа**» ( ) позволяет изменять масштаб в окне символа. Увеличение производится щелчком в окне символа (или с использованием горячей клавиши *Z*), уменьшение — щелчком при нажатой клавише-модификаторе *Alt* (или с использованием горячей клавиши *X*).

Инструмент «**Свободное рисование**» ( ) позволяет создавать неровные контуры. Для рисования зажмите ЛКМ в области рисования, затем проведите необходимые линии. После этого вернитесь к инструменту «**Указатель**», чтобы выделить точки на нарисованном контуре. При выборе точки контура она подсвечивается желтым цветом. Можно также выбрать и переместить контрольные точки, чтобы изменить форму кривой.

Инструмент «**Перо**» ( ) позволяет добавить точку на кривой и переместить ее контрольные точки.

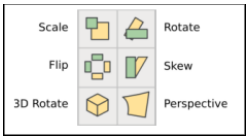
Инструмент «**Спиро**» ( ) активирует режим рисования spi-кривых, который позволяет создавать кривые, изменяющие форму при перемещении узлов.

Инструмент «**Нож**» ( ) позволяет разрезать контур между точками. На образующихся концах контура создаются две новые точки кривых, между которыми нет соединения. Чтобы разрезать контур, надо провести курсор в точке разреза, удерживая нажатой ЛКМ. Может оказаться полезным, если для дальнейшей работы требуется только часть нарисованной фигуры.

Инструмент «**Линейка**» ( ) позволяет измерять расстояние, угол и смещение по осям *X* и *Y* от точки, где была отпущена ЛКМ до текущего положения курсора. При использовании отображается "всплывающая подсказка" рядом с курсором, предоставляющая более подробные сведения об измерениях и координатах.

Инструменты преобразования

Панель инструментов преобразования выглядит следующим образом:



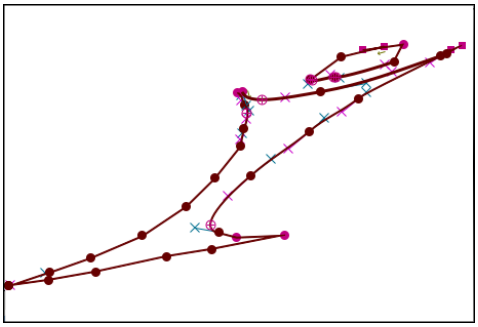
При двойном клике по любому инструменту трансформации можно ввести числовые значения. Инструмент «**Масштабирование**» (*Scale*) позволяет изменять масштаб объекта вручную с возможностью сохранения пропорций при удержании клавиши *Shift*.

Инструмент «**Поворот**» (*Rotate*) используется для произвольного вращения объекта вокруг начальной точки нажатия мыши.

Инструмент «**Поворот в 3D**» (*3D rotate*) позволяет вращать объект в 3D и отображать результат на плоскости *XY*.

Инструмент «**Отразить**» (*Flip*) отражает выделение по горизонтали или вертикали с использованием точки начального нажатия мыши в качестве центра преобразования.

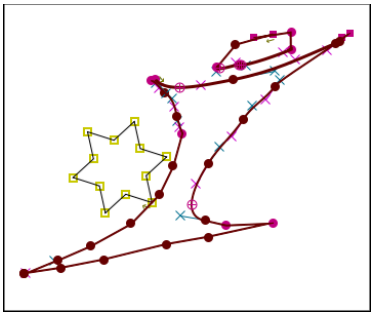
Инструмент «**Наклонить**» (*Skew*) позволяет наклонить фигуру.



Инструменты Прямоугольник, Эллипс, Многоугольник, Звезда

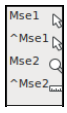
Инструменты позволяют быстро рисовать примитивные геометрические фигуры, без необходимости построения их из отдельных отрезков линий. Чтобы переключиться на альтернативный инструмент, щелкните по зоне шеврона в этих инструментах, а для открытия параметров формы выполните двойной щелчок.

Для прямоугольника можно настроить углы и ограничивающую рамку, для эллипса – ограничивающий прямоугольник или центрирование, для многоугольника можно задать количество вершин, а для звезды – количество точек и их глубину в процентах.



Действия кнопок мыши

Панель инструментов для действий кнопок мыши выглядит следующим образом:



На панели инструментов можно просмотреть текущий инструмент и доступные операции для кнопок мыши:

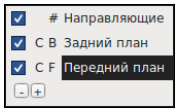
- ЛКМ (*Mse1*);
- *Ctrl* + ЛКМ (*^Mse1*);

- Кнопка колесика мыши (*Mse2*);
- *Ctrl* + Кнопка колесика мыши (*^Mse2*).

Так можно использовать несколько различных инструментов, не прибегая к многократному поиску на панели инструментов.

Слои

Панель инструментов для слоев выглядит следующим образом:



Холст в **FontForge** имеет три слоя: направляющий, задний план и передний план. Направляющие слои предназначены для вставки направляющих, для рисования используются передний и задний план. Для создания окончательного шрифта будет использован только верхний слой переднего плана.

Активный флаг показывает видимость каждого слоя. Флаг можно снять, чтобы сделать слой невидимым. Символы *C* (или *Q*) показывают, какие кривые используются – кубические или квадратные, символы *#*, *B* или *F* указывают тип каждого слоя. Дополнительные слои можно создавать или удалять с помощью кнопок «**+**» или «**−**» на панели. Типом слоя и кривой также можно управлять щелчком правой кнопки мыши (при наличии дополнительных слоев).

Аудиоплеер Audacious

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** audacious-4.0.5-1

Audacious — аудиоплеер с открытым исходным кодом. Позволяет перетаскивать папки и отдельные аудио-файлы в окно плеера, искать исполнителей и альбомы во всей музыкальной библиотеке или создавать и редактировать собственные списки воспроизведения, а также слушать компакт-диски или трансляции музыки из Интернета.

В **audacious** есть возможность настраивать звук с помощью графического эквалайзера или изменять динамический диапазон с помощью звуковых эффектов. С помощью подключаемых модулей **audacious** способен извлекать тексты аудио-файлов, отображать уровень громкости, а с помощью «скинов» позволяет изменять внешний интерфейс, например, на **Winamp Classic**.

Для установки **audacious** перейдите в сеанс пользователя **root**:

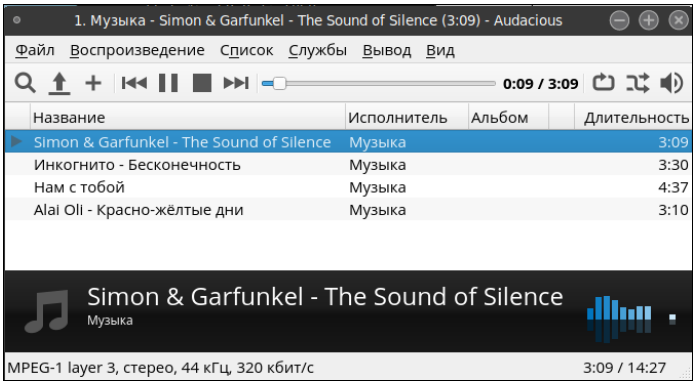
```
su -
```

и выполните команду:

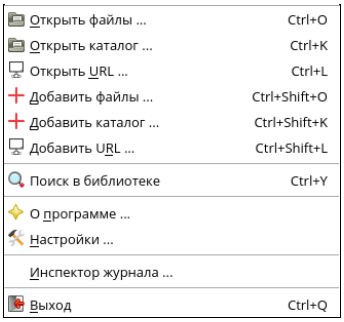
```
dnf install audacious
```

Далее работа в программе выполняется с правами локального пользователя.

После установки аудио-проигрыватель будет доступен из «**Главного меню**» - «**Аудио и видео**» - «**Audacious**».

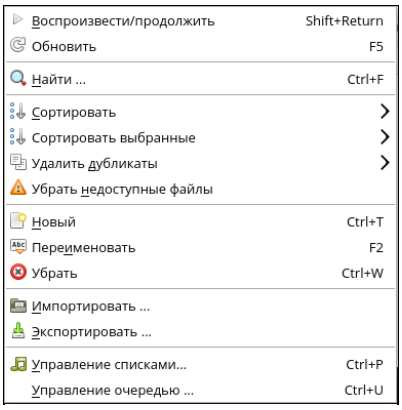


Из пункта меню «**Файл**» доступны базовые функции для добавления отдельных аудиозаписей и каталогов, а также URL списков трансляции медиа-потока из Интернета.



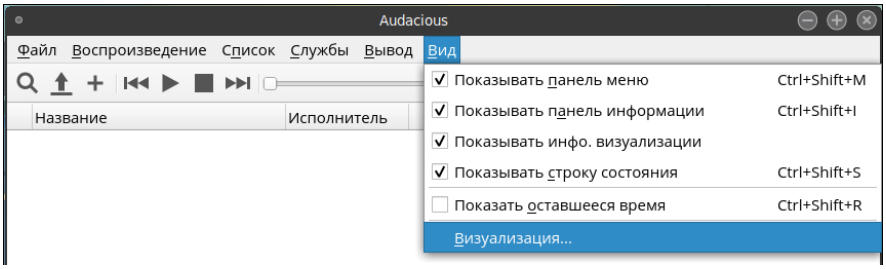
Функции пункта меню «**Воспроизведение**» интуитивно простые, элементы управления («**Воспроизведение**», «**Пауза**», «**Стоп**» и др.) представлены на верхней панели проигрывателя, также есть возможность включить повтор конкретного трека или перемешать все треки в списке аудиозаписей.

Из пункта меню «**Список**» можно создавать и управлять своими списками аудио. Здесь доступны функции сортировки, поиска определенного трека из списка, удаление дубликатов, а также экспорт и импорт списка.

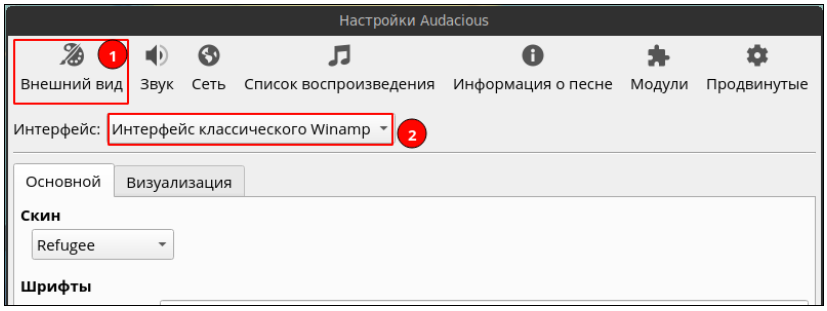


Также в Audacious есть возможность изменить вид приложения под классический интерфейс проигрывателя **Winamp**, для этого необходимо:

- Открыть пункт меню «**Вид**»;
- Выбрать пункт «**Визуализация**»;



- Далее открыть вкладку «**Внешний вид**»;
- И параметре «**Интерфейс**» выбрать «**Интерфейс классического Winamp**».



В результате изменится внешний вид приложения **Audacious**.



AlsaMixer - настройка звуковых карт

Навигация в программе
Настройка звука с помощью AlsaMixer
Настройка микрофона с помощью AlsaMixer
Решение возникающих проблем

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: alsa-utils-1.2.7-1

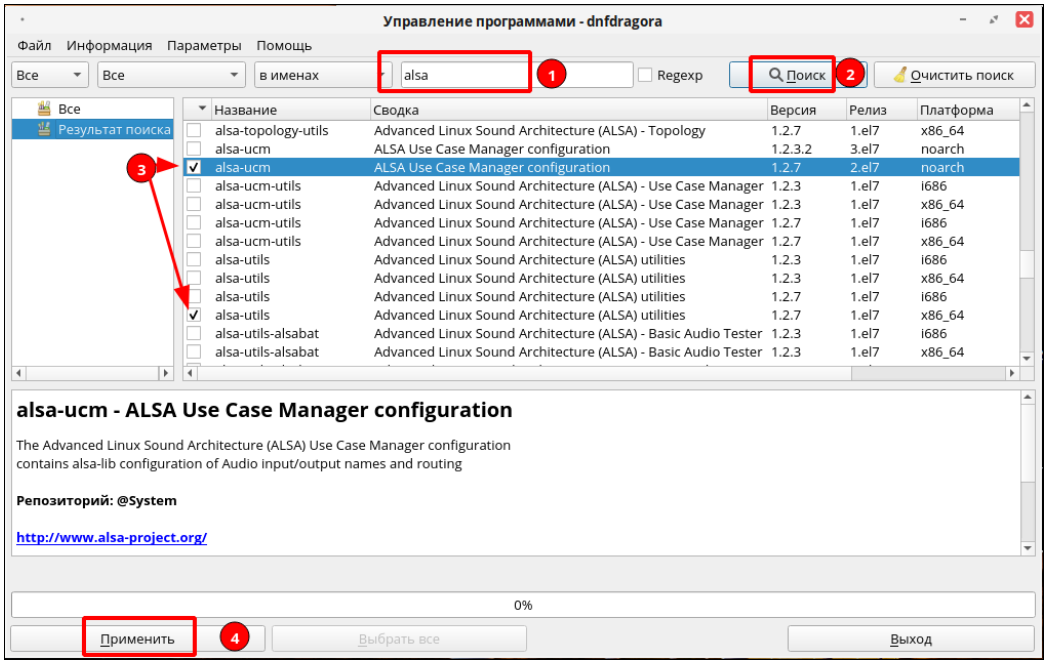
AlsaMixer — это псевдографическое приложение для просмотра и управления свойствами звуковых карт, установленных на компьютере.

В РЕД ОС **AlsaMixer** установлен по умолчанию и запускается с помощью команды с правами локального пользователя:

```
alsamixer
```

Однако, если на вашем компьютере приложение по каким-либо причинам отсутствует, установить его можно двумя способами — через графический менеджер пакетов или через терминал.

Для установки приложения через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимых пакетов по ключевому слову «**alsa**» и отметьте флагом пакеты **alsa-utils**, **alsa-ucm** и **alsa-plugins-pulseaudio** последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Подтвердите транзакцию, нажав кнопку «**Хорошо**». Установка займет некоторое время, после успешной установки окно с транзакцией исчезнет. Сам пакет будет отмечен как установленный.

Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install alsa-utils alsa-ucm alsa-plugins-pulseaudio
```

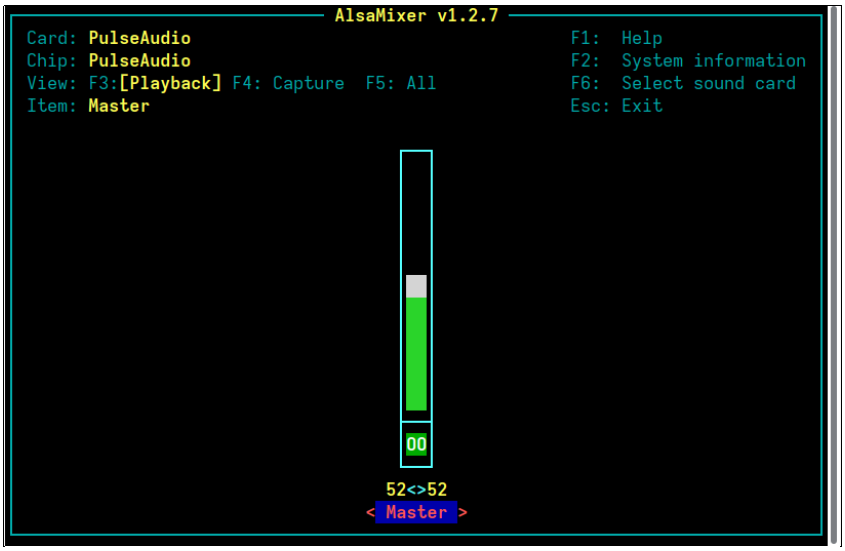
Дальнейшая работа в программе выполняется **от локального пользователя**.

Навигация в программе

После ввода команды запуска появится интерфейс программы с ползунком «**Master**», который управляет громкостью звуковых устройств по умолчанию. Можно управлять общим уровнем звука с помощью клавиш со стрелками вверх и вниз.

Также допускается управление отдельными звуковыми каналами:

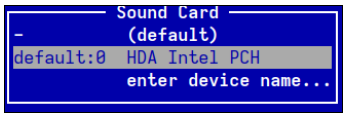
- **Q**, **Z** — для управления левым каналом;
- **E**, **C** — для управления правым каналом.



Слева вверху пользователю предоставляется информация о следующих параметрах устройства:

- **Card** — текущее звуковое устройство;
- **Chip** — драйвер звукового устройства;
- **View** — выбранный режим работы;
- **Item** — строка состояния выбранного параметра (чаще всего, показывает значения усиления в децибелах).

При нажатии клавиши **F6** появляется список звуковых устройств компьютера, в котором можно выбрать именно то устройство, которое нуждается в дополнительной настройке.

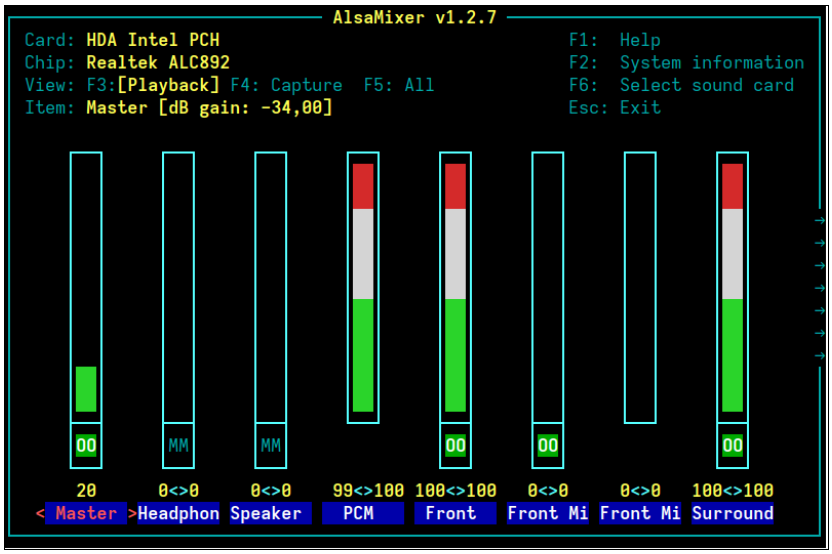


Также звуковую карту можно выбрать с помощью команды в консоли при запуске **AlsaMixer**:

```
alsamixer -c<b>N</b>
```

где **N** — целое число, обозначающее ID звукового устройства (по умолчанию имеет значение 0).

После выбора звуковой карты из списка количество настраиваемых параметров на экране заметно увеличится.



Переключаться между ползунками можно с помощью клавиш со стрелками вправо и влево. Для отключения параметра ползунка, нажмите клавишу **M**, тогда в нижней части ползунка надпись «**OO**» сменится на «**MM**», что и будет означать отключение ползунка (некоторые ползунки отключены по умолчанию).

По умолчанию программа запускается в режиме настройки воспроизведения. Если необходимо настроить микрофон или другие устройства ввода звука, следует переключится в режим настройки соответствующих устройств с помощью клавиши **F4**. Также с помощью клавиши **F5** можно перейти в общий режим, в котором объединены ползунки для настройки воспроизведения и ввода звука. Вернуться в режим настройки только устройств воспроизведения можно нажатием клавиши **F3**. Переключение между режимами также доступно с помощью клавиши **Tab**.

Настройка звука с помощью AlsaMixer

В зависимости от устройства количество настраиваемых свойств может меняться. Среди общих параметров всех устройств можно выделить следующие:

- **Master** — отвечает за весь вывод звука вне зависимости от устройства, за исключением параметра **Master Mono**. Обычно не должен быть отключён;
- **Headphone** — отвечает за вывод звука устройств, подключённых к передней панели компьютера;
- **Headphone Jack Sense** — если этот параметр включён, то все звуковые выходы отключаются при подключении устройства к передней панели компьютера;
- **PCM** — отвечает за воспроизведение всех звуковых и видео файлов. Отключить его нельзя, но важно следить, чтобы усиление этого параметра не превышало **0 dB**;
- **External Amplifier** — отвечает за воспроизведение звука источников с дополнительным питанием (например, колонки).

Настройка микрофона с помощью AlsaMixer

Ключевые параметры настройки захвата аудио меняются в зависимости от установленного устройства. Чаще всего при настройке микрофона необходимо настраивать следующие параметры:

- **Capture** — параметр, отвечающий за чувствительность микрофона;
- **Mic Boost** — позволяет дополнительно увеличивать чувствительность микрофона;
- **Input Source** — определяет, с какого входа будет захватываться звук (с передней панели или напрямую, с материнской платы).

Решение возникающих проблем

Alsamixer не определяет звуковую карту

Необходимо обновить ядро системы и пакеты **alsa**. Для этого воспользуйтесь нашей инструкцией «Обновление ядра Linux до версии 5.15 в РЕД ОС 7.3».

Обновить **AlsaMixer** можно командой:

```
dnf update alsa-utils
```

Нет звука

Убедитесь, что ползунки «**Master**» и «**PCM**» не отключены.

Также в некоторых случаях помогает установка дополнительного пакета **alsa-sof-force**. Установить его можно командой в терминале:

```
dnf install alsa-sof-force
```

Искажение звука

Убедитесь, что усиление параметра «**PCM**» не превышает **0**.

Ошибка при запуске AlsaMixer

Убедитесь, что запуск программы **AlsaMixer** производится от имени локального пользователя, а **не** от пользователя **root**.

Если же вы сталкиваетесь с ошибкой вида:

```
alsamixer: сбой функции snd_ctl_open по умолчанию: такого устройства нет
```

необходимо вручную выбрать устройство, которое будете настраивать программой **AlsaMixer**, с помощью команды:

```
alsamixer -c**N**
```

где **N** — целое число, обозначающее ID звукового устройства (по умолчанию имеет значение 0).

Если вы подключили к компьютеру альтернативную или внешнюю звуковую карту, можно открыть её настройки, обращаясь к устройству по имени. Например:

```
alsamixer -c usb
```

hdajackretask - управление портами звуковых устройств

hdajackretask — графическая утилита, предназначенная для управления портами звуковых устройств на звуковых картах *HDA Intel*. **hdajackretask** входит в набор **alsa-tools**.

Для установки **alsa-tools** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

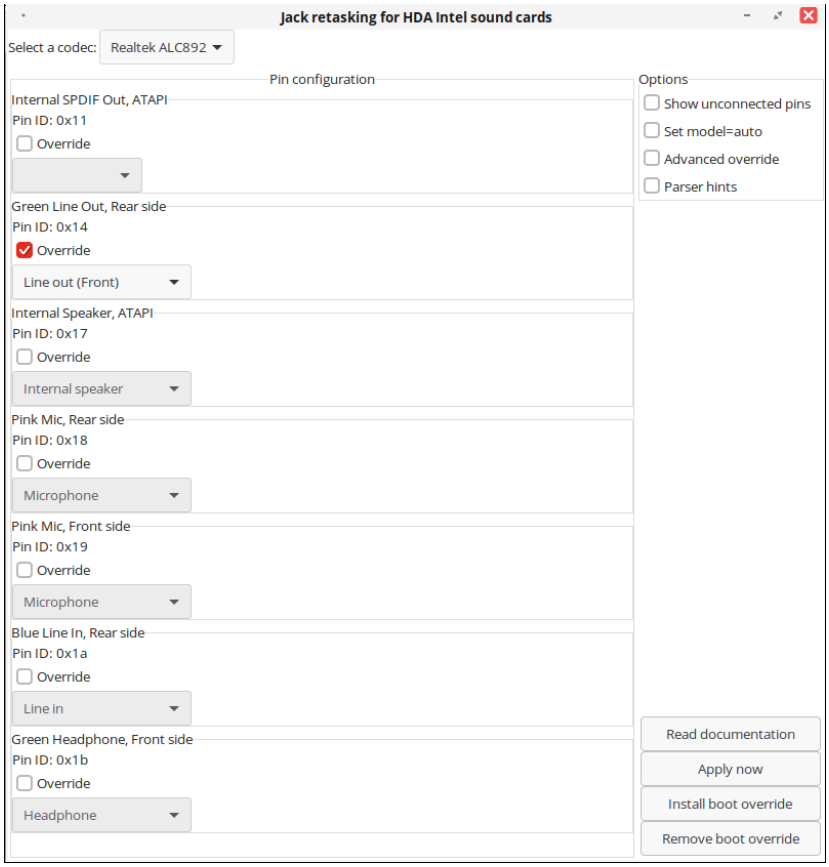
```
dnf install alsa-tools
```

Дальнейшая работа в программе выполняется с правами **локального пользователя**.

После установки **hdajackretask** доступен из «**Главного меню**» — «**Аудио и Видео**» — «**HDAJackRetask**» или из терминала командой:

```
hdajackretask
```

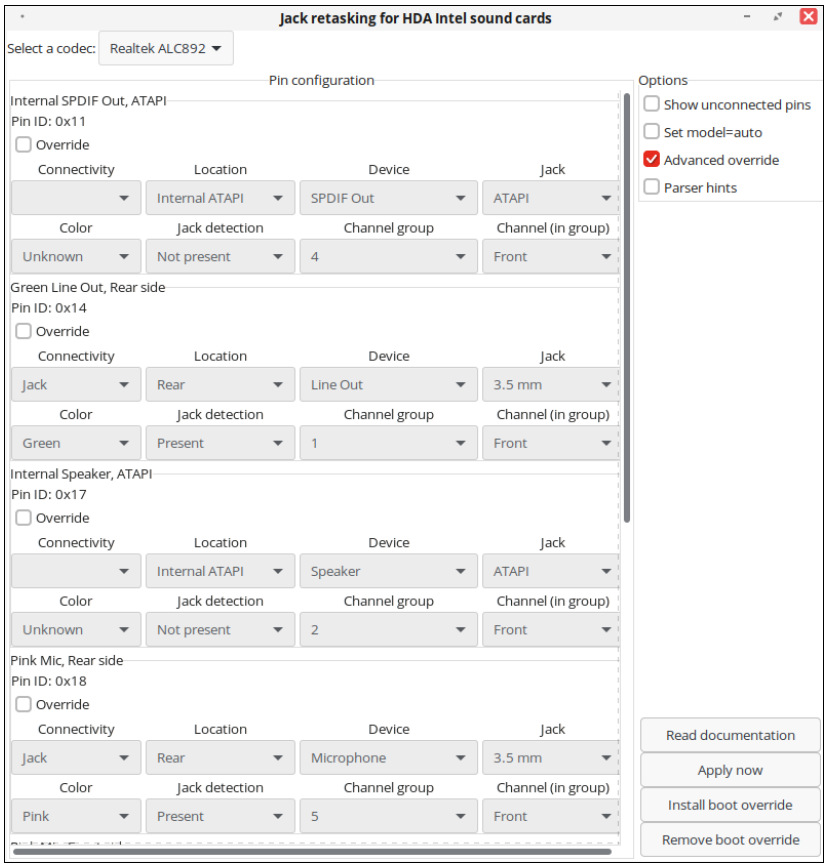
Окно программы выглядит следующим образом:



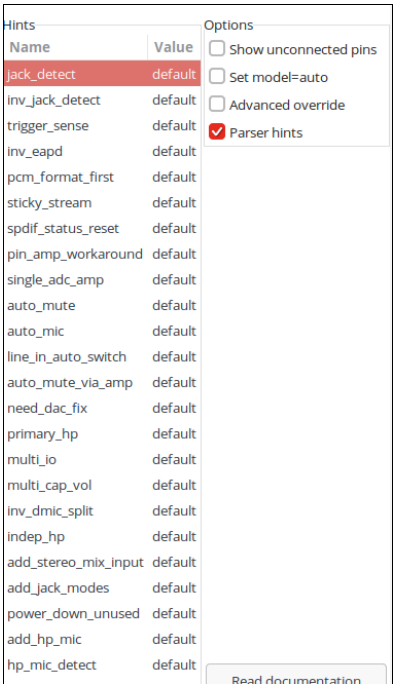
На верхней панели окна программы есть возможность выбрать используемый кодек звуковой карты. Как правило, к звуковым устройствам компьютера относится только первый кодек в выпадающем списке, а остальные кодеки относятся к HDMI.

В разделе «**Options**» находятся дополнительные настройки, влияющие как на работу звукового оборудования, так и на количество параметров, редактируемых в разделе «**Pin configuration**». Рассмотрим их подробнее:

1. **Show unconnected pins** — BIOS компьютера иногда может давать сбой и не показывать по умолчанию все существующие порты. В таком случае можно попробовать установить флаг для этой настройки, тогда в разделе «**Pin configuration**» появятся новые порты, которые физически могут отсутствовать в вашей системе, но существует большая вероятность появления необходимого для работы порта.
2. **Set model = auto** — некоторые кодеки, особенно старые, игнорируют переопределения, созданные пользователем в программе. Во многих подобных случаях помогает установка флага для этого параметра. Однако существует вероятность, что звуковая карта не примет новые параметры в том случае, если она является устаревшей или установленное в системе ядро имеет версию 3.8 или ниже.
3. **Advanced override** — расширенный режим, который открывает доступ к дополнительным параметрам каждого порта. Не рекомендуется для неопытных пользователей. Прежде чем изменять расширенные параметры портов, необходимо ознакомиться со спецификацией *Intel High-Definition Audio*.



4. **Parser hints** — позволяет пользователю отправлять специальные «подсказки» для драйвера, которые помогают избежать конфликтов или несовпадений между конфигурациями BIOS и драйверами звуковой карты. Для неопытных пользователей, которые не ознакомлены с документацией к драйверу, рекомендуется оставлять значения всех параметров «**default**».



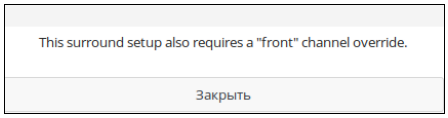
Все настройки портов находятся в графе «**Pin configuration**», которая представляет собой список всех портов, которые смог обнаружить BIOS компьютера. Каждый порт в стандартном виде имеет всего один параметр — тип устройства, которое будет с ним работать. Обычно предлагаемые устройства можно разделить на следующие группы:

- **Line Out** — активные устройства для вывода звука. Например, колонки, которым нужен дополнительный источник питания. Как правило, на такие устройства звук выводится с большим усилением;
- **Line In** — устройства для ввода звука;
- **Internal speaker / mic** — встроенный динамик/микрофон на материнской плате ПК;
- **Headphones** — устройства для вывода звука, которые не требуют дополнительного источника питания. На такие устройства

звук выводится с меньшим усилением, чем на устройствах типа **Line Out**.

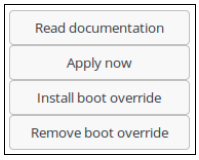
Для того чтобы иметь возможность редактировать параметры, следует пометить порт как переопределяемый (установить на нём флаг **Override**).

Важно учитывать, что если попытаться переопределить устройство **Line Out (Back)**, то обязательно нужно переопределить или пометить как переопределяемое устройство **Line Out (Front)**. Если попытаться переопределить устройство **Line Out (Center/LFE)**, то необходимо переопределить или пометить как переопределяемые устройства **Line Out (Back)** и **Line Out (Front)**. При игнорировании этих условий, если пользователь попытается принять изменения, программа выдаст ошибку следующего вида:



В правом нижнем углу окна программы находятся четыре кнопки, которые отвечают за следующие функции:

- **Read documentation** — вызывает окно с краткой инструкцией по работе в программе;
- **Apply now** — применяет изменения, внесённые пользователем. После перезагрузки компьютера изменения не сохраняются;
- **Install boot override** — сохраняет изменения в загрузочном секторе компьютера, чтобы они сохранялись даже после перезагрузки;
- **Remove boot override** — удаляет информацию об изменениях в загрузочном секторе компьютера. При следующем включении компьютера все параметры загружаются со значениями по умолчанию.



Настройка звука с помощью PulseAudio

Настройка звука с помощью графического интерфейса PulseAudio
Настройка звука с помощью pavucontrol
Настройка звука с помощью PulseAudio через терминал

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pulseaudio-15.0-2, pavucontrol-3.0-6

PulseAudio — кроссплатформенный звуковой сервер, созданный в качестве улучшенной замены таких серверов, как ESD, ARts.

PulseAudio принимает звук от одного или нескольких источников (процессов или устройств) и направляет одному или нескольким приёмникам (звуковым платам, серверам PulseAudio или процессам). Одной из основных целей проекта является предоставление возможности перенаправления любых звуковых потоков, включая и потоки от процессов, требующих прямого доступа к аудиоустройствам. Это достигается с помощью специальных псевдоустройств, работающих непосредственно с другими звуковыми системами, такими как aRts или ESD.

В РЕД ОС пользователь может настроить систему ALSA так, чтобы она использовала виртуальное устройство, созданное сервером **PulseAudio**. Тогда программы, работающие со звуком через драйвер ALSA, будут на самом деле работать с **PulseAudio**, который взаимодействует с помощью ALSA уже с реальным устройством.

Основные возможности:

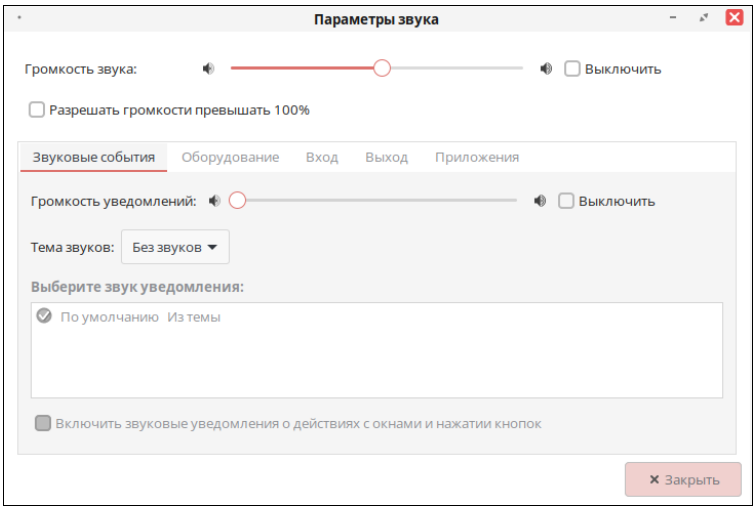
- раздельная установка уровней громкости для разных программ;
- смешивание потоков от разных звуковых плат;
- расширяемая модульная система с поддержкой динамически загружаемых библиотек;
- совместимость со многими популярными аудиоприложениями;
- работа с несколькими источниками и приёмниками звука;
- приемлемая для повседневного непрофессионального использования задержка и возможность ею управлять;
- использование технологии zero-copy, сберегающей машинное время;
- интерфейс командной строки с возможностью использования сценариев;
- демон, перенастраиваемый с помощью командной строки;
- встроенное преобразование аудиоформатов;
- синхронизация потоков воспроизведения;
- смешиваемые потоки могут иметь разные частотные характеристики;
- эффективный микшер, даже для звуковых плат без микшера, предотвращающий «монополизацию» звукового устройства отдельной программой.

Настройка звука с помощью графического интерфейса PulseAudio

Работа с утилитой

Утилита настройки звука доступна из «**Главного меню**» — «**Параметры**» — «**Звук**». Также открыть утилиту можно, нажав ПКМ на иконку регулировки громкости и выбрав пункт «**Параметры звука**».

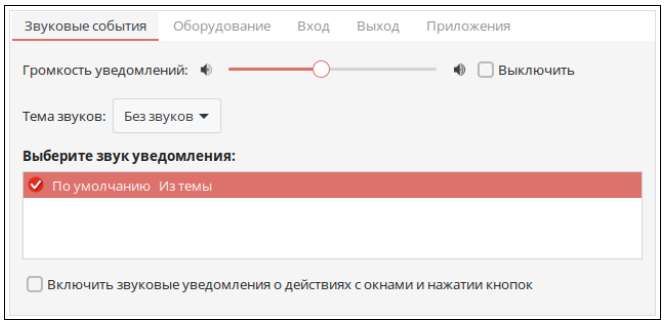
Окно программы выглядит следующим образом:



В верхней части окна находится регулировка громкости звука, флаг полного выключения звука и флаг увеличения максимального порога громкости до 150%.

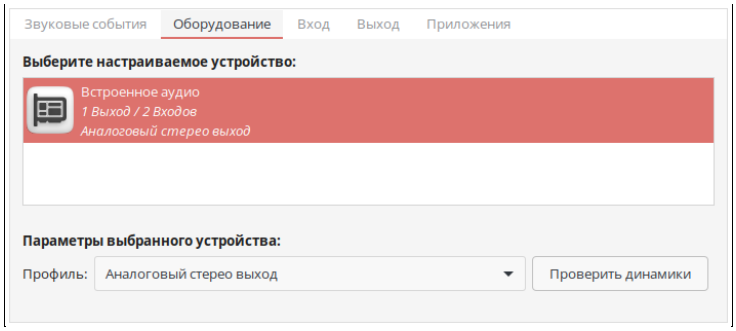
Вкладка «Звуковые события»

На вкладке «**Звуковые события**» можно выбрать тему звуковых событий, а также их громкость.



Вкладка «Оборудование»

В графе «**Выберите настраиваемое устройство**» можно выбрать звуковую карту для настройки.



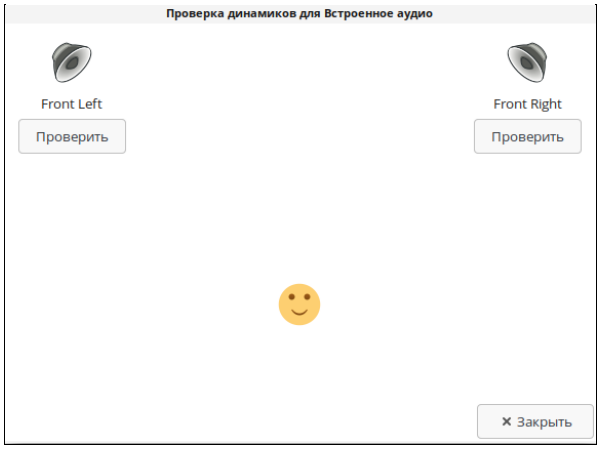
Главным параметром для настройки выбранной звуковой карты является выпадающий список «**Профиль**», в котором доступен выбор режима работы звукового устройства. Утилита предлагает на выбор следующие виды звуковых профилей:

- *Аналоговый стерео дуплекс* — работает с устройствами ввода и вывода звука одновременно;
- *Аналоговый стерео выход* — работает только с устройствами вывода звука;
- *Аналоговый стерео вход* — работает только с устройствами ввода звука;
- *Цифровой стерео выход* — позволяет получать более высокое качество звука, но не все устройства способны поддерживать этот режим;
- *Цифровой стерео выход + Аналоговый стерео вход* — позволяет использовать аналоговые устройства ввода звука одновременно с цифровыми устройствами вывода звука;
- *Выключено* — отключает звуковое устройство.

Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.

При нажатии на кнопку «**Проверить динамики**» появляется окно, позволяющее воспроизводить тестовые звуковые дорожки в различных каналах, количество которых зависит от звукового устройства.

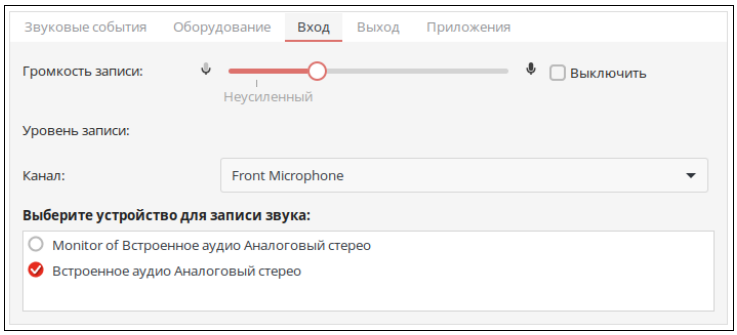


При нажатии кнопки «**Проверить**» рядом с иконкой по выбранному каналу будет воспроизведена звуковая дорожка. Например, при использовании наушников и нажатии кнопки «**Проверить**» возле иконки «**Front Left**» воспроизводимую звуковую дорожку будет слышно только в левом наушнике.

Вкладка «Вход»

Параметр «**Громкость записи**» позволяет пользователю настраивать чувствительность микрофона под свои нужды.

В момент настройки можно наблюдать за уровнем чувствительности микрофона по шкале «**Уровень записи**».



Выпадающий список «**Канал**» предлагает на выбор следующие каналы для работы устройств ввода звука:

- *Front Microphone* — канал микрофона с порта на передней панели компьютера;
- *Rear Microphone* — канал микрофона с порта на материнской плате;
- *Line In* — канал для устройств ввода звука с дополнительного порта на материнской плате. Отличительной особенностью от обычного канала для микрофона является более низкая чувствительность. Данный канал предназначен для электронных устройств, которые имеют возможность ввода звука в компьютер. Например, микшеры, синтезаторы, дрампады и др.

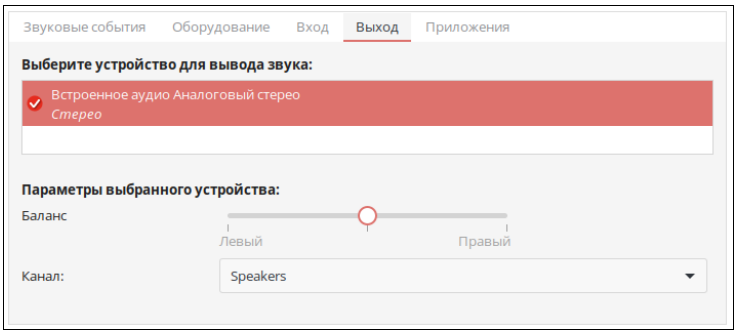
Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.

Последним пунктом настроек на этой вкладке является выбор устройства для записи звука. От выбранного устройства также зависит количество настроек на вкладке.

Вкладка «Выход»

В отличие от вкладки «**Вход**» список устройств для вывода звука предоставляется сразу. От выбранного устройства зависит набор настраиваемых параметров.



Настройка баланса позволяет отрегулировать громкость звучания в каналах относительно друг друга. Доступен следующий выбор каналов:

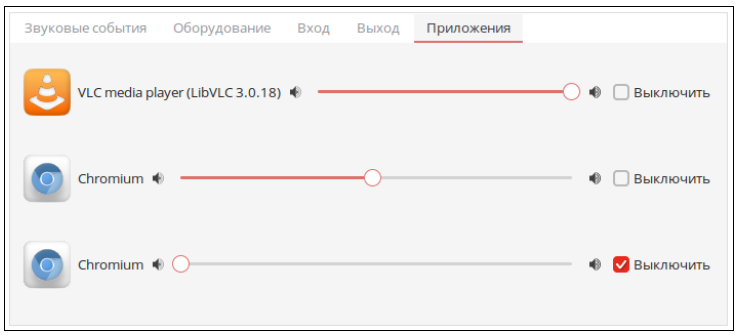
- *Speakers* — канал устройств вывода звука с порта на передней панели компьютера;
- *Headphones* — канал устройств вывода звука с порта на материнской плате;
- *Line Out* — канал устройств вывода звука с дополнительного порта на материнской плате без усиления. Чаще всего используется для подключения усилителей или активных колонок. На обычных устройствах звук будет очень тихим.

Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.

Вкладка «Приложения»

Данная вкладка позволяет установить громкость звучания для определённого приложения или отключить звук в нём совсем.



Настройка звука с помощью pavucontrol

Pavucontrol — это регулятор громкости для **PulseAudio** с расширенными возможностями.

Для его установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install pavucontrol
```

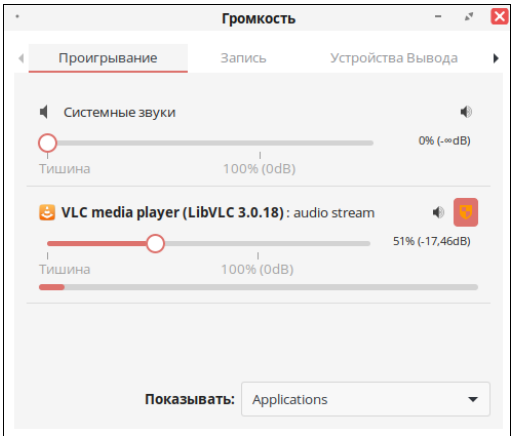
После установки запуск утилиты **pavucontrol** доступен из «**Главного меню**» — «**Аудио и Видео**» — «**Регулятор громкости PulseAudio**» или через терминал командой:

```
pavucontrol
```

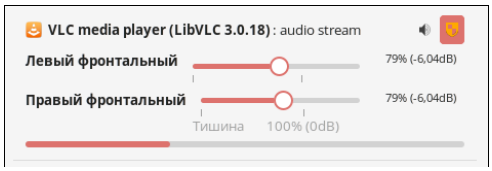
Программа представляет из себя окно с пятью вкладками: «**Проигрывание**», «**Запись**», «**Устройства вывода**», «**Устройства ввода**» и «**Конфигурация**».

Вкладка «Проигрывание»

Данная вкладка позволяет регулировать уровень громкости запущенных приложений и системных звуков независимо друг от друга.



Для системных звуков доступен только ползунок регулировки громкости. Для приложений дополнительно добавляются настройки амплитуды сигнала. При нажатии на иконку динамика () звук выбранного канала будет заглушен. Нажатие на иконку щита () позволяет регулировать звуковые каналы устройства по отдельности.

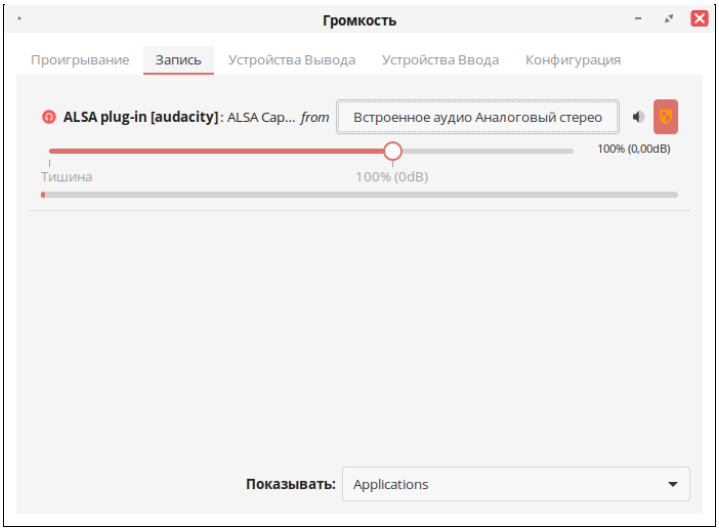


В нижней части окна есть выпадающий список, сортирующий выводимые на экран приложения. Список состоит из трёх пунктов:

- *Applications* — показывает потоки приложений в системе;
- Virtual Streams — показывает потоки виртуальных приложений;
- *All Streams* — показывает все звуковые потоки в системе.

Вкладка «Запись»

На этой вкладке можно настроить уровни чувствительности микрофона для каждого приложения в отдельности. Интерфейс по внешнему виду схож с интерфейсом во вкладке «**Проигрывание**». Каждое приложение с запущенной записью имеет свой ползунок для настройки чувствительности записи и показатель амплитуды сигнала.



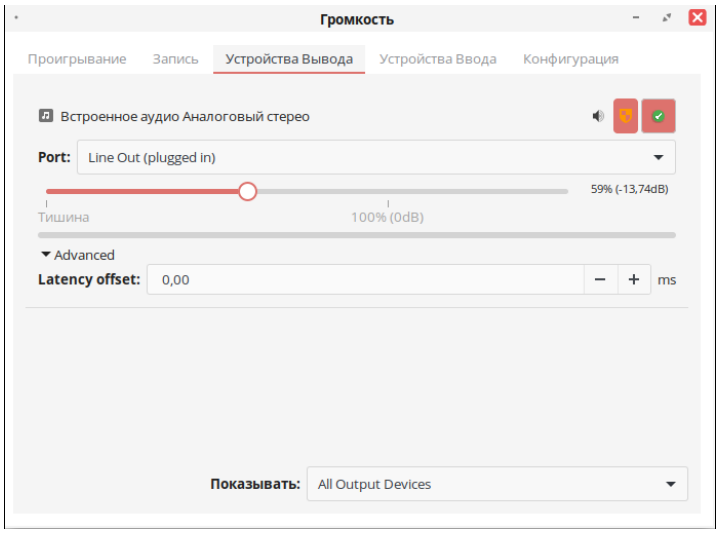
Нажатие на иконку динамика () останавливает запись звука в приложении. При нажатии на иконку щита () появляется возможность редактирования записи в разные каналы независимо друг от друга.

Выпадающий список «**Показывать**» предлагает те же параметры, что и на вкладке «**Проигрывание**».

Вкладка «Устройства вывода»

Вкладка «**Устройства вывода**» отвечает за настройку подключенных устройств для вывода звука. Для каждого подключенного устройства основным параметром для настройки является параметр **Port**. **Port** — позволяет выбрать, с какого порта будет работать

подключенное устройство. Например, **Line Out** отвечает за использование портов на материнской плате, а **Handphones** — портов на передней панели компьютера.



Звуковое устройство имеет ползунок для регулировки громкости, показатель амплитуды сигнала, иконку динамика ( ), чтобы заглушить звук, иконку щита ( ) для регулировки каналов устройства по отдельности. Также доступна кнопка «**Set As Fallback**» ( ), которая указывает на устройство, выбранное системой как устройство по умолчанию.

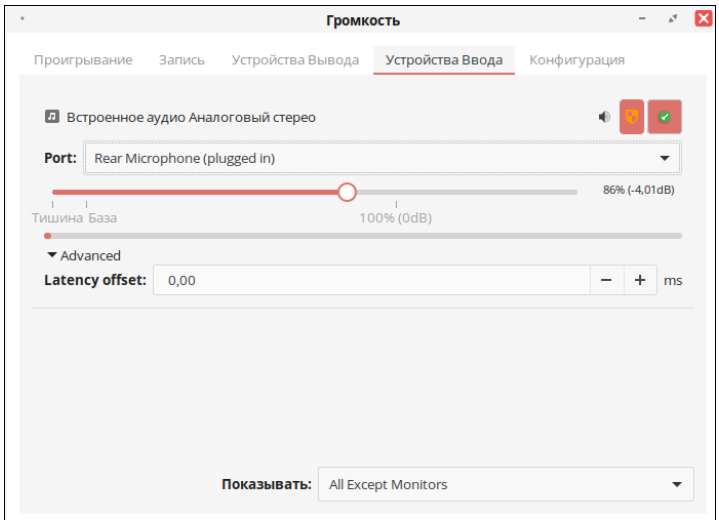
Параметр **Latency offset** отвечает за задержку воспроизведения звука. Он особенно полезен для тонкой настройки синхронизации между устройствами воспроизведения и устройствами ввода. Например, с помощью данной настройки можно избавиться от эффектов эха при разговорах по видеосвязи.

Выпадающий список «**Показывать**» имеет следующие варианты:

- *Hardware Output Devices* — показывает только физические устройства вывода;
- *Virtual Output Devices* — показывает только виртуальные устройства вывода;
- *All Output Devices* — показывает все устройства вывода.

Вкладка «Устройства ввода»

Вкладка для настройки устройств ввода схожа с содержимым вкладки «**Устройства вывода**» за исключением выпадающего списка «**Показывать**».



Выпадающий список «**Показывать**» имеет следующие параметры для сортировки звуковых устройств ввода:

- *Hardware Input Devices* — показывает только физические устройства ввода звука;
- *Virtual Input Devices* — показывает только виртуальные устройства ввода звука;
- *Monitors* — показывает только мониторы, подключённые через HDMI или DVI, т.к. они также являются звуковыми устройствами;
- *All Except Monitors* — показывает все устройства ввода звука, кроме мониторов;
- *All Input Devices* — показывает все устройства ввода звука.

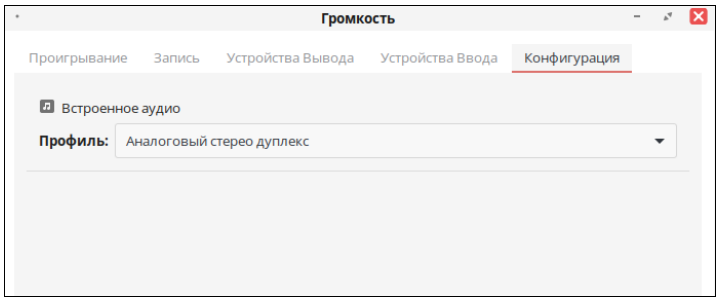
Вкладка «Конфигурация»

Вкладка «**Конфигурация**» содержит в себе только один параметр — **Профиль**. Выбор этого параметра работает аналогично такому же параметру в графическом интерфейсе **PulseAudio**:

- *Аналоговый стерео дуплекс* — работает с устройствами ввода и вывода звука одновременно;
- *Аналоговый стерео выход* — работает только с устройствами вывода звука;
- *Аналоговый стерео вход* — работает только с устройствами ввода звука;
- *Цифровой стерео выход* — позволяет получать более высокое качество звука, но не все устройства способны поддерживать этот режим;
- *Цифровой стерео выход + Аналоговый стерео вход* — позволяет использовать аналоговые устройства ввода звука одновременно с цифровыми устройствами вывода звука;
- *Выключено* — отключает звуковое устройство.

Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.



Настройка звука с помощью PulseAudio через терминал

Настраивать звуковые устройства с помощью **PulseAudio** через терминал можно с помощью утилиты **pactl**. Чтобы вывести на экран список всех звуковых устройств с полной информацией, необходимо выполнить команду:

```
pactl list
```

Список всех звуковых устройств может быть очень длинным, поэтому программе стоит уточнять, о каких конкретно устройствах вы хотите вывести информацию на экран. Для этого нужно указать тип устройства.

Для получения информации по устройствам ввода звука, используйте команду:

```
pactl list sources
```

Для получения информации по устройствам вывода звука, используйте команду:

```
pactl list sinks
```

```
[user@localhost ~]$ pactl list sinks
Аудиоприёмник №1
        Состояние: SUSPENDED
        Имя: alsa_output.pci-0000_00_1b.0.analog-stereo
        Описание: Встроенное аудио Аналоговый стерео
        Драйвер: module-alsa-card.c
        Спецификация отсчётов: s16le 2-канальный 4410
        Схема каналов: front-left,front-right
        Модуль-владелец: 20
        Звук выключен: нет
        Громкость: front-left: 38673 /  59% / -13,74 dB,   front-right: 38673 /
 59% / -13,74 dB
                баланс 0,00
        Базовая громкость: 65536 / 100% / 0,00 dB
        Мониторный источник: alsa_output.pci-0000_00_1b.0.analog-stereo.monitor
        Задержка: 0 мкс, настроено на 0 мкс
        Флаги: HARDWARE HW_MUTE_CTRL HW_VOLUME_CTRL DECIBEL_VOLUME LATENCY
        Свойства:
                alsa.resolution_bits = "16"
                device.api = "alsa"
                device.class = "sound"
                alsa.class = "generic"
                alsa.subclass = "generic-mix"
```

Важным параметром устройства, который следует запомнить, является «Имя». Имя устройства очень часто используется для настройки с помощью других команд.

Смена профиля работы звуковых устройств

Список доступных профилей можно посмотреть в информации к звуковой карте, для этого в терминале необходимо выполнить следующую команду:

```
pactl list cards
```

В строке «**Профиль**» отображаются доступные имена профиля и их краткие описания. Звуковые профили позволяют переключать количество активных выходов и входов на звуковой карте. Самым необходимым параметром профиля является его имя, оно указано в начале каждой строки.

```
    Профили:
            input:analog-stereo: Аналоговый стерео вход (аудиоприёмников: 0, источников: 1, приоритет: 32833, доступен: да)
            output:analog-stereo: Аналоговый стерео выход (аудиоприёмников: 1, источников: 0, приоритет: 39268, доступен: да)
            output:analog-stereo+input:analog-stereo: Аналоговый стерео дуплекс (аудиоприёмников: 1, источников: 1, приоритет: 39333, доступен: да)
            output:analog-surround-40: Аналоговый объёмный 4.0 выход (аудиоприёмников: 1, источников: 0, приоритет: 33968, доступен: да)
            output:analog-surround-40+input:analog-stereo: Аналоговый объёмный 4.0 выход + Аналоговый стерео вход (аудиоприёмников: 1, источников: 1, приоритет: 34033, доступен: да)
            output:iec958-stereo: Цифровой стерео (IEC958) выход (аудиоприёмников: 1, источников: 0, приоритет: 38268, доступен: да)
            output:iec958-stereo+input:analog-stereo: Цифровой стерео (IEC958) выход + Аналоговый стерео вход (аудиоприёмников: 1, источников: 1, приоритет: 38333, доступен: да)
            off: Выключено (аудиоприёмников: 0, источников: 0, приоритет: 0, доступен: да)
```

Для смены звукового профиля используется команда вида:

```
pactl set-card-profile <имя_карты> <имя_профиля>
```

Управление громкостью звуков

Громкость в **PulseAudio** регулируется командой вида:

```
pactl set-sink-volume <имя_устройства_вывода> <уровень_громкости>
```

Стоит отметить, что уровень громкости вводится от **0** до **65535** (от 0% до 100%). Если попытаться выставить громкость больше, чем на 65535, то звук будет выводится с усилением (и будет указываться больше, чем 100%). Слишком большое усиление может искажать звук.

Приостановка звука

Источник звука можно заглушить командой вида:

```
pactl suspend-sink <имя_источника> true
```

Вернуть звук из источника можно, поменяв значение последнего параметра с **true** на **false**:

```
pactl suspend-sink <имя_источника> false
```

Также последний параметр можно задавать целыми числами, где **1** — это *true*, а **0** — *false*.

Похожими действиями можно и приостановить запись из устройства ввода:

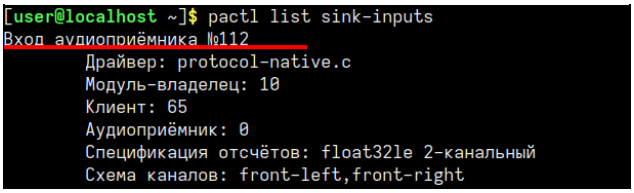
```
pactl suspend-source <имя_устройства_ввода> true
pactl suspend-source <имя_устройства_ввода> false
```

Громкость звука в приложениях

Чтобы изменять громкость звука для конкретного запущенного приложения, нужно сначала узнать для этого приложения номер входа аудиоприёмника (для приложений с проигрыванием звуков) или выход источника (для приложений с записью звука).

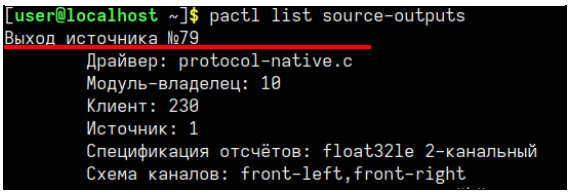
Чтобы узнать номера аудиоприёмников, в терминале необходимо выполнить команду:

```
pactl list sink-inputs
```

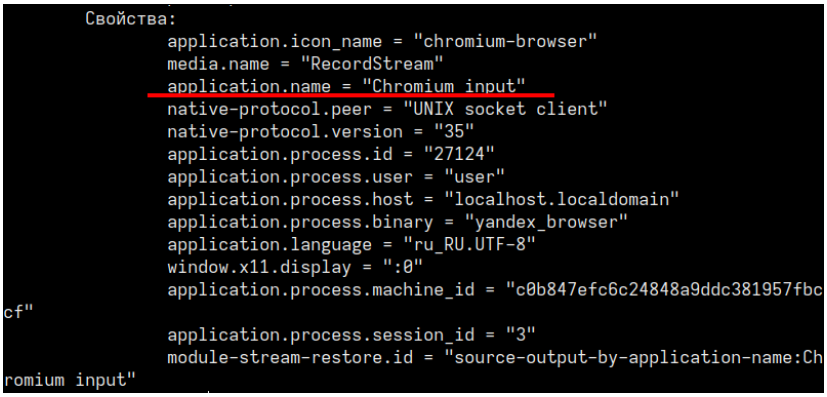


Для определения номера выхода источника команда будет выглядеть следующим образом:

```
pactl list source-outputs
```



У каждого входа аудиоприёмника и выхода источника есть свои свойства. Для определения номера конкретного приложения, следует обратить внимание на свойство «**application.name**», в котором указано название приложения:



Для регулировки звука следует использовать следующие команды:

```
pactl set-sink-input-volume <номер_входа_аудиоприёмника> <громкость_звука>
pactl set-source-output-volume <номер_выхода_источника> <громкость_звука>
```

Перемещение звукового потока

При необходимости перенести звук программы на другой источник звука (например, перенести звук с USB-колонок на наушники) можно воспользоваться следующей командой:

```
pactl move-sink-input <номер_входа_аудиоприёмника> <имя_источника>
```

Обратите внимание, что **pactl** не позволяет переносить звуки со всех приложений одновременно.

Audacity - редактор звуковых файлов

Установка
Описание программы
Запись звука
Сохранение результата
Звуковая дорожка
Обрезка треков
Объединение звука
Затухание и нарастание звука
Фильтрация шума

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** audacity-2.3.0-2

Audacity – мультиплатформенный редактор звуковых файлов, распространяемый на бесплатной основе.

Вы можете подробнее ознакомиться с работой редактора **audacity**, просмотрев наши обучающие видео:

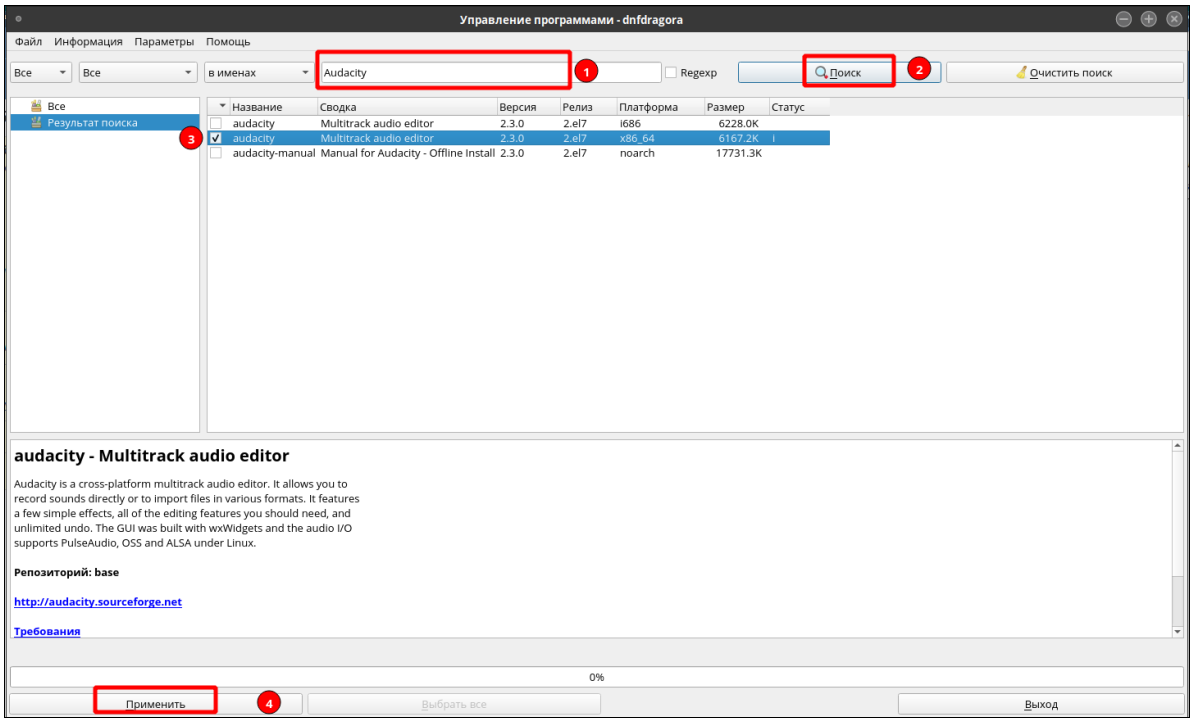
- на **RuTube** — Запись и обработка звука;
- в **Яндекс.Дзен** — Запись и обработка звука;
- в **VK Видео** — Запись и обработка звука.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**audacity**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install audacity
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

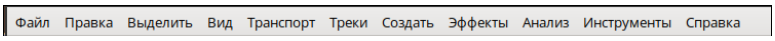
После установки программа будет доступна из «**Главного меню**» - «**Аудио и видео**» - «**Audacity**».

Описание программы

Звуковой редактор имеет простой и понятный интерфейс. В верхней части окна находятся кнопки управления записью, различные инструменты для работы и настройки устройств ввода. Все кнопки имеют поясняющие надписи, которые появляются при наведении курсора.

Рассмотрим их более подробно:

1. Вверху программы находится **основное меню** с доступными настройками как аудиодорожек, так и самой программы.



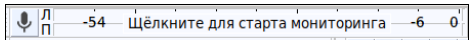
2. Крупными значками представлена **панель воспроизведения** с кнопками записи, начала воспроизведения, паузы и остановки, перехода в начало и конец трека.

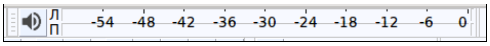


3. Следующая группа - **Инструменты** – выделение, масштабирование, отрисовка, сдвиг во времени и др.



4. **Индикация уровней звука** – сверху отражается уровень звука на входе (микрофон), снизу – на выходе (динамик).





5. **Панель отображения скорости воспроизведения**.



6. **Микшер** для управления параметрами звуковой карты. Правый устанавливает уровень сигнала на выходе (звуковая карта), а левый – на входе (микрофон).



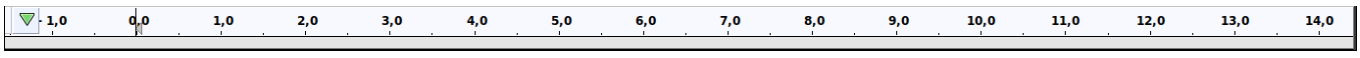
7. **Панель выбора устройств** - позволяет выбрать устройства, с которых будет вестись запись.



8. Раздел **Правка** – с помощью этой панели можно вырезать, копировать, заполнять тишиной выделенную зону, синхронизировать дорожки, масштабировать и др.



9. **Шкала времени** аудиодорожки.



Запись звука

Чаще всего **Audacity** используется для записи звука.

Перед записью необходимо выбрать устройство на **Панели выбора устройств**, с помощью которого будет записан аудиофрагмент, а затем запустить его мониторинг.

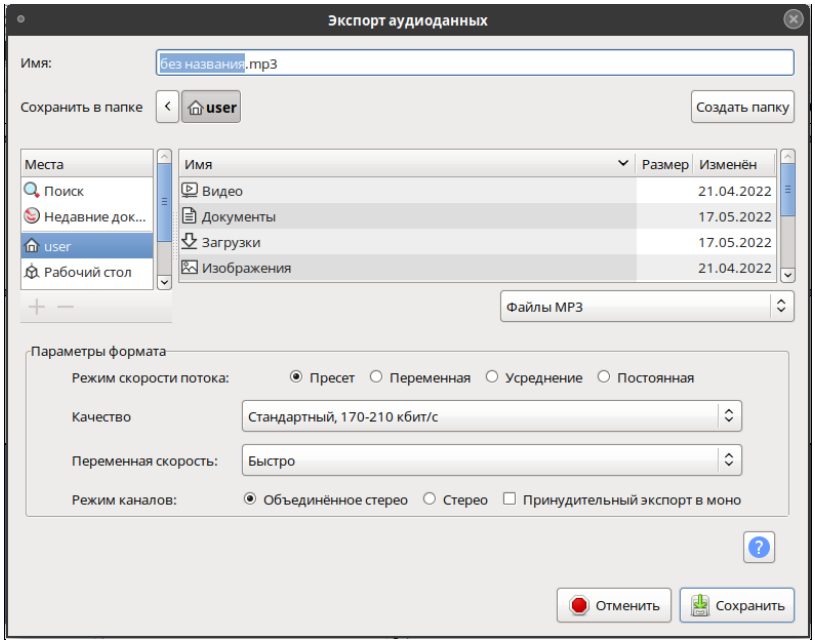
В выпадающем списке **Каналы записи** с **Панели выбора устройств** установите моно- или стереозапись.

Для начала записи нажмите на кнопку «**Запись**». После того как процесс окончен – нажмите «**Стоп**». Также запись можно приостановить, нажав на кнопку «**Пауза**», чтобы вскоре продолжить.

Прослушать записанный отрывок можно, нажав на кнопку «**Воспроизвести**».

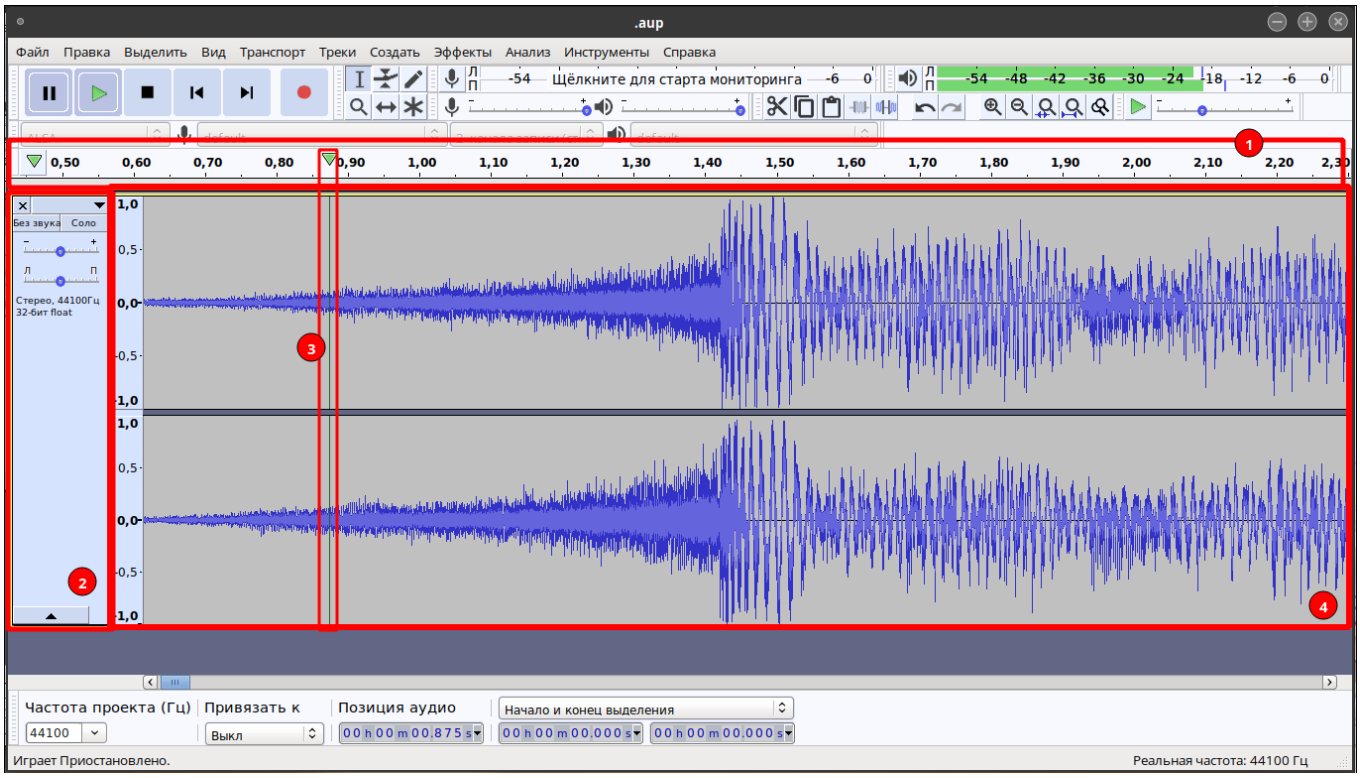
Сохранение результата

Для сохранения файла необходимо перейти в пункт меню «**Файл**» – «**Экспорт**», затем в открывшемся окне выбрать формат файла, качество, указать название и нажать кнопку «**Сохранить**».



Звуковая дорожка

Звуковая дорожка – это способ визуализации цифровой аудиозаписи. Она состоит из следующих компонентов:



1. **Шкала времени** – отображается вверху и показывает длительность трека.

2. **Свойства аудио** - здесь вы можете менять различные свойства аудиодорожки, отключается звучание текущей дорожки, изменяется вид её визуализации (волновая форма, спектр), цвета для окрашивания различных элементов трека. Также с помощью крестика вы

можете удалять композиции.

3. **Скруббер** – линия, которая отмечает текущую позицию, из которой начнётся проигрывание файла.

4. **Аудиодорожка** - визуализирует изменение сигнала на протяжении записи.

Любые дополнительные аудиодорожки будут расположены ниже.

Обрезка треков

Audacity позволяет вырезать фрагменты аудиофайлов. Для удобства можно изменить масштаб с помощью инструмента увеличить или уменьшить ().

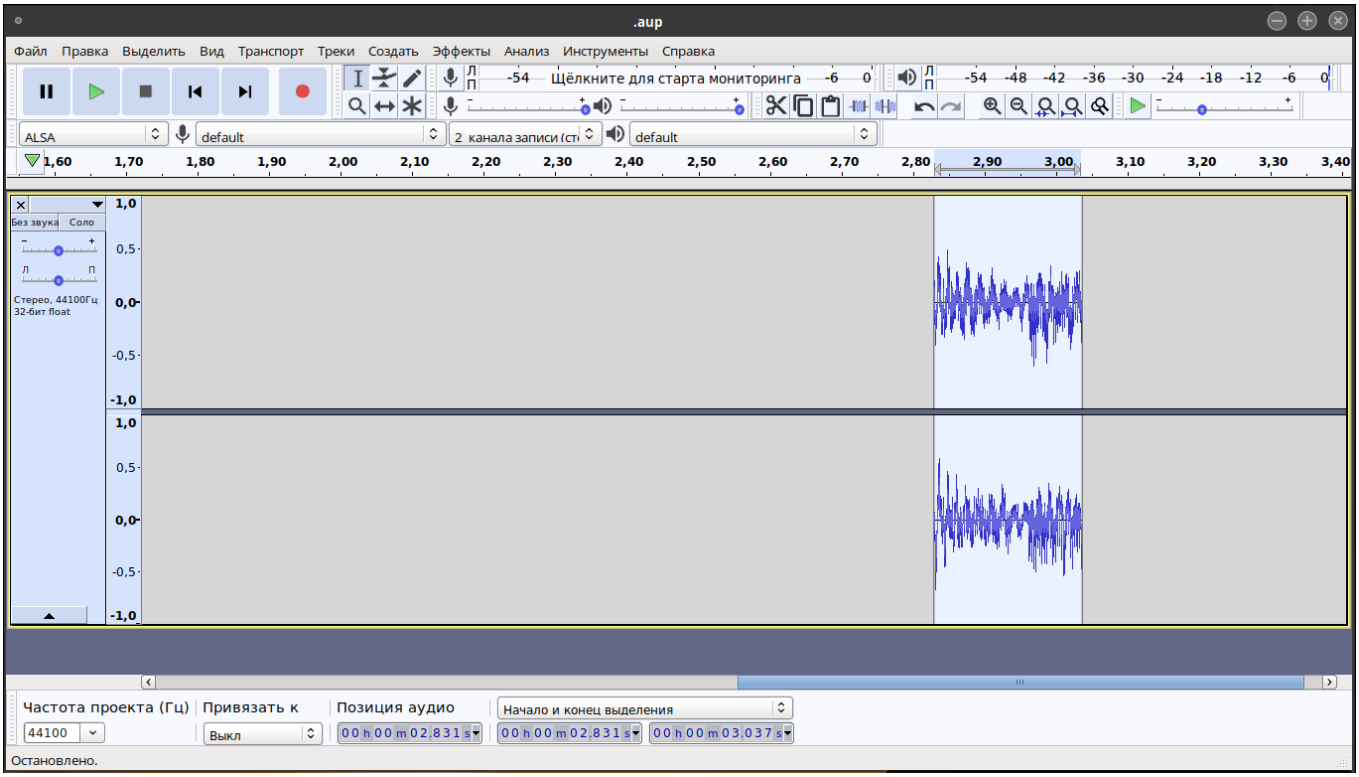
Прежде чем обрезать трек, нужно мышкой выделить необходимую часть и нажать кнопку «**Вырезать**». В таком случае вырезанная часть будет изъята из редактируемой аудиодорожки.

Однако если должен использоваться именно выделенный фрагмент, тогда для сохранения выделенного фрагмента аудиофайла необходимо выполнить следующие действия:

1. Переключитесь на инструмент «**Выделение**» и отметьте необходимую часть записи.

2. Откройте пункт меню «**Правка**» - «**Специальное удаление**» - «**Обрезать аудио**».

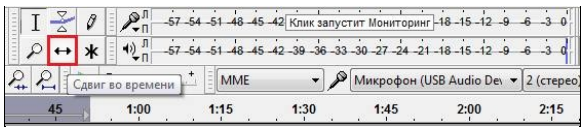
После этого останется доступен только выделенный фрагмент аудиофайла.

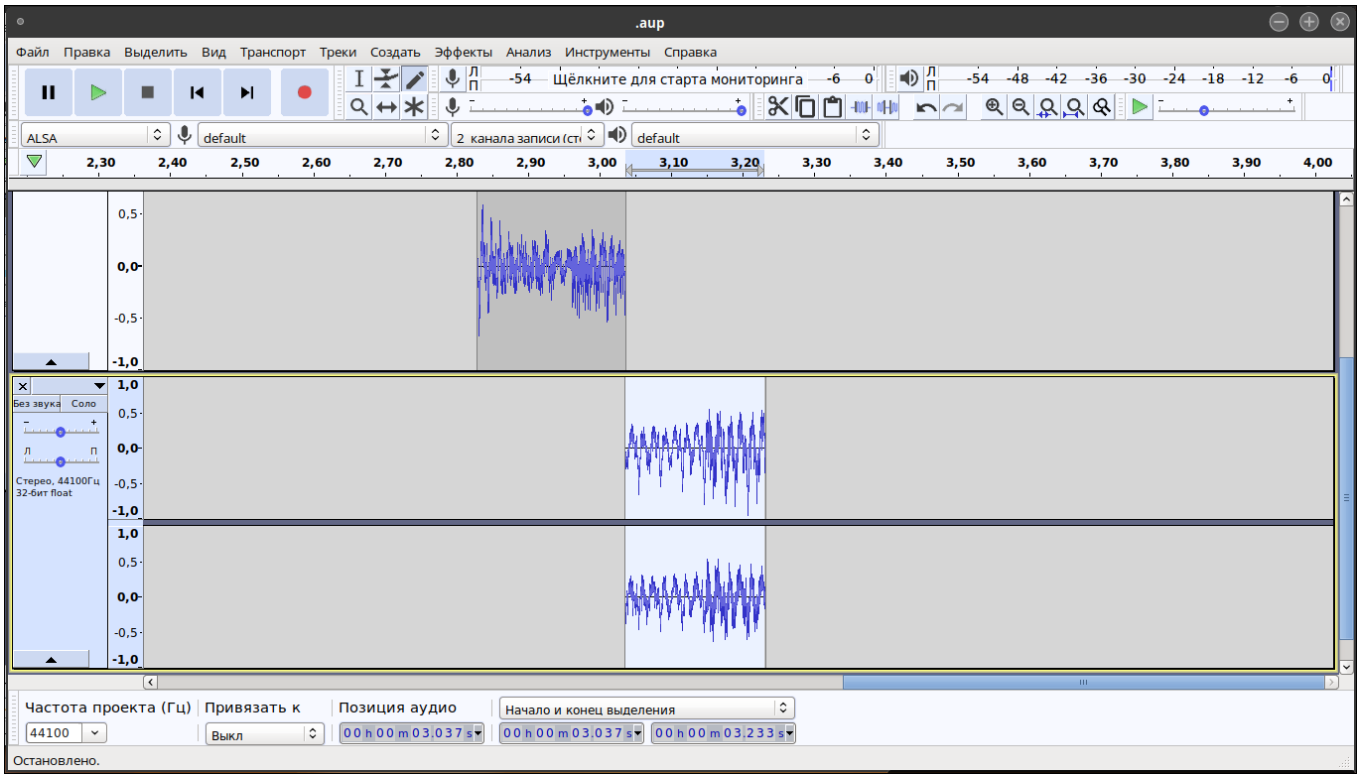


Объединение звука

Для соединения нескольких фрагментов аудио в один импортируйте («**Файл**» - «**Импорт**») все необходимые файлы и поместите их на разные дорожки.

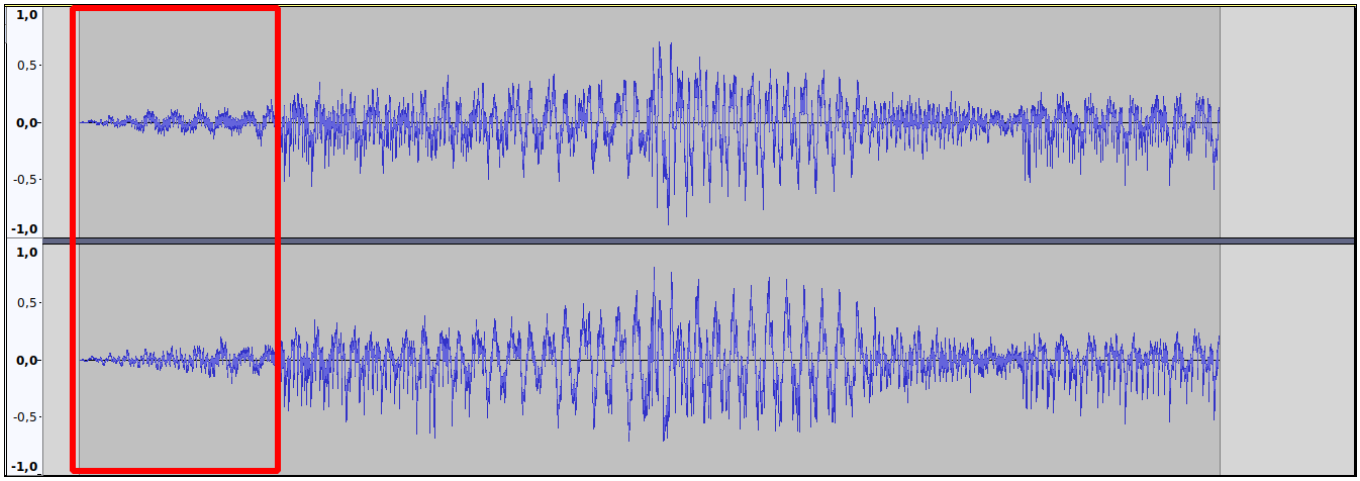
Затем, используя инструмент «**Сдвиг во времени**», необходимо переместить их визуально в нужном порядке.



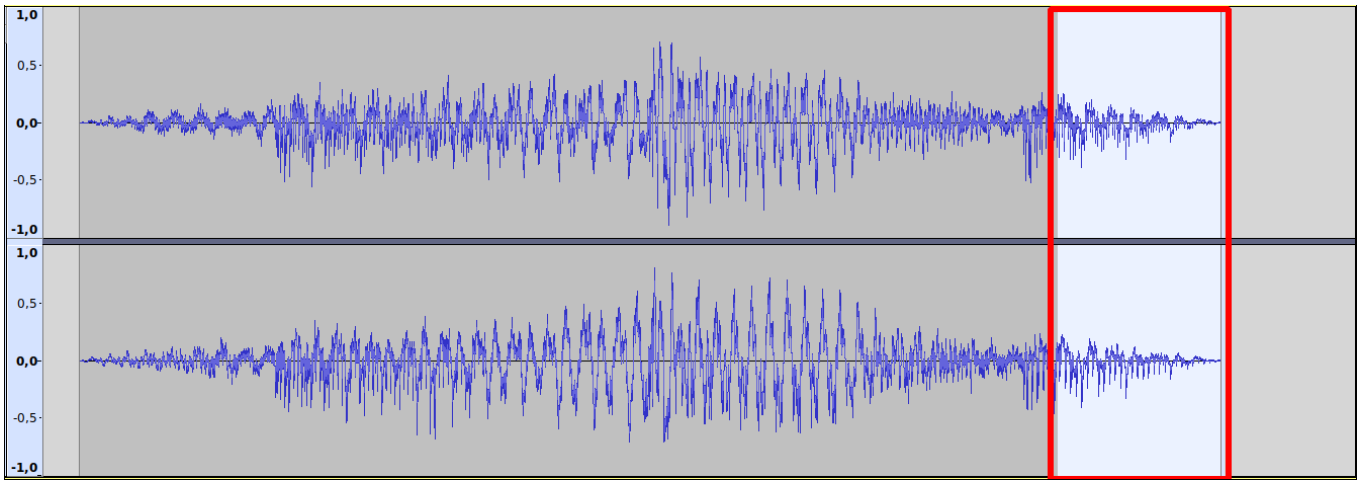


Затухание и нарастание звука

Рассмотрим создание нарастания в начале записи. Для этого выделите начальный фрагмент нужной длительности и перейдите в «**Эффекты**» – «**Фейд-вход**».



Также можно создать затухание — выделите фрагмент необходимой длины, затем перейдите в «**Эффекты**» и выберите «**Фейд-выход**».

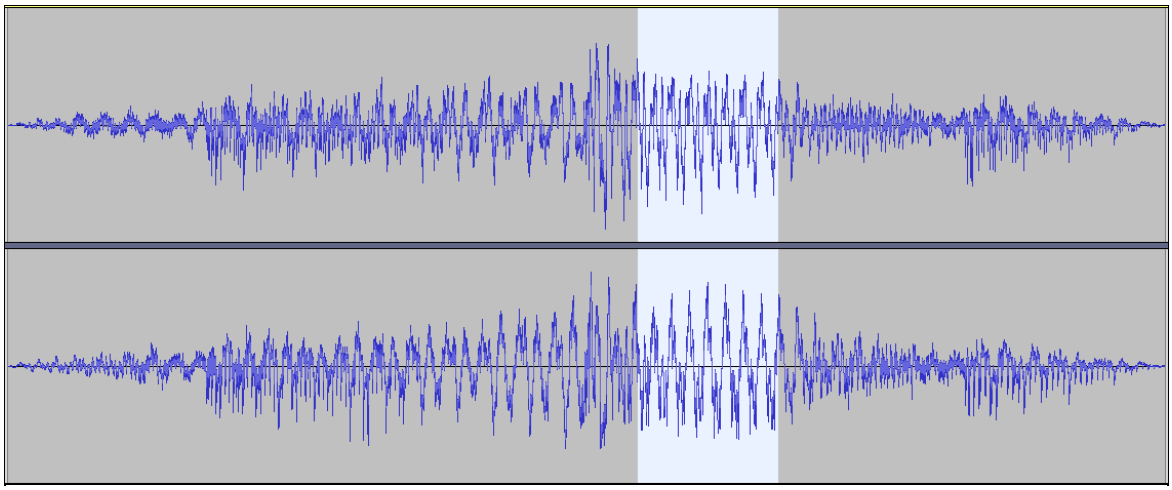


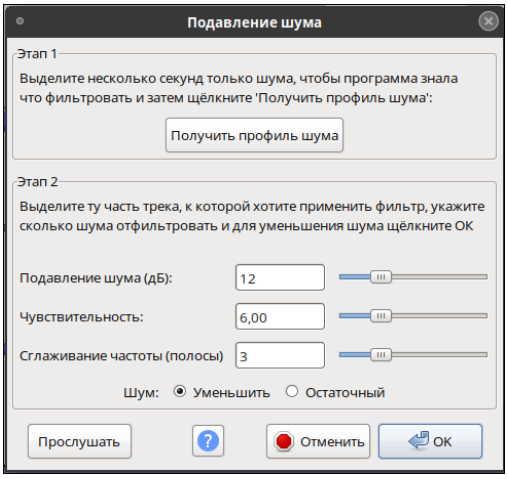
Фильтрация шума

Одним из самых полезных инструментов является фильтр шума. Бывает так, что при записи вы забыли отключить все посторонние предметы, которые издают шум, например, кулер компьютера. В таком случае на помощь приходят инструменты для очистки шума.

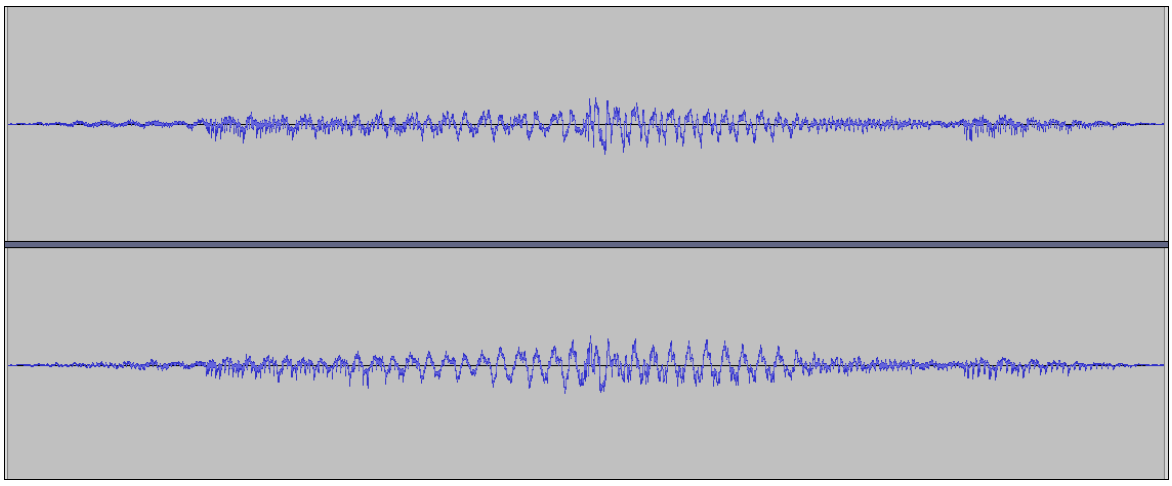
Удаление шумов, писка и других звуков совершается инструментами «**Подавление шума**» и «**Удаление щелчков**», расположенных на вкладке меню «**Эффекты**».

Сначала нужно «научить» функцию распознавать, где шум есть, а где его нет. Для этого выделите фрагмент аудио, где есть только шум, затем перейдите в пункт меню «**Эффекты**» и выберите пункт «**Подавление шума**». Будет открыто окно, в котором необходимо нажать на кнопку «**Получить профиль шума**», а также можно настроить чувствительность и другие параметры.





После этого выделите всю дорожку и еще раз откройте окно «**Подавление шума**», нажмите «**OK**», чтобы запустить процедуру удаления шума.



Посторонние шумы будут удалены со звуковой дорожки.

DeaDBeef - мультимедийный проигрыватель

Установка DeadBeef
Описание аудиопроигрователя DeadBeef
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: deadbeef-1.9.6-1

DeadBeef - это легковесный аудиоплеер, написанный на языках программирования *C* и *C++*.

Основные возможности **DeadBeef** включают:

- поддержку воспроизведения форматов MP3, OGG, FLAC/OGA, APE, WAV Pack, WV/ISO.WV, AAC/M4A, ALAS, MPC/MPP/MP+, TTA, WMA, SHN, SID, NSF, MOD, S3M, VTX, VGM/VGZ, PSF, MIDI, AUDIO CDF, а также других форматов, поддерживаемых через ffmpeg / libav;
- использование небольшого объема памяти и ресурсов процессора;
- поддержку расширения функционала с помощью плагинов;
- поддержку плейлистов CUE, M3U и PLS;
- поддержку воспроизведения интернет радио, а также обычных MP3 файлов по HTTP и HTTPS;
- глобальные горячие клавиши;
- поддержку чтения и записи ID3v1, ID3v2, APEv2, vorbiscomment;
- высокое качество передискретизации с помощью libsamplerate;
- воспроизведение с помощью Alsa, OSS и PulseAudio;
- встроенный скробблер last.fm/libre.fm;
- поддержку нескольких списков воспроизведения;
- 18-полосный эквалайзер;
- воспроизведение файлов прямо из архива;
- многоканальное воспроизведение аудиофайлов.

Установка DeadBeef

Для установки **DeadBeef** перейдите в сеанс пользователя **root**:

```
su -
```

Выполните команду:

```
dnf install deadbeef
```

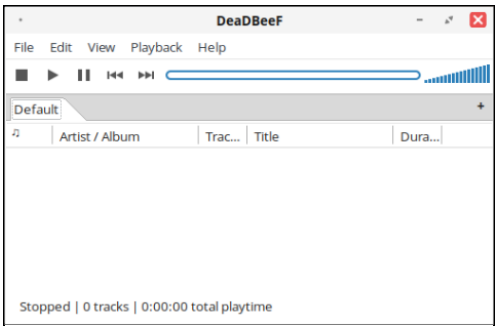
Завершите сеанс пользователя **root**:

```
exit
```

После установки запуск аудиопроигрывателя будет доступен из «**Главного меню**» - «**Аудио и видео**» - «**DeaDBeeF**» или через терминал (с правами непривилегированного пользователя):

```
deadbeef
```

Окно программы выглядит следующим образом:



Описание аудиопроигрователя DeadBeef

Аудиопроигрыватель имеет простой и понятный интерфейс. Рассмотрим подробнее элементы проигрывателя.

1. Вверху программы находится **основное меню**, состоящее из пяти основных пунктов**:** «**File**», «**Edit**», «**View**», «**Playback**», «**Help**».

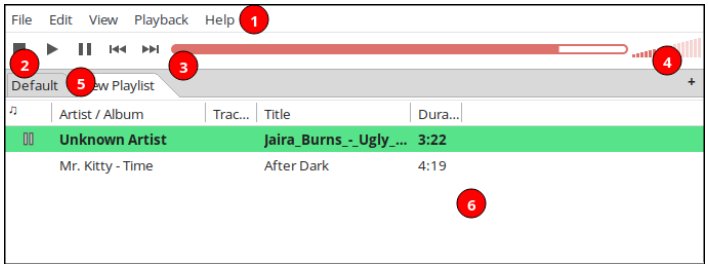
2. **Панель воспроизведения** с кнопками начала воспроизведения, паузы, остановки, перемотки трека.

3. Элемент **SeekBar** представляет собой слайдер, с помощью которого можно перемещаться по аудиозаписи.

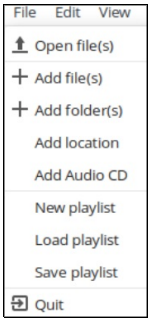
4. **Панель индикации** громкости звука показывает изменение уровня громкости.

5 . **Панель плейлистов** отображает список всех плейлистов, переключение между ними осуществляется однократным нажатием левой кнопки мыши.

6. Через **панель аудиозаписей** можно поменять порядок аудиозаписей или добавить новую композицию.

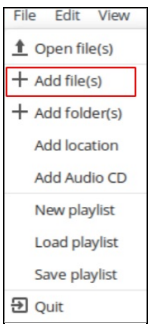


Из пункта меню «**File**» доступны базовые функции для добавления отдельных аудиозаписей и каталогов, а также URL списков трансляций медиапотока из интернета через пункт подменю «**Add location**».

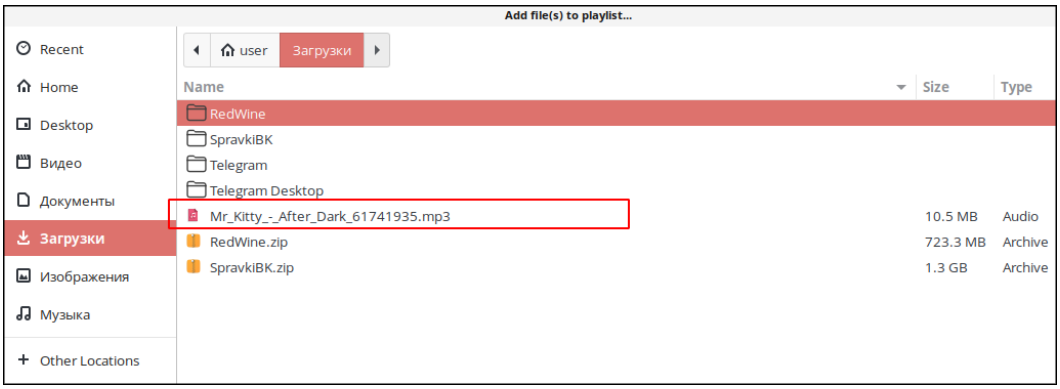


Функции «**Open file(s)**», «**Add file(s)**» и «**Add folder(s)**» отвечают за открытие файла, добавление аудиозаписи и папки с аудиозаписями.

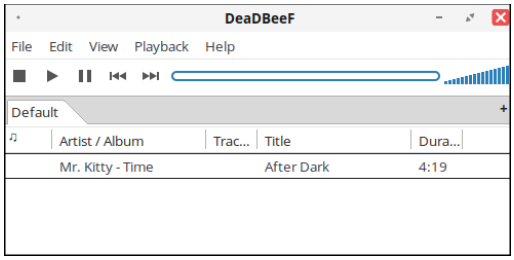
Для добавления аудиозаписи перейдите в меню «**File**» - подменю «**Add file(s)**».



Выберите файл, предварительно скачанный из интернета.



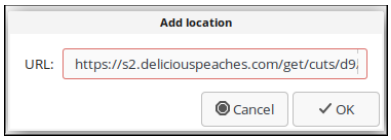
После этих действий аудиозапись должна появиться в вашем плейлисте.



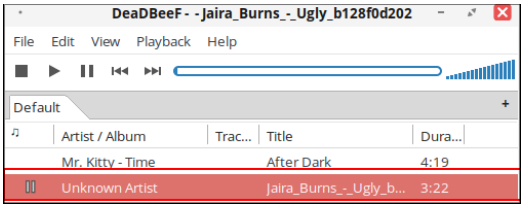
Функции «**Open file(s)**» и «**Add floder(s)**» работают по аналогии.

Функция «**Add location**» отвечает за добавление музыки по URL.

Для добавления музыки нужно скопировать прямую ссылку на выбранный трек и вставить ссылку в терминал, который появится после выбора функции «**Add location**».



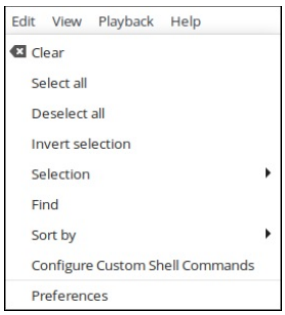
После выполненных действий аудиозапись отобразится в плейлисте проигрывателя.



Функция «**Add Audio CD**» добавляет в плейлист аудио из CD-проигрывателя.

Инструменты «**New playlist**», «**Load playlist**», «**Save playlist**» отвечают за манипуляции с плейлистами (создание нового, загрузку и сохранение плейлиста).

Функции меню «**Edit**» включают выделение, отмену выделения, удаление, обрезку аудиозаписей, сортировку по разным критериям.



Функции «**Select all**», «**Deselect all**» и «**Invert selection**» позволяют выделить все аудиозаписи, находящиеся в плейлисте, снять выделение со всех аудиозаписей, сделать выделенными те области, которые были ранее не выделенными.

Подменю «**Selection**» имеет 2 функции: «**Remove**» (позволяет удалить аудиозаписи из плейлиста) и «**Crop**» (позволяет вырезать их).

С помощью функции «**Find**» доступен быстрый поиск аудиозаписи по ее названию.

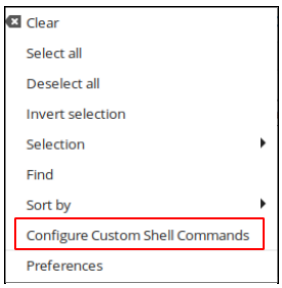
Функция «**Sort by**» отвечает за сортировку по различным критериям, например: «**Date**» — по дате, «**Artist**» — по авторам, «**Random**» — сортирует музыку рандомно (в случайном порядке).

С помощью функции «**Configure Custom Shell Commands**» можно создавать дополнительные команды (например, для записи радио или поиск данных об исполнителе и произведении).

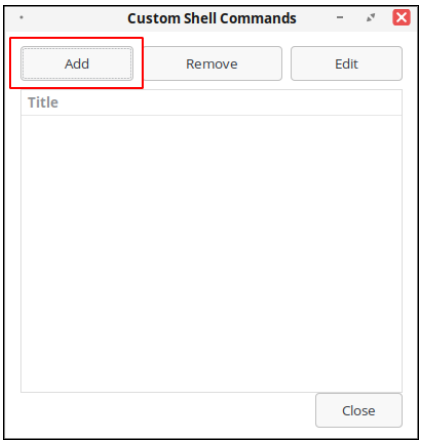
Пример работы

Создание команды для поиска данных об исполнителе.

1. Перейдите в меню «**Edit**» - подменю «**Configure Custom Shell Commands**».



2. Далее в появившемся окне нажмите кнопку «**Add**».



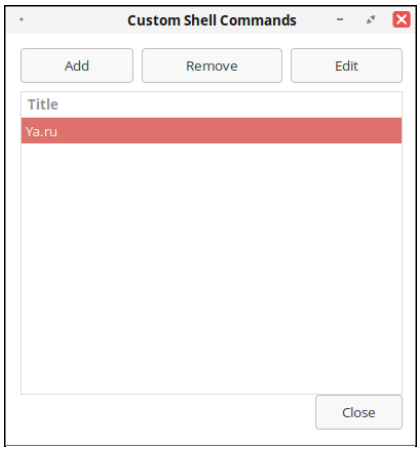
3. Добавьте информацию о поисковой системе, через которую будет происходить поиск данных (система может быть любая, рассмотрим на примере системы **Yandex**).

4. Укажите ссылку на поиск **ya.ru**: http://ya.ru/yandsearch.

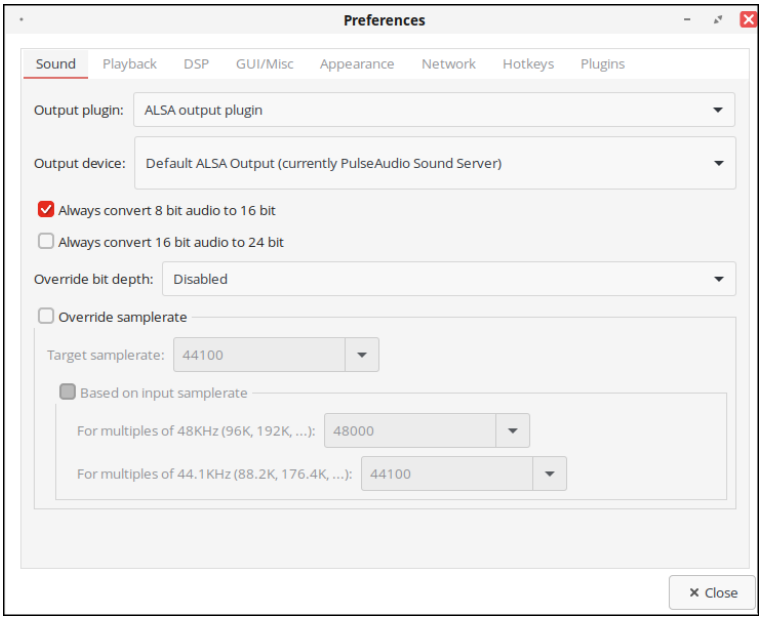
5. Отметьте флагами пункты «**Single Tracks**», «**Local**», «**Remote**».



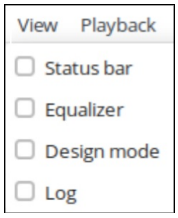
6. Далее команда появится в окне «**Configure Custom Shell Commands**».



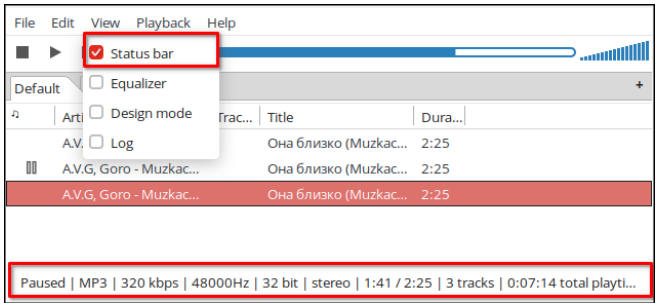
В меню «**Edit**» рассмотрим последний пункт «**Pereferenses**» . Он содержит общие настройки приложения: от звучания музыки до кастомизации приложения.



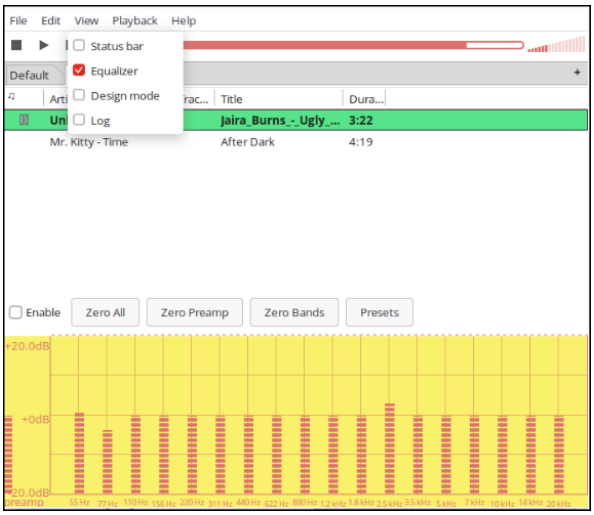
В меню «**View**» находятся параметры внешнего вида интерфейса приложения.



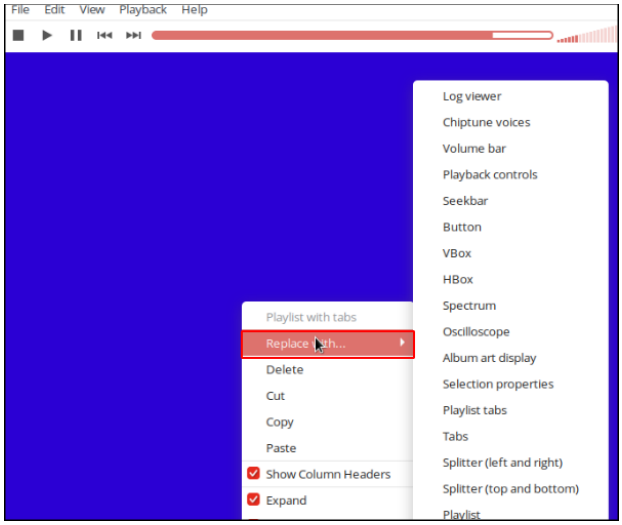
Функция «**Status bar**» добавляет информацию об статусе приложения.



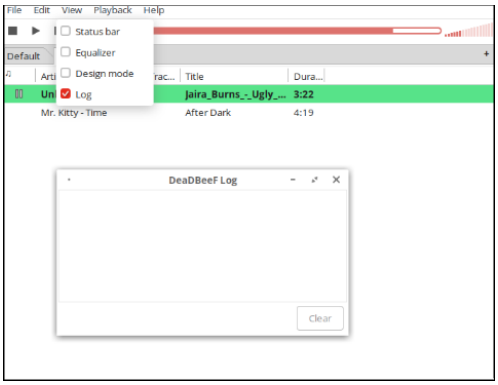
Функция «**Equaliser**» позволяет настраивать звучание музыки.



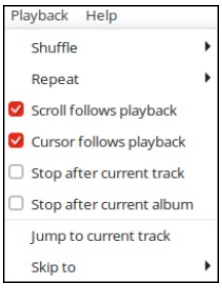
Функция «**Design mood**» добавляет на ПКМ возможность настройки внешнего вида приложения.



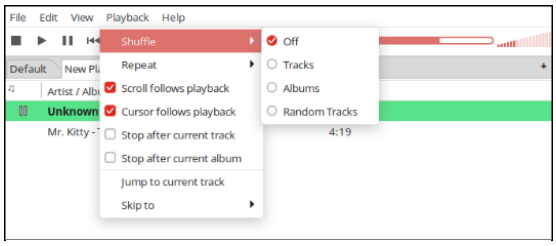
Функция «**Log**» отображает окно логов.



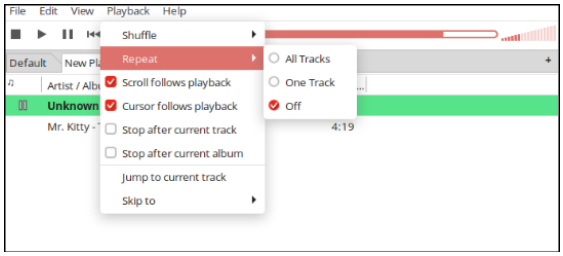
В меню «**Playback**» доступны параметры воспроизведения, повтора аудиозаписей, остановки после конкретной записи или ее пропуска.



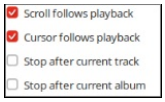
Функция «**Shuffle**» перемешивает воспроизведение аудиозаписей по трекам и альбомам.



Функция «**Repeat**» включает возможность повтора одной определенной аудиозаписи или всех записей, находящихся в плейлисте.

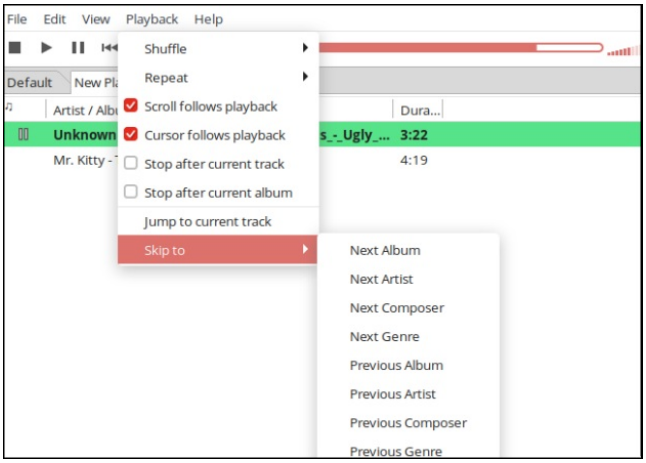


Установите флаги рядом с пунктами «**Scroll follows playback**», «**Cursor follows playback**», «**Stop after current track**», «**Stop after current album**» для отслеживания воспроизведения и остановки после определенных аудиозаписи или альбома.



Функция «**Jump to current track**» позволяет перейти к текущем треку.

С помощью «**Skip to**» имеется возможность пропуска треков по заданным параметрам.



Rhythmbox — музыкальный проигрыватель

Установка
Описание музыкального проигрывателя
Панель инструментов проигрывателя
Боковая панель
Источники воспроизведения
Настройки
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: rhythmbox-3.4.4

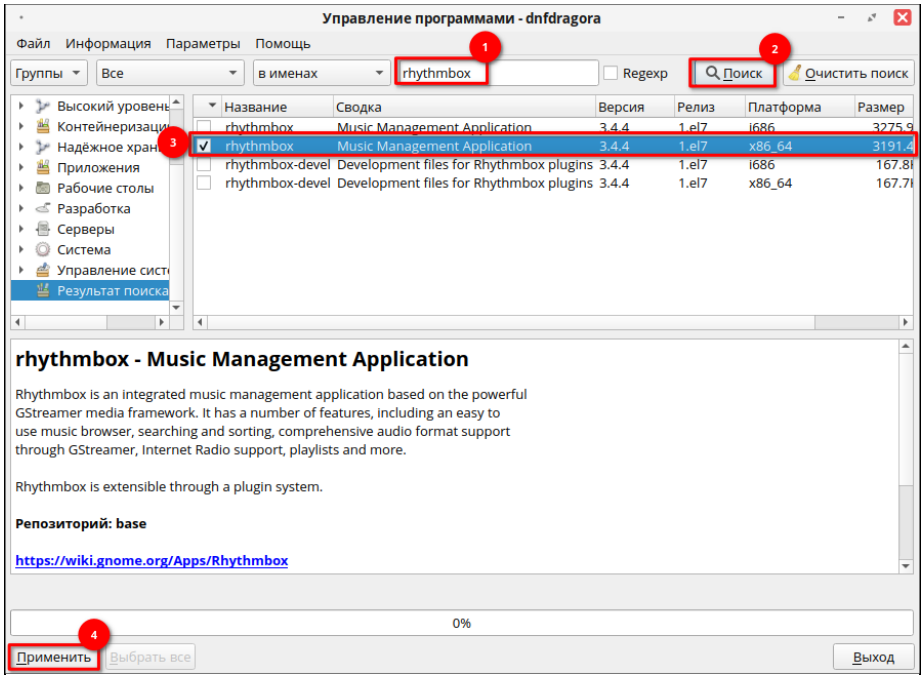
Rhythmbox — это музыкальный проигрыватель, который предлагает широкий спектр функций для управления музыкальной коллекцией. Он позволяет:

- импортировать музыку из различных источников;
- создавать и управлять списками воспроизведения;
- настроить **Rhythmbox** в качестве цифрового аудиосервера;
- подключаться к различным музыкальным сервисам, таким как Last.fm, Libre.fm и Magnatune, для получения рекомендаций;
- поддерживать различные форматы, включая MP3, OGG, FLAC;
- слушать интернет-радио;
- управлять музыкальной коллекцией с помощью простого и интуитивного интерфейса.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**rhythmbox**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



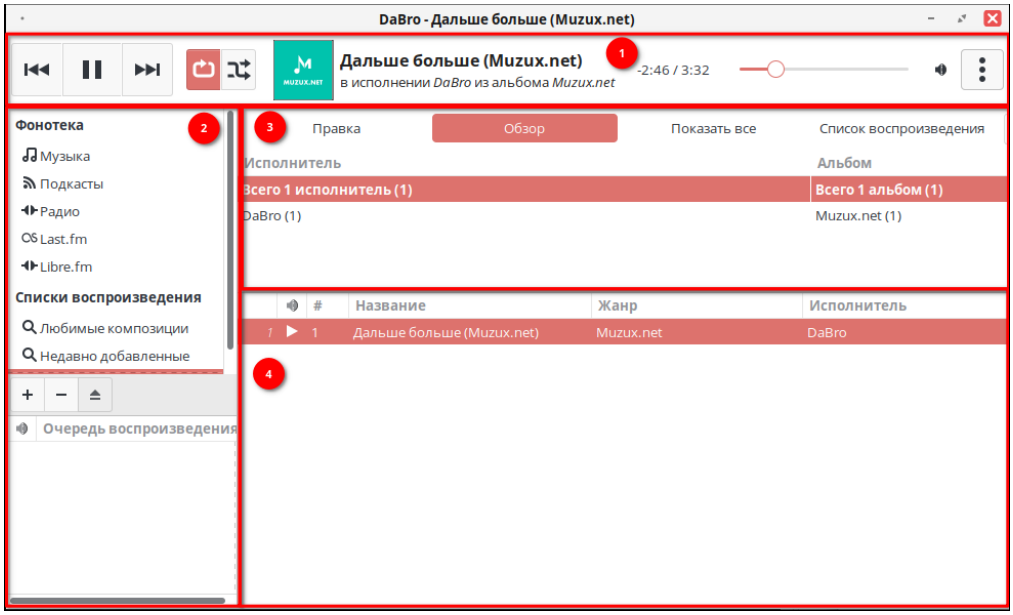
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install rhythmbox
```

После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**Rhythmbox**».

Описание музыкального проигрывателя

Окно музыкального проигрывателя выглядит следующим образом:



1. **Панель инструментов** — предоставляет доступ к функциям проигрывателя и информации о текущем треке. Включает в себя ползунок времени, который отображает позицию воспроизведения трека; позволяет перейти к другой части трека. Также включает в себя ползунок громкости и кнопку для доступа к меню приложения.

2. **Боковая панель** — отображает список доступных источников. Может также отображать очередь воспроизведения.

3. **Браузер** — позволяет просматривать и фильтровать треки в фонотеке по жанру, исполнителю или названию альбома. Также в браузер встроена функция поиска, с помощью которой можно просматривать только те треки, которые соответствуют нужным критериям.

4. **Список треков** — перечисляет треки из выбранного источника.

Панель инструментов проигрывателя

Область панели инструментов отображает подробности о воспроизводимой в данный момент дорожке.

 **Предыдущий** — переходит к предыдущему треку в плейлисте;

 **Воспроизвести** — начинает воспроизведение текущего трека;

 **Пауза** — приостанавливает воспроизведение текущего трека;

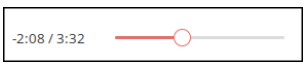
 **Следующий** — переходит к следующему треку в плейлисте;

 Повторять — повторяет воспроизведение дорожек с начала списка после окончания последней дорожки;

 **В случайном порядке** — воспроизводит дорожки в случайном порядке.

При воспроизведении или выборе дорожки отображается её название, а под ним — имя исполнителя и название альбома.

Также отображается индикатор, показывающий ход воспроизведения трека, и ползунок времени.



Для регулирования громкости используйте колёсико мыши, прокручивая её вверх или вниз, пока указатель мыши находится над кнопкой регулировки громкости  .

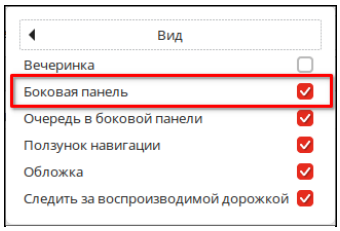
 **Основное меню** — открывает меню приложения, которое предоставляет доступ к различным опциям, таким как инструменты, параметры, справка.

Боковая панель

На боковой панели **Rhythmbox** можно получить доступ к следующим источникам:

- Музыка,
- Радио,
- Аудиодиски,
- Плейлисты,
- Подкасты,
- Сайты для обмена музыкой,
- Очереди воспроизведения.

Можно включить/выключить боковую панель, нажав кнопку  и включив/отключив флаг для параметра «**Вид**» — «**Боковая панель**».

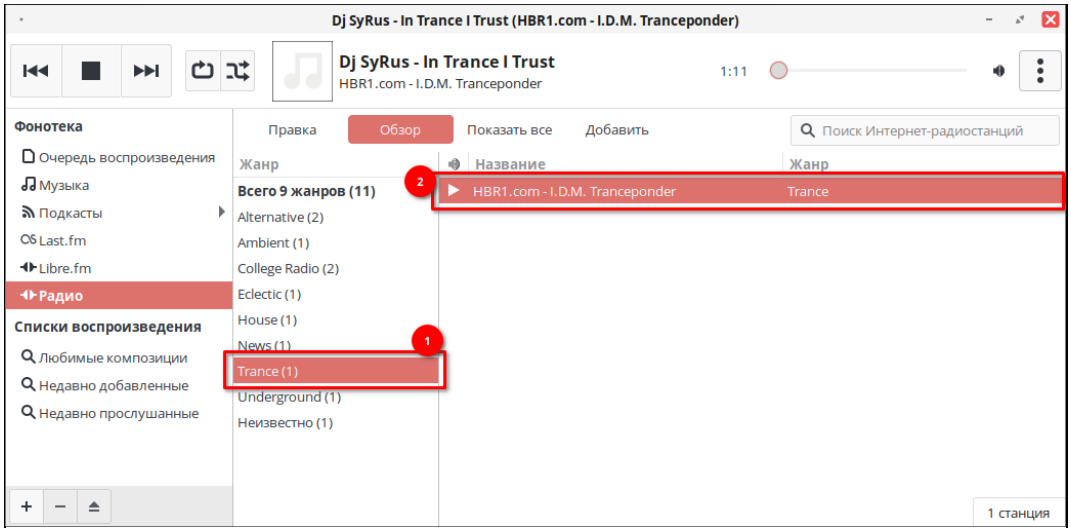


Источники воспроизведения

Источник «Радио»

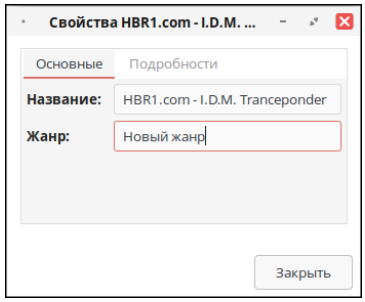
Для прослушивания потокового аудио из Интернета можно использовать источник «**Радио**».

Список радиостанций появится в различных категориях. Выберите жанр и радиостанцию, которую хотите слушать, дважды кликнув по ней.



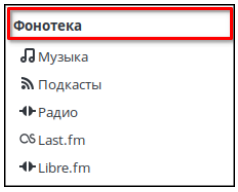
Для добавления новой радиостанции нажмите «**Добавить**» и введите URL-адрес радиостанции.

Для изменения жанра радиостанции щелкните на радиостанцию ПКМ и выберите «**Свойства**». В свойствах измените жанр на новый.



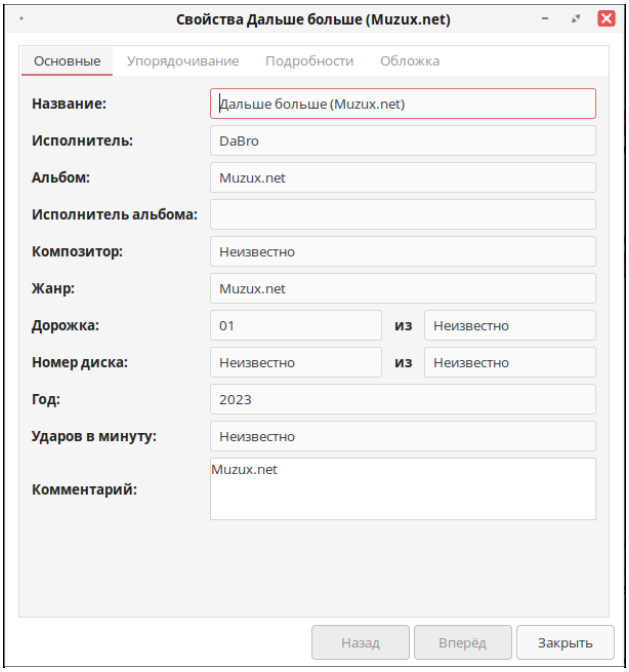
Источник «Фонотека»

Фонотека — основной источник, который содержит музыкальные файлы, импортированные в **Rhythmbox**.



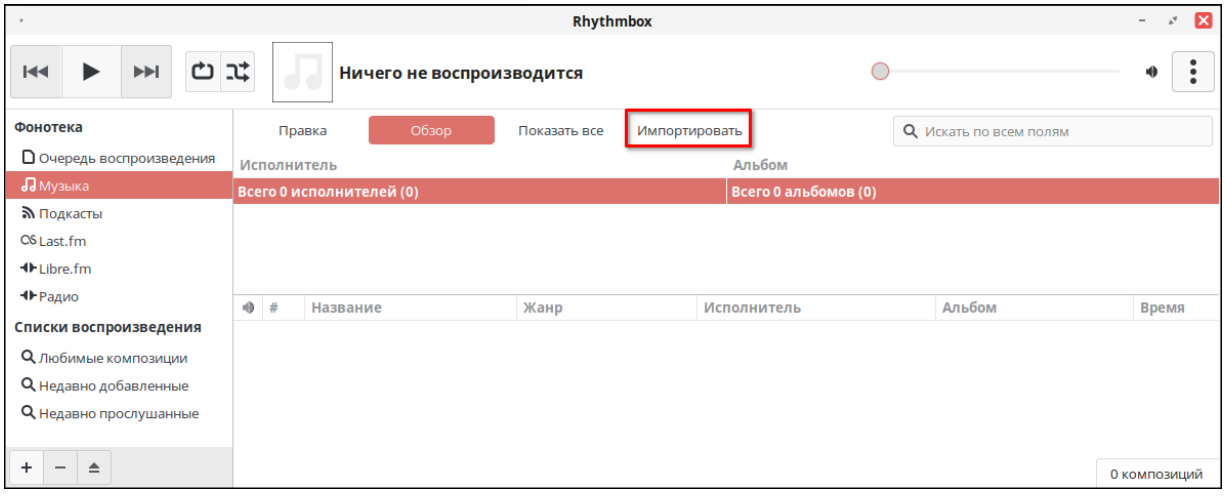
Библиотека может содержать не только музыкальные файлы, которые физически находятся на компьютере пользователя, но и музыкальные файлы, доступные через сетевые службы.

Файлы отображаются в списке треков вместе с информацией, сохранённой в тегах. Теги можно изменить, щёлкнув по файлу ПКМ, затем выбрав пункт «**Свойства**» и изменив информацию в появившемся окне.

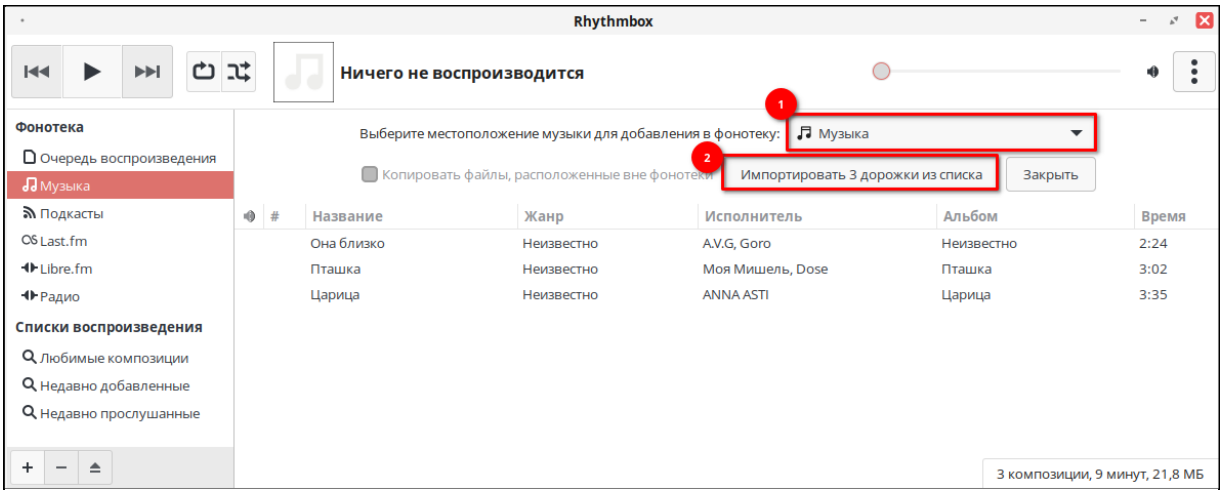


Для добавления дорожек можно воспользоваться следующими способами.

1. Для импорта нескольких музыкальных файлов в фонотеку нажмите «**Импортировать**» в браузере.



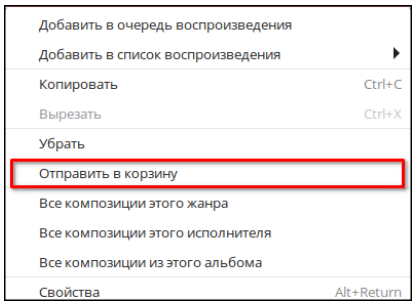
Выберите местоположение музыки, выберите папку в окне выбора файлов и нажмите кнопку «**Открыть**». Далее нажмите «**Импортировать дорожки из списка**», будут импортированы все музыкальные файлы, находящиеся в папке.



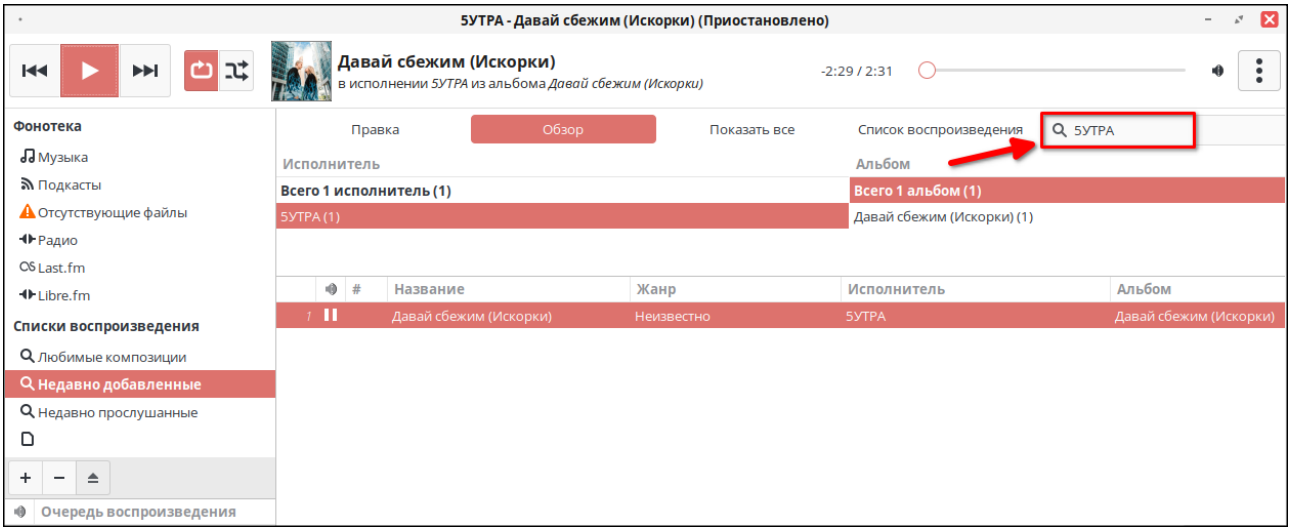
2. Переместите файлы путём перетаскивания из файлового менеджера в окно **Rhythmbox**.

Для удаления дорожки из фонотеки нажмите ПКМ на дорожку и выберите «**Убрать**».

Для удаления дорожки из фонотеки и с диска нажмите ПКМ на дорожку и выберите «**Отправить в корзину**». Дорожка будет удалена, а файл будет перемещён в корзину файлового менеджера.

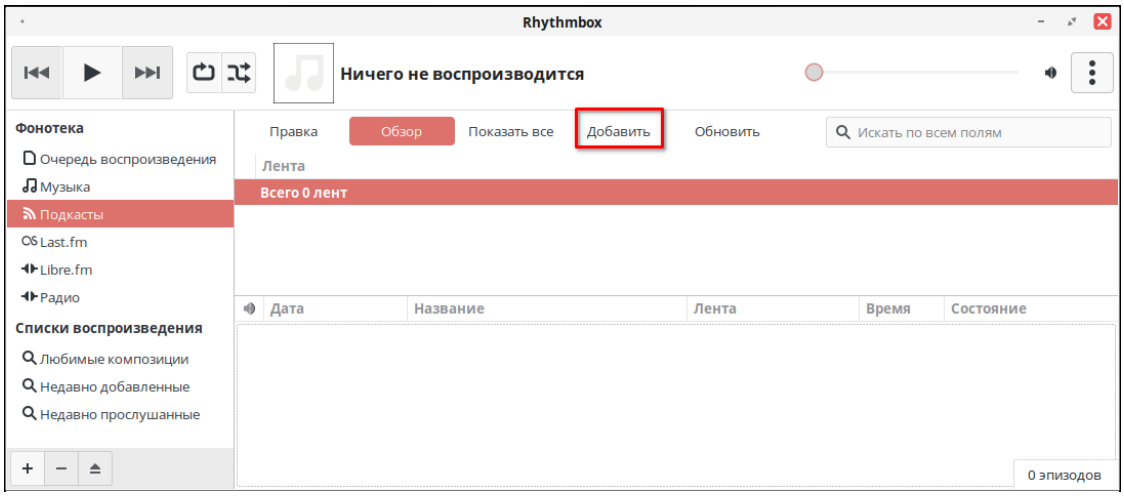


Для поиска дорожек по ключевому слову используйте поле поиска. Введите текст в поле поиска, и по мере ввода будут отображаться только дорожки, соответствующие введенному тексту.

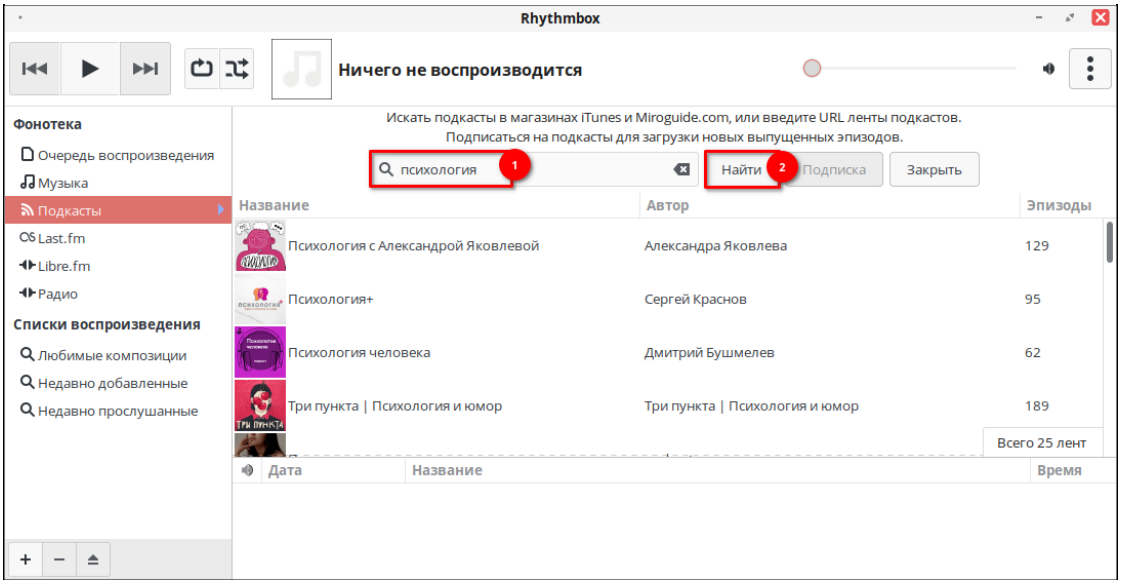


Источник «Подкасты»

В источнике «**Подкасты**» можно подписаться на каналы подкастов и при появлении новых эпизодов получать уведомления о них. Для добавления подкаста выберите «**Добавить**» в верхней части окна подкастов.



В появившемся окне в строке поиска введите ключевое слово (1) или URL-адрес подкаста и нажмите «**Найти**» (2). **Rhythmbox** получит список подкастов и эпизодов.



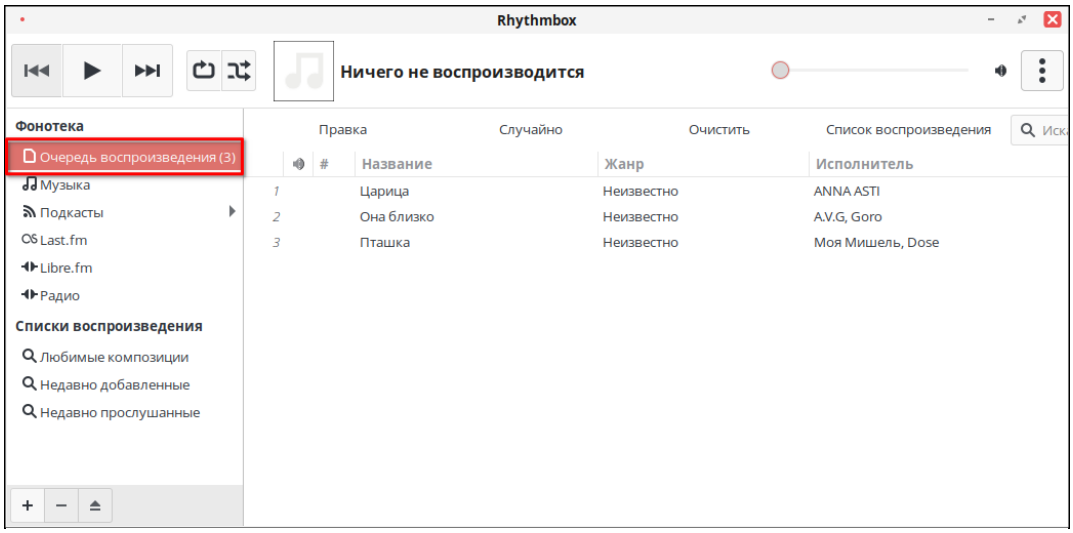
Выберите подкасты, на которые хотите подписаться, и нажмите «**Подписка**». Для отображения списка подкастов и доступных выпусков нажмите «**Закрыть**».

Для удаления подкаста щёлкните ПКМ на названии канала подкастов и выберите «**Удалить ленту подкастов**», затем выберите «**Удалить только ленту**» или выберите «**Удалить ленту и файлы**».

Для обновления подкастов щёлкните ПКМ на источнике «**Подкасты**» и выберите «**Обновить ленту подкастов**» или «**Обновить все ленты**».

Источник «Очередь воспроизведения»

Очередь воспроизведения — это источник, предназначенный для временного хранения треков. При добавлении трека в очередь воспроизведения музыкальный проигрыватель **Rhythmbox** автоматически переключается на этот источник после воспроизведения трека.



После воспроизведения трека он будет автоматически удалён из источника очереди воспроизведения. Как только очередь воспроизведения опустеет, музыкальный проигрыватель **Rhythmbox** перейдёт к источнику, который был воспроизведён ранее.

Источник «Звуковой компакт-диск»

Музыкальный проигрыватель **Rhythmbox** может воспроизводить и записывать аудиодиски.

Когда аудиодиск будет вставлен, он появится на боковой панели, а треки можно будет просмотреть в главном окне **Rhythmbox**.

Для управления воспроизведением, приостановкой и перемоткой используйте тот же порядок действий, что и в фонотеке.

Для записи на диск треков вставьте чистый компакт-диск, нажмите кнопку «**Создать**», начнётся процесс записи.

Источник «Портативные звуковые проигрыватели»

Rhythmbox может определять, когда портативный аудиоплеер подключен к компьютеру, и считывать сохранённые на нем треки.

При подключении портативного аудиоплеера к компьютеру **Rhythmbox** может автоматически обнаружить его и отобразить значок плеера на боковой панели. Этот источник работает так же, как и источник из библиотеки, пользователи могут воспроизводить музыку с плеера, как если бы она была сохранена на их компьютере.

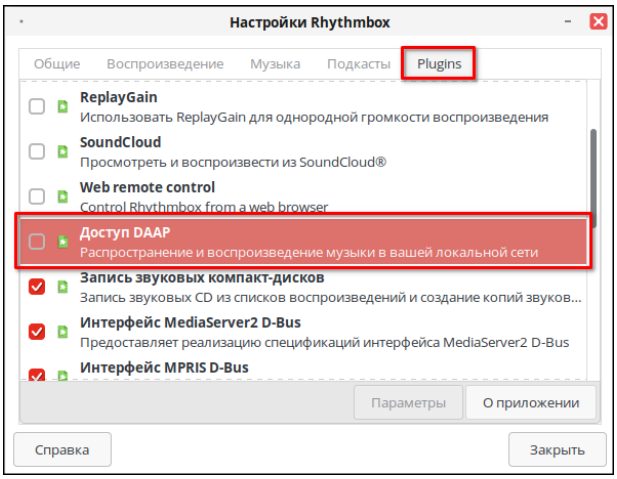
Rhythmbox совместим с большинством портативных аудиоплееров, включая Apple iPod, MTP-плееры и проигрыватели с накопителем данных.

Источник «Общий ресурс DAAP»

DAAP (Digital Audio Access Protocol) — это сетевой протокол для обмена цифровой музыкой между устройствами и приложениями. **Rhythmbox** поддерживает протокол DAAP, что позволяет пользователям обмениваться музыкой не только между собой, но и с пользователями других приложений, совместимых с DAAP, таких как iTunes.

После запуска **Rhythmbox** автоматически ищет общие ресурсы DAAP в локальной сети и отображает их в боковой панели. При включении общего доступа **Rhythmbox** публикует свою медиатеку и списки воспроизведения, что позволяет другим пользователям слушать музыку пользователя, а пользователю — слушать музыку, хранящуюся на компьютерах других пользователей.

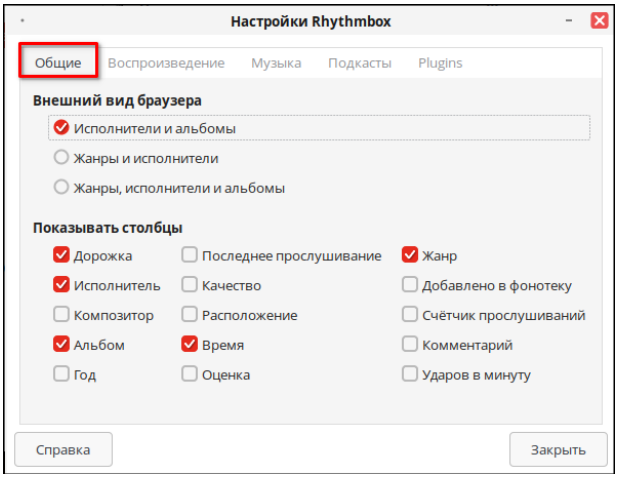
Для отключения функции обмена музыкой по протоколу DAAP в **Rhythmbox** перейдите в меню ⋮ — «**Параметры**». На вкладке «**Plugins**» снимите флаг «**Доступ DAAP**».



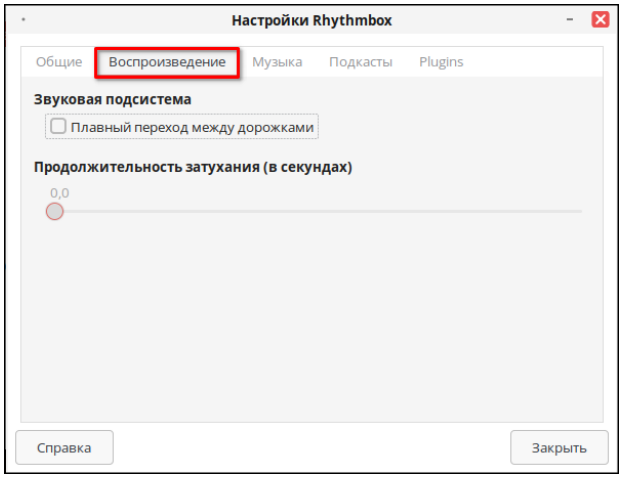
Настройки

Для настройки **Rhythmbox** перейдите в меню — «**Параметры**».

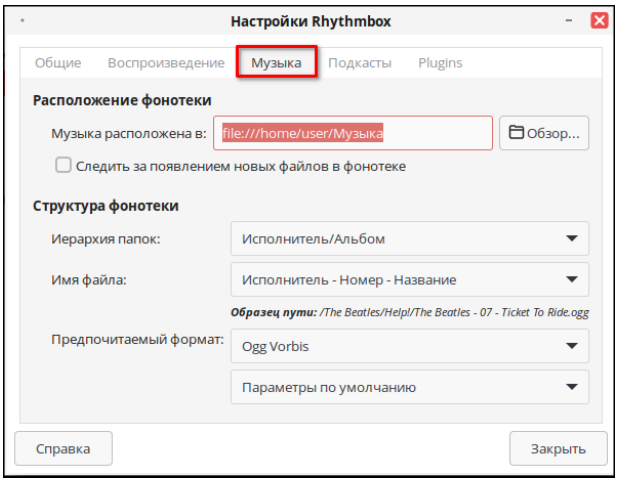
На вкладке «**Общие**» выберите столбцы для отображения в **Rhythmbox**.



На вкладке «**Воспроизведение**» задайте переходы между дорожками и установите продолжительность затухания.



На вкладке «**Музыка**» выберите расположение и структуру фонотеки. Задайте папку, за наличием новых композиций в которой будет следить **Rhythmbox**. Для отключения функции отслеживания новых файлов уберите флаг «**Следить за появлением новых файлов в фонотеке**».



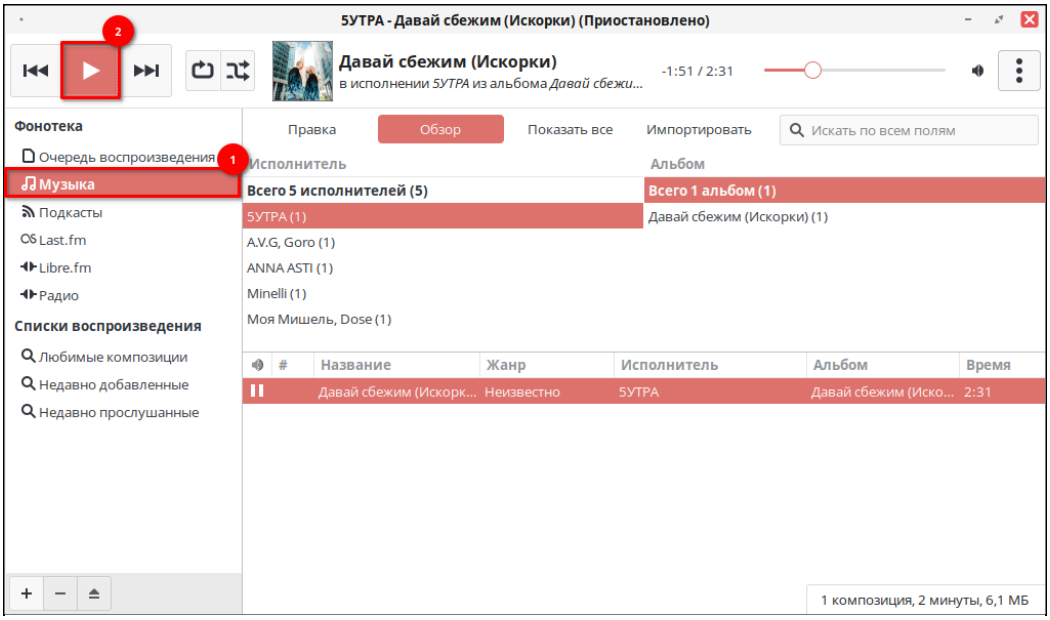
На вкладке «**Подкасты**» настройте параметры загрузки подкастов и частоту проверки новых эпизодов.

Для добавления на боковую панель дополнительных источников на вкладке «**Plugins**» отметьте флагом нужные плагины.

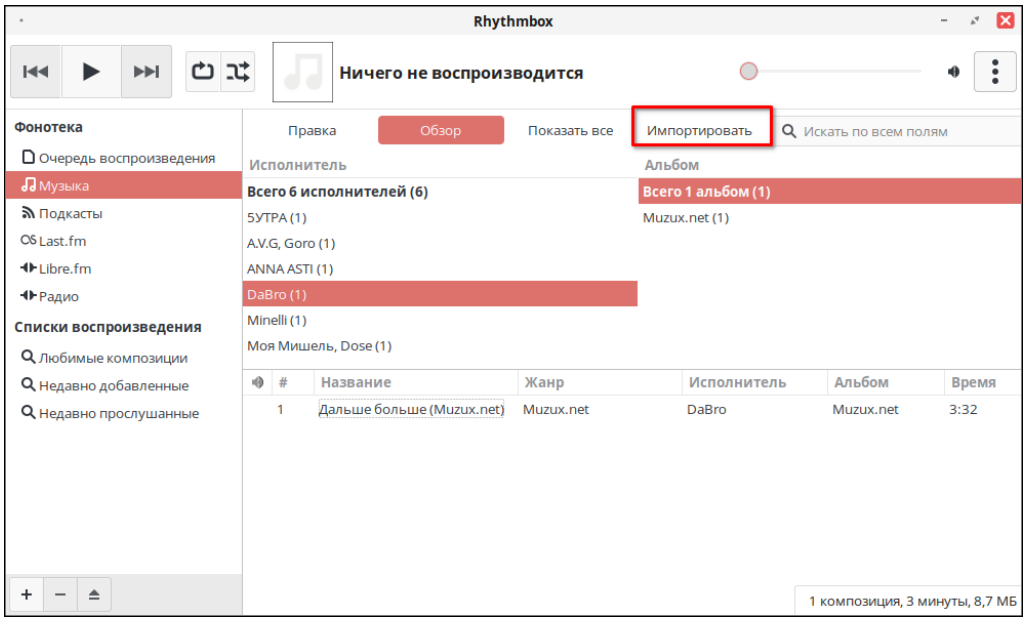
На боковой панели появятся дополнительные источники:

Пример работы

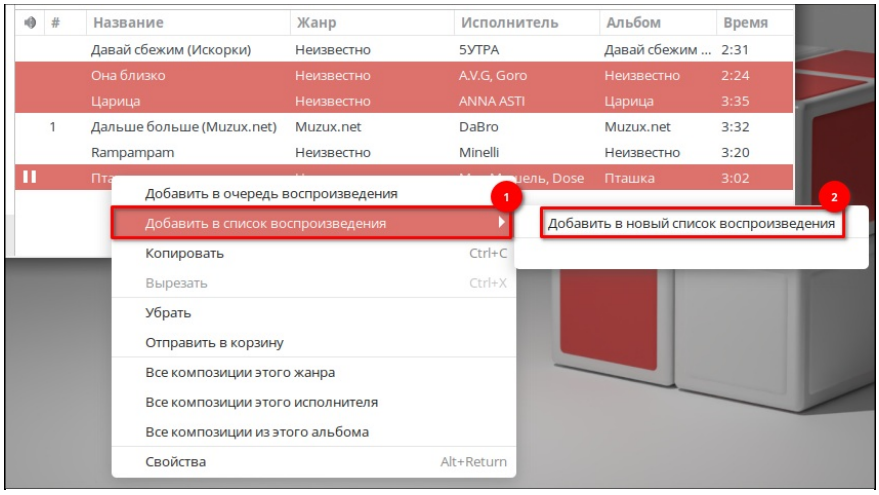
1. Для воспроизведения музыки с помощью **Rhythmbox** необходимо выбрать источник музыки на боковой панели и нажать «**Воспроизвести**» (или двойным нажатием щелкните по треку ЛКМ).



2. Для добавления музыки в фонотеку выберите «**Импортировать**» или перетащите файлы в окно **Rhythmbox**. После импорта файлов они появятся в соответствующих панелях.

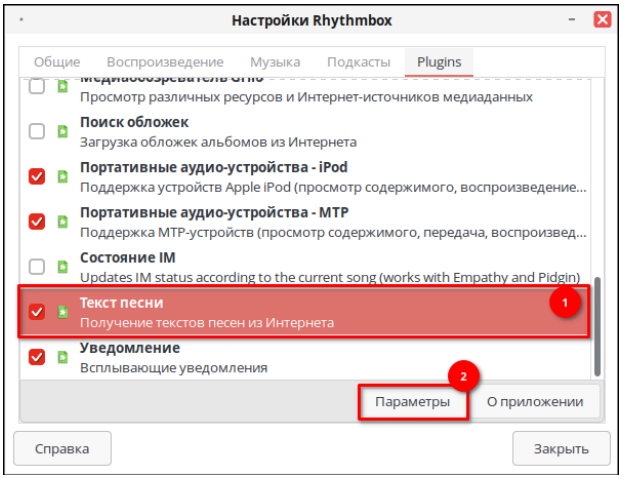


3. Для создания плейлиста выберите несколько треков и нажмите ПКМ на одном из них, а затем выберите «**Добавить в список воспроизведения**» — «**Добавить в новый список воспроизведения**».



4. Во время воспроизведения музыки можно использовать элементы управления воспроизведением в верхней части окна **Rhythmbox**.

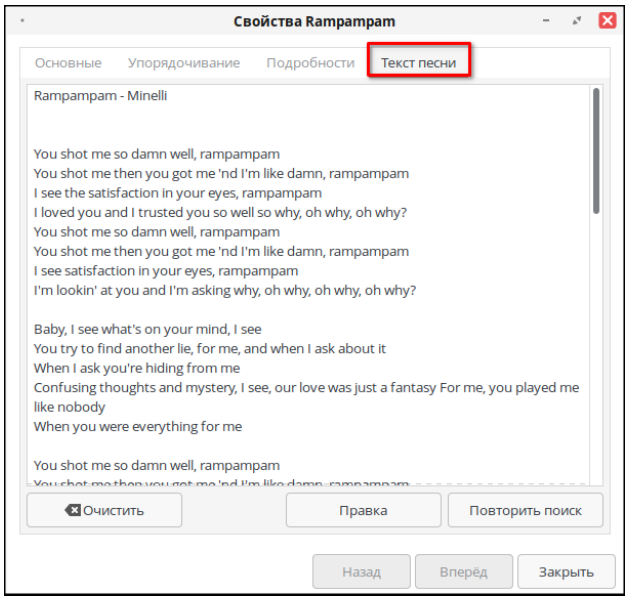
5. **Rhythmbox** предлагает плагины, которые можно активировать, чтобы получить дополнительную функциональность. Перейдите в основное меню — «**Параметры**». На вкладке «**Plugins**» активируйте необходимые плагины, например, «**Текст песни**» (1). Затем нажмите «**Параметры**» (2).



Выберите поисковые машины и папку с текстами песен.

Для просмотра текста песни нажмите на трек ПКМ и выберите «**Свойства**». Перейдите на вкладку «**Текст песни**». Если текст песни доступен, он будет отображаться в окне. Если текст песни не доступен, медиапроигрыватель начнет поиск интернете, в этом случае может потребоваться некоторое время, чтобы текст песни был загружен и отображен. Если текст песни не найден, в окне будет

выведено соответствующее сообщение.



Видеоредактор Kdenlive

Установка
Описание программы
Работа в программе

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** kdenlive-21.04.2-1

Kdenlive — это нелинейный видеоредактор, который позволяет добавлять эффекты и переходы, собирать видео в выбранный формат, при этом занимает мало места на диске и обладает обширным функционалом.

Вы можете подробнее ознакомиться с работой в **Kdenlive**, просмотрев наши обучающие видео:

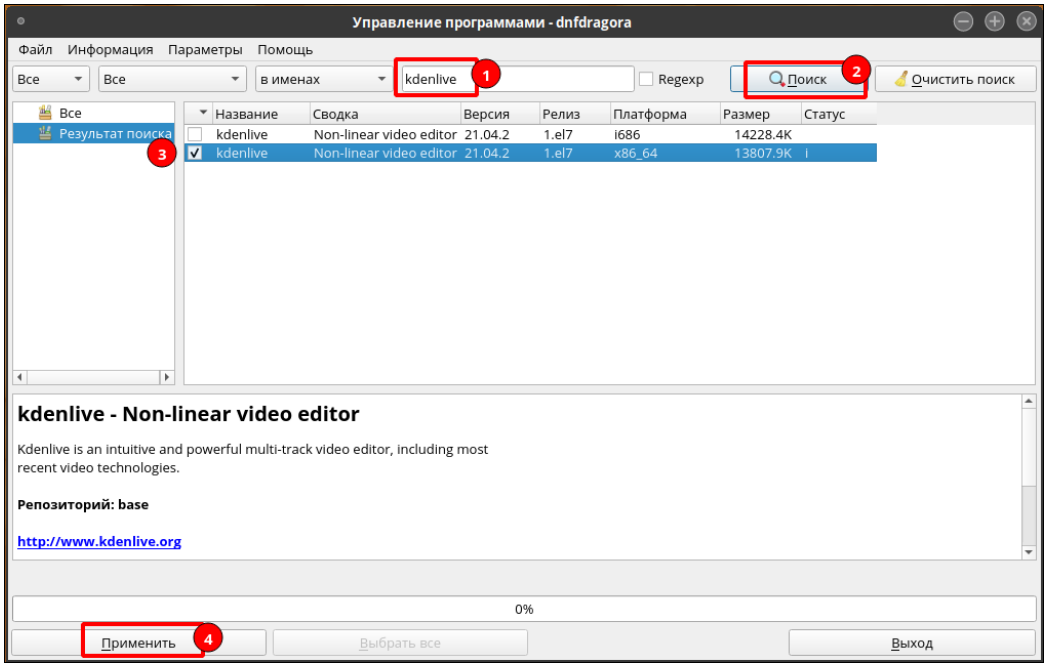
- на **RuTube** — Видеоредакторы. Установка и обзор Kdenlive;
- в **Яндекс.Дзен** — Видеоредакторы. Установка и обзор Kdenlive;
- в **VK Видео** — Видеоредакторы. Установка и обзор Kdenlive.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kdenlive**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

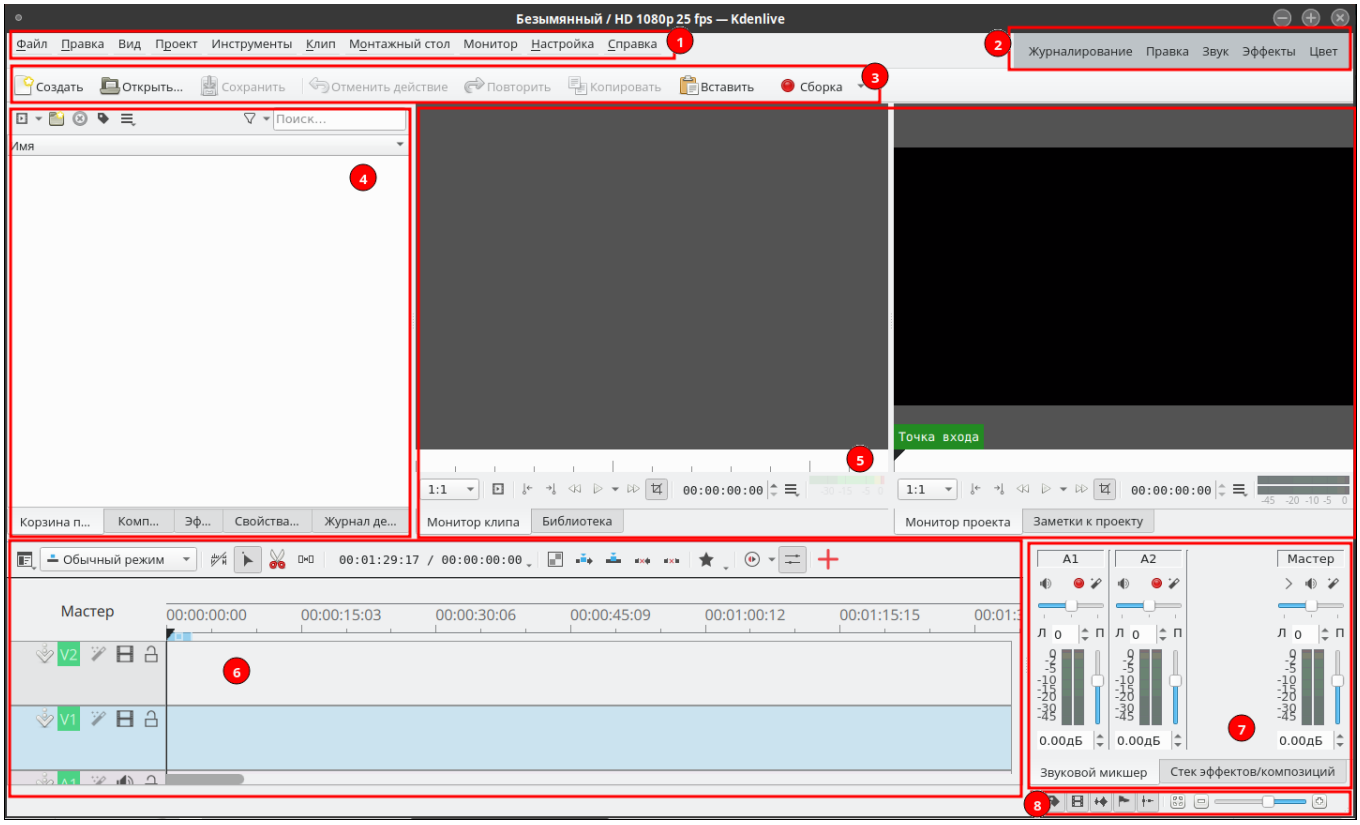
```
dnf install kdenlive
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Аудио и видео**» - «**Видеоредактор Kdenlive**».

Описание программы

Главное окно программы выглядит следующим образом:



Для комфортной работы необходимо отключить опцию «**Форсировать тему значков Breeze**» в пункте меню «**Настройки**», для применения изменений перезапустите программу.

1. *Основное меню* — основные настройки программы и действия для работы с файлами.

2. *Макеты* — шаблоны для выполнения различного рода задач: журналирование, правка, звук, эффекты, цвет.

3. Панель инструментов — основные действия для работы с проектом, таких как создание нового и открытие существующего проекта, сохранение проекта, отмена или повтор действия, копирование и вставка, а также сборка готового проекта.

4. *Корзина проекта* - все рабочие файлы проекта, доступно создание папок для упорядочивания открытых файлов, метки и быстрый поиск, если файлов большое количество.

Во вкладке **Композиции** и **Эффекты** доступны основные переходы и эффекты.

В **Свойствах клипа** отражается вся информация о выбранном видео.

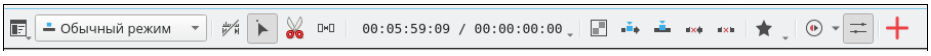
В **Журнале действий** отображается каждый выполненный шаг и можно отменить ошибочное действие.

5. *Монитор клипа* и *монитор проекта*. *Монитор клипа* позволяет посмотреть исходный материал в корзине проекта. *Монитор проекта* отражает видео с монтажного стола (timeline).

В каждом мониторе при наведении курсора мыши открываются свои функции, в том числе просмотр на весь экран.

В левом нижнем углу каждого монитора есть настройка с разрешением отображения, по умолчанию стоит **1:1**, но, при желании, можно изменить это значение.

6. *Монтажный стол* (Timeline). По умолчанию при открытии доступны 2 аудио- и 2 видеодорожки.



Первой располагается кнопка настроек композитинга дорожек, а также положения звуковых дорожек (по умолчанию звуковые дорожки находятся под видео).

Далее представлен список доступных режимов, по умолчанию установлен **Обычный режим**.

Затем располагаются инструменты для работы с дорожками: выбор, ножницы, вставка пробелов, соединение клипов и т. д.

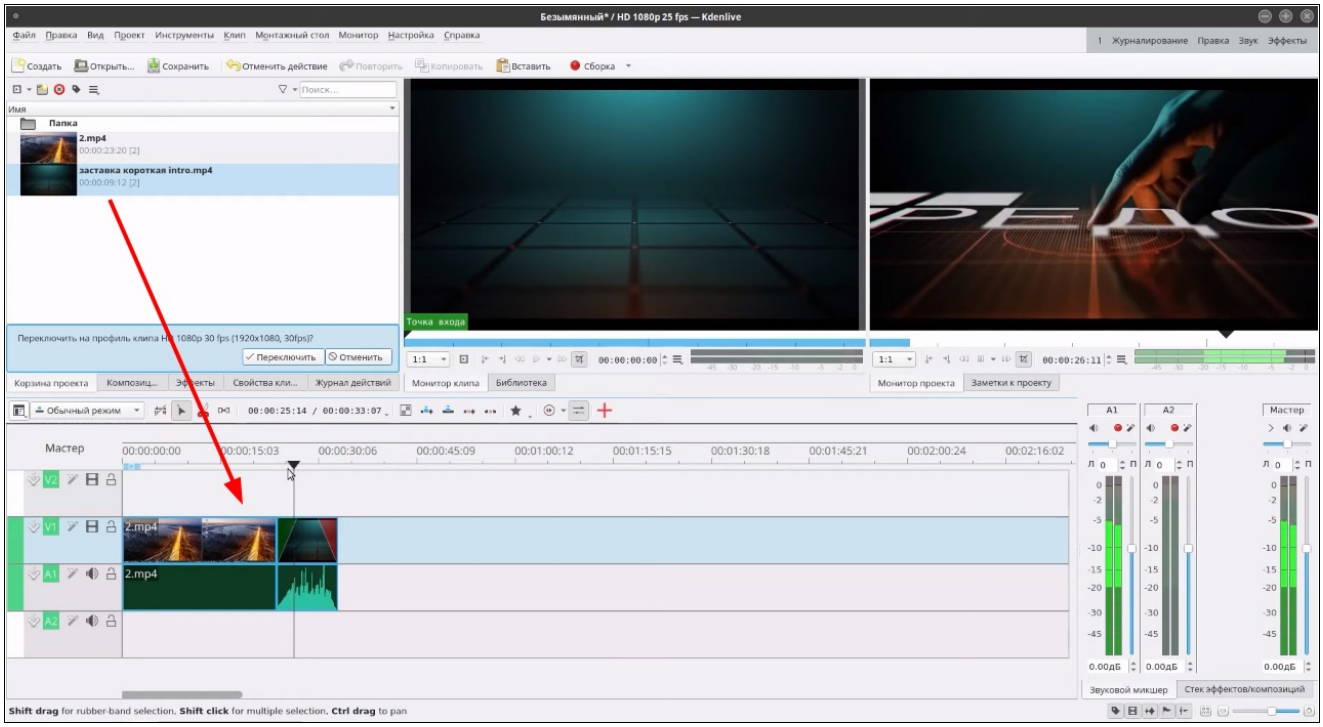
7. *Звуковые микшеры* - для первой и второй дорожек, а также один общий (мастер).

8. *Настройки для меток*, отображения миниатюр видео на монтажном столе, комментарии к маркерам, а также уровень масштабирования.

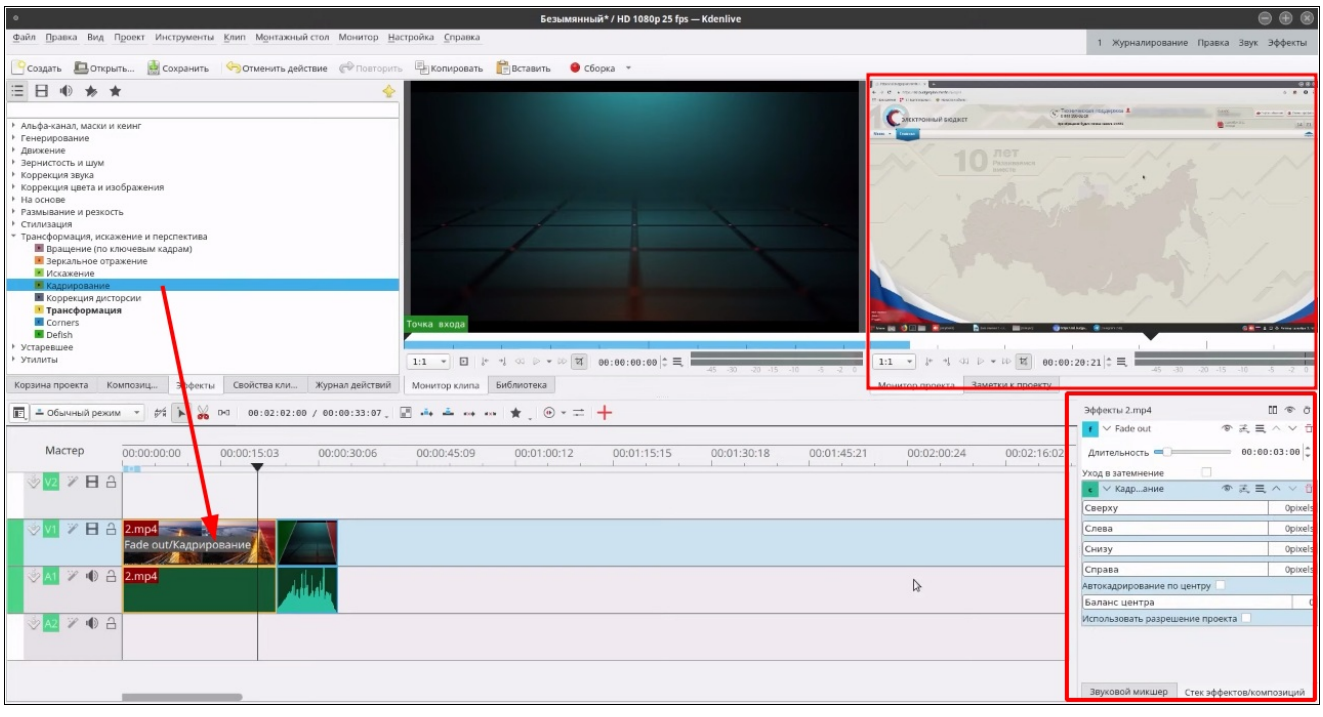
Вы можете установить удобные для себя настройки каждой области, а затем сохранить получившийся макет через пункт меню «**Вид**» - «**Сохранить макет**».

Работа с программой

Для создания нового клипа переместите из **Корзины проекта** нужные видео на **Монтажный стол**.



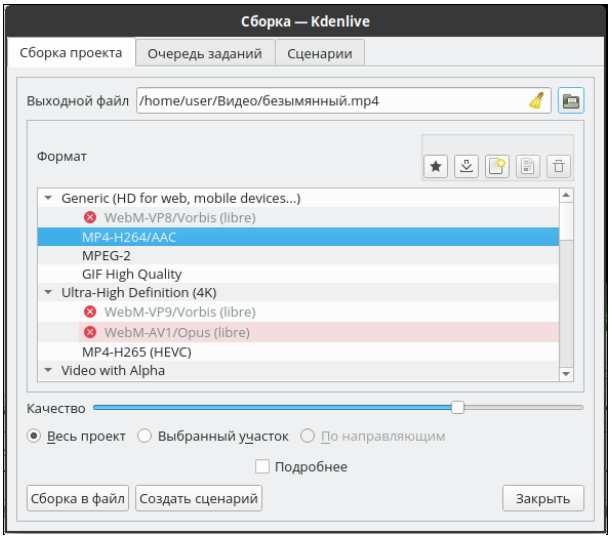
При наведении курсора на начало или конец клипа появляются точки бирюзового и красного цвета, при нажатии на которые применяется стандартный переход (fade in и fade out) соответственно. Их можно сделать короче или длиннее, перемещая точки на временной шкале. Также все примененные эффекты отображаются на миниатюре видео и в разделе **Стек эффектов**, раскрыв который вам будут доступны настройки. Дополнительно в *Стеке* можно удалить ненужный эффект либо посмотреть, как выглядело видео без примененного эффекта.



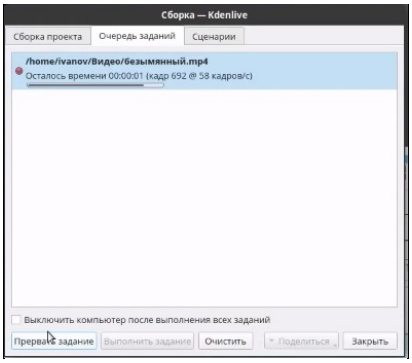
Если необходимо изменить длину отрезка видео, то при активном **Инструменте выбора** можно растянуть края видео и добиться желаемого результата. **Инструмент обрезки** делает это при наведении курсора и нажатии левой кнопки мыши, оставляя отрезанную

часть.

При завершении работы над проектом необходимо его собрать в итоговое видео. Для этого нажмите «**Сборка**» на панели инструментов. Далее потребуется выбрать путь и название для выходного файла, а также формат сохраняемого проекта.



Здесь также есть возможность сборки *всего проекта* либо *выбранного участка*. После определения всех настроек нажмите кнопку «**Сборка в файл**», будет открыта вкладка **Очередь заданий** с прогрессом готовности проекта. Здесь можно установить флаг «**Выключить компьютер после выполнения всех заданий**», если проект большой и сборка выполняется длительное время.



Видеоредактор Shotcut

Возможности Shotcut
Установка
Описание интерфейса
Создание проекта
Импорт медиафайлов
Добавление файлов на временную шкалу
Редактирование видео
Добавление аудио
Экспорт проекта

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: shotcut-21.03.21

Shotcut — это бесплатная программная платформа для редактирования видео- и аудиоформатов, которая предоставляет пользователю широкие возможности для создания собственного контента.

Возможности Shotcut

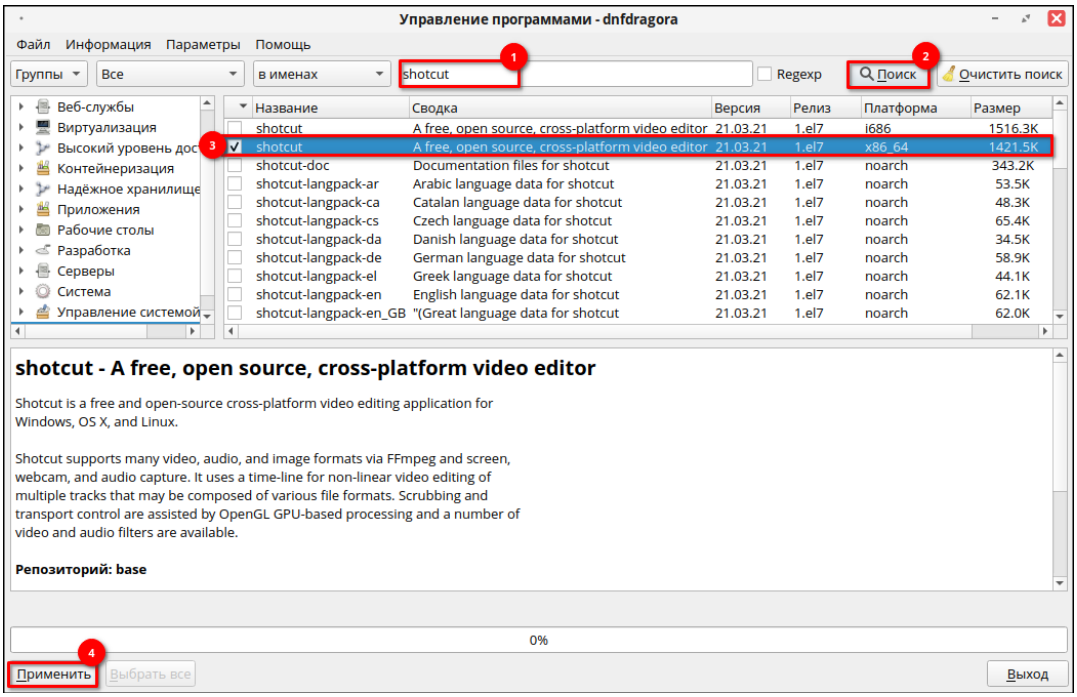
Основными возможностями программы Shotcut являются:

- простой и удобный интерфейс;
- поддержка видео- и аудиоформатов, включая HD и 4K;
- импорт различных типов файлов в проекты;
- добавление эффектов и фильтров к видео (стабилизация изображения, цветокоррекция, наложение текста и др.);
- монтаж звука;
- наложение звука на видео;
- регулировка уровня звука;
- экспорт видео в различные форматы и разрешения;
- большое количество бесплатных образцов (эффекты, фильтры, шрифты и др.).

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**shotcut**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install shotcut
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Для запуска программы через терминал введите команду:

```
shotcut
```

После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**Видеоредактор Shotcut**» (РЕД ОС 7.3) или «**Shotcut**» (РЕД ОС 8.0).

Описание интерфейса

Интерфейс Shotcut в РЕД ОС 7.3 не русифицирован по умолчанию. Для смены языка программы перейдите в меню «**Settings**» — «**Language**» — **Russian**. После выполнения настройки интерфейс станет частично русифицированным.

Интерфейс программы в РЕД ОС 8.0 русифицирован, что делает его использование более удобным.

Окно программы можно визуально разделить на шесть основных зон:

1. **Основное меню** состоит из шести пунктов.

- **Файл** — позволяет открыть/закрыть, создать или экспортировать видеоролик.
- **Правка** — используется для отмены и повтора действий, а также для вырезания, копирования и вставки.
- **Вид** — настройка видимых панелей, размера окна и прочих параметров отображения.
- **Проигрыватель** — используется для настройки времени перехода вперёд/назад, обрезки клипа, а также для переключения между источником и проектом.
- **Настройки** — настройка параметров программы.
- **Справка** — содержит различную информацию, включая ссылки на полезные статьи, форумы, уроки, раздел вопросов и ответов.

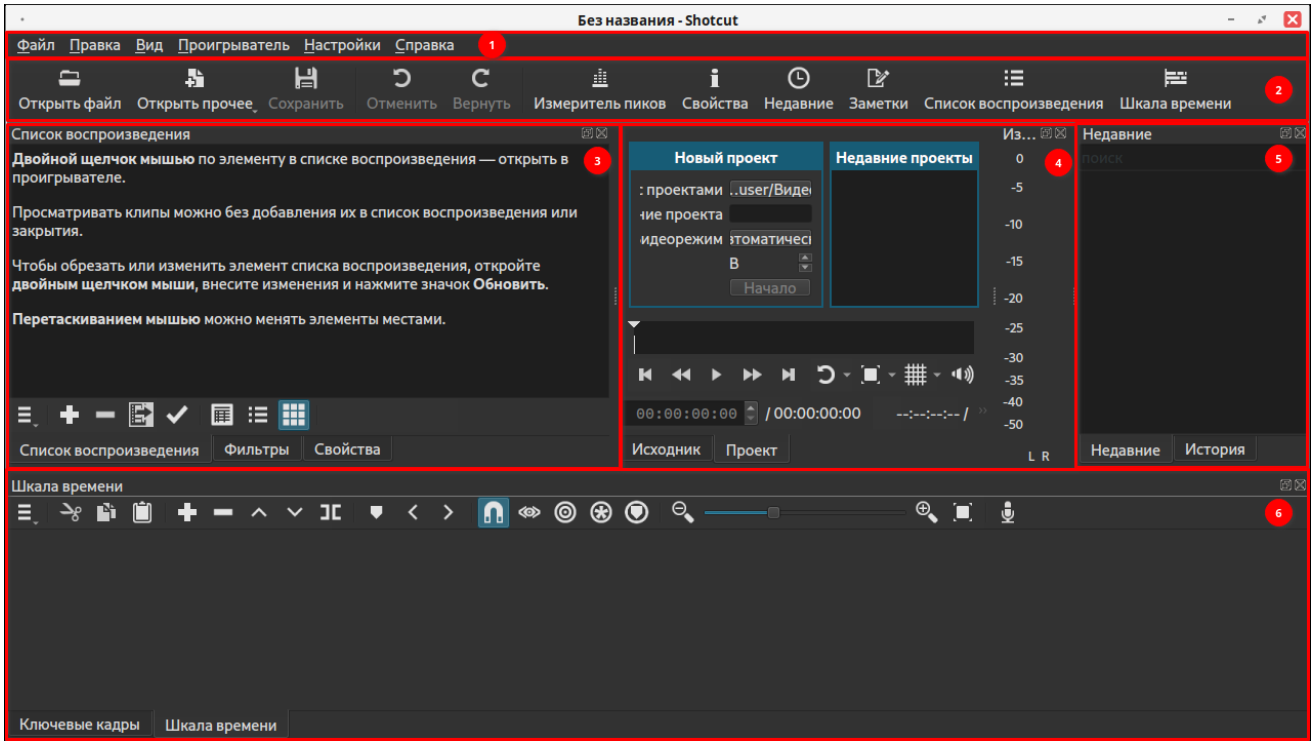
2. **Панель инструментов** — предоставляет быстрый доступ к основным опциям программы. По умолчанию видны не все доступные опции, чтобы увидеть полный список, нажмите на стрелку справа.

3. **Свойства** — отображает все данные о ролике, с которым ведётся работа в текущий момент. Здесь также расположен список использованных фильтров и список воспроизведения.

4. **Проигрыватель** — область для просмотра видеоролика.

5. **Дополнительная информация** — по умолчанию в этой зоне отображается список файлов, с которыми пользователь недавно работал. Также здесь откроется перечень заданий либо история.

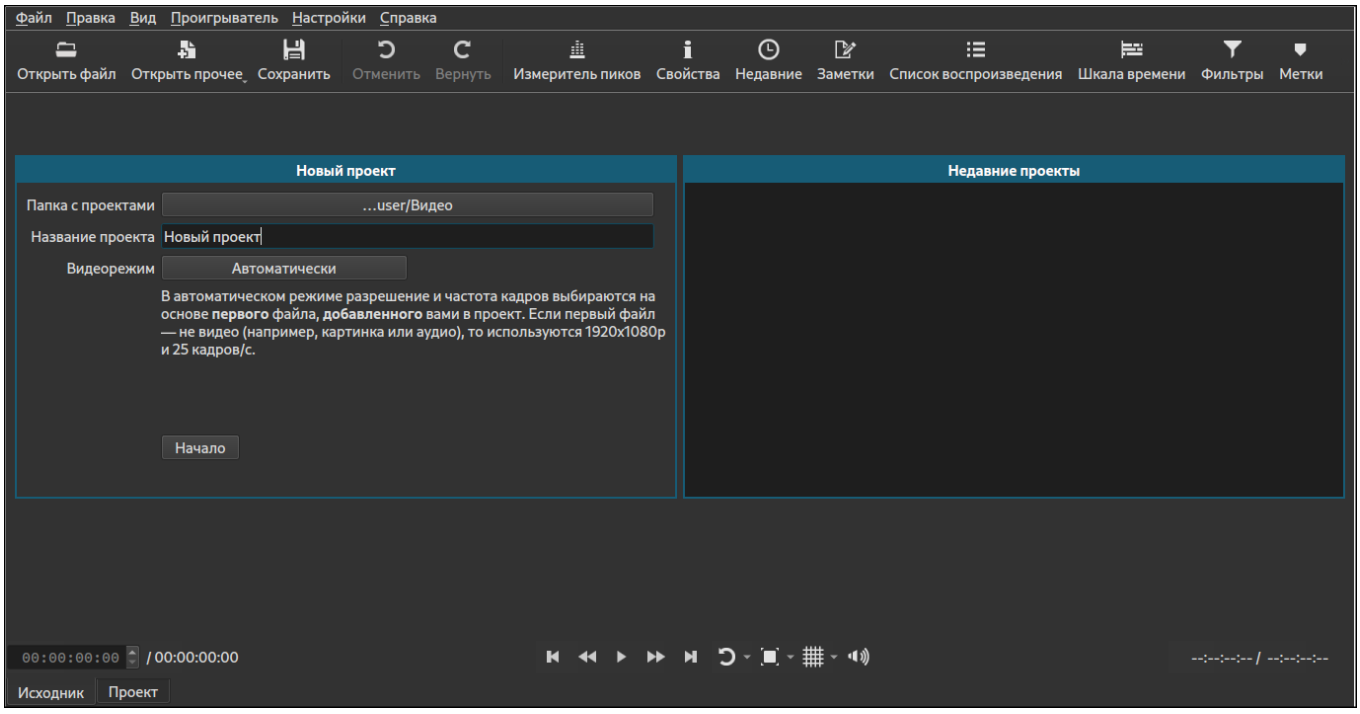
6. **Область монтажа** — по умолчанию в этой области расположены шкала времени и ключевые кадры видеоролика, внизу окна находится переключатель вкладок.



Создание проекта

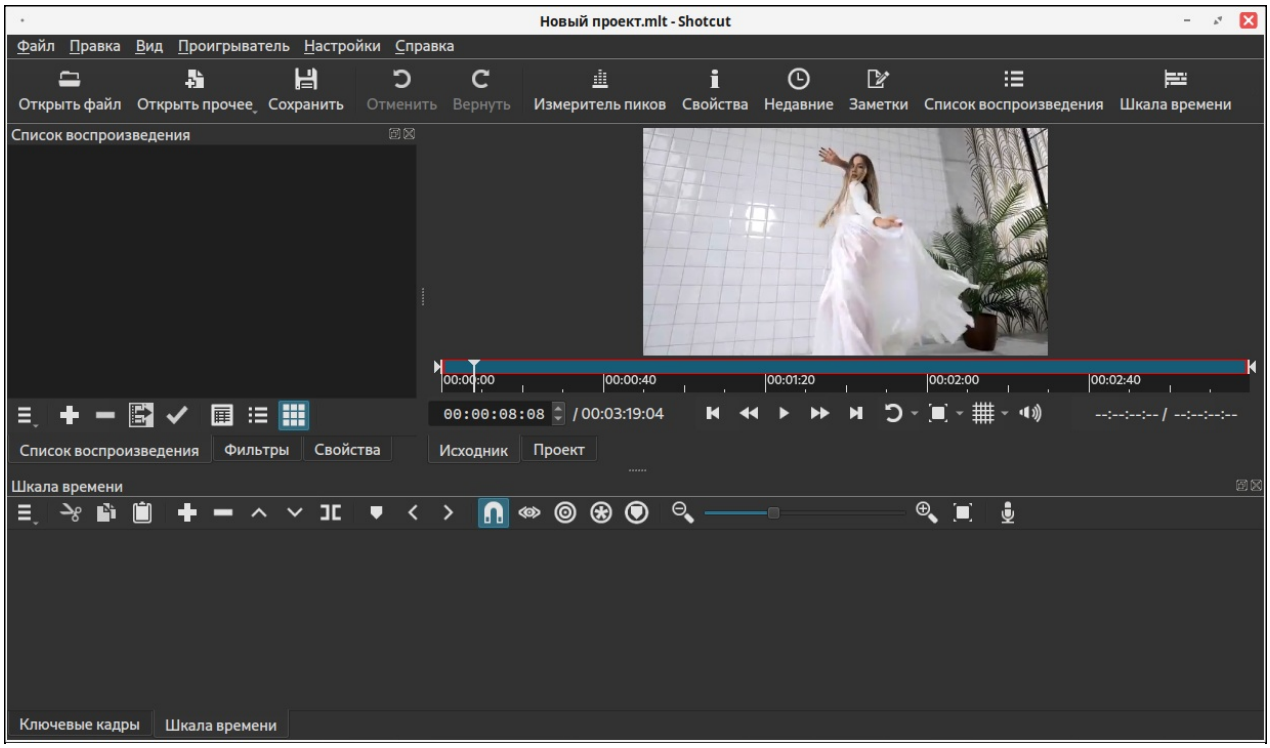
Окно создания нового проекта автоматически открывается сразу же после запуска программы.

Для создания нового проекта выберите в основном меню пункт «**Файл**» — «**Новый**» или нажмите комбинацию клавиш Ctrl+N. В открывшемся окне выберите папку для сохранения проекта, укажите название проекта, при необходимости выберите видеорежим.



Импорт медиафайлов

Для импорта медиафайла в проигрыватель перейдите в меню «**Файл**» — «**Открыть файл...**». Выберите видеоролик и нажмите «**Открыть**». Видеоролик появится в проигрывателе. При добавлении нескольких файлов они отображаются в списке воспроизведения.



Добавление файлов на временную шкалу

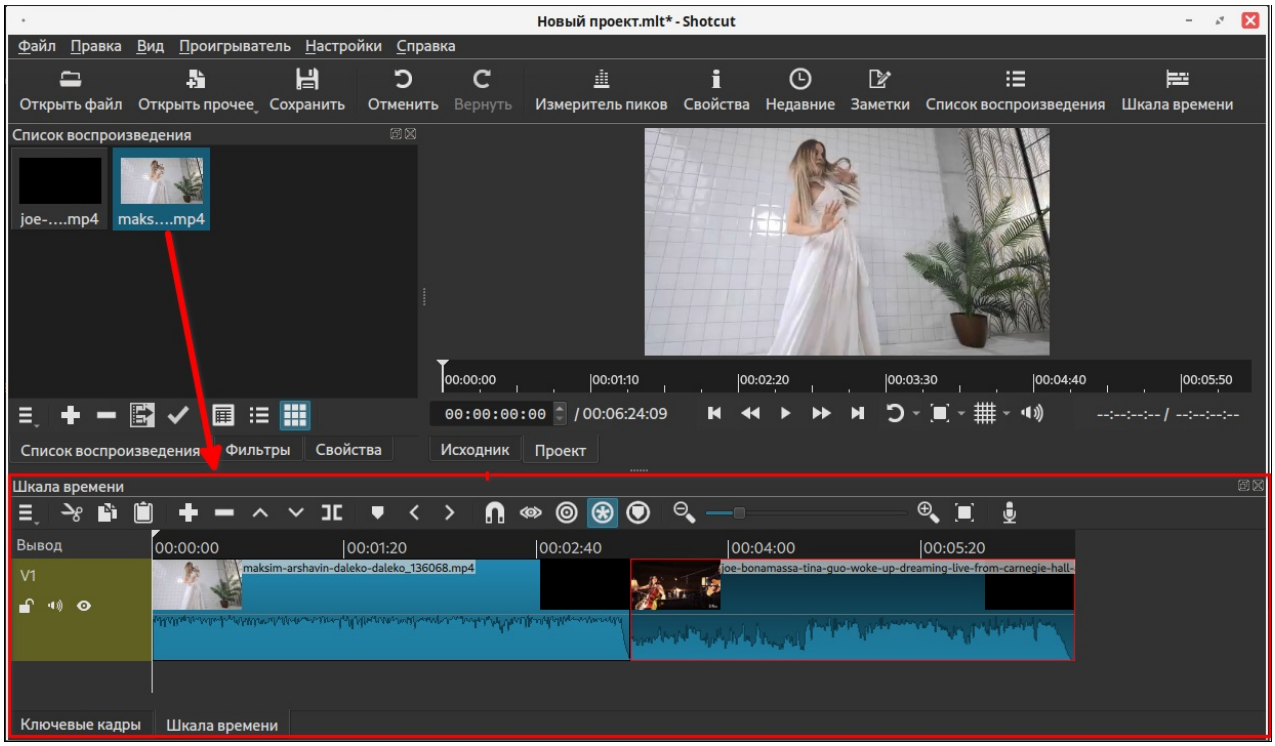
Добавление файлов на временную шкалу позволяет организовать и упорядочить медиафайлы в проекте.

Первый способ:

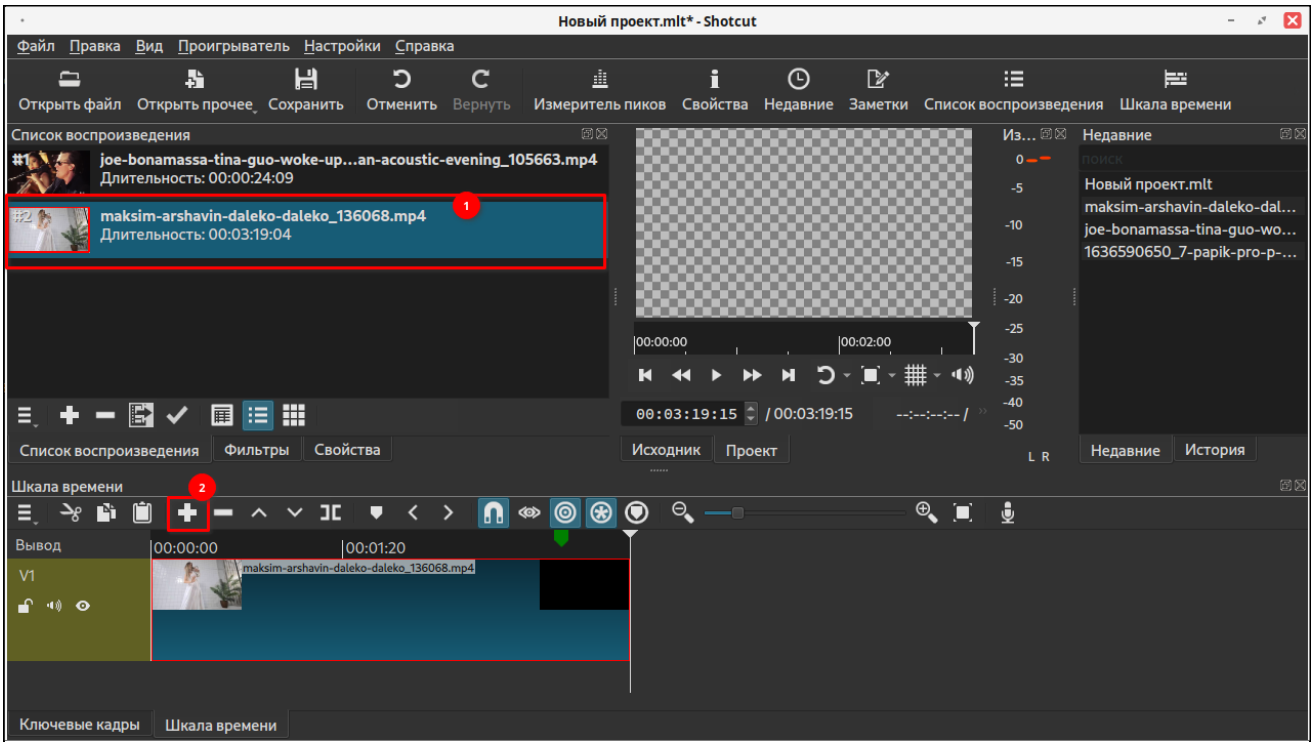
1. Импортируйте необходимые файлы в проект.

2. Перетащите файлы из списка воспроизведения на временную шкалу.

3. Разместите файлы в нужном порядке.

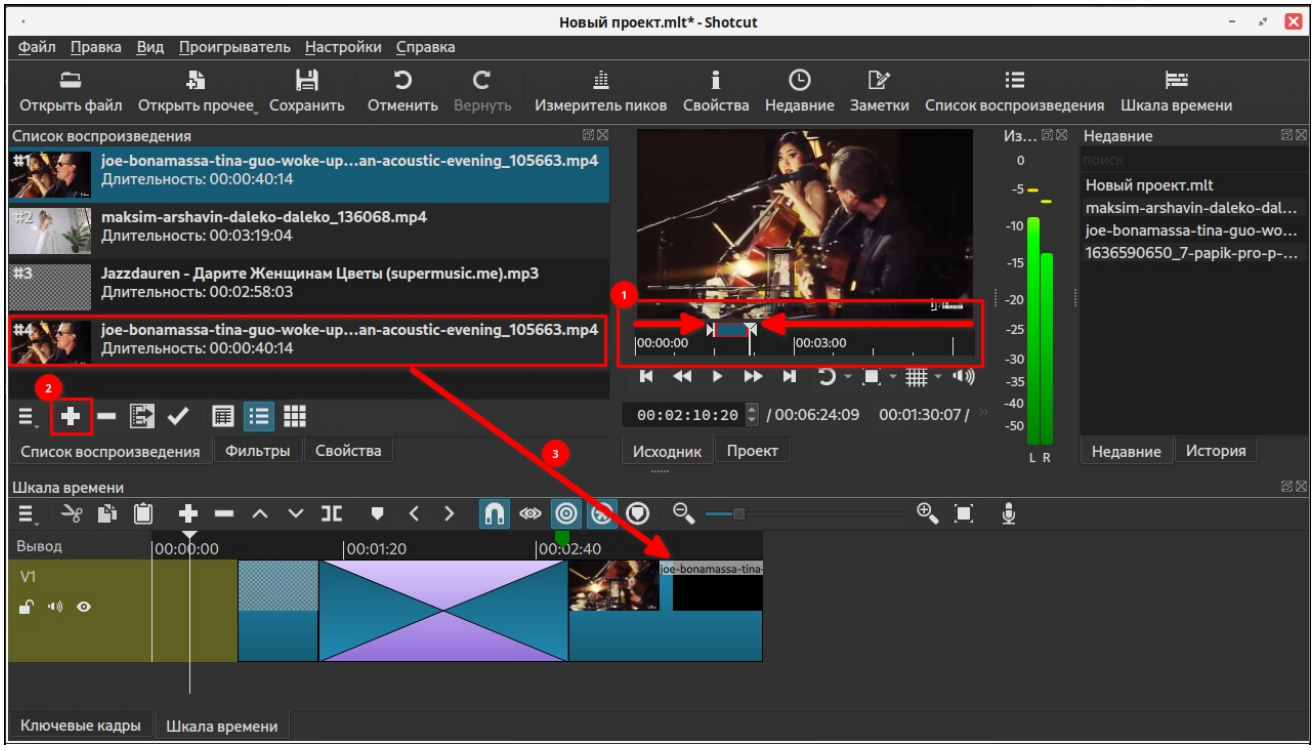


Второй способ. Для добавления файлов на временную шкалу дважды щелкните по нужному видео в списке воспроизведения (1) и на панели инструментов временной шкалы нажмите кнопку «**Добавить**» (2).



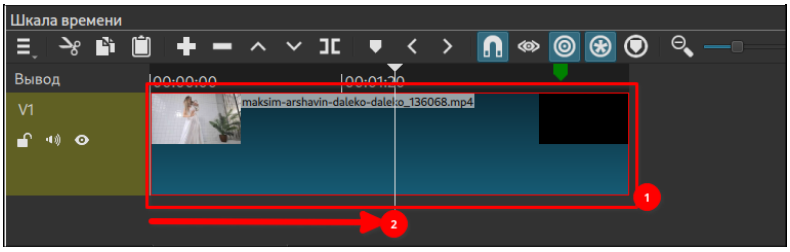
Редактирование видео

Для использования части видео в проигрывателе сдвиньте временные метки (1), нажмите «**Добавить источник в список воспроизведения**» (2) и перетащите сцену на временную шкалу (3).

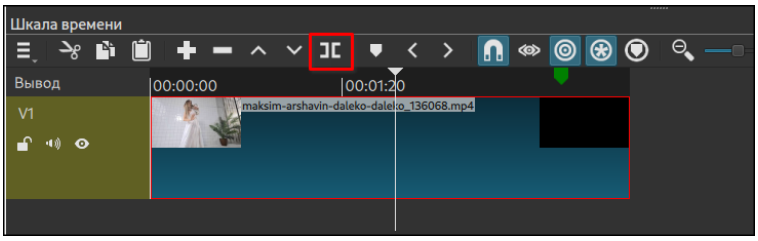


Для обрезки видео выполните следующие действия.

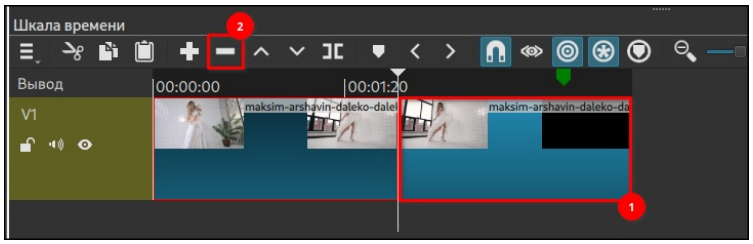
1. Выделите кадр и переместите указатель воспроизведения к точке, где клип нужно разделить.



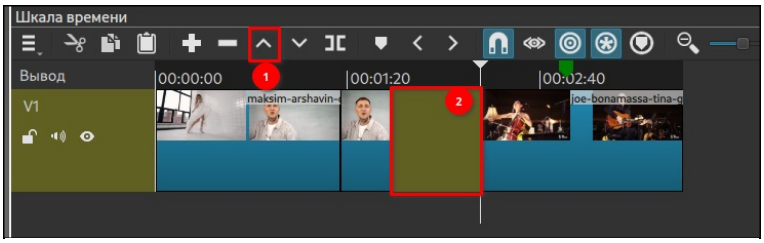
2. Выберите инструмент «**Разделение по точкам воспроизведения**».



В результате появятся два фрагмента видео. Для удаления лишнего фрагмента выберите его (1) и нажмите кнопку «**Удалить**» (2). Лишний фрагмент будет удалён. Следующий клип сдвинется на место вырезанного фрагмента.



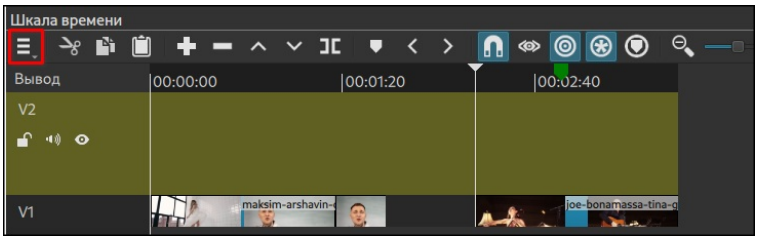
Если необходимо оставить пустое пространство вместо вырезанного фрагмента, выберите фрагмент и нажмите «**Поднять**» (1). На месте вырезанного фрагмента останется незаполненное пространство (2).



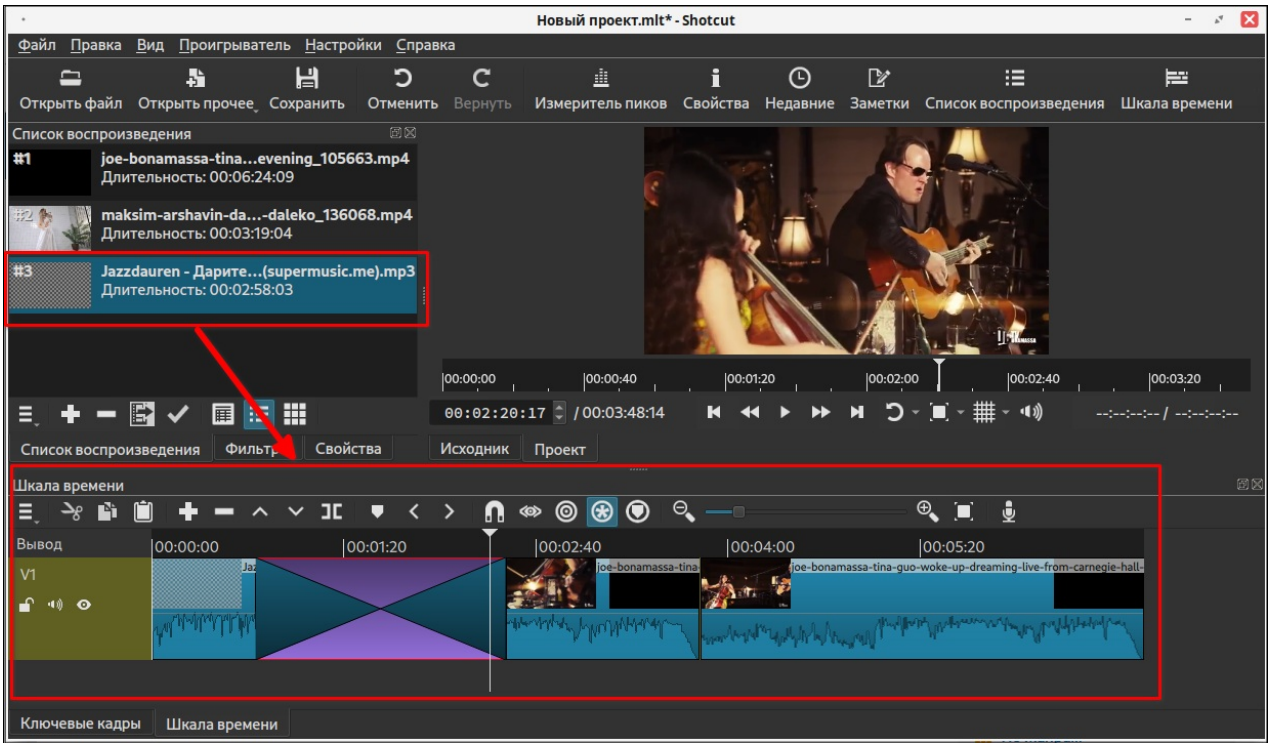
Добавление аудио

Shotcut позволяет использовать аудиофайлы с компьютера для озвучки. Пользователи могут полностью заменить звук или изменить его частично.

Для добавления аудиодорожки перейдите в меню временной шкалы и из выпадающего списка выберите «**Действия с дорожкой**» — «**Вставить дорожку**». На временной шкале отобразится аудиодорожка.



Для добавления аудио в проект перетащите аудиофайлы из списка воспроизведения на аудиодорожку на временной шкале. Настройте громкость и добавьте эффекты.

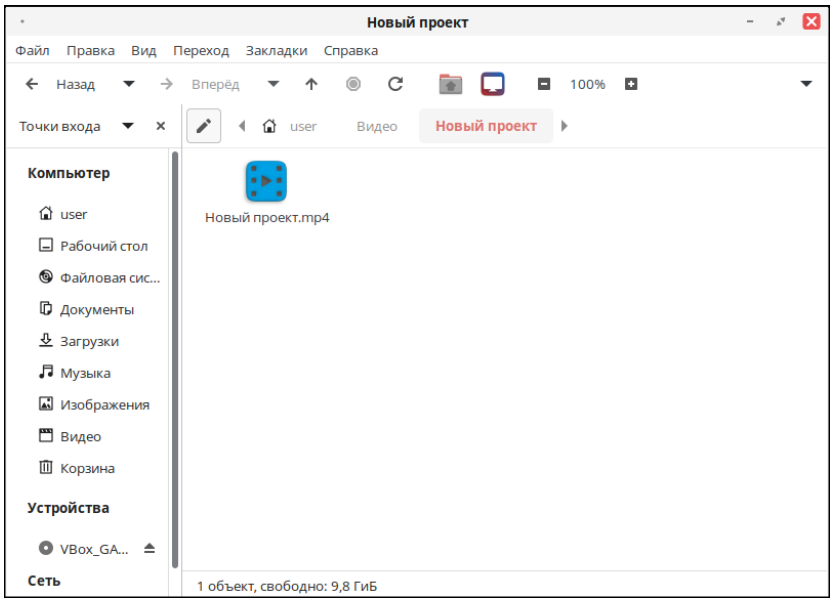


Экспорт проекта

После завершения обработки материала можно сохранить проект. Для этого перейдите в меню «**Файл**» — «**Экспорт**» — «**Видео...**».

Введите название проекта, выберите каталог и нажмите «**Сохранить**».

Проект будет экспортирован в выбранный видеоформат.



Видеоредактор OBS Studio

Установка
Описание программы
Первоначальная настройка
Настройки звука/микрофона, видео
Запись аудио
Запись экрана и звука
Ремультиплексирование записей

Окружение

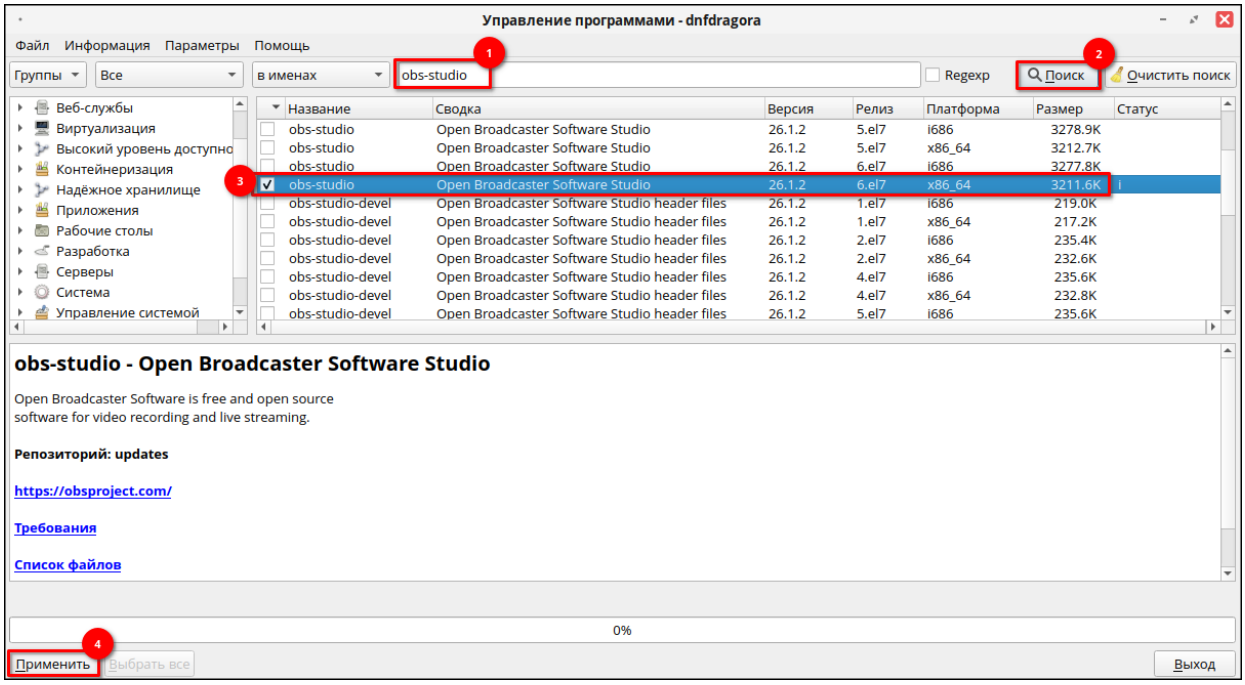
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: obs-26.1.2

OBS Studio (Open Broadcaster Software Studio) — это программа для потокового вещания (стримов) и записи видео. Приложение поддерживает работу с несколькими источниками одновременно, позволяет комбинировать различные видео/аудиопотоки, создавая непрерывную трансляцию, что подходит для трансляций игр, проведения семинаров, онлайн-фестивалей.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**obs-studio**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install obs-studio
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

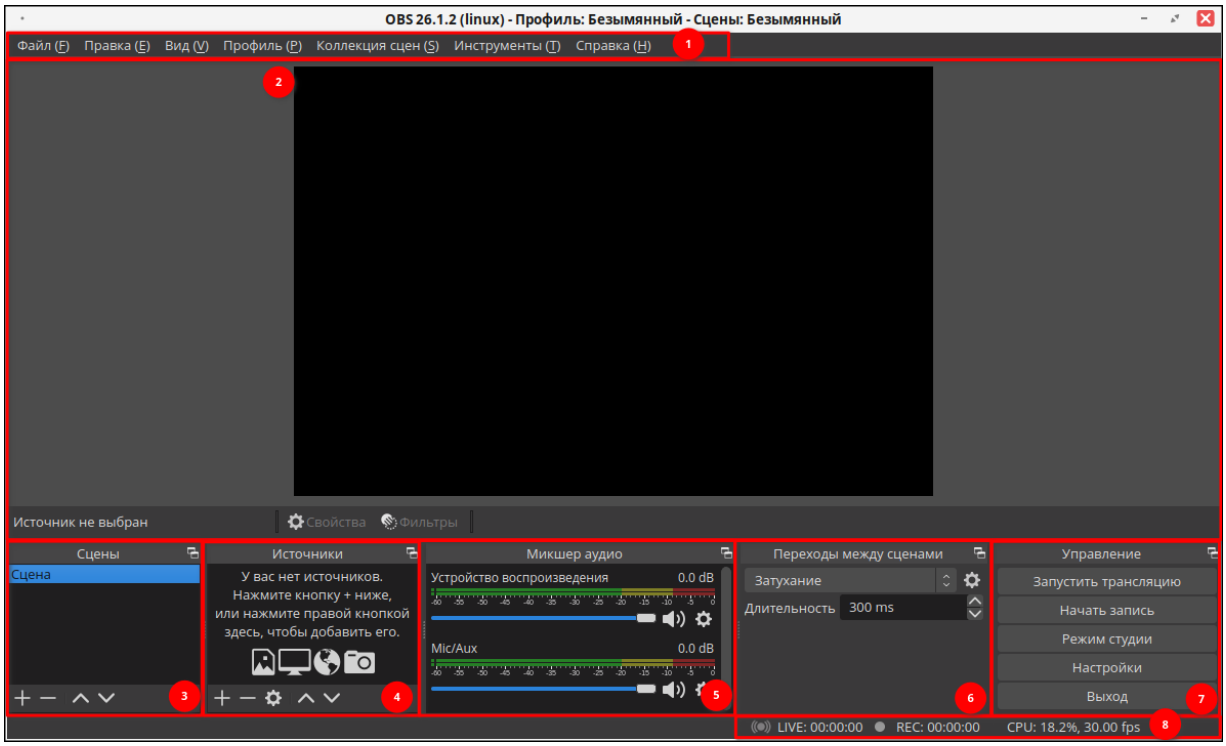
Для запуска программы через терминал введите команду:

```
obs studio
```

После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**OBS Studio**».

Описание программы

Главное окно программы состоит из нескольких типовых частей.



1. **Основное меню программы** позволяет выполнять различные действия с создаваемым файлом, а также настраивать программу и панель инструментов.

2. **Рабочая область** отображает видео- и аудиоконтент.

3. **Сцены** — список всех сцен, которые созданы в **OBS Studio**.

4. **Источники** — список всех источников (например, видеокамеры, микрофоны, экраны).

5. **Микшер аудио** позволяет регулировать уровни аудиосигналов и настраивать аудиоэффекты.

6 . **Переходы между сценами** позволяют настроить переходы между сценами, чтобы сделать видео более плавным и профессиональным.

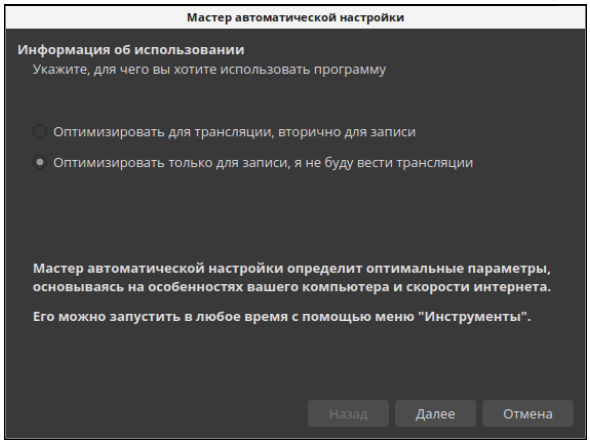
7 . **Панель управления трансляцией** позволяет настроить параметры трансляции, такие как выбор сервера, настройка качества видео и аудио, и т. д.

8. **Строка состояния трансляции** отображает информацию о текущем состоянии трансляции, например, статус соединения, качество видео и аудио, и т. д.

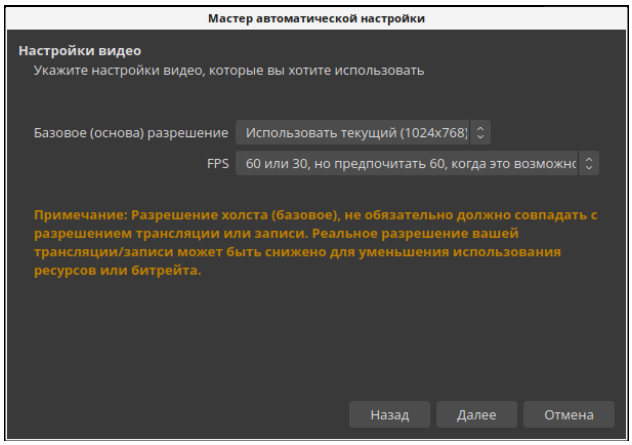
Первоначальная настройка

Для первоначальной настройки необходимо выполнить следующий алгоритм действий:

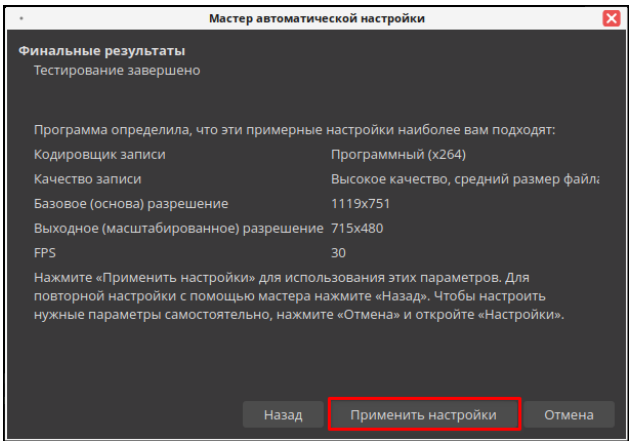
1. При первой загрузке **OBS Studio** запустится мастер автоматической настройки.



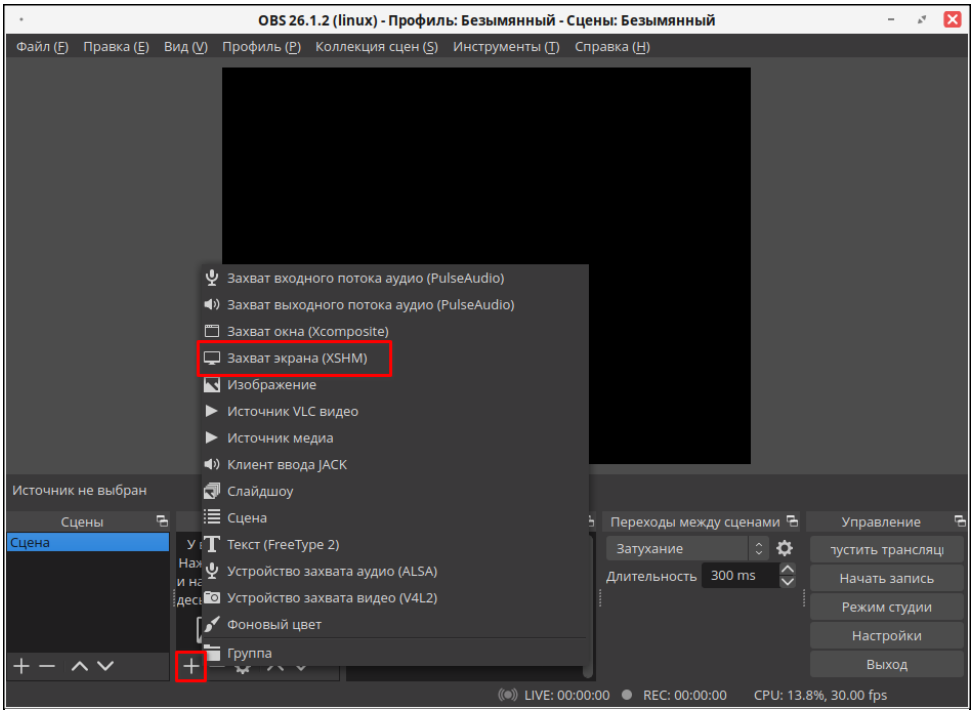
Следуйте инструкциям, чтобы получить подходящие начальные настройки видео.



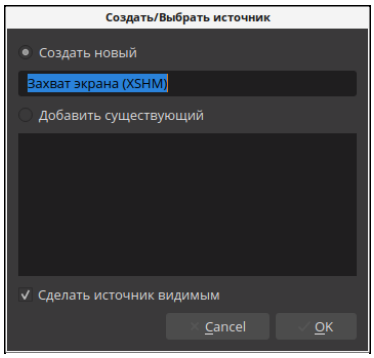
По окончании настроек нажмите «**Применить настройки**» для использования выбранных параметров.



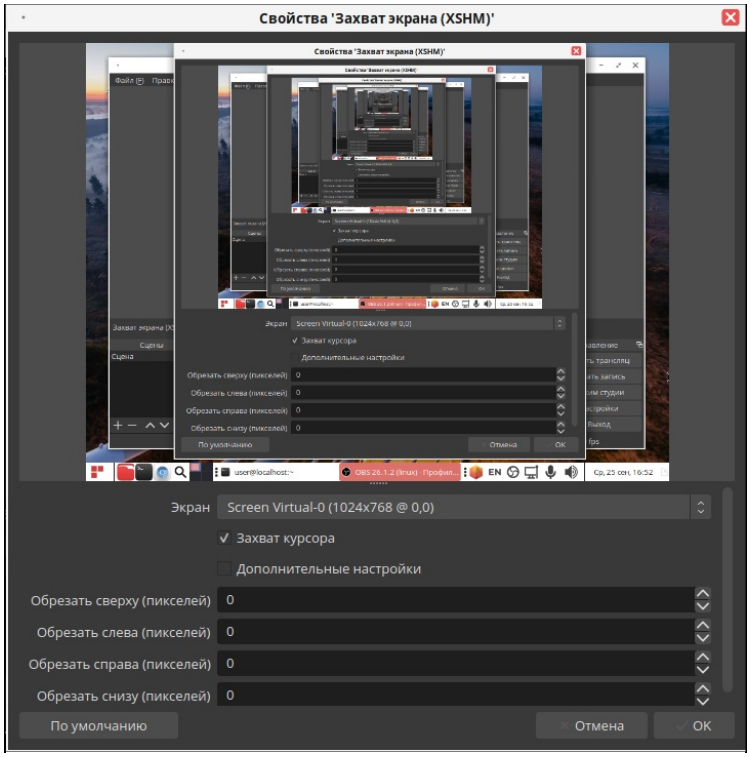
2. Добавьте источники к сценам. Для добавления нового источника нажмите на значок  на панели «**Источники**», расположенной в нижней части главного экрана. Выберите источник, например, «**Захват экрана (XSHM)**».



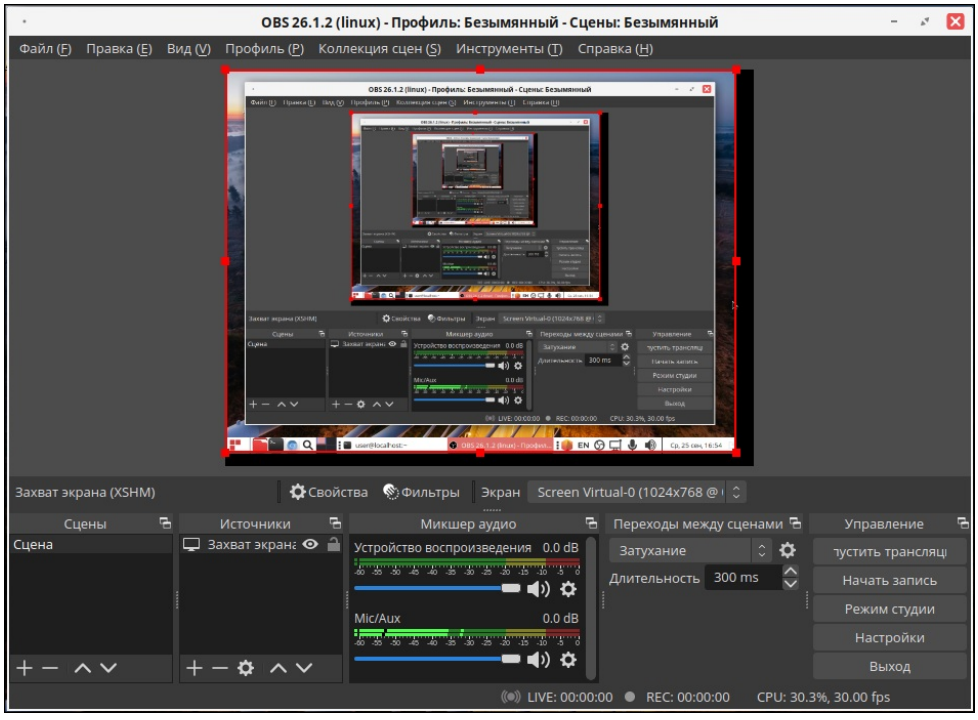
Напишите наименование источника и нажмите «**OK**».



В открывшемся окне выберите экран и нажмите «**OK**».



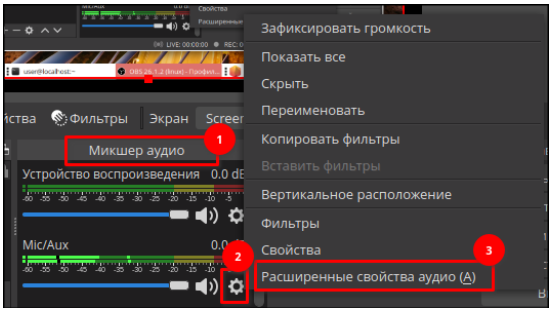
Выбранный экран отобразится в рабочей области.



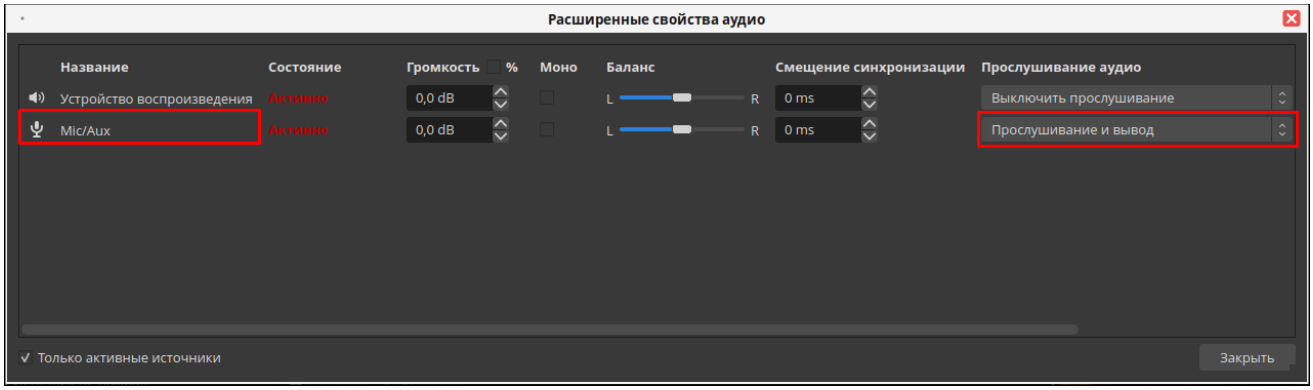
Для изменения размера источника кликните на его название и в рабочей области появится красная граница вокруг него. Для изменения размера потяните мышкой за одну из сторон источника.

3. Настройте аудио. В панели «**Микшер аудио**» (1) выберите рядом с источником медиа «**Свойства**» (2) — «**Расширенные настройки**

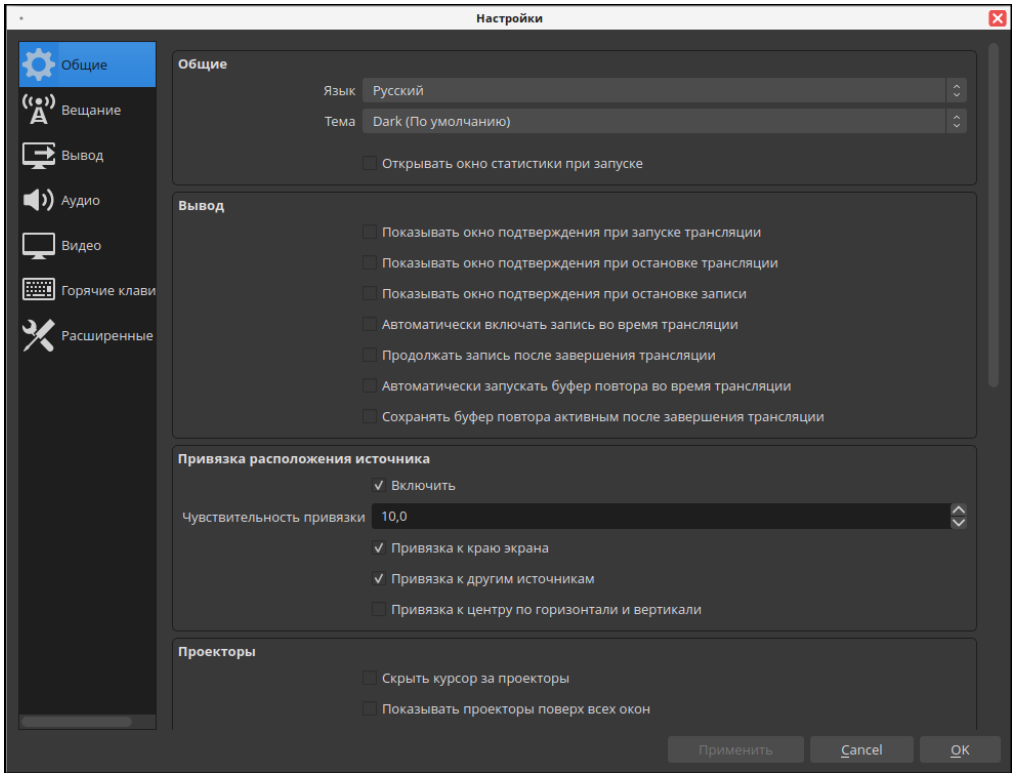
аудио»(3).



В окне настроек аудио выберите желаемый источник аудио и в параметре «**Прослушивание аудио**» выберите «**Прослушивание и вывод**».



4. Откройте панель с общими настройками в меню «**Файл**» — «**Настройки**». После открытия окна с общими настройками можно выбрать необходимые параметры.



В разделе Общие можно выбрать тёмную или светлую тему оформления, выбрать привязку расположения источника, показывать подтверждение для запуска/остановки потоков, включить/отключить автоматическую запись при потоковой передаче.

В разделе Вещание можно выбрать одну из включенных служб, установить пользовательский сервер потоковой передачи, выбрать сервер, ввести свой ключ потока.

В разделе Вывод можно настроить расширенный режим вывода для настройки потока и записи.

В разделе Аудио можно изменить частоту дискретизации, выбрать до двух настольных аудиоустройств, до трех микрофонов, вспомогательных устройств, включить дополнительные функции для каждого устройства.

В разделе Видео можно задать разрешение. **Базовое разрешение** — должно соответствовать разрешению дисплея используемого

монитора. **Выходное разрешение** — должно соответствовать выходному разрешению потока/записи. **Общее значение** FPS должно соответствовать желаемому выходному FPS.

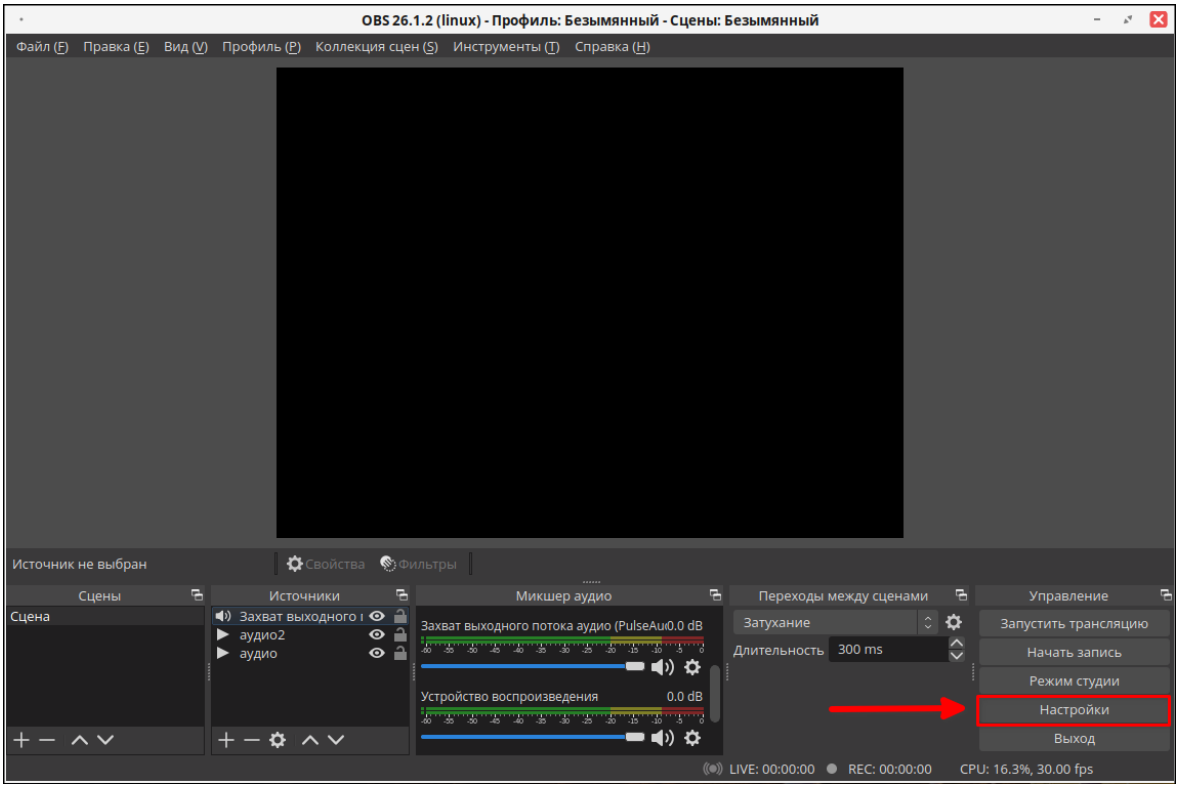
В разделе Горячие клавиши можно настроить быстрый доступ к тем или иным действиям.

В разделе Расширенные настройки можно активировать задержку потока, настроить автоматическое повторное подключение.

Настройки звука/микрофона, видео

Чтобы настроить **OBS Studio** для записи видео, выполните следующий алгоритм действий:

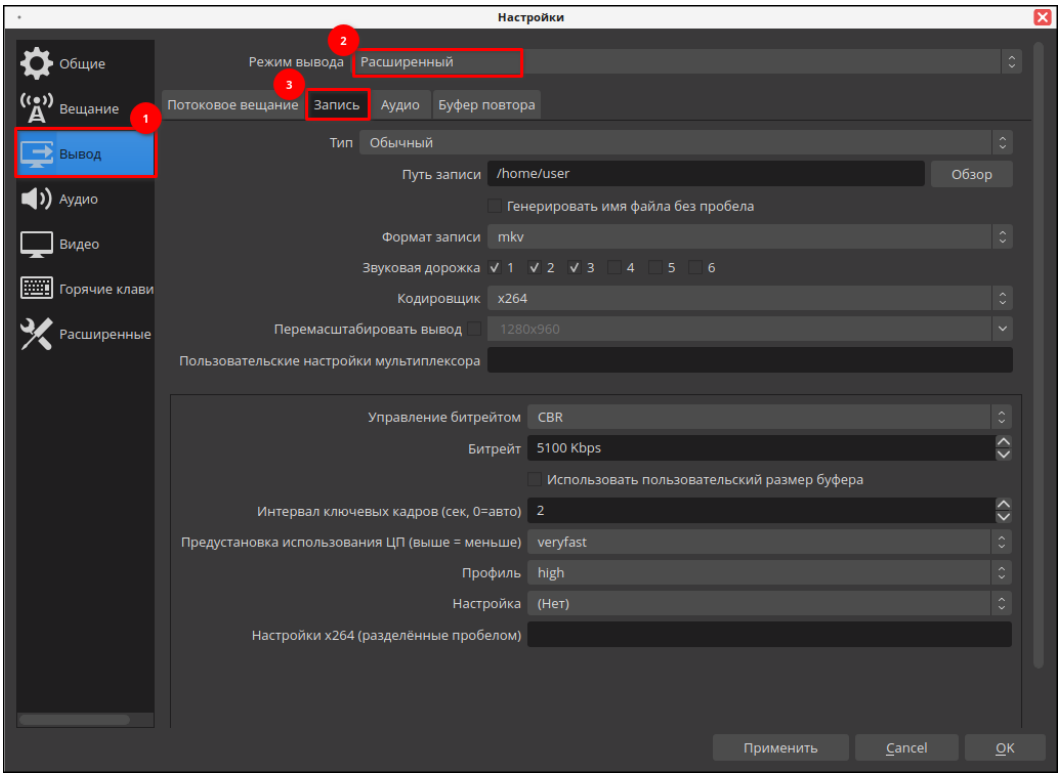
1. На панели управления трансляцией откройте «**Настройки**».



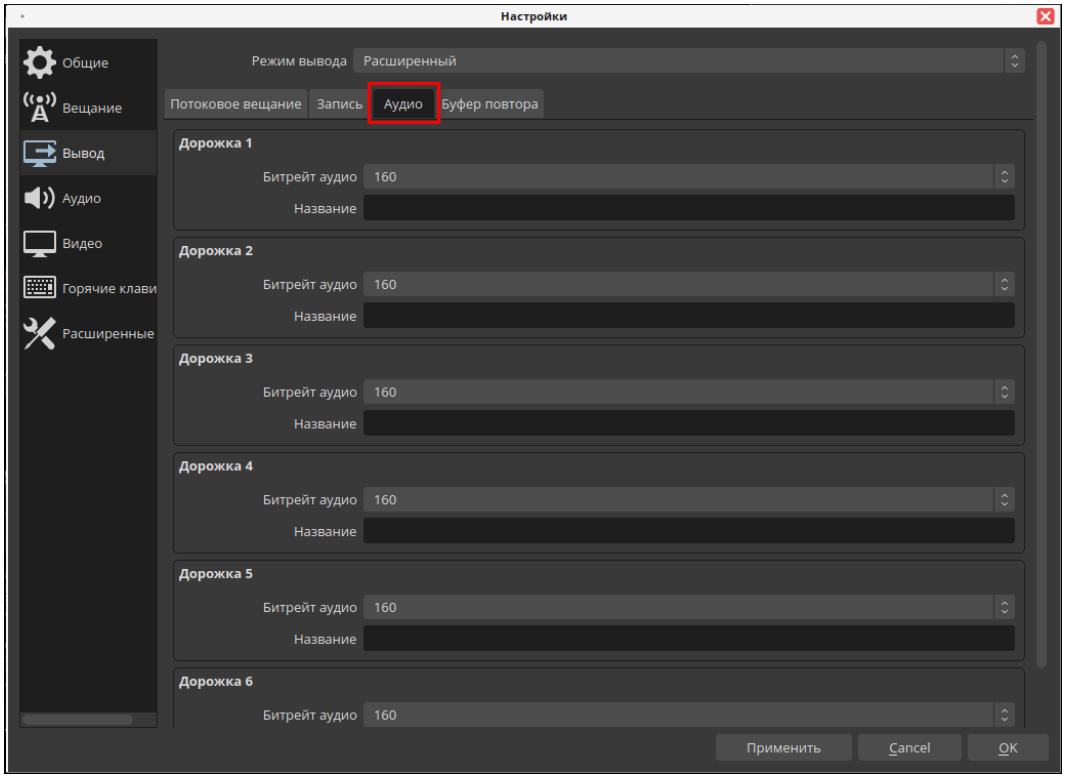
2. Перейдите в раздел Вывод. Установите режим вывода на «**Расширенный**».

На вкладке «**Запись**» установите следующие параметры:

- Тип записи: обычный;
- Путь записи: укажите удобный путь для записи;
- Формат записи: MKV;
- Звуковая дорожка: установите звуковые дорожки: 1, 2, 3 (например, дорожка 2 - микрофон, дорожка 3 - все системные звуки);
- Кодировщик: выберите кодировщик;
- Битрейт: 5100 Kbps;
- Интервал ключевых кадров: 2 сек.;
- Предустановка использования ЦП: veryfast;
- Профиль: high.



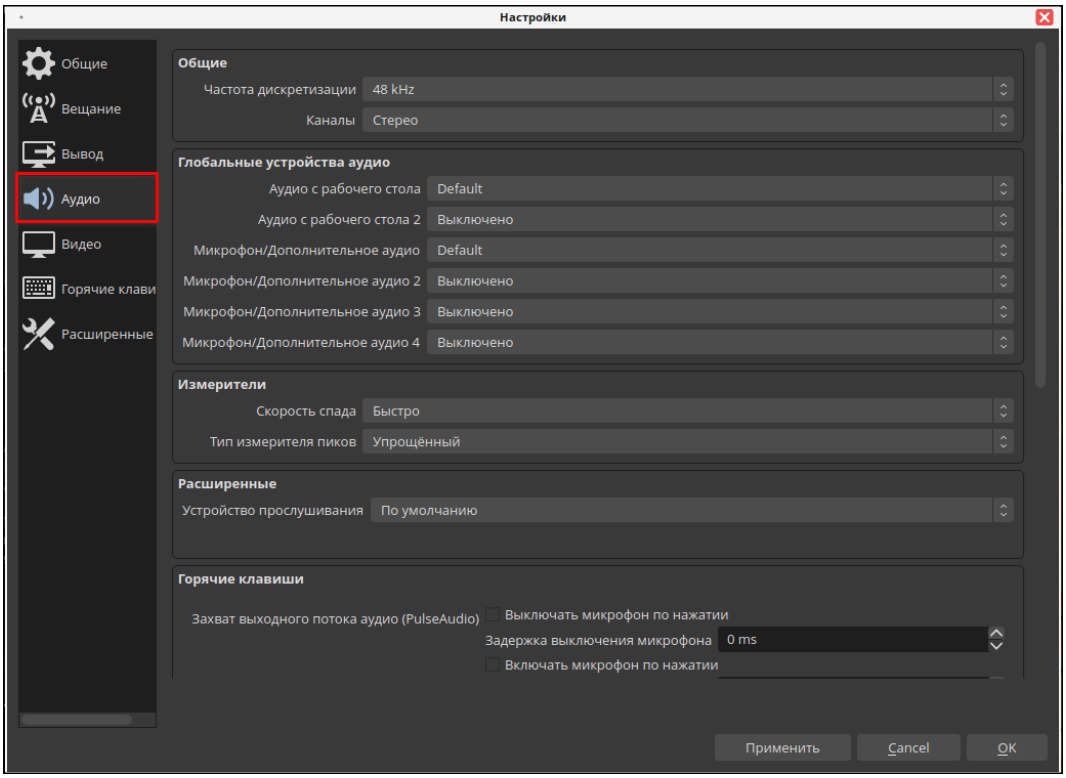
На вкладке «**Аудио**» установите битрейт аудио на дорожках — 160.



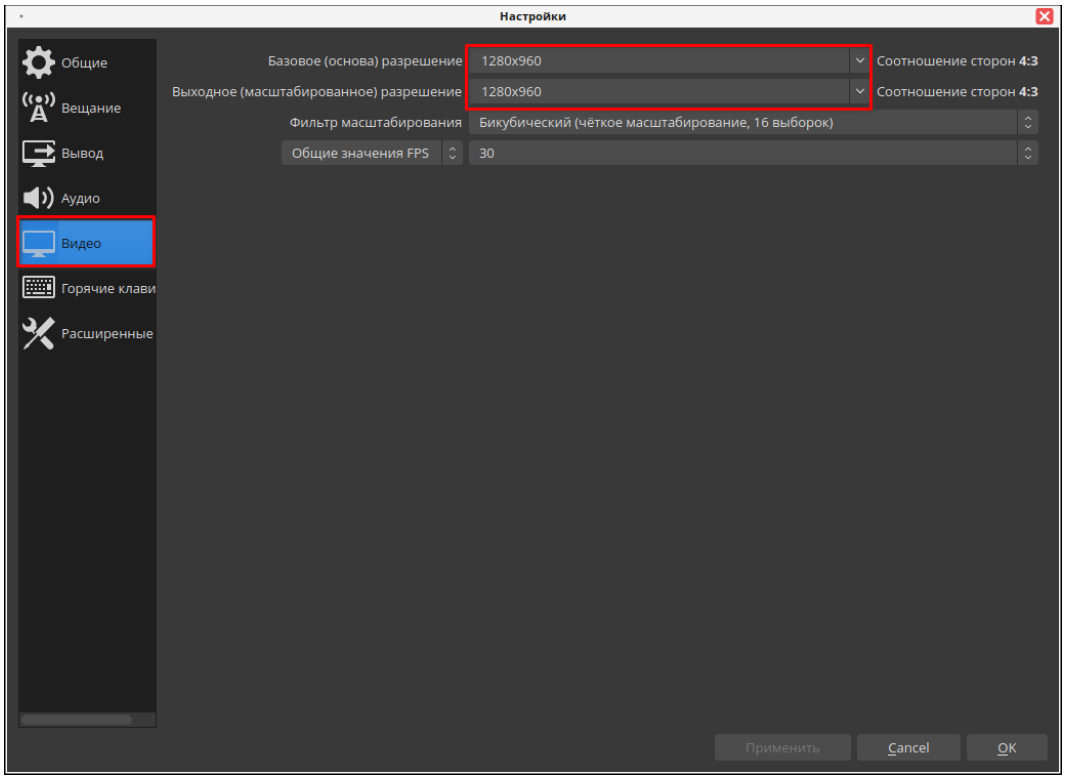
3. Перейдите в раздел Аудио.

Установите следующие параметры:

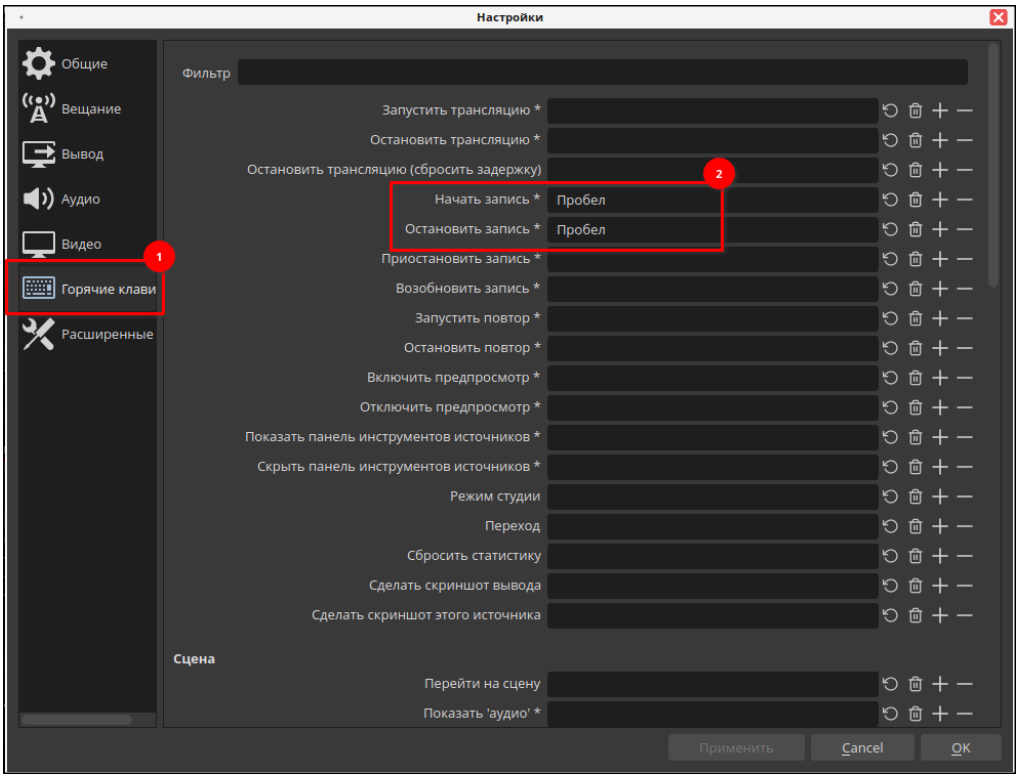
- Частота дискретизации: 48;
- Каналы: Стерео;
- Аудио с рабочего стола: Default;
- Звук рабочего стола: отключено;
- Микрофон: Default.



4. В разделе Видео установите разрешение экрана используемого монитора. Например, 1280*960.

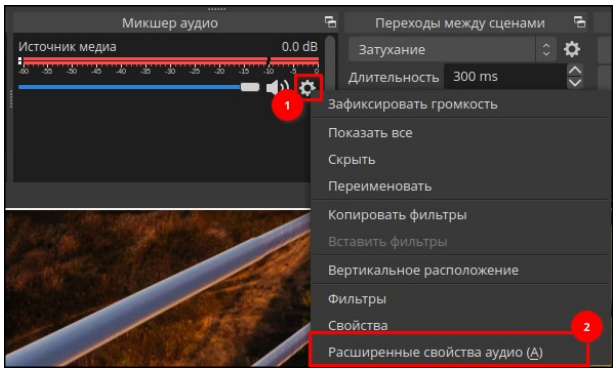


5. В разделе Горячие клавиши установите значение «**Пробел**» для пунктов «**Начать запись**» и «**Остановить запись**».



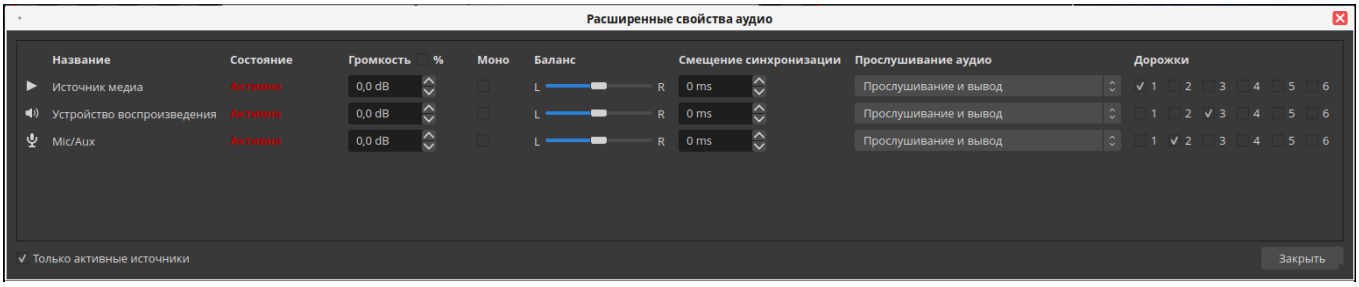
Нажмите «**Применить**» и «**OK**».

6. Перейдите в Микшер аудио, щёлкните на значок  и выберите «**Расширенные свойства аудио**».



В левой части окна отобразятся названия источников звука, а в правой — звуковые дорожки.

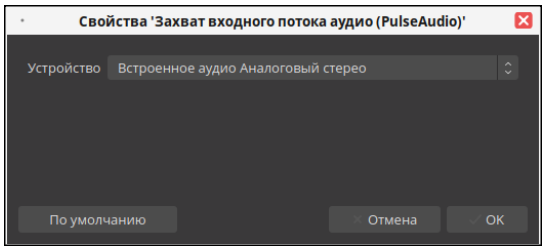
Установите напротив каждого источника флаг рядом с определенной дорожкой.



Запись аудио

Для записи аудио выполните следующий алгоритм действий:

1. Нажмите на кнопку  и выберите источник звука «**Захват входного потока аудио**». Выберите устройство.



2. Нажмите «**Начать запись**» (или воспользуйтесь горячей клавишей), чтобы начать запись видео с экрана. Красная точка на значке REC в нижней части экрана указывает на то, что запись началась.

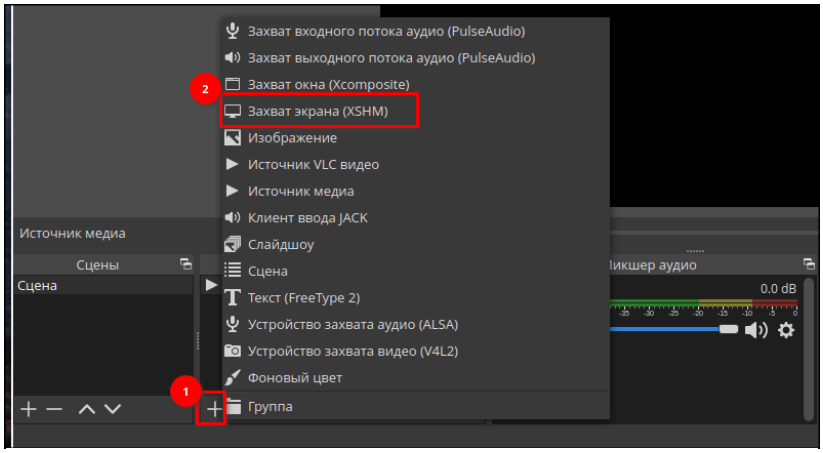
3. Чтобы остановить запись, нажмите на кнопку «**Остановить запись**» (или используйте горячую клавишу).

4. Для просмотра записей перейдите в меню «**Файл**» — «**Показать записи**».

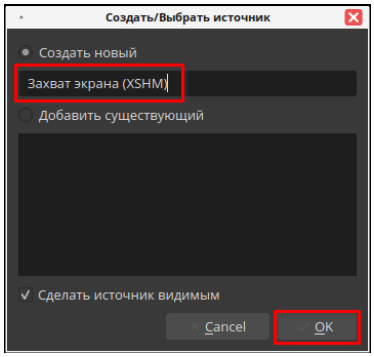
Запись экрана и звука

Для записи видео экрана и звука используется функция захвата экрана.

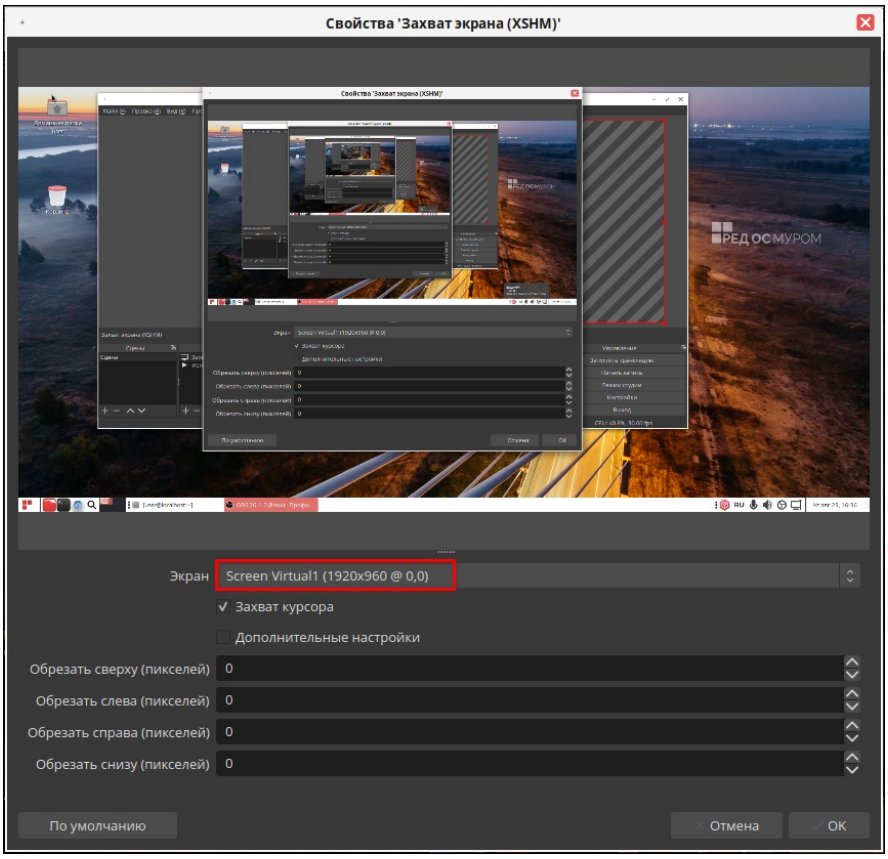
1.Нажмите на кнопку  и выберите «**Захват экрана**» из списка источников.



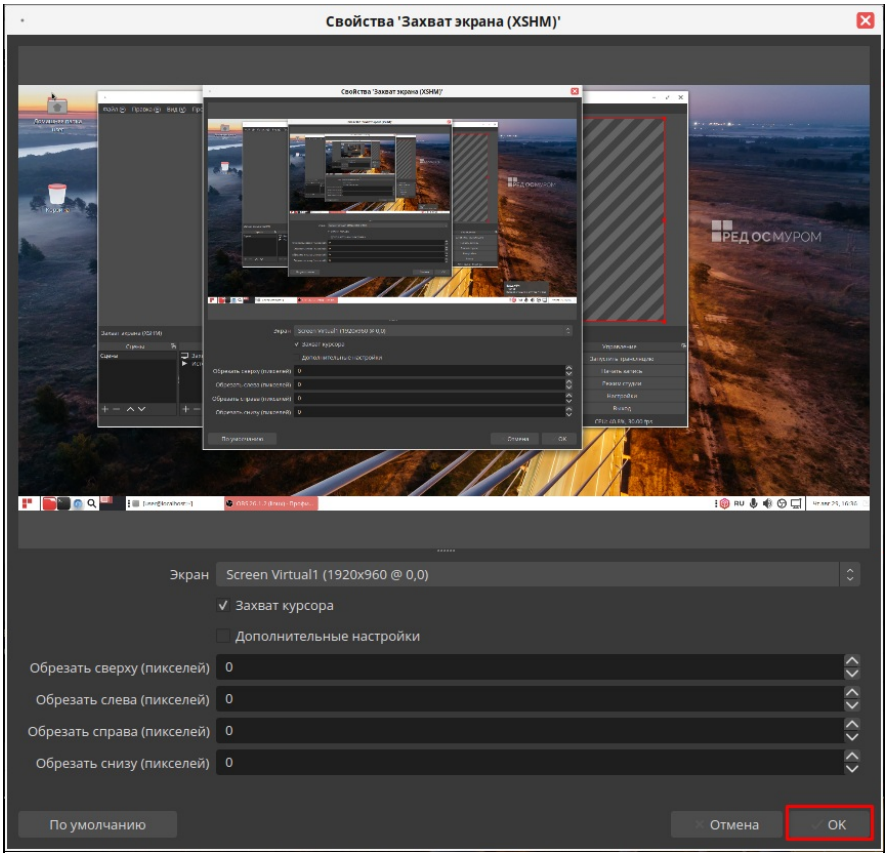
2. Введите название для источника захвата экрана и нажмите «**OK**».



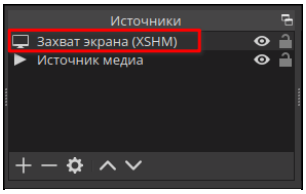
3. В открывшемся окне выберите экран, который необходимо записать. Если несколько экранов, убедитесь, что вы выбрали правильный. Запомните разрешение экрана, так как оно понадобится при редактировании видео.



4. Нажмите «**OK**» для сохранения настроек захвата экрана.

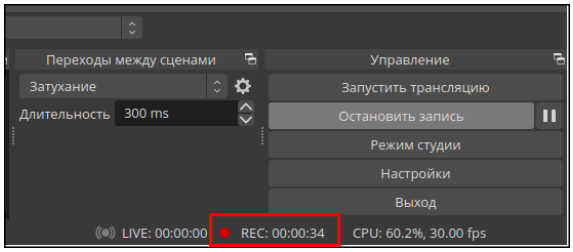


5. В списке источников будет отображен новый источник «**Захват экрана**».



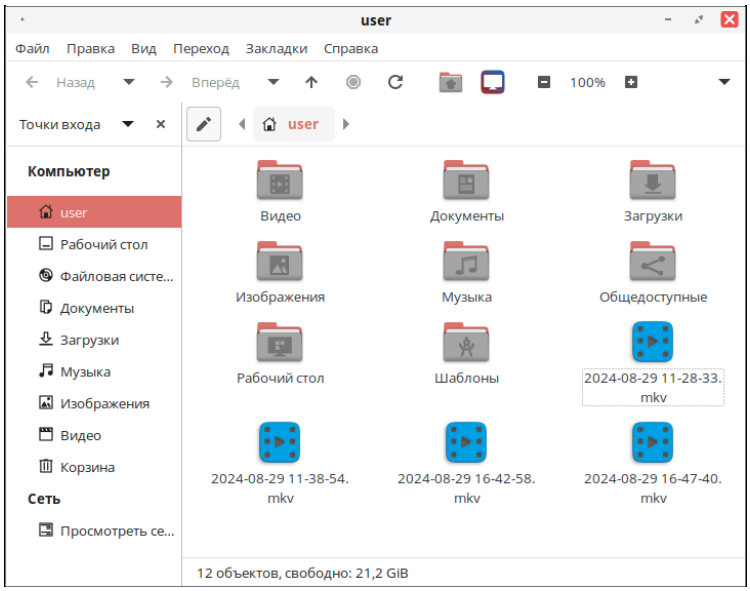
6. Нажмите «**Начать запись**» (или воспользуйтесь горячей клавишей), чтобы начать запись видео с экрана. Красная точка на значке

REC в нижней части экрана указывает на то, что запись началась.



7. Чтобы остановить запись, нажмите на кнопку «**Остановить запись**» или используйте горячую клавишу.

8. Для просмотра записей перейдите в меню «**Файл**» — «**Показать записи**». После этого можно начинать редактирование или просмотр записей.

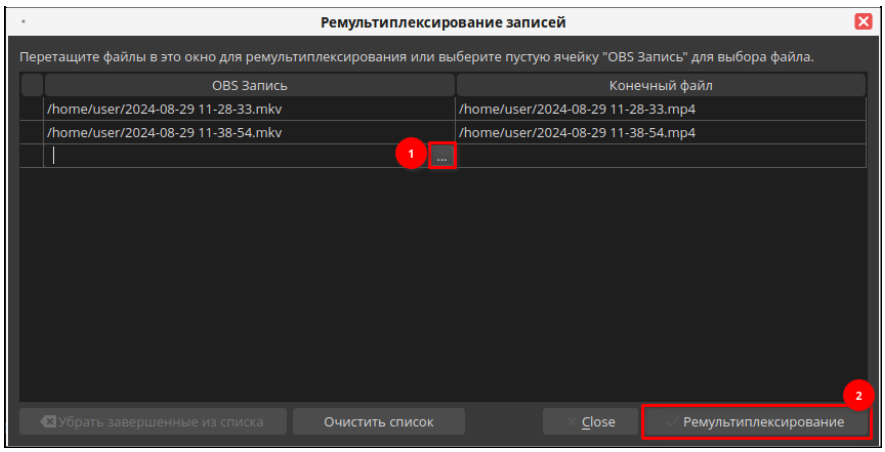


Если необходимо записывать только звук, а не показывать какие-либо изображения, можно:

- поместить источник захвата экрана позади всех других источников;
- отредактировать преобразование источника захвата экрана, чтобы установить размер с нулевой шириной на нулевую высоту.

Ремультиплексирование записей

Ремультиплексирование записей (перекомпоновка) — позволяет конвертировать любой формат видео в mp4-формат. Для конвертирования записей в другом формате перейдите в меню «**Файл**» — «**Ремультиплексирование записей**». В открывшемся окне загрузите файл, нажав на значок ... и выбрав запись (или несколько записей). Затем нажмите «Ремультиплексирование».



SimpleScreenRecorder — программа записи экрана

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: simplescreenrecorder-0.4.3

Вы можете подробнее ознакомиться с созданием скриншотов и возможностью записи видео с экрана, просмотрев наши обучающие видео:

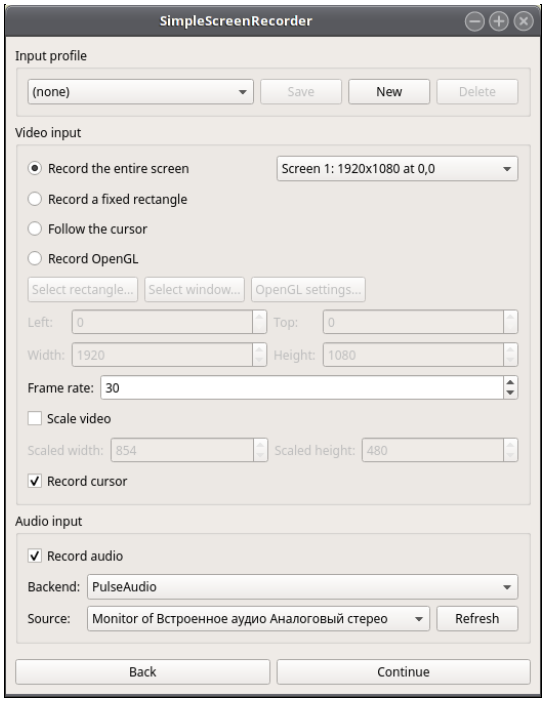
- на **RuTube** — Запись видео с экрана;
- в **Яндекс.Дзен** — Запись видео с экрана.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы выполните команду (потребуются права **администратора**):

```
sudo dnf install simplescreenrecorder
```

Запуск программы доступен из «**Главного меню**» - «**Аудио и Видео**» - «**SimpleScreenRecorder**».



Раздел Video input содержит параметры:

1) **Record the entire screen** — в случае если мониторов несколько, можно указать, какой именно записывать и захватывать с него видео.

2) **Record a fixed rectangle** — в случае, когда снимать видео необходимо с определенного участка экрана, с помощью инструмента Select rectangle можно выделить область при помощи мыши. Select window — инструмент, при помощи которого можно выбрать любое окно, с которого необходимо захватывать видео.

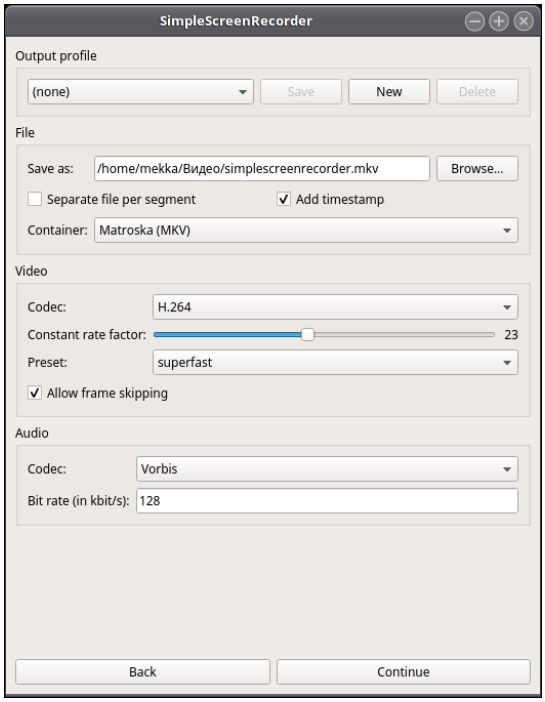
3) **Follow the cursor** — в таком режиме можно захватывать видео только в пределах движения курсора. Этот самый предел необходимо указывать в параметре Width и Height.

4) **Record OpenGL** — запись видео с программ, поддерживающих OpenGL (в основном касается игр).

Frame Rate — частота кадров записи (чем больше, тем плавнее итоговая картинка, но размер больше). Учтите, что человек воспринимает нормально 24 кадра или более, меньше кадров для человека будет казаться изображением дёрганным.

Audio Input — если видео запись звука не нужна, можно выключить, сняв галку с атрибута « **Record Audio**».

Все настройки можно сохранить в профиль для будущих записей в Разделе Input Profile.



Для создаваемого профиля можно задать различные настройки, в том числе, путь для сохранения файла.



Начать запись можно с помощью кнопки «**Start Recording**». Закончить с помощью той же кнопки (на кнопке будет надпись «**Pause Recording**»).

Start Preview — необходима для проверки записи без фактической записи в файл в реальном времени. Для создаваемого профиля можно задать различные настройки, в том числе, путь для сохранения файла.

Видеоредактор VLC

Установка
Описание программы
Запись видео с экрана
Запись аудио- и видеофайла
Настройки
Сброс настроек
Просмотр списка воспроизведения
Преобразование и сохранение медиафайла
Настройка потокового вещания VLC

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: vlc-3.0.21

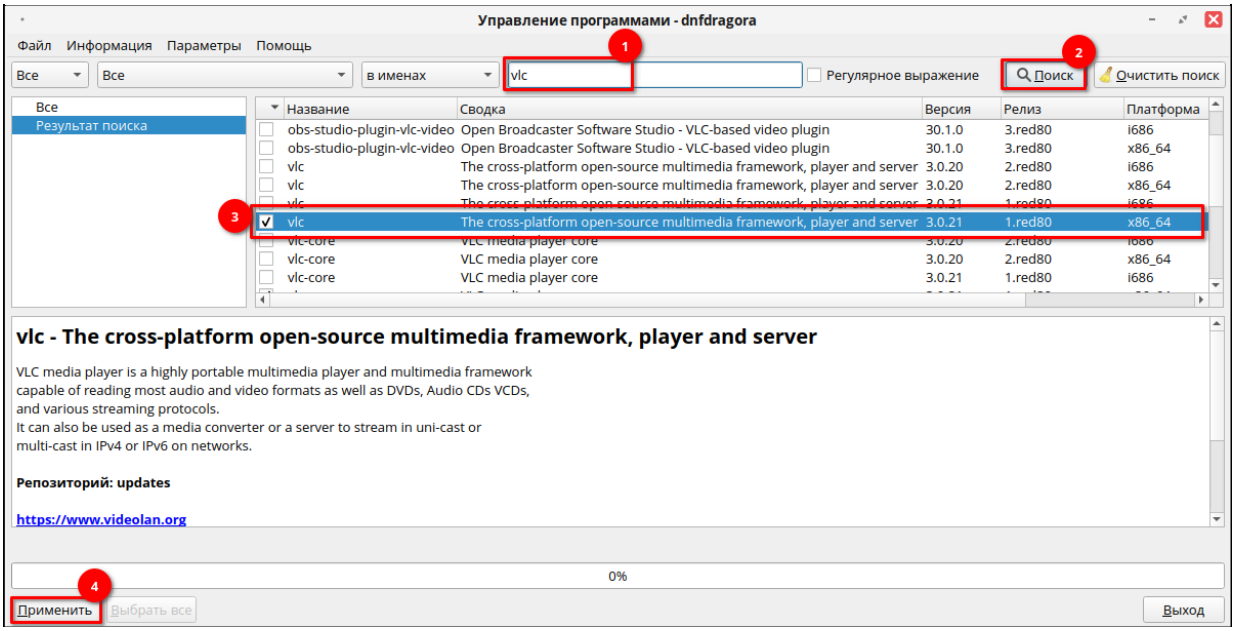
VLC Media Player — кроссплатформенный медиапроигрыватель, разрабатываемый проектом VideoLAN. Плеер **VLC** можно использовать в качестве сервера для трансляции потока аудио/видео по сети. Для воспроизведения файлов мультимедиа не требуется установка дополнительных кодеков.

VLC может воспроизводить DVD и потоковое незашифрованное видео (IPTV) и интернет-радио. Также программа может записывать потоковое аудио/видео на компьютер. **VLC Media Player** поддерживает следующие форматы: **MKV**, **MP4**, **AVI**, **MOV**, **OGG**, **FLAC**, **CD**, **ASF**, **TS**, **M2TS**, **Webm** и **AAC**.

Установка

По умолчанию программа уже предустановлена в РЕД ОС. Если программа у вас не установлена, установить её можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**vlc**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install vlc
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

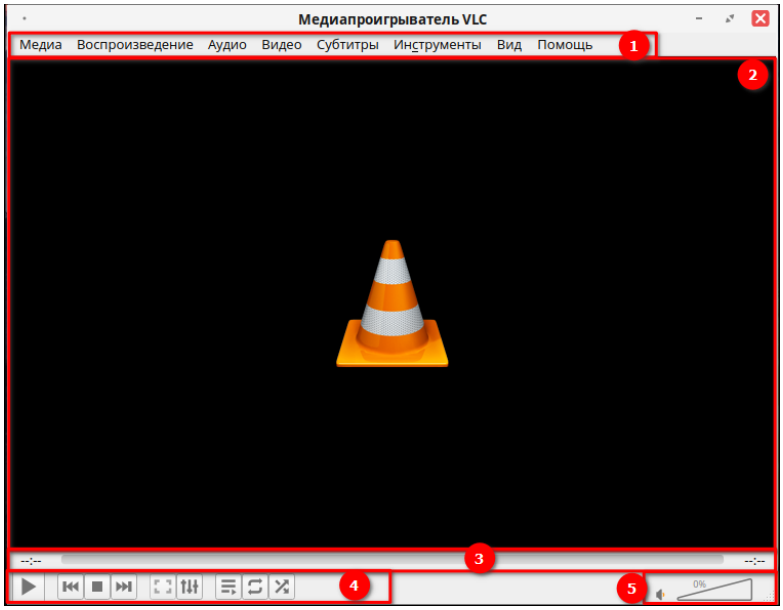
Для запуска программы через терминал введите команду:

```
vlc
```

Для запуска программы через графический интерфейс перейдите в «**Главное меню**» — «**Аудио и Видео**» («**Мультимедиа**») — «**Медиаплеер VLC**».

Описание программы

Главное окно программы выглядит следующим образом:



1. **Основное меню** позволяет выполнять различные действия с создаваемым видео, а также настраивать программу и плейлист.

2. **Рабочая область** предназначена для размещения элементов.

3. **Слайдер дорожки** находится поверх кнопок управления. Он показывает ход воспроизведения медиафайла. Вы можете перетащить ползунок дорожки влево для перемотки назад или вправо для перемотки вперёд воспроизводимой дорожки.

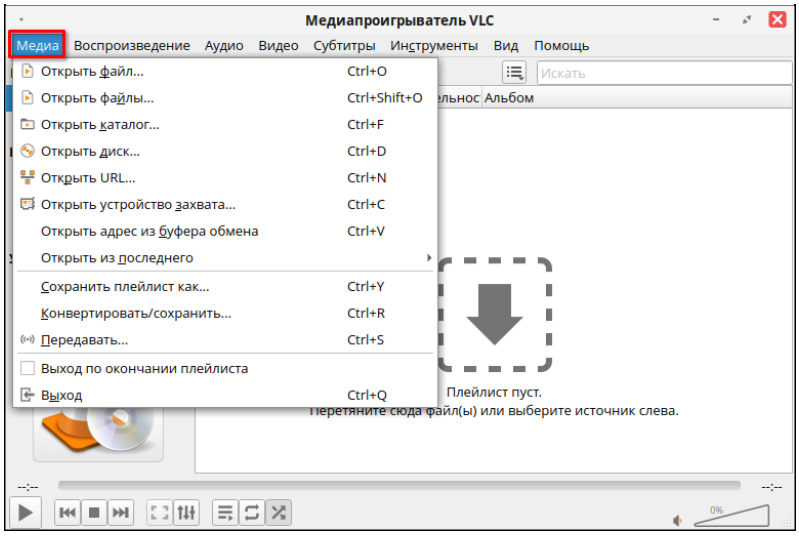


4. **Панель инструментов** — основные действия для работы с плейлистом, такие как воспроизведение, открытие файла, предыдущая или следующая позиция плейлиста, режим повтора, случайный порядок.

5. **Регулятор громкости** расположен в правом нижнем углу окна. Значок динамика увеличивает, уменьшает громкость или отключает звук. Ползунок показывает текущую громкость воспроизведения. Нажатие на него изменяет громкость. Громкость воспроизведения также отображается в процентах поверх ползунка.

Меню «Медиа»

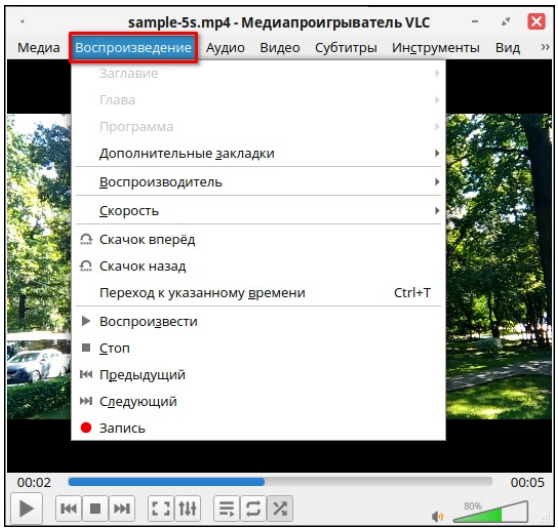
Из пункта меню «**Медиа**» доступны базовые функции для добавления и сохранения видео- и аудиозаписей.



Для воспроизведения медиафайла перейдите в меню «**Медиа**» — «**Открыть файл**». Выберите файл.

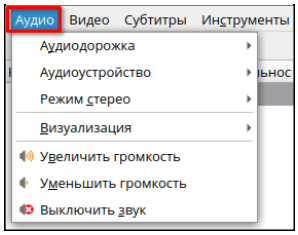
Меню «Воспроизведение»

В пункте меню «**Воспроизведение**» размещены основные действия для работы с плейлистом.



Меню «Аудио»

Для настройки параметров звука перейдите в меню «**Аудио**» и выберите все необходимые настройки.



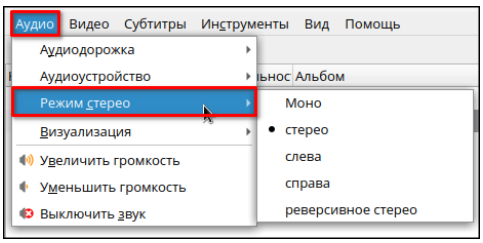
Раздел «**Аудиодорожка**» позволяет включать и отключать аудиодорожки.

Для включения аудиодорожки выберите в меню «**Аудио**» — «**Аудиодорожка**» — «**Дорожка 1**».

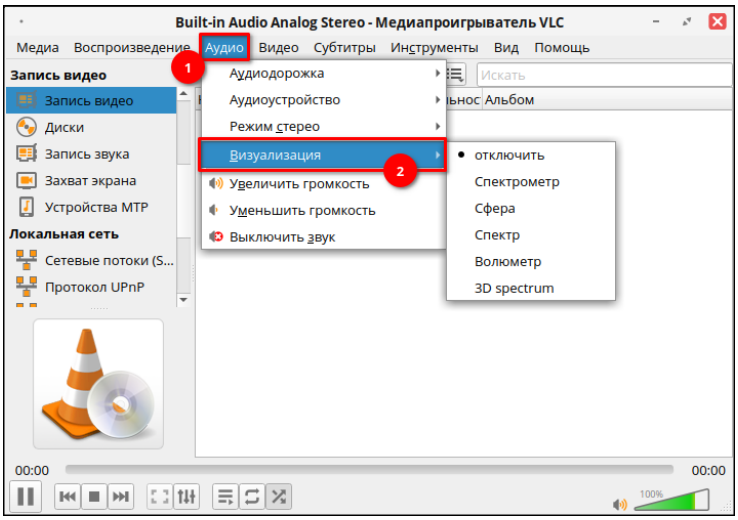
Для отключения аудиодорожки перейдите в «**Аудио**» — «**Аудиодорожка**» — «**Отключить**».

Опция «**Режим стерео**» позволяет прослушивать аудиофайлы в различных режимах:

- ***моно*** (монофонический звук) использует один канал для воспроизведения звука;
- ***стерео*** относится к звуку, который использует два канала для воспроизведения звука или стереофонического звучания;
- при выборе опции ***слева*** музыка будет воспроизводиться только в левом динамике;
- при выборе опции ***справа*** музыка будет воспроизводиться только из динамика справа;
- ***реверсивное стерео*** предназначено для воспроизведения звука одновременно с видео.

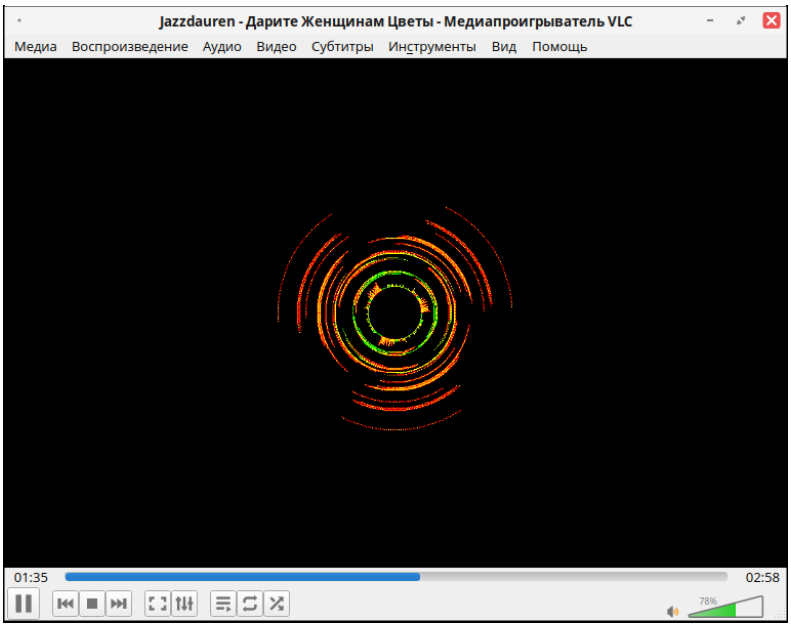


Для просмотра доступных визуальных эффектов перейдите в меню «**Аудио**» — «**Визуализация**».



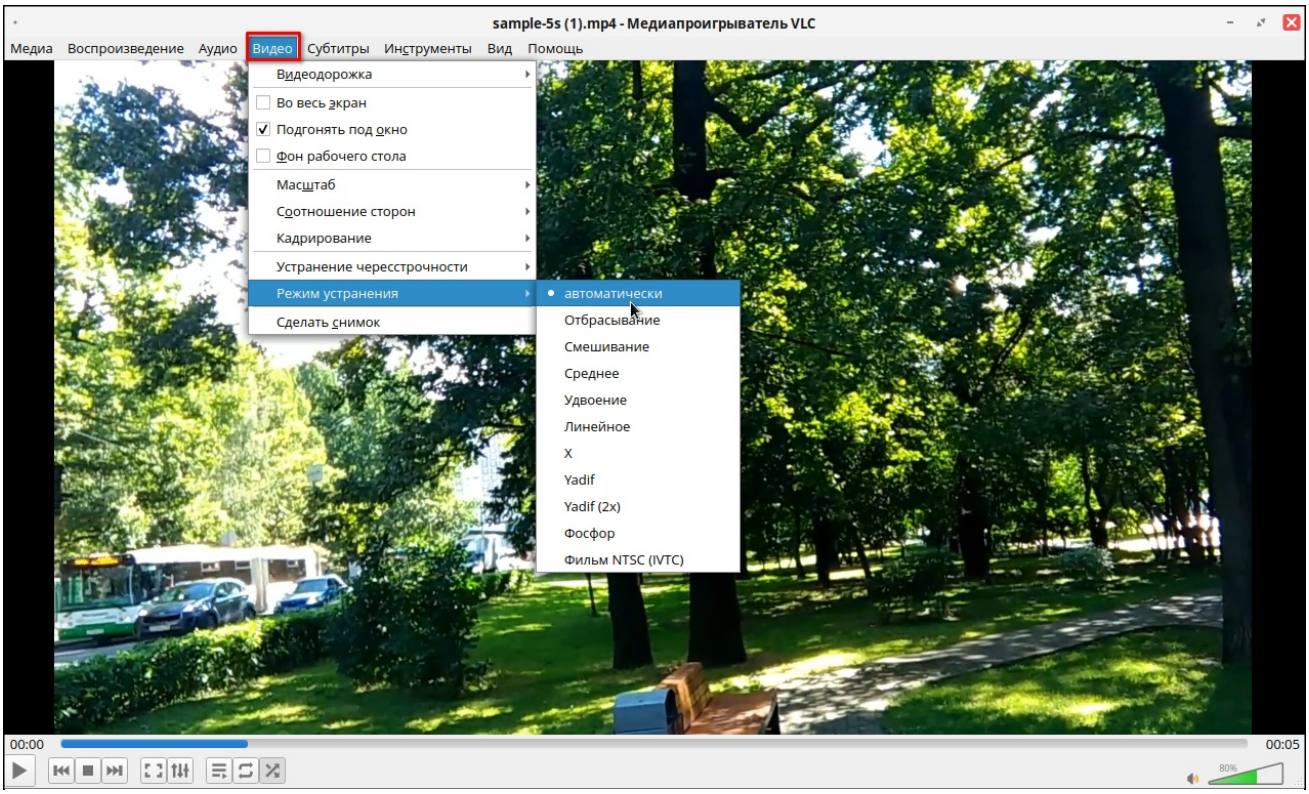
С помощью визуализации можно добавить спектрометр, сферу, волюметр, геометрические формы, которые будут генерировать изображения на основе музыкального произведения.

Спектрометр отображает звуковые частоты аудио в виде графического спектра:



Меню «Видео»

В меню «**Видео**» содержатся настройки, которые позволяют пользователю управлять отображением и воспроизведением видео.



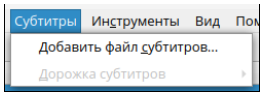
Меню «Субтитры»

Старые форматы файлов (например, ***.avi**) не могут обрабатывать субтитры напрямую. Файл субтитров содержит текст субтитров и временные метки.

Для добавления файла субтитров перейдите в меню «**Субтитры**» — «**Добавить файл субтитров...**».

Субтитры можно скачать с официального сайта.

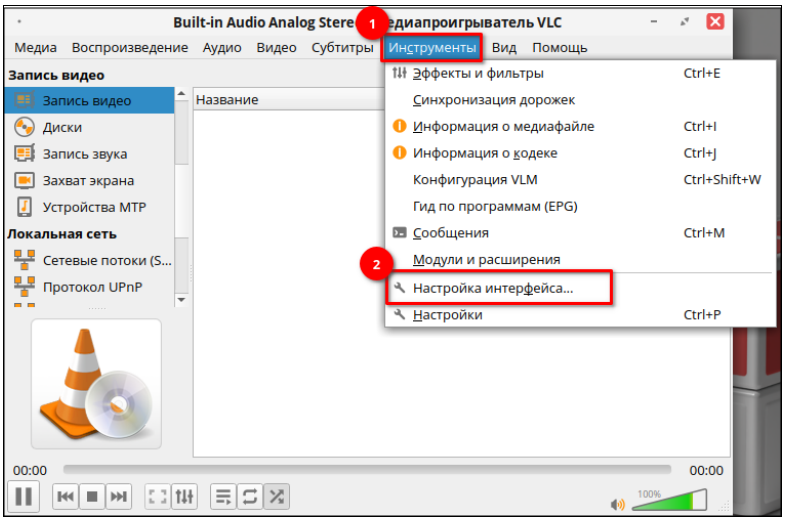
Примечание. Для автоматической загрузки субтитров убедитесь, что файл субтитров находится в той же папке, что и видеофайл, имеет такое же имя (за исключением расширения), как видеофайл, и использует поддерживаемый формат (например, ***.cdg**, ***.idx**, ***.srt**, ***.sub**, ***.ass**, ***.ssa** и другие). Например, если ваш видеофайл называется **film.mp4**, то файл субтитров должен называться **film.srt**.



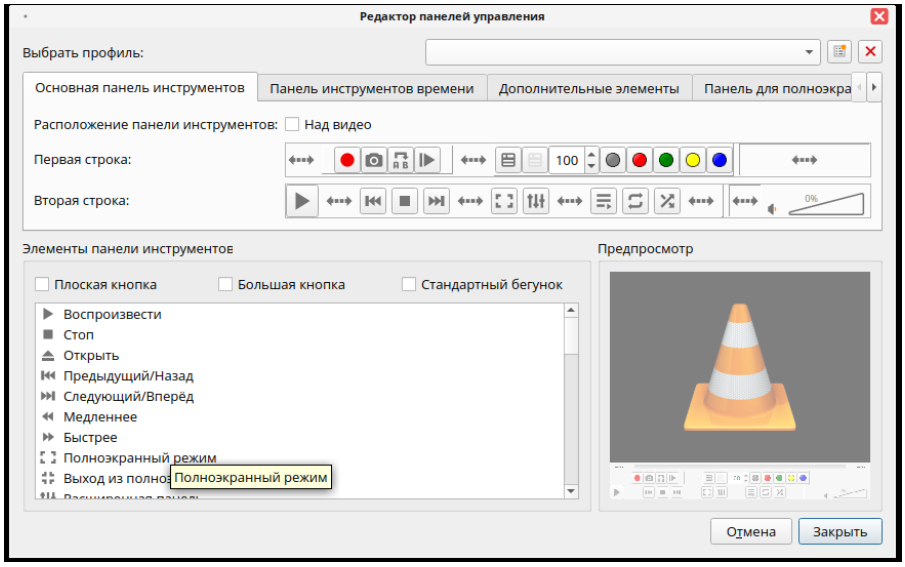
После добавления субтитров вы сможете включить их в меню: «**Субтитры**» — «**Дорожка субтитров**». Будут перечислены все треки с субтитрами. Для отключения опции выберите «**Субтитры**» — «**Дорожка субтитров**» — «**Отключить**».

Меню «Инструменты»

Изменить настройки элементов интерфейса можно в меню «**Инструменты**» (1) — «**Настройка интерфейса...**» (2).



В открывшемся окне можно производить настройку интерфейса плеера.



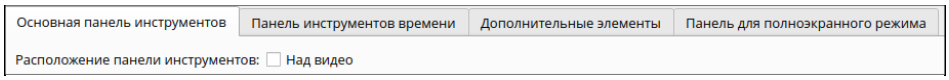
Рядом со строкой выбора профиля находятся две кнопки.



 — позволяет создать собственный профиль.

 — удаляет профиль.

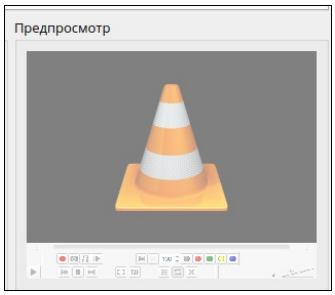
В области ниже можно выбрать тот участок интерфейса, в котором нужно изменить расположение кнопок и ползунков. Переключаться между такими участками позволяют четыре вкладки.



Кнопки и ползунки можно перемещать, зажав нужный элемент ЛКМ, после чего перенести его в нужное место или удалить. Для удаления элемента необходимо просто перетащить его за рабочую область.



Просмотреть результат изменений можно в окне предпросмотра.

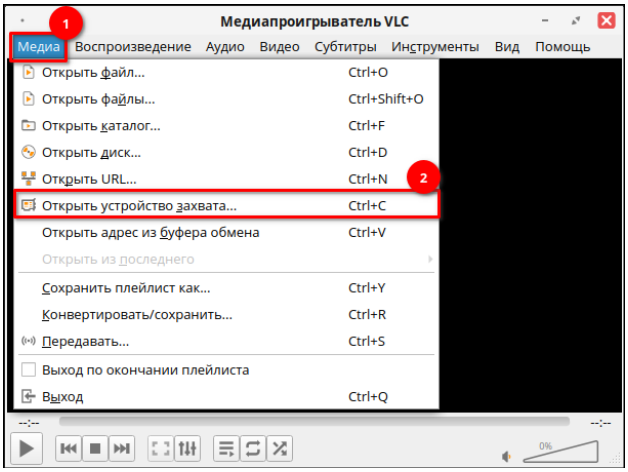


По окончании всех изменений нужно будет просто нажать кнопку «**Закрыть**». Это позволит сохранить все настройки и просмотреть результат в самом плеере. На этом процесс настройки интерфейса завершён.

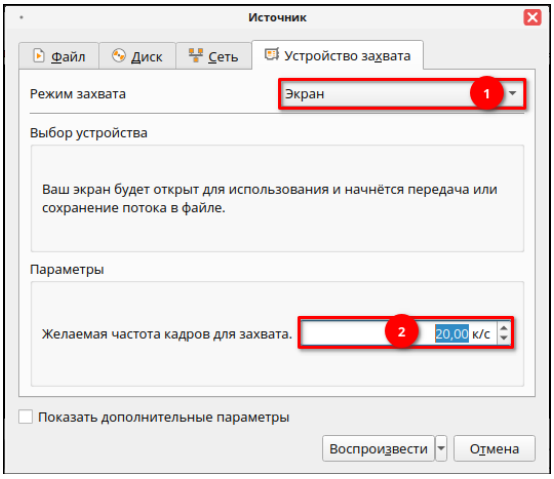
Запись видео с экрана

Для записи видео экрана вашего компьютера необходимо выполнить следующие действия:

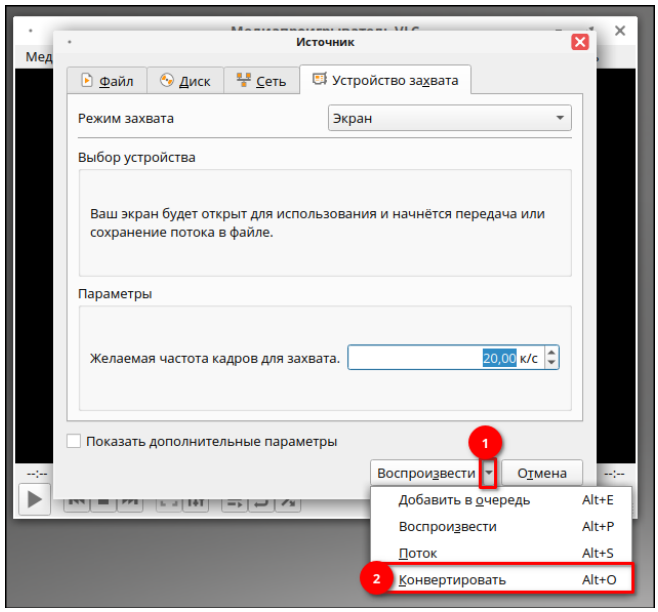
1. Открыть меню «**Медиа**» и выбрать пункт «**Открыть устройство захвата...**».



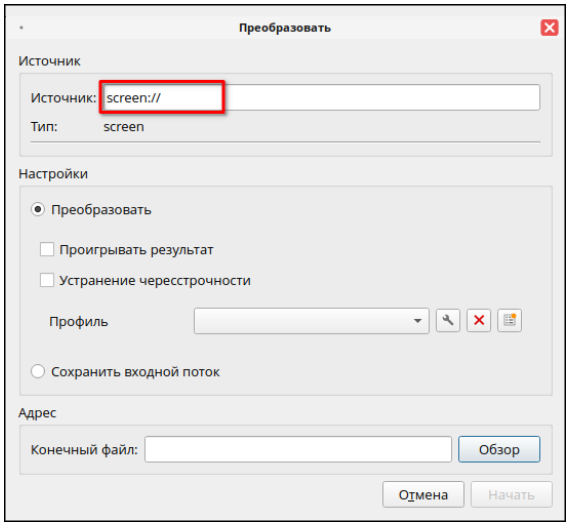
2. В режиме захвата выбрать «**Экран**», в параметрах указать желаемую частоту кадров. Рекомендуется указать значение **20 к/с**, в зависимости от желаемой плавности видео и свободной памяти (чем выше количество кадров в секунду, тем более качественное видео и больший размер выходного файла).



3. Раскрыть выпадающий список, нажав на стрелку рядом с кнопкой «**Воспроизвести**» и выбрать «**Конвертировать**» для продолжения процесса.

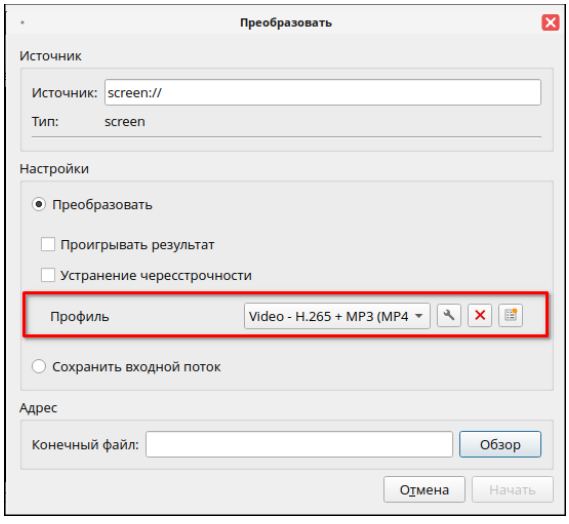


4. После нажатия кнопки «**Конвертировать**» должно появится окно «**Преобразовать**». Необходимо убедиться, что источником видео является экран компьютера (в строке «**Источник**» должно отображаться **screen://)**.

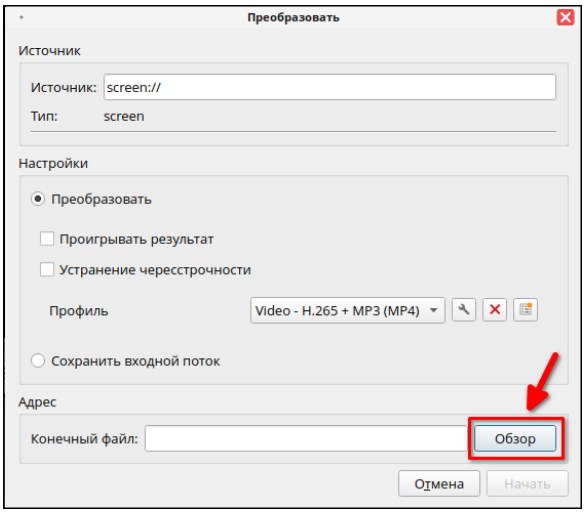


5. В Профиле настроить параметры видео, выбрать подходящий кодек. Например, **Video - H.264 + MP3 (MP4)**.

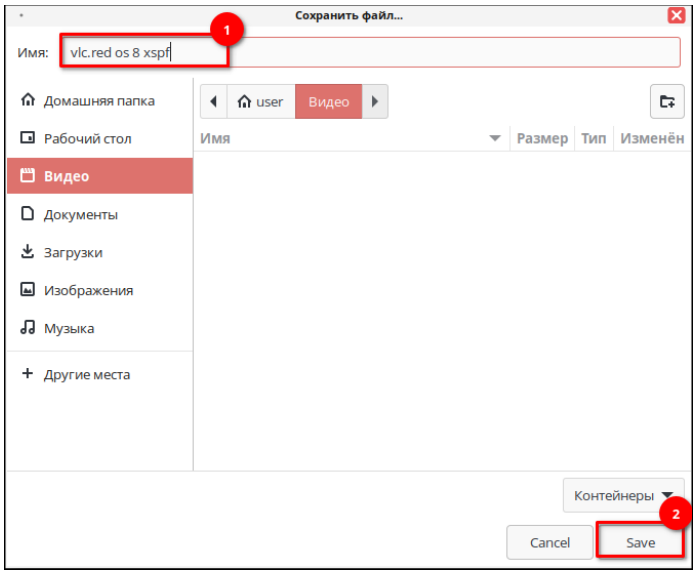
Кодеки – это специальные программы для кодирования и сжатия видео- и аудиодорожки.



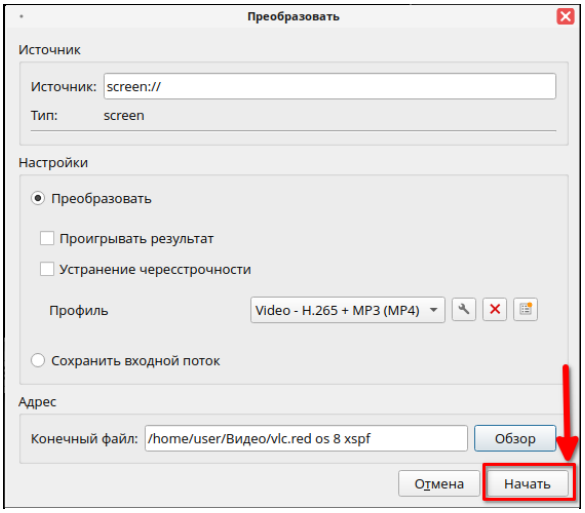
6. Для сохранения видеофайла нажать кнопку «**Обзор**».



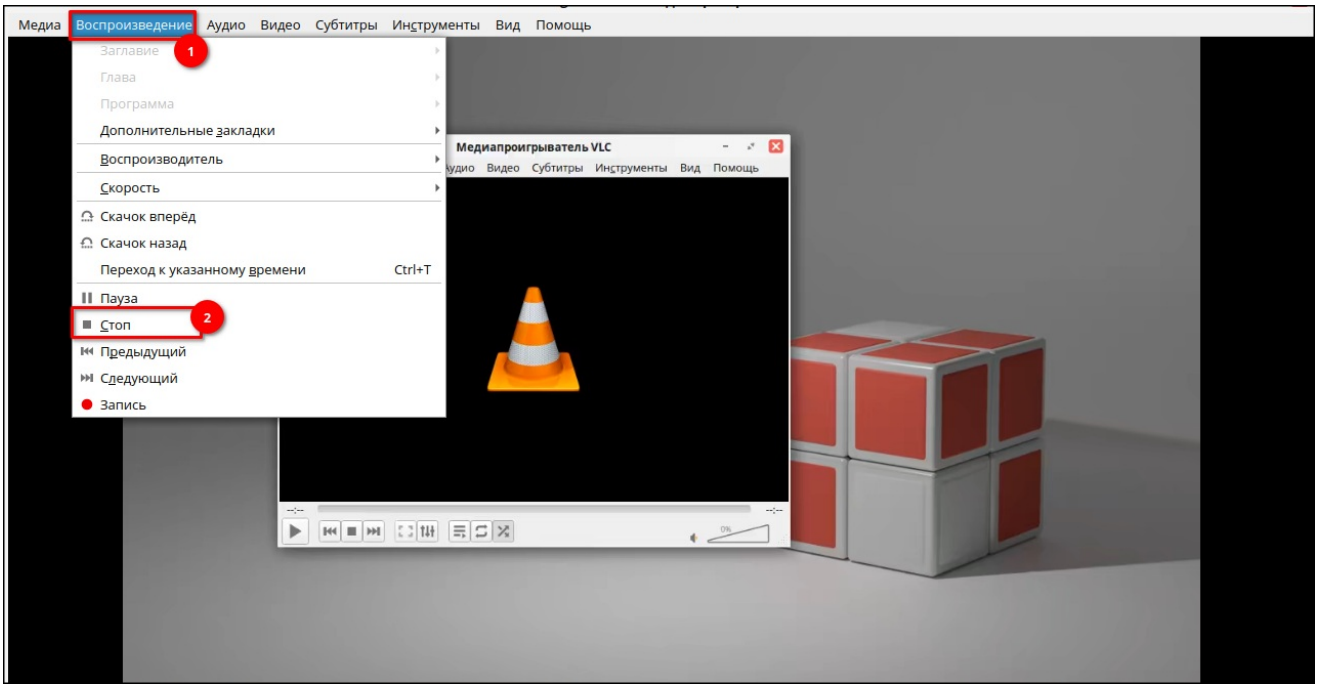
В открывшемся окне выбрать путь, ввести имя для сохранения файла и нажать «**Save**».



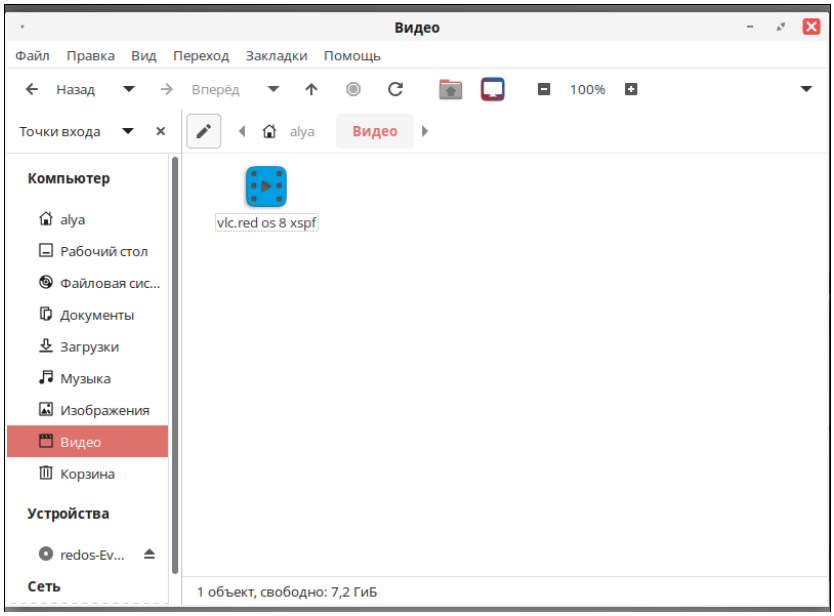
7. Для начала записи нажать кнопку «**Начать**». Начнётся запись видео всего рабочего стола. Запись можно поставить на паузу, а затем восстановить.



8. Для остановки записи перейти в меню «**Воспроизведение**» (1) — «**Стоп**» (2).

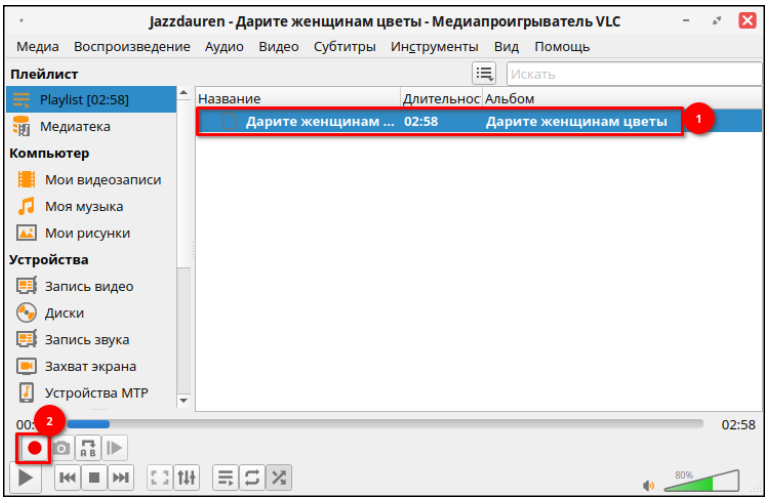


9. После окончания записи видео необходимо проверить его сохранение в диспетчере файлов, щёлкнуть по нему для просмотра результата записи.



Запись аудио- и видеофайла

Для записи аудио- и видеофайла на панели инструментов отобразите кнопку  . Для этого выберите в меню «**Вид**» — «**Доп. элементы управления**». Откройте аудио- или видеофайл (1) и нажмите на кнопку записи (2).



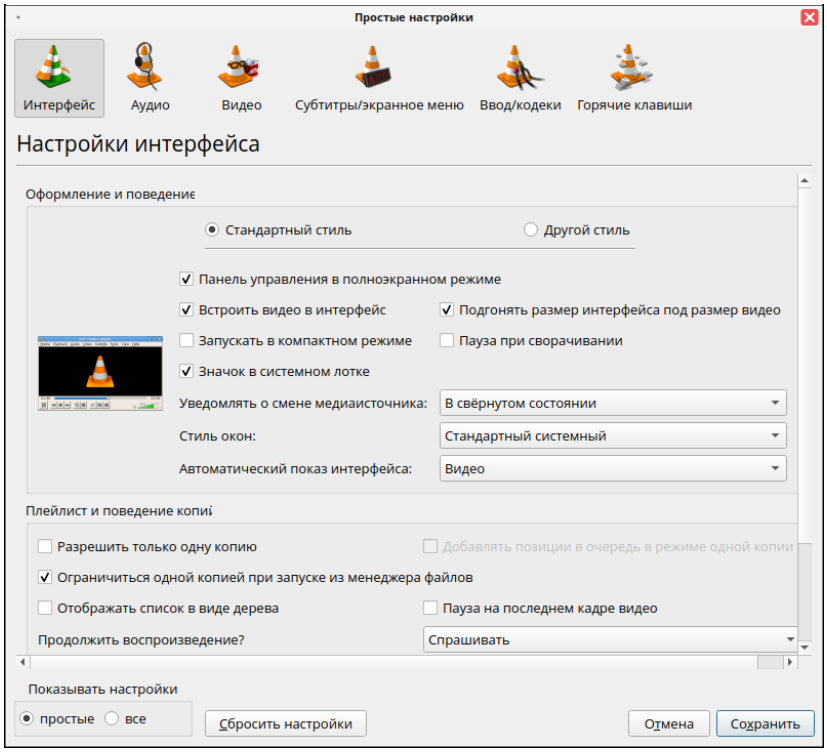
После записи медиафайла снова нажмите на красную кнопку.

Запись будет сохранена в отдельном файле в разделе «**Компьютер**» — «**Моя музыка**» или «**Мои видеозаписи**».

Для обрезки видео используйте кнопку  .

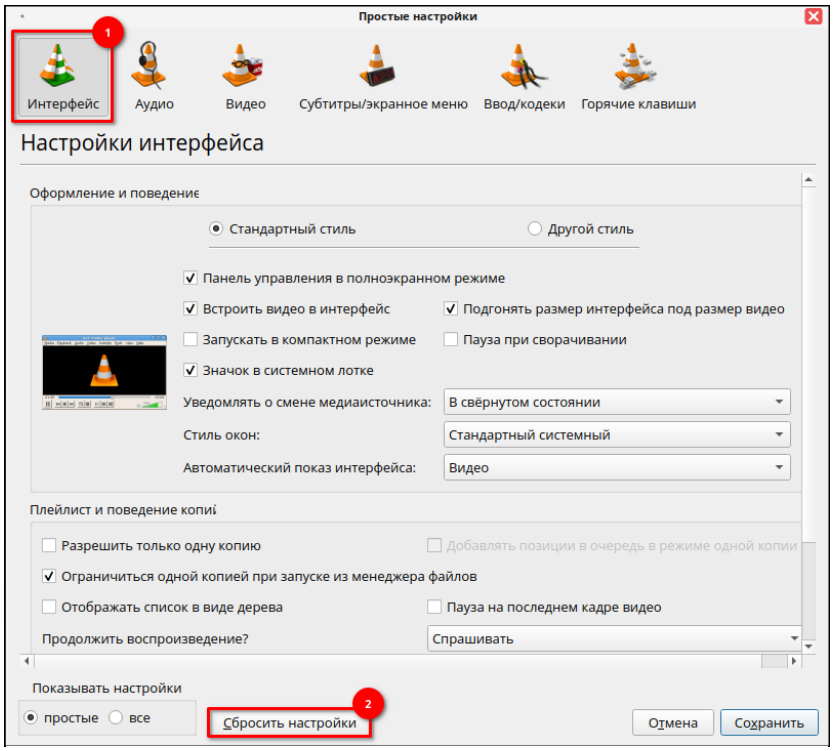
Настройки

Для доступа к панели настроек перейдите в меню «**Инструменты**» — «**Настройки**». Панель настроек позволяет изменять основные параметры VLC.



Сброс настроек

Для сброса настроек перейдите в меню «**Инструменты**» — «**Настройки**». Выберите вкладку с необходимыми настройками (1) и нажмите кнопку «**Сбросить настройки**» (2).



Просмотр списка воспроизведения

Для просмотра списка воспроизведения перейдите в меню «**Вид**» — «**Плейлист**».

1. **Плейлист** — текущий плейлист позволяет просматривать и управлять текущим списком воспроизведения мультимедийных файлов. Медиатека содержит все доступные аудио- и видеофайлы.

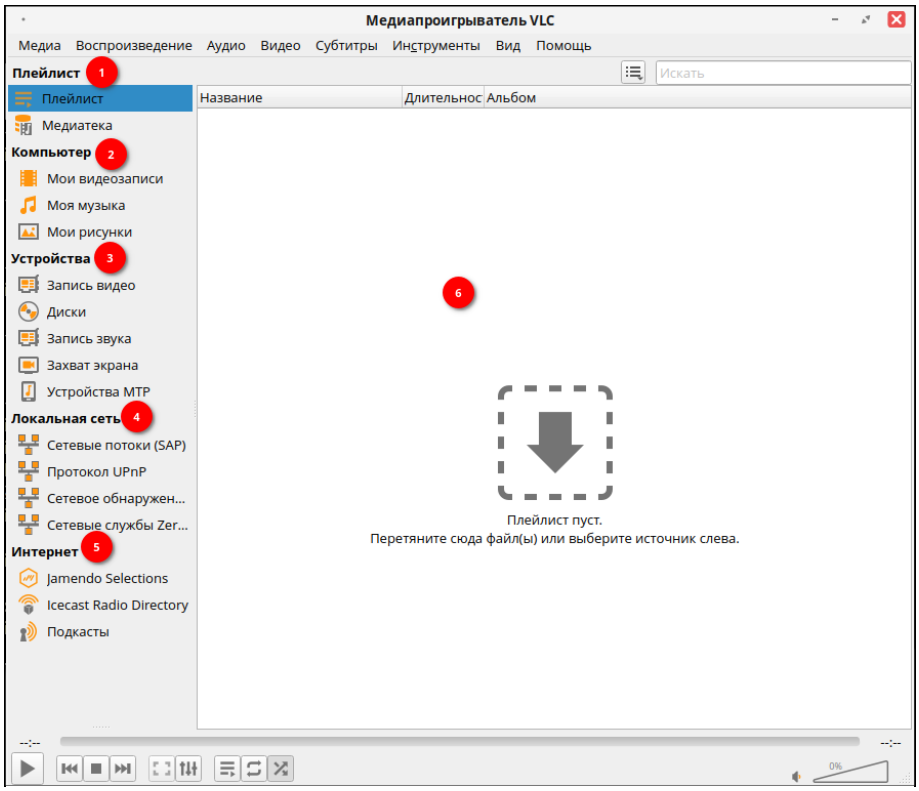
2. В разделе **Компьютер** отображаются стандартные каталоги и папки на компьютере, где обычно хранятся видео-, аудио- и снимки экрана.

3. **Устройства** — доступ к оптическим устройствам.

4. **Локальная сеть** — источники локальной сети, где можно обращаться к медийным файлам, которые доступны в локальной сети, используя различные сетевые протоколы, такие как SAP (Session Announcement Protocol), UPnP (Universal Plug and Play).

5. **Интернет** — раздел предлагает доступ к различным интернет-источникам, таким как подкасты, онлайн радиостанции и другие потоковые сервисы для онлайн прослушивания или просмотра.

6. **Список медиафайлов** — отображаются все доступные на устройстве медиафайлы.



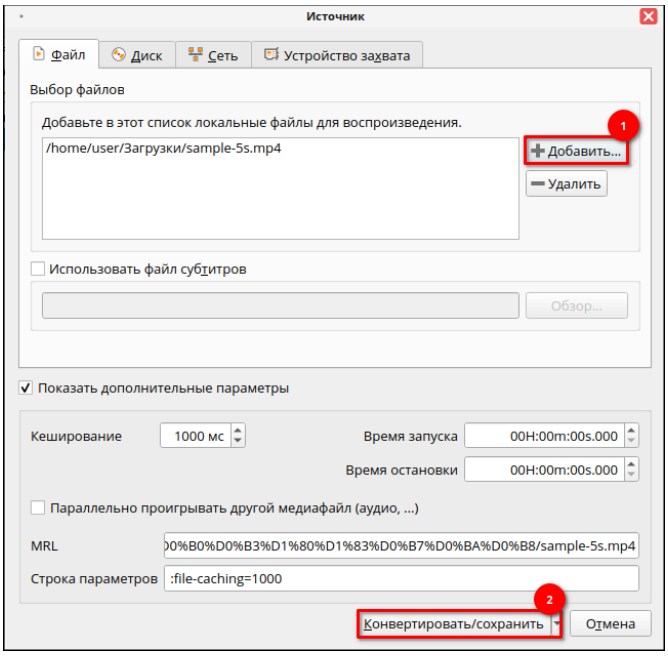
Преобразование и сохранение медиафайла

Для преобразования медиафайла из одного формата в другой выполните следующие шаги:

1. Перед конвертацией убедитесь, что выбранный формат поддерживается VLC. Перейдите в меню «**Медиа**» и выберите пункт «**Конвертировать/сохранить**». Появится диалоговое окно «**Источник**».

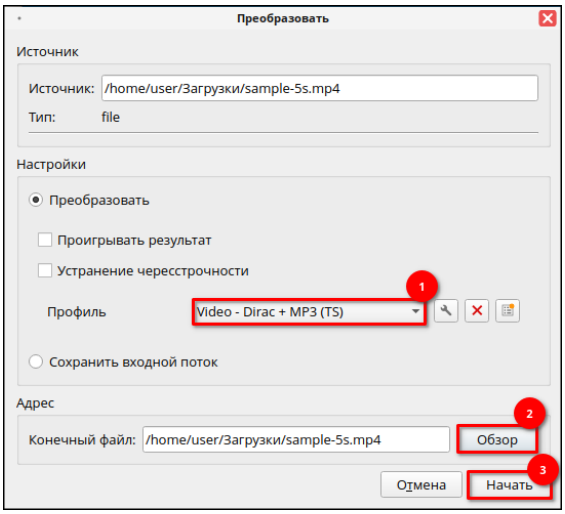
2. Для добавления файла нажмите «**Добавить...**» (1) и выберите файлы для конвертирования.

3. После добавления файла в список, нажмите на кнопку «**Конвертировать/сохранить**» (2). Перед началом конвертации вы можете настроить параметры выходного файла, такие как формат, качество и расположение сохранения.



4. Для конвертации медиафайла в появившемся диалоговом окне «**Преобразовать**» выберите **Профиль** для преобразования медиафайла (1).

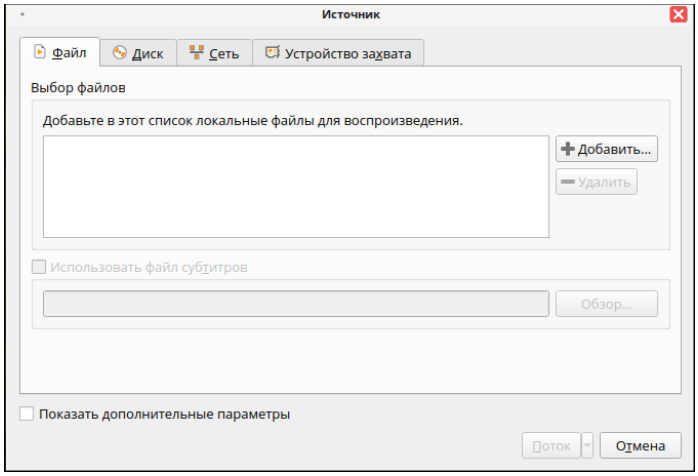
Для сохранения медиафайла нажмите «**Обзор**» (2), выберите имя и адрес конечного файла. Для запуска процесса конвертации и сохранения видео нажмите «**Начать**» (3). Дождитесь окончания конвертации и сохранения медиафайла.



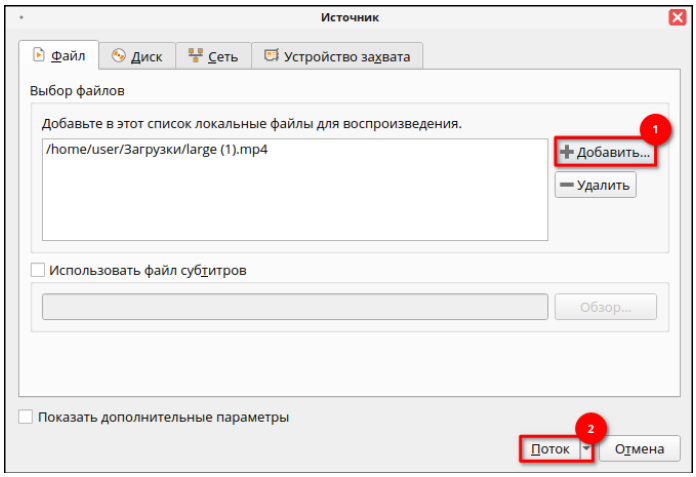
Настройка потокового вещания VLC

Для настройки видеовещания в рамках локальной сети выполните следующий алгоритм действий:

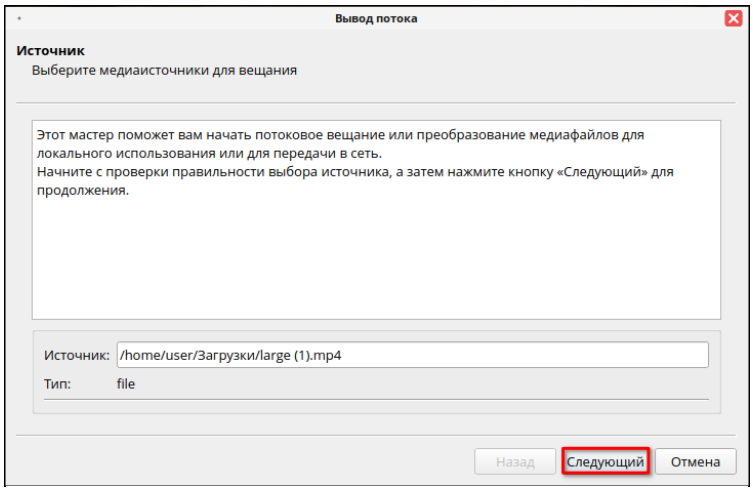
1. Перейдите в меню «**Медиа**» — «**Передавать...**». Откроется диалоговое окно «**Источник**».



2. Нажмите кнопку «**Добавить**» (1), выберите файл для воспроизведения и нажмите « **Поток**» (2).

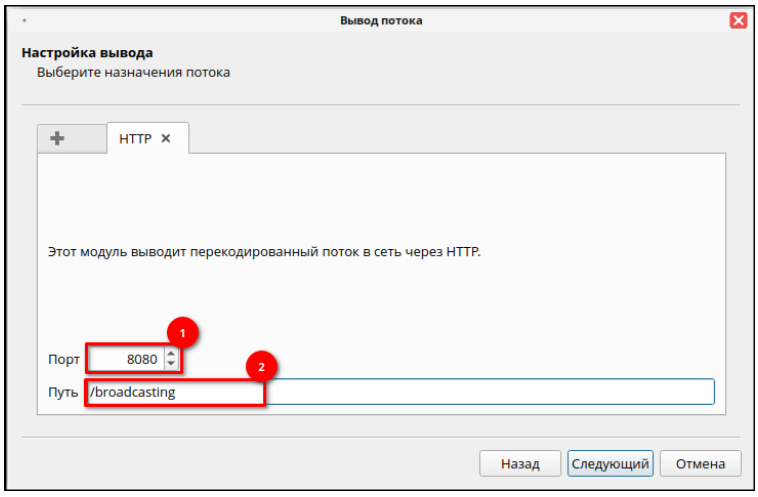


3. В окне «**Вывод потока**» проверьте выбор медиаисточника и нажмите кнопку «**Следующий**» для продолжения.

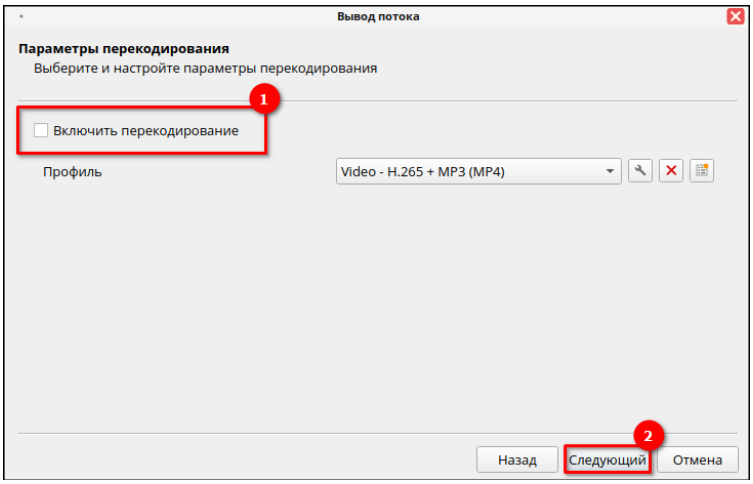


4. Выберите протокол для вещания из выпадающего списка. Отметьте HTTP и нажмите «**Добавить**».

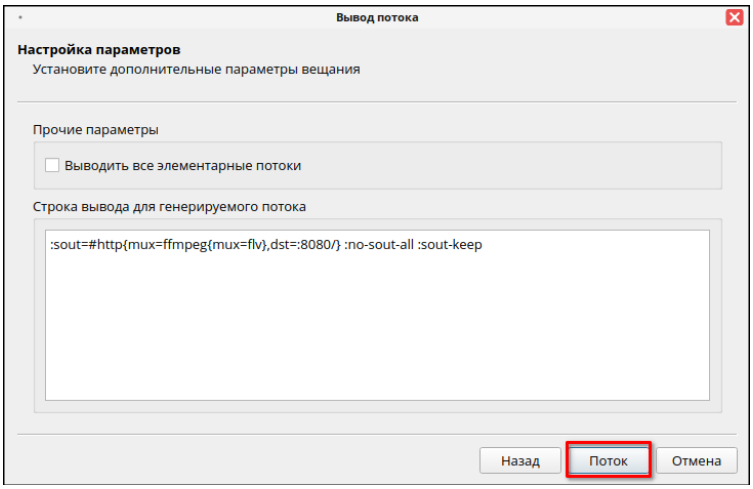
5. Укажите порт (например, **8080**) и произвольное слово в поле «**Путь**» (например, "**/broadcasting**").



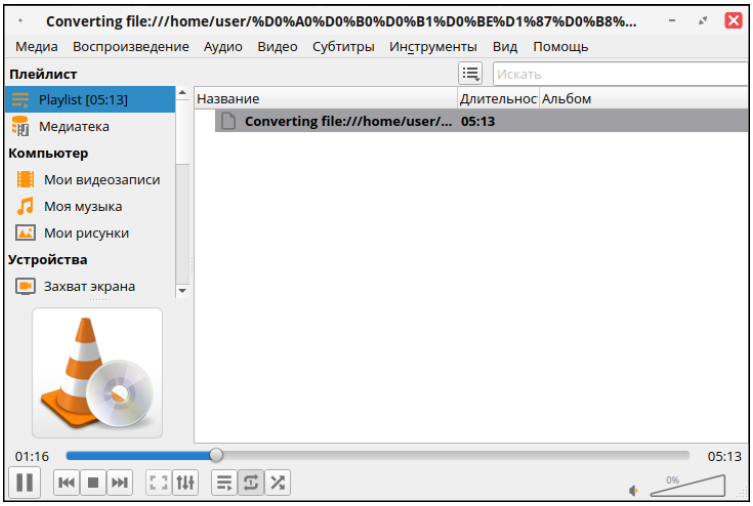
6. Выберите и настройте параметры перекодирования (1) и нажмите «**Следующий**» (2).



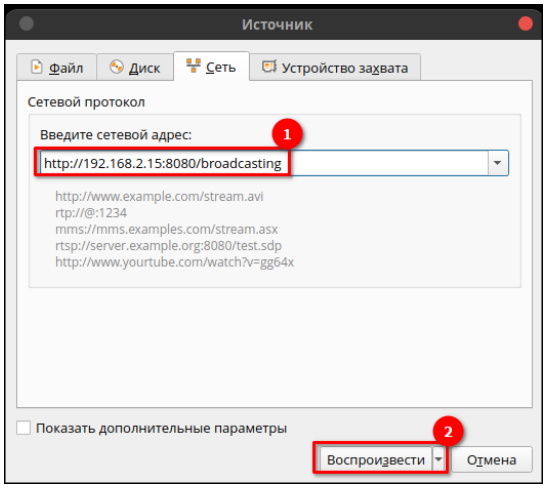
7. Подтвердите настройки, нажав «**Поток**».



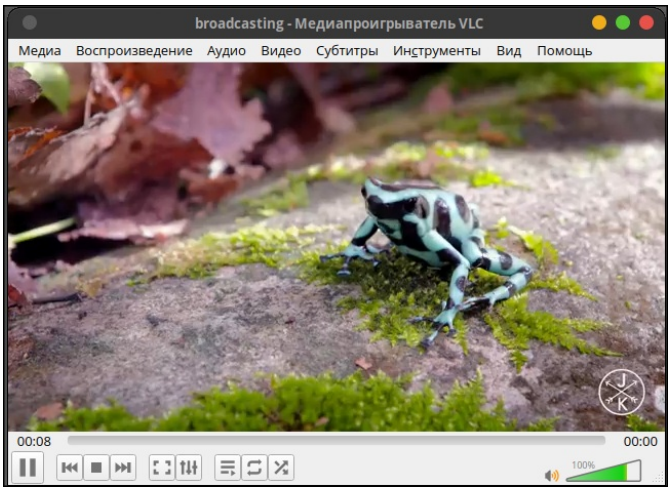
Трансляция отобразится в плеере.



8. Проверьте правильность настройки трансляции. Откройте другой плеер VLC. Перейдите в меню «**Медиа**» — «**Открыть URL**». В появившемся окне введите локальный IP-адрес. Добавьте порт и путь, указанные при потоковой настройке. Например, «**http://192.168.2.15:8080/broadcasting**». Замените адрес 192.168.2.15 на свой локальный (сетевой) IP-адрес. Нажмите кнопку «**Воспроизвести**».



В другом плеере отобразится видеовещание **broadcasting**.


broadcasting - Медиапроигрыватель VLC
Медиа Воспроизведение Аудио Видео Субтитры Инструменты Вид Помощь
00:08
00:00
100%

DaVinci Resolve - редактирование видео

Установка
Первоначальная настройка

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** DaVinci_Resolve_18.0.4

DaVinci Resolve — приложение для цветокоррекции и нелинейного редактирования видео, также является единственным в мире решением для монтажа и цветокоррекции, наложения визуальных эффектов, создания графики и постобработки звука в единой программной среде.

DaVinci Resolve используется для монтажа фильмов, сериалов, рекламных роликов, телепрограмм и видеоклипов.

Примечание.

Программа работает только с проприетарными видеодрайверами **Nvidia** и **AMD**. По большей части *DaVinci Resolve* оптимизирована под *Nvidia*, поэтому убедитесь что у вас установлена последняя версия видеодрайвера.

Подробную информацию об установке видеодрайвера см. в нашей статье «Установка драйвера Nvidia в РЕД ОС 7.3 ».

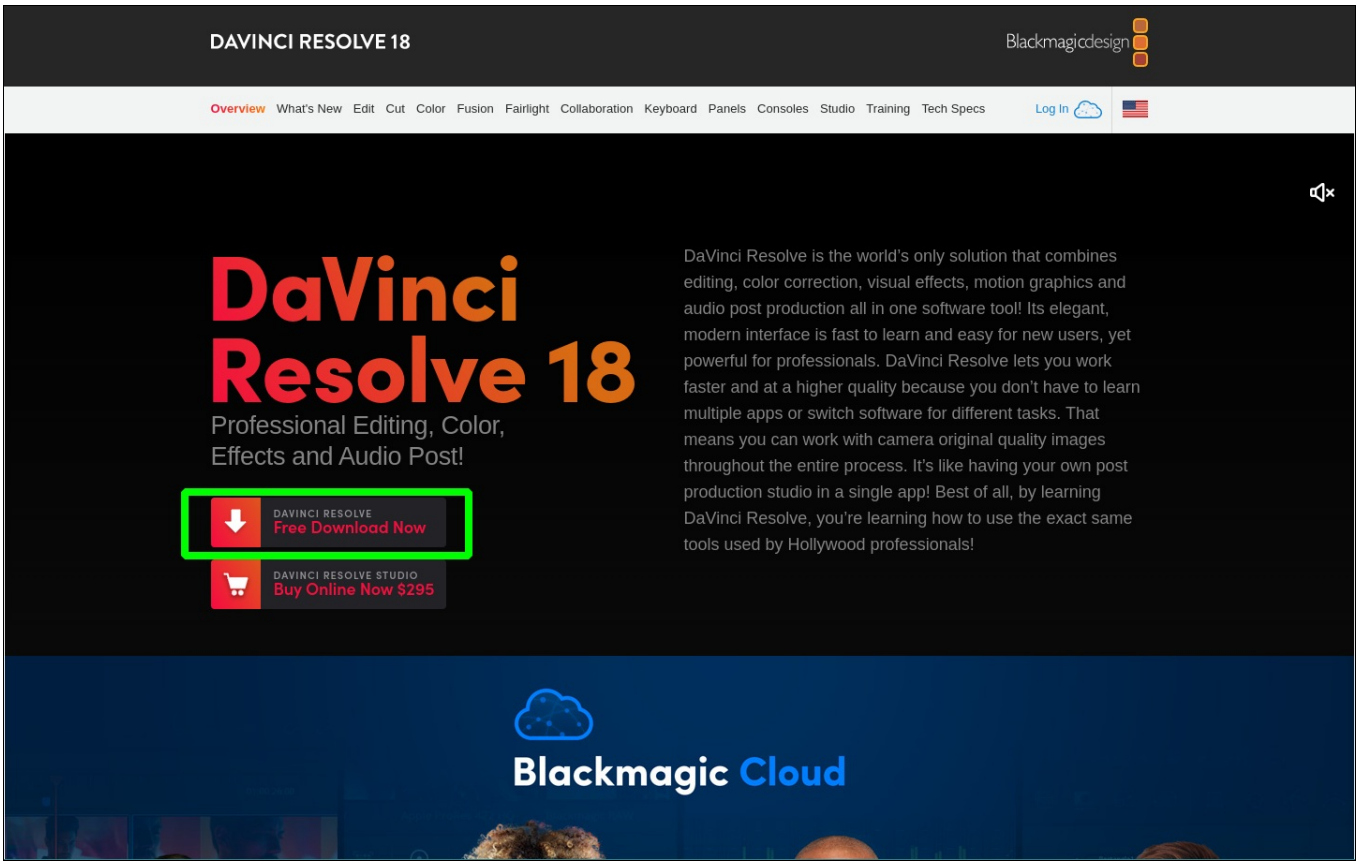
Вы можете подробнее ознакомиться с установкой и работой программы **DaVinci Resolve**, просмотрев наши обучающие видео:

- на **RuTube** — Установка DaVinci Resolve в РЕД ОС;
- в **Яндекс.Дзен** — Установка DaVinci Resolve в РЕД ОС;
- в **VK Видео** — Установка DaVinci Resolve в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Перейдите на официальный сайт DaVinci Resolve и нажмите **Загрузить сейчас**.



Потребуется ввести контактные данные, а затем можно будет загрузить дистрибутив. В данном случае будет загружена бесплатная редакция.

После загрузки нужно распаковать скачанный архив. Для этого перейдите в папку с архивом (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
```

И выполните команду распаковки:

```
unzip ./DaVinci_Resolve_18.0.4_Linux.zip
```

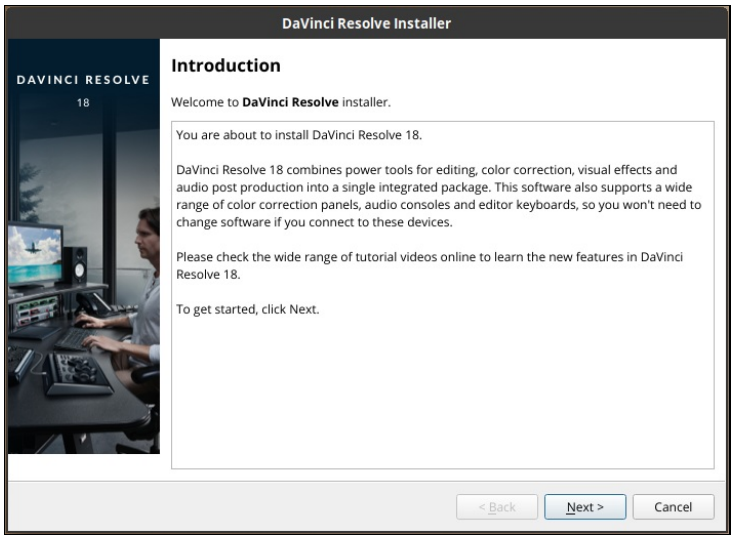
Назначьте файлу установки права на исполнение:

```
chmod +x ./DaVinci_Resolve_18.0.4_Linux.run
```

Для установки программы выполните:

```
./DaVinci_Resolve_18.0.4_Linux.run -i
```

Запуск установки также можно осуществить графически, дважды кликнув по файлу **DaVinci_Resolve_18.0.4_Linux.run**. Появится окно установщика.



Нажмите **Next**, ознакомьтесь с описанием программы, примите лицензионное соглашение и начните установку. Потребуется ввести пароль администратора или суперпользователя (**root**) системы.

Первоначальная настройка

После завершения процедуры установки перед непосредственным запуском программы потребуется произвести первоначальную настройку.

Программа устанавливается в каталог **/opt/resolve/bin/**. Перейдите в данный каталог и попробуйте запустить программу через терминал, чтобы убедиться в отсутствии каких-либо ошибок.

```
cd /opt/resolve/bin/
./resolve
```

Возможно появление сообщения вида:

```
./resolve: error while loading shared libraries: libgpudetect.so: cannot open shared object file: No such file or directory
```

Для решения данной проблемы необходимо создать символьную ссылку:

```
ln -s /lib64/libcrypt.so.2.0.0 libgpudetect.so
```

А также потребуется установить дополнительный пакет, выполнив команду:

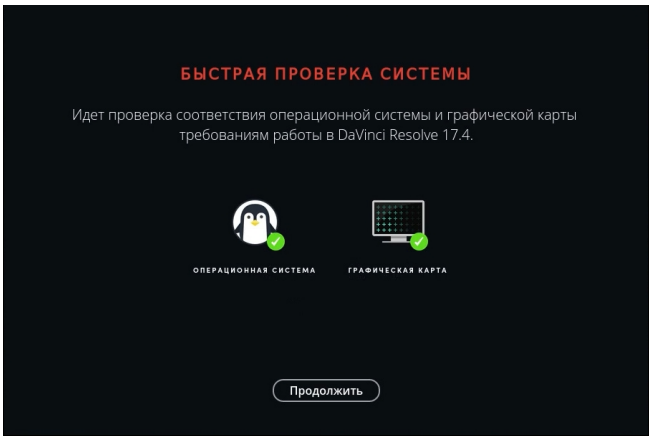
```
dnf install libxcrypt-compat
```

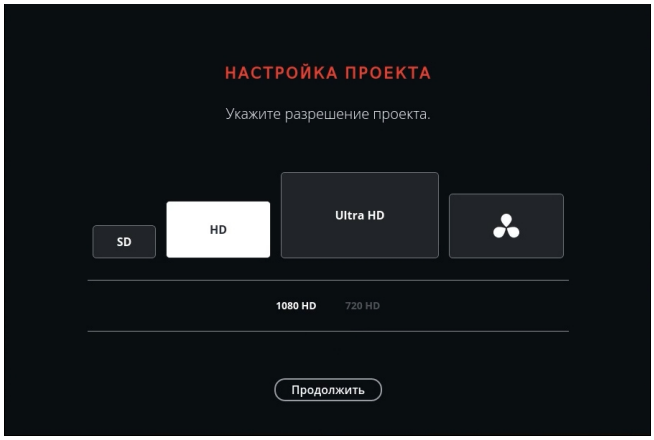
На этом подготовка системы окончена, и теперь можно запускать программу из «**Главного меню**» — «**DaVinci Resolve**» — «**DaVinci Resolve**».

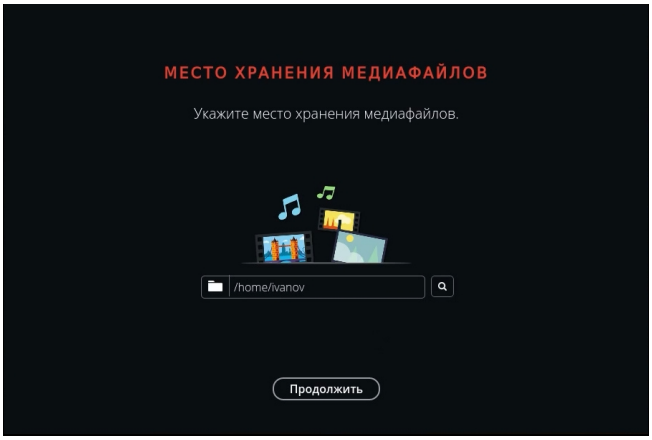
Приветственное окно программы выглядит следующим образом:

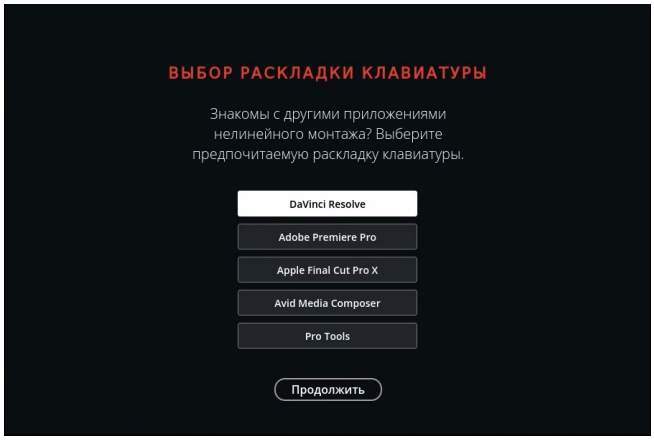


На начальном этапе можно установить русский язык и кратко ознакомиться с нововведениями. При нажатии на кнопку «**Продолжить**» можно пройти процедуру проверки и настройки, в том числе изменить место сохранения медиафайлов и настроить раскладку клавиатуры.

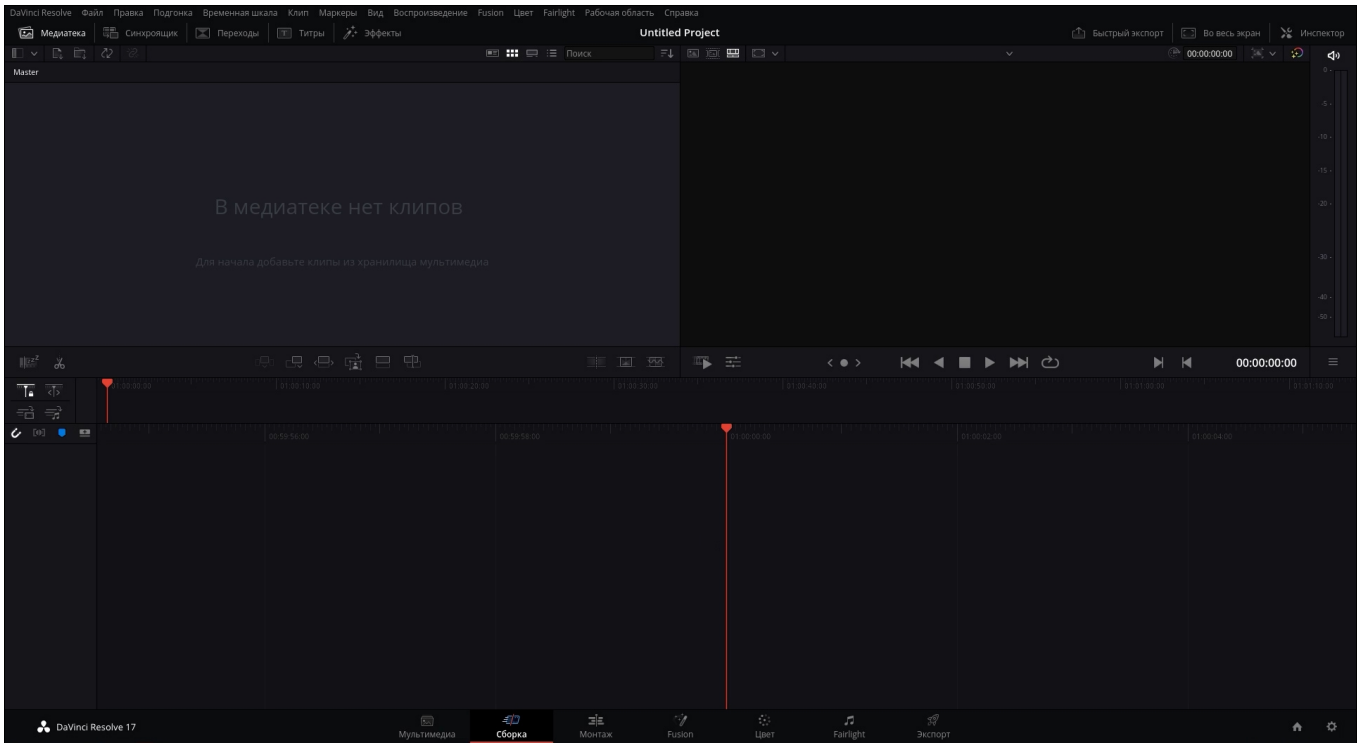








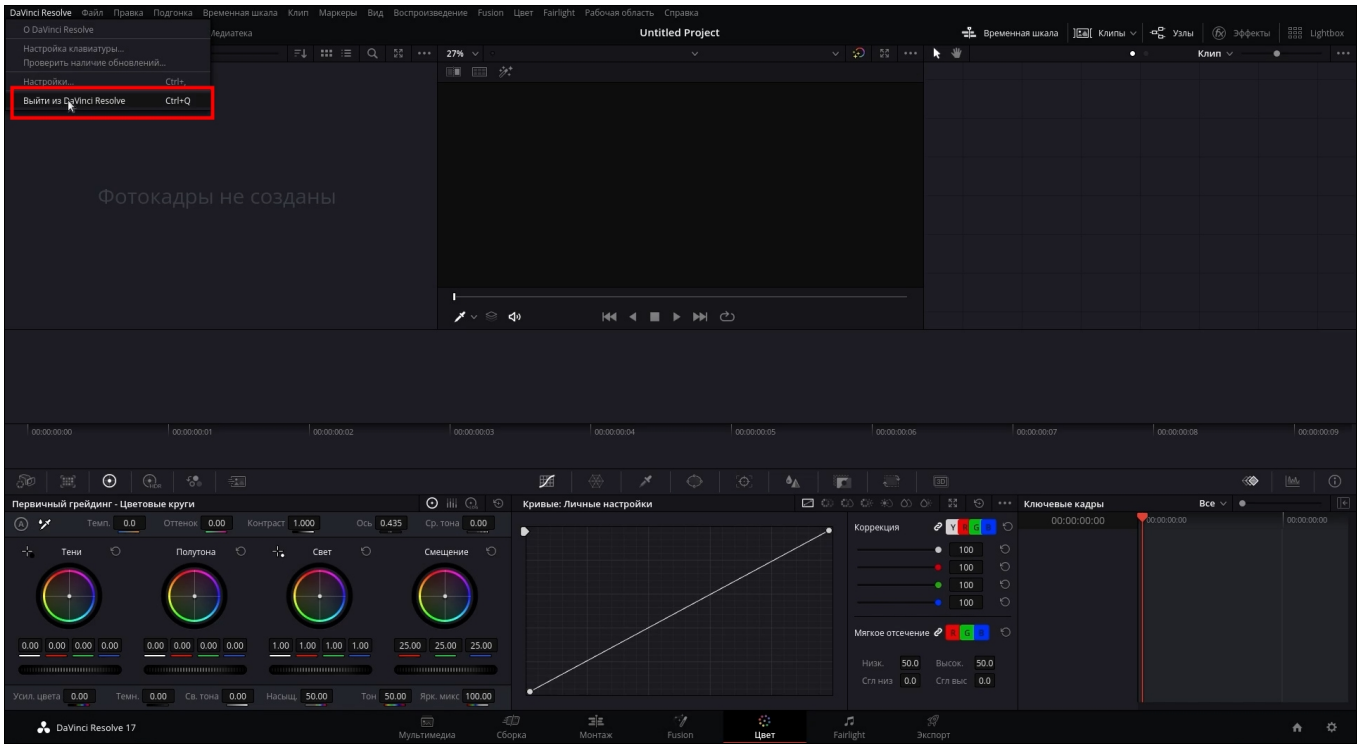
По завершении откроется главное окно видеоредактора **DaVinci Resolve**.



Интерфейс программы состоит из нескольких частей, переход между которыми можно осуществлять кнопками в нижней части экрана.



У приложения отсутствует рамка окна, поэтому для выхода необходимо выбрать пункт меню «**DaVinci Resolve**» - «**Выход из приложения**».



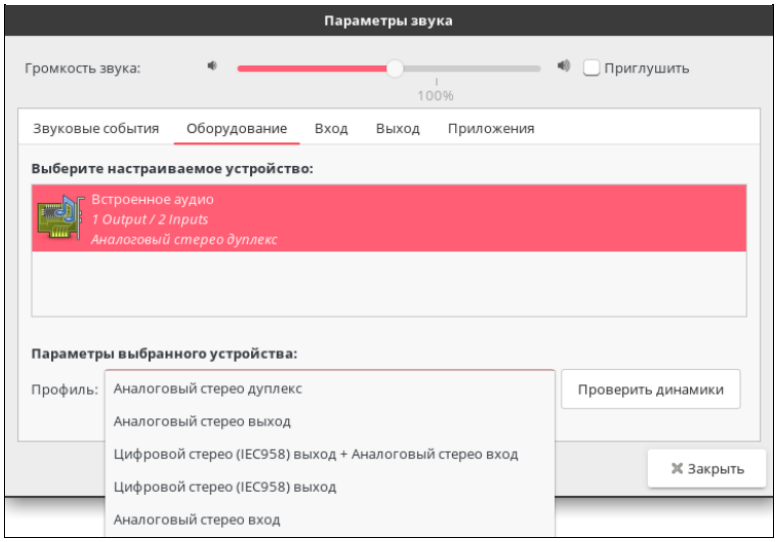
Решение проблем со звуком

Выбор оборудования
Отсутствует оборудование в списке доступных
Выбор оборудования через alsamixer
Проверка поддержки устройства ядром
Отсутствует звук у доменного пользователя

При возникновении проблем, связанных со звуком, существует несколько вариантов их решения.

Выбор оборудования

Бывают ситуации, когда необходимо вручную выбрать, какое именно устройство должно использоваться в ОС для ввода и вывода аудио-информации. Для этого выберите устройство в списке оборудования и установите для него необходимые параметры.

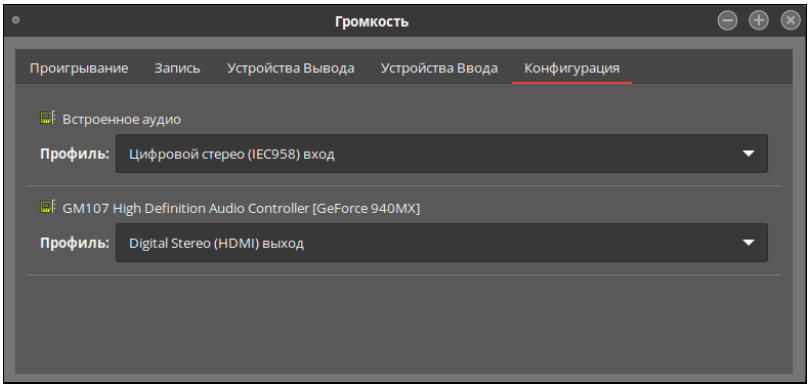


Отсутствует оборудование в списке доступных

Для решения данной проблемы на некоторых моделях ПК может подойти установка дополнительного пакета (потребуются права администратора):

```
dnf install alsa-sof-force
```

После установки необходимо перезагрузить ПК и проверить наличие аудиовыходов в параметрах звука.



Также не стоит забывать о системных обновлениях, соответственно, необходимо проверить работу оборудования на актуальных пакетах ОС. Для этого выполните следующие команды (потребуются права администратора):

```
dnf makecache
dnf update
dracut -f -v --regenerate-all
```

Затем для корректной загрузки необходимо обновить конфигурацию **GRUB**:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

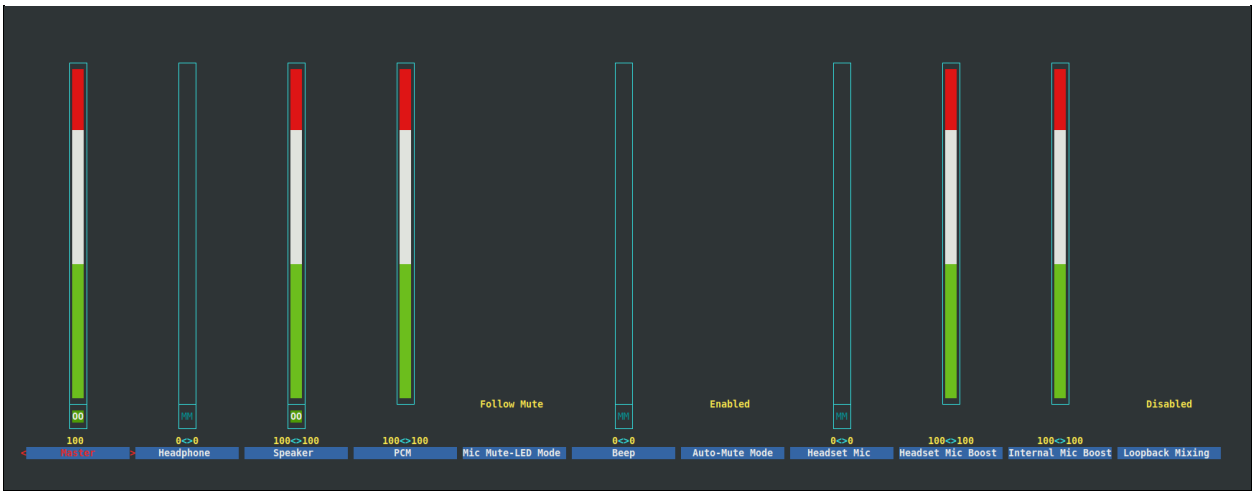
```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Для применения настроек потребуется перезагрузить ПК:

```
reboot
```

Выбор оборудования через alsamixer

В решении проблем со звуком также может помочь вариант с выбором звуковой карты из консоли через утилиту **alsamixer**.



С помощью клавиши **F6** можно выбрать необходимую звуковую карту.

Проверка поддержки устройства ядром

С выходом нового оборудования при возникновении проблем стоит обратить внимание на поддержку такого оборудования ядром. Проверить поддержку можно по нашей инструкции «Поддержка звука».

Отсутствует звук у доменного пользователя

Если звук отсутствует у доменного пользователя, в первую очередь необходимо проверить наличие файла **/var/lib/AccountsService/users/<доменный_пользователь>**. Если файл отсутствует, его необходимо создать по примеру файла локального пользователя.

Также попробуйте добавить пользователя в группу *audio*:

```
usermod -aG audio <доменный_пользователь>@<домен>
```

Если предложенные рекомендации не помогли с решением проблемы, необходимо собрать диагностическую информацию с помощью утилиты loginfo для дальнейшего ее изучения.

Почтовый клиент Evolution

Установка Evolution
Основные функции

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: evolution-3.44.4-5

Evolution – свободно распространяемая программа для работы с электронной почтой, управления адресной книгой и функцией планировщика задач. Входит в состав среды рабочего стола **GNOME** в качестве поставляемой по умолчанию почтовой программы.

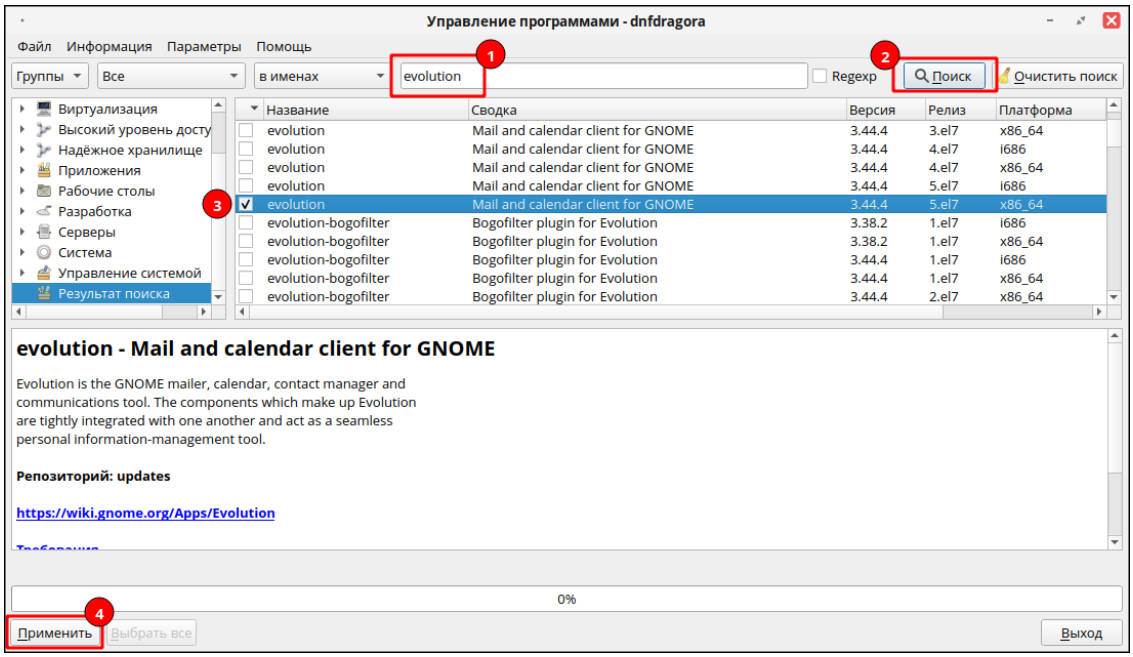
Evolution поддерживает следующие функции и протоколы:

- получение электронной почты по протоколам **POP3** и **IMAP** и её отправка по **SMTP**;
- поддержка расширений протокола **IMAP4** для быстрого обновления содержимого папок **Quick Resync** и уведомлений со стороны сервера **IMAP IDLE**;
- поддержка локальной почты на **UNIX**-системах;
- поддержка защищённых протоколов связи **SSL**, **TLS** и **STARTTLS**;
- шифрование переписки при помощи **GPG** и **S/MIME**;
- использование библиотеки **NSS** для управления сертификатами, что позволяет использовать общее хранилище между совместимыми программами, например, **Mozilla Firefox**, **Mozilla Thunderbird**, **LibreOffice** и пр;
- поиск по почтовым папкам и сортировка почты по критериям;
- автоматическая фильтрация спама с использованием **SpamAssassin** и **Bogofilter**;
- возможность работы с серверами **Microsoft Exchange Server**, **Novell GroupWise** и **Kolab**;
- календарь с поддержкой формата файлов **iCalendar** и протоколов **WebDAV**, **CalDAV** и возможностью подключения к **Google Calendar**;
- адресная книга с поддержкой локальных контактов, протоколов **CardDAV**, **LDAP** и контактов **Google**;
- интеграция адресной книги с **LibreOffice**;
- поддержка аватаров пользователей из адресной книги, из заголовков **X-Face**, **Face** и автоматический поиск их по хешу адреса электронной почты на сервисе **Gravatar**;
- поддержка расширений для чтения лент новостей **RSS**, синхронизации с мобильными устройствами и **VoIP** приложением **Ekiga**;
- импорт почты из архивов **Microsoft Outlook** (файлы с расширениями **.dbx**, **.pst**) и **Berkley Mailbox**.

Установка Evolution

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Evolution** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**evolution**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

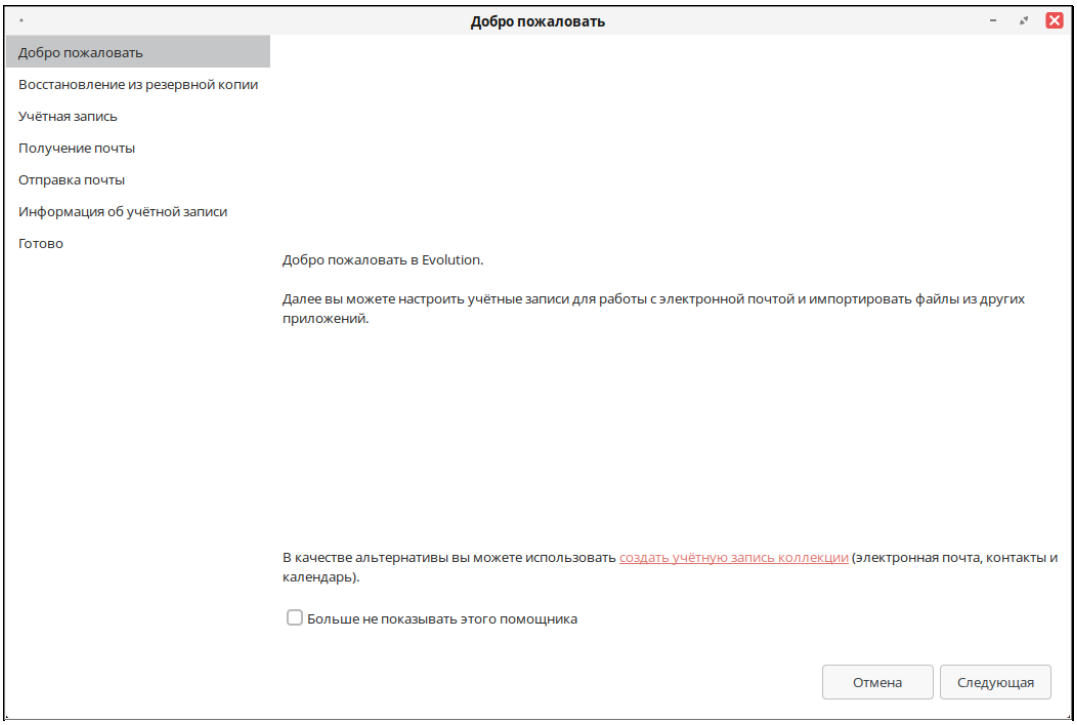
```
dnf install evolution
```

После установки **Evolution** будет доступен из «**Главного меню**» – «**Офис**» – «**Evolution**».

При первом запуске почтового клиента будет выведено окно с настройкой основных функций для работы программы. Здесь вы можете создать новую учетную запись или импортировать файлы из уже существующей, задать параметры почтового сервера, настроить параметры получения и отправки почты.

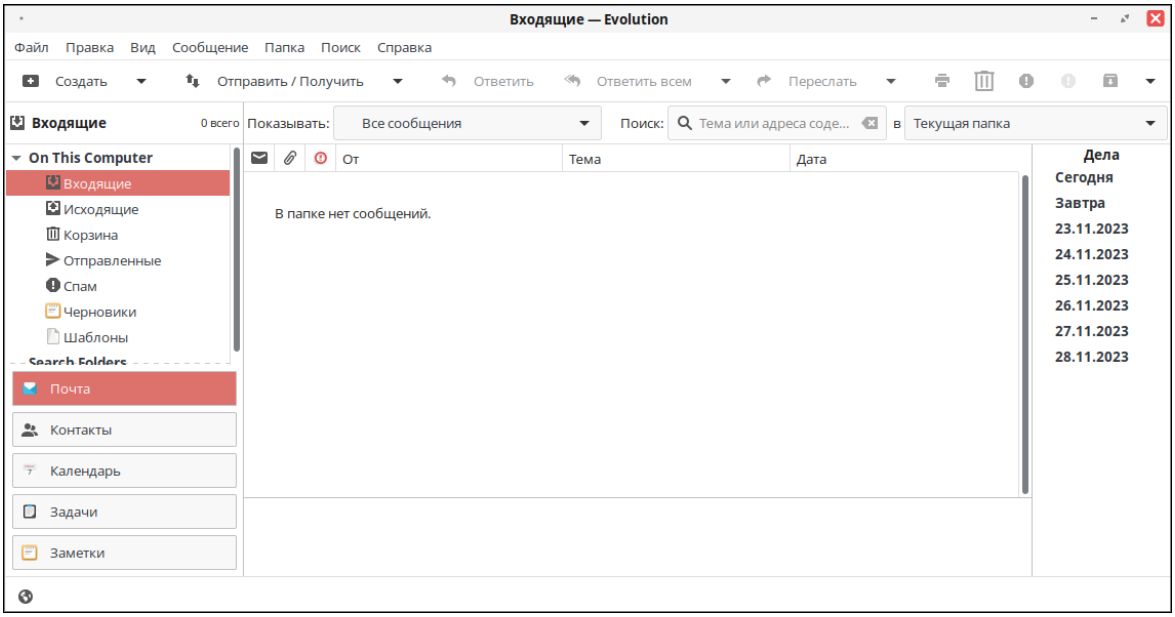
На шаге «**Информация об учетной записи**» необходимо проверить правильность введенных данных и указанных параметров почтового сервера. Если все настроено верно, перейдите к шагу «**Готово**» и начните пользоваться почтовым клиентом.

В противном случае нажмите «**Назад**» и внесите необходимые изменения в настройки клиента.

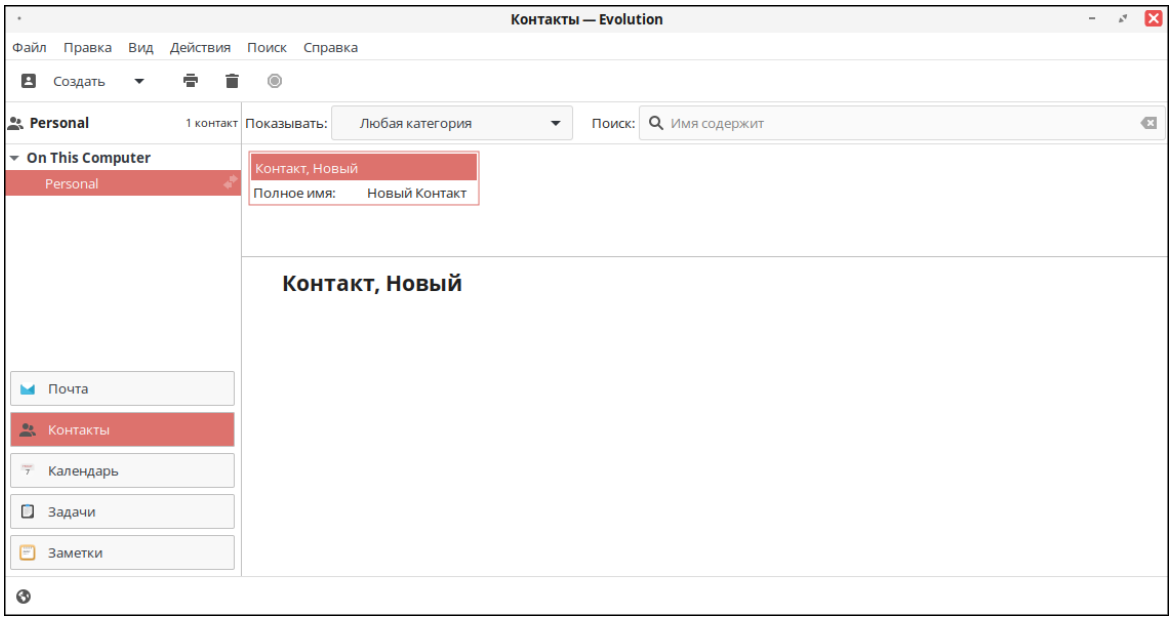


Основные функции

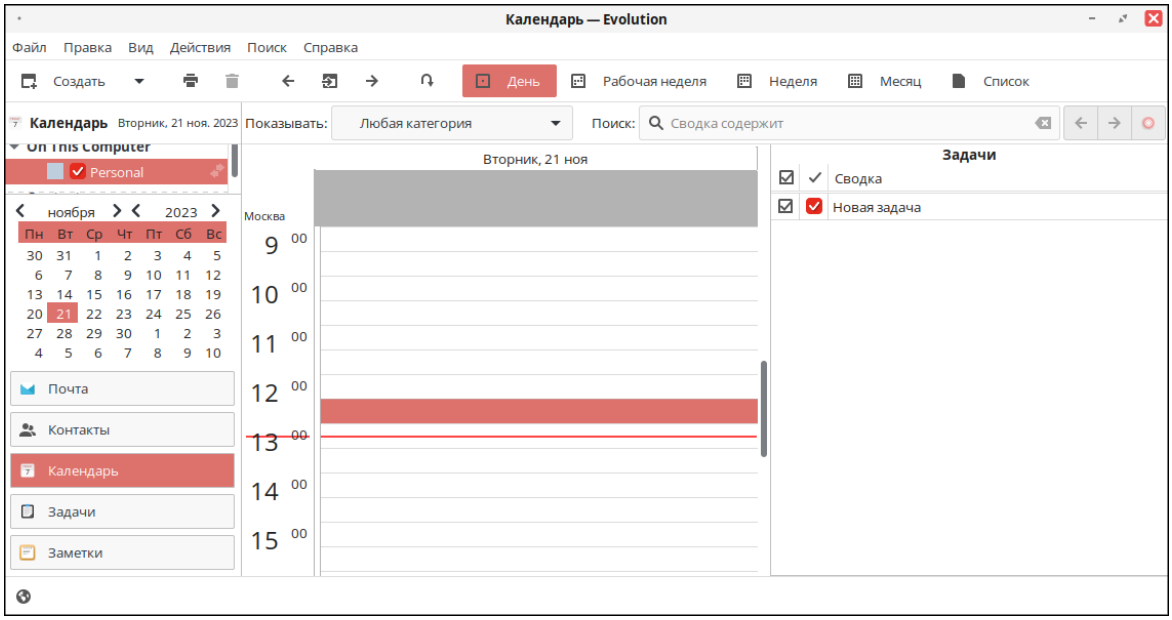
В **Evolution** реализованы стандартные функции почтового клиента – работа непосредственно с электронный почтой.



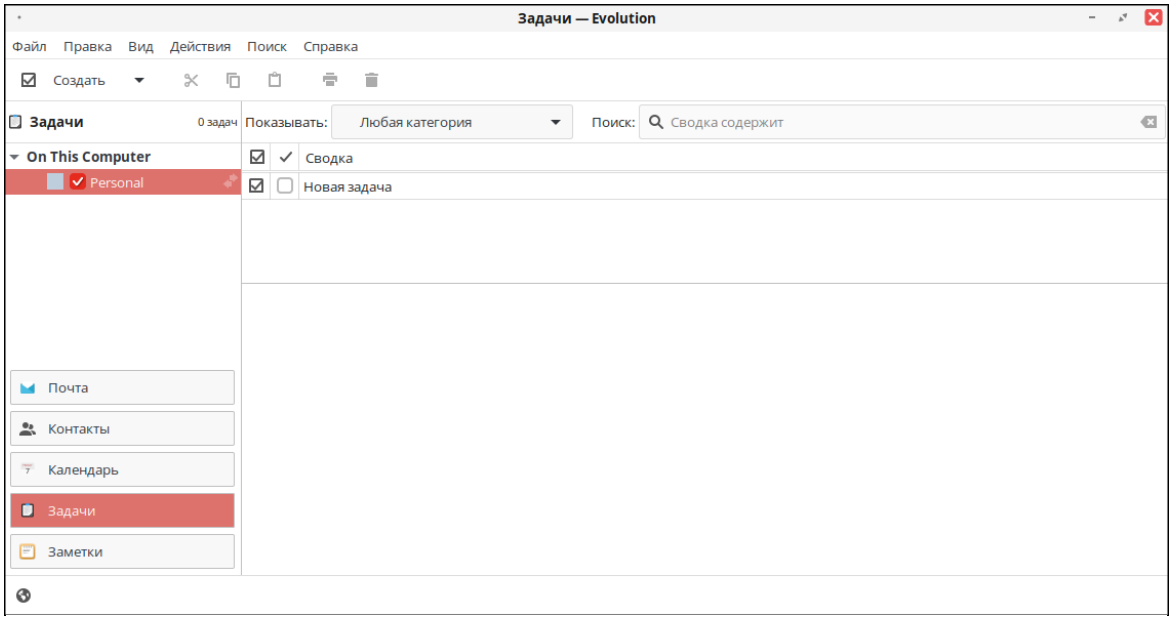
Отдельная вкладка для работы с контактами – добавьте новые контакты.



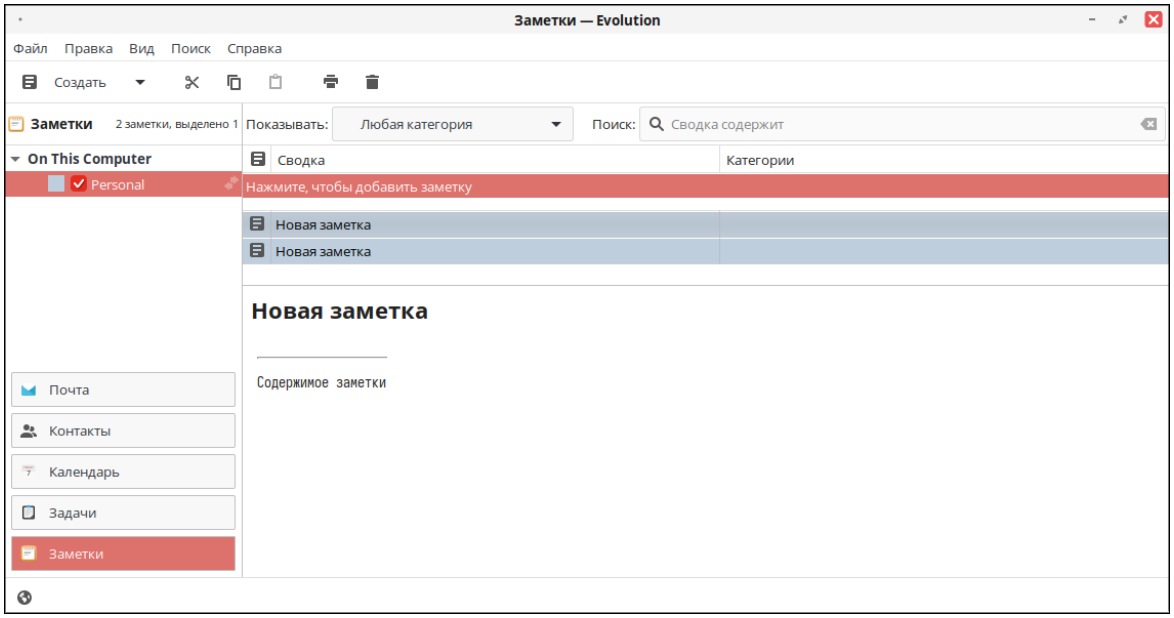
Календарь, в котором можно добавлять мероприятия на определенный день, настраивать оповещение о предстоящем мероприятии или событии.



Вкладка «**Задачи**» – возможность создавать задачи, устанавливать сроки их выполнения, приоритет и текущее состояние.



Также доступно ведение заметок.



Почтовый клиент Thunderbird

Установка
Основные возможности программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: thunderbird-102.15.0-1

Mozilla Thunderbird — это бесплатное приложение для работы с электронной почтой, разработанное командой *Mozilla Foundation*. Это один из самых популярных почтовых клиентов, который предоставляет широкие возможности для организации и управления электронной почтой.

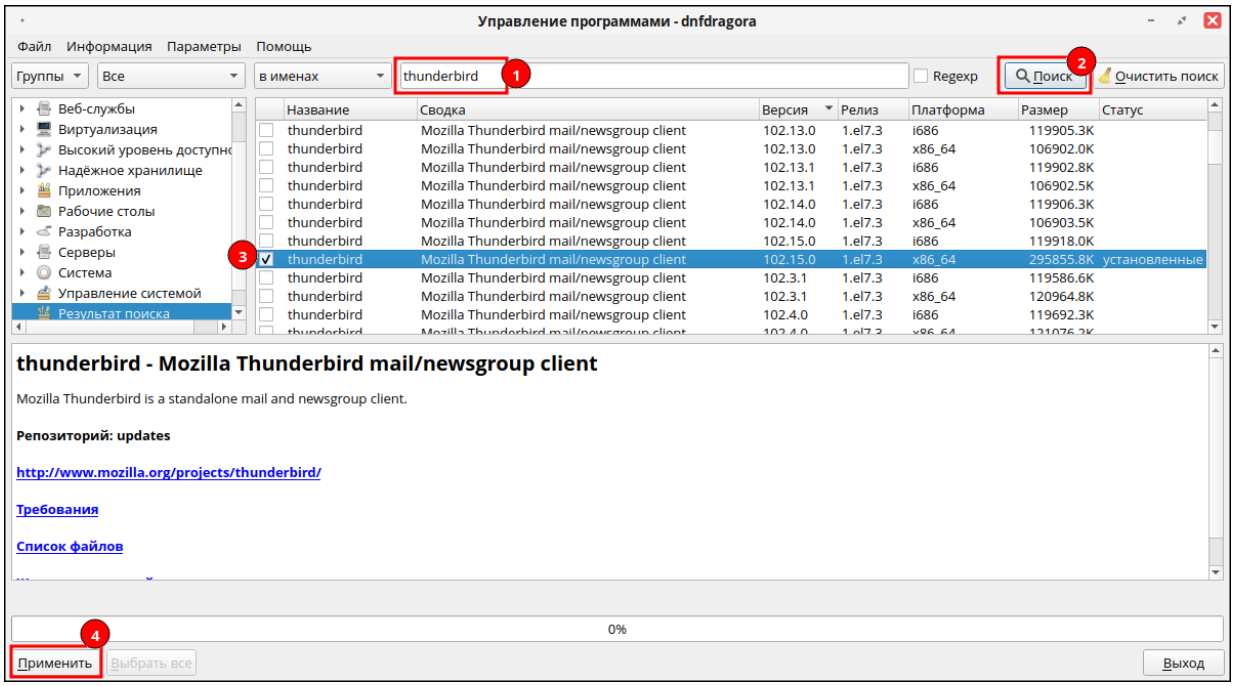
Thunderbird позволяет гибко настраивать учетную запись электронной почты, устанавливать и настраивать различные фильтры и правила, создавать папки для организации писем, устанавливать шаблоны и многое другое. Все письма и контакты хранятся локально на компьютере, обеспечивая безопасность и конфиденциальность данных.

Поддерживаются популярные почтовые протоколы, включая **POP3**, **IMAP** и **SMTP**. Есть возможность подключать почтовые ящики от разных провайдеров с автоматическим обнаружением настроек и управлять ими из одного интерфейса.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Thunderbird** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**thunderbird**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

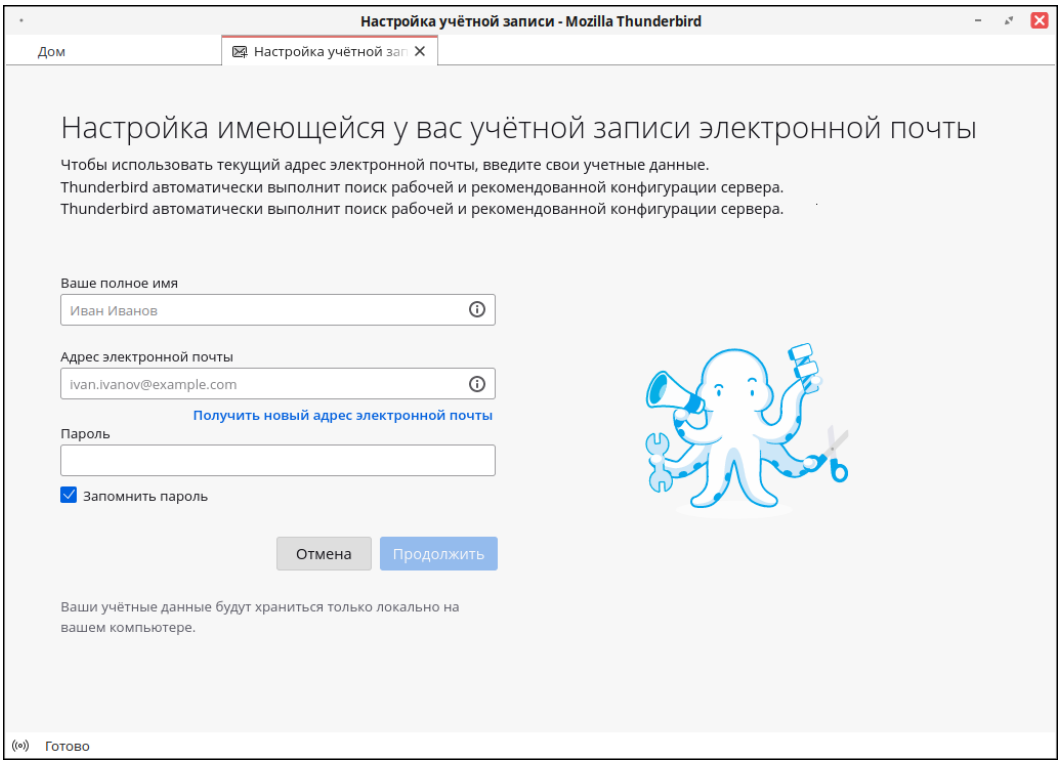
```
su -
```

и выполните команду:

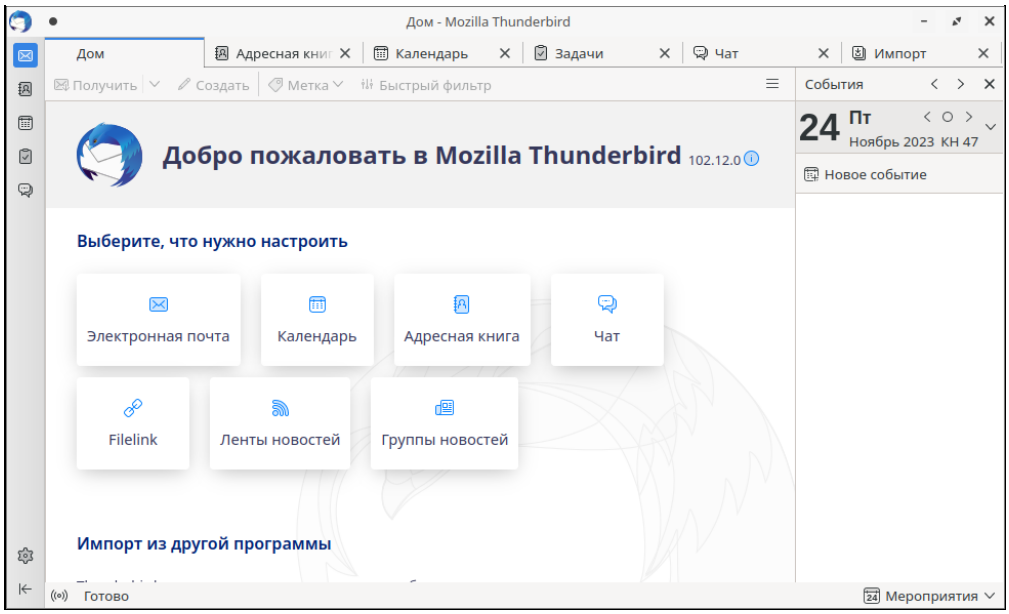
```
dnf install thunderbird
```

После установки **Thunderbird** будет доступен из «**Главного меню**» – «**Интернет**» – «**Почтовый клиент Thunderbird**».

При первом запуске почтового клиента будет предложено ввести данные существующей учетной записи для автоматического определения настроек сервера.

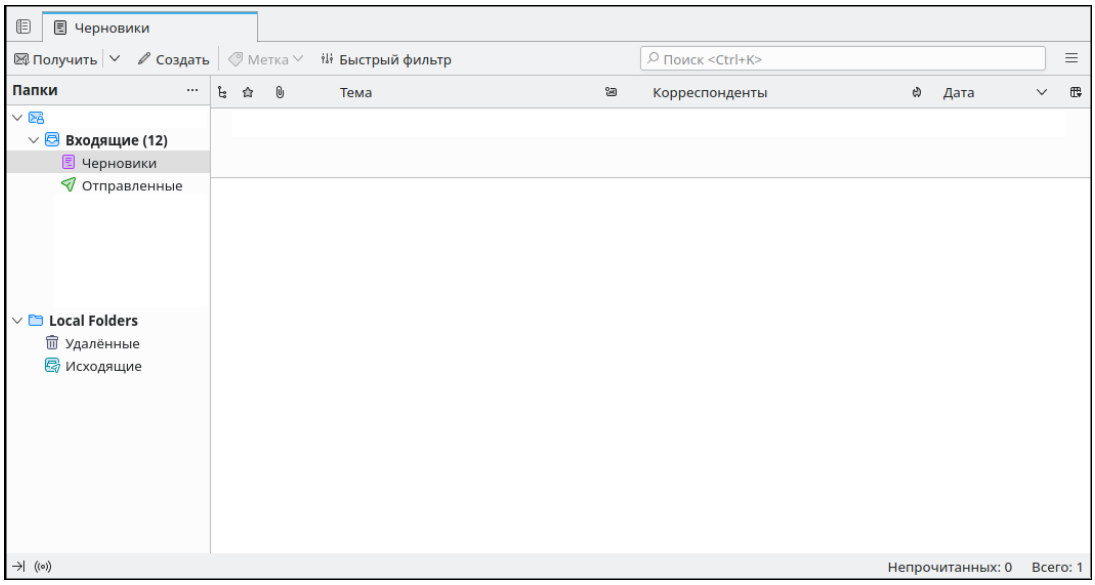


После входа в учетную запись будет открыта домашняя страница почтового клиента, где можно выбрать, что нужно настроить.



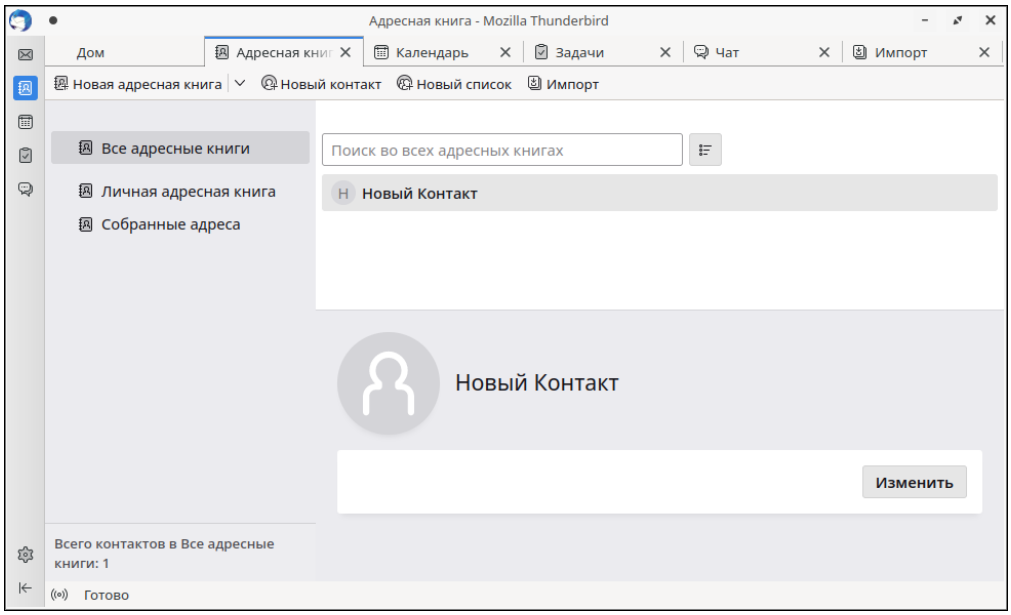
Основные возможности программы

Thunderbird имеет стандартный набор функций почтового клиента, основная из которых – работа с электронной почтой. Thunderbird умеет сохранять письма и вложения локально на компьютере, что обеспечивает доступ к ним даже без интернета. Кроме того, встроенный поиск позволяет быстро находить нужные сообщения.

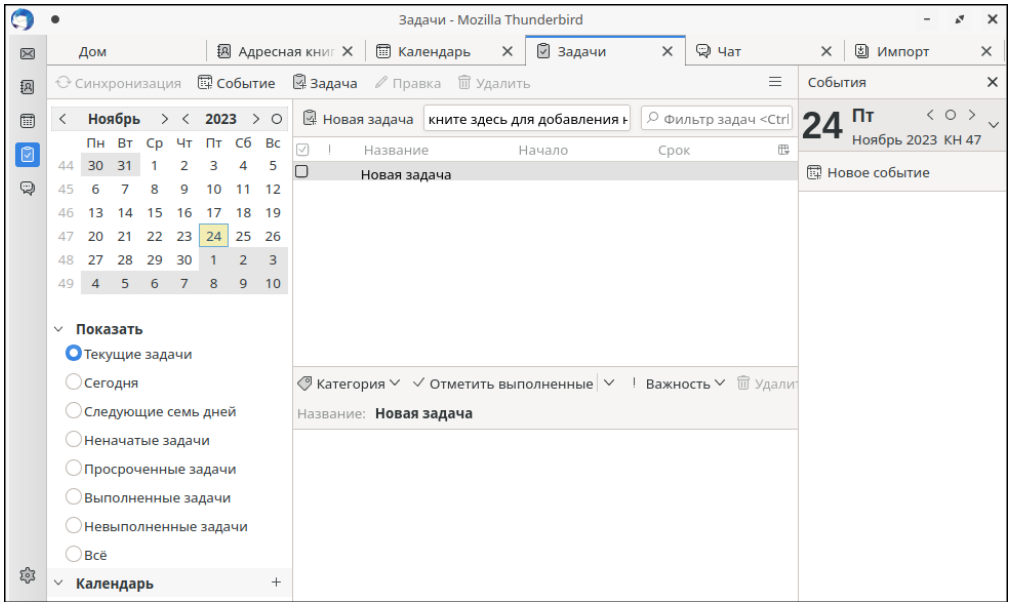


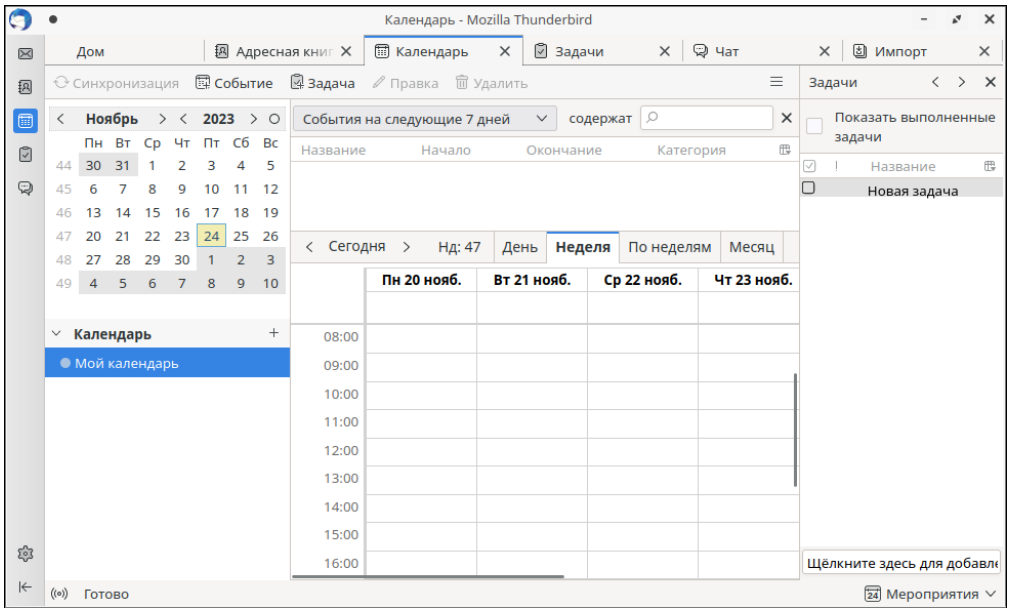
Thunderbird включает встроенные инструменты для борьбы со спамом и обнаружения вредоносных программ. Он также поддерживает шифрование и аутентификацию, чтобы обеспечить безопасность ваших электронных писем.

Также доступна возможность работы с адресной книгой.

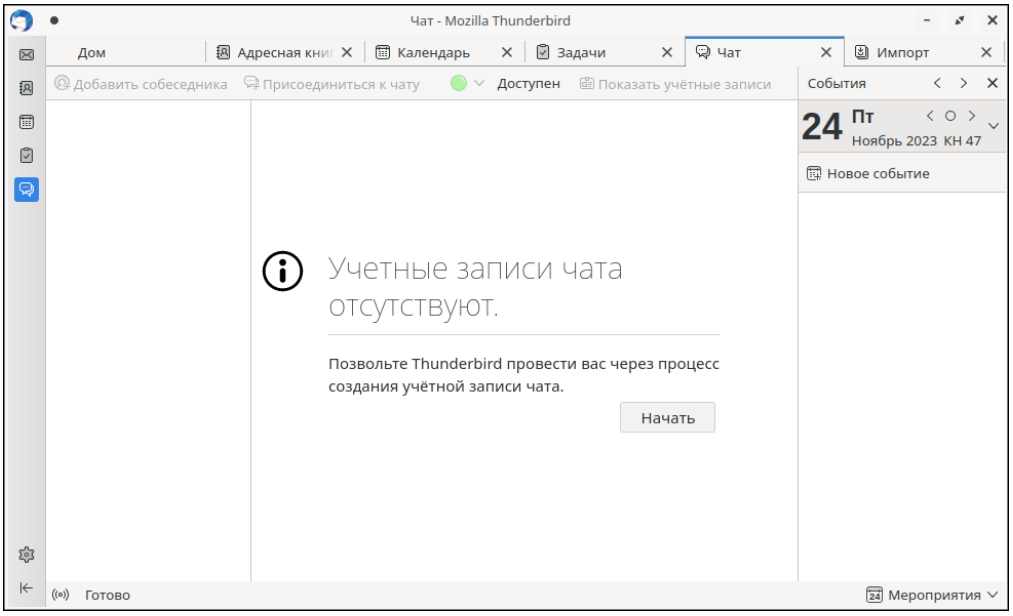


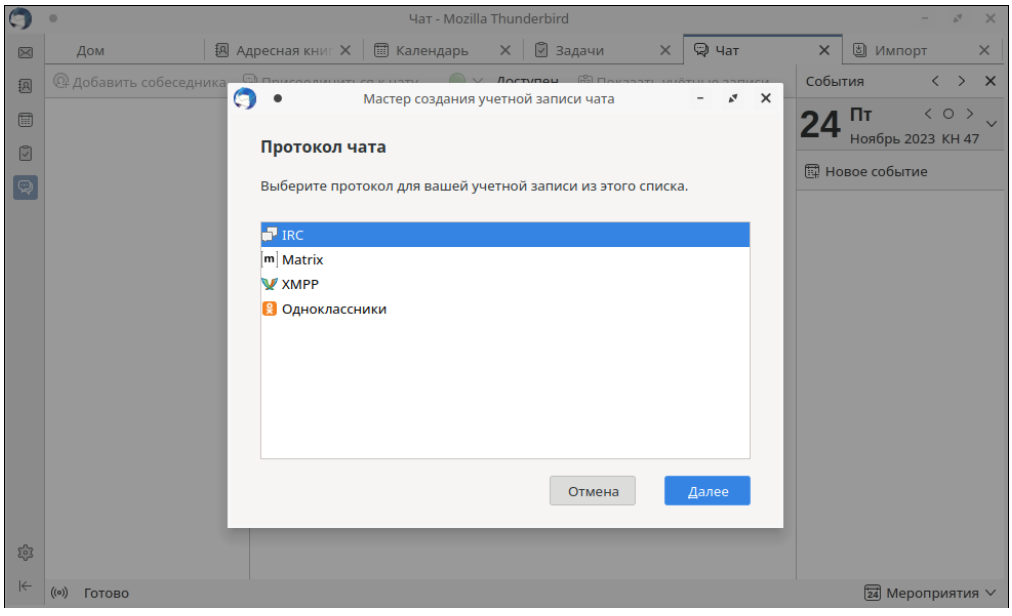
Присутствуют функции календаря, совмещенного с задачами, что позволяет управлять своим временем и не пропускать важные события.





Имеется возможность подключения учетной записи для чата, для выбора доступны такие протоколы, как **IRC**, **Matrix**, **XMPP**, **Одноклассники**.

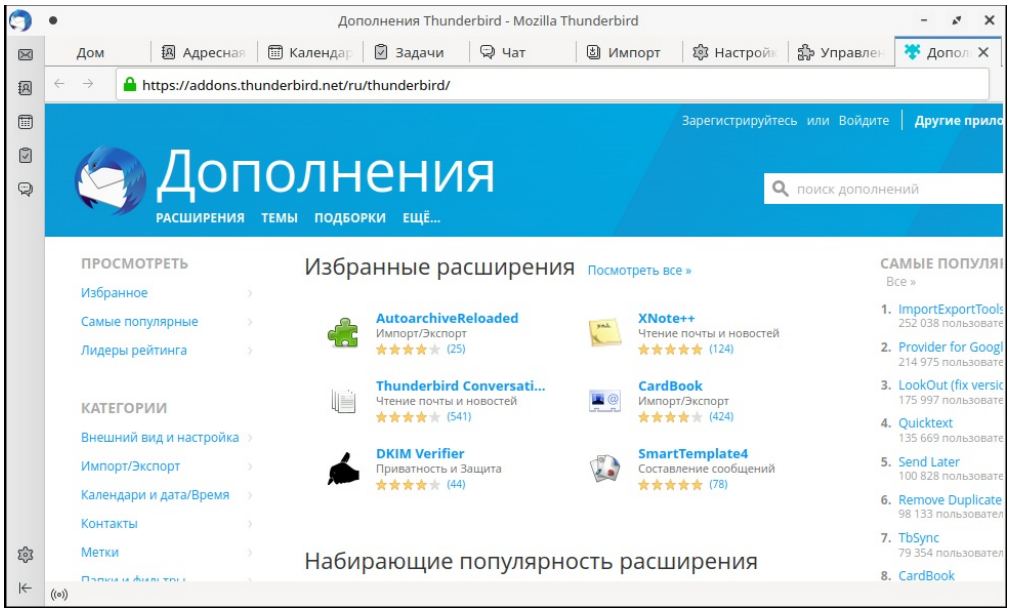




Thunderbird поддерживает подписку на новостные рассылки и чтение **RSS**-каналов, позволяя вам получать свежие новости и информацию из интересующих источников.

Главным достоинством **Thunderbird** можно назвать возможность установки различных дополнений, тем оформления, расширений. Это

позволяет гибко настраивать внешний вид почтового клиента под свой вкус, а также расширять функционал и возможности программы.



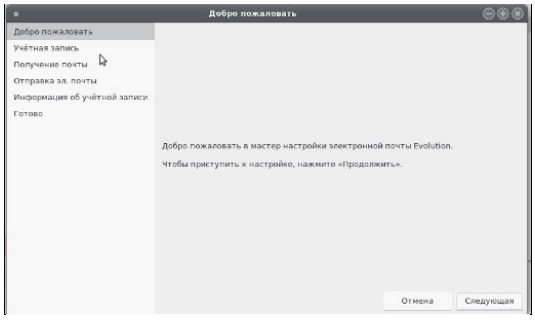
Настройка в Evolution подключения к MS Exchange

У вас должен быть установлен плагин для работы **EWS**. Установить его можно командой:

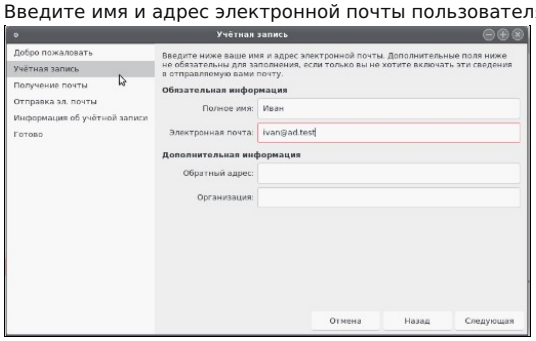
```
dnf install evolution-ews
```

Перейдите в меню »Файл > Создать > Учетная запись почты».

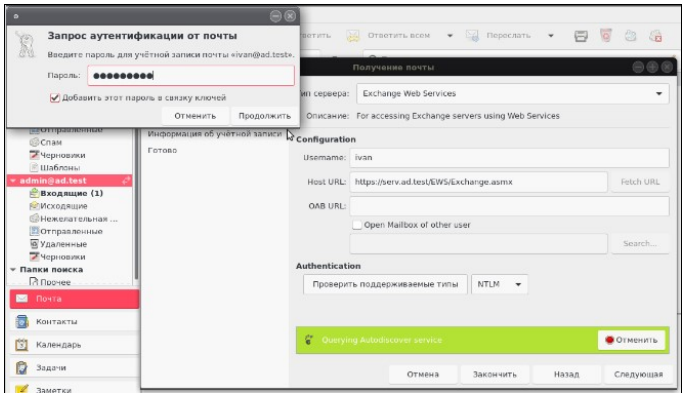
Откроется окно. Нажмите кнопку «Следующая».



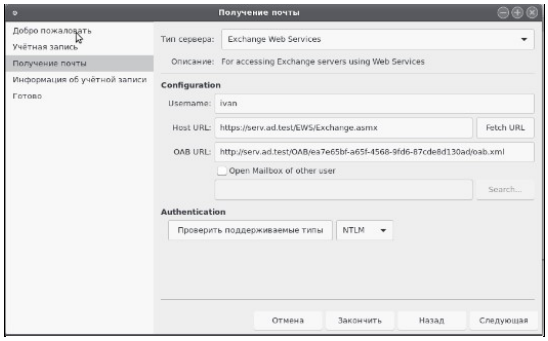
Введите имя и адрес электронной почты пользователя и нажмите кнопку «Следующая».



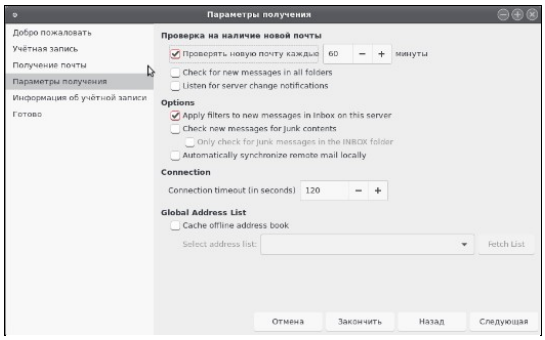
Выберете тип сервера Exchange Web Services. Введите правильный адрес к EWS и нажмите кнопку «Fetch URL».
Если все сделано правильно, откроется окно ввода пароля пользователя. Введите пароль и нажмите кнопку «Продолжить».



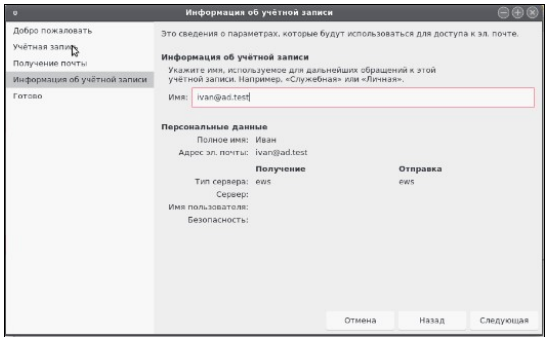
Если пароль введен верно, сервер вернет OAB URL, он отобразится в соответствующем окне. Нажмите кнопку «Следующая».



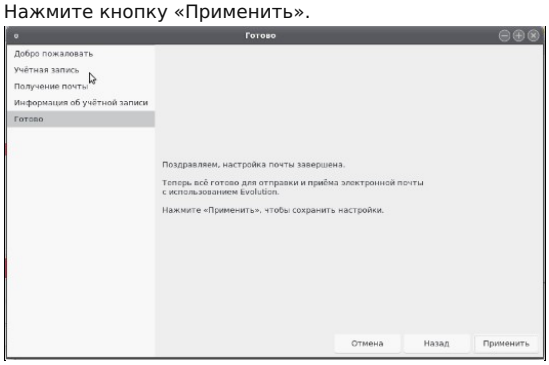
В следующем окне настройте параметры получения или оставьте их по умолчанию. Нажмите кнопку «Следующая».



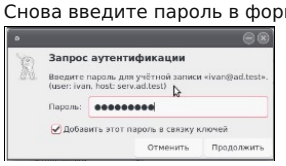
Укажите имя учетной записи для обращений или оставьте значение по умолчанию. Нажмите кнопку «Следующая».



Нажмите кнопку «Применить».



Снова введите пароль в форме ввода пароля.



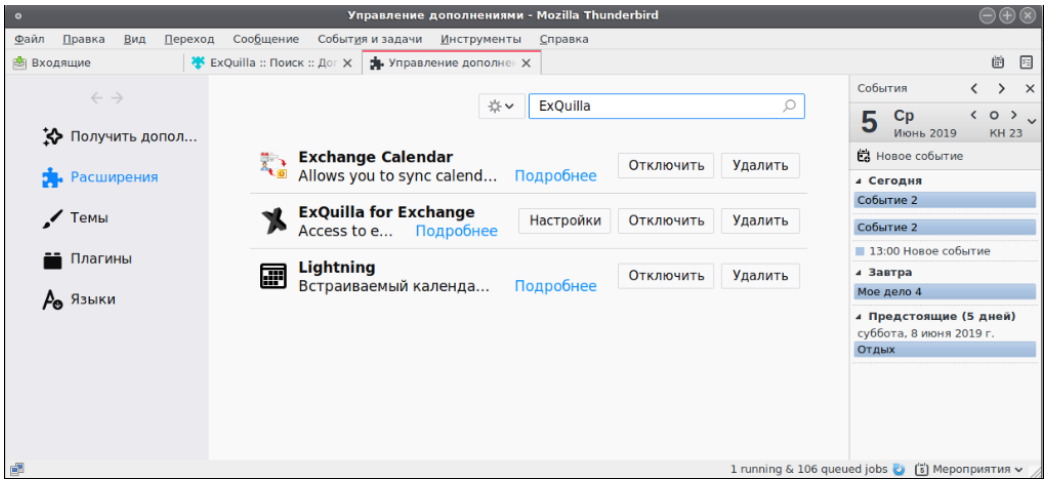
На этом почта подключена. Также автоматически подключен календарь, задачи, заметки. Есть возможность просмотра адресных книг.

Настройка календаря Exchange в Thunderbird

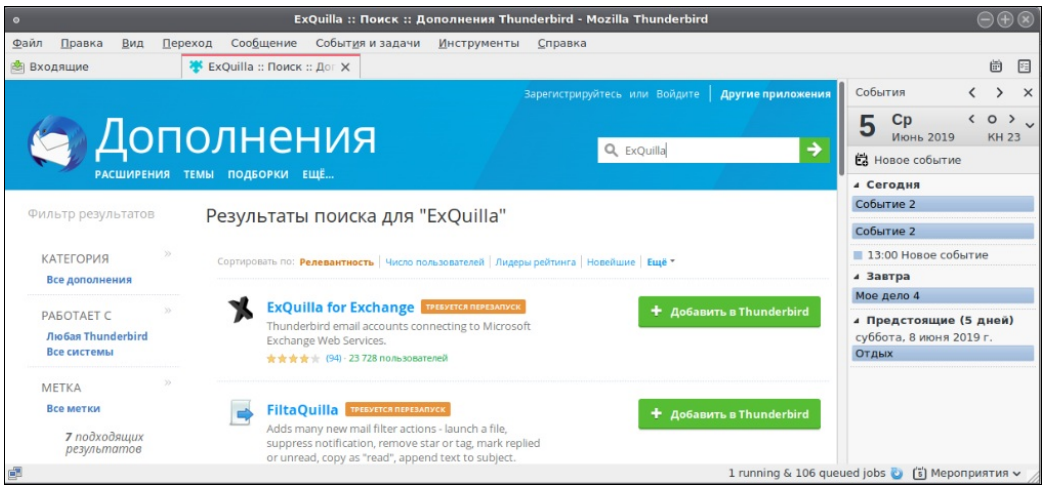
Настройка почты

Для подключения почты Exchange к Thunderbird скачайте и установите плагин ExQuilla for Exchange.

Для этого в меню нажмите Инструменты > Дополнения. В открывшемся окне выберите Расширения и в верхнем правом углу в строку поиска введите "ExQuilla".



В списке найденного нажмите кнопку "Добавить в Thunderbird" напротив плагина ExQuilla for Exchange. После установки перезагрузите почтовый клиент.

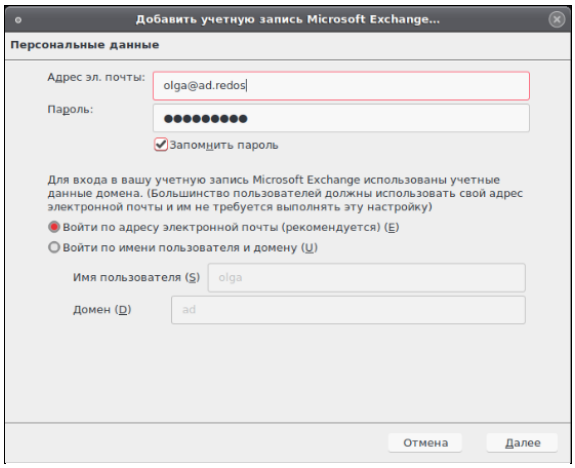


ВАЖНО

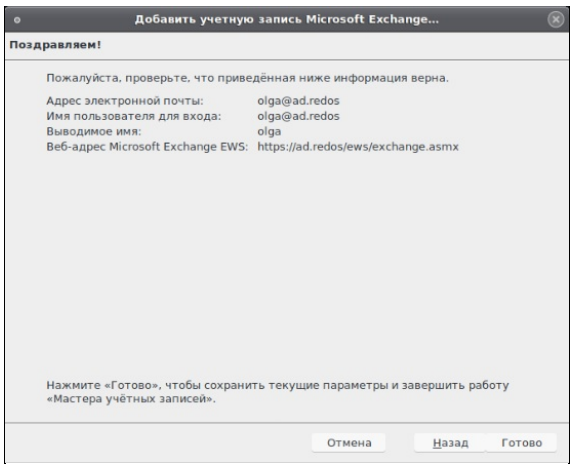
У вас должен быть установлен плагин Lighting

Далее подключите календарь. Выберите меню "Файл" > "Создать" > "Добавить учетную запись Microsoft Exchange".

В открывшемся окне введите адрес эл. почты, пароль и нажмите кнопку "Далее"

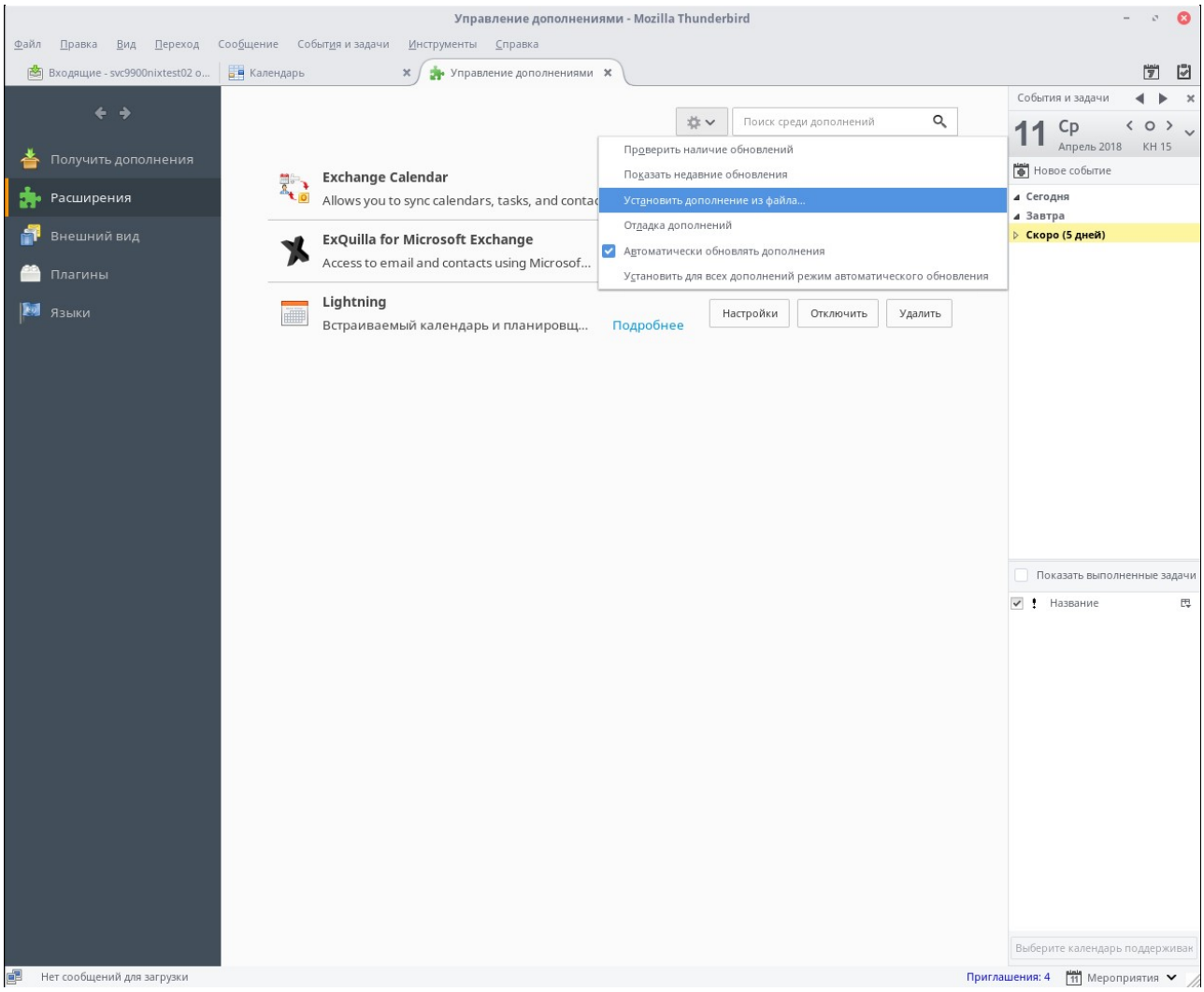


Должен автоматически определится адрес почтового сервера и появиться окно с успешным подключением. Остается только нажать кнопку "Готово".



Настройка календаря

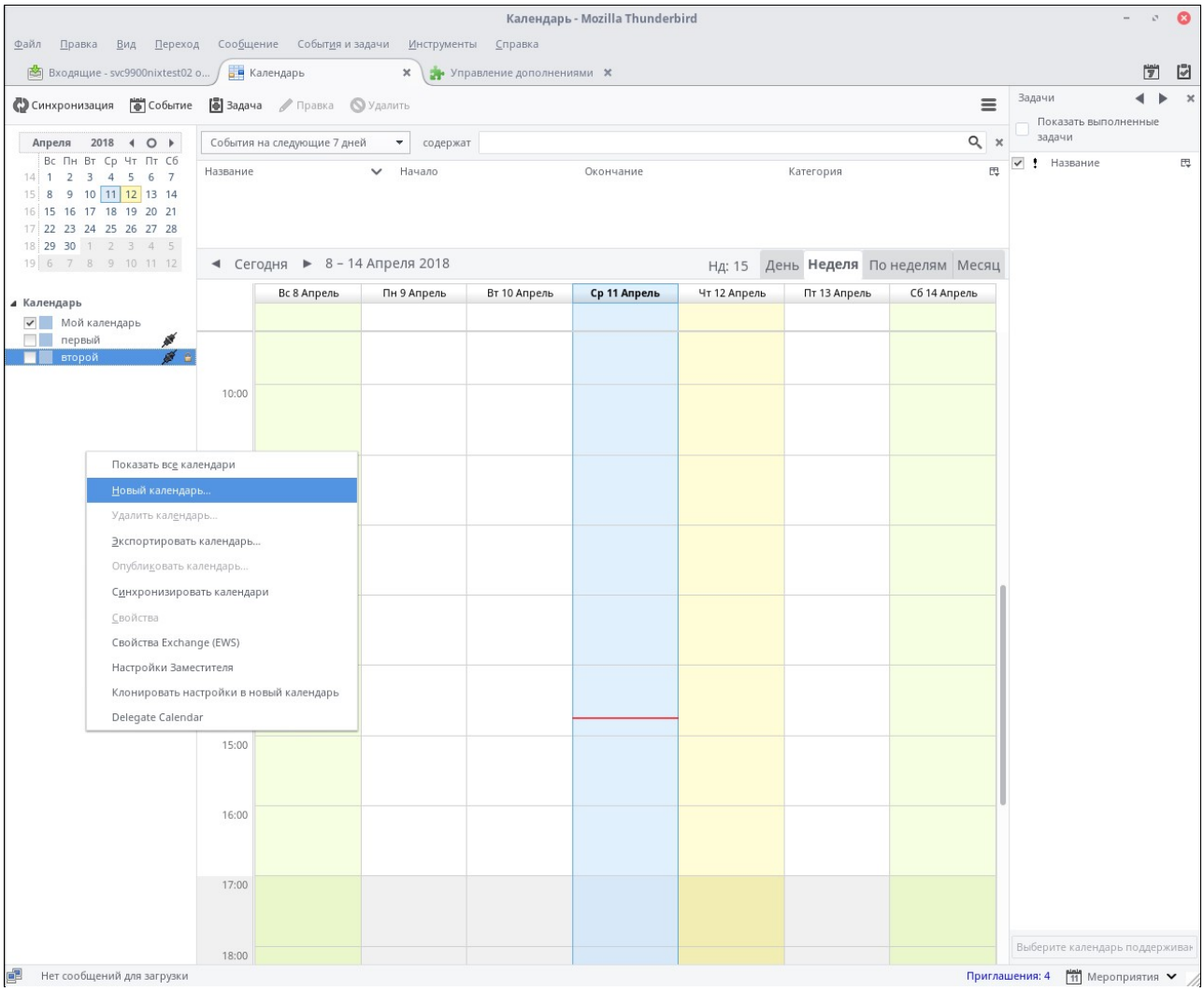
1. Скачайте дополнение ExchangeCalendar по ссылке:
https://github.com/ExchangeCalendar/exchangecalendar/releases
Откройте Thunderbird перейдите в меню и выберите пункт “Дополнения”.
Перейдите на вкладку “Расширения” и нажмите на шестеренку, затем выберите пункт “Установить дополнение из файла”.



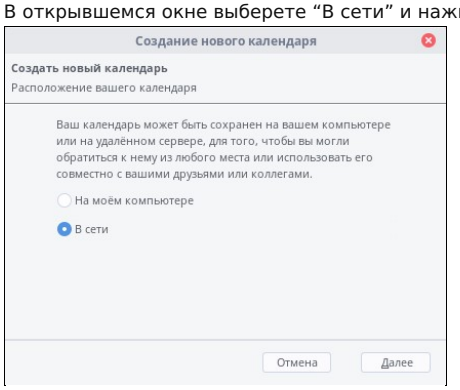
Выберите скачанный файл дополнения и нажмите “Ок”. Затем установите его и перезагрузите почтовый клиент.

2. Добавьте календарь.

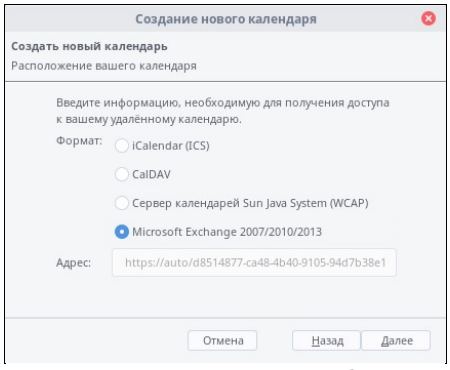
Откройте Thunderbird перейдите на вкладку “Календарь”.
В списке календарей нажмите на правую кнопку мыши и выберете “Новый календарь”.



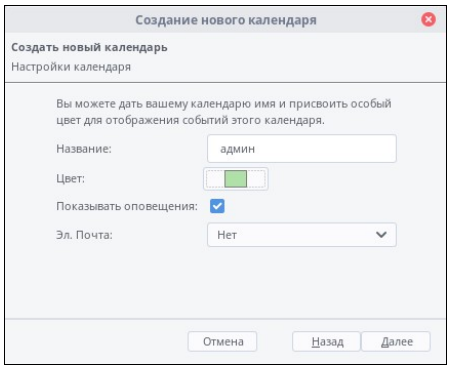
В открывшемся окне выберете “В сети” и нажмите кнопку “Далее”.



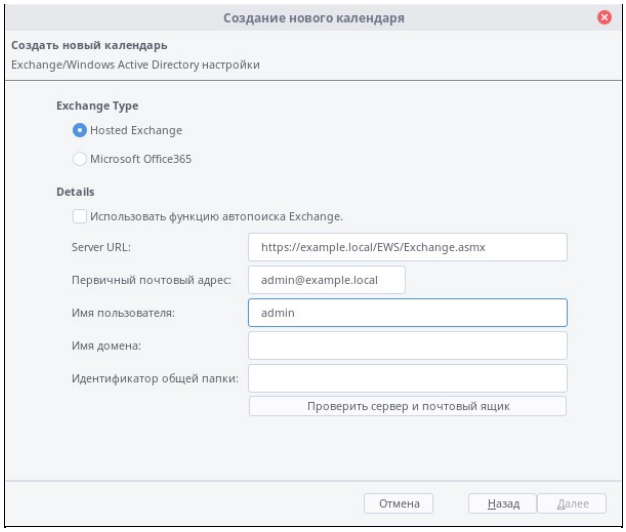
Выберите пункт “Microsoft Exchange 2007/2010/2013” и нажмите кнопку “Далее”.



Введите название календаря, выберите цвет, при выборе электронной почты укажите её или выберите “Нет” и нажмите кнопку “Далее”.



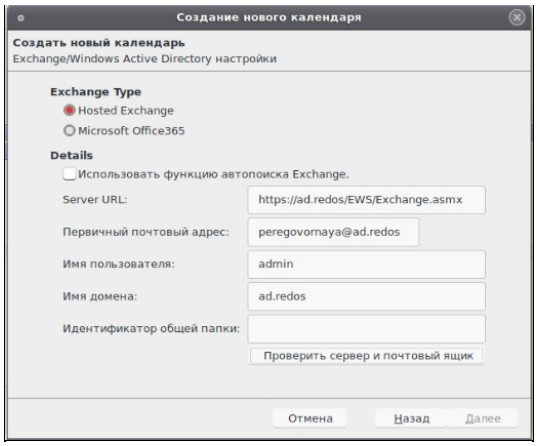
Выберите “Hosted Exchange”, введите Server URL. Обычно, адрес следующий https://<имя почтового сервера>/EWS/Exchange.asmx. Введите первичный почтовый адрес и имя пользователя, затем нажмите кнопку “Проверить сервер и аккаунт”.



В открывшемся окне введите пароль от аккаунта. Окно может появляться несколько раз.
Теперь нажмите кнопку “Далее” и “Готово”.
Календарь подключен.

Подключение общего календаря помещений или оборудования

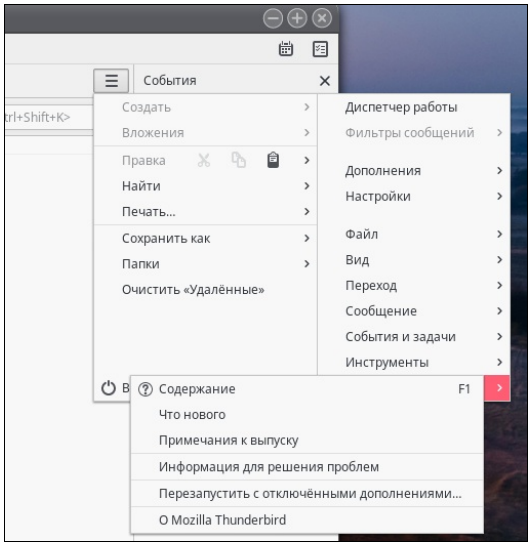
Для подключения любого общего календаря нужно при его подключении вписать в поле "Первичный почтовый адрес" адрес этого календаря. Пример на скриншоте ниже.

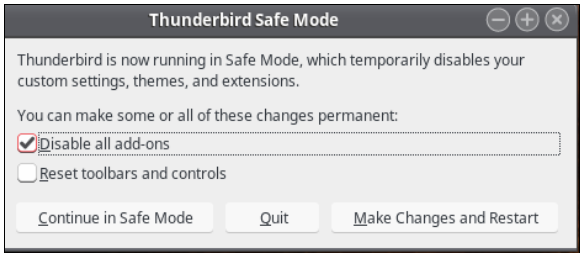


Thunderbird запуск Google-почты

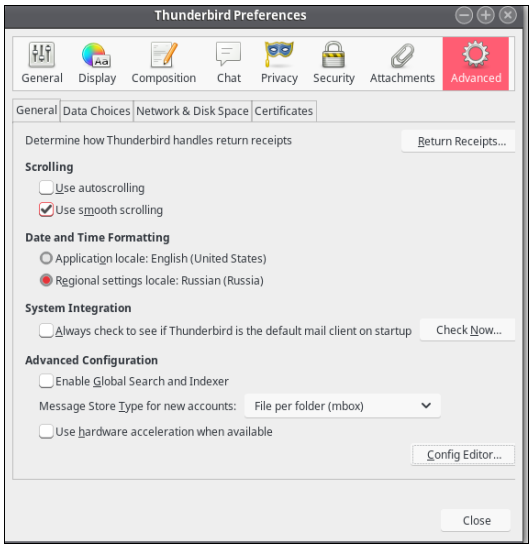
Настройка добавления Google аккаунта в ThunderBird при возникновении проблемы при авторизации с использованием OAuth2:

Включите Безопасный Режим Thunderbird для этого зайдите в Справку-> Перезапустить с отключенными дополнениями -> Disable all add-ons -> Continue in safe mode



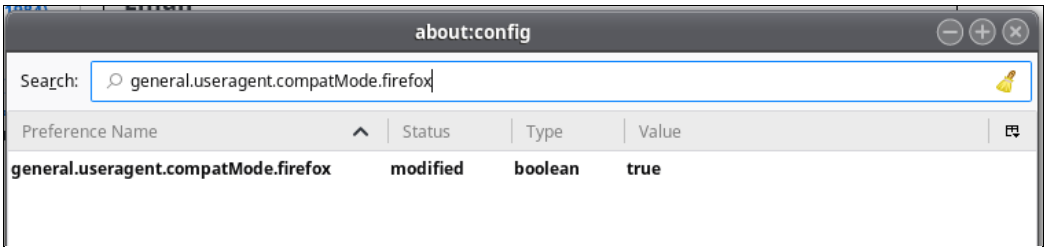


После запуска в безопасном режиме откройте Thunderbird Preferences -> Advanced -> General -> Config Editor -> согласитесь с уведомлением, откроется список доступных конфигураций



Воспользуйтесь поиском **general.useragent.compatMode.firefox** и измените значение на true.

Если параметр отсутствует, добавьте его с меткой boolean, значение true.



Выйдите из безопасного режима и попробуйте ввести данные Google аккаунта.

Firefox

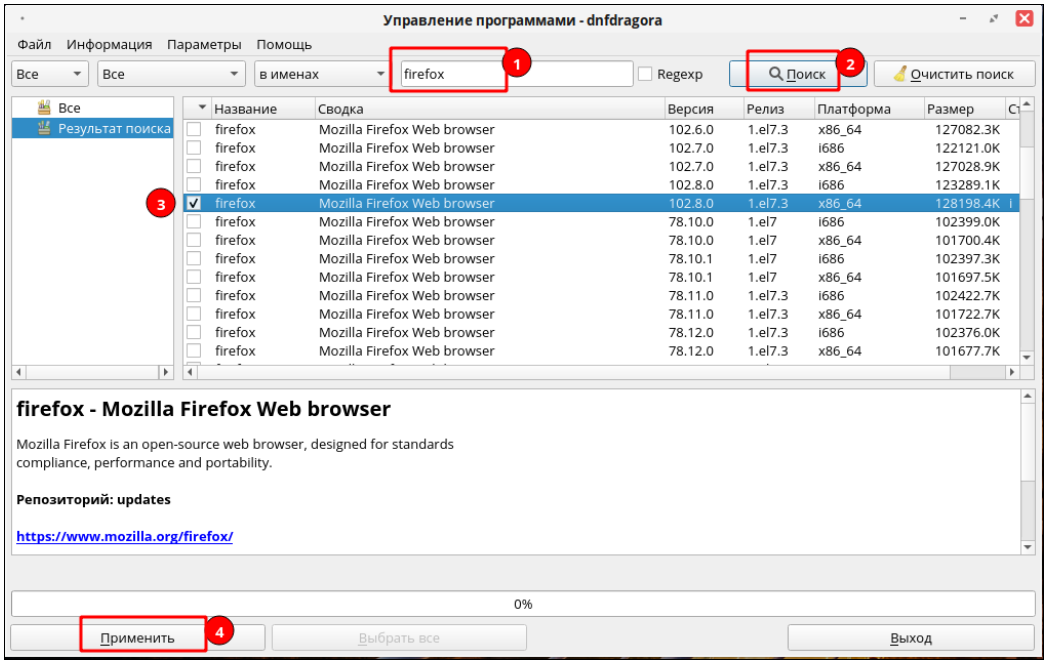
Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: firefox-102.8.0-1

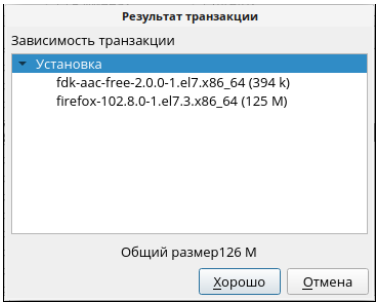
Firefox — свободный интернет-браузер, созданный компанией **Mozilla Corporation** на основе движка **Quantum**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**firefox**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Согласитесь с установкой зависимых пакетов, нажав кнопку «**Хорошо**».



Установка займет некоторое время, после успешной установки окно с транзакцией исчезнет. Сам пакет будет отмечен как установленный.

Для установки браузера через терминал перейдите в сеанс пользователя **root**:

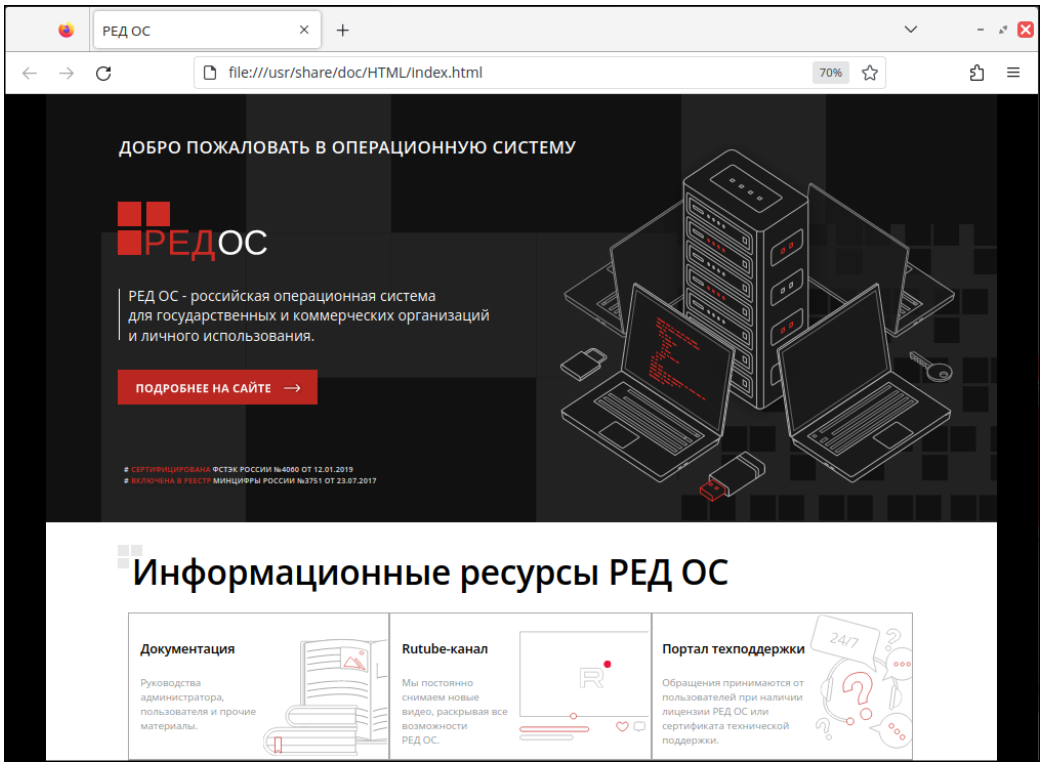
```
su -
```

и выполните команду:

```
dnf install firefox
```

Работа в программе выполняется от локального пользователя.

После установки браузер будет доступен из «**Главного меню**» — «**Интернет**» — «**Интернет-браузер Firefox**».


РЕД ОС
file:///usr/share/doc/HTML/index.html
70%
ДОБРО ПОЖАЛОВАТЬ В ОПЕРАЦИОННУЮ СИСТЕМУ
РЕДОС
РЕД ОС - российская операционная система
для государственных и коммерческих организаций
и личного использования.
ПОДРОБНЕЕ НА САЙТЕ
СЕРТИФИЦИРОВАНА ФСТЭК РОССИИ №4060 ОТ 12.01.2019
ВКЛЮЧЕНА В РЕЕСТР МИНЦИФРЫ РОССИИ №3751 ОТ 23.07.2017
Информационные ресурсы РЕД ОС
Документация
Руководства администратора, пользователя и прочие материалы.
Rutube-канал
Мы постоянно снимаем новые видео, раскрывая все возможности РЕД ОС.
Портал техподдержки
Обращения принимаются от пользователей при наличии лицензии РЕД ОС или сертификата технической поддержки.
24/7

Яндекс.Браузер

Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora
Решение проблем

Окружение

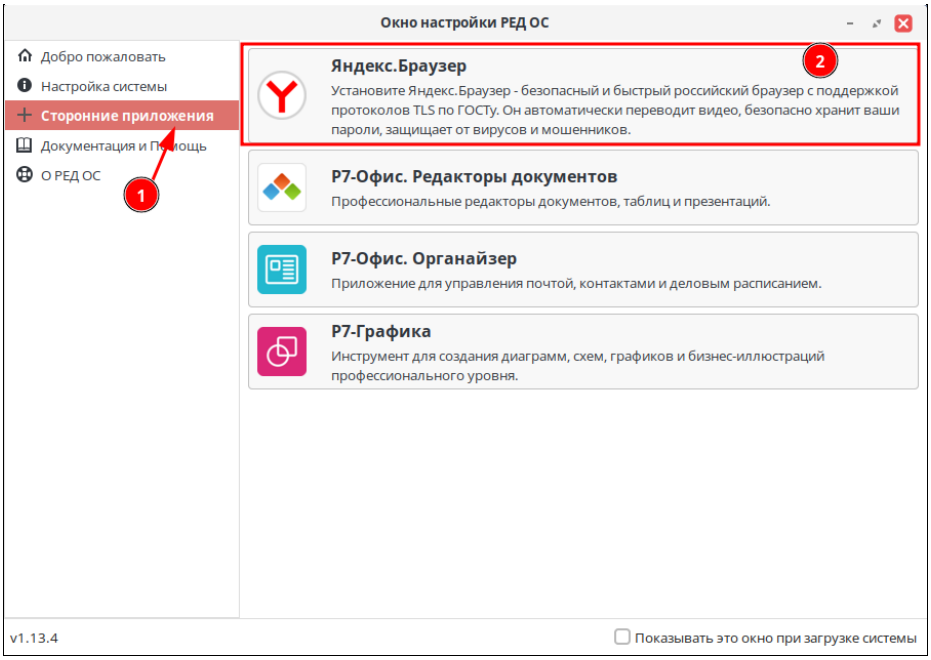
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** yandex-browser-release-2.0-1, yandex-browser-stable-24.6.1.867-1

Яндекс.Браузер для РЕД ОС размещается в отдельном подключаемом (с помощью пакета **yandex-browser-release**) репозитории. **Яндекс.Браузер** в данном репозитории был собран специально для работы в РЕД ОС и использует зависимости и кодеки из репозитория РЕД ОС. Репозиторий подключен **во всех** поддерживаемых версиях и редакциях РЕД ОС.

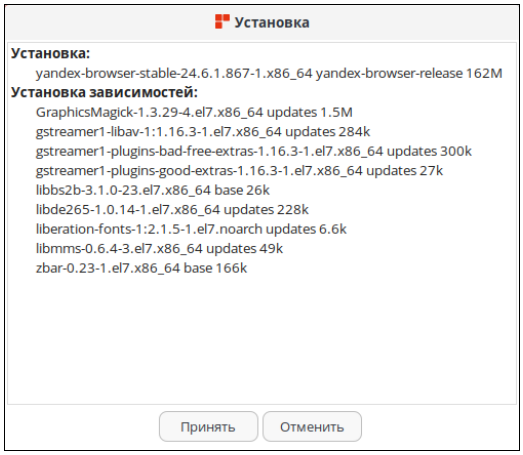
Установка через «Окно настройки РЕД ОС»

Откройте утилиту «Окно настройки РЕД ОС».

Перейдите на вкладку «**Сторонние приложения**», затем выберите из списка **Яндекс.Браузер**.



Далее в появившемся окне «**Установка**» со списком устанавливаемых пакетов и зависимостей нажмите кнопку « **Принять**». Начнётся установка **Яндекс.Браузера**.



После установки **Яндекс.Браузер** будет доступен из «**Главного меню**» - «**Интернет**» - «**Yandex Browser**».

Установка через терминал

Для установки браузера через терминал выполните команду (потребуются права **администратора**):

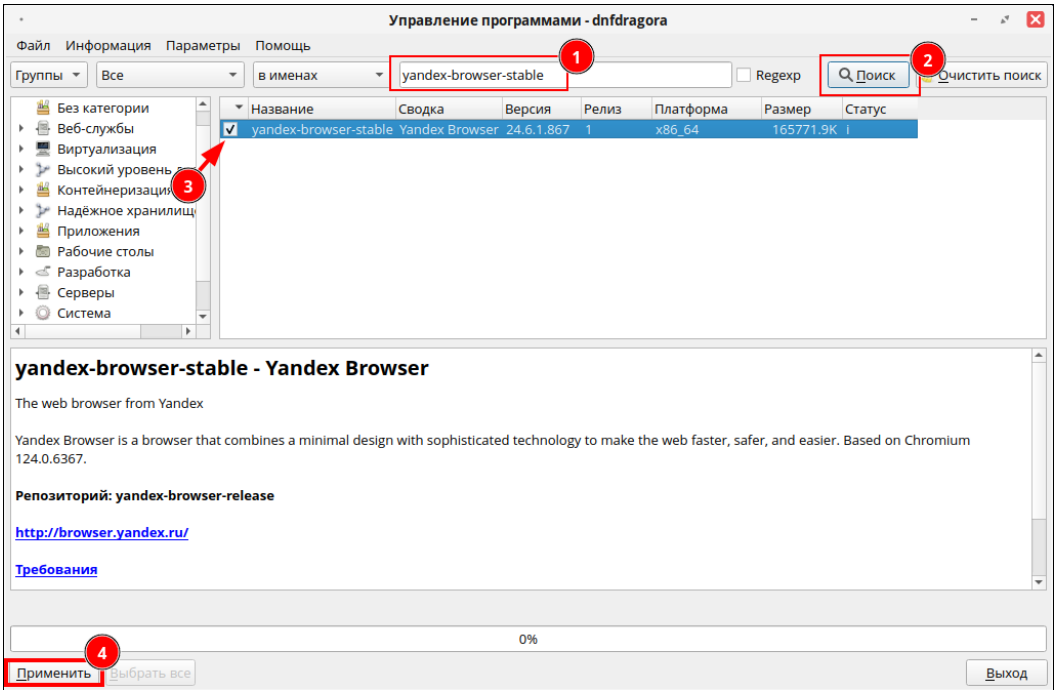
```
sudo dnf install yandex-browser-stable
```

После установки **Яндекс.Браузер** будет доступен из «**Главного меню**» - «**Интернет**» - «**Yandex Browser**».

Установка через dnfdragora

Для установки **Яндекс.Браузера** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**yandex-browser-stable**».

В результатах поиска появится пакет **yandex-browser-stable**. Отметьте флагом пакет и нажмите кнопку «**Применить**» для его установки.



После установки браузер будет доступен из «**Главного меню**» - «**Интернет**» - «**Yandex Browser**».

Решение проблем

В некоторых случаях при попытке установить **Яндекс.Браузер** через терминал или менеджер пакетов dnfdragora пакет **yandex-browser-stable** может быть не найден. Такая ситуация может произойти, если в используемой системе по каким-либо причинам не подключен репозиторий браузера **yandex-browser-release**.

Для решения данной проблемы в терминале рекомендуется выполнить команду подключения репозитория и установки браузера (потребуются права **администратора**):

```
dnf install yandex-browser-release && dnf install yandex-browser-stable
```

Сквозная аутентификация в браузерах

Chromium
Яндекс
Mozilla Firefox
SSO для нескольких доменов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Технология единого входа (англ. **Single Sign-On**) - это механизм, позволяющий пользователю пройти аутентификацию (вход со своими учетными данными) единовременно и получить доступ к различным программным продуктам, используя один идентификатор.

Предварительно необходимо ввести в домен компьютер по инструкции и убедиться, что доменный пользователь получает билет **Kerberos**.

Chromium

Создайте папку, выполнив в консоли команду от пользователя **root**:

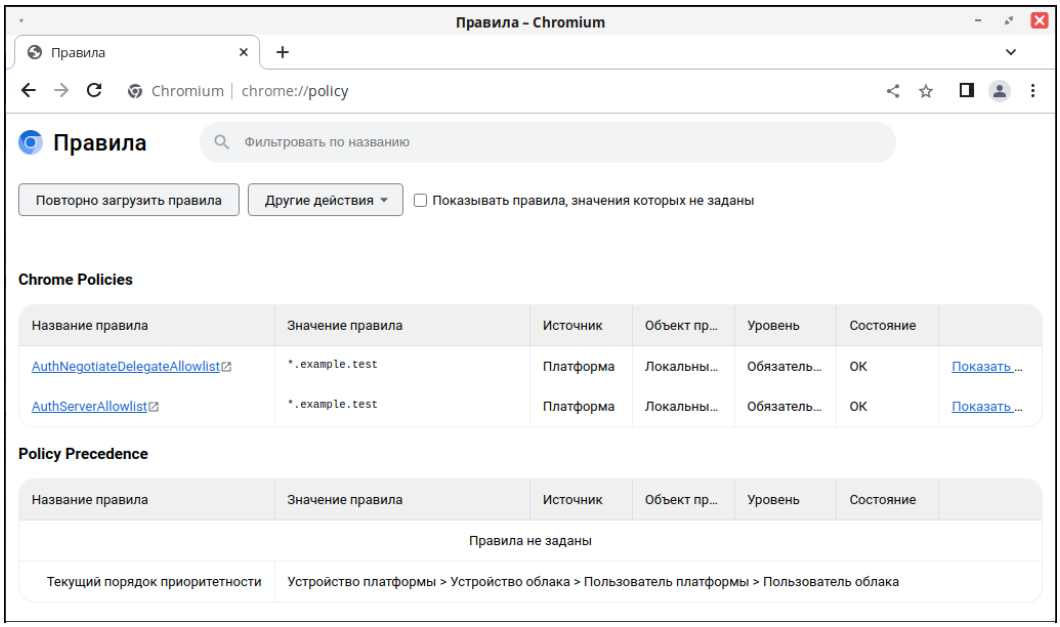
```
mkdir -p /etc/chromium/policies/managed/
```

В ней создайте файл **mydomain.json** следующего содержания:

```
{
 "AuthServerAllowlist": "*.example.test",
 "AuthNegotiateDelegateAllowlist": "*.example.test"
 }
```

где ***.example.test** - имя вашей kerberos-области (**realm**).

После сохранения файла созданные политики будут отображаться в браузере по адресу `chrome://policy`.



Яндекс

Создайте папку, выполнив в консоли команду от пользователя **root**:

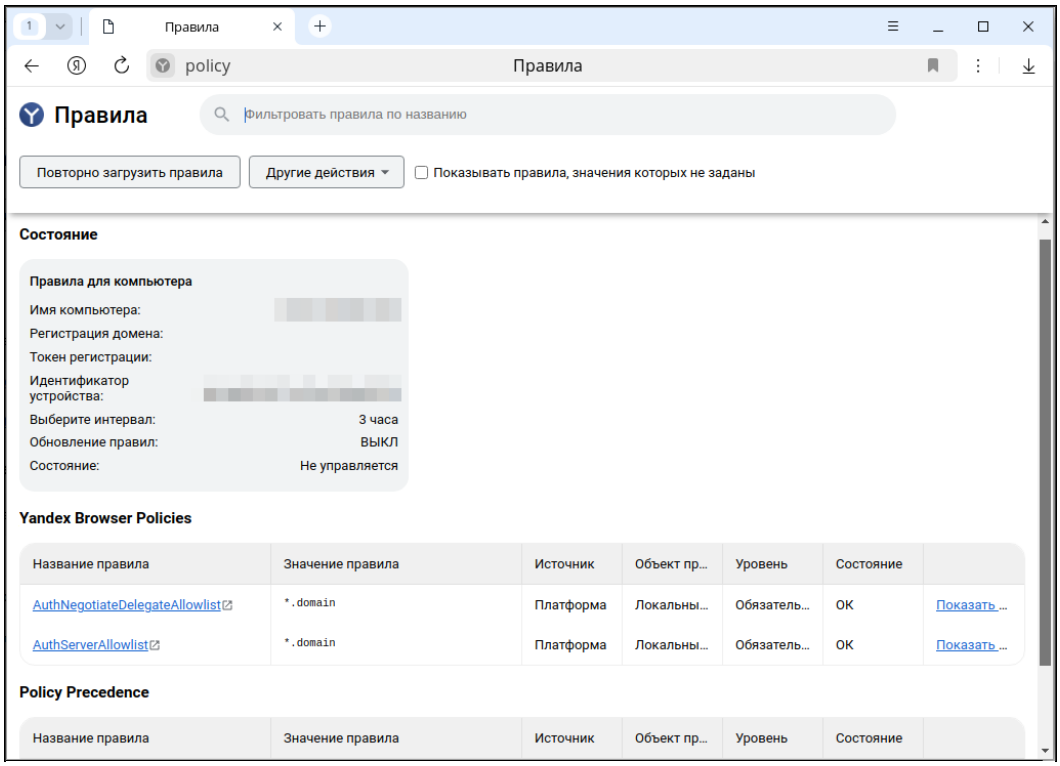
```
mkdir -p /etc/opt/yandex/browser/policies/managed/
```

В папке **managed** создайте файл **mydomain.json** и добавьте в него код:

```
{
 "AuthServerAllowlist": "*.domain",
 "AuthNegotiateDelegateAllowlist": "*.domain"
 }
```

где ***.domain** — имя Kerberos-области (**realm**).

После сохранения файла созданные политики будут отображаться в браузере по адресу browser://policy/.



Mozilla Firefox

В адресной строке введите **about:config**, затем необходимо согласиться с тем, что вы понимаете риски.

В строке поиска найдите параметры:

```
network.negotiate-auth.trusted-uris,
network.automatic-ntlm-auth.trusted-uris,
network.negotiate-auth.delegation-uris
```

и укажите в этих параметрах имя вашей kerberos-области (**realm**):

```
.example.test
```

Теперь вы можете успешно войти на сайт, поддерживающий SSO, под доменным пользователем.

SSO для нескольких доменов

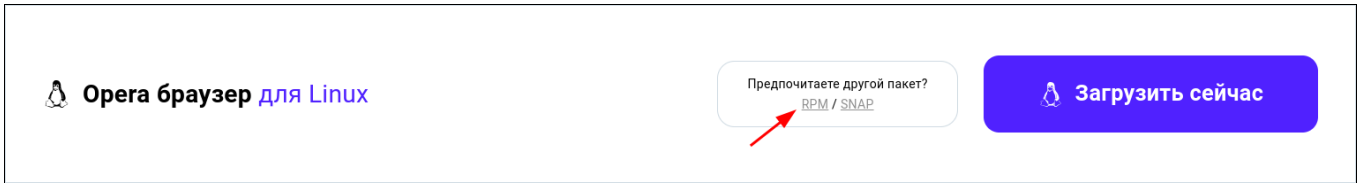
Для включения технологии единого входа *для нескольких доменов* синтаксис файла **.json** должен быть иметь следующий вид:

```
{
"AuthNegotiateDelegateAllowlist": "domain1.example.com,domain2.example.com"
"AuthServerAllowlist": "URL1,URL2"
}
```

Opera

Для установки браузера **Opera** перейдите на официальный сайт разработчика.

Перейдите к разделу «**Загрузить все браузеры Opera**» и раскройте список доступных пакетов для нужного браузера. Рядом с «**Opera браузер для Linux**» нажмите на **RPM**. Начнется загрузка RPM-пакета браузера.



После загрузки перейдите в каталог, куда был скачан пакет (в примере **/home/user/Загрузки/**), кликните ПКМ по файлу и в появившемся контекстном меню выберите «**Открыть в Средство установки пакетов dnfdragora**». Введите пароль *администратора* системы для начала установки пакета.

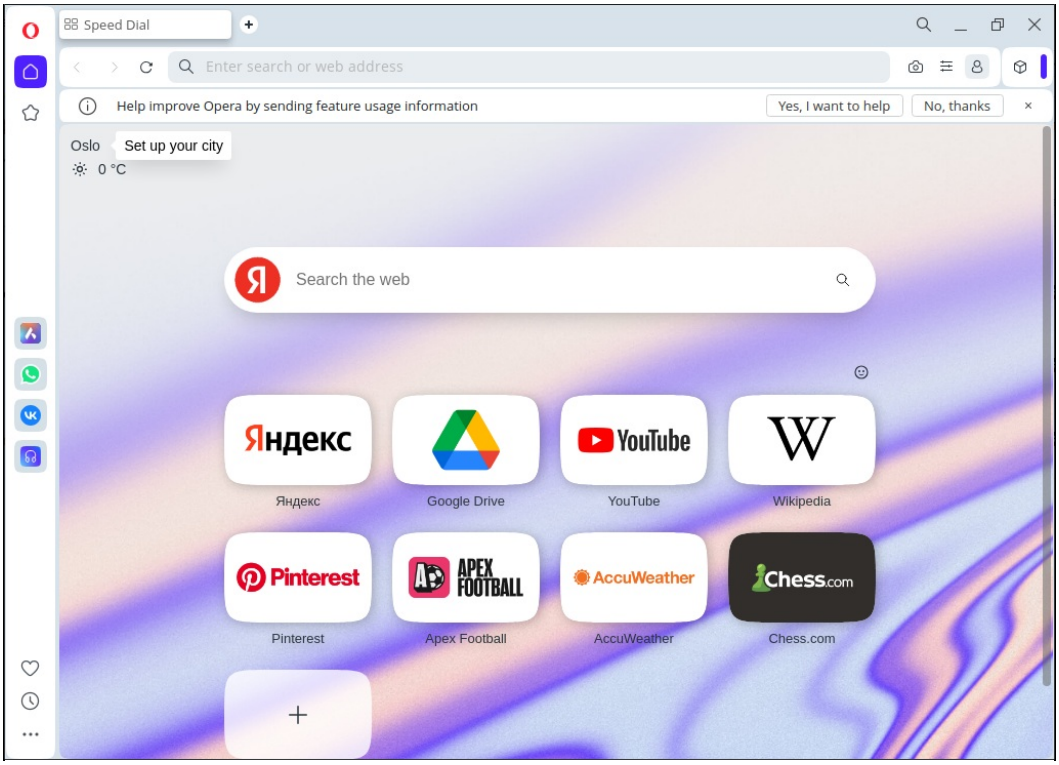
Установку также можно выполнить через терминал (потребуются права *администратора* системы). Перейдите в каталог со скачанным пакетом:

```
cd /home/user/Загрузки/
```

выполните установку:

```
sudo dnf install ./opera-stable_109.0.5097.35_amd64.rpm
```

После установки браузер будет доступен из «**Главного меню**» - «**Интернет**» - «**Opera**».



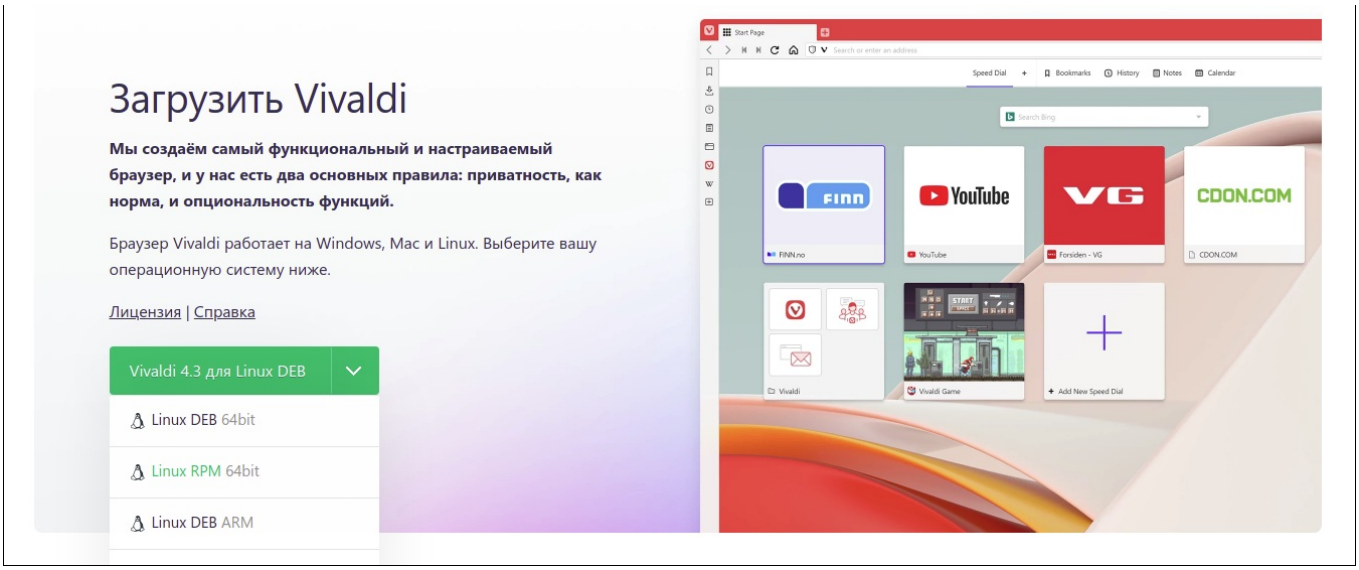
Vivaldi

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Vivaldi - 5.4.2753

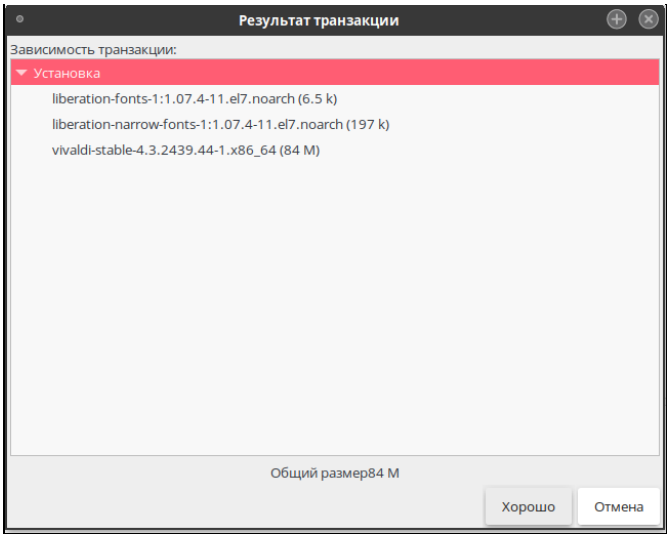
Vivaldi — интернет-браузер, созданный компанией **Vivaldi Technologies** на основе движка **Blink**. Первая тестовая версия стала доступна 27 января 2015 года.

Для загрузки данного браузера необходимо перейти на сайт разработчика и скачать файл «**Linux RPM 64bit**».



После завершения загрузки необходимо перейти в папку, куда был загружен RPM-пакет, и запустить установку двойным нажатием на него.

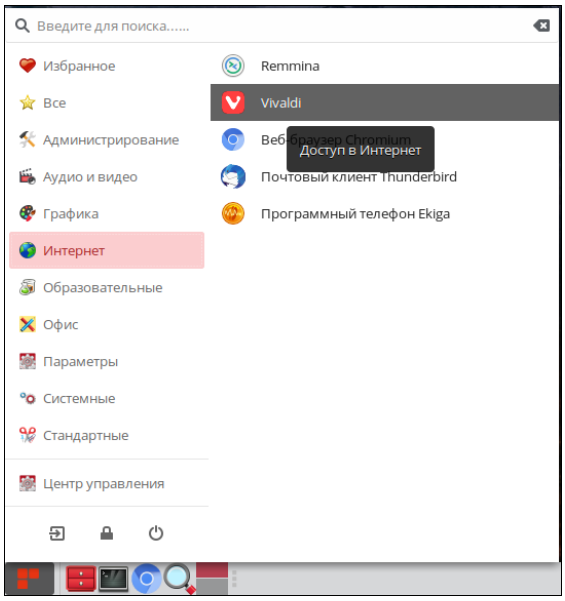
В результате откроется диалоговое окно:



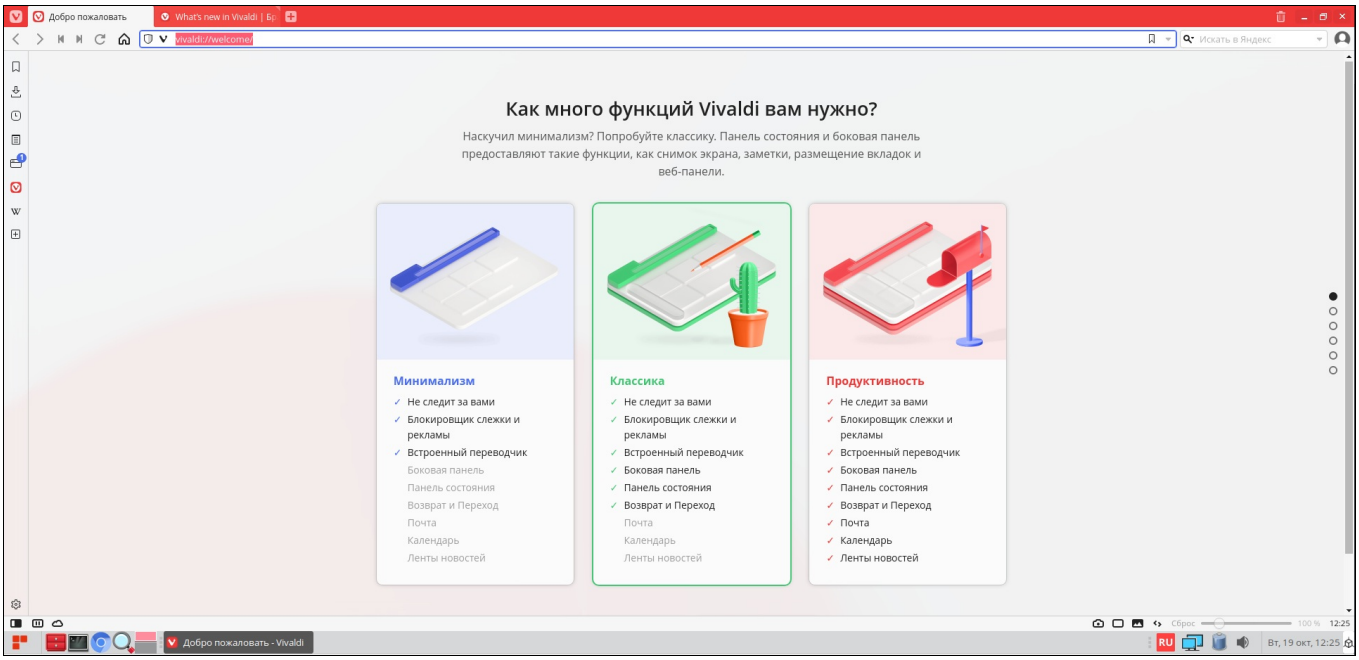
Для установки браузера из консоли потребуется открыть терминал в той директории, куда был скачан RPM-пакет, и выполнить команду:

```
sudo -E dnf install ./vivaldi-stable-5.4.2753.51-1.x86_64.rpm
```

По завершении установки браузер станет доступен из «**Меню**» - «**Интернет**».



При первом запуске **Vivaldi** предоставит возможность выбора режима функциональности для дальнейшей работы, после этого можно будет приступить непосредственно к работе с браузером.



Сбор и просмотр диагностической информации браузеров

[Сбор информации в браузерах на основе Chrome](#)
[Просмотр лога NetExport с помощью Net Log Viewer](#)

Окружение

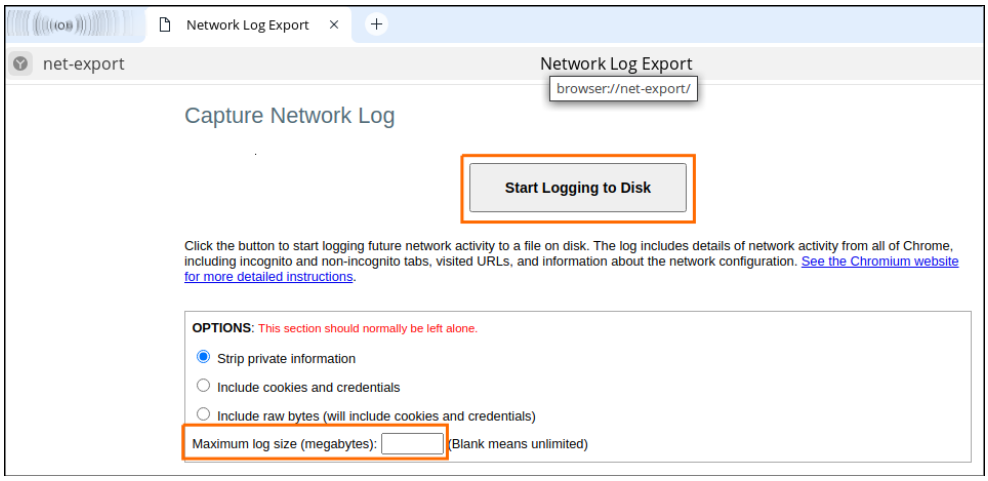
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Сбор информации в браузерах на основе Chrome

При возникновении проблем подключения, отображения информации, производительности может потребоваться анализ логов, полученных посредством встроенного в браузер инструмента **NetLog**. **NetLog** позволяет собирать следующие данные:

- попытки **TCP**-соединений к **IP**-адресам;
- эффективные (применённые) настройки прокси;
- изменение настроек прокси в процессе сбора логов;
- события изменения сети;
- задержки при постановке в очередь **DNS**-запросов;
- результаты предварительных **DNS**-запросов;
- попадания в кеш при разрешении **DNS**-запросов;
- информация о чтениях/записях в кеш браузера;
- прочие ошибки.

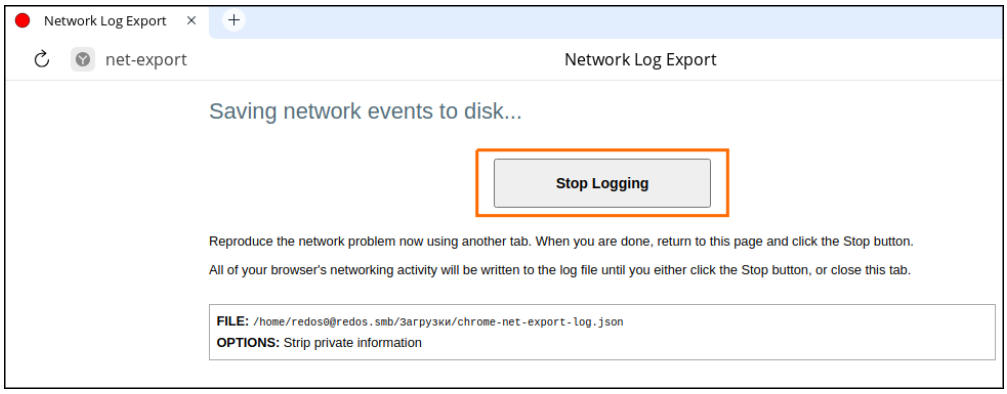
Для запуска сбора логов необходимо открыть браузер, ввести в адресной строке chrome://net-export (для браузера *Яндекс* — browser://net-export) и нажать **Enter**. Откроется страница настройки и запуска сбора информации.



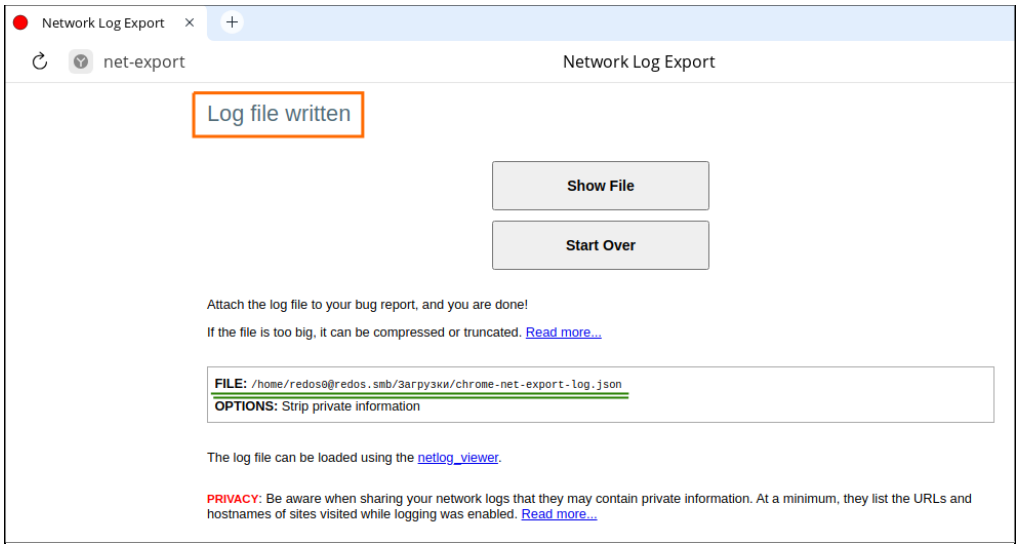
По умолчанию сбор информации не включает приватные данные (*cookies* и данные аутентификации) и не ограничен по размеру. Для ограничения размера файла лога можно указать значение (в мегабайтах) в поле **Maximum log size**. Для начала записи следует нажать кнопку «**Start Logging to Disk**». Появится диалог сохранения файла лога, в котором будет необходимо выбрать его местоположение и имя.

Следующим шагом, не закрывая текущей вкладки «**Network Log Export**», следует воспроизвести действия, при которых проявляется исследуемая проблема.

Затем осуществить переход на вкладку «**Network Log Export**» и нажать кнопку «**Stop Logging**».



Страница обновится и на ней появится надпись «**Log file written**», что свидетельствует об успешной записи файла лога.



Полный путь к сформированному файлу будет отображён в информационном поле **FILE** ниже кнопок **Show File** и **Start Over**.

Просмотр лога NetExport с помощью Net Log Viewer

Инструмент **Net Log Viewer** позволяет просмотреть сохраненный ранее лог в формате удобном для анализа.

1. Установка пакета **git** (потребуются права администратора):

```
sudo dnf install git
```

2. В результате выполнения следующей команды в текущем каталоге будет создан подкаталог catapult, куда будет загружен необходимый набор утилит:

```
git clone https://chromium.googlesource.com/catapult
```

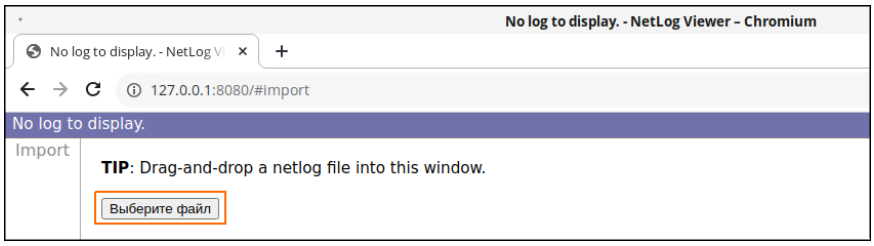
> **Примечание.**
>
> Для размещения набора утилит **Catapult** потребуется около **1 Гб** свободного дискового пространства.

3. Запуск инструмента **Net Log Viewer** производится командой:

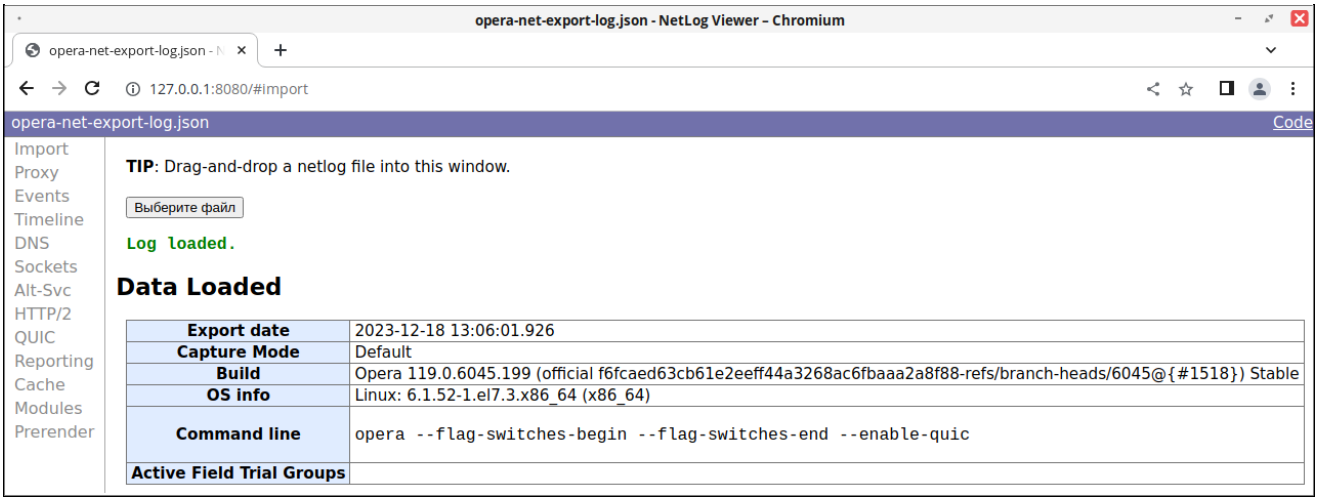
```
./catapult/netlog_viewer/bin/serve_static
```

4. При выполнении команды из п. 3 будет запущен HTTP-сервер, прослушивающий TCP-порт **8080**, к которому следует подключиться для загрузки и обработки лога. **URL** для ввода в адресную строку браузера: http://127.0.0.1:8080 или http://localhost:8080.

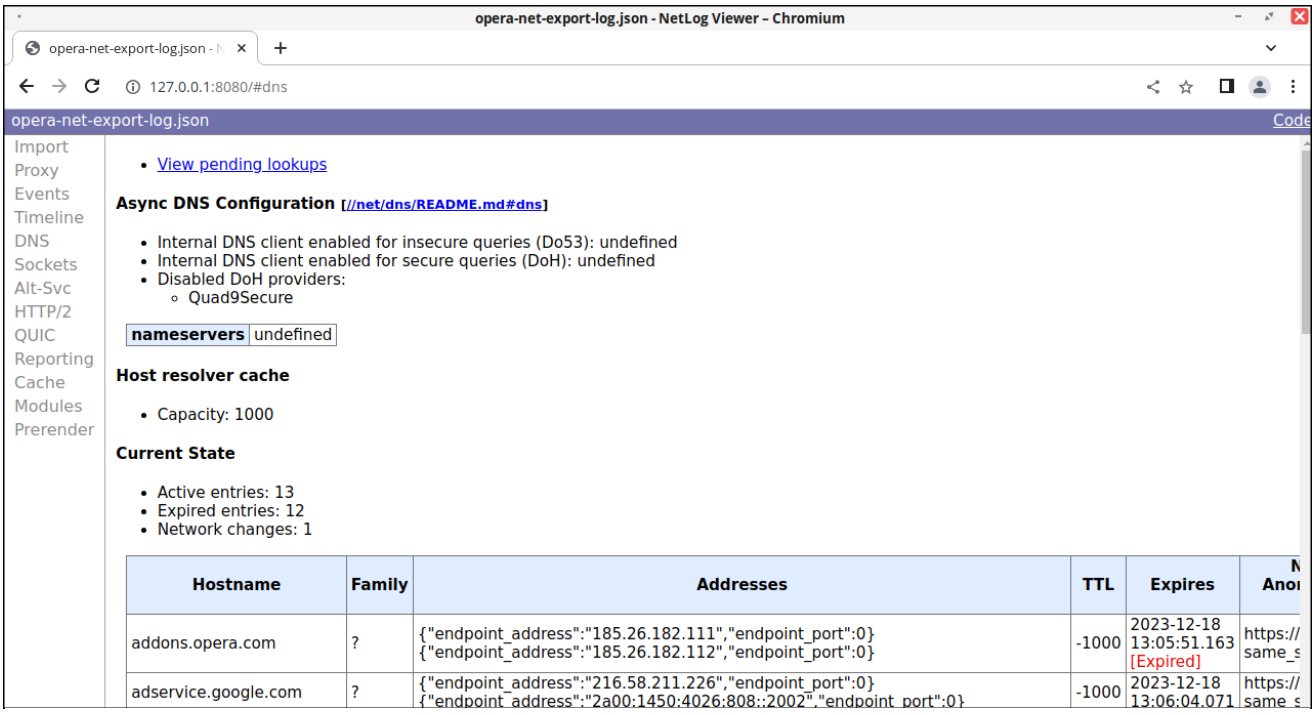
При переходе на указанный выше адрес отобразится страница импорта файла, созданного инструментом **NetLog**. Для выбора файла лога предназначена кнопка «**Выберите файл**».



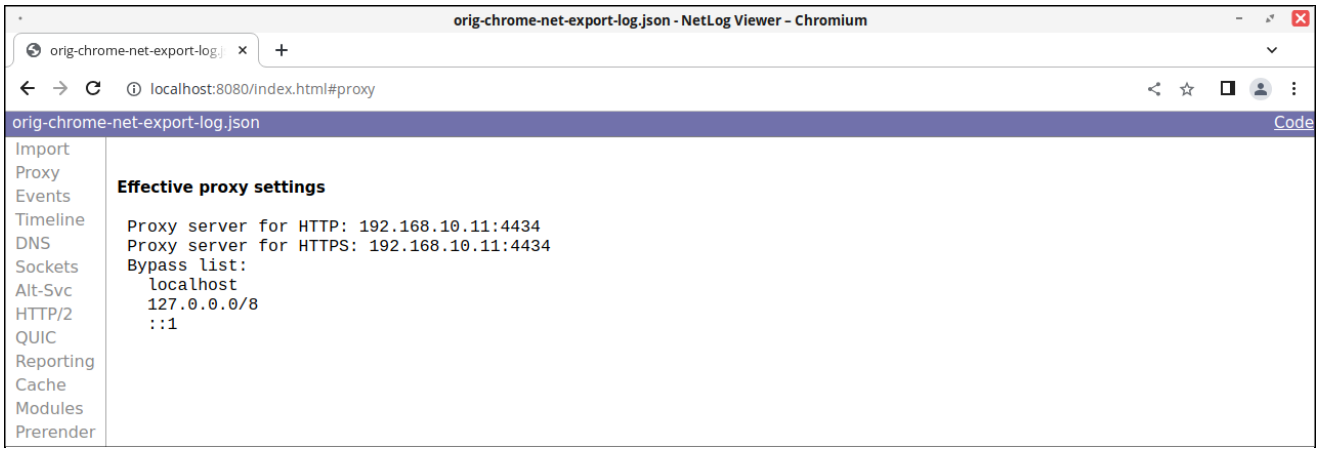
5. После успешной загрузки будет отображена общая информация об условиях сбора лога и запуска браузера. Поле **Command line** может быть полезно для определения параметров, переданных при запуске исполняемого файла, часть которых могла быть скрыта в командной строке посредством применения alias или промежуточного сценария запуска. В правой части страницы будет выведен список, который используется для перехода к различным типам данных.



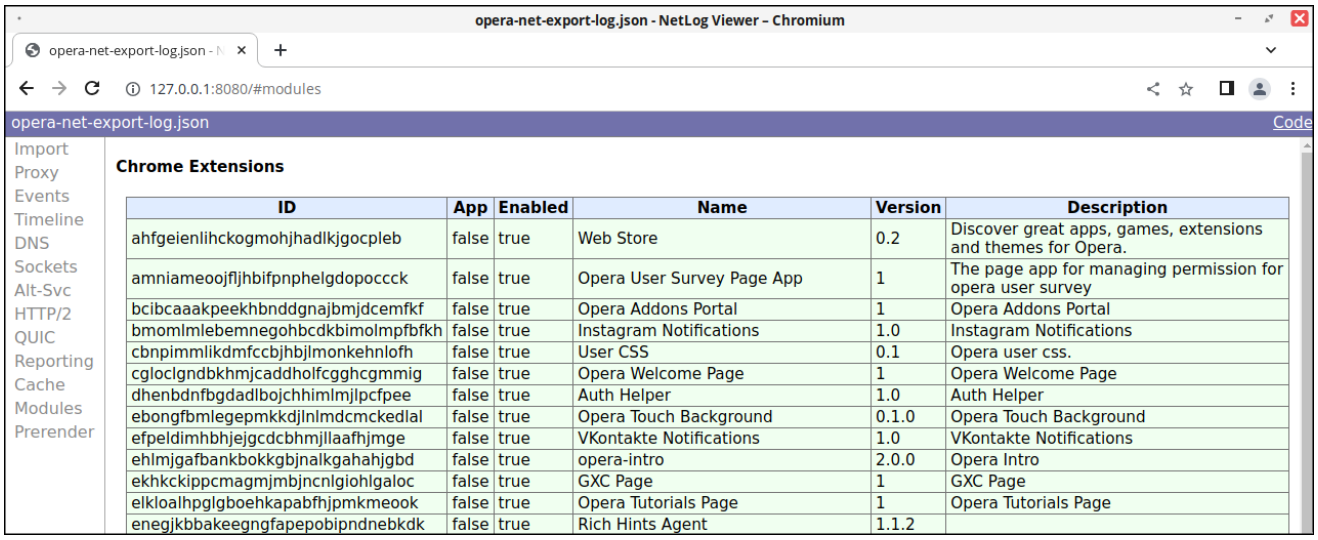
На странице **DNS** отображаются данные конфигурации **DNS**, состояние записей в кеше браузера.



На странице **Proxy** доступна информация об эффективных (действовавших на момент сбора лога) адресах прокси-серверов и адресах исключений. Значения данных параметров могли быть переданы браузеру различными способами (через параметры командной строки, переменные окружения, настройки в графическом режиме, WPAD), поэтому при анализе проблем доступности важно знать эффективные (действующие) значения.



На странице **Modules** в таблице представлена общая информация о загруженных расширениях браузера.



ID	App	Enabled	Name	Version	Description
ahfgeienlihckogmohjhadlkjgocpleb	false	true	Web Store	0.2	Discover great apps, games, extensions and themes for Opera.
amniameoojfljhbifpnphelgdopoccck	false	true	Opera User Survey Page App	1	The page app for managing permission for opera user survey
bcibcaaakpeekhbnddgnajbmjdcemfkf	false	true	Opera Addons Portal	1	Opera Addons Portal
bmomlmlebemnegohbcdkbimolmpfbfkh	false	true	Instagram Notifications	1.0	Instagram Notifications
cbnpimmlikdmfccbjhbjlmonkehnlofh	false	true	User CSS	0.1	Opera user css.
cgloclgndbkhmjcaddholfcgghcgmmig	false	true	Opera Welcome Page	1	Opera Welcome Page
dhenbdnfbgdadlbojchhimlmjlpcfpee	false	true	Auth Helper	1.0	Auth Helper
ebongfbmlegepmkkdjlnlmdcmckedlal	false	true	Opera Touch Background	0.1.0	Opera Touch Background
efpeldimhbhjejgcdcbhmjllaafhjmge	false	true	VKontakte Notifications	1.0	VKontakte Notifications
ehlmjgafbankbokkgbjnalkgahahjgbd	false	true	opera-intro	2.0.0	Opera Intro
ekhkckippcmagmjmbjncnlgiohlgaloc	false	true	GXC Page	1	GXC Page
elkloalhpglgboehkapabfhjpmkmeook	false	true	Opera Tutorials Page	1	Opera Tutorials Page
enegjkbbakeegngfapepobipndnebkdk	false	true	Rich Hints Agent	1.1.2	

Настройка Openfire

Openfire — кроссплатформенный XMPP-сервер, написанный на **Java** и использующий двойное лицензирование под *Apache License 2.0* и коммерческой лицензией.

Большая часть задач администрирования сервера решается через веб-интерфейс под управлением **Jetty** (контейнер сервлетов *javax.servlet*, реализующий спецификацию *Servlets 3.1* и предоставляющий функциональность *J2EE*, http-сервера и http-клиента), доступный на портах **9090** (HTTP) и **9091** (HTTPS) по умолчанию; администраторам доступно редактирование настроек сервера, добавление и удаление пользователей, комнат конференций и так далее.

Установка сервера *Openfire* выполняется командой:

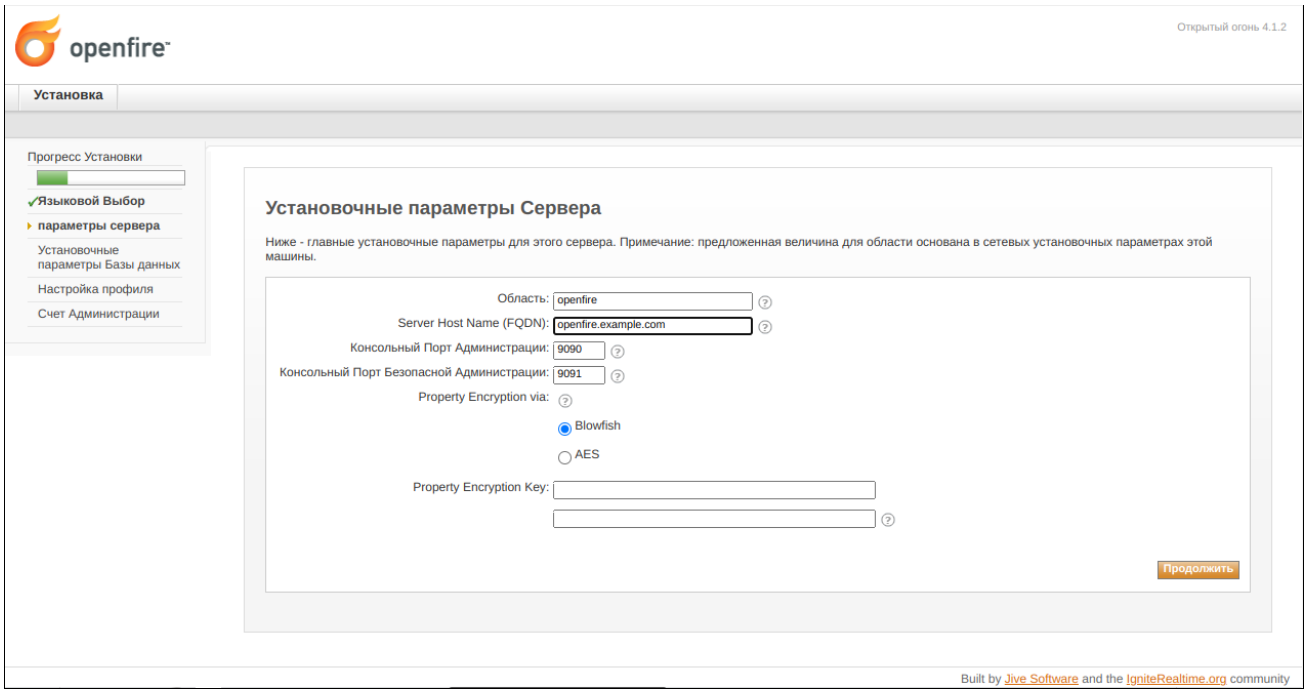
```
dnf install openfire
```

Добавить в автозагрузку и запустить сервер:

```
systemctl enable openfire --now
```

Для дальнейшей настройки Openfire-сервера откройте браузер и перейдите по адресу **http://<IP-адрес сервера>:9090**.

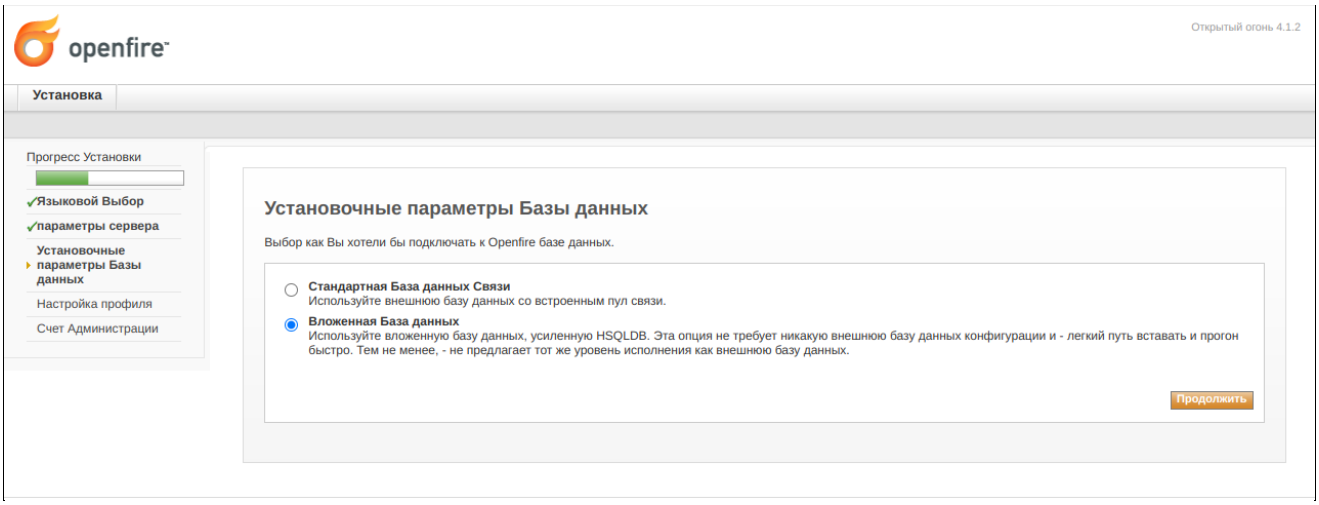
После выбора языка в параметрах сервера нужно заполнить графы «*Область*» и «*Имя хост-сервера (Server Host Name)*». В графе «**Область**» нужно вписать имя сервера, а в «**Server Host Name**» - имя домена.



На следующем шаге необходимо выбрать тип базы данных, которую будет использовать *openfire*.

«*Стандартная База данных Связи*» использует внешнюю базу данных, такие как MySQL, MariaDB и др.

«*Вложенная База данных*» использует встроенную базу данных, которую не нужно настраивать, но предлагающую меньший уровень исполнения, чем внешняя. В нашем примере будем использовать тип «Вложенная База данных».

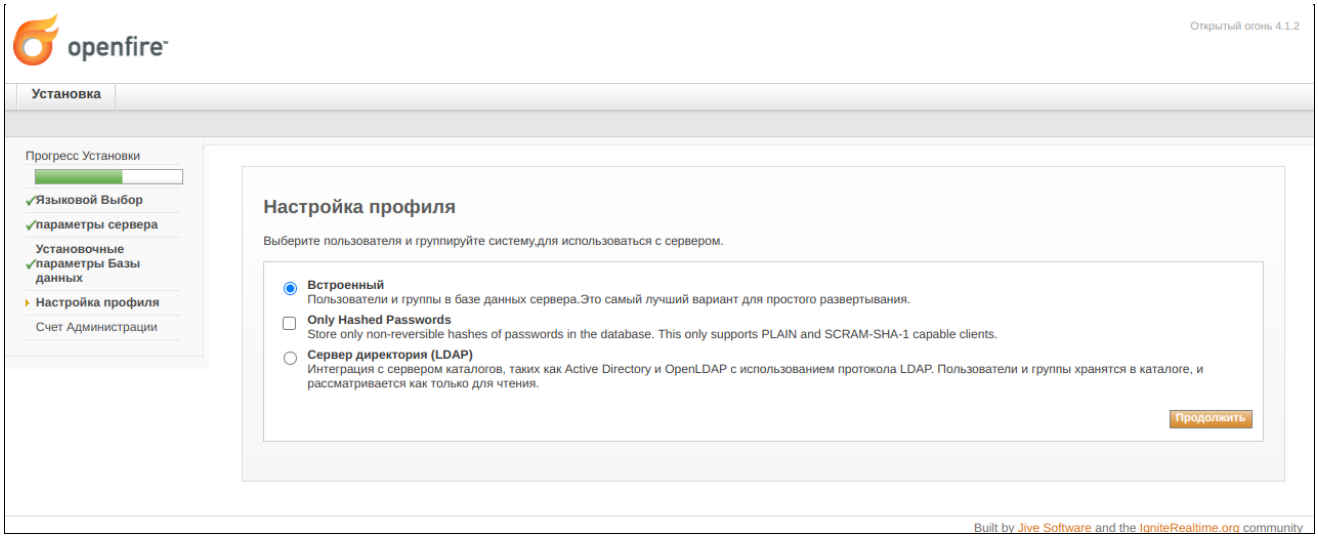


Переходим к настройкам профиля. В настройке профиля выбираем «*Встроенный*».

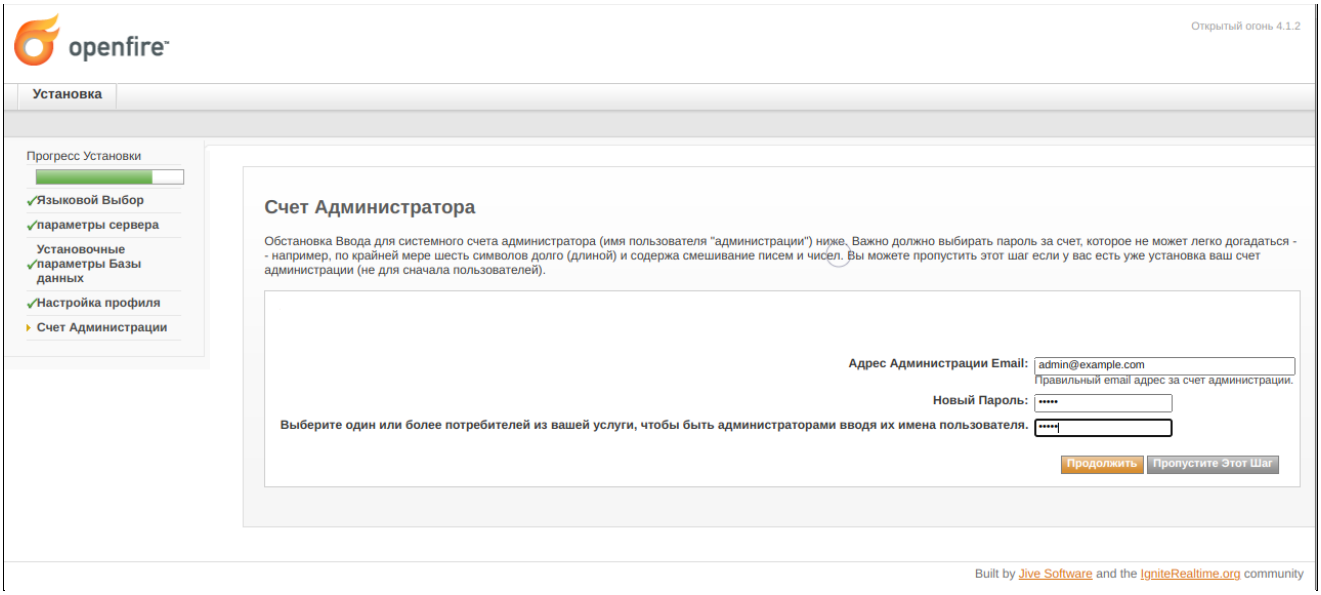
Встроенный профиль – уже настроенный профиль для простого развертывания сервера.

Only Hashed Passwords – используется для хранения в базе данных только необратимых хэш-паролей.

Сервер директория (LDAP) – использование сервера каталогов (Active Directory, LDAP) с использованием протокола **LDAP**. Пользователи и группы хранятся в каталоге и рассматриваются как «только для чтения».



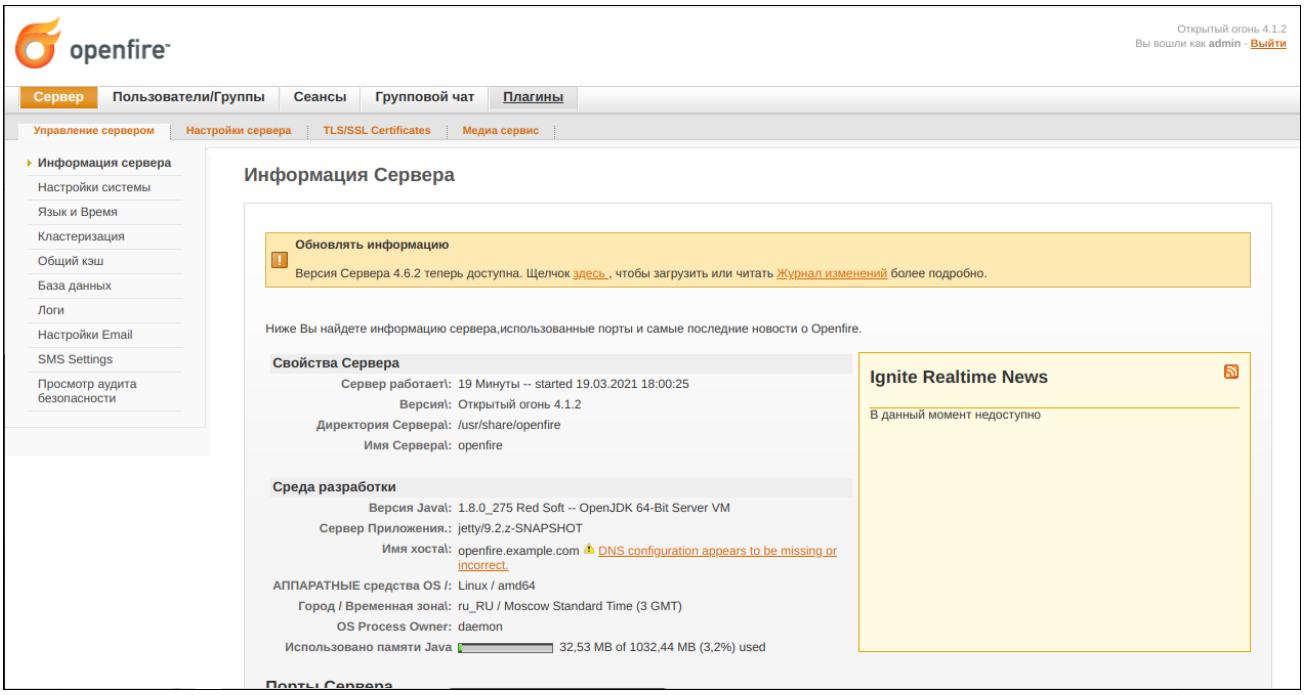
В настройках администратора впишите свой пароль и почту.



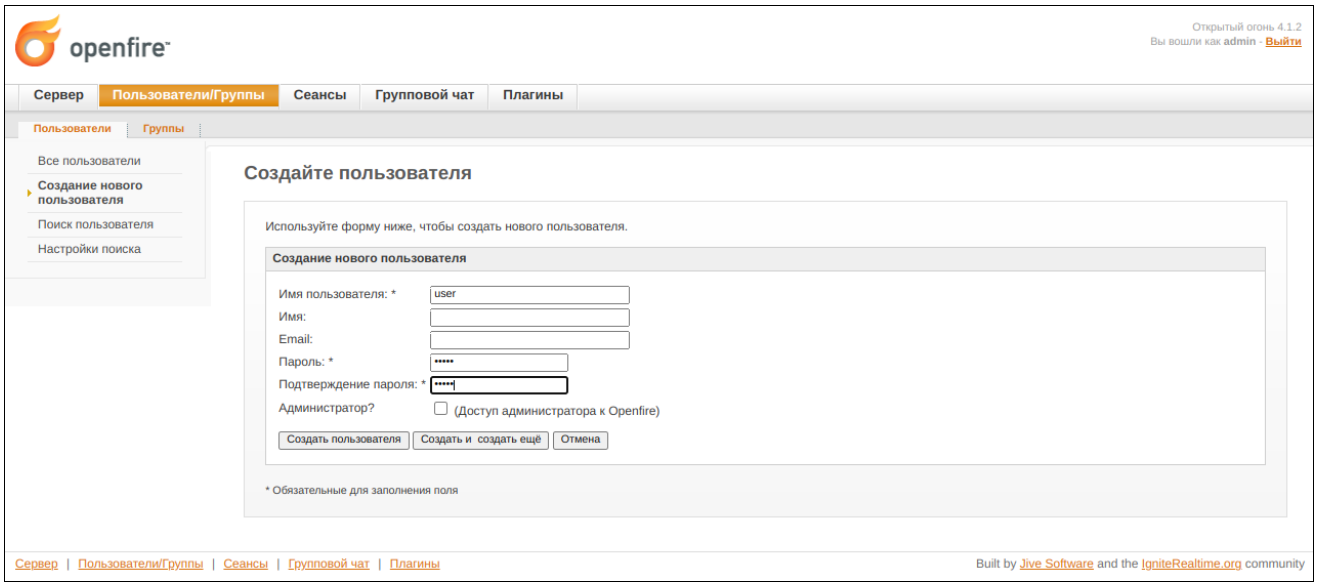
Затем необходимо войти в консоль администрации. Имя пользователя по умолчанию **admin**.

В консоли администратора доступны следующие настройки:

- *Создание кластеризации* – если у вас не встроенная база данных, вы можете с помощью кластеризации соединить несколько Openfire-серверов для более удобной работы. В подвкладке «Настройка сервера» также есть настройка «Сервер-сервер», позволяющая настроить соединение с удаленным сервером.
- *Сообщения оффлайн* – настройка хранения сообщений в автономном режиме, чтобы отправляемые сообщения занимали меньше места на сервере.
- *Хранение закрытых данных* – дает возможность пользователю скрывать свои настройки.
- Во вкладке «*Пользователи/группы*» вы можете создавать пользователей и распределять их по созданным группам (см. создание пользователя ниже).
- Во вкладке «*Сеансы*» вы можете посмотреть сеансы клиента/сервера и компоненты сеансов, а так же настроить их в «*Инструментах*».
- Во вкладке «*Групповой чат*» вы можете создать комнату и общаться с пользователями, а так же настроить сервис.
- Во вкладке «*Плагины*» вы можете установить удобные плагины для работы с Openfire-сервером.



Последний шаг – создание пользователей. Заходим в раздел *«Пользователи/группы»* – *«Создание нового пользователя»*. Вводим имя пользователя, пароль, подтверждение пароля и нажимаем «*Создать пользователя*».



Настройка SSO openfire

Настройка сервера jabber/xmpp с базой данных единого входа SSO на FreeIPA.

Требования

- Нужен рабочий домен ipa.

В примере домен IPA - IPA.EXAMPLE.COM. Сервер, содержащий каталог kercos kdc, ldap и DNS-сервер, - ipa.example.com.

- сервер, подключенный к домену IPA, где мы установим программное обеспечение jabber/xmpp.

В данном случае сервер openfire.example.com.

Установка

Установите его от пользователя root:

```
[root@openfire ~] dnf install openfire
```

Конфигурирование

Переведите selinux в режим disabled.

На время настройки сервиса переведите selinux в режим disabled. Для этого измените содержимое конфигурационного файла:

```
nano /etc/selinux/config
```

Заменив текст SELINUX=enforcing на SELINUX=disabled

Более подробно см.ссылку
Не забудьте включить selinux после завершения настройки.

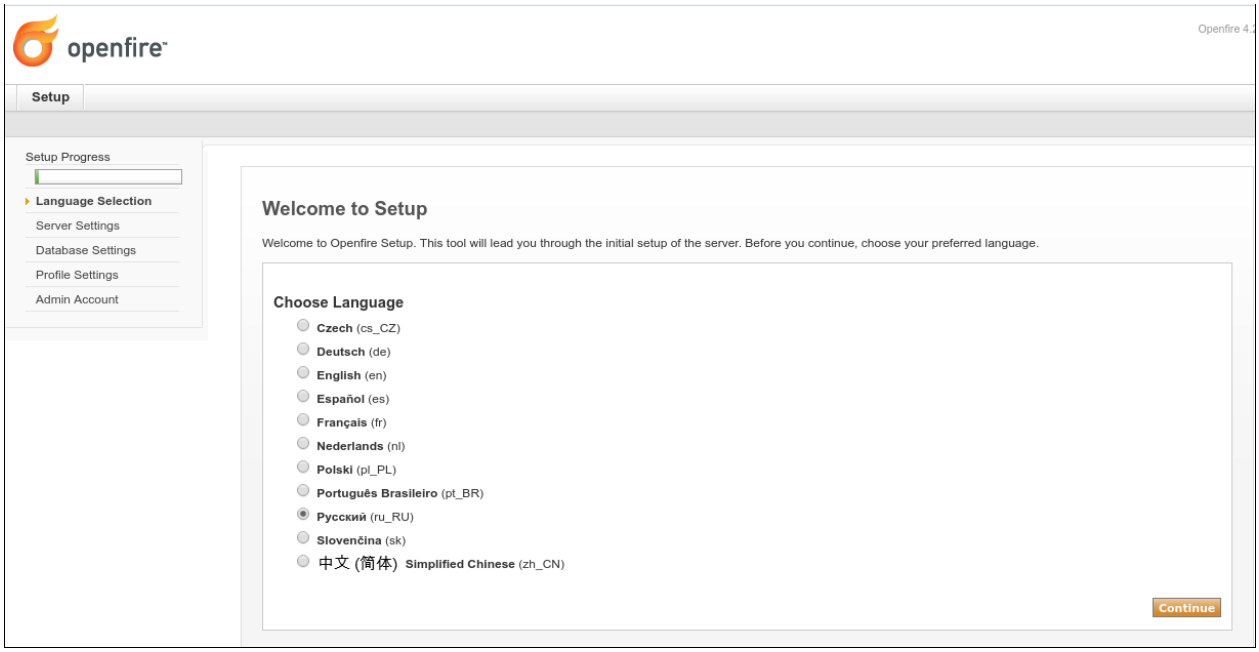
Openfire имеет приятный веб-интерфейс для настройки чат-сервера. Чтобы получить доступ к нему, нам нужно сначала запустить демон openfire:

Запуск демона

```
[root@openfire ~] systemctl start openfire
[root@openfire ~] # systemctl enable openfire
```

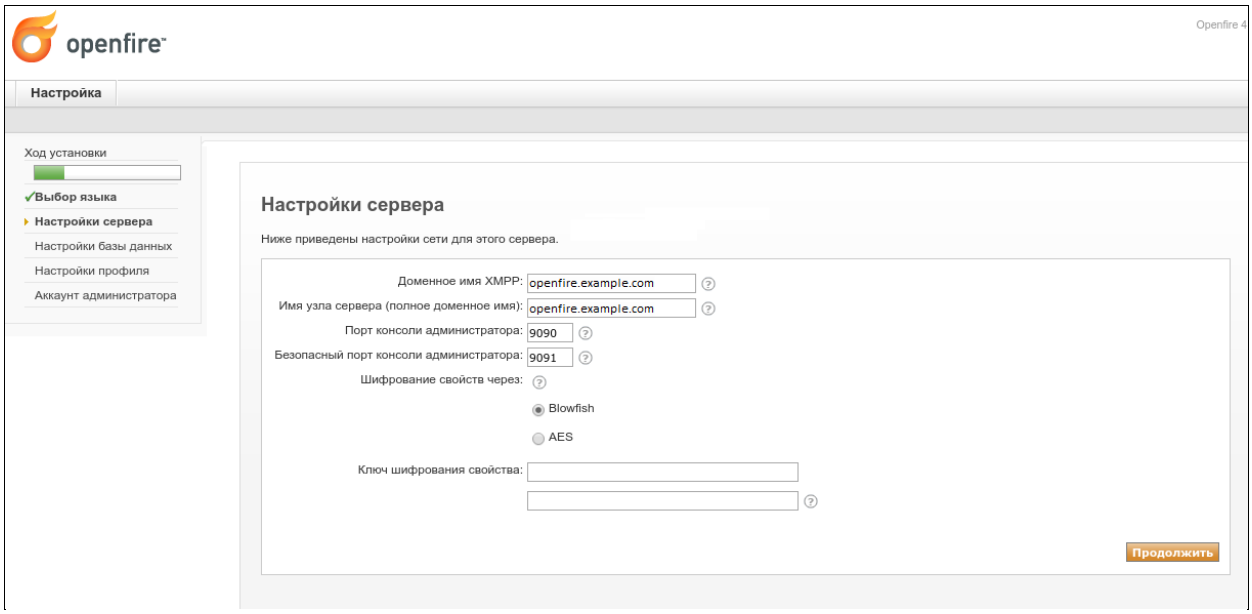
Настройка из веб-интерфейса

Веб-интерфейс доступен по адресу localhost:9090

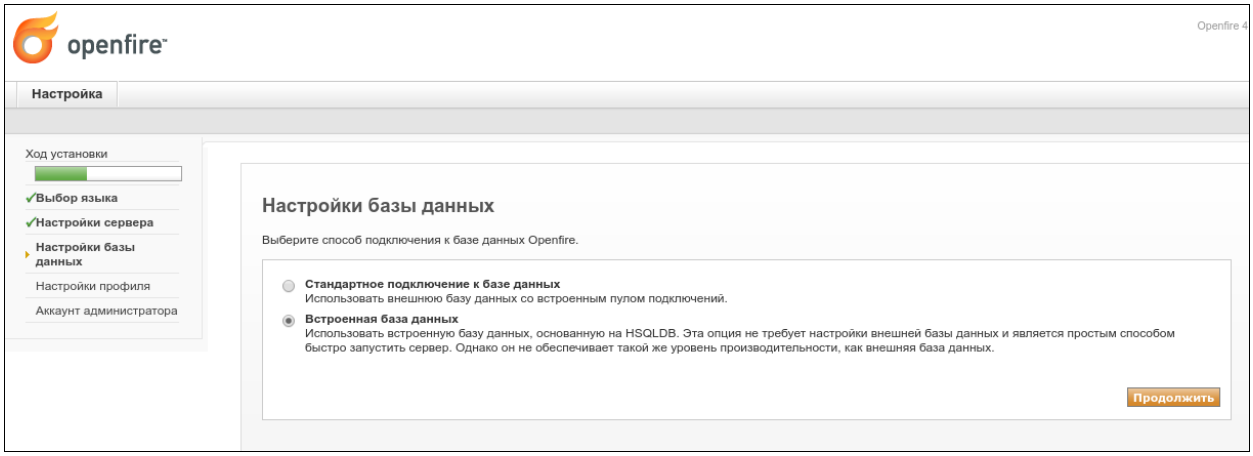


Выберите русский язык и нажмите кнопку «Continue»;

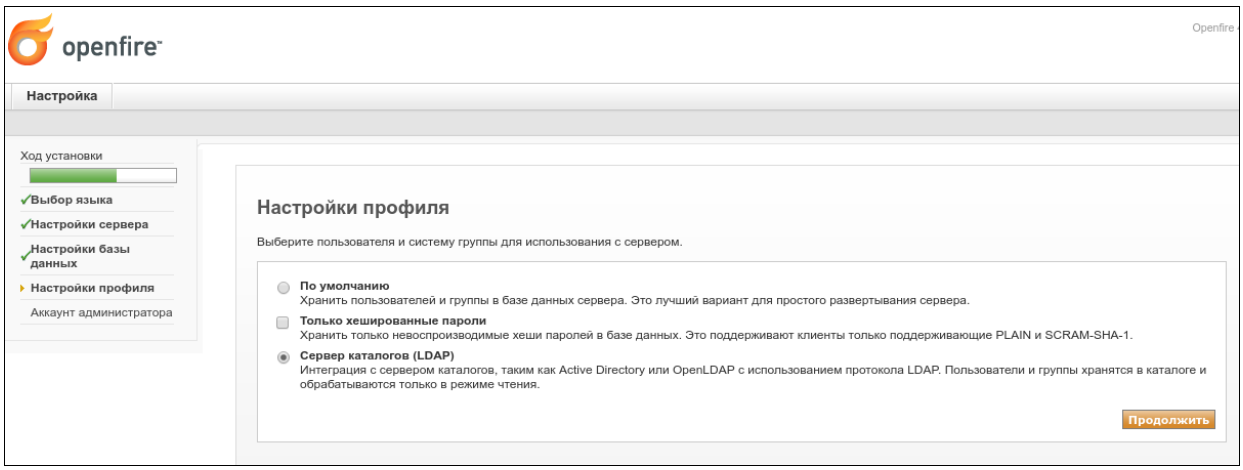
В поле «Доменное имя XMPP» введите fqdn чат-сервера: openfire.example.com. Другие настройки можно оставить без изменений, затем нажмите «Продолжить»;



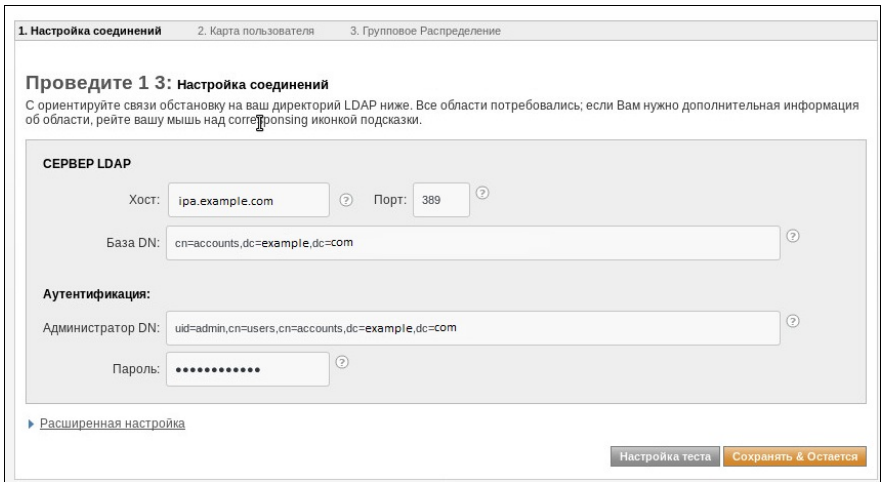
Подключите стороннюю базу данных или используйте встроенную базу данных. Нажмите «Продолжить»;



Выберите «Сервер каталогов (LDAP)» и нажмите «Продолжить»;



Далее заполните fqdn ldap-сервера, в нашем случае:.ipa.example.com. Оставьте стандартный порт ldap (389) и в качестве базы ldap выберите cn= accounts,dc =example,dc = com. Введите администратора DN, в данном случае uid=admin,cn=users,cn=accounts,dc=example,dc=com как на скриншоте.



Оставьте поля аутентификации пустыми (если вы не изменили стандартную установку ipa, ipa разрешает анонимные привязки ldap, если вы отключили это, тогда вам нужно будет ввести имя пользователя / пароль для привязки к серверу ldap) и нажать «Тест», вы должны увидеть сообщение об успешном завершении.

Следующий экран (Настройки профиля: User Mapping) можете ничего не изменять. Просто убедитесь, что в поле «имя пользователя» стоит значение «uid» и нажмите «Продолжить». Вы также можете нажать «Настройки теста», и вы должны увидеть некоторую информацию о своих пользователях ipa, поскольку openfire сопоставляет их с собственной базой данных.

Следующий экран - Настройки профиля: Групповое сопоставление. Откройте «дополнительные настройки» и заполните там "(cn = ipausers)". Этот фильтр получит все члены группы ldap «ipausers» (которая является стандартной группой для каждого пользователя). Его можно использовать, чтобы автоматически добавлять эту группу в адресную книгу каждому клиенту.

Можно использовать фильтр ldap для получения нескольких групп. Если у нас есть 2 группы, ipausers и yurist, мы можем использовать этот фильтр для создания двух групп openfire:

```
(|(cn=ipausers)(cn=yurist))
```

Вы можете отредактировать ldap-фильтр после настройки на веб-интерфейсе (вкладка свойств сервера).

Последним шагом в настройке является учетная запись администратора, введите «admin», и подтвердите. После этого вы можете войти в консоль администратора openfire. Введите имя пользователя и пароль администратора.

Если теперь вы нажмете «Пользователи/Группы», вы увидите своих пользователей ipa на сервере openfire.

Конфигурация SSO

dns autodiscovery

Клиенты xmpp/jabber могут использовать записи dns srv для поиска серверов. Это очень полезно. Мы добавим следующую запись srv в нашу dns зону ipa.example.com:

```
_xmpp-client._tcp 0 100 5222 openfire
```

где _xmpp-client._tcp - это запись, 0 - приоритет, 100 - вес, 5222 - это порт tcp, а openfire – сервер. У вас должна существовать A запись сервера openfire.

Проверьте запись:

```
$ host -t srv _xmpp-client._tcp.example.com
_xmpp-client._tcp.example.com имеет запись SRV 0 100 5222 openfire.example.com.
```

Теперь мы можем подключиться к pidgin только с доменом example.com вместо openfire.example.com, автообнаружение dns автоматически обнаружит сервер.

Создать основную цель службы xmpp

Нам нужно создать основную службу обслуживания kerberos и подключить ее к чат-серверу openfire.example.com. Используйте веб-интерфейс ipa или консоль (у вас должен быть действительный билет администратора kerberos):

```
kinit admin
ipa service-add xmpp/openfire.example.com
```

Проверьте созданную службу:

```
admin@openfire ~] $ipa service-find openfire.example.com
------------------
2 services matched
------------------
  Principal: postgres/openfire.example.com@EXAMPLE.COM
  Keytab: True
  Managed by: openfire.example.com
  Principal: xmpp/ openfire.example.com@ EXAMPLE.COM
  Keytab: True
  Managed by: openfire.example.com
----------------------------
Number of entries returned 2
```

Как вы видите, у этого хоста есть два принципиала: обслуживания и xmpp.

Получите keytab для принципиала службы xmpp

Выполните на сервере openfire команду

```
ipa-getkeytab -s ipa.example.com -p xmpp/openfire.example.com -k openfire.keytab -e des3-hmac-sha1
```

Здесь мы выгружаем keytab для xmpp/openfire.example.com в файл openfire.keytab с правильным шифрованием.

```
[admin@openfire ~] $klist -k -t openfire.keytab
Имя ключевого слова: WRFILE: openfire.keytab
Главный администратор KVNO
---- ----------------- ---------------------------- --------------------------
   3 06/15/12 18:29:53 xmpp/openfire.example.com@EXAMPLE.COM
```

Поместите openfire.keytab в /usr/share/openfire/conf/, сделайте его читаемым только для пользователя - daemon (openfire работает как пользовательский демон).

```
[admin@openfire ~] $ cp /root/openfire.keytab /usr/share/openfire/conf/
[admin@openfire ~] $ chown daemon:daemon /usr/share/openfire/conf/openfire.keytab
```

Проверьте keytab:

```
# kinit -k -t openfire.keytab xmpp/openfire.example.com
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: xmpp/openfire.example.com@EXAMPLE.COM

Valid starting     Expires            Service principal
06/16/12 23:28:35  06/17/12 23:28:35  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

gss.conf

создайте файл gss.conf в /opt/openfire/conf с похожим контентом:

```
com.sun.security.jgss.accept {
   com.sun.security.auth.module.Krb5LoginModule
   required
   storeKey=true
   keyTab="/usr/share/openfire/conf/openfire.keytab"
   doNotPrompt=true
   useKeyTab=true
   realm="EXAMPLE.COM"
   principal="xmpp/openfire.example.com@EXAMPLE.COM"
   debug=true
   isInitiator=false;
};
```

openfire.xml

последний шаг - отредактировать /usr/share/openfire/conf/openfire.xml и добавить блок gssapi/sasl. Добавьте его в конец файла перед тегами <setup>true</setup></jive>

```
  <sasl>
     <mechs>GSSAPI</mechs>
```

```
    <realm>EXAMPLE.COM</realm>
    <gssapi>
      <debug>true</debug>
      <config>/usr/share/openfire/conf/gss.conf</config>
      <useSubjectCredsOnly>false</useSubjectCredsOnly>
    </gssapi>
  </sasl>
```

Перезапустите демон openfire

```
# systemctl restart openfire
```

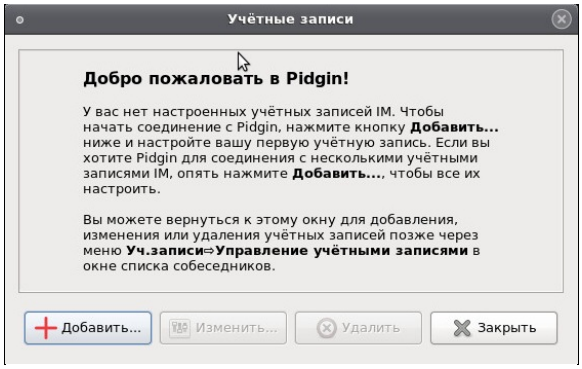
Стоит отметить, что в файле openfire.xml, по-видимому, не хватает информации, которую мы только что добавили после перезагрузки демона. Информация была добавлена в базу данных, но она исчезла из XML-файла. На веб-интерфейсе сервера openfire на вкладке настроек сервера будут установлены настройки.

Логин с SSO

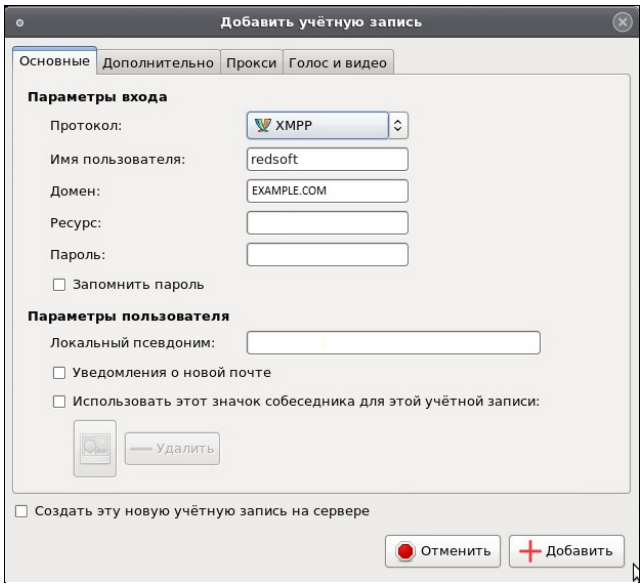
На рабочей станции введенной в домен установите пакет krb5-workstation и pidgin:

```
# dnf –y install krb5-workstation pidgin
```

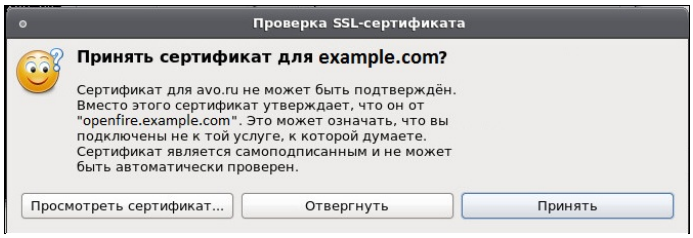
Запустите pidgin (приложения -> интернет ->Клиент обмена мгновенными сообщениями Pidgin);



Добавьте учетную запись xmpp: в закладке «Имя пользователя» введите имя пользователя с именем пользователя ipa, которое вы хотите протестировать, в поле домена заполните имя домена (EXAMPLE.COM); на вкладке «Дополнительно» должен быть заполнен только «порт подключения» (5222), а «Безопасность подключения» должна «требовать шифрования». Вот и все, нажмите «Сохранить», и вам будет предложено принять сертификат с сервера.



Примите SSL-сертификат

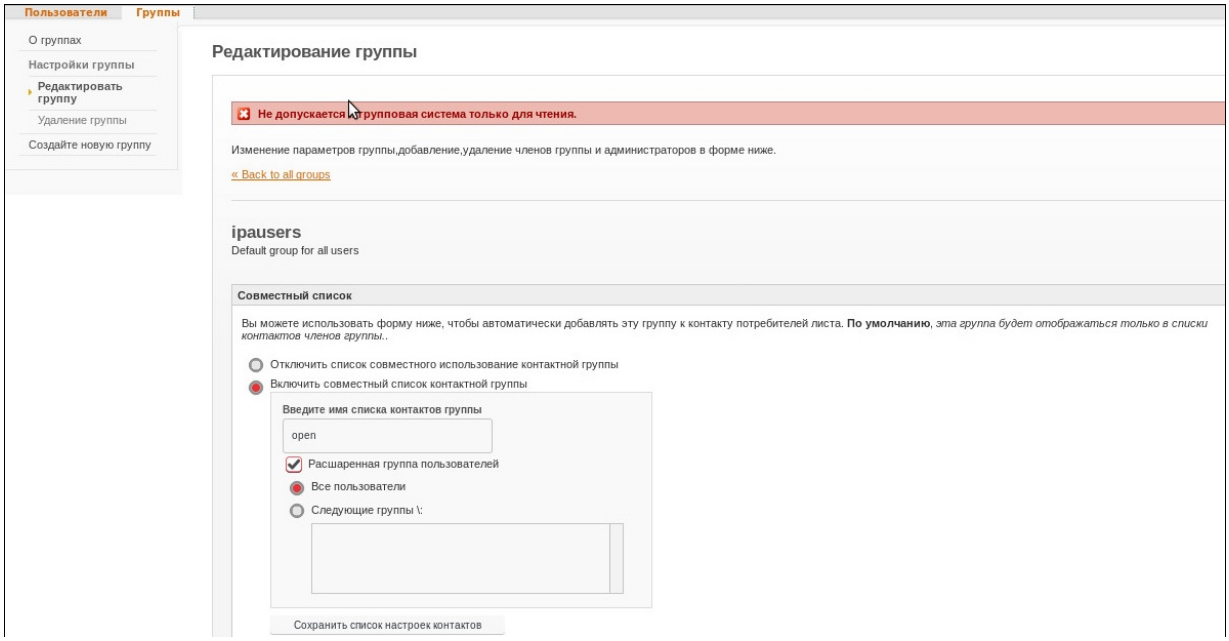


Проверьте получение дополнительного билета kerberos с сервере xmpp:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_500
Default principal: ipauser1@IPA.ASENJO.NX

Valid starting     Expires            Service principal
06/16/12 23:29:03  06/17/12 23:29:00  krbtgt/EXAMPLE.COM@EXAMPLE.COM
    renew until 06/23/12 23:29:00
06/16/12 23:29:09  06/17/12 23:29:00  xmpp/openfire.example.com@EXAMPLE.COM
    renew until 06/23/12 23:29:00
```

Для того, что бы у клиентов появился список пользователей, настройте это на openfire сервере.

Перейдите на вкладку Пользователи и группы, Группы. Нажмите на группу ipausers. Включите совместный список контактной группы и введите её название. Выберите «Разрешенная группа пользователей» и «Все пользователи».



Нажмите на кнопку «Сохранить список настроек контактов».

Pidgin

Pidgin - это чат-программа, которая позволяет вам входить в учетные записи в нескольких чат-сетях одновременно. Это означает, что вы можете одновременно общаться с друзьями на XMPP и сидеть в IRC-канале. *Pidgin* работает на *Windows, Linux* и других UNIX-подобных операционных системах.

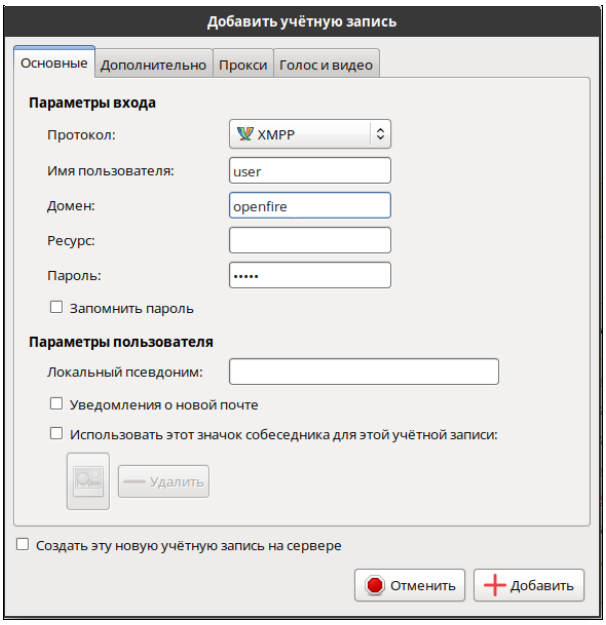
Pidgin поддерживает множество функций этих чат-сетей, такие как передача файлов, удаленные сообщения, значки друзей, пользовательские смайлики и уведомления о вводе текста. Многочисленные плагины также расширяют функциональность Pidgin сверх стандартных функций.

Для установки выполните команду:

```
dnf install pidgin
```

Запуск *pidgin* осуществляется через *«Меню» - «Интернет» - «Клиент обмена мгновенными сообщениями Pidgin»*.

В открывшемся окне нажмите на кнопку «*Добавить*». Далее выберите протокол «*XMPP*» и в полях «*Имя пользователя*» и «*Пароль*» впишите данные одного из созданных на сервере пользователей. В поле «*Домен*» введите имя сервера, тип протокола выберите XMPP.



После создания учетной записи вам необходимо будет принять условия пользовательского соглашения, нажав кнопку «*Принять*». После этого вам будут доступны функции общения. Для создания чата, отправки сообщения и другого функционала нажмите «*Собеседники*».

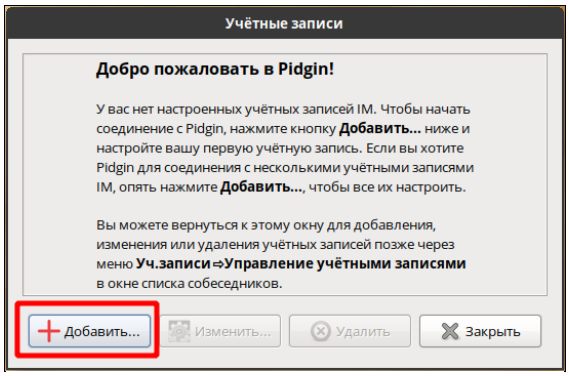
Расширение Pidgin для работы Skype for Business

Skype for business - коммуникационная программа-клиент, позволяющая пользователям общаться друг с другом в реальном времени, используя различные виды коммуникаций: мгновенные сообщения, видео- и голосовую связь, общий доступ к рабочему столу, конференции, передачу файлов. У программы также имеется собственная серверная часть. Тем самым программа является клиентом объединённых коммуникаций и позволяет пользователям общаться и обмениваться информацией.

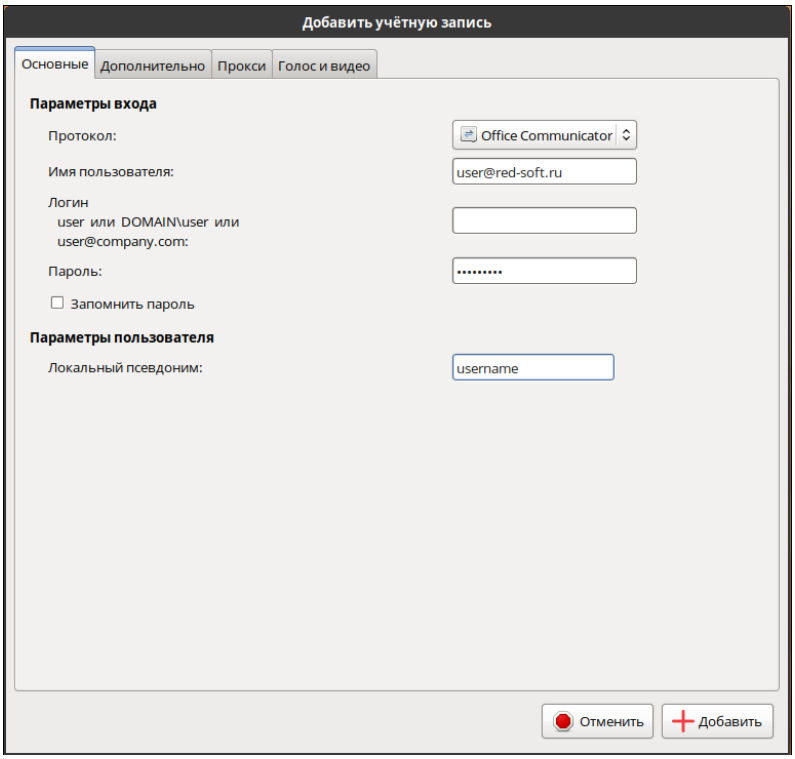
Пакет расширения можно установить следующей командой:

```
dnf install pidgin-sipe purple-sipe
```

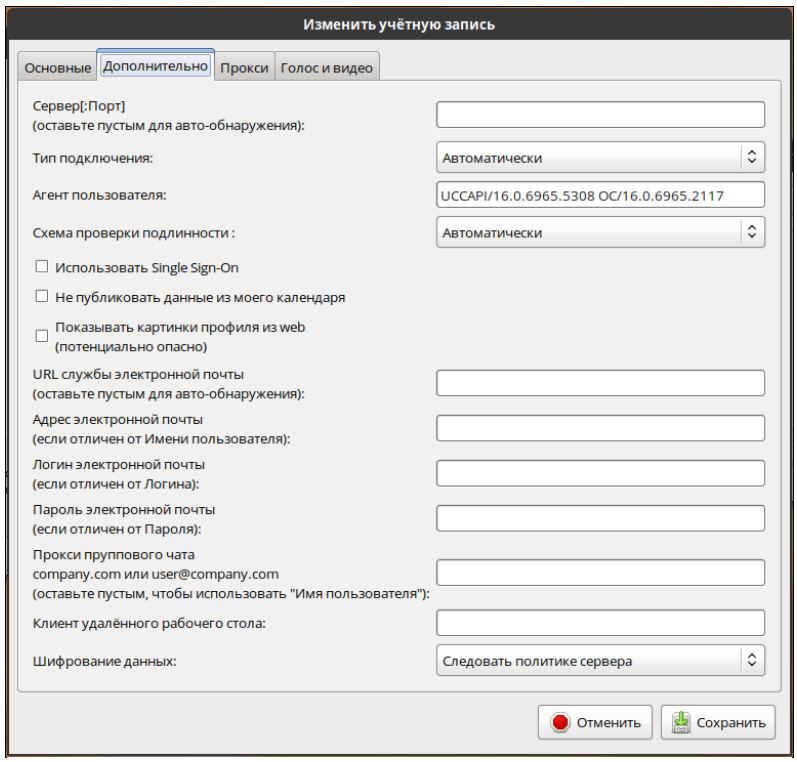
Далее необходимо создать аккаунт при запуске **Pidgin**, для этого нажмите «**Добавить...**».



В открывшемся окне выберите протокол – **Office communicator.**



Далее на вкладке **Дополнительно** пропишите данные вашего **Агента пользователя**, например:



После этого нажмите «**Сохранить**» и проверьте подключение к серверу.

PSI

PSI - это бесплатное приложение для обмена мгновенными сообщениями, предназначенное для сети XMPP. Быстрый и легкий *Psi* полностью открыт и совместим с *Windows, Linux* и *macOS*.

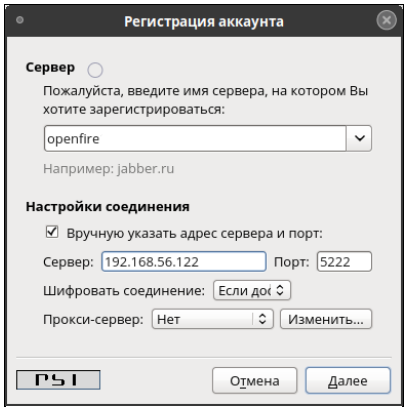
PSI очень удобен, благодаря полной поддержке *Unicode* и локализации, простой передаче файлов, настраиваемым наборам иконок и многим другим полезным функциям.

Для установки выполните команду:

```
dnf install psi
```

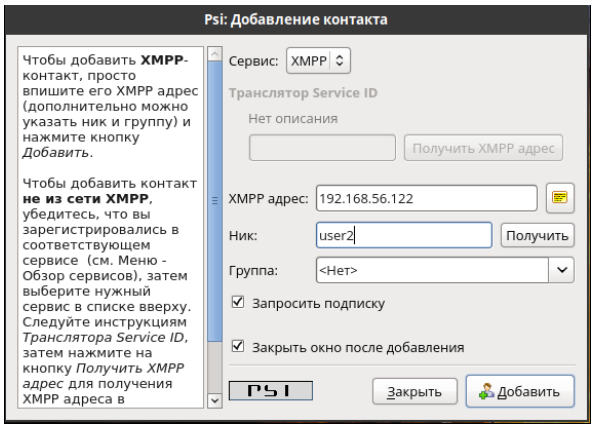
Запуск *psi* осуществляется через *«Меню» - «Интернет» - «Psi»*.

После запуска вам будет предложено создать нового пользователя — для этого введите имя пользователя и нажмите «*Добавить*». После чего откроется окно регистрации аккаунта. В поле «*Сервер*» введите имя сервера, установите галочку в поле «*Вручную указать адрес сервера и порт*», впишите ip-адрес сервера и нажмите «*Далее*».



После этого нажмите кнопку «*Доверять*» и впишите имя нового пользователя, не созданного на сервере, и пароль. Внизу нажмите на кнопку выбора статуса и установите параметр «*Доступен*», после чего учетная запись подключится к серверу.

Для добавления контактов в окне *Psi* в левом нижнем углу нажмите на значок **PSI** и выберите «*Добавить контакт*». В поле «*XMPP-адрес*» вводим ip-адрес сервера, а в графе «*Ник*» – никнейм нужного человека.



В окне *Psi* появится контакт.

Jitsi

Jitsi - это система интернет-телефонии и мгновенного обмена сообщениями, поддерживающая XMPP. Написана на *Java*.

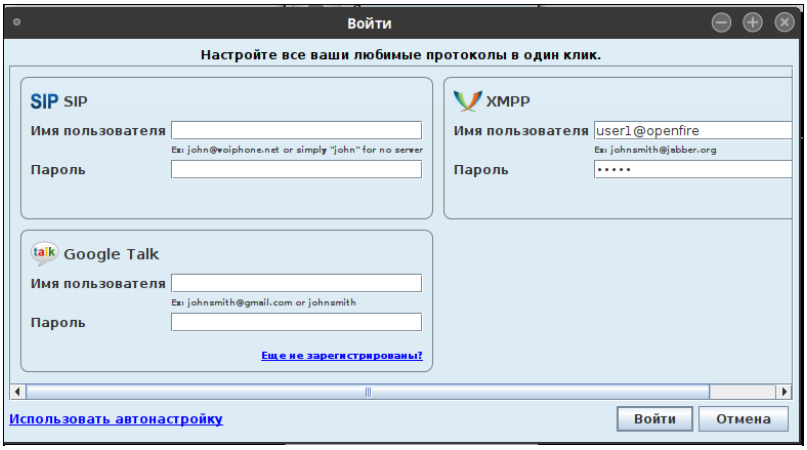
Программа также позволяет совершать видео-звонки и обеспечивает передачу файлов.

Для установки выполните команду:

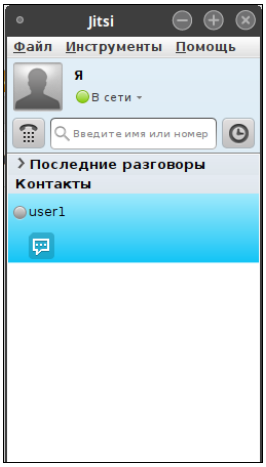
```
dnf install jitsi
```

Запуск *Jitsi* осуществляется через *«Меню» - «Интернет» - «Jitsi»*.

После запуска откроется окно с выбором протокола. В протоколе XMPP заполните поля «*Имя пользователя*» и «*Пароль*» и нажмите «*Войти*».



После этого откроется окно программы и список пользователей, зарегистрированных на одном сервере.



Linphone

Установка
Первый запуск и создание аккаунта
Дополнительные настройки linphone

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: linphone-2:4.3.2-1

Linphone – кроссплатформенный программный клиент IP-телефонии в стандарте **SIP** с открытым исходным кодом. Программа **linphone** предназначена для организации аудио и видео-вызовов, а также обмена текстовыми сообщениями.

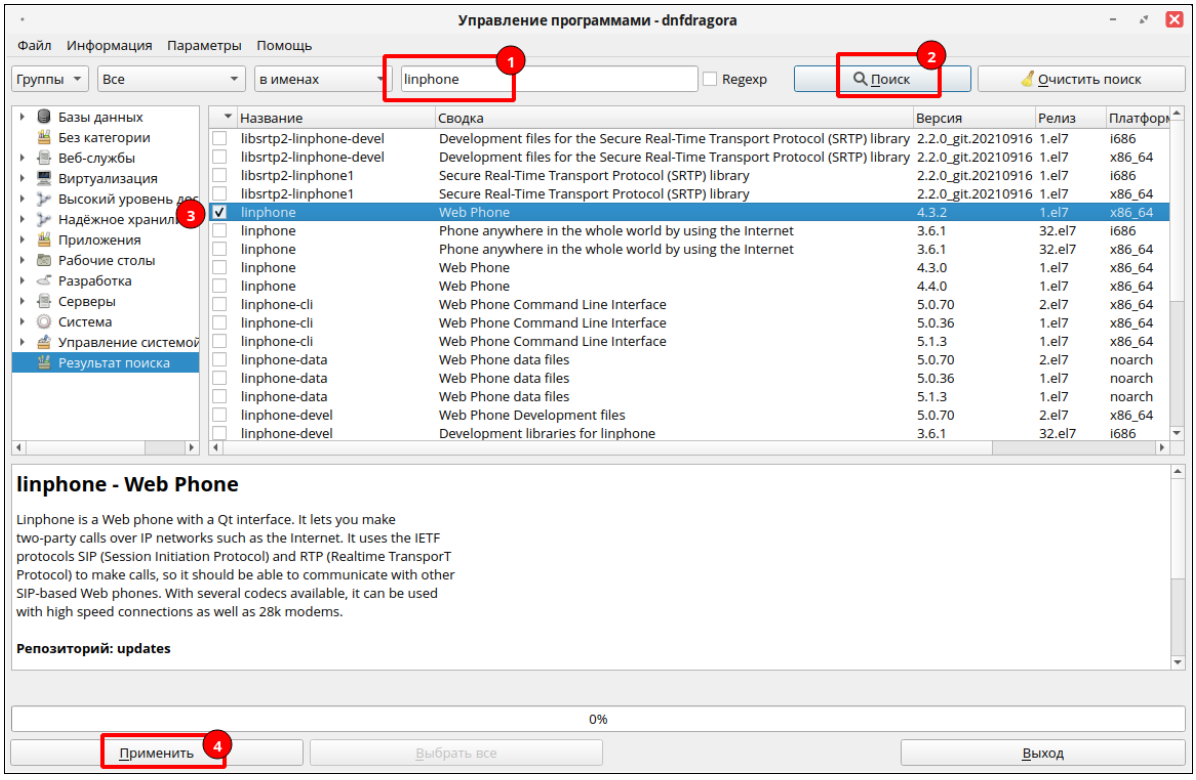
Возможности **Linphone**:

- аудио- и видеозвонки в фомате HD;
- аудиоконференции;
- переадресация вызовов;
- запись разговоров;
- адресная книга;
- поддержка IP-адресов;
- обмен смс-сообщениями;
- история вызовов;
- шифрование связи.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**linphone**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

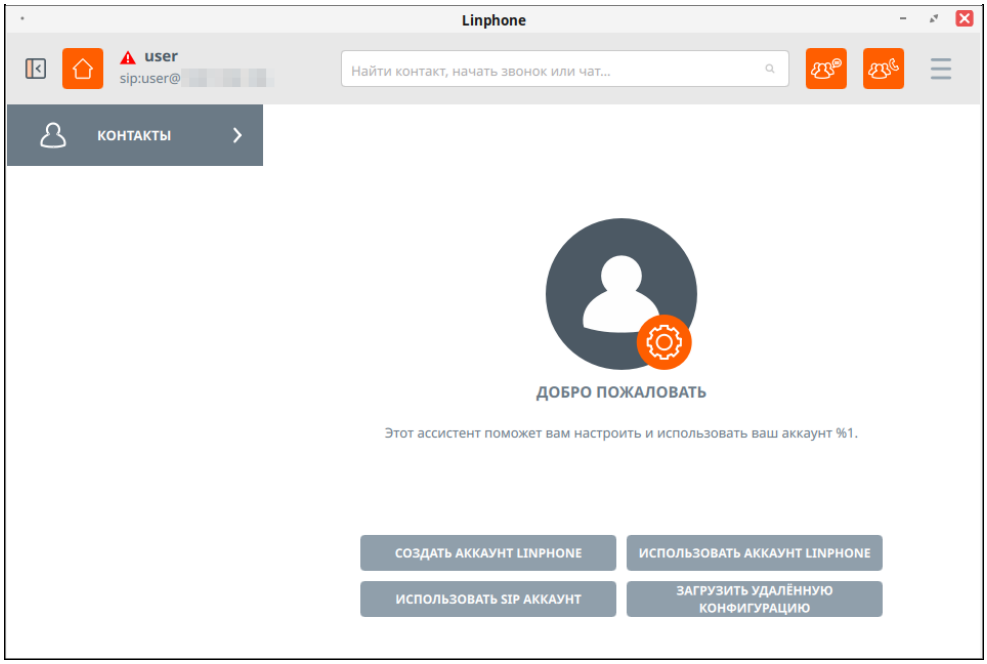
```
dnf install linphone
```

Дальнейшая работа в программе выполняется от локального пользователя.

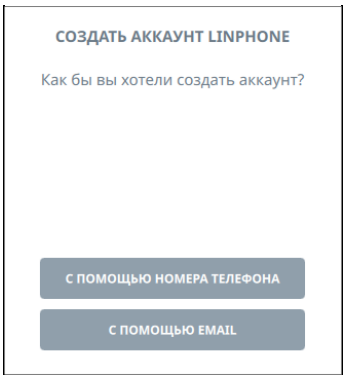
После установки программа будет доступна из «**Главного меню**» - «**Интернет**» - «**Linphone**».

Первый запуск и создание аккаунта

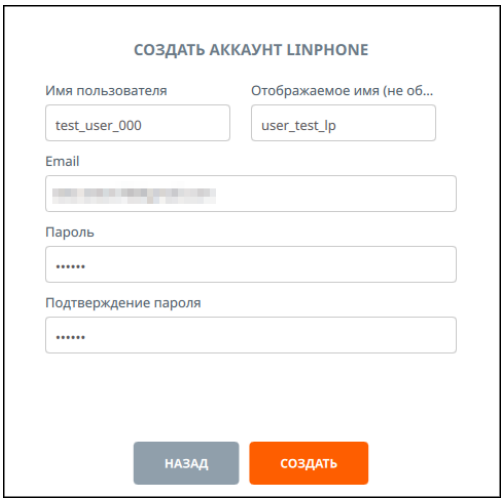
При первом запуске программы будет предложено выбрать способ авторизации.



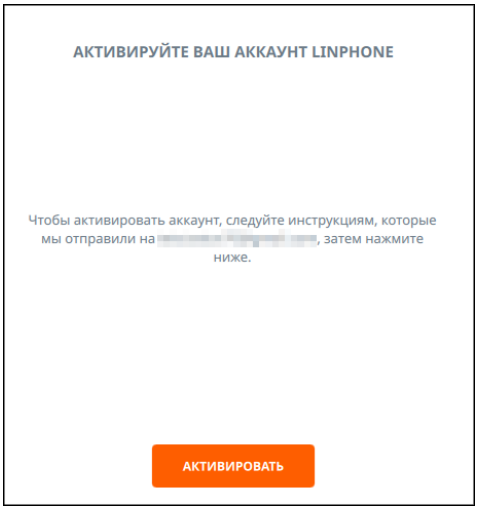
В примере рассмотрен вариант создания нового аккаунта. Нажмите кнопку «**Создать аккаунт Linphone**» и выберите предпочитаемый вариант регистрации – по *номеру телефона* или по *email* (в примере рассмотрен вариант регистрации по **email**).

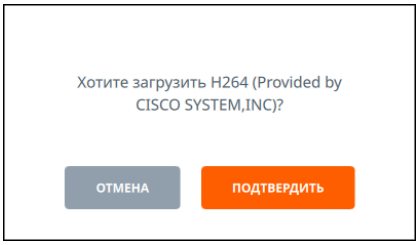


Далее будет открыта форма регистрации, в которой необходимо указать имя пользователя, никнейм (отображаемое имя), адрес электронной почты, а также задать пароль учетной записи. Нажмите «**Создать**».

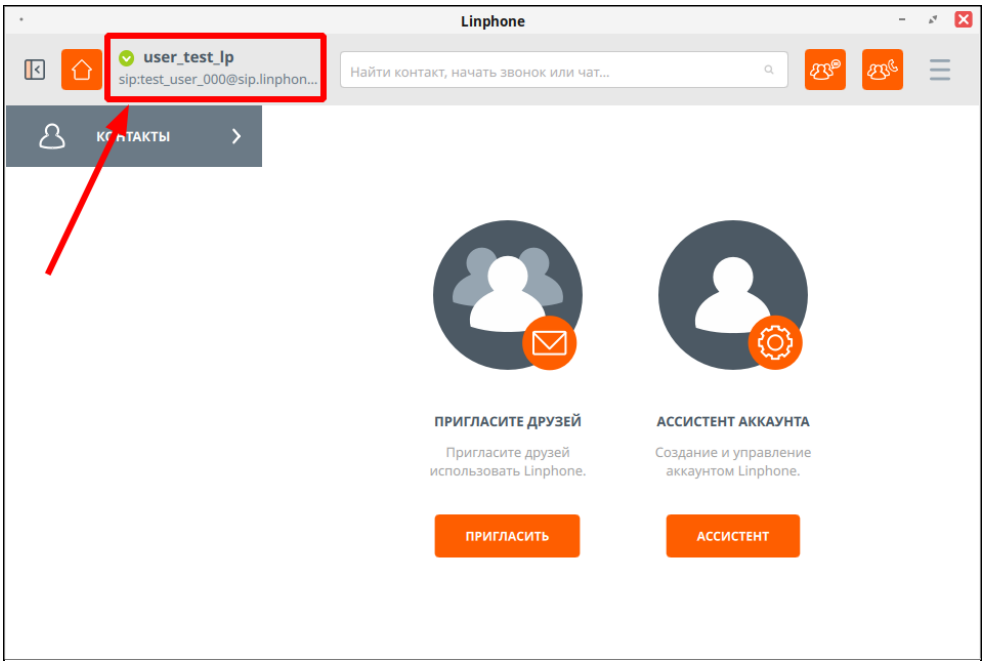


Затем необходимо активировать созданный аккаунт. Перейдите в сообщения электронной почты и следуйте подсказкам. После этого в окне **linphone** нажмите «**Активировать**», будет предложено загрузить дополнительный пакет, подтвердите загрузку.

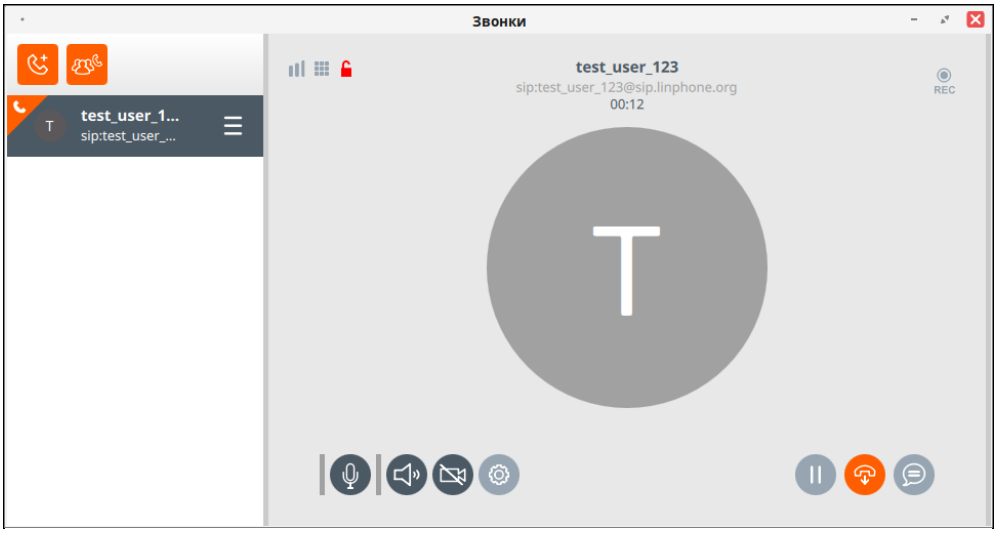




После активации аккаунта статус учетной записи будет изменен на «**Доступен**».

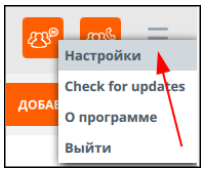


Для проверки работоспособности можно найти контакт по имени или номеру телефона и позвонить ему по аудио- или видеосвязи.

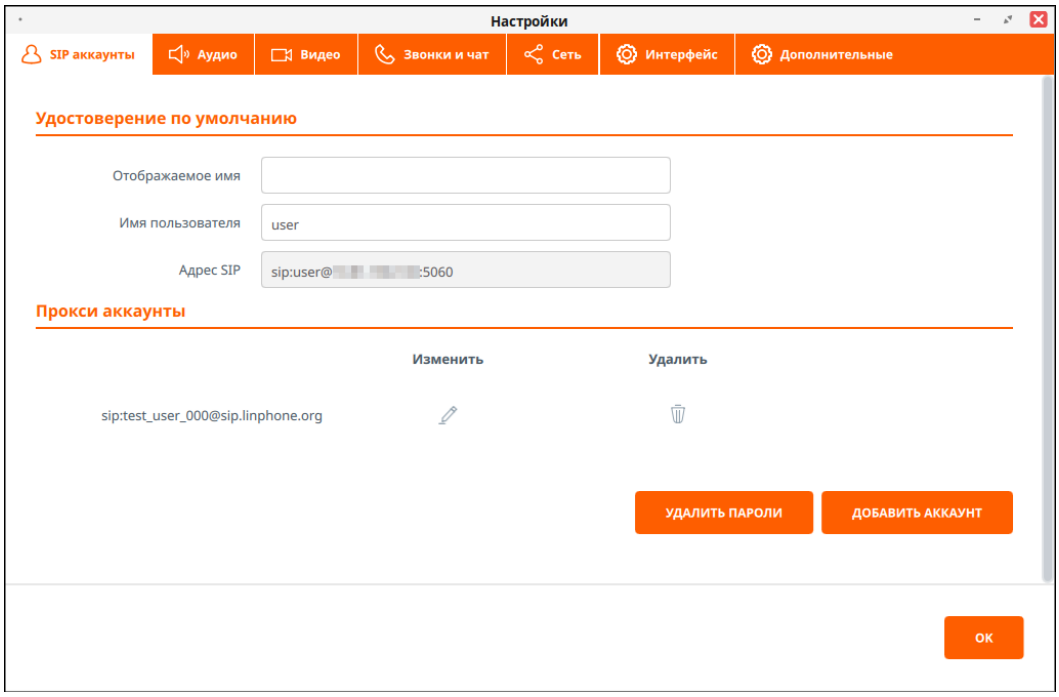


Дополнительные настройки linphone

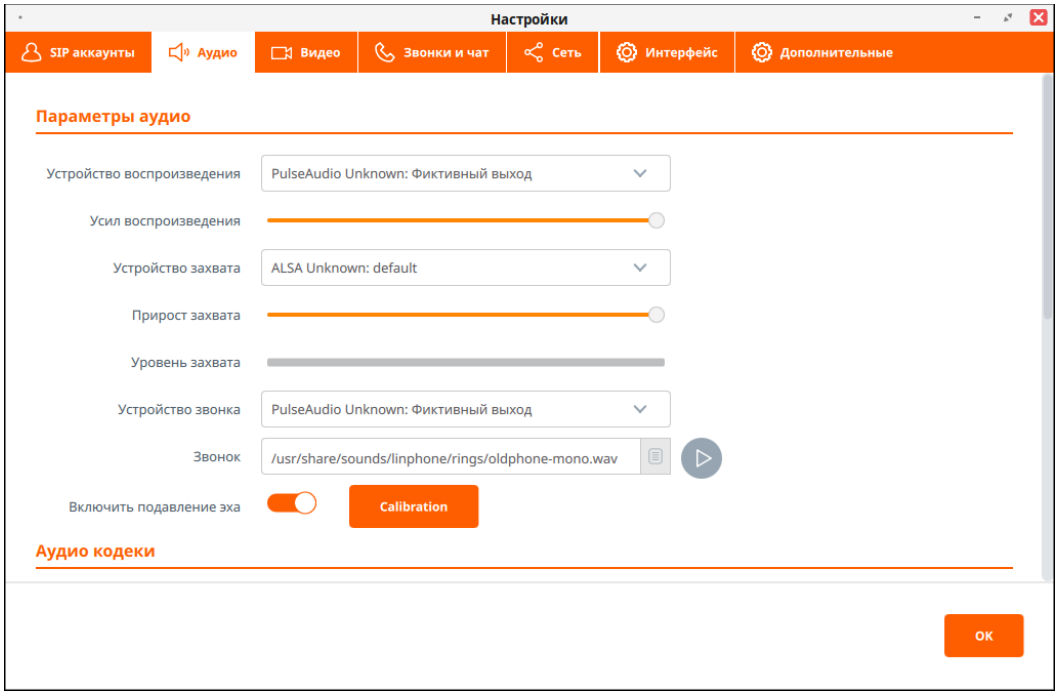
Для тонкой настройки каких-либо параметров выберите пункт меню **Настройки**.



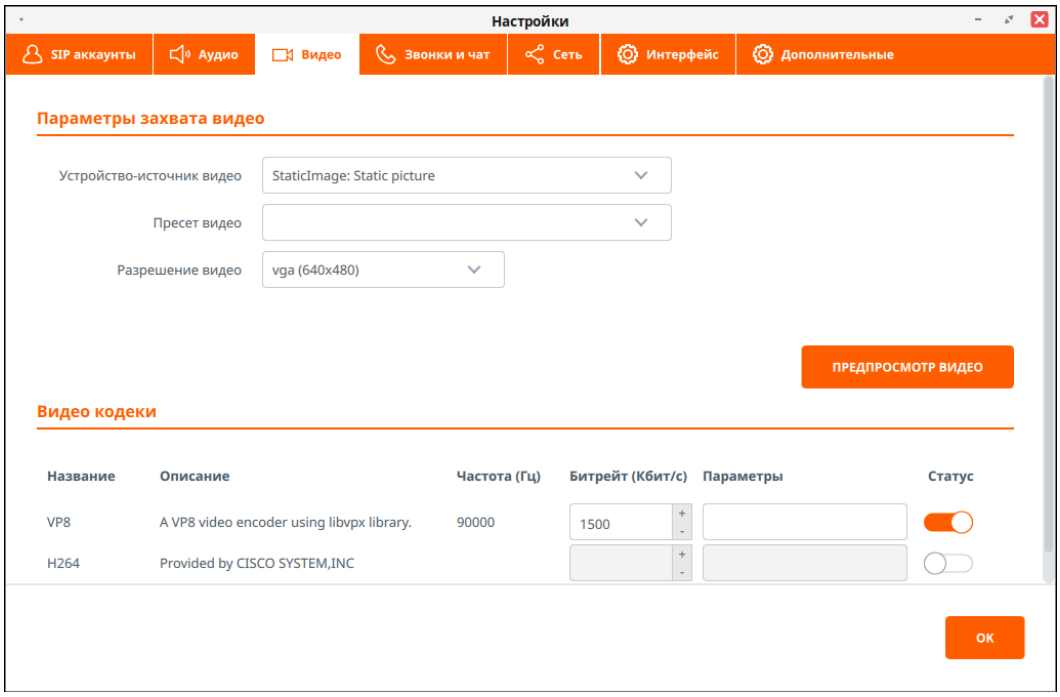
На вкладке «**SIP аккаунты**» можно изменять никнейм и имя пользователя, а также просматривать список аккаунтов.



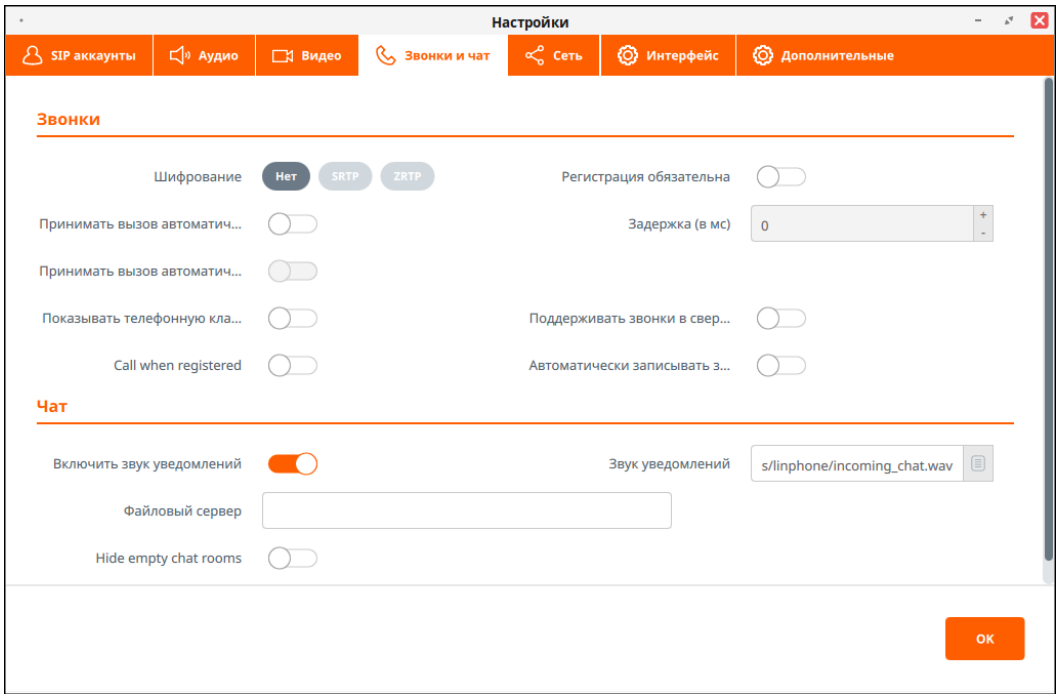
На вкладке «**Аудио**» настраиваются параметры аудио, такие как устройства воспроизведения, усиление воспроизведения, устройства захвата, уровень захвата, подавление эха, а также параметры аудиокодеков.



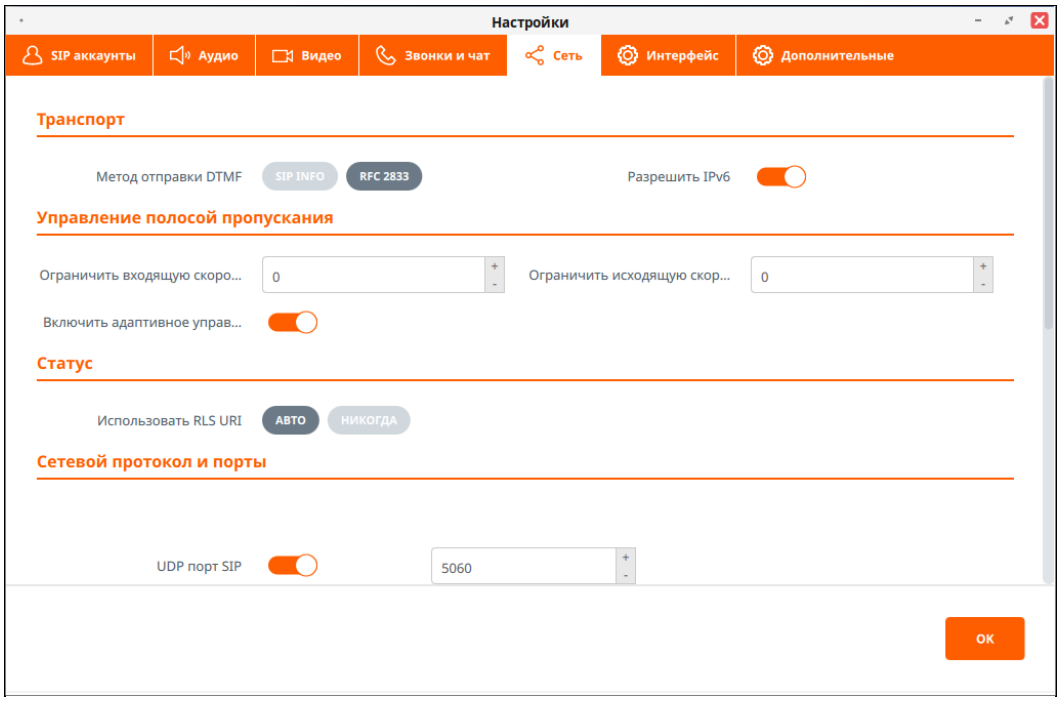
На вкладке «**Видео**» задаются параметры захвата видео и видеокодеки.



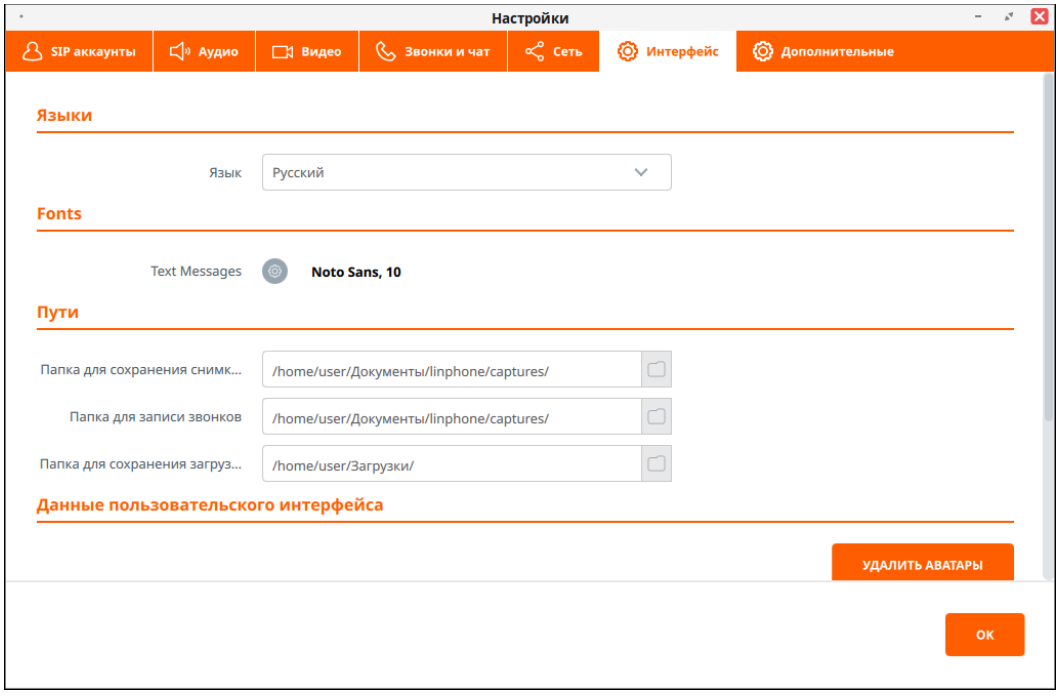
На вкладке «**Звонки и чат**» настраиваются уведомления, звуки уведомлений, шифрование звонков, прием вызовов, а также автоматическая запись звонков.



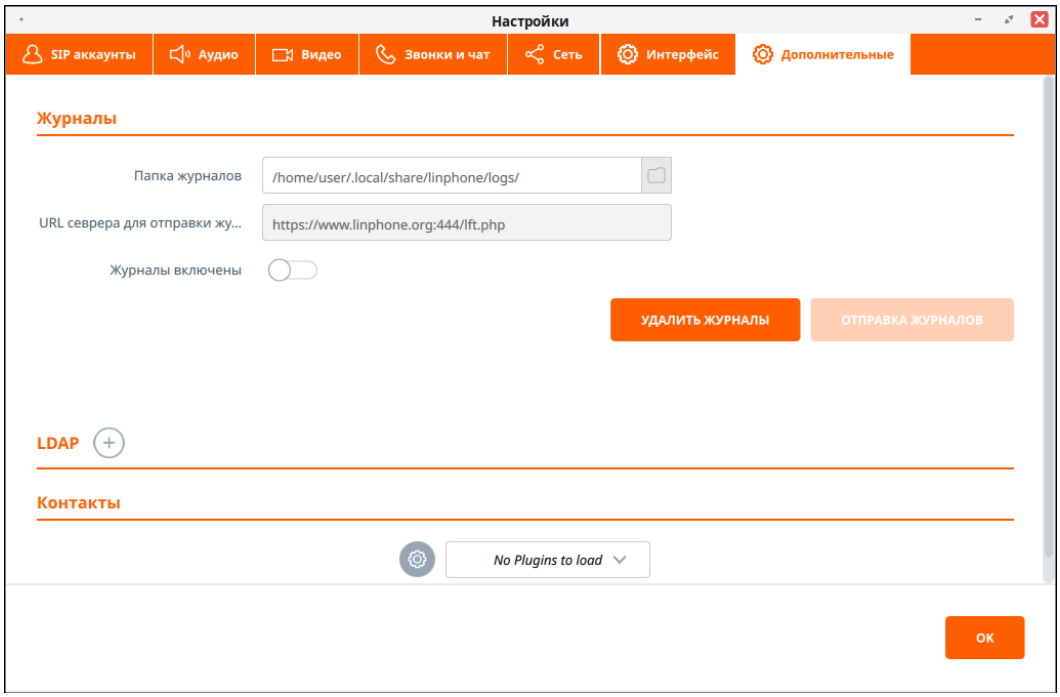
На вкладке «**Сеть**» доступна настройка используемого протокола сети, ограничение входящей и исходящей пропускной способности, безопасность сети и пр.



На вкладке «**Интерфейс**» устанавливается язык интерфейса, шрифт текстовых сообщений, каталоги хранения снимков, записей звонков и прочих загрузок.



На вкладке «**Дополнительные**» доступны настройки журналов, LDAP и контактов.


Настройки
SIP аккаунты
Аудио
Видео
Звонки и чат
Сеть
Интерфейс
Дополнительные
Журналы
Папка журналов
/home/user/.local/share/linphone/logs/
URL севрера для отправки жу...
https://www.linphone.org:444/lft.php
Журналы включены
УДАЛИТЬ ЖУРНАЛЫ
ОТПРАВКА ЖУРНАЛОВ
LDAP
Контакты
No Plugins to load
OK

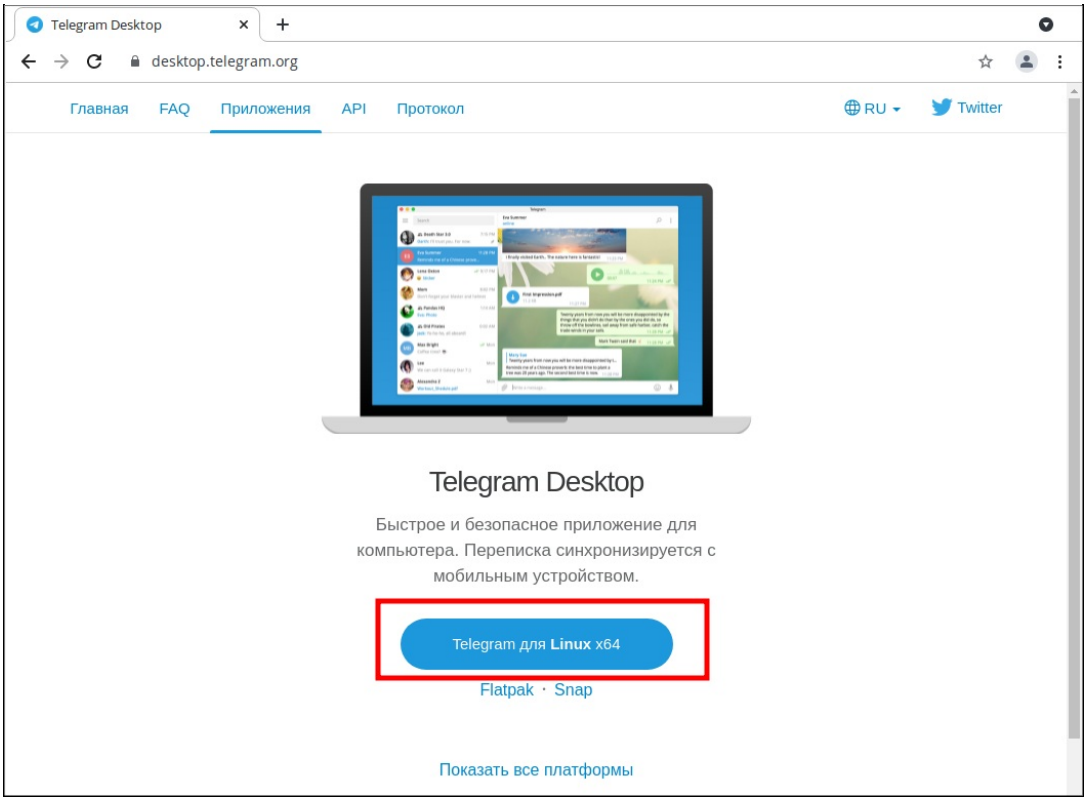
Telegram

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Telegram - 4.11.7

Перейдите на официальную страницу Telegram.

Нажмите на кнопку «**Telegram для Linux x64**». Будет запущен процесс загрузки архива приложения.

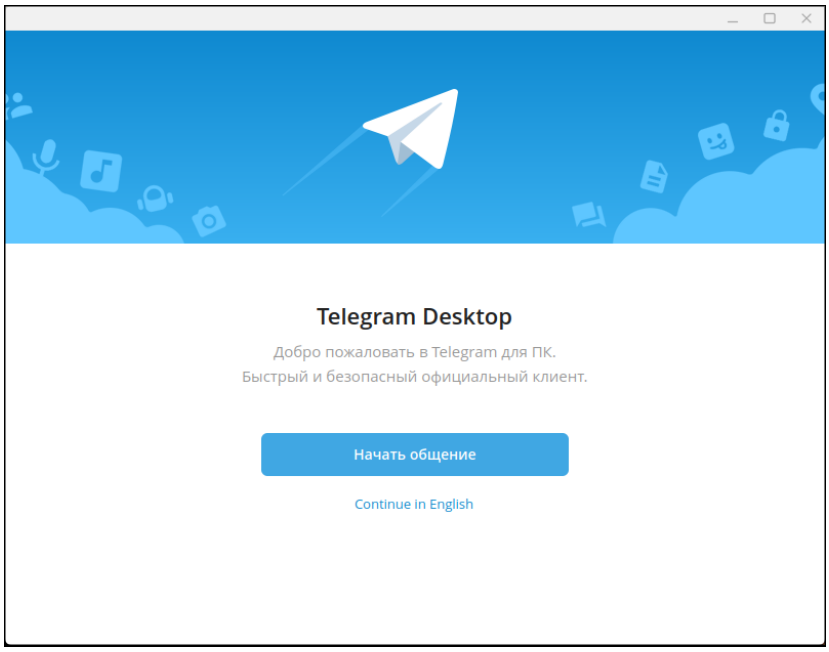


После завершения загрузки перейдите в каталог со скачанным архивом и распакуйте его:

```
cd /home/user/Загрузки
tar -xvf ./tsetup.4.11.7.tar.xz
```

Будет создан новый каталог с распакованными файлами - **/Telegram**, в нем необходимо запустить файл **Telegram** - будет открыто диалоговое окно мессенджера, в котором необходимо нажать кнопку «**Начать общение**» и выбрать способ авторизации.

```
./Telegram/Telegram
```



Запуск мессенджера доступен из «**Главного меню**» - «**Интернет**» - «**Telegram Desktop**».

Gajim

Установка и запуск
Создание учётной записи
О программе
Установка модулей
Добавление контакта в Gajim

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: gajim-1.1.3

Gajim представляет собой бесплатный мессенджер с открытым исходным кодом, совместимый с различными операционными системами и реализующий поддержку протокола Jabber. Разработанный на Python и использующий графический интерфейс GTK+, **Gajim** обладает широким спектром функций.

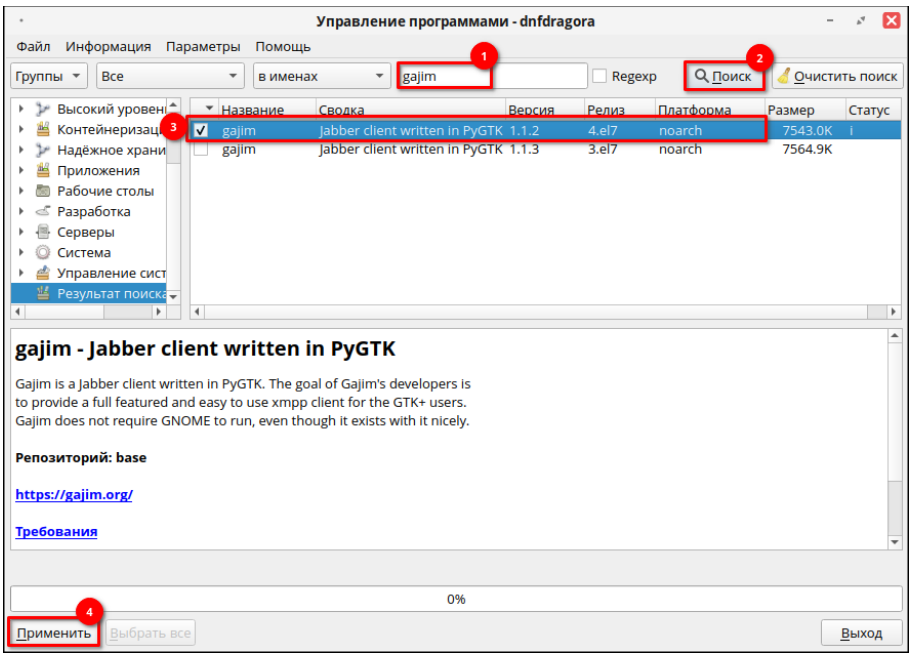
Основные возможности Gajim:

- поддержка многих языков, включая русский;
- смайлики, аватары, сообщения о статусе, поддержка расширенных статусов;
- вкладки в окне беседы, возможность объединить окно списка контактов (ростера) с окном беседы;
- поддержка метаконтактов;
- поддержка конференций (с протоколом MUC), приглашений, преобразования чата в конференцию, сокрытие конференций в ростере;
- закладки для комнат;
- поддержка транспортов;
- передача файлов;
- командная строка;
- шифрование паролей;
- генератор RST;
- OpenPGP-шифрование;
- URL-граббер, проверка орфографии, поддержка разметки текста reStructuredText.

Установка и запуск

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**gajim**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install gajim
```

Для запуска программы через терминал введите команду:

```
gajim
```

После установки программа будет доступна из «**Главного меню**» — «**Интернет**» — «**Gajim**».

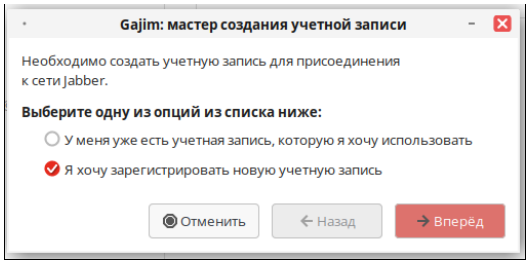
Когда программа запущена, в системном трее отображается значок  .

Создание учётной записи

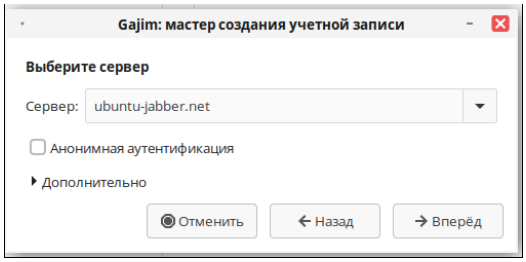
При первом запуске Gajim будет выведено диалоговое окно мастера создания учётной записи, предлагающее использовать существующую учётную запись или создать новую.

В случае наличия существующего аккаунта, пользователю следует выбрать опцию «**У меня уже есть учётная запись, которую я хочу использовать**».

Далее необходимо ввести свой **Jabber ID** (JID) и пароль в соответствующие поля вновь открывшегося окна. После ввода данных следует нажать на кнопку «**Сохранить**». Это действие завершит процесс аутентификации, и пользователь сможет перейти к следующему этапу.

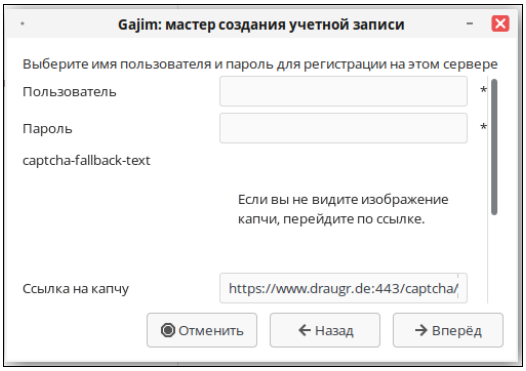


Если нужно создать новый аккаунт, то при выборе пункта «**Я хочу зарегистрировать новую учётную запись**» будет выведено окно, предлагающее ввести или выбрать из списка имя сервера, на котором нужно зарегистрироваться. Для этого необходимо выбрать какой-нибудь популярный сервер, например ubuntu-jabber.net, запомнить его и нажать кнопку «**Вперёд**».



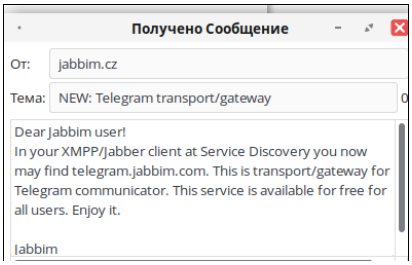
После инициализации процесса подключения **Gajim** выполнит проверку доступности сервера. В течение нескольких секунд по завершении проверки, будет отображено диалоговое окно, в котором пользователю будет предложено ввести свои учётные данные для аутентификации в системе.

Для регистрации нового пользователя необходимо ввести логин, пароль и выполнить проверку капчи. Рекомендуется придерживаться использования английских букв, цифр, символов подчёркивания, тире и точки при создании логина. После заполнения данных следует нажать кнопку «**Вперёд**».

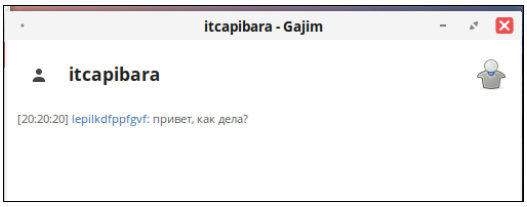


В случае, если выбранное имя пользователя уже зарегистрировано на сервере, система выведет сообщение об ошибке. Тогда потребуется вернуться к предыдущему шагу и выбрать альтернативное имя пользователя. По завершении процесса регистрации на экране появится уведомление, подтверждающее успешное создание учётной записи.

После завершения процесса регистрации пользователь может сообщить свой JID другим лицам для добавления в список контактов. Программа **Gajim** автоматически начнёт процедуру подключения к сети. Перед инициализацией подключения **Gajim** запросит пароль от учётной записи для подтверждения идентичности пользователя. В случае успешного ввода пароля и подключения к сети, в главном окне программы отобразится приветственное сообщение.

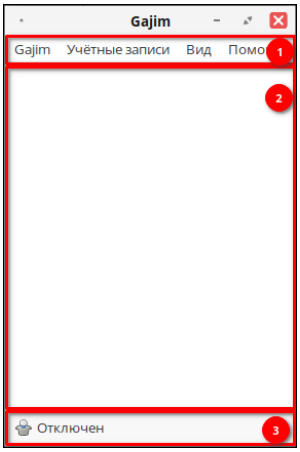


Если процедура регистрации и подключения к сети была выполнена корректно, окно чата **Gajim** будет выглядеть следующим образом:



О программе

Главное окно программы **Gajim** содержит следующие элементы:



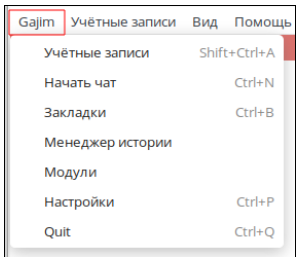
1. **Основное меню** — представляет собой выпадающий список, где доступны все действия для работы и настройки программы.

2. **Список контактов** (**ростер**) — позволяет просматривать и управлять контактами, создавать группы контактов и просматривать их статус.

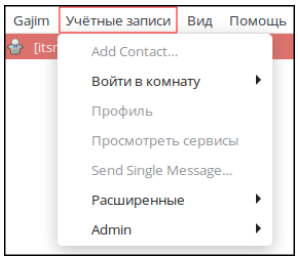
3. **Статусная строка** — отображает текущее состояние подключения.

В основном меню представлен доступ к основным функциям программы.

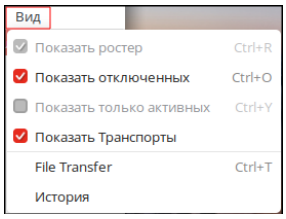
Меню «**Gajim**» отвечает за настройку учётных записей и различных параметров мессенджера, таких как конфигурация, аудио- и видеозвонки, уведомления и стиль интерфейса. Здесь можно добавлять, удалять и редактировать учётные записи, а также настраивать параметры подключения, такие как имя хоста, порт, протокол и шифрование.



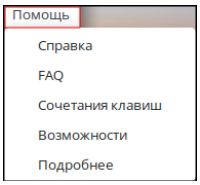
Меню **«Учётные записи»** отвечает за добавление контактов, настройки профиля, настройки архивации, списки доступа.



Меню **«Вид»** отвечает за изменение настроек отображения окна программы. С его помощью можно настроить отображение ростера, показать активные или отключённые контакты, показать транспорты и другие параметры.



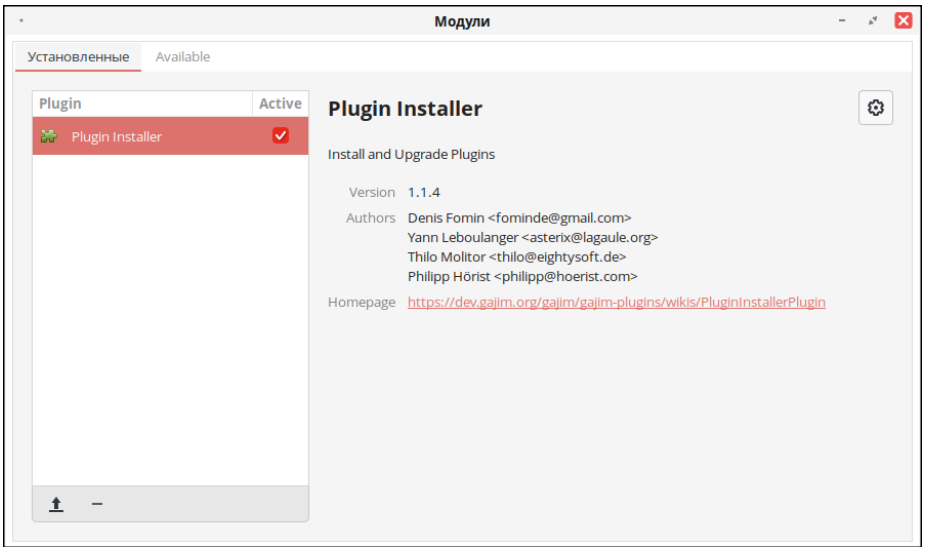
Меню **«Помощь»** отвечает за доступ к справочной информации и документации по программе. В этом меню можно найти информацию о различных функциях и настройках **Gajim**, а также ссылки на официальные ресурсы и форумы для получения дополнительной помощи и поддержки.



Установка модулей

Для расширения функционала программы можно установить модули. Для установки дополнительных модулей перейдите в меню «**Gajim**» — «**Модули**».

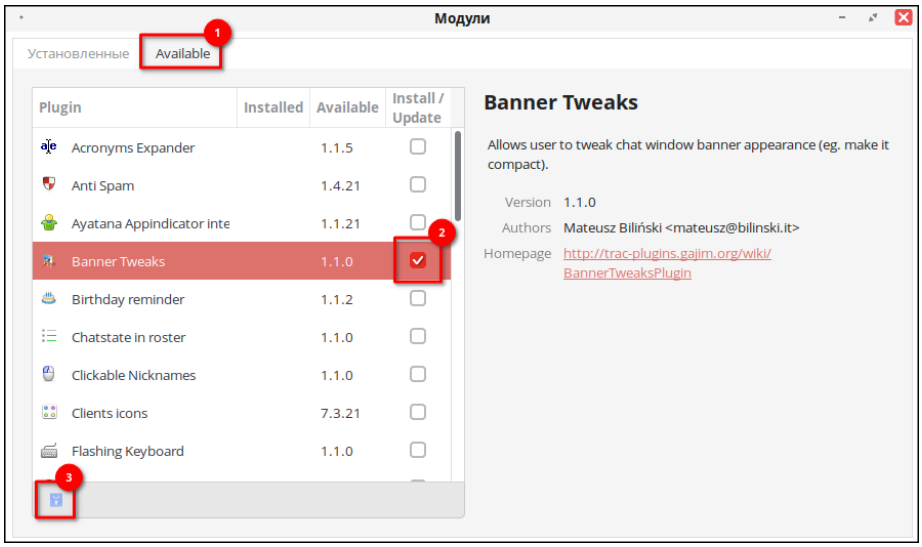
Вкладка «**Установленные**» показывает список установленных модулей. Первоначально установлен модуль «**Plugin Installer**» — это менеджер модулей, который позволяет искать, устанавливать, обновлять и удалять модули из **Gajim**.



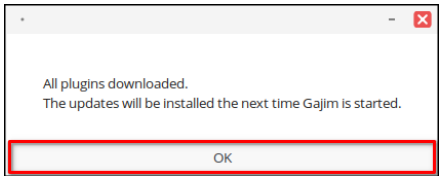
Вкладка «**Available**» в меню «**Модули**» Gajim показывает список всех доступных модулей, которые ещё не установлены в программе.

Для установки новых модулей через вкладку выполните следующие шаги:

1. Перейдите на вкладку «**Available**».
2. Выберите из списка модуль, который хотите установить, отметьте его флагом.
3. Нажмите на кнопку загрузки модуля.



4. В диалоговом окне с информацией об успешной загрузке модулей нажмите «**OK**».

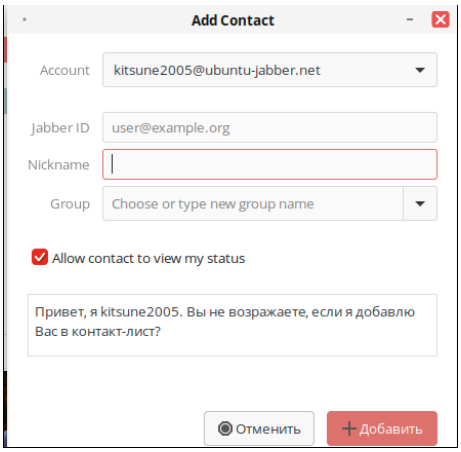


Плагины в **Gajim** добавляют дополнительные функциональные возможности. Далее приведён список наиболее популярных из доступных плагинов:

1. **Acronyms Expander** — автоматически расшифровывает аббревиатуры и акронимы в сообщениях.
2. **Anti Spam** — предназначен для борьбы со спамом, позволяет блокировать сообщения от неизвестных контактов или содержащие определённые слова или фразы.
3. **Clients icons** — отображает значки клиентов в реестре и групповых чатах.
4. **Message Box Size** — позволяет настраивать размер окна ввода сообщений, делая его больше или меньше в зависимости от ваших предпочтений.
5. **Now Listen** — может отображать информацию о музыке, которую вы слушаете, в вашем статусе, позволяя вашим контактам видеть, что играет у вас в данный момент.
6. **Quick replies** — предоставляет возможность быстро отвечать на сообщения, используя заранее настроенные короткие ответы.
7. **Regex Filter** — использует регулярные выражения для фильтрации входящих сообщений, позволяя блокировать или пропускать сообщения на основе сложных правил, заданных пользователем.
8. **Triggers** — позволяет настроить автоматические действия (триггеры) в ответ на различные события в Gajim.

Добавление контакта в Gajim

Для добавления собеседников в Gajim перейдите в меню «**Учётные записи**» — «**Add contact**». Появится окно, в котором нужно ввести JID, а также назначить никнейм и группу для контакта. После заполнения данных пользователя нажмите «**Добавить**».



В контактном списке появится добавленный контакт, отмеченный знаком вопроса (). Собеседнику придёт запрос на подписку.

Когда он примет его, значок контакта сменится на обычный ().

Skype

Предварительная подготовка
Установка skype

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: skype-8.105.0.208

Предварительная подготовка

В качестве предварительной подготовки необходимо установить пакет **snap**, который является отдельной изолированной "программной средой" для работы того или иного приложения. Подробную информацию о **snap** и его установке в РЕД ОС см. в нашей статье «Snap - изолированная среда для запуска приложений».

Установка skype

После успешной установки **snap** можно перейти к непосредственной установке **skype**.

Для этого в терминале необходимо выполнить команду:

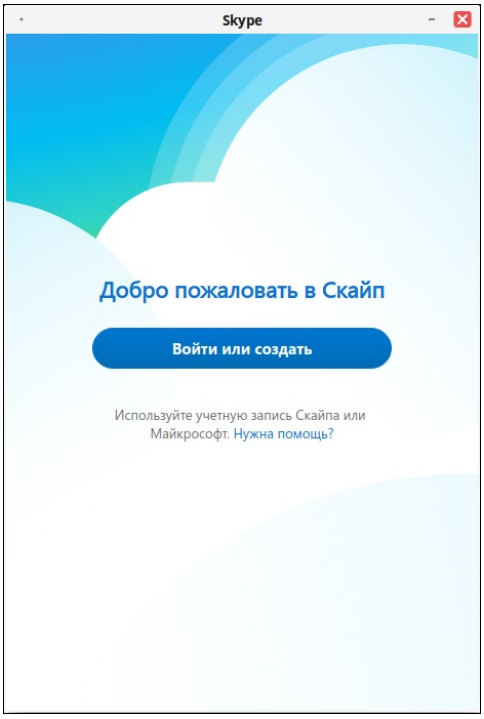
```
sudo snap install skype
```

Будет выполнена загрузка необходимых пакетов и установка **skype**.

Запуск программы доступен из «**Меню**» - «**Интернет**» - «**Skype**» или через терминал с помощью команды:

```
snap run skype
```

Для использования **Skype** необходимо войти под учетной записью *Skype* или *Microsoft* или зарегистрироваться.



Zoom

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zoom-6.2.3.2056-1

Сначала необходимо скачать **Zoom** с официального сайта, перейдя по ссылке.

Выберите тип Linux - **RedHat**, архитектура ОС - **64**-разрядная, версия - **8.0+**.

Для установки программы перейдите в сеанс **пользователя root**:

```
su -
```

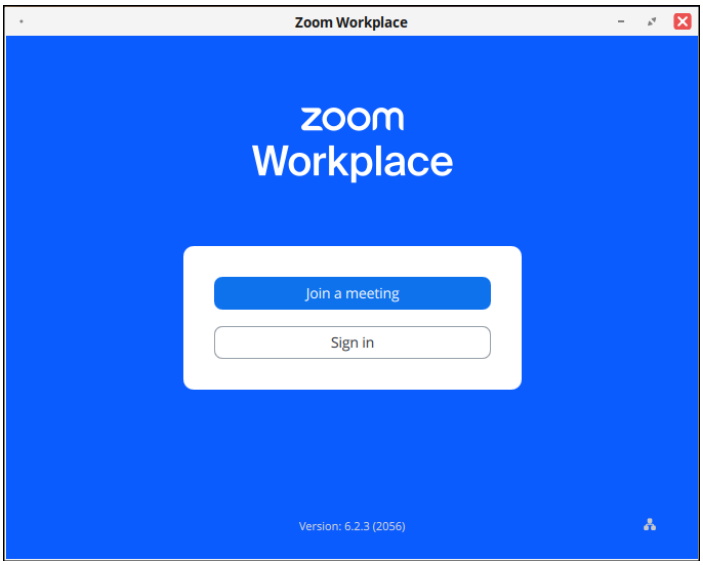
Перейдите в папку с загруженным файлом (в примере /home/user/Загрузки).

```
cd /home/user/Загрузки/
```

и выполните команду:

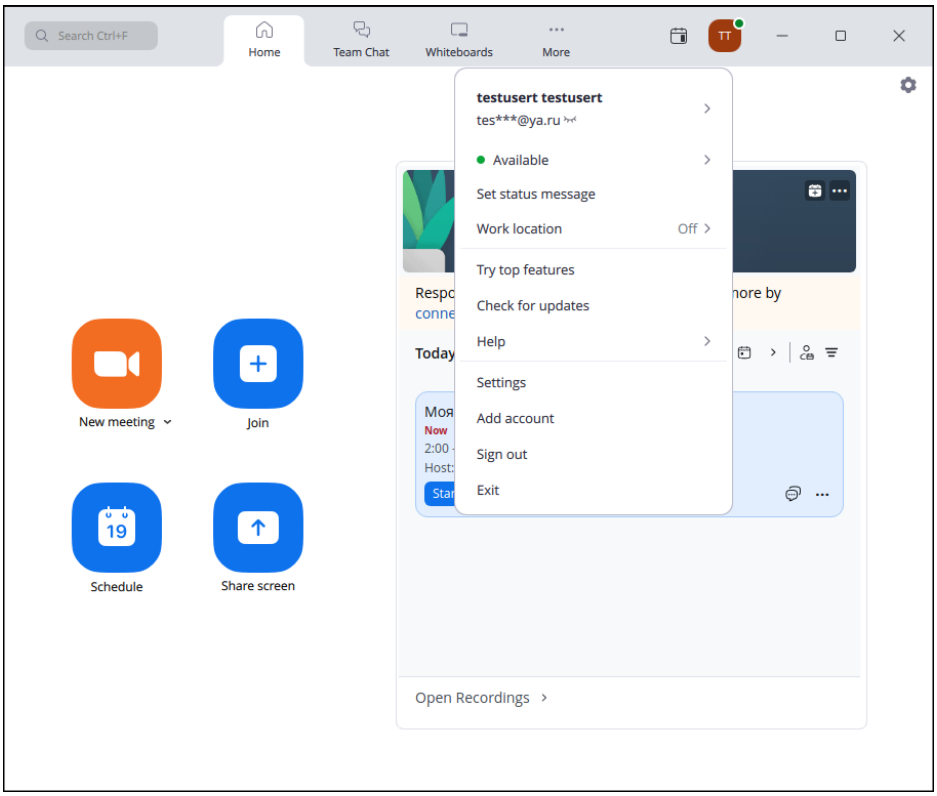
```
dnf install zoom_x86_64.rpm
```

После установки запуск программы доступен из «**Главного меню**» - «**Интернет**» - «**Zoom Workplace**».



После запуска программы будет предложено **Войти** или **Присоединиться к конференции**.

После ввода ваших данных приложение будет готово к использованию.



Для удаления программы **Zoom** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf remove zoom
```

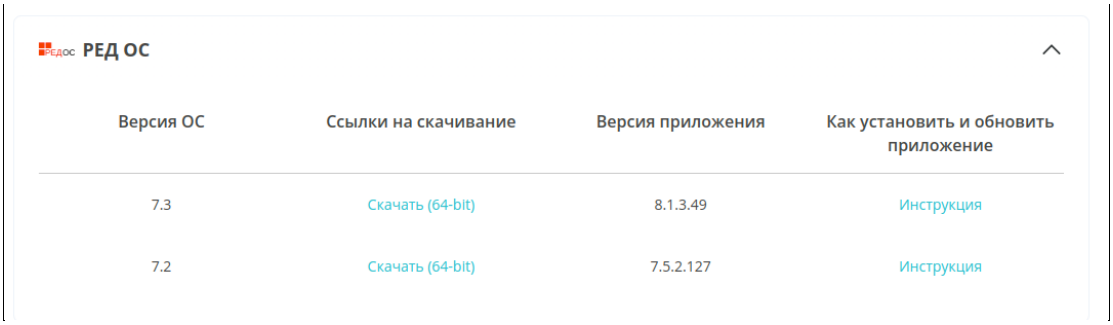
TrueConf

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: TrueConf - 8.1.3.49

TrueConf — российский аналог *Zoom*. Скачаем программу с официального сайта по ссылке.

Выберите используемую версию РЕД ОС и скачайте пакет.



Перейдите в сеанс пользователя **root**:

```
su -
```

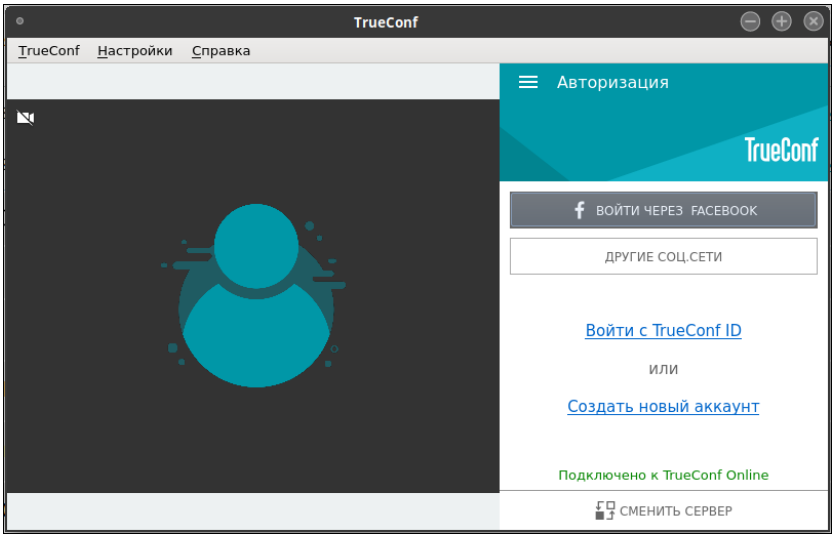
Перейдите в папку с загруженным файлом (в примере /home/user/Загрузки).

```
cd /home/user/Загрузки/
```

Выполните команду установки:

```
dnf install trueconf_client_redos73_x86_64.rpm
```

После установки запуск программы доступен из «**Главного меню**» - «**Интернет**» - «**TrueConf**».



Примечание.

В случае, если после установки **Trueconf** в **РЕД ОС 7.3 Сертифицированной редакции** при попытке запуска программы из терминала выводится сообщение вида:

```
/opt/trueconf/TrueConf: error while loading shared libraries: libatomic.so.1: cannot open shared object file: No such file or directory
```

для решения данной проблемы необходимо обновить библиотеку **libatomic1** командой:

```
dnf install libatomic1
```

В случае, если после установки **Trueconf** в **РЕД ОС 7.3 Стандартной редакции** при запуске программы из терминала выводится сообщение вида:

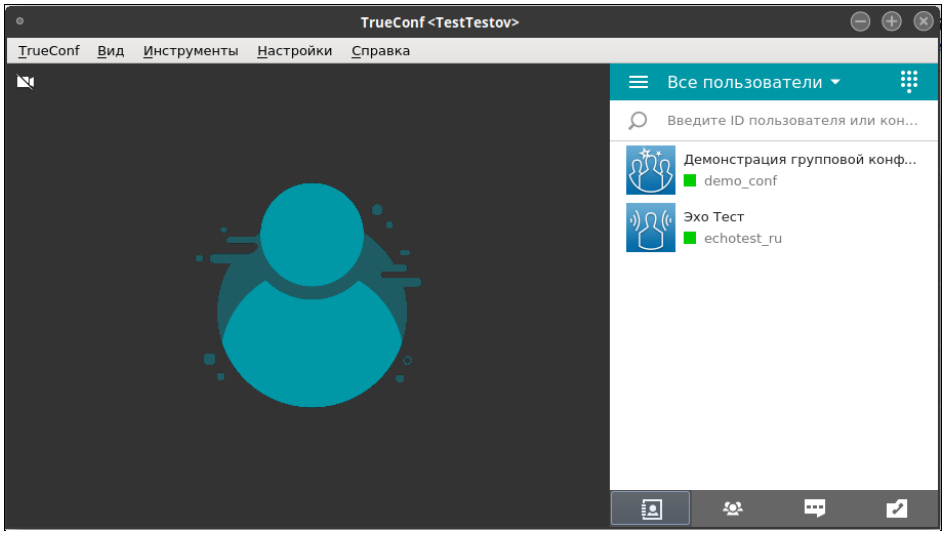
```
/opt/trueconf/TrueConf: error while loading shared libraries: libprotobuf.so.17: cannot open shared object file: No such file or directory
```

для решения данной проблемы необходимо понизить версию библиотеки **protobuf** командой:

```
dnf downgrade protobuf
```

После запуска программы будет предложено **Войти** или **Создать новый аккаунт**.

После ввода ваших данных приложение будет готово к использованию.



Для удаления программы **TrueConf** перейдите в сеанс пользователя **root:**

```
su -
```

и выполните команду:

```
dnf remove trueconf
```

Discord

Возможности программы
Загрузка дистрибутива
Настройка
Запуск

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** discord-0.0.21

Discord — кроссплатформенная проприетарная система мгновенного обмена сообщениями (мессенджер) с поддержкой **VoIP** и видеоконференций, предназначенная для использования различными сообществами по интересам.

Вы можете подробнее ознакомиться с возможностями мессенджера **Discord**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Discord в РЕД ОС;
- в **Яндекс.Дзен** — Установка Discord в РЕД ОС;
- в **VK Видео** — Установка Discord в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Возможности программы

Приложение способно организовывать голосовые конференции с настройкой канала связи и работать по принципу *push-to-talk*, создавать публичные и приватные чаты для обмена текстовыми сообщениями. Программа имеет браузерную версию, отличием от настольной версии является то, что режим *push-to-talk* работает, только если в браузере активна вкладка с приложением.

При включении режима «*стример*» скрывается вся личная информация, отключаются звуки и уведомления на рабочий стол. Режим можно включить автоматически (при запуске программ для трансляций, например, *Open Broadcaster Software*) или вручную.

Для аудио используется кодек *Opus*, который имеет возможности эхоподавления, подавления посторонних шумов и автоматической регулировки усиления. Для видео используется кодек *VP8*.

Функция «*оверлея*» обеспечивает возможность переключаться между каналами на сервере, серверами и групповыми чатами, увеличивать или уменьшать звук участников канала или личных сообщений по отдельности, включать и выключать микрофон и звук.

Поддерживается назначение «горячих клавиш».

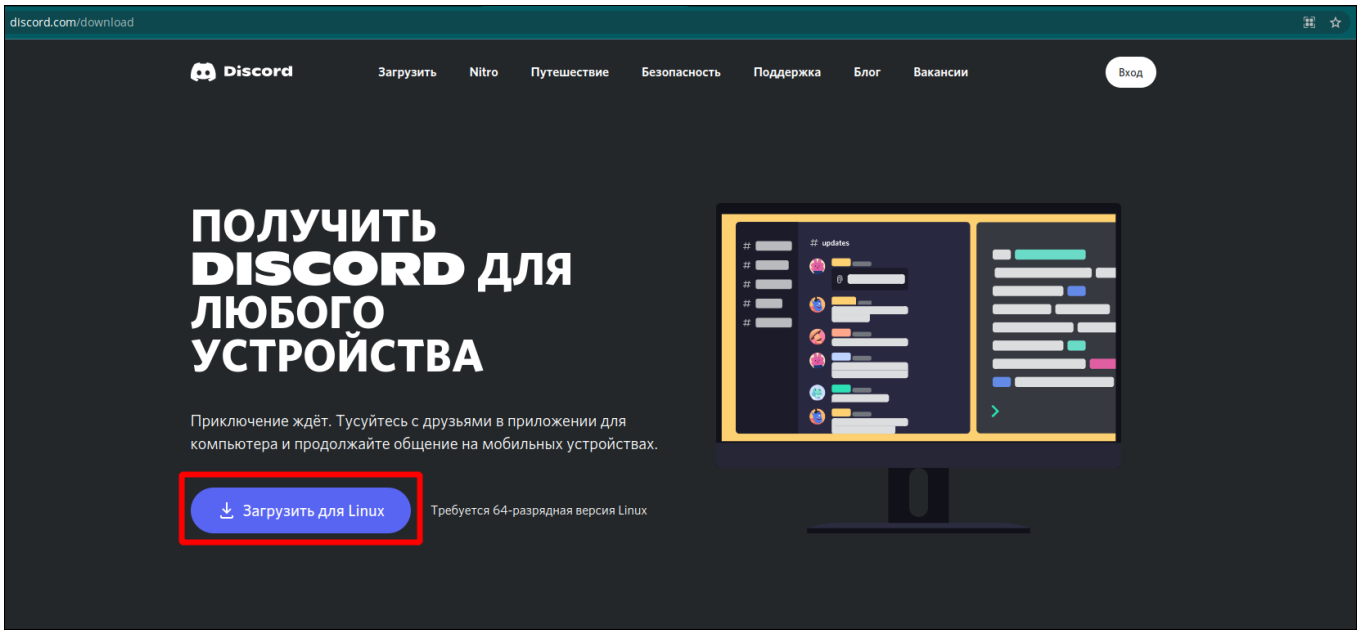
Реализована функция отключения уведомлений. Есть возможность включить озвучивание уведомлений. Можно заглушить отдельные серверы. Поддерживается поиск по чату личных сообщений или каналам сервера.

В текстовом чате поддерживается присоединение файлов, картинок, вставка ссылок (для некоторых сайтов работает предпросмотр), форматирование текста и смайлики, **без** платной подписки **Discord Nitro** размер вложения ограничен объёмом **8 МБ**.

Приложение имеет гибкие настройки интерфейса, возможно устанавливать различные темы и дополнения для расширения функциональности. Также возможно форматирование не только текста в сообщениях либо серверах, но и менять шрифты никнейма, используя специальные сервисы на основе символов *Unicode*.

Загрузка дистрибутива

Для загрузки дистрибутива перейдите на официальный сайт разработчика и нажмите кнопку «**Загрузить для Linux**». Выберите архив с расширением **tar.gz**.



После загрузки перейдите в папку со скачанным архивом и распакуйте его (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
tar -xzvf discord-0.0.21.tar.gz
```

Затем, используя команду cp, скопируйте извлеченные файлы в каталог **/opt**.

```
cp -r Discord /opt/
```

После этого создайте символическую ссылку на бинарный файл в каталог **/usr/bin**:

```
ln -sf /opt/Discord/Discord /usr/bin/Discord
```

Настройка

Далее необходимо добавить приложение в **Главное меню**, а затем создать иконку для запуска.

Используйте cp, чтобы взять включенный файл **discord.desktop** и поместить его в **/usr/share/applications/**. Это гарантирует, что программа будет отображаться на вашем компьютере, как и другие программы.

```
cp /opt/Discord/discord.desktop /usr/share/applications/discord.desktop
```

Назначьте файлу права на исполнение командой:

```
chmod +x /usr/share/applications/discord.desktop
```

Затем отредактируйте файл **discord.desktop**, находящийся в **/usr/share/applications/discord.desktop**.

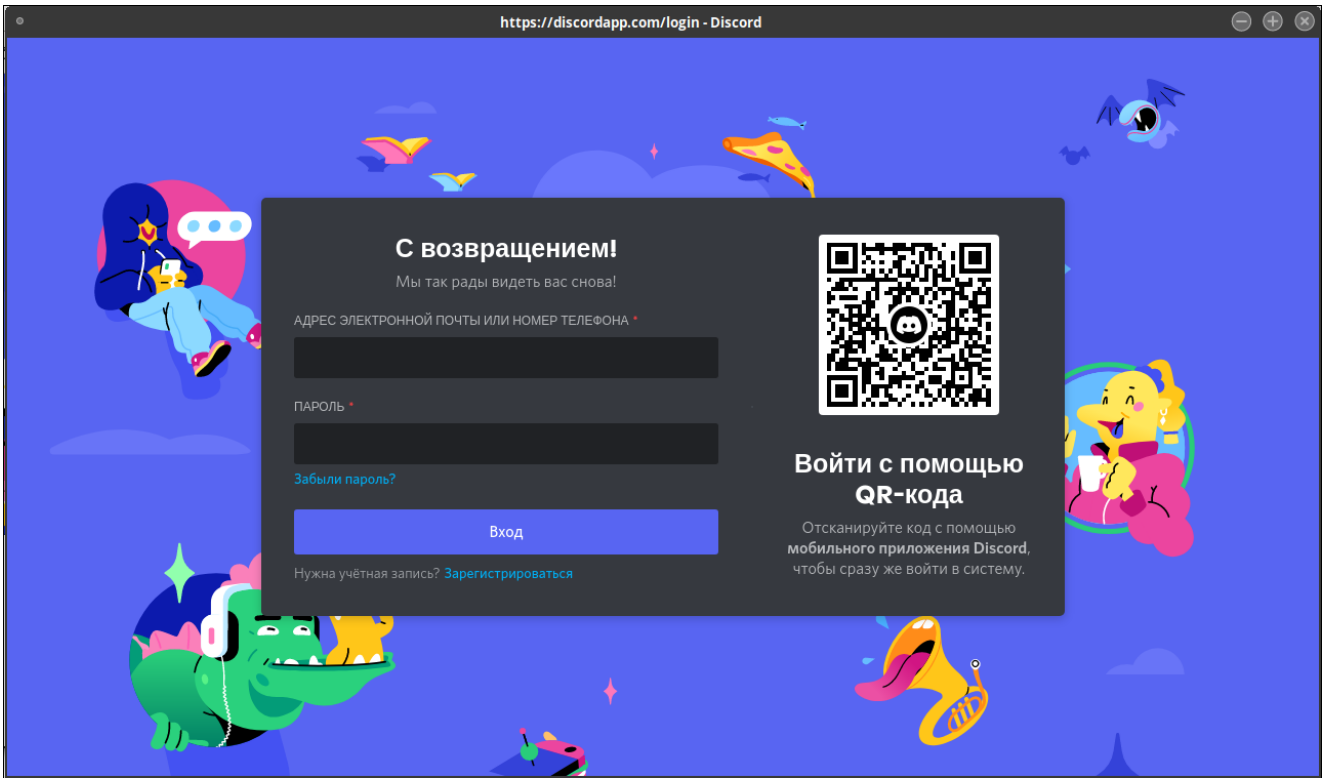
```
nano /usr/share/applications/discord.desktop
```

В нем необходимо привести следующие строки к виду:

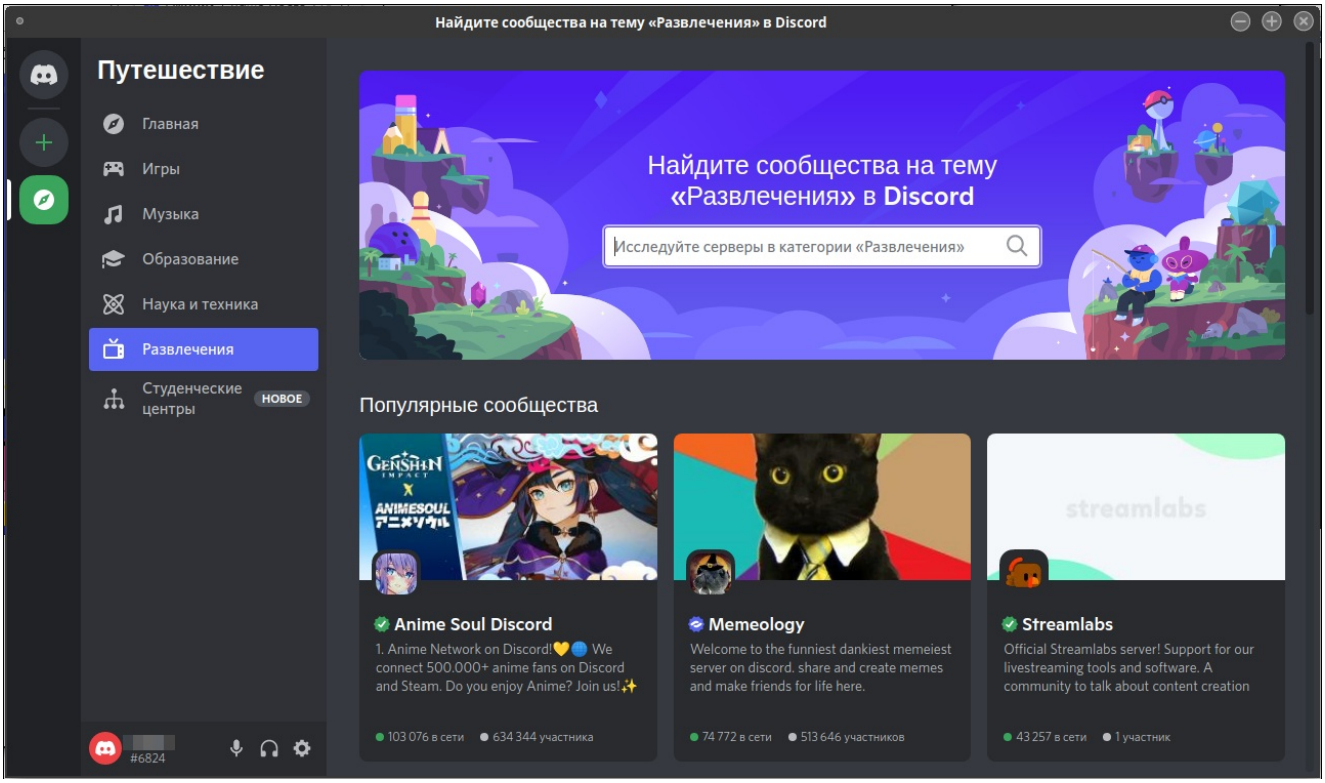
```
Exec=/usr/bin/Discord
Icon=/opt/Discord/discord.png
```

Запуск

После всех выполненных действий программа будет доступна из «**Главного меню**» - «**Интернет**» - «**Discord**».



После успешной регистрации или входа будет открыт ваш профиль.



Установка WINE

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки необходимо открыть терминал, войти под суперпользователем **root** и начать установку:

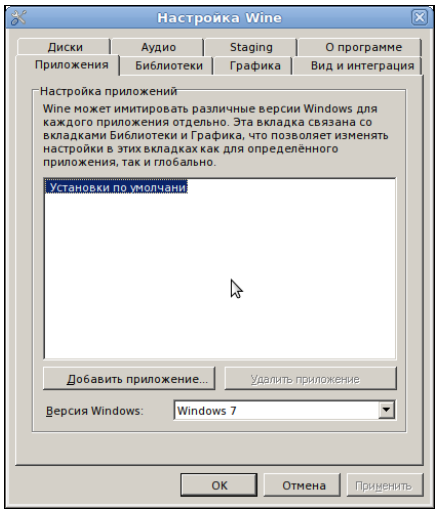
```
# dnf install wine
```

После установки запустите команду от имени обычного пользователя, чтобы увидеть конфигурацию *Wine*:

```
winecfg
```

Примечание.

При первом запуске команды **winecfg** создается префикс **.wine** 64-х разрядный по умолчанию.



Работа с программами в WINE

Установка программ в Wine
Запуск программы
Удаление программ в Wine

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка программ в Wine

Для легковесных программ достаточно команды:

```
wine filename.exe
```

Но чаще всего перед установкой программы в *wine* требуется настройка префикса.

Если при установке префикс не указывается, программа ставится в префикс по умолчанию.

Если установщик программы запускается файлом с расширением **.msi**, используем команду:

```
wine msiexec /i filename.msi
```

Установка в префикс не по умолчанию, например **.wine_prefix**, осуществляется следующим образом:

```
WINEPREFIX="/home/$USER/.wine_prefix" wine "/home/$USER/Downloads/filename.exe"
```

Запуск программы

Чтобы запустить программу, необходимо указать полный путь к исполняемой программе или имени программы, как показано в примере ниже:

```
wine /<путь_к_файлу>/program.exe
```

Первый запуск программы может длиться достаточно долгое время.

Запуск **bat**-файлов осуществляется командой:

```
wine start filename.bat
```

Удаление программ в Wine

Для удаления программ необходимо использовать команду:

```
wine uninstaller
```

или удаление из префикса:

```
WINEPREFIX="/home/$USER/.wine" wine uninstaller
```

После этого откроется окно «**Установка/удаление программ**», где следует выбрать нужную программу и нажать кнопку «**Удалить**».

При помощи **wine uninstaller** можно устанавливать программы, нажав на кнопку «**Установить**» и выбрав необходимую для установки программу.

Удаление программы без использования **GUI** осуществляется следующим образом:

```
wine uninstaller --remove <название_программы>
```

или из префикса:

```
WINEPREFIX="/home/$USER/.wine_prefix" wine uninstaller --remove <название_программы>
```

Также есть возможность удалить программу, используя ее собственную программу удаления:

```
wine /<путь_к_папке_с_программой>/uninstall.exe
```

Префиксы WINE

Настройка префикса
winefile - файловый менеджер Wine
Работа с реестром

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для разных программ могут потребоваться разные дополнительные компоненты, разные настройки *Wine* и т. п. Для этого существуют префиксы *Wine*. Используя для каждой программы свой префикс, вы можете обеспечить им индивидуальное окружение.

Для примера создадим и сконфигурируем 64-х разрядный префикс с именем **.wine_prefix** в домашнем каталоге пользователя:

```
WINEARCH=win64 WINEPREFIX="/home/$USER/.wine_prefix" winecfg
```

где **WINEARCH=win64** — указывает, что префикс создается под архитектуру **amd64**, что позволит запускать в нем 64-разрядные программы, а также 32-разрядные. Для создания 32-разрядного префикса необходимо заменить 64 на 32.

WINEPREFIX="/home/$USER/.wine_prefix" — указывает путь расположения создаваемого префикса.

> **Примечание.**
>
> Кавычки используются в случаях, если в имени папок содержится пробел, например **"/home/user/Рабочий стол"**.

winecfg — запускает программу конфигурирования префикса.

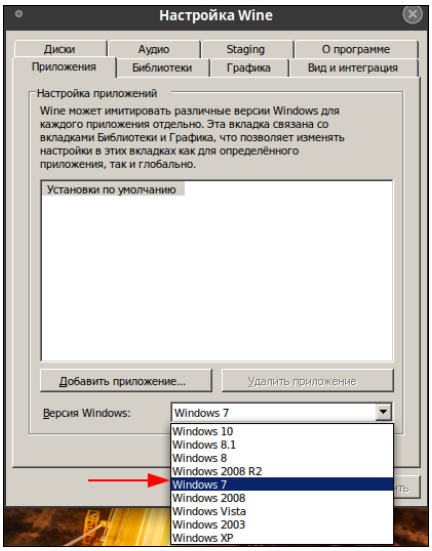
Для запуска программ с префиксом каждый раз указывать архитектуру не требуется, поэтому после создания параметр **WINEARCH=win64** прописывать не нужно.

Пример запуска программы *internet explorer* с префиксом:

```
WINEPREFIX=/home/$USER/.wine_prefix wine /home/$USER/.wine/drive_c/Program\ Files/Internet\ Explorer/iexplore.exe
```

Настройка префикса

Версия *Windows* позволяет выбирать режим запуска с необходимой версией Windows (Windows 7 - по умолчанию).



Вкладка «**Диски**» позволяет управлять виртуальными и физическими разделами. В стандартной конфигурации подключено 2 раздела: **C** и **Z**.

C — является системным каталогом префикса;

Z — ведет в корень файловой системы Linux, в некоторых случаях такое поведение нежелательно, поэтому данный диск рекомендуется удалить, тем самым изолировав префикс от основной системы.

> **Примечание.**
>
> Вредоносные программы для Windows потенциально способны нанести вред Linux-системе.

Вкладка «**Вид и интеграция**» дает возможность выбора ассоциаций каталогов Windows-пользователя с домашними каталогами Linux-пользователя. Данная возможность располагается в блоке «**Папки**» в нижней половине окна.

В префиксе стандартные каталоги Windows-пользователя располагаются по пути **/home/user/.wine_prefix/drive_c/users/$USER/**.

Ссылки в данном случае указывают на домашние каталоги Linux-пользователя, который создал префикс.

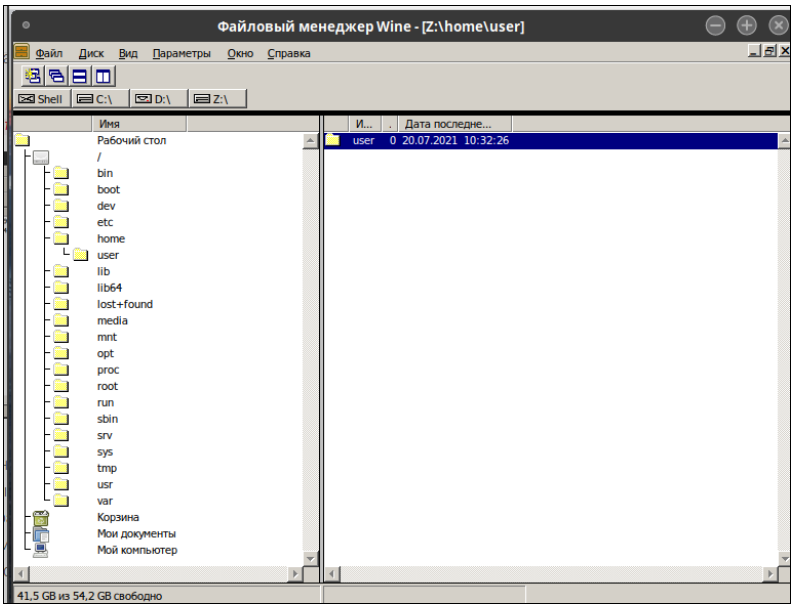
Остальные вкладки подробно описаны и интуитивно понятны.

winefile - файловый менеджер Wine

Winefile является аналогом проводника *Windows*.

Запуск **winefile** осуществляется командой:

```
WINEPREFIX="/home/$USER/.wine_prefix" wine winefile
```



Работа с реестром

Для открытия реестра используется инструмент **regedit**:

```
wine regedit
```

Чтобы перемещаться по реестру, кликните на ключах в левой части панели, чтобы перейти на следующий уровень глубины.

Чтобы удалить ключ, кликните на нем и в меню **Edit** выберите «**Delete**».

Чтобы добавить ключ или значение, определите место, где вы хотите поместить его, и выберите «**New**» из меню «**Edit**».

Чтобы изменить существующий ключ, выделите его в правой панели и выберите «**Modify**» из меню «**Edit**». Другой способ проделать то же самое, это щелчок правой кнопкой мыши на ключе или значении.

Файлы реестра располагаются в папке префикса, например:

```
/home/$USER/.wine_prefix/
```

- **system.reg** — содержит ветвь HKEY_LOCAL_MACHINE;
- **user.reg** — HKEY_CURRENT_USER;
- **userdef.reg** — HKEY_HKEY_USERS\.Default (содержит настройки Windows пользователя по умолчанию).

Установка winetricks

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Winetricks - вспомогательный скрипт для загрузки и установки различных распространяемых библиотек, необходимых для запуска некоторых программ в *Wine*, а также настройки окружения.

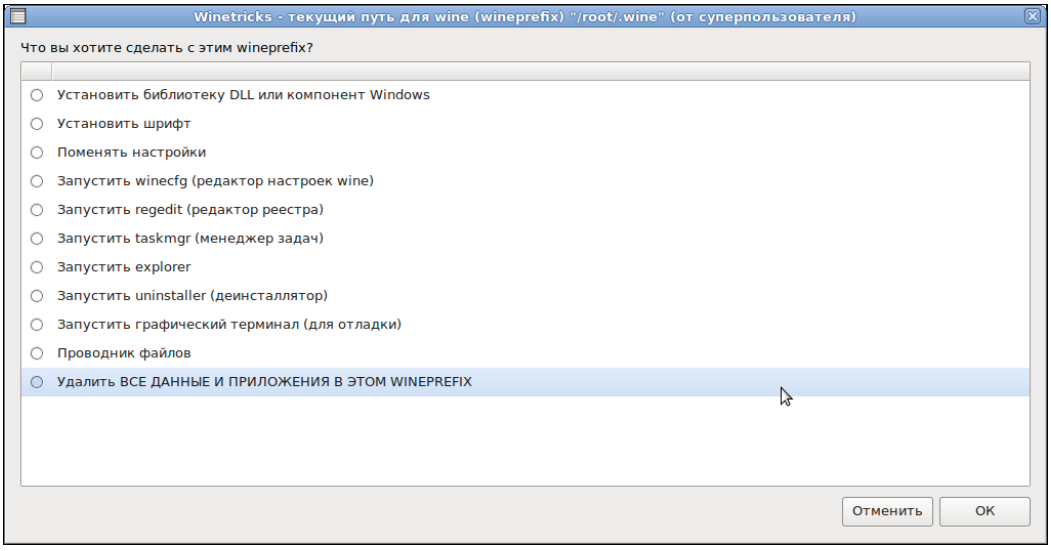
Для установки winetricks требуются права администратора:

```
# dnf install winetricks
```

Чтобы открыть диалоговое окно программы для работы в графическом режиме, необходимо вызвать команду:

```
winetricks
```

При выборе пункта меню, установленного по умолчанию, открывается следующее окно, которое содержит список доступных над wine-префиксом операций, где можно доустановить библиотеки, шрифты, вызвать редактор реестра или окошко настроек wine (**winecfg**).



Есть возможность установить пакеты напрямую через терминал:

```
winetricks <название_пакета>
```

Чтобы отобразить все установленные пакеты введите команду:

```
winetricks dlls list
```

Дополнительные возможности WINE

Пакет Dotnet
Пакет Mono
Установка Gecko
Виртуальный рабочий стол в Wine
Углубление в функционал Wine

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

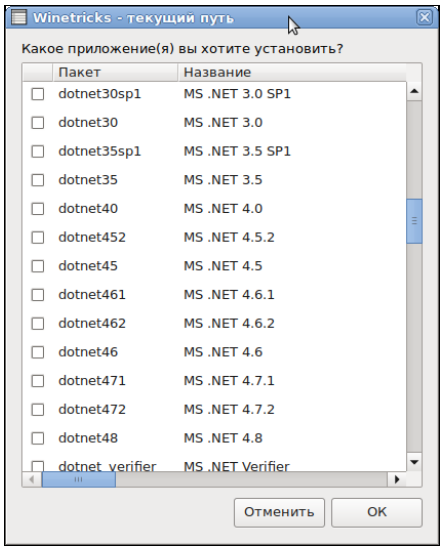
- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

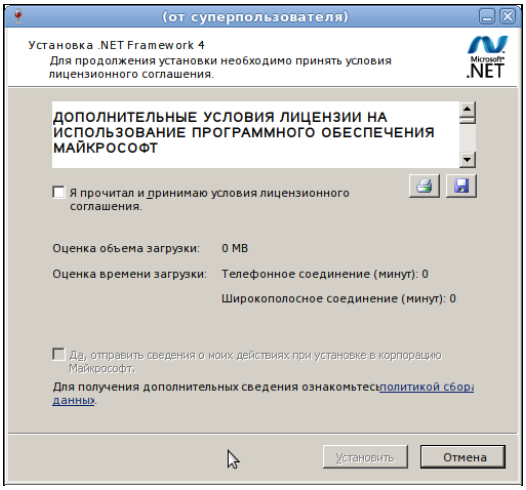
Пакет Dotnet

Для установки пакета в графическом режиме необходимо запустить **winetricks**.

При открытии окна выбрать пункт меню, установленный по умолчанию, затем необходимо выбрать пункт «**Установить библиотеку DLL или компонент Windows**». В списке приложений следует выбрать пакет для установки в зависимости от того, какая версия необходима, и нажать «**OK**».



Затем откроется окно установки программы, где необходимо изучить и принять условия лицензионного соглашения и следовать инструкциям по установке.



Для полуавтоматической установки (название и описание компонентов выводятся по ключу **-help**):

```
winetricks "components names"
```

Пример установки *.NET* Framework 4.5:

```
winetricks -q dotnet45
```

Пакет Mono

Mono — программная платформа, позволяющая разработчикам достаточно просто создавать развитые кроссплатформенные приложения.

В базовом варианте **Mono** состоит из нескольких компонентов:

- Компилятор языка C#;
- Среда исполнения **Mono** — состоит из среды исполнения (*CLI*) непосредственно, компилятора среды исполнения (*Just-In-Time, JIT*), генератора машинного кода (*Ahead-Of-Time, AOT*), загрузчика сборок, сборщика мусора, подсистемы управления многопоточностью и компонентов поддержки взаимодействия между сборками и *COM* (или аналогами в Linux, например *XCOM*);
- Базовая библиотека классов — набор стандартных классов, совместимых с классами *Microsoft .NET Framework;*
- Библиотека классов **Mono** — набор классов, поддерживающих дополнительные функции для разработки Linux-приложений. Например, классы для поддержки *Zip*, *OpenGL*, *Cairo*, *Gtk+*.

Данный пакет ставится автоматически при установке Wine из репозитория версии 4.4.

Установка Gecko

Gecko – это свободный движок вывода веб-страниц для браузера при работе в интернете **wine**. Если **wine** не работает с интернетом и вы не запускаете **windows.exe** браузер, то вам **Gecko** не нужен.

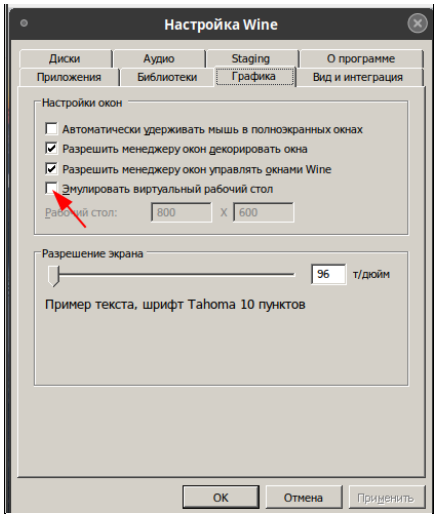
Обычно при запуске приложения для работы с веб-страницами *Wine* автоматически ищет *Gecko* сперва в **/usr/share/wine/gecko**. Если *Wine* не находит архив с *Gecko* там, то он автоматически загружает его из интернета, но некоторые приложения не любят ждать, пока загрузиться *Gecko* и зависают или вылетают.

Данный пакет ставится автоматически при установке Wine из репозитория версии 4.4.

Виртуальный рабочий стол в Wine

Имитация рабочего стола *Windows* в **wine** необходима для решения проблем, связанных с разрешением экрана, а также при сворачивании программ в **wine**.

Рабочий стол можно включить через **winecfg**.



Запущенная программа размещается в рамках виртуального рабочего стола.

Также есть возможность запустить рабочий стол, не используя интерфейс:

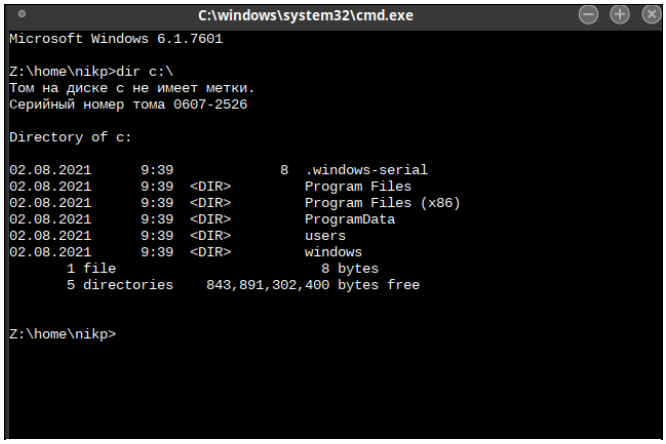
```
wine explorer /desktop="desk",800x600 regedit
```

- **explorer** — проводник *Windows*;
- **/desktop="desk",800x600 regedit** — создать рабочий стол с именем *desk* и разрешением *800x600*, затем запустить программу *regedit* (редактор реестра).

Углубление в функционал Wine

Wineconsole — позволяет запускать консоль *windows*, в основном используется для отладки.

```
wineconsole cmd
```



Wineserver — служба, исполняющая роль ядра Windows. Для каждого префикса запускается своя служба, что позволяет выполнять одновременно несколько программ из разных префиксов.

В случаях, когда программа зависла, поможет перезапуск **wineserver** (жесткая перезагрузка):

```
wineserver -k
```

или с префиксом:

```
WINEPREFIX="/home/$USER/.wine_prefix" wineserver -k
```

- **wineserver -d[n]:** — выводит отладочную информацию, имеет 3 уровня:
  - **0** — не выводит информацию;
  - **1** — выводит основную информацию;
  - **2** — выводит полную информацию.
- **wineserver -f:** — выводит сервер на передний план для упрощения отладки;
- **wineserver -p[n]:** — определяет время до остановки сервера, когда все клиентские процессы завершились, что позволяет быстрее запускать приложения, по умолчанию 3 секунды, если значение n не указано, сервер будет работать вечно;
- **wineserver -w:** — ожидает завершения предыдущей сессии ядра для корректного старта новой сессии.

Wineboot - выполняет инициализацию, запуск и перезагрузку префикса. Также выполняет симуляцию перезапуска и завершения работы программ (мягкая перезагрузка).

```
wineboot -r
```

Создание префикса через **wineboot**:

```
WINEPREFIX="/home/$USER/.wine_prefix" wineboot -i
```

- **-i** — инициализировать префикс.

Установка и запуск игр

Запуск с помощью AppImage
Установка игр из пакета
Установка игр через STEAM
Установка игр через платформу WINE
Установка игр через платформу Port Wine

Вы можете подробнее ознакомиться с возможностью установки игр на РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube**:
  - Как устанавливать игры в РЕД ОС;
  - Установка игр в РЕД ОС с помощью PortProton.
- в **Яндекс.Дзен**:
  - Как устанавливать игры в РЕД ОС;
  - Установка игр в РЕД ОС с помощью PortProton.
- в **VK Видео**:
  - Как устанавливать игры в РЕД ОС;
  - Установка игр в РЕД ОС с помощью PortProton.

На наших каналах вы также сможете найти много другой полезной информации.

Запуск с помощью AppImage

Большинство современных игр и программ требуют для своей работы дополнительные компоненты (библиотеки, утилиты и так далее). Это значит, что для того, чтобы запустить такую игру в РЕД ОС, нужно сначала дополнительно установить эти компоненты.

Для запуска игр и программ без привязки к дополнительным компонентам был разработан формат **AppImage**.

Ключевая идея AppImage заключается в том, что *одна программа – это один файл*. Программы в формате AppImage состоят всего из одного файла с расширением AppImage, например, *gimp.AppImage*.

Работать с программами в формате AppImage очень просто. Вы просто скачиваете программу, делаете файл программы исполняемым и запускаете. Ничего не нужно устанавливать, программа просто работает.

Поэтому сначала рассмотрим самый простой способ запуска игр – без установки. В этом случае пакет сразу готов к запуску. Для этого необходимо:

1. Скачать пакет с сайта с интересующим вас приложением или игрой через браузер по ссылке, например:

https://blub-game.com/download.html

или в терминале выполнить следующую команду:

```
$ wget https://blub-game.com/d/linux64/blubVolley.AppImage
```

2. Необходимо предоставить права на исполнение для полученного файла:

```
$ chmod +x blubVolley.AppImage
```

3. Последним шагом осталось запустить игру, выполнив команду:

```
$ ./blubVolley.AppImage
```

Приложение запускается в отдельном окне – так, как если бы оно было установлено у вас в системе.

Установка игр из пакета

Далее рассмотрим способ установки игры из готовых пакетов. Пакеты могут быть получены у стороннего разработчика или входить в используемый репозиторий. Для установки игры необходимо:

1. Скачать пакет(ы) через браузер по ссылке, например:

https://centos.pkgs.org/7/epel-x86_64/aisleriot-3.22.2-1.el7.x86_64.rpm.html

или в терминале выполнить следующую команду:

```
$ wget https://rpmfind.net/linux/epel/7/x86_64/Packages/a/aisleriot-3.22.2-1.el7.x86_64.rpm
```

2. От root-пользователя запустить локальную установку пакета с зависимостями, выполнив команду:

```
# dnf localinstall aisleriot-3.22.2-1.el7.x86_64.rpm
```

После установки пакета и зависимостей терминал выведет приблизительно следующее сообщение:

```
Установлено:
 aisleriot.x86_64 1:3.22.2-1.el7
Установлены зависимости:
 gc.x86_64 0:7.2d-7.el7 guile.x86_64 5:2.0.13-1.el7
Выполнено!
```

3. Запуск игры производится через *«Главное меню»* – *«Игры»*.



Рис. 1 - Запуск игры из пакета

Установка игр через STEAM

Для того чтобы установить и запустить игру через онлайн-сервис цифрового распространения компьютерных игр и программ Steam, необходимо с правами root-пользователя установить клиент **Steam**, выполнив команду:

```
# dnf install steam
```

В *«Главном меню»* - *«Интернет»* отобразится установленное приложение Steam, при нажатии на которое появится значок запуска на рабочем столе. После первого запуска Steam необходимо дождаться скачивания всех обновлений, а затем выполнить его настройку.

Сначала пользователю необходимо создать аккаунт Steam, если его еще не существует. Если аккаунт Steam уже есть, можно выполнить вход.

Далее для более удобной работы можно изменить языковые настройки в меню *«Steam»* - *«Settings»* - *«Interface»*. После смены языка потребуется перезапуск Steam.

Затем в меню *«Steam»* - *«Настройки»* необходимо выбрать пункт *«Совместимость»* и активировать функцию на *«Включить Steam Play для всех других продуктов»* (Рис. 2). Это нужно для того, чтобы Steam Play включался во всех играх библиотеки пользователя. Также требуется выбрать версию **Proton**, который будет способствовать запуску игр.

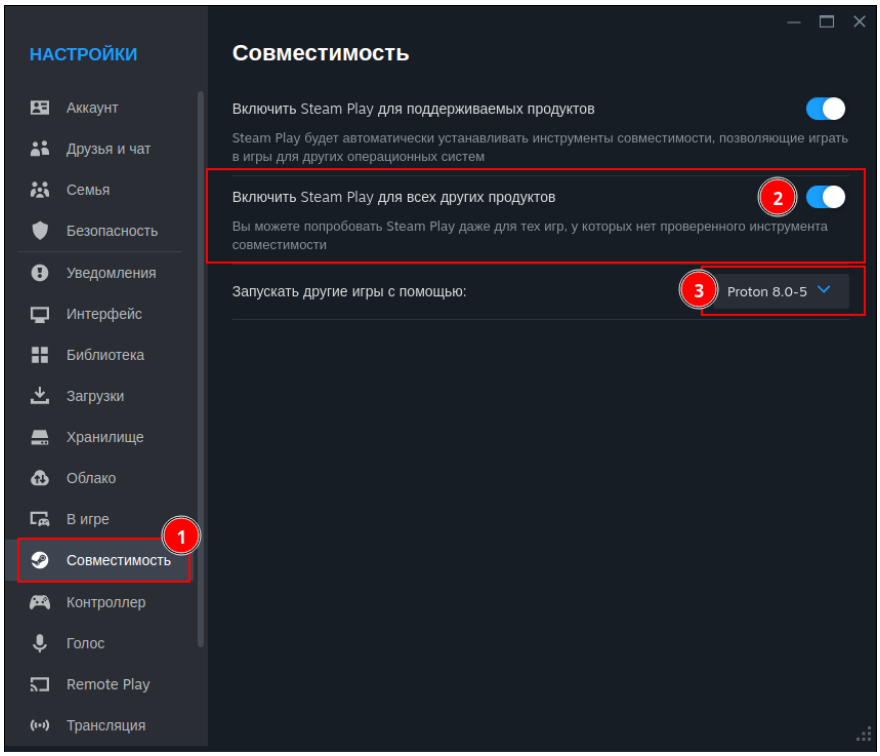


Рис. 2 – Установка флажка включения Steam Play

Существует сайт www.protondb.com, где перечислены все игры, поддерживаемые *Proton*, и указаны статусы к каждой игре. Перейдя в раздел с игрой, можно узнать более подробную информацию о возможности запуска игры, а также о дополнительных настройках, если при запуске возникают трудности.

После настройки Steam можно перейти в библиотеку пользователя или в магазин и скачать нужную игру. В данном случае с сайта *protondb.com* выбрана бесплатная нативная игра **«Toy Robot»**.

После скачивания игры необходимо перейти в библиотеку игр пользователя и нажать правой кнопкой мыши на игре из списка. В контекстном меню выбрать пункт *«Свойства...»*. Во вкладке *«Совместимость»* установить флажок на использование инструментов совместимости и выбрать необходимую версию Proton для запуска игры (Рис. 3).

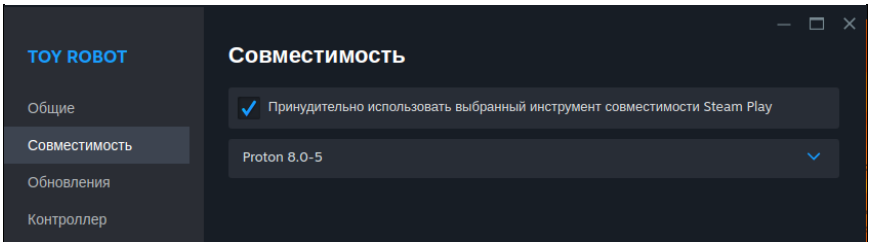


Рис. 3 – Установка флажка на использование Proton

На этом процедура настройки завершена. Можно запускать игру.

Установка игр через платформу WINE

WINE – это свободное программное обеспечение, позволяющее пользователям UNIX-подобных ОС исполнять 16-, 32- и 64-х битные приложения, том числе игры, созданные исключительно для *Microsoft Windows*, без наличия при этом установленной Microsoft Windows.

Название **W.I.N.E.** – рекурсивный акроним и расшифровывается как *«Wine Is Not an Emulator»* - «W.I.N.E. – это не эмулятор». Имеется в виду, что Wine не является эмулятором компьютера или виртуальной машиной, как Virtual Box и другие, Wine – это альтернативная, свободная реализация *Windows API*.

Для того чтобы установить Wine, необходимо в терминале с правами root-пользователя выполнить команду:

```
# dnf install wine
```

После установки в *«Главном меню»* появится раздел *«Wine»*, который включает в себя несколько программ:

1. ***Notepad*** – простой блокнот.

2. ***Regedit*** – инструмент для открытия реестра, также можно открыть в консоли, выполнив команду:

```
$ wine regedit
```

3. ***Wine Boot*** – инструмент, с помощью которого можно симулировать перезагрузку.

4. ***Wine Configuration*** – маленькая, но мощная утилита, которая позволяет настраивать Wine в соответствии с нуждами пользователя. *Winecfg* можно запустить под правами обычного пользователя через терминал, набрав команду:

```
$ winecfg
```

В *Winecfg* есть несколько вкладок, отвечающих за настройки Wine.

Вкладка *«Приложения»* позволяет создавать конфигурации, выбираемые при запуске в Wine определенных приложений, а также выбирать версию Windows для обеспечения совместимости.

Вкладка *«Библиотеки»* позволяет контролировать работу Wine с библиотеками Windows. Это особенно важно, т.к. некоторые приложения не совместимы с определенными версиями библиотек или требуют определенных нестандартных библиотек.

Вкладка *«Графика»* позволяет устранять проблемы с разрешением экрана или менеджером окон.

Вкладка *«Вид и интеграция»* позволяет менять внешний вид приложений, запущенных в Wine, если в этом есть необходимость.

Вкладка *«О программе»* содержит сведения о текущей версии Wine.

Вкладка *«Staging»* представляет собой набор чекбоксов, которые позволяют включать или отключать различные возможности, предоставляемые патчами.

Вкладка *«Аудио»* позволяет настраивать ввод и вывод звука. Вкладка *«Диски»* позволяет осуществлять доступ к подключенным устройствам.

5. ***Wine File*** – файловый менеджер.

После установки Wine в домашней папке пользователя будет создан профиль **.wine** (изначально он скрыт, чтобы отобразить профиль необходимо ПКМ нажать в пустом месте папки и выбрать пункт «Скрытые файлы»). Профиль создается конфигуратором Wine. Можно создавать несколько профилей, т.к. для разных программ могут требоваться разные дополнительные компоненты и разные настройки Wine. Для этого существуют ***префиксы*** Wine, благодаря которым можно избежать конфликтов и создать свое окружение для подобного рода программ.

Для создания нового профиля в *Wine Configuration* нужно указать путь к папке профиля через переменную окружения или в терминале выполнить следующую команду:

```
WINEPREFIX=~/.wine_for_games winecfg
```

Если папки не было изначально, она будет автоматически создана. Разные профили между собой не связаны, они существуют как несколько Windows на одном компьютере.

Чтобы установить заранее скачанную игру для Windows через Wine, необходимо в терминале выполнить команду:

```
$ wine [/путь_к _файлу/program.exe]
```

В нашем примере команда будет выглядеть следующим образом:

```
$ wine /home/user/Stalker/setup.exe
```

После выполнения команды запускается установщик пакета (Рис. 4), где предлагается выбрать папку установки, создание ярлыка, а также язык и установку дополнительного ПО.



Рис. 4 – Подготовка к установке игры

После выбора всех нужных пунктов необходимо нажать кнопку *«Установить»*, начнется процесс установки игры. После установки игры следует нажать кнопку *«Завершить»*. Игра установлена и готова к запуску.

Установка игр через платформу Port Wine

Port Wine – это модифицированная версия *Wine*, которая позволяет запускать более сложные и энергоемкие игры в Linux, которые не поддерживает обычный *Wine*.

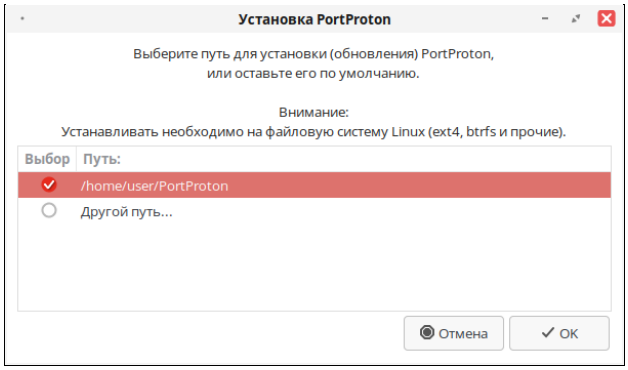
Для корректной работы **PortWine** необходимо сначала установить дополнительные пакеты:

```
dnf install curl icoutils libcurl wget zenity bubblewrap zstd cabextract tar goverlay openssl steam
```

После этого необходимо скачать установочный файл **PortWine** и запустить его установку:

```
wget -c "https://github.com/Castro-Fidel/PortProton_ALT/raw/main/portproton" && sh portproton
```

Появится окно настройки параметров перед установкой - необходимо будет выбрать путь установки **PortProton**.



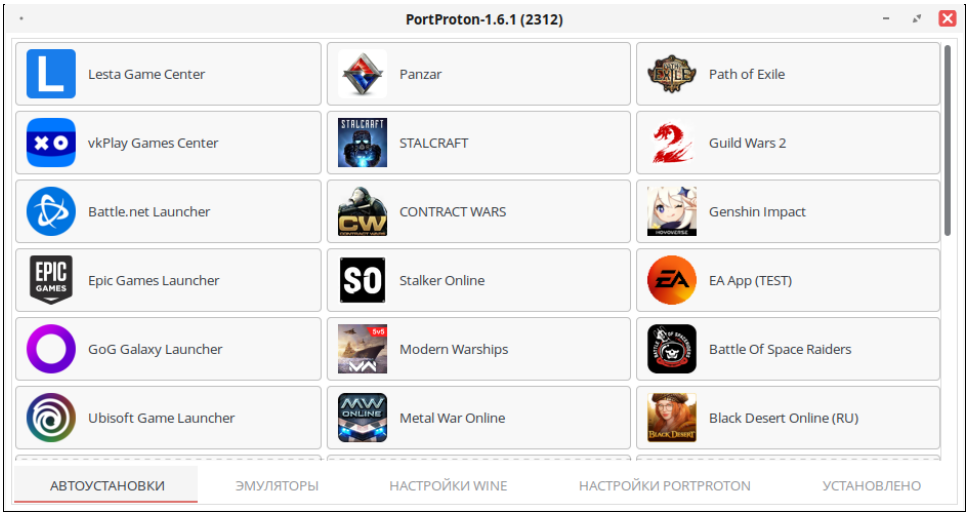
Начнется процесс установки.

После завершения установки программа будет доступна из «**Главного меню**» - «**Игры**» - «**PortProton**».

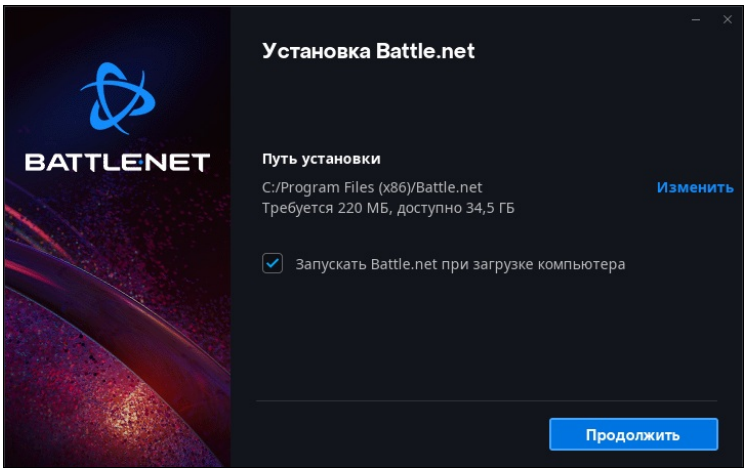
При первом запуске произойдет автоматическая загрузка необходимых библиотек и инициализация приложения.



После завершения первого запуска будет открыто окно с выбором необходимого лаунчера:



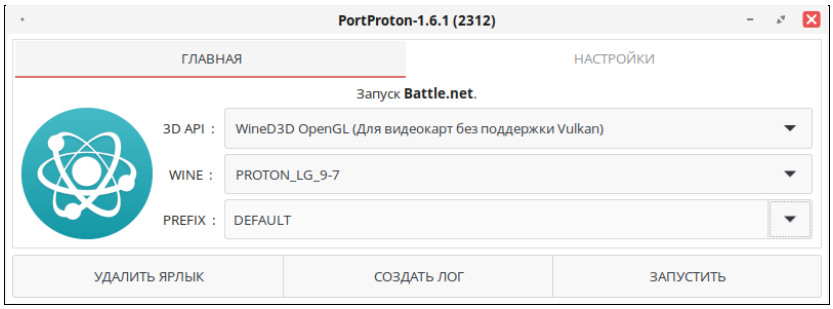
Выберите **Battle.net Launcher**. При первом запуске лаунчера также произойдет обновление конфигураций. Далее появится окно установщика **Battle.net**.



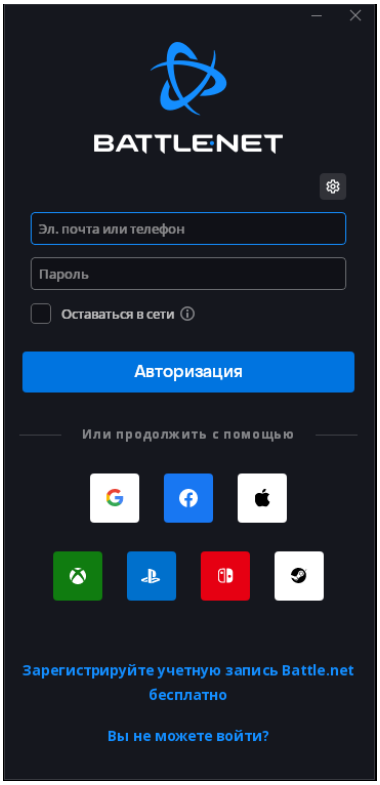
Для запуска установки нажмите «**Продолжить**».

После завершения установки будет выведено информационное окно, в котором необходимо указать, добавлять ли значок **Battle.net** в «**Главное меню**» - «**Игры**».

Запустите программу и установите необходимые настройки для запуска. Выбор зависит от возможностей используемой видеокарты.



После запуска **BattleNet** откроется окно авторизации пользователя.

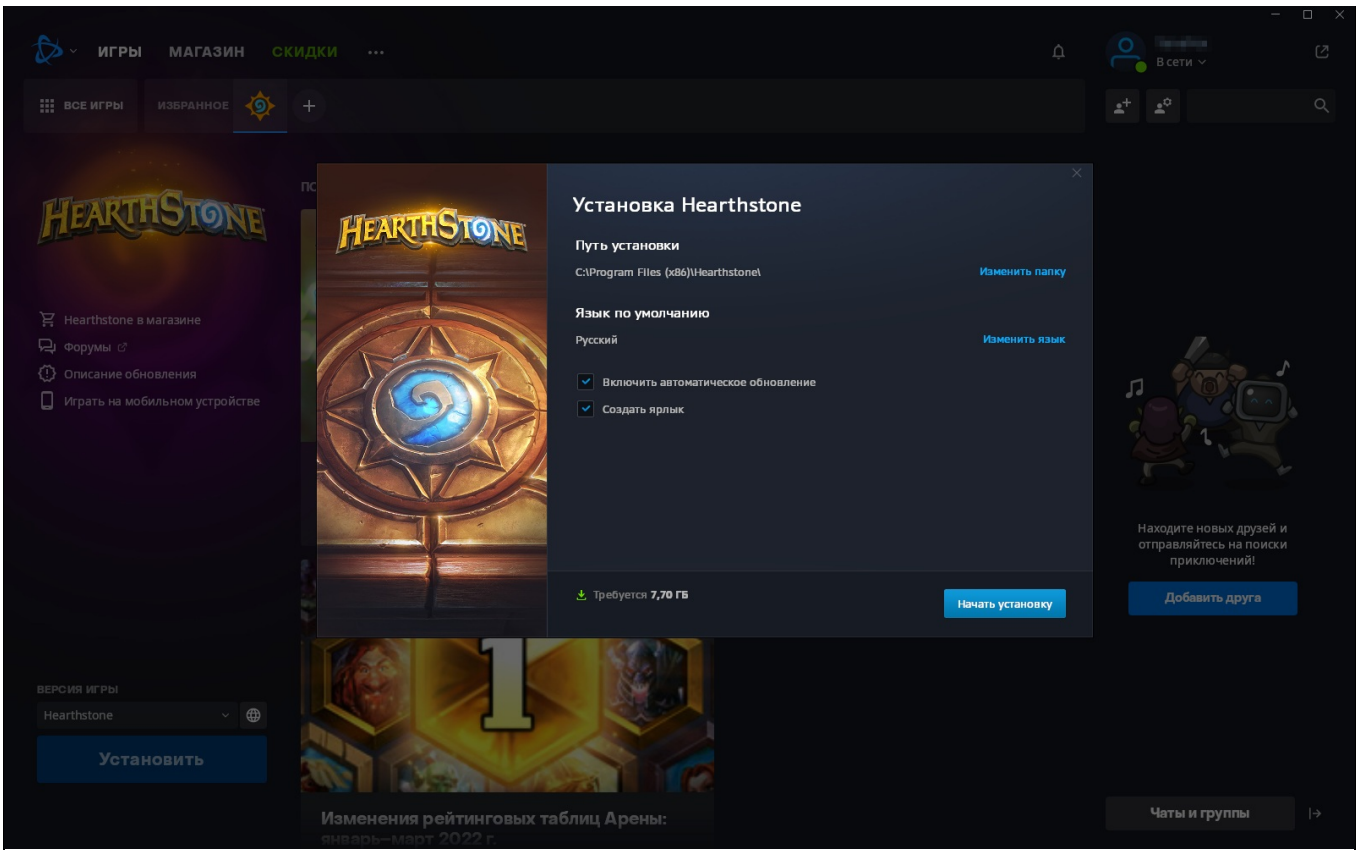


Если аккаунт в системе уже есть, просто выполняется вход, если же его нет, необходимо зарегистрироваться.

При регистрации необходимо указать дату рождения, имя и фамилию, номер телефона (необязательное поле) и адрес электронной почты. Далее потребуется указать имя пользователя в системе или оставить случайно сгенерированное имя и установить пароль для входа в систему. После этого регистрация завершится и будет выполнен вход в учетную запись.

Из списка игр следует выбрать интересующую (в данном случае **Hearthstone**) и нажать на кнопку «**Установить**».

После этого откроется окно менеджера установки, где потребуется выбрать путь к игре, включение или отключение автоматических обновлений и создание ярлыка на рабочем столе. После настройки необходимо нажать кнопку «**Начать установку**» для скачивания и установки игры.



После завершения установки игра будет доступна для использования.



Автоматическое исправление ввода текста с помощью XNeuralSwitcher

Установка
Описание программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** xneur-1:0.20.0-5, gxneur-1:0.20.0-4

X Neural Switcher — программа для автоматического переключения раскладок клавиатуры, в зависимости от набираемого текста. Т.е. при наборе текста, если он набирается на неверном языке, программа автоматически (или по запросу) переключит язык на нужный.

Вы можете подробнее ознакомиться с возможностями программы **X Neural Switcher**, просмотрев наши обучающие видео:

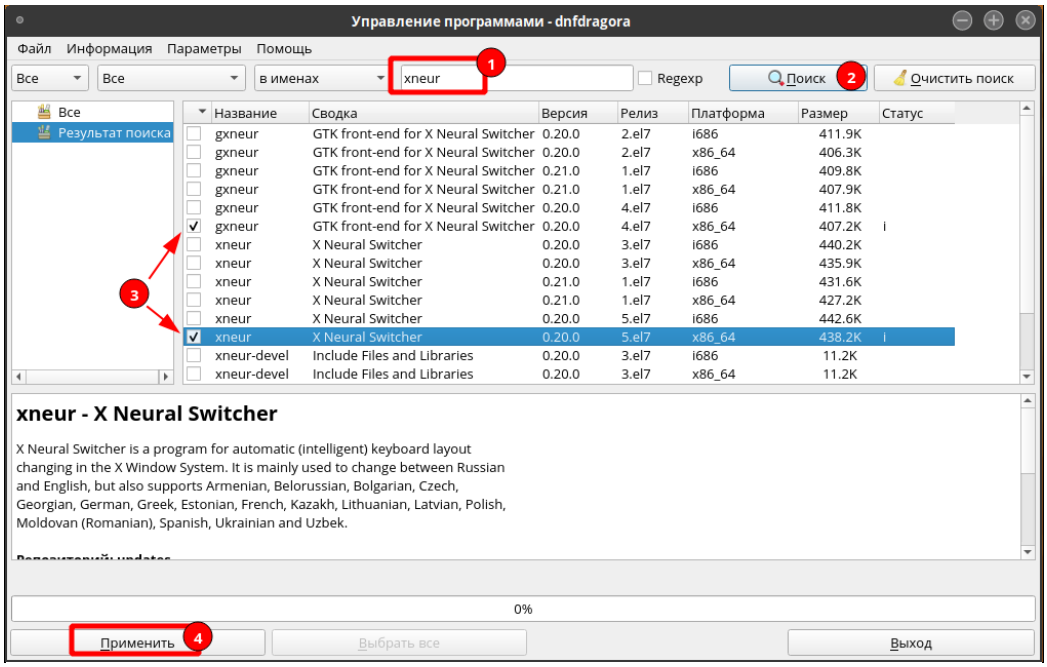
- на **RuTube** — Авто-исправление ввода текста;
- в **Яндекс.Дзен** — Авто-исправление ввода текста;
- в **VK Видео** — Авто-исправление ввода текста.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**xneur**» и отметьте флагом пакеты последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install gxneur xneur
```

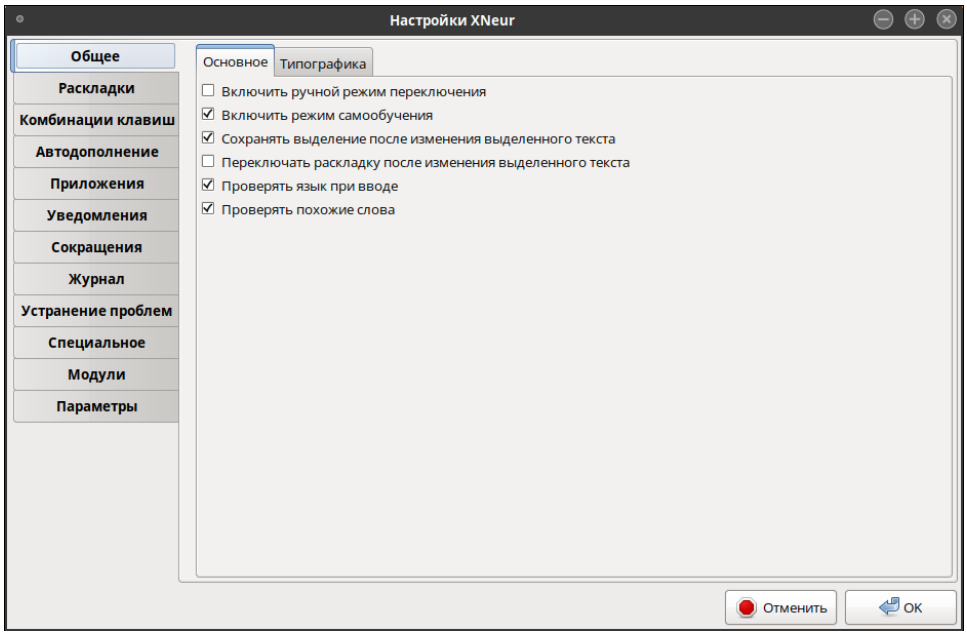
Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Специальные возможности**» - «**Переключатель раскладок клавиатуры**».

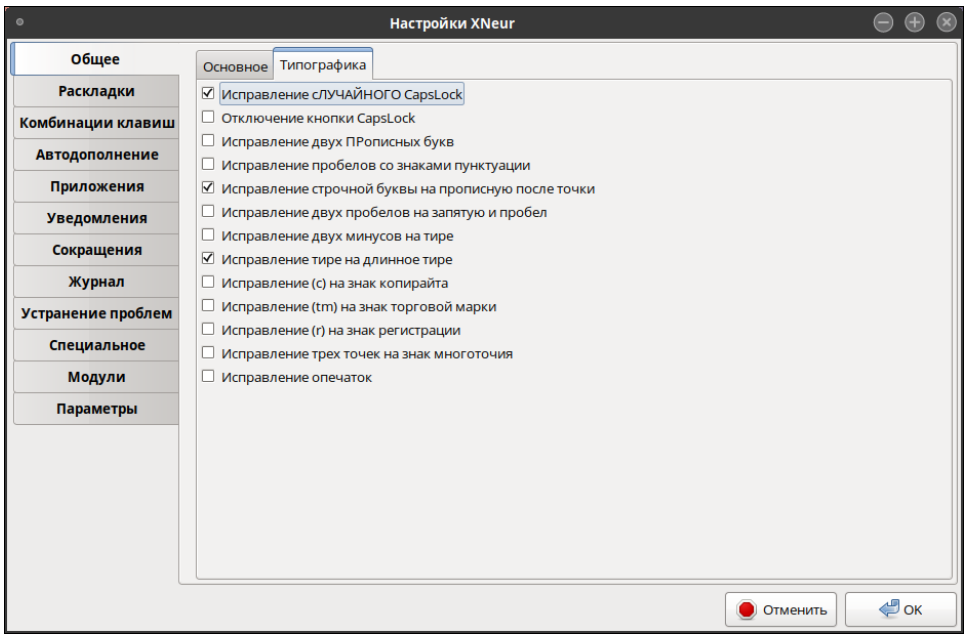
Описание программы

После запуска в системном трее появится соответствующий значок (). Нажмите по нему ПКМ и в контекстном меню выберите «**Параметры**» — здесь доступна детальная настройка программы.

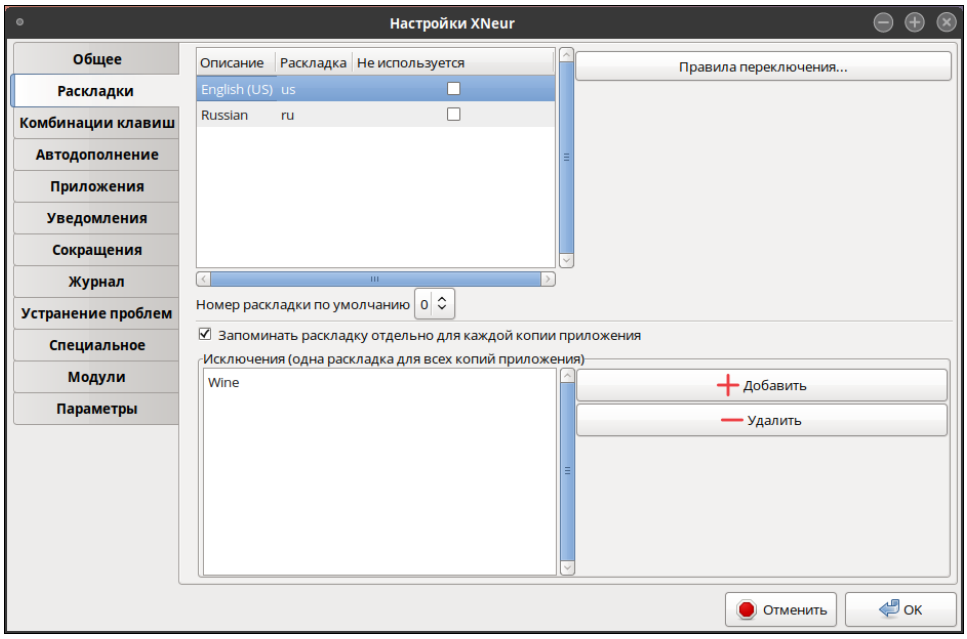
В разделе «**Общее**» на вкладке «**Основное**» доступны настройки включения ручного режима переключения, а также отключение режима самообучения. Функция самообучения полезна при использовании трудных слов, которые не попадают под словарные, а также сокращенных аббревиатур. Если несколько раз исправить аббревиатуру, нажав «**Break**», **xneur** запомнит ее и не будет исправлять.



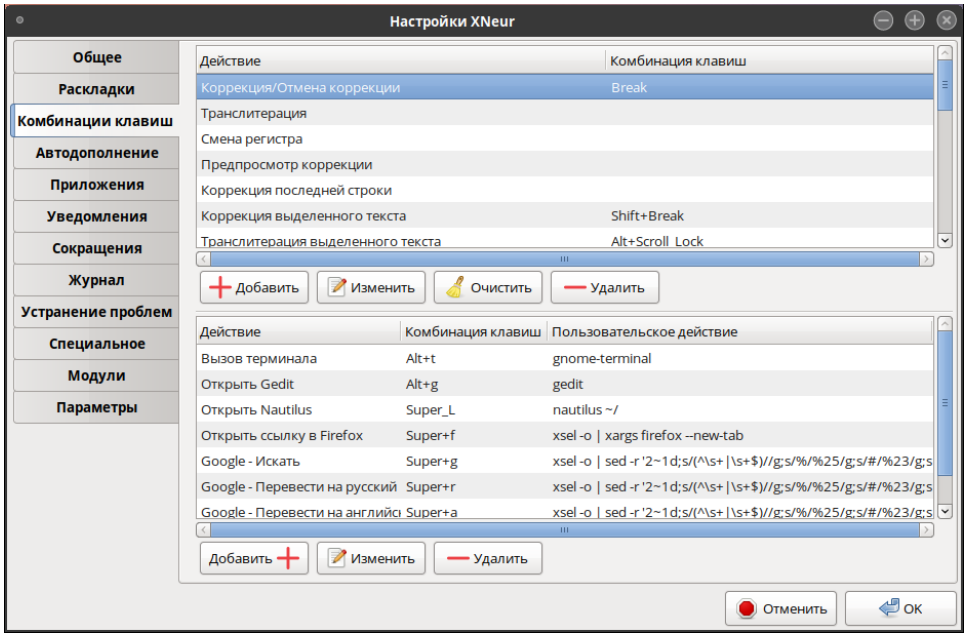
На вкладке «**Типографика**» доступны настройки по исправлению случайного *CapsLock*, двух ПРописных букв, а также много удобных и полезных функций, в том числе замена определенных последовательностей символов на знаки копирайта, торговой марки, регистрации и т. д.



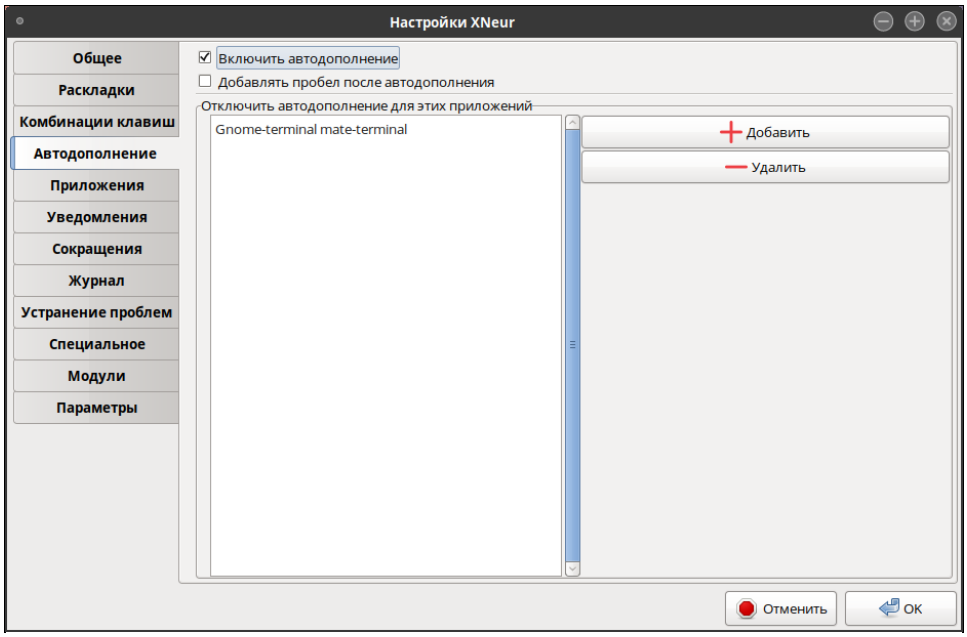
В разделе «**Раскладки**» можно указать одну раскладку для всех копий приложения или в каждой использовать свою личную.



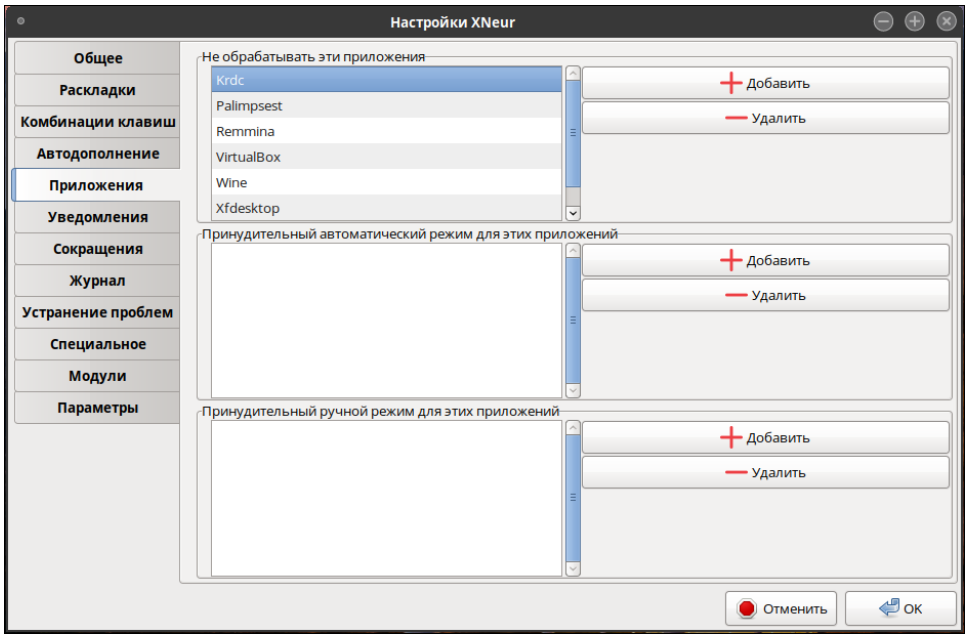
В разделе «**Комбинации клавиш**» есть возможность назначить свои сочетания клавиш для скриптов или запуска приложений. При работе в ручном режиме **xneur** не отслеживает набор, но позволяет автоматически изменять раскладку последнего набранного слова (кнопка «**Pause/Break**»), последней набранной строки (сочетание клавиш «**Ctrl+Break**»), выделенного текста (сочетание клавиш «**Shift+Break**»), а также настраивать другие полезные функции. Вы можете назначить удобное для вас сочетание клавиш.



В разделе «**Автодополнение**» по умолчанию включено автоматическое дополнение часто набираемых слов. Можно включить добавление пробела после дополненного слова и настроить данную функцию для отдельных приложений, например, по-умолчанию она отключена для терминала.



В разделе «**Приложения**» можно указать приложения, в которых **xneur** будет работать в автоматическом режиме, ручном режиме или не будет работать вообще.



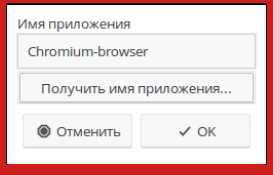
ВАЖНО!

В некоторых приложениях могут возникать проблемы с автоматическим исправлением текста, например:

- некорректное исправление текста;
- невозможность ввода текста;
- невозможность ручного переключения раскладки клавиатуры и пр.

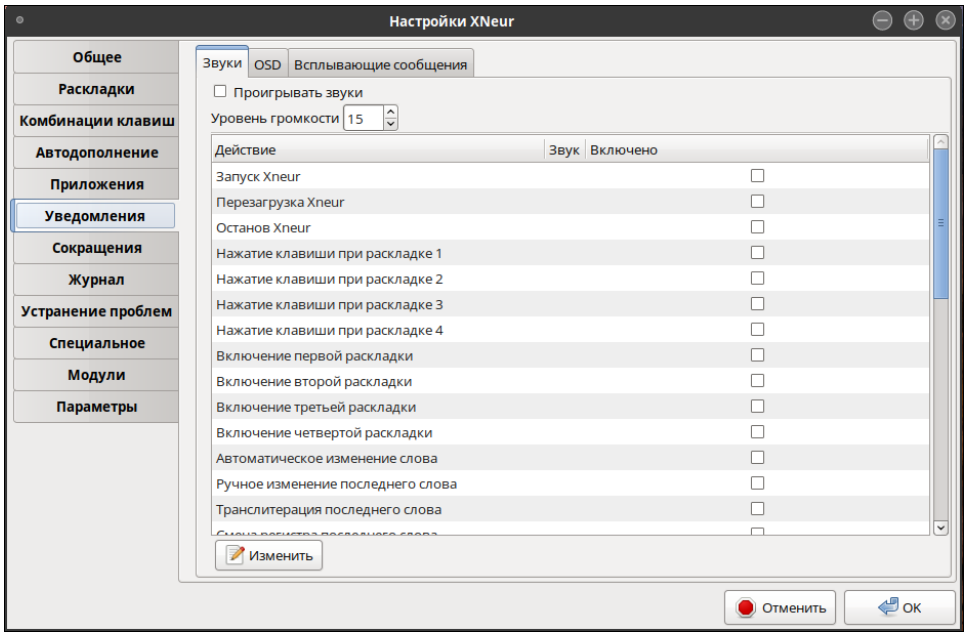
Во избежание возникновения подобных проблем рекомендуется добавлять такие приложения в исключения. Для этого в разделе «**Приложения**» в секции «**Не обрабатывать эти приложения**» нажмите «**Добавить**» и в появившейся форме укажите наименование приложения.

В форме также доступно автоматическое определение наименования того или иного приложения. Достаточно нажать на «**Получить имя приложения...**» и щелкнуть ЛКМ по открытому окну приложения, в котором наблюдаются проблемы.

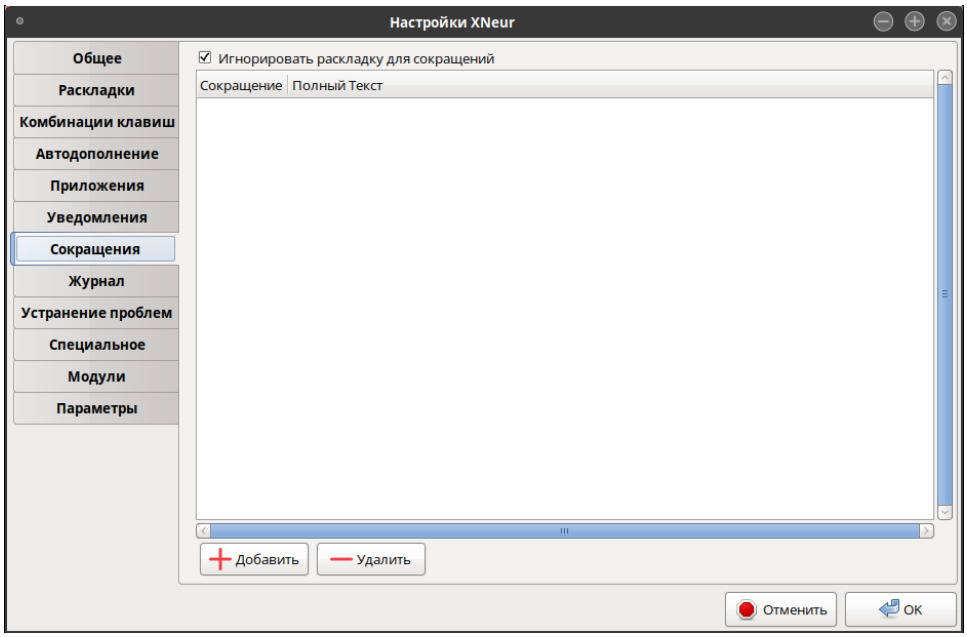


Раздел «**Уведомления**» позволяет настраивать звуковое сопровождение для выбранных действий, выводить экранные или

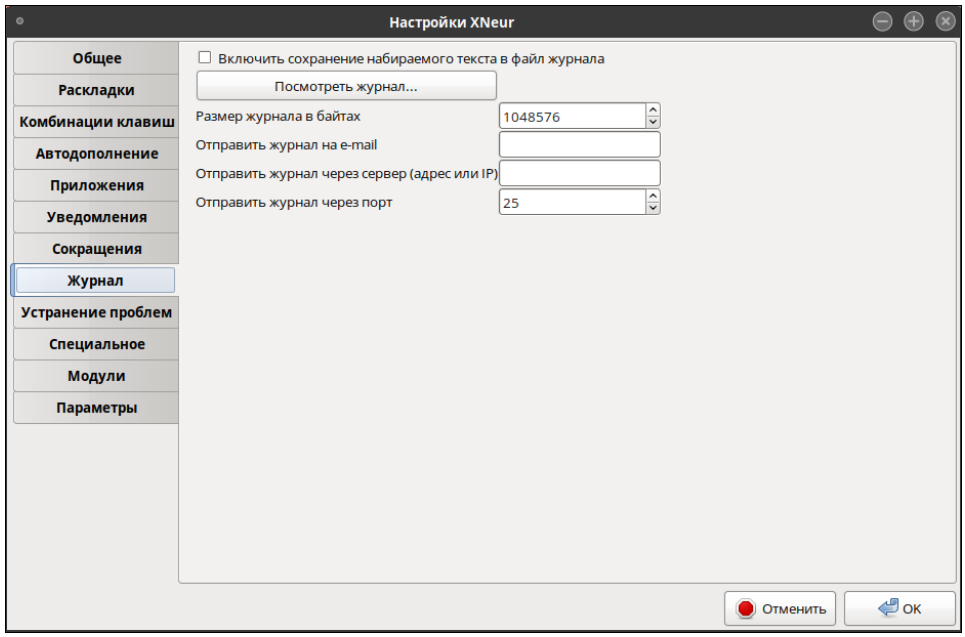
всплывающие уведомления о переключении.



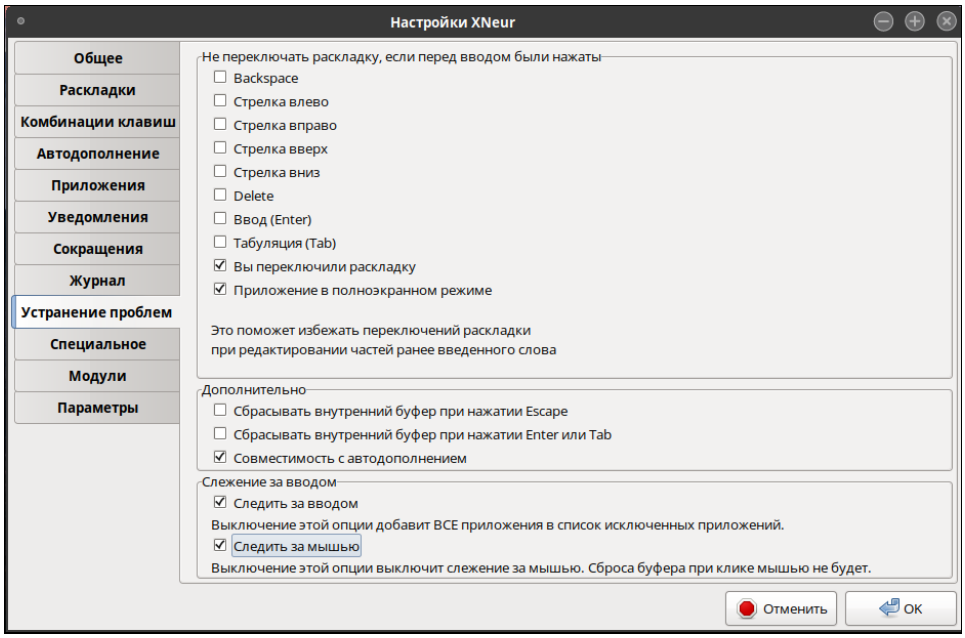
В разделе «**Сокращения**» можно настроить замену собственным сокращениям. Напечатав всего две буквы и нажав собственное сочетание клавиш, у вас появится необходимое предложение.



В разделе «**Журнал**» можно включить сохранение набираемого текста, а затем просмотреть набранный текст с разбивкой по дате и по приложению, в котором он был набран.

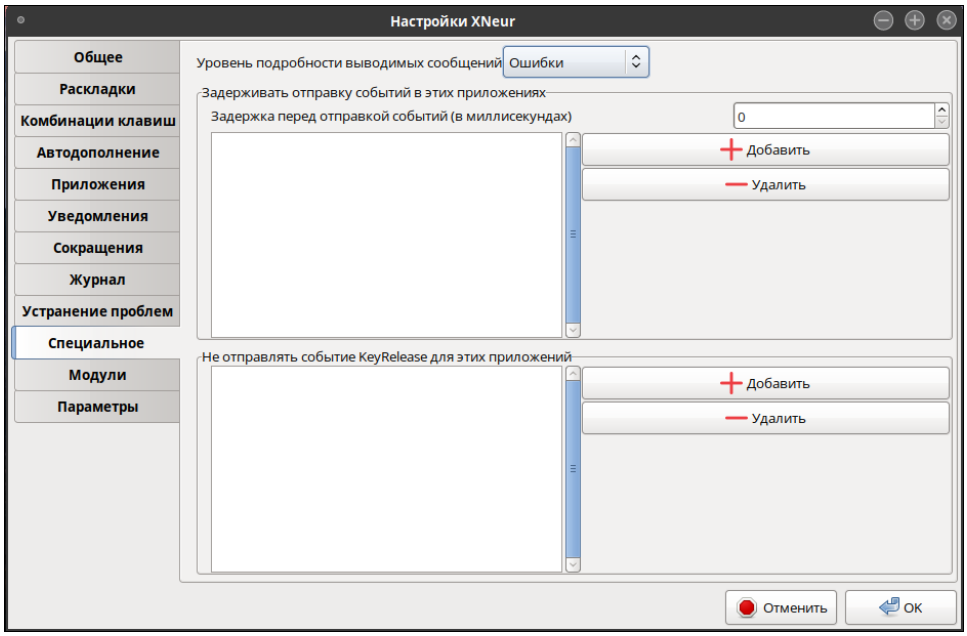


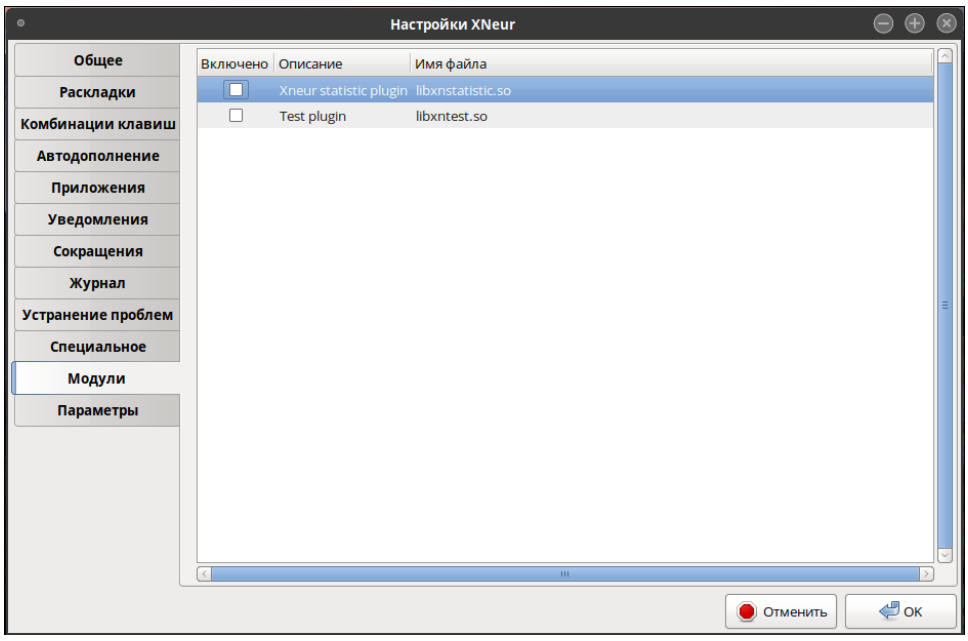
В разделе «**Устранение проблем**» перечислены тонкие настройки. Если вы часто играете в полноэкранные игры, вы можете отключить **xneur** во всех полноэкранных приложениях.

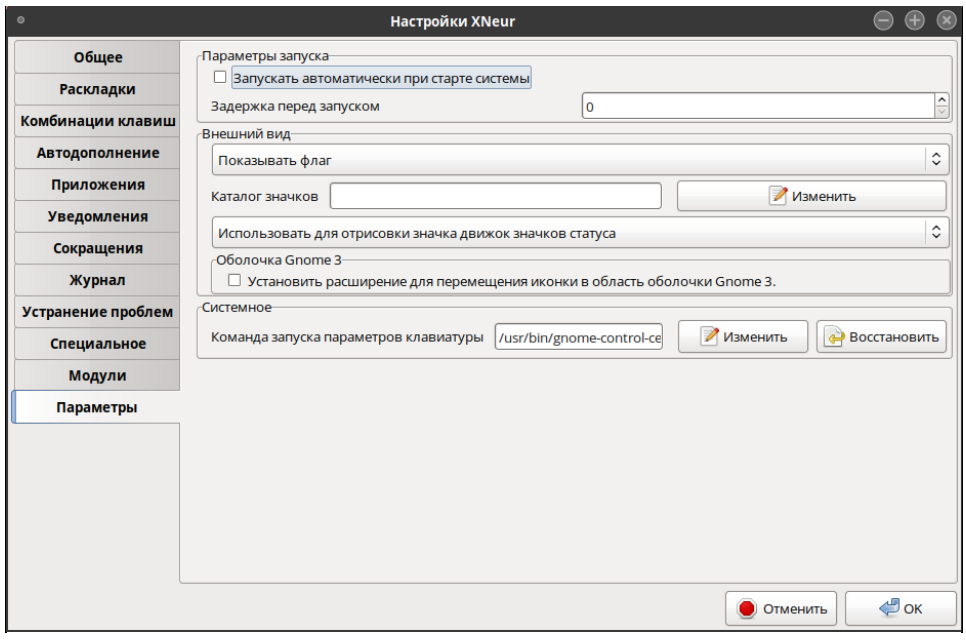


Далее расположены разделы «**Специальное**», «**Модули**» и «**Параметры**».

В разделе «**Параметры**» можно включить опцию запуска программы при старте системы. При необходимости также можно настроить задержку перед запуском.







Несомненным плюсом является включение и отключение различных опций, что позволит максимально удобно настроить работу приложения персонально для каждого пользователя.

Для сохранения настроек нажмите «**OK**».

CherryTree – программа систематизации и ведения заметок

Базовые функции cherrytree
Вкладки cherrytree
Параметры cherrytree

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** cherrytree-0.38.11-1

Cherrytree - это удобное приложение для записи коротких заметок, позволяющее иерархически структурировать всю нужную информацию в наглядном виде. Утилита может выступать в качестве текстового редактора, позволяя вставлять в текст таблицы, изображения, ссылки и другие элементы.

Установка производится командой:

```
dnf install cherrytree
```

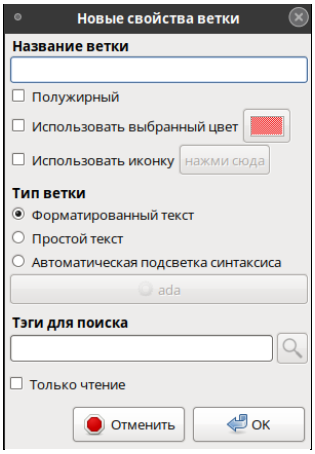
Вы можете подробнее ознакомиться с настройкой и работой утилиты **cherrytree**, просмотрев наши обучающие видео:

- на **RuTube** — CherryTree - программа систематизации и ведения заметок;
- в **Яндекс.Дзен** — CherryTree - программа систематизации и ведения заметок;
- в **VK Видео** — CherryTree - программа систематизации и ведения заметок.

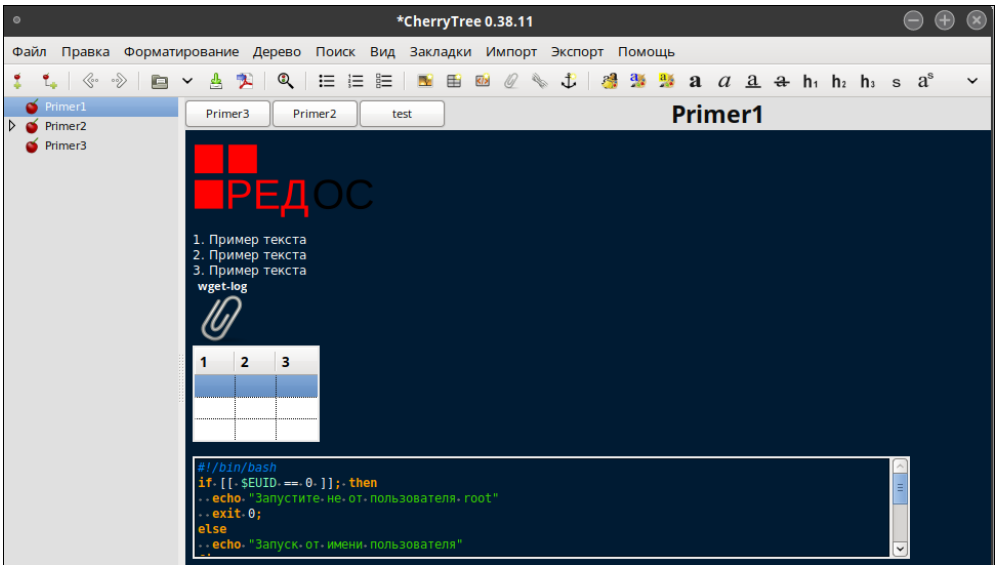
На наших каналах вы также сможете найти много другой полезной информации.

Базовые функции cherrytree

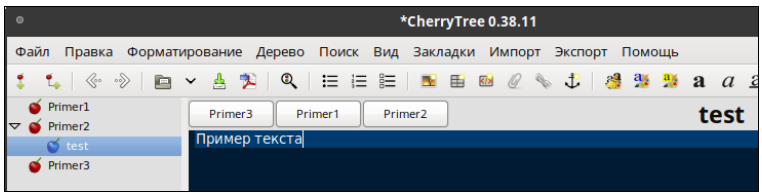
Программа представляет собой иерархическую структуру для хранения информации. Для добавления нового дерева необходимо нажать на иконку «**Добавить ветку с тем же родителем**», либо в верхнем меню выбрать пункт «**Дерево**», в котором будут находиться расширенные настройки ветвей. Необходимо задать название и выбрать тип ветки:



Созданную ветку можно использовать как текстовый редактор, в котором можно добавить изображение, таблицу, ссылку на файл или веб-сайт, так же можно вставить блок кода разных языков программирования. Для применения вышеперечисленных функций используйте верхнюю панель инструментов:

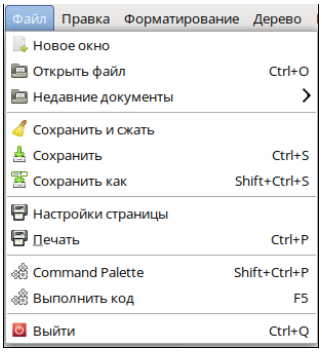


Для каждой ветки можно добавить дочернюю ветвь, для её добавления нажмите правой кнопкой мыши по необходимой ветке и выберите «**Добавить дочернюю ветвь**». В ней также можно хранить информацию, при нажатии на стрелочку возле основной ветви будет открываться дочерняя ветвь:

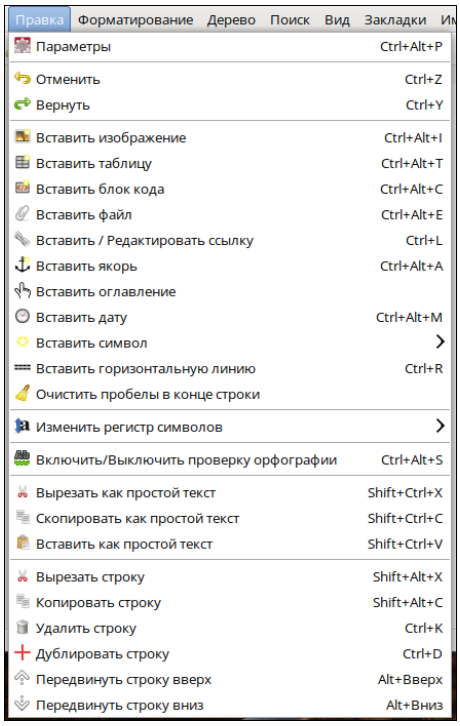


Вкладки cherrytree

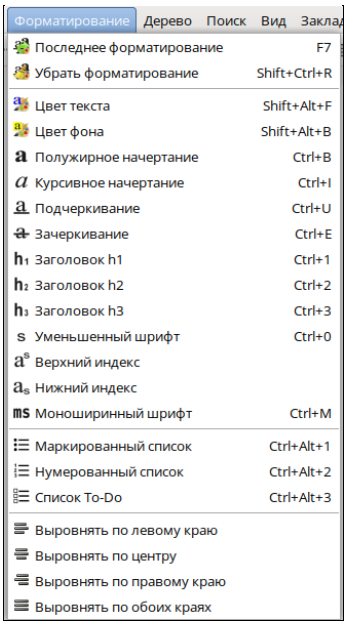
Вкладка «**Файл**» - позволяет сохранить текущий файл или открыть новый, настроить печать и выполнить код.



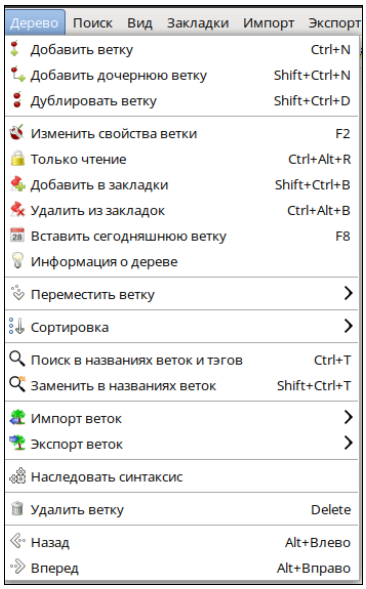
Вкладка «**Правка**» - позволяет перейти в параметры, отменить или вернуть действие, применить базовые функции и т.д.



Вкладка «**Форматирование**» - позволяет изменить настройки текста: цвет, фон, выравнивание, нумерация и т.д.



Вкладка «Дерево» - позволяет добавить или дублировать ветки, изменить свойства, отсортировать, импортировать или экспортировать ветки и т.д.



Вкладка «**Поиск**» - позволяет осуществлять поиск по определённым, либо по всем веткам.

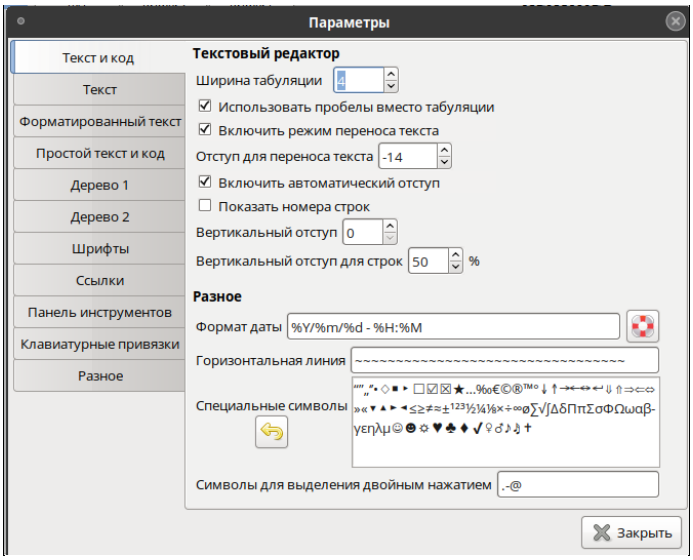
Вкладка «**Вид**» - позволяет настроить видимые части интерфейса программы.

Вкладка «**Закладки**» - позволяет переходить на ранее сохранённые ветви.

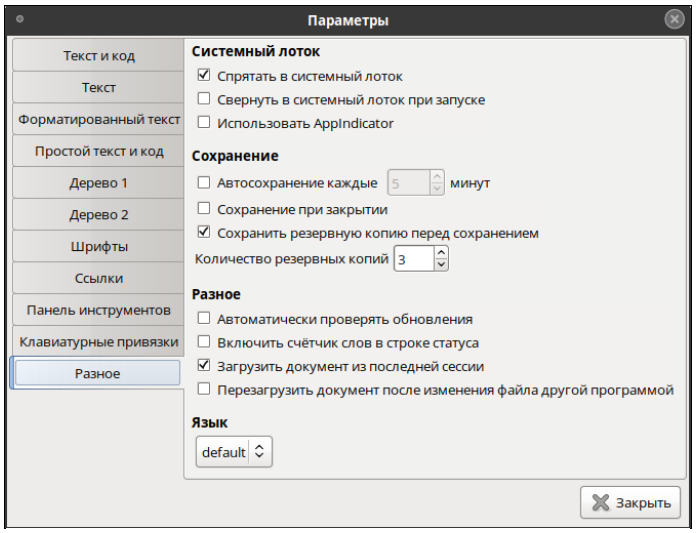
Вкладки «**Импорт/Экспорт**» - позволяют импортировать или экспортировать файл в разные форматы (PDF, HTML, текстовый файл, документ CherryTree).

Параметры cherrytree

В параметрах утилиты можно настроить формат текста, интерфейс деревьев, изменить кнопки на панели управления, добавить горячие клавиши и т.д.



Программу можно добавить в системный трей. Для добавления зайдите в раздел «**Разное**» и поставьте галочки «**Спрятать в системный лоток**» или «**Свернуть в системный лоток при запуске**».


Параметры
Текст и код
Текст
Форматированный текст
Простой текст и код
Дерево 1
Дерево 2
Шрифты
Ссылки
Панель инструментов
Клавиатурные привязки
Разное
Системный лоток
Спрятать в системный лоток
Свернуть в системный лоток при запуске
Использовать AppIndicator
Сохранение
Автосохранение каждые
5
минут
Сохранение при закрытии
Сохранить резервную копию перед сохранением
Количество резервных копий
3
Разное
Автоматически проверять обновления
Включить счётчик слов в строке статуса
Загрузить документ из последней сессии
Перезагрузить документ после изменения файла другой программой
Язык
default
Закрыть

ClipIt – менеджер буфера обмена

Clipit — удобный менеджер буфера обмена. Легковесное и простое в использовании приложение, которое позволяет сохранить историю работы с буфером обмена для дальнейшего использования ранее помещенного в него текста.

Вы можете подробнее ознакомиться с работой в **ClipIt**, просмотрев наши обучающие видео:

- на **RuTube** — ClipIt - менеджер буфера обмена;
- в **Яндекс.Дзен** — ClipIt - менеджер буфера обмена;
- в **VK Видео** — ClipIt - менеджер буфера обмена.

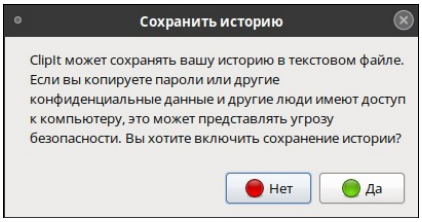
На наших каналах вы также сможете найти много другой полезной информации.

Устанавливается следующей командой:

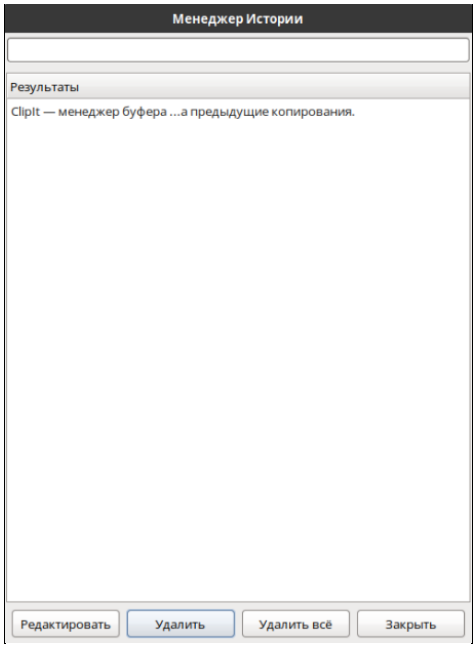
```
dnf install clipit
```

Для запуска необходимо перейти в *«Меню» - «Стандартные» - «Clipit»*.

При первом запуске программа предложит вам включить сохранение истории.



Программа при запуске добавляет свой значок в панель задач. При клике на значок открывается выпадающее меню со списком последних копирований в буфер обмена (история копирований). Если кликнуть по какому-либо элементу в истории, то соответствующий текст автоматически попадет в буфер обмена.



Если стартовые настройки программы вам не подходят, то при помощи пункта меню «*Параметры*» можно произвести более тонкую донастройку.

В настройках программы *Clipit* можно:

- указать количество элементов, которые необходимо хранить в истории (значение от 5 до 1000);
- задать количество элементов, которые будут отображаться в выпадающем меню (значение от 5 до 100);
- выполнить настройки внешнего вида меню;
- добавить фильтры, чтобы текст, удовлетворяющий фильтру, не попадал в историю (в качестве фильтра необходимо задать регулярное выражение).

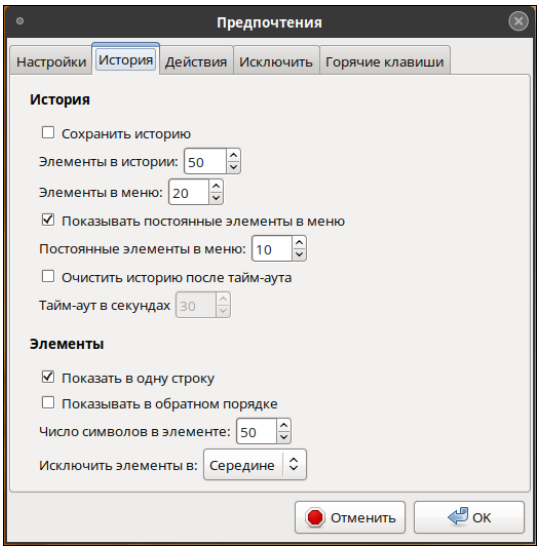
Clipit поддерживает использование горячих клавиш. Например, чтобы открыть выпадающее меню с историей, нужно нажать «**Ctrl+Alt+H**». Меню при этом отображается сразу рядом с курсором мыши, и вы можете тут же выбрать любой элемент. Переназначить горячие клавиши можно в настройках программы во вкладке «*Горячие клавиши*».

Установка количества элементов, которые должны храниться в истории и которые будут отображаться в выпадающем меню, осуществляется на вкладке «*История*».

Если указанное количество элементов в меню меньше указанного количества элементов в истории, то при превышении указанного в настройках предела элементов в меню более старые элементы автоматически скрываются.

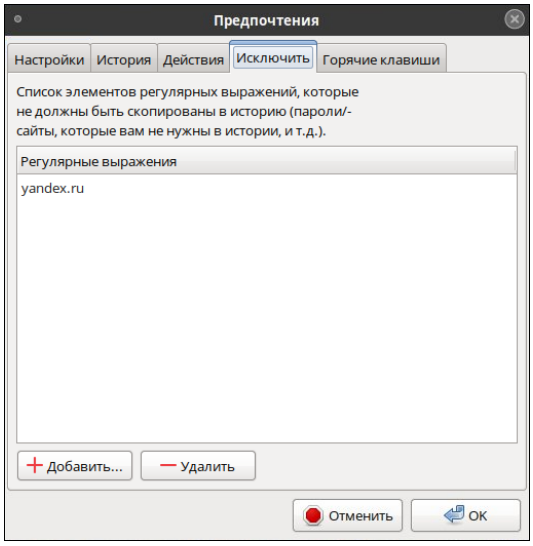
Если в процессе работы вам необходимо будет вернуться к скрытым элементам, необходимо будет выбрать пункт «*Управление историей*» в меню программы, затем найти нужный элемент и дважды кликнуть по нему левой кнопкой мыши.

Однако если превышен указанный предел элементов в истории, то самые старые элементы удаляются.



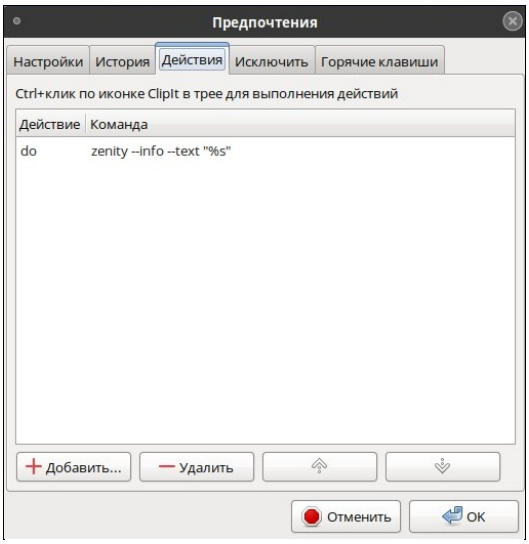
Clipit также поддерживает исключение списка элементов регулярных выражений, которые не должны быть скопированы, например, пароли или важная информация, которые не нужны в истории.

Например, при добавлении в регулярные выражения сайта **yandex.ru** данная ссылка не будет скопирована в историю.

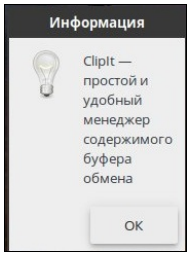


Программа также дает возможность создавать действия во вкладке настроек « *Действия*».

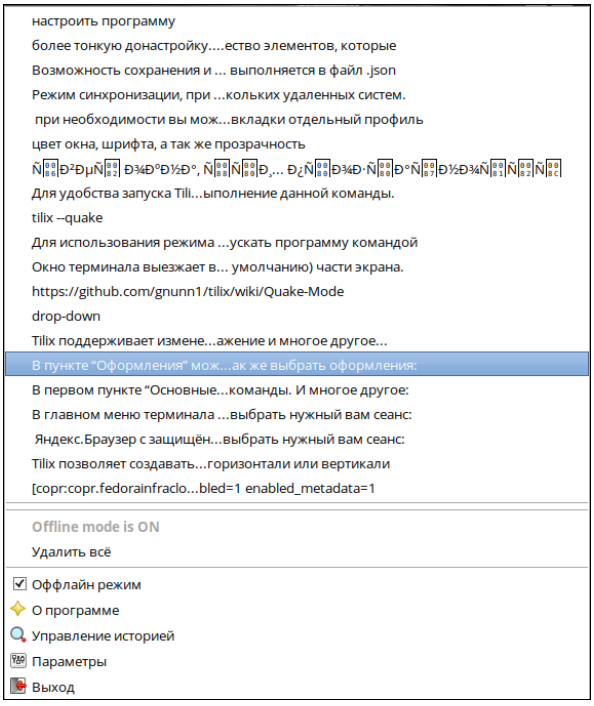
Действия — это какие-либо команды, которые вы можете выполнять над элементами в списке истории. Например, определим действие **do** и команду **zenity --info --text "%s"**.



При выполнении действия (сочетание клавиш «**Ctrl+Alt+A**») будет получено всплывающее окно с текстом из буфера обмена.



В меню программы присутствует галочка «*Оффлайн режим*», при её включении скопированный текст не будет попадать в менеджер истории, а в меню появится информационное сообщение «**Offline mode is ON**».



Торренты

Принцип работы
qbittorrent
transmission

В настоящее время компьютерные файлы уже не такие легковесные, как раньше, и даже короткие HD-видео могут иметь размер более гигабайта. Проблема в том, что чем файл больше, тем труднее им поделиться.

Если большое число пользователей одновременно будут пытаться получить доступ к большому файлу, то работа даже мощного сайта может быть очень медленной. В итоге даже может произойти сбой загрузки. Для решения данной проблемы были созданы торренты.

Торренты – это способ распространения данных. Торренты передают данные по протоколу **BitTorrent**. Скачивая файл через **BitTorrent**, загрузка идет тем быстрее, чем большее количество людей участвует в ней. Это работает с любыми типами файлов.

Вы можете подробнее ознакомиться с торрентами, просмотрев наши обучающие видео:

- на **RuTube** — Торренты и как с ними жить;
- в **Яндекс.Дзен** — Торренты и как с ними жить;
- в **VK Видео** — Торренты и как с ними жить.

На наших каналах вы также сможете найти много другой полезной информации.

Принцип работы

Большой файл условно разбивается на маленькие блоки. Программе, работающей по протоколу **BitTorrent**, для начала процесса скачивания большого файла необходима служебная информация обо всех этих блоках. Эта информация хранится в файле, который называется торрент. **Торрент** - это служебный файл, содержащий всю информацию о нужном файле, и о его частях, которые нужны для завершения загрузки.

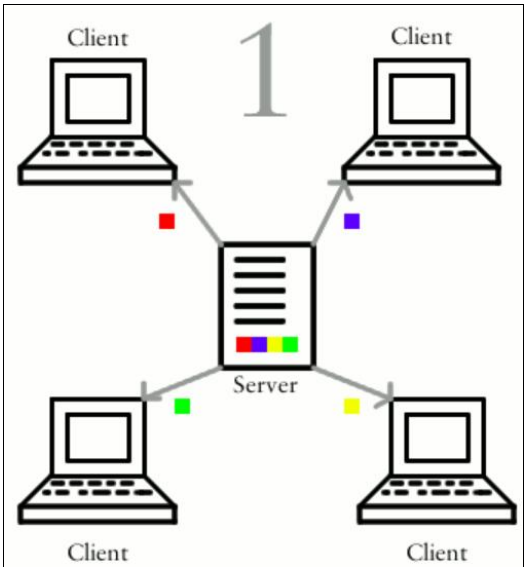
BitTorrent решил проблему медленного скачивания файлов с одного сервера, делая каждого участника процесса - источником. Таким образом, пользователи получают части файла и отдают их друг другу. Те, кто скачивает, или скачали и хранят файл, становятся сетью из нескольких источников. Все обеспечивают частями файлов друг друга. Это делает загрузку быстрой и надежной.

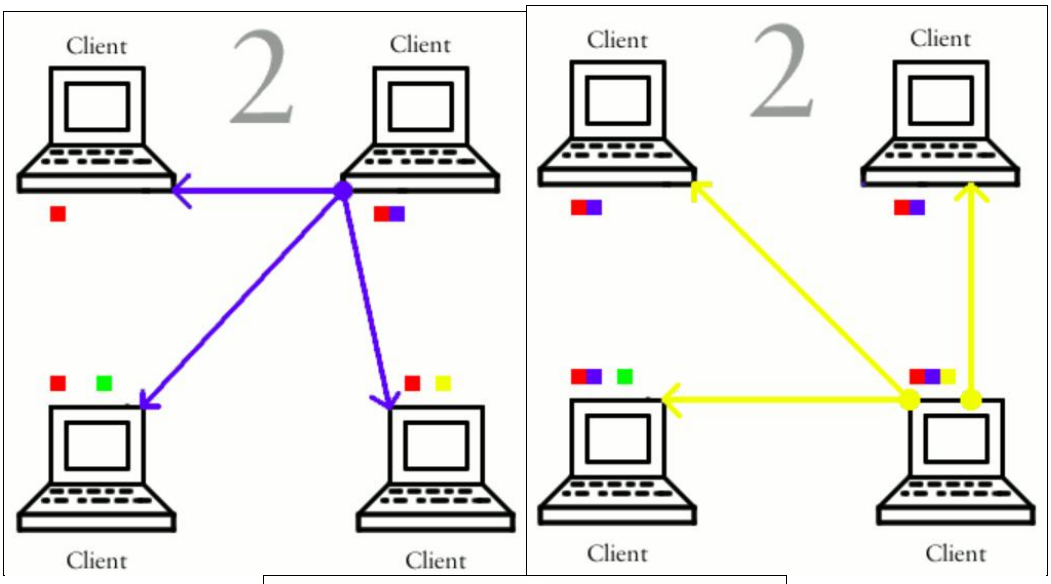
Для обеспечения такого взаимодействия в сети существует выделенный сервер - **ТРЕКЕР**, он регистрирует всех качающих и раздающих, и присваивает им статусы:

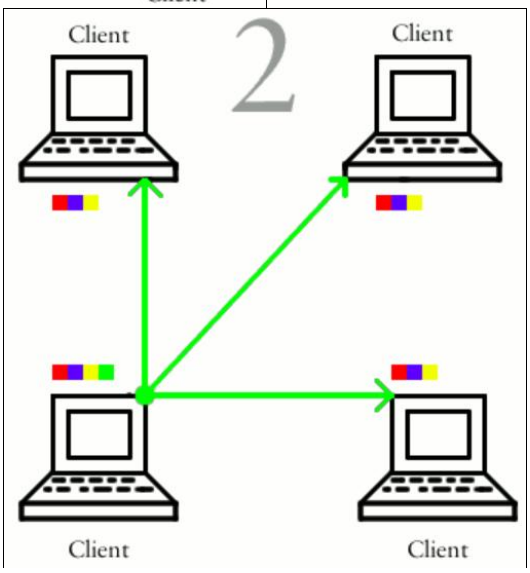
- **ПИР**, если идет загрузка.
- **СИД**, если загрузка закончена и происходит процесс раздачи.
- **ЛИЧ**, если файл загружен не полностью, но загрузка приостановлена.

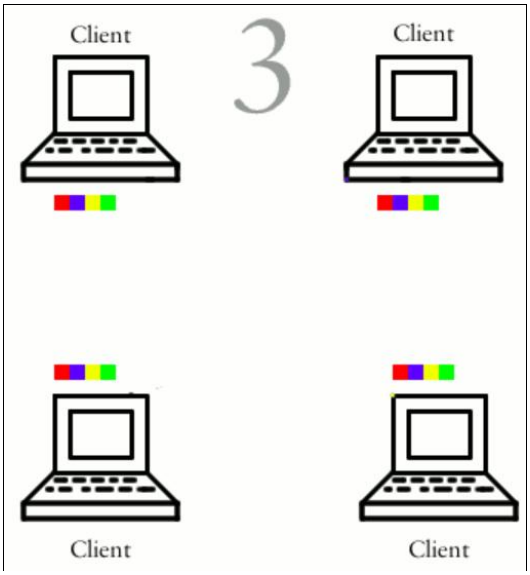
Процесс получения файла с помощью **BitTorrent** условно можно разделить на три этапа:

1. Регистрация пользователя в трекере с помощью торрент-файла и получение первых сегментов файла с сервера.
2. Получение остальных частей файлов от ПИРов, ЛИЧей и СИДов.
3. Перевод статуса пользователя в СИД или ЛИЧ, ожидание новой раздачи.

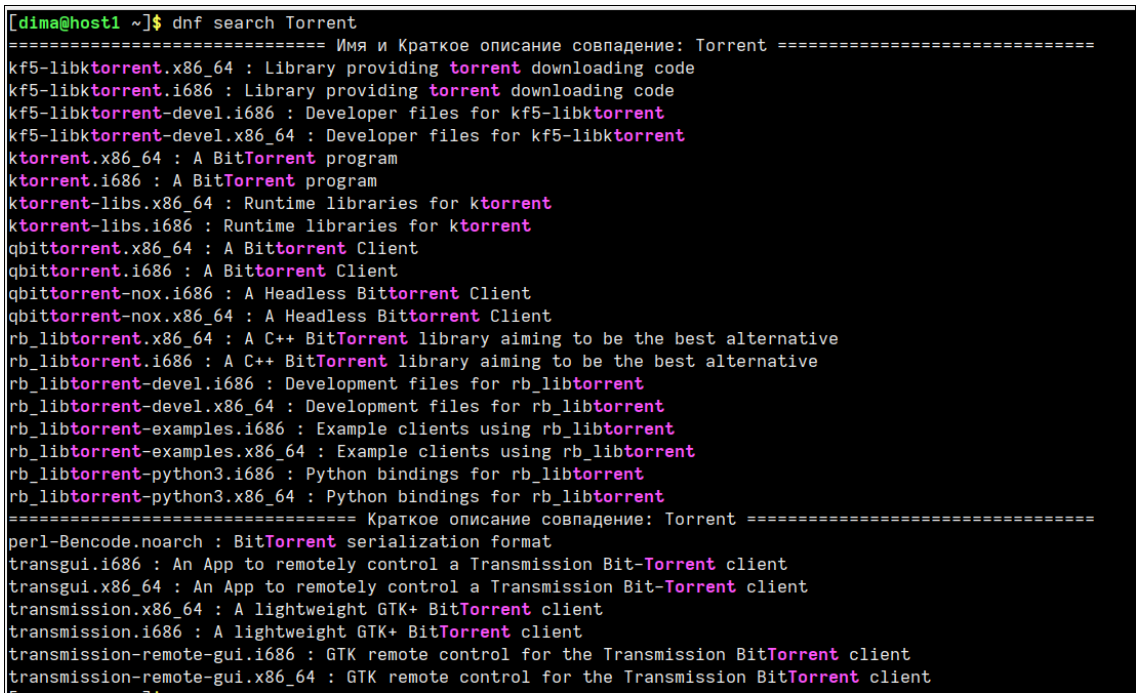








В репозиториях РЕД ОС имеется ряд приложений, реализующих поддержку протокола **BitTorrent**, для загрузки файлов. Менеджер пакетов нам подскажет, что это за программы, если мы осуществим поиск по строке «**Torrent**»:



Из полученного списка видно, что в поиске отобразились несколько **BitTorrent**-клиентов и несколько различных библиотек. Рассмотрим две программы из списка - **qbittorrent** и **transmission**.

qbittorrent

Интерфейс **qbittorrent** предельно прост и минималистичен, что и требуется для программы подобного рода. Программа практически не требует первоначальной настройки параметров, только указания папки для сохранения файлов.

Интерфейс состоит из нескольких частей:

1. **Панель меню**, в котором доступны «*Файл*», «*Правка*», «*Вид*», «*Инструменты*», «*Справка*». Состав меню минимален и, в тоже время, достаточен для работы программы.
2. **Панель инструментов** содержит основные кнопки, может быть скрыта с помощью опции меню «*Вид*».
3. **Панель закладок**. Это функциональные закладки, которые позволяют переключаться между разными функциями программы, такими как «*Управление торрентами*», «*Поиск торрентов*», «*Менеджер RSS подписок*», «*Журнал активности*». По умолчанию доступны только две первые закладки, остальные скрыты через меню «*Вид*».
4. **Панель статуса**. Может быть скрыта через меню «*Вид*». Отображает сведения о соединении, имеет несколько полей, которые позволяют переходить к настройкам программы или переключать режим её работы.

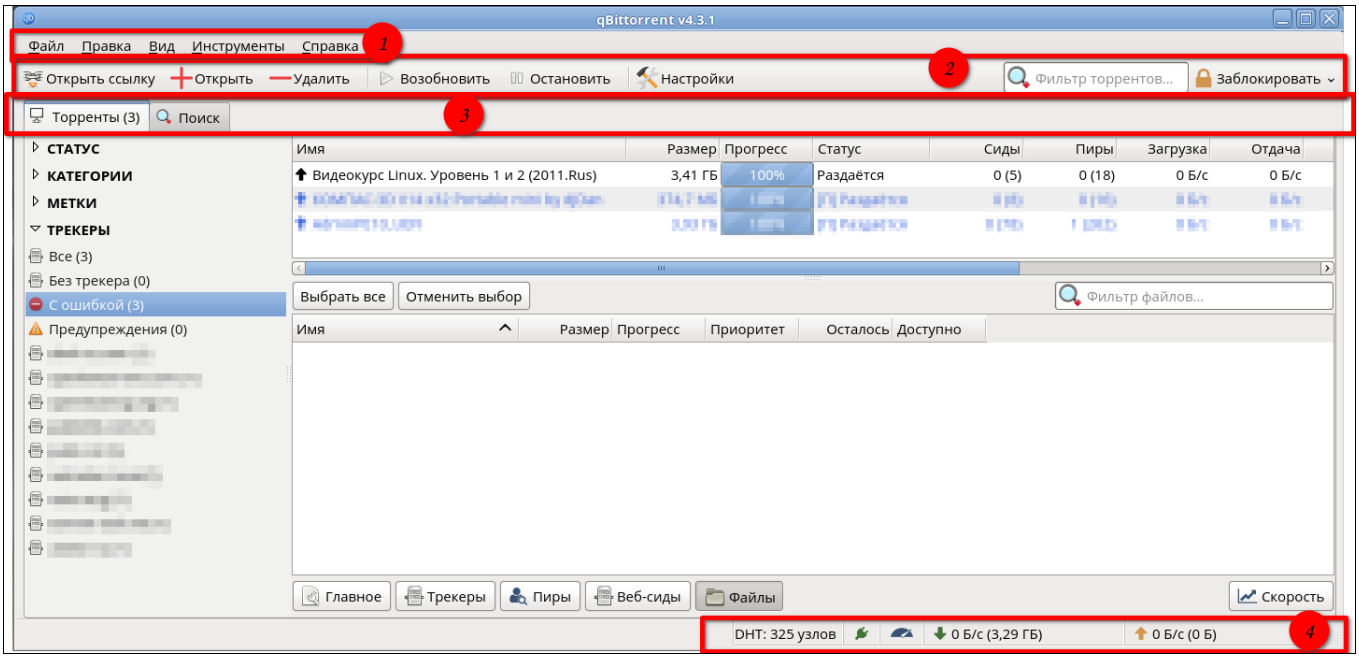
Для установки **qbittorrent** перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

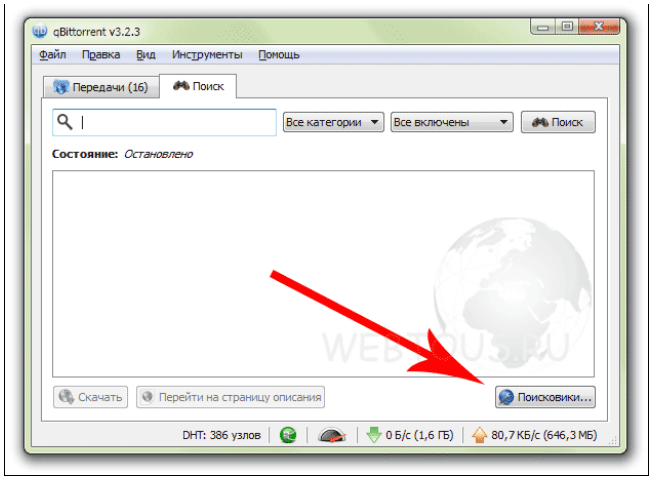
```
dnf install qbittorrent
```

После установки программа будет доступна из «**Главного меню**» - «**Интернет**» - «**qBittorrent**».

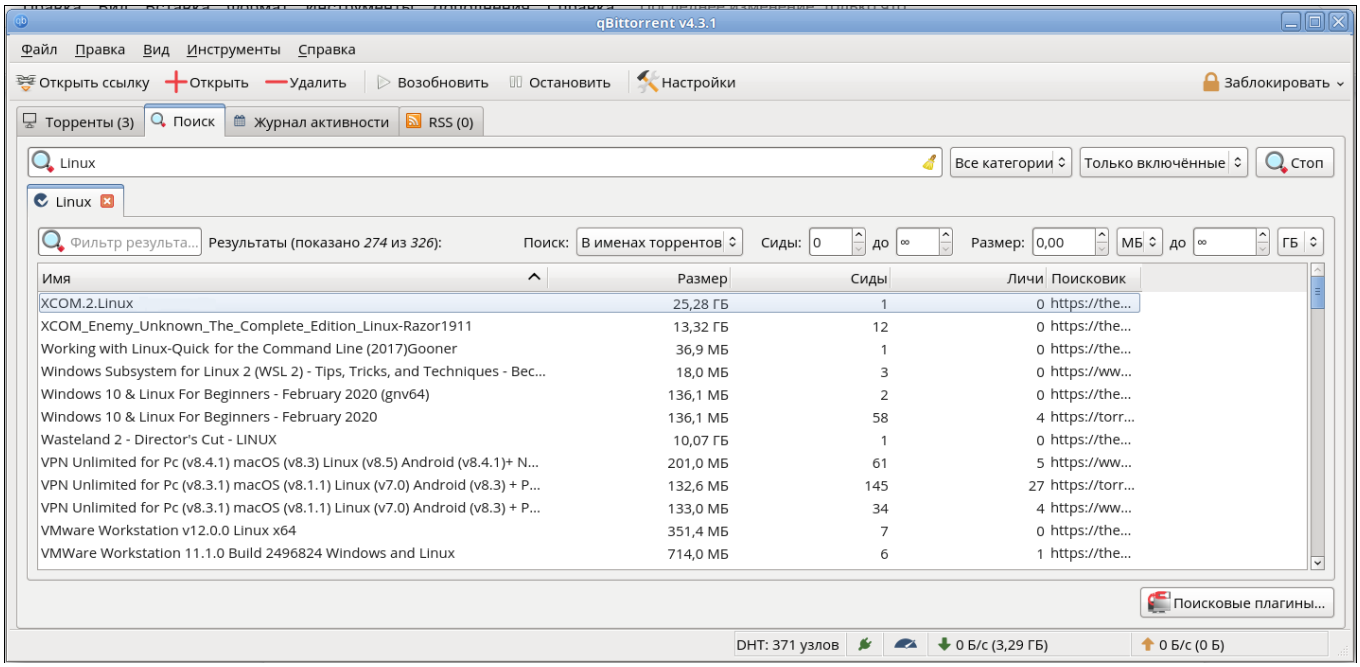


Закладка «Поиск»

При помощи закладки «*Поиск*» можно искать торренты, для этого нужно добавить необходимые ссылки. По умолчанию список пуст, поэтому можно просто нажать кнопку «*Поисковые плагины*» и проверить обновления. Вы получите небольшой список сайтов, по которым уже можно искать торренты. Можно добавлять свои ссылки на источники. Ссылки в списке можно отключать без удаления.



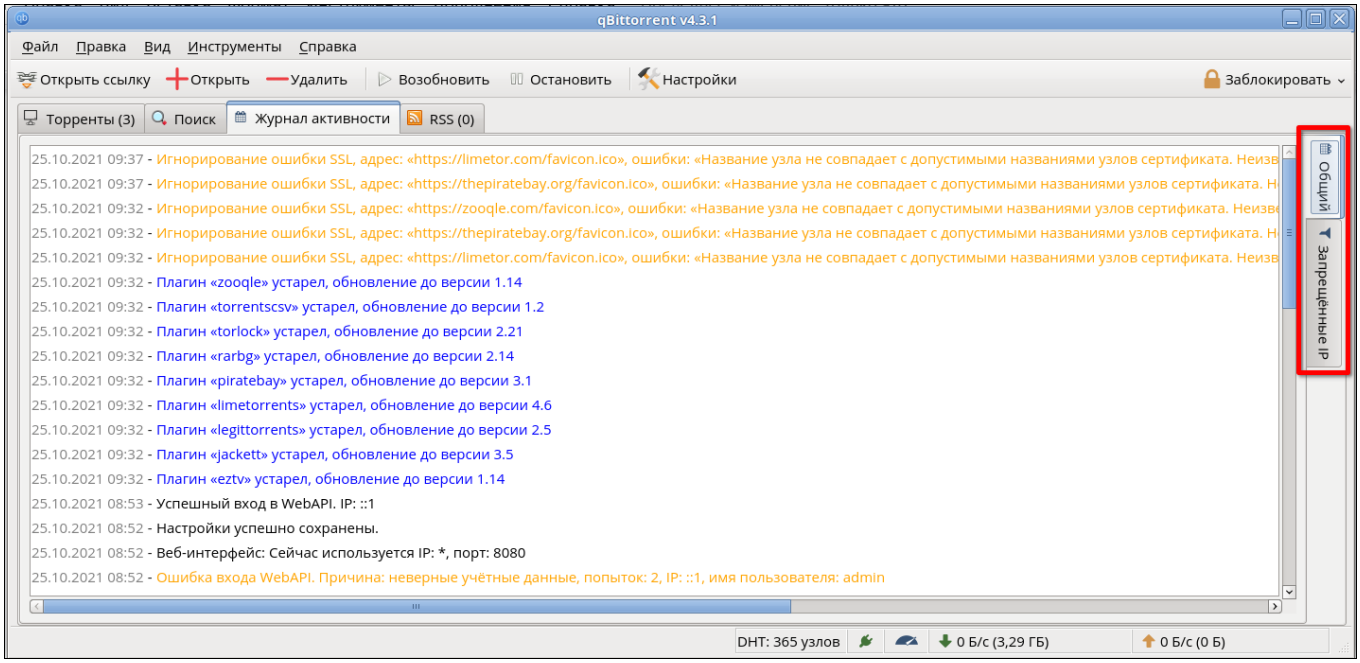
После добавления источников в строке поиска можно вводить нужные фразы и осуществлять поиск торрентов.



Для каждого найденного торрента доступна ссылка на страницу описания и кнопка «**Загрузить**».

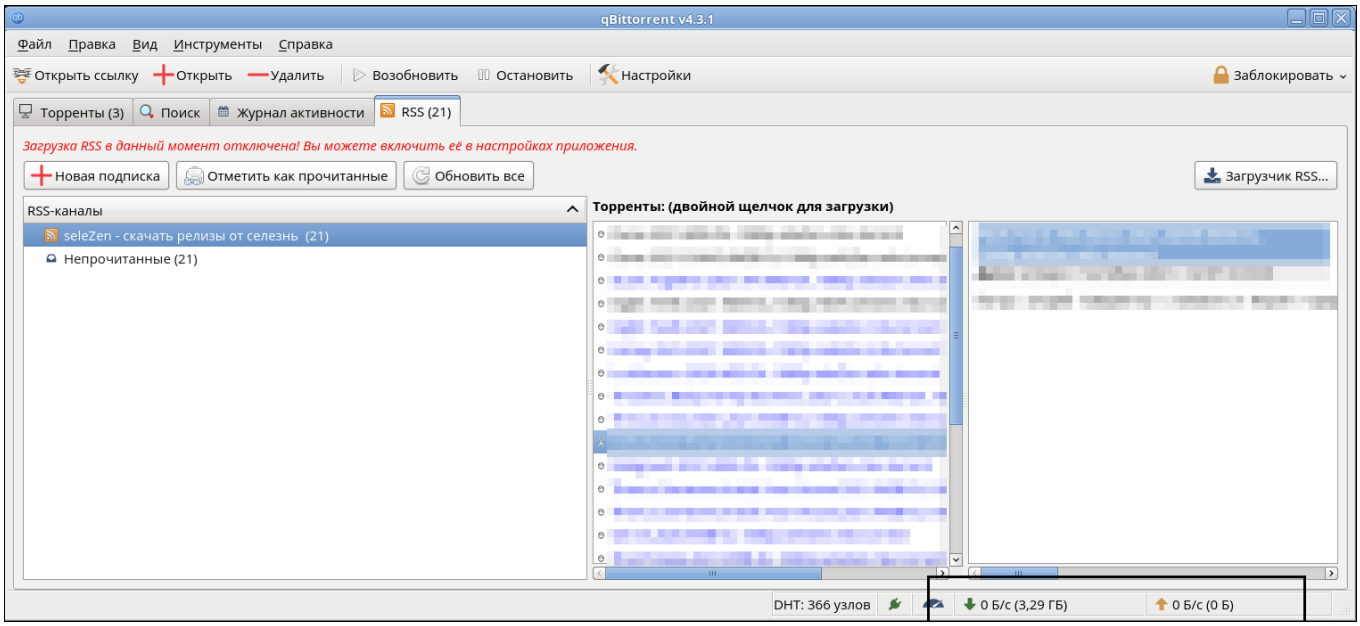
Закладка «Журнал активности»

На данной вкладке отображается список служебных сообщений о состоянии программы. Отображается два журнала – «*Общий*» и «*Запрещенные IP*».



Закладка «RSS»

RSS (Rich Site Summary, полная сводка сайта) – это автоматически генерируемая сводка в формате **rss** или **xml**, в которой отображаются недавно опубликованные статьи и новости. **RSS** - это отличный способ структурирования и фильтрации данных.

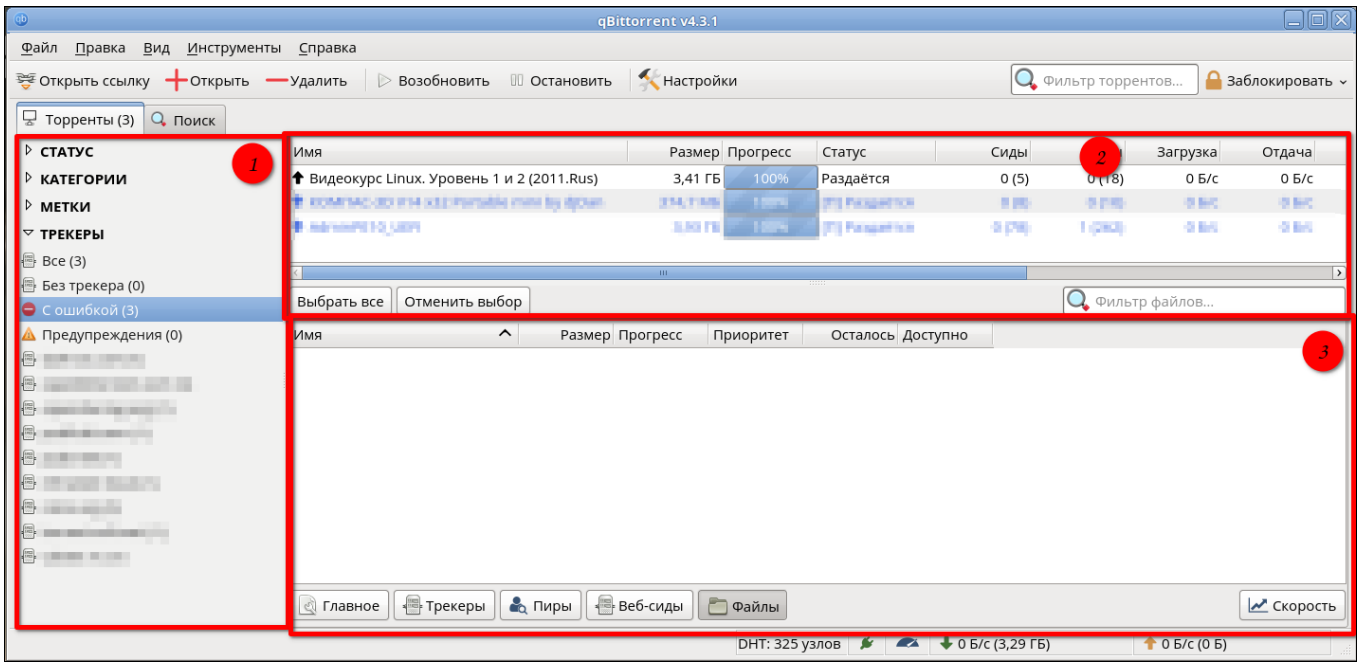


Для настройки подписок будет необходимо поискать ссылки на **RSS** в интернете. После этого добавьте найденную ссылку, нажмите «*Обновить*» и из полученного списка можно добавить в загрузку любой торрент.

Закладка «Торренты»

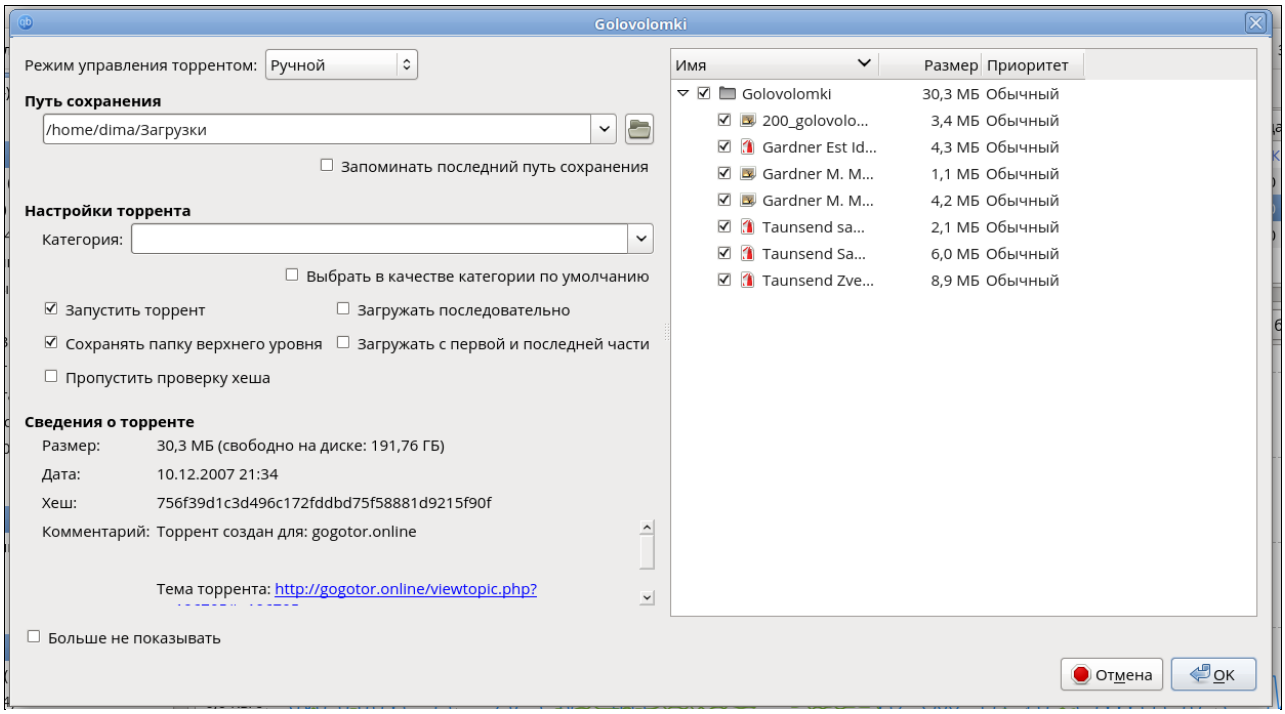
Перейдем к рассмотрению основной закладки программы. Она разделена на 3 части:

1. **Список фильтров** имеющихся торрентов. Если вы активно пользуетесь торрентами, то ваш список может быть довольно большим. Выбрав для отображения категорию, например, по статусу «*Загружаются*», можно увидеть во втором блоке список загружаемых торрентов.
2. **Таблица добавленных в программу торрентов** с некоторыми параметрами, например, процесс загрузки. В каждой строчке отображается отдельный торрент. Выделять группу можно стандартно с помощью зажатой клавиши «*Shift*». Для одиночного или группового выделения доступно контекстное меню с дополнительными функциями.
3. **Блок отображения свойств торрентов**. В нижней части третьего блока имеются кнопки, которые как отображают содержимое, за которое они отвечают, так и скрывают это содержимое, позволяя увеличить область отображения второго блока. Всего кнопок 6 - «*Главное*», «*Трекеры*», «*Пиры*», «*Веб-сиды*», «*Файлы*» и «*Скорость*».



Добавление торрента в загрузку

После получения торрент-файла откройте его с помощью программы qbittorrent, появится окно добавления торрента. Укажите путь сохранения и выберите загружаемый торрент. Остальное можно оставить без изменения. Нажмите «*OK*», файл добавится в список торрентов программы и начнется процесс загрузки.



transmission

Transmission — самый простой торрент-клиент. Любое действие можно сделать несколькими щелчками мышью. Клиент имеет простую и интуитивно понятную оболочку. **Transmission** использует минимум системных ресурсов компьютера.

В программе очень мало настроек, но они все нужны, чтобы оптимизировать приложение. По сравнению с qbittorrent, тут нет **RSS**, поиска торрентов и других сложных функций, но программа всё равно обладает всем необходимым функционалом. Добавлять в неё торрент-файлы, управлять процессом загрузки и скоростью так же просто. Осталось только попробовать и выбрать понравившуюся программу.

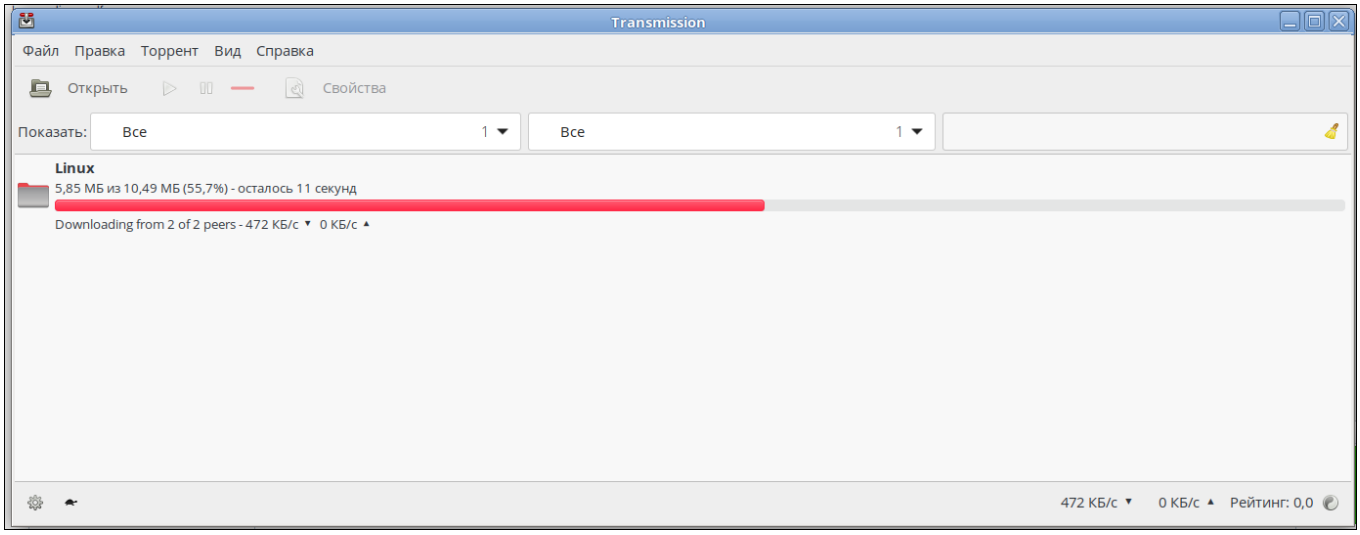
Для установки **transmission** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install transmission
```

После установки программа будет доступна из «**Главного меню**» - «**Интернет**» - «**Transmission**».



Важно отметить, что в данной статье рассмотрены не все функции и возможности торрент-клиентов, а только самые необходимые. Здесь не рассмотрены процесс удалённого доступа к программам, возможность организации трекера и многое другое. Однако, рассмотренных возможностей вполне достаточно, чтобы определиться с выбором программы для работы и перейти к её

использованию и изучению.

Автоматическое обнаружение сторонних ОС с помощью os-prober

Возможности
Вывод информации о других операционных системах
Отображение дополнительных операционных систем при загрузке

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: os-prober-1.77-3

Утилита **os-prober** автоматически обнаруживает другие установленные операционные системы на компьютере и предоставляет результаты в удобном формате, что упрощает идентификацию доступных загрузочных вариантов.

Возможности

Основные возможности утилиты **os-prober**:

- **os-prober** позволяет обнаружить различные операционные системы, установленные на вашем компьютере;
- утилита работает совместно с загрузчиком **grub2** для автоматического обнаружения операционных систем, отличных от Linux;
- **os-prober** поддерживает различные файловые системы.

Вывод информации о других операционных системах

При выполнении в терминале команды os-prober:

```
sudo os-prober
```

Утилита просканирует все доступные диски в системе на наличие других операционных систем и выведет информацию о их наличии на компьютере.

Для каждой обнаруженной ОС будет выведена строка в формате:

```
<раздел>:<описательное_имя>:<короткое_имя>:<тип_загрузчика>
```

Пример вывода:

```
/dev/sda1:Windows 10:Windows:chain
```

Если на диске существует только одна ОС, вывод утилиты будет пустым.

Отображение дополнительных операционных систем при загрузке

Для отключения обнаружения сторонних операционных систем при включении ПК необходимо добавить соответствующий параметр в конфигурационный файл **/etc/default/grub**.

Откройте файл конфигурации **/etc/default/grub** в текстовом редакторе:

```
sudo nano /etc/default/grub
```

Добавьте в конец файла параметр:

```
GRUB_DISABLE_OS_PROBER=true
```

Сохраните файл. Пример файла конфигурации **/etc/default/grub**:



Для применения внесённых настроек в файле **/etc/default/grub** выполните обновление конфигурации **grub2** командой:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Для вступления в силу изменений выполните команду перезагрузки:

```
reboot
```

Оптимизация команд с помощью hyperfine

Установка
Синтаксис
Опции
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: hyperfine-1.17.0-1

Hyperfine — это инструмент командной строки, предназначенный для измерения и сравнения производительности различных команд, алгоритмов или сценариев. Он работает путём многократного запуска команды или сценария и измерения времени, необходимого для её выполнения. Затем он вычисляет среднее время выполнения, медиану и стандартное отклонение, чтобы дать пользователю представление о производительности команды.

Hyperfine учитывает различные факторы, которые могут повлиять на производительность — кеширование, нагрузка на систему и другие процессы, работающие в фоновом режиме. Это позволяет получить более точные результаты и принимать обоснованные решения о том, как оптимизировать свои команды и сценарии.

Установка

Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install hyperfine
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
hyperfine [опции] <команда>
```

Опции

Основные опции утилиты:

- **-w, --warmup <число>** — выполняет число прогревающих запусков перед фактическим тестированием производительности;
- **-m, --min-runs <число>** — выполняет не менее указанного количества запусков для каждой команды (по умолчанию: 10);
- **-M, --max-runs <число>** — выполняет не более указанного количества запусков для каждой команды (по умолчанию ограничения нет);
- **-r, --runs <число>** — выполняет ровно указанное количество запусков для каждой команды (если эта опция не указана, **hyperfine** автоматически определяет количество запусков);
- **-s, --setup <команда>** — выполняет команду перед каждым набором запусков;
- **-p, --prepare <команда>** — выполняет команду перед каждым запуском;
- **-c, --cleanup <команда>** — выполняет команду после завершения всех тестовых запусков для каждой команды;
- **-P, --parameter-scan <значение> <MIN> <MAX>** — выполняет тесты для каждого значения в указанном диапазоне;
- **-D, --parameter-step-size <шаг>** — определяет шаг перебора значений в диапазоне;
- **-L, --parameter-list <значение> <список_значений>** — выполняет тесты для каждого значения из списка;
- **-S, --shell <оболочка>** — устанавливает оболочку, используемую для выполнения команд;
- **-N** — алиас для ***--shell=none*** (оболочка не будет использоваться);
- **-i, --ignore-failure** — игнорирует ненулевые коды возврата тестируемых программ;

- **--style <тип>** — устанавливает стиль вывода:
    - **auto** — автоматически определяет стиль вывода (по умолчанию),
    - **basic** — отключает цветовую схему вывода и интерактивные элементы,
    - **full** — включает все эффекты,
    - **nocolor** — вывод без цвета,
    - **color** — вывод в цвете,
    - **none** — отключает все выходные данные;
- **--sort <метод>** — указывает порядок сортировки сводки сравнения производительности и экспортированных таблиц для форматов разметки (Markdown, AsciiDoc, org-mode):
    - **auto** — автоматически определяет порядок сортировки (по умолчанию),
    - **command** — сортирует результаты по имени команды,
    - **mean-time** — сортирует результаты по среднему времени выполнения команды;
- **-u, --time-unit <единица>** — устанавливает единицу времени (по умолчанию: секунда, возможные значения: миллисекунда, секунда);
- **--export-asciidoc <файл>** — экспортирует сводную статистику синхронизации в виде таблицы AsciiDoc в указанный файл;
- **--export-csv <файл>** — экспортирует сводную статистику синхронизации в формате **CSV** в указанный файл;
- **--export-json <файл>** — экспортирует сводную статистику синхронизации и тайминги отдельных запусков в формате JSON в данный файл;
- **--export-markdown <файл>** — экспортирует сводную статистику времени в виде таблицы Markdown в данный файл;
- **--export-orgmode <файл>** — экспортирует сводную статистику времени как таблицу Emacs в указанный файл;
- **--show-output** — выводит стандартный вывод (stdout) и вывод ошибок (stderr);
- **--output <путь>** — перенаправляет выходные данные:
    - **null** — данные не будут сохранятся или отображаться (по умолчанию);
    - **pipe** — данные будут переданы через канал перед тем, как будут удалены из вывода,
    - **inherit** — данные будут отображены в терминале,
    - **путь к файлу** — вывод будет записан в указанный файл;
- **--input <путь>** — считывает входные данные из заданного файла (null или путь к файлу);
- **-n, --command-name <имя>** — устанавливает команде имя;
- **-h, --help** — выводит справку;
- **-V, --version** — выводит версию программы.

Примеры использования

1. Измерение времени выполнения команды 'ls -l':

```
hyperfine 'ls -l'
```

Результат:

```
Benchmark 1: ls -l
  Time (mean ± σ):      0.7 ms ±  0.6 ms    [User: 0.8 ms, System: 0.7 ms]
  Range (min … max):    0.3 ms …  9.0 ms    267 runs
```

где:

- **Benchmark** — используется для измерения времени выполнения команд или программ;
- **Time** — среднее время выполнения команды, включая стандартное отклонение (σ). Среднее время выполнения команды 'ls -l' составляет 0.7 мс со стандартным отклонением 0.6 мс;
- **Range** — диапазон времени выполнения команды от минимального до максимального значения. Минимальное время выполнения команды составляет 0.3 мс, а максимальное — 9.0 мс.

2. Сравнение времени выполнения нескольких команд ('ls -l' и 'ls -a'):

```
hyperfine 'ls -l' 'ls -a'
```

Результат:

```
Benchmark 1: ls -l
  Time (mean ± σ):      1.5 ms ±  0.5 ms    [User: 0.7 ms, System: 1.1 ms]
  Range (min … max):    1.1 ms …  4.7 ms    928 runs  Benchmark 2: ls -a
  Time (mean ± σ):      0.8 ms ±  0.6 ms    [User: 0.5 ms, System: 0.7 ms]
  Range (min … max):    0.4 ms …  5.7 ms    700 runs  Summary  ls -a ran
    1.87 ± 1.42 times faster than ls -l
```

где:

- **Summary** — сводный итог сравнительной производительности команд (**ls -a** выполнялась в среднем в 1.87 раз быстрее, чем команда **ls -l** со стандартным отклонением 1.42 мс).

3. Выполнение 5 предварительных запусков перед основными измерениями:

```
hyperfine -w 5 'ls -a'
```

Результат:

```
Benchmark 1: ls -a
  Time (mean ± σ):      0.1 ms ±  0.4 ms    [User: 0.5 ms, System: 0.3 ms]
  Range (min … max):    0.0 ms …  4.5 ms    1230 runs
```

4. Ограничение количества запусков команды:

```
hyperfine -M 50 'ls -a'
```

Результат:

```
Benchmark 1: ls -a
  Time (mean ± σ):      0.8 ms ±  0.2 ms    [User: 0.5 ms, System: 0.8 ms]
  Range (min … max):    0.6 ms …  1.3 ms    50 runs
```

5. Экспорт статистики в формате CSV в файл:

```
hyperfine --export-csv sample4.csv 'ls'
```

Результат:

```
Benchmark 1: ls
  Time (mean ± σ):      0.3 ms ±  1.1 ms    [User: 0.5 ms, System: 0.4 ms]
  Range (min … max):    0.0 ms … 13.7 ms    191 runs
```

6. Экспорт статистики и результатов запусков в формате JSON:

```
hyperfine --export-json sample1.json 'ls'
```

Результат:

```
Benchmark 1: ls
  Time (mean ± σ):      0.1 ms ±  0.3 ms    [User: 0.5 ms, System: 0.3 ms]
  Range (min … max):    0.0 ms …  4.2 ms    860 runs
```

7. Направление вывода результатов в файл:

```
hyperfine --output ./3d.txt 'ls -v' -N
```

Результат:

```
Benchmark 1: ls -v
```

```
  Time (mean ± σ):      1.1 ms ±  0.4 ms    [User: 0.3 ms, System: 0.6 ms]
  Range (min … max):    0.9 ms …  5.0 ms    2737 runs
```

Улучшение визуализации различий в коде с утилитой diff-so-fancy

Возможности
Установка
Синтаксис
Опции
Рекомендуемые стандартные цвета
Настройка дополнительных цветов
Сравнение файлов с помощью diff-so-fancy
Настройка внешнего вида diff-so-fancy

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: diff-so-fancy-1.4.4

Утилита **diff-so-fancy** предназначена для улучшения визуального представления вывода команды git diff. Она форматирует вывод, делая его более читаемым и удобным для анализа. Благодаря улучшенному форматированию и цветовой подсветке, разработчики могут легко понять, какие изменения были внесены.

Возможности

Основные возможности **diff-so-fancy**:

1. **Улучшенное форматирование** — выделение изменённых строк и слов внутри строк для лучшей наглядности.
2. **Удаление избыточной информации** — сокрытие ненужных символов и заголовков, что делает вывод более компактным и чистым.
3. **Цветовое выделение** — использование различных цветов для выделения добавленных и удалённых строк.

Установка

Для установки **diff-so-fancy** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install diff-so-fancy
```

Синтаксис

Утилита **diff-so-fancy** доступна для запуска через терминал при помощи команды следующего вида:

```
diff-so-fancy [--version] [--help] [<опции>] [<аргументы>]
```

Опции

Основные опции утилиты:

- **--width <ширина>** — устанавливает ширину вывода в символах. Например, --width 120 задает ширину 120 символов;
- **--theme <тема>** — применяет заданную тему оформления для вывода;
- **--no-inline** — отключает отображение изменений в строке;
- **--color <цвет>** — настраивает цветовую схему для различных элементов вывода;
- **--ignore-space-change** — игнорирует изменения пробелов при сравнении;
- **--no-abbrev** — отключает укороченное отображение идентификаторов коммитов.

Рекомендуемые стандартные цвета

Для просмотра рекомендованных цветов выполните команду:

```
diff-so-fancy --colors
```

Для настройки цветов включите цветовое отображение:

```
git config --global color.ui true
```

Для настройки цвета обычного текста (ДО изменений) выполните:

```
git config --global color.diff-highlight.oldNormal "red bold"
```

Для настройки цвета выделенного текста (ДО изменений) выполните:

```
git config --global color.diff-highlight.oldHighlight "red bold 52"
```

Для настройки цвета обычного текста (ПОСЛЕ изменений) выполните:

```
git config --global color.diff-highlight.newNormal "green bold"
```

Для настройки цвета выделенного текста (ПОСЛЕ изменений) выполните:

```
git config --global color.diff-highlight.newHighlight "green bold 22"
```

Настройка дополнительных цветов

Для более удобного восприятия изменений в файлах можно настроить дополнительные цвета для различных элементов diff.

Для настройки дополнительных цветов для метаданных выполните:

```
git config --global color.diff.meta "yellow"
```

Git поддерживает стандартные цветовые названия, такие как red, green, blue, yellow, magenta, cyan, white, black и т. д.

Для настройки цветов заголовков фрагментов выполните:

```
git config --global color.diff.frag "magenta bold"
```

Для настройки цветов коммитов выполните:

```
git config --global color.diff.commit "yellow bold"
```

Для настройки цветов строк, которые были удалены или изменены в старой версии файла, выполните:

```
git config --global color.diff.old "red bold"
```

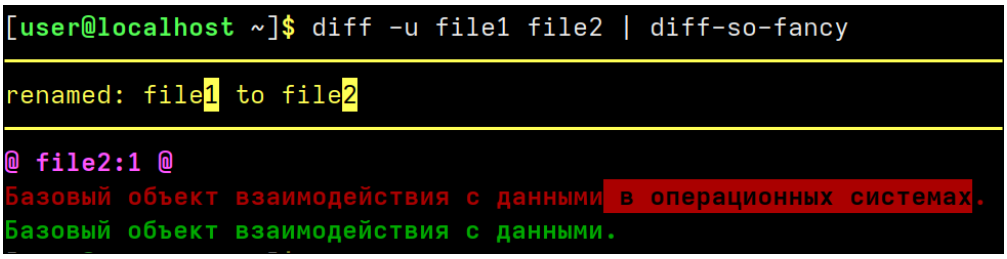
Для настройки цветов пробелов выполните:

```
git config --global color.diff.whitespace "red reverse"
```

Сравнение файлов с помощью diff-so-fancy

Для сравнения содержимого двух файлов с помощью утилиты **diff-so-fancy** введите следующую команду:

```
diff -u file1 file2 | diff-so-fancy
```



Эта команда улучшает восприятие результатов сравнения, делая их более удобными для анализа.

Настройка внешнего вида diff-so-fancy

Утилита **diff-so-fancy** предоставляет гибкие возможности для настройки отображения изменений, позволяя адаптировать вывод под предпочтения пользователя.

Для настройки вывода через аргументы командной строки, используйте следующую команду:

```
git diff --color | diff-so-fancy --width 120 --theme solarized-dark
```

где:

- **--width 120** — устанавливает ширину вывода в 120 символов;
- **--theme solarized-dark** — применяет тему оформления solarized-dark.

Ведение финансового учета с помощью kmymoney

Возможности
Установка
Настройка
Описание
Счета
Создание графиков
Статьи бюджета
Метки
Контрагенты
Книга учёта
Инвестиции
Отчёты
Бюджеты
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kmymoney-5.1.3

KMyMoney — это бесплатная программа для ведения домашней бухгалтерии, которая предлагает широкий спектр функций, сравнимых с коммерческими программами управления личными финансами.

KMyMoney не предназначена для удовлетворения потребностей среднего и крупного бизнеса, но может быть подходящим решением для малого бизнеса. Она может быть адаптирована под требования данной категории пользователей с помощью дополнительных модулей.

Возможности

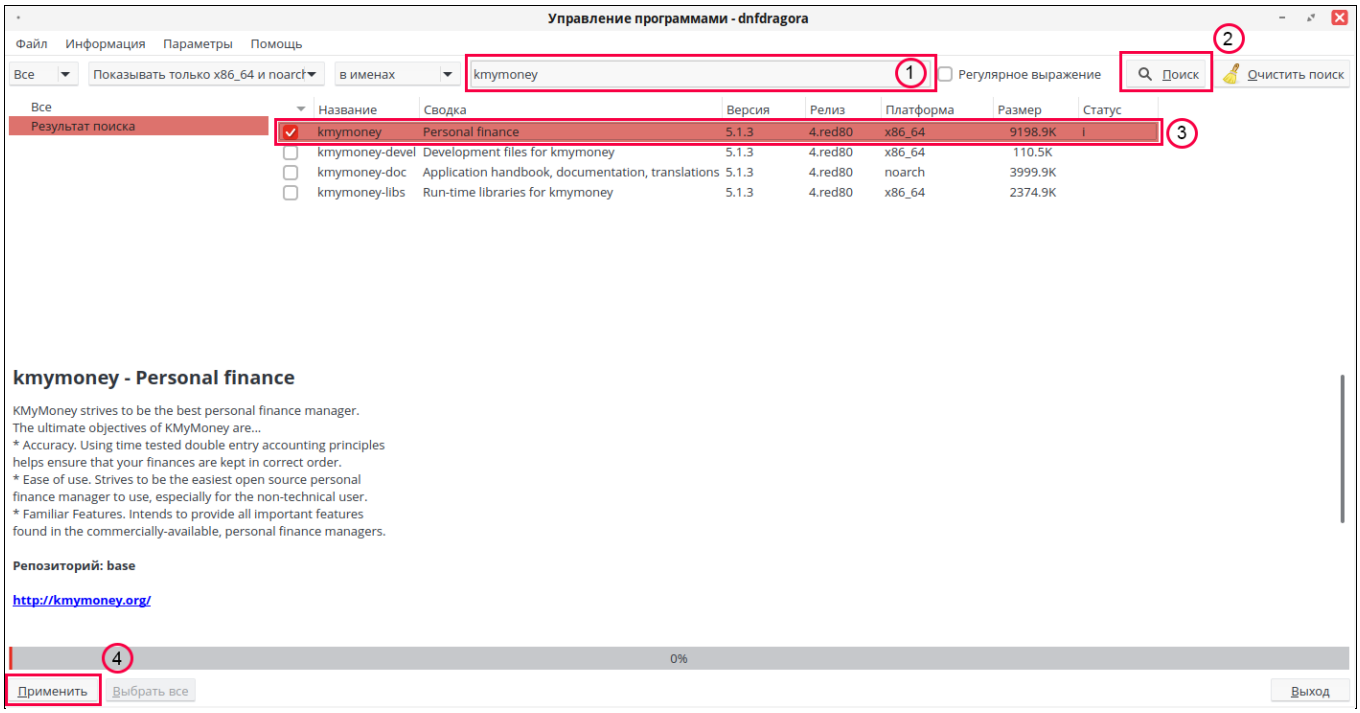
Основные возможности **KMyMoney**:

- поддерживает несколько валют, что позволяет вести учёт в разных валютах одновременно;
- позволяет создавать и управлять несколькими счетами, что удобно для учёта доходов и расходов по разным категориям;
- позволяет создавать бюджеты и отслеживать их выполнение;
- предоставляет инструменты для анализа финансовых показателей;
- поддерживает импорт и экспорт данных в различных форматах, что упрощает обмен данными с другими программами;
- синхронизирует данные с облачными сервисами, такими как Dropbox или Google Drive;
- обеспечивает защиту данных с помощью шифрования и паролей;
- отправляет пользователям напоминания о предстоящих платежах и событиях, связанных с финансами;
- предоставляет пользователям различные графики и диаграммы, которые помогают визуализировать финансовые данные и лучше понимать их.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kmymoney**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install kmymoney
```

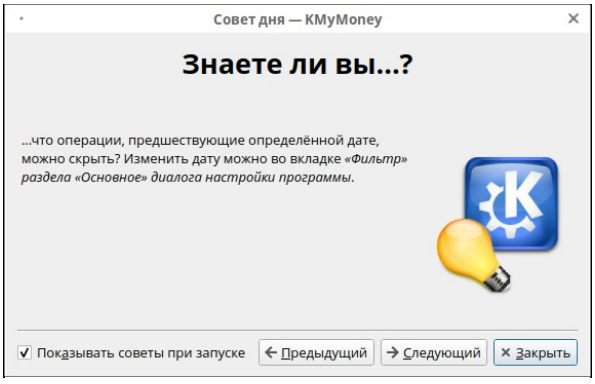
Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Для запуска программы через терминал введите команду:

```
kmymoney
```

После установки программа будет доступна из «**Главного меню**» — «**Офис**» — «**KmyMoney**».

Настройка

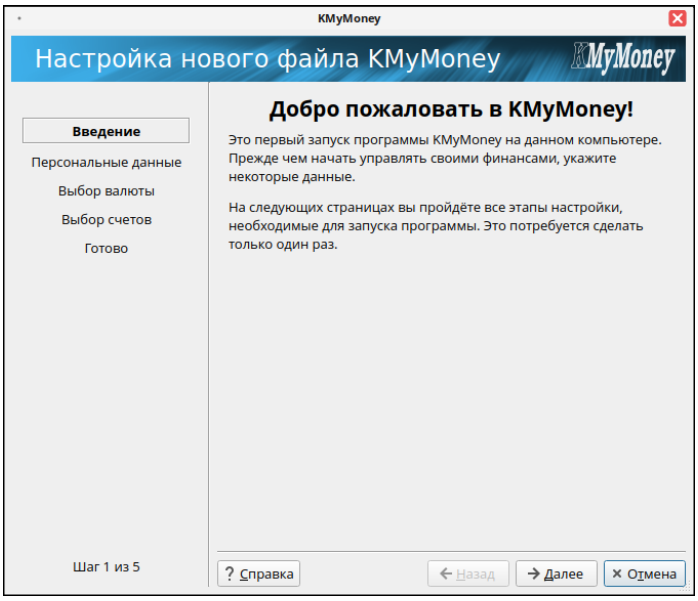
По завершении загрузки **KMyMoney** будут показаны два окна. Первое окно «**Совет дня**» содержит полезные советы по работе с приложением.



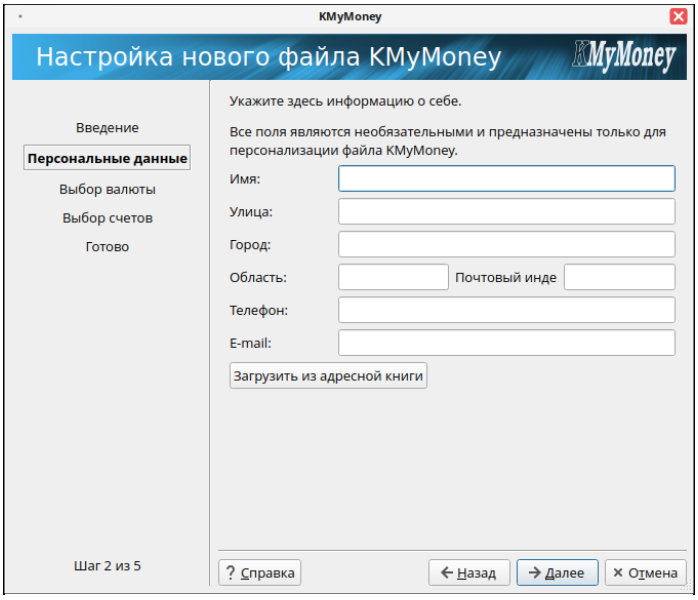
Рекомендуется ознакомиться с содержанием советов. По умолчанию окно будет показано вновь при следующем запуске **KMyMoney**. Для его отключения снимите соответствующий флаг «**Показывать советы при запуске**».

Для включения окна с советами выберите в меню «**Справка**» — «**Показывать совет дня**». Чтобы закрыть диалог «**Совет дня**», нажмите кнопку «**Закрыть**».

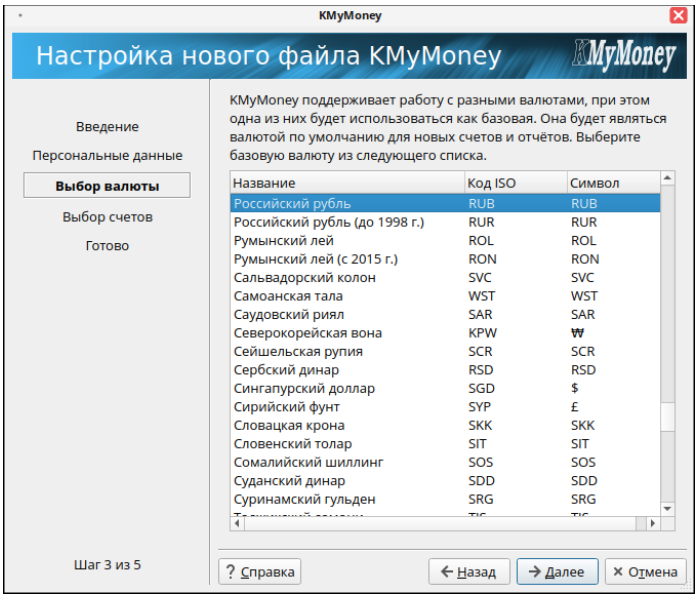
При первом запуске **KMyMoney** необходимо провести первоначальную настройку в соответствии с целями, для которых используется приложение. Так как все поля являются необязательными, можно оставить их пустыми и продолжить использовать **KmyMoney.**



Укажите имя и адрес и нажмите кнопку «**Далее**».

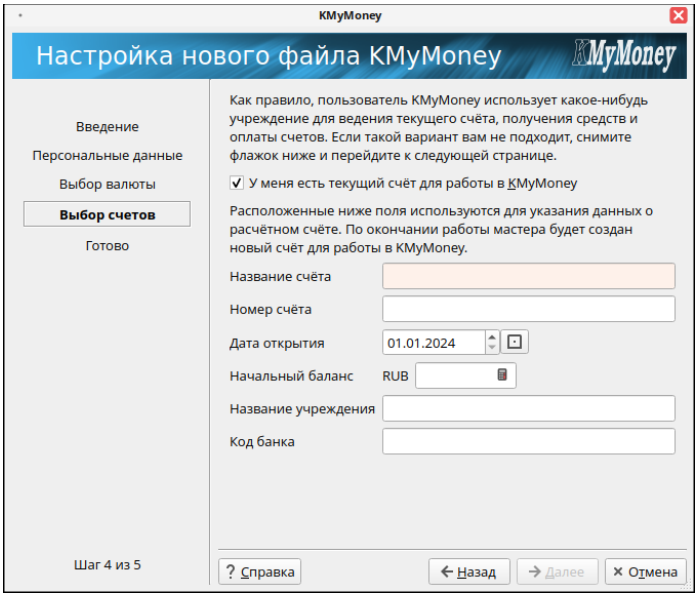


В **KMyMoney** можно работать с несколькими валютами, но одна будет использоваться как базовая. Задайте базовую валюту и нажмите кнопку «**Далее**». В приведённом примере в качестве базовой валюты выбран Российский рубль.



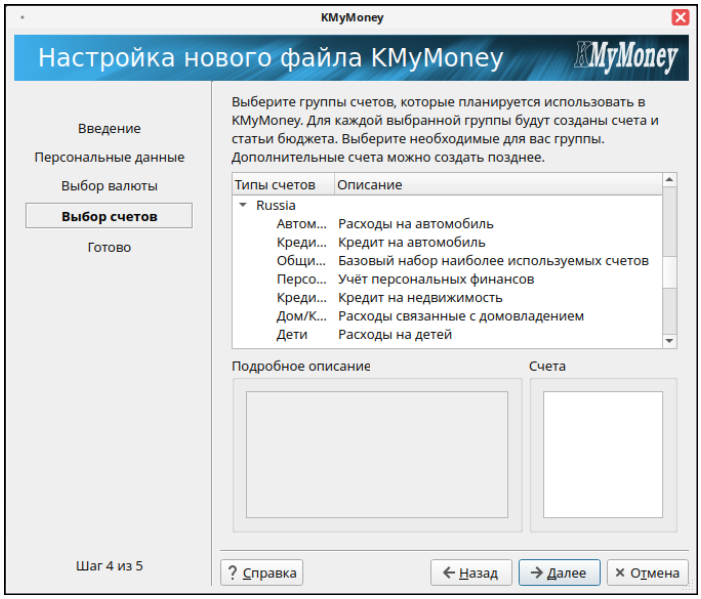
Укажите название и номер счёта. Введите дату открытия счёта и его начальный баланс. Для управления финансовыми данными, начиная с 1 января 2024 года, укажите баланс счёта на эту дату. Нужное значение можно узнать из банковской выписки. Далее укажите название и код учреждения (для работы с онлайн-банком).

Если создавать начальный счёт не требуется, снимите соответствующий флаг. По завершении ввода данных перейдите к следующему шагу, нажав кнопку «**Далее**».

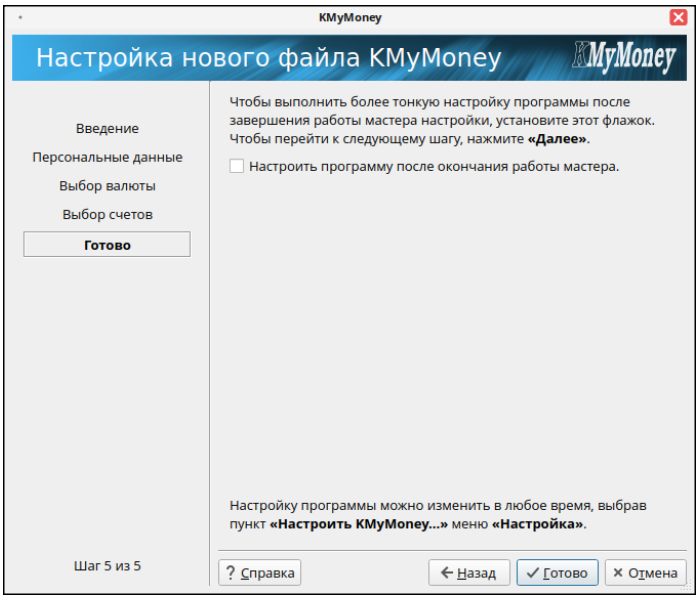


Выберите страну и шаблон. Каждый шаблон имеет свой набор статей бюджета для организации финансовых данных. Чтобы выбрать несколько шаблонов, зажмите **Ctrl**, затем щёлкните по нужным шаблонам. Программа отобразит иерархию счетов в области предварительного просмотра.

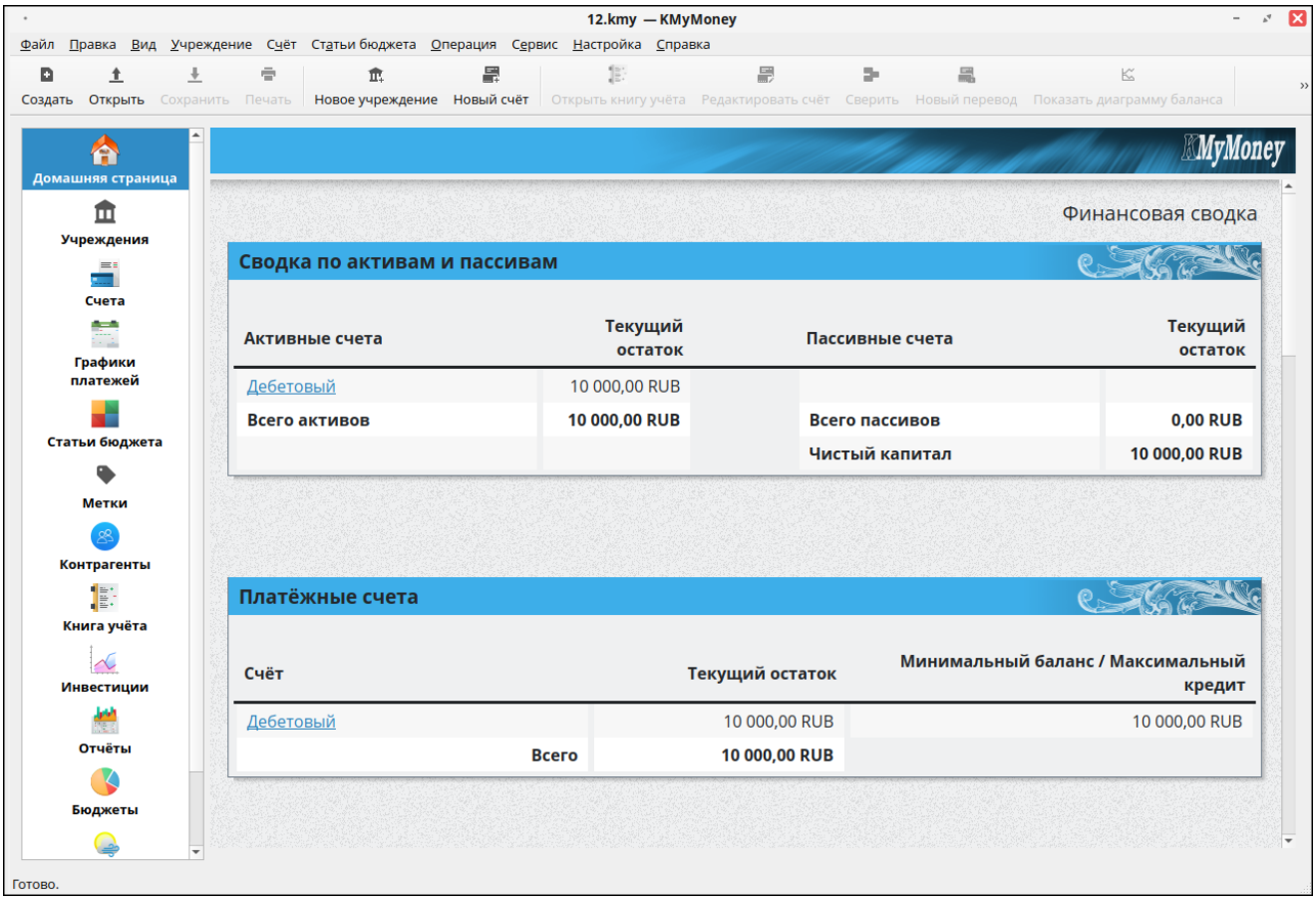
Если вам не удаётся найти подходящий шаблон, вы можете пропустить этот шаг и настроить статьи бюджета вручную позже. Затем вы сможете настроить пользовательские предпочтения. Если вы установили соответствующий флаг, после окончания работы мастера будет показан диалог настройки параметров приложения. Введите все необходимые данные и нажмите кнопку «**Далее**» для продолжения.



На последней странице мастера можно выбрать расширенную настройку программы. После первоначальной настройки приложение готово к работе. Нажмите кнопку «**Готово**».

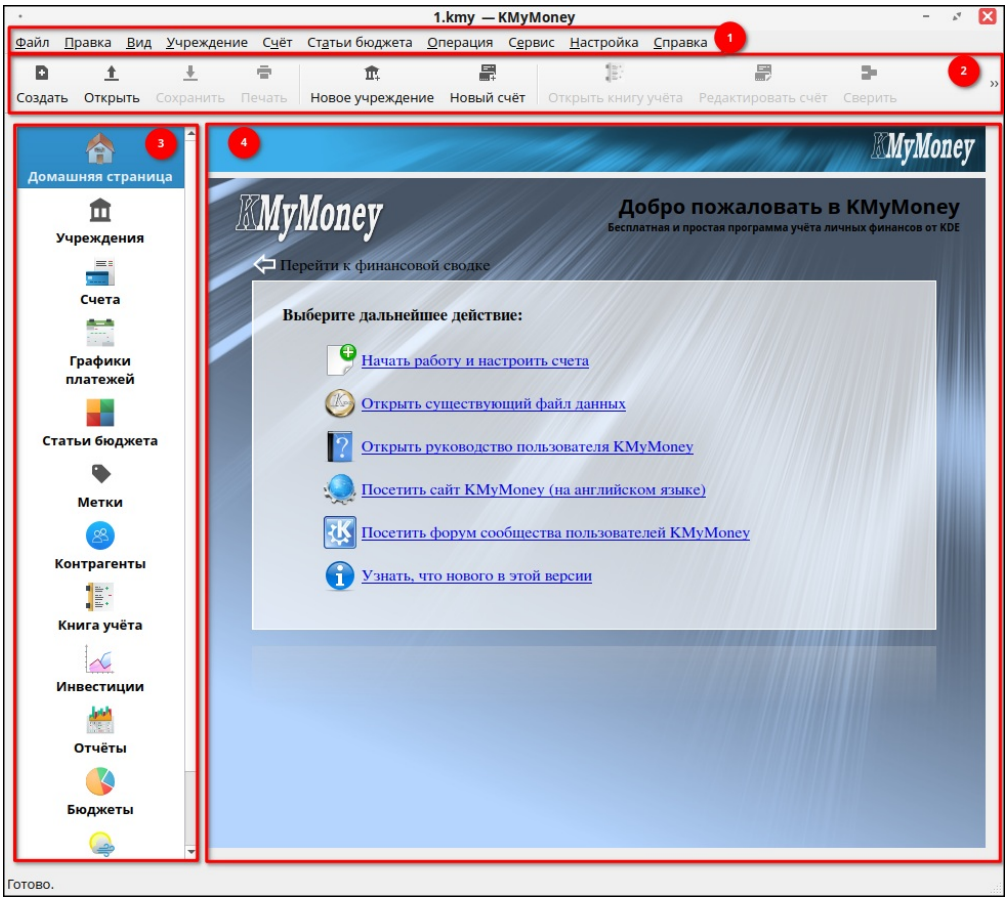


KMyMoney создаст и откроет файл.



Описание программы

Главное окно программы выглядит следующим образом:



1. **Основное меню** программы — здесь собраны основные возможности программы.

2. **Панель инструментов** — настраиваемая панель для быстрого доступа к наиболее востребованным функциям программы. Для её настройки перейдите в пункт меню «**Настройки**» — «**Панели инструментов...**».

3. **Меню выбора представления**. В этом меню отображаются различные варианты просмотра финансовых данных. Можно выбрать из доступных представлений, которые зависят от установленного программного обеспечения. Модули, подключенные к программе, могут добавить новые варианты. Щёлкните по значку, чтобы открыть соответствующее представление в области просмотра. Каждое представление обеспечивает детализированный обзор финансового положения, предоставляя доступ к просмотру и редактированию соответствующих данных.

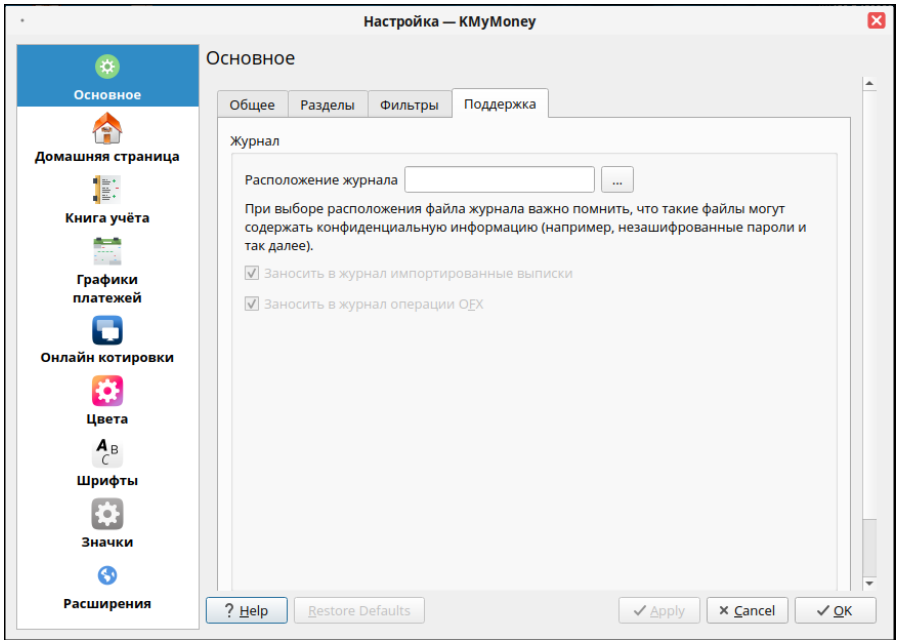
Меню выбора представления содержит следующие значки:

- **Домашняя страница**: отображение сводных данных о вашем финансовом положении.
- **Учреждения**: иерархическое представление всех учреждений и счетов, связанных с ними.
- **Счета**: иерархическое представление всех счетов, позволяющее просматривать и управлять вашими финансами.
- **Графики платежей**: отображение повторяющихся выплат и поступлений, помогающее планировать ваш бюджет.
- **Статьи бюджета**: специальные счета, которые группируют связанные операции.
- **Метки**: дополнительные счета, которые могут быть использованы в сочетании со статьями бюджета для группировки связанных операций.
- **Контрагенты**: список всех контрагентов, с которыми вы работаете, включая лица и учреждения, которым вы платите или от которых получаете деньги.
- **Книга учёта**: подробный журнал операций по счетам.
- **Инвестиции**: обзор портфеля ценных бумаг.
- **Отчёты**: набор полезных отчётов,который позволяет просматривать ваше финансовое состояние с различных сторон.
- **Бюджеты**: ваши бюджеты.

- **Прогноз**: представление, которое позволяет просматривать прогноз для счетов и статей.
- **Исходящие**: представление, используемое модулем сетевой работы с банками для отображения сообщений о выполненных операциях.

4. **Область просмотра**. Данная область предназначена для работы с текущей вкладкой рабочей панели.

Для расширенной настройки **KMyMoney** выберите пункт «**Настройка**» — «**Настроить KMyMoney...**». Будет открыто окно настройки, в котором можно персонализировать программу:



Счета

Счета используются для создания операций. Операции могут быть связаны с одним или несколькими счетами.

Счета-Активы — это счета, на которых хранятся деньги и имущество, которое требуется отслеживать. Типы активов:

- Текущий счёт,
- Сберегательный счёт,
- Наличные,
- Ссудный счёт,
- Инвестиции,
- Актив (имущество, коллекции и т.д.).

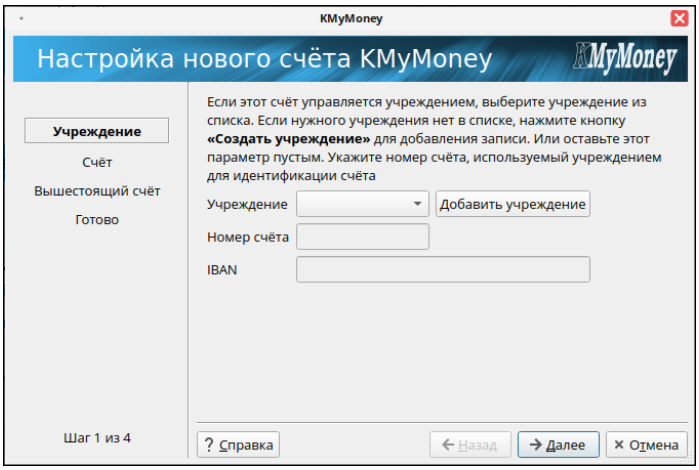
Счета-Пассивы — это счета, которые представляют долги и заёмные средства, которые требуется отслеживать. Типы пассивов:

- Кредитная карта,
- Ссудный счёт,
- Пассив (любое обязательство пользователя, отличное от кредита).

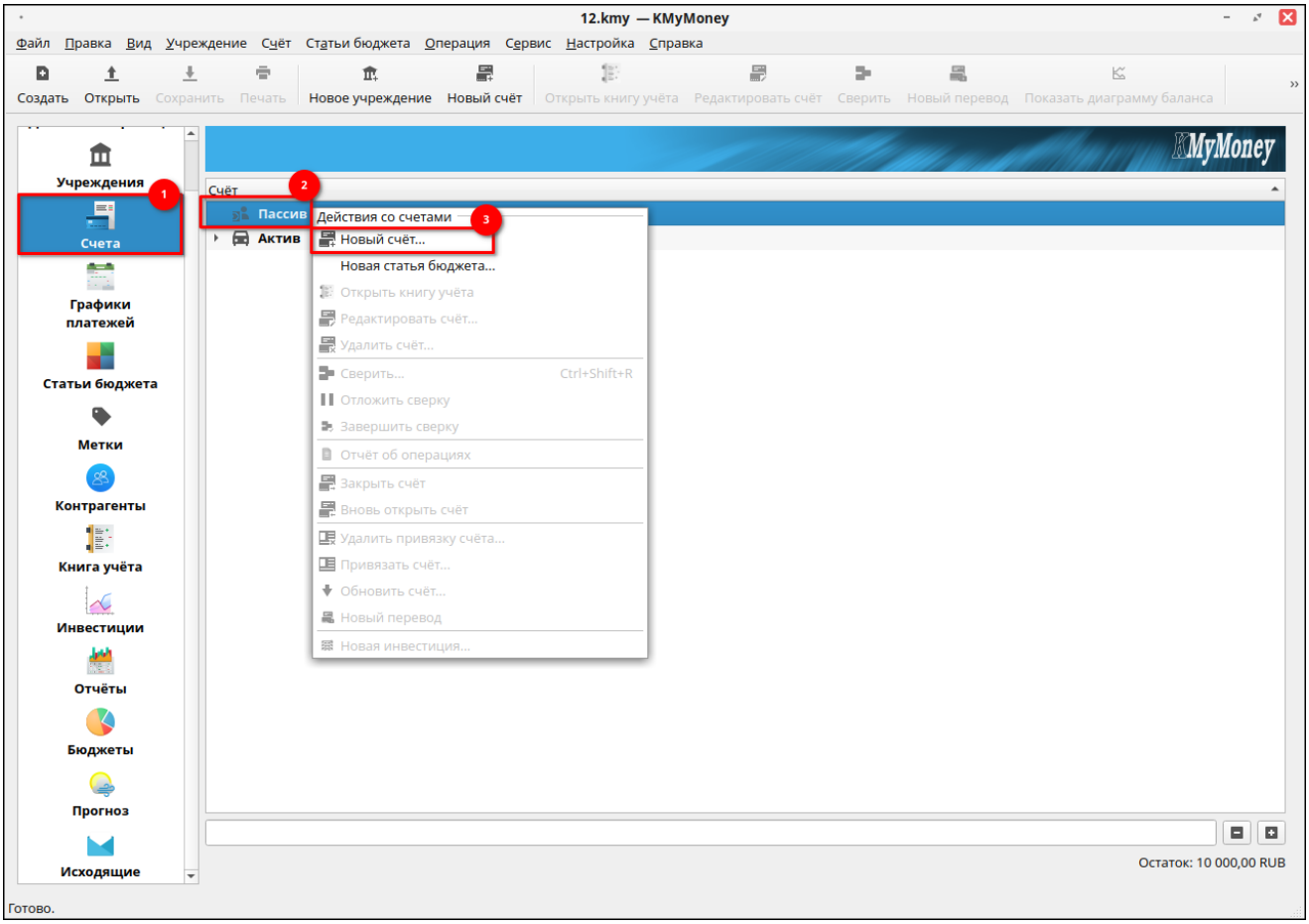
В представлении «**Счета**» можно внести информацию о наличных деньгах и пластиковых картах.

Существует несколько способов создания счёта. При любом способе вызывается **Мастер создания нового счета**. Мастер позволяет поэтапно указать сведения о счёте. Создайте счёт с помощью одного из нижеприведенных способов.

1. Для создания счёта с помощью меню выберите пункт меню «**Счёт**» **—** «**Новый счёт...**».



2. Для создания счёта с помощью представления счетов откройте представление «**Счета**» (1). Щёлкните ПКМ по значку дерева «**Пассивы**» (2) или «**Активы**» в рабочей области и выберите в контекстном меню пункт « **Новый счёт...**» (3).



3. Для создания счёта с помощью панели инструментов нажмите на значок «**Новый счёт**».

Для отслеживания счёта с помощью **KMyMoney** выберите счёт в меню « **Файл**» — «**Создать**».

Если ранее использовалась другая программа для управления личными финансами, её данные можно импортировать в **KMyMoney**.

Сводная информация по счетам будет показана на домашней странице.

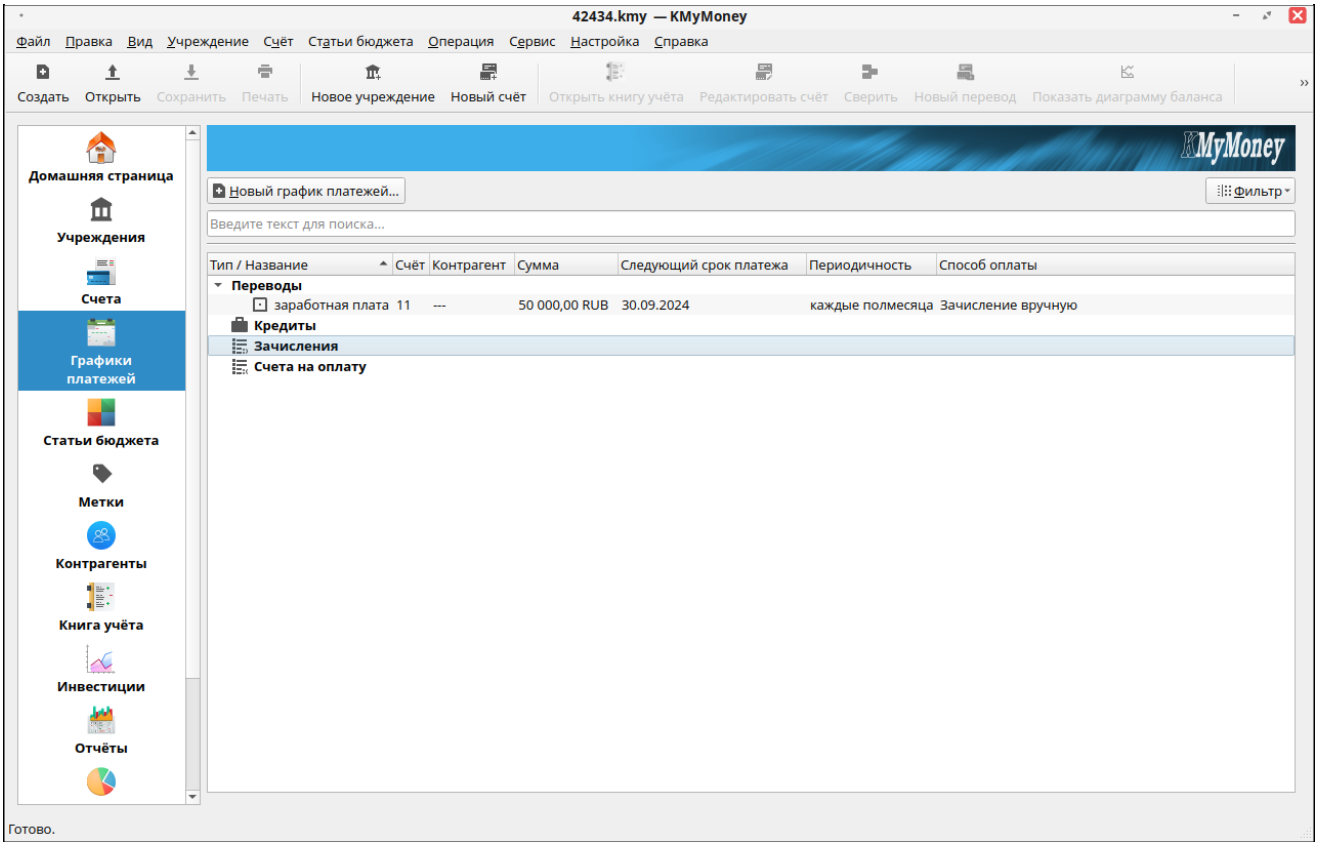
Операции можно создавать вручную в «**Книге учёта**» или автоматически, выполнив настройку параметров в представлении «**Графики**».

Создание графиков

С помощью графиков можно отражать поступление или расходование денежных средств, которое происходит на регулярной основе: платежи по заработной плате, налогам и сборам, страховке, кредитным картам, кредитам, ипотеке, аренде и коммунальным платежам. Планирование регулярных выплат позволяет получать напоминания.

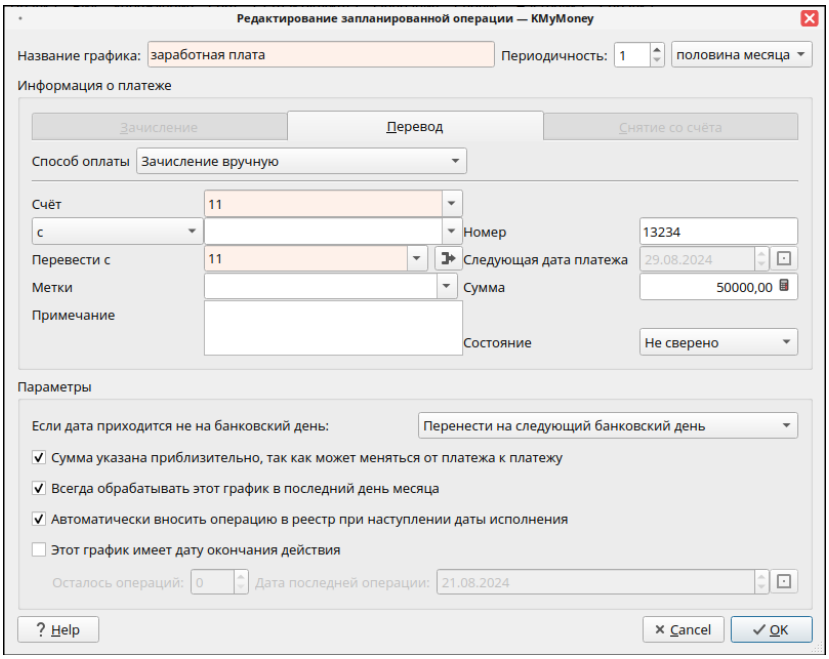
Типы графиков:

- **Переводы** — предназначен для средств, которые снимаются с одного счёта и поступают на другой;
- **Кредиты** — предназначен для работы с кредитным счётом;
- **Зачисления** — предназначен для средств, поступающих на счёт;
- **Счета на оплату** — предназначен для средств, выплачиваемых со счета.



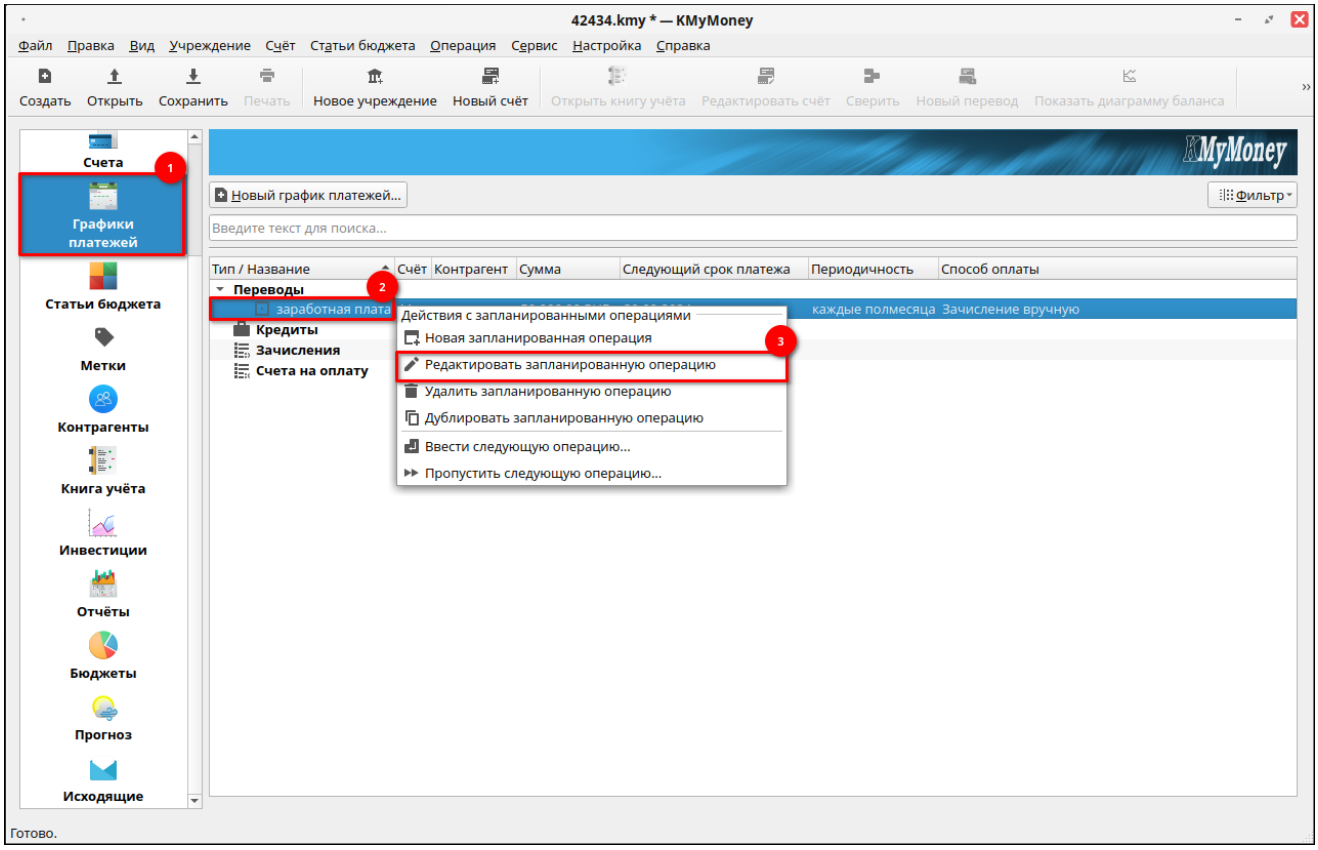
Для настройки графика платежей щёлкните по значку «**Графики**» в меню выбора представления. Необходимо указать следующие данные:

- Название графика,
- Периодичность,
- Способ оплаты,
- Следующая дата платежа,
- Сумма,
- Параметры операций,
- Параметры расписания.



По завершении настройки нажмите кнопку «**OK**».

Для редактирования графика выберите его в списке, щёлкните по нему ПКМ и выберите в контекстном меню пункт « **Редактировать запланированную операцию**».



Появится диалоговое окно, в котором можно указать необходимые данные.

Для удаления графика выберите график, щёлкните по нему ПКМ и выберите в контекстном меню пункт « **Удалить запланированную операцию**».

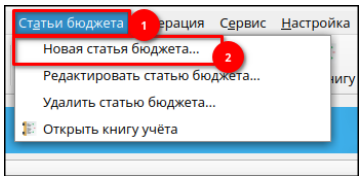
Для дублирования графика щёлкните по нему ПКМ и из контекстного меню выберите опцию « **Дублировать запланированную операцию**».

Статьи бюджета

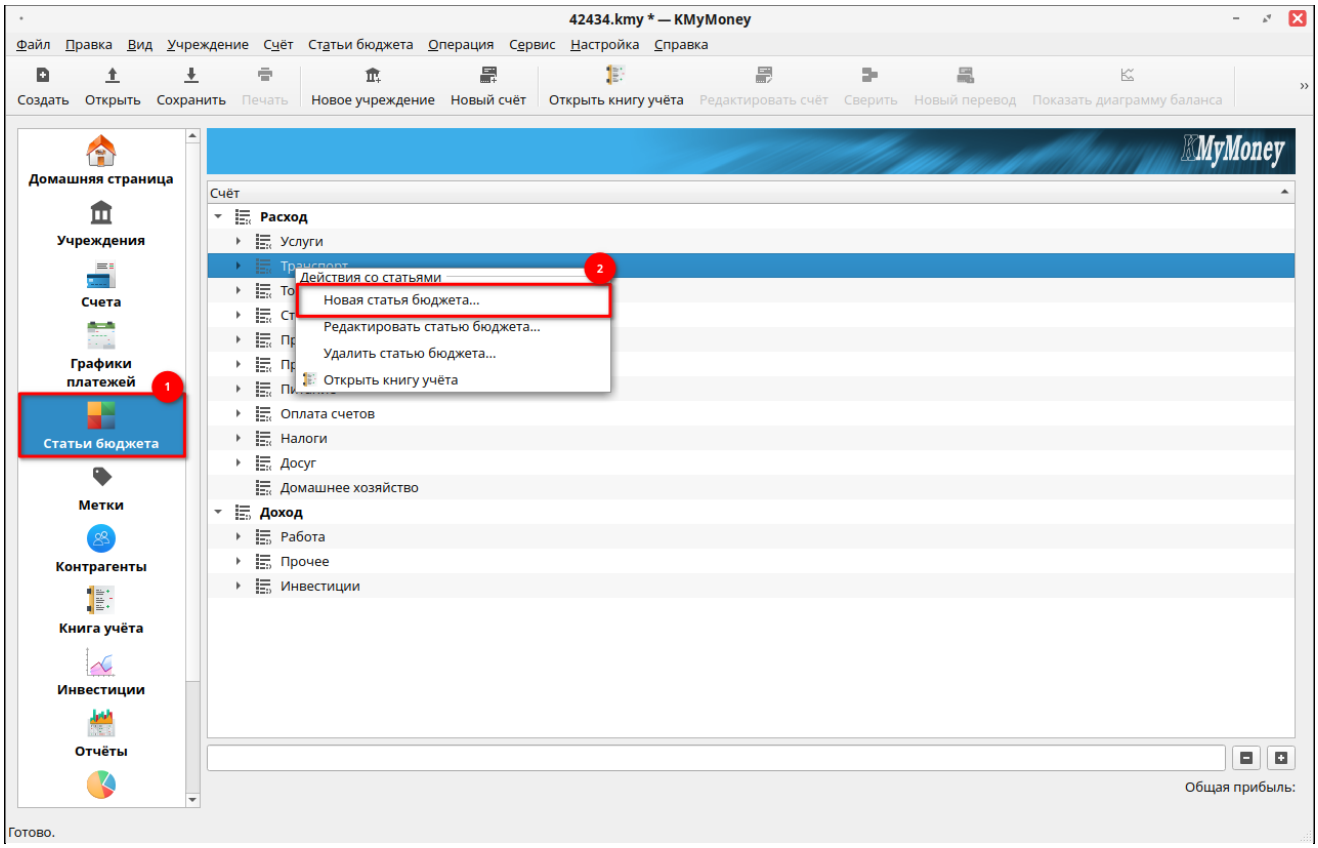
В представлении «**Статьи бюджета**» создаются статьи расходов и доходов. Для каждой из статей бюджета отображается общая сумма по операциям.

Для создания статьи выберете один из следующих способов.

1. Выберите пункт меню «**Статьи бюджета**» (1) — «**Новая статья бюджета...**» (2).



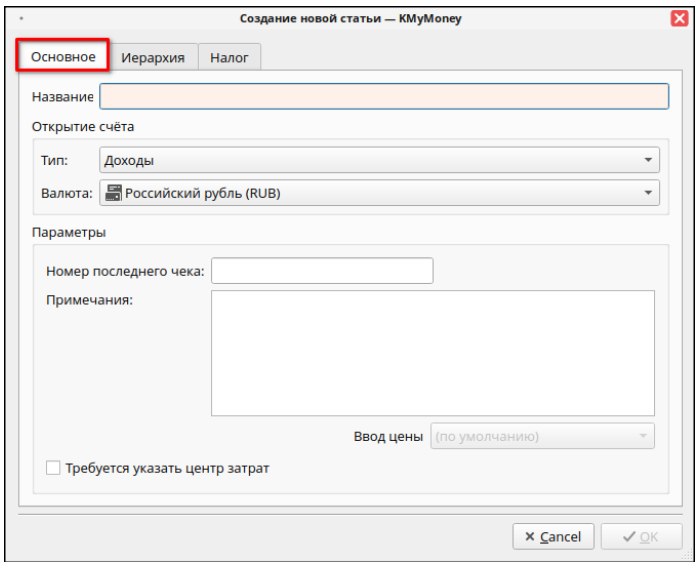
2. Выберите родительский элемент в дереве представления «**Статьи бюджета**» (1), щёлкните по нему ПКМ и выберите в контекстном меню пункт «**Новая статья бюджета...**» (2).



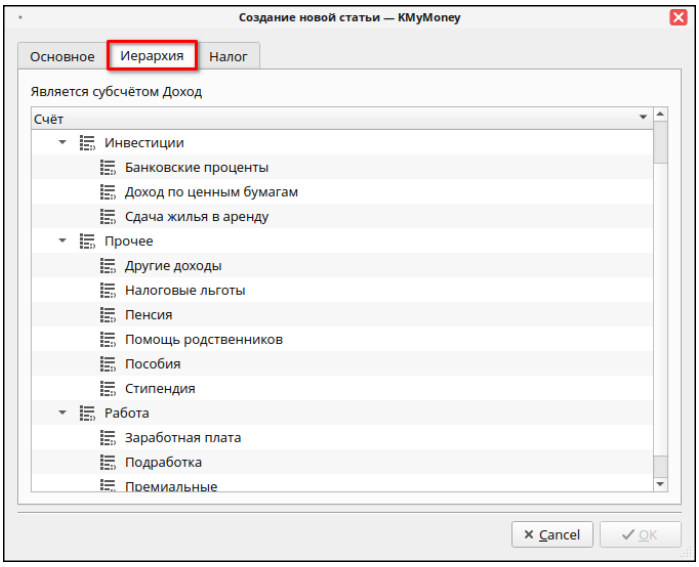
3. Укажите название новой статьи при добавлении или редактировании операции в книге учёта.

При любом способе будет открыто диалоговое окно «**Создание новой статьи**», которое содержит три вкладки: «**Основное**», «**Иерархия**», «**Налог**». На каждой из них можно изменить определённые параметры статьи.

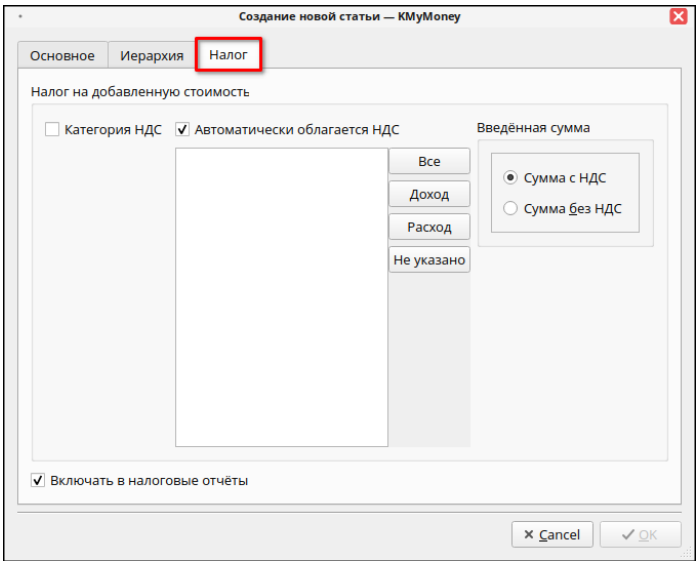
Вкладка «**Основное**» содержит редактируемые поля, в которых можно указать название, тип и валюту, а также поля « **Номер последнего чека**», «**Примечания**» и флаг «**Требуется указать центр затрат**».



На вкладке «**Иерархия**» для статьи можно выбрать подходящий вышестоящий счёт.



На вкладке «**Налог**» можно указать или изменить параметры НДС, а также установить флаг для включения статьи в налоговые отчёты. Статью расходов или доходов можно преобразовать в статью НДС и указать процентную ставку.



Для настройки статьи бюджета щёлкните по значку в меню выбора представления. Представление «**Статьи бюджета**» содержит сводные данные по всем существующим в текущей базе данных статьям бюджета. Статьи подразделены на доходы и расходы и расположены в алфавитном порядке. Для каждой из статей показано соответствующее значение баланса.

Для редактирования статьи щёлкните по её названию ПКМ и выберите в контекстном меню пункт « **Редактировать статью бюджета...**».

Для удаления статьи выберите её в дереве статей, щёлкните по ней ПКМ, в открывшемся контекстном меню нажмите « **Удалить**». Если со статьёй не связаны операции, графики платежей или бюджеты, она не установлена в качестве статьи по умолчанию для новых операций, она будет удалена.

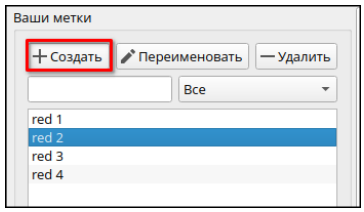
При удалении статей, имеющих связи, будет предложено определить другую статью для привязки связанных элементов или выбрать, следует ли удалять подкатегории.

Метки

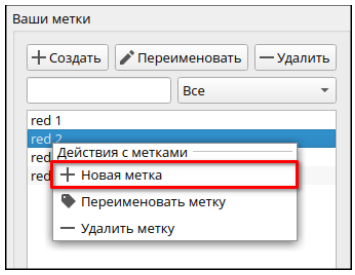
Представление «**Метки**» представляет собой счёта без управления, которые не имеют стоимости, использовать их необязательно.

Добавить новую метку можно тремя способами.

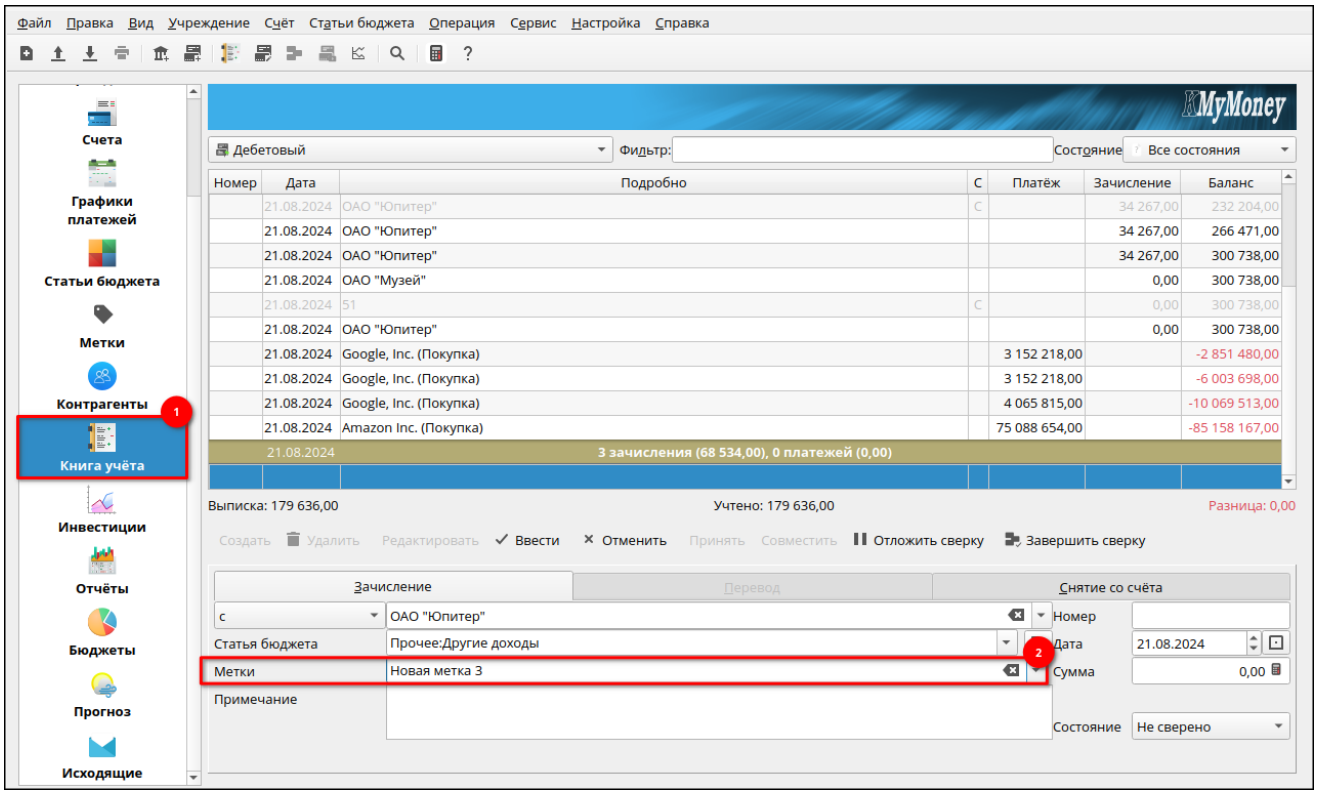
1. Щёлкните по кнопке «**Создать**», расположенной над списком меток.



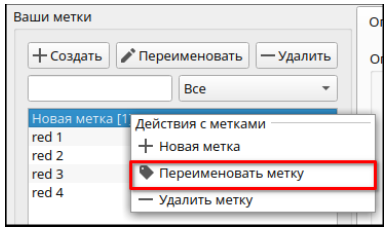
2. Щёлкните ПКМ по любой метке и выберите в контекстном меню пункт «**Новая метка**».



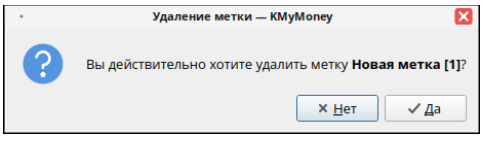
3. Введите название в поле «**Метки**» непосредственно на странице книги учёта или в окне разбивки операции.



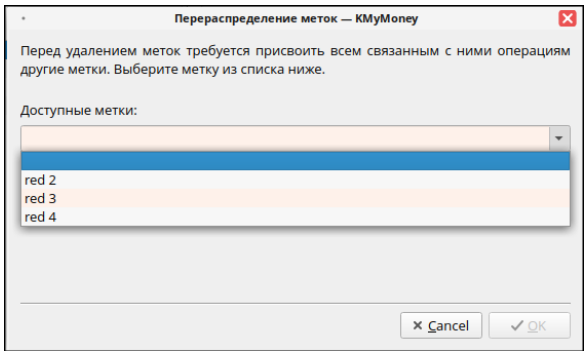
Для переименования метки щёлкните по её названию ПКМ и выберите в контекстном меню пункт « **Переименовать метку**».



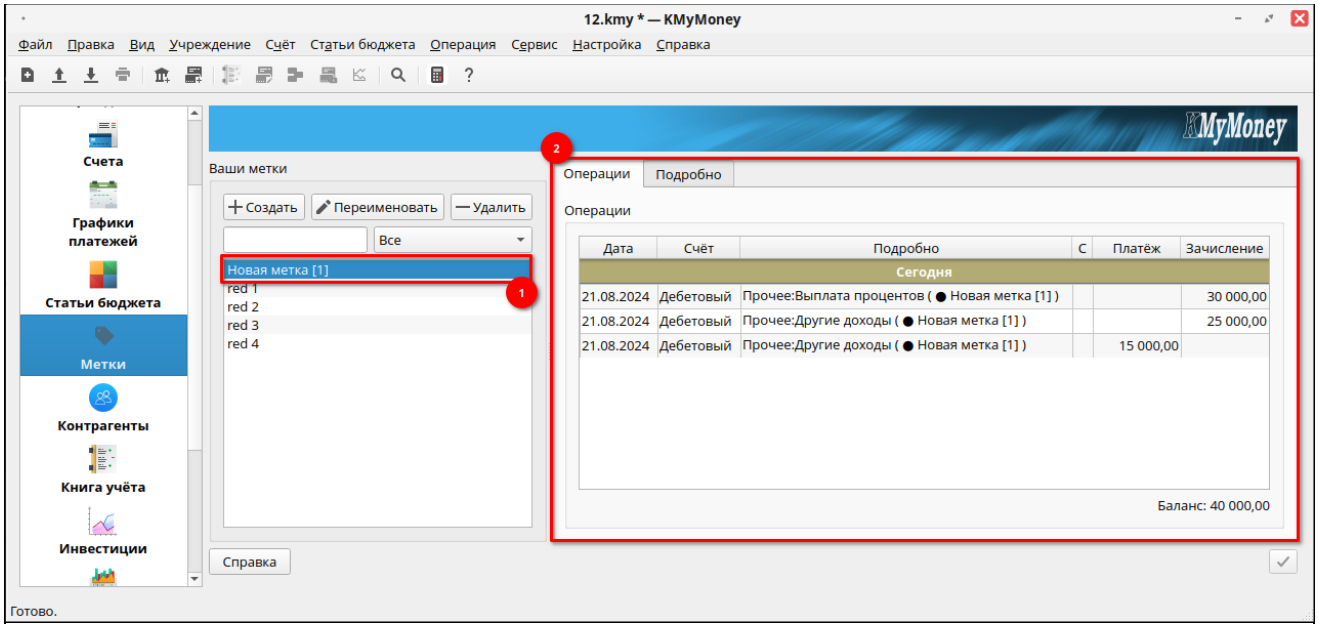
Для удаления метки щёлкните по её названию ПКМ и выберите в контекстном меню пункт «**Удалить метку**».



Если метка используется для каких-либо операций, появится диалоговое окно, которое позволяет назначить для них другую метку.

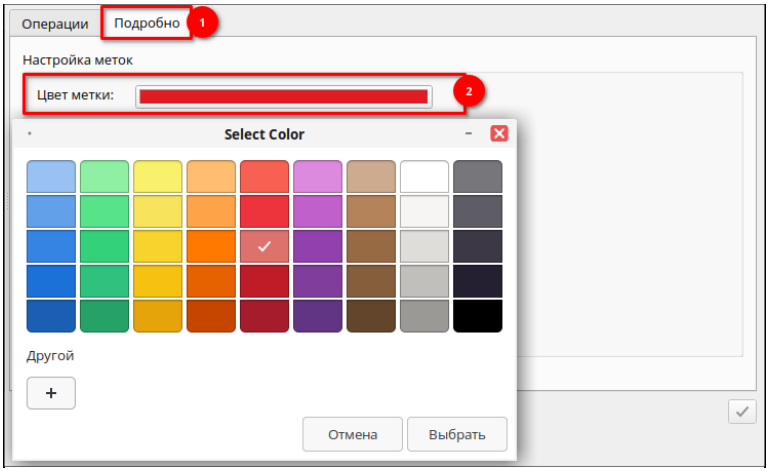


Для просмотра или редактирования операций, связанных с конкретной меткой выберите метку в списке и затем выберите соответствующую вкладку в правой части диалогового окна.



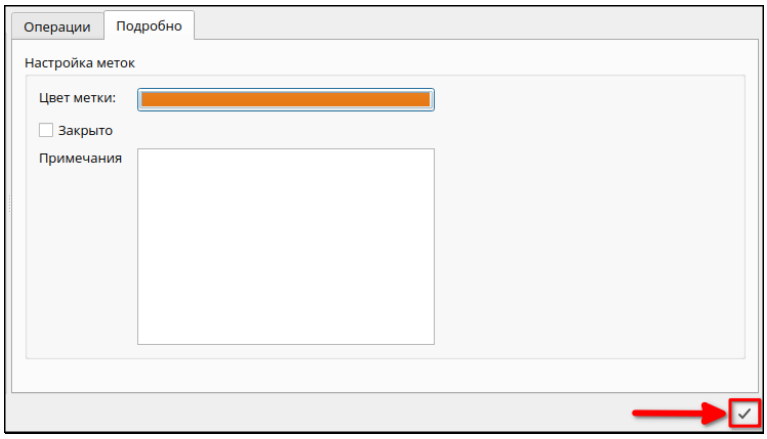
Для просмотра списка операций, для которых назначена выбранная метка, перейдите на вкладку «**Операции**». По двойному щелчку по записи операции она будет показана в книге учёта для счета, на котором к операции была добавлена метка.

Для просмотра и редактирования сведений, связанных с конкретной меткой, перейдите на вкладку «**Подробно**». Для вызова диалогового окна выбора цвета щёлкните по цветовой полосе.



Установка флага «**Закрыто**» сделает невозможным использование метки для новых операций.

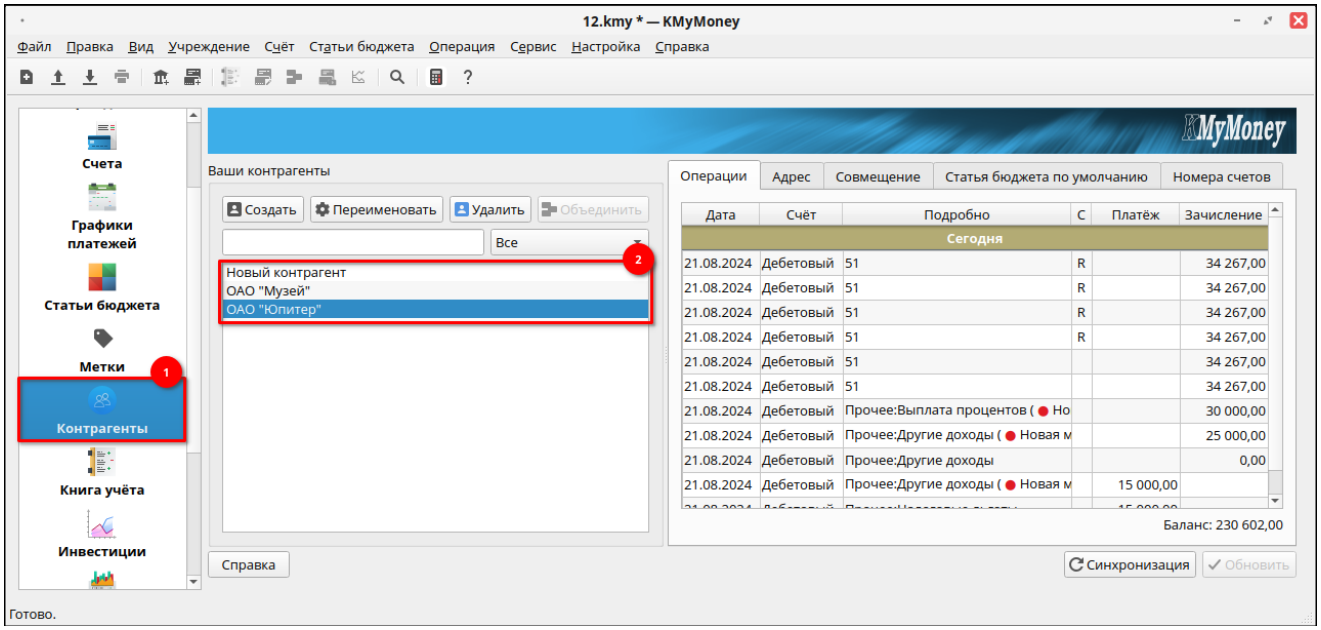
По завершении настройки нажмите кнопку «**Принять**», которая расположена в правой нижней части окна.



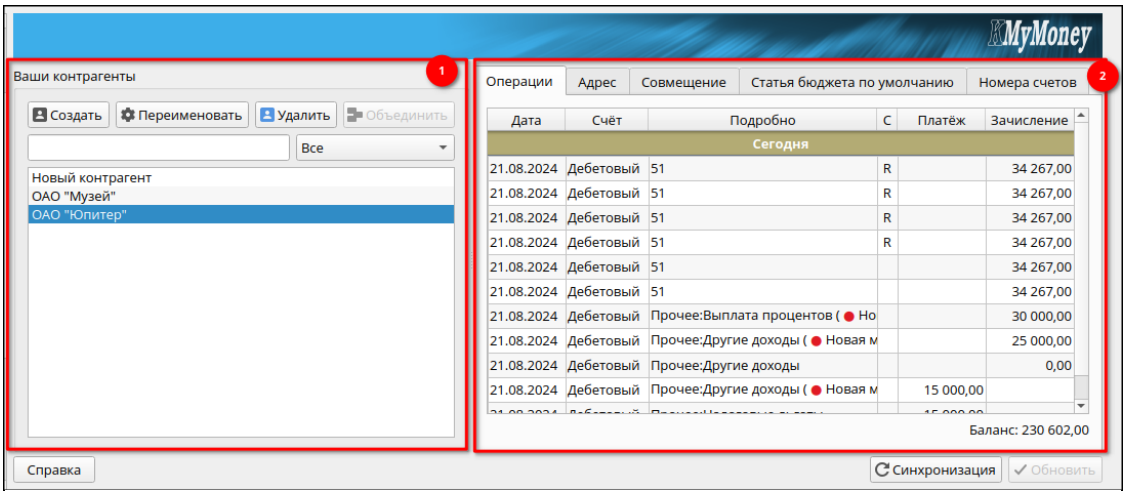
Контрагенты

Представление «**Контрагенты**» (1) содержит подробные сведения обо всех получателях и плательщиках, участвующих в операциях.

Сведения о контрагентах сохраняются на основе существующих операций, можно выбрать получателя из списка (2).



Представление «**Контрагенты**» содержит основные две области: «**Ваши контрагенты**» (1) и **область сведений** (2).



В области «**Ваши контрагенты**» можно создавать, переименовывать, удалять и объединять записи контрагентов. Контрагенты в списке упорядочены по алфавиту.

В **области сведений** доступны вкладки: операции, адрес, совмещение, статья бюджета по умолчанию и номера счетов для выбранного контрагента.

Для просмотра всех операций, связанных с контрагентом, выберите его в списке и перейдите в область сведений на вкладку

«**Операции**». Для открытия операции в «**Книге учёта**» дважды щёлкните по интересующей операции.

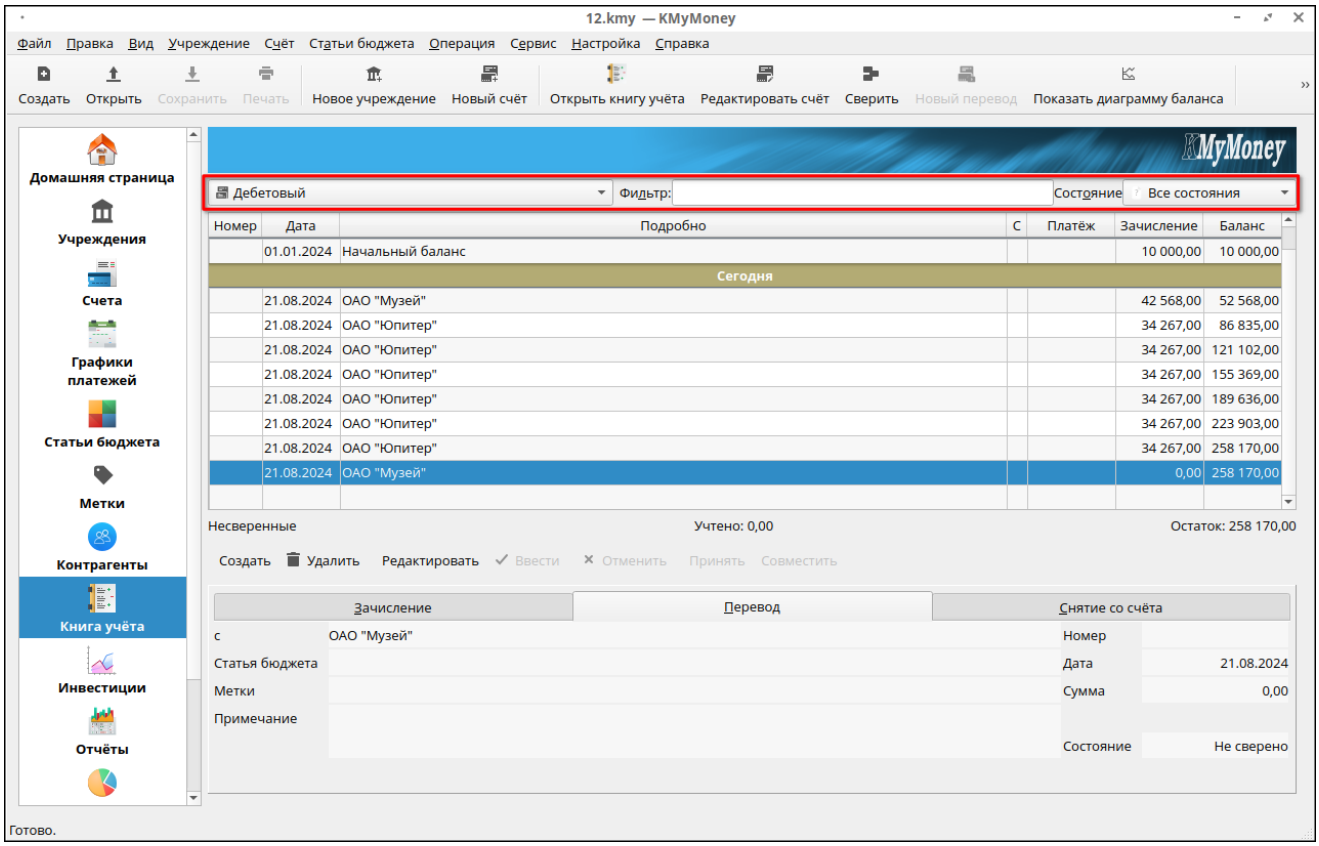
Книга учёта

Представление «**Книга учёта**» позволяет вносить, отслеживать, удалять и редактировать операции по заданным счетам.

Представление содержит три части:

- Область фильтра,
- Список операций,
- Форма ввода операций.

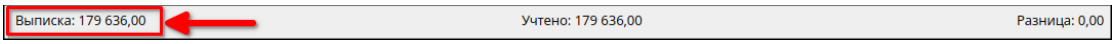
В области фильтра можно выбрать любой счёт. Параметры формы ввода операций зависят от типа счета.



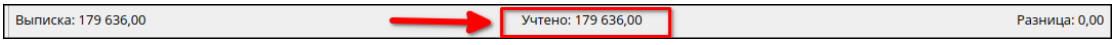
Внесённая операция будет показана в списке операций. Здесь можно изменить свойства операции или создать новую операцию. По умолчанию операции упорядочены по дате. Для изменения порядка сортировки операций щёлкните по заголовку списка операций ПКМ.

Под списком операций расположены три значения:

- **Последняя сверка**. Дата последней сверки счёта. Для выполнения сверки счета откройте его в книге учёта и, щёлкнув по значку, выберите пункт меню «**Счёт**» **—** «**Сверить...**».



- **Учтено**. Общая сумма по всем учтённым и сверенным операциям по счёту. Более подробные сведения об учёте и сверке операций доступны в этом разделе.



- **Остаток** представляет собой сумму всех операций по счёту. Остаток будет показан только при выборе одной операции.

Номер	Дата	Подробно	С	Платёж	Зачисление	Баланс
	01.01.2024	Начальный баланс			10 000,00	10 000,00
		Сегодня				
	21.08.2024	ОАО "Музей"	R		42 568,00	52 568,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	86 835,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	121 102,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	155 369,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	189 636,00
	21.08.2024	ОАО "Юпитер"			34 267,00	223 903,00
	21.08.2024	ОАО "Юпитер"			34 267,00	258 170,00
	21.08.2024	ОАО "Музей"			0,00	258 170,00

Несверенные | Учтено: 179 636,00 | Остаток: 258 170,00

При выборе нескольких операций будет показана их сумма.

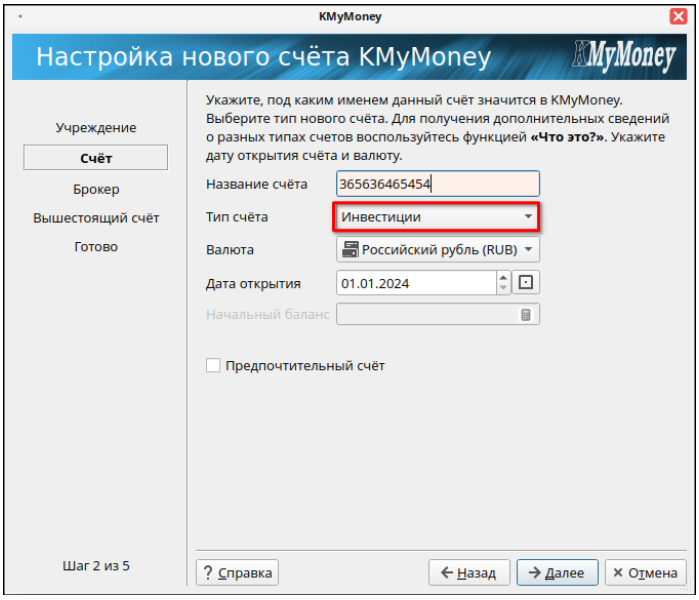
Номер	Дата	Подробно	С	Платёж	Зачисление	Баланс
	01.01.2024	Начальный баланс			10 000,00	10 000,00
		Сегодня				
	21.08.2024	ОАО "Музей"	R		42 568,00	52 568,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	86 835,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	121 102,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	155 369,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	189 636,00
	21.08.2024	ОАО "Юпитер"			34 267,00	223 903,00
	21.08.2024	ОАО "Юпитер"			34 267,00	258 170,00
	21.08.2024	ОАО "Музей"			0,00	258 170,00

Несверенные | Учтено: 179 636,00 | ∑: 102 801

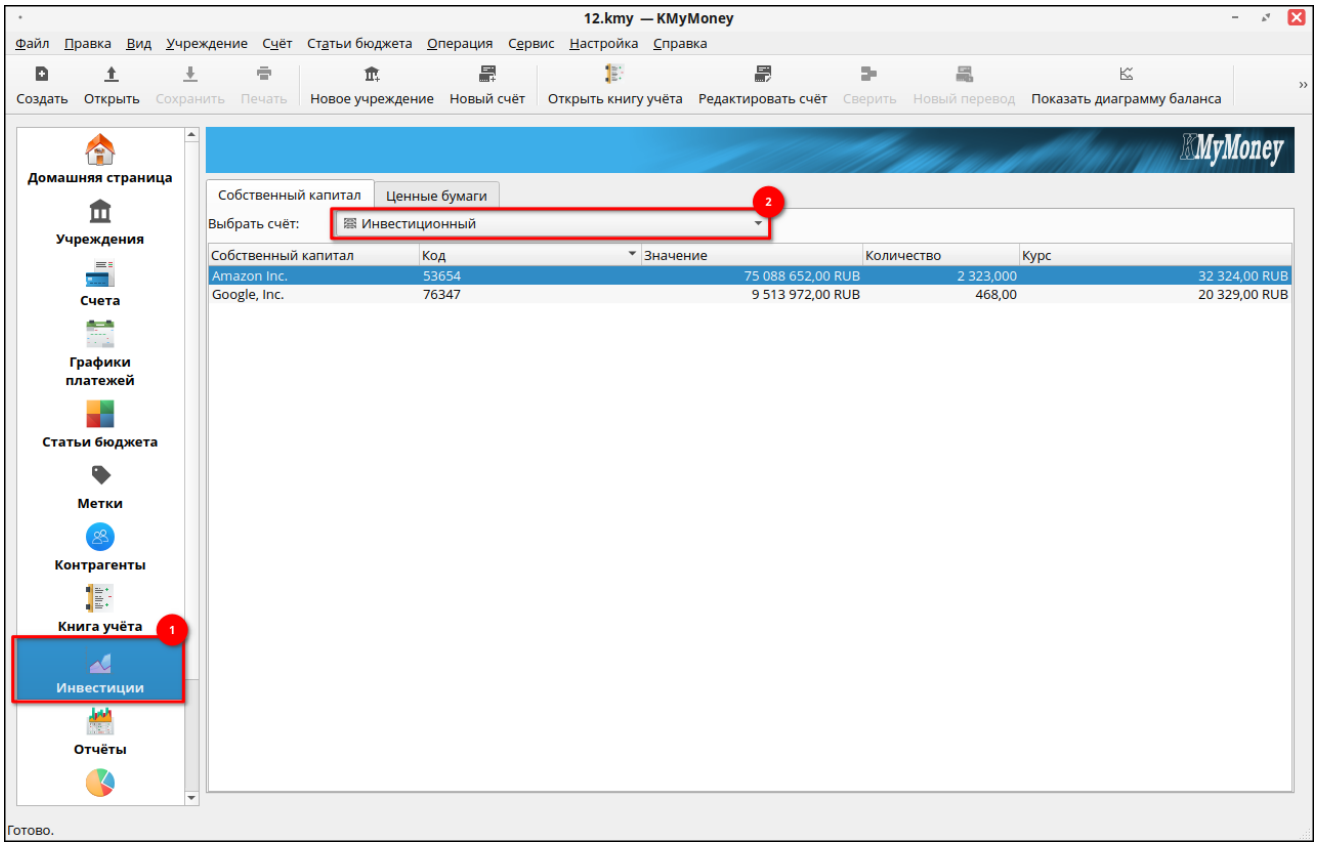
Инвестиции

Инвестиционные счета KMyMoney предназначены только для ценных бумаг. У каждой ценной бумаги имеется базовая валюта, в которой она продаётся или покупается. Если при инвестиционной операции присутствуют денежные средства, она должна быть связана с **брокерским счётом**, на котором хранятся деньги.

Для создания инвестиционного счёта для хранения информации о ценных бумагах выберите пункт меню «**Счёт**» — «**Новый счёт...**». При создании счёта укажите в поле тип счёта «**Инвестиции**».

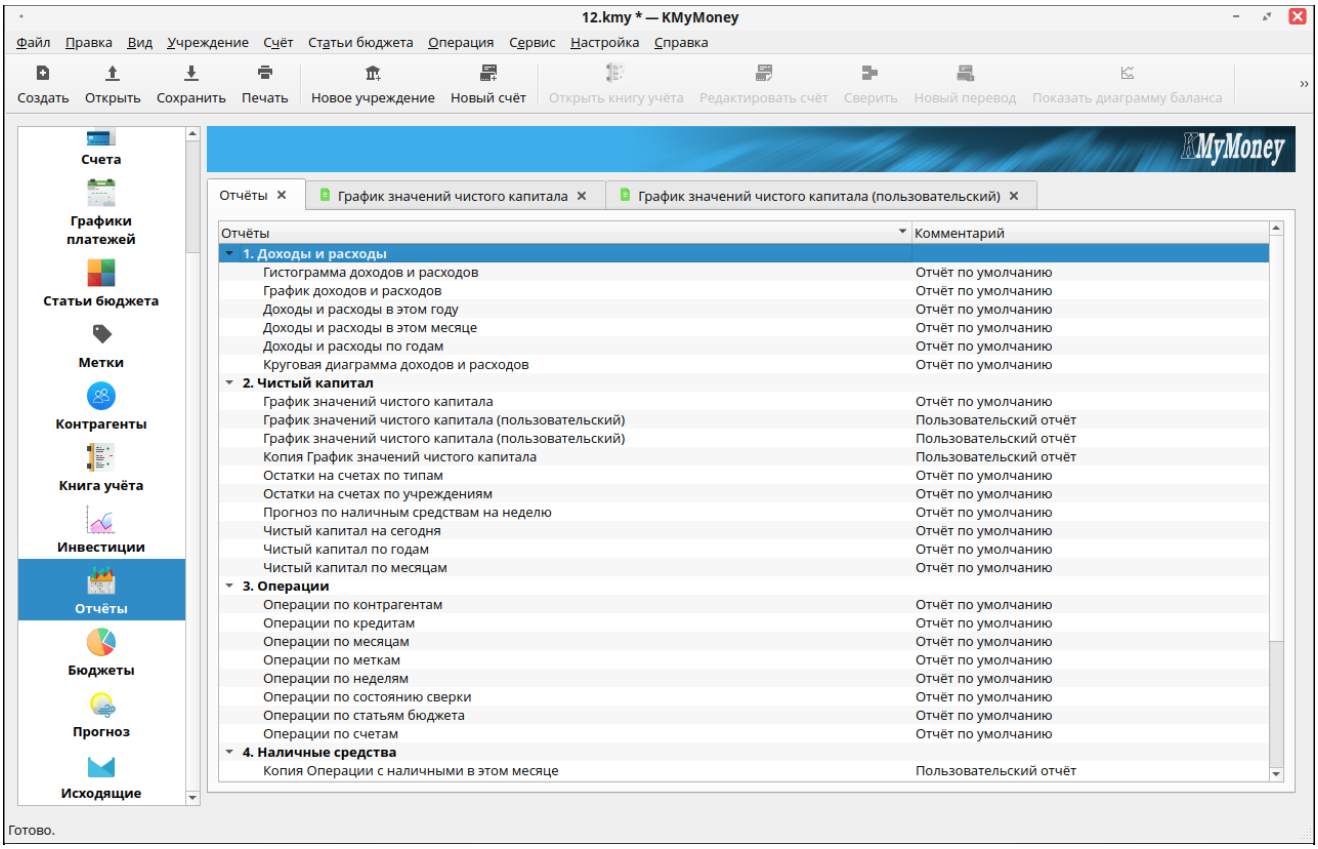


Для работы с новым инвестиционным счётом перейдите к просмотру представления «**Инвестиции**» (1) и выберите созданный счёт в раскрывающемся списке «**Выбрать счёт**» (2).

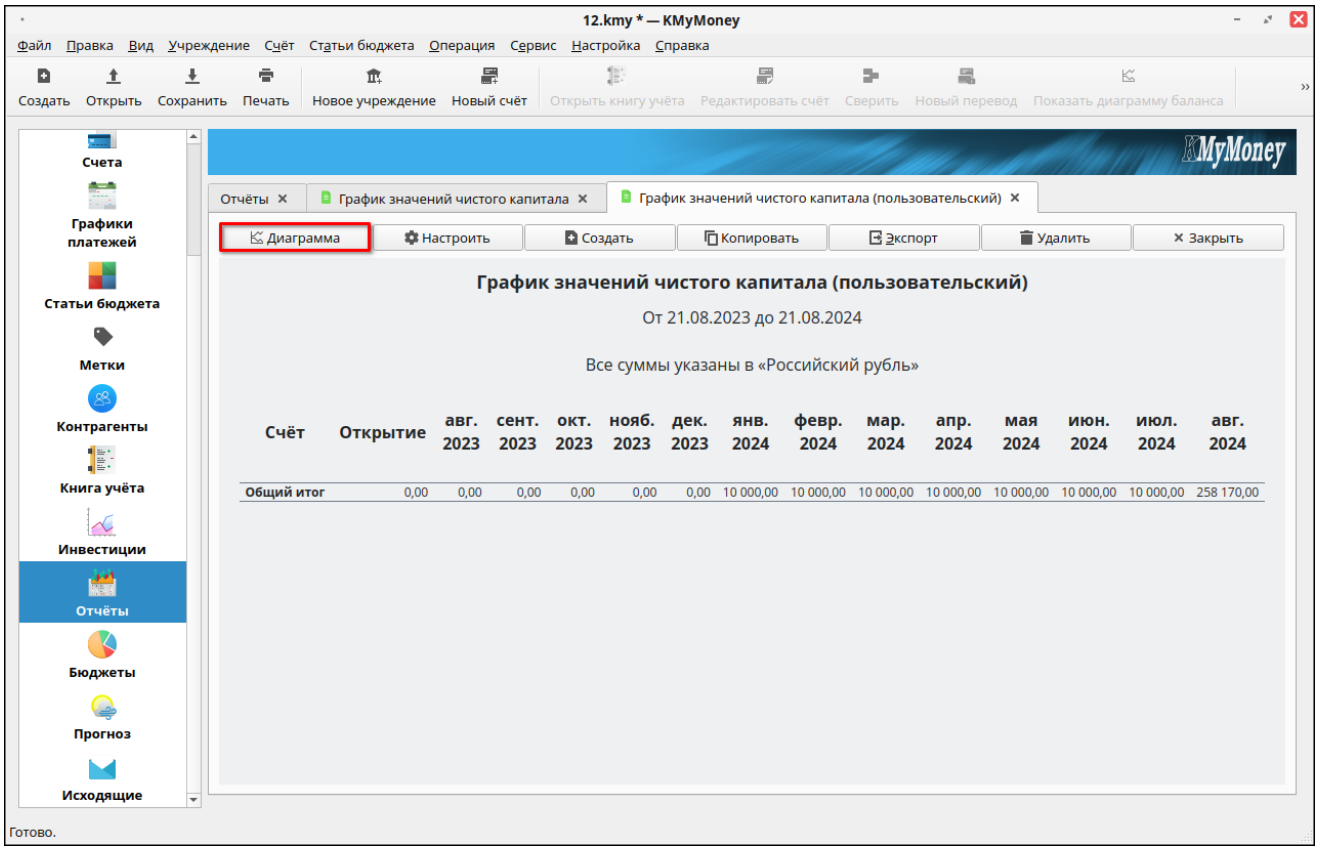


Отчёты

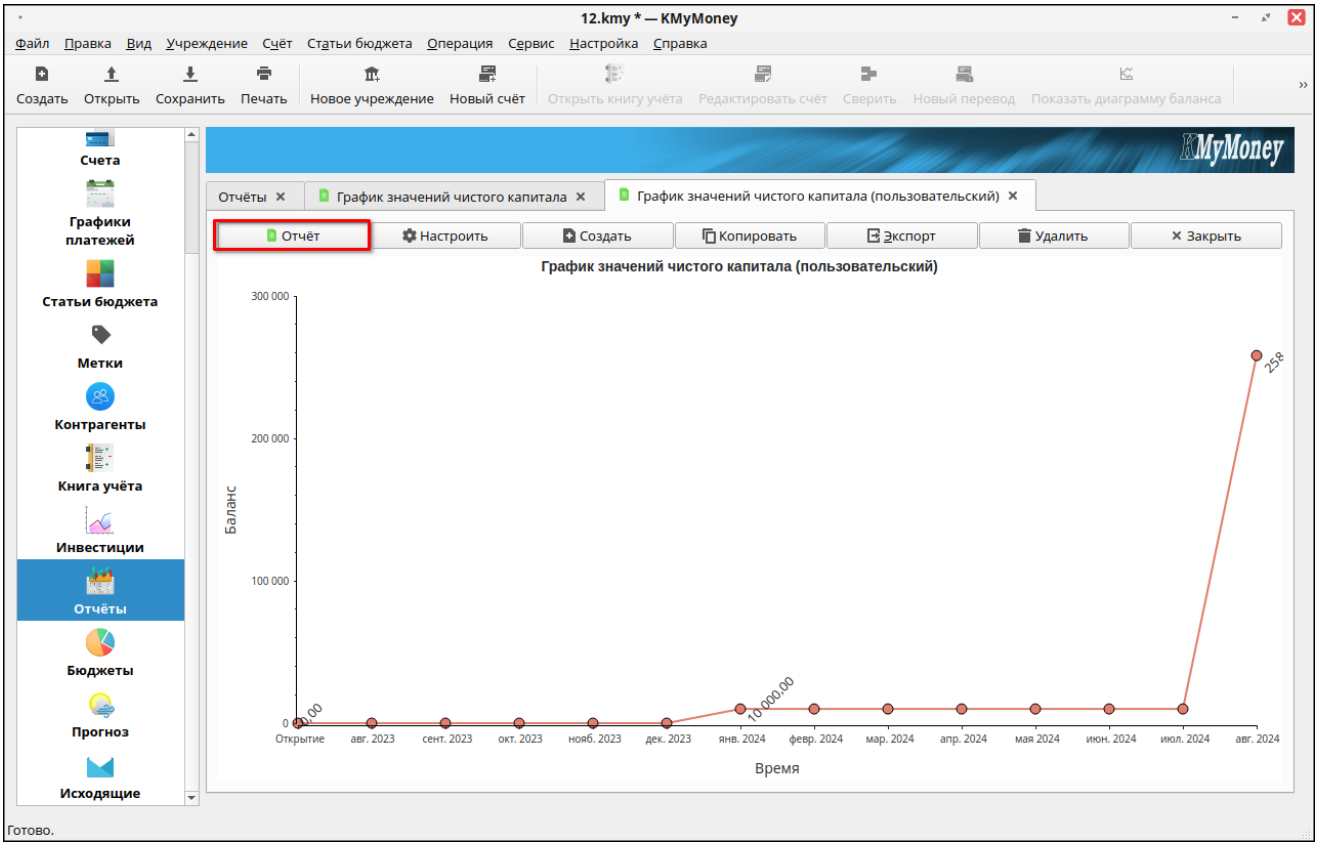
Итоги отчётного периода можно посмотреть в представлении «**Отчёты**» в текстовом или в графическом виде. **KmyMoney** позволяет выводить множество отчётов. Имеется набор стандартных отчётов. Ссылку на любой отчёт можно разместить на домашней странице.



Переключиться на графическое представление отчёта можно с помощью кнопки «**Диаграмма**».

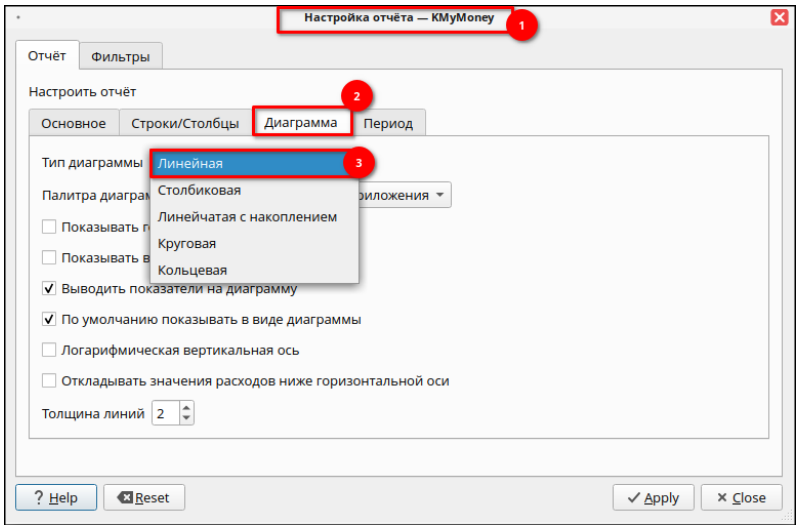


Переключиться на текстовое представление отчёта можно с помощью кнопки «**Отчёт**».

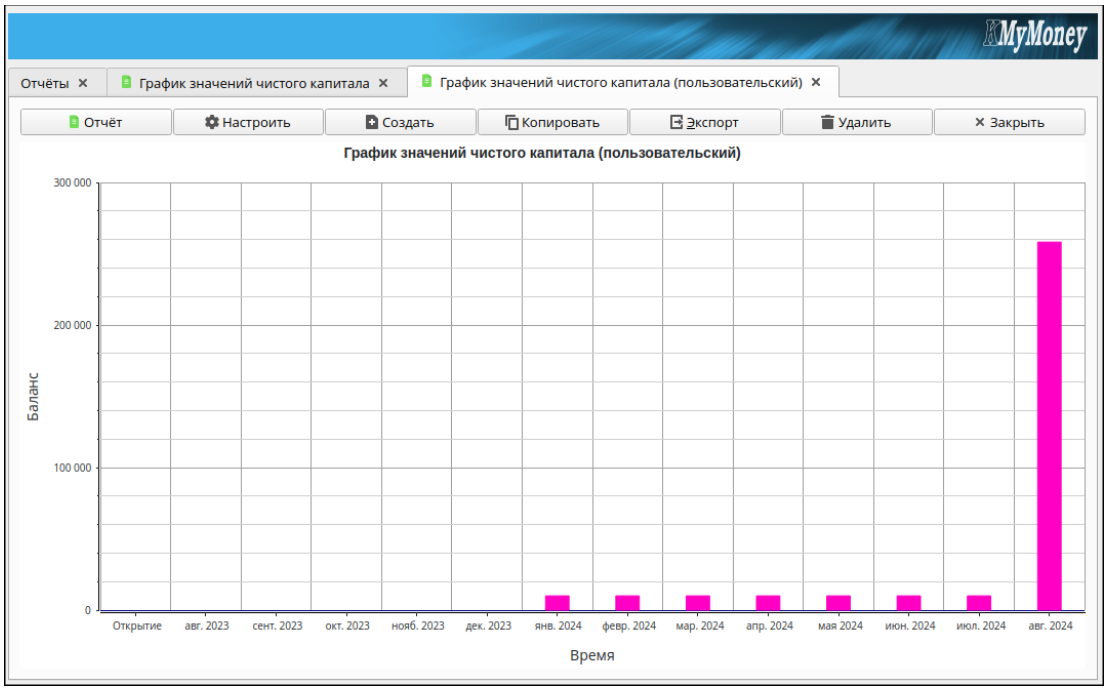


Внешний вид отчётов можно редактировать с помощью диалогового окна настройки отчёта.

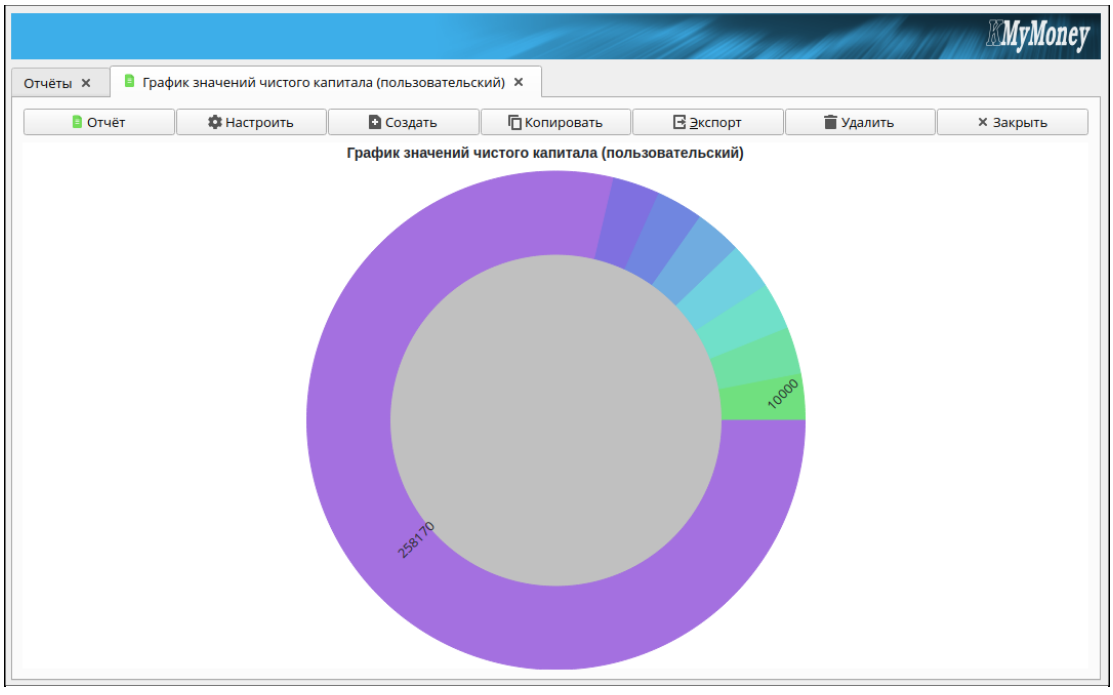
В настройках отчёта (1) на вкладке «**Диаграмма**» (2) можно задать тип диаграммы (3):



Столбиковая диаграмма аналогична линейной, но в ней для каждого временного среза будет показан столбец, соответствующий значениям.



Кольцевая диаграмма похожа на круговую, но в ней будет показано по одному кольцу для каждого временного среза в отчёте.



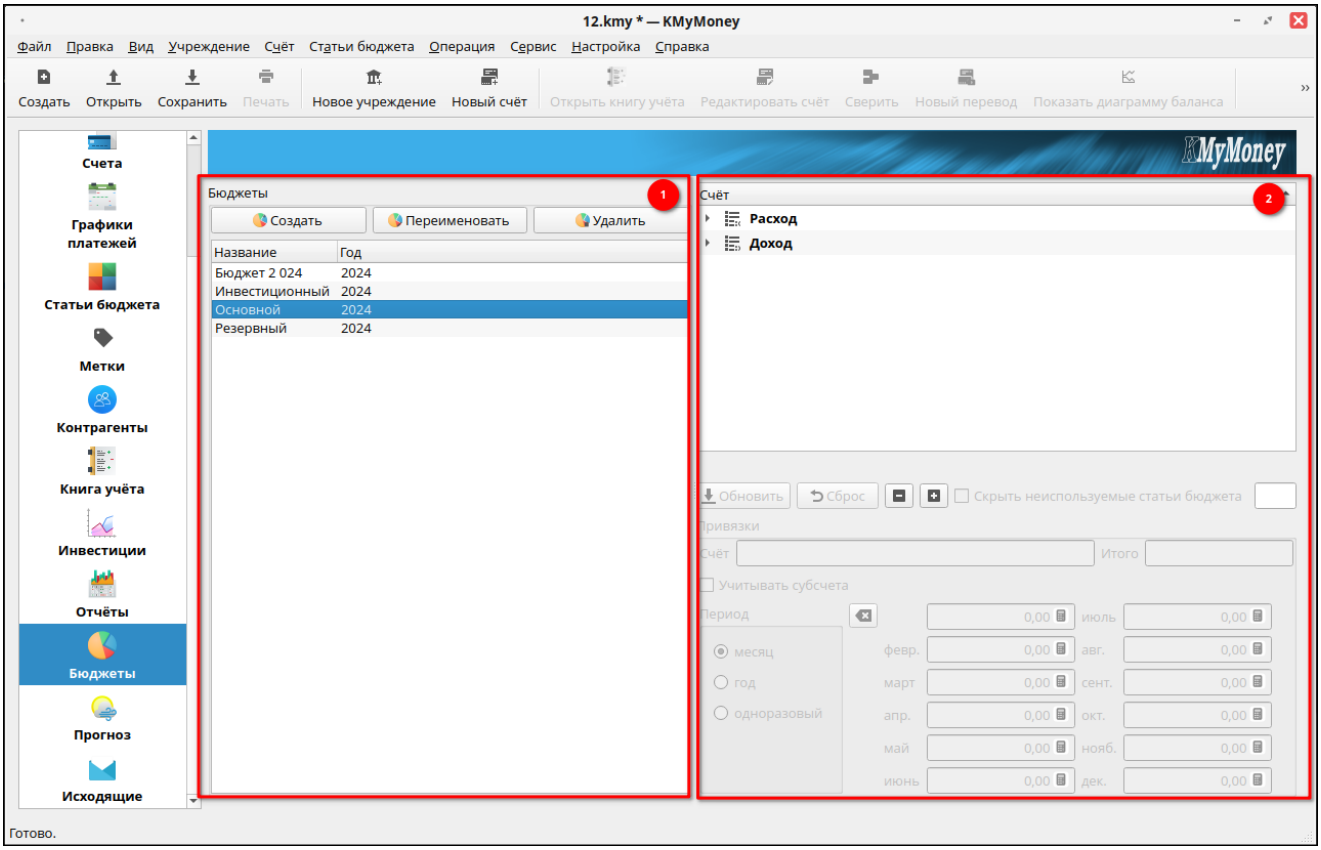
Бюджеты

Бюджет — это упорядоченный по статьям список ожидаемых доходов и расходов за определённый период. Для одного года можно создать несколько бюджетов.

В представлении «**Бюджеты**» есть две основных части:

1. Слева доступны список бюджетов пользователя и кнопки для создания, переименования и удаления бюджетов.

2. Справа отображается: список счетов и дополнительные параметры настройки бюджета.

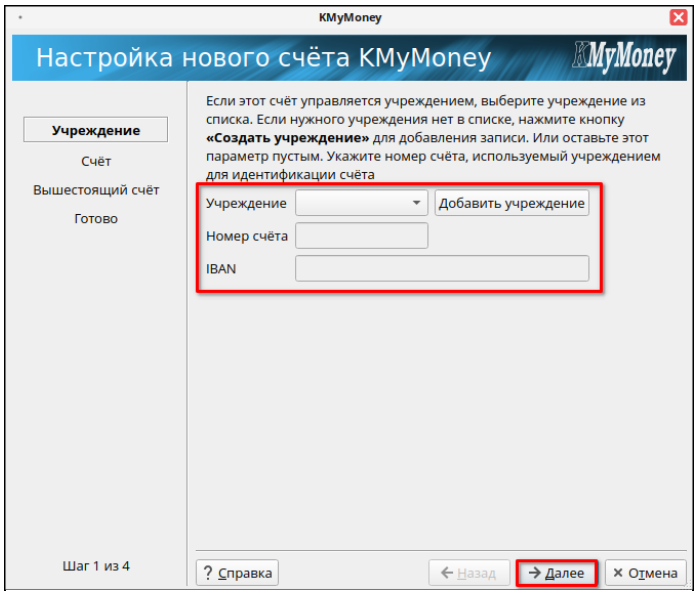


Пример работы

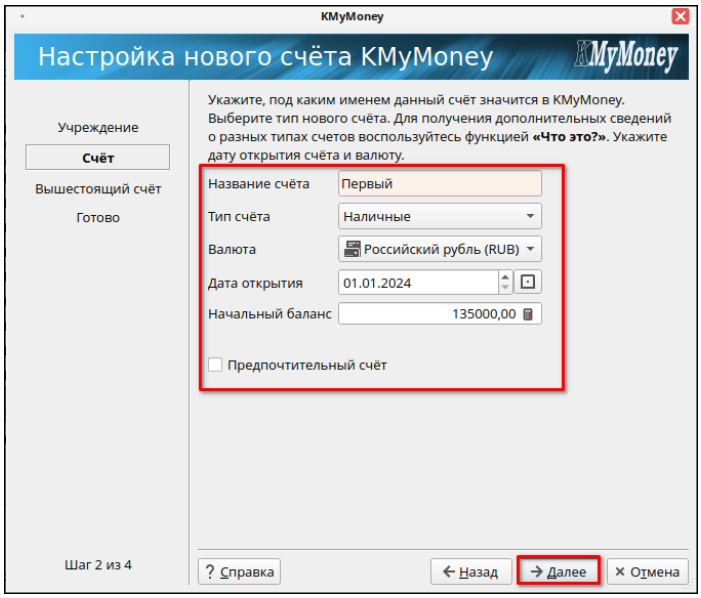
Рассмотрим пример ведения бюджета в личных целях.

1. Первоначально создайте счёт для учёта наличных денег. Для этого перейдите в меню «**Счёт**» — «**Новый счёт**».

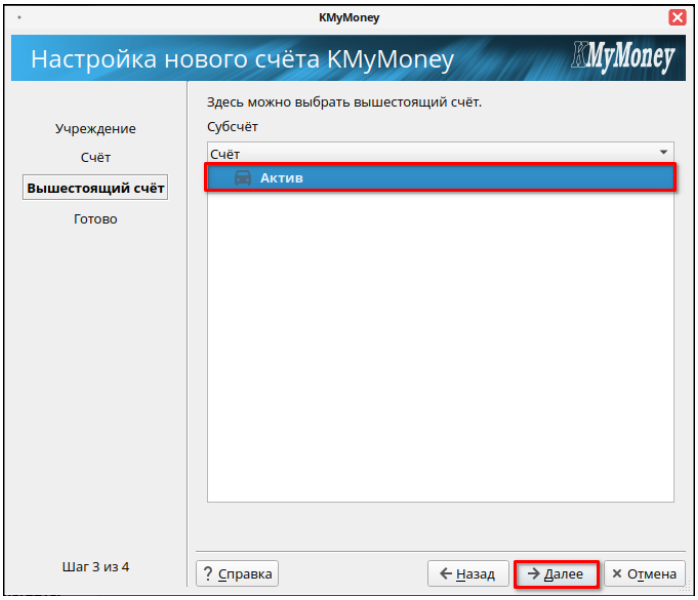
В мастере создания счета на первом шаге предлагается указать учреждение, в котором находятся деньги. Вы можете пропустить этот шаг и нажать «**Далее**».



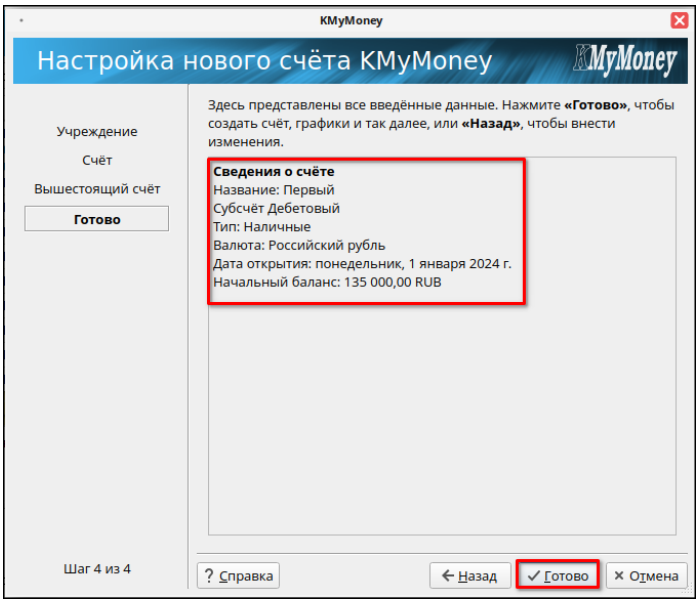
2. Введите название счёта, из списка выберите тип счёта «**Наличные**», укажите валюту и начальный остаток на счёте. Если вы хотите, чтобы этот счёт использовался по умолчанию, установите флажок рядом с опцией «**Предпочтительный счёт**».



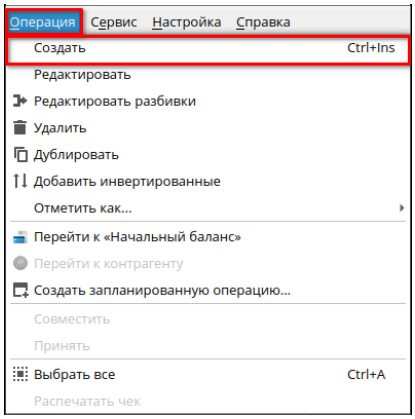
3. На следующем шаге выберите родительский счёт, укажите «**Актив**» и нажмите «**Далее**».



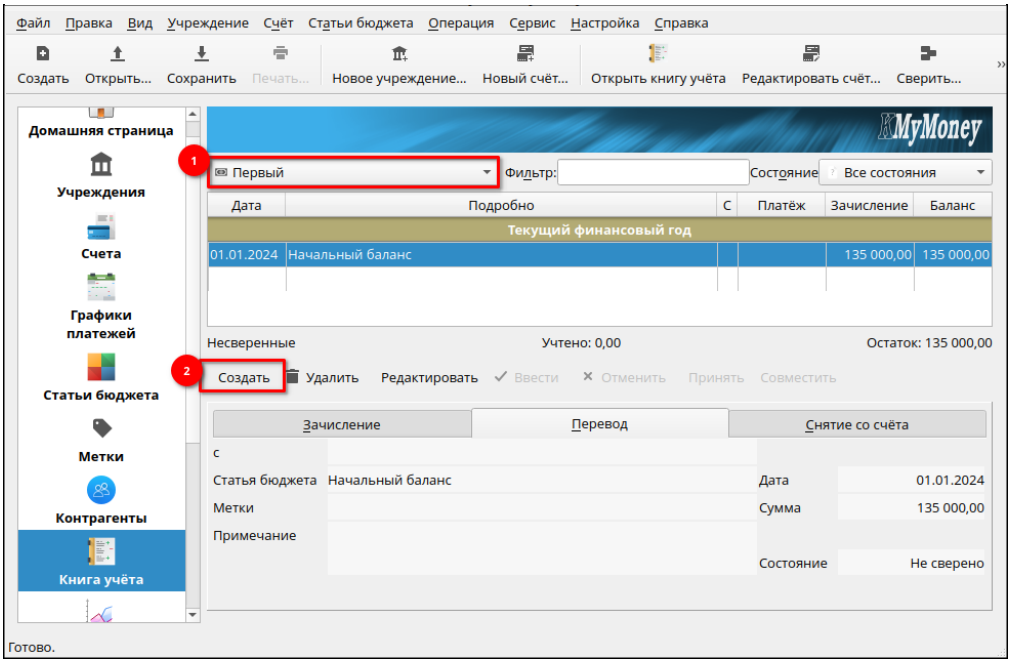
4. Просмотрите сводную информацию о созданном счёте и нажмите «**Готово**».



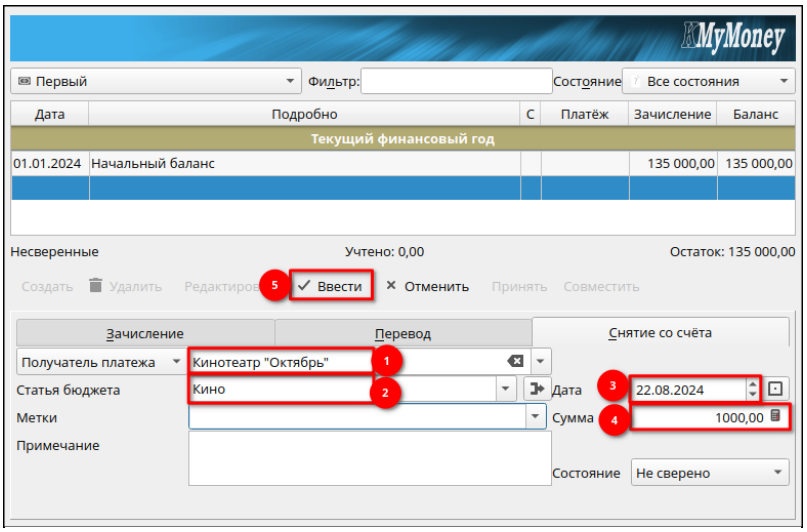
5. Для учёта расходов выберите в меню «**Операция**» — «**Создать**».



6. Выберите из списка счёт (1), с которого вы производите платёж. Это тот счёт, с которого будут списаны денежные средства. Нажмите кнопку «**Создать**» (2).

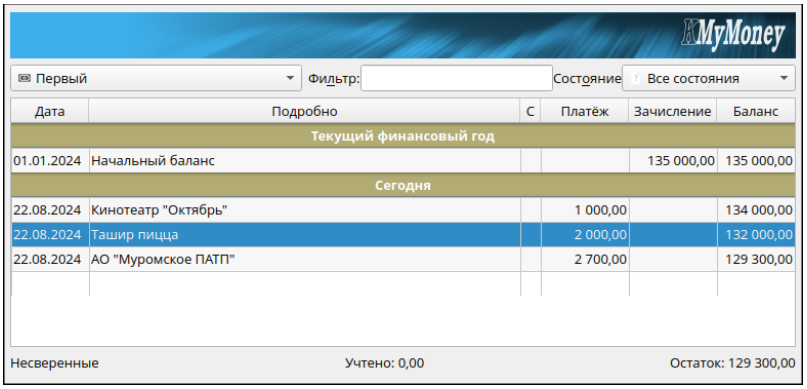


7. Перейдите на вкладку «**Снятие со счета**». Введите данные о получателе платежа (1) и согласитесь на добавление получателя. Укажите статью бюджета (2), дату (3) и сумму платежа (4). При желании добавьте примечание. Нажмите «**Сохранить**» или клавишу **Enter**. Повторите этот процесс для всех ваших платежей.

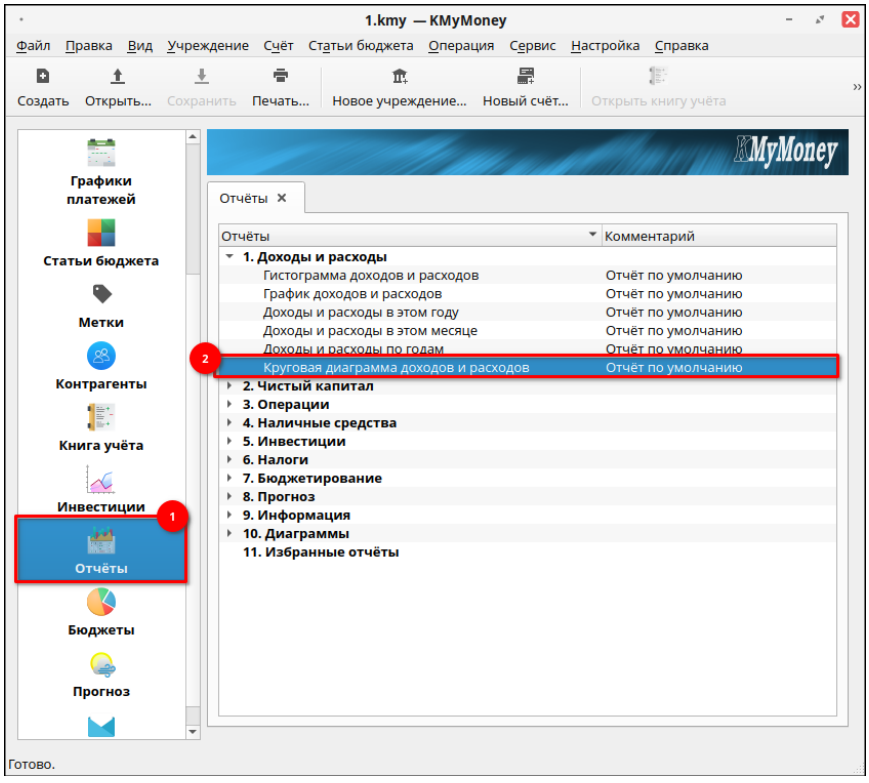


8. Доходы учитываются на вкладке «**Зачисления**». Если вы переводите деньги со счёта в кошелёк, используйте вкладку « **Перевод**».

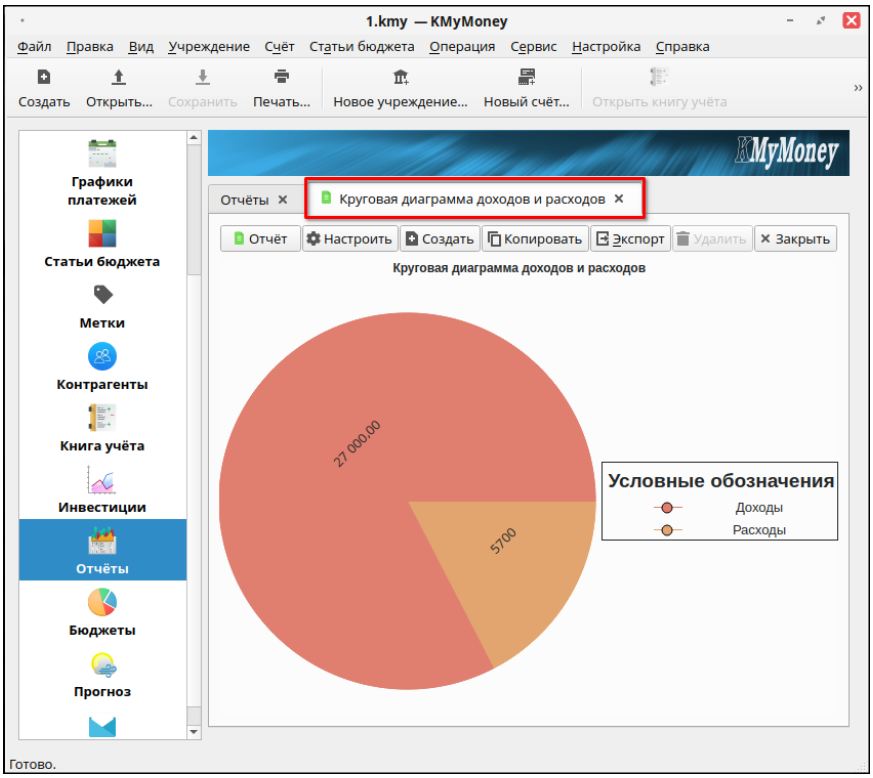
9. В окне операций отображаются все проведённые операции со счётом: зачисления, списания, остатки после каждой операции и текущий остаток, а также получатели и отправители платежей.



10. Для отслеживания движения денежных средств нажмите на значок «**Отчёты**» (1). В открывшемся списке выберите нужный вид отчёта (2).



Программа отобразит выбранную диаграмму. В примере круговая диаграмма доходов и расходов.


1.kmy — KMyMoney
Файл Правка Вид Учреждение Счёт Статьи бюджета Операция Сервис Настройка Справка
Создать Открыть... Сохранить Печать... Новое учреждение... Новый счёт... Открыть книгу учёта
Графики платежей
Статьи бюджета
Метки
Контрагенты
Книга учёта
Инвестиции
Отчёты
Бюджеты
Прогноз
KMyMoney
Отчёты
Круговая диаграмма доходов и расходов
Отчёт Настроить Создать Копировать Экспорт Удалить Закрыть
Круговая диаграмма доходов и расходов
27 000.00
5700
Условные обозначения
Доходы
Расходы
Готово.

Livemedia-creator – создание образа системы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** lorax-31.11-1

Livemedia-creator автоматизирует процесс создания образа системы. *Livemedia-creator* входит в состав пакета **lorax**. Процесс создания установочного образа в *livemedia-creator* включает два этапа: сначала создается временный образ дистрибутива в соответствии с настройками в файле **kickstart**, затем *livemedia-creator* создает загрузочный образ.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install lorax
```

Также необходимо установить дополнительные пакеты:

```
dnf install virt-install libvirt qemu-kvm
```

Livemedia-creator использует **virt-install** для создания временной виртуальной машины, где будет запущен процесс создания образа. Для создания образа потребуется файл *kickstart* и загрузочный ISO-образ.

Пример использования:

```
livemedia-creator --make-iso --iso=/home/user/redos-MUROM-7.3.1-20220225.0-Everything-x86_64-DVD1.iso --ks=/root/test-ks.cfg --tmp=/home/user/lmc --iso-only --project=REDOS --releasever=7.3.1
```

Опции:

- **--iso** - путь к установочному образу;
- **--ks** - путь к файлу *kickstart*;
- **--tmp** - указывает директорию, в которую будет сохранен образ. По умолчанию используется **/var/tmp**;
- **--iso-only** - после завершения создания образа будет сохранен только загрузочный образ (ISO-файл);
- **--project** - имя операционной системы, которое будет отображаться в загрузчике;
- **--releasever** - версия операционной системы в загрузчике.

Более подробную информацию о других опциях можно узнать из официальной документации по ссылке: https://weldr.io/lorax/livemedia-creator.html.

Информацию по созданию kickstart-файла см. в нашей статье «Автоматизация развертывания (kickstart)».

После выполнения команды будет запущена временная виртуальная машина, где начнется процесс создания образа. К машине можно подключиться через **VNC**, чтобы понаблюдать за процессом установки. По умолчанию адрес VNC **127.0.0.1:0**.

После завершения установки образ будет сохранен в указанной директории в виде файла с названием **boot.iso** (по умолчанию). Также путь к этому файлу и к файлам логов будут указаны в выводе команды *livemedia-creator*. Название итогового образа можно задать при его создании с помощью опции **--iso-name**. Полученный загрузочный образ системы можно примонтировать в систему, чтобы убедиться, что файловая система была создана правильно. Далее образ можно записать на носитель и загрузиться с него в качестве Live-системы.

Пример kickstart-файла для создания загрузочного образа с конфигурацией минимального сервера:

```
# Generated by Anaconda 33.25.4
# Generated by pykickstart v3.30
#version=F33
%packages --multilib
@^server-minimal
dracut-live
```

```
syslinux
memtest86+
grub2-efi
redos-logos

%end

# Keyboard layouts
keyboard --xlayouts='us','ru' --switch='grp:alt_shift_toggle'
# System language
lang ru_RU.UTF-8

# Network information
network --bootproto=dhcp --device=ens18 --ipv6=auto --no-activate
network --hostname=localhost.localdomain

# Use CDROM installation media
cdrom

# Run the Setup Agent on first boot
#firstboot --enable
firstboot --disable
eula --agreed
shutdown

# Generated using Blivet version 3.3.0
ignoredisk --only-use=sda
part swap --asprimary --size=1024
part / --fstype ext4 --size=6000

# Partition clearing information
clearpart --none --initlabel

# System timezone
timezone Europe/Moscow --utc
timesource --ntp-disable

# Root password

rootpw --iscrypted $6$5pjWyUOcrx5BkA2/$x.ZzjsgX4NUcUjSgGG.8EWiLfAIxfNy.m8xRKRMLUraz1MGJ99xohK
FEs3S9PDoHSecJvuBbxLdbsvF3an52s.v

user --groups=wheel --name=user --password=$6$Jsrft0ayMeAAOTaN$1gm9H9qwqBKYuBM7U3AkvJLzR78tDHqZWc55P0zWgJFx
fSDKAEqBmSz5fdeqscN04sc6zw3tqlJiAEZBhxv1a/ --iscrypted --gecos="user"


%anaconda
pwpolicy root --minlen=6 --minquality=1 --notstrict --nochanges --notempty
pwpolicy user --minlen=6 --minquality=1 --notstrict --nochanges --emptyok
pwpolicy luks --minlen=6 --minquality=1 --notstrict --nochanges --notempty
%end
```

ISO Master – утилита для редактирования ISO-образов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: isomaster-1.3.15-1

ISO Master – программа для редактирования ISO-образов оптических дисков. **ISO Master** не создаёт ISO-образы с компакт-дисков и не записывает их на диски, а только позволяет создавать их из произвольных каталогов и файлов или извлекать и изменять содержимое уже существующих образов. При необходимости к образу можно присоединить скрытые файлы или каталоги. **ISO Master** поддерживает различные файловые системы (960, Joliet, Rock Ridge и др.).

Ключевые особенности **ISO Master**:

- извлечение, удаление, добавление файлов и каталогов;
- поддержка ISO-образов, а также большинства NRG-образов и некоторых однотрековых MDF-образов;
- возможность переименования файлов и каталогов;
- выбор типа имён файлов Rock Ridge и/или Joliet;
- возможность выбора имени диска и издателя;
- просмотр и редактирование файлов внешними редакторами;
- просмотр и изменение правовых атрибутов файлов и каталогов;
- возможность работы с загрузочной записью – извлечение, удаление, установка из файла;
- поддержка файловых систем ISO 9660, Joliet, Rock Ridge, El Torito.

ISO Master простой в использовании графический редактор образов. Он может открывать файлы ISO, NRG и некоторые файлы MDF, но сохранение возможно только в формате ISO.

Меню **ISO Master** переведено на русский язык, поэтому выполнять задачи с помощью утилиты смогут даже начинающие пользователи. Из минусов программы выделяют отсутствие интегрированного рекордера, готовые образы можно записать на оптический диск только посредством дополнительных инструментов.

Установка

Утилита **ISO Master** находится в репозитории РЕД ОС, для установки перейдите в сеанс пользователя **root**:

```
su -
```

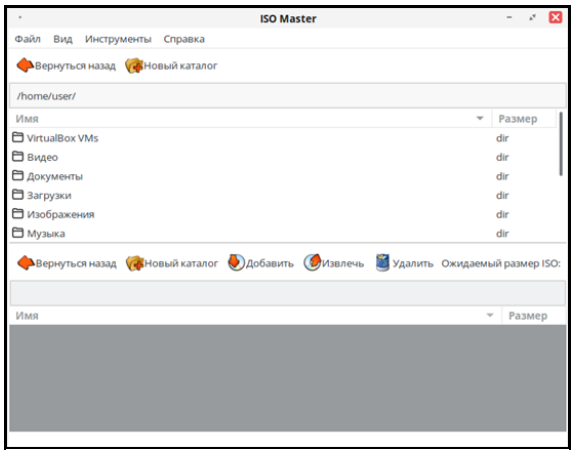
и выполните команду:

```
dnf install isomaster
```

После установки запуск программы доступен из «Главного меню» — «Аудио и видео» — «ISO Master» или через терминал (с правами локального пользователя) командой:

```
isomaster
```

Интерфейс утилиты **ISO Master** выглядит следующим образом:



Окно **ISO Master** разделено на две части:

- верхняя область окна отображает файлы и каталоги на используемой системе;
- нижняя область окна отображает файлы и каталоги в образе диска.

Для открытия существующего образа (ISO) нажмите «Файл» - «Открыть».

Для создания нового образа нажмите «Файл» - «Новый».

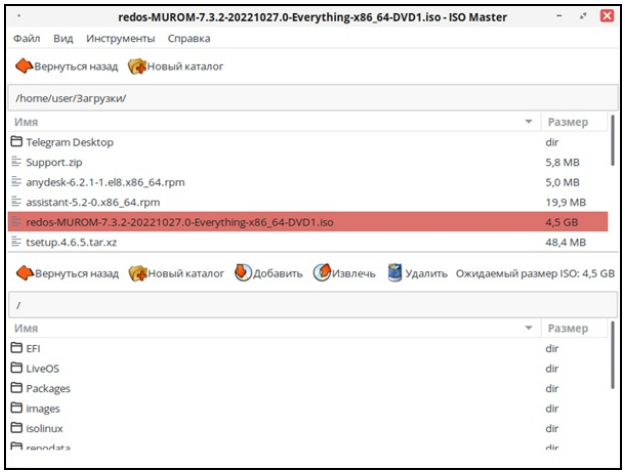
Для добавления одного или нескольких файлов или каталогов в образ выберите их в верхней области окна и нажмите «Добавить в образ» на панели инструментов в центре окна.

Для извлечения одного или нескольких файлов из образа выберите их в нижней области окна и нажмите «Извлечь из образа» на панели инструментов в центре окна.

Доступно удаление файлов и каталогов из образа, а также создание каталогов как в образе, так и на используемой системе. Дополнительные опции появляются при нажатии ПКМ по выбранному элементу в нижней части окна.

После внесения изменений в новый образ для сохранения результатов нажмите «Образ» - «Сохранить как». Обратите внимание, что исходный образ перезаписать нельзя.

При выборе какого-либо образа содержимое отображается в нижней части окна.



Отдельно стоит отметить, что **ISO Master** предоставляет пользователю возможность создавать или удалять загрузочную запись, а также создавать автозагрузочный файл, работающий без эмуляции. То есть создать загрузочный диск или флешку можно без каких-либо дополнительных инструментов.

genisoimage - утилита создания ISO-образов файловой системы

Установка
Синтаксис
Работа с утилитой
Создание ISO-образа отдельного каталога
Создание образа работающей системы
Создание копии локального репозитория

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: genisoimage-1.1.11-42

Genisoimage — это инструмент командной строки для создания образов файловой системы. Обычно используется для создания загрузочных компакт-дисков, дисков резервного копирования или для распространения больших объемов данных в одном файле. Полученный ISO-образ можно записать на носитель с помощью программного обеспечения для записи или смонтировать как виртуальный привод.

С помощью **genisoimage** можно создать:

- ISO-образ отдельного каталога;
- ISO-образ работающей системы;
- ISO-образ копии локального репозитория.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install genisoimage
```

Дальнейшая работа с утилитой производится с правами **администратора** или суперпользователя **root**.

Синтаксис

Синтаксис утилиты имеет вид:

```
genisoimage [<опции>] [-o <имя_образа>] <путь_к_источнику> [<путь_к_источнику_2> ...]
```

где:

- `<опции>` – необходимые опции;
- `<имя_образа>` – имя создаваемого образа, допускается указывать полный путь к создаваемому образу;
- `<путь_к_источнику>` – путь к источнику, из которого будет создан образ; может быть указано несколько источников с использованием опции `-graft-points`.

Пример использования опции `-graft-points`:

```
genisoimage -V test_iso -r -o test_iso.iso -graft-points /downloads=/home/user/Загрузки/ /docs=/home/user/Документы/
/images=/home/user/Изображения/
```

Необходимые источники указываются в формате `<цель>=<источник>` через пробел.

Работа с утилитой

Создание ISO-образа отдельного каталога

Рассмотрим пример создания копии раздела **/home**.

Для этого необходимо выполнить команду:

```
genisonimage -V home_iso -r -o /home.iso /home
```

где:

- `-V home_iso` – задать метку образа, которая будет видна при его монтировании;
- `-r` – сгенерировать записи SUSP и RR, необходимые для создания файловой системы **ISO9660**;
- `-o /home.iso` – имя созданного файла образа;
- `/home` – источник, из которого создается образ.

Создание образа работающей системы

Для создания образа работающей системы необходимо:

- создать временный каталог, в котором будет создаваться ISO-образ:

```
mkdir /tmp/iso
```

- примонтировать корневой раздел **/** в каталог **/mnt**.

В случае использования **LVM** выполнить команду:

```
mount /dev/ro_redos/root /mnt
```

- скопировать содержимое раздела **/** в каталог **/tmp/iso**:

```
cp -a /mnt/* /tmp/iso
```

- размонтировать **/mnt**:

```
umount /mnt
```

- после этого создать ISO-образ:

```
genisoimage -r -o /redos.iso /tmp/iso
```

где:

- `/redos.iso` – место расположения и название созданного образа;
- `/tmp/iso` – ранее созданный каталог; источник, из которого создается ISO-образ.

Примечание.

Процесс может занять некоторое время в зависимости от размера корневой файловой системы.

Создание копии локального репозитория

Утилита **genisonimage** позволяет создавать копии локального репозитория.

Для этого необходимо предварительно создать локальный репозиторий по нашей инструкции «Создание локального репозитория».

Далее для каждого репозитория необходимо создать отдельный образ:

```
genisonimage -V redos-7.3base -r -o /tmp/iso/redos-7.3base.iso /var/www/html/repo/red-os-7.3/base7.3
genisonimage -V redos-7.3update -r -o /tmp/iso/redos-7.3update.iso /var/www/html/repo/red-os-7.3/base7.3
genisonimage -V redos-7.3update -r -o /tmp/iso/redos-7.3kernels.iso /var/www/html/repo/red-os-7.3/kernels7.3
```

где:

- `-V redos-7.3base` – метка образа, которая видна при его монтировании;
- `-r` – сгенерировать записи SUSP и RR, необходимые для создания файловой системы ISO9660;
- `-o /tmp/iso/redos-7.3base.iso` – путь до создаваемого образа;
- `/var/www/html/repo/red-os-7.3/base7.3` – источник, из которого создается образ.

Примечание.

Процесс может занять некоторое время в зависимости от размера локального репозитория.

Dracut - ПО для создания загрузочного образа (initramfs)

Основные опции
Создание образа initramfs
Информация об образе

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dracut-056-9

Dracut — набор инструментов, обеспечивающих расширенные функции для автоматизации процесса загрузки Linux. Инструмент под названием *dracut* используется для создания загрузочного образа Linux (**initramfs**) путем копирования инструментов и файлов из установленной системы и объединения их со средой *dracut*, которая обычно находится в каталоге **/usr/lib/dracut/modules.d**.

В отличие от существующих загрузочных образов Linux, платформа *Dracut* пытается ввести как можно меньше жестко запрограммированной логики в **initramfs**. По сути, **initramfs** имеет одну цель: найти и смонтировать настоящую корневую файловую систему, чтобы процесс загрузки мог перейти к ней. Эта функция зависит от доступности устройства. Поэтому вместо жестко запрограммированных сценариев для определения доступности и пригодности устройства **initramfs** *dracut* зависит от диспетчера устройств Linux (**udev**) для создания символических ссылок на узлы устройств. Когда появляется узел устройства корневой файловой системы, *Dracut* монтирует его как новую корневую файловую систему, что помогает сократить время, необходимое для **initramfs**.

Основные опции

К основным опциям *dracut* относятся:

- `--kver <версия_ядра>` - позволяет создать образ с указанной версией ядра (по умолчанию образ сохраняется в каталог **/boot**);
- `-f, --force` - перезаписать существующий файл **initramfs**;
- `-a, --add <список_модулей_dracut>` - добавить список модулей *dracut* (через пробел) к набору модулей по умолчанию;
- `-o, --omit <список_модулей_dracut>` - отключить указанный список модулей *dracut* (через пробел);
- `-m, --modules <список_модулей_dracut>` - список модулей *dracut* (через пробел) для вызова при сборке **initramfs**. Этот параметр позволяет *dracut* включать только указанные модули;
- `--add-drivers <список_модулей_ядра>` - список модулей ядра (через пробел) для добавления в **initramfs**. Модули ядра должны быть указаны без суффикса «**.ko**»;
- `--filesystems <список_модулей_ФС>` - список модулей файловой системы ядра (через пробел) для включения в **initramfs** только общего назначения. Модули должны быть указаны без суффикса «**.ko**»;
- `-H, --hostonly` - создать образ только с теми параметрами, которые необходимы для загрузки конкретной машины.

Создание образа initramfs

Для создания образа **initramfs** используется команда:

```
dracut
```

Данная команда создаст образ **initramfs** общего назначения со всеми возможными функциями, полученными в результате комбинации установленных модулей *dracut* и системных инструментов. Образ **/boot/initramfs-<версия_ядра>.img** будет содержать модули используемого в данный момент системой ядра.

Если такой **initramfs**-образ уже существует, будет выведена ошибка с предложением использования опции **--force** для перезаписи уже существующего образа.

```
dracut

dracut: Will not override existing initramfs (/boot/initramfs-5.15.125-1.el7.3.x86_64.img) without --force
```

Также можно указать собственное имя для создаваемого образа, передав его команде в качестве аргумента:

```
dracut new-images-03-10-2023.img
```

Файлы образов по умолчанию хранятся в каталоге **/boot**. Однако обратите внимание, что при указании собственного имени образа (как приведено в примере выше) он будет сохранен в той директории, из которой выполнялась команда. Для сохранения образа в необходимом каталоге потребуется указать полный путь к создаваемому образу, например:

```
dracut /boot/new-images-03-10-2023.img
```

Для просмотра содержимого каталога **/boot** и списка имеющихся образов выполните следующую команду:

```
ll /boot
```

```
[root@localhost user]# ll /boot
итого 322044
-rw-r--r--. 1 root root    243138 авг 17 10:15 config-5.15.125-1.el7.3.x86_64
-rw-r--r--. 1 root root    242516 окт  6  2022 config-5.15.72-1.el7.3.x86_64
-rw-r--r--. 1 root root    243099 янв 16  2023 config-5.15.87-1.el7.3.x86_64
drwxr-xr-x. 3 root root      4096 июл  6 14:27 efi
drwxr-xr-x. 2 root root      4096 июл  6 14:31 grub
drwx------. 6 root root      4096 окт  4 14:16 grub2
-rw-------. 1 root root 109608962 сен 18 15:18 initramfs-0-rescue-d10c8030d88c4fb5b67dc7aab5e80a0b.img
-rw-------. 1 root root  33126818 сен 18 15:16 initramfs-5.15.125-1.el7.3.x86_64.img
-rw-------. 1 root root  35105011 июл  6 16:56 initramfs-5.15.72-1.el7.3.x86_64.img
-rw-------. 1 root root  32775360 сен 18 15:15 initramfs-5.15.87-1.el7.3.x86_64.img
drwxr-xr-x. 3 root root      4096 июл  6 14:41 loader
drwx------. 2 root root     16384 июл  6 14:23 lost+found
-rw-------. 1 root root  33667660 окт  4 15:27 new-images-03-10-2023.img
-rw-r--r--. 1 root root    280149 авг 17 10:18 symvers-5.15.125-1.el7.3.x86_64.gz
-rw-r--r--. 1 root root    279524 окт  6  2022 symvers-5.15.72-1.el7.3.x86_64.gz
-rw-r--r--. 1 root root    279819 янв 16  2023 symvers-5.15.87-1.el7.3.x86_64.gz
-rw-------. 1 root root   5949734 авг 17 10:15 System.map-5.15.125-1.el7.3.x86_64
-rw-------. 1 root root   5892910 окт  6  2022 System.map-5.15.72-1.el7.3.x86_64
-rw-------. 1 root root   5919259 янв 16  2023 System.map-5.15.87-1.el7.3.x86_64
-rwxr-xr-x. 1 root root  17647264 сен 18 15:16 vmlinuz-0-rescue-d10c8030d88c4fb5b67dc7aab5e80a0b
-rwxr-xr-x. 1 root root  17647264 авг 17 10:15 vmlinuz-5.15.125-1.el7.3.x86_64
-rwxr-xr-x. 1 root root  15288800 окт  6  2022 vmlinuz-5.15.72-1.el7.3.x86_64
-rwxr-xr-x. 1 root root  15502336 янв 16  2023 vmlinuz-5.15.87-1.el7.3.x86_64
```

Информация об образе

Для просмотра информации об используемом образе можно воспользоваться командой:

```
lsinitrd | less
```

В выводе отображается имя образа, его размер, версия *dracut* и список включенных в образ модулей *dracut*:

```
Image: /boot/initramfs-5.15.125-1.el7.3.x86_64.img: 33M
================================================================================
Version: dracut-056-9.el7

Arguments:  --force

dracut modules:
bash
systemd
systemd-initrd
systemd-sysusers
nss-softokn
dbus-broker
rngd
dbus
i18n
network-manager
network
ifcfg
drm
plymouth
dm
kernel-modules
kernel-modules-extra
kernel-network-modules
...
```

Некоторые модули в dracut по умолчанию отключены, но их можно добавить, используя файл конфигурации /etc/dracut.conf или команду вида:

```
dracut --add module <название_модуля>
```

Используя команду `dracut --list modules`, можно вывести список всех модулей *dracut*, доступных в системе:

```
dracut --list modules

bash
systemd
systemd-network-management
warpclock
fips
systemd-ac-power
systemd-ask-password
systemd-coredump
systemd-hostnamed
systemd-initrd
systemd-integritysetup
systemd-journald
systemd-ldconfig
systemd-modules-load
systemd-networkd
systemd-repart
systemd-resolved
systemd-rfkill
systemd-sysctl
...
```

Все модули *dracut* расположены в каталоге **/usr/lib/dracut/modules.d**. В этом каталоге все модули представлены в виде подкаталогов и содержат ряд скриптов. Каждый модуль обеспечивает определенную функциональность.

После секции модулей выведен список содержимого сжатого образа:

```
========================================================================
drwxr-xr-x  12 root     root          0 Sep  6 17:12 .
crw-r--r--   1 root     root      5,   1 Sep  6 17:12 dev/console
crw-r--r--   1 root     root      1,  11 Sep  6 17:12 dev/kmsg
crw-r--r--   1 root     root      1,   3 Sep  6 17:12 dev/null
crw-r--r--   1 root     root      1,   8 Sep  6 17:12 dev/random
crw-r--r--   1 root     root      1,   9 Sep  6 17:12 dev/urandom
lrwxrwxrwx   1 root     root          7 Sep  6 17:12 bin -> usr/bin
drwxr-xr-x   2 root     root          0 Sep  6 17:12 dev
drwxr-xr-x  15 root     root          0 Sep  6 17:12 etc
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/authselect
-rw-r--r--   1 root     root       2428 Jul 31 10:58 etc/authselect/nsswitch.conf
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/cmdline.d
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/conf.d
-rw-r--r--   1 root     root        124 Sep  6 17:12 etc/conf.d/systemd.conf
drwxr-xr-x   7 root     root          0 Sep  6 17:12 etc/dbus-1
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/dbus-1/interfaces
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/dbus-1/services
-rw-r--r--   1 root     root        838 Oct 10  2022 etc/dbus-1/session.conf
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/dbus-1/session.d
-rw-r--r--   1 root     root        833 Oct 10  2022 etc/dbus-1/system.conf
...
```

Функционал программы также предоставляет возможность ручного добавления драйверов, отключения ненужных модулей, добавление дополнительной информации для ускорения загрузки. Дополнительно реализована возможность поиска корневого раздела на сетевом диске.

Подробную информацию о работе с *dracut* можно получить, выполнив команду:

```
man dracut
```

О репозиториях

Репозито́рий РЕД ОС представляет собой хранилище (место), где хранятся и поддерживаются пакеты программ в формате **.rpm**.

Кроме официального репозитория существует множество сторонних, но их подключение настоятельно не рекомендовано. Это может приводить к коллизиям пакетов и проблеме несовместимости версий.

Поскольку репозитории Linux расположены в интернете, существует вероятность подмены репозитория злоумышленником на свой, содержащий модифицированные пакеты. Наш репозиторий имеет защиту от подмены. Защита реализована при помощи сверки цифровых подписей.

На клиенте подключенный репозиторий представляет из себя файл с расширением **.repo**, содержащий информацию о репозитории. Находится он по пути **/etc/yum.repos.d/**.

Для управления пакетами в РЕД ОС используется пакетный менеджер **DNF**, графический пакетный менеджер **dnfdragora** и утилиты для обслуживания **dnf-utils**.

Все действия по разворачиванию репозитория происходят на серверной части.

Создание локального репозитория

Предварительная настройка
Зеркало для репозитория РЕД ОС 7.3 стандартной редакции
Зеркало для репозитория РЕД ОС 7.3 сертифицированной редакции
Настройка на клиентском ПК
Настройка обновления репозитория

Вы можете подробнее ознакомиться с созданием локальных репозиториев, просмотрев наши обучающие видео:

- на **RuTube** — Создание локального репозитория РЕД ОС;
- в **Яндекс.Дзен** — Создание локального репозитория РЕД ОС;
- в **VK Видео** — Создание локального репозитория РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка сервера

Действия по созданию локального репозитория выполняются от имени пользователя **root**:

```
su -
```

2) Установите необходимые пакеты:

```
dnf install httpd createrepo yum-utils
```

3) Настройка web-службы **HTTPD**:

```
nano /etc/httpd/conf/httpd.conf
```

Установите строку с параметром *Options* внутри секции `<Directory "/var/www/html">` в следующее значение:

```
Options Indexes FollowSymLinks Includes
```

Сделать это можно командой:

```
sudo sed -i_lrepo_bak '/<Directory "\/var\/www\/html">/,/<\/Directory>/{/Includes/! s/^\([^#]*Options.*\).*$/\1 Includes/}'
/etc/httpd/conf/httpd.conf
```

Добавьте в автозагрузку и запустите ***httpd***.

```
systemctl enable httpd --now
```

В подразделе Настройка на клиентском ПК приводится информация о настройке клиентского ПК - с изменением адреса в файлах **.repo**.

Можно добавить запись **repo.red-soft.ru = <ip-адрес_сервера>** в ваш DNS-сервер. В этом случае менять конфигурацию на клиенте не потребуется.

ВАЖНО!

Для создания локальных репозиториев **Base, Updates, Kernels и Kernels6** необходимо предварительно убедиться, что у вас есть необходимый объем требуемого свободного дискового пространства.

Для получения информации о необходимом объеме для какого-либо определенного репозитория выполните команду:

```
dnf repoinfo <название_репозитория> | grep "Размер репозитория"
```

Чтобы узнать более точный размер **всех подключенных** репозиториев, можно воспользоваться командой:

```
dnf repoinfo | grep "Размер репозитория" | awk -F ':' '{size = $2; sub(/M$/, "", size); if (index($2, "M") > 0) total += size / 1024; else
```

```
total += size} END {printf "Общий вес \033[41mвсех подключенных\033[0m репозиториев: %.2f G\n", total}'
```

Зеркало для репозитория РЕД ОС 7.3 стандартной редакции

Создайте запись для репозитория в каталоге **/etc/yum.repos.d/**.

```
nano /etc/yum.repos.d/red.os.7.3.repo
```

с содержимым:

```
# RedOS-Standard.repo
 #
 [base7.3]
 name=RedOS Standard - Base 7.3
 baseurl=https://repo1.red-soft.ru/redos/7.3/$basearch/os,https://mirror.yandex.ru/redos/7.3/$basearch/os,http://repo.red-
soft.ru/redos/7.3/$basearch/os
 enabled=0
 gpgcheck=1
 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
```

Для размещения репозиториев можно использовать каталог, отличный от **/var/www/html/**, создав для него символическую ссылку и установив правильный контекст SELinux (для файловых систем с поддержкой *Extended File Attributes* - ext2, ext3, ext4, jfs, xfs, btrfs):

```
ln -s /mnt/repo/ /var/www/html/
semanage fcontext -a -t httpd_sys_content_t "/mnt/repo(/.*)?"
restorecon -Rv /mnt/repo/
```

Здесь в качестве примера используется каталог **/mnt/repo/**. Обратите внимание, что для пользователя или группы **apache** файлы и каталоги в директории репозитория должны быть доступны для чтения. Управление правами доступа подробно описано в статье «Настройка прав доступа к файлам и каталогам». Восстановление прав и контекста SELinux командой `restorecon` необходимо произвести после создания репозитория (`createrepo`).

Создайте каталог для репозиториев:

```
mkdir -p /var/www/html/repo/red-os-7.3
cd /var/www/html/repo/red-os-7.3
```

Запустите процедуру создания зеркала репозитория-источника. Начнется загрузка пакетов репозитория. Обратите внимание, что на машине должен быть **доступ к сети Интернет**.

```
reposync --repoid=base7.3 --downloadcomps --download-metadata
```

В окне терминала выполните следующую команду:

```
createrepo -v /var/www/html/repo/red-os-7.3/base7.3 -g comps.xml
```

Восстановите контекст SELinux каталога, в котором находится репозиторий. Например, при расположении репозитория в каталоге **/var/www/html/repo/** необходимо выполнить:

```
restorecon -Rv /var/www/html/repo/
```

Команда `restorecon` не следует по символическим ссылкам, поэтому необходимо указывать прямой путь до каталога с репозиторием.

Репозиторий для РЕД ОС 7.3 стандартной редакции готов.

ВАЖНО!

По аналогии создайте зеркало репозитория с обновлениями системы - **RedOS - Updates, RedOS - kernels и RedOS - kernels6**

Конфигурация репозитория **RedOS - Updates** находится в файле **/etc/yum.repos.d/RedOS-Updates.repo**, конфигурация **RedOS - kernels** в файле **/etc/yum.repos.d/RedOS-kernels.repo**.

Для репозитория **updates** и **kernels** команду `createrepo` запустите без параметра `-g comps.xml`.

Зеркало для репозитория РЕД ОС 7.3 сертифицированной редакции

Создайте конфигурационный файл для репозитория в каталоге **/etc/yum.repos.d/**.

```
nano /etc/yum.repos.d/redos7.3c.repo
```

с содержимым:

```
[base7.3c]
 name=RedOS Cert - Base 7.3
 baseurl=https://repo1.red-soft.ru/redos/7.3c/$basearch/os,https://mirror.yandex.ru/redos/7.3c/$basearch/os,http://repo.red-soft.ru/redos/7.3c/$basearch/os
 enabled=0
 gpgcheck=1
 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
```

Для размещения репозиториев можно использовать каталог, отличный от **/var/www/html/**, создав для него символическую ссылку и установив правильный контекст SELinux (для файловых систем с поддержкой *Extended File Attributes* - ext2, ext3, ext4, jfs, xfs, btrfs):

```
ln -s /mnt/repo/ /var/www/html/
semanage fcontext -a -t httpd_sys_content_t "/mnt/repo(/.*)?"
restorecon -Rv /mnt/repo/
```

Здесь в качестве примера используется каталог **/mnt/repo/**. Обратите внимание, что для пользователя или группы **apache** файлы и каталоги в директории репозитория должны быть доступны для чтения. Управление правами доступа подробно описано в статье «Настройка прав доступа к файлам и каталогам». Восстановление прав и контекста SELinux командой `restorecon` необходимо произвести после создания репозитория (`createrepo`).

Создайте каталог для репозиториев.

```
mkdir -p /var/www/html/repo/red-os-7.3c
cd /var/www/html/repo/red-os-7.3c
```

Загрузите в этот каталог пакеты из внешнего репозитория РЕД ОС 7.3 сертифицированной редакции, для этого выполните команды:

```
reposync --repoid=base7.3c --downloadcomps --download-metadata
```

Далее, в окне терминала, выполните команду:

```
createrepo -v /var/www/html/repo/red-os-7.3c/base7.3c -g comps.xml
```

Восстановите контекст SELinux каталога, в котором находится репозиторий. Например, при расположении репозитория в каталоге **/var/www/html/repo/** необходимо выполнить:

```
restorecon -Rv /var/www/html/repo/
```

Команда `restorecon` не следует по символическим ссылкам, поэтому необходимо указывать прямой путь до каталога с репозиторием.

Репозиторий для РЕД ОС 7.3 сертифицированной редакции готов.

ВАЖНО!

По аналогии создайте зеркало репозитория с обновлениями системы - **RedOS - Updates, RedOS - kernels и RedOS - kernels6**

Конфигурация репозитория **RedOS - Updates** находится в файле **/etc/yum.repos.d/RedOS-Updates.repo** и конфигурация **RedOS - kernels** в файле **/etc/yum.repos.d/RedOS-kernels.repo**.

Для репозитория **updates** и **kernels** команду `createrepo` запустите без параметра `-g comps.xml`.

Настройка на клиентском ПК

Если у вас используется DNS-сервер, то самый простой путь - это создать на нём соответствующую запись (указать для адресов репозиториев ip-адрес в локальной сети).

Для подключения локального репозитория на клиенте создайте запись для репозитория в каталоге **/etc/yum.repos.d/**, например:

```
nano /etc/yum.repos.d/redos7.3c.repo
```

с содержимым, в котором измените значение параметра **baseurl**, вписав путь к вашему репозиторию, например:

```
# RedOS-Cert.repo
 #
 [base7.3c]
 name=RedOS Cert - Base 7.3c
 baseurl=http://192.168.0.1/repo/redos7.3c/base7.3c
 gpgcheck=1
 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
```

В иных репозиториях, которые находятся по пути **/etc/yum.repos.d/**, измените значение параметра **enabled** на **enabled=0** (если такого значения в файлах нет, впишите его самостоятельно), чтобы не возникало конфликтов.

Например, файл **RedOS-Base.repo**, используемый по умолчанию, должен выглядеть так:

```
[base]
 name=RedOS - Base
 baseurl=https://repo1.red-soft.ru/redos/7.3/$basearch/os
 enabled=0
 gpgcheck=1
 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
```

ВАЖНО!

Настройка обращения к локальным репозиториям **Base** и **Updates** может быть осуществлена двумя способами:

- созданием собственных файлов репозиториев;
- редактированием файлов репозиториев, используемых по умолчанию.

При создании собственных файлов локальных репозиториев **не рекомендуется** удалять имеющиеся файлы репозиториев по умолчанию (**RedOS-Base.repo**, **RedOS-Updates.repo**) – их необходимо отключить, изменив значение параметра `enabled=1` на `enabled=0`! Иначе при обновлении системы данные файлы вновь появятся в каталоге **/etc/yum.repos.d/**.

В случае если были изменены и настроены файлы репозиториев по умолчанию (**RedOS-Base.repo**, **RedOS-Updates.repo**), после обновления системы в каталоге **/etc/yum.repos.d/** будут сохранены новые файлы расширением **.rpmnew** – они являются резервной копией стандартных конфигурационных файлов и не повлияют на текущую настройку локальных репозиториев, удалять их **не рекомендуется**.

Обновите информацию о репозиториях, для этого выполните следующие команды:

```
dnf makecache
dnf update
```

Настройка синхронизации локального репозитория

Для синхронизации локального репозитория воспользуйтесь нашей инструкцией Настройка синхронизации локального репозитория.

Создание локального репозитория с использованием HTTPS

Настройка сервера
Настройка клиента

Настройка сервера

Сначала потребуется установить пакеты, необходимые для работы веб-сервера. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install @web-server
```

Далее необходимо создать локальный репозиторий. Для этого воспользуйтесь нашей статьей «Создание локального репозитория».

Затем создайте самоподписанный сертификат:

```
openssl req -x509 -nodes -newkey rsa:2048 -keyout /var/lib/dnf/server.key -out /var/lib/dnf/server.cert
```

где:

- `-x509` — определяет необходимость создания самоподписанного сертификата, а не запроса на подпись;
- `-nodes` — пропустить опцию защиты сертификата с помощью пароля;
- `-newkey rsa:2048` — указывает необходимость генерации нового сертификата и нового ключа RSA длиной 2048 бит;
- `-keyout` — каталог хранения и имя закрытого ключа;
- `-out` — каталог хранения и имя создаваемого сертификата.

Потребуется указать некоторые данные для запроса сертификата - страну, область, город или другой населенный пункт, наименование организации, наименование подразделения организации и сервер. Важным параметром здесь является `Common Name (CN)`, где необходимо указать доменное имя сервера или его IP-адрес.

```
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/var/lib/dnf/server2.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:msk
Locality Name (eg, city) [Default City]:msk
Organization Name (eg, company) [Default Company Ltd]:rs
Organizational Unit Name (eg, section) []:rs
Common Name (eg, your name or your server's hostname) []:server-repo
Email Address []:admin@rs.ru
```

Далее в файле **/etc/httpd/conf.d/ssl.conf** необходимо указать путь к созданным файлам сертификата и ключа:

```
nano /etc/httpd/conf.d/ssl.conf
```

```
# Point SSLCertificateFile at a PEM encoded certificate. If
 # the certificate is encrypted, then you will be prompted for a
 # pass phrase. Note that restarting httpd will prompt again. Keep
 # in mind that if you have both an RSA and a DSA certificate you
 # can configure both in parallel (to also allow the use of DSA
 # ciphers, etc.)
```

```
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile /var/lib/dnf/server.cert

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile /var/lib/dnf/server.key
```

Если SELinux на сервере включен, необходимо изменить метку файлов сертификата и ключа, чтобы **httpd** мог получить к ним доступ:

```
semanage fcontext -a -s system_u -t cert_t /var/lib/dnf/server.cert
semanage fcontext -a -s system_u -t cert_t /var/lib/dnf/server.key
restorecon -vF /var/lib/dnf/server.key /var/lib/dnf/server.cert
```

После этого потребуется перезапустить службу **httpd** командой:

```
systemctl restart httpd
```

Настройка клиента

С сервера, на котором настроен локальный репозиторий, необходимо скопировать самоподписанный сертификат в хранилище доверенных корневых сертификатов клиента:

```
cp server.cert /etc/pki/ca-trust/source/anchors/
update-ca-trust extract
```

Далее в директории **/etc/yum.repos.d/*** следует создать файл репозитория со следующим содержимым, например:

```
[repo]
 baseurl=https://<server_hostname>/<repo-id>
 enabled=1
 #sslverify=false
```

По умолчанию параметр `sslverify=true`, однако в случае если сертификат не был добавлен в доверенные корневые сертификаты клиента, необходимо использовать значение `false` (раскомментировать строку `#sslverify=false`) для пропуска его проверки.

Настройка синхронизации локального репозитория

Вы можете подробнее ознакомиться с возможностью обновления репозиториев в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Обновления и изменения в принципах работы с репозиториями РЕД ОС;
- в **Яндекс.Дзен** — Обновления и изменения в принципах работы с репозиториями РЕД ОС;
- в **VK Видео** — Обновления и изменения в принципах работы с репозиториями РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

1) Перейдите в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

2) Обновите данные о пакетах в основном репозитории.

```
dnf clean all
dnf repolist
```

3) Синхронизируйте пакеты основного репозитория с локальным.

Пример синхронизации:

```
reposync -p /var/www/html/repo/red-os-7.3/base7.3/ --repo base7.3 --downloadcomps --download-metadata --norepopath
```

Если нужно синхронизировать только новые пакеты и удалить пакеты из локального репозитория, которых уже нет в основном, то воспользуйтесь командой:

```
reposync -p /var/www/html/repo/red-os-7.3/base7.3/ --repo base7.3 --downloadcomps --download-metadata --norepopath --newest-only --delete
```

4) Обновите метаданные репозитория.

```
createrepo --update /var/www/html/repo/red-os-7.3/base7.3/ -g comps.xml
```

Также для обновления репозитория можно воспользоваться скриптом по созданию локального репозитория.

Пример содержимого скрипта:

```
#!/bin/bash
 DESTDIR=/var/www/html/repo/red-os-7.3
 REPOIDS="base7.3 updates7.3 kernels7.3"
 dnf makecache
 for REPOID in $REPOIDS; do
   if [[ -f "$DESTDIR/$REPOID/.repodata" ]];
    then
      rm -rf $DESTDIR/$REPOID/.repodata
   fi
   reposync --repo $REPOID --newest-only --downloadcomps -p $DESTDIR
   if [[ -f "$DESTDIR/$REPOID/comps.xml" ]];
    then
      createrepo --update $DESTDIR/$REPOID -g comps.xml
    else
      createrepo --update $DESTDIR/$REPOID
   fi
 done
```

В переменной **DESTDIR** укажите свой путь до местонахождения вашего репозитория.

В строковой переменной **REPOIDS** указываются идентификаторы ваших репозиториев, а в цикле скрипта обрабатывается каждый из них.

Следующим шагом добавьте этот скрипт в планировщик задач **crontab**.

Модули ядра

Общая информация
Загрузка/выгрузка модулей ядра
Автозагрузка модулей
Черный список

Модули ядра – это фрагменты кода, которые могут быть загружены и выгружены в ядро по требованию. Они расширяют функциональность ядра без необходимости перезагрузки системы. Модуль может быть настроен, как встроенный в ядро или как загружаемый во время работы операционной системы.

Примеры модулей ядра – это *драйверы* различных устройств.

Общая информация

Все модули хранятся в папке **/lib/modules/**. Т.к. модули рассчитаны только на определенную версию ядра, для каждой установленной версии создается свой подкаталог.

Чтобы просмотреть список установленных версий ядра, выполните следующую команду:

```
ls /lib/modules/
```

Если у вас только одна версия ядра, терминал выведет примерно следующее:

```
5.10.29-1.el7.x86_64
```

Если версий ядра несколько, все они будут указаны.

Может возникнуть необходимость просмотреть все установленные модули для текущего ядра в системе, для этого следует выполнить команду:

```
find /lib/modules/$(uname -r) -name *.ko

/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/crc4.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/crc8.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/lz4/lz4_compress.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/lz4/lz4hc_compress.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/reed_solomon/reed_solomon.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/objagg.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/lru_cache.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/ts_bm.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/crc-itu-t.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/ts_fsm.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/math/cordic.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/crc7.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/crc64.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/ts_kmp.ko
/lib/modules/5.10.29-1.el7.x86_64/kernel/lib/parman.ko
```

Иногда возникает необходимость уточнить, установлен ли какой-либо конкретный модуль ядра, для этого можно отфильтровать вывод поиска с помощью **grep**. Рассмотрим команду на примере модуля **ip_tables**:

```
find /lib/modules -name *.ko | grep ip_tables

/lib/modules/5.10.29-1.el7.x86_64/kernel/net/ipv4/netfilter/ip_tables.ko
```

Для просмотра драйверов и модулей, загруженных в данный момент в системе, используется команда:

```
lsmod

Module      Size  Used by
nls_utf8     16384  1
isofs     53248  1
snd_hrtimer     16384  1
rfkill     28672  2
vsock_loopback     16384  0
```

```
vmw_vsock_virtio_transport_common 36864  1 vsock_loopback
vmw_vsock_vmci_transport   32768  2
vsock      49152  7 vmw_vsock_virtio_transport_common, vsock_loopback, vmw_vsock_vmci_transport
sunrpc      651264  1
snd_ens1371     36864  4
```

Вывод представляет собой таблицу, в которой три столбца:

- *Module* — название модуля;
- *Size* — размер модуля (в байтах);
- *Used by* — количество экземпляров модуля, используемое в настоящее время. Нулевое значение говорит о том, что модуль не используется. Разделенный запятыми список после количества показывает, какие зависимости есть у модуля.

Если список загруженных в данный момент модулей большой, а интересует узнать, загружен ли какой-либо конкретный модуль, следует отфильтровать вывод командой **grep**:

```
lsmod | grep ip_tables
```

Если модуль загружен, *lsmod* его выведет. В противном случае — ответа на команду не будет.

В нашем случае модуль загружен и команда его показывает следующим образом:

```
ip_tables   28672  0
```

Для отображения подробной информации о модуле используется команда:
modinfo <имя_модуля>.

Выполним ее на примере модуля *fuse*:

```
modinfo fuse

filename: /lib/modules/5.10.29-1.el7.x86_64/kernel/fs/fuse/fuse.ko
alias:  devname:fuse
alias:  char-major-10-229
alias:  fs-fuseblk
alias:  fs-fuse
license: GPL
description: Filesystem in Userspace
author:  Miklos Szeredi <miklos@szeredi.hu>
alias:   fs-fusectl
depends:
retpoline: Y
intree:  Y
name:  fuse
vermagic: 5.10.29-1.el7.x86_64 SMP mod_unload
sig_id:  PKCS#7
signer:  Red Soft Kernel Signing key
sig_key: 1B:2C:9A:D2:F1:D0:C7:8D:82:8F:62:82:B1:3E:F9:0D:7E:66:FF:01
sig_hashalgo: sha256
signature: 6E:62:46:91:B3:AE:74:0A:BA:67:28:61:A8:A4:FD:CC:A2:2E:DF:85:
  E5:C2:38:56:8C:EB:C3:82:24:4F:8A:EA:5B:12:E0:E1:E9:78:D5:00:
  FF:EA:53:C2:3A:4D:6B:35:43:CC:6A:41:F4:8B:E0:D5:57:23:F9:F2:
  D9:ED:10:4B:8A:83:0A:34:CF:4E:BF:B6:EC:CD:E5:7F:C1:30:BA:2D:
  B4:84:1A:F1:69:C7:BA:C3:39:0B:9C:56:BD:6C:1B:F8:CC:14:8A:32:
  42:C5:82:37:78:43:C2:6B:1C:E8:99:EE:85:27:48:79:C1:68:07:AE:
  3E:02:B8:64:8E:4F:06:C2:E3:5C:55:D2:96:1B:0E:56:49:A6:97:C2:
  D6:5C:0A:DA:75:A4:48:C0:F3:1F:D0:A2:4F:92:5A:F7:9F:AB:B4:9D:
  19:C4:5F:2C:E4:CB:33:20:41:4D:3A:64:02:2B:47:A1:C1:5E:89:35:
  76:54:CD:06:D7:77:C5:44:C5:BB:FA:F4:77:62:C7:D8:7B:93:E9:F4:
  CB:20:81:B5:33:52:7D:8B:B7:49:C4:54:56:34:89:B2:79:5C:29:8D:
  BF:1B:64:19:8E:0E:4D:51:9D:B3:CC:38:5F:3C:4D:CB:EC:27:D5:B5:
  EE:9C:59:AA:56:D4:AA:A7:25:5C:0D:64:BA:8E:C7:15:CE:7F:FB:D2:
  9D:FB:F0:DA:E1:09:AD:8F:50:12:A3:6A:F9:B0:C9:52:FE:7E:67:B6:
  FD:F3:3A:76:5C:14:63:D5:B5:4C:99:06:A4:32:B8:03:3F:6B:DC:DC:
  07:12:90:08:2F:9A:11:ED:B8:DD:63:A3:AC:15:B7:20:7B:8E:C3:30:
  60:B7:73:E7:6D:AF:5C:3B:AE:56:43:6F:F1:80:A4:29:3F:C8:01:EE:
  C2:8E:78:30:2E:5E:22:38:7D:37:AE:61:C6:F7:35:3B:D5:A7:1E:C8:
  7B:07:E9:27:B5:13:AC:7C:E7:86:40:98:9B:D1:23:52:35:3E:FA:A6:
  10:EE:0B:9E:23:17:D4:1D:0A:C9:0C:7B:D2:7F:F9:BB:54:83:B8:17:
  9B:BD:D5:CC:E8:65:0F:C7:14:33:42:78:27:78:AF:7E:9D:5D:A4:D1:
  4C:87:E8:0A:DE:CD:45:DE:18:09:CD:77:AD:55:10:4F:3C:8C:25:09:
```

```
  11:5F:29:EF:69:26:57:0B:23:90:FC:4A:8C:38:EF:FA:26:47:94:22:
  21:C8:12:A3:B2:76:F5:91:9C:FF:7B:8D:C6:03:40:A8:5E:6F:A5:0B:
  07:4F:84:48:0D:1F:66:6E:37:59:0C:4D:11:9D:C5:F0:2C:26:78:62:
  29:97:C6:D5:D0:2A:D5:BB:8F:14:10:67
parm:  max_user_bgreq:Global limit for the maximum number of backgrounded requests an unprivileged user can set (uint)
parm: max_user_congthresh:Global limit for the maximum congestion threshold an unprivileged user can set (uint)
```

Есть возможность просмотреть список опций, установленных для загруженного модуля. Просмотр осуществляется командой **systool**:

```
systool [<опция> [имя_модуля]]

  -a   Show attributes
  -b <bus_name> Show a specific bus
  -c <class_name> Show a specific class
  -d   Show only devices
  -h   Show usage
  -m <module_name> Show a specific module
  -p   Show path to device/driver
  -v   Show all attributes with values
  -A <attribute_name> Show attribute value
  -D   Show only drivers
  -P   Show device's parent
```

Команда **systool** без переданных параметров выводит список всех модулей, разделенный на секции: *bus, class, devices, modules*. Это сделано для того, чтобы можно было корректно передавать команде опции и получать правильный вывод.

Чтобы отобразить конфигурацию определенного модуля, например **ip_tables**, выполним команду:

```
modprobe –c | grep ip_tables

alias ipt_icmp ip_tables
alias symbol:ipt_alloc_initial_table ip_tables
alias symbol:ipt_do_table ip_tables
alias symbol:ipt_register_table ip_tables
alias symbol:ipt_unregister_table ip_tables
alias symbol:ipt_unregister_table_exit ip_tables
alias symbol:ipt_unregister_table_pre_exit ip_tables
```

Получить список зависимостей модуля (или псевдонима), включая сам модуль, с созданием (возможно пустого) набора имён файлов модулей, по одному в строке, каждое из которых начинается с «*insmod*», можно с помощью команды:

```
modprobe –-show-depends fuse

insmod /lib/modules/5.10.29-1.el7.x86_64/kernel/fs/fuse/fuse.ko
```

Загрузка/выгрузка модулей ядра

Загрузка модулей ядра осуществляется командами **modprobe** и **insmod**. Принцип их действия один и тот же, но отличаются передаваемые параметры. Команде **modprobe** передается только название модуля **modprobe <имя_модуля>**.

Например:

```
modprobe fuse
```

Для команды **insmod** необходимо передать адрес файла модуля (его можно узнать командой *modinfo*):

```
modinfo fuse | grep filename

filename: /lib/modules/5.10.29-1.el7.x86_64/kernel/fs/fuse/fuse.ko
 insmod /lib/modules/5.10.29-1.el7.x86_64/kernel/fs/fuse/fuse.ko
```

Для выгрузки (выключения) модуля из ядра также можно использовать одну из двух команд - **modprobe** или **rmmode**. Команде **modprobe** обязательно требуется передать опцию **–r**:

```
modprobe –r fuse
```

Альтернативная команда выглядит несколько проще:

```
rmmode fuse
```

Если после выполнения команды выгрузки возникает ошибка типа:

```
modprobe: FATAL: Module fuse is in use.
```

это значит, что в данный момент модуль выгружен быть не может, т.к. он используется. Бывает, что в ошибке явно указывается, какими модулями используется необходимый к выгрузке, и тогда сперва требуется выгрузить их.

Автозагрузка модулей

Для того чтобы каждый раз не производить ручную загрузку тех или иных модулей, работать с которыми требуется регулярно, в РЕД ОС существует отдельный каталог, в котором можно настроить автоматическую загрузку модулей при старте системы - **/etc/modules-load.d/**. В каталоге хранятся конфигурационные файлы ***.conf**, содержащие наименования необходимых модулей.

Кроме указанной выше директории также считываются файлы конфигурации из **/run/modules-load.d/*.conf** и **/usr/lib/modules-load.d/*.conf**. Если директории пустые, то можно создать файл и поместить нужные модули для автозагрузки. Каждый файл конфигурации имеет имя вида:
***/modules-load.d/<program>.conf**

Файлы конфигурации содержат список имён модулей ядра для загрузки, разделённых символами новой строки. Пустые строки и строки, чей первый не пробельный символ - **#** (решётка) или **;** (точка с запятой) игнорируются.

Например, можно создать файл **autorun.conf** в каталоге **/etc/modules-load.d/**:

```
nano /etc/modules-load.d/autorun.conf
```

В данный файл построчно добавляются все необходимые модули, например:

```
video
e1000
serio_raw
```

При следующей загрузке системы указанные в файле модули будут автоматически загружены.

Черный список

Чёрный список в контексте модулей ядра – это механизм, предотвращающий загрузку того или иного модуля. Это может быть полезно, если связанное оборудование не требуется или загрузка этого модуля вызывает проблемы. Например, могут быть два модуля ядра, которые пытаются управлять одним и тем же компонентом оборудования, и загрузка их вместе приведёт к конфликту.

Для запрета загрузки определенного модуля ядра создайте конфигурационный файл **block_modules.conf** в каталоге **/etc/modprobe.d/** и добавьте в нем строку для каждого модуля, который вы хотите добавить в чёрный список, используя ключевое слово «**blacklist**».

Например, если вы хотите запретить загрузку модуля **pcspkr**, создайте файл **/etc/modprobe.d/block_modules.conf** и добавьте в него строку:

```
blacklist pcspkr /bin/true
```

* где */bin/true* устанавливает запрет на загрузку модулей, зависящих от занесенного в черный список.

Некоторые модули загружаются как часть **initramfs**. То есть можно выделить модули, которые загружаются:

- из файлов **.ko**;
- как часть initramfs (initial ramdisk).

Для запрета загрузки модулей первого типа (загружаемых из файлов **.ko**) достаточно внести запись об этом модуле в файл **/etc/modprobe.d/*.conf** с директивой **blacklist**.

Для запрета загрузки модулей второго типа, кроме создания конфигурационного файла, необходимо также пересоздать **initramfs**. Пересоздание *initramfs* осуществляется следующей командой:

```
dracut --force /boot/initramfs-5.10.29-1.el7.x86_64.img 5.10.29-1.el7.x86_64 -v
```

* где **5.10.29-1.el7.x86_64** - это текущая версия ядра.

Настройка zswap

Включение и выключение Zswap
Изменение параметров

Zswap – это функция ядра, предоставляющая сжатый кэш в оперативной памяти для страниц подкачки. Страницы, которые ранее выгружались на жесткий диск, вместо этого сжимаются и сохраняются в пуле ОЗУ. Как только этот пул памяти заполнен или доступная оперативная память исчерпана, давно не использовавшиеся страницы разжимаются и выгружаются в подкачку, а сжатая её версия удаляется из пула. После того как страница была перемещена в режим подкачки, сжатая версия в пуле памяти может быть освобождена и использована снова.

Для дальнейшей настройки **zswap** перейдите в сеанс пользователя **root**:

```
su -
```

Далее все команды выполняются с правами пользователя **root**, если не указано иное.

Сначала необходимо определить, включен ли **Zswap** и какие у него настройки, выполнив команду в терминале:

```
grep -R . /sys/module/zswap/parameters

/sys/module/zswap/parameters/same_filled_pages_enabled:Y     # (функция идентификации страниц с одинаковыми значениями)
/sys/module/zswap/parameters/enabled:N      # (zswap выключен)
/sys/module/zswap/parameters/max_pool_percent:20     # (максимальный размер пула в оперативной памяти)
/sys/module/zswap/parameters/compressor:lzo     # (алгоритм сжатия данных)
/sys/module/zswap/parameters/zpool:zbud     # (zpool алгоритм управления памятью)
/sys/module/zswap/parameters/accept_threshold_percent:90     # (пороговое значение, при котором zswap снова начнет принимать страницы после того, как заполнится)
```

Дополнительную проверку наличия Zswap в ядре можно осуществить командой:

```
cat /boot/config-`uname -r` | grep -i zswap

CONFIG_ZSWAP=y     # (буква «y» означает, что поддержка есть)
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_DEFLATE is not set
CONFIG_ZSWAP_COMPRESSOR_DEFAULT_LZO=y
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_842 is not set
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_LZ4 is not set
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_LZ4HC is not set
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_ZSTD is not set
CONFIG_ZSWAP_COMPRESSOR_DEFAULT="lzo"
CONFIG_ZSWAP_ZPOOL_DEFAULT_ZBUD=y
# CONFIG_ZSWAP_ZPOOL_DEFAULT_Z3FOLD is not set
# CONFIG_ZSWAP_ZPOOL_DEFAULT_ZSMALLOC is not set
CONFIG_ZSWAP_ZPOOL_DEFAULT="zbud"
# CONFIG_ZSWAP_DEFAULT_ON is not set
```

Просмотреть сообщение, отображающееся при загрузке системы, можно командой:

```
dmesg | grep zswap

[ 0.781818] zswap: loaded using pool lzo/zbud
```

Включение и выключение Zswap

Для разового включения модуля **Zswap** выполните команду:

```
echo 1 > /sys/module/zswap/parameters/enabled
```

Чтобы отключить **Zswap** в работающей системе, необходимо сделать замену параметра с «**1**» на «**0**»:

```
echo 0 > /sys/module/zswap/parameters/enabled
```

Обратите внимание, что после перезагрузки операционной системы, значения параметров будут возвращены к величине по умолчанию.

Проверка состояния производится командой:

```
cat /sys/module/zswap/parameters/enabled
```

Буква «**Y**» в выводе команды означает, что **Zswap** активирован.

Команды для включения и отключения модуля **Zswap** при старте операционной системы:

- команда для включения:

```
grubby --update-kernel ALL --args zswap.enabled=1
```

- команда для отключения:

```
grubby --update-kernel ALL --args zswap.enabled=0
```

Изменение параметров

Изменить размер пула (по умолчанию размер пула составляет 20% от всей оперативной памяти) можно, выполнив команду:

```
echo 15 > /sys/module/zswap/parameters/max_pool_percent
```

На системах с небольшим количеством оперативной памяти обычно устанавливается размер пула 5 - 15%, если оперативной памяти больше 2 Гб — 20 - 25%.

Убедитесь, что размер пула изменился:

```
cat /sys/module/zswap/parameters/max_pool_percent
```

Для изменения алгоритма управления памятью необходимо выполнить команду:

```
echo zsmalloc > /sys/module/zswap/parameters/zpool
```

По умолчанию **Zswap** использует алгоритм сжатия **lzo**, также может использовать любой алгоритм, поддерживаемый **api** ядра (например, lz4, zstd, deflate, lz4hc, lzo-rle), но для этого должен быть установлен модуль сжатия.

Проверьте наличие модуля **lz4** в системе командой:

```
modprobe lz4
```

Если команда ничего не выводит, значит модуль загружен, если выводится сообщение об ошибке — модуль отсутствует в ядре.

Чтобы изменить алгоритм сжатия на **lz4**, используйте команду:

```
echo lz4 > /sys/module/zswap/parameters/compressor
```

После перезагрузки операционной системы значения параметров, в которые были внесены изменения, будут возвращены к величине по умолчанию.

Сохранить внесенные изменения после перезагрузки можно следующим способом, для этого выполните команду:

```
grubby --update-kernel ALL --args "zswap.enabled=1 zswap.compressor=lz4 zswap.max_pool_percent=10 zswap.zpool=zsmalloc"
```

Выполните перезагрузку операционной системы:

```
reboot
```

Если необходимо получить статистику использования **Zswap**, используйте команду:

```
sudo grep -r . /sys/kernel/debug/zswap
```

Поддержка оборудования в ядре ОС

Поддержка железа
Поддержка звука
Поддержка сети

Некоторые модели поддерживаемого оборудования указаны в разделе «Оборудование, совместимое с РЕД ОС».

Вопрос поддержки оборудования ядром и драйверами актуален всегда. Для того чтобы понять, как именно осуществляется проверка поддержки, рассмотрим основные инструменты и ссылки.

Для получения краткой сводки о комплектующих вашего ПК выполните команду:

```
loginfo.sh --hw-id
```

Предварительно **loginfo** должен быть обновлен до актуальной версии:

```
dnf update loginfo
```

Поддержка железа

Одним из популярных сайтов, в котором собраны ID устройств, является https://linux-hardware.org.

Однако, чтобы определить, какие **Vendor ID** (**VID**) и **Device ID** (**DID**) требуется вводить для понимания поддержки, воспользуйтесь утилитой **inxi**.

```
inxi -F -v 8
```

пример ID для **USB Bluetooth** / **USB Wi-Fi,** которые потребуются для эксперимента:

```
...

Device-2: 1-4:2 info: Realtek Bluetooth Radio type: Bluetooth driver: rtk_btusb interfaces: 2 rev: 1.1
speed: 12 Mb/s chip ID: 0bda:8771 serial: 00E04C239987
Device-3: 1-6:3 info: Realtek RTL8188EUS 802.11n Wireless Network Adapter type: Network driver: 8188eu
interfaces: 1 rev: 2.0 speed: 480 Mb/s chip ID: 0bda:8179 serial: 00E04C0001

...
```

В выводе отображаются 2 интересующих нас ID:

- Bluetooth - **0bda:8771**;
- Wi-Fi - **0bda:8179**.

Также рассмотрим альтернативу *linux-hardware.org* — **https://cateee.net**

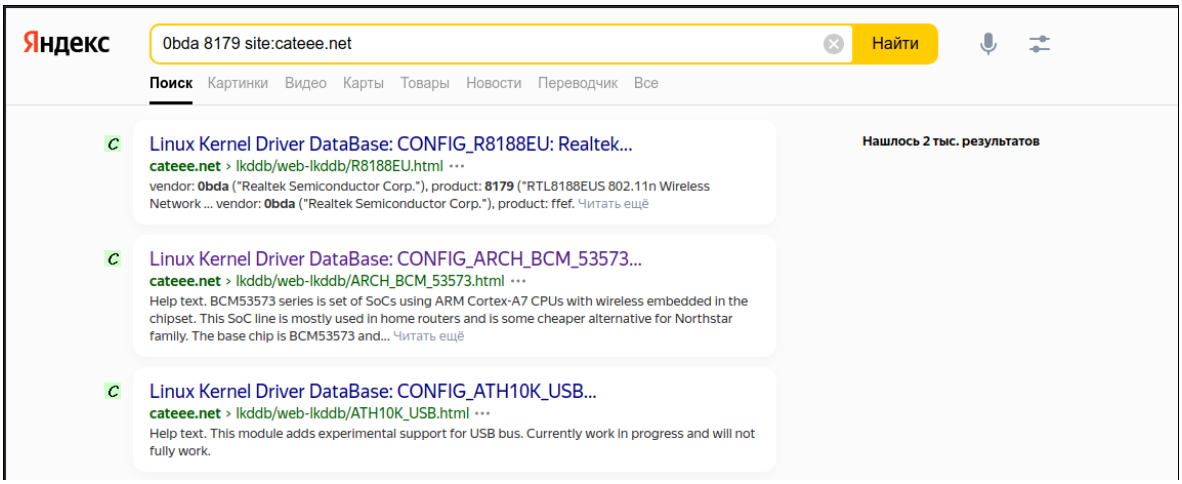
Данный сайт осуществляет поиск аналогично по ID. Для этого в поисковой строке требуется задать запрос вида:

<VID> <DID> site:cateee.net

или по одному из нужных ID.

Попробуем найти **0bda 8179** (**Wi-Fi**).

Имеется ряд результатов, в которых описывается, какой именно драйвер требует устройство:



Стоит упомянуть еще пару полезных ссылок для определения поддержки железа ядром:

- https://wireless.wiki.kernel.org/en/users/drivers
- https://h-node.org/hardware/catalogue/en

Также обращаем внимание на пункт **Driver** в выводе **inxi** - если он имеет значение отличное от **n/a**, значит у вас имеется поддержка устройства драйвером. Что это означает? Это значит, что вы можете найти данное устройство в заявленных драйвером через **modinfo**.

Bluetooth:

```
modinfo rtk_btusb | grep -i 0BDA

alias: usb:v0BDAp*d*dc*dsc*dp*icE0isc01ip01in*
```

В выводе показано, что есть метка **alias (алиас)**, являющаяся маской, по которой драйвер применяется к тому или иному устройству.

Аналогичную картину можно наблюдать для **Wi-Fi** адаптера:

```
modinfo 8188eu | grep -i 0BDA

alias: usb:v0BDAp8179d*dc*dsc*dp*ic*isc*ip*in*
```

Теперь рассмотрим проверку ядра на наличие интересующего драйвера.

Сначала проверим, установлен ли уже драйвер:

```
find /lib/modules/$(uname -r) -name *.ko | grep -i 8188eu

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/net/wireless/8188eu.ko
/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/staging/r8188eu/r8188eu.ko

find /lib/modules/$(uname -r) -name *.ko | grep -i rtk_btusb

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/bluetooth/rtk_btusb.ko
```

Как видно из вывода консоли, для ядра **5.15.10-3** данные драйвера имеются.

Существует также способ просмотра параметров ядра, с которыми оно было собрано. Для проверки того, какие были выбраны опции для драйвера, выполните команду:

```
cat /boot/config-$(uname -r) | grep -i 8188

CONFIG_RTL8188EE=m
CONFIG_R8188EU=m
```

А вот для bluetooth-драйвера вывод может выглядеть сомнительно:

```
cat /boot/config-$(uname -r) | grep -i BTUSB
```

```
CONFIG_BT_HCIBTUSB=m
CONFIG_BT_HCIBTUSB_AUTOSUSPEND=y
CONFIG_BT_HCIBTUSB_BCM=y
# CONFIG_BT_HCIBTUSB_MTK is not se t
CONFIG_BT_HCIBTUSB_RTL=y
```

Для того чтобы развеять сомнения, имеется ли драйвер - проверим его наличие следующим образом:

```
dnf provides *rtk_btusb.ko
```

Из полученного списка необходимо выбрать драйвер под свое ядро:

```
rtl8761b_5.15.10-3.el7.x86_64-1.0-8.el7.3.x86_64 : Kernel module for RTL8761B
Репозиторий        : kernels
Совпадения с:
Другое       : *rtk_btusb.ko
```

В случае, если драйвер отсутствует и в ядре, и в репозитории, существует вариант поиска необходимого драйвера на **github**.

Для этого необходимо в поиске по репозиториям **github** знать название нужного драйвера и попробовать найти интересующий. Так, к примеру, драйвер **8188eu** имеет множество разветвлений, которые охватывают широкий спектр устройств - примеры двух популярных вариаций драйвера:

- https://github.com/drygdryg/rtl8188eus;
- https://github.com/lwfinger/rtl8188eu.

Поддержка звука

Для проверки поддержки звука необходимо выполнить команду:

```
inxi -a -A

Audio:
 Device-1: NVIDIA vendor: ASUSTeK driver: snd_hda_intel v: kernel
 bus ID: 01:00.1 chip ID: 10de:10fa
 Device-2: AMD Family 17h HD Audio vendor: ASUSTeK driver: snd_hda_intel
 v: kernel bus ID: 05:00.6 chip ID: 1022:15e3
 Sound Server: ALSA v: k5.15.35-1.el7.3.x86_64

modinfo snd_hda_intel | grep -i 10de

alias:          pci:v0000 10DEd*sv*sd*bc04sc03i00*
```

Также можно попробовать поиск через легкое регулярное выражение, когда «**:**» заменяется на «**.***», что означает любые символы.

```
modinfo snd_hda_intel | grep -i 1022.*15e3

alias:          pci:v0000 1022d000015E3sv*sd*bc*sc*i*
```

Поддержка сети

Для проверки поддержки сети выполните команду:

```
inxi -a -N

Network:
 Device-1: Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet
 vendor: ASUSTeK driver: r8169 v: kernel port: e000 bus ID: 02:00.0
 chip ID: 10ec:8168
 Device-2: Realtek RTL8821CE 802.11ac PCIe Wireless Network Adapter
 vendor: AzureWave driver: rtw_8821ce v: N/A modules: rtw88_8821ce
 port: d000 bus ID: 04:00.0 chip ID: 10ec:c821

modinfo r8169 | grep -iE 10ec.*8168
```

```
alias:          pci:v000010ECd00008168sv*sd*bc*sc*i*
```

Бывают случаи, когда поле **driver** не определено (driver = N/A), но присутствует поле **module**, тогда стоит производить проверку по данному полю:

```
modinfo rtw88_8821ce | grep -iE 10ec.*c821

alias:          pci:v000010ECd0000C821sv*sd*bc*sc*i*
```

kernel-manager - утилита управления ядрами

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kernel-manager-0.1-6

В репозитории РЕД ОС доступна специальная утилита для управления ядрами операционной системы - **kernel-manager**.

Утилита содержит список всех доступных в репозитории версий ядра.

Вы можете подробнее ознакомиться с работой утилиты управления ядрами **kernel-manager**, просмотрев наши обучающие видео:

- на **RuTube** — kernel manager - утилита управления ядрами;
- в **Яндекс.Дзен** — kernel manager - утилита управления ядрами;
- в **VK Видео** — kernel manager - утилита управления ядрами.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

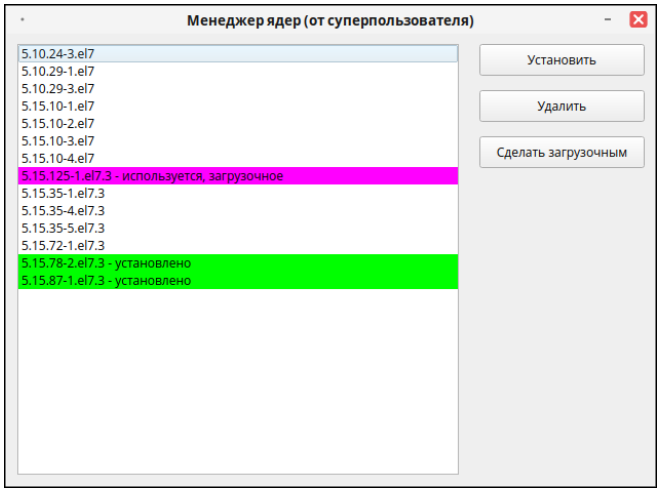
```
dnf install kernel-manager
```

После установки запуск утилиты доступен из «**Главного меню**» - «**Стандартные**» - «**Менеджер ядер**» или через терминал командой:

```
kernel-manager
```

Для работы с утилитой необходимы права суперпользователя **root**.

Окно утилиты выглядит следующим образом:

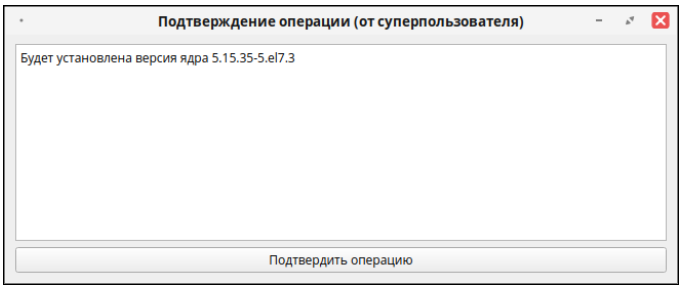


В списке слева отображаются все доступные в репозитории версии ядра. Розовым цветом подсвечивается используемое в данный момент операционной системой ядро. Зеленым цветом подсвечиваются установленные в системе версии ядра. Версии ядра без подсветки — не установлены в системе.

Справа доступны три кнопки действий:

- **Установить** — можно установить любую еще не установленную версию ядра из списка;
- **Удалить** — можно удалить любую установленную версию ядра, кроме используемой в данный момент;
- **Сделать загрузочным** — любую установленную версию ядра можно сделать загрузочной. При следующей загрузке системы использоваться будет именно она.

Для исключения случайного выполнения какого-либо действия выводится специальная форма с описанием операции, где необходимо нажать кнопку «**Подтвердить операцию**» в случае согласия или закрыть окно, в случае если действие выполнять не требуется.


Подтверждение операции (от суперпользователя)
Будет установлена версия ядра 5.15.35-5.el7.3
Подтвердить операцию

kdump — инструмент для анализа причин сбоев ядра

Минимальные требования
Настройка Selinux
Запуск служб и проверка работы

Kdump — это стандартный механизм для создания дампа содержимого памяти компьютера при сбое ядра.

Минимальные требования

Минимальные требования к окружению:

- версия ядра системы – **kernel-lt-5.15.131** и выше;
- набор инструментов dracut – **dracut-056-9** и выше;
- механизм kexec – **kexec-tools-2.0.27** и выше.

Если в системе используются пакеты более ранних версий, обновите их:

```
dnf update
```

Если в системе пакеты не установлены, выполните команду:

```
dnf install dracut kexec-tools
```

Перезагрузите систему:

```
reboot
```

Затем задайте размер для дампа ядра (в примере выделено **256 Мб** памяти). Для этого в файле **/etc/default/grub** добавьте в конец строки `GRUB_CMDLINE_LINUX=` параметр `crashkernel=256M` как показано в примере:

```
GRUB_CMDLINE_LINUX="rhgb quiet crashkernel=256M"
```

Настройка Selinux

Переведите **SELinux** в режим **permissive**. Для этого откройте файл **/etc/selinux/config**:

```
nano /etc/selinux/config
```

и замените строку `SELINUX=enforcing` на `SELINUX=permissive`.

Перезагрузите систему:

```
reboot
```

Запуск служб и проверка работы

В **dmesg** проверьте, что выделенная под дампы ядра память была зарезервирована:

```
dmesg | grep crashkernel

[    0.002111] Reserving 256MB of memory at 3312MB for crashkernel (System RAM: 4095MB)

kdumpctl status

Kdump: Kdump is not operational
```

Для оценки выделенной памяти используйте команду:

```
kdumpctl estimate
```

Далее запустите службу **kdump**и добавьте ее в автозагрузку:

```
kdumpctl start
systemctl enable kdump.service --now
```

Проверьте статус службы:

```
kdumpctl status
systemctl status kdump.service
```

В выводе должно быть **active (running)**.

Для проверки работы можно выполнить команду вызова паники ядра:

```
echo c > /proc/sysrq-trigger
```

Если настройка выполнена верно, в каталоге **/var/crash/<timestamp>** будут располагаться файлы дампов **kexec-dmesg.log**, **vmcore** и **vmcore-dmesg.txt**.

grubby - утилита настройки загрузчика ОС

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** grubby-8.40-40

GRUB является эталонной реализацией загрузчика, соответствующего спецификации Multiboot, и может загрузить любую совместимую с ней операционную систему. Кроме того GRUB может по цепочке передавать управление другому загрузчику, что позволяет ему загружать, например, ОС Windows, установленную рядом с РЕД ОС.

После настройки GRUB при включении компьютера пользователь видит список операционных систем, которые установлены на его компьютер и которые можно загрузить, выбрав подходящую и нажав «**Enter**».

GRUB позволяет при загрузке задавать произвольные параметры и передавать их в ядро Multiboot-совместимой ОС для дальнейшей обработки. GRUB — самый популярный загрузчик для Linux и является загрузчиком по умолчанию в большинстве известных дистрибутивов.

Здесь и далее под названием загрузчика GRUB подразумевается GRUB 2, который используется в Linux-системах, до него использовался GRUB первой версии, в настоящее время известный как GRUB Legacy. GRUB 2 полностью переписан с нуля и не имеет ничего общего с GRUB Legacy, разработка которого была остановлена в пользу более совершенного и мощного GRUB 2.

grubby является утилитой командной строки для настройки, отображения и обновления конфигураций загрузчика GRUB. По умолчанию **grubby** предустановлен в РЕД ОС.

Если в вашей системе утилита не установлена, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install grubby
```

Работа с утилитой **grubby** предоставляет множество преимуществ, включая простоту и согласованность во многих дистрибутивах. Для использования **grubby** не требуется обладать глубокими знаниями о файлах конфигурации утилиты.

Для генерации файла конфигурации GRUB 2 используется команда:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

После внесения изменений в файл конфигурации необходимо перезагрузить систему, чтобы изменения вступили в силу.

Для получения информации о работающем ядре системы выполните команду:

```
grubby --default-kernel

/boot/vmlinuz-5.15.35-5.el7.3.x86_64
```

Более подробную информацию о текущем ядре можно получить, выполнив команду:

```
grubby --info /boot/vmlinuz-$(uname -r)

index=1
kernel=/boot/vmlinuz-5.15.10-1.el7.x86_64
args="ro resume=/dev/mapper/ro_redos-swap rd.lvm.lv=ro_redos/root rd.lvm.lv=ro_redos/swap rhgb quiet rd.driver.blacklist=nouveau
modprobe.blacklist=nouveau nvidia-drm.modeset=1"
root=/dev/mapper/ro_redos-root
initrd=/boot/initramfs-5.15.10-1.el7.x86_64.img
title=RED OS (5.15.10-1) MUROM (7.3.1)
```

Для просмотра информации обо всех имеющихся версиях ядра используйте команду:

```
grubby --info ALL
```

С другими доступными опциями можно ознакомиться, выполнив:

```
grubby --help
```

Также можно отфильтровать вывод всех имеющихся версий ядра командой:

```
grubby --info=ALL | grep ^kernel

kernel=/boot/vmlinuz-5.15.35-5.el7.3.x86_64
kernel=/boot/vmlinuz-5.15.10-1.el7.x86_64
kernel=/boot/vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
kernel=/boot/vmlinuz-5.15.35-5.el7.3.x86_64
kernel=/boot/vmlinuz-5.15.10-1.el7.x86_64
kernel=/boot/vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
```

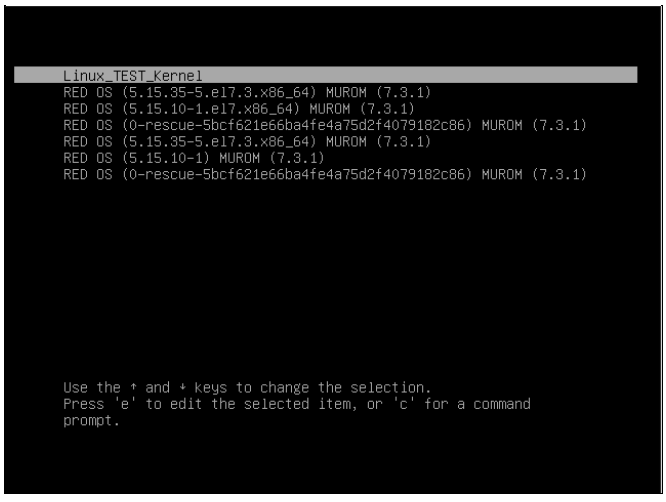
Для добавления новой записи в загрузчик выполните:

```
grubby --grub2 \
 > --add-kernel=/boot/vmlinuz-4.18.0-348.2.1.el8_5.x86_64 \
 > --title="Linux_TEST_Kernel" \
 > --initrd=/boot/initramfs-4.18.0-348.2.1.el8_5.x86_64.img \
 > --copy-default
```

Проверьте, добавлена ли новая запись:

```
grubby --info=ALL | grep -E "^kernel|^index"

index=0
kernel=/boot/vmlinuz-4.18.0-348.2.1.el8_5.x86_64
index=1
kernel=/boot/vmlinuz-5.15.35-5.el7.3.x86_64
index=2
kernel=/boot/vmlinuz-5.15.10-1.el7.x86_64
index=3
kernel=/boot/vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
index=4
index=5
kernel=/boot/vmlinuz-5.15.35-5.el7.3.x86_64
index=6
index=7
index=8
index=9
kernel=/boot/vmlinuz-5.15.10-1.el7.x86_64
index=10
index=11
kernel=/boot/vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
index=12
```

После перезагрузки новая запись доступна для выбора в загрузчике.



Также можно добавить аргументы в ядро, чтобы загрузчик мог их обработать, командой:

```
grubby --update-kernel=current_kernel --args="kernel_args"
```

Например, для добавления новых записей и исключения **IPv6**:

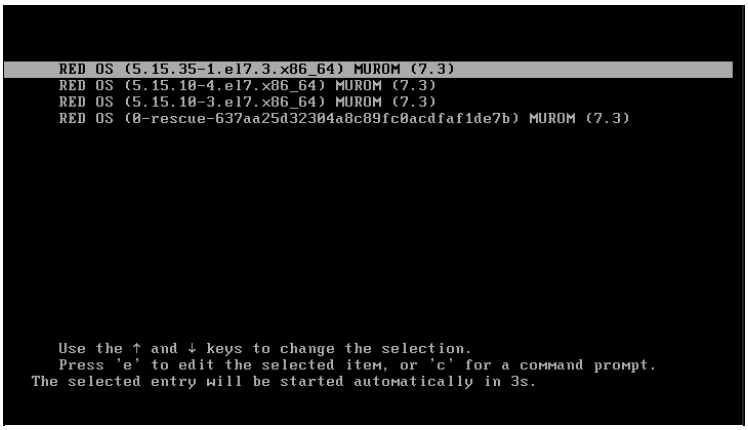
```
grubby --update-kernel=/boot/vmlinuz-$(uname -r) --remove-args="ipv6.disable=1" --args="console=ttys0"
```

Загрузчик во время загрузки передает параметры ядру в буфер памяти, файл **/proc/cmdline** в псевдо-файловой системе **/proc** также содержит копию данных параметров. Проверить это можно при помощи команды:

```
cat /proc/cmdline

BOOT_IMAGE=/vmlinuz-5.15.35-5.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro rd.driver.blacklist=nouveau modprobe.blacklist=nouveau
nvidia-drm.modeset=1 resume=/dev/mapper/ro_redos-swap rd.lvm.lv=ro_redos/root rd.lvm.lv=ro_redos/swap rhgb quiet
```

grub-customizer - утилита редактирования загрузчика ОС

GRUB (**Grand Unified Bootloader**) – программа-загрузчик операционной системы, которая позволяет выбирать и загружать операционные системы, установленные на компьютере. Помимо этого **grub** инициализирует параметры ядра системы и подготавливает систему к загрузке.



Настройка и редактирование загрузчика **grub** могут быть произведены с помощью графической утилиты **grub-customizer**. Данный вариант является довольно удобным и понятным.

Вы можете подробнее ознакомиться с установкой и настройкой утилиты **grub-customizer**, просмотрев наши обучающие видео:

- на **RuTube** — Удаление старых ядер из системы;
- в **Яндекс.Дзен** — Удаление старых ядер из системы;
- в **VK Видео** — Удаление старых ядер из системы.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты **grub-customizer** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install grub-customizer
```

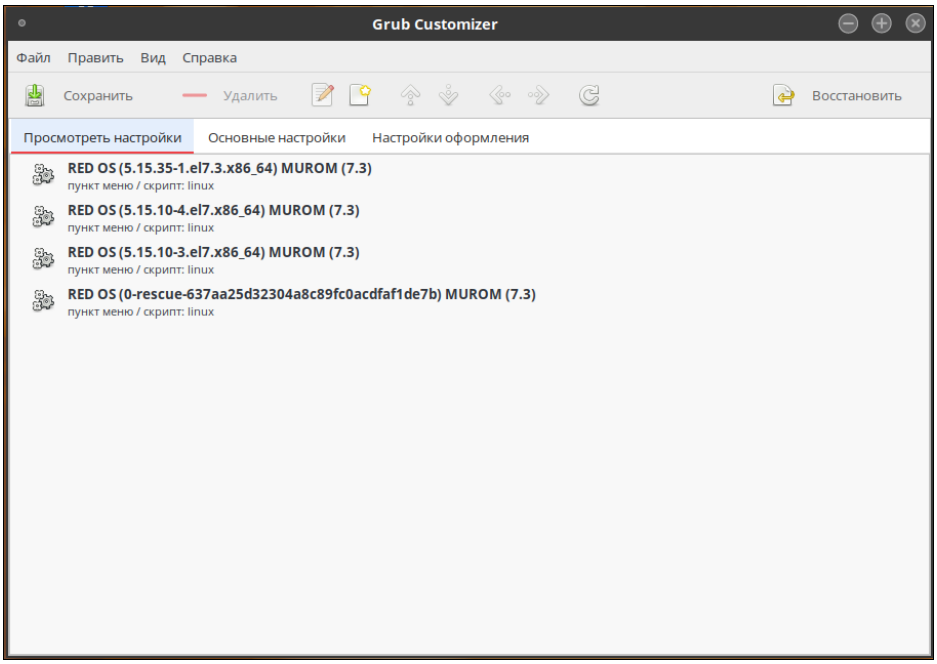
После установки запуск утилиты доступен из «**Главного меню**» - «**Администрирование**» - «**Настройки загрузчика**» или через консоль командой:

```
grub-customizer
```

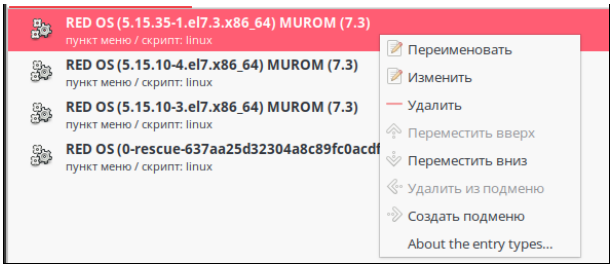
Перед запуском утилиты потребуется ввести пароль, так как для редактирования загрузчика операционной системы требуются права администратора.

Настройка утилиты

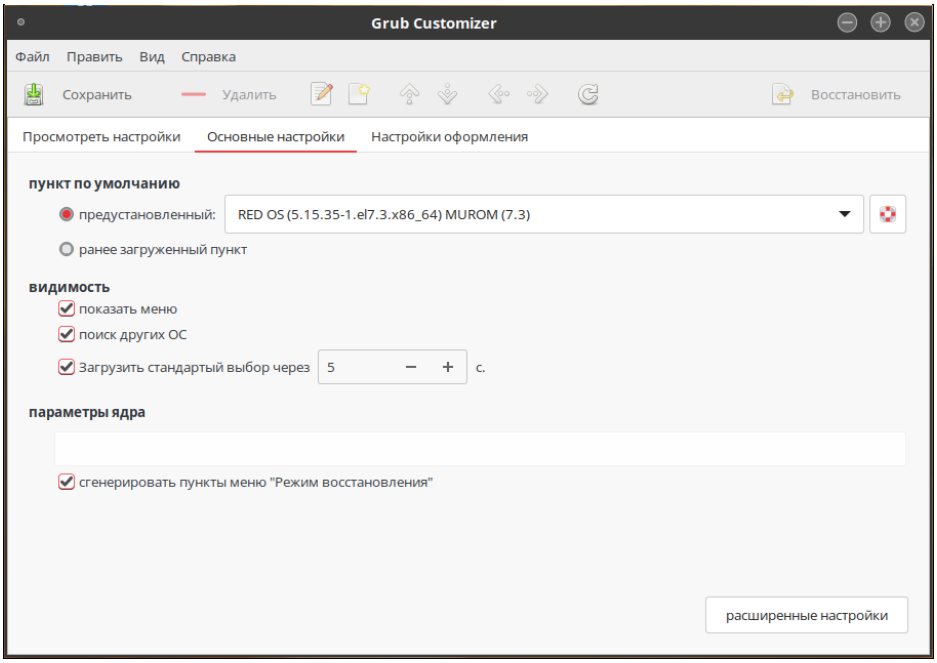
В главном окне программы отображается список доступных операционных систем, а в случае, если установлена одна ОС, то список представляет собой доступные версии ядра для загрузки.



В контекстном меню, вызываемом нажатием правой кнопкой мыши по требуемой ОС или версии ядра, есть возможность переименовать, отредактировать или переместить конфигурацию каждой ОС.

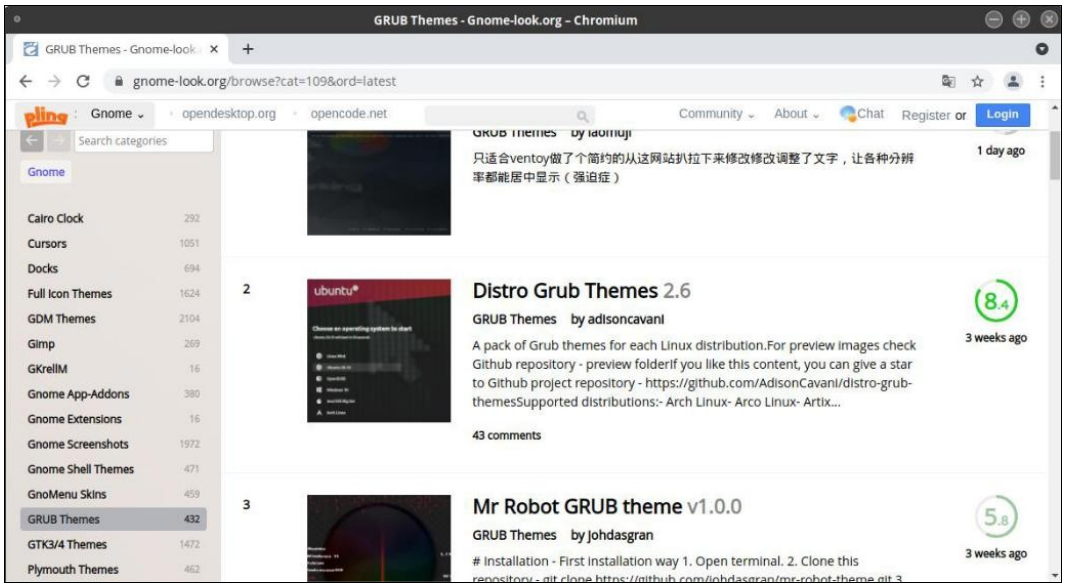


На вкладке «**Основные настройки**» можно выбрать необходимый пункт загрузчика, который будет использоваться по умолчанию, время, на протяжении которого будет отображаться меню **grub**, и параметры ядра для каждого пункта по умолчанию.



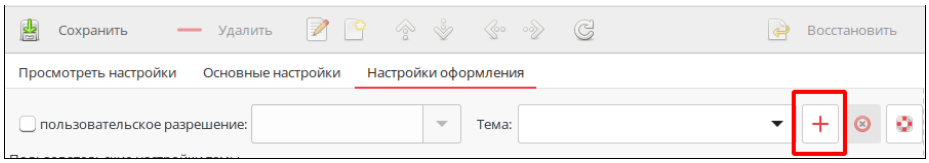
Вкладка «**Настройки оформления**» позволяет настроить отображение меню **grub**, а именно — цвет текста и фон. Также можно добавлять различные темы и устанавливать удобное разрешение экрана.

Для установки темы необходимо скачать архив понравившегося оформления меню **grub** с сайта gnome-look.org.

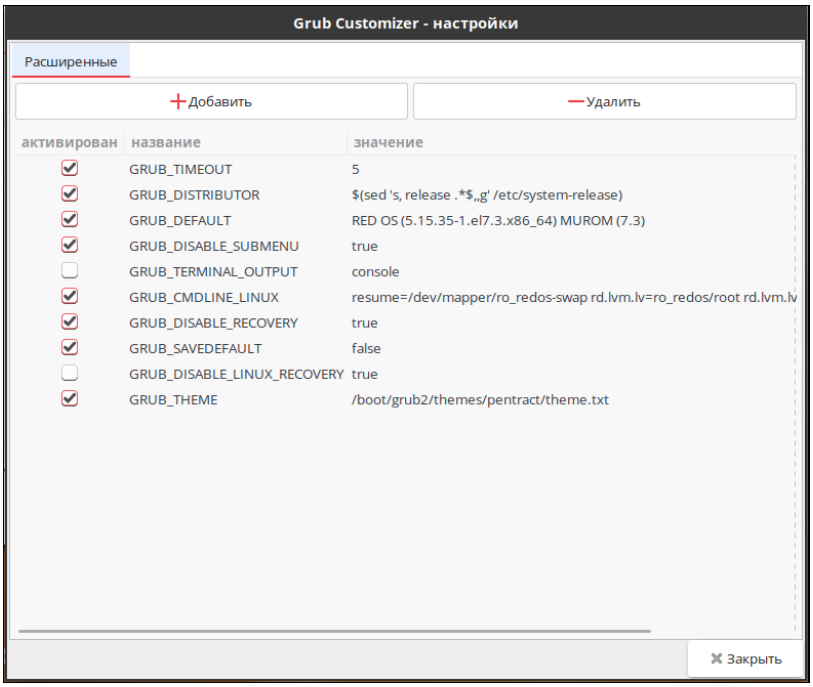


После того как архив выбранной темы будет скачан, с ним необходимо провести следующие преобразования: извлечь из архива папку с названием темы и заархивировать её отдельно. Данные действия необходимы для архивов, в которых помимо основной папки есть файл с разрешением **.sh**.

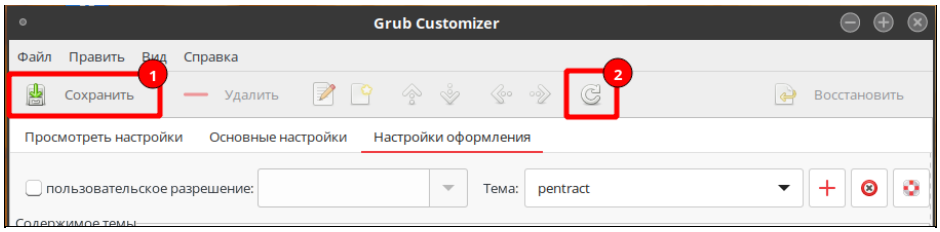
Для того чтобы добавить тему через утилиту **grub-customizer**, необходимо нажать на знак «**+**» рядом с раскрывающимся списком тем.



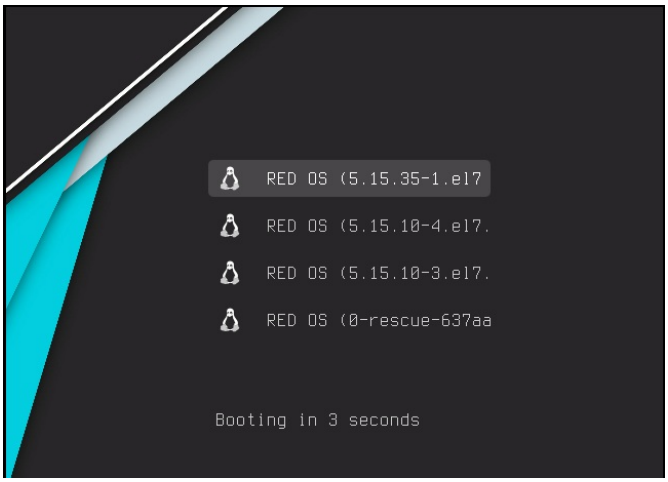
Кроме того, внизу экрана есть кнопка «**Расширенные настройки**». В открывшемся окне можно более детально настроить значения переменных из конфигурационного файла **/etc/default/grub**.



Когда настройка **grub** будет завершена, необходимо нажать кнопки «**Сохранить**» и «**Обновить**» на верхней панели инструментов.



При следующей перезагрузке системы меню **grub** будет выглядеть в соответствии с выбранной и настроенной темой.


RED OS (5.15.35-1.el7
RED OS (5.15.10-4.el7.
RED OS (5.15.10-3.el7.
RED OS (0-rescue-637aa
Booting in 3 seconds

Назначение пароля на загрузчик GRUB2

Вы можете подробнее ознакомиться с возможностью назначения пароля на загрузчик **grub2**, просмотрев наши обучающие видео:

- на **RuTube** — Назначение пароля на загрузчик GRUB2;
- в **Яндекс.Дзен** — Назначение пароля на загрузчик GRUB2;
- в **VK Видео** — Назначение пароля на загрузчик GRUB2.

На наших каналах вы также сможете найти много другой полезной информации.

Для защиты от несанкционированных изменений и прерывания нормальной загрузки ОС рекомендуется установить пароль на загрузчик GRUB.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду, в ответе которой назначьте новый пароль и, для исключения ошибок ввода, повторите его:

```
grub2-setpassword
Enter password: <новый_пароль>
Confirm password: <повторите_пароль>
```

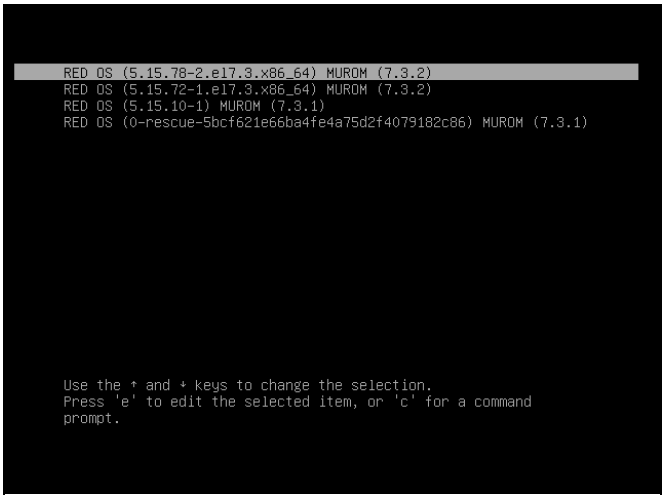
На системах с загрузкой посредством **UEFI** команду необходимо выполнить в таком варианте:

```
grub2-setpassword -o /boot/efi/EFI/redos/
```

Для применения настроек перезагрузите систему:

```
reboot
```

Далее при запуске системы нажмите клавишу «**e**».



Будет открыта форма для авторизации:

```
Enter username:
root
Enter password:
<введите_пароль_для_grub2>
```

Если необходимо убрать с определенного пункта меню GRUB запрос пароля, в конфигурационном файле **/boot/grub2/grub.cfg** найдите загрузочную строку и добавьте параметр **--unrestricted**.



```
  GNU nano 4.3                                  /boot/grub2/grub.cfg

### BEGIN /etc/grub.d/40_custom_proxy ###
menuentry 'RED OS (5.15.78-2.el7.3.x86_64) MUROM (7.3.2)' --class red --class gnu-linux --class gnu --class os --unrestricted $menuentry_id_>
        load_video
        set gfxpayload=keep
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msd>
        else
          search --no-floppy --fs-uuid --set=root 514b64bc-7505-422e-9642-f0e926608f31
        fi
        linux   /vmlinuz-5.15.78-2.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro resume=/dev/mapper/ro_redos-swap rd.lvm.lv=ro_redos/root r>
        initrd /initramfs-5.15.78-2.el7.3.x86_64.img
}
```

Для систем с **UEFI** файл конфигурации располагается в по адресу **/boot/efi/EFI/redos/grub.cfg**.

Восстановление загрузчика GRUB2

Восстановление загрузчика для систем, использующих BIOS
Восстановление загрузчика для систем, использующих UEFI

Вы можете подробнее ознакомиться с восстановлением загрузчика **grub2** и восстановлением для систем, просмотрев наши обучающие видео:

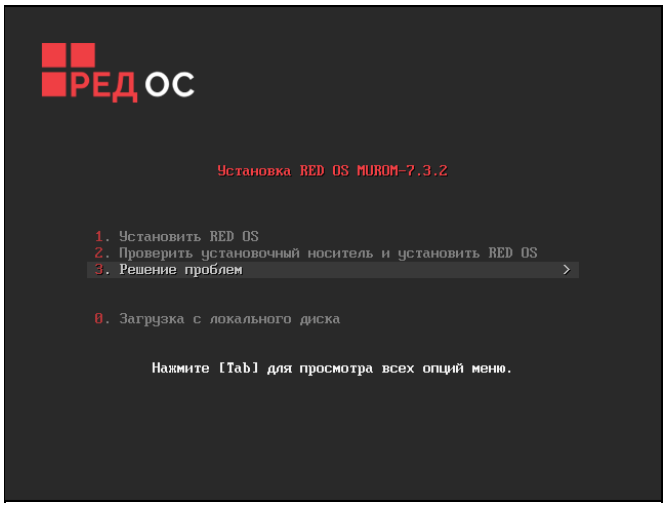
- на **RuTube** — Восстановление загрузчика GRUB2;
- в **Яндекс.Дзен** — Восстановление загрузчика GRUB2;
- в **VK Видео** — Восстановление загрузчика GRUB2.

На наших каналах вы также сможете найти много другой полезной информации.

Для восстановления необходимо загрузиться с установочного образа вашей версии РЕД ОС, поставив ваш носитель первым в списке предпочтения загрузки.

Восстановление загрузчика для систем, использующих BIOS

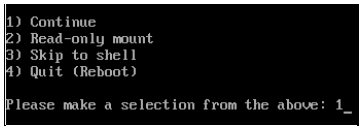
В появившемся меню следует выбрать пункт «**Решение проблем**».



Далее нужно выбрать пункт «**Исправить установленную RED OS**»:



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***:



Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Для определения диска, на котором установлена система, можно использовать следующую команду:

```
lsblk
```

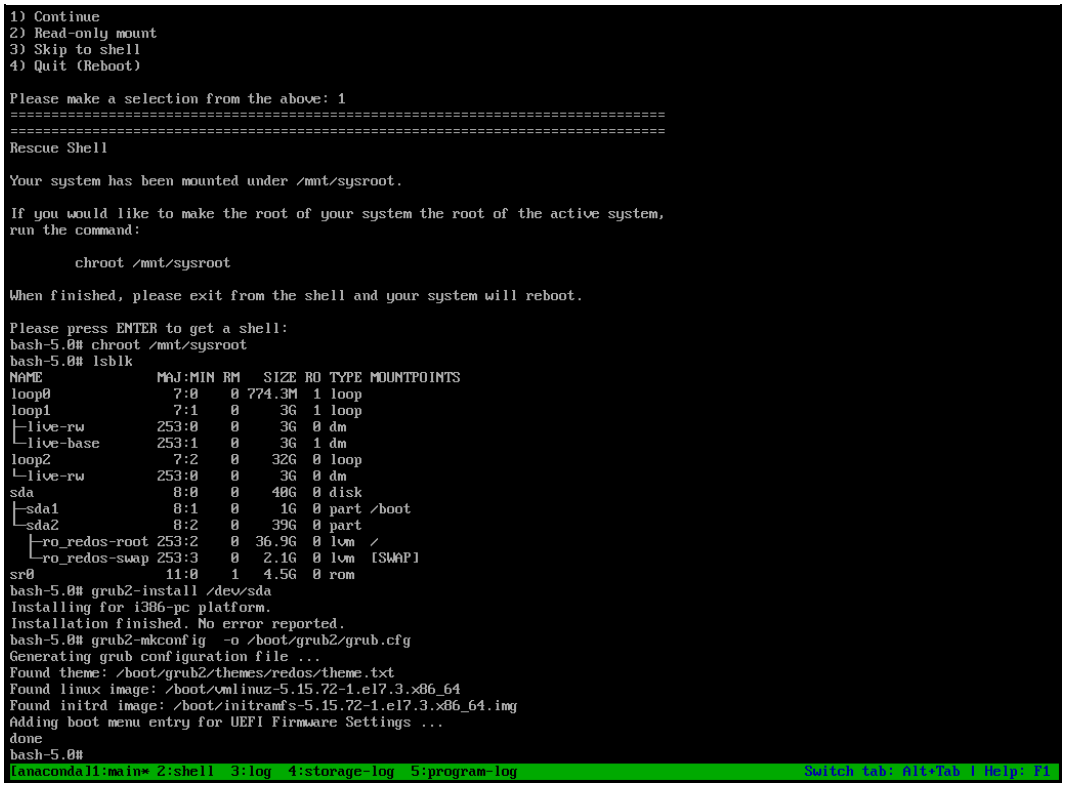
Далее выполните установку загрузчика командой (в конце указывается нужный диск):

```
grub2-install /dev/sda
```

Теперь создайте новый конфигурационный файл загрузчика с помощью команды:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Восстановление загрузчика для систем, использующих UEFI

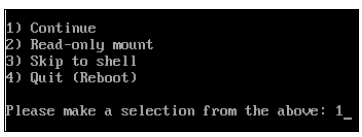
В появившемся меню следует выбрать пункт «**Troobleshooting**».



Далее нужно выбрать пункт «**Rescue a RED OS system**».



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***.



Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

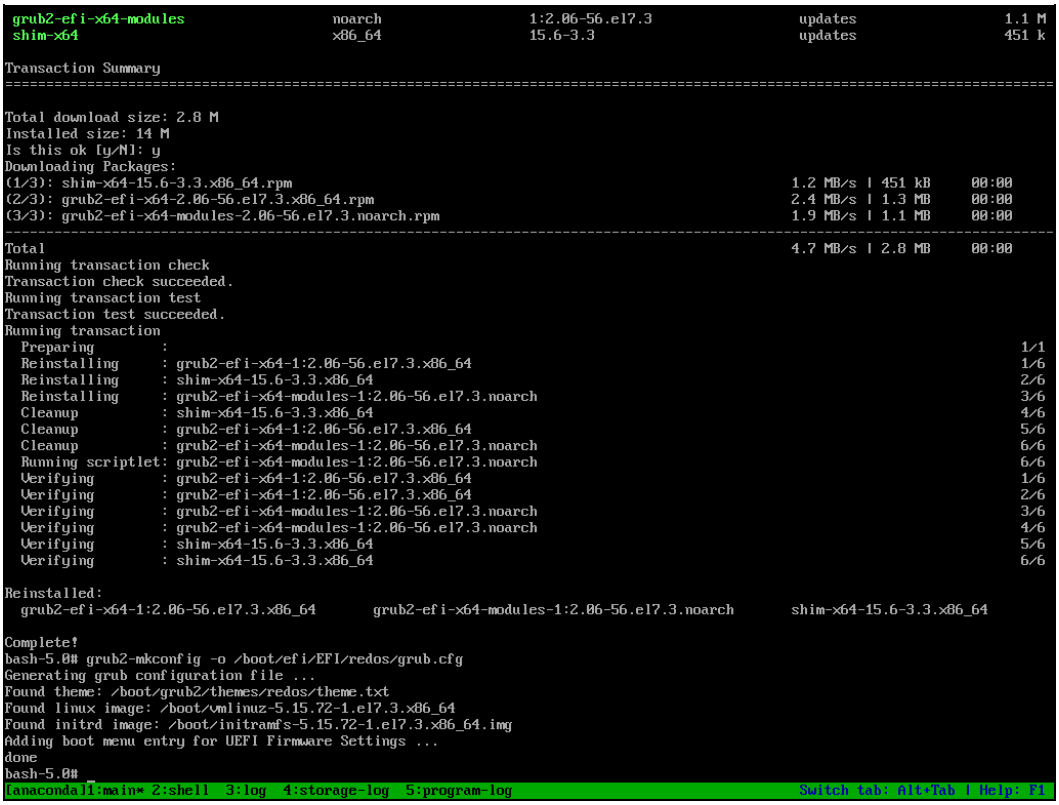
Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Затем потребуется обновить конфигурацию загрузчика с помощью команд:

```
dnf reinstall grub2-efi-x64  shim-x64 grub2-efi-x64-modules
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Описание процесса разметки диска

Так же, как и в других файловых системах, все данные хранятся на диске по определенным адресам. Эти адреса сохранены в метаданных. И тут уже начинаются различия. Все метаданные организованны в виде b-деревьев. Это дает большую производительность при работе с файловой системой, а также позволяет добавлять неограниченное количество файлов.

Но даже это еще не все. Когда вы перезаписываете файл, данные не перезаписываются, а лишь модифицированная часть копируется в новое место, затем просто обновляются метаданные. Это позволяет создавать мгновенные снимки файловой системы, которые не занимают места на диске, пока не было внесено много изменений. Если же старый блок больше не нужен, потому что он не является частью какого-либо снимка, то он автоматически удаляется.

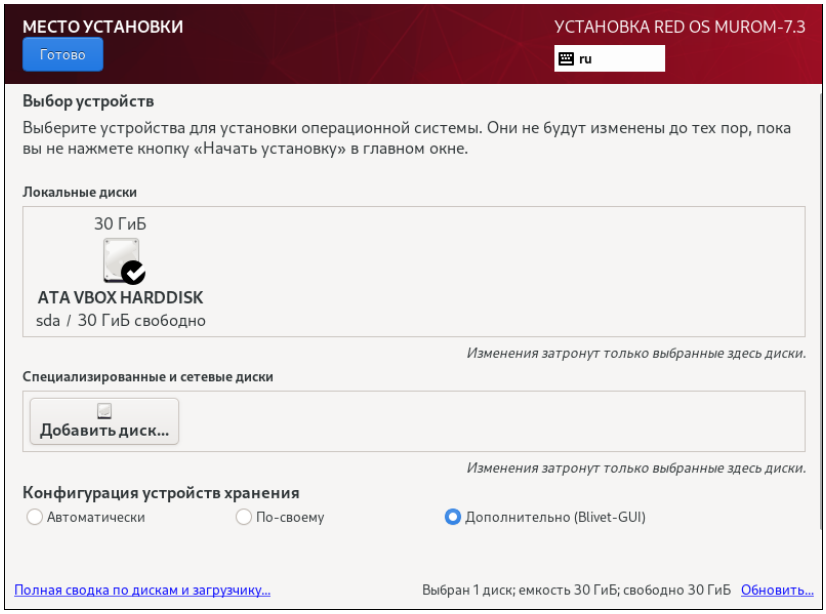
Каждый диск, независимо от его размера, делится на блоки по **1 Гб** для данных и **256 Мб** для метаданных. Затем эти блоки собираются в группы, каждая из которых может храниться на разных устройствах, количество таких блоков в группе может зависеть от уровня RAID для группы. Менеджер томов уже интегрирован в файловую систему, поэтому больше никакое дополнительное ПО использовать не нужно.

Защита и сжатие данных также поддерживается на уровне файловой системы, так что здесь вам тоже не нужны дополнительные программы. Также файловая система btrfs поддерживает зеркалирование данных на нескольких носителях. Вот другие особенности btrfs, которые можно упомянуть:

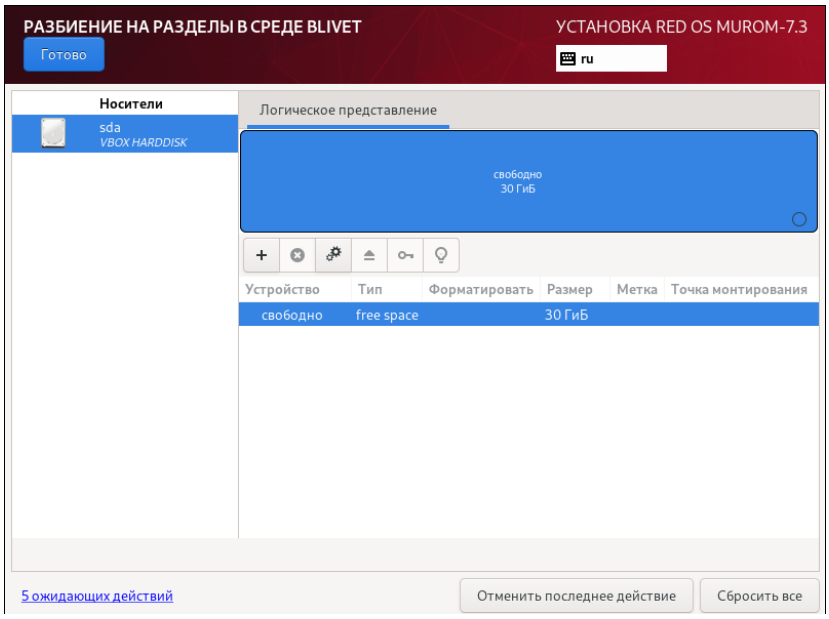
- Поддержка снимков файловой системы, только для чтения или для записи;
- Контрольные суммы для данных и метаданных с помощью алгоритма **crc32**. Таким образом, можно очень быстро определить любые повреждения блока;
- Сжатие с помощью **Zlib** и **LZO**;
- Оптимизация для работы с **SSD**, файловая система автоматически определяет **ssd** и начинает вести себя по-другому;
- Фоновый процесс для обнаружения и исправления ошибок, а также дефрагментации и дедупликации в реальном времени;
- Поддерживается преобразование из **ext4** и **ext3**.

Создание тома при установке ОС (через blivet-gui)

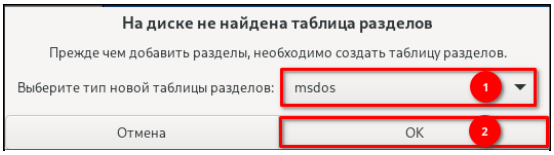
При установке ОС для создания тома при помощи **blivet-gui**, нужно в «**Конфигурации устройств хранения**» выбрать пункт «**Дополнительно (Blivet-GUI)**», после чего нажать кнопку «**Готово**», которая находится сверху слева.



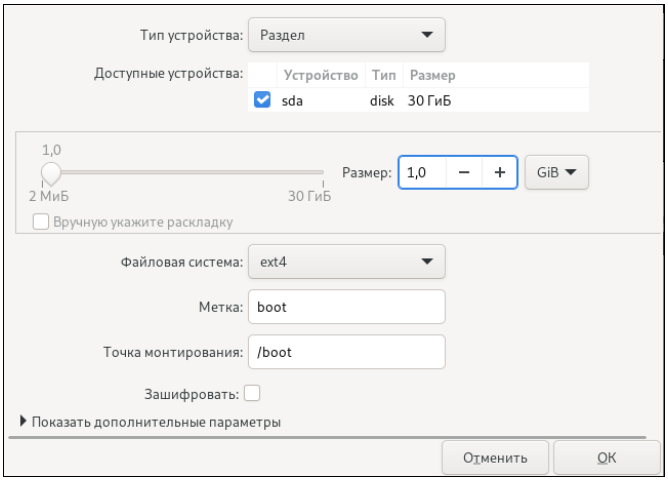
Далее происходит переход в раздел «**Разбиение на разделы в среде BLIVET**», где уже можно создать необходимые тома и подтома. Для создания раздела нужно нажать на кнопку «**+**».



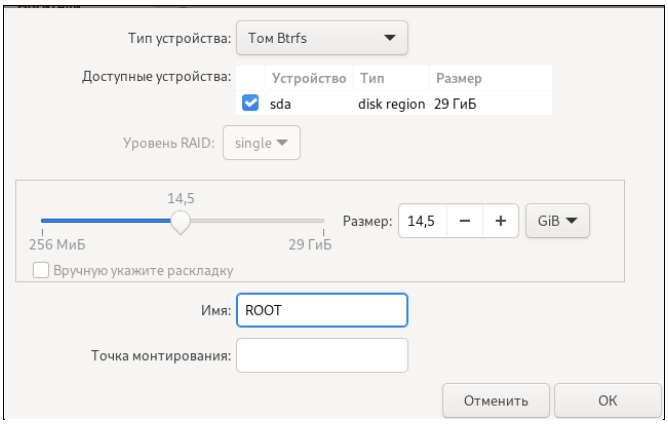
При появлении следующего окна установите тип новой таблицы разделов **msdos** и нажмите «**OK**».



Сначала необходимо создать раздел с местом установщика системы, нажав на кнопку «**+**».



Для создания тома необходимо выбрать носитель, на котором будут создаваться тома, и нажать на кнопку «**+**». После чего появится окно:



В данном окне предлагается выбрать тип устройства, размер, выделяемый на это устройство, файловую систему и точку монтирования.

Для создания тома с файловой системой **btrfs**:

- измените пункт «**Тип устройства**» на «**Том Btrfs**»;

- измените размер тома на необходимый;
- укажите имя тома;
- поле «**Точка монтирования**» оставьте без изменений;
- нажмите «**OK**».

Создастся новый том со своим названием.

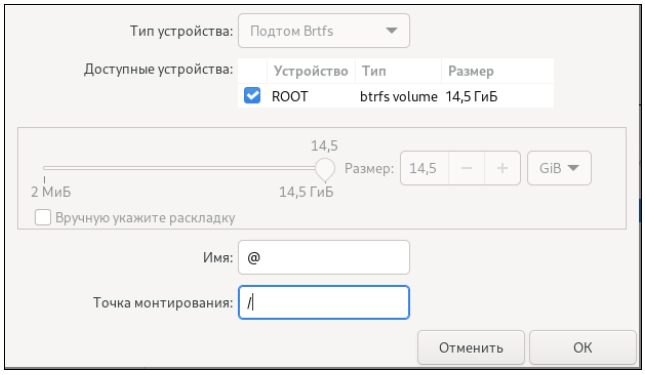


Для того чтобы создать подтом, нужно нажать на новый том и снова нажать на кнопку «**+**», после чего появится окно редактирования настроек.

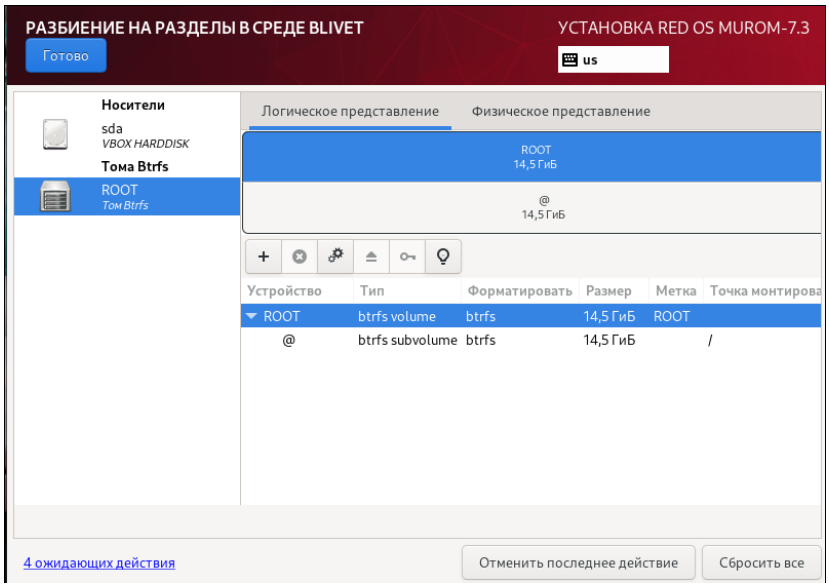
При создании можно выбрать необходимый из доступных томов, чтобы в нём создать подтом.

Также в данном окне необходимо задать имя подтома и точку монтирования. В данном случае в поле «**Точка монтирования**» задано значение «**/**», которое включает в себя корневая директорию, содержащая всю файловую иерархию.

После чего нажиманием «**OK**».



После чего в списке устройств, можно увидеть созданный том и подтом.



Работа с квотами диска

Сначала можно посмотреть список доступных **subvolume** командой:

```
sudo btrfs subvolume list /

ID 256 gen 4371 top level 5 path @
ID 261 gen 4354 top level 256 path var/lib/portables
```

Для создания **subvolume** требуется ввести команду:

```
sudo btrfs subvolume create /@QUOTA

Create subvolume '//@QUOTA'
```

Для включения поддержки квот выполните команду:

```
sudo btrfs quota enable /@QUOTA
```

Для просмотра списка доступных **subvolume**, на которые можно ввести ограничения, требуется выполнить команду:

```
sudo btrfs qgroup show /

qgroupid         rfer         excl
--------         ----         ----
0/5         16.00Kib     16.00Kib
0/256        5.85Kib      5.85Kib
0/261       16.00Kib     16.00Kib
0/266       16.00Kib     16.00Kib
```

Для выбора нужного **ID** необходимо провести аналогию с выводом из команды `btrfs subvolume list /`, и на основе сопоставления **qgroupid** и **ID** назначать квоту.

В данном случае **ID** - **0/266** является только что созданной **subvolume** - **/@QUOTA**.

Для того чтобы ввести ограничения на **subvolume**, нужно выполнить:

```
sudo btrfs qgroup limit 1G /@QUOTA/
```

findmnt - получение информации о подключенных файловых системах

Findmnt – это утилита командной строки, используемая для отображения списка подключенных файловых систем или поиск файлов системы в **/etc/fstab**, **/etc/mtab** или **/proc/self/mountinfo**. Если устройство или точка монтирования не заданы, будут обнаружены все регистрируемые файловые системы.

Для отображения списка подключенных файловых систем выполните команду:

```
findmnt

TARGET                   SOURCE     FSTYPE  OPTIONS
/                        /dev/mapper/ro_redos-root
│                                   ext4    rw,relatime,seclabel
├─/sys                   sysfs      sysfs   rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/kernel/security securityfs securit rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/cgroup       cgroup2    cgroup2 rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/pstore       pstore     pstore  rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/bpf          bpf        bpf     rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/selinux      selinuxfs  selinux rw,relatime
│ ├─/sys/kernel/debug    debugfs    debugfs rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/kernel/tracing  tracefs    tracefs rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/fuse/connections fusectl    fusectl rw,nosuid,nodev,noexec,relatime
│ └─/sys/kernel/config   configfs   configf rw,nosuid,nodev,noexec,relatime
├─/proc                  proc       proc    rw,nosuid,nodev,noexec,relatime
│ └─/proc/sys/fs/binfmt_misc systemd-1  autofs  rw,relatime,fd=30,pgrp=1,timeout
├─/dev                   devtmpfs   devtmpf rw,nosuid,noexec,seclabel,size=4
│ ├─/dev/shm             tmpfs      tmpfs   rw,nosuid,nodev,seclabel,inode64
│ ├─/dev/pts             devpts     devpts  rw,nosuid,noexec,relatime,seclab
│ ├─/dev/hugepages       hugetlbfs  hugetlb rw,relatime,seclabel,pagesize=2M
│ └─/dev/mqueue          mqueue     mqueue  rw,nosuid,nodev,noexec,relatime,
├─/run                   tmpfs      tmpfs   rw,nosuid,nodev,seclabel,size=19
│ ├─/run/user/42         tmpfs      tmpfs   rw,nosuid,nodev,relatime,seclabe
│ ├─/run/user/1000       tmpfs      tmpfs   rw,nosuid,nodev,relatime,seclabe
│ │ └─/run/user/1000/gvfs    gvfsd-fuse fuse.gv rw,nosuid,nodev,relatime,user_id
│ └─/run/media/user/redos-MUROM-7.3 x86_64
│                         /dev/sr0   iso9660 ro,nosuid,nodev,relatime,nojolie
├─/boot                  /dev/sda1  ext4    rw,relatime,seclabel
└─/var/lib/nfs/rpc_pipefs  sunrpc     rpc_pip rw,relatime
```

В выводе отображается точка монтирования **TARGET**, исходное устройство **SOURCE**, тип файловой системы **FSTYPE** и дополнительные параметры **OPTIONS** для каждой файловой системы.

По умолчанию команда findmntвыводит данные в древовидном формате. Чтобы отобразить информацию в виде списка, используйте опцию **-l** :

```
findmnt -l

TARGET                           SOURCE                  FSTYPE          OPTIONS
/sys                             sysfs                   sysfs           rw,nosuid,nodev,noexec,relatime,seclabel
/proc                            proc                    proc            rw,nosuid,nodev,noexec,relatime
/dev                             devtmpfs                devtmpfs        rw,nosuid,noexec,seclabel,size=4096k,nr_inodes=65536,mode=755,inode64
/sys/kernel/security             securityfs              securityfs      rw,nosuid,nodev,noexec,relatime
/dev/shm                         tmpfs                   tmpfs           rw,nosuid,nodev,seclabel,inode64
/dev/pts                         devpts                  devpts          rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000
/run                             tmpfs                   tmpfs           rw,nosuid,nodev,seclabel,size=199140k,nr_inodes=819200,mode=755,inode64
/sys/fs/cgroup                   cgroup2                 cgroup2         rw,nosuid,nodev,noexec,relatime,seclabel,nsdelegate
/sys/fs/pstore                   pstore                  pstore          rw,nosuid,nodev,noexec,relatime,seclabel
/sys/fs/bpf                      bpf                     bpf             rw,nosuid,nodev,noexec,relatime,mode=700
/                                /dev/mapper/ro_redos-root ext4          rw,relatime,seclabel
/sys/fs/selinux                  selinuxfs               selinuxfs       rw,relatime
/proc/sys/fs/binfmt_misc         systemd-1               autofs
rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=17271
/dev/hugepages                   hugetlbfs               hugetlbfs       rw,relatime,seclabel,pagesize=2M
/dev/mqueue                      mqueue                  mqueue          rw,nosuid,nodev,noexec,relatime,seclabel
/sys/kernel/debug                debugfs                 debugfs         rw,nosuid,nodev,noexec,relatime,seclabel
/sys/kernel/tracing              tracefs                 tracefs         rw,nosuid,nodev,noexec,relatime,seclabel
/sys/fs/fuse/connections         fusectl                 fusectl         rw,nosuid,nodev,noexec,relatime
/sys/kernel/config               configfs                configfs        rw,nosuid,nodev,noexec,relatime
/boot                            /dev/sda1               ext4            rw,relatime,seclabel
/var/lib/nfs/rpc_pipefs          sunrpc                  rpc_pipefs      rw,relatime
/run/user/42                     tmpfs                   tmpfs
rw,nosuid,nodev,relatime,seclabel,size=99568k,nr_inodes=24892,mode=700,uid=42,gid=42,inode64
```

```
/run/user/1000                  tmpfs                  tmpfs
rw,nosuid,nodev,relatime,seclabel,size=99568k,nr_inodes=24892,mode=700,uid=1000,gid=1000,inode64
/run/user/1000/gvfs             gvfsd-fuse             fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=1000,group_id=1000
/run/media/user/redos-MUROM-7.3 x86_64 /dev/sr0        iso9660
ro,nosuid,nodev,relatime,nojoliet,check=s,map=n,blocksize=2048,uid=1000,gid=1000,dmode=500,fmode=400,iocharset=utf8
```

Для отображения только определенной файловой системы используется параметр **-t**, в качестве аргумента которому необходимо передать тип файловой системы. Например:

```
findmnt -t ext4

TARGET  SOURCE                  FSTYPE OPTIONS
/       /dev/mapper/ro_redos-root ext4   rw,relatime,seclabel
└─/boot /dev/sda1               ext4   rw,relatime,seclabel
```

Найти файловую систему также можно, используя точку монтирования. Например, команда `findmnt --fstab /boot` отобразит все файловые системы **/etc/fstab**, где каталогом точки монтирования является **/boot**.

```
findmnt --fstab /boot

TARGET SOURCE                                FSTYPE OPTIONS
/boot  UUID=890a40d8-ab34-44b8-9632-6f6026dcb78e ext4   defaults
```

Чтобы вывести все файловые системы **/etc/fstab** и преобразовать теги *LABEL* и *UUID* в реальные имена устройств, необходимо в команду добавить ключ **--evaluate**.

```
findmnt --fstab /boot --evaluate

TARGET SOURCE    FSTYPE OPTIONS
/boot  /dev/sda1 ext4   defaults
```

Findmnt также позволяет отслеживать действия по монтированию и размонтированию в файловой системе. Для этого используется команда:

```
findmnt -p
```

Для отображения определенных событий следует указать точку монтирования, например, **/mnt/test**:

```
findmnt --poll --mountpoint /mnt/test
```

Для проверки правильности точек проверки следует контрольная команда (с правами администратора системы или суперпользователя **root**):

```
findmnt --verify

Success, no errors or warnings detected
```

Для получения более подробной информации в выводе используется параметр **--verbose** :

```
findmnt --verify --verbose

/
   [ ] target exists
   [ ] source /dev/mapper/ro_redos-root exists
   [ ] FS type is ext4
/boot
   [ ] target exists
   [ ] UUID=890a40d8-ab34-44b8-9632-6f6026dcb78e translated to /dev/sda1
   [ ] source /dev/sda1 exists
   [ ] FS type is ext4
none
   [ ] source /dev/mapper/ro_redos-swap exists
   [ ] FS type is swap
Success, no errors or warnings detected
```

Проверка файловой системы на наличие ошибок

Параметры fsck
Пример проверки диска на ошибки с помощью fsck
Запуск автоматической проверки и исправления найденных ошибок
Ручное добавление параметров в меню GRUB при загрузке ОС
Добавление параметров в меню GRUB с помощью утилиты grubby
Создание файла /forcefsck
Запуск проверки в ручном режиме
Использование загрузочного диска/flash для проверки файловой системы на ошибки
Проверка LVM-разделов с помощью утилиты fsck

В определенных случаях (в результате сбоя или некорректного завершения работы) на файловой системе могут накапливаться ошибки. В РЕД ОС для проверки файловой системы и исправления ошибок имеется утилита **fsck** ("file system consistency check").

Инструмент fsck обладает следующим функционалом:

- проверка файловой системы при возникновении проблем (не загружается система/поврежденные файлы) или в качестве профилактического обслуживания;
- диагностика состояния внешних накопителей, таких как SD-карты или USB-накопители.

Базовый синтаксис соответствует следующему шаблону:

```
fsck <опции> <файловая_система>
```

В качестве *файловой системы* может быть устройство, точка монтирования или раздел, в том числе LVM.

Вы можете подробнее ознакомиться с возможностями проверки файловой системы на наличие ошибок, просмотрев наши обучающие видео:

- на **RuTube** — Проверка файловой системы на наличие ошибок;
- в **Яндекс.Дзен** — Проверка файловой системы на наличие ошибок;
- в **VK Видео** — Проверка файловой системы на наличие ошибок.

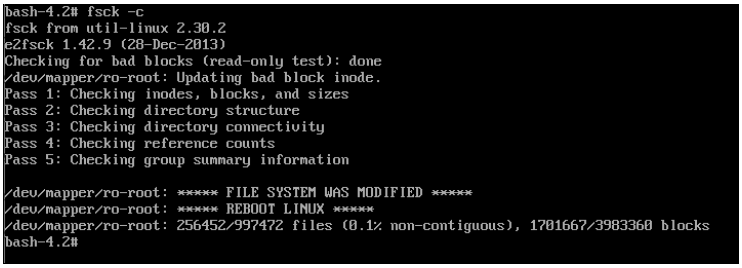
На наших каналах вы также сможете найти много другой полезной информации.

Параметры fsck

fsck -p – утилита автоматически исправит найденные ошибки.

Вывод аналогичен простой проверке.

fsck -c – проверка файловой системы на поврежденные сектора.



Для получения списка команд наберите **fsck --help** или **fsck -h.**

Опция	Описание
-a	Устаревшая опция. Указывает исправлять все найденные ошибки без одобрения пользователя.
-r	Применяется для файловых систем ext. Указывает fsck спрашивать пользователя перед исправлением каждой ошибки
-n	Выполняет только проверку ФС, без исправления ошибок. Используется также для получения информации о ФС
-c	Применяется для файловых систем ext3/4. Помечает все повреждённые блоки для исключения последующей записи в них
-f	Принудительно проверяет ФС, даже если ФС исправна
-y	Автоматически подтверждает запросы к пользователю

-b	Задаёт адрес суперблока
-p	Автоматически исправлять найденные ошибки. Заменяет устаревшую опцию -a
-A	Проверяет все ФС
-C [<fd>]	Показывает статус выполнения. Здесь fd – дескриптор файла при отображении через графический интерфейс
-l	Блокирует устройство для исключительного доступа
-M	Запрещает проверять примонтированные ФС
-N	Показывает имитацию выполнения, без запуска реальной проверки
-P	Проверять вместе с корневой ФС
-R	Пропускает проверку корневой ФС. Может использоваться только совместно с опцией -A
-r [<fd>]	Выводит статистику для каждого проверенного устройства
-T	Не показывать заголовок при запуске
-t <тип>	Задаёт ФС для проверки. Можно задавать несколько ФС, перечисляя через запятую
-V	Выводит подробное описание выполняемых действий

Пример проверки диска на ошибки с помощью fsck

Запуск автоматической проверки и исправления найденных ошибок

Существует несколько способов запуска автоматической проверки на ошибки:

1. Ручное добавление параметров в меню **GRUB** при загрузке ОС.

2. Добавление параметров в меню **GRUB** с помощью утилиты **grubby**.

3. Создание файла **/forcefsck**.

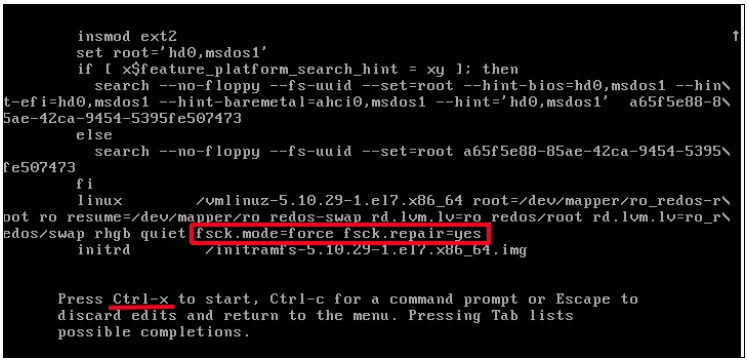
1. Ручное добавление параметров в меню GRUB при загрузке ОС

Первый вариант проверки и исправления ошибок на разделах жесткого диска.

В меню **GRUB** перейдите в режим редактирования загрузочной строки, нажав при этом клавишу **e**. Добавьте параметры:

```
fsck.mode=force fsck.repair=yes
```

в конец предпоследней строки.



Нажмите **Ctrl+X** для запуска ОС с этими параметрами, во время запуска будет произведена проверка разделов диска, и при наличии ошибок произведено их исправление.

2. Добавление параметров в меню GRUB с помощью утилиты grubby

Существует еще один способ добавления параметров ядра для принудительной проверки файловой системы на ошибки и их исправления. Добавить параметры можно командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --args="fsck.mode=force fsck.repair=yes"
```

Удалить установленные параметры можно следующей командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --remove-args="fsck.mode=force fsck.repair=yes"
```

3. Создание файла /forcefsck

Бывают ситуации, когда систему необходимо проверить на наличие ошибок в *незапланированный* момент. Для этого можно **принудительно** запустить утилиту **fsck** для проверки при следующей перезагрузке. Запуск осуществляется командой:

```
sudo touch /forcefsck
```

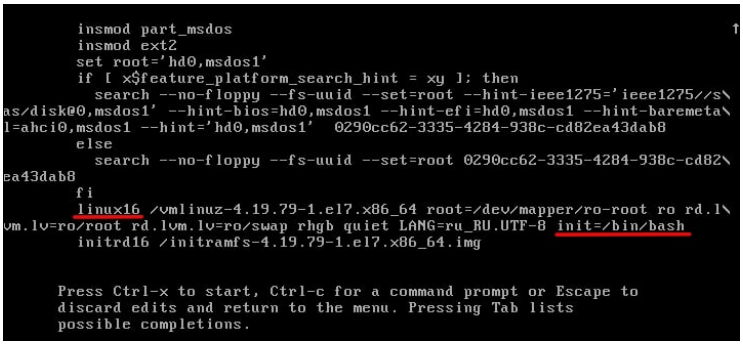
Команда **sudo** (после ввода пароля) предоставит права для создания с помощью **touch** пустого файла в корне диска **/forcefsck**, который послужит сигналом (флагом) для **fsck**, что нужно проверить диски.

Останется только перезагрузить компьютер и **fsck** начнет проверять все жесткие диски, указанные в **/etc/fstab**.

Запуск проверки в ручном режиме

Следующий метод относится к проверке диска, когда операционная система загружена в режиме **single mode**.

1. Запустим ОС в single mode, для этого пропишите в меню загрузки grub параметр init=/bin/bash в конце строки, которая начинается на linux16, см. рисунок.



Также данная строка может начинаться с linuxefi, этот параметр характерен для систем с загрузкой в UEFI. Нажмите **"ctrl+x"** для запуска с этим параметром(init=/bin/bash).

2. Запустите проверку выполнив команду:

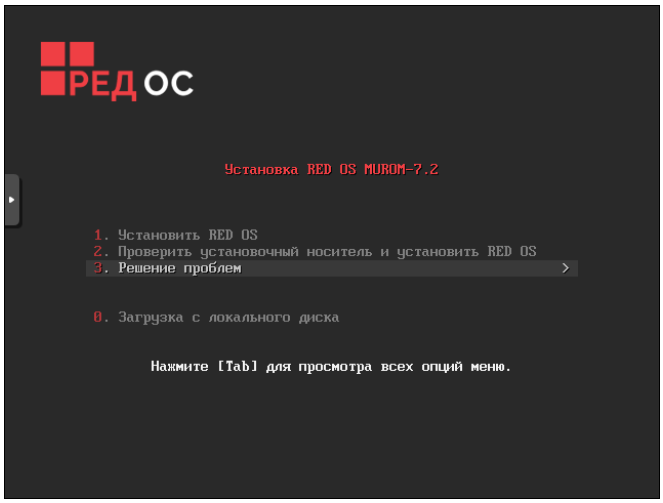
```
/usr/sbin/fsck -ACVfyv
```

Во время проверки на экране появится отчет о выполненных операциях, если отчет длинный, то можно его можно пролистать вверх сочетанием клавиш shift+PageUp. После проверки дисков перезагрузите компьютер, нажав на кнопку на системном блоке.

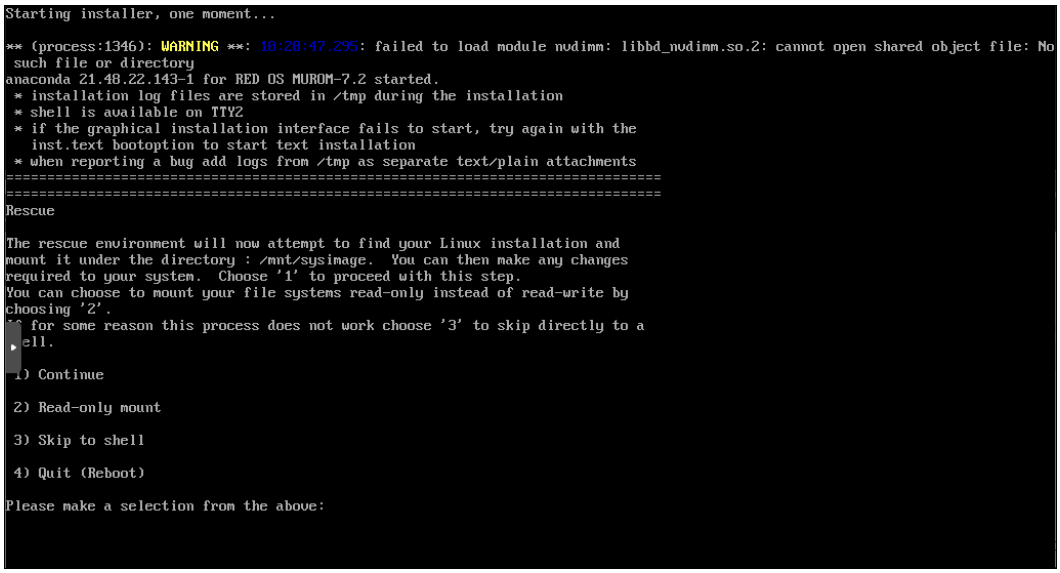
Наглядное видео примера проверки диска на ошибки:

Использование загрузочного диска/flash для проверки файловой системы на ошибки.

Загрузившись в режим восстановления операционной системы РЕД ОС с помощью загрузочного диска или съемного накопителя с установленным образом операционной системы РЕД ОС. Выберите пункт: **«Решение проблем» -> «Исправить установленную RED OS»**.



Система перезагрузится в режим восстановления. Введите «**2**» и нажмите 2 раза **Enter**. Так вы смонтируете операционную систему в режим «**Только для чтения**»



Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Потом введите команду:

```
# chroot /mnt/sysimage
```

После этого можете вводить **fsck**:

```
# fsck -ACVfyv
```

Если проверка завершится с такой ошибкой:

```
[путь_к_файловой_системе] is mounted
```

Введите:

```
umount [путь_к_файловой_системе]
```

И еще раз запустите утилиту **fsck**:

```
# fsck -ACVfyv
fsck from util-linux 2.30.2
...
```

Если система не выявит ошибок, то получится такой вывод:

```
[путь_к_файловой_системе] clean …
```

Чтобы выйти из режима восстановления, вы должны смонтировать все разделы, которые были отмонтированы командой **umount**, с помощью команды **mount**, нажать сочетание клавиш **ctrl+d**, а затем ввести команду **reboot**, которая перезапустит вашу операционную систему.

```
# reboot
```

По умолчанию, утилита **fsck** при проверке будет использовать разделы, указанные в **/etc/fstab/**, сформированные при установке операционной системы РЕД ОС.

Проверка LVM-разделов с помощью утилиты fsck

Перед проведением проверки необходимо найти устройство и размонтировать его.

Для просмотра всех подключенных устройств и проверки расположения диска выполните команду:

```
lsblk

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 20G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 19G 0 part
├─ro_redos-root 253:0 0 17G 0 lvm /
└─ro_redos-swap 253:1 0 2G 0 lvm [SWAP]
sr0 11:0 1 4,3G 0 rom /run/media/user/redos-MUROM-7.3.1 x86_64
```

При попытке запустить проверку на смонтированном диске или разделе в консоли появляется предупреждение о том, что невозможно продолжить проверку, так как диск смонтирован.

```
fsck -nf /dev/ro_redos/root

fsck из util-linux 2.37.3
e2fsck 1.44.6 (5-Mar-2019)
Warning! /dev/mapper/ro_redos-root is mounted.
```

Для того чтобы размонтировать диск, следует использовать команду:

```
umount <файловая_система>
```

Однако попытка выполнить данную процедуру на работающей ОС ни к чему не приведет.

```
umount /dev/ro_redos/root

umount: /: target is busy.
```

Также проблемой при попытке проверить LVM-разделы может быть и то, что они являются не активными. Для проверки следует использовать команду:

```
lvscan

ACTIVE '/dev/ro_redos/swap' [2,00 GiB] inherit
ACTIVE '/dev/ro_redos/root' [<17,00 GiB] inherit
```

Для активации раздела служит команда:

```
vgchange –ay <раздел>
```

Таким образом, можно сделать вывод, что проверка LVM-разделов через консоль с использованием утилиты **fsck** невозможна. Но это не значит, что LVM-разделы совсем не подлежат проверке. Существует как минимум два способа, позволяющие провести диагностику LVM-разделов.

Первым способом является проведение проверки через консоль загрузчика операционной системы **GRUB**.

А вторым - запуск утилиты **fsck** в **live-сессии** системы.

Очевидным плюсом при проверке дисковых пространств, в том числе LVM-разделов, через live-сессию является то, что разделы там по умолчанию являются не смонтированными. Поэтому проверка LVM-раздела будет выполнена с первого раза.

```
[root@redos ~]# fsck /dev/ro_redos/root
fsck из util-linux 2.34
e2fsck 1.44.6 (5-Mar-2019)
/dev/mapper/ro_redos-root: recovering journal
Clearing orphaned inode 423398 (uid=0, gid=0, mode=0100644, size=229605)
Clearing orphaned inode 172559 (uid=0, gid=0, mode=0100644, size=24992)
Clearing orphaned inode 387 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 386 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 384 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 296594 (uid=1000, gid=1000, mode=0100644, size=9059)
Setting free inodes count to 890417 (was 890569)
Setting free blocks count to 2578845 (was 2585477)
/dev/mapper/ro_redos-root: clean, 223695/1114112 files, 1876579/4455424 blocks
```

Получение сведений о процессах в РЕД ОС

Содержимое каталога /proc
Назначение файлов в каталогах процессов /proc/<PID>
Структура каталога /proc/sys

Процесс — это экземпляр запущенной программы. Каждый раз, когда в терминале выполняется какая-либо команда, система создает новый процесс. Процессы в операционной системе имеют числовой идентификатор, называемый **PID**.

Программы пространства пользователя в РЕД ОС не могут обращаться к ядру системы напрямую. Однако для получения информации от ядра были созданы некоторые специальные каталоги, с помощью которых любая программа или пользователь может получить данные о состоянии компьютера и ядра – это каталоги **/proc** и **/sys**.

Вы можете подробнее ознакомиться с назначением каталога **/proc** и файловой системы **procfs**, просмотрев наши обучающие видео:

- на **RuTube** — Файловая система procfs;
- в **Яндекс.Дзен** — Файловая система procfs.
- в **VK Видео** — Файловая система procfs.

На наших каналах вы также сможете найти много другой полезной информации.

С дополнительной информацией о работе с процессами можно ознакомиться в нашей статье «Процессы в РЕД ОС».

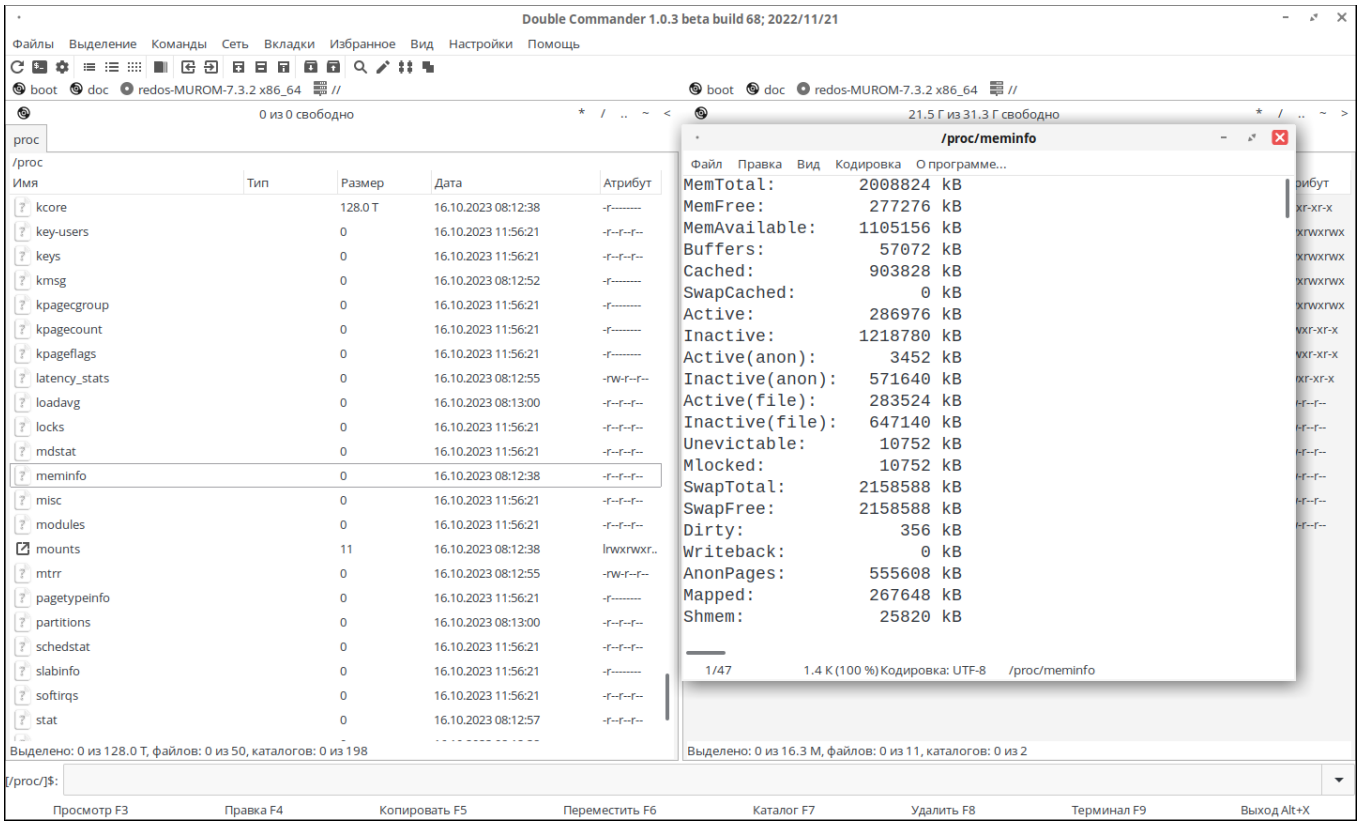
В рамках текущей статьи будет рассмотрен механизм получения сведений о процессах, на котором основаны все программы, позволяющие работать с процессами – работа с каталогом **/proc**.

В каталог **/proc** монтируется специальная файловая система **procfs**.

procfs — специальная файловая система, используемая в UNIX-подобных операционных системах, позволяющая получить доступ к информации из ядра о системных процессах, необходима для выполнения таких команд, как `ps`, `w`, `top`.

На самом деле каталог **/proc** – это не обычный каталог. Все подкаталоги, файлы и хранящаяся в них информация генерируются ядром «на лету», как только пользователь ее запрашивает. Работа построена таким образом, что пользователь может не заметить разницы между обычной файловой системой и **proc**, если откроет ее с помощью файлового менеджера.

Каталог **/proc** содержит файлы нулевого размера, у каждого файла отображается текущая дата создания. Например, файл **/proc/meminfo** будет содержать разные данные при каждом открытии, поскольку использование памяти постоянно изменяется.



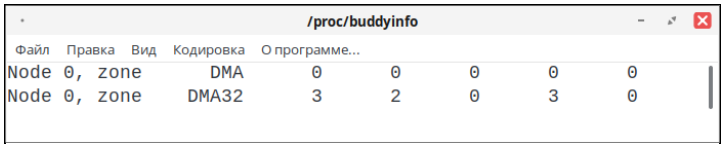
С помощью такого механизма разработчики придерживаются главной концепции Unix: «Всё – есть файл». Все файлы доступны для изменения любым редактором, и все они представлены в простом текстовом формате, но для того чтобы проанализировать весь

каталог, необходимы права суперпользователя (**root**).

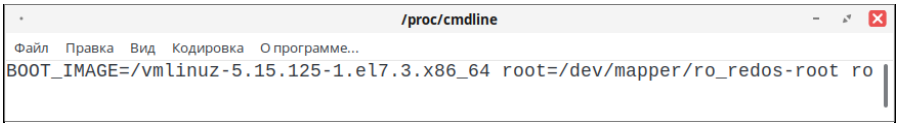
Большинство файлов в каталоге **/proc** доступны только для чтения, с их помощью можно только просмотреть информацию. Однако существуют и доступные для записи файлы, в частности – каталог **/proc/sys**, с помощью которого можно настраивать различные параметры ядра.

Содержимое каталога /proc

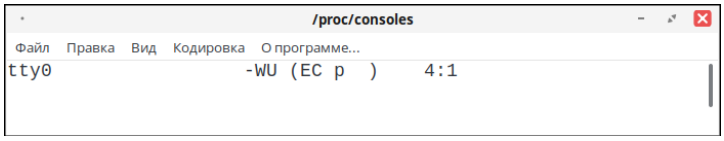
/proc/buddyinfo – файл отображает информацию о фрагментации памяти в ядре системы. Чаще всего используется для диагностики проблем с фрагментацией памяти.



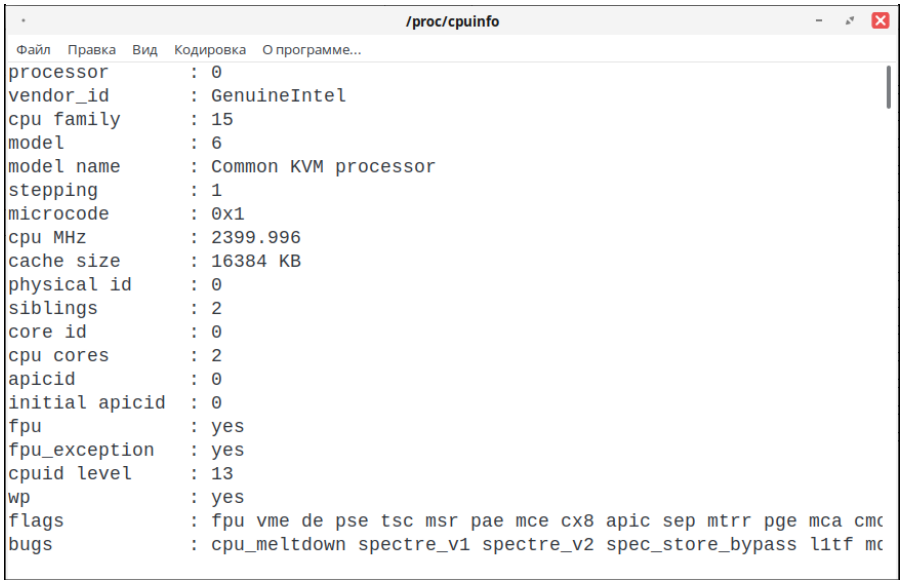
/proc/cmdline – файл отображает информацию о параметрах, которые были указаны в строке запуска ядра загрузчиком **grub**. Может быть полезно при поиске и устранении проблем с загрузкой ядра или в случае необходимости выявления файла, использованного для загрузки.



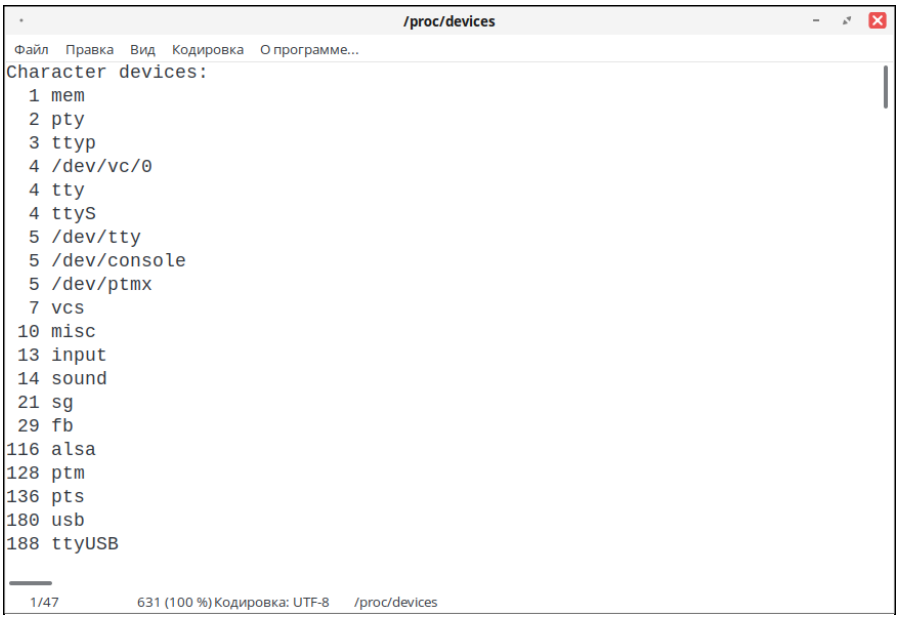
/proc/consoles – файл отображает информацию о зарегистрированных в ядре символических устройствах для системной консоли **/dev/console**.



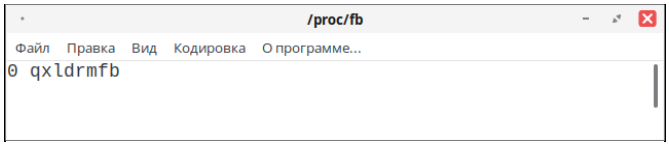
/proc/cpuinfo – файл отображает очень подробную информацию о процессоре. Здесь можно просмотреть производителя, количество ядер, объем кеша, активные ядра, частоту, поддерживаемые расширения и многое другое. Ту же информацию можно получить с помощью специальных команд, однако все скрипты, выводящие информацию о процессоре, берут ее из каталога **/proc**.



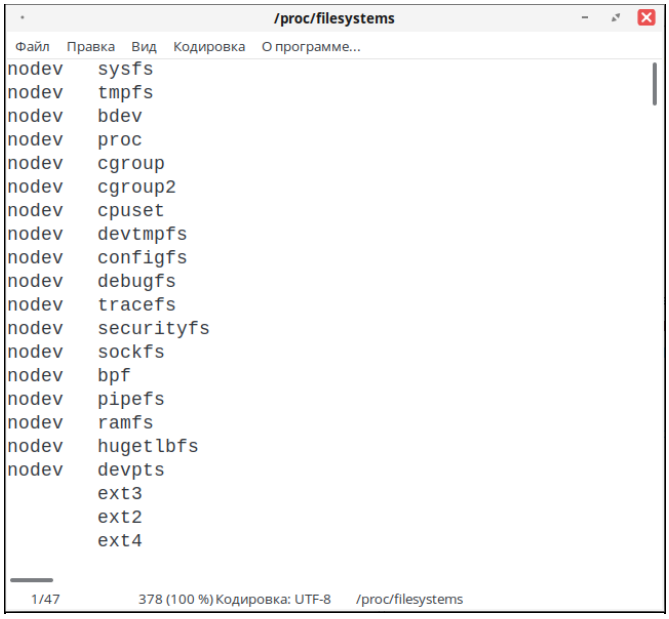
/proc/devices – файл отображает информацию о различных блочных и символических устройствах, подключенных к системе, кроме тех, для которых не загружены модули ядра. Устройства разделены на *символические* и *блочные*. У символических устройств нет буфера хранения, поэтому они отправляют ядру данные определенного размера. Блочные устройства имеют буфер для данных и предназначены для сохранения информации, например, на жесткие диски.



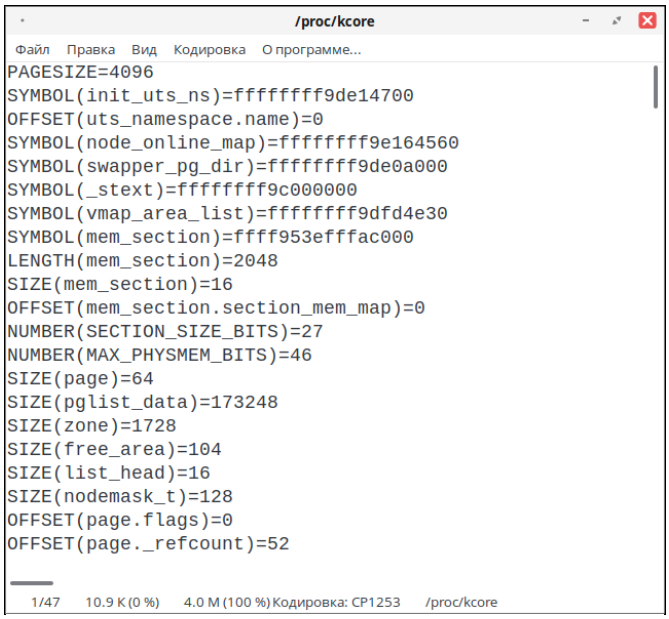
/proc/fb – файл отображает информацию об устройствах фреймбуфера (экраны), а также используемые графические драйверы. Файл является одним из способов просмотра используемого драйвера видеокарты.



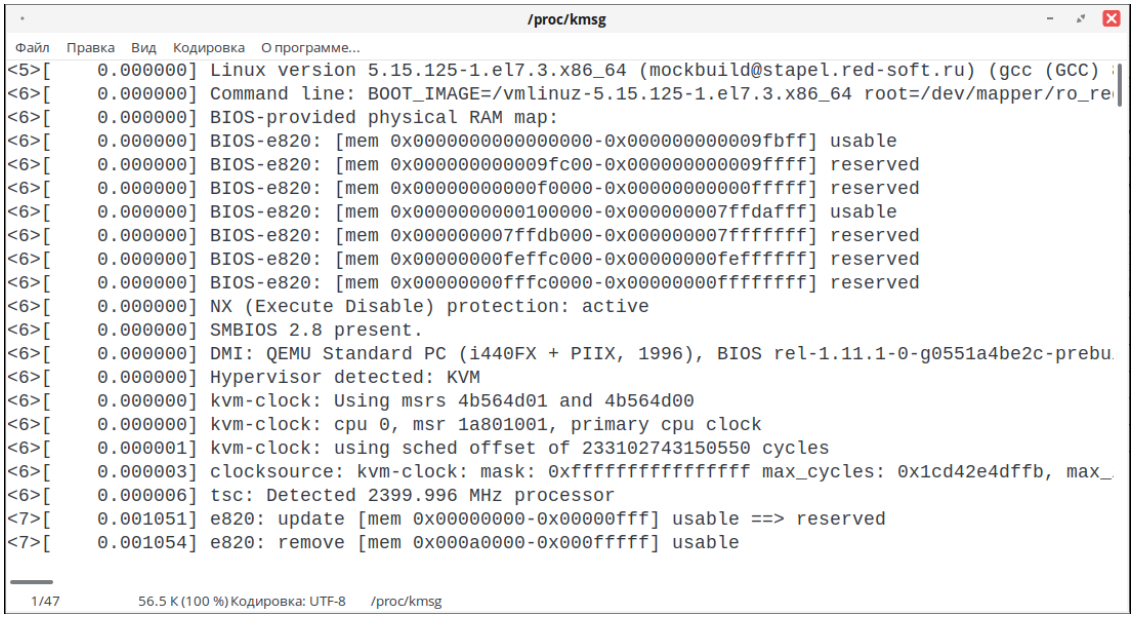
/proc/filesystems – файл содержит список файловых систем, которые на данный момент поддерживаются ядром. Значение **nodev** показывает, что это файловая система специального назначения, и она не используется для хранения данных на носителях.



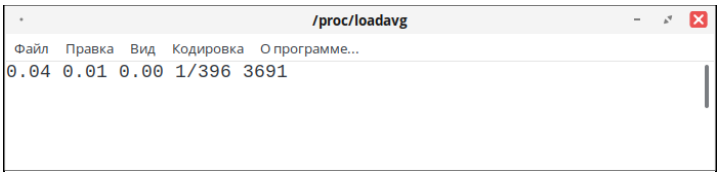
/proc/kcore – это все содержимое оперативной памяти, представленное в одном файле. В отличие от других у этого файла есть размер – объем ОЗУ плюс 4 Кб. Для доступа к файлу необходимы права суперпользователя (**root**). Перед работой с файлом его необходимо скопировать в другой каталог, а затем выполнять требуемые действия.



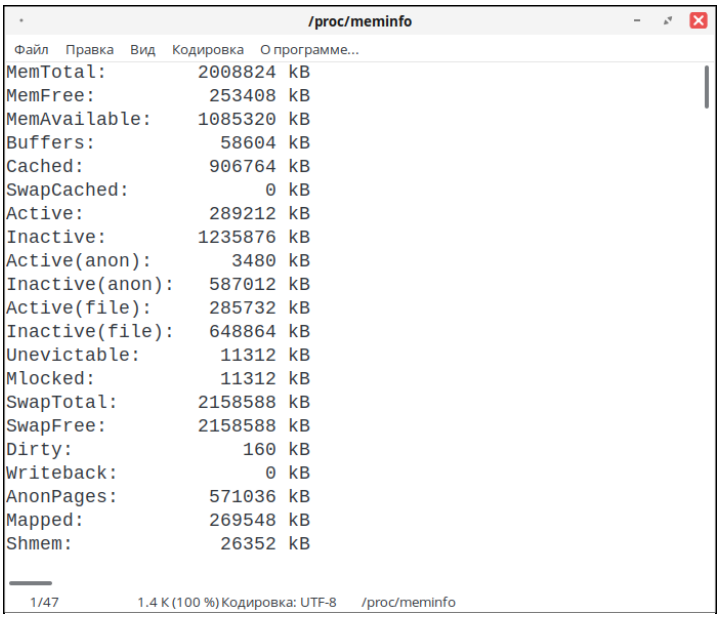
/proc/kmsg – файл накапливает и сохраняет сообщения ядра. Сообщения можно посмотреть также с помощью утилиты **dmesg**. Для доступа к файлу потребуются права суперпользователя (**root**).



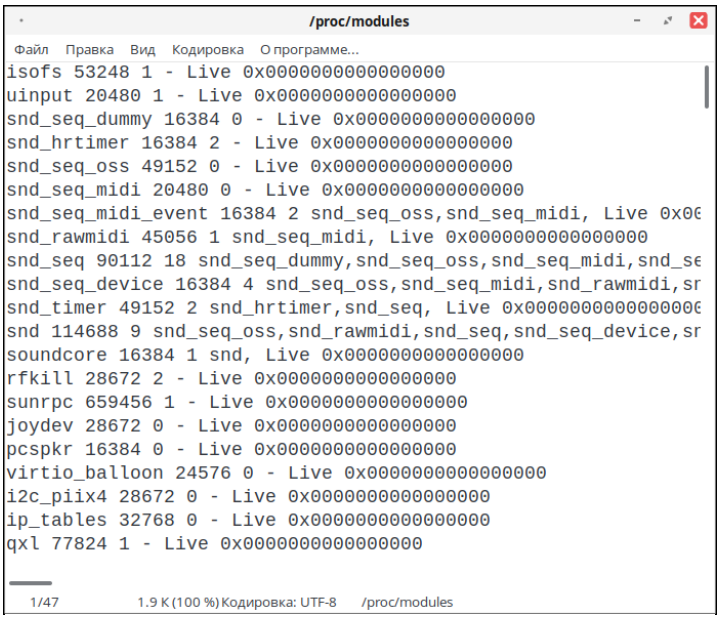
/proc/loadavg – файл позволяет оценить среднюю нагрузку на систему. Первые три цифры показывают нагрузку на процессор в данный момент времени, 5 минут назад и 15 минут назад, следующие два столбца показывают количество активных процессов и общее количество запущенных процессов. Последняя цифра — это идентификатор последнего процесса (**PID**).



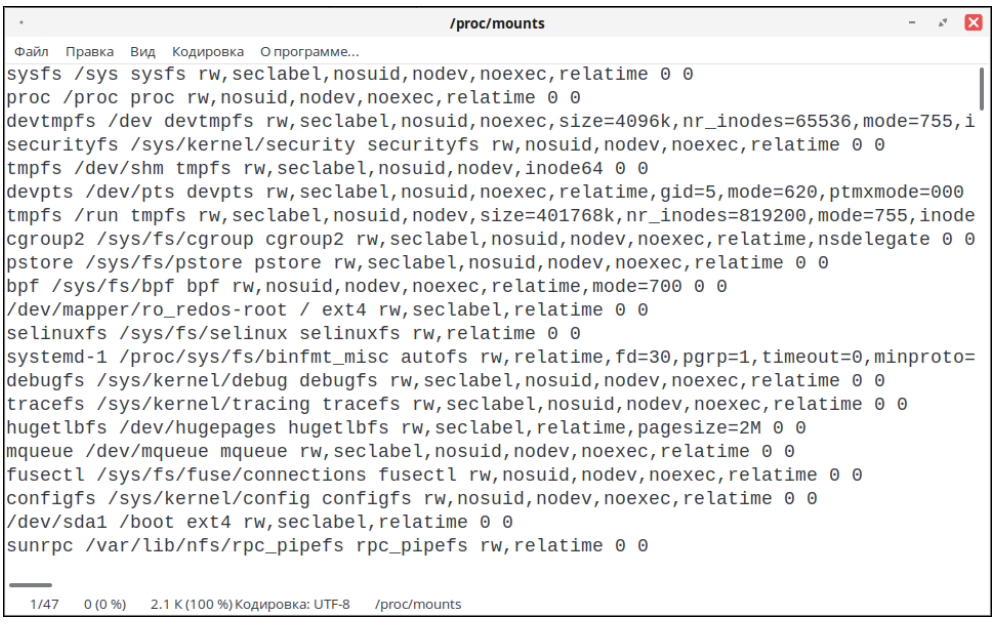
/proc/meminfo – файл отображает всю доступную информацию об оперативной памяти и пространстве подкачки.



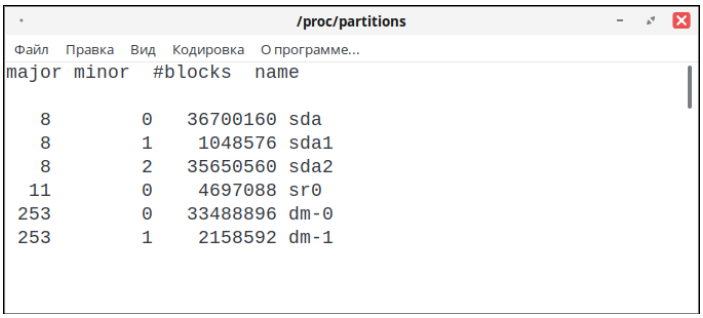
/proc/modules – файл содержит список всех загруженных модулей ядра. Ту же информацию можно увидеть, выполнив команду **lsmod**.



/proc/mounts – файл содержит все точки монтирования и все подключенные файловые системы.



/proc/partitions – в файле отображены все подключенные к системе разделы жестких дисков или других запоминающих устройств.



Назначение файлов в каталогах процессов /proc/<PID>

Для отображения файлов какого-либо процесса следует открыть каталог с номером необходимого процесса. В каждом каталоге более 50 файлов.

Далее будет рассмотрено назначение некоторых файлов:

- **cmdline** – содержит команду, с помощью которой был запущен процесс, а также переданные ей параметры;
- **cwd** – символическая ссылка на текущий рабочий каталог процесса;
- **exe** – ссылка на исполняемый файл;
- **root** – ссылка на каталог суперпользователя (**root**);
- **environ** – переменные окружения, доступные для процесса;
- **fd** – содержит файловые дескрипторы, файлы и устройства, которые использует процесс;
- **maps**, **statm**, и **mem** – информация о памяти процесса;
- **stat**, **status** – состояние процесса.

Структура каталога /proc/sys

Каталог **/proc/sys** содержит файлы с параметрами ядра. Файлы доступны не только для чтения, но и для редактирования с целью передачи ядру ОС новых значений параметров.

Каталог содержит подкаталоги, разделённые по типам хранимых параметров. Далее будет рассмотрено назначение некоторых файлов:

- **debug** – содержит отладочную информацию, она будет полезна для разработчиков ядра;
- **dev** – содержит параметры различных устройств, подключенных к системе;
- **fs** – содержит всю информацию о файловой системе;
- **kernel** – позволяет напрямую настраивать ядро;
- **net** – позволяет настраивать различные параметры сети;
- **vm** – содержит ряд файлов и подкаталогов, соответствующих переменным ядра с подсистемой виртуальной памяти.

Более подробную информацию о каталоге **/proc** также можно просмотреть, выполнив команду:

```
man proc
```

Изменение приоритета процесса

Изменение приоритетов процессов с помощью терминала
Изменение приоритетов процессов с помощью графических средств

Изменение приоритетов процессов с помощью терминала

Утилита nice — программа, предназначенная для запуска процессов с изменённым приоритетом nice. Приоритет nice (целое число) процесса используется планировщиком процессов ядра ОС при распределении процессорного времени между процессами

Приоритет nice — число, указывающее планировщику процессов ядра ОС приоритет, который пользователь хотел бы назначить процессу.

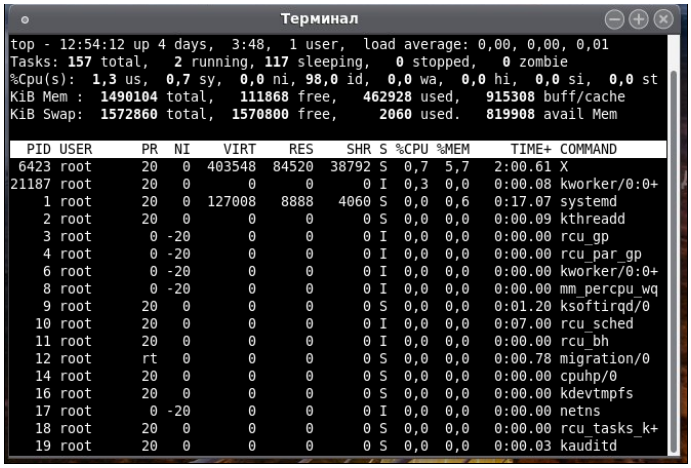
Утилита nice, запущенная без аргументов, выводит приоритет nice, унаследованный от родительского процесса. nice принимает аргумент «смещение» в диапазоне от -20 (наивысший приоритет) до +19 (низший приоритет). Если указать смещение и путь к исполняемому файлу, утилита nice получит приоритет своего процесса, изменит его на указанное смещение и использует системный вызов семейства exec() для замещения кода своего процесса кодом из указанного исполняемого файла. Команда nice сделает то же, но сначала выполнит системный вызов семейства fork() для запуска дочернего процесса (англ. sub-shell). Если смещение не указано, будет использовано смещение +10. Привилегированный пользователь (root) может указать отрицательное смещение.

Приоритет nice и приоритет планировщика процессов ядра ОС — разные числа. Число nice — приоритет, который пользователь хотел бы назначить процессу. Приоритет планировщика — действительный приоритет, назначенный процессу планировщиком. Планировщик может стремиться назначить процессу приоритет, близкий к nice, но это не всегда возможно, так как в системе может выполняться множество процессов с разными приоритетами. Приоритет nice является атрибутом процесса и, как и другие атрибуты, наследуется дочерними процессами. В выводе утилит top, ps, htop и др. приоритет nice называется «NI» — сокращение от «nice», а приоритет планировщика — «PRI» — сокращение от «priority». Обычно, NI = PRI - 20, но это верно не всегда. По умолчанию NI=0, соответственно PRI=20.

Планировщик процессов ядра ОС Linux поддерживает приоритеты от 0 (реальное время) до 139 включительно. Приоритеты -20...+19 утилиты или команды nice соответствуют приоритетам 100...139 планировщика процессов. Другие приоритеты планировщика процессов можно установить командой chrt из пакета util-linux.

Посмотреть приоритет процессов можно например с помощью утилиты **top**, для этого в терминале нужно выполнить:

```
top
```



Для просмотра приоритета уже запущенного конкретного процесса существует команда:

```
ps -o pid,comm,nice -C [name]
```

Например:

```
ps -o pid,comm,nice -C top

PID COMMAND NI
21244 top 0
```

nice

Синтаксис:

```
nice [-n смещение] [--adjustment=смещение] [команда [аргумент...]]
```

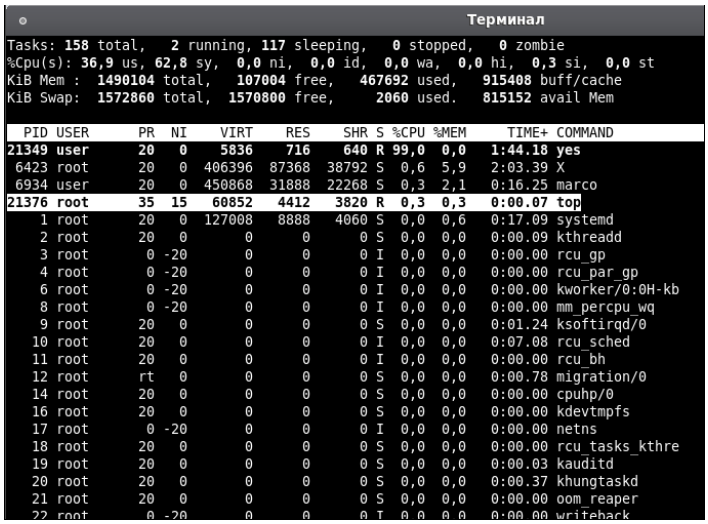
Параметры:

```
-n <смещение>
--adjustment=<смещение>
```

Установить приоритет nice, равный сумме текущего приоритета nice и указанного числа «смещение». Если этот аргумент не указан, будет использовано число 10.

Для примера зададим приоритет 15 при старте процесса top:

```
nice -n 15 top
```



Чтобы установить значение nice ниже нуля, требуются права суперпользователя. В противном случае будет установлено значение 0. Попробуем задать значение nice -1 без прав root:

```
nice -n -1 yes > /dev/null &nice: cannot set niceness: Permission denied
```

Поэтому, чтобы задать значение nice меньше 0, необходимо запускать программу как root, или использовать sudo.

renice

Для того, чтобы изменить приоритет у существующего процесса (т.е. такого процесса, который ранее был уже запущен), необходимо воспользоваться командой:

```
renice [значение приоритета] -p [id процесса]
```

У запущенной программы с помощью команды renice можно изменить назначенный приоритет. Предположим, что есть работающая программа yes со значением nice 10. Чтобы изменить его значение, можно использовать команду renice со значением nice и PID процесса. Изменим значение nice на 15:

```
renice -n 15 -p 21349
21349 (process ID) old priority 0, new priority 15
```

Согласно правилам, обычный пользователь может только увеличивать значение nice (уменьшать приоритет) любого процесса. Если попробовать изменить значение nice с 15 до 10, мы получим следующее сообщение об ошибке:

```
renice -n 10 -p 21349
renice: failed to set priority for 5645 (process ID): Permission denied
```

Также, команда renice позволяет суперпользователю изменять значение nice процессов любого пользователя. Это делается с помощью ключа -u. Следующая команда изменяет значение приоритета всех процессов пользователя на -19:

```
renice -n -19 -u lubos
1000 (user ID) old priority 0, new priority -19
```

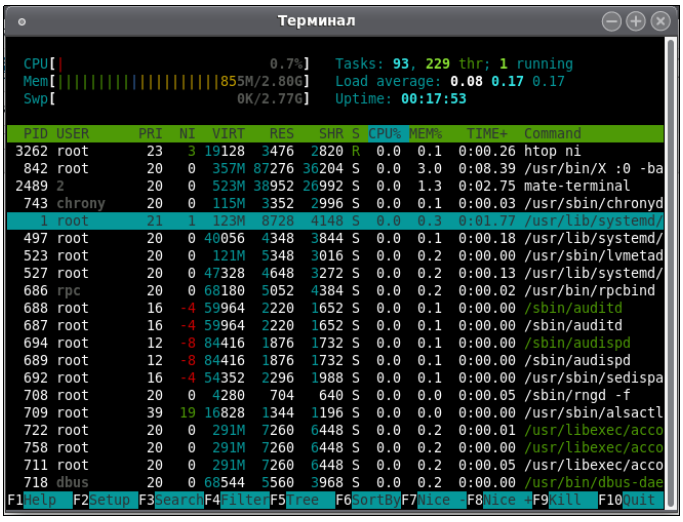
htop

htop представляет собой продвинутый монитор процессов, аналог **top.** В отличие от top, htop показывает все процессы в системе. Также показывает время непрерывной работы, использование процессоров и памяти. htop часто применяется в тех случаях, когда информации даваемой утилитой top недостаточно, например при поиске утечек памяти в процессах. htop написан на языке Си и использует для отображения библиотеку Ncurses.

Устанавливается командой:

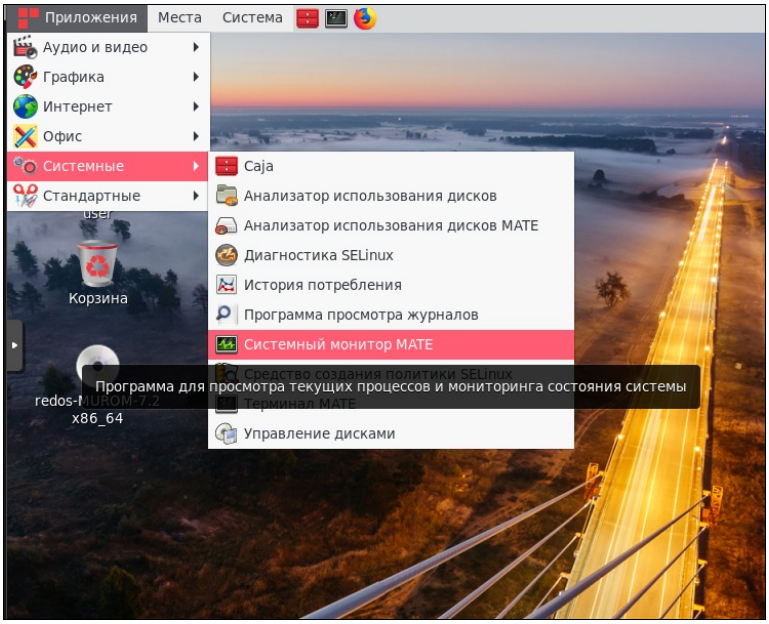
```
dnf install htop
```

На нижней панели интерфейса отображены основные действия. Переключаться межуд процессами можно кнопками «Вверх» и «Вниз». При нажатии F7 и F8 на выбранном процессе изменяется приоритет вниз и вверх соответственно.



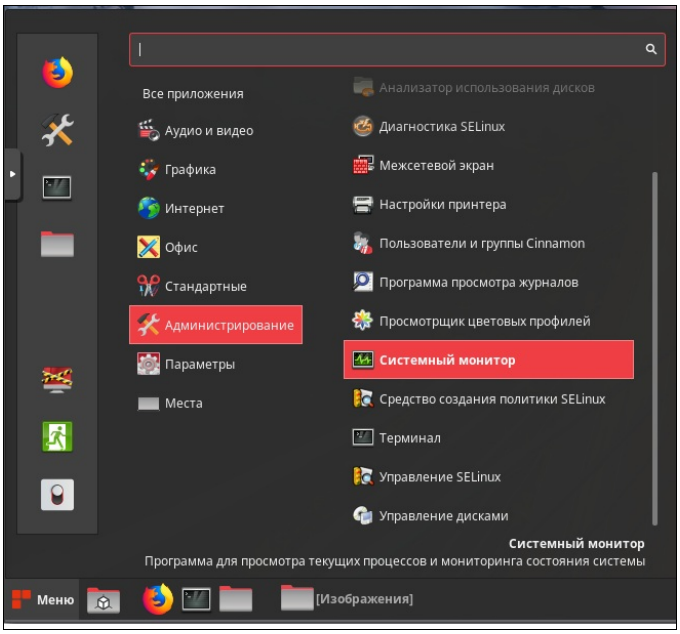
Изменение приоритетов процессов с помощью графических средств

Изменять приоритеты процессов можно с помощью утилиты **Системный монитор**.

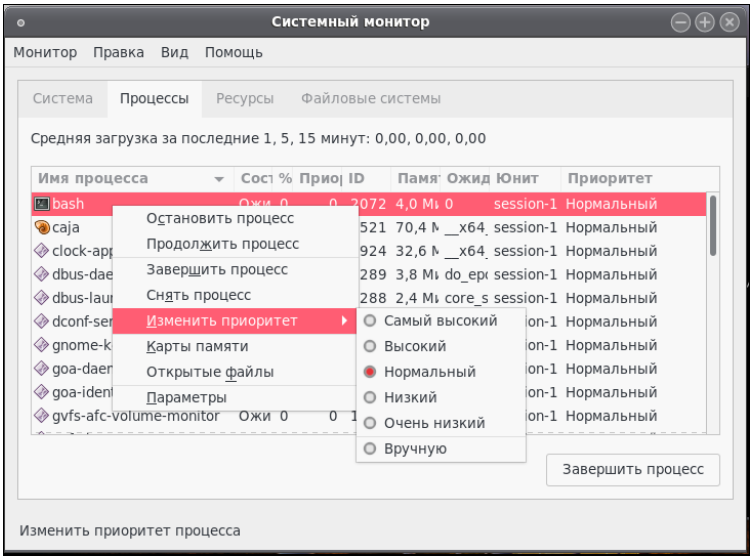


Для Cinnamon необходимо установить отдельно:

```
dnf install gnome-system-monitor.x86_64
```



Перейдите на вкладку Процессы. Выберите процесс, щелкните правой кнопкой мыши по нему и выберите в выпадающем меню пункт Изменить приоритет. Выберите нужный приоритет и выберите его.



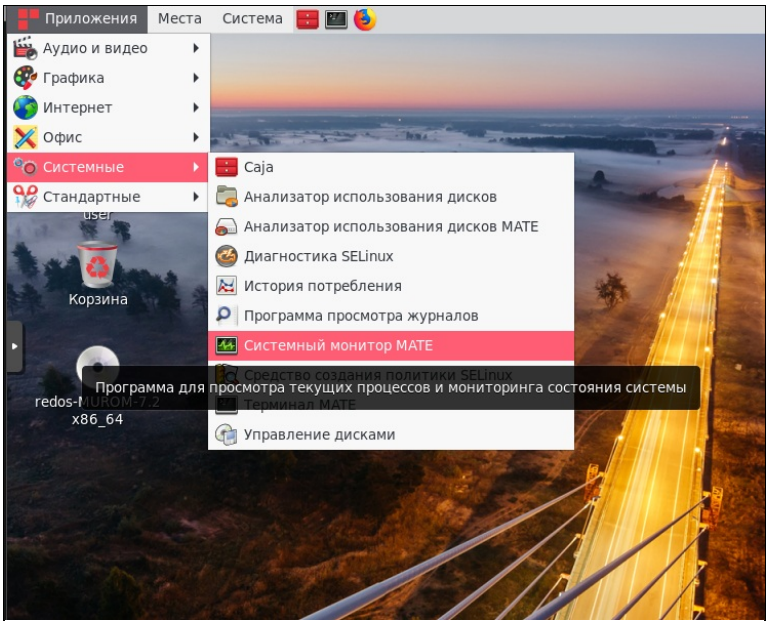
Системный монитор

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

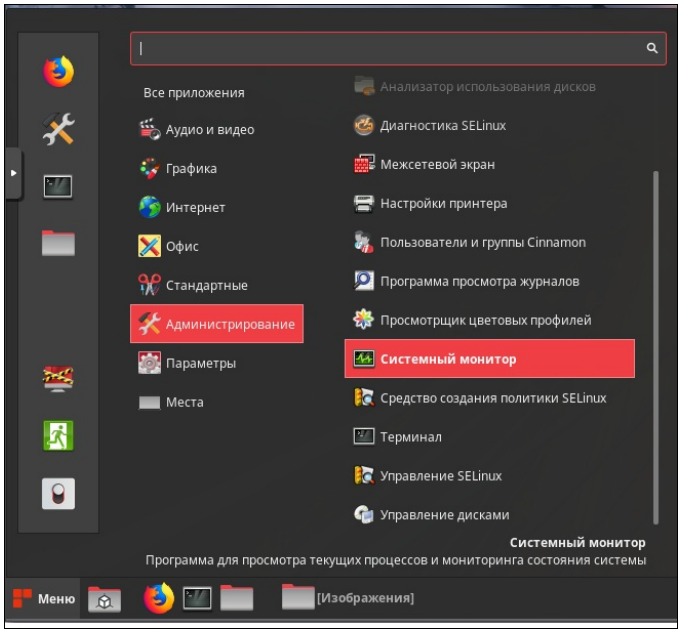
Утилита «**Системный монитор**» - аналогия диспетчера задач в Windows.



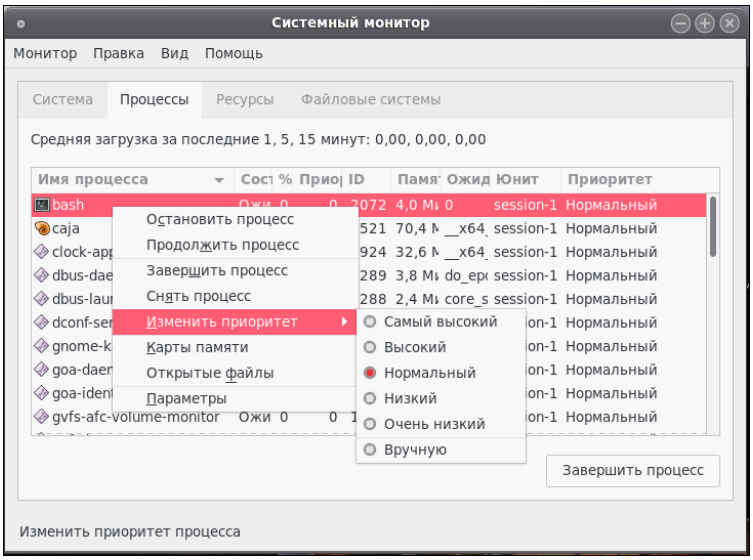
Для **Cinnamon** необходимо установить отдельно:

```
sudo dnf install gnome-system-monitor
```

Расположение утилиты в **Cinnamon**:



Графический интерфейс утилиты интуитивно понятен, вся информация распределена по четырем вкладкам (Cinamon — 3 вкладки). Выглядит следующим образом:



Вкладка **«Система»** - выводится базовая минимальная информация о системе.

Вкладка **«Процессы»** - можно просматривать и управлять, работающими процессами. Каждый процесс можно приостановить, остановить, изменить приоритет.

Вкладка **«Ресурсы»** - утилита выводит в виде графиков информацию в реальном времени о ресурсах использования процессора, использование оперативной памяти и файла подкачки, и использование сети.

Вкладка **«Файловые системы»** - отображает информацию о имеющихся устройствах хранения информации.

top

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер минимальный, Сервер графический

top — утилита, с помощью которой можно вывести список работающих в системе процессов и информацию о них. Данная утилита установлена в РЕД ОС по умолчанию.

С утилитой **top** вы можете подробнее ознакомиться, просмотрев наши обучающие видео:

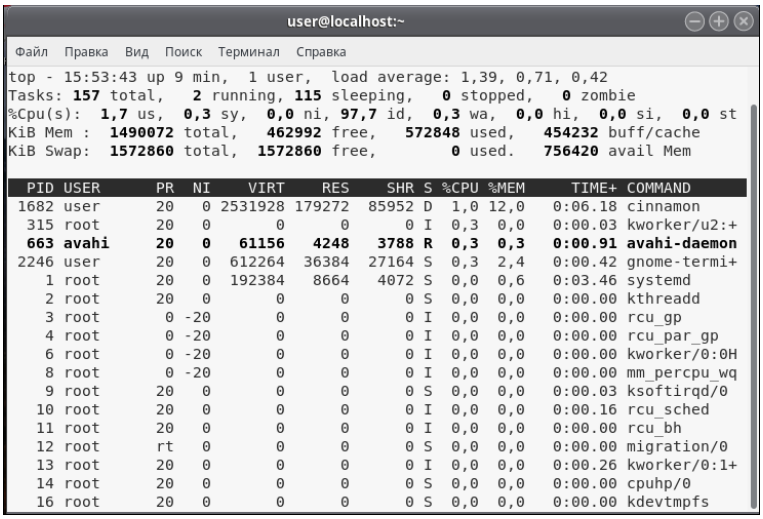
- на **RuTube** — Утилита мониторинга процессов top;
- в **Яндекс.Дзен** — Утилита мониторинга процессов top;
- в **VK Видео** — Утилита мониторинга процессов top.

На наших каналах вы также сможете найти много другой полезной информации.

Для запуска утилиты необходимо в терминале выполнить команду (с правами обычного **непривилегированного** пользователя):

```
top
```

После запуска в терминале можно увидеть вывод, примерно следующего содержания:



Где первая строка:

- текущее время (**15:53:43**);
- время работы системы (**up 9 min**);
- количество открытых пользовательских сессий (**1 users**);
- среднюю загрузку системы (**load average: 1.39, 0.71, 0.42**).

Вторая строка:

- общее количество процессов в системе (**157 total**);
- количество работающих в данный момент процессов (**2 running**);
- количество ожидающих событий процессов (**115 sleeping**);
- количество остановленных процессов (**0 stopped**);
- количество процессов, ожидающих родительский процесс для передачи статуса завершения (**0 zombie**).

Третья строка выводит информацию о работе процессора:

- использование центрального процессора (в процентах) пользовательскими процессам (**1.7 us**);
- использование центрального процессора (в процентах) системными процессами (**0.3 sy**);
- использование центрального процессора (в процентах) процессами с приоритетом, повышенным при помощи вызова nice (0.0 ni);
- время (в процентах), когда центральный процессор не используется (**97,7 id**);
- использование центрального процессора (в процентах) процессами, ожидающими завершения операций ввода-вывода (**0.3 wa**);
- использование центрального процессора (в процентах) обработчиками аппаратных прерываний (**0.0 hi - Hardware IRQ** (аппаратные прерывания));
- использование центрального процессора (в процентах) обработчиками программных прерываний (**0.0 si - Software Interrupts** (программные прерывания));
- количество ресурсов центрального процессора "заимствованных" у виртуальной машины гипервизором для других задач (таких, как запуск другой виртуальной машины), это значение будет равно нулю на настольных компьютерах и серверах, не

использующих виртуальные машины (**0.0 st - Steal Time** (заимствованное время)).

Четвертая и пятая строка показывает информацию об использовании физической оперативной памяти и раздела подкачки (swap):

- общее количество памяти (в килобайтах);
- количество используемой памяти (в килобайтах);
- количество свободной памяти (в килобайтах);
- количество памяти в кэше буферов (в килобайтах).

Далее идет список процессов, отсортированных по величине использования центрального процессора:

- **PID** – идентификатор процесса;
- **USER** - имя пользователя, который является владельцем процесса;
- **PR** - приоритет процесса;
- **NI** - значение "NICE", влияющие на приоритет процесса;
- **VIRT** - объем виртуальной памяти, используемый процессом;
- **RES** - объем физической памяти, используемый процессом;
- **SHR** - объем разделяемой памяти процесса;
- **S** - указывает на статус процесса:
  - S=sleep (ожидает событий);
  - R=running (работает);
  - Z=zombie (ожидает родительский процесс);

- **%CPU** - процент использования центрального процессора данным процессом;
- **%MEM** - процент использования оперативной памяти данным процессом;
- **TIME+** - общее время активности процесса;
- **COMMAND** - имя процесса.

Далее приведено описание наиболее часто используемых интерактивных команд, которые вы можете выполнять во время работы программы:

- **h** - вывод справки по утилите;
- **q (Ctrl+C)** - выход из **top**;
- **A** - выбор цветовой схемы;
- **d** или **s** - изменить интервал обновления информации;
- **H** - выводить потоки процессов;
- **k** - послать сигнал завершения процессу;
- **W** - записать текущие настройки программы в конфигурационный файл;
- **Y** - посмотреть дополнительные сведения о процессе, открытые файлы, порты, логи и т д;
- **Z** - изменить цветовую схему;
- **l** - скрыть или вывести информацию о средней нагрузке на систему;
- **m** - выключить или переключить режим отображения информации о памяти;
- **x** - выделять жирным колонку, по которой выполняется сортировка;
- **y** - выделять жирным процессы, которые выполняются в данный момент;
- **z** - переключение между цветным и одноцветным режимами;
- **c** - переключение режима вывода команды, доступен полный путь и только команда;
- **F** - настройка полей с информацией о процессах;
- **o** - фильтрация процессов по произвольному условию;
- **u** - фильтрация процессов по имени пользователя;
- **V** - отображение процессов в виде дерева;
- **i** - переключение режима отображения процессов, которые сейчас не используют ресурсы процессора;
- **n** - максимальное количество процессов, для отображения в программе;
- **L** - поиск по слову;
- **<>** - перемещение поля сортировки вправо и влево;
- **t** - по кругу переключает вид строки обобщённой информации об использовании процессора.

Примечание.

Обратите внимание, что для использования интерактивных команд, обозначаемых заглавными буквами (A, H, W, Y, Z и т.д.), необходимо одновременно нажимать клавишу *Shift* и соответствующую букву. Например, для выполнения интерактивной команды **A** следует использовать сочетание *Shift+a*.

Для получения более подробной справки необходимо нажать клавишу «**h**» во время работы утилиты.

Использование top в пакетном режиме

Утилита **top** также поддерживает использование опций командной строки. Большинство из этих опций соответствуют рассмотренным выше интерактивным командам — для их использования перед буквой требуется поставить дефис.

Также утилита **top** может использоваться в пакетном режиме. Для запуска утилиты в пакетном режиме применяется опция `-b`. Данный

режим полезен для отправки выходных данных утилиты в другую программу или в файл. В пакетном режиме утилита **top** не принимает ввод и работает до достижения заданного опцией `-n` предела повторений. Например, запуск команды **top** в пакетном режиме с одним обновлением информации будет выглядеть следующим образом:

```
top -b -n 1
```

Для сохранения результатов команды **top** в файл в *текущей директории* используйте следующую команду:

```
top -n 1 -b > top-output.txt
```

htop

Установка
Работа с утилитой
Горячие клавиши htop

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер минимальный, Сервер графический.
- **Версия ПО**: htop-3.3.0-1

htop — утилита командной строки, позволяющая пользователю интерактивно отслеживать жизненно важные ресурсы системы или процессы в режиме реального времени. **htop** поддерживает работу с мышью, использует цвет в своих выходных данных и дает визуальные указания об использовании процессора.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Основные параметры:

- `-d`, `--delay=<число>` – задержка между обновлениями в секундах;
- `-C`, `--no-color`, `--no-colour` – запуск в монохромном режиме;
- `--directory=<путь_к_каталогу>` – директория, используемая для тестирования **I/O**;
- `-h`, `--help` – вывод справки;
- `-p`, `--pid=<PID>,<PID>...` – отображение только процессов с указанными **PID**;
- `-s`, `--sort-key` – сортировка таблицу по указанному столбцу;
- `-u`, --user=<имя_пользователя> – отображение только процессов заданного пользователя;
- `-v`, `--version` – вывод версии утилиты;
- `-t`, `--tree` – отображение процессов в виде дерева.

Установка

Установка утилиты выполняется командой (потребуются права **администратора**):

```
sudo dnf install htop
```

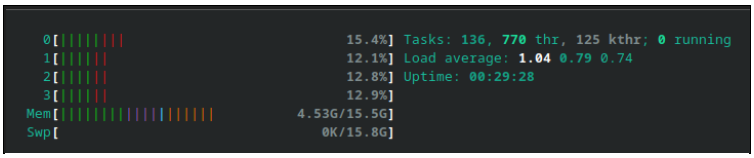
Работа с утилитой

Для запуска утилиты используется команда (с правами обычного **непривилегированного** пользователя):

```
htop
```

Общая информация

При запуске утилиты выводится общая информация о загруженности системы:

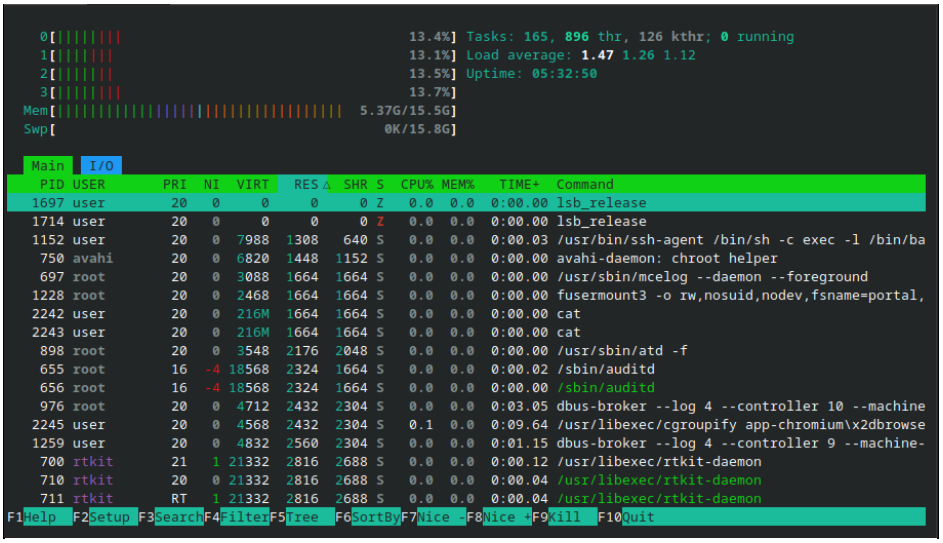


где:

- 0, 1, 2, 3 ... – нагрузка на каждое ядро процессора;
- Mem – используемая оперативная память и её общий объем;
- Swp – уровень заполненности раздела подкачки;
- Tasks/running – количество процессов и сколько из них активны;
- Load average – средняя загрузка системы за последние 1, 5, 15 минут;
- Uptime – время непрерывной работы системы.

Таблица main

На вкладке **main** выводится информация о запущенных процессах:



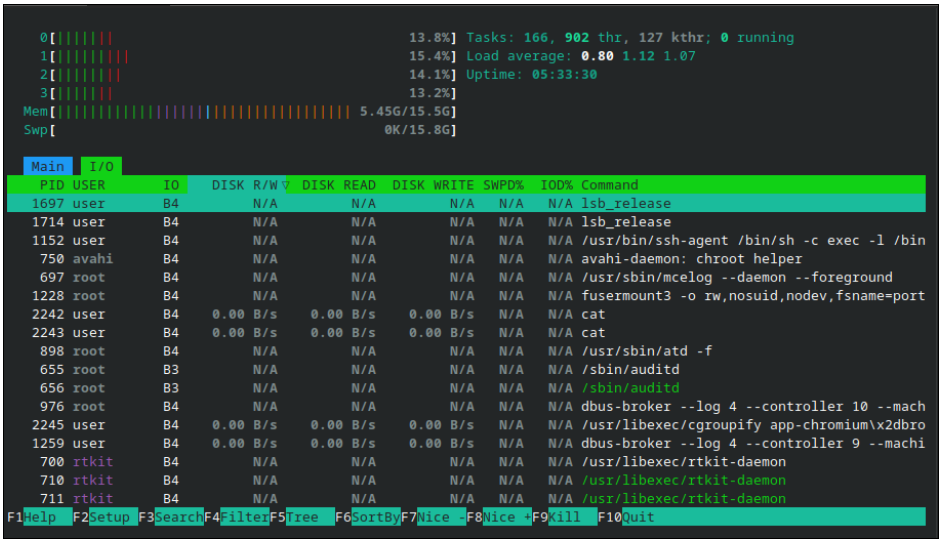
где:

- PID – уникальный идентификатор процесса;
- User – владелец процесса;
- PRI – приоритет в пространстве ядра;
- NI – приоритет процесса в пространстве пользователя (-20 самый высокий приоритет, 19 – самый низкий);
- VIRT – общее количество виртуальной памяти, занимаемое процессом;
- RES – физическая память, используемая процессом;
- SHR – объём памяти, который может быть использован совместно с другими процессами;
- S – состояние процесса:
  - R – процесс готов к выполнению и ожидает выделения процессорного времени;
  - S – процесс находится в состоянии сна, ожидая события (например, завершения ввода-вывода, сигнала таймера или другого процесса);
  - D – процесс находится в состоянии сна, ожидая ввода-вывода с диска;
  - Z – процесс завершился, но его запись в таблице процессов существует, пока родительский процесс не получит информацию о завершении;
  - T – процесс остановлен с помощью сигнала;
  - t – процесс остановлен для отладки (трассировки);
  - X – процесс завершился и его запись удалена из таблицы процессов;
  - W – процесс ожидает подкачки данных в RAM;

- CPU% – процент процессорного времени, который процесс использует в данный момент;
- MEM% – процент оперативной памяти, который процесс использует в данный момент;
- TIME+ – задержки ввода-вывода для достижения заданной цели;
- Command – имя выполняемой программы и аргументы.

Таблица I/O

На вкладке **I/O** отображаются данные о выполняемых операциях ввода/вывода:



где:

- IO – класс планирования ввода-вывода, за которым следует приоритет, если класс его поддерживает:
  - R – класс реального времени; процессам этого класса первым предоставляется доступ к диску;
  - B – класс планирования; процессы этого класса получают доступ к диску в порядке приоритета;
  - id – класс простоя; процессы этого класса получают доступ к диску только когда его не используют другие процессы;
- DISK R/W – сумма скорости ввода-вывода для чтения и для записи;
- DISK READ – скорость ввода-вывода для данного процесса при чтении;
- DISK WRITE – скорость ввода-вывода для данного процесса при записи;
- SWPD% – процент времени, затраченного на подкачку страниц;
- IOD% – процент времени, затраченного на ожидание завершения синхронного блочного ввода-вывода.

Горячие клавиши htop

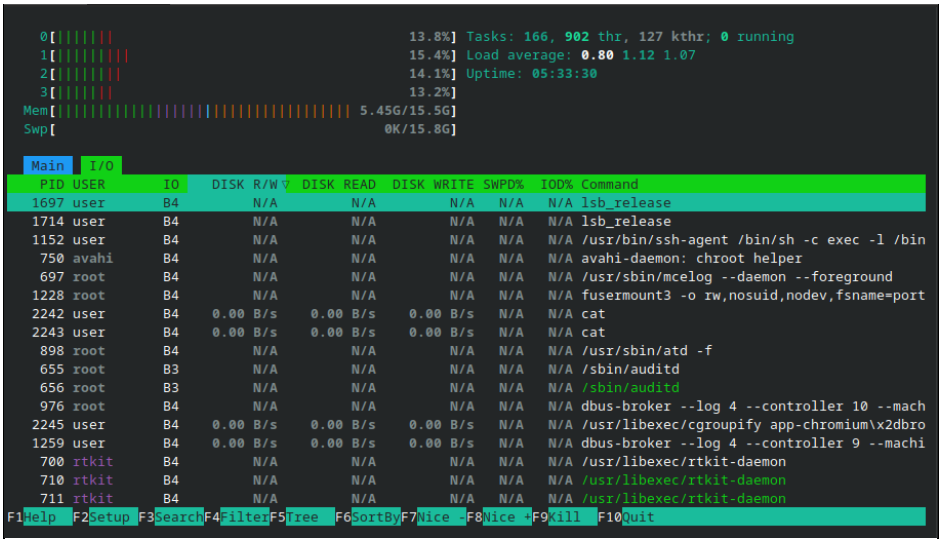
Клавиши навигации и выделения процессов

Для навигации и выбора нужных процессов используются следующие клавиши:

- курсорные клавиши (←, →, ↑, ↓) – прокрутка списка процессов;
- **PgUp**, **PgDn** – прокрутка списка вверх и вниз;
- **Home** – прокрутка к началу списка;
- **End** – прокрутка к концу списка;
- **Ctrl-a**, **^** – прокрутка к началу строки;
- **Ctrl-e**, **$** – прокрутка к концу строки;
- **Пробел** – выбор нескольких процессов. После этого введённые команды, такие как **kill (f9)** или изменение приоритета, будут применяться к группе выделенных процессов вместо подсвеченного в данный момент;
- **Shift-u** – снятие выделения со всех процессов;
- **l** – вывод файлов, открытых выделенным процессом. Для работы этой функции должна быть установлена утилита **lsof**.

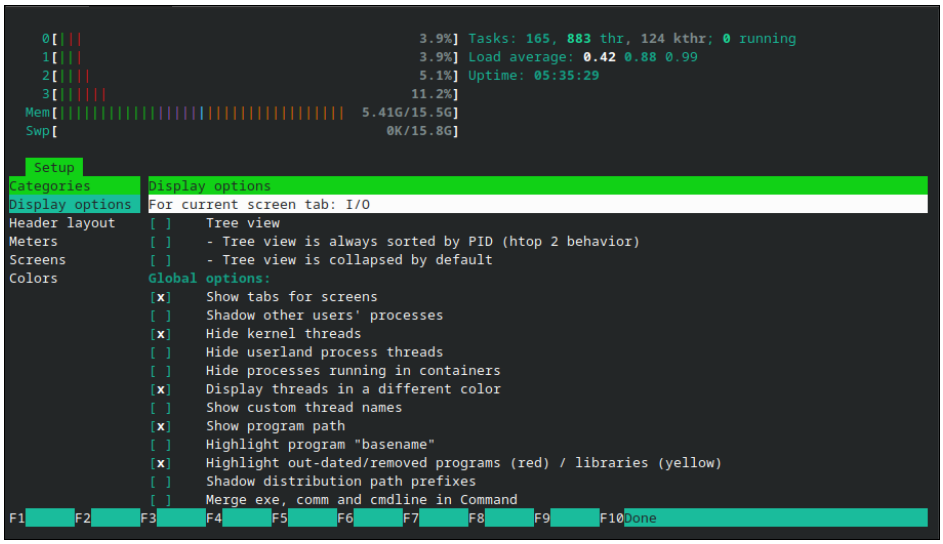
F1 Help

Выводит на экран сообщение помощи:



F2 Setup

Открывает экран настройки утилиты, в котором можно сконфигурировать счетчики, отображаемые в верхней части экрана – настройки отображения, выбор цветовой палитры, столбцы и их порядок.



F3 Search

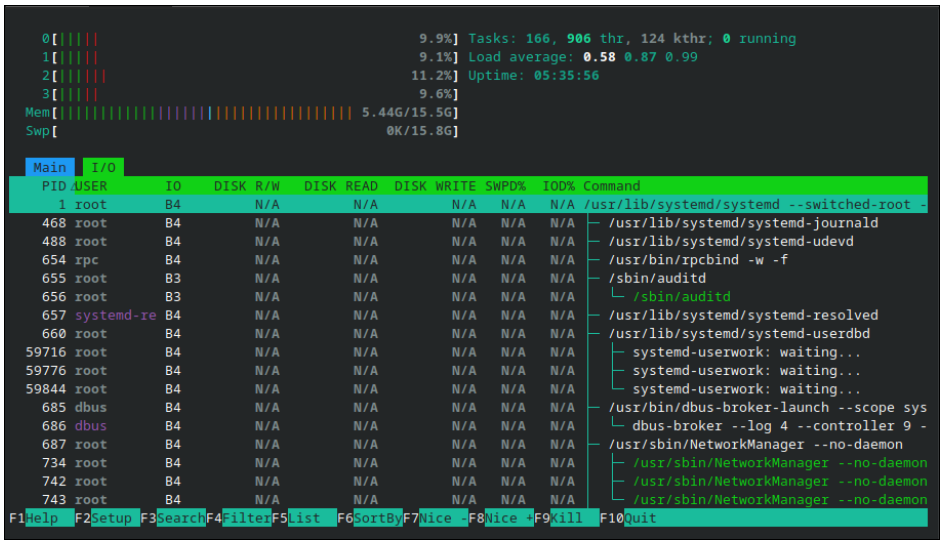
Поэтапный поиск в командах всех отображаемых процессов. Выбранная в данный момент (выделенная) команда будет обновляться по мере ввода. В режиме поиска нажатие клавиши **F3** приведет к цикличному просмотру подходящих процессов.

F4 Filter

Фильтрация процессов. Будут отображены только те процессы, названия которых содержат указанный фрагмент.

F5 Tree

Отображение процессов в виде дерева. При запуске нового процесса, процесс, который его запускает, принято называть *родительским* или просто *родителем*. Таким образом, новый процесс – это дочерний процесс родительского. Эти отношения образуют структуру в виде дерева.



F6 SortBy

Сортировка процессов по выбранному столбцу таблицы.

F7 Nice – и F8 Nice +

Увеличивает и уменьшает приоритет процесса.

F9 Kill

Системный вызов, который может послать сигнал процессу**.** Работает аналогично команде **kill**.

F10 Quit

Выход из утилиты.

atop

atop — интерактивный полноэкранный монитор производительности. Является аналогом **top**, но в отличие от него выводит только новые изменения об активных системных процессах. Основным преимуществом утилиты **atop** является функция ведения логов.

В состав пакета входит утилита **atopsar** — встроенный анализатор логов **atop**, который позволяет быстро найти проблему и просмотреть лог за определенный промежуток времени. Подробнее об утилите **atopsar** см. в нашей статье «atopsar — встроенный анализатор логов atop».

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

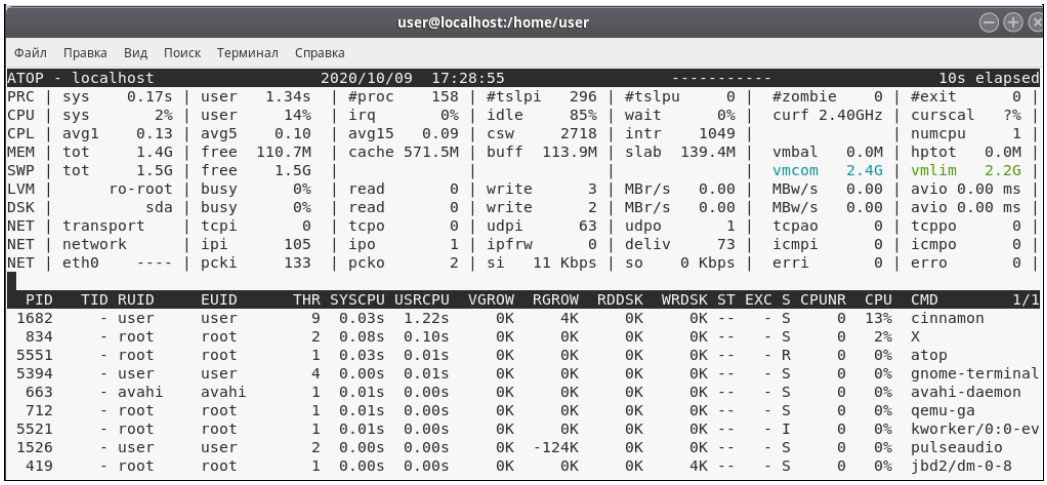
Установить **atop** можно командой (потребуются права **администратора**):

```
$ sudo dnf install atop
```

Для запуска утилиты необходимо в терминале выполнить команду:

```
$ atop
```

После запуска в терминале можно увидеть вывод, примерно следующего содержания:



Описание столбцов вывода **atop**:

- **PID** - идентификатор процесса;
- **RUID** — реальный UID, под которым обрабатывается процесс;
- **EUID** — эффективный UID, под которым обрабатывается процесс (Обычно реальный и эффективный идентификаторы совпадают, т.е. процесс имеет в системе те же права, что и пользователь, запустивший его.);
- **THR** - общее количество потоков для процесса;
- **SYSCPU** - потребление CPU за последний интервал в режиме system. (обычно системные вызовы);
- **USRCPU** - потребление CPU за последний интервал в режиме user;
- **VGROW** - рост виртуальной памяти в течении последнего интервала;
- **RGROW** - резидентный(реальный, занятый процессом ОП) рост памяти в течении последнего интервала. Может быть отрицательным, если процесс выгружается из памяти в swap;
- **RDDSK** - показывает кол обращений к физическому диску для считывания с него данных(минуя кеш);
- без установленного патча - количество данных считаные с диск(минуя кеш);
- **WRDSK** - показывает кол обращений к физическому диску для записи на него данных(минуя кеш);
- **ST** - статус процесса (N в первой позиции говорит, что процесс был запущен во время последнего интервала. Вторая позиция показывает закончился ли процесс за время последнего интервала: E — exit, S - прекращено, C - прекращено но остался core dump);
- **EXC** - код выхода процесса;
- **S** - состояние процесса. (S=sleep (ожидает событий) R=running (работает) Z=zombie (ожидает родительский процесс);
- **CPUNR** - идентифицирует CPU который обрабатывает процесс;
- **CPU** - процент занятости выбранного ресурса;
- **CMD** - имя процесса.

Далее приведено описание наиболее часто используемых интерактивных команд, которые вы можете выполнять во время работы программы:

- **m** — отсортирует процессы по занятой памяти;
- **d** — отсортирует процессы по использованию диска;
- **n** — отсортирует процессы по использованию сети (доступно только с установленным патчем);
- **v** — покажет более подробную информацию о процессах (пользователя, дату и время начала процесса);
- **u** — отсортирует таблицу по пользователям. Использование **shift**+(**d,m,n**) выстроит текущий список по выше указанным параметрам;
- **i** — изменение времени проверки, по умолчанию 10 секунд;
- **g** — вернет все в дефолтный вывод;
- **c** - вывести полный путь запущенного процесса (столбец **COMMAND**).

Для посуточного ведения логов необходимо отредактировать конфигурационный файл **atop**:

```
vi /etc/sysconfig/atop
```

Добавьте в конец файл следующие строки:

```
# Имя файла логов

OUTFILE="$LOGPATH/$CURDAY.log"
```

Общий вид конфига будет следующего содержания:

```
# sysconfig atop
#

# Current Day format
CURDAY=`date +%Y%m%d`
# Log files path
LOGPATH=/var/log/atop
# Binaries path
BINPATH=/usr/bin
# PID File
PIDFILE=/var/run/atop.pid
# interval (default 10 minutes)
INTERVAL=600
# Имя файла логов
OUTFILE="$LOGPATH/$CURDAY.log"
```

По умолчанию **atop** делает снимок раз в 10 минут, это значение регулируется параметром **INTERVAL** в конфиге **/etc/sysconfig/atop**, указывается в секундах, при необходимости поменяйте данный параметр.

После внесения изменений перезапустите **atop**:

```
sudo systemctl restart atop.service
```

Для просмотра дневного лога необходимо в терминале выполнить команду:

```
atop -r /var/log/atop/atop_20201009
```

где **/var/log/atop/atop_20201009** путь до нужного лога.

Для навигации по времени в дневном логе используются клавиши:

- **t** - перейти вперед по времени;
- **Shift + t** - перейти назад по времени.

Для остановки сбора логов необходимо выполнить:

```
sudo systemctl stop atop.service
```

atopsar — встроенный анализатор логов atop

atopsar — встроенный анализатор логов **atop**, который позволяет быстро найти проблему и смотреть лог за определенный промежуток времени. Входит в состав пакета утилиты **atop**.

Подробнее об **atop** см. в нашей статье «Интерактивные утилиты динамического мониторинга процессов. Atop».

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install atop
```

Дальнейшая работа с утилитой выполняется с правами **непривилегированного** пользователя. Выйдите из сеанса пользователя **root**:

```
exit
```

Все логи сохраняются в каталоге по пути **/var/log/atop/**, файлы именуются по формату `atop_<дата>`.

Основные ключи:

- **-r** — считывание данных из файла;
- **-b** — с какого времени вывести лог;
- **-e** — до какого времени вывести лог.

Дополнительные опции для анализа:

- **-d** — нагрузка на каждый диск;
- **-m** — нагрузка на оперативную память и **swap**;
- **-c** — нагрузка на процессор, отдельно по каждому ядру;
- **-p** — количество процессов и потоков;
- **-w** — нагрузка на сетевой трафик;
- **-i** — нагрузка на интерфейс;
- **-O** — топ-3 процессов по использованию процессора;
- **-G** — топ-3 процессов по использованию памяти;
- **-D** — топ-3 процессов по использованию диска;
- **-N** — топ-3 процессов по использованию сети;
- **-A** — все возможные отчеты.

Например, можно смотреть нагрузку на диск по анализу логов за определенный день и время, используя ключ **-d**:

```
atopsar -r /var/log/atop/atop_20231130 -d -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -d -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02  disk           busy read/s KB/read  writ/s KB/writ avque avserv _dsk_
14:18:02  sda              4%    1.8    95.3    10.3    24.9  32.1   3.39766 ms
14:28:02  sda              7%    4.7    61.7    11.7    24.5  35.9   4.07435 ms
14:38:02  sda              5%    5.1   108.5    10.1    24.3  32.5   3.02773 ms
14:48:02  sda              4%    1.6    99.0    10.0    20.1  37.0   3.54848 ms
14:58:02  sda              6%    2.9    79.1    11.0    23.2  31.2   4.16561 ms
15:08:02  sda              6%    6.1    48.0    10.3    22.9  28.2   3.52879 ms
15:18:02  sda              8%   15.8    71.4    10.9    29.7  17.9   2.97726 ms
15:28:02  sda              4%    5.3    96.6    10.4    23.2  30.2   2.34367 ms
15:38:02  sda              5%    3.7    89.0     9.7    23.1  36.4   3.47787 ms
15:48:02  sda              7%    4.6   114.6     9.2    21.6  31.5   5.42570 ms
15:58:02  sda              6%    3.3    99.6    10.0    22.5  32.9   4.68405 ms
```

где:

- **busy** — процент занятости ресурса;
- **read/s** — количество запросов чтения в секунду;
- **KB/read** — объем прочитанных данных в секунду;
- **writ/s** — количество запросов на запись в секунду;
- **KB/writ** — объем записанных данных в секунду;
- **avque** — среднее число запросов;
- **avserv** — среднее время обработки запроса.

Используя ключ **-m**, можно посмотреть, как изменялись значения ОЗУ в указанном диапазоне времени:

```
atopsar -r /var/log/atop/atop_20231130 -m -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -m -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02  memtotal memfree buffers cached dirty slabmem  swptotal swpfree _mem_
14:18:02      954M     64M      4M   301M    0M    102M     1843M   1211M
14:28:02      954M     64M      9M   328M    3M    102M     1843M   1180M
14:38:02      954M     63M      2M   344M    9M    102M     1843M   1160M
14:48:02      954M     72M      3M   336M    2M    101M     1843M   1157M
14:58:02      954M     69M      3M   351M    1M    101M     1843M   1138M
15:08:02      954M     65M      6M   367M    6M    101M     1843M   1120M
15:18:02      954M     78M      4M   376M    5M    102M     1843M   1064M
15:28:02      954M     85M      3M   387M    0M    102M     1843M   1048M
15:38:02      954M     70M      3M   400M    0M    102M     1843M   1034M
15:48:02      954M     67M      3M   410M    0M    101M     1843M   1024M
15:58:02      954M     71M      3M   405M    2M    102M     1843M   1013M
```

где:

- **memtotal** — общий объем оперативной памяти;
- **memfree** — доступный объем оперативной памяти;
- **buffers** — объем буферной памяти;
- **cached** — объем кэш-памяти;
- **dirty** — объем памяти в кэше страниц, который еще нужно сбросить на диск;
- **slabmem** — объем динамической памяти, выделяемой ядром;
- **swptotal** — общий объем памяти подкачки (**swap**);
- **swpfree** — доступный объем памяти подкачки (**swap**).

Узнать, какие топ-3 приложения потребляют память, можно используя ключ **-G**:

```
atopsar -r /var/log/atop/atop_20231130 -G -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -G -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02    pid command  mem% |   pid command  mem% |   pid command  mem%_top3_
14:18:02   8954 rdbserve  26% |   989 Xorg       7% |  1794 mate-scr   4%
14:28:02   8954 rdbserve  24% |   989 Xorg       7% |  1794 mate-scr   4%
14:38:02   8954 rdbserve  22% |   989 Xorg       8% |  1794 mate-scr   4%
14:48:02   8954 rdbserve  22% |   989 Xorg       7% |  1794 mate-scr   4%
14:58:02   8954 rdbserve  22% |   989 Xorg       7% |  1794 mate-scr   4%
15:08:02   8954 rdbserve  20% |   989 Xorg       7% |  1794 mate-scr   4%
15:18:02   8954 rdbserve  18% |   989 Xorg       7% |  1794 mate-scr   4%
15:28:02   8954 rdbserve  16% |   989 Xorg       7% |  1794 mate-scr   3%
15:38:02   8954 rdbserve  17% |   989 Xorg       6% |  1794 mate-scr   3%
15:48:02   8954 rdbserve  16% |   989 Xorg       7% |  1794 mate-scr   4%
15:58:02   8954 rdbserve  16% |   989 Xorg       6% |  1794 mate-scr   4%
```

где:

- **pid** — идентификатор процесса;
- **command** — наименование процесса;
- **mem%** — процент использования памяти процессом.

Аналогично, можно получить топ-3 приложения по загрузке процессора, выполняя команду с ключом **-O**, и по использованию диска с ключом **-D**:

```
atopsar -r /var/log/atop/atop_20231130 -D -O -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -D  -O -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02    pid command  cpu% |   pid command  cpu% |   pid command  cpu%_top3_
14:18:02   8954 rdbserve  99% |   609 qemu-ga    0% |    47 kswapd0    0%
14:28:02   8954 rdbserve  98% |  9265 dnf        0% |   609 qemu-ga    0%
14:38:02   8954 rdbserve  99% |   609 qemu-ga    0% |  9288 gdbus      0%
14:48:02   8954 rdbserve  99% |   609 qemu-ga    0% |  1981 dnfdrago   0%
14:58:02   8954 rdbserve  99% |   609 qemu-ga    0% |    47 kswapd0    0%
15:08:02   8954 rdbserve  99% |   989 Xorg       0% |  9346 mate-scr   0%
15:18:02   8954 rdbserve  97% |  9433 dnfdaemo   0% |    47 kswapd0    0%
15:28:02   8954 rdbserve  99% |  9461 dnf        0% |   609 qemu-ga    0%
15:38:02   8954 rdbserve  98% |   609 qemu-ga    0% |    47 kswapd0    0%
15:48:02   8954 rdbserve  98% |   609 qemu-ga    0% |  9491 mate-scr   0%
15:58:02   8954 rdbserve  98% |   609 qemu-ga    0% |    47 kswapd0    0%

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02    pid command  dsk% |   pid command  dsk% |   pid command  dsk%_top3_
14:18:02   8954 rdbserve  94% |  1005 systemd-   3% |   480 systemd-   2%
14:28:02   8954 rdbserve  79% |     1 systemd   16% |  1005 systemd-   2%
14:38:02   8954 rdbserve  56% |  1794 mate-scr  37% |   480 systemd-   2%
14:48:02   8954 rdbserve  90% |  1005 systemd-   5% |   480 systemd-   3%
14:58:02   8954 rdbserve  95% |  1005 systemd-   2% |   480 systemd-   1%
15:08:02   8954 rdbserve  66% |  1794 mate-scr  20% |   989 Xorg       4%
15:18:02   8954 rdbserve  57% |     1 systemd   29% |  1470 systemd    8%
15:28:02   8954 rdbserve  60% |     1 systemd   31% |   914 master     5%
15:38:02   8954 rdbserve  91% |  9476 pickup     4% |     1 systemd    2%
15:48:02   8954 rdbserve  53% |  1794 mate-scr  38% |  1005 systemd-   2%
15:58:02   8954 rdbserve  98% |  9519 systemd-   1% |     1 systemd    0%
```

iotop - утилита мониторинга использования диска

Установка
Основные опции программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** iotop 0.6-15

Утилита **iotop** позволяет просмотреть сведения об общем и текущем количестве операций обращения к диску.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

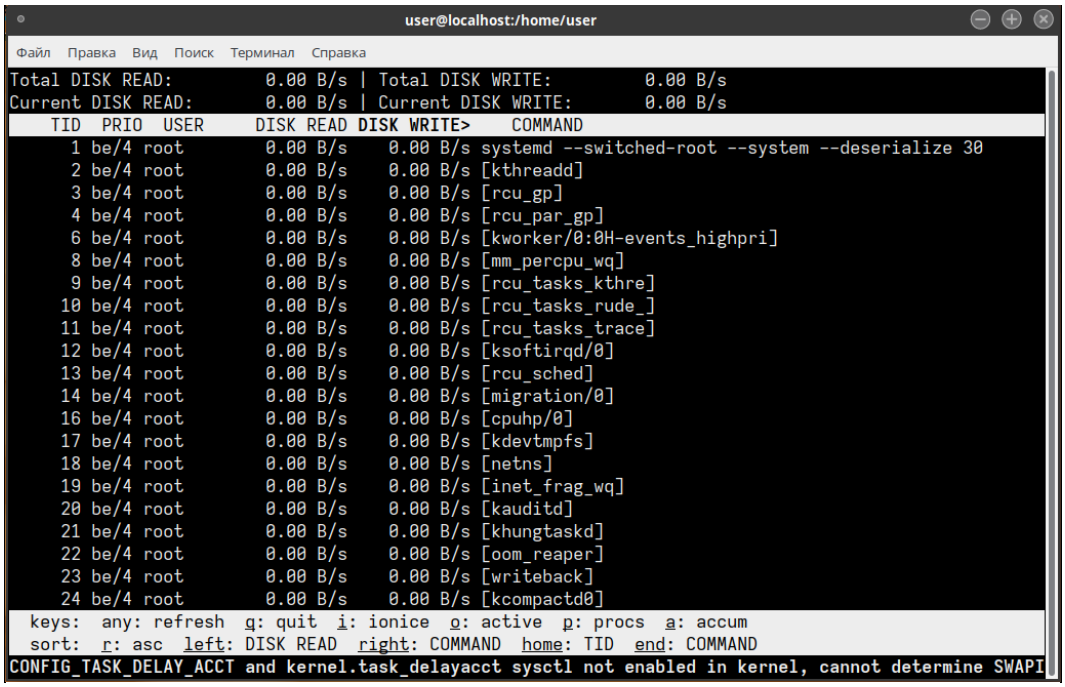
```
su -
```

и выполните команду:

```
dnf install iotop
```

Запустите утилиту через терминал, выполнив:

```
iotop
```



Основные опции программы

Опции для работы в программе описаны в таблице ниже.

Опции	Описание
--version	показать номер версии программы и выйти
-h, --help	показать данное справочное сообщение и выйти
-o, --only	отображать только процессы, которые в данный момент выполняют операции I/O с диском (по умолчанию — отображаются все активные процессы)
-b, --batch	неинтерактивный режим
-n <число>, --iter=<число>	количество итераций до окончания [бесконечно]
-d <сек>, --delay=<сек>	задержка между итерациями [1 секунда]
-p <PID_процесса>, --pid= <PID_процесса>	PID процесса, который нужно отслеживать
-u <имя_пользователя>, --user= <имя_пользователя>	имя пользователя, которого нужно отследить
-P, --processes	отображать только процессы (по умолчанию — все процессы и потоки)
-a, --accumulated	показывать накопленный ввод-вывод вместо пропускной способности
-k, --kilobytes	отображать информацию в КБ
-t, --time	добавить отображение времени выполнения проверки
-q, --quiet	уменьшить количество выводимой информации (подразумевается --batch)

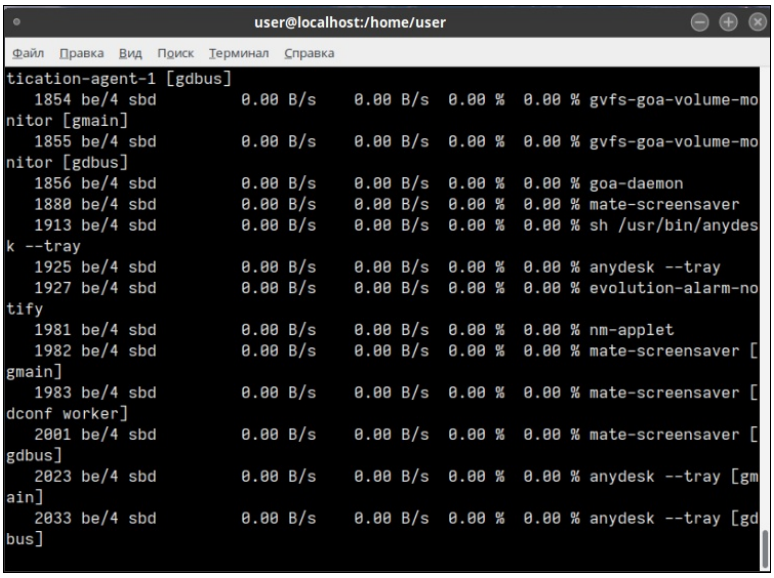
Также **iotop** поддерживает некоторое управление клавиатуры:

- стрелки **влево**-**вправо** — изменить сортировку колонок;
- **r** — изменить сортировку строк в выбранной колонке на обратную (a-z > z-a);
- **i** — изменить nice процесса (утилитой **ionice**);

Пример работы

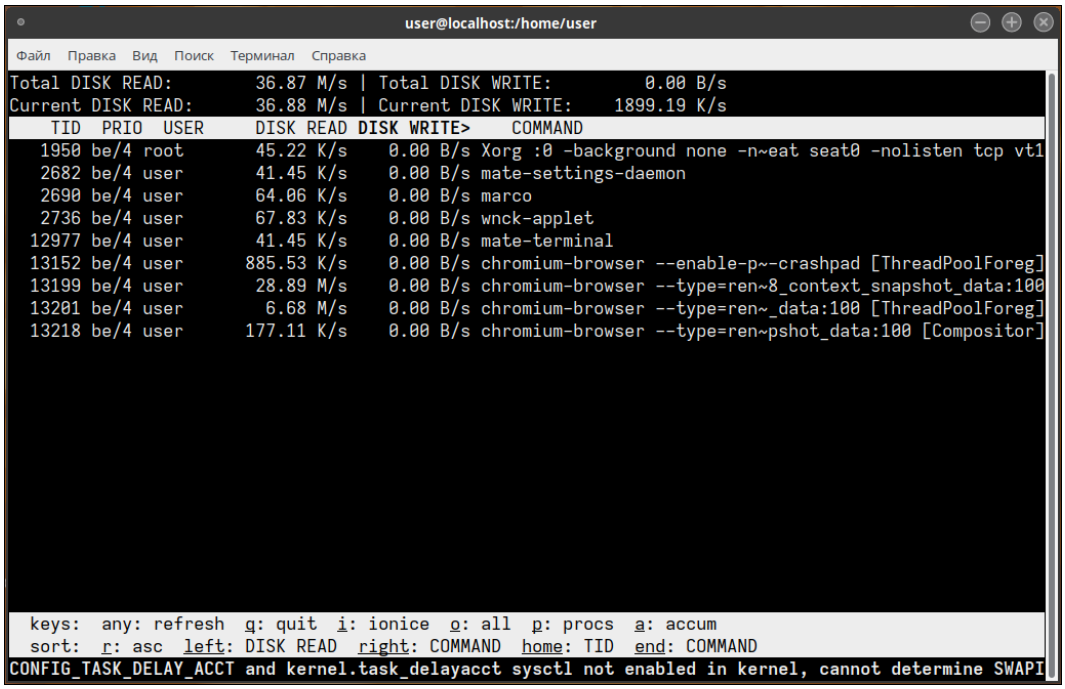
Для отключения интерактивного вида используйте:

```
iotop -b
```



Для отображения только процессов, которые в данный момент выполняют операции I/O с диском:

```
iotop -o
```

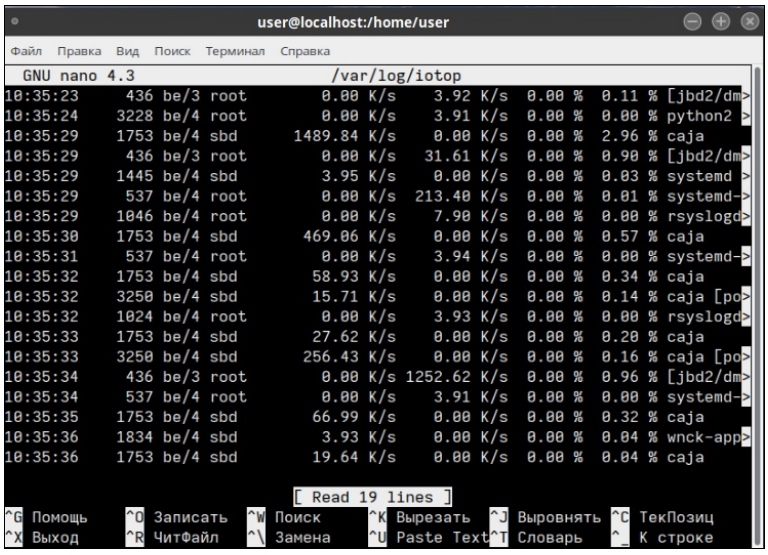


Программа позволяет не только выводить информацию, но и записывать ее для решения проблем в будущем.

Пример команды:

```
iotop -botqqqk --iter=60 >> /var/log/iotop
```

Результат можно посмотреть в указанном файле:



sar

Установка
Синтаксис
Параметры
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: sysstat-12.3.1-1

Sar (System Activity Report) — утилита для сбора статистической информации о производительности системы. **Sar** позволяет наблюдать за производительностью различных подсистем в реальном времени.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Утилита **sar** входит в пакет **sysstat**, для установки выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install sysstat
```

Дальнейшая работа в программе производится с правами непривилегированного пользователя.

Для получения дополнительной информации выполните команду:

```
man sar
```

Список опций можно получить с помощью параметра **--help**:

```
sar --help
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
sar [<параметры>] [<интервал>[<счётчик>]]
```

Параметры

Основные параметры утилиты:

- **-B** — статистика обмена страниц;
- **-b** — статистика ввода-вывода и скорости передачи;
- **-d** — статистика блочных устройств;
- **-F [MOUNT]** — статистика файловых систем;
- **-H** — статистика использования **hugepages** (больших страниц оперативной памяти);
- **- I { <список> | SUM | ALL }** — статистика прерываний;

- **-m { <ключ> | ALL }** — статистика управления питанием. Возможные значения:
  - **CPU** — текущая частота работы ЦП;
  - **FAN** — скорость вращения вентиляторов;
  - **FREQ** — средняя частота работы ЦП;
  - **IN** — входные напряжения;
  - **TEMP** — температура устройств;
  - **USB** — подключенные USB-устройства.
- **-n { <ключ> | ALL }** — сетевая статистика. Возможные значения:
  - **DEV** — статистика сетевых интерфейсов, включая количество принятых и переданных пакетов;
  - **EDEV** — статистика ошибок сетевых интерфейсов;
  - **NFS** — статистика клиента NFS;
  - **NFSD** — статистика сервера NFS;
  - **SOCK** — сокеты;
  - **IP** — IP-трафик;
  - **EIP** — ошибки IP-трафика;
  - **ICMP** — ICMP-трафик;
  - **EICMP** — ошибки ICMP-трафика;
  - **TCP** — TCP-трафик;
  - **ETCP** — ошибки TCP-трафика;
  - **UDP** — UDP-трафик;
  - **SOCK6** — сокеты IPv6;
  - **IP6** — IP-трафик IPv6;
  - **EIP6** — ошибки IP-трафика IPv6;
  - **ICMP6** — ICMP-трафик IPv6;
  - **EICMP6** — ошибки ICMP-трафика IPv6;
  - **UDP6** — UDP-трафик IPv6;
  - **FC** — адаптер Fibre channel;
  - **SOFT** — программная сетевая обработка.
- **-q [<ключ> | PSI | ALL]** — статистика по загрузке и провалов нагрузки системы. Возможные значения ключа:
  - **LOAD** — статистика длины очереди и средней загрузки;
  - **CPU** — статистика провалов нагрузки ЦП CPU;
  - **IO** — статистика провалов нагрузки ВВ/ВЫВ;
  - **MEM** — статистика провалов нагрузки памяти;
- **-r [ALL]** — статистика использования памяти;
- **-S** — статистика использования области подкачки;
- **-u [ALL]** — статистика использования ЦП;
- **-v** — статистика таблиц ядра;
- **-W** — статистика раздела подкачки;
- **-w** — статистика создания задач и системных переключений;
- **-y** — статистика устройств TTY.

Примеры использования

1. Сбор и отображение полной статистики работы процессора в течение 5 циклов с интервалом 2 секунды:

```
sar -u ALL 2 5
```

Пример вывода:

```
15:24:40      CPU    %usr   %nice    %sys %iowait  %steal    %irq   %soft  %guest  %gnice   %idle
15:24:42      all    0,50    0,00    0,25    0,00    0,00    1,50    2,51    0,00    0,00   95,24
15:24:44      all    0,25    0,00    0,00    0,00    0,00    1,50    2,26    0,00    0,00   95,99
15:24:46      all    1,25    0,00    0,50    0,75    0,00    1,75    2,01    0,00    0,00   93,73
15:24:48      all    0,25    0,00    0,25    0,00    0,00    1,51    2,02    0,00    0,00   95,97
15:24:50      all    0,75    0,00    0,50    0,00    0,00    1,51    2,26    0,00    0,00   94,97
Среднее:      all    0,60    0,00    0,30    0,15    0,00    1,56    2,21    0,00    0,00   95,18
```

где:

- **%usr** — процент времени, затраченного процессором на выполнение кода, запущенного на уровне пользователя;
- **%nice** — процент времени, затраченного процессором на выполнение кода в пользовательском пространстве с пониженным приоритетом;
- **%sys** — процент времени, затраченного процессором на выполнение кода в системном пространстве;
- **%iowait** — процент времени, затраченного процессором на ожидание завершения операций ввода/вывода;
- **%steal** — процент времени, проведенного в вынужденном ожидании виртуальным процессором или ЦПУ, пока гипервизор обслуживал другой виртуальный процессор;
- **%irq** — процент времени, затраченного процессором на обслуживание аппаратных прерываний;
- **%soft** — процент времени, затраченного процессором на обслуживание системных прерываний;
- **%guest** — процент времени, затраченного процессором на выполнение кода, запущенного внутри виртуальной машины;
- **%gnice** — процент времени, затраченного процессором на выполнение кода, запущенного с помощью команды nice внутри виртуальной машины;
- **%idle** — процент времени, когда процессор простаивает и не выполняет никаких задач.

Анализ результатов статистики состояния процессора:

- **idle < 20%** — указывает на высокую загрузку процессора. Необходимо определить, обусловлена ли нагрузка пользовательскими приложениями (usr) или системными процессами (sys);
- **usr > 70%** — процессор перегружен пользовательскими приложениями. Используйте инструменты, такие как **top**, **htop**, или **pidstat**, чтобы найти самые ресурсозатратные процессы;
- **sys > 30%** — высокая системная нагрузка, ядро работает слишком интенсивно, система перегружена системными вызовами, прерываниями, драйверами; проверьте работу драйверов или включите диагностику через **iostat** и **vmstat;**
- **iowait > 10%** — процессоры ждут операций ввода-вывода, указывая на проблемы с подсистемой хранения данных (диск или сеть), используйте **iostat** или **sar -d** для диагностики подсистемы ввода-вывода;
- **steal > 5%** — в виртуальной среде это говорит о конкуренции за **CPU** с другими виртуальными машинами.

2. Сбор и вывод статистики по свободной и занятой памяти:

```
sar -r 2 5 --human
```

где:

--human — отображение результата в удобочитаемом формате.

Пример вывода:

```
17:17:48   kbmemfree   kbavail kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
17:17:50     473,6M      1,3G    339,9M     17,3%    22,6M   1004,0M      3,4G     86,4%    811,0M    463,1M    104,0k
17:17:52     345,2M      1,2G    438,6M     22,4%    22,9M      1,0G      4,9G    124,4%    931,3M    463,3M    848,0k
17:17:54     285,9M      1,2G    463,1M     23,6%    22,9M      1,0G      5,0G    126,8%    988,0M    463,6M     1,4M
17:17:56     193,9M      1,1G    554,6M     28,3%    23,0M      1,0G      5,8G    146,7%      1,0G    465,2M     2,5M
17:17:58     184,3M      1,1G    563,1M     28,7%    23,2M      1,0G      6,4G    161,6%      1,0G    468,5M     3,2M
Среднее:     296,6M      1,2G    471,9M     24,1%    22,9M      1,0G      5,1G    129,2%    974,1M    464,7M     1,6M
```

где:

- **kbmemfree** — свободная память;
- **kbavail** — доступная память;

- **kbmemused** — использованная память;
- **%memused** — процент использованной памяти;
- **kbbuffers** — память, используемая ядром как буфер;
- **kbcached** — память, используемая ядром для кеширования данных;
- **kbcommit** — память, необходимая для текущей рабочей нагрузки;
- **%commit** — процент памяти, необходимый для рабочей нагрузки;
- **kbactive** — память, использовавшаяся недавно;
- **kbinact** — память, использовавшаяся давно;
- **kbdirty** — память, ожидающая перезаписи.

3. Сбор и вывод статистики по использованию устройств ввода/вывода:

```
sar -b 2 5
```

Пример вывода:

```
15:37:53        tps     rtps     wtps     dtps   bread/s   bwrtn/s   bdscd/s
15:37:55       0,00     0,00     0,00     0,00      0,00      0,00      0,00
15:37:57       0,00     0,00     0,00     0,00      0,00      0,00      0,00
15:37:59      37,50    37,50     0,00     0,00  69324,00      0,00      0,00
15:38:01     104,50   101,00     3,50     0,00 154636,00    128,00      0,00
15:38:03     191,50   187,50     4,00     0,00 154880,00    208,00      0,00
Среднее:     66,70    65,20     1,50     0,00  75768,00     67,20      0,00
```

где:

- **tps** — общее число передач в секунду, отправленных на физические устройства;
- **rtps** — число запросов на чтение (в сек.), отправленных на физические устройства;
- **wtps** — число запросов на запись (в сек.), отправленных на физические устройства;
- **dtps** — число запросов на удаление (в сек.), отправленных на физические устройства;
- **bread/s** — количество блоков, прочитанных (в сек.);
- **bwrtn/s** — количество блоков, записанных (в сек.);
- **bdscd/s** — количество блоков, отброшенных (в сек.).

4. Сбор и вывод статистики по трафику IPv4:

```
sar -n SOCK 3 5
```

Пример вывода:

```
15:41:48     totsck   tcpsck   udpsck   rawsck  ip-frag   tcp-tw
15:41:51       869       34        8        1        0        1
15:41:54       927       55       18        1        0        2
15:41:57       930       59       12        1        0        2
15:42:00       964       81       15        1        0        2
15:42:03       976       97       12        1        0        4
Среднее:       933       65       13        1        0        2
```

где:

- **totsck** — общее количество сокетов в системе;
- **tcpsck** — количество сокетов TCP (Transmission Control Protocol);
- **udpsck** — количество сокетов UDP (User Datagram Protocol);
- **rawsck** — количество сокетов RAW (сокеты, которые используются для передачи данных без использования транспортного протокола);
- **ip-frag** — количество фрагментов IP-пакетов, которые ожидают сборки;
- **tcp-tw** — количество сокетов TCP, находящихся в состоянии TIME-WAIT (ожидание закрытия соединения).

5. Сбор и вывод статистики по средней загрузке:

```
sar -q 2 5
```

Пример вывода:

```
15:45:06     runq-sz  plist-sz   ldavg-1   ldavg-5  ldavg-15   blocked
15:45:08           1       532      0,45      0,34      0,16         0
15:45:10           0       532      0,58      0,37      0,17         0
15:45:12           2       562      0,58      0,37      0,17         0
15:45:14           4       579      1,17      0,49      0,22         1
15:45:16           3       582      1,17      0,49      0,22         0
Среднее:           2       557      0,79      0,41      0,19         0
```

где:

- **runq-sz** — количество задач, ожидающих начала выполнения;
- **plist-sz** — количество задач в списке задач;
- **ldavg-1** — средняя загрузка системы за последнюю минуту;
- **ldavg-5** — средняя загрузка системы за последние 5 минут;
- **ldavg-15** — средняя загрузка системы за последние 15 минут;
- **blocked** — количество задач, заблокированных в данный момент.

6. Сбор статистики ввода-вывода на уровне устройств:

```
sar -d 2 4
```

Пример вывода:

```
09:06:07        DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:09        sda      3,98      0,00     35,82      0,00      9,00      0,00      0,62      0,05
09:06:09        sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
09:06:09      zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

09:06:09        DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:11        sda      4,50      0,00    482,00      0,00    107,11      0,01      1,22      0,50
09:06:11        sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
09:06:11      zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

09:06:11        DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:13        sda      1,00      0,00     44,00      0,00     44,00      0,01      3,00      0,25
09:06:13        sdb      1,50      0,00      8,00      0,00      5,33      0,07     21,67      3,25
09:06:13      zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

09:06:13        DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:15        sda     28,00      0,00    126,00      0,00      4,50      0,12      4,12      0,50
09:06:15        sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
09:06:15      zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

Среднее:        DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
Среднее:        sda      9,36      0,00    171,79      0,00     18,35      0,03      3,37      0,32
Среднее:        sdb      0,37      0,00      2,00      0,00      5,33      0,02     21,67      0,81
Среднее:      zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
```

где:

- **DEV** — имя устройства, для которого собирается статистика (например, **sda**, **sdb** или **nvme0n1**);
- **tps** — количество операций ввода-вывода в секунду на устройство;
- **rkB/s** — скорость чтения данных с устройства в КБ/сек.;
- **wkB/s** — скорость записи данных на устройство в КБ/сек.;
- **dkB/s** — скорость операций **discard** (освобождения места) в КБ/сек.;
- **areq-sz** — средний размер операций ввода-вывода в КБ;
- **aqu-sz** — среднее количество операций ввода-вывода, ожидающих выполнения;

- **await** — среднее время (в миллисекундах), которое запросы ввода-вывода ожидали выполнения;
- **%util** — процент времени, в течение которого устройство было занято обработкой запросов.

Как интерпретировать статистику:

- высокие значения **tps**, **rkB/s**, **wkB/s** указывают на активную загрузку устройства;
- высокий **%util** (>70-80%) указывает на то, что устройство может стать узким местом;
- высокий **await** говорит о задержках в обработке операций, что может быть вызвано очередями или высокой нагрузкой.

pmap

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Команда **pmap** предоставляет подробную карту памяти, используемой процессом. Для работы с этой командой необходимо сначала найти идентификатор нужного процесса. Его можно получить командой **ps**, или даже командой **top**, если речь идет о процессе, потребляющем много процессорного времени.

Для запуска утилиты необходимо в терминале выполнить команду:

```
pmap <параметр> <идентификатор процесса>
```

Например:

```
[root@localhost ~]# pmap -x 34770
34770:   bash
Address           Kbytes     RSS   Dirty Mode  Mapping
0000000000400000    1036     952       0 r-x-- bash
0000000000702000       4       4       4 r---- bash
0000000000703000      36      36      36 rw--- bash
000000000070c000      40      28      28 rw---   [ anon ]
0000000000b1d000    1452    1352    1352 rw---   [ anon ]
00007f1219258000      44      44       0 r-x-- libnss_files-2.28.so
00007f1219263000    2048       0       0 ----- libnss_files-2.28.so
00007f1219463000       4       4       4 r---- libnss_files-2.28.so
00007f1219464000       4       4       4 rw--- libnss_files-2.28.so
00007f1219465000      24       0       0 rw---   [ anon ]
00007f121946b000      40      40       0 r-x-- libnss_sss.so.2
00007f1219475000    2044       0       0 ----- libnss_sss.so.2
00007f1219674000       4       4       4 r---- libnss_sss.so.2
00007f1219675000       4       4       4 rw--- libnss_sss.so.2
00007f1219676000  212648     512       0 r---- locale-archive
```

Основные параметры:

- **-x** - эта опция используется для отображения карты памяти в расширенном формате.
- **-p** - эта опция используется для отображения полного пути к файлам.
- **-d** - эта опция используется для отображения формата устройства.
- **-q** - эта опция используется для игнорирования имен столбцов при отображении отчета карты памяти.
- **-A** - эта опция используется для отображения результатов в заданном диапазоне. Обратите внимание, что аргументы **low** и **high** — это одна строка, разделенная запятой.
- **-XX** - эта опция используется для отображения всего, что предоставляет ядро.
- **-n** - эта опция используется для создания новой конфигурации.
- **-c** - эта опция используется для чтения конфигурации по умолчанию.
- **-h** - эта опция используется для отображения текста справки.
- **-v** - эта опция используется для отображения информации о версии и выхода.

nmon

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

nmon — это утилита измерения и настройки производительности для системных администраторов. Она может отображать информацию о ЦП, оперативной памяти, сети, дисках (в виде мини графиков или числовых данных), файловых системах, NFS, самых нагружающих процессах, ресурсах (версия Linux и процессоры).

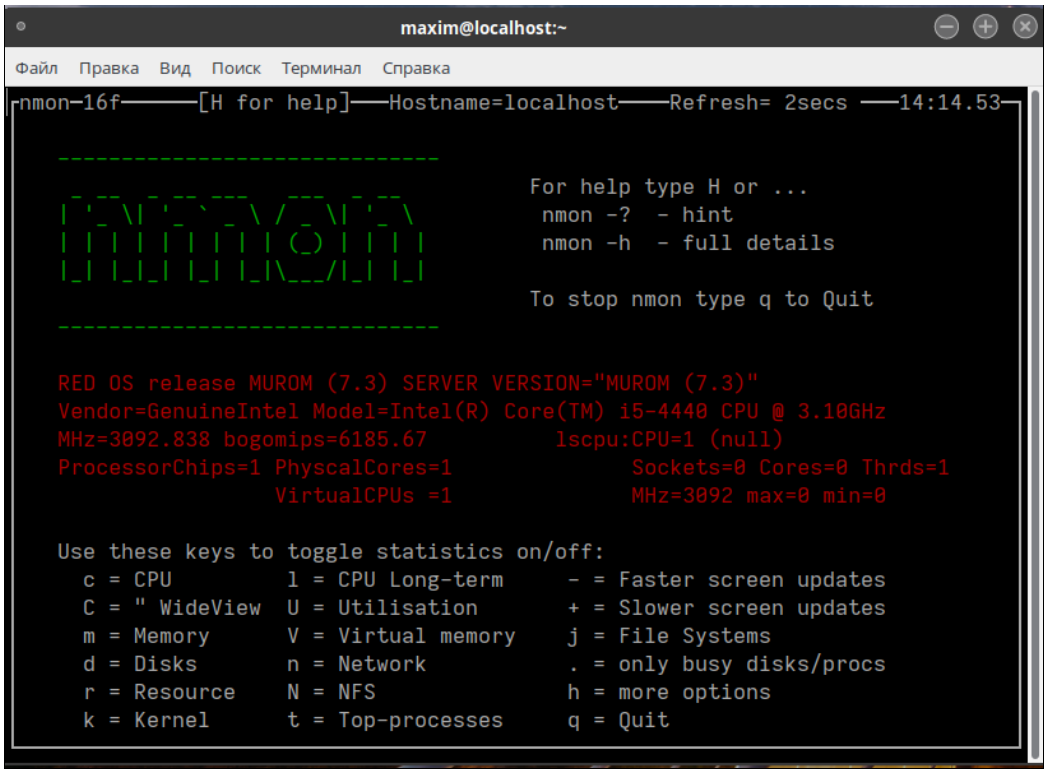
Устанавливается командой:

```
sudo dnf install nmon
```

Для запуска утилиты необходимо в терминале выполнить команду:

```
nmon
```

После запуска в терминале можно увидеть вывод, примерно следующего содержания:



Для отображения информации по определенному ресурсу используются следующие клавиши:

- **c = CPU** - Показывает нагрузку каждого ядра процессора и среднюю нагрузку процессора, загруженность системой, пользователем и ожидание.
- **m = Memory** - Показывает общее количество оперативной памяти, занятой в мегабайтах и процентах, файла подкачки, кэшированной памяти, буфера и другу информацию о состоянии памяти.
- **d = Disks** - Показывает информацию о состоянии дисков и их разделов (информация файла /proc/diskstats). Информация представлена в виде таблицы и графика, в котором показаны имя физического диска и томов, количество занятой памяти, текущее чтение и запись с раздела диска (в килобайтах), для каждого раздела существует график со шкалой от 0 до 100 процентов, для визуальной наглядности загруженности дисков. Также присутствует информация о суммарной скорости чтения и записи.
- **r = Resources** - Показывает информацию о версии и типе ядра, процессоре, архитектуре компьютера, операционной системе и ее версии.
- **k = Kernel** - Показывает информацию о ядре в виде таблицы, запущенных очередях, форках, прерываниях, переключениях. Также показывает среднюю нагрузку, холостой ход, длительность полной работы системы и средней нагрузки ядра на процессор.
- **j = Filesystems** - Показывает информацию о файловой системе в виде таблицы, имя раздела (путь к папке), полный размер (MB),

свободное и занятое место (MB), тип файловой системы и точка монтирования.

- **n = Network** - Показывает информацию о сетевых интерфейсах, количестве и размеру отправленных/полученных пакетов, также уведомляет об сетевых ошибках в виде аккуратной таблицы.
- **N = NFS** - Показывает информацию о сетевой файловой системе (NetworkFileSystem), загруженности сети, клиентом и сервером, в моем случае NFS версии 2 и 3.
- **t = Top processes** - Показывает список процессов в виде таблицы (очень похоже на команду top), столбцы: PID процесса, нагрузка на процессор, количество занятой оперативной памяти и т. д.
- **V = Virtual memory** - Показывает информацию о виртуально памяти, в частности о разделе подкачки.
- **v = Verbose hints** - Показывает информацию о ресурсах в плане безопасности, степень предупреждения и опасности (в процентах).
- **l = CPU long-term** - Показывает наглядный график загруженности процессора.

vmstat

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

vmstat – утилита для определения производительности системы. Она является эффективным средством для оценки необходимого объема ресурсов, предоставляя информацию о загруженности процессора, интенсивности операций дискового ввода-вывода и использовании оперативной памяти.

Устанавливается командой (если утилита не установлена):

```
sudo dnf install sysstat
```

Простой запуск без ключей будет выглядеть так:

```
vmstat
```

```
[root@localhost user]# vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0  36068 177128  13656 353808    0   66  1676   291  214  395  6  3 86  6  0
```

Значения каждой колонки:

Procs

- **r**: количество запущенных процессов (работающих или ожидающих выполнения).
- **b**: количество спящих процессов.

Memory

- **swpd**: объем используемой виртуальной памяти.
- **free**: объем свободной памяти.
- **buff**: количество памяти, используемой в качестве буферов.
- **cache**: объем памяти, используемой в качестве кеша.
- **inact**: количество неактивной памяти (опция -a).
- **active**: количество активной памяти. (опция -a).

Swap

- **si**: объем памяти, выгруженный с диска (/s).
- **so**: объем памяти, перенесенный на диск (/s).

IO

- **bi**: блоки, полученные от блочного устройства (blocks/s).
- **bo**: блоки, отправленные на блочное устройство (blocks/s).

System

- **in**: количество прерываний в секунду, включая часы.
- **cs**: количество переключений контекста в секунду.

CPU

Здесь проценты от общего времени процессора.

- **us**: время, потраченное на запуск кода, не относящегося к ядру (время пользователя).
- **sy**: время, потраченное на выполнение кода ядра (системное время).
- **id**: время бездействия. До версии Linux 2.5.41 это включает время ожидания ввода-вывода.
- **wa**: время, проведенное в ожидании ввода/вывода
- **st**: время, украденное из виртуальной машины.

Опции vmstat

- **-a** — переключение колонки memory в active/inactive значение вместо buff/cache (active — память, реально используемая в данный момент определённым процессом, inactive — память, выделенная ранее какому-то процессу, которого уже нет);
- **-f** — информация о количестве системных вызовов fork, vfork и rfork, выполненных с момента старта системы, и количество страниц виртуальной памяти, задействованных каждым из них;
- **-m** — использование динамической памяти ядра, выделенной с использованием malloc;
- **-n** — задаёт интервал выполнения в секундах;
- **-s** — изменение вида отображение результатов (в две колонки);
- **-d** — статистика использования дисков;
- **-w** — увеличивает визуальный размер поля для больших объемов;
- **-p** [partition name] — с указанием имени раздела, информация по конкретном разделу (read/writes);
- **-t** – добавляление временной метки к каждой выходной строке;
- **-d** – отображение статистики диска
- **-D** – сделать отчет об активности диска;
- **-S [k | K | m | M]** — с указанием в чем выводить информацию (килобиты, килобайты, мегабиты, мегабайты соответственно);
- **-V** — версия vmstat. Кроме того, после указания опций можно задать две цифры — интервал между выполнением, и количество повторов:

```
vmstat 2 5 -t
```

```
[root@localhost user]# vmstat 2 5 -t
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu----- -----timestamp-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st                 MSK
 2  0   9464  87188  19860 403008    0   13   991    51  125  275  2  2 92  5  0 2021-05-11 10:54:49
 0  0   9464  87156  19860 403008    0    0     0    78  111  239  1  1 98  0  0 2021-05-11 10:54:51
 1  0   9464  87156  19868 403008    0    0     0    22   75  125  1  1 97  2  0 2021-05-11 10:54:53
 0  0   9464  87164  19868 403008    0    0     0     0   71  151  1  0 99  0  0 2021-05-11 10:54:55
 0  0   9464  87196  19868 403008    0    0     0     0   69  130  1  0 99  0  0 2021-05-11 10:54:57
```

vmstat выполнен 5 раз с интервалом в 2 секунды.

dstat

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

dstat - инструмент для мониторинга состояния системы.

Установка в РЕД ОС 7.3:

```
dnf install dstat
```

Использование.

Отображение информации по процессу и статистики записи/чтения на диски:

```
python3 /usr/bin/dstat -s -d -top-bio
```

Пример по использованию памяти:

```
python3 /usr/bin/dstat -g -l -m -s -top-mem
```

Потребление ресурсов процессора:

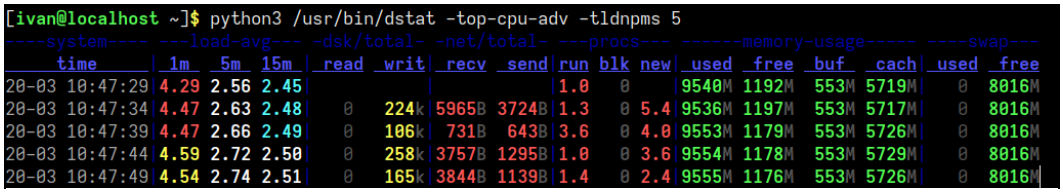
```
python3 /usr/bin/dstat -c -y -l -proc-count -top-cpu
```

или

```
python3 /usr/bin/dstat -c -top-cpu -d -top-bio -top-latency
```

Еще одна комбинация:

```
python3 /usr/bin/dstat -top-cpu-adv -tldnpms 5
```



Описание параметров:

- **l** - средняя загрузка системы;
- **d** - использования дисков;
- **n** - загрузка сетевых устройств;
- **p** - активность процессов;
- **m** - использование памяти;
- **s** - использование подкачки;
- **5** - интервалов в 5 секунд;
- **t** - вывод текущего времени;
- **-top-cpu-adv** - показать самый "дорогой" процесс ввода-вывода (включая pid и другую статистику).

SysMonTask - диспетчер задач РЕД ОС

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: SysMonTask - 1.3.9-2

SysMonTask — утилита, которая в режиме реального времени предоставляет информацию о процессах, выполняемых на компьютере, а также используемых ими ресурсах (об оперативной памяти, процессоре и др.).

SysMonTask имеет схожий с диспетчером задач Windows интерфейс.

Вы можете подробнее ознакомиться с работой диспетчера задач **SysMonTask**, просмотрев наши обучающие видео:

- на **RuTube** — Альтернативный диспетчер задач в РЕД ОС. Sysmontask;
- в **Яндекс.Дзен** — Альтернативный диспетчер задач в РЕД ОС. Sysmontask;
- в **VK Видео** — Альтернативный диспетчер задач в РЕД ОС. Sysmontask.

На наших каналах вы также сможете найти много другой полезной информации.

Установка SysMonTask

Для установки **SysMonTask** используется команда:

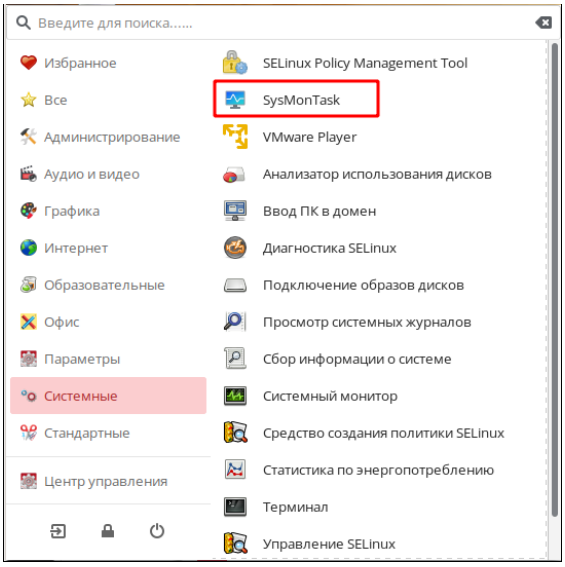
```
dnf install sysmontask
```

Использование SysMonTask

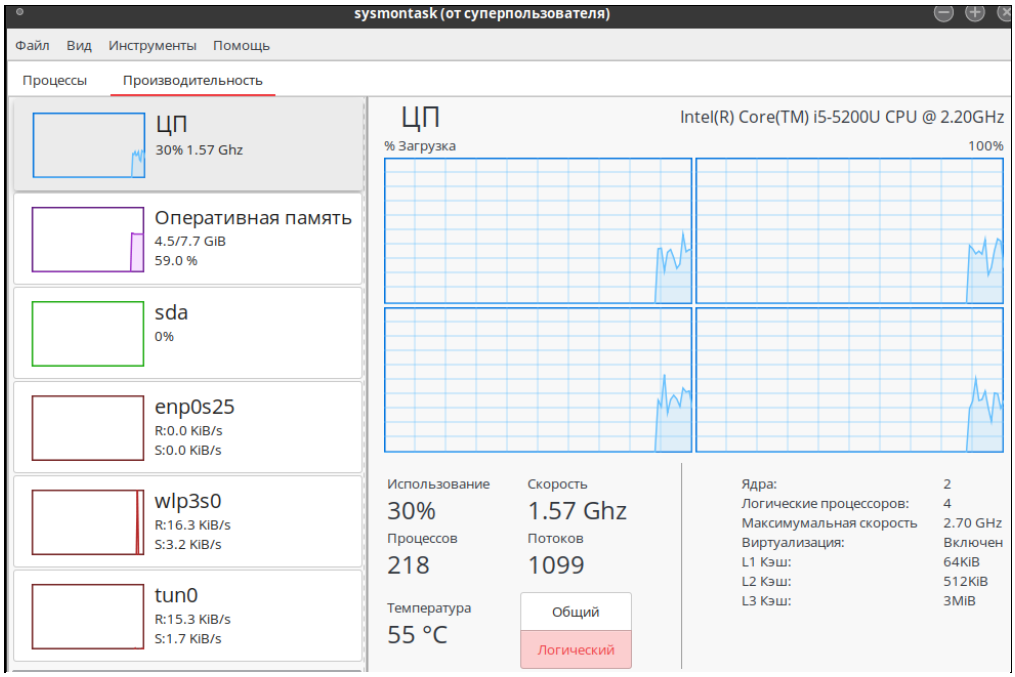
SysMonTask можно открыть из терминала командой:

```
sysmontask
```

или через пользовательский интерфейс из пункта меню «**Системные**».

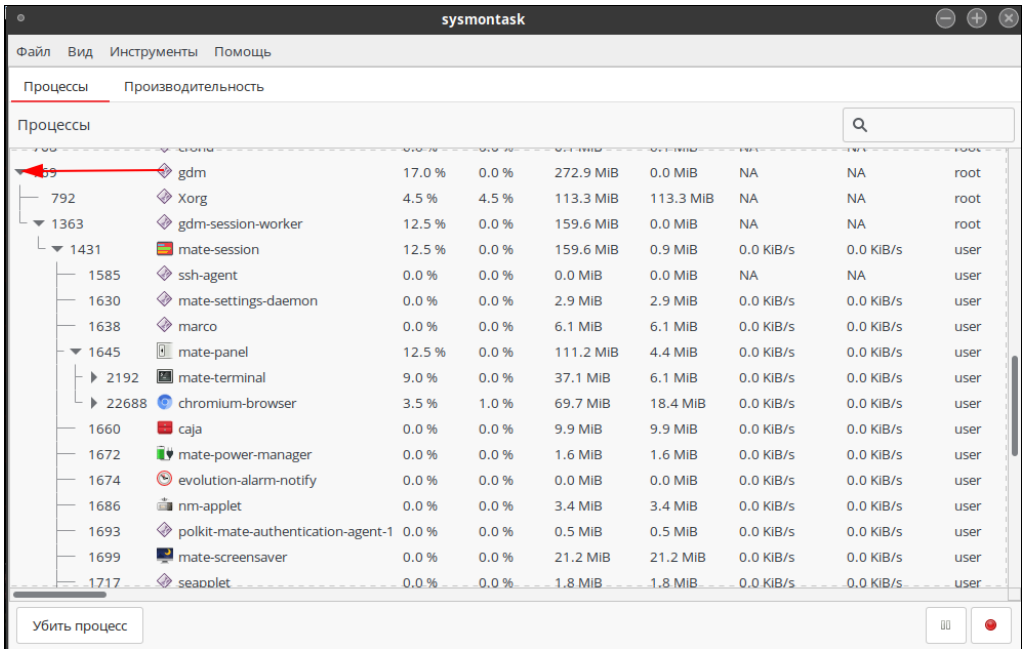


Во вкладке «**Производительность**» отображается общее потребление аппаратных ресурсов:



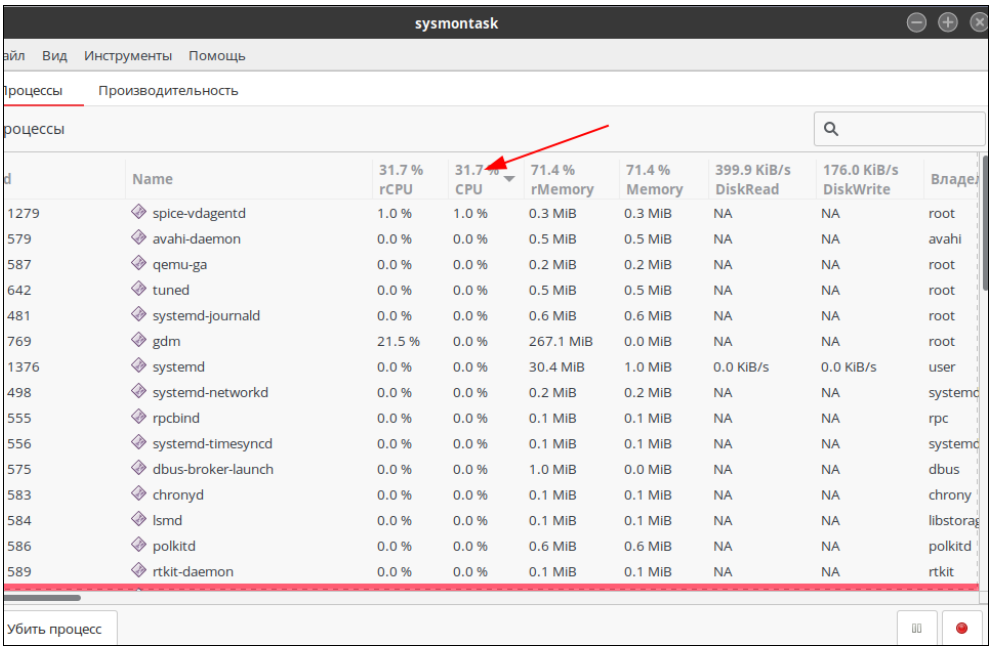
Во вкладке «**Процессы**» отображаются все выполняющиеся в данный момент процессы.

Если вы не находите какой-либо процесс, то скорее всего он является подпроцессом, чтобы его увидеть, необходимо развернуть дерево процессов.

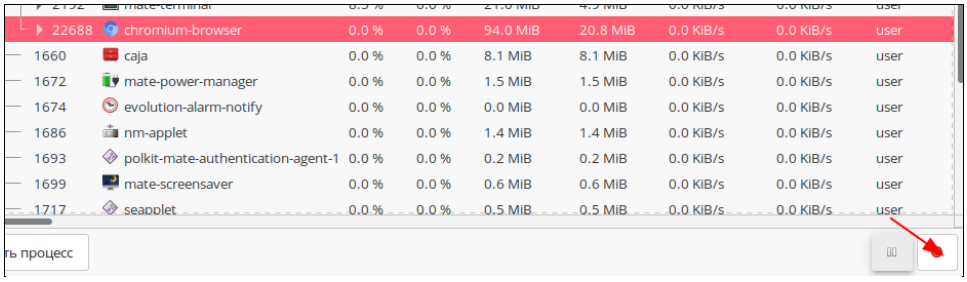


Кнопка «**Убить процесс**» завершает выбранный процесс.

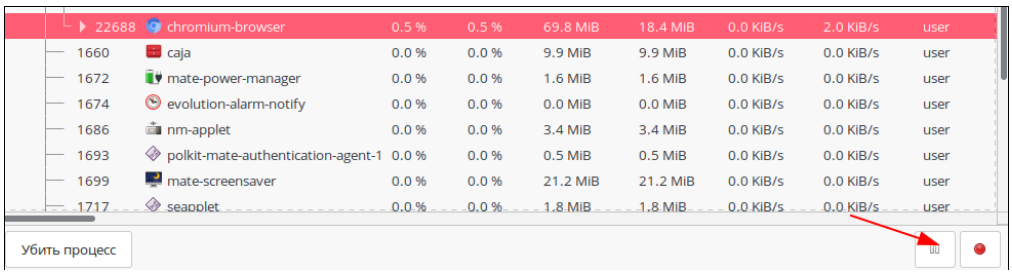
Чтобы отсортировать процессы по какому-либо параметру, необходимо нажать на заголовок столбца:



SysMonTask позволяет записывать потребление ресурсов, для этого необходимо нажать на кнопку записи в правом нижнем углу окна.



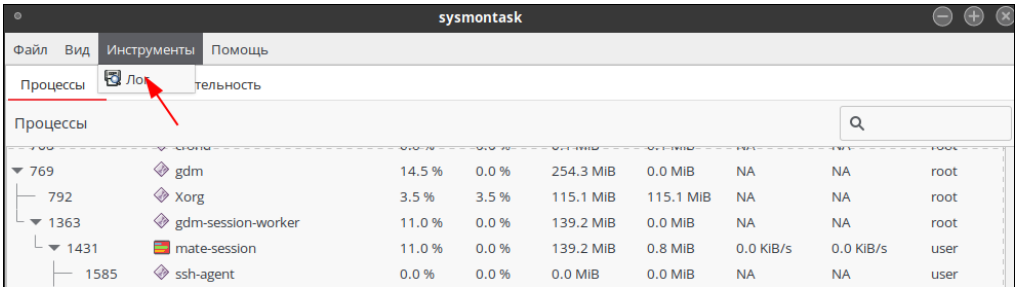
Запись можно приостановить нажав на кнопку паузы в правом нижнем углу окна.



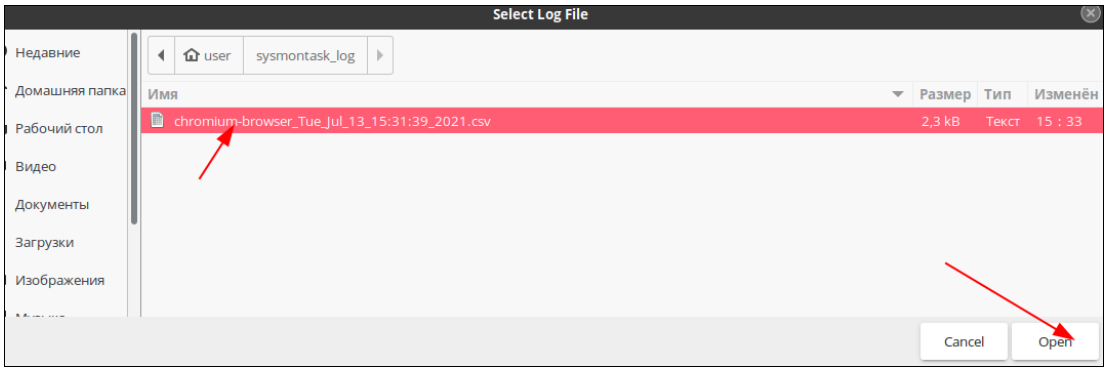
Для того чтобы просмотреть запись, должна быть установлена библиотека **matplotlib**, для этого используем следующую команду:

```
pip3 install matplotlib
```

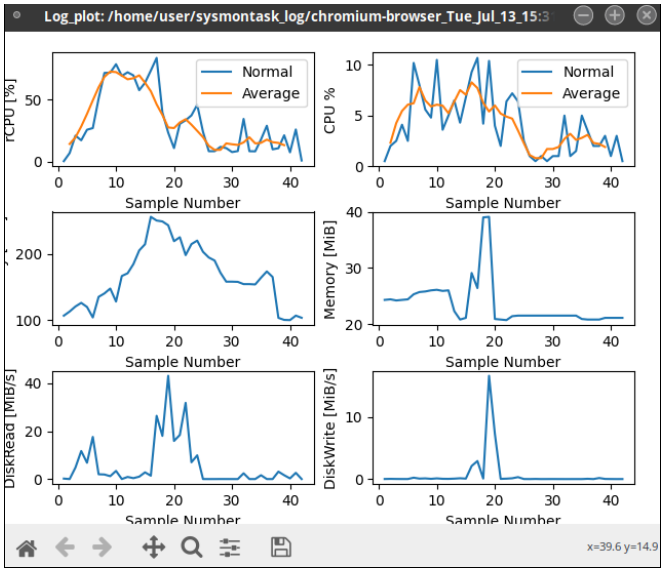
Далее в **SysMonTask** для открытия записи необходимо в меню «**Инструменты**» выбрать «**Лог**».



Выбираем нужную запись и нажимаем «**Открыть**»:

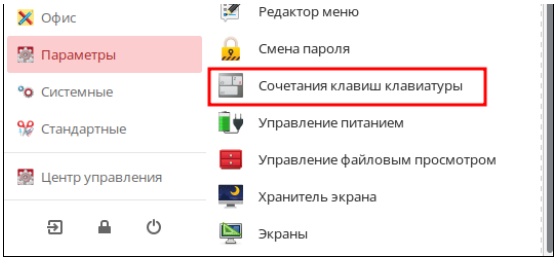


В результате отобразится график использования ресурсов.



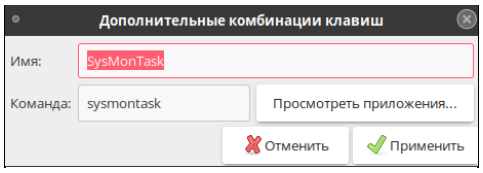
Можно настроить вызов **SysMonTask** с помощью сочетания клавиш «**Ctrl+Alt+Delete**», как в Windows.

Для этого в меню «**Параметры**» выбираем «**Сочетания клавиш клавиатуры**».

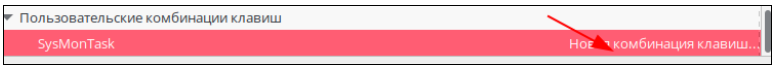


Нажимаем кнопку «**Добавить**».

Вписываем имя процедуры и команду «**sysmontask**», затем «**Применить**».



Далее выбираем поле «**Сочетание клавиш**» напротив **SysMonTask**:



И нажимаем «**Ctrl+Alt+Delete**».

Systemd-analyze - анализ системных процессов

Systemd-analyze — утилита, которая используется для просмотра отчетов о производительности системы. С помощью **systemd-analyze** можно получить информацию о том, сколько времени потребовалось для загрузки системы, а также сколько времени потребовалось для запуска каждого модуля.

Для просмотра информации о количестве времени, которое затрачивается при загрузке системы с разбивкой на ядро и пользовательское пространство, необходимо выполнить следующую команду:

```
systemd-analyze

Startup finished in 1.557s (kernel) + 4.996s (initrd) + 45.794s (userspace) = 52.348s
graphical.target reached after 45.780s in userspace
```

Также можно просмотреть подробную информацию о затраченном времени каждым блоком (процессом) в отдельности, для этого используется следующая команда:

```
systemd-analyze blame

25.298s plymouth-quit-wait.service
17.432s dnf-makecache.service
15.769s accounts-daemon.service
13.800s udisks2.service
 9.440s postfix.service
 5.744s vmware.service
 5.604s initrd-switch-root.service
 4.708s NetworkManager-wait-online.service
 4.668s systemd-udev-settle.service
 3.925s avahi-daemon.service
 3.546s lvm2-monitor.service
 3.343s lm_sensors.service
 3.108s smartd.service
 2.957s usbsrvd.service
 2.721s sshd.service
 2.216s ModemManager.service
 2.212s NetworkManager.service
 2.143s chronyd.service
 1.830s systemd-homed.service
 1.826s sysstat.service
 1.814s systemd-logind.service
 1.789s upower.service
 1.596s rtkit-daemon.service
 ...
```

С помощью полученной информации можно оптимизировать время загрузки системы. Список отсортирован по затраченному времени в порядке убывания.

Так как список процессов может быть довольно большим, существует возможность отсортировать вывод при помощи команды head (обычно первых 10 записей достаточно, чтобы найти требующие большого количества времени службы):

```
systemd-analyze blame | head
```

Также можно просмотреть подробную информацию в виде дерева критической по времени цепочки событий. Для этого необходимо выполнить команду:

```
systemd-analyze critical-chain

The time when unit became active or started is printed after the "@" character.
The time the unit took to start is printed after the "+" character.

graphical.target @45.780s
└─multi-user.target @45.780s
  └─plymouth-quit-wait.service @20.481s +25.298s
    └─systemd-user-sessions.service @20.211s +156ms
      └─remote-fs.target @20.176s
        └─remote-fs-pre.target @20.176s
          └─nfs-client.target @16.448s
            └─gssproxy.service @15.158s +1.266s
              └─network.target @15.140s
                └─wpa_supplicant.service @42.982s +143ms
                  └─basic.target @11.186s
```

```
└─dbus-broker.service @10.563s +618ms
  └─dbus.socket @10.556s
    └─sysinit.target @10.548s
      └─systemd-userdbd.service @31.778s +78ms
        └─systemd-userdbd.socket @4.150s
          └─system.slice
            └─-.slice
```

В выводе можно увидеть цепочку событий, отсортированных по времени (когда служба стала активной) в порядке убывания.

Значение после символа «**@**» в каждом событии - это время, когда служба стала активной.

Значение после символа «**+**» в каждом блоке показывает время, которое потребовалось для запуска службы.

Из полученной выше информации можно установить, какие службы запускаются дольше и, в свою очередь, вызывают медленную загрузку системы.

Такие службы можно отключить, если они не требуются для запуска при загрузке. Кроме того, можно отключить все службы, которые занимают меньше времени, но не требуются при загрузке, поскольку они также влияют на время загрузки системы.

Для того чтобы отключить какую-либо службу, необходимо выполнить следующую команду:

```
systemctl disable <имя_службы>
```

Systemd-analyze также позволяет получить и другие данные о состоянии и трассировке системы. Для ознакомления с дополнительной информацией о работе с утилитой и ее возможностях просмотрите справку:

```
man systemd-analyze
```

Pidstat — утилита для мониторинга и отчётности по статистике производительности процессов

Установка
Синтаксис
Параметры
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: sysstat-12.3.1-1

Pidstat (Process ID Statistic) — утилита, используемая для мониторинга и отчётности по статистике производительности процессов. Она может контролировать либо конкретный процесс, либо все запущенные процессы в системе.

Установка

Утилита **pidstat** входит в пакет **sysstat**, для установки выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install sysstat
```

Дальнейшая работа в программе производится с правами непривилегированного пользователя. Для получения дополнительной информации выполните команду:

```
man pidstat
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
pidstat [<параметры> ] [ <интервал> [ <счётчик> ] ] [ -e <программа> <аргументы> ]
```

Параметры

Основные параметры утилиты:

-d — вывод статистики ввода вывода;

-H — отображение статистики ввода/вывода с использованием удобного формата;

-h — справка;

-I — статистика прерываний;

-l — вывод пути до программы.

-R — статистика страниц памяти;

-r — вывод статистики сбоя страниц и использования памяти;

-s — статистика операций записи;

-t — статистика по зависимым процессам в формате дерева;

-U [<имя_пользователя>] — статистика процессов, принадлежащих указанному пользователю;

-u — статистика процессов в режиме пользователя;

-V — версия программы;

-v — вывод подробной статистики процессов;

-w — статистика процессов, которые находятся в состоянии ожидания;

-C <команда> — статистика процессов, запущенных с указанной командой;

-G <имя_процесса> — вывод статистики по имени процесса;

-p { <идентификатор_процесса> [,...] | SELF | ALL } — вывод статистики для выбранного процесса;

-T { TASK | CHILD | ALL } — статистика процессов в зависимости от типа (задача, дочерний процесс или все процессы);

--dec={ 0 | 1 | 2 } — устанавливает формат вывода чисел (0 - по умолчанию, 1 - с запятой, 2 - с точкой);

--human — вывод статистики в удобном формате.

Пример работы

1. Команда для вывода статистики по всем процессам:

```
pidstat -p ALL
```

Результат:

```
[user@localhost ~]$ pidstat -p ALL
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:48:51      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:48:51        0         1    0,03    0,03    0,00    0,02    0,06     1  systemd
23:48:51        0         2    0,00    0,00    0,00    0,00    0,00     1  kthreadd
23:48:51        0         3    0,00    0,00    0,00    0,00    0,00     0  pool_workqueue_release
23:48:51        0         4    0,00    0,00    0,00    0,00    0,00     0  kworker/R-rcu_g
23:48:51        0         5    0,00    0,00    0,00    0,00    0,00     0  kworker/R-rcu_p
23:48:51        0         6    0,00    0,00    0,00    0,00    0,00     0  kworker/R-slub_
23:48:51        0         7    0,00    0,00    0,00    0,00    0,00     0  kworker/R-netns
23:48:51        0        10    0,00    0,00    0,00    0,00    0,00     0  kworker/0:0H-events_highpri
23:48:51        0        11    0,00    0,00    0,00    0,00    0,00     0  kworker/u4:0-ext4-rsv-conversion
23:48:51        0        12    0,00    0,00    0,00    0,00    0,00     0  kworker/R-mm_pe
23:48:51        0        13    0,00    0,00    0,00    0,00    0,00     0  rcu_tasks_kthread
23:48:51        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:48:51        0        15    0,00    0,00    0,00    0,00    0,00     0  rcu_tasks_trace_kthread
23:48:51        0        16    0,00    0,00    0,00    0,00    0,00     0  ksoftirqd/0
23:48:51        0        17    0,00    0,01    0,00    0,05    0,01     0  rcu_preempt
23:48:51        0        18    0,00    0,00    0,00    0,00    0,00     0  migration/0
23:48:51        0        19    0,00    0,00    0,00    0,00    0,00     0  idle_inject/0
```

где:

- **UID** — идентификатор пользователя, от имени которого работает процесс;
- **PID** — идентификационный номер отслеживаемой задачи (процесса);
- **%usr** — процент ресурсов процессора, затраченных на выполнение пользовательских приложений;
- **%system** — процент ресурсов процессора, затраченных выполнение системных задач;
- **%guest** — процент ресурсов процессора, затраченных на работу виртуального процессора;
- **%wait** — процент ресурсов процессора, израсходованных задачей во время ожидания запуска;
- **%CPU** — общий процент процессорного времени, используемого задачей;
- **CPU** — номер процессора, к которому привязана задача;
- **Command** — имя команды процесса.

2. Вывод статистики о работе определённого процесса 6 раз каждые 5 секунд:

```
pidstat -p 14 5 6
```

Результат:

```
[user@localhost ~]$ pidstat -p 14 5 6
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:51:59      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:52:04        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:09        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:14        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:19        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:24        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:29        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
Среднее:        0        14    0,00    0,00    0,00    0,00    0,00     -  rcu_tasks_rude_kthread
```

3. Вывод статистики процесса по имени:

```
pidstat -C 'kworker'
```

Результат:

```
[user@localhost ~]$ pidstat -C 'kworker'
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:58:03      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:58:03        0        11    0,00    0,00    0,00    0,00    0,00     0  kworker/u4:0-ext4-rsv-conversion
23:58:03        0        28    0,00    0,00    0,00    0,00    0,00     1  kworker/u6:0-events_unbound
23:58:03        0        53    0,00    0,00    0,00    0,00    0,00     0  kworker/0:1H-kblockd
23:58:03        0        67    0,00    0,02    0,00    0,01    0,02     1  kworker/1:2-events
23:58:03        0       221    0,00    0,00    0,00    0,00    0,00     1  kworker/1:1H-kblockd
23:58:03        0       448    0,00    0,01    0,00    0,02    0,01     0  kworker/0:5-events
23:58:03        0      2452    0,00    0,00    0,00    0,00    0,00     1  kworker/u5:4-flush-8:0
23:58:03        0      2512    0,00    0,00    0,00    0,00    0,00     0  kworker/u5:0-events_unbound
23:58:03        0      2658    0,00    0,00    0,00    0,00    0,00     1  kworker/u6:3-flush-8:0
23:58:03        0      3138    0,00    0,00    0,00    0,00    0,00     1  kworker/1:0-ata_sff
```

4. Статистика ввода-вывода (I/O) для процесса с PID 14, обновляемая каждую секунду:

```
pidstat -p 14 -d 1
```

Результат:

```
[user@localhost ~]$ pidstat -p 14 -d 1
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:59:57      UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
23:59:58        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
23:59:59        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:00        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:01        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:02        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:03        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:04        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:05        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:06        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
```

где:

- **kB_rd/s** — скорость (КБ в секунду), с которой процесс читает с диска;
- **kB_wr/s** — скорость (КБ в секунду), с которой процесс записывает на диск;
- **kB_ccwr/s** — скорость (КБ в секунду), с которой запись на диск была отменена процессом;
- **Iodelay** — задержка ввода/вывода блока контролируемого процесса, измеряемая в тактах.

5. Сбор и вывод статистики по свободной и занятой памяти:

```
pidstat -p 14 -r 1
```

Результат:

```
[user@localhost ~]$ pidstat -p 14 -r 1
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:02:25      UID       PID  minflt/s  majflt/s     VSZ     RSS   %MEM  Command
00:02:26        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:27        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:28        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:29        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:30        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:31        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:32        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:33        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:34        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:35        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:36        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:37        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
```

где:

- **minflt/s** — общее количество незначительных ошибок, совершенных процессом за секунду, которые не требовали загрузки страницы памяти с диска;
- **majflt/s** — общее количество значительных ошибок, совершенных процессом за секунду, которые требовали загрузки страницы памяти с диска;
- **VSZ** — виртуальная память (КБ), используемая задачей;
- **RSS** — физическая память (КБ), используемая задачей;
- **%MEM** — процент доступной физической памяти, используемой процессором.

6. Вывод статистики производительности всех процессов, имя которых содержит org_kde_powerde (заменить на необходимое):

```
pidstat -C org_kde_powerde -l
```

Результат:

```
[user@localhost ~]$ pidstat -C org_kde_powerde -l
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:19:30      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
00:19:30     1000      2368    0,01    0,01    0,00    0,05    0,02     0  /usr/libexec/org_kde_powerdevil
[user@localhost ~]$ pidstat -C dnfdragora-upda -l
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:20:45      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
00:20:45     1000      2169    0,02    0,01    0,00    0,02    0,03     1  /usr/bin/python3 /usr/bin/dnfdragora-updater --qt
```

7. Вывод статистики по родительским и дочерним процессам:

```
pidstat -T CHILD
```

Результат:

```
[user@localhost ~]$ pidstat -T CHILD
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:15:13      UID       PID    usr-ms system-ms  guest-ms  Command
00:15:13        0         1      4900      4870         0  systemd
00:15:13        0        11         0        20         0  kworker/u4:0-ext4-rsv-conversion
00:15:13        0        16         0        40         0  ksoftirqd/0
00:15:13        0        17         0       320         0  rcu_preempt
00:15:13        0        18         0        10         0  migration/0
00:15:13        0        23       140         0         0  migration/1
00:15:13        0        24         0        40         0  ksoftirqd/1
00:15:13        0        37         0        40         0  kcompactd0
00:15:13        0        53         0       110         0  kworker/0:1H-kblockd
00:15:13        0        54         0       100         0  kswapd0
00:15:13        0        67         0      1010         0  kworker/1:2-events
00:15:13        0       221         0        80         0  kworker/1:1H-kblockd
00:15:13        0       301         0        10         0  scsi_eh_1
```

где:

- **usr-ms** — общее количество миллисекунд, затраченных процессом и его производными на пользовательские задачи;

- **system-ms** — общее количество миллисекунд, затраченных процессом и его производными на системные задачи;
- **guest-ms** — общее количество миллисекунд, затраченных процессом и его производными на задачи виртуальной машины.

8. Вывод статистики в формате дерева:

```
pidstat -t
```

Результат:

```
[user@localhost ~]$ pidstat -t
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:16:33      UID      TGID       TID    %usr %system  %guest   %wait    %CPU   CPU  Command
00:16:33        0         1         -    0,02    0,02    0,00    0,02    0,04     1  systemd
00:16:33        0         -         1    0,02    0,02    0,00    0,02    0,04     1  |__systemd
00:16:33        0        11         -    0,00    0,00    0,00    0,00    0,00     0  kworker/u4:0-ext4-rsv-conversion
00:16:33        0         -        11    0,00    0,00    0,00    0,00    0,00     0  |__kworker/u4:0-ext4-rsv-conversion
00:16:33        0        16         -    0,00    0,00    0,00    0,00    0,00     0  ksoftirqd/0
00:16:33        0         -        16    0,00    0,00    0,00    0,00    0,00     0  |__ksoftirqd/0
00:16:33        0        17         -    0,00    0,01    0,00    0,05    0,01     0  rcu_preempt
00:16:33        0         -        17    0,00    0,01    0,00    0,05    0,01     0  |__rcu_preempt
00:16:33        0        18         -    0,00    0,00    0,00    0,00    0,00     0  migration/0
00:16:33        0         -        18    0,00    0,00    0,00    0,00    0,00     0  |__migration/0
00:16:33        0        23         -    0,00    0,00    0,00    0,00    0,00     1  migration/1
00:16:33        0         -        23    0,00    0,00    0,00    0,00    0,00     1  |__migration/1
00:16:33        0        24         -    0,00    0,00    0,00    0,00    0,00     1  ksoftirqd/1
00:16:33        0         -        24    0,00    0,00    0,00    0,00    0,00     1  |__ksoftirqd/1
```

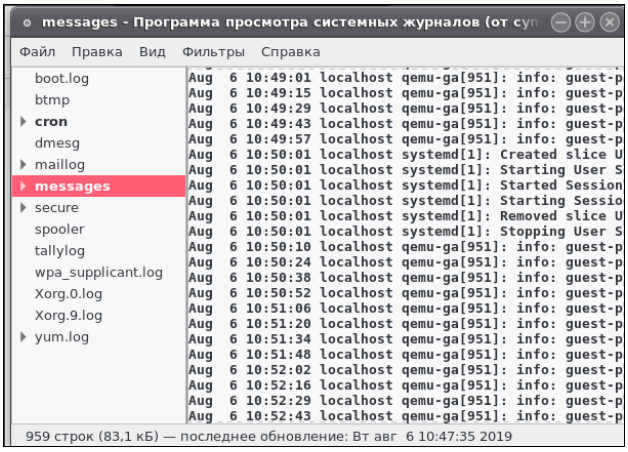
где:

- **TGID** — идентификационный номер главного процесса;
- **TID** — идентификационный номер контролируемого процесса.

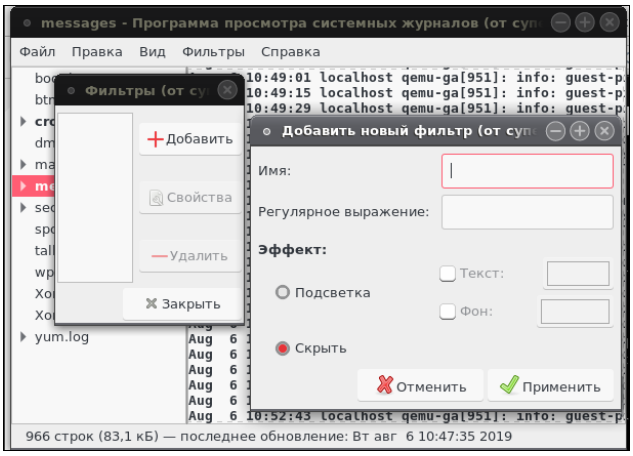
Просмотр системных журналов с помощью графического интерфейса

При работе в **РЕД ОС 7.3 и выше (Mate)** для просмотра системных логов требуется открыть **«Меню» -> «Системные» -> «Просмотр системных журналов»**.

После ввода root-пароля откроется следующее окно:



Здесь можно выбрать нужный вам раздел, также здесь присутствуют фильтры, которые можно настроить под свой запрос:



Утилита tail

tail — это утилита, используемая для вывода N-го количества последних строк файла. Обычно она показывает в стандартном выводе 10 последних строк. Команда tail позволяет также выводить новые строки в интерактивном режиме. Вывод последних 10 строк файла производится следующей командой:

```
tail /var/log/messages

Jun 4 11:29:02 localhost gdm-Xorg-:0[1338]: (EE) No surface to present from.
Jun 4 11:29:04 localhost journal[2595]: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
Jun 4 11:29:34 localhost systemd[1]: Starting Fingerprint Authentication Daemon...
Jun 4 11:29:34 localhost systemd[1]: Started Fingerprint Authentication Daemon.
Jun 4 11:29:34 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Jun 4 11:29:39 localhost audit[2641]: USER_AUTH pid=2641 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success'
Jun 4 11:29:39 localhost audit[2641]: USER_ACCT pid=2641 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success'
Jun 4 11:29:39 localhost audit[2641]: CRED_ACQ pid=2641 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success'
Jun 4 11:29:39 localhost su[2641]: (to root) user on pts/0
Jun 4 11:29:39 localhost audit[2641]: USER_START pid=2641 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/0 res=success'
```

Увеличить количество выводимых строк можно с помощью опции -n:

```
tail -n 100 /var/log/messages

Jun 4 11:28:04 localhost systemd[1367]: Closed Sound System.
Jun 4 11:28:04 localhost systemd[1367]: Stopping D-Bus User Message Bus...
Jun 4 11:28:04 localhost systemd[1367]: systemd-tmpfiles-setup.service: Succeeded.
Jun 4 11:28:04 localhost systemd[1367]: Stopped Create User's Volatile Files and Directories.
Jun 4 11:28:04 localhost dbus-broker[1387]: Dispatched 26 messages @ 78(±172)µs / message.
Jun 4 11:28:04 localhost systemd[1367]: dbus-broker.service: Succeeded.
Jun 4 11:28:04 localhost systemd[1367]: Stopped D-Bus User Message Bus.
...
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (DB) vmware(0): New layout.
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (DB) vmware(0): 0: 0 0 1356 797
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (DB) vmware(0):
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (EE) No surface to present from.
Jun 4 11:30:55 localhost systemd[1742]: dbus-:1.2-org.freedesktop.Notifications@1.service: Succeeded.
Jun 4 11:32:37 localhost /etc/gdm/Xsession[2726]: [2726:2726:0723/113237.473025:ERROR:shared_image_manager.cc(214)] SharedImageManager::ProduceSkia: Trying to Produce a Skia representation from a non-existent mailbox.
```

Для просмотра логов в реальном времени используется опция -f:

```
tail -f /var/log/messages

Jun 4 11:30:44 localhost gdm-Xorg-:0[1338]: (EE) No surface to present from.
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (DB) vmware(0): New layout.
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (DB) vmware(0): 0: 0 0 1356 797
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (DB) vmware(0):
Jun 4 11:30:46 localhost gdm-Xorg-:0[1338]: (EE) No surface to present from.
Jun 4 11:30:55 localhost systemd[1742]: dbus-:1.2-org.freedesktop.Notifications@1.service: Succeeded.
Jun 4 11:32:37 localhost /etc/gdm/Xsession[2726]: [2726:2726:0723/113237.473025:ERROR:shared_image_manager.cc(214)] SharedImageManager::ProduceSkia: Trying to Produce a Skia representation from a non-existent mailbox.
Jun 4 11:33:51 localhost systemd[1742]: Starting Cleanup of User's Temporary Files and Directories...
Jun 4 11:33:51 localhost systemd[1742]: systemd-tmpfiles-clean.service: Succeeded.
Jun 4 11:33:51 localhost systemd[1742]: Finished Cleanup of User's Temporary Files and Directories.
```

Вы можете открыть несколько файлов одновременно, перечислив их в параметрах:

```
tail /var/log/messages /var/log/Xorg.0.log
```

```
[root@localhost user]# tail /var/log/messages /var/log/Xorg.0.log
==> /var/log/messages <==
Jun  4 13:50:23 localhost su[2651]: (to root) user on pts/0
Jun  4 13:50:51 localhost journal[2652]: No devices in use, exit
Jun  4 13:59:33 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input13
Jun  4 14:00:05 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input14
Jun  4 14:00:08 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input15
Jun  4 14:00:14 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input16
Jun  4 14:00:23 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input17
Jun  4 14:00:46 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input18
Jun  4 14:00:53 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input19
Jun  4 14:01:08 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input20

==> /var/log/Xorg.0.log <==
[  1883.971] (**) spice vdagent tablet: (accel) keeping acceleration scheme 1
[  1883.971] (**) spice vdagent tablet: (accel) acceleration profile 0
[  1883.971] (**) spice vdagent tablet: (accel) acceleration factor: 2.000
[  1883.971] (**) spice vdagent tablet: (accel) acceleration threshold: 4
[  1883.972] (II) config/udev: Adding input device spice vdagent tablet (/dev/input/js0)
[  1883.972] (II) No input driver specified, ignoring this device.
[  1883.972] (II) This device may have been added with another device file.
[  1884.411] AUDIT: Fri Jun  4 14:01:09 2021: 833: client 41 connected from local host ( uid=1000 gid
=1000 pid=1550 )
  Auth name: MIT-MAGIC-COOKIE-1 ID: 643
[  1884.422] AUDIT: Fri Jun  4 14:01:09 2021: 833: client 41 disconnected
```

Для удобства, вы можете выбирать не все строки, а отфильтровать интересующие вас с помощью опции grep:

```
tail /var/log/messages | grep s
```

```
[root@localhost user]# tail /var/log/messages | grep s
Jun  4 13:50:23 localhost su[2651]: (to root) user on pts/0
Jun  4 13:50:51 localhost journal[2652]: No devices in use, exit
Jun  4 13:59:33 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input13
Jun  4 14:00:05 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input14
Jun  4 14:00:08 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input15
Jun  4 14:00:14 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input16
Jun  4 14:00:23 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input17
Jun  4 14:00:46 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input18
Jun  4 14:00:53 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input19
Jun  4 14:01:08 localhost kernel: input: spice vdagent tablet as /devices/virtual/input/input20
```

Основные опции tail

- *-c* - выводить указанное количество байт с конца файла;
- *-f* - обновлять информацию по мере появления новых строк в файле;
- *-n* - выводить указанное количество строк из конца файла;
- *--pid* - используется с опцией -f, позволяет завершить работу утилиты, когда завершится указанный процесс;
- *-q* - не выводить имена файлов;
- *--retry* - повторять попытки открыть файл, если он недоступен;
- *-v* - выводить подробную информацию о файле.

Утилита less

less - утилита командной строки, которая отображает содержимое файла или вывод команды по одной странице за раз.

Открыть содержимое файла можно следующей командой:

```
less /var/log/Xorg.0.log
 X.Org X Server 1.20.9
 X Protocol Version 11, Revision 0
 [    83.753] Build Operating System: RED OS  [    83.753] Current Operating System: Linux localhost.localdomain 5.10.29-1.el7.x86_64 #1 SMP Mon Apr 12 13:55:18 MSK 2021 x86_64 [    83.753] Kernel command line: BOOT_IMAGE=/vmlinuz-5.10.29-1.el7.x86_64 root=/dev/mapper/ro_redos-root ro resume=/dev/mapper/ro_redos-swap rd.lvm.lv=ro_redos/root rd.lvm.lv=ro_redos/swap rhgb quiet [    83.754] Build Date: 28 November 2020  03:39:28PM [    83.754] Build ID: xorg-x11-server 1.20.9-7.el7  [    83.754] Current version of pixman: 0.40.0 [    83.754]    Before reporting problems, check http://wiki.x.org        to make sure that you have the latest version. [    83.754] Markers: (--) probed, (**) from config file, (==) default setting,        (++) from command line, (!!) notice, (II) informational,        (WW) warning, (EE) error, (NI) not implemented, (??) unknown. [    83.757] (==) Log file: "/var/log/Xorg.9.log", Time: Mon May 31 10:31:52 202 1 [    83.875] (==) Using config directory: "/etc/X11/xorg.conf.d" [    83.875] (==) Using system config directory "/usr/share/X11/xorg.conf.d" [    83.994] (==) No Layout section.  Using the first Screen section. [    83.994] (==) No screen section available. Using defaults....
```

Командная строка исчезнет, а в окне терминала откроется указанный вами документ. После этого его можно читать, пользуясь для прокручивания строк вперед и назад клавишами **Enter** и **Y**.

Внизу окна вы увидите поле с мигающим курсором — здесь можно напечатать какую-либо внутреннюю команду, например, задать утилите паттерн поиска.

Для открытия файла могут задаваться определённые опции, их список представлен ниже:

- *-a* — не осуществлять поиск в тексте, который в данный момент отображен на экране;
- *-bn* — задать размер буфера памяти;
- *-c* — листать текст, полностью стирая содержимое экрана (построчная прокрутка работать не будет);
- *-Dxcolor, --color=xcolor* — задать цвет отображаемого текста;
- *-E* — выйти, когда утилита достигнет конца файла;
- *-e* — выйти, когда утилита второй раз достигнет конца файла;
- *-F* — выйти, если содержимое файла помещается на одном экране;
- *-f* — открыть специальный файл;
- *-hn* — задать максимальное количество строк для прокрутки назад;
- *-yn* — задать максимальное количество строк для прокрутки вперёд;
- *-i* — игнорировать регистр;
- *-I* — игнорировать регистр, даже если паттерн для поиска содержит заглавные буквы;
- *-jn* — указать, в какой строке должна быть выведена искомая информация;
- *-J* — пометить строки, соответствующие результатам поиска;
- *-n* — не выводить номера строк;
- *-N* — вывести номера строк;
- *-s* — заменить множество идущих подряд пустых строк одной пустой строкой;
- *-w* — выделить первую строку нового фрагмента текста.

Если вам нужно найти то или иное слово, напечатайте в поле с мигающим курсором **/текст** (для поиска вниз по тексту) или **?текст** (чтобы выполнить поиск вверх по тексту) и нажмите **Enter**:

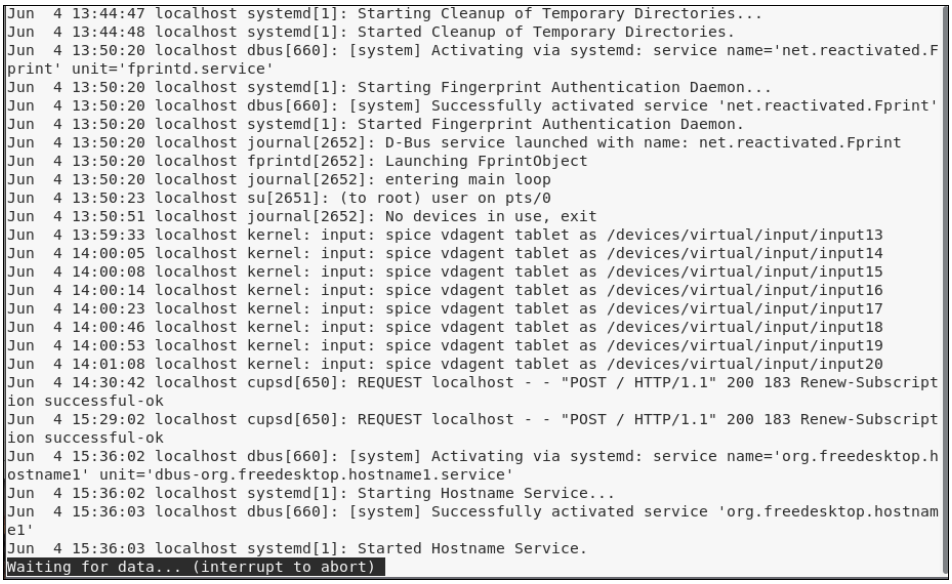
```
[    24.500] (II) config/udev: Adding input device VirtualPS/2 VMware VMMouse (/dev/input/event3)
[    24.500] (**) VirtualPS/2 VMware VMMouse: Applying InputClass "evdev pointer catchall"
[    24.500] (II) Using input driver 'evdev' for 'VirtualPS/2 VMware VMMouse'
[    24.500] (**) VirtualPS/2 VMware VMMouse: always reports core events
[    24.500] (**) evdev: VirtualPS/2 VMware VMMouse: Device: "/dev/input/event3"
[    24.500] (--) evdev: VirtualPS/2 VMware VMMouse: Vendor 0x2 Product 0x13
[    24.500] (--) evdev: VirtualPS/2 VMware VMMouse: Found 3 mouse buttons
[    24.500] (--) evdev: VirtualPS/2 VMware VMMouse: Found scroll wheel(s)
[    24.500] (--) evdev: VirtualPS/2 VMware VMMouse: Found relative axes
[    24.500] (--) evdev: VirtualPS/2 VMware VMMouse: Found x and y relative axes
[    24.500] (II) evdev: VirtualPS/2 VMware VMMouse: Configuring as mouse
[    24.500] (II) evdev: VirtualPS/2 VMware VMMouse: Adding scrollwheel support
[    24.500] (**) evdev: VirtualPS/2 VMware VMMouse: YAxisMapping: buttons 4 and 5
[    24.500] (**) evdev: VirtualPS/2 VMware VMMouse: EmulateWheelButton: 4, EmulateWheelInertia: 10,
EmulateWheelTimeout: 200
[    24.500] (**) Option "config_info" "udev:/sys/devices/platform/i8042/serio1/input/input3/event3"
[    24.500] (II) XINPUT: Adding extended input device "VirtualPS/2 VMware VMMouse" (type: MOUSE, id
8)
[    24.501] (II) evdev: VirtualPS/2 VMware VMMouse: initialized for relative axes.
[    24.501] (**) VirtualPS/2 VMware VMMouse: (accel) keeping acceleration scheme 1
[    24.501] (**) VirtualPS/2 VMware VMMouse: (accel) acceleration profile 0
[    24.501] (**) VirtualPS/2 VMware VMMouse: (accel) acceleration factor: 2.000
[    24.501] (**) VirtualPS/2 VMware VMMouse: (accel) acceleration threshold: 4
[    24.501] (II) config/udev: Adding input device VirtualPS/2 VMware VMMouse (/dev/input/mouse1)
[    24.501] (II) No input driver specified, ignoring this device.
[    24.501] (II) This device may have been added with another device file.
[    24.501] (II) config/udev: Adding input device VirtualPS/2 VMware VMMouse (/dev/input/event2)
[    24.501] (**) VirtualPS/2 VMware VMMouse: Applying InputClass "evdev pointer catchall"
[    24.501] (II) Using input driver 'evdev' for 'VirtualPS/2 VMware VMMouse'
[    24.501] (**) VirtualPS/2 VMware VMMouse: always reports core events
```

Less позволяет просматривать одновременно несколько файлов, переключаясь между ними, для этого нужно после команды less написать название двух файлов, чтобы просмотреть следующий файл, нажмите «:», а затем нажмите «n»:

```
less /var/log/Xorg.0.log /var/log/messages
```



Для просмотра содержимого файла изменений в режиме реального времени используется опция **+F**:



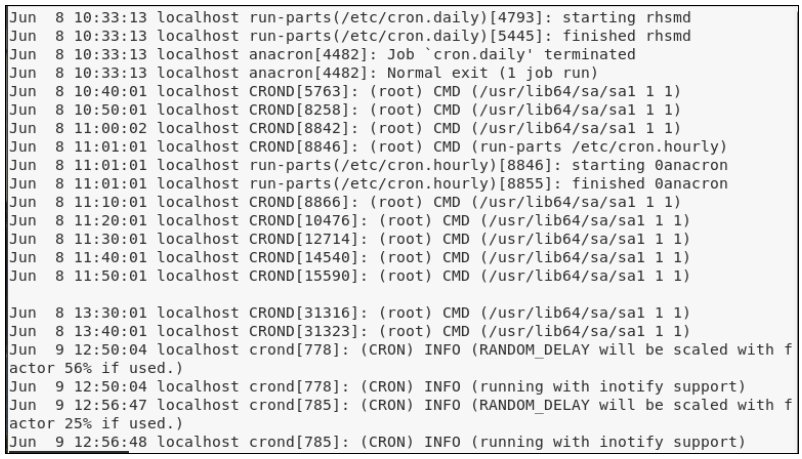
При открытии файла с большим количеством текста в нём могут встречаться множество идущих подряд пустых строк, для примера откроем такой файл без опций:

```
less  /var/log/log
```



При открытии с опцией -s, множество пробелов сокращается до одного пробела между строками:

```
less -s /var/log/log
```



Во время просмотра содержимого файла утилитой можно управлять при помощи внутренних команд, набирая их на клавиатуре. Наиболее часто используемые из них:

- *h, H* — справка;
- *Space, Ctrl+V, f, Ctrl+F* — прокрутить текст на один экран вперёд;
- *Enter, Return, Ctrl+N, e, Ctrl+E, j, Ctrl+J* — прокрутить текст на n строк вперед, по умолчанию n=1;
- *y, Ctrl+Y, Ctrl+P, k, Ctrl+K* — прокрутить текст на n строк назад, по умолчанию n=1;
- *Ctrl+→* — прокрутить текст по горизонтали в конец строки;
- *Ctrl+←* — прокрутить текст по горизонтали в начало строки;
- *:d* — удалить текущий файл из списка файлов;
- *Ctrl+G, :f* — вывести основную информацию о файле;
- *q, Q, :q, :Q, ZZ* — выход.

Настройка журналов с помощью утилиты journalctl

Ограничение размера журнала
Удаление журналов
Вывод лога в текстовый файл
Фильтрация по приоритету
Сокращение или расширение области вывода
Запись логов в стандартный вывод
Справка по утилите

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с работой утилиты **journalctl**, просмотрев наши обучающие видео:

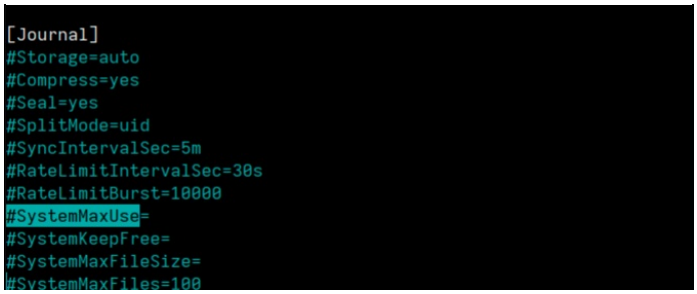
- на **RuTube** — Работа с журналами в РЕД ОС. Journalctl;
- в **Яндекс.Дзен** — Работа с журналами в РЕД ОС. Journalctl;
- в **VK Видео** — Работа с журналами в РЕД ОС. Journalctl.

На наших каналах вы также сможете найти много другой полезной информации.

Ограничение размера журнала

Если **journald** настроен, чтобы сохранять журналы после перезагрузки, то по умолчанию размер журнала ограничен 10% от объема файлового раздела и максимально может занять 4 Гб дискового пространства.

Максимальный объем журнала можно скорректировать, раскомментировав и отредактировав следующий параметр в файле конфигурации **/etc/systemd/journald.conf**.



В блоке **[journal]** надо изменить параметр **SystemMaxUse**, например **SystemMaxUse=50M**. Допустимые обозначения единиц - **K, M, G, T, P, E**.

Удаление журналов и определение текущего использования дискового пространства

Удалить файлы архивных журналов, можно вручную с помощью rm или использовать **journalctl**.

Удалить журналы, оставив только последние *100 Мб*:

```
journalctl --vacuum-size=100M
```

Удалить журналы, оставив журналы только за последние *7 дней*:

```
journalctl --vacuum-time=7d
```

Определить, сколько места занимает журнал на диске, используя флаг *--disk-usage*:

```
journalctl --disk-usage
```

Вывод лога в текстовый файл

Если необходимо вывести лог в текстовый формат, используйте конструкцию `<команда> > <путь_к_текстовому_файлу>`

Например:

```
journalctl -b > /home/user/loginfo.log
```

Фильтрация по приоритету

Фильтрация может применяться к приоритету сообщения, если вы хотите отфильтровать конкретное сообщение, такое как “**warning**” или “**error**” и т.д.

В таблице ниже перечислены все уровни приоритета:

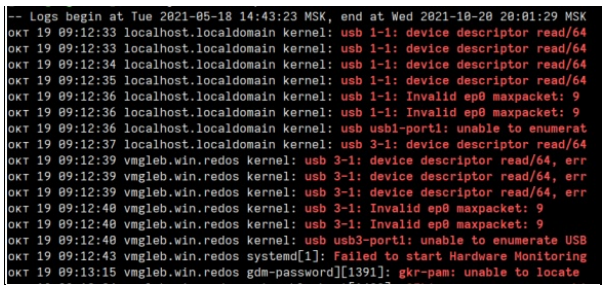
Приоритет	Код
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

Например:

```
journalctl -p 3 –b
```

или

```
sudo journalctl -p err –b
```

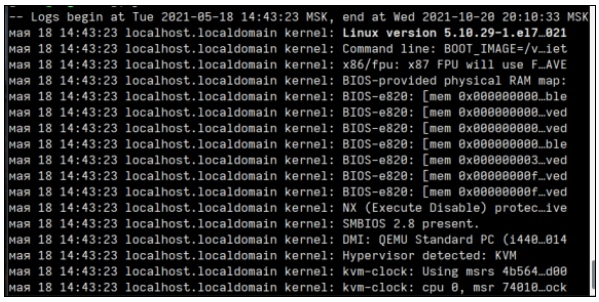


Сокращение или расширение области вывода

По умолчанию **journalctl** выводит на страничном модуле всю запись целиком так, что записи доходят до правого края экрана. Если вы предпочитаете урезать вывод, где удалена информация, вы можете использовать опцию **--no-full**.

Например:

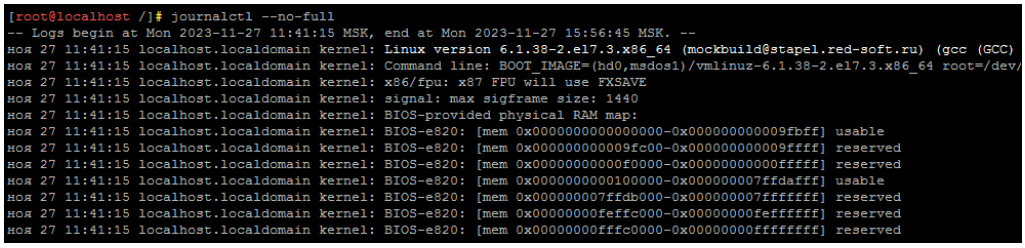
```
journalctl --no-full
```



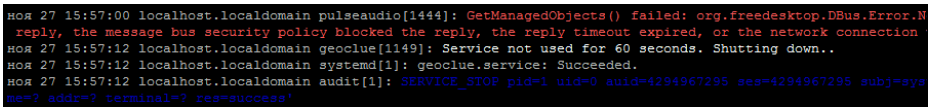
Запись логов в стандартный вывод

По умолчанию **journalctl** использует для вывода утилиту **less**. В этом случае к данным нельзя применять стандартные утилиты для обработки текстовых данных. При добавлении опции `--no-pager` все сообщения будут записываться в стандартный вывод.

Например:



С добавлением опции `--no-pager`:



Справка по утилите

Получить актуальные ключи команды:

```
journalctl --help
```

Чтение всех логов:

```
journalctl
```

Логи с момента запуска системы:

```
journalctl -b
```

Показывать записи журнала с момента запуска системы с расшифровкой ошибок:

```
journalctl -xb
```

Показать самые последние записи журнала и продолжать печатать новые записи при добавлении их в журнал:

```
journalctl -f
```

Просмотр информации о недавних событиях:

```
journalctl -n
```

По умолчанию на консоль выводится информация о последних 10 событиях. С опцией `-n` можно указать необходимое число событий:

```
journalctl -n 20
```

Для фильтрации по дате и времени важны два ключа

- `--since` - вывод от такого-то момента времени;
- `--until` - вывод до такого-то момента времени.

В качестве значений для этих ключей могут использоваться:

- Формат **YYYY-MM-DD HH:MM:SS**:

```
journalctl --since "2019-05-05 00:01" --until "2019-05-06 01:40"
```

- Слова «**yesterday**», «**today**», «**tomorrow**», «**now**»:

```
journalctl --since "yesterday" --until "2019-05-06 01:40"
```

Показывать в реальном времени все записи, независимо от их размера и кодировки:

```
journalctl -af
```

Просмотр сообщений ядра:

```
journalctl -k
```

Все сообщение конкретной утилиты, например, **systemd**:

```
journalctl /usr/lib/systemd/systemd
```

Все сообщения конкретного процесса:

```
journalctl _PID=1
```

Все сообщения конкретного приложения или службы:

```
journalctl -u netcfg
```

Все сообщения процессов, запущенных от имени конкретного пользователя:

```
journalctl _UID=33
```

Для справки в таблице ниже приведено расположение файлов журналов некоторых наиболее часто используемых служб:

Сервис	Путь
WEB-сервер Apache	/var/log/httpd/
Система управления печатью Cups	/var/log/cups/
Антивирус kaspersky	/var/log/kaspersky/
Системный журнал Syslog	/var/log/anaconda/syslog*
Samba	/var/log/samba/
X server	/var/log/Xorg.*.log
Графический менеджер gdm	/var/log/gdm/
Основной список логов	/var/log/messages

Средство просмотра журналов Log File Navigator (LNAV)

Установка и запуск
Параметры
Синтаксис
Навигация
Фильтры

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** lnav-0.9.0-1

lnav (**Log File Navigator**) - является расширенным средством просмотра файлов журналов, которое использует любую семантическую информацию, которую можно почерпнуть из просматриваемых файлов, таких как отметки времени и уровни журналов. Используя эту дополнительную семантическую информацию, *lnav* может делать такие вещи, как чередование сообщений из разных файлов, генерация гистограмм сообщений с течением времени и предоставление горячих клавиш для навигации по файлу.

Навигатор журналов *lnav* понимает ряд форматов файлов:

- */var/log/messages* - глобальный системный журнал, в котором пишутся сообщения с момента запуска системы, от ядра Linux, различных служб, обнаруженных устройств, сетевых интерфейсов и много другого;
- */var/log/secure* — информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации;
- */var/log/dmesg* — информация о драйверах устройств. Одноименной командой можно просмотреть вывод содержимого файла. Размер журнала ограничен; когда файл достигнет своего предела, старые сообщения будут перезаписаны более новыми;
- */var/log/anaconda/anaconda.log* — записи, зарегистрированные во время установки системы;
- */var/log/audit/audit* — записи, созданные службой аудита **auditd**;
- */var/log/boot.log* — информация, которая пишется при загрузке операционной системы;
- */var/log/cron* — отчет службы **crond** об исполняемых командах и сообщения от самих команд;
- */var/log/cups* — информация обо всем, что связано с печатью и принтерами;
- */var/log/maillog/* — журнал почтового сервера, используемого на ОС;
- */var/log/samba/* — логи файлового сервера **Samba**, который используется для доступа к общим папкам Windows и предоставления доступа пользователям Windows к общим папкам Linux;
- */var/log/spooler* — для представителей старой школы, содержит сообщения **USENET**. Чаще всего бывает пустым и заброшенным;
- */var/log/Xorg.0.log* — логи X-сервера. Чаще всего бесполезны, но если в них есть строки начинающиеся с **EE**, то следует обратить на них внимание;
- */var/log/lastlog* — последняя сессия пользователей;
- произвольные записи с временными отметками;
- gzip, bzip;
- журнал VMWare ESXi/vCenter.

Установка и запуск

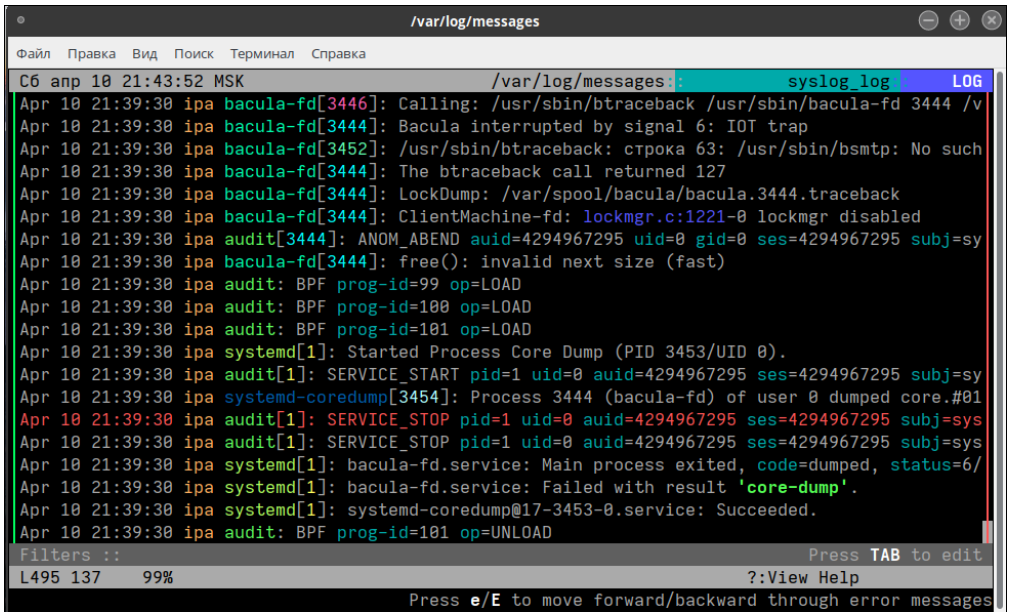
Для установки *lnav* выполните команду (потребуются права **администратора**):

```
sudo dnf install lnav
```

Дальнейшая работа с утилитой должна производиться с правами **администратора**, если не указано иное.

Запуск *lnav* производится командой:

```
lnav
```



При вводе команды без параметров *lnav* автоматически отображает информацию в реальном времени из файла */var/log/messages* на основе самых последних отметок времени из всех файлов журналов.

Параметры

Для того чтобы посмотреть информацию об отдельном файле, нужно использовать команду с определёнными параметрами (опциями). Список параметров представлен ниже:

- *-h* - распечатать сообщение и выйти;
- *-H* - показать на дисплее справку;
- *-I <путь>* - дополнительный каталог;
- *-i* - установить данный формат файла и выйти;
- *-C* - проверить конфигурацию и выйти;
- *-d <имя_файла>* - написать отладочные сообщения в указанный файл;
- *-V* - распечатать информацию версии;
- *-a* - загрузить самый последний файл журнала типов;
- *-r* - загрузка старого *rotated* журнала;
- *-t* - добавление метки к линиям данных, чтение в стандартном вводе;
- *-w <имя_файла>* - содержимое стандартного ввода в файл;
- *-c <команда>* - выполнить команду после того, как файлы были загружены;
- *-f <путь_к _файлу>* - выполнить команды в указанный файл;
- *-n* - работать без пользовательского интерфейса *UI*;
- *-q* - не печатать сообщения журнала после выполнения всех команд, или когда *lnav* читает из **stdin**;

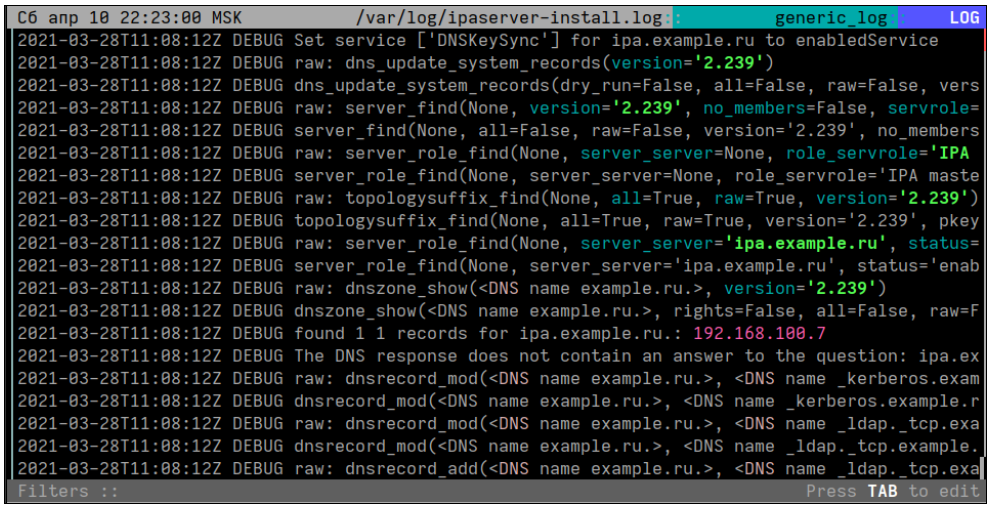
Синтаксис

Синтаксис утилиты выглядит следующим образом:

```
lnav <опция> <log_файл_1 log_файл_2 ...>
```

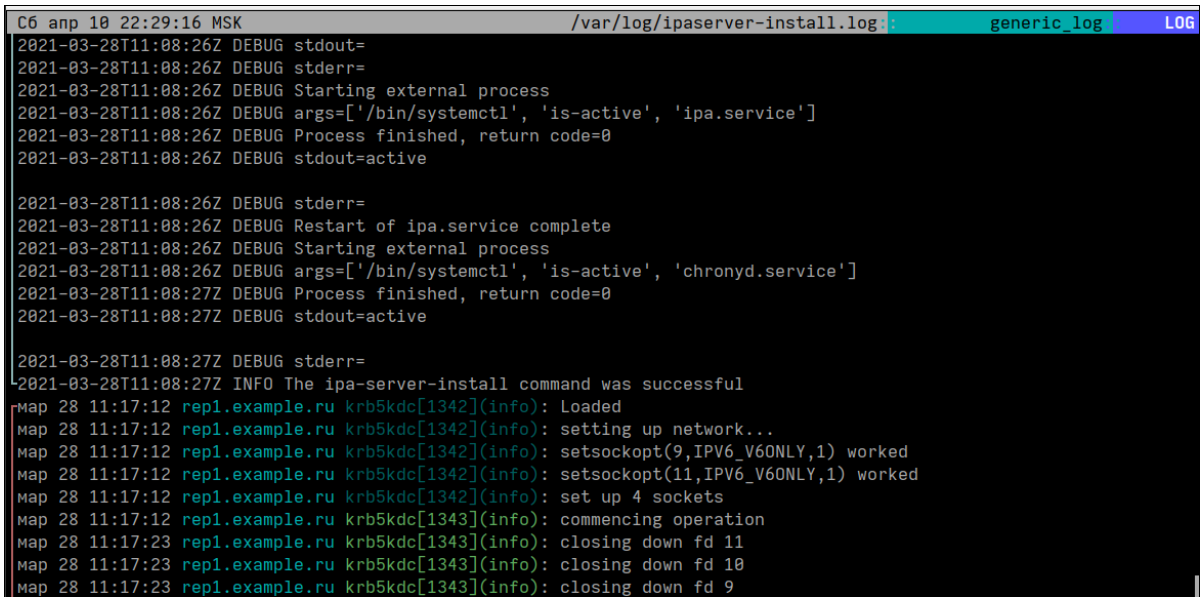
Например, просмотрим информацию из файла */var/log/ipaserver-install.log*:

```
lnav /var/log/ipaserver-install.log
```



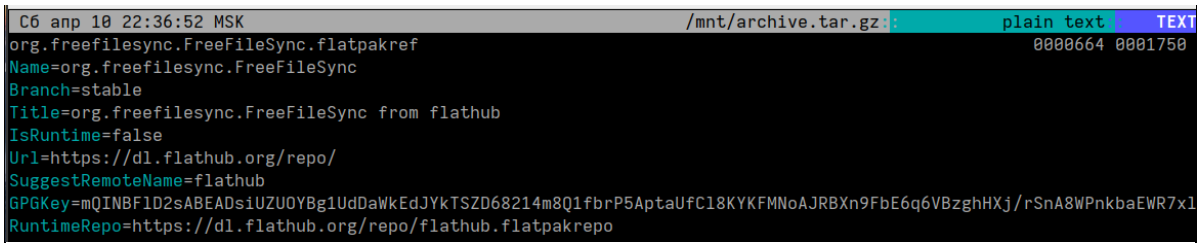
Так же в *lnav* можно открывать несколько файлов сразу и переключаться между ними:

```
lnav /var/log/ipaserver-install.log /var/log/krb5kdc.log
```

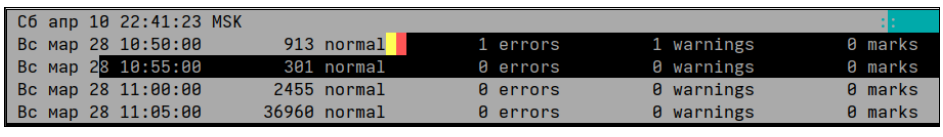


Программа умеет напрямую открывать архивный файл:

```
lnav -r /mnt/archive.tar.gz
```



Программа показывает гистограмму информативных сообщений, предупреждений и ошибок, если нажать клавишу «**i**»:



Навигация

Список горячих клавиш для работы с *lnav*:

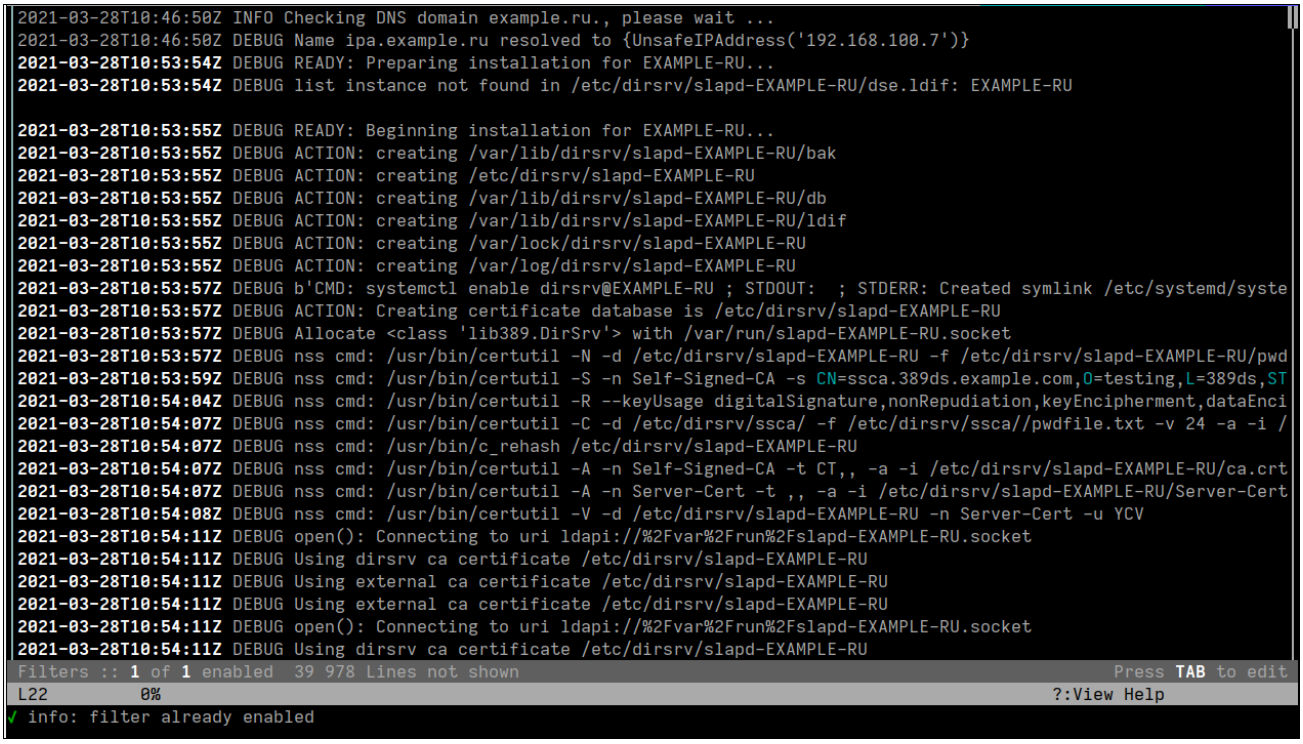
- *Shift + D* – вперед/назад на 24 часа;
- *Shift + [1-6]* – следующая/предыдущая *n*-я десятая минута часа;
- *Shift + 0* – следующий/предыдущий день;
- *Shift + R* – вперед/назад по относительному времени, которое в последний раз использовалось с командой **goto**;

- *M* – отметить/снять отметку с верхней строки;
- *Shift + M* – отметить/снять отметку с диапазона строк от последней отмеченной до верхней;
- *Shift + J* – отметить/снять отметку со следующей строки после ранее отмеченной;
- *Shift + W* – вернуться к предыдущему предупреждающему сообщению;
- *Shift + E* – перейти к последнему сообщению об ошибке;
- *Shift + K* – отметить/снять отметку с предыдущей строки;
- *C* – скопировать отмеченные строки в буфер обмена;
- *Shift + C* – очистить отмеченные линии;
- *?* – просмотр/выход из встроенной справки;
- *Q* – возврат к предыдущему виду/выход;
- *Shift + P* – переключится в/из отображаемого журнала или текстовых файлов;
- *Shift + T* – отображать прошедшее время между строками;
- *T* – переключиться в/из просмотра текстового файла;
- *I* – переключиться в/из просмотра гистограммы;
- *Shift + I* – переключиться в/из просмотра гистограммы;
- *V* – переключиться в/из представления результатов *sql*;
- *Shift + V* – переключиться в/из представления результатов *SQL* и перейти к соответствующему столбцу **log_line**;
- *P* – переключить отображение результата парсера журнала;
- *Tab* – циклический переход от столбцов к графику в представлении результатов *SQL*;
- *Ctrl + L* – переключиться в режим **li-fi**. Отображаемые строки журнала будут выгружены на терминал без каких-либо украшений, чтобы их можно было легко скопировать;
- */* - поиск регулярного выражения;
- *;* - выполнить SQL-запрос;
- *:* - выполнить внутреннюю команду;
- *Ctrl +]* – прервать.

Фильтры

Если вы хотите отображать только строки, соответствующие определенному шаблону, вы можете сделать это с помощью фильтров. Сначала войдите в командный режим, нажав двоеточие, а затем введите нужный текст с фильтром **filter-in**, чтобы отображались только строки, содержащие необходимый текст. Например:

filter-in example



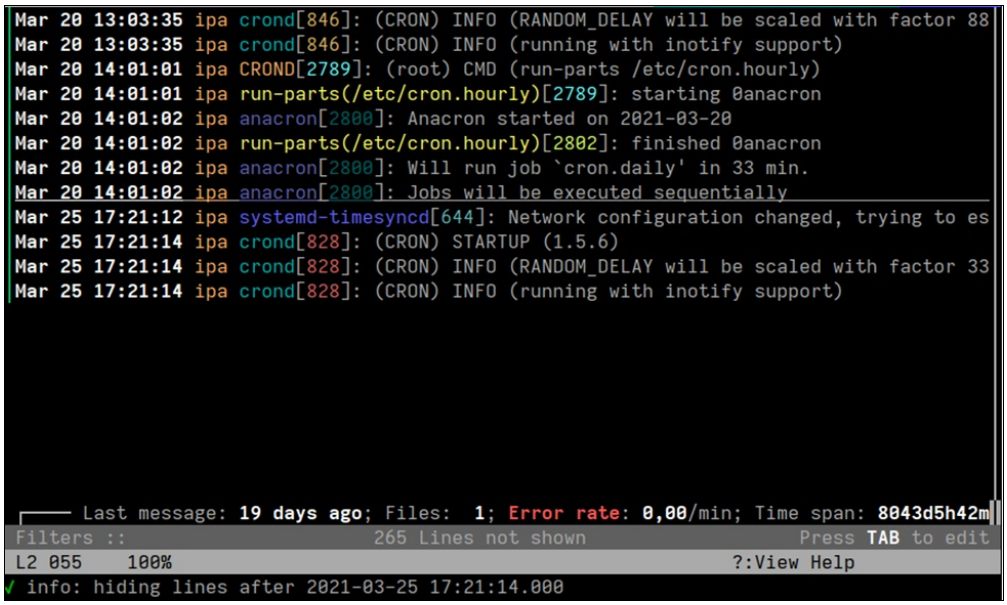
Точно так же вы можете использовать фильтрацию, чтобы показать все данные, кроме отфильтрованных строк, для этого введите текст с фильтром **filter-out**.

filter-out example

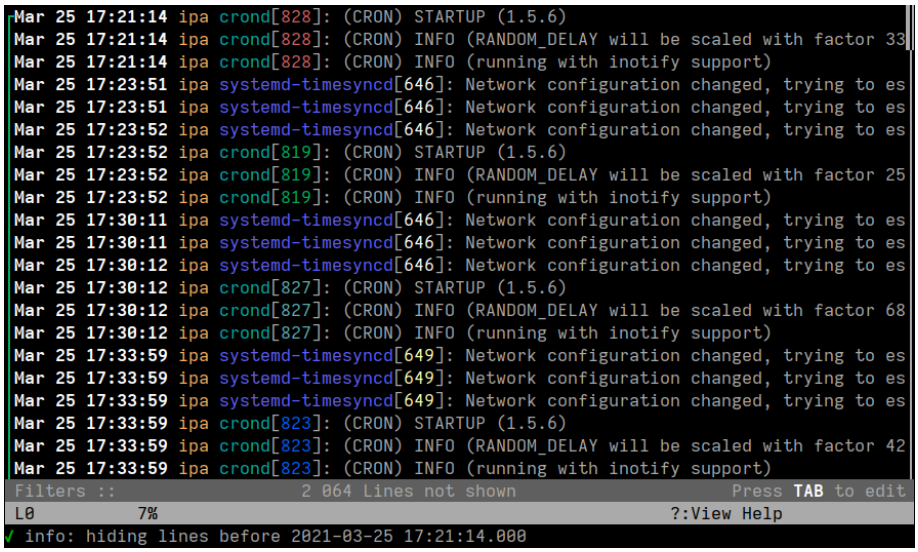
После применения фильтра данные с текстом «*example*» выводиться не будут.

Также можно использовать фильтры **hide-lines-after** и **hide-lines-before**.

Фильтр **hide-lines-after** скрывает строки, которые записаны *позже* заданного времени.



Фильтр **hide-lines-before** скрывает строки, которые записаны *раньше* заданного времени.



Скрытые строки можно снова показать с помощью команды **show-lines-before-and-after**.

Эти фильтры будут применяться ко всему файлу, поэтому, пока вы не отмените их (с помощью **Ctrl + R**), любые другие действия будут выполняться с отфильтрованным журналом, а не с журналом в целом.

Утилита incron

Установка
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: incron-0.5.10-9

Утилита **incron** предназначена для мониторинга событий в файловой системе и выполнения указанных действий при их обнаружении.

Основные функции утилиты:

- возможность задания разнообразных событий;
- возможность выполнения необходимых действий при обнаружении заданного события.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install incron
```

Запустите службу **incrond** и добавьте ее в автозагрузку:

```
systemctl enable incrond --now
```

Работа с утилитой производится через терминал с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

Для запуска утилиты необходимо выполнить команду **incrontab** с добавлением ключей.

Список ключей, с которыми может быть запущена утилита:

- `-e` – редактировать таблицу мониторинга текущего пользователя.

Редактирование таблицы мониторинга выполняется через редактор **vi**. Также доступно использование любого другого удобного текстового редактора, для смены редактора по умолчанию выполните команду:

```
export EDITOR="/usr/bin/nano"
```

- `-r` – удалить таблицу текущего пользователя;
- `-l` – вывести таблицу текущего пользователя.

Например, для редактирования таблицы мониторинга текущего пользователя выполните:

```
incrontab -e
```

Редактирование таблицы выполняется построчно для текущего пользователя, в таблицу необходимо добавить строку вида:

```
<объект> <событие> <действие>
```

где:

- `<объект>` — полный путь к файлу или директории, за которыми нужно наблюдать (рекурсивное наблюдение за директориями не поддерживается);

- `<команда>` — команда или скрипт, которые необходимо выполнить при наступлении события;
- `<событие>` — событие, на предмет наступления которого нужно наблюдать за объектом. Если событий несколько, они разделяются между собой запятой без пробела.

Доступные события приведены в таблице ниже.

Событие	Значение
IN_ACCESS	Файл был прочитан
IN_ATTRIB	Метаданные изменены (разрешения, временные метки, расширенные атрибуты и т. д.)
IN_CLOSE_WRITE	Файл, открытый для записи, был закрыт
IN_CLOSE_NOWRITE	Файл, не открытый для записи, был закрыт
IN_CLOSE	**IN_CLOSE_WRITE** или **IN_CLOSE_NOWRITE**
IN_CREATE	Создан файл или каталог
IN_DELETE	Удален файл или каталог
IN_DELETE_SELF	Удален файл или каталог, который мониторится
IN_MODIFY	Файл изменен
IN_MOVE_SELF	Файл или каталог, который мониторится, был перемещен
IN_MOVED_FROM	Файл был перемещен из каталога, который мониторится
IN_MOVED_TO	Файл перемещен в каталог, который мониторится
IN_MOVE	**IN_MOVED_FROM** или **IN_MOVED_TO**
IN_MOVED_TO	Файл был открыт
IN_ALL_EVENTS	Все перечисленные события

Примеры использования

В таблице мониторинга строка вида:

```
/etc/passwd IN_MODIFY cp /etc/passwd /tmp
```

означает, что при изменении файла **/etc/passwd**, например, при авторизации, файл будет скопирован в каталог **/tmp**.

В таблице мониторинга строка вида:

```
/etc/ssh/sshd_config IN_MODIFY systemctl restart sshd
```

означает, что при изменении конфигурации файла **sshd_config** будет перезагружен **sshd**-сервер.

Утилиты inotifywatch и inotifywait

Утилита inotifywatch
Установка
Примеры использования

Утилита inotifywait
Установка
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: inotify-tools-3.14-21

Утилита inotifywatch

Утилита **inotifywatch** предназначена для наблюдения за событиями файловой системы. Утилита выводит суммарное количество событий, произошедших с каждым файлом или директорией. Собранные данные отображаются только по завершении работы утилиты, выводятся на стандартный вывод в виде таблицы с одним столбцом для каждого вида события и одной строкой для каждого наблюдаемого файла или директории. Таблица отображает, сколько раз указанное событие произошло с каждым из файлов или каталогов.

Установка

Утилита входит в состав пакета **inotify-tools**.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install inotify-tools
```

Работа с утилитой производится через терминал с правами **непривилегированного** пользователя, выйдите из сеанса суперпользователя **root**:

```
exit
```

Синтаксис утилиты имеет вид:

```
inotifywatch [<опции>] <файл_1> [<файл_2>] [ ... ]
```

где:

- `<опции>` – необходимые для работы утилиты опции;
- `<файл_1>`, `<файл_2>` … – путь к файлу, мониторинг которого необходимо производить.

Для запуска утилиты необходимо выполнить команду **inotifywatch** с добавлением необходимых опций.

Список опций, с которыми может быть запущена утилита:

- `-h` – вывести справку по работе с утилитой;
- `-r` – рекурсивное наблюдение за всеми подкаталогами указанного каталога;
- `-t <время>` – время мониторинга в секундах, в течение которого будет производиться наблюдение (если опция не указана, мониторинг будет производиться непрерывно);
- `-e <событие>` – наблюдение только за указанными событиями.

Примеры использования

Для мониторинга файла **/etc/passwd** выполните:

```
inotifywatch /etc/passwd
```

Для мониторинга файла **/etc/passwd** в течение **10 секунд** на события типа **ACCESS** выполните:

```
inotifywatch -t 10 -e access /etc/passwd
```

Утилита inotifywait

Утилита **inotifywait** предназначена для наблюдения за событиями файловой системы. Утилита отображает в реальном времени информацию о наступлении запрашиваемых событий.

Установка

Утилита входит в состав пакета **inotify-tools**.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install inotify-tools
```

Работа с утилитой производится через терминал с правами **непривилегированного** пользователя, выйдите из сеанса суперпользователя **root**:

```
exit
```

Синтаксис утилиты имеет вид:

```
inotifywait [<опции>] <файл_1> [<файл_2>] [ ... ]
```

где:

- `<опции>` – необходимые для работы утилиты опции;
- `<файл_1>`, `<файл_2>`... – путь к файлу, мониторинг которого необходимо производить.

Для запуска утилиты необходимо выполнить команду **inotifywait** с добавлением необходимых опций.

Список опций, с которыми может быть запущена утилита:

- `-h` – вывести справку по работе с утилитой;
- `-m` – не останавливать мониторинг после наступления первого события, продолжать мониторинг до остановки пользователем;
- `-o` – вывести события в файл;
- `-r` – рекурсивное наблюдение за всеми поддиректориями;
- `-t` – время мониторинга в секундах, в течение которого будет производиться наблюдение;
- `-e` – наблюдение за определенными событиями;
- `--format <формат_вывода>` – задать формат вывода:
    - **%w** – указать имя наблюдаемого файла или директории;
    - **%f** – если событие происходит с файлом внутри наблюдаемой директории, указать имя этого файла;
    - **%e** – указать наименование произошедшего события, наименования разделяются запятыми;
    - **%T** – указать текущее время в формате **ЧЧ:ММ:СС**;

- **--timefmt <формат_вывода>** – установить формат времени.

Примеры использования

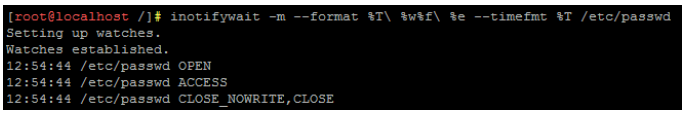
Для наблюдения за файлом **/etc/passwd**, не завершая наблюдение после наступления первого события и используя пользовательский формат вывода, добавляющий текущее время к каждому событию, выполните команду:

```
inotifywait -m --format %T\ %w%f\ %e --timefmt %T /etc/passwd
```

где:

- **inotifywait -m** – не прерывать выполнение после первого события;
- **--format %T\ %w%f\ %e** – задать формат вывода, где:
  - **%w** – указать имя отслеживаемого файла,
  - **%f** – при отслеживании директории указать имя файла, в котором произошли изменения,
  - **%e** – показать события, которые произошли.
  - **--timefmt %T /etc/passwd** – добавить текущее время.

Результат выполнения команды:



Для рекурсивного наблюдения за директорией **/etc**, не завершая наблюдение после наступления первого события, используя пользовательский формат вывода, добавляющий текущее время к каждому событию, и записывая вывод в файл **/tmp/inotifywait**, выполните команду:

```
inotifywait -m --format %T\ %w%f\ %e --timefmt %T -o /tmp/inotifywait -r /etc/ &
```

Утилита fswatch

Установка
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: fswatch-1.17.1-2

Утилита **fswatch** предназначена для мониторинга изменений файлов и каталогов в реальном времени.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fswatch
```

Работа с утилитой производится через терминал. Права для работы с утилитой определяются установленным доступом к отслеживаемому каталогу или файлу.

Синтаксис утилиты имеет вид:

```
fswatch [<опции>] ... <путь> ...
```

где:

- `<опции>` – необходимые для работы утилиты опции;
- `<путь>` – путь к каталогу или файлу, мониторинг которого необходимо производить.

Для запуска утилиты необходимо выполнить команду **fswatch** с добавлением необходимых ключей.

Список основных ключей, с которыми может быть запущена утилита:

- `-h`, `--help` – вывод справки по утилите;
- `--event=<событие>` – отслеживать только указанные события;
- `-e <шаблон>`, `--exclude=<шаблон>` – исключение каталогов/файлов, совпадающих с шаблоном, из мониторинга;
- `-f` – вывод времени события в заданном формате;
- `-l` – интервал мониторинга;
- `-r` – рекурсивный просмотр каталогов;
- `-v` – печать подробного вывода.

Примеры использования

Для вывода изменений каталога **/tmp** с интервалом **20 секунд** выполните команду вида:

```
fswatch -l 20 /tmp
```

где

- **-l 20** – время мониторинга в секундах;
- **/tmp** – каталог мониторинга.

Результат выполнения команды:

```
 fswatch -l 20 /tmp

/tmp
/tmp/ test
/tmp
/tmp/ test
/tmp
/tmp/ test
/tmp
```

В каталоге был создан и удален каталог **/test**.

Для вывода времени изменения файла **/test.sh** с интервалом **2 секунды** выполните команду вида:

```
fswatch -t -l 2 /test.sh
```

где:

- **-t** – вывод времени наступления события.

Результат выполнения команды:

```
 fswatch -t -l 2 /test.sh

Пн 29 янв 2024 09:30:13 /test.sh
Пн 29 янв 2024 09:30:15 /test.sh
Пн 29 янв 2024 09:30:15 /test.sh
Пн 29 янв 2024 09:30:15 /test.sh
Пн 29 янв 2024 09:30:22 /test.sh
Пн 29 янв 2024 09:30:22 /test.sh
```

Для вывода времени изменения каталога **/** с интервалом **2 секунды** с указанием производимых действий выполните команду:

```
fswatch -x -t -l 2 /
```

где:

- **-x** – вывод произошедших изменений.

Результат выполнения команды:

```
 fswatch -x -t -l 2 /

Пн 29 янв 2024 09:33:44 / IsDir
Пн 29 янв 2024 09:33:44 //test Created
Пн 29 янв 2024 09:33:47 / IsDir
Пн 29 янв 2024 09:33:47 //test PlatformSpecific
Пн 29 янв 2024 09:33:49 / IsDir
Пн 29 янв 2024 09:33:49 //test PlatformSpecific
Пн 29 янв 2024 09:33:49 / IsDir
Пн 29 янв 2024 09:33:49 //test Removed
```

Rsyslog – сервис управления системными журналами

Содержимое конфигурационного файла rsyslog.conf
Создание правил в системе
Другие варианты написания правил
Отправка лог-сообщений на удаленный сервер

Rsyslog — это очень быстрый, расширяемый сервис для управления логами с огромным количеством возможностей. Среди его возможностей можно отметить поддержку фильтрации контента, а также передачу логов по сетям. Основные возможности:

- Многопоточность;
- TCP, SSL, TLS, RELP;
- Поддержка MySQL, PostgreSQL, Oracle;
- Фильтрация журналов;
- Полностью настраиваемый формат вывода.

Вы можете подробнее ознакомиться с работой сервиса управления логами **Rsyslog**, просмотрев наши обучающие видео:

- на **RuTube** — Rsyslog - сервис управления логами;
- в **Яндекс.Дзен** — Rsyslog - сервис управления логами;
- в **VK Видео** — Rsyslog - сервис управления логами.

На наших каналах вы также сможете найти много другой полезной информации.

Каталогом по умолчанию для хранения логов является каталог **/var/log**, в файлы которого записывается вся информация о состоянии системы и используемых программ, а также информация об ошибках. Лог-файлы можно просмотреть, выполнив команду:

```
ls -l /var/log/
```

Содержимое конфигурационного файла rsyslog.conf

Главным конфигурационным файлом сервиса **rsyslog** является **rsyslog.conf**. Для просмотра содержимого конфигурационного файла можно воспользоваться командой:

```
nano /etc/rsyslog.conf
```

Файл разделен на 3 основных секции:

- Modules — содержит параметры, предназначенные для настройки методов работы сервиса с лог-сообщениями;
- Global derectives — содержит глобальные параметры работы службы **rsyslog**;
- Rules — содержит правила сортировки логов.

Секция Modules

В секции Modules загружаются все необходимые модули программы. Секция имеет следующим вид:

```
#### MODULES ####

 module(load="imuxsock"    # provides support for local system logging (e.g. via logger command)
   SysSock.Use="off")     # Turn off message reception via local log socket;
                          # local messages are retrieved through imjournal now.
 module(load="imjournal"   # provides access to the systemd journal
   StateFile="imjournal.state")     # File to store the position in the journal
 #module(load="imklog")    # reads kernel messages (the same are read from journald)
 #module(load"immark")     # provides --MARK-- message capability

 # Provides UDP syslog reception
 # for parameters see http://www.rsyslog.com/doc/imudp.html
 #module(load="imudp")     # needs to be done just once
 #input(type="imudp" port="514")
```

```
# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp")     # needs to be done just once
#input(type="imtcp" port="514")
```

Существует четыре типа модулей:

- *Модули ввода* — можно рассматривать, как способ сбора информации из различных источников, начинаются с **im**;
- *Модули вывода* — позволяют отправлять сообщения в файлы, по сети или в базу данных, начинаются с **om**;
- *Модули фильтрации* — позволяют отфильтровывать сообщения по разным параметрам, начинаются с **fm**;
- *Модули парсинга* — предоставляют расширенные возможности для синтаксического анализа сообщения, начинаются с **pm**.

Модуль **imuxsock** позволяет сервису получать сообщения от приложений, работающих в локальной системе. По умолчанию отключено прослушивание сокета **/dev/log** из-за параметра `SysSock.Use="off"`.

Модуль **imjournal** предоставляет возможность импорта сообщений структурированного журнала из журнала *systemd* в системный журнал. Обратите внимание, что этот модуль читает базу данных журнала, что считается относительно интенсивной операцией. Таким образом, производительность конфигурации с использованием этого модуля может быть заметно ниже, чем при использовании **imuxsock**. По умолчанию ограничение скорости активировано и позволяет обрабатывать 20 000 сообщений в течение 10 минут, чего должно быть достаточно для большинства случаев использования. Если импорт структурированных данных необходим, используйте **imjournal**, в противном случае следует задействовать модуль **imuxsock**.

Модуль **imklog** предназначен для получения сообщений ядра.

Модуль **mark** позволяет маркировать соединения или выводить сообщения о том, что **syslog** все еще работает.

Секция Global directives

Глобальные директивы используются для настройки службы **rsyslog**. Как правило, они указывают значение для конкретной предопределенной переменной, которая влияет на функциональность правил или самой службы **rsyslog**.

Секция **Global directives** имеет следующий вид:

```
#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")
```

Описание переменных:

- `global(workDirectory="/var/lib/rsyslog")` — задает директорию, которая будет использоваться для рабочих файлов службы **rsyslog**;
- `module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")` — задает стандартный формат хранения времени, в секундах с 1970 года;
- `include(file="/etc/rsyslog.d/*.conf" mode="optional")` — задает директорию, которая будет использоваться для дополнительных файлов конфигурации.

Секция Rules

Данный раздел содержит правила сортировки логов. Каждое правило имеет свой синтаксис: сначала идет *источник* и *приоритет*, затем *действие*. Если источник и приоритет совпадают, сообщение отправляется в указанный файл. *Источников* и *приоритетов* может быть несколько, их можно разделять точкой с запятой.

Содержимое секции имеет следующий вид:

```
#### RULES ####
```

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure

# Log all the mail messages in one place.
mail.*                                          -/var/log/maillog

# Log cron stuff
cron.*                                          /var/log/cron

# Everybody gets emergency messages
*.emerg                                         :omusrmsg:*
# Save news errors of level crit and higher in a special file.

uucp,news.crit                                  /var/log/spooler

# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
```

Источниками являются места, откуда поступают сообщения.

Источники могут принимать следующие значения:

- **auth** — все, что связано с авторизацией пользователей, например, *login* и *su* (безопасность/права доступа);
- **authpriv** — то же самое, что и **auth**, однако сообщения этой категории записываются в файл, который могут читать лишь некоторые пользователи (категория выделена, потому что принадлежащие ей сообщения могут содержать открытые пароли пользователей, которые не должны попадать на глаза посторонним людям, и, следовательно, файлы протоколов должны иметь соответствующие права доступа);
- **cron** — сообщения от системного планировщика;
- **daemon** — сообщения от системных служб, которые в отличие от FTP или LPR не имеют специально-выделенных категорий;
- **kern** — сообщения ядра;
- **lpr** — сообщения от системы печати;
- **mail** — сообщения от почтовой системы;
- **mark** — присваивается отдельным сообщениям, формируемым службой syslog;
- **security** — эквивалентно auth;
- **syslog** — система протоколирования может протоколировать сообщения от самой себя;
- **uucp** — копирование файлов между компьютерами (Unix-to-Unix CoPy);
- **user** — сообщения пользовательских программ;
- **local0 ... local7** — зарезервированные категории для использования администратором системы. Категория local7 обычно используется для сообщений, генерируемых на этапе загрузки системы;
- ***** — Выбор всех источников.

Приоритетом является степень важности сообщения.

Приоритеты могут принимать следующие значения:

- **emerg** (раньше *panic*) — чрезвычайная ситуация, система неработоспособна;
- **alert** — тревога, требуется немедленное вмешательство;
- **crit** — критическая ошибка (критическое состояние);
- **error** (раньше *err*) — сообщение об ошибке;
- **warn** (раньше *warning*) — предупреждение;
- **notice** — информация о каком-либо нормальном, но важном событии;
- **info** — информационное сообщение;

- **debug** — сообщения, формируемые в процессе отладки;
- ***** — выбор всех приоритетов;
- **none** — сообщения от источника с любым приоритетом будут исключены для действия.

Действием является отправка сообщений, которые подходят под заданные ранее параметры в заданное место.

Действия могут принимать следующие значения:

- **/путь/к/файлу** — отправка сообщений в обычный файл;
- **/dev/console** — отправка сообщений в терминал или консоль;
- **@xx.xx.xx.xx:514** — отправка сообщений на удаленную машину с помощью **UDP**;
- **@@xx.xx.xx.xx:514** — отправка сообщений на удаленную машину с помощью **TCP**;
- **user,user2,root** — отправка сообщений пользователям на терминал (разделенный запятыми список пользователей, получающих сообщения).

Создание правил в системе

В общем случае синтаксис правил выглядит следующим образом:

```
<источник>.<приоритет> <действие>
```

В качестве примера разберем правило:

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

Первым *источником* событий являются все сообщения с приоритетом **info**. Также к *источникам* добавляются и другие сообщения, разделенные между собой точкой с запятой. Из правил следует, что *источники* **mail**, **authpriv**, **cron** будут исключены, так как имеют *приоритет* **none**. *Действием* для данного правила является отправка сообщений в файл **/var/log/messages**.

Другие варианты написания правил

Фильтрация на основе свойств сообщения

Фильтрация данного вида имеет следующий синтаксис:

```
:<переменная>, <операция_сравнения>, "<искомое_значение>" <действие>
```

Переменные могут принимать значение:

- **msg** — тело сообщения;
- **hostname** — имя хоста/IP-адреса из сообщения;
- **fromhost** — имя хоста, от которого пришло сообщение;
- **fromhost-ip** — адрес хоста, от которого пришло сообщение (127.0.0.1 для локальных сообщений);
- **syslogtag** — имя и номер процесса (`"rsyslogd[12125]:"`), который выдал сообщение (извлекается из сообщения);
- **programname** — имя процесса, который выдал сообщение (извлекается из сообщения);
- **pri** — источник и приоритет, в виде числа;
- **pri-text** — декодированные источник и приоритет (`facility.priority`, например `syslog.emer`);
- **syslogfacility** — только источник в виде числа;
- **syslogfacility-text** — только декодированный источник (`"local0"`);
- **syslogseverity** — только приоритет в виде числа;
- **syslogseverity-text** — только декодированный уровень (`"debug"`);
- **timegenerated** — время получения (с высоким разрешением);
- **timereported** — время, извлечённое из сообщения;
- **inputname** — имя входного модуля;

- **$hour, $minute** — текущее время;
- **$myhostname** — имя хоста обработки.

Операция сравнения может принимать значение:

- **contains** — проверяет соответствие `<искомое_значение>` с любой частью строки в переменная;
- **isequal** — проверяет, совпадает (целиком) ли `<искомое_значение>` с переменной;
- **isempty** — проверяет, является ли переменная пустой;
- **startswith** — проверяет, начинается ли переменная с `<искомое_значение>`;
- **regex** — сравнивает поле с регулярным выражением.

Искомое значение может принимать значение имени программы, службы или источника (источники были рассмотрены ранее в данной статье).

Действие принимает значения, рассмотренные ранее в статье.

Теперь можно составить правило для логирования приложения. Пример составления правила:

```
:syslogtag, isequal, "wireguard:" /var/log/wireguard.log
 &stop
```

& stop необходим для того, чтобы остановить регистрацию сообщения после его совпадения.

Фильтрация RainerScript

Фильтрация данного вида имеет следующий синтаксис:

```
if $<переменная> <операция_сравнения> "<искомое_значение>" then <действие>
```

Операция сравнения может принимать значения:

- **==** — равно;
- **!=** — не равно.

Пример правила для логирования приложения будет выглядеть следующим образом:

```
if $syslogtag == "wireguard" then /var/log/wireguard.log
```

Отправка лог-сообщений на удаленный сервер

Настройка сервера, который будет принимать лог-сообщения

Если на сервере используется брандмауэр, необходимо открыть порты **TCP/UDP 514**. На примере **iptables** открытие портов производится командами:

```
iptables -A INPUT -p tcp --dport 514 -j ACCEPT
iptables -A INPUT -p udp --dport 514 -j ACCEPT
```

Затем настройте SELinux, если он используется:

```
semanage port -m -t syslogd_port_t -p tcp 514
semanage port -m -t syslogd_port_t -p udp 514
```

Для разрешения серверу принимать соединение по **TCP** и **UDP** в конфигурационном файле **/etc/rsyslog.conf** раскомментируйте строки в секции **Modules**:

```
module(load="imudp") # needs to be done just once
 input(type="imudp" port="514")

 module(load="imtcp") # needs to be done just once
 input(type="imtcp" port="514")
```

Не обязательно открывать соединение по обоим протоколам, можно выбрать только тот, который необходим именно вам.

В эту же секцию после модулей для TCP- и UDP-соединения необходимо добавить следующее:

```
$template RemoteLogs,"/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
 *.* ?RemoteLogs
 & ~
```

Таким образом создается шаблон, по которому лог-сообщения от любого источника с любым уровнем будут сохраняться в каталог сервера **/var/log/rsyslog/<имя_компьютера-отправителя_лога>/<приложение-отправитель_лога>.log**.

После проделанных настроек необходимо перезагрузить службу **rsyslog** командой:

```
systemctl restart rsyslog.service
```

Настройка сервера на этом закончена. Для проверки открытия порта выполните команду:

```
netstat -pnltu
```

```
[root@localhost ~]# netstat -pnltu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3831/sshd: /usr/sbi
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1016/master
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN      99121/cupsd
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      107443/rsyslogd
tcp6       0      0 :::22                   :::*                    LISTEN      3831/sshd: /usr/sbi
tcp6       0      0 :::631                  :::*                    LISTEN      99121/cupsd
tcp6       0      0 :::514                  :::*                    LISTEN      107443/rsyslogd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1016/master
udp        0      0 127.0.0.1:323           0.0.0.0:*                           668/chronyd
udp        0      0 0.0.0.0:45131           0.0.0.0:*                           656/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           656/avahi-daemon: r
udp6       0      0 ::1:323                 :::*                                668/chronyd
udp6       0      0 :::41782                :::*                                656/avahi-daemon: r
udp6       0      0 :::5353                 :::*                                656/avahi-daemon: r
[root@localhost ~]#
```

Настройка клиента, который будет отправлять лог-сообщения

Для создания правила на клиенте воспользуйтесь директорией **rsyslog.d**, которая является дополнительной для конфигурационных файлов.

Создайте конфигурационный файл, который будет отправлять на сервер сообщения от *источника* **auth** с любым *приоритетом*. Для этого выполните команду:

```
nano /etc/rsyslog.d/auth.conf
```

И добавьте правило:

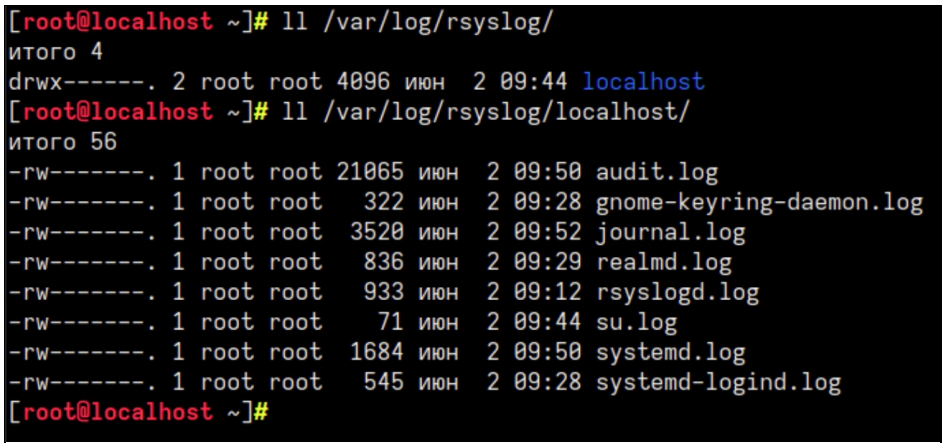
```
auth.* @@xx.xx.xx.xx:514
```

где **@@xx.xx.xx.xx:514** — адрес сервера и его порт для протокола **TCP**. Для протокола **UDP** нужно указывать действие в виде **@xx.xx.xx.xx:514**.

Сохраните изменения и перезагрузите службу **rsyslog** командой:

```
systemctl restart rsyslog.service
```

При корректной настройке на сервере в каталоге **/var/log/rsyslog** должна появиться директория с именем (hostname) ПК, который отправляет лог-файлы, и, непосредственно, лог-файлы.


[root@localhost ~]# ll /var/log/rsyslog/
итого 4
drwx------. 2 root root 4096 июн 2 09:44 localhost
[root@localhost ~]# ll /var/log/rsyslog/localhost/
итого 56
-rw-------. 1 root root 21065 июн 2 09:50 audit.log
-rw-------. 1 root root   322 июн 2 09:28 gnome-keyring-daemon.log
-rw-------. 1 root root 3520 июн 2 09:52 journal.log
-rw-------. 1 root root   836 июн 2 09:29 realmd.log
-rw-------. 1 root root   933 июн 2 09:12 rsyslogd.log
-rw-------. 1 root root   71 июн 2 09:44 su.log
-rw-------. 1 root root 1684 июн 2 09:50 systemd.log
-rw-------. 1 root root   545 июн 2 09:28 systemd-logind.log
[root@localhost ~]#

LogAnalyzer – веб-приложение для просмотра системных журналов

Установка необходимых пакетов
Настройка MariaDB и Apache
Настройка rsyslog
Установка LogAnalyzer
Настройка веб-приложения LogAnalyzer
Изменения кодировки в приложении LogAnalyzer

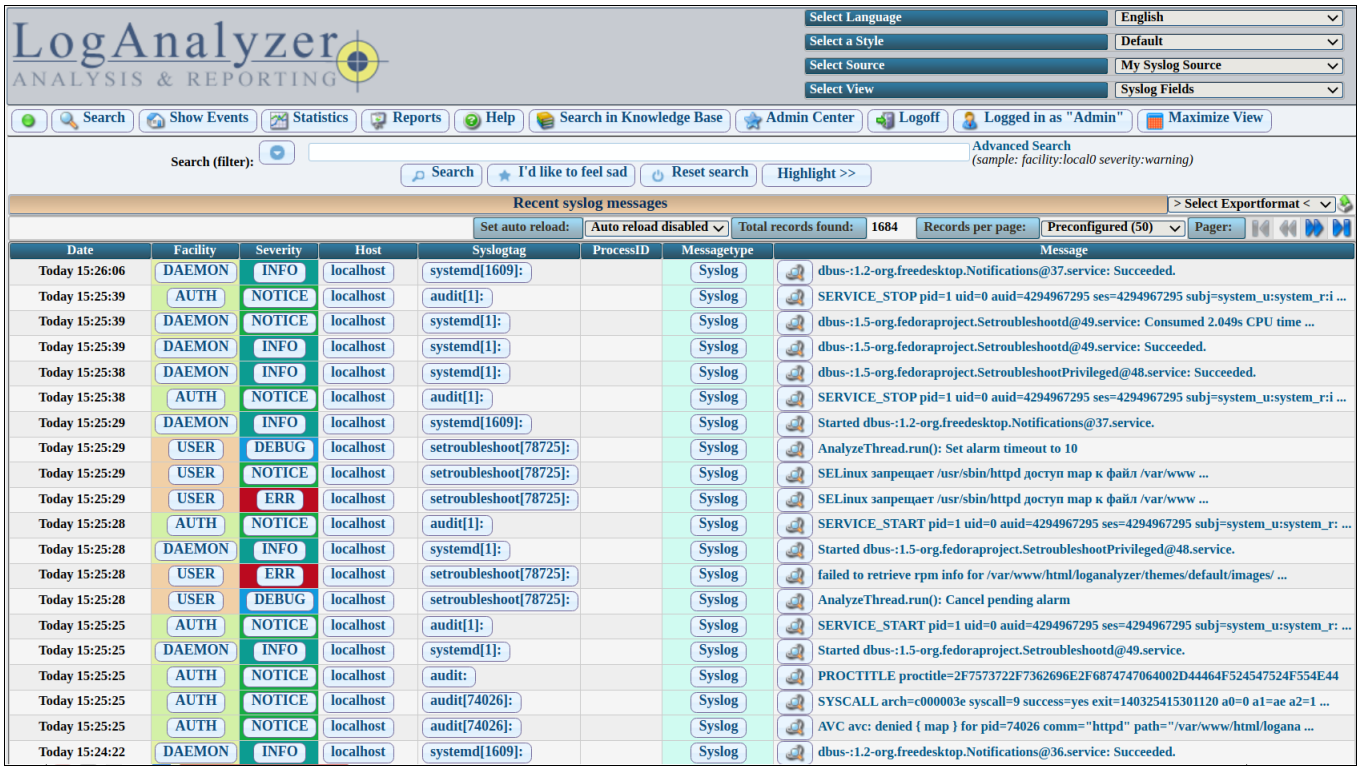
Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: loganalyzer-4.1.13

LogAnalyzer — веб-приложение, предназначенное для просмотра логов системных событий, полученных от **rsyslog**, при помощи веб-браузера.

Rsyslog — быстрый, расширяемый сервис для управления логами с огромным количеством возможностей. Среди его особенностей можно отметить поддержку фильтрации контента, а также передачу логов по сети.

С помощью этих программ можно создать централизованный сервер логов, где будут отображаться все события от различных устройств в сети с удобным архивированным поиском событий.



Установка необходимых пакетов

Для установки пакетов перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install mariadb-server rsyslog-mysql php php-mysql httpd
```

Настройка MariaDB и Apache

Настройте SELinux:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_can_network_connect_db 1
```

Далее необходимо настроить **MariaDB** и **Apache**.

После установки пакетов запустите и добавьте в автозагрузку службы **httpd** и **mariadb**:

```
systemctl enable httpd --now
systemctl enable mariadb --now
```

По умолчанию пользователь root базы данных **MariaDB** имеет пустой пароль, поэтому следует обезопасить конфигурацию, задав новый пароль:

```
mariadb-admin -u root password <пароль>
```

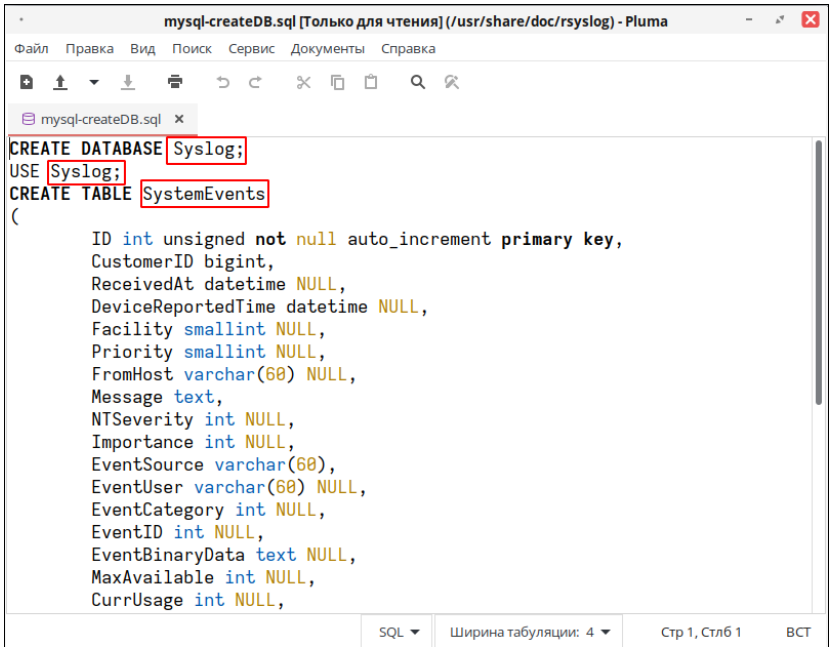
где вместо **<пароль>** нужно вписать ваш новый пароль.

Далее необходимо импортировать схему базы данных **rsyslog** в **MariaDB**:

```
mariadb -u root -p < /usr/share/doc/rsyslog/mysql-createDB.sql
```

Будет запрошен пароль пользователя **root** базы данных **MariaDB**, который был задан на предыдущем шаге.

По умолчанию имя схемы базы данных — **Syslog**, имя таблицы — **SystemEvents**. Опционально данные могут быть изменены. Для этого до импорта схемы в базу данных следует открыть файл **mysql-createDB.sql** и указать новое имя в первой и второй строке для имени базы данных. В третьей строке — для имени таблицы. Имя базы данных и имя таблицы понадобятся позднее для настройки веб-приложения.



Рекомендуется ограничивать доступ приложений к базе данных, поэтому необходимо создать специального пользователя для доступа к БД — **rsyslog**. Для этого перейдите в командную строку управления базой данных с правами пользователя **root**:

```
mariadb -u root -p
```

Введите пароль.

Затем создайте пользователя **rsyslog** и предоставьте ему права к базе данных **Syslog** следующей командой:

```
GRANT ALL ON Syslog.* TO 'rsyslog'@'localhost' IDENTIFIED BY '<пароль_пользователя_rsyslog>';
```

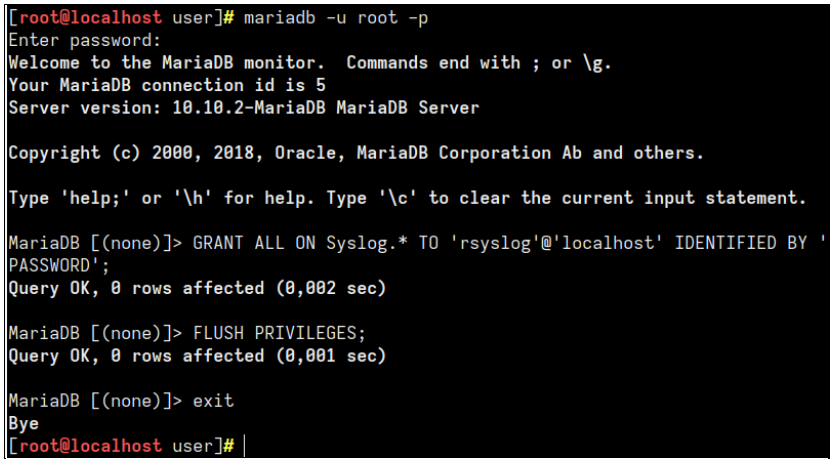
Выполните команду для немедленного применения всех прав:

```
FLUSH PRIVILEGES;
```

Теперь можно выйти из командной строки управления БД:

```
exit
```

После выполнения каждой команды должно выводиться сообщение об успешном ее применении.



Настройка rsyslog

Для настройки **rsyslog** откройте файл конфигурации:

```
nano /etc/rsyslog.conf
```

и добавьте в конец секции `MODULES` новый модуль:

```
module(load="ommysql")
```

В секцию `RULES` добавьте правило для пересылки логов в базу данных:

```
*.* :ommysql:localhost,Syslog,rsyslog,<пароль_пользователя_rsyslog>
```

где ***.*** — означает, что сообщения от любого источника с любым приоритетом будут отправляться в базу данных, расположенную на данной машине (*localhost*). Также указывается название базы данных — **Syslog**, ранее созданный пользователь **rsyslog** и его **пароль**.

Для применения внесенных изменений перезагрузите службу **rsyslog**:

```
systemctl restart rsyslog.service
```

Установка LogAnalyzer

Теперь можно перейти к установке веб-приложения **LogAnalyzer**. Для установки выполните команду:

```
dnf install loganalyzer
```

Создайте символьную ссылку на приложение в каталоге веб-сервера по умолчанию:

```
ln -s /usr/share/loganalyzer/ /var/www/html/loganalyzer
```

Перейдите в каталог веб-сервера:

```
cd /var/www/html/loganalyzer
```

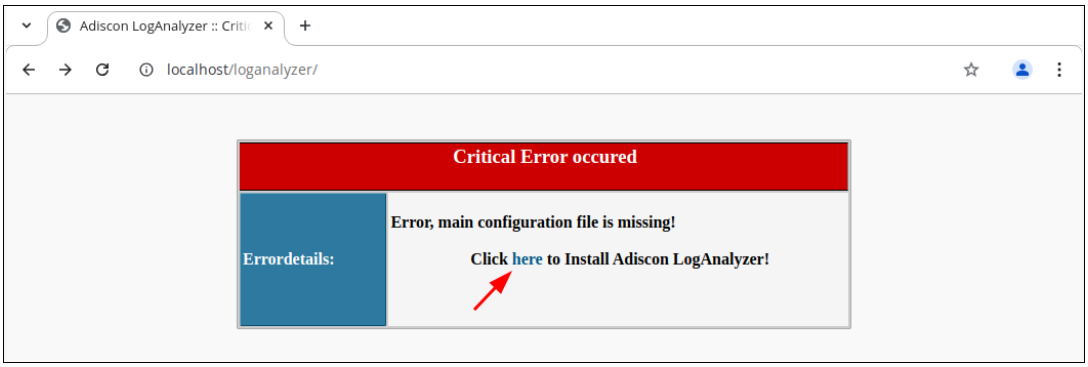
Настройте SELinux:

```
restorecon -R /var/www/html/loganalyzer
chcon -t httpd_sys_rw_content_t config.php
```

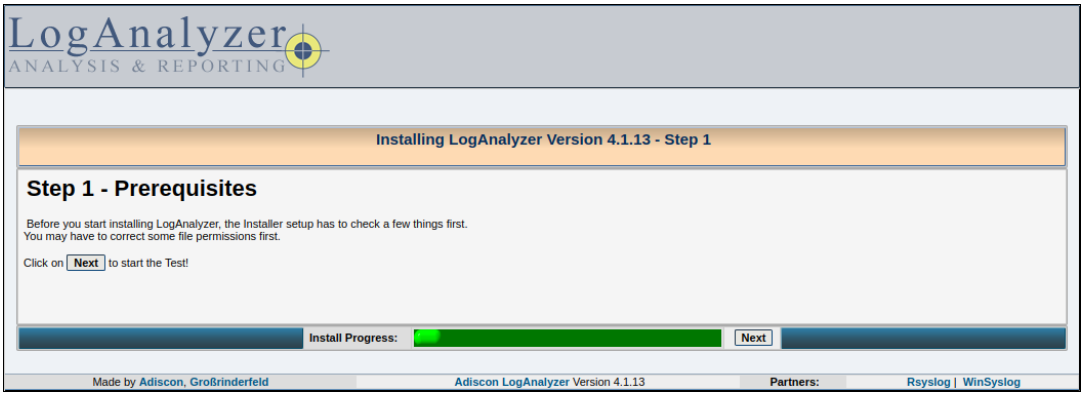
После этого можно переходить к настройке веб-приложения.

Настройка веб-приложения LogAnalyzer

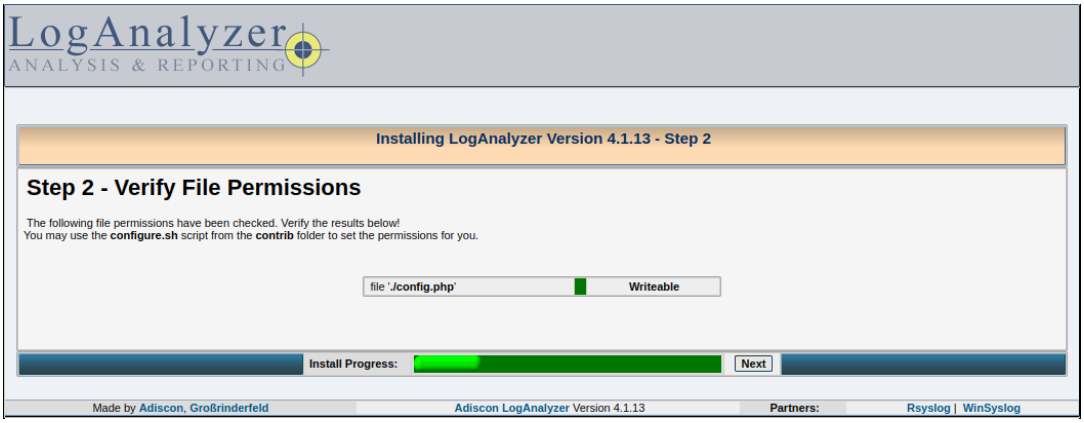
Откройте браузер и в адресной строке пропишите http://localhost/loganalyzer/. Будет открыта страница с ошибкой, т. к. приложение еще не настроено. В тексте описания ошибки нажмите на слово «**here**» для продолжения настройки.



Шаг №1. На стартовой странице нажмите **Next**.



Шаг №2. На втором шаге производится проверка на наличие файла конфигурации **config.php**. В него будут записаны последующие настройки. Рядом с обнаруженным файлом обязательно должна отображаться надпись «**Writeable**». При ее отсутствии в файл не могут быть записаны настройки.



Шаг №3. На третьей странице задается базовая конфигурация приложения.

Рассмотрим подробнее некоторые из параметров:

Frontend Options — параметры отображения сообщений:

- количество сообщений системного журнала на страницу — **50** (по умолчанию);
- лимит символов сообщения для основного вида — **80** (по умолчанию);
- ограничение на отображение символов для всех строк — **30** (по умолчанию);
- отображение всплывающего окна сведений о сообщении — **yes** (по умолчанию).

UserDatabase Options — параметры подключения к базе данных.

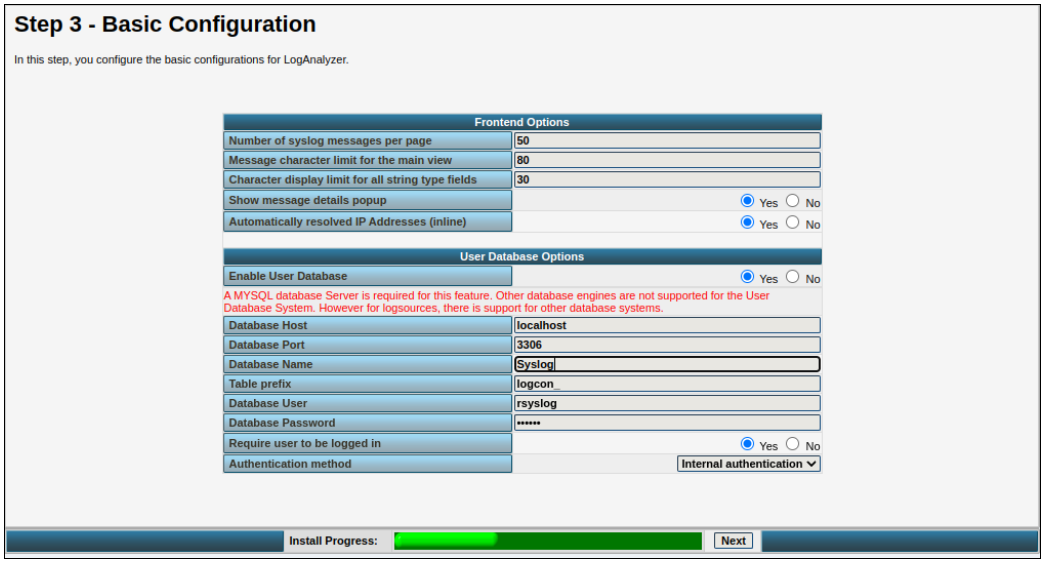
Измените значения следующих параметров:

- **Database Name** — укажите имя таблицы **Syslog** (по умолчанию имя схемы базы данных);
- **Database User** — укажите имя пользователя **rsyslog**, который был создан для доступа к базе данных **Syslog**;

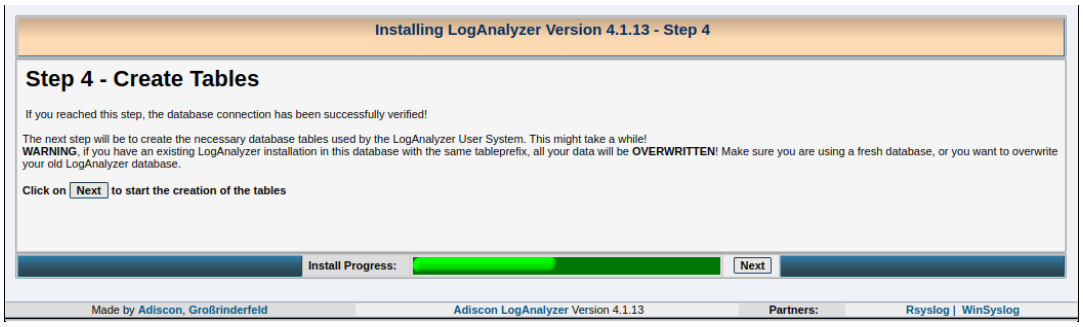
- **Database Password** — укажите пароль пользователя **rsyslog**;
- **Require user to be logged in** — выберите **yes**.

Примечание.

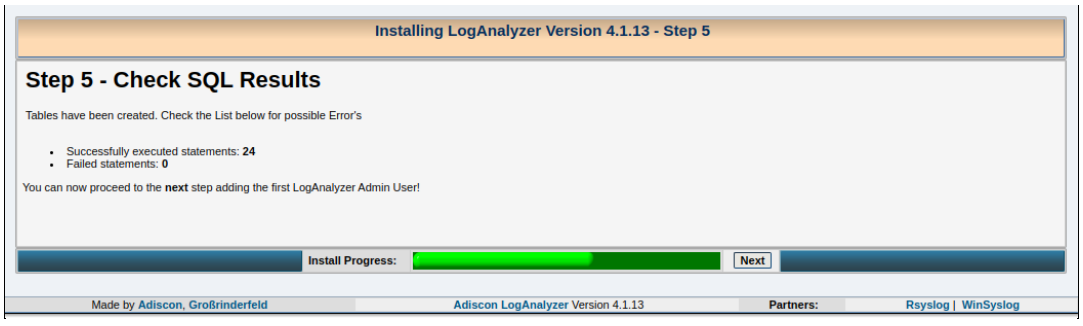
Обратите внимание, что поля формы **РЕГИСТРОЗАВИСИМЫ**!



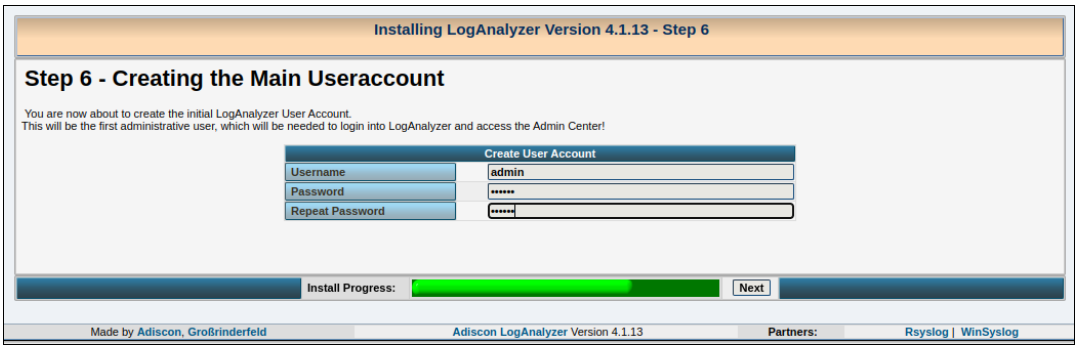
Шаг №4. Если настройка проведена корректно, будет открыта страница с предупреждением о внесении изменений в конфигурационный файл **config.php**. Подключение к базе данных успешно установлено. Нажмите **Next**.



Шаг №5. На данной странице будет выведено сообщение об успешном создании таблицы в базе данных, а также отобразится количество успешных операций и ошибок.



Шаг №6. Здесь будет предложено создать первого пользователя для веб-приложения. Данный пользователь будет иметь административные права и доступ к центру администрирования. Можно создать любого пользователя.



Шаг №7. На этой странице необходимо снова указать источник, который ведет системный журнал.

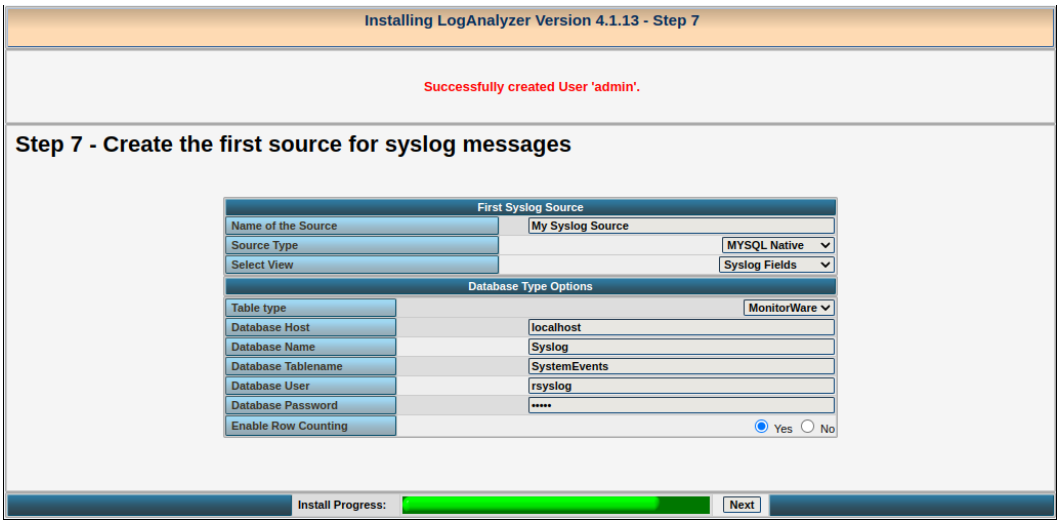
Name of the Source — при желании укажите имя источника, которое будет отображаться в веб-приложении. Позднее в приложении можно будет добавить другие источники.

Source Type — выберите тип базы данных, укажите **MYSQL Native**.

Опции базы данных заполняются так же, как и на **шаге №3** — имя базы данных, логин пользователя базы данных и его пароль.

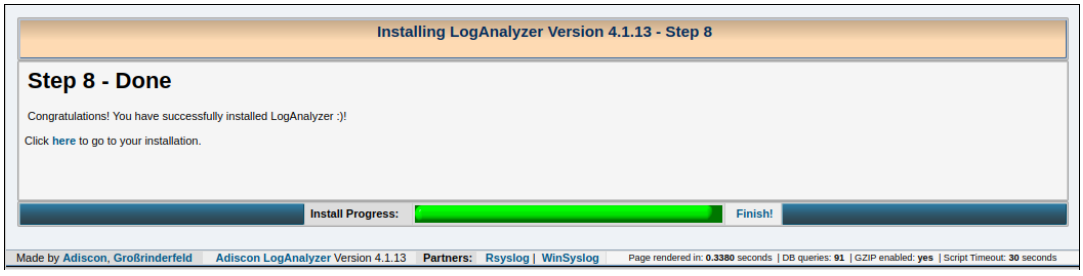
Database Tablename — укажите имя таблицы базы данных **SystemEvents**.

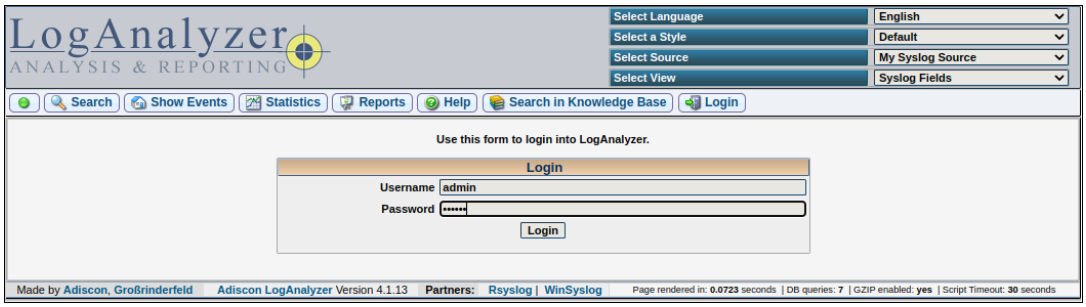
> **Примечание.**
>
> Обратите внимание, что поля формы **РЕГИСТРОЗАВИСИМЫ**!

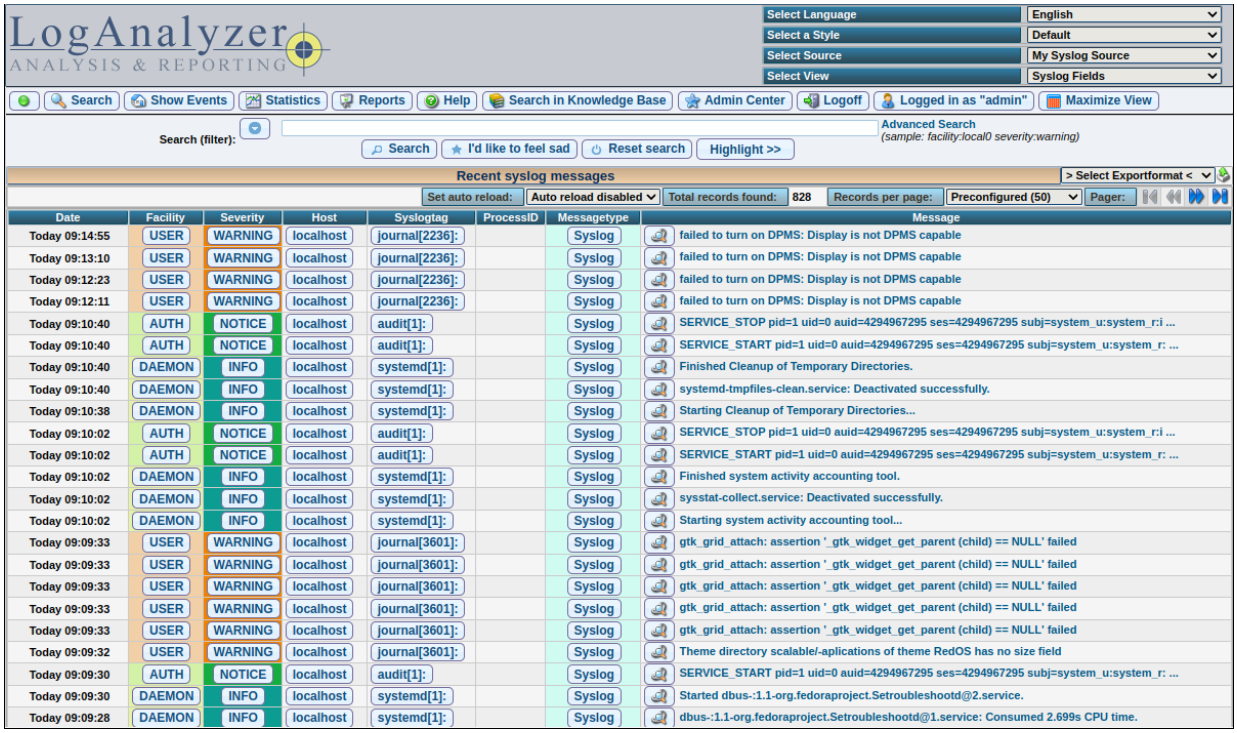


Шаг №8. Если настройка выполнена верно, будет открыта страница с сообщением об успешной установке **LogAnalyzer**. Нажмите **Finish** для перехода на страницу аутентификации.

После успешной аутентификации будут открыты логи в удобном для просмотра формате.

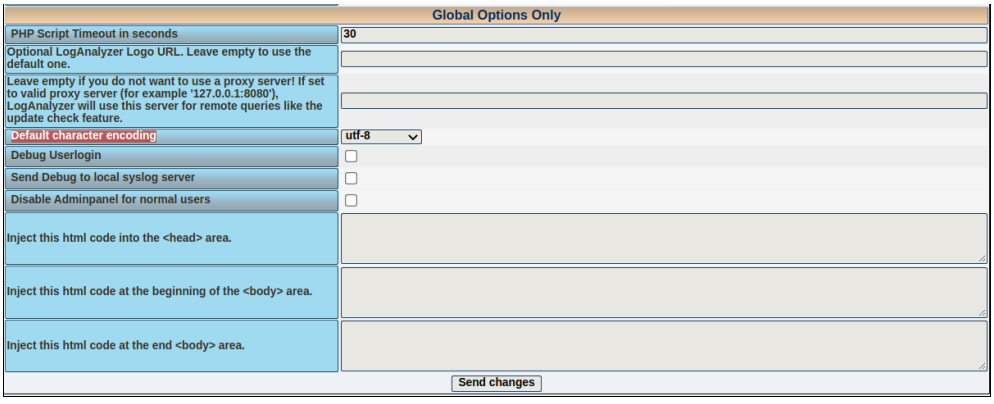






Изменения кодировки в приложении LogAnalyzer

Для корректного отображения сообщений на русском языке необходимо изменить кодировку в веб-приложении. Для этого перейдите в **Admin Center**, в разделе **Global Options Only** измените параметр **Default character encoding** на **utf-8**. Сохраните изменения с помощью кнопки **Send changes** внизу страницы.



Logrotate – настройка ротации (хранения) системных журналов

Основные параметры для настройки
Вспомогательные настройки
Проверка конфигурации

В РЕД ОС большинство сервисов и программ, которые работают в фоне, записывают информацию о своем состоянии, результатах работы и ошибках в файлы, называемые **журналами**. Стандартное расположение журналов или, как их еще называют, **логов** - в папке **/var/log**.

С помощью анализа этих файлов можно понять, что работает не так, почему произошла ошибка и как решить возникшую проблему. Однако существует некоторая проблема - размер журналов постоянно растет, они занимают все больше и больше места на диске, поэтому необходимо вовремя удалять устаревшие записи, чтобы они не мешали нормальной работе компьютера. Делать это можно вручную или воспользоваться утилитой **logrotate**.

Утилита **logrotate** предназначена для автоматизации обработки журналов. Она может выполнять необходимые действия в зависимости от определенных условий и правил соответствия. Например, можно сжимать журналы в архив или отправлять на другой сервер, когда они достигают определенного размера, возраста или других параметров.

Проверку условий можно настроить ежедневно, еженедельно или ежемесячно - это позволяет создать схему ротации логов, удобную именно для вас и вашего сервера.

Logrotate — популярная утилита, поэтому в большинстве дистрибутивов она поставляется по умолчанию.

Вы можете подробнее ознакомиться с возможностью настройки ротации логов при помощи утилиты **logrotate**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка ротации логов: logrotate;
- в **Яндекс.Дзен** — Настройка ротации логов: logrotate;
- в **VK Видео** — Настройка ротации логов: logrotate.

На наших каналах вы также сможете найти много другой полезной информации.

В дистрибутиве РЕД ОС программа также является предустановленной, поэтому даже установка ОС подробно записывается в журнал:

```
ls /var/log/anaconda/

anaconda.log     journal.log            packaging.log    X.log
dbus.log         ks-script-mmizpj2u.log  program.log
dnf.librepo.log  ks-script-z8uq2i_g.log  storage.log
hawkey.log       lvm.log                syslog
```

Все основные настройки программы находятся в файле **/etc/logrotate.conf**.

Для дополнительных настроек в основном файле указана папка **/etc/logrotate.d**. Собственные настройки лучше сохранять именно в данном каталоге, так ими будет проще управлять.

```
nano /etc/logrotate.conf

# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

Основные параметры для настройки

Чтобы указать частоту выполнения проверок на совпадение условий, используются следующие директивы:

- *hourly* - каждый час;
- *daily* - каждый день;
- *weekly* - каждую неделю;
- *monthly* - каждый месяц;
- *yearly* - каждый год.

По умолчанию настроена еженедельная (*weekly*) проверка.

Рассмотрим основные параметры управления и обработки журналов:

- **rotate** — указывает, сколько старых логов нужно хранить (в параметрах передается количество);
- **create** — создание пустого файла лога после перемещения старого;
- **dateext** — перед заголовком старого лога добавляется дата ротации;
- **compress** — сжатие логов;
- **delaycompress** — не сжимать последний и предпоследний журнал;
- **extension** — сохранять оригинальный лог-файл после ротации, если у него указано расширение;
- **mail** — отправлять e-mail после завершения ротации;
- **maxage** — выполнять ротацию журналов, если они старше, чем указано;
- **missingok** — не выдавать ошибки, если лог-файла не существует;
- **olddir** — перемещать старые логи в отдельную папку;
- **postrotate/endscript** — выполнить произвольные команды после ротации;
- **start** — номер, с которого будет начинаться нумерация старых логов;
- **size** — размер лога, когда он будет перемещен.

По умолчанию настроено хранение четырех старых файлов журналов, создание нового пустого файла журнала после перемещения старых и использование даты ротации при создании файлов журнала.

Вспомогательные настройки

В каталоге дополнительных настроек **/etc/logrotate.d** находятся несколько файлов, по названиям и содержимому которых можно определить, к журналам какой программы они относятся:

```
ls /etc/logrotate.d/

bootlog   chrony   glusterfs   kadmind   ppp    samba   syslog         wtmp
btmp      dnf      iscsiuiolog krb5kdc   psacct sssd    wpa_supplicant yum
```

В файлах содержатся правила обработки отдельных журналов.

В качестве примера рассмотрим параметры файла конфигурации **bootlog**:

```
cat /etc/logrotate.d/bootlog

    /var/log/boot.log
    {
1.      missingok
2.      daily
3.      copytruncate
4.      rotate 7
5.      notifempty
    }
```

Файл состоит из одной записи, которая, в свою очередь, разделена на две части:

- *имя файла*, который нужно обрабатывать (**/var/log/boot.log**);
- *параметры обработки*, указанные в фигурных скобках.

Описание параметров обработки:

1. **missingok** – не выдавать ошибки, если лог-файла не существует;
2. **daily** – обрабатывать журнал каждый день;
3. **copytruncate** – обрезать оригинальный файл до нулевого размера после создания копии вместо переименования оригинального файла и создания нового.
4. **rotate** 7 – необходимо хранить 7 старых файлов журналов;
5. **notifempty** – не ротировать файл лога, если он пуст.

Рассмотрим ещё один файл конфигурации - **sssd**.

```
cat /etc/logrotate.d/sssd

/var/log/sssd/*.log {
    weekly
    missingok
    notifempty
    sharedscripts
    rotate 2
    compress
    delaycompress
    postrotate
        /bin/kill -HUP `cat /var/run/sssd.pid  2>/dev/null`  2> /dev/null || true
    endscript
```

Здесь та же структура, но в конфигураторе дополнительно указана команда терминала, заключенная в postrotate и endscript. Строки, находящиеся между данными служебными словами, каждое из которых должно находиться в отдельной строке, выполняются с использованием **/bin/sh** после ротации файла журнала.

Проверка конфигурации

После настройки какого-либо файла конфигурации **logrotate** желательно проверить его корректность. Для этого необходимо запустить утилиту **logrotate** с опцией **-d**, она выведет все, что планируется сделать, но не будет изменять файлы на диске.

Рассмотрим действие утилиты на примере файла **/var/log/bootlog**:

```
logrotate -d /etc/logrotate.d/bootlog

 WARNING: logrotate in debug mode does nothing except printing debug messages!  Consider using verbose mode (-v) instead if this is not what you want.

reading config file /etc/logrotate.d/bootlog
Reading state from file: /var/lib/logrotate/logrotate.status
Allocating hash table for state file, size 64 entries

Handling 1 logs

rotating pattern: /var/log/boot.log
 after 1 days (7 rotations)
empty log files are not rotated, old logs are removed
considering log /var/log/boot.log
  Now: 2022-12-05 07:56
  Last rotated at 2022-12-02 00:00
  log does not need rotating (log is empty)
```

Если сообщений об ошибках нет, можно считать, что настройка завершена успешно.

Сбор диагностической информации о РЕД ОС (loginfo)

Графический интерфейс
Консольный вариант

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** loginfo-0.15-1

loginfo – утилита сбора технической информации о РЕД ОС для технической поддержки.

Вы можете подробнее ознакомиться с работой утилиты **loginfo**, просмотрев наши обучающие видео:

- на **RuTube** — Сбор диагностической информации о РЕД ОС;
- в **Яндекс.Дзен** — Сбор диагностической информации о РЕД ОС;
- в **VK Видео** — Сбор диагностической информации о РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

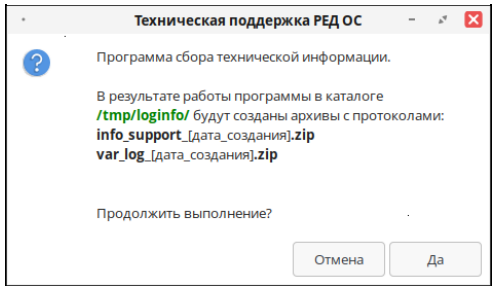
и выполните команду:

```
dnf install loginfo
```

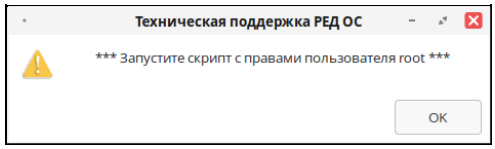
Графический интерфейс

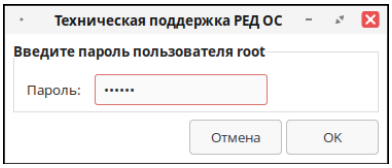
Запуск утилиты доступен из «**Главного меню**» - «**Системные**» - «**Сбор информации о системе**».

При инициализации утилиты вы увидите следующее диалоговое окно:

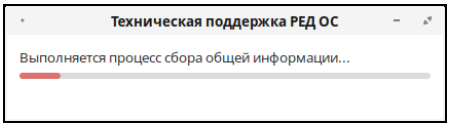


Т.к. для работы в программе необходимы права пользователя **root**, будет выведено следующее предупреждение и произведен запрос на ввод пароля пользователя **root**.



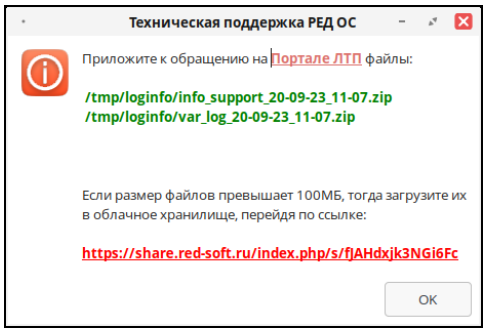


Будет запущен процесс сбора информации.



После сбора информации будет выведено информационное сообщение с контактами для отправки собранных данных в техническую поддержку.

Архивные файлы будут сформированы по пути **/tmp/loginfo**.



Консольный вариант

Для работы с утилитой необходимы права пользователя **root**:

```
su -
```

Для запуска процесса сбора информации выполните:

```
loginfo.sh
```

Loginfo также поддерживает дополнительный функционал, для просмотра выполните:

```
loginfo.sh --help
```

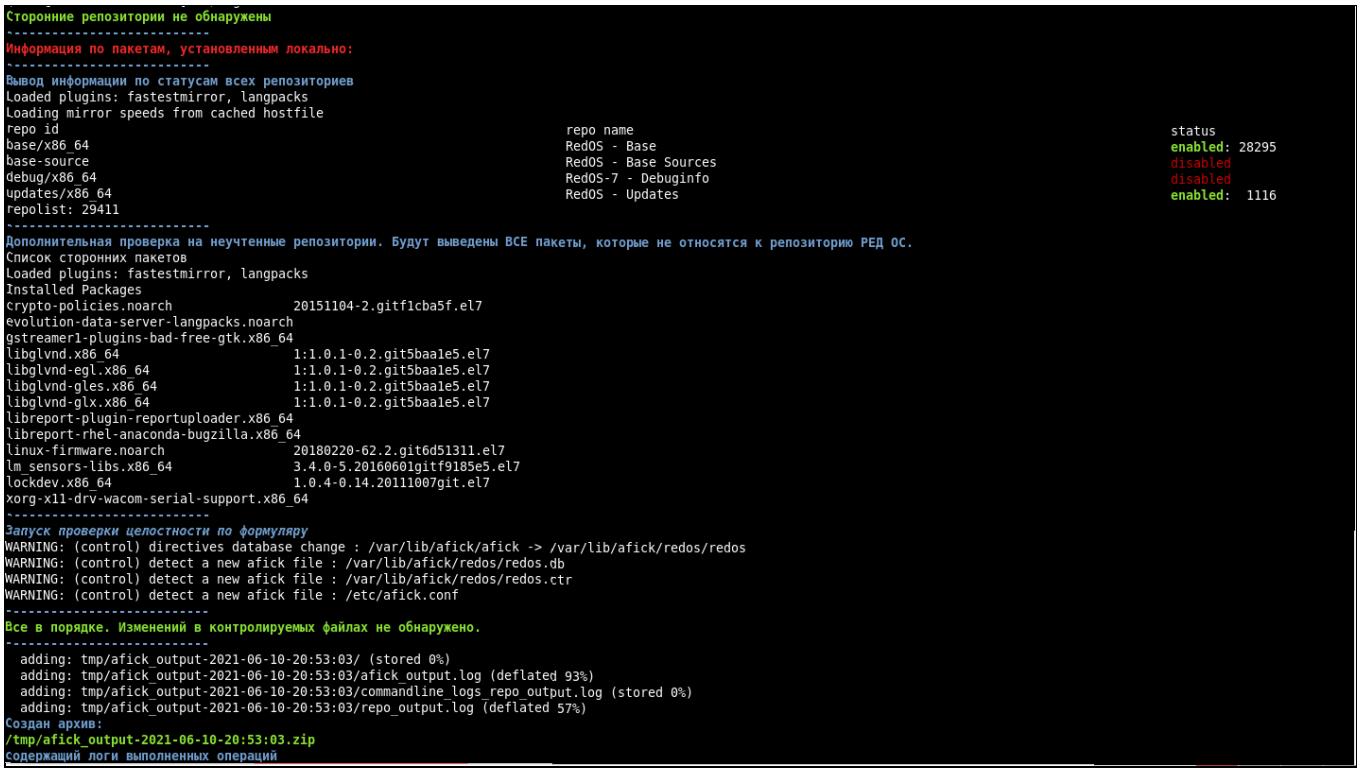
Для примера выполним дополнительную диагностику ОС.

Создание краткой сводки по аппаратным характеристикам:

```
loginfo.sh --hw-id

Создан файл /tmp/loginfo/hw-id-2022-06-21-11-50-35.txt
```

Проверка целостности сертифицированной редакции РЕД ОС:

```
loginfo.sh --afick
```



Контроль целостности системы РЕД ОС также осуществляется с помощью утилиты **afick**. Подробнее см. в нашей статье «Afick - утилита контроля целостности системы».

Настройка systemd-coredump для автоматического сбора дампов в РЕД ОС 7.3

Настройка сбора дампов
Изменение места сохранения дампов
Проверка работоспособности создания дампа
Чтение дампов ядра
Настройка сбора дампов в СУБД Ред База Данных

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: systemd-246.10-16

Дамп памяти (*core dump*) — содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы, например, значения регистров процессора и содержимое стека. Многие операционные системы позволяют сохранять дамп памяти для отладки программы. Как правило, дамп памяти процесса сохраняется автоматически, когда процесс завершается из-за критической ошибки (например, из-за ошибки сегментации). Дамп также можно сохранить вручную через отладчик или любую другую специальную программу.

Настройка сбора дампов

В РЕД ОС 7.3 для автоматического сбора дампов используется обработчик дампов **systemd-coredump** — он собирает информацию о процессе при аварийном завершении программы. Для проверки сбора дампов выполните команду:

```
cat /proc/sys/kernel/core_pattern
|/usr/lib/systemd/systemd-coredump %P %u %g %s %t %c %h
```

Размер дампов определяется в файле конфигурации **/etc/systemd/coredump.conf**. Для изменения размера дампов в секции [Coredump] необходимо раскомментировать следующие параметры:

```
Compress=yes
ProcessSizeMax=<максимальный_размер_дампов>
ExternalSizeMax=<максимальный_размер_сжатого_дампа>
```

Далее будут подробнее рассмотрены параметры конфигурационного файла:

- Storage — определяет место хранения дампа процесса, может принимать одно из значений: *none*, *external*, *journal*.
  - *none* — дампы ядра записываются (включая обратную трассировку, если возможно), но не сохраняются;
  - *external* — значение по умолчанию, дампы сохраняются в каталоге **/var/lib/systemd/coredump/**;
  - *journal* — дампы будут храниться в журнале и перезаписываться в соответствии со стандартными принципами ротации журналов.
- Compress — используется для сжатия дампов ядра. Принимает логический аргумент — *yes* или *no*:
  - *yes* — дампы сжимаются при сохранении (значение по умолчанию);
  - *no* — дампы сохраняются без сжатия.
- ProcessSizeMax — определяет максимальный размер дампа процесса, который может быть сохранен. Если размер дампа превышает значение этого параметра, то дамп сохранен не будет. Это позволяет ограничить размер дампов и избежать переполнения дискового пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *до 1ГБ* — в 32-битных системах, *32ГБ* — в 64-битных системах. Параметры Storage=none и ProcessSizeMax=0 отключает всю обработку дампа памяти, за исключением записи журнала.
- ExternalSizeMax и JournalSizeMax — определяет максимальный (сжатый или несжатый) размер дампа процесса, который будет сохранен на диске (по умолчанию *1 ГБ* — в 32-разрядных системах, *2 ГБ* — в 64-разрядных системах), или в журнале системы (по умолчанию 10M).
- MaxUse — определяет максимальный объем общего дискового пространства, который может быть использован для хранения дампов процессов. Если общий размер всех дампов превышает значение этого параметра, старые дампы будут удаляться для освобождения места для новых. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию ограничение равно *10% от общего размера диска*.
- KeepFree — определяет минимальный объем свободного дискового пространства, который должен оставаться на диске при хранении дампов. Если свободного места на диске становится меньше указанного значения, новые дампы не будут создаваться

до тех пор, пока не будет предоставлено достаточного объема свободного пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *15% от общего размера диска* должно оставаться свободным. Старые дампы ядра также удаляются в зависимости от времени с помощью **systemd-tmpfiles**.

Изменение места сохранения дампов

Дампы по умолчанию будут создаваться в каталоге **/var/lib/systemd/coredump**. Служба **systemd-coredump** не имеет параметра конфигурации для изменения каталога, в котором будут храниться дампы.

Для смены каталога создания дампов необходимо использовать **bind-mount**:

1. В файле **/etc/fstab** пропишите монтирование нужной директории для сохранения дампов следующим образом:

```
/каталог/для/дампов /var/lib/systemd/coredump none defaults,bind 0 0
```

2. Примонтируйте каталог:

```
mount /var/lib/systemd/coredump
```

3. Перезапустите службу **systemd** для применения изменений:

```
systemctl daemon-reload
```

Проверка работоспособности создания дампа

Для проверки создания дампа необходимо выполнить в терминале:

```
sleep 3600 &
kill -11 %1
```

Проверьте создание дампа с помощью утилиты **coredumpctl**:

```
coredumpctl
```

Рассмотрим дополнительные опции **coredumpctl**:

- **list** — список доступных дампов ядра;
- **info <PID>** — вывод подробной информации об указанном дампе ядра;
- **gdb <файл>** — запускает отладчик **gdb** (GNU Debugger) для анализа дампа ядра;
- **dump <PID>** — создает дамп ядра с указанным идентификатором (PID). Дамп ядра будет передан на стандартный вывод, если не указан выходной файл с помощью **--output=**;
- **debug <PID>** — запуск процесса с указанным PID в режиме отладки. По умолчанию используется **gdb**. Отладчик может быть изменен с помощью параметра **--debugger=** или переменной среды **$SYSTEM_DEBUGGER**. Для передачи отладчику дополнительных аргументов командной строки используется параметр **--debugger-arguments=**.

Чтение дампов ядра

Сводную информацию о дампе ядра, соответствующем определенному процессу, в котором произошел сбой, можно получить, выполнив команду:

```
coredumpctl info _PID=<PID_процесса,по_которому_создан_дамп>
```

```
[user@localhost ~]$ coredumpctl info _PID=2772
           PID: 2759 (bash)
           UID: 1000 (user)
           GID: 1000 (user)
        Signal: 6 (ABRT)
     Timestamp: Fri 2023-03-31 11:46:40 MSK (20min ago)
  Command Line: bash 1212.sh
    Executable: /usr/bin/bash
 Control Group: /user.slice/user-1000.slice/session-2.scope
          Unit: session-2.scope
         Slice: user-1000.slice
       Session: 2
     Owner UID: 1000 (user)
       Boot ID: df6eee73274847bf9b977b2b77d47391
    Machine ID: 1e8ddb949cf549d8a2785068c77b85cd
      Hostname: localhost.localdomain
       Storage: /var/lib/systemd/coredump/core.bash.1000.df6eee73274847bf9b977b2b77d47391.2759.16802
       Message: Process 2759 (bash) of user 1000 dumped core.

                Stack trace of thread 2759:
                #0  0x00007fe88a6e715b __waitpid (libc.so.6 + 0xcc15b)
                #1  0x0000000000451619 waitchld.isra.12 (bash + 0x51619)
                #2  0x000000000052dfa wait_for (bash + 0x52dfa)
                #3  0x000000000043fbd7 execute_command_internal (bash + 0x3fbd7)
                #4  0x000000000043fe76 execute_command (bash + 0x3fe76)
                #5  0x0000000000426a21 reader_loop (bash + 0x26a21)
                #6  0x0000000000425144 main (bash + 0x25144)
                #7  0x00007fe88a642413 __libc_start_main (libc.so.6 + 0x27413)
                #8  0x00000000004256ce _start (bash + 0x256ce)
lines 1-28/28 (END)
```

Для полного чтения дампа необходимо установить утилиту **gdb**, выполнив команду (с правами суперпользователя **root** или администратора системы):

```
dnf install gdb
```

Запустите анализ дампа, выполнив команду:

```
coredumpctl gdb _PID=<PID_процесса,по_которому_создан_дамп>
```

```
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/bash...

warning: Unable to open "librpm.so.8" (librpm.so.8: cannot open shared object file: No such file or d
irectory), missing debuginfos notifications will not be displayed
Missing separate debuginfo for /usr/bin/bash
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/58/dbe494d53a3772d3e6f32b6c97e5b573
228ef.debug
Reading symbols from .gnu_debugdata for /usr/bin/bash...
(No debugging symbols found in .gnu_debugdata for /usr/bin/bash)
[New LWP 2759]
Missing separate debuginfo for /lib64/libiniparser.so.1
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/8c/f382586277a70f91a9befa609e0e1393
4ee12.debug
Missing separate debuginfo for /lib64/libtinfo.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/b7/b929fb355f28f374b5054d3191fc05a7
b5802.debug
Missing separate debuginfo for /lib64/libdl.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/e7/e6d7db0bca11a7f7da45896c9165d369
d14ab.debug
Missing separate debuginfo for /lib64/libc.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/75/b55efed6938ccb77e0e40fff7571aae0
ffcc0.debug
Missing separate debuginfo for /lib64/ld-linux-x86-64.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/73/db0afd7ec02589302cf7bd90ae12d482
6a6e3.debug
Core was generated by `bash 1212.sh'.
Program terminated with signal SIGABRT, Aborted.
#0  0x00007fe88a6e715b in waitpid () from /lib64/libc.so.6
(gdb)
```

Настройка сбора дампов в СУБД Ред База Данных

Для сбора дампов *СУБД Ред База Данных* необходимо в файл службы **/usr/lib/systemd/system/firebird.service** в секцию [Service] добавить строку:

```
LimitCORE=infinity
```

Для этого необходимо воспользоваться редактированием модуля юнита с помощью команды:

```
systemctl edit firebird
```

И добавить следующие строки:

```
[Service]
LimitCORE=infinity
```

После сохранения сформируется файл **/etc/systemd/system/firebird.service.d/override.conf**.

При загрузке модуля **systemd** в памяти соединит фрагмент сформированного файла (**/etc/systemd/system/firebird.service.d/override.conf**) с полным файлом модуля (**/usr/lib/systemd/system/firebird.service**). Директивы фрагмента получат приоритет над найденными директивами в оригинальном файле модуля. Для проверки всех подгружаемых фрагментов необходимо выполнить:

```
systemctl cat firebird
```

Если СУБД при работе потребляет большой объем памяти (настроен большой страничный кэш), то создание дампа на диске после падения может продолжаться некоторое время. В конфигурационном файле службы **coredump** может быть настроен таймаут работы, после которого она будет остановлена. Для того чтобы времени на создание дампа было достаточно, необходимо увеличить таймаут, например, до 30 минут, изменив значение параметра `RuntimeMaxSec` в файле **/usr/lib/systemd/system/systemd-coredump@.service**:

```
RuntimeMaxSec=30min
```

ВАЖНО!

Дампы ядра полезны для устранения неполадок, однако могут являться причиной “утечки” конфиденциальных данных. Рекомендуется отключать дампы ядра и включать их только тогда, когда это действительно необходимо.

Для отключения сбора дампов ядра необходимо остановить службу **systemd-coredump**:

```
systemctl disable systemd-coredump
systemctl stop systemd-coredump
```

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

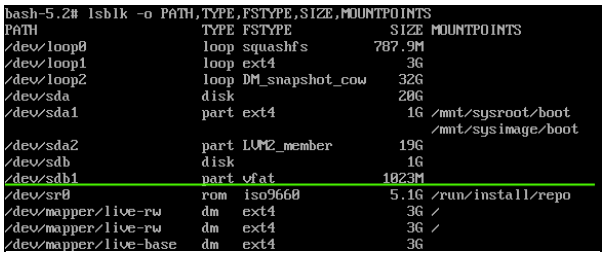
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

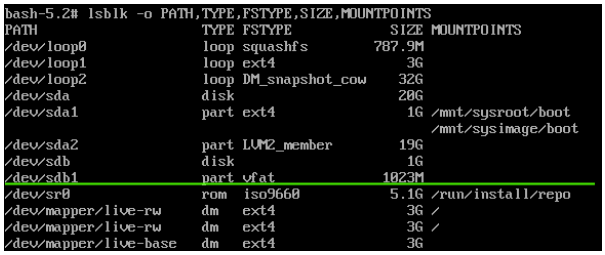
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Рекомендации по анализу журналов и дампов

1. Системные журналы событий ОС находятся в каталоге **/var/log/**, также можно использовать утилиту **journalctl** для просмотра журналов.

Подробную информацию по работе с утилитой **journalctl** см. в нашей статье «Работа с логами (утилита journalctl)».

Пример фильтрации содержимого журнала по типу ошибок:

```
journalctl -p err
journalctl -p alert
```

2. При анализе логов следует обращать внимание на ключевые слова, которые фигурируют в строках журналов:

- **failed** – обычно указывает на неудачное выполнение какой-либо операции или задачи. Например, сообщение вида authentication failed означает, что аутентификация завершилась неудачно;
- **error** – указывает на наличие ошибки. Далее может быть расшифровка ошибки и представлен ее код;
- **panic** – может появиться в записях, связанных с *Kernel Panic*, ошибками ядра Linux;
- **exception** – указывает на исключения (нештатную ситуацию или ошибку, которую программа или ядро не может обработать) в приложениях или ядре;
- **segfault** – ошибка сегментации, указывает на попытку доступа к памяти, к которой нет разрешения;
- **denied** – указывает на отказ в доступе, например, сообщение вида permission denied может быть связано с проблемами в правах доступа;
- **unable** – такие записи могут указывать на неспособность системы выполнить какое-либо определенное действие;
- **timeout** – задержки и таймауты могут указывать на проблемы с сетью или системными ресурсами;
- **crash** – аварийное завершение приложений или служб;
- **warning** – предупреждение о потенциальных проблемах, которые не вызывают сбоев, но требуют внимания;
- **critical** – критические события;
- **fatal** – критическая ошибка, которая приводит к сбою;
- **corruption** – обычно указывает на повреждение данных или файлов.

3. После определения кода или названия ошибки, которая связана со сбоем, уточняется ее более подробное описание, возможные причины возникновения, способы устранения. Поиск осуществляется в общедоступных поисковых системах, в системах отслеживания ошибок (*Bug tracking system*) по исследуемому компоненту или программе, а также соответствующим запросом в Техническую Поддержку программного продукта, в котором произошел инцидент.

4. Инструкция по работе с **coredump** — «Настройка systemd-coredump для автоматического сбора дампов».

5. Инструменты для анализа логов:

- средство просмотра файлов журналов **lnav** — «Средство просмотра журналов Log File Navigator (LNAV)»;
- веб-приложение для просмотра логов **loganalyzer** — «LogAnalyzer – веб-приложение для просмотра системных журналов».

Командные оболочки (интерпретаторы)

Для управления ОС используется командные интерпретаторы (shell). Зайдя в систему, пользователь увидит приглашение - строку, содержащую символ «$» (далее этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора - передавать команды пользователя операционной системе. При помощи командных интерпретаторов можно писать небольшие программы - сценарии (скрипты). Оболочкой по умолчанию в РЕД ОС является «**Bash**» (Bourne Again Shell) Чтобы проверить, какая оболочка используется, необходимо выполнить команду:

```
echo $SHELL
```

Вы можете подробнее ознакомиться с возможностями работы **bash**, просмотрев наши обучающие видео:

- на **RuTube**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **Яндекс.Дзен**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **VK Видео**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.

На наших каналах вы также сможете найти много другой полезной информации.

Командная оболочка Bash

В bash имеется несколько приемов для работы со строкой команд. Например, используя клавиатуру, можно:

- **Ctrl + A** - перейти на начало строки.
- **Ctrl + U** - удалить текущую строку.
- **Ctrl + C** - остановить текущую задачу.

Можно использовать «;» для того, чтобы ввести несколько команд одной строкой. Клавиши «вверх» и «вниз», позволяют вам перемещаться по истории команд.

Для того чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, необходимо набрать:

Ctrl + R

Команды, присутствующие в истории, отображаются в списке пронумерованными. Для того, чтобы запустить конкретную команду, наберите:

```
! <номер_команды>
```

если ввести:

```
!!
```

запустится последняя из набранных команд. Иногда имена программ и команд слишком длинны. Bash сам может завершать имена. Нажав клавишу [TAB], можно завершить имя команды, программы или каталога. Например, предположим, что необходимо использовать программу декомпрессии bunzip2. Для этого нужно набрать:

```
bu
```

затем нажать [TAB]. Если ничего не происходит, то, вероятно, существует несколько возможных вариантов завершения команды.

Нажав клавишу [TAB] еще раз, пользователь получит список имен, начинающихся с «bu». Например, может быть:

```
bu buildhash builtin bunzip2
```

Если далее добавить:

n

(bunzip - это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу [TAB], оболочка дополнит имя и остается лишь нажать «Enter», чтобы запустить команду. Программу, вызываемую из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH.

По умолчанию, в этот перечень каталогов не входит текущий каталог, обозначаемый «./» (точка слэш), поэтому для запуска программы **prog** из текущего каталога, надо дать команду:

```
./prog
```

Базовые команды оболочки Bash

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации используйте команду **man.**Пример:

```
man ls
```

Команда su

Позволяет получить права администратора. Когда пользователь набирает su, оболочка запрашивает пароль суперпользователя (root). Необходимо ввести пароль и нажать **Enter**. Чтобы вернуться к правам основного пользователя, необходимо набрать **exit**.

Команда cd

Позволяет сменить каталог. Она работает как с абсолютными, так и с относительными путями. Предположим, что находясь в своем домашнем каталоге и пользователь хочет перейти в его подкаталог **docs/**. Для этого нужно ввести относительный путь:

```
cd docs/
```

Чтобы перейти в каталог **/usr/bin** , нужно набрать (абсолютный путь):

```
cd /usr/bin/
```

Некоторые варианты команды:

```
cd ..
```

позволяет сделать текущим родительский каталог,

```
cd -
```

позволяет вернуться в предыдущий каталог. Команда cd без параметров переводит в домашний каталог.

Команда ls

ls (list) выдает список файлов в текущем каталоге. Синтаксис:

```
ls
```

Две основные опции:

- -a - просмотр всех файлов, включая скрытые,
- -l - отображение более подробной информации.

Команда rm

Эта команда используется для удаления файлов. Синтаксис:

```
rm <имя_файла>
```

У данной программы существует ряд параметров. Самые часто используемые:

- -i - запрос на удаление файла,
- -r - рекурсивное удаление (т.е. удаление, включая подкаталоги и скрытые файлы).

Команды mkdir и rmdir

Команда **mkdir** позволяет создать каталог, тогда как **rmdir** удаляет каталог, при условии, что он пуст. Синтаксис:

```
mkdir <имя_каталога>
```

```
rmdir <имя_каталога>
```

Команда **rmdir** часто заменяется командой **rm-rf** , которая позволяет удалять каталоги, даже если они не пусты.

Команда less

less позволяет постранично просматривать текст.

Синтаксис:

```
less <имя_файла>
```

Для выхода нужно нажать q.

Команда grep

Данная команда имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep <шаблон_поиска> <файл>
```

Команда ps

Отображает список текущих процессов. Колонка команд указывает имя процесса, колонка PID (идентификатор процесса) - номер процесса (этот номер используется, для операций с процессом, например чтобы «убить» его командой **kill**).

Синтаксис:

```
ps <аргументы>
```

Аргумент -u предоставляет больше информации, а -x позволяет просмотреть те процессы, которые не принадлежат пользователю (такие как те, что были запущены во время процесса загрузки).

Команда kill

Если программа перестала отвечать или зависла, необходимо использовать данную команду, чтобы её завершить.

Синтаксис:

```
kill <PID_номер>
```

Иногда необходимо будет использовать **kill -9** (когда обычная команда **kill** не дает желательного эффекта). Номер PID выясняется при помощи команды **ps**.

Горячие комбинации клавиш в Bash

Для удобства запоминания сочетания клавиш сгруппированы по действию. Обратите внимание, что **в комбинациях следует использовать левую клавишу Alt**, т.к. правая Alt Gr используется как клавиша Compose (специальная клавиша, позволяющая вводить символы с помощью определённых комбинаций клавиш).

Перемещение по тексту

Сочетание	Действие
Ctrl+a, Home	Переместить курсор в начало командной строки
Ctrl+e, End	Переместить курсор в конец командной строки
Ctrl+b, ←	Переход на один символ назад от курсора
Ctrl+f, →	Переход на один символ вперёд от курсора
Alt+b, Esc+b	Переместить курсор назад на одно слово
Alt+f, Esc+f	Переместить курсор вперёд на одно слово
Ctrl+xx	Переход от курсора в начало строки и обратно

Редактирование строки

Сочетание	Действие
Alt+?, Tab+Tab	Автодополнение команды или имени файла
Ctrl+u	Удалить все символы от курсора до начала командной строки
Ctrl+k	Удалить все символы от курсора до конца командной строки
Ctrl+w	Удалить символы от курсора до пробела слева
Alt+Backspace	Удалить символы от курсора до начала слова
Alt+d, Esc+d	Удалить символы от курсора до конца слова
Ctrl+y	Вставить символ, слово или текст, которые были удалены при помощи сочетаний клавиш, приведенных выше
Alt+y	Просмотреть буфер удалённых слов и вставить интересующее. Работает после нажатия Ctrl+y
Ctrl+h	Удалить перед курсором один символ
Ctrl+d	Удалить под курсором один символ
Alt+	Удалить любое количество пробелов вокруг курсора
Ctrl+_	Откатить редактирование
Alt+r, Esc+r	Отменить все изменения содержимого строки
Alt+c	Заменяет под курсором букву на заглавную и переводит курсор в конец слова
Alt+u	Переводит все буквы от курсора и до конца слова в заглавные
Alt+l	Переводит все буквы от курсора и до конца слова в нижний регистр
Alt+t	Замена текущего слова под курсором на предыдущее слово
Ctrl+t	Замена символа перед курсором на предыдущий символ

История команд

Сочетание	Действие
Ctrl+r	Искать команду по истории

Ctrl+g	Выйти из режима поиска в истории
Ctrl+p, ↑	Предыдущая команда в истории
Ctrl+n, ↓	Следующая команда в истории
Alt+<	Переход к первой команде в буфере истории
Alt+., Esc+.	Вставить последний аргумент предыдущей команды
Ctrl+o	Выполняет введённую команду и оставляет её же в командной строке

Выполнение и вывод на экран

Сочетание	Действие
Ctrl+l	Очистка экрана
Ctrl+s	Остановить вывод на экран
Ctrl+q	Возобновить вывод на экран, если он был приостановлен указанной выше командой
Ctrl+c	Прервать выполнение текущей команды
Ctrl+z	Приостановить выполнение текущей команды (для возобновления выполните fg)
Ctrl+d	Выйти из командной оболочки Bash

Информационный вывод

Сочетание	Действие
***+Alt+?, *+Tab+Tab**	Показать каталоги, кроме скрытых
$+Alt+?, $+Tab+Tab	Показать все системные переменные

Специальные клавиши

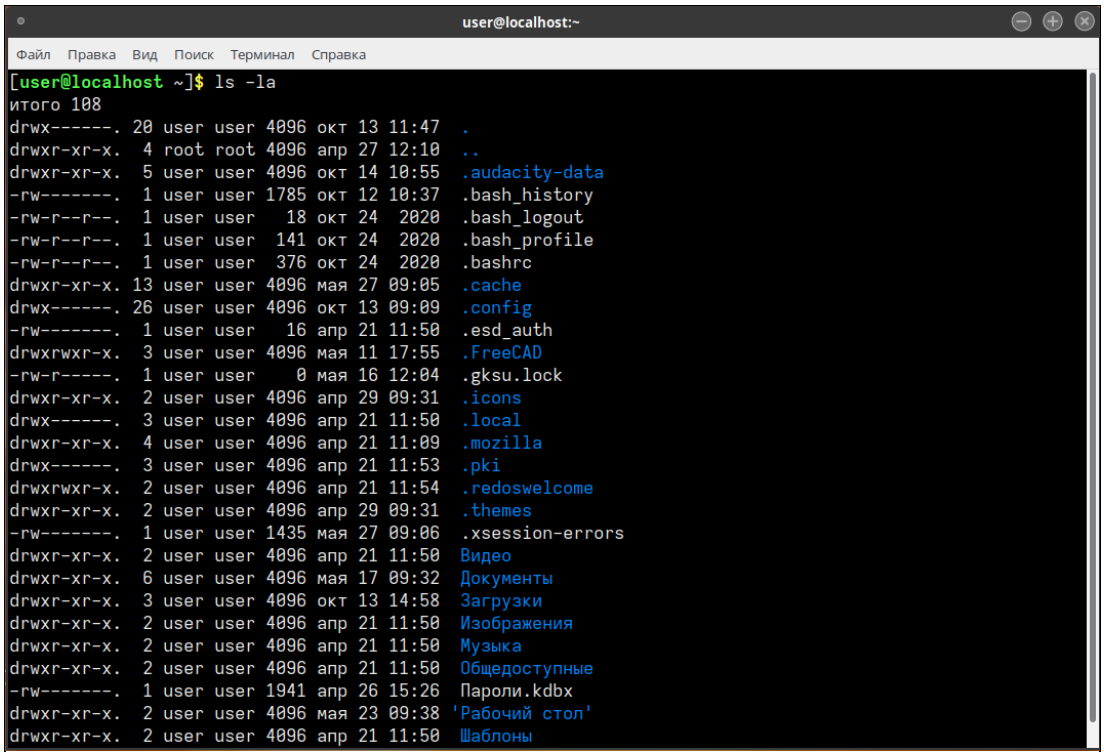
Сочетание	Действие
Ctrl+i	Tab
Ctrl+m	Enter
Ctrl+[	Esc

Основные утилиты в консоли РЕД ОС

ls

Утилита для просмотра содержимого каталогов. По умолчанию показывает содержимое текущего каталога. Если в параметрах указан путь к каталогу, она перечислит содержимое конечного каталога. Полезные опции:

- **-l** (list) - форматирует вывод в виде списка с более подробной информацией;
- **-a** (--all) - включает показ скрытых файлов;
- **--h** (help) - вывести справку по использованию утилиты.

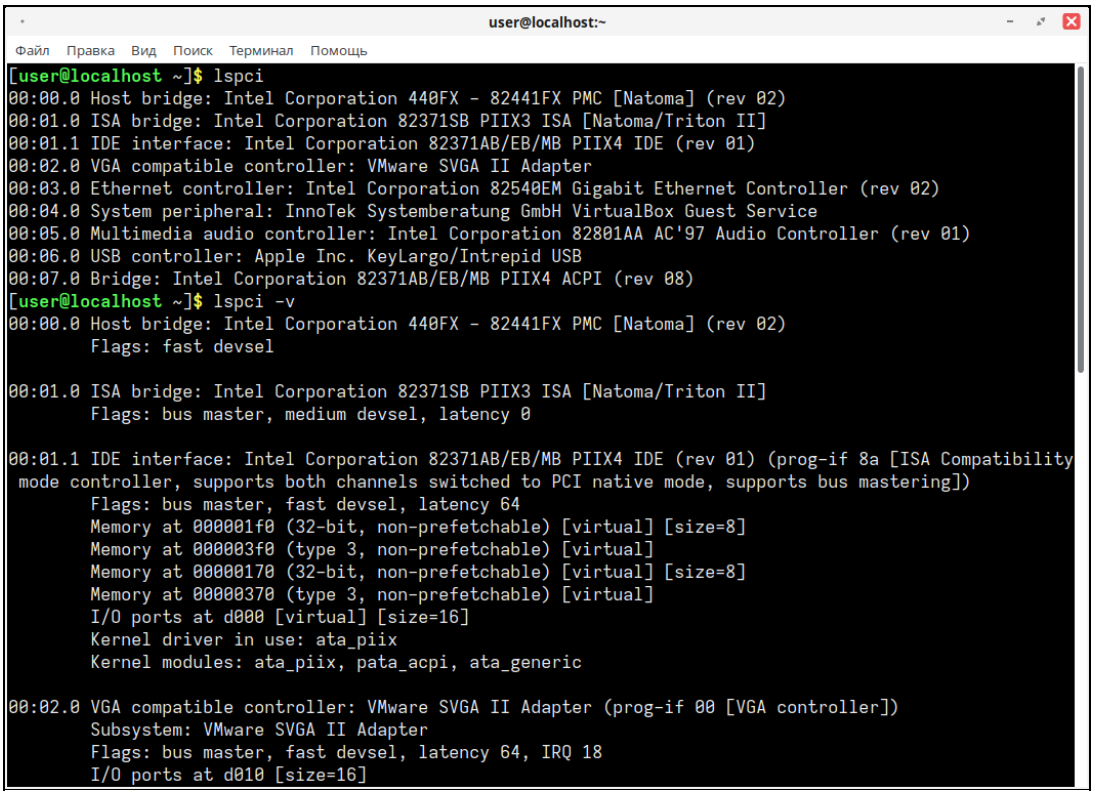


lspci

Команда **lspci** позволяет задействовать одноименную утилиту, предназначенную для вывода информации о PCI-шинах и подключенных к ним устройствах. Она поддерживает все разновидности PCI-шин: классическую шину **PCI** (Peripheral Component Interconnect), ее серверный вариант **PCI-X** и ее современный вариант **PCIe** (PCI-Express). Обычно к данной шине подключаются такие устройства, как графические, звуковые и сетевые карты, Wi-Fi и Bluetooth-адаптеры, SSD-накопители, а также множество других устройств.

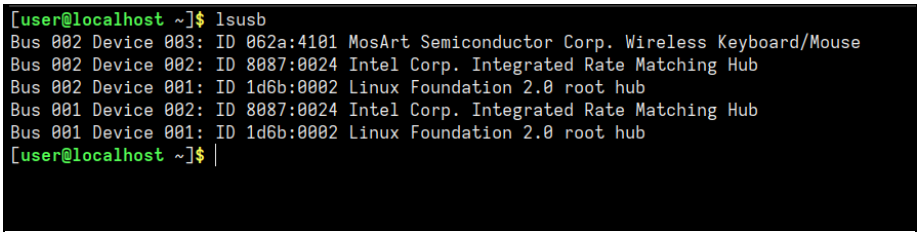
Наиболее полезные опции:

- **-m** и **-mm** — для вывода установленных производителем идентификаторов устройств;
- **-t** — для вывода информации в древовидном формате;
- **-v** — для вывода подробной информации об устройствах;
- **-n** — для вывода идентификаторов устройств;
- **-s** и **-d** — для вывода информации об устройствах в заданных слотах и с заданными идентификаторами соответственно.



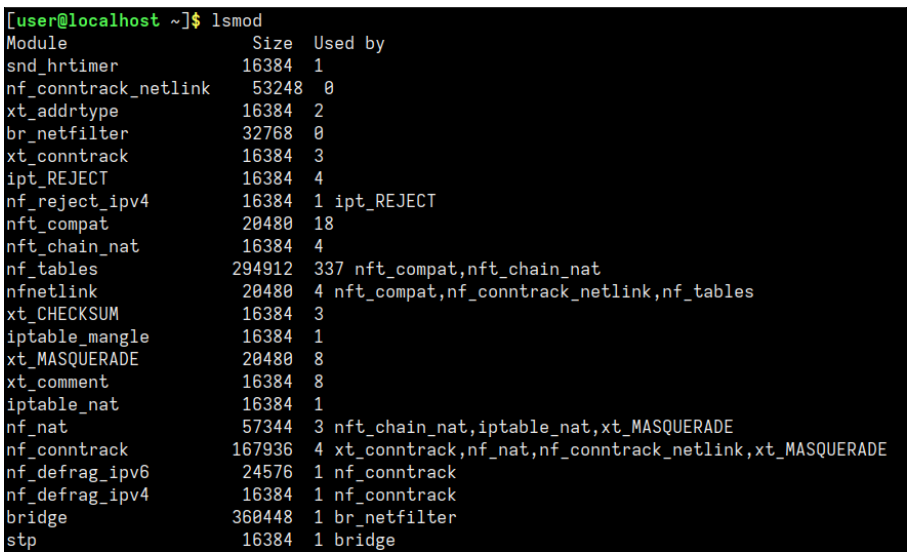
lsusb

Команда lsusb позволяет задействовать одноименную утилиту, предназначенную для вывода информации о USB-шинах и подключенных к ним устройствах. Каждое из устройств имеет пару 16-битных идентификаторов: идентификатор производителя (**Vendor ID**) и идентификатор устройства (**Device ID**), которые следует использовать для идентификации устройств и поиска драйверов в случае их отсутствия в ядре ОС, а также несколько дополнительных идентификаторов, устанавливаемых производителем.



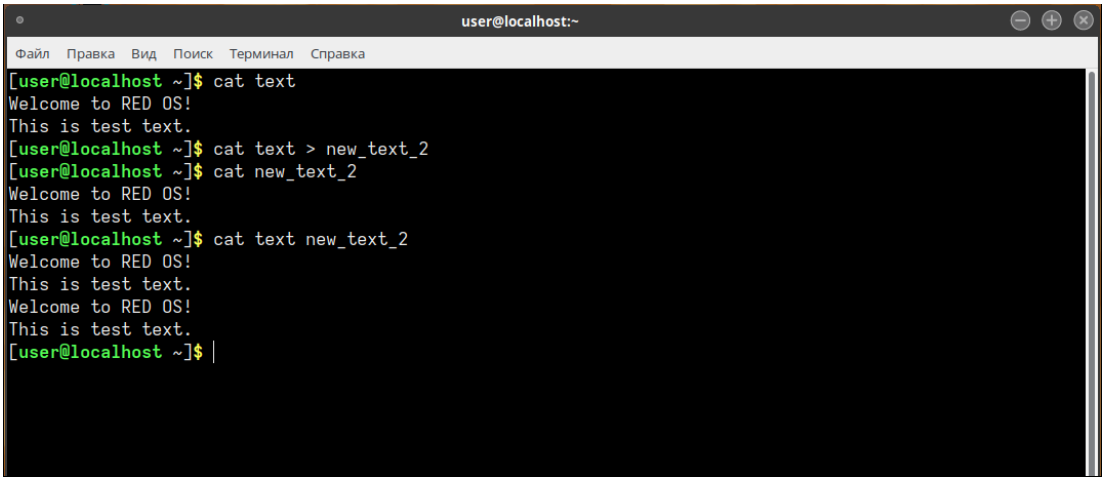
lsmod

Команда **lsmod** показывает, какие модули ядра загружены в системе в данный момент.



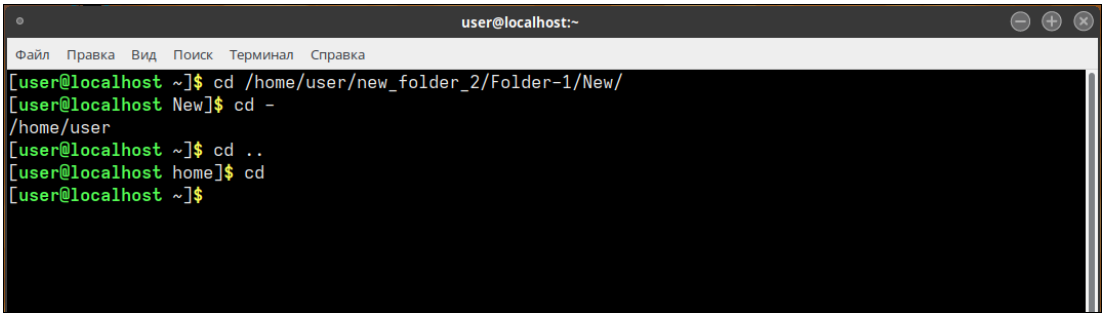
cat

Печатает содержимое файла, переданного в параметре, в стандартный вывод. Если передать несколько файлов, команда объединит их. Также можно перенаправить вывод в ещё один файл с помощью символа « **>** ».



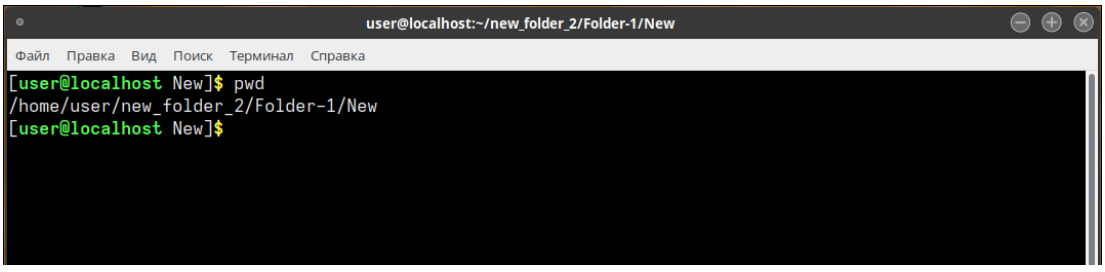
cd

Позволяет перейти из текущего каталога в указанный. Если запустить без параметров - возвращает в домашний каталог. Вызов с двумя точками (**cd ..**) - возвращает на уровень выше относительно текущего каталога. Вызов с тире (**cd -**) возвращает к предыдущему каталогу.



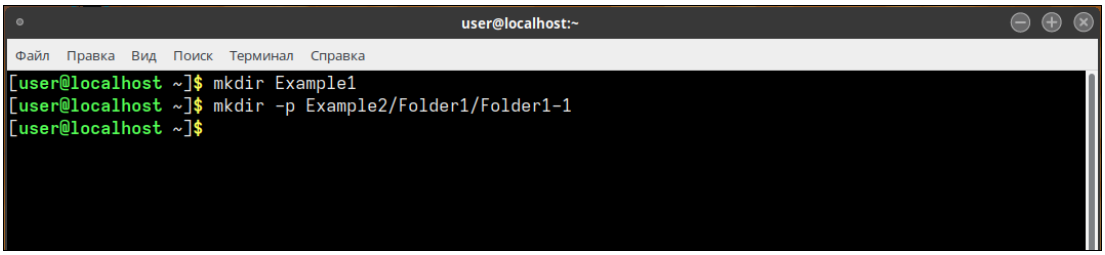
pwd

Выводит полный путь к текущему/рабочему каталогу.



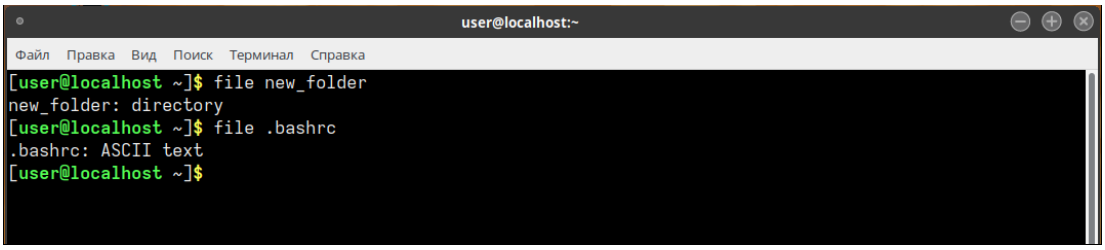
mkdir

Создание новых каталогов. Наиболее удобная опция **-p** (parents), позволяет создать всю структуру подкаталогов одной командой, даже если они ещё не существуют.



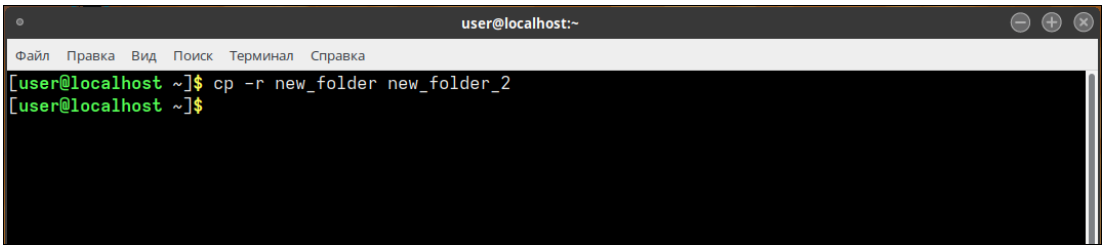
file

Показывает тип файла. В Linux файлы не обязаны всегда иметь расширения для того, чтобы с ними работать. Поэтому пользователю иногда трудно определить, какой именно перед ним файл. Данная утилита решает такую проблему.



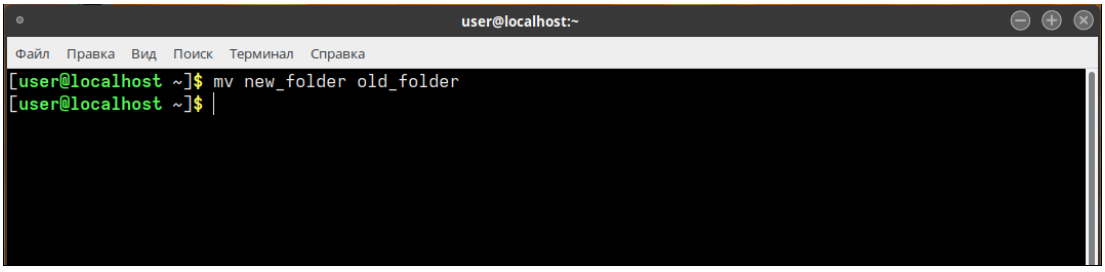
cp

Копирование файлов и каталогов. Утилита по умолчанию не копирует каталоги рекурсивно, поэтому необходимо добавить опцию **-r** (recursive) или **-a** (archive). Последняя включает режим сохранения атрибутов, владельца и временного штампа в дополнение к рекурсивному копированию.



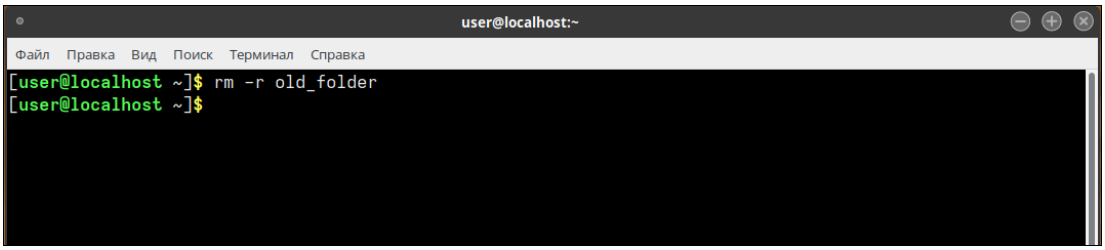
mv

Перемещение или переименование файлов и каталогов. В Linux это одна и та же операция. Переименование - это перемещение файла в ту же папку с другим именем.



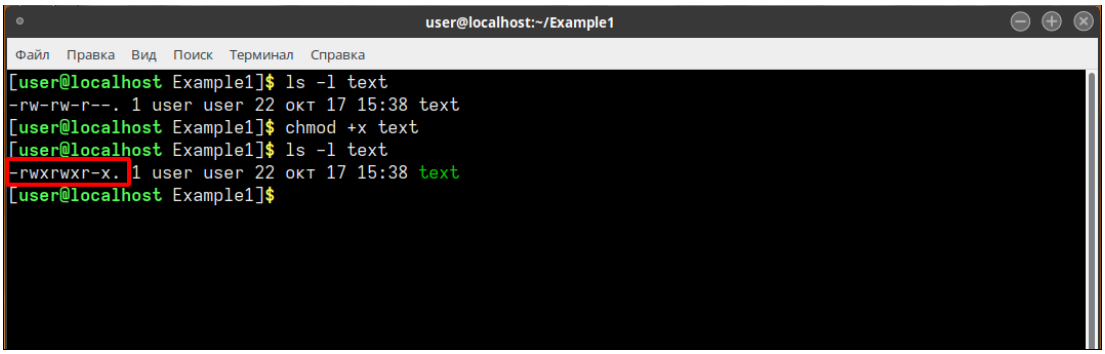
rm

Удаляет файлы и папки. Если нужно рекурсивное удаление, используйте опцию **-r**. **Rm** удаляет файлы не в корзину, из которой потом данные можно будет восстановить, а полностью их стирает. Действия оператора **rm** необратимы.



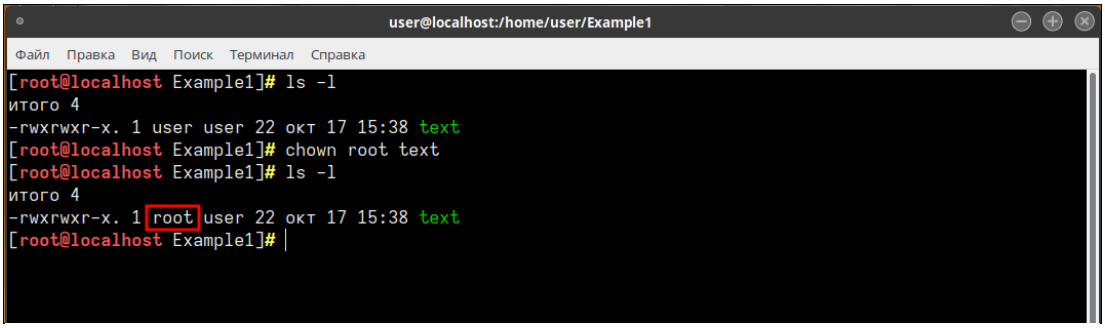
chmod

Изменяет права доступа к файлу - чтение, запись и выполнение. Каждый пользователь может изменять права для своих файлов.



chown

Изменяет владельца файла. Только суперпользователь может изменять владельцев. Для рекурсивного изменения используйте опцию **-R**.

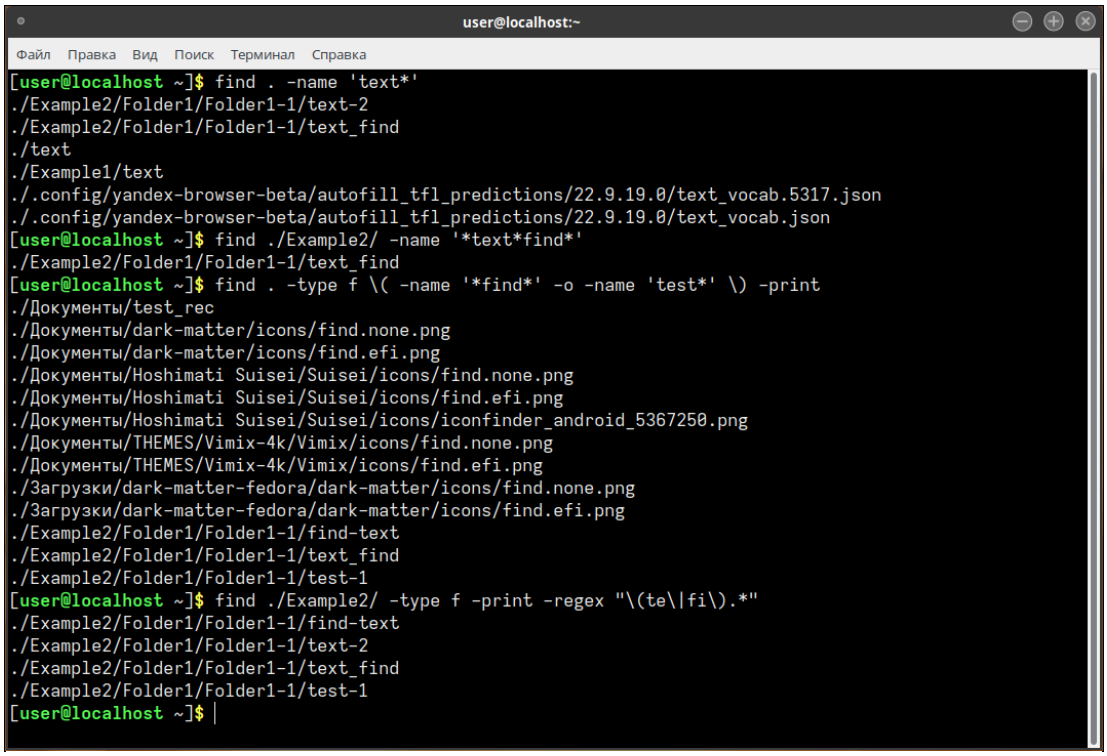


find

Очень гибкая и мощная команда Linux не только из-за своих способностей удобного поиска, но и благодаря возможности выполнять произвольные команды для найденных файлов. Поиск может осуществляться как в одном, так и в нескольких каталогах, имеется поддержка регулярных выражений для более точного поиска.

Основные опции:

- **-type** [f=файл, d=каталог (directory), l=ссылка (link), p=канал (pipe), s=сокет] - поиск по типу файла;
- **-name** '<имя_файла>' - поиск по имени файла, можно использовать как полное имя, так и его часть ('text' или 'te*');
- **-regex** "<регулярное_выражение>" - поиск файлов по регулярному выражению;
- **-print** - показать на экране найденные файлы.

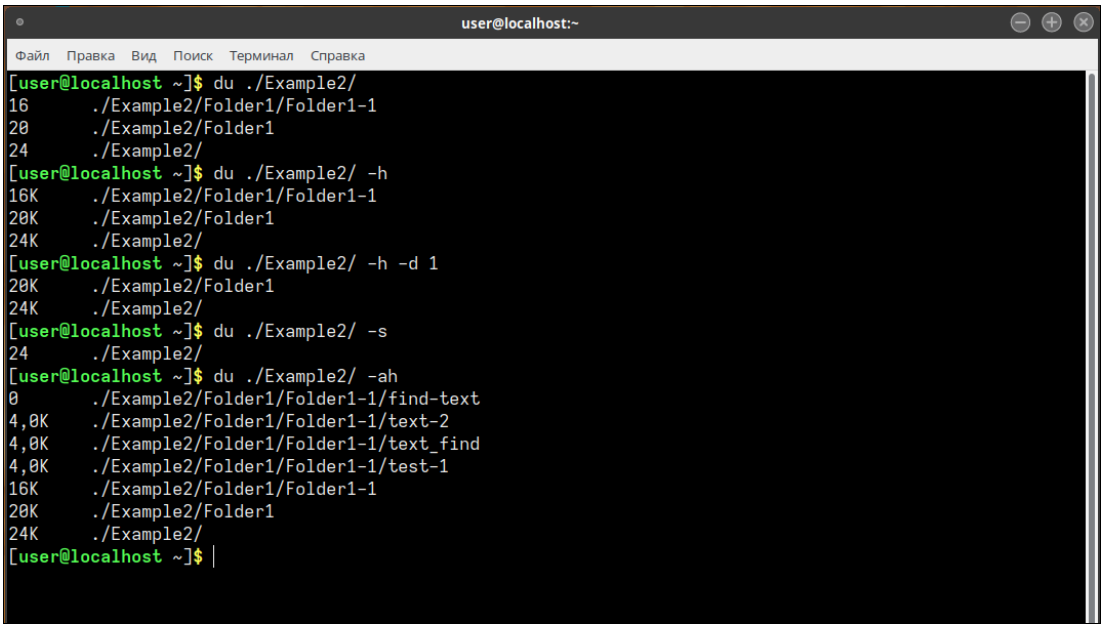


du

Показывает размер файла или каталога для оценки занимаемого файлового пространства.

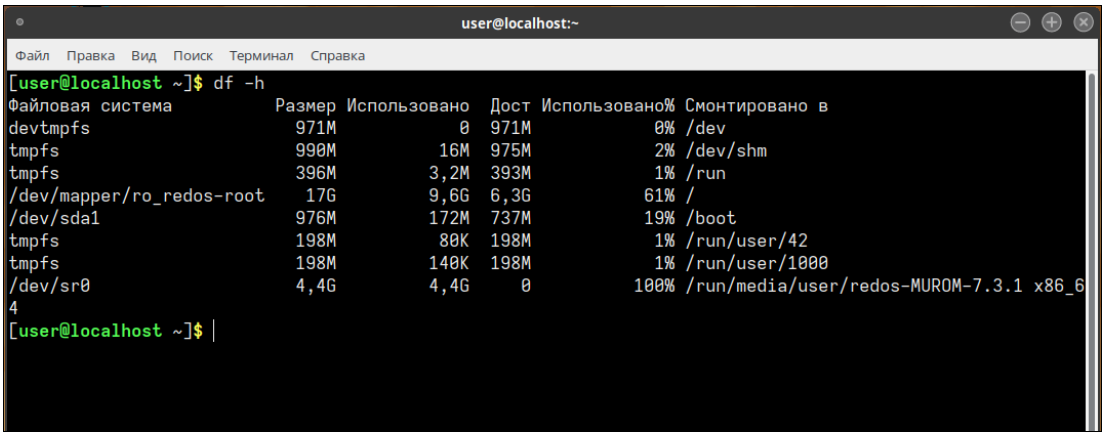
Полезные опции:

- **-a** (--all) - выводить размер для всех файлов, а не только для директорий, по умолчанию размер выводится только для папок;
- **-d** (--max-depth) - максимальная глубина вложенности директорий;
- **-h** (--human-readable) - преобразует размеры файлов в удобный формат;
- **-s** (--summarize) - выводит минимум данных.



df

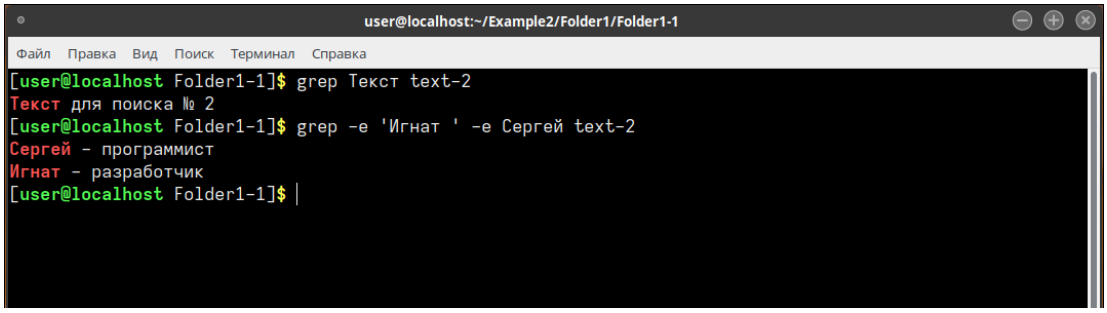
Используется для получения полной сводной информации о доступном и используемом дисковом пространстве файловой системы. По умолчанию вывод достаточно подробный: перечислены все файловые системы, их размер, количество использованного и свободного пространства. Для удобства можно использовать опцию **-h**, которая отобразит размеры удобными для чтения.



grep

Утилита **grep** ищет заданный шаблон или регулярное выражение из стандартного ввода или файла и печатает соответствующие заданным критериям строки. Утилита может вывести как полностью совпадающие, так и частично совпадающие строки и их контекст.

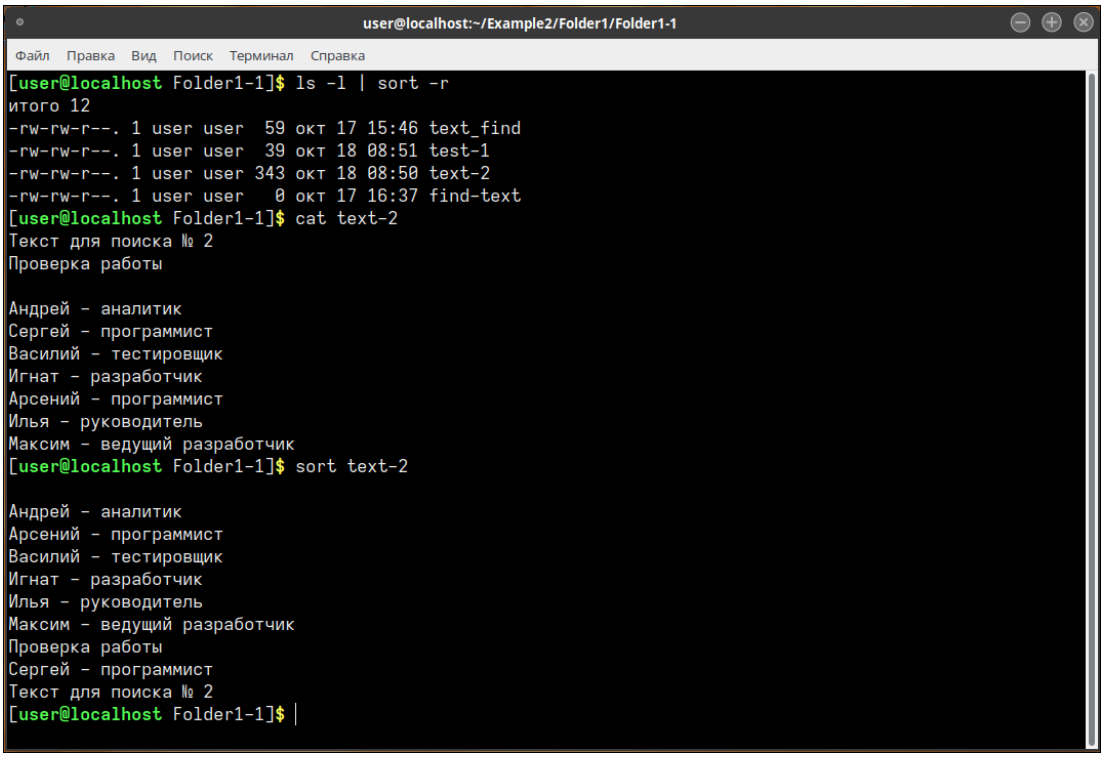
Команде **grep** также можно передавать и несколько параметров. Для этого перед каждым аргументом пишется ключ **-e**. Эту команду система понимает, как "или-или" и выводит все вхождения указанных слов. Кавычками выделяются только строки, содержащие пробел.

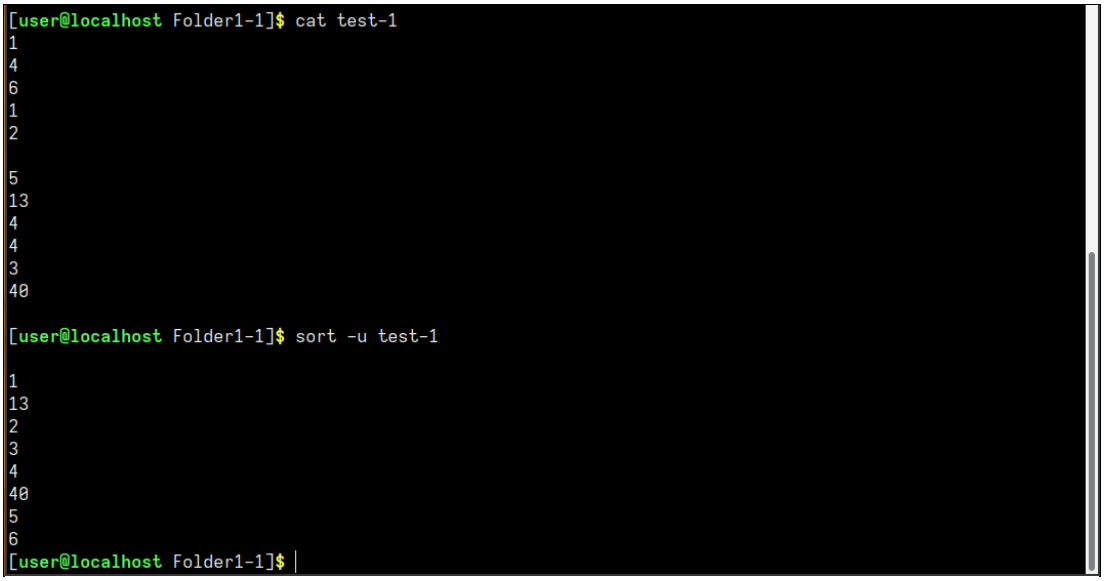


sort

Сортировка строк текста из одного или нескольких файлов по различным критериям, также может быть выполнена сортировка для вывода какой-либо команды. Наиболее полезные опции:

- **-b** - не учитывать пробелы;
- **-c** - проверить был ли отсортирован файл;
- **-n** (numeric) - сортирует по числовому значению;
- **-o** - вывести результат в файл;
- **-u** - игнорировать повторяющиеся строки
- **-r** (reverse) - сортирует в обратном порядке.



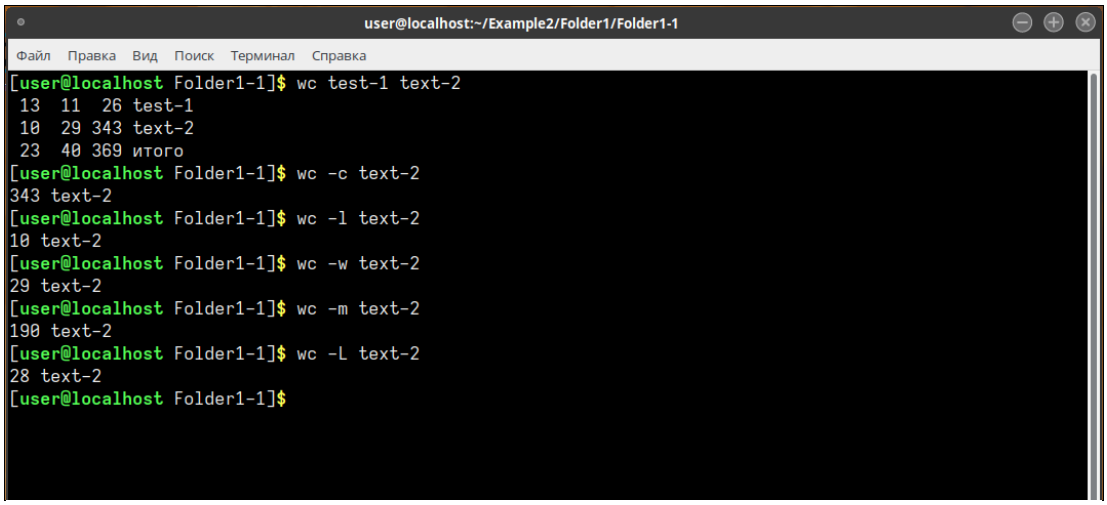


wc

Выводит число переводов строк, слов и байт для каждого указанного файла и итоговую строку, если было задано несколько файлов.

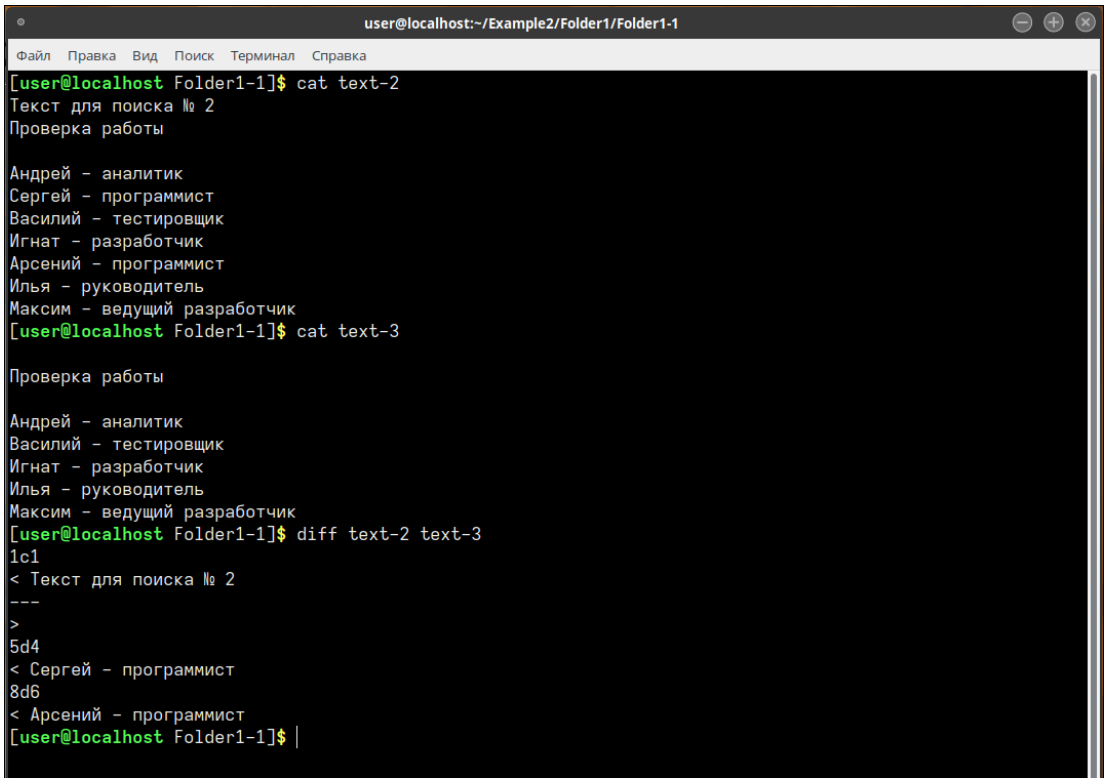
Основные опции:

- **-c**, **--bytes** – вывод размера файла в байтах;
- **-m**, **--chars** – вывод числа символов в файле;
- **-l**, **--lines** – вывод числа строк в файле;
- **-L**, **--max-line-length** – вывод максимальной длины строки в файле;
- **-w**, **--words** – вывод числа слов в файле.

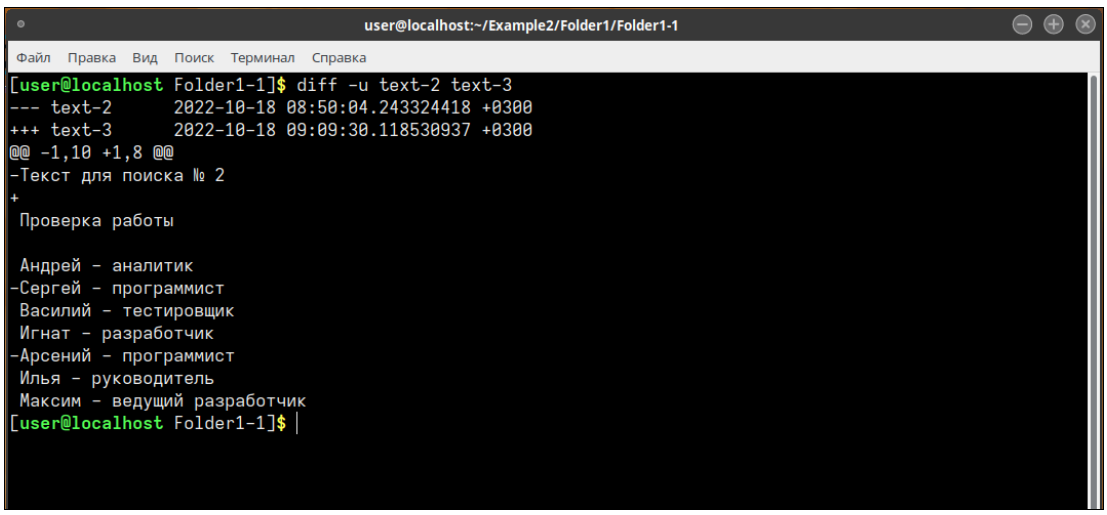


diff

Показывает различия между двумя файлами в построчном сравнении. Причём выводятся только строки, в которых обнаружены отличия. Измененные строки отмечаются символом «**c**», удаленные - «**d**», а новые - «**a**». Добавленные и удаленные строки обозначаются с помощью символов **>** и **<** соответственно.



Для вывода информации о различиях в унифицированном формате можно использовать опцию **-u**:



ps / pgrep

Предназначена для просмотра списка процессов. Чтобы завершить/приостановить какой-либо процесс, необходим его идентификатор. Один из способов получить его - утилита **ps**. Для отображения всех запущенных процессов можно использовать опцию **a**. Следует обратить внимание, что это только снимок состояния на момент вызова, информация не будет обновляться.

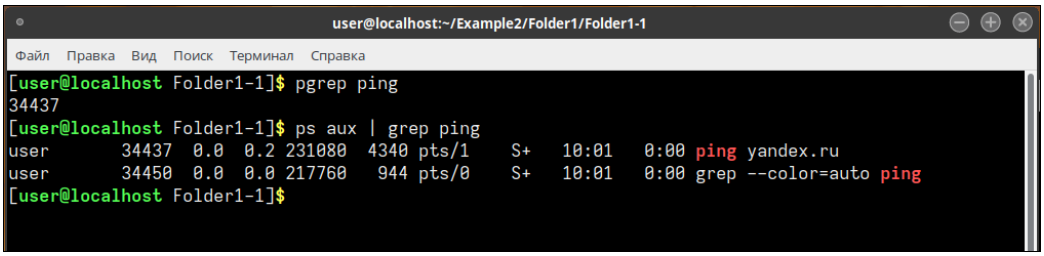
Для получения полной информации о процессах и определения идентификатора процесса (**PID**) выполните команду:

```
ps aux
```

Для конкретизации поиска определенного процесса рекомендуется использовать утилиту grep, например:

```
ps aux | grep ping
```

Утилита **pgrep** работает следующим образом: вы задаете имя процесса, а утилита показывает его идентификатор.



kill / xkill / pkill / killall

Данные команды служат для завершения процессов, однако они принимают различные параметры для идентификации процессов. **Kill** - нужен PID процесса, **xkill** - достаточно кликнуть по окну, чтобы закрыть его, **killall** и **pkill** - принимают имя процесса. Можно использовать любую из утилит, которая будет удобна в определенной ситуации.

Для определения идентификатора процесса (**PID**) воспользуйтесь утилитами ps или pgep, описанными выше.

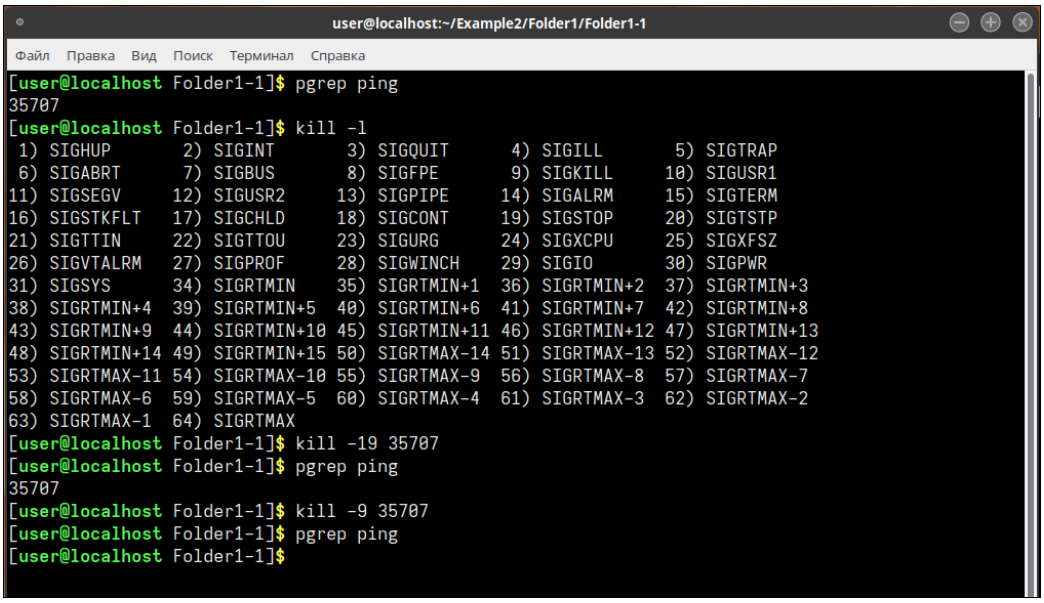
Для утилит kill и killall доступно несколько сигналов, которые также можно использовать для прерывания, завершения или приостановки процессов:

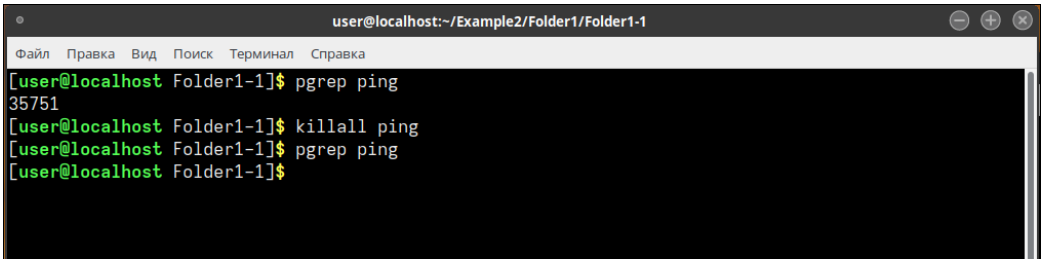
```
kill -l
killall -l
```

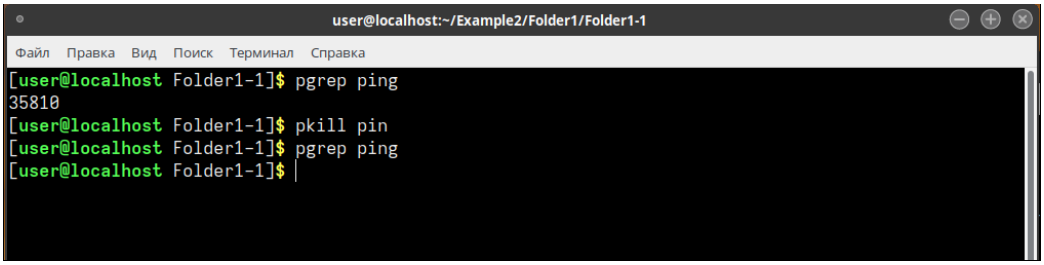
Принудительно завершить процесс можно, используя команды:

```
kill <PID_процесса>
killall <имя_процесса>
pkill <шаблон>
```

Утилита pkill может использовать как полное имя процесса для его завершения, так и часть имени. Утилита сопоставляет переданное ей имя процесса и может по ошибке завершить процесс с похожим именем, поэтому работу с утилитой следует проводить с осторожностью.

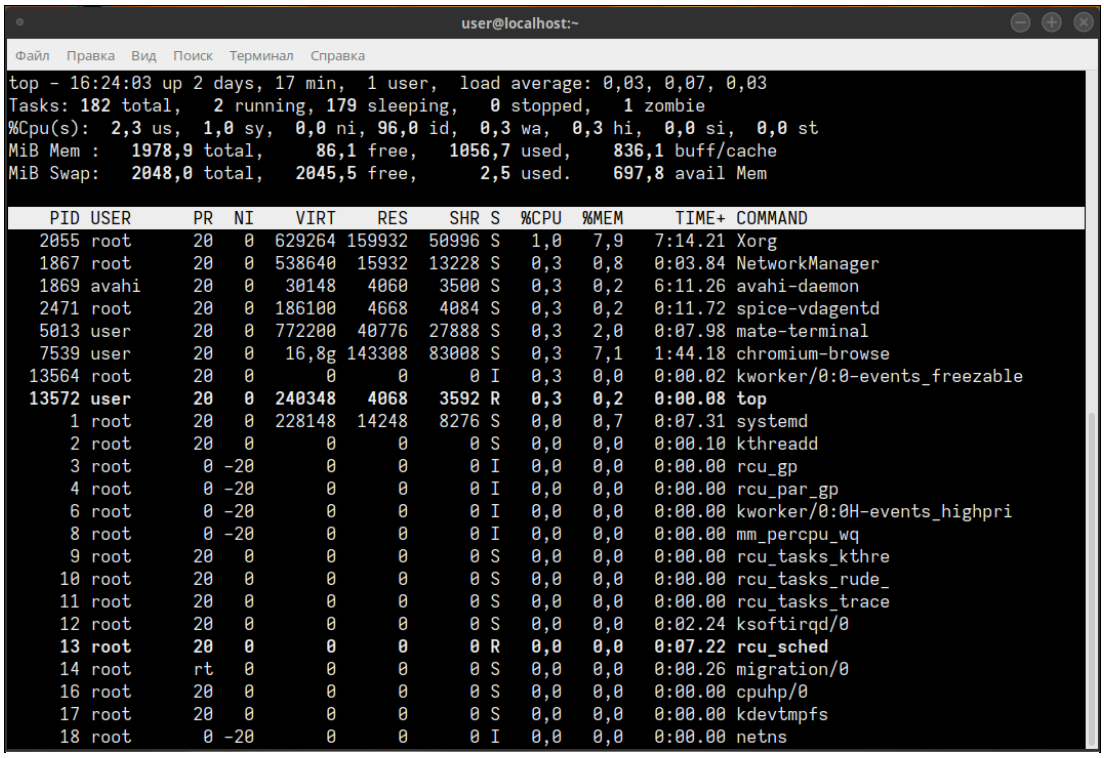






top / htop

Обе команды похожи, обе отображают процессы и могут быть использованы как консольные системные мониторы. **htop** - это улучшенная версия **top**. Вы сможете не только просматривать, но и контролировать процессы через его интерактивный интерфейс.



date

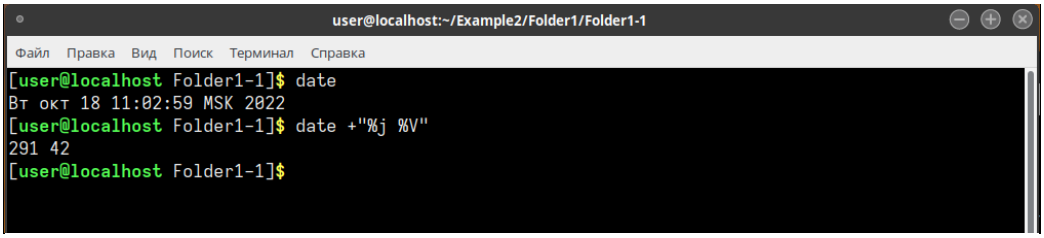
В отличие от **time**, выводит текущую дату и время в различных форматах и позволяет устанавливать системное время. Его можно форматировать в зависимости от ваших потребностей: вывести год, месяц, день, установить 12-ти или 24-ти часовой формат, получить наносекунды или номер недели. Например, **date +"%j %V"** выведет день в году и номер недели в формате ISO.

Установка системных даты и времени производится с правами администратора или суперпользователя (**root**) системы командой:

```
date ММДДччмм[[ВВ]ГГ][.сс]
```

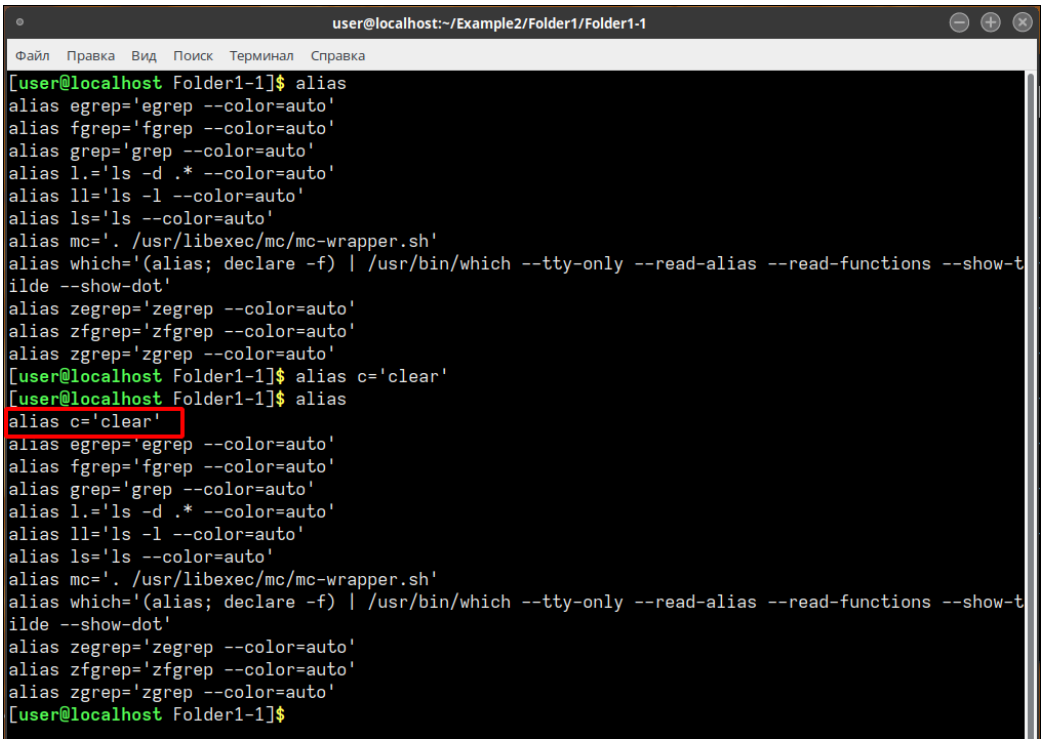
где:

- ММ - Месяц (от 01 до 12);
- ДД - День (от 01 до 28, 29, 30 или 31 в зависимости от месяца);
- чч - Часы (от 00 до 24);
- мм - Минуты (от 00 до 59);
- ГГ - Две последние цифры года (от 00 до 99, не обязательно);
- ВВ - Век (от 00 до 99, используется вместе с предыдущим элементом, не обязательно);
- .сс - Секунды (от 00 до 59 с символом точки, не обязательно).



alias

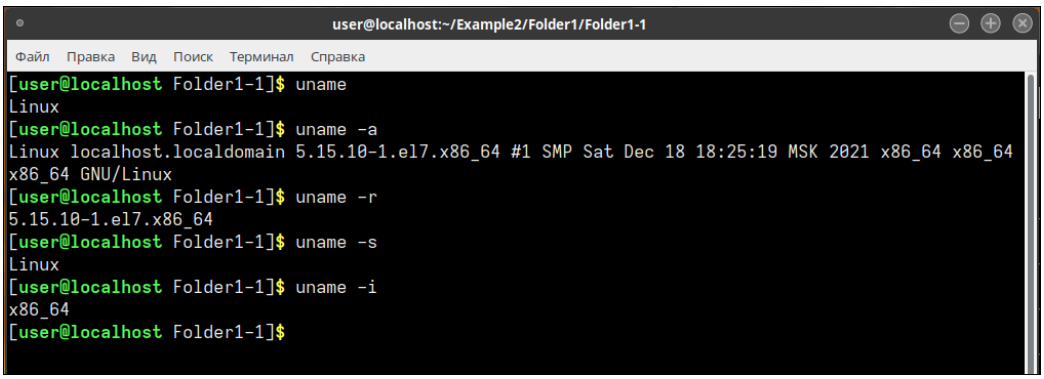
Команда создаёт синонимы для других команд Linux. То есть вы можете создать новые команды или группы команд, а также переименовывать существующие. Это очень удобно для сокращения длинных названий команд, которые вы часто используете, или создания более понятных имен для команд, которые вы используете нечасто или не можете запомнить.



uname

Выводит основную информацию о системе. Основные опции:

- **-a** (all) - информация о ядре, имени хоста и архитектуре процессора;
- **-i** - имя аппаратной реализации (платформы);
- **-r** - информация о релизе системы;
- **-s** - имя операционной системы, опция используется по умолчанию.

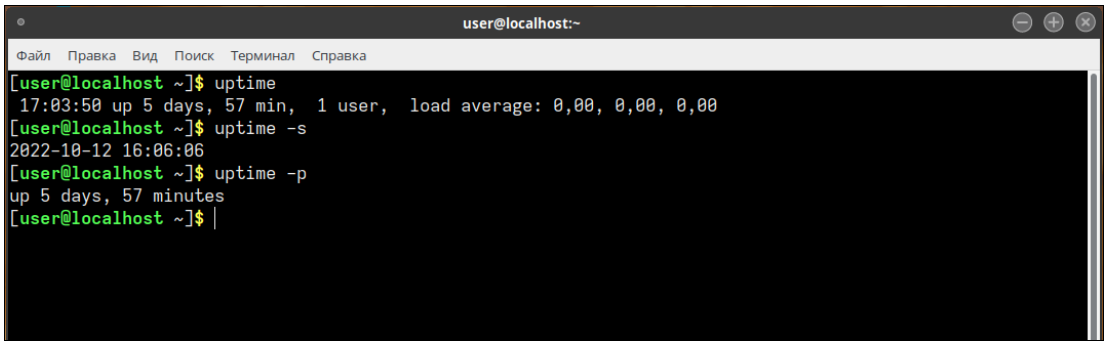


uptime

Выводит время работы системы, количество текущих в данный момент пользователей и среднюю загрузку системы за последние 1, 5 и 15 минут.

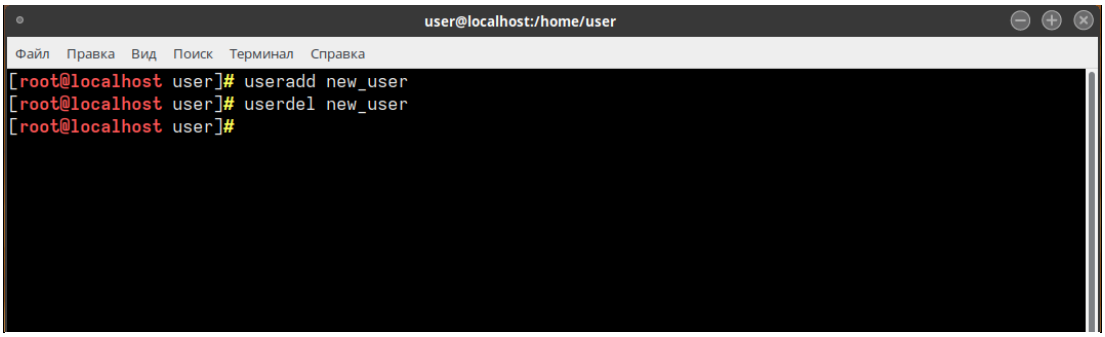
Можно использовать опции:

- **-s** (--since) - вывести время запуска системы. Это время, начиная с которого, отсчитывается время работы системы. Время выводится в формате YYYY-MM-DD HH:MM:SS;
- **-p** (--pretty) - вывести только время работы системы.



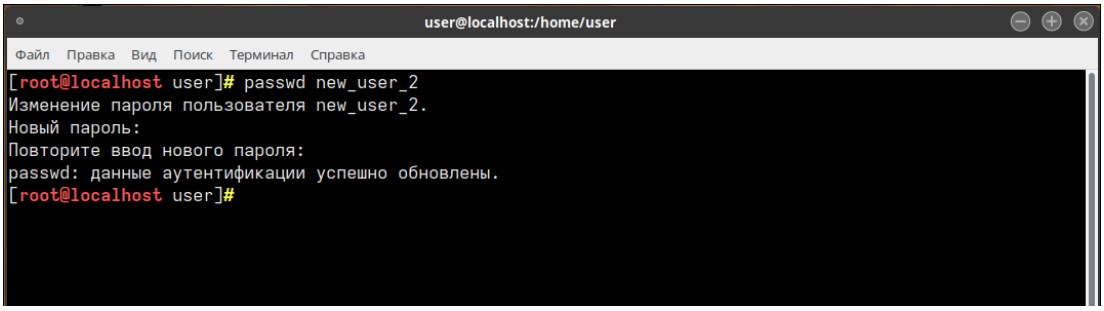
+ useradd / userdel / usermod

Эти команды позволяют добавлять, удалять и изменять учетные записи пользователей, для использования команд необходимы права администратора или суперпользователя (**root**) системы.



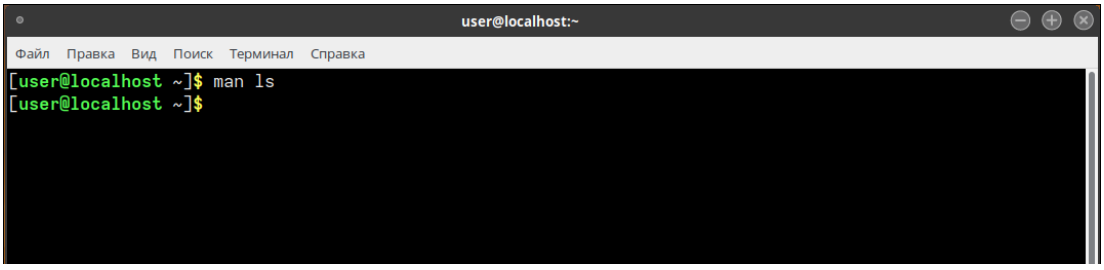
+ passwd

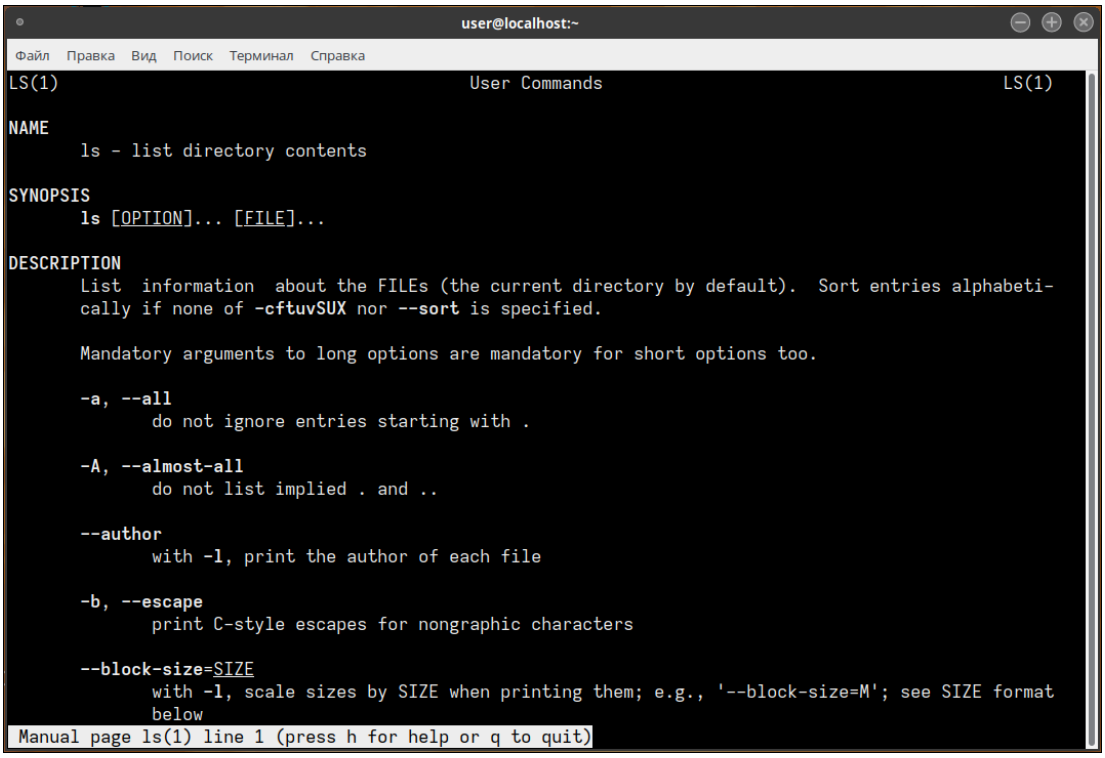
Эта команда позволяет изменить пароль учетной записи пользователя. Для использования команды необходимы права администратора или суперпользователя (**root**) системы.

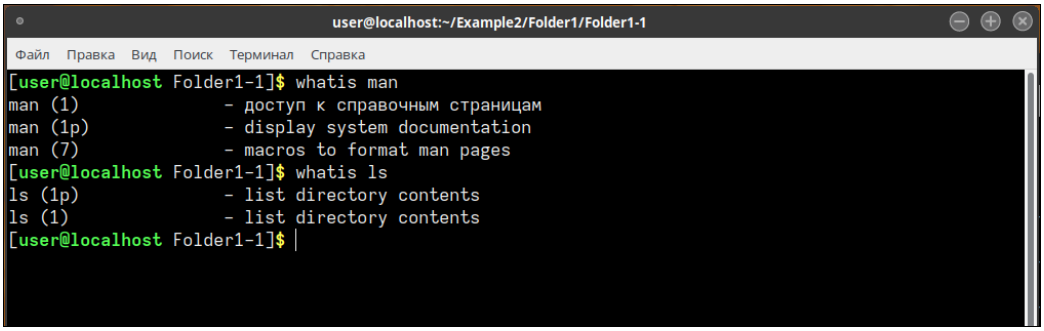


+ man / whatis

Команда **man** открывает руководство по определённой команде. Для всех основных команд Linux есть **man**-страницы. **Whatis** показывает, какие разделы руководств есть для данной команды.

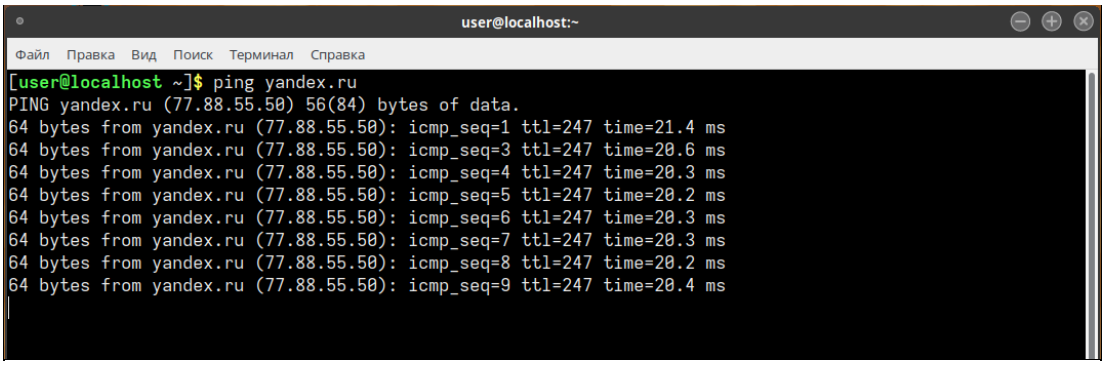






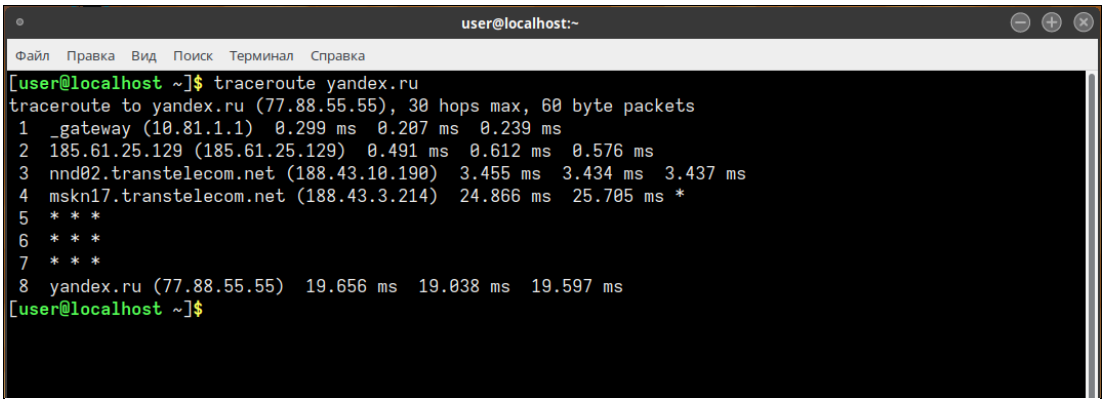
ping

Утилита **ping** может быть очень полезным диагностическим инструментом. Она поможет быстро проверить, подключены ли вы к маршрутизатору или к интернету, и дает некоторое представление о качестве этой связи.



traceroute

Это усовершенствованная версия **ping**. Мы можем увидеть не только полный маршрут сетевых пакетов, но и доступность узла, а также время доставки этих пакетов на каждый из узлов.



journalctl

journald — системная служба, отвечающая за сбор, хранение и управление данными журналов в ОС, также выполняет ротацию, сжатие и индексацию лог-файлов. **journalctl** позволяет просматривать и фильтровать данные, собираемых службой **journald**.

Полезные опции:

- **-f** — показать последние записи журнала и продолжить вывод новых записей при добавлении их в журнал;
- **-xb** — вывод записей журнала с момента запуска текущей сессии с расшифровкой ошибок.

```
[user@localhost ~]$ journalctl -f
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-tmpfiles-setup.service: Suc
ceeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped Create User's Volatile File
s and Directories.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus-broker.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped D-Bus User Message Bus.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus.socket: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Closed D-Bus User Message Bus Socke
t.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Shutdown.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-exit.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Finished Exit the Session.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Exit the Session.
```

ip

ip — утилита командной строки из пакета **iproute2**, которая позволяет выполнять настройку сетевой подсистемы и является заменой таких утилит, как *ifconfig*, *route*, *arp*.

```
[user@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group d
efault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    altname enp0s25
    inet [redacted] brd [redacted] scope global dynamic noprefixroute eno1
       valid_lft 90149sec preferred_lft 90149sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever
4: anbox0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group de
fault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet [redacted] scope global anbox0
       valid_lft forever preferred_lft forever
```

netstat

netstat — утилита командной строки, выводящая состояние TCP-соединений (как входящих, так и исходящих), таблицы

маршрутизации, число сетевых интерфейсов и сетевую статистику по протоколам.

```
[root@localhost user]# netstat --inet -pl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:46825         0.0.0.0:*               LISTEN      1088/containerd
tcp        0      0 0.0.0.0:ideafarm-door   0.0.0.0:*               LISTEN      1055/vmware-authdla
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      1086/sshd: /usr/sbi
tcp        0      0 localhost:54329         0.0.0.0:*               LISTEN      1113/postgres
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2133/dnsmasq
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      1078/cupsd
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN      1258/master
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2180/dnsmasq
udp        0      0 0.0.0.0:40848           0.0.0.0:*                           791/avahi-daemon: r
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2180/dnsmasq
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2180/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*                           1/systemd
udp        0      0 localhost:323           0.0.0.0:*                           848/chronyd
```

df

Утилита **df** — консольная утилита, которая позволяет проверить использование дискового пространства в операционной системе. Эта команда отображает информацию об общем, свободном и используемом объеме памяти файловых систем. Утилита **df** предоставляет множество опций, которые позволяют настроить ее вывод.

```
[root@localhost user]# df
Файловая система 1K-блоков Использовано  Доступно Использовано% Смонтировано в
devtmpfs              4096            0      4096            0% /dev
tmpfs              4011852       608496   3403356           16% /dev/shm
tmpfs              1604744         3632   1601112            1% /run
/dev/sdb1        234213368    181416340  40826880           82% /
/dev/sda4        530945160    134478724 369422392           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1          106496       106496         0          100% /var/lib/snapd/snap/core/16928
/dev/loop0          108032       108032         0          100% /var/lib/snapd/snap/core/16574
/dev/loop2           57088        57088         0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3           57088        57088         0          100% /var/lib/snapd/snap/core18/2812
/dev/loop4           73088        73088         0          100% /var/lib/snapd/snap/webinar/7
/dev/loop6             128          128         0          100% /var/lib/snapd/snap/bare/5
/dev/loop7          168832       168832         0          100% /var/lib/snapd/snap/gnome-3-28-1804/198
/dev/loop5          382848       382848         0          100% /var/lib/snapd/snap/anbox/186
/dev/loop8           93952        93952         0          100% /var/lib/snapd/snap/gtk-common-themes/1535
/dev/loop9           72960        72960         0          100% /var/lib/snapd/snap/webinar/6
tmpfs               802368          160    802208            1% /run/user/1000
[root@localhost user]# df -h
Файловая система Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs           4,0M            0  4,0M            0% /dev
tmpfs              3,9G          595M  3,3G           16% /dev/shm
tmpfs              1,6G          3,6M  1,6G            1% /run
/dev/sdb1          224G          174G   39G           82% /
/dev/sda4          507G          129G  353G           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1         104M          104M     0          100% /var/lib/snapd/snap/core/16928
/dev/loop0         106M          106M     0          100% /var/lib/snapd/snap/core/16574
/dev/loop2          56M           56M     0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3          56M           56M     0          100% /var/lib/snapd/snap/core18/2812
```

free

Команда **free** предоставляет информацию об общем объеме физической памяти и памяти подкачки, а также о свободной и используемой памяти.

```
[user@localhost ~]$ free
               total        used        free      shared  buff/cache   available
Mem:         8023704     6372008      367168      575088     1284528      781116
Swap:        5122228     4663944      458284
[user@localhost ~]$ free -m
               total        used        free      shared  buff/cache   available
Mem:            7835        6225         355         561        1254         760
Swap:           5002        4554         447
[user@localhost ~]$ free -h
               total        used        free      shared  buff/cache   available
Mem:           7,7Gi       6,1Gi       355Mi       565Mi       1,2Gi       759Mi
Swap:          4,9Gi       4,4Gi       447Mi
[user@localhost ~]$
```

Получение справочной информации об использовании утилит с помощью man

Установка
Навигация
Разделы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО:** man-db-2.7.6.1-1, man-pages-4.16-1

man — утилита, предназначенная для форматирования и вывода справочных страниц. Каждая страница справки является самостоятельным документом и пишется разработчиками соответствующего программного обеспечения.

Установка

В РЕД ОС по умолчанию утилита уже установлена. Однако, если по каким-либо причинам она отсутствует, ее можно установить. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install man man-pages
```

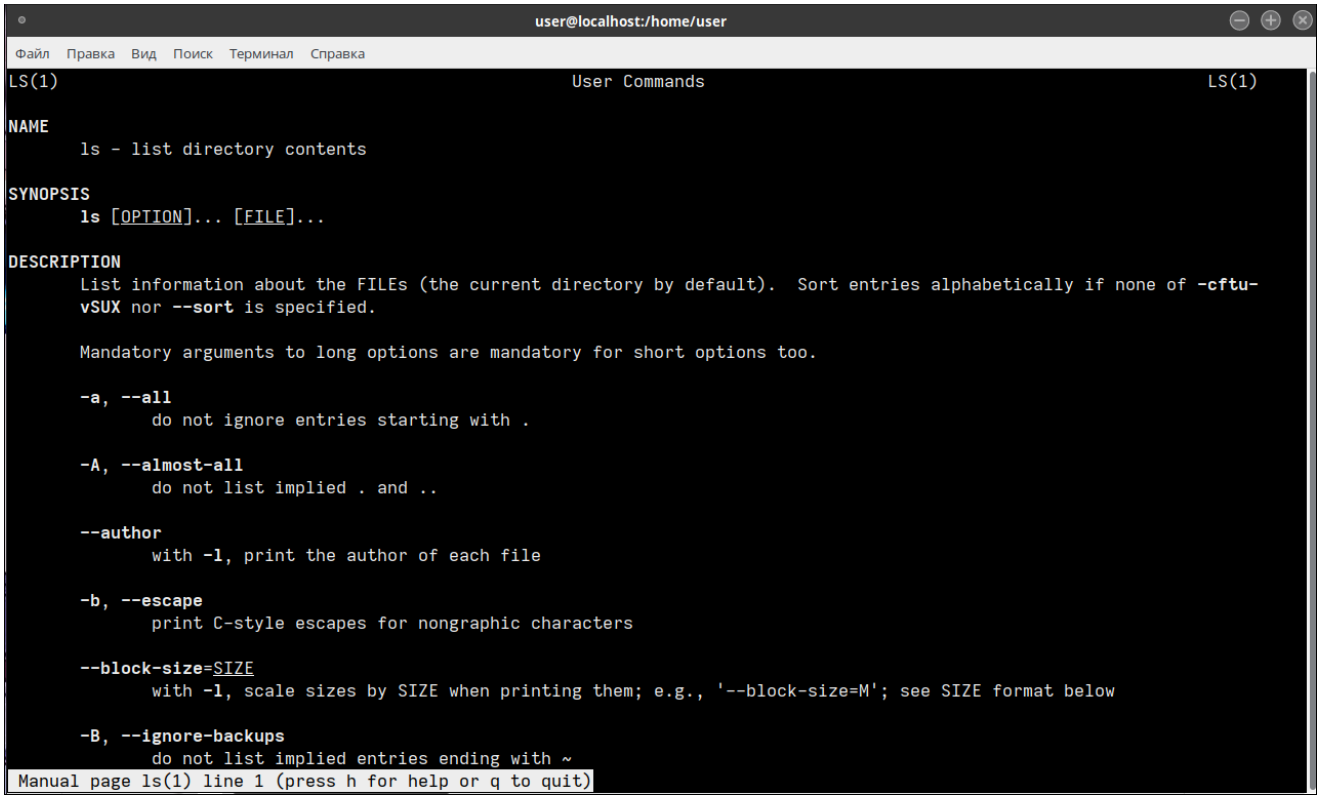
Далее команды будут выполняться с правами **локального пользователя**, если не указано иное.

Для вывода справочного руководства по какой-либо команде или пакету с возможностью запуска в терминале необходимо выполнить команду вида:

```
man <команда>
```

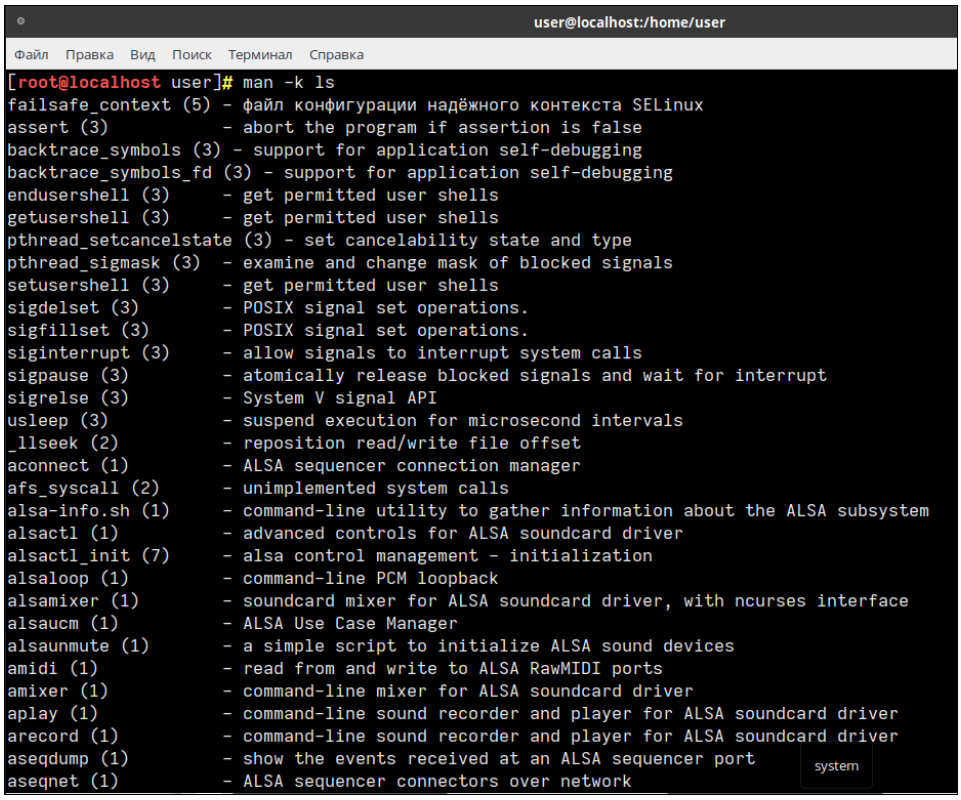
Например:

```
man ls
```



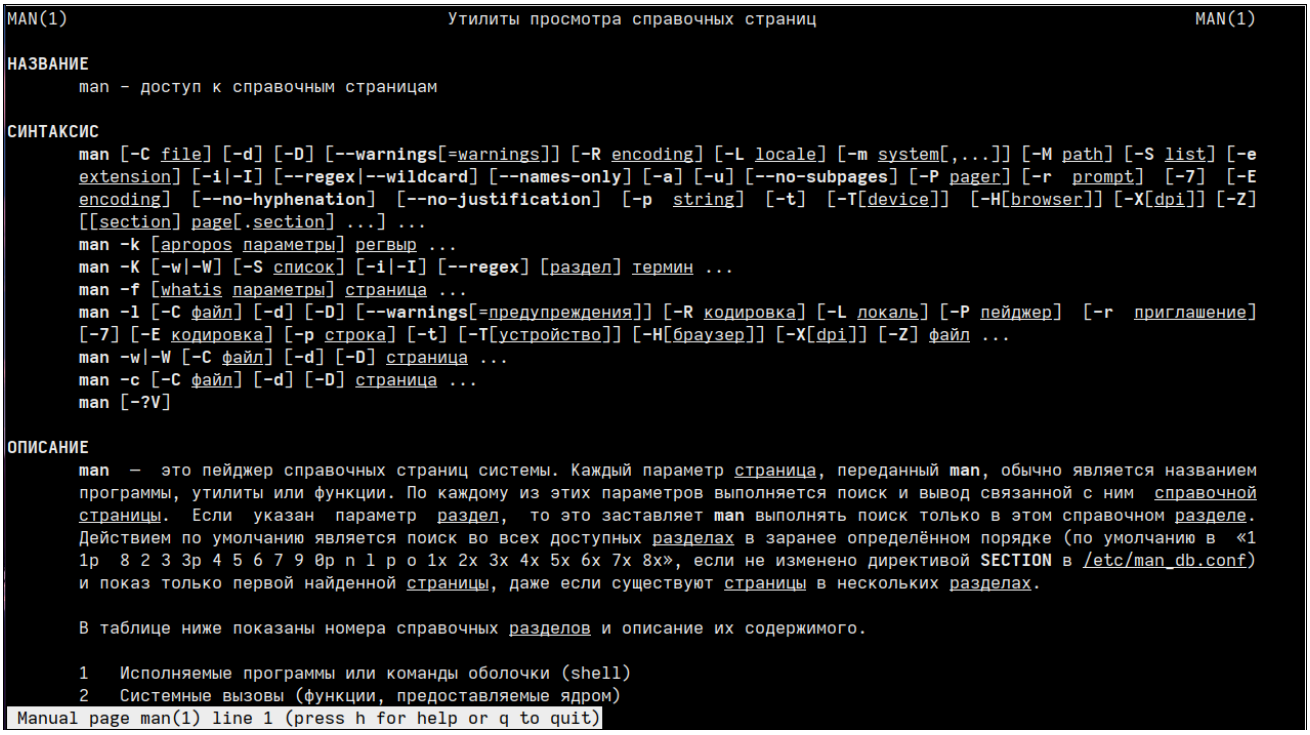
Опция **-k** выполняет поиск и выводит список man-страниц, в которых встречается искомый запрос.

```
man -k ls
```



Другие полезные опции утилиты **man** можно посмотреть командой:

```
man man
```



Навигация

Для навигации по страницам руководства используются следующие сочетания клавиш:

- ↑ и ↓ — для построчного перехода по руководству;
- **PgUp** и **PgDown** — для постраничного перехода по руководству;

- **/** — поиск по странице; введите **/** и искомое слово, затем нажмите **Enter**;
- **?** — поиск в обратном направлении (снизу вверх); введите **?** и искомое слово, затем нажмите **Enter**;
- **n** — переход к следующему подсвеченному вхождению;
- **Shift+n** — переход к предыдущему подсвеченному вхождению;
- **&** — поиск внутри страницы; выводятся только строки, где было найдено искомое слово;
- **h** — открыть справку по командам и горячим клавишам, для закрытия справки нажмите **q**;
- **q** — закрыть man-страницу.

Разделы

Справочные страницы поделены на 8 стандартных разделов и один дополнительный. Каждый из разделов соответствует той или иной тематике.

Раздел	Краткое описание
1	Прикладные программы и команды оболочки
2	Системные вызовы ядра (функции языка Си)
3	Библиотечные вызовы (функции различных библиотек, установленных в систему)
4	Специальные файлы (находящиеся обычно в каталоге **/dev**)
5	Форматы файлов и соглашения
6	Игры
7	Различные описания, соглашения и прочее
8	Команды администрирования системы, которые обычно запускаются от имени суперпользователя
9	Ядро операционной системы (нестандартный раздел)

Номер раздела в команде **man** указывается вторым аргументом, перед названием справочной страницы. Если номер раздела опущен, то поиск справочной страницы ведётся по всем разделам по порядку.

```
man kill  # раздел 1
man 1 kill  # раздел 1
man 2 kill  # раздел 2
```

Менеджер сервисов systemd

Файл сервиса systemd
Типы служб
Замещение файла юнита
Компоненты system
Запуск сервисов после подключения к сети

Systemd – менеджер системы и сервисов в операционной системе РЕД ОС.

Systemd приносит концепцию юнитов **systemd**. Юниты представлены конфигурационными файлами, размещенными в одной из директорий:

- **/usr/lib/systemd/system/** – юниты из установленных пакетов RPM.
- **/run/systemd/system/** — юниты, созданные в рантайме. Этот каталог приоритетнее каталога с установленными юнитами из пакетов.
- **/etc/systemd/system/** — юниты, созданные и управляемые системным администратором. Этот каталог приоритетнее каталога юнитов, созданных в рантайме.

Юниты содержат информацию о системных сервисах, прослушиваемых сокетах, сохраненных снапшотах состояний системы и других объектах, относящихся к системе инициализации.

Типы юнитов **systemd**:

- *.service* – системный сервис,
- *.target* — группа юнитов **systemd**,
- *.automount* – точка автомонтирования файловой системы,
- *.device* – файл устройства, распознанного ядром,
- *.mount* – точка монтирования файловой системы,
- *.path* – файл или директория в файловой системе,
- *.scope* – процесс, созданный извне,
- *.slice* – группа иерархически организованных юнитов, управляющая системными процессами,
- *.snapshot* – сохраненное состояние менеджера **systemd**,
- *.socket* – сокет межпроцессного взаимодействия,
- *.swap* – свап-устройство или свап-файл (файл подкачки),
- *.timer* – таймер **systemd**.

Во время загрузки **systemd** прослушивает сокеты для всех системных сервисов, поддерживает этот тип активации и передает сокеты этим сервисам сразу после старта сервисов. Это позволяет **systemd** не только запускать сервисы параллельно, но также дает возможность перезапускать сервисы без потери любых отправленных им сообщений, пока сервисы были недоступны. Соответствующий сокет остается доступным и все сообщения выстраиваются в очередь.

Системные сервисы, использующие D–Bus для межпроцессного взаимодействия, могут быть запущены по требованию, когда клиентское приложение пытается связаться с ними.

Системные сервисы, поддерживающие активацию, основанную на устройствах, могут быть запущены, когда определенный тип оборудования подключается или становится доступным.

Системные сервисы могут поддерживать этот вид активации, если изменяется состояние папки или директории.

Система может сохранять состояние всех юнитов и восстанавливать предыдущее состояние системы.

Systemd отслеживает и управляет точками монтирования и автомонтирования.

Агрессивная параллелизация **Systemd** запускает системные сервисы параллельно из-за использования активации, основанной на сокетах. В комбинации с сервисами, поддерживающими активацию по требованию, параллельная активация значительно уменьшает время загрузки системы.

До активации и деактивации юнитов **systemd** вычисляет их зависимости, создает временную транзакцию и проверяет целостность этой транзакции. Если транзакция не целостная, systemd автоматически пытается исправить ее и удалить не требующиеся задания из нее до формирования сообщения об ошибке.

SystemD полностью поддерживает скрипты инициализации **SysV**, как описано в спецификации Linux Standard Base (LSB), что упрощает переход на systemd.

По способу использования сервисные юниты *.service* напоминают скрипты инициализации. Для просмотра, старта, остановки, перезагрузки, включения или выключения системных сервисов используется команда systemctl. Команды service и chkconfig по-прежнему включены в систему, но только по соображениям совместимости.

При использовании **systemctl** указывать расширение файла не обязательно.

Основные команды *systemctl*:

systemctl start name.service – запуск сервиса,
systemctl stop name.service — остановка сервиса,
systemctl restart name.service — перезапуск сервиса,
systemctl try-restart name.service — перезапуск сервиса только, если он запущен,
systemctl reload name.service — перезагрузка конфигурации сервиса,
systemctl status name.service — проверка, запущен ли сервис с детальным выводом состояния сервиса,
systemctl is-active name.service — проверка, запущен ли сервис с простым ответом: active или inactive,
systemctl list-units --type service --all – отображение статуса всех сервисов,
systemctl --failed – отображение списка юнитов, которые не удалось запустить,
systemctl enable name.service – активирует сервис (позволяет стартовать во время запуска системы),
systemctl disable name.service – деактивирует сервис,
systemctl reenable name.service – деактивирует сервис и сразу активирует его,
systemctl is-enabled name.service – проверяет, активирован ли сервис,
systemctl list-unit-files --type service – отображает все сервисы и проверяет, какие из них активированы,
systemctl cat name.service – позволит просмотреть содержимое файла юнита и связанных с ним drop-in сниппетов,
systemctl mask name.service – заменяет файл сервиса симлинком на /dev/null, делая юнит недоступным для systemd,
systemctl unmask name.service – возвращает файл сервиса, делая юнит доступным для systemd.

Файлы целей **systemd .target** предназначены для группировки вместе других юнитов systemd через цепочку зависимостей. Например, юнит **graphical.target**, использующийся для старта графической сессии, запускает системные сервисы GNOME Display Manager (*gdm.service*) и Accounts Service (*accounts-daemon.service*) и активирует **multi-user.target**. В свою очередь **multi-user.target** запускает другие системные сервисы, такие как Network Manager (*NetworkManager.service*) или D-Bus (*dbus.service*) и активирует другие целевые юниты **basic.target**.

В РЕД ОС присутствуют предопределенные цели, похожие на стандартный набор уровней запуска. По соображениям совместимости они также имеют псевдонимы на эти цели, которые напрямую отображаются в уровнях запуска *SysV*.

poweroff.target (runlevel0.target) – завершение работы и отключение системы
rescue.target (runlevel1.target) – настройка оболочки восстановления
multi-user.target (runlevel2.target, runlevel3.target, runlevel4.target) – настройка неграфической многопользовательской системы
graphical.target (runlevel5.target) – настройка графической многопользовательской системы
reboot.target (runlevel6.target) – выключение и перезагрузка системы

Команды **runlevel** и **telinit** по-прежнему доступны, но оставлены в системе по соображениям совместимости. Рекомендуется использовать **systemctl** для изменения или настройки системных целей.

Для определения, какой целевой юнит используется по умолчанию, полезна следующая команда:

```
systemctl get-default
```

Для просмотра всех загруженных целевых юнитов воспользуйтесь командой:

```
systemctl list-units --type target
```

а для просмотра вообще всех целевых юнитов командой:

```
systemctl list-units --type target --all
```

Для изменения цели по умолчанию поможет команда:

```
systemctl set-default name.target
```

Для изменения текущей цели:

```
systemctl isolate name.target
```

Команда запустит целевой юнит и все его зависимости и немедленно остановит все остальные.

В РЕД ОС *systemctl* заменяет значительное количество команд управления питанием. Прежние команды сохранены для совместимости, но рекомендуется использовать *systemctl*:

- **systemctl halt** – останавливает систему,
- **systemctl poweroff** – выключает систему,
- **systemctl reboot** – перезагружает систему,
- **systemctl suspend** – переводит систему в режим ожидания,

- **systemctl hibernate** – переводит систему в спящий режим,
- **systemctl hybrid-sleep** – переводит систему в режим гибридного сна.

Systemd позволяет управлять удаленной машиной по SSH. Для управления используйте команду:

```
systemctl --host <user_name>@<host_name> <command>
```

где **user_name** – имя пользователя, **host_name** – имя хоста, которым осуществляется удаленное управление, а **command** – выполняемая команда **systemd**. Подробная информация о всех параметрах файла *.service* есть в соответствующем разделе документации по **systemd**.

Файл сервиса systemd

```
[Unit]
Description=Daemon to detect crashing apps
After=syslog.target

[Service]
ExecStart=/usr/sbin/abrtd
Type=forking

[Install]
WantedBy=multi-user.target
```

Давайте посмотрим на секцию **[Unit]**. Она содержит общую информацию о сервисе. Такая секция есть не только в сервис-юнитах, но и в других юнитах (например при управлении устройствами, точками монтирования и т.д.). В примере мы даем описание сервиса и указываем на то, что демон должен быть запущен после **Syslog**.

В следующей секции **[Service]** непосредственно содержится информация о нашем сервисе. Используемый параметр *ExecStart* указывает на исполняемый файл нашего сервиса. В *Type* мы указываем, как сервис уведомляет **systemd** об окончании запуска.

Финальная секция **[Install]** содержит информацию о цели, в которой сервис должен стартовать. В данном случае мы говорим, что сервис должен быть запущен, когда будет активирована цель *multi–user.target*. Это минимальный работающий файл сервиса **systemd**. Написав свой, для тестирования скопируйте его в **/etc/systemd/system/.service**. Выполните команду:

```
systemctl daemon-reload
```

Systemd узнает о сервисе и вы сможете его запустить.

Типы служб

Службы различаются по типу запуска, что следует учитывать при написании юнитов. Тип определяется параметром **Type=** в разделе [**Service**]:

- **Type=simple** (по умолчанию): systemd запустит эту службу незамедлительно. Процесс при этом не должен разветвляться (fork). Если после данной службы должны запускаться другие, то этот тип использовать не стоит (исключение — служба использует сокетную активацию).
- **Type=forking**: systemd считает службу запущенной после того, как процесс разветвляется с завершением родительского процесса. Используется для запуска классических демонов за исключением тех случаев, когда в таком поведении процесса нет необходимости. Укажите параметр **PIDFile=**, чтобы systemd мог отслеживать основной процесс.
- **Type=oneshot**: удобен для сценариев, которые выполняют одно задание и завершаются. Если задать параметр **RemainAfterExit=yes**, то systemd будет считать процесс активным даже после его завершения.
- **Type=notify**: идентичен параметру **Type=simple**, но с уточнением, что демон пошлет systemd сигнал готовности. Реализация уведомления находится в библиотеке **libsystemd-daemon.so**.
- **Type=dbus**: служба считается находящейся в состоянии готовности после появления указанного **BusName** в системной шине DBus.
- **Type=idlel**: systemd отложит выполнение двоичного файла службы до окончания запуска остальных ("более срочных") задач. В остальном поведение аналогично **Type=simple**.

Замещение файла юнита

Можно полностью заместить файл юнита /usr/lib/systemd/system/<юнит>, для этого необходимо создать файл с таким же именем

/etc/systemd/system/<юнит> и включить заново юнит для обновления символических ссылок.

```
systemctl edit --full <юнит>
```

Эта команда откроет файл **/etc/systemd/system/<юнит>** в текстовом редакторе (если файл ещё не существует, будет скопирован оригинал) и автоматически перезагрузит юнит после завершения редактирования.

Компоненты system

- **systemd-boot** — простой менеджер загрузки для UEFI;
- **systemd-firstboot** — инициализация системных настроек при первой загрузке;
- **systemd-homed** — переносимые аккаунты пользователей;
- **systemd-logind** — управление сеансами;
- **systemd-networkd** — управление сетевыми настройками;
- **systemd-nspawn** — приложение для контейнеризации процессов;
- **systemd-resolved** — разрешение сетевых имён;
- **systemd-sysusers** — создание системных пользователей/групп и добавление пользователей в группы при установке пакетов и загрузке системы;
- **systemd-timesyncd** — синхронизация системных часов по сети;
- **systemd/Журнал** — системные логи;
- **systemd/Таймеры** — таймеры для управления событиями и службами, альтернатива *cron*.

Запуск сервисов после подключения к сети

Для того чтобы запускать сервис только после подключения к сети, добавьте такие зависимости в **.service**-файле:

```
nano /etc/system/system/foo.service

[Unit]
…
Wants=network-online.target
After = network-online.target
…
```

Управление задачами в командной строке

РЕД ОС является многозадачной системой, способной одновременно выполнять несколько задач (или процессов). На самом деле одно ядро процессора может выполнять только один процесс в определённый момент времени. Но ядро Linux управляет задачами и чередует их выполнение на процессоре так, что пользователю кажется их выполнение одновременным. Всеми процессами можно управлять из командной строки.

Существует множество команд для управления процессами из командной строки, рассмотрим некоторые из них:

- **ps** — список запущенных процессов на компьютере;
- **kill** — отправка сигнала одному или нескольким процессам;
- **jobs** — просмотр списка собственных задач сеанса оболочки;
- **bg** — выполнение задачи в фоновом режиме;
- **fg** — возврат задачи из фонового режима.

Вы можете подробнее ознакомиться со способами управления задачами, просмотрев наши обучающие видео:

- на **RuTube** — Управление задачами в bash;
- в **Яндекс.Дзен** — Управление задачами в bash;
- в **VK Видео** — Управление задачами в bash.

На наших каналах вы также сможете найти много другой полезной информации.

Для примера будет использоваться утилита ping с отправкой запросов каждые 9 секунд:

```
ping -i 9 red-soft.ru
```

Таким образом активирован процесс, привязанный к данному терминалу, из-за чего работа с командной строкой становится невозможной. Но, поскольку командная строка необходима для дальнейшей работы, прервём выполнение команды «горячими» клавишами оболочки — «**Ctrl+C**» и запустим данную команду в фоновом режиме, для этого в конце команды необходимо добавить символ «**&**»:

```
ping -i 9 red-soft.ru &
```

Теперь командная строка доступна для работы, и каждые 9 секунд демонстрируется результат команды ping. И хотя процесс не занимает собой командную строку оболочки, он всё равно привязан к текущему терминалу. В таком случае говорят, что процесс стал собственной задачей текущего сеанса оболочки.

Для отображения списка задач в текущем сеансе оболочки можно воспользоваться командой jobs:

```
jobs [1]+ Запущен ping -i 9 red-soft.ru
```

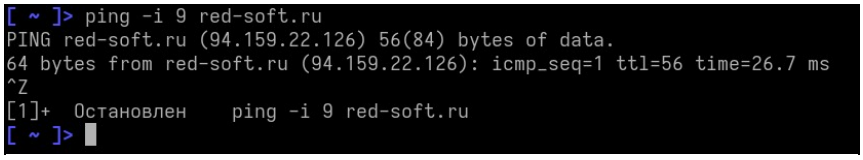
В квадратных скобках указан номер задачи в текущем терминале, его можно использовать в том числе и для завершения процесса утилитой kill, но в отличие от идентификатора процесса, который указывается «обычным» цифровым значением, перед номером задачи ставится знак «**%**». Например:

```
kill %1
```

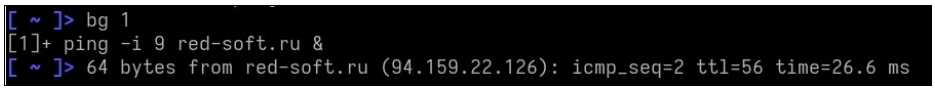
Для возвращения фонового процесса обратно в интерактивный режим необходимо использовать утилиту fg (**foreground**). Данную команду необходимо выполнять с переданным в качестве аргумента номером фоновой задачи (получить его можно из вывода команды **jobs**):

```
fg 1
```

Клавиатурное сочетание «**Ctrl+Z**» отправляет задачу в фон и ставит её выполнение на паузу. Иными словами, процесс не получает ресурсов центрального процессора для своего выполнения и находится в режиме ожидания.



Когда понадобится продолжить выполнение остановленной задачи, можно воспользоваться утилитой fg, описанной выше, или другой командой — bg (**background**). Утилита bg пробуждает задачу и отправляет её в фон:



В выводе команды отображаются результаты отправки ICMP-пакета (основная задача **ping**) и выводятся на экран — это значит, что процесс снова работает на заднем плане, не взаимодействуя с командной строкой.

Добавление команд в автозагрузку

Добавление через управление автозапускаемыми приложениями
Добавление через сервис
Добавление команды в crontab
Выполнение команд через desktop-файлы

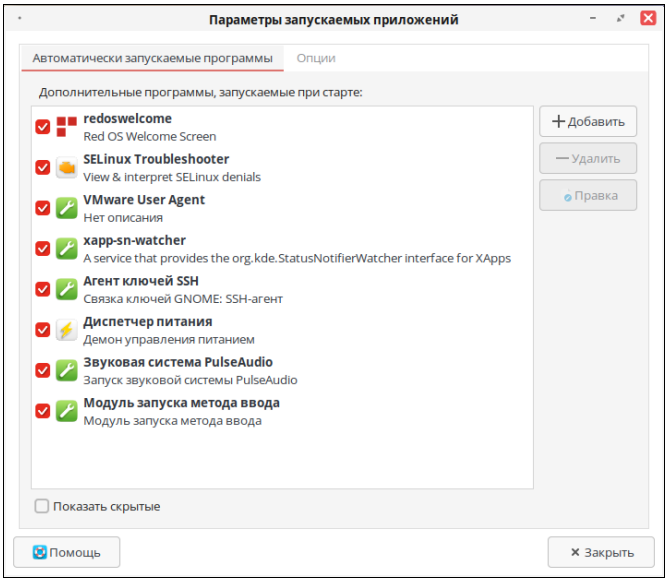
Вы можете подробнее ознакомиться с добавлением команд в автозагрузку, просмотрев наши обучающие видео:

- на **RuTube** — Добавление команд в автозагрузку;
- в **Яндекс.Дзен** — Добавление команд в автозагрузку;
- в **VK Видео** — Добавление команд в автозагрузку.

На наших каналах вы также сможете найти много другой полезной информации.

Добавление через управление автозапускаемыми приложениями

Для добавления в автозагрузку требуется открыть «**Меню**» - «**Параметры**» - «**Запуск приложений**». Будет показан текущий список автозагрузок пользователя.



Добавление осуществляется нажатием кнопки «**Добавить**», можно добавлять либо пользовательскую команду, либо приложение.

В случае приложения - будет доступен список установленных приложений, которые можно добавить в автозагрузку.

В случае команды пользователя - указывается имя команды, путь к ней и, если требуется, комментарий с задержкой выполнения команды.

Добавление через службу

Выберите скрипт, который будет запускаться через созданную службу, в примере используется **/etc/default/script**.

Создайте новую службу. Пример содержимого новой службы приведен ниже:

```
nano /etc/systemd/system/testservice.service
```

Содержимое службы:

```
[Unit]
 Description=service description
 After=gdm.service
 [Service]
 ExecStart=/etc/default/script
 Type=oneshot
 User=root
 RemainAfterExit=yes
```

```
[Install]
WantedBy=multi-user.target
```

Также с помощью следующих команд можно указать, от имени какого именно пользователя будет проходить выполнение, в примере - **root**:

```
chmod 664 /etc/systemd/system/testservice.service
systemctl daemon-reload
systemctl enable testservice.service
systemctl start testservice.service
```

Добавление команды в crontab

Добавление скрипта в **crontab** происходит следующим образом:

1. В консоли пропишите команду:

```
crontab -e
```

Откроется окно редактирования, в нем необходимо нажать «**Insert**» для редактирования.

Формат ввода данных представлен ниже:

```
* * * * * Команда, которая будет выполнена- - - - -
| | | | |
| | | | - День недели 0 - 7) (воскресенье = 0 или 7)
| | | --- Месяц (1 - 12)
| | --- День месяца (1 - 31)
| ---- Час (0 - 23)
----- Минута (0 - 59)
```

2. После завершения написания данных нажмите «**Esc**» и выполните:

```
:wq!
```

3. Для удаления заданий введите:

```
crontab -r
```

4. Для вывода списка текущих заданий введите:

```
crontab -l
```

Подробную информацию о **crontab** см. в нашей инструкции «Планировщик заданий crontab».

Выполнение команд через desktop-файлы

Для выполнения команд через **desktop**-файлы необходимо:

1. Создать файл запуска со следующим содержимым (потребуются права пользователя **root** или **администратора** системы):

```
nano /etc/xdg/autostart/test.desktop
```

```
[Desktop Entry]
Type=Application
Exec=/home/user/test.sh
Hidden=false
Name=MyAutostart
```

где `Exec=<путь_к_файлу>/test.sh` — это команда/скрипт, которую требуется выполнить.

2. Создать скрипт **/test.sh** со следующим содержимым:

```
```

```
nano /home/user/test.sh
```

```
#!/usr/bin/bash
if [ -f /home/user/test.sh ]; then
v_date=`date "+%m.%d.%y %k:%M:%S"`
echo "Время запуска скрипта: "$v_date >> ${HOME}/test.log
fi
```

3. Назначить скрипту права на выполнение:

```
chmod +x /home/user/test.sh
```

4. Выполнить проверку.

Выйдите и войдите в сеанс пользователя либо перезагрузите систему.

В домашнем каталоге пользователя будет создан файл **test.log**, в который будут записаны дата и время исполнения скрипта.

```
cat /home/user/test.log

Время запуска скрипта: 07.10.23 11:34:57
```

Создание псевдонимов команд с помощью alias

Alias - псевдоним, который позволяет пользователю запускать любую команду или группу команд, в том числе с опциями, параметрами и файлами, вводом всего одного слова или даже символа.

Вы можете подробнее ознакомиться с работой **Alias**, просмотрев наши обучающие видео:

- на **RuTube** — Alias - создание псевдонимов команд;
- в **Яндекс.Дзен** — Alias - создание псевдонимов команд;
- в **VK Видео** — Alias - создание псевдонимов команд.

На наших каналах вы также сможете найти много другой полезной информации.

Проверить уже заданные псевдонимы можно вводом команды **alias** без параметров.

```
alias

alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mc='. /usr/libexec/mc/mc-wrapper.sh'
alias vi='vim'
alias view='vim -R'
alias which='(alias; declare -f) | /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot'
alias zegrep='zegrep --color=auto'
alias zfgrep='zfgrep --color=auto'
alias zgrep='zgrep --color=auto'
```

Команда показывает все псевдонимы для текущего пользователя.

Синтаксис **alias**:

```
alias <имя_псевдонима>=“<значение>/<команда> <аргумент>/<путь_к_файлу>”
```

Созданные псевдонимы сохраняются и будут работать только в данном терминале и только до его закрытия.

Пример создания алиаса для частоиспользуемой команды очистки вывода терминала **clear**:

```
alias c="clear"
alias

alias c='clear'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mc='. /usr/libexec/mc/mc-wrapper.sh'
alias vi='vim'
alias view='vim -R'
alias which='(alias; declare -f) | /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot'
alias zegrep='zegrep --color=auto'
alias zfgrep='zfgrep --color=auto'
alias zgrep='zgrep --color=auto'
```

Для очистки терминала в таком случае можно использовать только символ **c**.

Команда **unalias** удаляет созданный псевдоним.

```
unalias c
alias

alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
```

```
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mc='. /usr/libexec/mc/mc-wrapper.sh'
alias vi='vim'
alias view='vim -R'
alias which='(alias; declare -f) | /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot'
alias zegrep='zegrep --color=auto'
alias zfgrep='zfgrep --color=auto'
alias zgrep='zgrep --color=auto'
```

Т.к. псевдонимы сохраняются только до закрытия терминала, необходимо их создавать в начале каждой терминальной сессии. Для этого можно добавить все необходимые команды в файл **~/.bashrc** , который представляет собой обычный bash-скрипт, исполняемый каждый раз при открытии терминала.

```
[user@localhost pub]$ cat ~/.bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]
then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
```

Для удобства можно создать отдельный файл - **~/.bash_aliases**, в котором будут храниться все псевдонимы. Также это позволит уменьшить риск работы с **~/.bashrc**.

Для этого в конец файла **~/.bashrc** нужно добавить строки:

```
if [ -f ~/.bash_aliases ]; then
. ~/.bash_aliases
fi
```

Далее создать отдельный файл **~/.bash_aliases** командой:

```
nano ~/.bash_aliases
```

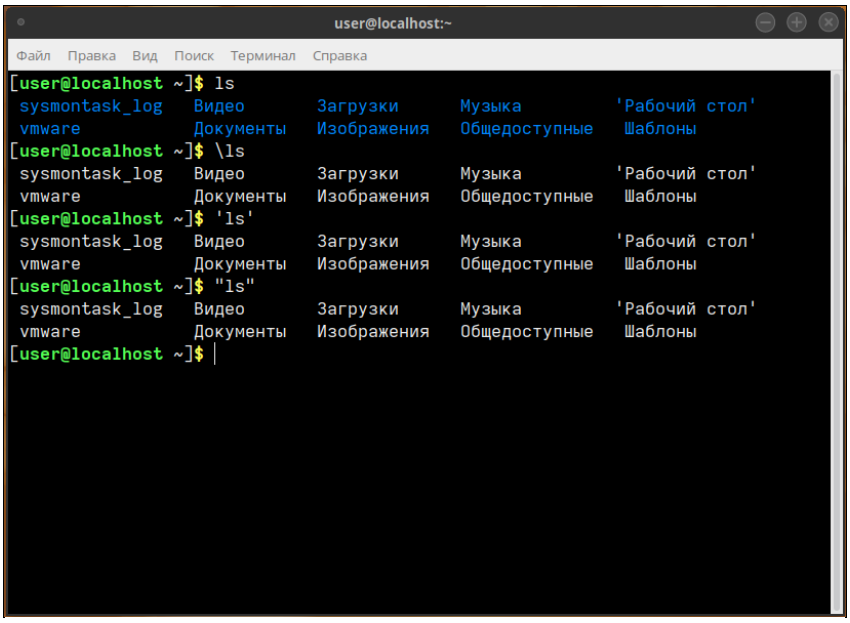
И вписать туда все нужные псевдонимы, например:

```
#Custom aliases XD
alias c=“clear“
alias cr=“cd /“
alias .=“cd ../“
alias up=“dnf update && dnf upgrade“
```

После обновления файла **~/.bashrc** (его исполнения или перезапуска терминала) все псевдонимы будут доступны при каждом входе в систему.

Чтобы временно отключить работу **alias** (например, когда созданный псевдоним совпадает с именем команды), при этом его не удаляя, необходимо перед командой поставить «\» либо использовать кавычки, например:

```
\c
“c“
'c'
```


user@localhost:~
Файл Правка Вид Поиск Терминал Справка
[user@localhost ~]$ ls
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$ \ls
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$ 'ls'
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$ "ls"
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$

Утилита записи терминальной сессии asciinema

Установка
Запись терминальных сессий
Воспроизведение записанного сеанса
Выгрузка записанного сеанса

Asciinema — простая и эффективная утилита командной строки, которая запускает запись терминальной сессии.

Asciinema использует псевдотерминал, чтобы сохранить все символы, которые выводятся в консоль, а также информацию о времени. Записанный файл занимает очень мало места.

При воспроизведении все сохраненные символы повторно отображаются на экране с установленными интервалами. При этом все вводимые и выводимые символы при необходимости можно скопировать в буфер обмена.

Установка

Для установки **asciinema** перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

```
dnf install asciinema
```

Запись терминальных сессий

Для начала записи с сохранением в локальный файл выполните команду:

```
asciinema rec <имя_файла>
```

После этого действия в терминале записываются и сохраняются в файле под указанным названием (в примере — test_rec) в текущем рабочем каталоге.

Для того чтобы закончить запись, необходимо нажать комбинацию клавиш «Ctrl+d» или ввести команду exit. Когда запись будет завершена, на экране отобразится соответствующее сообщение.

Например:

```
asciinema rec test_rec

asciinema: recording asciicast to test_rec
asciinema: press <ctrl-d> or type "exit" when you're done

lsb_release -a

LSB Version: :core-4.1-amd64:core-4.1-noarch
Distributor ID: RED SOFT
Description: RED OS release MUROM (7.3.1) DESKTOP Standard Edition
Release: 7.3.1
Edition: Standard
Codename: MUROM

mkdir test_dir
ls -l

drwxrwxr-x. 2 user user 4096 апр 26 10:05 test_dir
-rw-rw-r--. 1 user user 2997 апр 26 10:05 test_rec

exit

exit
asciinema: recording finished
asciinema: asciicast saved to test_rec
```

Воспроизведение записанного сеанса

Для воспроизведения ранее записанного сеанса в терминале выполните команду:

```
asciinema play <имя_файла>
```

Выгрузка записанного сеанса

Локальную запись терминального сеанса можно выгрузить на сервер asciinema.org, для того чтобы можно было поделиться этой записью с другими людьми.

Для этого необходимо выполнить команду:

```
asciinema upload <имя_файла>
```

Например:

```
asciinema upload test_rec

View the recording at:

https://asciinema.org/a/5yyTPW5jud4nqhlUzPd3uCby3

This installation of asciinema recorder hasn't been linked to any asciinema.org
account. All unclaimed recordings (from unknown installations like this one)
are automatically archived 7 days after upload.

If you want to preserve all recordings made on this machine, connect this
installation with asciinema.org account by opening the following link:

https://asciinema.org/connect/da5948fa-55c2-4c21-a87d-4d63fd4be02a
```

В результате будет предоставлена ссылка, перейдя по которой можно просмотреть запись. Также в плеере можно скопировать в буфер обмена все, что вводится и выводится в терминале.

Существует возможность выгрузки записи сразу после ее окончания (без предварительного локального сохранения). Для этого выполните команду без указания имени файла:

```
asciinema rec

asciinema: recording asciicast to /tmp/tmp6imx6gtm-ascii.cast
asciinema: press <ctrl-d> or type "exit" when you're done

uname -r

5.15.10-1.el7.x86_64

exit

exit
asciinema: recording finished
asciinema: press <enter> to upload to asciinema.org, <ctrl-c> to save locally

View the recording at:

https://asciinema.org/a/TyRdslPzDQtAmJZQH0zfXUOzX

This installation of asciinema recorder hasn't been linked to any asciinema.org
account. All unclaimed recordings (from unknown installations like this one)
are automatically archived 7 days after upload.

If you want to preserve all recordings made on this machine, connect this
installation with asciinema.org account by opening the following link:

https://asciinema.org/connect/da5948fa-55c2-4c21-a87d-4d63fd4be02a
```

После окончания записи будет предложено 2 варианта:

- нажать «**Enter**», чтобы выгрузить запись на сервер;
- нажать комбинацию «**Ctrl+c**», чтобы сохранить запись локально.

Screen - запуск виртуальных терминалов в режиме сессий

Screen – это приложение, позволяющее запускать несколько виртуальных терминалов в режиме сессий. После того как сессия создана, от неё можно отключиться, а позже — снова подключиться, причём с любого другого хоста, на котором установлен SSH-клиент.

Процессы, запущенные в **screen**, продолжают выполняться и после того, как пользователь отключается от сессии или вообще от хоста в целом. Это ещё одна причина (кроме повышения удобства работы в командной строке вследствие использования возможности перехода между окнами), по которой используется **screen**.

Если соединение с интернетом ненадёжное, или у пользователя нет возможности поддерживать постоянное соединение, или существует необходимость запустить выполнение процесса в офисе, а остановить – дома, то использование **screen** – способ решить подобные проблемы.

Вы можете подробнее ознакомиться с информацией о работе терминальных мультиплексоров, просмотрев наши обучающие видео:

- на **RuTube** — Многооконность в консоли;
- в **Яндекс.Дзен** — Многооконность в консоли;
- в **VK Видео** — Многооконность в консоли.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы **screen** выполните команду:

```
dnf install screen
```

Для запуска новой сессии **screen** выполните команду:

```
screen
```

Все управляющие команды начинаются с комбинации клавиш «**Ctrl + a**», затем следует буква или сочетание клавиш. Буквы разных регистров выполняют разные команды. Также сочетания можно заменять текстом. Для его ввода нажмите «**Ctrl + a**» и «**:**», после чего вводите текст.

Команда **screen** обладает большим набором горячих клавиш. Полный их список можно посмотреть с помощью комбинации клавиш «**Ctrl+a ?**».

Рассмотрим основные из них:

- «**Ctrl+a c**» - Создать новое окно;
- «**Ctrl+a n**» - Перейти к следующем окну;
- «**Ctrl+a p**» - Перейти к предыдущему окну;
- «**Ctrl+a a**» - Изменить имя окна;
- «**Ctrl+a k**» - Закрыть текущее окно;
- «**Ctrl+a 1**» - Перейти к окну с номером 1 (можно использовать цифры от 0 до 9);
- «**Ctrl+a “**» - Вывести список окон, стрелками выбрать необходимую для перехода;
- «**Ctrl+a S**» - Разделить экран по горизонтали;
- «**Ctrl+a |**» - Разделить экран по вертикали;
- «**Ctrl+a Tab**» - Переключение между окнами;
- «**Ctrl+a d**» - Отключиться от сессии screen (при этом процессы и приложения запущенные в сессии продолжают выполняться).

При создании новой сессии **screen** можно задать для нее название с помощью ключа **-S <имя>**:

```
screen -S session1
```

Просмотреть список активных сессий можно командой:

```
screen -ls
```

Чтобы подключиться к существующей сессии, выполните команду:

```
screen -x <имя_сессии> | <ID_сессии>
```

Рассмотрим пример использования утилиты при работе на удаленном хосте через ssh-соединение.

После подключения к удаленному хосту создайте новую сессию screen с названием **session1**:

```
screen -S session1
```

Затем выполните на хосте необходимые действия и команды. Для примера запустим **ping** до ресурса **ya.ru**:

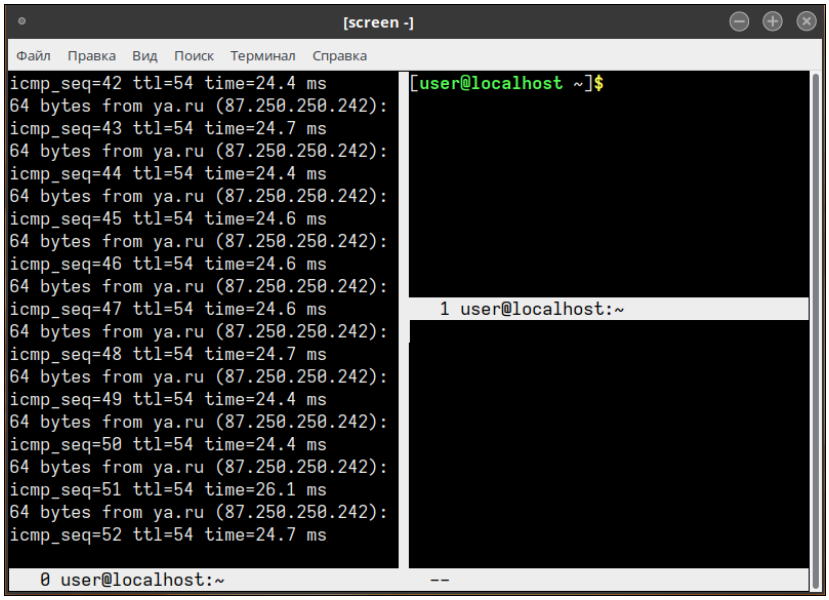
```
ping ya.ru
```

Для отключения от сессии нажмите сочетание «**Ctrl+a d**». При этом процесс **ping** продолжит выполнение, даже если разорвать ssh-подключение к удаленной машине. Чтобы вернуться в нашу сессию выполним команду:

```
screen -r session1
```

Можно увидеть, что утилита **ping** все еще работает.

Для того чтобы разделить экран терминала пополам, нужно сначала нажать комбинацию «**Ctrl+a**», а затем «**S**» или «|» (т.е. «**Shift + **»). При разделении окон новая оболочка не запускается на вновь созданной панели, для этого необходимо перейти в новое пространство с помощью «**Ctrl+a+Tab**» и вызвать новый экземпляр оболочки вручную с помощью «**Ctrl+a+C**».



Менеджер терминалов tmux

Tmux - это аналог утилиты **screen**, который имеет больше функций.

Вы можете подробнее ознакомиться с информацией о работе терминальных мультиплексоров, просмотрев наши обучающие видео:

- на **RuTube** — Многооконность в консоли;
- в **Яндекс.Дзен** — Многооконность в консоли;
- в **VK Видео** — Многооконность в консоли.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты выполните команду:

```
dnf install tmux
```

Чтобы создать новую сессию выполните команду:

```
tmux
```

Также можно создать сессию с указанием имени:

```
tmux new-session -s <имя_сессии>
```

По умолчанию для активации сочетания клавиш нужно нажать «**Ctrl+b**», отпустить, а потом нажать нужную клавишу.

Основные сочетания клавиш **tmux**:

- «**Ctrl+b c**» - создать новое окно;
- «**Ctrl+b w**» - выбрать окно из списка;
- «**Ctrl+b 0-9**» - открыть окно по его номеру;
- «**Ctrl+b ,**» - переименовать текущее окно;
- «**Ctrl+b %**» - разделить текущую панель по вертикали;
- «**Ctrl+b "**» - разделить текущую панель по горизонтали;
- «**Ctrl+b <стрелка>**» - перейти на панель, находящуюся в стороне, куда указывает стрелка;
- «**Ctrl+b Ctrl+<стрелка>**» - изменить размер текущей панели;
- «**Ctrl+b o**» - перейти на следующую панель;
- «**Ctrl+b ;**» - переключаться между текущей и предыдущей панелью;
- «**Ctrl+b x**» - закрыть текущую панель;
- «**Ctrl+b [**» - войти в режим копирования (подробнее ниже);
- «**Ctrl+b]**» - вставить из внутреннего буфера обмена **tmux**;
- «**Ctrl+b d**» - отключится от текущей сессии;
- «**Ctrl+b :**» - открыть командную строку.

По умолчанию поддержка мыши в **tmux** отключена, но если вы работаете в графическом окружении, можно её включить. Это даст несколько преимуществ: вы сможете выбирать активную панель мышкой, копировать текст во внутренний буфер обмена, менять размер панелей, использовать прокрутку для просмотра истории вывода и т.д. Для включения поддержки мыши откройте файл **~/.tmux.conf**:

```
nano ~/.tmux.conf
```

и добавьте следующие строки:

```
set-option -g -q mouse on bind-key -T root WheelUpPane if-shell -F -t = "#{alternate_on}" "send-keys -M" "select-pane -t =; copy-mode -e; send-keys -M" bind-key -T root WheelDownPane if-shell -F -t = "#{alternate_on}" "send-keys -M" "select-pane -t =; send-keys -M"
```

В сессии **tmux** нажмите сочетание «**Ctrl+b :**», чтобы открыть командную строку, и введите команду:

```
source-file ~/.tmux.conf
```

Теперь поддержка мыши включена.

Основные команды **tmux** для управления сессиями:

- **attach-session (attach)** - подключиться к уже существующей сессии. В параметре необходимо передать опцию **-t** и идентификатор сессии;
- **detach-session (detach)** - отключить всех клиентов (или переданного с помощью опции **-t**) от сессии, переданной в опции **-s**;
- **has-session** - проверить существует ли сессия, аналогично, надо передать идентификатор сессии;
- **kill-server** - остановить все запущенные сессии;
- **kill-session** - завершить сессию, переданную в параметре **-t**;
- **list-clients (lsc)** - посмотреть клиентов, подключенных к сессии **-t**;
- **list-sessions (ls)** - вывести список всех запущенных сессий;
- **new-session (new)** - создать новую сессию, можно передать имя сессии в опции **-s** и стартовую директорию в опции **-c**;
- **rename-session** - переименовать сессию, нужно передать идентификатор сессии и новое имя.

Принцип работы с **tmux** аналогичен работе со **screen**.

Создайте на хосте новую сессию:

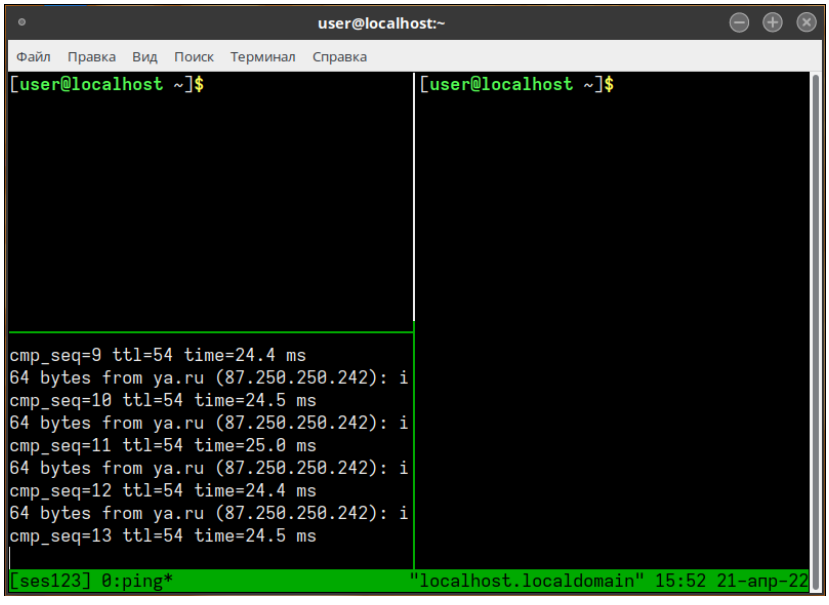
```
tmux new -s session1
```

Выполните необходимые действия. Отключитесь от сессии через комбинацию «**Ctrl+a d**».

Чтобы вернуться в сессию, выполните команду:

```
tmux attach -t session1
```

В рамках одной сессии может быть задействовано неограниченное количество окон; каждое из них может быть, в свою очередь, разделено на части.



Эмулятор терминала terminator

Установка
Функционал
Основные комбинации клавиш

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: terminator-2.0.1-1

Terminator — эмулятор терминала в РЕД ОС, который имеет возможность отображения нескольких терминалов в одном окне. Новые терминалы можно добавлять, разбивая текущее окно по горизонтали и по вертикали. **Terminator** позволяет экономить рабочее пространство, предоставляя возможность работы в одном окне.

Вы можете подробнее ознакомиться с информацией о работе терминальных мультиплексоров, просмотрев наши обучающие видео:

- на **RuTube** — Многооконность в консоли;
- в **Яндекс.Дзен** — Многооконность в консоли;
- в **VK Видео** — Многооконность в консоли.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

По умолчанию **terminator** предустановлен в РЕД ОС.

Если по каким-либо причинам утилита отсутствует в вашей системе, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду установки:

```
dnf install terminator
```

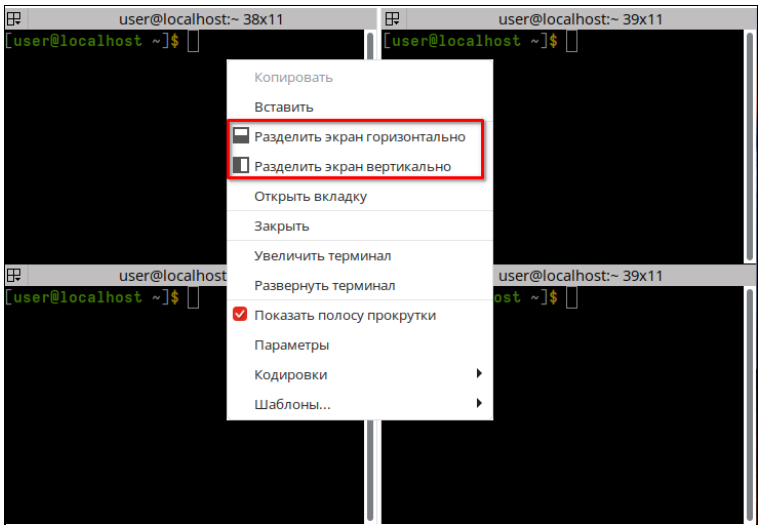
Работа в **terminator** не отличается от работы в **mate-terminal** и **gnome-terminal**.

Для запуска утилиты через терминал введите команду:

```
terminator
```

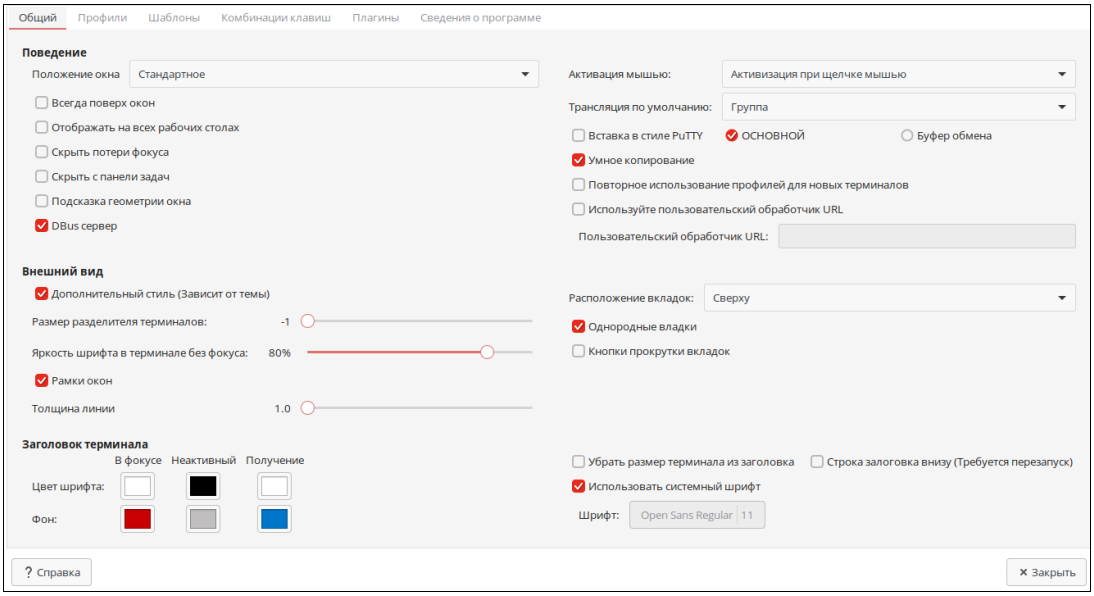
Функционал

Одной из отличительных особенностей **terminator** является разделение экрана на несколько окон. Сделать это можно, нажав ПКМ по пустому пространству окна и выбрав соответствующие опции.

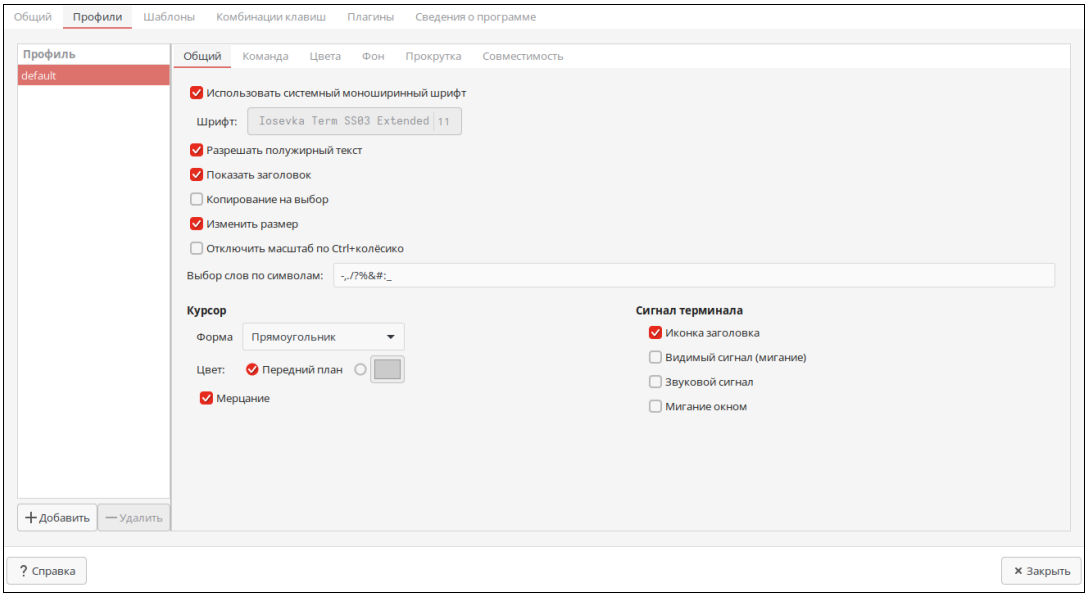


Утилита поддерживает большое количество настроек, которые можно определить индивидуально, для этого нажмите ПКМ по пустому пространству окна и перейдите в раздел «**Параметры**».

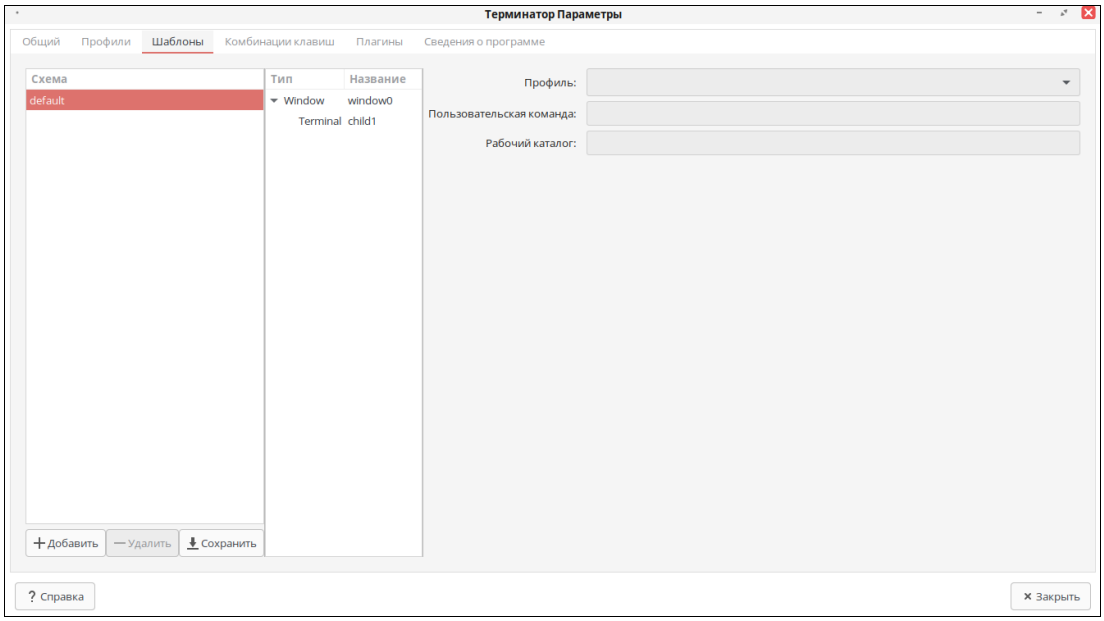
На вкладке «**Общие**» настраиваются основные параметры терминала. Здесь можно выбрать шрифт и размер шрифта по умолчанию, включить или отключить различные функции, такие как прокрутка назад или мигающий текст, а также указать размер и положение окна по умолчанию.



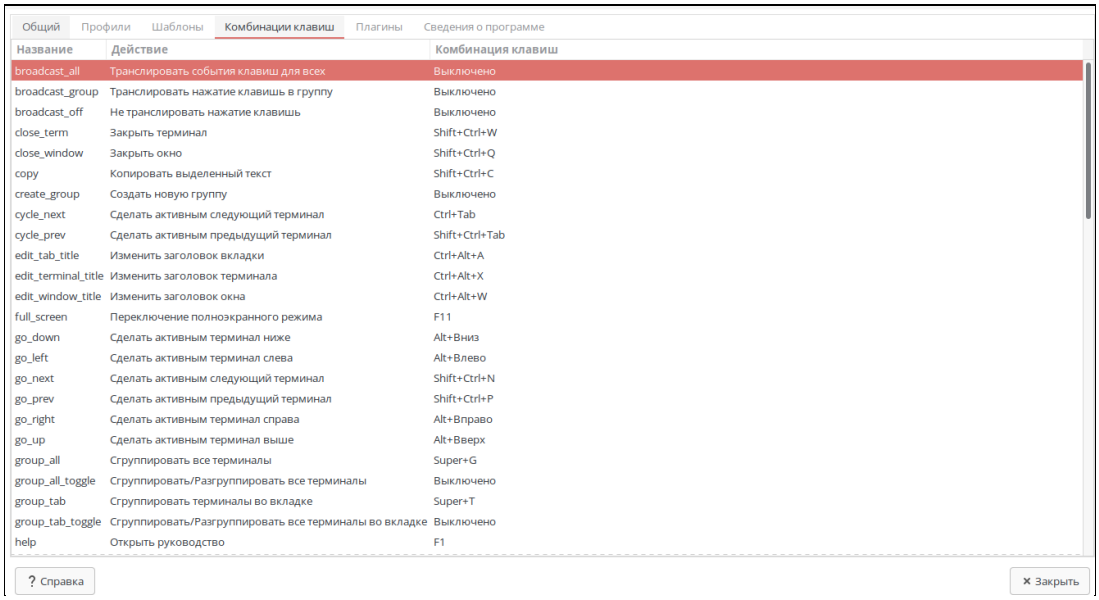
На вкладке «**Профили**» можно создавать и управлять профилями терминала. Профили можно дублировать и удалять, также есть возможность установить профиль по умолчанию при открытии новых окон и задать различные настройки для каждого профиля, такие как цветовая схема терминала, начальный рабочий каталог и команда, запускаемая при старте терминала.



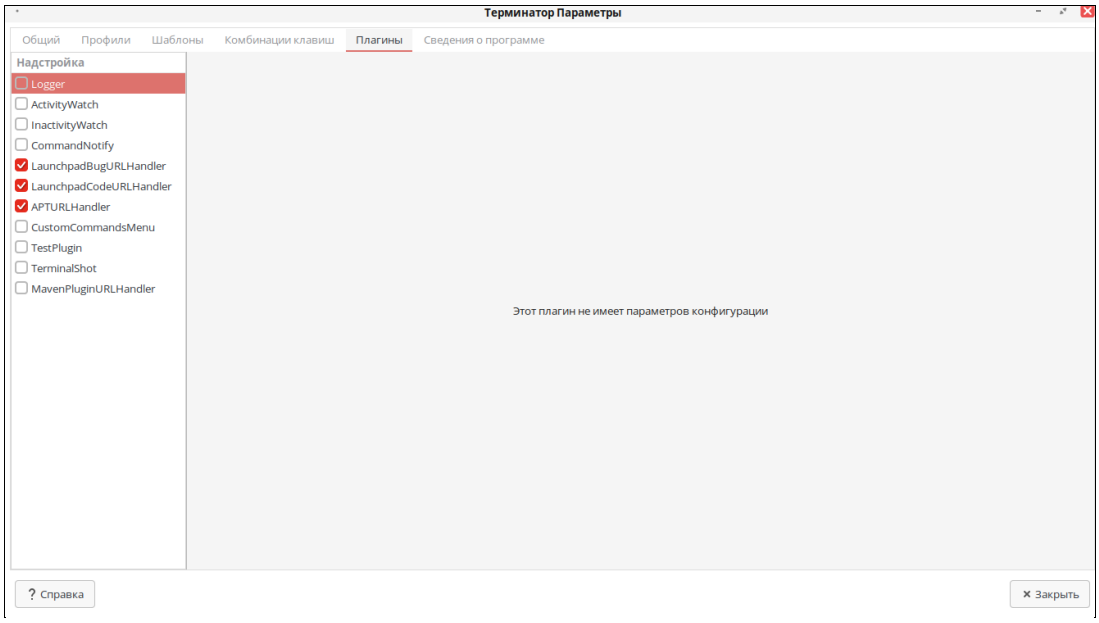
На вкладке «**Шаблоны**» настраивается макет окна **terminator**, включая количество рядов и столбцов терминалов, их размер и положение, а также то, как они должны быть расположены — горизонтально или вертикально. Здесь также можно сохранять и загружать различные конфигурации макета для быстрого переключения между различными вариантами расположения терминалов.



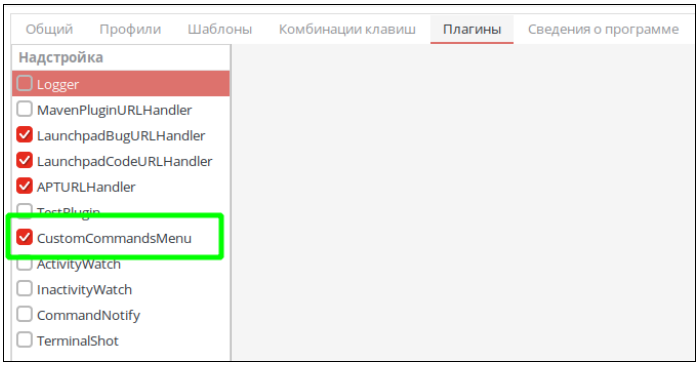
На вкладке «**Сочетания клавиш**» можно настроить существующие сочетания клавиш или создать новые для выполнения определенных действий, таких как разделение текущего терминала по вертикали или горизонтали, переключение между терминалами или переход в полноэкранный режим.



Утилита поддерживает различные плагины, которые добавляют дополнительные возможности и функциональность. На вкладке «**Плагины**» можно управлять и настраивать эти плагины. Также можно включить или отключить определенные плагины, указать специфические настройки плагина.

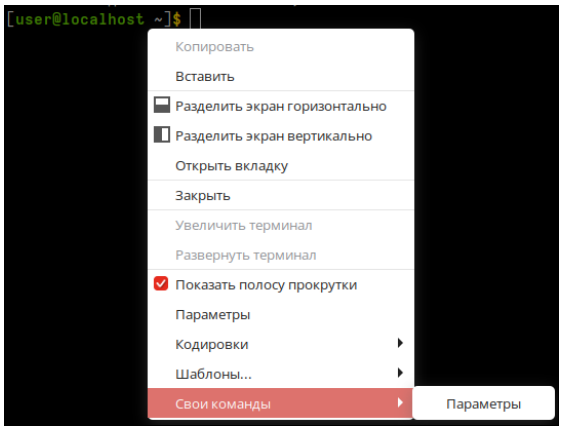


В качестве примера рассмотрим работу плагина **CustomCommandsMenu**, который добавляет пользовательские команды для быстрого доступа в контекстное меню терминала. Для этого в параметрах терминала на вкладке «**Плагины**» включите плагин **CustomCommandsMenu**, установив на нем галочку.

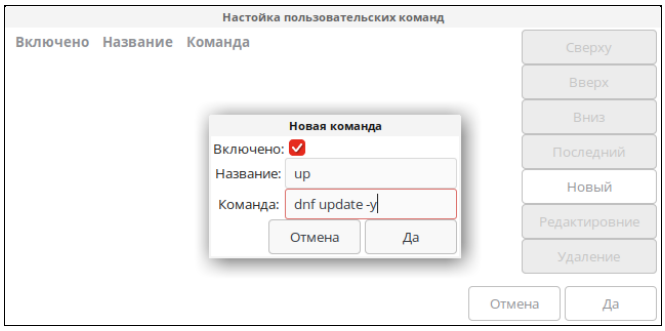


Закройте окно настроек.

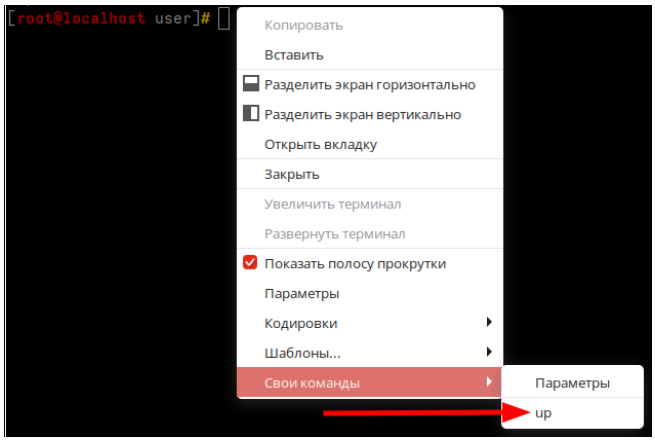
После этого нажмите ПКМ по свободной части окна терминала и в контекстном меню выберите «**Свои команды**» — «**Параметры**».



В открывшемся окне нажмите «**Новый**» для создания нового профиля команды. В окне «**Новая команда**» в поле «**Включено**» установите галочку, затем укажите название команды и пропишите непосредственно команду, которую должен будет выполнять терминал. Для сохранения изменений нажмите «**Да**».



После выполнения вышеперечисленных действий команда станет доступна из контекстного меню терминала. Для ее вызова нажмите ПКМ по свободной части окна терминала, в контекстном меню выберите «**Свои команды**» — «**up**».



Если все настроено верно, команда будет выполнена.

Основные комбинации клавиш

Следующие сочетания клавиш клавиатуры установлены по умолчанию и являются самыми часто используемыми в **terminator**:

- «Ctrl + Shift + O» — разделение окна терминала по вертикали;
- «Ctrl + Shift + E» — разделение окна терминала по горизонтали;
- «Alt + ←|↑|→|↓» — изменение фокуса терминала;
- «Ctrl + Tab» — перемещение между терминалами;
- «F11» — переход в полноэкранный режим;
- «Ctrl + колесо мыши» — увеличение и уменьшение шрифта;
- «Ctrl + 0» — сброс настроек до исходного состояния;
- двойной клик ЛКМ по красной строке — изменение имени окон.

expect - инструмент для автоматизации и тестирования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: expect-5.45.4-1

Expect — инструмент для автоматизации и тестирования, входящий в состав РЕД ОС. Предназначен для интерактивных приложений, таких как *telnet*, *ftp*, *passwd*, *fsck*, *rlogin*, *tip*, *ssh* и других.

Для установки **expect** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install expect
```

Для проверки работоспособности инструмента будет создан небольшой bash-скрипт, которому потребуется взаимодействие с пользователем. Для примера скрипт будет назван **questions**.

nano ./questions

```
#!/bin/bash
echo "Hello, what's your name?"
read $REPLY
echo "Can I ask you some question?"
read $REPLY
echo "What's your favorite OS?"
read $REPLY
```

Затем будет создан expect-скрипт, который запустит скрипт **questions** и ответит на его вопросы:

nano ./answerbot

```
#!/usr/bin/expect -f
set timeout -1
spawn ./questions
expect "Hello, what's your name?\r"
send -- "Im Dmitry\r"
expect "Can I ask you some question?\r"
send -- "Sure\r"
expect "What's your favorite OS?\r"
send -- "RedOS\r"
expect eof
```

В начале скрипта находится строка идентификации, которая (в данном примере) содержит путь к **expect**, т. к. интерпретацией скрипта будет заниматься именно **expect**. Во второй строке отключается тайм-аут путем присвоения переменной **timeout** значения **-1**. Остальная часть кода – это и есть автоматизация работы с bash-скриптом.

Сначала с помощью команды **spawn** запускается bash-скрипт с указанием пути к нему. Вместо пути к скрипту можно указать любую другую утилиту командной строки. Далее задана последовательность вопросов, поступающих от bash-скрипта, и ответов, которые дает expect-скрипт. Получив вопрос от подпроцесса, **expect** выдает ему заданный ответ и ожидает получения следующего вопроса.

В последней строке expect ожидает признака конца файла и скрипт, выполнив все действия до этой команды, завершается.

Рассмотрим данный пример на практике. Назначим скриптам права на исполнение с помощью команд:

```
chmod +x ./answerbot
chmod +x ./questions
```

и вызовем answerbot:

./answerbot

```
spawn ./questions
Hello, what's your name?
```

```
Im Dmitry
Can I ask you some question?
Sure
What's your favorite OS?
RedOS
```

Обратите внимание, что после запуска скрипта **answerbot** всё происходит полностью в автоматическом режиме. То же самое можно проделать для любой утилиты командной строки. Здесь необходимо отметить, что bash-скрипт в примере устроен очень просто, мы точно знаем, какие именно данные он выводит, поэтому написать expect-скрипт для взаимодействия с ним несложно.

Задача усложняется при работе с программами, которые написаны другими разработчиками. Однако здесь на помощь приходит средство для автоматизированного создания expect-скриптов.

Autoexpect — автоматизированное создание expect-скриптов

Autoexpect позволяет запускать программы, которые необходимо автоматизировать, после чего записывает то, что они выводят, и то, что пользователь вводит, отвечая на их вопросы. Вызовем **autoexpect** для нашего скрипта командой:

```
autoexpect ./questions

autoexpect started, file is script.exp
Hello, what's your name?
Dmitry
Can I ask you some question?
Sure
What's your favorite OS?
RED OS
autoexpect done, file is script.exp
```

В этом режиме взаимодействие с bash-скриптом ничем не отличается от обычного – мы сами вводим ответы на его вопросы.

После завершения работы с bash-скриптом **autoexpect** сообщит о том, что собранные данные записаны в файл **script.exp**. Проверим содержимое этого файла.

```
cat ./script.exp

set timeout -1
spawn ./questions
match_max 100000
expect -exact "Hello, what's your name?\r
"
send -- "Dmitry\r"
expect -exact "Dmitry\r
Can I ask you some question?\r
"
send -- "Sure\r"
expect -exact "Sure\r
What's your favorite OS?\r
"
send -- "RED OS\r"
expect eof
```

В целом, за исключением некоторых деталей, перед нами такой же скрипт, который мы написали самостоятельно. Если запустить этот скрипт, результат будет тем же.

Таким образом, можно автоматизировать работу практически любого bash-скрипта.

Общая информация

РЕД ОС, как и любой UNIX – многопользовательская операционная система. Также имеются группы пользователей, основное предназначение которых - облегчить управление большим количеством пользователей, а также более точно распределить права доступа к различным объектам системы. Пользователи и группы внутри системы обозначаются цифровыми идентификаторами - UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод ее может быть примерно следующим:

```
id

uid=1000(test) gid=1000(test) группы=1000(test),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 1000) входит в группы *test* и *wheel*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Вы можете подробнее ознакомиться с информацией по управлению пользователями в системе, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

ВНИМАНИЕ!

В связи с тем, что в дистрибутивах РЕД ОС большинство привилегированных системных утилит имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

Роли пользователей

Роль sysadm - администратор системы
Роль — пользователь системы

В ОС пользователи по умолчанию сопоставляются SELinux-пользователю <**unconfined_u**>. SELinux-пользователь <**unconfined_u**>, в свою очередь, сопоставлен ролям <**unconfined_r**> и <**system_r**>.

Обе роли <**unconfined_r**> и <**system_r**> сопоставляются доменам безопасности SELinux. Домены безопасности SELinux - это определённые окружения безопасности для процессов.

Неограниченный домен безопасности <**unconfined_t**> - зарезервированное окружение для процессов, которые в значительной степени освобождены от ограничений SELinux. Роль <**system_r**> сопоставляется доменам безопасности для системных процессов.

SELinux-пользователь <**unconfined_u**> имеет доступ к роли <**system_r**>, чтобы иметь возможность запускать системные процессы в своих доменах безопасности. SELinux-пользователь <**unconfined_u**> работает в домене безопасности <**unconfined_t**> через роль <**unconfined_r**>, которой он сопоставлен.

Команда «semanage» позволяет добавлять, изменять и удалять сопоставления между ОС- и SELinux-пользователями, так же как и другие настройки, касающиеся управления SELinux.

Чтобы с помощью команды «semanage» посмотреть какому SELinux- пользователю по умолчанию сопоставлены пользователи ОС, наберите:

```
semanage login -l | grep default
```

В примере выше пользователи по умолчанию сопоставлены SELinux- пользователю <**unconfined_u**>.

Чтобы изменить это и сопоставить пользователей по умолчанию ограниченному SELinux-пользователю с именем <**user_u**>, просто наберите:

```
semanage login -m -s user_u "__default__"
```

В результате все новые пользователи будут по умолчанию сопоставляться ограниченному SELinux-пользователю <**user_u**>.

Вы можете переопределить данное сопоставление при добавлении пользователей командой «**useradd**» используя опцию «**-Z**». Эта опция определяет, какому SELinux-пользователю должен быть сопоставлен пользователь ОС.

Например, наберите:

```
useradd -Z guest_u joe
```

В результате будет создан новый пользователь с именем **joe**, который будет сопоставлен SELinux-пользователю <**guest_u**>, вместо определённого по умолчанию SELinux-пользователя.

Также для изменения сопоставления между пользователем и SELinux-пользователем может быть использована команда «**usermod**» с опцией «**-Z**».

Существует несколько предопределённых профилей SELinux-пользователей. Список данных профилей можно вывести командой «**semanage**», наберите:

```
semanage user -l
```

SELinux-пользователь <**unconfined_u**> - это среда, в которой по умолчанию работают все пользователи. Этот пользователь в значительной степени освобождён от ограничений, накладываемых SELinux. Если Вы хотите повысить безопасность вашей системы, тогда не следует сопоставлять реальных пользователей, не пользователя root, SELinux-пользователю <**unconfined_u**>.

Вход пользователя root должен быть запрещён. Root должен иметь возможность войти с терминала только в случае крайней необходимости. Чтобы повысить безопасность использования root, можно сопоставить пользователя root SELinux-пользователю <**sysadm_u**>.

Ролевой доступ SELinux используется для обеспечения возможности назначения нескольких ограниченных окружений SELinux одному SELinux-пользователю.

В SELinux роли пользователя (*User Roles*) - это домены пользователя или пользовательские домены (*User Domains*). Когда упоминаются роли, часто имеется в виду дополнительный (*secondary*) пользовательский домен пользователя SELinux. Часто роли, предназначенные для использования в качестве дополнительных доменов пользователя, отличаются от основных (*primary*) доменов. Это объясняется тем, что пользователи ОС фактически не используют для входа в систему роли, созданные как дополнительные домены пользователя. Вместо этого пользователи Linux, используя команду «**sudo**» или комбинацию команд «**su**» и «**newrole**», осуществляют переключение домена или доменный переход (*Domain Transition*) к их дополнительной роли.

Роль sysadm - администратор системы

Пример роли, предназначенной для использования в качестве основного домена пользователя. SELinux пользователь <**sysadm_u**> сопоставлен роли <**sysadm_r**>. Это сопоставление можно увидеть, выполнив команду:

```
semanage user -l | grep sysadm_u
```

По умолчанию пользователи ОС, сопоставленные пользователю SELinux <**sysadm_u**>, работают с ролью <**sysadm_r**>. В этом случае <**sysadm_r**> — это основной домен пользователя.

SELinux пользователь <**staff_u**> также сопоставлен роли <**sysadm_r**>. Основным пользовательским доменом пользователя SELinux <**staff_u**> является (роль) <**staff_r**>. Контексты по умолчанию, обозначенные в **/etc/selinux/targeted/contexts/users/staff_u**, определяют, с какими пользовательскими доменами пользователи будут подключаться по умолчанию и с какими пользовательскими доменами пользователи могут войти, указав домен пользователя при входе.

По умолчанию SELinux пользователь <**staff_u**> входит в систему в домен пользователя <**staff_t**>. Роль <**sysadm_r**>, предназначенная для использования в качестве основного домена пользователя, может быть использована при входе, например, следующим образом:

```
ssh joe/sysadm_r@localhost.localdomain.tld
```

Также роль <**sysadm_r**> может быть использована при переходе домена выполнением команд «**sudo**» и «**su**» вместе с «**newrole**», как это предусмотрено для дополнительных доменов пользователей.

Пользовательский домен <**sysadm_t**> является окружением по умолчанию для SELinux-пользователя <**sysadm_u**> и предназначен для использования в качестве дополнительного окружения для SELinux-пользователя <**staff_u**>, хотя даже SElinux-пользователь <**staff_u**> может настроить подключаемый модуль аутентификации (*Pluggable Authentication Module*) <**pam_selinux**> для использования <**sysadm_t**> в качестве его основного домена пользователя.

Роль <user_r> — пользователь системы

Пользовательский домен, используемый только в качестве основного. Описание пользователя SELinux <**user_u**> приведено ранее.

Какие-то домены пользователей могут использоваться пользователями для входа в систему, потому что эти домены, например, имеют полномочия по доступу к домашней директории пользователя. Такие домены в предыдущей части назывались основными (*primary*) пользовательскими доменами. Другие домены созданы в качестве дополнительных. Пользователи, используя команды «**sudo**» или «**su**» вместе с «**newrole**», могут осуществить доменный переход (*Domain Transition*) к этим дополнительным доменам.

Дополнительные домены не могут использоваться для входа в систему. Далее будет продемонстрировано как создаётся такой дополнительный пользовательский домен. Целью является реализовать привилегированную роль SELinux, которой предоставлены полномочия по управлению DNS службой Bind.

Начнём с создания нового дополнительного домена пользователя с названием «**bindadm**», основанного на предустановленном домене SELinux <**webadm_t**>. Новый домен пользователя основан на двух файлах с исходным текстом политики SELinux (SELinux Source Policy):

- webadm.te;
- webadm.if.

Файлы исходных текстов политики SELinux с расширением "**.te**" называются Type Enforcement файлы. Файлы с расширением "**.if**" называются интерфейсными (Interface files). Файлы *Type Enforcement* содержат описания (*Declarations*) и политику (*Policy*), персональные или локальные для данного домена (*Domain*). Интерфейсные файлы содержат описания и политики, общие для этого домена и других доменов, желающими взаимодействовать с данным доменом.

```
mkdir ~/bindadm; cd ~/bindadm
echo "policy_module(bindadm, 0.0.1)" >> bindadm.te
echo "role bindadm_r" >> bindadm.te
echo "userdom_base_user_template(bindadm)" >> bindadm.te
echo "allow bindadm_t self:capability { dac_override dac_read_search kill sys_ptrace sys_nice" >> bindadm.te
echo "files_dontaudit_search_all_dirs(bindadm_t)" >> bindadm.te
echo "files_manage_generic_locks(bindadm_t)" >> bindadm.te
echo "files_list_var(bindadm_t)" >> bindadm.te
echo "selinux_get_enforce_mode(bindadm_t)" >> bindadm.te
echo "seutil_domtrans_setfiles(bindadm_t)" >> bindadm.te
echo "logging_send_syslog_msg(bindadm_t)" >> bindadm.te
echo "userdom_dontaudit_search_user_home_dirs(bindadm_t)" >> bindadm.te
```

Это основное содержимое для привилегированного дополнительного домена пользователя. Исключена политика, специфичная для управления службой Apache.

Теперь добавим политику, специфичную для управления службой Bind. Можно позаимствовать эту политику из исходных текстов политики для Bind. Как уже отмечалось, общая политика располагается в интерфейсных файлах. Это значит, что если мы хотим включить общую политику, относящуюся к Bind, можно посмотреть в соответствующем файле политики **bind.if**. Для включения этой политики в наш Type Enforcement файл требуется всего лишь добавить вызов этого интерфейса:

```
echo "bind_admin(bindadm_t, bindadm_r)" >> bindadm.te
```

На этом Type Enforcement файл bindadm заканчивается. Далее необходимо обеспечить другим доменам возможность взаимодействия с нашим доменом <**bindadm_t**>. Реализуем эту часть политики, взяв за основу файл **webadm.if**.

```
echo "## Bind administrator role" > bindadm.if
echo "########################################" >> bindadm.if
echo "##" >> bindadm.if
echo "## Change to the bind administrator role." >> bindadm.if
echo "##" >> bindadm.if
echo '##' >> bindadm.if
echo "##" >> bindadm.if
echo "## Role allowed access." >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "#" >> bindadm.if
echo "interface(\`bindadm_role_change',\`" >> bindadm.if
echo " gen_require(\`" >> bindadm.if
echo " role bindadm_r;" >> bindadm.if
echo " ')" >> bindadm.if
echo " allow  $1 bindadm_r;" >> bindadm.if
echo "')" >> bindadm.if
```

Позже общая политика администратора **Bind** (Bind Administrator Shared policy) будет использоваться в нашем основном специально созданном пользовательском домене SELinux.

Следующим шагом будет создание специализированного пользовательского домена SELinux для обслуживания Bind, разрешающего данному домену осуществлять переход к роли <**bindadm_r**> вызовом интерфейса <**bindadm_role_change**>. Создаваемый домен SELinux будет основан на пользовательском домене <**staff_t**>, описание политики смотрим в файле **staff.te**.

```
echo "policy_module(bindguy, 0.0.1)" > bindguy.te
echo "role bindguy_r;" >> bindguy.te
echo "userdom_unpriv_user_template(bindguy)" >> bindguy.te
echo "sudo_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "ssh_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "kernel_read_ring_buffer(bindguy_t)" >> bindguy.te
echo "kernel_getattr_core_if(bindguy_t)" >> bindguy.te
echo "kernel_getattr_message_if(bindguy_t)" >> bindguy.te
echo "kernel_read_software_raid_state(bindguy_t)" >> bindguy.te
echo "auth_domtrans_pam_console(bindguy_t)" >> bindguy.te
echo "libs_manage_shared_libs(bindguy_t)" >> bindguy.te
echo "seutil_run_newrole(bindguy_t, bindguy_r)" >> bindguy.te
echo "netutils_run_ping(bindguy_t, bindguy_r)" >> bindguy.te
echo "domain_read_all_domains_state(bindguy_t)" >> bindguy.te
echo "domain_getattr_all_domains(bindguy_t)" >> bindguy.te
echo "domain_obj_id_change_exemption(bindguy_t)" >> bindguy.te
echo "files_read_kernel_modules(bindguy_t)" >> bindguy.te
echo "kernel_read_fs_sysctls(bindguy_t)" >> bindguy.te
echo "modutils_read_module_config(bindguy_t)" >> bindguy.te
echo "modutils_read_module_deps(bindguy_t)" >> bindguy.te
echo "miscfiles_read_hwdata(bindguy_t)" >> bindguy.te
echo "term_use_unallocated_ttys(bindguy_t)" >> bindguy.te
```

Чтобы разрешить домену <**bindguy_t**> осуществлять переход в ограниченное окружение SELinux <**bindadm_t**>, добавим вызов интерфейса <**bindadm_role_change**>, определённого в нашем интерфейсном файле **bindadm.if**:

```
echo "bindadm_role_change(bindguy_r)" >> bindguy.te
```

Можно также автоматически создать сопоставление пользователя SELinux с именем <**bindguy_u**> ролям <**bindguy_r**>, <**bindadm_r**> и <**system_r**>. Роль <**system_r**> включается, чтобы <**bindadm_t**> мог остановить, запустить и перезапустить системную службу **bind**.

```
echo "gen_user(bindguy_u, user, bindguy_r system_r bindadm_r, s0,  s0 - mls_systemhigh,
mcs_allcats)" >> bindguy.te
```

Чтобы программы входа знали, что bindguy допустимый пользователь, добавим контексты по умолчанию для этого пользователя, взяв за основу контексты по умолчанию пользователя <**staff_u**>:

```
cp /etc/selinux/targeted/contexts/users/staff_u
/etc/selinux/targeted/contexts/users/bindguy_u
sed -i 's/staff/bindguy/g'
/etc/selinux/targeted/contexts/users/bindguy_u
```

Теперь можно собрать и установить обе политики bindguy и bindadm:

```
make -f /usr/share/selinux/devel/Makefile
semodule -i bindguy.pp bindadm.pp
```

Далее командой «**useradd**», опцией «**-Z**» и параметром <**bindguy_u**> можно создать нового пользователя Linux:

```
useradd -Z bindguy_u bindguy
```

Для того чтобы разрешить пользователю *bindguy* использовать команду «**sudo**» для автоматического перехода к пользователю root и SELinux-домену <**bindadm_t**>, добавим в **/etc/sudoers**:

```
echo "bindguy ALL=(ALL) ROLE=bindadm_r TYPE=bindadm_t ALL" » /etc/sudoers
```

При входе пользователя bindguy в систему он оказывается в пользовательском домене <**bindguy_t**>, основанном на домене <**staff_t**>. Домен <**bindguy_t**> может осуществлять переход в домен <**bindadm_t**>, используемый с правами root и позволяющий управлять службой Bind.

Например, выполнив следующую команду, пользователь bindguy сможет перезапустить службу bind:

```
service named restart
```

Также пользователю *bindguy* разрешается редактировать различные конфигурационные файлы и файлы информационного наполнения Bind. При этом, например, пользователь *bindguy* не имеет прав изменить пароль пользователя root.

Подведём итог. Процессы и файлы маркируются метками - контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально). Когда SELinux включён, вся эта информация используется для принятия решения о предоставлении доступа.

В контексте SELinux используется следующий синтаксис SELinux:

```
<user>:<role>:<type>:<level>:<пользователь_SELinux>
```

<**Пользователь_SELinux**> - это сущность, определённая в политике, которая отвечает за определённый набор ролей и за определённый набор MLS-уровней. Каждый пользователь ОС сопоставлен пользователю SELinux посредством политики SELinux. Это позволяет пользователям наследовать ограничения, установленные на пользователей SELinux. Сопоставленные сущности пользователей SELinux используются в контексте SELinux для процессов в сессии, в порядке определения, для каких ролей и уровней они применимы.

Роль - это часть модели безопасности Ролевого управления доступом **Role-Based Access Control** (RBAC). Роль - это атрибут RBAC. Пользователи SELinux авторитетны для ролей, а роль авторитетна для доменов. Каждая конкретная роль определяет, какие домены могут быть доступны для пользователей с этой ролью. Роль служит промежуточным звеном между доменами и пользователями SELinux. Роль, которой обладает пользователь, определяет, в какие домены может попасть пользователь - фактически, этот механизм управляет доступностью объектов. Таким образом, уменьшается риск, связанный с уязвимостью повышения привилегий в системе. По умолчанию пользователям назначена неопределённая роль, не накладывающая ограничений на пользователя. Но есть и предопределённые роли пользователя и администратора системы, которые могут быть назначены администратором для повышения безопасности системы.

Тип - это атрибут *Type Enforcement*. Тип определяет домен для процессов и тип для файлов. Правила политики SELinux определяют, как типы взаимодействуют друг с другом, является ли тип доменом, получающим доступ к типу, или доменом, получающим доступ к другому домену. Доступ разрешается, только если существует определённое правило политики SELinux, позволяющее данное действие.

Контекст безопасности записывается в атрибуты файла (в файловой системе) и создаётся при установке SELinux (операция **labeling**). Уже присвоенный контекст безопасности может быть впоследствии изменён - операцией «**transition**».

Пароли пользователей

/etc/passwd — файл, содержащий в текстовом формате список пользовательских учётных записей (аккаунтов).

Является первым и основным источником информации о правах пользователя операционной системы. Существует в большинстве версий и вариантов UNIX-систем. Обязан присутствовать в POSIX-совместимой операционной системе.

Принцип:

```
login : password : UID : GID : GECOS : home : shell
```

Каждая строка файла описывает одного пользователя и содержит семь полей, разделённых двоеточиями:

- регистрационное имя или логин;
- хеш пароля;
- идентификатор пользователя;
- идентификатор группы по умолчанию;
- информационное поле GECOS;
- начальный (он же домашний) каталог;
- регистрационная оболочка, или shell.

Вы можете подробнее ознакомиться с информацией о файле **/etc/passwd**, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Основным назначением **/etc/passwd** является сопоставление логина и идентификатора пользователя (UID). Изначально поле пароля содержало хеш пароля и использовалось для аутентификации. Однако, в связи с ростом вычислительных мощностей процессоров появилась серьёзная угроза применения простого перебора для взлома пароля. Поэтому все пароли были перенесены в специальные файлы, такие как **/etc/shadow**. Эти файлы недоступны для чтения обычным пользователям. Такой подход называется механизмом скрытых паролей.

Регистрационные имена должны быть уникальными и представлять собой строки не длиннее 32 символов (любые, кроме двоеточия и символа новой строки). По сути, имя пользователя — это его короткий и легко запоминаемый псевдоним, который используется при входе в систему и часто включается в адреса электронной почты.

Идентификатор пользователя — это число от 0 до 2^{32}-1. Пользователь с идентификатором «0» (обычно *root*) называется суперпользователем и имеет право на выполнение любых операций в системе. Принято соглашение о выделении «специальным» пользователям (*bin, daemon*), назначение которых — только запуск определённых программ, маленьких идентификаторов (меньше 100 или, в некоторых дистрибутивах Linux, меньше 500).

В UNIX пользователь может принадлежать к одной или нескольким группам, которые используются для задания прав более чем одного пользователя на тот или иной файл. Максимальное количество групп, в которых может состоять один пользователь, разное в разных вариантах системы.

Список групп с их участниками задаётся в **/etc/group**. В файле же **/etc/passwd** указывается идентификатор группы по умолчанию.

Всем файлам, созданным пользователем после регистрации в системе, будет автоматически присвоен этот номер группы (исключение — если для каталога, в котором создаётся файл, установлен в правах бит SGID, то будет присвоена такая же группа, как у самого каталога).

/etc/group содержит записи обо всех группах в системе. Каждая его строка содержит:

- символьное имя группы;
- пароль группы — устаревшее поле, сейчас не используется. В нём обычно стоит «x»;
- идентификатор группы, или GID;
- список имён участников, разделённых запятыми.

Пример записи:

```
bin:x:1:root,bin,daemon
```

Здесь сообщается, что группа *bin* имеет *GID=1*, а входят в неё пользователи *root, bin и daemon*.

GECOS

Поле GECOS хранит вспомогательную информацию о пользователе (номер телефона, адрес, полное имя и так далее). Оно не имеет чётко определённого синтаксиса.

Тем не менее, демон **fingerd** предполагает, что в нём содержатся следующие элементы, разделённые запятыми:

- полное имя;
- адрес офиса или домашний адрес;
- рабочий телефон;
- домашний телефон.

С помощью утилиты **chfn** можно изменять эту информацию, а с помощью **finger** — узнать, например, полное имя любого пользователя в системе (или даже на другом компьютере сети).

Пример строки с заполненным полем GECOS:

```
tester:x:210:8:Edward Chernenko,Marx Street 10,4554391,5454221:/home/ed:/bin/bash
```

После входа в систему пользователь оказывается в своём домашнем каталоге. Исторически сложилось так, что домашний каталог пользователя *root* называется **/root**, а остальные имеют вид **/home/**. Но могут применяться и другие схемы.

Если на момент входа в систему домашний каталог отсутствует, то система выдаёт сообщение об ошибке и отказывается допустить пользователя к командной строке. Такое поведение НЕ характерно для GNU/Linux; в большинстве дистрибутивов этой ОС просто выводится предупреждение, после чего пользователь попадает в каталог «/». Это можно изменить посредством установки параметра **DEFAULT_HOME** в файле **/etc/login.defs** в значение «**no**».

Следует отметить, что при использовании графического интерфейса (KDE, GNOME) пользователь не увидит предупреждения или сообщения об ошибке, но просто будет выведен из системы безо всяких объяснений (так как оконный менеджер не сможет выполнить запись в нужный каталог, такой как **~/.gnome**).

В поле регистрационной оболочки задаётся **shell**, то есть интерпретатор командной строки. Здесь может быть указана любая программа, и пользователь может сам выбирать для себя наиболее подходящую при помощи команды **chsh**. Тем не менее, некоторые системы в целях безопасности требуют, чтобы суперпользователь явно разрешил использовать приложение в качестве интерпретатора командной строки. Для этого используется специальный файл **/etc/shells**, содержащий список «допустимых» оболочек.

vipw - запускает текстовый редактор, указанный в переменной среды *EDITOR* (или редактор по умолчанию, обычно *vi*), загружая в него копию файла **/etc/passwd**. После закрытия редактора переносит временную копию в сам файл. Не позволяет двум пользователям выполнять редактирование одновременно.

В файле **/etc/shadow** хранятся хеши паролей всех пользователей в системе. Процессы суперпользователя могут читать его напрямую, а для остальных создана специальная библиотека PAM. Она позволяет непривилегированным приложениям спрашивать у неё, правильный ли пароль ввёл пользователь, и получать ответ. Библиотека PAM как правило действует с привилегиями вызвавшего процесса. Таким образом, хеш не попадает «в чужие руки».

В ранних UNIX пароль шифровался с помощью одного из вариантов DES, теперь используется MD5-хеширование или blowfish-хеширование (bcrypt). MD5-хеши всегда записываются после префикса «**1**».

Перед хешированием к паролю добавляются случайные символы — «*salt*» (соль, от англ. add salt to something — сделать что-либо более интересным; в русскоязычных источниках иногда используется термин «затравка»). *Salt* также приписывается к началу полученного хеша. Благодаря *salt* нельзя при простом просмотре файла обнаружить пользователей с одинаковыми паролями.

Кроме имени (первое поле каждой строки) и хеша (второе поле) в файле **/etc/shadow** также хранятся:

- дата последнего изменения пароля;
- через сколько дней можно будет поменять пароль;
- через сколько дней пароль устареет;
- за сколько дней до того, как пароль устареет, начать напоминать о необходимости смены пароля;
- через сколько дней после того, как пароль устареет, заблокировать учётную запись пользователя;
- дата, при достижении которой учётная запись блокируется;
- зарезервированное поле.

Даты обозначаются как число дней с *1 января 1970 года* (начало эпохи UNIX).

Обязательная регулярная смена паролей — это популярная административная мера, призванная сделать учётные записи более защищёнными. К сожалению, многие пользователи после принудительного изменения возвращают себе старый пароль.

Утилита passwd

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия ПО:** passwd 0.80-9

Утилита **passwd** поддерживает традиционные опции *passwd* и утилит *shadow*.

Синтаксис:

```
passwd
```

Вы можете подробнее ознакомиться с информацией о работе с утилитой **passwd**, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Возможные опции:

Опция	Значение опции
-d,- -delete	Удалить пароль для указанной записи.
-f,- -force	Форсировать операцию.
-k,- -keep-tokens	Сохранить не устаревшие пароли.
-l,- -lock	Блокировать указанную запись.
--stdin	Прочитать новые пароли из стандартного ввода.
-S,- -status	Дать отчет о статусе пароля в указанной записи.
-u,- -unlock	Разблокировать указанную запись.
-?,- -help	Показать справку и выйти.
--usage	Дать короткую справку по использованию.
-V,- -version	Показать версию программы и выйти.

Код выхода:

При успешном завершении **passwd** заканчивает работу с кодом выхода **0**. Код выхода **1** означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Примеры:

Удаление пароля пользователя:

```
passwd -d <имя_пользователя>
```

Добавление пароля из стандартного ввода:

```
passwd --stdin <имя_пользователя>
```

Блокировка пароля:

```
passwd -l <имя_пользователя>
```

Разблокировать пароль:

```
passwd -u <имя_пользователя>
```

Создать новый пароль:

```
passwd <имя_пользователя>
```

Добавление нового пользователя

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для добавления нового пользователя используйте команды **useradd** и **passwd**.

Вы можете подробнее ознакомиться с информацией по добавлению новых пользователей, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

В примере в качестве первоначально введенного пароля указана последовательность символов «*123*», затем введен надежный пароль:

```
useradd test1
passwd test1

Изменение пароля пользователя test1.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

В результате описанных действий в системе появился пользователь *test1* с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды **passwd** - но если он попытается поставить слабый пароль, система откажет ему (в отличие от **root**) в изменении.

В дистрибутивах ОС для проверки паролей на слабость используется модуль PAM **passwdqc**.

Программа **useradd** имеет множество параметров, которые позволяют менять ее поведение по умолчанию. Например, можно принудительно указать, какой будет **UID** или какой группе будет принадлежать пользователь.

Синтаксис:

```
useradd [-u <идентификатор> [-o] [-i]] [-g <группа>] [-G <группа>[[,<группа>] . . .]] [-d <каталог>] [-s <shell>] [-c <комментарий>] [-m [-k <skel_dir>]] [-f <inactive>] [-e <expire>] [-p <passgen>] [-a <событие>[, . . .]] <рег_имя>
```

Опции:

Опция	Значение опции
-u <идентификатор>	Идентификационный номер пользователя (**UID**). Этот номер должен быть неотрицательным целым числом, не превосходящим **MAXUID**, определенным в **sys/param.h**. По умолчанию используется следующий доступный (уникальный) не устаревший **UID**, больший 99. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (**NIS**).
-o	Опция позволяет дублировать **UID** (сделать его не уникальным). Поскольку защита системы в целом, а также целостность контрольного журнала (**audit trail**) и учетной информации (**accounting information**) в частности, зависит от однозначного соответствия каждого **UID** определенному лицу, использовать эту опцию не рекомендуется (чтобы обеспечить учет действий пользователей). Опция действительна только с использованием опции -u.
-g <группа>	Имя или числовой идентификатор первичной группы пользователя. Группа с таким именем должна существовать. Опция задает основную группу (**primary group**) для нового пользователя. По умолчанию используется стандартная группа, указанная в файле **/etc/default/useradd**. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (**NIS**).
-G <группа>[[,<группа>] . . .]	Список дополнительных групп, членом которых также является пользователь. Каждая группа отделяется от следующей запятой без пробелов. На группы распространяются те же ограничения, что и на группу, указанную с параметром -g. По умолчанию пользователь принадлежит только к начальной группе. Опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (**NIS**).
-d <каталог>	Начальный каталог (**home directory**) нового пользователя. Длина этого поля не должна превышать 256 символов. По умолчанию используется **HOMEDIR/a**, где **HOMEDIR** - базовый каталог для начальных каталогов новых пользователей, **a** - регистрационное имя нового пользователя.
-s <shell>	Полный путь к программе, используемой в качестве начального командного интерпретатора для пользователя сразу после регистрации. Длина этого поля не должна превышать 256 символов. По умолчанию это поле - пустое, что заставляет систему использовать стандартный командный интерпретатор **/usr/bin/sh**. В качестве значения **shell** должен быть указан существующий выполняемый файл.

Опция	Значение опции
-c <комментарий>	Любая текстовая строка. Обычно, здесь коротко описывается учётная запись, и в настоящее время используется как поле для имени и фамилии пользователя. Информация хранится в записи пользователя в файле **/etc/passwd**. Длина этого поля не должна превышать 128 символов.
-m	Создает начальный каталог нового пользователя, если он еще не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу.
-k <skel_dir>	Основной каталог, содержащий файлы и каталоги, которые будут скопированы в домашнюю директорию пользователя, когда домашняя директория создается с помощью **useradd**. Этот параметр действителен только в том случае, если задан параметр -m (или --create-home). Если этот параметр не задан, основной каталог определяется переменной SKEL в **/etc/default/useradd** или, по умолчанию, **/etc/skel**.
-f <inactive>	Срок действия учетной записи. Если значение равно 0, учетная запись блокируется сразу после того, как пароль устареет, а если значение равно -1, то эта функция не используется. Если значение не указано, **useradd** будет использовать срок действия по умолчанию, указанный переменной INACTIVE в файле **/etc/default/useradd**, или -1 по умолчанию.
-e <expire>	Дата, с которой учетная запись пользователя будет отключена. Дата указывается в формате **ГГГГ-ММ-ДД**. Если значение не указано, **useradd** будет использовать дату истечения срока действия по умолчанию, указанную переменной EXPIRE в файле **/etc/default/useradd**, или пустую строку (без истечения срока действия) по умолчанию.
<рег_имя>	Строка печатных символов, задающая регистрационное имя для нового пользователя. В ней не должно быть двоеточий (:) и символов перевода строки (\n). Она также не должна начинаться с прописной буквы.

Редактирование имеющихся пользовательских записей

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для модификации уже имеющихся пользовательских записей применяется утилита **usermod**:

```
usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь *test1* - теперь это audio, rpm, test1.

```
usermod -l test2 test1
```

Будет произведена смена имени пользователя с *test1* на *test2*.

Вы можете подробнее ознакомиться с информацией по изменению имеющихся пользовательских записей, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Команды **usermod -L test2** и **usermod -U test2** соответственно временно блокируют возможность входа в систему пользователю *test2* и возвращают все на свои места.

> **Примечание.**
>
> Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используйте утилиту **chpasswd**. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как **<имя>:<пароль>**.

Удаление пользователей

Удаление локальных пользователей
Удаление доменных пользователей

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Удаление локальных пользователей

Для удаления локальных пользователей используется утилита **userdel**. Например:

```
userdel test2
```

Данная команда удалит пользователя **test2** из системы. Если будет дополнительно задан параметр **-r**, будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

Вы можете подробнее ознакомиться с информацией по удалению пользователей из системы, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Утилиты **vigr** и **vipw** используются для ручного редактирования файлов **/etc/passwd** и **/etc/group**, в которых хранятся основные записи о пользователях и группах в системе.

Не рекомендуется создавать пользователей с правами сверх необходимых. Предпочтительнее создать серию новых групп и включить в них требуемого пользователя. А для данных групп установить соответствующие права на объектах файловой системы (утилиты **chmod** и **chown**).

Удаление доменных пользователей

Для удаления доменного пользователя из системы необходимо:

1. Удалить домашний каталог доменного пользователя:

```
rm -rf /home/<имя_пользователя>
```

2. Удалить его учетную запись с экрана входа в систему:

```
rm /var/lib/AccountsService/users/<имя_пользователя>
```

Управление пользователями и группами из консоли

Просмотреть всех локальных пользователей:

```
cat /etc/passwd
```

Просмотреть все локальные группы:

```
cat /etc/group
```

Посмотреть группы, в которых состоит пользователь.

Формат вывода: `<основная_группа> : <группы>`

```
groups user
```

Для добавления нового пользователя используйте команды `useradd` и `passwd`. В примере в качестве первоначально введенного пароля указана последовательность символов «123», затем введен надежный пароль:

```
useradd test1
passwd test1

Смена пароля для пользователя test1
Новый пароль:
Повторите ввод нового пароля:
passwd: все токены проверки подлинности успешно обновлены.
```

Добавить пользователя в группу:

```
usermod <опции> <имя_пользователя>
```

Опции:

- **-G** - дополнительные группы, в которые нужно добавить пользователя;
- **-g** - изменить основную группу для пользователя;

```
usermod -a -G <имя_группы> <имя_пользователя>
```

Для смены имени пользователя с *test1* на *test2*.

```
usermod -l test2 test1
```

Чтобы включить пользователя в группу, для основной группы используется опция *-g*:

```
sudo usermod -g test sergiy
```

Удалить пользователя из группы можно той же командой с опцией *-G*, перечислив список групп, куда пользователь должен входить (через запятую и без пробелов):

```
sudo usermod -G <группа_1>,<группа_2>,<группа_3> <пользователь>
```

После выполнения данной команды пользователь будет входить только в указанные группы, а из остальных будет удален.

Для удаления пользователей используйте **userdel**.

```
userdel test2
```

Для удаления группы выполните:

```
groupdel user
```

Управление пользователями с помощью графической утилиты system-config-users

Установка
Обзор программы
Добавление нового пользователя
Свойства пользователя
Добавление новой группы
Свойства группы
Фильтры
Сортировка
Системные пользователи и группы
Удаление пользователей
Удаление групп

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: system-config-users-1.3.8-8

system-config-users — графическая утилита для управления пользователями в РЕД ОС. Утилита предоставляет различные функции администрирования пользователей, включая создание, удаление и изменение учетных записей пользователей, управление паролями, настройку прав доступа, а также администрирование групп пользователей.

Вы можете подробнее ознакомиться с работой утилиты **system-config-users**, просмотрев наши обучающие видео:

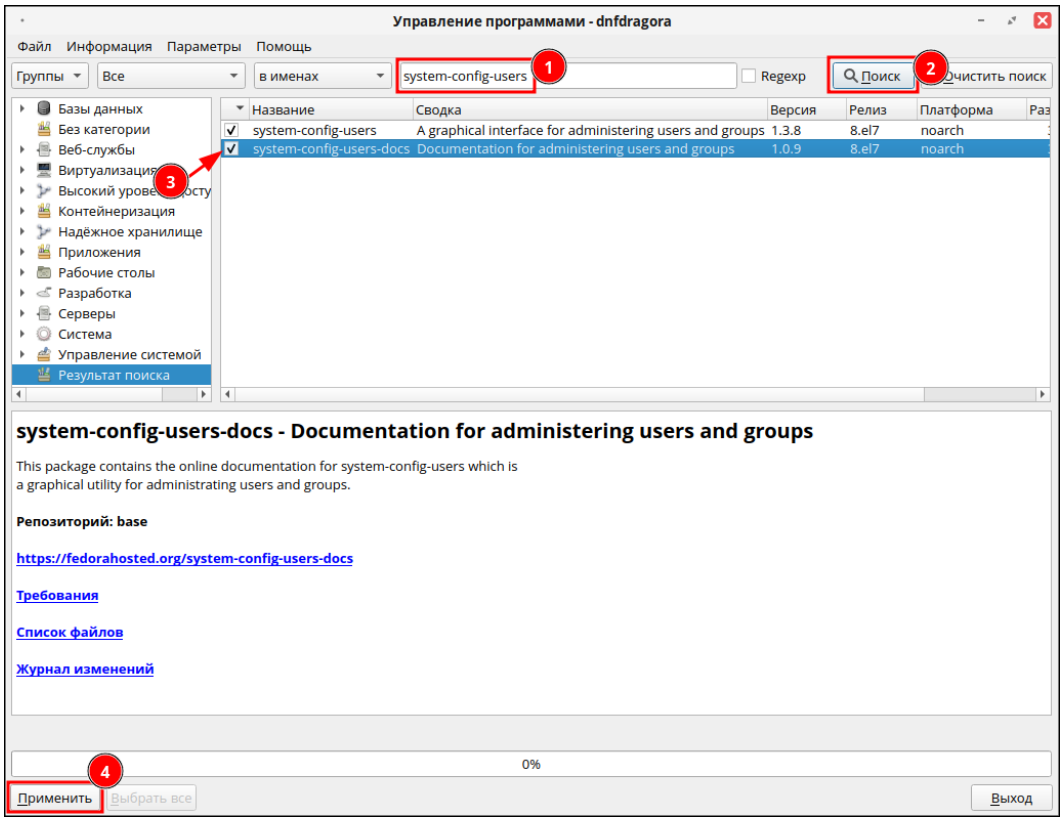
- на **RuTube** — Графическое управление пользователями в РЕД ОС 7.3;
- в **Яндекс.Дзен** — Графическое управление пользователями в РЕД ОС 7.3;
- в **VK Видео** — Графическое управление пользователями в РЕД ОС 7.3 .

На наших каналах вы также сможете найти много другой полезной информации.

Установка

По умолчанию утилита предустановлена в РЕД ОС 7.3, однако если по каким-либо причинам утилита отсутствует в вашей системе, установить ее можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**system-config-users**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс **пользователя root**:

```
su -
```

и выполните команду:

```
dnf install system-config-users
```

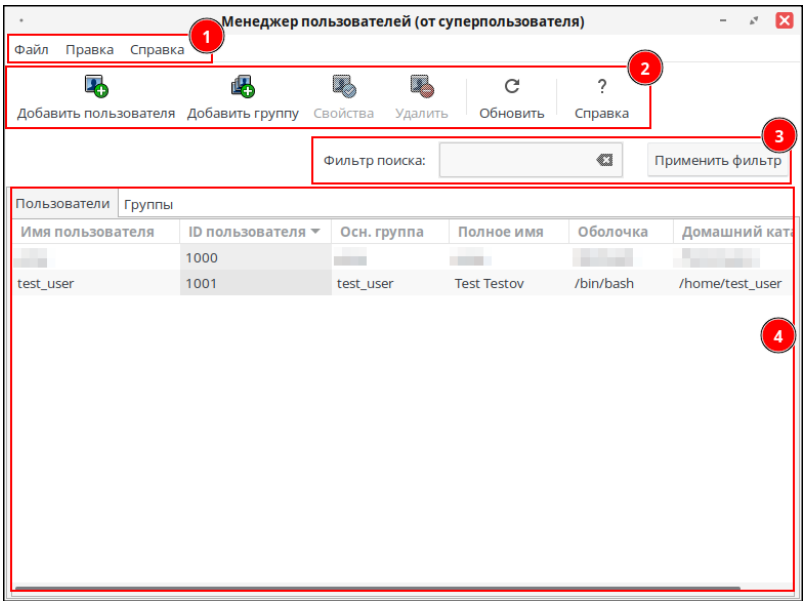
Дальнейшая работа в программе выполняется с правами **администратора** системы или **суперпользователя root**.

После установки программа доступна из «**Главного меню**» — «**Администрирование**» — «**Управление пользователями**» или через терминал с помощью команды:

```
system-config-users
```

Обзор программы

Главное окно программы выглядит следующим образом:



1. *Основное меню программы* – содержит все доступные действия для работы в программе.

2. *Панель инструментов* – содержит главные операции для работы, такие как создание пользователя, создание группы, свойства, удаление, обновление списков и вывод справки.

3. *Фильтр поиска* – для быстрого поиска пользователей или групп.

4. Непосредственно *список пользователей и групп*. В окне программы доступно 2 вкладки:

- вкладка «**Пользователи**» – для управления пользователями (открыта по умолчанию);
- вкладка «**Группы**» – для управления группами.

Для просмотра списка локальных пользователей системы перейдите на вкладку **Пользователи**. Для просмотра локальных групп системы перейдите на вкладку **Группы**.

Добавление нового пользователя

Для добавления нового пользователя нажмите «**Добавить пользователя**». В открывшемся окне введите имя пользователя (логин) и полное имя нового пользователя (ФИО) в соответствующие поля. Задайте пароль пользователя в поле «**Пароль**» и повторите заданный пароль в поле «**Повторите пароль**» с целью избежания ошибок и опечаток. Пароль должен содержать ***не менее 6 символов***.

Примечание.

В целях безопасности учетной записи рекомендуется использовать сложный и длинный пароль.

Не рекомендуется использовать пароли, основанные на простых словах и последовательностях. Используйте комбинации различных букв, цифр и специальных символов.

Выберите оболочку. Если вы не уверены, какая оболочка нужна, оставьте значение по умолчанию – **/bin/bash**.

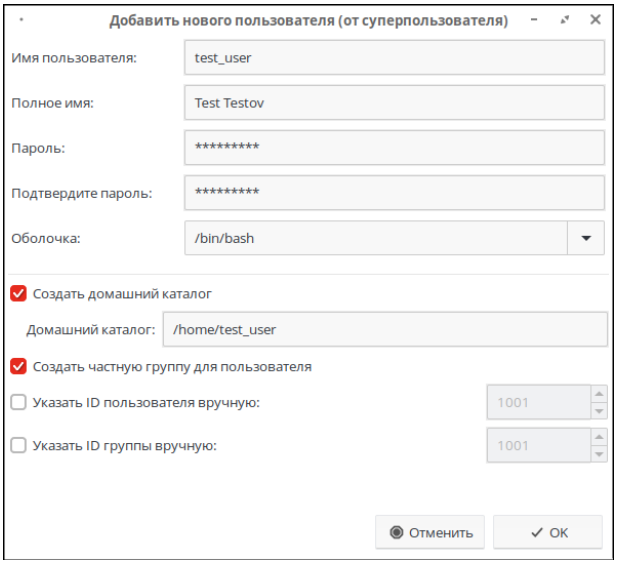
Домашний каталог пользователя по умолчанию будет расположен в **/home/<username>/**. Можно изменить домашний каталог или не создавать его, сняв флаг с параметра «**Создать домашний каталог**».

Если создание домашнего каталога было подтверждено, по умолчанию в него будут скопированы конфигурационные файлы из каталога **/etc/skel/**.

По умолчанию также используется схема *user private group (UPG)* – создание частной группы пользователя. Это означает, что каждый раз при создании нового пользователя, создаётся новая группа с таким же именем. Если такую группу создавать не требуется, снимите флаг с поля «**Создать частную группу для пользователя**».

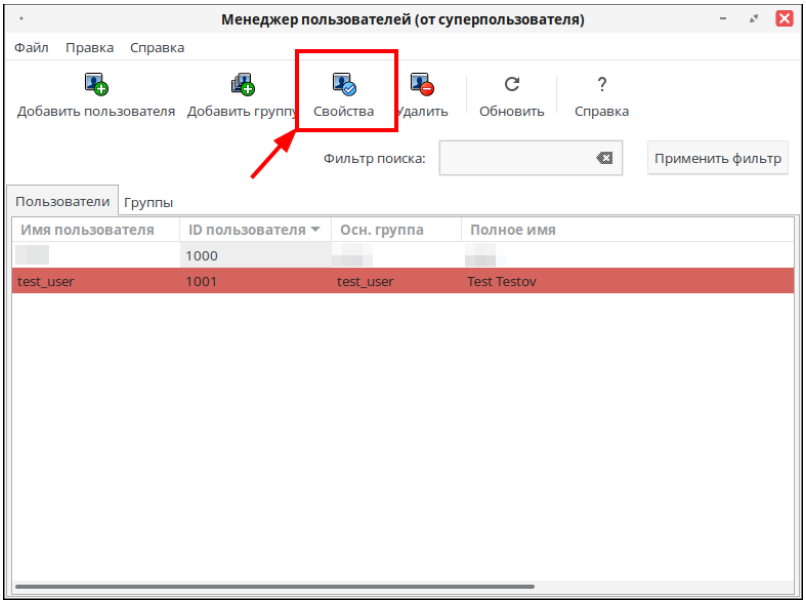
Чтобы указать специальное значение **ID** для пользователя, активируйте пункт «**Указать ID пользователя вручную**». Если параметр не активен, для пользователя будет установлен следующий доступный пользовательский **ID** со значением **выше 500**. Пользовательские **ID** со значением ***ниже 500*** зарезервированы ***для системных пользователей***, поэтому не рекомендуется вручную присваивать значения ID от 1 до 499.

Нажмите «**OK**» для создания нового пользователя.



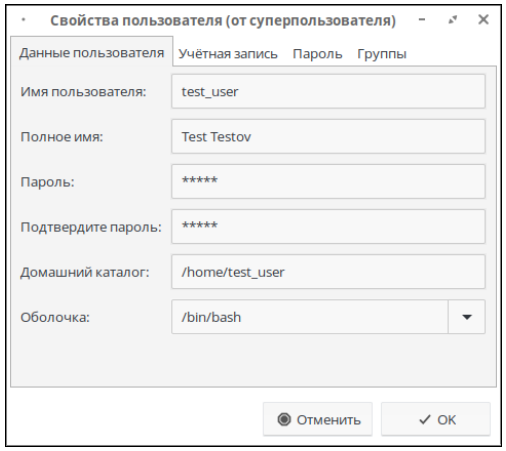
Свойства пользователя

Для просмотра свойств существующих пользователей на вкладке «**Пользователи**» выберите пользователя из списка и нажмите кнопку «**Свойства**» в основном меню или выберите пункт меню « **Файл**» – «**Свойства**». Будет открыто окно «**Свойства пользователя**».

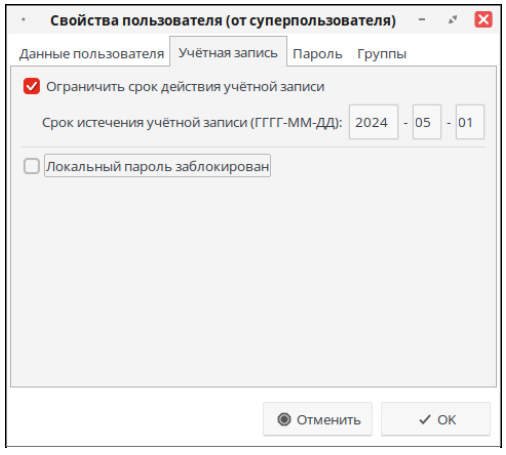


Окно «**Свойства пользователя**» содержит несколько вкладок:

- вкладка «**Данные пользователя**» – показывает основную информацию о настройках пользователя, указанную при его добавлении. Может быть использована для смены полного имени пользователя, пароля, домашнего каталога или системной оболочки.

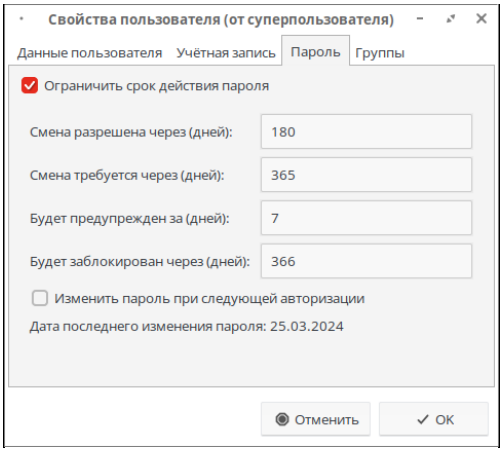


- вкладка «**Учетная запись**» — позволяет настроить доступ пользователя к системе. Для ограничения срока действия учетной записи активируйте соответствующее поле и введите срок истечения учетной записи. Для блокировки учётной записи пользователя и запрета входа пользователя в систему активируйте параметр «**Локальный пароль заблокирован**».

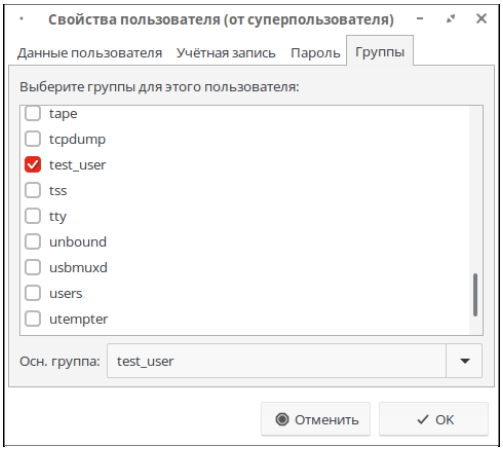


- вкладка «**Пароль**» – отображает дату последнего изменения пароля. Для принудительной смены пароля можно ограничить срок действия пароля, активировав соответствующий параметр и указав необходимые значения в поле «**Смена разрешена через**

(дней)». Для указания количества дней ДО истечения срока действия пароля впишите значение в поле «**Смена требуется через (дней)**». Дополнительно можно задать напоминание пользователю о смене пароля, указав значение в поле «**Будет предупрежден за (дней)**», а также количество дней, по истечении которых пароль будет заблокирован. Также в целях безопасности можно запросить смену выданного пользователю пароля при следующей его авторизации в системе, активировав параметр «**Изменить пароль при следующей авторизации**».

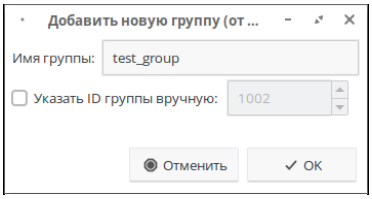


- на вкладке «**Группы**» можно просмотреть и настроить основную группу пользователя и другие группы, в состав которых должен входить указанный пользователь.



Добавление новой группы

Для добавления новой группы нажмите «**Добавить группу**». Будет открыто окно «**Новая группа**». Введите имя новой группы.

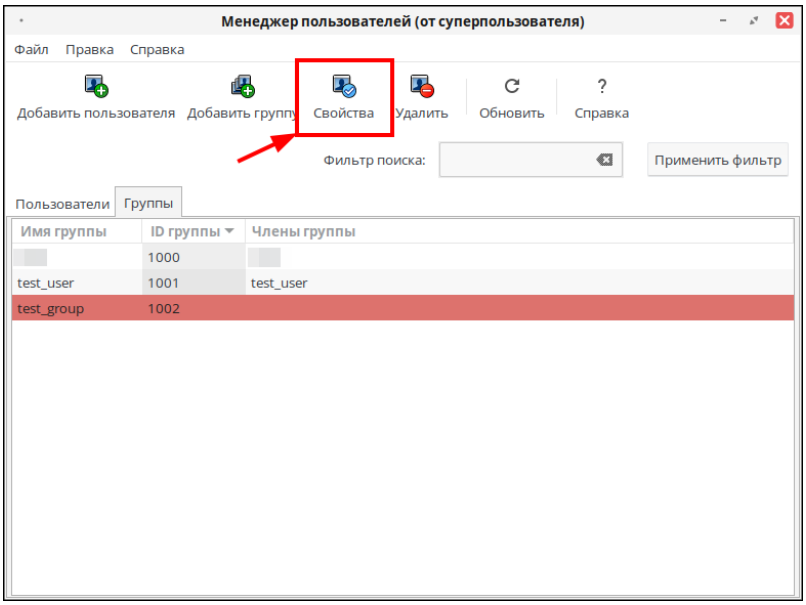


Для указания собственного **ID** новой группы, активируйте параметр «**Указать ID группы вручную**» и выберите **GID**. Обратите внимание, что номера **GID** со значениями ***менее 500*** зарезервированы ***для системных групп***.

Нажмите «**OK**» для создания группы. Новая группа будет добавлена в список групп.

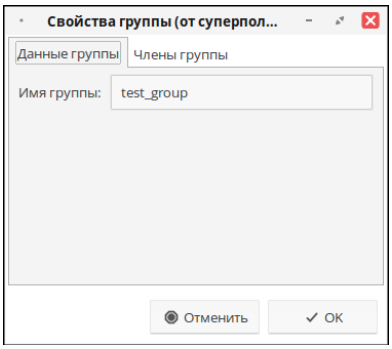
Свойства группы

Для просмотра свойств существующей группы выберите группу из списка и нажмите на панели инструментов «**Свойства**» или выберите пункт меню «**Файл**» — «**Свойства**».

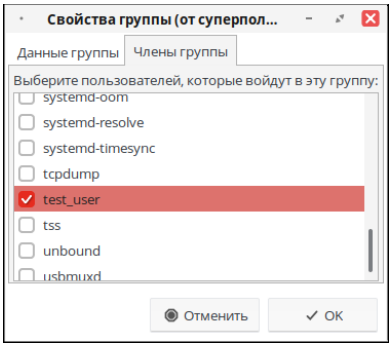


В свойствах группы доступны две вкладки:

- вкладка «**Данные группы**» — позволяет изменить имя группы;



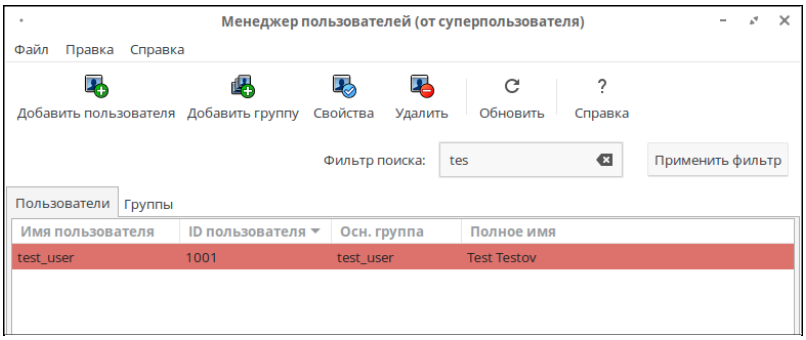
- вкладка «**Члены группы**» — отображает пользователей и членов выбранной группы. Здесь можно добавить или удалить пользователя из группы.



Нажмите «**OK**» для сохранения изменений.

Фильтры

Для поиска определённого пользователя или группы начните вводить первые символы имени в поле «**Фильтр поиска**». Нажмите *Enter* или «**Применить фильтр**» для вывода результата поиска.

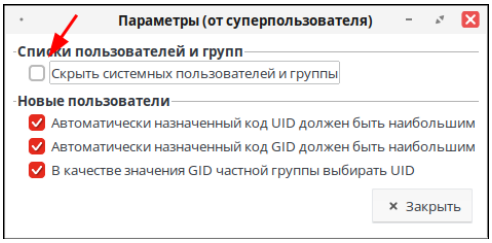


Сортировка

Для сортировки имён пользователей или групп щёлкните по заголовку столбца. Имена пользователей или групп будут упорядочены.

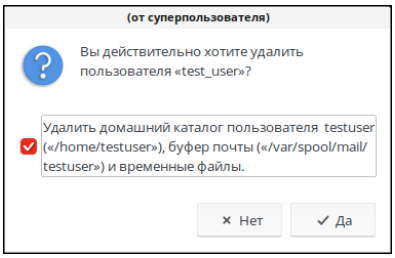
Системные пользователи и группы

Пользовательские **ID** со значением ***менее 500*** зарезервированы ***для системных пользователей***. По умолчанию *Менеджер пользователей* не отображает системных пользователей. Для отображения всех пользователей системы выберите пункт меню «**Правка**» – «**Параметры**» и в открывшемся окне снимите флаг с пункта «**Скрыть системных пользователей и группы**».



Удаление пользователей

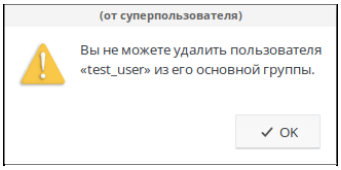
Для удаления пользователя выберите нужного пользователя из списка и нажмите «**Удалить**» или выберите пункт меню «**Файл**» – «**Удалить**». Для подтверждения удаления пользователя, а также удаления его домашнего каталога (при наличии), буфера почты и прочих временных файлов, нажмите «**Да**».



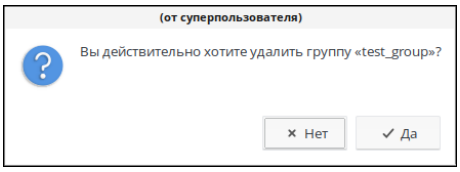
Удаление групп

Для удаления группы выберите нужную группу из списка и нажмите «**Удалить**» или выберите пункт меню «**Файл**» – «**Удалить**».

Если в группе находятся пользователи будет выведено информационное сообщение о невозможности удаления группы.



Если в группе нет ни одного пользователя, будет выведено окно запросом подтверждения удаления группы. Для подтверждения операции нажмите «**Да**».



Для подтверждения удаления пользователя, а также удаления его домашнего каталога (при наличии), буфера почты и прочих временных файлов, нажмите «**Да**».

Автоматическая авторизация пользователя (автовход)

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция

Для активации автоматического входа пользователя (автовход) в GDM без ввода пароля при загрузке ОС, необходимо в файл **/etc/gdm/custom.conf** в секцию **[daemon]** добавить 2 строки:

```
AutomaticLogin=<имя_пользователя>
 AutomaticLoginEnable=True
```

При использовании этой конфигурации, при завершении сеанса пользователя, произойдет обратный автоматический вход в текущего пользователя.

Чтобы иметь возможность переключиться в сеанс другого пользователя, приведите в файле **/etc/gdm/custom.conf** секцию **[daemon]** к виду:

```
[daemon]
 WaylandEnable=false
 TimedLoginEnable = true
 TimedLogin = <имя_пользователя>
 TimedLoginDelay = 10
```

здесь в параметре **TimedLoginDelay** указывается время (в секундах) ожидания до автоматического входа в пользователя.

За это время можно успеть войти в рабочий стол другого пользователя.

Создание и настройка собственного default-профиля пользователя при помощи SKEL

Настройка браузера по умолчанию для всех пользователей
Примеры создания default-профиля пользователя
Настройка ярлыков рабочего стола
Создание шаблонов документов
Установка плагинов в браузеры
Настройка профиля skel
Создание профиля Wine
Настройка профиля skel с wine

Для запуска домашнего каталога при первом создании пользователя в РЕД ОС используется каталог **/etc/skel/**. В нем можно задавать и хранить настройки новых пользователей, в частности для этого используется файл **.bashrc**. Доступ к файлу осуществляется с правами администратора.

Вы можете подробнее ознакомиться с возможностью создания эталонного пользователя, просмотрев наши обучающие видео:

- на **RuTube** — Создание универсального профиля пользователя;
- в **Яндекс.Дзен** — Создание универсального профиля пользователя;
- в **VK Видео** — Создание универсального профиля пользователя.

На наших каналах вы также сможете найти много другой полезной информации.

В файле **.bashrc** в секции «**# User specific aliases and functions**» необходимо прописать функции и настройки, которые будут применяться к каждому новому пользователю.

```
nano /etc/skel/.bashrc

# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
  . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]
then
PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions

alias cls=clear
alias diskspace='df -h'
alias data
```

После сохранения внесенных изменений можно создавать нового пользователя (создание новых пользователей осуществляется с правами суперпользователя) следующей командой:

```
adduser <имя_пользователя>
```

С помощью данной команды будет создан новый профиль пользователя, параметры для которого будут взяты из папки **/etc/skel/**.

Примечание.

Каталог **/skel** определен в файле **/etc/default/useradd**.

```
nano /etc/default/useradd

# useradd defaults file
GROUP=100
```

```
HOME=/home

INACTIVE=-1
EXPIRE=
SHELL=/bin/bash

SKEL=/etc/skel

CREATE_MAIL_SPOOL=yes
```

Местоположение **SKEL** по умолчанию можно установить любое, которое удобно. Также можно изменить и базовый домашний каталог **HOME** на любой другой.

Настройка браузера по умолчанию для всех пользователей

Добавьте в файл **/etc/skel/.bashrc** в секцию «**# User specific aliases and functions**» следующую команду (в зависимости от необходимого вам браузера):

Яндекс.Браузер:

```
if ! [ $(xdg-settings get default-web-browser | grep yandex) ]; then xdg-settings set default-web-browser yandex-browser-beta.desktop; fi
```

Opera:

```
if ! [ $(xdg-settings get default-web-browser | grep opera) ]; then xdg-settings set default-web-browser opera.desktop; fi
```

Vivaldi:

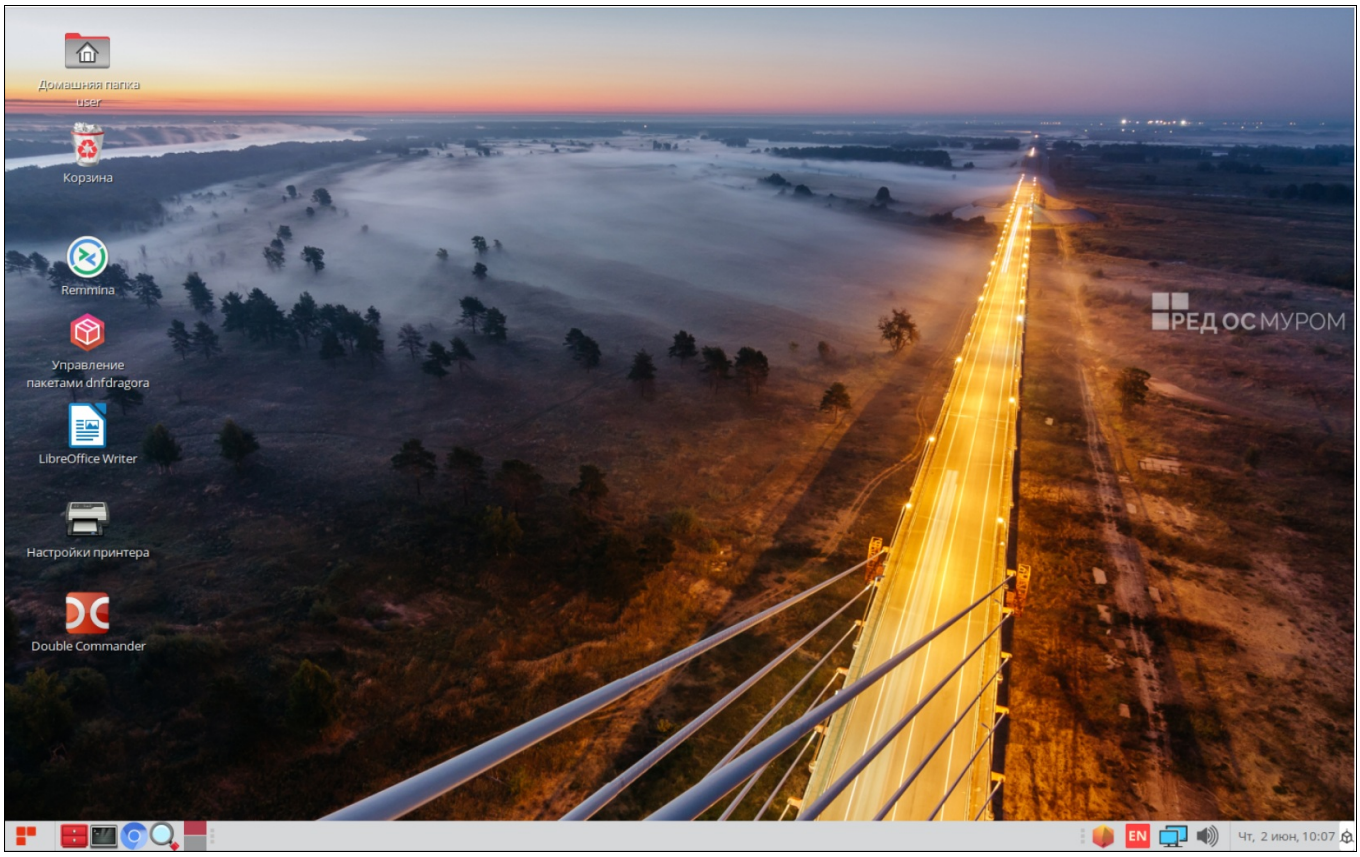
```
if ! [ $(xdg-settings get default-web-browser | grep vivaldi) ]; then xdg-settings set default-web-browser vivaldi-stable.desktop; fi
```

После сохранения внесенных изменений каждый новый созданный пользователь будет использовать указанный вами браузер, как браузер по умолчанию.

Примеры создания default-профиля пользователя

Настройка ярлыков рабочего стола

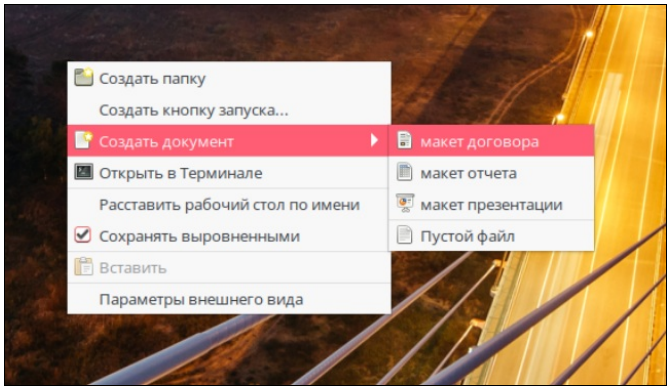
На **Рабочем столе** можно создать необходимые пользователям для работы ярлыки. Проще всего создать ярлыки через «**Главное меню**» – выбрать нужное приложение, нажать **ПКМ** – «**Переместить на Рабочий стол**».



Создание шаблонов документов

Можно создать шаблоны, например, макеты договоров, презентаций и отчетов. Для этого в офисном пакете необходимо создать и сохранить частично заполненные документы в папку **~/Шаблоны**.

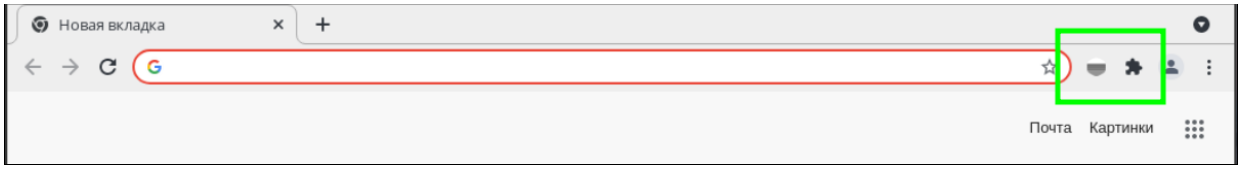
Проверьте, что созданные шаблоны доступны из контекстного меню при нажатии **ПКМ** по **Рабочему столу**.



Установка плагинов в браузеры

В качестве примера будет установлен плагин **Госуслуг**.

Установка стандартная, перейдите по ссылке и нажмите кнопку «**Установить**».



Настройка профиля skel

Необходимо создать файл, который будет служить для изменения старых путей пользователя на новые.

Примечание.

Обратите внимание на строку WHO="/home/user", вместо **/home/user** – пропишите путь до **вашего** домашнего каталога.

```
nano ~/.reconfigure_profile.sh
```

```
#!/bin/bash
WHO="/home/user"
NEW_NAME=$(whoami)
grep -rlE "$WHO" ~ > ~/.output_grep
while read line; do
sed -i "s|$WHO|/home/$NEW_NAME|g" "$line";
done < ~/.output_grep
rm -rf ~/.output_grep
```

Далее необходимо произвести синхронизацию необходимых каталогов домашнего пользователя с **/etc/skel**, для этого создайте скрипт:

```
nano ~/sync_path.sh
```

```
WHO="/home/user"
mkdir -p /etc/skel/.mozilla/ /etc/skel/.config/
cp -rfu $WHO/.{local,pki,redoswelcome}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/{Видео,Документы,Загрузки,Изображения,Музыка,Общедоступные,Рабочий\ стол,Шаблоны}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/.mozilla/{extensions,plugins}/ /etc/skel/.mozilla/ 2>/dev/null || :
cp -rfu $WHO/.config/{caja,caja-actions,chromium,dconf,mate,mate-session}/ /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.config/{monitors.xml,user-dirs.dirs} /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.{reconfigure_profile.sh,bash_logout,bash_profile,bashrc} /etc/skel/ 2>/dev/null || :
```

Запустите созданный скрипт (с правами администратора):

```
bash ./sync_path.sh
```

Отредактируйте файл **/etc/skel/.bashrc**, чтобы при первом входе нового пользователя произошел вызов вашего скрипта. В конец файла допишите:

```
if [ -f ~/.reconfigure_profile.sh ]; then
bash ~/.reconfigure_profile.sh
rm -rf ~/.reconfigure_profile.sh
fi
```

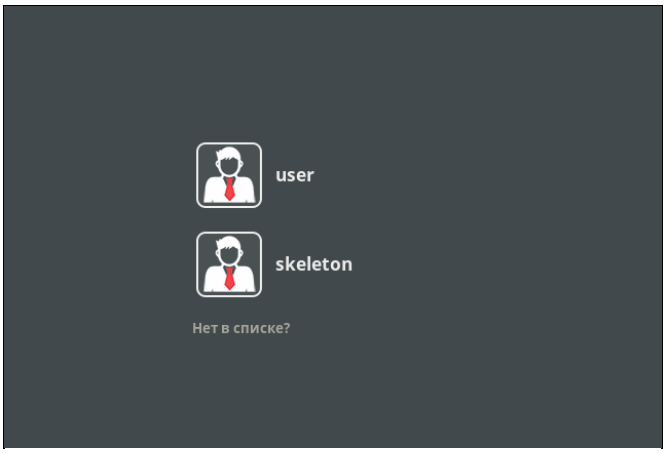
Примечание.

Чем больше будет размер **/etc/skel**, тем дольше будет происходить создание нового пользователя.

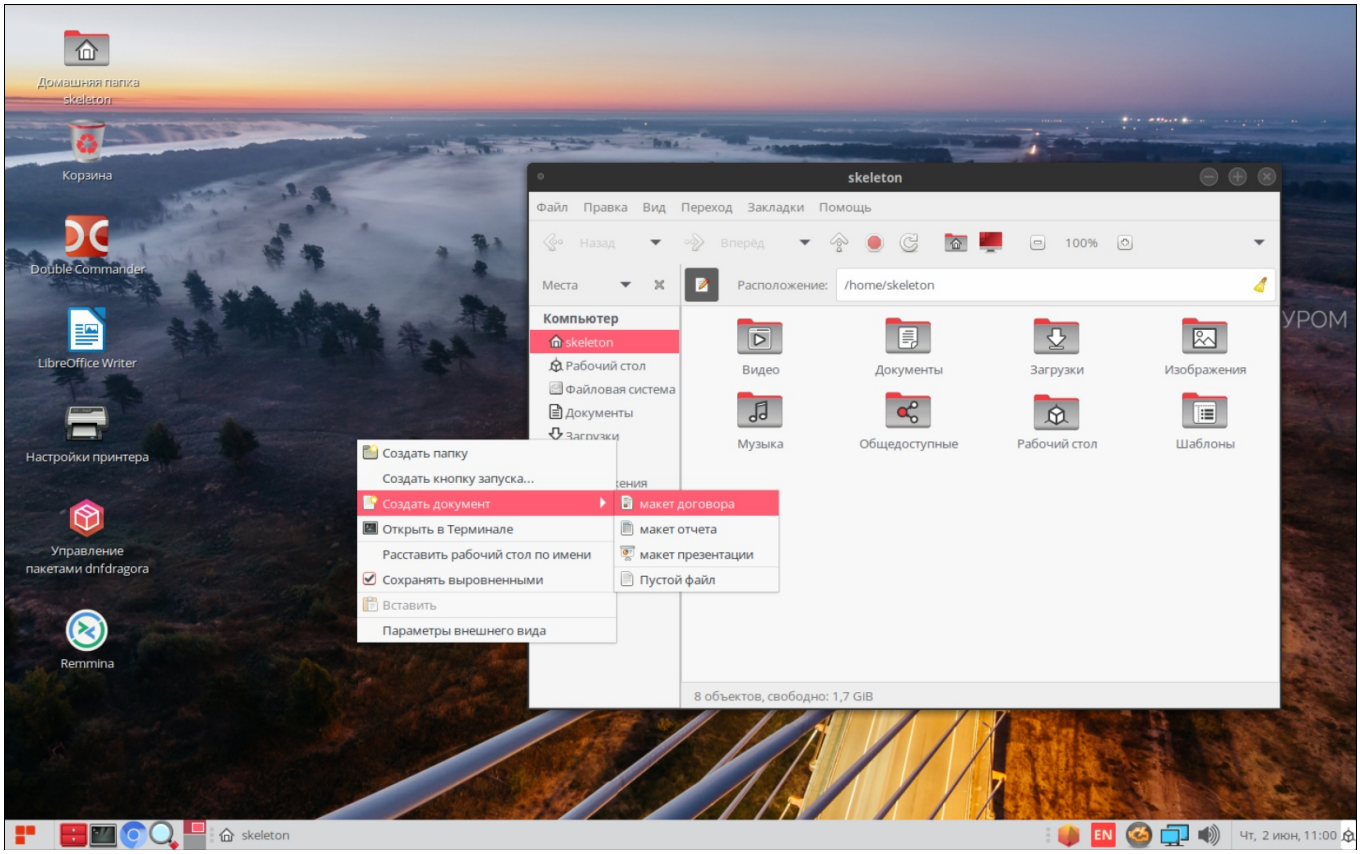
Для проверки работоспособности создайте нового пользователя:

```
useradd skeleton
passwd skeleton
```

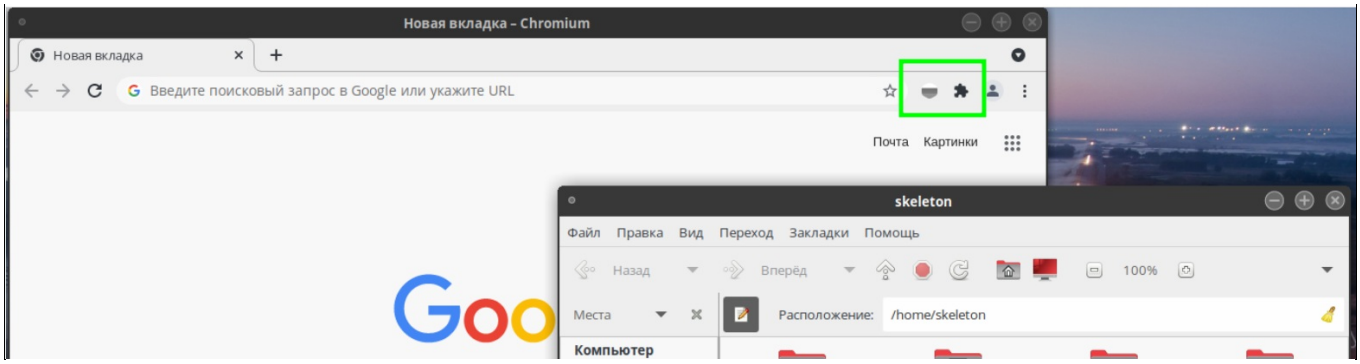
Выйдите из текущей сессии и авторизуйтесь под учетной записью нового пользователя.



Рабочий стол и **Домашняя папка** успешно созданы.



Проверьте браузер на наличие плагина Госуслуг:



Создание профиля Wine

В данном примере будет произведена базовая инициализация wine на примере notepad.

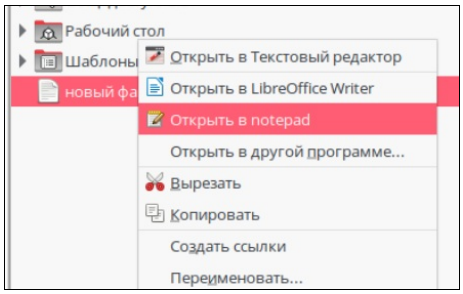
Перейдите в сеанс пользователя root:

```
su -
```

и установите wine и winetricks командой:

```
dnf install wine winetricks
```

После установки в **Главном меню** появится раздел **Wine**, который включает в себя несколько программ, в том числе **notepad**.



Настройка профиля skel с wine

Необходимо создать файл, который будет служить для изменения старых путей пользователя на новые.

> **Примечание.**
>
> Обратите внимание на строку WHO="/home/user", вместо **/home/user** – пропишите путь до **вашего** домашнего каталога.

```
nano ~/.reconfigure_profile.sh
```

```
#!/bin/bash
WHO="/home/user"
NEW_NAME=$(whoami)
grep -rlE "$WHO" ~ > ~/.output_grep
while read line; do
sed -i "s|$WHO|/home/$NEW_NAME|g" "$line";
done < ~/.output_grep
rm -rf ~/.output_grep

NAME=$(sed -e 's|\"||g' <<< $(sed -e 's|.*\"USERNAME\"\=\"||g' <<< $(grep -rnE '"USERNAME"="' ~/.wine)))
grep -rlE '\\{2}'$NAME'\\{2}' ~/.wine | xargs sed -i 's|\\\\'$NAME'\\\\|\\\\'$NEW_NAME'\\\\|g'
grep -rlE '\\{2}'$NAME'\"' ~/.wine | xargs sed -i 's|\\\\'$NAME'\"|\\\\'$NEW_NAME'\"|g'
grep -rlE '"="'$NAME'"' ~/.wine | xargs sed -i 's|\"\=\"'$NAME'\"|\"\=\"'$NEW_NAME'\"|g'
mv ~/.wine/drive_c/users/$NAME ~/.wine/drive_c/users/$NEW_NAME
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Desktop ~/Рабочий\ стол
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Documents ~/Документы
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Downloads ~/Загрузки
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Music ~/Музыка
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Pictures ~/Изображения
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Videos ~/Видео
```

Далее необходимо произвести синхронизацию необходимых каталогов домашнего пользователя с **/etc/skel**, для этого создайте скрипт:

```
nano ~/sync_path.sh
```

```
WHO="/home/user"
mkdir -p /etc/skel/.mozilla/ /etc/skel/.config/
cp -rfu $WHO/.{local,pki,redoswelcome,wine}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/{Видео,Документы,Загрузки,Изображения,Музыка,Общедоступные,Рабочий\ стол,Шаблоны}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/.mozilla/{extensions,plugins}/ /etc/skel/.mozilla/ 2>/dev/null || :
```

```
cp -rfu $WHO/.config/{caja,caja-actions,chromium,dconf,mate,mate-session}/ /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.config/{monitors.xml,user-dirs.dirs} /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.{reconfigure_profile.sh,bash_logout,bash_profile,bashrc} /etc/skel/ 2>/dev/null || :
```

Запустите созданный скрипт (с правами администратора):

```
bash ./sync_path.sh
```

Отредактируйте файл **/etc/skel/.bashrc**, чтобы при первом входе нового пользователя произошел вызов вашего скрипта. В конец файла допишите:

```
if [ -f ~/.reconfigure_profile.sh ]; then
bash ~/.reconfigure_profile.sh
rm -rf ~/.reconfigure_profile.sh
fi
```

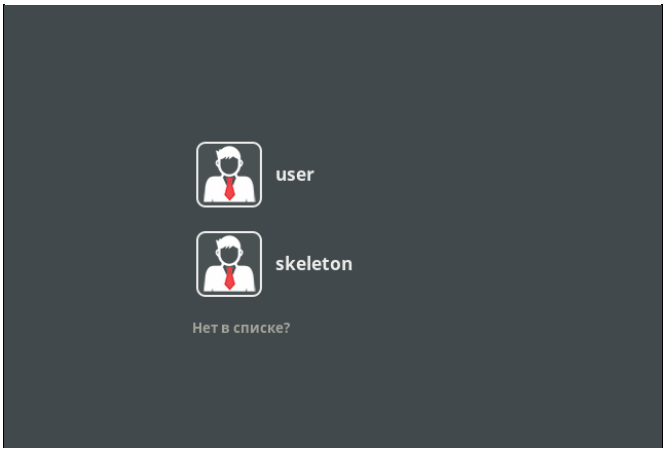
Примечание.

Чем больше будет размер **/etc/skel**, тем дольше будет происходить создание нового пользователя.

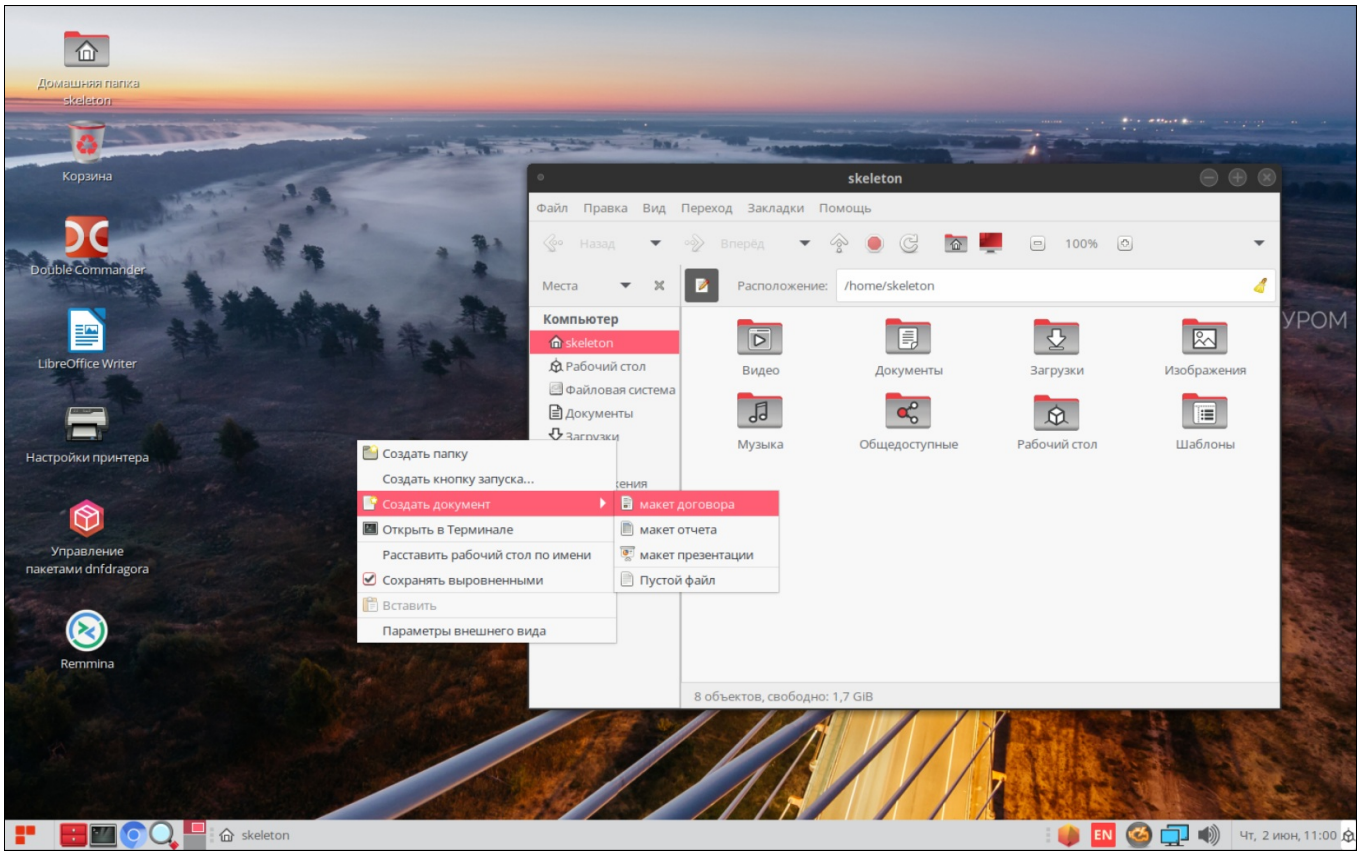
Для проверки работоспособности создайте нового пользователя:

```
useradd skeleton
passwd skeleton
```

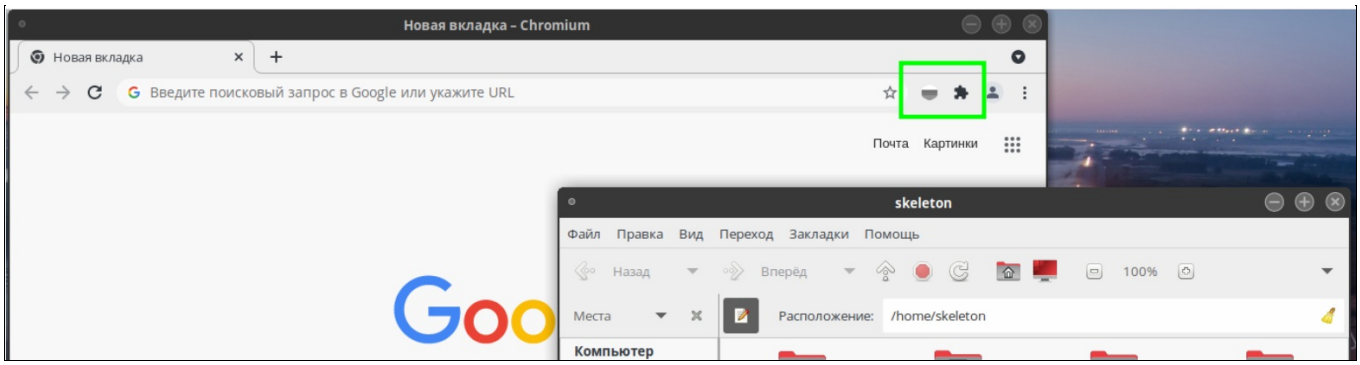
Выйдите из текущей сессии и авторизуйтесь под учетной записью нового пользователя.



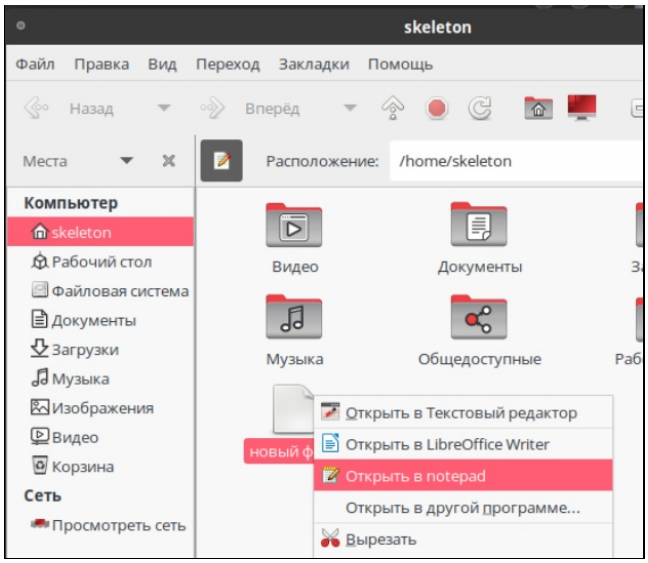
Рабочий стол и **Домашняя папка** успешно созданы.



Проверьте браузер на наличие плагина Госуслуг:



Префикс **wine** также будет скопирован вместе с пунктом **notepad** в контекстном меню.



Управление сеансами пользователей с помощью systemd-logind

Systemd-logind — системная служба, которая управляет сеансами пользователей в операционной системе.

Файлом конфигурации службы **systemd-logind** является **logind.conf**. Для редактирования файла необходимы права **суперпользователя root**.

Откройте файл командой:

```
nano /etc/systemd/logind.conf
```

Содержимое файла выглядит следующим образом:

```
[Login]
 #NAutoVTs=6
 #ReserveVT=6
 #KillUserProcesses=no
 #KillOnlyUsers=
 #KillExcludeUsers=root
 #InhibitDelayMaxSec=5
 #HandlePowerKey=poweroff
 #HandleSuspendKey=suspend
 #HandleHibernateKey=hibernate
 #HandleLidSwitch=suspend
 #HandleLidSwitchExternalPower=suspend
 #HandleLidSwitchDocked=ignore
 #PowerKeyIgnoreInhibited=no
 #SuspendKeyIgnoreInhibited=no
 #HibernateKeyIgnoreInhibited=no
 #LidSwitchIgnoreInhibited=yes
 #HoldoffTimeoutSec=30s
 #IdleAction=ignore
 #IdleActionSec=30min
 #RuntimeDirectorySize=10%
 #RuntimeDirectoryInodes=400k
 RemoveIPC=no
 #InhibitorsMax=8192
 #SessionsMax=8192
```

Основные моменты настройки **systemd-logind**:

Параметр **NAutoVTs=** отвечает за количество виртуальных терминалов, предоставляемых по умолчанию (к ним можно обращаться с использованием сочетания клавиш «*Ctrl+Alt+F[2-6]*»). В РЕД ОС предоставляется 6 виртуальных терминалов. Для изменения их количества необходимо раскомментировать данную строку и указать требуемое число терминалов. Например:

```
NAutoVTs=3
```

Параметр **ReserveVT** определяет один виртуальный терминал, который будет зарезервирован и останется доступным, даже если он не входит в диапазон параметра **NAutoVTs**.

Параметр **KillUserProcesses** отвечает за работу процессов пользователей, которые вышли из системы. Может принимать значения:

- **yes** — все процессы пользователя будут завершены при выходе из системы;
- **no** — процессы пользователя продолжат свою работу даже после завершения сеанса.

По умолчанию данный параметр установлен в значение **no**.

Параметры **KillOnlyUsers**, **KillExcludeUsers** переопределяют параметр **KillUserProcesses** и принимают в качестве значения разделенные пробелами имена пользователей.

Параметр **KillExcludeUsers** (при **KillUserProcesses=yes**) отменяет завершение процессов указанных пользователей после выхода из сеанса.

Параметр **KillOnlyUsers** завершает процессы только указанных пользователей после выхода из сеанса. Если значение параметра не задано, будет применяться параметр **KillUserProcesses**.

Параметр **InhibitDelayMaxSec=** задает максимальное время задержки запроса на выключение системы или переход в спящий режим. Значение по умолчанию равно 5 секунд.

Параметры **HandlePowerKey=**, **HandleSuspendKey=**, **HandleHibernateKey=**, **HandleLidSwitch=**, **HandleLidSwitchExternalPower=**, **HandleLidSwitchDocked=** отображают, каким образом **logind** обрабатывает запросы включения системы, перезагрузки и перехода в спящий режим, а также выключения и приостановки работы системы. Параметры могут принимать значения *ignore*, *poweroff*, *reboot*, *halt*, *kexec*, *suspend*, *hibernate*, *hybrid-sleep*, *suspend-then-hibernate*, *lock* и *factory-reset*.

Параметры **PowerKeyIgnoreInhibited=**, **SuspendKeyIgnoreInhibited=**, **HibernateKeyIgnoreInhibited=**, **LidSwitchIgnoreInhibited=** определяют, подлежат ли блокировке действия клавиш управления питанием, перехода в спящий режим или перезагрузки. Параметры могут принимать значения *no* (действия блокируются) или *yes* (действия не блокируются).

Параметр **HoldoffTimeoutSec=** задает время ожидания после запуска системы или возобновления работы системы, в течение которого система не реагирует на события. Такая задержка необходима для обнаружения системой устройств с горячий подключением. Значение по умолчанию 30 секунд.

Параметр **IdleAction=** отображает действие, которое необходимо выполнять, пока система находится в режиме ожидания. Может принимать такие значения, как *ignore*, *poweroff*, *reboot*, *halt*, *kexec*, *suspend*, *hibernate*, *hybrid-sleep*, *suspend-then-hibernate* и *lock*. Значение по умолчанию *ignore*.

Параметр **IdleActionSec=** задает время, по истечении которого настроенное действие в **IdleAction=** будет выполняться.

Параметр **RuntimeDirectorySize=** отвечает за максимальный размер временных каталогов, создаваемых для пользователей во время работы системы. Принимает размер в байтах, но можно использовать стандартные суффиксы K, M, G и T. Также значение может быть отображено в процентном соотношении. По умолчанию используется 10% физической памяти, но ее можно увеличить. Этот параметр может быть полезен для контроля использования дискового пространства и предотвращения переполнения диска.

Параметр **RemoveIPC=** отвечает за удаление межпроцессного взаимодействия (IPC) при выходе пользователя из системы. Если параметр установлен в значение yes, то все IPC-объекты, созданные пользователем, будут удалены при его выходе из системы.

Параметр **InhibitorsMax=** определяет максимальное количество процессов, которые могут быть заблокированы одновременно. Эти процессы могут быть заблокированы для предотвращения перезагрузки или выключения системы во время их выполнения. Если значение параметра указано 0, то блокировка процессов отключена. Если значение параметра установлено как отрицательное число, то количество заблокированных процессов не ограничено.

Параметр **SessionsMax=** определяет максимальное количество одновременных сеансов пользователя. Если значение параметра установлено в 0, то количество сеансов не ограничено. Если значение параметра больше 0, то это означает максимальное количество сеансов, которые пользователь может открыть одновременно. Если пользователь пытается открыть новый сеанс, когда уже достигнуто максимальное количество сеансов, то ему будет выдано сообщение об ошибке. Этот параметр может быть полезен для ограничения количества одновременных сеансов пользователей и повышения безопасности системы.

С подробной информацией об остальных параметрах файла можно ознакомиться, выполнив команду:

```
man logind.conf
```

По окончании редактирования конфигурационного файла для применения внесенных изменений следует перезагрузить ПК или перезапустить службу **systemd-logind** командой:

```
systemctl restart systemd-logind
```

Ограничение ресурсов пользователя

Для ограничения ресурсов, доступных пользователю, используется конфигурационный файл **/etc/security/limits.conf**. Для включения лимитов необходимо добавить библиотеку **PAM pam_limits.so** в соответствующем модуле. Например:

```
session required pam_limits.so
```

в файле **/etc/pam.d/login**.

Для изменения лимитов редактируем файл **/etc/security/limits.conf**. Формат файла:

```
<группа/пользователь>  <лимит>(жёсткий/мягкий)  <параметр>  <значение>
```

Описание параметров:

- *core* - размер core-файлов (KB);
- *data* - максимальный размер данных (KB);
- *fsize* - максимальный размер файла (KB);
- *memlock* - максимальное заблокированное адресное пространство (KB);
- *nofile* - максимальное количество открытых файлов;
- *rss* - максимальный размер памяти для резидент-программ (KB);
- *stack* - максимальный размер стэка (KB);
- *cpu* - максимальное процессорное время (MIN);
- *nproc* - максимальное количество процессов;
- *as* - ограничение адресного пространства (KB);
- *maxlogins* - максимальное число одновременных регистраций в системе;
- *maxsyslogins* - максимальное количество учётных записей;
- *priority* - приоритет запущенных процессов;
- *locks* - максимальное количество блокируемых файлов пользователем;
- *sigpending* - максимальное количество сигналов, которые можно передать процессу;
- *msgqueue* - максимальный размер памяти для очереди POSIX-сообщений (bytes);
- *nice* - максимальный приоритет, который можно выставить: [-20, 19];
- *rtprio* - максимальный приоритет времени выполнения;
- *chroot* - изменить директорию root'a (Debian-specific).

Вместо можно использовать групповой символ «*» (для всех) и групповой символ «**%**» для wildcast’а групп.

Ограничение полномочий пользователей по использованию виртуальных терминалов

Ограничение полномочий пользователей по использованию виртуальных терминалов можно настроить следующим образом:

Перейдите в сеанс пользователя **root**:

```
su -
```

и добавьте строку в файл **/etc/security/limits.conf**:

```
petrov hard maxlogins 2
```

Добавить строку можно следующей командой:

```
echo "petrov hard maxlogins 2" >> /etc/security/limits.conf
```

где `petrov` - имя пользователя, которому необходимо ограничить число запускаемых виртуальных терминалов.

Затем для ограничения количества запускаемых виртуальных терминалов **для группы пользователей** добавьте в файл **/etc/security/limits.conf** следующую строку:

```
@users hard maxlogins 2
```

где **@users**- это название группы пользователей (для обозначения группы перед её названием используется символ '**@**').

После добавления правила, ограничивающего число сеансов для пользователя *petrov* равным 2, при попытке открыть 3 сеанс в виртуальном терминале возникает ошибка вида:

```
Too many logins for 'petrov'.

Permission denied
```

Для ограничения количества допустимых **tty** (в том числе и отключение их) для всех пользователей, следует изменить содержимое файла **/etc/systemd/logind.conf**:

```
nano  /etc/systemd/logind.conf
```

раскомментировать строку и указать число 1:

```
NAutoVTs=1
```

после перезагрузки доступ к остальным **tty** будет закрыт, вы увидите только черный экран.

Управление дисковыми квотами

Система **diskquota** обеспечивает механизм для управления используемым дисковым пространством. Ограничения могут быть установлены для каждого пользователя в отдельности, для любой или для всех файловых систем. Система ограничений (**quota**) будет предупреждать пользователей, когда они превысят свой дозволенный лимит, но будет позволять использовать некоторое дополнительное пространство для текущей работы. Система ограничений (**quota system**) является частью ядра LINUX.

Вы можете подробнее ознакомиться с управлением дисковыми квотами, просмотрев наши обучающие видео:

- на **RuTube** — Управление дисковыми квотами;
- в **Яндекс.Дзен** — Управление дисковыми квотами;
- в **VK Видео** — Управление дисковыми квотами.

На наших каналах вы также сможете найти много другой полезной информации.

Команда **quota** позволяет просмотреть любые ограничения дискового пространства для каждого пользователя.

Доступны два типа ограничений, которые могут быть наложены на пользователя, обычно, если используется одно из ограничений, то и второе тоже будет использоваться. Ограничение может быть установлено как на все дисковое пространство пользователя, которое используется этим пользователем, так и на число файлов (**inodes**), которыми он может владеть. Quota обеспечивает информацию на ограничения, которые были установлены системным администратором на каждую из областей, которые используются в данный момент. Ограничения по **inodes** и **block** накладываются как на uid (идентификатор пользователя), так и на gid (идентификатор группы). Если вы входите в группу, которая превысила наложенное на нее ограничение, то вы не сможете использовать дисковое пространство, даже если вы все еще можете использовать его как пользователь.

Существуют четыре числа для каждого ограничения:

- используемое в данное время ограничение;
- "мягкое" ограничение (softlimit);
- "жесткое" ограничение (hardlimit);
- промежуток времени, после истечения которого "мягкое" ограничение интерпретируется как "жесткое".

"Мягкое" ограничение определяет число блоков размером 1Кбайт, которое пользователь может немного превысить. "Жесткое" ограничение не может быть превышено ни каким образом. Если пользователь пытается превысить данное число, то он получает сообщение о невозможности сделать это. При этом ядро возвращает код ошибки **EDQUOT**. После того как пользователь превысит доступное для него "мягкое" ограничение (softlimit) устанавливается время, после истечения которого "мягкое" ограничение становится "жестким" (hardlimit). Обычно срок этого периода истекает после 7 дней (1 неделя). В этот период времени пользователь может удалить ненужные ему файлы, после чего он вновь может использовать "мягкое" ограничение до момента истечения указанного промежутка времени. После истечения указанного промежутка времени "мягкое" ограничение становится "жестким" и у пользователя больше нет ресурсов для создания новых файлов.

Для того чтобы установить систему ограничений дискового пространства (quota) в ОС, системному администратору необходимо сделать несколько шагов:

- выбрать файловую систему, на которую будут накладываться ограничения;
- разрешить (включить) систему ограничений;
- произвести проверку файловой системы на ограничения дискового пространства;
- произвести проверку ограничений дискового пространства как для пользователей, так и для групп;
- запретить ограничения для пользователей и групп.

В первую очередь необходимо решить, на какую файловую систему необходимо наложить ограничения (quotas). Чаще всего ограничения накладываются на файловую систему, в которой располагаются домашние каталоги пользователей или на файловую систем, которая смонтирована в каталог **/usr**, и пользователи имеют право записывать на нее информацию. Для того чтобы разрешить ограничения на дисковое пространство на необходимой файловой системе, вы должны отредактировать файл **/etc/fstab**, добавив к указанной системе опции для ограничения дискового пространства (как для пользователей, так и для групп).

Отредактированный файл **/etc/fstab** может иметь вид:

```
#
# /etc/fstab
#
/dev/hda1           /            ext2    defaults
/dev/hda2           none           swap    sw
/dev/hda3           /usr          ext2    defaults
/dev/hdb1           /usr/users      ext2    defaults,usrquota,grpquota
/dev/hdb2           /usr/src       ext2    defaults,usrquota
none              /proc         proc    defaults
```

Зарезервированное слово "usrquota" в поле опций включает ограничение дискового пространства (quotas) для пользователей (userquota) на данном устройстве. Зарезервированное слово "grpquota" включает ограничение дискового пространства для групп (groupquota) на данном устройстве. Во то время, когда вы используете опции "usrquota" и "grpquota" без '=', ваши файлы ограничений (quotafile) будут находиться в корневом каталоге каждой файловой системы, в которой используются ограничения на дисковое пространство. Файл называемый "**aquota.user**" будет использоваться для ограничений пользователей, а файл "**aquota.group**" будет

использоваться для ограничений групп. Однако вы сами можете определить ваши файлы ограничений. Например, строка "**usrquota=/usr/adm/quotasrc.user**" установит файл ограничений для пользователей в каталоге **/usr/adm**, который будет называться "**quotarc.user**". Однако будьте внимательны и отслеживайте длину строки в файле **/etc/fstab** (смотрите ее определение в файле **mntent.h**).

Периодически (в основном после некорректной перезагрузки системы и во время первого разрешения ограничений на дисковое пространство) записи, содержащиеся в файле ограничений, должны быть проверены на целостность действительного числа блоков и файлов, выделенных для пользователя. Для выполнения этой операции может быть использована команда **quotacheck**.

Данную команду необязательно выполнять для неподмонтированных файловых систем или на файловых системах, на которых отключено ограничение на дисковое пространство (quotas). Для проверки файловой системы на число блоков, используемых пользователем, а так же для установки и изменения всех файлов ограничений (quotafiles), выполните команду:

```
quotacheck -avug
```

Вы можете вставить данную команду в один из rc-скриптов и запускать ее на файловой системе так же, как и **fsck**, только тогда, когда не установлен флаг **fastreboot**. Данная программа не поддерживает одновременную параллельную проверку нескольких файловых систем. Для того чтобы включить систему ограничений на дисковое пространство на вашем компьютере, добавьте строку **/usr/bin/quotaon -avug** в один из ваших **/etc/rc-файлов**. Данная команда будет включать поддержку ограничений дискового пространства во время загрузки вашей системы.

Только суперпользователь может использовать команду quota для проверки используемых ограничений любого пользователя и команду repquota для проверки используемого пространства и ограничений для всех пользователей на данной файловой системе.

Для того чтобы получить информацию об ограничениях, наложенных на всех пользователей, необходимо выполнить команду:

```
repquota -ua
```

после чего на экране можно будет видеть таблицу, в которой указаны ограничения, наложенные на каждого пользователя.

Содержимое экрана после выполнения выше приведенной команды может иметь вид:

```
                Block limits            File limits
User          used    soft    hard  grace    used  soft  hard  grace
root      --  487082       0       0        12147     0     0
daemon    --     399       0       0            2     0     0
news      --     626       0       0           46     0     0
```

Для получения информации о группах необходимо выполнить команду:

```
repquota -ga
```

Для редактирования ограничения дискового пространства необходимо использовать программу **edquota**. Для редактирования ограничений дискового пространства для конкретного пользователя

необходимо использовать программу **edquota** с опцией **-u**, а для группы необходимо использовать ту же программу, но с опцией **-g**. Редактировать необходимо только число , которое следует за словом *hard* или *soft*. Например, после выполнения команды:

```
edquota -u cola
```

содержимое экрана может иметь вид:

```
Quotas for user cola:
/dev/hdb3: blocks in use: 345, limits (soft = 1, hard = 0)
        inodes in use: 94, limits (soft = 0, hard = 0)
```

После чего вы можете изменить значения, указанные после слов hard и soft. При редактировании используется редактор, который указывается в переменной окружения **EDITOR**.

Для каждой файловой системы, имеющей ограничение на дисковое пространство, вы видите две строки. Слово **soft** означает, что на данную файловую систему наложено "мягкое" ограничение (softlimit), при этом пользователь или группа имеют некоторый интервал времени (grace period), в течении которого они могут превысить указанное значение. Данный интервал времени можно изменить с помощью команды **edquota -t**.

Например, после выполнения команды:

```
edquota -t
```

содержимое экрана может иметь вид:

```
Time units may be: days, hours, minutes, or seconds
Grace period before enforcing soft limits for users:
/dev/hdb3: block grace period: 10 minutes, file grace period: 10 minutes
```

После чего вы можете изменить значения, указанные по умолчанию. По умолчанию используется значение, определенное в файле <LINUX quota.h>. Если пользователь или группа не удалят лишних файлов в течении указанного периода времени, то данные файлы переходят в разряд "жестких" ограничений (hardlimit). Слово **hard** означает, что на данную файловую систему наложено "жесткое" ограничение. Жесткое ограничение является максимальным значением, которое может иметь пользователь или группа на данной файловой системе. Пользователь/группа не может иметь больше файлов или inodes, чем указано в hard.

Строка:

```
/dev/hdb3: blocks in use: 345, limits (soft = 1, hard = 0)
```

сообщает, какое число блоков может быть выделено для данного пользователя или группы.

Строка:

```
inodes in use: 94, limits (soft = 0, hard = 0)
```

сообщает, какое число inode (файлов, устройств, поименованных каналов (pipes) и т.д.) может быть выделено для данного пользователя или группы.

В большинстве случаев вам приходится иметь группу пользователей, которые должны иметь одинаковые ограничения на дисковое пространство на указанной файловой системе. Самый быстрый путь - отредактировать ограничения на дисковое пространство для этих пользователей и создать прототип одного из пользователей или группы для всех других. С помощью команды:

```
edquota -u <имя_пользователя/группы_который_станет_прототипом>
```

отредактировать ограничения на дисковое пространство, после чего с помощью команды:

```
edquota -p <имя_прототипа> *
```

отредактировать ограничения для всех оставшихся пользователей.

Например, для того чтобы в качестве ограничений дискового пространства (quota) для пользователя ola использовались ограничения, наложенные на пользователя cola, вам необходимо выполнить команду:

```
edquota -p cola ola
```

Для проверки ограничений дискового пространства для пользователя и группы используется программа quota.

Синтаксис этой программы:

```
quota [-guqv]
quota [-qv] -u username ...
quota [-qv] -g groupname ...
```

Используйте опцию **-v** для вывода информации о:

- файловых системах, которые не имеют включенными ограничения на дисковое пространство (quota);
- файловых системах, на которых вы уже установили систему ограничения дискового пространства, но на которых еще не занят ни один блок.

Используйте опцию **-q** для просмотра файловых систем, на которых превышено значение "мягкого" (softlimit) и "жесткого" (hardlimit) ограничения.

Опция **-g** дает вам возможность просмотреть все ограничения, которые наложены на группы, членом которых вы являетесь.

Например, с помощью команды:

```
quota -u cola
```

вы можете получить информацию об ограничениях дискового пространства, которые наложены на пользователя cola. Содержимое экрана после выполнения данной команды может иметь вид:

```
Disk quotas for user cola (uid 1002):
 Filesystem  blocks   quota   limit   grace   files   quota   limit  grace
```

```
/dev/hdb3    345*    1     0   none     94      0      0
```

Если вы захотели запретить ограничения, наложенные на какого-то пользователя или на группу, то вам необходимо воспользоваться программой **edquota** для редактирования значений **hard** и **soft**. Установите эти значения в 0. После чего для данного пользователя или группы не будет существовать ограничений на дисковое пространство, и он/она сможет создавать неограниченное количество файлов (ограниченное только дисковым пространством).

Настройка прав доступа к файлам и каталогам

Поскольку Linux — система многопользовательская, вопрос об организации разграничения доступа к файлам и каталогам является одним из существенных вопросов, которые должна решать операционная система.

В основе механизмов разграничения доступа лежат имена пользователей и имена групп пользователей. В Linux каждый пользователь имеет уникальное имя, под которым он входит в систему (логируется). Кроме того, в системе создается некоторое число групп пользователей, причем каждый пользователь может быть включен в одну или несколько групп. Создает и удаляет группы суперпользователь, он же может изменять состав участников той или иной группы. Члены разных групп могут иметь разные права по доступу к файлам, например, группа администраторов может иметь больше прав, чем группа программистов.

Вы можете подробнее ознакомиться с назначением прав доступа к файлам и каталогам, просмотрев наши обучающие видео:

- на **RuTube**:
    - Атрибуты файлов и каталогов в РЕД ОС;
    - Расширенные права доступа.
- в **Яндекс.Дзен**:
    - Атрибуты файлов и каталогов в РЕД ОС;
    - Расширенные права доступа.
- в **VK Видео**:
    - Атрибуты файлов и каталогов в РЕД ОС;
    - Расширенные права доступа.

На наших каналах вы также сможете найти много другой полезной информации.

В индексном дескрипторе каждого файла записаны имя так называемого владельца файла и группы, которая имеет права на этот файл. Первоначально, при создании файла его владельцем объявляется тот пользователь, который этот файл создал. Точнее — тот пользователь, от чьего имени запущен процесс, создающий файл. Группа тоже назначается при создании файла — по идентификатору группы процесса, создающего файл. Владельца и группу файла можно поменять в ходе дальнейшей работы с помощью команд **chown** и **chgrp**.

Выполним команду **ls -l**. Но зададим ей в качестве дополнительного параметра имя конкретного файла, например, файла, задающего саму команду **ls**.

```
$ ls -l /bin/ls
-rwxr-xr-x 1 root root 49940 Sep 12 1999 /bin/ls
```

В данном случае владельцем файла является пользователь *root* и группа *root*. Но нас сейчас в выводе этой команды больше интересует первое поле, определяющее тип файла и права доступа к файлу. Это поле в приведенном примере представлено цепочкой символов **-rwxr-xr-x**. Эти символы можно условно разделить на 4 группы.

Первая группа, состоящая из единственного символа, определяет тип файла. Этот символ в соответствии с возможными типами файлов может принимать такие значения:

- — обычный файл;

d — каталог;

b — файл блочного устройства;

c — файл символьного устройства;

s — доменное гнездо (socket);

p — именованный канал (pipe);

l — символическая ссылка (link).

Далее следуют три группы по три символа, которые и определяют права доступа к файлу соответственно для владельца файла, для группы пользователей, которая сопоставлена данному файлу, и для всех остальных пользователей системы. В нашем примере права доступа для владельца определены как **rwx**, что означает, что владелец (root) имеет право читать файл (**r**), производить запись в этот файл (**w**), и запускать файл на выполнение (**x**). Замена любого из этих символов прочерком будет означать, что пользователь лишается соответствующего права. В том же примере мы видим, что все остальные пользователи (включая и тех, которые вошли в группу root) лишены права записи в этот файл, т. е. не могут файл редактировать и вообще как-то изменять.

Права доступа и информация о типе файла в UNIX-системах хранятся в индексных дескрипторах в отдельной структуре, состоящей из двух байтов, т. е. из 16 бит. Четыре бита из этих 16-ти отведены для кодированной записи о типе файла. Следующие три бита задают особые свойства исполняемых файлов. И, наконец, оставшиеся 9 бит определяют права доступа к файлу. Эти 9 бит разделяются на 3 группы по три бита. Первые три бита задают права пользователя, следующие три бита — права группы, последние 3 бита определяют

права всех остальных пользователей (т. е. всех пользователей, за исключением владельца файла и группы файла).

При этом, если соответствующий бит имеет значение 1, то право предоставляется, а если он равен 0, то право не предоставляется. В символьной форме записи прав единица заменяется соответствующим символом (r, w или x), а 0 представляется прочерком.

Право на чтение (**r**) файла означает, что пользователь может просматривать содержимое файла с помощью различных команд просмотра, например, командой more или с помощью любого текстового редактора. Но, подредактировав содержимое файла в текстовом редакторе, вы не сможете сохранить изменения в файле на диске, если не имеете права на запись (**w**) в этот файл. Право на выполнение (**x**) означает, что вы можете загрузить файл в память и попытаться запустить его на выполнение как исполняемую программу. Конечно, если в действительности файл не является программой (или скриптом shell), то запустить этот файл на выполнение не удастся, но, с другой стороны, даже если файл действительно является программой, но право на выполнение для него не установлено, то он тоже не запустится.

Если выполнить ту же команду **ls -l**, но в качестве последнего аргумента ей указать не имя файла, а имя каталога, мы увидим, что для каталогов тоже определены права доступа, причем они задаются теми же самыми символами rwx. Например, выполнив команду **ls –l /**, мы увидим, что каталогу bin соответствует строка:

```
drwxr-xr-x 2 root root 2048 Jun 21 21:11 bin
```

Естественно, что по отношению к каталогам трактовка понятий «право на чтение», «право на запись» и «право на выполнение» несколько изменяется. Право на чтение по отношению к каталогам легко понять, если вспомнить, что каталог — это просто файл, содержащий список файлов в данном каталоге. Следовательно, если вы имеете право на чтение каталога, то вы можете просматривать его содержимое (этот самый список файлов в каталоге). Право на запись тоже понятно — имея такое право, вы сможете создавать и удалять файлы в этом каталоге, т. е. просто добавлять в каталог или удалять из него запись, содержащую имя какого-то файла и соответствующие ссылки. Право на выполнение в данном случае означает право переходить в этот каталог. Если вы, как владелец, хотите дать доступ другим пользователям на просмотр какого-то файла в своем каталоге, вы должны дать им право доступа в каталог, т. е. дать им «право на выполнение каталога». Более того, надо дать пользователю право на выполнение для всех каталогов, стоящих в дереве выше данного каталога. Поэтому в принципе для всех каталогов по умолчанию устанавливается право на выполнение как для владельца и группы, так и для всех остальных пользователей. И, уж если вы хотите закрыть доступ в каталог, то лишите всех пользователей (включая группу) права входить в этот каталог.

После прочтения предыдущего абзаца может показаться, что право на чтение каталога не дает ничего нового по сравнению с правом на выполнение. Однако разница в этих правах все же есть. Если задать только право на выполнение, вы сможете войти в каталог, но не увидите там ни одного файла (этот эффект особенно наглядно проявляется в том случае, если вы пользуетесь каким-то файловым менеджером, например, программой Midnight Commander). Если вы имеете право доступа в каком-то из подкаталогов этого каталога, то вы можете перейти в него (командой **cd**), но, как говорится «вслепую», по памяти, потому что списка файлов и подкаталогов текущего каталога вы не увидите.

Алгоритм проверки прав пользователя при обращении к файлу можно описать следующим образом. Система вначале проверяет, совпадает ли имя пользователя с именем владельца файла. Если эти имена совпадают (т. е. владелец обращается к своему файлу), то проверяется, имеет ли владелец соответствующее право доступа: на чтение, на запись или на выполнение (не удивляйтесь, суперпользователь может лишить некоторых прав и владельца файла). Если право такое есть, то соответствующая операция разрешается. Если же нужного права владелец не имеет, то проверка прав, предоставляемых через группу или через группу атрибутов доступа для остальных пользователей, уже даже не проверяются, а пользователю выдается сообщение о невозможности выполнения затребованного действия (обычно что-то вроде «Permission denied»).

Если имя пользователя, обращающегося к файлу, не совпадает с именем владельца, то система проверяет, принадлежит ли владелец к группе, которая сопоставлена данному файлу (далее будем просто называть ее группой файла). Если принадлежит, то для определения возможности доступа к файлу используются атрибуты, относящиеся к группе, а на атрибуты для владельца и всех остальных пользователей внимания не обращается. Если же пользователь не является владельцем файла и не входит в группу файла, то его права определяются атрибутами для остальных пользователей. Таким образом, третья группа атрибутов, определяющих права доступа к файлу, относится ко всем пользователям, кроме владельца файла и пользователей, входящих в группу файла.

Для изменения прав доступа к файлу используется команда **chmod**. Ее можно использовать в двух вариантах. В первом варианте вы должны явно указать, кому какое право даете или кого этого права лишаете:

```
chmod wXp
```

где вместо символа **w** подставляется

- либо символ **u** (т. е. пользователь, который является владельцем);
- либо **g** (группа);
- либо **o** (все пользователи, не входящие в группу, которой принадлежит данный файл);
- либо **a** (все пользователи системы, т. е. и владелец, и группа, и все остальные).

Вместо **X** ставится:

- либо **+** (предоставляем право);
- либо **–** (лишаем соответствующего права);
- либо **=** (установить указанные права вместо имеющихся),

Вместо **p** — символ, обозначающий соответствующее право:

- **r** (чтение);
- **w** (запись);
- **x** (выполнение).

Вот несколько примеров использования команды chmod:

```
chmod a+x
```

предоставляет всем пользователям системы право на выполнение данного файла.

```
chmod go-rw
```

удаляет право на чтение и запись для всех, кроме владельца файла.

```
chmod ugo+rwx
```

дает всем права на чтение, запись и выполнение.

Если опустить указание на то, кому предоставляется данное право, то подразумевается, что речь идет вообще обо всех пользователях, т. е. Вместо

```
chmod a+x
```

можно записать просто

```
chmod +x
```

Второй вариант задания команды **chmod** (он используется чаще) основан на цифровом представлении прав. Для этого мы кодируем символ *r* цифрой 4, символ *w* — цифрой 2, а символ *x* — цифрой 1. Для того, чтобы предоставить пользователям какой-то набор прав, надо сложить соответствующие цифры. Получив, таким образом, нужные цифровые значения для владельца файла, для группы файла и для всех остальных пользователей, задаем эти три цифры в качестве аргумента команды **chmod** (ставим эти цифры после имени команды перед вторым аргументом, который задает имя файла). Например, если надо дать все права владельцу (4+2+1=7), право на чтение и запись — группе (4+2=6), и не давать никаких прав остальным, то следует дать такую команду:

```
chmod 760
```

Если вы знакомы с двоичным кодированием восьмеричных цифр, то вы поймете, что цифры после имени команды в этой форме ее представления есть не что иное, как восьмеричная запись тех самых 9 бит, которые задают права для владельца файла, группы файла и для всех пользователей.

Выполнять смену прав доступа к файлу с помощью команды **chmod** может только сам владелец файла или суперпользователь. Для того, чтобы иметь возможность изменить права группы, владелец должен дополнительно быть членом той группы, которой он хочет дать права на данный файл.

Надо рассказать еще о трех возможных атрибутах файла, устанавливаемых с помощью той же команды **chmod**. Это те самые атрибуты для исполняемых файлов, которые в индексном дескрипторе файла в двухбайтовой структуре, определяющей права на файл, занимают позиции 5-7, сразу после кода типа файла.

Первый из этих атрибутов — так называемый "бит смены идентификатора пользователя". Смысл этого бита состоит в следующем.

Обычно, когда пользователь запускает некоторую программу на выполнение, эта программа получает те же права доступа к файлам и каталогам, которые имеет пользователь, запустивший программу. Если же установлен "бит смены идентификатора пользователя", то программа получит права доступа к файлам и каталогам, которые имеет владелец файла программы (таким образом, рассматриваемый атрибут лучше называть "битом смены идентификатора владельца"). Это позволяет решать некоторые задачи, которые иначе было бы трудно выполнить. Самый характерный пример — команда смены пароля **passwd**. Все пароли пользователей хранятся в файле **/etc/passwd**, владельцем которого является суперпользователь **root**. Поэтому программы, запущенные обычными пользователями, в том числе команда **passwd**, не могут производить запись в этот файл. А, значит, пользователь как бы не может менять свой собственный пароль. Но для файла **/usr/bin/passwd** установлен "бит смены идентификатора владельца", каковым является пользователь root. Следовательно, программа смены пароля **passwd** запускается с правами **root** и получает право записи в файл **/etc/passwd** (уже средствами самой программы обеспечивается то, что пользователь может изменить только одну строку в этом файле).

Установить "бит смены идентификатора владельца" может суперпользователь с помощью команды

```
chmod +s file_name
```

Аналогичным образом работает "бит смены идентификатора группы".

Еще один возможный атрибут исполняемого файла — это "бит сохранения задачи" или "*sticky bit*" (дословно — "бит прилипчивости").

Этот бит указывает системе, что после завершения программы надо сохранить ее в оперативной памяти. Удобно включить этот бит для задач, которые часто вызываются на выполнение, так как в этом случае экономится время на загрузку программы при каждом новом запуске. Этот атрибут был необходим на старых моделях компьютеров. На современных быстродействующих системах он используется редко.

Если используется цифровой вариант задания атрибутов в команде **chmod**, то цифровое значение этих атрибутов должно предшествовать цифрам, задающим права пользователя:

```
chmod 4775
```

При этом веса этих битов для получения нужного суммарного результата задаются следующим образом:

4 — "бит смены идентификатора пользователя",

2 — "бит смены идентификатора группы",

1 — "бит сохранения задачи (sticky bit)".

Если какие-то из этих трех битов установлены в 1, то несколько изменяется вывод команды **ls -l** в части отображения установленных атрибутов прав доступа. Если установлен в 1 "бит смены идентификатора пользователя", то символ "x" в группе, определяющей права владельца файла, заменяется символом "s". Причем, если владелец имеет право на выполнение файла, то символ "x" заменяется на маленькое "s", а если владелец не имеет права на выполнение файла (например, файл вообще не исполняемый), то вместо "x" ставится "S". Аналогичные замены имеют место при задании "бита смены идентификатора группы", но заменяется символ "x" в группе атрибутов, задающих права группы. Если равен 1 "бит сохранения задачи (sticky bit)", то заменяется символ "x" в группе атрибутов, определяющей права для всех остальных пользователей, причем "x" заменяется символом "t", если все пользователи могут запускать файл на выполнение, и символом "T", если они такого права не имеют.

Таким образом, хотя в выводе команды **ls -l** не предусмотрено отдельных позиций для отображения значений битов смены идентификаторов и бита сохранения задачи, соответствующая информация выводится. Вот небольшой пример того, как это будет выглядеть:

```
ls -l prim1
-rwSrwsrwT 1 kos root 12 Dec 18 23:17 prim1
```

umask (от англ. user file creation mode mask — маска режима создания пользовательских файлов) — функция среды POSIX, изменяющая права доступа, которые присваиваются новым файлам и директориям по умолчанию. Права доступа файлов, созданных при конкретном значении **umask**, вычисляются при помощи следующих побитовых операций (umask обычно устанавливается в восьмеричной системе счисления): побитовое «**И**» между унарным дополнением аргумента (используя побитовое «**НЕ**») и режимом полного доступа.

Фактически, **umask** указывает, какие биты следует сбросить в выставляемых правах на файл — каждый установленный бит **umask** запрещает выставление соответствующего бита прав. Исключением из этого запрета является бит исполняемости, который для обычных файлов зависит от создающей программы (трансляторы ставят бит исполняемости на создаваемые файлы, другие программы — нет), а для каталогов следует общему правилу. **umask 0** означает, что следует (можно) выставить все биты прав (rwxrwxrwx), **umask 777** запрещает выставление любых прав.

Допустим, что значение **umask** равняется **174**, тогда каждый новый файл будет иметь права доступа 602, а каждая новая директория 603.

Режим Киоска в РЕД ОС

Включение режима киоска
Выключение режима киоска

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: redos-kiosk-utils-0.16-1

Режим киоска представляет собой рабочую среду для пользователя или группы пользователей с четко ограниченным функционалом – пользователи имеют доступ только к тем приложениям, которые явно указаны для их профиля.

Режим киоска в РЕД ОС реализуется с помощью доработанной командной оболочки *Bash* и окружения рабочего стола *MATE*.

Базовый функционал киоска реализован в нескольких пакетах и находится в выключенном состоянии. Режим киоска с утилитами для его настройки становится доступным после установки пакета **redos-kiosk-utils**.

Вы можете подробнее ознакомиться с организацией режима киоска в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Режим Киоска в РЕД ОС;
- в **Яндекс.Дзен** — Режим Киоска в РЕД ОС;
- в **VK Видео** — Режим Киоска в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки пакета **redos-kiosk-utils** выполните команду (потребуются права **администратора**):

```
sudo dnf install redos-kiosk-utils
```

В текущей версии для настройки режима киоска имеются только консольные утилиты, которые должны выполняться **с правами суперпользователя root**.

При включенном режиме киоска пользователю становятся недоступны:

- запуск программ с графическим интерфейсом, кроме явно разрешённых (ярлыки таких приложений находятся на *Рабочем столе*);
- выполнение сценариев на любом языке при явном их запуске пользователем;
- запуск на выполнение файлов с установленным битом *SUID*;
- изменение свойств и содержимого главной панели на *Рабочем столе*;
- изменение содержимого *Рабочего стола* (создание/удаление/изменение ярлыков, создание/удаление/изменение иных файлов);
- автоматическое монтирование внешних накопителей;
- смена виртуальной консоли по сочетанию клавиш **Ctrl+Alt+F*n***.

Также имеются следующие ограничения в режиме киоска:

- главная панель *Рабочего стола* в режиме киоска не имеет кнопки главного меню (типа «Пуск») и пиктограмм быстрого запуска приложений. Кнопки выхода из сессии, блокировки экрана и выключения/перезагрузки ПК вынесены на главную панель слева;
- Центр управления *MATE* недоступен, но, даже в случае его ручного запуска, приложение блокируется;
- блокирован запуск *Терминала MATE*;
- из консольных утилит блокированы **dconf** и **gsettings** с целью исключения изменений настроек как *MATE*, так и графической системы;
- просмотр справочной системы недоступен как при вызове по клавише **F1**, так и по нажатию кнопки «**Помощь**», также блокируется в ряде апплетов показ диалогового окна «**О программе**»;
- дополнительное усечение прав и возможностей пользователя путём запуска приложений в «песочнице» (**Firejail**).

Включение режима киоска

Для *включения режима киоска* конкретному пользователю применяется команда **kiosk-mode-on** с указанием имени этого пользователя (опция `-u` или `--username`) и перечнем приложений (опция `-a` или `--appname`), которые разрешаются к запуску пользователем в данном режиме. Также доступны следующие опции:

- `-t`, `--timelock` – указание времени (в минутах) бездействия в сессии перед включением хранителя экрана и блокировки экрана; по умолчанию, а также при указании значения 0 минут блокировка экрана отключается;
- `-b`, `--blockbtn` – отображение кнопки блокирования экрана на главной панели (по умолчанию кнопка не отображается);
- `-i`, `--autohide` – включение автоматического скрытия главной панели *Рабочего стола* (по умолчанию она постоянно отображается);
- `-f`, `--firejail` – при необходимости запуска разрешённых приложений в «песочнице» для более значимых ограничений (проект использует пакет **Firejail**). Если требуется задать какую-либо опцию для **firejail** (согласно его официальной документации), то данные ключи можно привести в двойных кавычках либо сразу после опции, либо после знака равенства;
- `-q` или `--quiet` – подавление вывода на экран (например, для использования в сценариях оболочки). Подавляется вывод не только информационных сообщений, но и сообщений об ошибках.

Например:

- для пользователя **sidorov** разрешить запуск текстового редактора **LibreOffice Writer** и почтового клиента **Mozilla Thunderbird** с блокировкой экрана после **5 минут** бездействия:

```
kiosk-mode-on -u sidorov -a libreoffice-writer,thunderbird -t 5
```

- для пользователя **ivanov** разрешить запуск только интернет-браузера **Firefox** с подключением по сетевому интерфейсу **enp1s3**:

```
kiosk-mode-on -u ivanov -a firefox --firejail="--net=enp1s3"

  или
kiosk-mode-on -u ivanov -a firefox -f"--net=enp1s3"
```

Обе команды равнозначны.

Приложения указываются путём перечисления имён *desktop*-файлов, имеющихся в каталоге **/usr/share/applications** без указания суффикса «**.desktop**». Иные приложения не допускаются к разрешению в режиме киоска.

По умолчанию на главной панели *Рабочего стола* имеются кнопки выключения, перезагрузки системы и завершения сеанса/смены пользователя, причём для перезагрузки или выключения системы потребуется ввести пароль администратора (**root**).



Выключение режима киоска

Для *выключения режима киоска* и возврата настроек пользователя к обычному состоянию используется команда **kiosk-mode-off** с указанием имени этого пользователя (`-u` или `--username`). Например:

```
kiosk-mode-off -u sidorov
```

multiseat - настройка нескольких рабочих мест

Требования аппаратному обеспечению
Установка
Настройка видеокарт
Назначение устройств

Multiseat — это режим, при котором несколько пользователей одновременно работают на одном компьютере. Данная возможность достигается за счет наличия нескольких мониторов, нескольких клавиатур и мышей.

Преимущества данного решения:

- меньшее энергопотребление (только один компьютер);
- меньшее количество оборудования для покупки.

В РЕД ОС мультитерминальный режим настраивается с помощью графической утилиты **Multiseat**.

Вы можете подробнее ознакомиться с настройкой мультитерминального режима, просмотрев наши обучающие видео:

- на **RuTube** — Делаем из одного компьютера два. Режим multiseat в РЕД ОС;
- в **Яндекс.Дзен** — Делаем из одного компьютера два. Режим multiseat в РЕД ОС;
- в **VK Видео** — Делаем из одного компьютера два. Режим multiseat в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Требования аппаратному обеспечению

Минимальные требования для аппаратного обеспечения:

1) Видеокарта для каждого рабочего места. Главное требование — видеокарты должны быть совместимы друг с другом.

2) Процессор и память. Необходим как минимум 2-х ядерный процессор и объем оперативной памяти, рассчитанной на 2-х и более пользователей.

3) Клавиатура и мышь для каждого рабочего места. Могут подойти любые стандартные PS/2 или USB клавиатура и мышь.

Установка

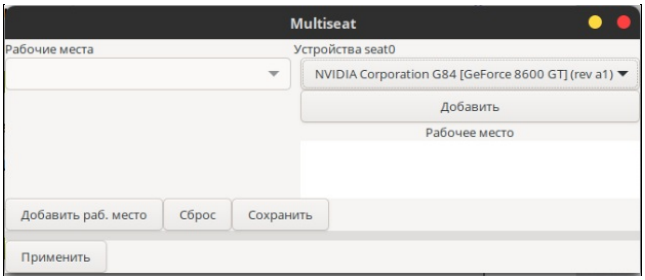
Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install multiseat
```

После установки программа будет доступна из «**Главного меню**» — «**Прочие**» — «**Multiseat**».

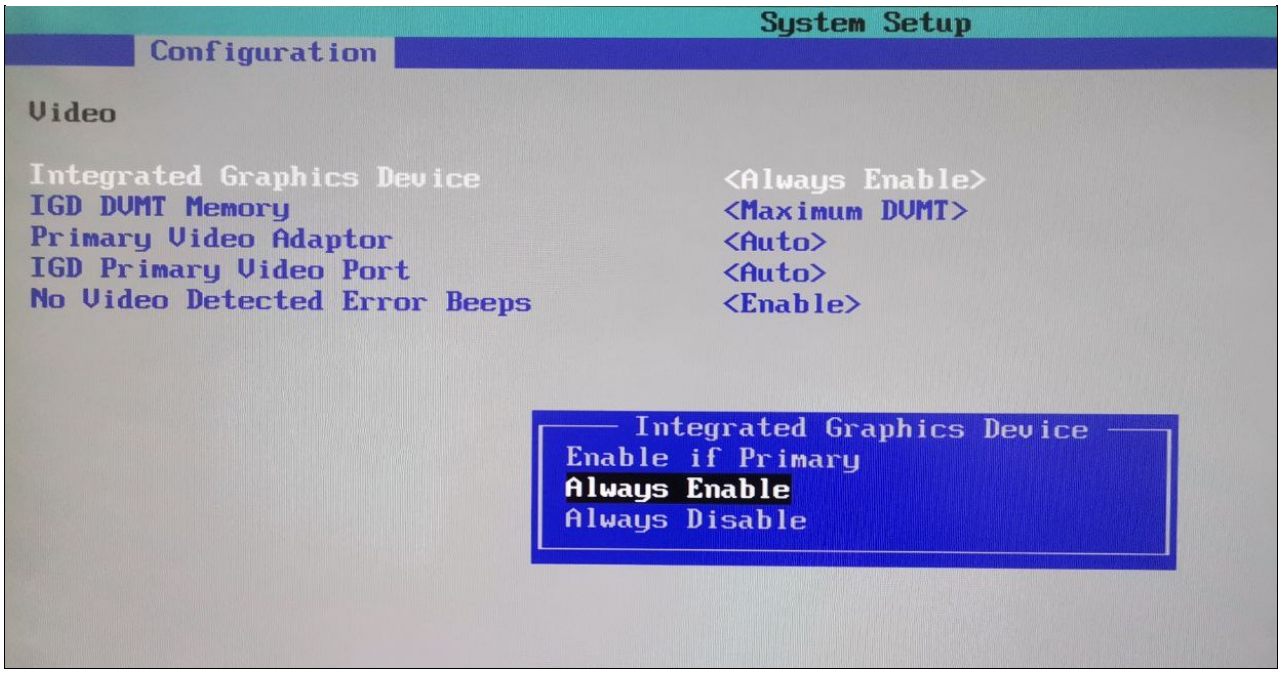


Настройка видеокарт

Примечание.

Главным условием для создания и организации нескольких рабочих мест является наличие **нескольких видеокарт**. Так для создания двух рабочих мест потребуется две видеокарты, одна из которых может быть встроенной.

При использовании связки видеокарт встроенная + дискретная, необходимо разрешить BIOS использовать встроенную графику при работающей дискретной. Для этого при загрузке системы необходимо нажать клавишу «**F2**», чтобы открыть настройки BIOS. Далее следует найти настройки графики и установить значение параметра **Integrated Graphics Device** в **Always Enable**.



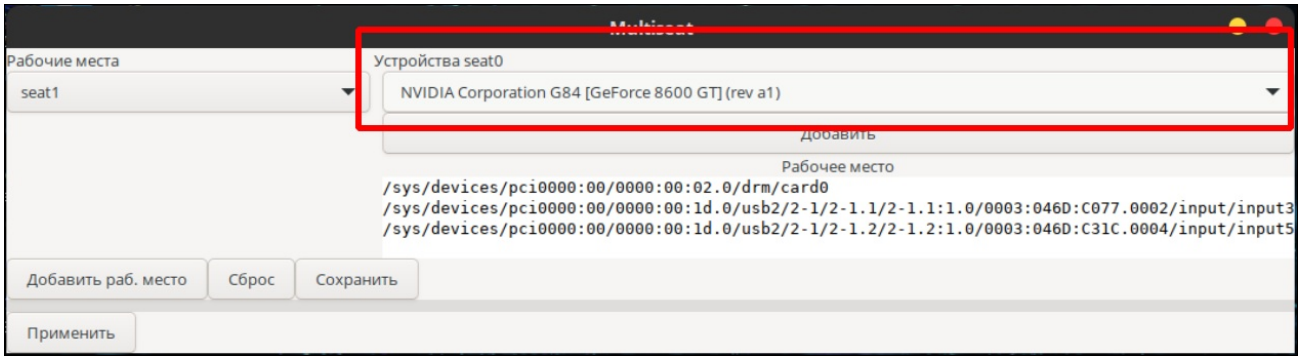
Сохраните настройки и выйдите из BIOS.

После загрузки системы видеовыход должен осуществляться на оба устройства (**Device-1** и **Device-2**), проверить это можно командой:

```
inxi -G

Graphics:
  Device-1: Intel Xeon E3-1200 v2/3rd Gen Core processor Graphics
  driver: i915 v: kernel

  Device-2: NVIDIA G84 [GeForce 8600 GT] driver: nouveau v: kernel
  Display: x11 server: X.Org 1.20.14 driver: modesetting
  unloaded: fbdev,vesa resolution: 1920x1080~60Hz
  OpenGL: renderer: NV84 v: 3.3 Mesa 20.2.4
```

Назначение устройств

По умолчанию в системе существует только одно рабочее место с именем **seat0**, к которому подключены все доступные устройства, они перечислены в выпадающем списке **Устройства seat0**. Это рабочее место нельзя удалить или изменить.



Для создания нового рабочего места нажмите на кнопку «**Добавить раб. место**». Новое рабочее место будет создано с именем **seat1** и отобразится в списке «**Рабочие места**».

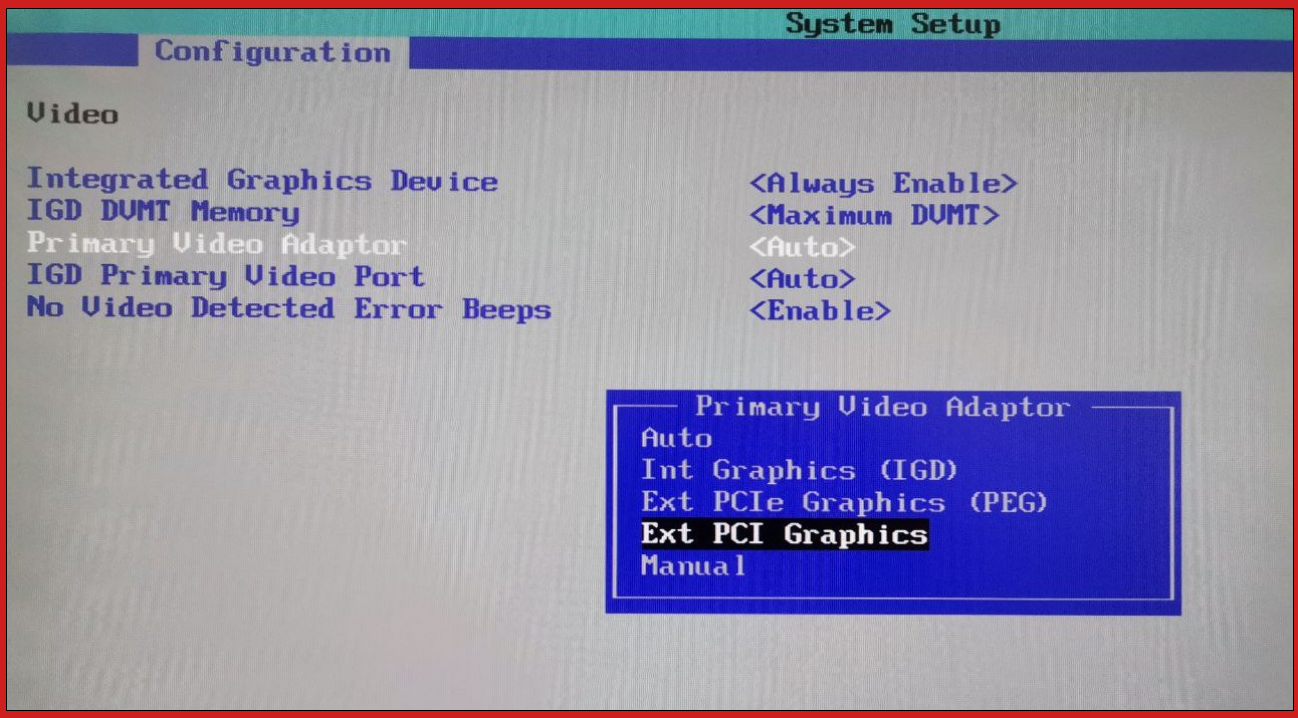
Примечание.

Все устройства и рабочие места нумеруются с нуля (**seat0**, **card0**, **usb0** и т. д.).

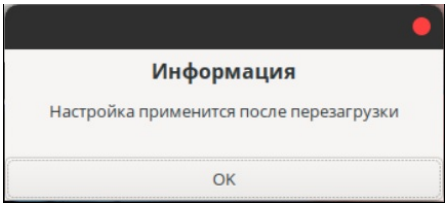
После этого новому рабочему месту необходимо назначить устройства для работы (видеокарту, клавиатуру, мышь и т. д.). Выберите устройство из списка подключенных устройств рабочего места — **seat0** и нажмите кнопку «**Добавить**». В поле «**Рабочее место**» отобразится выбранное устройство. Таким образом поочередно добавьте рабочему месту нужные устройства.

ВАЖНО!

Т.к. все рабочие места создаются на базе видеокарт, необходимо сначала определить, какая видеокарта назначается первой к системе, и закрепить её за местом по умолчанию - **seat0**. Обозначить приоритет загрузки видеокарты можно также в BIOS в разделе «**Primary Video Adaptor**».



После добавления всех необходимых устройств для каждого созданного нового рабочего места нажмите кнопку «**Сохранить**», а затем «**Применить**». Будет выведено следующее информационное окно:



Перезагрузите систему.

Если все настроено верно, созданные рабочие места будут загружены и готовы к работе.

Примечание.

В случае, если вам удалось вытеснить другого пользователя из системы или появилась необходимость удалить рабочее место, откройте утилиту **multiseat** и нажмите кнопку «**Сброс**».

Особенности служб синхронизации времени

Chrony и ntp
Chrony и systemd-timesyncd
Сравнительная таблица

Chrony и ntp

Преимущества **chrony**:

- **chrony** может эффективно работать в среде, где доступ к временной привязке прерывистый, в то время как **ntp** нуждается в регулярном опросе сервера для стабильной работы;
- **chrony** синхронизирует часы быстрее и с большей точностью;
- **chrony** быстро адаптируется к внезапным изменениям частоты тактовых импульсов (например, из-за изменения температуры кварцевого осциллятора). **ntp** может потребоваться много времени, чтобы снова синхронизироваться;
- **chrony** может работать при перегруженной сети, даже если она перегружена длительное время;
- **chrony** никогда не изменяет время в конфигурации по умолчанию, чтобы не нарушать работу других запущенных программ. В **ntp** можно произвести настройку так, чтобы он никогда не изменял время, но в таком случае должны использоваться другие средства настройки часов, что может отрицательно сказаться на точности времени;
- **chrony** использует меньше памяти и задействует процессор только при необходимости, что лучше экономит энергию.

Уникальные особенности **chrony**:

- поддержка механизма аутентификации *Network Time Security* (**NTS**);
- поддержка аппаратно-временной метки в системе для обеспечения стабильной и точной синхронизации в локальной сети;
- просмотр исправленных ошибок в обновлениях для определения скорости, с которой компьютер выигрывает или теряет время, и использования этой оценки для последующего сжатия времени компьютера;
- поддержка определения коэффициента усиления или потери времени, когда компьютер выключен. chrony может использовать эти данные при загрузке системы для установки системного времени на основе исправленной версии часов реального времени.

Уникальные особенности **ntp**:

- поддержка всех режимов работы **RFC 5905**, включая широковещательный, многоадресный и сервер/клиент. Однако широковещательный и многоадресный режимы менее точны и безопасны, чем обычный режим сервер/клиент, и их, как правило, следует избегать;
- поддержка протокола *Autokey* (**RFC 5906**) для аутентификации серверов с помощью криптографии с открытым ключом;
- **ntp** импортирован на различные операционные системы;
- поддержка большого количества драйверов для различных аппаратных эталонных часов.

Chrony и systemd-timesyncd

systemd-timesyncd — служба для синхронизации локальных системных часов с удаленным сервером по протоколу сетевого времени (**NTP**). В отличие от реализации **chrony** **systemd-timesyncd** реализует только клиентскую часть, сосредоточившись на запросе времени с одного удаленного сервера и синхронизации локальных часов с ним.

В systemd-timesyncd также имеются цели, имитирующие общие уровни запуска **SystemVinit**, поэтому можно переключаться между целями, используя команду:

```
telinit <уровень_выполнения>
```

Преимущества **chrony**:

- использование NTP-сервером другого доступного хоста для синхронизации времени;
- получение информации о синхронизации NTP из нескольких источников;
- получение информации о синхронизации с локальных часов.

Chrony — реализует клиентский и серверный режимы полного протокола NTPv4.

Systemd-timesyncd - реализует только клиентский режим протокола **SNTP**, сложные варианты использования не охватываются **systemd-timesyncd**.

Например, SNTP не может сделать его более точным, извлекая время из нескольких источников, как это делает NTP по умолчанию. В результате **systemd-timesyncd** не может обеспечить точную синхронизацию времени, как **chrony**.

Сравнительная таблица служб синхронизации времени

	chrony	**ntp**	**systemd-timesyncd**
Базовая характеристика			
Лицензия	GPLv2	MIT + BSD	CC-BY-SA-3.0
Размер рабочего демона	287 KB	889 KB	192 KB
Источники времени			
NTP	+	+	+
Эталонные часы	+	+	+
Ручной ввод	+	+	+
Отслеживание источника			
Фиксированная фильтрация сэмпла	+	+	+
Адаптивная фильтрация сэмпла	+	-	-
Взвешивание выборки	+	-	-
Отслеживание частоты	+	-	-
Восстановить состояние из файла	+	-	-
Часовая дисциплина			
Независимая регулировка фазы и частоты	+	-	-
Разрешенный случайный интервал обновления	+	-	+
Максимальная скорость нарастания	100000 (настраивается)	500	500
Температурная компенсация	+	-	-
NTP-режимы			
Сервер	+	+	-
Клиент	+	+	+
Сервер трансляции	+	+	-
Клиент трансляции	-	+	+
Чередующийся сервер	+	-	-
Чередующийся клиент	+	-	-
Аутентификация по протоколу NTP			
Симметричный ключ	+	+	-
Автоключ (небезопасный)	-	+	-
Безопасность сетевого времени	+	-	-
MS-SNTP через Samba	+	+	+
Хэш-функции MAC	MD5, SHA-1, SHA-2	MD5, SHA-1, SHA-2	-
Шифры CMAC	AES-128, AES-256	AES-128	-

Установка и настройка ntp

Установка
Настройка
Просмотр статуса

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ntp-4.2.8p13-4

NTP — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Службой **NTP** является **ntpd.service**, она вычисляет отклонения системных часов и регулярно их корректирует.

Преимущества **ntpd**:

- поддержка всех режимов работы RFC 5905, включая широковещательный и многоадресный сервер/клиент;
- поддержка большого количества драйверов для различных аппаратных эталонных часов.

Недостатки **ntpd**:

- необходимость регулярного опроса источника для стабильной работы;
- необходимость некоторого количества времени для синхронизации.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **ntp** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ntp
```

Настройка

Для добавления/удаления серверов необходимо отредактировать конфигурационный файл **/etc/ntp.conf**.

По умолчанию указаны следующие серверы:

```
# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server ntp1.vniiftri.ru
server ntp2.vniiftri.ru
server ntp3.vniiftri.ru
server ntp4.vniiftri.ru
```

Если необходимо добавить собственные адреса серверов, следует заменить строки `ntp[1-4].vniiftri.ru`.

Для применения изменений необходимо перезапустить службу:

```
systemctl restart ntpd
```

Просмотр статуса

Для просмотра дополнительной информации используется ntpq, например:

```
ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 ntp1.vniiftri.r .MRS.           1 u    1   64    1  18.925   -2.210   0.000
 ntp2.vniiftri.r .MRS.           1 u    1   64    1  19.125   -2.105   0.000
 ntp3.vniiftri.r .MRS.           1 u    2   64    1  13.567    0.322   0.000
 ntp4.vniiftri.r .MRS.           1 u    2   64    1  13.947    0.199   0.000
```

Утилита синхронизации времени ntpdate

В РЕД ОС синхронизировать время можно следующими основными способами:

- вручную при помощи утилиты **ntpdate**;
- автоматически при помощи сервиса **ntp**.

Программа **ntpdate** - позволяет разово синхронизировать локальное время с эталонным сервером времени в интернете. Подобных эталонов существует достаточно много. Для примера можно воспользоваться одним из них — **pool.ntp.org**.

Запускаем синхронизацию времени:

```
ntpdate pool.ntp.org
```

Утилита провела синхронизацию, в результате которой к системному времени было добавлено число секунд, необходимое для приближения к эталонному. Если в результате работы синхронизации возникает ошибка: «**no server suitable for synchronization found**», то попробуйте в работе утилиты использовать непривилегированный порт. По-умолчанию ntpdate работает по 123 порту. Если он закрыт на фаерволе, то помочь в синхронизации поможет следующий параметр:

```
ntpdate -u pool.ntp.org
```

Если у вас запуск ntpdate завершается ошибкой — «**the NTP socket is in use, exiting**», значит у вас уже установлена и запущена служба ntpd, которая заняла необходимый udp-порт, необходимый для работы ntpdate.

Сервер времени ntp использует в своей работе одноименный протокол — *Network Time Protocol*, которому для работы необходим UDP-порт 123. Так что перед установкой и настройкой службы времени убедитесь, что на фаерволе открыт этот порт.

Устанавливаем сервер ntp:

```
dnf install ntp
```

Теперь отредактируем файл конфигурации **/etc/ntp.conf**, удалив все лишнее:

```
cat /etc/ntp.conf

driftfile /var/lib/ntp/drift
restrict default nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict ::1

server 0.redos.pool.ntp.org iburst
server 1.redos.pool.ntp.org iburst
server 2.redos.pool.ntp.org iburst
server 3.redos.pool.ntp.org iburst

disable monitor
logfile /var/log/ntp.log
```

Параметры:

server	Список серверов для синхронизации времени.
Driftfile	Задает адрес файла, в котором хранится история изменений времени во время синхронизации. Если по каким-то причинам синхронизация времени с внешними источниками станет невозможна, служба времени изменит системные часы в соответствии с записями в этом файле.
Restrict 127.0.0.1	Указывает, что пользоваться нашим сервером времени можно только непосредственно с локального интерфейса. Если вам необходимо разрешить другим компьютерам в вашей локальной сети синхронизировать время с текущей машины, то укажите в данном параметре адрес вашей сети, например:

restrict 192.168.10.0 mask 255.255.255.0

restrict default nomodify notrap nopeer noquery - Параметры указывают на то, что клиентам данного сервиса времени запрещено изменять его настройки, получать его статус. Они могут только забрать с него значения точного времени.

disable monitor - Данный параметр повышает безопасность, предотвращая использования одной из уязвимостей сервиса ntpd, которую можно использовать для проведения DDoS атак.

Logfile - Указывает путь к файлу с логами сервиса.

После завершения редактирования файла настроек запускаем службу синхронизации времени:

```
systemctl start ntpd
```

Проверяем запустился ли сервер:

```
netstat -tulnp | grep 123
```

Все в порядке, служба слушает положенный порт 123. Проверим на всякий случай системные логи используемой ОС:

```
cat /var/log/messages | grep ntpd
cat /var/log/ntp.log
```

Теперь настроим автозапуск ntp вместе с загрузкой используемой ОС:

```
systemctl enable ntpd
```

Наблюдать за работой службы ntp можно с помощью команды:

```
ntpq -p
```

Данные вывода:

remote	Адрес удаленного эталона времени, с которого была синхронизация.
Refid	Указывает, откуда каждый эталон получает точное время. Это могут быть другие сервера времени, система GPS и другое.
St	Уровень (Stratum) это число от 1 до 16, которое указывает на точность эталона. 1- максимальная точность, 16 — сервер недоступен. Уровень вашего сервера будет равен уровню наименее точного удаленного эталона плюс 1.
poll	Интервал в секундах между опросами.
Reach	Восьмеричное представление массива из 8 бит, отражающего результаты последних восьми попыток соединения с эталоном. Бит выставлен, если удаленный сервер ответил.
Delay	Время задержки ответа на запрос о точном времени.
Offset	Разница между вашим и удаленным сервером
jitter	Дисперсия (Jitter) — это мера статистических отклонений от значения смещения (поле offset) по нескольким успешным парам запрос-ответ. Чем меньше значение дисперсии, тем лучше, поскольку позволяет точнее синхронизировать время.

Установка и настройка chrony

Установка и запуск
Настройка
Управление Chronyd

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** chrony-4.0-5

Chrony – альтернативный клиент и сервер протокола сетевого времени **NTP**. **Chrony** может быстрее синхронизировать системные часы с лучшей точностью времени, и он может быть особенно полезен для систем, которые не работают в сети все время.

Основные преимущества:

- эффективная работа в среде, где доступ к временной связке прерывистый;
- адаптация к внезапным изменениям частоты тактовых импульсов;
- работа в перегруженной сети, даже если перегрузка продолжается длительное время;
- время в конфигурации по умолчанию никогда не изменяется, чтобы не нарушать работу других запущенных программ;
- использование меньшего объема памяти и запуск процессов только при необходимости в целях экономии энергии.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и запуск

Действия по установке и настройке требуется производить под пользователем **root** или пользователем с правами администратора.

Chrony доступен по умолчанию в репозитории РЕД ОС.

Для установки **Chrony** необходимо выполнить следующую команду:

```
dnf install chrony
```

После установки необходимо добавить сервис chronyd.service в автозагрузку и запустить его командой:

```
systemctl enable --now chronyd.service
```

Настройка

Клиенты **NTP** должны знать, с какими серверами **NTP** они должны связаться, чтобы получить текущее время. Серверы **NTP** могут быть указаны в директиве **server** в файле конфигурации **NTP**.

Отредактируйте конфигурационный файл **/etc/chrony.conf** для добавления/удаления серверов.

Данные по умолчанию:

```
# Use public servers from the pool. ntp. org project.
 # Please consider joining the pool (http: //www. pool. ntp. org/join.html).
server ntp1.vniiftri.ru iburst
server ntp2.vniiftri.ru iburst
server ntp3.vniiftri.ru iburst
server ntp4.vniiftri.ru iburst
```

Параметр **iburst** используется для ускорения начальной синхронизации.

Управление Chronyd

Для **chrony** есть утилита командной строки с именем **chronyc** для управления и мониторинга сервиса **chrony (chronyd)**.

Для проверки синхронизации **chrony**, можно использовать команду tracking, как показано ниже:

```
chronyc tracking
```

Вывод должен выглядеть следующим образом:

```
Reference ID    : 596DFB17 (ntp3.vniiftri.ru)
Stratum         : 2
Ref time (UTC)  : Wed May 24 08:18:40 2023
System time     : 0.000260688 seconds fast of NTP time
Last offset     : +0.000226291 seconds
RMS offset      : 0.001286364 seconds
Frequency       : 8.707 ppm slow
Residual freq   : +0.024 ppm
Skew            : 3.054 ppm
Root delay      : 0.016705679 seconds
Root dispersion : 0.000947660 seconds
Update interval : 64.9 seconds
Leap status     : Normal
```

Перечисленные пункты содержат следующую информацию:

- **Reference ID** — идентификатор и имя сервера, с которым компьютер в настоящее время синхронизирован;
- **Stratum** — количество переходов к серверу с установленными эталонными часами;
- **Ref time** — время по Гринвичу, в которое было выполнено последнее измерение из эталонного источника;
- **System time** — задержка системных часов от синхронизированного сервера;
- **Last offset** — расчетное смещение последнего обновления часов;
- **RMS offset** — долгосрочное среднее арифметическое значения смещения;
- **Frequency** — частота, на которой часы системы будут работать неправильно, если хронограф не проведет коррекцию. Она выражена в ppm — ч/м (частей на миллион);
- **Residual freq** — остаточная частота указывает на разницу между измерениями от опорного источника и используемой в настоящее время частотой;
- **Skew** — расчетная погрешность, связанная с погрешностью частоты;
- **Root delay** — суммарная задержка сетевого пути к опорному серверу, с которым синхронизируется компьютер;
- **Leap status** — статус скачка (изменения) времени, который может иметь одно из следующих значений:
- *«Normal»* – означает нормальную корректировку времени;
- *«Insert second»* – означает, что произведена корректировка времени добавлением дополнительной секунды в последнюю минуту текущего месяца;
- *«Delete second»* – означает, что произведена корректировка времени удалением дополнительной секунды из последней минуты текущего месяца;
- *«Not synchronised»* – означает, что компьютер в данный момент времени не синхронизирован.

Также есть возможность проверить текущие источники времени, которые использует **chrony**:

```
chronyc sources
```

Вывод должен выглядеть следующим образом:

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^+ ntp1.vniiftri.ru              1   6   272   271   -264us[ +347us] +/- 7394us
^+ ntp2.vniiftri.ru              1   6   377    77  +2910us[+3321us] +/- 9806us
^* ntp3.vniiftri.ru              1   6   377    13   +848us[+1296us] +/- 6958us
^+ ntp4.vniiftri.ru              1   6   377    11   +895us[ +895us] +/- 6879us
```

Утилита **Chronyc** может находить статистику каждого источника, например, скорость дрейфа и процесс оценки смещения, используя команду **sourcestats**:

```
chronyc sourcestats
```

Вывод должен выглядеть следующим образом:

```
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
==============================================================================
ntp1.vniiftri.ru            7   5   517     -1.228      4.945  -1149us   242us
ntp2.vniiftri.ru            7   5   388     +4.855     22.098  +1466us  1091us
ntp3.vniiftri.ru           11   9   646     +1.307      6.637  -5544ns  1036us
ntp4.vniiftri.ru           11   7   647     +1.544      3.566   +599us   501us
```

Чтобы сообщить **Chrony**, что вы больше не подключены к глобальной сети Интернет, выполните следующие действия:

```
chronyc offline
```

Для проверки статуса источников **NTP**, необходимо запустить следующую команду:

```
chronyc activity
```

Вывод должен выглядеть следующим образом:

```
200 OK
4 sources online
0 sources offline
0 sources doing burst (return to online)
0 sources doing burst (return to offline)
0 sources with unknown address
```

Когда система будет вновь подключена к Интернету, необходимо сообщить об этом **chrony**, используя команду:

```
chronyc online
```

Для более подробного объяснения всех параметров следует руководствоваться *Справочными страницами*.

```
man chronyc
man chronyd
```

Настройка systemd-timesyncd

systemd-timesyncd – это системная служба, которую можно использовать для синхронизации локальных системных часов с удаленным сервером по протоколу сетевого времени (**NTP**). В отличие от служб **chronyd** или **ntpd**, которые могут предоставлять время для клиентов, служба **systemd-timesyncd** реализует только клиентскую часть **SNTP**. Этот сервис способен регулировать системные часы для больших смещений по времени или медленно настраивает их для меньших дельт.

Преимущества:

- реализация только клиентского режима протокола SNMP;
- поддержка большого количества сервисов, многие из которых не являются обязательными, поэтому их можно отключить.

Недостатки:

- сложные варианты использования не охватываются systemd-timesyncd;
- невозможность обеспечения точной синхронизации времени.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Чтобы перейти к настройке службы **systemd-timesyncd** предварительно необходимо проверить статус служб **ntpd** и **chronyd**. Если они запущены (имеют статус active(running)), исключите их из автозапуска с помощью команд:

```
systemctl disable ntpd --now
systemctl disable chronyd --now
```

Такие действия необходимы для корректной синхронизации через **systemd-timesyncd**.

Настройка

Настройка **systemd-timesyncd** производится через файл конфигурации **/etc/systemd/timesyncd.conf**.

Чтобы указать список серверов времени для синхронизации, добавьте в файл **/etc/systemd/timesyncd.conf** в раздел [**Time**] параметр «NTP»:

```
NTP=ntp0.vniiftri.ru ntp1.vniiftri.ru ntp2.vniiftri.ru ntp3.vniiftri.ru
```

Параметр «FallbackNTP» определит список резервных серверов времени:

```
FallbackNTP=ntp1.niiftri.irkutsk.ru
```

В итоге файл конфигурации должен выглядеть примерно следующим образом:

```
[Time]
NTP=ntp0.vniiftri.ru ntp1.vniiftri.ru ntp2.vniiftri.ru ntp3.vniiftri.ru
FallbackNTP=ntp1.niiftri.irkutsk.ru
```

Для применения изменений необходимо перезапустить службу:

```
systemctl restart systemd-timesyncd
```

Для проверки текущего статуса синхронизации времени выполните команду:

```
timedatectl status

               Local time: Ср 2023-05-24 16:21:46 MSK
           Universal time: Ср 2023-05-24 13:21:46 UTC
                 RTC time: Ср 2023-05-24 13:21:46
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
```

```
          RTC in local TZ: no
```

Детальную информацию о состоянии синхронизации времени можно посмотреть командой:

```
timedatectl timesync-status

       Server: 89.109.251.23 (ntp3.vniiftri.ru)
Poll interval: 34min 8s (min: 32s; max 34min 8s)
         Leap: normal
      Version: 4
      Stratum: 1
    Reference: MRS
    Precision: 4us (-18)
Root distance: 167us (max: 5s)
       Offset: -3.099ms
        Delay: 19.587ms
       Jitter: 2.683ms
 Packet count: 14
    Frequency: +3,370ppm
```

Утилита настройки системной локали localectl

Синтаксис
Основные команды
Опции утилиты
Примеры работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: localectl v246.10-17

Locale (локаль) – это региональные настройки операционной системы.

Каждая операционная система поставляется с конкретными региональными настройками. Эти настройки влияют на язык:

- интерфейса;
- сообщений об ошибках;
- справочной информации;
- вывода консольных утилит.

Также локаль влияет на формат чисел, даты и времени, денежной валюты и пр.

Для получения и изменения региональных настроек в РЕД ОС используется утилита командной строки **localectl**. Она позволяет просматривать и настраивать текущую локаль и список доступных раскладок клавиатуры, а также устанавливать новые значения.

Localectl может быть полезна для пользователей, которые работают в многоязычных средах или на компьютерах с разными макетами клавиатуры.

Синтаксис

Синтаксис утилиты имеет вид:

```
localectl [<опции>...] <команда>
```

Основные команды

Команды утилиты:

- **status** – показать текущие настройки локали;
- **set-locale <локаль>** – установить системную локаль;
- **list-locales** – вывести список доступных локалей;
- **set-keymap <раскладка_клавиатуры>** – установить раскладку клавиатуры для консоли;
- **list-keymaps** – вывести доступные раскладки клавиатуры виртуальной консоли;
- **set-x11-keymap <раскладка_клавиатуры>** – установить раскладку для X11;
- **list-x11-keymap-models** – вывести список доступных моделей раскладок для X11;
- **list-x11-keymap-layouts** – вывести список доступных раскладок для X11;
- **list-x11-keymap-variants [<раскладка_клавиатуры>]** – вывести список доступных вариантов раскладок для X11;
- **list-x11-keymap-options** – вывести список доступных опций для раскладок X11.

Опции утилиты

Основные опции утилиты:

- `-h`, `--help` – вывести справочную информацию;

- `--version` – вывести версию утилиты;
- `--no-ask-password` – не запрашивать пароль администратора при выполнении операций, которым необходимы дополнительные привилегии;
- `-H`, `--host=[<имя_пользователя>@]<имя_хоста>[:<порт>]` – выполнить команду на удаленном хосте;
- `-M`, `--machine=<контейнер>` – выполнить операцию в локальном контейнере;
- `--no-convert` – не преобразовывать раскладку клавиатуры из консоли в X11 и наоборот.

Примеры работы

Примеры работы утилиты:

- просмотр текущих настроек локали:

```
localectl

System Locale: LANG=ru_RU.UTF-8
VC Keymap: ru
X11 Layout: ru,us
X11 Variant: ,
X11 Options: grp:alt_shift_toggle
```

- просмотр списка доступных локалей:

```
localectl list-locales

C.UTF-8
aa_DJ.UTF-8
aa_ER.UTF-8
aa_ER.UTF-8@saaho
aa_ET.UTF-8
af_ZA.UTF-8
agr_PE.UTF-8
ak_GH.UTF-8
am_ET.UTF-8
an_ES.UTF-8
anp_IN.UTF-8
ar_AE.UTF-8
...
```

- просмотр списка доступных раскладок клавиатуры:

```
localectl list-keymaps

ANSI-dvorak
al
al-plisi
amiga-de
amiga-us
apple-a1048-sv
apple-a1243-sv
apple-a1243-sv-fn-reverse
apple-internal-0x0253-sv
apple-internal-0x0253-sv-fn-reverse
applkey
...
```

Для добавления поддержки русского языка выполните команду:

```
localectl set-locale LANG=ru_RU.UTF-8
```

Для добавления раскладки клавиатуры выполните следующую команду:

```
localectl set-keymap --no-convert ctrl_shift
```

Пример установки английской и русской раскладки, которые будут переключаться сочетанием клавиш *Ctrl+Shift*:

```
localectl --no-convert set-x11-keymap us,ru "" "" grp:ctrl_shift_toggle
```

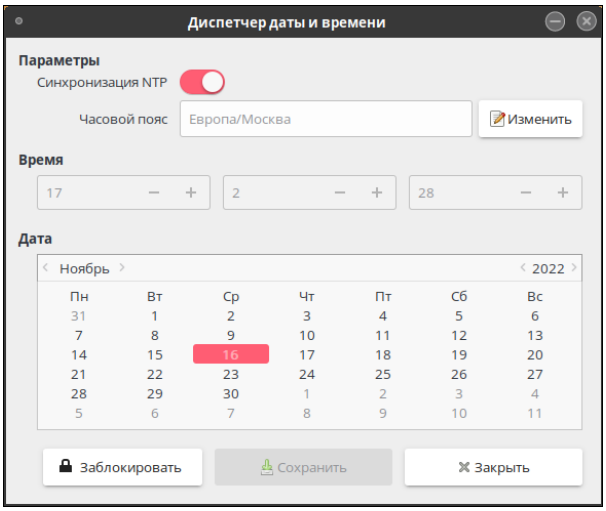
Для применения настроек выполните:

```
systemctl restart display-manager
```

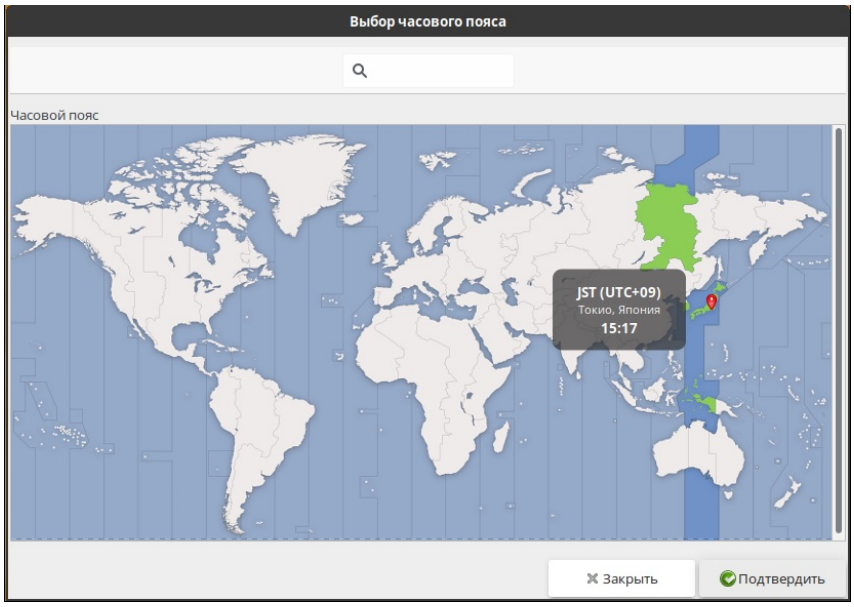
Localectl также может быть использован с другими утилитами командной строки, такими как **systemctl** и **timedatectl**, для управления системными настройками.

Диспетчер настройки даты и времени

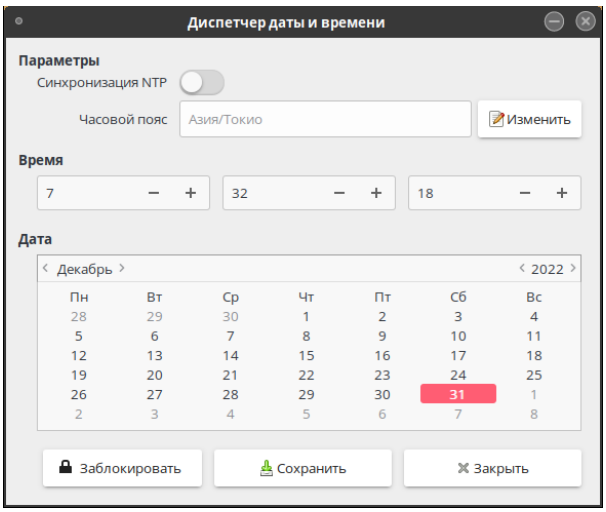
Для настройки даты и времени в РЕД ОС по умолчанию доступна графическая утилита «**Диспетчер даты и времени**», которая располагается в «**Главном меню**» - «**Администрирование**» - «**Дата и время**».



По умолчанию включена синхронизация по NTP, поэтому настройка даты и времени вручную отключена, доступна только смена часового пояса.



Для изменения настроек отключите синхронизацию по NTP, выберите часовой пояс, установите время и дату, для применения изменений нажмите кнопку «**Сохранить**».



Утилита настройки даты и времени system-config-date

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: system-config-date-1.10.6-6

System-config-date также является графической утилитой для настройки системной даты и времени, однако, в отличие от стандартного *Диспетчера*, функционал данной утилиты шире.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

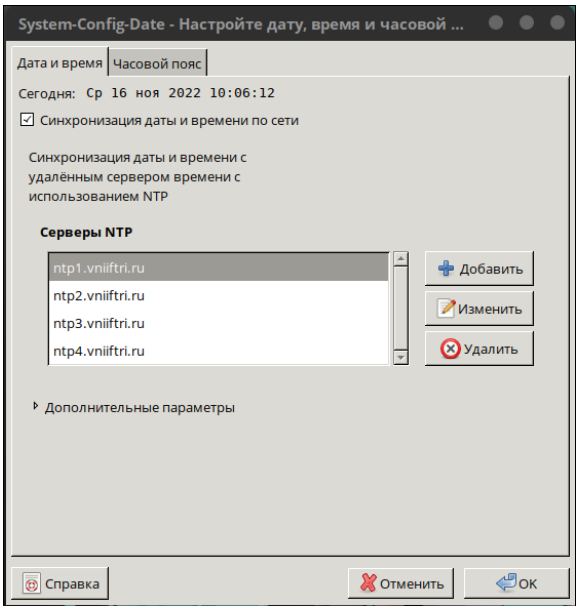
Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

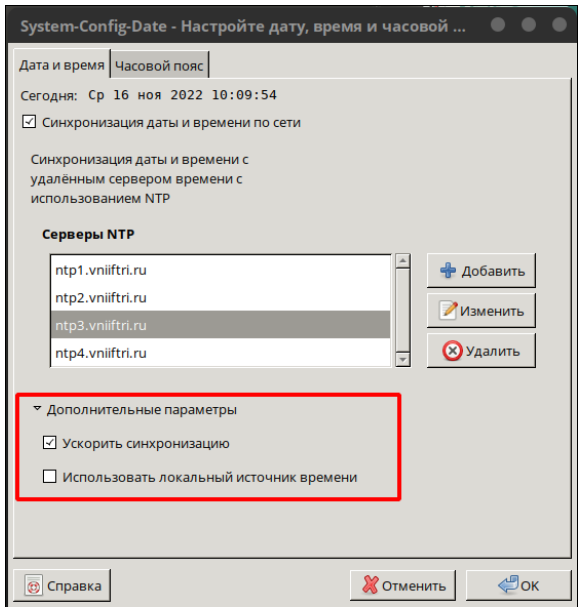
```
dnf install system-config-date
```

После установки программа доступна из «**Главного меню**» - «**Администрирование**» - «**System-Config-Date**».

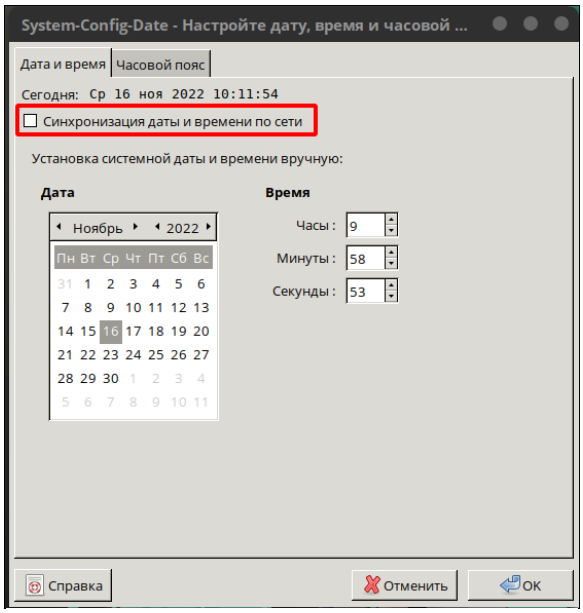


На вкладке **Дата и время** есть возможность включить/отключить **Синхронизацию даты и времени по сети**.

При включенной синхронизации можно настроить **Серверы NTP** — добавить новые серверы для синхронизации времени, изменить или удалить существующие. В **Дополнительных параметрах** можно ускорить синхронизацию и использовать локальный источник времени.



При выключенной синхронизации установка системной даты и времени производится вручную.

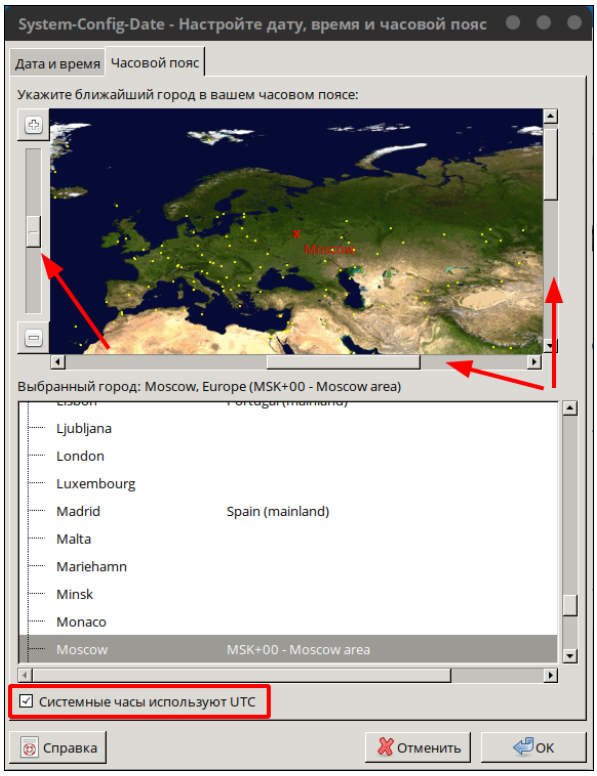


Для применения изменений нажмите «**OK**».

На вкладке **Часовой пояс** доступен выбор необходимого часового пояса на карте или в списке.

Для навигации по карте используются вертикальная и горизонтальная полосы прокрутки. Для изменения масштаба можно использовать кнопки «**+**» и «**-**» слева от карты либо колесико мыши.

Также доступна настройка использования UTC — функции автоматического перехода с зимнего на летнее время.



Для применения установленных настроек нажмите «**OK**».

Утилита настройки даты и времени timedatectl

Изменение часового пояса
Изменение даты и времени
Графические утилиты настройки даты и времени

Изменение часового пояса

Для подробного вывода информации об установленных дате, времени и выбранном часовом поясе, а также их настройке, используется утилита **timedatectl**.

Просмотр текущих настроек осуществляется командой:

```
timedatectl

               Local time: Вт 2022-11-15 11:36:46 MSK
           Universal time: Вт 2022-11-15 08:36:46 UTC
                 RTC time: Вт 2022-11-15 08:36:46
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

здесь:

- **Local time** (местное время) — это время, которое применяется в определенном географическом регионе или месте. Оно основано на солнечном времени и связано с часовым поясом данной местности;
- **Universal time** (универсальное время) — известно также как координированное всемирное время (UTC), универсальное время является международным стандартом времени, применяемым во всем мире. UTC не зависит от географического положения и не имеет смещения;
- **RTC time** (Real-Time Clock time) — это время, которое хранится во встроенных часах реального времени (RTC) компьютера или устройства. RTC используется для отслеживания текущего времени, даже когда устройство отключено от источника питания. **RTC time** используется при запуске системного времени и может быть синхронизировано с локальным временем операционной системы.
- **Time Zone** — установленная временная зона или часовой пояс;
- **System clock synchronized** — синхронизация системного времени с сервером **ntp**, принимает значения - *yes* (синхронизация производится) и *no* (синхронизация отключена);
- **NTP service** — доступность службы **ntp**;
- **RTC in local TZ** — синхронизация RTC с локальным временем операционной системы, принимает значения - *yes* (синхронизация производится) и *no* (синхронизация отключена).

Если часовой пояс указан неверно, его можно задать без перезагрузки системы с помощью команды:

```
tzselect

Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
 1) Africa
 2) Americas
 3) Antarctica
 4) Asia
 5) Atlantic Ocean
 6) Australia
 7) Europe
 8) Indian Ocean
 9) Pacific Ocean
10) coord - I want to use geographical coordinates.
11) TZ - I want to specify the time zone using the Posix TZ format.

#? 7
```

Будет предложено выбрать континент (в данном случае выбран вариант **7 - Europe**).

Затем потребуется выбрать страну (в примере выбран вариант **38 - Russia**) и регион (в примере выбран вариант **23 - Magadan**).

```
Please select a country whose clocks agree with yours.
```

```
 1) Albania    18) Guernsey      35) Poland
 2) Andorra    19) Hungary       36) Portugal
 3) Austria    20) Ireland       37) Romania
 4) Belarus    21) Isle of Man   38) Russia
 5) Belgium    22) Italy         39) San Marino
 6) Bosnia & Herzegovina  23) Jersey      40) Serbia
 7) Britain (UK)   24) Latvia      41) Slovakia
 8) Bulgaria    25) Liechtenstein    42) Slovenia
 9) Croatia    26) Lithuania     43) Spain
10) Czech Republic   27) Luxembourg    44) Svalbard & Jan Mayen
11) Denmark    28) Malta      45) Sweden
12) Estonia    29) Moldova       46) Switzerland
13) Finland    30) Monaco        47) Turkey
14) France    31) Montenegro     48) Ukraine
15) Germany    32) Netherlands    49) Vatican City
16) Gibraltar    33) North Macedonia    50) Åland Islands
17) Greece    34) Norway
#? 38

Please select one of the following time zone regions.
 1) MSK-01 - Kaliningrad  15) MSK+04 - Kemerovo
 2) MSK+00 - Moscow area  16) MSK+04 - Krasnoyarsk area
 3) Crimea    17) MSK+05 - Irkutsk, Buryatia
 4) MSK+00 - Kirov    18) MSK+06 - Zabaykalsky
 5) MSK+01 - Astrakhan    19) MSK+06 - Lena River
 6) MSK+01 - Volgograd    20) MSK+06 - Tomponsky, Ust-Maysky
 7) MSK+01 - Saratov    21) MSK+07 - Amur River
 8) MSK+01 - Ulyanovsk    22) MSK+07 - Oymyakonsky
 9) MSK+01 - Samara, Udmurtia  23) MSK+08 - Magadan
10) MSK+02 - Urals    24) MSK+08 - Sakhalin Island
11) MSK+03 - Omsk    25) MSK+08 - Sakha (E); North Kuril Is
12) MSK+04 - Novosibirsk  26) MSK+09 - Kamchatka
13) MSK+04 - Altai    27) MSK+09 - Bering Sea
14) MSK+04 - Tomsk
#? 23
```

После этого будет предложено проверить установленные параметры и, если все верно, подтвердить свой выбор.

```
The following information has been given:

 Russia
 MSK+08 - Magadan

Therefore TZ='Asia/Magadan' will be used.
Selected time is now: Tue Nov 15 19:38:15 +11 2022.
Universal Time is now: Tue Nov 15 08:38:15 UTC 2022.
Is the above information OK?
1) Yes
2) No
#? 1

You can make this change permanent for yourself by appending the line
 TZ='Asia/Magadan'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
Asia/Magadan
```

Далее для применения настроек перейдите в домашний каталог пользователя (в примере **/home/user/**) и создайте файл **.profile**:

```
cd /home/user/
nano .profile
```

Добавьте в него строку, указанную в выводе команды `tzselect` (выделена зеленым цветом):

```
TZ='Asia/Magadan'; export TZ
```

Сохраните изменения в файле и перезапустите сеанс пользователя.

Еще один способ изменения часового пояса доступен через утилиту **timedatectl**. Список доступных часовых поясов выводится командой:

```
timedatectl list-timezones
```

Чтобы выбрать нужный часовой пояс, используется команда:

```
timedatectl set-timezone <часовой_пояс>
```

Например:

```
timedatectl set-timezone America/Los_Angeles
timedatectl status

               Local time: Чт 2022-01-13 04:05:00 PST
           Universal time: Чт 2022-01-13 12:05:00 UTC
                 RTC time: Чт 2022-01-13 12:05:00
                Time zone: America/Los_Angeles (PST, -0800)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Изменение даты и времени

Для изменения даты и времени используется команда:

```
timedatectl -- set-time "<дата> <время>"
```

Однако при попытке вноса изменений может возникнуть следующая ошибка:

```
timedatectl -- set-time "2002-08-28 00:00:00"

Failed to set time: Automatic time synchronization is enabled
```

Она означает, что в системе включена автоматическая синхронизация. Отключить ее можно следующей командой:

```
timedatectl set-ntp no
```

Проверка статуса синхронизации:

```
timedatectl status

               Local time: Ср 2002-08-28 00:00:03 MSD
           Universal time: Вт 2002-08-27 20:00:03 UTC
                 RTC time: Вт 2002-08-27 20:00:04
                Time zone: Europe/Moscow (MSD, +0400)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

После этого необходимо повторить запрос на изменение даты и времени. Чтобы убедиться, что изменения вступили в силу, можно еще раз вывести статус настроек:

```
timedatectl -- set-time "2002-08-28 00:00:00"
timedatectl status

               Local time: Ср 2002-08-28 00:00:03 MSD
           Universal time: Вт 2002-08-27 20:00:03 UTC
                 RTC time: Вт 2002-08-27 20:00:04
                Time zone: Europe/Moscow (MSD, +0400)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

С помощью данной команды дату и время можно изменять как в совокупности, так и отдельно. Для этого в команде следует указывать только один из параметров.

```
timedatectl -- set-time "2002-08-28"

  или

timedatectl -- set-time "15:30:00"
```

Графические утилиты настройки даты и времени

Подробную информацию о смене часового пояса и настройке системных даты и времени в графических утилитах см. в инструкциях «Диспетчер даты и времени» и «system-config-date».

Настройка и использование systemd-таймеров

Системные таймеры и чтение информации о них
Примеры использования таймеров
Создание таймеров
Преимущества и недостатки работы с таймерами

Таймеры — файлы юнитов **systemd**, имя которых имеет суффикс **.timer**; они позволяют контролировать файлы **.service** или определенные события. Эти таймеры могут быть использованы в качестве замены **cron**. Таймеры имеют встроенную поддержку календарных и регулярных событий и могут запускаться в асинхронном режиме.

Вы можете подробнее ознакомиться с созданием и настройкой systemd-таймеров, просмотрев наши обучающие видео:

- на **RuTube** — Настраиваем таймеры systemd вместо заданий cron;
- в **Яндекс.Дзен** — Настраиваем таймеры systemd вместо заданий cron;
- в **VK Видео** — Настраиваем таймеры systemd вместо заданий cron.

На наших каналах вы также сможете найти много другой полезной информации.

Системные таймеры и чтение информации о них

Когда система РЕД ОС устанавливается на компьютер, создается несколько системных таймеров, являющихся частью процедур обслуживания системы.

Чтобы увидеть, какие таймеры работают на данный момент, введите команду:

```
systemctl status *timer

● dnf-makecache.timer - dnf makecache --timer
     Loaded: loaded (/usr/lib/systemd/system/dnf-makecache.timer; enabled; vendo
     Active: active (waiting) since Thu 2022-06-23 10:03:35 MSK; 4h 37min ago
    Trigger: Thu 2022-06-23 15:18:12 MSK; 37min left
   Triggers: ● dnf-makecache.service

июн 23 10:03:35 localhost.localdomain systemd[1]: Started dnf makecache --timer.

● sysstat-summary.timer - Generate summary of yesterday's process accounting
     Loaded: loaded (/usr/lib/systemd/system/sysstat-summary.timer; enabled; ven
     Active: active (waiting) since Thu 2022-06-23 10:03:35 MSK; 4h 37min ago
    Trigger: Fri 2022-06-24 00:07:00 MSK; 9h left
   Triggers: ● sysstat-summary.service

июн 23 10:03:35 localhost.localdomain systemd[1]: Started Generate summary of ye

● systemd-tmpfiles-clean.timer - Daily Cleanup of Temporary Directories
     Loaded: loaded (/usr/lib/systemd/system/systemd-tmpfiles-clean.timer; stati
     Active: active (waiting) since Thu 2022-06-23 10:03:35 MSK; 4h 37min ago
    Trigger: Fri 2022-06-24 10:19:11 MSK; 19h left
   Triggers: ● systemd-tmpfiles-clean.service
       Docs: man:tmpfiles.d(5)
             man:systemd-tmpfiles(8)

июн 23 10:03:35 localhost.localdomain systemd[1]: Started Daily Cleanup of Tempo

● sysstat-collect.timer - Run system activity accounting tool every 10 minutes
     Loaded: loaded (/usr/lib/systemd/system/sysstat-collect.timer; enabled; ven
     Active: active (waiting) since Thu 2022-06-23 10:03:35 MSK; 4h 37min ago
    Trigger: Thu 2022-06-23 14:50:00 MSK; 9min left
   Triggers: ● sysstat-collect.service

июн 23 10:03:35 localhost.localdomain systemd[1]: Started Run system activity ac
```

С каждым таймером связано, по меньшей мере, шесть строк, содержащих сведения о нём:

1. Имя файла таймера и короткое описание цели существования этого таймера (но не всегда).
2. Сведения о состоянии таймера - загружен ли таймер, полный путь к файлу таймера, состояние **vendor preset** (**disabled** или

enabled).

3. Сведения об активности таймера, куда входят данные о том, когда именно таймер был активирован.
4. Дата и время следующего запуска таймера и примерное время, оставшееся до его запуска.
5. Имя сервиса или события, вызываемого таймером.
6. Некоторые (но не все) таймеры содержат указатели на документацию.

Примеры использования таймеров

Самым простым примером использования таймеров можно считать системный таймер **systemd-tmpfiles-clean**. Как следует из названия, данный таймер раз в некоторое время производит очистку временных файлов системы.

```
● systemd-tmpfiles-clean.timer - Daily Cleanup of Temporary Directories
   Loaded: loaded (/usr/lib/systemd/system/systemd-tmpfiles-clean.timer; stati
   Active: active (waiting) since Thu 2022-06-23 10:03:35 MSK; 4h 37min ago
  Trigger: Fri 2022-06-24 10:19:11 MSK; 19h left
 Triggers: ● systemd-tmpfiles-clean.service
     Docs: man:tmpfiles.d(5)
           man:systemd-tmpfiles(8)
```

Данный таймер является системным и включен по умолчанию.

Создание таймеров

В системе РЕД ОС юниты **systemd** располагаются в следующих директориях:

- **/usr/lib/systemd/system** – юниты, поставляемые вместе с системой и устанавливаемыми приложениями;
- **/etc/systemd/system** – юниты системного администратора.

Для примера будет создан простой файл конфигурации сервиса, запускающий команду **free** (утилита, выводящая информацию об использовании оперативной памяти). Это может пригодиться, если необходимо регулярно отслеживать объём свободной памяти.

Создайте **unit**-файл с именем **ramMonitor.service** в папке **/etc/systemd/system**.

```
nano /etc/systemd/system/ramMonitor.service
```

И добавьте в него следующие строки:

```
[Unit]
Description=Monitors RAM # Описание сервиса
Wants=ramMonitor.timer # Зависимость, отсылается к таймеру (будет создан позже)

[Service]
Type=oneshot # Тип службы, означающий выполнение одного задания и завершение
ExecStart=/usr/bin/free # Указывается полный путь к исполняемому файлу программы

[Install]
WantedBy=multi-user.target # Указывается, на каком уровне происходит запуск сервиса. Параметр multi-user.target указывает на запуск в многопользовательском режиме без графики
```

Данный файл можно назвать простейшим файлом конфигурации сервиса.

После проведенных манипуляций, проверьте состояние вашего сервиса командой:

```
systemctl status ramMonitor.service

● ramMonitor.service - Monitors RAM
   Loaded: loaded (/etc/systemd/system/ramMonitor.service; disabled; vendor pr
   Active: inactive (dead)
```

Сервис существует, но не активен. Запустите сервис и проверьте его статус:

```
systemctl start ramMonitor.service
systemctl status ramMonitor.service

● ramMonitor.service - Monitors RAM
   Loaded: loaded (/etc/systemd/system/ramMonitor.service; disabled; vendor pr
   Active: inactive (dead)

июн 23 15:08:44 localhost.localdomain systemd[1]: Starting Monitors RAM...
июн 23 15:08:44 localhost.localdomain systemd[1]: ramMonitor.service: Succeeded.
июн 23 15:08:44 localhost.localdomain systemd[1]: Finished Monitors RAM.
июн 23 15:08:44 localhost.localdomain free[3914]:               total        use
июн 23 15:08:44 localhost.localdomain free[3914]: Mem:         995784      53659
июн 23 15:08:44 localhost.localdomain free[3914]: Swap:       2097148        927
```

При включении сервиса в терминале не выводится никаких сообщений. Это происходит, потому что по умолчанию стандартный вывод (**stdout**) от программ, запускаемых **systemd**, перенаправляется в журнал **systemd**.

Чтобы проверить этот журнал, воспользуйтесь командой:

```
journalctl -u ramMonitor.service

-- Logs begin at Thu 2022-04-21 11:49:59 MSK, end at Thu 2022-06-23 15:12:30 MSK
июн 23 15:08:44 localhost.localdomain systemd[1]: Starting Monitors RAM...
июн 23 15:08:44 localhost.localdomain systemd[1]: ramMonitor.service: Succeeded.
июн 23 15:08:44 localhost.localdomain systemd[1]: Finished Monitors RAM.
июн 23 15:08:44 localhost.localdomain free[3914]:               total        use
июн 23 15:08:44 localhost.localdomain free[3914]: Mem:         995784      53659
июн 23 15:08:44 localhost.localdomain free[3914]: Swap:       2097148        927
```

С помощью ключа -S вы можете указать временной период, за который утилита **journalctl** будет искать записи. Например, `journalctl -S today -u ramMonitor.service` выведет записи, сделанные за сегодня.

Убедившись в работоспособности сервиса, создайте для него таймер. Для этого необходимо создать в той же папке файл с названием ramMonitor.timer.

```
nano /etc/systemd/system/ramMonitor.timer
```

В файл добавьте следующее содержимое:

```
[Unit]
Description=Monitors RAM
Requires=ramMonitor.service # Указание строгой зависимости

[Timer]
Unit=ramMonitor.service # Ссылка на сервис
OnCalendar=*-*-* *:*:00 # Срабатывание таймера по условию календаря. В данном случае – каждую минуту

[Install]
WantedBy=timers.target
```

В секции **[Timer]** указываются условия запуска. Таймеры могут быть двух типов: событийные и монотонные. Первые активируются по событию, вторые выполняются периодически. Из событий таймеров можно выделить **OnBootSec**, срабатывающий через определенное время после запуска системы. Из монотонных следует выделить:

- **OnUnitActiveSec** - срабатывает через указанное время после активации целевого юнита;
- **OnUnitInactiveSec** — срабатывает так же, как **OnUnitActiveSec**, только время отсчитывается с момента прекращения работы целевого юнита, хорошо подходит для «длительных» задач, например, бекапов.
- **OnCalendar** - срабатывает по условию календаря.

В качестве формата даты для календаря используется формат:

```
DOW YYYY-MM-DD HH:MM:SS
```

(где **DOW** – **D**ay **O**f **W**eek – *день недели*, необязательный параметр; за ним следует указание *года*, *месяца*, *дня* через дефис и *часы*, *минуты* и *секунды* через двоеточие. Для указания любого значения используется «*», перечисления делаются через запятую, а

диапазоны через «**..**»).

После завершения настройки нужно запустить таймер и проверить его статус:

```
systemctl start ramMonitor.timer
systemctl status ramMonitor.timer

● ramMonitor.timer - Monitors RAM
     Loaded: loaded (/etc/systemd/system/ramMonitor.timer; disabled; vendor pres
     Active: active (waiting) since Thu 2022-06-23 15:16:22 MSK; 7s ago
    Trigger: Thu 2022-06-23 15:17:00 MSK; 29s left
   Triggers: ● ramMonitor.service

июн 23 15:16:22 localhost.localdomain systemd[1]: Started Monitors RAM.
```

Если все настроено верно, таймер будет иметь состояние **active (waiting)**, а ниже будет указано время до его запуска.

Преимущества и недостатки работы с таймерами

Основные преимущества:

- Задачи могут быть легко запущены сразу, независимо от их таймеров - это упрощает отладку.
- Каждая задача может быть настроена для работы в определенной среде.
- Задачи могут быть настроены в зависимости от других юнитов **systemd**.
- Задачи регистрируются в журнале **systemd**.

Единственным недостатком можно считать сложность создания таких таймеров: чтобы настроить задачу, запускаемую в определенное время при помощи **systemd**, нужно создать два файла и использовать команды **systemctl**. По сравнению с добавлением одной строки в crontab. Кроме того в **systemd** отсутствует встроенный аналог *cron*'овского **MAILTO** для отправки писем при сбоях.

Планировщик заданий crontab

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Crontab - таблицы, управляющие работой службы **cron**. Файл содержит инструкции службы *cron* в общей форме: запускать указанную команду в заданное время и в заданные дни. На компьютере обычно имеются общесистемный файл (**/etc/crontab**) и индивидуальные файлы (**/var/spool/cron/**) для пользователей системы. Таким образом, команды в файле будут выполняться с правами этих пользователей или, в случае общесистемного файла, с правами пользователя, указанного в командной строке при запуске службы. У служб **Uucp** и **News** обычно есть свои собственные *crontab*, устраняющие необходимость в явном запуске **su** в рамках команды *cron*.

> **Примечание!** Хотя **cron**, по сути, является обыкновенным текстовым файлом, он не должен редактироваться обычными средствами. Для создания, изменения и удаления следует использовать специальную утилиту - **crontab**.

Вы можете подробнее ознакомиться с работой службы **cron**, просмотрев наши обучающие видео:

- на **RuTube** — Планировщик задач в РЕД ОС. Cron;
- в **Яндекс.Дзен** — Планировщик задач в РЕД ОС. Cron;
- в **VK Видео** — Планировщик задач в РЕД ОС. Cron.

На наших каналах вы также сможете найти много другой полезной информации.

Пустые строки, ведущие пробелы и символы табуляции игнорируются. Строки, начинающиеся с символа «**#**», считаются комментариями и игнорируются. Заметьте, что комментарии не допускаются в тех же строках, где расположены команды *cron*, так как они будут распознаны как части команды. По этой же причине комментарии не разрешены в строках, задающих переменные среды.

Строка-директива представляет собой либо задание переменной среды, либо команду *cron*.

Задание переменной среды:

Можно определять среду (набор переменных среды), в которой будет выполняться команда. Задание переменной среды осуществляется в следующей форме:

```
<имя_переменной> = <значение>
```

где пробелы вокруг знака равенства («**=**») не обязательны, и любые пробелы после будут использованы как часть значения переменной . Строка может быть заключена в кавычки (одинарные или двойные) для возможности сохранения пробелов в начале и конце.

Несколько переменных среды устанавливаются автоматически службой *cron*. SHELL устанавливается в /**bin/sh**, а **LOGNAME** и **HOME** определяются по файлу **/etc/passwd** (в соответствии с владельцем *crontab*). Значения переменных HOME и SHELL можно переопределить директивами crontab.

В дополнение к *LOGNAME, HOME и SHELL* cron может использовать переменную **MAILTO** в случаях, если в данном crontab была указана отправка почты. Если MAILTO определена (и не пуста), электронная почта отправляется указанному в переменной пользователю. Если MAILTO определена, но пустая (MAILTO = ' '), электронная почта отправляться не будет. В противном случае, почта посылается владельцу crontab. Эта переменная полезна при запуске команд от псевдопользователей, для которых не определены почтовые адреса в системе.

Команды cron:

Существует две конфигурации cron: системная и пользовательская. Общесистемная настройка crontab работает безусловно для всех пользователей РЕД ОС. Пользовательская настройка является дополнительной и выполняется в сессиях пользователей.

Для редактирования файла необходимо ввести команду:

```
crontab -e
```

Для просмотра содержимого расписания:

```
crontab -l
```

Каждая стока в системной конфигурации cron, расположенной в каталоге **/etc**, состоит из шести полей и команды:

```
<минута> <час> <число> <месяц> <день_недели> <пользователь> <команда>
```

Каждая строка в пользовательской конфигурации cron, расположенной в домашнем каталоге пользователя, состоит из пяти полей и команды:

```
<минута> <час> <число> <месяц> <день_недели> <команда>
```

Поля отделяются друг от друга пробелами или символами табуляции. Команда может состоять из нескольких полей. Допустимые значения полей:

Поле	Допустимые значения
<минута>	* или 0-59
<час>	* или 0-23
<число>	* или 1-31
<месяц>	*, 1-12 или имя месяца (см. ниже)
<день_недели>	*, 0-7 или имя дня (воскресенье - это 0 и 7)
<пользователь>	имя существующего пользователя
<команда>	строка

Допустимо указание нескольких значений (и диапазонов через тире) через запятую. Примеры:

' '1 , 2, 5 , 9' ' ' '0-4, 8-12' '.

Диапазон указывается как два числа, разделенных дефисом. Указываемые числа включаются в диапазон. Например, значение поля <час> 8-11 приведёт к выполнению команды в 8, 9, 10 и 11 часов.

При указании диапазона можно пропускать некоторые его значения, указав шаг в форме **/<число>**. Например: «0-23/2» для поля означает запуск команды через два часа (по стандарту V7 пришлось бы указывать «0,2,4,6,8,10,12,14,16,18,20,22»). Шаг можно указывать также после звёздочки: «каждые два часа» соответствует значению «*/2».

Звёздочка («*****») без шага соответствует полному диапазону значений.

Для задания полей <месяц> и <день_недели> и можно использовать имена. Указывайте первые три буквы нужного дня или месяца на английском, регистр букв не имеет значения. Диапазоны или списки имён не разрешены.

Поле <команда> (остаток строки) определяет запускаемую по расписанию команду. Вся оставшаяся часть строки до символа перевода строки или символа «%», будет выполнен вызов **/bin/sh** или другой оболочки, определенной в переменной SHELL в crontab. Знак процента («%») в команде (если он не экранирован обратной косой чертой («\»)) будет соответствовать символу перевода строки и все данные после первого «%» будут посланы для команды на стандартный ввод.

Служба cron запускает команды, когда значения полей <минута>, <час>, <месяц> и хотя бы одно из полей <число> и <день_недели>, совпадают с текущим временем (см. замечание ниже). Служба cron сверяет директивы с текущим временем раз в минуту.

ЗАМЕЧАНИЕ

День выполнения команды может быть задан в двух полях - <число> и <день_недели>. Если оба поля определены (т.е. не равны «*»), то команда будет запущена, когда любое поле совпадёт с текущим временем. Например, запись:

30 4 1,15 * 5

приведёт к выполнении команды в 4:30 по полуночи первого и пятнадцатого числа каждого месяца, плюс в каждую пятницу.

Вместо первых пяти полей допустимо указание одного из восьми специальных триггеров:

Строка	Значение
@reboot	Выполнить команду один раз, при запуске cron(8).
@yearly	Выполнять команду каждое 1 января, "0 0 1 1*"
@annually	(эквивалентно @yearly).
@monthly	Выполнять команду в начале каждого месяца, "0 0 1 * *"
@weekly	Выполнять команду каждое воскресенье, "0 0 * * 0".
@daily	Выполнять команду в полночь, "0 0 * * *".
@midnight	(эквивалентно @daily).
@hourly	Выполнять команду раз в час, "0 * * * *".

Планировщик заданий at

Отправка задач с помощью at
Непосредственный ввод команд
Запуск скрипта
Утилита atq
Указание очереди
Формат ввода даты
Утилита atrm
Файлы конфигурации

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** at-3.1.23-1

Бывают ситуации, когда необходимо однократно выполнить команды или скрипт в определённое время. Такую задачу можно решить с помощью планировщика **at**, представленного службой **atd**.

Для использования службы **atd** сначала необходимо ее запустить:

```
systemctl start atd
```

Проверить статус службы можно командой:

```
systemctl status atd
```

Обратите внимание, что служба **atd** не имеет связанного терминала. Одной из определяющих характеристик службы **atd** является то, что она отказывается от связи с терминалом, который ее запустил.

Вы можете подробнее ознакомиться с настройкой утилиты **at**, просмотрев наши обучающие видео:

- на **RuTube** — Планировщик задач в РЕД ОС. Команда at;
- в **Яндекс.Дзен** — Планировщик задач в РЕД ОС. Команда at;
- в **VK Видео** — Планировщик задач в РЕД ОС. Команда at.

На наших каналах вы также сможете найти много другой полезной информации.

Отправка задач с помощью at

Команда **at** используется для отправки заданий и запуска в определенное время сервису **atd**. Задания, созданные с помощью **at** , выполняются только один раз.

Подробную информацию об утилите можно посмотреть с помощью команды:

```
man at
```

Справка по использованию утилиты доступна при выполнении команды:

```
at --help
```

Непосредственный ввод команд

Если выполнить **at** только с указанием времени, он предложит ввести необходимые к выполнению команды с помощью стандартного ввода (клавиатуры). После ввода последовательности команд нажмите сочетание клавиш «**Ctrl+D**», чтобы выйти и сохранить задание. При вводе непосредственно с терминала «**Ctrl+D**» указывает на "конец файла".

```
at 8:22

warning: commands will be executed using /bin/sh
at> echo "$(date)" > /home/user/at.txt
```

```
at>
job 1 at Thu Dec  8 08:22:00 2022
```

Запуск скрипта

Если необходимо разово в определенное время запустить скрипт, тогда кроме нужного времени потребуется указать путь к файлу сценария, используя ключ **-f**. Можно дополнительно указать ключ **-m**, чтобы получить системное сообщение на почту при любом исходе выполнения команды.

```
at -f <имя_файла> -m <время>
```

Например:

```
at -f /home/user/at.sh -m 10:30

warning: commands will be executed using /bin/sh
job 4 at Thu Dec  8 10:30:00 2022
```

Утилита atq

Проверка установленного для исполнения задач порядка и времени может осуществляться с помощью утилиты **atq** или команды `at -l`.

```
atq

2 Wed Dec  7 16:45:00 2022 a user
4 Thu Dec  8 10:30:00 2022 a user
1 Thu Dec  8 08:22:00 2022 a user
3 Thu Dec  8 10:30:00 2022 a user
```

В выводе перечислены все задания, по одному в каждой строке. Каждая строка включает *номер* задания, *дату*, *время*, *букву* очереди и *имя пользователя*.

Указание очереди

По умолчанию задания, созданные с помощью **at**, планируются в очереди с именем «**a**».

Запросы могут иметь имена от «**a**» ... «**z**» до «**A**» ... «**Z**». Очереди со строчными буквами имеют приоритет над очередями с прописными буквами.

Вы можете указать очередь с помощью опции **-q**. Например, чтобы установить задание в **M**-очередь, необходимо выполнить команду вида:

```
at monday +2 hours -q M
at -f /home/user/at.sh 10:30 -q M
atq

2 Wed Dec  7 16:45:00 2022 a user
5 Mon Dec 12 15:32:00 2022 M user
4 Thu Dec  8 10:30:00 2022 a user
1 Thu Dec  8 08:22:00 2022 a user
6 Thu Dec  8 10:30:00 2022 M user
3 Thu Dec  8 10:30:00 2022 a user
```

Формат ввода даты

При формировании команды необходимо указывать время запуска, однако также предусмотрено указание и даты.

Если дата не указана, то принимается текущая, а если указанное время в текущий день уже прошло, задача планируется на следующий день.

Время дня можно указать в формате **ЧЧ:ММ** с суффиксом «**am**» или «**pm**». Также могут использоваться термины «**midnight**», «**noon**», и «**teatime**».

Дата также может быть указана в нескольких форматах, включая **ММ/ДД/ГГ**.

Более подробное описание команды можно найти на странице справки:

```
man at
```

Утилита atrm

Запланированные к исполнению задачи могут быть удалены из очереди с помощью утилиты `atrm` или `at -r`. Для этого достаточно ввести команду и указать номер запланированной задачи.

Например:

```
atrm 5
atq

2 Wed Dec  7 16:45:00 2022 a user
4 Thu Dec  8 10:30:00 2022 a user
1 Thu Dec  8 08:22:00 2022 a user
6 Thu Dec  8 10:30:00 2022 M user
3 Thu Dec  8 10:30:00 2022 a user
```

Файлы конфигурации

Можно использовать файлы конфигурации **/etc/at.allow** и **/etc/at.deny** для четкого указания пользователей, которые могут или не могут планировать исполнение задач с помощью службы **atd**.

Файл **/etc/at.allow** содержит список пользователей, которым позволено осуществлять планирование исполнения задач с помощью службы **atd**. В том случае, если файла **/etc/at.allow** не существует, служба **atd** может использоваться любым пользователем, имя которого не внесено в файл **/etc/at.deny**.

Файл **/etc/at.deny** содержит список пользователей, которым запрещено осуществлять планирование исполнения задач с помощью службы **atd**.

В случае, если не существует ни одного из этих файлов, службу **atd** по прямому назначению может использовать любой пользователь.

Примечание.

Если вы планируете передать **at** команду, требующую прав **суперпользователя**, помните, что она будет выполняться без присмотра — sudo не будет работать, т.к. никто не может ввести пароль. Для возможности отслеживания действий сначала войдите в систему как пользователь **root**, либо используйте команду `sudo at`.

Планировщик заданий anacron

Описание работы
Пример использования
Файл настроек
Сравнение cron и anacron

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** cronie-anacron-1.5.6-1

Программа **anacron**, как и **cron**, используется для настройки команд на многократное или регулярное выполнение.

Cron — это служба, используемая для запуска запланированных задач. **Cron** хорошо подходит для запуска запланированных задач на машинах, которые будут работать непрерывно 24/7, таких как серверы. Причём, если в запланированное время компьютер будет выключен, задача выполнена не будет.

Anacron — асинхронный или анахроничный **cron**. Используется для периодического запуска команд с частотой, определенной в днях. Его работа несколько отличается от работы **cron**, предполагая, что машина не будет включена все время.

Anacron подходит для выполнения *ежедневных*, *еженедельных* и *ежемесячных* запланированных заданий на ноутбуках или ПК. Если используется **anacron**, можно быть уверенным, что при следующем включении компьютера или ноутбука запланированная задача обязательно будет выполнена.

Вы можете подробнее ознакомиться с настройкой **anacron**, просмотрев наши обучающие видео:

- на **RuTube** — Планировщик задач в РЕД ОС. Anacron;
- в **Яндекс.Дзен** — Планировщик задач в РЕД ОС. Anacron;
- в **VK Видео** — Планировщик задач в РЕД ОС. Anacron.

На наших каналах вы также сможете найти много другой полезной информации.

Описание работы

В РЕД ОС есть *man*-страница с информацией по использованию и применению **anacron**, вызываемая командой:

```
man anacron
```

Утилита **anacron**, как и **cron**, имеет таблицу планирования. Задания **anacron** перечислены в файле **/etc/anacrontab**, их можно запланировать в следующем формате (комментарии внутри файла **anacrontab** должны начинаться с **#**):

```
#period  delay  job-identifier  command
```

где:

- *period* – это частота выполнения задания, указанная в днях или в виде: **@daily**, **@weekly** или **@monthly** для одного раза в *день*, *неделю* или *месяц* соответственно. Также можно использовать числа: *1 – ежедневно*, *7 – еженедельно*, *30 – ежемесячно* и *N – количество дней*;
- *delay* – это количество минут ожидания перед выполнением задания. Желательно для каждого задания указывать разное время, чтобы несколько заданий не запускались одновременно;
- *job-id* – это отличительное имя для задания, записанное в файлах журнала. Это имя используется для создания файла контроля задания. Файл создаётся в папке **/var/spool/anacron/** и содержит сведения, позволяющие программе **anacron** контролировать выполнение задания;
- *command* – это команда или путь к сценарию оболочки, который будет выполнен.

Anacron использует не такие подробные параметры, как **cron**. Наименьший интервал, который существует в **anacron** – день. Это значит, что **anacron** нужно использовать как дополнение к **cron**, а не в качестве его замещения.

Anacron имеет следующий принцип работы — он проверяет, выполнено ли задание за указанный период в поле **period**. Если нет, **anacron** выполняет команду из поля **command** после ожидания определенного количества минут (**delay**).

После выполнения задания **anacron** записывает дату в файл метки времени в каталоге **/var/spool/anacron** с именем, указанным в поле

id задания (имя файла метки времени).

Пример использования

Приведенный пример будет запускать скрипт **/home/user/backup.sh** каждый день:

```
#period delay  job-identifier  command
@daily  10   example.daily   /bin/bash /home/user/backup.sh
```

Если машина выключена, когда ожидается выполнение задания **backup.sh**, anacron запустит выполнение этого задания через 10 минут после следующего включения машины, не ожидая еще 7 дней.

Файл настроек

В файле **anacrontab**, кроме запланированных заданий, также есть важные переменные, которые необходимо понимать:

```
cat /etc/anacrontab

# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# the maximal random delay added to the base delay of the jobs
RANDOM_DELAY=45

# the jobs will be started during the following hours only
START_HOURS_RANGE=3-22


#period in days   delay in minutes  job-identifier   command
1    5  cron.daily  nice run-parts /etc/cron.daily
7    25  cron.weekly  nice run-parts /etc/cron.weekly
@monthly    45  cron.monthly  nice run-parts /etc/cron.monthly
```

Здесь:

- **RANDOM_DELAY** — определяет максимальную случайную задержку в минутах, добавляемую к пользовательской задержке задания (по умолчанию 45 мин);
- **START_HOURS_RANGE** — задает временной интервал, в течение которого будут запускаться задания (т.е. задания будут выполнятся только в течение следующих часов).

Сравнение cron и anacron

Cron	Anacron
является службой	не является службой
подходит для серверных машин	подходит для ПК и ноутбуков
позволяет запускать запланированные задания каждую минуту	позволяет запускать запланированные задания только на ежедневной основе
если машина выключена, запланированное задание не выполняется	если машина выключена, когда запланировано задание, *anacron* выполнит запланированное задание при следующем включении машины
может использоваться как **локальными пользователями**, так и суперпользователем **root**	может использоваться **только** суперпользователем **root**, если не указано иное (включено для обычных пользователей с конкретными настройками)

Основное различие между **cron** и **anacron** заключается в том, что **cron** эффективно работает на машинах, которые будут работать непрерывно, в то время как **anacron** предназначен для машин, которые будут отключены через день или неделю.

Графическая утилита для планирования заданий zeit

Установка
Работа с утилитой

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zeit-0.6.0-1

Cron — это служба, используемая для запуска запланированных задач. **Cron** подходит для запуска запланированных задач на машинах, которые могут работать непрерывно 24/7, таких как серверы. Причём, если в запланированное время компьютер будет выключен, задача выполнена не будет.

zeit – графическая утилита для планирования заданий cron.

К запланированным заданиям можно отнести такие операции, как резервное копирование, очистка дискового пространства и прочие задачи обслуживания системы.

Установка

Для установки утилиты **zeit** перейдите в сеанс пользователя **root**:

```
su -
```

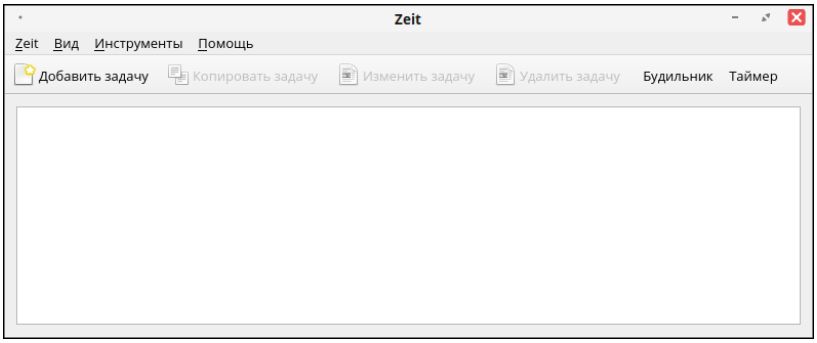
и выполните команду:

```
dnf install zeit
```

После установки запуск утилиты доступен из «**Главного меню**» – «**Системные**» – «**Планировщик заданий**» или через терминал (запуск производится с правами **непривилегированного** пользователя):

```
[ "$EUID" -ne 0 ] && zeit || echo "Команда не должна выполняться с правами пользователя root!"
```

Главное окно утилиты **zeit** выглядит следующим образом:

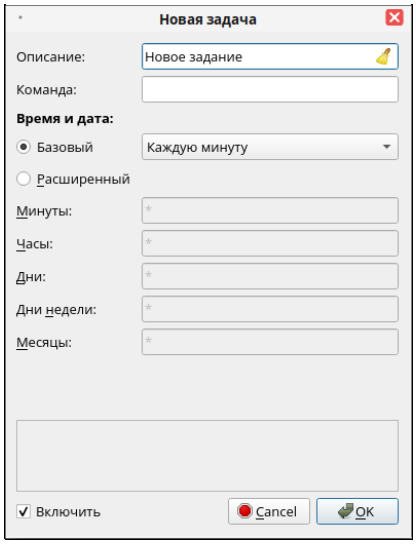


Интерфейс утилиты довольно прост и интуитивно понятен – здесь доступны:

- 4 основные опции:
  - Добавить;
  - Копировать;
  - Изменить;
  - Удалить;
- 2 дополнительные опции:
  - Будильник;
  - Таймер.

Работа с утилитой

Для создания нового запланированного задания нажмите кнопку «**Добавить задачу**».



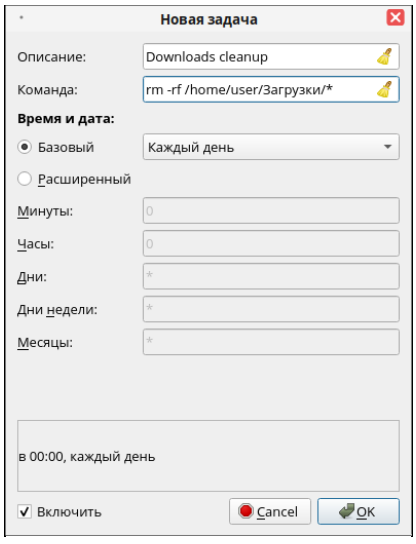
В появившемся окне задайте описание задания, непосредственно задание в виде команды **bash**, а также укажите временной интервал, по которому будет выполняться команда.

В списке **Базовый** предлагаются следующие параметры временного интервала:

- Каждую минуту;
- Каждый час;
- Каждый день;
- Каждую неделю;
- Каждый месяц;
- Кроме выходных.

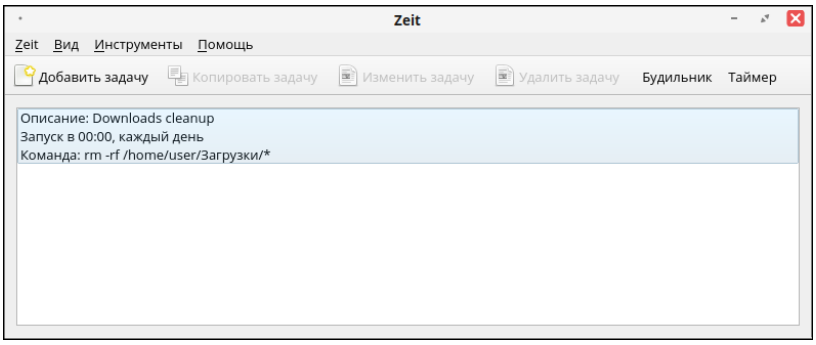
Если необходимо указать конкретную дату и время, выберите вариант **Расширенный** и установите собственные значения в соответствующих полях.

Для примера будет создана простая задача – ежедневная очистка каталога «**Загрузки**».



Нажмите **OK**, чтобы создать задание **cron**.

После этого созданное задание будет отображено в списке.



Для проверки активности задания выведите содержимое файла **crontab** с помощью команды:

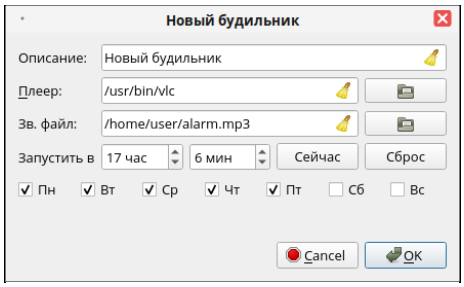
```
crontab -l

#Downloads cleanup
0 0 * * * rm -rf /home/user/Загрузки/*
```

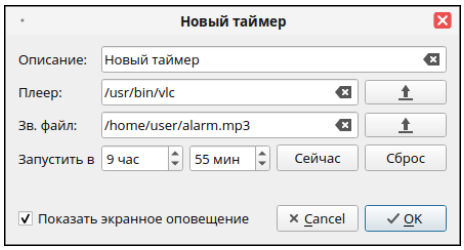
Задание будет выполняться каждый день в 0:00.

Для редактирования запланированного задания выберите его из списка утилиты и нажмите кнопку «**Изменить задачу**». Внесите необходимые изменения и нажмите **OK** для обновления задачи.

Для удаления запланированного задания выберите его из списка утилиты и нажмите кнопку «**Удалить задачу**».

В **zeit** также представлены две дополнительные опции: *будильник* и *таймер*. Будильник будет проигрывать звуковой сигнал в определенное время в выбранные дни недели, таймер будет проигрывать звуковой сигнал только в указанное время. Будильники/таймеры могут быть полезны для напоминания о чем-то важном.





Сервер электронной почты postfix

Работа в режиме SMTP-сервера
Пакеты postfix
Конфигурационные файлы
Доменная информация
Postfix на узлах с удалённым доступом к сети
Postfix на клиентской машине локальной сети
Почтовый сервер для небольших доменов и сетей
Алиасы и преобразования адресов
Защита от нежелательной корреспонденции
Прочие настройки
Использование Postfix

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** postfix-3.7.2-1

Сервер электронной почты **postfix** позволяет организовать обмен электронной почтой с Интернет и внутри локальной сети. postfix рекомендуется к установке в любой конфигурации РЕД ОС. Это объясняется тем, что в UNIX-подобных системах возможность отправлять почту с помощью вызова команды из командой оболочки практически обязательна. Некоторые программы (например, служба исполнения заданий по расписанию **crond**) пользуются этим для отправки сообщений пользователям.

Рекомендуется настраивать систему таким образом, чтобы доставкой всей электронной почты, проходящей через машину, занималась служба **MTA** (**Mail Transport Agent**), в нашем случае - postfix. Хотя многие почтовые программы способны отправлять сообщения на удалённый SMTP-сервер, имеет смысл поручить и эту задачу системному серверу электронной почты, чтобы не было необходимости следить за отсылкой отправленных писем.

Помимо postfix существуют и другие популярные реализации MTA, например, **qmail**, **exim** и даже ветеран Интернета **Sendmail**, хотя последний сейчас используется всё реже, поскольку неоправданно сложен в настройке. Однако по разным причинам, включая соображения безопасности, в любом дистрибутиве РЕД ОС по умолчанию в качестве MTA предлагается postfix.

Работа в режиме SMTP-сервера

Обратите внимание, что по умолчанию после установки postfix не работает в режиме SMTP-сервера. Для того, чтобы принимать сообщения по протоколу SMTP или ESMTP, как извне, так и локально, необходимо переключить службу postfix в режим работы **server** командой **control postfix server**. По умолчанию после установки служба postfix находится в режиме *local*, в котором postfix не принимает соединений из сети, ограничиваясь приёмом локальных соединений посредством сокетов семейства UNIX (UNIX-domain socket). Для большинства рабочих станций работа в режиме SMTP-сервера не требуется (и нежелательна с точки зрения безопасности), а в качестве SMTP-сервера должен использоваться какой-то внешний узел сети.

Пакеты postfix

Базовый RPM-пакет для установки сервера postfix в РЕД ОС носит, как нетрудно догадаться, имя postfix. Ряд дополнений, расширяющих возможности postfix, выделены в отдельные пакеты, полный список которых можно получить командой:

```
dnf search postfix-
```

Конфигурационные файлы

Файлы настройки postfix располагаются в каталоге **/etc/postfix**. Основные параметры определяются в файле **main.cf**; в частности, все параметры, о которых говорится далее в этом разделе, устанавливаются именно в этом файле, остальные случаи оговариваются специально.

Для простоты ориентации в настройке postfix в файле *main.cf* указываются только параметры, выставленные администратором системы, плюс некоторые из значений по умолчанию, которые администратору с большой вероятностью нужно будет изменить. Значения по умолчанию для всех остальных параметров перечислены в файле **main.cf.default** (этот файл не следует редактировать, он служит только для справок). Довольно полный список параметров с развёрнутыми комментариями и примерами приведён в файле **main.cf.dist**, а наиболее полную информацию по всем возможным параметрам следует искать в руководстве postconf.

Обратите внимание, что если вы изменили конфигурацию при запущенной службе postfix, новые настройки нужно активизировать командой **systemctl restart postfix**.

Доменная информация

Имя хоста и домена, которые считаются локальными при обработке email-адресов, необходимы для функционирования почтового сервера. Если эти имена для postfix должны отличаться от того, что выдаёт команда hostname, установите их с помощью параметров **myhostname** и **mydomain**.

Postfix на узлах с удалённым доступом к сети

Существует несколько проблем, возникающих при попытке отправки исходящей почты с машин, которые не являются полноценными узлами сети Интернет, например, в системах с модемным и другими непостоянными соединениями, не всегда возможно немедленно отправить сообщения удалённым адресатам по SMTP, и их приходится держать в очереди до тех пор, пока соединение не будет установлено. Для этого используется параметр **defer_transports**, например:

```
defer_transports = smtp
```

Доставка активизируется командой **/usr/sbin/sendmail -q**, которая в РЕД ОС исполняется автоматически при установке PPP-соединения.

Как любой полноценный MTA, postfix позволяет доставлять сообщения, связываясь напрямую с сервером, обслуживающим получателя письма. Тем не менее, для dialup-машин непосредственная доставка сообщений нежелательна, поскольку время соединения ограничено. К тому же это излюбленная тактика распространителей спама, поэтому многие почтовые серверы сверяют IP-адрес отправителя с базой известных адресов провайдерских пулов, после чего сообщения с таких адресов отвергаются. Поэтому целесообразно доверить доставку исходящей почты SMTP-серверу провайдера. Этим управляет параметр **relayhost**, например:

```
relayhost = [smtp.provider.net]
```

Postfix на клиентской машине локальной сети

Рабочие станции в локальной сети или машины в провайдерской сети, отделённой от Интернета с помощью межсетевого экрана/NAT, должны переправлять исходящую почту на почтовый сервер, обслуживающий данную сеть. Для этого также используется параметр **relayhost**, описанный выше. Если сервер задан IP-адресом, можно отключить использование DNS для ускорения работы:

```
disable_dns_lookups = yes
```

Для того чтобы в доменной части адреса отправителя фигурировал домен сети, а не имя конкретной машины в этой сети, установите параметр **myorigin** равным имени домена:

```
myorigin = $mydomain
```

Почтовый сервер для небольших доменов и сетей

Домены, для которых сервер получает почту, отличные от значения **mydomain** и не сконфигурированные как виртуальные домены postfix, нужно перечислить с помощью параметра **mydestination**, либо в дополнительном файле, на который ссылается этот параметр. Аналогичным образом параметр **mynetworks** описывает блоки IP-адресов, которые считаются внутренними и с которых разрешён приём исходящих сообщений. Не следует записывать в *mynetworks* блоки адресов, не принадлежащих сети, которую обслуживает сервер, поскольку этим могут воспользоваться распространители спама.

Для пользователей, желающих отправлять сообщения через данный сервер, когда они находятся вне пределов локальной сети, следует организовать SMTP-аутентификацию. В postfix для этой задачи следует использовать библиотеку SASL (начиная с версии 2.3 в postfix появилась возможность использовать разные реализации SASL). На текущий момент доступно две реализации: **Cyrus** (пакет postfix-cyrus) или **Dovecot** (пакет postfix-dovecot). Cyrus, кроме того, можно использовать в postfix для аутентификации в качестве клиента на удалённых SMTP-серверах.

Для шифрования соединений в этой схеме используется протокол *SSL/TLS*, для включения поддержки которого в postfix необходимо установить пакет **postfix-tls**. Используя postfix-tls следует принимать во внимание, что это расширение включает в postfix значительный объём исходных текстов, в меньшей степени проверенного в плане безопасности. Настройка аутентификации посредством *TLS/SASL* описана в файлах *TSL_README* и *SASL_README* в документации postfix.

Преобразование глобальных почтовых адресов в локальные адреса назначения устанавливается с помощью таблиц типа **virtual**:

```
virtual_alias_maps = cdb:/etc/postfix/virtual
```

Пример содержимого **/etc/postfix/virtual**:

```
domain1.ru # Домен в стиле postfix (текст здесь игнорируется) name1@domain1.ru user1 name2@domain2.ru user2@otherbox
@domain2.ru user3
```

После редактирования не забудьте активизировать изменения командой **systemctl restart postfix**.

Алиасы и преобразования адресов

Имена локальных адресатов либо совпадают с именами учётных записей пользователей системы, либо подставляются из таблицы **aliases**:

```
alias_maps = cdb:/etc/postfix/aliases
alias_database = cdb:/etc/postfix/aliases
```

При установке postfix «с нуля» в этой таблице создаётся алиас на имя root: вся корреспонденция, предназначенная администратору и поступающая на другие системные адреса, будет доставляться на имя реального пользователя, который осуществляет функции администратора. Изначально им становится первый зарегистрированный в системе реальный пользователь. Таблица алиасов отличается от остальных таблиц, используемых postfix; имена в поле слева (псевдонимы) отделяются от значений в поле справа (адреса доставки) двоеточиями. Адресаты в списке перечисляются через запятую. В качестве способа доставки можно использовать почтовые адреса, команды (обозначаются символом | в начале правой части; сообщение подаётся на стандартный поток ввода команды) и имена файлов:

```
John.Smith: john
chief: chief@bosscomputer
trio: stock, hausen, walkman
robot: | /usr/bin/robot --process-mail
filebox: /dir/file
```

Рабочий образ таблицы строится с помощью команды **newaliases**, а также при актуализации всех изменений посредством команды **systemctl restart postfix**.

При отправке сообщения postfix формирует адрес отправителя автоматически из имени учётной записи пользователя и значения собственного домена (или значения myorigin, если этот параметр выставлен). Даже если почтовый клиент выставил заголовок **From:**, этот адрес попадает в служебные заголовки сообщения и может быть использован получателем, что не всегда желательно. Преобразование адресов отправителей к глобальным адресам можно задать в таблице типа **canonical**:

```
sender_canonical_maps = cdb:/etc/postfix/sender_canonical
```

Аналогичная таблица **recipient_canonical** и соответствующий параметр **recipient_canonical_maps** могут быть использованы для преобразования адресов назначения. Для актуализации изменений таблиц используйте команду **systemctl restart postfix**.

Защита от нежелательной корреспонденции

Противодействие спаму (массовым рассылкам непрошеной корреспонденции) - отдельная большая тема, которую невозможно полностью раскрыть в этом руководстве; здесь даны лишь несколько практических советов применительно к конфигурации postfix. По умолчанию сервер сконфигурирован так, что отвергает попытки переслать сообщения извне на другие удалённые серверы. Со спамом, адресованным локальным получателям, дело обстоит сложнее.

В postfix предусмотрены возможности передачи почтовых сообщений на проверку на спам как внутренним фильтрам, так и внешним программам. Подробности о фильтрации почты см. в *FILTER_README* в документации postfix. Режим фильтрации почты включается в РЕД ОС командой **control postfix filter**.

Один из возможных способов - опираться на данные служб, организованных по принципу «чёрного списка» IP-адресов (MAPS RBL и ей подобные). Чтобы задействовать эти сервисы, предварительно ознакомившись с условиями их использования, занесите имена доменов, работающих по принципу RBL, в конфигурацию:

```
smtpd_client_restrictions = permit_mynetworks, reject_maps_rbl
maps_rbl_domains = relays.ordb.org, blackholes.mail-abuse.org
```

В некоторых случаях требуется адресная работа с отдельными нарушителями почтового этикета. Адресная работа заключается в блокировании SMTP-соединений с их адресов, сетей либо доменов. Для этого предусмотрены таблицы типа access:

```
smtpd_client_restrictions = permit_mynetworks, cdb:/etc/postfix/access
```

Пример таблицы:

```
1.2.3.4 550 No more canned meat, please

1.2.5 REJECT

goodguy.generallybad.com OK

.generallybad.com REJECT
```

Как и с другими таблицами, закончив редактирование, приведите новые настройки в действие командой **systemctl restart postfix**.

Прочие настройки

По умолчанию размер файла почтового ящика при локальной доставке ограничен 51200000 байтами. Это ограничение можно изменить с помощью параметра **mailbox_size_limit**. Установка параметра в 0 снимает ограничение.

Использование Postfix

После того, как postfix настроен и запущен как служба с предсказуемым именем postfix, в настройках почтовых клиентов можно указывать имя или адрес машины (например, localhost) в качестве SMTP-сервера. Для получения почты с удалённых серверов можно использовать программу **fetchmail**, которая работает в связке с postfix, опрашивая внешние почтовые ящики пользователей по протоколам POP3 или IMAP и передавая полученные сообщения системному MTA для локальной доставки. Подробнее о работе с fetchmail см. в документации соответствующего пакета. Файлы журналов postfix находятся в каталоге **/var/log/mail**.

Установка Iredmail на РЕД ОС 7.3

Общая информация
Настройка машины и установка Iredmail
Проверка работоспособности

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: iredmail-1.3.2-21

Общая информация

iRedMail — это:

1) Полноценный почтовый сервер.

2) Работает как на обычной системе, так и под управлением виртуальной машины, например, **VMware**, **OpenVZ**, **Xen**.

3) Поддержка архитектур **i386** и **x86_64**.

4) Использует для установки и настройки совместимые компоненты, такие как **Postfix**, **Dovecot**, **SpamAssassin**, **SOGo** и т.д.

5) При установке использует бинарные пакеты из дистрибутива.

6) Проект с открытым исходным кодом, распространяемый под лицензией **GPL v2**.

7) Поддержка двух бэкэндов для хранения виртуальных доменов и пользователей: **OpenLDAP** и **MySQL**.

8) Безлимитное число поддержки доменов, пользователей, почтовых алиасов.

9) Поддержка двух веб-интерфейсов (**RoundCube** и **SquirrelMail**).

Основная специфика **SOGo** — это общие календари, контакты, почта.

Настройка машины и установка Iredmail

Для работы потребуется **mysql** (**mariadb** — это аналог **mysql**, который присутствует в репозитории РЕД ОС).

Перейдите в сеанс пользователя **root** и выполните установку базы данных:

```
su -
dnf install mariadb mariadb-server
```

Запустите службу **mariadb**:

```
systemctl start mariadb
```

Выполните настройку БД:

```
/usr/bin/mysql_secure_installation
```

На первом шаге должен быть задан пароль **root**, по умолчанию пароль не задан, нажмите **Enter**.

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none): <нажмите_Enter>
OK, successfully used password, moving on...
```

Далее укажите свой пароль **root** и удалите анонимных пользователей:

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

Sett root password? [Y/n] y
New password: <задайте_пароль_root>
Re-enter new password: <повторите_пароль_root>
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!
```

Запретите удаленный вход для **root**, если необходимо:

```
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
```

Удалите тестовую базу данных и обновите таблицу привилегий:

```
By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Настройте хостовое имя компьютера:

```
hostnamectl set-hostname dc1.irwol.ru
```

Отредактируйте файл:

```
nano /etc/hosts
```

Добавьте строку:

```
127.0.0.1 dc1.irwol.ru
```

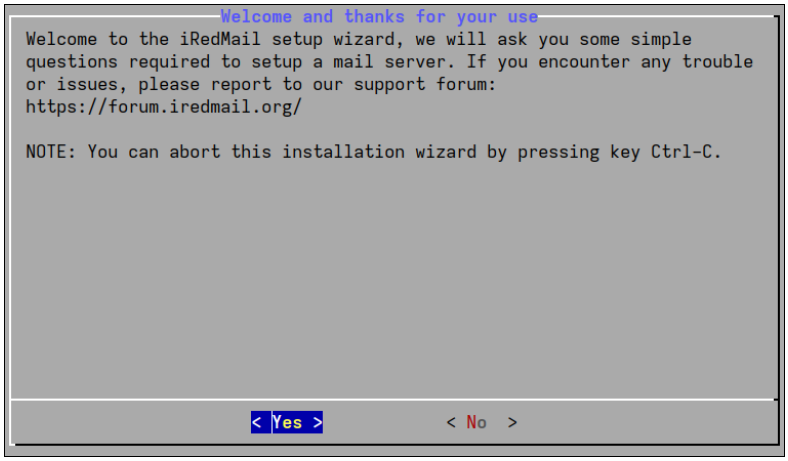
Выполните установку **iredmail**:

```
dnf install iredmail
```

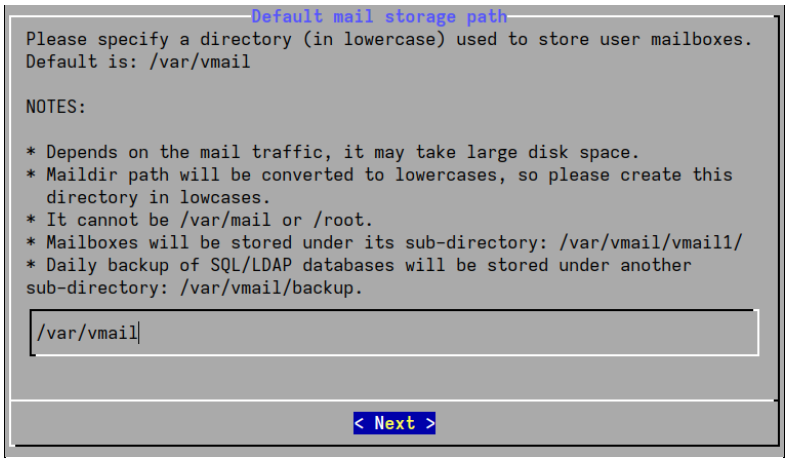
Для запуска настройки выполните:

```
iredmail
```

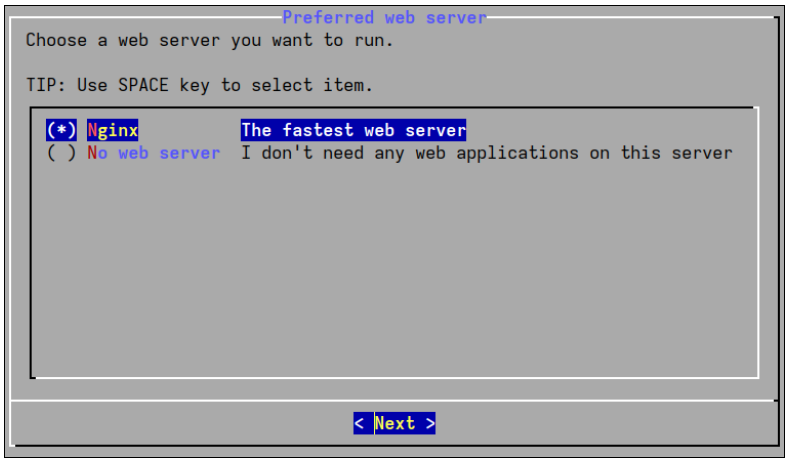
Для запуска настройки **iRedMail** выберите **Yes** и нажмите **Enter**.



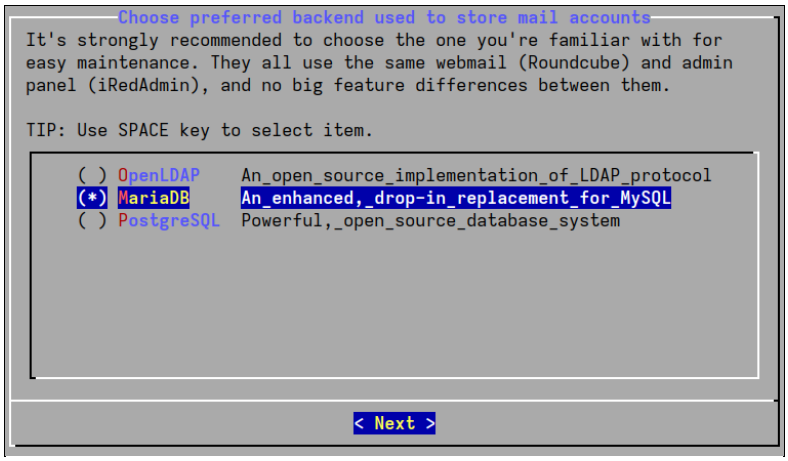
Укажите каталог для хранения почты. Можно оставить значение по умолчанию — **/var/vmail**. Нажмите **Enter** для продолжения.



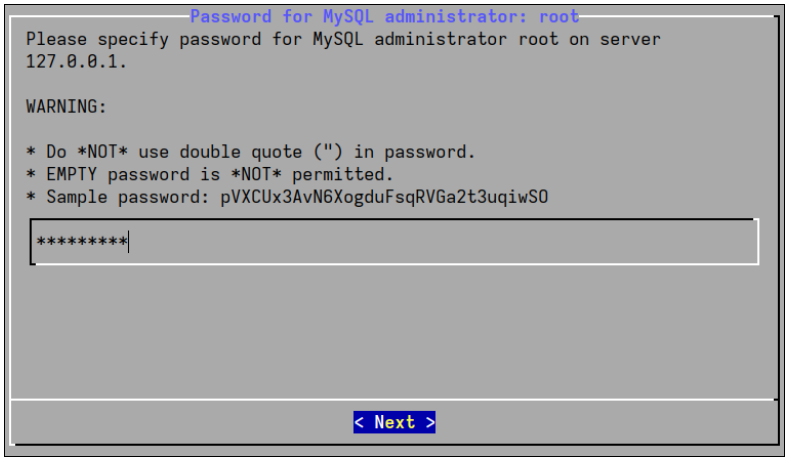
Выберите веб-сервер — **nginx**. Нажмите **Enter** для продолжения.



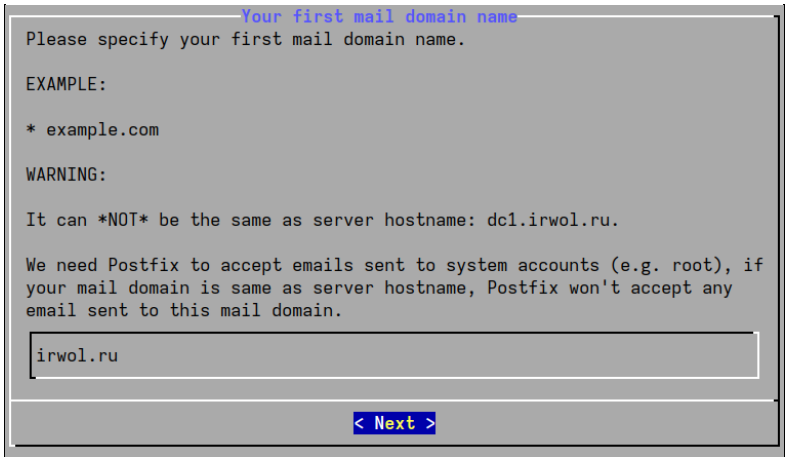
Выберите БД — **MariaDB** (для выбора нажмите клавишу **Space**). Нажмите **Enter** для продолжения.



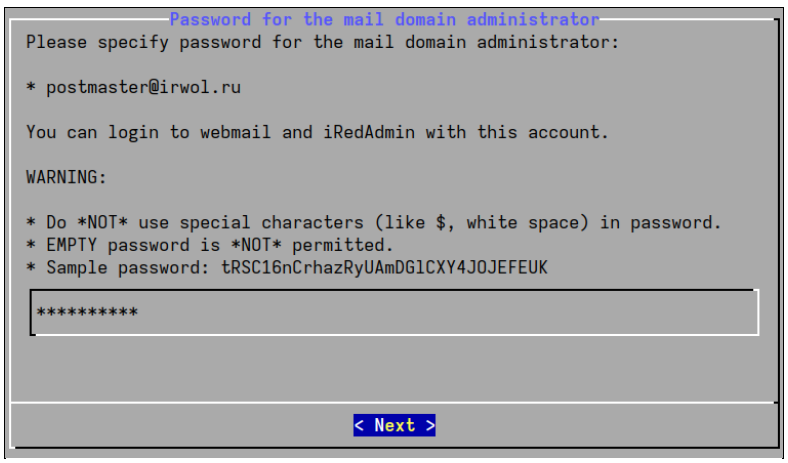
Введите пароль **root** для **MySQL**, указанный при настройке БД. Нажмите **Enter** для продолжения.



Укажите домен сервера — в рассматриваемом примере **irwol.ru**. Нажмите **Enter** для продолжения.

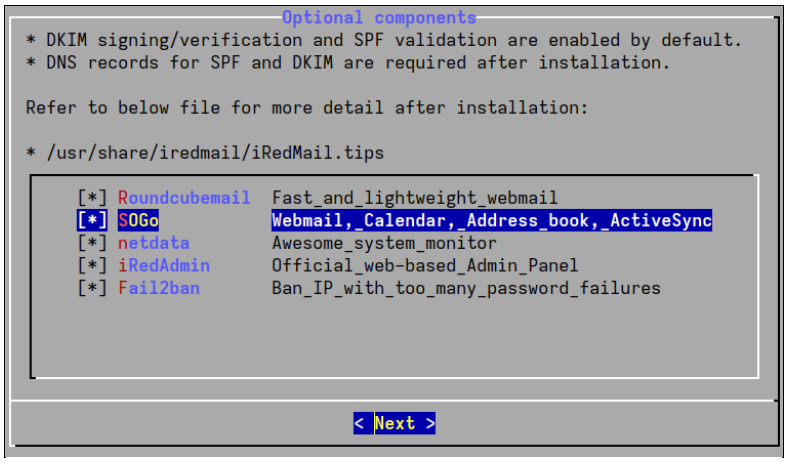


Задайте пароль для администратора почтового сервера. Нажмите **Enter** для продолжения.

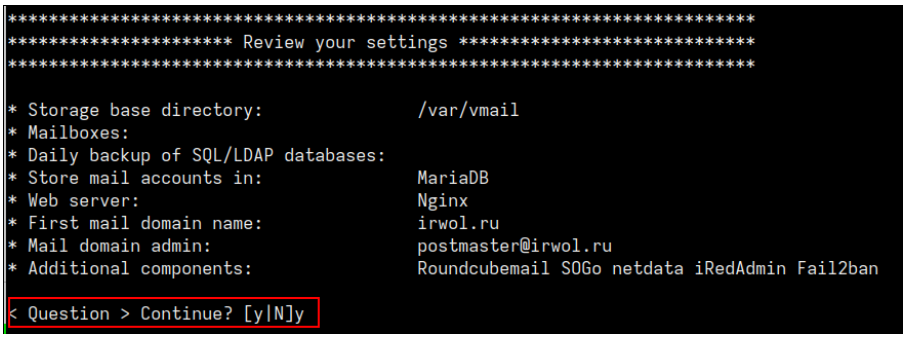


Выберите компоненты почтового сервера — необходимо выбрать все пункты (не выбранным по умолчанию является SOGo, его тоже

необходимо включить). Нажмите **Enter** для продолжения.



Далее необходимо проверить введенные данные. Если все указано верно, для продолжения введите **y**.

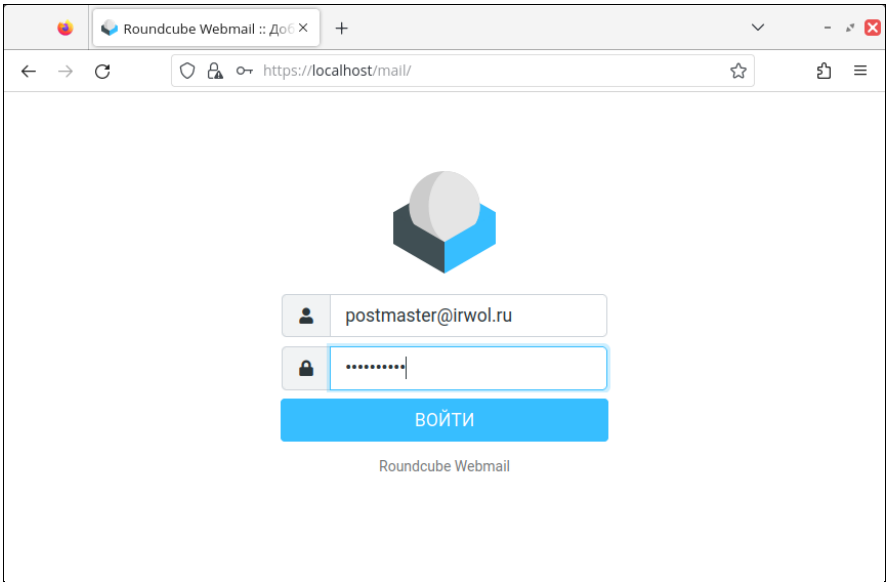


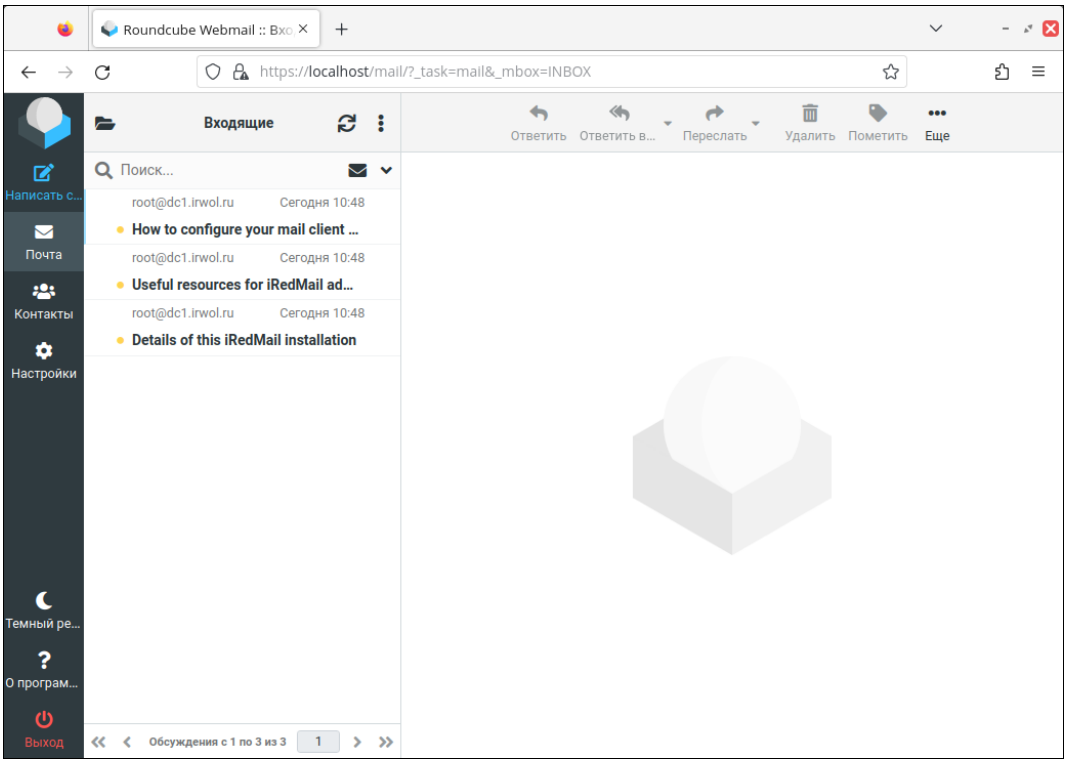
После завершения настройки перезапустите систему.

Проверка работоспособности

Откройте браузер и впишите в адресную строку https://localhost/mail, после принятия сертификата откроется форма авторизации.

Войти можно по ранее настроенной учетной записи администратора почтового сервера postmaster@irwol.ru.





Также проверьте ссылки других служб, связанных с **iRedMail**. Для авторизации используются логин и пароль администратора почтового сервера:

- https://localhost/iredadmin;
- https://localhost/sogo;
- https://localhost/netdata.

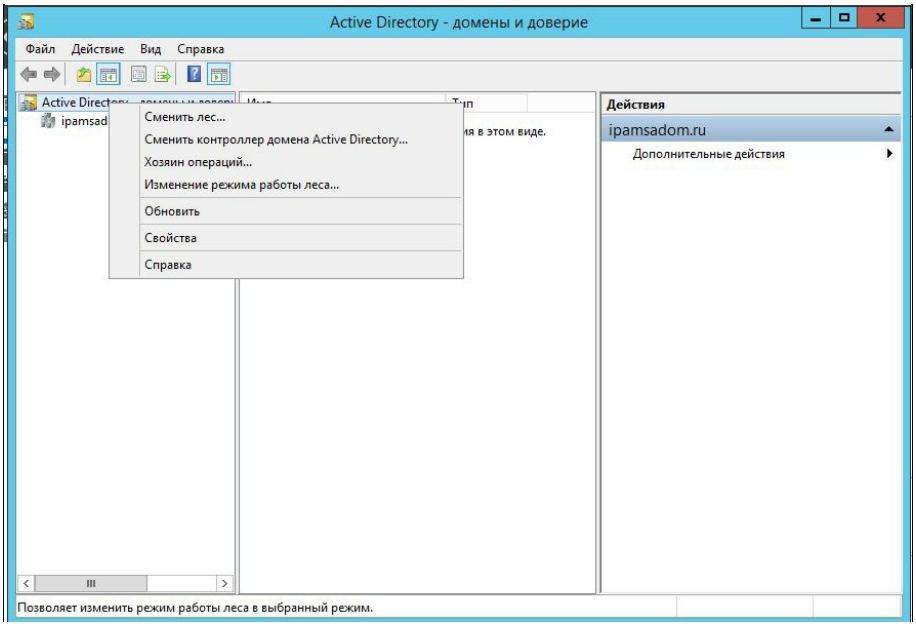
Интеграция Iredmail с MS AD

1 Настройка машины с ms ad
2 Настройка машины с iredmail
3 Настройка дополнительных конфигураций

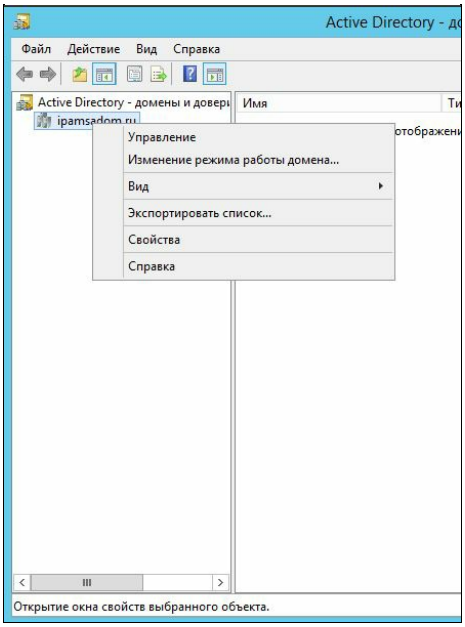
Настройка интеграции с ms ad

1 Настройка машины с MS AD

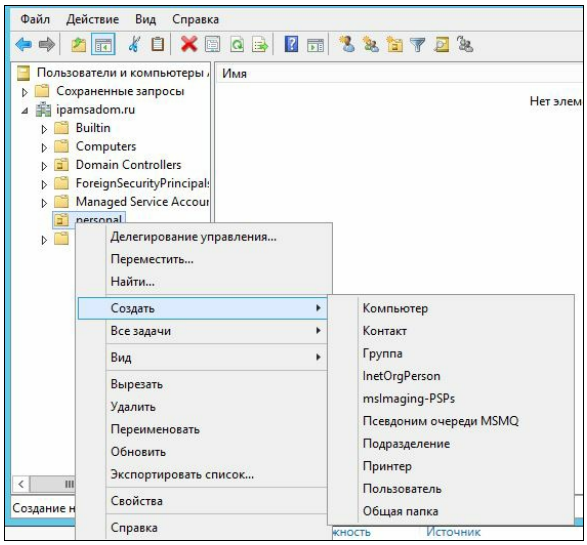
Зайдите в active directory домены и доверие
Откройте свойства



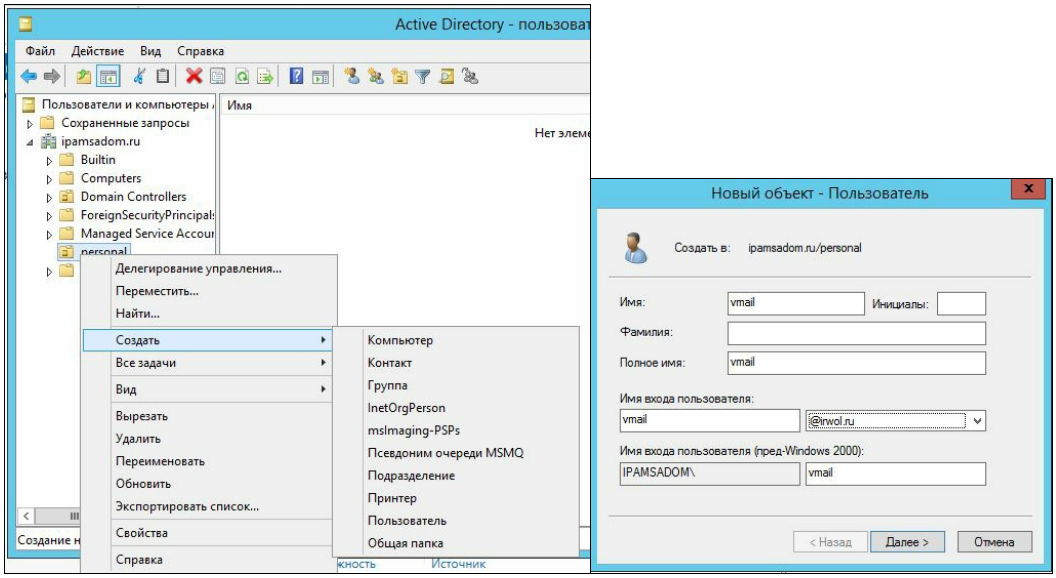
Впишите домен сервера на котором iredmail, нажмите принять
В свойствах домена ms ad выберите пункт управление



Создайте подразделение внутри домена ms ad, пример "personal"



Добавьте в подразделение - пользователя iredmail, домен укажите машины с ms ad
Добавьте еще одного пользователя, домен укажите сервера iredmail



2 Настройка машины с iredmail

Установка openldap:

для РЕД ОС версии 7.3 и старше:

```
sudo dnf install openldap-clients postfix-ldap
```

Проверка соединения с ms ad

```
ldapsearch -x -h 10.81.1.231 -D 'vmail@irwol.ru' -W -b 'dc=ipamsadom,dc=ru' (домен и ip указаны для примера)
```

При корректном выполнении будет список с информацией о ms ad

Т.к. мы будем использовать интеграцию с AD, необходимо отключить параметры в конфиге postfix, которые используются для работы с MySQL

```
postconf -e virtual_alias_maps='' && postconf -e sender_bcc_maps='' && postconf -e recipient_bcc_maps='' && postconf -e relay_domains='' && postconf -e relay_recipient_maps='' && postconf -e sender_dependent_relayhost_maps=''
```

Добавляем почтовый домен

```
postconf -e smtpd_sasl_local_domain='irwol.ru' && postconf -e virtual_mailbox_domains='irwol.ru'
```

Меняем транспорт:

```
postconf -e transport_maps='hash:/etc/postfix/transport'
```

Экспортируем в базу данных Postfix:

```
postmap hash:/etc/postfix/transport
```

Добавляем запросы для подключения к AD:

```
postconf -e smtpd_sender_login_maps='proxy:ldap:/etc/postfix/ad_sender_login_maps.cf' && postconf -e
virtual_mailbox_maps='proxy:ldap:/etc/postfix/ad_virtual_mailbox_maps.cf' && postconf -e
virtual_alias_maps='proxy:ldap:/etc/postfix/ad_virtual_group_maps.cf'
```

Создаем или добавляем в файл строку для транспорта (домен указывается сервера с iredmail)

```
nano /etc/postfix/transport
```

```
irwol.ru dovecot
```

Создаем файл для подключения к AD:

```
nano /etc/postfix/ad_sender_login_maps.cf
```

```
server_host      = 10.81.1.231
server_port      = 389
version          = 3
bind             = yes
start_tls        = no
bind_dn          = vmail    имя пользователя из ms ad, созданного в 1 пункте
bind_pw          = ***      укажите пароль пользователя
search_base = ou= personal,dc=ipamsadom,dc=ru
scope            = sub
query_filter     = (&(userPrincipalName=%s)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
result_attribute = userPrincipalName
debuglevel       = 0
```

Создаем файл групп AD:

```
nano /etc/postfix/ad_virtual_mailbox_maps.cf
```

```
server_host      = 10.81.1.231
server_port      = 389
version          = 3
bind             = yes
start_tls        = no
bind_dn          = vmail имя пользователя из ms ad, созданного в 1 пункте
bind_pw          = ***         укажите пароль пользователя
search_base = ou= personal,dc=ipamsadom,dc=ru
scope            = sub
query_filter     = (&(objectclass=person)(userPrincipalName=%s))
result_attribute = userPrincipalName
result_format    = %d/%u/Maildir/
debuglevel       = 0
```

Создаем файл для подключения к AD:

```
nano /etc/postfix/ad_virtual_group_maps.cf
```

```
server_host             = 10.81.1.231
server_port             = 389
version                 = 3
bind                    = yes
start_tls               = no
bind_dn                 = vmail    имя пользователя из ms ad, созданного в 1 пункте
bind_pw                 = ***      укажите пароль пользователя
search_base = ou= personal,dc=ipamsadom,dc=ru
scope                   = sub
query_filter = (&(objectClass=group)(userPrincipalName=%s))
special_result_attribute = member
```

```
leaf_result_attribute    = mail
debuglevel               = 0
```

Требуется удалить обе строчки в файле

```
nano /etc/postfix/main.cf
```

```
check_policy_service inet:127.0.0.1:7777
```

```
smtpd_end_of_data_restrictions =
check_policy_service inet:127.0.0.1:7777
```

Проверка соединения с ms ad (пользователь указывается который был создан вторым в ms ad, домен прописывается сервера iredmail)

```
postmap -q vmail@irwol.ru ldap:/etc/postfix/ad_virtual_mailbox_maps.cf
```

Если все успешно, то вывод будет не пустым и без ошибок

Вторая команда проверки

```
postmap -q vmail@irwol.ru ldap:/etc/postfix/ad_sender_login_maps.cf
```

При успешном выполнении выдаст

```
vmail@irwol.ru
```

Редактируем файл конфига

```
nano /etc/dovecot/dovecot.conf
```

и приводим секцию Virtual mail accounts к виду:

```
Virtual mail accounts.
userdb {
args = /etc/dovecot/dovecot-ldap.conf
driver = ldap
}
passdb {
args = /etc/dovecot/dovecot-ldap.conf
driver = ldap
}
```

Создаем файл

```
nano /etc/dovecot/dovecot-ldap.conf
```

```
hosts           = 10.81.1.231:389
ldap_version    = 3
auth_bind       = yes
dn              = vmail    имя пользователя из ms ad, созданного в 1 пункте
dnpass          = ***      укажите пароль пользователя
base = ou=personal,dc=ipamsadom,dc=ru
scope           = subtree
deref           = never
user_filter     = (&(userPrincipalName=%u)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
pass_filter = (&(userPrincipalName=%u)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
pass_attrs = userPassword=password
default_pass_scheme = CRYPT
user_attrs = =home=/var/vmail/vmail1/%Ld/%Ln/Maildir/,=mail=maildir:/var/vmail/vmail1/%Ld/%Ln/Maildir/
```

Перезапускаем службы

```
systemctl restart postfix
systemctl restart dovecot
```

Теперь при добавлении нового пользователя в ms ad и указании домена iredmail, пользователю будет автоматически создаваться почтовый ящик в iredmail. Проверить можно будет на машине с iredmail.

https://localhost/mail

Логин пользователя и пароль ms ad соответственно

3 Настройка дополнительных конфигураций

Если в AD есть группы рассылки, тогда отключаем iRedAPD т.к. при работе с AD он не нужен:

```
systemctl disable iredapd
```

По умолчанию, iRedMail позволяет задавать квоты на размер почтового ящика, можно указать дисковую квоту для всех пользователей сразу:

```
nano /etc/dovecot/dovecot.conf
```

Находим строку:

```
quota_rule = *:storage2G
```

Это и есть размер почтового ящика для пользователей- 2Гб. Квота задается для всех пользователей разом!

Подключение адресной книги

```
nano /opt/www/roundcubemail/config/config.inc.php
```

Найдите раздел // Global LDAP address book
Удалите все ниже до конца файла и вставляем строки:

```
$rcmail_config['ldap_public']["irwol.ru"] = array(
'name' => 'Общая адр. книга',
'hosts' => array('10.81.1.231'),
'port' => 389,
'use_tls' => false,
// Search accounts in the same domain.
'user_specific' => false, // If true the base_dn, bind_dn and bind_pass default to the user's IMA$
'base_dn' => 'ou=personal,dc=ipamsadom,dc=ru',
'bind_dn' => 'cn=vmail,dc=ipamsadom,dc=ru',
'bind_pass' => 'xxxxxxx',
'writable' => false, //запретим запись в AD
'ldap_version' => '3',
// 'search_fields' => array('mail', 'cn', 'givenName', 'sn'),
'search_fields' => array('mail', 'cn', 'sAMAccountName', 'displayname', 'sn', 'givenName'),
// 'name_field' => 'cn',
'email_field' => 'mail',
'surname_field' => 'displayName',
// 'firstname_field' => 'givenName',
'sort' => 'cn',
'scope' => 'sub',
// 'filter' => '(&(enabledService=mail)(enabledService=deliver)(enabledService=displayedInG$
'filter' => "(mail=*@*)",
'fuzzy_search' => true);
$config['autocomplete_addressbooks'] = array('sql', 'irwol.ru');
$rcmail_config['list_cols'] = array('flag','attachment', 'from', 'subject', 'status', 'date', 'size' );
```

Настройка конфига SOGo
открываем файл конфигурации и добавляем строки

```
nano /etc/sogo/sogo.conf
```

```
// Authentication using LDAP - Active Directory

SOGoUserSources = (
{
// Used for user authentication
id = directory;
displayName = "Active Directory";
```

```
canAuthenticate = YES;
type = ldap;
CNFieldName = cn;
IDFieldName = sAMAccountName;
UIDFieldName = sAMAccountName;
baseDN = "ou=personal,dc=ipamsadom,dc=ru";
bindDN = "cn=vmail,dc=ipamsadom,dc=ru";
bindFields = (sAMAccountName);
bindPassword = xxxxxxx;
hostname =10.81.1.231;
},
{
// Used for global address book
id = sambaShared;
displayName = "Общая адр. книга";
canAuthenticate = NO;
isAddressBook = YES;
type = ldap;
CNFieldName = cn;
IDFieldName = mail;
UIDFieldName = mail;
hostname = ldap://10.81.1.231;
baseDN = "ou=personal,dc=ipamsadom,dc=ru";
bindDN = "cn=vmail,dc=ipamsadom,dc=ru";
bindPassword = xxxxxxx;
filter = "((NOT isCriticalSystemObject='TRUE') AND (mail=\'*\') AND (NOT objectClass=contact))";
//мои параметры
scope = SUB;
CNFieldName = cn;
SearchFieldNames = (mail, cn, sAMAccountName, displayname, sn, givenName);
//Uncomment to list local users in WebUI without searching (small directories only)
//listRequiresDot = NO;
},
{
id = sambaContacts;
displayName = "Общие контакты";
canAuthenticate = NO;
isAddressBook = YES;
type = ldap;
CNFieldName = cn;
IDFieldName = mail;
UIDFieldName = mail;
hostname = ldap://10.81.1.231;
baseDN = "ou=personal,dc=ipamsadom,dc=ru";
bindDN = "cn=vmail,dc=ipamsadom,dc=ru";
bindPassword = xxxxxxx;
filter = "((((objectClass=person) AND (objectClass=contact) AND ((uidNumber>=2000) OR (mail='*')))
AND (NOT isCriticalSystemObject='TRUE') AND (NOT showInAdvancedViewOnly='TRUE') AND (NOT uid=Guest))
OR (((objectClass=group) AND (gidNumber>=2000)) AND (NOT isCriticalSystemObject='TRUE') AND (NOT
showInAdvancedViewOnly='TRUE')))";
mapping = {
displayname = ("cn");
//Uncomment to list contacts in WebUI without searching (few contacts only)
//listRequiresDot = NO;
};
}
);
```

Перезапуск служб:

```
systemctl restart postfix
systemctl restart dovecot
systemctl restart sogod
```

Почтовый клиент Evolution

Установка Evolution
Основные функции

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: evolution-3.44.4-5

Evolution – свободно распространяемая программа для работы с электронной почтой, управления адресной книгой и функцией планировщика задач. Входит в состав среды рабочего стола **GNOME** в качестве поставляемой по умолчанию почтовой программы.

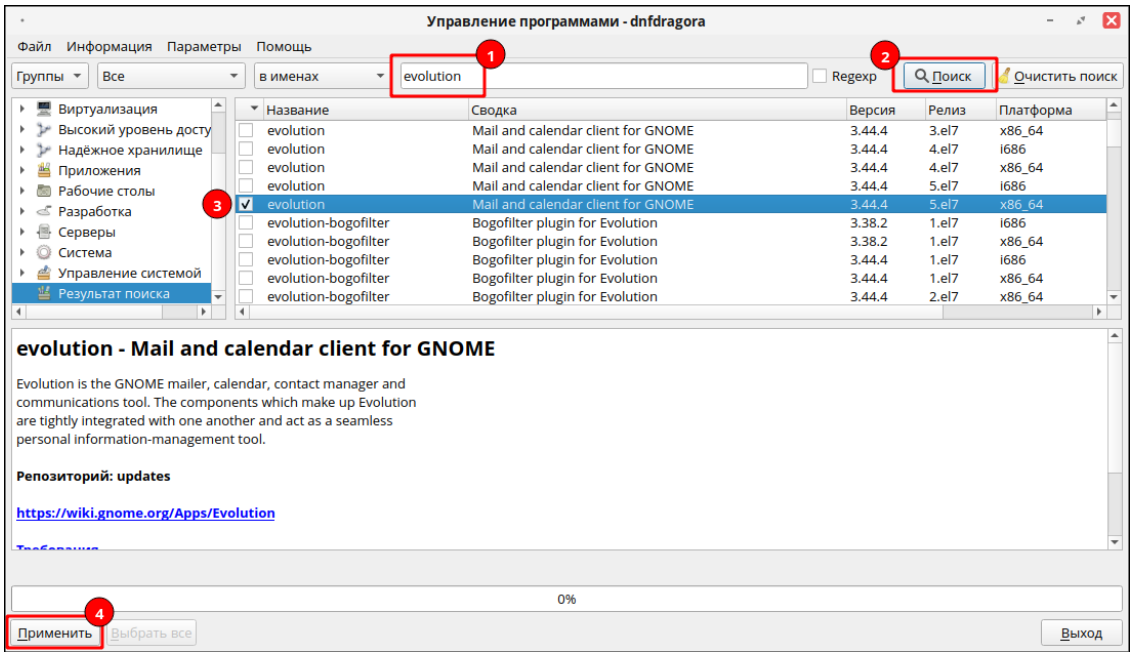
Evolution поддерживает следующие функции и протоколы:

- получение электронной почты по протоколам **POP3** и **IMAP** и её отправка по **SMTP**;
- поддержка расширений протокола **IMAP4** для быстрого обновления содержимого папок **Quick Resync** и уведомлений со стороны сервера **IMAP IDLE**;
- поддержка локальной почты на **UNIX**-системах;
- поддержка защищённых протоколов связи **SSL**, **TLS** и **STARTTLS**;
- шифрование переписки при помощи **GPG** и **S/MIME**;
- использование библиотеки **NSS** для управления сертификатами, что позволяет использовать общее хранилище между совместимыми программами, например, **Mozilla Firefox**, **Mozilla Thunderbird**, **LibreOffice** и пр;
- поиск по почтовым папкам и сортировка почты по критериям;
- автоматическая фильтрация спама с использованием **SpamAssassin** и **Bogofilter**;
- возможность работы с серверами **Microsoft Exchange Server**, **Novell GroupWise** и **Kolab**;
- календарь с поддержкой формата файлов **iCalendar** и протоколов **WebDAV**, **CalDAV** и возможностью подключения к **Google Calendar**;
- адресная книга с поддержкой локальных контактов, протоколов **CardDAV**, **LDAP** и контактов **Google**;
- интеграция адресной книги с **LibreOffice**;
- поддержка аватаров пользователей из адресной книги, из заголовков **X-Face**, **Face** и автоматический поиск их по хешу адреса электронной почты на сервисе **Gravatar**;
- поддержка расширений для чтения лент новостей **RSS**, синхронизации с мобильными устройствами и **VoIP** приложением **Ekiga**;
- импорт почты из архивов **Microsoft Outlook** (файлы с расширениями **.dbx**, **.pst**) и **Berkley Mailbox**.

Установка Evolution

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Evolution** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**evolution**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

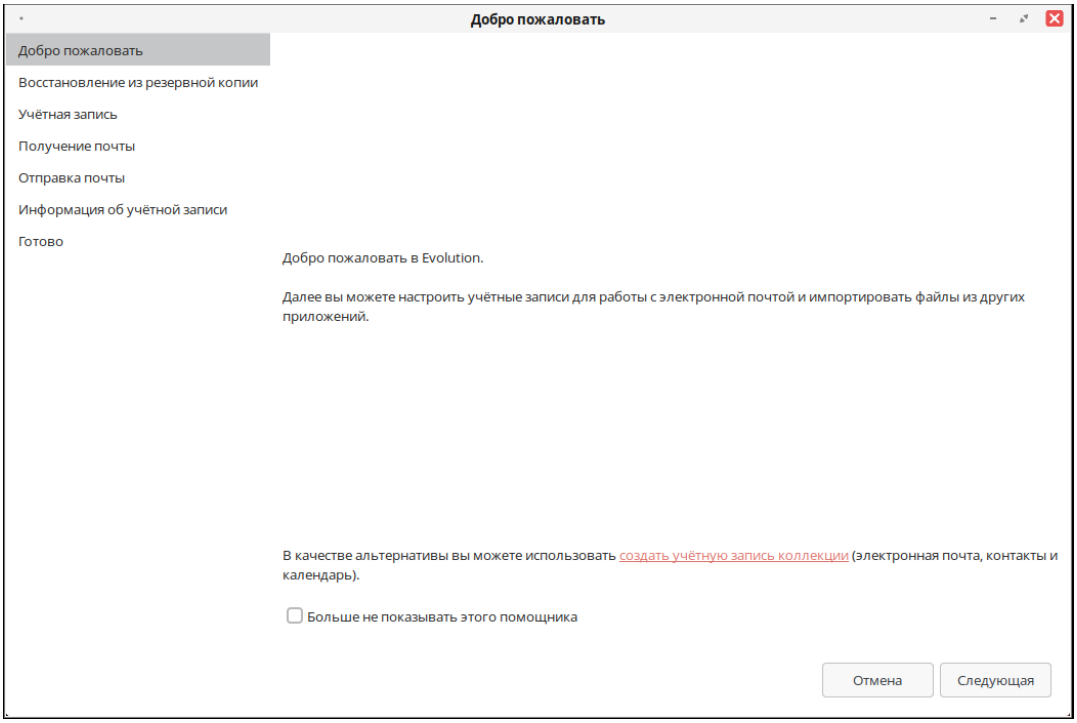
```
dnf install evolution
```

После установки **Evolution** будет доступен из «**Главного меню**» – «**Офис**» – «**Evolution**».

При первом запуске почтового клиента будет выведено окно с настройкой основных функций для работы программы. Здесь вы можете создать новую учетную запись или импортировать файлы из уже существующей, задать параметры почтового сервера, настроить параметры получения и отправки почты.

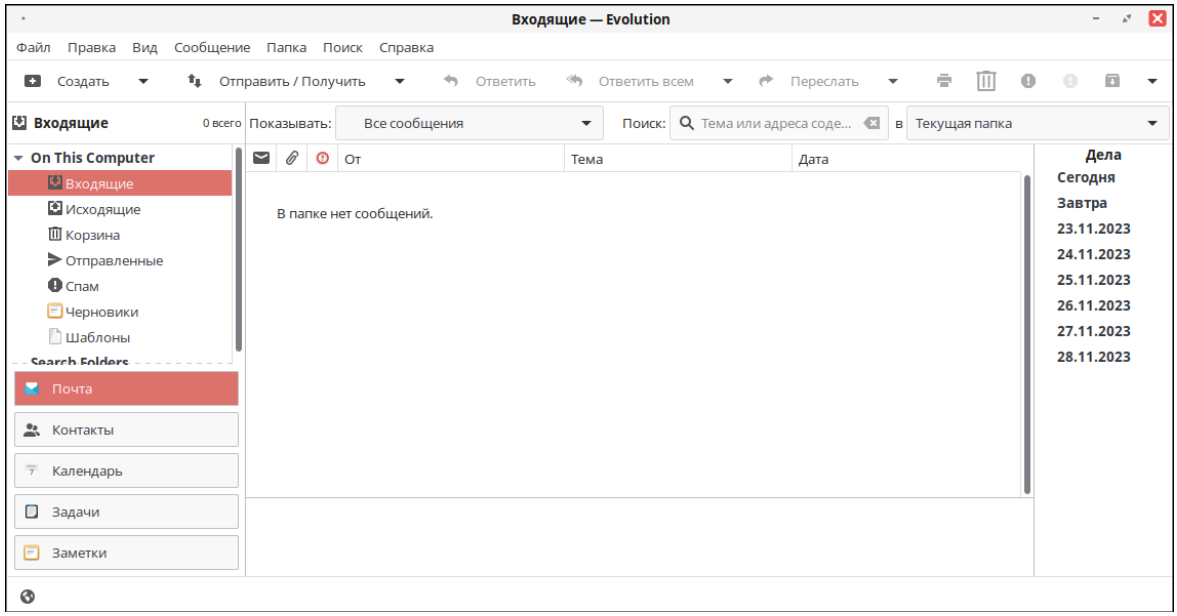
На шаге «**Информация об учетной записи**» необходимо проверить правильность введенных данных и указанных параметров почтового сервера. Если все настроено верно, перейдите к шагу «**Готово**» и начните пользоваться почтовым клиентом.

В противном случае нажмите «**Назад**» и внесите необходимые изменения в настройки клиента.

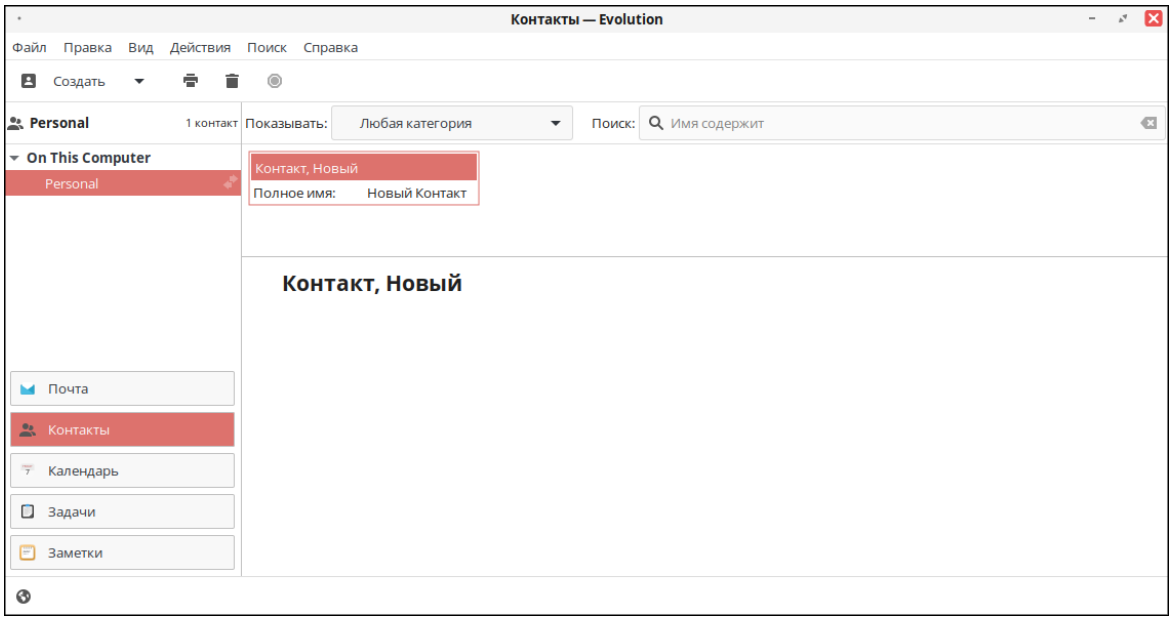


Основные функции

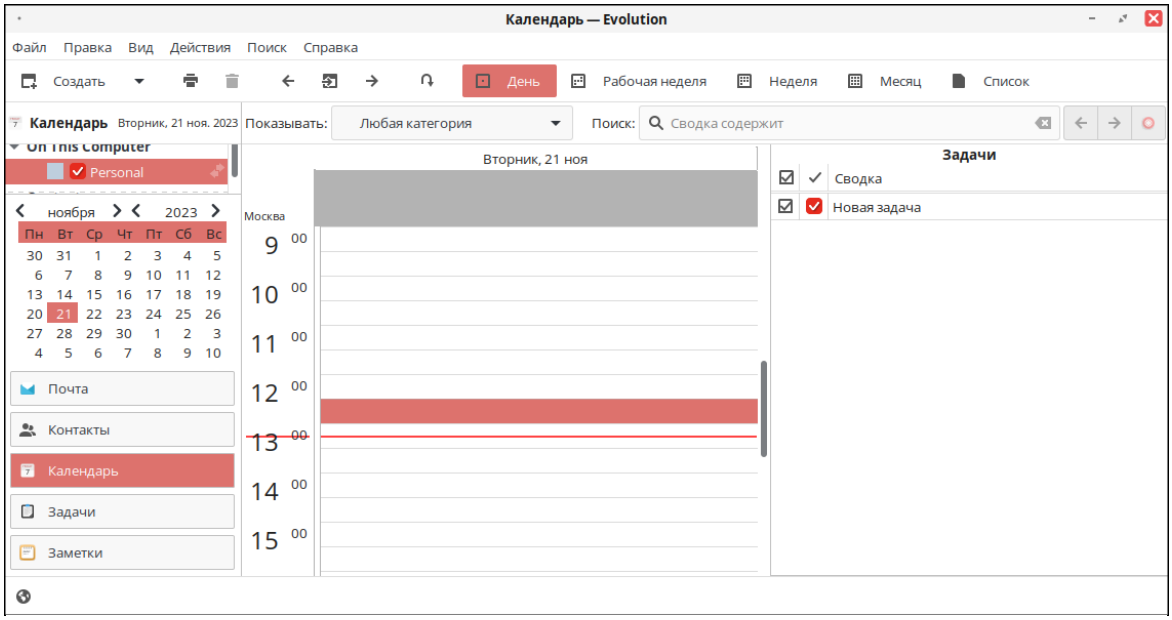
В **Evolution** реализованы стандартные функции почтового клиента – работа непосредственно с электронный почтой.



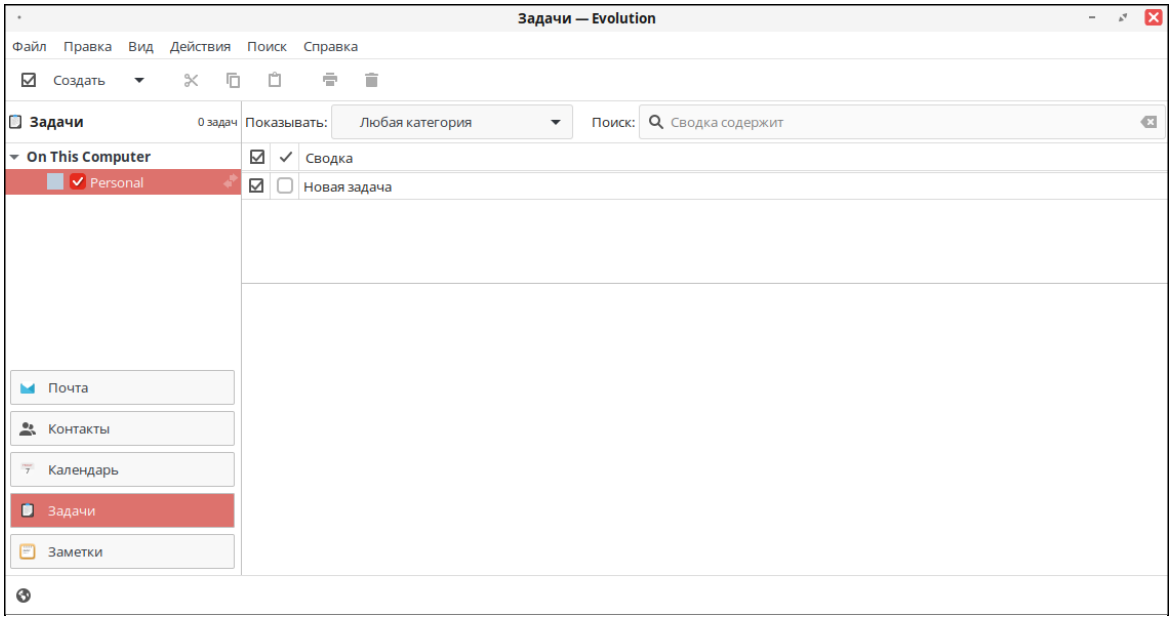
Отдельная вкладка для работы с контактами – добавьте новые контакты.



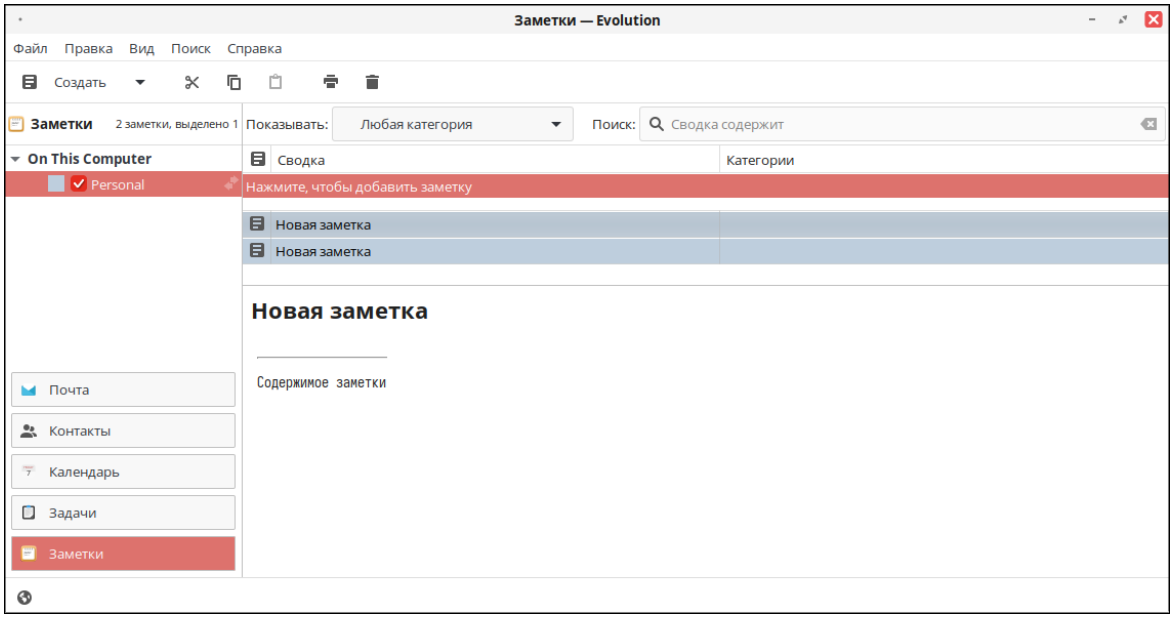
Календарь, в котором можно добавлять мероприятия на определенный день, настраивать оповещение о предстоящем мероприятии или событии.



Вкладка «**Задачи**» – возможность создавать задачи, устанавливать сроки их выполнения, приоритет и текущее состояние.



Также доступно ведение заметок.



Почтовый клиент Thunderbird

Установка

Основные возможности программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: thunderbird-102.15.0-1

Mozilla Thunderbird — это бесплатное приложение для работы с электронной почтой, разработанное командой *Mozilla Foundation*. Это один из самых популярных почтовых клиентов, который предоставляет широкие возможности для организации и управления электронной почтой.

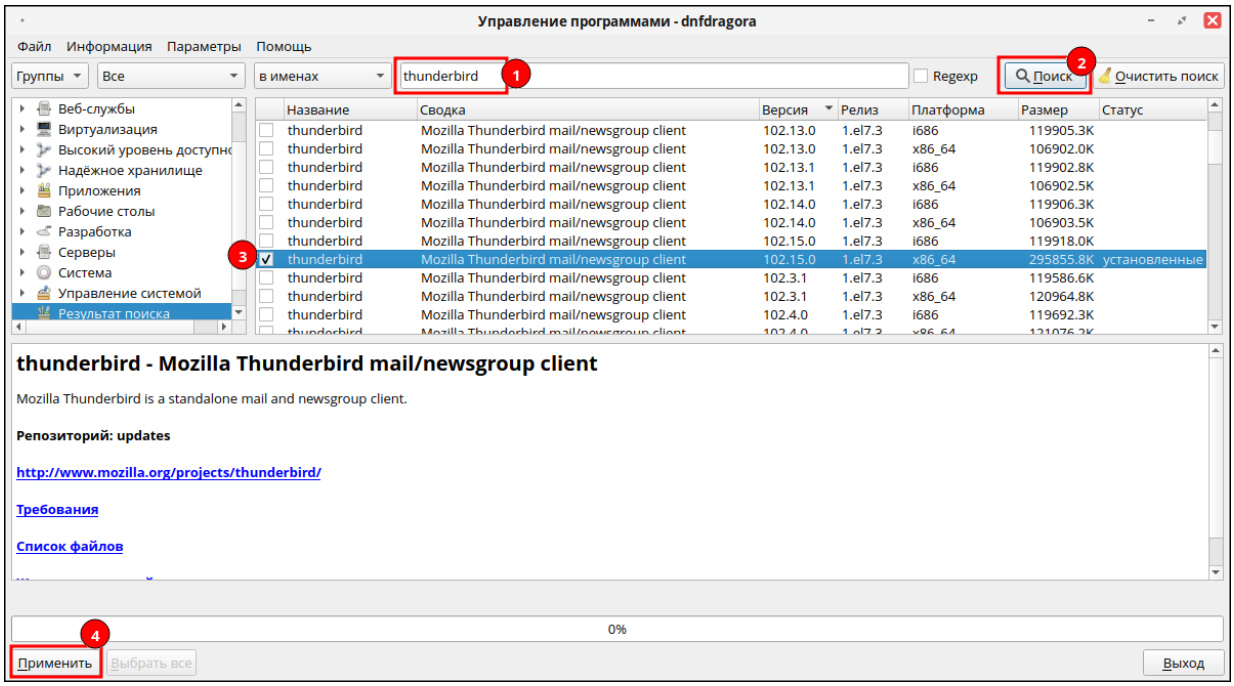
Thunderbird позволяет гибко настраивать учетную запись электронной почты, устанавливать и настраивать различные фильтры и правила, создавать папки для организации писем, устанавливать шаблоны и многое другое. Все письма и контакты хранятся локально на компьютере, обеспечивая безопасность и конфиденциальность данных.

Поддерживаются популярные почтовые протоколы, включая **POP3**, **IMAP** и **SMTP**. Есть возможность подключать почтовые ящики от разных провайдеров с автоматическим обнаружением настроек и управлять ими из одного интерфейса.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Thunderbird** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**thunderbird**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

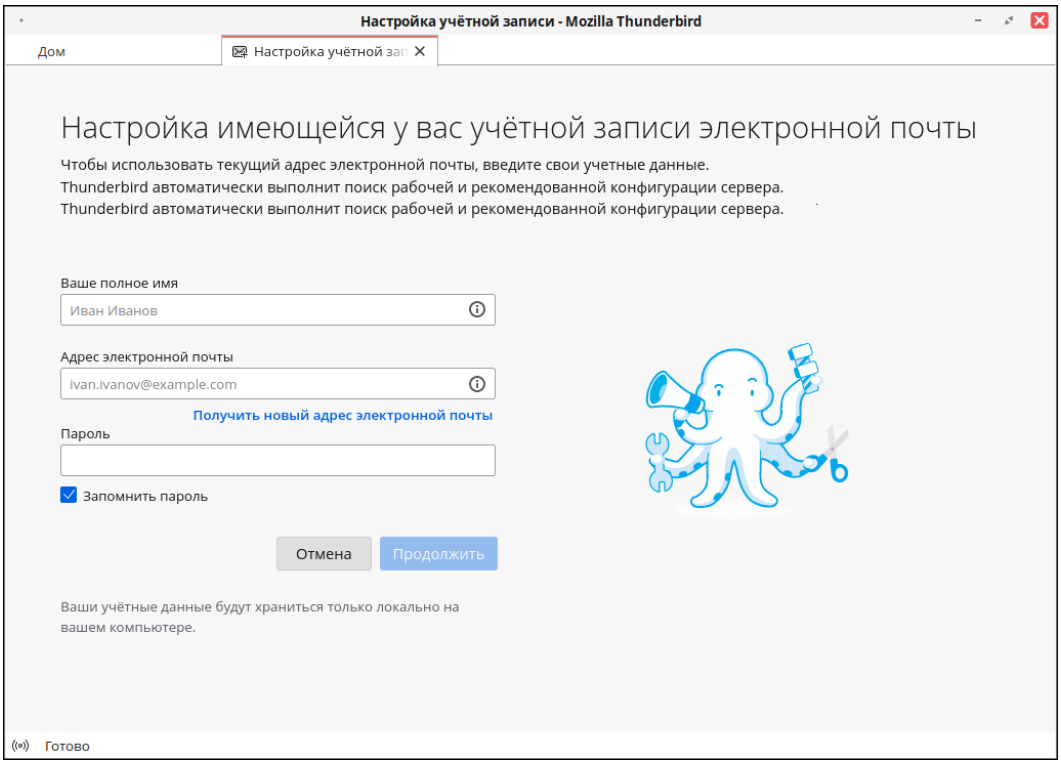
```
su -
```

и выполните команду:

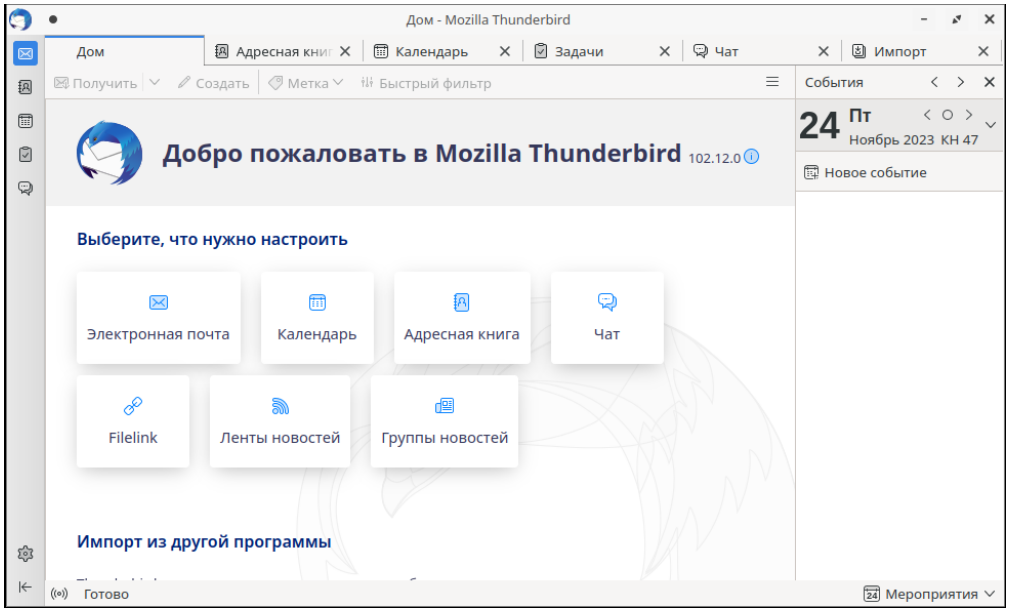
```
dnf install thunderbird
```

После установки **Thunderbird** будет доступен из «**Главного меню**» – «**Интернет**» – «**Почтовый клиент Thunderbird**».

При первом запуске почтового клиента будет предложено ввести данные существующей учетной записи для автоматического определения настроек сервера.

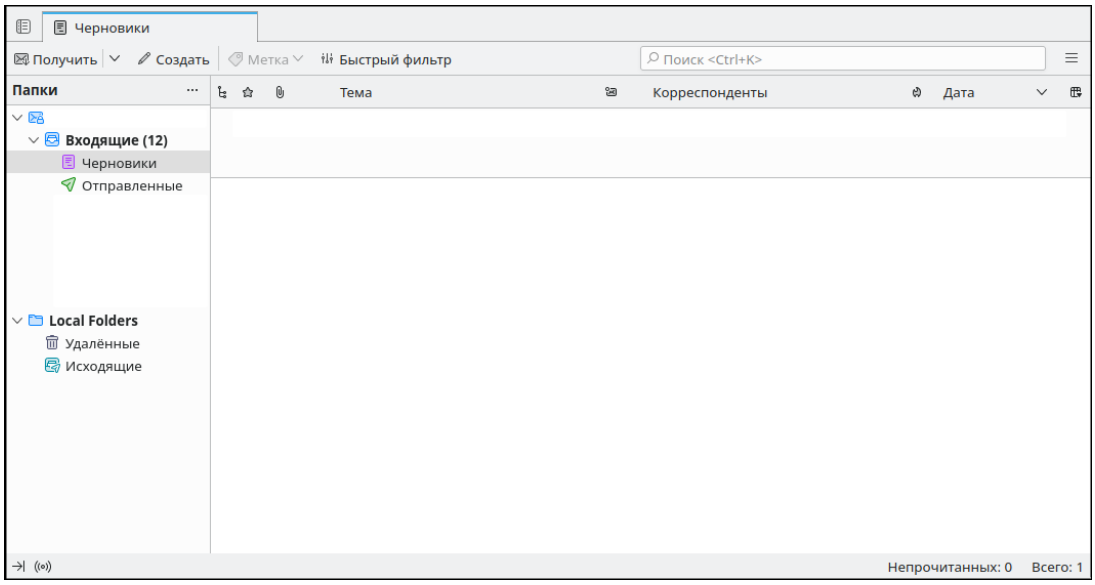


После входа в учетную запись будет открыта домашняя страница почтового клиента, где можно выбрать, что нужно настроить.



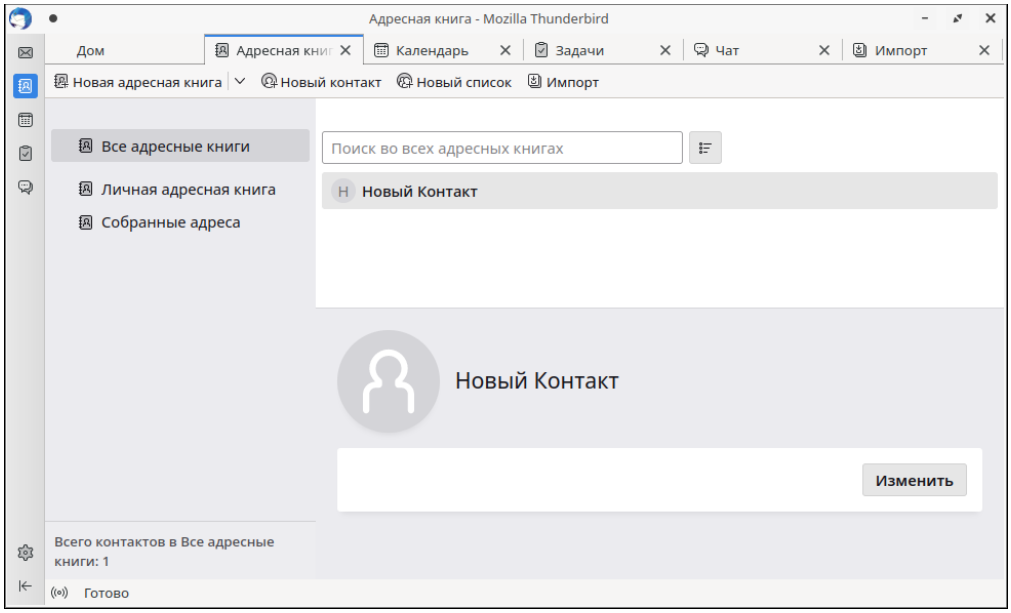
Основные возможности программы

Thunderbird имеет стандартный набор функций почтового клиента, основная из которых – работа с электронной почтой. Thunderbird умеет сохранять письма и вложения локально на компьютере, что обеспечивает доступ к ним даже без интернета. Кроме того, встроенный поиск позволяет быстро находить нужные сообщения.

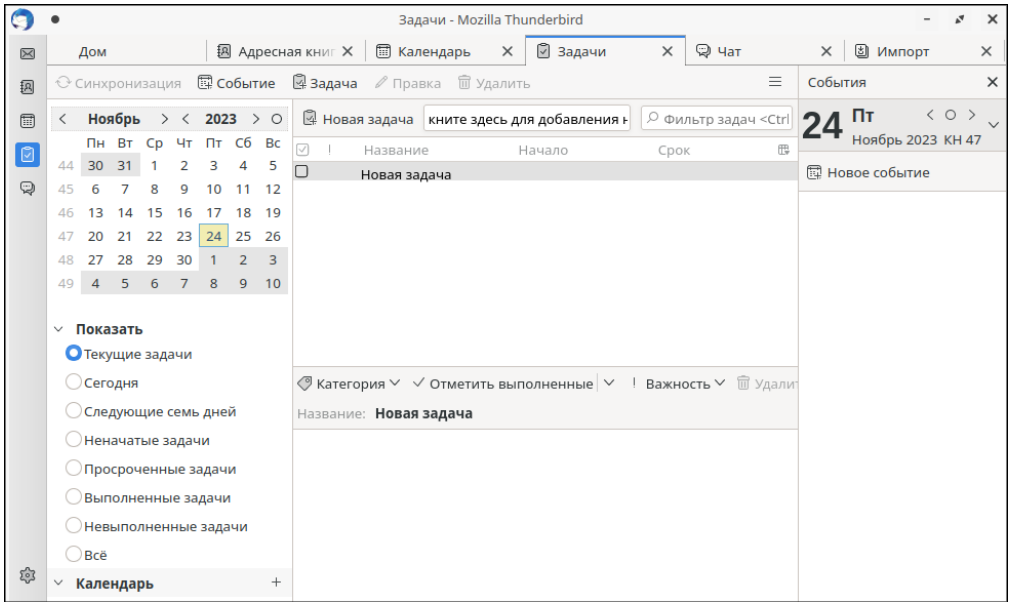


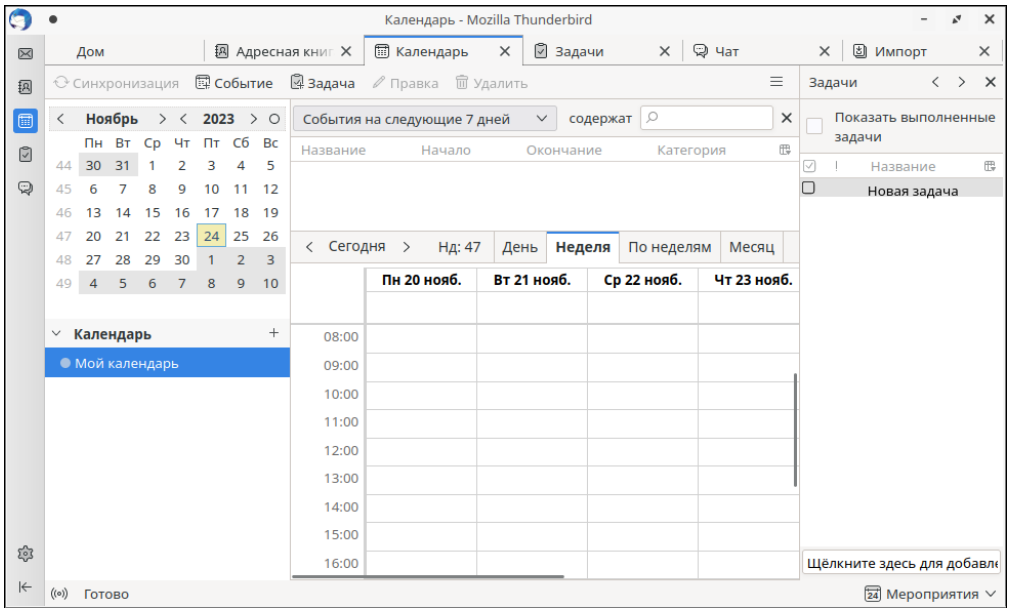
Thunderbird включает встроенные инструменты для борьбы со спамом и обнаружения вредоносных программ. Он также поддерживает шифрование и аутентификацию, чтобы обеспечить безопасность ваших электронных писем.

Также доступна возможность работы с адресной книгой.

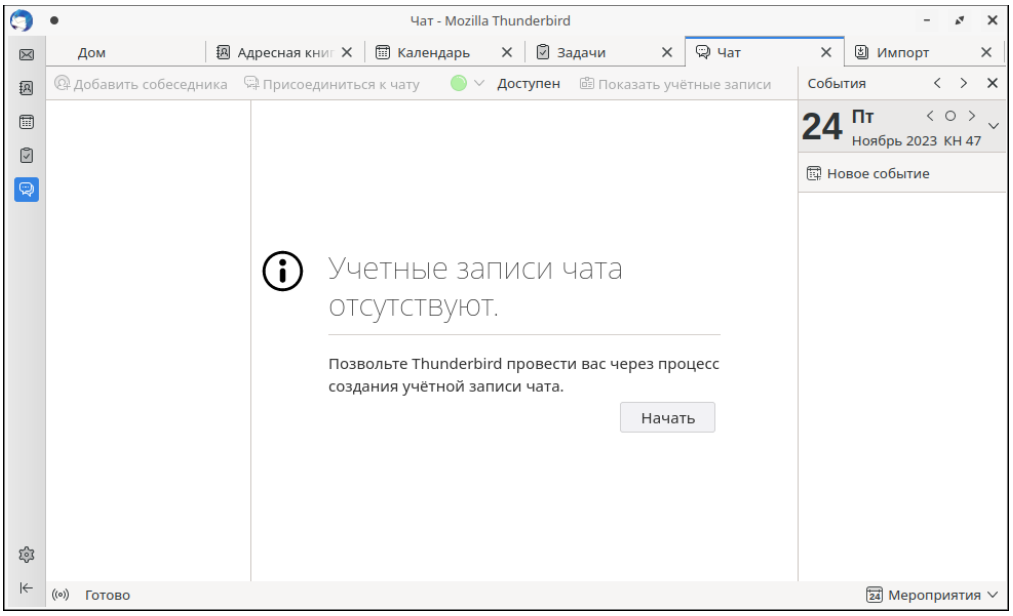


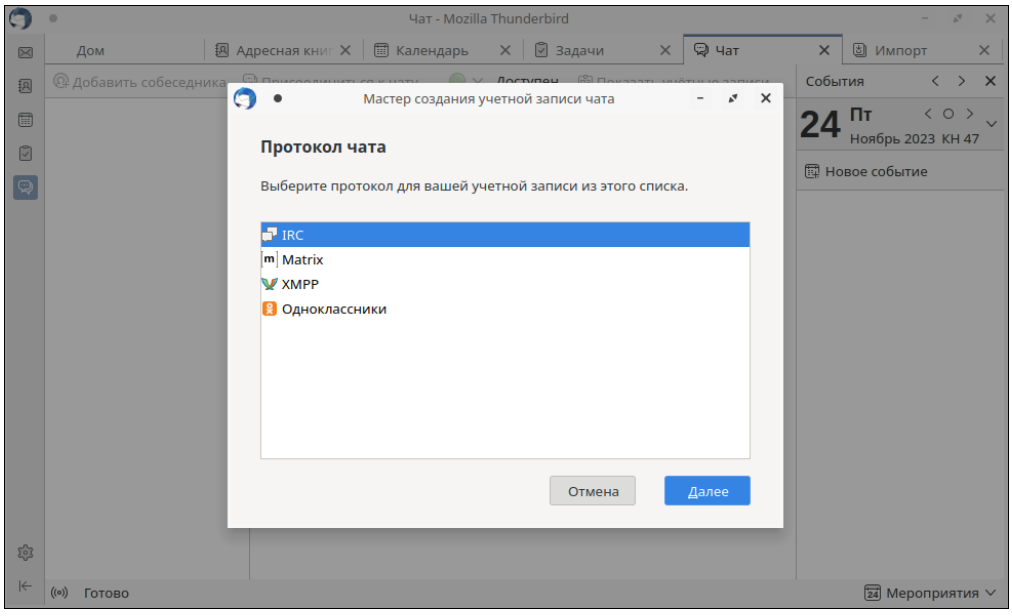
Присутствуют функции календаря, совмещенного с задачами, что позволяет управлять своим временем и не пропускать важные события.





Имеется возможность подключения учетной записи для чата, для выбора доступны такие протоколы, как **IRC**, **Matrix**, **XMPP**, **Одноклассники**.

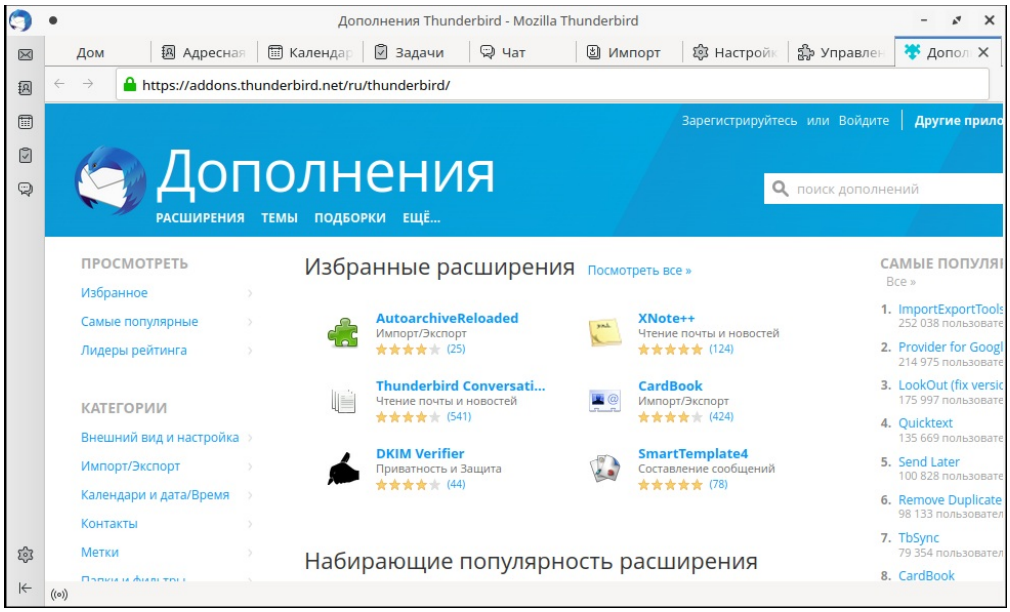




Thunderbird поддерживает подписку на новостные рассылки и чтение **RSS**-каналов, позволяя вам получать свежие новости и информацию из интересующих источников.

Главным достоинством **Thunderbird** можно назвать возможность установки различных дополнений, тем оформления, расширений. Это

позволяет гибко настраивать внешний вид почтового клиента под свой вкус, а также расширять функционал и возможности программы.



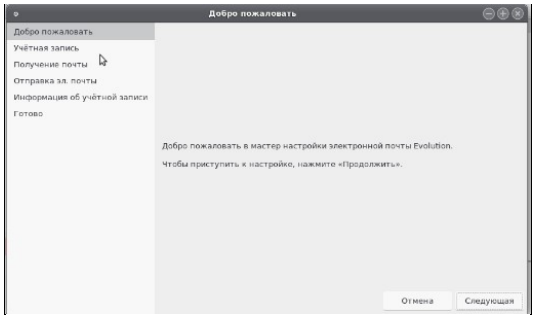
Настройка в Evolution подключения к MS Exchange

У вас должен быть установлен плагин для работы **EWS**. Установить его можно командой:

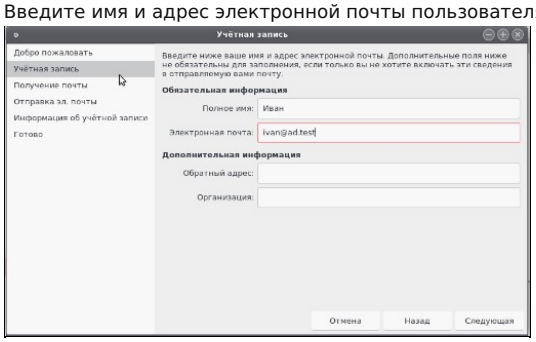
```
dnf install evolution-ews
```

Перейдите в меню »Файл > Создать > Учетная запись почты».

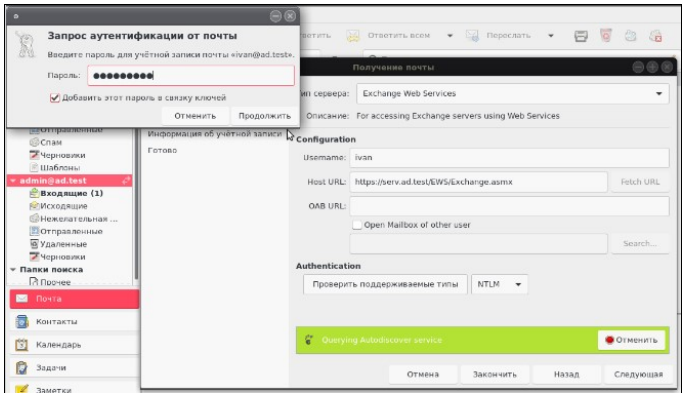
Откроется окно. Нажмите кнопку «Следующая».



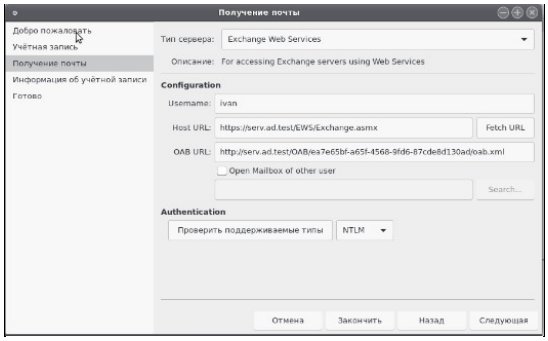
Введите имя и адрес электронной почты пользователя и нажмите кнопку «Следующая».



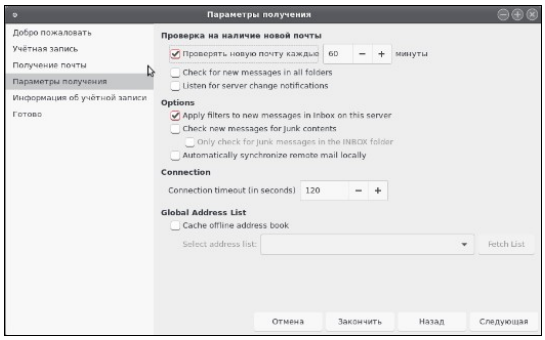
Выберете тип сервера Exchange Web Services. Введите правильный адрес к EWS и нажмите кнопку «Fetch URL».
Если все сделано правильно, откроется окно ввода пароля пользователя. Введите пароль и нажмите кнопку «Продолжить».



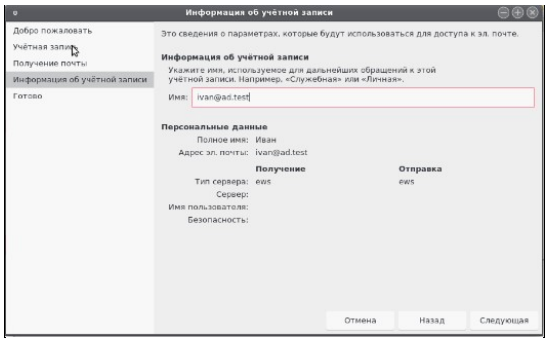
Если пароль введен верно, сервер вернет OAB URL, он отобразится в соответствующем окне. Нажмите кнопку «Следующая».



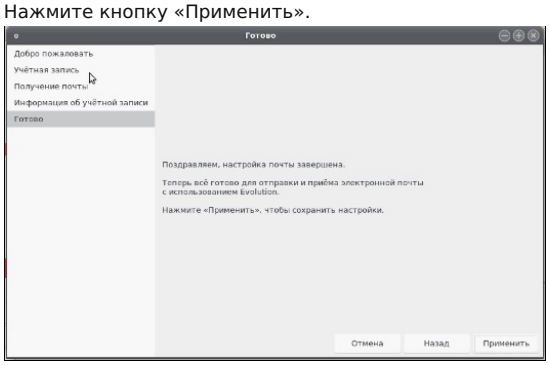
В следующем окне настройте параметры получения или оставьте их по умолчанию. Нажмите кнопку «Следующая».



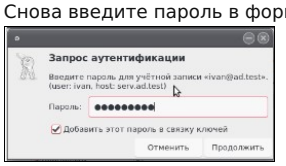
Укажите имя учетной записи для обращений или оставьте значение по умолчанию. Нажмите кнопку «Следующая».



Нажмите кнопку «Применить».



Снова введите пароль в форме ввода пароля.



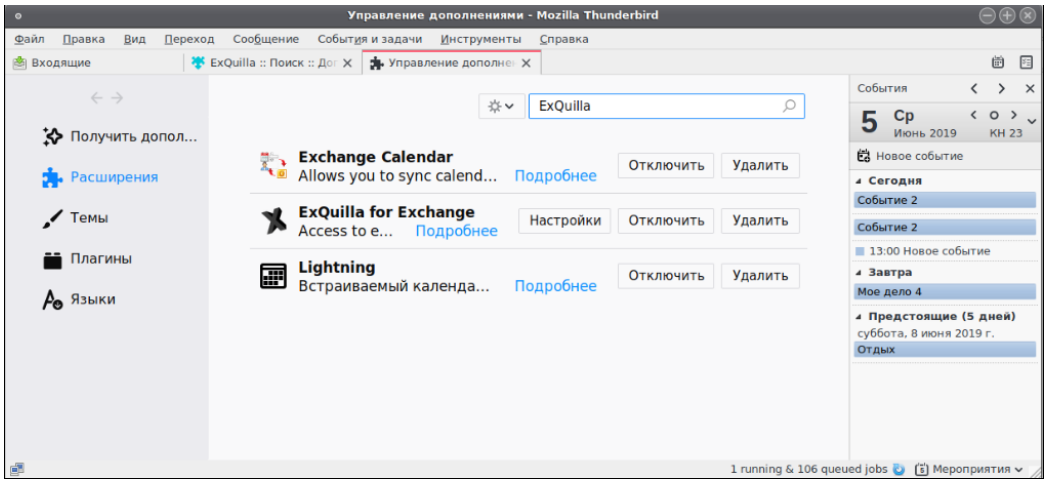
На этом почта подключена. Также автоматически подключен календарь, задачи, заметки. Есть возможность просмотра адресных книг.

Настройка календаря Exchange в Thunderbird

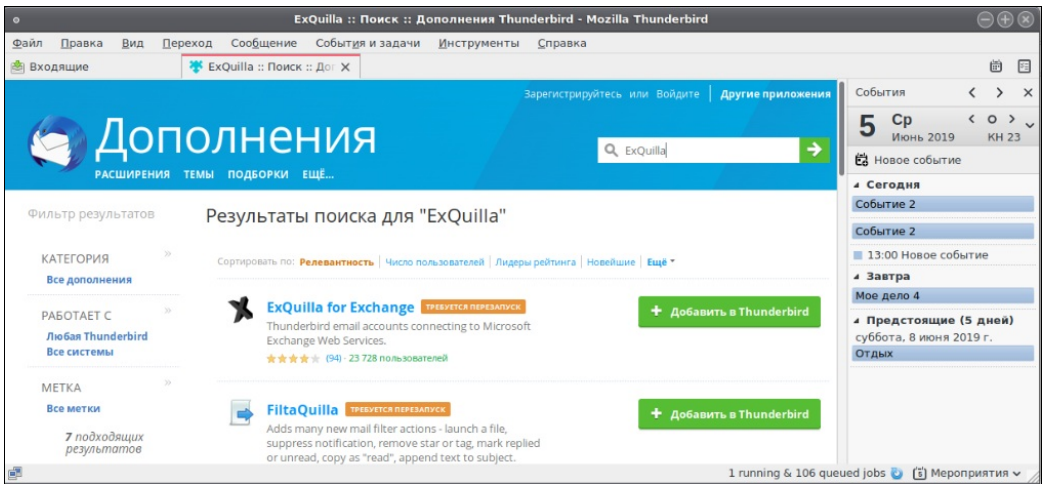
Настройка почты

Для подключения почты Exchange к Thunderbird скачайте и установите плагин ExQuilla for Exchange.

Для этого в меню нажмите Инструменты > Дополнения. В открывшемся окне выберите Расширения и в верхнем правом углу в строку поиска введите "ExQuilla".



В списке найденного нажмите кнопку "Добавить в Thunderbird" напротив плагина ExQuilla for Exchange. После установки перезагрузите почтовый клиент.

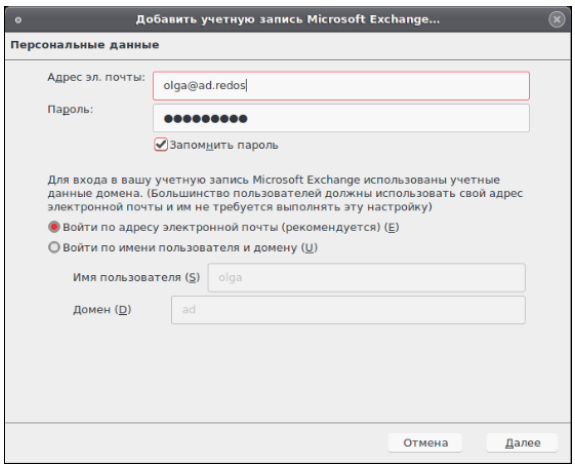


ВАЖНО

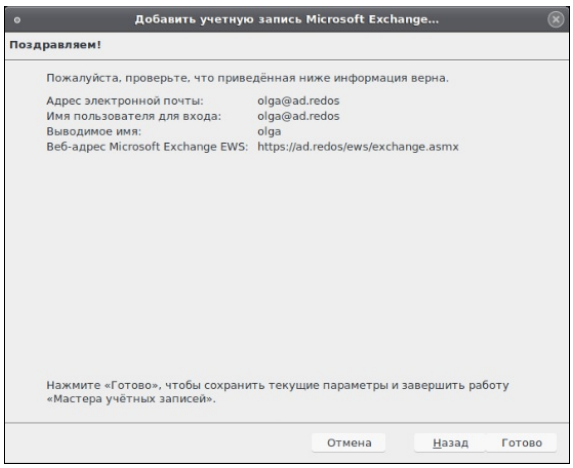
У вас должен быть установлен плагин Lighting

Далее подключите календарь. Выберите меню "Файл" > "Создать" > "Добавить учетную запись Microsoft Exchange".

В открывшемся окне введите адрес эл. почты, пароль и нажмите кнопку "Далее"

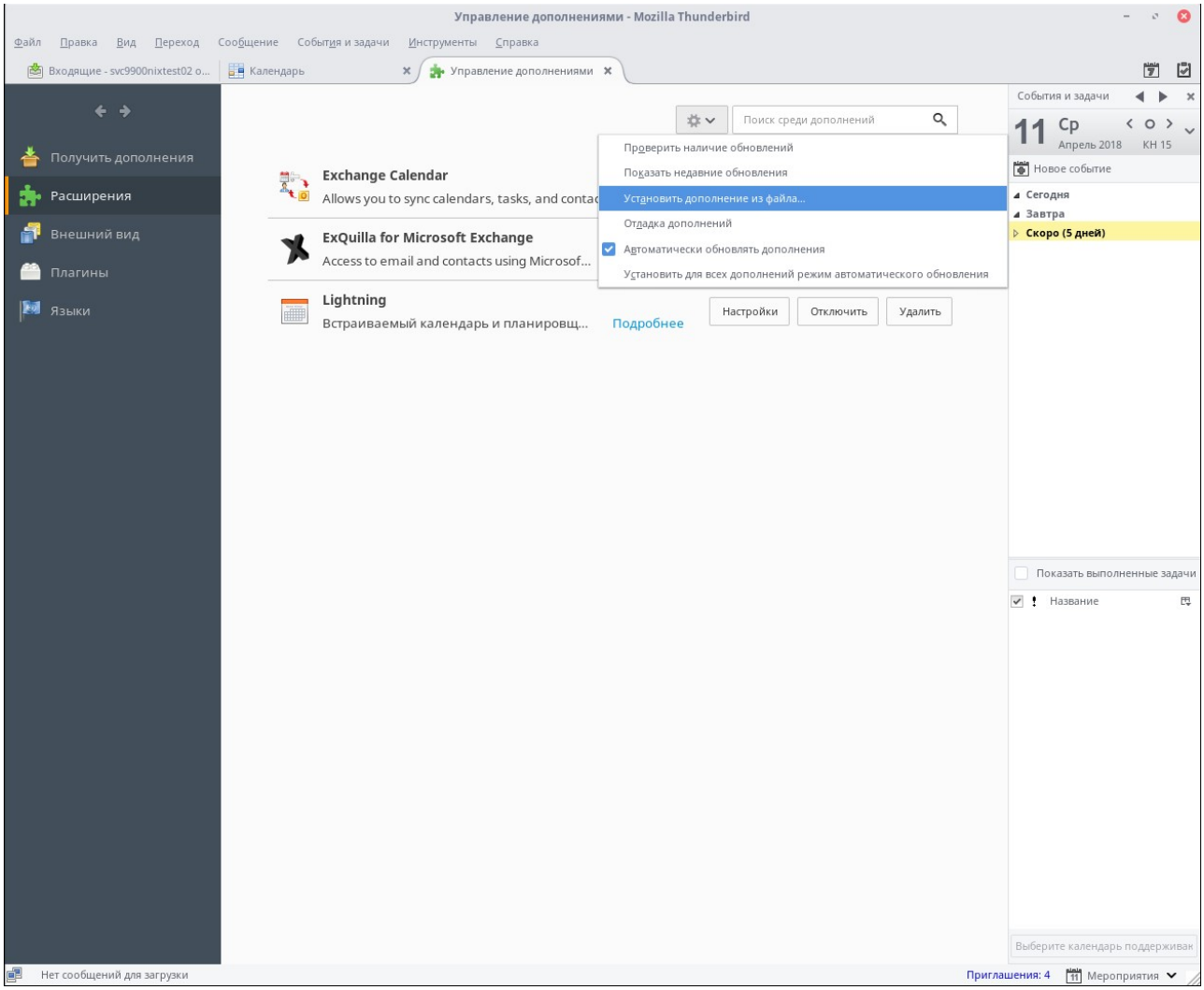


Должен автоматически определится адрес почтового сервера и появиться окно с успешным подключением. Остается только нажать кнопку "Готово".



Настройка календаря

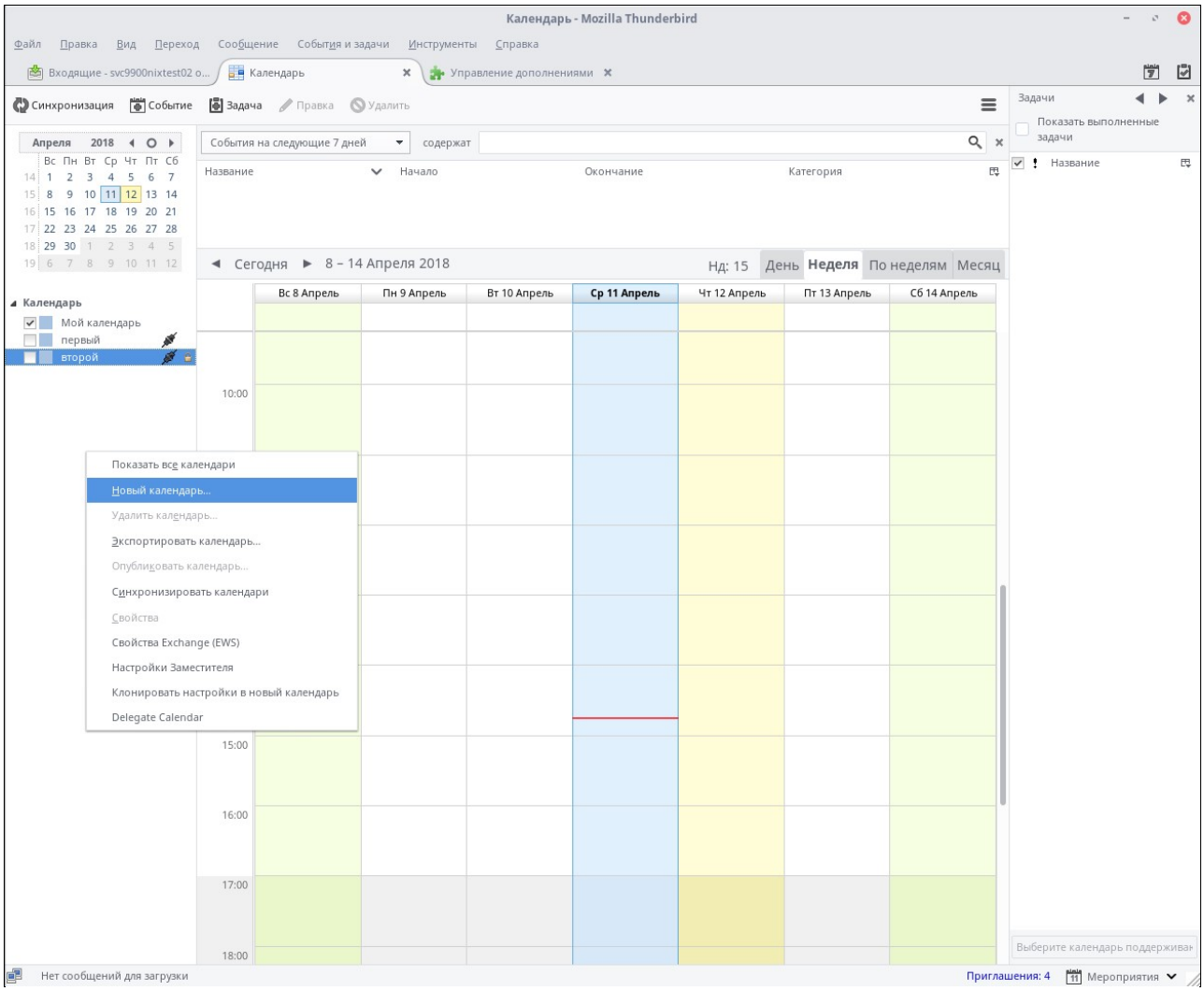
1. Скачайте дополнение ExchangeCalendar по ссылке:
https://github.com/ExchangeCalendar/exchangecalendar/releases
Откройте Thunderbird перейдите в меню и выберите пункт “Дополнения”.
Перейдите на вкладку “Расширения” и нажмите на шестеренку, затем выберите пункт “Установить дополнение из файла”.



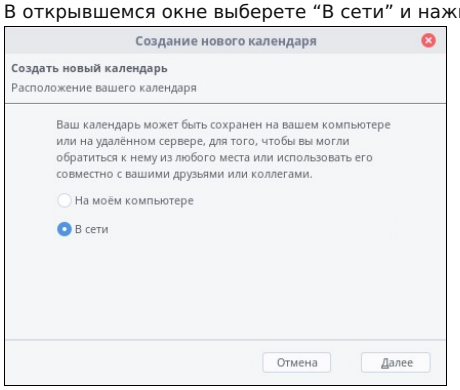
Выберите скачанный файл дополнения и нажмите “Ок”. Затем установите его и перезагрузите почтовый клиент.

2. Добавьте календарь.

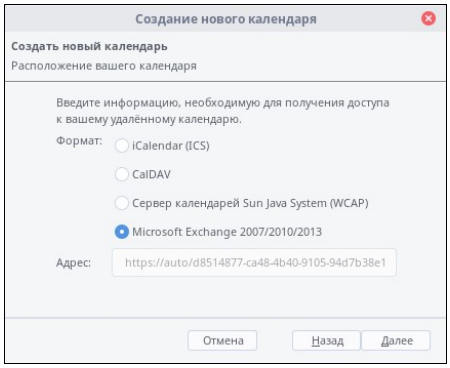
Откройте Thunderbird перейдите на вкладку “Календарь”.
В списке календарей нажмите на правую кнопку мыши и выберете “Новый календарь”.



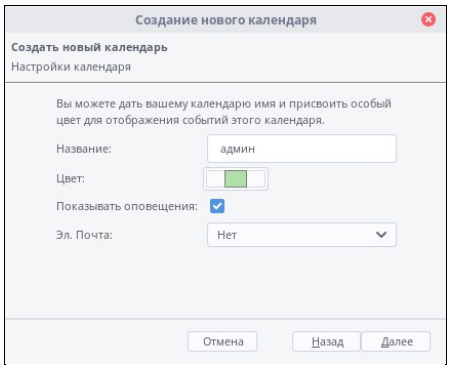
В открывшемся окне выберете “В сети” и нажмите кнопку “Далее”.



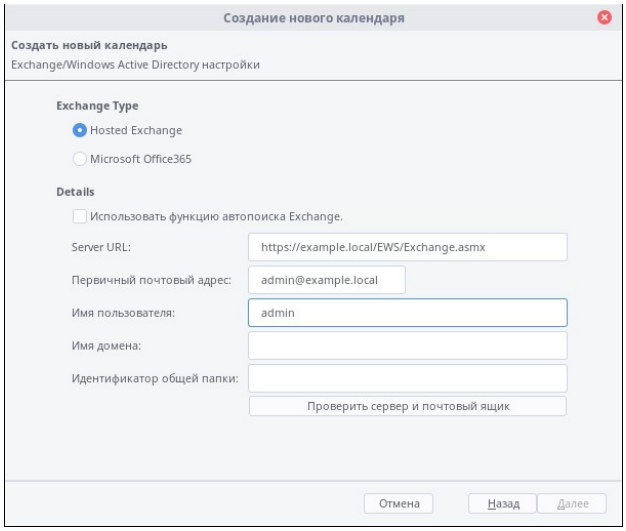
Выберите пункт “Microsoft Exchange 2007/2010/2013” и нажмите кнопку “Далее”.



Введите название календаря, выберите цвет, при выборе электронной почты укажите её или выберите “Нет” и нажмите кнопку “Далее”.



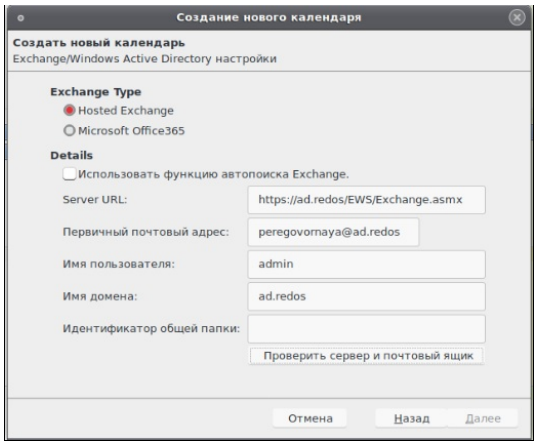
Выберите “Hosted Exchange”, введите Server URL. Обычно, адрес следующий https://<имя почтового сервера>/EWS/Exchange.asmx. Введите первичный почтовый адрес и имя пользователя, затем нажмите кнопку “Проверить сервер и аккаунт”.



В открывшемся окне введите пароль от аккаунта. Окно может появляться несколько раз.
Теперь нажмите кнопку “Далее” и “Готово”.
Календарь подключен.

Подключение общего календаря помещений или оборудования

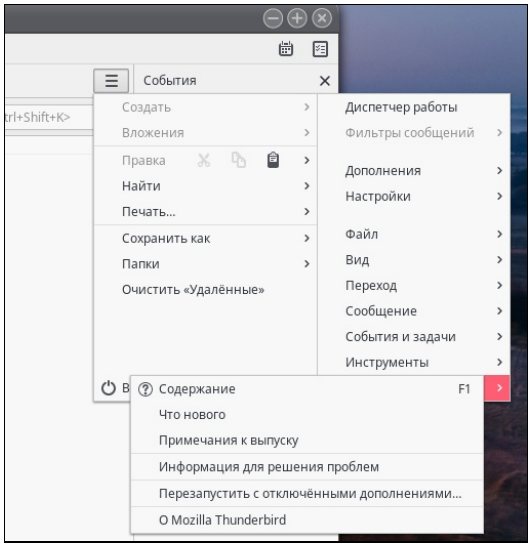
Для подключения любого общего календаря нужно при его подключении вписать в поле "Первичный почтовый адрес" адрес этого календаря. Пример на скриншоте ниже.

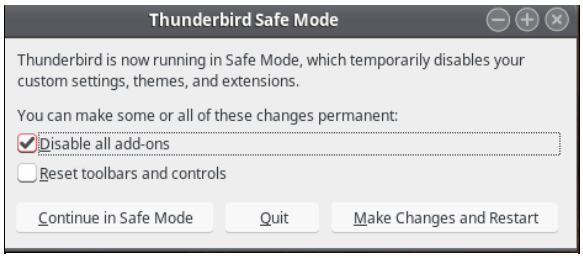


Thunderbird запуск Google-почты

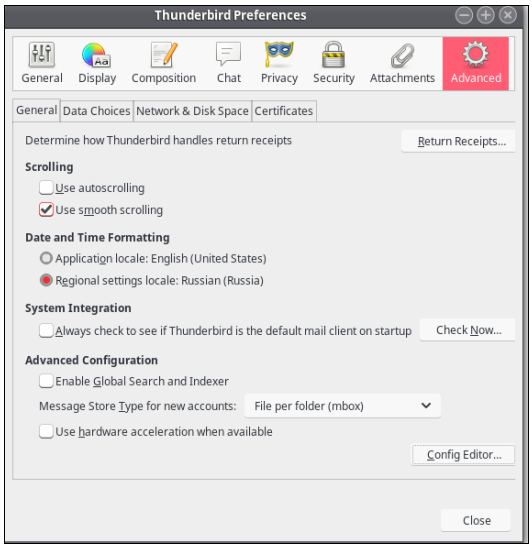
Настройка добавления Google аккаунта в ThunderBird при возникновении проблемы при авторизации с использованием OAuth2:

Включите Безопасный Режим Thunderbird для этого зайдите в Справку-> Перезапустить с отключенными дополнениями -> Disable all add-ons -> Continue in safe mode



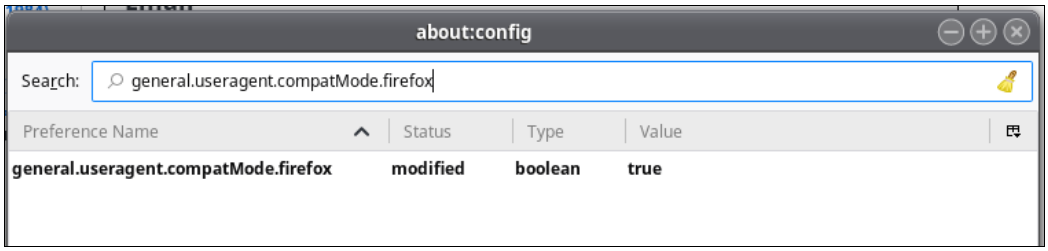


После запуска в безопасном режиме откройте Thunderbird Preferences -> Advanced -> General -> Config Editor -> согласитесь с уведомлением, откроется список доступных конфигураций



Воспользуйтесь поиском **general.useragent.compatMode.firefox** и измените значение на true.

Если параметр отсутствует, добавьте его с меткой boolean, значение true.



Выйдите из безопасного режима и попробуйте ввести данные Google аккаунта.

Настройка NextCloud с СУБД MySQL и ПО для веб-сервера Apache

Установка необходимых пакетов
Настройка SELinux
Настройка MySQL
Установка NextCloud
Настройка NextCloud

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** nextcloud-27.1.10-1, php-8.1.29-1, mariadb-3:10.11.6-2

Nextcloud — набор клиент-серверных программ для создания и использования облачного хранилища. *Nextcloud* можно установить как на хосте, так и на собственном сервере. По доступной функциональности похож на *Dropbox*.

В отличие от проприетарных сервисов, таких как *Dropbox*, открытая архитектура *Nextcloud* позволяет добавлять функциональность на сервер в виде приложений и дает возможность пользователям полностью контролировать свои данные.

Nextcloud позволяет совместно работать с офисными документами, файлами и информацией для планирования задач и мероприятий. Платформа также включает надстройки для доступа к электронной почте, обмена сообщениями, организации видеоконференций и чатов.

Аутентификация пользователей может производиться как по локальной базе, так и через интеграцию с *LDAP/Active Directory, Kerberos, IMAP*, в том числе с применением двухфакторной аутентификации, *SSO* (Single-sign-on) и привязки новых систем к учётной записи по QR-коду. Версионный контроль изменений позволяет отслеживать изменения в файлах, комментариях, правилах совместного доступа и тегах.

Также облачное хранилище поддерживает синхронизацию и обмен данными, предоставляет возможность просмотра и редактирования данных с любого устройства в любой точке сети. Доступ к данным может быть организован как при помощи web-интерфейса, так и с использованием протокола **WebDAV** и его расширений **CardDAV** и **CalDAV**.

Сервер *Nextcloud* можно развернуть на любом хостинге, поддерживающем выполнение PHP-скриптов и предоставляющем доступ к *SQLite, MariaDB/MySQL* или *PostgreSQL*.

Основные компоненты платформы Nextcloud:

1. **Files** - организация хранения, синхронизации, совместного доступа и обмена файлами. Доступ может быть осуществлён как через *Web*, так и при помощи клиентского ПО для настольных и мобильных систем. Предоставляются такие расширенные возможности, как полнотекстовый поиск, прикрепление файлов при отправке комментариев, выборочный контроль доступа, создание защищённых паролем ссылок для загрузки, интеграция с внешними хранилищами (*FTP, CIFS/SMB, SharePoint, NFS, Google Drive, Dropbox* и т.п.).
2. **Flow** - оптимизирует бизнес-процессы через автоматизацию выполнения типовых работ, таких как преобразование документов в PDF, отправка сообщений в чаты при загрузке новых файлов в определённые каталоги, автоматическое назначение тегов. Возможно создание собственных обработчиков, выполняющих действия в привязке к определённым событиям.
3. **Встроенные средства** совместного редактирования документов, электронных таблиц и презентаций на базе пакета *ONLYOFFICE*. Обеспечена полная интеграция *ONLYOFFICE* с остальными компонентами платформы, например, несколько участников могут одновременно редактировать один документ, параллельно обсуждая изменения в видеочате и оставляя заметки.
4. **Photos** - галерея изображений, упрощающая поиск, обмен и навигацию по совместной коллекции фотографий и изображений. Поддерживается ранжирование фотографий по времени, месту, тегам и частоте просмотра.
5. **Calendar** - календарь-планировщик, позволяющий координировать проведение встреч, планировать чаты и видеоконференции. Поддерживается загрузка событий с внешних ресурсов, поддерживающих протокол *WebCal*.
6. **Mail** - совместная адресная книга и web-интерфейс для работы с электронной почтой. Возможна привязка нескольких учётных записей к одному *inbox*. Поддерживается шифрование писем и прикрепление цифровых подписей на базе *OpenPGP*. Возможна синхронизация адресной книги при помощи *CalDAV*.
7. **Talk** - система обмена сообщениями и проведения web-конференций (чат, аудио и видео). Имеется возможность предоставления доступа к содержимому экрана и поддержка SIP-шлюзов для интеграции с обычной телефонией.

Установка необходимых пакетов

Примечание.

Для работы ***NextCloud*** версии ***27*** требуются пакеты ***php*** версии ***8***.

Для корректной настройки *NextCloud* **в РЕД ОС 7.3** необходимо подключить репозиторий **php81-release**, включающий в себя пакеты **php** версии **8**. Подробную информацию о подключении репозитория с пакетами необходимой версии **php** см. в нашей

инструкции «PHP 8.X на РЕД ОС».

Необходимо подготовить систему для установки **NextCloud**, для этого установите следующие пакеты (потребуются права **администратора** системы):

```
sudo dnf install httpd php php-dom php-mbstring php-gd php-pdo php-json php-xml php-zip php-curl php-mcrypt php-pear setroubleshoot-server bzip2 php-ldap php-mysqlnd mariadb mariadb-server mod_auth_kerb php-fpm
```

Настройка SELinux

Примените политики **SELinux**:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_graceful_shutdown 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P domain_can_mmap_files 1
setsebool -P daemons_dump_core 1
```

Настройка MySQL

В качестве базы данных используется **MySQl**.

Запустите и добавьте в автозагрузку службу **mariadb**:

```
sudo systemctl start mariadb && systemctl enable mariadb
```

Выполните скрипт **mysql_secure_installation**, чтобы защитить базу данных от злоумышленников:

```
sudo mysql_secure_installation
```

На первом шаге должен быть задан пароль **root**, по умолчанию пароль не задан, нажмите **Enter**.

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none): <нажмите_Enter>
OK, successfully used password, moving on...
```

Далее укажите свой пароль **root** и удалите анонимных пользователей:

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

Sett root password? [Y/n] y
New password: <задайте_пароль_root>
Re-enter new password: <повторите_пароль_root>
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!
```

Запретите удаленный вход для **root**, если необходимо:

```
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
```

Удалите тестовую базу данных и обновите таблицу привилегий:

```
By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Затем создайте базу данных и пользователя, которые будут использованы для дальнейшей работы.

Для подключения к базе используйте команду **mysql**:

```
mysql -u root -p

CREATE   DATABASE nextcloud;
CREATE USER 'nc_user'@'localhost' IDENTIFIED BY 'qwerqwer';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nc_user'@'localhost';
FLUSH PRIVILEGES;
quit
```

Установка NextCloud

Установите **NextCloud**, выполнив команду:

```
sudo dnf install nextcloud nextcloud-httpd nextcloud-mysql
```

Настройка NextCloud

Создайте виртуальный хост, для этого отредактируйте файл **/etc/httpd/conf.d/nextcloud.conf**:

```
nano /etc/httpd/conf.d/nextcloud.conf
```

Добавив в него следующее содержимое:

```
<VirtualHost *:80>
 ServerName localhost.localdomain
 ServerAdmin admin@localdomain
 DocumentRoot /usr/share/nextcloud
 <directory /usr/share/nextcloud>
 Require all granted
```

```
AllowOverride All
Options FollowSymLinks MultiViews
SetEnv HOME /usr/share/nextcloud
SetEnv HTTP_HOME /usr/share/nextcloud
</directory>
</VirtualHost>
```

где:

- **ServerName** - полное имя сервера.

Создайте пустой файл **CAN_INSTALL** для разрешения установки:

```
touch /usr/share/nextcloud/config/CAN_INSTALL
```

Назначьте владельцем каталога **nextcloud** пользователя **apache**:

```
sudo chown -R apache:apache /usr/share/nextcloud
```

Настройте SELinux:

```
chcon -R -t httpd_sys_rw_content_t /usr/share/nextcloud
```

Добавьте в автозагрузку службу **httpd** и запустите ее:

```
sudo systemctl enable httpd --now
```

Отредактируйте файл **/usr/share/nextcloud/config/config.php**.

Создайте секцию **trusted_domains** в массиве и впишите `<IP-адрес_сервера>` по образцу:

```
$CONFIG = array (
....
'trusted_domains' =>
  array (
    0 => '192.168.0.15',
),
...
)
```

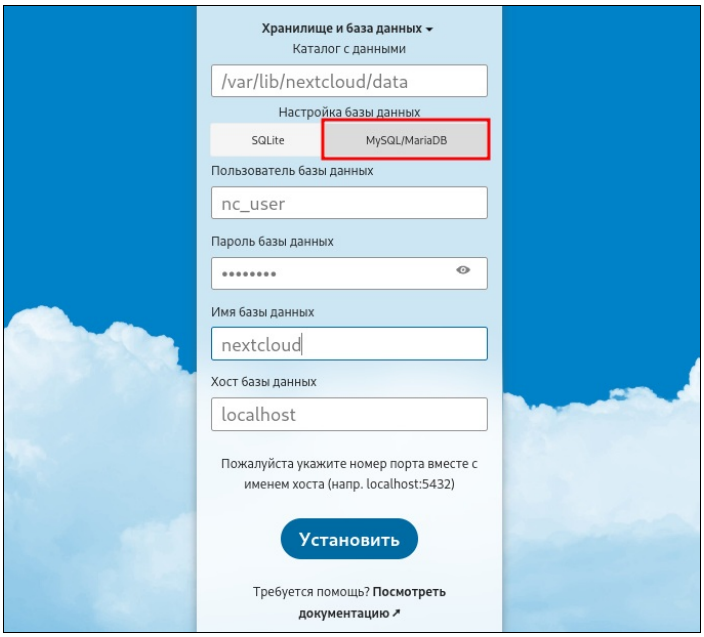
где:

- 192.168.0.15 - IP-адрес вашего сервера.

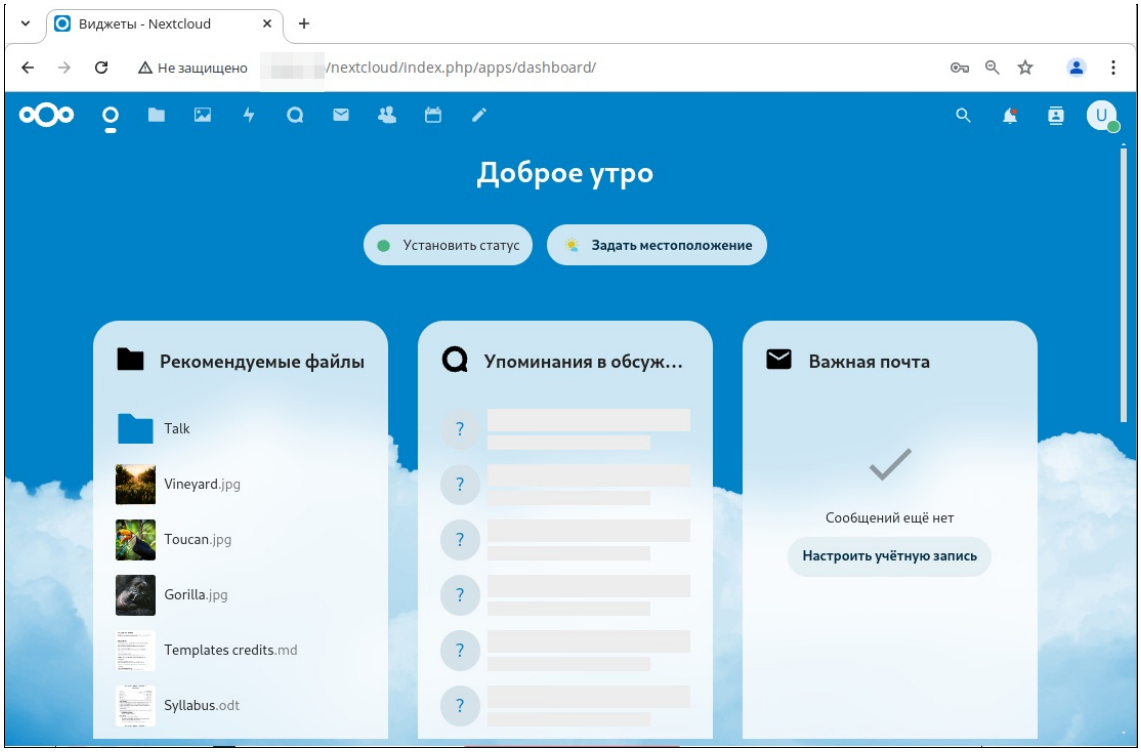
Далее, с помощью браузера, перейдите в веб-интерфейс по адресу - `http://<IP-адрес_сервера>/nextcloud`.

В открывшемся интерфейсе введите *имя* и *пароль* аккаунта будущего администратора сервера, а также выберите в качестве базы данных сервер **MySQL/MariaDB**. Введите ранее созданного пользователя **MySQL** и название базы данных:

- Пользователь: **nc_user**
- Пароль: **qwerqwer**
- Название базы: **nextcloud**
- Хост: **localhost**



Далее нажмите «**Установить**». Установка занимает некоторое время.



На данном этапе установка **NextCloud** завершена.

Настройка NextCloud с СУБД PostgreSQL и ПО для веб-сервера Ngnix

Предварительная подготовка сервера
Настройка SELinux
Установка Nextcloud
Установка PostreSQL14
Настройка PostreSQL
Настройка Nginx
Настройка Nextcloud

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** nextcloud-27.1.10-1, nginx-1:1.26.1-1, postgresql14-server-14.12-2

Nextcloud — набор клиент-серверных программ для создания и использования облачного хранилища. **Nextcloud** можно установить как на хосте, так и на собственном сервере.

Nextcloud позволяет совместно работать с офисными документами, файлами и информацией для планирования задач и мероприятий. Платформа также включает надстройки для доступа к электронной почте, обмена сообщениями, организации видеоконференций и чатов.

В **Nextcloud** есть выбор различных СУБД, в статье будет рассмотрена СУБД **PostgreSQL**, а в качестве ПО для веб-сервера будет выбран **Nginx**.

PostgreSQL — свободная объектно-реляционная система управления базами данных.

Nginx — это программное обеспечение с открытым исходным кодом, которое позволяет создавать веб-сервер.

Ранее мы также рассмотрели настройку **NextCloud** с СУБД **MySQL** и ПО для веб-сервера **Apache** в статье «Настройка NextCloud с СУБД MySQL и ПО для веб-сервера Apache».

Предварительная подготовка сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Настройка SELinux

Настройте **SELinux**:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_graceful_shutdown 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P domain_can_mmap_files 1
setsebool -P daemons_dump_core 1
```

Установка Nextcloud

Примечание.

Для работы ***NextCloud*** версии ***27*** требуются пакеты ***php*** версии ***8***.

Для корректной настройки *NextCloud* **в РЕД ОС 7.3** необходимо подключить репозиторий **php81-release**, включающий в себя пакеты **php** версии **8**. Подробную информацию о подключении репозитория с пакетами необходимой версии **php** см. в нашей инструкции «PHP 8.X на РЕД ОС».

Установка **nextcloud** для РЕД ОС осуществляется командой:

```
dnf install nextcloud nextcloud-postgresql nextcloud-nginx
```

Установка PostreSQL14

Установите **PostgreSQL**:

```
dnf install postgresql14-server
```

Настройка PostreSQL

Выполните инициализацию:

```
/bin/postgresql-14-setup initdb
```

Запустите сервер и добавьте в автозагрузку **PostgreSQL**, проверьте статус:

```
systemctl enable postgresql-14 --now
systemctl status postgresql-14
```

Зайдите под пользователем **PostgreSQL**:

```
su - postgres
```

Подключитесь к базе:

```
psql
```

Затем создайте пользователя и базу данных с именем **nextcloud** и предоставьте пользователю права на использование данной БД (**пароль укажите свой**):

```
CREATE ROLE nextcloud WITH NOSUPERUSER LOGIN PASSWORD 'nextcloudpassword';
CREATE DATABASE nextcloud WITH OWNER nextcloud;
GRANT ALL PRIVILEGES ON DATABASE nextcloud TO nextcloud;
```

Пример результата выполнения запросов:

```
postgres=# CREATE ROLE nextcloud WITH NOSUPERUSER LOGIN PASSWORD 'nextcloudpassword';
CREATE ROLE
postgres=# CREATE DATABASE nextcloud WITH OWNER nextcloud;
CREATE DATABASE
postgres=# GRANT ALL PRIVILEGES ON DATABASE nextcloud TO nextcloud;
GRANT
```

Тестовый запрос на получение списка баз данных:

```
\l
```

Выход из оболочки:

```
\q
```

Выйдите из текущей учетной записи:

```
exit
```

Добавьте разрешение для подключения:

```
nano /var/lib/pgsql/14/data/postgresql.conf
```

Приведите строку к следующему виду:

```
listen_addresses = '*'
```

Затем раскомментируйте строку:

```
#port = 5432
```

Отредактируйте файл **pg_hba.conf**, приведя строки **IPv4** и **IPv6** к следующему виду:

```
nano /var/lib/pgsql/14/data/pg_hba.conf
```

```
# or execute "SELECT pg_reload_conf()".
#
# Put your actual configuration here
# ----------------------------------
#
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.



# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local   all       all                     peer
# IPv4 local connections:
host    all       all    127.0.0.1/32     md5
# IPv6 local connections:
host    all       all    ::1/128          md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication    all                     peer
host    replication    all    127.0.0.1/32     scram-sha-256
host    replication    all    ::1/128          scram-sha-256
```

Затем выполните перезапуск демона **PostgreSQL**:

```
systemctl restart postgresql-14
```

Настройка Nginx

Запустите веб-сервер **Nginx**:

```
systemctl enable nginx  --now
systemctl status nginx
```

Приведите файл **nginx.conf** к следующему виду:

```
nano /etc/nginx/nginx.conf
```

```
....
 server {
    listen 80;
    listen [::]:80;
    server_name <ip_сервера>; #укажите IP-сервера
     proxy_connect_timeout 600s;
```

```
    proxy_send_timeout 600s;
    proxy_read_timeout 600s;
    fastcgi_send_timeout 600s;
    fastcgi_read_timeout 600s;
    sendfile on;
    root /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
    location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
      location = /50x.html {
    }
}
```

Перезапустите веб-сервер:

```
systemctl restart nginx
```

Выполните проверку настроек **Nginx**:

```
nginx -t
```

Вывод должен быть вида:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Откройте файл **php.ini** и приведите параметры к следующему виду:

```
nano /etc/php.ini
```

```
;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;
max_execution_time = 3600
max_input_time = 3600
max_input_vars = 1000 #расскоментировать строку
memory_limit = 512M
;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;
upload_tmp_dir = /tmp/
```

Настройка Nextcloud

Создайте пустой файл **CAN_INSTALL** для разрешения установки:

```
touch /usr/share/nextcloud/config/CAN_INSTALL
```

Назначьте владельцем каталога **nextcloud** пользователя **apache**:

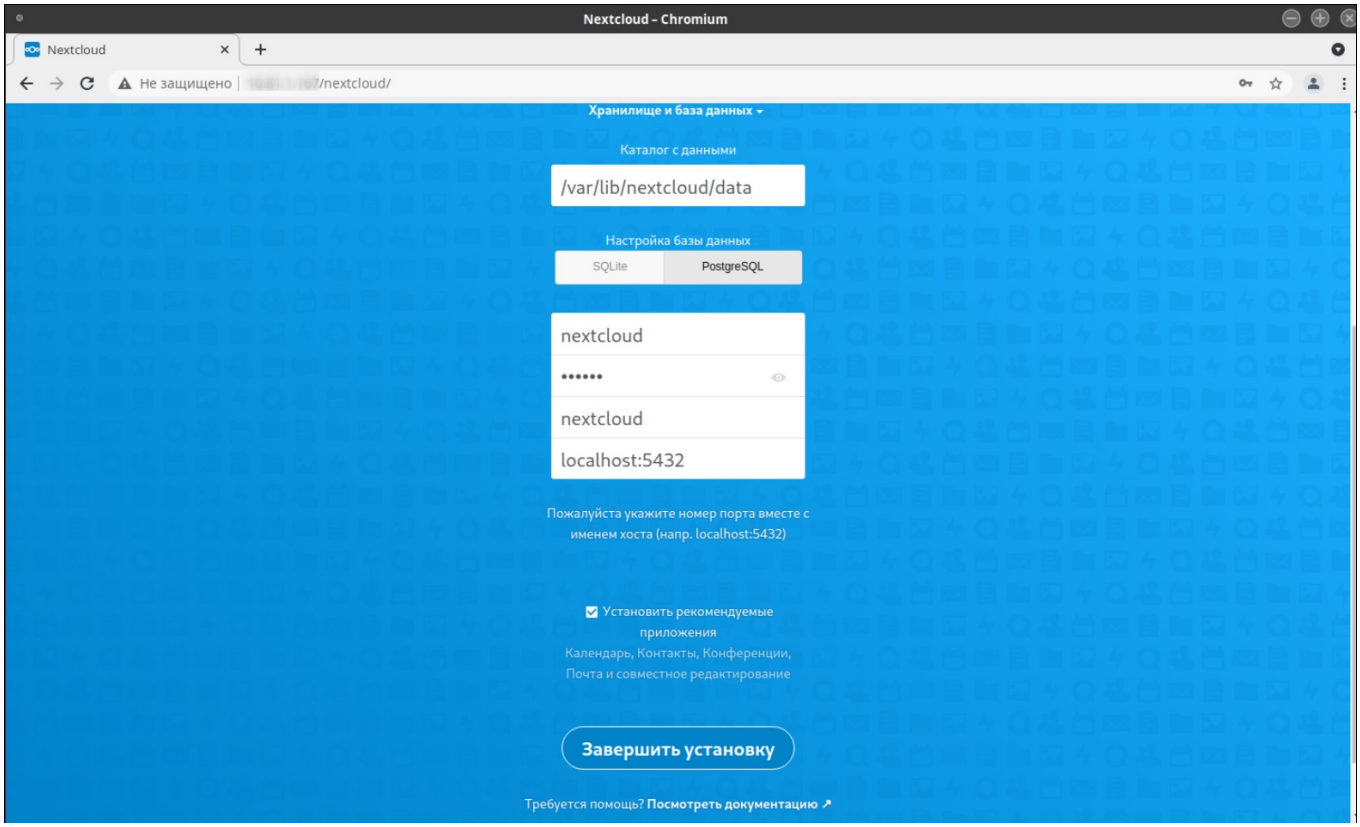
```
sudo chown -R apache:apache /usr/share/nextcloud
```

Настройте SELinux:

```
chcon -R -t httpd_sys_rw_content_t /usr/share/nextcloud
```

В браузере перейдите по ссылке вида http://<ip_сервера>/nextcloud.

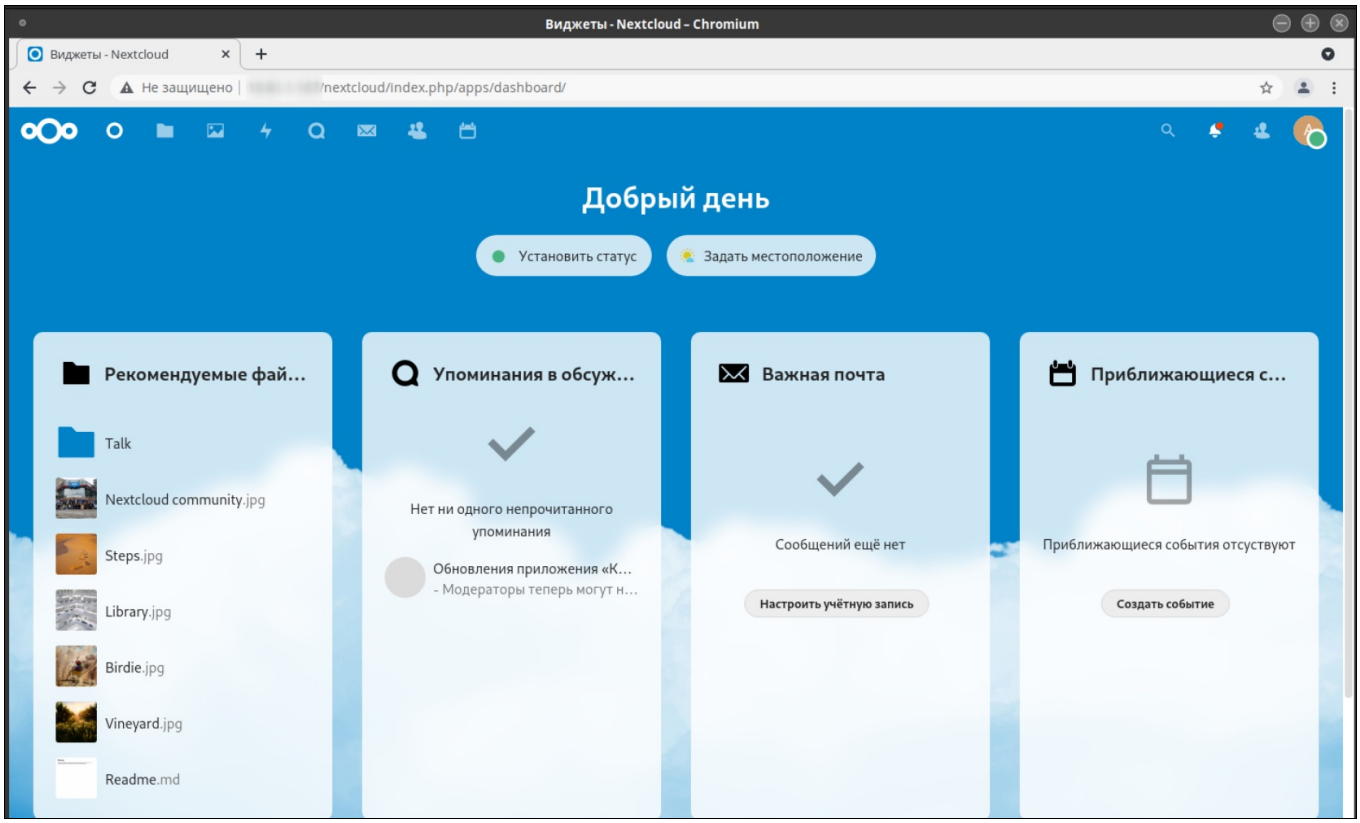
На данном этапе необходимо создать учетную запись администратора и выбрать в поле «**Хранилище и база данных**» - «**PostgreSQL**».



Укажите следующие данные для подключения:

- пользователь базы данных – **nextcloud**;
- пароль базы данных – **nextcloudpassword**;
- название базы данных – **nextcloud**;
- localhost – **localhost:5432**.

Далее нажмите «**Завершить установку**». Установка занимает некоторое время.



На данном этапе установка **Nextcloud** завершена.

Настройка автоматического входа в NextCloud в домене IPA

> Для автоматического входа сервер и клиенты **NextCloud** должны быть клиентами **IPA**. Должен быть выполнен вход под учетной записью IPA.

На сервере IPA получите kerberos-тикет администратора для создания сервиса HTTP и создайте его.

```
# kinit admin
# ipa service-add HTTP/nc.ipa.test
```

где, nc.ipa.test - это сервер NextCloud.

Сгенерируйте kerberos-тикет для сервера NextCloud.

```
# ipa-getkeytab -s dc.ipa.test -p HTTP/nc.ipa.test -k /etc/httpd/http.keytab
```

Назначьте необходимого владельца и права на файл тикета.

```
# chown root:apache /etc/httpd/http.keytab
# chmod 640 /etc/httpd/http.keytab
```

Отредактируйте конфигурационный файл NextCloud приведя его к следующему виду:

```
# nano /etc/httpd/conf.d/nextcloud.conf
Alias /nextcloud "/var/www/html/nextcloud/"
<Directory /var/www/html/nextcloud/>
  Options +FollowSymlinks
  AllowOverride All
<IfModule mod_dav.c>
  Dav off
</IfModule>
SetEnv HOME /var/www/html/nextcloud
SetEnv HTTP_HOME /var/www/html/nextcloud
</Directory>

<Location "/nextcloud/index.php/apps/user_saml/saml/login">
    AuthType Kerberos
    AuthName "Kerberos Login"
    KrbServiceName HTTP
    KrbMethodNegotiate On
    KrbLocalUserMapping On
    KrbMethodK5Passwd Off
    KrbSaveCredentials Off
    KrbVerifyKDC On
    KrbAuthRealms IPA.TEST
    Krb5KeyTab /etc/httpd/http.keytab
    Require valid-user
</Location>
```

Перезагрузите httpd

```
# systemctl restart httpd
```

Отредактируйте файл /usr/share/nextcloud/config/config.php

В секцию trusted_domains впишите hostname этого сервера по образцу:

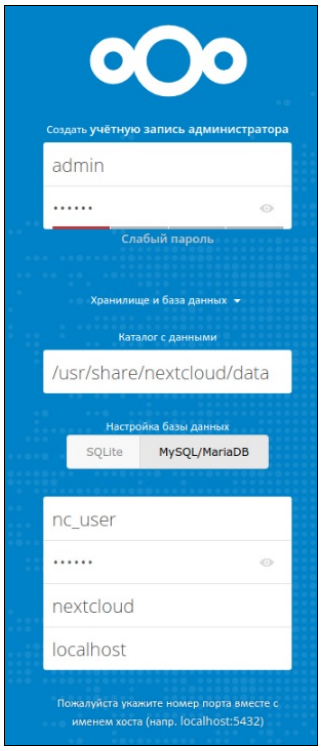
```
1 => 'nextc.ipa.test',
```

Далее, с помощью браузера, зайдите в веб интерфейс по адресу

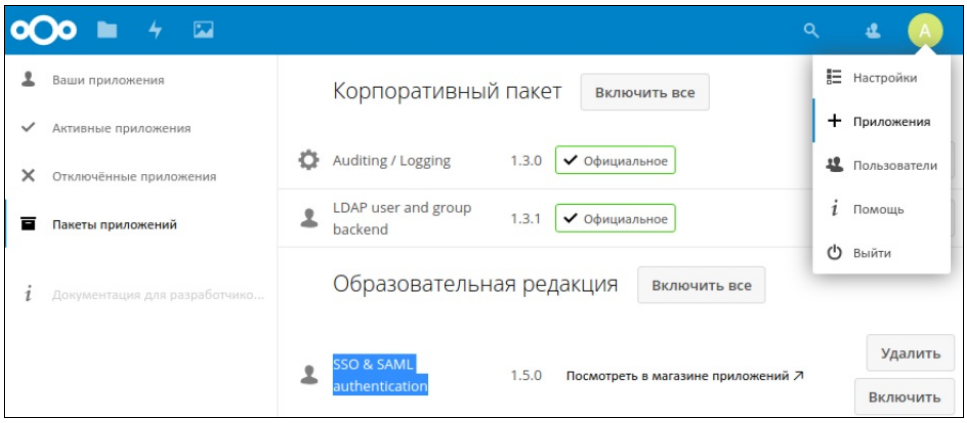
http://<ip адрес сервера>/nextcloud

В открывшемся интерфейсе введите имя и пароль аккаунта бедующего администратора сервера, а так же выберите в качестве базы данных сервер MySQL/MariaDB
Введите ранее созданного пользователя MySQL и название базы данных.
Пользователь: nc_user

Пароль: 12345
Название базы: nextcloud
Хост: localhost



Далее включите плагины для работы с LDAP и SSO. Для этого в правом верхнем углу выберите Приложения, в открывшемся окне, в меню выберите Пакеты приложений. Включите плагины LDAP user and group backend и SSO & SAML authentication.



Настройте доступ к LDAP.

Выберите в верхнем правом углу пункт Настройки, в открывшемся окне в меню пункт Интеграция LDAP/AD. Введите данные подключения.

Сервер: ldap://dc.ipa.test

Порт: 389

Пользователь DN: uid=admin,cn=users,cn=accounts,dc=ipa,dc=test

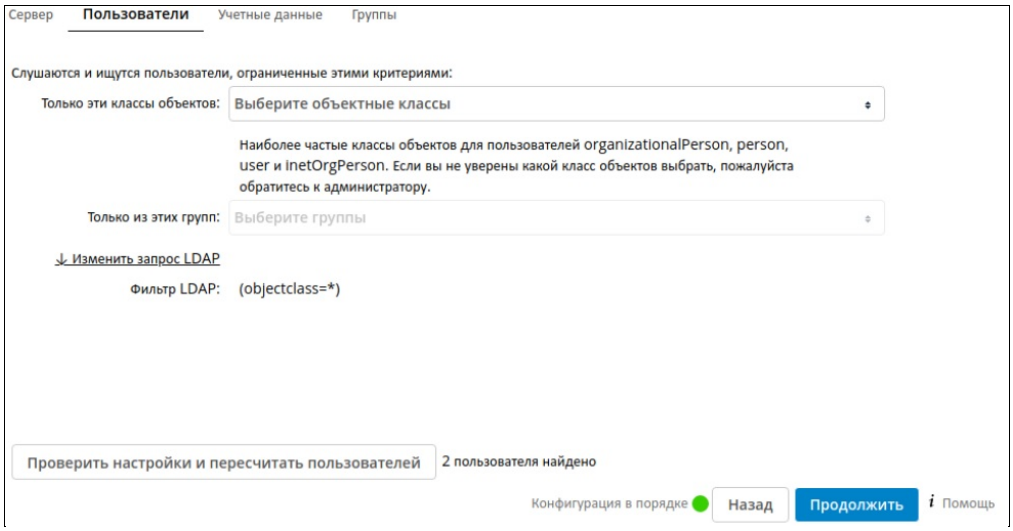
Пароль: qwerqwert12

База DN: dc=ipa,dc=test

Нажмите Проверить базу поиска DN

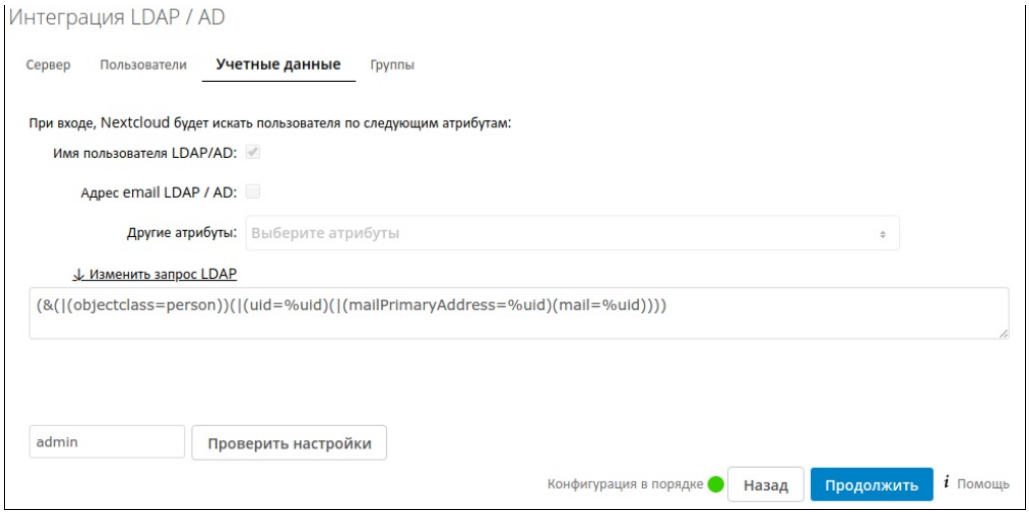
Если все хорошо, нажмите Продолжить.

Выставите все так, как на скриншоте ниже и нажмите "Проверить" и пересчитать пользователей.



В следующем окне измените запрос LDAP на
(&(|(objectclass=person))(|(uid=%uid)(|(mailPrimaryAddress=%uid)(mail=%uid))))

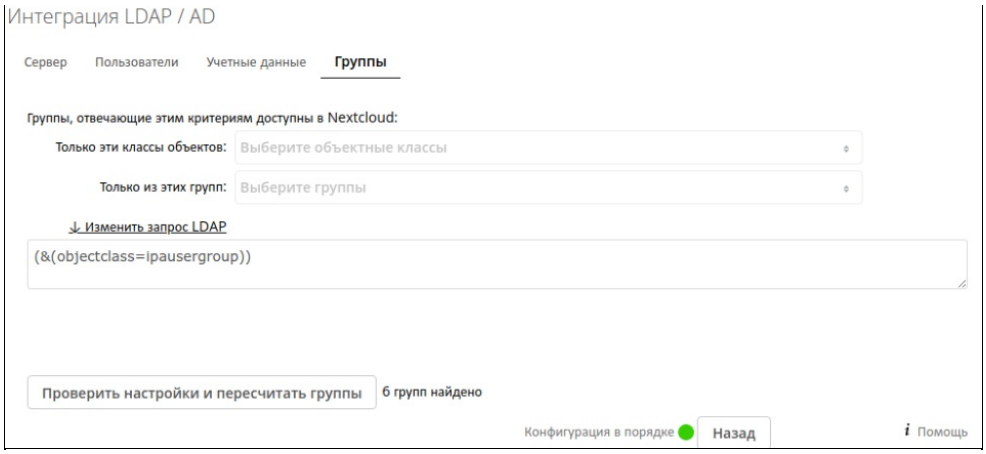
Впишите пользователя admin и проверьте настройки



В следующем окне измените запрос LDAP на

```
(&(objectclass=ipausergroup))
```

Нажмите Проверить базу поиска DN



На этом настройка LDAP завершена.

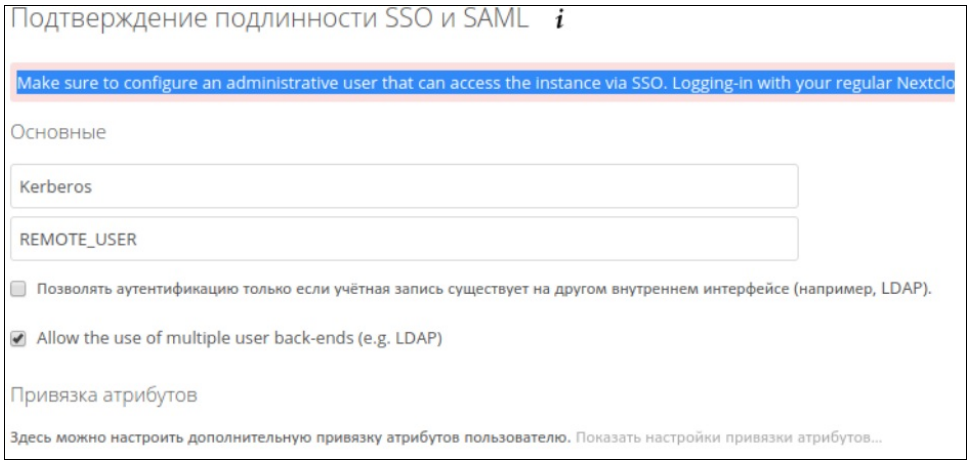
Перейдите к настройке SSO.

Перейдите в меню в пункт Подтверждение подлинности SSO и SAML

Выберите переменные окружения

Введите в верхнее поле отображаемое имя подключения, например Kerberos
В нижнее поле uid REMOTE_USER

Поставьте галку Allow the use of multiple user back-ends



На этом конфигурация закончена.

Настройка SSO на клиенте

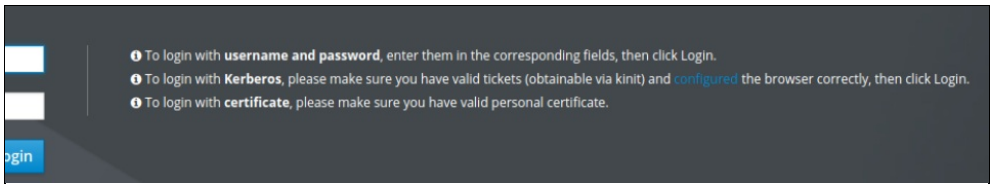
Зайдите на клиенте под учетной записью домена ipa.

Для работы с SSO нужно настроить браузер

Инструкцию по настройке можно найти в панель входа в ipa домен по адресу

https://<имя сервера ipa>

Нажать на ссылку Configured



Для Firefox

1. Импортируйте сертификат нажав на кнопку Import Certificate Authority certificate

Поставьте все три галки.

2. В адресной строке Firefox введите **about:config** для отображения списка текущих параметров конфигурации.
3. В поле «Поиск» введите, **negotiate**, чтобы ограничить список параметров.
4. Дважды щелкните запись network.negotiate-auth.trusted-uris, чтобы отобразить диалоговое окно «Введите значение(строка)».
5. Введите имя домена, в котором вы хотите выполнить аутентификацию, например, .ipa.test.
6. Перейдите на страницу Nextcloud в вашей сети и нажмите кнопку Kerberos. После этого вход будет произведен.

Подключение РЕД ОС к облачным сервисам

Веб-интерфейс
Специальная программа
WebDAV

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** yandex-disk-0.1.6.1080-1

В данной статье будут рассмотрены возможности подключения РЕД ОС к облачным сервисам на примере *Яндекс.Диска*.

Яндекс.Диск — это сервис, который позволяет вам хранить файлы на серверах Яндекса. Вы можете работать с файлами на Диске с любого устройства, подключенного к интернету.

Подключение к Диску можно осуществить тремя способами:

1. Через веб-интерфейс.

2. С помощью специальной программы.

3. С использованием протокола WebDAV.

Вы можете подробнее ознакомиться с возможностью подключения РЕД ОС к облачным сервисам, просмотрев наши обучающие видео:

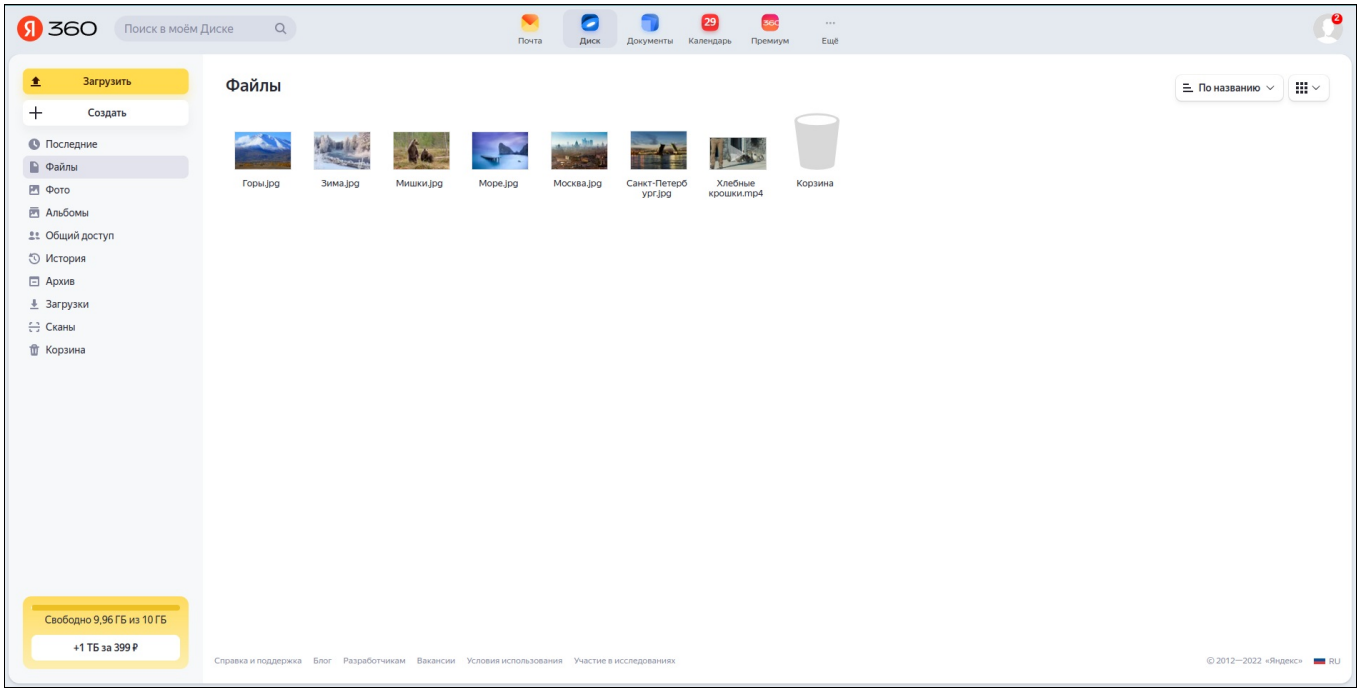
- на **RuTube** — Подключаем РЕД ОС (Linux) к облаку Яндекс.Диск. Web-Интерфейс, GUI программа или протокол WebDAV ;
- в **Яндекс.Дзен** — Подключаем РЕД ОС (Linux) к облаку Яндекс.Диск. Web-Интерфейс, GUI программа или протокол WebDAV .
- в **VK Видео** — Подключаем РЕД ОС (Linux) к облаку Яндекс.Диск. Web-Интерфейс, GUI программа или протокол WebDAV .

На наших каналах вы также сможете найти много другой полезной информации.

Веб-интерфейс

Для подключения через веб-интерфейс необходимо в браузере перейти на страницу Яндекс.Диска и войти в свою учетную запись или создать новую. После авторизации будет открыто ваше облачное хранилище.

Веб-интерфейс прост и интуитивно понятен.



Специальная программа

Для использования *Яндекс.Диска* на компьютере необходимо установить специальную программу.

Перейдите на страницу Яндекс.Диска. В открывшемся списке доступных программ выберите «**yandex-disk-latest.x86_64**» в формате **.rpm**. Начнется загрузка пакета.

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

Затем откройте папку со скачанным пакетом:

```
cd /home/user/Загрузки/
```

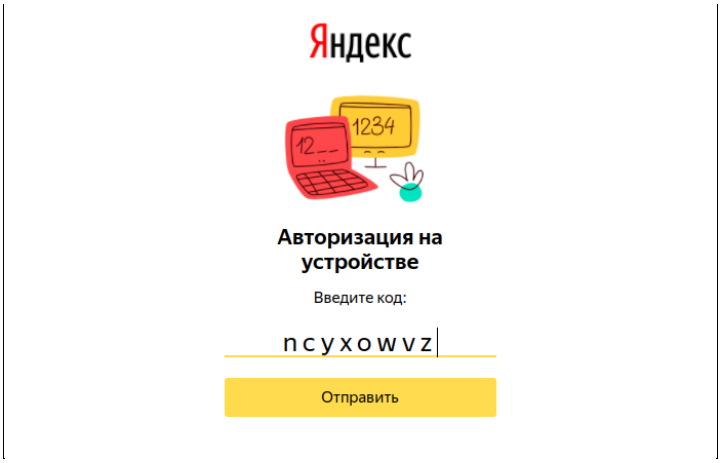
После этого запустите установку программы:

```
dnf install yandex-disk-latest.x86_64.rpm
```

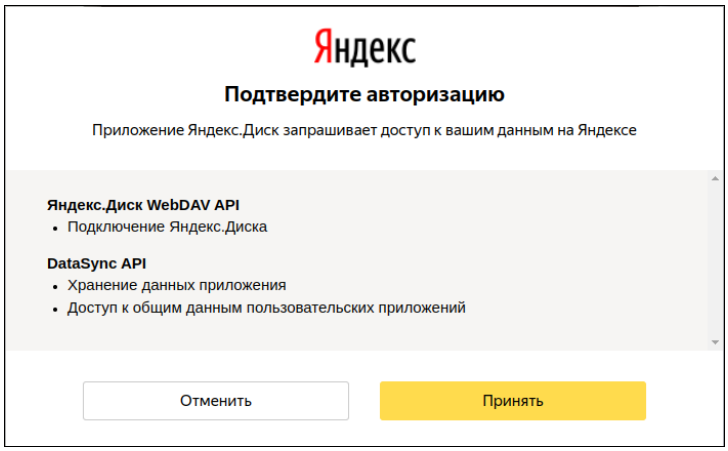
После установки программа сможет работать только в консольном режиме, поэтому необходимо открыть в терминал и выполнить команду:

```
yandex-disk setup

Использовать прокси-сервер? [y/N]: n
Авторизация
Если у вас ещё нет аккаунта на Яндексе, его можно завести по ссылке https://passport.yandex.ru/passport?mode=register

Откройте страницу 'https://ya.ru/device' и введите код ‘ncyxowvz’ в течение 300 секунд. Убедитесь, что вы авторизованы в браузере с нужным аккаунтом.
```

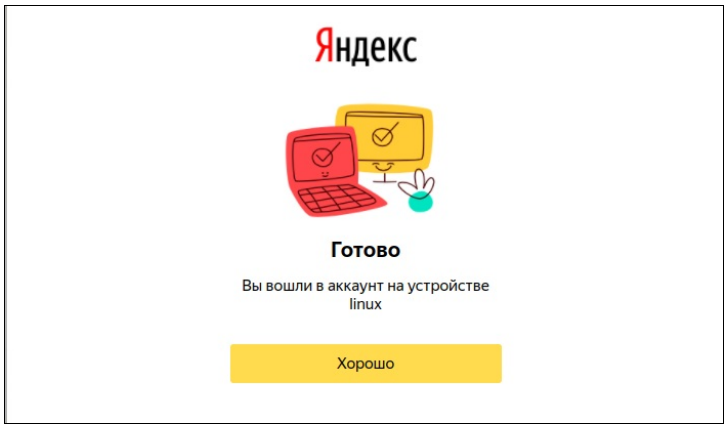
В выводе команды появится ссылка и код авторизации. В браузере перейдите по указанной ссылке и введите код. Убедитесь, что вы авторизованы в браузере с нужным аккаунтом.



Далее необходимо принять запрос на доступ к вашим данным на Диске.



Если все прошло успешно, появится следующее окно.



Проверить работу Яндекс.Диска можно командой:

```
yandex-disk status
```

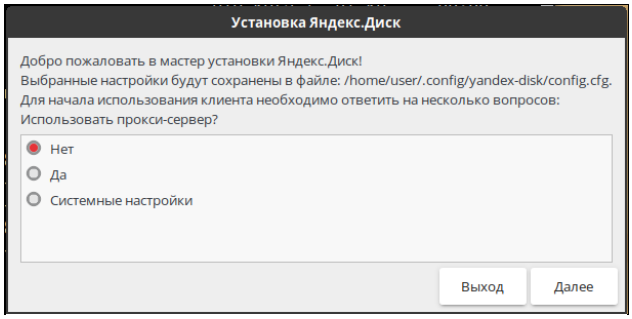
Для установки графической утилиты Диска, перейдите на страницу инструкции по установке «GUI для консольного клиента Linux». Для примера выбран вариант **YD-tools**. На открывшейся странице перейдите по ссылке с инструкцией и скачайте необходимый файл.

После этого откройте терминал, перейдите в папку со скачанным файлом и выполните установку утилиты:

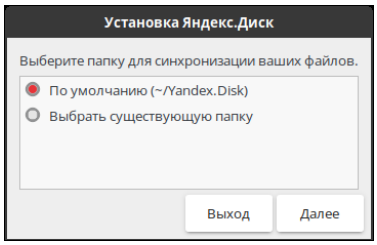
```
cd /home/user/Загрузки/
dnf install yandex-disk-indicator-1.11.0-1.noarch.rpm
```

После установки утилита будет доступна из «**Главного меню**» - «**Интернет**» - «**Индикатор Yandex.Disk**».

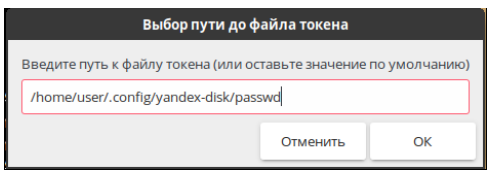
При первом запуске необходимо настроить сервис. На запрос использования прокси-сервера выберите «**Нет**».



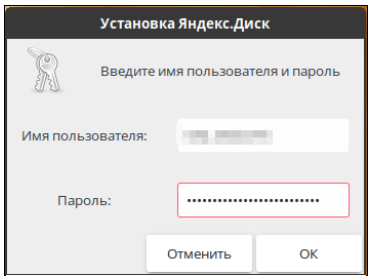
Далее необходимо указать папку, которая будет использоваться сервисом, в примере используется значение по умолчанию.



Затем необходимо указать путь к файлу, который будет хранить учетные данные для доступа к Яндекс.Диску.

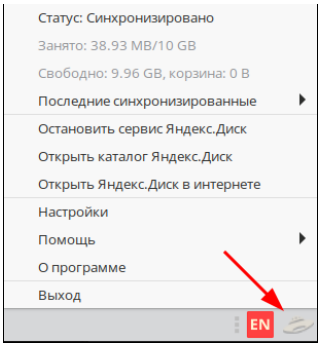


После этого необходимо указать логин и пароль вашей учетной записи на Яндекс.



На этом настройка сервиса завершена.

В системном трее появится соответствующий значок приложения, с помощью которого можно управлять всеми функциями Диска. При запуске программы автоматически будет запущена синхронизация Диска, данные будут сохранены в указанной вами папке при настройке консольной утилиты.

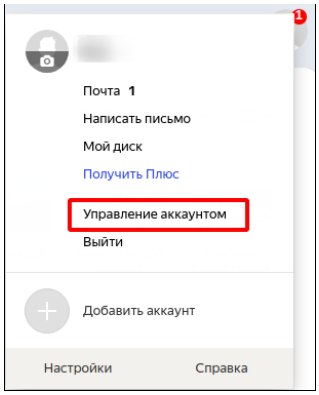


При наведении курсора на значок Яндекс.Диска в системном трее вы увидите надпись «**Синхронизировано**» - это означает, что Диск теперь подключен к компьютеру. Изменить параметры синхронизации можно в настройках.

WebDAV

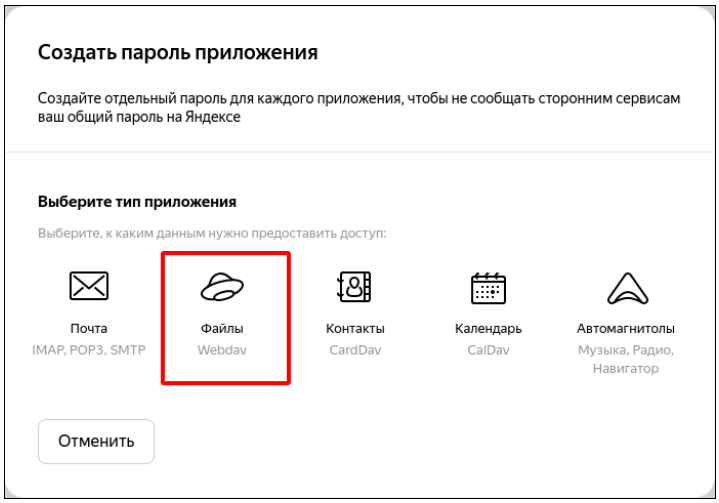
Существует также третий способ подключения РЕД ОС к облачному сервису — с использованием протокола **WebDAV**. Данный способ подключает облачный сервис как сетевой диск, некоторые возможности в таком режиме недоступны, однако работать с файлами удобнее, и требуется меньше ресурсов ОС.

Для того чтобы подключиться к Яндекс.Диску по протоколу **WebDAV**, необходимо создать пароль приложения. Для этого авторизуйтесь в своей учетной записи Яндекс и откройте страницу «**Управление аккаунтом**».

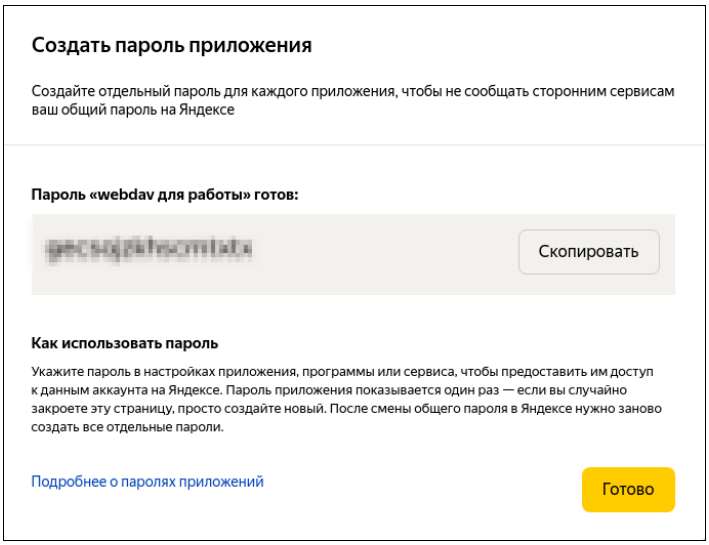


В разделе «Пароли и авторизация» выберите «**Включить пароли приложений**». Подтвердите действие и нажмите «**Создать новый пароль**».

Выберите тип приложения — **WebDAV**.



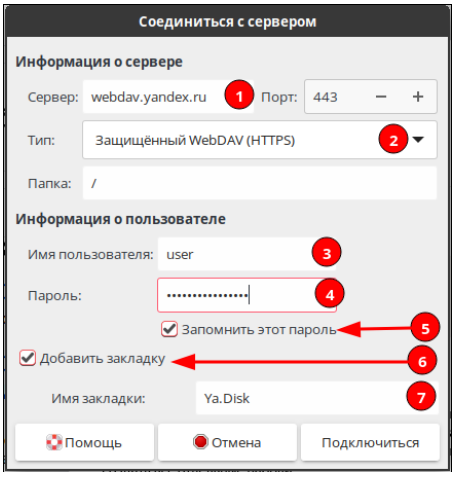
Введите понятное для вас название создаваемого пароля, например, «*webdav для работы*». Пароль с таким именем будет отображаться в списке. Нажмите кнопку «**Создать**». Пароль приложения отобразится во всплывающем окне.



Пароль приложения — это отдельный пароль, который будет создан специально для подключения вашего Яндекс.Диска по протоколу **WebDAV**. Такой пароль безопасен и не предоставит доступ к управлению вашим аккаунтом.

После создания отдельного защищенного пароля можно переходить к настройке подключения. Для этого откройте файловый менеджер *Caja*, перейдите в пункт меню «**Файл**» - «**Соединиться с сервером...**».

В появившемся окне введите следующие данные:



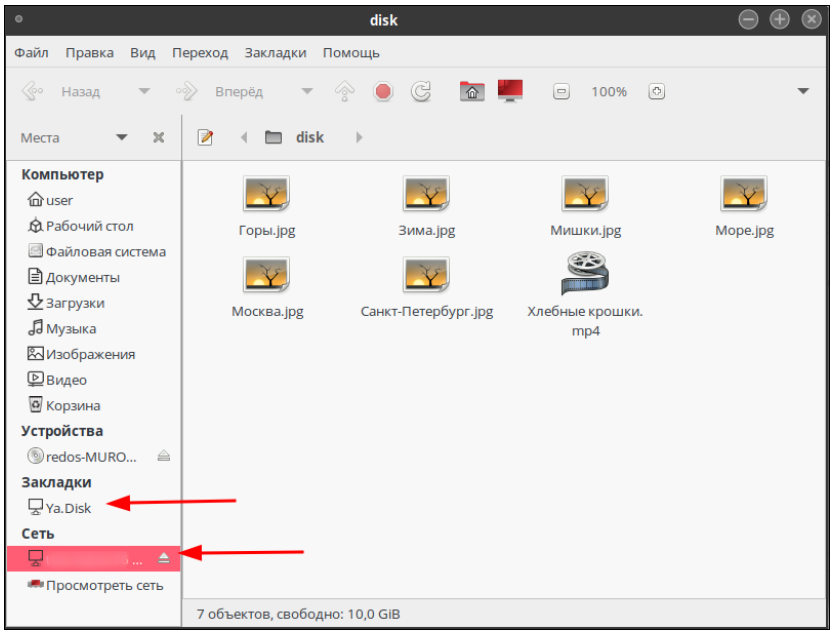
1. Имя сервера — **webdav.yandex.ru**.
2. Тип протокола для подключения — **Защищенный WebDAV (HTTPS)**.
3. **Имя** пользователя.
4. **Пароль** — созданный защищённый пароль.

5. Установить / снять флаг запоминания пароля.
6. Для восстановления подключения можно добавить закладку.
7. При добавлении закладки необходимо указать ее имя.

После этого нажмите «**Подключиться**».

После успешного подключения в группе **Сеть** будет активна запись, с правой стороны которой будет доступна кнопка **Извлечь** для отключения от Диска.

Если вы сохранили закладку, данная запись появится. Если закладку не сохраняли, то при активном соединении ее можно добавить через пункт меню «**Закладки**» - «**Добавить закладку**».



Облачные сервисы, которые поддерживают протокол **WebDAV**, настраиваются аналогичным образом.

WebDAV, neon и chezdav для настройки облачного сервиса

Утилита neon
Утилита chezdav
Синтаксис chezdav
Опции chezdav
WebDAV
Настройки облачного сервиса, поддерживающего протокол WebDAV

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: neon-0.32.1, chezdav-2.3

WebDAV (Web Distributed Authoring and Versioning) — это расширение протокола HTTP, которое позволяет клиентам выполнять удалённое управление и совместное использование файлов на веб-сервере. Оно предоставляет функции для работы с удалёнными файлами, включая создание, чтение, запись и удаление файлов, а также управление правами доступа и блокировками. Утилиты **neon** и **chezdav** являются клиентскими библиотеками, предназначенными для работы с WebDAV-серверами.

Утилита neon

Neon — клиентская библиотека HTTP и WebDAV, предоставляющая высокоуровневый интерфейс для методов HTTP и WebDAV, а также низкоуровневый интерфейс для обработки HTTP-запросов. Neon поддерживает постоянные подключения, прокси-серверы, базовую аутентификацию, Kerberos, SSL.

Neon предназначен для защиты от определённой модели угроз: использования вредоносного HTTP-сервера. В соответствии с этой моделью угроз против клиента возможен целый ряд атак, когда пользователя (или приложение) можно обманом заставить получить доступ к HTTP-серверу, который контролируется злоумышленником.

Возможности:

- Высокоуровневый интерфейс для общих методов **HTTP** и **WebDAV** позволяет отправлять GET- или MKCOL-запросы к ресурсу с помощью одного вызова функции;
- Низкоуровневый интерфейс для обработки HTTP-запросов, позволяющий реализовывать запросы с использованием произвольных методов и заголовков запросов, захватывать произвольные заголовки ответов и т. д.;
- Поддержка постоянного подключения — **neon** группирует набор запросов к серверу в "сеанс", запросы внутри этого сеанса могут использовать постоянно действующее соединение;
- Современная поддержка аутентификации, полная реализация нового стандарта аутентификации RFC2617, включая поддержку **Digest**, **Basic** и **Negotiate**;
- Сеанс может быть настроен на использование прокси-сервера, при этом аутентификация поддерживается как для прокси-сервера, так и для исходного сервера;
- Поддержка SSL/TLS с использованием OpenSSL или GnuTLS, предоставление уровня абстракции для проверки сертификатов сервера, обработки клиентских сертификатов и изучения свойств сертификатов;
- Полная поддержка SSL, простой интерфейс для включения SSL, скрывающий сложность прямого использования библиотеки SSL. Поддержка клиентских сертификатов, проверка сертификатов сервера на основе обратного вызова, а также функции для загрузки сертификатов доверенного центра сертификации. Клиентские сертификаты на основе смарт-карт поддерживаются через интерфейс-оболочку PKCS#11;
- Универсальный интерфейс синтаксического анализа XML для обработки содержимого XML-ответов с использованием SAX-подобных обратных вызовов;
- Поддержка WebDAV, включая блокировку, манипулирование свойствами и извлечение данных, поддержку ACL.

Для установки **neon** выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install neon
```

Основные функции:

- **ne_session *ne_session_create(const char *scheme, const char *hostname, unsigned int port)** — функция создаёт соединения с указанным хостом, принимает в качестве параметров схему, хост и порт, возвращает указатель на новый объект сеанса, который используется в других функциях для выполнения запросов;
- **int ne_get(ne_session *sess, const char *path, int fd)** — получение ресурса по пути path, результат записывается в указанный

int ne_get(ne_session *sess, const char *path, int fd) — получение ресурса по пути path, результат записывается в указанный файловый дескриптор;

- **int ne_put(ne_session *sess, const char *path, int fd)** — изменение ресурса по пути path из файлового дескриптора;
- **int ne_copy(ne_session *sess, int overwrite, int depth, const char *src, const char *dest)** — копирует ресурс из src в dest;
- **int ne_move(ne_session *sess, int overwrite, const char *src, const char *dest)** — перемещает ресурс из src в dest;
- **int ne_delete(ne_session *sess, const char *uri)** — удаляет ресурс по указанному пути;
- **int ne_mkcol(ne_session *sess, const char *uri)** — создаёт директорию struct ne_lock *ne_lock_create(void);
- **int ne_lock(ne_session *sess, struct ne_lock *lock)** — создаёт блокировку на ресурс;
- **int ne_unlock(ne_session *sess, const struct ne_lock *lock)** — снимает блокировку с ресурса;
- **ne_lock** и **ne_unlock** — принимают структуру **ne_lock** в качестве аргумента, содержащую информацию о блокировке на ресурсы.

  Описание полей структуры **ne_lock**:

  - **ne_uri uri** — URI-ресурса, который требуется заблокировать;
  - **int depth** — глубина блокировки, определяющая, на каком уровне блокировки будет применяться операция;
  - **enum ne_lock_type type** — тип блокировки (**shared** — разделяемая блокировка, **exclusive** — исключительная блокировка);
  - **enum ne_lock_scope scope** — область видимости блокировки;
  - **char *token** — уникальный идентификатор блокировки;
  - **char *owner** — владелец блокировки;
  - **long timeout** — таймаут блокировки в секундах.

Утилита chezdav

Утилита **chezdav** также предоставляет возможность работы с WebDAV-серверами, но основной упор делается на удобство использования и предоставление более высокоуровневых функций. Утилита **chezdav** запускает сервер WebDAV. Это позволяет клиентам получать доступ к вашим файлам и изменять их. Для просмотра файлов достаточно простого веб-браузера. Общей папкой по умолчанию является домашний каталог, но вы можете указать другую папку с помощью опции **-P**.

Для установки **chezdav** выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install chezdav
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Для запуска webdav-сервера выполните в терминале команду:

```
chezdav
```

Для вывода списка доступных команд и опций утилиты **chezdav**, а также краткого описания их использования введите команду:

```
chezdav --help
```

Синтаксис chezdav

Утилита **chezdav** доступна для запуска через терминал при помощи команды следующего вида:

```
chezdav [<опции>]
```

Опции chezdav

Основные опции утилиты:

- **-h, --help** — показать параметры справки;
- **--version** — вывести версию программы;
- **-v, --verbose** — подробный вывод;

- **-p, --port** — порт для прослушивания (по умолчанию порт выделяется случайным образом);
- **--local** — слушать только локально;
- **--public** — слушать на всех интерфейсах;
- **-P, --path** — путь для экспорта;
- **-d, --htdigest** — путь к файлу htdigest;
- **-r, --readonly** — только чтение.

WebDAV

Подробную информацию о подключении к облачному сервису с использованием протокола **WebDAV** см. в нашей инструкции «Подключение РЕД ОС к облачным сервисам».

Настройки облачного сервиса, поддерживающего протокол WebDAV

1. Выполните установку **davfs2** в терминале (потребуются права **администратора**):

```
sudo dnf install davfs2
```

2. Создайте точку монтирования (например, **/mnt/webdav**):

```
sudo mkdir /mnt/webdav
```

3. Откройте файл конфигурации **/etc/davfs2/davfs2.conf** на редактирование:

```
sudo nano /etc/davfs2/davfs2.conf
```

Раскомментируйте (уберите символ "#" в начале строки) и установите значение "0" для отключения блокировок в параметре **use_locks**:

```
use_locks 0
```

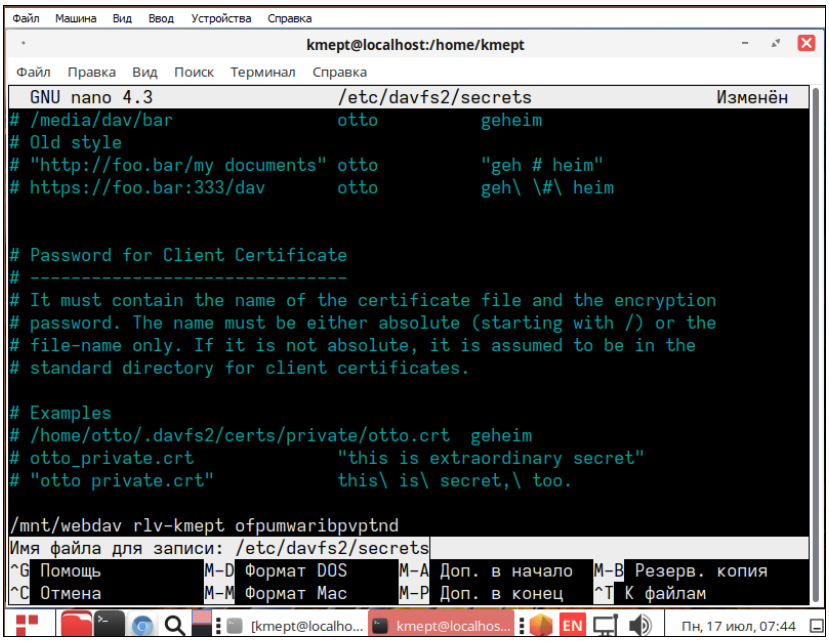
4. Создайте файл с учётными данными для аутентификации:

```
sudo nano /etc/davfs2/secrets
```

Добавьте строку в следующем формате (замените <имя_пользователя> и <пароль> на свои данные):

```
/mnt/webdav <имя_пользователя> <пароль>
```

Сохраните и закройте файл.



5. Установите права доступа для файла с учётными данными:

```
sudo chmod 600 /etc/davfs2/secrets
```

6. Добавьте свойства монтирования в файл **/etc/fstab** для автоматического монтирования при загрузке системы:

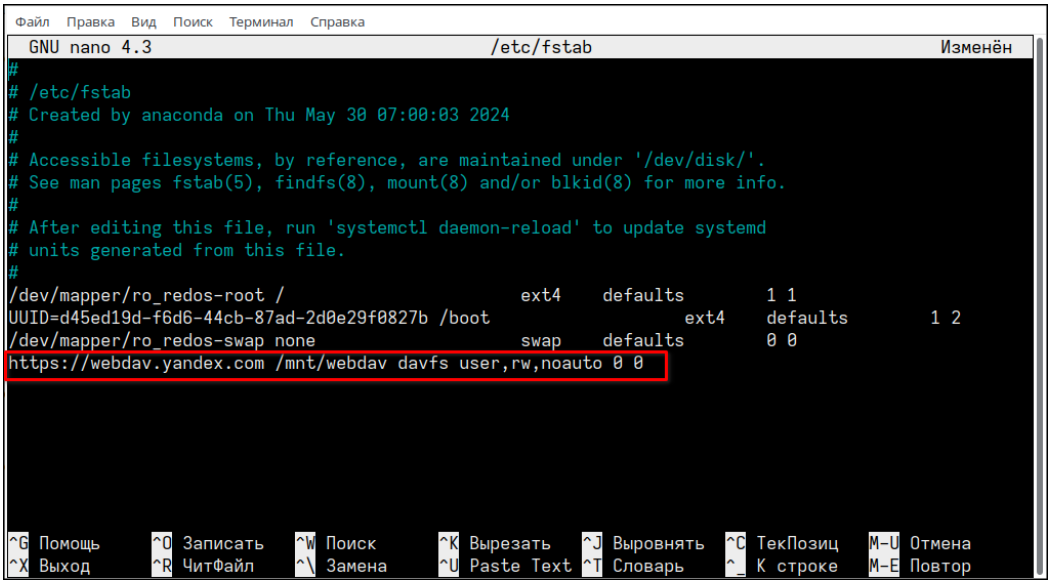
```
sudo nano /etc/fstab
```

Добавьте следующую строку в конец файла:

```
<URL_сервера_WebDAV> /mnt/webdav davfs user,rw,noauto 0 0
```

где:

<URL_сервера_WebDAV> необходимо заменить на URL вашего сервера WebDAV.

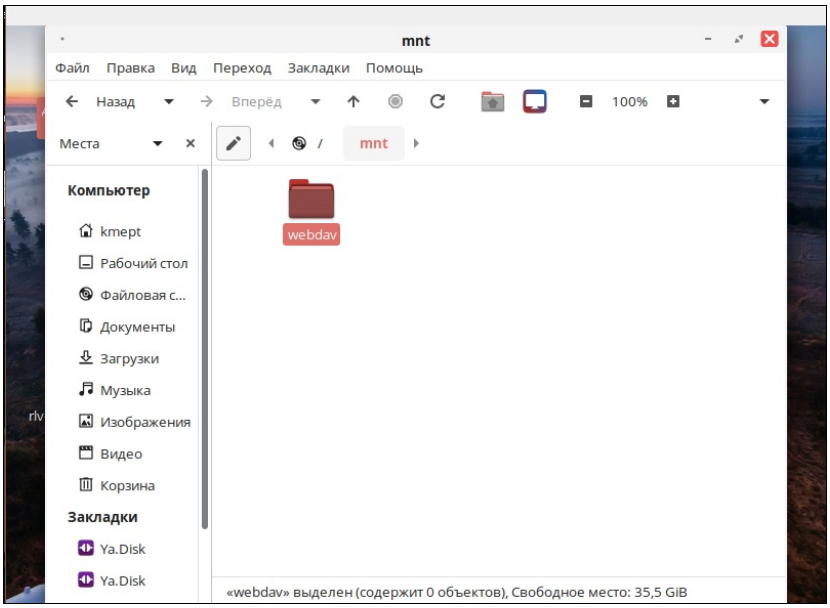


7. Сохраните и закройте файл.

8. Примонтируйте WebDAV-ресурс:

```
sudo mount /mnt/webdav
```

Теперь ваш WebDAV-ресурс должен быть успешно подключён и доступен для работы в каталоге **/mnt/webdav**.


mnt
Файл Правка Вид Переход Закладки Помощь
Назад
Вперёд
100%
Места
/
mnt
Компьютер
kmept
Рабочий стол
Файловая с...
Документы
Загрузки
Музыка
Изображения
Видео
Корзина
Закладки
Ya.Disk
Ya.Disk
webdav
«webdav» выделен (содержит 0 объектов), Свободное место: 35,5 GiB

Webmin - программный комплекс для удаленного администрирования

Установка и настройка
Обновление
Работа с Webmin
Файловый менеджер
Работа с консолью
Состояние сервера и служб
Резервное копирование конфигурационных файлов
Модуль «Пользователи в Webmin»
Bacula - резервное копирование системы
Ротация логов
Добавление и редактирование MIME типов
Read User Mail
Настройки Postfix
SSH Сервер
HTTP Tunnel
Protected Web Directories
Загрузка и сохранение
Команды пользователя
Модули Perl
Bandwidth Monitoring
TCP Wrappers
Запись на компакт-диски
Cluster Change Passwords
Cluster Copy Files
Cluster Shell Commands
Cluster Usermin Servers
Cluster Webmin Servers

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** webmin-1.981-4

Средство системного администрирования **Webmin** представляет собой бесплатное программное обеспечение, облегчающее работу системных администраторов операционных систем семейства Linux.

Webmin представляет собой простой веб-сервер, и несколько сотен скриптов, написанных на языке **Perl**, с помощью которых выполняются команды конфигурирования отдельных элементов системы, системных служб и самого Webmin. Практически, **Webmin** - это удобная панель управления, доступная через веб-браузер, а модули **Webmin** - это внешний интерфейс к консольным утилитам. При настройках по умолчанию, для доступа к **Webmin** достаточно в любом обозревателе открыть URL - https://host:10000

https://localhost:10000 - обычно, при настройках по умолчанию, доступ к средствам **Webmin** возможен только через петлевой интерфейс. После авторизации, пользователь получает доступ к настройкам как самого Webmin, так и тех составляющих операционной системы, поддержка которых реализована в его данной версии.

Webmin - это средство, облегчающее администрирование, упрощающее рутинные действия, позволяющее отображать данные в удобном для восприятия виде и выполнять настройки с меньшими затратами сил и средств.

Webmin работает фактически на всех *nix-платформах, включая Linux, AIX, HPUX, Solaris, OS X и другие. Он может работать практически на любом графическом браузере как локально так и удаленно. Данные, передаваемые между сервером и браузером, могут шифроваться при помощи SSL. Кроме того, для начинающего системного администратора Linux полезным свойством может быть то, что в **Webmin** имеется возможность изменить используемый язык и тему оформления.

Установка и настройка

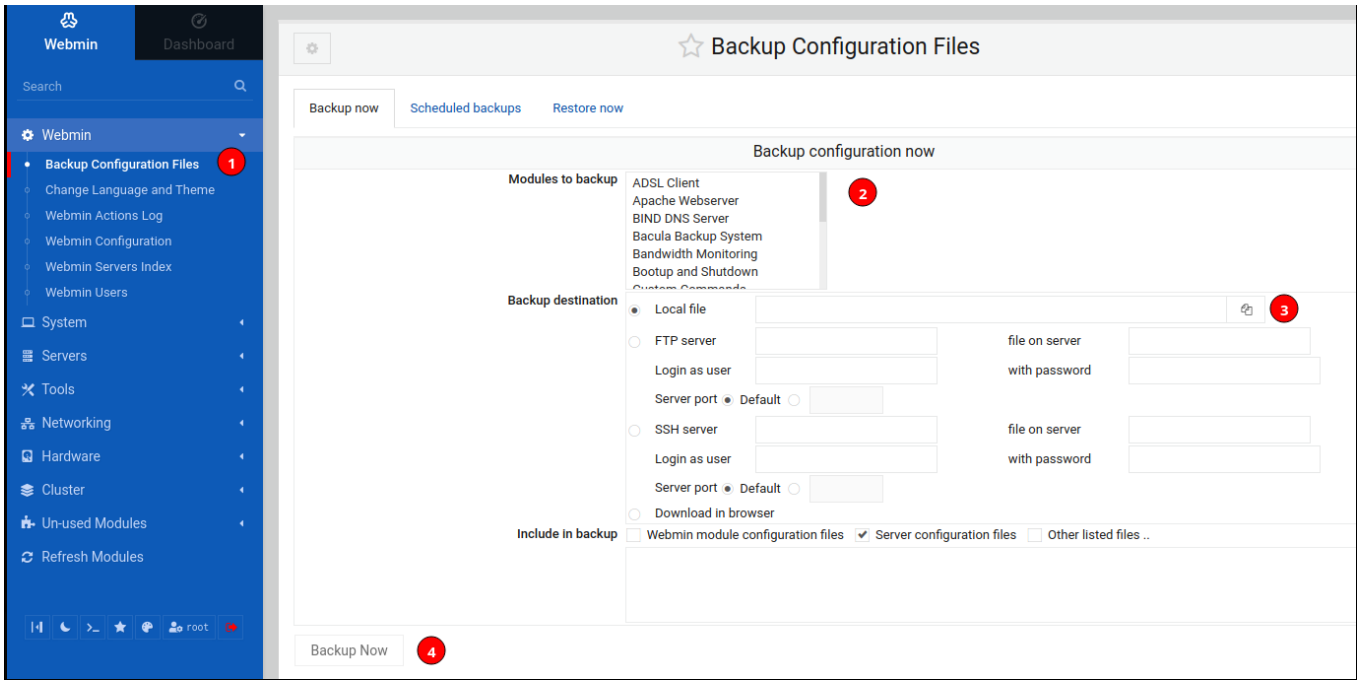
Установка должна выполняться под учетной записью суперпользователя и может быть выполнена в терминале с помощью команды:

```
dnf install webmin
```

Обновление

Для обновления уже установленной и настроенной системы webmin до актуальной версии необходимо выполнить следующие действия:

1. Создать резервную копию конфигурационных файлов webmin. Для этого в веб-интерфейсе во вкладке « **Webmin**» выберите модуль «**Backup Configuration Files**» (**1**).



Выделите модули, конфигурацию которых необходимо сохранить (**2**). Выберите место сохранения резервной копии и введите имя создаваемого архива (**3**). Обратите внимание, что расширение архива должно быть **tar.gz**. Затем нажмите на кнопку «**Backup Now**» (**4**).

2. Удалить установленную версию **webmin**:

```
dnf remove webmin
```

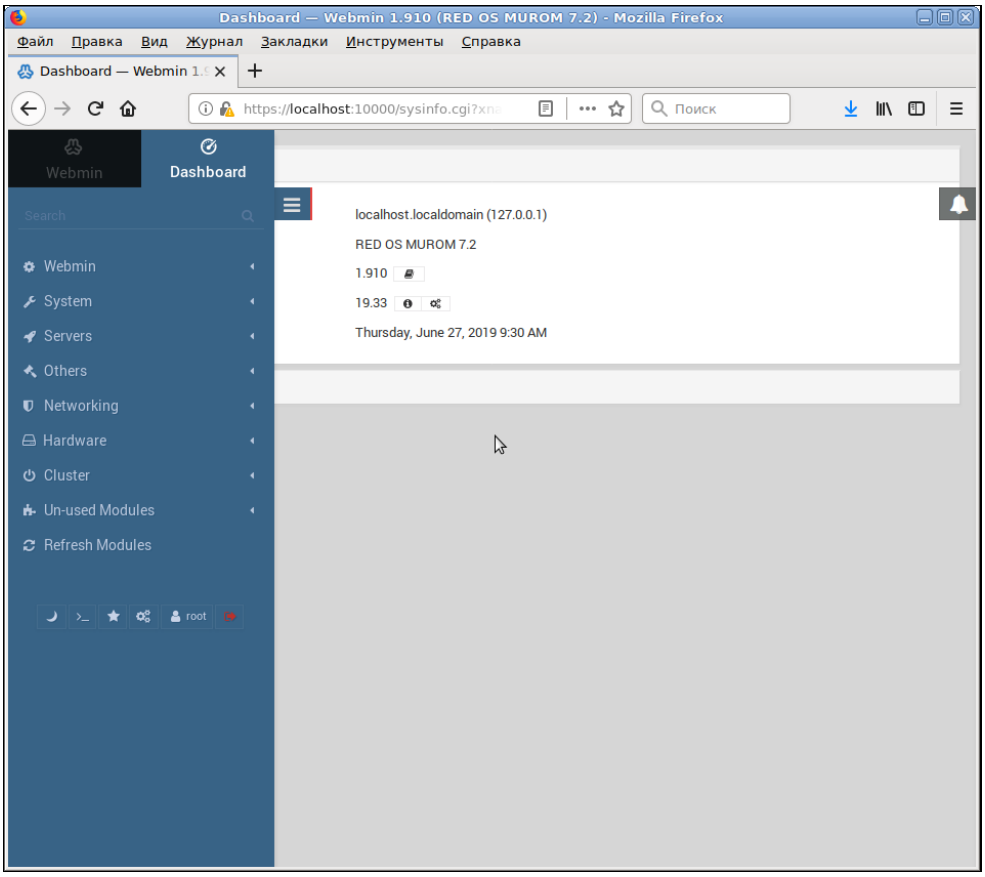
3. Установить актуальную версию из репозитория:

```
dnf install webmin
```

4. Перейти в веб-интерфейс **webmin**. Открыть модуль «**Backup Configuration Files**», во вкладке «**Restore now**» выполнить действия, аналогичные созданию резервной копии, и нажать кнопку «**Restore now**».

Работа с Webmin

В браузере открываем ссылку **https://localhost:10000/**. После ввода имени пользователя и пароля отобразится основное окно **Webmin**:



В правой части основного окна отображается информация о системе, в левой - разделы, доступные для настройки с использованием Webmin:

- **Webmin** - настройки модуля Webmin - настройка слушаемых сервером адресов и портов, настройки пользователей, язык и тема оформления, журналы действий, резервное копирование и т.п.
- **System** - информация и системные настройки - управление пользователями, процессами, службами, файловыми системами, системными журналами, резервное копирование и управление приложениями.
- **Servers** - настройки для установленных в системе серверов DNS, DHCP, FTP и т.п.
- **Others** - прочие инструменты для администрирования - командная оболочка, менеджер файлов, SSH-клиент и т.п.
- **Networking** - сетевые настройки, средства мониторинга сетевого трафика, брандмауэры и т.п.
- **Hardware** - системное время, средства управления принтерами, разделами на дисках, запись на CD/DVD.
- **Cluster** - управление несколькими системами, объединенными в кластер. Webmin устанавливается на одной из систем, входящих в кластер, и взаимодействие с остальными осуществляется через протокол удаленного вызова процедур RPC (Remote Procedure Call).
- **Un-used Modules** - неиспользуемые модули Webmin - модули которые были установлены, но в системе нет объектов для их использования. Если после установки Webmin выполнялась , например, установка сервера SSH, то для перевода его из категории неиспользуемых в категорию "Servers" (Серверы) необходимо выполнить обновление модулей (Refresh Modules в меню Webmin).
- **Search** - контекстный поиск в Webmin.
- **Refresh Modules** - обновить модули. Для того, чтобы изменения в составе модулей вступили в силу нужно завершить сеанс работы с Webmin (кнопка Logout) и повторно авторизоваться.
- **Logout** - выход из Webmin.

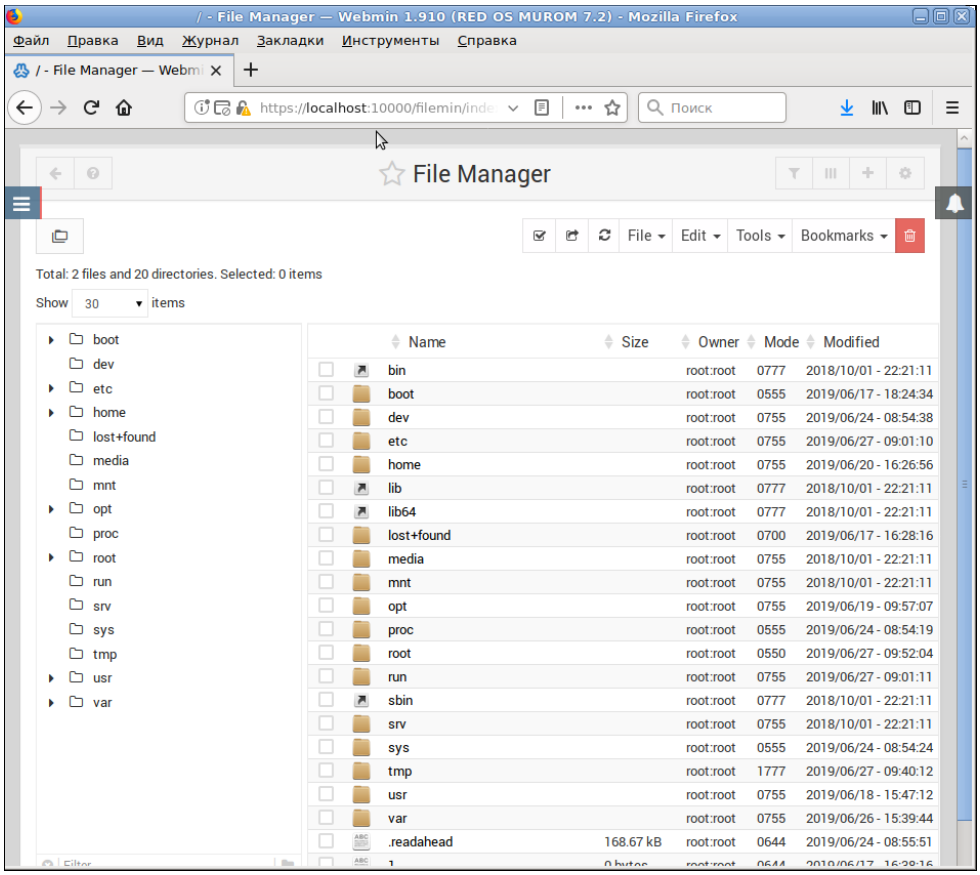
Для того, чтобы использовать Webmin с русским интерфейсом, нужно в меню **Webmin** выбрать пункт **Change Language and Theme** и установить персональный выбор **Personal choice** - русский язык **Russian (RU_UTF-8)**. После этого нажать кнопку **Make Changes**, выйти из Webmin и авторизоваться повторно.

При выполнении настроек с помощью Webmin необходимо учитывать тот факт, что в большинстве случаев, для того, чтобы установленные настройки вступили в силу, требуется нажатие кнопки "**Применить настройки**" (Apply Changes) и для некоторых сервисов - остановка и запуск. Многие модули Webmin, кроме собственных сценариев настроек позволяют выполнить прямое редактирование конфигурационных файлов, что позволяет выполнять настройки, не реализованные в текущей версии модуля.

Файловый менеджер

Файловый менеджер доступен по ссылке «**File Manager**» в разделе «**Прочее**» главного меню.

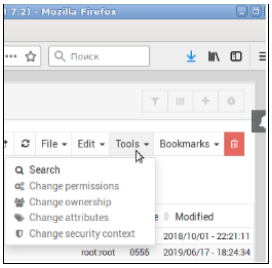
При открытии файлового менеджера отображается корневой каталог файловой системы. С помощью гиперссылок можно заходить в те или иные папки и открывать или загружать к себе на компьютер файлы.



Данный файловый менеджер позволяет выполнять лишь простейшие операции, такие как создание каталогов и текстовых файлов, редактирование текстовых файлов, создание архивов, распаковка архивов (при наличии, например, unzip), загрузка файлов с компьютера на сервер и наоборот.

Также стоит отметить возможность с помощью интерфейса файлового менеджера изменять владельцев файлов и папок и права доступа к ним.

Инструменты для изменения владельцев и прав доступны в меню «**Tools**».



Работа с консолью

Для работы с консолью служит страница «**Command Shell**» в разделе «**Прочее**». Поэтому, если необходим доступ к обычной консоли, Webmin предоставляет и такую возможность.

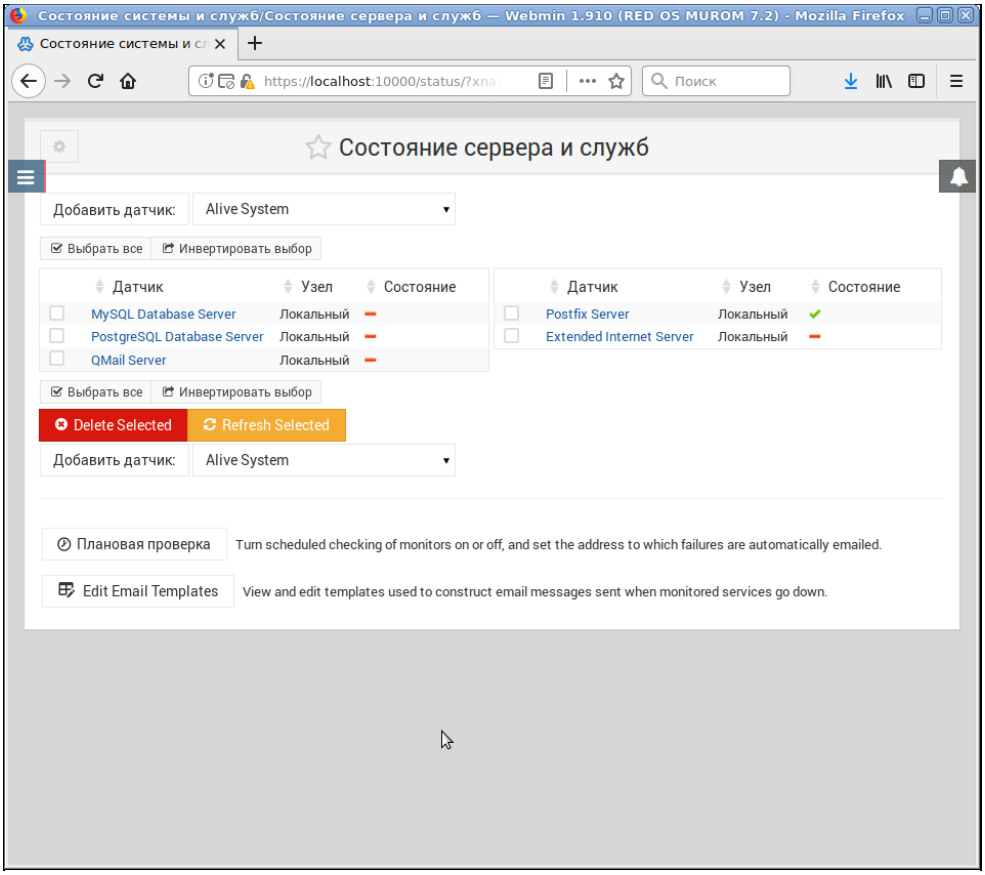
Состояние сервера и служб

Модуль доступен по ссылке «**Состояние сервера и служб**» в разделе «**Прочее**» главного меню.

Этот модуль позволяет отслеживать состояния выбранных серверов и запущенных демонов. С его помощью можно легко определить какие процессы выполняются должным образом или выявить те процессы, работа которых нарушена. Также можно сконфигурировать модуль таким образом, чтобы при проверке состояния сервера происходила отправка сообщения по e-mail или выполнялась какая-либо команда. Эта функция может быть полезна если система управляет серверами, от которых зависят другие люди, такими как Web или

DNS сервера.

Когда Вы входите в модуль «Состояние сервера и служб», то перед Вами появится главная страница, на которой отобразится таблица со всеми сконфигурированными мониторами. Несколько мониторов для общих серверов и служб будут определены по умолчанию, но Вы можете редактировать, удалять или добавлять их. На рисунке показан пример главной страницы модуля.



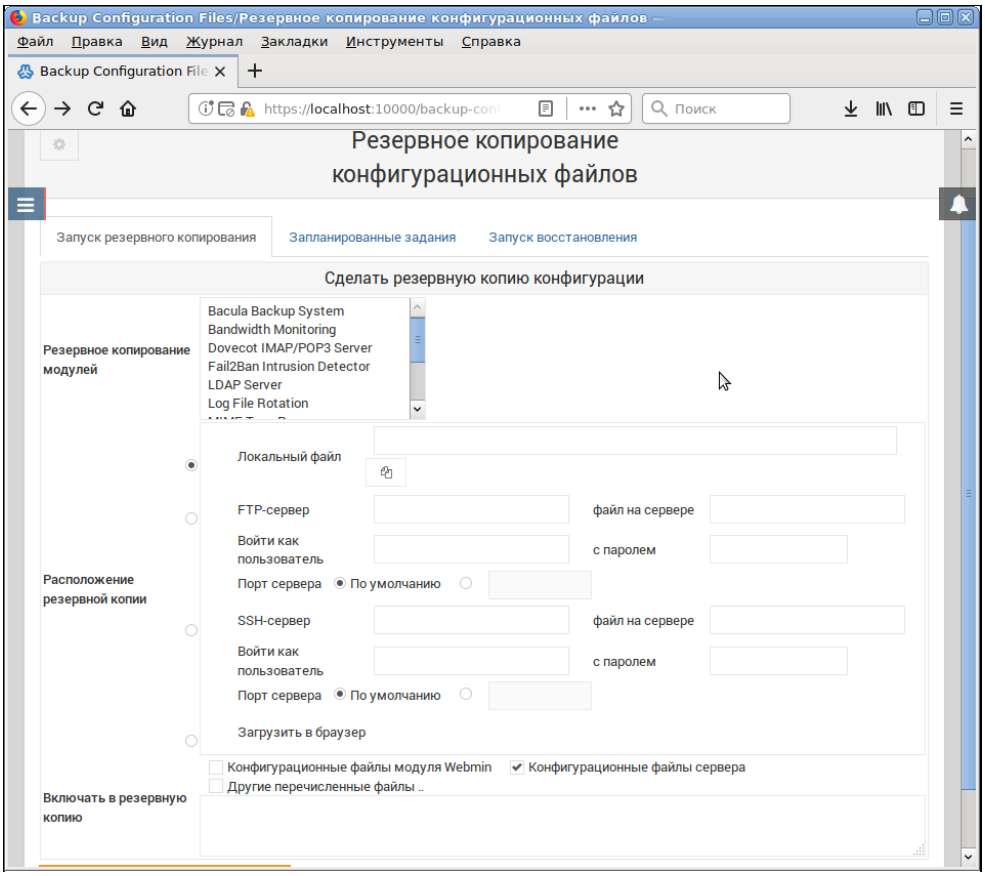
Каждый сервер или служба, за которым Вы хотите наблюдать, используя данный модуль, должен иметь свой монитор. Каждый монитор принадлежит к какому-либо типу, который указывает на то какие виды серверов им можно проверять, такие как Apache или BIND. Мониторы также имеют ряд дополнительных параметров, которые могут зависеть от типа. Модуль позволяет создавать множество различных типов мониторов, например, для проверки возможности запуска Sendmail или Squid путем наблюдения за интенсивностью использования сети или свободным дисковым пространством, или при помощи пингования или соединения с другим хостом.

Монитор может быть запущен, как в той же системе, в которой находится сам модуль, так и в другой системе, использующей Webmin. В последнем случае сервер должен быть определен в модуле **Webmin Server Index**. Также возможна проверка систем, на которых не установлен Webmin путем использования модулей типов remote TCP, HTTP и ping monitor.

По умолчанию состояния каждого монитора запрашиваются каждый раз при просмотре главной страницы модуля. Это может занять много времени, если запущено большое количество мониторов или происходит проверка статуса на удаленном хосте. Поэтому при необходимости в опциях конфигурации модуля можно установить запланированную проверку состояний. В этом случае при переходе на главную страницу будут отображаться состояния, полученные при проведении последней проверке.

Резервное копирование конфигурационных файлов

Резервное копирование и восстановление находится в разделе «**Система**».



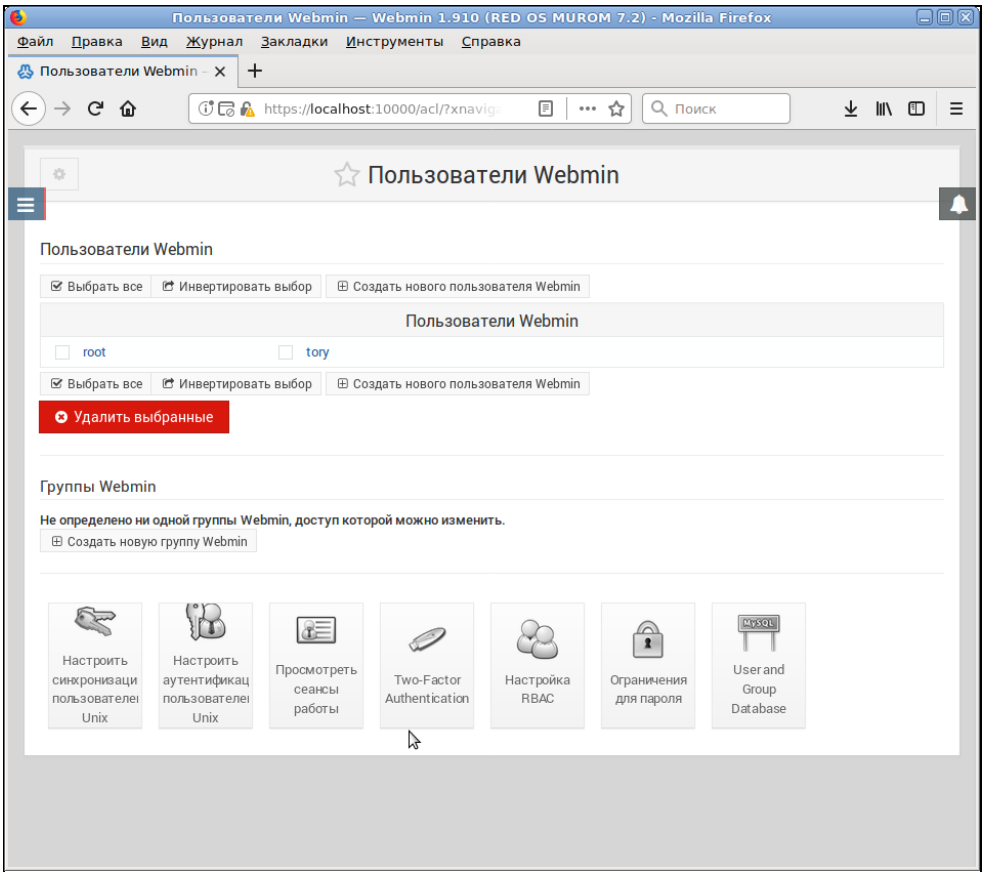
Здесь можно сделать резервное резервное копирование или восстановление, для этого следует выбрать необходимые модули, указать расположение резервной копии,и нажать кнопку «Запуск резервного копирования». Восстановление конфигурационных файлов проводится таким же образом.

Модуль «Пользователи в Webmin»

В Webmin, модуль **The Users and Groups** (Пользователи в Webmin), который находится в категории **System** (Система), может быть использован для создания, редактирования и удаления UNIX пользователей и групп в вашей системе. Нужно быть осторожным при использовании данного модуля для изменения существующих системных пользователей, таких как root и daemon, так как их изменение или удаление может вывести систему из строя. Некоторые пользователи имеют свою домашнюю директорию в корневом каталоге (/). Удаление таких пользователей вызовет удаление всех файлов вашей системы! Те пользователи, которых завели вы, обычно находятся в каталоге home.

В дополнение, к управлению UNIX пользователями в вашей системе, этот модуль также позволяет управлять пользователями, находящимися в других модулях. Например, Samba имеет свой собственный список пользователей и паролей, которые должны быть согласованы со списком паролей UNIX. Webmin может сделать это автоматически, используя функции других модулей, которые вызывают формы создания, редактирования и удаления пользователя. Однако, вы должны, разрешить это во всех модулях, которые хотите обновлять автоматически. По аналогии, в модуле также имеется опция согласования UNIX групп, например, с Samba группами. Но, поскольку эта функция работает только с Samba 3.0, которая все еще находится в стадии развития, это не включено в данную главу.

При открытии модуля, главная страница отображает в одной таблице список всех пользователей, а в другой – список всех групп, существующих в Вашей системе на данный момент. Если пользователей или групп слишком много, вместо таблиц отображаются небольшие формы, позволяющие выполнить поиск.



Bacula - резервное копирование системы

Bacula – пакет программ архитектуры «клиент-сервер» с открытым исходным кодом, предназначенный для создания резервных копий данных, находящихся на компьютерах с различными операционными системами, для восстановления и проверки хранящихся данных. Этот пакет имеет модульную архитектуру, легко масштабируется и может быть использован, как для небольшой локальной сети из нескольких компьютеров, так и для сети предприятия, состоящего из нескольких сотен компьютеров.

Система построена по технологии клиент-сервер, и для передачи данных использует протокол TCP. Резервные копии создаются в собственном, полностью открытом формате. Система резервирования данных Bacula состоит из четырёх основных элементов: *Director Daemon*, *Storage Daemon*, *File Daemon* и *Bacula Console*. Все эти элементы реализованы в виде самостоятельных приложений.

Director Daemon (DD) – это центральный элемент системы, осуществляющий управление её остальными компонентами. В его задачи входит управление процессом резервирования/восстановления данных, обеспечение интерфейса управления для администраторов и многое другое.

Storage Daemon (SD) – приложение, отвечающее за чтение/запись данных непосредственно на устройства хранения информации. Принимает управляющие команды от DD, а также резервируемые данные от/к File Daemon.

File Daemon (FD) – этот элемент ещё можно назвать Агентом. Ведь именно он работает в рамках операционной системы, данные которой необходимо резервировать. File Daemon выполняет всю рутину, осуществляя обращение к резервируемым файлам и их дальнейшую передачу к SD. Также на стороне FD выполняется шифрование резервных копий, если это определено конфигурацией.

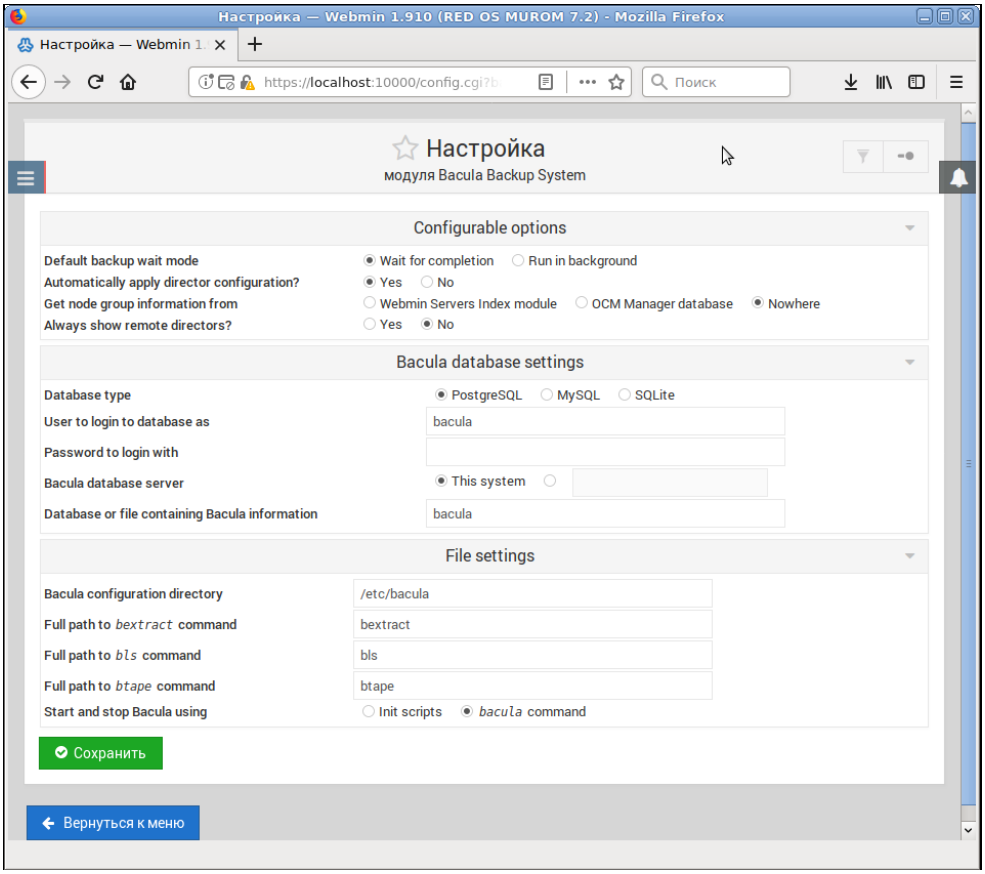
Bacula Console (BC) – интерфейс администратора системы. По своей сути, это командный интерпретатор для управления Bacula. Строго говоря, Bacula Console может быть расширена с помощью графических систем управления, которые, как правило, являются всего лишь надстройкой над BC. К таким системам можно отнести Tray Monitor и Bat. Первая устанавливается на компьютере администратора системы и осуществляет наблюдение за работой системы резервирования, а вторая обеспечивает возможность управления посредством графического интерфейса.

Bacula Catalog – база данных, в которой хранятся сведения обо всех зарезервированных файлах и их местонахождении в резервных копиях. Каталог необходим для обеспечения эффективной адресации к требуемым файлам. Поддерживаются MySql, PostgreSql и SqLite. Такое структурное деление позволяет организовать очень гибкую систему резервирования, когда Storage Daemon разворачивается на выделенном сервере с несколькими устройствами хранения данных. Также Bacula Director может управлять несколькими экземплярами SD, обеспечивая резервирование части данных на одно устройство хранения, а части – на другое.

Вы найдете системы резервного копирования Bacula в левой панели Webmin «**Система**» -> «**Bacula Backup System**». Если не находится там, попробуйте в разделе «**Неиспользуемые модули** (Un-used modules section)».

Нажмите на кнопку «**Резервное копирование системы Bacula**». Изначально сервер Bacula не включится автоматически. Для запуска Bacula сервера нажмите «**Настройки модуля**» - ссылку справа на странице «**Система резервного копирования Bacula**» (Bacula Backup System).

Заполняем все поля (вводим название БД, логин для нее и пользователя). Затем можно производить резервное копирование системы.



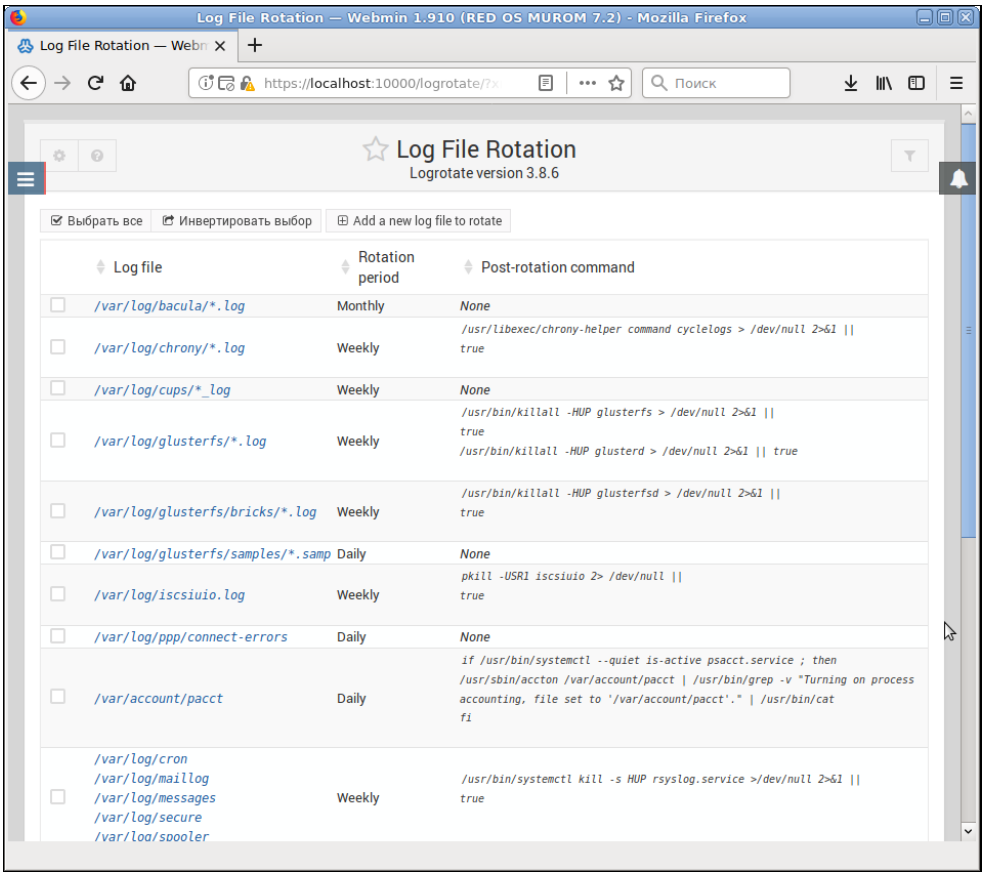
Ротация логов

В Linux, большинство сервисов и программ, которые работают в фоне, таких как Apache, Nginx, Postfix и других записывают информацию о своем состоянии, результатах работы и ошибках в лог файлы. Стандартное расположение логов или как их еще называют - журналов - в папке /var/log.

С помощью анализа логов вы можете понять что работает не так, почему произошла ошибка и как решить возникшую проблему. Но тут кроется одна проблема. Размер логов постоянно растет и они занимают все больше и больше места на диске, поэтому необходимо вовремя чистить логи и удалять устаревшие записи, чтобы они не мешали нормально работать.

Данная функция в Webmin предназначена для автоматизации обработки журналов. Она может выполнять с ними необходимые действия в зависимости от определенных условий и правил соответствия. Например, можно сжимать журналы в архив или отправлять на другой сервер когда они достигают определенного размера, возраста, или других параметров.

Вы найдете ротацию логов в левой панели Webmin консоли под **Система** -> **Log File Rotation**.

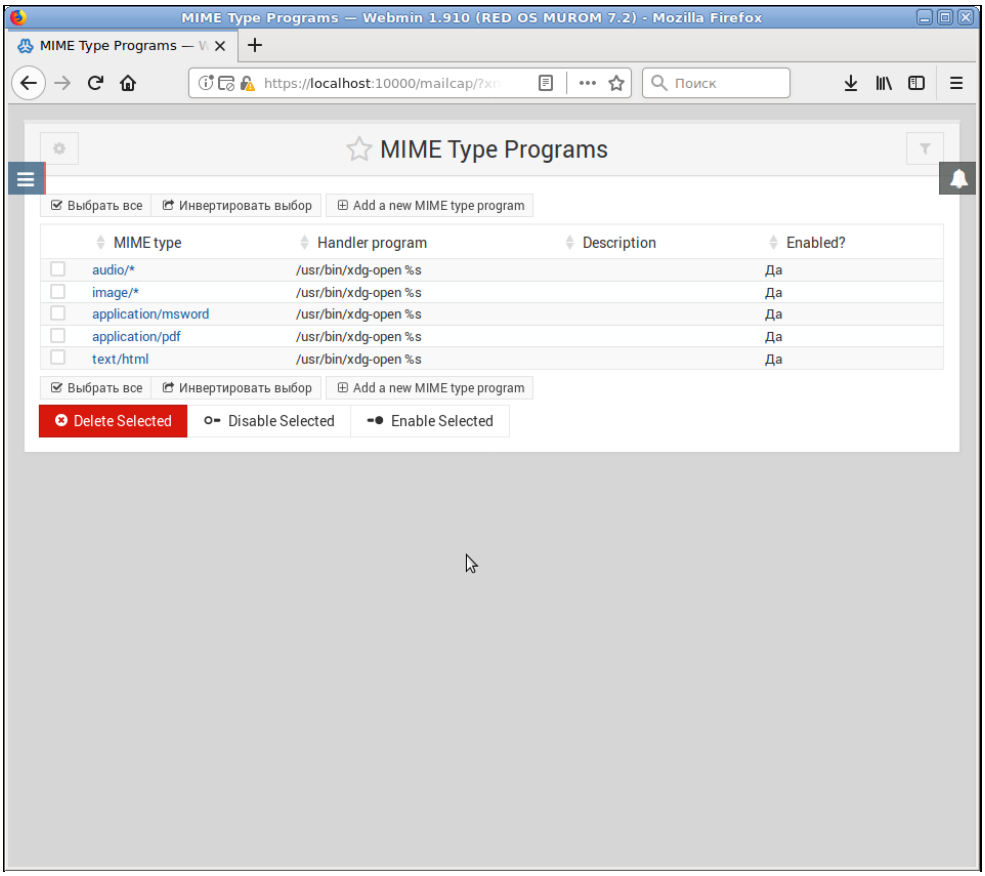


Проверку условий можно настроить ежедневно, еженедельно или ежемесячно. Это позволяет создать схему ротации логов, удобную именно для вас и вашего сервера. Также ротация логов может быть полезна на домашнем компьютере, но здесь она не так важна как на серверах, где только в логи Apache могут записываться до сотен тысяч строк ежедневно.

Добавление и редактирование MIME типов

MIME типы - это способ, который использует Apache, почтовые клиенты и многие другие программы для определения типа файлов или типа данных. MIME тип содержит два слова разделенные косой чертой. Например, text/html или video/mpeg. Как видно из примеров, первое слово это категория, а второе - реальное название типа содержимого.

Каждый ответ сервера Apache содержит запись о MIME типе, поэтому браузер "понимает" как показывать то или иное содержимое.



Apache имеет глобальный список MIME типов. Чтобы отредактировать его проделайте следующие шаги:

1. На главной странице модуля нажмите кнопку MIME Types(MIME типы).
2. Нажмите Add a new MIME type(Добавить новый MIME тип).
3. Введите имя вида text/foo в поле MIME type(MIME тип).
4. Введите расширения файлов, которые будут ассоциированы с этим типом, например .foo и .fo в поле Extensions(Расширения). Удостоверьтесь, что ни один другой MIME тип не связан с этими расширениями.
5. Нажмите кнопку Save(Сохранить).
6. Нажмите Apply Changes(Применить изменения), чтобы изменения вступили в силу.

MIME типы могут быть настроены для всех виртуальных серверов, для отдельного виртуального сервера или для отдельного каталога. Для этого выберите Сервер по умолчанию, отдельный виртуальный сервер или каталог соответственно.

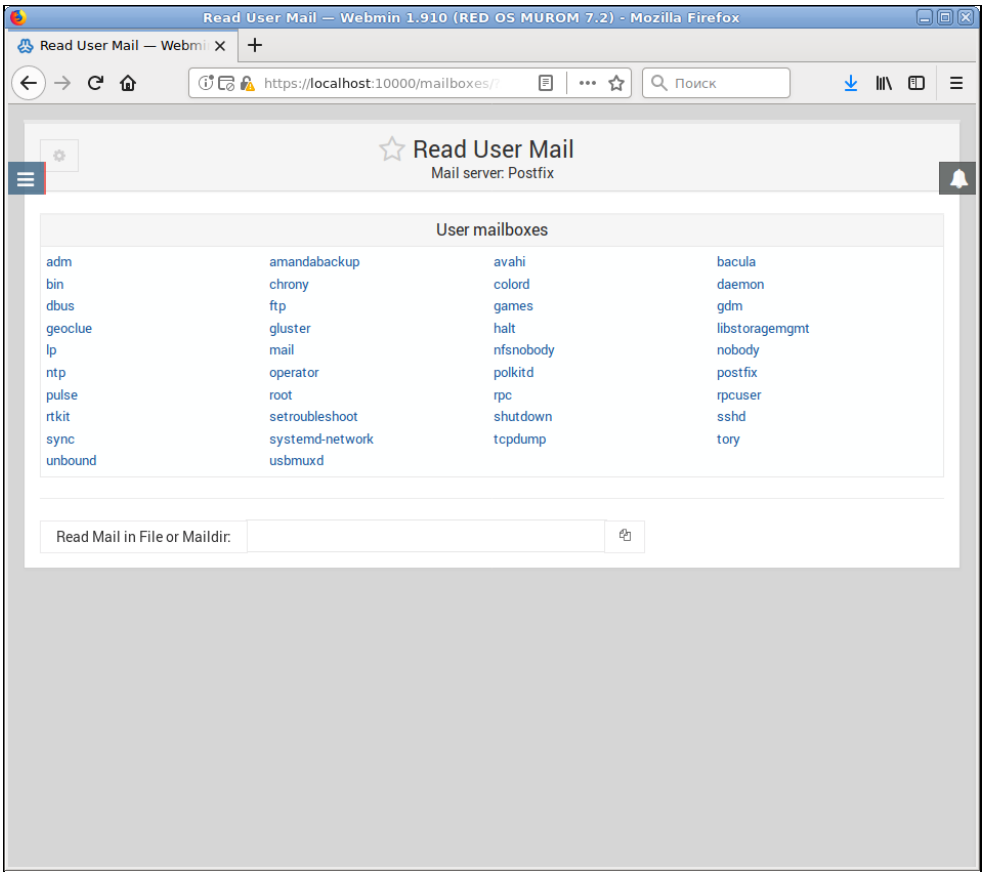
Чтобы отредактировать MIME тип или удалить его нажмите на его имя. После внесения изменений нажмите Save(Сохранить) и Apply Changes(Применить изменения). Чтобы удалить нажмите Delete(Удалить) на форме редактирования, затем Apply changes(Применить изменения), чтобы изменения вступили в силу.

На странице MIME типов есть очень полезное поле Default MIME тип(MIME тип по умолчанию). Если оно задано, то любое содержимое, которое Apache не может определить, будет отдано с этим значением.

Read User Mail

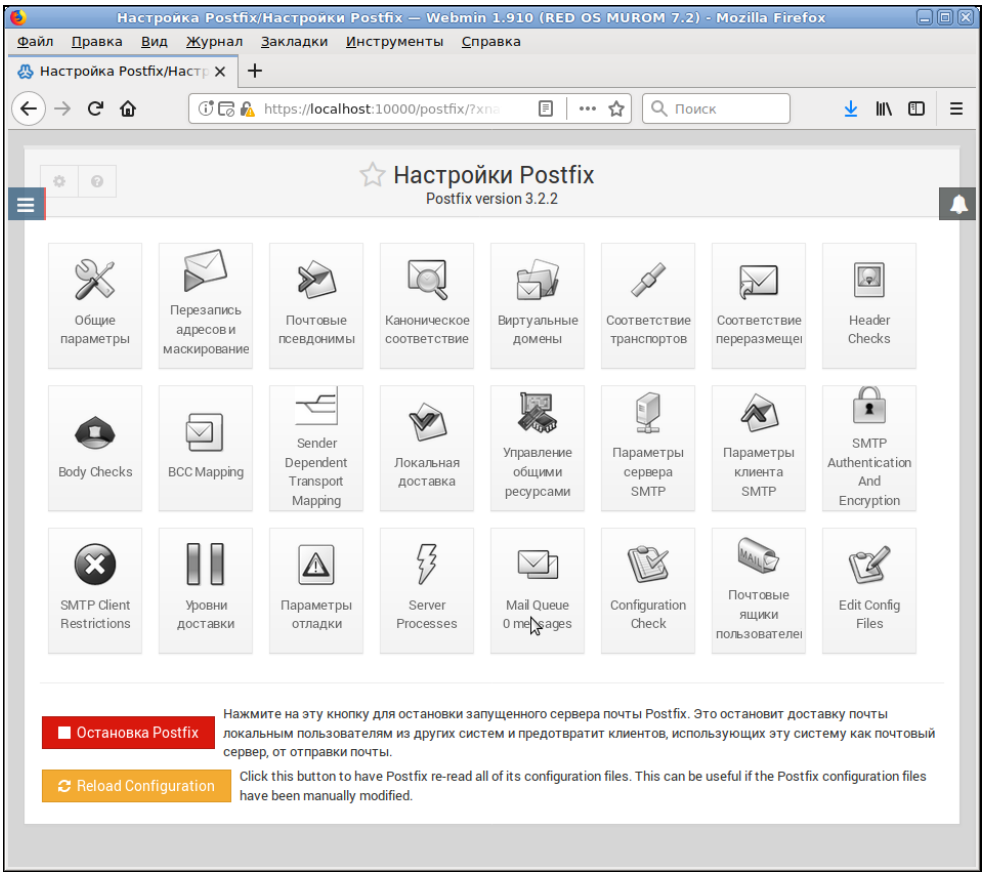
Webmin включает в себя очень полезный модуль, который позволяет администратору читать сообщения электронной почты любого пользователя. Модуль **Read User Mail** на самом деле является простым почтовым клиентом для доступа к почтовым ящикам пользователей почти для всех пользователей на сервере, и это один из стандартных модулей, установленных по умолчанию Webmin.

Выберите пользователя, у которого Вы хотите прочитать письма, или введите путь к почтовому файлу или MailDir, который Вы хотите прочитать. В почтовом ящике вы можете выбрать чтение писем из других папок.



Настройки Postfix

Postfix - это эффективный и многофункциональный почтовый сервер. Он был предназначен, чтобы быть заменой для популярного сервера. В то время как Sendmail был самым популярным почтовым сервером в течение многих лет, популярность Postfix, вероятно, выросла за пределы Sendmail из-за его простой конфигурации, исторически безопасной реализации и высокопроизводительной архитектуры. Кроме того, поскольку Postfix предназначен для внешнего поведения, как sendmail, это в основном замена для более старого, большого и медленного почтового сервера.



Настройка Postfix включает в себя следующие возможности:

1) Общие параметры

Страница общие параметры настраивает ряд параметров, касающихся общего поведения Postfix. В частности, здесь настраиваются большинство параметров конфигурации, влияющих на всех пользователей и все сообщения. Postfix, придерживаясь своей философии простоты, обычно требует всего нескольких изменений файла конфигурации, чтобы почтовый сервер работал эффективно и безопасно.

2) Перезапись адресов и маскирование

Postfix предлагает относительно простую в использовании и гибкую систему перезаписи адресов, позволяющую ей действовать как почтовый шлюз для большой сети или как шлюз между устаревшими почтовыми системами и интернетом в целом Переписывание адресов лежит в основе почтовой системы Postfix. Postfix переписывает адреса для самых разных целей. Некоторые из них просто косметические, а некоторые необходимы для доставки правильно отформатированной почты в нужное место назначения. Примерами переопределения адресов в постфикс являются:

- Преобразование неполного адреса в полный адрес. Например, превратить "имя пользователя" в "username@example.com" или преобразование "имя_пользователя@имя_хоста" в "username@hostname.example.com".

- Замена адреса эквивалентным адресом. Например, заменить "username@example.com" by "firstname.lastname@example.com" при отправке почты, и сделать обратное преобразование при получении почты.

- Замена внутреннего адреса на внешний адрес. Например, замените " username@localdomain.локальный "by" isp-аккаунт@isp.пример " при отправке почты с домашнего компьютера в интернет.

- Замена адреса несколькими адресами. Например, замените адрес псевдонима адресами, перечисленными под этим псевдонимом.

- Определение, как и куда доставлять почту по определенному адресу. Например, доставить почту для "username@example.com" с помощью агента доставки smtp на хосты, перечисленные в DNS в качестве почтовых серверов для домена "example.com".

3) Почтовые псевдонимы

Почтовые псевдонимы обеспечивают средства для перенаправления почты для локальных получателей. В частности, он позволяет доставлять почту, предназначенную для нескольких разных адресов, в один почтовый ящик. Обычно для этого используется прямая почта для пользователей, таких как postmaster, к реальному человеку. Эта страница разделена на две части. Верхний раздел с надписью Aliases Options содержит расположение и формат файлов псевдонимов, которые Postfix должен использовать для создания своих баз данных псевдонимов, и указывает тип используемой базы данных. В нижнем разделе представлен список всех настроенных псевдонимов в системе и сопоставление псевдонимов.

4)Каноническое соответствие

Каноническое сопоставление в Postfix используется для изменения почты во входящей очереди и изменяет как заголовки сообщений, так и информацию о конверте сообщения для локальной или удаленной почты. Это сопоставление может быть полезно для замены имен входа на Firstname, адреса стиля Lastname или для очистки нечетных адресов, созданных устаревшими почтовыми системами.

5) Виртуальные домены

Функциональность виртуальных доменов в Postfix предоставляет возможность перенаправлять сообщения в разные места, изменяя адрес конверта сообщения. Адрес заголовка не изменяется при сопоставлении виртуального домена. Хотя некоторые функции виртуальных доменов перекрываются с функциями, доступными в псевдонимах, виртуальные домены могут использоваться для локальных или нелокальных адресов, а псевдонимы могут использоваться только для локальных адресов.

6) Соответствие транспортов

Термин транспорт относится к механизму, используемому для доставки части электронной почты. В частности, SMTP и UUCP - это почтовые транспорты, поддерживаемые Postfix. Транспортное сопоставление может быть использовано для ряда целей, в том числе SMTP для UUCP gatewaying, работы Postfix на брандмауэре с переадресацией на внутренний почтовый сервер и т. д.

7) Соответствие переразмещения

С помощью этой опции можно уведомить отправителей, если локальный пользователь переехал на другой адрес. Например, если пользователь покидает организацию, но по-прежнему время от времени получает почту на свой локальный адрес, может быть удобно уведомить любого отправителя почты пользователю о переезде и новой контактной информации для этого пользователя.

8) Локальная доставка

Локальная доставка -это то, что Postfix делает, когда он достигает конца всего своего списка сопоставлений и элементов управления доступом и все еще находит, что сообщение разрешено и предназначено для пользователя на локальной машине (т.е. сопоставление может потенциально отправить сообщение в другое место для окончательной доставки, поэтому все сопоставления, а также различные проверки доступа выполняются до достижения этого этапа). На этой странице настраивается ряд параметров, связанных с тем, как Postfix обрабатывает доставку почты для локальных пользователей.

9) Управление общими ресурсами

Эта страница предоставляет доступ к различным ограничениям памяти и процессов для Постфиксных процессов. Редко требуется изменять значения на этой странице, за исключением высоконагруженных серверов или машин с очень низким ресурсом.

10) Параметры сервера SMTP

Эта страница настраивает большинство параметров, которые непосредственно влияют на поведение части сервера SMTP Postfix, в частности части Postfix, которые влияют на поведение сервера по отношению к клиенту SMTP, который подключается к серверу.

11) Параметры клиента SMTP

Параметры SMTP-клиента настраивают поведение Postfix при работе с другими почтовыми серверами в качестве клиента, т.е. при отправке почты от имени пользователя. Эта часть конфигурации в первую очередь определяет, как сервер будет реагировать на определенные ошибки.

12) Уровни доставки

Эта страница содержит параметры для установки скорости по умолчанию и ограничений параллелизма для всех компонентов Postfix. Эти скорости обычно могут быть переопределены в их соответствующих разделах конфигурации.

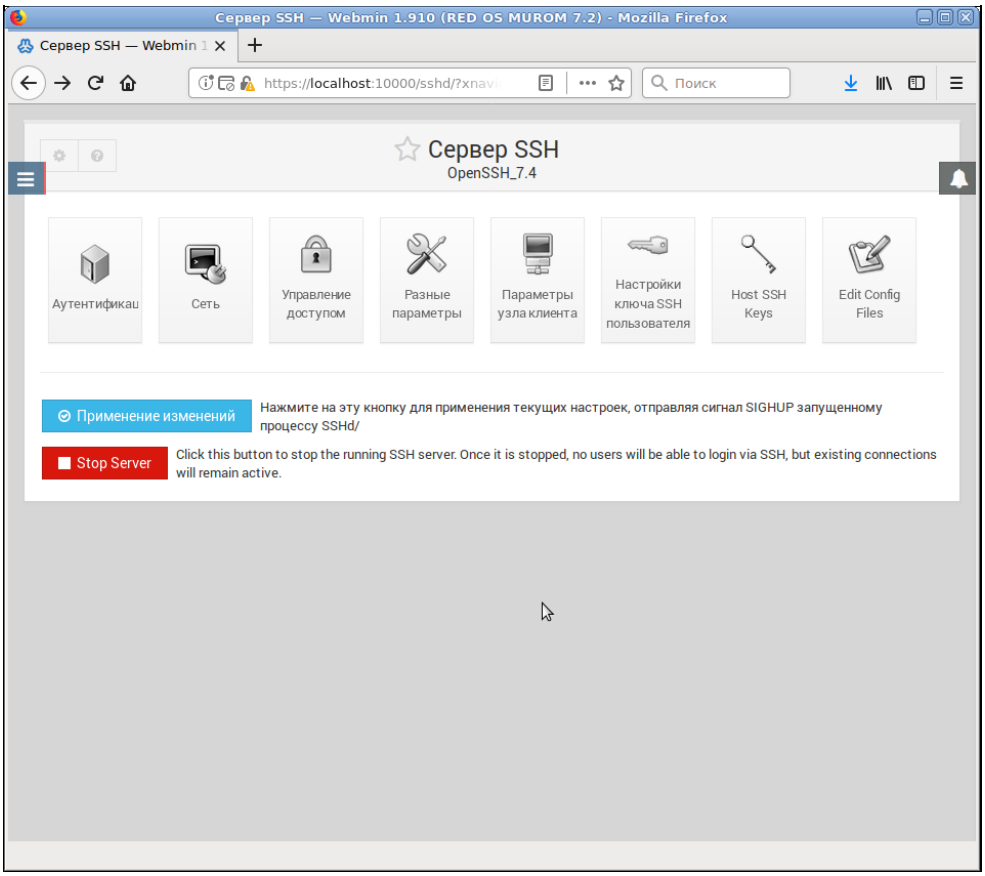
13) Параметры отладки

Postfix имеет два уровня ведения журнала. Первый уровень-обычный почтовый журнал, который сообщает обо всех обычных почтовых действиях, таких как полученная и отправленная почта, ошибки сервера, остановки и запуски. Второй уровень является более подробным и может быть настроен на ведение журнала действий, связанных с конкретными SMTP-клиентами, именами хостов или адресами. Эта страница содержит конфигурацию для второго уровня ведения журнала.

SSH Сервер

Настройки сервера SSH можно найти выбрав «**Службы**» → «**Сервер SSH**» в главном меню.

На главной странице всегда отображаются шесть значков, под каждым из которых находится форма, содержащая поля для настройки параметров, связанных с какой-либо категорией, например, аутентификация или сеть. В верхней части отображается реализация и версия установленного SSH, так что вы можете увидеть, какие из инструкций в этой главе относятся к вашей системе. В нижней части находится кнопка с надписью «**Применить изменения**», которые при нажатии сигнализируют SSH-серверу для повторного чтения файла конфигурации. Никакие изменения, внесенные в модуль вступят в силу, пока вы не нажмете эту кнопку.



1) Аутентификация

У всех реализаций SSH есть опции, связанные с тем, как клиенты аутентифицируются и сообщения, отображаемые им после входа в систему. В частности, вы можете разрешить или запретить аутентификацию по имени пользователя и паролю или по имени пользователя и сертификату, остановить вход в систему пользователя root и контролировать, являются ли файлы rrgin в стиле rlogin. Точные параметры довольно сильно различаются между версиями SSH, поэтому, что возможно с OpenSSH, может не быть, если вы используете коммерческий сервер SSH.

2) Управление доступом

По умолчанию любому пользователю Unix будет разрешено удаленно входить на сервер SSH в вашей системе или использовать его для загрузки и скачивания файлов. В системе почтового сервера или на том, на котором размещаются веб-сайты, это может быть неуместно - вместо этого вы можете разрешить большинству пользователей входить на серверы POP3, FTP или Usermin. Хотя этого можно добиться, предоставив им оболочку типа / bin / false, это может вызвать другие проблемы с заданиями пользователя Cron или At.

3) Сеть

SSH-сервер имеет несколько параметров, которые позволяют настроить IP-адрес, который он слушает, порт, который он использует, и различные параметры, связанные с протоколом.

4) Параметры узла клиента

Несмотря на то, что этот модуль предназначен в основном для настройки SSH-сервера, он также позволяет устанавливать параметры, которые применяются ко всем клиентским подключениям, выполненным из вашей системы с помощью команд ssh и scp. Параметры могут быть установлены для соединений со всеми хостами или только с определенным. Вы можете установить порт для подключения, протокол и локальный и удаленный порты для пересылки. Настройки, сделанные в этом модуле применяются ко всем пользователям в системе, но могут быть переопределены для отдельных пользователей, редактировать ~/.файлы ssh / config. Это можно сделать вручную или с помощью Usermin, который имеет клиентский модуль SSH с идентичным интерфейсом, описанным здесь для редактирования глобальных параметров клиента. Многие настройки не имеет большого смысла устанавливать для всех пользователей, хотя это можно сделать с помощью Webmin. По этой причине инструкции в этом разделе охватывают только поля, полезные на глобальном уровне.

5) Настройки ключа SSH пользователя

Прежде чем пользователь Unix сможет использовать проверку подлинности сертификата для входа на сервер SSH, он должен создать закрытый ключ с помощью команды ssh-keygen. Этот модуль можно настроить для работы с модулем пользователи и группы, чтобы выполнить эту команду для всех вновь созданных пользователей. Если в вашей сети используются домашние каталоги, смонтированные на NFS,это позволит новым пользователям входить на другие хосты без необходимости вводить пароль без дополнительной настройки.

6) Разные параметры

Эта страница содержит параметры, которые не входят ни в одну из других категорий. Некоторые из менее очевидных вариантов, но полезные :

- Разрешить пересылку соединения X11?

  Если установлено значение Да, пользователи, которые делают SSH-вход с машины Unix, смогут запускать X-приложения на сервере и туннелировать X-соединение обратно через SSH-соединение на свой локальный дисплей.

- Устройство для ведения системного журнала

  Средство системного журнала, которое используется для регистрации ошибок и информационных сообщений с сервера SSH. Это можно использовать в сочетании с модулем системных журналов для управления тем, в какой файл записываются SSH-сообщения.

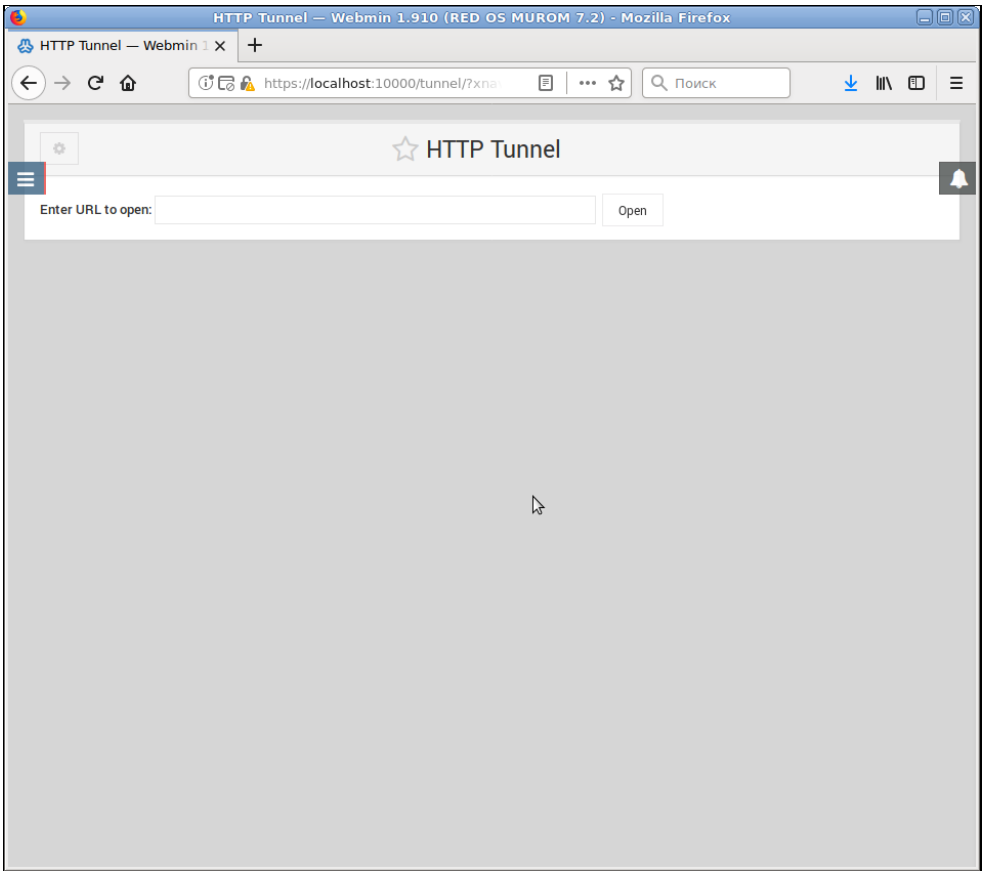
- Интервал регенерации ключа сервера

  Как часто сервер SSH повторно генерирует ключ, используемый для шифрования соединений.

HTTP Tunnel

Модуль доступен по ссылке «**HTTP Tunnel**» в разделе «**Прочее**» главного меню.

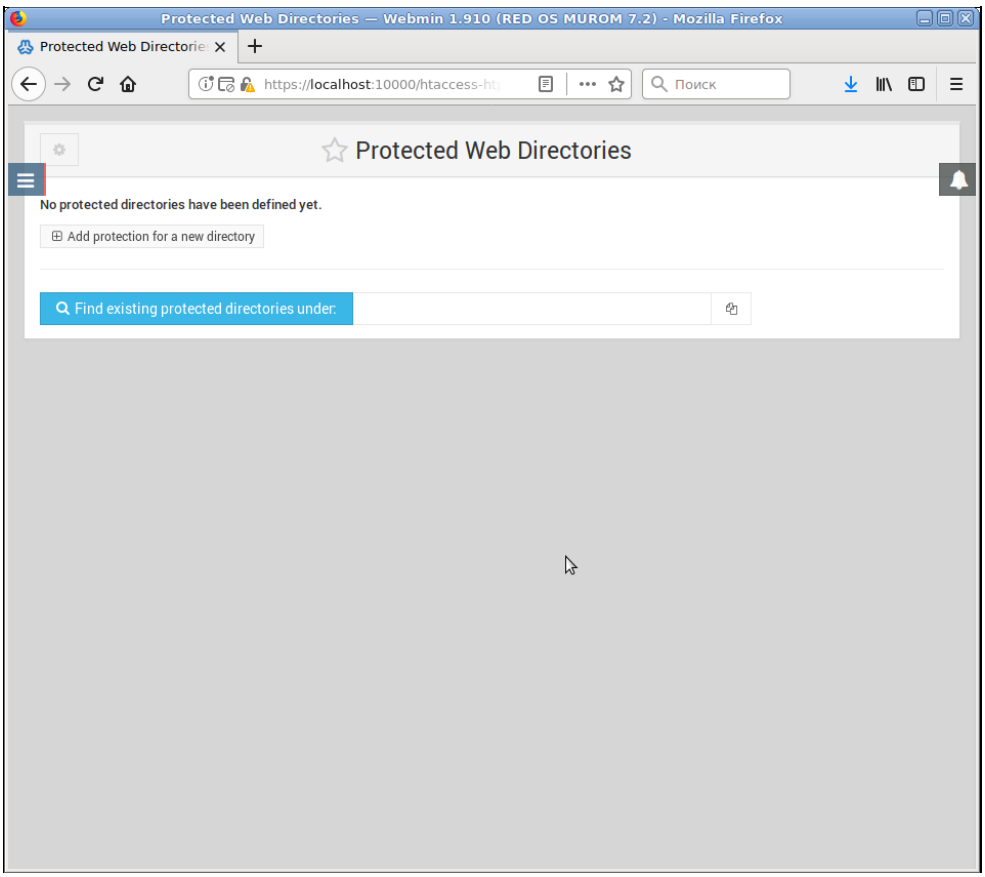
Модуль туннеля HTTP позволяет системному администратору создать значок в Usermin, который фактически соединяет пользователей с другим веб-сервером. Однако, вместо того, чтобы просто ссылаться на какой-либо URL-адрес, все запросы туннелируются через Usermin, и поэтому не появляются из браузера пользователя вообще. С точки зрения безопасности он абсолютно безвреден.



Protected Web Directories

Модуль доступен по ссылке «**Protected Web Directories**» в разделе «**Прочее**» главного меню.

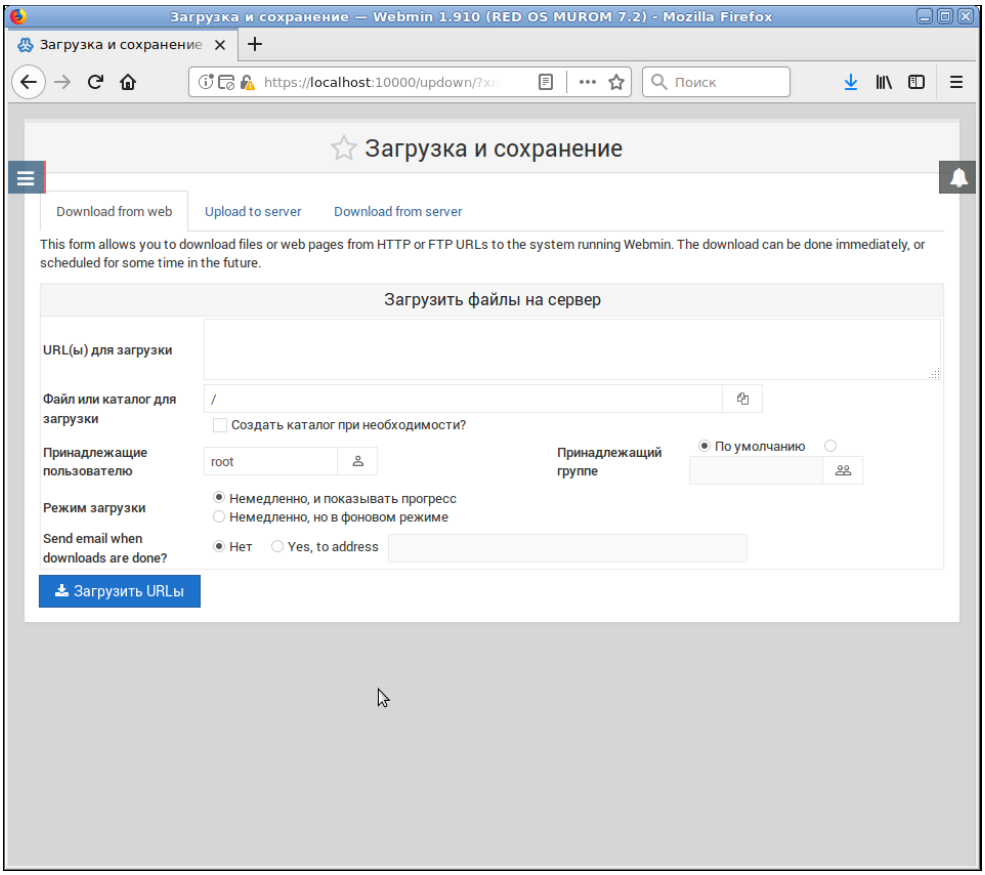
Модуль защищенных веб-каталогов позволяет управлять защищенными веб-каталогами **.htaccess** и **.htpasswd** файлов.



Загрузка и сохранение

Модуль доступен по ссылке «**Загрузка и сохранение**» в разделе «**Прочее**» главного меню.

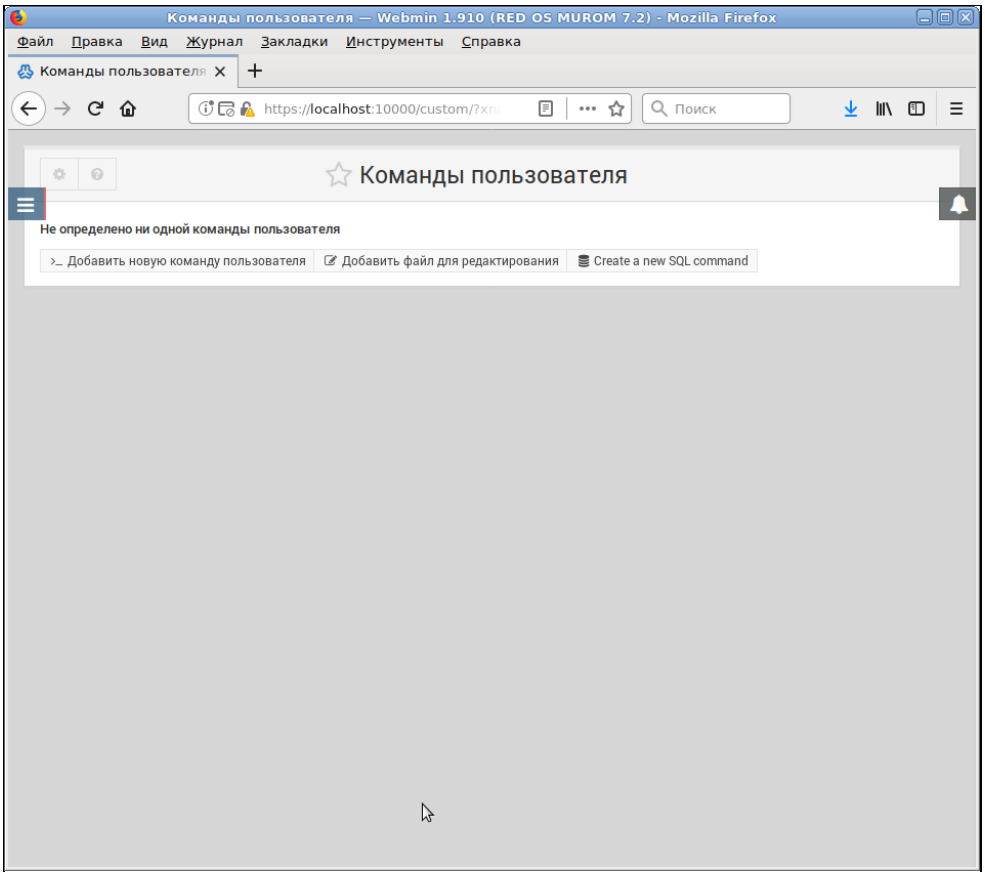
Эта форма позволяет загружать файлы или веб-страницы с URL-адресов HTTP или FTP в систему под управлением Webmin. Загрузка может быть выполнена немедленно или запланирована на некоторое время в будущем.



Команды пользователя

Вы найдете пункт «Команды пользователя» в левой панели Webmin консоли под **Прочее** -> **Команды пользователя**.

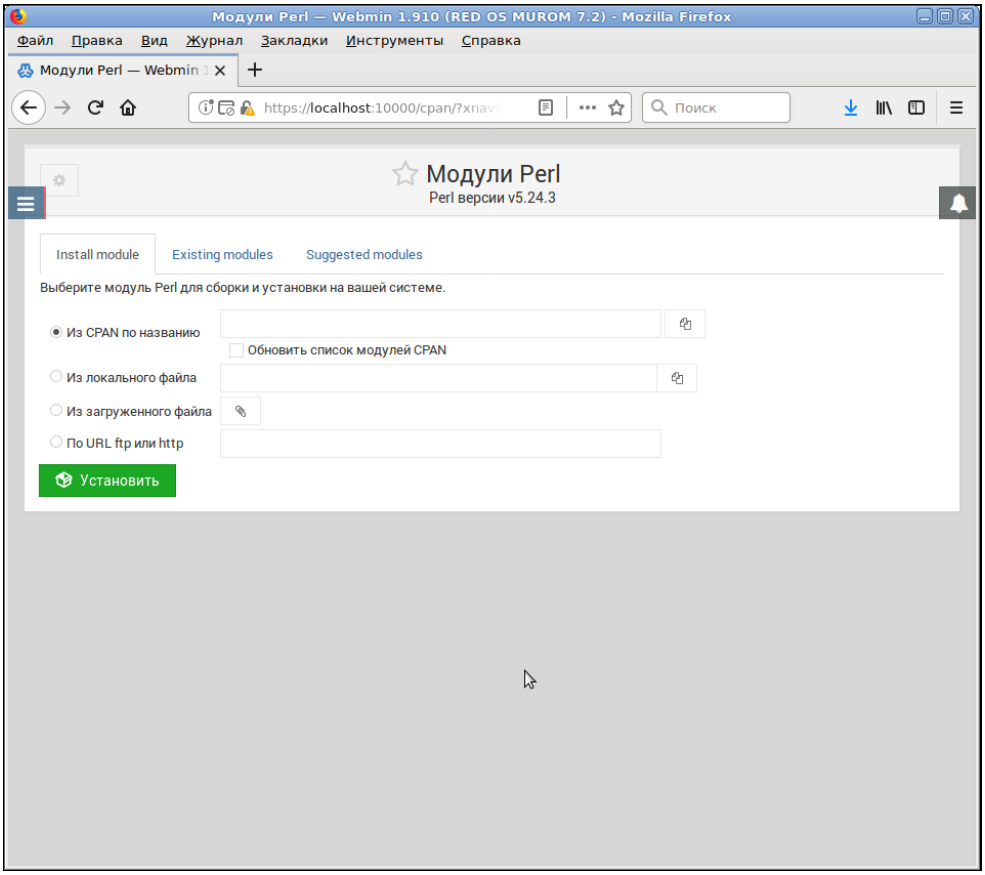
Позволяет неподготовленным пользователям выполнять команды или скрипты нажатием одной кнопки. Админу достаточно создать команду, заполнив соответствующие поля (прописать команду, задать параметры, пользователя, от имени которого будет выполняться команда, добавить описание и пр.). Здесь же во вкладке “**Прочее**” найдете и менеджер файлов (требует поддержки JAVA), который позволит получить доступ к файлам на удаленном компьютере в удобной графической оболочке.



Модули Perl

В категории другие в Webmin находится модуль **Perl Modules**, который можно использовать для просмотра, установки и удаления модулей Perl из вашей системы. Когда Вы вводите его, главная страница перечисляет все модули, которые в настоящее время установлены. Для каждого модуля отображается имя, краткое описание, дата установки и количество подмодулей. Подмодули - это термин Webmin для модулей Perl, включенных в tar дистрибутива.файл GZ вместе с основным модулем.

Поскольку Perl ведет себя одинаково во всех версиях Unix, этот модуль Webmin имеет одинаковый пользовательский интерфейс и функциональность во всех операционных системах.



Bandwidth Monitoring

Модуль мониторинга полосы пропускания может использоваться для создания простых отчетов об использовании полосы пропускания портом, хостом, протоколом и временем для трафика, отправляемого или маршрутизируемого через вашу систему. Это полезно как для автономных хостов, так и для тех, которые действуют как шлюз (возможно, с NAT) для сети.

Прежде чем его можно будет использовать, модуль должен настроить несколько правил брандмауэра и запись системного журнала для захвата трафика, отправленного и полученного через вашу систему. Во время установки необходимо выбрать внешний сетевой интерфейс системы, на котором будет отслеживаться трафик. Обычно это интерфейс PPP, используемый для подключения dialup или ADSL, или интерфейс Ethernet, подключенный к кабельному модему или вышестоящему маршрутизатору.

После захвата трафика продолжительностью не менее часа модуль может использоваться для создания отчетов, суммирующих трафик по одной из следующих категорий :

- *Час*. Дата и час получения данных.
- *День*. Дата, на которую эти данные были получены.
- *Хост*. Узел во внутренней сети или узел брандмауэра, который отправил или получил данные.
- *Внутренний порт*. Порт на внутреннем узле или узле брандмауэра, на который были отправлены данные. Этот режим полезен для определения объема трафика, генерируемого соединениями с каждым из серверов.
- *Внешний порт*. Порт на каком-либо сервере вне сети, на который были отправлены данные. С его помощью можно определить, к каким службам обращаются пользователи Сети.
- *Порт*. Как внутренние, так и внешние порты. Полезно для сравнения всего использования сети по типу службы.

Можно также ограничить отчет выбором узла, порта или протокола. Хост может быть введен по IP-адресу, имени хоста или сетевому адресу, например 192.168.1.0. Порт может быть введен по имени или номеру и будет соответствовать TCP и UDP.

Отчет также может быть ограничен трафиком, собранным между выбранными часами, используя поля для трафика после и для трафика до. Поскольку трафик суммируется по часам, нельзя ограничить отчет с большей точностью, чем по часам.

TCP Wrappers

Модуль TCP Wrappers использует простой язык управления доступом, основанный на шаблонах клиента (имя хоста/адрес, имя пользователя) и сервера (имя процесса, имя хоста/адрес).

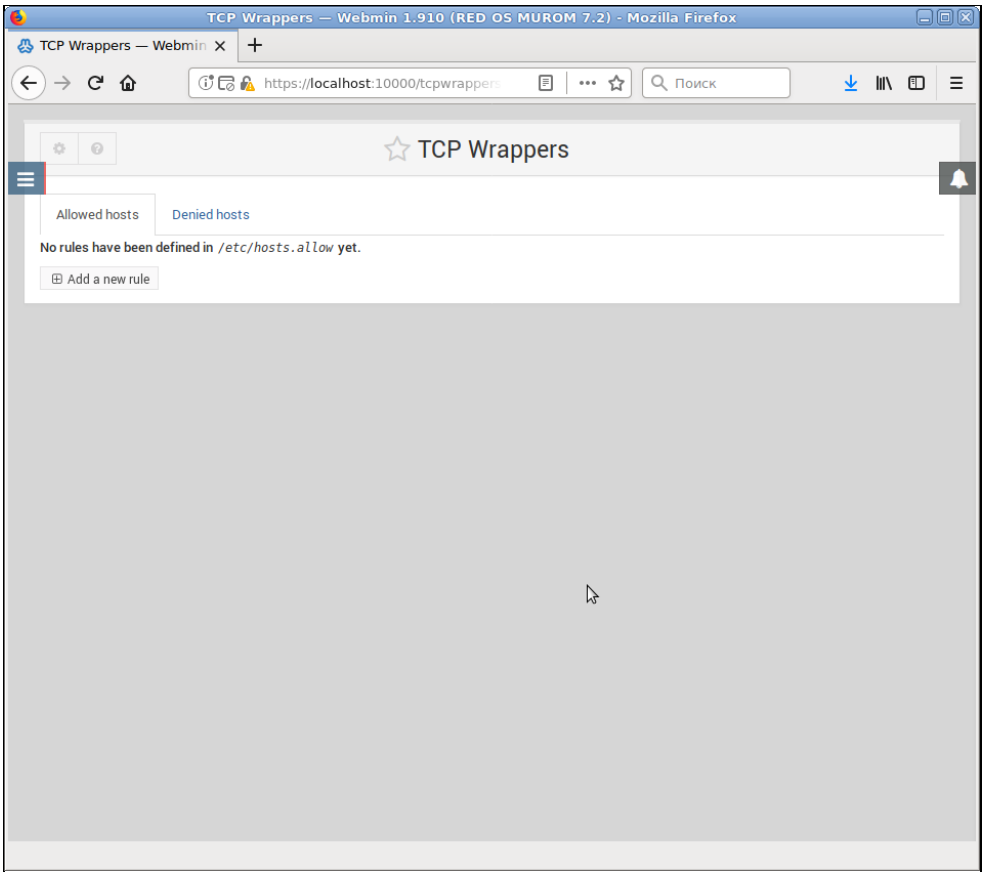
Расширенная версия языка управления доступом описана в документе **hosts_options**. Расширения включаются во время сборки программы с помощью команды - **PROCESS_OPTIONS**.

Контроль доступа к файлам

Программное обеспечение для контроля доступа использует шаблоны, описанные в двух файлах - **hosts.allow** и **hosts.deny**. Поиск шаблона будет остановлен при первом совпадении. Таким образом, вся цепочка будет выглядеть следующим образом:

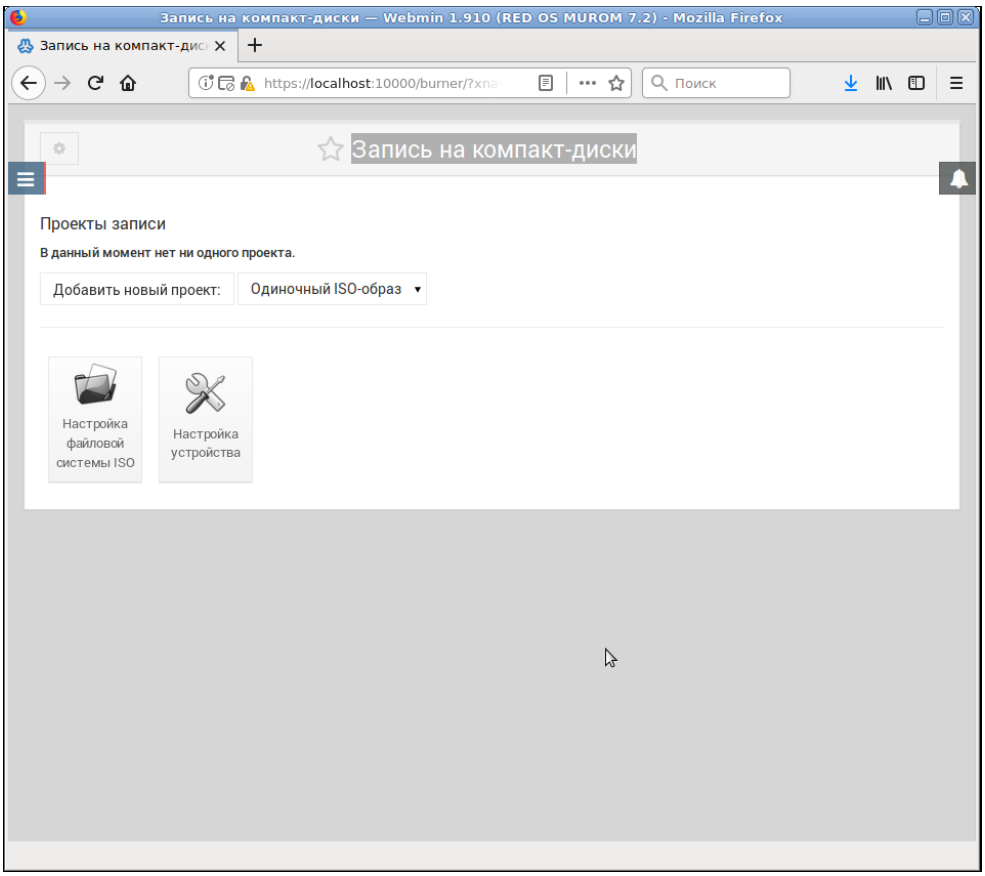
- сначала поиск осуществляется в файле **/etc/hosts.allow**. При совпадении пары (демон, клиент) доступ будет предоставлен;
- в случае, если в файле hosts.allow пара не найдена, поиск будет осуществлён в файле **/etc/hosts.deny**. Если поиск найдёт совпадение - доступ будет запрещён;
- в том случае, если поиск не найдёт совпадений в обоих файлах - доступ будет предоставлен.

В том случае если данных конфигурационных файлов в каталоге /etc не существует, они обрабатываются как "пустые". Таким образом, управление доступом можно отключить.



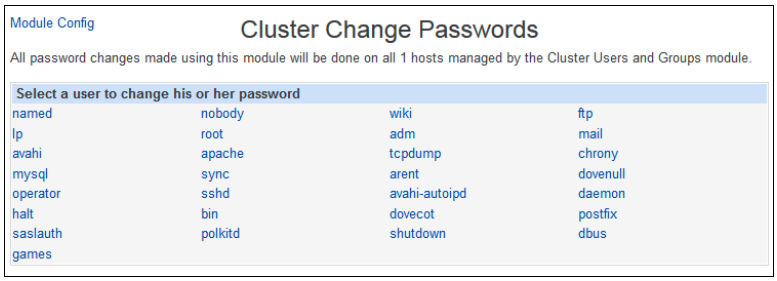
Запись на компакт-диски

Модуль диски находится в категории «**Оборудование**». Он предоставляет вам веб-интерфейс к CD / DVD burner, подключенному к Webmin-хосту.



Cluster Change Passwords

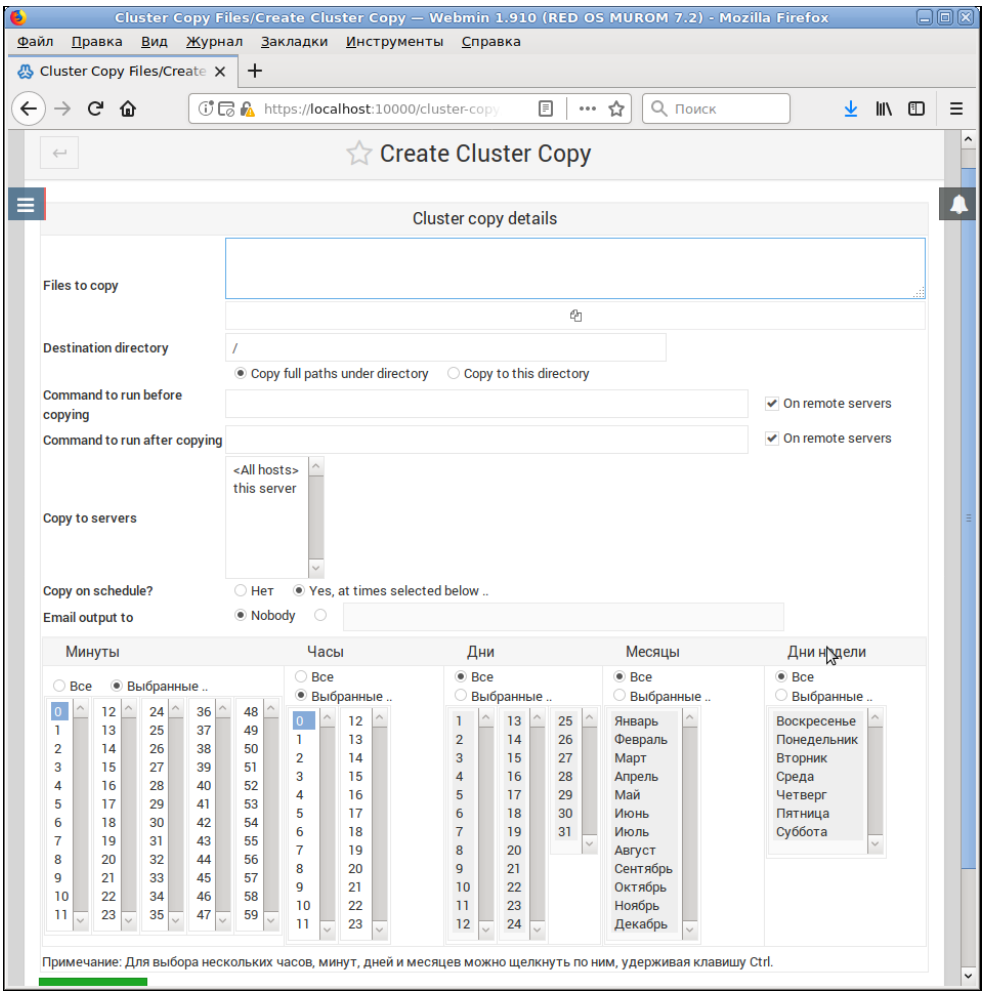
Модуль изменение паролей кластера-это способ изменить все пароли в кластере сразу.



Cluster Copy Files

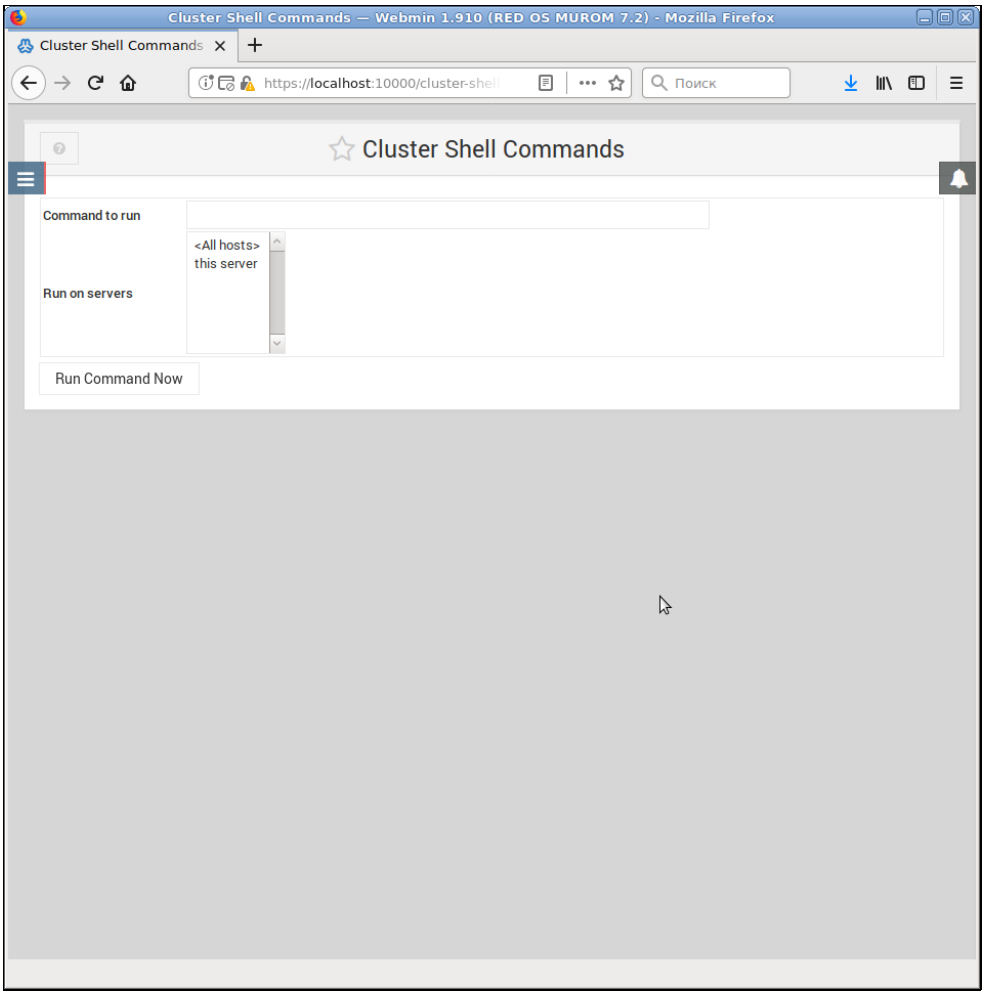
Модуль «**Копирование файлов кластера**» позволяет настроить запланированную передачу файлов с главного сервера на другие серверы кластера Webmin. Это может быть полезно для распространения файлов, таких как /etc/hosts, httpd.conf и другие, для которых нет сетевого протокола, такого как NIS или LDAP.

На главной странице модуля перечислены все определенные запланированные копии, и есть ссылка для создания новой. Для каждой копии можно определить исходные файлы, каталог назначения, целевые серверы и время выполнения. Целевые объекты должны быть сначала созданы в модуле индекса серверов Webmin с логином и паролем.



Cluster Shell Commands

Модуль команды оболочки кластера похож на командную оболочку, но позволяет выполнять простые команды на нескольких серверах одновременно, а не только на этом сервере. На главной странице можно ввести команду для запуска (или выбрать старую) и выбрать один или несколько серверов или групп для ее выполнения. В списке будут отображаться только серверы, созданные в модуле Webmin Servers Index с логином и паролем.



Cluster Usermin Servers

Модуль Cluster Usermin Servers позволяет управлять модулями, темами, пользователями и группами на нескольких серверах usermin с помощью одного интерфейса. Он сочетает в себе функции из модулей Usermin Configuration и Usermin Users с возможностью выполнения действий (таких как установка темы или создание пользователя) на нескольких серверах одновременно.

Управляемый сервер

В верхней части главной страницы под заголовком «Управляемые серверы» перечислены другие серверы Webmin, модули и пользователи которые управляются этим модулем. Чтобы добавить сервер в этот список, необходимо сначала добавить его в модуль серверы Webmin, указав имя пользователя и пароль для входа в Webmin на этом сервере. Затем можно выбрать сервер из списка рядом с кнопкой «Добавить сервер».

Когда сервер будет добавлен, он будет проверен, чтобы убедиться, что он работает под управлением поддерживаемой версии Usermin (0.985 или более поздней версии) и что на нем установлены необходимые модули. Списки всех модулей, тем, пользователей и групп с сервера будут загружены и кэшированы локально.

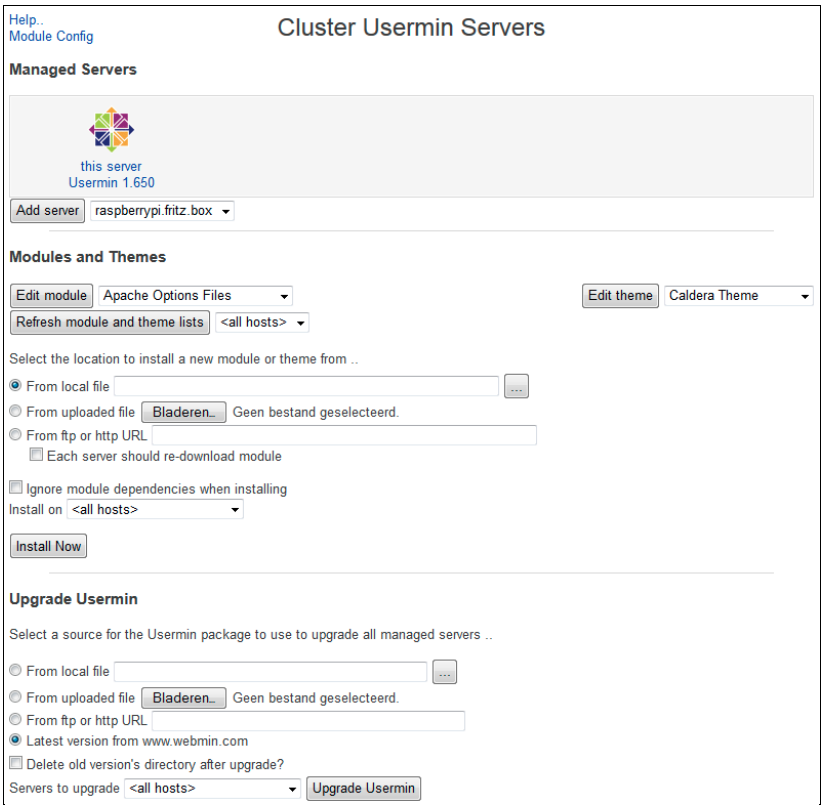
При наличии хотя бы одного значка в разделе управляемые серверы можно использовать кнопки в разделе «Пользователи и группы» для редактирования, создания или установки списков управления доступом для пользователей и групп на любом сервере. Пользователи и группы, которые вы создадите, будут созданы на всех управляемых серверах, но те, которые уже существуют, которые редактируются или удаляются, будут изменены только на серверах, на которых они уже существуют.

Модули и темы

В середине страницы в разделе модули и темы находятся кнопки для редактирования модулей и тем, установленных на любом управляемом сервере, и форма для установки нового модуля или темы на всех серверах.

Обновление Usermin

В нижней части страницы Вы можете обновить Usermin на всех управляемых серверах.

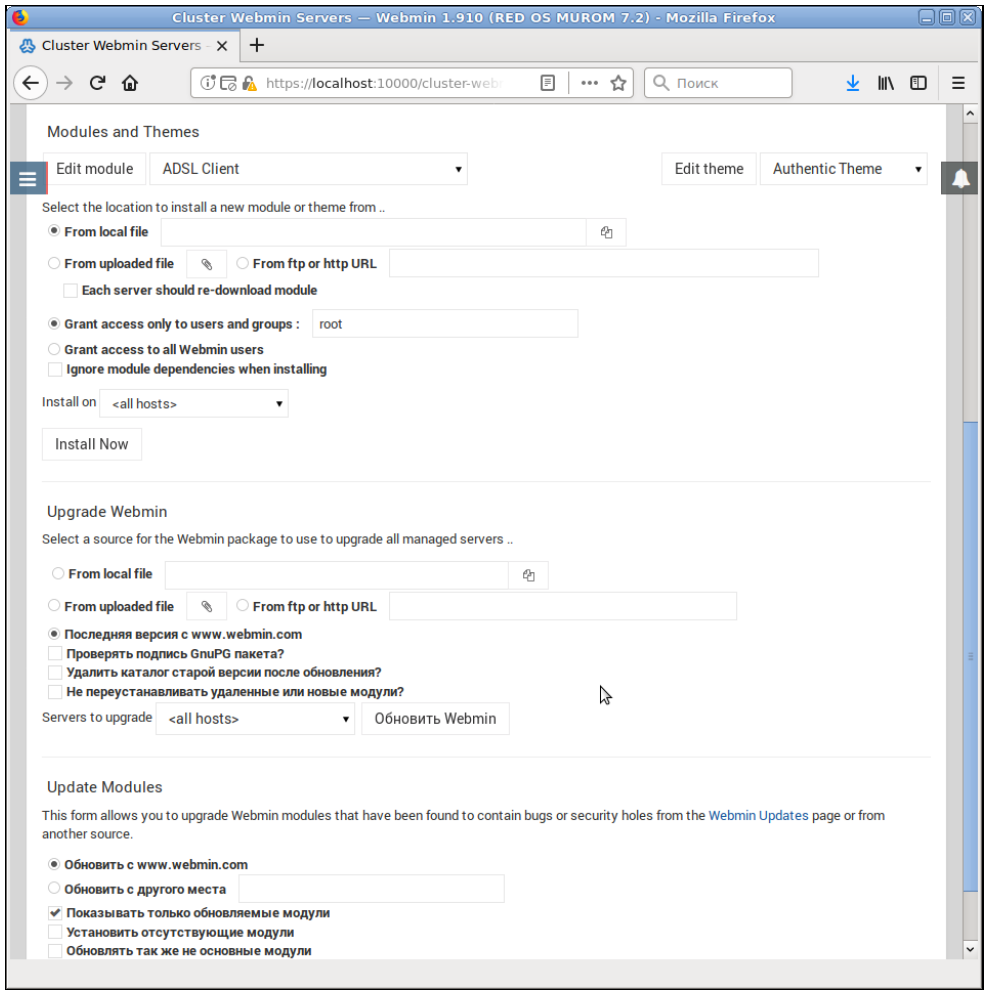


Cluster Webmin Servers

Модуль Cluster Webmin Configuration имеет две цели - управление пользователями и группами Webmin в нескольких системах, а также установка и удаление модулей и тем. Если в Вашей сети несколько серверов Webmin, этот модуль может быть очень полезен для синхронизации их списков пользователей и настроек контроля доступа. И это обеспечивает простой способ развертывания нового модуля на большом количестве серверов одновременно.

Как и другие кластерные модули, этот хранит списки модулей, тем, пользователей и групп с каждого управляемого сервера в главной системе. Это ускоряет поиск, но создает потенциал для несоответствий между тем, как настроены основные системы в других системах, и тем, какие они на самом деле. Например, если Вы устанавливаете модуль или обновляете управляемый хост, главная система не будет знать об этом, пока он не будет обновляться ежегодно, как объясняется в разделе «Обновление списков пользователей и модулей».

Если щелкнуть на значок модуля в категории «Кластер» в главном меню Webmin, отобразится главная страница. Вверху находится таблица значков, по одной для каждого из управляемых серверов. Под каждым значком указана версия Webmin, которую он в данный момент использует, определяется, когда он был добавлен в модуль или последний раз обновлен. Предполагая, что у вас есть несколько серверов в списке, под ними находятся формы для редактирования и добавления пользователей и групп, за которыми следуют дополнительные формы для установки и поиска модулей и тем.


Cluster Webmin Servers — Webmin 1.910 (RED OS MUROM 7.2) - Mozilla Firefox
Cluster Webmin Servers
https://localhost:10000/cluster-web
Поиск
Modules and Themes
Edit module
ADSL Client
Edit theme
Authentic Theme
Select the location to install a new module or theme from ..
From local file
From uploaded file
From ftp or http URL
Each server should re-download module
Grant access only to users and groups :
root
Grant access to all Webmin users
Ignore module dependencies when installing
Install on
<all hosts>
Install Now
Upgrade Webmin
Select a source for the Webmin package to use to upgrade all managed servers ..
From local file
From uploaded file
From ftp or http URL
Последняя версия с www.webmin.com
Проверять подпись GnuPG пакета?
Удалить каталог старой версии после обновления?
Не переустанавливать удаленные или новые модули?
Servers to upgrade
<all hosts>
Обновить Webmin
Update Modules
This form allows you to upgrade Webmin modules that have been found to contain bugs or security holes from the Webmin Updates page or from another source.
Обновить с www.webmin.com
Обновить с другого места
Показывать только обновляемые модули
Установить отсутствующие модули
Обновлять так же не основные модули

Ansible - система автоматизации настройки и развертывания ПО

Установка Ansible
Подключение клиентских хостов
Проверка подключения клиентских хостов
Создание плейбука и его выполнение
Выполнение одиночной команды
Обновление Ansible до версии 6.4.0

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** ansible-6.4.0-1

Ansible — система управления конфигурациями, написанная на Python, с использованием декларативного языка разметки для описания конфигураций. Используется для автоматизации настройки и развертывания программного обеспечения. Обычно используется для управления Linux-узлами, но Windows также поддерживается. Поддерживает работу с сетевыми устройствами, на которых установлен Python версии 2.4 и выше по SSH или WinRM соединению.

Установка Ansible

Для установки **Ansible** открываем терминал в режим суперпользователя командой:

```
su -
```

и выполните команду:

```
dnf install ansible
```

Подключение клиентских хостов

1) В файле **/etc/ansible/hosts** прописать все хосты, на которые будет распространяться конфигурация. Хосты можно разделить по группам, а так же, если у вас есть домен, то автоматически экспортировать список из домена. Можно прописывать как ip адреса так и имена хостов, если они резолвятся DNS ом в сети. Для теста пропишем 2 хоста.

```
[test]
10.10.1.111
10.10.1.74
```

2) Подключение к хостам осуществляется по протоколу **ssh** с помощью rsa ключей. Сгенерировать серверный ключ можно командой ниже. При её выполнении везде нажмите **Enter**.

```
ssh-keygen -C "$(whoami)@$(hostname)-$(date -I)"
```

3) Далее нужно распространить ключ на все подключенные хосты. Распространить ключи на хосты можно командой:

```
ssh-copy-id root@server
```

где:

- **root** - это пользователь, от имени которого будут выполняться плейбуки;
- **server** - IP-адрес хоста.

Пример: `root@10.10.1.74` .

Проверка подключения клиентских хостов

Пингуем удаленные хосты с помощью **Ansible**:

```
ansible test -m ping

test-1 | success >> {
    "changed": false, U
    "ping": "pong"
}

test-2 | success >> {
    "changed": false,
    "ping": "pong"
}
```

Где **test** - это группа хостов, указанная в файле **hosts**. В результате под каждым хостом должно быть написано `"ping": "pong"`.

Создание плейбука и его выполнение

Плейбуки являются сценариями, выполняемыми на удаленных хостах. Создаем каталог, для хранения наших **playbooks**, которые пишутся на языке **YAML**:

```
mkdir /etc/ansible/playbooks
```

Для примера создадим плейбук, устанавливающий программы. В каталоге **/etc/ansible/playbooks** создаем файл **install_programm.yml**:

```
touch /etc/ansible/playbooks/install_programm.yml
```

Содержимое файла следующее:

```
---
- hosts: all
tasks:
- name: Install programm
dnf:
name: "{{ packages }}"
vars:
packages:
- unrar
- p7zip
```

В данном примере для установки используется модуль **dnf**. Применяется массив **packages** для установки. В него вписываются необходимые для установки программы.

Если хотите, можно проверить, на каких хостах будет происходить работа, командой:

```
ansible-playbook /etc/ansible/playbooks/install_programm.yml --list-host
```

Запустить только что созданный набор инструкций можно следующей командой:

```
ansible-playbook /etc/ansible/playbooks/install_programm.yml
```

Выполнение одиночной команды

С помощью **Ansible** возможно сразу на всех клиентах выполнить команду **bash** без создания плейбуков. Просмотрим информацию об использовании оперативной памяти на удаленных хостах:

```
ansible test -a "free -h"

test-1 | success | rc=0 >>
             total       used       free     shared    buffers     cached
Mem:          7.6G       6.4G       1.2G       471M        64M       1.2G
-/+ buffers/cache:       5.2G       2.4G
Swap:         4.0G       616M       3.4G
```

```
test-2 | success | rc=0 >>
             total       used       free     shared    buffers     cached
Mem:          3.9G       3.3G       573M       333M       4.8M       442M
-/+ buffers/cache:       2.9G       1.0G
Swap:         4.0G       1.7G       2.3G
```

Обновление Ansible до версии 6.4.0

Пакеты **Ansible** версии **6.X** располагаются в подключаемом репозитории, поэтому порядок обновления несколько отличается от обычного.

Установка и обновление пакетов **Ansible** до версии **6.X** на **РЕД ОС 7.3** производится с помощью следующих команд (потребуются права пользователя **root**):

```
dnf install ansible6-release    # подключение репозитория
dnf clean all     # очистка метаданных
dnf makecache     # загрузка метаданных из всех репозиториев
dnf install ansible     # установка новой версии ansible 6.4
```

Puppet - централизованное управление конфигурацией ОС и ПО

Предварительная подготовка
Установка Puppet-сервера
Установка Puppet-клиента
Подключение клиента к серверу

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия puppet:** puppet-7.12.0-4

Puppet - это кроссплатформенная структура, позволяющая системным администраторам выполнять общие задачи с использованием кода. Код позволяет выполнять различные задачи от установки новых программ до проверки прав доступа файлов или обновлений пользовательских учетных записей. В большинстве случаев **puppet** используется в конфигурации клиент/сервер.

Вы можете подробнее ознакомиться с организацией централизованного управления конфигурацией ОС и ПО при помощи **Puppet**, просмотрев наши обучающие видео:

- на **RuTube** — Puppet - централизованное управление конфигурацией ОС и ПО;
- в **Яндекс.Дзен** — Puppet - централизованное управление конфигурацией ОС и ПО;
- в **VK Видео** — Puppet - централизованное управление конфигурацией ОС и ПО.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка

Сначала необходимо установить статические имена хостов на сервере и на клиенте соответственно:

```
hostnamectl set-hostname puppet.server --static
hostnamectl set-hostname puppet.client --static
```

Затем в базу данных доменных имен необходимо добавить имя и IP-адрес сервера Puppet, а также клиента Puppet:

```
echo '192.168.0.34 puppet.server' >> /etc/hosts
echo '192.168.0.35 puppet.client' >> /etc/hosts
```

Установка Puppet-сервера

На *серверной* машине установите пакет сервера Puppet:

```
dnf install puppetserver
```

Затем требуется отредактировать конфигурационный файл сервера Puppet **/etc/puppetlabs/puppet/puppet.conf**, добавив следующие настройки:

```
[main]
server =  puppet.server
ca_server =  puppet.server
[server]
vardir = /opt/puppetlabs/server/data/puppetserver
logdir = /var/log/puppetlabs/puppetserver
rundir = /var/run/puppetlabs/puppetserver
pidfile = /var/run/puppetlabs/puppetserver/puppetserver.pid
codedir = /etc/puppetlabs/code
dns_alt_names = puppet
```

dns_alt_names — список имен хостов, которые серверу разрешено использовать в качестве основного сервера. Имя хоста, которое ваши агенты используют в настройках своего сервера, должно быть включено либо в этот параметр, либо в параметр имени сертификата основного сервера. Этот параметр используется только при первоначальной генерации сертификата основного сервера.

Далее перезагрузите/запустите сервер Puppet:

```
systemctl restart puppetserver
```

Проверьте, что статус сервиса Puppet изменился на активный:

```
systemctl status puppetserver

● puppetserver.service - puppetserver Service
  Loaded: loaded (/usr/lib/systemd/system/puppetserver.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2021-12-07 12:09:44 MSK; 45s ago
 Main PID: 1084 (java)
   Tasks: 45 (limit: 4915)
  Memory: 1.2G
    CPU: 1min 47.001s
  CGroup: /system.slice/puppetserver.service
          └─1084 /usr/bin/java -Xms2g -Xmx2g -Djruby.logger.class=com.puppetlabs.jruby_utils.jruby.Slf4jLogger -
XX:+CrashOnOutOfMemoryError -XX:ErrorFile=/var/log/puppetlabs/puppetserver/p
```

Установка Puppet-клиента

На *клиентской* машине необходимо установить пакет клиента Puppet:

```
dnf install puppet
```

Затем требуется отредактировать конфигурационный файл клиента Puppet, добавив следующие настройки в файл **/etc/puppetlabs/puppet/puppet.conf**:

```
[main]
server = puppet.server
```

После этого запустите клиент Puppet:

```
systemctl start puppet
```

Проверьте, что статус клиента Puppet активен:

```
systemctl status puppet

● puppet.service - Puppet agent
  Loaded: loaded (/usr/lib/systemd/system/puppet.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2021-12-07 12:16:36 MSK; 13s ago
 Main PID: 1321 (puppet)
   Tasks: 1 (limit: 1963)
  Memory: 52.0M
    CPU: 2.879s
  CGroup: /system.slice/puppet.service
          └─1321 /opt/puppetlabs/puppet/bin/ruby /opt/puppetlabs/puppet/bin/puppet agent --no-daemonize
```

Подключение клиента к серверу

Далее на *серверной* машине необходимо перечислить узлы клиента Puppet на сервере Puppet:

```
/opt/puppetlabs/bin/puppetserver ca list --all
```

Затем нужно добавить имя хоста Puppet-клиента к Puppet-серверу:

```
/opt/puppetlabs/bin/puppetserver ca sign --certname  puppet.client
```

После этого на *клиентской* машине необходимо запустить тест соединения с сервером Puppet:

```
/opt/puppetlabs/bin/puppet agent -t
```

```
Info: Using environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Caching catalog for puppet.agent-node
Info: Applying configuration version '1638876480'
Notice: Applied catalog in 0.28 seconds
```

Давайте проверим корректность работы Puppet-клиента и Puppet-сервера, установив пакет **httpd** с помощью манифеста.

Для этого сначала убедитесь, что на текущий момент на клиентской машине не установлен пакет **httpd**:

```
rpm -qa | grep -i httpd
```

Затем на серверной машине создайте манифест нового модуля **install_pkg** сервера Puppet, добавив задачу установки пакета **httpd** в файле **/etc/puppetlabs/code/environments/production/manifests/init.pp**:

```
class install_pkg {
  package { httpd:
  ensure => installed
  }
}
```

И создайте манифест, подключающий модуль **install_pkg** сервера Puppet в файле **/etc/puppetlabs/code/environments/production/manifests/site.pp**:

```
node default {
  include install_pkg
}
```

После этого на *клиентской* машине принудительно запустите агент сервера Puppet:

```
/opt/puppetlabs/bin/puppet agent -t
Info: Using environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Caching catalog for puppet.client
Info: Applying configuration version '1638877024'
Notice: /Stage[main]/Install_pkg/Package[httpd]/ensure: created
Notice: Applied catalog in 22.35 seconds
```

Убедитесь, что на *клиентской* машине пакет **httpd** был успешно установлен:

```
rpm -qa | grep -i httpd
httpd-tools-2.4.46-4.el7.x86_64
httpd-filesystem-2.4.46-4.el7.noarch
httpd-2.4.46-4.el7.x86_64
```

Проверка связи между сервером и клиентом прошла успешно.

Citrix Linux VDA

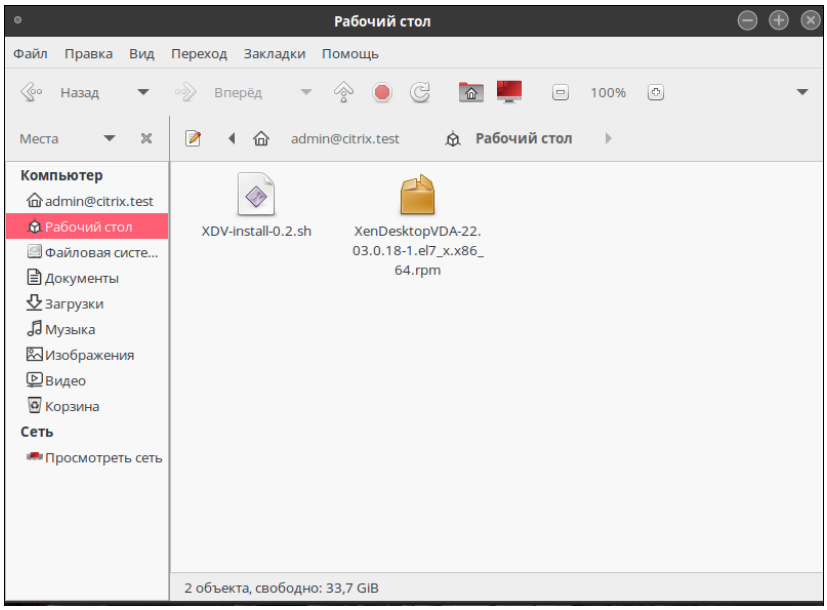
Автоматическая подготовка к настройке Citrix Linux VDA
Ручная подготовка к настройке Citrix Linux VDA
Настройка Citrix Linux VDA

Примечание.

Установка **VDA** выполняется на версии **XenDesktopVDA-22.03.0.18-1.el7_x.x86_64**.

Автоматическая подготовка к настройке Citrix Linux VDA

1) Загрузите скрипт XDV-install-0.2.sh в папку, где расположен установочный пакет **XenDesktopVDA**:



2) Откройте терминал. Для этого нажмите **ПКМ** – **Открыть в терминале**.

3) Перейдите в сеанс пользователя **root**:

```
su -
```

4) Перейдите в папку, где лежит скрипт и установочный пакет. Например:

5) Запустите скрипт:

```
sh XDV-install-0.2.sh
```

Ручная подготовка к настройке Citrix Linux VDA

1) Перейдите в сеанс пользователя **root**:

```
su -
```

2) Отключите **Selinux**:

```
sed -i 's/^SELINUX=.*$/SELINUX=disabled/' /etc/selinux/config
```

3) Обновите систему:

```
dnf update
```

4) Установите необходимые пакеты:

```
dnf install qt5-qtbase ibus nss-tools gperftools-libs cyrus-sasl-gssapi python2 postgresql-jdbc postgresql-server java-11-openjdk icoutils firewalld policycoreutils-python-utils python3-policycoreutils dbus dbus-common dbus-daemon dbus-tools dbus-x11 xorg-x11-server-utils xorg-x11-xinit libXpm libXrandr libXtst motif pam util-linux util-linux-user xorg-x11-utils bash findutils gawk sed cups foomatic-filters ghostscript libxml2 libmspack libxcrypt-compat
```

5) Обновите **Java**:

```
yum update java-11-openjdk
```

6 Установите следующие пакеты:

```
yum install postgresql-server postgresql-jdbc
```

7) Запустите настройку **Postgresql**:

```
postgresql-setup initdb
```

8) Запустите и добавьте в автозагрузку **Postgresql**:

```
systemctl enable postgresql --now
```

9) Введите машину в домен:

```
join-to-domain.sh
```

10) Выполните установку **dotnet-sdk-6.0**:

```
dnf install dotnet-sdk-6.0
```

11) Запустите установку **XenDesktopVDA**:

```
dnf localinstall XenDesktopVDA*.rpm
```

12) Запустите настройку **Citrix Linux VDA**:

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
```

Настройка Citrix Linux VDA

В поле **Путь среды выполнения DotNet Core**: нажмите **Enter**.

В поле **Если не указано, Linux VDA будет использовать GNOME/KDE/Unity по умолчанию**: введите **mate**.

В поле **Включить поддержку записей DNS CNAME? (y/n) [n]**: нажмите **Enter**.

В поле **Укажите полное доменное имя по крайней мере одного контроллера Delivery Controller**: введите *полное доменное имя* Delivery Controller, например, **cvad.citrix.test**.

В поле **Укажите порт TCP/IP, который служба Virtual Delivery Agent (ctxvda) должна использовать для обмена данными с контроллером Delivery Controller [80]**: нажмите **Enter**.

В поле **Citrix Scout на контроллере Delivery Controller. Укажите TCP/IP-порт, через который служба Citrix Telemetry Service должна прослушивать Citrix Scout. [7503]**: нажмите **Enter**.

В поле **Citrix Scout на контроллере Delivery Controller. Укажите TCP/IP-порт, через который служба Citrix Telemetry Service должна обмениваться данными с Citrix Scout. [7502]**: нажмите **Enter**.

В поле **Зарегистрировать эти службы для запуска при загрузке? (y/n) [y]**: нажмите **Enter**.

В поле **Открыть автоматически необходимые порты (по умолчанию — порты 80, 1494, 2598, 8008 и 6001~6099) в системном брандмауэре для Linux VDA? (y/n) [y]**: нажмите **Enter**.

В поле **Выберите один из вышеприведенных вариантов (1–5) [1]**: введите **4**.

В поле **Включить функцию HDX 3D Pro? (y/n) [n]**: нажмите **Enter**.

В поле **Включить режим рабочих столов VDI (один сеанс)? (y/n) [n]**: нажмите **Enter**.

В поле **Если необходимо, укажите имя локального сайта DNS. [<none>]**: нажмите **Enter**.

В поле **Если необходимо, укажите адрес в формате "полное доменное имя:порт" как минимум одного сервера LDAP. [<none>]**: нажмите **Enter**.

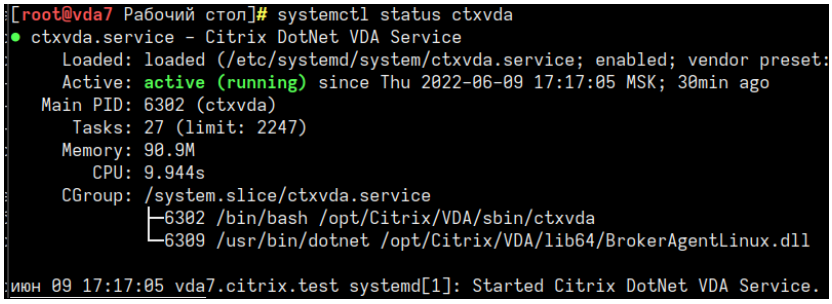
В поле **Если необходимо, укажите базу поиска LDAP. [<none>]**: нажмите **Enter**.

В поле **При необходимости укажите список FAS-серверов (например, fasserver.company.com). [<none>]**: нажмите **Enter**.

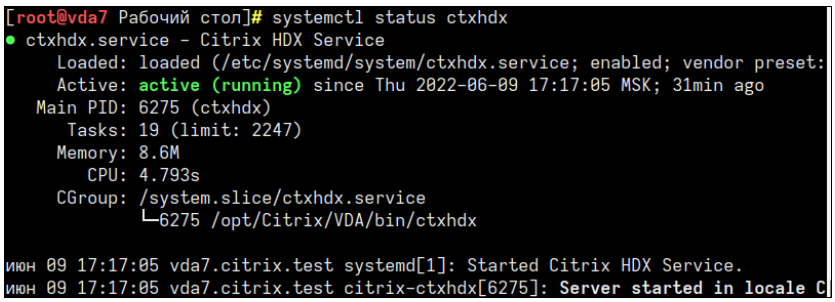
В поле **Запустить эти службы после завершения конфигурации? (y/n) [y]**: нажмите **Enter**.

После настройки **Citrix Linux VDA** проверьте службы **ctxvda** и **ctxhdx**:

```
systemctl status ctxvda
```




```
systemctl status ctxhdx
```



В случае, если обе службы успешно запущены (**active (running)**), добавьте машину в **Citrix Studio**.

ВАЖНО!

Linux VDA не поддерживает одновременное распространение приложений и рабочего стола, т. е. необходимо 2 машины для распространения каждого пункта.

Установка VirtualBox

Установка
Расширение размера диска виртуальной машины

Для установки **VirtualBox** у локального пользователя должны быть **права администратора** (пользователь должен входить в **sudoers**).

Вы можете подробнее ознакомиться с возможностями работы **VirtualBox**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с VirtualBox в РЕД ОС;
- в **Яндекс.Дзен** — Работа с VirtualBox в РЕД ОС;
- в **VK Видео** — Работа с VirtualBox в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Устанавливаем пакет **VirtualBox** с помощью утилиты **dnf**.

Установка **VirtualBox** вместе с гостевыми дополнениями и модулями ядра:

```
dnf install VirtualBox VirtualBox-guest-additions VirtualBox-kmod_$(uname -r)
```

В названии пакета **VirtualBox-kmod** добавляется **$(uname -r)** для того, чтобы установился модуль для текущей версии ядра, на которой загружена ОС.

После установки пакетов выполните перезагрузку ОС.

Для того чтобы **VirtualBox** поддерживал **Usb 3.0** и **Usb 2.0**, зайдите на страницу https://www.virtualbox.org/wiki/Downloads и скачайте **VirtualBox Extension Pack**. Для установки Extension Pack'а перейдите в "**Файл**" - "**Инструменты**" - "**Менеджер плагинов**", щелкните "**Установить**", найдите папку, в которую был скачан (обычно «Загрузки») Extension Pack, и двойным щелчком добавьте его.

ВНИМАНИЕ!

ДЛЯ ДОБАВЛЕНИЯ И УДАЛЕНИЯ ПЛАГИНОВ ТРЕБУЕТСЯ ПОЛЬЗОВАТЕЛЬ С **ПРАВАМИ АДМИНИСТРАТОРА**.

Для того чтобы в виртуальных машинах можно было использовать USB-устройства, подключённые к ПК, необходимо выполнить следующую команду:

```
usermod -a -G vboxusers user
```

где **user** - это пользователь, которому нужно разрешить проброс USB.

Затем перезайдите в сеанс пользователя **user**.

Расширение размера диска виртуальной машины

Применимо только к дискам формата **.VDI** и не работает с дисками форматов **.VHD** и **.VMDK**. Такие диски можно клонировать в диск формата **VDI**.

Данный метод актуален только для динамических дисков и не работает с дисками фиксированного размера. Однако такие диски можно клонировать в динамический диск.

Перед изменением размера диска необходимо выключить виртуальную машину и сделать клон диска.

Изменить размер диска можно из командной строки:

```
vboxmanage modifyhd YOUR_HARD_DISK.vdi --resize SIZE_IN_MB
```

или из меню графического менеджера виртуальных машин (если используемая версия Oracle VirtualBox поддерживает эту возможность: Меню "**Файл**" - "**Менеджер виртуальных носителей**".

Если на вашей машине содержится несколько снимков, то нужно изменить размер диска каждого диска Это можно сделать в графическом менеджере виртуальных носителей, или командой вида:

```
vboxmanage modifyhd YOUR_HARD_DISK.vdi --resize SIZE_IN_MB
for x in Snapshots/*.vdi ; do vboxmanage modifyhd $x --resize SIZE_IN_MB ; done
```

Изменение размера диска не изменяет размеры дисковых разделов. Для того, чтобы гостевая машина получила доступ к дополнительному дисковому пространству, нужно изменить размер дисковых разделов. Для этого нужно загрузить виртуальную машину с Live-CD, либо примонтировать диск к другой виртуальной машине. И в первом, и во втором случае изменение дисковых разделов можно сделать с помощью программы **GParted**.

Установка РЕД ОС в VirtualBox

Создание новой ВМ в VirtualBox
Установка РЕД ОС
Настройка виртуальной машины с помощью командной строки

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VirtualBox-7.0.12-1

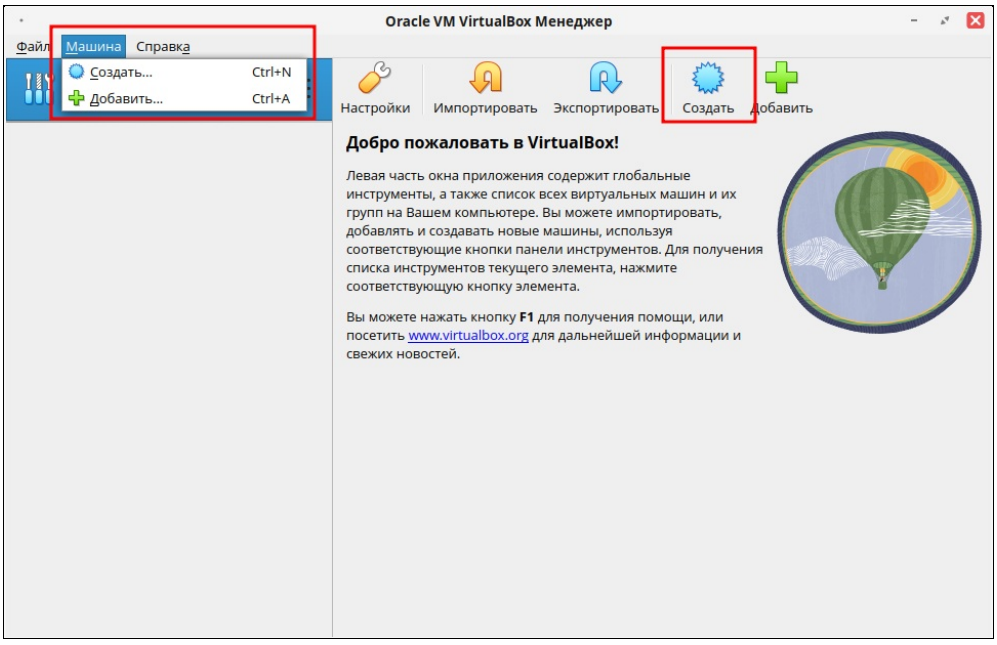
Вы можете подробнее ознакомиться с информацией по установке системы в VirtualBox, просмотрев наши обучающие видео:

- на **RuTube** — Установка РЕД ОС в виртуальных средах на примере Oracle VM VirtualBox ;
- в **Яндекс.Дзен** — Установка РЕД ОС в виртуальных средах на примере Oracle VM VirtualBox ;
- в **VK Видео** — Установка РЕД ОС в виртуальных средах на примере Oracle VM VirtualBox .

На наших каналах вы также сможете найти много другой полезной информации.

Создание новой ВМ в VirtualBox

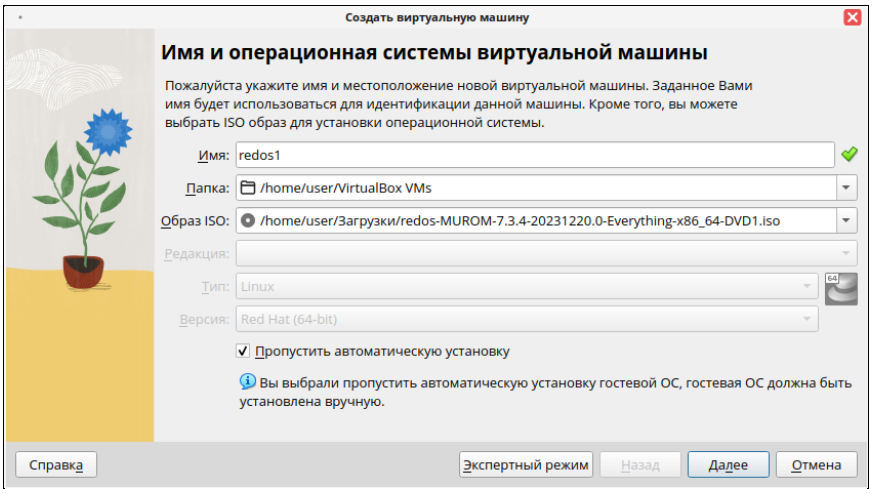
Для создания новой ВМ в окне приветствия **VirtualBox** нажмите «**Создать**» или выберите пункт меню «**Машина**» – «**Создать**».



В окне создания ВМ необходимо:

- задать имя будущей ВМ;
- указать каталог хранения данных ВМ;
- выбрать ISO-образ ОС;
- установить флаг пропуска автоматической установки ОС (по желанию).

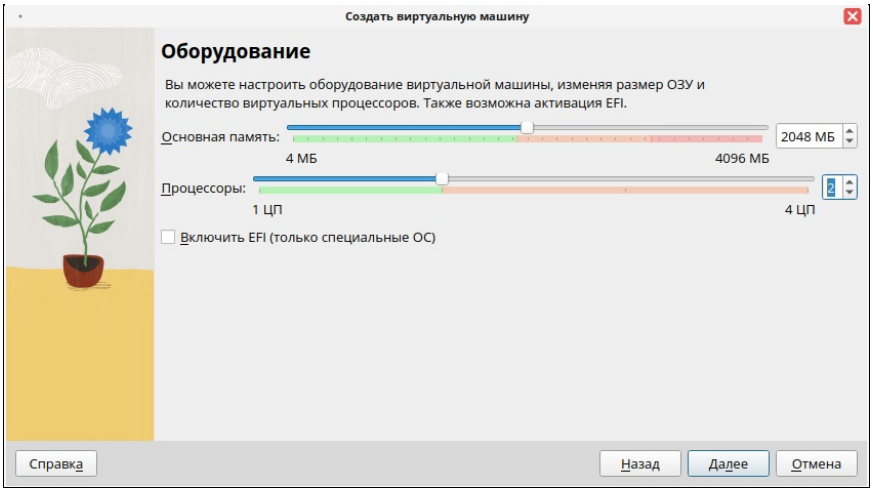
Нажмите «**Далее**».



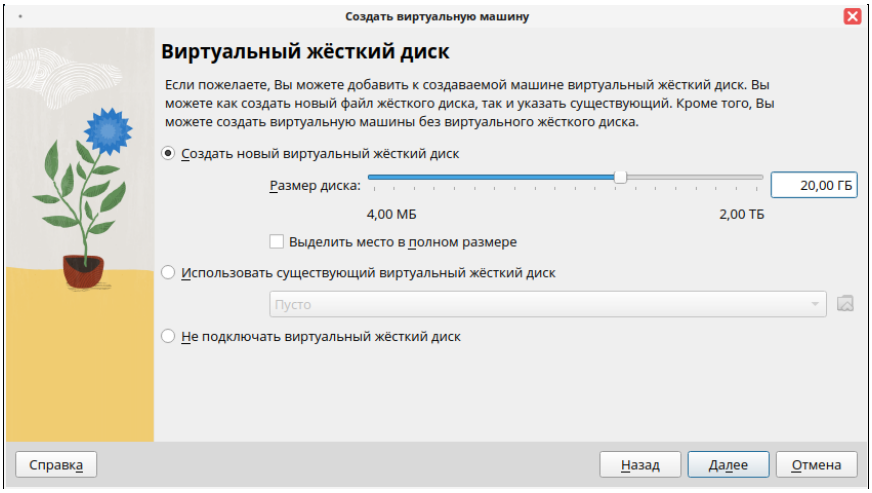
Выполните настройку оборудования:

- укажите объем ОЗУ (рекомендуется **не менее 2 ГБ**);
- укажите количество процессоров.

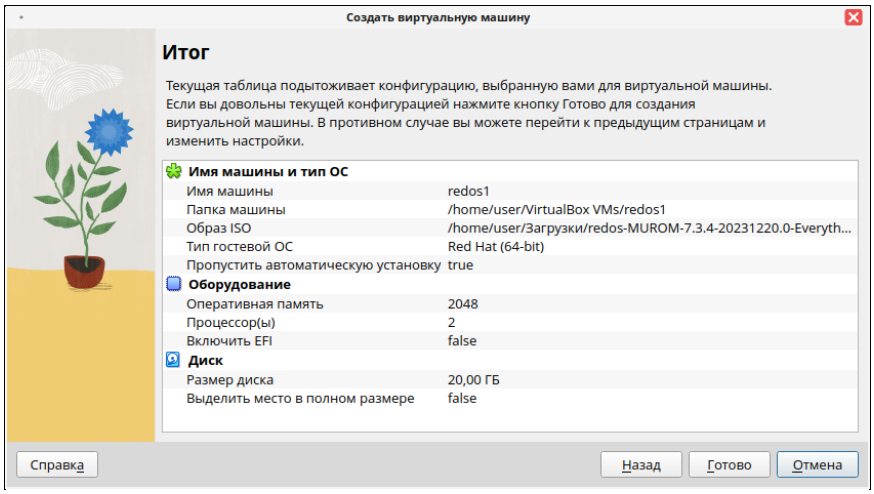
Нажмите «**Далее**».



Создайте новый виртуальный жесткий диск. Объем жесткого диска рекомендуется задать не менее 20 ГБ.



Проверьте параметры ВМ. Если все настроено верно, нажмите «**Готово**». В противном случае нажмите «**Назад**» и внесите необходимые изменения.



На данном этапе процесс создания новой ВМ завершен.

Для тонкой настройки ВМ перед ее запуском нажмите «**Настроить**» () и задайте необходимые параметры будущей системы по своему усмотрению.

Для запуска ВМ нажмите «**Запустить**» ().

Установка РЕД ОС

Установка ОС выполняется так же, как и на обычном ПК.

Определите необходимые настройки для стандартной установки РЕД ОС. Подробную информацию о настройке ОС перед установкой см. в нашей инструкции «Обзор установки».

Настройка виртуальной машины с помощью командной строки

Для создания виртуальной машины и регистрации её в системе выполните команду:

```
vboxmanage createvm --name RedOS --ostype Linux_64 --register
```

Для задания параметров созданной виртуальной машины выполните команду (укажите количество оперативной памяти, число процессоров и необходимые порты):

```
vboxmanage modifyvm RedOS --cpus 1 --memory 2048 --audio none --usb off --acpi on --boot1 dvd --nic1 nat
```

Для запуска виртуальной машины необходимо создать жёсткий и подключить его с помощью следующих команд:

```
vboxmanage created \
--filename /home/user/virtualbox/RedOS/RedOS.vdi \
--size 12000
```

```
VBoxManage storagectl RedOS --name "SATA" --add sata
VBoxManage storagectl RedOS --name "IDE" --add ide
```

```
vboxmanage storageattach RedOS --storagectl "SATA" \
  --port 0 --device 0 --type hdd \
  --medium /home/user/virtualbox/RedOS/RedOS.vdi
```

Для установки виртуальной машины необходимо подключить к виртуальной машине ISO-образ, с которого будет происходить установка:

```
vboxmanage storageattach RedOS --storagectl "IDE" \
  --port 0 --device 1 --type dvddrive \
  --medium /home/user/data/iso/redos-MUROM-7.3-x86_64-DVD1.iso
```

Для запуска виртуальной машины выполните команду:

```
vboxmanage startvm RedOS
```

Экспортировать виртуальную машину можно командой:

```
vboxmanage export RedOS --output RedOS.ova
```

Импортировать виртуальную машину можно командой:

```
vboxmanage import RedOS.ova
```

Автостарт виртуальной машины в VirtualBox при запуске системы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** VirtualBox 6.1.28

Вы можете подробнее рассмотреть автоматический запуск ВМ в VirtualBox, просмотрев наши обучающие видео:

- на **RuTube** — Автостарт виртуальной машины в VirtualBox при запуске системы ;
- в **Яндекс.Дзен** — Автостарт виртуальной машины в VirtualBox при запуске системы ;
- в **VK Видео** — Автостарт виртуальной машины в VirtualBox при запуске системы .

На наших каналах вы также сможете найти много другой полезной информации.

Настройка сервиса автозапуска виртуальной машины

Запустите терминал и выполните команду с привилегиями пользователя root:

```
echo -e "VBOXAUTOSTART_DB=/etc/vbox\nVBOXAUTOSTART_CONFIG=/etc/vbox/autostartvm.cfg" | tee /etc/default/virtualbox
```

VBOXAUTOSTART_DB - определяет абсолютный путь к каталогу базы данных автозапуска, обычно это / etc / vbox.

VBOXAUTOSTART_CONFIG - определяет путь к конфигурации автозапуска виртуальной машины. Настройка конфигурации автостарта, создайте файл.

```
nano /etc/vbox/autostartvm.cfg
```

Содержимое файла (смените **user** - на вашего пользователя):

```
default_policy = deny
user = {allow = true
startup_delay = 10
}
```

- default_policy - определяет, разрешать или запрещать автоматический запуск виртуальной машины по умолчанию. В примере выше мы отказали кому-либо в автоматическом запуске виртуальной машины и явно разрешили одному пользователю user.
- username (user) - с помощью политики запрета по умолчанию вы можете определить конкретных пользователей, которым разрешено автоматически запускать виртуальную машину (allow = trues). Вы также можете определить, как долго задерживать запуск виртуальной машины. 10 секунд используется в этой демонстрации.

Определение владельца директории базы данных автозапуска

Для определения владельца директории базы данных автозапуска выполните следующие команды:

```
usermod -aG vboxusers user
chgrp vboxusers /etc/vbox
```

Назначьте группе разрешения на запись в каталоге базы данных автозапуска:

```
chmod -R 777 /etc/vbox/
```

Как user, вы можете включить автозапуск для отдельных машин. Для этого необходимо сначала определить путь к каталогу базы данных.

```
VBoxManage setproperty autostartdbpath /etc/vbox/
```

Добавление виртуальной машины в автозапуск

```
vboxmanage modifyvm redos --autostart-enabled on
```

где redos - это UUID или имя вашей виртуальной машины.

Далее нужно создать скрипт для автозапуска машины:

```
nano /etc/default/start
```

```
#!/bin/bash
VBoxAutostart --start -c /etc/vbox/autostartvm.cfg
```

Сделайте созданный файл исполняемым:

```
chmod +x /etc/default/start
```

Проверьте, что файл выполняется успешно:

```
/etc/default/start
```

Пример вывода результата команды:

```
Oracle VM VirtualBox Autostart 6.1.16_REDSOFT
(C) 2021 Oracle Corporation
All rights reserved.

00:00:00.000404 main VirtualBox Autostart 6.1.16_REDSOFT r140961 linux.amd64 (Apr 12 2021 17:37:04) release log
00:00:00.000406 main Log opened 2021-05-24T06:54:30.722810000Z
00:00:00.000407 main Build Type: release
00:00:00.000411 main OS Product: Linux
00:00:00.000411 main OS Release: 5.10.29-1.el7.x86_64
00:00:00.000412 main OS Version: #1 SMP Mon Apr 12 13:55:18 MSK 2021
00:00:00.000445 main DMI Product Name: System Product Name
00:00:00.000452 main DMI Product Version: System Version
00:00:00.000457 main Firmware type: UEFI
00:00:00.001190 main Secure Boot: Disabled
00:00:00.001234 main Host RAM: 7826MB (7.6GB) total, 2378MB (2.3GB) available
00:00:00.001238 main Executable: /usr/lib64/virtualbox/VBoxAutostart
00:00:00.001239 main Process ID: 9566
00:00:00.001239 main Package type: LINUX_64BITS_GENERIC (OSE)
00:00:00.002388 main IPC socket path: /tmp/.vbox-wolandius-ipc/ipcd
```

Виртуальная машина должна будет запуститься в virtualbox. Далее создайте сервис, который будет использоваться для автоматического запуска виртуальной машины (смените user — на вашего пользователя):

```
nano /etc/systemd/system/vmsautostart.service
```

```
[Unit]
Description=vms autostart
Before=graphical.target

[Service]
ExecStart=/etc/default/start
Type=oneshot
Gr oup=vboxusers
User=user
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

Предоставьте необходимые права следующей командой:

```
chmod 664 /etc/systemd/system/vmsautostart.service
```

Добавьте сервис в автозагрузку и запустите его:

```
systemctl daemon-reload
systemctl enable vmsautostart.service
```

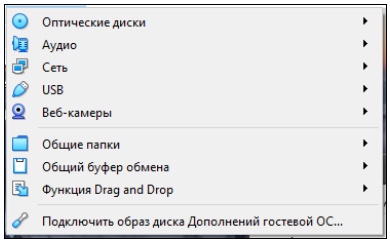
```
systemctl start vmsautostart.service
```

При успешном старте сервиса проверьте virtualbox на наличие работающей машины. При перезагрузке системы машина запустится до ввода пароля пользователя. Для отключения автозапуска виртуальной машины выполните команды:

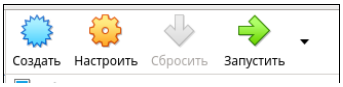
```
vboxmanage modifyvm redos --autostart-enabled off
systemctl disable vmsautostart.service
systemctl stop vmsautostart.service
```

Настройка общей папки в VirtualBox

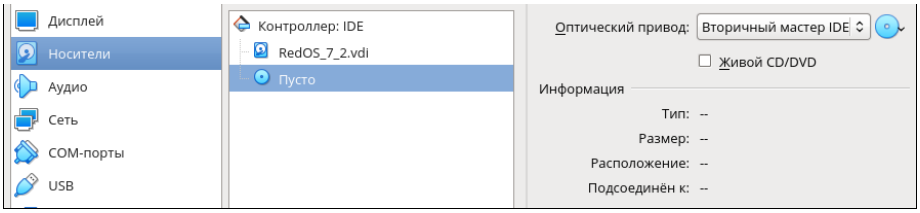
Guest Additions — дополнительное программное обеспечение для виртуальных машин на основе программного обеспечения VirtualBox, которое позволяет вам активировать дополнительные функции, такие как полноэкранный режим, автоматическое расширение окна с помощью системы, совместное использование буфера обмена или перемещение файлов путем перетаскивания. Для установки гостевых дополнений требуется перейти в пункт «Устройства» и выбрать «*Подключить образ диска Дополнений гостевой ОС*»:



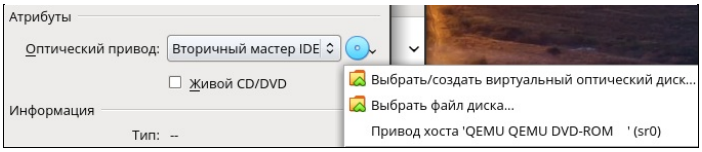
После этого запустится окно автозапуска установки гостевых дополнений. Введите пароль root пользователя и дождитесь завершения установки. По завершении потребуется перезапустить виртуальную машину для работоспособности буфера обмена и дополнений. Если загрузка образа не произошла по умолчанию (иногда актуально, когда в качестве хоста выступает Windows), то вы можете скачать образ гостевых дополнений под вашу версию VirtualBox, перейдите на страницу download.virtualbox.org/virtualbox/, выберите версию VirtualBox и найдите файл под названием, где вместо VERSION указаны ваши числа: *VBoxGuestAdditions_**VERSION**.iso*. После скачивания зайдите в **VirtualBox -> «Настроить» -> «Носители»**.



Выберите пустой образ оптического диска:



В пункте «*Оптический привод*» нажмите на диск и перейдите в « *Выбрать файл диска*», выберите скачанный образ:



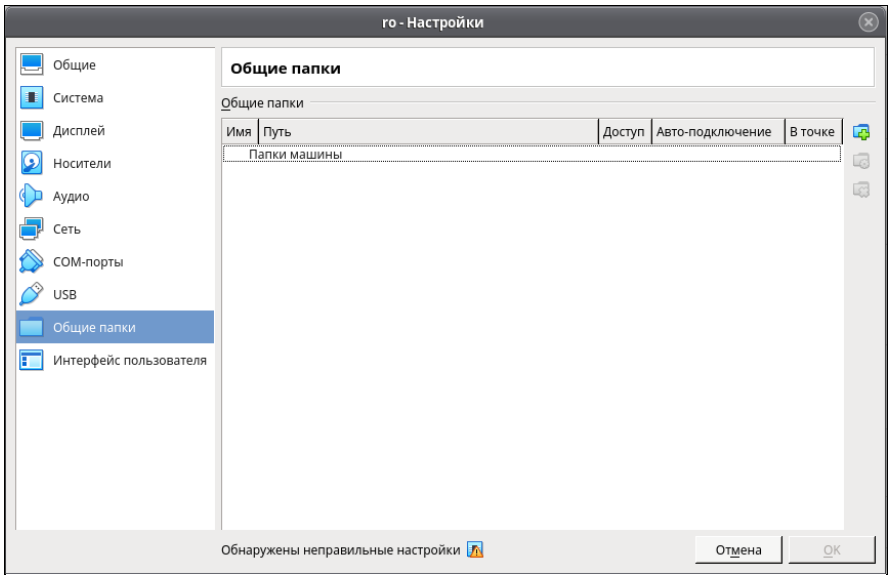
Запустите виртуальную машину и выполните команду (указав версию VirtualBox и имя пользователя):

```
/run/media/user/VBox_GAs_6.1.16/autorun.sh
```

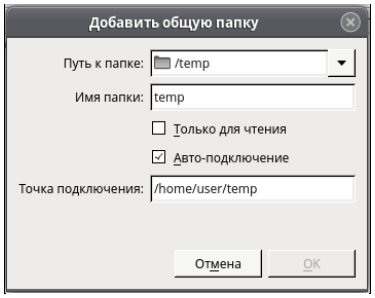
Запустится установка гостевых дополнений, введите пароль root и дождитесь завершения установки. По завершении потребуется перезапустить виртуальную машину для работоспособности буфера обмена и дополнений.

Настройки общей папки, когда в качестве хоста выступает РЕД ОС

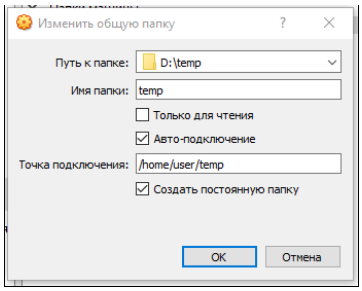
Выберите пункт общие папки для вашей виртуальной машины:



Пропишите путь к папке хоста, укажите авто-подключение, если папка будет часто использоваться. В качестве меры безопасности, чтобы файлы папки хоста не были испорчены пользователем виртуальной машины, можно указать пункт «Только для чтения». Укажите точку подключения, в данную папку будет произведено монтирование общей папки хоста.

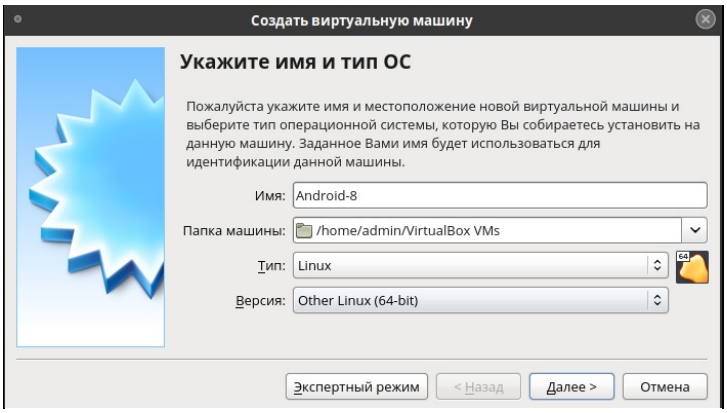


Для добавления общей папки, когда в качестве хоста выступает Windows, требуется воспроизвести абсолютно те же самые действия, что и для РЕД ОС, отличием будет лишь вид **пути к общей папке**:

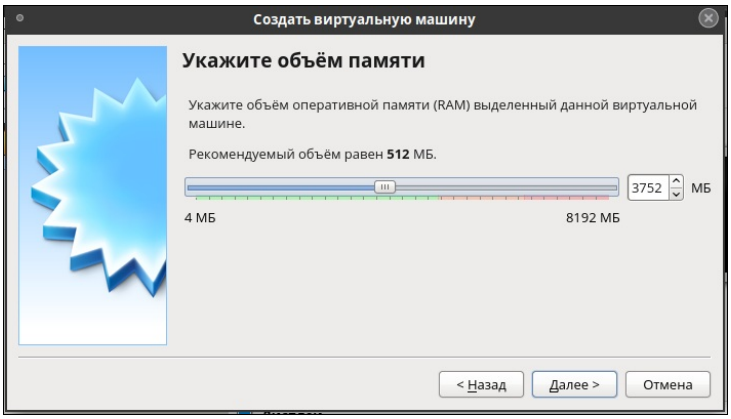


Установка эмулятора Android-x86

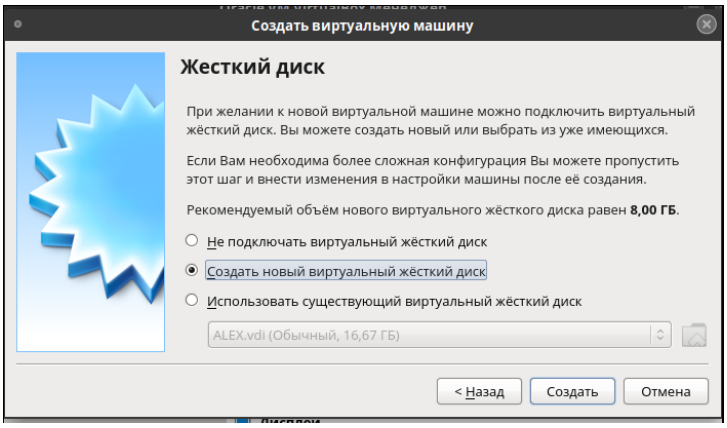
В VirtualBox Менеджере нажмите на кнопку *«Создать»*.
Появится окно, где необходимо указать **Имя**, **Папку машины**, **Тип**, **Версию ОС**.
Имя можно указать любое, остальные параметры представлены на рисунке.



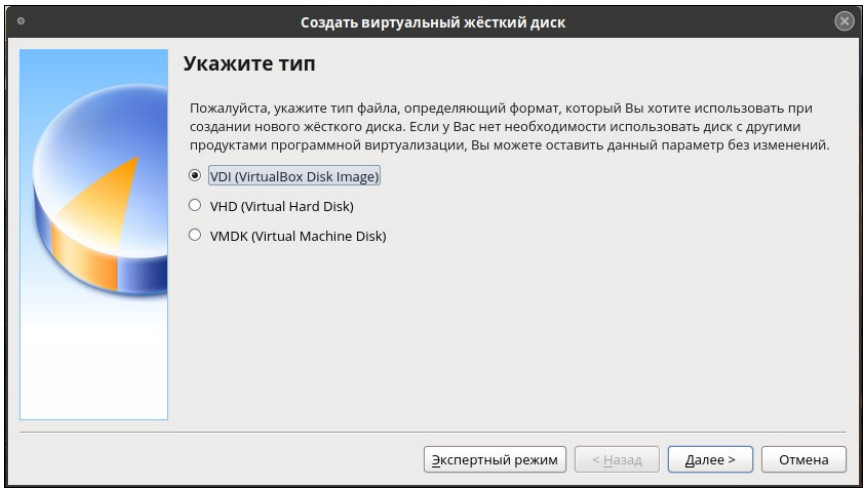
Далее указывается объём опреативной памяти (RAM). Можно установить любой объем памяти, но **не менее 512МБ**.



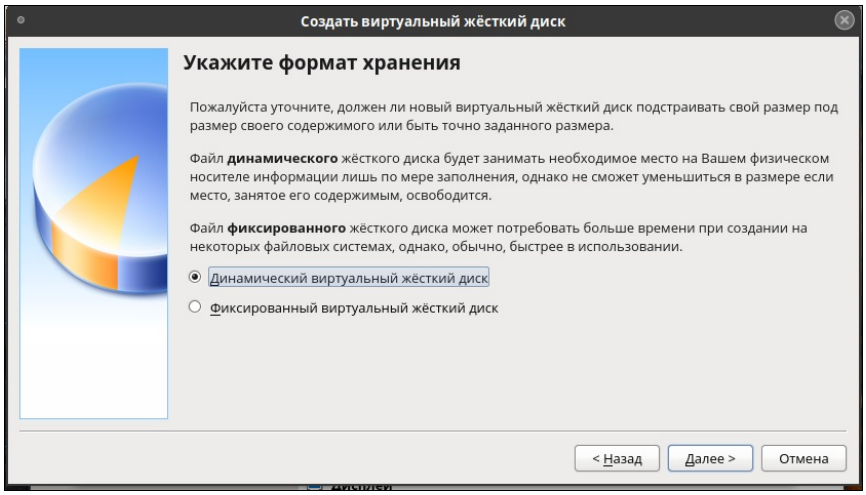
Затем необходимо выбрать пункт *«Создать новый виртуальный жесткий диск»*.



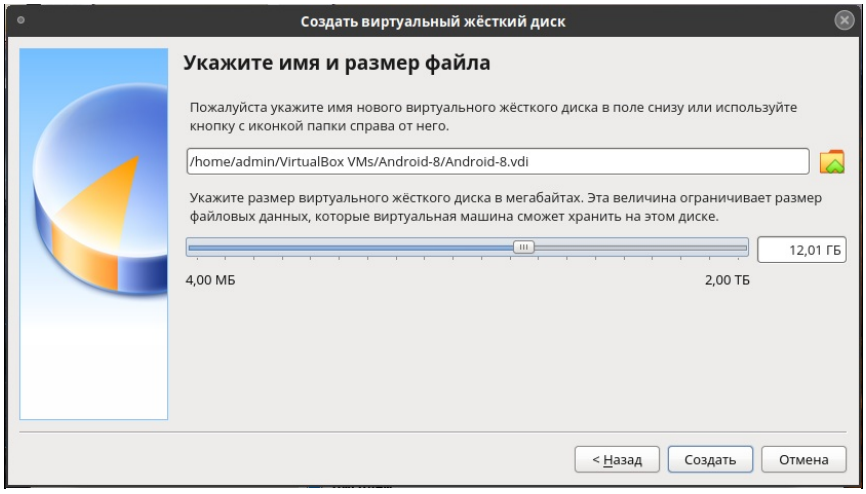
Тип диска установите **VDI**.



Формат хранения выберите *«Динамический виртуальный жесткий диск»*.

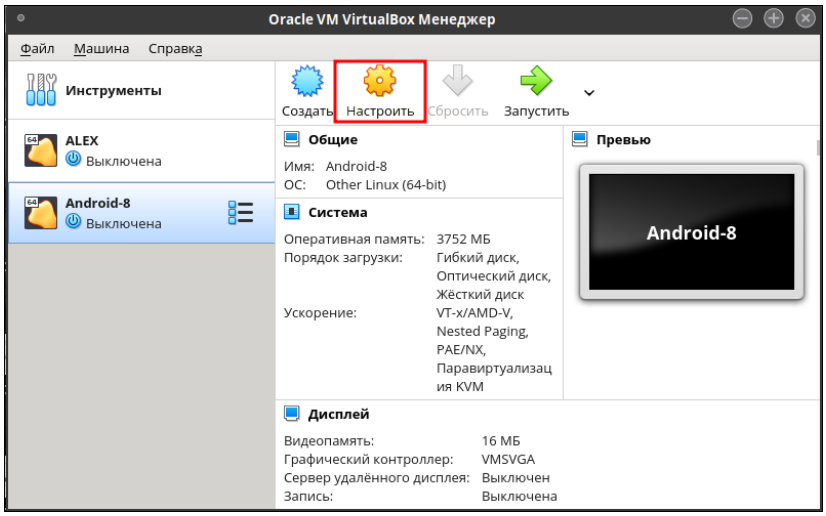


Объем виртуального жесткого диска задайте **не менее 8 ГБ**. Если планируется устанавливать на Андроид приложения, необходимо выделить больше свободного места.

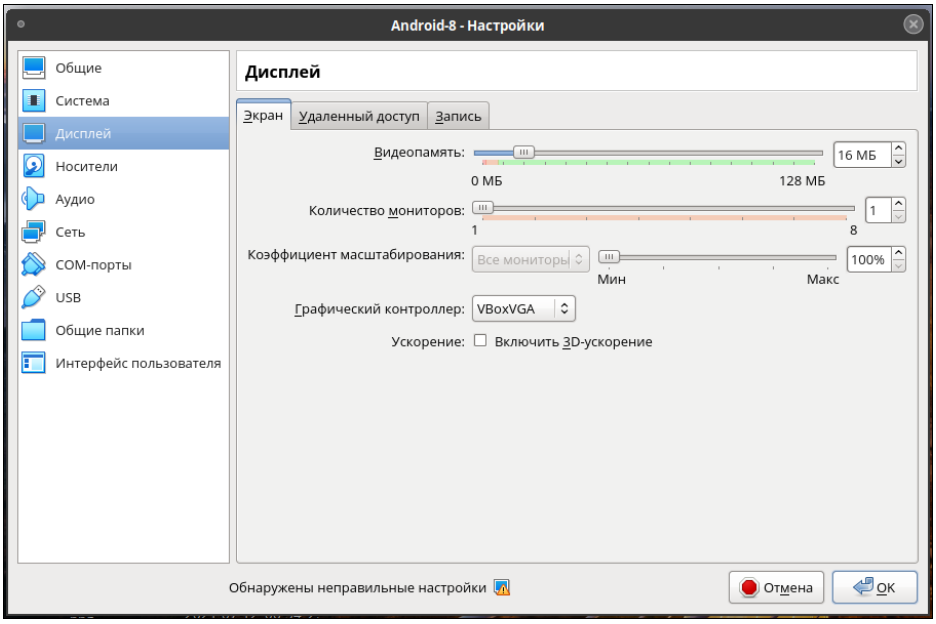


Настройка Android

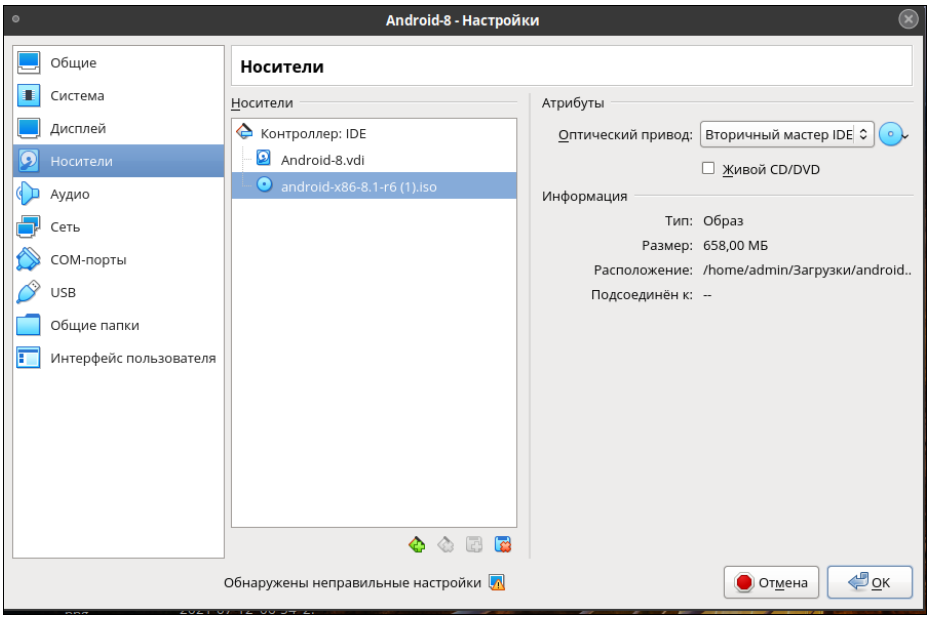
Перед запуском необходимо настроить Android.
Нажмите на кнопку **«Настроить»**.



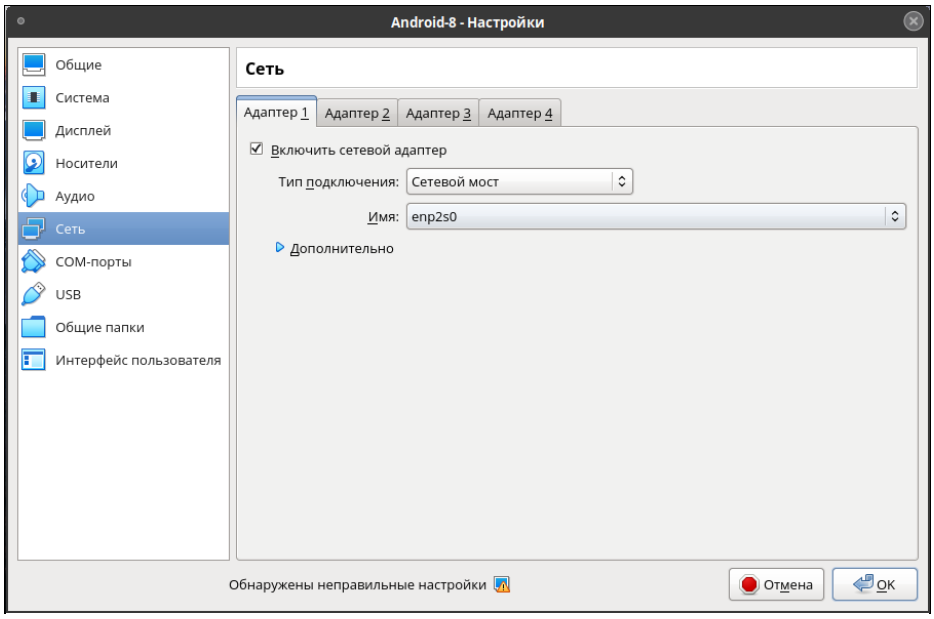
Зайдите в меню **«Система»** - **«Процессор»**, установите 4 ядра процессора и активируйте **PAE/NX**.
Затем перейдите в меню **«Дисплей»**, установите видеопамять **16 МБ** и выберите Графический контроллер **«VboxVGA»**.



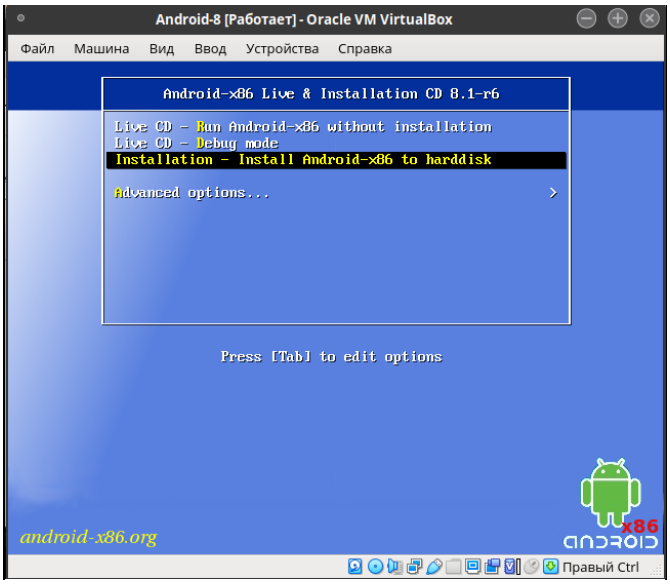
В меню **«Носители»** укажите оптический привод - *iso-файл* андроида.



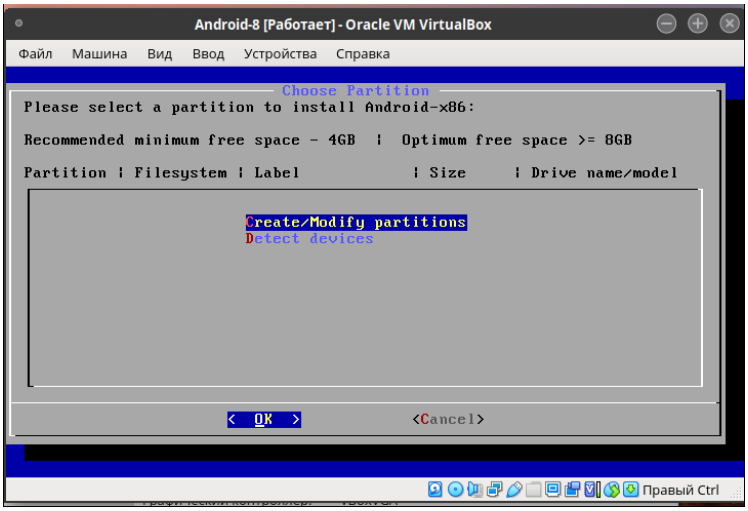
Перейдите в меню «**Сеть**» и выберите Тип подключения **«Сетевой мост»**.



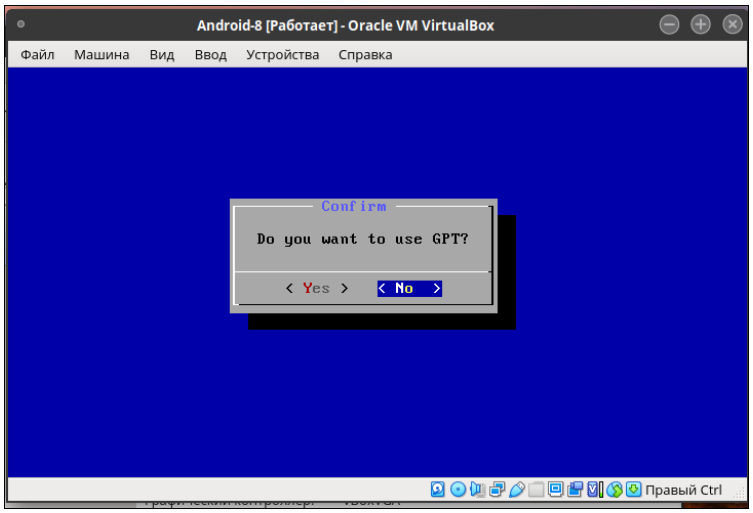
В VirtualBox Менеджере нажмите на кнопку **«Запустить»**.
Откроется boot-меню. Среди доступных способов выберите **«Installation - Install Android-x86 to harddisk»**.



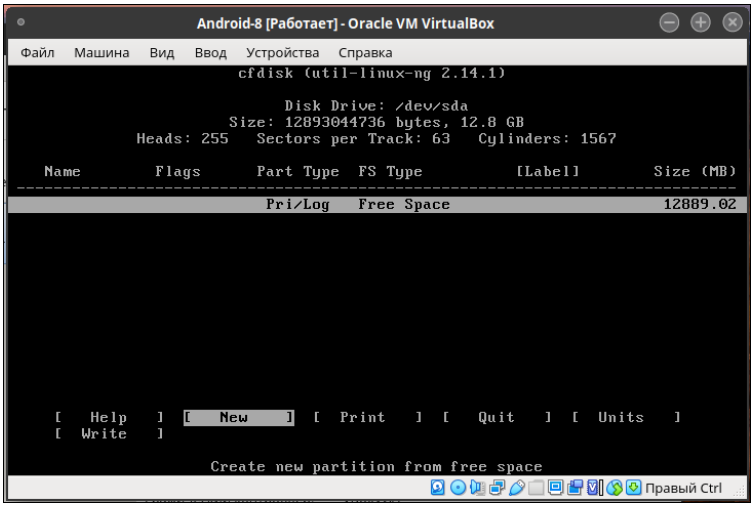
Вам будет предложено выбрать раздел для установки операционной системы. Нажмите на **«Create/Modify partitions»**.



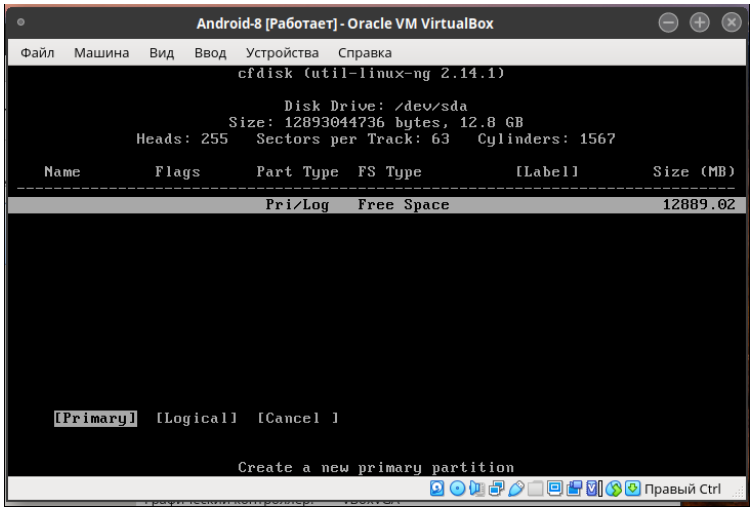
На предложение использовать GPT ответьте **«No»**.



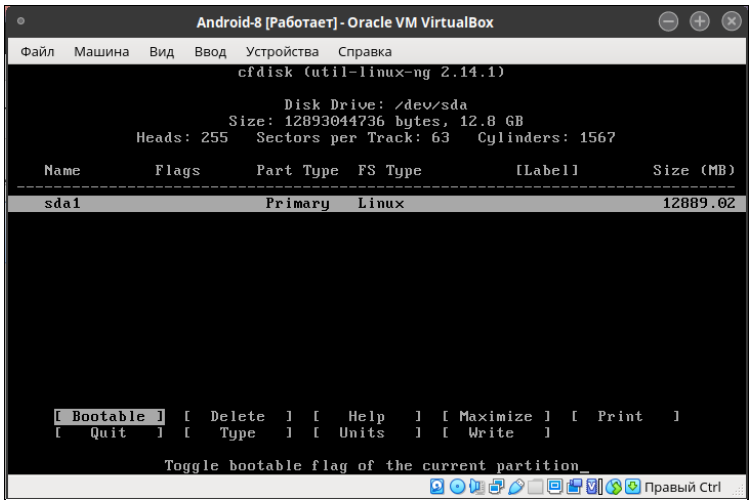
Загрузится утилита **cfdisk**, в которой необходимо будет создать раздел и задать ему некоторые параметры. Выберите **«New»** для создания раздела.



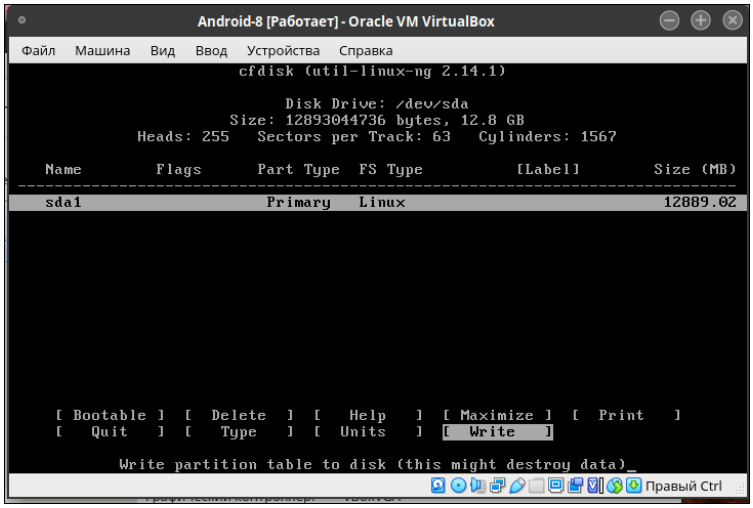
Назначьте раздел главным, выбрав **«Primary»**.



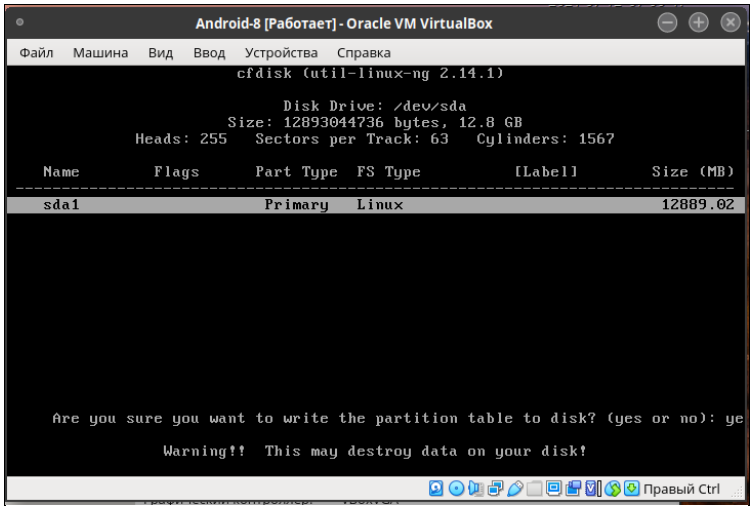
Сделайте раздел загрузочным, задав ему параметр **«Bootable»**.



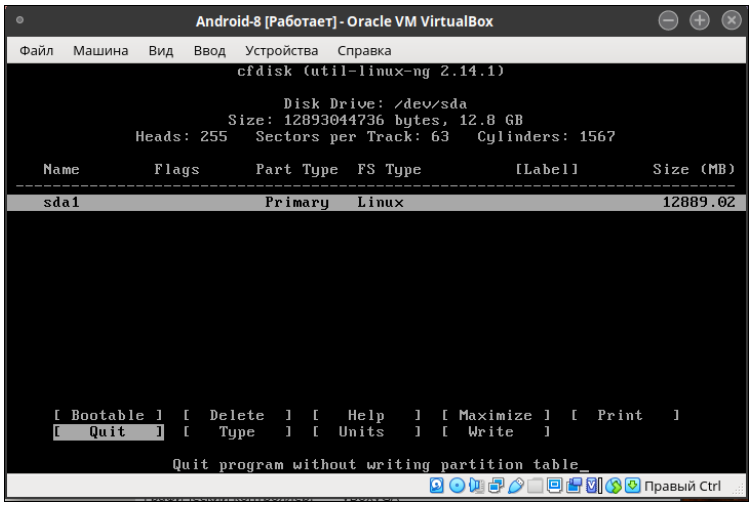
Примените все выбранные параметры, выбрав кнопку **«Write»**.



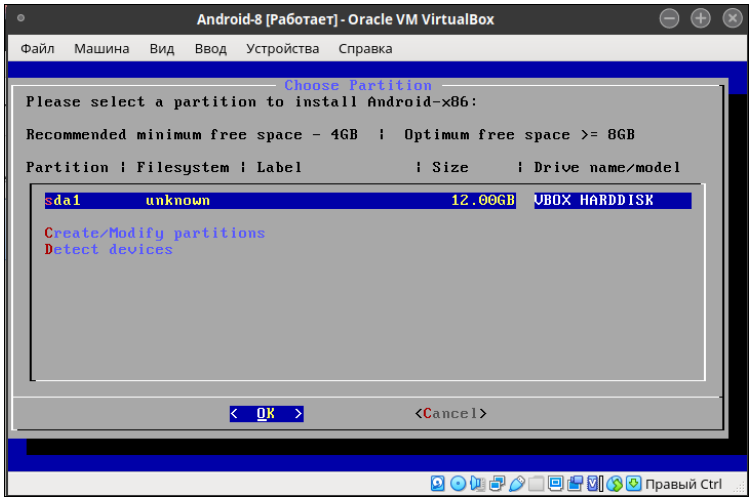
Для подтверждения записи диска необходимо ответить **«yes»** и нажать **Enter**.



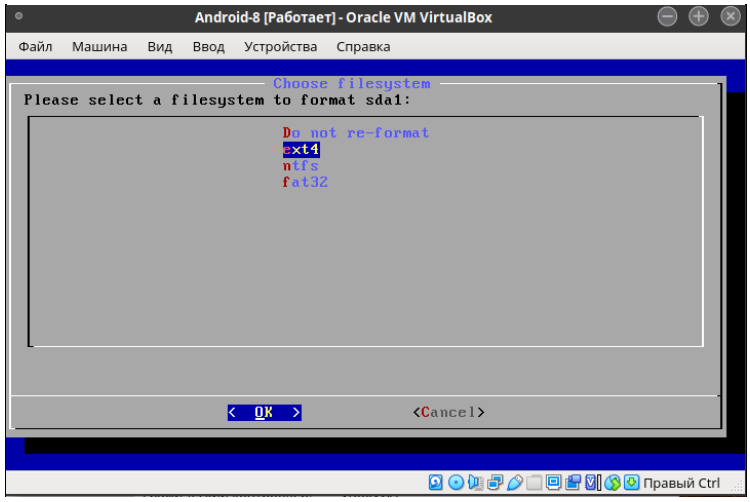
Чтобы выйти из утилиты **cfdisk**, выберите кнопку **«Quit»**.



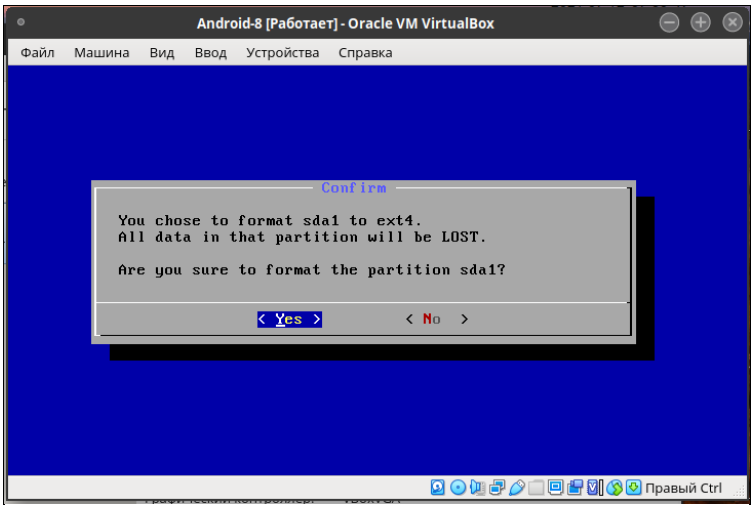
Вы снова попадете в окно установщика. Выберите созданный раздел — на него будет устанавливаться Андроид.



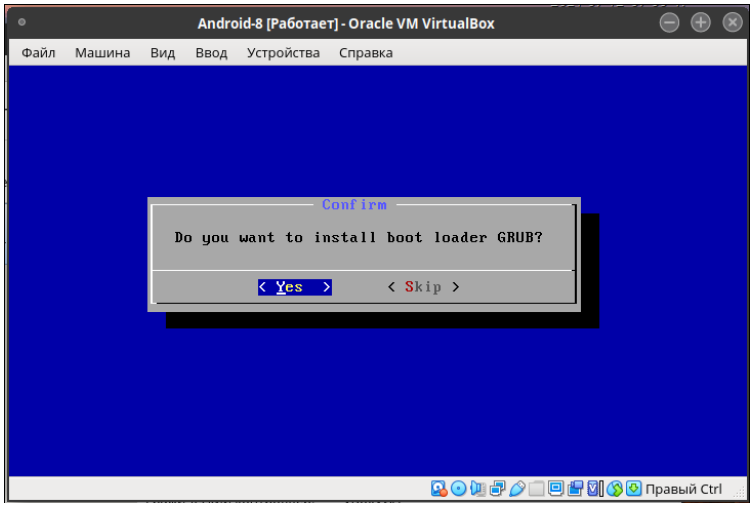
Установите для раздела в файловую систему **«ext4»**.



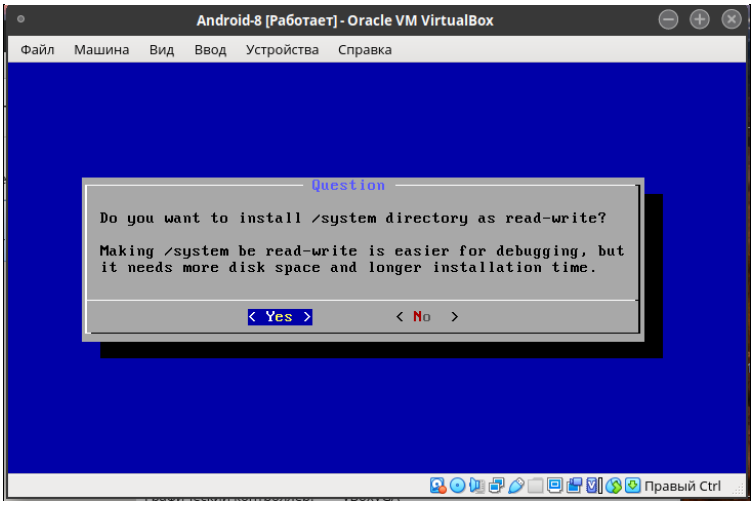
В окне с подтверждением форматирования выберите **«Yes»**.



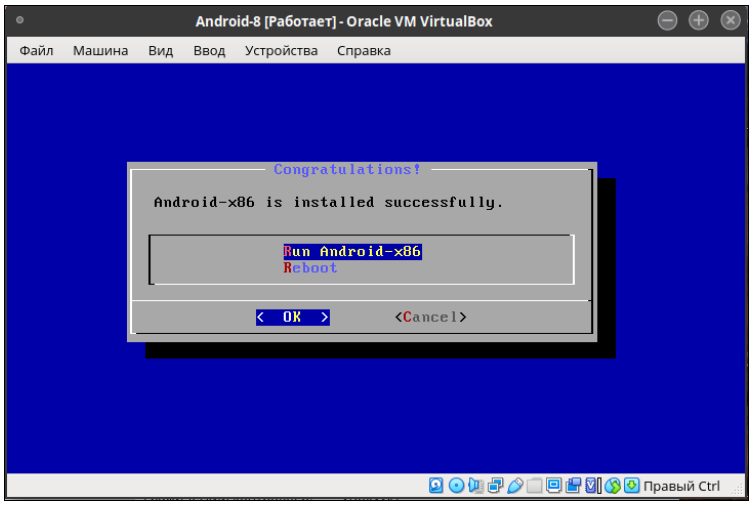
На предложение установить загрузчик GRUB ответьте **«Yes»**.



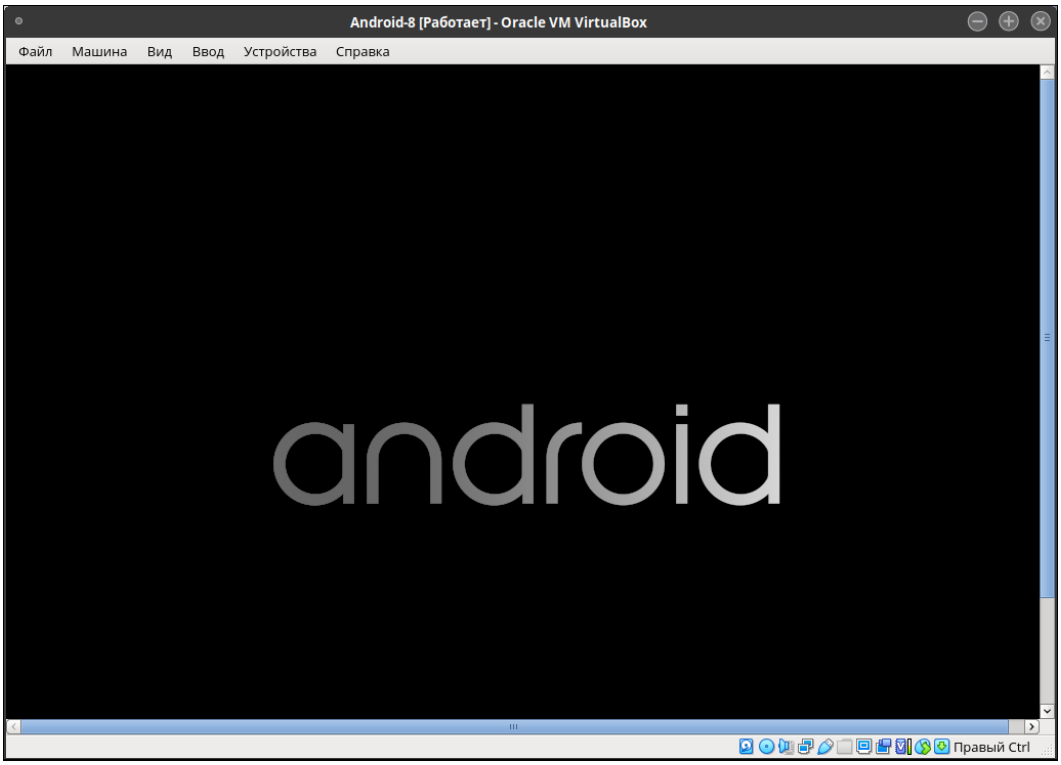
Устанавливаем директорию **\system** доступной для чтения\записи, отвечаем **«Yes»**.



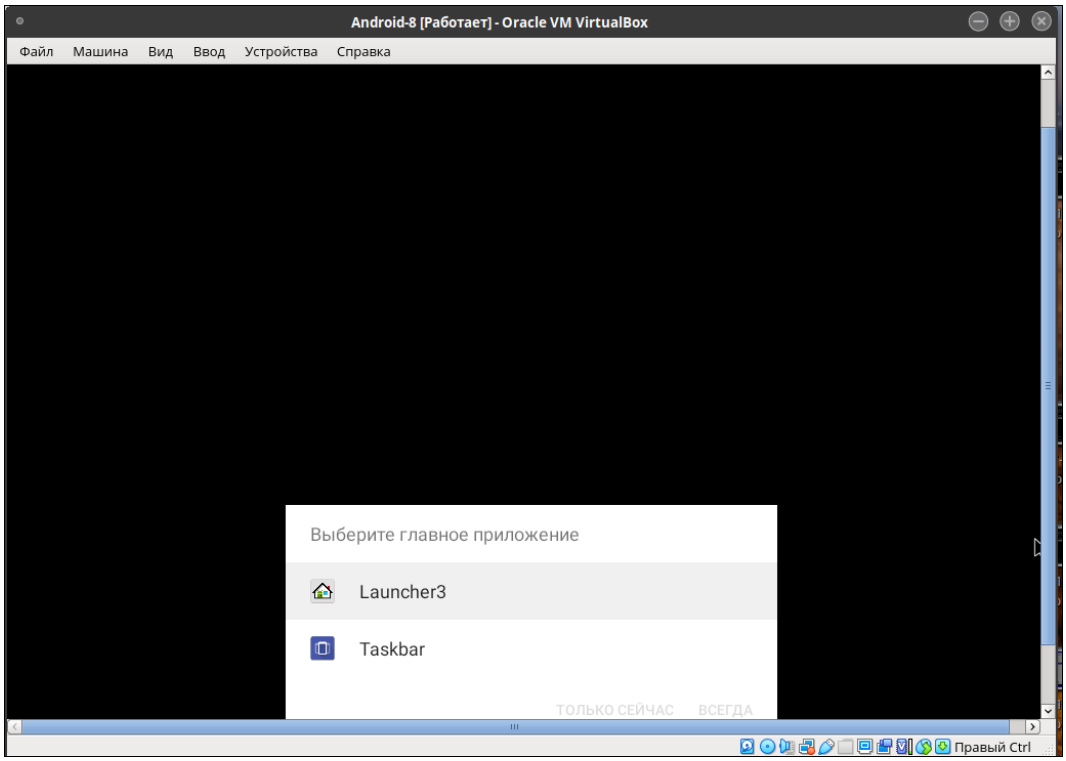
Когда установка будет завершена, будет предложено запустить систему или перезагрузить виртуальную машину. Выберите желаемый пункт.



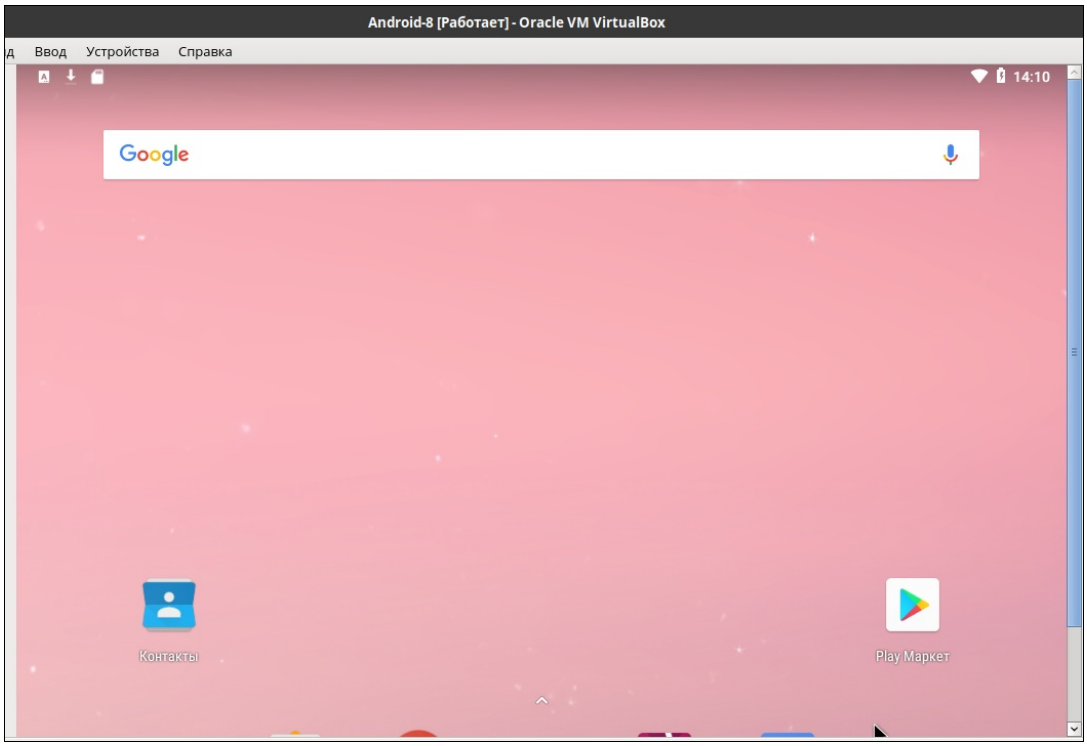
При запуске Android вы увидите фирменный логотип.



Далее систему нужно донастроить: выберите нужный язык, укажите имя пользователя, выполните настройку необходимых параметров и отключите те, которые вам не нужны, затем нажмите кнопку **«Принимаю»**.
Затем в качестве оболочки выбираем **«Launcher3»**.

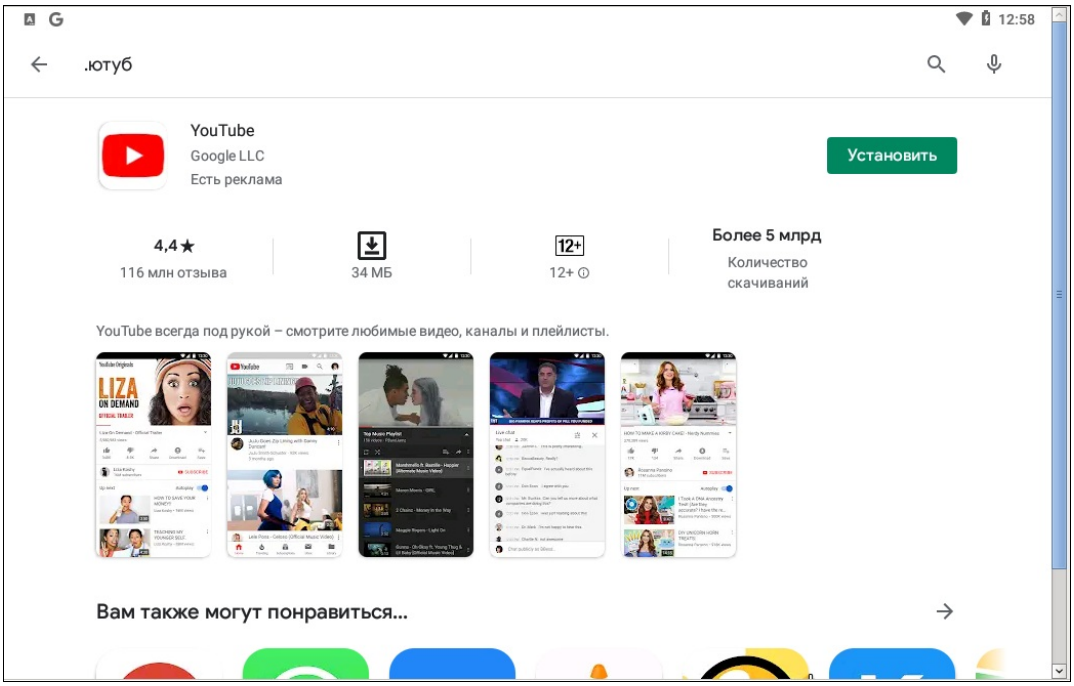


После успешной установки и настройки вы попадете на рабочий стол Android.

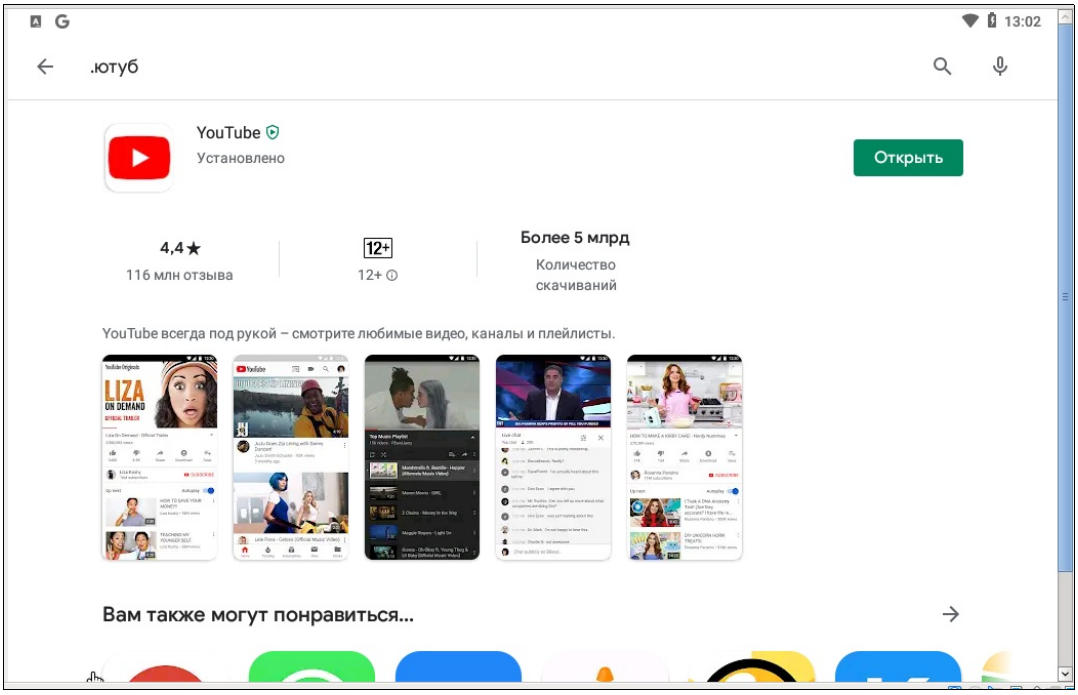


Установка приложения на Android

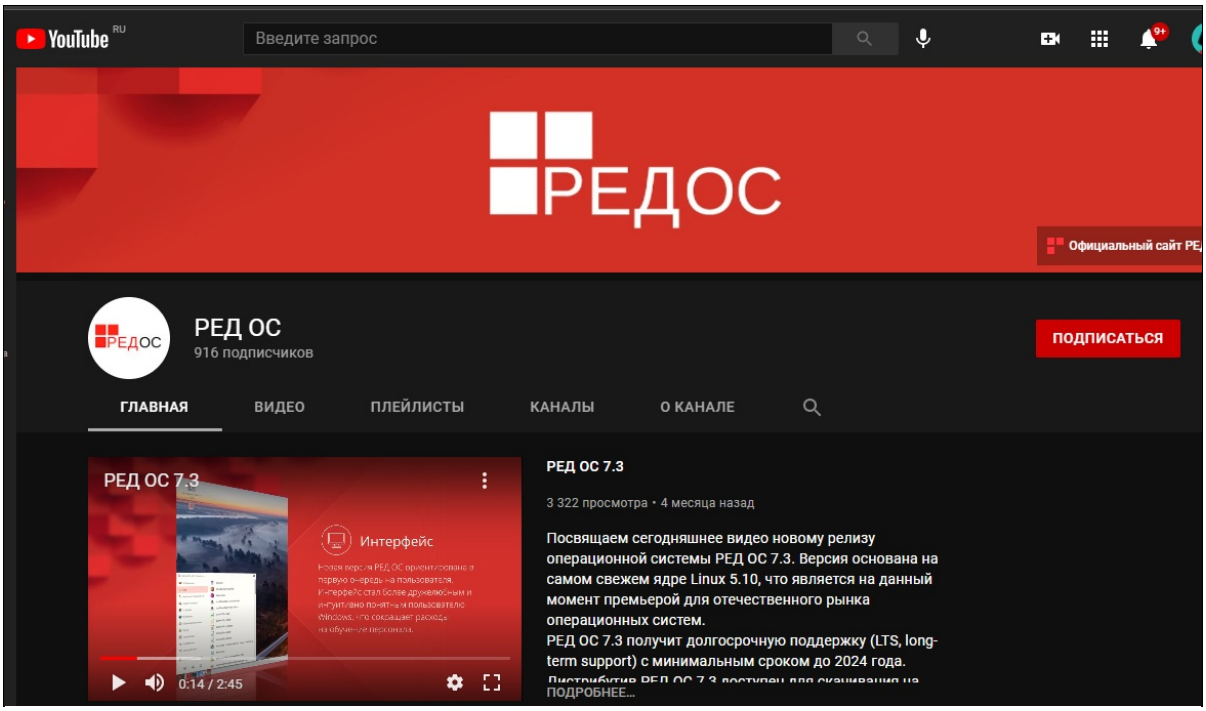
Заходим в *Play Market*, выбираем нужное приложение (для примера взят YouTube), нажимаем **«Установить»**.



После установки приложения нажимаем **«Открыть»**.



Приложение работает корректно.


YouTube RU
Введите запрос
РЕДОС
Официальный сайт РЕ
РЕД ОС
916 подписчиков
ПОДПИСАТЬСЯ
ГЛАВНАЯ
ВИДЕО
ПЛЕЙЛИСТЫ
КАНАЛЫ
О КАНАЛЕ
РЕД ОС 7.3
Интерфейс
0:14 / 2:45
РЕД ОС 7.3
3 322 просмотра • 4 месяца назад
Посвящаем сегодняшнее видео новому релизу операционной системы РЕД ОС 7.3. Версия основана на самом свежем ядре Linux 5.10, что является на данный момент премьерой для отечественного рынка операционных систем.
РЕД ОС 7.3 получит долгосрочную поддержку (LTS, long-term support) с минимальным сроком до 2024 года.
ПОДРОБНЕЕ...

Установка и настройка QEMU-KVM

Предварительная настройка
Установка и начальная настройка
Создание виртуальной машины
Управление ВМ
Управление ВМ через графический менеджер
Управление ВМ с помощью утилиты virsh
Клонирование виртуальных машин
Создание снапшотов
Решение возникающих проблем

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: libvirt-7.6.0-6, qemu-kvm-15:7.2.7-1, virt-manager-4.1.0-1

Виртуализация — предоставление набора вычислительных ресурсов или их логического объединения, независимое от аппаратной реализации и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.

Поддержка виртуализации в РЕД ОС обеспечивается технологией **KVM** (Kernel-based Virtual Machine). Программное обеспечение KVM состоит из загружаемого модуля ядра **kvm.ko**, предоставляющего базовый сервис виртуализации, процессорно-специфического загружаемого модуля **kvm-amd.ko** или **kvm-intel.ko** и компонентов пользовательского режима **QEMU**.

QEMU — средство эмуляции аппаратного обеспечения различных платформ, поддерживающее также аппаратную виртуализацию, основанную на технологии Intel-VT или AMD-V, на процессорах Intel и AMD.

Управление средой виртуализации в РЕД ОС осуществляется посредством набора инструментов **libvirt**, предоставляющего единый API к различным технологиям виртуализации. Главным компонентом сервера виртуализации является служба **libvirtd**.

Менеджер виртуальных машин **virt-manager** предоставляет графический интерфейс для доступа к гипервизорам и виртуальным машинам как в локальной, так и в удаленных системах.

Дополнительную информацию о настройке и работе с QEMU см. в **Руководстве администратора РЕД ОС**.

Вы можете подробнее ознакомиться с работой **QEMU**, просмотрев наши обучающие видео:

- на **RuTube** — Установка и настройка QEMU-KVM;
- в **Яндекс.Дзен** — Установка и настройка QEMU-KVM;
- в **VK Видео** — Установка и настройка QEMU-KVM.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная настройка

Сначала необходимо проверить, поддерживает ли ваш процессор аппаратную виртуализацию. Проверка осуществляется командой:

```
egrep '(vmx|svm)' /proc/cpuinfo

flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc aperfmperf eagerfpu pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm epb retpoline kaiser tpr_shadow vnmi flexpriority ept vpid fsgsbase smep erms xsaveopt dtherm ida arat pln pts
```

Если вывод команды не пуст, значит процессор поддерживает аппаратную виртуализацию.

В случае если у команды пустой вывод, возможно, процессор не поддерживает виртуализацию либо функция отключена в BIOS материнской платы.

После проверки можно приступать к развертыванию средства виртуализации.

Установка и начальная настройка

Для установки пакетов сервера виртуализации **libvirt** выполните команду:

```
dnf install libvirt qemu-kvm virt-install virt-manager openssh-askpass OVMF boost-random boost-program-options boost-regex
```

Затем запустите и добавьте в автозагрузку службу сервера **libvirtd**:

```
systemctl enable libvirtd --now
```

Проверьте статус службы сервера **libvirtd**:

```
systemctl status libvirtd
```

В статусе должно быть указано **active (running)**.

Перезагрузите компьютер для загрузки модулей ядра **kvm** (если используется процессор Intel, также должен загрузиться модуль **intel-kvm**).

После перезагрузки проверьте загрузку модулей.

```
lsmod | grep kvm

kvm_intel   196608   3
kvm         598016   1    kvm_intel
```

Дополнительно рекомендуется проверить сетевые подключения:

```
ifconfig
```

Должно появиться дополнительное подключение **virbr0**.

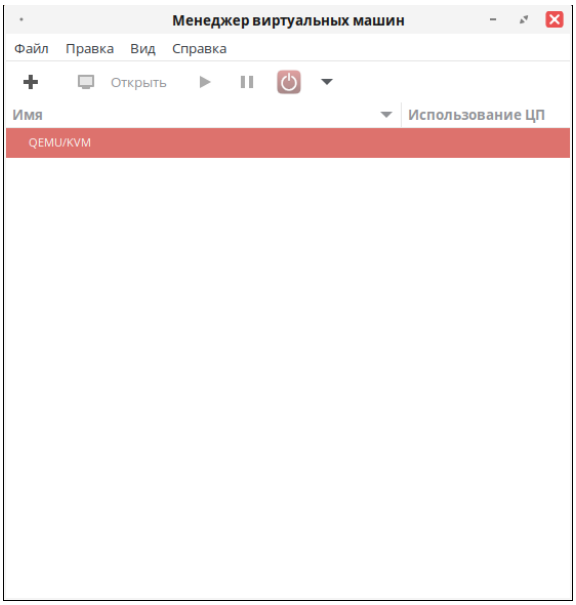
Добавьте пользователя (в примере **user**), используемого для управления виртуальными машинами, в группу **libvirt**.

```
usermod -a -G libvirt user
```

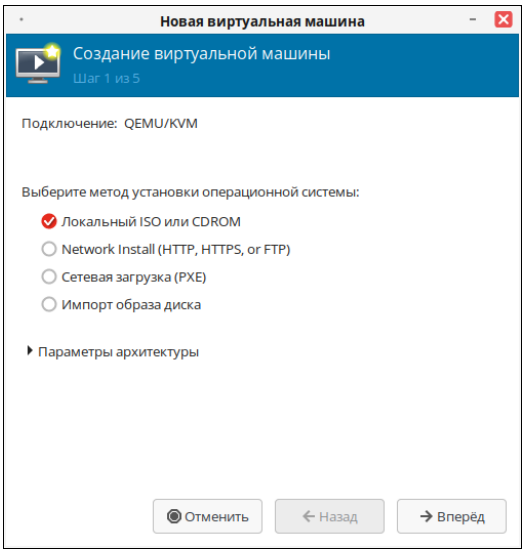
На этом установка и начальная настройка завершены.

Создание виртуальной машины

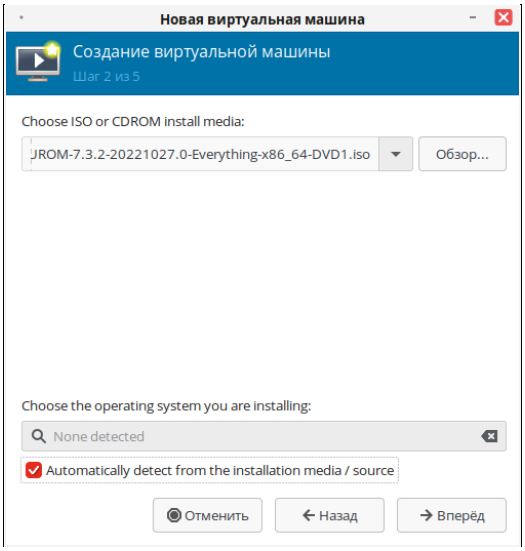
Для создания виртуальной машины можно воспользоваться графической утилитой **virt-manager**. Запуск утилиты доступен из «**Главного меню**» — «**Системные**» — «**Менеджер виртуальных машин**».



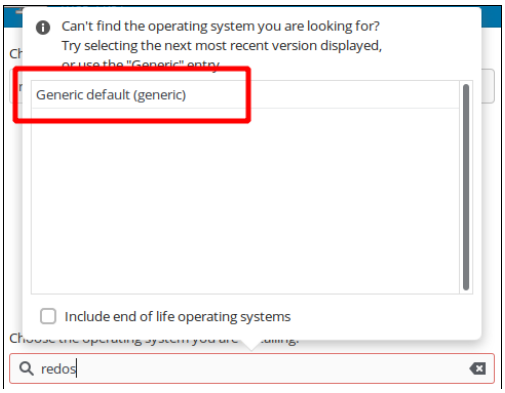
В меню **Файл** выберите **Создать виртуальную машину**. В открывшемся окне выберите метод, с помощью которого будет производиться установка операционной системы. В примере, установка производится из образа **iso**. Нажмите **Вперед**.



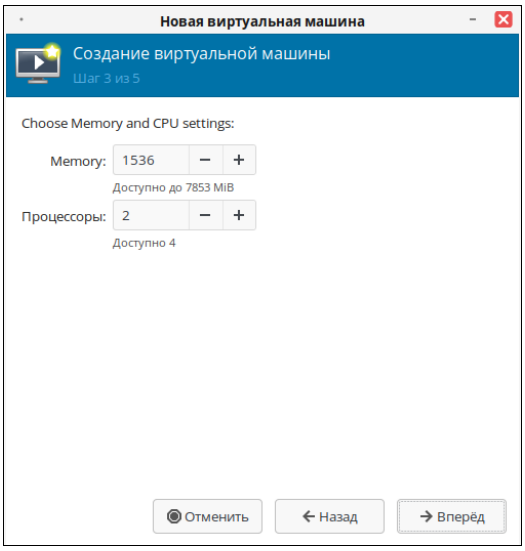
Далее необходимо указать путь к ISO-образу устанавливаемой системы, нажав кнопку «**Обзор...**».



Снимите флаг в поле «**Automatically detect from the installation media/source**» и в строке выбора типа ОС начните вводить ее название (в примере **redos**), будет выведен список доступных ОС, из которых потребуется выбрать нужную систему. Если нужной ОС нет в списке, выберите стандартную конфигурацию — **Generic**.

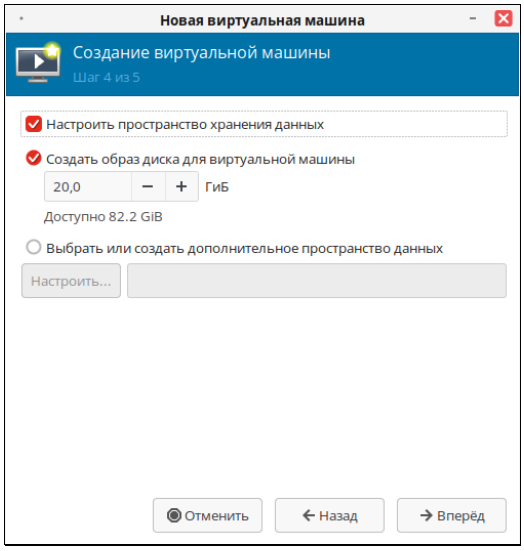


Определите оптимальное количество ОЗУ и процессоров, исходя из доступных данных. Виртуальной машине понадобится достаточный для ее работы объем оперативной памяти (как минимум 512 Мбайт). Стоит помнить, что ВМ используют физическую память. Выполнение слишком большого числа гостевых ОС или предоставление ОС недостаточного объема памяти может привести к повышенному использованию виртуальной памяти и области подкачки.



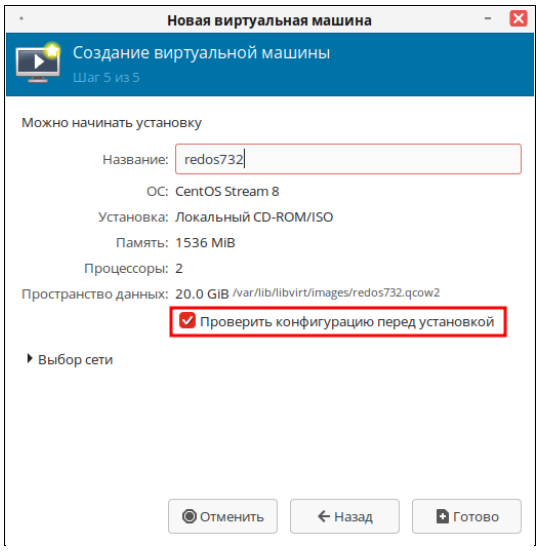
Далее необходимо настроить хранилище данных. Объем хранилища должен превышать минимально необходимый объем памяти, требуемый для установки системы. Минимально рекомендуемым объемом для РЕД ОС является **20 ГБ**.

Также, при желании, можно выделить дополнительное пространство для гостевой ОС.

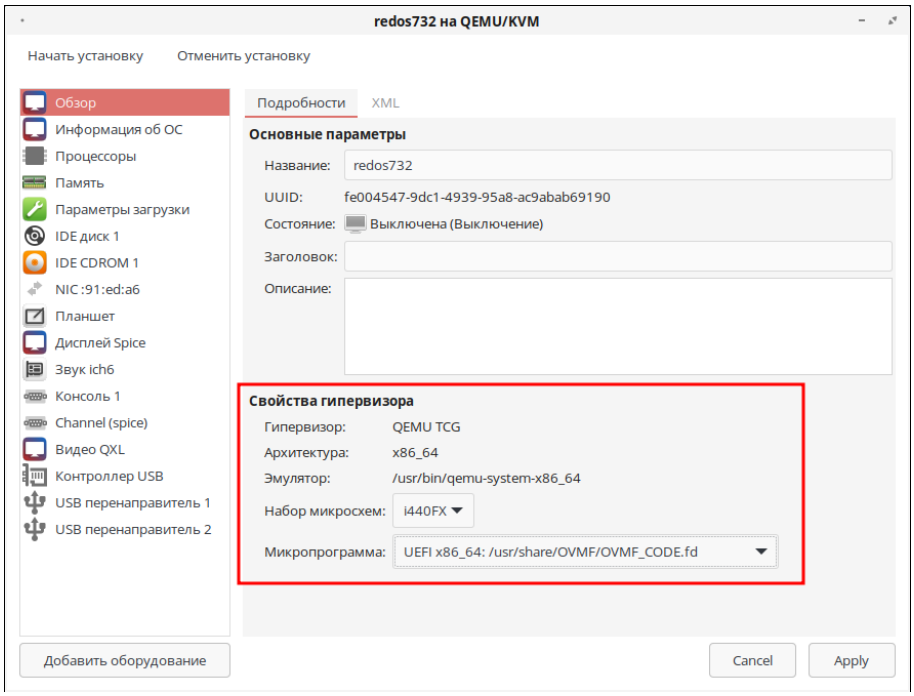


Проверьте правильность всех настроенных параметров. Если необходимо внести изменения, нажмите кнопку «**Назад**». Установите флаг в пункте «**Проверить конфигурацию перед установкой**».

Настройте сеть, если необходимо. Если все настроено верно, нажмите кнопку «**Готово**».

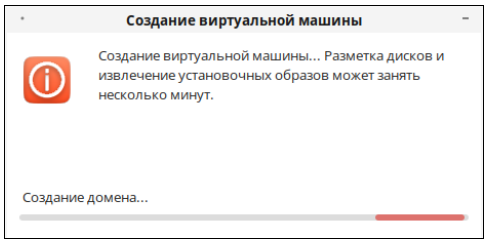


Будут открыты параметры виртуальной машины, где можно будет произвести дополнительные настройки. В свойствах гипервизора доступен выбор загрузчика системы — BIOS или UEFI. Для применения изменений нажмите «**Применить**».

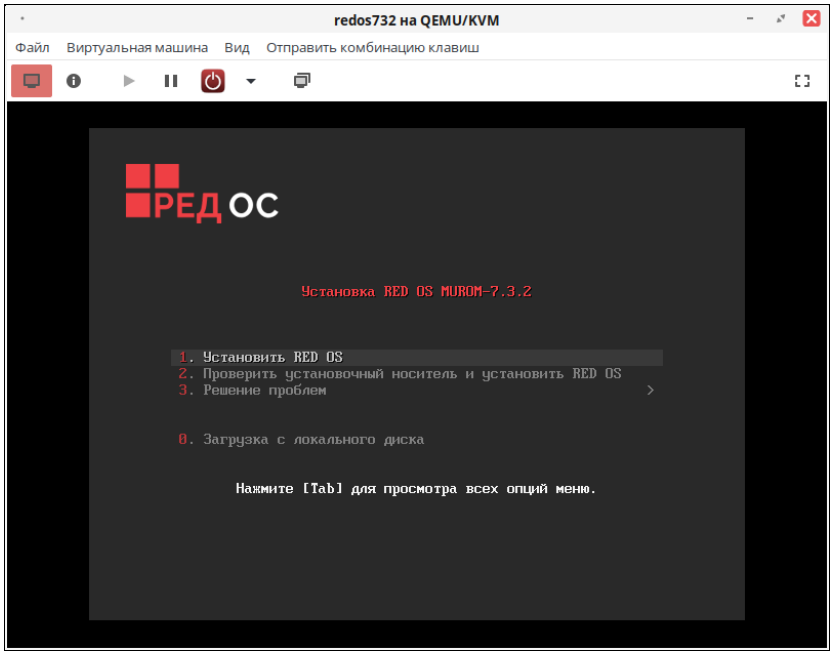


Если все необходимые настройки заданы, нажмите «**Начать установку**» в верхнем левом углу окна.

Будет запущен процесс создания ВМ.



После успешного создания ВМ будет открыта консоль, в которой можно приступить к стандартной установке ОС.



Управление ВМ

Под управлением ВМ подразумеваются такие действия, как:

- мониторинг состояния и ресурсов ВМ;
- управление питанием ВМ;
- создание снимков гостевой системы.

Управление ВМ через графический менеджер

Менеджер **virt-manager** предоставляет графический интерфейс для доступа к гипервизорам и виртуальным машинам в локальной и удаленных системах.

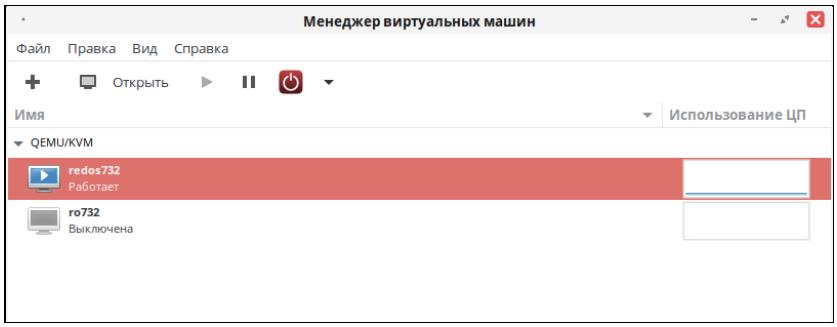
Кроме того, **virt-manager** выполняет управляющие функции:

- выделение памяти;
- выделение виртуальных процессоров;
- мониторинг производительности;
- сохранение и восстановление, приостановка и возобновление работы, запуск и завершение работы виртуальных машин;
- доступ к текстовой и графической консоли.

Просмотр информации о гостевой системе

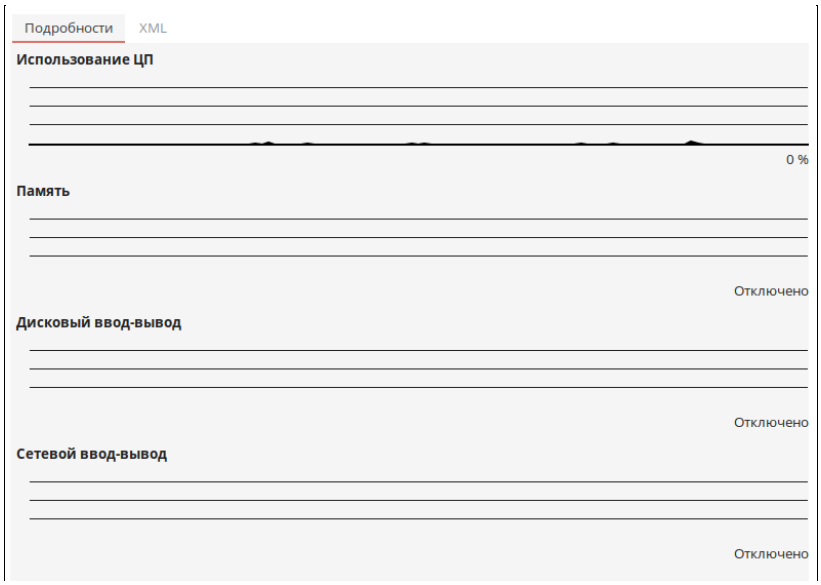
С помощью менеджера виртуальных машин можно получить доступ к подробной информации обо всех виртуальных машинах. Для этого выполните следующий алгоритм действий:

1. В главном окне менеджера выберите виртуальную машину.



2. В пункте меню «**Правка**» выберите «**Свойства виртуальной машины**» или дважды нажмите ЛКМ по имени ВМ.

Будет выведено окно с подробными сведениями о виртуальной машине, на вкладке «**Производительность**» будет доступна информация об использовании ресурсов процессора и памяти.

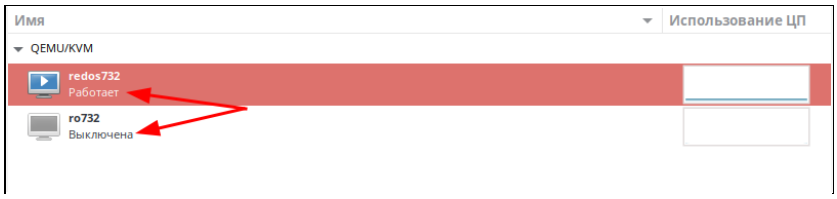


Просмотр состояния виртуальной машины

Состояния ВМ отображаются в главном окне менеджера в списке созданных ВМ под их названием.

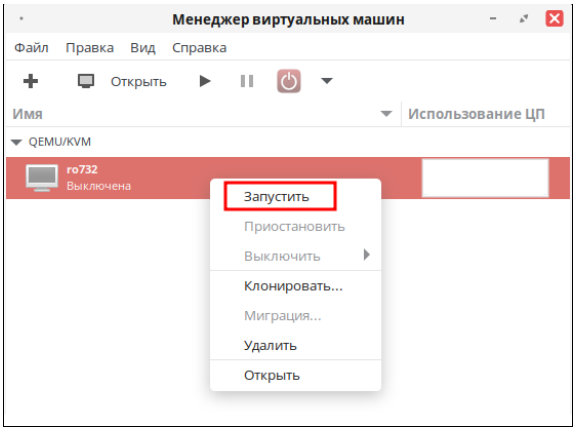
Состояния могут принимать следующие значения:

- работает;
- выключена;
- пауза;
- сохранено.



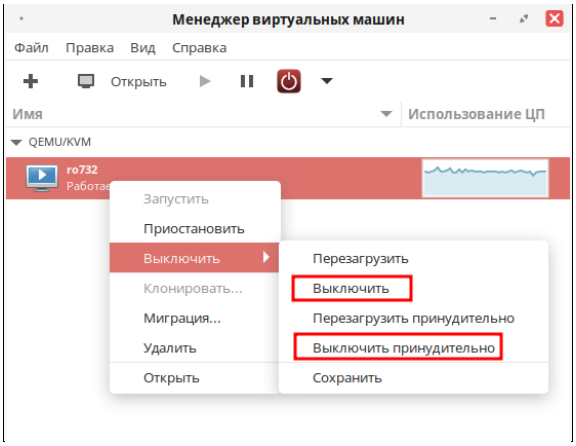
Запуск ВМ

Для запуска ВМ выберите ее в списке, нажмите ПКМ и выберите «**Запустить**».



Выключение ВМ

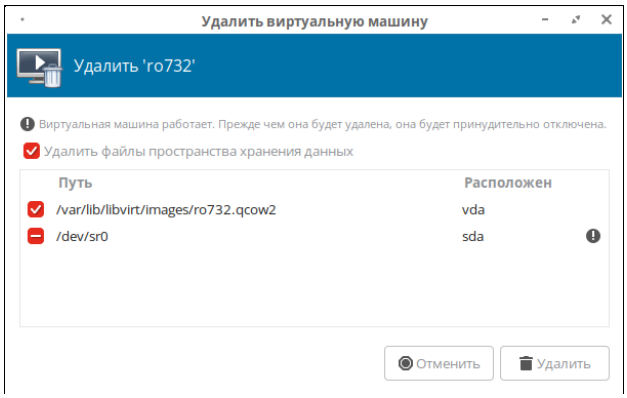
Для выключения ВМ выберите ее в списке, нажмите ПКМ и выберите «**Выключить**» — «**Выключить**» или «**Выключить**» — «**Выключить принудительно**».



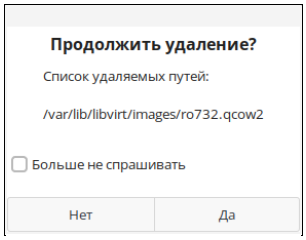
Удаление ВМ

Для удаления ВМ в менеджере необходимо выбрать нужную ВМ и нажать ПКМ по ее имени. В открывшемся контекстном меню выберите «**Удалить**».

Далее потребуется указать необходимость удаления пространства хранения данных. После определения всех настроек нажмите «**Удалить**».



Подтвердите удаление ВМ и всех ее данных.



После этого выбранная ВМ будет полностью удалена.

Управление ВМ с помощью утилиты virsh

Просмотр списка виртуальных машин ВМ

Для просмотра списка виртуальных машин и их состояния выполните:

```
virsh list
```

Можно добавить аргументы:

- `--inactive` — покажет список неактивных доменов (неактивным считается тот домен, который был определен, но в настоящий момент не является активным).
- `--all` — покажет все виртуальные машины независимо от их состояния.

Например:

```
 virsh list --all

ID    Имя       Состояние
----------------------------
1     ro732     работает
-     redos732  выключен
```

Столбец «**Состояние**» может содержать следующие значения:

- `работает` — работающие виртуальные машины, т.е. те машины, которые используют ресурсы процессора в момент выполнения команды;
- `заблокирован` — заблокированные, неработающие машины. Такой статус может быть вызван ожиданием ввода/вывода или пребыванием машины в спящем режиме;
- `приостановлен` — приостановленные домены. Данное состояние наступает, когда администратор нажал кнопку паузы в окне менеджера виртуальных машин или выполнил команду virsh suspend. В приостановленном состоянии гостевая ОС продолжает потреблять ресурсы, но не может занимать больше процессорных ресурсов;
- `выключен` — виртуальные машины, завершающие свою работу. При получении виртуальной машиной сигнала завершения работы, она начнет завершать все процессы. Стоит отметить, что некоторые операционные системы не отвечают на такие сигналы.

Запуск ВМ

Для запуска ВМ выполните команду вида:

```
virsh start <ID_домена, имя_домена, UUID_домена>
```

Приостановка ВМ

Для приостановки ВМ выполните команду вида:

```
virsh suspend <ID_домена, имя_домена, UUID_домена>
```

В этом состоянии виртуальная машина все еще продолжает использовать системную память, но освобождает ресурсы процессора. Операции ввода и вывода приостанавливаются. Работа виртуальной машины может быть возобновлена с помощью команды `resume`.

Возобновление работы ВМ

Для возобновления работы ВМ выполните команду вида:

```
virsh resume <ID_домена, имя_домена, UUID_домена>
```

Работа машины будет возобновлена немедленно.

Сохранение состояния ВМ

Для сохранения текущего состояния ВМ выполните команду:

```
virsh save <ID_домена, имя_домена, UUID_домена> <файл>
```

В результате выполнения данной команды виртуальная машина будет остановлена, а ее данные будут сохранены в заданный файл (это может занять некоторое время в зависимости от доступного гостевой ОС объема памяти). Состояние может быть позднее восстановлено с помощью команды `restore`.

Восстановление виртуальной машины

Чтобы восстановить виртуальную машину, ранее сохраненную с помощью команды `virsh save`, выполните команду:

```
virsh restore <файл>
```

Сохраненная машина будет восстановлена из файла и перезапущена, что может занять некоторое время. Имя и идентификатор **UUID** виртуальной машины останутся неизменными, но будет предоставлен новый идентификатор домена.

Завершение работы виртуальной машины

Для завершения работы ВМ выполните:

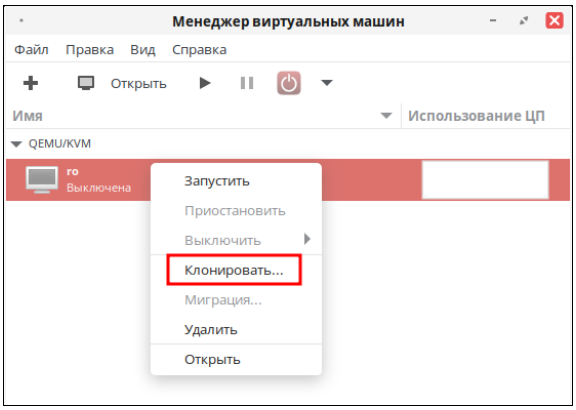
```
virsh shutdown <ID_домена, имя_домена, UUID_домена>
```

Поведение выключаемой гостевой ОС можно контролировать с помощью параметра `on_shutdown` в ее файле конфигурации.

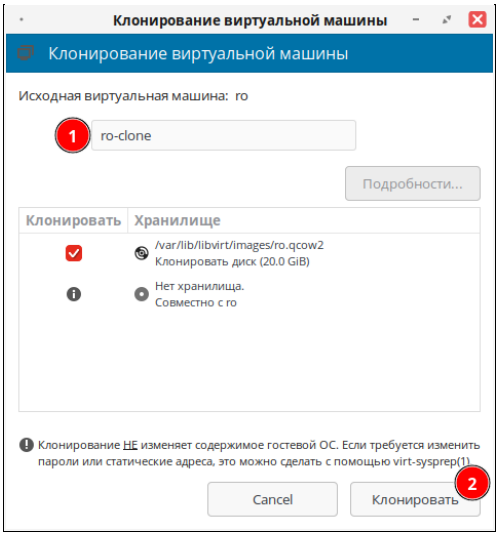
Клонирование виртуальных машин

Клонирование ВМ представляет собой процесс создания точной копии существующей ВМ. Этот метод устраняет необходимость ручной настройки каждой новой виртуальной машины, экономя значительное время и усилия системных администраторов. Клонирование может использоваться для различных целей, включая создание резервных копий, настройку тестовых сред, развертывание нескольких экземпляров одной и той же системы и облегчение разработки и тестирования программного обеспечения.

Для клонирования настроенной ВМ необходимо ее предварительно выключить. После этого в графическом менеджере виртуальных машин выберите необходимую ВМ и вызовите контекстное меню, нажав ПКМ по выбранном ВМ. В появившемся меню выберите «**Клонировать...**».



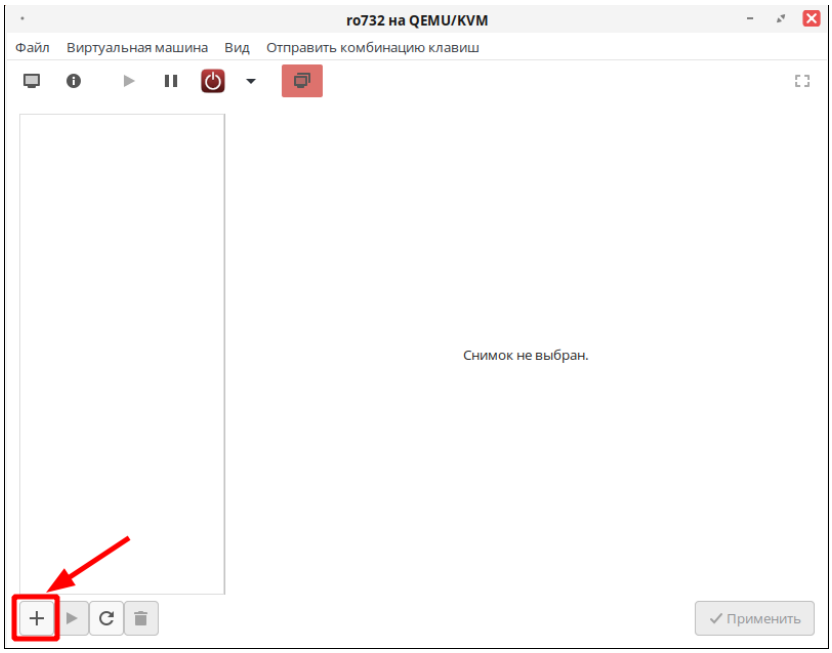
Укажите название новой ВМ и выберите клонируемое хранилище данных. Нажмите «**Клонировать**».



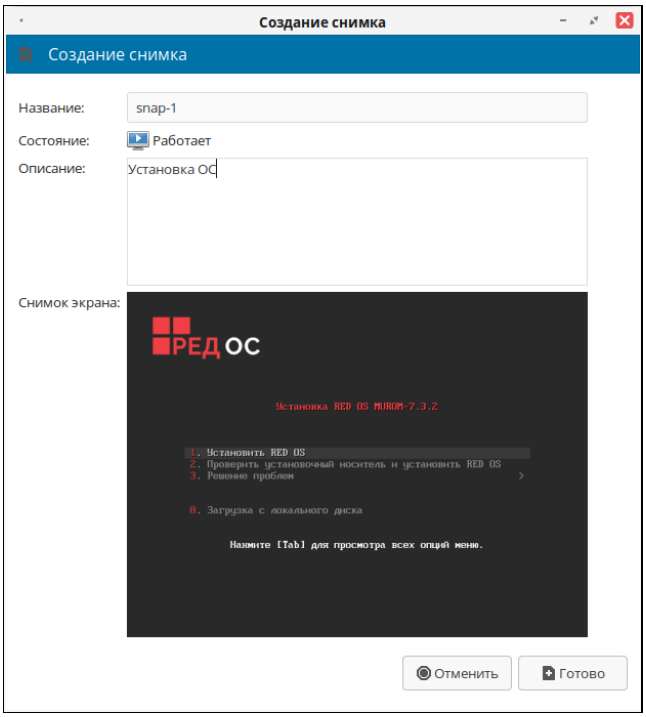
Создание снапшотов

Для создания снимка (снапшота) ВМ необходимо открыть консоль ВМ и перейти на вкладку «**Снимки**», нажав кнопку «**Управление снимками**» ().

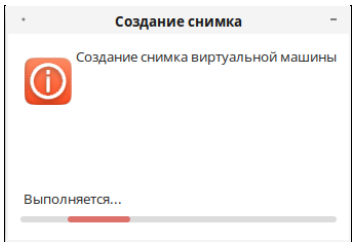
Для создания нового снимка ВМ нажмите кнопку «**Создать новый снимок**».



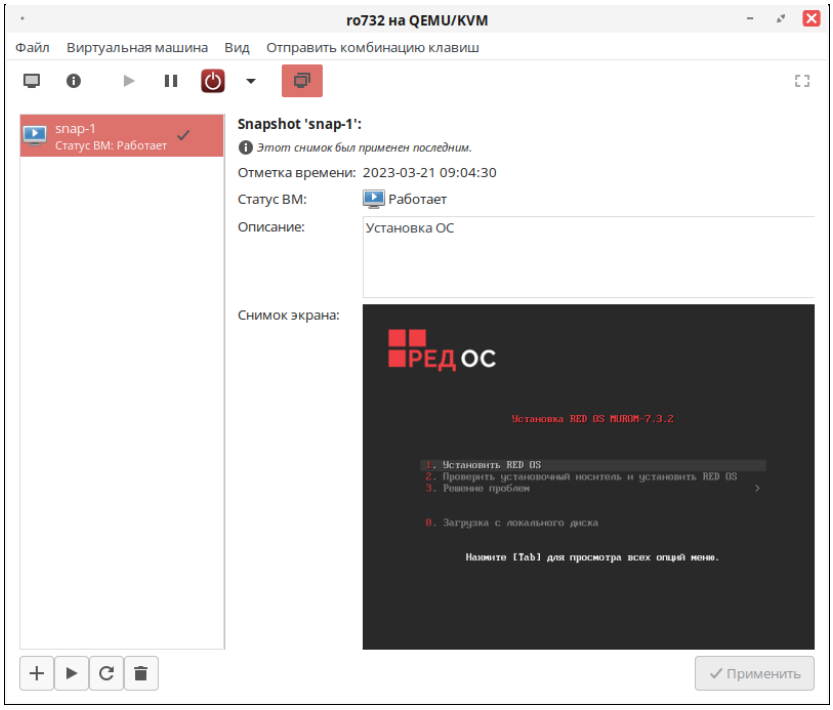
Будет открыто окно «**Создание снимка**», в котором необходимо указать название (обязательно) и описание (по желанию) снимка.



Нажмите кнопку «**Готово**» для запуска процесса создания снимка ВМ.



После этого снимок будет доступен в списке для дальнейшей работы. При выборе конкретного снимка будет отображена подробная информация о нем.



Снимки можно восстанавливать и удалять, нажав ПКМ по нужному снимку либо выбрав снимок и нажав одну из кнопок — «**Запуск выбранного снимка**» ( ) или «**Удалить выбранный снимок**» ( ).

Обновить список доступных снимков можно, нажав кнопку «**Refresh snapshot list**» ( ).

Снапшоты можно создавать как при включенной, так и при выключенной виртуальной машине.

Решение возникающих проблем

После обновления пакета **edk2-ovmf** ВМ (с загрузчиком UEFI) может не запуститься. Внешним признаком является высокая загрузка виртуального процессора (до 100%).

Данная проблема возникает из-за того, что пакет **edk2-ovmf** содержит *firmware* и шаблоны *NVRAM*. При создании виртуальных машин на основе шаблонов пакета **edk2-ovmf** формируются файлы **nvram**. После обновления пакета **edk2-ovmf** *firmware* обновляются, а файлы *nvram* остаются не обновленными. Совместимость нарушается.

Для решения данной проблемы необходимо в **XML** виртуальной машины в разделе `<os>` указать новое имя *nvram*-файла, чтобы он заново сформировался на основе нового шаблона.

Например, было: `<nvram>/var/lib/libvirt/qemu/nvram/myVM_VARS.fd</nvram>`.

Нужно задать новое имя, например: `<nvram>/var/lib/libvirt/qemu/nvram/redos733_VARS.fd</nvram>`.

Конвертация образа машины VirtualBox для KVM

Сначала требуется установить необходимый для виртуализации набор пакетов из стандартного репозитория. Для этого воспользуйтесь командой:

```
dnf install qemu-kvm libvirt python3-libvirt virt-install virt-manager openssh-askpass OVMF
```

После чего будет установлен **Virtual Machine Manager**.

Следующее, что нужно сделать – это установить **VirtualBox** (если он еще не установлен):

```
dnf install VirtualBox VirtualBox-guest-additions VirtualBox-kmod
```

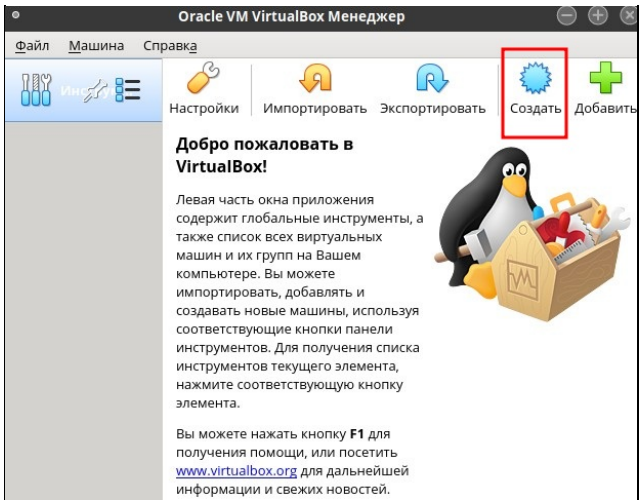
Он будет доступен в **Главном меню - «Администрирование» - «Oracle VM VirtualBox».**

Вы можете подробнее ознакомиться с процессом конвертации образа машины VirtualBox для KVM, просмотрев наши обучающие видео:

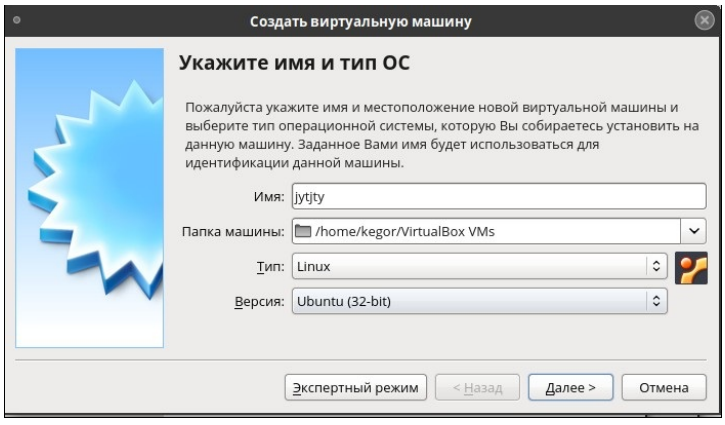
- на **RuTube** — Конвертация образа машины VirtualBox для KVM;
- в **Яндекс.Дзен** — Конвертация образа машины VirtualBox для KVM;
- в **VK Видео** — Конвертация образа машины VirtualBox для KVM.

На наших каналах вы также сможете найти много другой полезной информации.

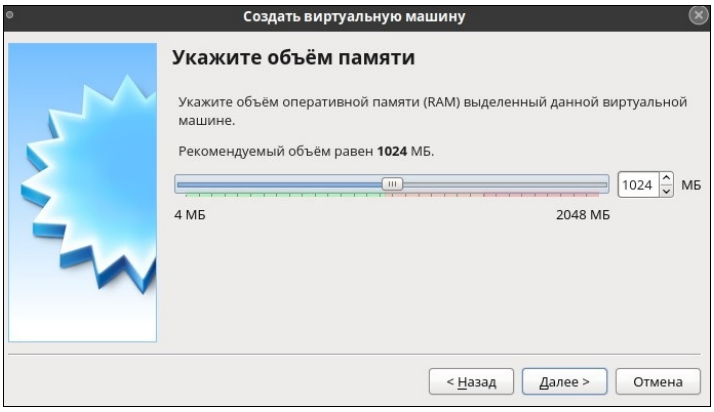
Затем **VirtualBox** Менеджере необходимо создать новый виртуальный образ ОС, для этого нажмите на кнопку « **Создать**».



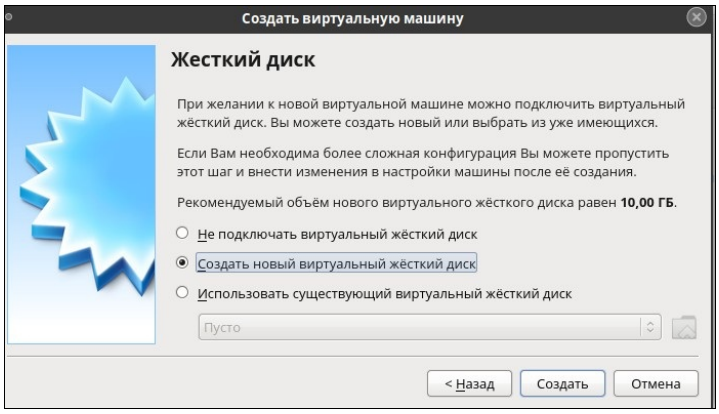
Появится окно, где необходимо указать **Имя**, **Папку машины**, **Тип**, **Версию ОС**.



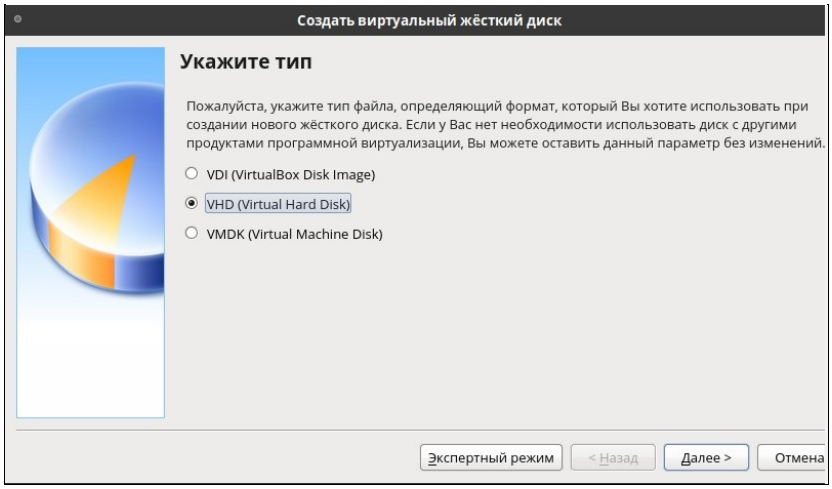
Далее указывается объём оперативной памяти (**RAM**). Можно установить любой объем памяти, но **не менее 1024 МБ**.



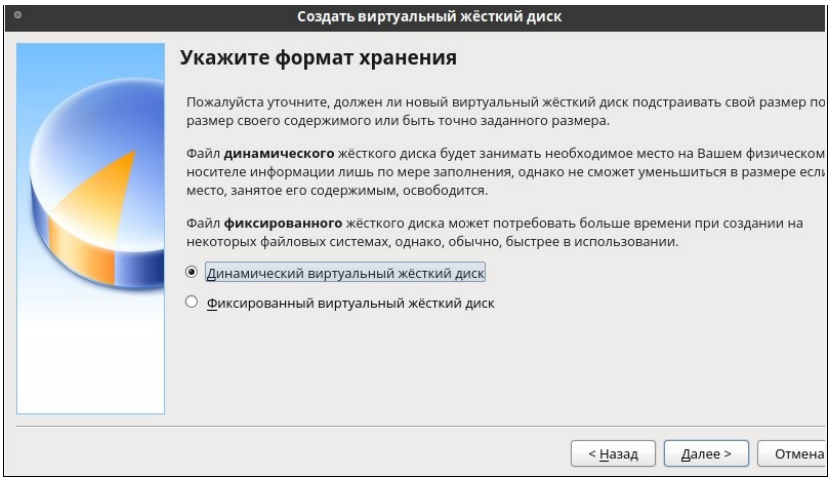
Затем необходимо выбрать пункт «*Создать новый виртуальный жесткий диск*».



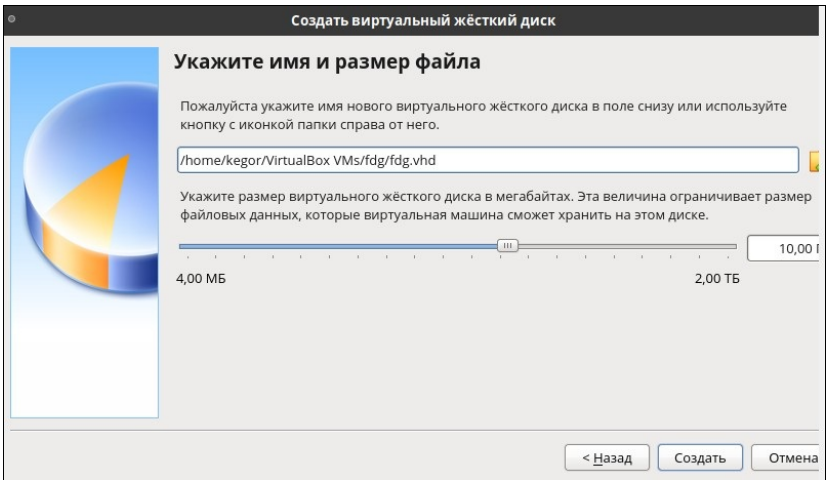
Тип диска установите **VHD**.



Формат хранения выберите «*Динамический виртуальный жесткий диск*».



Затем необходимо задать **Имя** и **Размер** виртуального жесткого диска.



После успешного создания виртуального образа операционной системы *для конвертации* выполните команду:

```
qemu-img convert -f vdi -O qcow2 <название_файла> multifunct.qcow2
```

Установка cloud-init, сценарии и использование в облачных средах

Установка cloud-init
Основные этапы работы и модули cloud-init
Сценарии для cloud-init
Локальный запуск cloud-init
Пример использования локальных сценариев
Примеры сценариев
Использование cloud-init в облачных средах
Отключение cloud-init

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: cloud-init-23.2

Cloud-init — программное обеспечение, разработанное для автоматической настройки виртуальных машин пользователя при первичном запуске. Виртуальные машины с помощью **cloud-init** автоматически конфигурируются при первой загрузке сетевыми настройками, ключами SSH, пакетами, новыми пользователями и другими системными аспектами.

Cloud-init позволяет системным администраторам экономить время и усилия по сравнению с ручной настройкой каждой виртальной машины.

Установка cloud-init

Предварительно пакет **cloud-init** должен быть установлен на виртуальной машине.

Для установки **cloud-init** выполните следующие действия:

1. Авторизуйтесь на виртуальной машине.

2. Установите пакет **cloud-init** на виртуальной машине, выполнив в терминале следующую команду с правами администратора:

```
sudo dnf install cloud-init
```

3. После установки службу **cloud-init** необходимо добавить в автозагрузку, чтобы она запускалась автоматически при старте системы. Таким образом, **cloud-init** начинает работать с момента запуска машины (**до подключения сети**), выполняя первоначальную конфигурацию.

Для запуска и добавления **cloud-init** и сопутствующих служб в гостевой системе в автозагрузку выполните команду:

```
sudo systemctl enable cloud-init cloud-config cloud-final --now
```

4. Для проверки текущего состояния служб используйте следующую команду:

```
sudo systemctl status cloud-init cloud-config cloud-final
```

При успешно выполненных настройках в статусе каждой службы должно отображаться **active (exited)**.

При возникновении проблем можно просмотреть логи **cloud-init**, которые могут помочь в диагностике:

```
sudo tail -f /var/log/cloud-init.log
```

```
sudo tail -f /var/log/cloud-init-output.log
```

Основные этапы работы и модули cloud-init

Работу **cloud-init** можно разделить на несколько ключевых этапов, каждый из которых выполняет определенные задачи для конфигурации системы. Эти этапы можно объединить в три основные фазы, каждая из которых активирует соответствующие службы **cloud-init**.

1. **Обнаружение** (**Detect**) и **локализация** (**Local**) — на этих этапах **cloud-init** определяет платформу виртуальной машины и находит

локальные источники данных. Также на этом этапе применяется сетевая конфигурация, включая резервную, и очищаются устаревшие настройки. Активные службы:

- **cloud-init-local.service**,
- **cloud-init.service**.

2. **Сетевой этап** (**Network**) и **этап конфигурации** (**Config**) — на этих этапах обрабатываются пользовательские данные, выполняются модули disk_setup и mounts, а также запускаются модули конфигурации. Активная служба:

- **cloud-config.service**.

3. **Финальный этап** (**Final**) — данный этап завершает процесс загрузки системы, начинается выполнение пользовательских задач, такие как установка пакетов, выполнение плагинов систем управления конфигурациями и запуск пользовательских скриптов. Активные службы:

- **cloud-final.service**,
- **cloud-init-hotplugd.service**.

В **cloud-init** доступно множество дополнительных модулей, расширяющих возможности конфигурации системы. Дополнительную информацию по модулям можно получить на официальном сайте. Модули можно добавлять или удалять. Они выполняются последовательно на каждом из этапов. Модули разделены на три группы в зависимости от этапа, на котором они запускаются:

- **cloud_init_modules** — модули, выполняемые на этапе инициализации, до подключения к сети;
- **cloud_config_modules** — модули, активируемые после подключения к сети на этапе конфигурации;
- **cloud_final_modules** — модули, выполняемые на финальном этапе.

Сценарии для cloud-init

При запуске системы **cloud-init** проверяет конфигурационные файлы, написанные в формате YAML, и выполняет указанные в них инструкции.

Основным конфигурационным файлом **cloud-init** является **/etc/cloud/cloud.cfg**.

Этот файл содержит ключевые настройки системы и представляет собой главный сценарий конфигурации, в котором прописываются директивы и их параметры. Каждая директива связана с конкретным модулем **cloud-init**, который выполняет определённую задачу. Конфигурационный файл можно редактировать, используя текстовый редактор.

Локальный запуск cloud-init

Для локального запуска **cloud-init** и проверки его работы можно использовать несколько команд. Эти команды помогут инициализировать, запустить модули и проверить результат работы **cloud-init**.

1. Для запуска **cloud-init** в локальном режиме используйте следующую команду:

```
sudo cloud-init init --local
```

Эта команда выполняет только локальные модули и сценарии, которые предназначены для выполнения **ДО** подключения к сети.

2. Запуск модулей **cloud-init**. Можно запускать различные модули **cloud-init** в зависимости от стадии инициализации. Команда запускает конфигурационные модули, которые предназначены для конфигурации системы, используя доступные сетевые ресурсы:

```
sudo cloud-init modules --mode=config
```

Для запуска финальных модулей, которые запускаются после полной конфигурации системы, используйте команду:

```
sudo cloud-init modules --mode=final
```

3. Для проверки текущего состояния **cloud-init** и корректного выполнения модулей используйте команду:

```
cloud-init status
```

Вывод `status: done` означает, что **cloud-init** завершил свою работу без ошибок.

Пример использования локальных сценариев

Подход позволяет автоматизировать задачи по конфигурации системы, задавая параметры на этапе запуска виртуальной машины. Сценарии могут включать установку пакетов, настройку пользователей, управление сервисами и многое другое.

Для настройки имени хоста при загрузке виртуальной машины выполните следующие действия:

1. Создайте новый файл конфигурации **my-cloud-config.cfg** в каталоге **/etc/cloud/cloud.cfg.d/**.

Все файлы с расширением ***.cfg** в этом каталоге будут прочитаны с помощью #cloud-init. Они читаются в лексическом порядке. Более поздние файлы перезаписывают значения в более ранних файлах.

```
sudo nano /etc/cloud/cloud.cfg.d/my-cloud-config.cfg
```

2. Вставьте следующее содержимое сценария в файл:

```
#cloud-config
hostname: my-server
fqdn: my-server.ru
manage_etc_hosts: true
```

где:

- **#cloud-config** — указывает на то, что это инструкции для cloud-init передаются в формате YAML;
- **hostname** — задает короткое имя хоста;
- **fqdn** — задает полное имя хоста;
- **manage_etc_hosts** — разрешает cloud-init управлять файлом **/etc/host.**

3. Сохраните и закройте файл, нажав Ctrl+O, затем Enter, чтобы сохранить, и Ctrl+X, чтобы выйти.

4. Проверьте конфигурацию. После создания или редактирования сценария можно проверить конфигурацию, запустив cloud-init в режиме проверки:

```
sudo cloud-init init --local
sudo cloud-init modules --mode=config
sudo cloud-init modules --mode=final
```

5. Примените изменения.

Для применения внесенных в конфигурацию изменений выполните:

```
sudo systemctl restart cloud-init
```

Для полной переинициализации cloud-init (Внимание! Это может привести к сбросу некоторых настроек!) выполните команды:

```
sudo cloud-init clean
sudo cloud-init init
```

6. В некоторых случаях может потребоваться перезагрузка системы:

```
reboot
```

7. Проверьте, что изменения были применены.

Например, для проверки имени хоста выполните команду:

```
hostname
```

Примеры сценариев

Пример 1. Настройка имени хоста.

```
#cloud-config
hostname: my-server
```

```
fqdn: my-server.ru
manage_etc_hosts: true
```

Пример 2. Установка пакетов.

```
#cloud-config
packages:
- git
- tox
- htop
```

Пример 3. Настройка сети.

```
#cloud-config
network:
version: 2
ethernets:
eth0:
dhcp4: true
```

При запуске новой виртуальной машины или физического сервера, система автоматически настраивает сетевой интерфейс eth0 для использования DHCPv4. Это означает, что интерфейс будет отправлять запросы на роутер или сервер DHCP в сети, чтобы получить IP-адрес и другие параметры сети.

Проверить применение настроек файла конфигурации можно с помощью команды:

```
ip addr
```

Пример 4. Запуск скриптов.

```
#cloud-config
runcmd:
- echo "Hello, World!" > /home/user/hello.txt
- systemctl start firebird.service
```

где:

- **echo "Hello, World!" > /home/user/hello.txt** — создает (или перезаписывает) файл **/home/user/hello.txt** с текстом "Hello, World!".
- **systemctl start firebird.service** — запускает службу Firebird, если она установлена на виртуальной машине.

Проверить применение настроек файла конфигурации можно с помощью команды:

```
cat /home/user/hello.txt
systemctl status firebird.service
```

Пример 5. Установка и настройка временной зоны.

```
#cloud-config
timezone: US/Eastern
```

где:

- **timezone** — настройка временной зоны.

Для проверки timezone используйте команду:

```
timedatectl           Local time: Пт 2024-09-20 06:34:40 EDT
      Universal time: Пт 2024-09-20 10:34:40 UTC
            RTC time: Пт 2024-09-20 10:34:40
           Time zone: US/Eastern (EDT, -0400)
System clock synchronized: yes
          NTP service: active
      RTC in local TZ: no
```

Пример 6. Запуск нескольких команд при первой загрузке.

Приведенный сценарий сохраняет содержимое веб-страницы в файл и запускает команду **echo** с аргументами.

```
#cloud-config
 runcmd:
- [ wget, "https://ya.ru/", -O, /tmp/index.html ]
- [ sh, -xc, "echo $(date) ': hello world!'" ]
```

где:

- **runcmd** — используется для указания списка команд, которые должны быть выполнены после завершения основной конфигурации cloud-init, но ДО первого входа в систему;
- **wget** — используется для загрузки веб-страницы https://ya.ru/ и сохранения ее содержимого в файл **/tmp/index.html**;
- **sh -xc** — запускает команду echo с аргументами **$(date) ': hello world!'**. Аргумент **-x** указывает, что команда должна быть выведена на экран перед выполнением, а **-c** указывает, что следующая строка — команда, которую нужно выполнить.

Проверьте содержимое файла **/tmp/index.html**. Если команда **wget** была выполнена успешно, то в этом файле должно быть сохранено содержимое веб-страницы. Можно просмотреть содержимое файла в терминале:

```
cat /tmp/index.html
```

Использование cloud-init в облачных средах

Применение в облачных средах:

1. **Развертывание масштабируемых приложений**.

В облачных средах для быстрого развертывания большого количества виртуальных машин **cloud-init** позволяет сократить время на настройку и конфигурацию серверов.

2. **Упрощение управления инфраструктурой**.

Вместо ручной конфигурации каждой виртуальной машины, администраторы могут создавать шаблоны конфигураций с помощью **cloud-init**. Шаблоны могут автоматически применяться к новым экземплярам виртуальных машин при их создании.

3. **Обеспечение единообразия окружения**.

Используя **cloud-init**, можно гарантировать, что каждая виртуальная машина будет иметь одинаковую базовую конфигурацию, что снижает вероятность ошибок, связанных с ручной настройкой.

Алгоритм для использования конфигурации с помощью облачного провайдера

1. **Создание конфигурационного файла**. Сохраните файл конфигурации, например, **/etc/cloud/cloud.cfg.d/my-cloud-config.cfg** в формате YAML.

2. **Использование cloud-init с образом ВМ**. Убедитесь, что ваш облачный провайдер поддерживает **cloud-init**. При создании нового экземпляра виртуальной машины в облаке загрузите созданный YAML-файл в качестве пользовательских данных.

3. **Запуск виртуальной машины**. Запустите экземпляр ВМ. **Cloud-init** автоматически выполнит конфигурацию при первом запуске.

Настройка cloud-init в облачных сервисах

В каждом облаке существует сервис, передающий виртуальной машине информацию о её окружении. Эта информация поступает в несколько типов данных, которые **cloud-init** использует в определённой последовательности.

1. **Пользовательские данные** (**user-data**). Это настройки и директивы, указанные в конфигурационном файле **/etc/cloud/cloud.cfg**. В них могут быть прописаны файлы для выполнения, пакеты для установки, скрипты оболочки и другие инструкции. Пользовательские данные, как правило, служат для настройки конкретного экземпляра виртуальной машины. Данные используются для автоматизации различных сценариев, таких как установка необходимого ПО, настройка сервера или управление конфигурациями. **Cloud-init** считывает пользовательские данные и, если они заданы в поддерживаемом формате, выполняет действия, описанные в этих данных.

2. **Метаданные** (**meta-data**). Информация об окружении виртуальной машины, такая как имя сервера, внутренний и публичный IP-адрес, идентификатор экземпляра, публичный SSH-ключ и тип виртуальной машины. Метаданные используются для настройки после применения пользовательских данных.

3 . **Данные поставщиков** (**vendor-data**). Информация, предоставляемая облачными провайдерами или разработчиками, которая помогает настроить образ виртуальной машины для корректной работы в облаке. Эти данные обычно задают конфигурации по умолчанию и применяются после метаданных.

Отключение cloud-init

В некоторых случаях, когда автоматическая настройка ВМ с использованием **cloud-init** не требуется, служба может быть отключена.

Для отключения **cloud-init** доступно несколько способов.

Способ 1. Файл отключения службы. Для отключения **cloud-init** необходимо создать пустой файл **/etc/cloud/cloud-init.disabled**:

```
sudo touch /etc/cloud/cloud-init.disabled
```

Во время загрузки система инициализации операционной системы проверит существование этого файла. Если он существует, **cloud-init** не будет запущен.

Способ 2. Отключение через конфигурацию загрузчика. Для отключения **cloud-init** необходимо добавить параметр **cloud-init=disabled** в конфигурацию загрузчика и применить настройки для загрузчика:

- для систем с **BIOS**:

```
sudo bash -c 'echo "GRUB_CMDLINE_LINUX=\"cloud-init=disabled\"" >> /etc/default/grub'
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем с **UEFI**:

```
sudo bash -c 'echo "GRUB_CMDLINE_LINUX=\"cloud-init=disabled\"" >> /etc/default/grub'
sudo grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Способ 3. Указание переменной окружения. Для отключения **cloud-init** также можно передать переменную окружения **KERNEL_CMDLINE=cloud-init=disabled** для каждого из процессов **cloud-init**:

```
sudo bash -c 'echo "DefaultEnvironment=KERNEL_CMDLINE=cloud-init=disabled" >> /etc/systemd/system.conf'
```

Установка VMware

Загрузите файл установки с официального сайта VMware.

После загрузки необходимо назначить файлу права на исполнение:

```
chmod +x /home/user/Загрузки/VMware-Player-16.1.2-17966106.x86_64.bundle
```

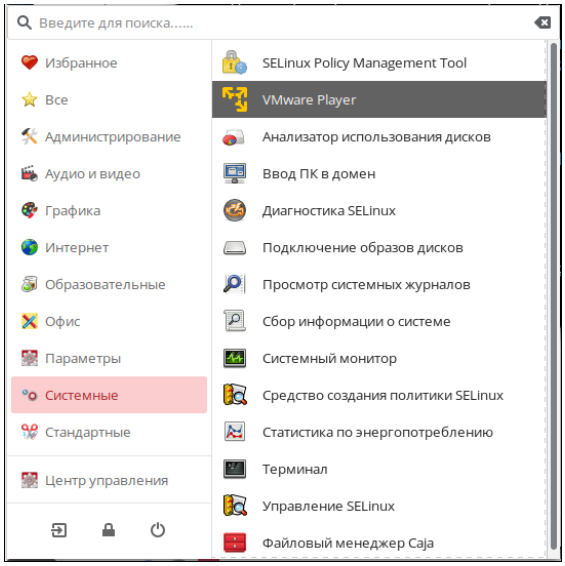
и установить дополнительные пакеты (с правами пользователя **root**):

```
dnf install gcc kernel-lt-devel
```

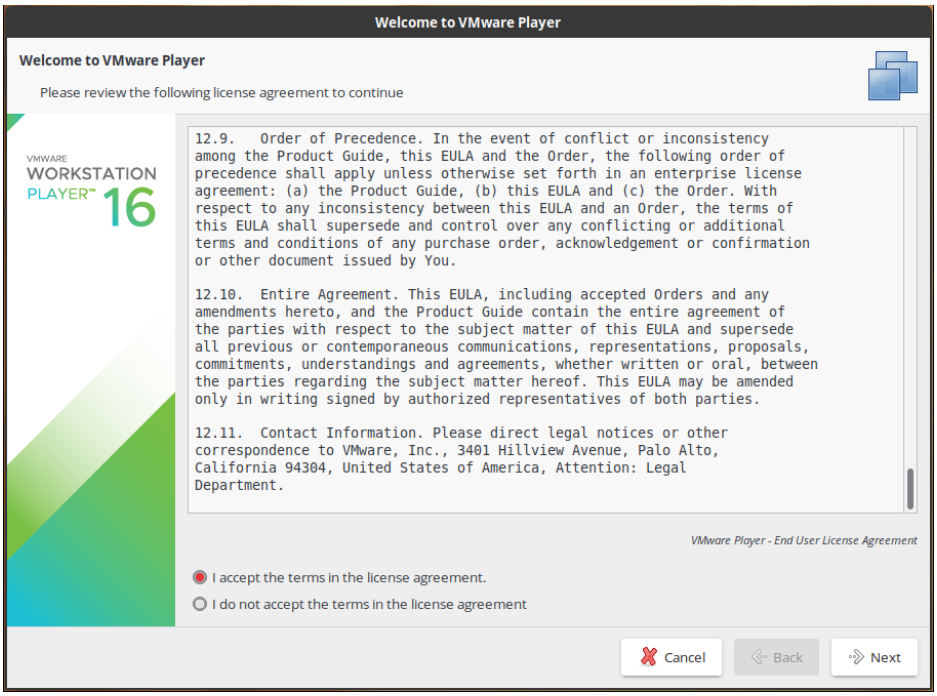
Перейдите в папку с загруженным файлом и выполните установку программы:

```
cd /home/user/Загрузки/
./VMware-Player-16.1.2-17966106.x86_64.bundle
```

После успешной установки программу можно найти в «*Главном меню — Системные — VMware Player*».

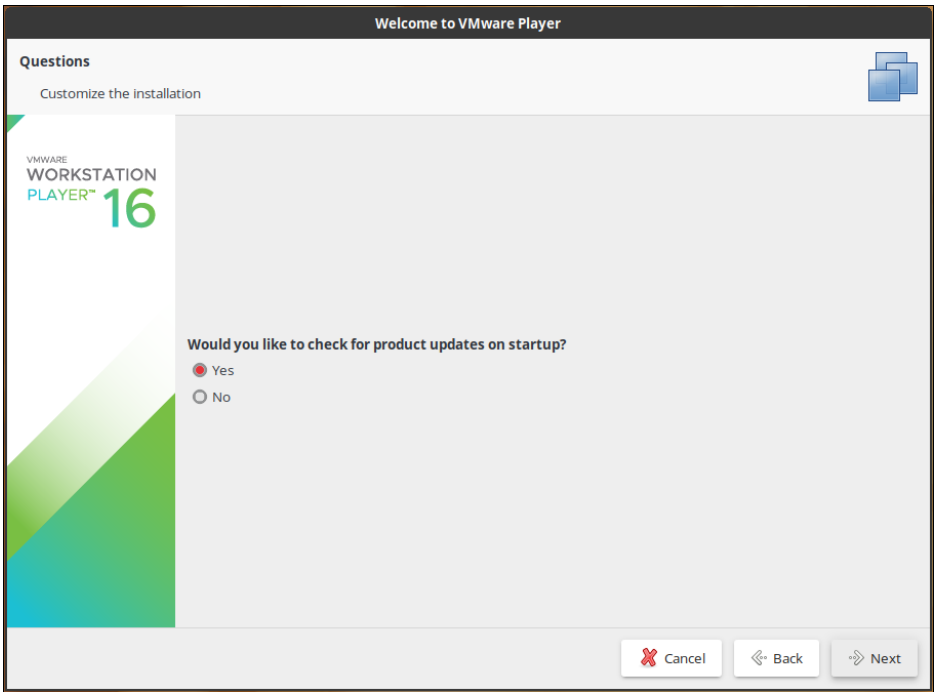


Первый запуск программы будет выглядеть следующим образом:

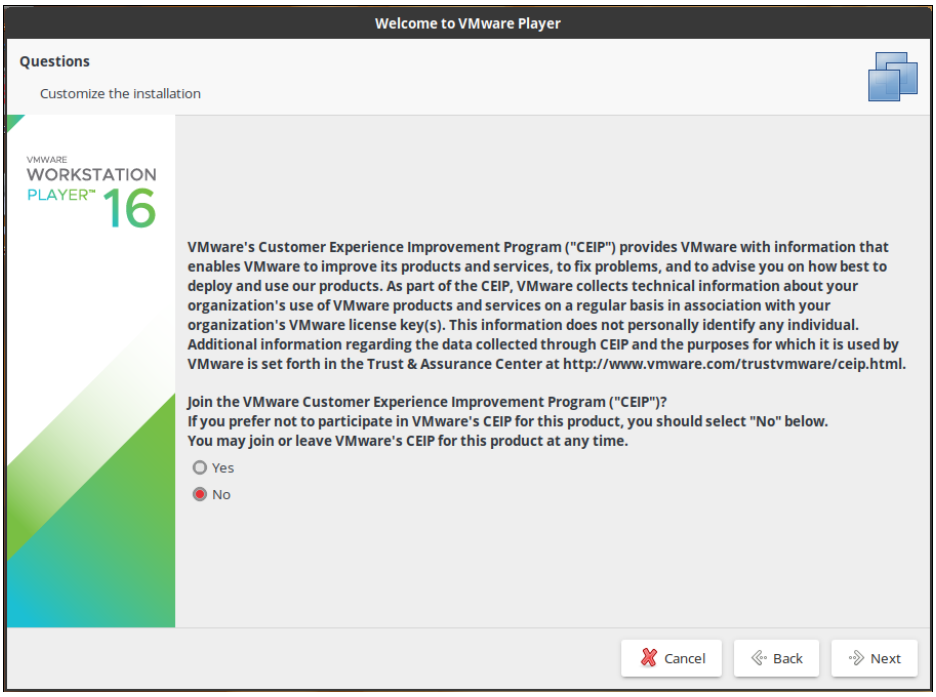


После запуска необходимо прочесть лицензионное соглашение, выбрать пункт «**I accept the terms in the license agreement**» и нажать кнопку «**Next**».

Далее необходимо указать, хотите ли вы проверять наличие обновлений при каждом последующем запуске программы. Выбираем пункт «**Yes**» (можно выбрать пункт «**No**», тогда проверка наличия обновлений будет производиться вручную).

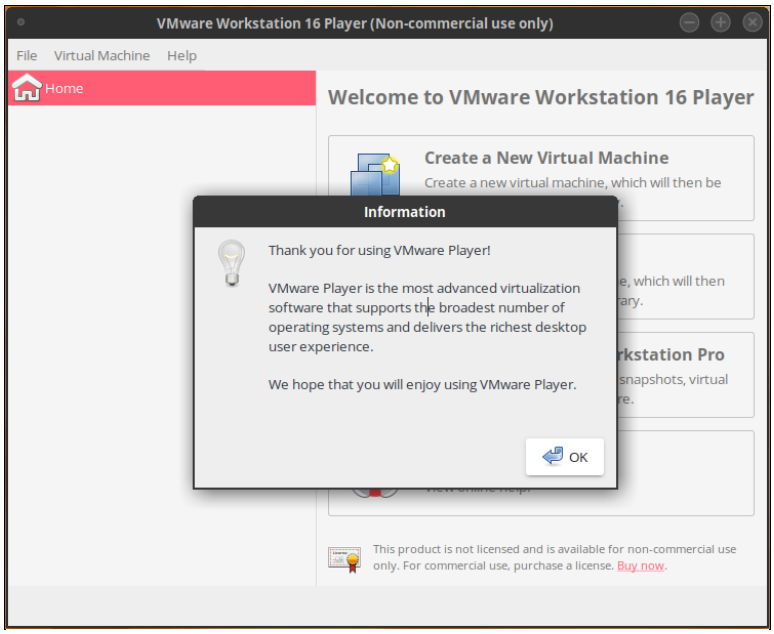


После нажатия кнопки «**Next**» установщик уточняет, хотите ли вы принимать участие в программе улучшения качества обслуживания клиентов. Это нужно для сбора технической информации об использовании VMware. Можно выбрать любой пункт, на ваше усмотрение. В данном случае выберем «**No**».



В завершении установки программа предложит ввести лицензионный ключ (при коммерческом использовании продукта) либо выбрать пункт «**Use VMware Player 16 for free for non-commercial use**» (бесплатное некоммерческое использование продукта). Выберите последний пункт и нажмите кнопку «**Finish**».

После этого откроется **VMware Workstation 16 Player** и приветственное окно.



Нажмите «**OK**» и после этого можно приступать к работе.

Установка РЕД ОС в VMware

Окружение

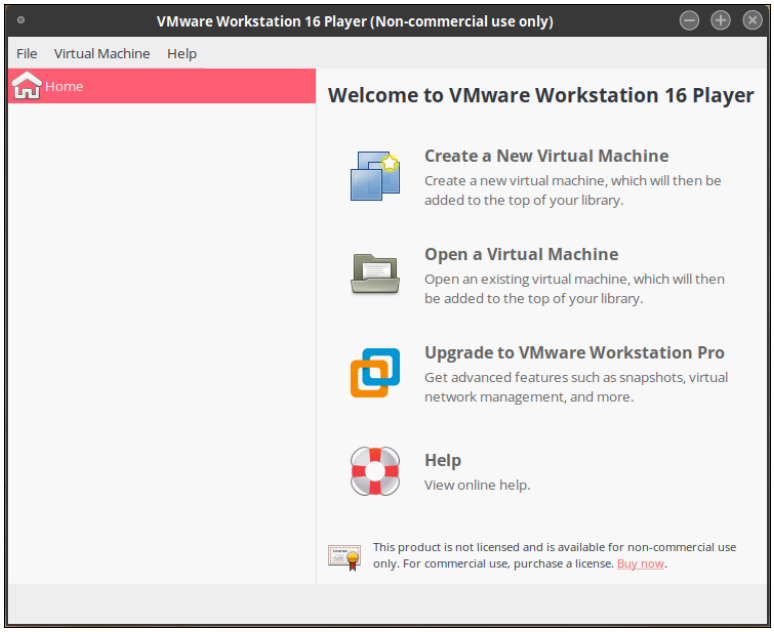
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VMware-Player-Full-16.2.4-20089737

Вы можете подробнее ознакомиться с информацией по установке системы в VMware, просмотрев наши обучающие видео:

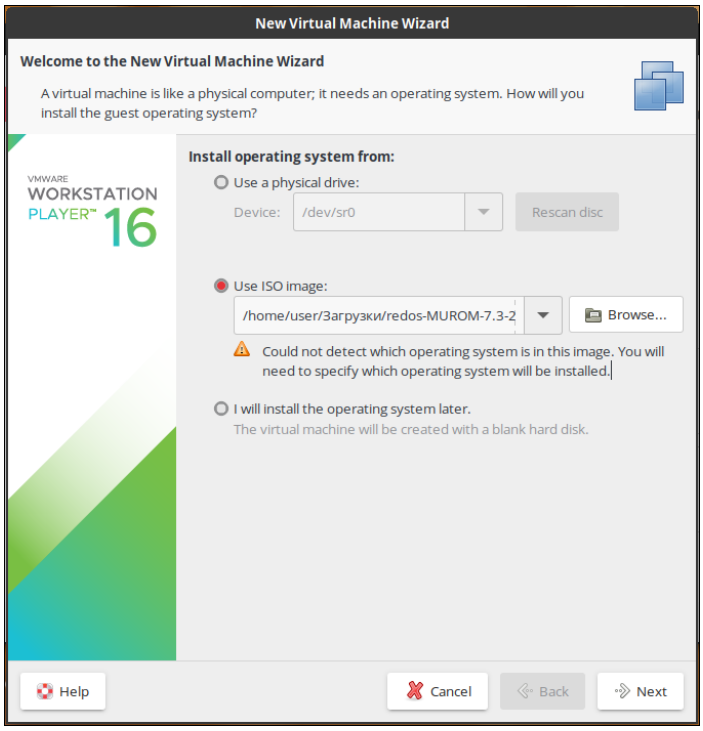
- на **RuTube** — Установка РЕД ОС в виртуальных средах на примере VMWare;
- в **Яндекс.Дзен** — Установка РЕД ОС в виртуальных средах на примере VMWare;
- в **VK Видео** — Установка РЕД ОС в виртуальных средах на примере VMWare.

На наших каналах вы также сможете найти много другой полезной информации.

Для того чтобы начать работу в новой системе, необходимо создать новую виртуальную машину. Для этого выберите на домашней странице программы пункт «**Create a New Virtual Machine**».



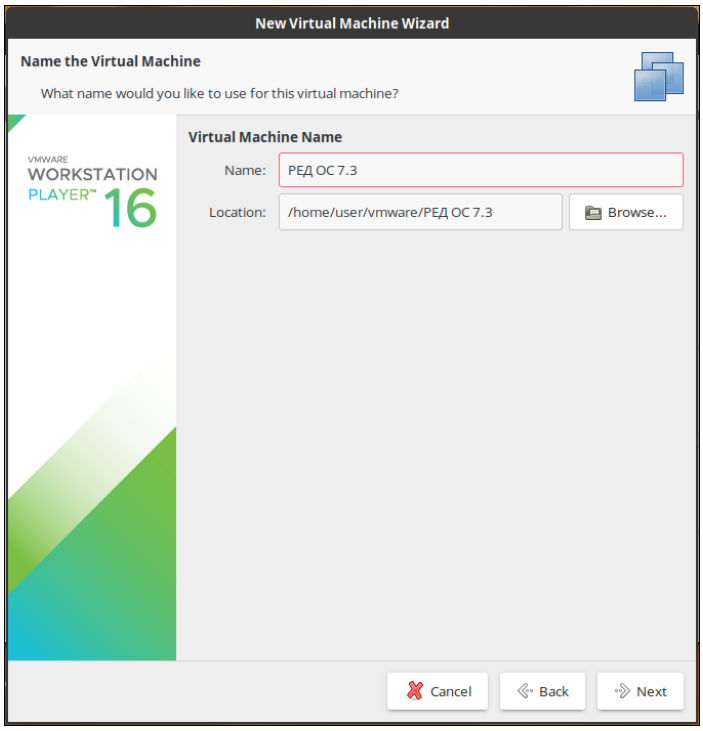
После этого откроется мастер установки, на начальном экране которого необходимо выбрать установочный диск для новой машины. Это может быть ISO-образ, сохраненный в файловой системе, или реальный привод оптических дисков.



Затем необходимо выбрать тип ОС и версию.



Указываем имя машины и ее расположение на диске основной системы.

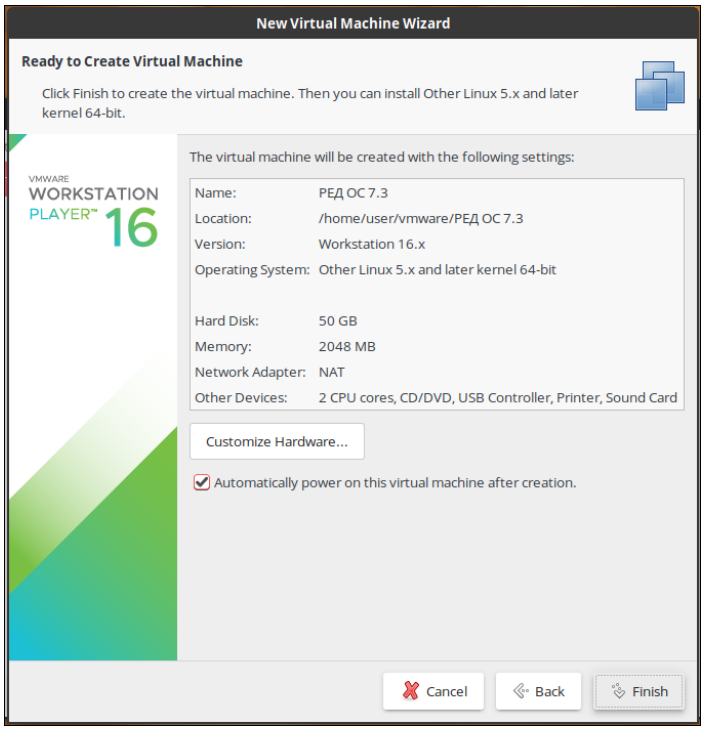


Затем необходимо установить максимальный размер жесткого диска, на который будет установлена система и будут храниться необходимые данные. Указанное значение не должно быть ниже минимально допустимого (более подробную информацию о системных требованиях см. по ссылке).

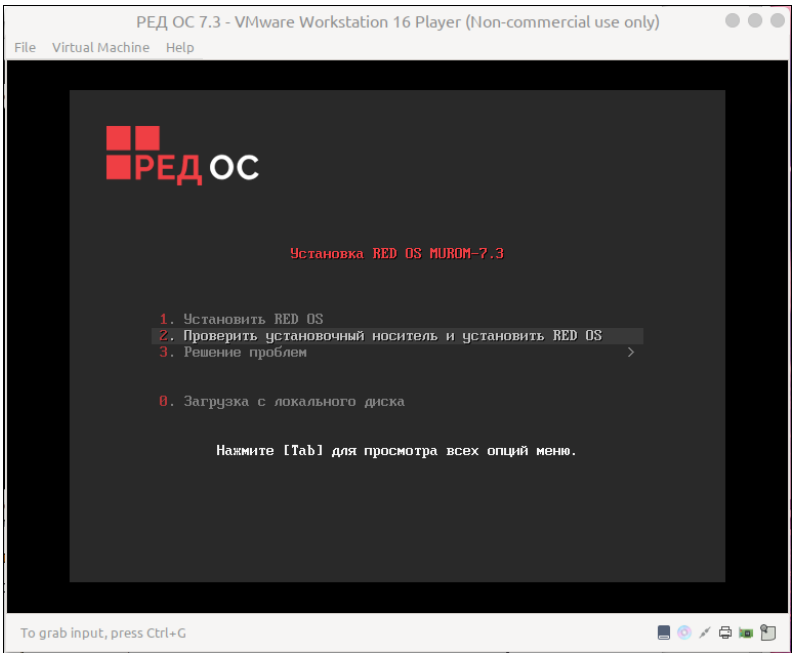
Также предлагается выбрать, разбивать ли на части жесткий диск. Обычно, если вы не планируете записывать его на небольшие носители, разбивать его не нужно.



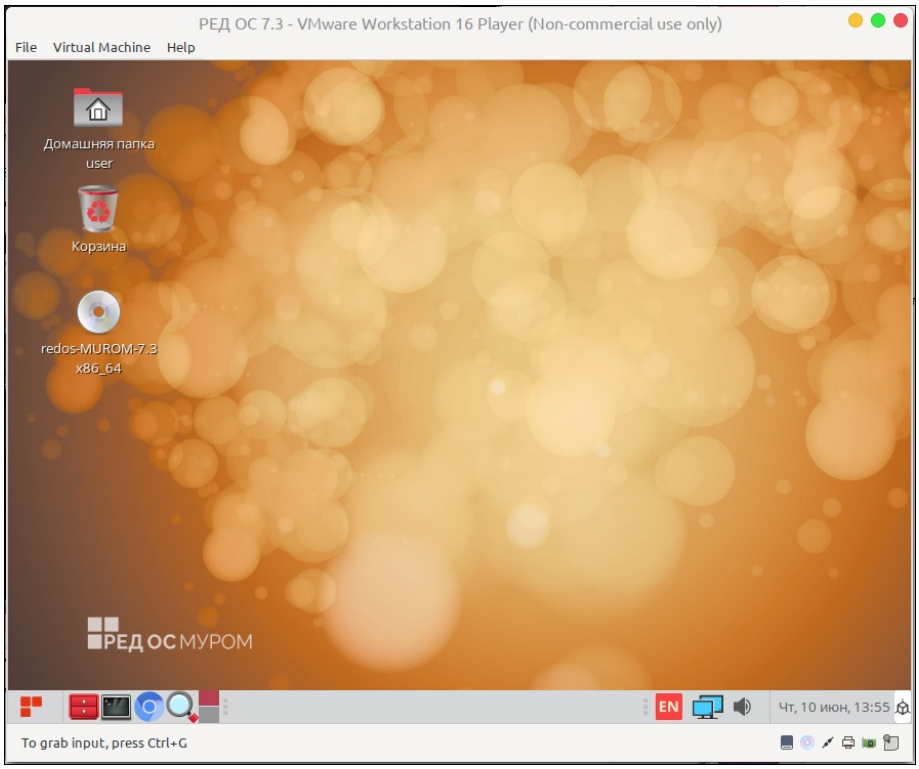
На последнем этапе предлагается просмотреть установленные данные для будущей системы, а также настроить (при необходимости) аппаратное обеспечение (кнопка «**Customize Hardware...**»).



После нажатия кнопки «**Finish**» будет произведен запуск новой виртуальной машины и можно будет начать установку непосредственно системы (подробную информацию об установке РЕД ОС см. по ссылке).



После успешной установки система будет автоматически запущена и готова к работе.


РЕД ОС 7.3 - VMware Workstation 16 Player (Non-commercial use only)
File
Virtual Machine
Help
Домашняя папка
user
Корзина
redos-MUROM-7.3
x86_64
РЕД ОС МУРОМ
EN
Чт, 10 июн, 13:55
To grab input, press Ctrl+G

Установка VMware Tools

VMWare tools — это набор специализированного программного обеспечения, который повышает производительность и обеспечивает дополнительные возможности по управлению гостевой операционной системой.

Основным преимуществом является возможность копировать/вставлять текст и перетаскивать файлы между хостом и гостевой ОС. Также в *VMware Tools* входят драйверы, необходимые для корректной работы гостевой ОС в среде виртуализации.

Возможны 2 варианта установки *VMware Tools*:

- из оригинального дистрибутива;
- из дистрибутива с открытым исходным кодом (*Open VM Tools*).

VMware рекомендует использовать дистрибутив с открытым исходным кодом, т.к. он прост в установке и обновлении, а также совместим практически со всеми популярными версиями Linux. Также он доступен в репозитории операционной системы РЕД ОС.

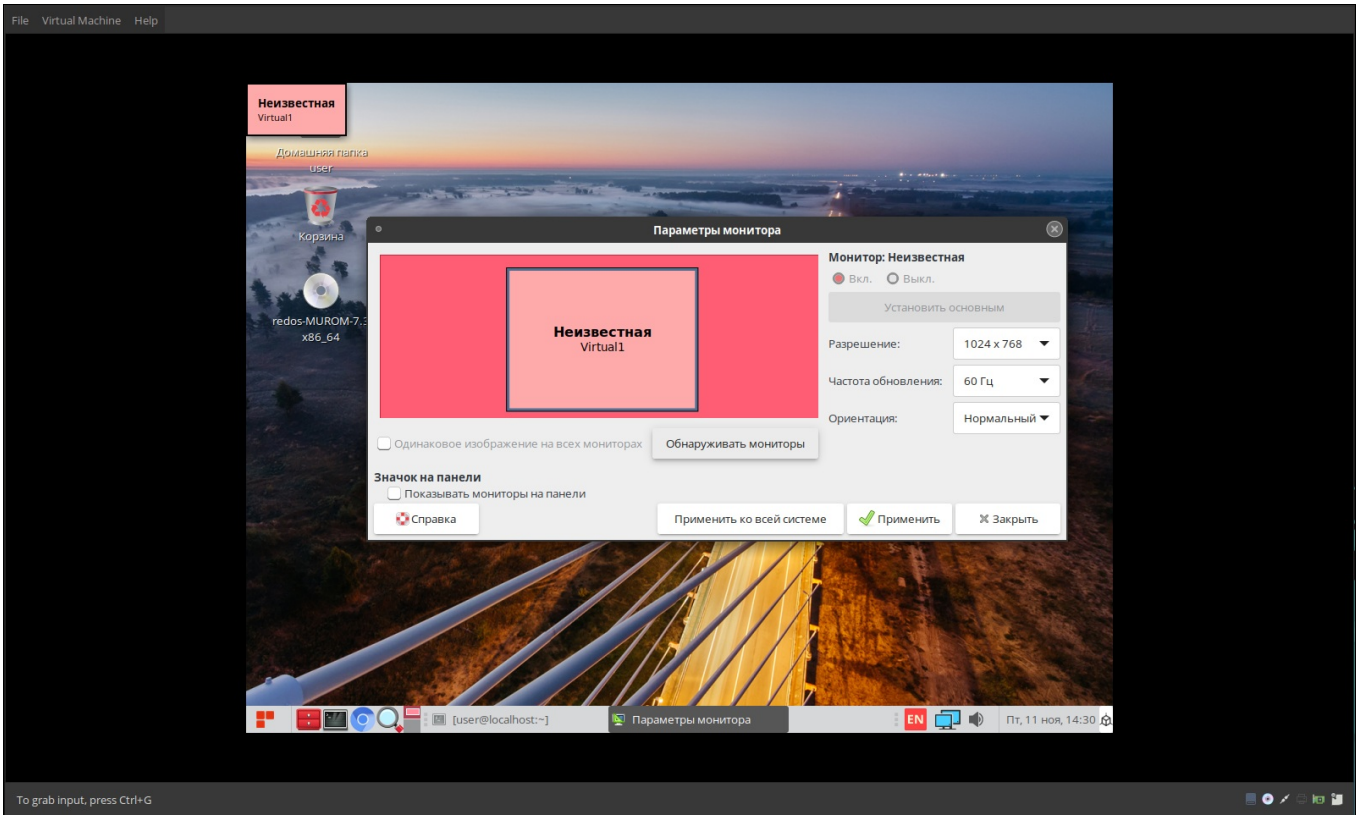
Вы можете подробнее ознакомиться с установкой специализированного ПО VMware Tools, просмотрев наши обучающие видео:

- на **RuTube** — Установка VMware Tools;
- в **Яндекс.Дзен** — Установка VMware Tools;
- в **VK Видео** — Установка VMware Tools.

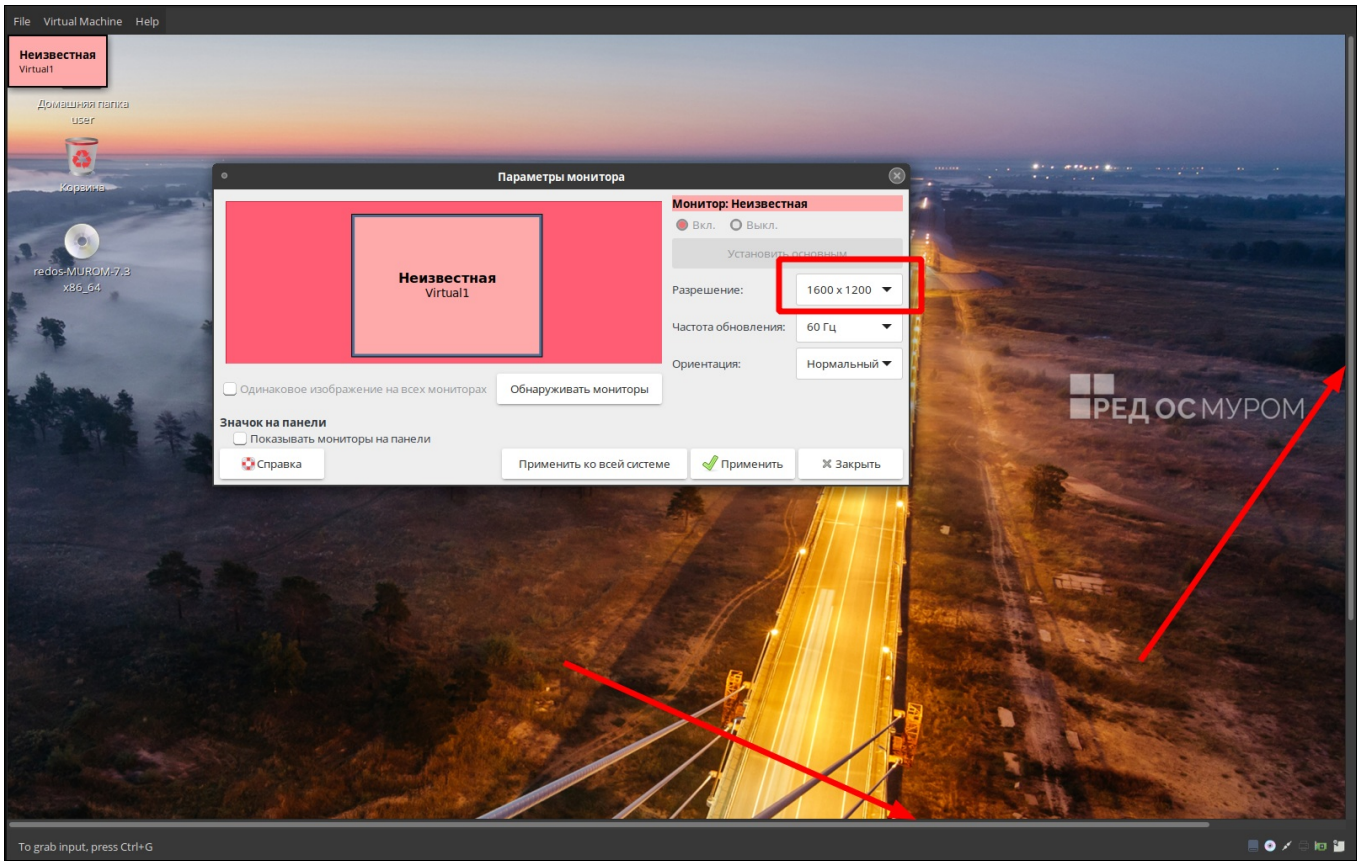
На наших каналах вы также сможете найти много другой полезной информации.

Использование дистрибутива с открытым исходным кодом

Откройте *VMware* и запустите РЕД ОС.



Разрешение экрана при этом низкое, попробуйте изменить его через «**Главное меню**» — «**Параметры**» — «**Экраны**».



Отображение экрана производится некорректно, появляются ползунки для навигации по экрану.

Для устранения данной проблемы необходимо установить пакет open-vm-tools.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**open-vm-tools**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.

Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install open-vm-tools open-vm-tools-desktop
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

Для того чтобы изменения вступили в силу, необходимо перезагрузить ВМ.

Для примера можно скопировать ссылку из браузера основной машины и вставить ее в браузер виртуальной машины.

Использование оригинального дистрибутива

Рассмотрим второй способ установки — из оригинального дистрибутива. Он будет полезен, если у вас нет доступа к сети для скачивания пакета через репозиторий.

Загрузите гостевую систему и выберите в панели меню *VMWare* пункт «**Virtual Machine**» - «**Install VMware Tools**».

В терминале перейдите в сеанс пользователя **root**:

```
su -
```

Создайте папку:

```
mkdir /mnt/cdrom
```

Смонтируйте образ к гостевой системе следующей командой:

```
mount /dev/cdrom /mnt/cdrom
```

Смените директорию на **tmp** и распакуйте архив с установочными скриптами:

```
cd /tmp
tar -zxvf /mnt/cdrom/VMwareTools-<версия>.tar.gz
```

Запустите скрипт установки *VMware Tools*:

```
/tmp/vmware-tools-distrib/vmware-install.pl
```

На все вопросы терминала можно просто нажать **Enter**.

После установки сразу же изменится размер экрана.

Проверьте работоспособность (если все в порядке, в выводе будет отображено `active`):

```
systemctl is-active vmware-tools
```

После этого можно удалить временные файлы в **/tmp**:

```
rm -rf /tmp/vmware-tools-distrib
```

Перезагрузите ВМ будет доступен весь функционал.

Для примера можно скопировать текстовый файл с основной машины на виртуальную простым перетаскиванием.

Установка РЕД ОС 7.3 в Hyper-V

Включение Hyper-V
Создание виртуальной машины
Настройка сети для ВМ
Настройка ВМ
Службы интеграции Hyper-V
Примечание

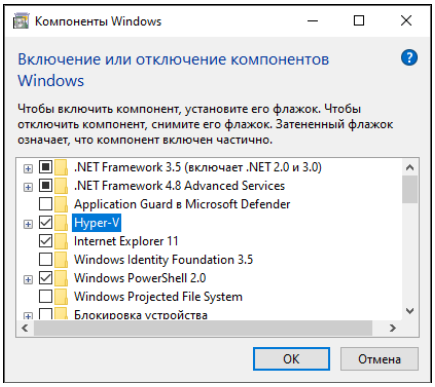
Вы можете подробнее ознакомиться с примером установки системы в Hyper-V, просмотрев наши обучающие видео:

- на **RuTube** — Установка РЕД ОС в виртуальных средах на примере Hyper-V;
- в **Яндекс.Дзен** — Установка РЕД ОС в виртуальных средах на примере Hyper-V;
- в **VK Видео** — Установка РЕД ОС в виртуальных средах на примере Hyper-V.

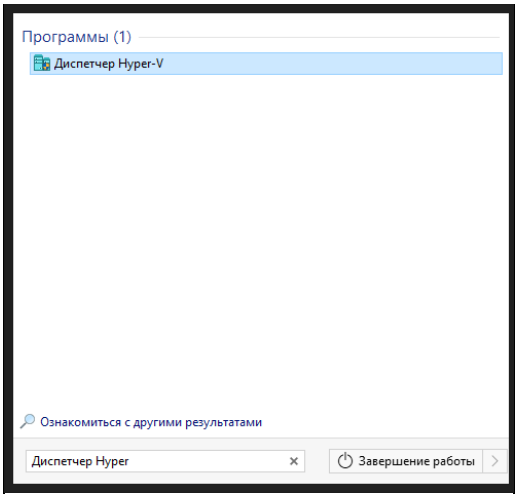
На наших каналах вы также сможете найти много другой полезной информации.

Включение Hyper-V

Убедитесь, что компоненты **Hyper-V** включены. Для этого перейдите в «**Панель управления**» - «**Программы и компоненты**» - «**Включение и отключение компонентов Windows**». Если не включены, установите флажок, нажмите «**OK**» и перезагрузите компьютер.

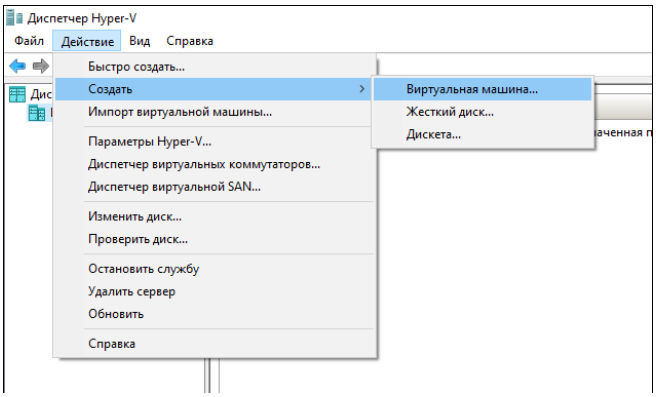


Запустите **Диспетчер Hyper-V**.

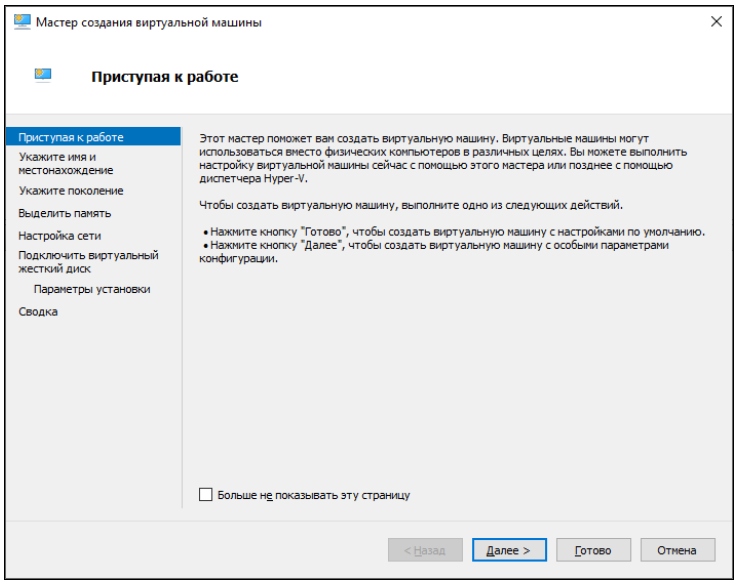


Создание виртуальной машины

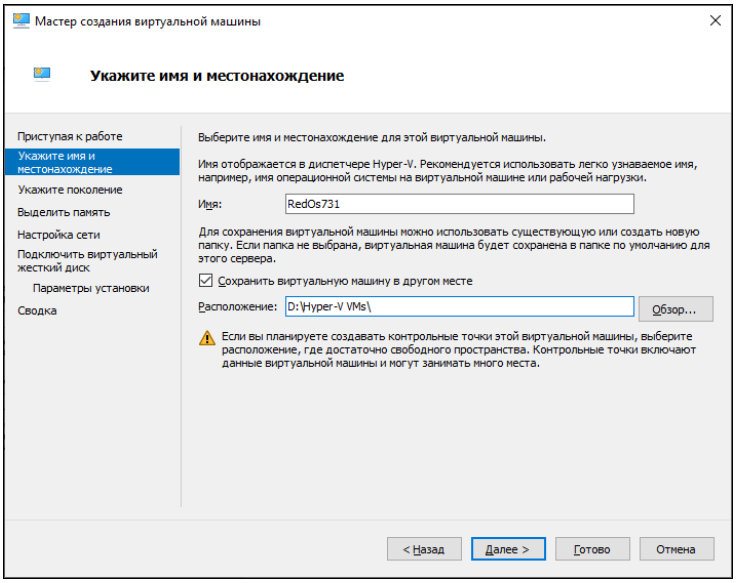
В **Диспетчере Hyper-V** нажмите на пункт меню «**Действие**» - «**Создать**» - «**Виртуальная машина**».



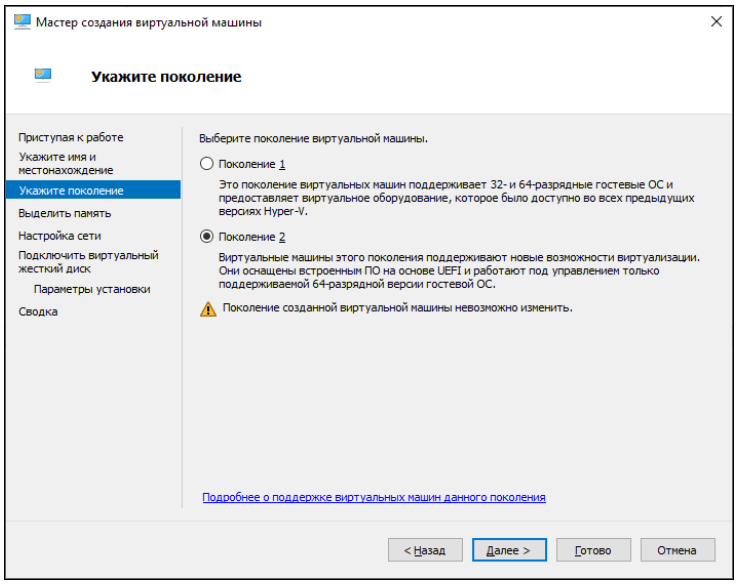
Откроется окно начальной настройки ВМ. Нажмите «**Далее**».



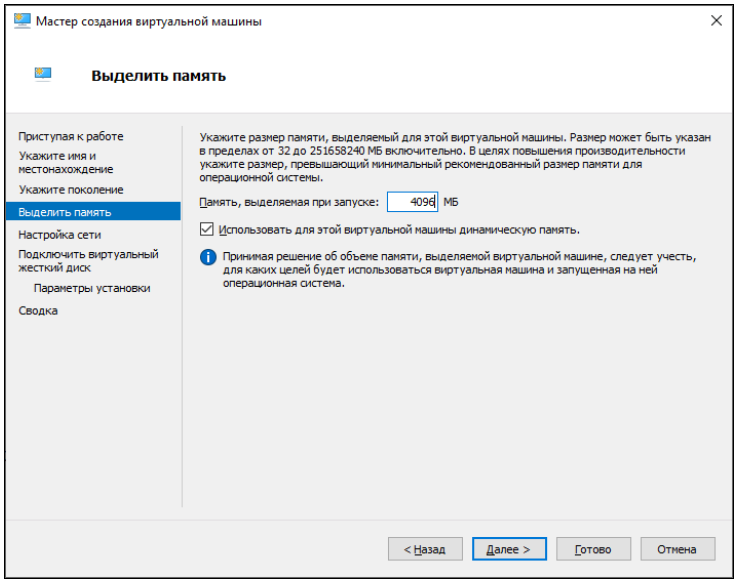
Укажите имя виртуальной машины и ее место расположения (по умолчанию она будет находиться на диске **C**). Нажмите «**Далее**».



Выберите «**Поколение 2**» виртуальной машины. Нажмите «**Далее**».

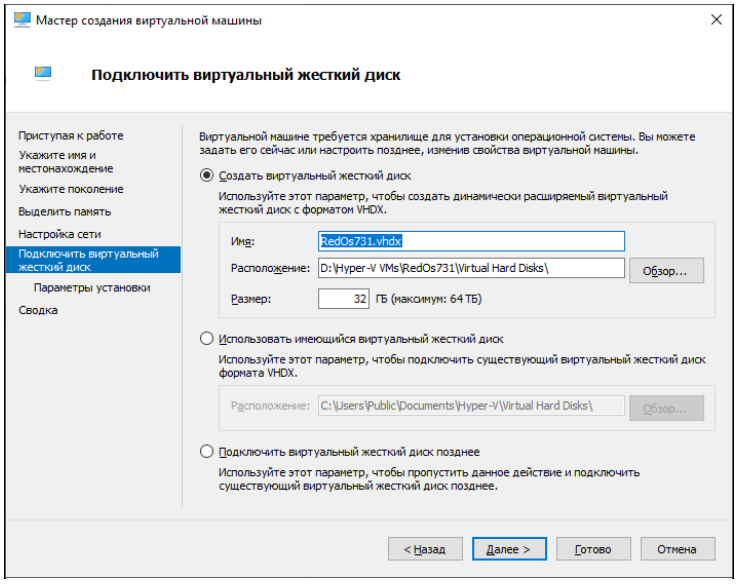


Установите максимальный объём оперативной памяти, который будет выделен для ВМ. С минимальными системными требованиями для установки РЕД ОС 7.3 можно ознакомиться по ссылке.

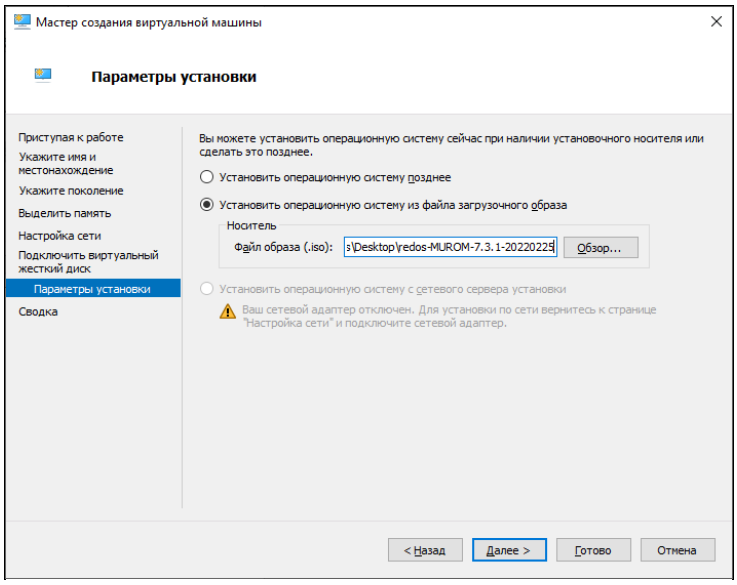


Пункт настроек сети временно пропустите.

Перейдите к настройке жесткого диска. Укажите имя жесткого диска, его место расположения и размер. Нажмите «**Далее**».



Укажите путь к установочному образу РЕД ОС 7.3.1. Нажмите «**Далее**».

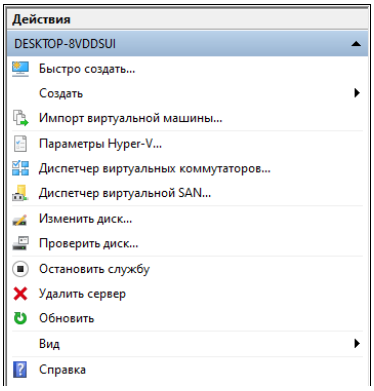


В «**Сводке**» проверьте настроенные данные и нажмите «**Готово**».

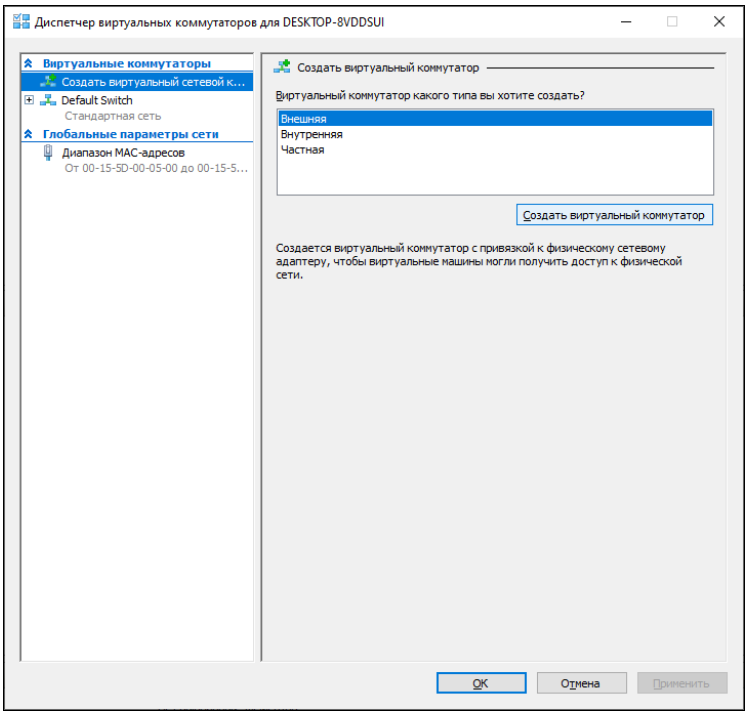
Настройка сети для ВМ

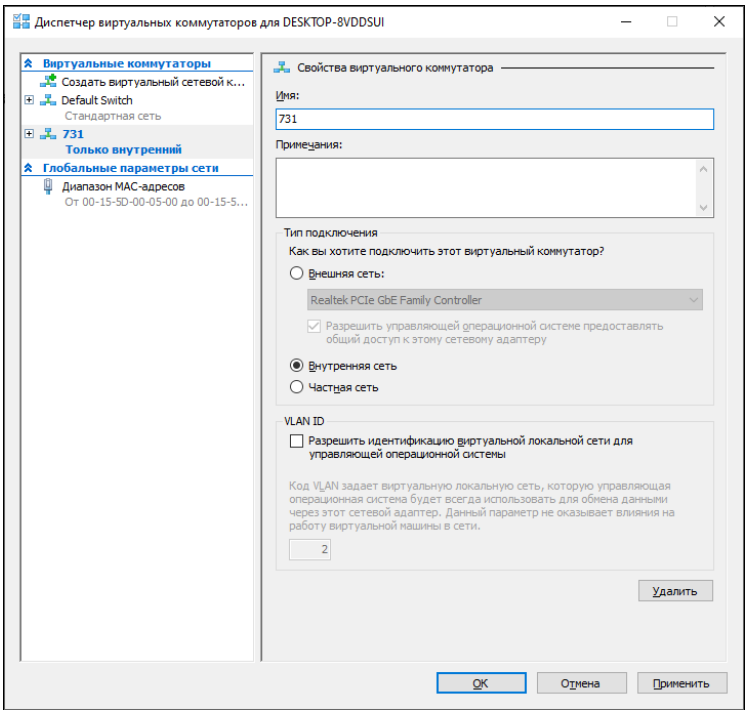
После создания ВМ настройте для нее сеть.

Для этого откройте «**Диспетчер виртуальных коммутаторов**».



Создайте виртуальный коммутатор.

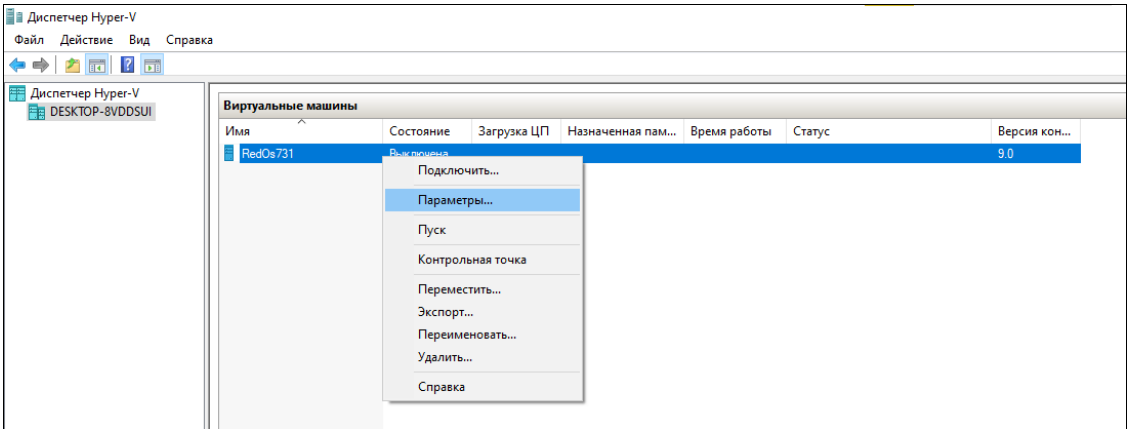




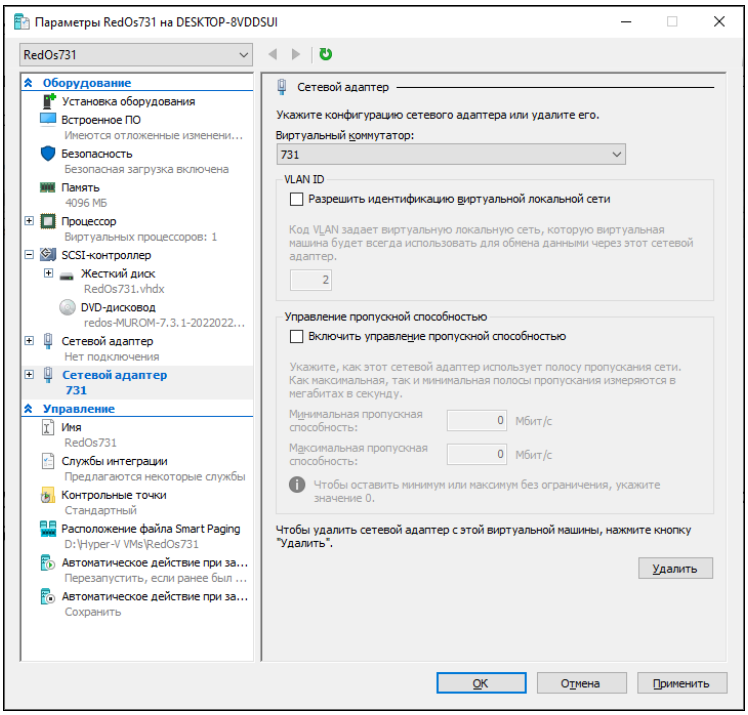
После этого закройте настройки коммутаторов и перейдите в настройки виртуальной машины.

Настройка ВМ

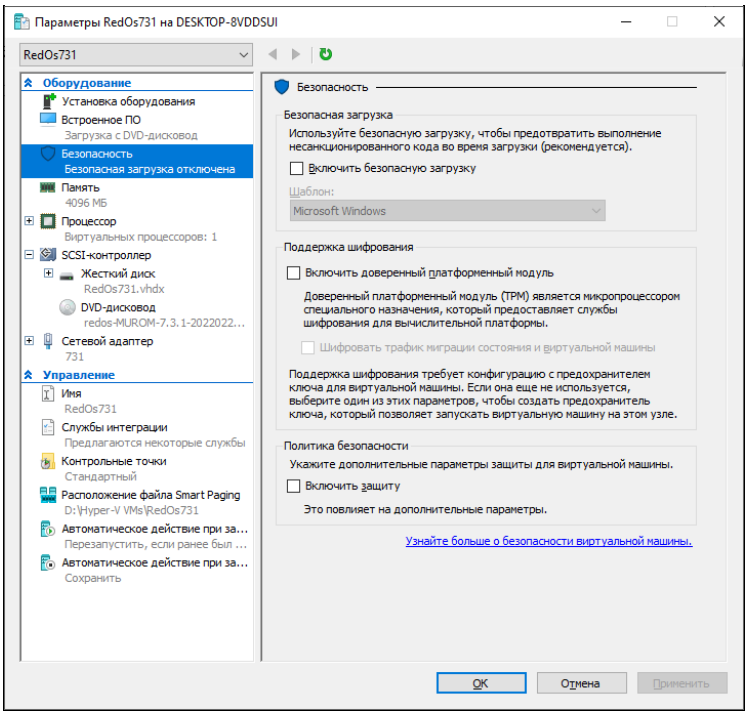
Кликните правой кнопки мыши по созданной виртуальной машине и выберите пункт «**Параметры**».



В пункте «**Установка оборудования**» выберите «**Сетевой адаптер**» и нажмите кнопку «**Добавить**». Выберите раннее созданный коммутатор.



В пункте «**Безопасность**» отключите безопасную загрузку.

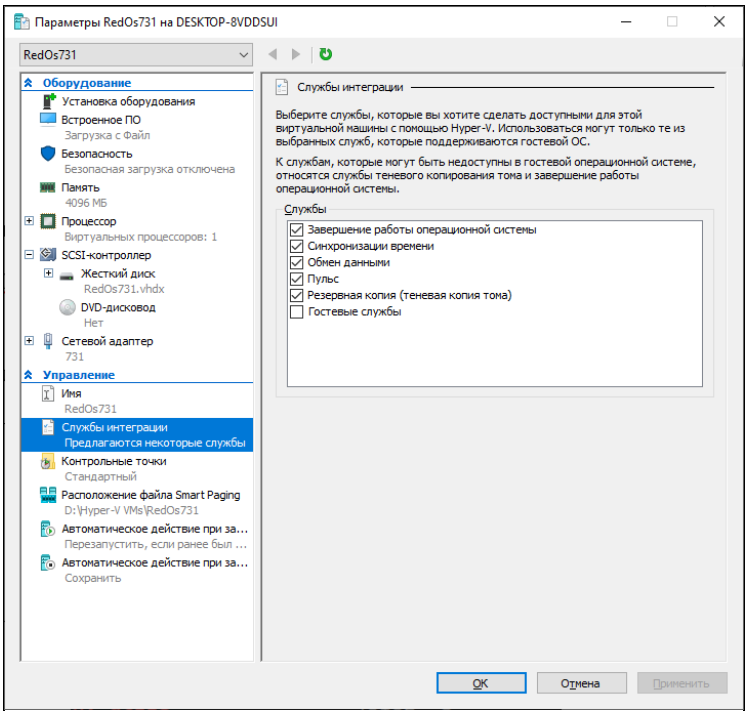


Службы интеграции Hyper-V

В РЕД ОС 7.3.1 работают службы интеграции **Hyper-V**.

Службы интеграции - это службы, позволяющие виртуальной машине связываться с узлом **Hyper-V**.

Чтобы перейти к меню управления службами интеграции, нажмите правой кнопкой мыши по ВМ, далее «**Параметры**» - «**Службы интеграции**».

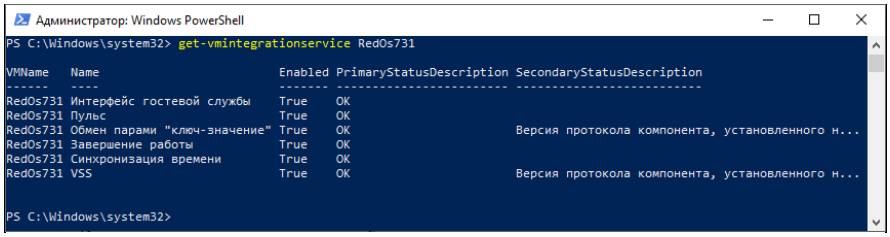


В данном меню можно включать или отключать службы интеграции.

Установите флажок в пункте «**Гостевые службы**».

Чтобы проверить состояние данных служб, в **PowerShell** введите команду:

```
get-vmintegrationservice <название_ВМ>
```

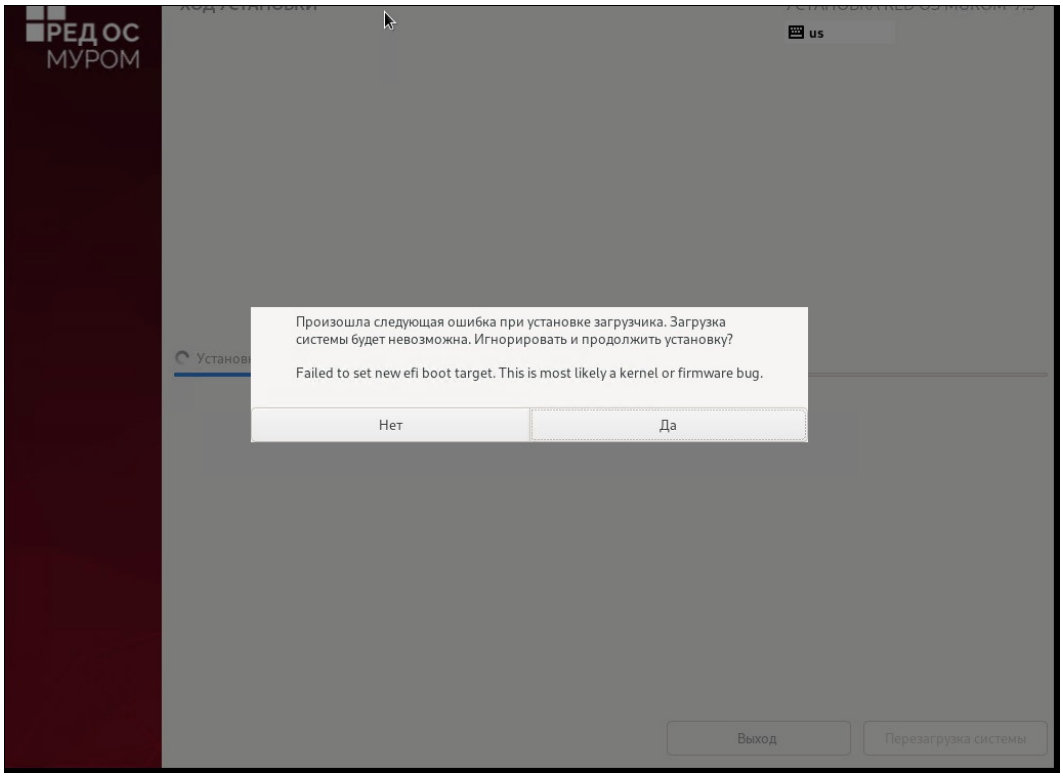


Все службы успешно работают.

После выполненных настроек запустите виртуальную машину и установите ОС в штатном режиме. Подробную информацию об установке системы см. по ссылке.

Примечание

В случае возникновения ошибки "Failed to set new efi boot target. This is most likely kernel or firmware bug. " ее можно проигнорировать и продолжить установку виртуальной машины:



На работоспособность ОС данная ошибка не влияет.

Взаимодействие Hyper-V с РЕД ОС 7.3

Изменение разрешения экрана
Служба обмена данными Hyper-V (KVP)
Служба запросов на теневое копирование томов Hyper-V
Интерфейс гостевой службы Hyper-V
Служба мониторинга состояния ВМ
Служба завершения работы в качестве гостя
Служба синхронизации времени

Изменение разрешения экрана

Чтобы изменить разрешение экрана, воспользуйтесь командой:

```
grubby --update-kernel=ALL --args="video=hyperv_fb:<разрешение_экрана>"
```

Перезапустите виртуальную машину.

Служба обмена данными Hyper-V (KVP)

Позволяет виртуальной машине и узлу обмениваться между собой простыми метаданными.

За работу службы обмена данными в системе РЕД ОС отвечает сервис **hypervkvpd.service**.

```
[user@localhost ~]$ systemctl status hypervkvpd.service
● hypervkvpd.service - Hyper-V KVP daemon
     Loaded: loaded (/usr/lib/systemd/system/hypervkvpd.service; static)
     Active: active (running) since Wed 2022-06-08 03:32:23 EDT; 1h 30min ago
   Main PID: 677 (hypervkvpd)
      Tasks: 1 (limit: 4667)
     Memory: 440.0K
        CPU: 3ms
     CGroup: /system.slice/hypervkvpd.service
             └─677 /usr/sbin/hypervkvpd -n

июн 08 03:32:23 localhost.localdomain systemd[1]: Started Hyper-V KVP daemon.
июн 08 03:32:24 localhost.localdomain KVP[677]: KVP starting; pid is:677
июн 08 03:32:24 localhost.localdomain KVP[677]: KVP LIC Version: 3.1
```

Служба запросов на теневое копирование томов Hyper-V

Позволяет службе теневого копирования томов выполнить резервное копирование виртуальной машины без ее выключения.

За работу данной службы в системе РЕД ОС отвечает сервис **hypervvssd.service**.

```
[user@localhost ~]$ systemctl status hypervvssd.service
● hypervvssd.service - Hyper-V VSS daemon
     Loaded: loaded (/usr/lib/systemd/system/hypervvssd.service; static)
     Active: active (running) since Wed 2022-06-08 03:32:23 EDT; 1h 32min ago
   Main PID: 678 (hypervvssd)
      Tasks: 1 (limit: 4667)
     Memory: 252.0K
        CPU: 866us
     CGroup: /system.slice/hypervvssd.service
             └─678 /usr/sbin/hypervvssd -n

июн 08 03:32:23 localhost.localdomain systemd[1]: Started Hyper-V VSS daemon.
июн 08 03:32:24 localhost.localdomain hypervvssd[678]: Hyper-V VSS: VSS starting; pid is:678
июн 08 03:32:24 localhost.localdomain hypervvssd[678]: Hyper-V VSS: VSS: kernel module version: 129
```

Интерфейс гостевой службы Hyper-V

Предоставляет интерфейс для узла **Hyper-V** для копирования файлов с виртуальной машины и на виртуальную машину.

За работу данной службы в системе РЕД ОС отвечает сервис **hypervfcopyd.service**.

```
[user@localhost ~]$ systemctl status hypervfcopyd.service
● hypervfcopyd.service - Hyper-V FCOPY daemon
     Loaded: loaded (/usr/lib/systemd/system/hypervfcopyd.service; static)
     Active: active (running) since Wed 2022-06-08 03:33:52 EDT; 1h 31min ago
   Main PID: 1459 (hypervfcopyd)
      Tasks: 1 (limit: 4667)
     Memory: 328.0K
        CPU: 2ms
     CGroup: /system.slice/hypervfcopyd.service
             └─1459 /usr/sbin/hypervfcopyd -n

июн 08 03:33:52 localhost.localdomain systemd[1]: Started Hyper-V FCOPY daemon.
июн 08 03:33:52 localhost.localdomain HV_FCOPY[1459]: starting; pid is:1459
июн 08 03:33:52 localhost.localdomain HV_FCOPY[1459]: kernel module version: 1
```

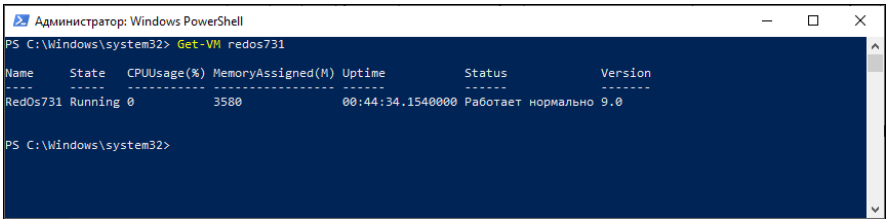
Служба мониторинга состояния ВМ

Сообщает узлу **Hyper-V**, что на виртуальной машине установлена операционная система и что она загрузилась надлежащим образом.

Чтобы увидеть статус виртуальной машины в **PowerShell** от имени администратора введите команду:

```
Get-VM <имя_виртуальной_машины>
```

За работу данной службы в системе РЕД ОС отвечает модуль **hv_utils**.



Служба завершения работы в качестве гостя

Позволяет узлу **Hyper-V** запрашивать завершение работы виртуальной машины. Компьютер виртуальной машины всегда может принудительно выключить виртуальную машину, но это похоже на нажатие кнопки выключения в отличие от корректного завершения работы.

У этой службы крайне высокая степень влияния на работу системы, т. к. при неработоспособности этой службы при каждом отключении узел не сможет корректно завершить работу ВМ, что может привести к потере или повреждению данных.

За работу данной службы в системе РЕД ОС отвечает модуль **hv_utils**.

Служба синхронизации времени

Синхронизирует системное время виртуальной машины с системным временем физического компьютера.

Эта служба также обладает высокой степенью влияния на работу, так как при каждом выключении ВМ время будет случайным образом меняться.

За работу данной службы в системе РЕД ОС отвечает модуль **hv_utils**.

Проверить, загружены ли модули, можно с помощью следующей команды:

```
lsmod | grep hv
```

```
[user@localhost ~]$ sudo lsmod|grep hv
hv_balloon             40960  0
hv_utils               49152  3
hv_netvsc              98304  0
hv_storvsc             24576  3
scsi_transport_fc      90112  1 hv_storvsc
hv_vmbus              143360  8 hv_balloon,hv_utils,hv_netvsc,hid_hyperv,hv_storvsc,hyperv_keyboard,
hyperv_drm,hyperv_fb
```

DOSBox - программный эмулятор DOS

Установка
Запуск программ
Файл конфигурации
Список горячих клавиш
Автозапуск программ
Исправление проблем

DOSBox - это программный эмулятор PC, создающий окружение **DOS**. Программа *DOSBox* является свободным программным обеспечением, которое позволяет запускать старые программы и игры на современных компьютерах и устройствах под управлением операционных систем *Windows, Linux, Android* и других.

Под *DOSBox* уверенно запустятся и будут работать различные файловые менеджеры времен **MS-DOS**, бухгалтерские и банковские программы, среды программирования, программы для радиолюбительских измерений и коммуникаций.

Установка

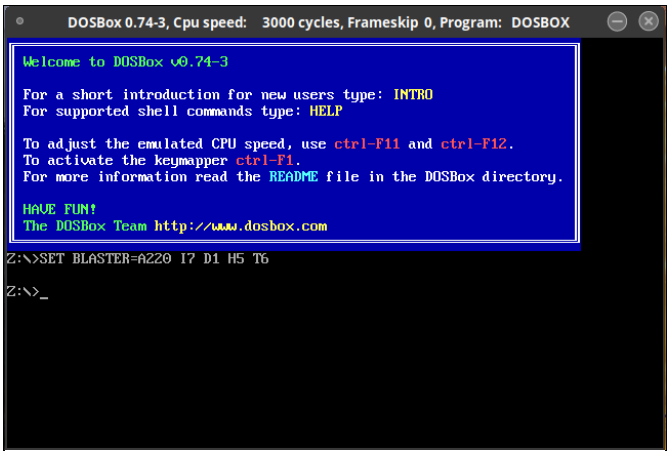
Установить *DOSBox* можно из репозитория РЕД ОС 7.3 командой:

```
dnf install dosbox
```

Запустить программу можно из *«Меню» → «Системные» → «DOSBox»* или из терминала командой:

```
dosbox
```

После запуска программы появится консоль *DOSBox*.



Запуск программ

Рассмотрим несколько вариантов запуска программ в эмуляторе *DOS*.
Первый и самый простой способ запуска программы - это ввести в терминале внешней ОС команду **dosbox**, а в качестве атрибута указать *путь к запускаемому файлу*.

Пример:

```
dosbox /home/user/Program/Doom/DOOMS/SETUP.EXE
```



Второй способ - это запустить *DOSBox* и производить все манипуляции с файлами уже через его терминал.

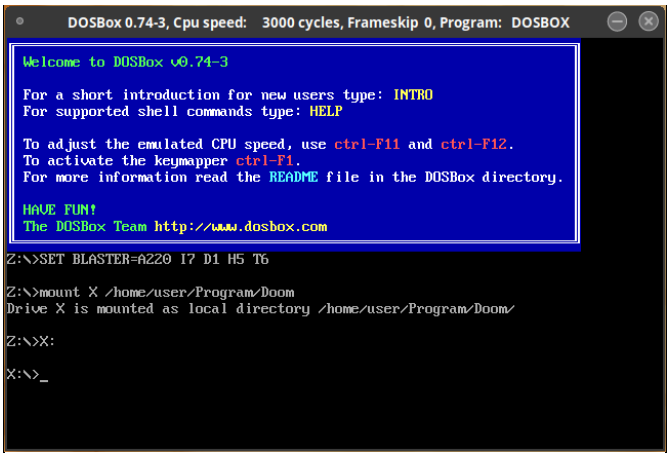
Для начала нам потребуется примонтировать каталог с программой, которую мы хотим запустить.

```
mount X /home/user/Program/DoomDrive X is mounted as local directory /home/user/Program/Doom/
```

Перейти в смонтированый каталог можно, введя:

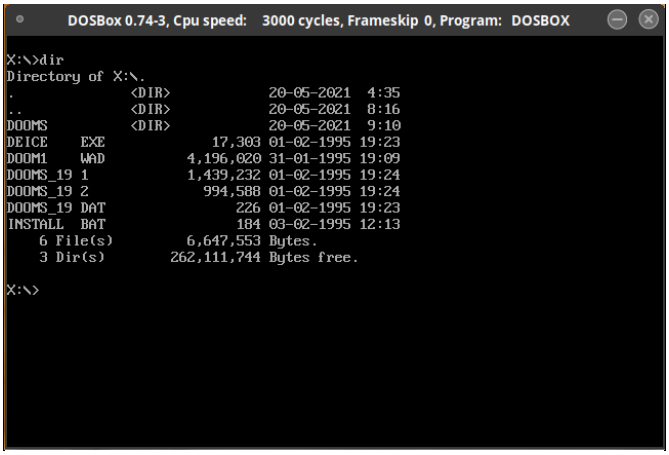
```
X:
```

где «X» - это имя диска, к которому был примонтирован каталог внешней ОС.



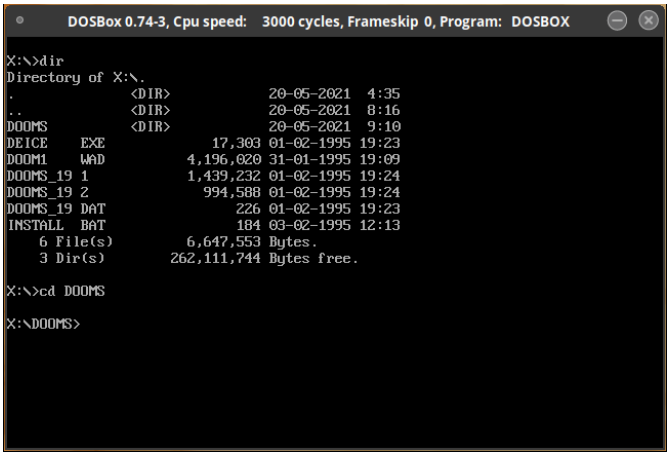
Вывод файлов в каталоге осуществляется командой:

```
dir
```



Перемещение по каталогам осуществляется командой **cd** . Например:

```
cd DOOMS
```

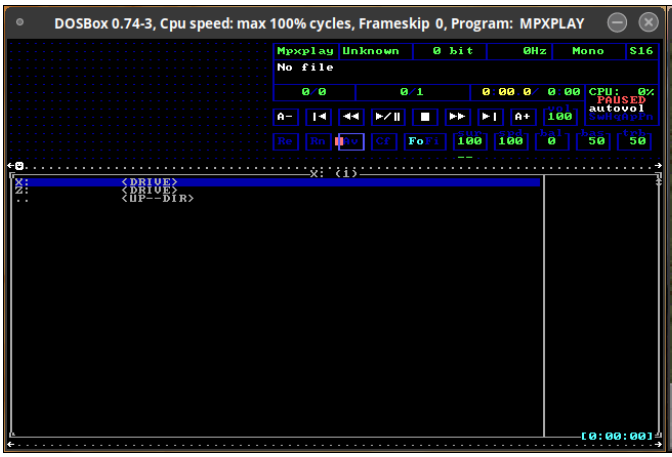


Для запуска программы необходимо ввести её название с расширением.

В данном случае команда будет выглядеть следующим образом:

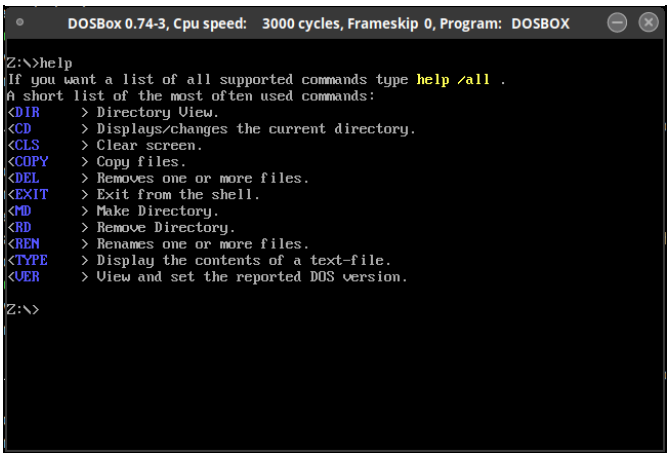
```
SETUP.EXE
```

Примеры запущенных программ





Также в DOSBox можно вывести список всех доступных команд. Для этого необходимо ввести **help**.



Файл конфигурации

Для каждой программы можно создать свой конфигурационный файл с уникальными для нее параметрами эмуляции.

После первого запуска *DOSBox* будет автоматически создан конфигурационный файл по умолчанию - **dosbox.conf**. Файл располагается **~/.dosbox**.

Для редактирования файлов конфигурации можно использовать любой текстовый редактор — **nano**, **pluma** и другие.

Чтобы запустить эмулятор с определенным конфигурационным файлом, нужно выполнить команду:

```
dosbox -conf  /
```

Например:

```
dosbox -conf  /home/user/Program/Doom/Dconf.conf
```

где **Dconf.conf** — имя конфигурационного файла.

Список горячих клавиш

Ниже приведен список основных горячих клавиш эмулятора:

1. «*ALT + ENTER*» - включение/выключение полноэкранного режима;
2. «*ALT + PAUSE*» - приостановка работы эмулятора *DosBox*;
3. «*CTRL + F1*» - запуск редактора горячих клавиш;
4. «*CTRL + F4*» - обновление кеша примонтированых директорий;
5. «*CTRL + ALT + F5*» - запуск и остановка захвата экрана с последующим сохранением в видеофайл;
6. «*CTRL + F5*» - захват и сохранение скриншота;
7. «*CTRL + F6*» - запуск и остановка записи звука в *Wav*-файл;
8. «*CTRL + ALT + F7*» - старт и остановка записи *OPL*-команд;

9. «*CTRL + ALT + F8*» - старт и остановка записи разных *MIDI*-команд;
10. «*CTRL + F7*» - уменьшить количество пропускаемых кадров;
11. «*CTRL + F8*» - увеличить количество пропускаемых кадров;
12. «*CTRL + F9*» - холодное выключение *DOSBox* (**kill**);
13. «*CTRL + F10*» - включение и отключение захвата мышки;
14. «*CTRL + F11*» - замедление эмулятора, уменьшение количества циклов микропроцессора;
15. «*CTRL + F12*» - ускорение эмулятора, увеличение количества циклов микропроцессора;
16. «*ALT + F12*» - отключение лимита скорости.

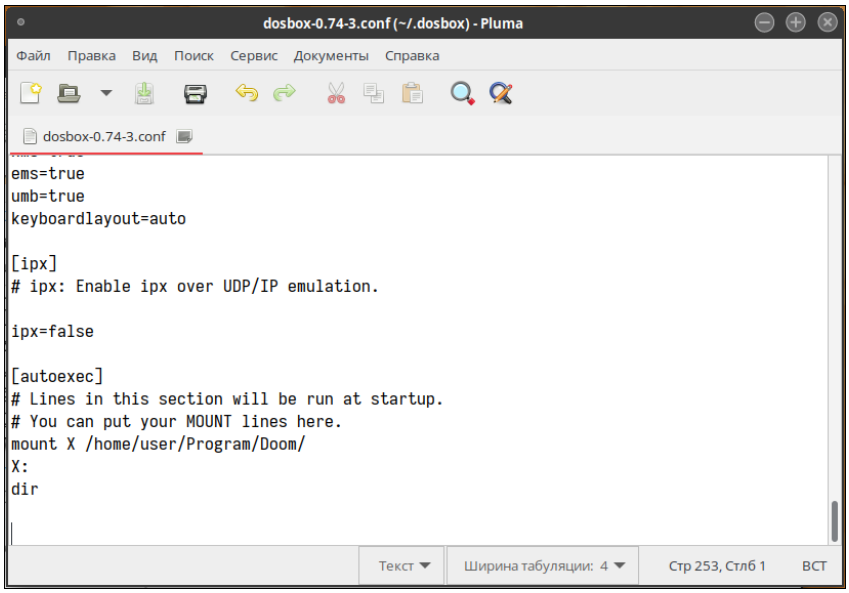
Автозапуск программ

Иногда полезно, чтобы при запуске эмулятора выполнялись определенные команды, например, монтирование каталога или запуск программ. В *DOSBox* это реализовано через файл конфигурации.

Чтобы задать команды для автостарта, в *DOSBox* нужно добавить список этих команд в конфигурационный файл в специальную секцию под названием **[autoexec]**.

Открываем в текстовом редакторе конфигурационный файл и ищем в конце секцию **[autoexec]** - все заданные там команды будут автоматически выполнены по порядку после запуска эмулятора.

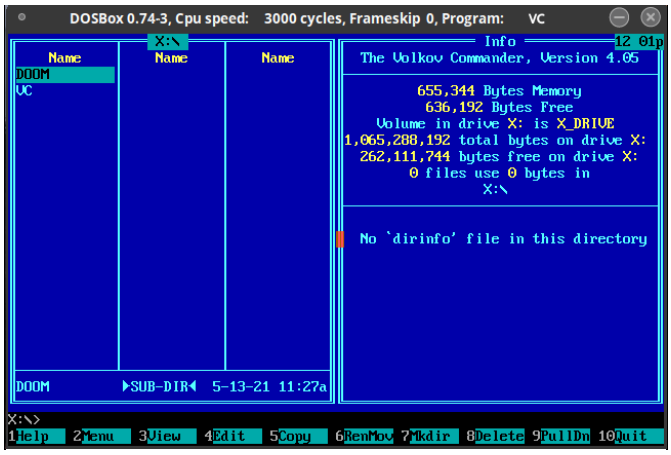
В примере настройка происходит в файле конфигурации **dosbox.conf**, используемом по умолчанию.



Для работы в более привычном формате можно добавить в автозагрузку оболочку типа **Volkov Commander** или **DOS Navigator**.

Распакуем *Volkov Commander* в директорию «*vc*», которая расположена в монтируемом каталоге *X*. Добавляем в конфигурационный файл примера, что приведен выше, строчку: «**x:/vc/vc.com**».

В показанном выше примере при запуске *DOSBox* автоматически примонтируется диск *X* и запустится *Volkov Commander*:



Исправление проблем

Для исправления неверного отображения символов кириллицы в *DOS* служат утилиты - руссификаторы клавиатуры.

В случае использования *DOSBox* достаточно добавить в конфигурационный файл в секцию **[autoexec]** строку:

```
keyb ru 866
```

После перезагрузки эмулятора проблема должна исчезнуть.

Установка и настройка docker

Установка docker
Доступ к среде контейнеризации
Команды docker
Настройка зеркал общедоступного хранилища образов Docker Hub
Реестр образов РЕД ОС
Базовые образы
Настройка собственного локального реестра docker-образов
Установка и настройка локального реестра docker-образов из репозитория РЕД ОС
Настройка локального реестра образов путем создания контейнера в docker
Загрузка docker-образов в локальный реестр
Настройка контейнеров для автоматического запуска в systemd
Установка Portainer
Установка Portainer из репозитория РЕД ОС
Установка Portainer путем создания контейнера в Docker
Автоматизированное создание контейнера

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: docker-ce-4:20.10.24-1, docker-ce-cli-1:20.10.24-1, registry-2.8.2-1, portainer-ce-2.18.3-2

Docker — программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации. Позволяет "упаковать" приложение со всем его окружением и зависимостями в контейнер, который может быть развернут на любой Linux-подобной системе с поддержкой контрольных групп в ядре, а также предоставляет набор команд для управления этими контейнерами.

Установка docker

Для установки средства контейнеризации необходимо выполнить команду (потребуются права **администратора**):

```
dnf install docker-ce docker-ce-cli
```

После успешной установки необходимо запустить сервис контейнеризации **docker** и добавить его в автозагрузку:

```
systemctl enable docker --now
```

Убедитесь, что сервис запущен, проверив статус запущенной службы:

```
systemctl status docker
```

В статусе должно быть отображено **active (running)**.

Для получения информации об установленном **docker** выполните команду:

```
docker info
```

При корректной настройке будет получен соответствующий ответ от сервиса **Docker**.

Доступ к среде контейнеризации

По умолчанию доступ к среде контейнеризации и запуску сервисов имеет только **суперпользователь**. Демон **docker** подключается к сокету Unix, к которому также имеет доступ только **суперпользователь**.

Для использования и управления средой контейнеризации **обычным** пользователем необходимо добавить его в отдельную группу, пользователям которой будет разрешено выполнять необходимые манипуляции. Такая группа создается в процессе установки среды контейнеризации и имеет название `docker`.

Добавьте необходимого пользователя в группу **docker** командой:

```
usermod -aG docker <имя_пользователя>
```

Проверить назначенные права можно, выполнив загрузку тестового образа с правами обычного пользователя:

```
docker info
```

При корректной настройке будет получен соответствующий ответ от сервиса **Docker**.

Команды docker

Часто используемые команды (аргументы команд для краткости не указаны):

Команда	Краткое описание
docker attach	Подключить стандартные каналы ввода-вывода (stdin, stdout, stderr) к активному контейнеру.
docker build	Построить Docker-образ из Docker-файла.
docker builder	Управление модулем построения Docker-образов.
docker commit	Создание нового Docker-образа из активного контейнера.
docker config	Управление конфигурациями Docker.
docker container	Управление контейнерами: • docker container create - создать новый контейнер; • docker container exec - выполнить команду в активном контейнере; • docker container run - выполнить команду в новом контейнере; • docker container start - активировать контейнер (контейнеры); • docker container stop - деактивация контейнера.
docker context	Управление контекстами Docker.
docker cp	Копирование файлов или каталогов между локальной файловой системой и файловой системой контейнера.
docker create	Создать новый изменяемый слой в указанном контейнере.
docker diff	Вывести список файлов и каталогов, изменённых с момента создания контейнера.
docker events	Вывести событий, произошедших с различными объектами Docker.
docker exec	Выполнить команду в активном контейнере.
docker export	Экспортировать файловую систему контейнера как архив формата tar.
docker history	Показать историю образа
docker image	Управление образами: • docker image build - создание нового образа.
docker images	Вывести список образов верхнего уровня.
docker import	Создать файловую систему образа из архива.
docker info	Вывод системной информации.
docker inspect	Вывод подробной информации об объектах Docker.
docker kill	Принудительно деактивировать активный контейнер (контейнеры).
docker load	Загрузить образ из архива tar или из стандартного ввода.
docker login	Войти в реестр образов.
docker logout	Выйти из реестра образов.
docker logs	Извлечь журналы контейнера.
docker manifest	Управление манифестами и списками манифестов Docker.
docker network	Управление сетями.
docker node	Управление узлами кластеров Docker.
docker pause	Приостановить все процессы в активном контейнере (контейнерах).
docker plugin	Управление плагинами.
docker port	Вывести список отображения портов контейнера.

docker ps	Вывести список активных контейнеров.
docker pull	Загрузить образ на локальный компьютер из реестра образов.
docker push	Загрузить образ с локального компьютера в реестр образов.
docker rename	Переименовать контейнер.
docker restart	Перезапустить контейнер (контейнеры).
docker rm	Удалить контейнер (контейнеры).
docker rmi	Удалить образ (образы).
docker run	Выполнить команду в новом контейнере, то есть: создать в существующем образе новый изменяемый слой, и выполнить команду, сохраняя изменения в этом слое. • docker run --rm - удалить новый (изменённый) слой после деактивации контейнера, т.е. сохранить образ неизменным.
docker save	Сохранить образ (образы) в архиве tar (через стандартный вывод по умолчанию).
docker search	Поиск образов Docker в сети Интернет.
docker secret	Управление паролями кластеров Docker.
docker service	Управление сервисами кластеров Docker.
docker stack	Управление стеками.
docker start	Запустить контейнер (контейнеры).
docker stats	Отобразить в режиме реального времени статистику потребления ресурсов контейнером.
docker stop	Остановить активный контейнер (контейнеры).
docker swarm	Управление кластерами Docker.
docker system	Управление службой Docker.
docker tag	Создать тег (метку) образа, ссылающийся на существующий образ.
docker top	Вывести список процессов активного контейнера.
docker trust	Управление ключами и подписями образов.
docker unpause	Продолжить выполнение приостановленного активного контейнера (контейнеров).
docker update	Обновить конфигурацию контейнера (контейнеров).
docker version	Отобразить версию Docker.
docker volume	Управление томами хранения данных для контейнеров.
docker wait	Ожидание завершения работы контейнера (контейнеров) и вывод кодов завершения.

Настройка зеркал общедоступного хранилища образов Docker Hub

При возникновении проблем с обращением к образам из общедоступного хранилища **Docker Hub** для обеспечения возможности продолжения корректной работы с образами рекомендуется настроить подготовленные зеркала.

Для настройки обращения **docker** к определенному зеркалу необходимо выполнить следующий алгоритм действий:

1а. В файл **/etc/docker/daemon.json** добавить строку вида:

```
"registry-mirrors": ["<адрес_зеркала>"]
```

где **<адрес_зеркала>** – адрес настроенного зеркала хранилища образов.

Например:

```
"registry-mirrors": ["https://mirror.gcr.io/"]
```

где **https://mirror.gcr.io/** – публичное зеркало хранилища образов **Docker Hub** от компании **Google**.

1б. Если файл **/etc/docker/daemon.json** пуст или не существует, внести строки вида:

```
{
 "registry-mirrors": ["<адрес_зеркала>"]
 }
```

где **<адрес_зеркала>** – адрес настроенного зеркала хранилища образов.

Например:

```
{
 "registry-mirrors": ["https://mirror.gcr.io/"]
 }
```

где **https://mirror.gcr.io/** – публичное зеркало хранилища образов **Docker Hub** от компании **Google**.

2. Перезапустить службу **docker**:

```
systemctl daemon-reload
systemctl restart docker
```

Реестр образов РЕД ОС

На пакетной базе РЕД ОС разработан ряд docker-образов и создан собственный реестр docker-образов — **registry.red-soft.ru/ubi7**.

Для получения списка доступных образов в реестре необходимо выполнить:

```
docker search registry.red-soft.ru/ubi7
```

Для установки требуемого образа из реестра необходимо выполнить:

```
docker pull registry.red-soft.ru/ubi7/<название_образа>
```

Базовые образы

Универсальные базовые образы (**UBI**) — это легковесная и безопасная основа для создания облачных и веб-приложений в контейнерах. На основе **UBI** можно создавать свои контейнерные приложения и собственные образы.

В реестре образов РЕД ОС на данный момент доступны следующие базовые образы:

- **ubi** – "урезанный образ", который использует **dnf** в качестве менеджера пакетов;
- **ubi-minimal** – еще более "урезанный" образ, который использует **microdnf** в качестве менеджера пакетов;
- **ubi-micro** – максимально "урезанный" образ, в котором отсутствует собственный менеджер пакетов. Для установки пакетов используется менеджер пакетов хостовой ОС, на котором разворачивается образ.

Также в реестре образов доступны образы типа **S2I** (*Source-to-Image*).

S2I — это процесс сборки для создания воспроизводимых образов контейнеров из исходного кода. **S2I** создает готовые к использованию образы на основе исходных кодов приложений, которые, в свою очередь, могут запускаться в виде собранного приложения.

В реестре образов РЕД ОС доступны следующие образы **S2I**:

- **s2i-core** — предоставляет образам инструменты, необходимые для использования функциональности *source-to-image*, сохраняя при этом минимальный размер образа;
- **s2i-base** — основан на *s2i-core*, предоставляет образам инструменты, необходимые для использования функциональности *source-to-image*, а также содержит различные библиотеки, которые служат основой для создания других **s2i**-образов — таких как *s2i-python*, *s2i-ruby*, *s2i-nodejs* и прочих.

Настройка собственного локального реестра docker-образов

В централизованном хранилище хранятся доступные docker-образы.

Одним из примеров общедоступных хранилищ образов является **Docker Hub**, по умолчанию *Docker* настроен на поиск образов в нем. Также есть возможность настройки своего собственного хранилища.

При использовании команд `docker pull` или `docker run` требуемые образы будут извлекаться из настроенного хранилища. Когда используется команда `docker push`, образ помещается в настроенное хранилище образов.

Установка и настройка локального реестра docker-образов из репозитория РЕД ОС

Для установки локального реестра docker-образов из репозитория РЕД ОС выполните команду:

```
dnf install registry
```

Запустите службу **registry**:

```
systemctl enable registry.service --now
```

Убедитесь, что служба активна, выполнив:

```
systemctl status registry.service
```

В статусе должно быть указано **active(running)**.

ВАЖНО!

Необходимо настроить демон **docker** на обращение к приватному реестру образов. Для этого добавьте в файл **/etc/docker/daemon.json** следующую строку:

```
"insecure-registries": ["127.0.0.1:5000"],
```

Локальный реестр docker-образов готов к использованию. Для проверки корректности настройки локального реестра см. п. «Загрузка docker-образов в локальный реестр».

Настройка локального реестра образов путем создания контейнера в docker

Для настройки локального хранилища образов путем использования контейнеров в реестре docker-образов РЕД СОФТ предоставлен образ **registry.red-soft.ru/ubi7/registry**, являющийся реализацией инструмента хранения и обмена образами *Docker Registry*.

Для создания локального хранилища образов запустите контейнер на основе образа **registry.red-soft.ru/ubi7/registry** командой:

```
docker run -d -p 5000:5000 --restart=always --name test_reg_2 registry.red-soft.ru/ubi7/registry:latest
```

где:

- `-p 5000:5000` — порт для обращения к реестру по умолчанию;
- `--restart=always` — автоматический запуск контейнера после перезапуска хостовой ОС;
- `--name test_reg_2` — имя контейнера;
- `registry.red-soft.ru/ubi7/registry:latest` — необходимый образ.

Локальный реестр образов готов к использованию. Для проверки корректности настройки локального реестра см. п. «Загрузка docker-образов в локальный реестр».

Изменение расположения хранилища образов

Локальное хранилище образов является контейнером и хранит образы внутри себя в каталоге **/var/lib/registry**. Однако при переустановке контейнера все данные внутри него будут уничтожены. Для избежания потери данных к контейнеру необходимо подключить внешнее хранилище данных.

Для этого на хостовой ОС сначала следует создать каталог, предназначенный для хранения образов:

```
mkdir /reg_images
```

Далее необходимо остановить и уничтожить имеющийся контейнер с локальным хранилищем:

```
docker container stop test_reg_2 && docker container rm -v test_reg_2
```

После этого следует запустить контейнер снова с дополнительным ключом, который отвечает за подключение к нему ранее созданного каталога:

```
docker run -d -p 5000:5000 --restart=always --name test_reg_2 -v /reg_images:/var/lib/registry registry.red-soft.ru/ubi7/registry:latest
```

где:

- `-p 5000:5000` — порт для обращения к реестру по умолчанию;
- `--restart=always` — автоматический запуск контейнера после перезапуска хостовой ОС;
- `--name test_reg_2` — имя контейнера;
- `-v /reg_images:/var/lib/registry` — подключение каталога **/reg_images** к контейнеру в качестве каталога **/var/lib/registry**;
- `registry.red-soft.ru/ubi7/registry:latest` — необходимый образ.

Для проверки корректности настройки локального хранилища образов в качестве примера будет загружен образ **nodejs-18** из реестра образов РЕД СОФТ **registry.red-soft.ru/ubi7**:

```
docker pull registry.red-soft.ru/ubi7/nodejs-18
```

Далее будет добавлен тег к загруженному образу:

```
docker tag registry.red-soft.ru/ubi7/nodejs-18 localhost:5000/js18_test:latest
```

Затем образ загружается в локальное хранилище:

```
docker push localhost:5000/js18_test:latest

The push refers to repository [localhost:5000/js18_test]
0932ece797fa: Pushed
6512634988ef: Pushed
526374a3d4d5: Pushed
latest: digest: sha256:fe07d0235d269961ba25f5853809ff81807f52d0aa75a77e51899a540975a675 size: 954
```

Проверка наличия загруженного образа в созданном каталоге **/reg_images**:

```
ls /reg_images/docker/registry/v2/repositories/

js18_test
```

Локальное хранилище с подключенным внешним каталогом успешно работает.

Загрузка docker-образов в локальный реестр

Для загрузки образа *docker* в локальное хранилище необходимо сперва создать тег образа, ссылающийся на существующий образ (в примере использован образ **ubi-minimal** из реестра образов РЕД СОФТ **registry.red-soft.ru/ubi7**), командой:

```
docker tag registry.red-soft.ru/ubi7/ubi-minimal localhost:5000/test_reg
```

где:

- `registry.red-soft.ru/ubi7/ubi-minimal` — имеющийся образ *docker*;
- `localhost` — имя или IP-адрес хостовой ОС;
- `5000` — порт для обращения к реестру по умолчанию;
- `test_reg` — новое имя образа.

Убедитесь, что тег образа был успешно создан:

```
docker images

REPOSITORY                          TAG      IMAGE ID       CREATED        SIZE
localhost:5000/test_reg             latest   60d2a5f5b971   24 hours ago   102MB
registry.red-soft.ru/ubi7/ubi-minimal latest   60d2a5f5b971   24 hours ago   102MB
```

После этого образ можно загрузить в локальное хранилище командой:

```
docker push localhost:5000/test_reg:latest
```

Ответ команды должен выглядеть примерно следующим образом:

```
The push refers to repository [localhost:5000/test_reg]
00983af53c2c: Pushed
latest: digest: sha256:fde90838c647d829131f124a6d87801ac28c2a05619efff983dde04e1d6c16c3 size: 529
```

В корректности загрузки docker-образов в локальный реестр можно убедиться, удалив имеющиеся образы из *docker* (следующие команды удаляют образы из *docker*, но не затрагивают образы в локальном реестре):

```
docker image remove registry.red-soft.ru/ubi7/ubi-minimal

Untagged: registry.red-soft.ru/ubi7/ubi-minimal:latest
Untagged: registry.red-soft.ru/ubi7/ubi-minimal@sha256:fde90838c647d829131f124a6d87801ac28c2a05619efff983dde04e1d6c16c3

docker image remove localhost:5000/test_reg

Untagged: localhost:5000/test_reg:latest
Untagged: localhost:5000/test_reg@sha256:fde90838c647d829131f124a6d87801ac28c2a05619efff983dde04e1d6c16c3
Deleted: sha256:60d2a5f5b971ce5a1938d692175ece7416e148394f0d3987c9ff7e80b88e3e66
Deleted: sha256:00983af53c2c493b01c7f747c4197794c6250140357fba2cfbc0fb0c312162c0

docker images

REPOSITORY TAG IMAGE ID CREATED SIZE
```

Примечание.

При загрузке docker-образов в локальный реестр, настроенный как контейнер *docker*, установленный образ **registry.red-soft.ru/ubi7/registry** удалять не нужно!

После этого загрузите образ из локального реестра командой:

```
docker pull localhost:5000/test_reg

Using default tag: latest
latest: Pulling from test_reg
ebc434fd7dc8: Pull complete
Digest: sha256:fde90838c647d829131f124a6d87801ac28c2a05619efff983dde04e1d6c16c3
Status: Downloaded newer image for localhost:5000/test_reg:latest
localhost:5000/test_reg:latest

docker images

REPOSITORY              TAG      IMAGE ID       CREATED        SIZE
localhost:5000/test_reg   latest   60d2a5f5b971   24 hours ago   102MB
```

Локальный реестр образов работает корректно.

Настройка контейнеров для автоматического запуска в systemd

Бывают ситуации, когда контейнеры могут быть остановлены вследствие определенных факторов. Для того чтобы остановленные контейнеры не приходилось запускать вручную, можно использовать настройку их автоматического запуска.

Далее будет рассмотрен пример настройки автоматического запуска локального реестра **registry**, настроенного как контейнер с именем **test_reg_systemd** и внешним каталогом для хранения образов **/reg_images_sys**.

Примечание.

Настройка автоматического запуска контейнера через службу **systemd** актуальна только в тех случаях, когда при запуске контейнера командой `docker run` не была использована опция `--restart=always`.

Предварительно был создан внешний каталог для хранения образов **/reg_images_sys** и запущен контейнер с локальным хранилищем следующими командами:

```
mkdir /reg_images_sys
docker run -d -p 5000:5000 --name test_reg_systemd -v /reg_images_sys:/var/lib/registry registry.red-soft.ru/ubi7/registry:latest
```

После запуска контейнера **registry** необходимо создать файл настройки для службы **systemd** со следующим содержимым:

```
nano /etc/systemd/system/registry.service
```

```
[Unit]
Description=registry container
Requires=docker.service
After=docker.service

[Service]
Restart=always
ExecStart=/usr/bin/docker start -a test_reg_systemd
ExecStop=/usr/bin/docker stop -t 15 test_reg_systemd
TimeoutSec=30

[Install]
WantedBy=multi-user.target
```

Сохраните изменения в файле и закройте его.

После этого необходимо запустить настроенную службу и добавить ее в автозагрузку командой:

```
systemctl enable registry.service --now
```

Проверьте статус службы:

```
systemctl status registry.service
```

В статусе должно быть указано **active(running)**.

После перезагрузки хостовой ОС проверьте статус контейнера командой:

```
docker ps -a
```

В графе **STATUS** должно отображаться **Up**:

```
CONTAINER ID   IMAGE                                  COMMAND                  CREATED         STATUS         PORTS                                       NAMES
5cee2dc6e925   registry.red-soft.ru/ubi7/registry:latest   "entrypoint.sh /etc/..."   20 minutes ago   Up 49 seconds   0.0.0.0:5000->5000/tcp,
:::5000->5000/tcp   test_reg_systemd
```

Установка Portainer

Установка **Portainer** доступна как из репозитория РЕД ОС, так и с помощью **docker** путем создания контейнера **portainer**.

Установка Portainer из репозитория РЕД ОС

Для установки **portainer** из репозитория РЕД ОС выполните команду (потребуются права **администратора**):

```
dnf install portainer-ce
```

Запустите службу **portainer**:

```
systemctl enable portainer.service --now
```

Убедитесь, что служба активна, выполнив:

```
systemctl status portainer.service
```

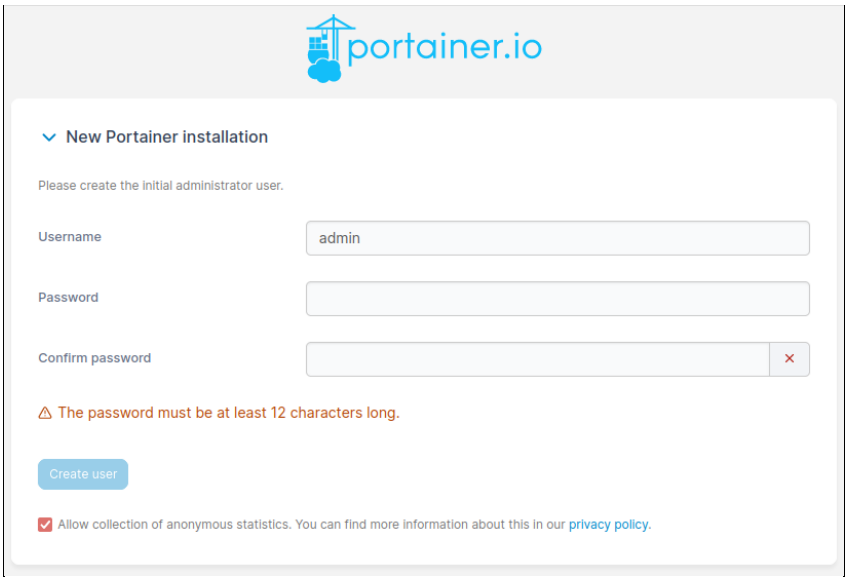
В статусе должно быть указано **active(running)**.

ВАЖНО!

Для корректной работы в **Portainer** должен быть установлен и активен **docker**.

Получить доступ к **Portainer** можно через веб-интерфейс на порту **9443**. Для этого в адресной строке браузера пропишите **https://localhost:9443**.

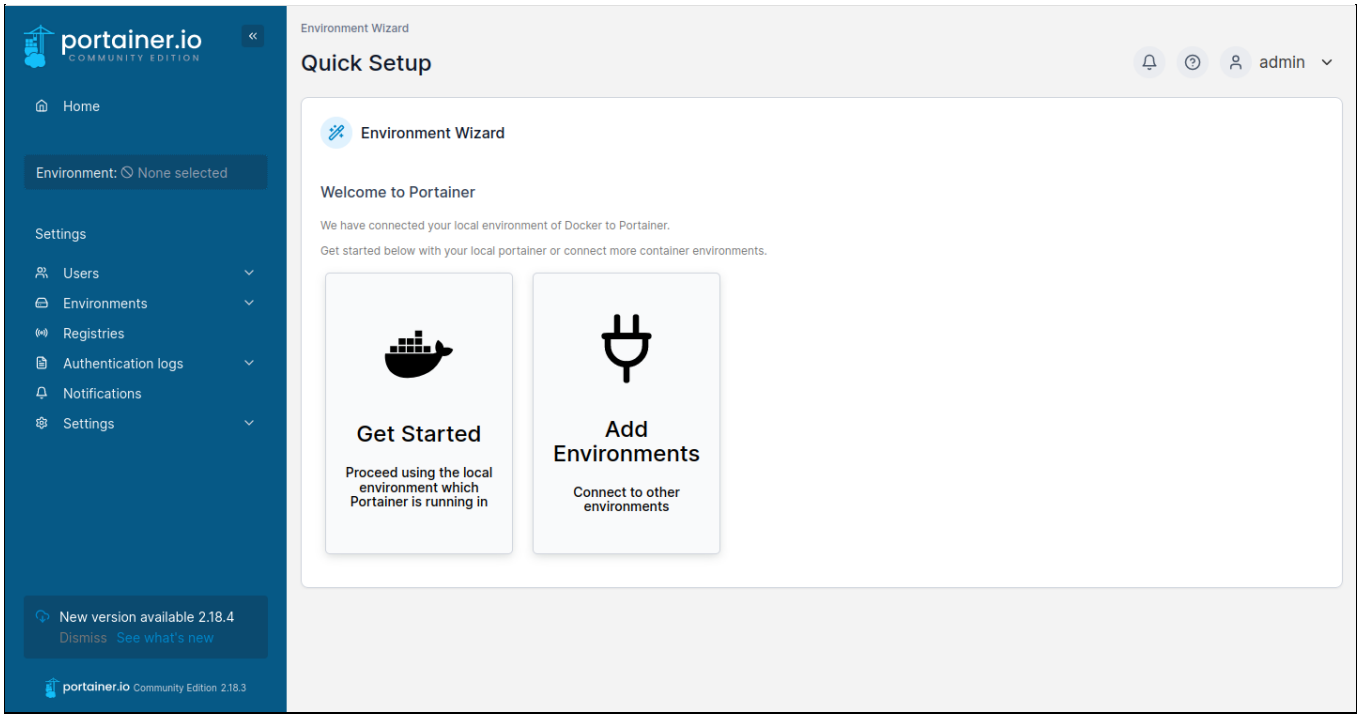
Будет открыта страница с веб-интерфейсом **portainer** и формой для создания пользователя, под которым будет производиться вход в систему.

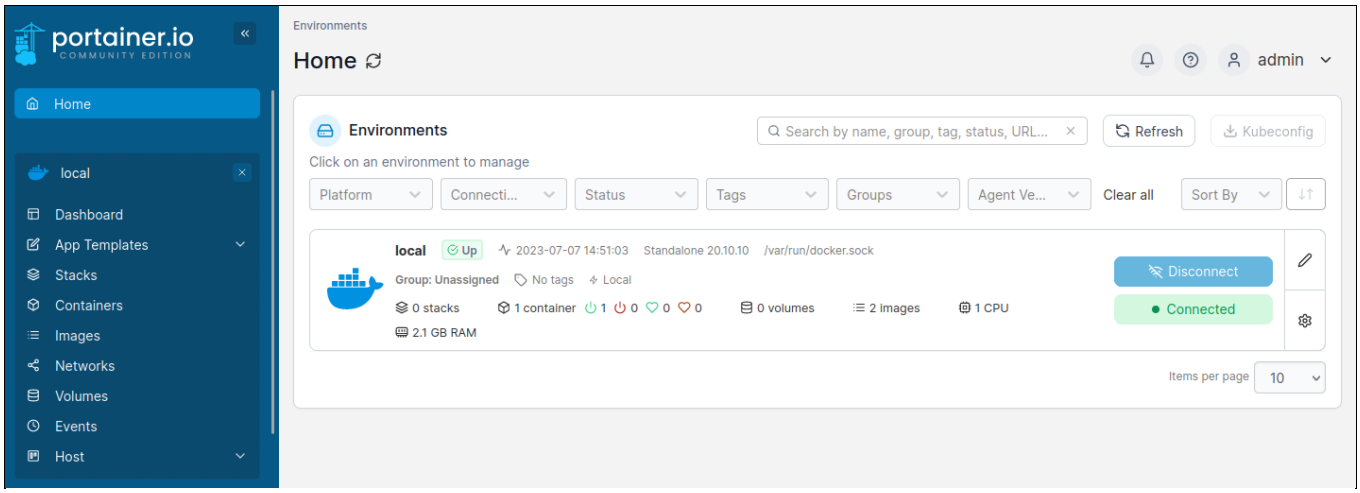


В форме необходимо задать сложный пароль длиной *не менее 12 символов*.

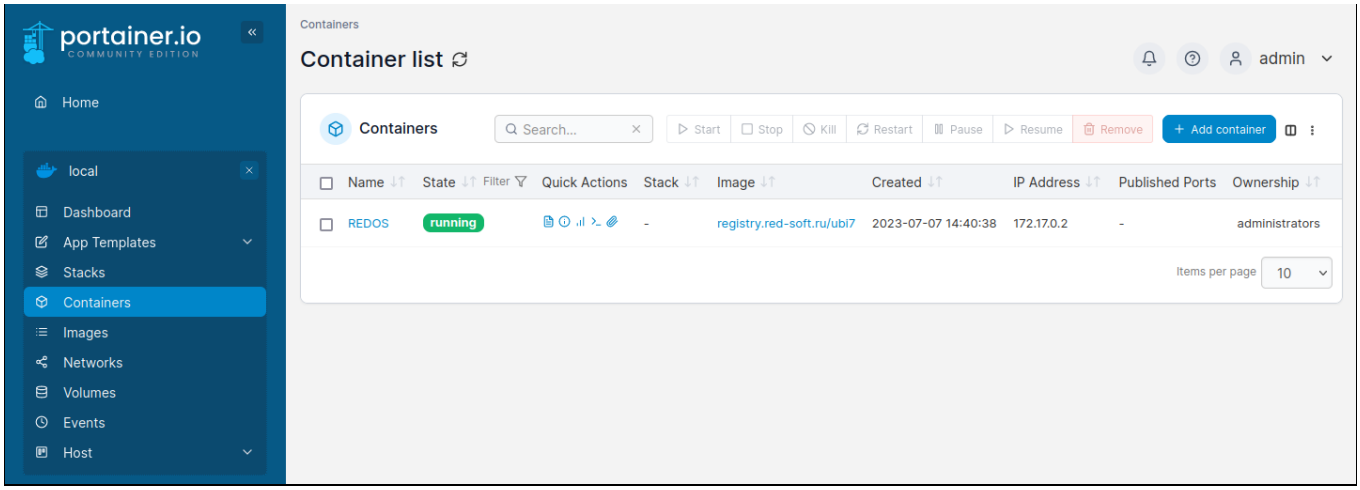
После того, как имя пользователя и пароль заданы, следует нажать «**Create user**».

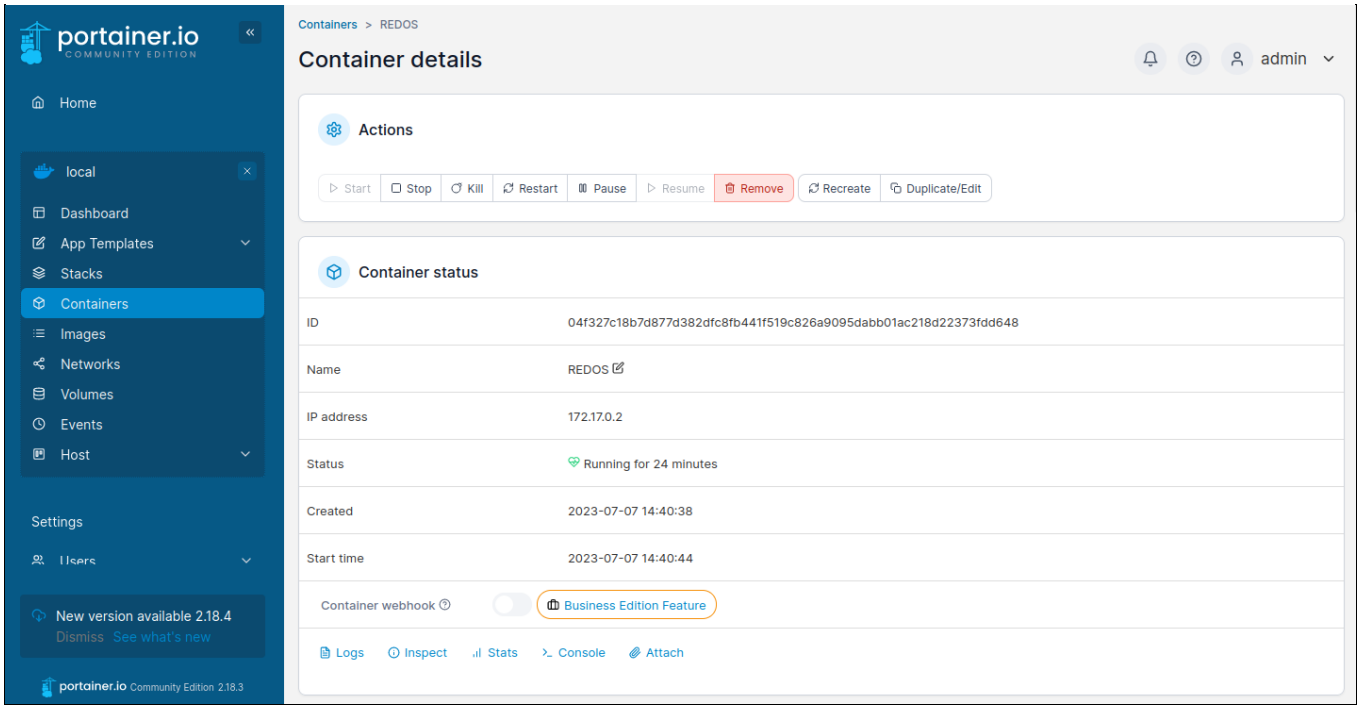
Далее будет открыта приветственная страница, где нужно выбрать «**Get started**», после чего откроется панель управления, где будет отображено локальное окружение, в котором хранятся установленные контейнеры.





На вкладке «**Containers**» представлены все доступные контейнеры. При выборе контейнера будет открыта страница с подробными сведениями.





Установка Portainer путем создания контейнера в Docker

Для развертывания контейнера с **Portainer** необходимо сначала создать хранилище данных командой:

```
docker volume create portainer_data
```

Затем для установки и запуска контейнера следует выполнить команду:

```
docker run -d -p 8000:8000 -p 9000:9000 --name=portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v
portainer_data:/var/lib/portainer/data registry.red-soft.ru/ubi7/portainer
```

Получить доступ к **Portainer** можно через веб-интерфейс на порту **9000**. Для этого в адресной строке браузера пропишите https://localhost:9000. Будет открыта страница с веб-интерфейсом **portainer**. Подробнее о веб-интерфейсе **portainer** см. выше.

Автоматизированное создание контейнера

Для автоматизированного создания контейнера необходимо создать скрипт со следующим содержимым:

nano create_minimal_image_moby.sh

```
#!/usr/bin/env bash
#
# Create a base RedOS Docker image.
#
# This script is useful on systems with yum installed (e.g., building
# a RedOS image on RedOS).
### version is 7.3

set -e

usage() {
 cat << EOOPTS
$(basename $0) [OPTIONS]
OPTIONS:
  -p ""  The list of packages to install in the container.
                The default is blank. Can use multiple times.
  -g ""    The groups of packages to install in the container.
                The default is "Core". Can use multiple times.
  -y      The path to the yum config to install packages from. The
                default is /etc/yum.conf for Redos 7.1/7.2 and /etc/dnf/dnf.conf for Redos 7.3
  -t          Specify Tag information.
                default is referred at /etc/{redos,system}-release
EOOPTS
 exit 1
}

# option defaults
yum_config=/etc/yum.conf
if [ -f /etc/dnf/dnf.conf ] && command -v dnf &> /dev/null; then
 yum_config=/etc/dnf/dnf.conf
 alias yum=dnf
fi
# for names with spaces, use double quotes (") as install_groups=('Core' '"Compute Node"')
install_groups=()
install_packages=()
version=
while getopts ":y:p:g:t:h" opt; do
 case $opt in
  y)
   yum_config=$OPTARG
   ;;
  h)
   usage
   ;;
  p)
   install_packages+=("$OPTARG")
   ;;
  g)
   install_groups+=("$OPTARG")
   ;;
  t)
   version="$OPTARG"
   ;;
  \?)
   echo "Invalid option: -$OPTARG"
   usage
   ;;
```

```
 esac
done
shift $((OPTIND - 1))
name=$1

if [[ -z $name ]]; then
 usage
fi

# default to Core group if not specified otherwise
if [ ${#install_groups[*]} -eq 0 ]; then
 install_groups=('Core')
fi

target=$(mktemp -d --tmpdir $(basename $0).XXXXXX)

set -x

mkdir -m 755 "$target"/dev
mknod -m 600 "$target"/dev/console c 5 1
mknod -m 600 "$target"/dev/initctl p
mknod -m 666 "$target"/dev/full c 1 7
mknod -m 666 "$target"/dev/null c 1 3
mknod -m 666 "$target"/dev/ptmx c 5 2
mknod -m 666 "$target"/dev/random c 1 8
mknod -m 666 "$target"/dev/tty c 5 0
mknod -m 666 "$target"/dev/tty0 c 4 0
mknod -m 666 "$target"/dev/urandom c 1 9
mknod -m 666 "$target"/dev/zero c 1 5

# amazon linux yum will fail without vars set
if [ -d /etc/yum/vars ]; then
 mkdir -p -m 755 "$target"/etc/yum
 cp -a /etc/yum/vars "$target"/etc/yum/
fi

if [[ -n "$install_groups" ]]; then
 yum -c "$yum_config" --installroot="$target" --releasever=/ --setopt=tsflags=nodocs \
  --setopt=group_package_types=mandatory -y groupinstall "${install_groups[@]}"
fi

if [[ -n "$install_packages" ]]; then
 yum -c "$yum_config" --installroot="$target" --releasever=/ --setopt=tsflags=nodocs \
  --setopt=group_package_types=mandatory -y install "${install_packages[@]}"
fi

yum -c "$yum_config" --installroot="$target" -y clean all

cat > "$target"/etc/sysconfig/network << EOF
NETWORKING=yes
HOSTNAME=localhost.localdomain
EOF

# effectively: febootstrap-minimize --keep-zoneinfo --keep-rpmdb --keep-services "$target".
#  locales
rm -rf "$target"/usr/{{lib,share}/locale,{lib,lib64}/gconv,bin/localedef,sbin/build-locale-archive}
#  docs and man pages
rm -rf "$target"/usr/share/{man,doc,info,gnome/help}
#  cracklib
rm -rf "$target"/usr/share/cracklib
#  i18n
rm -rf "$target"/usr/share/i18n
#  yum cache
rm -rf "$target"/var/cache/yum
mkdir -p --mode=0755 "$target"/var/cache/yum
#  sln
rm -rf "$target"/sbin/sln
#  ldconfig
rm -rf "$target"/etc/ld.so.cache "$target"/var/cache/ldconfig
mkdir -p --mode=0755 "$target"/var/cache/ldconfig

if [ -z "$version" ]; then
 for file in "$target"/etc/{redos,system}-release; do
```

```
  if [ -r "$file" ]; then
   version="$(sed 's/^[^0-9\]*\([0-9.]\+\).*$/\1/' "$file")"
   break
  fi
 done
fi

if [ -z "$version" ]; then
 echo >&2 "warning: cannot autodetect OS version, using '$name' as tag"
 version=$name
fi

tar --numeric-owner -c -C "$target" . | docker import - $name:$version

docker run -i -t --rm $name:$version /bin/bash -c 'echo success'

rm -rf "$target"
```

Затем необходимо предоставить скрипту права на исполнение командой:

```
chmod +x ./create_minimal_image_moby.sh
```

При запуске скрипта будет выдан краткий мануал по его использованию:

```
./create_minimal_image_moby.sh

create_minimal_image_moby.sh [OPTIONS] <name>
OPTIONS:
  -p "<packages>"  The list of packages to install in the container.
                   The default is blank. Can use multiple times.
  -g "<groups>"    The groups of packages to install in the container.
                   The default is "Core". Can use multiple times.
  -y <yumconf>     The path to the yum config to install packages from. The
                   default is /etc/yum.conf for Redos 7.1/7.2 and /etc/dnf/dnf.conf for Redos 7.3
  -t <tag>         Specify Tag information.
                   default is referred at /etc/{redos,system}-release
```

Вы можете указать дополнительные опции, как описано выше, или указать только имя контейнера, который требуется создать.

Пример:

```
./create_minimal_image_moby.sh ro73
```

В результате выполнения данный образ станет доступен при просмотре имеющихся образов:

```
docker images -a

REPOSITORY                          TAG       IMAGE ID       CREATED          SIZE
ro73                                7.3.2     ca3c44d23c7c   10 seconds ago   396MB
registry.red-soft.ru/ubi7/ubi-minimal   latest    ce2ca5ca47d4   4 weeks ago      102MB
registry.red-soft.ru/ubi7               latest    4e5d2ab41464   4 weeks ago      242MB
...
```

Kubernetes. Основные понятия

Kubernetes — это программная платформа для автоматического управления контейнеризованными приложениями. Она предлагает базовые механизмы для их развертывания, масштабирования и поддержки.

Nodes (узлы, ноды) - физические или виртуальные машины, на которых разворачиваются и запускаются контейнеры с приложениями. Совокупность нод образует кластер Kubernetes.

Nodes бывают двух типов:

Master (мастер-нода) — узел, управляющий всем кластером. Он отслеживает остальные ноды и распределяет между ними нагрузку с помощью менеджера контроллеров и планировщика. Обычно *master* занимается только управлением и не берет на себя рабочие нагрузки. Для повышения отказоустойчивости необходимо наличие нескольких мастер-нод.

Worker (рабочие ноды) — узлы, на которых работают контейнеры. В зависимости от параметров ноды (объема памяти и центрального процессора) на одном узле может работать большое количество контейнеров. Чем больше рабочих узлов, тем больше приложений можно запустить. Также количество влияет на отказоустойчивость кластера, потому что при выходе из строя одной ноды нагрузка переносится на другие.

Установка kubernetes с использованием контейнерного движка containerd

Настройка Master-node
Настройка рабочих нод
Подключение worker к кластеру
Полезные команды

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** kubernetes-1.24.12-1, kubernetes-kubeadm-1.24.12-1

Для дальнейшей настройки необходимо перейти в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Настройка Master-node

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

```
swapoff -a
```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

```
swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **containerd**:

```
nano /etc/modules-load.d/containerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-tools tc ipvsadm ebtables socat conntrack git curl wget runc containerd
```

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Установите настройки по умолчанию для конфигурации контейнера:

```
containerd config default | sudo tee /etc/containerd/config.toml
```

7. Для разрешения использования **cgroup** переключите флаг параметра systemdCgroup в конфигурационном файле **/etc/containerd/config.toml**:

```
sed -i 's/SystemdCgroup \= false/SystemdCgroup \= true/g' /etc/containerd/config.toml
```

8. Запустите службу **containerd** и добавьте ее в автозагрузку:

```
systemctl enable --now containerd
```

9. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

10. Загрузите образы контейнеров, необходимых **kubeadm** для инициализации ноды кластера:

```
kubeadm config images pull
```

11. Запустите инициализацию мастер-ноды в одноранговом кластере. Данная команда выполнит начальную настройку и подготовку основного узла кластера. Ключ **--pod-network-cidr** задает адрес внутренней подсети для вашего кластера.

```
kubeadm init --pod-network-cidr=10.244.0.0/16
```

В случае успешной инициализации, в конце вывода команды будет отображаться примерно следующее:

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 192.168.186.86:6443 --token kb0ejg.qtsdbljcnfcc3acd \
 --discovery-token-ca-cert-hash sha256:92d275184e764076086f4cc86bca47f6ecedd46526568cc494d97dc27958bec7
```

12. Настройте параметры управления кластером. Настройку можно выполнить как для локального пользователя, так и для суперпользователя root.

Для управления кластером от имени локального пользователя выполните команды:

```
mkdir /home/$USER/.kube
cp -i /etc/kubernetes/admin.conf /home/$USER/.kube/config
chown $USER. /home/$USER/.kube /home/$USER/.kube/config
```

Для управления кластером от имени суперпользователя root выполните команды:

```
echo "export KUBECONFIG=/etc/kubernetes/admin.conf" >> /root/.bashrc
source .bashrc
export KUBECONFIG=/etc/kubernetes/admin.conf
```

Примечание.

Если настройка производилась для локального пользователя, выйдите из сеанса пользователя **root** командой exit и дальнейшие действия по настройке кластера выполняйте от имени локального пользователя.

13. Установите внутреннюю конфигурацию сети в кластере (в примере используется **calico**).

```
kubectl apply -f https://raw.githubusercontent.com/projectcalico/calico/v3.25.0/manifests/calico.yaml
```

14. Проверьте список и статус всех подов в кластере:

```
kubectl get pod -n kube-system
```

15. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname masternode
```

Проверьте изменения:

```
hostname && hostname -I

masternode192.168.186.86
```

16. В файл **/etc/hosts** внесите данные о master-node и рабочих nodes:

```
sudo nano /etc/hosts
```

```
192.168.186.86 masternode
 192.168.186.106 worker
```

Для вывода команды присоединения рабочих node к кластеру выполните:

```
kubeadm token create --print-join-command

kubeadm join 10.81.186.86:6443 --token kb0ejg.qtsdbljcnfcc3acd --discovery-token-ca-cert-hash
sha256:92d275184e764076086f4cc86bca47f6ecedd46526568cc494d97dc27958bec7
```

Настройка рабочих нод

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **containerd**:

```
nano /etc/modules-load.d/containerd.conf
```

```
overlay
 br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
 net.ipv4.ip_forward = 1
 net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-tools tc ipvsadm ebtables socat conntrack git curl wget runc containerd
```

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Установите настройки по умолчанию для конфигурации контейнера:

```
containerd config default | sudo tee /etc/containerd/config.toml
```

7. Для разрешения использования **cgroup** переключите флаг параметра systemdCgroup в конфигурационном файле **/etc/containerd/config.toml**:

```
sed -i 's/SystemdCgroup \= false/SystemdCgroup \= true/g' /etc/containerd/config.toml
```

8. Запустите службу **containerd** и добавьте ее в автозагрузку:

```
systemctl enable --now containerd
```

9. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

10. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname worker
```

Проверьте изменения:

```
 hostname && hostname -I

worker192.168.186.106
```

11. В файл **/etc/hosts** внесите данные о *master* и *worker*:

```
sudo nano /etc/hosts
```

```
192.168.186.86 masternode
 192.168.186.106 worker
```

После этого можно приступать к присоединению *worker* к кластеру.

Подключение worker к кластеру

1. На master-ноде получите команду присоединения *worker*:

```
kubeadm token create --print-join-command

kubeadm join 192.168.186.86:6443 --token l1py3b.pboa64i6uoz63hzp --discovery-token-ca-cert-hash
sha256:92d275184e764076086f4cc86bca47f6ecedd46526568cc494d97dc27958bec7
```

2. На *worker* выполните полученную команду:

```
kubeadm join 192.168.186.86:6443 --token t48hdu.lh2sica7ga921pez --discovery-token-ca-cert-hash
sha256:92d275184e764076086f4cc86bca47f6ecedd46526568cc494d97dc27958bec7

[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

3. На *master* выполните команду для вывода списка нод кластера и их статуса:

```
kubectl get nodes

NAME                STATUS   ROLES         AGE   VERSION
localhost.localdomain   Ready    control-plane   18h   v1.24.12
worker              Ready    <none>        18h   v1.24.12
```

4. Дополнительно можно проверить работу нод на *master*. Запустите **nginx**:

```
kubectl run nginx --image=nginx

pod/nginx created
```

Проверьте размещение пода:

```
kubectl get pods

NAME    READY   STATUS    RESTARTS   AGE
nginx   1/1     Running   0          18h
```

Просмотреть детальную информацию можно с помощью команды:

```
kubectl get pod -o wide

NAME    READY   STATUS    RESTARTS   AGE   IP             NODE     NOMINATED NODE   READINESS GATES
nginx   1/1     Running   0          2m    10.244.171.65   worker   <none>         <none>
```

Откройте браузер и в адресной строке пропишите IP-адрес, указанный в детальной информации о поде nginx, **10.244.171.65**:



Полезные команды

Далее приведены некоторые полезные для работы команды:

- `kubectl delete node <имя_ноды>` - удалить ноду;
- `kubectl exec -it nginx -- /bin/bash` - выполнить вход в виртуальную консоль;
- `kubectl delete pods <имя_пода>` - удалить под;
- `kubectl get pod -o wide` - детальная информация о подах;
- `kubectl get service --all-namespaces` - подробная информация о сервисах.

Установка kubernetes с использованием контейнерного движка cri-o

Настройка Master-node
Настройка рабочих нод
Подключение worker к кластеру
Полезные команды

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** kubernetes-1.24.12-1, kubernetes-kubeadm-1.24.12-1

Для дальнейшей настройки необходимо перейти в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Настройка Master-node

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

```
swapoff -a
```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

```
swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **crio**:

```
nano /etc/modules-load.d/crio.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-o cri-tools
```

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Установите настройки по умолчанию для конфигурации контейнера:

```
sed -i '/^\[crio\.runtime\]/a seccomp_profile = "\/etc\/containers\/policy.json"' /etc/crio/crio.conf
```

7. Запустите службу **crio** и добавьте ее в автозагрузку:

```
systemctl enable --now crio
```

8. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

9. Загрузите образы контейнеров, необходимых **kubeadm** для инициализации ноды кластера:

```
kubeadm config images pull
```

10. Запустите инициализацию мастер-ноды в одноранговом кластере. Данная команда выполнит начальную настройку и подготовку основного узла кластера. Ключ **--pod-network-cidr** задает адрес внутренней подсети для вашего кластера.

```
kubeadm init --pod-network-cidr=10.244.0.0/16
```

В случае успешной инициализации, в конце вывода команды будет отображаться примерно следующее:

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 192.168.186.86:6443 --token sj5u6t.m8wl18o26fhj4gml \
 --discovery-token-ca-cert-hash sha256:53cbbbaf46036dadd55d348eea7b7585d7e7e048a554f7b684a5e5322f9ba498
```

11. Настройте параметры управления кластером. Настройку можно выполнить как для локального пользователя, так и для суперпользователя root.

Для управления кластером от имени локального пользователя выполните команды:

```
mkdir /home/$USER/.kube
cp -i /etc/kubernetes/admin.conf /home/$USER/.kube/config
chown $USER. /home/$USER/.kube /home/$USER/.kube/config
```

Для управления кластером от имени суперпользователя root выполните команды:

```
echo "export KUBECONFIG=/etc/kubernetes/admin.conf" >> /root/.bashrc
source .bashrc
export KUBECONFIG=/etc/kubernetes/admin.conf
```

Примечание.

Если настройка производилась для локального пользователя, выйдите из сеанса пользователя **root** командой exit и дальнейшие действия по настройке кластера выполняйте от имени локального пользователя.

12. Установите внутреннюю конфигурацию сети в кластере (в примере используется **calico**).

```
kubectl apply -f https://raw.githubusercontent.com/projectcalico/calico/v3.25.0/manifests/calico.yaml
```

13. Проверьте список и статус всех подов в кластере:

```
kubectl get pod -n kube-system
```

14. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname masternode
```

Проверьте изменения:

```
 hostname && hostname -I

masternode192.168.186.86 192.168.186.67 10.85.0.1 1100:200::1
```

15. В файл **/etc/hosts** внесите данные о master и worker:

```
sudo nano /etc/hosts
```

```
192.168.186.86 masternode
 192.168.186.106 worker
```

Для вывода команды присоединения worker к кластеру выполните:

```
 kubeadm token create --print-join-command

kubeadm join 192.168.186.86:6443 --token nxuiy0.xt5ts9u4ynhdoowr --discovery-token-ca-cert-hash
sha256:53cbbbaf46036dadd55d348eea7b7585d7e7e048a554f7b684a5e5322f9ba498
```

Настройка рабочих нод

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **crio**:

```
 nano /etc/modules-load.d/crio.conf
```

```
overlay
 br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
 net.ipv4.ip_forward = 1
 net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-o cri-tools
```

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Установите настройки по умолчанию для конфигурации контейнера:

```
sed -i '/^\[crio\.runtime\]/a seccomp_profile = "\/etc\/containers\/policy.json"' /etc/crio/crio.conf
```

7. Запустите службу **crio** и добавьте ее в автозагрузку:

```
systemctl enable --now crio
```

8. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

9. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname worker
```

Проверьте изменения:

```
 hostname && hostname -I

worker192.168.186.106192.168.186.142
```

10. В файл **/etc/hosts** внесите данные о *master* и *worker*:

```
sudo nano /etc/hosts
```

```
192.168.186.86 masternode
 192.168.186.106 worker
```

Подключение worker к кластеру

1. На master-ноде получите команду присоединения *worker*:

```
 kubeadm token create --print-join-command

kubeadm join 192.168.186.86:6443 --token nxuiy0.xt5ts9u4ynhdoowr --discovery-token-ca-cert-hash
sha256:53cbbbaf46036dadd55d348eea7b7585d7e7e048a554f7b684a5e5322f9ba498
```

2. На *worker* выполните полученную команду:

```
kubeadm join 192.168.186.86:6443 --token nxuiy0.xt5ts9u4ynhdoowr --discovery-token-ca-cert-hash
sha256:53cbbbaf46036dadd55d348eea7b7585d7e7e048a554f7b684a5e5322f9ba498

[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

3. На *master* выполните команду для вывода списка нод кластера и их статуса:

```
kubectl get nodes

NAME                STATUS     ROLES          AGE   VERSION
localhost.localdomain   Ready      control-plane   57m   v1.24.12
worker              NotReady   <none>         19s   v1.24.12
```

4. Дополнительно можно проверить работу нод на *master*. Запустите **nginx**.

Примечание.

Обратите внимание, что для запуска контейнера необходимо указывать **реестр образов**.

```
kubectl run nginx --image=docker.io/nginx:latest

pod/nginx created
```

Примечание.

В случае если необходимо определить реестр образов по умолчанию, отредактируйте файл конфигурации **/etc/containers/registries.conf** — в конце файла добавьте следующие строки:

```
[[registry]]
 location="<реестр_образов>"
 insecure=true
```

Проверьте размещение пода:

```
kubectl get pods

NAME    READY   STATUS    RESTARTS   AGE
nginx   1/1     Running   0          104m
```

Просмотреть детальную информацию можно с помощью команды:

```
kubectl get pod -o wide

NAME    READY   STATUS    RESTARTS   AGE    IP          NODE     NOMINATED NODE   READINESS GATES
nginx   1/1     Running   0          105m   10.85.0.2   worker   <none>           <none>
```

Откройте браузер и в адресной строке пропишите IP-адрес, указанный в детальной информации о поде nginx, **10.85.0.2**:



Полезные команды

Далее приведены некоторые полезные для работы команды:

- `kubectl delete node <имя_ноды>` - удалить ноду;
- `kubectl exec -it nginx -- /bin/bash` - выполнить вход в виртуальную консоль;
- `kubectl delete pods <имя_пода>` - удалить под;
- `kubectl get pod -o wide` - детальная информация о подах;
- `kubectl get service --all-namespaces` - подробная информация о сервисах.

Установка kubernetes с использованием контейнерного движка cri-dockerd

Настройка Master-node
Настройка рабочих нод
Подключение worker к кластеру
Полезные команды

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** kubernetes-1.24.12-1, kubernetes-kubeadm-1.24.12-1

Для дальнейшей настройки необходимо перейти в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Настройка Master-node

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm docker-ce tc ipvsadm ebtables socat conntrack git curl wget
```

3. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

4. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **cri-dockerd**:

```
nano /etc/modules-load.d/cridockerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

5. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
```

```
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

6. Установите дополнительный плагин для docker:

```
dnf install cri-dockerd
```

7. Запустите службу **docker** и добавьте ее в автозагрузку:

```
systemctl enable --now docker
```

8. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

9. Запустите службу **cri-docker.service** и добавьте ее в автозагрузку:

```
systemctl enable --now cri-docker.service
```

10. Запустите сокет **cri-docker.socket** и добавьте его в автозагрузку:

```
systemctl enable --now cri-docker.socket
```

11. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

12. Загрузите образы контейнеров, необходимых **kubeadm** для инициализации ноды кластера:

```
kubeadm config images pull --cri-socket unix:///var/run/cri-dockerd.sock
```

13. Запустите инициализацию мастер-ноды в одноранговом кластере. Данная команда выполнит начальную настройку и подготовку основного узла кластера. Ключ **--pod-network-cidr** задает адрес внутренней подсети для вашего кластера.

```
kubeadm init --pod-network-cidr=10.244.0.0/16 --cri-socket unix:///var/run/cri-dockerd.sock
```

В случае успешной инициализации, в конце вывода команды будет отображаться примерно следующее:

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 192.168.186.86:6443 --token eplom1.7ddo46uit86m9m4j \
 --discovery-token-ca-cert-hash sha256:125dd8b83146c7c1ca5a44ae1c1467337ba0e07a3e83d8578a779279a7046c5a
```

14. Настройте параметры управления кластером. Настройку можно выполнить как для локального пользователя, так и для суперпользователя root.

Для управления кластером от имени локального пользователя выполните команды:

```
mkdir /home/$USER/.kube
cp -i /etc/kubernetes/admin.conf /home/$USER/.kube/config
chown $USER. /home/$USER/.kube /home/$USER/.kube/config
```

Для управления кластером от имени суперпользователя root выполните команды:

```
export KUBECONFIG=/etc/kubernetes/admin.conf
```

> **Примечание.**
>
> Если настройка производилась для локального пользователя, выйдите из сеанса пользователя **root** командой exit и дальнейшие действия по настройке кластера выполняйте от имени локального пользователя.

15. Установите внутреннюю конфигурацию сети в кластере (в примере используется **calico**).

```
kubectl apply -f https://raw.githubusercontent.com/projectcalico/calico/v3.25.0/manifests/calico.yaml
```

16. Проверьте список и статус всех подов в кластере:

```
kubectl get pod -n kube-system
```

17. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname masternode
```

Проверьте изменения:

```
 hostname && hostname -I

masternode192.168.186.86 192.168.186.67 172.17.0.1 10.244.102.128
```

18. В файл **/etc/hosts** внесите данные о master и worker:

```
sudo nano /etc/hosts
```

```
192.168.186.86 masternode
 192.168.186.106 worker
```

Для вывода команды присоединения worker к кластеру выполните:

```
 kubeadm token create --print-join-command

kubeadm join 192.168.186.86:6443 --token 25hv1v.sot5sgkb5eqsih9l --discovery-token-ca-cert-hash
sha256:125dd8b83146c7c1ca5a44ae1c1467337ba0e07a3e83d8578a779279a7046c5a
```

Настройка рабочих нод

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm docker-ce tc ipvsadm ebtables socat conntrack git curl wget
```

3. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

4. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **cri-dockerd**:

```
nano /etc/modules-load.d/cridockerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

5. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

6. Установите дополнительный плагин для docker:

```
dnf install cri-dockerd
```

7. Запустите службу **docker** и добавьте ее в автозагрузку:

```
systemctl enable --now docker
```

8. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

9. Запустите службу **cri-docker.service** и добавьте ее в автозагрузку:

```
systemctl enable --now cri-docker.service
```

10. Запустите сокет **cri-docker.socket** и добавьте его в автозагрузку:

```
systemctl enable --now cri-docker.socket
```

11. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

12. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname worker
```

Проверьте изменения:

```
hostname && hostname -I
```

```
worker192.168.186.106
```

13. В файл **/etc/hosts** внесите данные о master и worker:

```
sudo nano /etc/hosts
```

```
192.168.186.86 masternode
 192.168.186.106 worker
```

Подключение worker к кластеру

1. На master-ноде получите команду присоединения *worker*:

```
 kubeadm token create --print-join-command

kubeadm join 192.168.186.86:6443 --token 25hv1v.sot5sgkb5eqsih9l --discovery-token-ca-cert-hash
sha256:125dd8b83146c7c1ca5a44ae1c1467337ba0e07a3e83d8578a779279a7046c5a
```

2. На *worker* выполните полученную команду:

```
 kubeadm join 192.168.186.86:6443 --token 25hv1v.sot5sgkb5eqsih9l --discovery-token-ca-cert-hash
sha256:125dd8b83146c7c1ca5a44ae1c1467337ba0e07a3e83d8578a779279a7046c5a --cri-socket unix:///run/cri-dockerd.sock

[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

3. На *master* выполните команду для вывода списка нод кластера и их статуса:

```
 kubectl get nodes

NAME                STATUS   ROLES          AGE     VERSION
localhost.localdomain   Ready    control-plane   79m     v1.24.12
worker              Ready    <none>         2m44s   v1.24.12
```

4. Дополнительно можно проверить работу нод на *master*. Запустите **nginx**:

```
 kubectl run nginx --image=nginx

pod/nginx created
```

Проверьте размещение пода:

```
 kubectl get pods

NAME    READY   STATUS    RESTARTS   AGE
nginx   1/1     Running   0          27m
```

Просмотреть детальную информацию можно с помощью команды:

```
kubectl get pod -o wide

NAME    READY   STATUS    RESTARTS   AGE    IP            NODE     NOMINATED NODE   READINESS GATES
nginx   1/1     Running   0          2m5s   10.244.171.65   worker   <none>           <none>
```

Откройте браузер и в адресной строке пропишите IP-адрес, указанный в детальной информации о поде nginx, **10.244.171.65**:



Полезные команды

Далее приведены некоторые полезные для работы команды:

- `kubectl delete node <имя_ноды>` - удалить ноду;
- `kubectl exec -it nginx -- /bin/bash` - выполнить вход в виртуальную консоль;
- `kubectl delete pods <имя_пода>` - удалить под;
- `kubectl get pod -o wide` - детальная информация о подах;
- `kubectl get service --all-namespaces` - подробная информация о сервисах.

Установка kubernetes с использованием контейнерного движка cri-o без доступа в Интернет

Входные данные
Установка Docker Registry
Настройка сети
Установка docker
Загрузка образов
Загрузка образов из сети Интернет
Загрузка образов из архива
Запуск локального registry
Настройка Master-node
Настройка рабочих нод
Подключение worker к кластеру

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** kubernetes-1.24.12-1, kubernetes-kubeadm-1.24.12-1

Входные данные

В рамках данной инструкции предполагается, что в работе используется три машины:

- **Registry** – для размещения локального хранилища образов,
- **Master** – мастер-нода,
- **Worker** – рабочая нода,

которые располагаются в закрытой сети **10.0.2.0/24**.

Для дальнейшей настройки необходимо перейти в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Установка Docker Registry

Настройка сети

Измените хостовое имя машины:

```
hostnamectl set-hostname registry
```

В файл **/etc/hosts** внесите данные о **registry**:

```
nano /etc/hosts
```

```
10.0.2.20 registry
```

Установка docker

Для установки **docker** выполните команду:

```
dnf install docker-ce
```

Запустите службу **docker** и добавьте ее в автозагрузку командой:

```
systemctl enable --now docker
```

В файле конфигурации демона **docker** необходимо указать, что с созданным хранилищем можно взаимодействовать:

```
nano /etc/docker/daemon.json
```

```
{
 "insecure-registries": ["10.0.2.20:5000"],
 "log-driver": "journald",
 "live-restore": true,
 "icc": false,
 "disable-validation": true
 }
```

где:

- 10.0.2.20 – IP-адрес машины с локальным **regisrty** (настраиваемая машина);
- 5000 – порт для подключения к локальному **regisrty** (по умолчанию).

Для сохранения настройки перезапустите службу **docker**:

```
systemctl restart docker
```

Загрузка образов

Для дальнейшей настройки локального хранилища необходимые образы должны быть предварительно загружены и доступны при вызове команды `docker images`.

Загрузка образов из сети Интернет

Для загрузки образов из официального хранилища компании РЕД СОФТ выполните:

```
docker pull registry.red-soft.ru/ubi7/registry:latest
docker pull registry.red-soft.ru/ubi7/ubi:latest
```

Загруженным образам необходимо задать теги командой:

```
docker tag registry.red-soft.ru/ubi7/registry:latest 10.0.2.20:5000/registry:latest
docker tag registry.red-soft.ru/ubi7/ubi:latest 10.0.2.20:5000/ubi:latest
```

Примечание.

Обратите внимание, что загрузить и задать теги следует **для всех** необходимых образов.

Загрузка образов из архива

В случае если настройка локального **registry** производится в полностью изолированном контуре, необходимо загрузить образы на машину с доступом к сети Интернет, аналогично п. «Загрузка образов из сети Интернет», и задать соответствующие теги.

Затем сохраните образы в архив:

```
docker save 10.0.2.20:5000/registry:latest > ~/registry.tar
docker save 10.0.2.20:5000/ubi:latest > ~/ubi.tar
```

Примечание.

Обратите внимание, что загрузить, задать теги и сохранить следует **все** необходимые образы.

После этого перенесите сохраненные образы на изолированную машину с **registry**, например, с помощью утилиты **scp**:

```
scp ubi.tar registry.tar registry:~
```

После получения архивов на изолированной машине с **registry** распакуйте их:

```
docker load -i ~/registry.tar
docker load -i ~/ubi.tar
```

Если передача образов была выполнена корректно, вывод команды docker images должен иметь следующий вид:

```
docker images

REPOSITORY            TAG    IMAGE ID     CREATED      SIZE
10.0.2.20:5000/registry latest ec0246191e3d 34 hours ago 77MB
10.0.2.20:5000/ubi      latest 59db2d81180c 34 hours ago 202MB
```

Запуск локального registry

Создайте и запустите контейнер **registry** командой:

```
docker run -d -p 5000:5000 --restart=always --name registry 10.0.2.20:5000/registry:latest
```

В случае если образы необходимо хранить отдельно от контейнеров (не в каталоге по умолчанию – **/var/lib/registry**), создайте новый каталог и примонтируйте его при запуске **registry**, заменив каталог по умолчанию:

```
mkdir ~/registry
docker run -d -p 5000:5000 --restart=always --name registry -v ~/registry:/var/lib/registry 10.0.2.20:5000/registry:latest
```

Поместите образы в настроенное локальное хранилище:

```
docker push 10.0.2.20:5000/registry:latest
docker push 10.0.2.20:5000/ubi:latest
```

Для проверки работоспособности настроенного локального хранилища попробуйте извлечь из него какой-либо образ, например:

```
docker pull 10.0.2.20:5000/ubi:latest
```

Если все настроено верно, вывод команды будет иметь примерно следующий вид:

```
latest: Pulling from ubi
06fcd37e7f38: Pull complete
Digest: sha256:169d5d23b82be10e4517058c4372ecff4e1fc3255fcb017ee3bbcecd6d3db397
Status: Downloaded newer image for 10.0.2.20:5000/ubi:latest
10.0.2.20:5000/ubi:latest
```

Настройка Master-node

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **crio**:

```
nano /etc/modules-load.d/crio.conf
```

```
overlay
 br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
 net.ipv4.ip_forward = 1
 net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-o cri-tools
```

ВАЖНО!

Если настраиваемая машина не имеет доступа в Интернет, потребуется предварительно настроить локальный репозиторий ОС, из которого будет производиться дальнейшая установка необходимых для работы пакетов. Подробную информацию о настройке локального репозитория см. в нашей статье «Создание локального репозитория».

5. Настройте проброс портов в **iptables**:

```
 iptables -P FORWARD ACCEPT
```

6. Запустите службу **crio** и добавьте ее в автозагрузку:

```
systemctl enable --now crio
```

7. Установите настройки по умолчанию для конфигурации контейнера:

```
sed -i '/^\[crio\.runtime\]/a seccomp_profile = "\/etc\/containers\/policy.json"' /etc/crio/crio.conf
```

8. Внесите изменения в файл конфигурации **/etc/crio/crio.conf**:

```
nano /etc/crio/crio.conf
```

Замените строку:

```
# pause_image = "registry.k8s.io/pause:3.6"
```

на:

```
pause_image = "10.0.2.20:5000/pause:3.7"
```

9. В конце файла **/etc/containers/registries.conf** добавьте строки:

```
[[registry]]
```

```
location="10.0.2.20:5000"
insecure=true
```

10. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

11. Перезапустите службу **crio**:

```
systemctl restart crio
```

12. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

13. Проверьте доступность локального хранилища:

```
ping 10.0.2.20

PING 10.0.2.20 (10.0.2.20) 56(84) bytes of data.
64 bytes from 10.0.2.20: icmp_seq=1 ttl=64 time=0.248 ms
64 bytes from 10.0.2.20: icmp_seq=2 ttl=64 time=0.312 ms
64 bytes from 10.0.2.20: icmp_seq=3 ttl=64 time=0.391 ms
64 bytes from 10.0.2.20: icmp_seq=4 ttl=64 time=0.413 ms
--- 10.0.2.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.248/0.341/0.413/0.065 ms
```

14. Проверьте доступность образов:

```
kubeadm config images list --image-repository 10.0.2.20:5000

[I1121 13:16:04.377507   33239 version.go:256] remote version is much newer: v1.28.4; falling back to: stable-1.24
10.0.2.20:5000/kube-apiserver:v1.24.17
10.0.2.20:5000/kube-controller-manager:v1.24.17
10.0.2.20:5000/kube-scheduler:v1.24.17
10.0.2.20:5000/kube-proxy:v1.24.17
10.0.2.20:5000/pause:3.7
10.0.2.20:5000/etcd:3.5.6-0
10.0.2.20:5000/coredns:v1.8.6
```

15. Загрузите образы контейнеров из локального хранилища, необходимые **kubeadm** для инициализации ноды кластера:

```
kubeadm config images pull --image-repository 10.0.2.20:5000 --cri-socket unix:///var/run/crio/crio.sock
```

16. Запустите инициализацию мастер-ноды в одноранговом кластере. Данная команда выполнит начальную настройку и подготовку основного узла кластера. Ключ `--pod-network-cidr` задает адрес внутренней подсети для вашего кластера.

```
kubeadm init --image-repository 10.0.2.20:5000 --pod-network-cidr=10.244.0.0/16 --cri-socket unix:///var/run/crio/crio.sock
```

В случае успешной инициализации, в конце вывода команды будет отображаться примерно следующее:

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/
```

```
Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

17. Настройте параметры управления кластером. Настройку можно выполнить как для **локального** пользователя, так и для суперпользователя **root**.

Для управления кластером от имени **локального** пользователя выполните команды:

```
mkdir /home/$USER/.kube
cp -i /etc/kubernetes/admin.conf /home/$USER/.kube/config
chown $USER. /home/$USER/.kube /home/$USER/.kube/config
```

Для управления кластером от имени суперпользователя **root** выполните команду:

```
export KUBECONFIG=/etc/kubernetes/admin.conf
```

Выполните настройку **/etc/resolv.conf**. В случае если настройка **/etc/resolv.conf** не предполагается, внесите изменения в **configmap** для **coredns**:

```
kubectl edit configmap coredns -n kube-system
```

удалите следующие строки:

```
forward . /etc/resolv.conf {
   max_concurrent 1000
 }
```

> **Примечание.**
>
> Если настройка производилась для *локального* пользователя, **выйдите** из сеанса пользователя **root** командой exit и дальнейшие действия по настройке кластера выполняйте от имени *локального* пользователя.

18. Настройте внутреннюю конфигурацию сети в кластере (в примере используется **calico**).

19.1 Для этого на машине с выходом в Интернет необходимо загрузить следующие образы:

```
docker pull docker.io/calico/cni:v3.25.0
docker pull docker.io/calico/node:v3.25.0
docker pull docker.io/calico/kube-controllers:v3.25.0
```

19.2 Задать теги для загруженных образов:

```
docker tag docker.io/calico/cni:v3.25.0 10.0.2.20:5000/cni:v3.25.0
docker tag docker.io/calico/node:v3.25.0 10.0.2.20:5000/node:v3.25.0
docker tag docker.io/calico/kube-controllers:v3.25.0 10.0.2.20:5000/kube-controllers:v3.25.0
```

19.3 Сохранить в архив и отправить образы на машину с настроенным локальным **registry**:

```
docker save 10.0.2.20:5000/cni:v3.25.0 > cni.tar
docker save 10.0.2.20:5000/node:v3.25.0 > node.tar
docker save 10.0.2.20:5000/kube-controllers:v3.25.0 > kube-ctrl.tar
scp cni.tar node.tar kube-ctrl.tar registry:~
```

19.4 Распаковать образы на машине с настроенным локальным **registry**:

```
docker load -i cni.tar
docker load -i node.tar
docker load -i kube-ctrl.tar
```

19.5 Загрузить распакованные образы в локальное хранилище:

```
docker push 10.0.2.20:5000/cni:v3.25.0
docker push 10.0.2.20:5000/node:v3.25.0
docker push 10.0.2.20:5000/kube-controllers:v3.25.0
```

19.6 На машине с выходом в Интернет необходимо дополнительно скачать файл конфигурации **calico**:

```
curl -o calico.yaml https://raw.githubusercontent.com/projectcalico/calico/v3.25.0/manifests/calico.yaml
```

и привести следующие строки:

Номер строки	Имя образа
4443	docker.io/calico/cni:v3.25.0
4471	docker.io/calico/cni:v3.25.0
4514	docker.io/calico/node:v3.25.0
4540	docker.io/calico/node:v3.25.0
4757	docker.io/calico/kube-controllers:v3.25.0

к следующему виду:

Номер строки	Имя образа
4443	10.0.2.20:5000/cni:v3.25.0
4471	10.0.2.20:5000/cni:v3.25.0
4514	10.0.2.20:5000/node:v3.25.0
4540	10.0.2.20:5000/node:v3.25.0
4757	10.0.2.20:5000/kube-controllers:v3.25.0

Например:

было:

```
- name: upgrade-ipam
    image: docker.io/calico/cni:v3.25.0
    imagePullPolicy: IfNotPresent
    command: ["/opt/cni/bin/calico-ipam", "-upgrade"]
    envFrom:
```

стало:

```
- name: upgrade-ipam
    image: 10.0.2.15:5000/cni:v3.25.0
    imagePullPolicy: IfNotPresent
    command: ["/opt/cni/bin/calico-ipam", "-upgrade"]
    envFrom:
```

Сохраните внесенные в конфигурацию изменения и передайте файл на машину с настраиваемой **master**-нодой.

19.7 На **master**-ноде примените внутреннюю конфигурацию сети в кластере:

```
kubectl apply -f calico.yaml
```

Потребуется некоторое время для настройки (от 2 до 5 минут).

20. После применения конфигурации проверьте список и статус всех подов в кластере:

```
kubectl get all -n kube-system
```

21. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname masternode
```

Проверьте изменения:

```
hostname && hostname -I
```

```
masternode
10.0.2.16
```

22. В файл **/etc/hosts** внесите данные о **master** и **worker**:

```
sudo nano /etc/hosts
```

```
10.0.2.16 masternode
10.0.2.17 worker
```

Для вывода команды присоединения **worker** к кластеру выполните:

```
kubeadm token create --print-join-command

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

Настройка рабочих нод

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **crio**:

```
 nano /etc/modules-load.d/crio.conf
```

```
overlay
 br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
 net.ipv4.ip_forward = 1
 net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-o cri-tools
```

ВАЖНО!

Если настраиваемая машина не имеет доступа в Интернет, потребуется предварительно настроить локальный репозиторий ОС, из которого будет производиться дальнейшая установка необходимых для работы пакетов. Подробную информацию о настройке локального репозитория см. в нашей статье «Создание локального репозитория».

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Запустите службу **crio** и добавьте ее в автозагрузку:

```
systemctl enable --now crio
```

7. Установите настройки по умолчанию для конфигурации контейнера:

```
sed -i '/^\[crio\.runtime\]/a seccomp_profile = "\/etc\/containers\/policy.json"' /etc/crio/crio.conf
```

8. Внесите изменения в файл конфигурации **/etc/crio/crio.conf**:

```
nano /etc/crio/crio.conf
```

Замените строку:

```
# pause_image = "registry.k8s.io/pause:3.6"
```

на:

```
pause_image = "10.0.2.20:5000/pause:3.7"
```

9. В конце файла **/etc/containers/registries.conf** добавьте строки:

```
[[registry]]
 location="10.0.2.20:5000"
 insecure=true
```

10. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

11. Перезапустите службу **crio**:

```
systemctl restart crio
```

12. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

13. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname worker
```

Проверьте изменения:

```
hostname && hostname -I

worker
10.0.2.17
```

14. В файл **/etc/hosts** внесите данные о **master** и **worker**:

```
sudo nano /etc/hosts
```

```
10.0.2.16 masternode
10.0.2.17 worker
```

Подключение worker к кластеру

1. На master-ноде получите команду присоединения *worker*:

```
kubeadm token create --print-join-command

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

2. На *worker* выполните полученную команду:

```
kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 --discovery-token-ca-cert-hash
sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391 --cri-socket unix:///var/run/crio/crio.sock

[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

3. На *master* выполните команду для вывода списка нод кластера и их статуса:

```
kubectl get nodes

NAME                STATUS   ROLES          AGE    VERSION
localhost.localdomain   Ready    control-plane   5h3m   v1.24.17
worker              Ready    <none>         89s    v1.24.17
```

Установка kubernetes с использованием контейнерного движка containerd без доступа в Интернет

Входные данные
Установка Docker Registry
Настройка сети
Установка docker
Загрузка образов
Загрузка образов из сети Интернет
Загрузка образов из архива
Запуск локального registry
Настройка Master-node
Настройка рабочих нод
Подключение worker к кластеру

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** kubernetes-1.24.17-6, kubernetes-kubeadm-1.24.17-6

Входные данные

В рамках рассматриваемого далее примера развертывания программной платформы kubernetes предполагается, что в работе используется три машины:

- **Registry** – для размещения локального хранилища образов с присвоенным статическим IP-адресом **10.0.2.20**,
- **Master** – мастер-нода с присвоенным статическим IP-адресом **10.0.2.16**,
- **Worker** – рабочая нода с присвоенным статическим IP-адресом **10.0.2.17**,

которые располагаются в закрытой сети **10.0.2.0/24**.

> **Примечание.**
>
> Указанные IP-адреса необходимо заменить на фактически используемые значения в сети.

Для дальнейшей настройки необходимо перейти в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Установка Docker Registry

Настройка сети

Измените хостовое имя машины:

```
hostnamectl set-hostname registry
```

В файл **/etc/hosts** внесите данные о **registry**:

```
nano /etc/hosts
```

```
10.0.2.20 registry
```

Установка docker

Для установки **docker** выполните команду:

```
dnf install docker-ce
```

Запустите службу **docker** и добавьте ее в автозагрузку командой:

```
systemctl enable --now docker
```

В файле конфигурации демона **docker** необходимо указать, что с созданным хранилищем можно взаимодействовать:

```
nano /etc/docker/daemon.json
```

```
{
 "insecure-registries": ["10.0.2.20:5000"],
 "log-driver": "journald",
 "live-restore": true,
 "icc": false,
 "disable-validation": true
 }
```

где:

- `10.0.2.20` – IP-адрес машины с локальным **regisrty** (настраиваемая машина);
- `5000` – порт для подключения к локальному **regisrty** (по умолчанию).

Для сохранения настройки перезапустите конфигурацию системных служб и службу **docker**:

```
systemctl daemon-reload
systemctl restart docker
```

Загрузка образов

Для дальнейшей настройки локального хранилища необходимые образы должны быть предварительно загружены и доступны при вызове команды `docker images`.

Загрузка образов из сети Интернет

Для загрузки образов из официального хранилища компании РЕД СОФТ выполните:

```
docker pull registry.red-soft.ru/ubi7/registry:latest
docker pull registry.red-soft.ru/ubi7/ubi:latest
```

Загруженным образам необходимо задать теги командой:

```
docker tag registry.red-soft.ru/ubi7/registry:latest 10.0.2.20:5000/registry:latest
docker tag registry.red-soft.ru/ubi7/ubi:latest 10.0.2.20:5000/ubi:latest
```

Примечание.

Обратите внимание, что загрузить и задать теги следует **для всех** необходимых образов.

Загрузка образов из архива

В случае если настройка локального **registry** производится в полностью изолированном контуре, необходимо загрузить образы на машину с доступом к сети Интернет, аналогично п. «Загрузка образов из сети Интернет», и задать соответствующие теги.

Затем сохраните образы в архив:

```
docker save 10.0.2.20:5000/registry:latest > ~/registry.tar
docker save 10.0.2.20:5000/ubi:latest > ~/ubi.tar
```

Примечание.

Обратите внимание, что загрузить, задать теги и сохранить следует **все** необходимые образы.

После этого перенесите сохраненные образы на изолированную машину с **registry**, например, с помощью утилиты **scp**. Синтаксис утилиты имеет вид:

```
scp ubi.tar registry.tar registry:~
```

После получения архивов на изолированной машине с **registry** распакуйте их:

```
docker load -i ~/registry.tar
docker load -i ~/ubi.tar
```

Если передача образов была выполнена корректно, вывод команды docker images должен иметь следующий вид:

docker images

```
REPOSITORY            TAG    IMAGE ID     CREATED      SIZE
10.0.2.20:5000/registry latest ec0246191e3d 34 hours ago 77MB
10.0.2.20:5000/ubi      latest 59db2d81180c 34 hours ago 202MB
```

Запуск локального registry

Создайте и запустите контейнер **registry** командой:

```
docker run -d -p 5000:5000 --restart=always --name registry 10.0.2.20:5000/registry:latest
```

В случае если образы необходимо хранить отдельно от контейнеров (не в каталоге по умолчанию – **/var/lib/registry**), создайте новый каталог и примонтируйте его при запуске **registry**, заменив каталог по умолчанию:

```
mkdir ~/registry
docker run -d -p 5000:5000 --restart=always --name registry -v ~/registry:/var/lib/registry 10.0.2.20:5000/registry:latest
```

Поместите образы в настроенное локальное хранилище:

```
docker push 10.0.2.20:5000/registry:latest
docker push 10.0.2.20:5000/ubi:latest
```

Для проверки работоспособности настроенного локального хранилища попробуйте извлечь из него какой-либо образ, например:

```
docker pull 10.0.2.20:5000/ubi:latest
```

Если все настроено верно, вывод команды будет иметь примерно следующий вид:

```
latest: Pulling from ubi
06fcd37e7f38: Pull complete
Digest: sha256:169d5d23b82be10e4517058c4372ecff4e1fc3255fcb017ee3bbcecd6d3db397
Status: Downloaded newer image for 10.0.2.20:5000/ubi:latest 10.0.2.20:5000/ubi:latest
```

Настройка Master-node

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

```
swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **containerd**:

```
nano /etc/modules-load.d/containerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-tools iproute-tc ebtables socat conntrack git curl wget runc containerd
```

ВАЖНО!

Если настраиваемая машина не имеет доступа в Интернет, потребуется предварительно настроить локальный репозиторий ОС, из которого будет производиться дальнейшая установка необходимых для работы пакетов. Подробную информацию о настройке локального репозитория см. в нашей статье «Создание локального репозитория».

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Запустите службу **containerd** и добавьте ее в автозагрузку:

```
systemctl enable --now containerd
```

7. Установите настройки по умолчанию для конфигурации контейнера:

```
containerd config default | sudo tee /etc/containerd/config.toml
```

8. Внесите изменения в файл конфигурации **/etc/containerd/config.toml**:

```
nano /etc/containerd/config.toml
```

8.1 Настройте доступ к локальному **registry**.

Для этого замените строку:

```
[plugins."io.containerd.grpc.v1.cri".registry.mirrors]
```

на:

```
[plugins."io.containerd.grpc.v1.cri".registry.mirrors."10.0.2.20:5000"]
  endpoint = ["http://10.0.2.20:5000"]
```

8.2 Настройте доступ к контейнеру **pause**. Обратите внимание, что текущая версия Kubernetes (**1.24.17**) совместима с контейнером pause только версии **3.7**.

Замените строку:

```
[plugins."io.containerd.grpc.v1.cri"]
 ...
  sandbox_image = "registry.k8s.io/pause:3.8"
```

на:

```
[plugins."io.containerd.grpc.v1.cri"]
 ...
  sandbox_image = "10.0.2.20:5000/pause:3.7"
```

8.3 Настройте расположение сетевых плагинов.

Замените строку:

```
[plugins."io.containerd.grpc.v1.cri".cni]
  bin_dir = "/opt/cni/bin"
```

на:

```
[plugins."io.containerd.grpc.v1.cri".cni]
  bin_dir = "/usr/libexec/cni"
```

8.4 Настройте использование драйвера **cgroup**.

Замените строку:

```
[plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc.options]
 ...
  SystemdCgroup = false
```

на:

```
[plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc.options]
 ...
  SystemdCgroup = "true"
```

9. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

10. Перезапустите службу **containerd**:

```
systemctl restart containerd
```

11. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

12. Проверьте доступность локального хранилища:

```
ping 10.0.2.20
```

```
PING 10.0.2.20 (10.0.2.20) 56(84) bytes of data.
64 bytes from 10.0.2.20: icmp_seq=1 ttl=64 time=0.248 ms
64 bytes from 10.0.2.20: icmp_seq=2 ttl=64 time=0.312 ms
64 bytes from 10.0.2.20: icmp_seq=3 ttl=64 time=0.391 ms
64 bytes from 10.0.2.20: icmp_seq=4 ttl=64 time=0.413 ms
--- 10.0.2.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.248/0.341/0.413/0.065 ms
```

13. Для инициализации мастер-ноды необходимо:

13.1 Вывести конфигурацию по умолчанию командой:

```
kubeadm config print init-defaults > kubeadm-config.yaml
```

13.2 Привести содержимое конфигурации к следующему виду:

```
apiVersion: kubeadm.k8s.io/v1beta3
bootstrapTokens:
- groups:
  - system:bootstrappers:kubeadm:default-node-token
  token: abcdef.0123456789abcdef
  ttl: 24h0m0s
  usages:
  - signing
  - authentication
kind: InitConfiguration
localAPIEndpoint:
  advertiseAddress: 10.0.2.16
  bindPort: 6443
nodeRegistration:
  criSocket: unix:///var/run/containerd/containerd.sock
  imagePullPolicy: IfNotPresent
  name: node
  taints: null
---
apiServer:
  timeoutForControlPlane: 4m0s
apiVersion: kubeadm.k8s.io/v1beta3
certificatesDir: /etc/kubernetes/pki
clusterName: kubernetes
controllerManager: {}
dns: {}
etcd:
  local:
    dataDir: /var/lib/etcd
    imageRepository: 10.0.2.20:5000
    imageTag: 3.5.15
imageRepository: 10.0.2.20:5000
kind: ClusterConfiguration
kubernetesVersion: 1.24.17
networking:
  dnsDomain: cluster.local
  serviceSubnet: 10.96.0.0/12
  podSubnet: 10.244.0.0/16
scheduler: {}
```

13.3 Сохранить внесенные в конфигурацию изменения.

13.4 Запустить инициализацию мастер-ноды в одноранговом кластере. Данная команда выполнит начальную настройку и подготовку основного узла кластера.

```
```

```
kubeadm init --config=kubeadm-config.yaml
```

В случае успешной инициализации в конце вывода команды будет отображаться примерно следующее:

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 10.0.2.16:6443 --token abcdef.0123456789abcdef \
 --discovery-token-ca-cert-hash sha256:fff28749381ebebba6754155104ac8ce0ad3b5a992f9cf73757ea2d352b7785a
```

14. Настройте параметры управления кластером. Настройку можно выполнить как для локального пользователя, так и для суперпользователя root.

Для управления кластером от имени **локального** пользователя выполните команды:

```
mkdir /home/$USER/.kube
cp -i /etc/kubernetes/admin.conf /home/$USER/.kube/config
chown $USER. /home/$USER/.kube /home/$USER/.kube/config
```

Для управления кластером от имени суперпользователя **root** выполните команду:

```
echo "export KUBECONFIG=/etc/kubernetes/admin.conf" >> /root/.bashrc
source /root/.bashrc
export KUBECONFIG=/etc/kubernetes/admin.conf
```

ВАЖНО!

Если в используемой системе файл, отвечающий за настройки разрешения доменных имен (**/etc/resolv.conf**), располагается по нестандартному пути или имеет нестандартное наименование, скорректируйте путь расположения файла в configmap. Для этого выполните команду:

```
kubectl edit configmap coredns -n kube-system
```

и внесите следующие изменения:

```
forward . /<путь_к_файлу>/<имя_файла> {
 max_concurrent 1000
 }
```

Примечание.

Если настройка производилась для *локального* пользователя, **выйдите** из сеанса пользователя **root** командой exit и дальнейшие действия по настройке кластера выполняйте от имени *локального* пользователя.

15. Настройте внутреннюю конфигурацию сети в кластере (в примере используется **flannel**).

15.1 Импортируйте образы на хосте с настроенным локальным **registry**:

```
docker load -i ~/flannel-cni-plugin-flannel.tar.xz
docker load -i ~/flannel-flanneld.tar.xz
```

15.2 Задайте новые имена для загруженных образов командой вида:

```
docker tag <имя_распакованного_образа>:<тег> <IP-адрес_registry>:<порт>/<имя_образа>:<тег>
```

где:

- `<IP-адрес_registry>` — IP-адрес хоста с настроенным локальным **registry**;
- `<порт>` — порт для подключения к локальному **registry** (по умолчанию **5000**);
- `<имя_образа>` — имя образа;
- `<тег>` — тег образа.

Например:

```
docker tag registry.red-soft.ru/k8s7c/flannel-cni-plugin-flannel:240916 10.0.2.20:5000/flannel-cni-plugin-flannel:240916docker tag
registry.red-soft.ru/k8s7c/flannel-flanneld:240919 10.0.2.20:5000/flannel-flanneld:240919
```

где:

- `10.0.2.20` — IP-адрес хоста с настроенным локальным **registry**;
- `5000` — порт для подключения к локальному **registry** (по умолчанию **5000**);
- `flannel-cni-plugin-flannel`, `flannel-flanneld` — имена образов;
- `240916`, `240919` — теги образов.

15.3 Загрузите распакованные образы в локальное хранилище:

```
docker push 10.0.2.20:5000/flannel-cni-plugin-flannel:240916docker push 10.0.2.20:5000/flannel-flanneld:240919
```

15.4 На **master**-ноде создайте файл конфигурации **kube-flannel.yaml** со следующим содержимым:

```
apiVersion: v1
 kind: Namespace
 metadata:
   labels:
     k8s-app: flannel
     pod-security.kubernetes.io/enforce: privileged
   name: kube-flannel
 ---
 apiVersion: v1
 kind: ServiceAccount
 metadata:
   labels:
     k8s-app: flannel
   name: flannel
   namespace: kube-flannel
 ---
 apiVersion: rbac.authorization.k8s.io/v1
 kind: ClusterRole
 metadata:
   labels:
     k8s-app: flannel
   name: flannel
 rules:
   - apiGroups:
       - ""
     resources:
       - pods
     verbs:
```

```
    - get
  - apiGroups:
    - ""
    resources:
    - nodes
    verbs:
    - get
    - list
    - watch
  - apiGroups:
    - ""
    resources:
    - nodes/status
    verbs:
    - patch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  labels:
    k8s-app: flannel
  name: flannel
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: flannel
subjects:
  - kind: ServiceAccount
    name: flannel
    namespace: kube-flannel
---
apiVersion: v1
kind: ConfigMap
metadata:
  labels:
    app: flannel
    k8s-app: flannel
    tier: node
  name: kube-flannel-cfg
  namespace: kube-flannel
data:
  cni-conf.json: |
    {
      "name": "cbr0",
      "cniVersion": "0.3.1",
      "plugins": [
        {
          "type": "flannel",
          "delegate": {
            "hairpinMode": true,
            "isDefaultGateway": true
          }
        },
        {
          "type": "portmap",
          "capabilities": {
            "portMappings": true
          }
```

```
      }
     ]
    }
  net-conf.json: |
    {
     "Network": "10.244.0.0/16",
     "EnableNFTables": false,
     "Backend": {
      "Type": "vxlan"
     }
    }
---
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    app: flannel
    k8s-app: flannel
    tier: node
  name: kube-flannel-ds
  namespace: kube-flannel
spec:
  selector:
    matchLabels:
      app: flannel
      k8s-app: flannel
  template:
    metadata:
      labels:
        app: flannel
        k8s-app: flannel
        tier: node
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: kubernetes.io/os
                    operator: In
                    values:
                      - linux
      containers:
        - args:
            - --ip-masq
            - --kube-subnet-mgr
          command:
            - flanneld
          env:
            - name: POD_NAME
              valueFrom:
                fieldRef:
                  fieldPath: metadata.name
            - name: POD_NAMESPACE
              valueFrom:
                fieldRef:
                  fieldPath: metadata.namespace
            - name: EVENT_QUEUE_DEPTH
```

```
        value: "5000"
      image: 10.0.2.20:5000/flannel-flanneld:240919
      name: kube-flannel
      resources:
        requests:
          cpu: 100m
          memory: 50Mi
      securityContext:
        capabilities:
          add:
            - NET_ADMIN
            - NET_RAW
        privileged: false
      volumeMounts:
        - mountPath: /run/flannel
          name: run
        - mountPath: /etc/kube-flannel/
          name: flannel-cfg
        - mountPath: /run/xtables.lock
          name: xtables-lock
  hostNetwork: true
  initContainers:
    - args:
        - -f
        - /flannel
        - /usr/libexec/cni/flannel
      command:
        - cp
      image: 10.0.2.20:5000/flannel-cni-plugin-flannel:240916
      name: install-cni-plugin
      volumeMounts:
        - mountPath: /usr/libexec/cni
          name: cni-plugin
    - args:
        - -f
        - /etc/kube-flannel/cni-conf.json
        - /etc/cni/net.d/10-flannel.conflist
      command:
        - cp
      image: 10.0.2.20:5000/flannel-flanneld:240919
      name: install-cni
      volumeMounts:
        - mountPath: /etc/cni/net.d
          name: cni
        - mountPath: /etc/kube-flannel/
          name: flannel-cfg
  priorityClassName: system-node-critical
  serviceAccountName: flannel
  tolerations:
    - effect: NoSchedule
      operator: Exists
  volumes:
    - hostPath:
        path: /run/flannel
      name: run
    - hostPath:
        path: /usr/libexec/cni
      name: cni-plugin
```

```
      - hostPath:
          path: /etc/cni/net.d
        name: cni
      - configMap:
          name: kube-flannel-cfg
        name: flannel-cfg
      - hostPath:
          path: /run/xtables.lock
          type: FileOrCreate
        name: xtables-lock
```

Сохраните внесенные в конфигурацию изменения.

15.5 На master-ноде примените внутреннюю конфигурацию сети в кластере:

```
kubectl apply -f kube-flannel.yaml
```

Потребуется некоторое время для настройки (от 2 до 5 минут).

16. После применения конфигурации проверьте список и статус системных компонентов Kubernetes, а также компонентов сетевого плагина flannel:

```
kubectl get all -n kube-system
kubectl get all -n kube-flannel
```

17. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname masternode
```

Проверьте изменения:

```
hostname && hostname -I

masternode
10.0.2.16
```

18. В файл **/etc/hosts** внесите данные о **master** и **worker**:

```
sudo nano /etc/hosts
```

```
10.0.2.16 masternode
 10.0.2.17 worker
```

Для вывода команды присоединения **worker** к кластеру выполните:

```
kubeadm token create --print-join-command

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

Настройка рабочих нод

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **containerd**:

```
nano /etc/modules-load.d/containerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

3. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

4. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm cri-tools iproute-tc ebtables socat conntrack git curl wget runc containerd
```

ВАЖНО!

Если настраиваемая машина не имеет доступа в Интернет, потребуется предварительно настроить локальный репозиторий ОС, из которого будет производиться дальнейшая установка необходимых для работы пакетов. Подробную информацию о настройке локального репозитория см. в нашей статье «Создание локального репозитория».

5. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

6. Запустите службу **containerd** и добавьте ее в автозагрузку:

```
systemctl enable --now containerd
```

7. Установите настройки по умолчанию для конфигурации контейнера:

```
containerd config default | sudo tee /etc/containerd/config.toml
```

8. Внесите изменения в файл конфигурации **/etc/containerd/config.toml**:

```
nano /etc/containerd/config.toml
```

8.1 Настройте доступ к локальному **registry**.

Для этого замените строку:

```
[plugins."io.containerd.grpc.v1.cri".registry.mirrors]
```

на:

```
[plugins."io.containerd.grpc.v1.cri".registry.mirrors."10.0.2.20:5000"]
```

```
    endpoint = ["http://10.0.2.20:5000"]
```

8.2 Настройте доступ к контейнеру **pause**. Обратите внимание, что текущая версия Kubernetes (**1.24.17**) совместима с контейнером pause только версии **3.7**.

Замените строку:

```
[plugins."io.containerd.grpc.v1.cri"]
  ...
    sandbox_image = "registry.k8s.io/pause:3.8"
```

на:

```
[plugins."io.containerd.grpc.v1.cri"]
  ...
    sandbox_image = "10.0.2.20:5000/pause:3.7"
```

8.3 Настройте расположение сетевых плагинов.

Замените строку:

```
[plugins."io.containerd.grpc.v1.cri".cni]
    bin_dir = "/opt/cni/bin"
```

на:

```
[plugins."io.containerd.grpc.v1.cri".cni]
    bin_dir = "/usr/libexec/cni"
```

8.4 Настройте использование драйвера **cgroup**.

Замените строку:

```
[plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc.options]
  ...
    SystemdCgroup = false
```

на:

```
[plugins."io.containerd.grpc.v1.cri".containerd.runtimes.runc.options]
  ...
    SystemdCgroup = "true"
```

9. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

10. Перезапустите службу **containerd**:

```
systemctl restart containerd
```

11. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

12. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname worker
```

Проверьте изменения:

```
 hostname && hostname -I

worker10.0.2.17
```

13. В файл **/etc/hosts** внесите данные о *master* и *worker*:

```
sudo nano /etc/hosts
```

```
10.0.2.16 masternode
 10.0.2.17 worker
```

После этого можно приступать к присоединению *worker* к кластеру.

Подключение worker к кластеру

1. На master-ноде получите команду присоединения *worker*:

```
 kubeadm token create --print-join-command

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

2. На *worker* выполните полученную команду:

```
 kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 --discovery-token-ca-cert-hash
sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391

[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

3. На *master* выполните команду для вывода списка нод кластера и их статуса:

```
 kubectl get nodes

NAME                STATUS   ROLES          AGE    VERSION
localhost.localdomain   Ready    control-plane   5h3m   v1.24.17
worker              Ready    <none>         89s    v1.24.17
```

Установка kubernetes с использованием контейнерного движка cri-dockerd без доступа в Интернет

Входные данные
Установка Docker Registry
Настройка сети
Установка docker
Загрузка образов
Загрузка образов из сети Интернет
Загрузка образов из архива
Запуск локального registry
Настройка Master-node
Настройка рабочих нод
Подключение worker к кластеру

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** kubernetes-1.24.12-1, kubernetes-kubeadm-1.24.12-1

Входные данные

В рамках данной инструкции предполагается, что в работе используется три машины:

- **Registry** – для размещения локального хранилища образов,
- **Master** – мастер-нода,
- **Worker** – рабочая нода,

которые располагаются в закрытой сети **10.0.2.0/24**.

Для дальнейшей настройки необходимо перейти в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Установка Docker Registry

Настройка сети

Измените хостовое имя машины:

```
hostnamectl set-hostname registry
```

В файл **/etc/hosts** внесите данные о **registry**:

```
nano /etc/hosts
```

```
10.0.2.20 registry
```

Установка docker

Для установки **docker** выполните команду:

```
dnf install docker-ce
```

Запустите службу **docker** и добавьте ее в автозагрузку командой:

```
systemctl enable --now docker
```

В файле конфигурации демона **docker** необходимо указать, что с созданным хранилищем можно взаимодействовать:

```
nano /etc/docker/daemon.json
```

```
{
 "insecure-registries": ["10.0.2.20:5000"],
 "log-driver": "journald",
 "live-restore": true,
 "icc": false,
 "disable-validation": true
 }
```

где:

- 10.0.2.20 – IP-адрес машины с локальным **regisrty** (настраиваемая машина);
- 5000 – порт для подключения к локальному **regisrty** (по умолчанию).

Для сохранения настройки перезапустите службу **docker**:

```
systemctl restart docker
```

Загрузка образов

Для дальнейшей настройки локального хранилища необходимые образы должны быть предварительно загружены и доступны при вызове команды `docker images`.

Загрузка образов из сети Интернет

Для загрузки образов из официального хранилища компании РЕД СОФТ выполните:

```
docker pull registry.red-soft.ru/ubi7/registry:latest
docker pull registry.red-soft.ru/ubi7/ubi:latest
```

Загруженным образам необходимо задать теги командой:

```
docker tag registry.red-soft.ru/ubi7/registry:latest 10.0.2.20:5000/registry:latest
docker tag registry.red-soft.ru/ubi7/ubi:latest 10.0.2.20:5000/ubi:latest
```

Примечание.

Обратите внимание, что загрузить и задать теги следует **для всех** необходимых образов.

Загрузка образов из архива

В случае если настройка локального **registry** производится в полностью изолированном контуре, необходимо загрузить образы на машину с доступом к сети Интернет, аналогично п. «Загрузка образов из сети Интернет», и задать соответствующие теги.

Затем сохраните образы в архив:

```
docker save 10.0.2.20:5000/registry:latest > ~/registry.tar
docker save 10.0.2.20:5000/ubi:latest > ~/ubi.tar
```

Примечание.

Обратите внимание, что загрузить, задать теги и сохранить следует **все** необходимые образы.

После этого перенесите сохраненные образы на изолированную машину с **registry**, например, с помощью утилиты **scp**. Синтаксис утилиты имеет вид:

```
scp ubi.tar registry.tar registry:~
```

После получения архивов на изолированной машине с **registry** распакуйте их:

```
docker load -i ~/registry.tar
docker load -i ~/ubi.tar
```

Если передача образов была выполнена корректно, вывод команды docker images должен иметь следующий вид:

```
docker images

REPOSITORY            TAG    IMAGE ID     CREATED      SIZE
10.0.2.20:5000/registry latest ec0246191e3d 34 hours ago 77MB
10.0.2.20:5000/ubi      latest 59db2d81180c 34 hours ago 202MB
```

Запуск локального registry

Создайте и запустите контейнер **registry** командой:

```
docker run -d -p 5000:5000 --restart=always --name registry 10.0.2.20:5000/registry:latest
```

В случае если образы необходимо хранить отдельно от контейнеров (не в каталоге по умолчанию – **/var/lib/registry**), создайте новый каталог и примонтируйте его при запуске **registry**, заменив каталог по умолчанию:

```
mkdir ~/registry
docker run -d -p 5000:5000 --restart=always --name registry -v ~/registry:/var/lib/registry 10.0.2.20:5000/registry:latest
```

Поместите образы в настроенное локальное хранилище:

```
docker push 10.0.2.20:5000/registry:latest
docker push 10.0.2.20:5000/ubi:latest
```

Для проверки работоспособности настроенного локального хранилища попробуйте извлечь из него какой-либо образ, например:

```
docker pull 10.0.2.20:5000/ubi:latest
```

Если все настроено верно, вывод команды будет иметь примерно следующий вид:

```
latest: Pulling from ubi
06fcd37e7f38: Pull complete
Digest: sha256:169d5d23b82be10e4517058c4372ecff4e1fc3255fcb017ee3bbcecd6d3db397
Status: Downloaded newer image for 10.0.2.20:5000/ubi:latest
10.0.2.20:5000/ubi:latest
```

Настройка Master-node

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm docker-ce tc ipvsadm ebtables socat conntrack git curl wget
```

ВАЖНО!

Если настраиваемая машина не имеет доступа в Интернет, потребуется предварительно настроить локальный репозиторий ОС, из которого будет производиться дальнейшая установка необходимых для работы пакетов. Подробную информацию о настройке локального репозитория см. в нашей статье «Создание локального репозитория».

3. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

4. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **cri-dockerd**:

```
nano /etc/modules-load.d/cridockerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

5. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

6. Установите дополнительный плагин для **docker**:

```
dnf install cri-dockerd
```

7. Запустите службу **cri-docker.service** и добавьте ее в автозагрузку:

```
systemctl enable --now cri-docker.service
```

8. Запустите службу **docker** и добавьте ее в автозагрузку:

```
systemctl enable --now docker
```

9. Внесите изменения в файл конфигурации службы **cri-docker.service**:

```
nano /usr/lib/systemd/system/cri-docker.service
```

Замените строку:

```
ExecStart=/usr/bin/cri-dockerd --container-runtime-endpoint fd://
```

на

```
ExecStart=/usr/bin/cri-dockerd --pod-infra-container-image=<registry>/pause:<версия> --container-runtime-endpoint fd://
```

где:

- <registry> – путь к настроенному локальному хранилищу образов (в примере **10.0.2.20:5000/registry**);
- <версия> – версия пакета pause (для **kubernetes-1.24** используется версия **pause:3.7**).

10. В файле конфигурации демона **docker** укажите, что с созданным хранилищем можно взаимодействовать:

```
nano /etc/docker/daemon.json
```

```
{
 "insecure-registries": ["10.0.2.20:5000"],
 "log-driver": "journald",
 "live-restore": true,
 "icc": false,
 "disable-validation": true
 }
```

где:

- 10.0.2.20 – IP-адрес машины с локальным **regisrty**;
- 5000 – порт для подключения к локальному **regisrty** (по умолчанию).

11. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

12. Перезапустите службу **docker**:

```
systemctl restart docker
```

13. Перезапустите службу **cri-docker.service**:

```
systemctl restart cri-docker.service
```

14. Запустите сокет **cri-docker.socket** и добавьте его в автозагрузку:

```
systemctl enable --now cri-docker.socket
```

15. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

16. Проверьте доступность локального хранилища:

```
ping 10.0.2.20

PING 10.0.2.20 (10.0.2.20) 56(84) bytes of data.
64 bytes from 10.0.2.20: icmp_seq=1 ttl=64 time=0.248 ms
64 bytes from 10.0.2.20: icmp_seq=2 ttl=64 time=0.312 ms
64 bytes from 10.0.2.20: icmp_seq=3 ttl=64 time=0.391 ms
64 bytes from 10.0.2.20: icmp_seq=4 ttl=64 time=0.413 ms
--- 10.0.2.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.248/0.341/0.413/0.065 ms
```

17. Проверьте доступность образов:

```
kubeadm config images list --image-repository 10.0.2.20:5000

[I1121 13:16:04.377507   33239 version.go:256] remote version is much newer: v1.28.4; falling back to: stable-1.24
10.0.2.20:5000/kube-apiserver:v1.24.17
10.0.2.20:5000/kube-controller-manager:v1.24.17
10.0.2.20:5000/kube-scheduler:v1.24.17
10.0.2.20:5000/kube-proxy:v1.24.17
10.0.2.20:5000/pause:3.7
```

```
10.0.2.20:5000/etcd:3.5.6-0
10.0.2.20:5000/coredns:v1.8.6
```

18. Загрузите образы контейнеров из локального хранилища, необходимые kubeadm для инициализации ноды кластера:

```
kubeadm config images pull --image-repository 10.0.2.20:5000 --cri-socket unix:///var/run/cri-dockerd.sock
```

19. Запустите инициализацию мастер-ноды в одноранговом кластере. Данная команда выполнит начальную настройку и подготовку основного узла кластера. Ключ `--pod-network-cidr` задает адрес внутренней подсети для вашего кластера.

```
kubeadm init --image-repository 10.0.2.20:5000 --pod-network-cidr=10.244.0.0/16 --cri-socket unix:///var/run/cri-dockerd.sock
```

В случае успешной инициализации, в конце вывода команды будет отображаться примерно следующее:

```
Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

20. Настройте параметры управления кластером. Настройку можно выполнить как для локального пользователя, так и для суперпользователя root.

Для управления кластером от имени ***локального*** пользователя выполните команды:

```
mkdir /home/$USER/.kube
cp -i /etc/kubernetes/admin.conf /home/$USER/.kube/config
chown $USER. /home/$USER/.kube /home/$USER/.kube/config
```

Для управления кластером от имени суперпользователя **root** выполните команду:

```
export KUBECONFIG=/etc/kubernetes/admin.conf
```

Выполните настройку **/etc/resolv.conf**. В случае если настройка **/etc/resolv.conf** не предполагается, внесите изменения в **configmap** для **coredns**:

```
kubectl edit configmap coredns -n kube-system
```

удалите следующие строки:

```
forward . /etc/resolv.conf {
   max_concurrent 1000
 }
```

> **Примечание.**
>
> Если настройка производилась для *локального* пользователя, **выйдите** из сеанса пользователя **root** командой `exit` и дальнейшие действия по настройке кластера выполняйте от имени *локального* пользователя.

21. Настройте внутреннюю конфигурацию сети в кластере (в примере используется **calico**).

21.1 Для этого на машине с выходом в Интернет необходимо загрузить следующие образы:

```
docker pull docker.io/calico/cni:v3.25.0
docker pull docker.io/calico/node:v3.25.0
docker pull docker.io/calico/kube-controllers:v3.25.0
```

21.2 Задать теги для загруженных образов:

```
docker tag docker.io/calico/cni:v3.25.0 10.0.2.20:5000/cni:v3.25.0
docker tag docker.io/calico/node:v3.25.0 10.0.2.20:5000/node:v3.25.0
docker tag docker.io/calico/kube-controllers:v3.25.0 10.0.2.20:5000/kube-controllers:v3.25.0
```

21.3 Сохранить в архив и отправить образы на машину с настроенным локальным registry:

```
docker save 10.0.2.20:5000/cni:v3.25.0 > cni.tar
docker save 10.0.2.20:5000/node:v3.25.0 > node.tar
docker save 10.0.2.20:5000/kube-controllers:v3.25.0 > kube-ctrl.tar
scp cni.tar node.tar kube-ctrl.tar registry:~
```

21.4 Распаковать образы на машине с настроенным локальным registry:

```
docker load -i cni.tar
docker load -i node.tar
docker load -i kube-ctrl.tar
```

21.5 Загрузить распакованные образы в локальное хранилище:

```
docker push 10.0.2.20:5000/cni:v3.25.0
docker push 10.0.2.20:5000/node:v3.25.0
docker push 10.0.2.20:5000/kube-controllers:v3.25.0
```

21.6 На машине с выходом в Интернет необходимо дополнительно скачать файл конфигурации calico:

```
curl -o calico.yaml https://raw.githubusercontent.com/projectcalico/calico/v3.25.0/manifests/calico.yaml
```

и привести следующие строки:

Номер строки	Имя образа
4443	docker.io/calico/cni:v3.25.0
4471	docker.io/calico/cni:v3.25.0
4514	docker.io/calico/node:v3.25.0
4540	docker.io/calico/node:v3.25.0
4757	docker.io/calico/kube-controllers:v3.25.0

к следующему виду:

Номер строки	Имя образа
4443	10.0.2.20:5000/cni:v3.25.0
4471	10.0.2.20:5000/cni:v3.25.0
4514	10.0.2.20:5000/node:v3.25.0
4540	10.0.2.20:5000/node:v3.25.0
4757	10.0.2.20:5000/kube-controllers:v3.25.0

Например:

было:

```
- name: upgrade-ipam
    image: docker.io/calico/cni:v3.25.0
    imagePullPolicy: IfNotPresent
    command: ["/opt/cni/bin/calico-ipam", "-upgrade"]
    envFrom:
```

стало:

```
- name: upgrade-ipam
      image: 10.0.2.20:5000/cni:v3.25.0
      imagePullPolicy: IfNotPresent
      command: ["/opt/cni/bin/calico-ipam", "-upgrade"]
      envFrom:
```

Сохраните внесенные в конфигурацию изменения и передайте файл на машину с настраиваемой **master**-нодой.

21.7 На **master**-ноде примените внутреннюю конфигурацию сети в кластере:

```
kubectl apply -f calico.yaml
```

Потребуется некоторое время для настройки (от 2 до 5 минут).

22. После применения конфигурации проверьте список и статус всех подов в кластере:

```
kubectl get all -n kube-system
```

23. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname masternode
```

Проверьте изменения:

```
hostname && hostname -I

masternode
10.0.2.16
```

24. В файл **/etc/hosts** внесите данные о **master** и **worker**:

```
sudo nano /etc/hosts
```

```
10.0.2.16 masternode
 10.0.2.17 worker
```

Для вывода команды присоединения **worker** к кластеру выполните:

```
kubeadm token create --print-join-command

kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

Настройка рабочих нод

1. Для работы **kubelet** отключите **swap**:

- выполните команду для разового отключения:

  ```
  swapoff -a
  ```

- чтобы **swap** не появился после перезагрузки сервера, выполните команду:

  ```
  swapoff -a && sed -i '/ swap / s/^\(.*\)$/#\1/g' /etc/fstab
  ```

2. Установите необходимые пакеты:

```
dnf install kubernetes kubernetes-kubeadm docker-ce tc ipvsadm ebtables socat conntrack git curl wget
```

ВАЖНО!

Если настраиваемая машина не имеет доступа в Интернет, потребуется предварительно настроить локальный репозиторий ОС, из которого будет производиться дальнейшая установка необходимых для работы пакетов. Подробную информацию о настройке

локального репозитория см. в нашей статье «Создание локального репозитория».

3. Настройте проброс портов в **iptables**:

```
iptables -P FORWARD ACCEPT
```

4. Создайте файл для автозагрузки модулей ядра, необходимых для работы сервиса **cri-dockerd**:

```
nano /etc/modules-load.d/cridockerd.conf
```

```
overlay
br_netfilter
```

Загрузите модули в ядро:

```
modprobe overlay
modprobe br_netfilter
```

Проверьте, что данные модули работают:

```
lsmod | egrep "br_netfilter|overlay"
```

5. Создайте конфигурационный файл для работы сети внутри **kubernetes**:

```
nano /etc/sysctl.d/99-kubernetes-cri.conf
```

```
net.bridge.bridge-nf-call-iptables = 1
net.ipv4.ip_forward = 1
net.bridge.bridge-nf-call-ip6tables = 1
```

Примените параметры командой:

```
sysctl --system
```

6. Установите дополнительный плагин для **docker**:

```
dnf install cri-dockerd
```

7. Запустите службу **cri-docker.service** и добавьте ее в автозагрузку:

```
systemctl enable --now cri-docker.service
```

8. Запустите службу **docker** и добавьте ее в автозагрузку:

```
systemctl enable --now docker
```

9. Внесите изменения в файл конфигурации службы **cri-docker.service**:

```
nano /usr/lib/systemd/system/cri-docker.service
```

Замените строку:

```
ExecStart=/usr/bin/cri-dockerd --container-runtime-endpoint fd://
```

на

```
ExecStart=/usr/bin/cri-dockerd --pod-infra-container-image=<registry>/pause:<версия> --container-runtime-endpoint fd://
```

где:

- <registry> – путь к настроенному локальному хранилищу образов (в примере **10.0.2.20:5000/registry**);
- <версия> – версия пакета pause (для **kubernetes-1.24** используется версия **pause:3.7**).

10. В файле конфигурации демона **docker** укажите, что с созданным хранилищем можно взаимодействовать:

```
nano /etc/docker/daemon.json
```

```
{
 "insecure-registries": ["10.0.2.20:5000"],
 "log-driver": "journald",
 "live-restore": true,
 "icc": false,
 "disable-validation": true
 }
```

где:

- 10.0.2.20 – IP-адрес машины с локальным **regisrty**;
- 5000 – порт для подключения к локальному **regisrty** (по умолчанию).

11. Перезагрузите конфигурации служб:

```
systemctl daemon-reload
```

12. Перезапустите службу **docker**:

```
systemctl restart docker
```

13. Перезапустите службу **cri-docker.service**:

```
systemctl restart cri-docker.service
```

14. Запустите сокет **cri-docker.socket** и добавьте его в автозагрузку:

```
systemctl enable --now cri-docker.socket
```

15. Добавьте службу **kubelet** в автозагрузку:

```
systemctl enable kubelet.service
```

16. Выполните дополнительную настройку сети:

```
sudo hostnamectl set-hostname worker
```

Проверьте изменения:

```
hostname && hostname -I

worker
10.0.2.17
```

17. В файл **/etc/hosts** внесите данные о master и worker:

```
sudo nano /etc/hosts
```

```
10.0.2.16 masternode
 10.0.2.17 worker
```

Подключение worker к кластеру

1. На master-ноде получите команду присоединения *worker*:

```
kubeadm token create --print-join-command
```

```
kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 \
 --discovery-token-ca-cert-hash sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391
```

2. На *worker* выполните полученную команду:

```
 kubeadm join 10.0.2.16:6443 --token bh5nw3.uz8a96nhao7u0ue2 --discovery-token-ca-cert-hash
sha256:e3623f73dadb313ea38e5f04736da6b662925aa78b07d00c50fca6aa0f30e391 --cri-socket unix:///var/run/cri-
dockerd.sock

[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiserver and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.
```

3. На *master* выполните команду для вывода списка нод кластера и их статуса:

```
 kubectl get nodes

NAME                 STATUS   ROLES          AGE    VERSION
localhost.localdomain   Ready    control-plane   5h3m   v1.24.17
worker               Ready    <none>         89s    v1.24.17
```

Flatpak - изолированная среда для запуска приложений

Добавление репозиториев
Поиск по репозиториям
Установка пакетов
Запуск программ flatpak
Удаление программ
Обновление программ
Поиск и установка программ с помощью Flathub

Flatpak - это утилита для развёртывания, управления пакетами и виртуализации для Linux. Предоставляет специально выделенную, изолированную среду, в которой пользователи могут запускать приложения без влияния на основную систему.

Для работы с утилитой *Flatpak* пакеты могут использовать как **Flathub** (репозиторий разработчика), так и сторонние репозитории. Библиотеки приложений могут находиться в одном пакете вместе с приложением или же в окружениях, общих для нескольких пакетов.

Для установки утилиты *flatpak* необходимо выполнить команду:

```
sudo dnf install flatpak
```

Добавление репозиториев

Для добавления репозитория *flathub* используется команда:

```
flatpak remote-add --user --if-not-exists flathub https://flathub.org/repo/flathub.flatpakrepo
```

Кроме того существует ещё несколько репозиториев, например:

- репозиторий программ *Gnome*:

```
flatpak remote-add --user --if-not-exists gnome-nightly https://nightly.gnome.org/gnome-nightly.flatpakrepo
```

- репозиторий программ *KDE*:

```
flatpak remote-add --user --if-not-exists kdeapps --from https://distribute.kde.org/kdeapps.flatpakrepo
```

Посмотреть все добавленные репозитории можно, выполнив команду:

```
flatpak remotes

 Name      Параметры
flathub    user
```

Поиск по репозиториям

Вы можете посмотреть все пакеты, которые есть в репозитории. Для этого следует выполнить команду **remote-ls** с переданным ей именем репозитория:

```
flatpak remote-ls --user flathub
```

```
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.12
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.13
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.14
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.15
Footprints              org.kicad.KiCad.Library.Footprints           stable
Packages3D              org.kicad.KiCad.Library.Packages3D           5.1
Packages3D              org.kicad.KiCad.Library.Packages3D           stable
Symbols                 org.kicad.KiCad.Library.Symbols              stable
Templates               org.kicad.KiCad.Library.Templates            stable
Help                    org.libreoffice.LibreOffice.Help             stable
Codecs                  org.pitivi.Pitivi.Codecs                     stable
bdj                     org.videolan.VLC.Plugin.bdj                  3-19.08
bdj                     org.videolan.VLC.Plugin.bdj                  3-20.08
fdkaac                  org.videolan.VLC.Plugin.fdkaac               3-19.08
fdkaac                  org.videolan.VLC.Plugin.fdkaac               3-20.08
makemkv                 org.videolan.VLC.Plugin.makemkv              3-19.08
makemkv                 org.videolan.VLC.Plugin.makemkv              3-20.08
```

Данная команда выводит полный список пакетов, входящих в репозиторий.

Для того чтобы найти нужный пакет по имени, используйте команду **flatpak search** . Рассмотрим на примере *pidgin*:

```
flatpak search pidgin
```

```
[user@master ~]$ flatpak search pidgin
Имя        Полное описание                          ID Приложения        Версия     Ветка      Удаленные репозитории
Pidgin     Клиент для мгновенного обмена сообщениями  im.pidgin.Pidgin     2.14.13    stable     flathub
```

Для установки программы вам понадобится имя пакета программы из колонки **Application ID** и имя репозитория из колонки **Remotes**.

Установка пакетов

Для установки пакета *flatpak* используйте команду **flatpak install** . Например, установим Pidgin, найденный предыдущей командой:

```
flatpak install flathub im.pidgin.Pidgin
```

```
[user@master ~]$ flatpak install flathub im.pidgin.Pidgin
Поиск похожих запросов...

Разрешения im.pidgin.Pidgin:
    ipc                 network               pulseaudio                  x11
    file access [1]     dbus access [2]       system dbus access [3]

    [1] xdg-download
    [2] org.freedesktop.Notifications
    [3] org.freedesktop.Avahi


       ID                        Ветка      Оп     Удалённый репозиторий    Загрузка
 1. [✓] im.pidgin.Pidgin.Locale  stable     i      flathub                  234,0 kB / 13,6 MB
 2. [/] im.pidgin.Pidgin         stable     i      flathub                    7,5 MB / 8,9 MB

Установка 2/2... ▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕ 100%  7,5 MB/s
```

Если вы не хотите добавлять репозиторий в систему, вы можете установить программу по ссылке из сети. Просто скопируйте ссылку на файл **.flatpakref** и передайте её программе:

```
flatpak install --user --from https://dl.flathub.org/repo/appstream/im.pidgin.Pidgin.flatpakref
```

Посмотреть все установленные программы можно выполнив команду:

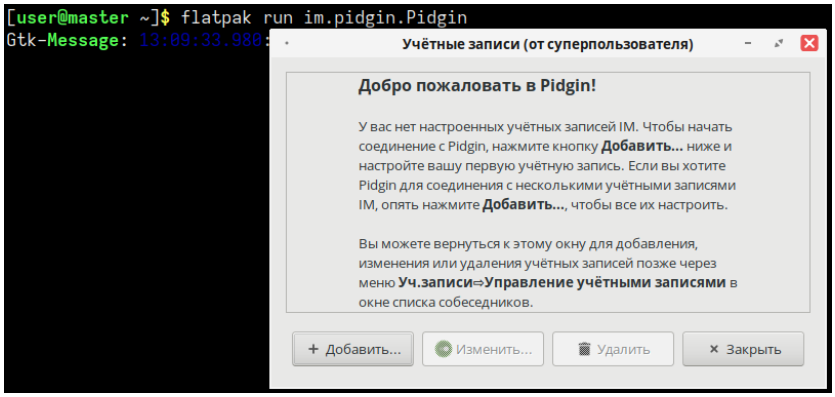
```
flatpak list
```

```
[user@master ~]$ flatpak list
Имя                                ID Приложения                          Версия     Ветка          Тип установки
Pidgin                             im.pidgin.Pidgin                       2.14.13    stable         user
Mesa                               org.freedesktop.Platform.GL.default    24.1.3     23.08          user
Mesa (Extra)                       org.freedesktop.Platform.GL.default    24.1.3     23.08-extra    user
openh264                           org.freedesktop.Platform.openh264      2.4.1      2.4.1          user
GNOME Application Platform version 46  org.gnome.Platform                              46             user
```

Запуск программ flatpak

Программы, установленные с помощью *flatpak*, можно запустить из главного меню. Для запуска с помощью терминала можно использовать команду **flatpak run**:

```
flatpak run im.pidgin.Pidgin
```



Удаление программ

Для удаления программы используйте команду **flatpak uninstall** , например, для Pidgin:

```
flatpak uninstall im.pidgin.Pidgin

   ID                  Ветка    Op
1. im.pidgin.Pidgin          stable   r
2. im.pidgin.Pidgin.Locale   stable   r
```

После удаления пакета можно удалить неиспользуемые компоненты, чтобы освободить место на диске:

```
flatpak uninstall --unused
```

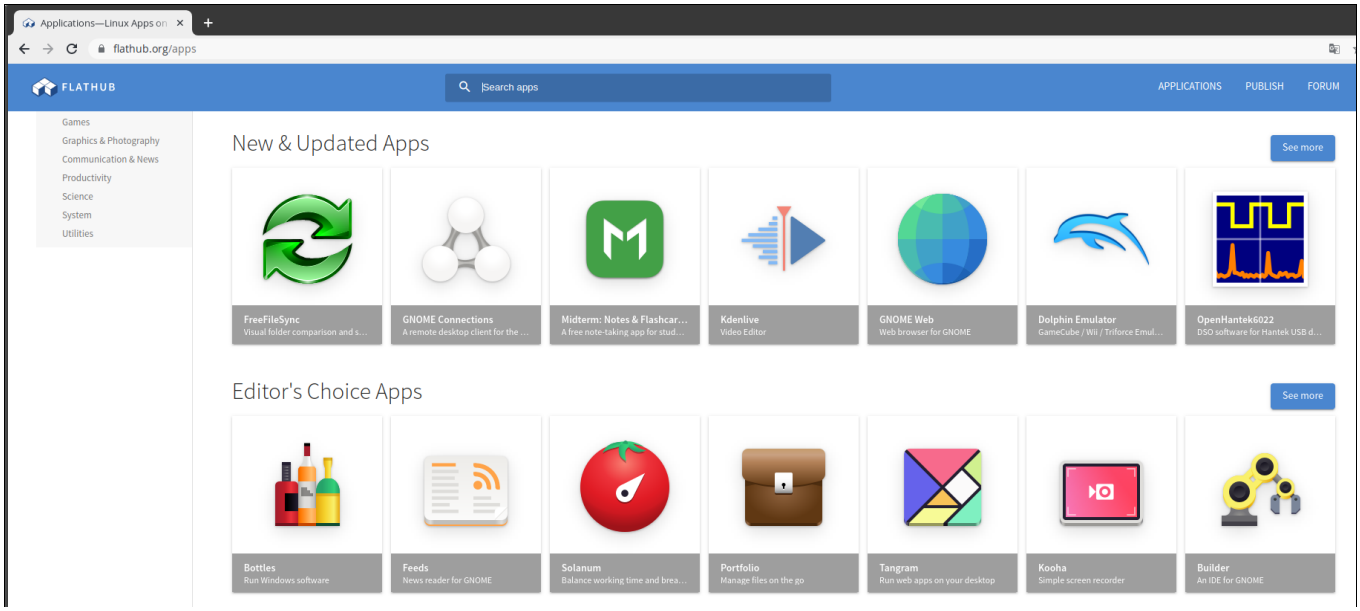
Обновление программ

Как и в любом другом пакетном менеджере, в *flatpak* можно обновлять установленные программы до самой новой версии. Для этого используется команда:

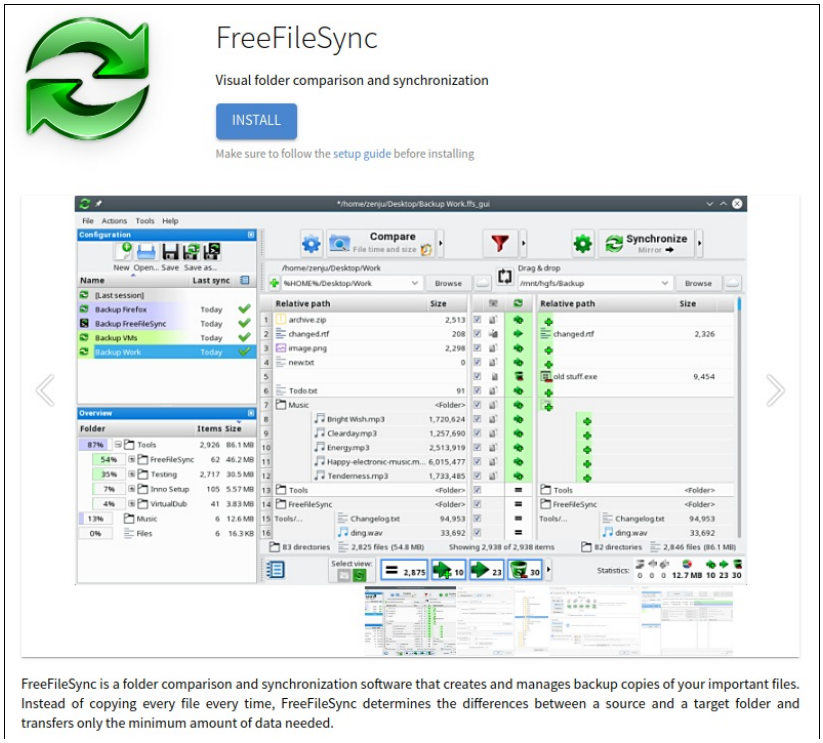
```
flatpak update
```

Поиск и установка программ с помощью Flathub

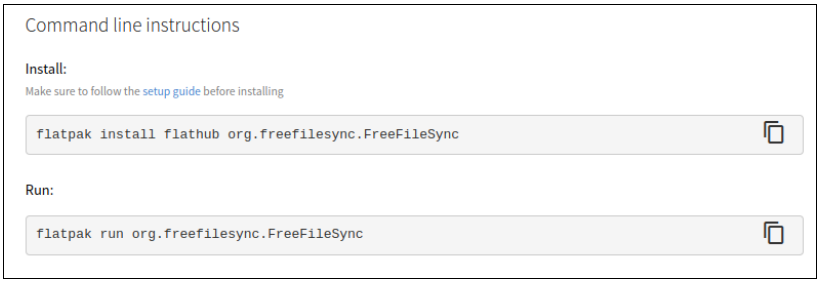
Несмотря на то, что *Flatpak* децентрализованный, большинство самых популярных пакетов вы можете найти на сайте *FlatHub*. Выберите нужную программу из списка на сайте https://flathub.org/apps:



Откройте её страницу и нажмите кнопку **Install** для установки программы с помощью центра приложений:



Кроме того внизу страницы есть инструкция, как установить программу с помощью терминала:



Для установки скачанного файла выполните команду:

```
flatpak install --user ~/Загрузки/org.freefilesync.FreeFileSync.flatpakref
```

```
org.freefilesync.FreeFileSync permissions:
    ipc       network               pulseaudio            wayland
    x11       file access [1]       dbus access [2]
        ID                                                Ветка            Op            Удалённый репозиторий            Download
 1. [✓] org.freefilesync.FreeFileSync.Locale              stable           i             flathub                            101,3 kB / 6,2 MB
 2. [|] org.gnome.Platform.Locale                         3.38             i             flathub                          < 326,2 MB (partial)
 3. [ ] org.gnome.Platform                                3.38             i             flathub                          < 346,5 MB
 4. [ ] org.freefilesync.FreeFileSync                     stable           i             flathub                           < 31,2 MB

Installing 2/4…
```

Snap - изолированная среда для запуска приложений

Установка
Работа со snap-пакетами. Установка пакетов
Работа со snap-пакетами. Обновление пакетов
Работа со snap-пакетами. Просмотр установленных пакетов
Работа со snap-пакетами. Поиск пакетов
Работа со snap-пакетами. Информация о пакете
Работа со snap-пакетами. Удаление пакетов
Работа со snap-пакетами. Откат обновления
Работа со snap-пакетами. Временно отключить пакет
Работа со snap-пакетами. Запуск snap-пакетов
Snap Store

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** snapd 2.54.3

Snap — это пакет, который помимо готовой сборки самого приложения, включает в себя все необходимые зависимости и может работать практически в любом дистрибутиве Linux.

Когда вы устанавливаете в систему приложение из Snap-пакета, установка не влияет на другие пакеты и приложения. То есть такое приложение работает в своей «программной среде», но при этом оно может взаимодействовать с другими программами в системе.

Вы можете подробнее ознакомиться с работой и настройкой изолированной программной среды **Snap**, просмотрев наши обучающие видео:

- на **RuTube** — Snap - изолированная среда для запуска приложений. Snap Store;
- в **Яндекс.Дзен** — Snap - изолированная среда для запуска приложений. Snap Store;
- в **VK Видео** — Snap - изолированная среда для запуска приложений. Snap Store.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для того чтобы установить пакет **snap**, необходимо сперва установить демон управления **snap**-пакетами — **snapd**. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install snapd
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

После установки модуль **systemd**, управляющий основным коммуникационным сокетом **snap**, должен быть включен:

```
systemctl enable --now snapd.socket
```

Чтобы включить поддержку классической привязки, введите следующую команду, чтобы создать символическую ссылку между **/var/lib/snapd/snap** и **/snap**:

```
ln -s /var/lib/snapd/snap /snap
```

После этого перезагрузите систему, чтобы убедиться, что пути **snap** были обновлены правильно.

Работа со snap-пакетами

Установка пакетов

Для установки пакетов используется команда вида **snap install <имя_пакета>**.

Пример установки графического редактора **GIMP** из **snap**-пакета:

```
snap install gimp
```

После установки программа доступна из «**Главного меню**» - «**Графика**» - «**GNU Image Manipulation Program**».

Обновление пакетов

Обновление всех установленных пакетов выполняется командой:

```
snap refresh
```

Обновление какого-либо определенного пакета выполняется командой вида **snap refresh <имя_пакета>**. Например:

```
snap refresh gimp
```

Просмотр установленных пакетов

Для просмотра списка установленных пакетов используется следующая команда:

```
snap list
```

```
Name               Version                    Rev    Tracking       Publisher     Notes
bare               1.0                        5      latest/stable  canonical✓    base
core18             20211215                   2284   latest/stable  canonical✓    base
gimp               2.10.28                    383    latest/stable  snapcrafters  -
gnome-3-28-1804    3.28.0-19-g98f9e67.98f9e67 161    latest/stable  canonical✓    -
gtk-common-themes  0.1-59-g7bca6ae            1519   latest/stable  canonical✓    -
snapd              2.53.4                     14295  latest/stable  canonical✓    snapd
```

Поиск пакетов

Для поиска пакетов используется команда вида **snap find <запрос>**. Например:

```
snap find gimp
```

```
Name                   Version  Publisher        Notes  Summary
gimp                   2.10.28  snapcrafters     -      GNU Image Manipulation Program
gutenprint-printer-app 1.0      openprinting✓    -      Gutenprint Printer Application
photogimp              2.10.20  pedro.ermarinho  -      Patch para o GIMP
djpdf                  0.1.6    unrud            -      Create small, searchable PDFs from scanned documents
lazpaint               7.1.6    chronoscz        -      Image editor with raster and vector layers.
```

Информация о пакете

Для получения информации о каком-либо пакете используется команда вида **snap info <имя_пакета>**. Например:

```
snap info gimp
```

Удаление пакетов

Для удаления пакетов используется команда вида **snap remove <имя_пакета>**. Например:

```
snap remove gimp
```

Откат обновления

Если по каким-то причинам вам необходимо отменить обновления, которые были выполнены над каким-либо snap-пакетом, можно

использовать команду вида snap revert <имя_пакета>, чтобы вернуть пакет к предыдущей версии.

Например:

```
snap revert gimp
```

Временно отключить пакет

Чтобы временно отключить пакет, используется команда вида **snap disable <имя_пакета>**. Например:

```
snap disable gimp
```

Запуск snap-пакетов

Для запуска snap-пакета можно использовать команду вида **snap run <имя_пакета>**. Например:

```
snap run gimp
```

Также приложения, установленные через **snap**, можно запускать через **Главное меню**.

Snap Store

Snap Store — это графическое приложение для обнаружения, установки и управления **snap**.

В **Snap Store** представлены избранные и популярные приложения с полезными описаниями, рейтингами, обзорами и скриншотами.

Приложения можно найти либо через просмотр категорий, либо через поиск.

Snap Store также можно использовать для переключения каналов, просмотра и изменения разрешений привязки, а также для просмотра и отправки отзывов и оценок.

Snap Store основан на программном обеспечении **GNOME**, оптимизированном для работы со **snap**.

Для установки **Snap Store** выполните команду:

```
snap install snap-store
```

После установки программа будет доступна в «**Главном меню**» - «**Системные**» - «**Магазин Snap**».

Firejail - система изолированного запуска приложений

Установка

Работа с утилитой

Дополнительные настройки

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** firejail 0.9.56

Firejail — это простая в использовании система изолированного выполнения графических, консольных и серверных приложений, которая снижает риск нарушений безопасности за счет ограничения рабочей среды потенциально уязвимых программ с использованием пространств имен (**namespaces**), фильтрации системных вызовов (**seccomp-bpf**) и возможностей **AppArmor**.

Вы можете подробнее ознакомиться с настройкой и работой системы **firejail**, просмотрев наши обучающие видео:

- на **RuTube** — firejail - система изолированного запуска приложений;
- в **Яндекс.Дзен** — firejail - система изолированного запуска приложений;
- в **VK Видео** — firejail - система изолированного запуска приложений.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **firejail** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install firejail
```

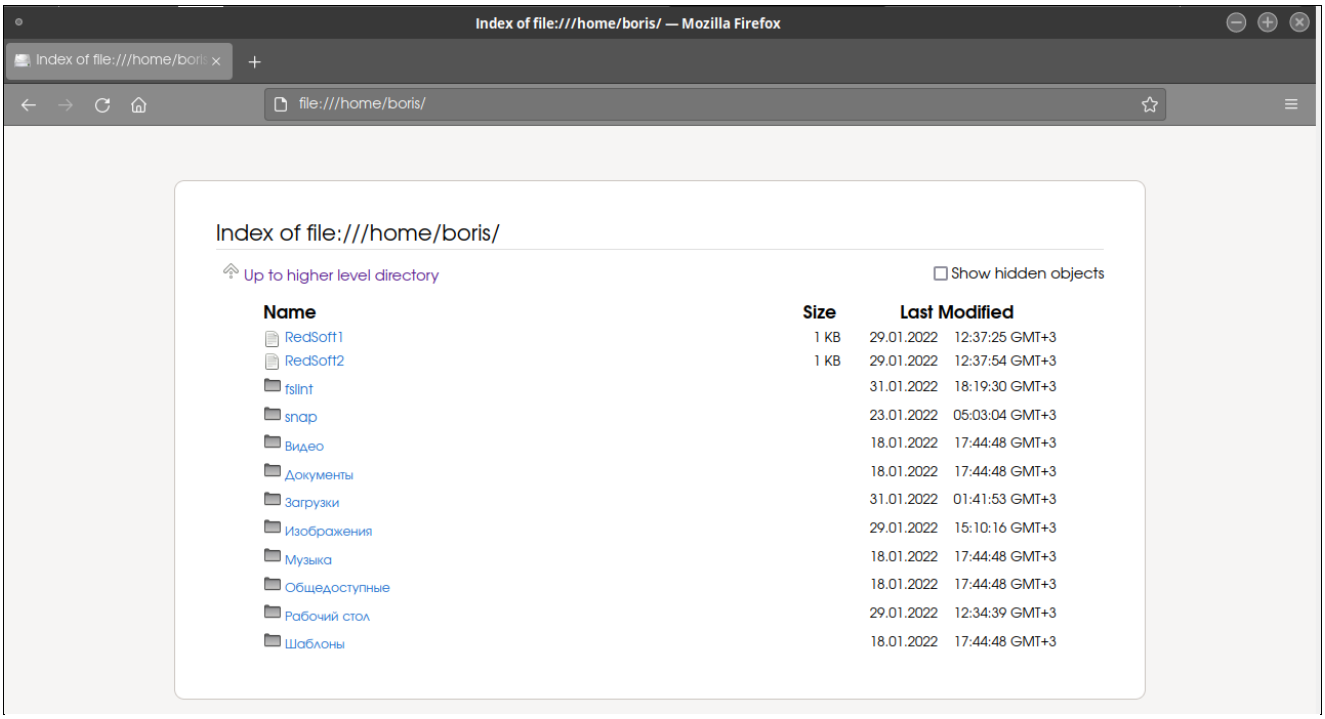
Работа с утилитой

Для того чтобы запустить приложение изолированно, нужно выполнить команду вида **firejail <имя_программы>**:

Например:

```
firejail firefox
```

При запуске браузера обычным способом доступны следующие данные пользователя:



При запуске браузера из контейнера доступ к большинству пользовательских данных ограничен.

Дополнительные настройки

Для просмотра доступных профилей приложений, которые поддерживает **firejail**, выполните:

```
ls /etc/firejail
```

```
[root@localhost firejail]# ls
0ad.profile                         lmms.profile
2048-qt.profile                     lobase.profile
7za.profile                         localc.profile
7z.profile                          lodraw.profile
7zr.profile                         loffice.profile
abrowser.profile                    lofromtemplate.profile
acat.profile                        login.users
adiff.profile                       loimpress.profile
akonadi_control.profile             lollypop.profile
akregator.profile                   lomath.profile
als.profile                         loweb.profile
amarok.profile                      lowriter.profile
amule.profile                       luminance-hdr.profile
android-studio.profile              lximage-qt.profile
anydesk.profile                     lxmusic.profile
aosp.profile                        lynx.profile
apack.profile                       lzcat.profile
apktool.profile                     lzcmp.profile
arch-audit.profile                  lzdiff.profile
archaudit-report.profile            lzegrep.profile
ardour4.profile                     lzfgrep.profile
ardour5.profile                     lzgrep.profile
arduino.profile                     lzip.profile
arepack.profile                     lzless.profile
aria2c.profile                      lzmadec.profile
ark.profile                         lzmainfo.profile
arm.profile                         lzma.profile
artha.profile                       lzmore.profile
```

Далее настройка будет выполняться на примере firefox.

Firejail имеет стандартные настройки по умолчанию. Даже если приложение находится в контейнере, каталог **~/Downloads** и каталоги плагинов в системе доступны. Для того чтобы добавить больше элементов в белый список, перейдите в раздел *whitelist* конфигурационного файла и пропишите свои собственные правила.

Откройте файл:

```
nano /etc/firejail/firefox.profile
```

В нем вы можете настроить доступ к файлам, вносить их в черный и белый списки.

```
# Firejail profile for firefox
 # Description: Safe and easy web browser from Mozilla
 # This file is overwritten after every install/update
 # Persistent local customizations
 include firefox.local
 # Persistent global definitions
 include globals.local

 noblacklist ${HOME}/.cache/mozilla
 noblacklist ${HOME}/.mozilla

 mkdir ${HOME}/.cache/mozilla/firefox
 mkdir ${HOME}/.mozilla
 whitelist ${HOME}/.cache/mozilla/firefox
 whitelist ${HOME}/.mozilla

 # firefox requires a shell to launch on Arch.
 #private-bin firefox,which,sh,dbus-launch,dbus-send,env,bash
 # private-etc must first be enabled in firefox-common.profile
 #private-etc firefox

 # Redirect
 include firefox-common.profile
```

Для того чтобы внести файл в белый список, необходимо прописать:

```
whitelist ~/<расположение_файла>
```

Например:

```
whitelist ~/Pictures
```

Для того чтобы внести файл в черный список, необходимо прописать:

```
blacklist ~/<расположение_файла>
```

Например:

```
blacklist ~/ secret/file/area
```

AppImage - запуск приложений без установки

AppImage — формат для распространения переносимых приложений для большинства систем. Программы в формате **AppImage** состоят всего из одного файла с расширением **.appImage**, например, **gimp.appImage**. Для того чтобы **AppImage**-приложения работали, нужен пакет **fuse** (он уже установлен в систему по умолчанию).

Вы можете подробнее ознакомиться с возможностями **AppImage**, просмотрев наши обучающие видео:

- на **RuTube** — AppImage - запуск приложений без установки;
- в **Яндекс.Дзен** — AppImage - запуск приложений без установки;
- в **VK Видео** — AppImage - запуск приложений без установки.

На наших каналах вы также сможете найти много другой полезной информации.

Рассмотрим работу с **AppImage** на примере **kdenlive**.

Сначала необходимо скачать **kdenlive** с расширением **.appimage** с официального сайта.

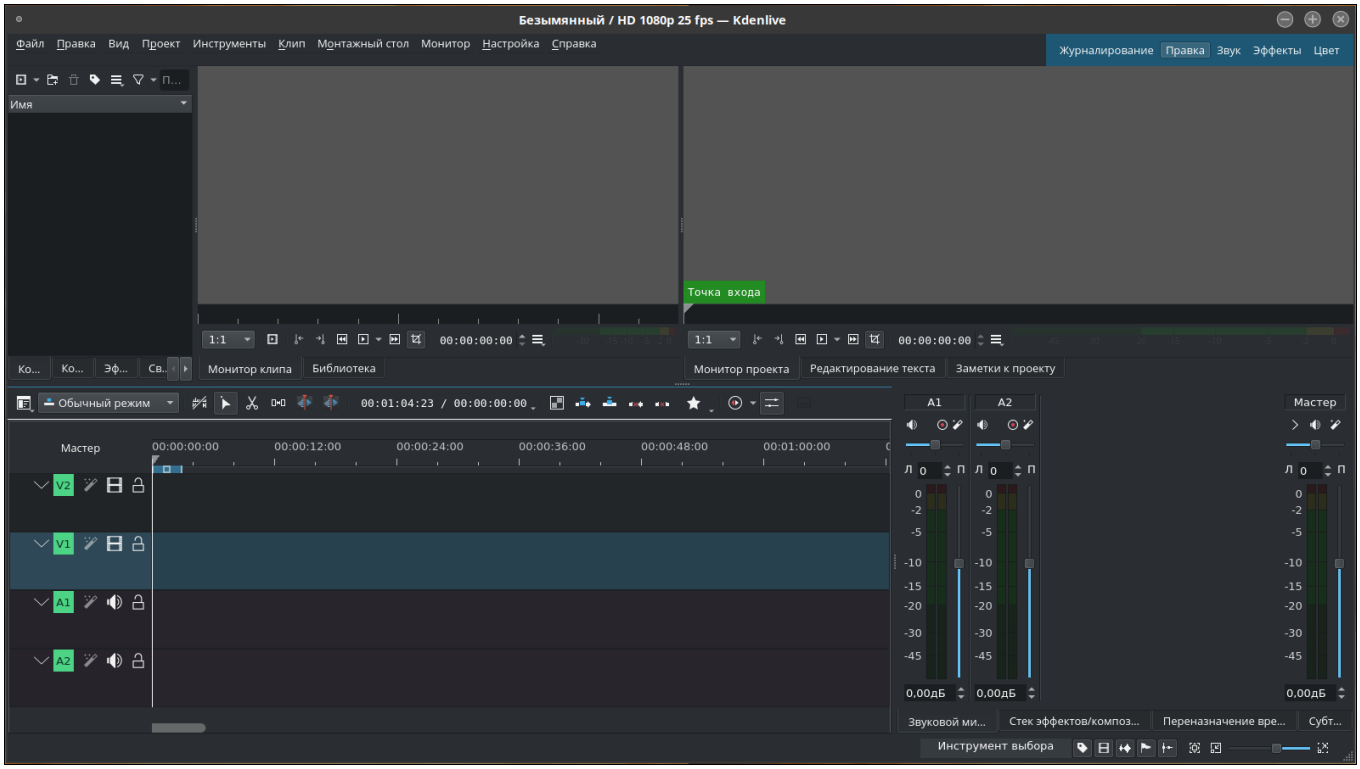
Затем нужно предоставить скачанному файлу права на исполнение. Для этого выполните следующие команды:

```
cd Загрузки
chmod +x kdenlive-21.12.3-x86_64.appimage
```

После этого запустите программу либо двойным щелчком по файлу, либо прописав имя файла в консоли:

```
./kdenlive-21.12.3-x86_64.appimage
```

Если всё было сделано правильно, программа успешно запустится.



Удаление пакетов .appimage

Для удаления программы **AppImage** достаточно удалить соответствующий файл с расширением **.appImage**.

PlayOnLinux - программа запуска приложений Windows

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: playonlinux-4.4-6

PlayOnLinux — программа, позволяющая запускать *Windows*-приложения без эмуляции с помощью прослойки совместимости **Wine**.

PlayOnLinux — это графическая оболочка над **Wine**, которая очень облегчает использование программы. Она содержит готовые скрипты установки, разработанные пользователями. Эти скрипты содержат все необходимое для установки программы.

Вы можете подробнее ознакомиться с установкой и работой утилиты **PlayOnLinux**, просмотрев наши обучающие видео:

- на **RuTube** — PlayOnLinux - программа запуска приложений Windows;
- в **Яндекс.Дзен** — PlayOnLinux - программа запуска приложений Windows;
- в **VK Видео** — PlayOnLinux - программа запуска приложений Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**playonlinux**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.

Для установки **PlayOnLinux** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install playonlinux
```

Для запуска программы через терминал введите команду:

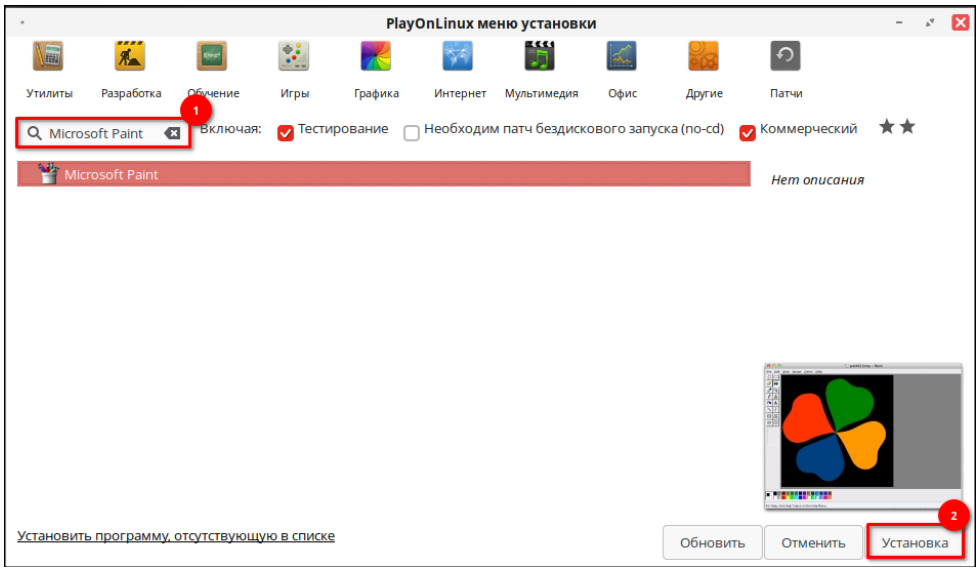
```
playonlinux
```

Для запуска в графическом режиме откройте **«Главное меню**» — «**Стандартные**» — «**PlayOnLinux**».

Интерфейс программы достаточно прост:

- Вверху окна находится **основное меню**, с помощью которого можно получить доступ к большинству функций программы;
- Чуть ниже находится **панель инструментов**, которые позволяют делать основные действия;
- Дальше окно разделено на две панели. На **левой** находятся ярлыки основных действий, например, для установки программ;
- На **правой панели** будет размещен список программ, которые были установлены;
- В нижней части окна находится **статус бар**, где отображается статус обновления или другие данные.

Для установки нужной программы необходимо выбрать в меню пункт «**Установить программу**». Для примера можно установить «**Microsoft Paint**».

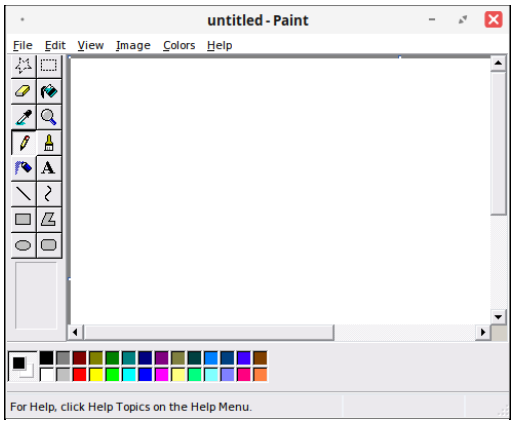


После нажатия на кнопку «**Установка**» откроется мастер установки. Нажмите «**Далее**».

Для загрузки необходимых компонентов и их распаковки нажмите кнопку «**Установить**».

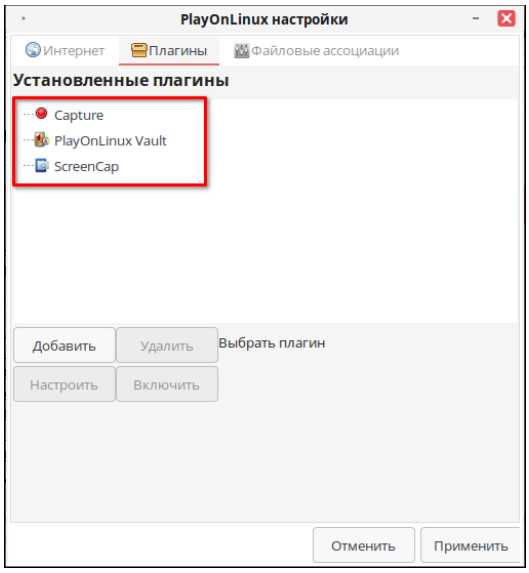
Затем программа предложит установить дополнительные компоненты, загрузить установщик программы **Microsoft Paint** и установить его в стандартном режиме *Windows*.

После всех выполненных действий программа будет готова к работе.



Также **PlayOnLinux** позволяет использовать различные плагины, например;

- **Capture** - позволяет записывать аудио *ALSA* и видео данные *OpenGL* от программы *Wine*, очень полезно для захвата видео;
- **PlayOnLinux Vault** - резервное копирование папок с программами и системными файлами *Wine* и их восстановление;
- **ScreenCap** - создание снимков экрана.



Объединённая служба каталога (LDAP)

Основные термины
Объекты и атрибуты
Установка и настройка
Настройка сервера
База данных ldbm
Настройка репликации
Настройка клиента
Использование LDAP

Служба каталога (Directory Service) — это программный комплекс для хранения и каталогизации информации. По своей сути это очень похоже на обычную базу данных, но с «уклоном» скорее на чтение данных, нежели на их добавление или изменение. Обычно служба каталога базируется на клиент-серверной архитектуре. Одна из наиболее известных таких систем — DNS (Domain Name Service): DNS-сервер производит взаимную «трансляцию» имён машин и их IP-адресов. Другие машины в сети могут обращаться к такому серверу за информацией о соответствии имени и адреса. Однако это очень простой пример каталогизации информации. Объекты в такой базе имеют ограниченное количество атрибутов — таких как имя, адрес и ещё несколько дополнительных параметров.

Протокол **LDAP** (Lightweight Directory Access Protocol) позволяет реализовать доступ по TCP/IP к службе каталогов и может легко расширяться.

Существует несколько реализаций данного протокола от различных фирм. Наиболее известные из них — Netscape Directory Service™, Novell Directory Service™ и Microsoft Active Directory™. Из некоммерческих реализаций LDAP наибольшее распространение получил проект **OpenLDAP**. Именно его мы и будем рассматривать в дальнейшем, хотя большинство понятий и определений применимо и к другим реализациям сервера LDAP.

Основные термины

Данные каталога хранятся в виде объектов или сущностей (от англ. entry), состоящих из специальных полей, называемых атрибутами (attributes). Набор атрибутов, их синтаксис и правила поиска определяются схемой каталога (scheme). Все объекты каталога идентифицируются специальным атрибутом — DN (Distinguished Name).

Данные в каталоге можно представить в виде древовидной структуры — *DIT* (Directory Information Tree). Это очень похоже на структуру, используемую многими файловыми системами. Вершиной такого дерева является корневой объект (*Root Entry*). DN корневого объекта одновременно является суффиксом каталога.

Каждый последующий объект в структуре каталога идентифицируется уникальным значением DN, который описывает путь к объекту в каталоге. Если продолжить аналогию с файловой системой, то DN любого объекта так же включает DN всех объектов, стоящих выше по иерархии. Отличие в данном случае только в том, что DN формируется не слева направо, как путь к файлу, а наоборот — справа налево.

DN администратора каталога (Root Distinguished Name) — это специальный объект, описывающий администратора каталога. Этот объект указывается в конфигурации сервера, но может отсутствовать в самом каталоге. К такому объекту не применяются списки доступа (ACL). В некоторых реализациях LDAP такой объект может не иметь суффикса.

База поиска (Base Distinguished Name) — объект каталога, начиная с которого производится поиск. Дело в том, что не всегда есть необходимость производить поиск по всему дереву каталога; ограничить область поиска можно указанием в запросе базы поиска. По умолчанию этот параметр соответствует суффиксу.

Объекты и атрибуты

Серверы LDAP могут поставляться с несколькими вариантами бэкенда (backend). Например, OpenLDAP имеет такие варианты, как **LDBM** — собственный формат хранения данных в текстовых файлах; **SHELL** — интерфейс к базе данных, использующий команды UNIX; **PASSWD** — простейшая база, использующая стандартные файлы **/etc/passwd** и **/etc/group**; **SQL** — интерфейс к любой базе данных, использующей SQL.
Для процедур импорта и экспорта данных всеми серверами LDAP поддерживается единый формат обмена данными — **LDIF**. Вот пример такого файла с описанием двух объектов:

```
dn: dc=example,dc=com
objectClass: top
objectClass: organization
o: example.com
o: Example Inc.

dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People
description: Example Inc. workers
description: Stuff area
```

Описание каждого объекта в таком файле начинается с атрибута DN. Специальный атрибут **objectClass** указывает, к каким классам относится данный объект и, следовательно, какие атрибуты он может иметь. В нашем случае принадлежность к классу **top** означает,

что объект обязательно должен иметь атрибут **objectClass**, а принадлежность к классу **organization** предполагает наличие нескольких атрибутов, из которых атрибут **o** является обязательным.

Второй объект находится на одну ступеньку ниже по иерархии и поэтому в его DN включён DN объекта верхнего уровня. Этот объект относится к классу **organizationalUnit** и поэтому имеет обязательный атрибут **ou**.

Можно заметить, что некоторые атрибуты (для которых это применимо) могут иметь несколько значений. В данном примере атрибут **description** имеет два значения. А вот для атрибута **dn** допустимо только одно значение.

Классы, характеризующие объекты, и атрибуты, составляющие классы, описываются схемой базы. Её пример приведён ниже.

```
attributetype ( 2.5.4.10 NAME ( 'o' 'organizationName' )
  SUP name
)
attributetype ( 2.5.4.13 NAME 'description'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024}
)
objectclass ( 2.5.6.4 NAME 'organization' SUP top STRUCTURAL
  MUST o
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
    x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ st $ l $ description
  )
)
```

В данном фрагменте приводятся описания двух атрибутов и одного класса. Вот что означают эти записи:
Атрибут **o** (его можно также называть *organizationName*) является расширением атрибута **name**.
Атрибут **description** — это строка длиной до 1024 байт; при поиске в ней регистр символов не учитывается.
Класс **organization** является расширением класса **top** и, следовательно, он включает в себя все атрибуты, составляющие этот класс плюс дополнительные атрибуты, такие как **userPassword, businessAddress, street, postOfficeBox** и т.д. Кроме того, атрибут **o** является обязательным.

Установка и настройка

Процесс сборки и установки сервера OpenLDAP не отличается от установки другого программного обеспечения, поставляемого в виде готового пакета.

Настройка сервера

Сервер LDAP состоит из двух серверных процессов: **slapd** и **slurpd**. Процесс *slapd* занимается приёмом и обработкой запросов от клиентов; это основной процесс, который непосредственно работает с базой данных. Сервис *slurpd* используется в тех случаях, когда данные нужно реплицировать на другие сервера — он контролирует изменения в базе и, при необходимости, пересылает их на подчинённые сервера.

Приведём пример конфигурационного файла:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/nis.schema
```

В первых строках мы подключаем необходимые схемы; в поставке *OpenLDAP* их около полутора десятков. Подключите только те, которые будете использовать. В принципе, схемы являются частью конфигурационного файла, но для наглядности они вынесены в отдельные фрагменты.

```
LSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCertificateFile /etc/openldap/ssl/slapd.pem
TLSCertificateKeyFile /etc/openldap/ssl/slapd.pem
```

LDAP можно использовать для централизованной авторизации пользователей сети вместо **NIS+**. В таких случаях из каталога может запрашиваться конфиденциальная информация — например, пароль. Для предотвращения перехвата этих данных желательно использовать протокол LDAPS (LDAP via SSL/TLS).

База данных ldbm

В качестве способа хранения используется собственный формат LDBM. Если предполагается обычная конфигурация сервера, то данный формат предпочтителен.

```
suffix "dc=example,dc=com"
```

Корнем информационной структуры будет являться объект **dc=example, dc=com**. В принципе, суффикс для каталога можно взять любой, например, *o=Example Inc., c=RU* — это не накладывает абсолютно никаких ограничений на функциональность. Однако последнее время всё чаще используется именно первый вид суффикса, который подчёркивает, что информационная структура данного предприятия тесно связана со структурой его домена.

```
rootdn "cn=admin,dc=server,dc=com"
rootpw secret
```

DN, описывающий администратора и его пароль. В данном случае пароль записан в открытом виде, поэтому файл конфигурации сервера должен иметь соответствующие права доступа, ограничивающие его чтение обычными пользователями. Пароль можно записать и в виде хеша DES или MD5 — тогда строка будет иметь следующий вид:

```
rootpw {MD5}IFJFxyGN3Hap7xsJFBmeTA==
```

Эти опции нужны только на время первичной настройки базы. После того как структура создана и можно регулировать права доступа с помощью ACL, эти опции рекомендуется отключить.

```
index objectClass eq
```

Формат *ldbm* поддерживает простейшие индексы с целью ускорения операций поиска. Такие индексы желательно создавать по атрибутам, предполагающим наибольшее количество запросов. Последний параметр данной опции указывает по какому критерию создаётся индекс. Это могут быть **pres, eq, approx, sub, none** (present, equality, approximate, substring, no index).

```
access to attr=userPassword
  by dn=".*,ou=Admins,dc=example,dc=com" write
  by self write
  by anonymous auth
  by * none

access to * by * read
```

Данные каталога не всегда находятся в публичном доступе. Для управления доступом могут использоваться списки доступа (*access lists*). В данном примере приводятся два списка — в первом из них ограничивается доступ к атрибуту **userPassword** (полный доступ к нему могут иметь только сам объект либо администраторы базы; для всех остальных доступ запрещён). Второе правило гласит, что всем даётся доступ на чтение любых данных (кроме ограниченного предыдущим правилом).

После настройки можно сразу запустить процесс **slapd** — например, такой командой:

```
# service slapd start
```

Первый объект, который нужно создать в базе — корневой элемент (*root entry*), который указан в конфигурационном файле как **suffix**.

Настройка репликации

Одной из важных особенностей LDAP являются встроенные средства репликации данных. Этот механизм реализован в виде отдельного серверного процесса, контролирующего изменения в базе данных и пересылающего эти изменения на другие серверы. Прежде чем включить такую репликацию, необходимо убедиться в том, что соответствующие данные на обоих серверах идентичны. Это связано с тем, что *slurpd* пересылает именно изменения на текущем сервере — он не проверяет и не анализирует состояние данных на удалённом сервере. Настройки *slurpd* находятся в том же файле, что и настройки *slapd*, поэтому перечислим, что нужно добавить к перечисленным выше параметрам:

```
replica /var/log/slapd.replog
```

Прежде всего, укажем файл, в который *slapd* будет записывать все свои действия и из которого *slurpd* будет их читать.

```
replica uri=ldap://ldap2.example.com
  bindmethod=simple
  binddn="cn=slurpd,ou=Apps,dc=example,dc=com"
  credentials=secret
```

Реплика такого вида описывается для каждого подчинённого сервера. На подчинённом сервере нужно создать соответствующий объект и указать, что он имеет права на изменение информации. Это делается с помощью соответствующего списка доступа и параметров **updatedn** и **updateref**.

Настройка клиента

Существует огромное количество клиентов, работающих с LDAP. Это могут быть почтовые программы, которые обращаются к каталогу в поисках адреса электронной почты сотрудника или за информацией о маршрутизации почты, FTP-сервер, который берет информацию для авторизации своего клиента и многие другие программы — однако все они имеют схожие настройки. Прежде всего это адрес сервера и порт, на котором работает LDAP (обычно это 389 или, если сервер поддерживает протокол LDAPS, 636). Вторым важным параметром является база поиска (*Base DN*) — в большинстве случаев этот параметр соответствует суффиксу сервера, однако иногда имеет смысл сузить область поиска. Например, если мы ищем пользователя, чтобы авторизовать его на почтовом сервере, то вряд ли его нужно искать среди групп пользователей или списка компьютеров локальной сети. Третий важный параметр — фильтр поиска, т.е. критерий, по которому мы выбираем объект из базы. Кроме того, существуют параметры, позволяющие ограничить поиск снизу — например, только самой базой или базой и её подобъектами первого уровня, параметры, управляющие поиском в алиасах (*alias*), и т.п.

Трёх этих параметров (сервер, база поиска и фильтр) в большинстве случаев достаточно, чтобы выполнить запрос к любому серверу LDAP. Однако, если на сервере существуют ограничения на доступ к данным, может потребоваться авторизация. Авторизоваться в LDAP можно, указав DN одного из объектов базы данных LDAP; пароль для такого объекта будет искаться в его атрибуте **userPassword**.

Ниже приводится фрагмент настройки почтового сервера Postfix:

```
virtual_maps = ldap:virtual, hash:/etc/postfix/virtual
virtual_server_host = localhost
virtual_search_base = ou=People,dc=example,dc=ru
virtual_query_filter = (&(objectclass=inetLocalMailRecipient)(cn=%s))
virtual_result_attribute = mailLocalAddress,mailRoutingAddress
```

В данном фрагменте описывается, что при определении адреса получателя делается запрос в LDAP с целью найти объект, которому это письмо адресовано. Поиск делается по атрибуту **cn**. Результат берётся из атрибутов **mailLocalAddress** и **mailRoutingAddress**. Эти классы и атрибуты описаны схемой **misc**.

Использование LDAP

LDAP может использоваться в самых различных ситуациях. Здесь мы рассмотрим несколько наиболее распространённых его применений. Поскольку в LDAP хранится полная информация о сотрудниках предприятия, мы можем брать справочную информацию для почтовых программ прямо оттуда. Для начала настроим сервер:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/misc.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/openldap.schema

pidfile        /var/run/slapd.pid
argsfile       /var/run/slapd.args

loglevel 512

database       ldbm
directory      /var/lib/ldap/base/example.com
password-hash  {MD5}

suffix         "dc=example,dc=com"
#rootdn         "cn=admin,dc=example,dc=com"
#rootpw         secret

access to attr=userPassword
  by dn=".*,ou=Admins,dc=example,dc=com"
  by anonymous auth
  by self write
  by * none
access to * by * read

index objectClass,uid,uidNumber,gidNumber     eq
index cn,mail,surname,givenname               eq,sub
```

После этого создадим пользователя **ldap**, от имени которого будет работать наш сервер и запустим процесс **slapd** следующей командой:

```
# slapd -u ldap -h 'ldap://127.0.0.1/ ldap//ldap.example.com/ ldaps://ldap.example.com'
```

Теперь можно создать базу данных — например, с помощью утилиты ldapadd или slapadd:

```
# ldapadd -xWD cn=admin,ou=Admins,dc=example,dc=com -H ldaps://ldap.server.com -f initial.ldif
```

Или, если сервер не запущен:

```
# slapadd -b dc=example,dc=com -l initial.ldif # chown ldap:ldap /var/lib/ldap/bases/example.com/*
```

Содержимое файла **initial.ldif** будет такое:

```
dn: dc=example,dc=com
objectClass: top
objectClass: organization
o: Exapmle Inc.
o: exapmle.com

dn: ou=Admins,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Admins
description: Administrators

dn: cn=admin,ou=Admins,dc=example,dc=com
objectClass: top
objectClass: person
cn: admin
sn: Bender
givenName: Ostap
userPassword: secret
description: Our smart admin

dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People
description: Stuff area

dn: uid=obender,ou=People,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
cn: Ostap Bender
sn: Bender
givenName: Ostap
uid: obender
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/obender
loginShell: /bin/bash
userPassword: {md5}$1$ION4SIII$EYyGEeYt4g2hEe9tjICac.
mail: obender@example.com
mail: obender@attiresandtoes.com

....

dn: ou=Groups,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Groups
description: Groups of users

dn: cn=obender,ou=Groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
cn: luser
gidNumber: 1000
description: Default group for users presented by LDAP
```

Проверим, что сервер работает, сделав к нему анонимный запрос:

```
$ ldapsearch -xLLL "(uid=obender)"
```

```
dn: uid=obender,ou=People,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
cn: Ostap Bender
sn: Bender
givenName: Ostap
uid: migor
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/obender
loginShell: /bin/bash
mail: obender@example.com
mail: obender@attiresandtoes.com
```

Поскольку, согласно нашим настройкам, доступ к атрибуту **userPassword** имеют только сам пользователь и администратор, то этот атрибут мы не получили.

Настройка доступа к компьютеру по его сетевому имени

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для подключения к компьютеру в сети удобнее обращаться к нему по сетевому имени, потому что IP-адрес компьютера может динамически измениться, если адрес был назначен dhcp сервером.
Если у вас не используется DNS сервер для разрешения имен ПК, то включите разрешение имени **NetBIOS** — это процесс определения **IP-адреса** по имени.
Для этого откройте (от root) файл на редактирование /etc/nsswitch.conf, найдите строку с параметром **hosts** и приведите ее к следующему виду (добавив параметр **wins)**:

```
hosts: files wins dns myhostname mdns4_minimal [NOTFOUND=return]
```

В РЕД ОС версии 7.3 и старше изменять конфигурацию /etc/nsswitch.conf следует через файл

```
nano /etc/authselect/user-nsswitch.conf
```

после чего выполнить применение настроек:

```
authselect apply-changes
```

Включите службу winbind:

```
systemctl enable winbind
systemctl start winbind
```

Включите службу nmb:

```
systemctl enable nmb
systemctl start nmb
```

Проверьте работу:

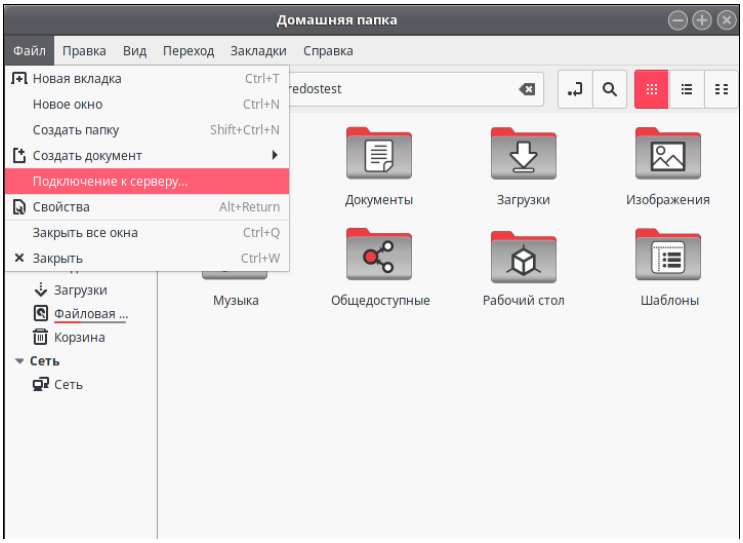
```
ping win10
```

где win10 — это имя компьютера с ОС Windows.

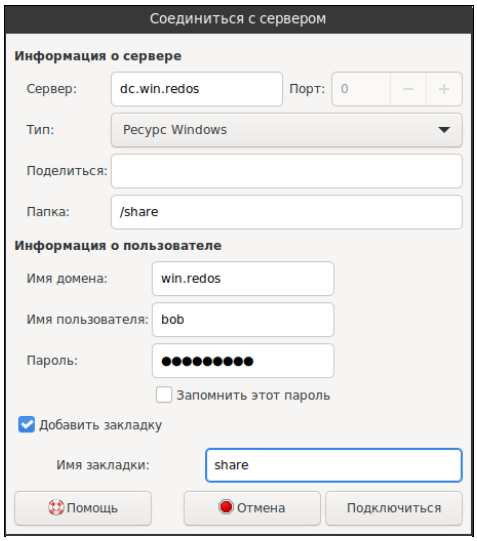
Подключение сетевых директорий с помощью графического приложения

Для авторизованного входа к сетевым ресурсам windows воспользуйтесь логином и паролем.

1. Откройте файловый менеджер, перейдите в меню «**Файл**» — «**Подключение к серверу**».



2. В открывшемся окне выберите тип подключения «**Общий ресурс Windows**». В разделе «**Информация о сервере**» в поле «**Сервер**» укажите IP-адрес сервера или доменное имя, в поле «**Папка**» впишите имя подключаемого сетевого каталога. В разделе «**Информация о пользователе**» заполните поля «**Имя домена**», «**Имя пользователя**» и «**Пароль**». Нажмите кнопку «**Соединиться**». При успешном соединении будет открыта сетевая папка.



Также можно установить флаг «**Добавить закладку**», чтобы ресурс появился в меню слева в файловом менеджере для быстрого доступа.

Подключение сетевых директорий с помощью fstab

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

1. Создайте файл с авторизационными данными:

```
# nano /root/.smbuser
```

```
username=имя_пользователя
password=пароль_пользователя
domain=ДОМЕН
```

Для безопасности ограничьте доступ к файлу с указанными данными:

```
# chmod 400 /root/.smbuser
```

2. Для подключения сетевой директории впишите в конец файла **/etc/fstab** её параметры.

Откройте его в текстовом редакторе:

```
# nano /etc/fstab
```

Синтаксис строки подключения для windows или samba-ресурсов следующий.

```
//<адрес_сервера>/<имя_сетевого_каталога> <каталог_для_монтирования> cifs
credentials=<путь_до_файла_с_авторизационными_данными>,iocharset=utf8,file_mode=0777,dir_mode=0777 0 0
```

При подключении используйте свои параметры.

В случае возникновения ошибки при монтировании общего ресурса, который находится на ПК с ОС Windows, нужно добавить в строку подключения следующий параметр:

```
vers=1.0
```

Пример:

```
//windows_pc/common /mnt/common/ cifs credentials=/root/.smbuser,vers=1.0,iocharset=utf8,file_mode=0777,dir_mode=0777 0 0
```

3. Создайте каталог, куда будет монтироваться папка и назначьте ей права.

```
# mkdir /mnt/common
# chmod 777 /mnt/common
```

Для удобства, можете создать ярлык каталога на рабочем столе, для этого выполните нижеследующую команду, вписав имя своего пользователя.

```
ln -s /mnt/common/ /home/<имя_пользователя>/Рабочий\ стол/Общая
```

4. Выполните монтирование каталога

```
mount -a
```

ВАЖНО!

В некоторых случаях, при загрузке компьютера монтирование происходит быстрее получения IP-адреса, тем самым, монтирование не происходит. Связано это с особенностями конфигурации сети. Для предотвращения подобных случаев можно вписать команду монтирования в файл **/etc/gdm/PreSession/Default**. Тогда монтирование будет происходить при входе пользователей в систему.

Откройте файл **/etc/gdm/PreSession/Default** и впишите в конец строку монтирования, после неё переведите курсор на новую строку и сохраните.

```
# nano /etc/gdm/PreSession/Default
...

mount -a &
```

ВАЖНО!

При подключении сетевой папки на windows server 2003 в опции монтирования надо дописать параметр `vers=1.0`, а так же логин и пароль не должны содержать кириллических символов.

Подключение сетевых директорий с использованием automount (autofs)

Автоматическое монтирование ресурсов CIFS
Автоматическое монтирование FTP-ресурсов
Автоматическое монтирование SSH-ресурсов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версии пакетов**: openssh-8.9p1-6, autofs-5.1.6-7

Установите или обновите пакет **cifs-utils** и **autofs**.

Для этого перейдите в сеанс пользователя **root** и запустите команду:

```
su -
dnf install cifs-utils autofs
```

Автоматическое монтирование ресурсов CIFS

1. Добавьте строку для монтирования в файл **/etc/auto.master**:

```
/mnt/samba    /etc/auto.samba    --ghost
```

- Первое поле - базовая точка монтирования, каталог /mnt/samba вручную создавать **не нужно**, он автоматически создается службой **autofs**.
- Второе поле - файл таблицы (map-файл), соответствующий этой точке монтирования.
- Третье поле необязательно и может содержать опции, которые будут применены ко всем записям таблицы.

2. Создайте файл **/etc/auto.samba** и впишите строку:

```
share    -fstype=cifs,rw,noperm,credentials=/root/.smbuser    ://win10/public
```

- Первое поле - имя автоматически создаваемой autofs папки, в которую монтируется шара.
- Второе поле - параметры подключения и путь к файлу с авторизационными данными.
- Третье поле - адрес сетевого каталога.

Если в пути имеются кириллические символы, то возьмите их в кавычки:
://win10/'мой каталог'

ВАЖНО!

При подключении сетевой папки на **windows server 2003** в опции монтирования надо дописать параметр **vers=1.0**.

Логин и пароль пользователя не должны содержать кириллических символов.

Версия **ядра** РЕД ОС должна быть **ниже 5.15.72**.

Проверьте, что компьютер доступен по имени, например, выполните команду:

```
ping <имя_пк>
```

если отклика нет, то запустите службу **winbind**:

```
systemctl enable winbind --now
```

а в файле **/etc/nsswitch.conf** приведите строку, начинающуюся с hosts, к виду:

```
hosts: files dns myhostname wins
```

Изменять конфигурацию **/etc/nsswitch.conf** следует через файл:

```
nano /etc/authselect/user-nsswitch.conf
```

после чего выполнить применение настроек:

```
authselect apply-changes
```

3. Создайте файл **/root/.smbuser** с логином и паролем пользователя для доступа к общему каталогу.

> **Примечание.**
>
> Если к общему каталогу разрешён анонимный доступ, тогда SMB-пароль задавать не нужно.
>
> Значения параметров в файле с реквизитам учётной записи /root/.smbuserзадавать тоже не нужно (после знака "=" ничего не указывать не надо).

> **ВАЖНО!**
>
> Задайте SMB-пароль пользователю (например, для ivan.ivanov):
>
> ```
> smbpasswd -a ivan.ivanov
> ```

```
nano /root/.smbuser
```

```
username=ivan.ivanov
password=12345678
domain=WORKGROUP
```

Если домена нет, то укажите в параметре domain имя рабочей группы windows.

Для безопасности ограничим доступ к файлу с нашими данными:

```
chmod 400 /root/.smbuser
```

4. Запустите **autofs** и добавьте его в автозагрузку.

```
systemctl enable autofs.service --now
```

Автоматическое монтирование FTP-ресурсов

С подробной информацией о возможности автоматического монтирования FTP-ресурсов можно ознакомиться в нашей статье «Настройка FTP-сервера».

Автоматическое монтирование SSH-ресурсов

1. Устанавливаем дополнительный пакет **sshfs**:

```
dnf install sshfs
```

2. Генерируем ключ ssh:

```
ssh-keygen
```

Когда генератор запросит фразу-пароль, просто нажмите **Enter**.

3. Копируем открытый ключ на удаленный сервер, доступ к которому необходимо настроить:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@10.10.1.7
```

где 10.10.1.7 - адрес удаленного сервера.

А закрытый ключ копируем в домашнюю директорию **root** (не требуется, если предыдущие действия выполнялись от root):

```
sudo cp ~/.ssh/id_rsa /root/.ssh/id_rsa
```

4. Редактируем файл **/etc/auto.master**:

```
nano /etc/auto.master

/mnt/ssh    /etc/auto.ssh    --ghost
```

5. Создаем файл:

```
nano /etc/auto.ssh
```

```
ssh -fstype=fuse,rw,allow_other,IdentityFile=/home/user/.ssh/id_rsa :sshfs\#user@10.10.1.7\:/home/user
```

6. Выполняем перезапуск сервиса **autofs**:

```
systemctl restart autofs
```

Подключение сетевых директорий с помощью fstab и механизма Kerberos

Установите необходимые пакеты:

```
dnf install cifs-utils samba-client krb5-workstation
```

ВАЖНО!

Рабочая станция должна быть введена в домен. Инструкция по вводу доступна в разделе «Работа с доменом MS AD».

Подключение сетевых директорий с помощью fstab

Для подключения сетевой директории впишите в конец файла **/etc/fstab** её параметры.

Откройте его в текстовом редакторе.

Пример:

```
# nano /etc/fstab
//win.ad.test/Public /mnt/pub/ cifs rw,users,sec=krb5,_netdev,nofail,domain=AD.TEST
```

где:

- //win.ad.test/Public - доменное имя файлового сервера и каталог;
- /mnt/pub/ - каталог, в который будет произведено монтирование;
- cifs - тип монтируемой файловой системы;
- rw,users,noauto,sec=krb5 - параметры монтирования;
- domain=AD.TEST - имя домена.

ВАЖНО

при подключении сетевой папки на windows server 2003 в опции монтирования надо дописать параметр vers=1.0, а так же логин и пароль не должны содержать кириллических символов

Создайте каталог, куда будет монтироваться папка и назначьте ей права.

```
# mkdir /mnt/pub
# chmod 777 /mnt/pub
```

Для удобства, можете создать ярлык каталога на рабочем столе, для этого выполните нижеследующую команду, вписав имя своего пользователя.

```
ln -s /mnt/pub/ /home/<имя пользователя>/Рабочий\ стол/Общая
```

Проверьте полученный билет керберос:

```
# klist
```

Если его нет, получите его:

```
# kinit <имя-пользователя>
```

Разрешим выполнять mount от имени суперпользователя (root):

```
# chmod u+s /usr/sbin/mount.cifs
```

Выполните монтирование каталога:

```
mount -a
```

Подключение сетевых директорий с использованием automount (autofs) и механизма Kerberos

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

autofs - это служба, которая автоматически монтирует файловые системы при их использовании, и отключает их позже, когда файловые системы перестают использоваться. **autofs** может работать с сетевыми файловыми системами, компакт-дисками и т. д.

ВАЖНО!

Рабочая станция должна быть введена в домен. Инструкции по вводу рабочей станции в домен доступны в разделе «Работа с доменом MS AD».

Вы можете подробнее ознакомиться с возможностью автоматического монтирования ресурсов и директорий, просмотрев наши обучающие видео:

- на **RuTube**:
  - Монтирование файловых систем в РЕД ОС;
  - Подключение сетевых директорий с помощью automount (autofs) и механизма Kerberos .
- в **Яндекс.Дзен**:
  - Монтирование файловых систем в РЕД ОС;
  - Подключение сетевых директорий с помощью automount (autofs) и механизма Kerberos .
- в **VK Видео**:
  - Монтирование файловых систем в РЕД ОС;
  - Подключение сетевых директорий с помощью automount (autofs) и механизма Kerberos .

На наших каналах вы также сможете найти много другой полезной информации.

1. Установите пакет **cifs-utils** и **autofs** (если они не установлены). Для этого перейдите в сеанс пользователя **root** или запустите команду от sudo-пользователя:

```
$ su -
# dnf install cifs-utils autofs
```

2. Войдите в систему **под учетной записью доменного пользователя** и проверьте билет Керберос командой (именно **от доменного пользователя**, а не от root):

```
$ klist
```

Пример вывода команды:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_51105
Default principal: u1@WIN.REDOS

Valid starting       Expires              Service principal
23.01.2020 15:41:54  24.01.2020 01:41:54  krbtgt/WIN.REDOS@WIN.REDOS
 renew until 30.01.2020 12:04:05
```

Для выполнения **всех** последующих действий перейдите в сеанс пользователя root (**su -**) или выполните действия от sudo-пользователя.

3. Добавьте строку для монтирования в файл **/etc/auto.master**

Для РЕД ОС 7.3 целесообразно создать точку монтирования сетевой папки в **/media**, потому что каталоги, созданные в **/media**, будут отображаться на рабочем столе и в файловых менеджерах *Nemo/Caja* (в левой колонке). В файловых менеджерах

Nemo/Caja монтировать данные каталоги можно будет одним кликом.

```
# nano /etc/auto.master
```

```
/media/samba    /etc/auto.samba    --ghost
```

- Первое поле (в примере - **/media/samba**) - базовая точка монтирования, которая выступает родительским каталогом для подключаемых общих сетевых ресурсов (они будут располагаться именно в этом каталоге)
- Второе поле (в примере - **/etc/auto.samba**) - файл таблицы (map-файл), соответствующий этой точке монтирования.
- Третье поле (в примере это –-**ghost**) необязательно и может содержать опции, которые будут применены ко всем записям таблицы.

4. Создайте файл **/etc/auto.samba** и впишите туда строку

```
# nano /etc/auto.samba
```

```
share    -fstype=cifs,multiuser,cruid=$UID,sec=krb5,iocharset=utf8,domain=WIN.REDOS ://dc.win.redos/share
```

- Первое поле (в примере - **share**) - имя автоматически создаваемой **autofs** папки, в которую монтируется общая папка **//dc2.wintest.redostest/share**.
- Второе поле (в примере - -**fstype**) - параметры подключения и указание на использования механизма *Kerberos.*
- Третье поле (в примере - **://dc.win.redos/share**) - адрес сетевого хранилища.
- Параметр **cruid** может принимать значение идентификатора пользователя или доменного имени пользователя.

ВАЖНО!

При подключении сетевой папки на *windows server 2003* в опции монтирования надо дописать параметр **vers=1.0**. Логин и пароль пользователя не должны содержать кириллических символов.

Для подключения скрытых сетевых каталогов необходимо экранировать символ **$**

```
share -fstype=cifs,multiuser,cruid=$UID,sec=krb5,iocharset=utf8,domain=WIN.REDOS ://dc.win.redos/share\$
```

Если в имени каталога имеются пробелы, то пробелы необходимо экранировать с помощью символа backslash(\):

```
share -fstype=cifs,multiuser,cruid=$UID,sec=krb5,iocharset=utf8,domain=WIN.REDOS ://dc.win.redos/Новая\ папка
```

5. Добавьте **autofs** в автозагрузку и запустите службу:

```
systemctl enable autofs --now
```

Теперь подключённые общие сетевые ресурсы будут автоматически монтироваться при обращении пользователя к каталогу-точке монтирования (по запросу пользователя, а не при загрузке ОС на ПК, что позволяет снизить нагрузку на сервер). В нашем примере точкой монтирования выступает каталог **/media/samba**.

Подключение сетевых директорий с помощью NFS

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для монтирования сетевой папки необходимо создать папку на локальном компьютере:

```
mkdir ~/test
```

Монтирование вручную

Для монтирования папки вручную необходимо выполнить в терминале команду:

```
sudo mount -t nfs -O uid=1000,iocharset=utf-8 *IP-сервера*:/data ~/test
```

ВАЖНО

Следует помнить, что, как в настройках сервера, так и в настройках клиента при монтировании, путь к общему каталогу указывается полный. Данный пример показывает, что каталог **/data** находится в корне файловой системы.

Монтирование с записью в fstab

Для большего удобства можно добавить запись с сетевой папкой в fstab.

Целесообразно создать точку монтирования сетевой папки в **/media**, потому что каталоги, созданные в **/media**, будут отображаться на рабочем столе и в файловых менеджерах Nemo/Caja (в левой колонке). В файловых менеджерах Nemo/Caja монтировать данные каталоги можно будет одним кликом.

```
sudo mkdir /media/test
```

В файл /etc/fstab добавляем подобную запись:

```
*IP-сервера*:/data /media/test nfs rsize=8192,wsize=8192,timeo=14,intr 0 0
```

Опция «noauto» запрещает автоматическое монтирование сетевого диска при старте системы.

Проблемы

Использование на ноутбуке
При монтировании удаленных папок NFS посредством fstab, в ситуации, когда сеть с сервером будет не доступна, ноутбук невозможно выключить или отправить в спящий режим. Для использования удаленных папок NFS на ноутбуке лучше воспользоваться монтированием при помощи autofs

Монтирование с помощью autofs

Данный способ монтирования позволяет автоматически монтировать папку после обращения к ней в Nemo, Caja (к примеру, через закладки) или в терминале и автоматически отмонтировать при отсутствии активности.
Для реализации данного способа необходимо установить пакет autofs (если он ещё не установлен):

```
dnf install autofs
```

Для настройки autofs в файле /etc/auto.master необходимо добавить строку

```
/nfs /etc/auto.nfs --timeout=60
```

Здесь --timeout=60
указывает системе отмонтировать раздел при отсутствии активности на нём более чем 60 секунд.
Создаем в корне файловой системы папку /nfs :

```
touch /etc/auto.nfs && mkdir /nfs
```

В файле */etc/auto.nfs* добавляем строку

```
server  -rw,soft,intr,rsize=8192,wsize=8192 *IP-адрес*:/path_to_share
```

где:
• **-rw,soft,intr,rsize=8192,wsize=8192** – параметры монтирования;
• **server** – папка, которая будет создаваться в каталоге /nfs при монтировании удаленных папок;
• ***IP-адрес*:/path_to_share** – IP-адрес и общая папка сервера.

Добавляем службу autofs в автозапуск и перезапускаем для применения настроек:

```
sudo systemctl enable autofs
```

```
sudo systemctl restart autofs
```

ВАЖНО

При подключении сетевой папки на windows server 2003 в опции монтирования надо дописать параметр vers=1.0. Логин и пароль не должны содержать кириллических символов.

Автоматическое монтирование ресурсов при входе пользователя с помощью pam_mount

Для автоматического монтирования разделяемых файловых ресурсов при входе пользователя используется PAM-модуль pam_mount, предоставляемый пакетом pam_mount, то есть для автоматического монтирования разделяемых файловых ресурсов на компьютере-клиенте должны быть установлены пакет **cifs-utils** и **pam_mount**:

```
dnf install cifs-utils pam_mount
```

Настройка модуля pam_mount осуществляется с помощью конфигурационного файла **/etc/security/pam_mount.conf.xml**.

Вы можете подробнее ознакомиться с возможностью автоматического монтирования ресурсов, просмотрев наши обучающие видео:

- на **RuTube** — Монтирование файловых систем в РЕД ОС;
- в **Яндекс.Дзен** — Монтирование файловых систем в РЕД ОС;
- в **VK Видео** — Монтирование файловых систем в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Описание возможностей модуля pam_mount и формат его конфигурационного файла приведены в руководстве man для pam_mount и pam_mount.conf.

Для монтирования с помощью pam_mount разделяемых файловых ресурсов в конфигурационном файле должны быть указаны параметра монтируемого тома, например:

```
<?xml version="1.0" encoding="utf-8" ?>
 <!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
 <!-- See pam_mount.conf(5) for a description.-->
 <pam_mount>
 <mntoptions allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow_other" />
 <mntoptions require="nosuid,nodev" />
 <mkmountpoint enable="1" remove="true" />
 <debug enable="0" />

 <logout wait="500000" hup="1" term="1" kill="1" />

 <cifsmount>
 mount.cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o %(OPTIONS)
 </cifsmount>

 <volume
 fstype="cifs"
 server="dc.example.ru"
 path="share-pam"
 mountpoint="~/share-pam"
 options="username=%(USER),uid=%(USERUID),pass=%(PASSWD),rw,setuids,sec=ntlmv2i"
 />

 <volume
 fstype="cifs"
 server="dc.example.ru"
 path="share-pam"
 mountpoint="~/share-pam"
 options="username=%(USER),cruid=%(USERUID),setuids,file_mode=0664,dir_mode=0775,sec=krb5i"
 />

 </pam_mount>
```

где:

- server — машина, откуда производится монтирование. Обычно, если сеть не является доменной структурой, допустимо использование IPv4-адреса;
- path — каталог, который необходимо смонтировать с сервера;

- mountpoint — точка монтирования, другими словами - куда монтировать ресурс;
- options — атрибуты монтирования.

После настройки **pam_mount.conf.xml** необходимо внести изменения в файл **postlogin** профиля **authselect** и применить новую конфигурацию.

Для этого выполните следующее:

1. Определите используемый профиль:

```
authselect current
```

1.1. В случае если компьютер введен в домен, но используется профиль **sssd**, создайте профиль **sssd_domain**:

```
authselect create-profile sssd_domain -b sssd
```

> **Примечание.**
>
> В опции -b указывается профиль, который будет основой для создаваемого.

1.2. В случае если компьютер введен в домен, но используется профиль **winbind**, создайте профиль **winbind_domain**:

```
authselect create-profile winbind_domain -b winbind
```

1.3. В случае если компьютер введен в домен и уже используется профиль **sssd_domain** или **winbind_domain**, создавать профиль не нужно.

2. Отредактируйте файл **/etc/authselect/<идентификатор_профиля>/postlogin**:

```
nano /etc/authselect/<идентификатор_профиля>/postlogin
```

где <идентификатор_профиля> может принимать следующие значения:

- для **sssd_domain** — custom/sssd_domain;
- для **winbind_domain** — custom/winbind_domain.

и добавьте в конец файла следующую строку:

```
session optional pam_mount.so
```

> **Примечание.**
>
> Модуль **pam_mount.so** с атрибутом disable_interactive допустим только при аутентификации через **krb5** и **krb5i**.

3. Примените отредактированный профиль:

```
authselect select <идентификатор_профиля>
```

Аутентификация через Kerberos при использовании модуля pam_mount

Для использования Kerberos-аутентификации на введенной в домен рабочей станции в конфигурационном файле **/etc/security/pam_mount.conf.xml** в строке с опциями монтирования укажите параметр аутентификации:

- **sec=krb5i** – предпочтительно с точки зрения безопасности, но требует больше ресурсов;
- **sec=krb5** – при монтировании будет использоваться текущий кеш Kerberos-пользователя.

Также можно добавить атрибут disable_interactive к модулю **pam_mount.so**, который позволяет авторизоваться на сетевом ресурсе без повторного ввода пароля (в файле **/etc/authselect/<идентификатор_профиля>/postlogin**). Для применения изменений, внесенных в профиль, выполните:

```
authselect select <идентификатор_профиля>
```

Примечание.

Обратите внимание, что настроенный автоматический вход в систему не производит автоматическую авторизацию сетевых ресурсов при использовании модуля **pam_mount.so** с атрибутом disable_interactive.

ВАЖНО!

При подключении сетевой папки на **windows server 2003** в опции монтирования необходимо дописать параметр vers=1.0. Логин и пароль **не должны** содержать кириллических символов. Обратите внимание, что начиная с версии ядра **5.15** в клиенте CIFS прекращена поддержка NTLM и менее надёжных алгоритмов аутентификации, основанных на алгоритме DES и используемых в протоколе SMB1.

При повторном вводе в домен внесенные изменения в профиль **authselect** будут удалены в связи с повторным конфигурированием профиля.

Подключение сетевых директорий через сервис systemd

Выполните в терминале команду:

```
systemctl enable NetworkManager-wait-online.service
```

ВАЖНО!

Пример настройки приведен для использования на ПК в домене. Если не используется домен, тогда опции надо использовать другие (описание опций можно посмотреть в мануале, для этого в терминале введите команду man mount).

Создайте сервис для монтирования:

```
nano /etc/systemd/system/mnt-pub.mount
```

где:

- **mnt-pub** - путь до точки монтирования (разделение указываются в этом случае через "дефис");
- **.mount** - расширение, указывающее на то, что данный модуль является опцией для монтирования.

ВАЖНО!

Имя файла должно соответствовать созданной точке монтирования, иначе сервис работать не будет.

Содержимое:

```
[Unit]
 Description=User's mount service
 Requires=network-online.target
 After=gdm.service

 [Mount]
 What=//dc1.winhost.ru/share
 Where=/mnt/pub
 Type=cifs
 Options=multiuser,cruid=$UID,sec=krb5,domain=WINHOST.RU

 [Install]
 WantedBy=multi-user.target
```

cruid - уникальный идентификатор пользователя, состоящий из последовательности цифр. Его можно увидеть в выводе команды:

```
id <имя_пользователя>
```

Параметр cruid = Arg устанавливает UID владельца кеша учетных данных. В первую очередь, эта опция полезна с sec = krb5. По умолчанию используется реальный идентификатор процесса, выполняющего монтирование. Установка этого параметра указывает upcall искать кеш учетных данных, принадлежащий этому пользователю.

Другой вариант создания сервиса с явным указанием *пользователя* и *пароля*:

```
[Unit]
 Description=User's mount service
 Requires=network-online.target
 After=gdm.service

 [Mount]
 What=//dc1.winhost.ru/share
 Where=/mnt/pub
 Type=cifs
 Options=rw,user=admin,password=password,domain=WINHOST.RU
```

```
[Install]
WantedBy=multi-user.target
```

где:

- `user=` - ваше имя пользователя;
- `password=` - ваш пароль для указанного пользователя.

ВАЖНО!

При подключении сетевой папки на **windows server 2003** в опции монтирования надо дописать параметр **vers=1.0**, а так же логин и пароль не должны содержать кириллических символов.

Добавьте сервис в автозагрузку:

```
systemctl enable mnt-pub.mount
```

Создайте папку, в которую будет происходить монтирование, и назначьте права:

```
mkdir -p /mnt/pub && chmod 777 /mnt/pub
```

Выполните команду:

```
chmod u+s /usr/sbin/mount.cifs
```

Вывод ярлыка папки на рабочий стол:

```
ln -s /mnt/pub/ $HOME/Рабочий\ стол/Share
```

РЕД ОС в рабочей группе

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия Kernel**: 5.15.10
- **Конфигурация**: Рабочая станция

Для включения РЕД ОС в рабочую группу, необходимо в конфигурационном файле samba, секцию **[global]** привести к виду:

```
# nano /etc/samba/smb.conf
```

```
[global]
workgroup = WORKGROUP
security = user
passdb backend = tdbsam
map to guest = bad user

netbios name = mycomputer
client min protocol = NT1
client max protocol = SMB3
wins support = yes

# UTF кодировка
unix charset = UTF-8
dos charset = cp1251
store dos attributes = yes
```

Включим сервис **smb** в автозагрузку и запустим его:

```
systemctl enable smb --now
```

Также поступим и с сервисом **nmb**:

```
systemctl enable nmb --now
```

nmb - сервер имен NetBIOS для предоставления клиентам услуг именования NetBIOS через IP.
Теперь машины с операционными системами Windows или Linux смогут найти ваш компьютер в сети.
Также и РЕД ОС в рабочей группе WORKGROUP сможет увидеть другие ПК.

Подключение сетевых директорий с помощью утилиты connectfolder

Окружение

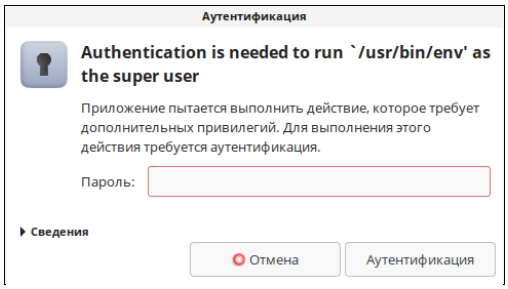
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** connectfolder 0.2.4

connectfolder - графическая утилита для подключения сетевых каталогов, открытых в общий доступ по протоколу *smb* в рабочей группе или домене *Windows/Samba*. Для монтирования сетевых директорий программа использует технологию **autofs**.

```
dnf install connectfolder
```

После установки программа доступна через «*Главное меню > Системные > Подключение сетевого каталога*».

Работа с *connectfolder* требует прав администратора, поэтому во время запуска программы необходимо ввести пароль пользователя **root**.

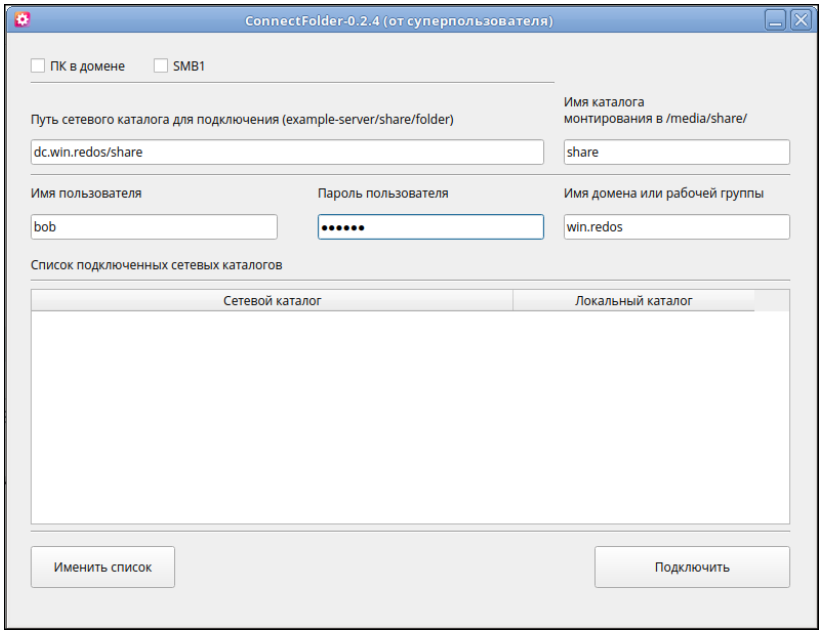


После успешной аутентификации откроется окно программы.

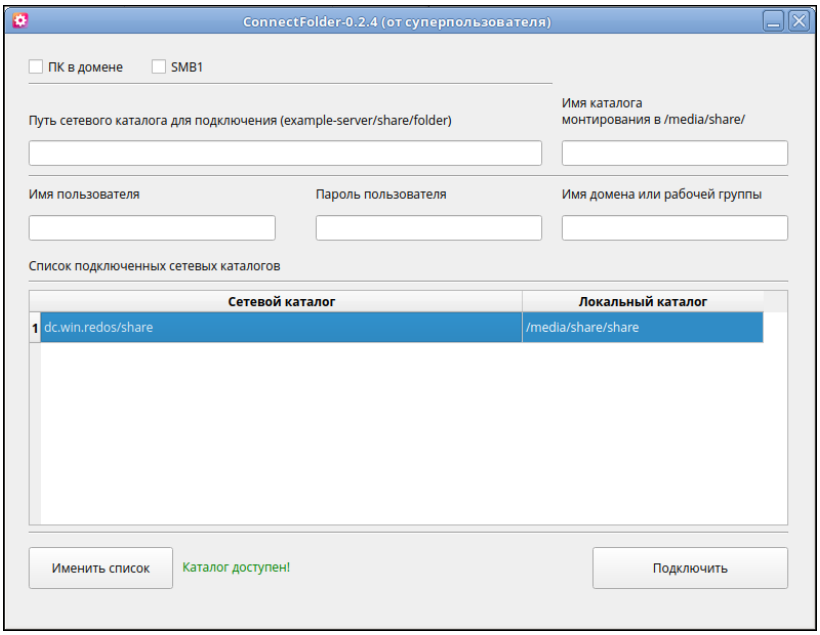
В первой строке указывается путь к сетевому каталогу, который необходимо подключить.

По умолчанию программа монтирует сетевые каталоги в локальную директорию **/media/share/** в предварительно указанный каталог. Этот каталог назначается в поле «*Имя каталога монтирования в /media/share/*».

При необходимости впишите *имя пользователя* для доступа к сетевому ресурсу, *пароль*, *имя рабочей группы или домена*.

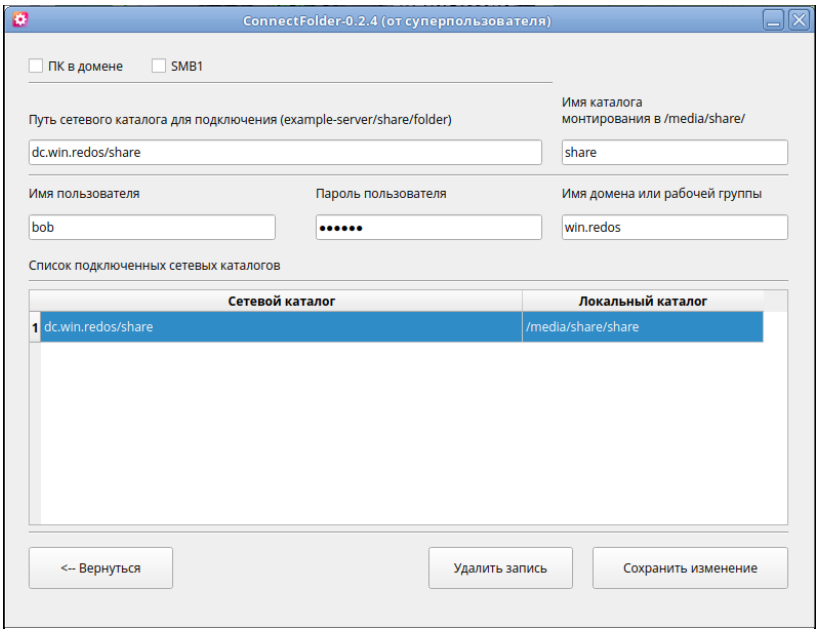


В данном примере после нажатия на кнопку «*Подключить*» инициализируется подключение (монтирование в linux) сетевого каталога «**dc.win.redos/share**» в локальную директорию **/media/share/share**. В случае успеха появится соответствующая запись в списке подключенных сетевых ресурсов.

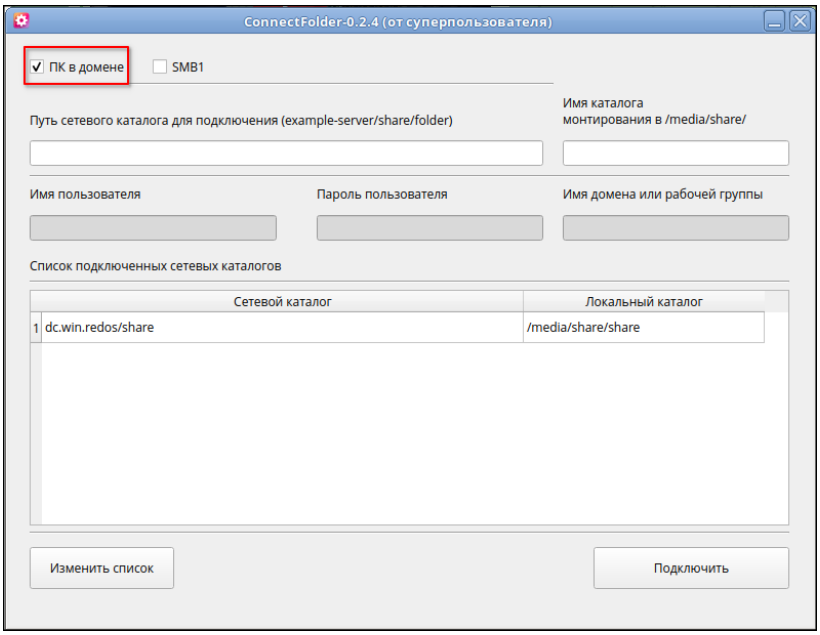


При выборе мышкой данной записи из списка будет произведен тест доступности каталога, и при успешном подключении появится надпись «*Каталог доступен*!».

При нажатии на кнопку «*Изменить список*» будет активирован режим редактирования, в котором можно изменять поля для подключения или совсем отключить подключенный сетевой ресурс, нажав на кнопку «*Удалить запись*», предварительно выбрав необходимую запись из списка.



Если ПК с РЕД ОС, на котором запускается *connectfolder*, введен в домен, то программа это автоматически обнаружит и установит флаг «*ПК в домене*». В таком случае поля «*Имя пользователя*», «*Пароль пользователя*» и «*Имя домена или рабочей группы*» будут автоматически не активны, т.к. для подключения к сетевому ресурсу будут использоваться права доступа доменного пользователя. При необходимости можно снять выбор «*ПК в домене*» и тогда ранее неактивные поля будут доступны для редактирования.



Переключатель «*SMB1*» активирует использование протокола версии **SMB1** при монтировании сетевого ресурса. Это может быть использовано при возникновении проблем с подключением к файловым серверам, которые продолжают работать на устаревшей версии протокола **SMB**.

Подключение сетевых директорий с помощью GIO

Установка и возможности GIO
Примеры использования
Автомонтирование сетевых ресурсов

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: gvfs-1.48.2-1

GIO (*GNOME Input/Output*) — это библиотека ввода-вывода, предоставляющая абстрактный интерфейс для работы с файлами, сетевыми соединениями, устройствами и другими ресурсами.

В РЕД ОС **gio** входит в состав пакета **gvfs**. **GVFS** предоставляет полную инфраструктуру виртуальной файловой системы и управления хранилищем.

Для идентификации **GIO** использует адреса на основе стандарта URI. Такие адреса имеют вид `<протокол>://user@server/path` и являются ключевой информацией, определяющей вид услуги и протокола, по которому воспроизводится передача данных. Для монтирования ресурсов используется **GVFS**.

GVFS монтирует съемные носители в каталог **/var/run/user/<uid_пользователя>/gvfs**.

Установка и возможности GIO

Пакет **gvfs** с **gio** по умолчанию предустановлен в РЕД ОС.

Если по каким-либо причинам пакет отсутствует в вашей системе, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду установки:

```
dnf install gvfs
```

GIO предоставляет несколько команд, которые могут быть полезны для написания скриптов и тестирования. Команды описаны в таблице ниже.

Команда	Описание
help	Напечатать справку
version	Вывести номер версии
cat	Объединить файлы и вывести содержимое на стандартный вывод
copy	Копировать один или несколько файлов
info	Показать информацию о расположениях
list	Показать содержимое расположений
mime	Получить или установить обработчик для типа MIME
mkdir	Создать каталог
monitor	Отслеживать изменение файлов и каталогов
mount	Монтирование или размонтирование расположений
move	Переместить один или несколько файлов
open	Открыть файлы приложением по умолчанию
rename	Переименовать файл
remove	Удалить один или несколько файлов
save	Прочитать содержимое стандартного входа и сохранить
set	Установить атрибут файла

trash	Переместить файлы или каталоги в корзину
tree	Показать содержимое расположений в виде дерева

В РЕД ОС **gio** используется для монтирования распределенной файловой системы **DFS** (*Distributed File System*).

Примеры использования

Монтирование сетевого ресурса к доменному пользователю

В данном примере рассмотрено монтирование сетевого ресурса к пользователю в домене *Microsoft AD*.

Перед монтированием необходимо авторизоваться под доменным пользователем.

> **Примечание.**
>
> Пользователю должен быть разрешён доступ к монтируемому ресурсу.

Монтирование производится командой:

```
gio mount smb://<сервер>/<общий_ресурс>
```

Например:

```
gio mount smb://dc.win.redos/test
```

Монтирование сетевого ресурса к локальному пользователю

Для анонимного доступа к ресурсу применяется ключ **-a**:

```
gio mount -a smb://<сервер>/<общий_ресурс>/
```

При выполнении команды без ключа анонимного доступа будет запрошена аутентификационная информация:

```
gio mount smb://10.81.81.1
Требуется аутентификация
Введите пользователя и пароль для «10.81.81.1»:
User [user]:
Domain [SAMBA]:
Password:
```

Просмотр и копирование файлов с использованием ssh

Для просмотра файла на удалённом ресурсе используется операнд `cat`:

```
gio cat ssh://user@<ip-адрес>/home/user/test.txt
```

Для копирования файла с удалённого ресурса используется операнд `copy`:

```
gio copy ssh://user@<ip-адрес>/home/user/test.txt /<место_сохранения>/
```

Монтирование сетевого ресурса с использованием ftp

Для монтирования FTP-ресурса выполните команду:

```
gio mount ftp://<сервер>/<общий_ресурс>/
```

Автомонтирование сетевых ресурсов

Файл автозагрузки

Для автоматизации монтирования необходимо в директории **/etc/xdg/autostart** создать файл автозапуска с расширением **.desktop**:

```
nano /etc/xdg/autostart/gio.desktop
```

со следующим содержимым:

```
[Desktop Entry]
Name=GIO mount
Type=Application
Exec=gio mount smb://<сервер>/<общий_ресурс>/
Terminal=false
```

здесь:

- `gio mount smb://<сервер>/<общий_ресурс>/` — команда монтирования. Таким же образом можно настроить автомонтирование для FTP-ресурса.

Добавление параметра в .bashrc

Для автоматизации монтирования под доменным пользователем необходимо добавить команду в файл **.bashrc** в домашнем каталоге пользователя. Сделать это можно командой:

```
echo "timeout 4 gio mount smb://10.81.81.1 &> /dev/null" >> ./.bashrc
```

Предварительная подготовка компьютера к вводу в домен

Описывается ввод в домены, организованные на версиях Windows Server 2008r2 и выше. Для ввода в домен на Windows server 2003 смотрите дополнительные примечания в тексте.

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.
Порты брандмауэра, необходимые для присоединения к домену AD
TCP 464 (Kerberos Password V5 – Used when user change their password from desktop)
TCP 636 (LDAP SSL)
TCP 53 (DNS)
TCP 88 (Kerberos Key Distribution Center)
TCP 135 (Remote Procedure Call)
TCP 139 (NetBIOS Session Service)
TCP 389 (LDAP)
TCP 445 (SMB,Net Logon)
UDP 389 (LDAP, DC Locator, Net Logon)
TCP 49152-65535 (Randomly allocated high TCP ports)

+ DNS-имена могут содержать только буквы (a–z), цифры (0–9), знак ''минус'' (-) и точку (.). Точки разрешено использовать только для разделения компонентов имен, заданных в формате доменных.

Имена узлов DNS не могут содержать следующие символы:

- Запятая (,)
- Тильда (~)
- Двоеточие (:)
- Восклицательный знак (!)
- Знак "@"
- Символ решетки (#)
- Знак доллара ($)
- Знак процента (%)
- Крышка (^)
- Амперсанд (&)
- Апостроф (')
- Точка (.)
- Круглые скобки (())
- Фигурные скобки ({})
- Символ подчеркивания (_)
- Пробел ( )

1. Измените имя компьютеру, **имя должно содержать домен**, то есть должно быть, например *client1.win.redos*

```
hostnamectl set-hostname <Имя компьютера>.<домен>
```

Например:

```
hostnamectl set-hostname client1.win.redos
```

2. Проверьте имя ПК

```
hostname
```

3. Для регистрации рабочей станции с РЕД ОС в домене **Active Directory** с автоматическим обновлением **DNS-записей** добавьте в файл **/etc/hosts** строку вида:

```
127.0.0.1 <Имя компьютера>.<домен> <Имя компьютера>
```

С помощью команды:

```
sudo sh -c "echo '127.0.0.1  `hostname -f` `hostname -s`' >> /etc/hosts"
```

Пример файла **/etc/hosts** (добавленная строка выделена жирным шрифтом):

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1  client1.win.redos client1
```

При выводе из домена эту строку нужно удалить

4. Проверьте настройку сети

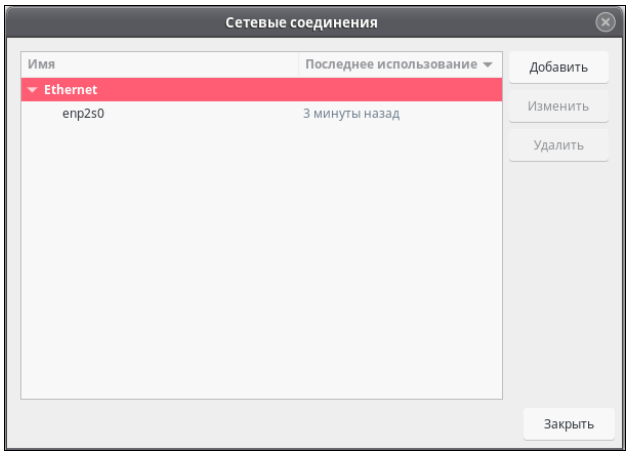
```
ifconfig
```

5. Проверьте работу сети

```
ping ya.ru -c 4
```

6. Настройте сетевой адаптер и проверьте, что первый DNS - это DNS контроллера домена, и укажите в качестве поискового домена домен MS AD.

Для настройки сетевого адаптера откройте утилиту **"Сетевые соединения"**, выберите доступное соединение и нажмите **"Изменить"**. Утилита находится по адресу:
"Меню" → "Параметры" → "Сетевые соединения"



Перейдите на вкладку **"Параметры IPv4"**. В поле **"Метод"** выберите **"Автоматический (DHCP, только адрес)"**, укажите нужные значения в полях **"Дополнительные серверы DNS"** и **"Дополнительные поисковые домены"**.

Нажмите кнопку "Сохранить" и перезапустите сервис **Network Manager**.

```
sudo systemctl restart NetworkManager
```

Проверьте, что введенные настройки сохранились.

```
cat /etc/resolv.conf
```

В выводе команды должна быть запись вида:

```
# Generated by NetworkManager
search <название домена>
nameserver <IP контроллера домена>
```

ВАЖНО

В работе используются только 3 первые DNS-сервера.

7. Проверьте разрешение имен

```
nslookup <IP контроллера домена>
nslookup <FQDN имя контроллера домена>
```

Ввод РЕД ОС в домен MSAD с помощью утилиты join-to-domain

Графический режим работы программы ввода/вывода РЕД ОС из домена
Консольный режим работы программы ввода РЕД ОС в домен
Консольный режим работы join-to-domain с входными параметрами

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: join-to-domain-0.6.5

Перед вводом РЕД ОС в домен проверьте настройки сети. Контроллер домена должен быть доступен по имени, например, это можно проверить запустив команду **ping**:

```
ping -c 3 dc.win.redosPING dc.win.redos (10.81.1.196) 56(84) bytes of data.
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=1 ttl=128 time=0.320 ms
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=2 ttl=128 time=0.601 ms
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=3 ttl=128 time=0.701 ms
```

Если ваш DHCP-сервер не раздает клиентам доменный суффикс, то укажите его в сетевых настройках, в поле «**Поисковый домен**».

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

В РЕД ОС имеется утилита **join-to-domain**, которая предназначена для ввода компьютера в домен *Windows* или домен на базе *SAMBA*. В РЕД ОС 7.3 программа **join-to-domain** предустановлена в системе по умолчанию, но перед использованием необходимо обновить утилиту до последней версии:

```
dnf update join-to-domain
```

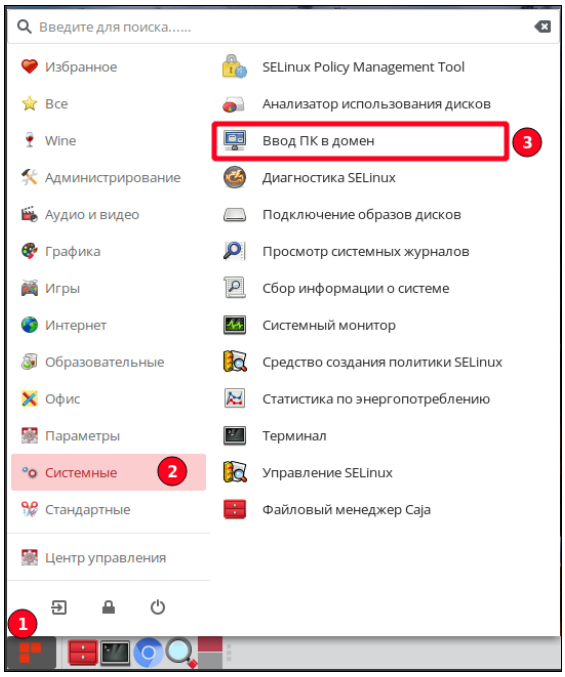
join-to-domain может выполняться в трех режимах:

- с графическим интерфейсом;
- в консоли (интерактивный режим);
- в консоли с входными параметрами.

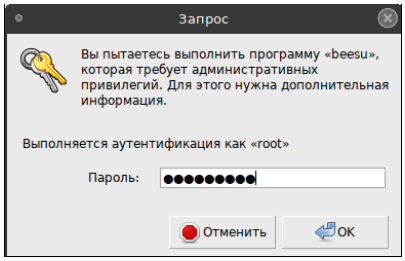
Графический режим работы программы ввода/вывода РЕД ОС из домена

В РЕД ОС для быстрого ввода компьютера в домен *Windows/SAMBA* используется утилита **join-to-domain**. Утилита может быть запущена в консольном (текстовом) и в графическом режиме. Описание работы **join-to-domain** в консоли будет рассмотрено ниже.

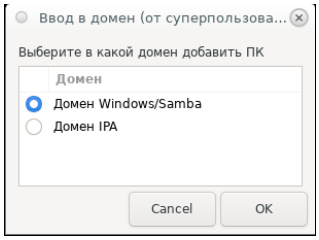
Для запуска **join-to-domain** в графическом режиме откройте «**Главное меню**» - «**Системные**» - «**Ввод ПК в домен**».



Запуск программы требует ввода пароля от пользователя **root**.



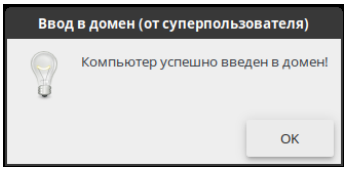
После успешной аутентификации откроется окно выбора типа домена на базе **SAMBA** или **FreeIPA**. Для ввода в домен **SAMBA** выберите пункт «**Домен Windows/SAMBA**».



После успешной аутентификации откроется основное окно, в котором необходимо заполнить все поля:

После нажатия на кнопку «**Да**» начнется процесс присоединения ПК к домену.

В случае успешного ввода в домен появится уведомление:

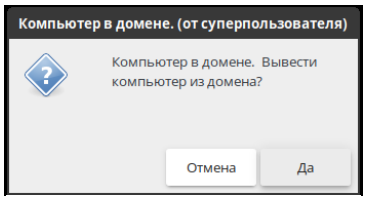


Перезагрузите компьютер и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

Процесс ввода в домен, а также возможные ошибки при работе протоколируются в файл **/var/log/join-to-domain.log**.

Для вывода ПК из домена *Windows*, следует снова запустить **join-to-domain** «**Главное меню**» - «**Системные**» - «**Ввод ПК в домен**».

В этот раз программа определит, что РЕД ОС введен в домен и предложит выйти из него.



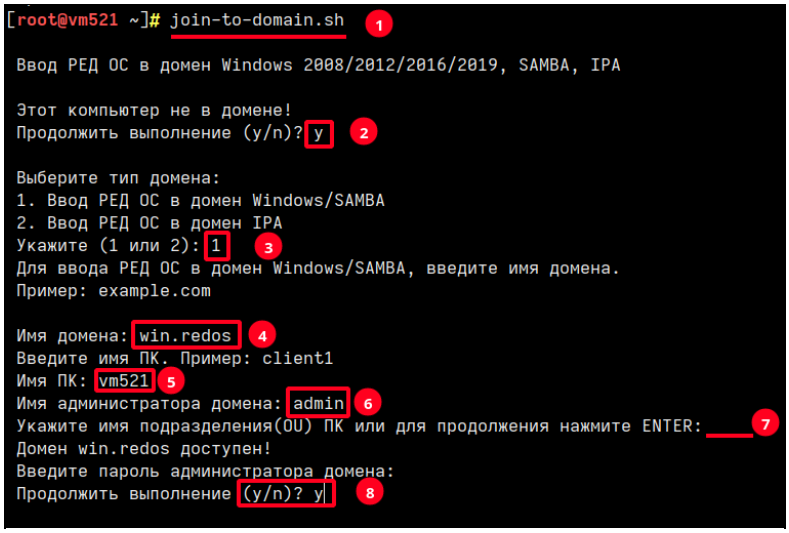
Консольный режим работы программы ввода РЕД ОС в домен

Откройте консоль и выполните запуск **join-to-domain.sh** с привилегиями суперпользователя **root**.

```
join-to-domain.sh
```

Программа запросит пользователя выбрать тип домена, к которому необходимо присоединить РЕД ОС, в данном случае необходимо выбрать первый пункт «**Ввод РЕД ОС в домен Windows/Samba**».

Введите имя домена, имя компьютера, имя администратора домена и подтвердите ваши действия для начала процесса ввода ПК в домен.

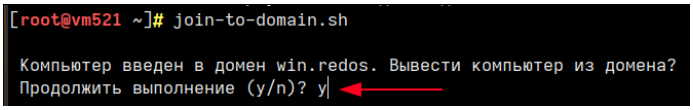


Протокол ввода в домен записывается в файл **/var/log/join-to-domain.log**.

Перезагрузите компьютер и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

Для вывода РЕД ОС из домена выполните в консоли команду с привилегиями суперпользователя **root**:

```
join-to-domain.sh
```



Подтвердите действие, после чего начнется процесс вывода из домена, по окончании всех действий перезагрузите ПК.

Консольный режим работы join-to-domain с входными параметрами

Пример №1 - ввод в домен Windows или SAMBA:

```
join-to-domain.sh -d win.redos -n client07 -u admin -p password
```

Пример №2 - ввод в домен с добавлением ПК в OU:

```
join-to-domain.sh -d example.com -n client1 -u admin -p password --ou "OU=МоиПК,OU=ОтделIT" -y
```

Пример №3 - удаление учетной записи ПК с подключением к определенному DC:

```
join-to-domain.sh --delete-computer -u <admin_login> -d <domain_name> --dc <domain_controller> -n <pc_name>
```

Пример №4 - вывод из домена. Выполните команду join-to-domain.sh, в результате программа определит, что данный ПК в домене и предложит выйти из него.

```
join-to-domain.sh

Компьютер введен в домен win.redos. Вывести компьютер из домена?
Продолжить выполнение (y/n)? y
Удаление учетной записи ПК из домена.
Введите имя контроллера домена или для продолжения нажмите ENTER:
Введите имя администратора домена: admin
Password for admin@WIN.REDOS:
```

Пример №5 - ввод в домен с поддержкой kerberos-аутентификации на SSH-сервере и предоставление прав доменной группе пользователей на использование sudo:

```
join-to-domain.sh -d <domain_name> -n <pc_name> -u <admin_login> -p <password> --sg "Администраторы домена" --sk -y
```

Описание параметров запуска:

Параметр	Описание параметра
-d	Имя домена
-n	Имя компьютера
-u	Имя администратора домена
-p	Пароль администратора домена
--ou	Имя подразделения компьютера (OU), формат ввода "**OU=МоиПК,OU=ОтделIT**". Порядок указания OU снизу вверх
--dc	Имя контроллера домена
-w	Позволяет ввести в домен, используя **Winbind** (по умолчанию применяется SSSD)
--sk	Включение поддержки kerberos-аутентификации на SSH-сервере при вводе в домен
--sg	Предоставление прав доменной группе пользователей использовать sudo, см. пример №5
-y	Автоматическое подтверждение запросов на выполнение действий при работе скрипта с параметрами
-f	Принудительный ввод в домен (вывод из домена) под своим прежним именем ПК (игнорируется существующая учетная запись ПК в домене)
--wg	Указать "**Имя домена (пред-Windows 2000)**" (необязательный ключ)
--delete-computer	Удаляет учётную запись ПК из домена (не выводит сам ПК из домена), см. пример №3
--sssd-lower-case	Принудительно устанавливает имя пользователя в нижнем регистре
-g	Запуск скрипта с графическим интерфейсом
-h, --help	Показать справку
-v	Вывод версии

Ввод РЕД ОС в домен MSAD с помощью консольных команд

Ввод в домен консольными командами
Список команд для быстрого ввода в домен через консоль
Ограничение доступа входа на ПК для доменных пользователей

ВАЖНО!

Имя ПК должно содержать только буквы (a–z), цифры (0–9), знак ''минус'' (-) и точку (.).

Данная инструкция не подходит для ПК, на которых установлено ПО SecretNet версии 1.9.

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Ввод в домен консольными командами

Подключаемся к домену Active Directory с помощью realmd.

Realmd (Realm Discovery) – это сервис, позволяющий производить настройку сетевой аутентификации и членства в домене MS AD без сложных настроек. Информация о домене обнаруживается автоматически. Для аутентификации и проверки учетных записей realmd использует SSSD (через Kerberos и LDAP) (также может использоваться и Winbind).

1. **Настройка NTP клиента**

Время на контроллере домена и на клиенте должно быть одинаково. Для синхронизации времени клиентского ПК с контроллером домена используйте клиент chrony. Откройте файл конфигурации NTP клиента CHRONY с помощью команды:

```
sudo nano /etc/chrony.conf
```

Удалите или закомментируйте в нем строки с серверами по умолчанию, а в качестве сервера времени укажите сервер контроллера домена:

```
server <FQDN_имя_контроллера_домена> iburst
```

После изменений конфигурационного файла вам надо перезапустить chronyd:

```
sudo systemctl restart chronyd
```

Проверьте работу chrony с помощью двух команд::

```
systemctl status chronyd
```

```
chronyc tracking
```

Пример вывода команды:

```
$ systemctl status chronyd
  chronyd.service - NTP client/server
    Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
    Active: active (running) since Вт 2019-07-09 11:13:49 MSK; 5min ago
  Process: 683 ExecStartPost=/usr/libexec/chrony-helper update-daemon (code=exited, status=0/SUCCESS)
  Process: 639 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 650 (chronyd)
    CGroup: /system.slice/chronyd.service
            └─650 /usr/sbin/chronyd
```

Пример вывода команды:

```
$ chronyc tracking
Reference ID    : 10.81.1.196 (dc.win.redos)
```

```
Stratum         : 4
Ref time (UTC)  : Wed Mar  4 09:44:17 2020
System time     : 0.000169261 seconds slow of NTP time
Last offset     : -0.000182217 seconds
RMS offset      : 0.000182217 seconds
Frequency       : 1.939 ppm slow
Residual freq   : -0.602 ppm
Skew            : 1.234 ppm
Root delay      : 0.047364 seconds
Root dispersion : 0.087531 seconds
Update interval : 64.7 seconds
Leap status     : Normal
```

2. **Установите необходимые пакеты, если они ещё не установлены**

```
sudo dnf install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation
```

3. **Выполните команду поиска домена**

```
realm discover < realm name >
```

ВАЖНО!

!!! Не рекомендовано использовать домен .local !!! Он зарезервирован для автоматически конфигурируемых сетей.

При использовании домена local

Если нужно получить доступ к ресурсам в уже существующей среде (Windows AD). То необходимо внести изменения в процесс разрешения хостов на linux машине. Отредактируйте /etc/nsswitch.conf. Изначально интересующий нас раздел содержит следующие записи:

```
hosts:          files mdns4_minimal [NOTFOUND=return] dns
```

Соответственно, в этом режиме сначала производится поиск в файле /etc/hosts, затем запрос идет к mdns, после чего возвращается ответ "не найдено". Mdns кэширует данные и работает с демоном Avahi. Модифицируйте эту "схему" к классическому виду:

```
hosts:          files dns
```

В РЕД ОС 7.3 изменять конфигурацию /etc/nsswitch.conf следует через файл

```
nano /etc/authselect/user-nsswitch.conf
```

после чего выполнить применение настроек:

```
authselect apply-changes
```

4. **Введите компьютер в домен, указав логин и пароль администратора домена**

```
sudo realm join -U -v <имя_администратора_домена> <realm_name>
```

Пример:

```
sudo realm join -U -v администратор win.redos
```

При успешном вводе ПК в домен, в конце вы увидите сообщение *"* Successfully enrolled machine in realm"*

5. **Теперь, если ввести команду realm list, то получим информацию о домене, а в консоли "Users and Computers" домена Active Directory появится новый компьютер.**

```
$ realm list
win.redos
```

```
type: kerberos
realm-name: WIN.REDOS
domain-name: win.redos
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
login-formats: %U@win.redos
login-policy: allow-realm-logins
```

6. **Некоторые действия и информацию можно получить с помощью утилиты** `adcli`**.**

```
$ adcli info win.redos
[domain]
domain-name = win.redos
domain-short = WIN
domain-forest = win.redos
domain-controller = dc.win.redos
domain-controller-site = Default-First-Site-Name
domain-controller-flags = pdc gc ldap ds kdc timeserv closest writable full-secret ads-web
domain-controller-usable = yes
domain-controllers = dc.win.redos
[computer]
computer-site = Default-First-Site-Name
```

7. **Откройте для редактирования файл** `/etc/sssd/sssd.conf`

```
sudo nano /etc/sssd/sssd.conf
```

Приведите строки к указанному ниже виду:

```
use_fully_qualified_names = False
ad_gpo_access_control = permissive
```

- use_fully_qualified_names = False - отключение режима полных имён для пользователей;
- ad_gpo_access_control = permissive - режим политики GPO входа пользователя в систему. В данном примере GPO оценивается, но не применяется.

8. **Разрешите доменным пользователям создавать домашние директории, для чего выполните команду:**

```
sudo authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

9. **Далее нужно отредактировать конфигурационный файл** ***/etc/krb5.conf***

Для доступа к сетевым ресурсам без запроса пароля (с помощью Kerberos) в файле /etc/krb5.conf нужно закомментировать строку

```
default_ccache_name = KEYRING:persistent:%{uid}
```

После нее вставить строку:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

Изменить значение параметра можно следующей командой:

```
sudo sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

В секцию `[libdefaults]` нужно добавить параметр `default_realm = REALM NAME`

Пример записи для домена **win.redos**:

```
default_realm = WIN.REDOS
```

Добавить параметр можно следующей командой (вместо `REALM NAME` укажите название своего домена ПРОПИСНЫМИ буквами):

```
sudo sed -i '/krb5cc_%{uid}/a default_realm = REALM NAME' /etc/krb5.conf
```

Этот параметр позволит пользователям при выполнении команды `kinit` не указывать полное имя пользователя (то есть можно использовать короткое имя пользователя *user* вместо *user@WIN.REDOS*).

Пример:

```
$ kinit user
Password for user@WIN.REDOS:
```

+ Для контроллера домена на базе Windows Server 2008 выполните дополнительные действия

  В связи с тем, что клиент Kerberos в Linux использует самый безопасный алгоритм шифрования при подключении к серверу Kerberos на MS AD, а 2008 версия windows не поддерживает его, вам придется явно указать, какими алгоритмами пользоваться клиенту. Отредактируйте файл /etc/krb5.conf. В секцию [libdefaults] впишите

  ```
  [libdefaults]
  ...
  default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
  default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
  preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
  ```

  Перезагрузите компьютер и попробуйте зайти под учетной записью доменного пользователя.

10. **Проверьте состояние службы sssd, в выводе статуса должно быть написано active (running)**

```
$ systemctl status sssd
 sssd.service - System Security Services Daemon
  Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset: disabled)
  Active: active (running) since Вт 2019-08-27 11:26:16 MSK; 2h 5min ago
Main PID: 31918 (sssd)
  CGroup: /system.slice/sssd.service
          ├─31918 /usr/sbin/sssd -i --logger=files
          ├─31919 /usr/libexec/sssd/sssd_be --domain implicit_files --uid 0 --gid 0 --logger=files
          ├─31920 /usr/libexec/sssd/sssd_be --domain win.redos --uid 0 --gid 0 --logger=files
          ├─31921 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --logger=files
          └─31922 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. **Пример настройки файла конфигурации /etc/samba/smb.conf**

Далее будут приведены примерные настройки конфигурационного файла **smb.conf**:

В блоке **[global]** указываются общие настройки.

Укажите свои данные домена для параметров **workgroup** и **realm**:

```
# Короткое имя домена в верхнем регистре
workgroup = WIN

# Домен в верхнем регистре
realm = WIN.REDOS
```

+ Остальные настройки можно оставить без изменений.

  ```
  # тип аутентификации, используемый для подключения к домену.
  security = ADS
  # определяет базу данных, которая будет использоваться для хранения учетных записей.
  passdb backend = tdbsam

  # определяет, будет ли winbind перечислять группы из домена.
  winbind enum groups = Yes
  # определяет, будет ли winbind перечислять пользователей из домена.
  winbind enum users = Yes
  ```

```
# определяет, будет ли winbind перечислять пользователей из домена.
winbind offline logon = Yes
# определяет, будет ли использоваться домен по умолчанию при входе в систему пользователей без указания имени домена.
winbind use default domain = No
# определяет, будет ли winbind обновлять билеты Kerberos.
winbind refresh tickets = Yes



# определяет время кэширования ID-отображений.
idmap cache time = 900
# настройки отображения ID между Windows и Unix.
idmap config * : backend = tdb
idmap config * : range = 10000-99999
idmap config SMBIND : backend = rid
idmap config SMBIND : range = 100000-999999

# минимальная версия SMB протокола клиента.
client min protocol = NT1
# максимально возможная версия SMB протокола клиента.
client max protocol = SMB3

# путь к файлу ключей Kerberos.
dedicated keytab file = /etc/krb5.keytab
# метод аутентификации Kerberos.
kerberos method = secrets and keytab

# время обновления пароля машины.
machine password timeout = 60
# определяет объекты VFS, используемые при монтировании файловой системы.
vfs objects = acl_xattr
# определяет, будет ли ACL-наследование применяться при создании файлов и каталогов.
map acl inherit = yes
# определяет, будут ли атрибуты DOS храниться в расширенных атрибутах файла.
store dos attributes = yes

printing = cups
printcap name = cups
load printers = yes
cups options = raw
```

Настройки блока **[global]** завершены.

Далее следует изменить блок **[homes]**, в котором необходимо указать настройки для доступа к папкам пользователей:

```
[homes]
comment = Home Directories
# "valid users" определеяет список пользователей или групп пользователей, которые имеют доступ к ресурсу.
# %S - подстановочный символ, который заменяется на имя текущей службы,
# %D - подстановочный символ, который заменяется на имя домена,
# %w - подстановочный символ, который заменяется на имя текущей машины.
valid users = %S, %D%w%S
# отключает/включает отображение данного ресурса в списке доступных ресурсов в проводнике или браузере файлов.
browseable = No
# разрешает запись на ресурс
read only = No
# позволяет унаследовать доступы на файлы и папки, если они не были явно настроены для данного ресурса.
inherit acls = Yes
```

В блоке **[printers]** укажите настройки для доступа к принтерам:

```
[printers]
comment = All Printers
path = /var/tmp
# устанавливает, что данная секция является принтером
printable = Yes
# права доступа для создания файлов
create mask = 0600
browseable = No
```

В блоке **[print$]** укажите параметры печати:

```
[print$]
comment = Printer Drivers
# путь к директории, которая будет использоваться для хранения драйверов принтеров
path = /var/lib/samba/drivers
# список пользователей/групп, имеющих права на запись
write list = @printadmin root
# устанавливает группу, которая будет установлена при создании файла/директории
force group = @printadmin
# устанавливает права доступа для создания файлов
create mask = 0664
# устанавливает права доступа для создания директорий
directory mask = 0775
```

Настройка файла **smb.conf** завершена. Обратите внимание, что приведены **примерные** настройки, которые могут быть изменены при необходимости.

12. **Также можно добавить новое правило в /etc/sudoers, чтобы доменный пользователь из группы администраторов домена мог получать права администратора локального компьютера:**Откройте файл /etc/sudoers для редактирования от пользователя root:

```
$ sudo nano /etc/sudoers
```

Добавьте в файл следующую строку, сохраните изменения и закройте редактор.

```
%администраторы\ домена ALL=(ALL) ALL
```

Данный параметр можно добавить командой:

```
sudo sh -c "echo '%администраторы\ домена ALL=(ALL) ALL' >> /etc/sudoers"
```

13. **Перезагрузите компьютер и войдите в ОС под учетной записью доменного пользователя.**

ВАЖНО!

Имя доменного пользователя должно состоять **из латинских символов** (кириллицу в имени пользователя использовать не рекомендуется).

Список команд для быстрого ввода в домен через консоль

В данном разделе собраны команды из раздела Ввод в домен консольными командами. Описание всех команд можно посмотреть в вышеуказанном подразделе. Не забудьте выполнить предварительную настройку ПК (задать имя и настроить сетевое соединение).

1. Настройте NTP-клиент

Здесь введите **своё FQDN имя контроллера домена**.

```
sudo sed -i 's/server/#server/g' /etc/chrony.conf
sudo sh -c "echo 'server <FQDN_имя_контроллера_домена> iburst' >> /etc/chrony.conf"
```

```
sudo systemctl restart chronyd
chronyc tracking
```

2. Установите необходимые пакеты, выполните поиск и настройку домена и введите компьютер в домен.

```
sudo dnf install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation
realm discover <имя_домена>
sudo realm join -U -v <имя_администратора_домена> <имя_домена>
```

При успешном вводе машины в домен вы увидите сообщение ***«* Successfully enrolled machine in realm»***

3. Отредактируйте файл sssd.conf и разрешите доменным пользователям создавать домашние директории.

```
sudo sed -i 's/use_fully_qualified_names = True/use_fully_qualified_names = False/g' /etc/sssd/sssd.conf
sudo sh -c "echo 'ad_gpo_access_control = permissive' >> /etc/sssd/sssd.conf"
sudo authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

4. Чтобы убрать предупреждение `"rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)"` **при выводе команды** `testparm -s`**:**

```
sudo sh -c "echo '*               -       nofile          16384' >> /etc/security/limits.conf"
sudo sh -c "echo 'root            -       nofile          16384' >> /etc/security/limits.conf"
```

+ Если контроллер домена основан на базе Windows Server 2008, то выполните следующую команду:

```
sudo sed -i '/\[libdefaults\]/a \    default_tkt_enctypes = RC4-HMAC, DES-CBC-CRC, DES3-CBC-SHA1,DES-CBC-MD5\n
default_tgs_enctypes = RC4-HMAC, DES-CBC-CRC, DES3-CBC-SHA1, DES-CBC-MD5' /etc/krb5.conf
```

5. **Для доступа доменных пользователей к сетевым ресурсам без запроса пароля (с помощью Kerberos) в файле /etc/krb5.conf нужно изменить параметр** `default_ccache_name`**:**

```
sudo sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

Добавление параметра `default_realm = REALM NAME` в секцию `[libdefaults]` позволит пользователям при выполнении команды `kinit` не указывать полное имя пользователя (то есть можно использовать короткое имя пользователя user вместо *user@WIN.REDOS*). Добавить параметр можно следующей командой (вместо `REALM NAME` укажите название своего домена ПРОПИСНЫМИ буквами):

```
sudo sed -i '/krb5cc_%{uid}/a default_realm = REALM NAME' /etc/krb5.conf
```

6. **Также можно добавить новое правило в /etc/sudoers, чтобы доменный пользователь из группы администраторов домена мог получать права администратора локального компьютера:**Данный параметр можно добавить командой:

```
sudo sh -c "echo '%администраторы\ домена ALL=(ALL) ALL' >> /etc/sudoers"
```

Ограничение доступа входа на ПК для доменных пользователей

Для данной настройки необходимо внести изменения в конфигурационный файл sssd.conf

```
access_provider = simple
simple_allow_users = user1@example.com, user2@example.com
simple_allow_groups = group@example.com
```

Параметр **access_provider = simple** определяет список доступа на основе имен пользователей или групп.

Настройка отображения общих ресурсов

> Данная инструкция применима для файловых ресурсов, находящихся в домене и развернутых на базе **Windows Server 2008r2** или **Windows Server 2012**.

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Для отображения в файловом менеджере общих ресурсов, которые расположены в доменах **Microsoft Active Directory**, нужно отредактировать на клиентском ПК конфигурационный файл samba - **/etc/samba/smb.conf**, а также включить на сервере службу «*Браузер компьютеров*».

В качестве примера рассматривается: домен **win.redos**, имя контроллера домена - **dc.win.redos**

1) На сервере Windows нужно включить службу *«Браузер компьютеров»*. Укажите «Тип запуска» службы - «Автоматически», после чего произведите запуск службы.

2) В файле **/etc/samba/smb.conf** в секции [**global**] на клиенте нужно изменить некоторые параметры. По умолчанию в файле указываются параметры **workgroup = SAMBA** и **security = user**. Измените значения параметров или закомментируйте данные строки, добавив нужные параметры после них (если в конфигурационном файле один и тот же параметр указан несколько раз, то используется последний указанный параметр).

Пример настройки **/etc/samba/smb.conf** изменённые и добавленные параметры выделены жирным шрифтом):

```
[global]

security = ADS
workgroup = WIN
realm = win.redos
idmap config * : range = 10000-99999
client max protocol = NT1
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните команду проверки:

```
# testparm -s

Load smb config files fr om /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows lim it (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
```

Предупреждение **«rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)»** отображается в связи с тем, что в Linux по умолчанию установлен лимит на **1024** одновременно открытых файлов, а в Windows лимит равен **16384**. Чтобы убрать это предупреждение, добавьте в конец файла **/etc/security/limits.conf** строки:

```
*           -       nofile          16384
root        -       nofile          16384
```

3) В файле **/etc/krb5.conf** нужно закомментировать строку:

```
default_ccache_name = KEYRING:persistent:%{uid}
```

Вместо нее вставить параметр:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

4) Далее следует перезагрузить ПК.

После выполнения данных действий общие ресурсы будут отображаться в файловом менеджере.

В файловом менеджере **Caja (Mate)** в боковой панели слева нужно выбрать пункт *«Просмотреть сеть»*.

В файловом менеджере **Nemo (Cinnamon)** в боковой панели слева нужно выбрать пункт *«Сеть».*

В целях безопасности на сервере Windows может быть отключен протокол **smb1**, в результате при подключении с РЕД ОС к серверу не будут видны общие сетевые ресурсы. Чтобы это исправить, в файле **/etc/samba/smb.conf** необходимо повысить версию протокола, указав **client max protocol = SMB2** или **client max protocol = SMB3**.

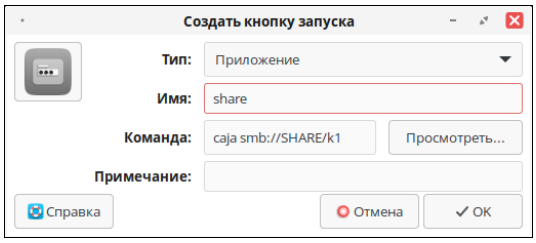
Создание кнопки запуска доступа к сетевому ресурсу

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для создания кнопки запуска сетевого ресурса на рабочем столе нужно нажать правой кнопкой мыши по свободному месту рабочего стола и выбрать пункт «*Создать кнопку запуска...*».

В открывшемся окне в поле «**Имя**» впишите отображаемое имя под кнопкой (название ярлыка). В поле «**Команда**» впишите `caja` и через пробел `путь к сетевому каталогу`. Его можно скопировать в адресной строке в файловом менеджере, находясь в нужном сетевом каталоге. Общий вид команды может быть, например, таким: `caja smb://SHARE/k1`. После всех действий нажмите кнопку «**OK**».



Отключение отображения определенного пользователя на экране входа в систему

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Для того, чтобы отключить отображение определенного пользователя на экране входа в систему, нужно:

1. Перейти в каталог **/var/lib/AccountsService/users**:

```
sudo cd /var/lib/AccountsService/users
```

2. Отредактировать файл настроек определенного пользователя, например, `user:`

```
sudo nano user
```

```
[User]
 Language=
 XSession=
 SystemAccount=false
```

3. Изменить значение параметра `SystemAccount` на `true`:

```
SystemAccount=true
```

Для применения изменений перезагрузите ПК.

Предоставление права пользователям домена выполнять команды от пользователя root

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция

Выполните вход в РЕД ОС под доменным пользователем Active Directory.

Выведите список групп, в которых пользователь состоит, выполнив команду:

```
groups
```

Пример:

```
[admin@win.red-soft.ru]$ groups
"пользователи домена администраторы домена dnsadmins"
```

Запомните группу в выводе, к примеру **dnsadmins**.

Откройте файл /etc/sudoers для редактирования от пользователя **root**:

```
su
nano /etc/sudoers
```

Найдите строку:

```
%wheel  ALL=(ALL)    ALL
```

После этой строки вставьте название группы из AD по аналогии с предыдущей:

```
%dnsadmins ALL=(ALL)    ALL
```

Сохраните файл.

ВАЖНО!

Если в названии группы имеется **пробел**, то его необходимо экранировать с помощью обратного слеша — '\'.

Пример:

```
%администраторы\ домена ALL=(ALL) ALL
```

Данный параметр можно добавить командой:

```
sudo sh -c "echo '%администраторы\ домена ALL=(ALL) ALL' >> /etc/sudoers"
```

Примечание.

Если вы используете **winbind** при вводе ПК в домен, то в файл **/etc/sudoers** нужно добавлять пользователей и группы в следующем виде:

```
%DOMAIN\\group   ALL=(ALL) ALL
%DOMAIN\\user   ALL=(ALL) ALL
```

Теперь проверьте, что пользователю или группе пользователей можно выполнять команды от имени суперпользователя **root**. Выполните команду:

```
cat /etc/sudoers
cat: /etc/sudoers: Отказано в доступе
```

Но, если выполнить эту команду, добавив `sudo` и введя пароль пользователя, то `cat` выведет содержимое файла:

```
sudo cat /etc/sudoers
```

Вывод РЕД ОС из домена MSAD

Вывод из домена с помощью графической программы
Вывод из домена консольными командами

Вы можете подробнее ознакомиться с информацией по выводу компьютера из домена, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Вывод из домена с помощью графической программы

Вывести компьютер из домена можно с помощью графической программы **join-to-domain**, установка данной программы:

```
sudo dnf install join-to-domain
```

После установки зайдите в меню, в разделе "*Администрирование*" выберите новый пункт *"Ввод ПК в домен"*.

Если ПК находится в домене, то при запуске утилиты она предложит вывести компьютер из домена. Для вывода из домена нужно подтвердить выполнение, дождаться окончания процесса и перезагрузить ПК.

Вывод из домена консольными командами

Для получения списка сконфигурированных доменов выполните:

```
realm list
```

Если в выводе присутствует одна запись:

```
sudo realm leave -v -U <username>@<domain>
```

Если в выводе присутствует две записи (две записи присутствуют при использовании двух client-software - winbind и sssd), тогда нужно выполнить две команды:

```
sudo realm leave -v --client-software=sssd -U <username>@<domain>
sudo realm leave -v --client-software=winbind -U <username>@<domain>
```

Нужно ввести пароль пользователя *<username>@<domain>*, который является Администратором домена. Для вывода из домена требуются права администратора. Поэтому при запросе пароля привилегированного пользователя нужно ввести пароль локального пользователя с правами администратора.

В конце вывода команды должно выдаваться сообщение об успешном выводе из домена:
`Successfully unenrolled machine from realm`

Проверить, успешно ли ПК был выведен из домена, можно командой `realm list` - в выводе не должно быть никаких записей

Если в окне входа в пользовательскую учетную запись после вывода из домена отображаются пользователи домена, выполните с привилегиями суперпользователя команду очистки кэша sssd

```
sudo sss_cache -E
```

Каталог общего сетевого доступа на РЕД ОС в домене MSAD

Графический вариант
Работа из файлового менеджера
Консольный вариант

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: share_directory 6.0-1

Рассмотрен механизм создания в РЕД ОС каталога с общим сетевым доступом по протоколу smb. РЕД ОС предварительно необходимо включить в домен *MS AD* согласно инструкциям текущего раздела «Работа с доменом MS AD».

Графический вариант

Утилита публикации сетевого ресурса в домене *Samba / MS AD* доступна в РЕД ОС 7.3.

Установите утилиту командой:

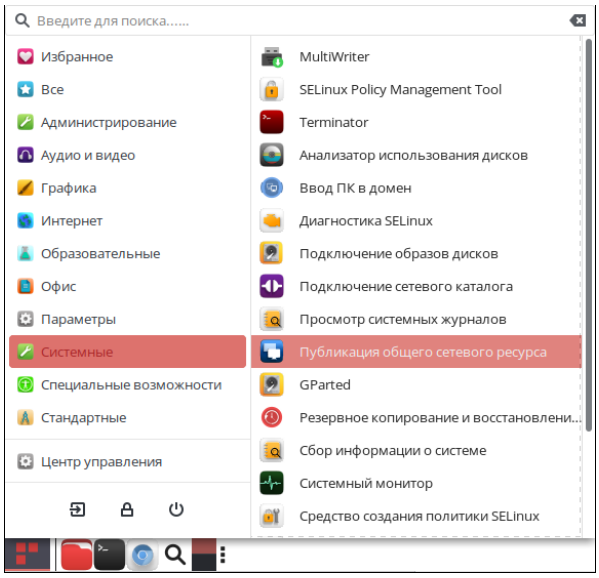
```
dnf install share_directory
```

От имени **root**-пользователя получите **kerberos ticket**:

```
su -
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

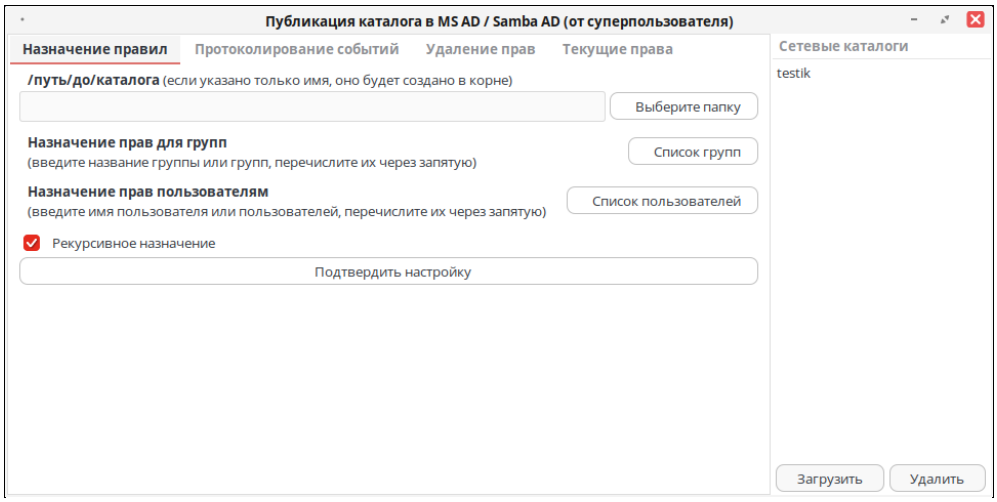
Запуск утилиты доступен через главное меню:



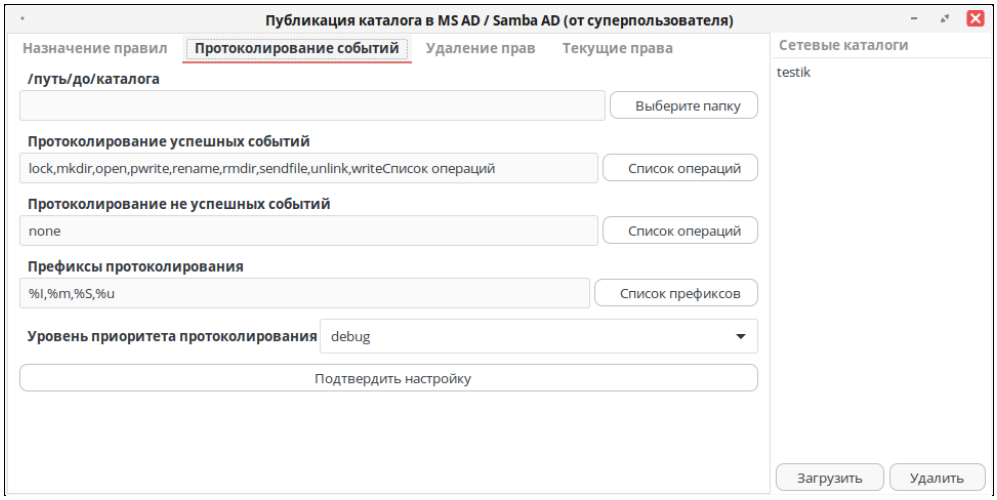
или через терминал:

```
share-directory
```

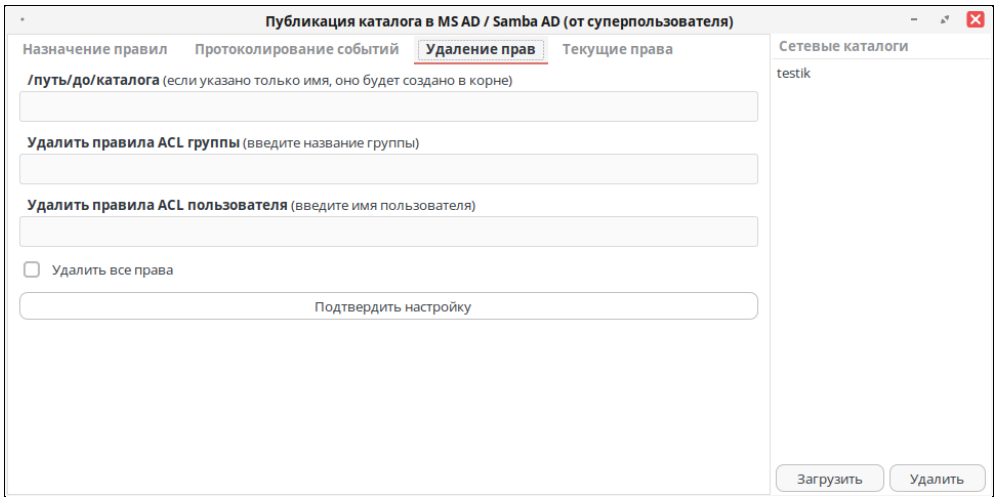
Для публикации сетевого ресурса в домене требуется задать путь к директории, пользователей и/или групп и соответствующие им права.



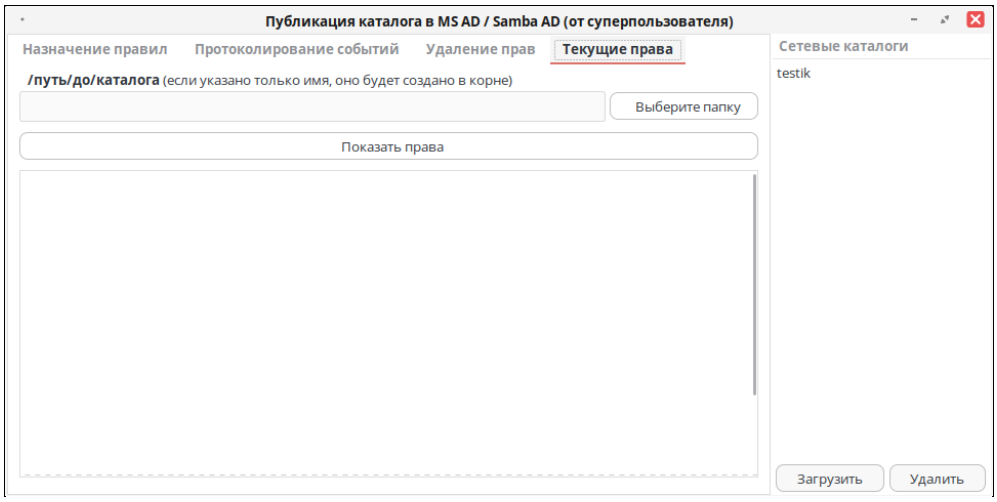
Для протоколирования событий предусмотрена соответствующая вкладка.



Для того чтобы *удалить права* с директории, требуется указать путь к ресурсу и прописать определенного пользователя или группу, которых требуется удалить. Так же доступно полное удаление ACL-прав с директории.



Для удобства *отслеживания прав* можно посмотреть текущие права директории, указав путь к интересующей.



Работа из файлового менеджера

Для включения быстрой настройки сетевой директории из файлового менеджера **caja** необходимо установить дополнительное расширение. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install share_directory-caja
```

Затем получите **kerberos ticket**:

```
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

Выйдите из учетной записи **root** командой:

```
exit
```

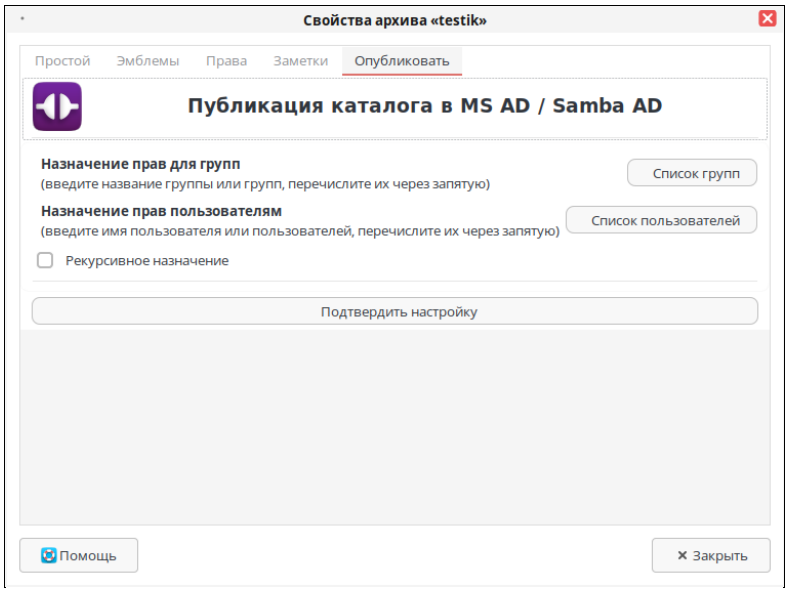
Затем обновите конфигурацию **caja** от имени **локального** пользователя:

```
caja -q
```

Или выполните выход из учетной записи пользователя и обратную авторизацию.

После обновления списка расширений **caja** станет доступен новый пункт в свойствах директории.

Вызовите контекстное меню правой кнопкой мыши для необходимой директории в файловом менеджере, затем выберите пункт «**Свойства**» – «**Опубликовать**».



Консольный вариант

Примечание.

Предполагается, что рабочая станция введена в домен посредством утилиты **join-to-domain** с выбором **sssd**.

Все указанные действия производятся от имени **суперпользователя** (**root**).

1. Добавьте параметр winbind в конце строк, начинающихся с group, passwd и shadow, в файле профиля *authselect* **/etc/authselect/custom/sssd_domain/nsswitch.conf** командой:

```
sed -i_bak '/^\(group:\|passwd:\|shadow:\)/ {s/\(winbind \)\(.*\)$/\2 winbind/; /winbind/ ! s/$/ winbind/}'
/etc/authselect/custom/sssd_domain/nsswitch.conf
```

2. Примените изменения профиля *authselect* командой:

```
authselect apply-changes
```

3. Проверьте возможность получения *kerberos*-билета для доменного пользователя:

```
kinit username
klist
```

4. Проверьте доступность входа доменного пользователя в систему:

```
su username
exit
```

5. Создайте каталог для общего доступа:

```
mkdir -p /share/
```

6. Назначьте права доступа. Пример для домена *wintest*:

```
chown -R root:"wintest\Пользователи домена" /share
chmod 2770 /share
setfacl -m default:group:"wintest\Администраторы домена":rwx /share/
setfacl -m default:group:"wintest\Пользователи домена":r-x /share/
setfacl -m default:other::--- /share/
```

В данном примере с помощью команды **setfacl** были выданы полные (rwx) права группе «**Администраторы домена**» на каталог **/share**.

Группе «**Пользователи домена**» домена *wintest* были выданы права только на чтение и выполнение (просмотр содержимого каталога).

7. Настройте политику *SELinux* для общего каталога и примените её:

```
semanage fcontext -a -t samba_share_t "/share(/.*)?"
restorecon -R -v /share
```

8. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) в секции [global] проверьте наличие следующих строк:

```
vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab
```

9. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) создайте раздел настроек общего ресурса [share] (с этим именем ресурс будет отображаться для клиентов):

```
[share]
 path = /share/
 read only = no
 browseable = yes
 create mask = 0664
 directory mask = 0775
```

10. Дополнительная настройка прав:

- установить полные права на каталог для группы:

```
setfacl -m g:"wintest\Группа_Пользователей":rwx /share
```

- установить полные права на каталог для пользователя:

```
setfacl -m u:"wintest\Пользователь":rwx /share
```

- удалить ACL для определённого пользователя:

```
setfacl -x u:alex /share
```

- удалить все ACL-права каталога:

```
setfacl -b /share
```

- просмотреть ACL-права на каталог:

```
getfacl /share
```

Подробное описание списков контроля доступа (ACL) и параметров команды **setfacl** доступно в нашей статье «Списки контроля доступа ACL»

11. Установите автоматический запуск служб *samba*:

```
systemctl enable smb --now
systemctl enable nmb --now
systemctl enable winbind --now
```

12. Перезагрузите рабочую станцию. Проверьте статус служб:

```
systemctl is-failed smb
systemctl is-failed nmb
systemctl is-failed winbind
```

При корректной настройке каждая команда должна вывести сообщение «active».

О домене IPA

Что такое домен IPA?

Домен IPA (FreeIPA) - это интегрированное решение идентификации и авторизации для РЕД ОС. Сервер FreeIPA обеспечивает централизованную аутентификацию, авторизацию и предоставление учетной информации путем хранения данных о пользователе, группах, хостах и других объектах, необходимых для управления аспектами безопасности компьютерной сети.

FreeIPA построена на основе хорошо известных Open Source компонентов и стандартных протоколов с очень сильной ориентацией на простоту управления и автоматизацию задач установки и настройки.

Несколько FreeIPA-серверов можно легко настроить в домене FreeIPA, чтобы обеспечить избыточность и масштабируемость. 389 Directory Server является основным хранилищем данных и предоставляет полный LDAPv3 мульти-мастер инфраструктуры каталогов. Аутентификация с использованием единого входа осуществляется через MIT Kerberos KDC. Возможности аутентификации дополняются интегрированным центром сертификации на основе проекта Dogtag . При желании можно управлять именами доменов с помощью интегрированного сервера DNS .

Управление полностью централизовано и управляется через веб - интерфейс или инструмент командной строки.

Вы можете подробнее ознакомиться с доменом IPA, просмотрев наши обучающие видео:

- на **RuTube** — Обзор домена FreeIPA;
- в **Яндекс.Дзен** — Обзор домена FreeIPA;
- в **VK Видео** — Обзор домена FreeIPA.

На наших каналах вы также сможете найти много другой полезной информации.

Зачем использовать домен IPA?

Для обеспечения эффективности, соблюдения и снижения рисков организациям необходимо централизованно управлять и сопоставлять важную информацию о безопасности, включая:

- **Идентификацию** (машин, пользователей, виртуальных машин, групп, учетных данных для проверки подлинности)
- **Политики** (управление доступом на основе хоста, правил sudo, пользовательских карт SELINUX)
- **SSO** - технология единого доступа к различным сервисам и ресурсам

Домен на основе IPA сфокусирован на том, чтобы информация о пользователе, политиках и аудите была легко централизованной, совместимой и управляемой. Так же, имеет возможность взаимодействовать с Windows доменами и многое другое.

Рекомендации по развертыванию

ВАЖНО!

Некоторые параметры и решения, не учтенные до развертывания IPA очень трудно изменить позже или даже невозможно. Поэтому в этом пункте приводятся важнейшие особенности и решения, необходимые для успешного развертывания.

Вы можете подробнее ознакомиться с доменом IPA, просмотрев наши обучающие видео:

- на **RuTube** — Обзор домена FreeIPA;
- в **Яндекс.Дзен** — Обзор домена FreeIPA;
- в **VK Видео** — Обзор домена FreeIPA.

На наших каналах вы также сможете найти много другой полезной информации.

DNS

DNS преднамеренно отображается первым, поскольку DNS играет важную роль в функциях управления идентификацией, особенно Kerberos.

Домен

IPA всегда должен иметь собственный основной домен, например example.ru или ipa.example.ru, который не должен использоваться совместно с другой системой управления идентификацией на основе Kerberos, поскольку в противном случае на уровне системы Kerberos будут возникать конфликты. Например, если IPA и Active Directory используют один и тот же домен, доверительные отношения никогда не будут возможны, а также автоматическое обнаружение клиентского сервера через DNS SRV-записи.

Избегайте коллизий имен. Мы настоятельно рекомендуем вам не использовать доменное имя, которое не делегировано вам, даже в частной сети. Например, вы не должны использовать доменное имя example.ru, если у вас нет действительного делегирования для него в общедоступном дереве DNS. Если это правило не соблюдается, доменное имя будет разрешено по-разному в зависимости от конфигурации сети. В результате сетевые ресурсы станут недоступными. Использование доменных имен, которые не делегированы вам, также затрудняет развертывание и обслуживание DNSSEC. Дополнительную информацию об этой проблеме можно найти в FAQ ICANN по вопросам коллизий доменных имен.

Клиентские машины не обязательно должны находиться в том же домене, что и IPA-серверы. Например, IPA может быть доменом ipa.example.ru и иметь клиентов в домене clients.example.ru, просто нужно иметь четкое сопоставление между доменом DNS и областью Kerberos. Стандартным методом для создания сопоставления являются записи TXT DNS (IPA DNS добавляет их автоматически).

ВАЖНО

!!! Не называйте свой домен .local !!! Он зарезервирован для автоматически конфигурируемых сетей.

Если нужно получить доступ к ресурсам в уже существующей среде (Windows AD). То необходимо внести изменения в процесс разрешения хостов на linux машине. Отредактируйте /etc/nsswitch.conf. Изначально интересующий нас раздел содержит следующие записи:

```
hosts:      files mdns4_minimal [NOTFOUND=return] dns
```

Соответственно, в этом режиме сначала производится поиск в файле /etc/hosts, затем запрос идет к mdns, после чего возвращается ответ "не найдено". Mdns кэширует данные и работает с демоном Avahi. Модифицируйте эту "схему" к классическому виду:

```
hosts:      files dns
```

Особенности для интеграции с Active Directory

Домен Active Directory - сложная система. Он включает в себя логически структурированный набор ресурсов (машины, пользователи, службы и т. д.), которые принадлежат потенциально нескольким доменам DNS. Несколько доменов DNS могут быть частью одного домена AD (где домен AD по определению совпадает с областью AD Kerberos). Несколько доменов AD можно объединить в лес. Самый

первый домен AD, созданный в лесу, называется **лесной корневой домен** . Верхнее имя основного домена DNS домена AD используется как имя домена Kerberos AD.

Домен IPA тоже представляет собой сложную систему. Он включает в себя логически структурированный набор ресурсов (машины, пользователи, службы и т. д.), которые принадлежат потенциально нескольким доменам DNS. В отличие от Active Directory у нас есть один домен / область IPA для развертывания, а для Active Directory этот единственный домен IPA выглядит как отдельный лес Active Directory. Active Directory считает основной домен DNS, используемый в качестве основы для области Kerberos IPA, как корневой домен леса для домена IPA (например, корневой домен леса для Active Directory).

Домен IPA может быть размещен в **любом** домене DNS, который не имеет прямого совпадения с любым доменом в лесу Active Directory. Он может быть, например, ipa.example.ru, если эта зона DNS не занята каким-либо другим доменом AD в том же лесу. Или может быть ipa.ad.example.ru, если нет перекрытий на одном уровне зоны DNS.

Доверие между двумя лесами Active Directory всегда устанавливается как доверие между корневыми доменами этих лесов. Если домен IPA использует ipa.ad.example.ru в качестве основной зоны DNS, мы будем говорить об установлении доверительного отношения к лесу между лесом Active Directory ad.example.ru и доменом IPA ipa.ad.example.ru. Если существует несколько зон DNS, принадлежащих домену IPA, рекомендуется размещать записи kerberos указывающие на имя области IPA в каждом из них для правильного обнаружения сетевых ресурсов клиентами IPA.

DNS-сервер

Домен IPA может обслуживаться либо интегрированной службой DNS, либо внешней службой. Рекомендуется использовать интегрированную службу DNS.

При использовании интегрированной службы DNS пакет bind-dyndb-ldap должен быть установлен перед разворачиванием IPA сервера.

При использовании внешнего сервера имен возможно использование функций управления идентификацией или доверия, однако конфигурация будет намного сложнее и подвержена ошибкам.

Имя области Kerberos

Когда вы начинаете устанавливать сервер IPA, вы всегда определяете имя области Kerberos для этой установки. При выборе названия области выполните следующие правила:

- Имя области не должно конфликтовать с любым другим существующим именем области Kerberos (например, имя, используемое Active Directory).
- Имя области должно быть верхним регистром (EXAMPLE.RU) основного DNS-имени домена (example.ru).
- Клиенты IPA из разных доменов DNS (example**.net**, example**.org,** example**.com**) могут быть объединены в единую область Kerberos (EXAMPLE**.RU**)
- Одна установка IPA всегда представляет собой единую область Kerberos.

ВАЖНО

Невозможно изменить основной домен и область IPA после установки. Продумайте его тщательно. Не ожидайте перехода от лабораторной / промежуточной среды к рабочей среде (например, сменить lab.example.ru на ipa.example.ru)

Множественное развертывание

Серверы и клиенты IPA могут распространяться в разных географических точках. Механизм местоположения DNS позволяет разделить топологию на отдельные области, называемые *местоположениями*. Клиенты, использующие записи DNS SRV (например, SSSD) в одном месте, используют близлежащие серверы IPA.

При планировании развертывания важно иметь в виду, что функции DNS в IPA требуют, по крайней мере, одного DNS-сервера в каждом месте. Если это необходимо, можно использовать несколько DNS-представлений на внешних DNS-серверах вместо развертывания DNS-сервера для каждого местоположения, но такие настройки обычно менее устойчивы.

PKI

Когда выполнена настройка PKI, хосты и службы IPA могут получать подписанные сертификаты от IPA CA. Затем сертификаты могут использоваться для аутентификации или проверки подлинности в настроенных службах.

В настоящее время существует 3 типа, настройки среды сертификатов IPA:

1. Без смешивания - IPA просто устанавливается с собственной службой PKI и самозаверяющим сертификатом ЦА
2. Внешний ЦА - IPA установлен с собственной PKI, но сертификат ЦА подписан внешним центром сертификации (служба сертификации Active Directory или другая пользовательская служба сертификации). Для этого требуется, чтобы внешний ЦС разрешил субцентры.
3. Установка без ЦА- IPA не настраивает собственный ЦС, но использует подписанные сертификаты хоста из внешнего ЦС.

ВАЖНО

После установки невозможно изменить базу данных сертификата IPA. Продумайте это тщательно. По умолчанию используется О

```
= $ REALM
```

Серверы/Реплики

Исключительность сервера IPA

Настоятельно рекомендуется избегать развертывания других приложений или служб на виртуальной машине IPA по нескольким основным причинам:

- Причины производительности - сервер IPA может быть ресурсозатратным для машины, особенно когда количество объектов LDAP велико;
- Стабильность - IPA интегрирована в систему, и если стороннее приложение меняет конфигурацию или службы IPA, домен может сломаться
- Легче перенести сервер IPA на более новую платформу

Количество серверов

IPA работает в реплицированной среде с несколькими мастерами. Количество серверов зависит от нескольких факторов:

- Сколько записей в системе?
- Сколько у вас разных географически распределенных центров обработки данных?
- Насколько активны приложения и клиенты в отношении аутентификации и поиска LDAP.

Как правило, рекомендуется иметь по меньшей мере 2-3 реплики в каждом центре обработки данных. В каждом центре обработки данных должна быть по крайней мере одна реплика с дополнительными службами IPA, такими как PKI или DNS, если они используются. Обратите внимание, что не рекомендуется иметь более 4 реплик в одном месте. В следующем примере показана рекомендуемая инфраструктура:

Клиенты

У каждого клиента для отказоустойчивости должно быть как минимум 2 DNS сервера, настроенных в /etc/resolv.conf. Обновите конфигурацию resolv.conf и *DHCPd* .

Для каждого клиента, использующего ipa-client-install, требуется доступ к порту 443 (HTTPS) на сервере IPA. Это связано с тем, что после регистрации клиент загружает собственные ключи SSH и выполняет несколько операций. IPI CLI также использует тот же порт для связи с ведущим IPA. Таким образом, требуется доступ к HTTPS (443) с клиентской стороны.

Интеграция с Active Directory

Чтобы настроить доверительные отношения, необходимо правильно настроить DNS, IPA должен иметь собственный первичный DNS-домен, и соответствующую ему область Kerberos. DNS-домен и область Kerberos должны отличаться от домена DNS Active Directory.

Еще одним важным требованием является стек IPv6. Рекомендуемым способом для современных сетевых приложений является только открытие сокетов IPv6 для прослушивания, поскольку IPv4 и IPv6 используют один и тот же диапазон локальных портов. IPA использует Samba как часть интеграции с Active Directory, а Samba **требует включенного стека IPv6** на машине.

НЕ используйте ipv6.disable = 1 в командной строке ядра: он отключает весь стек IPv6 и ломает Samba.

Если необходимо, добавьте ipv6.disable_ipv6 = 1, это будет поддерживать функциональность стека IPv6, но не будет назначать адреса IPv6 для ваших сетевых устройств. Это рекомендуемый подход для случаев, когда вы не используете сети IPv6.

Добавление следующих строк в /etc/sysctl.d/ipv6.conf, позволит не назначать адреса IPv6 для определенного сетевого интерфейса:

```
net.ipv6.conf.all.disable_ipv6 = 1
# Отключение «все» не применяется к интерфейсам, которые уже используются, когда применяются параметры sysctl.
net.ipv6.conf.<интерфейс0>.disable_ipv6 = 1
```

где *interface0* - ваш специализированный интерфейс. Обратите внимание, что все, что нам нужно, это то, чтобы стек IPv6 был включен на уровне ядра, это рекомендуется для разработки сетевых приложений уже давно.

SSL

Из-за CVE-2014-3566 протокол протокола Secure Socket Layer версии 3 (SSLv3) должен быть отключен в модуле mod_nss. Вы можете сделать это, выполнив следующие шаги:

1. Отредактируйте файл/etc/httpd/conf.d/nss.conf и установите параметр *NSSProtocol* (для обратной совместимости) и TLSv1.1.

```
NSSProtocol TLSv1.0, TLSv1.1
```

2. Перезапустите httpd-службу.

```
# service httpd restart
```

Установка сервера IPA

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер минимальный
- **Версия ПО**: ipa-server-4.10.1-2

Вы можете подробнее ознакомиться с информацией по установке в РЕД ОС сервера IPA, просмотрев наши обучающие видео:

- на **RuTube** — Установка и настройка FreeIPA в РЕД ОС;
- в **Яндекс.Дзен** — Установка и настройка FreeIPA в РЕД ОС;
- в **VK Видео** — Установка и настройка FreeIPA в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Подготовка сервера

Настройка синхронизации времени с помощью chronyd

Откройте файл конфигурации:

```
# nano /etc/chrony.conf
```

Если есть необходимость, то пропишите в файле сервера времени, перед стандартными серверами.

```
server ntp1.vniiftri.ru iburst
server ntp2.vniiftri.ru iburst
server ntp3.vniiftri.ru iburst
server ntp4.vniiftri.ru iburst
```

Отключите сервис:

```
# systemctl disable --now systemd-timesyncd
```

Установите часовой пояс:

```
# timedatectl set-timezone Europe/Moscow
```

Настройте сетевой адаптер

ВАЖНО!

IP-адрес сервера никогда не должен изменяться. Сделайте его статическим в вашей сети.

Более подробное описание конфигурирования сетевого адаптера вы можете найти в статье «Настройка сетевого адаптера».

Назначьте имя серверу

Используйте полное доменное имя. Имя серверу можно назначить командой

```
# hostnamectl set-hostname server.redosipa.ru
```

Установите ipa-server

Установите IPA сервер:

```
# dnf install ipa-server-dns ipa-server-trust-ad python3-packaging pki-ca pki-kra pki-acme
```

ВАЖНО! ТОЛЬКО ДЛЯ РЕД ОС ВЕРСИИ 7.3

Для того чтобы при установке избежать появления ошибки **"CA configuration failed"**, выполните следующие действия:
1. Убедитесь, что используется Java OpenJDK версии 8:

```
java -version
```

2. Если используется Java 11, то необходимо переключиться на 8-ую версию. Для этого выполните команды:

```
update-alternatives --config java
update-alternatives --config jre_openjdk
```

в каждой выберите нужную версию, указав ее порядковый номер. После чего нажмите *Enter*.

3. Удалите пакет:

```
rpm -e java-17-openjdk-headless --nodeps
```

Удалите пакет Java OpenJDK версии 11:

```
rpm -e java-11-openjdk-headless --nodeps
```

Настройка сервера

Есть два варианта настройки, интерактивный и автоматический.

ВАЖНО!

Невозможно изменить конфигурацию ЦС после создания домена, и невозможно перенести его из одной конфигурации в другую. Крайне важно, чтобы требования ЦС были рассмотрены до начала процесса установки.

Если каждая машина в домене будет клиентом IPA, добавьте адрес сервера IPA в конфигурацию DHCP.

Заметка

Сценарий ipa-replica-install включает в себя утилиту ipa-replica-conncheck, которая проверяет статус требуемых портов. Вы также можете запускать ipa-replica-conncheck отдельно для устранения неполадок.

+ Опции и параметры автоматической установки.

Основные параметры

-r *REALM_NAME*, **--realm**=*REALM_NAME (REALM имя)*

Имя области Kerberos для сервера IPA

-n *DOMAIN_NAME*, **--domain**=*DOMAIN_NAME* (*доменное имя)*

Ваше доменное имя DNS

-p *DM_PASSWORD*, **--ds-password**=*DM_PASSWORD (DM пароль)*

Пароль, который будет использоваться сервером каталогов для пользователя Менеджера каталогов

-P *MASTER_PASSWORD*,

--master-password=*MASTER_PASSWORD (мастер паролей)*

Главный пароль kerberos (обычно генерируемый автоматически)

-a *ADMIN_PASSWORD*,

--admin-password=*ADMIN_PASSWORD (пароль администратора*)

Пароль для пользователя admin IPA

--hostname=*HOST_NAME (имя хоста*)

Полное DNS-имя этого сервера. Если имя хоста не совпадает с именем системного хоста, системное имя хоста соответственно, будет обновляться, чтобы предотвратить сбои службы.

--ip-address=*IP_ADDRESS* (*IP адрес*)

IP-адрес этого сервера. Если этот адрес не соответствует адресу, который хост разрешает, и --setup-dns не выбран, установка завершится с ошибкой. Если имя хоста сервера не разрешимо, запись для имени хоста и IP_ADDRESS добавляется в / etc / hosts.

-N, **--no-ntp** *(нет **ntp**)*

Не настраивать NTP

--idstart=*IDSTART*

Начальный идентификатор пользователя и группы (по умолчанию случайный)

--idmax=*IDMAX*

Максимальный идентификатор пользователя и группы (по умолчанию: idstart + 199999). Если установлено равным нулю, будет использоваться значение по умолчанию.

--no_hbac_allow *(не разрешать hbac)*

Не устанавливайте правило allow_all (разрешить всё) HBAC. Это правило позволяет любому пользователю с любого хоста получать доступ к любой службе на любом другом хосте. Ожидается, что пользователи удалят это правило перед переходом на производство.

--no-ui-redirect *(не перенаправлять ui)*

Не следует автоматически перенаправлять веб-интерфейс,

--ssh-trust-dns *(ssh доверить dns)*

Настройте клиент OpenSSH для проверки записей DNS SSHFP,

--no-ssh *(нет ssh)*

Не настраивайте клиента OpenSSH,

--no-sshd *(нет sshd)*

Не настраивать сервер OpenSSH,

-d, **--debug** (*отладить*)

Включить ведение журнала отладки, когда требуется более подробный вывод,

-U, **--unattended** (*без запроса*)

Автоматическая установка, которая никогда не будет запрашивать,

для ввода пользователем.

Параметры системы сертификата

--external-ca

Генерировать CSR, который должен быть подписан внешним CA

--external_cert_file=*ФАЙЛ*

Файл, содержащий сертификат PKCS # 10

--external_ca_file= *ФАЙЛ*

Файл, содержащий PKCS # 10 внешней CA-цепи

--dirsrv_pkcs12= *ФАЙЛ*

Файл PKCS # 12, содержащий сертификат SSL сервера каталогов

***--http_pkcs12**= ФАЙЛ*

Файл PKCS # 12, содержащий сертификат SSL Apache Server

--dirsrv_pin=*DIRSRV_PIN*

Пароль файла PKCS # 12 сервера каталогов

--*http_pin*=*HTTP_PIN*

Пароль файла Apache Server PKCS # 12

--subject=*ПРЕДМЕТ*

База данных сертификата (по умолчанию O = REALM.NAME)

--selfsign

Настройте самозаверяющий экземпляр CA для выдачи сертификатов сервера вместо использования dogtag для сертификатов.

ПРЕДУПРЕЖДЕНИЕ. Использование этой опции ограничивает возможности управления сертификатами сервера. Пожалуйста, имейте в виду, что этот способ не меняется.

Опции (выбор) DNS

--setup-dns *(настройка DNS)*

Создайте зону DNS, если она еще не существует, и настройте DNS-сервер. Эта опция требует, чтобы вы либо указали по крайней мере один переадресатор DNS через параметр **--forwarder**, либо использовали параметр **--no-forwarders**.

Обратите внимание, что вы можете настроить DNS в любое время после установки первого сервера IPA, выполнив ipa-dns-install.

--forwarder=*IP_ADDRESS* (*IP адрес*)

Добавьте DNS-переадресацию в конфигурацию DNS. Вы можете использовать эту опцию несколько раз, чтобы указать больше пересылок, но по крайней мере один должен быть предоставлен, если не указана опция **--no-forwarders**.

--no-forwarders

Не добавляйте DNS-пересылок. Вместо этого будут использоваться корневые DNS-серверы.

--reverse-zone=*REVERSE_ZONE* (*обратная зона*)

Зона обратного использования DNS

--no-reverse *(без обратной зоны)*

Не создавать обратную зону DNS

--zonemgr *(зона mgr)*

Адрес электронной почты менеджера зоны DNS. По умолчанию hostmaster @ DOMAIN

--no-persistent-search *(нет постоянного поиска)*

Не включать механизм постоянного поиска для обновления списка зон DNS на сервере имен. Если постоянный поиск отключен, а параметр -zone-refresh не установлен на ненулевом значении, новые зоны не будут запускаться, пока сервер имен не будет перезагружен.

--zone-refresh=*ZONE_REFRESH* *(зона обновления)*

Если установлено ненулевое значение, механизм обновления постоянной зоны поиска будет отключен, а сервер имен будет использовать механизм опроса для загрузки новых зон DNS каждые секунды ZONE_REFRESH.

--no-host-dns *(нет хоста DNS)*

Не используйте DNS для поиска имени хоста во время установки

--no-dns-sshfp *(нет DNS sshfp)*

Нельзя автоматически создавать записи DNS SSHFP.

--no-serial-autoincrement *(нет последовательного автоматического увеличения)*

Не включайте функцию автоматического автообновления SOA. Последовательность SOA должна быть обновлена автоматически или другие функции DNS, такие как передача зоны, DNSSEC не будут работать должным образом. Для этой функции требуется постоянный механизм обновления зоны поиска.

Параметры удаления

--uninstall *(удаление, деинсталяция)*

Удалите существующую установку IPA

-U, **--unattended** *(без сопровождения*)

Автоматическая деинсталляция, которая никогда не будет

приглашение для ввода пользователем

Статус выхода

0, если установка (un) прошла успешно

1, если произошла ошибка

Интерактивная установка

```
# ipa-server-install --mkhomedir
```

Помимо аутентификации, IPA может управлять DNS-записями для хостов. Это может облегчить настройку и управление хостами.

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Далее нужно указать имя хоста сервера, доменное имя и пространство Kerberos.

```
Server host name [server.redosipa.ru]:
Please confirm the domain name [redosipa.ru]:
Please provide a realm name [REDOSIPA.RU]:
```

Затем создайте пароль для менеджера каталогов LDAP и пароль администратора IPA, который будет использоваться при аутентификации в IPA в качестве администратора.

Если нужно, добавляем ретранслятор службы имен (DNS relay). Этот шаг необязателен, и необходим в том случае, если у Вас предполагается использовать внешний сервер для обработки запросов службы имен DNS. Учитываете, что по-умолчанию, сервер IPA предполагает, что будет пользоваться собственным сервером имен, который развертывает локально.

```
Do you want to configure DNS forwarders? [yes]:
```

Выбирайте [yes] (да), в случае, если присутствует внешний ретранслятор службы имен, иначе, выбирайте [no] – нет. Далее впишите дополнительные реверс зоны, если они нужны.

```
Do you want to configure these servers as DNS forwarders?
```

Инициируем создание обратной зоны для службы имен.

```
Do you want to search for missing reverse zones? [yes]:
Do you want to create reverse zone for IP 192.168.1.123 [yes]:
Please specify the reverse zone name [1.168.192.in-addr.arpa.]:
```

и имя NetBIOS для домена IPA. По умолчанию он определяется на основе доменного имени DNS.

```
NetBIOS domain name:
```

Подтвердите конфигурацию. После этого запустится программа установки.

```
Continue to configure the system with these values? [no]: yes
```

Убедитесь, что сервер IPA работает:

```
kinit admin
ipa user-find admin
```

Установите оболочку по умолчанию для пользователей:

```
ipa config-mod --defaultshell=/usr/bin/bash
```

Подробную информацию о вводе хоста РЕД ОС в домен IPA см. в нашей инструкции «Ввод клиентских машин в домен IPA».

Настройка репликации IPA

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** ipa-4.8.10

Предварительная настройка сервера

Задайте хостнейм

Он должен быть в области домена IPA сервера. Например, если ваш домен example.ru, то хостнейм реплики может быть - rep1.example.ru

```
# hostnamectl set-hostname rep1.example.ru
```

Отредактируйте hosts

На уже созданном IPA сервере и на будущей реплике внесите в /etc/hosts адреса друг друга.

Открыть файл хостов можно в текстовом редакторе nano.

```
# nano /etc/hosts
10.81.1.181   ipa.example.ru
10.81.1.182   rep1.example.ru
```

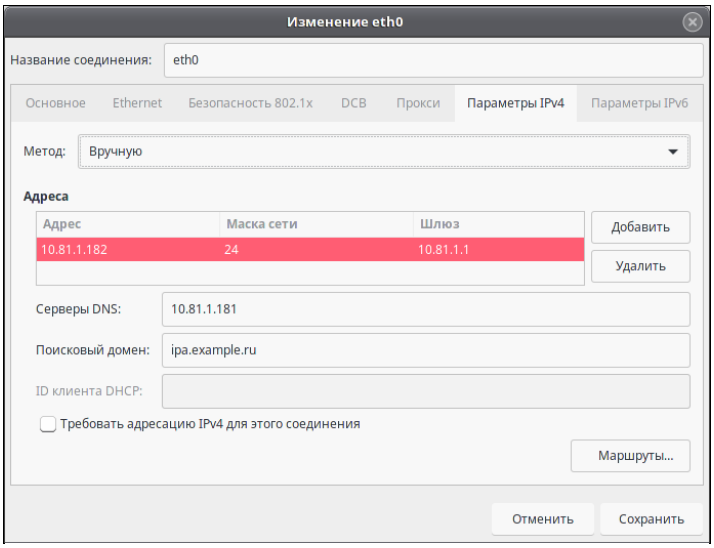
Настройте сетевой адаптер

ВАЖНО!

IP адрес сервера никогда не должен изменяться. Сделайте его статическим в вашей сети.

Пропишите настройки DNS, домена и поискового сервера по умолчанию в создаваемой реплике, укажите в качестве DNS ваш IPA сервер. Подробнее о настройке сети см. в нашей статье «Настройка сетевого адаптера».

Пример:



Перезагрузите сеть.

```
# systemctl restart NetworkManager
```

Проверка настроек

Проверьте заданные настройки в файле /etc/resolv.conf

```
# cat /etc/resolv.conf
search example.ru
domain example.ru
nameserver 10.81.1.181
```

Для корректной синхронизации реплики и сервера требуется на стороне сервера и реплики выполнить:

```
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
ntpdate time.yandex.ru
nano /etc/ntp.conf

добавьте строчку
server time.yandex.ru

закомментируйте строки:
#server ntp1.vniiftri.ru
#server ntp2.vniiftri.ru
#server ntp3.vniiftri.ru
#server ntp4.vniiftri.ru
```

Так же выполните команду:

```
# dig SRV _ldap._tcp.example.ru
```

в выводе нужно удостоверится, что SRV запись берется из DNS контроллера домена, в нашем случае с ipa.example.ru. Примерный вывод представлен ниже.

```
[root@localhost ~]# dig SRV _ldap._tcp.example.ru
; <<>> DiG 9.9.4-GosLinux-9.9.4-52.el7 <<>> SRV _ldap._tcp.example.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24642
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_ldap._tcp.ipa.murom.          IN      SRV
;; ANSWER SECTION:
_ldap._tcp.ipa.murom.   86400   IN      SRV     0 100 389 ipa.example.ru.
;; AUTHORITY SECTION:
example.ru.             86400   IN      NS      ipa.example.ru.
;; ADDITIONAL SECTION:
ipa.example.ru.         1200    IN      A       10.81.1.181
ipa.example.ru.         1200    IN      A       10.9.0.2
;; Query time: 1 msec
;; SERVER: 10.81.1.181#53(10.81.1.181)
;; WHEN: Вт дек 28 12:46:05 MSK 2017
;; MSG SIZE  rcvd: 112
```

Настройка синхронизации времени с помощью chronyd

После успешной синхронизации выполните

```
systemctl stop ntpd
systemctl disable ntpd
systemctl start chronyd
systemctl enable chronyd
```

Установка ipa-client

Установите ipa-client:

```
dnf install ipa-client ipa-server-dns
```

После установки, убедитесь что используется Java OpenJDK версии 8:

```
java -version
```

Если используется Java 11, то необходимо переключиться на 8-ую версию. Для этого выполните команды:

```
update-alternatives --config java
update-alternatives --config jre_openjdk
```

в каждой выберите нужную версию, указав ее порядковый номер. После чего нажмите Enter.

Настройте клиента.

Впишите в команду данные для вашей сети:

```
ipa-client-install -d --mkhomedir --enable-dns-updates
```

Скрипт установки должен автоматически найти настройки на ipa сервере, вывести их и спросить подтверждение для найденных параметров:

```
Continue to configure the system with these values? [no]:
```

Ответьте yes.

Затем введите имя администратора. Можно просто использовать администратора по умолчанию IPA, который был создан при установке сервера:

```
User authorized to enroll computers: admin
```

Введите пароль администратора IPA, который был установлен во время настройки сервера IPA.

После этого клиент IPA подготовит систему.

Если установка прошла успешно, в конце вывода вы увидите:

```
Client configuration complete.
The ipa-client-install command was successful
```

Далее нужно создать обратный адрес для реплики на DNS сервере основного сервера. Зайдите в веб управление и перейдите в Network Services > DNS > Зоны DNS. Выберете в таблице запись вашего домена, например org.lan. и в открывшемся списке откройте запись вашей реплики, например ipareplica0. Нажмите на ip адрес в поле A записи и на ссылку в открывшемся окне. Обратная запись создана.

После этого хост должен появиться в веб-интерфейсе.

Настройка обратной зоны DNS на сервере IPA

Если реплика находится в другой подсети, создайте для нее обратную зону и добавьте в неё PTR запись для реплики.

Если реплика находится в одной подсети с IPA сервером, достаточно просто создать PTR запись для реплики.

Настройка репликации

Перейдите к настройке репликации

Выполните:

```
ipa-replica-install
```

Введите пароль администратора:

```
Password for admin@EXAMPLE.RU:
```

Дождитесь установки и настройки репликации.

Установка CA сервера

Перейдите к установке CA сервера:

```
ipa-ca-install
```

Введите Directory Manager password:

```
Directory Manager (existing master) password:
```

После завершения зайтите на любой веб-интерфейс и проверьте топологию**:**

Настройте DNS-сервер на реплике

Выполните команду:

```
ipa-dns-install
```

Разрешите форвардеров.

У вас автоматически возьмутся днс сервера из файла /etc/resolv.conf, если там только один основной сервер ipa, укажите дополнительно основной DNS сервер в сети.

```
Enter an IP address for a DNS forwarder, or press Enter to skip:
```

Если вдруг ваша реплика находится в другом регионе, можно указать другие форвардеры.

Мониторинг запущенных процессов

Необходимо мониторить запущенные процессы, открытые порты и самое главное мониторить срок действия корневого CA-сертификата. Проверить сертификат можно в веб управлении IPA сервера.

Вывод клиента из домена Ipa

Для вывода клиента из домена Ipa выполните команду:

```
ipa-client-install --uninstall
```

Настройка резервного копирования домена IPA

Резервное копирование полного сервера IPA
Резервная копия только для данных
Создание резервной копии
Автоматизация резервного копирования
Восстановление резервной копии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер минимальный
- **Версия ПО:** ipa-server-4.8.10-12

IPA предлагает два варианта резервного копирования: резервное копирование полного сервера **IPA** и резервная копия только для данных.

Резервное копирование полного сервера IPA

Полное резервное копирование создает копию всех файлов сервера **IPA**, а также данных LDAP, что делает его автономной резервной копией. **IPA** затрагивает сотни файлов: файлы, сочетание целых каталогов и определенных файлов, таких как файлы конфигурации или файлы журналов. Они относятся непосредственно к **IPA** или к различным его службам.

Поскольку полносерверная резервная копия является копией необработанных файлов, она выполняется в автономном режиме. Скрипт, выполняющий полное серверное резервное копирование, останавливает все службы **IPA**, чтобы обеспечить безопасный ход процесса резервного копирования.

Резервная копия только для данных

Резервная копия только для данных создает копию данных **LDAP** и журнала изменений. Этот процесс поддерживает **IPA-REALM** и может также создавать резервные копии нескольких серверных частей или только одну; серверная часть включает **PA** и **CA Dogtag**. Этот тип резервного копирования также поддерживает запись содержимого **LDAP**, хранящегося в **LDIF**. Резервная копия данных может выполняться как в режиме онлайн, так и в автономном режиме.

Создание резервной копии

По умолчанию **IdM** хранит созданные резервные копии в каталоге **/var/lib/ipa/backup/**.

Для полного резервного копирования сервера **IPA** выполните команду:

```
ipa-backup
```

Например:

```
ipa-backup

Preparing backup on server.redosipa.ru
Local roles match globally used roles, proceeding.
Stopping IPA services
Backing up ipaca in REDOSIPA-RU to LDIF
Packing up userRoot in REDOSIPA-RU to LDIF
Backing up REDOSIPA-RU
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2823-87-04-16-35-31
The ipa-backup command was successful
```

Для резервной копии только данных без остановки сервера выполните:

```
ipa-backup --data --online
```

где:

- **--data** — выполняет резервное копирование только данных,
- **--online** — выполняет онлайн-резервное копирование этот параметр доступен только с резервными копиями только для данных.

Например:

```
ipa-backup --data --online

Preparing backup on server.redosipa.ru
Local roles match globally used roles, proceeding.
Backing up ipaca in REDOSIPA-RU to LDIF
Waiting for LDIF to finish
Backing up userRoot in REDOSIPA-RU to LDIF
Waiting for LDIF to finish
Backing up REDOSIPA-RU
Waiting for BAK to finish
Backed up to /var/lib/ipa/backup/ipa-data-2823-87-84-16-48-44
The ipa-backup command was successful
```

Автоматизация резервного копирования

Для автоматизации можно использовать **cron**. Отредактируйте файл **/etc/crontab**. Например для создания ежедневной копии только данных в 23.30 впишите следующую строку.

```
30 23 * * * root ipa-backup --data --online
```

Восстановление резервной копии

Для восстановления резервной копии необходимо, чтобы на ПК уже был установлен и настроен **IPA**-сервер по нашей инструкции «Установка сервера IPA».

Далее перейдите в каталог с резервной копией IPA-сервера и выполните команду восстановления:

```
ipa-restore <имя_РК>
```

Например:

```
cd /var/lib/ipa/backup
ipa-restore ipa-full-2023-07-04-21-40-49

SystemWide CA database updated.
Restoring from userRoot in REDOSIPA-RU
Restoring from ipaca in REDOSIPA-RU
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restarting IPA services
Restoring umask to 18
The ipa-restore command was successful
```

Создание доверительных отношений IPA и MSAD в РЕД ОС 7.3

Для примера создания доверительных отношений будут использоваться следующие данные:
Домен IPA - **redos.ipa**
Сервер IPA - **dc1.redos.ipa** - **10.81.1.67**
Домен MS AD - **win.redos**
Сервер MS AD - **dc.win.redos** - **10.81.1.196**

1 Настройки на IPA

1.1 Отключение проверки DNSSEC

Для этого в файле **/etc/named/ipa-options-ext.conf** приведите параметр к виду:

```
dnssec-validation no;
```

Перезагрузить сервер или службу IPA командой:

```
# systemctl restart ipa
```

Примечание.

На время настройки сервиса переведите **selinux** в режим уведомлений. Для этого измените содержимое конфигурационного файла:

```
nano /etc/selinux/config
```

Заменив текст SELINUX=enforcing на SELINUX=permissive

Выполните:

```
setenforce 0
```

Более подробно см.ссылку.

Не забудьте включить selinux после завершения настройки.

1.2 Отредактируйте /etc/hosts

Впишите туда адрес сервера MS AD и его хостнейм.

```
10.81.1.196 dc.win.redos dc
```

1.3 Настройка времени

На всех серверах и рабочих станциях время должно быть синхронизировано.

```
nano /etc/chrony.conf
```

Удалите все остальные строки, начинающиеся на **server**.

Вставьте следующие строки в файл:

```
server ntp1.stratum2.ru iburst
server ntp2.stratum2.ru iburst
server ntp3.stratum2.ru iburst
```

Укажите подсеть:

```
allow 10.81.1.0/24
```

Перезапустите сервис chronyd:

```
systemctl restart chronyd
```

Проверка:

```
chronyc sources
```

1.4 Настройка зоны перенаправления на IPA сервере

На сервере IPA добавьте условный сервер пересылки (зону пересылки dns) для домена Windows AD:

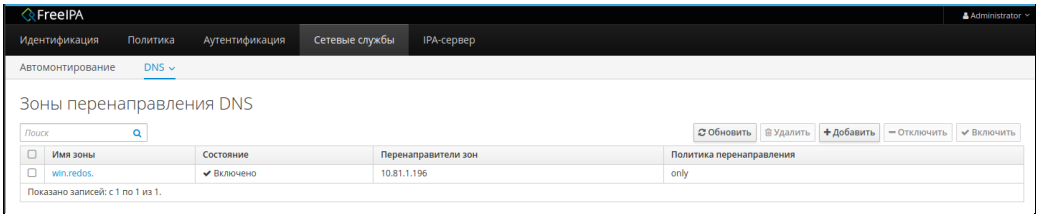
```
# kinit admin
# ipa dnsforwardzone-add win.redos --forwarder=10.81.1.196 --forward-policy=only
```

здесь **10.81.1.196** - windows server;

win.redos - имя домена windows.

С помощью web GUI в параметрах DNS-сервера IPA укажите ip-адрес перенаправителя, им должен быть сервер Windows.

У вас должно получится примерно следующее:



Проверьте, резолвится ли сервер MS AD. Воспользуйтесь командой:

```
# nslookup dc.win.redos
Server:      10.81.1.67
Address:     10.81.1.67#53
Non-authoritative answer:
Name:  dc.win.redos
Address: 10.81.1.196
```

Вам должен вернуться адрес вашего MS AD.

Так же проверьте SRV записи.

```
# dig SRV _ldap._tcp.redos.ipa

# dig SRV _ldap._tcp.win.redos
```

1.5 Переустановка samba-dc

Убедитесь, что установлена актуальная версия samba:

```
dnf update samba
```

Для корректной работы IPA сервера и MS AD требуется версия samba с поддержкой MIT Kerberos. Для ее установки выполните команду:

```
dnf dg samba
```

После этого перезапустите сервис **ipa**:

```
systemctl restart ipa.service
```

Проверьте **Samba** на наличие **MIT Kerberos**:

```
smbd -b | grep HAVE_KADM5SRV_MIT
```

Должны получить вывод:

```
HAVE_KADM5SRV_MIT
```

Для исключения пакетов samba из обновлений, в файл **/etc/dnf/dnf.conf** добавьте строку:

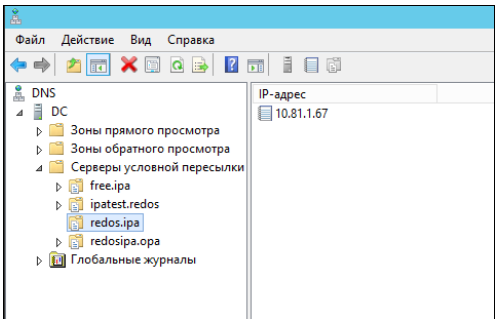
```
exclude=libsmbclient libwbclient python3-samba python3-samba-dc samba*
```

2 Настройка DNS на сервере Windows

Вам нужно сделать так, что бы доменом IPA сервера управлял DNS IPA.

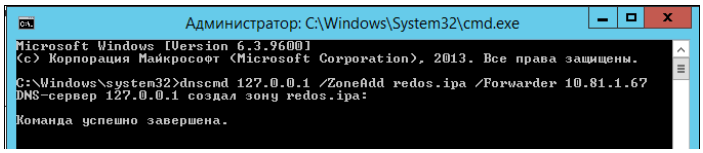
В случае разных доменов создайте сервер условной пересылки.

1. Откройте Диспетчер DNS и перейдите на вкладку «**Серверы условной пересылки**».
2. В контекстном меню выберите «**Создать сервер условной пересылки**».
3. Впишите DNS домен сервера IPA и его ip адрес.
4. Выберите «**Все DNS серверы в этом лесу**» и нажмите **OK**.
5. Ниже приведен примерный результат:

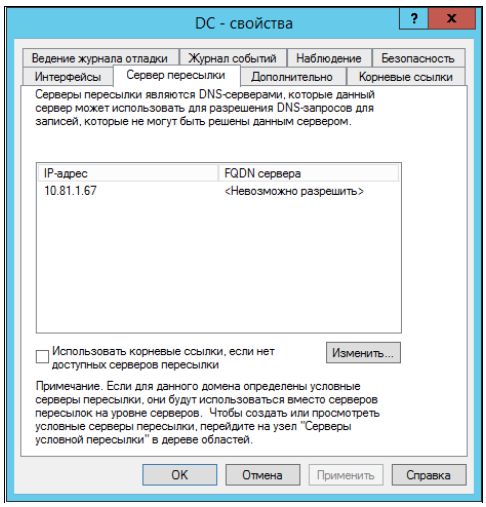


Также это можно сделать с помощью команды:

```
dnscmd 127.0.0.1 /ZoneAdd redos.ipa /Forwarder 10.81.1.67
```



Кроме этого необходимо добавить глобальный "**Сервер пересылки**" в свойствах dns сервера windows. Для этого в диспетчере DNS нажмите правой клавиши мыши на сервере DNS (SERV) и в выпадающем меню выберите "**Свойства**", перейдите на вкладку "**Сервер пересылки**", нажмите на кнопку "**Изменить**" и в открывшемся окне введите ip-адрес сервера IPA.



Также это можно сделать с помощью команды:

```
dnscmd 127.0.0.1 /ResetForwarders 10.81.1.67 /Slave
```

Проверьте конфигурацию DNS на сервере Windows.

Чтобы убедиться, что сервер AD может корректно видеть IPA, проверьте, правильно ли разрешены записи SRV.

```
C:\> nslookup
> set type=srv
> _ldap._tcp.win.redos
> _ldap._tcp.redos.ipa
> quit
```

3 Добавьте доверительные отношения между доменами

3.1 Сконфигурируйте сервер IPA для доверительных отношений с AD.

```
# ipa-adtrust-install
```

Отвечайте на все вопросы скрипта положительно (yes)

При доступе пользователей AD к IPA-клиентам обязательно запустите ipa-adtrust-install на каждом IPA-сервере, к которому будут подключаться клиенты IPA.

3.2 Добавьте доверительные отношения.

```
#ipa trust-add --type=ad win.redos --range-type ipa-ad-trust --admin admin --password --two-way=TRUE
```

На этом этапе будет установлено двустороннее доверие между **FreeIPA** и **Active Directory**. Для создания таких отношений используется опция **--two-way=true**.

При появлении запроса введите пароль администратора.

```
Пароль администратора домена Active Directory:
----------------------------------------------------------------------------
Добавлено отношение доверия Active Directory для области (realm) "win.redos"
----------------------------------------------------------------------------
Имя области (realm): win.redos
Имя домена NetBIOS: WIN
Идентификатор безопасности домена: ***
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Установлено и проверено
```

ВАЖНО!

Учетная запись пользователя, используемая при создании доверия (аргумент опции --admin в командеipa trust-add), должна быть членом группы Domain Admins. Имя учетной записи должно быть на английском языке.

3.3 После того, как установлена доверительное отношение на стороне AD, необходимо получить список доверенных доменов леса со стороны AD. Это делается с помощью следующей команды:

```
# ipa trust-fetch-domains "win.redos"
```

При успехе IPA получит информацию о доверенных доменах и создаст для них все необходимые идентификаторы.

Используйте «trustdomain-find», чтобы просмотреть список доверенных доменов из доверенного леса:

```
# ipa trustdomain-find "win.redos"
```

3.4 Создать внешнюю группу, сопоставленную с группой **posix freeipa**: это позволит предоставить право внешней группе. Затем **active directory** группа администраторов домена сопоставляется с группой **ad_admins**, которая принадлежит пользователю **admins**. В этом случае каждый администратор домена windows имеет некоторый грант администратора **freeipa**:

```
ipa group-add --desc='ad domain external map' ad_admins_external --external
ipa group-add --desc='ad domain users' ad_admins
ipa group-add-member ad_admins_external --external 'WIN.REDOS\Администраторы домена'
ipa group-add-member ad_admins --groups ad_admins_external
```

Ввод клиентских машин в домен IPA

Предварительная настройка РЕД ОС
Присоединение к домену IPA с помощью утилиты join-to-domain
Ручная установка IPA клиента и ввод в домен

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ipa-client-4.8.10-12

Предварительная настройка РЕД ОС

Задайте имя компьютера

Он должен быть в области домена IPA сервера. Например, если ваш домен example.ru, то хостнейм клиента должен быть - client.example.ru.

```
# hostnamectl set-hostname client.example.ru
```

Настройте DNS

Пропишите настройки DNS и домен в создаваемом клиенте, укажите в качестве DNS ваш IPA сервер и опцию, для того, что бы по DHCP не принимался DNS адрес.

Для этого, используйте утилиту **«Сетевые соединения»**, расположенную в **«Меню» → «Параметры» → «Сетевые соединения»** в графическом окружении **Cinnamon** или **«Система» → «Параметры» → «Сетевые соединения»** в графическом окружении **Mate**. Выберите ваше активное подключение, нажмите кнопку **«Изменить»,** перейдите на вкладку **«Параметры IPv4»**, поменяйте **«Метод»** н а **«Вручную»**, в поле «**Дополнительные серверы DNS**» напишите адрес **IPA-сервера** (например 172.16.0.11), в поле **«Дополнительные поисковые домены»** введите поисковый домен (например example.ru), нажмите применить и переподключитесь к сети.

Проверка настроек

Проверьте заданные настройки в файле /etc/resolv.conf:

```
cat /etc/resolv.conf

search  example.ru
nameserver 172.16.0.11
```

Так же выполните команду:

```
dig SRV _ldap._tcp. example.ru
```

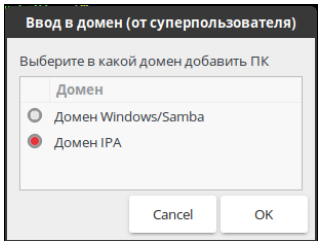
в выводе нужно удостоверится, что SRV запись берется из DNS контроллера домена Примерный вывод представлен ниже.

```
dig SRV _ldap._tcp. example.ru

; <<>> DiG 9.11.4-P2-RedOS-9.11.4-5.P2.el7 <<>> SRV _ldap._tcp. example.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24642
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_ldap._tcp.ipa.murom.          IN      SRV
;; ANSWER SECTION:
_ldap._tcp.ipa.example.   86400   IN      SRV     0 100 389 ipa.example.ru.
;; AUTHORITY SECTION:
example.ru.             86400   IN      NS
ipa.example.ru.
;; ADDITIONAL SECTION:
ipa.example.ru.         1200    IN      A       172.16.0.11
;; Query time: 1 msec
```

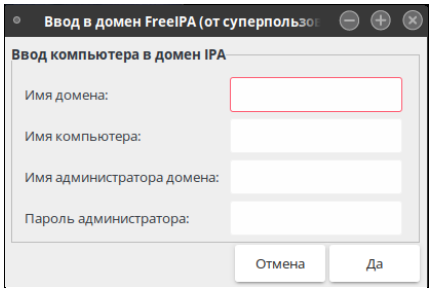
```
;; SERVER: 172.16.0.11#53(172.16.0.11)
;; WHEN: Ср май 06 10:47:20 MSK 2020
;; MSG SIZE  rcvd: 112
```

Присоединение к домену IPA с помощью утилиты join-to-domain

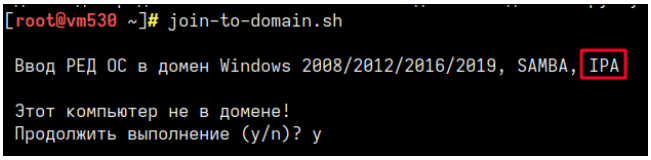
Откройте главное меню - «**Системные**» - «**Ввод ПК в домен**». Выберите «**Домен IPA**».



Заполните все поля:



Кроме графического варианта утилитой **join-to-domain** можно воспользоваться в терминале.



На следующем шаге нужно выбрать способ ввода, а именно "**2. Ввод РЕД ОС в домен IPA**"

Далее введите все предлагаемые значения. По окончании ПК будет введен в домен IPA.

Ручная установка IPA клиента и ввод в домен

```
dnf install ipa-client
```

Присоединение клиента к домену IPA

Впишите в команду данные для вашей сети:

```
ipa-client-install --mkhomedir --enable-dns-updates
```

Скрипт установки должен автоматически найти настройки на ipa сервере, вывести их и спросить подтверждение для найденных параметров:

```
Continue to configure the system with these values? [no]:
```

Ответьте **yes**.

Затем введите имя администратора. Можно просто использовать администратора по умолчанию IPA, который был создан при установке сервера:

```
User authorized to enroll computers: admin
```

Введите пароль администратора IPA, который был установлен во время настройки сервера IPA.

После этого клиент IPA подготовит систему.

Если установка прошла успешно, в конце вывода вы увидите:

```
Client configuration complete.
The ipa-client-install command was successful
```

После этого хост должен появиться в веб-интерфейсе ipa сервера.

Интеграция файлового сервера SAMBA с IPA

Установка необходимых пакетов на сервере SAMBA
Настройка серверов IPA и Samba
Настройка сетевого каталога на сервере Samba

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: ipa-client-4.10.1-2, samba-4.17.5-2h

Установка необходимых пакетов на сервере SAMBA

Для установки пакетов **samba** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ipa-client sssd-libwbclient samba samba-client ipa-client-samba
```

Установите имя хоста samba-сервера:

```
hostnamectl set-hostname samba.redosipa.ru
```

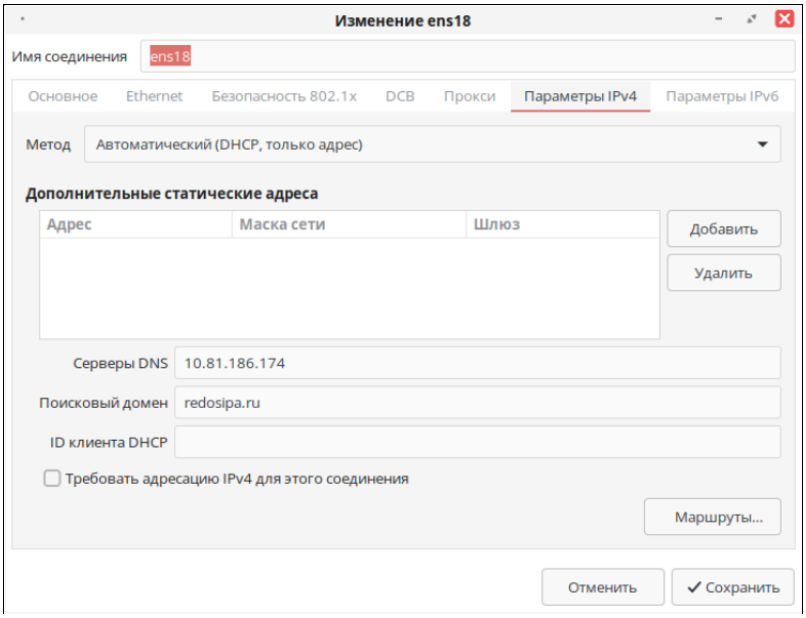
Добавьте запись в **/etc/hosts**, по какому IP обращаться к домену IPA, например:

```
10.81.186.174 server.redosipa.ru
```

Отключите службу:

```
systemctl disable --now systemd-timesyncd
```

В сетевых настройках укажите поисковый DNS IPA-сервера, например:



Присоедините файловый сервер к домену IPA:

```
join-to-domain.sh
```

Выполните автоматическую конфигурацию системных служб на сервере **samba** для работы в домене IPA:

```
authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

Настройка серверов IPA и Samba

Для правильного распределения DNS выполните следующие команды на сервере IPA:

```
kinit admin
ipa dnsrecord-add redosipa.ru --a-rec=samba --a-ip-address=10.81.186.124
```

Запустите настройку домена для обработки классов и атрибутов объектов, специфичных для **Samba**:

```
ipa-adtrust-install --add-sids
reboot
```

На сервере **samba** выполните ipa-client-samba, который создаст **cifs** и отредактирует **/etc/samba/smb.conf** для работы *samba* с **ipa**:

```
ipa-client-samba
```

Отредактируйте в файле **/etc/samba/smb.conf** значение netbios name, указав рабочую группу домена, в данном случае **smb.conf** будет выглядеть следующим образом:

```
...
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 ...
```

Далее отредактируйте секции по примеру из **smb.conf**:

```
[global]
 max smbd processes = 1000
 dedicated keytab file = FILE:/etc/samba/samba.keytab
 kerberos method = dedicated keytab
 log file = /var/log/samba/log.%m
 log level = 1
 server role = member server
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 idmap config * : range = 0 - 0
 idmap config * : backend = tdb


 idmap config REDOSIPA : range = 14000000 - 14199999
 idmap config REDOSIPA : backend = sss

 security = ads
 printing = cups
 printcap name = cups
 load printers = yes
 cups options = raw

 [homes]
 read only = no
 comment = Home Directories
 valid users = %S, %D%w%S
 browseable = No
 read only = No
 inherit acls = Yes
```

```
[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775
```

Создайте структуру ролей и привилегий для **samba**. Действия выполняются на контроллере домена **ipa**:

```
ipa permission-add "CIFS server can read user passwords" --attrs={ipaNTHash,ipaNTSecurityIdentifier} --type=user --right=
{read,search,compare} --bindtype=permission
ipa privilege-add "CIFS server privilege"
ipa privilege-add-permission "CIFS server privilege" --permission="CIFS server can read user passwords"
ipa role-add "CIFS server"
ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
ipa role-add-member "CIFS server" --services=cifs/samba.redosipa.ru
```

На samba-сервере внесите изменения в **/etc/krb5.conf**:

```
sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

Получите тикет и создайте **keytab**:

```
kinit admin
ipa-getkeytab -s server.redosipa.ru -p cifs/samba.redosipa.ru -k /etc/samba/samba.keytab
reboot
```

Настройка сетевого каталога на сервере Samba

На samba-сервере создайте каталог:

```
mkdir -p /share/
```

Назначьте права на созданный каталог:

```
chown -R :users /share
chmod -R 777 /share
setfacl -m default:user:"admin":rwx /share
setfacl -R -m default:user:"admin":rwx /share
```

Затем настройте метки SELinux:

```
semanage fcontext -a -t samba_share_t /share/
restorecon -R -v /share/
```

На контроллере домена **IPA** получите SID:

```
net getdomainsid
```

На файловом сервере **samba** настройте идентификатор безопасности (введите SID, полученный ранее):

```
 net setdomainsid <SID>
```

На сервере **samba** выполните:

```
net -s /dev/null groupmap add sid=S-1-5-32-546 unixgroup=nobody type=builtin
```

В **/etc/samba/smb.conf** укажите настройки для каталога:

```
[share]
 path = /share
 writable = yes
 browsable=yes
 valid users = admin
 read list = admin
 write list = admin
 guest ok = no
 inherit acls = Yes
 create mask = 0660
 directory mask = 0770
```

Добавьте в автозапуск службы **samba** и **winbind**, перезагрузите сервер **samba**:

```
systemctl enable smb winbind --now
reboot
```

Для проверки доступности сетевого каталога на сервере **samba** необходимо получить тикет (если он отсутствует) и выполнить команду подключения к сетевому каталогу:

```
kinit admin
smbclient //samba.redosipa.ru/share -N --kerberos=required
```

В случае, если все настроено верно, появится следующее сообщение:

```
Try "help" to get a list of possible commands.
 smb: \>
```

Основные понятия

Общие сведения о Samba

Данный продукт представляет собой комплект серверного и клиентского программного обеспечения для осуществления связи UNIX-машин с сетями **Microsoft** и **LanManager**, которые сами по себе представляют собой подклассы сетей **SMB**.

Samba использует протокол «**NetBIOS over TCP/IP**», что позволяет ей успешно взаимодействовать с такими реализациями **SMB**, как входящие в OS/2 3-4, Windows 9X-ME, NT3.5-4/2000/XP/Vista/7, UNIX-системами с Samba и, возможно, другими подобными. Samba не может работать без использования **TCP/IP** (на NetBIOS и NetBEUI). Об этом не стоит забывать при проектировании сетей.

Для работы в сетях SMB необходимы:

- клиент;
- сервер;
- средства администрирования.

Все это есть в пакетах **samba-client**, **samba-client-cups**, **samba-common**, **samba, samba-swat**, входящих в состав дистрибутива.

При использовании **SMB** доступны следующие ресурсы:

- сетевые диски;
- прямые пути к дискам;
- принтеры;
- доменная авторизация и управление.

Первые три пункта поддерживаются **Samba** в полном объеме, последний - частично, но это направление стремительно развивается и весьма полно реализовано в **Samba**, описанной ниже.

Также доступен весьма объемный комплект документации в пакете **samba-doc**; большинство ссылок данного раздела будут указывать именно на содержимое этого пакета.

Краткий обзор каталогов и файлов

Все файлы конфигурации и авторизации **Samba** расположены в каталоге **/etc/samba** и его подкаталогах. Рассмотрим их несколько подробнее.

Файл конфигурации	**Описание файла конфигурации**
MACHINE.SID	Системный идентификатор машины, формируется автоматически при старте сервера и предназначен для идентификации компьютера в домене сети Microsoft.
codepages/	Каталог, содержащий файлы с таблицами перекодировки.
Lmhosts	То же, что и **/etc/hosts**, но он предназначен для преобразования **IP<=>NetBIOS**. Как правило, содержит только одну запись: **127.1.0.1 localhost**, но туда можно заносить хосты из других подсетей (когда по ряду причин невозможно надежно провести преобразование **IP<=>NetBIOS** ни широковещательными запросами, ни с использованием **WINS**) или наоборот - ключевые сервера собственного домена.
secrets.tdb	Ключевой файл для идентификации машины в домене сети Microsoft. С точки зрения безопасности имеет ту же ценность, что и файлы **/etc/tcb/*/shadow** - а потому права доступа должны быть **root.root 0600**.
smb.conf	Основной конфигурационный файл **Samba**. Он нужен не только серверной части, но и всем остальным компонентам этой системы.
Smbpasswd	Аналог **/etc/passwd** и **/etc/tcb/*/shadow** - файл пользователей сервера **Samba** с паролями. С точки зрения безопасности имеет ту же ценность, что и **/etc/tcb/*/shadow** - а потому права доступа должны быть **root.root 0600**. Соответствие пользователей **Samba** и системных производится на основе общего **UID**; данный файл используется **Samba** при отсутствии данных о пользователе на **PDC** или при отсутствии самого **PDC**.
Smbusers	Файл соответствий имен сетевых и локальных пользователей **SMB**; это удобный метод для организации административных и гостевых входов на сервер. Соответствие пользователей **Samba** и системных производится на основе символьных имен.
/var/log/samba/*	Лог-файлы серверной части **Samba**. Из них **log.smbd**, **log.nmbd**, **log.winbind** - журналы соответствующих процессов, а все прочие - логи взаимодействия сервера с отдельными клиентскими хостами в формате именования по умолчанию **log.<Client_NetBIOS_NAME>**. При превышении заданного в smb.conf предела производится ротация логов и формируются файлы ***.old**.
/var/spool/samba	Каталог динамического спулинга печати сервера **Samba**. На не сильно загруженных серверах печати он обычно пуст; наличие там множества файлов в то время, когда ни один из клиентов не печатает - явный признак сбоев сервера печати.
/var/cache/samba/*	Файлы (как правило, двоичные базы данных), формируемые в процессе работы различных компонентов **Samba**.

Наиболее примечательны:

Файл конфигурации	Описание файла конфигурации
browse.dat и wins.dat	текстовые файлы, их названия говорят сами за себя;
winbindd*.tdb	базы данных доменных пользователей, формируемых **winbind**. Время от времени их необходимо архивировать: если при апгрейде, «переезде» или переустановке сервера **winbind** сгенерирует эти файлы с нуля, то соответствия системных и доменных символьных и числовых имен изменятся, и права доступа на восстановленные из архива файлы окажутся заведомо перепутанными. Поэтому настоятельно рекомендуется архивировать файлы **/var/cache/samba/winbindd*.tdb**;
/var/lib/samba/	служебные каталоги для администратора сервера.

Список выполняемых файлов **Samba** можно получить командой:

```
rpm -qa | grep samba | xargs rpm -ql | grep bin/
```

и подробно ознакомиться с каждым, прочитав соответствующие разделы документации.

Далее описаны самые важные и наиболее часто используемые компоненты.

Серверные компоненты:

Компонента	Описание компоненты
/usr/sbin/nmbd	сервер преобразования имен и адресов;
/usr/sbin/smbd	файловый сервер;
/usr/sbin/winbindd	сервер импорта пользователей и групп с PDC;
/usr/sbin/swat	средство конфигурирования Samba с web-интерфейсом;
/etc/init.d/smb и /etc/init.d/winbind	управляющие скрипты инициализации сервисов.

Следует отметить, что у скрипта **/etc/init.d/smb** есть два режима рестарта - **restart** и **reload**, которые радикально отличаются следующими особенностями.

restart производит полный рестарт процессов **smbd** и **nmbd** со сбросом текущих соединений. Как правило, клиенты сами производят автоматический реконнект к ресурсам, однако если в момент рестарта были открыты файлы, то возможны проблемы с клиентскими приложениями (например, MS Office и 1С).

reload заставляет **smbd** и **nmbd** только лишь перечитывать файлы конфигурации без рестарта и сброса соединений. При этом старые соединения продолжают существовать по старым правилам, а ко всем новым соединениям будут применены уже новые правила на основании файлов конфигурации.

Клиентские компоненты:

Компонента	Описание компоненты
/usr/bin/smbclient	интерактивное приложение для просмотра сетевых ресурсов;
/sbin/mount.smb, /sbin/mount.smbfs, /usr/bin/smbumount, /usr/sbin/smbmnt, /usr/bin/smbmount	средства монтирования/размонтирования сетевых файловых систем.

Утилиты:

Утилита	Описание утилиты
/usr/bin/smbpasswd	Управление пользователями и подключением к домену;
/usr/bin/wbinfo	Отображение списка пользователей, импортированных **winbindd**;
/usr/bin/testparm	Проверка синтаксиса конфигурационных файлов;
/usr/bin/smbstatus	Отображение статуса процессов **smbd** и **nmbd**;
/usr/bin/nmblookup	Программа разрешения имен **WINS** (аналог **nslookup** для DNS).

Настройка

В большинстве случаев настройка **Samba** заключается в редактировании основного конфигурационного файла **/etc/samba/smb.conf** и управлении пользователями с помощью **smbpasswd**.

Обычный сервер:

Под таковым понимается компьютер, предоставляющий в сеть файловые ресурсы. Фактически это простейший независимый файловый сервер, имеющий собственную базу авторизации пользователей.

Для того чтобы создать такой сервер, необходимо лишь немного подправить стандартный конфигурационный файл **smb.conf** (подставить требуемые имя рабочей группы и имена ресурсов) и создать учетные записи пользователей, как описано ниже, а также учесть рекомендации по безопасности, изложенные в конце раздела.

Вот основные записи в **smb.conf**, которые создадут нам «обычный сервер».

```
[global]
```

Секция [**global**] определяет общие настройки серверной части **Samba** в целом для всех ресурсов.

Имя рабочей группы:

```
OFFICE workgroup = OFFICE
```

Уровень определения прав доступа на уровне пользователей:

```
security = user
```

Приоритет данного сервера среди других компьютеров рабочей группы: определяет, кто именно будет главной машиной, отвечающей за отображение ресурсов сети.

Для сравнения, у **Win9X os level = 34**, а у **NT4 os level = 64**.

```
os level = 65
```

Очевидно, что раз нет домена - нет и мастера.

```
domain master = no
```

Не стоит становиться сервером паролей для окрестных машин.

```
domain logons = no
```

Обычно в простейшей сети **WINS** не нужен, мы его отключаем и у себя тоже.

```
wins support = no
```

Далее надо определить, какие именно каталоги предоставим в сеть. Для каждого ресурса существует отдельная секция.

Самый простейший вариант для обычных ресурсов - обычный каталог с именем **public**:

Имя ресурса, видимое в сети

```
[public]
```

Комментарий, видимый в сети как комментарий к ресурсу:

```
comment = Public Stuff
```

Путь к каталогу ресурса:

```
path = /home/samba/public
```

Отметка о доступе на чтение всем авторизованным пользователям (в том числе и гостевым, если они определены):

```
public = yes
```

Запрет работы на запись всем пользователям:

```
writable = no
```

Разрешение работы на запись всем пользователям, входящим в системную группу **staff**:

```
write list = @staff
```

Подобным образом можно создать различные сетевые ресурсы сервера с различными правами доступа.

Поскольку **Samba** исполняется не в **chroot**, внутри ресурсов можно использовать любые символические ссылки на расположенные локально и в сети (NFS, SMB, Coda и т.д.) файловые обьекты, что очень удобно в плане администрирования системы.

Особые ресурсы - например, домашние каталоги пользователей:

имя ресурса, которое автоматически будет заменено именем домашнего каталога пользователя, под которым подключился клиент и именно название его домашнего каталога будет отображено в сети как имя ресурса. Для получения доступа к этому ресурсу клиент должен предоставить серверу соответствующие имя и пароль, все прочие пользователи к этому ресурсу доступа не имеют вовсе.

```
[homes]
```

Комментарий, видимый в сети как комментарий к ресурсу:

```
comment = Home Directories
```

Признак невидимости - данный ресурс виден в сети только тому пользователю, который является его владельцем. К этому ресурсу можно обратиться непосредственно задав его имя, но в браузинге сети он будет виден только владельцу:

```
browseable = no
```

Разрешение на запись:

```
writable = yes
```

Принтеры:

Имя ресурса, которое будет видно в сети. Кроме него, в сети будут также видны и локальные принтеры под теми же именами, что и в системе по команде **lpq**.

```
[printers]
```

Комментарий, который игнорируется:

```
comment = All Printers
```

Путь к каталогу, в котором располагается спул принтеров, предоставляемых в сеть через **Samba**:

```
path = /var/spool/samba
```

Невидимость ресурса в браузинге, он подменяется системным ресурсом:

```
browseable = no
```

Разрешение на печать для гостевого захода:

```
guest ok = yes
```

Запрещение на запись, поскольку в спул пишет сама **Samba**, а не пользователь.

```
writable = no
```

Признак того, что это именно принтер, а не файловый ресурс:

```
printable = yes
```

Маска для создания файлов заданий на печать:

```
create mode = 0700
```

Команды, выполняемые **Samba** для того, чтобы напечатать документ.

Использование драйвера клиента, применяется для не-UNIX клиентов.

```
print command = lpr-cups -P %p -o raw %s -r
```

Использование драйвера **CUPS** на стороне сервера (на стороне клиентов используется generic **PostScript** драйвер):

```
; print command = lpr-cups -P %p %s
```

Следующие команды являются стандартными при установке **printing=cups**, их можно изменить в случае необходимости.

```
lpq command = lpq -P %p lprm command = cancel %p-%j
```

Сервер в составе существующего домена NT

Подключите вновь созданную машину **Samba** с именем **COMP** к существующему домену **DOM**, администратором которого является пользователь **Administrator** и **PDC** этого домена реализован на другом компьютере.

Первым делом необходимо убедиться, что машины с таким же именем, как и та, которую вы собираетесь подключить, в домене еще нет. В противном случае эту машину необходимо удалить из состава домена средствами самого **PDC** или выбрать другое имя.

На машине **COMP** в **/etc/samba/smb.conf** необходимо внести следующие изменения:

[global]

```
workgroup = DOM
netbios name = COMP
security = domain
password server = *
allow trusted domains = yes
nt acl support = yes
```

После чего необходимо остановить Samba-сервер, если он работает, командой:

```
service smb stop
```

Теперь необходимо послать запрос на **PDC** с целью авторизации нового члена домена с помощью следующей команды:

```
smbpasswd -j DOM -r DOMPDC -U Administrator
```

и в ответ на запрос ввести пароль пользователя **Administrator** - тот самый, с которым этот пользователь зарегистрирован в домене.

Если получено сообщение:

```
Joined domain DOM.
```

все работает; иначе в **smb.conf** надо написать:

```
[global] log level = 4,
```

повторить последнюю команду и по подробным логам разбираться, что не так. При таком уровне **log level** в **log.smbd** содержится подробный отчет об обмене с **PDC**. Вполне возможно, что были допущены ошибки в написании имен или ошибочно введен пароль; также возможны какие-либо неполадки на стороне **PDC**.

С этого момента, когда к **Samba** обратился пользователь «*user123*» с паролем «*passw*», она:

Сначала ищет его в **/etc/samba/smbpasswd**, если пароль и имя совпадают - пускает, иначе отказывает в авторизации или считает гостем (в зависимости от настройки);

- если такого имени в упомянутом файле нет - смотрит в **/etc/passwd** (проверив соответствия через файл **/etc/samba/smbusers**) и если такой пользователь есть - спрашивает **PDC**, числится ли за пользователем «*user123*» полученный пароль «*passw*»;
- если это так - пускает, иначе отказывает в авторизации либо переключает на гостевой заход, в соответствии с настройкой.

Обычно при работе в домене на рядовых рабочих станциях **/etc/samba/smbpasswd** должен быть абсолютно пустым либо содержать только административные учетные записи, с доменом никак не связанные.

Данная логика работы применима только в том случае, если не используется **winbind**. Для того, чтобы доменные пользователи автоматически оказывались в **/etc/passwd** при первом же удачном обращении (правильность паролей была подтверждена PDC), в **/etc/samba/smb.conf** необходимо написать одну строку:

[global]

```
add user script = /usr/sbin/useradd -d /home/domain/%u -g 600 -m -k /etc/skel_domain -s /bin/false %u
```

соответственно каталоги **/home/domain** и **/etc/skel_domain**, а также группа 600 должны уже существовать. Все конкретные имена и опции **useradd** можно менять в зависимости от конкретных применений.

По директиве **add user script**, которая активизируется в тех случаях, когда пользователь еще не зарегистрирован на данной машине, можно вызывать не только **/usr/sbin/useradd** с ключами, но и любые другие программы.

При этом не стоит забывать и о безопасности - программы, запущенные при помощи **add user script**, будут выполняться от всемогущего в пределах системы пользователя root, а параметры их вызова частично определяются пользователем, что потенциально опасно!

Теперь можно включить сервер **Samba** командой:

```
service smb start
```

и работать в домене сети Windows на правах рядового члена домена.

Сервер как PDC домена

Для создания **Primary Domain Controller** (PDC) необходимо в **smb.conf** внести/изменить следующие записи

[global]

Имя сервера, если данный параметр не определен, то он примет значение, соответствующее имени хоста:

```
netbios name = COOLSERVER
```

Имя домена:

```
workgroup = COOLDOMAIN
```

Режим работы системы авторизации сервера:

```
security = user
```

Разрешение на использование шифрованных паролей:

```
encrypt passwords = yes
```

Путь к локальному файлу паролей:

```
smb passwd file = /etc/samba/smbpasswd
```

Стать мастер-браузером для домена:

```
local master = yes
```

Быть PDC:

```
domain master = yes
```

Сразу при старте постараться стать мастер-браузером домена:

```
preferred master = yes
```

Быть сервером паролей домена:

```
domain logons = yes
```

Расположение профайла пользователей домена:

```
logon path = \\%L\Profiles\%U
```

Административная группа домена, присутствие в списке пользователя **administrator** весьма желательно, без этого данный пользователь не получит административных прав на клиентских машинах Windows:

```
domain admin group = root @wheel administrator
```

Быть WINS-сервером. WINS-сервер имеет смысл когда в сети более 10 машин, работающих по протоколу **SMB**. Наличие такого сервера в сложных сетях существенно снижает широковещательный трафик:

```
wins support = yes
```

Порядок разрешения имен **NetBIOS**, по аналогии с записью в **/etc/host.conf** для разрешения имен **DNS**. Значение wins имеет смысл только при наличии в сети wins-сервера, в противном случае оно замедлит работу:

```
name resolve order = wins lmhosts bcast
```

Также необходимо создать ресурсы для работы домена.

Ресурс **netlogon** необходим для работы **PDC** и домена в целом. Он просто должен существовать.

[netlogon]

```
comment = Network Logon Service
path = /var/lib/samba/netlogon
guest ok = yes
writable = no
write list = admin, administrator
```

Данный ресурс необходим для создания и хранения профайлов пользователей домена:

[Profiles]

```
path = /var/lib/samba/profiles
browseable = no
read only = no
create mask = 0600
directory mask = 0700
```

При создании пользователя домена в **/var/lib/samba/profiles** автоматически создается каталог с именем, идентичным имени создаваемого пользователя и принадлежащий ему (с правами 0700). В этом каталоге будут храниться личные настройки пользователя.

Для того чтобы включить клиентскую машину в домен, необходимо произвести следующие действия:

Первый метод - вручную.

Прежде всего, необходимо создать локального пользователя системы с именем, соответствующим NetBIOS-name подключаемой к домену машины. К имени на конце добавляется символ ''**$**''. Для добавления машины с именем **machine_name** необходимо от имени пользователя **root** выполнить следующие команды:

```
/usr/sbin/useradd -g machines -d /dev/null -c "machine nickname" -s /bin/false machine_name$
passwd -l machine_named$
```

Теперь, когда создан пользователь (символ ''**$**'' в конце имени означает что это NetBIOS-имя компьютера, а не имя пользователя), можно добавить его в домен, выполнив от имени **root** команду:

```
smbpasswd -a -m machine_name
```

Теперь компьютер подключен к домену.

Второй метод - автоматический.

Работу по созданию машинного акаунта можно переложить на Samba, включив в **smb.conf** следующую запись:

[global]

```
add user script = /usr/sbin/useradd -d /dev/null -g machines -s /bin/false -M %u
```

Теперь **Samba** будет принимать от клиентских машин запросы на включение в домен и автоматически регистрировать их аналогично **NT Server.**

С этого момента начинает существовать домен и PDC на базе Samba-сервера. Пользователи могут входить под своими именами и паролями с любой машины домена с сохранением настроек, а также самостоятельно менять свои пользовательские пароли без помощи администратора сети.

Учетные записи пользователей

Все учетные записи хранятся в файле /etc/samba/smbpasswd.

Учетные записи пользователей, используемые Samba, делятся на две категории:

- записи о компьютерах, входящих в домен;
- записи о пользователях, зарегистрированных на данном сервере.

Следует учитывать, что для того, чтобы создать и использовать любую учетную запись в **/etc/samba/smbpasswd**, предварительно необходимо создать соответствующую запись в **/etc/passwd**. Общее правило - для каждого пользователя в **/etc/samba/smbpasswd** обязательно должен существовать пользователь в **/etc/passwd**. Обратное утверждение неверно.

Для управления учетными записями предназначена утилита **smbpasswd**; полный список ее возможностей можно узнать из соответствующей man-страницы, здесь же рассмотрим наиболее частые методы использования.

Создание нового пользователя:

```
smbpasswd -a <User_name>
```

Смена пароля у существующего пользователя:

```
smbpasswd <User_name>
```

Удаление существующего пользователя:

```
smbpasswd -x <User_name>
```

Приостановление учетной записи без удаления:

```
smbpasswd -d <User_name>
```

Подключение данного компьютера к существующему домену:

```
smbpasswd -j <Domain_name> -U <Administrator_name>
```

Использование winbind

Сервис **winbind** является новым средством, предназначенным для более полной интеграции Samba в домены Windows; он появился, начиная с **Samba 2.2.0**. Данный сервис считывает свою конфигурацию из **/etc/samba/smb.conf** и динамически взаимодействует с PDC домена, автоматически синхронизируя списки пользователей и групп домена и машины **Samba**. Таким образом, **winbind** является весьма удобным средством для автоматического поддержания актуальности базы пользователей домена на рабочих станциях **Samba**.

Работа данного сервиса происходит без изменения содержимого каких-либо авторизационных файлов в **/etc** и при перезагрузке машины доменные пользователи появляются в системе только после запуска **winbindd**. Если во время работы остановить **winbindd**, то доменные пользователи и группы не исчезнут из системы до перезагрузки, однако динамического обновления списков имен и паролей происходить не будет.

Для того чтобы при рестарте компьютера (или только сервиса winbindd) не нарушались соответствия внутренних **UID** и доменных **SID**, он сохраняет текущее состояние списков в файлах **/var/cache/samba/winbindd*.tdb**.

Для нормального функционирования winbindd в файле /etc/samba/smb.conf обязательно должны быть обьявлены следующие директивы:

[global]

Диапазон номеров локальных пользователей, который будет использован для динамического создания пользователей домена:

```
winbind uid = 10000-20000
```

Диапазон номеров локальных групп пользователей, который будет использован для динамического создания групп пользователей домена:

```
winbind gid = 10000-20000
```

Символ-разделитель, используемый для составления доменных имен пользователей и располагающийся между именем домена и именем пользователя:

```
winbind separator = +
```

Интервал времени (в секундах) между запросами **winbind** к PDC в целях синхронизации списков пользователей и групп:

```
winbind cache time = 10
```

Шаблон имени домашних каталогов доменных пользователей, автоматически присваиваемых каждому пользователю. Сами каталоги, однако, динамически не создаются. Вместо переменой **%D** подставляется имя домена, а вместо **%U** подставляется имя пользователя:

```
template homedir = /home/%D/%U
```

Командный интерпретатор, назначаемый по умолчанию для пользователей, авторизованных через **winbindd**.

```
template shell = /bin/bash
```

Также необходимо внести изменения в файле **/etc/nsswich.conf** в разделы **passwd** и **group**, вписав директиву **winbind** - например, таким образом:

```
passwd: files winbind
group: files winbind
```

С этого момента можно использовать имена доменных пользователей в **/etc/samba/smb.conf** с целью разграничения доступа, в правах на файлы и каталоги, для подключения к сетевым ресурсам данного хоста со стороны других хостов.

Обычный клиент

Клиентские функции **Samba** представлены средствами просмотра сетевого окружения и монтирования файловых систем **/usr/bin/smbclient** и **/usr/bin/smbmount** соответственно. Также доступны **mount.smb** и **mount.smbfs**, являющиеся символическими ссылками на **/usr/bin/smbount**.

При запуске эти программы считывают текущую конфигурацию из файла **/etc/samba/smb.conf** и используют доменные функции в случае, если машина подключена к домену Windows.

Также файловые системы возможно монтировать системной командой mount, указав в качестве типа файловой системы **smbfs**, и использовать эти записи в /etc/fstab для автоматического монтирования при загрузке системы.

Например, для того что бы смонтировать в каталог **/mnt/disk** ресурс **public** с машины **SMALLSERVER** под именем **cooluser**, нужно выполнить команду:

```
smbmount //smallserver/public /mnt/disk -o username=cooluser
```

Регистр написания имен компьютеров, ресурсов и пользователей роли не играет. Для того, что бы получить список Samba-ресурсов данной машины и список машин рабочей группы или домена достаточно выполнить команду:

```
#smbclient -L localhost -N
```

Более подробные сведения можно прочесть в man-страницах по **smbclient** и **smbmount**.

Клиент в составе существующего домена NT

Подключение происходит аналогично рассмотренному подключению сервера в составе существующего домена NT. Далее вся работа происходит точно так же, как описано в предыдущем пункте.

Принт-сервер на CUPS

По умолчанию **Samba** сконфигурирована на использование **CUPS** в качестве спулера печати. Подразумевается, что **CUPS** уже настроен и запущен. В **/etc/samba/smb.conf** присутствуют следующие директивы:

[global]

```
printcap name = lpstat
load printers = yes
printing = cups
```

Также необходимо создать ресурс [**printers**] - его создание и назначение директив подробно описано в подпункте «**Обычный сервер**» в части «**Особые ресурсы**».

Особенности локализации клиента и сервера

Для того, чтобы все компоненты **Samba** правильно работали с русскими именами файловых объектов и ресурсов, в **/etc/samba/smb.conf** необходимо добавить следующие директивы:

[global]

```
client code page =
character set =
```

Далее приводятся наборы значений этих директив и системных кодировок, наиболее часто используемых в России, Белоруссии и на Украине:

```
$LANG = ru_RU.KOI8-R
client code page = 866
character set = koi8-r
$LANG = ru_RU.CP2151 client code page = 866 character set = 1251
$LANG = be_BY.CP1251 client code page = 866 character set = 1251
$LANG = uk_UA.KOI8-U client code page = 1125 character set = koi8-u
$LANG = uk_UA.CP1251 client code page = 1125 character set = 1251U
$LANG = ru_UA.CP1251 client code page = 1125 character set = 1251U
```

В двух последних случаях **1251U** - специальное обозначение внутри **Samba** для комбинации «**локально 1251 - удаленно 1125**». В **Samba** определение удаленной кодировки делается по имени локальной.

Также необходимо проследить, чтобы на тех компьютерах Windows, с которыми предполагается взаимодействие через **Samba**, были установлены соответствующие системные настройки локализации. В противном случае велика вероятность, что вместо кириллических символов будут отображены знаки ''**?**'' либо другие символы.

Указанные директивы **/etc/samba/smb.conf** воздействуют на работу всех компонентов **Samba** - и серверных, и клиентских. На данный момент поддерживаются кириллические написания имен - файлов, каталогов и ресурсов.

Некоторые вопросы безопасности

Данный раздел относится в основном к серверной части **Samba**.

Прежде всего необходимо определить, какие интерфейсы должны прослушиваться **Samba** в ожидании запроса на соединение (по умолчанию прослушиваются все имеющиеся в системе).

Например, для того чтобы ограничить прослушивание локальным хостом и первой сетевой картой, необходимо написать в **/etc/samba/smb.conf**:

[global]

```
interfaces = 127.0.0.1 eth0
bind interfaces only = Yes
```

Далее можно ограничить диапазоны адресов, с которых позволительно обращаться к данному серверу. Действие данных директив аналогично воздействию **/etc/hosts.allow** и **/etc/hosts.deny** на **xinetd** и **ssh**: если IP-адрес хоста не подпадает под разрешающее правило, то соединение не будет установлено вовсе. Для того, что бы ограничить доступ двумя подсетями и локальной системой, дополнительно исключив при этом один хост, можно написать:

[global]

```
hosts allow = 192.168.1. 192.168.2. 127.
hosts deny = 192.168.1.12
```

Все вышеперечисленные директивы ограничивают соединения на уровне интерфейсов и IP-адресов до какой либо авторизации.

Следующие директивы управляют режимом авторизации пользователей.

Во избежание перехвата чувствительных данных при передаче их по сети открытым текстом принято шифровать пароли. **Samba** и все версии Windows, начиная с версии Win98, по умолчанию используют шифрование паролей. Данная директива включает его в **Samba**:

[global]

```
encrypt passwords = yes
```

Файл переопределений имен пользователей является весьма мощным средством управления пользовательскими акаунтами, однако при неразумном использовании это средство опасно и поэтому по умолчанию отключено. Внимательно ознакомьтесь с содержимым файла **/etc/samba/smbusers** прежде, чем использовать его.

[global]

```
username map = /etc/samba/smbusers
```

Особенности использования samba 3.0

Samba 3.0 имеет заметные отличия от более ранних версий; наиболее выдающимися из них являются улучшенная по сравнению с версией 2.2 поддержка Unicode, поддержка гораздо большего количества кодовых страниц, новая утилита администрирования net, призванная заменить **smbpasswd**.

Задание кодовых страниц

Для задания кодировок используются следующие новые параметры **smb.conf**:

```
unix charset = <charset>
dos charset = <charset>
display charset = <charset>
```

где <**charset**> - любая кодировка, поддерживаемая **iconv**.

Список возможных кодировок можно узнать, выполнив команду:

```
iconv --list
```

Параметры **client code page** и **character set** больше не поддерживаются. Параметр **unix charset** указывает кодировку, в которой будут храниться файлы на диске, в которой заданы параметры в **smb.conf**.

Параметр **dos charset** указывает кодировку, в которой **Samba** будет общаться с клиентами, не поддерживающими **Unicode**. Все версии Windows, начиная с 95, понимают Unicode - но все же стоит установить **dos charset = cp866**, что соответствует **client code page = 866** в более старых версиях.

Параметр **display charset** указывает, в какой кодировке должны выводить информацию программы, непосредственно обменивающиеся информацией с пользователем, например **smbclient**, **net**, **wbinfo** и другие.

Утилита net

Утилита **net** призвана заменить **smbpasswd** и обеспечивает гораздо большие возможности по получению информации о сети и управлению сетью. Формат команд утилиты очень похож на формат одноименной команды Windows NT/2000.

Основные применения команды **net**:

- создание и удаление пользователей: **net user**;
- включение машины в домен: net ads join - Active Directory; **net rpc join - NT Domain**;
- получение информации о домене, машине, открытых файлах, сессиях: **net info**, **net ads status**, **net rpc status**;
- создание и удаление разделяемых ресурсов на удаленных машинах: **net share**;
- синхронизация времени с windows-сервером: **net time**.

Управление машиной с Samba из Microsoft Management Console

Начиная с версии **2.2**, **Samba** имеет возможнось удаленного администрирования из **MMC** (Microsoft Management Console). Эта возможность полезна, когда **Samba** является членом NT-домена или **AD**. Администратор домена может создавать, удалять и изменять

сетевые ресурсы на UNIX-машине с запущенной **Samba**.

Для управления ресурсами служат параметры **/etc/samba/smb.conf**:

[global]

```
add share command = <add script>
```

Параметр указывает скрипт, который будет вызван при попытке создания нового ресурса в **MMC**. Скрипту передается четыре параметра:

- имя конфигурационного файла (например, **/etc/samba/smb.conf**);
- имя создаваемого ресурса;
- путь к существующей директории на диске;
- комментарий.

Скрипт должен завершаться с кодом **0**, в случае успешного создания, и ненулевым - в случае ошибки.

```
change share command = <change script>
```

Параметр указывает скрипт, который будет вызван при попытке изменения существующего ресурса в MMC. Скрипту передается четыре параметра:

- имя конфигурационного файла (например, **/etc/samba/smb.conf**);
- имя создаваемого ресурса;
- путь к существующей директории на диске;
- комментарий.

Скрипт должен завершаться с кодом **0**, в случае успешного создания, и ненулевым - в случае ошибки.

```
delete share command = <delete script>
```

Параметр указывает скрипт, который будет вызван при попытке удаления существующего ресурса в MMC (Stop sharing). Скрипту передается два параметра:

- имя конфигурационного файла (например **/etc/samba/smb.conf**);
- имя создаваемого ресурса.

Скрипт должен завершаться с кодом **0**, в случае успешного создания, и ненулевым - в случае ошибки.

Чтобы скрипты могли изменять конфигурационные файлы **Samba**, они должны выполняться с правами **root**. Для этого нужно установить отображение пользователей домена, имеющих право изменять ресурсы, в **root**. Это можно сделать либо с помощью файла **/etc/samba/smbusers**, прописав там строку вида:

```
root = administrator <user 1> ... <user n>
```

либо с помощью параметра **admin users** в **/etc/samba/smb.conf**:

```
admin users = administrator
```

При создании нового ресурса Windows позволяет просматривать дерево директорий. Для этого в **/etc/samba/smb.conf** нужно задать служебные ресурсы, заканчивающиеся символом `'$'`, например:

```
[C$]
path = /drives/c
```

После этого при создании нового ресурса можно будет просматривать и выбирать все директории ниже **/drives/c**.

Работа в среде Active Directory

Для объединения компьютеров в домены Widows 2000 Server использует схему, отличную от NT- доменов, которая называется Active Directory; эта схема обладает гораздо большей масштабируемостью и позволяет централизованно администрировать машины, входящие в домен. Active Directory базируется на протоколе авторизации Kerberos, при котором имя пользователя и пароль не передаются по сети, а используется механизм так называемых билетов, выдаваемых сервером на определенное время. Получив билет, машина, входящая в домен, может авторизоваться на других машинах домена без участия сервера.

Установка Samba

Samba 3.0, в отличие от более ранних версий Samba, имеет возможность работать в сетях Wndows, работающих в режиме Active Directory (или Windows 2000 native mode). Если требуется эта функциональность, следует установить **samba3 samba2**.

Active Directory имеет другую схему именования доменов, компьютеров и пользователей, основанную на DNS. Допустим, существует сеть с именем **my.firm.com** и компьютерами **host1.my.firm.com**, **host2.my.firm.com**, **host3.my.firm.com**; тогда домен Active Directory будет называться **my.firm.com**, а пользователи Active Directory будут иметь имена вида user@my.firm.com.

Настройка

/etc/krb5.conf должен содержать, по крайней мере, следующие строки:

[realms]

```
MY.FIRM.COM = {
kdc = your.kerberos.server
}
```

г д е **MY.FIRM.COM** - имя домена (или «царства», в терминологии Kerberos; задается обязательно в верхнем регистре), а **your.kerberos.server** - имя или IP-адрес KDC (Kerberos Domain Controller), аналог PDC (Primary Domain Controller) в доменах Windows NT - например, **server.my.firm.com** или **192.168.117.11**.

Правильность указания параметров можно проверить, выполнив команду (замените имя пользователя на актуальное - например, administrator@MY.FIRM.COM):

```
kinit username@REALM
```

и убедившись, что пароль был принят сервером. REALM всегда задается в верхнем регистре.

Также нужно убедиться, что возможно получить имя KDC по его IP адресу (так называемый Reverse DNS lookup). Имя KDC должно либо совпадать с NetBIOS-именем компьютера (имя машины в сети Windows без указания домена) либо состоять из NetBIOS-имени и имени домена. Если получить имя KDC по адресу невозможно, вы получите ошибку "**local error**" при попытке войти в домен.

Если DNS не поддерживает Reverse **lookup** либо KDC не зарегистрирован в DNS, вы можете указать соответствие IP-адреса и имени в **/etc/hosts**.

Редактирование /etc/samba/smb.conf:

Для работы в Active Directory smb.conf должен содержать следующие параметры:

```
[global]

# Задаёт Kerberos realm, обычно совпадает с именем домена в
# верхнем регистре, например realm = MY.FIRM.COM
realm = <REALM>

# Это обычно часть реалма до первой точки, например
# workgroup = MY
workgroup = <WORKGROUP>

# Тип домена - Active Directory.
security = ADS

# В случае Active Directory пароли всегда шифруются.
encrypt passwords = true

# Обычно этот параметр указывать не обязательно, т.к. Samba сама
# определяет адрес KDC, если в сети есть WINS-сервер и он указан
# в smb.conf
ads server = <your.kerberos.server>
```

Регистрация компьютера в Active Directory домене

Убедитесь что **Samba** не запущена. Если запущена, ее нужно остановить:

```
service smb stop; service winbind stop
```

Чтобы включить компьютер в домен, выполните команду:

```
net ads join -U administrator
```

где **administrator** - имя пользователя домена, имеющего право создавать новые учетные записи.

Если не было выдано сообщение об ошибке, то машина успешно зарегистрирована в домене - иначе проверьте правильность задания параметров в **/etc/samba/smb.conf** и **/etc/krb5.conf**. Убедитесь, что пользователь, указанный после **-U** в **net ads join**, имеет необходимые права на создание новых учетных записей.

Теперь можно запустить необходимые службы:

```
service smb start; service winbind start
```

Проверка правильной работы в Active Directory

Для работы с компьютерами, зарегистрированными в Active Directory, не требуется указывать имя пользователя и пароль. Попробуйте выполнить команду:

```
smbclient -k -L <имя компьютера в домене>
```

Вы должны получить список доступных ресурсов, при этом **smbclient** не должен запрашивать имя пользователя и пароль.

Чтобы проверить, что доступ к ресурсам вашей машины возможен с других машин домена, вы можете попробовать выполнить все ту же команду:

```
smbclient -k -L <имя вашего компьютера в домене>
```

и получить список доступных ресурсов. Можно также попробовать открыть какой-нибудь ресурс на вашей машине с Windows-машины, входящей в домен. В любом случае, имя пользователя и пароль запрашиваться не должны.

Некоторые особенности работы в Active Directory

В отличие от доменов Windows NT, авторизация в Active Directory производится не по имени и паролю, а с помощью билетов протокола **Kerberos**. Из-за этого работа с **smbclient** может поначалу показаться необычной.

Во-первых, при вызове smbclient нужно указывать опцию **-k**. Во-вторых, билеты **Kerberos** даются на определенное время (обычно на сутки, но это зависит от настроек сервера). Поэтому их нужно периодически обновлять с помощью команды **kinit**:

```
kinit username@realm
```

где **username** - ваше имя в Active Directory домене **REALM**.

Так что если **smbclient** вдруг перестает подключаться к доменным ресурсам, попробуйте обновить билет - скорее всего, дело именно в этом.

Установка сервера SAMBA DC

Предварительная настройка сервера
Обновление пакетов
Установка необходимых пакетов
Отключение SELinux
Присваивание серверу доменного имени
Настройка сетевого интерфейса
Настройка сетевого интерфейса вручную
Настройка сетевого интерфейса с помощью утилиты nmtui
Создание нового домена под управлением контроллера домена Samba DC
Создание резервных копий файлов
Настройка конфигурации Kerberos
Первоначальное полуавтоматическое конфигурирование сервера с помощью утилиты samba-tool
Дополнительная настройка сервера
Запуск и проверка работоспособности службы samba

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: samba-4.17.5-2h, krb5-devel-1.20.1-1

Вы можете подробнее ознакомиться с установкой и настройкой **SAMBA**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка Samba как контроллера домена в РЕД ОС 7.2 ;
- в **Яндекс.Дзен** — Настройка Samba как контроллера домена в РЕД ОС 7.2 .

На наших каналах вы также сможете найти много другой полезной информации.

В обучающем видео рассмотрен пример установки и настройки сервера **SAMBA** на **РЕД ОС 7.2**. В настоящее время актуальной версией ОС является **РЕД ОС 7.3**, в которой используется пакетный менеджер **dnf** вместо **yum**.

Предварительная настройка сервера

Обновление пакетов

Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните обновление всех пакетов:

```
dnf makecache && dnf upgrade
```

Все дальнейшие действия выполняются с правами пользователя **root**, если не указано иное.

Установка необходимых пакетов

Для установки необходимых пакетов выполните:

```
dnf install samba* krb5*
```

Отключение SELinux

На время настройки переведите SELinux в режим уведомлений:

```
setenforce 0
```

Статус службы SELinux можно посмотреть командой **sestatus**.

Замените в файле конфигурации **/etc/selinux/config** режим `enforcing` на `permissive` командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

После перезагрузки системы служба SELinux будет запущена — в режиме, который указан в конфигурационном файле.

Присваивание серверу доменного имени

Сервер контроллера домена должен иметь собственное уникальное доменное имя и статический IP-адрес. Назначьте серверу полное доменное имя: например, если короткое имя сервера **dc1**, то для домена **skynet.murom** полное имя сервера имеет вид **dc1.skynet.murom**:

```
hostnamectl set-hostname dc1.skynet.murom
```

Настройка сетевого интерфейса

По умолчанию сетевой интерфейс настроен для получения IP-адреса по **DHCP**. Нужно установить серверу контроллера домена статический IP-адрес.

Настройку сетевого интерфейса можно выполнить несколькими способами, в данной статье рассматриваются два из них:

- вручную, путём редактирования файла настроек;
- с помощью графической консольной утилиты **nmtui**.

Настройка сетевого интерфейса вручную

Настройки хранятся в файле **/etc/NetworkManager/system-connections/<имя_сетевого_интерфейса>.nmconnection**. Именуются они, например, как **enp0s3** или **enp0s4**.

В данном примере сетевой интерфейс имеет имя **enp0s3**.

Откройте конфигурационный файл в текстовом редакторе:

```
nano /etc/NetworkManager/system-connections/enp0s3.nmconnection
```

Внесите следующие изменения:

1) измените тип соединения на статический:

```
method=manual
```

2) установите значение для игнорирования DNS из DHCP:

```
ignore-auto-dns=true
```

3) укажите IP-адрес контроллера, маску подсети и IP-адрес шлюза:

```
address1=192.168.1.96/24,192.168.1.1
```

4) укажите в качестве *DNS-сервера* IP-адрес создаваемого контроллера домена:

```
dns=192.168.1.96
```

5) впишите домен поиска (в данном примере это `skynet.murom`):

```
dns-search=skynet.murom;
```

Итоговый файл настройки должен иметь вид:

```
[connection]
 id=enp0s3
 uuid=97def639-603a-4167-9613-edd5bd902ef8
```

```
type=ethernet
interface-name=enp0s3
timestamp=1704763284

[ethernet]

[ipv4]
address1=192.168.1.96/24,192.168.1.1
dns=192.168.1.96;
dns-search=skynet.murom;
ignore-auto-dns=true
method=manual

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

Перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Для проверки настроек статической IP-адресации воспользуйтесь командой `ifconfig` или `ip addr`.

Настройка сетевого интерфейса с помощью утилиты nmtui

Запустите утилиту в консоли:

```
nmtui
```

В настройках сетевого интерфейса в конфигурации **IPv4** укажите следующие значения:

- тип конфигурирования – «**Вручную**»;
- IP-адрес создаваемого сервера и маску подсети – **192.168.1.96/24**;
- адрес шлюза – **192.168.1.1**;
- IP-адрес первого DNS-сервера – IP-адрес сервера с доступом к локальному репозиторию или интернету, например **8.8.8.8** (при добавлении контроллера домена РЕД АДМ в существующий домен указать IP-адрес контроллера домена существующего домена);
- IP-адрес второго DNS-сервера – IP-адрес создаваемого контроллера домена, **192.168.1.96**;
- домен поиска – **skynet.murom**.

Перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Проверьте доступные серверы имен, просмотрев файл **resolv.conf**:

```
cat /etc/resolv.conf
```

Вывод команды должен иметь примерно следующий вид:

```
# Generated by NetworkManager
search skynet.murom
nameserver 8.8.8.8
nameserver 192.168.1.96
```

Создание нового домена под управлением контроллера домена Samba DC

Создание резервных копий файлов

Переименуйте файл **/etc/smb.conf**, он будет создан позднее в процессе выполнения команды **samba-tool**. Наличие данного файла на момент запуска полуавтоматической конфигурации может вызвать ошибку.

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Создайте резервную копию используемого по умолчанию конфигурационного файла **kerberos**:

```
cp /etc/krb5.conf /etc/krb5.conf.bak
```

Настройка конфигурации Kerberos

Откройте файл **/etc/krb5.conf**:

```
nano /etc/krb5.conf
```

В секции [libdefaults] установите имя домена, используемое по умолчанию:

```
default_realm = SKYNET.MUROM
```

В ту же секцию добавьте время жизни тикета керберос:

```
ticket_lifetime = 24h
 forwardable = yes
```

Пример листинга конфигурации **krb5.conf**:

```
[libdefaults]
 default_realm = SKYNET.MUROM
 dns_lookup_realm = false
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 forwardable = yes

 [realms]
 SKYNET.MUROM = {
 kdc = dc1.skynet.murom
 admin_server = dc1.skynet.murom
 }

 [domain_realm]
 .skynet.murom = SKYNET.MUROM
 skynet.murom = SKYNET.MUROM
```

Откройте файл **/etc/krb5.conf.d/crypto-policies**:

```
nano /etc/krb5.conf.d/crypto-policies
```

и приведите его содержание к следующему виду:

```
[libdefaults]
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
```

Первоначальное полуавтоматическое конфигурирование сервера с помощью утилиты samba-tool

Конфигурирование в интерактивном режиме выполняется командой:

```
samba-tool domain provision --use-rfc2307 --interactive
```

Описание некоторых опций (параметров) этой команды:

- use-rfc2307 – параметр добавляет POSIX атрибуты (UID / GID) на схеме AD. Он понадобится при аутентификации клиентов Linux, BSD, или OS X (в том числе, на локальной машине), в дополнение к Microsoft Windows;
- interactive – запуск в интерактивном режиме;
- realm – указывает на полное DNS-имя домена, которое настроено в **/etc/hosts**, в верхнем регистре (в рассматриваемом примере это SKYNET.MUROM);
- Domain – краткое имя домена *NetBIOS* (в примере – **SKYNET**);
- Server Rules – роль сервера (например, DC – **domain controller**);
- DNS backend – DNS-сервер. Возможные значения – **SAMBA_INTERNAL** (внутренний DNS сервера), **BIND9_FLATFILE**, **BIND9_DLZ**, **NONE**;
- DNS forwarder IP address – данный параметр позволяет указать IP-адрес DNS-сервера, на который будут перенаправлены DNS-запросы, в том случае, когда сервер не сможет их разрешить.

Более подробная информация доступна в Wiki-справке проекта Samba по адресу https://wiki.samba.org, на странице “**Setting up Samba as an Active Directory Domain Controller**”.

Пример сокращённого листинга настройки для тестового домена **skynet.murom**:

```
Realm [SKYNET.MUROM]:
Domain [SKYNET]:
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.1.96]: 192.168.1.1
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce uniqueness constraint on local domainSIDs
Adding DomainDN: DC=skynet,DC=muromAdding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=skynet,DC=muromCreating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with this one. Do not create a symlink!
Setting up fake yp server settings
Once the above files are installed, your Samba AD server will be ready to use
Server Role: active directory domain controller
Hostname:dc1
NetBIOS Domain:SKYNET
DNS Domain: skynet.murom
```

```
DOMAIN SID:S-1-5-21-4010603892-1310842104-1159347701
```

После запуска автоматической настройки файлы конфигурации будут созданы автоматически.

Дополнительная настройка сервера

Настройки сервера находятся в файле **/etc/samba/smb.conf**. Конфигурирование сервера выполняется путём внесения изменений в этот файл:

```
nano /etc/samba/smb.conf
```

Начиная с версии **3.3.0** в Samba есть модуль **acl_xattr**, который позволяет Samba корректно обрабатывать Windows ACL (Access Control List) и обеспечивает полноценную поддержку прав доступа к файлам.

Для подключения этого модуля добавьте в файл **/etc/samba/smb.conf** в секцию [global] следующие строки (либо отредактируйте существующие):

```
vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
```

Для включения автоматического обновления записей в DNS добавьте следующий параметр в секцию [global]:

```
allow dns updates = nonsecure
```

В секцию [global] добавьте поддержку расширений схемы Samba AD (Active Directory):

```
dsdb:schema update allowed = true
```

Пример содержания файла **/etc/samba/smb.conf** с внесёнными дополнительными изменениями:

```
cat /etc/samba/smb.conf
```

```
#Global parameters
 [global]
 netbios name = DC1
 realm= SKYNET.MUROM
 server role = active directory domain controller
 workgroup= SKYNET
 idmap_ldb:use rfc2307 = yes
 vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 dsdb:schema update allowed = true

 [netlogon]
 path = /var/lib/samba/sysvol/skynet.murom/scripts
 read only = No

 [sysvol]
 path = /var/lib/samba/sysvol
 read only = No
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните проверку:

```
testparm
```

Пример вывода команды:

```
Load smb config files from /etc/samba/smb.conf
vfs objects specified without required AD DC module: dfs_samba4
```

```
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
```

Запуск и проверка работоспособности службы samba

Запустите и добавьте в автозагрузку службу **samba**:

```
systemctl enable samba --now
```

Проверьте статус служб:

```
systemctl status samba
```

> **Примечание.**
>
> Не запускайте службу **winbind** вручную на контроллере домена Samba Active Directory. Служба запускается автоматически как подпроцесс **samba**.

Проверьте работу динамического обновления **DNS**:

```
samba_dnsupdate --verbose --all-names
```

Для более быстрой проверки рекомендуется отключить **IPv6**. Сделать это можно с помощью утилиты **nmtui**.

Администрирование контроллера SAMBA

Средства администрирования удаленного сервера от MS
Подготовка резервного контроллера домена
Добавление резервного контроллера в домен
Установка необходимых пакетов
Присоединение сервера в качестве вторичного контроллера домена
Дополнительная настройка сервера
Запуск служб
Настройка NTP на контроллере домена dc1.skynet.murom
Настройка NTP на резервном контроллере домена dc2.skynet.murom
Настройка двунаправленной репликации sysvol и netlogon с помощью Unison

Средства администрирования удаленного сервера от MS

Введение ПК с Windows в домен Samba производится точно так же, как и ввод компьютера в домен MS AD.

Для администрирования домена Samba установите **RSAT** - https://wiki.samba.org/index.php/Installing_RSAT.

Включите компоненты: «**Установка удаление программ**» - «**Включение отключение компонентов**» - «**Средства удаленного администрирования сервера**».

После настройки перезагрузите ПК.

В управлении DNS подключитесь к **dc1.skynet.murom**, добавьте обратную зону и PTR-запись для контроллера домена **dc1**. Кроме работы с DNS через оснастку Windows существует способ добавления обратной зоны dns с помощью команд в терминале.

Для этого, предварительно, получите kerberos-тикет:

```
kinit administrator@SKYNET.MUROM
```

Добавьте обратную зону:

```
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 1.81.10.in-addr.arpa
samba-tool dns add dc1.skynet.murom 1.81.10.in-addr.arpa 96 PTR dc1.skynet.murom -U administrator
```

в последней команде **96** - это последний октет (четвертый) в IP-адресе (**10.81.1.96**) сервера samba.

Следующие зоны, вероятно, создавать не обязательно, но такие зоны автоматически настроены на Windows srv:

```
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 0.in-addr.arpa
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 127.in-addr.arpa
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 255.in-addr.arpa
```

Подготовка резервного контроллера домена

Настройте сеть, по примеру **DC1**.

Для этого, используйте утилиту «**Сетевые соединения**», расположенную в «**Меню**» → «**Параметры**» → «**Сетевые соединения**» в графическом окружении Cinnamon или «**Система**» → «**Параметры**» → «**Сетевые соединения**» в графическом окружении Mate. Выберите ваше активное подключение, нажмите кнопку «**Изменить**», перейдите на вкладку «**Параметры IPv4**», поменяйте «**Метод**» на «**Вручную**» и укажите IP-адрес, маску и шлюз. В поле «**Серверы DNS**» напишите адрес IP-адрес машины, а в поле «Поисковые **домены**» введите skynet.murom, нажмите применить и перезапустите NetworManager.

Проверьте, что все изменилось, выведя содержимое файла **resolv.conf**:

```
 cat /etc/resolv.conf

nameserver 10.81.1.96
search skynet.murom
```

С помощью **hostnamectl** измените доменное имя машины на **dc2.skynet.murom**:

```
hostnamectl set-hostname dc2.skynet.murom
```

В **/etc/hosts** пропишите:

```
<IP-адрес-сервера-DC2> dc2.skynet.murom dc2
```

Добавление резервного контроллера в домен

Установка необходимых пакетов

Установите необходимые пакеты командой:

```
dnf install samba* krb5*
```

Присоединение сервера в качестве вторичного контроллера домена

Скопируйте конфигурации самбы с основного контроллера **/etc/samba/smb.conf** и **/etc/krb5.conf**.

Измените в **/etc/samba/smb.conf** значение следующего параметра:

```
netbios name=DC2
```

Получите билет:

```
# kinit Administrator
```

и проверьте вывод:

```
# klist
```

Добавьте **winbind** в файл **/etc/nsswitch.conf**.

Winbind будет использоваться как прокси между AD и связкой **PAM** и **NSS**. Для аутентификации AD **winbind** использует **kerberos**, а LDAP используется для получения информации.

```
nano /etc/nsswitch.conf

passwd: winbind sss files systemd
group:  winbind sss files systemd
shadow: winbind files sss
hosts:  files dns wins
```

Выполните команду присоединения к домену в роли "**backend**":

```
samba-tool domain join skynet.murom DC -U Administrator --dns-backend=SAMBA_INTERNAL --realm=skynet.murom
```

Введите пароль от доменного *Администратора контроллера домена*.

При этом в прямой зоне DNS должна появиться соответствующая A-запись.

Дополнительная настройка сервера

Выполните дополнительную настройку сервера аналогично тому, как это сделано в подразделе Дополнительная настройка основного сервера.

Отредактируйте файл **/etc/samba/smb.conf** и добавьте в секцию [global] следующие строки (либо отредактируйте существующие):

```
vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 allow dns updates = nonsecure
 dns update command = /usr/sbin/samba_dnsupdate --all-names
 dsdb:schema update allowed = true
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните проверку:

```
testparm
```

Пример вывода команды:

```
Load smb config files from /etc/samba/smb.conf
vfs objects specified without required AD DC module: dfs_samba4
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
```

Удалите из настроек сетевого интерфейса из списка DNS-серверов IP-адрес внешнего сервера, который был указан ранее. В данном примере это 8.8.8.8. Перезагрузите сетевой интерфейс.

Запуск служб

Запустите и добавьте в автозагрузку службы **samba**:

```
systemctl enable samba --now
```

Проверьте статус службы:

```
systemctl status samba
```

В DNS добавьте PTR-запись второго сервера в обратную зону.

Для проверки репликации выполните:

```
samba-tool drs showrepl
```

Предупреждение Warning: No NC replicated for Connection! можно проигнорировать (см. FAQ в Samba Wiki).

Для запуска принудительной репликации выполните:

```
samba-tool drs replicate dc2.skynet.murom dc1.skynet.murom dc=skynet,dc=murom
```

В качестве первого аргумента должен быть указан приемник, в качестве второго - источник.

По умолчанию автоматическая *внутрисайтовая репликация* в Windows AD занимает *5 сек*, *межсайтовая репликация - 15 мин*. Данные значения не регулируются. Без успешной двунаправленной репликации в течение *14 дней* DC исключается из Active Directory.

Настройка NTP на контроллере домена dc1.skynet.murom

Для установки NTP выполните:

```
dnf install ntp
```

Измените группу и права:

```
chgrp ntp /var/lib/samba/ntp_signd/
chmod 750 /var/lib/samba/ntp_signd/
```

Отредактируйте конфигурационный файл:

```
nano /etc/ntp.conf
```

Добавьте следующие строки:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
server 0.pool.ntp.org iburst prefer
```

```
server 1.pool.ntp.org iburst prefer
ntpsigndsocket /var/lib/samba/ntp_signd/
```

Закомментируйте строки:

```
#driftfile /var/lib/ntp/ntp.drift
#logfile /var/log/ntp
```

Описание параметров файла конфигурации NTP:

- **ntpsigndsocket /usr/local/samba/ntp_signd/** - позволит клиентским машинам отправлять NTP-запросы к серверу используя Active Directory;
- **Server** - указывает на сервера синхронизации времени;
- **restrict 127.0.0.1** - обмен данным с самим собой;
- **iburst** — отправлять несколько пакетов (повышает точность);
- **prefer** — указывает на предпочитаемый сервер времени;
- **server 127.127.1.0** — позволит, в случае отказа сети Интернет, брать время из своих системных часов.

Старт NTP и добавление в автозапуск:

```
systemctl disable chronyd --now
systemctl enable ntpd --now
```

Проверка статуса NTP:

```
systemctl status ntpd.service
```

Проверить состояние получения эталонного времени можно командой:

```
ntpq -p
```

Настройка NTP на резервном контроллере домена dc2.skynet.murom

Отключите службу **chrony**:

```
systemctl disable chronyd --now
```

Запустите службу **NTP**:

```
systemctl enable ntpd --now
```

В файл **/etc/ntp.conf** на резервном контроллере добавьте строки:

```
server dc1.skynet.murom iburst prefer
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
```

Проверка:

```
[root@dc2 ~]# ntpq -p
remote refid st t when poll reach   delay offset jitter
==============================================================================
*dc1.skynet.murom 62.33.136.11 2 u - 64 1 0.272 0.177 0.618
cello.corbina.n 194.58.202.20 2 u - 64 1 14.088 2.191 0.673
62.183.87.106 194.190.168.1 2 u 1 64 1 48.239 9.129 10.577
```

Настройка двунаправленной репликации sysvol и netlogon с помощью Unison

Информацию о настройке Samba на поддержку репликации SysVol через DFS-R или FRS см. по ссылке.

Папка **SYSVOL** содержит групповые политики и скрипты. Отсутствие репликации приведет к неправильной работе групповых политик и сценариев входа. Есть два варианта: однонаправленная синхронизации и двунаправленная. В первом случае, реплика снимается с основного контроллера и распространяется на все резервные.

Во втором работает в обе стороны. Используем для этого Rsync и Unison (программа двунаправленной синхронизации файлов).

Для установки пакетов выполните:

```
dnf install rsync unison
```

Создание для ssh rsa-ключей и копирование публичного ключ на **DC2**:

```
[root@dc1 ~]# ssh-keygen -t rsa
[root@dc1 ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub root@DC2.skynet.murom
```

Теперь без ввода пароля можно попасть по ssh с **DC1** на **DC2** выполнив команду:

```
ssh dc2.skynet.murom
```

При низких скоростях в сети, unison может некорректно работать, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
mkdir ~/.ssh/ctl
cat << EOF > ~/.ssh/ctl/config
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

Лог файл репликации (следим за размером лога!)

```
touch /var/log/sysvol-sync.log
chmod 640 /var/log/sysvol-sync.log
```

Создайте файла конфигурации unison, для этого создадим каталог **.unison**:

```
mkdir /root/.unison
```

а теперь создайте в нем файл конфигурации:

```
nano /root/.unison/default.prf
```

с содержимым:

```
root = /var/lib/samba
# Note that 2 x / behind DC2, it is required
root = ssh://root@DC2.skynet.murom//var/lib/samba
# Путь синхронизации
path = sysvol
#ignore = Path stats  ## ignores /var/www/stats
auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
copythreshold=0
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress --old-args
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace --compress --old-args
copyquoterem = true
copymax = 1
logfile = /var/log/sysvol-sync.log
```

Установка **rsync** и **unison** на DC2:

```
dnf install rsync unison
```

Сделайте **backup sysvol**, потом запустите команду синхронизации:

```
/usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol
root@dc2.skynet.murom:/var/lib/samba && /usr/bin/unison
&> /dev/null
```

в этой строке программа **rsync** создает структуры каталогов с расширенными атрибутами, а затем программа **Unison** копирует только эти расширенные атрибуты файлов.

Межсайтовая синхронизация настраивается через оснастку (*mmc*) "**Active Directory Sites and Services**" в Windows. Оснастка входит в пакет RSAT.

Настройка доверительных отношений SAMBA и MSAD

Исходные данные
Настройка сервера Samba
Настройка DNS на сервере Windows
Настройка доверительных отношений

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия Samba:** 4.15.9-2h
- **Версия Windows Server:** 2012 R2

Исходные данные

Для примера создания доверительных отношений будут использоваться следующие данные:

Сервер Samba - **dc.skynet.murom**, IP - **10.81.1.199**

Сервер MS AD – **dcms.msnet.murom**, IP - **10.81.1.210**

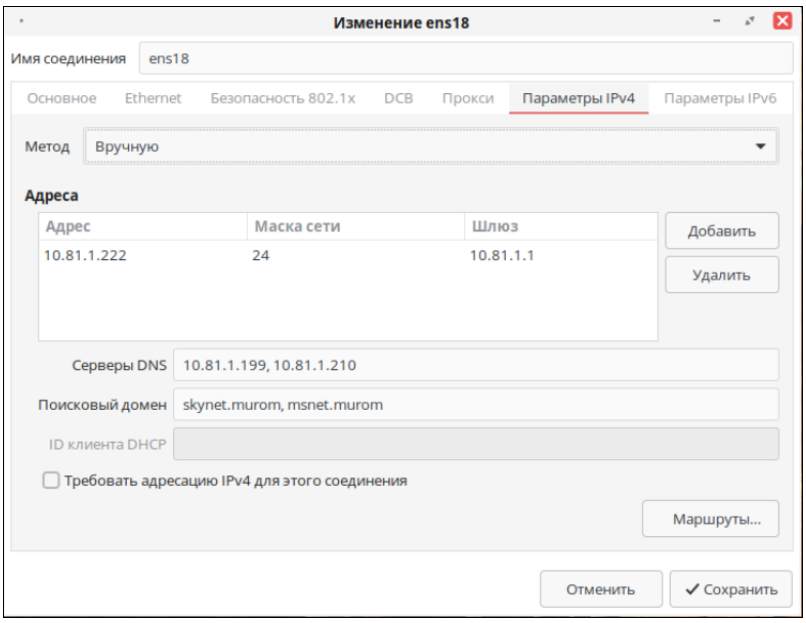
Предполагается, что сервер *Samba* был настроен по инструкции «Установка сервера Samba DC».

Настройка сервера Samba

В сетевых настройках сервера Samba требуется указать DNS адрес контроллера домена MS AD и поисковый домен MS AD. После применения настроек в файле **/etc/resolv.conf** должны содержаться следующее записи:

```
cat /etc/resolv.conf

# Generated by NetworkManager
search skynet.murom msnet.murom
nameserver 10.81.1.199
nameserver 10.81.1.210
```

Пример настройки DNS:



Далее потребуется изменить файл конфигурации:

```
nano /etc/samba/smb.conf
```

В строке dns forwarder пропишите IP-адрес *MS AD*:

```
dns forwarder = 10.81.1.210
```

Если доверительные отношения создаются с доменом **.local**, то в файле **/etc/nsswitch.conf** приведите строку, которая начинается на **hosts**, к виду:

```
hosts:      files dns resolve [!UNAVAIL=return] myhostname mdns4_minimal
```

Затем отредактируйте файл **/etc/krb5.conf**:

```
nano /etc/krb5.conf
```

Добавив строки в [**realms**], где нужно описать *kerberos* область Windows-домена:

```
MSNET.MUROM = {
kdc = dcms.msnet.murom
kdc = dcms2.msnet.murom
admin_server = dcms.msnet.murom
}
```

Если имеется резервный контроллер домена, то его также следует добавить. В примере это `kdc = dcms.msnet.murom.`

Пример вывода:

```
cat /etc/krb5.conf:

[libdefaults]
      default_realm = SKYNET.MUROM
      dns_lookup_realm = false
      dns_lookup_kdc = true
        ticket_lifetime = 24h
        forwardable = yes

[realms]
SKYNET.MUROM = {
      default_domain = skynet.murom
}
MSNET.MUROM = {
   kdc = dcms.msnet.murom
   kdc = dcms2.msnet.murom
   admin_server = dcms.msnet.murom
}

[domain_realm]
       dc = SKYNET.MUROM
```

Проверьте разрешения SRV-записей командой:

```
host -t srv _kerberos._tcp.msnet.murom

_kerberos._tcp.msnet.murom has SRV record 0 100 88 dcms.msnet.murom.
```

Запросите тикет Kerberos:

```
kinit admin@MSNET.MUROM
```

Проверьте, что тикет успешно получен:

```
klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@MSNET.MUROM

Valid starting  Expires   Service principal
25.07.2022  15:19:37 26.07.2022  01:19:37 krbtgt/MSNET.MUROM@MSNET.MUROM
```

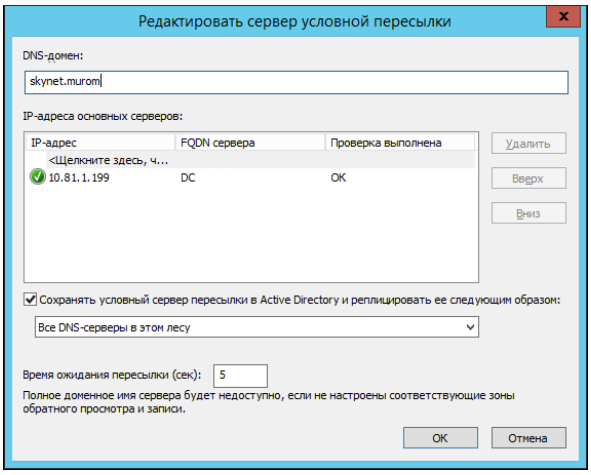
renew until 26.07.2022 15:19:34

Настройка DNS на сервере Windows

Создайте сервер условной пересылки, для этого откройте **Диспетчер DNS** и перейдите на вкладку «**Серверы условной пересылки**».

В контекстном меню выберите «**Создать сервер условной пересылки**».

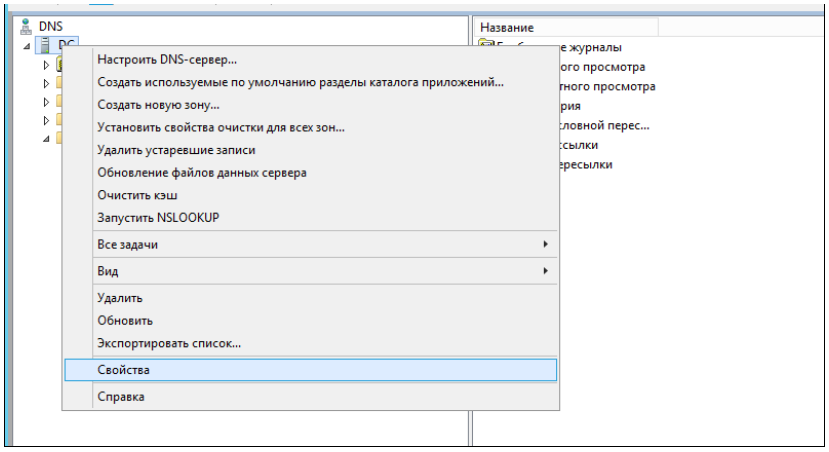
Впишите DNS домен сервера SAMBA и его IP-адрес. Выберите «**Все DNS серверы в этом лесу**» и нажмите **OK**.

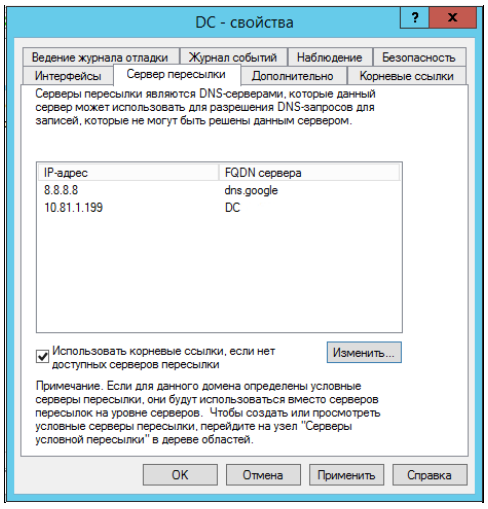


Также необходимо добавить глобальный «**Сервер пересылки**» в свойствах DNS сервера *Windows*.

Для этого в диспетчере DNS нажмите правой кнопкой мыши на сервере DNS (**SERV**) и в выпадающем меню выберите «**Свойства**», перейдите на вкладку «**Сервер пересылки**», нажмите на кнопку «**Изменить**» и в открывшемся окне введите IP-адрес сервера *SAMBA*.

Перейдите в свойства DNS сервера *MS AD*.





Чтобы убедиться, что сервер *AD* может корректно видеть *Samba*, проверьте, правильно ли разрешены записи *SRV*.

```
C:\> nslookup.exe
> set type=srv
> _ldap._tcp.msnet.murom
> _kerberos._tcp.msnet.murom
> exit
```

Настройка двухсторонних транзитивных доверительных отношений

Добавьте доверительные отношения командой:

```
samba-tool domain trust create msnet.murom --type=forest --direction=both --create-location=both -U admin@msnet.murom

LocalDomain Netbios[SKYNET] DNS[skynet.murom] SID[S-1-5-21-3278458734-1377290257-482432228]
RemoteDC Netbios[DC] DNS[dc.msnet.murom] ServerType[PDC, GC, LDAP, DS, KDC, TIMESERV, CLOSEST, WRITABLE, GOOD_TIMESERV,
FULL_SECRET_DOMAIN_6, SERVICE, DS_8, __unknown_00008000__]
```

где:

- `--type=external` - указывает тип доверительного отношения, может принимать значения *external* и *forest*.
    - **external** (внешнее) - означает, что доверительное отношение будет создано с внешним доменом;
    - **forest** (лес) - указывает, что доверительное отношение будет создано с другим лесом. В этом случае, доверительное отношение будет устанавливаться между вашим лесом и другим лесом.
- `--direction=incoming` - определяет направление доверительного отношения. Значение **incoming** указывает, что доверительное отношение будет установлено только для входящих запросов, и ваш сервер Samba будет доверять внешнему домену MS при получении запросов от него;
- `--create-location=local` - указывает место создания доверительного отношения. Значение **local** означает, что доверительное отношение будет создано локально на вашем сервере Samba, и ваш сервер Samba будет инициировать процесс создания доверительного отношения с внешним доменом MS;
- `--direction=both` - доверительное отношение будет устанавливаться в обоих направлениях. Ваш сервер Samba будет доверять другому лесу, и взаимно другой лес будет доверять вашему лесу. Таким образом, обе стороны смогут обмениваться аутентификационной информацией и ресурсами;
- `--create-location=both` - указывает, что доверительное отношение будет создаваться и на вашем сервере Samba, и на другом сервере в другом лесу. Таким образом, создание доверительного отношения происходит с обеих сторон, что обеспечивает взаимное доверие и возможность обмена информацией.

При появлении запроса введите пароль администратора. Если все настроено верно, будет установлено доверие к домену *AD*.

```
Password for [Admin@msnet.murom]:
RemoteDomain Netbios[MSNET] DNS[msnet.murom] SID[S-1-5-21-2219352354-104895378-3667193527]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Validating outgoing trust...
OK: LocalValidation: DC[\\dcms.msnet.murom] CONNECTION[WERR_OK] TRUST[WEER_OK] VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dcms.skynet.murom] CONNECTION[WERR_OK] TRUST[WEER_OK] VERIFY_STATUS_RETURNED
Success.
```

Проверить установленные доверительные отношения можно командой:

```
samba-tool domain trust show msnet.murom

LocalDomain Netbios[SKYNET] DNS[skynet.murom] SID[S-1-5-21-3278458734-1377290257-482432228]
TrustedDomain:

NetbiosName:MSNET
DnsName:msnet.murom
SID:   S-1-5-21-3278458734-1377290257-482432228
Type:    0x2 (UPLEVEL)
Direction:  0x3 (BOTH)
Attributes:   0x4 (QUARANTINED_DOMAIN)
PosixOffset:   0x00000000 (0)
```

```
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96)
```

Если между **samba** и **windows** установлены двухсторонние доверительные отношения с типом связи **Лес**, то рабочую станцию с РЕД ОС нужно вводить в домен **samba** через **winbind**.

Для ввода компьютера в домен Samba используйте следующую команду, которая введет ПК в домен через **windind**:

```
join-to-domain.sh -d  <ваш_домен_samba> -n  <имя_пк> -u  <имя_администратора_samba> -w
```

Если планируется создать односторонние доверительные отношения между Samba и Windows, то для этого на сервере Samba используется команда:

```
samba-tool domain trust create msnet.murom -U admin@msnet.murom
```

При такой связи устанавливаются не транзитивные доверительные отношения (*External Trust*) между двумя доменами Samba и Windows из разных лесов.

Установка сервера SAMBA DC

Предварительная настройка сервера
Обновление пакетов
Установка необходимых пакетов
Отключение SELinux
Присваивание серверу доменного имени
Настройка сетевого интерфейса
Настройка сетевого интерфейса вручную
Настройка сетевого интерфейса с помощью утилиты nmtui
Создание нового домена под управлением контроллера домена Samba DC
Создание резервных копий файлов
Настройка конфигурации Kerberos
Настройка DNS-сервера BIND
Первоначальное полуавтоматическое конфигурирование сервера с помощью утилиты samba-tool
Дополнительная настройка сервера
Запуск и проверка работоспособности службы samba

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: samba-4.17.5-2h, krb5-devel-1.20.1-1, bind-32:9.16.27-1

Предварительная настройка сервера

Обновление пакетов

Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните обновление всех пакетов:

```
dnf makecache && dnf upgrade
```

Все дальнейшие действия выполняются с правами пользователя **root**, если не указано иное.

Установка необходимых пакетов

Для установки необходимых пакетов выполните:

```
dnf install samba* krb5* bind
```

Отключение SELinux

На время настройки переведите SELinux в режим уведомлений:

```
setenforce 0
```

Статус службы SELinux можно посмотреть командой **sestatus**.

Замените в файле конфигурации **/etc/selinux/config** режим `enforcing` на `permissive` командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

После перезагрузки системы служба SELinux будет запущена — в режиме, который указан в конфигурационном файле.

Присваивание серверу доменного имени

Сервер контроллера домена должен иметь собственное уникальное доменное имя и статический IP-адрес. Назначьте серверу полное доменное имя: например, если короткое имя сервера **dc1**, то для домена **skynet.murom** полное имя сервера имеет вид **dc1.skynet.murom**:

```
hostnamectl set-hostname dc1.skynet.murom
```

Настройка сетевого интерфейса

По умолчанию сетевой интерфейс настроен для получения IP-адреса по **DHCP**. Нужно установить серверу контроллера домена статический IP-адрес.

Настройку сетевого интерфейса можно выполнить несколькими способами, в данной статье рассматриваются два из них:

- вручную, путём редактирования файла настроек;
- с помощью графической консольной утилиты **nmtui**.

Настройка сетевого интерфейса вручную

Настройки хранятся в файле **/etc/NetworkManager/system-connections/<имя_сетевого_интерфейса>.nmconnection**. Именуются они, например, как **enp0s3** или **enp0s4**.

В данном примере сетевой интерфейс имеет имя **enp0s3**.

Откройте конфигурационный файл в текстовом редакторе:

```
nano /etc/NetworkManager/system-connections/enp0s3.nmconnection
```

Внесите следующие изменения:

1) измените тип соединения на статический:

```
method=manual
```

2) установите значение для игнорирования DNS из DHCP:

```
ignore-auto-dns=true
```

3) укажите IP-адрес контроллера, маску подсети и IP-адрес шлюза:

```
address1=192.168.1.96/24,192.168.1.1
```

4) укажите в качестве *DNS-сервера* IP-адрес создаваемого контроллера домена:

```
dns=192.168.1.96
```

5) впишите домен поиска (в данном примере это skynet.murom):

```
dns-search=skynet.murom;
```

Итоговый файл настройки должен иметь вид:

```
[connection]
 id=enp0s3
 uuid=97def639-603a-4167-9613-edd5bd902ef8
 type=ethernet
 interface-name=enp0s3
 timestamp=1704763284

 [ethernet]

 [ipv4]
 address1=192.168.1.96/24,192.168.1.1
 dns=192.168.1.96;
```

```
dns-search=skynet.murom;
ignore-auto-dns=true
method=manual

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

Перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Для проверки настроек статической IP-адресации воспользуйтесь командой `ifconfig` или `ip addr`.

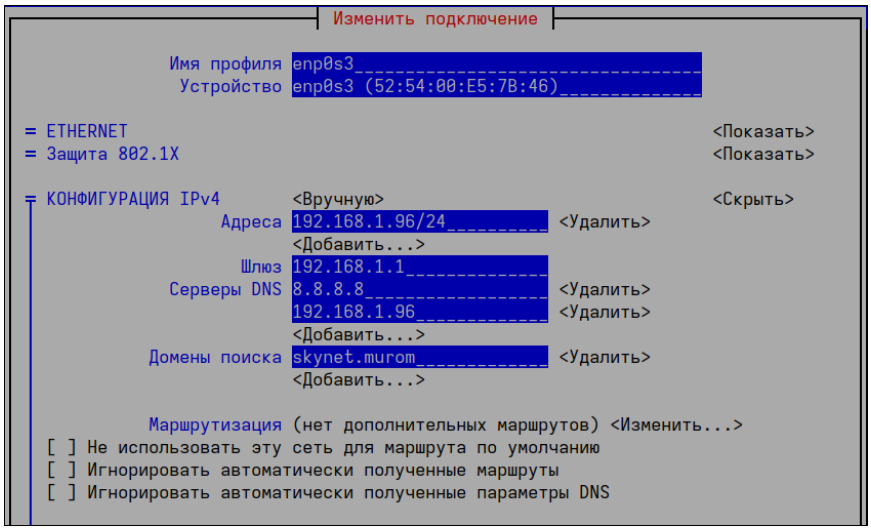
Настройка сетевого интерфейса с помощью утилиты nmtui

Запустите утилиту в консоли:

```
nmtui
```

В настройках сетевого интерфейса в конфигурации **IPv4** укажите следующие значения:

- тип конфигурирования – «**Вручную**»;
- IP-адрес создаваемого сервера и маску подсети – **192.168.1.96/24**;
- адрес шлюза – **192.168.1.1**;
- IP-адрес первого DNS-сервера – IP-адрес сервера с доступом к локальному репозиторию или интернету, например **8.8.8.8** (при добавлении контроллера домена РЕД АДМ в существующий домен указать IP-адрес контроллера домена существующего домена);
- IP-адрес второго DNS-сервера – IP-адрес создаваемого контроллера домена, **192.168.1.96**;
- домен поиска – **skynet.murom**.



Перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Проверьте доступные серверы имен, просмотрев файл **resolv.conf**:

```
cat /etc/resolv.conf
```

Вывод команды должен иметь примерно следующий вид:

```
nameserver 8.8.8.8
nameserver 192.168.1.96
search skynet.murom
```

Создание нового домена под управлением контроллера домена Samba DC

Создание резервных копий файлов

Переименуйте файл **/etc/smb.conf**, он будет создан позднее в процессе выполнения команды **samba-tool**. Наличие данного файла на момент запуска полуавтоматической конфигурации может вызвать ошибку.

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Создайте резервную копию используемого по умолчанию конфигурационного файла **kerberos**:

```
cp /etc/krb5.conf /etc/krb5.conf.bak
```

Настройка конфигурации Kerberos

Проверьте права на доступ к файлу **/etc/krb5.conf**:

```
ls -l /etc/krb5.conf
```

Пользователем-владельцем файла должен быть **root**, а группой-владельцем – **named**. Пример корректного вывода:

```
-rw-r--r-- 1 root named 104 фев 7 11:05 /etc/krb5.conf
```

При необходимости смените владельцев:

```
chown root:named /etc/krb5.conf
```

Откройте файл **/etc/krb5.conf**:

```
nano /etc/krb5.conf
```

В секции [libdefaults] установите имя домена, используемое по умолчанию:

```
default_realm = SKYNET.MUROM
```

Добавьте в секции [realms] и [domain_realm] информацию об именах домена и сервера:

```
[realms]
 SKYNET.MUROM = {
  kdc = dc1.skynet.murom
  admin_server = dc1.skynet.murom
 }

[domain_realm]
  .skynet.murom = SKYNET.MUROM
  skynet.murom = SKYNET.MUROM
```

Пример содержания файла после редактирования:

```
includedir /etc/krb5.conf.d/

[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  dns_lookup_realm = false
  ticket_lifetime = 24h
```

```
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    dns_canonicalize_hostname = fallback
    qualify_shortname = ""
    default_realm = SKYNET.MUROM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 SKYNET.MUROM = {
    kdc = dc1.skynet.murom
    admin_server = dc1.skynet.murom
 }

[domain_realm]
    .skynet.murom = SKYNET.MUROM
    skynet.murom = SKYNET.MUROM
```

Откройте файл **/etc/krb5.conf.d/crypto-policies**:

```
nano /etc/krb5.conf.d/crypto-policies
```

и приведите его содержание к следующему виду:

```
[libdefaults]
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
```

Настройка DNS-сервера BIND

Откройте файл **/etc/named.conf**:

```
nano /etc/named.conf
```

и внесите в блок `options {` следующие значения параметров (при необходимости, добавив отсутствующие параметры):

```
listen-on port 53 { 192.168.1.96; };
 allow-query { any; };
 dnssec-validation no;
 tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
 minimal-responses yes;
 forwarders { 8.8.8.8; };
```

где:

- `192.168.1.96` – IP-адрес создаваемого DNS-сервера, совпадает с адресом контроллера домена;
- `allow-query` – разрешает выполнять запросы всем, но из соображений безопасности можно ограничить доступ для конкретной сети, например, вместо `any` прописать **192.168.1.0/24**;
- `dnssec-validation` – включение валидации **dnssec**, укажите **no**;
- `tkey-gssapi-keytab` и `minimal-responses` – установка этих опций позволит включить динамическое обновление DNS с использованием **Kerberos**;
- `forwarders` – значения IP-адресов внешних DNS-серверов с выходом во внешнюю сеть, для перенаправления на них запросов, например, **{ 8.8.8.8; }**.

Добавьте в конец списка с директивами `include` строку:

```
include "/var/lib/samba/bind-dns/named.conf";
```

Файл должен иметь примерно следующий вид:

```
options {
 listen-on port 53 { 192.168.1.96; };
 listen-on-v6 port 53 { ::1; };
 directory "/var/named";
 dump-file "/var/named/data/cache_dump.db";
 statistics-file "/var/named/data/named_stats.txt";
 memstatistics-file "/var/named/data/named_mem_stats.txt";
 secroots-file "/var/named/data/named.secroots";
 recursing-file "/var/named/data/named.recursing";
 allow-query { any; };
 recursion yes;
 dnssec-validation no;
 managed-keys-directory "/var/named/dynamic";
 geoip-directory "/usr/share/GeoIP";
 pid-file "/run/named/named.pid";
 session-keyfile "/run/named/session.key";
 tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
 minimal-responses yes;
 forwarders { 8.8.8.8;};
 include "/etc/crypto-policies/back-ends/bind.config";
 };

 logging {
 channel default_debug {
 file "data/named.run";
 severity dynamic;
 };
 };

 zone "." IN {
 type hint;
 file "named.ca";
 };

 include "/etc/named.rfc1912.zones";
 include "/etc/named.root.key";
 include "/var/lib/samba/bind-dns/named.conf";
```

Первоначальное полуавтоматическое конфигурирование сервера с помощью утилиты samba-tool

Конфигурирование в интерактивном режиме выполняется командой:

```
samba-tool domain provision --use-rfc2307 --interactive
```

Описание некоторых опций (параметров) этой команды:

- use-rfc2307 – параметр добавляет POSIX атрибуты (UID / GID) на схеме AD. Он понадобится при аутентификации клиентов Linux, BSD, или OS X (в том числе, на локальной машине), в дополнение к Microsoft Windows;
- interactive – запуск в интерактивном режиме;
- realm – указывает на полное DNS-имя домена, которое настроено в **/etc/hosts**, в верхнем регистре (в рассматриваемом примере это **SKYNET.MUROM**);
- Domain – краткое имя домена *NetBIOS* (в примере – **SKYNET**);
- Server Rules – роль сервера (например, DC – **domain controller**);
- DNS backend – DNS-сервер. Возможные значения – **SAMBA_INTERNAL** (внутренний DNS сервера), **BIND9_FLATFILE**, **BIND9_DLZ**, **NONE**;

- DNS forwarder IP address – данный параметр позволяет указать IP-адрес DNS-сервера, на который будут перенаправлены DNS-запросы, в том случае, когда сервер не сможет их разрешить.

Более подробная информация доступна в Wiki-справке проекта Samba по адресу https://wiki.samba.org, на странице "**Setting up Samba as an Active Directory Domain Controller**".

Пример сокращённого листинга настройки для тестового домена **skynet.murom**:

```
Realm [SKYNET.MUROM]:
Domain [SKYNET]:
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: BIND9_DLZ
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce uniqueness constraint on local domainSIDs
Adding DomainDN: DC=skynet,DC=murom
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=skynet,DC=murom
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with this one. Do not create a symlink!
Setting up fake yp server settings
Once the above files are installed, your Samba AD server will be ready to use
Server Role: active directory domain controller
... Hostname:dc1
... NetBIOS Domain:SKYNET
... DNS Domain: skynet.murom
... DOMAIN SID:S-1-5-21-4010603892-1310842104-1159347701
```

После запуска автоматической настройки файлы конфигурации будут созданы автоматически.

Дополнительная настройка сервера

Настройки сервера находятся в файле **/etc/samba/smb.conf**. Конфигурирование сервера выполняется путём внесения изменений в этот файл:

```
nano /etc/samba/smb.conf
```

Начиная с версии **3.3.0** в Samba есть модуль **acl_xattr**, который позволяет Samba корректно обрабатывать Windows ACL (Access Control List) и обеспечивает полноценную поддержку прав доступа к файлам.

Для подключения этого модуля добавьте в файл **/etc/samba/smb.conf** в секцию [global] следующие строки (либо отредактируйте существующие):

```
vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
```

Для включения автоматического обновления записей в DNS добавьте два параметра в секцию [global]:

```
allow dns updates = nonsecure
 nsupdate command = /usr/bin/nsupdate -g
```

В секцию [global] добавьте поддержку расширений схемы Samba AD (Active Directory):

```
dsdb:schema update allowed = true
```

Пример содержания файла **/etc/samba/smb.conf** с внесёнными дополнительными изменениями:

```
cat /etc/samba/smb.conf
```

```
#Global parameters
 [global]
 netbios name = DC1
 realm= SKYNET.MUROM
 server role = active directory domain controller
 server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
 workgroup= SKYNET
 idmap_ldb:use rfc2307 = yes
 vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 nsupdate command = /usr/bin/nsupdate -g
 dsdb:schema update allowed = true

 [sysvol]
 path = /var/lib/samba/sysvol
 read only = No

 [netlogon]
 path = /var/lib/samba/sysvol/skynet.murom/scripts
 read only = No
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните проверку:

```
testparm
```

Пример вывода команды:

```
Load smb config files from /etc/samba/smb.conf
vfs objects specified without required AD DC module: dfs_samba4
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
```

Запуск и проверка работоспособности службы samba

Запустите и добавьте в автозагрузку службы **samba** и **named**:

```
systemctl enable samba named --now
```

Проверьте статус служб:

```
systemctl status samba named
```

Примечание.

Не запускайте службу **winbind** вручную на контроллере домена Samba Active Directory. Служба запускается автоматически как подпроцесс **samba**.

Проверьте работу динамического обновления **DNS**:

```
samba_dnsupdate --verbose --all-names
```

Для более быстрой проверки рекомендуется отключить **IPv6**. Сделать это можно с помощью утилиты **nmtui**.

Администрирование контроллера SAMBA

Средства администрирования удаленного сервера от MS
Подготовка резервного контроллера домена
Добавление резервного контроллера в домен
Установка необходимых пакетов
Создание резервных копий файлов
Настройка конфигурации Kerberos
Настройка DNS-сервера BIND
Присоединение сервера в качестве вторичного контроллера домена
Дополнительная настройка сервера
Запуск служб
Настройка NTP на контроллере домена dc1.skynet.murom
Настройка NTP на резервном контроллере домена dc2.skynet.murom
Настройка двунаправленной репликации sysvol и netlogon с помощью Unison

Средства администрирования удаленного сервера от MS

Введение ПК с Windows в домен Samba производится точно так же, как и ввод компьютера в домен MS AD.

Для администрирования домена Samba установите **RSAT** - https://wiki.samba.org/index.php/Installing_RSAT.

Включите компоненты: «**Установка удаление программ**» - «**Включение отключение компонентов**» - «**Средства удаленного администрирования сервера**».

После настройки перезагрузите ПК.

В управлении DNS подключитесь к **dc1.skynet.murom**, добавьте обратную зону и PTR-запись для контроллера домена **dc1**. Кроме работы с DNS через оснастку Windows существует способ добавления обратной зоны dns с помощью команд в терминале.

Для этого, предварительно, получите kerberos-тикет:

```
kinit administrator@SKYNET.MUROM
```

Добавьте обратную зону:

```
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 1.81.10.in-addr.arpa
samba-tool dns add dc1.skynet.murom 1.81.10.in-addr.arpa 96 PTR dc1.skynet.murom -U administrator
```

в последней команде **96** - это последний октет (четвертый) в IP-адресе (**10.81.1.96**) сервера samba.

Следующие зоны, вероятно, создавать не обязательно, но такие зоны автоматически настроены на Windows srv:

```
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 0.in-addr.arpa
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 127.in-addr.arpa
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 255.in-addr.arpa
```

Подготовка резервного контроллера домена

Предварительная настройка резервного сервера осуществляется аналогично предварительной настройке основного сервера.

В данной статье в качестве примера рассматривается добавление нового контроллера домена с IP-адресом **10.81.1.97** и с доменным именем **dc2** к домену **skynet.murom** под управлением контроллера домена со статическим IP-адресом **10.81.1.96** и доменным именем **dc1** и со значениями прочих параметров, указанных в примере Установка сервера Samba DC. Соответственно, для создаваемого дополнительного контроллера домена значения сетевых параметров следующие:

- краткое доменное имя сервера – **dc2**;
- полное доменное имя сервера – **dc2.skynet.murom**;
- IP-адрес создаваемого сервера и маска подсети – **10.81.1.97**;
- маска подсети – **24**;
- адрес шлюза – **10.81.1.1**;
- IP-адрес первого DNS-сервера – IP-адрес существующего контроллера домена (созданного по инструкции Установка сервера Samba DC) – **10.81.1.96**;
- домен поиска – **skynet.murom**.

Добавление резервного контроллера в домен

Установка необходимых пакетов

Установите необходимые пакеты командой:

```
dnf install samba* krb5* bind
```

Создание резервных копий файлов

Переименуйте конфигурационный файл Samba, тем самым создав его резервную копию:

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Настройка конфигурации Kerberos

Проверьте права на доступ к файлу **/etc/krb5.conf**:

```
ls -l /etc/krb5.conf
```

Пользователем-владельцем файла должен быть **root**, а группой-владельцем – **named**. Пример корректного вывода:

```
-rw-r--r-- 1 root named 104 фев 7 11:05 /etc/krb5.conf
```

При необходимости смените владельцев:

```
chown root:named /etc/krb5.conf
```

Откройте файл **/etc/krb5.conf**:

```
nano /etc/krb5.conf
```

Добавьте в секции `[realms]` и `[domain_realm]` информацию об именах домена и сервера:

```
[realms]
  SKYNET.MUROM = {
    kdc = dc1.skynet.murom
    admin_server = dc1.skynet.murom
  }

 [domain_realm]
    .skynet.murom = SKYNET.MUROM
    skynet.murom = SKYNET.MUROM
```

Пример содержания файла после редактирования:

```
includedir /etc/krb5.conf.d/

 [logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

 [libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
```

```
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    dns_canonicalize_hostname = fallback
    qualify_shortname = ""
    default_realm = SKYNET.MUROM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 SKYNET.MUROM = {
    kdc = dc1.skynet.murom
    admin_server = dc1.skynet.murom
 }

[domain_realm]
    .skynet.murom = SKYNET.MUROM
    skynet.murom = SKYNET.MUROM
```

Откройте файл **/etc/krb5.conf.d/crypto-policies**:

```
nano /etc/krb5.conf.d/crypto-policies
```

и приведите его содержание к следующему виду:

```
[libdefaults]
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
```

Настройка DNS-сервера BIND

В файл **/etc/named.conf** в блок [options] впишите следующие значения параметров:

```
listen-on port 53 { 10.81.1.97; };
 allow-query { any; };
 dnssec-validation no;
 tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
 minimal-responses yes;
 forwarders { 8.8.8.8; };
```

Добавьте в конец списка с директивами **include** строку:

```
include "/var/lib/samba/bind-dns/named.conf";
```

Файл должен иметь вид:

```
options {
    listen-on port 53 { 10.81.1.97; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    allow-query { any; };
    recursion yes;
    dnssec-validation no;
    managed-keys-directory "/var/named/dynamic";
    geoip-directory "/usr/share/GeoIP";
```

```
  pid-file "/run/named/named.pid";
  session-keyfile "/run/named/session.key";
  tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
  minimal-responses yes;
  forwarders { 8.8.8.8; };
  include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
  channel default_debug {
    file "data/named.run";
    severity dynamic;
  };
};

zone "." IN {
  type hint;
  file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/var/lib/samba/bind-dns/named.conf";
```

Присоединение сервера в качестве вторичного контроллера домена

Для присоединения сервера в качестве резервного выполните команду:

```
samba-tool domain join skynet.murom DC -U Administrator --dns-backend=BIND9_DLZ --realm=skynet.murom
```

Вывод команды в случае успеха:

```
INFO 2023-03-03 18:21:40,227 pid:3673 /usr/lib64/python3.8/site-packages/samba/join.py #1544: Joined domain SKYNET (SID S-1-5-21-4085579788-2882808393-2576280794) as a DC
```

Дополнительная настройка сервера

Выполните дополнительную настройку сервера аналогично тому, как это сделано в подразделе Дополнительная настройка основного сервера.

Отредактируйте файл **/etc/samba/smb.conf** и добавьте в секцию [global] следующие строки (либо отредактируйте существующие):

```
vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 allow dns updates = nonsecure
 dns update command = /usr/sbin/samba_dnsupdate --all-names
 dsdb:schema update allowed = true
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните проверку:

```
testparm
```

Пример вывода команды:

```
Load smb config files from /etc/samba/smb.conf
vfs objects specified without required AD DC module: dfs_samba4
Loaded services file OK.
Weak crypto is allowed
```

```
Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
```

Удалите из настроек сетевого интерфейса из списка DNS-серверов IP-адрес внешнего сервера, который был указан ранее. В данном примере это 8.8.8.8. Перезагрузите сетевой интерфейс.

Запуск служб

Запустите и добавьте в автозагрузку службы **samba** и **named**:

```
systemctl enable samba named --now
```

Проверьте статус служб:

```
systemctl status samba named
```

Проверьте работу динамического обновления DNS:

```
samba_dnsupdate --verbose --all-names
```

Через несколько минут можно проверить репликацию:

```
samba-tool drs showrepl
```

Пример отклика команды при успешном запуске репликации:

```
==== KCC CONNECTION OBJECTS ====

 Connection --
Connection name: 09f8315a-7f54-4a99-b3ba-ca918776a462
Enabled : TRUE
Server DNS name : dc1.skynet.murom
Server DN name : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=skynet,DC=murom
TransportType: RPC
options: 0x00000001
Warning: No NC replicated for Connection!
```

Предупреждение Warning: No NC replicated for Connection! можно проигнорировать (см. FAQ в Samba Wiki).

Настройка NTP на контроллере домена dc1.skynet.murom

Установка:

```
dnf install ntp
```

Измените группу и права:

```
chgrp ntp /var/lib/samba/ntp_signd/
chmod 750 /var/lib/samba/ntp_signd/
```

Отредактируйте конфигурационный файл:

```
nano /etc/ntp.conf
```

Добавьте следующие строки:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
server 0.pool.ntp.org iburst prefer
server 1.pool.ntp.org iburst prefer
ntpsigndsocket /var/lib/samba/ntp_signd/
```

Закомментируйте строки:

```
driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp
```

Описание параметров файла конфигурации NTP:

- **ntpsigndsocket /usr/local/samba/ntp_signd/** - позволит клиентским машинам отправлять NTP-запросы к серверу используя Active Directory;
- **Server** - указывает на сервера синхронизации времени;
- **restrict 127.0.0.1** - обмен данным с самим собой;
- **iburst** — отправлять несколько пакетов (повышает точность);
- **prefer** — указывает на предпочитаемый сервер времени;
- **server 127.127.1.0** — позволит, в случае отказа сети Интернет, брать время из своих системных часов.

Старт NTP и добавление в автозапуск:

```
systemctl disable chronyd --now
systemctl enable ntpd --now
```

Проверка статуса NTP:

```
systemctl status ntpd.service
```

Проверить состояние получения эталонного времени можно командой:

```
ntpq -p
```

Настройка NTP на резервном контроллере домена dc2.skynet.murom

Отключите службу **chrony**:

```
systemctl disable chronyd --now
```

Запустите службу **NTP**:

```
systemctl enable ntpd --now
```

В файл **/etc/ntp.conf** на резервном контроллере добавьте строки:

```
server dc1.skynet.murom iburst prefer
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
```

Проверка:

```
[root@dc2 ~]# ntpq -p
remote refid st t when poll reach   delay offset jitter
==============================================================================
*dc1.skynet.murom 62.33.136.11 2 u - 64 1 0.272 0.177 0.618
cello.corbina.n 194.58.202.20 2 u - 64 1 14.088 2.191 0.673
62.183.87.106 194.190.168.1 2 u 1 64 1 48.239 9.129 10.577
```

Настройка двунаправленной репликации sysvol и netlogon с помощью Unison

https://wiki.samba.org/index.php/SysVol_replication_(DFS-R)

Папка **SYSVOL** содержит групповые политики и скрипты. Отсутствие репликации приведет к неправильной работе групповых политик и сценариев входа. Есть два варианта: однонаправленная синхронизации и двунаправленная. В первом случае, реплика снимается с основного контроллера и распространяется на все резервные.

Во втором работает в обе стороны. Используем для этого Rsync и Unison (программа двунаправленной синхронизации файлов).

Установка:

```
dnf install rsync unison
```

Создание для ssh rsa-ключей и копирование публичного ключ на **DC2**:

```
[root@dc1 ~]# ssh-keygen -t rsa
[root@dc1 ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub root@DC2.skynet.murom
```

Теперь без ввода пароля можно попасть по ssh с **DC1** на **DC2** выполнив команду:

```
ssh dc2.skynet.murom
```

При низких скоростях в сети, unison может некорректно работать, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
mkdir ~/.ssh/ctl
cat << EOF > ~/.ssh/ctl/config
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

Лог файл репликации (следим за размером лога!)

```
# touch /var/log/sysvol-sync.log
# chmod 640 /var/log/sysvol-sync.log
```

Создайте файла конфигурации unison, для этого создадим каталог **.unison**:

```
# mkdir /root/.unison
```

а теперь создайте в нем файл конфигурации:

```
# nano /root/.unison/default.prf
```

с содержимым:

```
root = /var/lib/samba
# Note that 2 x / behind DC2, it is required
root = ssh://root@DC2.skynet.murom//var/lib/samba
# Путь синхронизации
path = sysvol
#ignore = Path stats  ## ignores /var/www/stats
auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
copythreshold=0
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress --old-args
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace --compress --old-args
copyquoterem = true
copymax = 1
logfile = /var/log/sysvol-sync.log
```

Установка rsync и unison на DC2:

```
# dnf install rsync unison
```

Сделайте backup sysvol, потом запустите команду синхронизации:

```
/usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol
root@dc2.skynet.murom:/var/lib/samba && /usr/bin/unison
&> /dev/null
```

в этой строке программа rsync создает структуры каталогов с расширенными атрибутами, а затем программа Unison копирует только эти расширенные атрибуты файлов.

Межсайтовая синхронизации настраивается через оснастку (mmc) "Active Directory Sites and Services" в Windows. Оснастка входит в пакет RSAT.

Ввод клиентских машин в домен SAMBA

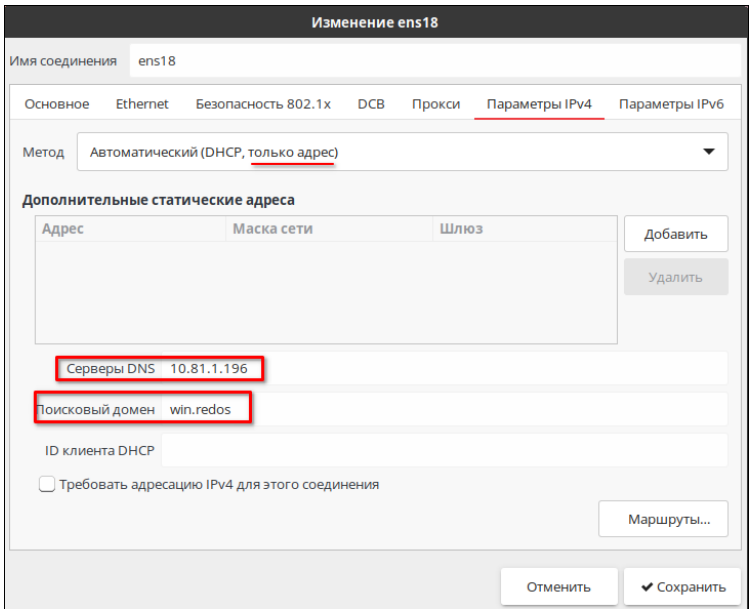
Предварительная подготовка компьютера к вводу в домен
Графический режим работы программы ввода РЕД ОС в домен SAMBA
Терминальный режим работы программы ввода РЕД ОС в домен SAMBA
Вывод РЕД ОС из домена SAMBA

Ввод РЕД ОС в домен **SAMBA** аналогичен вводу РЕД ОС в домен Windows, который описан в разделе «Ввод РЕД ОС в MS Active Directory».

Предварительная подготовка компьютера к вводу в домен

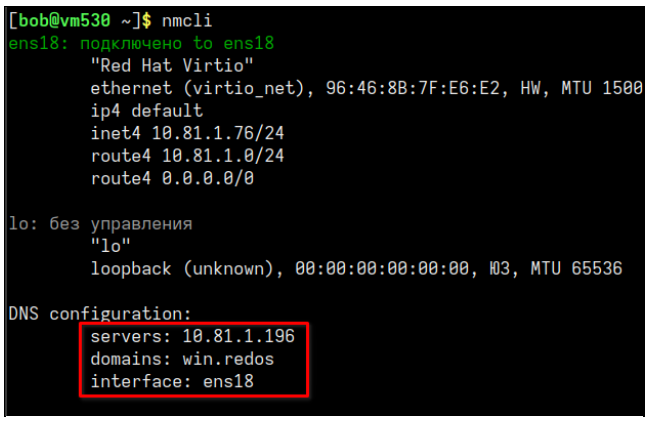
Важное условие для ввода в домен *SAMBA* – это доступность домена и контроллеров домена по их именам (**FQDN**). Обычно сетевые настройки распространяются через DHCP-сервер и сетевой карте вместе с IP-адресом присваивается DNS-сервер, а также поисковый домен.

Если необходимо указать другие настройки DNS и поискового домена, это можно выполнить в настройках сетевого соединения и указать свои значения DNS. Пример сетевых настроек:



Перед вводом в домен необходимо убедиться, что контроллер домена доступен с клиентского ПК, а в настройках сетевой карты назначен DNS-сервер домена.

Команда `nmcli` покажет действующие сетевые настройки.



Для проверки доступности контроллера домена можно запустить команду `ping` и передать ей имя контроллера, например:

```
ping -c 3 dc.win.redos

PING dc.win.redos (10.81.1.196) 56(84) bytes of data.
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=1 ttl=128 time=0.245 ms
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=2 ttl=128 time=0.288 ms
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=3 ttl=128 time=0.312 ms
```

Примечание.

Обращаем внимание, что «пинговать» нужно **имя**, а не IP-адрес, так вы сможете проверить, что на клиенте правильно обрабатываются DNS-имена домена.

Теперь можно приступить к вводу РЕД ОС в домен *SAMBA*.

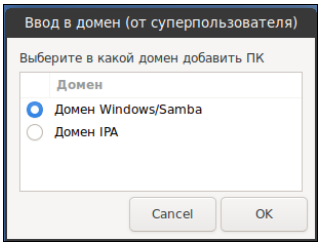
Графический режим работы программы ввода РЕД ОС в домен SAMBA

В РЕД ОС для быстрого ввода компьютера в домен SAMBA используется утилита join-to-domain. Утилита может быть запущена в консольном (текстовом) и в графическом режиме. Описание работы **join-to-domain** в консоли будет рассмотрено ниже.

Для запуска **join-to-domain** в графическом режиме откройте «**Главное меню**» - «**Системные**» - «**Ввод ПК в домен**».

Запуск программы требует ввода пароля от пользователя **root**.

После успешной аутентификации откроется окно выбора типа домена на базе *SAMBA* или *FreeIPA*. Для ввода в домен SAMBA выберите пункт «**Домен Windows/SAMBA**».

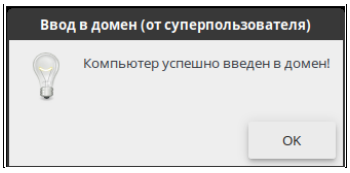


Будет открыто окно, в котором необходимо заполнить поля:

- имя домена;
- имя компьютера (это новое имя данного ПК);
- имя администратора домена;
- пароль администратора.

После нажатия на кнопку «**Да**» начнется процесс присоединения ПК к домену.

В случае успешного ввода в домен появится уведомление:



Перезагрузите компьютер и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

Процесс ввода в домен, а также возможные ошибки при работе протоколируются в файл **/var/log/join-to-domain.log**.

Терминальный режим работы программы ввода РЕД ОС в домен SAMBA

Откройте терминал и выполните запуск **join-to-domain.sh** с привилегиями суперпользователя **root**:

```
join-to-domain.sh
```

Программа запросит пользователя выбрать тип домена, к которому необходимо присоединить РЕД ОС, в данном случае необходимо выбрать первый пункт «**Ввод РЕД ОС в домен Windows/Samba**».

Введите имя домена, имя компьютера, имя администратора домена и подтвердите ваши действия для начала процесса ввода ПК в домен.

```
[root@vm530 ~]# join-to-domain.sh 1

Ввод РЕД ОС в домен Windows 2008/2012/2016/2019, SAMBA, IPA

Этот компьютер не в домене!
Продолжить выполнение (y/n)? y 2

Выберите тип домена:
1. Ввод РЕД ОС в домен Windows/SAMBA
2. Ввод РЕД ОС в домен IPA
Укажите (1 или 2): 1 3

Имя домена [win.redos]
Для подтверждения нажмите ENTER или введите имя домена вручную:

Введите имя ПК. Пример: client1
Имя ПК: vm530 4
Имя администратора домена: admin 5
Имя подразделения ПК(OU=MyComputers) без кавычек или для продолжения нажмите ENTER:
Домен win.redos доступен!
Введите пароль администратора домена:
Продолжить выполнение (y/n)? y 6
1) Установка необходимых пакетов...
2) Изменение имени ПК
   Новое имя ПК: vm530.win.redos
3) Настройка chronyd
4) Настройка hosts
5) Ввод в домен ...
6) Настройка sssd
7) Настройка limits
8) Настройка samba
9) Ввод samba в домен...
   Лог установки: /var/log/join-to-domain.log

   Выполнено. Компьютер успешно введен в домен! Перезагрузите ПК.
[root@vm530 ~]#
```

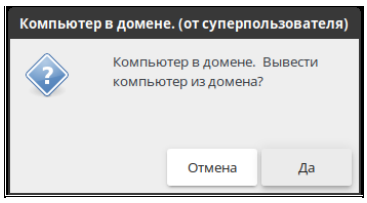
Перезагрузите ПК и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

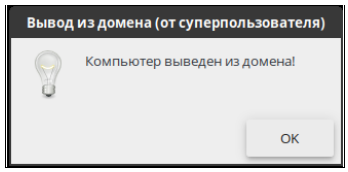
Протокол ввода в домен записывается в файл **/var/log/join-to-domain.log**.

Вывод РЕД ОС из домена SAMBA

Для вывода ПК из домена *SAMBA* следует снова запустить **join-to-domain** из «**Главного меню**» - «**Системные**» - «**Ввод ПК в домен**».

В этот раз программа определит, что РЕД ОС введена в домен и предложит выйти из него.





В режиме терминала вывод выполняется запуском команды с привилегиями суперпользователя **root**:

```
join-to-domain.sh
```

Если компьютер введен в домен, **join-to-domain** это обнаружит и предложит вывести его из домена.

```
[root@vm530 ~]# join-to-domain.sh

 Компьютер введен в домен win.redos. Вывести компьютер из домена?
 Продолжить выполнение (y/n)? y

 Удаление учетной записи ПК из домена.
 Введите имя контроллера домена или для продолжения нажмите ENTER:
 Введите имя администратора домена: admin
Password for admin@WIN.REDOS:

 Компьютер выведен из домена.
[root@vm530 ~]#
```

Управление пользователями и группами в домене SAMBA DC

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** samba 4.15.9-2h

Управление пользователями и группами

Список пользователей:

```
samba-tool user list
```

Создадим пользователя в Active Directory и делаем тесты:

```
samba-tool user create PetrovDA
```

или

```
smbpasswd -a USERNAME
smbpasswd -e USERNAME
```

- **username** - имя нового пользователя в AD;
- ключ **-a** - создает пользователя;
- ключ **-e** - активирует пользователя

Удаление пользователя:

```
samba-tool user delete PetrovDA
```

Изменение пароля пользователя:

```
samba-tool user setpassword PetrovDA
```

Отключить пользователя:

```
samba-tool user disable PetrovDA
```

Список групп:

```
samba-tool group list
```

Добавление группы:

```
samba-tool group add MyGroup
```

Удаление группы:

```
samba-tool group delete MyGroup
```

Добавление пользователя в группу:

```
samba-tool group addmembers MyGroup PetrovDA
```

Удаление пользователя из группы:

```
samba-tool group removemembers MyGroup PetrovDA
```

Проверка подключения к samba ресурсам

Вывести список сетевых ресурсов **samba**:

```
smbclient -L localhost -U%
```

Вывод команды:

```
smbclient -L localhost -U%

members MyGroup PetrovDA
Sharename Type Comment
--------- ---- -------
netlogon Disk
sysvol Disk
IPC$ IPC IPC Service (Samba 4.15.9)
Reconnecting with SMB1 for workgroup listing.
Server Comment
--------- -------
Workgroup Master
```

Проверьте вход с помощью учетной записи администратора домена:

```
smbclient //localhost/netlogon -U Administrator -c 'ls'

Enter SKYNET\Administrator's password:
. D 0 Sun Nov 4 10:56:52 2018
..D 0 Sun Nov 4 10:56:57 2018
6486016 blocks of size 1024. 4496892 blocks available
```

Проверьте выдачу билета керберос:

```
kinit administrator@SKYNET.MUROM
klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SKYNET.MUROM
Valid starting Expires Service principal
04.11.2018 12:03:05 04.11.2018 22:03:05 krbtgt/SKYNET.MUROM@SKYNET.MUROM
renew until 05.11.2018 12:02:56
```

Просмотр пользователей:

```
wbinfo -u
```

Просмотр групп:

```
wbinfo -g
```

Доступ к предыдущим версиям файлов с помощью shadow_copy

На время настройки сервиса переведите selinux в режим уведомлений. Для этого измените содержимое конфигурационного файла:

```
nano /etc/selinux/config
```

Заменив текст `SELINUX=enforcing` на `SELINUX=permissive`
Выполните:

```
setenforce 0
```

Более подробно см.ссылку
Не забудьте включить selinux после завершения настройки.

Процедура настройки «теневых копий» делится на две части:

- предоставление клиентам Microsoft Shadow Copy возможности просматривать снимки файловой системы как «теневые копии» в сетевых каталогах Samba;
- механизм создания «теневых копий».

Настройка в samba механизма «теневых копий»

Samba позволяет вам организовать хранение предыдущих версий файла так, чтобы они были доступны механизму учёта предыдущих версий в Windows. Для этого предназначен специальный модуль `vfs object` с именем **shadow_copy2**. Для активации этого механизма со стороны Samba просто добавьте в блок, описывающий нужную вам шару, несколько строк. Для примера создадим шару **secure**. Добавьте в её блок параметр, активирующий **shadow_copy2**, и параметр **shadow:snapdir**, указывающий, где будут храниться снапшоты. В данном случае, они будут храниться в скрытом каталоге с именем самой шары.

```
[secure]

 vfs objects = shadow_copy2
 shadow:snapdir = /srv/.share
 path = /srv/share
 valid users = @secure
 guest ok = no
 writable = yes
 browsable = yes
```

Теперь добавьте настройки в секции `[global]`:

```
[global]

 wide links = yes
 unix extensions = no
 allow insecure wide links = no
```

- `wide links` разрешает samba проходить по символьным ссылкам;
- `unix extensions =` запрещает *nix клиентам создание символьных ссылок (и еще несколько возможностей, которые вам могут не понадобиться);
- `allow insecure wide links` — эту опцию включаем в `yes` только при включенных `unix extensions`, иначе `wide links` останутся недоступны.

На этом настройку можно закончить. Дополнительные параметры приведены на сайте samba.org и доступны по ссылке.

Пример настройки файлового хранилища SAMBA

Графический вариант
Работа из файлового менеджера
Консольный вариант

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** Samba 4.15.9, share_directory 6.0-1

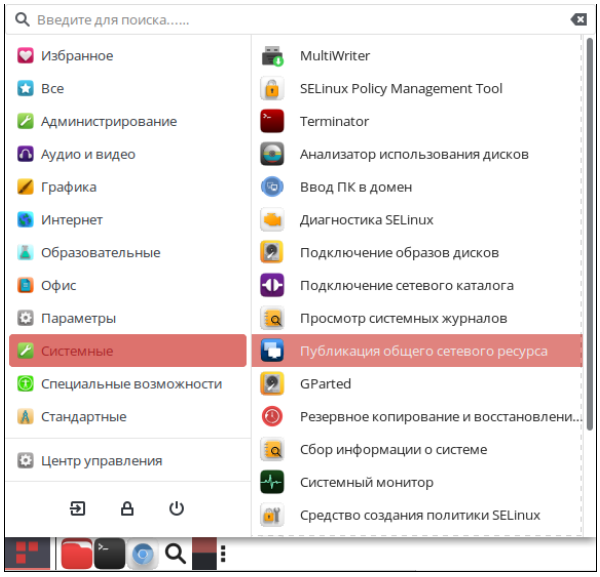
Графический вариант

Утилита публикации сетевого ресурса в рабочей группе доступна в РЕД ОС 7.3.

Установите утилиту командой:

```
dnf install share_directory
```

Запуск утилиты доступен через главное меню:

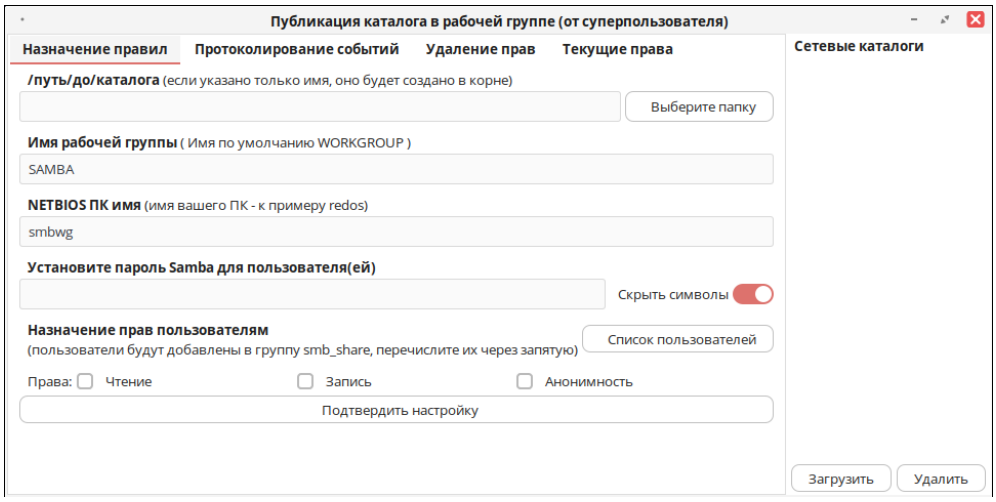


или через терминал:

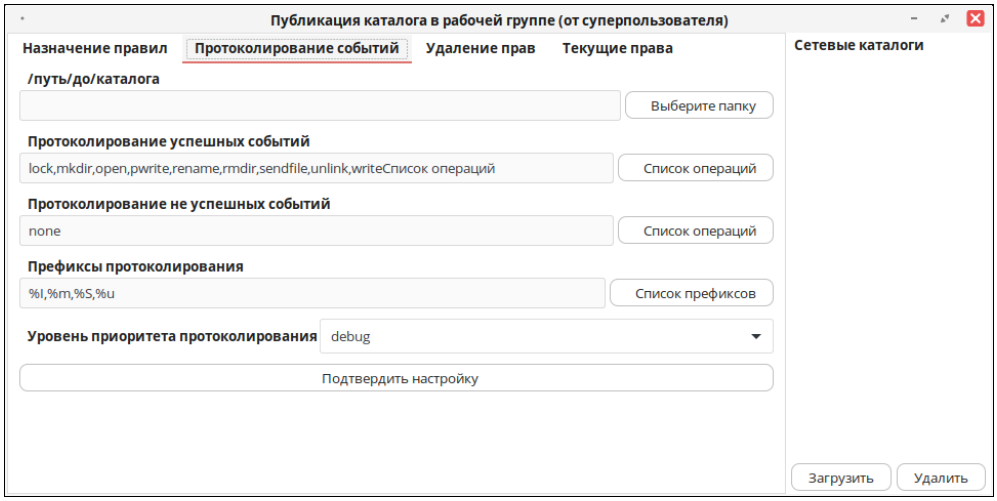
```
share-directory
```

Для того чтобы был запущен вариант утилиты по работе с рабочей группой, ПК не должен находиться в домене, в ином случае утилита запустится в режиме, указанном в данной инструкции «Каталог общего сетевого доступа на РЕД ОС в домене Windows» .

Для ***публикации*** сетевого ресурса в рабочей группе требуется задать путь к директории, задать Samba пароль и выбрать разрешенных пользователей с назначением соответствующих им прав.

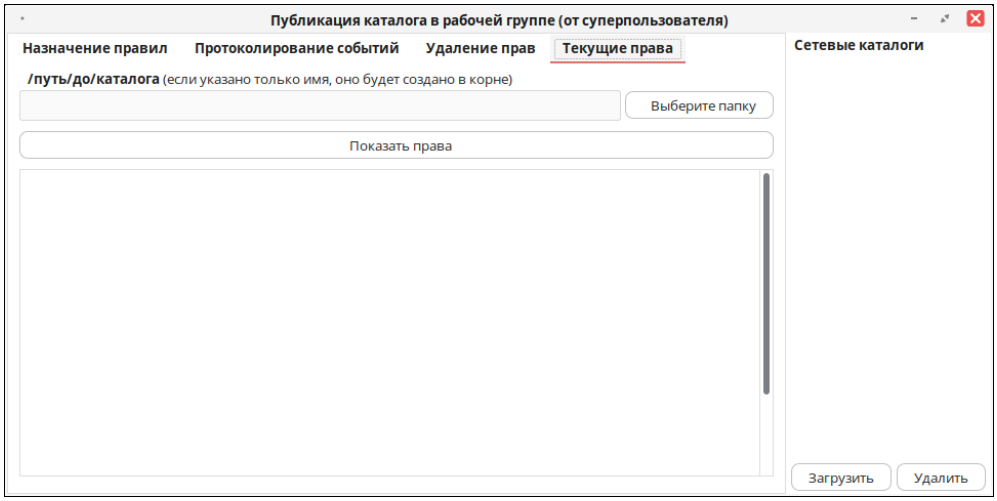


Для того чтобы назначить ***протоколирование событий*** директории, требуется указать путь к ресурсу и необходимые атрибуты.



Для того чтобы ***удалить права*** с директории, требуется указать путь к ресурсу и прописать определенного пользователя, которого требуется удалить. Также доступно полное удаление прав с директории.

Для удобства ***отслеживания прав*** можно посмотреть текущие права директории, указав путь к интересующей.



Работа из файлового менеджера

Для включения быстрой настройки сетевой директории из файлового менеджера **caja** необходимо установить дополнительное расширение. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install share_directory-caja
```

Выйдите из учетной записи **root** командой:

```
exit
```

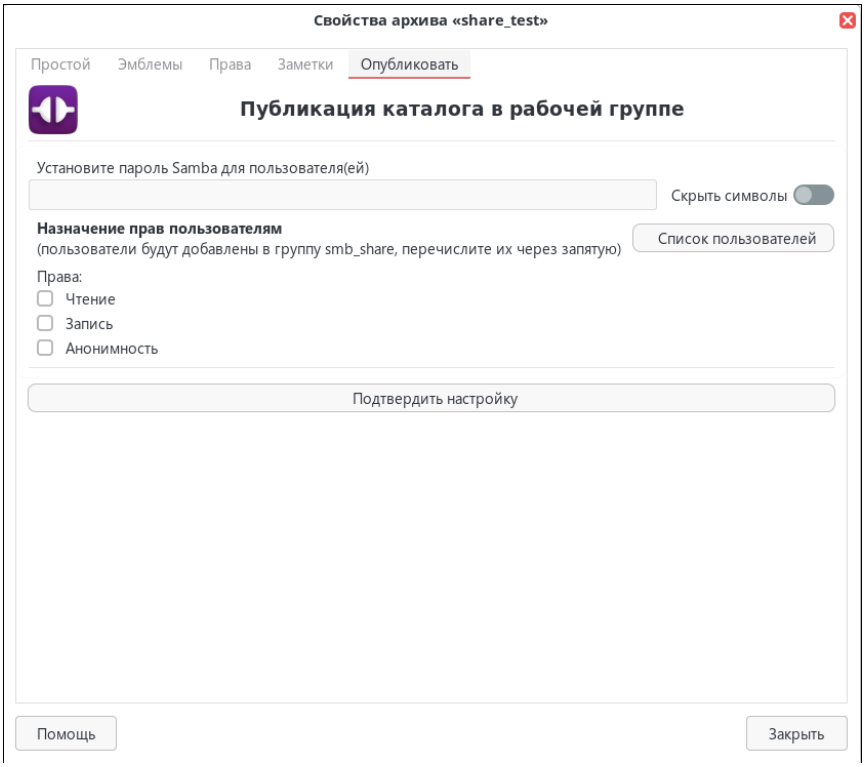
Затем обновите конфигурацию **caja** от имени **локального** пользователя:

```
[ "$EUID" -ne 0 ] && caja -q || echo "Команда не должна выполняться с правами пользователя root!"
```

Или выполните выход из учетной записи пользователя и обратную авторизацию.

После обновления списка расширений **caja** станет доступен новый пункт в свойствах директории.

Вызовите контекстное меню правой кнопкой мыши для необходимой директории в файловом менеджере, затем выберите пункт «**Свойства**» – «**Опубликовать**».



Далее потребуется назначить необходимые атрибуты доступа для директории и выбрать подтверждение настройки.

Консольный вариант

Данная конфигурация будет содержать общую папку obmen, в которую будут иметь доступ авторизованные пользователи. И каждый пользователь будет иметь свою папку, которая доступна только ему и администратору сервера.

Реализация

Автоматически права на пользовательские каталоги и файлы выставляются в 775, что означает – разрешать записывать читать и выполнять файлы только пользователю и группе, остальным только чтение.

Каждый новый пользователь включается в группу администратора для того, что бы он мог редактировать изменения администратора. Так же включаются в общую группу для доступа к общей папке. Администратор при создании новых пользователей включается в их группу для возможности редактирования файлов и каталогов пользователя. В каждый пользовательский сетевой каталог разрешается доступ пользователю и администратору.

Автоматически права на каталоги и файлы в общем каталоге выставляются в 777, что означает – все пользователи могут читать, записывать и выполнять файлы. Доступ к общей папке разрешается общей группе и администратору.

Создайте общий каталог.

```
mkdir /srv/obmen
```

Создайте приватный каталог пользователя:

```
mkdir /srv/user1
```

Создайте пользователя **user1** и **adminsmb**:

```
useradd -d /dev/null -s /usr/sbin/nologin user1
useradd -d /dev/null -s /usr/sbin/nologin adminsmb
```

Задайте пароль пользователю **user1** и **adminsmb**:

```
smbpasswd -a user1
smbpasswd -a adminsmb
```

Создайте общую группу пользователей:

```
groupadd obmen
```

Добавьте пользователя **user1** в группу **obmen**. Последующих пользователей также добавляйте в эту группу. Это позволит им подключаться к общей сетевой папке **obmen**. Пользователя **adminsmb** в группу пользователя **user1**.

```
usermod -a -G obmen user1
usermod -a -G user1 adminsmb
```

Проверьте успешное добавление:

```
groups user1
```

Установите группу **obmen** в качестве владельца папки **/srv/obmen** и предоставьте право на запись:

```
chown -R :obmen /srv/obmen
chmod 777 /srv/obmen
```

Так же установите права и группу на каталог пользователя **user1**.

```
chown -R user1 /srv/user1
chmod 777 /srv/user1
```

Проверить права и владельцев можно следующей командой:

```
ll /srv/
```

Настройка Selinux

SELinux позволяет **Samba** читать и записывать файлы, помеченные типом **samba_share_t**, если файл **/etc/samba/smb.conf** и разрешения Linux установлены соответствующим образом. Введите следующую команду от имени пользователя **root**, чтобы добавить изменение метки в конфигурацию файлового контекста.

```
semanage fcontext -a -t samba_share_t "/srv/obmen(/.*)?"
```

Используйте утилиту restorecon от имени пользователя **root**, чтобы применить изменения метки:

```
restorecon -R -v /srv/obmen
```

Повторите эти действия для остальных каталогов.

Настройка файла конфигурации SAMBA

В файл **/etc/samba/smb.conf** добавьте разделы для созданных сетевых папок.

```
nano /etc/samba/smb.conf
```

```
[global]
workgroup = WORKGROUP # имя рабочей группы
server string = Samba Server %v # описание сервера
netbios name = redos #netbios-имя сервера
security = user
passdb backend = tdbsam
# Создаем лог файл
log file = /var/log/samba/log.%m
max log size = 50

[obmen]
comment = Obmen share with authenticated access
path = /srv/obmen
browsable = yes
writable = yes
guest ok = no
valid users = @obmen adminsmb # указываем группу и конкретное имя пользователя для доступа
force directory mode = 0777
force create mode = 0676
vfs objects = full_audit

[user1]
comment = Private share with user #описание общей папки
path = /srv/user1
browsable = yes # «yes» — означает, что общая папка не будет скрытой
writable = yes # общая папка доступна для записи
guest ok = no # разрешен ли гостевой доступ
valid users = user1 adminsmb # указываем доступ для пользователей
force directory mode = 0775
force create mode = 0674
```

Перезагрузите службу **samba** для вступления изменений в силу.

```
systemctl restart smb
systemctl enable smb
```

Алгоритм создания новых пользователей

Создайте приватный каталог:

```
mkdir /srv/user2
```

Создайте самого пользователя:

```
useradd -d /dev/null -s /usr/sbin/nologin user2
```

Задайте пароль пользователю:

```
smbpasswd -a user2
```

Добавьте созданного пользователя в группу **obmen** и пользователя **adminsmb** в группу созданного пользователя.

```
usermod -a -G obmen user2
usermod -a -G user2 adminsmb
```

Так же установите права и группу на каталог пользователя.

```
chown -R user2. /srv/user2
chmod 777 /srv/user2
```

В файл **/etc/samba/smb.conf** добавьте раздел для созданной сетевой папки.

```
nano /etc/samba/smb.conf
```

```
[user2]
comment = Private share with user
path = /srv/user2
browsable = yes
writable = yes
guest ok = no
valid users = user2 adminsmb
force directory mode = 0775
force create mode = 0674
```

Перезагрузите службу **samba** для вступления изменений в силу.

```
systemctl restart smb
```

Анонимный доступ

- Создадим папку **/srv/guest** и настроим ее для анонимного доступа.

```
mkdir /srv/guest
```

- Назначим пользователя и группу **nobody** владельцем и группой для папки **/srv/guest**. Данный пользователь и группа автоматически присваиваются **samba** анонимным пользователям.

```
chown -R nobody:nobody /srv/guest
```

- Укажем права на директорию, разрешающие пользователю и группе читать и писать в папку.

```
chmod 775 /srv/guest
```

- Настройте конфигурацию **samba**. Файл конфигурации samba находится в **/etc/samba/smb.conf**. Он состоит из разделов. Приведите его к следующему виду:

```
[global]
workgroup = WORKGROUP
server string = Samba Server %v
netbios name = redos
security = user
passdb backend = tdbsam
# Опция bad user означает, что доступ будет предоставлен от имени пользователя nobody
map to guest = bad user

[guest]
comment = Share with anonymous access
path = /srv/guest
browsable = yes
writable = yes
guest ok = yes
```

Настройка Selinux для анонимного доступа:

```
semanage fcontext -a -t samba_share_t "/srv/guest(/.*)?"
restorecon -R -v /srv/guest
```

Каталог общего сетевого доступа на РЕД ОС в домене MSAD

Графический вариант
Работа из файлового менеджера
Консольный вариант

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: share_directory 6.0-1

Рассмотрен механизм создания в РЕД ОС каталога с общим сетевым доступом по протоколу smb. РЕД ОС предварительно необходимо включить в домен *MS AD* согласно инструкциям текущего раздела «Работа с доменом MS AD».

Графический вариант

Утилита публикации сетевого ресурса в домене *Samba / MS AD* доступна в РЕД ОС 7.3.

Установите утилиту командой:

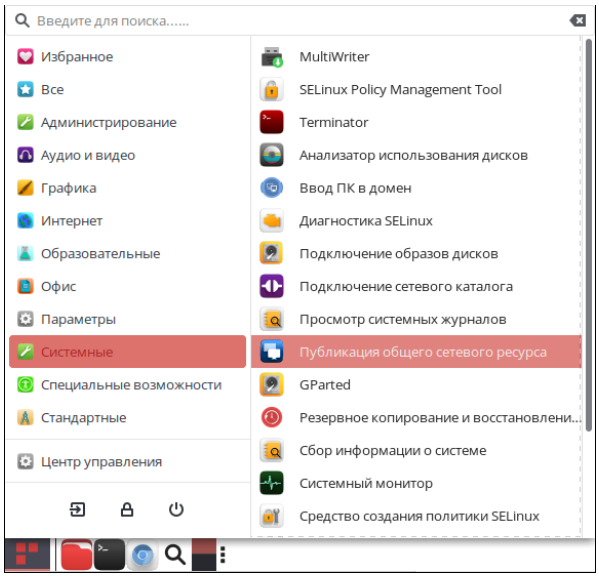
```
dnf install share_directory
```

От имени **root**-пользователя получите **kerberos ticket**:

```
su -
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

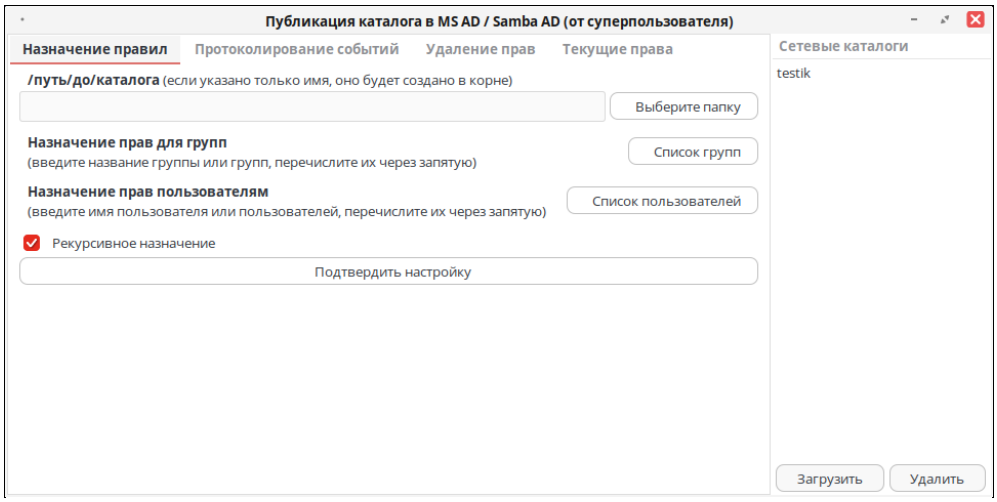
Запуск утилиты доступен через главное меню:



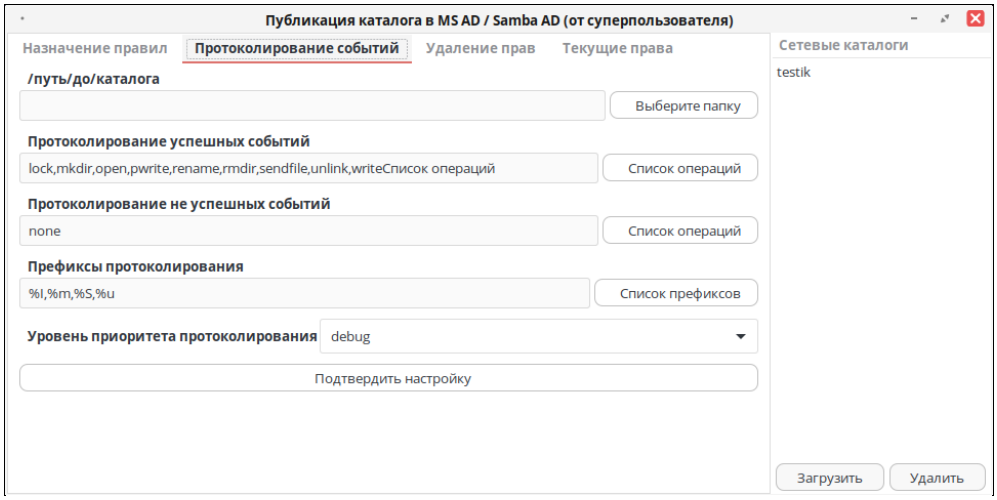
или через терминал:

```
share-directory
```

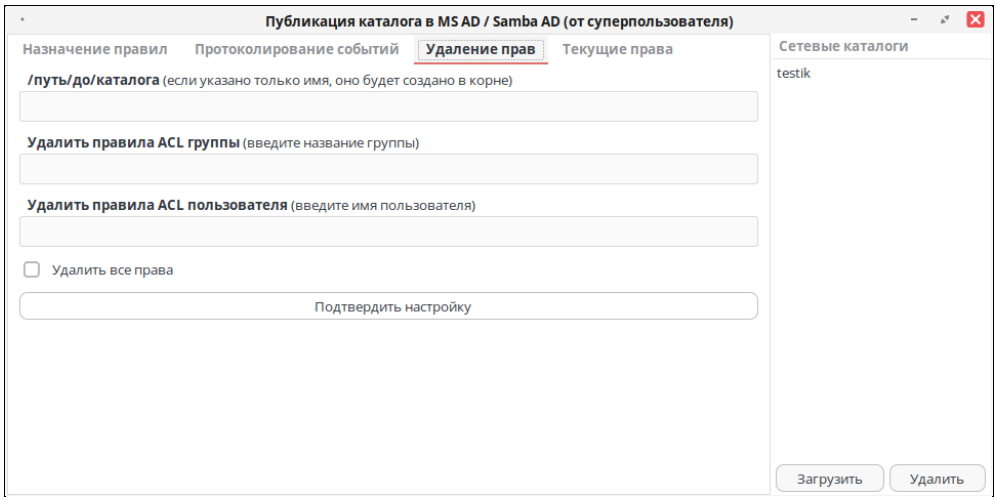
Для публикации сетевого ресурса в домене требуется задать путь к директории, пользователей и/или групп и соответствующие им права.



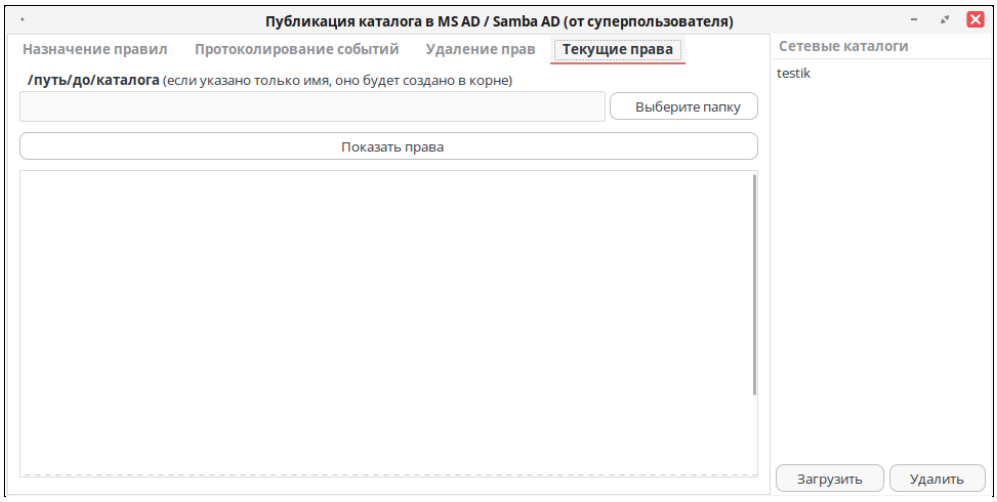
Для протоколирования событий предусмотрена соответствующая вкладка.



Для того чтобы *удалить права* с директории, требуется указать путь к ресурсу и прописать определенного пользователя или группу, которых требуется удалить. Так же доступно полное удаление ACL-прав с директории.



Для удобства *отслеживания прав* можно посмотреть текущие права директории, указав путь к интересующей.



Работа из файлового менеджера

Для включения быстрой настройки сетевой директории из файлового менеджера **caja** необходимо установить дополнительное расширение. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install share_directory-caja
```

Затем получите **kerberos ticket**:

```
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

Выйдите из учетной записи **root** командой:

```
exit
```

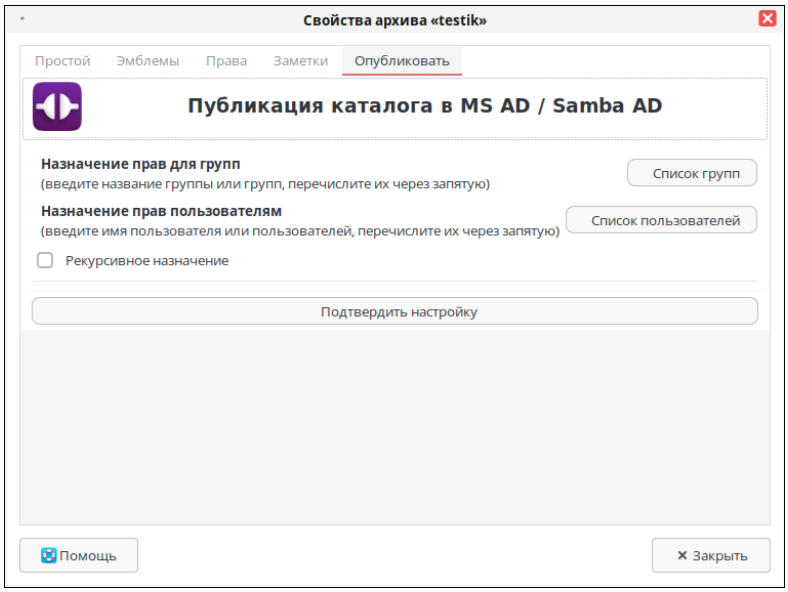
Затем обновите конфигурацию **caja** от имени **локального** пользователя:

```
caja -q
```

Или выполните выход из учетной записи пользователя и обратную авторизацию.

После обновления списка расширений **caja** станет доступен новый пункт в свойствах директории.

Вызовите контекстное меню правой кнопкой мыши для необходимой директории в файловом менеджере, затем выберите пункт «**Свойства**» – «**Опубликовать**».



Консольный вариант

Примечание.

Предполагается, что рабочая станция введена в домен посредством утилиты **join-to-domain** с выбором **sssd**.

Все указанные действия производятся от имени **суперпользователя** (**root**).

1. Добавьте параметр winbind в конце строк, начинающихся с group, passwd и shadow, в файле профиля *authselect* **/etc/authselect/custom/sssd_domain/nsswitch.conf** командой:

```
sed -i_bak '/^\(group:\|passwd:\|shadow:\)/ {s/\(winbind \)\(.*\)$/\2 winbind/; /winbind/ ! s/$/ winbind/}'
/etc/authselect/custom/sssd_domain/nsswitch.conf
```

2. Примените изменения профиля *authselect* командой:

```
authselect apply-changes
```

3. Проверьте возможность получения *kerberos*-билета для доменного пользователя:

```
kinit username
klist
```

4. Проверьте доступность входа доменного пользователя в систему:

```
su username
exit
```

5. Создайте каталог для общего доступа:

```
mkdir -p /share/
```

6. Назначьте права доступа. Пример для домена *wintest*:

```
chown -R root:"wintest\Пользователи домена" /share
chmod 2770 /share
setfacl -m default:group:"wintest\Администраторы домена":rwx /share/
setfacl -m default:group:"wintest\Пользователи домена":r-x /share/
setfacl -m default:other::--- /share/
```

В данном примере с помощью команды **setfacl** были выданы полные (rwx) права группе «**Администраторы домена**» на каталог **/share**.

Группе «**Пользователи домена**» домена *wintest* были выданы права только на чтение и выполнение (просмотр содержимого каталога).

7. Настройте политику *SELinux* для общего каталога и примените её:

```
semanage fcontext -a -t samba_share_t "/share(/.*)?"
restorecon -R -v /share
```

8. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) в секции [global] проверьте наличие следующих строк:

```
vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab
```

9. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) создайте раздел настроек общего ресурса [share] (с этим именем ресурс будет отображаться для клиентов):

```
[share]
 path = /share/
 read only = no
 browseable = yes
 create mask = 0664
 directory mask = 0775
```

10. Дополнительная настройка прав:

- установить полные права на каталог для группы:

```
setfacl -m g:"wintest\Группа_Пользователей":rwx /share
```

- установить полные права на каталог для пользователя:

```
setfacl -m u:"wintest\Пользователь":rwx /share
```

- удалить ACL для определённого пользователя:

```
setfacl -x u:alex /share
```

- удалить все ACL-права каталога:

```
setfacl -b /share
```

- просмотреть ACL-права на каталог:

```
getfacl /share
```

Подробное описание списков контроля доступа (ACL) и параметров команды **setfacl** доступно в нашей статье «Списки контроля доступа ACL»

11. Установите автоматический запуск служб *samba*:

```
systemctl enable smb --now
systemctl enable nmb --now
systemctl enable winbind --now
```

12. Перезагрузите рабочую станцию. Проверьте статус служб:

```
systemctl is-failed smb
systemctl is-failed nmb
systemctl is-failed winbind
```

При корректной настройке каждая команда должна вывести сообщение «active».

Интеграция файлового сервера SAMBA с IPA

Установка необходимых пакетов на сервере SAMBA
Настройка серверов IPA и Samba
Настройка сетевого каталога на сервере Samba

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: ipa-client-4.10.1-2, samba-4.17.5-2h

Установка необходимых пакетов на сервере SAMBA

Для установки пакетов **samba** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ipa-client sssd-libwbclient samba samba-client ipa-client-samba
```

Установите имя хоста samba-сервера:

```
hostnamectl set-hostname samba.redosipa.ru
```

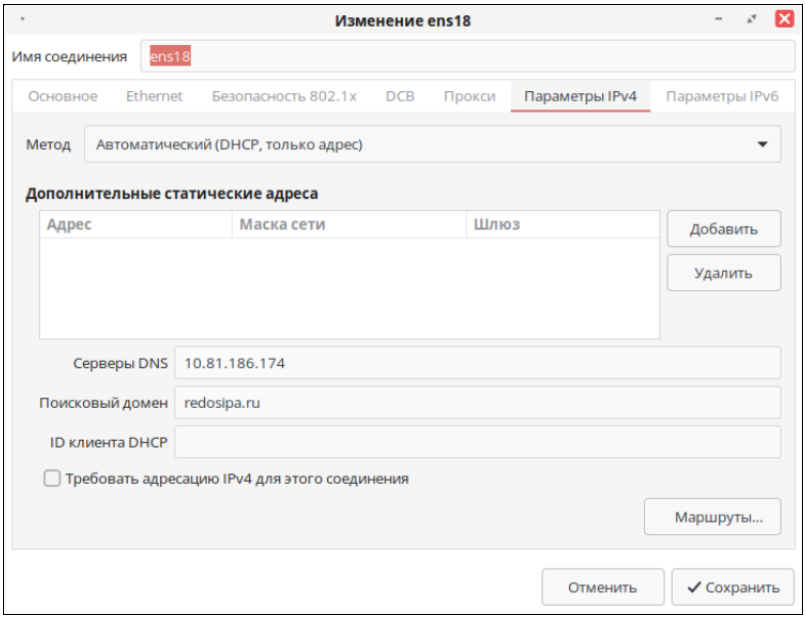
Добавьте запись в **/etc/hosts**, по какому IP обращаться к домену IPA, например:

```
10.81.186.174 server.redosipa.ru
```

Отключите службу:

```
systemctl disable --now systemd-timesyncd
```

В сетевых настройках укажите поисковый DNS IPA-сервера, например:



Присоедините файловый сервер к домену IPA:

```
join-to-domain.sh
```

Выполните автоматическую конфигурацию системных служб на сервере **samba** для работы в домене IPA:

```
authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

Настройка серверов IPA и Samba

Для правильного распределения DNS выполните следующие команды на сервере IPA:

```
kinit admin
ipa dnsrecord-add redosipa.ru --a-rec=samba --a-ip-address=10.81.186.124
```

Запустите настройку домена для обработки классов и атрибутов объектов, специфичных для **Samba**:

```
ipa-adtrust-install --add-sids
reboot
```

На сервере **samba** выполните ipa-client-samba, который создаст **cifs** и отредактирует **/etc/samba/smb.conf** для работы *samba* с **ipa**:

```
ipa-client-samba
```

Отредактируйте в файле **/etc/samba/smb.conf** значение netbios name, указав рабочую группу домена, в данном случае **smb.conf** будет выглядеть следующим образом:

```
...
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 ...
```

Далее отредактируйте секции по примеру из **smb.conf**:

```
[global]
 max smbd processes = 1000
 dedicated keytab file = FILE:/etc/samba/samba.keytab
 kerberos method = dedicated keytab
 log file = /var/log/samba/log.%m
 log level = 1
 server role = member server
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 idmap config * : range = 0 - 0
 idmap config * : backend = tdb


 idmap config REDOSIPA : range = 14000000 - 14199999
 idmap config REDOSIPA : backend = sss

 security = ads
 printing = cups
 printcap name = cups
 load printers = yes
 cups options = raw

 [homes]
 read only = no
 comment = Home Directories
 valid users = %S, %D%w%S
 browseable = No
 read only = No
 inherit acls = Yes
```

```
[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775
```

Создайте структуру ролей и привилегий для **samba**. Действия выполняются на контроллере домена **ipa**:

```
ipa permission-add "CIFS server can read user passwords" --attrs={ipaNTHash,ipaNTSecurityIdentifier} --type=user --right=
{read,search,compare} --bindtype=permission
ipa privilege-add "CIFS server privilege"
ipa privilege-add-permission "CIFS server privilege" --permission="CIFS server can read user passwords"
ipa role-add "CIFS server"
ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
ipa role-add-member "CIFS server" --services=cifs/samba.redosipa.ru
```

На samba-сервере внесите изменения в **/etc/krb5.conf**:

```
sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

Получите тикет и создайте **keytab**:

```
kinit admin
ipa-getkeytab -s server.redosipa.ru -p cifs/samba.redosipa.ru -k /etc/samba/samba.keytab
reboot
```

Настройка сетевого каталога на сервере Samba

На samba-сервере создайте каталог:

```
mkdir -p /share/
```

Назначьте права на созданный каталог:

```
chown -R :users /share
chmod -R 777 /share
setfacl -m default:user:"admin":rwx /share
setfacl -R -m default:user:"admin":rwx /share
```

Затем настройте метки SELinux:

```
semanage fcontext -a -t samba_share_t /share/
restorecon -R -v /share/
```

На контроллере домена **IPA** получите SID:

```
net getdomainsid
```

На файловом сервере **samba** настройте идентификатор безопасности (введите SID, полученный ранее):

```
 net setdomainsid <SID>
```

На сервере **samba** выполните:

```
net -s /dev/null groupmap add sid=S-1-5-32-546 unixgroup=nobody type=builtin
```

В **/etc/samba/smb.conf** укажите настройки для каталога:

```
[share]
 path = /share
 writable = yes
 browsable=yes
 valid users = admin
 read list = admin
 write list = admin
 guest ok = no
 inherit acls = Yes
 create mask = 0660
 directory mask = 0770
```

Добавьте в автозапуск службы **samba** и **winbind**, перезагрузите сервер **samba**:

```
systemctl enable smb winbind --now
reboot
```

Для проверки доступности сетевого каталога на сервере **samba** необходимо получить тикет (если он отсутствует) и выполнить команду подключения к сетевому каталогу:

```
kinit admin
smbclient //samba.redosipa.ru/share -N --kerberos=required
```

В случае, если все настроено верно, появится следующее сообщение:

```
Try "help" to get a list of possible commands.
 smb: \>
```

Журналирование событий SAMBA

Настройка протоколирования событий, связанных с файловым хранилищем *samba*, является довольно важным вопросом. Рассмотрим случай, когда на файловом сервере присутствуют сетевые папки, для которых необходимо организовать запись действий, которые пользователи производят в данной папке.

За настройку журналирования действий *samba* отвечает конфигурационный файл **/etc/samba/smb.conf**.

Рассмотрим пример сетевой папки, имеющей в своем теле конфигурацию для протоколирования событий.

Секция сетевой папки:

```
[share_domain]
path = /share_domain/
read only = no
browseable = yes
vfs objects = full_audit
full_audit:prefix = %u|%I|%m|%S
full_audit:failure = none
full_audit:success = lock write pwrite mkdirat open sendfile unlinkat write renameat
full_audit:facility = local5
full_audit:priority = debug
```

Рассмотрим детально, что означают данные параметры:

В параметре **vfs objects** указывается модуль **full_audit**, на основе которого будет происходить протоколирование событий.

Запись **full_audit:prefix = %u|%I|%m|%S** представляет из себя набор тех данных, которые будут записываться в логи при определенных действиях пользователей в сетевой папке.

▸ **Полный список допустимых переменных**

Параметры:

full_audit:failure = none

full_audit:success = lock write pwrite mkdirat open sendfile unlinkat write renameat

отвечают за протоколирование действий в случае успешного выполнения операции или неуспешного. Допустимо использование **none** - т.е. отсутствие протоколирования событий или команд.

▸ **Полный список допустимых команд**

Параметры:

full_audit:facility = local5 - категория событий *syslog*, в которую будут попадать записи.

Для того чтобы каждая сетевая папка вела свои собственные логи, требуется указывать отличные друг от друга значения, т.е. **local5**, **local6**, **local7** и т.д.

full_audit:priority = debug - категория событий *syslog*, в которую будут попадать записи.

Доступные приоритеты: **notice**, **debug**, **alert**

Необходимо помнить, для того чтобы настройки вступили в силу, требуется перезапустить сервис:

```
sudo -E systemctl restart smb
```

Настройка ведения логов в определенный файл

За пути логов отвечает конфигурационный файл **/etc/rsyslog.conf**, в конец файла вписывается для каждой сетевой папки свой параметр **local4**, **local5**, **local6** и т.д.:

```
local5.debug -/var/log/samba/audit.log
```

Вместо **debug** необходимо указать тот режим, который был указан в параметре **full_audit:priority**.

Также для удобства ведения логов можно назвать файл логов идентично имени сетевой папки, т.е.:

```
local5.debug -/var/log/samba/share_dir.log
```

Для применения изменений потребуется перезапустить сервис командой:

```
sudo -E systemctl restart rsyslog
```

Настройка ротации логов

За ротации логов отвечает конфигурационный файл **/etc/logrotate.d/samba**.

По умолчанию в системе уже настроена ротация логов *Samba* и конфигурационный файл имеет следующее содержимое:

```
/var/log/samba/log.* {
    compress
    dateext
    maxage 365
    rotate 99
    notifempty
    olddir /var/log/samba/old
    missingok
    copytruncate
}
```

Рассмотрим, за что отвечают параметры:

- **compress** - сжатие данных;
- **dateext** - добавляет дату ротации перед заголовком старого лога;
- **maxage** - значение, отвечающее за удаление логов старше X дней;
- **rotate** - параметр отвечает за частоту ротаций логов через X дней;
- **notifyempty** - не сдвигать журнал, если он пуст;
- **olddir /var/log/samba/old** - параметр отвечающий, куда сохранять старые логи;
- **missingok** - в случае отсутствия файла журнала перейти к обработке следующего, не выдавая сообщения об ошибке;
- **copytruncate** - после создания копии обрезать исходный файл журнала взамен перемещения старого файла журнала и создания нового. Данный параметр применяется в том случае, когда некоторой программе нельзя указать закрыть её журнал, и таким образом можно постоянно продолжать запись (добавление) в существующий файл журнала.

Запустить ротацию логов можно следующей командой:

```
sudo -E logrotate -v -f /etc/logrotate.conf
```

Резервное копирование домена SAMBA DC

Резервное копирование типа online
Резервное копирование типа offline
Восстановление домена из файла резервной копии
Обновление пакетов
Отключение SELinux
Присваивание серверу доменного имени
Настройка сетевого интерфейса
Установка необходимых пакетов
Создание резервных копий файлов
Процесс восстановления домена из резервной копии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: samba-4.17.5-2h, krb5-devel-1.20.1-1, bind-32:9.16.27-1

Резервное копирование **Samba** обеспечивает восстановление домена в случае серьезного сбоя.

> **Примечание.**
>
> Если в качестве файлового сервера используется DC, необходимо создать резервную копию для хранимых данных отдельно.

Существует два типа резервного копирования:

- **online** – создает клон базы данных работающего DC. По функциональности процесс похож на подключение нового DC к сети. Резервное копирование может быть произведено удаленно;
- **offline** (или локальное) — создает копию локальных файлов Samba, которые расположены на диске. Включает в себя метаданные репликации, которые являются локальными для данного DC. Резервное копирование выполняется только локально. При этом резервное копирование может быть выполнено на DC как в работающем, так и в не работающем состоянии.

Резервное копирование типа **online** лучше всего подходит для обеспечения долгосрочной замены домена. Его также можно использовать в качестве временной замены, но будет недоступно одновременное устранение неполадок с вышедшими из строя контроллерами домена. Выяснение причин сбоя домена Samba может занять много времени и быть технически сложной работой. В случае критичного сбоя домена, когда нет необходимости исследовать проблему и требуется просто вернуться к старой копии рабочего домена, данный вариант является оптимальным.

Резервное копирование типа **offline** лучше всего подходит для изучения информации о сбое, поскольку она содержит дополнительные данные, которые обычно не реплицируются. При резервном копировании типа **offline** быстрее выполняется автономное резервное копирование для большого домена, поскольку не возникает дополнительных затрат на отправку базы данных по сети и повторную запись ее на диск.

Два этих типа резервного копирования имеют несколько общих черт. Резервные копии создаются с использованием двух вариантов команды `samba-tool domain backup`. Каждая команда создает файл резервной копии ***.tar.bz2**, который содержит полную резервную копию домена (на основе данного DC). Затем файл резервной копии можно использовать для восстановления домена с помощью команды `samba-tool domain backup restore`.

Резервное копирование типа online

Для того чтобы запустить резервное копирование в режиме **online**, выполните команду:

```
samba-tool domain backup online --targetdir=<каталог_хранения_РК> --server=<имя_сервера_DC> -U Administrator
```

где:

- **--targetdir=** - путь до директории, в которую будет сохранен файл резервной копии в формате **tar.bz2**;
- **--server=** - доменное имя сервера, на котором будет производиться резервное копирование;
- **-U** - имя учетной записи администратора контроллера домена.

Команда может быть запущена как удаленно, так и локально на самом контроллере домена. Выполняя удаленное копирование, можно добавить параметр **--configfile** для включения в резервную копию правильных параметров файла **smb.conf** (т. е. локальный файл

smb.conf может не существовать или его параметры могут отличаться от используемого контроллера домена).

Пример команды:

```
samba-tool domain backup online --targetdir=<каталог_хранения_PK> --server=<имя_сервера_DC> -U Administrator --configfile
```

Полезно также будет скопировать содержание файла **/etc/krb5.conf**, для того чтобы скорректировать настройки **kerberos** при последующем восстановлении домена. Так как в резервную копию попадает лишь файл из **/var/lib/samba/private/krb5.conf**, который может отличаться от используемого файла в **/etc/krb5.conf**.

Резервное копирование типа offline

Для создания резервной копии в режиме **offline** войдите в систему, резервную копию которой необходимо создать, и укажите расположение целевого каталога для записи файла резервной копии. Пример:

```
samba-tool domain backup offline --targetdir=<каталог_хранения_PK>
```

где **--targetdir=** - путь до директории, в которую будет сохранен файл резервной копии в формате **tar.bz2**.

Во время выполнения копирования контроллер домена может находиться как в рабочем состоянии, так и в автономном (когда службы **samba** отключены).

Полезно также будет скопировать содержимое файла **/etc/krb5.conf**, для того чтобы скорректировать настройки **kerberos** при последующем восстановлении домена. Так как в резервную копию попадает лишь файл из **/var/lib/samba/private/krb5.conf**, который может отличаться от используемого файла в **/etc/krb5.conf**.

Восстановление домена из файла резервной копии

Будет рассмотрен пример восстановления домена из файла резервной копии на новом сервере.

Первые шаги восстановления похожи на установку нового сервера **Samba DC**.

Обновление пакетов

Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните обновление всех пакетов:

```
dnf makecache && dnf update
```

Все дальнейшие действия выполняются с правами пользователя **root**, если не указано иное.

Отключение SELinux

На время настройки переведите SELinux в режим уведомлений:

```
setenforce 0
```

Статус службы SELinux можно посмотреть командой sestatus.

Замените в файле конфигурации **/etc/selinux/config** режим **enforcing** на **permissive** командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

После перезагрузки системы служба SELinux будет запущена в режиме, который указан в конфигурационном файле.

Присваивание серверу доменного имени

Сервер контроллера домена должен иметь собственное уникальное доменное имя и статический IP-адрес. Назначьте серверу полное

доменное имя: например, если короткое имя сервера **dc1**, то для домена **skynet.murom** полное имя сервера имеет вид **dc1.skynet.murom**:

```
hostnamectl set-hostname dc1.skynet.murom
```

ВАЖНО!

Сервер должен иметь новое доменное имя, не совпадающее с доменным именем сервера, с которого была снята резервная копия.

Настройка сетевого интерфейса

По умолчанию сетевой интерфейс настроен для получения IP-адреса по **DHCP**. Нужно установить серверу контроллера домена статический IP-адрес.

Также необходимо установить адрес первого DNS-сервера с доступом к интернету или локальному репозиторию и адрес второго DNS-сервера самого контроллера домена.

После проведенных настроек перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Проверьте доступные серверы имен, просмотрев файл **resolv.conf**:

```
cat /etc/resolv.conf
```

Вывод команды должен иметь примерно следующий вид:

```
# Generated by NetworkManager
search skynet.murom
nameserver 8.8.8.8
nameserver 10.81.1.96
```

Установка необходимых пакетов

Для установки необходимых пакетов выполните:

```
dnf install samba* krb5*
```

Создание резервных копий файлов

Переименуйте используемые по умолчанию конфигурационные файлы **samba** и **kerberos**, тем самым создав их резервную копию:

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
mv /etc/krb5.conf /etc/krb5.conf.bak
```

Переместите все файлы из каталога **/var/lib/samba** в новый, тем самым создав их резервную копию:

```
mkdir /var/lib/samba.bak
mv /var/lib/samba/* /var/lib/samba.bak/
```

Процесс восстановления домена из резервной копии

Скопируйте файл резервной копии в формате ***.tar.bz2** на сервер. Выполните команду для восстановления домена из резервной копии:

```
samba-tool domain backup restore --backup-file=/home/user/backup_file.tar.bz2 --newservername=dc1 --targetdir=/var/lib/samba
```

где:

- **--backup-file=** - путь до файла с резервной копией;
- **--newservername=** - новое доменное имя для контроллера домена, оно не должно совпадать с именем старого контроллера домена, с которого была снята резервная копия.

Успешное выполнение команды должно сопровождаться следующими сообщениями:

```
Backup file successfully restored to /var/lib/samba
Please check the smb.conf settings are correct before starting samba.
```

Перенесите конфигурационные файлы командами:

```
cp /var/lib/samba/etc/smb.conf /etc/samba/
cp /var/lib/samba/private/krb5.conf /etc/
```

При необходимости можно изменить конфигурацию файла **krb5.conf** в соответствии с файлом **krb5.conf** старого контроллера домена, содержание которого было скопировано на этапе создания резервной копии.

Запустите службы **samba** командой:

```
systemctl enable samba --now
```

Проверьте статус служб **samba** командой:

```
systemctl status samba --now
```

В статусе возможно появление ошибки **winbind**. Если ошибка появилась, выполните:

```
systemctl restart samba.service
```

Для того чтобы повторно добавить старые контроллеры домена в сеть, присоединив их к восстановленному контролеру домена, выполните команду:

```
samba-tool domain join <dns-realm> DC --server=<restored-dc>
```

где:

- **<dns-realm>** - имя области присоединяемого домена;
- **<restored-dc>** - имя восстановленного контроллера домена.

smbpass – графическая утилита изменения пароля доменного пользователя (MSAD или SAMBA)

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** smbpass-0.4.2-1

Smbpass – это утилита для изменения пароля пользователя в домене Windows или Samba.

Для установки программы перейдите в сеанс пользователя **root**:

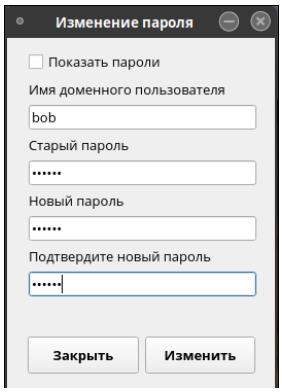
```
su -
```

и выполните команду:

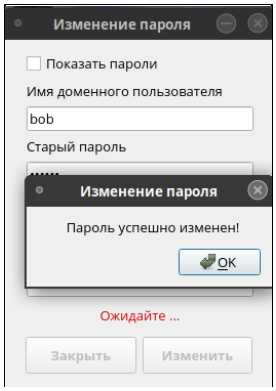
```
dnf install smbpass
```

После установки программа будет доступна из «**Главного меню**» – «**Системные**» - «**Изменение пароля доменного пользователя**».

Программа автоматически определит от имени какого доменного пользователя произошел запуск и подставит его *login* в поле «**Имя доменного пользователя**». Для изменения действующего пароля пользователя необходимо ввести текущий пароль и новый пароль с подтверждением.



Программа оповестит вас в случае успешного изменения пароля.



Сравнение функций Winbind и SSSD

Категория	Функция	Winbind	SSSD
Аутентификация	Аутентификация с использованием Kerberos	➖	➖
	Аутентификация с использованием LDAP	➖	➖
	Поддержка нескольких AD-доменов	➖	➖
	Поддержка AD-лесов	➖	➖
	Поддержка гетерогенных сред AD/FreeIPA	➕	➖
Безопасность	Простота настройки безопасной конфигурации	➕	➖
	Использование системы идентификации и ее ключа для защиты доступа к центральному серверу	➖	➖
	Поддержка NTLM	➖	➕
Поиск и сопоставление идентификаторов	Динамическое сопоставление идентификаторов AD (SID)	➖	➖
	Использование преимуществ конкретных расширений и протоколов AD	➖	➖
DNS	Обновление и очистка DNS AD	➕	➖
	Сайты DNS AD	➖	➖
Обмен файлами	Интеграция Samba FS	➖	➖
	Интеграция клиента CIFS	➖	➖
Служба печати	Сервер печати CUPS с использованием Kerberos	➖	➖
Политики	Централизованное управление контролем доступа на основе хоста через GPO	➕	➖
Интеграция на хосте с другими службами и приложениями	Интеграция с основными утилитами, такими как SSH, sudo, automount	➕	➖
	Расширенные интерфейсы идентификации по локальной шине сообщений D-Bus	➕	➖
	Специальные функции для приложений Docker, Cockpit, GSS Proxy и пр.	➕	➖

Организация отказоустойчивого кластера

Вводные данные
Предварительная подготовка кластера
Создание и настройка кластера
IPMI
STONITH

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: pcs - 0.10.14, pacemaker - 2.1.4, corosync - 3.1.6

Corosync - это программа с открытым исходным кодом, которая предоставляет возможности кластерного членства и обмена сообщениями, часто называемые уровнем обмена сообщениями, на клиентские серверы.

Pacemaker - это менеджер ресурсов кластера с открытым исходным кодом (CRM), который координирует ресурсы и службы, которые управляются и становятся доступными кластеру. По сути, *Corosync* позволяет серверам связываться как кластер, в то время как Pacemaker предоставляет возможность управлять тем, как ведет себя кластер.

Архитектура *pacemaker* состоит из трех уровней:

- *Кластеронезависимый уровень* - на этом уровне располагаются сами ресурсы и их скрипты, которыми они управляются, и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах.
- *Менеджер ресурсов* (Pacemaker), который реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Pacemaker, исходя из сложившейся ситуации, делает расчет наиболее оптимального состояния кластера и дает команды на выполнение действий для достижения этого состояния (остановка/перенос ресурсов или узлов).
- *Информационный уровень* - на этом уровне осуществляется сетевое взаимодействие узлов, т.е. передача сервисных команд (запуск/остановка ресурсов, узлов и т.д.), обмен информацией о полноте состава кластера (quorum) и т.д. На этом уровне работает Corosync.

Вводные данные

Администраторы самостоятельно определяют, какое количество нод необходимо для отказоустойчивого кластера в зависимости от ресурсов и задач. В данной статье в качестве примера будет рассмотрен кластер из двух узлов - **node1** и **node2**:

```
10.81.186.128 - node1
10.81.186.130 - node2
```

Предварительная подготовка кластера

Примечание.

Раздел «**Предварительная подготовка**» выполняется на каждом сервере.

Примечание.

Команды выполняются с правами пользователя **root**, если не указано иное.

1. Задайте имя ноды командой:

```
hostnamectl set-hostname <имя_ноды>
```

Например, задайте имя **node1**:

```
hostnamectl set-hostname node1
```

2. В файле **/etc/hosts** необходимо внести *IP* и *имя* каждой ноды, во избежание проблем с DNS, строкой вида:

```
127.0.0.1 <имя_ноды>
```

Пример файла **/etc/hosts** (добавленные строки выделены жирным шрифтом):

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

10.81.186.128 node1
10.81.186.130 node2
```

3. Установите необходимые компоненты:

```
dnf install pcs pacemaker corosync
```

4. Основная утилита управлением кластером - **pcs**. Данная утилита создает пользователя **hacluster**, для которого необходимо задать пароль:

```
passwd hacluster
```

5. Добавьте службы в автозапуск:

```
systemctl enable pcsd pacemaker corosync
```

6. Выполните запуск службы:

```
systemctl start pcsd
```

Создание и настройка кластера

1. Перед настройкой и первым запуском кластера необходимо однократно произвести авторизацию узлов в кластере:

```
pcs host auth node1 node2 -u hacluster -p password

node2: Authorized
node1: Authorized
```

2. Настройте кластер:

```
pcs cluster setup Cluster node1 node2

No addresses specified for host 'node1', using 'node1'
No addresses specified for host 'node2', using 'node2'
Destroying cluster on hosts: 'node1', 'node2'...
node2: Successfully destroyed cluster
node1: Successfully destroyed cluster
Requesting remove 'pcsd settings' from 'node1', 'node2'
node1: successful removal of the file 'pcsd settings'
node2: successful removal of the file 'pcsd settings'
Sending 'corosync authkey', 'pacemaker authkey' to 'node1', 'node2'
node2: successful distribution of the file 'corosync authkey'
node2: successful distribution of the file 'pacemaker authkey'
node1: successful distribution of the file 'corosync authkey'
node1: successful distribution of the file 'pacemaker authkey'
Sending 'corosync.conf' to 'node1', 'node2'
node1: successful distribution of the file 'corosync.conf'
node2: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.
```

3. Включите в автозагрузку и запустите кластер:

```
pcs cluster enable --all && pcs cluster start --all
```

```
node1: Cluster Enabled
node2: Cluster Enabled
node2: Starting Cluster...
node1: Starting Cluster...
```

4. Выполните следующие команды:

```
pcs property set stonith-enabled=false
pcs property set no-quorum-policy=ignore
```

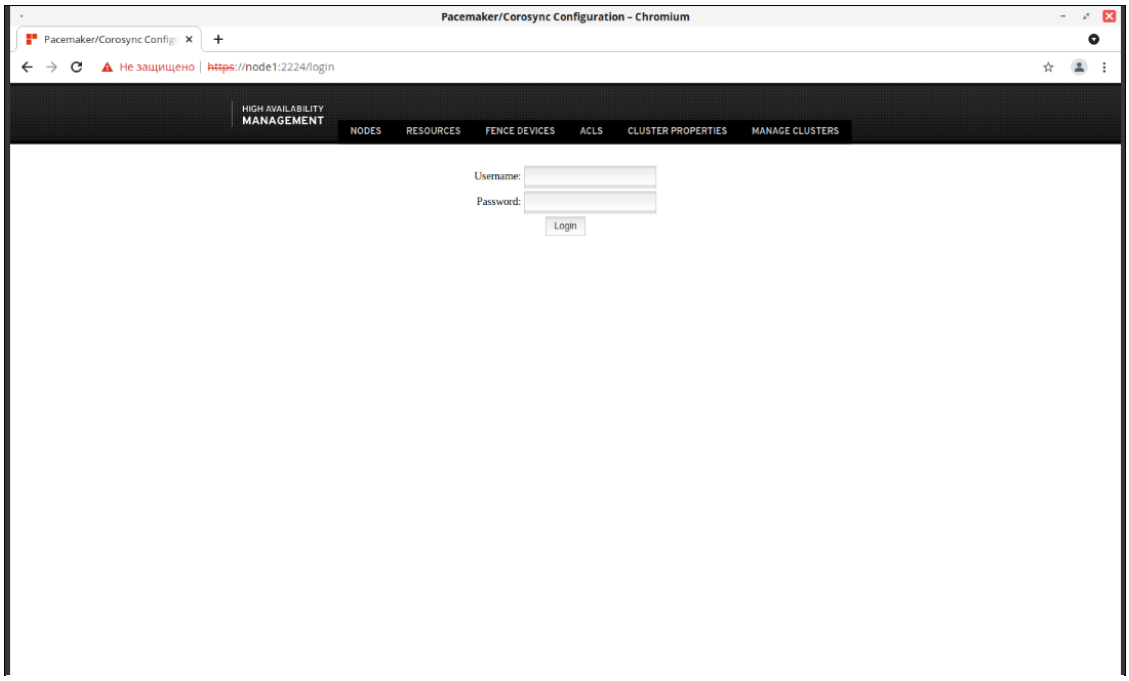
Если ноды разворачиваются на серверах с поддержкой **ipmi**, то в строке `pcs property set stonith-enabled` укажите значение `true`. **Stonith** используется для перезагрузки сервера в случае возникновения критической ошибки, которую не сможет устранить кластер.

Как настроить **ipmi** см. раздел «IPMI».

5. Проверьте состояние кластера командой:

```
pcs status

Cluster name: Cluster

WARNINGS:
No stonith devices and stonith-enabled is not false

Cluster Summary:
  * Stack: corosync
  * Current DC: node1 (version 2.1.4-1.el7-dc6eb4362e) - partition with quorum
  * Last updated: Tue Mar 28 22:17:57 2023
  * Last change:  Tue Mar 28 22:17:17 2023 by root via cibadmin on node1   * 2 nodes configured
  * 0 resource instances configured

Node List:
  * Online: [ node1 node2 ]

Full List of Resources:
  * No resources

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

Кроме консольных команд настройку кластеров можно производить также с панели администрирования, для этого в адресной строке браузера необходимо вписать **https://<имя_ноды>:2224** и авторизоваться пользователем **hacluster** с созданным ранее паролем.



IPMI

В случае возникновения критических неполадок серверов инженеры используют технологию **IPMI**. Данная технология позволяет удаленно реагировать на неполадки, вести мониторинг физического состояния оборудования и многое другое.

> **Примечание.**
>
> Настройка выполняется на каждом сервере.

Установите пакеты командой:

```
dnf install resource-agents fence-agents
```

Перед настройкой **IPMI** на серверах необходимо загрузить модули ядра. Для этого выполните следующие команды:

```
modprobe ipmi_devintf
modprobe ipmi_si
```

Затем необходимо настроить сеть на IPMI-интерфейсе в BIOS или через ОС.

Проверьте, что на интерфейсе используется статический адрес, выполните команду:

```
ipmitool lan print 1
```

Вывод команды должен иметь следующий вид:

```
IP Address Source : Static Address
```

Задайте сетевые параметры ipmi-интерфейсу, выполнив команды:

```
ipmitool lan set 1 ipsrc static <IP>
ipmitool lan set 1 netmask <netmask>
ipmitool lan set 1 defgw ipaddr <Gateway_IP>
```

Далее необходимо настроить **STONITH**.

STONITH

STONITH - метод изоляции отказавшего узла. **STONITH** изолирует неисправные узлы, перезагружая или отключая неисправный узел, чтобы он не вызывал нарушения работы кластера.

> **Примечание.**
>
> Настройка выполняется на каждом сервере.

Выведите список пользователей **ipmi** командой:

```
ipmitool user list 1

ID  Name     Callin  Link    Auth  IPMI Msg   Channel Priv Limit
2   ADMIN    false   false         true       ADMINISTRATOR
```

Вывод показывает, что существует пользователь с ID 2, следовательно, следующие идентификаторы свободны. Для примера будет создан пользователь **pcs** (по имени команды конфигурации кластера) с **ID 3** и с правами администратора для доступа. Для этого на сервере подсистем для *настройки привилегий пользователя root* необходимо выполнить следующие команды:

```
ipmitool user set name 3 pcs
ipmitool user set password 3 ipmitool channel setaccess 1 3 ipmi=on link=on callin=on privilege=4
ipmitool user priv 3 4 1
ipmitool user enable 3
```

где 3 - это **id** создаваемого пользователя и назначение ему привилегий.

Далее необходимо настроить **fence_ipmilan**, выполнив на сервере команды:

```
pcs stonith create <имя_stonith_ресурса_для_node1> fence_ipmilan auth=md5 ipaddr=<ip> passwd=******** login=pcs action=reboot pcmk_host_list=<node1> pcmk_host_check=static-list
pcs stonith create <имя_stonith_ресурса_для_node2> fence_ipmilan auth=md5 ipaddr=<ip> passwd=******** login=pcs action=reboot pcmk_host_list=<node2> pcmk_host_check=static-list
```

Для настройки **STONITH** также требуется осуществить привязку ресурсов к узлам кластера через **constraint**, которая жёстко задаёт ограничение запуска. Для этого на любом сервере выполните следующие команды:

```
pcs constraint location <имя_stonith_ресурса_для_node1> avoids node1=INFINITY
pcs constraint location <имя_stonith_ресурса_для_node2> avoids node2=INFINITY
```

Установка PostgreSQL

[Установка и настройка PostgreSQL](#)
[Ключевые моменты по работе с PostgreSQL](#)
[Дополнительные возможности для PostgreSQL](#)
[Решение проблемы](#)

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: postgresql15-15.2-3

Для установки и настройки **postgresql** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Примечание.

В наименовании пакетов и путях конфигурационных файлов для указания версии **PostgreSQL** используется число, выделенное в тексте статьи **красным цветом**.

Для **PostgreSQL 12** номер версии в названии пакета и путях к конфигурационным файлам отсутствует.

В репозитории РЕД ОС доступны следующие версии **PostgreSQL**:

- PostgreSQL 12;
- PostgreSQL 13;
- PostgreSQL 14;
- PostgreSQL 15.
- PostgreSQL 16.

Установка и настройка PostgreSQL

Для установки **postgresql** выполните команду:

```
dnf install postgresql15-server
```

Далее необходимо произвести инициализацию базы данных **postgresql**:

```
postgresql-15-setup initdb
```

После успешной инициализации запустите службу **postgresql** и добавьте ее в автозагрузку:

```
systemctl enable postgresql-15.service --now
```

Убедитесь, что служба запущена:

```
systemctl status postgresql-15.service
```

В статусе должно отображаться **active (running)**.

Ключевые моменты по работе с PostgreSQL

Авторизуйтесь пользователем **postgres**:

```
su - postgres
```

Для запуска **postgres shell** (запускается только от пользователя **postgres**) выполните:

```
psql
```

Тестовый запрос на получение списка баз данных производится командой (символ "\" также необходимо вводить):

```
\l
```

Тестовый запрос на получение списка таблиц производится командой:

```
\dt *
```

Для выхода из оболочки **postgres shell** выполните:

```
\q
```

Для выхода из текущей учетной записи **postgres** выполните:

```
exit
```

Дополнительные возможности для PostgreSQL

Для расширения возможностей **PostgreSQL** можно подключить каталог **contrib**. В нем содержатся модули, среди которых есть средства портирования, утилиты анализа и подключаемые функции, не включенные в состав основной системы **PostgreSQL**.

ВАЖНО!

Данные модули не включены в **PostgreSQL**, потому что они адресованы ограниченной аудитории или находятся в экспериментальном состоянии, не подходящем для основного дерева кода.

Для подключения каталога **contrib** выполните команду:

```
dnf install postgresql15-contrib
```

Решение проблемы: после установки не удается подключиться к PostgreSQL через pgadmin4

Откройте для редактирования файл **postgresql.conf**:

```
nano /var/lib/pgsql/15/data/postgresql.conf
```

Замените строку:

```
# listen_addresses = 'localhost'
```

на следующую:

```
listen_addresses = '*'
```

В файл **/var/lib/pgsql/15/data/pg_hba.conf** в качестве первой строки добавьте следующее:

```
host all all 0.0.0.0/0 md5
```

Данный параметр разрешает доступ ко всем базам данных для всех пользователей с зашифрованным паролем.

Далее необходимо задать пароль пользователю **postgres** для администрирования баз данных на сервере удаленно.

```
su - postgres
psql
ALTER USER postgres WITH ENCRYPTED PASSWORD 'yourpassword';
```

где вместо **yourpassword** укажите нужный пароль.

Для применения внесенных изменений в настройки требуется перезапустить службу **postgresql**:

```
systemctl restart postgresql-15.service
```

Для более гибкой настройки прав доступа рекомендуем обратиться к официальной документации разработчика программного обеспечения.

Установка Firebird

Установка Firebird 2.5
Установка Firebird 3.0

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** firebird 3.0.6.33328-1, firebird 2.5.9.27139.0-1

Установка Firebird 2.5

Установка осуществляется командой:

```
# dnf install firebird25
```

Для запуска **firebird** выполните команду:

```
# systemctl start firebird25-classic.socket
```

Проверка статуса службы выполняется командой:

```
$ systemctl status firebird25-classic.socket
```

Автозапуск **firebird** при запуске ОС осуществляется командой:

```
# systemctl enable firebird25-classic.socket
```

Основные файлы конфигурации будут находиться в каталоге **/etc/firebird25**, а утилиты в **/usr/lib64/firebird25/bin-classic**.

Установка Firebird 3.0

Для установки **firebird 3.0** выполните команду:

```
# dnf  install firebird
```

Для запуска **firebird** выполните команду:

```
# systemctl start firebird-superserver.service
```

Проверка статуса службы:

```
$ systemctl status firebird-superserver.service
```

Автозапуск **firebird** при запуске ОС осуществляется командой:

```
# systemctl enable firebird-superserver.service
```

Установка СУБД Ред База Данных

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** 3.0.10.0 RedDatabase

СУБД Ред База Данных (Red Database) – промышленная российская система управления базами данных с открытым кодом. Ядро СУБД Ред База Данных построено на основе одной из самых известных и распространенных в мире СУБД с открытым кодом – Firebird, которая используется в решениях.

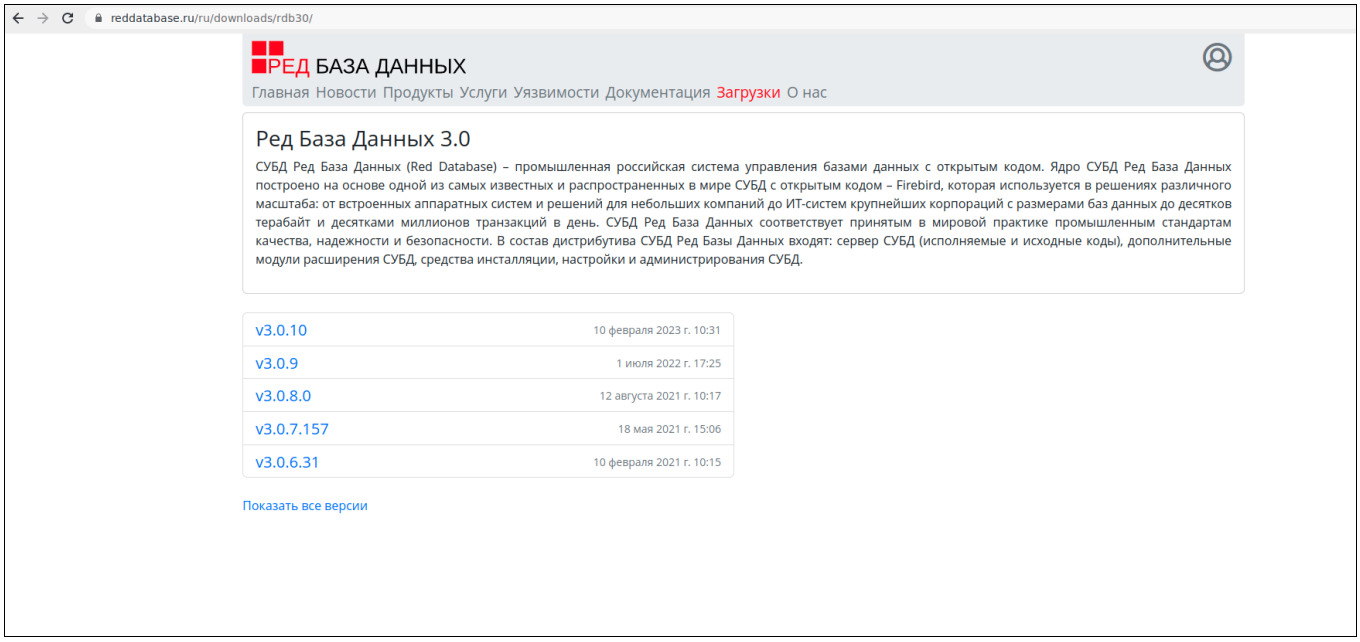
Вы можете подробнее ознакомиться с установкой **СУБД РЕД База Данных**, а также пройти обучающий курс по работе с **СУБД РЕД База Данных**, просмотрев наши обучающие видео:

- на **RuTube**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».
- в **Яндекс.Дзен**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».
- в **VK Видео**:
  - Установка СУБД Ред База Данных на РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Скачивание СУБД Ред База Данных

Скачать Red Database можно на официальном сайте - https://reddatabase.ru/downloads/rdb30/.



Для скачивания необходимо авторизоваться или зарегистрироваться.

Для установки на Linux необходимо скачать бинарный файл нужной разрядности и назначить на него права:

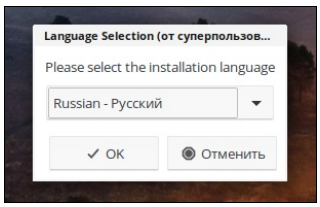
```
sudo chmod +x [путь до файла]
```

Для старта установки запускаем установочный бинарный файл:

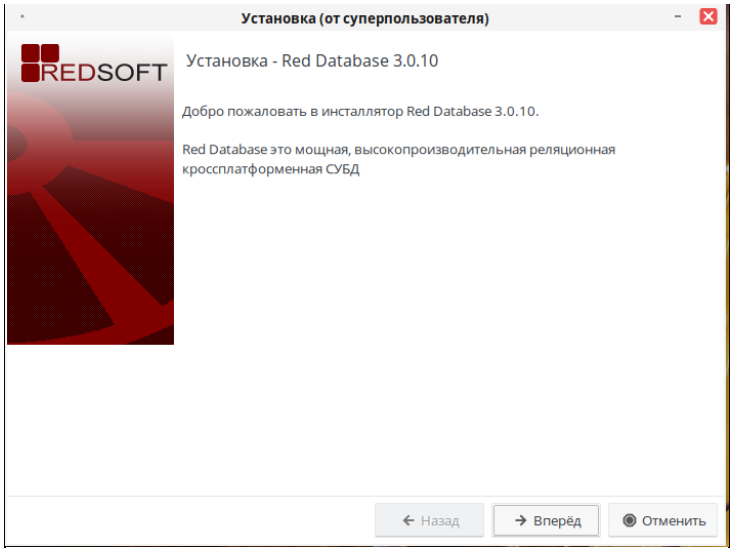
```
sudo ./rdb30-linux-x86_64-enterprise-3.0.10.bin
```

Установка

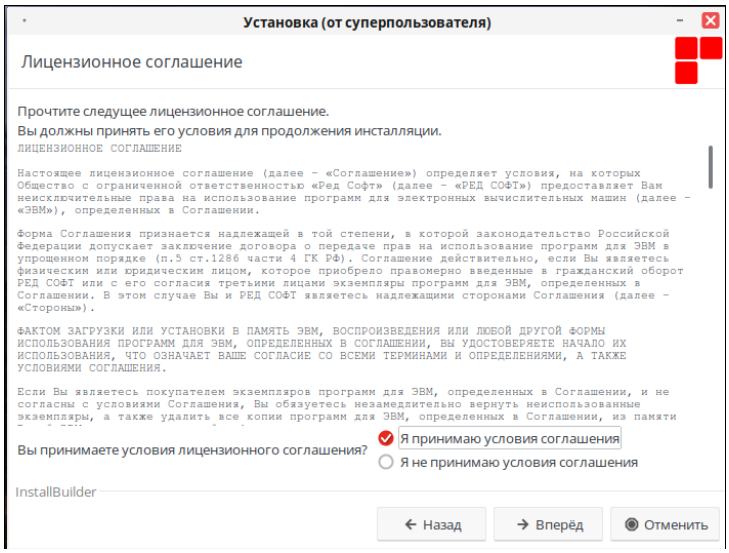
Выбор языка установки



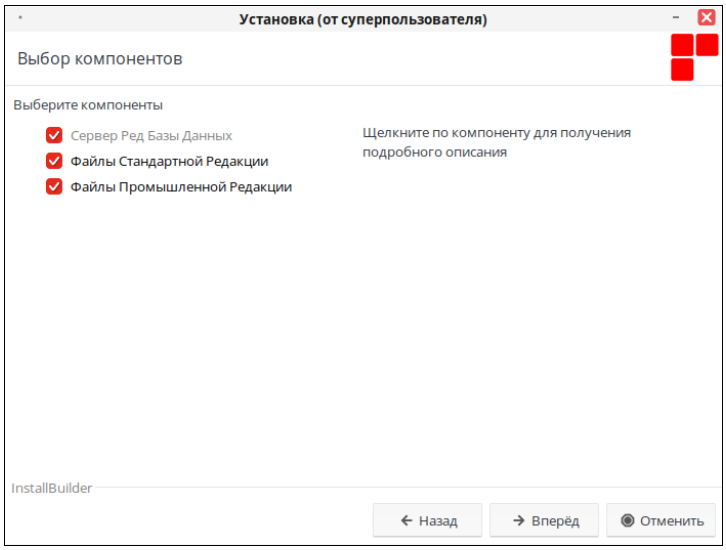
Нажмите вперед, для начала установки.



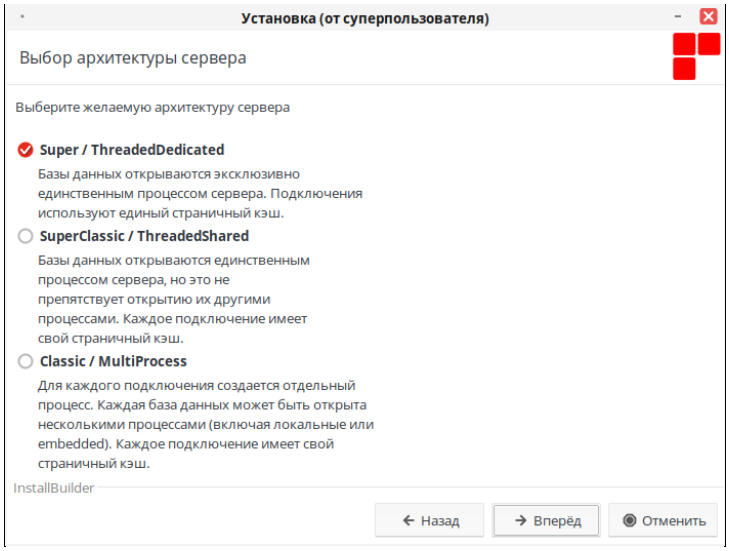
Необходимо принять условия лицензионного соглашения, перед этим прочитайте его.



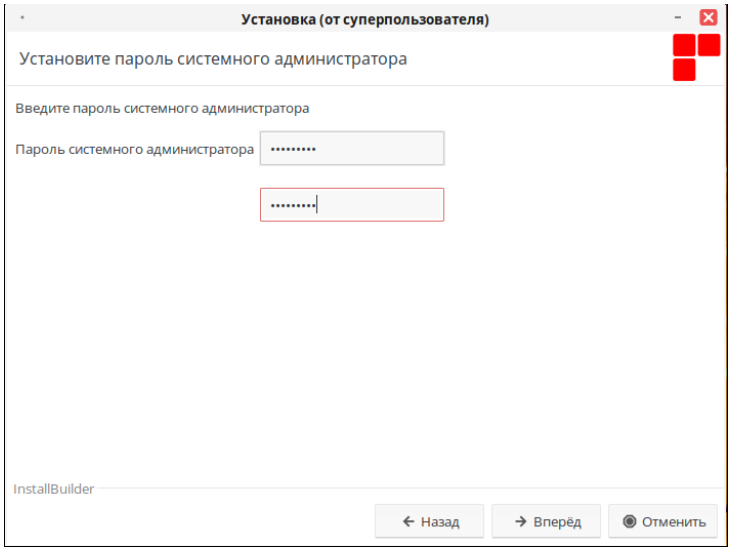
Выбор компонентов в зависимости от доступной редакции СУБД



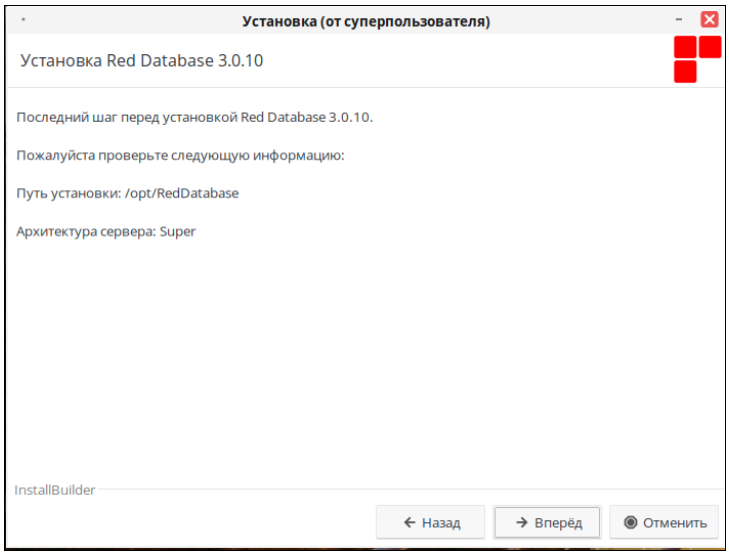
Выбор архитектуры



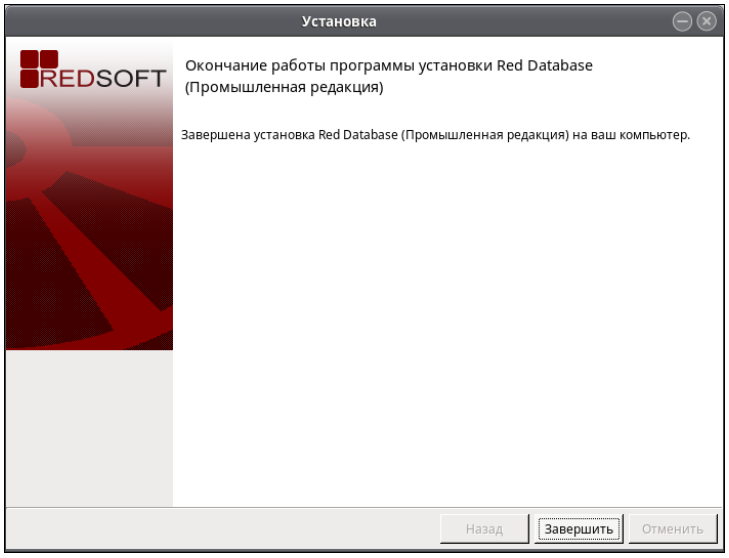
Пароль администратора, необходимо дважды указать пароль администратора.



Вывод выбранной информации.



После окончания установки необходимо нажать **"Завершить".**



Кратко об основных каталогах и файлах конфигурации.

По умолчанию все каталоги и файлы создаются в /opt/RedDatabase

/opt/RedDatabase/firebird.conf - Файл содержит параметры настройки сервера. Сервер читает все настройки с этого файла при старте (больше про настройку сервера можно прочитать в документации*)

/opt/RedDatabase/databases.conf – В этом текстовом файле можно задать алиас БД, чтобы затем в прикладных кодах использовать более короткий и удобный псевдоним для обращения к нужной базе данных. Также здесь указываются индивидуальные настройки для каждой конкретной базы данных.

Так же в каталоге /opt/RedDatabase/bin находятся утилиты для взаимодействия с БД и ее управлением.

pgAdmin4 - администрирование и разработка баз данных

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** pgadmin4-6.19-4

pgAdmin4 - это программный продукт для администрирования и разработки баз данных *PostgreSQL*. **pgAdmin4** позволяет выполнять задачи мониторинга, обслуживания, конфигурирования сервера *PostgreSQL*, а также создавать и выполнять SQL-запросы.

Для установки **pgAdmin4** перейдите в сеанс пользователя **root**:

```
su -
```

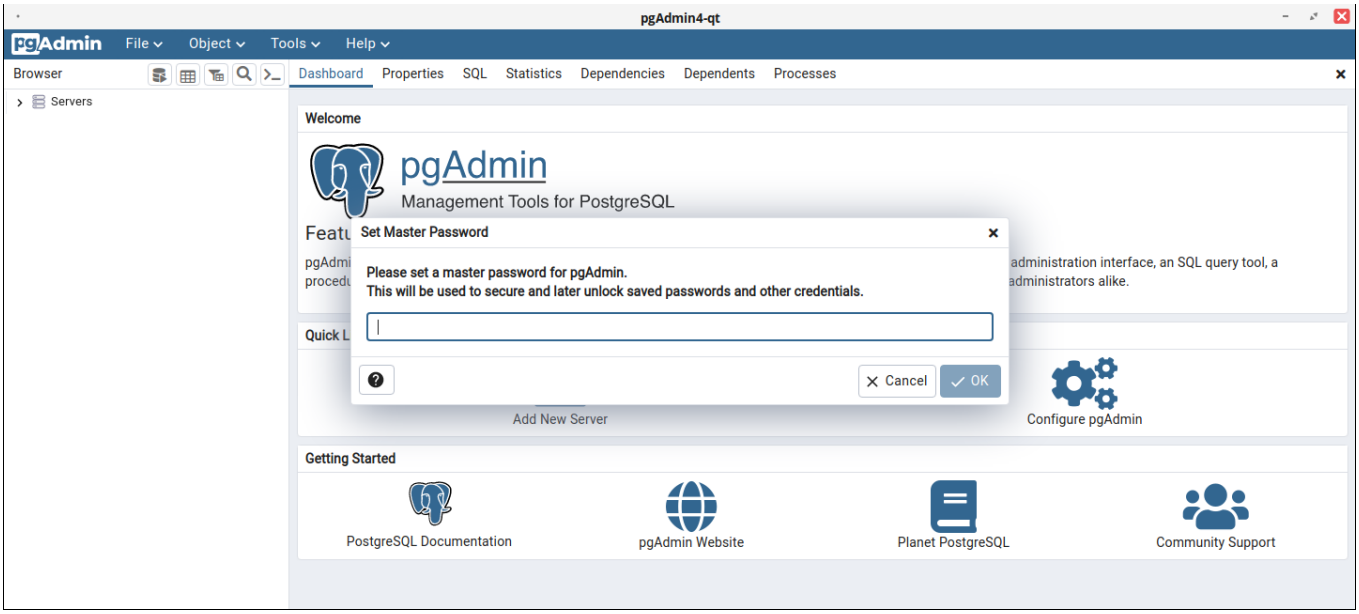
и выполните команду:

```
dnf install pgadmin4 pgadmin4-qt
```

В результате **pgAdmin4** будет доступен в **Главном меню** - «**Программирование**» - «**pgAdmin 4**».

При первом входе необходимо ввести пароль от учетной записи **root** или, при нажатии на кнопку «**Reset master Password**», установить собственный пароль для **pgadmin**.

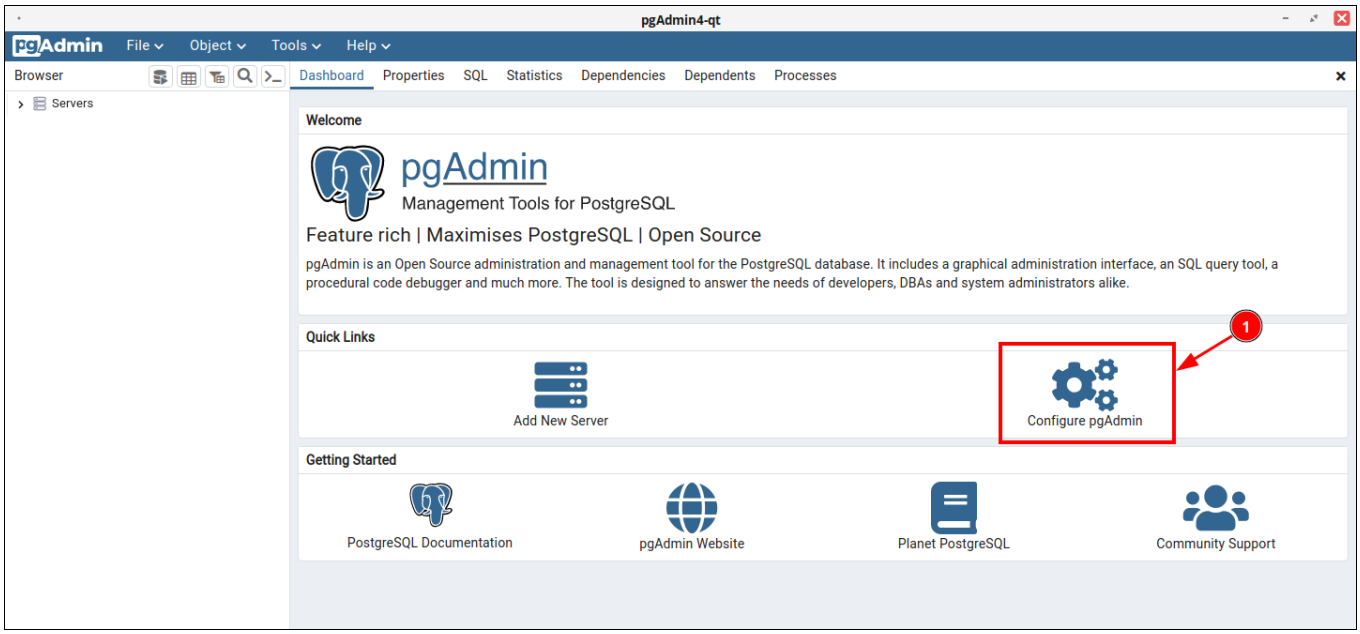
После авторизации в панели управления появится возможность настроить подключение к базам данных *PostgreSQL*.



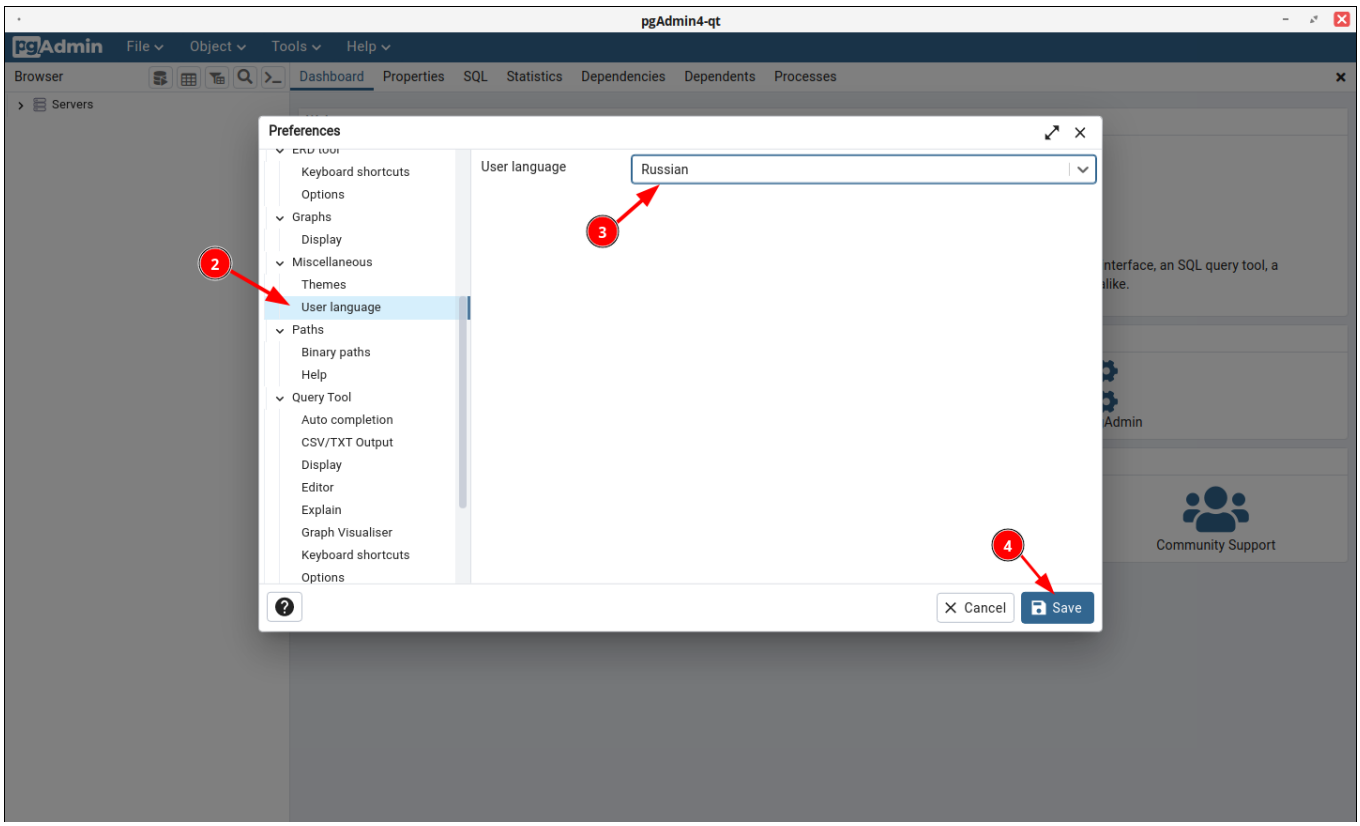
Для удобства работы можно изменить язык программы. Для этого сначала необходимо установить дополнительный пакет:

```
dnf install pgadmin4-langpack-ru
```

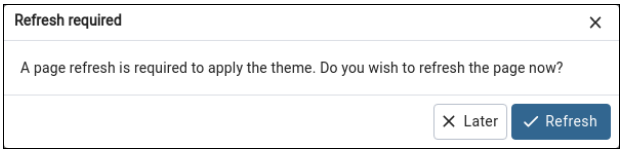
Затем на панели управления нужно выбрать «**Configure pgAdmin**».



И перейти на вкладку «**User language**», где в выпадающем списке выбрать русский язык.



После этого появится уведомление, и язык интерфейса изменится на выбранный.



В данной установке и настройке **pgAdmin4** работает только локально и нет возможности подключиться к нему с других ПК к панели администрирования.

Чтобы настроить **pgAdmin4** в качестве внешнего веб-сервиса с возможностью подключения к веб-панели **pgAdmin4** с других ПК, необходимо выполнить ряд настроек и установить дополнительные RPM-пакеты из репозитория РЕД ОС.

Настройка pgAdmin4 в качестве внешнего web-сервиса

Обратите внимание, что после настройки **pgAdmin4** в качестве внешнего веб-сервиса, графическое приложение **pgadmin4-qt** будет недоступно.

Установите дополнительные пакеты:

```
dnf install httpd python3-mod_wsgi pgadmin4-httpd
```

Создайте необходимые каталоги:

```
mkdir -p /var/log/pgadmin4/
```

Затем настройте **selinux**:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_can_network_connect_db 1
semanage fcontext -a -t httpd_sys_rw_content_t "/var/lib/pgadmin4(/.*)?"
semanage fcontext -a -t httpd_sys_rw_content_t "/var/log/pgadmin4(/.*)?"
restorecon -R /var/lib/pgadmin4/
restorecon -R /var/log/pgadmin4/
```

Запустите сервис **httpd**:

```
systemctl enable httpd --now
```

Откройте файл конфигурации для редактирования:

```
nano /usr/lib/pgadmin4/config_local.py
```

и приведите его к следующему виду:

```
import os
 from config import *
 HELP_PATH = '/usr/share/doc/pgadmin4/html/'
 DATA_DIR = os.path.realpath(os.path.expanduser(u'/var/lib/pgadmin4'))
 LOG_FILE = os.path.join(DATA_DIR, 'pgadmin4.log')
 SQLITE_PATH = os.path.join(DATA_DIR, 'pgadmin4.db')
 SESSION_DB_PATH = os.path.join(DATA_DIR, 'sessions')
 STORAGE_DIR = os.path.join(DATA_DIR, 'storage')
 AZURE_CREDENTIAL_CACHE_DIR = os.path.join(DATA_DIR, 'azurecredentialcache')
 KERBEROS_CCACHE_DIR = os.path.join(DATA_DIR, 'krbccache')
 TEST_SQLITE_PATH = os.path.join(DATA_DIR, 'test_pgadmin4.db')
```

Выполните команду настройки **pgadmin4**, при этом нужно будет ввести *адрес почты* и *пароль*:

```
python /usr/lib/pgadmin4/setup.py
```

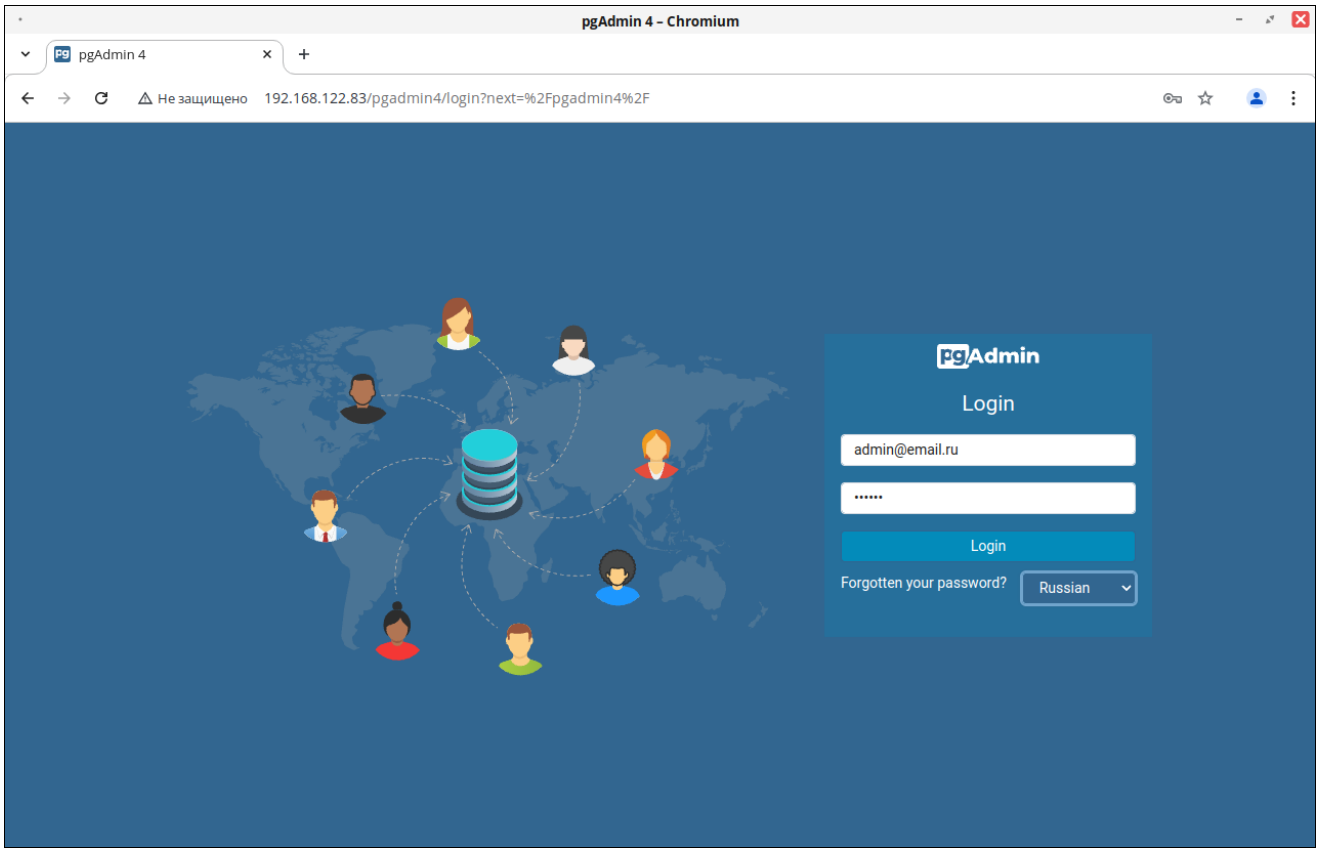
После этого выполните команду смены владельца для каталогов:

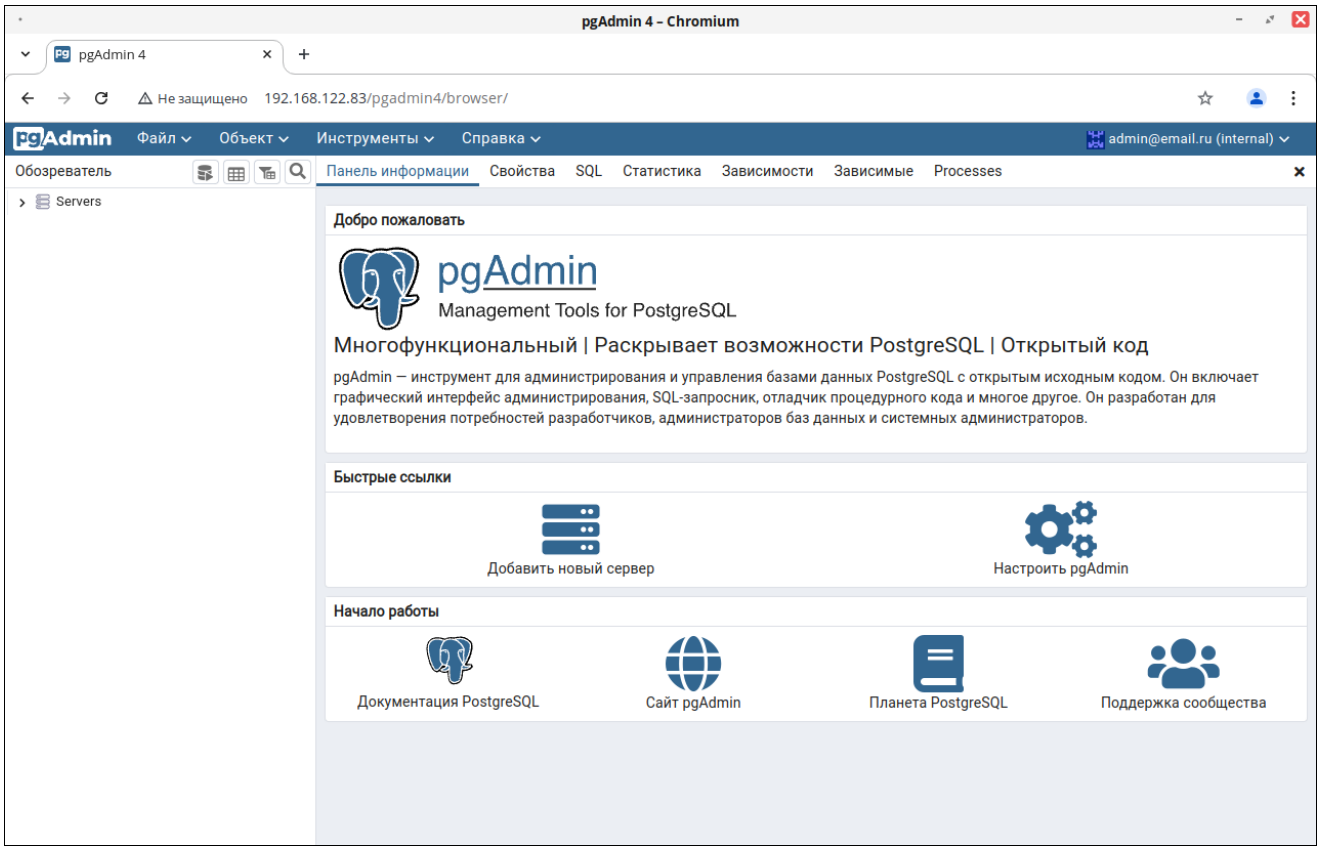
```
chown -R apache:apache /var/lib/pgadmin4 /var/log/pgadmin4
```

После чего перезапустите веб-службу:

```
systemctl restart httpd
```

После этих действий **pgadmin4** будет доступен в браузере через веб-интерфейс по адресу вашего сервера, например: http://<IP-адрес_сервера>/pgadmin4.


pgAdmin 4 – Chromium
pgAdmin 4
Не защищено
192.168.122.83/pgadmin4/login?next=%2Fpgadmin4%2F
pgAdmin
Login
admin@email.ru
Login
Forgotten your password?
Russian


pgAdmin 4 – Chromium
pgAdmin 4
Не защищено
192.168.122.83/pgadmin4/browser/
pgAdmin
Файл
Объект
Инструменты
Справка
admin@email.ru (internal)
Обозреватель
Servers
Панель информации
Свойства
SQL
Статистика
Зависимости
Зависимые
Processes
Добро пожаловать
pgAdmin
Management Tools for PostgreSQL
Многофункциональный | Раскрывает возможности PostgreSQL | Открытый код
pgAdmin — инструмент для администрирования и управления базами данных PostgreSQL с открытым исходным кодом. Он включает графический интерфейс администрирования, SQL-запросник, отладчик процедурного кода и многое другое. Он разработан для удовлетворения потребностей разработчиков, администраторов баз данных и системных администраторов.
Быстрые ссылки
Добавить новый сервер
Настроить pgAdmin
Начало работы
Документация PostgreSQL
Сайт pgAdmin
Планета PostgreSQL
Поддержка сообщества

Настройка Postgresql для 1С

Вы можете подробнее ознакомиться с настройкой **postgresql**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка сервера баз данных для сервера 1С;
- в **Яндекс.Дзен** — Настройка сервера баз данных для сервера 1С;
- в **VK Видео** — Настройка сервера баз данных для сервера 1С.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка postgresql

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Измените имя сервера:

```
hostnamectl set-hostname serv.1ctest.ru
```

где **serv.1ctest.ru** - нужное имя вашего сервера.

Отредактируйте **/etc/hosts**:

```
nano /etc/hosts
```

Добавьте строку:

```
127.0.0.1 serv.1ctest.ru
```

Установка

Установка **postgresql** для 1С:

```
dnf install postgresql-1c postgresql-1c-contrib postgresql-1c-libs postgresql-1c-plperl postgresql-1c-plpython3 postgresql-1c-pltcl postgresql-1c-server
```

Настройка **postgresql**:

```
su - postgres
```

Откройте файл, в котором будут заданы необходимые переменные окружения:

```
nano .bash_profile
```

> **Примечание.**
>
> Необходимо указать вашу версию **postgresql** (выделена красным цветом).

Добавляем в этот файл переменные:

```
export PATH=/usr/pgsql-14/bin:$PATH
export MANPATH=/usr/pgsql-14/share/man:$MANPATH
```

Пример листинга файла:

```
[ -f /etc/profile ] && source /etc/profile
PGDATA=/var/lib/pgsql/14/data export PGDATA
# If you want to customize your settings,
```

```
# Use the file below. This is not overridden
# by the RPMS.

export PATH=/usr/pgsql-14/bin:$PATH
export MANPATH=/usr/pgsql-14/share/man:$MANPATH

[ -f /var/lib/pgsql/.pgsql_profile ] && source /var/lib/pgsql/.pgsql_profile
```

Далее с правами того же пользователя **postgres** выполните команду инициализации БД:

> **Примечание.**
>
> **Минимальный объём** оперативной памяти для инициализации БД - **4 ГБ**.

```
initdb
```

Если команда не найдена, пропишите полный путь:

```
/usr/pgsql-14/bin/initdb
```

Выйдите из текущей учетной записи:

```
exit
```

Запуск и добавление в автозагрузку сервера **PostgreSQL**:

```
systemctl enable postgresql-14 --now
```

Проверка статуса сервиса:

```
systemctl status postgresql-14
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Изменение настроек сервера PostgreSQL

Для возможности пользователю **postgres** авторизоваться по паролю, внесите изменения в файл **/var/lib/pgsql/14/data/pg_hba.conf**:

```
nano /var/lib/pgsql/14/data/pg_hba.conf
```

```
host all all 0.0.0.0/0 trust

на

host all all 0.0.0.0/0 md5
```

Внесите изменения в файл **/var/lib/pgsql/14/data/postgresql.conf**, исходя из характеристик сервера:

```
nano /var/lib/pgsql/14/data/postgresql.conf
```

> **Примечание.**
>
> Подбор данных настроек производится индивидуально и зависит как от характеристик сервера, на котором будет работать сервер **PostgreSQL**, так и от характеристик информационных баз, которые будут обрабатываться на этом сервере.

Параметры, требующие настройки:

```
listen_addresses = '*'
```

```
password_encryption = md5
shared_buffers = 4096MB
temp_buffers = 256MB
work_mem = 128MB
maintenance_work_mem = 192MB
effective_cache_size = 4GB
```

Задайте пароль пользователю **postgres**, для того чтобы была возможность подключаться к серверу удаленно.

```
su - postgres
psql
ALTER USER postgres WITH ENCRYPTED PASSWORD 'yourpassword';
(вместо yourpassword поставьте нужный пароль)
```

Рестарт сервера **PostgreSQL**:

```
systemctl stop postgresql-14
systemctl start postgresql-14
systemctl status postgresql-14
```

1С-сервер для РЕД ОС 7.3

Установка 1С-сервера для РЕД ОС 7.3
Запуск сервиса для версии сервера 8.3.21.xxxx
Администрирование 1С

Вы можете подробнее ознакомиться с установкой и настройкой сервера 1С, просмотрев наши обучающие видео:

- на **RuTube** — Настройка сервера баз данных для сервера 1С;
- в **Яндекс.Дзен** — Настройка сервера баз данных для сервера 1С;
- в **VK Видео** — Настройка сервера баз данных для сервера 1С.

На наших каналах вы также сможете найти много другой полезной информации.

Установка 1С-сервера для РЕД ОС 7.3

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Перед началом установки сервера необходимо поставить последние обновления РЕД ОС.

```
dnf update
```

> **Примечание.**
>
> Для РЕД ОС 7.3 **рекомендуется** использовать сервер 1С:Предприятия **8.3.20.xxxx и выше**.

Загрузите дистрибутив 1С, который был запрошен у производителя для linux (***данные пакеты не являются нашей разработкой и, соответственно, отсутствуют в репозитории РЕД ОС***).

Установите дополнительные пакеты шрифтов:

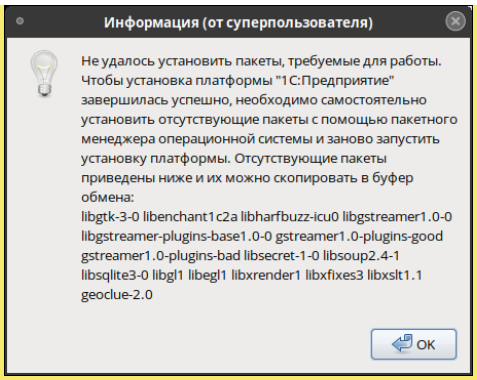
```
dnf install libxcrypt-compat msttcore-fonts-installer
```

Начиная с версии **8.3.20.xxxx**, фирма 1С изменила формат распространения дистрибутива для Linux-систем. Теперь он распространяется в формате **run**. Для установки сервера run-файл требуется сделать исполняемым, запустить и доустановить пакеты из репозитория:

```
chmod +x setup-full-8.3.21.1197-x86_64.run
./setup-full-8.3.21.1197-x86_64.run --mode unattended --disable-components client_full --enable-components
server,ws,server_admin,config_storage_server,liberica_jre
```

Будет произведена установка всех необходимых компонентов и модулей без отображения диалоговых окон установщика.

> **Примечание.**
>
> Если вы используете графический вариант установки сервера 1С, будет выведено предупреждение о возможных отсутствующих дополнительных пакетах. **Данное сообщение не является ошибкой!**



Запуск сервиса для версии сервера 8.3.21.xxxx

После установки необходимо создать ссылку на сервис сервера 1С:

```
systemctl link /opt/1cv8/x86_64/8.3.21.1197/srv1cv8-8.3.21.1197@.service
```

Запустите сервис и добавьте его в автозагрузку командой:

```
systemctl enable srv1cv8-8.3.21.1197@default.service --now
```

Команда проверки статуса сервиса:

```
systemctl status srv1cv8-8.3.21.1197@default.service
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Администрирование 1С

Настройка 1С-сервера производится через консоль администратора 1С.

Сначала запустите кластер серверов 1С следующей командой:

```
/opt/1cv8/x86_64/8.3.21.1197/ras --daemon cluster
```

Для получения информации о кластере в терминале введите команду:

```
/opt/1cv8/x86_64/8.3.21.1197/rac cluster list
```

Листинг информации:

```
cluster : 163e5d4d-152a-4584-a176-48109eb261f6
 host : ro731serv1c83211197
 port : 1541
 name : "Локальный кластер"
 expiration-timeout : 60
 lifetime-limit : 0
 max-memory-size : 0
 max-memory-time-limit : 0
 security-level : 0
 session-fault-tolerance-level : 0
 load-balancing-mode : performance
 errors-count-threshold : 0
 kill-problem-processes : 1
 kill-by-memory-with-dump : 0
```

Для дальнейших операций сохраните себе название кластера «**163e5d4d-152a-4584-a176-48109eb261f6**». Вместо элементов,

выделенных красным цветом, вставьте свои параметры.

Добавление базы производится командой:

```
/opt/1cv8/x86_64/8.3.21.1197/rac infobase --cluster=163e5d4d-152a-4584-a176-48109eb261f6 create --create-database --name=test_bd --dbms=PostgreSQL --db-server=ro731serv1c83211197 --db-name=test_bd --locale=ru --db-user=postgres --db-pwd=yourpassword  --license-distribution=allow
```

При добавлении новой базы данных может появиться ошибка вида:

```
Ошибка операции администрирования
Сервер баз данных не обнаружен
authentication method 10 not supported
```

Для решения данной проблемы необходимо:

1. В конфигурационном файле **postgresql.conf** скорректировать настройку **password_encryption** на **md5** вместо **scram-sha-256**:

```
password_encryption = md5  # scram-sha-256 or md5
```

2) Перезапустить службу **postgresql**:

```
systemctl restart postgresql-14
```

где **postgresql-14** - служба для РЕД ОС 7.3, .

3) Установить (Обновить) пароль пользователя, с правами которого настраивается подключение к **postgresql**. Ниже приведен пример для пользователя **postgres**:

```
su - postgres
psql
ALTER USER postgres WITH ENCRYPTED PASSWORD 'yourpassword';
```

где **yourpassword** - установленный вами пароль.

Краткая информация о параметрах команды:

Параметр	Описание
--create-database	При создании информационной базы создать базу данных
--name=<name>	(**обязательный**) имя информационной базы
--dbms=MSSQLServer | PostgreSQL | IBMDB2 | OracleDatabase	(**обязательный**) тип СУБД, в которой размещается информационная база: • *MSSQLServer* — MS SQL Server; • *PostgreSQL* — PostgreSQL; • *IBMDB2* — IBM DB2; • *OracleDatabase* — Oracle Database.
--db-server=<host>	(**обязательный**) имя сервера баз данных
--db-name=<name>	(**обязательный**) имя базы данных
--locale=<locale>	(**обязательный**) идентификатор национальных настроек информационной базы
--b-user=<name>	имя администратора базы данных
--db-pwd=<pwd>	пароль администратора базы данных
--descr=<descr>	описание информационной базы
--date-offset=<offset>	смещение дат в информационной базе
--security-level=<level>	уровень безопасности установки соединений с информационной базой
--scheduled-jobs-deny=on | off	управление блокировкой выполнения регламентных заданий: • *on* — выполнение регламентных заданий запрещено; • *off* — выполнение регламентных заданий разрешено.
--license-distribution=deny | allow	управление выдачей лицензий сервером 1С:Предприятия: • deny — выдача лицензий запрещена; • allow — выдача лицензий разрешена.

Для получения списка баз введите в терминале команду:

```
/opt/1cv8/x86_64/8.3.21.1197/rac infobase --cluster=163e5d4d-152a-4584-a176-48109eb261f6 summary list
```

Пример вывода:

```
infobase : 8a3f7235-37c7-403f-bd3c-bce5a8d9b40a
name : test_bd
descr :
```

Для удаления БД введите команду:

```
/opt/1cv8/x86_64/8.3.21.1197/rac infobase --cluster=163e5d4d-152a-4584-a176-48109eb261f6 drop --infobase=8a3f7235-37c7-403f-bd3c-bce5a8d9b40a
```

Не забудьте также удалить базу из **postgresql**:

```
su postgres
psql
\l
DR OP DATABASE test_bd;
\q
```

Публикация БД на web-сервере 1С

Подготовка веб-сервера
Установка 1С
Публикация БД

Примечание.

Для публикации базы на веб-сервере у вас уже должна быть подготовлена и настроена БД на сервере 1С.

Подготовка веб-сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Установите **apache**:

```
dnf install httpd
```

Настройте SELinux:

```
setsebool -P httpd_can_network_connect on
```

Запустите и добавьте в автозагрузку веб-сервер:

```
systemctl enable httpd --now
```

Статус службы веб-сервера можно проверить командой:

```
systemctl status httpd
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Далее необходимо проверить корректность работы **apache**. Для этого создайте в каталоге **/var/www/html/** файл **index.html** с любым содержанием, например, «**Page available**».

```
nano /var/www/html/index.html
```

Для сохранения внесенных изменений нажмите «**Ctrl+O**», «**Enter**» и для выхода из редактора - «**Ctrl+X**».

Установите имя веб-сервера:

```
hostnamectl set-hostname ro731webserv1c83211197
```

где **ro731webserv1c83211197** - нужное имя сервера.

Измените файл **/etc/hosts**, добавьте ip-адрес веб-сервера и его имя:

```
nano /etc/hosts
```

```
10.1.10.1 ro731webserv1c83211197
```

(вместо **10.1.10.1** введите IP-адрес вашего веб-сервера, а вместо **ro731webserv1c83211197** имя вашего веб-сервера).

Если БД находится на другом сервере, в **/etc/hosts** также необходимо прописать IP-адрес и имя сервера расположения базы.

Проверим доступность станицы http://ro731webserv1c83211197/ в браузере, где **ro731webserv1c83211197** - имя вашего веб-сервера.

Установка 1С

Загрузите дистрибутив 1С, который был запрошен у производителя для linux (***данные пакеты не являются нашей разработкой и, соответственно, отсутствуют в репозитории РЕД ОС***).

Установите дополнительные пакеты и назначьте run-файлу права на исполнение:

```
dnf install libxcrypt-compat msttcore-fonts-installer
chmod +x setup-full-8.3.21.1197-x86_64.run
```

Для запуска установки выполните команду:

```
./setup-full-8.3.21.1197-x86_64.run --mode unattended --disable-components client_full --enable-components
server,ws,server_admin,config_storage_server,liberica_jre
```

Публикация БД

После завершения установки перейдите в каталог 1С:

```
cd /opt/1cv8/x86_64/8.3.21.1197
```

Опубликуйте базу на веб-сервере командой:

```
./webinst -apache24 -wsdir test_bd -dir /var/www/test_bd -connstr "Srvr=ro731serv1c83211197;Ref=test_bd;" -confPath
/etc/httpd/conf/httpd.conf
```

(где **ro731serv1c83211197** - имя сервера расположения базы, которую вы хотите опубликовать, **test_bd** - имя вашей базы, которую вы хотите опубликовать, а **/var/www/test_bd** - каталог, в котором будет содержаться конфигурационный файл веб-клиента, он должен обязательно располагаться в **/var/www**).

Проверьте, что в конфигурационном файле **apache** появилась необходимая запись о загрузке:

```
nano /etc/httpd/conf/httpd.conf
```

Для версии **8.3.21.1197** запись в конце файла будет выглядеть:

```
LoadModule _1cws_module "/opt/1cv8/x86_64/8.3.21.1197/wsap24.so"
```

Добавьте в тот же файл строку:

```
ServerName ro731webserv1c8321119
```

(где **ro731webserv1c8321119** - имя вашего веб-сервера).

Параметры веб-сервера можно менять в файле **default.vrd**. В примере каталогом расположения данного файла будет **/var/www/test_bd**.

Проверка синтаксиса конфигурационных файлов **apache** осуществляется командой:

```
apachectl -t
```

Перезапустите **apache**:

```
systemctl restart httpd
```

Перезагрузите компьютер.

После перезагрузки сервера, если всё было настроено правильно, доступ к БД можно будет получить из браузера или через приложение, указав адрес http://ro731webserv1c8321119/test_bd, (где **ro731webserv1c8321119** - имя вашего веб-сервера, **test_bd** - имя вашей публикуемой базы).

1С-клиент

Установка клиента 1С
Подключение к БД
Установка драйвера ключа аппаратной лицензии
Решение возникающих проблем
Возможные проблемы при установке пакетов
Возможные проблемы при запуске программы

Вы можете подробнее ознакомиться с установкой и настройкой клиента 1С, просмотрев наши обучающие видео:

- на **RuTube** — Настройка сервера баз данных для сервера 1С;
- в **Яндекс.Дзен** — Настройка сервера баз данных для сервера 1С;
- в **VK Видео** — Настройка сервера баз данных для сервера 1С.

На наших каналах вы также сможете найти много другой полезной информации.

Установка клиента 1С

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Загрузите дистрибутив 1С, который был запрошен у производителя для linux (***данные пакеты не являются нашей разработкой и, соответственно, отсутствуют в репозитории РЕД ОС***).

Установка производится командой:

```
dnf install 1c-enterprise-8.3.19.1522-client-8.3.19.1522.x86_64.rpm 1c-enterprise-8.3.19.1522-common-8.3.19.1522.x86_64.rpm 1c-enterprise-8.3.19.1522-server-8.3.19.1522.x86_64.rpm
```

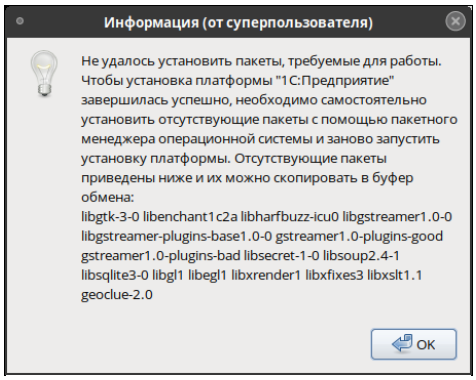
Начиная с версии **8.3.20.xxxx**, 1С:Предприятие для Linux распространяется в формате **run**, поэтому алгоритм установки отличается.

Для установки необходимо назначить run-файлу права на исполнение и запустить его:

```
chmod +x setup-full-8.3.21.1197-x86_64.run
./setup-full-8.3.21.1197-x86_64.run
```

Затем нужно следовать инструкциям в менеджере установки 1С.

При установке будет выведено предупреждение о возможных отсутствующих дополнительных пакетах (**не является ошибкой!**).



Установите необходимые шрифты:

```
dnf install msttcore-fonts-installer
```

Измените файл **/etc/hosts**, добавьте ip-адрес вашего сервера и его имя:

```
nano /etc/hosts
```

```
45.14.51.45 serv.1ctest.ru
```

где **45.14.51.45** - IP-адрес вашего сервера.

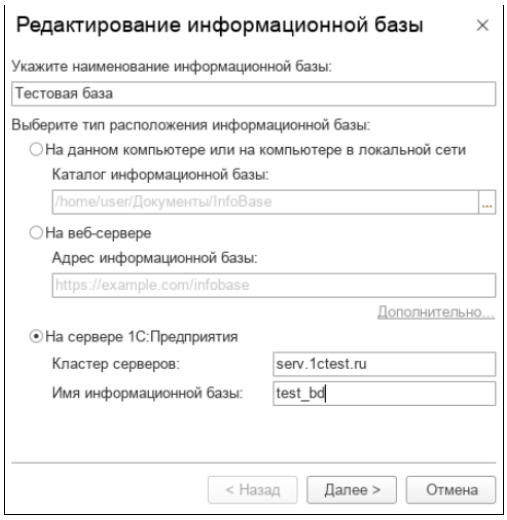
Перезагрузите систему. **После перезагрузки** установленная программа будет доступна в «**Главном меню**» - «**Офис**» - «**1С:Предприятие**».

Подключение к БД

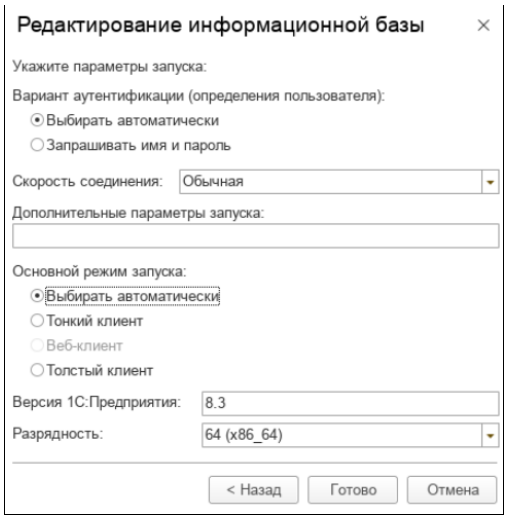
Для проверки подключения к базе данных, находящейся на сервере, запустите клиент 1С:Предприятия из «**Главного меню**» - «**Офис**» - «**1С:Предприятие**».

Выберите пункт «**Добавить**», затем «**Включение в список уже ранее созданной информационной базы**».

Введите **имя сервера** и **название информационной базы**:



После нажатия кнопки «**Далее**» необходимо выбрать **версию** 1С и **разрядность**:



При правильно введенных данных подключение к БД пройдет успешно.

Установка драйвера ключа аппаратной лицензии

Драйвер аппаратной лицензии можно скачать со страницы производителя:

https://thales-sentinel.ru/helpdesk/download-space/

Распакуйте архив в каталог удобным для вас способом и перейдите в него:

```
cd /home/user/Загрузки/Sentinel_LDK_RedHat_and_SuSE_RPM_Run-time_Installer
```

Внутри находятся пакеты под разные архитектуры. Установим **rpm** для **x86_64**:

```
dnf install aksusbd-8.43-1.x86_64.rpm
```

Статусы служб драйвера ключей и менеджера лицензий можно посмотреть следующими командами:

```
systemctl status aksusbd
systemctl status hasplmd
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Решение возникающих проблем

Возможные проблемы при установке пакетов

При попытке установки 1С-клиента может возникнуть ошибка вида:

```
 dnf install 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64

 Проблема: противоречивые запросы - nothing provides libwebkitgtk-3.0.so.0()(64bit) needed by 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64
```

Для решения данной проблемы выполните команду установки через менеджер пакетов RPM с выводом всех действий на экран и без контроля всех зависимостей:

```
rpm -ivh --nodeps 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64.rpm
```

Возможные проблемы при запуске программы

При запуске 1С-клиента может возникнуть ошибка вида:

```
 /opt/1cv8/x86_64/8.3.24.1467/1cv8s

 /opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libwebkit2gtk-4.0.so.37)
 /opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libjavascriptcoregtk-4.0.so.18)
```

где 8.3.24.1467 – используемая версия 1С-клиента.

Для решения данной проблемы рекомендуется создать символическую ссылку на библиотеку, используя следующие команды:

```
mv /opt/1cv8/common/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6
mv /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6
```

где 8.3.24.1467 – используемая версия 1С-клиента.

После этого повторите запуск клиента.

1С-клиент. Установка нескольких версий

Установка

Решение возникающих проблем

Возможные проблемы при установке пакетов

Возможные проблемы при запуске программы

Установка

Примечание.

Данные действия необходимы только при использовании клиентов 1С:Предприятие версии **8.3.18.xxxx или более ранних** .

Если вы используете версии новее, то установка нескольких версий предусмотрена уже самой фирмой 1С.

В качестве примера будет рассмотрена установка клиентов версий **8.3.16.1359** и **8.3.17.1989**. Далее по тексту «Клиент 1» и «Клиент 2» соответственно.

Распакуйте скачанные заранее архивы клиентов в разные для каждой версии каталоги.

```
mkdir ~/Загрузки/8.3.17
cp <название_архива> ~/Загрузки/8.3.17
cd ~/Загрузки/8.3.17
tar xvzf <название_архива>
```

Создайте папку для распаковки **.rpm** в каталоге «Клиента 2» (в примере **1С_8.3.17.1989**) и перейдите в него:

```
mkdir ~/Загрузки/8.3.17/1С_8.3.17.1989
cd ~/Загрузки/8.3.17/1С_8.3.17.1989
```

Выполните команду распаковки от **локального** пользователя (не от администратора):

```
for i in ../*.rpm; do rpm2cpio $i | cpio -id; done
```

В директории появятся каталоги **opt** и **usr**.

Скопируйте папку **1С_8.3.17.1989** с распакованными файлами, например, в корень. Для копирования в корень требуются права администратора:

```
cp -r ~/Загрузки/8.3.17/1С_8.3.17.1989 /
```

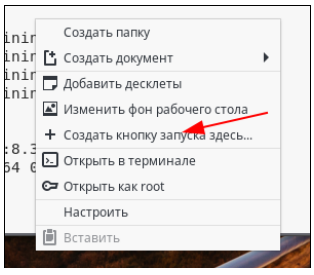
Затем установите «Клиент 1» 1С (в примере версия **8.3.16**):

```
cd ~/Загрузки
mkdir ~/Загрузки/8.3.16
cp <название_архива> ~/Загрузки/8.3.16
cd ~/Загрузки/8.3.16
tar xvzf <название_архива>
dnf install *.rpm
```

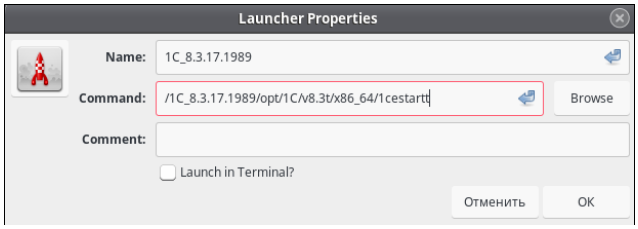
После всех выполненных действий можно запустить несколько версий платформы. Одну — через «**Главное меню**» - «**Офис**» (8.3.16), вторую — из каталога **1С_8.3.17**.

Можно создать кнопку для более удобного запуска «Клиента 2».

Нажмите правой кнопкой мыши по рабочему столу и выберите пункт «**Создать кнопку запуска здесь...**».



В открывшейся форме укажите **имя ярлыка** и **путь** до *1cestartt* (**/1C_8.3.17.1989/opt/1C/v8.3/x86_64/1cestartt**).



Решение возникающих проблем

Возможные проблемы при установке пакетов

При попытке установки 1С-клиента может возникнуть ошибка вида:

```
dnf install 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64

Проблема: противоречивые запросы - nothing provides libwebkitgtk-3.0.so.0()(64bit) needed by 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64
```

Для решения данной проблемы выполните команду установки через менеджер пакетов RPM с выводом всех действий на экран и без контроля всех зависимостей:

```
rpm -ivh --nodeps 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64.rpm
```

Возможные проблемы при запуске программы

Вариант 1. При запуске 1С-клиента может возникнуть ошибка вида:

```
/opt/1cv8/x86_64/8.3.24.1467/1cv8s

/opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libwebkit2gtk-4.0.so.37)
/opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libjavascriptcoregtk-4.0.so.18)
```

где 8.3.24.1467 – используемая версия 1С-клиента.

Для решения данной проблемы рекомендуется создать символическую ссылку на библиотеку, используя следующие команды:

```
mv /opt/1cv8/common/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6
mv /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6
```

где 8.3.24.1467 – используемая версия 1С-клиента.

После этого повторите запуск клиента.

Вариант 2. При запуске 1С-клиентов ранних версий (**до версии 8.3.20**) может возникать ошибка вида:

```
/opt/1cv8/common/1cestart

/opt/1C/v8.3/x86_64/1cestart: error while loading shared libraries: libwebkitgtk-3.0.so.0: cannot open shared object file: No such file or directory
```

Для решения данной проблемы необходимо проверить наличие установленных пакетов **webkit2gtk4.0** и **javascriptcoregtk4.0** в используемой системе:

```
rpm -qa | grep webkit2gtk4.0
```

```
rpm -qa | grep javascriptcoregtk4.0
```

По умолчанию пакеты установлены в РЕД ОС.

Если по каким-либо причинам пакеты в вашей системе не установлены, выполните команду:

```
dnf install webkit2gtk4.0 javascriptcoregtk4.0
```

Далее необходимо создать символические ссылки на библиотеки, выполнив команды:

```
ln -sf /usr/lib64/{libjavascriptcoregtk-4.0.so.18,libjavascriptcoregtk-3.0.so.0}
ln -sf /usr/lib64/{libjavascriptcoregtk-4.0.so.18,libjavascriptcoregtk-3.0.so.0.16.19}
ln -sf /usr/lib64/{libwebkit2gtk-4.0.so.37,libwebkitgtk-3.0.so.0}
ln -sf /usr/lib64/{libwebkit2gtk-4.0.so.37,libwebkitgtk-3.0.so.0.22.17}
```

После этого повторите запуск клиента.

Сбор логов сервера 1С

Для настройки сбора логов необходимо выполнить следующие действия:

1. Перейдите в пользователя **root**.

```
su -
```

2. Создайте папку для логов.

```
mkdir -p /var/log/log1c
```

3. Назначьте владельца.

```
chown usr1cv8:grp1cv8 /var/log/log1c
```

4. Создайте каталог **conf** в **/opt/1cv8/x86_64/current/**.

```
mkdir -p /opt/1cv8/x86_64/current/conf
```

5. Назначьте владельца каталогу **conf**.

```
chown usr1cv8:grp1cv8 /opt/1cv8/x86_64/current/conf
```

6. Создайте файл настроек технологического журнала 1С.

```
nano /opt/1cv8/x86_64/current/conf/logcfg.xml
```

Содержание файла:

```
<config xmlns="http://v8.1c.ru/v8/tech-log">
 <log location="/var/log/log1c" history="12">

 <event>
 <eq property="name" value="excp"/>
 </event>

 <event>
 <eq property="name" value="excpcntx"/>
 </event>

 <event>
 <eq property="name" value="admin"/>
 </event>

 <event>
 <eq property="name" value="clstr"/>
 </event>

 <event>
 <eq property="name" value="conn"/>
 </event>

 <event>
 <eq property="name" value="sesn"/>
 </event>

 <event>
 <eq property="name" value="proc"/>
 </event>
```

```
<event>
<eq property="name" value="DBPOSTGRS"/>
<ge property="Durationus" value="10000000"/>
</event>

<property name="all"/>
</log>
<plansql/>
</config>
```

7. Назначьте владельца файлу **logcfg.xml**.

```
chown usr1cv8:grp1cv8 /opt/1cv8/x86_64/current/conf/logcfg.xml
```

8. Подождите 1-2 минуты.

Данное условие связано с тем, что обнаружение файла настройки осуществляется опросом каталогов их возможного месторасположения в заданный промежуток времени.

9. Проверьте, что в **/var/log/log1c** начали появляться папки.

Если папки появляются – значит, все настроено верно.

Справочно-правовая система Консультант Плюс

Установка и настройка wine

Установите Wine.

```
dnf install wine winetricks
```

ВАЖНО!

Выполните следующую команду **от пользователя, для которого** устанавливается Консультант+ (**не из-под sudo или root**):

```
winetricks riched30 winhttp
```

Запустите конфигуратор wine, перейдя в меню по пути **Меню - Wine - Wine Configuration**.

ВАЖНО

Запускать конфигуратор Wine нужно **от того пользователя, под которым планируется работать в Консультант+**

Установите необходимые дополнительные библиотеки, которые попросит установить Wine.
На вкладке Графика уберите галочку в пункте "Разрешить менеджеру окон декорировать окна".

Настройка запуска Консультант+ на рабочей станции

Для запуска "Консультант Плюс" на рабочей станции подключите сетевой диск с "Консультантом", это можно сделать разными способами. Инструкции по подключению сетевых дисков вы можете прочитать по ссылке, используйте подходящий для вас вариант. Рекомендуется использовать **automount**.
Если клиентский ПК находится в домене, то для подключения сетевого каталога с К+ воспользуйтесь инструкцией по ссылке.

ВАЖНО!

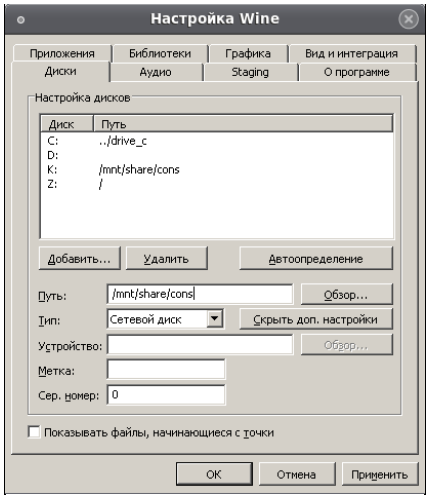
Дальнейшие команды выполняются **от того пользователя, под которым планируется работать в Консультант+** (**не от root**)

Проверьте, что команда whoami выдаёт имя вашего пользователя, а не *root*.

После того, как сетевой каталог с К+ был подключен, например в /mnt/share/cons/ , перейдем к настройке wine. Для Консультант Плюс в wine важно создать сетевой диск, для этого выполните команду в консоли от обычного пользователя:

```
winecfg
```

При этом откроется окно, в котором нужно создать сетевой диск, например K: и для него указать точку монтирования (каталог, в который был примонтирован Консультант+.), а тип диска обязательно выбрать "Сетевой диск".



Тогда, команда запуска Консультанта будет выглядеть следующим образом:

```
wine K:\cons.exe /linux /yes
```

Первый запуск Консультант+ производится долго, так как выполняется обновление конфигурации wine.

Далее должна запуститься процедура регистрации рабочей станции. Не закрывая окна обмена информацией с администратором, необходимо зарегистрировать рабочую станцию с машины администратора. Для регистрации рабочей станции с машины администратора, запустите Консультант+ с ключом /adm. Перейдите в меню на пункт ***Сервис > Регистрация новых пользователей***.

При успехе, на сервере и на клиенте будет увеличиваться прогресс регистрации в прогресс-баре.
В некоторых случаях могут возникать проблемы с регистрацией станций, т.е. при повторном запуске К+ снова просит зарегистрировать станцию. Это происходит из-за того, что у К+ есть ограничение по количеству различных прописываемых путей запуска К+ при регистрации станции. Их не может быть более пяти.
Т.е. если будет условно 50 станций, но у всех прописан одинаковый путь, то проблем с регистрацией быть не должно.

Создание ярлыка Консультант+

Если при установке Консультант+ автоматически не создался ярлык запуска, то создайте на рабочем столе файл с расширением .desktop и содержанием:

```
[Desktop Entry]
Name=ConsultantPlus
Exec=wine K:\cons.exe /linux /yes
Type=Application
StartupNotify=true
Comment=ConsultantPlus
Icon=/usr/share/icons/hicolor/cons.ico
StartupWMClass=cons.exe
```

В строке *"Exec=wine K:\cons.exe /linux /yes"* укажите свой каталог, в который был примонтирован Консультант+.
Переместите иконку cons.ico в /usr/share/icons/hicolor/ и укажите в параметрах ярлыка для значения **Icon** путь до него.

В случае замедленной работы можно добавить ключ /sprocess=0. При нормальной работе, не добавляйте этот ключ.
Ключ /yes необходим для подавления сообщения об ошибке [WNetGetUniversalName ...] : NO_NETWORK

Дополнительные ключи запуска КонсультантПлюс

Для регистрации

```
wine cons.exe /adm /reg
```

Для приема пополнения из RECEIVE

```
wine cons.exe /adm /receive /base*
```

Для приема пополнения через интернет

```
wine cons.exe /adm /receive_inet /base*
```

Для тестирования

```
wine cons.exe /adm /basetest /base*
```

Установка драйвера защиты "Консультант Плюс" для серверной части

Если **файл-серверная** часть "Консультант Плюс" будет располагаться на РЕД ОС, то для его работы нужно установить и запустить на РЕД ОС драйвер защиты conslin. Этот файл необходим для успешных регистрации и обновления баз. Для установки драйвера защиты "Консультант Плюс" требуется файл conslin с официального сайта Консультант+.
Поместите его в директорию /usr/local/bin. Переместить файл в этот каталог получится только с правами суперпользователя.

Перейдите в консоли в каталог с файлом conslin и выполните копирование:

```
# cp conslin /usr/local/bin
```

Владельцем conslin назначьте пользователя root и дайте права на выполнение:

```
# chown root:root /usr/local/bin/conslin
# chmod +x /usr/local/bin/conslin
```

Запустите conslin:

```
# /usr/local/bin/conslin
```

Результат успешного запуска conslin:

```
bind: Address already in use
```

Если conslin не запустился и выдал ошибку о том, что не нашел библиотек, установите дополнительно пакеты:

```
# dnf install glibc.i686 compat-libstdc++-33.x86_64 libstdc++.i686
```

Для автоматической загрузки драйвера защиты надо отредактировать файл rc.local

```
# nano /etc/rc.local
```

В конец файла добавить строку:

```
/usr/local/bin/conslin
```

Закрыть с сохранением файл и выполнить команду:

```
chmod a+x /etc/rc.local
```

Тест драйвера ККМ АТОЛ

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Драйвер ККТ - 10.9.3.1

ККМ АТОЛ — контрольно-кассовая техника ведущего российского производителя оборудования и разработчика ПО для решения задач, связанных с маркировкой товаров, **АТОЛ**.

В их линейке – более 20 онлайн-касс, соответствующих требованиям 54-ФЗ, принципиально новый класс контрольно-кассовой техники – «Ньюджеры», смарт-терминалы.

Облачный сервис компании «**АТОЛ Онлайн**» является первым и одним из самых крупных в РФ среди KaaS-решений («касса как сервис») по занимаемой доле рынка.

Также **АТОЛ** поставляет POS-оборудование и решения для автоматизации склада.

Для установки тестового приложения драйвера **ККТ АТОЛ** в Центре загрузок официального сайта компании необходимо открыть папку «**Контрольно-кассовая техника**» и скачать архив «**Драйвер ККТ 10.9.3.1**».

Распакуйте скачанный архив и перейдите в каталог с необходимыми для установки файлами:

```
unzip /home/user/Загрузки/10.9.3.1.zip
```

```
cd /home/user/Загрузки/10.9.3.1/installer/rpm
```

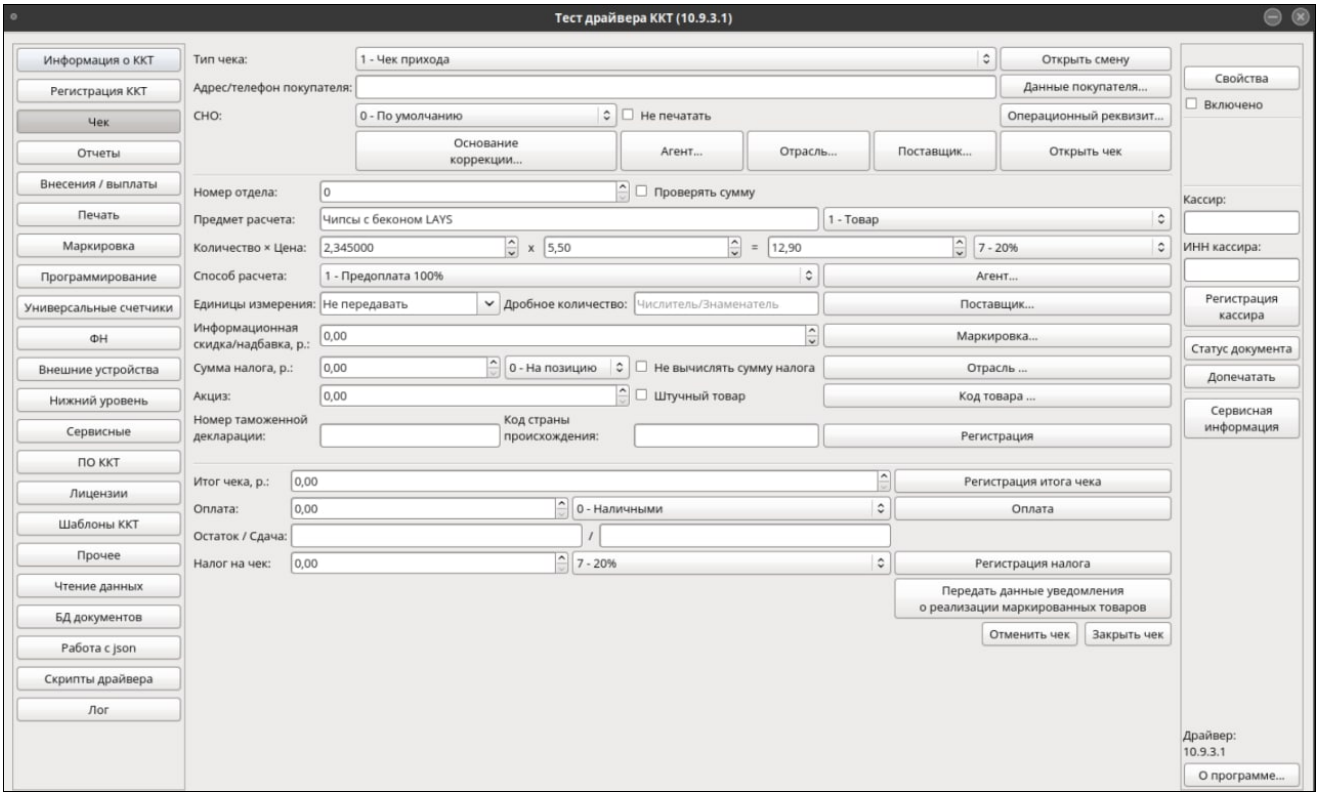
Для установки драйвера перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install libfptr10-gui-10.9.3.1-1.x86_64.rpm libfptr10-10.9.3.1-1.x86_64.rpm fptr10-test-util-10.9.3.1-1.x86_64.rpm
```

После установки программа будет доступна в «**Главном меню**» - «**Прочее**» - «**Тест драйвера ККТ v. 10**».



Установка ПО ГРАНД-Смета

Установка драйверов guardant
Предварительная подготовка
Установка ПО ГРАНД-Смета
Установка ПО ГРАНД-Смета через инсталлятор
Установка ПО ГРАНД-Смета через загрузчик

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: wine-9.0-1, autoconf-2.71-2, guardant-wine-0.5.8-1, smeta-2024.3.3

ГРАНД-Смета — программный комплекс для составления и проверки расчётов смет строительных работ, а также составления различных актов. Пользоваться программой может только обладатель уникального электронного ключа. Основными пользователями программного комплекса являются инженеры-сметчики. В составе ГРАНД-Сметы имеются различные базы, необходимые для работы инженера-сметчика.

Установка драйверов guardant

Guardant — семейство электронных ключей для защиты программного обеспечения от несанкционированного копирования и распространения. Разработаны российской компанией Актив.

В рамках данной статьи установка драйверов производится из репозитория РЕД ОС. Подробную информацию о драйверах **guardant** см. на официальной странице разработчика.

Предварительная подготовка

Установка пакетов

Для дальнейшей настройки необходимо установить дополнительные пакеты. Для этого перейдите в сеанс суперпользователя **root**:

```
su -
```

и выполните команду:

```
dnf install autoconf wine guardant-wine.i686
```

Выйдите из сеанса суперпользователя **root**:

```
exit
```

Дальнейшие действия выполняются с правами **локального пользователя**, если не указано иное.

Установка правил для udev

Скачайте архив с необходимыми правилами по ссылке.

После загрузки перейдите в каталог со скачанным архивом (в примере **/home/user/Загрузки**) и распакуйте его:

```
cd /home/user/Загрузки
tar -xvf udev-rules.tar.gz
```

Выполните установку правил (потребуются права **администратора системы**):

```
sudo ./install.sh
```

После успешной установки правил следует отсоединить электронный ключ от USB-порта и подсоединить его повторно.

Ключ готов к работе с защищенным приложением.

Настройка wine

В **wine** необходимо настроить 32-разрядную архитектуру:

```
export WINEARCH=win32
```

Убедитесь, что настройки применены:

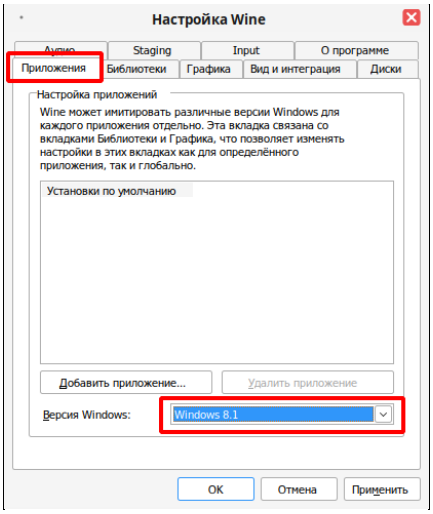
```
echo $WINEARCH

win32
```

Запустите конфигуратор **winecfg**:

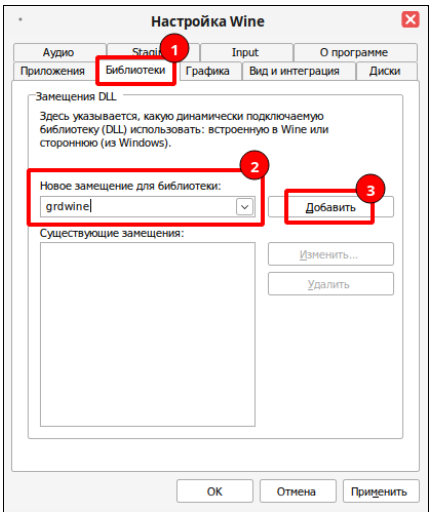
```
winecfg
```

> **Примечание.**
>
> Установка пакетов **mono** и **geco** не требуются для работы.

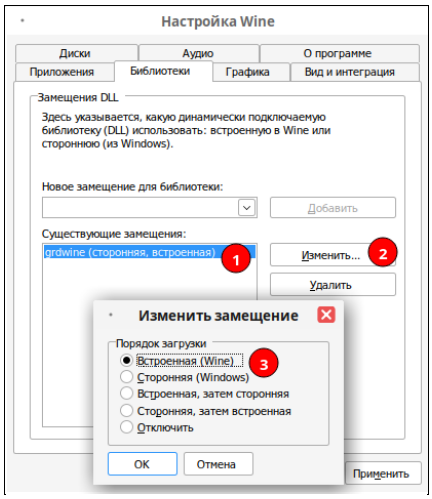
На вкладке **Приложения** выберите **Версию Windows** - *Windows 8.1*.



На вкладке **Библиотеки** введите **Новое замещение для библиотеки** - *grdwine*. Нажмите кнопку **Добавить**.



Затем выберите добавленную строку и нажмите **Изменить** для изменения порядка загрузки, установив значение - *Встроенная (Wine)*.



Нажмите **OK** для применения настроек.

Установка ПО ГРАНД-Смета

Подключите электронный ключ к компьютеру и запустите установку программы.

Установка ПО ГРАНД-Смета возможна двумя способами:

- через скачанный инсталлятор;
- через специальный загрузчик.

Установка ПО ГРАНД-Смета через инсталлятор

Перейдите на официальный сайт разработчика и запросите архив с необходимой версией **ПО ГРАНД-Смета** (в примере рассмотрена установка **ПО ГРАНД-Смета 2024.3.3**).

Перейдите в каталог со скачанным архивом (в примере **/home/user/Загрузки**) и распакуйте его:

```
cd /home/user/Загрузки
unzip smeta2024.3.3.zip -d ./smeta2024.3.3
```

Дополнительно для установки **ПО ГРАНД-Смета 2024.3** на РЕД ОС в **wine** необходимо использовать скрипт setup_run.sh.

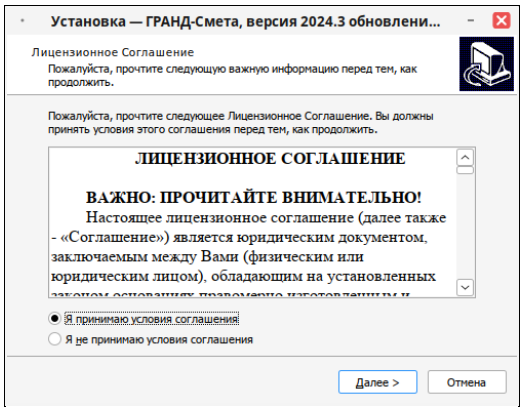
Скачайте скрипт **setup_run.sh** и поместите его в директорию с установочным файлом **Setup.exe** из распакованного архива, предоставьте скрипту права на исполнение:

```
mv setup_run.sh ./smeta2024.3.3
chmod +x ./smeta2024.3.3/setup_run.sh
```

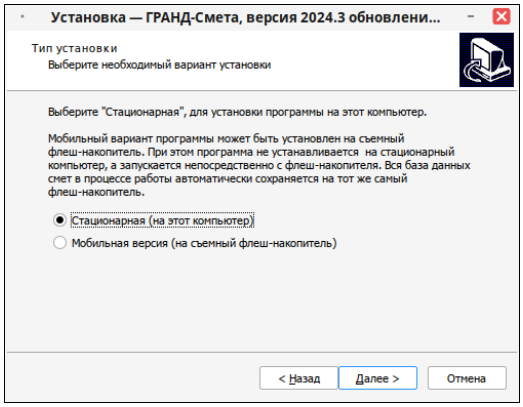
После этого запустите скрипт **setup_run.sh**:

```
./setup_run.sh Setup.exe
```

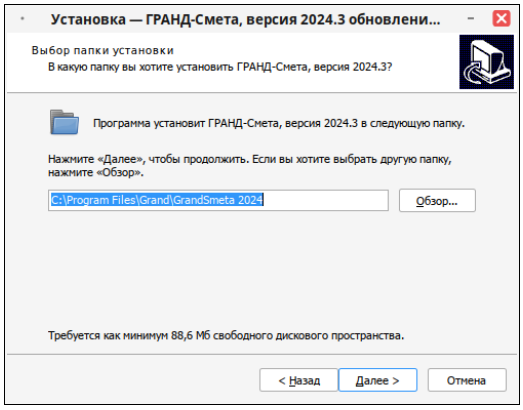
Для продолжения установки необходимо принять условия Лицензионного соглашения. Нажмите **Далее**.



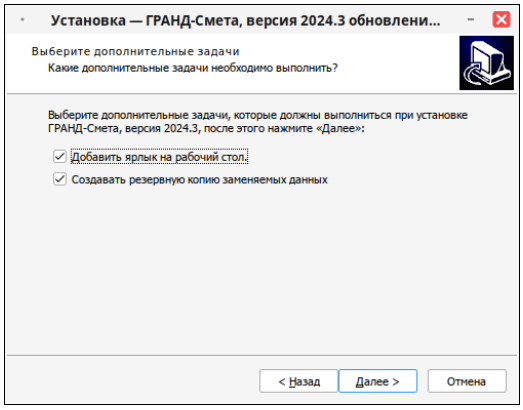
Выберите вариант установки — *Стационарная*. Нажмите **Далее**.



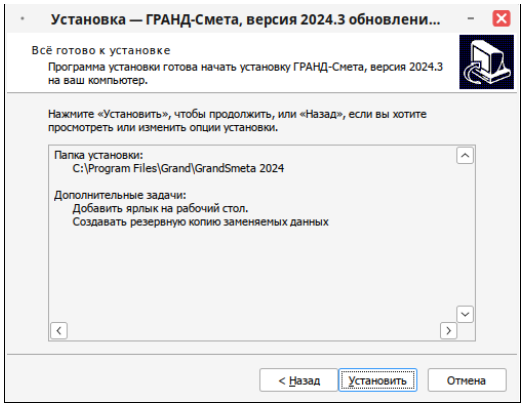
Выберите папку установки (можно оставить путь по умолчанию). Нажмите **Далее**.



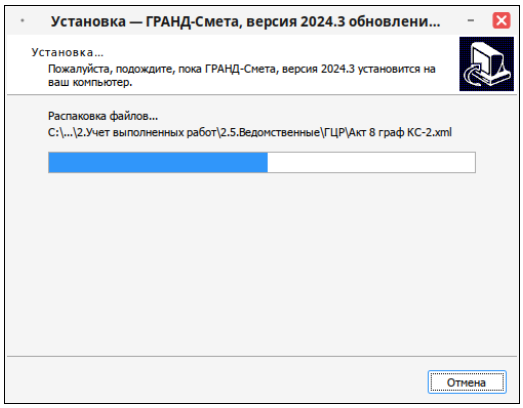
Установите дополнительные параметры. Нажмите **Далее**.



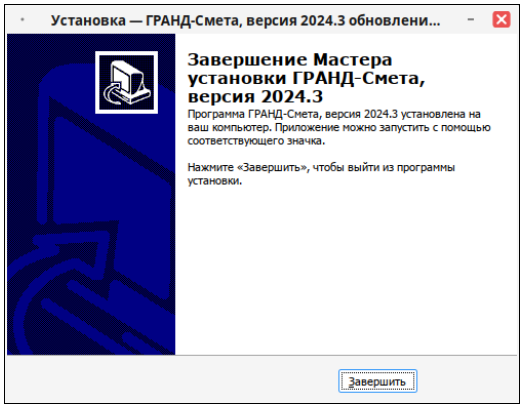
Проверьте правильность выбранных настроек и, если все верно, нажмите **Установить**.



Будет запущен процесс установки.



После окончания установки нажмите **Завершить** для выхода из программы установки.



Для завершения настройки выполните команду:

```
cp -rf /usr/lib/wine/i386-unix/grdwine.dll.so /home/user/.wine/drive_c/Program\ Files/Grand/GrandSmeta\ 2024/Client/grdwine.dll
```

На этом установка ПО ГРАНД-Смета завершена. На **Рабочем столе** появится ярлык для запуска программы.

Установка ПО ГРАНД-Смета через загрузчик

Перейдите на официальный сайт разработчика и скачайте **Утилиту загрузки программы ГРАНД-Смета**, нажав кнопку **Скачать и установить**.

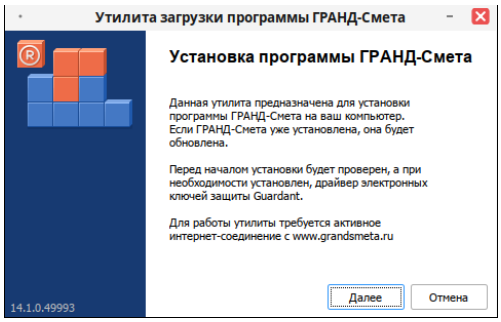
Перейдите в каталог со скачанным файлом (в примере **/home/user/Загрузки**):

```
cd /home/user/Загрузки
```

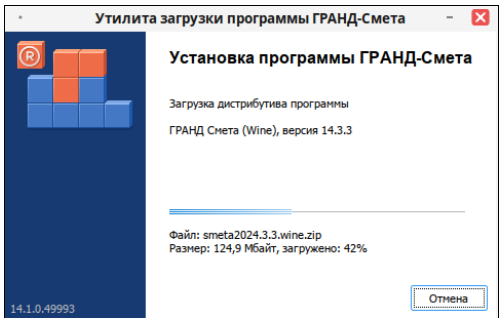
Для запуска установки выполните:

```
wine GrandSmetaDownloader.exe
```

Будет открыт загрузчик **ПО ГРАНД-Смета**. На приветственной странице нажмите **Далее**.

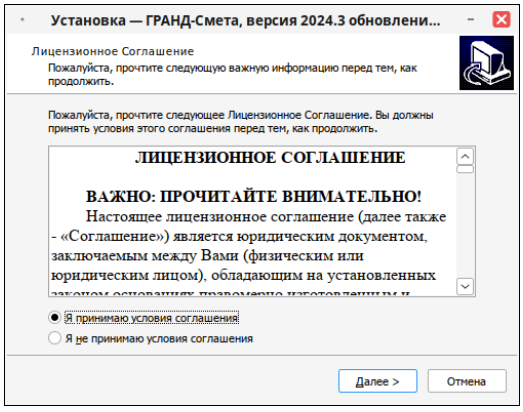


Будет произведена проверка драйверов электронных ключей. Если драйверы отсутствуют, они будут автоматически установлены. Также будет осуществлена проверка подключенного ключа защиты.

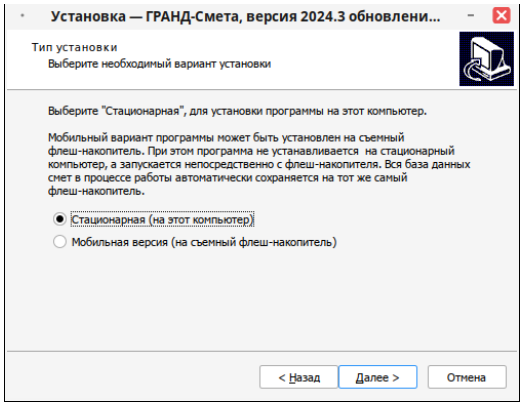


Затем будет загружен и распакован дистрибутив программы ГРАНД-Смета.

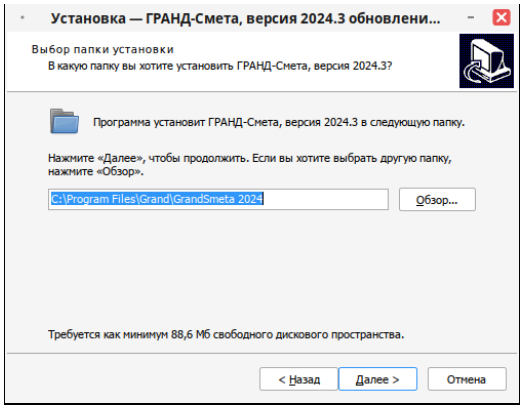
После распаковки дистрибутива будет открыто окно установщика, где необходимо принять условия Лицензионного соглашения.



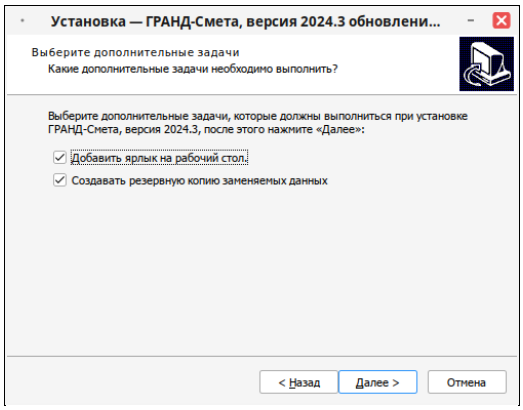
Выберите вариант установки — *Стационарная*. Нажмите **Далее**.



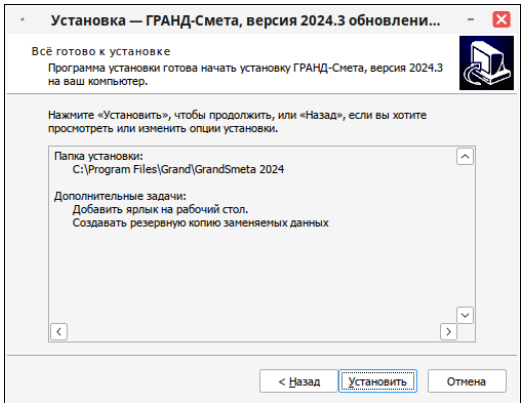
Выберите папку установки (можно оставить путь по умолчанию). Нажмите **Далее**.



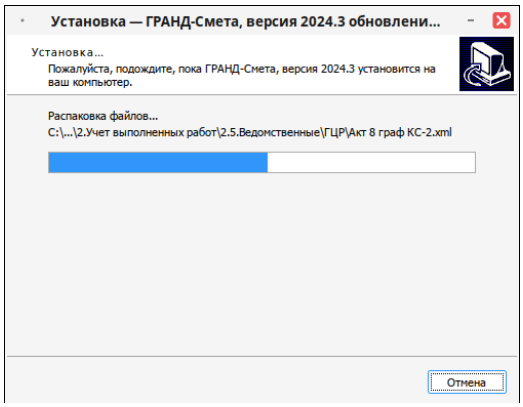
Установите дополнительные параметры. Нажмите **Далее**.



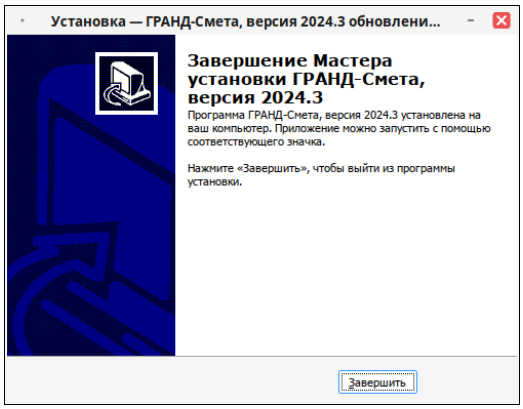
Проверьте правильность выбранных настроек и, если все верно, нажмите **Установить**.



Будет запущен процесс установки.



После окончания установки нажмите **Завершить** для выхода из программы установки.

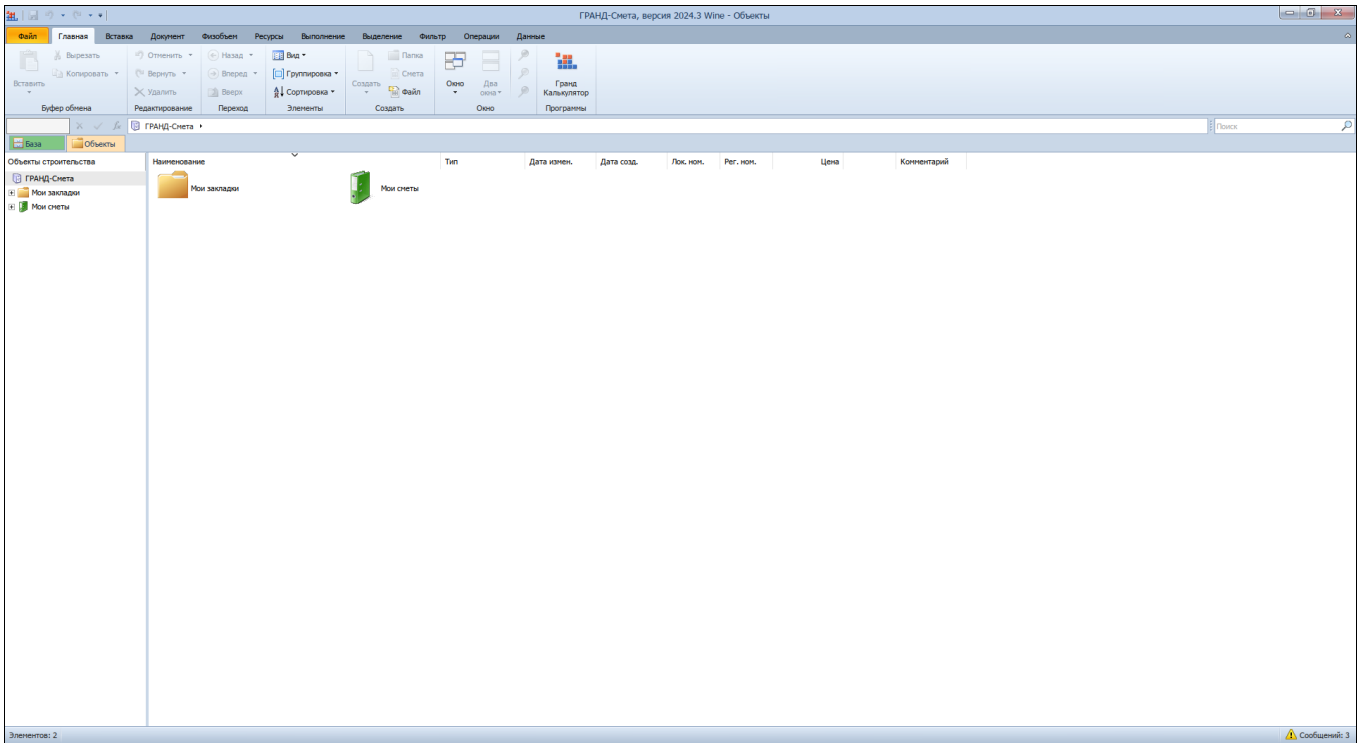


Для завершения настройки выполните команду:

```
cp -rf /usr/lib/wine/i386-unix/grdwine.dll.so /home/user/.wine/drive_c/Program\ Files/Grand/GrandSmeta\ 2024/Client/grdwine.dll
```

На **Рабочем столе** появится ярлык для запуска программы.

Окно программы выглядит следующим образом:


ГРАНД-Смета, версия 2024.3 Wine - Объекты
Файл
Главная
Вставка
Документ
Физобъем
Ресурсы
Выполнение
Выделение
Фильтр
Операции
Данные
Вставить
Вырезать
Копировать
Буфер обмена
Отменить
Вернуть
Удалить
Редактирование
Назад
Вперед
Вверх
Переход
Вид
Группировка
Сортировка
Элементы
Создать
Папка
Смета
Файл
Создать
Окно
Два окна
Окно
Гранд Калькулятор
Программы
ГРАНД-Смета
Поиск
База
Объекты
Объекты строительства
ГРАНД-Смета
Мои закладки
Мои сметы
Наименование
Тип
Дата измен.
Дата созд.
Лок. ном.
Рег. ном.
Цена
Комментарий
Мои закладки
Мои сметы
Элементов: 2
Сообщений: 3

Conky - программа для системного мониторинга

Графический менеджер conky

Conky - это системный монитор, который позволяет выводить на экран информацию о вашем процессоре, памяти, жестком диске, сетевом подключении, запущенных процессах и многом другом, что происходит в системе. Основная особенность *Conky* заключается в том, что данные выводятся на рабочий стол в виде виджета.

Вы можете подробнее ознакомиться с настройкой и работой утилиты **conky**, просмотрев наши обучающие видео:

- на **RuTube** — Conky - мощный и настраиваемый системный монитор;
- в **Яндекс.Дзен** — Conky - мощный и настраиваемый системный монитор;
- в **VK Видео** — Conky - мощный и настраиваемый системный монитор.

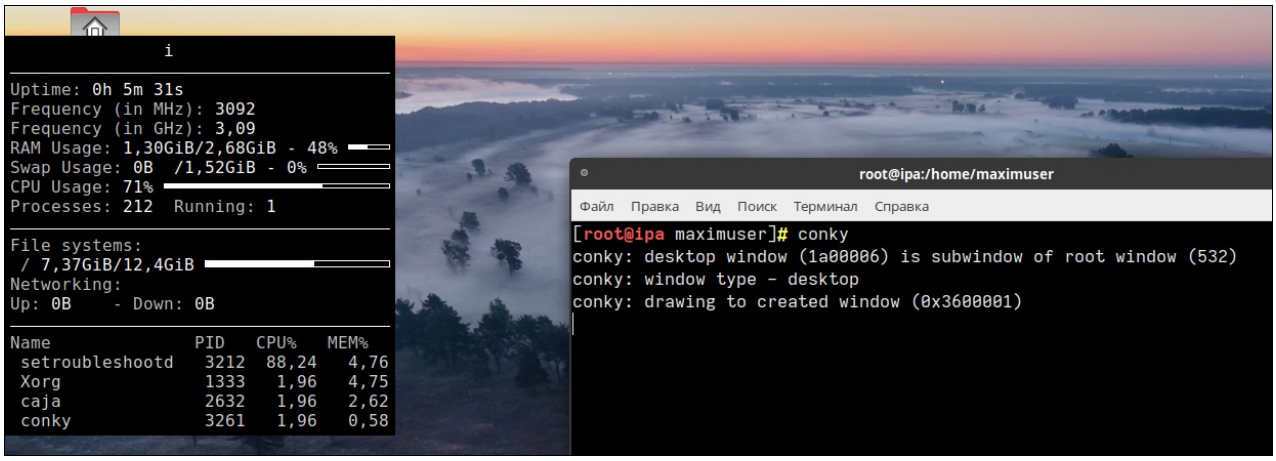
На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты необходимо выполнить команду:

```
dnf install conky
```

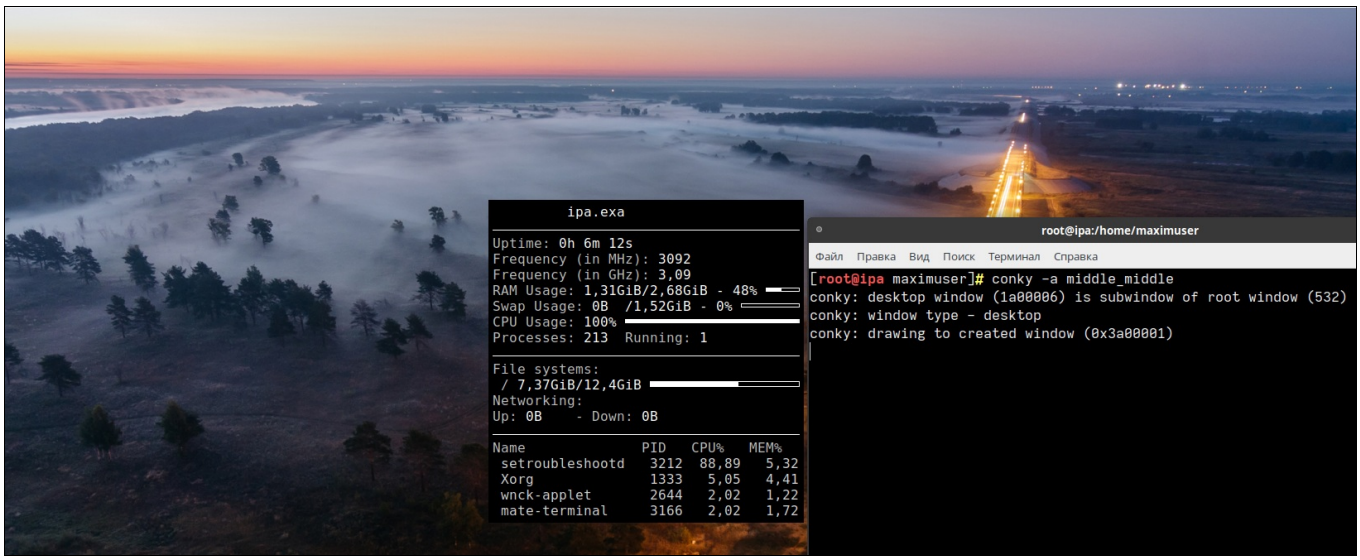
После установки запустим *conky* и увидим виджет с основной информацией о системе:

```
conky
```



Для того чтобы изменить положение виджета, необходимо использовать опцию **-a** и параметры **left, right, top, bottom, middle**, нужно указать положение по вертикали и по горизонтали. Например, установим виджет посередине:

```
conky -a middle_middle
```



При обновлении виджет мерцает, чтобы этого избежать, можно использовать двойную буферизацию. Для этого добавьте опцию **-b**:

```
conky -b -a middle_middle
```

Теперь перейдём к конфигурации виджета, для этого используется опция **-c**, она позволяет задать конфигурационный файл, из которого надо загружать тему. Так как мы будем изменять конфигурационный файл темы, чтобы не повредить стандартную тему, скопируйте его в домашнюю папку:

```
cp /etc/conky/conky.conf /etc/conky/conky.default
```

Перейдём в редактирование конфигурационного файла:

```
nano /etc/conky/conky.conf
```

По умолчанию любой конфигурационный файл *conky* делится на две секции - секция настроек и секция данных для вывода. Для начала изменим основные параметры секции настроек. Параметр **alignment = bottom_right** отвечает за расположение виджета, в данном случае - справа внизу. Параметр **gap_x = 50** используется для указания отступа от края по горизонтали, также можно указать отступ по вертикали - **gap_y**.

Сейчас окно чёрное, чтобы сделать его прозрачным, добавьте строку:

```
own_window_argb_visual = true
```

Затем можно настроить цвет и нужный уровень прозрачности с помощью следующих строк:

```
own_window_colour = '171717'
own_window_argb_value = 150
```

Цвет может быть практически любым. Значение прозрачности может быть от 0 до 255, где 0 - это полностью прозрачный и 255 - непрозрачный.

С помощью параметра **font** можно настраивать шрифт и его размер. Например, используем шрифт *Noto Mono, 13*:

```
font = 'Noto Mono:size=13'
```

За интервал обновления данных отвечает параметр **update_interval**, в данном случае - одна секунда, можно сделать полсекунды:

```
update_interval = 0.5
```

Если вы запустили программу без опции **-b**, то увидите, что при обновлении виджет немного мерцает. Чтобы этого избежать, включите двойную буферизацию, добавив строчку:

```
double_buffer = true
```

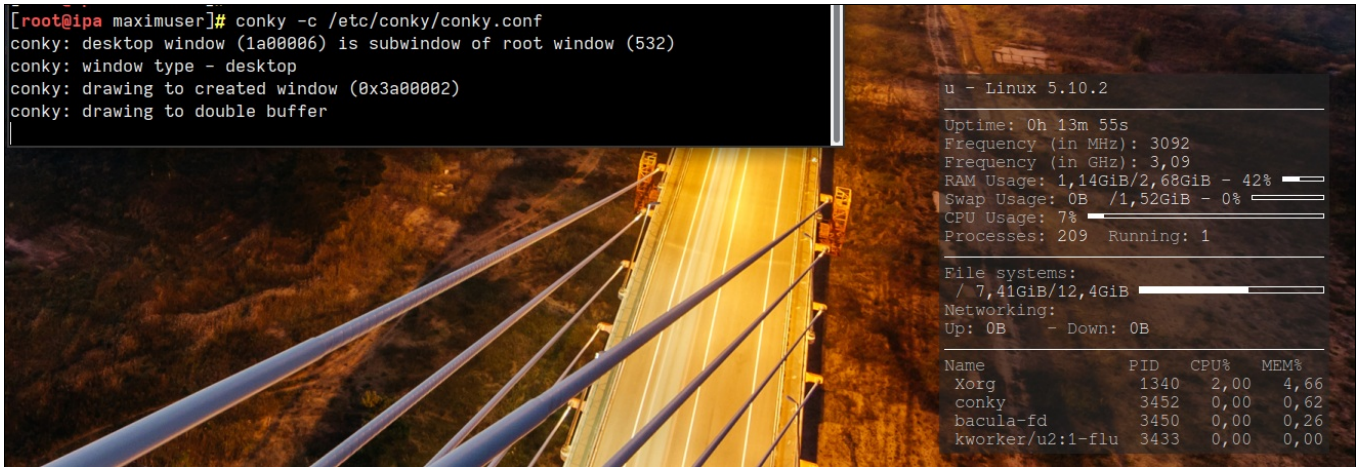
В секции настроек можно задать цвета, которые вы будете использовать потом в секции вывода. Это делать не обязательно, так как там можно сразу же указывать цвета, но это довольно удобно. Для установки цвета просто добавьте переменные *color1, color2, color3* и т.д.:

```
color1 = '#ff0000'
color2 = '#00ff00'
color3 = '#00ff00'
```

Теперь после изменения секции настроек она выглядит следующим образом:

```
conky.config = {
    alignment = 'bottom_right',
    background = false,
    border_width = 1,
    cpu_avg_samples = 2,
    default_color = 'white',
    default_outline_color = 'white',
    default_shade_color = 'white',
    draw_borders = false,
    draw_graph_borders = true,
    draw_outline = false,
    draw_shades = false,
    use_xft = true,
    font = 'Noto Mono:size=13',
    gap_x = 50,
    gap_y = 60,
    minimum_height = 5,
        minimum_width = 5,
    net_avg_samples = 2,
    no_buffers = true,
    out_to_console = false,
    out_to_stderr = false,
    extra_newline = false,
    own_window = true,
    own_window_class = 'Conky',
    own_window_type = 'desktop',
    own_window_argb_visual = true,
    own_window_colour = '171717',
    own_window_argb_value = 150,
    color1 = '#ff0000',
    color2 = '#00ff00',
    color3 = '#00ff00',
    stippled_borders = 0,
    update_interval = 0.5,
    double_buffer = true,
```

Сам виджет теперь выглядит так:



Перейдём к текстовой секции. В текстовой секции записывается текст, который будет выводиться в виджете. Синтаксис здесь следующий:

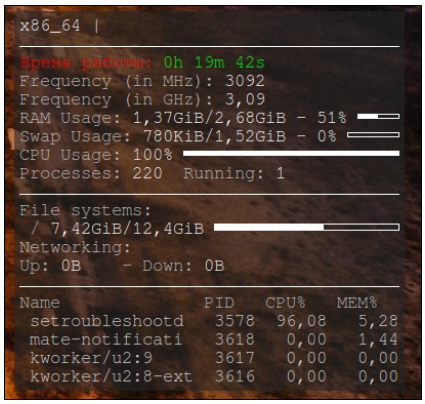
```
${<переменная> <параметр>}<текст>${<переменная> <параметр>}<текст>$<переменная>
```

Если для переменной нужны параметры, она пишется в скобках, если параметры не нужны, можно писать без скобок. Например:

```
${color1}Время работы:$color ${color2}$uptime$color
```

```
conky.text = [[
${scroll 16 $nodename - $sysname $kernel on $machine | }
$hr
${color1}Время работы:$color ${color2}$uptime$color
```

Теперь виджет выглядит следующим образом:



Все операции с выводом текста выполняются с помощью переменных. Основные переменные, которые вы можете использовать, можно посмотреть с помощью команды:

```
man conky
```

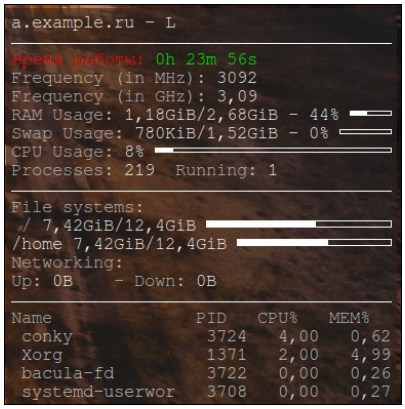
Примеры использования переменных

Для примера выведем свободное место в вашей домашней папке на виджет:

```
/home $color${fs_used /home}/${fs_size /home} ${fs_bar /home}
```

```
${color grey}File systems:
 / $color${fs_used /}/${fs_size /} ${fs_bar 6 /}
/home $color${fs_used /home}/${fs_size /home} ${fs_bar /home}
```

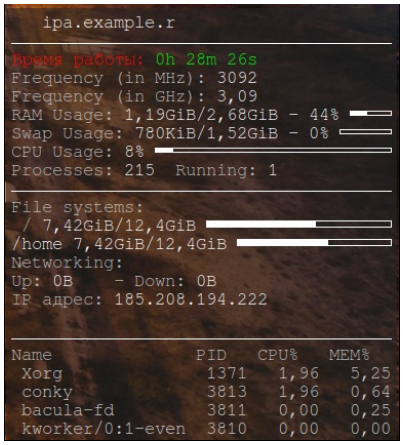
Теперь в разделе **File systems** выводится свободное место в домашней папке:



Аналогично можно сделать для необходимых каталогов. Чтобы показать ваш текущий IP-адрес, можно указать следующую строку:

```
${color grey}IP адрес: $alignr ${eval $${addrs ${gw_iface}}}
```

Теперь в разделе **Networking** выводится текущий IP-адрес:

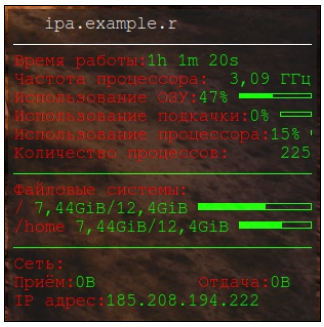


Зададим вывод данных на русском языке и изменим цвет выводимого текста:

```
${color1}Время работы:$color2${alignr}$uptime
${color1}Частота процессора:$color2${alignr}$freq_g ГГц
${color1}Использование ОЗУ:$color2$memperc% ${membar 4}
${color1}Использование подкачки:$color2$swapperc% ${swapbar 4}
${color1}Использование процессора:$color2$cpu% ${cpubar 4}
${color1}Количество процессов:$color2${alignr}$processes
${color1}Файловые системы:
${color1}/ $color2${fs_used /}/${fs_size /} ${fs_bar 6 /}
${color1}/home $color2${fs_used /home}/${fs_size /home} ${fs_bar /home}
${color1}Сеть:
${color1}Приём:$color2${upspeed enp24s0} ${color2} ${alignr} Отдача:$color2${downspeed enp24s0}
${color1}IP адрес:$color2${curl eth0.me}
```

```
conky.text = [[
${scroll 16 $nodename - $sysname $kernel on $machine | }
$hr
${color1}Время работы:$color${color2}$uptime$color
${color1}Частота процессора:$color2${alignr}$freq_g ГГц
${color1}Использование ОЗУ:$color2$memperc% ${membar 4}
${color1}Использование подкачки:$color2$swapperc% ${swapbar 4}
${color1}Использование процессора:$color2$cpu% ${cpubar 4}
${color1}Количество процессов:$color2${alignr}$processes
$hr
${color1}Файловые системы:
${color1}/ $color2${fs_used /}/${fs_size /} ${fs_bar 6 /}
${color1}/home $color2${fs_used /home}/${fs_size /home} ${fs_bar /home}
$hr
${color1}Сеть:
${color1}Приём:$color2${upspeed enp24s0} ${color1} ${alignr} Отдача:$color2${downspeed enp24s0}
${color1}IP адрес:$color2${curl eth0.me}
]]
```

Теперь виджет выглядит следующим образом:



Настройка *conky* завершена, у данного виджета присутствует множество вариаций оформления и выводимых данных, всё зависит от задаваемых параметров.

Графический менеджер conky

Утилита **conky** также имеет графический менеджер.

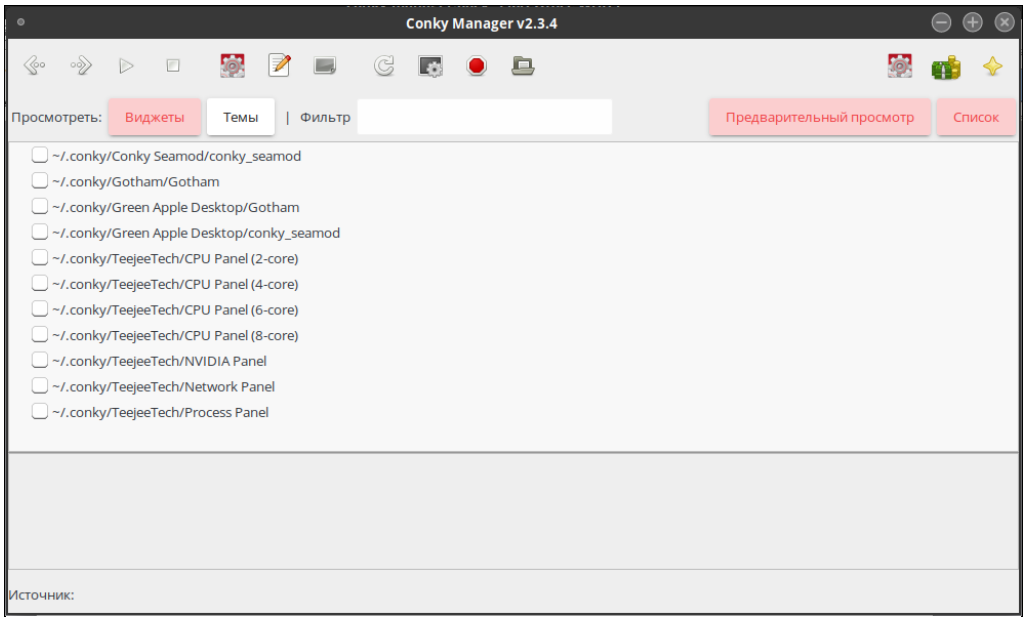
Для установки необходимо перейти в сеанс пользователя **root**:

```
su -
```

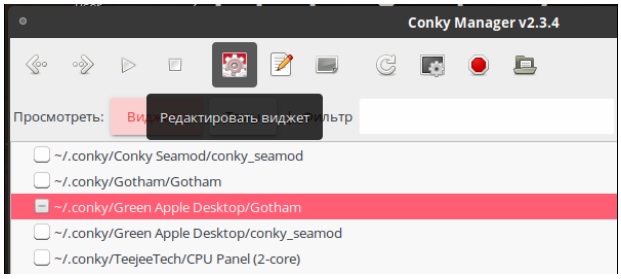
и выполнить команду:

```
dnf install conky-manager
```

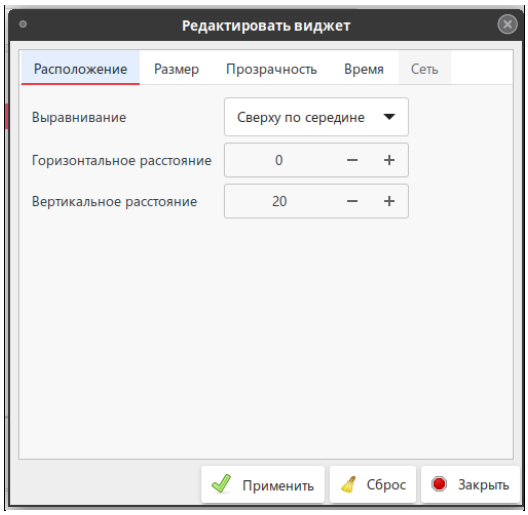
Запуск утилиты доступен из «**Главного меню**» – «**Стандартные**» – «**Conky Manager**».



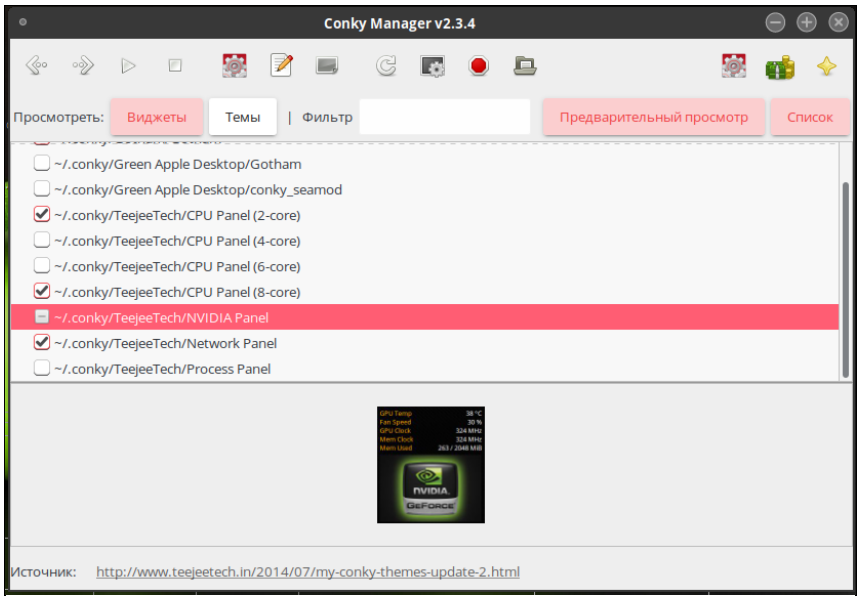
Утилита позволяет добавлять различные виджеты мониторинга системы, осуществлять предпросмотр этих виджетов на рабочем столе, а также редактировать их.



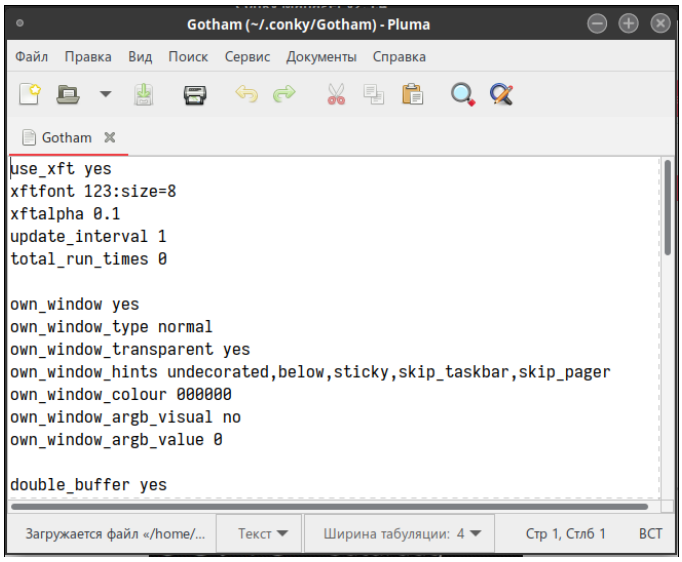
Можно отредактировать расположение виджета, его размер, цвет фона и прозрачность, формат отображаемого времени и сетевой интерфейс (если доступно).



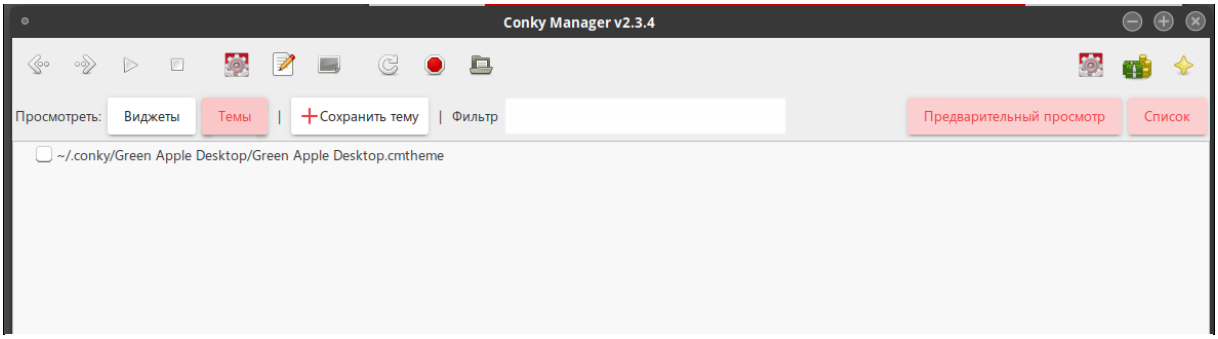
В **conky-manager** существует возможность запуска нескольких виджетов одновременно.



А также можно запускать свои созданные конфигурации для виджетов или изменять существующие. Для изменения уже существующих конфигураций редактируются две секции – секция настроек и секция данных для вывода.



В графическом менеджере также можно создавать и сохранять новые или редактировать уже имеющиеся темы для рабочего стола.



Glances - инструмент для мониторинга системы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** glances-3.1.4.1-1

Glances — это кросплатформенный инструмент для мониторинга системы на основе командной строки, написанный на языке **Python**, использующий библиотеку **psutil** для получения информации о системе. Так вы можете отслеживать использование процессора, средней нагрузки, памяти, сетевых интерфейсов, дискового ввода/вывода, процессов и файловой системы.

Информация о системе которая может выводится **Glances**:

- Информация о процессоре (пользовательские приложения, системные программы и незанятые программы).
- Общая информация о памяти, включая RAM, Swap, Free memory и т. д.
- Средняя загрузка процессора за последние 1, 5 и 15 минут.
- Скорость загрузки/выгрузки по сети.
- Общее количество процессов, активных и спящих процессов и т. д.
- Информация о скорости дискового ввода/вывода (чтение или запись).
- Подключенные устройства, использующие диск в настоящее время.
- top-процессы с использованием ЦП/памяти, именами и местоположением приложения.
- Текущие дата и время.
- Подсветка процесса, который потребляет максимальные системные ресурсы, красным цветом.

Атрибуты Glances

Поле указания атрибутов открывается клавишей «**Enter**» во время работы программы. Все доступные атрибуты можно посмотреть, нажав «**h**»:

- **a** – сортировать процессы автоматически;
- **c** – сортировать процессы по **CPU%**;
- **m** – сортировать процессы по **MEM%**;
- **p** – сортировать процессы по имени;
- **i** – сортировать процессы по скорости ввода/вывода;
- **d** – показать/скрыть статистику дискового ввода-вывода;
- **f** – показать/скрыть статистику директорий и файлов;
- **n** – показать/скрыть сетевую статистику;
- **s** – показать/скрыть статистику датчиков;
- **y** – показать/скрыть статистику **hddtemp**;
- **l** – показать/скрыть логи;
- **b** – байты или биты для сетевых входов/выходов;
- **w** – удалить журналы предупреждений;
- **x** – удалить предупреждения и критические журналы;
- **1** – общая статистика ЦП;
- **h** – показать/скрыть этот экран справки;
- **t** – просмотреть сетевой ввод/вывод как комбинации;
- **u** – просмотреть совокупный сетевой ввод/вывод;
- **q** – выйти (**Esc** и **Ctrl+C** тоже работают).

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

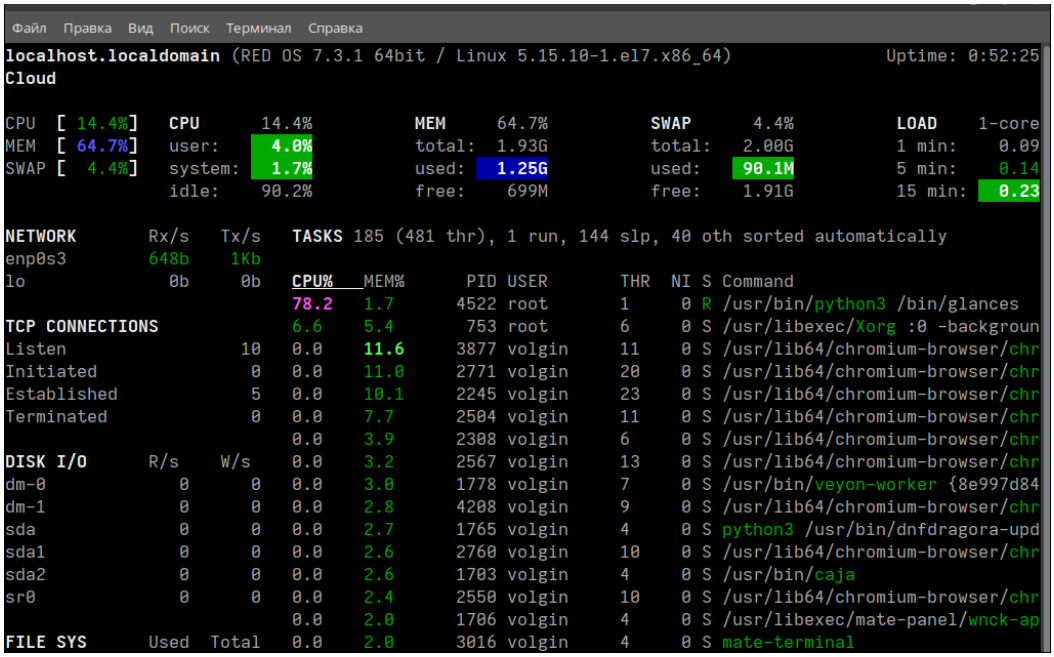
и выполните команду:

```
dnf install glances
```

Для запуска утилиты введите её название в терминале:

```
glances
```

Отображаемая по умолчанию информация:



iostat - утилита анализа загруженности системы

Установка
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** sysstat-12.3.1-1

Утилита **iostat** позволяет проанализировать загруженность системы. Она отображает основные параметры ввода/вывода данных на диск, скорость записи и чтения данных, а также объем записанных или прочитанных данных. Кроме того утилита выводит параметры загруженности процессора. Её можно использовать для оптимизации работы системы.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install sysstat
```

Основные опции утилиты:

- **-c** — отобразить только информацию об использовании процессора;
- **-d** — отобразить только информацию об использовании устройств;
- **-h** — выводить данные отчёта в удобном для чтения формате;
- **-k** — выводить статистику в килобайтах;
- **-m** — выводить статистику в мегабайтах;
- **-o JSON** — выводить статистику в формате JSON;
- **-p** — вывести статистику по устройству и всем его разделам;
- **-x** — вывести расширенную статистику;
- **-y** — отображать статистику с момента запуска утилиты, а не системы;
- **-z** — спрятать информацию о дисках, у которых нет активности.

Пример работы

Самый простой пример использования утилиты - это запуск без параметров:

```
iostat
```

```
Linux 5.15.10-1.el7.x86_64 (localhost.localdomain)      11.07.2022      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          1,15    0,01    0,91    0,25    0,03   97,65

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
dm-0             12,93       319,53        22,87         0,00    1156449      82756          0
dm-1              0,40         0,66         1,48         0,00       2384       5340          0
sda               7,31       322,56        24,38         0,00    1167410      88228          0
scd0              0,01         0,30         0,00         0,00       1072          0          0
```

В первой части отчёта находится информация о загруженности процессора. Здесь приведены следующие данные:

- **%user** — процент использования процессора программами, запущенными на уровне пользователя;
- **%nice** — процент использования процессора программами, запущенными в пространстве пользователя, но с изменённым приоритетом;
- **%system** — процент использования процессора ядром;
- **%iowait** — процент времени, затраченного на ожидание завершения операций ввода/вывода;

- **%steal** — процент простоя виртуального процессора во время передачи гипервизором мощности другому виртуальному процессору;
- **%idle** — процент времени простоя процессора (процессор не занят).

Для устройств ввода/вывода также отображается ряд данных со следующей информацией:

- **tps** — количество запросов на чтение или запись к устройству в секунду;
- **KB_read/s, MB_read/s** — количество килобайт или мегабайт, прочитанных с устройства за секунду;
- **KB_wrtn/s, MB_wrtn/s** — количество килобайт или мегабайт, записанных на устройство в секунду;
- **KB_dscd/s, MB_dscd/s** — скорость освобождения блоков данных на устройстве, килобайт или мегабайт в секунду;
- **KB_read, MB_read** — общее количество прочитанных данных с диска с момента загрузки системы;
- **KB_wrtn, MB_wrtn** — количество записанных данных с момента загрузки системы;
- **KB_dscd, MB_dscd** — количество освобождённых блоков на диске в результате выполнения операции **trim** в килобайтах или мегабайтах.

Для просмотра в более удобном формате выполните:

```
iostat -h
```

```
Linux 5.15.10-1.el7.x86_64 (localhost.localdomain)      11.07.2022      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0,6%    0,0%    0,6%    0,1%    0,0%   98,7%

      tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd Device
     5,82       135,9k        12,2k         0,0k       1,1G     102,0M       0,0k dm-0
     0,19         0,3k         0,7k         0,0k       2,8M       5,6M       0,0k dm-1
     3,36       137,2k        12,8k         0,0k       1,1G     107,7M       0,0k sda
     0,01         0,1k         0,0k         0,0k       1,0M       0,0k       0,0k scd0
```

Для отображения всей статистики выполните:

```
iostat -x
```

```
Linux 5.15.10-1.el7.x86_64 (localhost.localdomain)      11.07.2022      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0,56    0,01    0,55    0,13    0,03   98,72

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_awa
it wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz     f/s f_await  aqu-sz  %util
dm-0             4,21    135,48     0,00   0,00    2,04    32,18    1,60     12,13     0,00   0,00   16,
13     7,60    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,03   0,29
dm-1             0,03      0,33     0,00   0,00    4,67    12,87    0,16      0,66     0,00   0,00   25,
59     4,00    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,00   0,02
sda              2,31    136,72     2,01  46,45    1,55    59,14    1,04     12,81     0,72  40,98   16,
60    12,28    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,02   0,30
scd0             0,01      0,12     0,00   0,00    1,17    20,24    0,00      0,00     0,00   0,00    0,
00     0,00    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,00   0,00
```

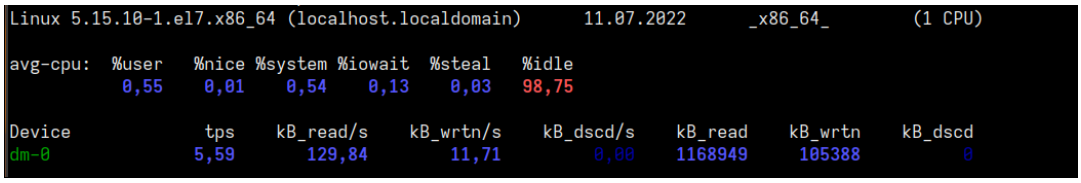
Описание вывода:

- **r/s** — количество запросов на чтение в секунду;
- **rKB/s** — скорость чтения с диска (КБ/сек);
- **rrqm/s** — обобщенное количество запросов на чтение в секунду;
- **%rrqm** — количество объединенных запросов чтения;
- **r_await** — среднее время (миллисекунды) на обработку запросов чтения к диску (включает в себя время, потраченное в очереди на обработку, и время на обработку запроса);
- **rareq-sz** — средний размер запроса для чтения;
- **w/s** — количество запросов на запись в секунду;
- **wKB/s** — скорость записи на диск (КБ/сек);
- **wrqm/s** — обобщенное количество запросов на запись в секунду;
- **%wrqm** — количество объединенных запросов записи;
- **w_await** — среднее время (миллисекунды) на обработку запросов записи к диску (включает в себя время, потраченное в очереди на обработку, и время на обработку запроса);

- **wareq-sz** — средний размер запроса для записи;
- **aqu-sz** — средняя длина очереди
- **%util** — % CPU, затраченный на передачу I/O запросов к диску («пропускная способность» диска).

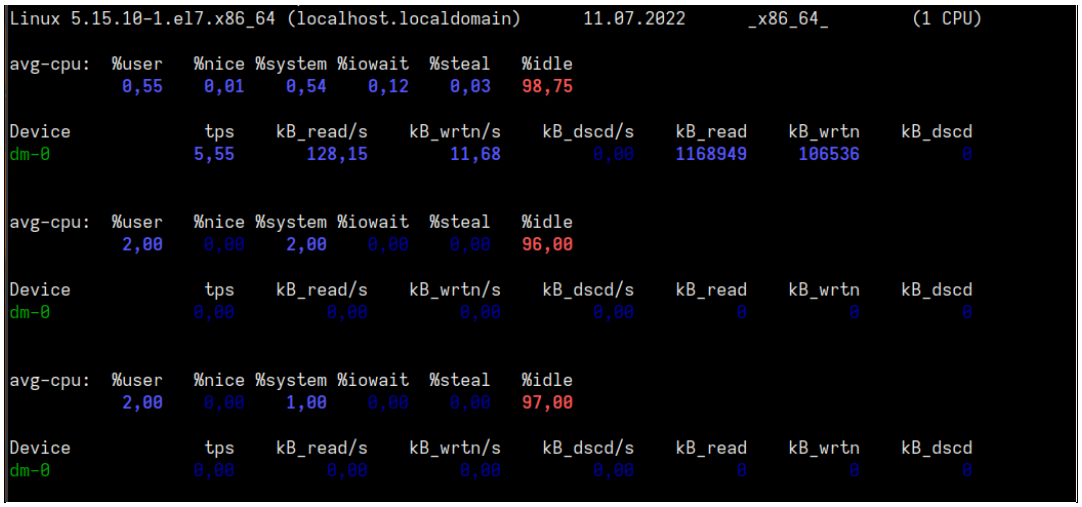
Можно просмотреть статистику по каждому разделу устройства, воспользовавшись опцией **-p**:

```
iostat -p /dev/dm-0
```



Чтобы утилита автоматически обновляла данные каждую секунду, необходимо добавить интервал (определяется в секундах):

```
iostat -p /dev/dm-0 1
```



iotop - утилита мониторинга использования диска

Установка
Основные опции программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** iotop 0.6-15

Утилита **iotop** позволяет просмотреть сведения об общем и текущем количестве операций обращения к диску.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

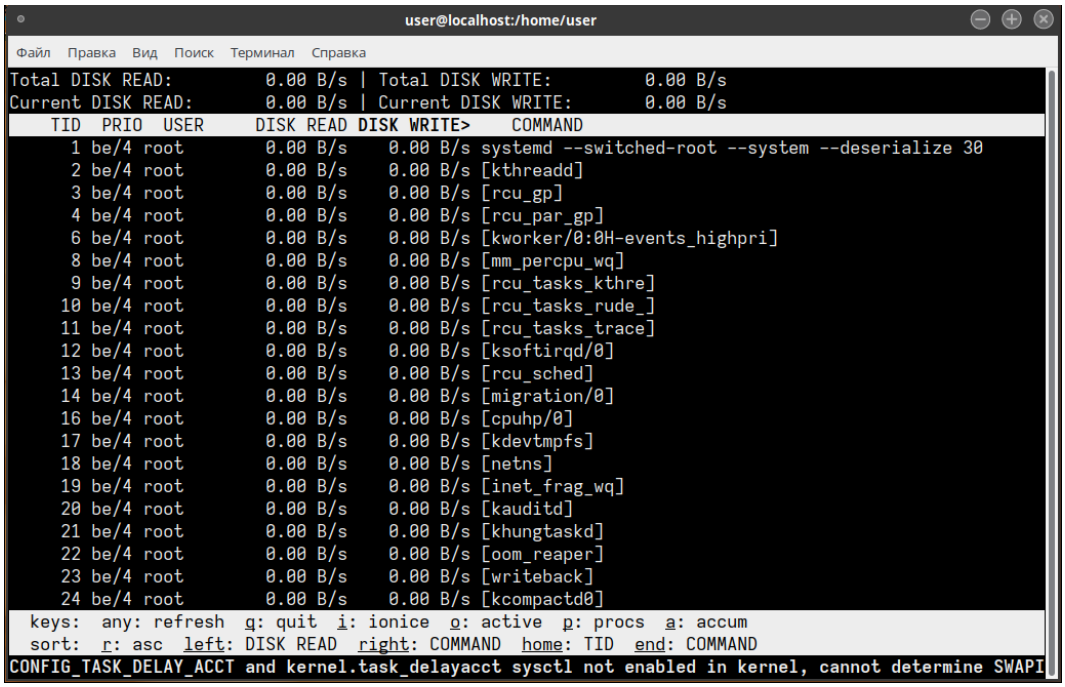
```
su -
```

и выполните команду:

```
dnf install iotop
```

Запустите утилиту через терминал, выполнив:

```
iotop
```



Основные опции программы

Опции для работы в программе описаны в таблице ниже.

Опции	Описание
--version	показать номер версии программы и выйти
-h, --help	показать данное справочное сообщение и выйти
-o, --only	отображать только процессы, которые в данный момент выполняют операции I/O с диском (по умолчанию — отображаются все активные процессы)
-b, --batch	неинтерактивный режим
-n <число>, --iter=<число>	количество итераций до окончания [бесконечно]
-d <сек>, --delay=<сек>	задержка между итерациями [1 секунда]
-p <PID_процесса>, --pid= <PID_процесса>	PID процесса, который нужно отслеживать
-u <имя_пользователя>, --user= <имя_пользователя>	имя пользователя, которого нужно отследить
-P, --processes	отображать только процессы (по умолчанию — все процессы и потоки)
-a, --accumulated	показывать накопленный ввод-вывод вместо пропускной способности
-k, --kilobytes	отображать информацию в КБ
-t, --time	добавить отображение времени выполнения проверки
-q, --quiet	уменьшить количество выводимой информации (подразумевается --batch)

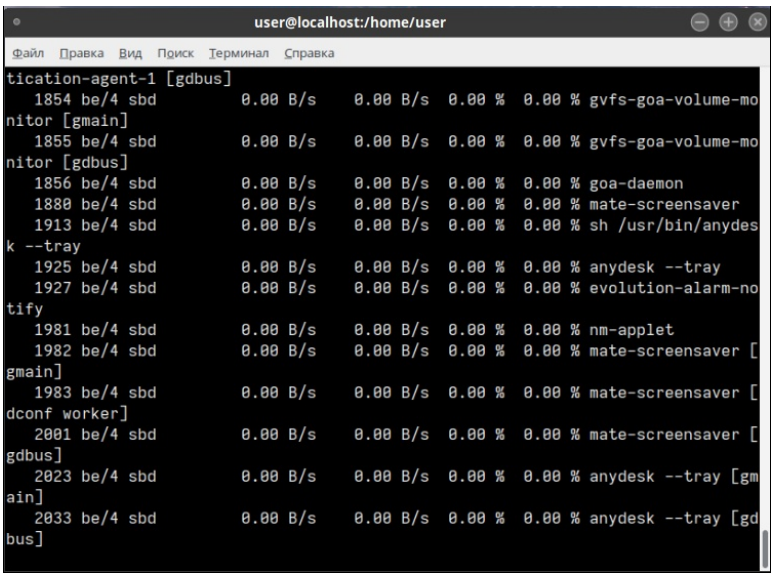
Также **iotop** поддерживает некоторое управление клавиатуры:

- стрелки **влево**-**вправо** — изменить сортировку колонок;
- **r** — изменить сортировку строк в выбранной колонке на обратную (a-z > z-a);
- **i** — изменить nice процесса (утилитой **ionice**);

Пример работы

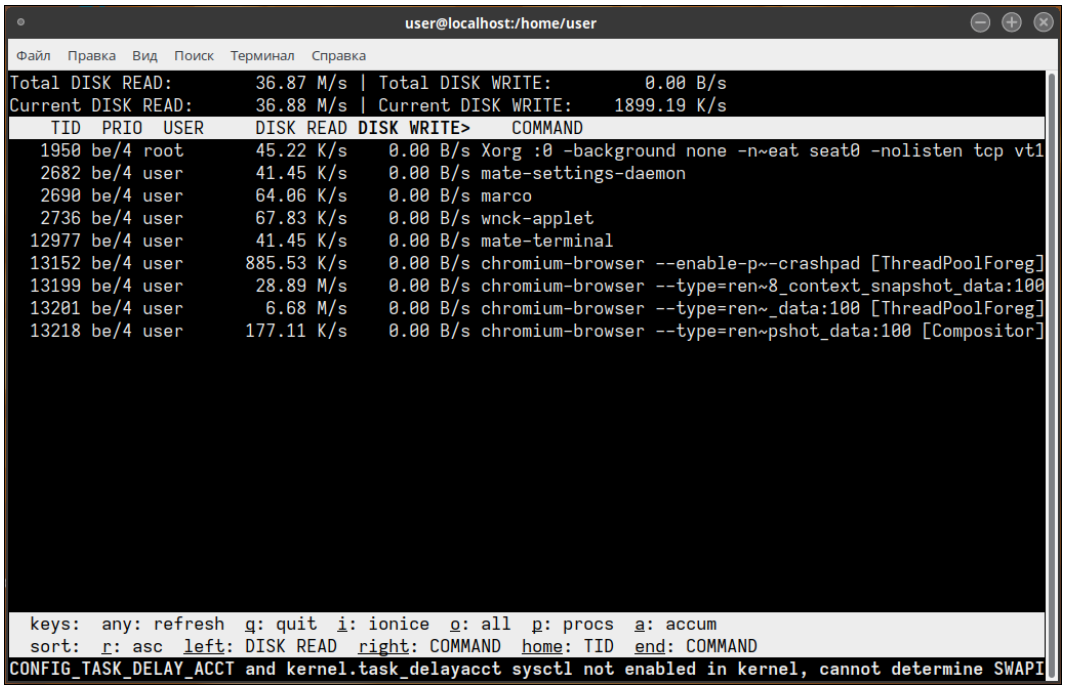
Для отключения интерактивного вида используйте:

```
iotop -b
```



Для отображения только процессов, которые в данный момент выполняют операции I/O с диском:

```
iotop -o
```

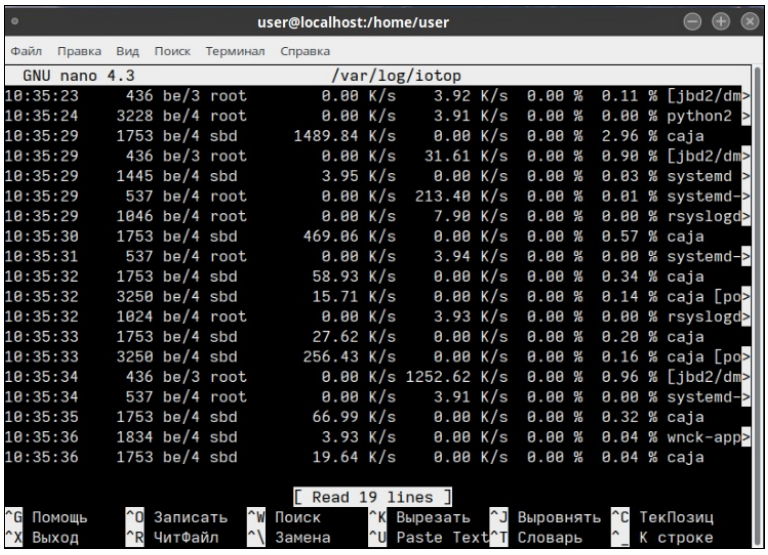


Программа позволяет не только выводить информацию, но и записывать ее для решения проблем в будущем.

Пример команды:

```
iotop -botqqqk --iter=60 >> /var/log/iotop
```

Результат можно посмотреть в указанном файле:



nfsiostat - утилита отображения статистики для файловых систем NFS

Синтаксис
Опции утилиты
Работа с утилитой

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: nfs-utils-1:2.5.2-0

nfsiostat – утилита отображения статистики операций ввода/вывода в файловых системах **NFS**.

Основные функции утилиты:

- отображение списка примонтированных NFS-каталогов;
- отслеживание скорости работы с каталогами;
- возможность просмотра статистики по определенному каталогу.

По умолчанию утилита предустановлена в РЕД ОС. Однако если по каким-либо причинам утилита отсутствует в вашей системе, для ее установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install nfs-utils
```

Для запуска утилиты перейдите в терминал и выполните команду (с правами **непривилегированного** пользователя):

```
nfsiostat
```

Синтаксис

Синтаксис утилиты имеет вид:

```
nfsiostat [ <интервал> [ <количество_отчетов> ] ] [ <опции> ] [ <точка_монтирования> ]
```

где:

- `<интервал>` – определяет интервал времени в секундах между каждым отчетом. Первый отчет содержит статистику за время с момента подключения файловой системы. Каждый последующий отчет содержит статистику, собранную за интервал времени, прошедший с момента предыдущего отчета. Отчет состоит из строки заголовка NFS, за которой следует строка статистики для каждой смонтированной сетевой файловой системы.
- `<количество_отчетов>` – определяет количество отчетов, созданных с интервалом в несколько секунд, можно указать вместе с параметром `<интервал>`. Если параметр `<интервал>` указан без параметра `<количество_отчетов>`, тогда утилита **nfsiostat** генерирует отчеты непрерывно.
- `<точка_монтирования>` – если указаны имена точек монтирования, будет отображаться статистика только для них. В противном случае перечисляются все точки монтирования NFS на клиенте.

Опции утилиты

Опции утилиты:

- **-h**, **--help** – вывод справки по утилите;
- **--version** – вывод версии утилиты.

Опции статистики:

- **-a**, **--attr** – отображать статистику, относящуюся к кешу атрибутов;

- **-d**, **--dir** – отображать статистику, относящуюся к операциям с каталогами;
- **-p**, **--page** – отображать статистику, относящуюся кешу страниц.

Опции формата отображения:

- **-s**, **--sort** – сортировать точки монтирования NFS по скорости работы;
- **-l <список>**, **--list=<список>** – выводить статистику только для первой точки монтирования в списке.

Работа с утилитой

Далее будут рассмотрены примеры работы с утилитой:

- вывод статистики с обновлением статистики каждые 5 секунд:

```
nfsiostat 5
```

где **5** – интервал обновления.

- вывод 10 отчетов с интервалом обновления статистики каждые 20 секунд:

```
nfsiostat 20 10
```

где:

- **20** – интервал обновления статистики;
- **10** – количество отчетов.
- запуск утилиты для определенной точки монтирования:

```
nfsiostat /home/test/
```

Пример:

На тестовом сервере примонтирован сетевой ресурс **/home/test** на источнике **10.81.186.174**. Запустим утилиту:

```
nfsiostat
```

```
[root@redos /]# nfsiostat

10.81.186.174:/home/test mounted on /home/test:

           ops/s       rpc bklog
           3.100           0.000

read:              ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                   0.000           0.000           0.000        0 (0.0%)           0.000           0.000           0.000        0 (0.0%)
write:             ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                   0.000           0.000           0.000        0 (0.0%)           0.000           0.000           0.000        0 (0.0%)
```

Утилита **nfsiostat** без параметров выведет список примонтированных ресурсов и текущую скорость работы с ними.

Запустим утилиту в момент копирования файла с источника.

Утилита **nfsiostat** покажет скорость загрузки.

```
[root@redos /]# nfsiostat

10.81.186.174:/home/test mounted on /home/test:

           ops/s       rpc bklog
          63.640           0.000

read:              ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                  63.430        8136.508         128.275        0 (0.0%)           0.399           0.496           0.027        0 (0.0%)
write:             ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                   0.000           0.000           0.000        0 (0.0%)           0.000           0.000           0.000        0 (0.0%)
```

В выводе утилиты также содержится важный параметр `avg RTT` – продолжительность времени с момента отправки ядром клиента запроса до момента получения ответа.

Высокий показатель `avg RTT` отражает высокую задержку в сети, которая влияет на производительность ввода-вывода, из-за чего могут возникнуть сложности работы с сетевым каталогом.

perf - анализ производительности ПО

Установка
Синтаксис
Опции
Команда bench
Команда stat
Команда top
Команда record
Команда report

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** perf 3.3.1-4

Perf - инструмент для анализа производительности программного обеспечения.

Через данную утилиту приложения могут использовать блок мониторинга производительности (PMU), точки трассировки и специальные счетчики в ядре для сбора статистики производительности.

Perf может не только анализировать проблемы производительности указанного приложения (для каждого потока), но и анализировать проблемы производительности ядра. Он также может анализировать код приложения и ядро одновременно, чтобы полностью понять узкие места производительности в приложении.

Установка

Для установки утилиты выполните команду:

```
sudo dnf install perf
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
perf [--version] [--help] [<опции>] <команда> [<аргументы>]
```

Опции

Основные опции утилиты:

- **--debug** — устанавливает для отладочных переменных значения от **0** до **10**, позволяя устанавливать следующие переменные:
    - **verbose** – базовые отладочные сообщения;
    - **ordered-events** – отладочные сообщения упорядоченных событий;
    - **data-convert** – отладочные сообщения команд преобразования данных;
    - **stderr** – запись отладочных сообщений (опция **-v**) на *stderr* в режиме браузера.

  Большее значение задает более подробный вывод.
- **--buildid-dir** — задает каталог кэширования идентификаторов сборки (эта опция имеет более высокий приоритет по сравнению с переменной buildid.dir в файле конфигурации);
- **-v, --version** — выводит версию программы *perf*;
- **-h, --help** — выводит справку о команде *perf*.

Команды утилиты

Команда bench

bench — общая база для тестов производительности.

Синтаксис

```
perf bench [<опции_общего_назначения>] <подсистемы> <тесты> [<опции_тестов>]
```

Опции общего назначения

- **-r, --repeat=<число>** - задаёт число повторения тестов (по умолчанию **10**);
- **-f, --format=<значение>** - задаёт стиль форматирования вывода:
  - **default** - принятый по умолчанию стиль, удобный для восприятия человеком;
  - **simple** - упрощённый стиль, удобный для обработки в программных сценариях.

Подсистемы

- **sched** - механизмы планировщиков и коммуникации между процессами (*IPC*);
- **mem** - производительность доступа к памяти;
- **numa** - планирование *NUMA* и производительность *MM*;
- **futex** -стрессовые тесты *Futex*;
- **epoll** - стрессовые тесты опроса событий (*epoll*);
- **all** - все подсистемы тестирования.

Тесты

Тесты для sched

messaging - набор тестов для оценки производительности механизмов планирования и IPC.

Опции *messaging*:

- **-p, --pipe** - использовать `pipe()` вместо `socketpair()`.
- **-t, --thread** - использовать множество потоков (`thread`) вместо множества процессов.
- **-g, --group=<число>** - задаёт число групп.
- **-l, --nr_loops=<число>** - задаёт число циклов.

pipe - тесты для системных вызовов `pipe()`.

Опции *pipe*:

- **-l, --loop=<число>** - задаёт число циклов.

Пример работы

```
 perf bench sched messaging

# Running 'sched/messaging' benchmark:
# 20 sender and receiver processes per group
# 10 groups == 400 processes run

     Total time: 2.886 [sec]

 perf bench sched messaging -t -g 20

# Running 'sched/messaging' benchmark:
# 20 sender and receiver threads per group
# 20 groups == 800 threads run
```

```
    Total time: 4.028 [sec]

 perf bench sched pipe

# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 9.023 [sec]

      9.023075 usecs/op
       110826 ops/sec

 perf bench sched pipe -l 1000

# Running 'sched/pipe' benchmark:
# Executed 1000 pipe operations between two processes

    Total time: 0.010 [sec]

     10.278000 usecs/op
        97295 ops/sec
```

Тесты для mem

memcpy - набор тестов для оценки скорости простых операций копирования в памяти различными способами.

Опции *memcpy*:

- **-s, --size** - размер копируемого блока (по умолчанию 1 Мбайт). Задаётся числом с суффиксом B, KB, MB, GB или TB (без учёта регистра символов).
- **-f, --function** - задаёт функцию копирования (по умолчанию **default**).
- **-l, --nr_loops** - задаёт повтор вызова memcpy указанное число раз.
- **-c, --cycles** - задаёт использование **perf** события `cpu-cycles` вместо системного вызова `gettimeofday`.

memset - набор тестов для оценки скорости простых операций установки памяти различными способами.

Опции для *memset*:

- **-s, --size** - размер копируемого блока (по умолчанию 1 Мбайт). Задаётся числом с суффиксом B, KB, MB, GB или TB (без учёта регистра символов).
- **-f, --function** - задаёт функцию копирования (по умолчанию **default**).
- **-l, --nr_loops** - задаёт повтор вызова memset указанное число раз.
- **-c, --cycles** - задаёт использование **perf** события `cpu-cycles` вместо системного вызова `gettimeofday`.

Пример работы

```
 perf bench mem memcpy

# Running 'mem/memcpy' benchmark:
# function 'default' (Default memcpy() provided by glibc)
# Copying 1MB bytes ...

     13.020833 GB/sec
# function 'x86-64-unrolled' (unrolled memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 1MB bytes ...

      9.765625 GB/sec
# function 'x86-64-movsq' (movsq-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 1MB bytes ...

      9.668936 GB/sec
# function 'x86-64-movsb' (movsb-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 1MB bytes ...
```

```
      9.964923 GB/sec


 perf bench mem memcpy -s 10MB -l 3

# Running 'mem/memcpy' benchmark:
# function 'default' (Default memcpy() provided by glibc)
# Copying 10MB bytes ...

     10.236504 GB/sec
# function 'x86-64-unrolled' (unrolled memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 10MB bytes ...

      3.372496 GB/sec
# function 'x86-64-movsq' (movsq-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 10MB bytes ...

      5.617809 GB/sec
# function 'x86-64-movsb' (movsb-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 10MB bytes ...

      5.426352 GB/sec
```

Тесты для numa

mem - набор тестов для оценки выполнения заданий NUMA.

Тесты для futex

- **hash** - тесты для оценки хэш-таблиц;
- **wake** - тесты для оценки вызовов *wake*;
- **wake-parallel** - тесты для оценки параллельных вызовов *wake*;
- **requeue** - тесты для оценки вызовов requeue;
- **lock-pi** - тесты для оценки вызовов *futex lock_pi*.

Опции, применимые для всех тестов:

- **-S, --shared** - использовать вызовы общих *futex* вместо приватных;
- **-s, --silent** - без вывода данных и деталей;
- **-t, --threads <число>** - задаёт число потоков (*thread*).

Опции для отдельных тестов:

- **-f, --futexes <число>** - задаёт число вызовов *futex* на поток (только *hash*);
- **-r, --runtime <число>** - задаёт время работы в секундах (*hash* и *lock-pi*);
- **-w, --nwakes <число>** - задаёт число потоков для разового пробуждения (*wake* и *wake-parallel*);
- **-q, --nrequeue <число>** - задаёт число потоков для разового изменения очерёдности (только *requeue*);
- **-M, --multi** - использовать множество *futex* (только *lock-pi*).

Тесты для epoll

wait - тесты для оценки одновременных вызовов **epoll_wait**.

Опции для *wait*:

- **-B, --nonblocking** - неблокируемое поведение *epoll_wait;*
- **-E, --edge** - использовать интерфейс **Edge-triggered** (по умолчанию *LT*);
- **-m, --multiq** - использовать множество экземпляров epoll (по одному на поток);
- **-S, --oneshot** - использовать семантику *EPOLLONESHOT*.

ctl - тесты для оценки множества вызовов **epoll_ctl**.

Опции, применимые для всех тестов:

- **-f, --nfds <число>** - задаёт число файловых дескрипторов для отслеживания каждым потоком;
- **-N, --nested <число>** - задаёт уровень вложенности для иерархии *epoll* (по умолчанию без вложенности - **0**);
- **-n, --noaffinity** - отключает близость CPU (*affinity*);
- **-R, --randomize** - задаёт выполнение случайных операций на случайных дескрипторах файлов;
- **-r, --runtime <число>** - задаёт время работы в секундах;
- **-t, --threads <число>** - задаёт число потоков (*thread*).;
- **-v, --verbose** - расширенный вывод.

Команда stat

stat - выполняет указанную параметром команду, собирая статистику работы.

Синтаксис

```
perf stat [-e <EVENT> | --event=EVENT] [-a] <команда>
perf stat [-e <EVENT> | --event=EVENT] [-a] - <команда> [<опции>]
perf stat [-e <EVENT> | --event=EVENT] [-a] record [-o <файл>] - <команда> [<опции>]
perf stat report [-i <файл>]
```

Опции команды

- **<command>...** - любая команда, которая может быть выполнена в консоли;
- **-e, --event=<значение>** - задаёт событие PMU;
- **-i, --no-inherit** - дочерние задачи не наследуют счётчики;
- **-p, --pid=<pid>** - события для процесса с заданными идентификаторами (список разделённых запятыми значений);
- **-t, --tid=<tid>** - события для потоков (*thread*) с заданными идентификаторами (список разделённых запятыми значений);
- **-a, --all-cpus** - сбор в масштабе системы от всех CPU (используется по умолчанию, если цель не задана);
- **--no-scale** - отключает масштабирование и нормализацию значений счётчиков;
- **-d, --detailed** - задаёт уровень детализации вывода;
- **-r, --repeat=<значение>** - повтор команды заданное число раз (**не более 100**) с усреднением и указанием стандартного отклонения. **0** - означает бесконечный повтор;
- **-B, --big-num** - задаёт вывод больших чисел с отделением тысяч в соответствии с установками **locale**;
- **-C, --cpu=<значение>** - задаёт учёт лишь указанных CPU, которые можно задать номерами через запятые без пробелов (**0,1**) или как диапазон (**0-2**). В режиме учёта по потокам эта опция игнорируется. Для мониторинга в масштабе системы сохраняется актуальность опции **-a**. По умолчанию учитываются все процессоры;
- **-A, --no-aggr** - отключает агрегирование счётчиков для отслеживаемых CPU;
- **-n, --null** - пустой прогон без запуска счётчиков;
- **-v, --verbose** - задаёт подробный вывод (показывает ошибки открытия счётчиков и т. п.);
- **--table** - задаёт вывод времени для каждого запуска (опция **-r**) в форме таблицы.

Пример работы

```
perf stat --null -r 5 --table perf bench sched pipe

# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes
```

```
    Total time: 8.769 [sec]

      8.769539 usecs/op
       114031 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 8.799 [sec]

      8.799256 usecs/op
       113645 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 8.958 [sec]

      8.958335 usecs/op
       111627 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 9.020 [sec]

      9.020829 usecs/op
       110854 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 9.080 [sec]

      9.080392 usecs/op
       110127 ops/sec

 Performance counter stats for 'perf bench sched pipe' (5 runs):

          # Table of individual measurements:
          8,7822 (-0,1613) #
          8,8164 (-0,1271) #
          8,9726 (+0,0291) #
          9,0432 (+0,0997) #
          9,1030 (+0,1595) #

          # Final result:
          8,9435 +- 0,0626 seconds time elapsed  ( +-  0,70% )
```

stat record - запись статистики в файл (по умолчанию **perf.data**).

Опции:

- **-i <файл>** - запись в выбранный файл.

stat raport - считывает файл данных **perf.data**, созданный командой perf record, и выводит профиль производительности, построенный по собранным ранее данным.

Опции:

- **-i <файл>, --input <файл>** - имя входного файла данных;
- **--per-socket** - объединение счётчиков по физическим процессорам для измерений в масштабе системы;
- **--per-core** - объединение счётчиков по ядрам одного физического процессора для измерений в масштабе системы;
- **-A, --no-aggr** - отключает объединение данных для всех отслеживаемых CPU.

Команда top

top - создание и вывод профиля производительности в реальном масштабе времени.

Синтаксис

```
perf top [-e <EVENT> | --event=EVENT] [<опции>]
```

Опции

- **-a, --all-cpus** - сбор данных на уровне системы в целом (используется по умолчанию);
- **-c <число>, --count=<число>** - период выборки событий;
- **-d <сек>, --delay=<сек>** - задает интервал обновления в секундах;
- **-v, --verbose** - задает подробный вывод (ошибки открытия счетчиков и т. п.).

Команда record

record - выполняет пользовательскую команду и записывает профиль работы в файл **perf.data**. Полученный файл можно затем использовать для подготовки отчёта с помощью perf report.

Синтаксис

```
perf record [-e <EVENT> | --event=EVENT] [-a] <команда>
perf record [-e <EVENT> | --event=EVENT] [-a] - <команда> [<опции>]
```

Опции

- **<command>...** - любая команда, которую можно выполнить в командном процессоре;
- **-c, --count=<число>** - период событий для выборки;
- **-o, --output=<файл>** - имя выходного файла;
- **-v, --verbose** - задаёт более подробный вывод (ошибки открытия счётчиков и т. п.);
- **-s, --stat** - задаёт запись счётчиков событий по потокам (*thread*). Для просмотра значений применяется команда perf report -T;
- **-d, --data** - запись виртуальных адресов выборок.

Команда report

report - считывает файл данных **perf.data**, созданный командой perf record, и выводит профиль производительности, построенный по собранным ранее данным.

Синтаксис

```
perf report [-i <файл> | --input=<файл>]
```

Опции

- **-i, --input=<файл>** - имя входного файла (по умолчанию **perf.data**, если *stdin* не является *fifo*);
- **-v, --verbose** - задаёт подробный вывод (адреса символов и т. п.);
- **-q, --quiet** - отменяет вывод сообщения, отменяя опцию **-v**;
- **-s, --sort=<ключ>** - задаёт сортировку гистограммы по указанным ключам.

tuned - служба оптимизации производительности системы

Tuned - это демон, который позволяет автоматически оптимизировать производительность системы под различные задачи, а также устанавливает системные параметры в соответствии с заданным профилем.

В службе **tuned** используются разные профили настроек для таких распространенных случаев использования, как высокая пропускная способность, низкая задержка или экономия энергии.

Служба **Tuned** по умолчанию предустановлена в РЕД ОС.

Вы можете подробнее ознакомиться с работой службы **tuned**, просмотрев наши обучающие видео:

- на **RuTube** — tuned - служба оптимизации производительности системы. Графическая утилита tuned-gtk;
- в **Яндекс.Дзен** — tuned - служба оптимизации производительности системы. Графическая утилита tuned-gtk;
- в **VK Видео** — tuned - служба оптимизации производительности системы. Графическая утилита tuned-gtk.

На наших каналах вы также сможете найти много другой полезной информации.

Включить **Tuned** можно командой:

```
systemctl enable --now tuned
```

Список профилей настроек:

Профиль	Описание профиля
balanced	Профиль для баланса между энергосбережением и производительностью
desktop	Профиль для повышения отклика графических приложений
throughput-performance	Профиль для установки максимальной пропускной способности
latency-performance	Профиль устанавливает низкую задержку за счет энергопотребления
network-latency	Профиль для установки дополнительных параметров настройки для обеспечения низкой задержки сети
network-throughput	Профиль для установки максимальной пропускной способности сети
powersave	Профиль для установки максимального энергосбережения
optimize-serial-console	Оптимизация для использования консоли
virtual-guest	Профиль оптимизации работы внутри гостевой системы при работе в среде виртуализации
virtual-host	Профиль оптимизации системы для максимальной производительности для запуска гостевых KVM
accelerator-performance	Настройка производительности с отключением состояний STOP с более высокой задержкой
hpc-compute	Оптимизация для вычислительных нагрузок HPC
intel-sst	Настройка для Intel Speed Select Technology (Intel SST)

Полный список **tuned** можно просмотреть при помощи команды:

```
tuned-adm list

Available profiles:
- accelerator-performance     - Throughput performance based tuning with disabled higher latency STOP states
- balanced                    - General non-specialized tuned profile
- desktop                     - Optimize for the desktop use-case
- hpc-compute                 - Optimize for HPC compute workloads
- intel-sst                   - Configure for Intel Speed Select Base Frequency
- latency-performance         - Optimize for deterministic performance at the cost of increased power consumption
- network-latency             - Optimize for deterministic performance at the cost of increased power consumption, focused on low latency
network performance
- network-throughput          - Optimize for streaming network throughput, generally only necessary on older CPUs or 40G+ networks
- optimize-serial-console     - Optimize for serial console use.
- powersave                   - Optimize for low power consumption
- throughput-performance      - Broadly applicable tuning that provides excellent performance across a variety of common server workloads
- virtual-guest               - Optimize for running inside a virtual guest
- virtual-host                - Optimize for running KVM guests
```

Проверка текущего профиля осуществляется командой:

```
tuned-adm active
```

```
No current active profile.
```

Для установки необходимого профиля нужно ввести команду:

```
tuned-adm profile <name>
```

где вместо **<name>** нужно указать необходимый профиль.

Далее следует проверить, что нужный профиль установлен, и подтвердить его командой:

```
tuned-adm active
```

Установите профиль максимальной производительности:

```
tuned-adm profile throughput-performance

tuned-adm active
Current active profile: throughput-perfomance
```

Для смены профиля на *сбалансированный* применяем аналогичные команды:

```
tuned-adm profile balanced
tuned-adm active Current active profile: balanced
```

Чтобы отключить данную службу нужно воспользоваться командами:

```
tuned-adm off
tuned-adm active No current active profile.
```

Графическая утилита tuned-gtk

Tuned можно настраивать через графическое приложение. Для установки пакета **tuned-gtk** перейдите в сеанс пользователя **root**:

```
su -
```

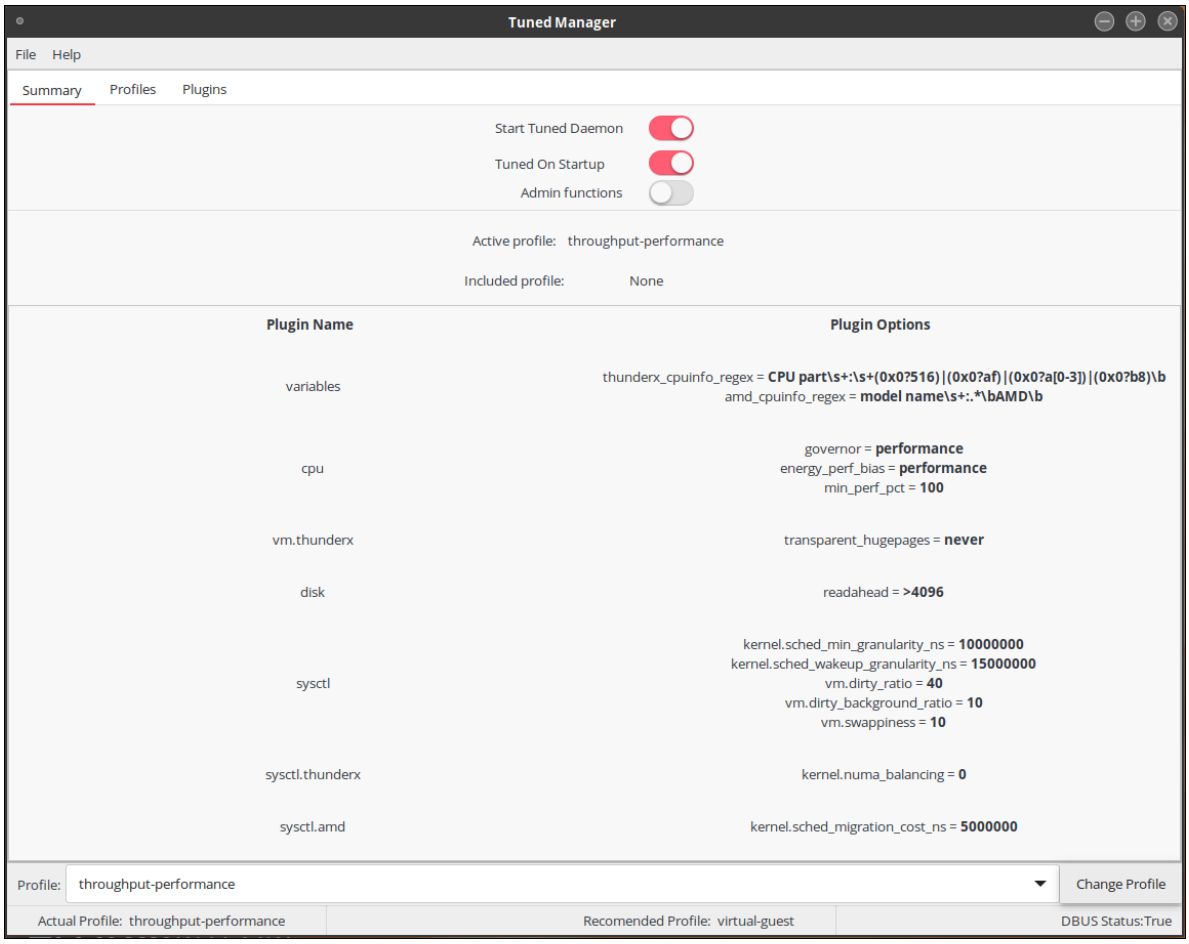
и выполните команду:

```
dnf install tuned-gtk
```

После установки утилита будет доступна из «**Главного меню**» — «**Параметры**» — «**tuned-gui**».

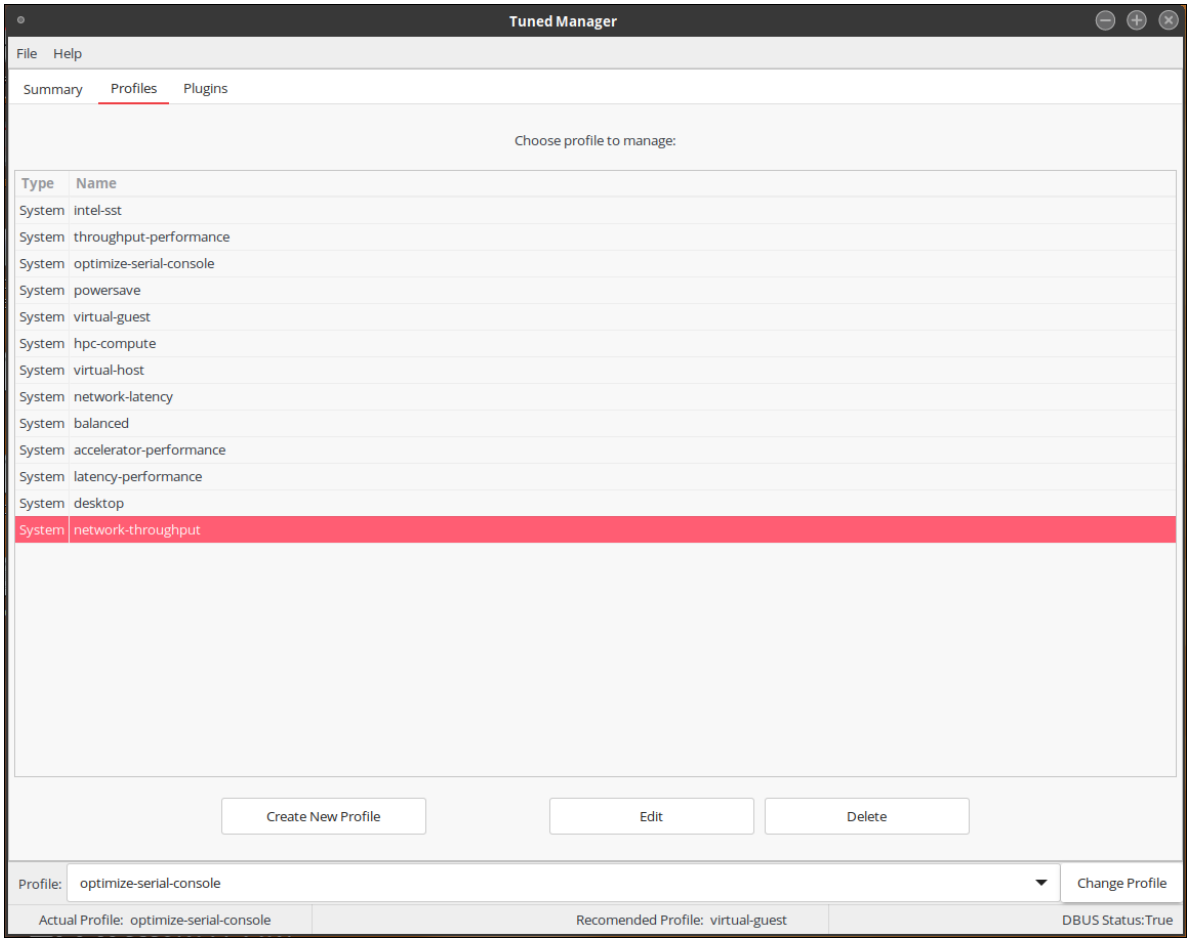
Обратите внимание, что перед использованием графической утилиты, необходимо сначала включить службу **Tuned** командой:

```
systemctl enable --now tuned
```

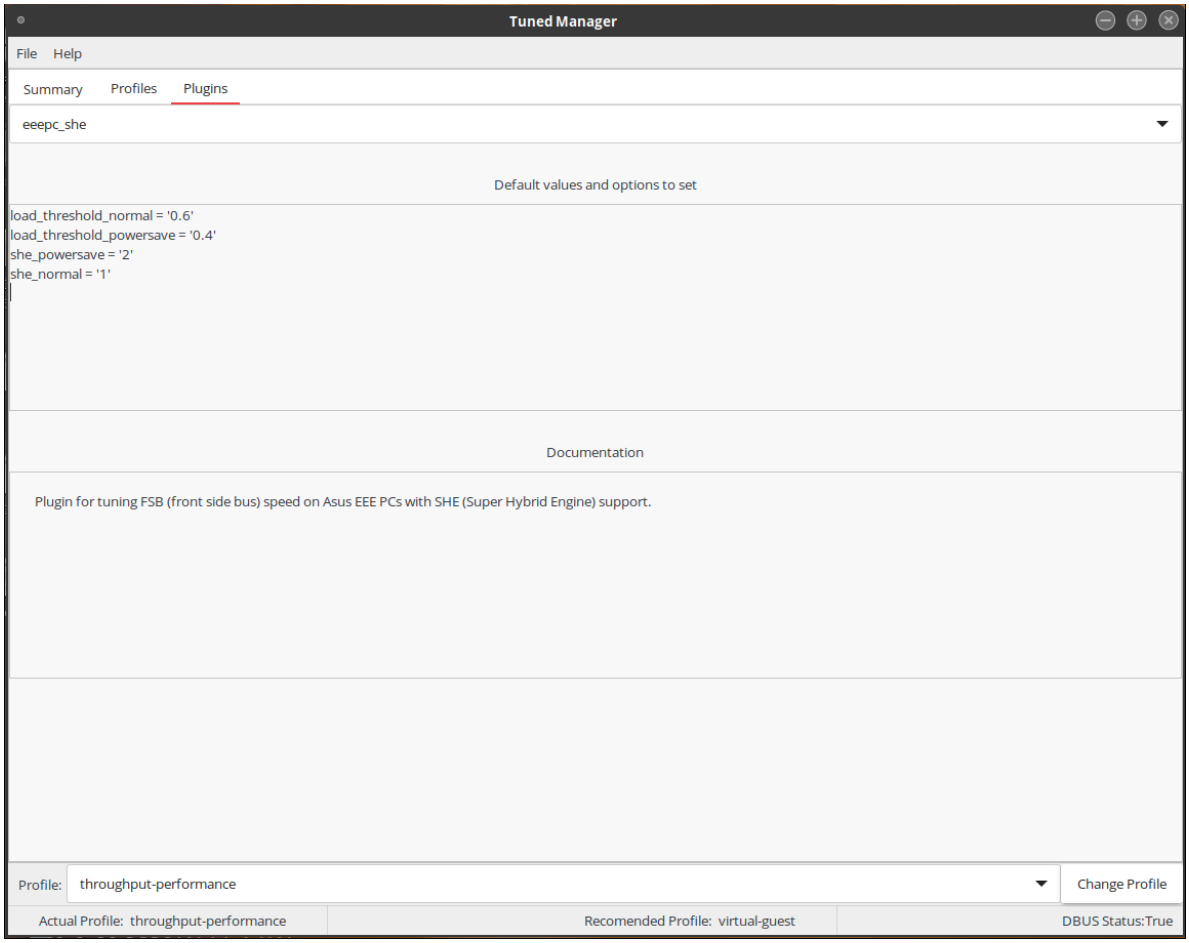


В приложении можно включить демон **tuned**, добавить его в автозапуск и выбрать необходимый профиль для работы системы. Изменить используемый профиль можно, выбрав профиль в списке «**Profile**» и затем нажав на кнопку «**Change Profile**».

На вкладке «**Profiles**» представлен список доступных профилей, а также есть возможность создать новый профиль, отредактировать или удалить уже имеющиеся профили.



Во вкладке «**Plugins**» в ниспадающем списке представлены имеющиеся плагины. При выборе любого из них будут выведены значения по умолчанию и поясняющая информация.



Тестирование производительности дисков с помощью fio

Установка
Синтаксис
Опции
Формат файла задания
Параметры файла задания
Примеры работы
Тесты производительности операций ввода-вывода в секунду
Тест скорости записи
Тест скорости чтения
Тест скорости чтения/записи
Тест пропускной способности
Использование файла задания
Тест с разными значениями iodepth
Удаление результатов тестирования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: fio-3.21-4

Fio (Flexible I/O Tester) — это инструмент, который позволяет запускать несколько потоков или процессов для выполнения операций ввода-вывода, заданных пользователем. Обычно **fio** используется для создания файла задания, описывающего нагрузку на ввод-вывод, которую необходимо смоделировать. Для получения точного результата тестирования производительности системы хранения данных важно учитывать несколько ключевых аспектов.

Выбор типов тестов и параметров **fio** является важным, поскольку такие настройки, как размер блока данных (**bs**) и количество задач (**numjobs**), могут существенно влиять на результаты. Изменение этих параметров может привести к получению различных данных о производительности. Поэтому следует стремиться к единообразию параметров на всех тестируемых стендах.

ВАЖНО!

Не запускайте тесты **fio** с рабочей нагрузкой на запись (**readwrite**, **randrw**, **write**, **trimwrite**) непосредственно на используемом устройстве. Для проведения таких тестов рекомендуется использовать тестовые среды или резервные устройства, чтобы избежать потери данных и негативных последствий для основного рабочего устройства.

Установка

Для установки утилиты выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install fio
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
fio [<Опции>] [<Файл задания>]
```

Опции

Основные опции **fio**:

- **--debug=<параметры>** — включает ведение журнала отладки;
- **--parse-only** — анализирует файл задания и выводит настройки, без операций ввода;
- **--merge-blktrace-only** — объединяет вывод **blktrace** (трассировка блоков) из предыдущих тестов;
- **--output=имя_файла** — указывает файл для записи результатов;

- **--output-format=формат** — устанавливает формат вывода;
- **--bandwidth-log** — включает ведение журнала пропускной способности;
- **--minimal** — выводит минимально необходимую информацию;
- **--append-terse** — дополняет короткий вывод предыдущих результатов;
- **--terse-version=версия** — указывает версию для короткого вывода;
- **--version** — выводит информацию о версии программы и завершает работу;
- **--help** — показывает справку по командам;
- **--cpuclock-test** — тестирует тактовую частоту процессора;
- **--crctest=[тест]** — запускает тест контрольной суммы;
- **--cmdhelp=команда** — выводит справку по указанной команде;
- **--enghelp=[ввод-вывод[,команда]]** — выводит справку по указанному механизму ввода-вывода и команде;
- **--showcmd** — показывает команду, которую нужно использовать для запуска текущей конфигурации;
- **--readonly** — работает в режиме только для чтения;
- **--eta=when** — показывает время до завершения (ETA) теста;
- **--eta-interval=время** — интервал обновления информации о ETA;
- **--eta-newline=время** — интервал добавления новой строки в вывод ETA;
- **--status-interval=время** — интервал обновления статуса;
- **--section=имя** — указывает конкретный раздел конфигурации для выполнения;
- **--alloc-size=kb** — устанавливает размер выделения памяти в КБ;
- **--warnings-fatal** — обрабатывает предупреждения как ошибки;
- **--max-jobs=номер** — максимальное количество параллельных задач;
- **--server=аргументы** — запускает **fio** в режиме сервера с указанными аргументами;
- **--daemonize=pid-файл** — запускает **fio** как фоновый процесс и записывает PID в файл;
- **--client=имя_хоста** — подключается к серверу **fio** на указанном хосте;
- **--remote-config=файл** — использует удалённый конфигурационный файл;
- **--idle-prof=опция** — формирует отчёт о простое процессора, опция может быть одной из следующих:
  - **calibrate** — выполняет калибровку и завершает работу;
  - **system** — показывает общий уровень простоя системы и единичную работу;
  - **percpu** — как system, но также показывает время простоя каждого процессора;
- **--inflate-log=журнал_регистрации** — увеличить размер лог-файла;
- **--trigger-file=файл** — выполняет команду запуска, когда файл существует;
- **--trigger-timeout=время** — время ожидания перед запуском триггера;
- **--trigger=команда** — устанавливает команду в качестве локального триггера;
- **--trigger-remote=команда** — устанавливает команду в качестве удалённого запуска;
- **--aux-path=путь** — вспомогательный путь для временных файлов вместо текущего рабочего каталога.

Формат файла задания

Любые параметры, следующие за **опциями**, будут считаться **файлами заданий**, если они не соответствуют параметру файла задания. В списке может быть несколько файлов заданий, и каждый файл задания будет рассматриваться как отдельная группа.

Fio принимает один или несколько файлов заданий, описывающих, что он должен делать. **Формат файла задания** — классический ini-файл, в котором имена, заключённые в квадратные скобки [], определяют название задания. Можно использовать любое имя в формате ASCII, кроме **global**, которое имеет предопределенное значение. После названия задания указывается последовательность из параметров, которые определяют поведение задания.

В разделе global устанавливаются значения по умолчанию для заданий, описанных в этом файле. Задание может переопределять параметр *global* section, а файл задания может также содержать несколько **глобальных параметров**.

Параметры файла задания

Для некоторых параметров используется параметр определённого типа, например, целое число или строка. Везде, где требуется числовое значение, можно использовать арифметическое выражение, при условии, что оно заключено в круглые скобки.

Поддерживаются следующие операции:

- сложение **(+)**,
- вычитание **(-)**,
- умножение **(*)**,
- деление **(/)**,
- модуль **(%)**,
- возведение в степень **(^)**.

Для значений времени в выражениях по умолчанию единицами измерения являются микросекунды.

Основные параметры для задания:

- **--name** — имя теста (можно изменить на любое другое);
- **--filename** — путь к файлу, который будет использоваться для тестирования I/O;
- **--directory** — каталог, который будет использоваться для тестирования I/O;
- **--size** — размер файла для теста;
- **--direct** — использование прямых I/O, обходящих кеш операционной системы;
- **--rw** — режим теста (чтение, запись или оба);
- **--bs** — размер блока ввода-вывода (I/O) для теста;
- **--ioengine** — механизм ввода-вывода, который будет использоваться для теста (например, libaio для асинхронного ввода-вывода);
- **--iodepth** — глубина очереди запросов на ввод-вывод для теста (количество одновременных запросов к файловой системе);
- **--runtime** — время выполнения теста;
- **--numjobs** — количество параллельных задач для теста;
- **--time_based** — время работы будет использоваться для определения длительности теста;
- **--group_reporting** — режим групповой отчётности (результаты будут отображаться для каждой группы рабочих нитей, а не для каждого рабочего потока);
- **--eta-newline** — интервал отображения прогресса выполнения теста и перевода строки.

Примеры работы

Тесты производительности операций ввода-вывода в секунду

Для тестирования пропускной способности используется одновременное чтение и запись небольшими блоками с использованием множества процессов. Тесты измеряют количество операций **чтения/записи**, которые система может выполнить за секунду.

Тесты являются показателем производительности хранилища данных или системы ввода-вывода и позволяют оценить **скорость обработки операций** ввода и вывода данных, независимо от их объёма. Чем выше значение **IOPS**, тем быстрее система может обрабатывать запросы на чтение и запись данных.

ВАЖНО!

При выполнении тестирования на запись в указанном файле данные перезаписываются. Поэтому не рекомендуется указывать в качестве файла блочное устройство с нужными данными.

Тест скорости записи

Перед выполнением теста убедитесь, что в указанной директории достаточно свободного места (более 5 ГБ) для завершения теста.

```
fio --name=fiotest --blocksize=4k --directory=/home/user --size=5g --ioengine=libaio --iodepth=256 --runtime=60 --rw=randwrite --direct=1
```

где:

- **--name=fiotest** — имя теста (можно изменить на любое другое);

- **--blocksize=4k** — размер блока данных для теста (4 КБ);
- **--directory=/home/user** — каталог, в котором будет проводиться тест;
- **--size=5g** — размер файла для теста (5 ГБ);
- **--ioengine=libaio** — использование libaio (асинхронный ввод-вывод);
- **--iodepth=256** — глубина очереди (256 запросов одновременно);
- **--runtime=60** — время выполнения теста (60 секунд);
- **--rw=randwrite** — режим теста (случайная запись);
- **--direct=1** — использование прямого доступа к устройству (чтобы избежать кеширования данных).

В результате запуска команды будет проведён тест производительности I/O на указанном каталоге с указанными параметрами.

Результат:

```
fiotest: (g=0): rw=randwrite, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
fio-3.28
Starting 1 process
fiotest: Laying out IO file (1 file / 5120MiB)
Jobs: 1 (f=1): [w(1)][100.0%][w=33.4MiB/s][w=8540 IOPS][eta 00m:00s]
fiotest: (groupid=0, jobs=1): err= 0: pid=3906: Tue Jul 30 12:05:52 2024
  write: IOPS=1354, BW=5418KiB/s (5548kB/s)(317MiB/60001msec); 0 zone resets
    slat (usec): min=4, max=7229.8k, avg=733.37, stdev=53817.01
    clat (usec): min=23, max=11931k, avg=188197.99, stdev=1188675.61
     lat (usec): min=89, max=11931k, avg=188931.83, stdev=1190998.57
    clat percentiles (msec):
     |  1.00th=[   10],  5.00th=[   12], 10.00th=[   12], 20.00th=[   13],
     | 30.00th=[   13], 40.00th=[   14], 50.00th=[   14], 60.00th=[   15],
     | 70.00th=[   20], 80.00th=[   27], 90.00th=[   75], 95.00th=[  184],
     | 99.00th=[ 7886], 99.50th=[11476], 99.90th=[11879], 99.95th=[11879],
     | 99.99th=[11879]
   bw (  KiB/s): min=    8, max=68669, per=100.00%, avg=17068.00, stdev=18091.84, samples=35
   iops        : min=    2, max=17167, avg=4266.94, stdev=4522.95, samples=35
  lat (usec)   : 50=0.01%, 100=0.01%, 250=0.01%, 500=0.02%, 750=0.02%
  lat (usec)   : 1000=0.02%
  lat (msec)   : 2=0.07%, 4=0.12%, 10=1.00%, 20=69.48%, 50=15.80%
  lat (msec)   : 100=5.15%, 250=4.88%, 500=0.76%, 750=0.08%, 1000=0.57%
  lat (msec)   : 2000=0.16%, >=2000=1.87%
  cpu          : usr=0.67%, sys=4.04%, ctx=77891, majf=0, minf=15
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=99.9%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=0,81270,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
  WRITE: bw=5418KiB/s (5548kB/s), 5418KiB/s-5418KiB/s (5548kB/s-5548kB/s), io=317MiB (333MB), run=60001-60001msec

Disk stats (read/write):
  sda: ios=3/77906, merge=0/1835, ticks=63/698196, in_queue=716266, util=95.37%
```

где:

- **slat** — задержка отправки (submission latency). Это время, которое затрачивается на передачу запроса ввода-вывода в очередь устройства;
- **clat** — задержка выполнения (completion latency). Это время, которое прошло с момента передачи запроса устройству до его завершения и возврата результата;
- **lat** — общая задержка (total latency) — это сумма slat+clat;
- **bw** — пропускная способность: количество образцов и процент от общей пропускной способности;
- **iops** — количество операций ввода-вывода, выполненных за одну секунду. Показатель производительности хранилища. Чем выше IOPS, тем больше операций устройство способно обработать за единицу времени;
- **lat (nsec/usec/msec)** — распределение задержек завершения операций ввода-вывода;
- **cpu** — отражает статистику использования ресурсов процессора (CPU) во время выполнения теста ввода-вывода;
- **IO depths** — распределение глубин ввода-вывода за время существования задания;
- **IO submit** — количество операций ввода-вывода, отправленных в одном вызове;

- **IO complete** — количество завершённых операций ввода-вывода;
- **IO issued rwt** — количество отправленных запросов на чтение/запись/обрезку, короткие или отброшенные;
- **IO latency** — задержки ввода-вывода для достижения заданной цели.

После того как каждый клиент был перечислен, появляются **статистические данные для группы**:

```
Run status group 0 (all jobs):
  WRITE: bw=5418KiB/s (5548kB/s), 5418KiB/s-5418KiB/s (5548kB/s-5548kB/s), io=317MiB (333MB), run=60001-60001msec
```

где:

- **WRITE** — указывает, что результаты относятся к операциям записи;
- **bw** — совокупная пропускная способность потоков в заданной группе, за которой следуют минимальная и максимальная пропускная способность всех потоков в группе. 5418KiB/s-5418KiB/s (5548kB/s-5548kB/s) — диапазон скоростей записи, достигнутых в ходе теста, является фиксированным;
- **io** — совокупный объём выполненных операций ввода-вывода всех потоков в группе;
- **run** — самое короткое и самое длинное время выполнения потоков в группе.

В конце выводится **статистика по дискам**:

```
Disk stats (read/write):
  sda: ios=3/77906, merge=0/1835, ticks=63/698196, in_queue=716266, util=95.37%
```

где:

- **ios** — количество операций ввода-вывода, выполненных всеми группами (**3** — количество операций чтения, **77906** — количество операций записи);
- **merge** — количество объединений, выполненных планировщиком ввода-вывода (иногда несколько операций могут быть объединены в одну, чтобы снизить нагрузку на систему). **0** — количество объединённых операций чтения, **1835** — количество объединённых операций записи.
- **ticks** — количество тактов, в течение которых диск был занят, **63** — время, затраченное на операции чтения (в миллисекундах), **698196** — время, затраченное на операции записи (в миллисекундах);
- **in_queue** — общее время, проведённое в очереди на выполнение (в миллисекундах);
- **util** — занятость устройства, отображаемая в процентах (**95.37%**). Значение, близкое к **100%**, может указывать на высокую загрузку диска и на необходимость оптимизации или добавления дополнительного оборудования.

Тест скорости чтения

Для корректного выполнения команды тестирования скорости чтения с приведёнными ниже параметрами необходимо выполнить следующие условия:

- для выполнения теста в директории /home/user автоматически будут созданы файлы для каждого задания, количество которых определяется параметром **--numjobs,** размер файлов определяется параметром **--size**;
- пользователь, под которым запускается команда **fio**, должен иметь права на чтение/запись файлов в директории /home/user.

```
 fio --directory=/home/user --direct=1 --rw=randread --bs=4k --ioengine=libaio --iodepth=256 --runtime=60 --numjobs=3 --time_based --group_reporting --name=iops-test-job --eta-newline=1 --size=1G
```

где:

- **--directory=/home/user** — каталог /home/user, в котором будут созданы тестовые файлы;
- **--direct=1** — включает режим прямого ввода-вывода, обходя кеширование в операционной системе;
- **--rw=randread** — тип выполняемых операций ввода-вывода (randread означает случайное чтение). В режиме randread **fio** будет случайным образом выбирать блоки для чтения;
- **--bs=4k** — устанавливает размер блока ввода-вывода на 4 КБ, каждая операция чтения будет обрабатывать 4 КБ данных;
- **--ioengine=libaio** — указывает механизм ввода-вывода, **libaio** использует асинхронные операции ввода-вывода, позволяет одновременно запускать несколько запросов ввода-вывода, не дожидаясь завершения предыдущих;
- **--iodepth=256** — задаёт глубину очереди операций ввода-вывода, 256 операций могут находиться в очереди на выполнение одновременно;
- **--runtime=60** — устанавливает время выполнения теста в секундах;

- **--numjobs=3** — определяет количество параллельно выполняемых заданий, тест будет выполняться с тремя потоками;
- **--time_based** — указывает, что тест должен быть основан на времени, а не на объёме данных;
- **--group_reporting** — включает групповой отчёт, результаты всех заданий будут объединены и представлены как один общий результат;
- **--name=iops-test-job** — имя задания;
- **--eta-newline=1** — опция, которая указывает **fio** обновлять строку с расчётным оставшимся временем (ETA) каждую секунду.

Результат:

```
iops-test-job: (g=0): rw=randread, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
...
fio-3.28
Starting 3 processes
Jobs: 3 (f=3): [r(3)][4.9%][r=129MiB/s][r=33.1k IOPS][eta 00m:58s]
Jobs: 3 (f=3): [r(3)][6.6%][r=120MiB/s][r=30.7k IOPS][eta 00m:57s]
Jobs: 3 (f=3): [r(3)][9.8%][r=128MiB/s][r=32.8k IOPS][eta 00m:55s]
Jobs: 3 (f=3): [r(3)][13.1%][r=138MiB/s][r=35.4k IOPS][eta 00m:53s]
Jobs: 3 (f=3): [r(3)][14.8%][r=139MiB/s][r=35.6k IOPS][eta 00m:52s]
Jobs: 3 (f=3): [r(3)][16.4%][r=137MiB/s][r=35.0k IOPS][eta 00m:51s]
Jobs: 3 (f=3): [r(3)][18.0%][r=139MiB/s][r=35.6k IOPS][eta 00m:50s]
Jobs: 3 (f=3): [r(3)][19.7%][r=139MiB/s][r=35.7k IOPS][eta 00m:49s]
Jobs: 3 (f=3): [r(3)][21.3%][r=133MiB/s][r=34.0k IOPS][eta 00m:48s]
Jobs: 3 (f=3): [r(3)][24.6%][r=139MiB/s][r=35.7k IOPS][eta 00m:46s]
Jobs: 3 (f=3): [r(3)][27.9%][r=138MiB/s][r=35.3k IOPS][eta 00m:44s]
Jobs: 3 (f=3): [r(3)][29.5%][r=140MiB/s][r=35.8k IOPS][eta 00m:43s]
Jobs: 3 (f=3): [r(3)][32.8%][r=139MiB/s][r=35.5k IOPS][eta 00m:41s]
Jobs: 3 (f=3): [r(3)][36.1%][r=140MiB/s][r=35.8k IOPS][eta 00m:39s]
Jobs: 3 (f=3): [r(3)][40.0%][r=139MiB/s][r=35.5k IOPS][eta 00m:36s]
Jobs: 3 (f=3): [r(3)][41.0%][r=139MiB/s][r=35.7k IOPS][eta 00m:36s]
Jobs: 3 (f=3): [r(3)][44.3%][r=140MiB/s][r=35.7k IOPS][eta 00m:34s]
Jobs: 3 (f=3): [r(3)][47.5%][r=138MiB/s][r=35.4k IOPS][eta 00m:32s]
Jobs: 3 (f=3): [r(3)][50.8%][r=139MiB/s][r=35.7k IOPS][eta 00m:30s]
Jobs: 3 (f=3): [r(3)][53.3%][r=138MiB/s][r=35.2k IOPS][eta 00m:28s]
Jobs: 3 (f=3): [r(3)][54.1%][r=126MiB/s][r=32.4k IOPS][eta 00m:28s]
Jobs: 3 (f=3): [r(3)][57.4%][r=139MiB/s][r=35.7k IOPS][eta 00m:26s]
Jobs: 3 (f=3): [r(3)][60.0%][r=139MiB/s][r=35.6k IOPS][eta 00m:24s]
Jobs: 3 (f=3): [r(3)][60.7%][r=139MiB/s][r=35.7k IOPS][eta 00m:24s]
Jobs: 3 (f=3): [r(3)][63.9%][r=139MiB/s][r=35.7k IOPS][eta 00m:22s]
Jobs: 3 (f=3): [r(3)][65.6%][r=139MiB/s][r=35.7k IOPS][eta 00m:21s]
Jobs: 3 (f=3): [r(3)][68.9%][r=139MiB/s][r=35.7k IOPS][eta 00m:19s]
Jobs: 3 (f=3): [r(3)][70.5%][r=136MiB/s][r=34.9k IOPS][eta 00m:18s]
Jobs: 3 (f=3): [r(3)][73.8%][r=134MiB/s][r=34.2k IOPS][eta 00m:16s]
Jobs: 3 (f=3): [r(3)][78.3%][r=135MiB/s][r=34.5k IOPS][eta 00m:13s]
Jobs: 3 (f=3): [r(3)][80.3%][r=135MiB/s][r=34.5k IOPS][eta 00m:12s]
Jobs: 3 (f=3): [r(3)][83.6%][r=136MiB/s][r=34.7k IOPS][eta 00m:10s]
Jobs: 3 (f=3): [r(3)][85.2%][r=133MiB/s][r=34.2k IOPS][eta 00m:09s]
Jobs: 3 (f=3): [r(3)][86.9%][r=134MiB/s][r=34.3k IOPS][eta 00m:08s]
Jobs: 3 (f=3): [r(3)][88.5%][r=133MiB/s][r=34.1k IOPS][eta 00m:07s]
Jobs: 3 (f=3): [r(3)][91.8%][r=136MiB/s][r=34.8k IOPS][eta 00m:05s]
Jobs: 3 (f=3): [r(3)][95.1%][r=128MiB/s][r=32.6k IOPS][eta 00m:03s]
Jobs: 3 (f=3): [r(3)][96.7%][r=126MiB/s][r=32.2k IOPS][eta 00m:02s]
Jobs: 3 (f=3): [r(3)][100.0%][r=130MiB/s][r=33.2k IOPS][eta 00m:00s]
iops-test-job: (groupid=0, jobs=3): err= 0: pid=3593: Tue Jul 30 21:43:19 2024
  read: IOPS=34.7k, BW=136MiB/s (142MB/s)(8133MiB/60007msec)
    slat (nsec): min=1166, max=97127k, avg=75924.61, stdev=510067.56
    clat (usec): min=2, max=123674, avg=22035.95, stdev=4534.57
     lat (msec): min=6, max=123, avg=22.11, stdev= 4.54
    clat percentiles (msec):
     |  1.00th=[   16],  5.00th=[   18], 10.00th=[   19], 20.00th=[   20],
     | 30.00th=[   21], 40.00th=[   21], 50.00th=[   22], 60.00th=[   23],
     | 70.00th=[   24], 80.00th=[   24], 90.00th=[   26], 95.00th=[   27],
     | 99.00th=[   34], 99.50th=[   40], 99.90th=[   91], 99.95th=[  101],
     | 99.99th=[  117]
   bw (  KiB/s): min=103294, max=148248, per=100.00%, avg=138926.83, stdev=2412.68, samples=357
   iops        : min=25823, max=37062, avg=34731.20, stdev=603.19, samples=357
  lat (usec)   : 4=0.01%
  lat (msec)   : 10=0.03%, 20=27.34%, 50=72.31%, 100=0.25%, 250=0.06%
  cpu          : usr=2.31%, sys=13.81%, ctx=45133, majf=0, minf=805
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
```

```
   submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
   complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
   issued rwts: total=2081938,0,0,0 short=0,0,0,0 dropped=0,0,0,0
   latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
  READ: bw=136MiB/s (142MB/s), 136MiB/s-136MiB/s (142MB/s-142MB/s), io=8133MiB (8528MB), run=60007-60007msec

Disk stats (read/write):
 sda: ios=2055328/37, merge=82/22, ticks=487922/130, in_queue=488058, util=80.34%
```

где:

- **iops** — среднее количество операций ввода/вывода в секунду (34,700 операций чтения в секунду);
- **bw** — средняя скорость передачи данных — 136 МБ/с;
- **latency** — среднее время, которое требуется для завершения одной операции чтения — 22.11 миллисекунды;
- **clat percentiles** — показывает время завершения операций (completion latency, clat) в миллисекундах (ms):
  - 1% операций завершается за 16 мс или меньше;
  - 50% операций завершается за 22 мс или меньше;
  - 99% операций завершается за 34 мс или меньше.
- **cpu** — процентное использование процессора: usr=2.31%, sys=13.81% (2.31% используется для пользовательских задач, 13.81% для системных задач), ctx - Количество переключений контекста (context switches) между процессами. Много переключений контекста может указывать на сильную конкуренцию за ресурсы или неэффективную работу с очередями I/O.
- **IO depths** — все операции ввода/вывода были выполнены с глубиной очереди 64 или больше: >=64=100.0%;
- **Run status group:**
  - io - общее количество данных прочитано: 8133 МБ (8.528 ГБ);
  - bw (Bandwidth) - средняя скорость чтения: 136 МБ/с;
  - run - общее время выполнения теста: 60007 мс (60.007 секунд);
- **Disk stats (read/write):**
  - ios=2055328/37 - выполнено 2055328 операций чтения и 37 операций записи.
  - merge=82/22 - показатель, сколько операций чтения/записи были объеденены в одно обращение.
  - ticks - Время обработки операций ввода-вывода: 487922 мс затрачено на операции чтения, 130 мс затрачено на операции записи.
  - in_queue - отражает суммарное время ожидания всех запросов в миллисекундах.
  - util - Утилизация диска (время, в течение которого устройство было занято обработкой операций) составила 80.34%.

Результат показывает:

- выполнение операций чтения с пропускной способностью в 136 МБ/с и 34.7k IOPS;
- среднее время задержки в 22 мс. Высокий показатель 95-го перцентиля (27 мс) указывает на стабильное выполнение большинства операций что задержки относительно стабильны и приемлемы для большинства операций;
- процент использования процессора относительно низкий, что указывает на то, что CPU не является узким местом в тесте.

Тест скорости чтения/записи

```
 fio --directory=/home/user --direct=1 --rw=randrw --bs=4k --ioengine=libaio --iodepth=256 --runtime=60 --numjobs=3 --time_based --group_reporting --name=iops-test-job --eta-newline=1
```

где:

- **--directory=/home/user** — директория, где будут производиться тесты ввода-вывода;
- **--direct=1** — активирует прямой ввод-вывод, что означает, что операции не будут кешироваться операционной системой;
- **--rw=randrw** — режим работы, тест будет одновременно выполнять операции чтения и записи в случайном порядке;
- **--bs=4k** — устанавливает размер блока для операций ввода-вывода, размер блока равен 4 КБ (4096 байт);
- **--ioengine=libaio** — механизм ввода-вывода, libaio — асинхронный ввод-вывод через библиотеку libaio;

- **--iodepth=256** — определяет глубину очереди ввода-вывода (256 — максимальное количество операций ввода-вывода, которые могут находиться в ожидании одновременно);
- **--runtime=60** — устанавливает время работы теста в секундах — 60 секунд (1 минута);
- **--numjobs=3** — количество задач, которые будут выполняться параллельно;
- **--time_based** — задаёт режим тестирования по времени, а не по количеству операций;
- **--group_reporting** — указывает, что результаты теста должны группироваться и выводиться в одном отчёте для всех задач, а не по отдельности для каждой;
- **--name=iops-test-job** — задаёт имя теста, которое будет отображаться в результатах;
- **--eta-newline=1** — выводит оставшееся время в следующей строке в процессе выполнения теста.

Результат:

```
iops-test-job: (g=0): rw=randrw, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
...
fio-3.28
Starting 3 processes
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1053564928, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1066758144, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1072381952, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1066737664, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1039486976, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1033895936, buflen=4096
fio: pid=3773, err=28/file:io_u.c:1845, func=io_u error, error=No space left on device
Jobs: 2 (f=2): [m(2),X(1)][4.9%][r=47.4MiB/s,w=46.8MiB/s][r=12.1k,w=12.0k IOPS][eta 00m:58s]
Jobs: 2 (f=2): [m(2),X(1)][8.2%][r=51.2MiB/s,w=50.3MiB/s][r=13.1k,w=12.9k IOPS][eta 00m:56s]
Jobs: 2 (f=2): [m(2),X(1)][9.8%][r=47.4MiB/s,w=48.7MiB/s][r=12.1k,w=12.5k IOPS][eta 00m:55s]
Jobs: 2 (f=2): [m(2),X(1)][11.5%][r=44.5MiB/s,w=44.5MiB/s][r=11.4k,w=11.4k IOPS][eta 00m:54s]
Jobs: 2 (f=2): [m(2),X(1)][13.1%][r=47.0MiB/s,w=46.6MiB/s][r=12.0k,w=11.9k IOPS][eta 00m:53s]
Jobs: 2 (f=2): [m(2),X(1)][16.4%][r=44.6MiB/s,w=45.0MiB/s][r=11.4k,w=11.5k IOPS][eta 00m:51s]
Jobs: 2 (f=2): [m(2),X(1)][18.0%][r=47.4MiB/s,w=47.5MiB/s][r=12.1k,w=12.2k IOPS][eta 00m:50s]
Jobs: 2 (f=2): [m(2),X(1)][21.3%][r=43.3MiB/s,w=43.6MiB/s][r=11.1k,w=11.2k IOPS][eta 00m:48s]
Jobs: 2 (f=2): [m(2),X(1)][23.0%][r=43.4MiB/s,w=43.7MiB/s][r=11.1k,w=11.2k IOPS][eta 00m:47s]
Jobs: 2 (f=2): [m(2),X(1)][26.2%][r=47.7MiB/s,w=47.3MiB/s][r=12.2k,w=12.1k IOPS][eta 00m:45s]
Jobs: 2 (f=2): [m(2),X(1)][29.5%][r=46.8MiB/s,w=47.2MiB/s][r=12.0k,w=12.1k IOPS][eta 00m:43s]
Jobs: 2 (f=2): [m(2),X(1)][32.8%][r=47.6MiB/s,w=47.4MiB/s][r=12.2k,w=12.1k IOPS][eta 00m:41s]
Jobs: 2 (f=2): [m(2),X(1)][36.1%][r=46.5MiB/s,w=47.1MiB/s][r=11.9k,w=12.1k IOPS][eta 00m:39s]
Jobs: 2 (f=2): [m(2),X(1)][40.0%][r=50.2MiB/s,w=49.8MiB/s][r=12.9k,w=12.7k IOPS][eta 00m:36s]
Jobs: 2 (f=2): [m(2),X(1)][41.0%][r=49.3MiB/s,w=49.1MiB/s][r=12.6k,w=12.6k IOPS][eta 00m:36s]
Jobs: 2 (f=2): [m(2),X(1)][44.3%][r=47.6MiB/s,w=47.6MiB/s][r=12.2k,w=12.2k IOPS][eta 00m:34s]
Jobs: 2 (f=2): [m(2),X(1)][47.5%][r=49.8MiB/s,w=49.7MiB/s][r=12.8k,w=12.7k IOPS][eta 00m:32s]
Jobs: 2 (f=2): [m(2),X(1)][49.2%][r=49.0MiB/s,w=48.8MiB/s][r=12.6k,w=12.5k IOPS][eta 00m:31s]
Jobs: 2 (f=2): [m(2),X(1)][53.3%][r=48.3MiB/s,w=49.3MiB/s][r=12.4k,w=12.6k IOPS][eta 00m:28s]
Jobs: 2 (f=2): [m(2),X(1)][56.7%][r=48.6MiB/s,w=49.0MiB/s][r=12.4k,w=12.5k IOPS][eta 00m:26s]
Jobs: 2 (f=2): [m(2),X(1)][60.0%][r=48.0MiB/s,w=47.8MiB/s][r=12.3k,w=12.2k IOPS][eta 00m:24s]
Jobs: 2 (f=2): [m(2),X(1)][60.7%][r=48.0MiB/s,w=48.1MiB/s][r=12.3k,w=12.3k IOPS][eta 00m:24s]
Jobs: 2 (f=2): [m(2),X(1)][63.9%][r=51.0MiB/s,w=50.6MiB/s][r=13.1k,w=13.0k IOPS][eta 00m:22s]
Jobs: 2 (f=2): [m(2),X(1)][67.2%][r=49.8MiB/s,w=49.5MiB/s][r=12.7k,w=12.7k IOPS][eta 00m:20s]
Jobs: 2 (f=2): [m(2),X(1)][70.5%][r=49.0MiB/s,w=50.3MiB/s][r=12.5k,w=12.9k IOPS][eta 00m:18s]
Jobs: 2 (f=2): [m(2),X(1)][73.8%][r=48.5MiB/s,w=49.4MiB/s][r=12.4k,w=12.7k IOPS][eta 00m:16s]
Jobs: 2 (f=2): [m(2),X(1)][78.3%][r=48.2MiB/s,w=47.3MiB/s][r=12.3k,w=12.1k IOPS][eta 00m:13s]
Jobs: 2 (f=2): [m(2),X(1)][80.3%][r=50.3MiB/s,w=49.4MiB/s][r=12.9k,w=12.7k IOPS][eta 00m:12s]
Jobs: 2 (f=2): [m(2),X(1)][83.6%][r=50.2MiB/s,w=49.0MiB/s][r=12.9k,w=12.5k IOPS][eta 00m:10s]
Jobs: 2 (f=2): [m(2),X(1)][85.2%][r=47.5MiB/s,w=47.7MiB/s][r=12.2k,w=12.2k IOPS][eta 00m:09s]
Jobs: 2 (f=2): [m(2),X(1)][86.9%][r=50.1MiB/s,w=49.5MiB/s][r=12.8k,w=12.7k IOPS][eta 00m:08s]
Jobs: 2 (f=2): [m(2),X(1)][90.2%][r=48.8MiB/s,w=49.6MiB/s][r=12.5k,w=12.7k IOPS][eta 00m:06s]
Jobs: 2 (f=2): [m(2),X(1)][93.4%][r=48.4MiB/s,w=47.4MiB/s][r=12.4k,w=12.1k IOPS][eta 00m:04s]
Jobs: 2 (f=2): [m(2),X(1)][96.7%][r=47.5MiB/s,w=48.7MiB/s][r=12.2k,w=12.5k IOPS][eta 00m:02s]
Jobs: 2 (f=2): [m(2),X(1)][98.4%][r=49.8MiB/s,w=49.5MiB/s][r=12.8k,w=12.7k IOPS][eta 00m:01s]
Jobs: 2 (f=2): [m(2),X(1)][100.0%][r=48.9MiB/s,w=47.9MiB/s][r=12.5k,w=12.3k IOPS][eta 00m:00s]
iops-test-job: (groupid=0, jobs=3): err=28 (file:io_u.c:1845, func=io_u error, error=No space left on device): pid=3771: Tue Jul 30 23:06:17
2024
  read: IOPS=12.3k, BW=48.1MiB/s (50.4MB/s)(2886MiB/60002msec)
    slat (nsec): min=1679, max=61519k, avg=57980.28, stdev=147149.84
    clat (usec): min=1126, max=163039, avg=20880.35, stdev=5236.80
     lat (usec): min=1188, max=163066, avg=20938.57, stdev=5236.55
    clat percentiles (usec):
     |  1.00th=[14746],  5.00th=[15664], 10.00th=[16057], 20.00th=[16581],
```

```
     | 30.00th=[17171], 40.00th=[17957], 50.00th=[18744], 60.00th=[21627],
     | 70.00th=[23200], 80.00th=[24773], 90.00th=[27132], 95.00th=[31327],
     | 99.00th=[36963], 99.50th=[39060], 99.90th=[49021], 99.95th=[51643],
     | 99.99th=[76022]
   bw (  KiB/s): min=35632, max=53506, per=100.00%, avg=49309.31, stdev=1275.25, samples=236
   iops        : min= 8907, max=13376, avg=12326.85, stdev=318.82, samples=236
  write: IOPS=12.3k, BW=48.1MiB/s (50.5MB/s)(2888MiB/60002msec); 0 zone resets
    slat (usec): min=2, max=112744, avg=98.70, stdev=586.77
    clat (usec): min=1013, max=162272, avg=20443.88, stdev=5185.99
     lat (usec): min=1125, max=163299, avg=20542.90, stdev=5202.03
    clat percentiles (usec):
     |  1.00th=[14353],  5.00th=[15401], 10.00th=[15795], 20.00th=[16319],
     | 30.00th=[16712], 40.00th=[17433], 50.00th=[18220], 60.00th=[21103],
     | 70.00th=[22938], 80.00th=[24249], 90.00th=[26608], 95.00th=[30802],
     | 99.00th=[36439], 99.50th=[38536], 99.90th=[48497], 99.95th=[51119],
     | 99.99th=[76022]
   bw (  KiB/s): min=37137, max=53249, per=100.00%, avg=49333.05, stdev=1188.12, samples=236
   iops        : min= 9283, max=13312, avg=12332.74, stdev=297.01, samples=236
  lat (msec)   : 2=0.01%, 4=0.01%, 10=0.02%, 20=56.72%, 50=43.18%
  lat (msec)   : 100=0.07%, 250=0.01%
  cpu          : usr=2.87%, sys=16.33%, ctx=447882, majf=0, minf=56
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=738903,739381,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
   READ: bw=48.1MiB/s (50.4MB/s), 48.1MiB/s-48.1MiB/s (50.4MB/s-50.4MB/s), io=2886MiB (3027MB), run=60002-60002msec
  WRITE: bw=48.1MiB/s (50.5MB/s), 48.1MiB/s-48.1MiB/s (50.5MB/s-50.5MB/s), io=2888MiB (3028MB), run=60002-60002msec

Disk stats (read/write):
  sda: ios=738033/738664, merge=43/87, ticks=767404/135599, in_queue=903136, util=72.27%
```

Тест пропускной способности

Для тестирования пропускной способности используется одновременное чтение и запись крупными блоками с использованием множества процессов. Эти тесты измеряют значение объёма данных, который может быть передан за определённое время. Чем выше значение пропускной способности, тем больше данных может быть передано или принято за единицу времени.

bw — основной параметр вывода для теста пропускной способности, означающий совокупную пропускную способность потоков в группе, за которой следуют минимальная и максимальная пропускная способность всех потоков.

> Перед выполнением теста убедитесь, что в указанной директории достаточно свободного места (более 10 ГБ) для завершения теста.

Тест чтения/записи:

```
fio --name=fiotest --blocksize=256k --directory=/home/user --size=10G --ioengine=psync --iodepth=1 --runtime=120 --rw=randrw --direct=1 --numjobs=25 --group_reporting
```

где:

• **--name=fiotest** — имя задания, используемое для отчётов;

• **--blocksize=256k** — устанавливает размер читаемого или записываемого блока данных на 256 КБ;

• **--directory=/home/user** — задаёт каталог /home/user, в котором будут созданы тестовые файлы;

• **--size=10G** — общий объем данных, который будет использоваться для каждого задания (10 ГБ);

• **--ioengine=psync** — устанавливает синхронный механизм ввода-вывода с использованием стандартных системных вызовов (pread/pwrite);

• **--iodepth=1** — глубина очереди ввода-вывода, которая равна 1, каждая операция будет дожидаться завершения перед началом следующей;

• **--runtime=120** — устанавливает время выполнения теста в 120 секунд;

• **--rw=randrw** — режим работы с диском: данные будут читаться и записываться случайным образом;

• **--direct=1** — включает режим прямого ввода-вывода, минуя кеширование в операционной системе;

• **--numjobs=25** — количество параллельно выполняемых заданий (25 заданий);

• **--group_reporting** — включает групповой отчёт, объединяющий результаты всех заданий.

Использование файла задания

Можно получить более последовательные результаты, если использовать файл задания вместо выполнения команды напрямую.

Для этого создайте файл задания **fiorandomreadwrite.fio**:

```
nano fiorandomreadwrite.fio
```

Добавьте в файл следующие строки:

```
[global]

name=fiotest
blocksize=4k
directory=/home/user
size=5g
ioengine=libaio
iodepth=256
runtime=60
rw=randwrite
direct=1
runtime=60
rw=randwrite
direct=1
[job1]
filename=directory=/home/user
```

Для выполнения файла задания используйте команду:

```
fio ./fiorandomreadwrite.fio
```

Результат:

```
job1: (g=0): rw=randwrite, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
fio-3.28
Starting 1 process
job1: Laying out IO file (1 file / 5120MiB)
Jobs: 1 (f=1): [w(1)][100.0%][w=53.5MiB/s][w=13.7k IOPS][eta 00m:00s]
job1: (groupid=0, jobs=1): err= 0: pid=4312: Tue Jul 30 12:29:40 2024
  write: IOPS=5104, BW=19.9MiB/s (20.9MB/s)(1197MiB/60001msec); 0 zone resets
    slat (usec): min=4, max=6968.9k, avg=192.75, stdev=21138.71
    clat (nsec): min=884, max=8563.0M, avg=49933698.53, stdev=420390411.52
     lat (usec): min=89, max=8563.0k, avg=50126.78, stdev=421252.44
    clat percentiles (msec):
     |  1.00th=[   11],  5.00th=[   12], 10.00th=[   12], 20.00th=[   13],
     | 30.00th=[   13], 40.00th=[   14], 50.00th=[   14], 60.00th=[   14],
     | 70.00th=[   14], 80.00th=[   18], 90.00th=[   25], 95.00th=[   43],
     | 99.00th=[  342], 99.50th=[ 2039], 99.90th=[ 7282], 99.95th=[ 8423],
     | 99.99th=[ 8423]
   bw (  KiB/s): min=    8, max=74003, per=100.00%, avg=38357.61, stdev=26329.13, samples=61
   iops        : min=    2, max=18500, avg=9589.21, stdev=6582.25, samples=61
  lat (nsec)   : 1000=0.01%
  lat (usec)   : 50=0.01%, 100=0.01%, 250=0.01%, 500=0.01%, 750=0.01%
  lat (usec)   : 1000=0.01%
  lat (msec)   : 2=0.01%, 4=0.04%, 10=0.45%, 20=82.69%, 50=12.38%
  lat (msec)   : 100=2.49%, 250=0.46%, 500=0.70%, 750=0.09%, 1000=0.01%
  lat (msec)   : 2000=0.16%, >=2000=0.50%
  cpu          : usr=1.00%, sys=15.06%, ctx=334602, majf=0, minf=16
```

```
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=0,306304,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
  WRITE: bw=19.9MiB/s (20.9MB/s), 19.9MiB/s-19.9MiB/s (20.9MB/s-20.9MB/s), io=1197MiB (1255MB), run=60001-60001msec
Disk stats (read/write):
  sda: ios=4/304465, merge=0/6666, ticks=446/976801, in_queue=983934, util=84.55%
```

Тест с разными значениями iodepth

> Перед выполнением теста убедитесь, что в указанной директории достаточно свободного места (более 5 ГБ) для завершения теста.

Основная цель данного теста — измерить производительность дисковой подсистемы при различных значениях iodepth.

Значение iodepth определяет, сколько операций ввода-вывода может быть выполнено одновременно. Чем **выше значение** iodepth, тем **выше нагрузка** на систему, и тест позволяет увидеть, как это влияет на скорость чтения/записи.

Тест можно использовать для:

- оценки производительности устройства хранения;
- выявления пределов производительности для различных сценариев загрузки;
- сравнения различных устройств хранения;
- оптимизации конфигураций серверов/приложений, особенно при высокой нагрузке.

Скрипт для тестирования диска с разными значениями iodepth (разным количеством одновременных запросов):

Создайте файл **run_fio_tests.sh**:

```
nano run_fio_tests.sh
```

Добавьте в файл следующие строки:

```
#!/bin/bash
for i in 1 2 4 8 16 32 64 128 256 512 1024; do
   echo "Testing with iodepth=$i"
   fio --name=fiotest --ioengine=libaio --direct=1 --rw=randread --bs=4k --size=5G --randrepeat=0 --norandommap --fsync=1 --numjobs=1 --runtime=60 --group_reporting --directory=/base/fio_test --iodepth=$i
   echo ""
done
```

где:

- **--name=fiotest** — название теста;
- **--ioengine=libaio** — задаёт используемый механизм ввода-вывода. libaio — асинхронный механизм ввода-вывода, который позволяет программе выполнять ввод-вывод в неблокирующем режиме;
- **--direct=1** — ввод-вывод будет осуществляться непосредственно на устройство, минуя кеш операционной системы;
- **--rw=randread** — тип операции ввода-вывода (read/write). randread означает, что будут выполняться случайные операции чтения;
- **--bs=4k** — размер блока ввода-вывода 4 КБ;
- **--size=5G** — определяет общий размер файла — 5 ГБ, который будет использоваться в тестировании;
- **--randrepeat=0** — указывает, что не нужно повторять одно и то же случайное последовательности ввода-вывода;
- **--norandommap** — отключает создание карты случайных блоков;
- **--fsync=1** — после каждой записи необходимо синхронизировать данные с устройством хранения;
- **--numjobs=1** — определяет количество параллельных задач, которые будут запущены. В примере 1 задача;

- **--runtime=60** — определяет продолжительность теста в секундах. Тест будет выполняться 60 секунд;
- **--group_reporting** — результаты должны быть собраны и отображены глобально;
- **--directory=/home/user** — определяет директорию, где будет осуществляться тестирование;
- **--iodepth=$i** — глубина очереди ввода-вывода, которая будет варьироваться от 1 до 1024 в зависимости от текущего значения $i в цикле.

Сделайте файл исполняемым:

```
chmod +x run_fio_tests.sh
```

Запустите скрипт:

```
./run_fio_tests.sh
```

Удаление результатов тестирования

Удалить файлы после тестирования можно с помощью следующей команды:

```
rm /home/user/fiotest*
```

где:

- **/home/user/fiotest*** — путь и шаблон имён файлов, которые нужно удалить.

Перед удалением можно проверить, что удаляются только нужные файлы:

```
ls /home/user/fiotest*
```

Примерный вывод:

```
/home/user/fiotest.0.0 /home/user/fiotest.1.0
```

Анализ производительности блочных устройств (blktrace) и построение графиков на основе собранных данных (iowatcher)

Установка
Возможности blktrace
Возможности iowatcher
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: blktrace-1.0.5-10, iowatcher-1.0-8

blktrace – это инструмент для трассировки событий блочного ввода/вывода, который использует трассировщик **blktrace** в ядре. Это низкоуровневый инструмент, отображающий множество событий для каждой операции ввода/вывода. **blktrace** используется в качестве вспомогательного инструмента в программных решениях, предназначенных для анализа и диагностики проблем производительности в системах хранения данных.

iowatcher – утилита, позволяющая анализировать данные, подготовленные с помощью **blktrace** и строить на основе этих данных графики (в том числе и анимированные). Т.е. инструмент **blktrace** позволяет записывать события в файлы трассировки для последующей визуализации с помощью утилиты **iowatcher**. Поэтому работу **iowatcher** не стоит рассматривать отдельно от **blktrace**.

С помощью **iowatcher** также можно запускать **blktrace** с последующим созданием графика трассировки одной командой.

Установка

Для установки утилит перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install blktrace iowatcher
```

Возможности blktrace

blktrace запускает трассировку драйвера блочного устройства в ядре и возвращает данные трассировки, которые можно обработать помимо **iowatcher** с помощью **blkparse**. Для удобства был также создан инструмент **btrace**, который запускает **blktrace** и **blkparse**, т.е. следующие команды дадут один и тот же вывод:

```
blktrace -d /dev/sda -o - | blkparse -i -
```

```
btrace /dev/sda
```

Ниже приведен пример трассировки события «*запись в файл на примере команды* `echo 1 > test.txt`».

```
btrace /dev/sdb

  8,16   5        1     0.000000000 193450 A RM  973080688 + 8 <- (8,17) 973078640
  8,16   5        2     0.000000744 193450  Q RM  973080688 + 8 [bash]
  8,16   5        3     0.000003993 193450 G RM  973080688 + 8 [bash]
  8,16   5        4     0.000004498 193450  P  N  [bash]
  8,16   5        5     0.000005205 193450  UT N  [bash] 1
  8,16   5        6     0.000005495 193450 I  RM  973080688 + 8 [bash]
  8,16   5        7     0.000014361   266 D RM  973080688 + 8 [kworker/5:1H]
  8,16   3        1     0.001309172     0  C  RM  973080688 + 8 [0]
  8,16   5        8     0.001354482 193450 A  W  976766976 + 8 <- (8,17) 976764928
  8,16   5        9     0.001354754 193450  Q  W  976766976 + 8 [bash]
  8,16   5       10     0.001356122 193450  G W  976766976 + 8 [bash]
  8,16   5       11     0.001356303 193450 P  N  [bash]
  8,16   5       12     0.001357581 193450 D  W  976766976 + 8 [bash]
```

```
 8,16  3      2    0.001417097    0   C  W  976766976 + 8 [0]
```

В выводе представлено несколько строк – по одной на каждое действие (событие), связанное с очередью блочного устройства или с самим устройством.

По умолчанию выводится семь столбцов:

1. Старший и младший номер устройства.

2. Идентификатор процессора.

3. Порядковый номер.

4. Время события в секундах от начала трассировки.

5. Идентификатор процесса.

6. Идентификатор действия: тип события.

7. Описание **RWBS**: флаги ввода/вывода.

Далее приведено описание идентификаторов из страницы справочного руководства для **blkparse**. Этот список показывает, какие события может наблюдать фреймворк **blktrace**:

- **A** – ввод/вывод был отображен на другое устройство;
- **B** – дополнительный ввод/вывод;
- **C** – ввод/вывод завершен;
- **D** – запрос передан драйверу;
- **F** – запрос добавлен в начало другого запроса, находившегося в очереди;
- **G** – выделение памяти для запроса;
- **I** – запрос добавлен в очередь планировщика ввода/вывода;
- **M** – запрос добавлен в конец другого запроса, находившегося в очереди;
- **P** – блокировка очереди для накопления нескольких запросов;
- **Q** – ввод/вывод передан коду, который управляет очередью;
- **S** – ожидание освобождения структуры для размещения запроса;
- **T** – разблокировка очереди по тайм-ауту;
- **U** – разблокировка очереди;
- **X** – запрос разделен.

Для нужд мониторинга ядро позволяет описать тип каждой операции ввода/вывода с помощью строки символов — rwbs. Она применяется в **blktrace** и в других инструментах трассировки, определена в функции ядра **blk_fill_rwbs()** и использует следующие символы:

- **R**: чтение (*read*);
- **W**: запись (*write*);
- **M**: метаданные (*metadata*);
- **S**: синхронная (*synchronous*);
- **A**: опережающее чтение (*read-ahead*);
- **F**: выталкивание на диск или принудительное обращение к блоку (*flush or force*);
- **D**: отмена (*discard*);
- **E**: стирание (*erase*);
- **N**: нет операции (none).

Символы могут комбинироваться. Например, «***WM***» означает «***запись метаданных***».

Возможности iowatcher

Наиболее часто используемые параметры запуска:

- **-d** – определяет, какое устройство отслеживать, параметр перенаправляется в **blktrace** для создания новой трассировки;
- **-p** – инициирует запуск другой программы во время снятия трассировки. Программа и аргументы ее запуска должны быть указаны после всех остальных параметров утилиты **iowatcher**;
- **-K** – сохраняет файлы **SVG** для создания анимированного графика;
- **-t** – определяет расположение и имя файла, в котором хранятся трассировки **blktrace**. Можно указывать только каталог с набором трассировок;
- **-l** – добавляет метки на графике;
- **-m** – создает анимированный график;
- **-T** – задает заголовок, который будет размещен в верхней части графика;
- **-o** – определяет расположение и имя файла для SVG или видео;
- **-h** – задает высоту графика;
- **-w** – задает ширину графика;
- **-c** – количество столбцов в графике;
- **-x** – ограничивает диапазон обрабатываемого времени;
- **-P** – различать процессы в графике ввода/вывода;
- **-O** – позволяет генерировать только необходимые графики (по умолчанию генерируются все);
- **-N** – противоположность параметра **-O**, определяет тот график, который нужно пропустить.

Варианты графиков – *io*, *tput*, *latency*, *queue_depth*, *iops*, *cpu-sys*, *cpu-io*, *cpu-irq*, *cpu-user*, *cpu-soft*.

Примеры использования

Для того чтобы снять показания с блочного устройства (диска) за определенный интервал времени, необходимо выполнить команду:

```
blktrace -w 600 -d /dev/sda1 -o- > trace.dump
```

где:

- `w 300` – интервал времени в секундах, в течение которого будут сниматься показания;
- `d /dev/sda` – устройство, с которого будет сниматься статистика ввода-вывода;
- `-o-` – вывод статистики в консоль;
- `trace.dump` – перенаправление из консоли в файл **trace.dump**.

Для создания графика используется утилита **iowatcher**.

```
iowatcher -t trace.dump -o trace.svg
```

Файл **trace.svg** можно открыть в браузере или любом другом графическом редакторе.

Дополнительные типовые примеры использования:

- Создать график из существующего файла трассировки:

```
iowatcher -t trace
```

- Пропустить график ввода/вывода в создаваемом файле **trace.svg**:

```
iowatcher -t trace.dump -o trace.svg -N io
```

- Сгенерировать график только с показаниями **latency** (задержка):

```
iowatcher -t trace.dump -o trace.svg -O latency
```

- Запустить тест **fio** и снять трассировку этого процесса через **blktrace** на устройстве **/dev/sda**, при этом **fio** будет запущен с

параметрами, которые указаны в `-p fio some_job_file`:

```
iowatcher -d /dev/sda -t trace.dump -T 'Fio Benchmark' -p 'fio some_job_file'
```

- Снять трассировку с диска **/dev/sdb** и сразу создать график:

```
iowatcher -d /dev/sdb -t trace -o trace.svg
```

- Анимированный график можно получить при помощи команды:

```
iowatcher -t trace.dump --movie -o trace.mp4
```

Настройка сервера на postgresql 13 и zabbix 6.2

Предварительная подготовка сервера
Настройка сервера на PostgreSQL 13
Установка и настройка zabbix 6
Настройка базы данных
Запуск процесса zabbix-сервера
Настройка из веб-интерфейса

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** postgresql-13.8-1, zabbix-6.2.1

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. **Zabbix** использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления практически для любого события и быстро реагировать на проблемы с серверами. **Zabbix** предлагает отличные функции отчетности и визуализации данных, основанные на данных истории. Это делает **zabbix** идеальным для планирования мощности и мониторинга состояния серверов.

Zabbix разделяется на два вида: **zabbix-agent** и **zabbix-server**.

Zabbix-server собирает данные со всех клиентов, обрабатывает их, выводя на экран в веб-интерфейсе, и рассылает уведомления.

Zabbix-agent установлен на серверах, с которых необходимо собирать информацию об их состоянии, таких агентов может быть множество.

Примечание.

Для **zabbix 6** требуется **postgresql 13 и выше**. В инструкции будет рассмотрен пример настройки сервера на **postgresql 13**.

Предварительная подготовка сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

1. Настройте политики безопасности с помощью команд:

```
setsebool -P httpd_can_network_connect on
setsebool -P httpd_can_network_connect_db on
```

2. Обновите систему.

```
dnf update
```

3. Установите следующие пакеты и добавьте пакет **httpd** в автозагрузку.

```
dnf install httpd zabbix-apache-conf zabbix-sql-scripts
systemctl enable httpd
```

Настройка сервера на PostgreSQL 13

1. Установите сервер баз данных **postgresql** и добавьте его в автозагрузку:

```
dnf install postgresql13 postgresql13-server
systemctl enable postgresql-13
```

2. Выполните инициализацию нового сервера баз данных **postgresql**:

```
/usr/bin/postgresql-13-setup initdb
```

3. Запустите **postgres**:

```
systemctl start postgresql-13
```

Установка и настройка zabbix 6

Установите **zabbix**:

```
dnf install zabbix-server-pgsql zabbix-web-pgsql zabbix-agent
```

Далее необходимо отредактировать файл **php.ini**:

```
nano /etc/php.ini
```

Приведите параметры к следующему виду:

```
date.timezone = Europe/Moscow      #обязательно укажите свой часовой пояс
post_max_size = 16M
max_execution_time = 300
max_input_time = 300
```

и сохраните изменения.

Настройка базы данных PostgreSQL

Сначала нужно создать пользователя и базу данных, для этого необходимо выполнить команду:

```
su postgres
```

и подключиться к серверу базы данных:

```
psql
```

Затем создайте пользователя и базу данных с именем **zabbix** и предоставьте пользователю права на использование данной БД (пароль укажите свой):

```
CREATE ROLE zabbix WITH NOSUPERUSER LOGIN PASSWORD 'zabbixpassword';
CREATE   DATABASE zabbix WITH OWNER zabbix;
GRANT ALL PRIVILEGES ON DATABASE zabbix TO zabbix;
```

Будет создан пользователь с именем **zabbix**, паролем **zabbixpassword** и база данных с именем **zabbix**.

При выполнении команд получится следующее:

```
postgres=# CREATE ROLE zabbix WITH NOSUPERUSER LOGIN PASSWORD 'zabbixpassword';
CREATE ROLE
postgres=# CREATE   DATABASE zabbix WITH OWNER zabbix;
CREATE   DATABASE
postgres=# GRANT ALL PRIVILEGES ON DATABASE zabbix TO zabbix;
GRANT
```

Проверьте, что таблицы создались:

```
\l
```

Отключитесь от базы:

```
\q
```

Завершите сессию пользователя **postgres**:

```
exit
```

Затем необходимо перенастроить сам сервер **postgresql**:

```
nano /var/lib/pgsql/13/data/postgresql.conf
```

Найдите строку:

```
listen_addresses = 'localhost'
```

и приведите ее к виду:

```
listen_addresses = '*'
```

Затем раскомментируйте строку:

```
#port = 5432
```

и сохраните изменения.

После этого необходимо предоставить права доступа пользователю **zabbix** к базе данных по паролю, для этого требуется отредактировать другой файл:

```
nano /var/lib/pgsql/13/data/pg_hba.conf
```

найдите строку:

```
host    replication     all             127.0.0.1/32            scram-sha-256
```

и перед ней добавьте запись, чтобы выглядело следующим образом:

```
host    zabbix  zabbix        127.0.0.1/32        password
host    replication     all             127.0.0.1/32            scram-sha-256
```

Далее замените все **scram-sha-256** на **md5**, конечный вариант файла:

```
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host zabbix         zabbix        127.0.0.1/32        password
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```

Перезапустите сервер **postgresql**:

```
systemctl restart postgresql-13
```

Импортируйте содержимое SQL-дампа в базу данных:

```
zcat /usr/share/zabbix-sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix
```

Сменить пароль **psql** можно так:

```
passwd postgres
```

На этом настройка базы данных закончена, осталось настроить **zabbix**-сервер.

Отредактируйте файл конфигурации сервера **zabbix**. Пропишите данные для подключения к базе данных:

```
nano /etc/zabbix/zabbix_server.conf
```

Измените строки (их нужно раскомментировать, если они закоментированы, и присвоить нужные значения, если их нет или они отличаются):

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbixpassword
```

Запуск процесса zabbix-сервера

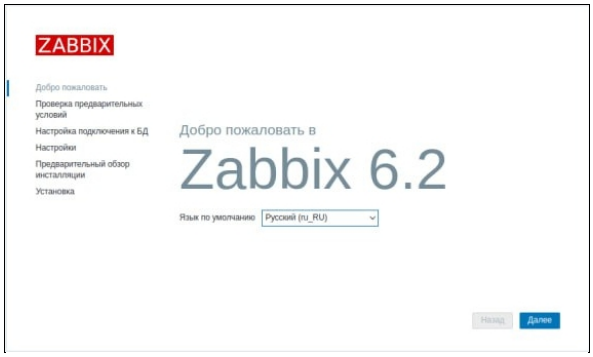
Запустите **zabbix**-сервер и добавьте его в автозагрузку:

```
systemctl restart zabbix-server
systemctl enable zabbix-server
systemctl restart zabbix-agent
systemctl enable zabbix-agent
systemctl restart httpd
```

Настройка из веб-интерфейса

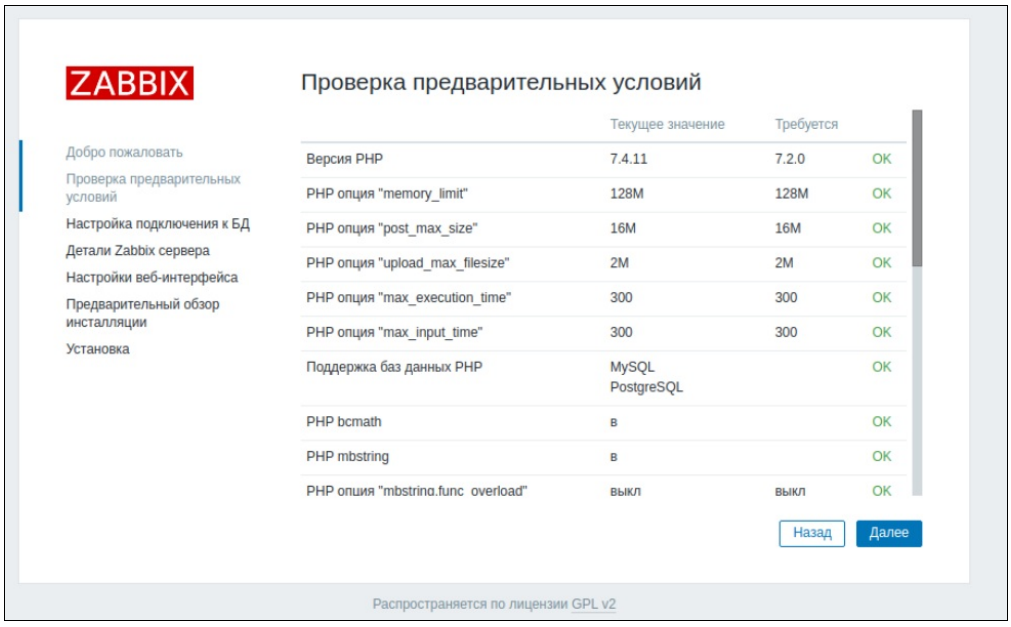
- Для того чтобы войти в веб-интерфейс, укажите в адресной строке браузера **http://<ip-адрес_сервера>/zabbix**.

Откроется страница приветствия.



Выберете язык и нажмите «**Далее**»

- Затем вы попадете на страницу преднастроек. Если вы ранее указали временную зону, то во всех пунктах должно быть « **OK**».



Нажмите «**Далее**».

- Укажите данные для подключения к ранее созданной базе данных.

В поле:

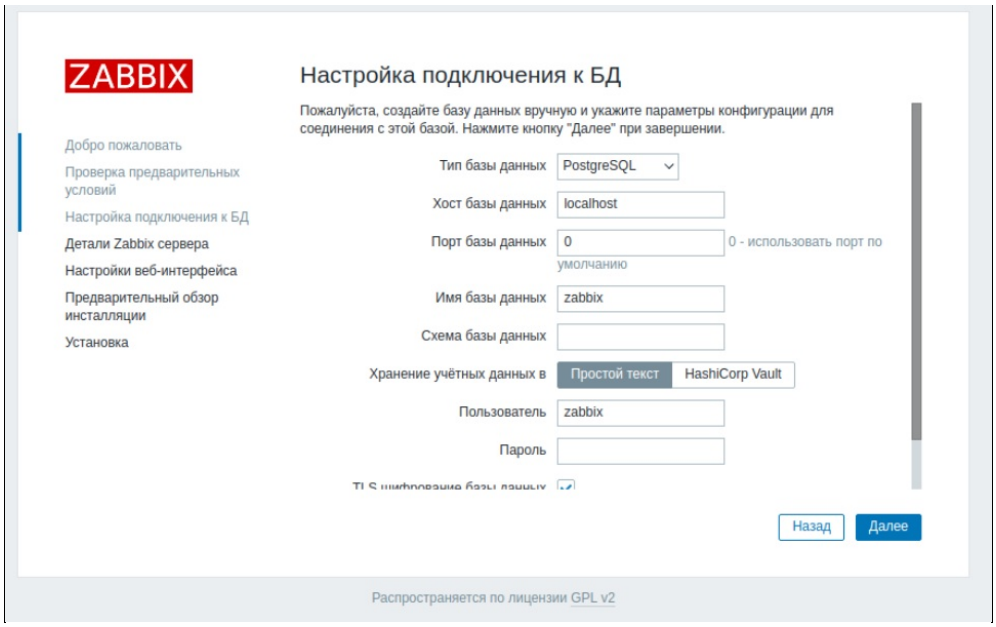
Database host — укажите адрес сервера **127.0.0.1**;

Database port — стандартный порт postgres **5432**;

Database name — имя базы данных **zabbix**;

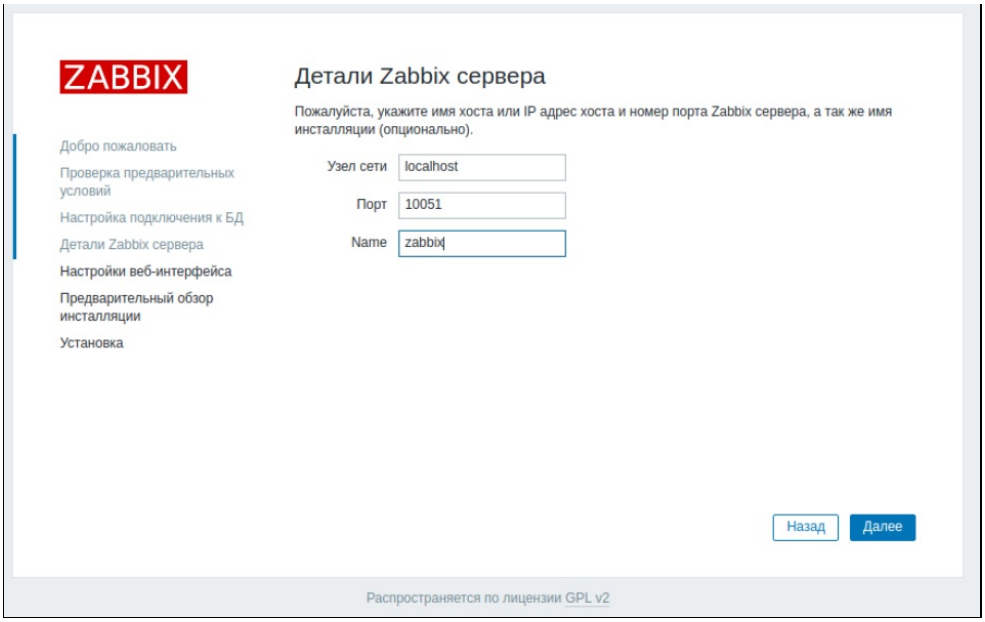
User — логин пользователя **zabbix**;

Password — пароль пользователя **zabbixpassword**.



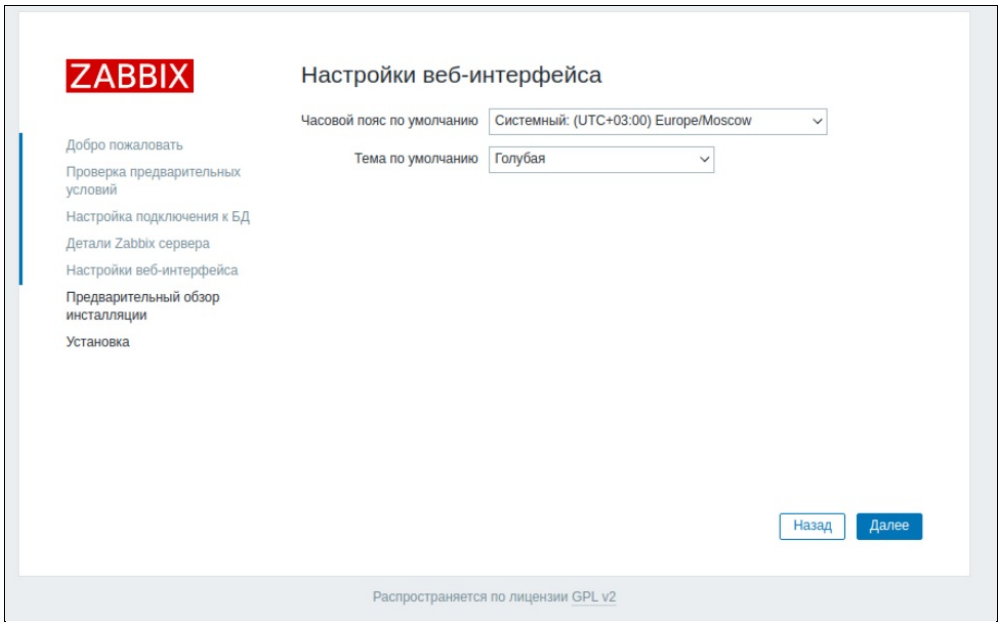
Нажмите «**Далее**». При неправильно указанных данных или неправильной конфигурации базы данных появится сообщение об ошибке подключения к базе.

- В следующем окне нужно ввести IP-адрес хоста сервера **zabbix** и номер порта для его работы. Можно оставить значения по умолчанию.

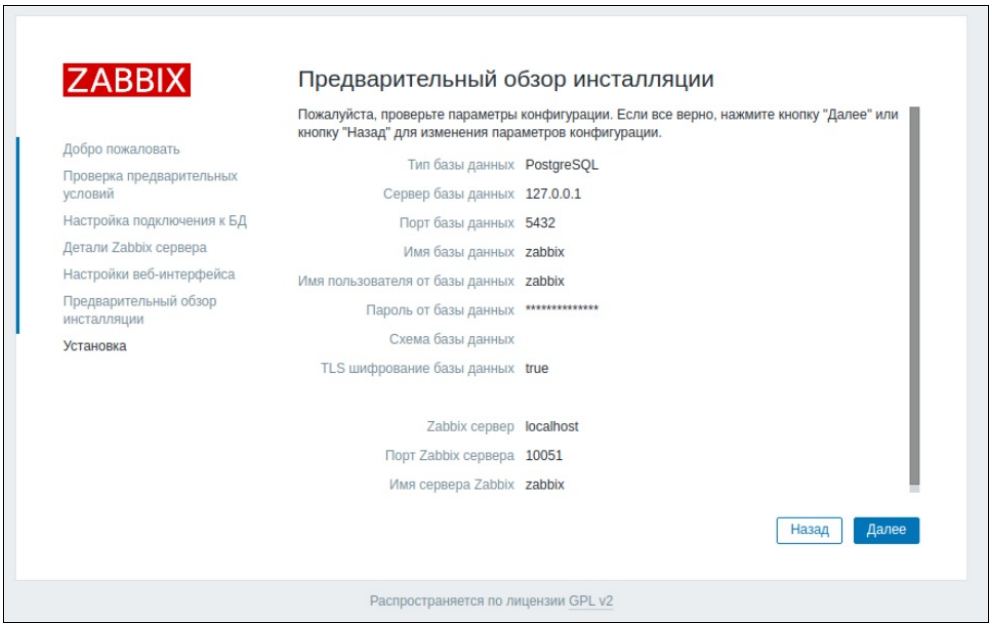


Нажмите «**Далее**».

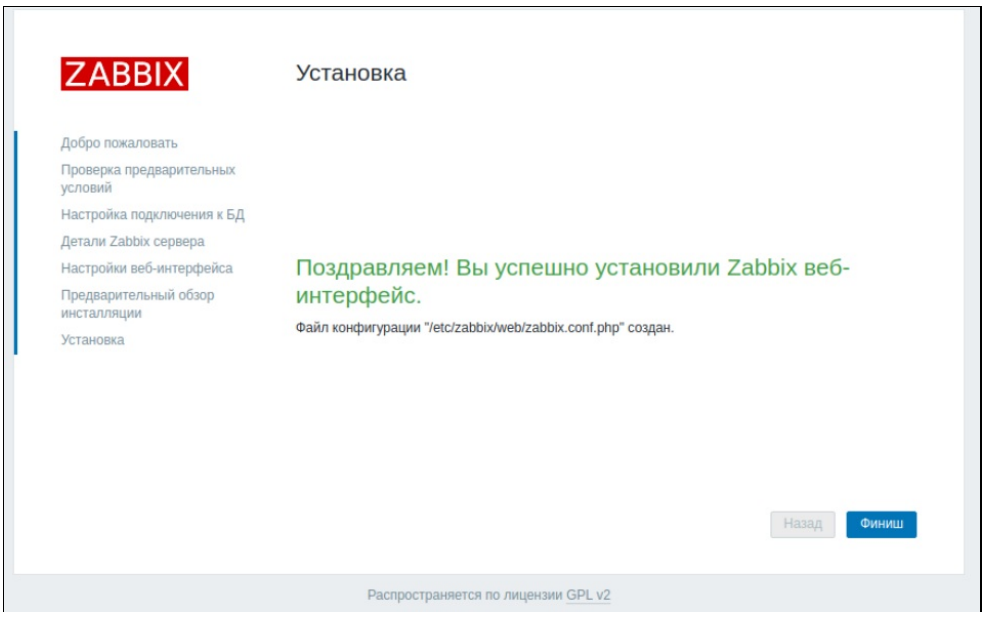
- Проверьте часовой пояс и нажмите «**Далее**».



- Проверьте правильность введенных данных и нажмите «**Далее**».

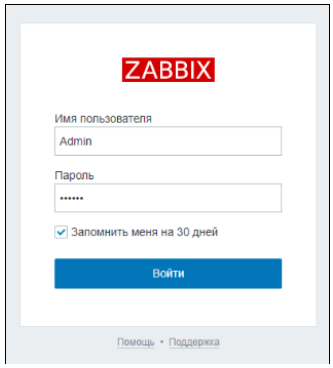


- При успешном окончании установки вы увидите следующую страницу.



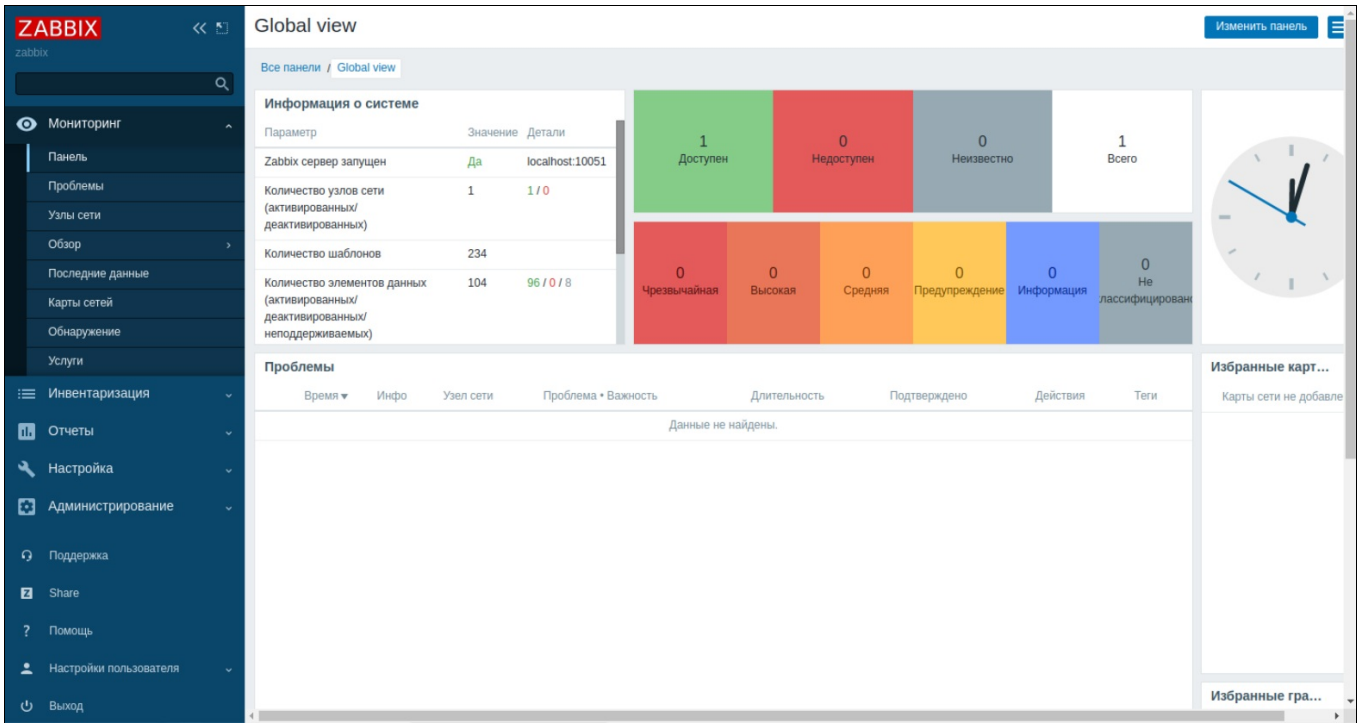
Нажмите «**Финиш**».

- Введите логин и пароль сервера **zabbix**. По умолчанию имя пользователя - **Admin** (регистр важен), пароль - **zabbix**.



Нажмите «**Войти**».

Вы попадете в панель управления. На этом настройка **zabbix** на **PSQL** завершена.



Настройка сервера на mysql и zabbix 6.2

Предварительная подготовка сервера
Настройка сервера на MYSQL
Настройка базы данных
Запуск процесса zabbix-сервера
Настройка из веб-интерфейса

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** mariadb-3:10.11.4-3, zabbix-6.2.1

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. **Zabbix** использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления практически для любого события и быстро реагировать на проблемы с серверами. **Zabbix** предлагает отличные функции отчетности и визуализации данных, основанные на данных истории. Это делает **zabbix** идеальным для планирования мощности и мониторинга состояния серверов.

Zabbix разделяется на два вида: **zabbix-agent** и **zabbix-server**.

Zabbix-server собирает данные со всех клиентов, обрабатывает их, выводя на экран в веб-интерфейсе, и рассылает уведомления.

Zabbix-agent установлен на серверах, с которых необходимо собирать информацию об их состоянии, таких агентов может быть множество.

Предварительная подготовка сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

1. Настройте политики безопасности с помощью команд:

```
setsebool -P httpd_can_network_connect on
setsebool -P httpd_can_network_connect_db on
```

2. Обновите систему.

```
dnf update
```

3. Установите следующие пакеты и добавьте пакет **httpd** в автозагрузку.

```
dnf install httpd zabbix-apache-conf zabbix-sql-scripts
systemctl enable httpd
```

Настройка сервера на MYSQL

1.Установите пакет для работы базами данных и включите его в автозагрузку:

```
dnf install mariadb mariadb-server zabbix-server-mysql zabbix-agent
systemctl start mariadb
systemctl enable mariadb.service
mysql_secure_installation
```

Настройка базы данных MYSQL

1. Создайте пользователя и базу данных для мониторинга:

```
mysql -uroot -pmasterkey
> create   database zabbix character set utf8 collate utf8_bin;
> grant all privileges on zabbix.* to zabbix@localhost identified by 'zabpassword';
> quit;
```

Создается база данных в **/var/lib/mysql/zabbix**, где:

- **masterkey** - пароль пользователя **root mysql**, это не системный **root**;
- **zabpassword** -пароль пользователя **zabbix**, у которого полный доступ к базе **mysql zabbix**.

2. Импортируйте схему базы данных и начальные данные.

Импортируйте содержимое SQL-дампа в базу данных следующим образом:

```
zcat /usr/share/zabbix-sql-scripts/mysql/create.sql.gz | mysql -uzabbix -pzabpassword zabbix
```

Для **zabbix 6**:

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -pzabpassword zabbix
```

3. После этого отредактируйте файл конфигурации сервера **zabbix**. Пропишите данные для подключения к базе данных:

```
nano /etc/zabbix/zabbix_server.conf
```

Измените строки (их нужно раскоментировать, если они закоментированы, и присвоить нужные значения, если их нет или они отличаются):

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabpassword
```

4. Также необходимо отредактировать файл:

```
nano /etc/php.ini
```

Приведите параметры к следующему виду (аналогичные параметры есть в **/etc/httpd/conf.d/zabbix.conf** - они должны соответствовать):

```
date.timezone = Europe/Moscow      # обязательно укажите свой часовой пояс!
post_max_size = 16M
max_execution_time = 300
max_input_time = 300
```

5. Запустите **zabbix** и **httpd**:

```
systemctl restart httpd
systemctl restart zabbix-server
```

Произведите проверку логов на предмет ошибок:

```
cat /var/log/zabbix/zabbix_server.log
```

Запуск процесса zabbix-сервера

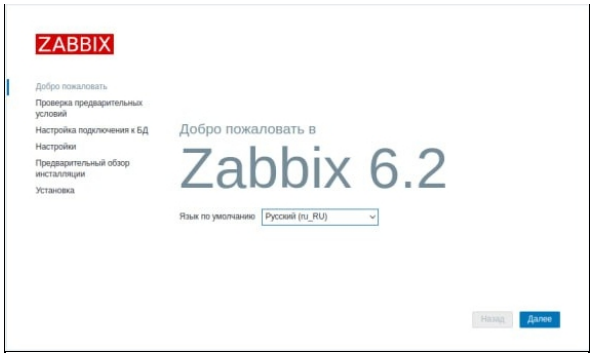
Запустите **zabbix**-сервер и добавьте его в автозагрузку:

```
systemctl restart zabbix-server
systemctl enable zabbix-server
systemctl restart zabbix-agent
systemctl enable zabbix-agent
systemctl restart httpd
```

Настройка из веб-интерфейса

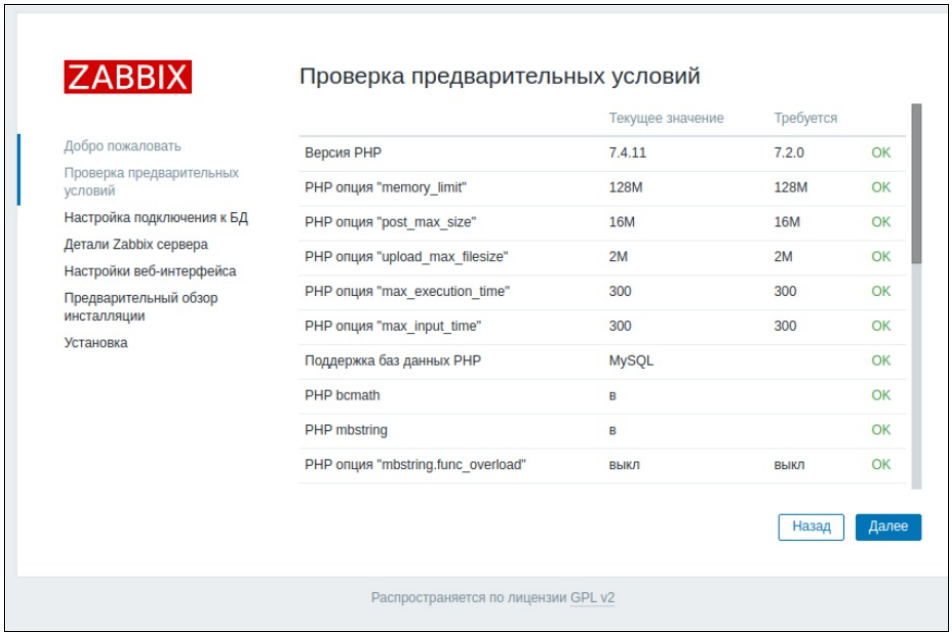
- Для того чтобы войти в веб-интерфейс, укажите в адресной строке браузера **http://<ip-адрес_сервера>/zabbix**.

Откроется страница приветствия.



Выберете язык и нажмите «**Далее**».

- Далее вы попадете на страницу преднастроек. Если вы ранее указали временную зону, то во всех пунктах должно быть « **OK**».



Нажмите «**Далее**».

- Укажите данные для подключения к ранее созданной базе данных.

В поле:

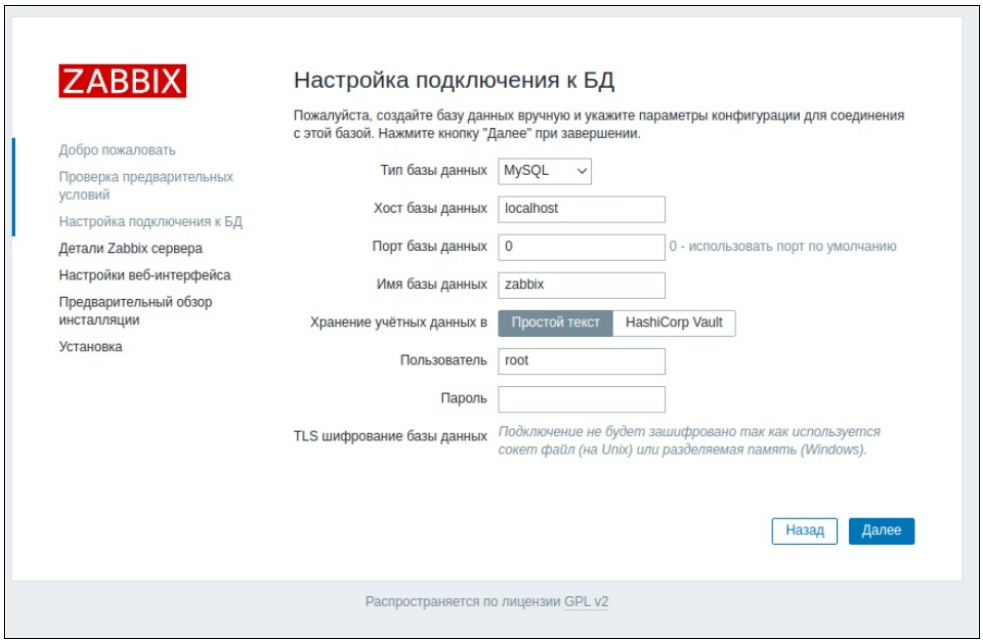
Database host — укажите адрес сервера **127.0.0.1**;

Database port — стандартный порт **MYSQL** (**3306**);

Database name — имя базы данных **zabbix**;

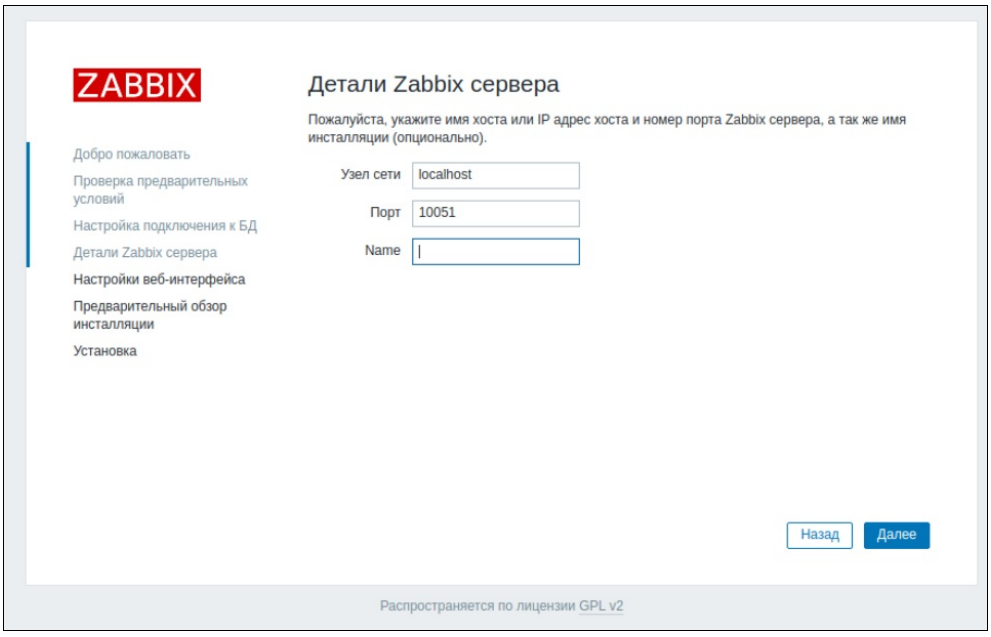
User — логин пользователя **zabbix**;

Password — пароль пользователя **zabpassword**.



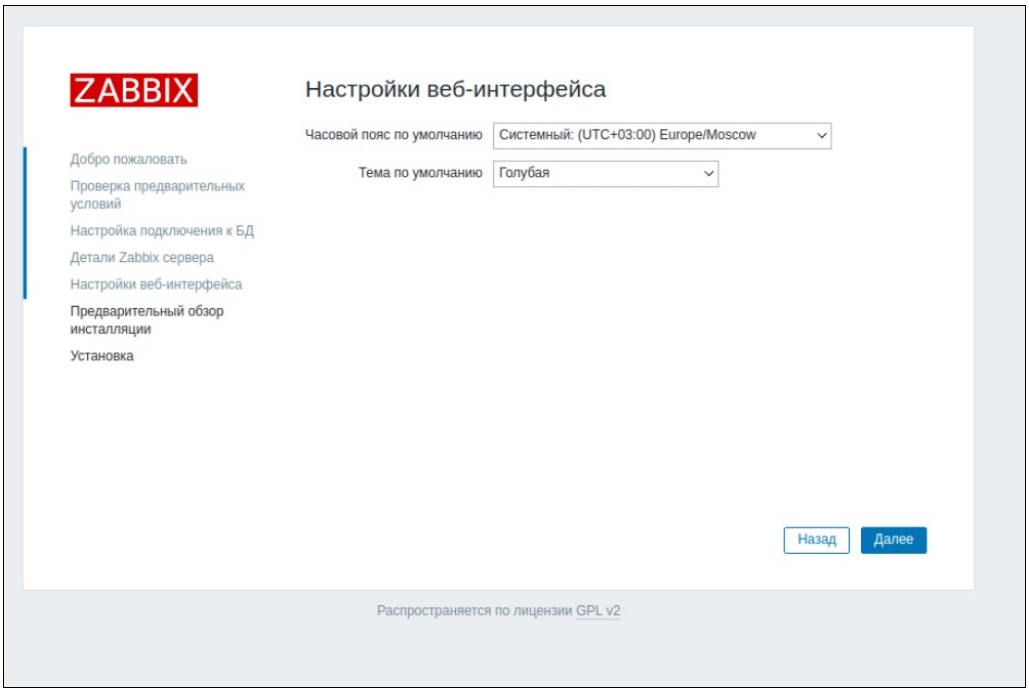
Нажмите «**Далее**». При неправильно указанных данных или неправильной конфигурации базы данных появится сообщение об ошибке подключения к базе.

- В следующем окне нужно ввести IP-адрес хоста сервера **zabbix** и номер порта для его работы. Можно оставить значения по умолчанию.

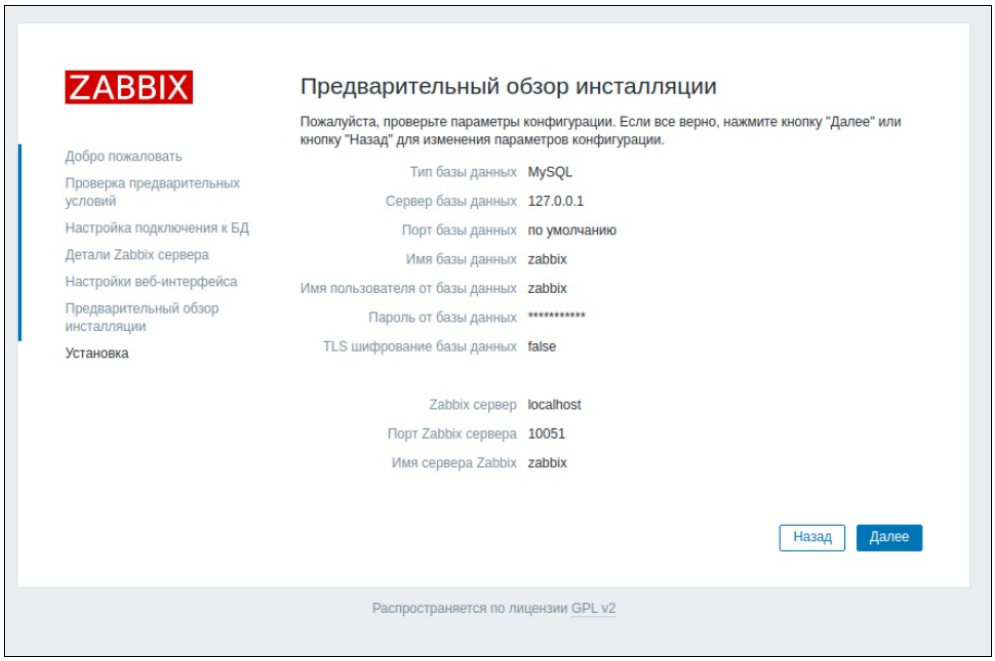


Нажмите «**Далее**».

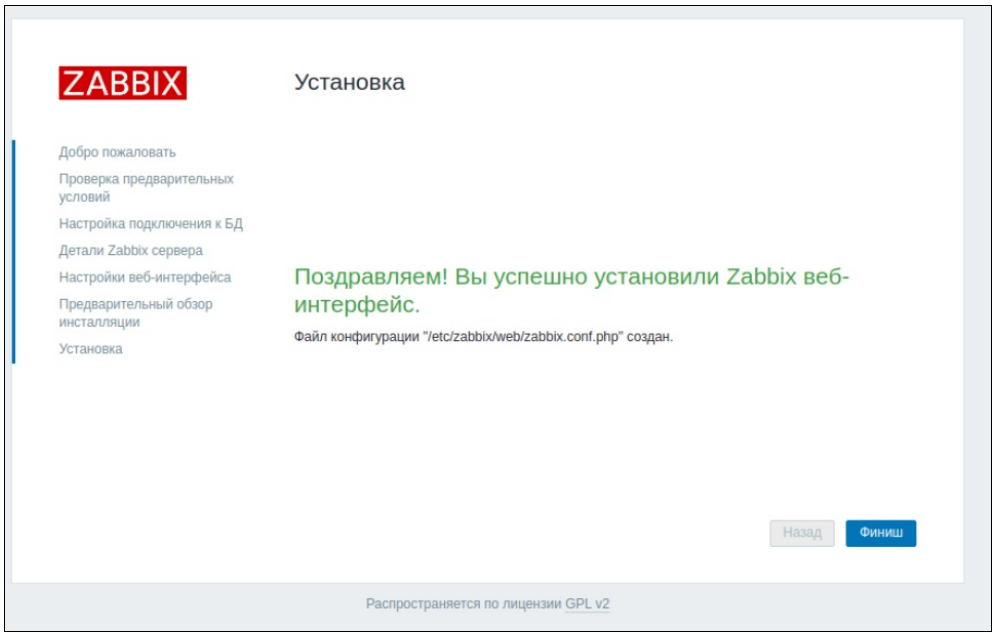
- Проверьте часовой пояс и нажмите «**Далее**».



- Проверьте правильность введенных данных и нажмите «**Далее**».

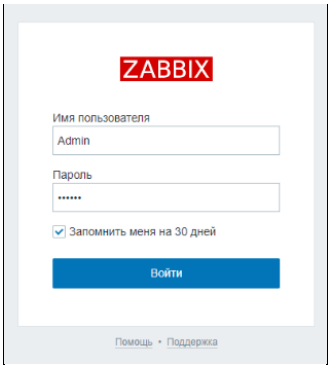


- При успешном окончании установки вы увидите следующую страницу.



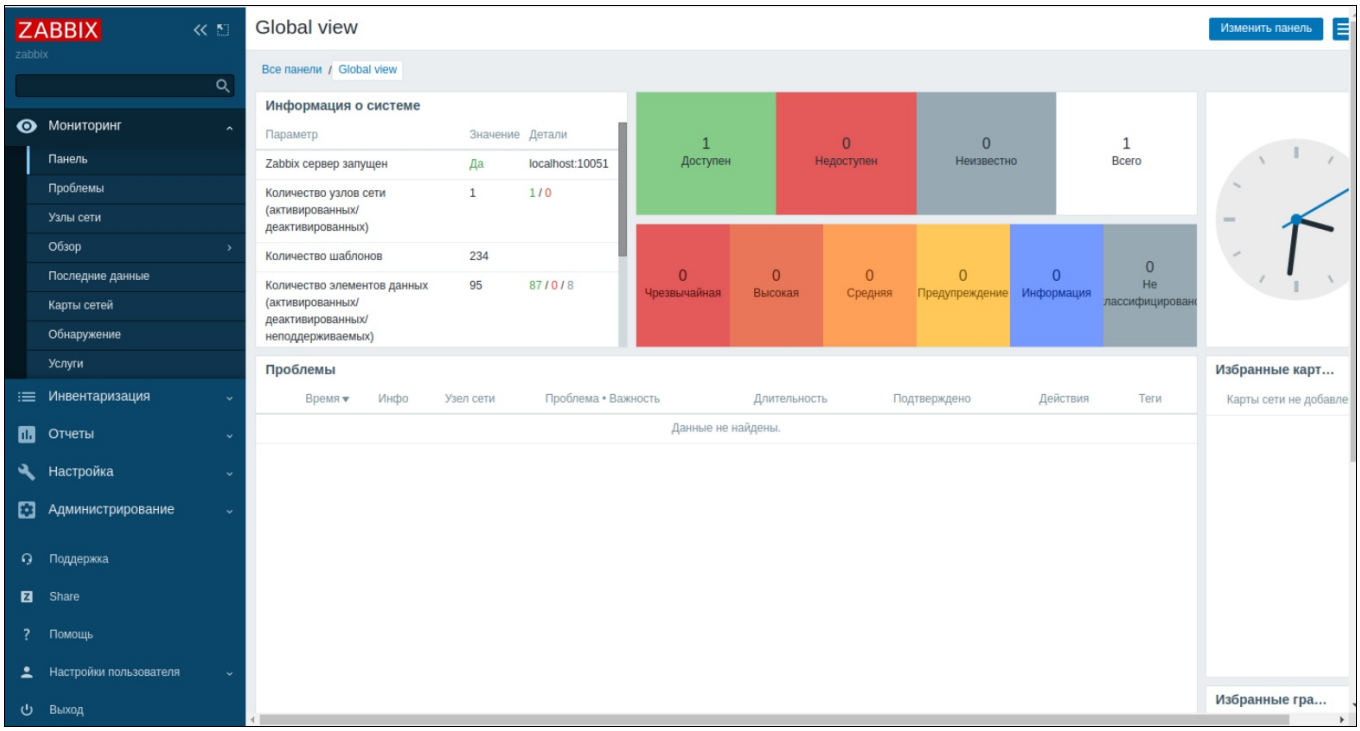
Нажмите «**Финиш**».

- Введите логин и пароль сервера **zabbix**. По умолчанию имя пользователя - **Admin** (регистр важен), пароль - **zabbix**.



Нажмите «**Войти**».

Вы попадете в панель управления. На этом настройка zabbix на MYSQL завершена.



Настройка агента zabbix

Настройка zabbix-agent
Добавление zabbix-agent

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** zabbix-6.2.1

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. **Zabbix** использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления практически для любого события и быстро реагировать на проблемы с серверами. **Zabbix** предлагает отличные функции отчетности и визуализации данных, основанные на данных истории. Это делает **zabbix** идеальным для планирования мощности и мониторинга состояния серверов.

Zabbix разделяется на два вида: **zabbix-agent** и **zabbix-server**.

Zabbix-server собирает данные со всех клиентов, обрабатывает их, выводя на экран в веб-интерфейсе, и рассылает уведомления.

Zabbix-agent установлен на серверах, с которых необходимо собирать информацию об их состоянии, таких агентов может быть множество.

Настройка zabbix-agent

На сервере, который необходимо отслеживать, выполните следующие действия:

1. Установите **zabbix-agent**:

```
dnf install zabbix-agent
```

2. Настройте файл конфигурации:

```
nano /etc/zabbix/zabbix_agentd.conf
```

По умолчанию достаточно просто прописать IP-адрес сервера мониторинга:

```
Server=<ip-адрес_сервера>
```

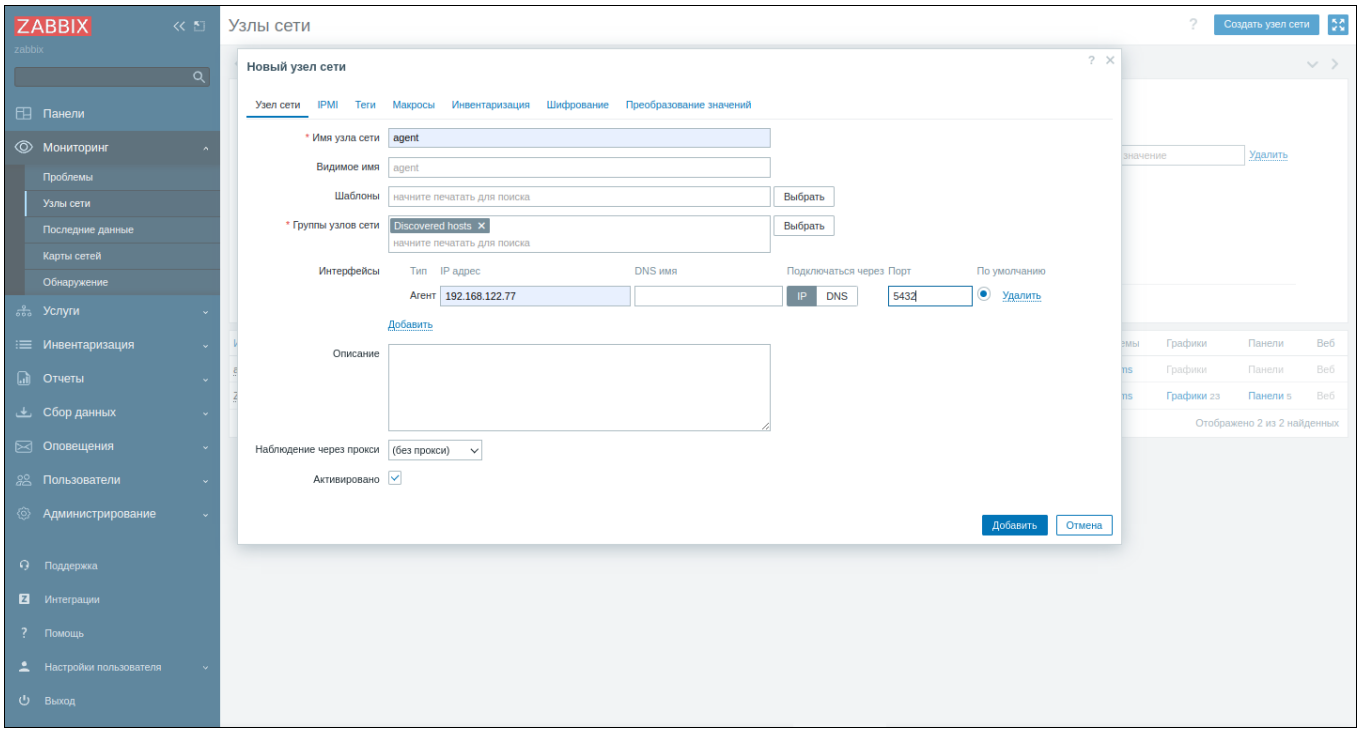
3. Запустите сервис и добавьте его в автозапуск:

```
systemctl enable zabbix-agent
systemctl start zabbix-agent
systemctl status zabbix-agent
```

Добавление zabbix-agent

В веб-интерфейсе **zabbix**-сервера добавьте новый узел в меню «**Мониторинг**» - «**Узлы сети**» - «**Создать узел сети**».

Далее впишите имя узла, укажите группу, в которой он должен состоять, для параметра «**Интерфейсы**» нажмите «**Добавить**», пропишите IP- или DNS-адрес узла и нажмите кнопку « **Добавить**».



На этом настройка **zabbix**-агента успешно завершена.

Более подробную информацию о **zabbix** можно найти на официальном сайте.

Настройка Prometheus с применением системы визуализации данных Grafana

Установка и настройка Prometheus на сервере
Установка экспортера на целевом (клиентском) сервере
Установка и настройка Grafana

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: grafana-11.2.4-1, golang-github-prometheus-2.49.1-1, prometheus-node_exporter-1.6.0-1

Prometheus — программное обеспечение с открытым исходным кодом, используемое для мониторинга различных систем (например, нагрузки на сервер). В **prometheus** происходит запись метрик в реальном времени в базу данных временных рядов.

Установка и настройка Prometheus на сервере

Для установки **prometheus** выполните команду:

```
dnf install golang-github-prometheus
```

Запустите **prometheus** и добавьте его в автозагрузку:

```
systemctl enable prometheus --now
```

Проверьте статус службы:

```
systemctl status prometheus
```

В статусе должно отображаться **active(running)**.

Мониторинг можно производить через веб-интерфейс, введя в адресную строку браузера `http://<IP-адрес_сервера>:9090/graph`.

Установка экспортера на целевом (клиентском) сервере

Экспортер — программное обеспечение (клиентская часть), задача которого заключается в экспорте информации о машине в формате, понятном **Prometheus**. Устанавливается и настраивается непосредственно на клиентском сервере.

Существует множество экспортеров для разных систем и сервисов. Большое количество экспортеров доступно на официальном сайте.

Установка node exporter из репозитория

В качестве примера будет рассмотрена настройка одного из самых популярных экспортеров — **Node Exporter**, который собирает множество системных метрик (процессор, память и т.д.) для оценки состояния сервера и его нагрузки. **Node Exporter** доступен в репозитории РЕД ОС.

Создайте пользователя **nodeusr**:

```
useradd -rs /bin/false nodeusr
```

Для установки экспортера выполните команду (потребуются права **администратора** системы):

```
sudo dnf install prometheus-node_exporter
```

Установка node exporter с внешнего ресурса

Однако не все из существующих экспортеров доступны для установки из репозитория РЕД ОС. Далее будет рассмотрен пример установки экспортера *node exporter* с официального сайта *Prometheus*. Согласно приведенному примеру можно устанавливать и другие экспортеры с официального сайта *Prometheus*.

Для установки экспортера скачайте последнюю версию программы на официальном сайте либо используйте команду:

```
wget https://github.com/prometheus/node_exporter/releases/download/v1.5.0/node_exporter-1.5.0.linux-amd64.tar.gz
```

Перейдите в каталог со скачанным архивом (в примере **/home/user/Загрузки**) и распакуйте его:

```
cd /home/user/Загрузки
tar -xvzf node_exporter-1.5.0.linux-amd64.tar.gz
```

Затем создайте пользователя **nodeusr**:

```
useradd -rs /bin/false nodeusr
```

Установите экспортер путем копирования:

```
mv node_exporter-1.5.0.linux-amd64/node_exporter /usr/bin/
```

Настройте политики безопасности SELinux:

```
restorecon -v /usr/bin/node_exporter
```

Настройка node exporter

Создайте службу для запуска:

```
nano /etc/systemd/system/node_exporter.service
```

со следующим содержимым:

```
[Unit]
Description=Node Exporter
After=network.target
[Service]
User=nodeusr
Group=nodeusr
Type=simple
ExecStart=/usr/bin/node_exporter
[Install]
WantedBy=multi-user.target
```

Запустите **node_exporter** и добавьте его в автозагрузку:

```
systemctl enable node_exporter --now
```

Проверьте статус службы:

```
systemctl status node_exporter
```

В статусе должно отображаться **active(running)**.

Для отображения метрик введите в адресную строку браузера `http://<IP-адрес_клиентского_сервера>:9100/metrics`.

На сервере откройте конфигурационный файл (необходимы права суперпользователя):

```
nano /etc/prometheus/prometheus.yml
```

и дополните секцию `scrape_configs` следующими строками:

```
  - job_name: 'node_1'
    static_configs:
      - targets: ['<IP-адрес_клиентского_сервера>:9100']
```

Для применения изменений перезапустите **prometheus**:

```
systemctl restart prometheus
```

> **Примечание.**
>
> Если после перезапуска **prometheus** в статусе отображается **failed**, необходимо проверить корректность заполнения файла конфигурации. Ошибки отображаются в журнале **/var/log/messages**.

Мониторинг можно производить через веб-интерфейс, указав в адресной строке браузера https://**<IP-адрес_сервера_Prometheus>**:9090/targets.

Установка и настройка Grafana

Grafana — платформа с открытым исходным кодом для визуализации, мониторинга и анализа данных. **Grafana** позволяет пользователям создавать дашборды с панелями, каждая из которых отображает определенные показатели в течение установленного периода времени. Каждый дашборд универсален, поэтому его можно настроить для конкретного проекта или с учетом любых потребностей разработки и/или бизнеса.

Установка Grafana

Для установки **Grafana** выполните команду:

```
dnf install grafana
```

Запустите **grafana-server** и добавьте его в автозагрузку:

```
systemctl enable grafana-server --now
```

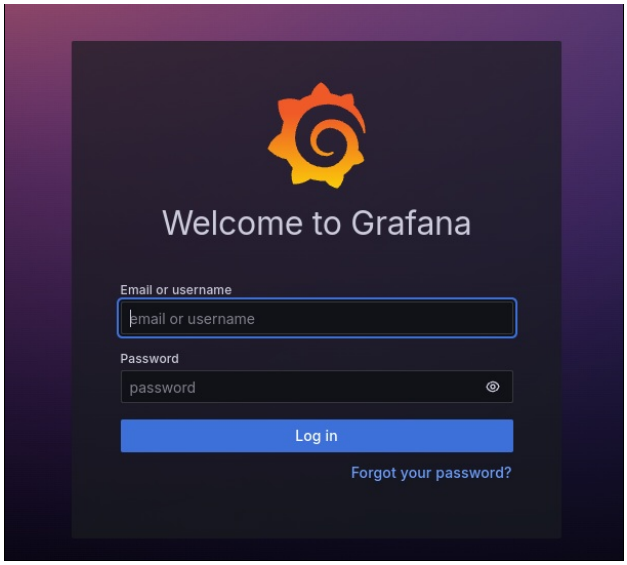
Проверьте статус сервера:

```
systemctl status grafana-server
```

В статусе должно отображаться **active(running)**.

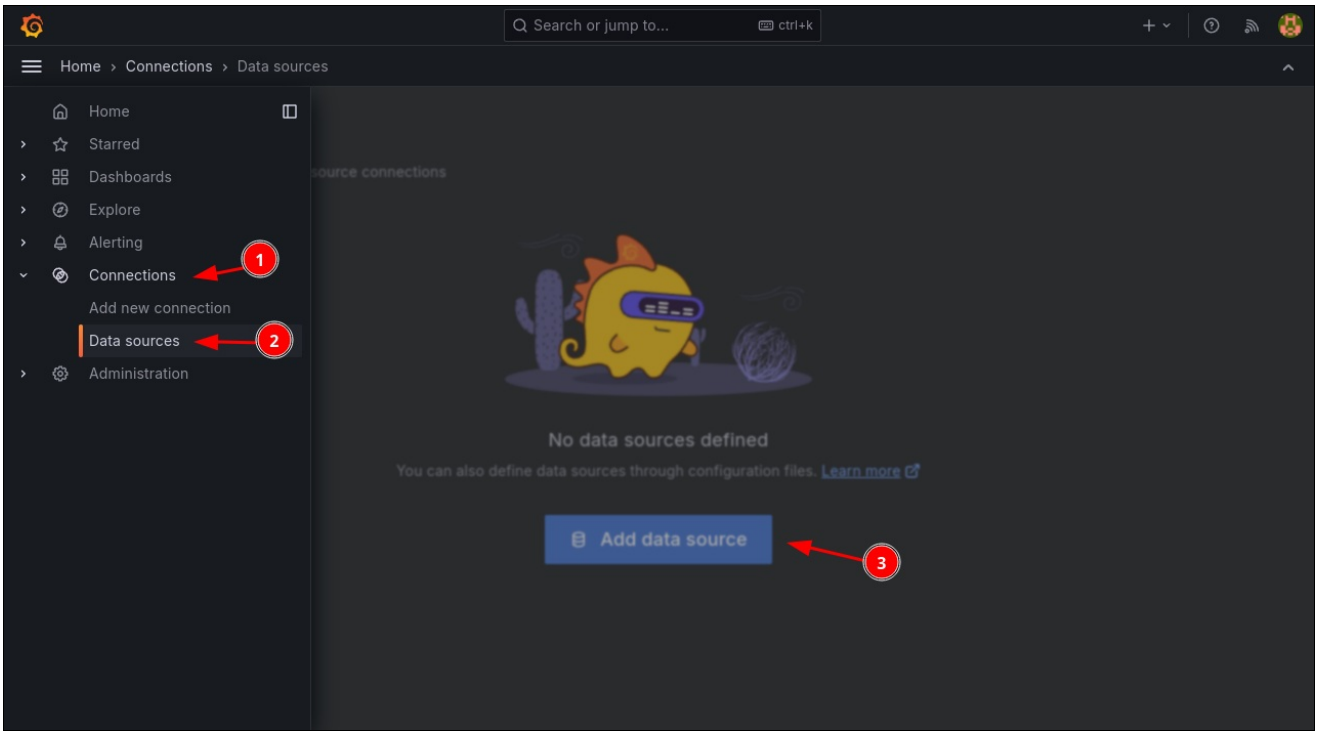
Настройка Grafana

Веб-интерфейс доступен по адресу http://**<IP-адрес_сервера>**:3000/.

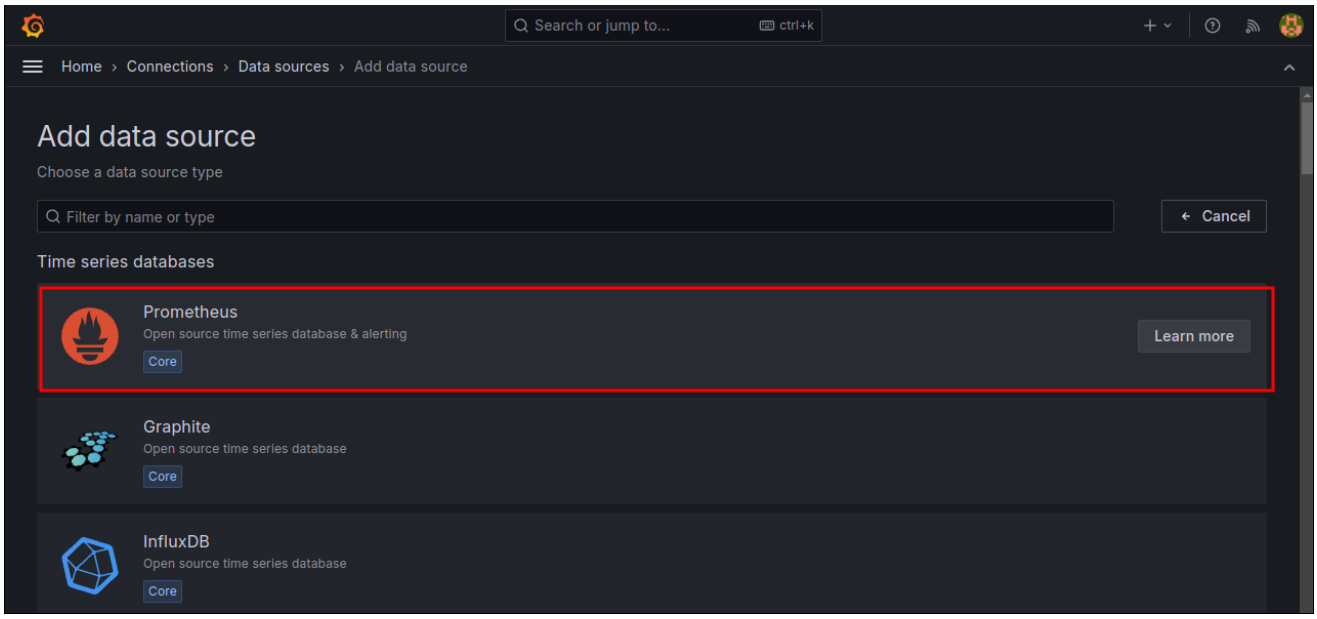


Логин и пароль для входа: **admin**/**admin**. При первом входе будет запрошена смена пароля.

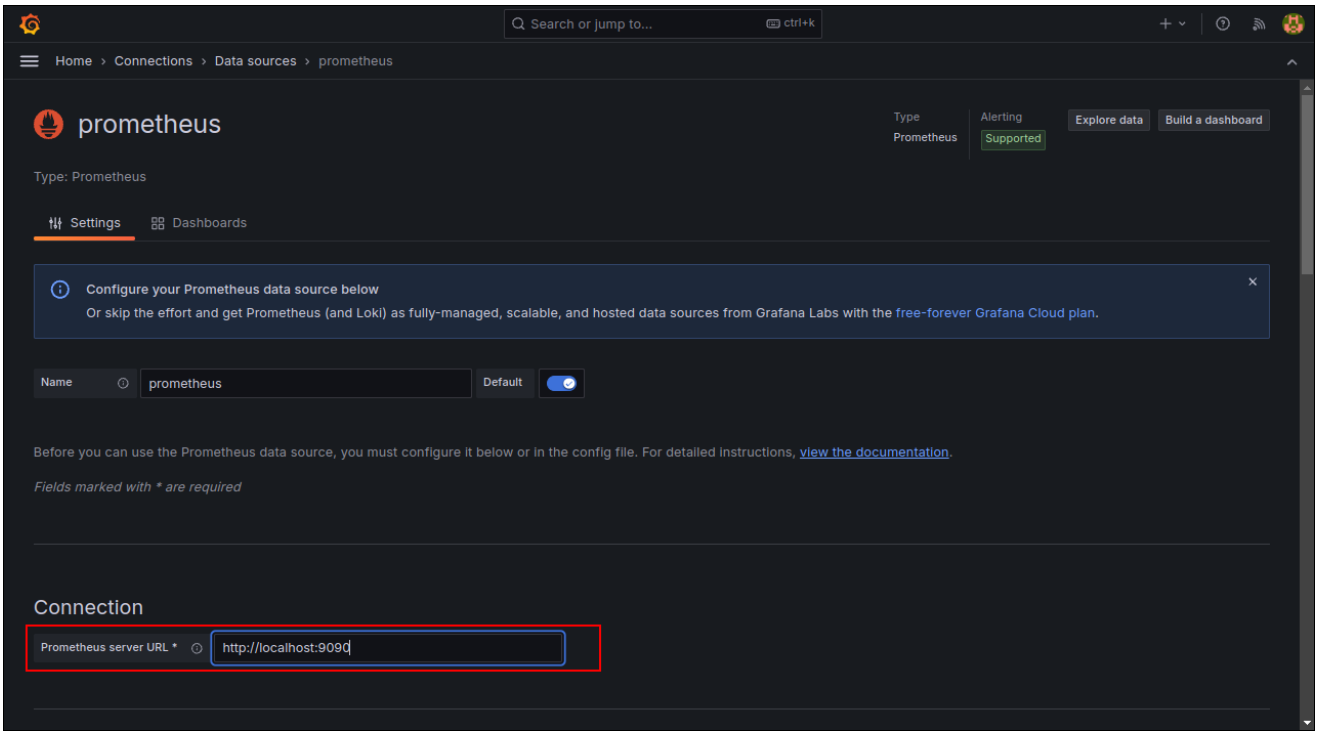
Далее добавьте источник данных для **Grafana**, выбрав **Home** - **Connections** - **Data Sources** - **Add data source**.

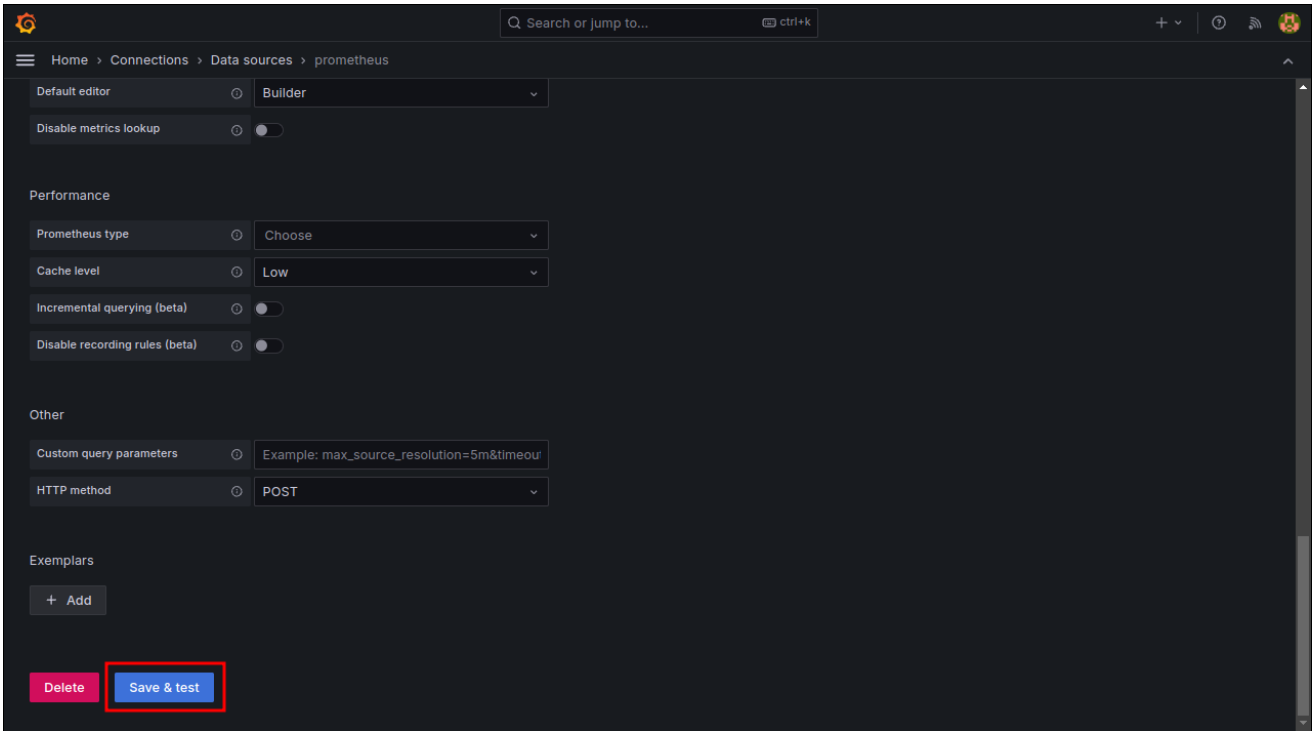


Выберите из списка **Prometheus**, кликнув по нему ЛКМ.



В настройках укажите *IP-адрес* и *порт* сервера с **Prometheus**, остальные настройки ситуативны и устанавливаются по желанию. Для сохранения настроек нажмите **Save & Test**.



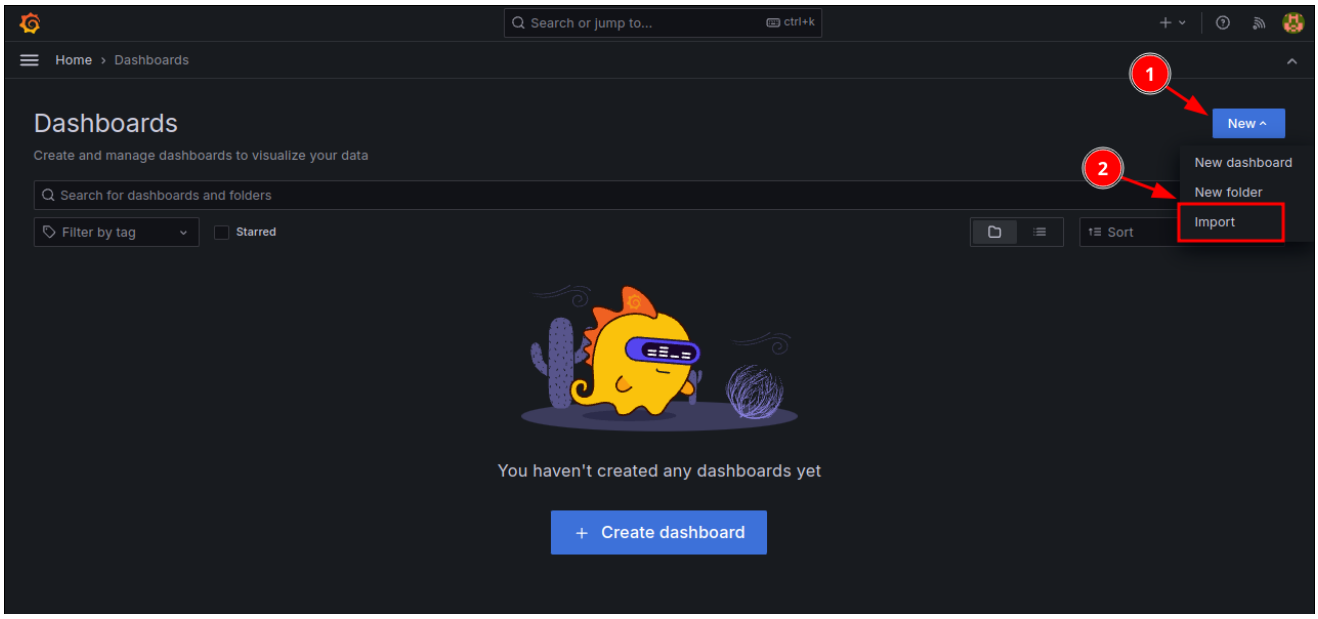


Загрузка дашбордов

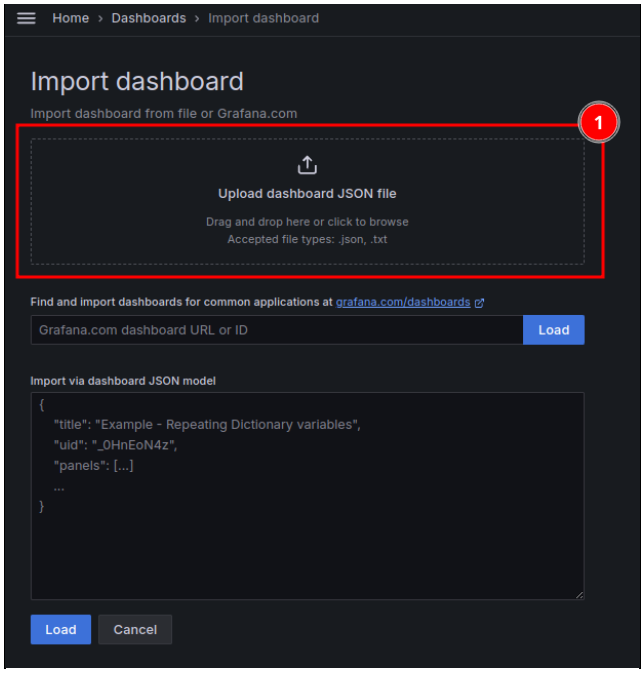
Существует множество готовых дашбордов (в формате JSON), которые можно импортировать. Например, *id=9614* или *id=13978*. Наиболее универсальным является *id=1860*, его можно скачать по ссылке (в примере использована *ревизия 27*).

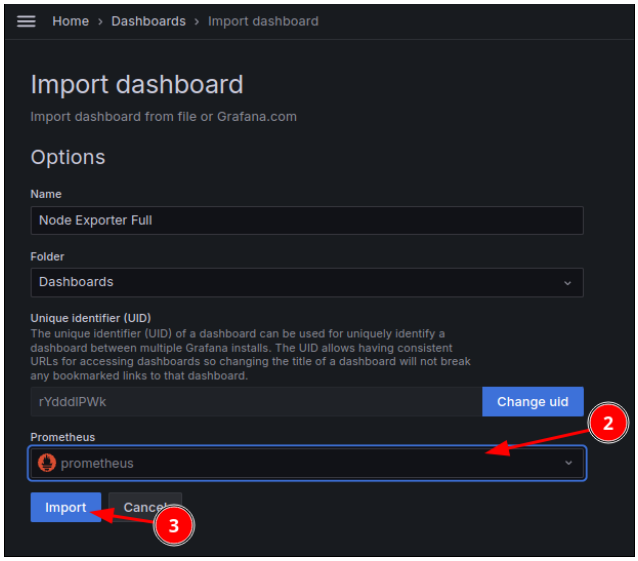
> **Примечание.**
>
> Для указанных в *Окружении* версий **Prometheus** и **Grafana** могут быть использованы дашборды с **ревизией 27 и ниже**. В случае использования *ревизий 28 и выше* при работе могут возникнуть ошибки.

Для импорта дашборда выберите **Home** - **Dashboards** и нажмите **New** - **Import**.

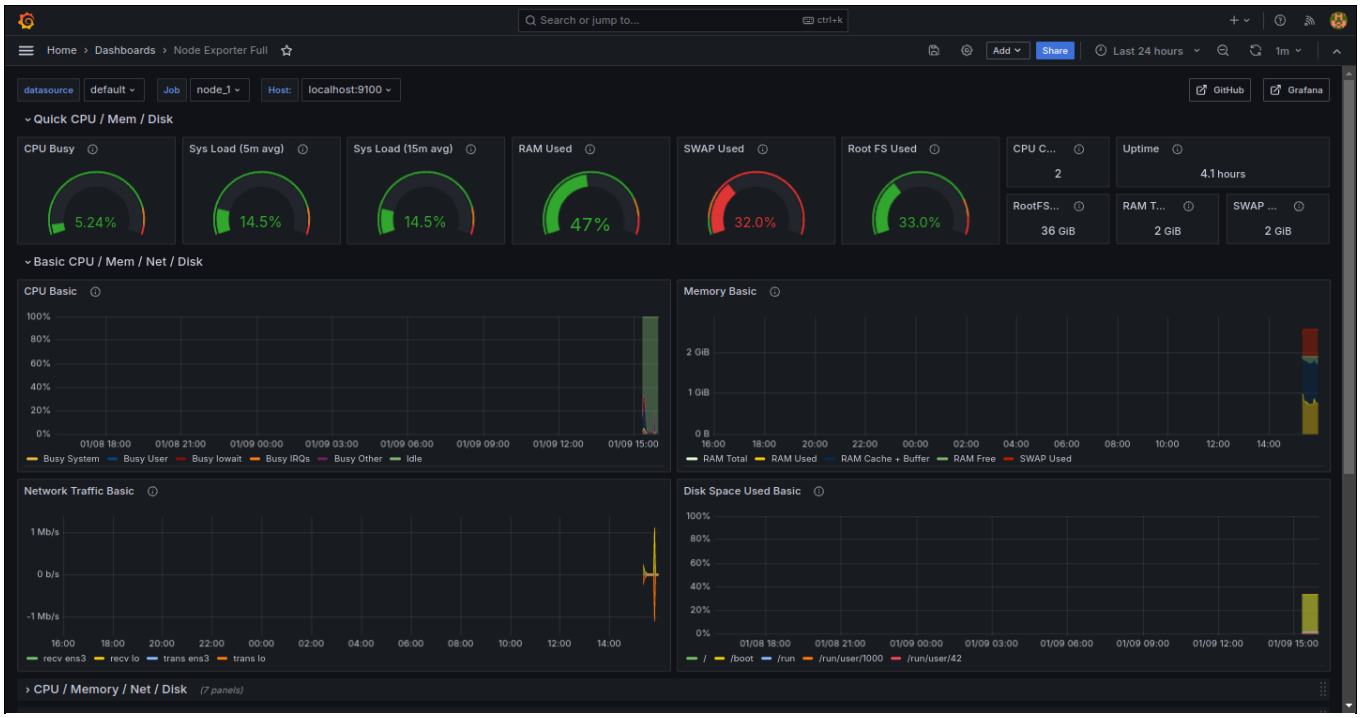


Далее, нажав **Upload dashboard JSON file**, выберите скачанный раннее JSON-файл. В появившемся окне **Options** выберите **Prometheus** и нажмите **Import**.





Загруженный *дашборд 1860* выглядит следующим образом:



Каталог с данными **prometheus** располагается по пути **/var/lib/prometheus**.

Настройка GLPI-сервера (для инвентаризации оборудования)

Установка GLPI
Настройка glpiinventory plugin на сервере
Настройка glpi-agent на клиенте
Установка дополнительных плагинов
Первичная настройка GLPI
Основные разделы GLPI. Заявки
Основные разделы GLPI. Уведомления
Основные разделы GLPI. Интерфейс
Основные разделы GLPI. Автоматические действия
Основные разделы GLPI. SLA
Основные разделы GLPI. Автоматическое назначение заявок
Основные разделы GLPI. Отчет

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** glpi-9.5.7-3

Gestionnaire libre de parc informatique (**GLPI**) - свободный менеджер ИТ-инфраструктуры - является системой работы с заявками и инцидентами, а также используется для инвентаризации компьютерного оборудования (компьютеры, программное обеспечение, принтеры и т.д.). Имеет расширенные функции, такие как работа системы отслеживания почты с уведомлением, методы для создания базы данных с основной информацией о топологии сети и т.д. *GLPI* - это веб-приложение, разрабатывающееся на PHP.

GLPI включает следующие возможности:

- инвентаризация компьютеров, периферийного оборудования, сетевых принтеров и связанных компонентов через интерфейс с OCS Inventory или FusionInventory;
- управление заявками и инцидентами;
- управление лицензиями, договорами (по стандарту ITIL);
- связывание пользователей и групп по географическому положению;
- управление деловой и финансовой информацией (договоры);
- управление статусом объектов;
- поддержка базы знаний и часто задаваемых вопросов (FAQ);
- генераторы отчетов;
- поддержка базы данных MySQL/MariaDB;
- поддержка UTF8;
- система оповещения о событиях.

GLPI позволяет увеличивать функциональность с помощью подключения плагинов.

Установка GLPI

Для установки необходимых пакетов откройте консоль и воспользуйтесь следующей командой (обратите внимание, что команды выполняются с правами администратора):

```
dnf install glpi mariadb mariadb-server php-pear-CAS php-ldap php-opcache php-apcu php-xmlrpc php-zip php-sodium
```

Выполните команду переразметки SELinux:

```
touch /.autorelabel
```

Инициализация БД – запомните пароль, создающийся для root-пользователя БД. На вопросы по умолчанию отвечайте «**Y**».

```
systemctl enable --now mariadb
```

```
/usr/bin/mysql_secure_installation
```

```
 mysql -u root -p
```

```
CREATE USER 'glpi'@'%' IDENTIFIED BY 'glpiDBSecret';
```

```
GRANT USAGE ON *.* TO 'glpi'@'%' IDENTIFIED BY 'glpiDBSecret';
CREATE     DATABASE IF NOT EXISTS `glpi` ;
GRANT ALL PRIVILEGES ON `glpi`.* TO 'glpi'@'%';
FLUSH PRIVILEGES;
EXIT
```

Проверка соединения с БД осуществляется командой:

```
mysql -uglpi -pglpiDBSecret glpi
```

```
exit
```

Далее запустите веб-сервис командой:

```
systemctl enable --now httpd
```

В файл конфигурации **/etc/httpd/conf/httpd.conf** добавьте строку:

```
Timeout 600
```

Перезапустите службу веб-сервиса для применения изменений:

```
systemctl restart httpd
```

Назначьте права на директорию:

```
chown -R apache /usr/share/glpi
```

Настройка SELinux

SELinux должен находиться в режиме **Enforcing**, если SELinux установлен в какой-либо другой режим работы, необходимо самостоятельно перевести его, выполнив команду:

```
nano /etc/selinux/config
```

Затем привести строку с установленным режимом к виду:

```
SELINUX=enforcing
```

Выполните команды:

```
setenforce 1
setsebool -P httpd_can_network_connect on
setsebool -P httpd_can_network_connect_db on
setsebool -P httpd_can_sendmail on
setsebool -P httpd_unified 1
setsebool -P httpd_read_user_content 1
```

Для настройки входа по IP-адресу выполните команду:

```
nano /etc/httpd/conf.d/glpi.conf
```

Добавьте в секцию **Require** ваш ip-адрес – в качестве примера «**192.168.1.56**»:

```
<IfModule mod_authz_core.c>
 # Apache 2.4
 Require local
 Require ip 192.168.1.56
 </IfModule>
```

Затем следует выполнить настройку защищенности файлов. Добавьте секцию:

```
<Directory /usr/share/glpi/files>
 <IfModule mod_authz_core.c>
```

```
Require all denied
</IfModule>
<IfModule !mod_authz_core.c>
deny from all
</IfModule>
</Directory>
```

+ Пример итогового конфигурационного файла:

```
Alias /glpi /usr/share/glpi
 <Directory /usr/share/glpi>
 Options None
 AllowOverride Limit Options FileInfo
 <IfModule mod_authz_core.c>
 Require local
 Require ip 192.168.1.56
 </IfModule>
 <IfModule !mod_authz_core.c>
 Order deny,allow
 Allow from all
 </IfModule>
 </Directory>
 <Directory /usr/share/glpi/install>
 <IfModule mod_authz_core.c>
 Require local
 </IfModule>
 <IfModule !mod_authz_core.c>
 Order Deny,Allow
 Deny from All
 Allow from 127.0.0.1
 Allow from ::1
 </IfModule>
 <IfModule mod_php5.c><
 php_value max_execution_time 0
 php_value memory_limit -1
 </IfModule>
 <IfModule mod_php7.c>
 php_value max_execution_time 0
 php_value memory_limit -1
 </IfModule>
 </Directory>
 <Directory /usr/share/glpi/config>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/locales>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/install/mysql>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/scripts>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/files>
```

```
<IfModule mod_authz_core.c>
Require all denied
</IfModule>
<IfModule !mod_authz_core.c>
deny from all
</IfModule>
</Directory>
```

Перезапустите сервис для применения внесенных изменений:

```
systemctl restart httpd
```

Для обновления меток selinux необходимо перезагрузить ПК.

Вход через браузер будет производиться по адресу:

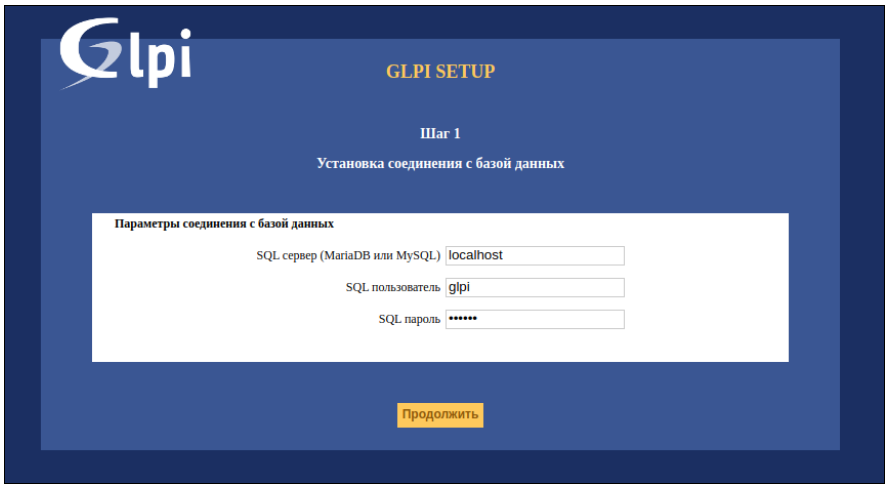
```
http://192.168.1.56/glpi/install/install.php
```

Статусы проверки должны быть успешными:

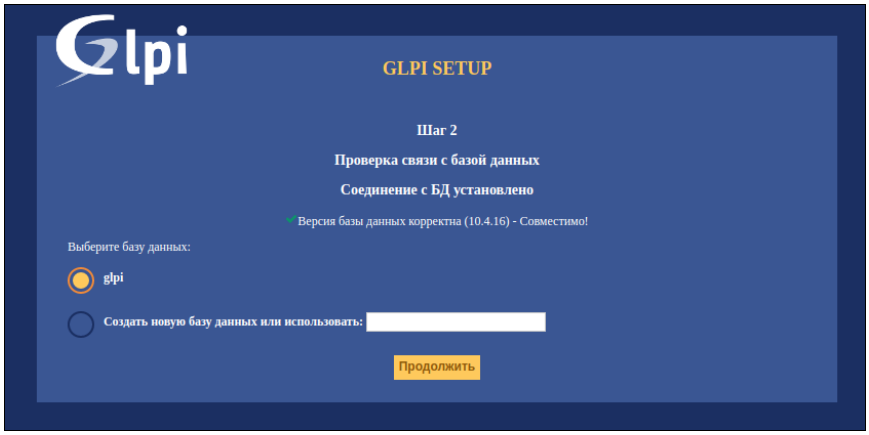


Настройка соединения с БД – требуется пароль, созданный для root-пользователя БД:

```
IP - 127.0.0.1
user - glpi
pass – {пароль glpi-пользователя БД}
```



Выберите Базу Данных GLPI:



После завершения установки вход в веб-форму администратора осуществляется по данным:

```
user - glpi
pass - glpi
```



Настройка glpiinventory plugin на сервере

Установите пакет:

```
dnf install glpi-plugin-glpiinventory
```

В браузере перейдите по ссылке:

```
http://192.168.1.56/glpi/front/plugin.php
```

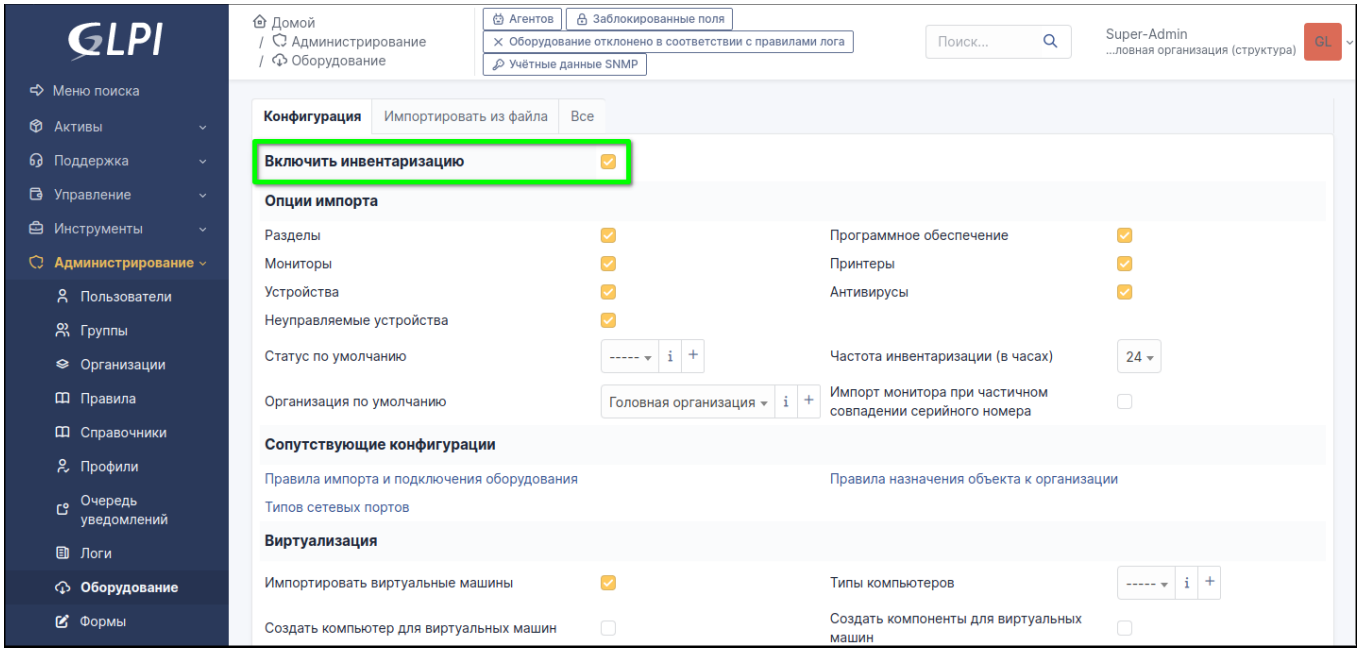
В списке плагинов должен отобразиться **GLPI Inverntory**, нажмите на иконку «**Установить**».



После этого плагин можно будет активировать.

Перейдите в пункт меню «**Администрирование**» — «**Оборудование**» либо по адресу: http://192.168.1.56/glpi/front/inventory.conf.php.

Включите инвентаризацию и сохраните изменения.



Настройка glpi-agent на клиенте

На клиентской машине установите пакет:

```
dnf install glpi-agent
```

Измените конфигурационный файл:

```
nano /etc/glpi-agent/agent.cfg
```

Впишите IP-сервера в строку, предварительно раскомментировав ее:

```
server = http://192.168.1.56/glpi/plugins/glpiinventory/
```

Выполните запуск службы:

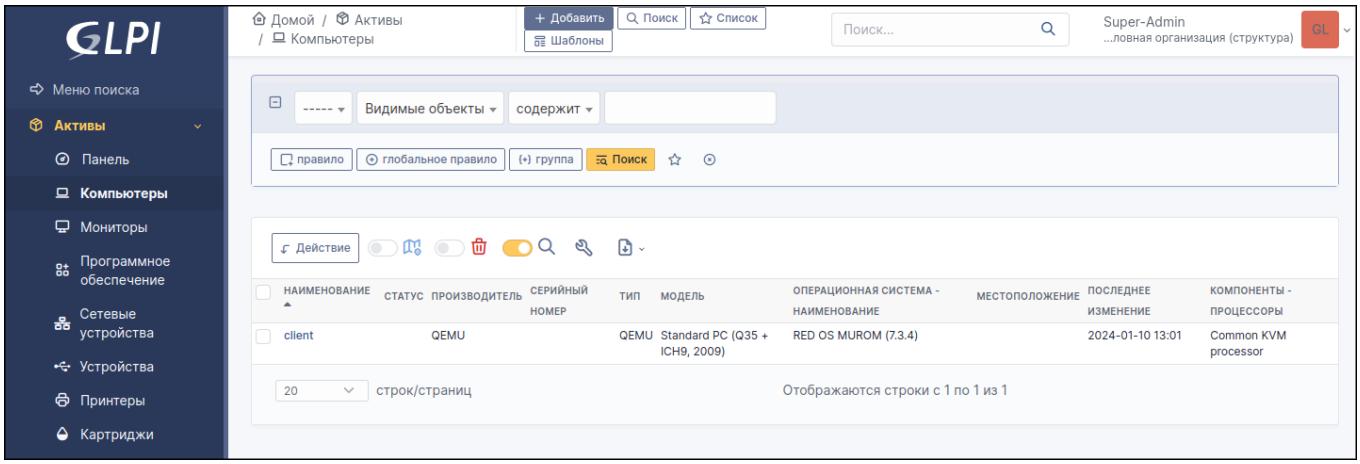
```
systemctl enable --now glpi-agent.service
```

По умолчанию инвентаризация будет запущена *через 1 час* после запуска службы. Этот параметр можно изменить, указав необходимое значение в секундах в строке delaytime в конфигурационном файле **/etc/glpi-agent/agent.cfg**.

Для ручного запуска инвентаризации на клиенте можно использовать команду:

```
glpi-agent -f --conf-file=/etc/glpi-agent/agent.cfg --daemon
```

После выполнения вышеперечисленных действий на сервере появится информация о ПК-клиенте:



Установка дополнительных плагинов

Список доступных плагинов в репозитории РЕД ОС можно получить, выполнив команду:

```
dnf search glpi-plugin
```

Для установки плагина необходимо выполнить команду вида:

```
dnf install glpi-plugin-<имя_плагина>
```

После установки пакета плагин будет отображаться в меню «**Настройки**» — «**Плагины**» веб-интерфейса сервера, где его можно будет установить и включить.

Первичная настройка GLPI

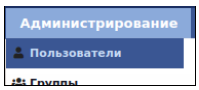
Удаление файла автонастройки install.php

После установки GLPI на главной странице появится уведомление о том, что надо удалить из корневой папки файл автонастройки **install/install.php**, удалите его командой:

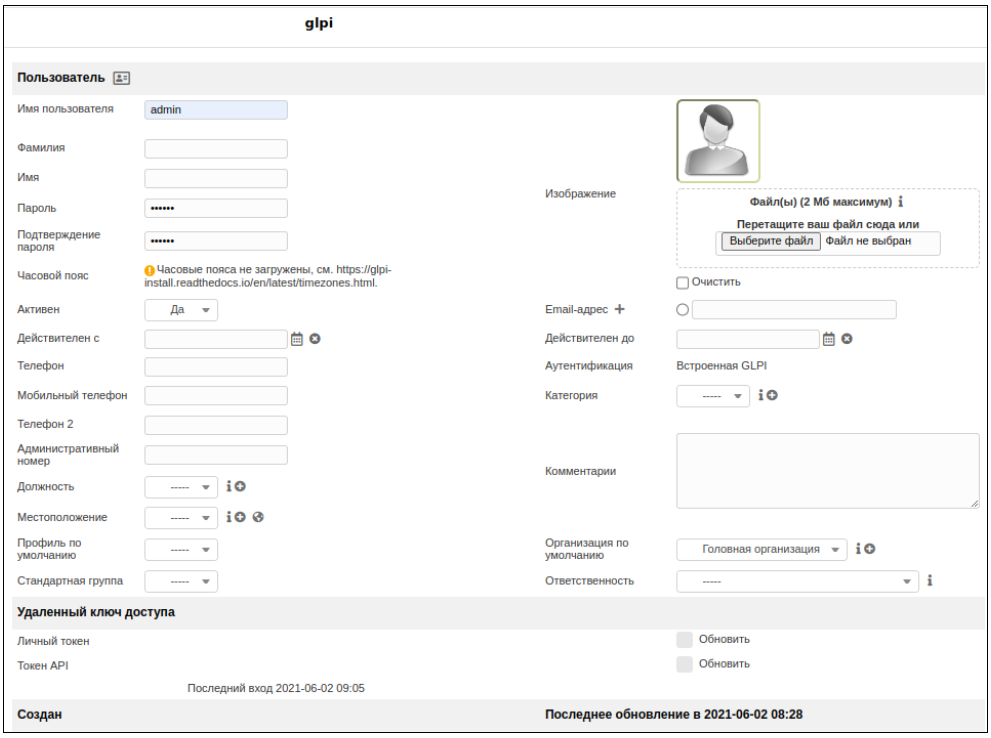
```
rm /usr/share/glpi/install/install.php
```

Переименовывание базовых пользователей

После завершения установки система автоматически создаст 4 учетных записи с паролем и логином по умолчанию. После входа в систему данные учетные записи нужно будет переименовать и сменить на них пароли. Для смены паролей необходимо перейти в *«Администрирование» -> «Пользователи»*:



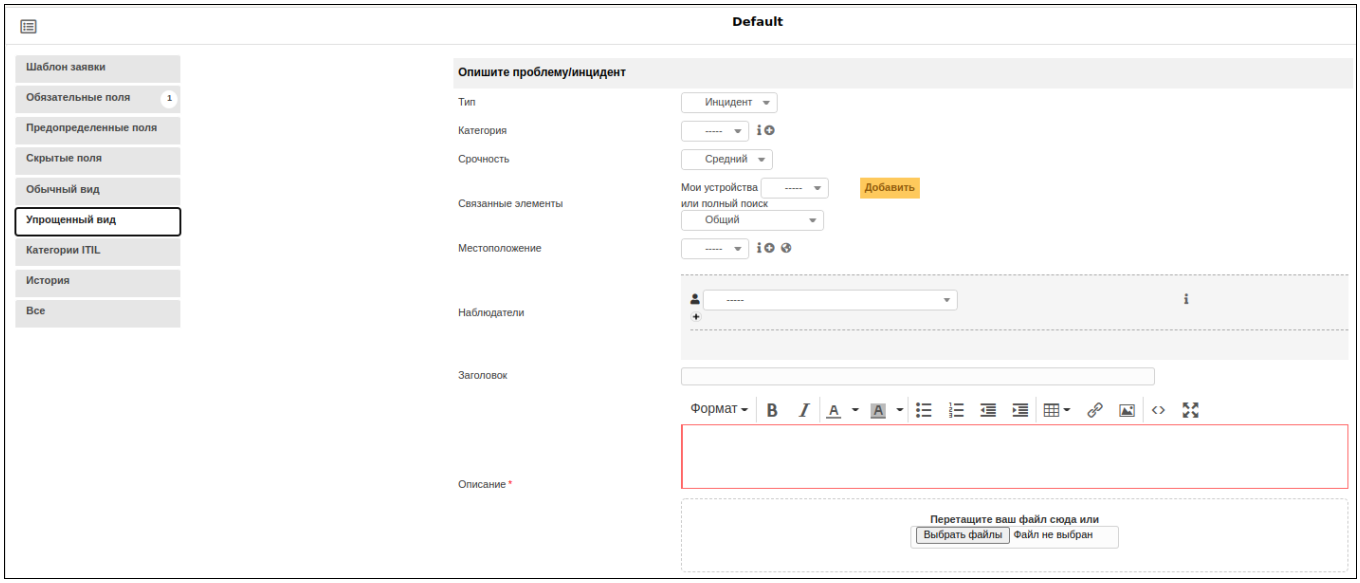
Переходим в настройки нужного пользователя и меняем необходимые данные:



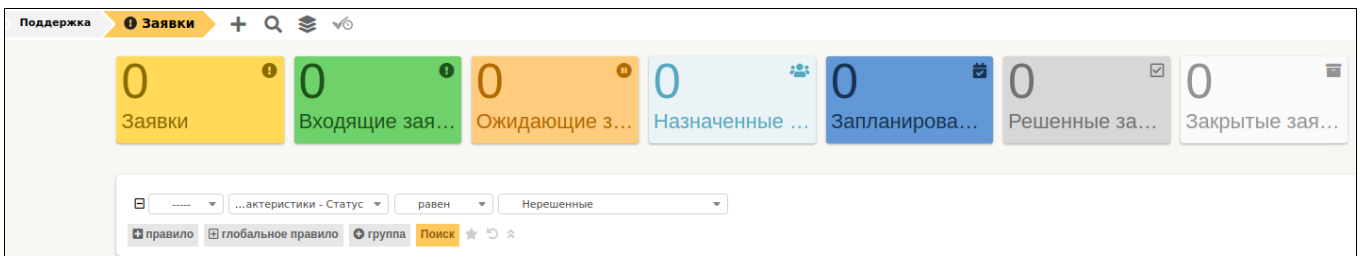
Основные разделы GLPI

Заявки

Для настройки заявок необходимо перейти в *«Поддержка» -> «Заявки» -> «Управление шаблонами»* (две горизонтальные линии с разрывом). Выбираем шаблон для настройки, в левой части находятся параметры данного шаблона:

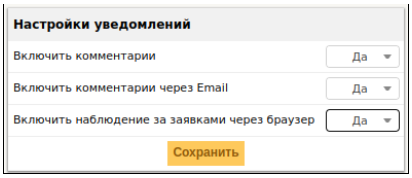


При переходе в меню заявок можно просмотреть список доступных заявок, создать собственную заявку или отсортировать список заявок:



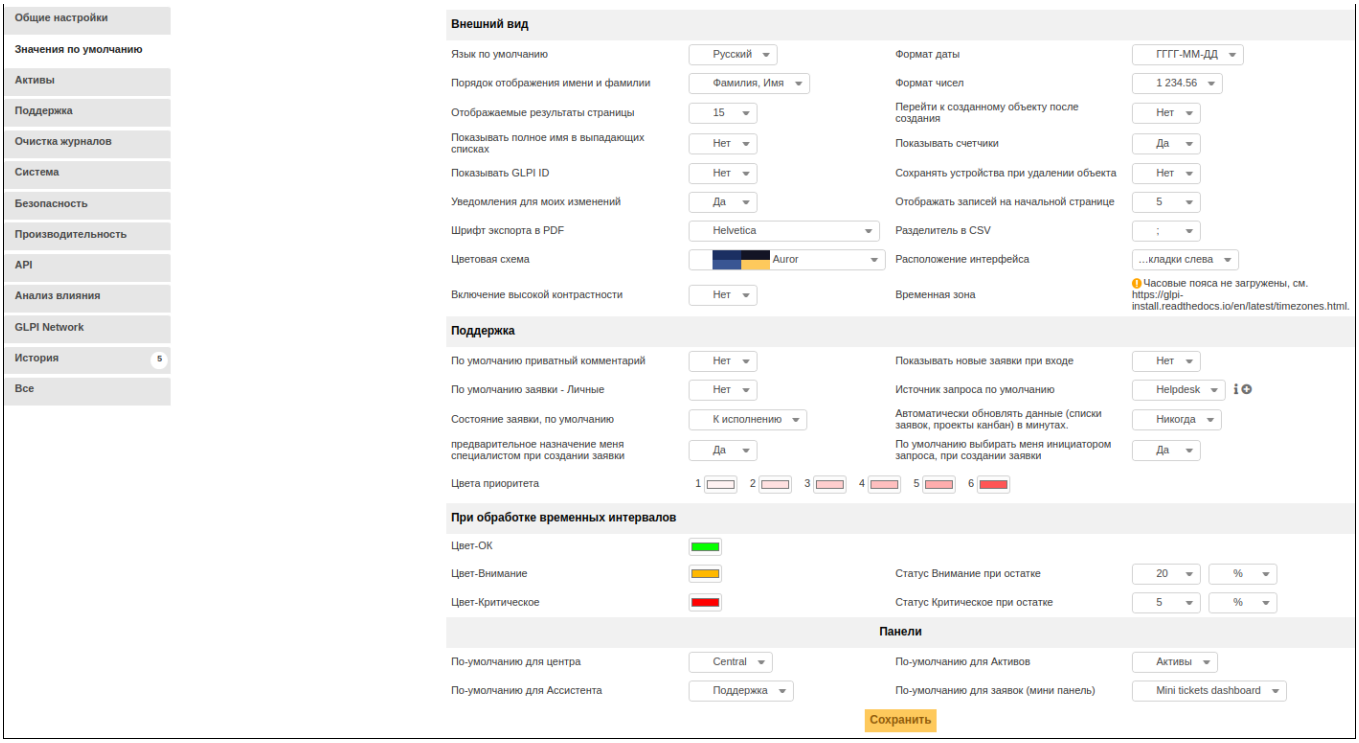
Уведомления

Для настройки уведомлений перейдите в *«Настройки» -> «Уведомления»* и включите уведомления о комментариях, уведомлениях по *e-mail* и браузерные оповещения:



Интерфейс

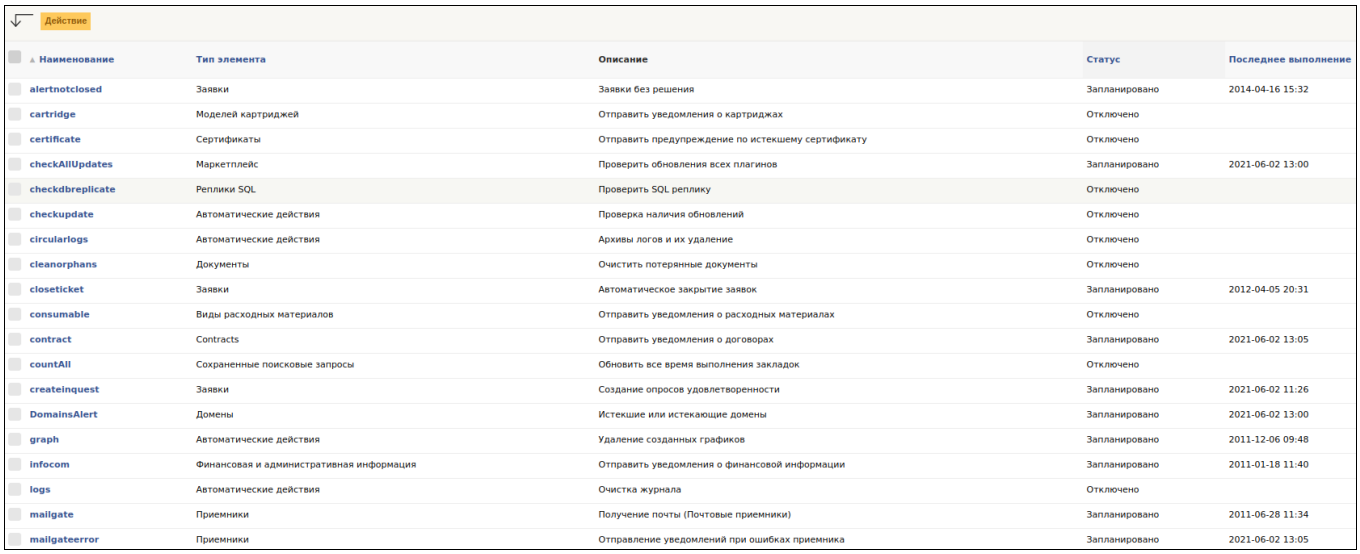
В GLPI есть несколько способов настроить отображаемый внешний вид вкладок и интерфейс. Для настройки первым способом перейдите в *«Настройки» -> «Общий» -> «Значения по умолчанию»*:



В открывшейся вкладке можно настроить интерфейс как вам удобно. Для настройки вторым способом (для конкретного пользователя) перейдите по имени профиля в правом верхнем углу -> *«Внешний вид»*.

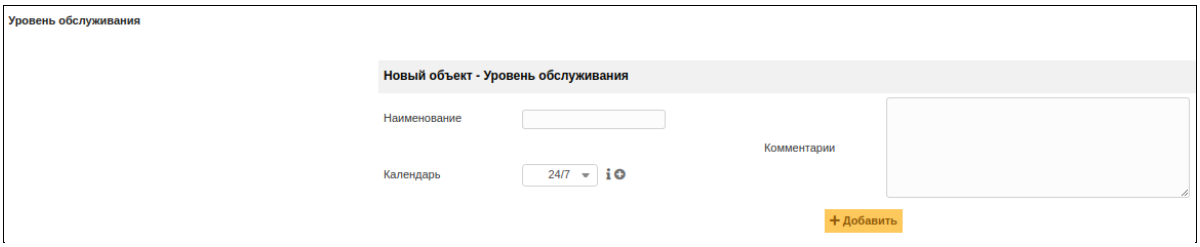
Автоматические действия

В GLPI имеется возможность запускать автоматически выполняемые команды. Для этого перейдите в *«Настройки» -> «Автоматические действия»*. С помощью действий можно настроить автоматическую отправку уведомлений, очистку журнала, закрытие заявок и т.д. Для данных команд можно настроить время запуска или при необходимости запустить вручную.



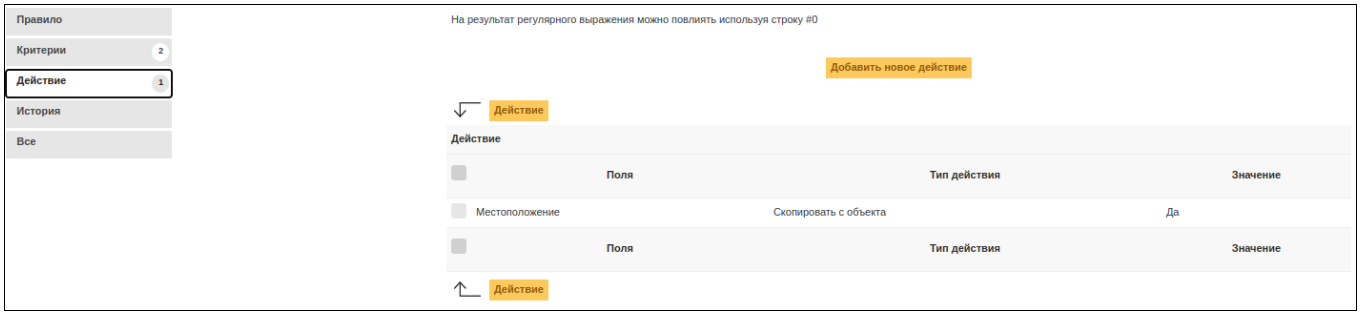
SLA

В GLPI имеется возможность добавления уровней обслуживания (SLA). Для этого перейдите в *«Настройки» -> «Уровни обслуживания»*, в открывшемся списке можно отсортировать имеющиеся уровни или добавить новый уровень, нажав на плюс в левой части панели:



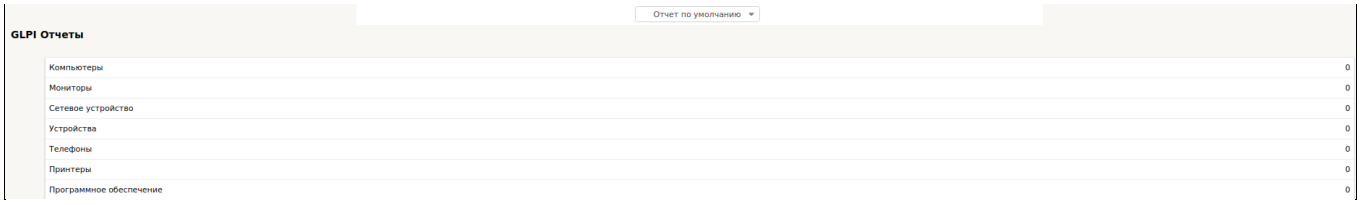
Автоматическое назначение заявок

Имеется возможность автоматического назначения заявки на сотрудника. Для этого перейдите в *«Администрирование» -> «Правила» -> «Бизнес-правила для заявок»*, в появившемся списке нужно выбрать правило и настроить его:



Отчет

Позволяет увидеть все, что происходит в системе, получить статистику и информацию по инвентаризации. Для просмотра отчёта переходим в *«Инструменты» -> «Отчет»* и выбираем необходимый тип отчёта:



OpenSearch — система распределенного поиска, сбора, анализа и визуализации данных

OpenSearch
Установка и настройка OpenSearch
OpenSearch Dashboards
Установка и настройка OpenSearch Dashboards
Logstash
Установка и настройка logstash
Beats
Установка и настройка filebeat
Установка и настройка auditbeat
Установка и настройка heartbeat
Установка и настройка metricbeat
Установка и настройка packetbeat
Отображение данных в OpenSearch Dashboards
Создание шаблона индексов
Создание информационной панели OpenSearch Dashboards
Использование Discover

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: opensearch-2.13.0, opensearch-dashboards-2.13.0, logstash-8.9.0, auditbeat-7.17.14, filebeat-7.17.14, heartbeat-7.17.14, metricbeat-7.17.14, packetbeat-7.17.14

OpenSearch стек (OpenSearch, Logstash, OpenSearch Dashboards) — это форк ELK стека (Elasticsearch, Logstash, Kibana). Конвейер обработки данных журнала состоит из трёх этапов: агрегация, обработка и хранение. В традиционном стеке обработка и агрегация данных осуществлялись с использованием **Logstash**. Из-за проблем с производительностью и сложностью обработки данных возникла потребность в использовании **Beats**.

Beats — это легковесные агенты сбора данных, каждый из которых предназначен для определенной задачи:

- **auditbeat** — сбор данных аудита безопасности;
- **filebeat** — мониторинг и сбор лог-файлов;
- **heartbeat** — проверка доступности служб;
- **metricbeat** — сбор метрик системы и служб;
- **packetbeat** — анализ трафика сетевых пакетов.

OpenSearch

Opensearch — это распределенная система полнотекстового поиска и анализа данных, работающая в режиме реального времени. После добавления данных в **opensearch** можно выполнять полнотекстовый поиск со сложными функциями: поиск по полю, поиск по нескольким индексам, повышение полей, ранжирование результатов по баллам, сортировка результатов по полю и агрегирование результатов.

Opensearch можно использовать в качестве серверной части для поискового приложения, система обеспечивает хорошую производительность и имеет возможность масштабироваться в зависимости от потребностей приложения.

Установка и настройка OpenSearch

Для установки **opensearch** выполните следующий алгоритм действий:

1. Выполните установку пакетов (потребуются права **администратора**).

Для установки **opensearch** необходимо определить собственный пароль администратора, чтобы настроить демонстрационную конфигурацию безопасности.

```
sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=<custom-admin-password> dnf install opensearch
```

где:

<custom-admin-password> — установите самостоятельно заданный пароль администратора длиной от 12 символов, содержащий прописные буквы (A-Z), строчные буквы (a-z), спецсимволы, цифры (0-9).

2. Перезагрузите конфигурацию диспетчера **systemd**:

```
sudo systemctl daemon-reload
```

3. Добавьте **opensearch** в автозагрузку и запустите службу:

```
sudo systemctl enable opensearch --now
```

4. Настройки **opensearch** находятся в файле ***/etc/opensearch/opensearch.yml***. Внесите изменения в конфигурационный файл:

```
sudo nano /etc/opensearch/opensearch.yml
```

5. Измените следующие строки:

```
network.host: 0.0.0.0
 discovery.seed_hosts: ["127.0.0.1", "[::1]"]
```

где:

- **0.0.0.0** — приём на всех интерфейсах;
- **["127.0.0.1", "[::1]"]** — локальный поиск хостов кластера.

Сохраните внесённые в конфигурацию изменения и перейдите в терминал.

6. Перезапустите службу **opensearch**:

```
sudo systemctl restart opensearch
```

7. Для проверки статуса службы **opensearch** можно использовать команду:

```
sudo systemctl status opensearch
```

При успешно выполненных настройках в статусе должно отображаться active (running).

8. Проверьте работу **opensearch**:

```
curl -X GET https://localhost:9200 -u 'admin:<custom-admin-password>' --insecure
```

В терминале должна отобразится информация приблизительно следующего содержания:

```
{
 "name" : "localhost.localdomain",
 "cluster_name" : "opensearch",
 "cluster_uuid" : "6c3fb4JuQJ2HJxQEfLiqIg",
 "version" : {
 "distribution" : "opensearch",
 "number" : "2.13.0",
 "build_type" : "tar",
 "build_hash" : "7ec678d1b7c87d6e779fdef94e33623e1f1e2647",
 "build_date" : "2024-05-13T00:00Z",
 "build_snapshot" : false,
 "lucene_version" : "9.10.0",
 "minimum_wire_compatibility_version" : "7.10.0",
 "minimum_index_compatibility_version" : "7.0.0"
 },
 "tagline" : "The OpenSearch Project: https://opensearch.org/"
 }
```

OpenSearch Dashboards

OpenSearch Dashboards — это веб-интерфейс для **opensearch**, предоставляющий комплексное решение для визуального анализа, обнаружения и запроса данных мониторинга. При работе с **opensearch** через консоль **OpenSearch Dashboards** использовать необязательно. Также вместо **OpenSearch Dashboards** в качестве веб-интерфейса можно использовать другие инструменты, например, **Grafana**.

Установка и настройка OpenSearch Dashboards

Для установки и настройки **opensearch-dashboards** выполните следующий алгоритм действий:

1. Выполните установку пакетов:

```
sudo dnf install opensearch-dashboards
```

2. Перезагрузите конфигурацию диспетчера **systemd**:

```
sudo systemctl daemon-reload
```

3. Затем запустите и добавьте в автозагрузку службу **opensearch-dashboards**:

```
sudo systemctl enable opensearch-dashboards --now
```

4. Откройте конфигурационный файл ***opensearch_dashboards.yml***:

```
nano /etc/opensearch-dashboards/opensearch_dashboards.yml
```

5. Добавьте строку для внешнего подключения к веб-панели:

```
server.host: "192.168.2.15"
```

где:

192.168.2.15 — IP-адрес хоста.

6. Перезапустите службу opensearch-dashboards:

```
sudo systemctl restart opensearch-dashboards
```

7. Проверьте статус службы opensearch-dashboards:

```
sudo systemctl status opensearch-dashboards
```

Отобразится текущий статус службы opensearch-dashboards, включая информацию о том, запущена ли служба, возникли ли ошибки или проблемы при запуске, а также последние записи журнала, связанные со службой. При успешном подключении в статусе должно отображаться: active (running).

Logstash

Logstash является механизмом обработки событий на стороне сервера. Утилита извлекает данные из широкого спектра источников, трансформирует их и отправляет в **opensearch** в реальном времени.

Возможности **logstash**:

- помогает централизовать данные из логов и метрик;
- выполняет обработку данных;
- формирует нужную пользователю выборку;
- позволяет строить масштабируемые контейнеры для сбора больших объемов разнообразных данных;
- нормализует и отправляет на хранение данные на различные ресурсы;
- обрабатывает все типы данных протоколирования;
- предоставляет фильтры ввода и плагины вывода.

Logstash принимает входные данные из следующих источников:

- STDIN,
- журналы,
- файлы,
- TCP / UDP,
- websocket,
- zeromq.

При наличии большого количества разрозненных данных их отправка напрямую в **opensearch** неудобна, в таких случаях можно использовать предобработку в **logstash**.

При использовании **logstash** на него отправляются данные со всех **beats** и настройки перемещаются в единый центр, где происходит управление, распределение индексов, изменение полей. При большой нагрузке есть возможность вынести **logstash** на отдельную машину.

Конвейер logstash состоит из трёх компонентов — **ввода**, **фильтров** и **вывода**. Таких блоков может быть любое количество.

```
input {
 input_plugin => {...}
 }

 filter {
 filter_plugin => {...}
 }

 output {
 output_plugin => {...}
 }
```

где:

- **input** — получает события из разных источников одновременно, используя коллекцию инструментов ввода с открытым исходным кодом под названием *beats* для сбора событий;
- **filter** — анализирует и обогащает события различными способами, располагает обширной коллекцией фильтров, которые преобразуют события и направляют их на вывод;
- **output** — отправляет отфильтрованные события в одно или несколько мест назначения.

Установка и настройка logstash

Для установки и настройки **logstash** выполните следующий алгоритм действий:

1. Выполните установку **logstash** (потребуются права **администратора**):

```
sudo dnf install logstash
```

2. Откройте для редактирования конфигурационный файл ***pipelines.yml***:

```
nano /etc/logstash/pipelines.yml
```

3. Добавьте следующие настройки:

```
- pipeline.id: main
 path.config: "/etc/logstash/conf.d/*.conf"
```

4. Создайте конфигурационный файл **input.conf**:

```
nano /etc/logstash/conf.d/input.conf
```

5. Добавьте в него следующие настройки:

```
input {
 beats {
 port => 5044
 }
 }
```

6. Создайте конфигурационный файл ***filter.conf***:

```
nano /etc/logstash/conf.d/filter.conf
```

7. Добавьте в него следующие настройки:

```
filter {
 if [type] == "syslog" {
 grok {
 match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%
{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }
 add_field => [ "received_at", "%{@timestamp}" ]
```

```
add_field => [ "received_from", "%{host}" ]
}
date {
match => [ "syslog_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]
}
}
}
```

8. Создайте файл ***output.conf***:

```
nano /etc/logstash/conf.d/output.conf
```

9. Добавьте в него следующие настройки:

```
output {
 opensearch {
 hosts => ["https://localhost:9200"]
 ssl => true
 ssl_certificate_verification => false
 user => "admin"
 password => "custom-admin-password"
 manage_template => false
 index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
 }
 }
```

10. Проверьте конфигурацию **logstash**:

```
sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t /usr/share/logstash/bin/logstash -f
```

Если конфигурация корректна, в ответе команды появится примерно следующее сообщение: Starting server on port: 5044. Если есть ошибки в конфигурации, будут показаны сообщения об ошибках, которые нужно исправить.

11. Добавьте службу **logstash** в автозагрузку:

```
systemctl enable logstash
```

12. Перезапустите службу **logstash**:

```
systemctl restart logstash
```

13. Проверьте статус **logstash**:

```
sudo systemctl status logstash
```

При успешном подключении появится статус: active (running).

Beats

Beats — это легковесные агенты для доставки данных с открытым исходным кодом, располагающиеся на стороне клиента. Их особенность заключается в задействовании небольшого количества ресурсов.

Beats содержит несколько пакетов, являющихся различными модулями системы обработки и анализа данных. Каждый из них предоставляет специальные возможности для сбора и анализа данных, что облегчает создание сквозных решений для анализа логов.

> **Примечание.**
>
> Компоненты **beats** и **logstash** являются взаимодополняемыми и в зависимости от задач можно использовать их либо вместе, либо по отдельности.

Установка и настройка filebeat

Модуль используется для сбора и доставки логов из локальных файлов в систему пользователя для мониторинга и анализа. Filebeat может мониторить различные источники данных, такие как логи приложений, системные журналы, а также JSON- и текстовые файлы.

1. Для установки программы **filebeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install filebeat
```

2. Откройте конфигурационный файл ***filebeat.yml***:

```
nano /etc/filebeat/filebeat.yml
```

3. В настройках укажите путь к файлам, которые необходимо собрать, и адрес, куда отправлять результаты.

В разделе Filebeat inputs включите опцию сбора лога:

```
filebeat.inputs:
 - type: log
 enabled: true
 paths:
 - /var/log/*.log
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

В разделе Logstash Output раскомментируйте следующие строки, вместо localhost укажите IP-адрес сервера:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

где:

- 192.168.2.15 – IP-адрес машины, на которой запущен logstash;
- 5044 – порт, который используется для подключения к logstash.

Сохраните изменения и закройте файл.

4. Активируйте модуль **logstash**:

```
sudo filebeat modules enable logstash
```

5. В файле **/etc/filebeat/modules.d/logstash.yml** измените настройки модуля. Вы должны включить хотя бы один набор файлов в модуле. По умолчанию наборы файлов отключены. Поменяйте значение **enabled: false** на **true**.

```
- module: logstash
  access:
    enabled: true
```

6. Перед запуском **filebeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo filebeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

7. Настройте автозагрузку **filebeat** и запустите службу:

```
sudo systemctl enable --now filebeat
```

8. Проверьте состояние **filebeat** с помощью команды:

```
sudo systemctl status filebeat
```

При успешно выполненных настройках в статусе службы должно отображаться active (running).

Установка и настройка auditbeat

Модуль системы обработки и анализа данных, предназначенный для мониторинга активности пользователей и процессов операционной системы. Он собирает данные об аудите безопасности, такие как журналы аудита, и отправляет их в **opensearch** или **logstash** для анализа и визуализации. **Auditbeat** отправляет эти события в режиме реального времени в opensearch для дальнейшего анализа. Можно следить за изменениями в определенных папках, идентифицировать потенциальные нарушения политики безопасности.

1. Для установки программы **auditbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install auditbeat
```

2. Настройте **auditbeat**:

```
sudo nano /etc/auditbeat/auditbeat.yml
```

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

Сохраните изменения и закройте файл.

3. Перед запуском **auditbeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo auditbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

4. После настройки файла конфигурации необходимо запустить и настроить службу **auditbeat** для автозагрузки:

```
sudo systemctl enable --now auditbeat
```

5. Проверьте состояние **auditbeat** с помощью команды:

```
sudo systemctl status auditbeat
```

При успешно выполненных настройках в статусе должно отображаться active (running).

Установка и настройка heartbeat

Это модуль мониторинга доступности, предназначенный для проверки доступности и производительности служб и ресурсов. Он может мониторить HTTP-эндпоинты, TCP-службы, DNS-серверы и другие ресурсы, отправляя тестовые запросы и анализируя ответы. Heartbeat отслеживает доступность служб с помощью активного поиска. Получив список URL-адресов, **heartbeat** задаёт вопрос о доступности системы и отправляет эту информацию и время отклика в остальную часть стека для дальнейшего анализа.

Для установки программы **heartbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install heartbeat
```

1. Откройте конфигурационный файл ***heartbeat.yml***:

```
sudo nano /etc/heartbeat/heartbeat.yml
```

2. Настройте параметры в файле ***heartbeat.yml*** в соответствии с примером:

Включите монитор, который необходимо использовать.

```
heartbeat.monitors:
 - type: http
 urls: ["https://192.168.2.15:9200"]
 schedule: '@every 60s'
 id: dashboards
 name: 'Opensearch Dashboards'
 username: "admin"
 password: "custom-admin-password"
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

Сохраните изменения и закройте файл.

В этом примере файл ***heartbeat.yml*** настраивает параметры мониторинга и управления кластером из двух узлов с использованием **heartbeat** для обеспечения высокой доступности. В случае неисправности одного из узлов, другой узел возьмёт на себя его роль.

Перед запуском **heartbeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo heartbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

3. После настройки файла конфигурации необходимо запустить и настроить службу **heartbeat** для автозагрузки:

```
sudo systemctl enable --now heartbeat-elastic
```

4. Проверьте состояние **heartbeat** с помощью команды:

```
sudo systemctl status heartbeat-elastic
```

При успешно выполненных настройках в статусе должно отображаться active (running).

Установка и настройка metricbeat

Metricbeat — это модуль сбора метрик, предназначенный для сбора различных системных метрик и сервисной статистики. Он может собирать данные о производительности хостов, сетевого трафика, использования ресурсов контейнеров и многого другого. Применяется для мониторинга серверов/приложений.

Для установки программы **metricbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install metricbeat
```

Для настройки **metricbeat** выполните следующий алгоритм действий:

1. Откройте основной файл конфигурации ***/etc/metricbeat/metricbeat.yml*** для редактирования:

```
sudo nano /etc/metricbeat/metricbeat.yml
```

2. Измените настройки.

В разделе Modules configuration измените значение параметра reload.enabled на true.

```
metricbeat.config.modules:
 path: ${path.config}/modules.d/*.yml
 reload.enabled: true
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

Сохраните изменения и закройте файл.

3. Откройте на редактирование конфигурационный файл ***metricbeat.reference.yml***:

```
sudo nano /etc/metricbeat/metricbeat.reference.yml
```

4. Заполните конфигурационный файл и сохраните настройки.

```
metricbeat.config.modules:
 path: ${path.config}/modules.d/*.yml
 reload.period: 10s

 reload.enabled: true
 metricbeat.max_start_delay: 10s

 metricbeat.modules:
 - module: system
 metricsets:
 - cpu
 - load
 - memory
 - network
 - process
 - process_summary
 - uptime
 - socket_summary
 enabled: true
 period: 10s
 processes: ['.*']
```

5. Перед запуском **metricbeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo metricbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

6. После настройки файла конфигурации, необходимо запустить и активировать автозагрузку **metricbeat**:

```
sudo systemctl enable --now metricbeat
```

7. Проверьте статус **metricbeat**:

```
sudo systemctl status metricbeat
```

При успешно выполненных настройках в статусе должно отображаться active (running).

8. Для просмотра всех модулей выполните команду:

```
metricbeat modules list
```

9. Активируйте нужные модули:

```
metricbeat modules enable logstash
```

Установка и настройка packetbeat

Packetbeat — модуль для сбора метрик, предназначенный для мониторинга и анализа сетевого трафика протоколов уровня приложений в реальном времени. **Packetbeat** может анализировать различные протоколы, такие как HTTP, DNS, MySQL и другие службы, а также обнаруживать аномалии и атаки в сети. Мониторинг сетевого трафика имеет важное значение для управления инфраструктурой, обеспечивая высокий уровень производительности и безопасности.

На клиентской машине нужно настроить агент-отправитель. После сбора и обработки данных с хостов и контейнеров агент отправляет сгенерированные отчеты в **logstash** или **opensearch**.

Для установки программы **packetbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install packetbeat
```

После установки **packetbeat** нужно настроить. Основной файл конфигурации ***packetbeat.yml*** находится в каталоге ***/etc/packetbeat/***. Откройте его для редактирования:

```
sudo nano /etc/packetbeat/packetbeat.yml
```

Настройте сетевые интерфейсы, которые **packetbeat** будет использовать для мониторинга трафика, например:

```
packetbeat.interfaces.device: any
```

где:

any — означает мониторинг всех доступных интерфейсов. Можно указать конкретный интерфейс, например eth0.

Включите и настройте протоколы, которые **packetbeat** будет анализировать. Например:

```
packetbeat.protocols:
 - type: http
 ports: [80, 8080, 8000, 5000, 8002]
 - type: mysql
 ports: [3306]
 - type: dns
 ports: [53]
 - type: redis
 ports: [6379]
```

Этот пример включает анализ HTTP, MySQL, DNS и Redis трафика на указанных портах.

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

Сохраните изменения и закройте файл.

Перед запуском packetbeat рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo packetbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

После настройки файла конфигурации, необходимо запустить и настроить службу **packetbeat** для автозагрузки:

```
sudo systemctl enable --now packetbeat
```

Проверьте статус **packetbeat**:

```
sudo systemctl status packetbeat
```

При успешно выполненных настройках в статусе должно отображаться active (running).

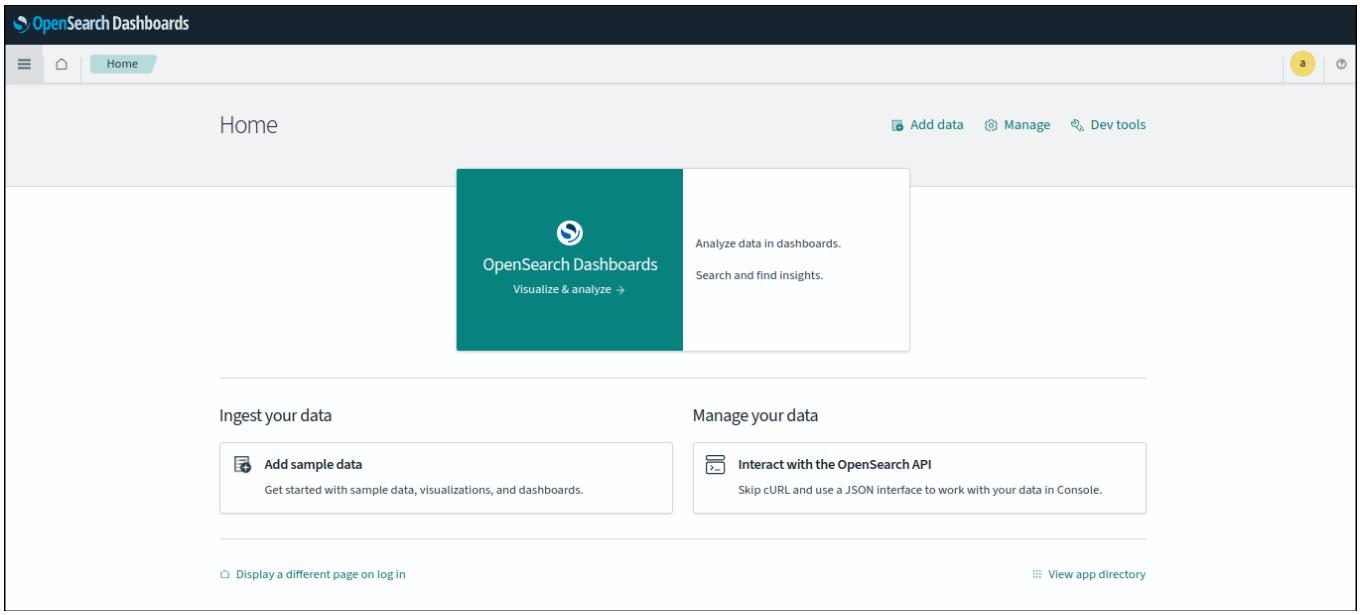
Отображение данных в OpenSearch Dashboards

Для просмотра данных в веб-панели **OpenSearch Dashboards** подключитесь через веб-браузер, используя IP-адрес машины, на которой развернут **logstash**:

```
http://192.168.2.15:5601
```

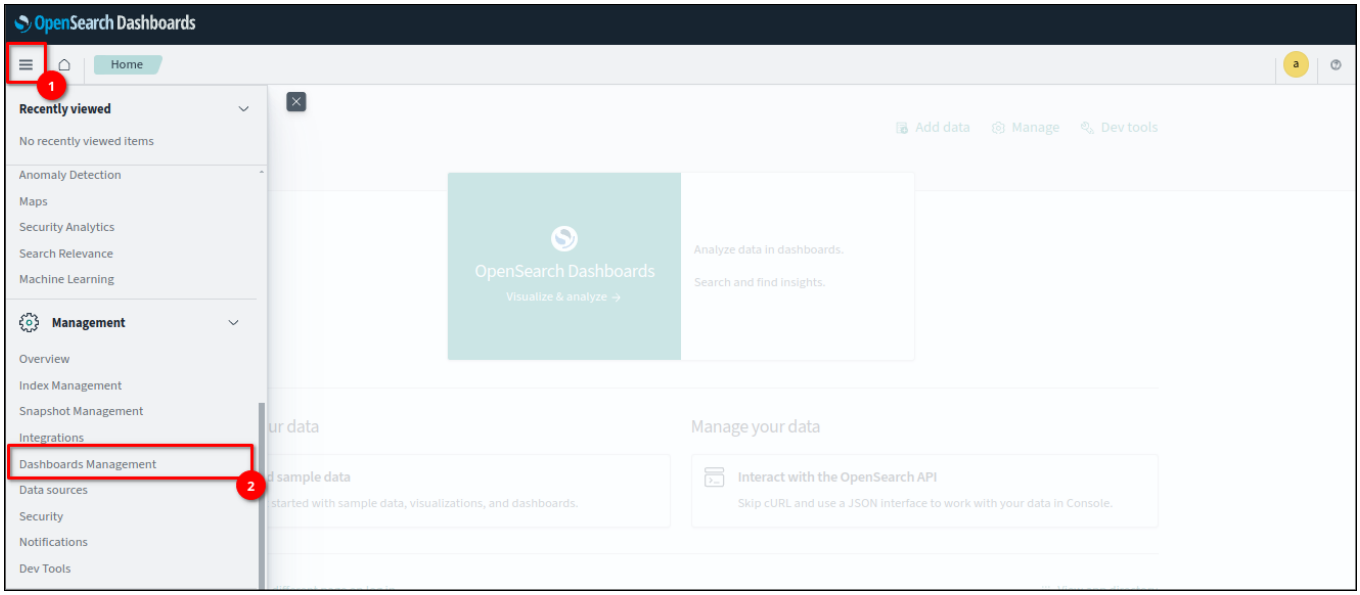


Введите аутентификационные данные, созданные при установке **opensearch**.

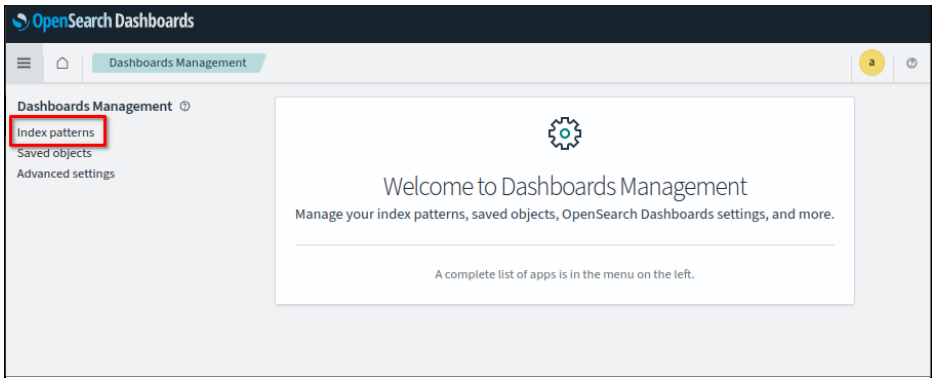


Создание шаблона индексов

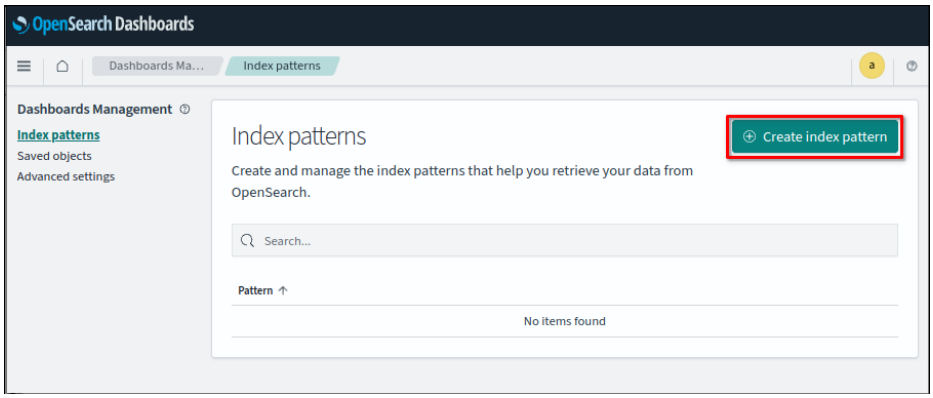
Для осуществления поиска данных с помощью **OpenSearch Dashboards** необходимо создать шаблон индексов. Перейдите в «**Основное меню**» (1) — «**Dashboards Management**» (2).



Выберите «**Index Pattern**».

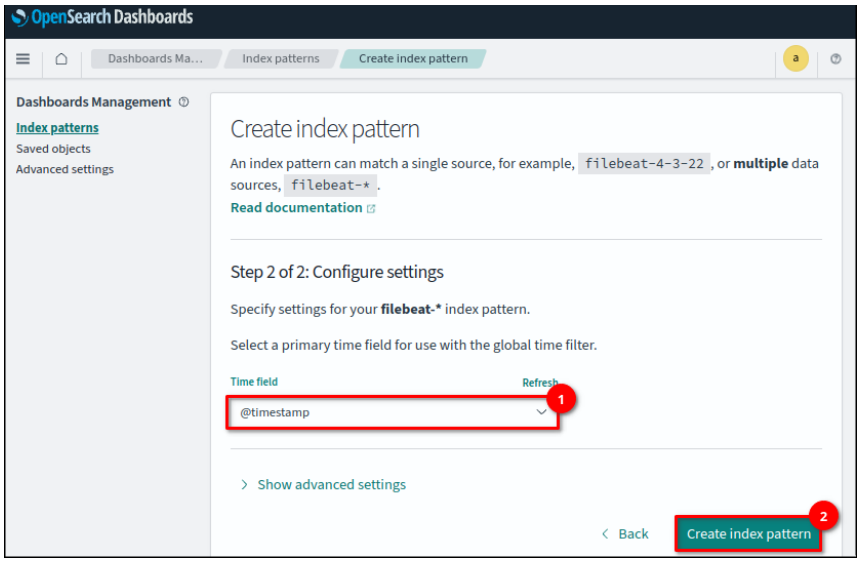


Нажмите кнопку «**Create index pattern**».



В поле «**Index pattern name**» (1) введите имя индекса «**filebeat-***» и нажмите «**Next step**» (2).

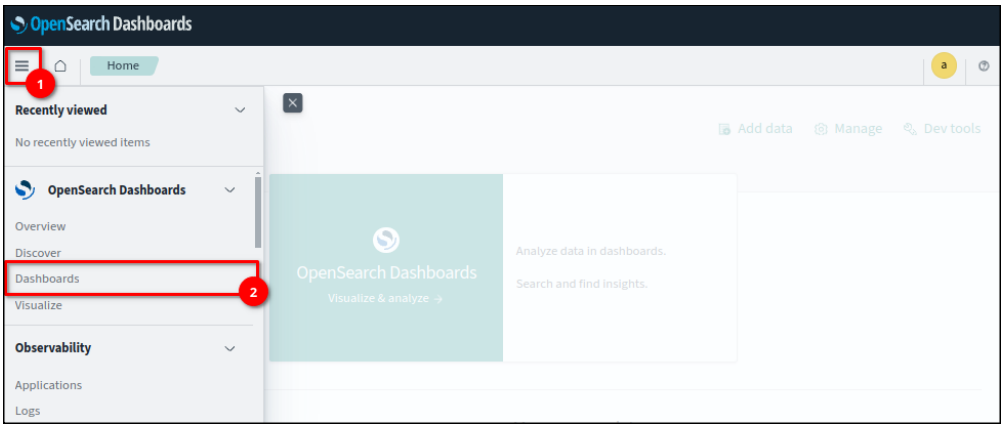
В поле «**Time field**» выберите значение «**@timestamp**» (1) и нажмите «**Create index pattern**» (2).



Аналогичным образом создаются индексы для **auditbeat-***, **heartbeat-***, **metricbeat-***, **packetbeat-*.**

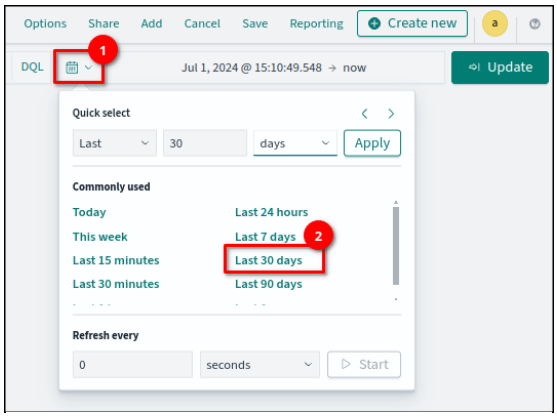
Создание информационной панели OpenSearch Dashboards

Для отображения данных в **OpenSearch Dashboards** необходимо создать информационную панель. Для этого перейдите в «**Основное меню**» (1) — «**Dashboards**» (2).

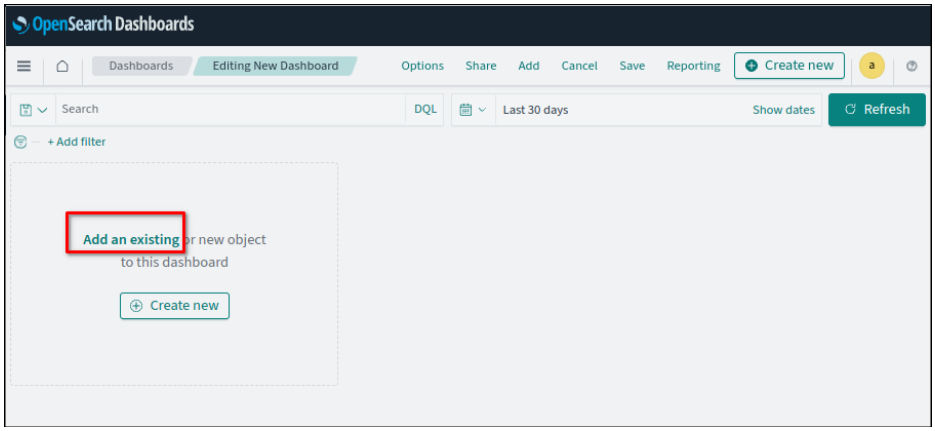


На панели «**Dashboards**» выберите «**Create**» — «**Dashboards**».

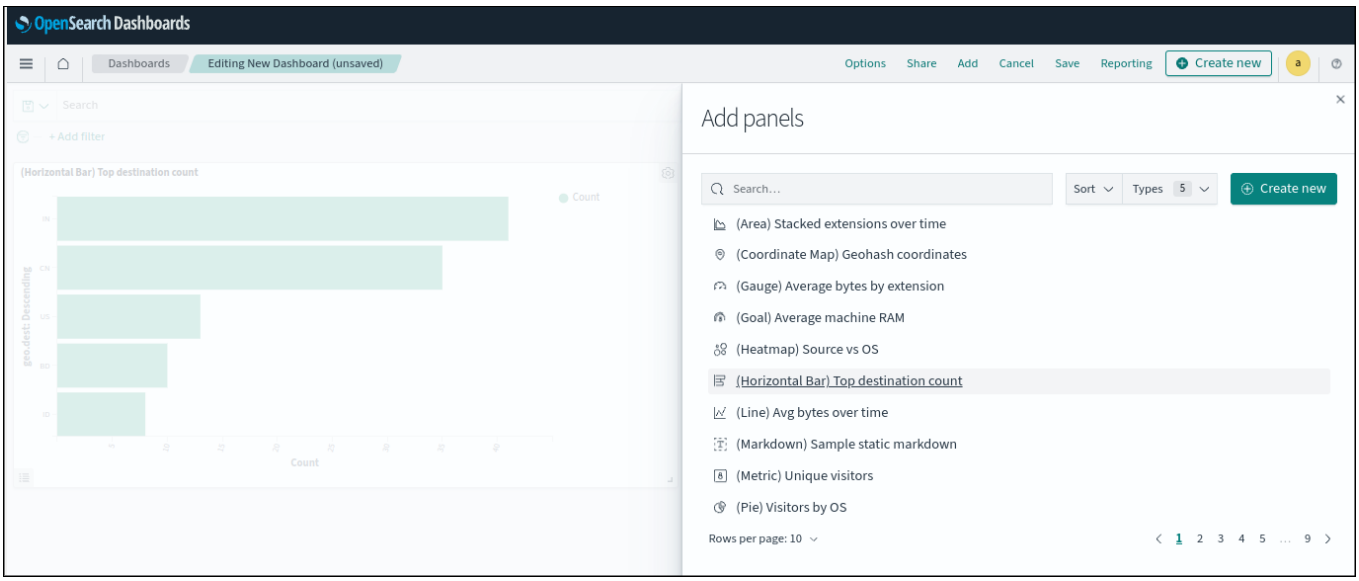
Выберите значок календаря и установите временной фильтр, например, 30 дней.



Выберите на панели «**Add an existing**» для добавления существующего объекта.



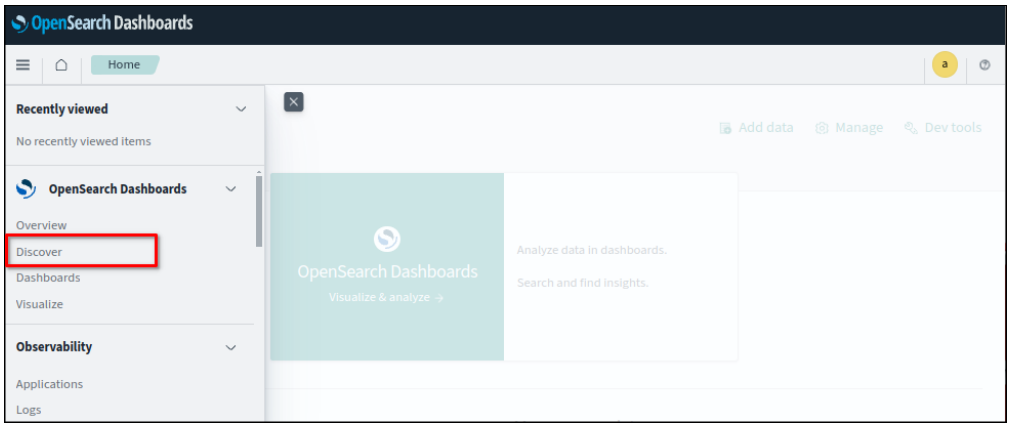
В окне **«Add panels»** выберите необходимую панель, а затем закройте панель. В результате будет создана базовая панель для мониторинга.



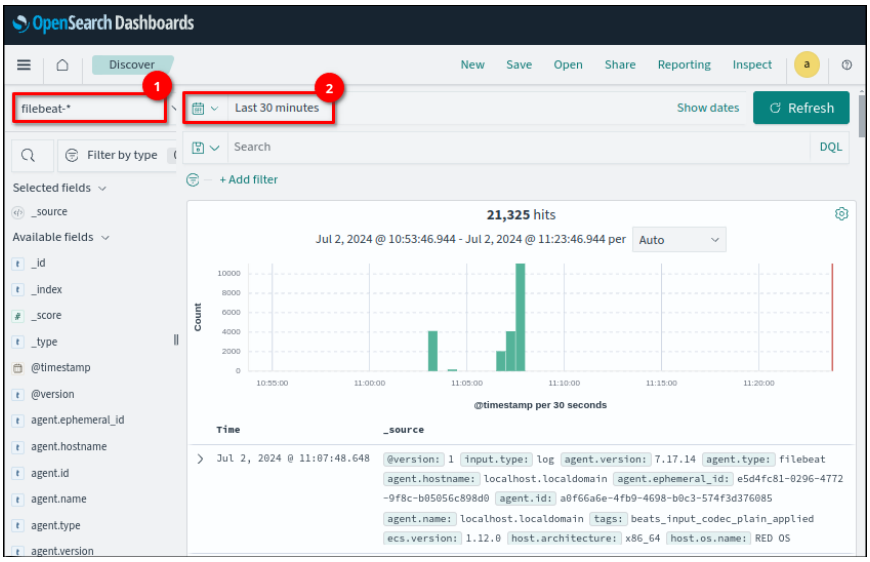
Использование Discover

С помощью раздела **Discover** можно выбирать данные для анализа, устанавливать временной диапазон для этих данных, выполнять поиск с помощью языка запросов Dashboards и фильтровать результаты.

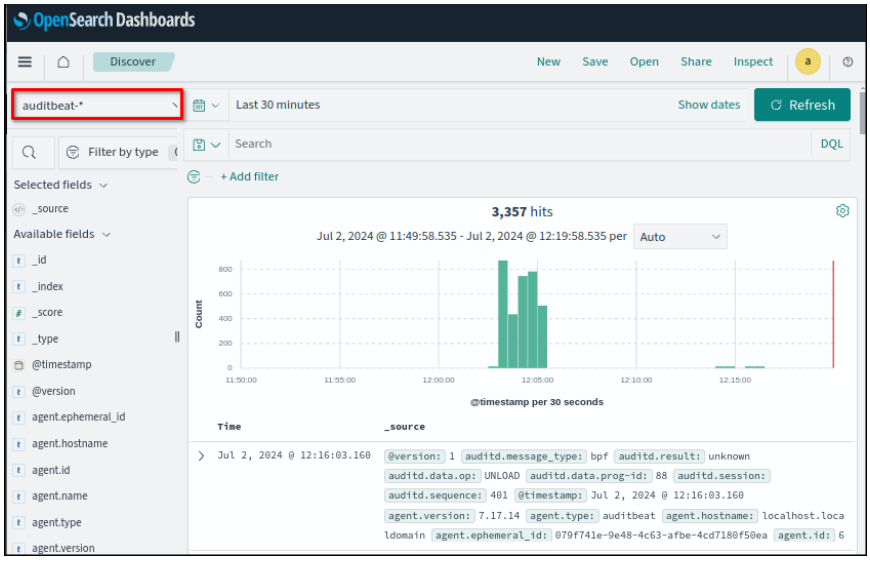
В навигационном меню **OpenSearch Dashboards** выберите раздел «**Discover**».



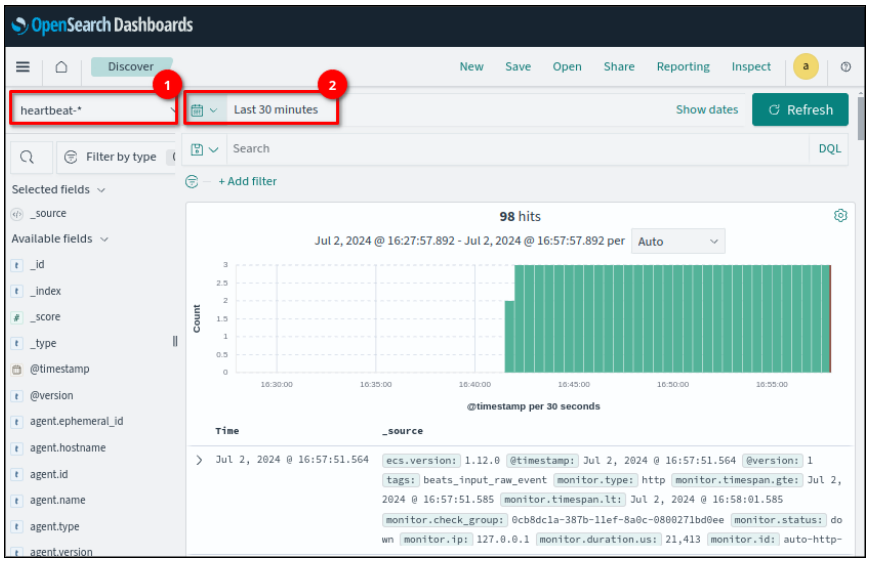
На странице **Discover** выберите шаблон индекса «**filebeat-***» (1) из выпадающего меню в левом верхнем углу. Выберите значок для изменения временного фильтра и установите значение «**Last 30 minutes**» (2).



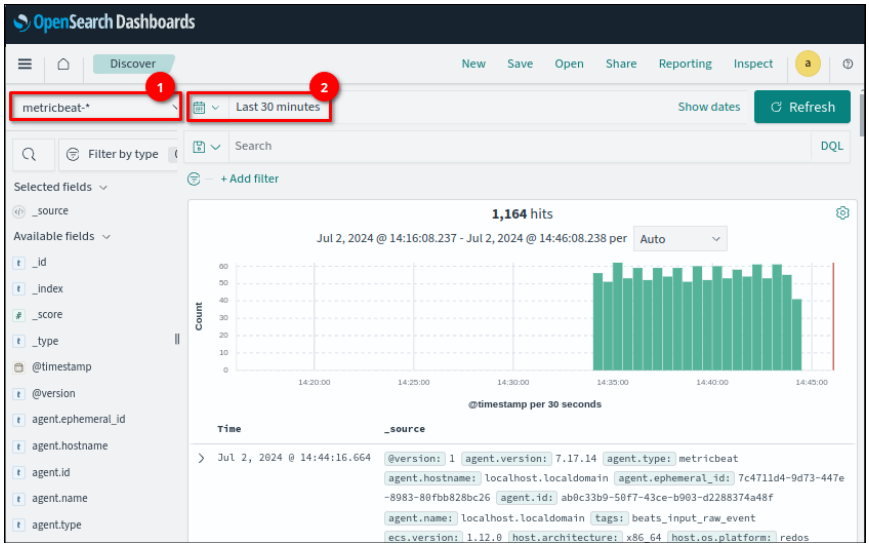
Результат для индекса «**auditbeat-***»:



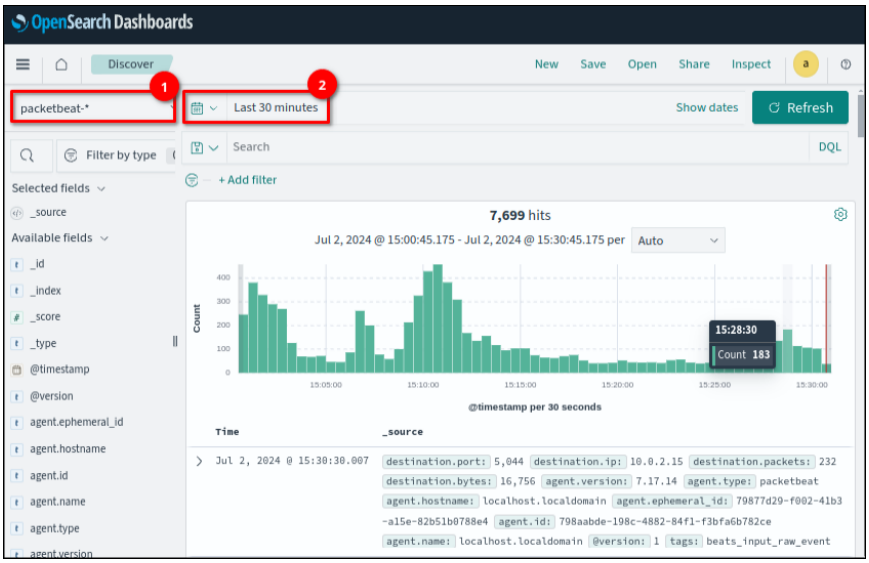
Результат для индекса «**heartbeat-***»:



Результат для индекса «**metricbeat-***»:



Результат для индекса «**packetbeat-***»:



Graylog — инструмент для централизированного сбора, хранения и анализа системных журналов

Установка Java 17
Установка MongoDB
Установка и настройка OpenSearch
Установка и настройка Graylog

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: graylog-server-5.2.9, java-17-openjdk-17.0.10, mongodb-org-7.0.8, opensearch-2.14.0

Graylog — это платформа для централизованного сбора, хранения, фильтрации, анализа и визуализации логов, которая помогает организациям получать ценные инсайты из своих данных.

Graylog предоставляет удобный интерфейс для работы с логами, позволяя администраторам и аналитикам быстро находить и устранять проблемы, а также отслеживать активность в реальном времени. Благодаря поддержке различных источников данных и гибким возможностям настройки **graylog** становится незаменимым инструментом для обеспечения безопасности и стабильности ИТ-инфраструктуры.

Graylog требует установки и настройки нескольких компонентов для полноценной работы.

1 . **Java 17** — обеспечивает совместимость и стабильность работы **graylog** (рекомендуется использовать последнюю стабильную версию для обеспечения безопасности и производительности).

2. **MongoDB** — база данных, которая используется **graylog** для хранения конфигурационных данных и метаданных.

3 . **OpenSearch** — поисковая и аналитическая система, которая позволяет обрабатывать большие объёмы данных, предоставляя обширные возможности для поиска и анализа логов.

4. **Сервер Graylog** — основной компонент, который собирает, обрабатывает и визуализирует логи.

Каждый из компонентов выполняет свою роль в общей системе управления логами.

Установка Java 17

Для установки **java-17** выполните следующие шаги:

1. Установите java-17, выполнив в терминале команду (потребуются права **администратора**):

```
sudo dnf install java-17-openjdk
```

2. Выберите версию по умолчанию 17:

```
update-alternatives --config java
```

Установка MongoDB

Для установки **mongodb** выполните следующий алгоритм действий:

1. Установите **mongodb**:

```
sudo dnf install mongodb-org
```

2. Перезагрузите конфигурацию системных служб:

```
sudo systemctl daemon-reload
```

3. Добавьте службу **mongod** в автозагрузку:

```
sudo systemctl enable mongod --now
```

4. Проверьте статус службы **mongod**:

```
sudo systemctl status mongod
```

В статусе должно отображаться active (running).

Установка и настройка OpenSearch

Для установки **opensearch** выполните следующий алгоритм действий:

1. Для установки **opensearch** необходимо определить собственный пароль администратора, чтобы настроить демонстрационную конфигурацию безопасности.

```
sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=<пароль> dnf install opensearch
```

где:

`<пароль>` — установите пароль администратора длиной от 12 символов, содержащий прописные буквы, строчные буквы, спецсимволы, цифры.

2. Настройки **opensearch** находятся в файле **/etc/opensearch/opensearch.yml**. Внесите изменения в конфигурационный файл:

```
sudo nano /etc/opensearch/opensearch.yml
```

3. Добавьте следующие строки:

```
cluster.name: graylog
 node.name: ${HOSTNAME}
 path.data: /var/lib/opensearch
 path.logs: /var/log/opensearch
 discovery.type: single-node
 network.host: 0.0.0.0
 action.auto_create_index: false
 plugins.security.disabled: true
```

4. Установите значение параметра виртуальной памяти vm.max_map_count:

```
sudo sysctl -w vm.max_map_count=262144
```

5. Добавьте параметр в файл конфигурации:

```
sudo echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

6. Перезагрузите конфигурацию системных служб, чтобы применить изменения:

```
sudo systemctl daemon-reload
```

7. Включите opensearch для автоматического запуска при загрузке системы:

```
sudo systemctl enable opensearch --now
```

8. Проверьте статус opensearch, чтобы убедиться, что он запущен и работает корректно:

```
sudo systemctl status opensearch
```

При успешно выполненных настройках в статусе должно отображаться active (running).

Установка и настройка Graylog

Для установки и настройки **graylog** выполните следующий алгоритм действий:

1. Установите **graylog**:

```
sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.rpm
```

2. Установите graylog-server:

```
sudo dnf install graylog-server
```

3. Создайте пароли для двух переменных **password_secret** и **root_password_sha2.** Без указанных переменных **graylog** не сможет запуститься.

Создайте хеш пароля администратора **graylog**. Используйте следующую команду, чтобы сгенерировать хеш для введенного `<пароля>`:

```
echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
```

Введите пароль:

```
Enter Password: <пароль>
```

В терминале отобразится хеш пароля:

```
<хеш_пароля>
```

Создайте секретный ключ password_secret:

```
< /dev/urandom tr -dc A-Z-a-z-0-9 | head -c${1:-96};echo;
```

В терминале отобразится секретный ключ:

```
<секретный_ключ>
```

Скопируйте полученные значения `<хеш_пароля>` и `<секретный_ключ>`.

4. Откройте конфигурационный файл **/etc/graylog/server/server.conf** на редактирование:

```
sudo nano /etc/graylog/server/server.conf
```

5. Измените следующие строки:

```
root_password_sha2 = <хеш_пароля>
 password_secret = <секретный_ключ>
 elasticsearch_hosts = http://localhost:9200
```

6. Перезагрузите конфигурацию системных служб:

```
sudo systemctl daemon-reload
```

7. Включение **graylog** для автоматического запуска:

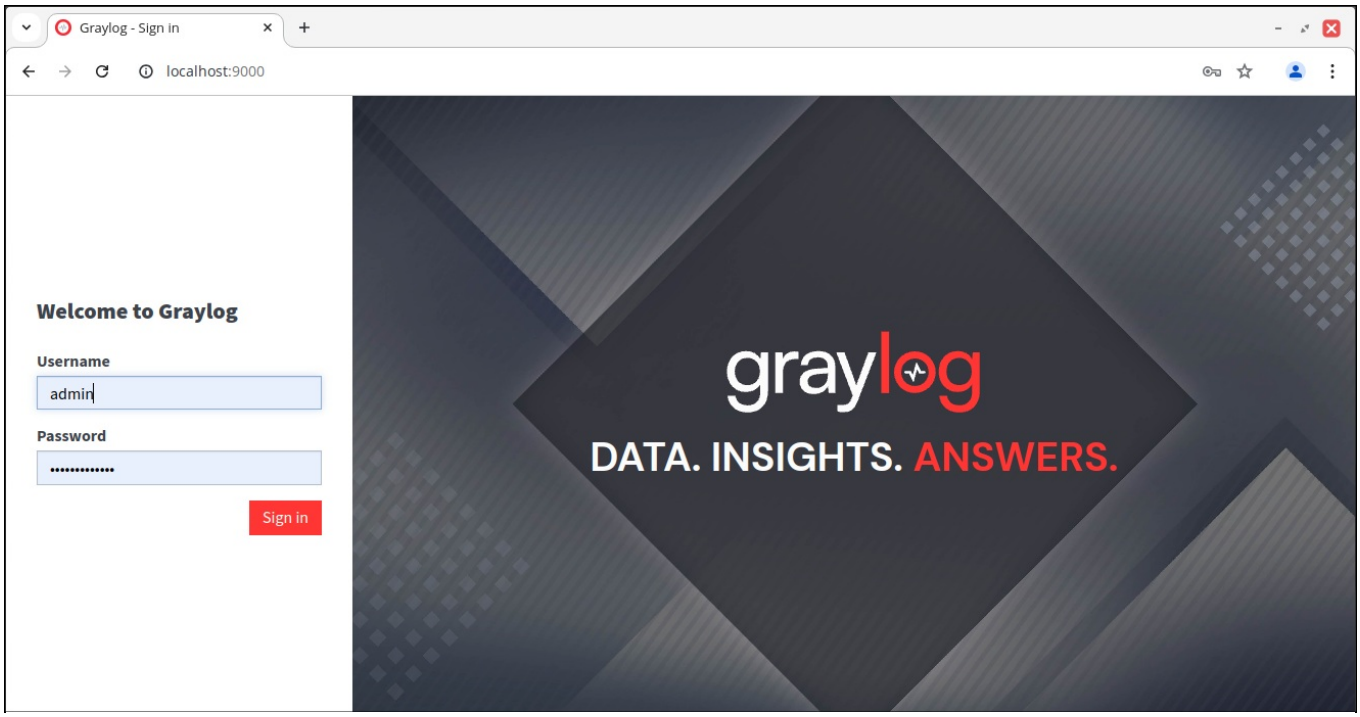
```
sudo systemctl enable graylog-server --now
```

8. Проверьте статус **graylog**:

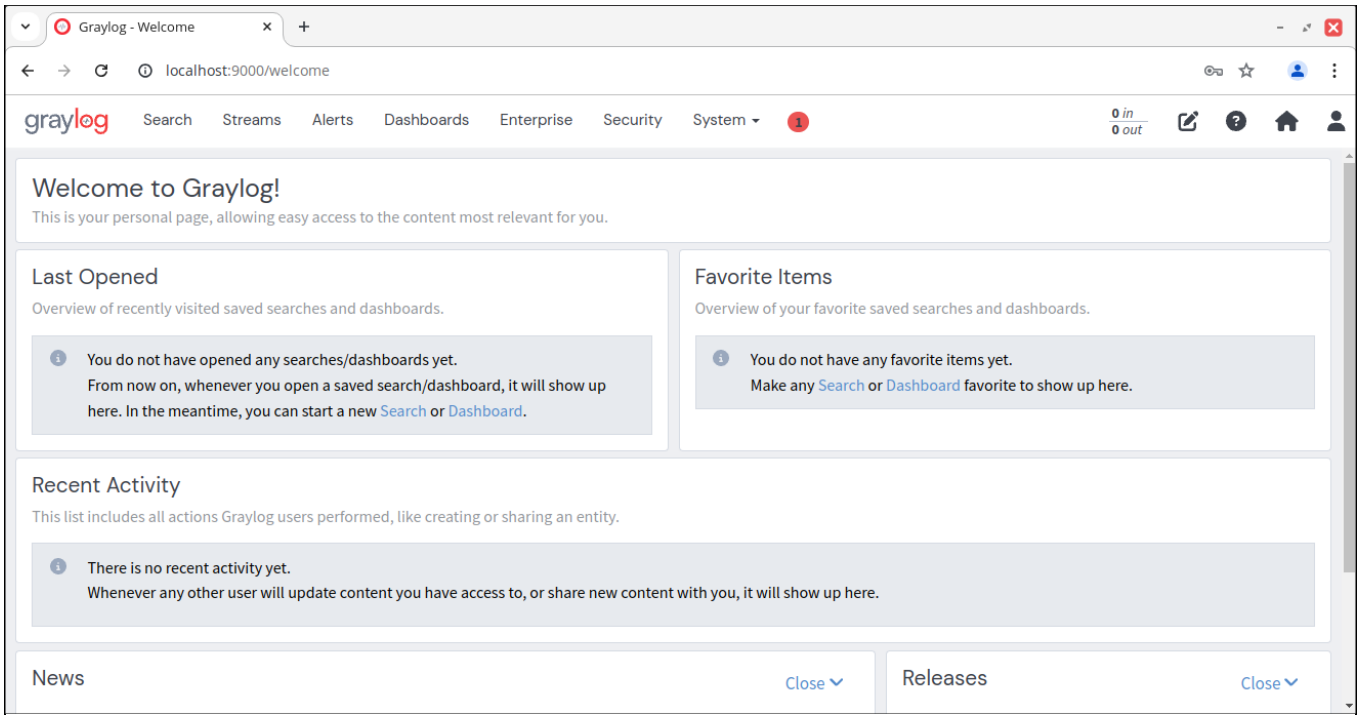
```
sudo systemctl --type=service --state=active | grep graylog
```

В случае успешного запуска сервера **graylog** в терминале отобразится сообщение: **loaded active running Graylog server**. Это означает, что сервер **Graylog** успешно запущен и работает.

9. Перейдите по адресу **http://localhost:9000** и войдите под учетной записью `admin: <пароль>`.



После входа в учетную запись отобразится веб-интерфейс **Graylog**. В этом интерфейсе можно управлять настройками **Graylog**, просматривать и анализировать логи, настраивать потоки данных, создавать дашборды и выполнять другие действия, связанные с мониторингом и анализом логов.



Создание резервных копий с помощью утилиты cp

Для создания резервных копий важных файлов пользователь может использовать команду **cp**.

cp — команда, предназначенная для копирования файлов из одного в другие каталоги (возможно, с другой файловой системой). Исходный файл остаётся неизменным, имя созданного файла может быть таким же, как у исходного, или изменится.

Чтобы скопировать файл

```
cp [ -f ] [ -h ] [ -i ] [ -p ][ -- ] исходный_файл целевой_файл
```

Чтобы скопировать файл или файлы в другой каталог

```
cp [-R] [-H | -L | -P] [-f | -i] [-pv] исходный_файл ... целевая_директория
```

Чтобы скопировать каталог в другой каталог (должен быть использован флаг -r или -R)

```
cp [ -f ] [ -h ] [ -i ] [ -p ] [ -- ] { -r | -R } исходная_директория ... целевая_директория
```

Опции команды:

- **-R, -r, --recursive (recursive)** — копировать директории рекурсивно (то есть все поддиректории и все файлы в поддиректориях).
- **-f (force)** — разрешает удаление целевого файла, в который производится копирование, если он не может быть открыт для записи.
- **-H** — используйте этот ключ, чтобы копировать символические ссылки. По умолчанию команда переходит по символическим ссылкам и копирует файлы, на которые те указывают.
- **-i (interactive)** — команда будет запрашивать, следует ли перезаписывать конечный файл, имя которого совпадает с именем исходного, то есть если в параметре целевой_каталог или целевой_файл встречается такое же имя файла, какое было задано в параметре исходный_файл или исходная_директория, то запрашивается подтверждение. Для того, чтобы перезаписать файл, следует ввести у или его эквивалент для данной локали. Ввод любого другого символа приведёт к отмене перезаписи данного файла.
- **-n, --no-clobber** — не перезаписывать существующий файл (отменяет предыдущий параметр -i).
- **-v, --verbose** — выводит имя каждого файла перед его копированием.
- **-p (preserve)** — повторяет следующие свойства исходного файла или директории у целевого файла или директории:
  - время последнего изменения и последнего доступа,
  - идентификатор пользователя и группы,
  - права доступа и биты SUID и SGID.

Создание резервных копий с помощью утилиты fsbackup

Создание файла конфигурации для резервного копирования
Скрипт создания бэкапа
Скрипт полного восстановления из бэкапа
Создание резервной копии
Восстановление резервной копии
Добавление/удаление директорий в резервной копии
Автоматизированное создание резервных копий

FSBACKUP - утилита для создания инкрементного или полного бэкапа отдельных файлов или целой файловой системы.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fsbackup
```

После установки программа будет находиться по пути **/usr/local/fsbackup/**.

Примеры конфигурационных файлов и документация расположены в каталоге **/usr/share/doc/fsbackup/**.

Создание файла конфигурации для резервного копирования

В конфигурационном файле перечислены настройки, которые используются во время процесса резервного копирования, а также необходимые файлы или директории, которые впоследствии будут сохранены в резервной копии.

Скопируйте пример конфигурационного файла и отредактируйте его. Таким образом можно создавать столько конфигураций резервного копирования, сколько требуется.

ВАЖНО!

Обратите внимание, что каждый конфигурационный файл должен иметь **уникальное имя**, отличающееся от других конфигурационных файлов, а также отдельный **СУЩЕСТВУЮЩИЙ** на момент запуска процесса бэкапа каталог сохранения резервной копии.

```
cp /usr/share/doc/fsbackup/cfg_example /usr/local/fsbackup/<имя_конфигурационного_файла>
nano /usr/local/fsbackup/<имя_конфигурационного_файла>
```

В скопированном примере конфигурационного файла все поля имеют пояснения на русском языке. Далее приведены обязательные настройки, которые необходимо отредактировать:

- **$cfg_backup_name** - имя файла бэкапа;
- **$cfg_save_old_backup** - сохранение старого бэкапа. По умолчанию старая копия помещается в папку OLD внутри директории бэкапа;
- **$cfg_backup_style** - выбор метода бэкапа. По умолчанию установлен инкрементный бэкап;
- **$cfg_local_path** - директория хранения бэкапа;
- **$cfg_cache_dir** - директория хранения хэша бэкапа. Не должна совпадать с директорией хранения самого бэкапа;
- **__DATA__** - пути к файлам и директориям, которые необходимо занести в бэкап.

Для наглядности создадим еще один конфигурационный файл для папок пользователей:

```
cp /usr/local/fsbackup/cfg_example /usr/local/fsbackup/cfg_users
nano /usr/local/fsbackup/cfg_users
```

Отредактируем необходимые поля.

```
$cfg_backup_name = "users";       # имя бэкапа
 $cfg_save_old_backup = 0;         # не сохранять бэкап
 $cfg_backup_style = "full_backup"; # создание полного бэкапа
 $cfg_local_path = "/mnt/personal"; # директория создания бэкапов
 $cfg_cache_dir = "/srv/cache";     # директория для помещения текущих хэшей
```

```
# Список файлов и условий для помещения в бэкап
__DATA__
/srv/user1
/srv/user2
```

Скрипт создания бэкапа

Далее отредактируйте скрипт создания бэкапа. Создайте для каждого конфигурационного файла свой файл создания бэкапа путем копирования исходного скрипта. Данный файл также имеет пояснения на русском языке.

```
cp /usr/local/fsbackup/create_backup.sh /usr/local/fsbackup/create_backup_users.sh
```

Отредактируйте необходимые параметры:

```
nano /usr/local/fsbackup/create_backup_users.sh
```

Самым главным параметром является **config_files**, в котором перечислены необходимые конфигурационные файлы.

```
config_files="cfg_users"      # укажите необходимые конфигурации файлы для создания по ним бэкапа
```

ВАЖНО!

Перед запуском бэкапа убедитесь, что скрипт запуска и конфигурационный файл расположены в одной папке вместе perl-скриптом **fsbackup.pl**.

Скрипт полного восстановления из бэкапа

Для полного восстановления скопируйте и отредактируйте скрипт **fsrestore.sh**, расположенный в каталоге **usr/local/fsbackup/scripts/**.

```
cp /usr/local/fsbackup/scripts/fsrestore.sh /usr/local/fsbackup/scripts/fsrestore_users.sh
nano /usr/local/fsbackup/scripts/fsrestore_users.sh
```

```
backup_name="users"           # имя бэкапа
 backup_path="/mnt/personal/"   # директория где находится бэкап
 restore_path="/ "             # корневая директория куда будут помещены данные, установите /, т.к распаковка происходит с полными
путями
```

Для каждой конфигурации создайте свой скрипт восстановления аналогичным образом.

Создание резервной копии

Дополнить архив новыми файлами или создать бэкап:

```
/usr/local/fsbackup/create_backup_users.sh
```

Восстановление резервной копии

Для восстановления отдельных файлов из бэкапа воспользуйтесь утилитой **tar**.

- **tar -tf <имя архива>** - просмотр директорий в архиве без его распаковки.
- **tar -xf <имя архива> <имя файла> <имя файла> -** разархивирование одного или нескольких файлов.

В текущем примере архив бэкапа находится по пути **/mnt/personal**.

После распаковки переместите извлеченный файл в нужный каталог.

Чтобы восстановить все файлы из бэкапа, воспользуйтесь ранее созданным скриптом **fsrestore_<...>.sh**. Помните, что файлы, созданные после процедуры бэкапа, останутся, а удаленные или измененные файлы вернутся в исходное состояние. В текущем примере скрипт восстановления назван **fsrestore_users.sh**

```
/usr/local/fsbackup/scripts/fsrestore_users.sh
```

Добавление/удаление директорий в резервной копии

Для добавления новых директорий в бэкап отредактируйте файл его создания.

Например, добавим пользователя **user3** в бэкап **users**. Для этого добавим папку с данными **user3** в конец секции **__DATA__**. Для удаления директорий из бэкапа удалите путь к директории из файла.

```
nano /usr/local/fsbackup/create_backup_users.sh
```

```
... __DATA__
 /srv/user1
 /srv/user2
 /srv/user3
```

Теперь каталоги трех пользователей будут добавляться в бэкап **users**.

Автоматизированное создание резервных копий

Для автоматизации можно использовать **cron**. Отредактируйте файл **/etc/crontab** с помощью текстового редактора:

```
nano /etc/crontab
```

Или специальной команды:

```
crontab -e
```

Например, для создания еженедельного бэкапа общего каталога пользователей в 23:30 по субботам впишите следующую строку в конец файла:

```
30 23 * * 6 root /usr/local/fsbackup/create_backup_users.sh
```

Подробную информацию о службе **cron** см. здесь.

Начало работы

Введение

fwbackups - многофункциональная программа для резервного копирования пользователей, которая позволяет вам легко создавать резервные копии ваших документов в любое время. Её простой, интуитивно понятный интерфейс предлагает следующие функции:

- каждый пользователь системы может настроить собственные резервные копии;
- по требованию или автоматическое резервное копирование файлов и папок с помощью наборов резервных копий;
- значок в трее, чтобы отслеживать текущий ход операций резервного копирования или восстановления;
- несколько резервных копий, включая сжатие и инкрементное резервное копирование;
- поддержка резервного копирования на удаленный хост через ssh / sftp;
- поддержка восстановления любых резервных копий.

Вы можете подробнее ознакомиться с работой утилиты **fwbackups**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с графической утилитой Fwbackups;
- в **Яндекс.Дзен** — Работа с графической утилитой Fwbackups;
- в **VK Видео** — Работа с графической утилитой Fwbackups.

На наших каналах вы также сможете найти много другой полезной информации.

Запуск fwbackups

Сначала установим программу.

```
dnf install fwbackups
```

Существует два способа запуска fwbackups:

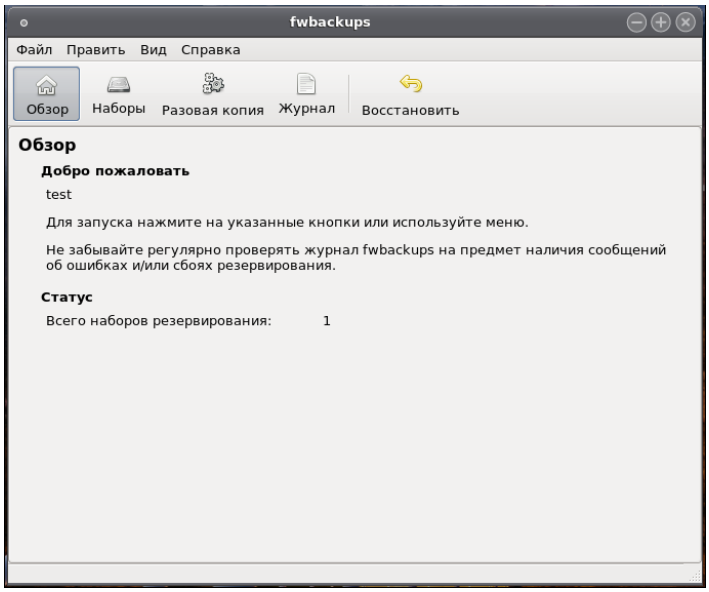
1. Графический (рекомендуется для большинства пользователей):

Выберите «**Приложения**» → «**Системные**» → «**fwbackups**» в меню;

2. Из интерфейса командной строки:

Запустите терминал, введите, **fwbackups** а затем нажмите клавишу «Enter» .

> Доступны дополнительные опции! Введите **fwbackups --help** все доступные параметры и их описания.



fwbackups открывает страницу «Обзор». Чтобы начать использовать **fwbackups**, просто нажмите одну из кнопок панели инструментов, чтобы переключать страницы.

Наборы

Создавайте, редактируйте или удаляйте наборы резервных копий, а также вручную запускайте заданную резервную копию.

Разовая копия

Выполнять «одноразовые» резервные копии (резервные копии, которые *не* планируется выполнять периодически).

Журнал

Отображает файл журнала, отображающий информацию о действиях **fwbackups** .

- Все сообщения журнала отформатированы следующим образом: *Month DD HH: MM: SS :: severity: message;*
- Сообщения из предыдущих сеансов отображаются фиолетовым цветом;
- Сообщения из текущего сеанса отображаются синим цветом;
- Ошибки и предупреждения отображаются красным и желтым цветом соответственно.

Восстановить

Позволяет восстановить любую резервную копию, которую вы ранее сделали с помощью **fwbackups**.

Использование fwbackups

Типы резервного копирования

fwbackups поддерживает два основных типа резервных копий: повторяющиеся резервные копии, которые автоматически резервируют ваши файлы по расписанию, и резервные копии, которые запускаются один раз и не запланированы снова. Они называются *резервными наборами* и *одноразовыми резервными копиями* соответственно.

Вы можете подробнее ознакомиться с работой утилиты **fwbackups**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с графической утилитой Fwbackups;
- в **Яндекс.Дзен** — Работа с графической утилитой Fwbackups;
- в **VK Видео** — Работа с графической утилитой Fwbackups.

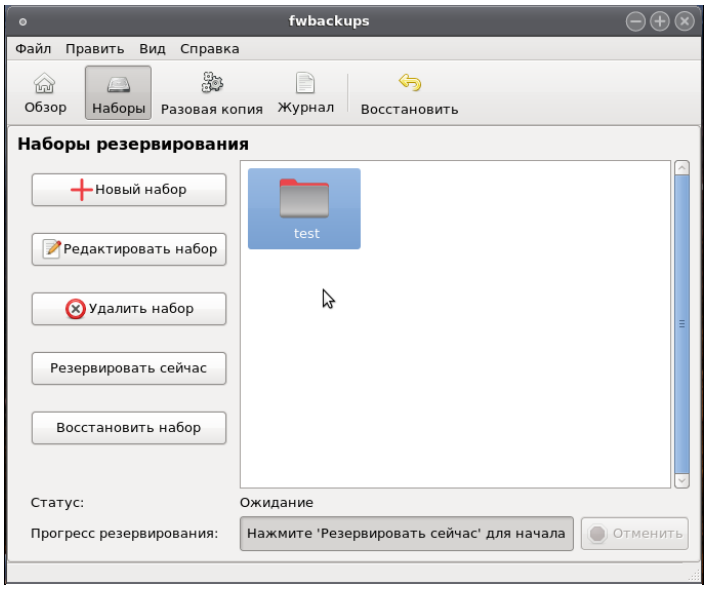
На наших каналах вы также сможете найти много другой полезной информации.

Вы сможете настроить любое количество наборов резервных копий, каждый из которых будет выполняться по регулярному графику в любое время по вашему выбору. Каждый набор работает независимо, поэтому, вы можете группировать файлы на два или более набора и производить их резервное копирование в разное время или в разные папки назначения. Вы также можете выполнять одноразовые операции, однако в этом случае резервное копирование не будет запланировано для запуска в будущем.

Когда использовать резервные наборы или одноразовые резервные копии

> Рекомендуется создать регулярные резервные копии для важных файлов, чтобы обеспечить сохранение резервной копии регулярно. Одноразовые резервные копии более подходят для создания резервных копий больших файлов, таких как музыкальная коллекция или видео, которые вы не хотите включать в набор резервных копий, который запускается ежедневно или еженедельно.

Создание набора резервных копий



Чтобы создать новый набор, нажмите «**Наборы**» на панели инструментов, а затем нажмите «**Новый набор**» слева.

Пути

Вкладка «Пути» позволяет выбрать, какие файлы и папки должны быть включены в резервную копию. Чтобы добавить файлы, нажмите «**Добавить файл** » или «**Добавить папку**». Если вы хотите удалить файл или папку из резервной копии, выберите один или несколько путей из списка и нажмите «**Удалить**» .

Каждый путь в списке будет иметь либо зеленый, либо красный значок рядом с ним. Зеленый значок указывает, что **fwbackups** способен читать путь, а красный значок указывает, что файл отсутствует или не может прочитать путь, и он будет исключен из будущих резервных копий.

Добавление файлов или папок так же возможно с помощью перетаскивания из любого файлового менеджера в список путей.

Назначение

Вкладка назначения определяет, где будет сохранена ваша резервная копия. Вы можете выбрать резервное копирование на локальный диск, съемное хранилище или удаленный компьютер, поддерживающий протокол SFTP (если на вашем компьютере запущен сервер OpenSSH, он, скорее всего, поддерживает SFTP).

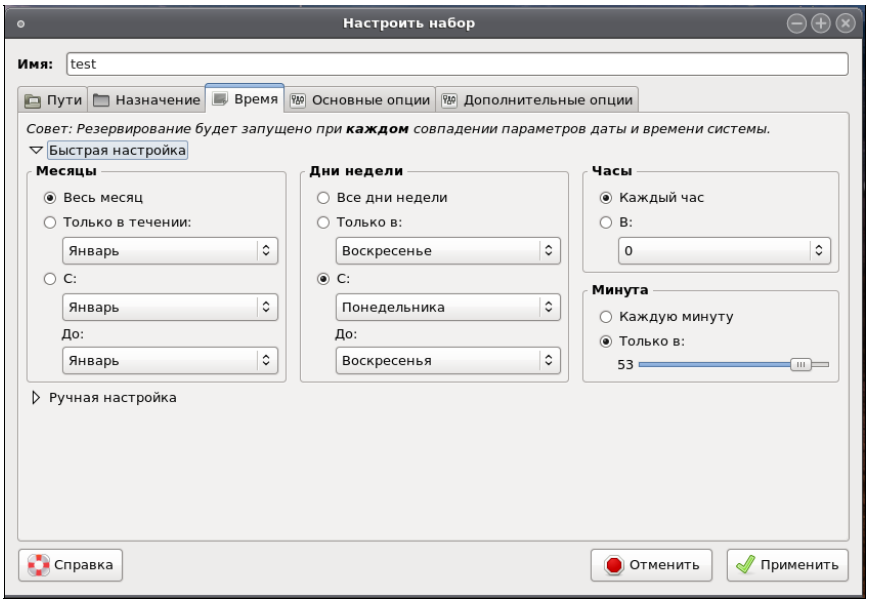
Не забудьте проверить настройки для удаленных пунктов назначения

Если вы решите сделать резервную копию на удаленном хосте, перед тем, как сохранить свой набор, обязательно нажмите «**Проверить настройки».** Опечатка в пароле (и в других полях) может сделать невозможным подключение к удаленному хосту, что приведет к неудачной резервной копии.

Время

Эта вкладка управляет временем и датой начала резервного копирования. Поддерживаются методы простой настройки и ручной настройки (crontab). Использование простой конфигурации рекомендуется для большинства пользователей.

Легкая конфигурация использует серию раскрывающихся списков и ползунков, чтобы определить, в какое время fwbackups должен запланировать резервное копирование. Резервное копирование набора выполняется каждый раз, когда дата соответствует выбранным параметрам. При этом будьте осторожны при выборе минуты для операции резервного копирования! Ошибка пользователя может вызвать резервирование **каждую минуту**. Вместо этого рекомендуется выбрать конкретную минуту, с которой начнется резервное копирование, например «0» (в начале часа) или «30» (в половине часа).



Если вы хотите дополнительно настроить время начала операции резервного копирования, вы можете использовать метод ручной настройки для этого. Он использует синтаксис crontab:

```
+ ------------- минута (0 - 59)
| + ------------ час (0 - 23)
| | + ---------- день месяца (1 - 31)
| | | + -------- месяц (1 - 12)
| | | | + ------ день недели (0 - 7) (воскресенье = 0 или 7)
| | | | | + ---- команда запуска
| | | | | |
* * * * * команда
```

Просто введите те же значения, что и в crontab, как указано выше, в обозначенные поля ввода. Обратите внимание, что вы не можете ввести все пять полей в одну строку. Кроме того, важно отметить, что в режиме ручной настройки проверка достоверности не выполняется при вводе пользователя, вы должны указать допустимые значения для полей. Шестое поле, используемое для команды, генерируется автоматически fwbackups.

- Используйте запятую (,), чтобы указать список значений

Пример 1. Использование запятой

2,4,5,7,8,9

- Используйте тире (-), чтобы указать диапазон значений

Пример 2. Использование тире

1-4 эквивалентна 1,2,3,4

- Используйте звездочку (*), чтобы указать все возможные значения

Пример 3. Использование звездочки

* в поле часов совпадает с 0-23 или 1,2,3, [...], 23

- Большинство версий cron поддерживают косую черту (/) для обозначения пропусков

Пример 4. Использование косой черты

* / 2 в поле минут эквивалентно 0,2,4,6,8, [...], 58

- В поле **дня недели**, как 0, так и 7 считаются воскресными.

Основные опции

Вкладка «**Основные опции»** позволяет вам установить параметры для вашей резервной копии. Кроме того, вкладка параметров позволяет вам выбрать формат резервного копирования и количество старых резервных копий для сохранения в любой момент времени.

Формат резервирования

Ваша резервная копия будет храниться по-разному в зависимости от выбранного формата резервного копирования.

Архивирование упаковывает все файлы в один (часто большой) архивный файл формата «tar». Архивные резервные копии не поддерживают инкрементное резервное копирование; каждый раз должен создаваться полный снимок. Также можно включить сжатие посредством gzip и bzip2. В этом случае к архиву будут приписаны .gz или .bz2 соответственно.

Уменьшение размера резервной копии при сжатии

> Включение сжатия будет использовать больше системных ресурсов во время резервного копирования, но приведет к меньшим размерам файлов. *gzip* - относительно легкое сжатие с хорошей степенью сжатия. Если вы хотите еще больше уменьшить размер своих резервных копий, подумайте о переходе на сжатие *bzip2* . Хотя он намного медленнее, чем gzip, bzip2 способен добиваться меньших размеров файлов.

При **прямом копировании** резервная копия будет просто копировать файлы и структуру папок как есть. Хотя этот тип резервного копирования не поддерживает сжатие, доступно инкрементное резервное копирование. Этот формат резервного копирования ранее назывался механизмом резервного копирования «rsync».

Увеличение скорости резервного копирования

> Включение параметра «**Прямое копирование файлов и папок» является инкрементным** вариантом, который будет выполнять инкрементную резервную копию вместо полной, копируя только изменения с момента последней резервной копии. В настоящее время инкрементные резервные копии не могут использоваться при резервном копировании на удаленный хост. Поддерживаются только полные прямые удаленные копии.
>
> Кроме того, при запуске инкрементного резервного копирования будет перезаписана папка бэкапа, поэтому старые резервные копии не будут сохранены.

Набор включен

Если этот параметр отключен, набор будет не запланирован для автоматического резервного копирования (недоступен в одноразовых резервных копиях).

Включая вложенные подпапки

Если выбрано, подпапки будут включены в резервную копию (рекомендуется). Если флажок снят, fwbackups будет делать только резервную копию файлов непосредственно внутри папок, указанных в разделе Пути, и не будет делать резервные копии файлов в подпапках.

Включая скрытые файлы

Если выбрано, скрытые файлы в системе (файлы и папки, начинающиеся с символа периода .) включены в резервную копию.

Следовать по ссылкам

Если выбрано, резервное копирование будет следовать символическим ссылкам и скопирует их цели, а не скопирует просто ссылку. Будьте осторожны с рекурсией ссылок!

Печатать информацию о геометрии диска в файле

Если выбрано, геометрия диска (включая разметку разделов) будет сохранена в файл, который будет добавлен в резервную копию.

Вывод установленных пакетов в текстовый файл

Если выбрано, список установленных имен и версий пакетов будет сохранен в текстовый файл, который будет добавлен в резервную копию. Этот параметр можно использовать для облегчения переустановки системы в неудачном случае сбоя или потери данных.

Сохраняется он в каталог tmp в бэкапе.

Эффективная поддержка разреженных файлов

Если выбрано, разреженные файлы на диске будут обработаны более эффективно.

Дополнительные опции

Вкладка «**Дополнительные опции»** включает технические или сложные параметры, которые можно использовать для настройки функций резервного копирования.

Команда для запуска до резервного копирования

Команда, введенная здесь, будет запущена в системной оболочке по умолчанию, прежде чем fwbackups начнет копировать файлы (недоступные в одноразовых резервных копиях).

Команда для запуска после резервного копирования

Команда, введенная здесь, будет запущена в системной оболочке по умолчанию после завершения резервного копирования fwbackups (недоступно в одноразовых резервных копиях).

Лексемы

Обе команды до и после резервного копирования поддерживают замену токенов. **fwbackups** заменит токены, которые вы используете в своих командах, с их соответствующими значениями:

[successful] Если резервная копия была успешно завершена без ошибок, этот токен будет заменен на 1. В случае ошибки сбоя или резервного копирования будет заменено 0.

[destination]

Целевая папка (см. Раздел «Назначение»). Если используется удаленный хост, то возвратится удаленная папка.

[set]

Имя набора

[date]

Дата в формате (YYYY-MM-DD_HH-MM) при запуске резервного копирования

[backup]

Имя файла резервной копии или папки, которая будет сохранена в месте назначения резервного копирования. По умолчанию *Backup-[set]-[date]*, плюс расширение архива, если это применимо.

[remote_host]

Имя хоста удаленного компьютера, на котором будет храниться резервная копия

[remote_port]

Порт для подключения к удаленному имени хоста

[remote_username]

Имя пользователя, используемое для подключения к удаленному хосту

[remote_password]

Пароль, используемый для подключения к удаленному хосту

> Используйте *[destination]/[backup],* если вам нужен абсолютный путь к новой папке или файлу резервной копии. Для экранирования одного из токенов (например, чтобы фактически использовать текст *[дата]* в команде), используйте обратную косую черту (\ *[дата]*).

Значение nice для процесса резервирования

Он контролирует приоритет резервного копирования (более низкое значение nice указывает более высокий приоритет). Только пользователь root может выбирать отрицательные nice значения.

Исключение из резервной копии

Файлы и папки, соответствующие шаблонам, перечисленным в этой текстовой записи, будут исключены из резервной копии. Файл, папка или шаблоны для исключения должны вводиться по одному в строке. Содержимое этой текстовой записи будет передаваться

непосредственно процессам tar или rsync при выполнении резервного копирования. В приведенном ниже примере все файлы в папке /home/username/Exclude, все файлы с расширением png, файл /home/username/foobar.jpg и, наконец, все имена файлов specificname.txt исключены из резервной копии.

Пример 5. Исключение файлов

/home/username/Exclude/*

*.png

/home/username/foobar.jpg

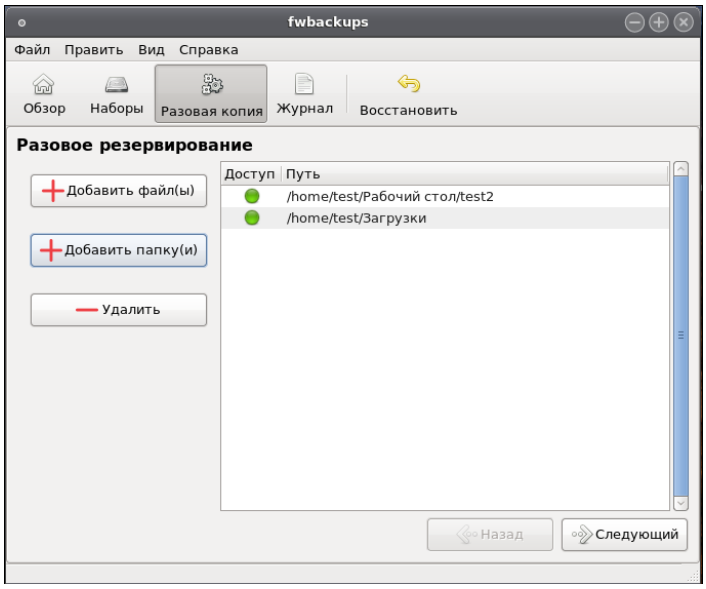
specificname.txt

Редактирование существующего набора

Перейдите на страницу «**Наборы резервирования»** и выберите нужный набор. Нажмите «**Редактировать набор»,** чтобы открыть диалоговое окно конфигурации резервного копирования. Вы можете настроить существующие наборы таким же образом, как и для нового набора (см. Раздел «Создание набора резервных копий»).

Запуск резервной копии только один раз

1. Переключитесь на страницу **разового резервного копирования**
2. Добавьте файлы и/или папки, которые вы хотите сделать резервными копиями. Вы можете использовать кнопки «**Добавить файлы» или «Добавить папки»**или просто перетащить файлы и папки в список. По завершении нажмите « **Далее»**.



3. Выберите варианты резервного копирования (см. Раздел «Основные опции»). По завершении нажмите «**Запуск резервирования»,**чтобы начать операцию.

Восстановление резервных копий

fwbackups может восстанавливать ваши файлы и папки из любого запланированного или одноразового резервного копирования.

1. Нажмите «**Восстановить»**на панели инструментов, чтобы открыть диалоговое окно восстановления.
2. Введите папку, в которую вы хотите восстановить свои файлы, в запись с надписью « **Восстановить в»**. Чтобы сделать выбор более удобным, вы можете использовать кнопку «**Обзор»**, чтобы открыть диалоговое окно браузера файлов. Зеленый значок указывает, что введенная папка доступна для записи, а красный значок указывает на то, что папка не может быть написана (необходимо выбрать другую и выполнить операцию восстановления).

Структура папок сохраняется в операциях восстановления, поэтому файлы будут восстановлены относительно их исходного местоположения. Например, восстановление резервной копии из **/home/myusername** для **/tmp** приведет к тому, что ваши файлы восстановятся в **/tmp/home/myusername**.

Установка места восстановления в корневой каталог приведет к восстановлению ваших файлов в их исходных местоположениях. Но при использовании такого варианта убедитесь что программа запущена с привилегиями суперпользователя.

3. Выберите, источник восстановления. Существует несколько возможных вариантов:

Набор резервирования

Используйте этот параметр для восстановления из созданных ранее резервных копий. Достаточно указать только набор и дату копирования.

Локальный архив

Используйте этот параметр для восстановления одноразовых архивных резервных копий, доступных на локальном хранилище (например, жестких дисках или съемных носителях). Нажмите «**Обзор»,** чтобы выбрать местоположение архивного файла для восстановления.

Локальная папка

Используйте этот параметр для восстановления одноразовых резервных копий как есть, доступных на локальном хранилище (таких как жесткие диски или съемные носители). Нажмите «**Обзор»** чтобы выбрать резервную папку для восстановления.

Удаленный архив (SSH)

То же, что и **локальный архив,** за исключением того, что архив будет извлечен с удаленного компьютера, после чего можно запустить восстановление из локального архива.

Удаленная папка (SSH)

То же, что и **локальная папка,** за исключением того, что папка будет извлекаться с удаленного компьютера, прежде чем восстановлена.

После того, как вы настроили операцию восстановления, нажмите «**Запуск восстановления»,** чтобы начать восстановление файлов. В зависимости от размера вашей резервной копии восстановление файлов может занять некоторое время.

Импорт или экспорт наборов

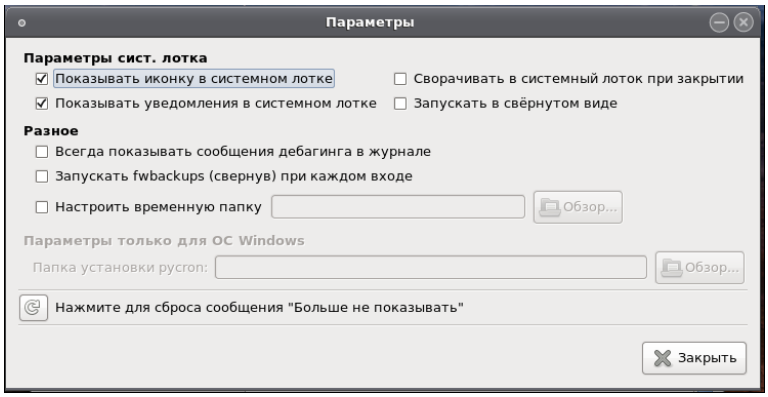
Чтобы импортировать установленные файлы конфигурации (**.conf** файлы), выберите «**Файл» → «Импорт наборов»,** а затем выберите файлы .conf, которые необходимо импортировать. Все версии **файлов** конфигурации **fwbackups** можно импортировать.

Чтобы экспортировать набор, выберите «**Файл» → «Экспорт наборов»** и выберите наборы, которые вы хотите экспортировать, установив флажок рядом с заданным именем. После выбора папки нажмите «**Экспортировать наборы»,** чтобы сохранить выбранные наборы в выбранную папку.

Местоположение, в котором хранятся установленные конфигурации, находится **~/.fwbackups/Sets.**

Изменение настроек программы

Выберите «**Править» → «Параметры»** в меню, чтобы открыть диалог настроек:



Показывать иконку в системном лотке

При переключении этого флажка будет отображаться или скрываться значок в трее.

Показывать уведомления в системном лотке

Выберите это, если вы хотите получать уведомления для важных событий.

Сворачивать в системный лоток при закрытии

При выборе этого флажка **fwbackups сворачивается** в трей при закрытии вместо выключения.

При нажатии на значок в трее откроется главное окно **fwbackups** .

Запускать в свёрнутом виде

Выберите, чтобы **fwbackups** отображал только значок в трее и скрывал главное окно при запуске.

Всегда показывать сообщения дебагинга в журнале

Эта опция позволяет отображать отладочные сообщения в средстве просмотра журналов. Используйте это, если вы пытаетесь устранить проблему.

Запуск fwbackups (свернув) при каждом входе

Выберите, чтобы fwbackups запускался свернутым при каждом входе в систему.

Настроить временную папку

Настройте временную папку для fwbackups.

«Больше не показывать»

Некоторые сообщения в **fwbackups** можно отключить, выбрав «**Больше не показывать**». Если вы хотите снова включить эти сообщения, нажмите кнопку.

Техническая информация

Вы можете подробнее ознакомиться с работой утилиты **fwbackups**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с графической утилитой Fwbackups;
- в **Яндекс.Дзен** — Работа с графической утилитой Fwbackups;
- в **VK Видео** — Работа с графической утилитой Fwbackups.

На наших каналах вы также сможете найти много другой полезной информации.

Форматы резервного копирования

В этом разделе описывается, как fwbackups создает резервные копии и требования к хранилищу каждого типа.

Архивные/tar-архивы

Архивные резервные копии используют один из двух методов для создания резервного архива в зависимости от операционной системы. Программа tar вызывается непосредственно для создания стандартного архива tar, опционально со сжатием gzip или bzip2. Сжатие резервной копии применяется «на лету» без необходимости создания архива tar.

Поскольку резервная копия находится в формате стандартного tar-архива, если нет возможности восстановить бэкап с помощью fwbackups, то любая утилита, поддерживающая формат tar может использоваться для извлечения файлов из резервной копии.

Резервное копирование Direct Copy/rsync

fwbackups определяет параметры, а затем делает вызов **rsync** для копирования файлов (rsync быстрее, чем shutil и, следовательно, используется, если rsync установлен в системе).

Поскольку файлы были скопированы напрямую, если fwbackups не может восстановить ваши файлы, достаточно просто скопировать их из места назначения резервного копирования в нужное место с помощью перетаскивания в вашем браузере файлов.

Минимальные требования к хранению

В зависимости от формата резервного копирования и назначения, минимальные требования к хранилищу для резервного копирования могут изменяться.

Для локальных резервных копий, как **архивных** и **прямого копирования** система будет копировать файлы с исходного диска к месту назначения без необходимости временного хранения, даже если сжатие включено.

Резервные копии для удаленных получателей имеют разные требования к хранению. **Архивные** резервные копии с удаленным получателем создают архив локально, а затем загружают его через SFTP на удаленный хост. Следовательно, вы должны иметь свободное пространство, равное размеру резервных копий файлов (если не включено сжатие, и в этом случае потребуется немного меньше). В резервной копии с **прямым** копированием с удаленным получателем файлы загружаются непосредственно на удаленный компьютер, и поэтому можно создать резервную копию полного диска. Однако следует предупредить, что удаленная прямая копия значительно медленнее резервной копии архива.

Сохранение владения файлами и другие атрибуты

fwbackups использует внутренние файлы tarfile и shutil для восстановления файлов (и paramiko для взаимодействия с удаленными узлами через SFTP). Разрешения на файлы, время модификации и время доступа всегда сохраняются, как и символические ссылки.

Локальные резервные копии должны сохранять право собственности на Unix-подобные операционные системы, однако ОС обычно не позволяют обычным пользователям изменять права собственности на файлы, и, таким образом, резервное копирование нужно будет извлечь вручную с правами root, чтобы сохранить право собственности. Удаленные резервные копии не сохранят право собственности, так как любые файлы, загруженные через SFTP, предполагают владельца пользователя, используемого для подключения к удаленному компьютеру. Обратите внимание, что в случае резервного копирования архива на удаленный хост это относится только к фактическому архиву. Сам архив может содержать информацию о владельце файла, и как только он был получен с удаленного хоста, его можно извлечь вручную аналогично резервной копии локального архива, если пользователь хочет сохранить права собственности на файл.

Другие атрибуты файлов, xattrs или ACL могут быть сохранены в резервной копии (в зависимости от формата резервной копии, ОС, на которой была создана резервная копия, и файловой системы), однако fwbackups не будет пытаться их восстановить.

Ожидаемые уровни надежности

fwbackups - это программа резервного копирования пользователей и, соответственно, должна иметь возможность резервировать ваши пользовательские данные без проблем. Хотя можно использовать fwbackups для резервного копирования всей операционной системы, это не было его целью, и этот сценарий пока не проверен. Пользователи должны ожидать, что fwbackups будут успешно выполнять резервное копирование и восстановление своих данных, однако (как описано выше) дополнительные метаданные, такие как владение файлами, списки ACL и расширенные атрибуты, которые ОС может потребовать для правильной работы, не подлежат восстановлению вместе с фактическими файловыми данными.

Пользователям рекомендуется регулярно проверять журнал fwbackups, чтобы гарантировать отсутствие ошибок, а также

периодически проверять резервные копии.

Testdisk - утилита для восстановления утраченных данных

Утилита **testdisk** предназначена для восстановления утраченных разделов и/или данных, если эти проблемы вызваны программно, вредоносным ПО или ошибками человека.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install testdisk
```

После установки запуск утилиты доступен по команде (с правами пользователя **root**):

```
testdisk
```

Вы можете подробнее ознакомиться с работой утилиты **testdisk**, просмотрев наши обучающие видео:

- на **RuTube** — Восстановление файлов в РЕД ОС;
- в **Яндекс.Дзен** — Восстановление файлов в РЕД ОС;
- в **VK Видео** — Восстановление файлов в РЕД ОС.

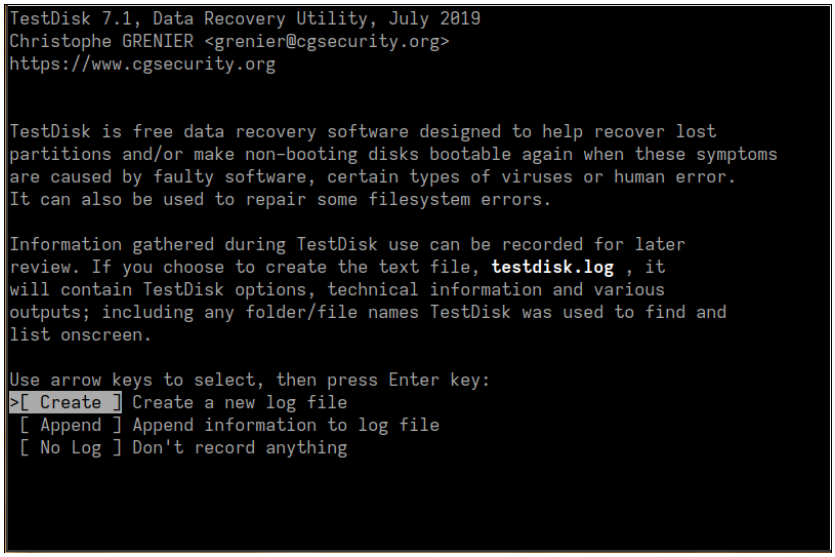
На наших каналах вы также сможете найти много другой полезной информации.

Утилита работает в окне терминала и имеет интуитивно понятный интерфейс.

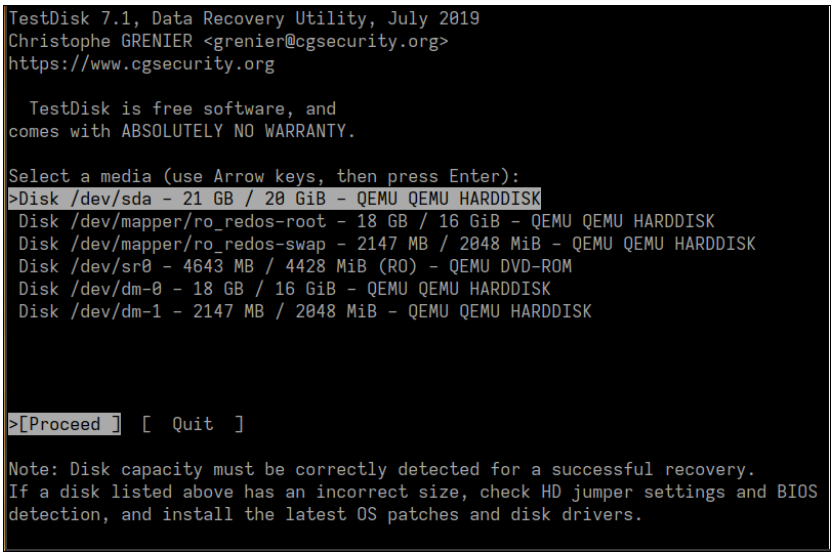
Сначала необходимо выбрать способ логирования данных:

- [**Create**] - создать новый файл журнала данных;
- [**Append**] - использовать существующий;
- [**No Log**] - ничего не регистрировать.

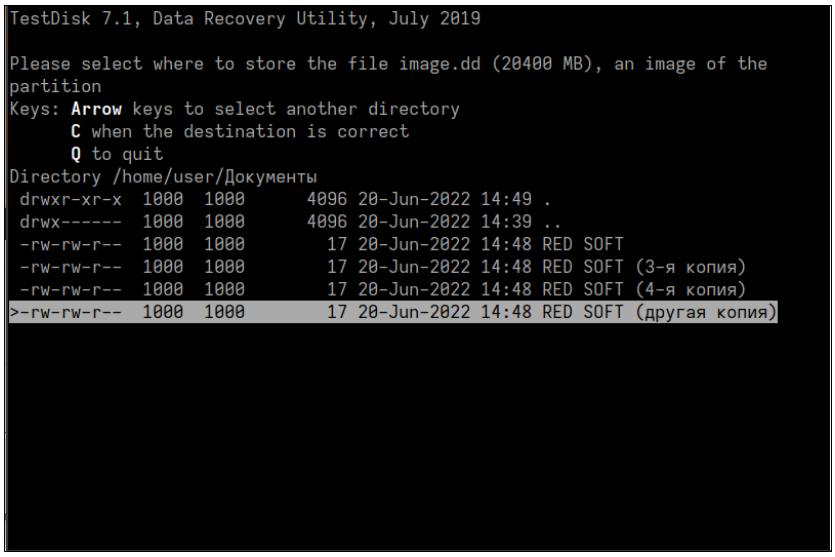
Выберите подходящий вам вариант.



Следующий шаг — выбор диска. Утилита отображает все диски, подключенные к системе, общий объем памяти каждого диска и его свободное пространство. Для продолжения работы необходимо выбрать диск, на котором хранится (хранилась) информация, подлежащая восстановлению.

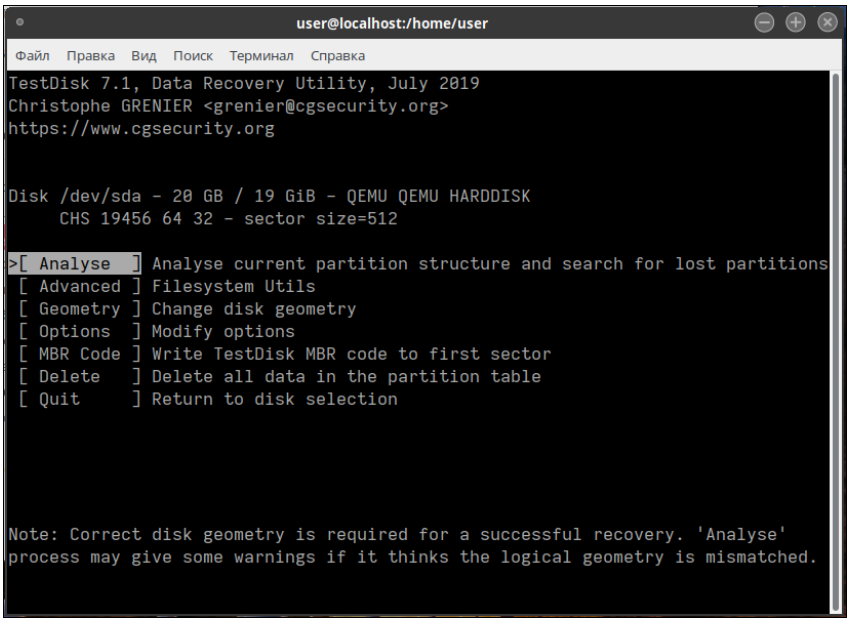


Перед тестированием утилиты было создано несколько файлов в папке «**Документы**». До момента их удаления они отображаются через утилиту **testdisk** в заданной папке, их также можно копировать в другие разделы и каталоги.

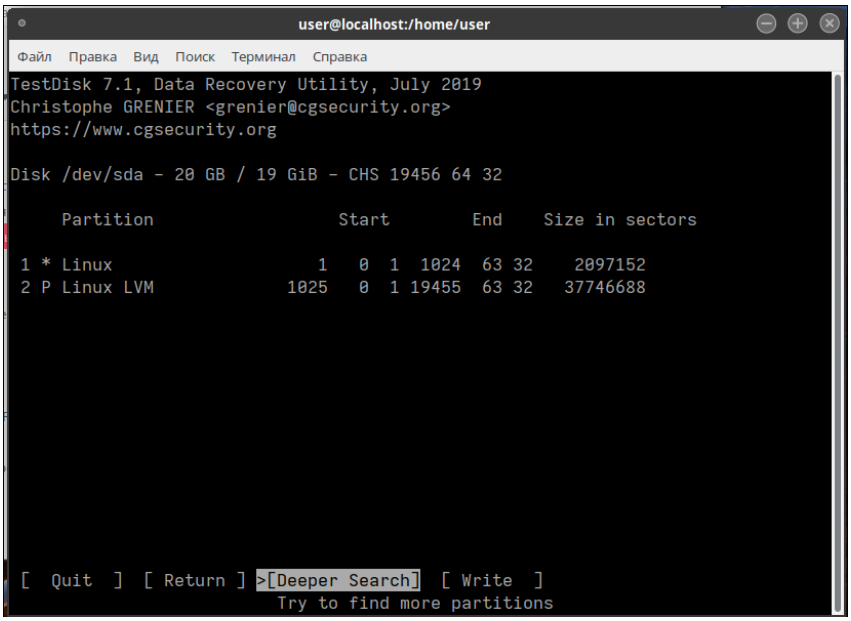


После того как некоторые документы были удалены, с помощью утилиты **testdisk** необходимо произвести анализ текущей структуры разделов необходимого диска.

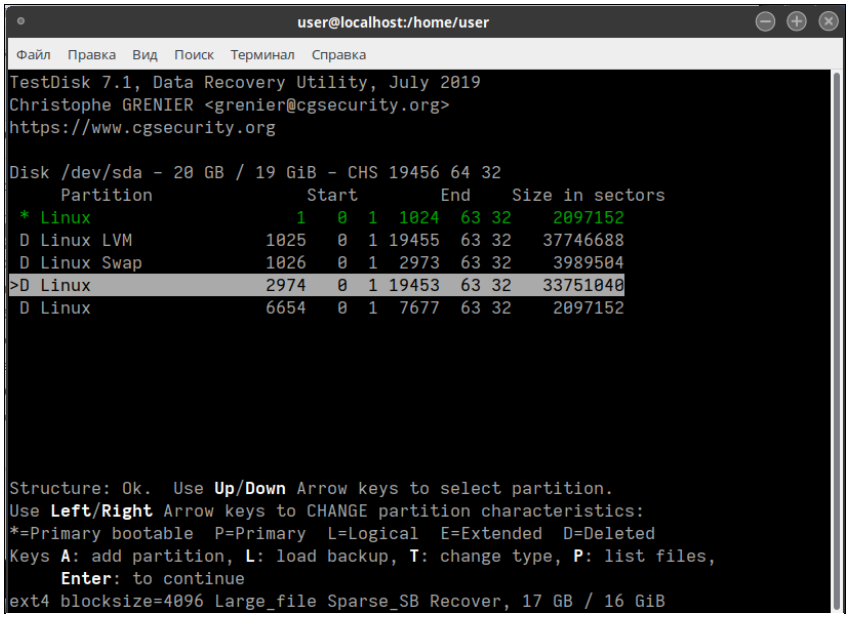
Для этого на требуемой таблице разделов необходимо выбрать из предложенных вариантов возможных действий — [**Analyse**], а затем нажать [**Quick Search**] для поиска разделов.



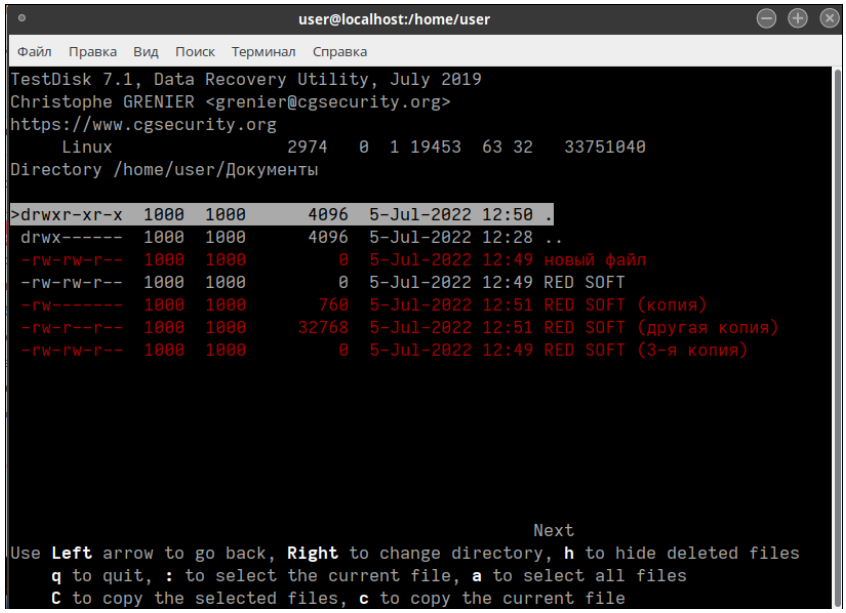
Утилита предложит выбрать раздел, который необходимо проанализировать. Для запуска анализа раздела нажмите [**Deeper Search**].



После завершения анализа будет выведена структура диска, где следует найти нужный раздел с содержимым.

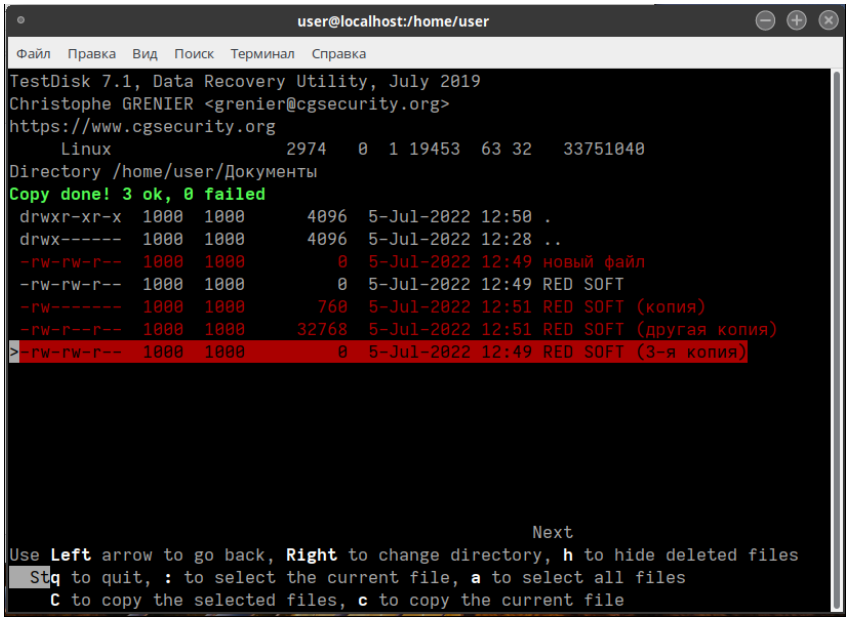


Нажмите **P** для отображения содержимого диска и перейдите в папку, из которой были удалены файлы. Удаленные файлы, подлежащие восстановлению, будут выделены красным цветом.

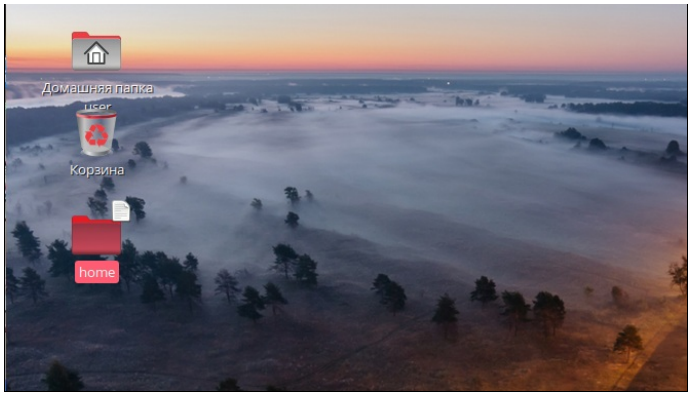


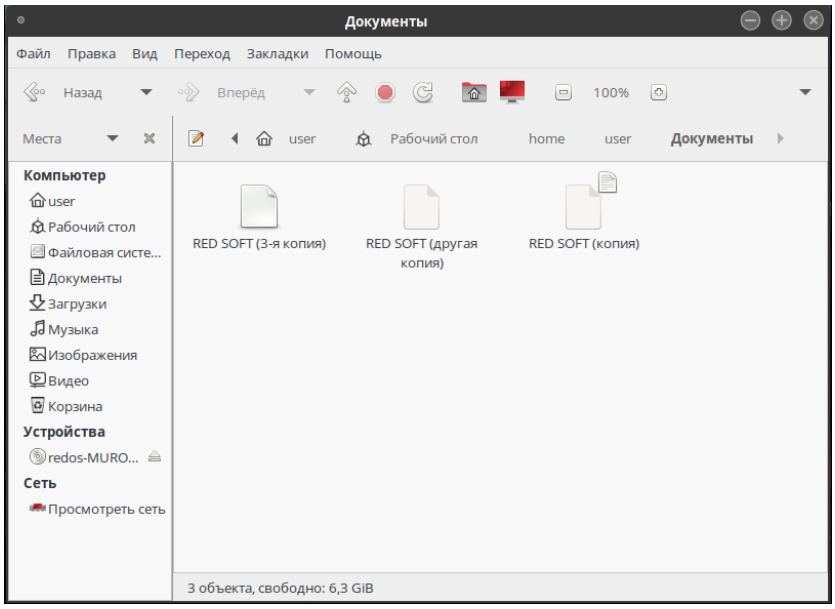
Внизу экрана даны инструкции по восстановлению данных. После копирования удаленных файлов появится список каталогов, в

которые его можно восстановить.



В данном примере файлы были восстановлены на «**Рабочий стол**». Восстановленные файлы отмечены специальным значком.



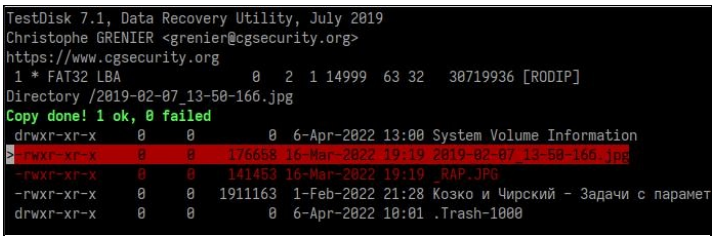


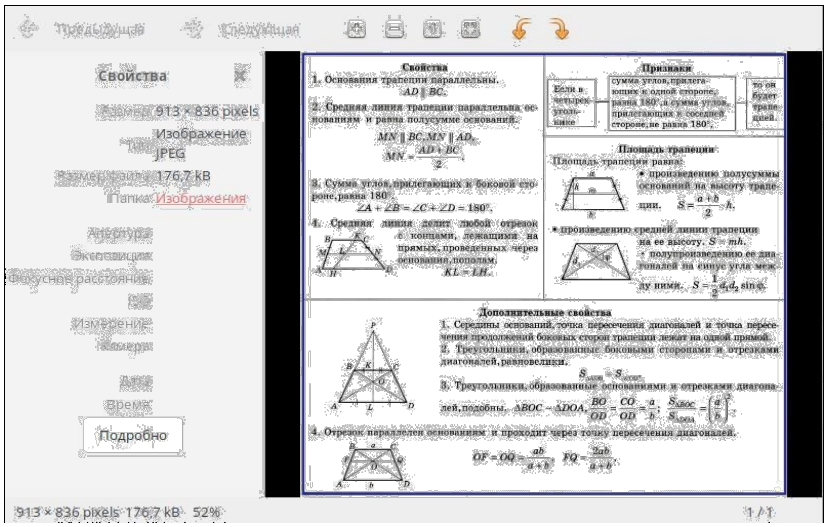
При работе со съемными носителями восстановление удаленных файлов производится несколько проще.

После выбора таблицы разделов диска необходимо выбрать пункт [**Advanced**] для работы с файловой системой. Выберите необходимый раздел и выполните [**Undelete**].

Будут показаны все файлы, содержащиеся на разделе, в том числе и удаленные (отмечены красным цветом).

Внизу экрана также описаны инструкции по восстановлению удаленных файлов. После копирования удаленного файла появится список каталогов, в которые его можно восстановить. В данном примере восстановление удаленного изображения производится в папку «**Изображения**».





Утилита **testdisk** - достаточно простой, но мощный инструмент для восстановления различных типов данных. Функционал утилиты также включает исправление таблицы разделов и восстановление загрузочного сектора. Обработке подлежат все типы дисков и разделов, включая LVM-разделы.

Timeshift. Работа со снимками ОС

Создание снимков ОС
Режим RSYNC
Режим BTRFS
Восстановление снимка ОС
Работа с timeshift в командной строке

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: timeshift-21.09.1-1

Timeshift — программа для автоматического периодического создания копий системы (снимков/snapshots).

Timeshift предназначен прежде всего для создания снимков системных файлов и настроек. Пользовательские данные по умолчанию не архивируются, поэтому в случае сбоя системы восстанавливаются системные файлы, а данные пользователей остаются в актуальном состоянии (при условии, что они не были повреждены).

Резервные копии не могут быть восстановлены на уровне отдельных файлов, восстановление всегда происходит в полном объеме настроек **Timeshift**.

Стоит учитывать, что **Timeshift** не предназначена для клонирования ОС с одного ПК на другой путем восстановления из снимка другого ПК.

Timeshift имеет 2 режима работы:

- RSYNC;
- BTRFS.

Вы можете подробнее ознакомиться с работой утилиты **timeshift**, просмотрев наши обучающие видео:

- на **RuTube** — Создание резервных копий и восстановление системы с помощью TimeShift;
- в **Яндекс.Дзен** — Создание резервных копий и восстановление системы с помощью TimeShift;
- в **VK Видео** — Создание резервных копий и восстановление системы с помощью TimeShift.

На наших каналах вы также сможете найти много другой полезной информации.

Создание снимков ОС

Для установки **timeshift** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install timeshift
```

После установки утилита доступна из «**Главного меню**» - «**Системные**» - «**Резервное копирование и восстановление**».

Режим RSYNC

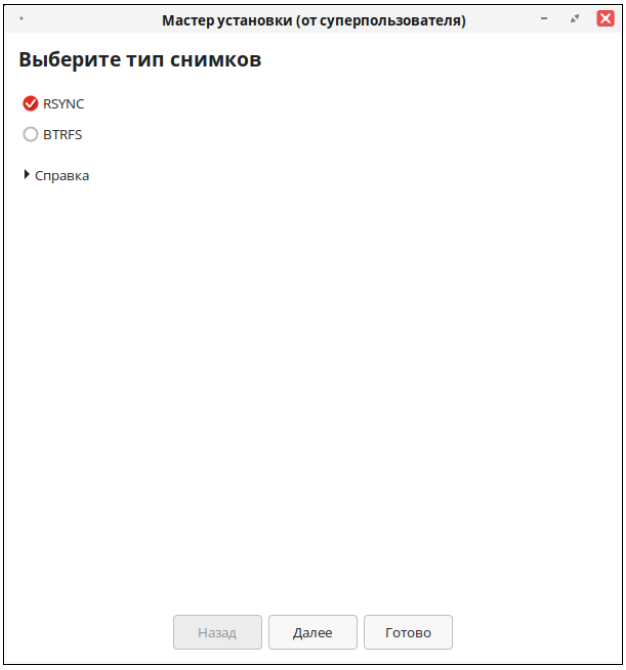
Первый режим является универсальным для всех файловых систем. Основные особенности режима **RSYNC**:

- снимки создаются путём копирования системных файлов при помощи *RSYNC* и создания жёстких ссылок на неизмененные файлы из предыдущего снимка;
- все файлы копируются при создании первого снимка, последующие снимки являются инкрементальными. Неизмененные файлы будут связаны с предыдущим снимком, если он доступен;
- создание первого снимка может занять до *10 минут*;
- системный раздел может быть отформатирован в любой файловой системе. Резервный раздел может быть отформатирован в любой файловой системе Linux, поддерживающей жесткие ссылки. Сохранение снимков на несистемный или внешний диск

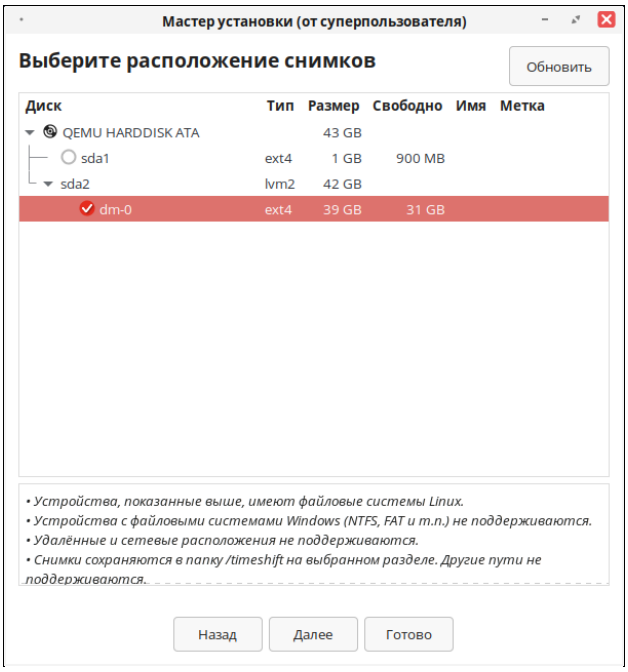
позволяет восстановить систему, даже если системный диск повреждён;

- можно задать исключения для файлов и каталогов для экономии дискового пространства;
- систему необходимо перезагрузить после восстановления снимка.

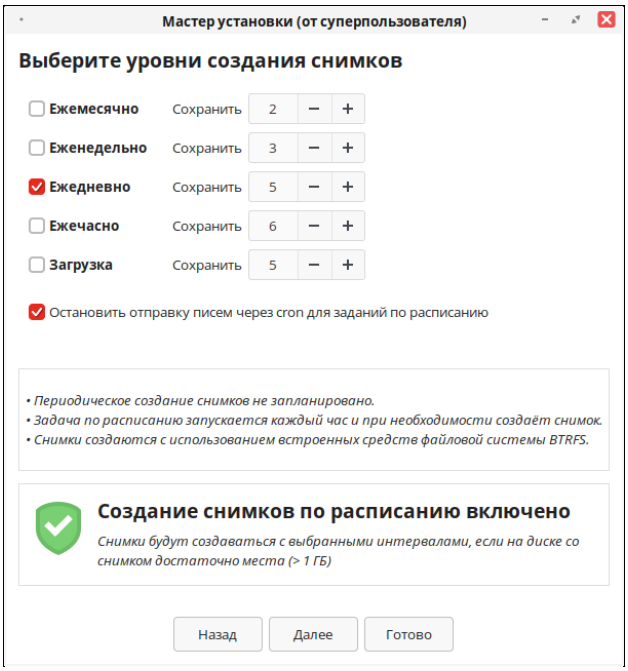
При запуске утилиты **timeshift** выберите тип снимков **RSYNC**.



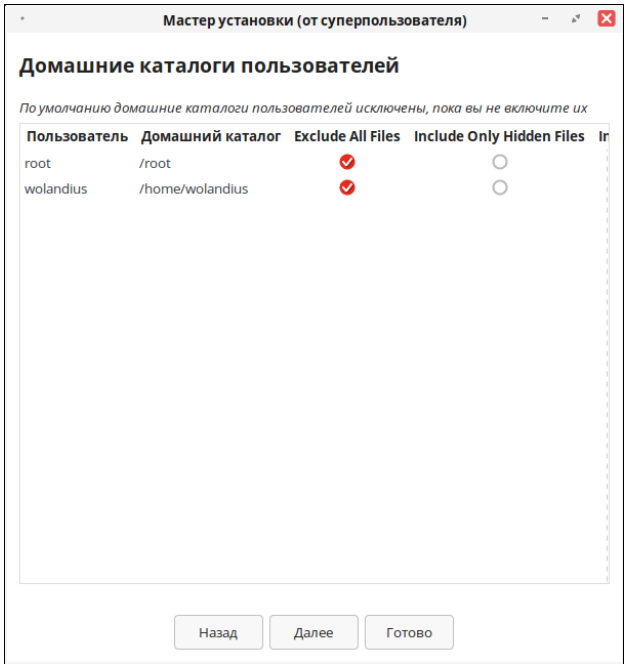
Выберите расположение снимков.



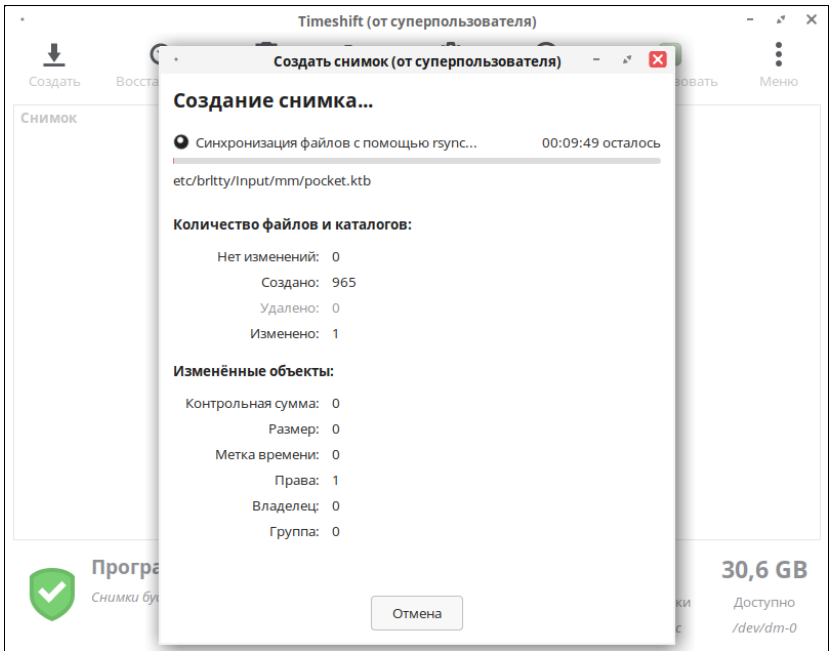
Настройте периодичность создания снимков.



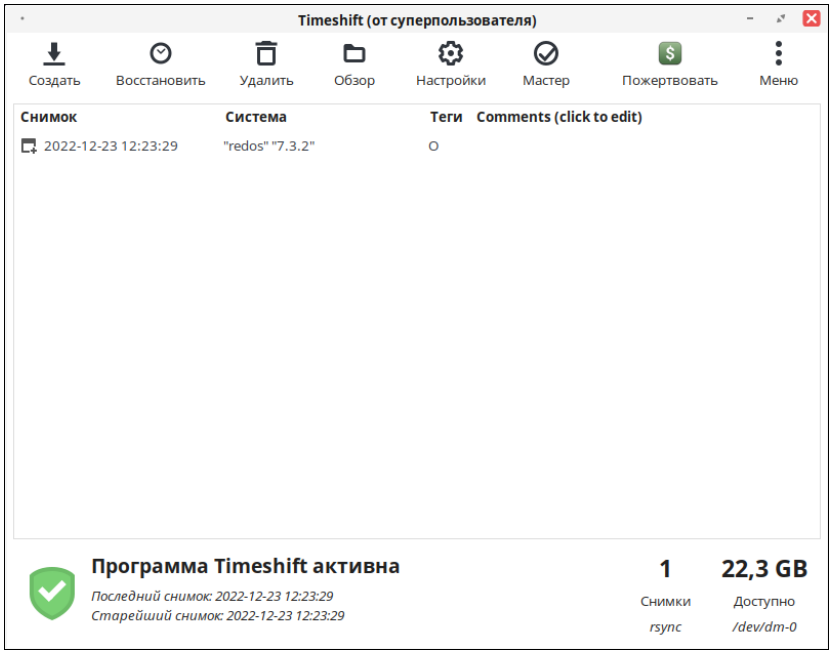
Включите ведение снимков для домашних каталогов пользователей.



Выберите пункт «**Создать**».



После завершения создания снимок появится в списке.



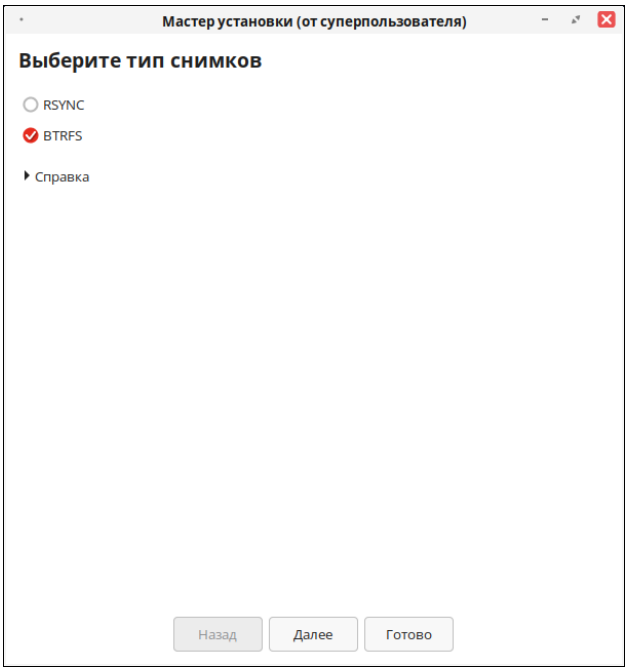
Режим BTRFS

Основные особенности режима **BTRFS**:

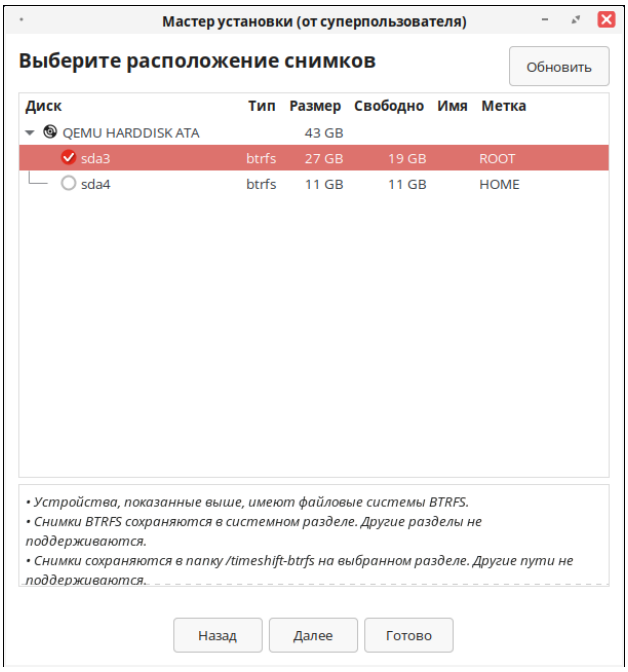
- снимки создаются с использованием встроенных средств файловой системы *BTRFS*;
- снимки создаются и восстанавливаются мгновенно (создание снимков — это атомарная транзакция на уровне файловой системы);
- снимки восстанавливаются путём замены системных подразделов. Поскольку файлы никогда не копируются, не удаляются и не перезаписываются, риск потери данных отсутствует. Существующая система сохраняется как новый снимок после восстановления;
- снимки сохраняются на том же диске, с которого они созданы (системном диске). Хранение на других дисках не поддерживается. Если системный диск выйдет из строя, снимки, хранящиеся на нём, будут потеряны вместе с системой;
- нет возможности исключать файлы и каталоги;
- размер снимков *BTRFS* изначально равен нулю. При изменении системных файлов, данные записываются в новые блоки, которые занимают дисковое пространство (копирование при записи). Файлы в снимке продолжают указывать на исходные блоки данных;
- ОС должна быть установлена на раздел *BTRFS* с разбивкой на подразделы **@** и **@home** (см. Описание процесса разметки диска). Другие виды разделов не поддерживаются;

- снимки можно восстановить без немедленной перезагрузки запущенной системы.

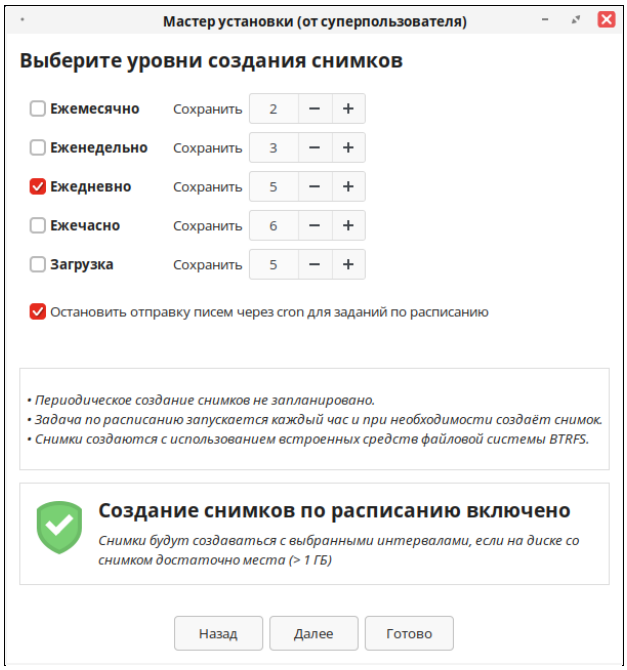
При запуске утилиты **timeshift** выберите тип снимков **BTRFS**.



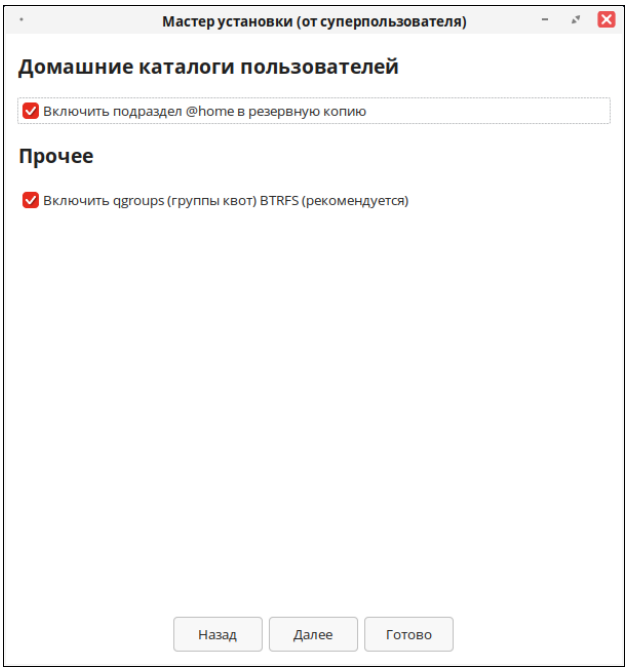
Выберите расположение снимков на том диске, где расположен подтом **@**.



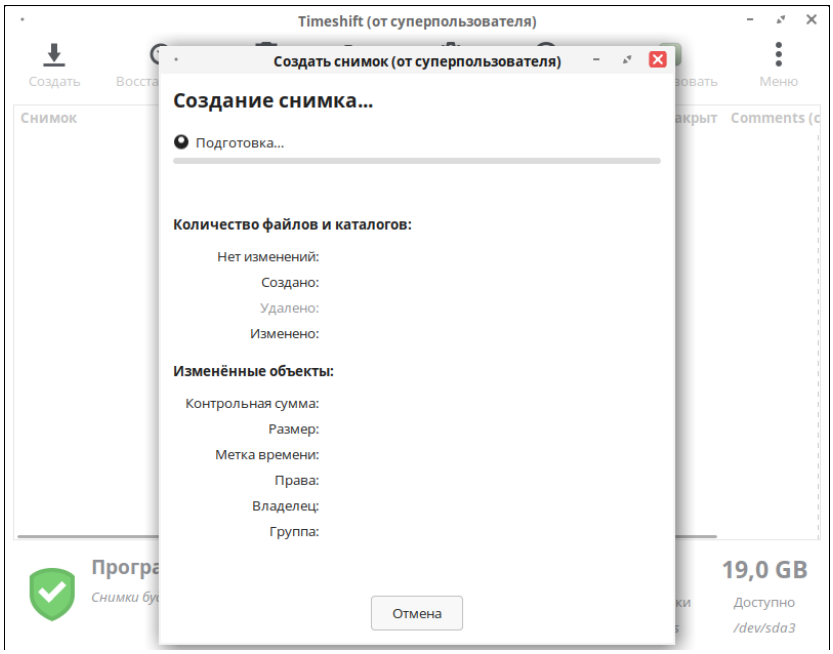
Настройте периодичность создания снимков.



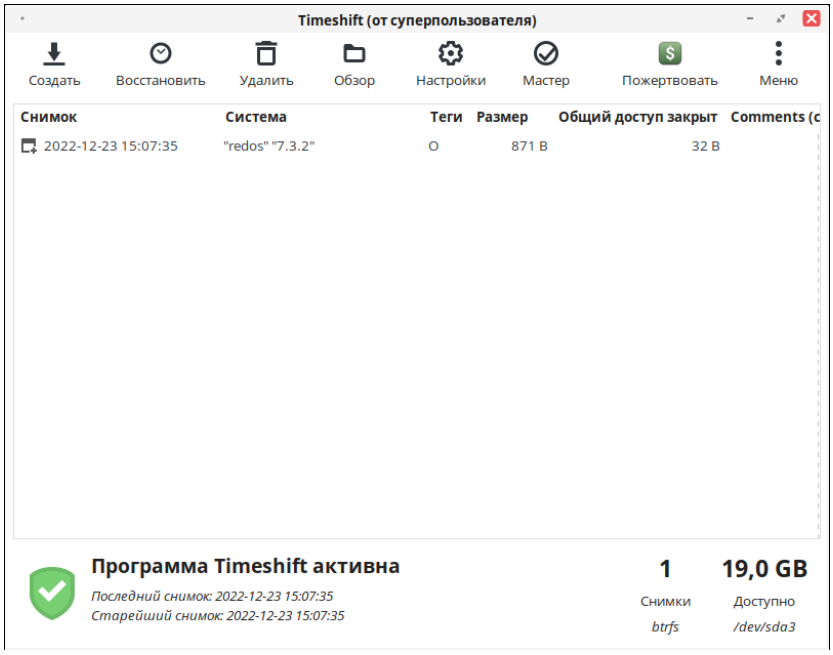
Включите ведение снимков для домашних каталогов пользователей.



Выберите пункт «**Создать**».

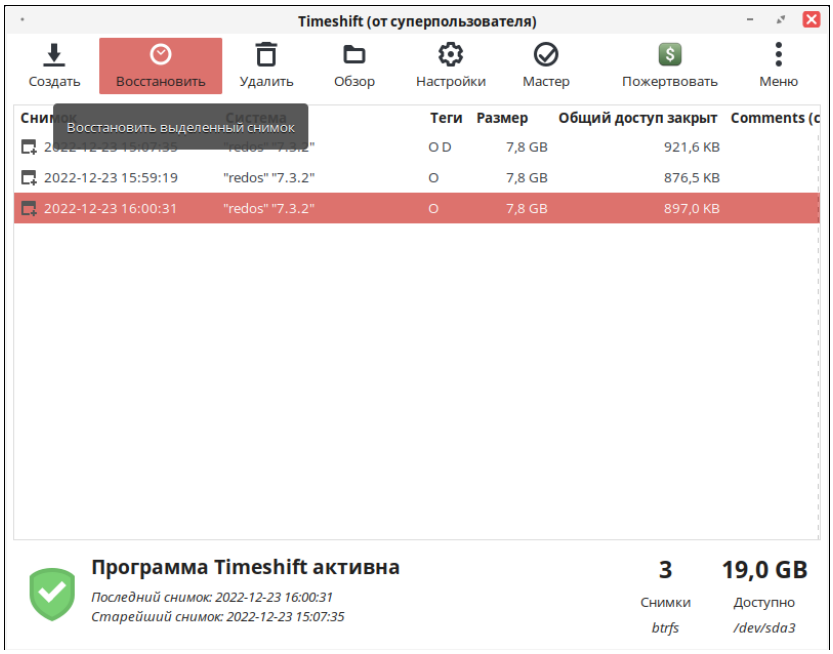


После завершения создания снимок появится в списке.

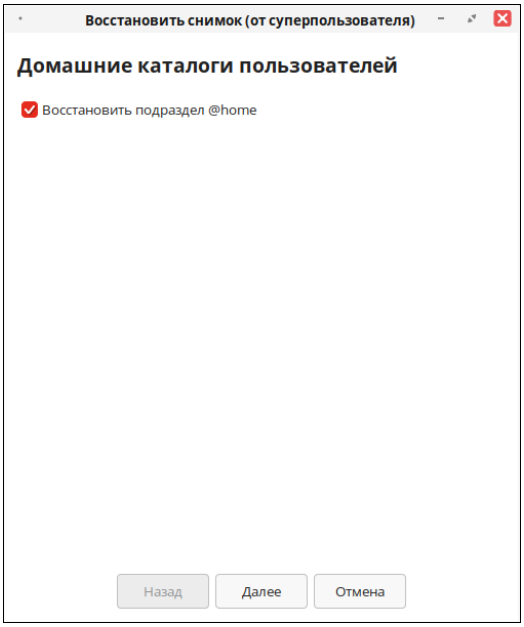


Восстановление снимка ОС

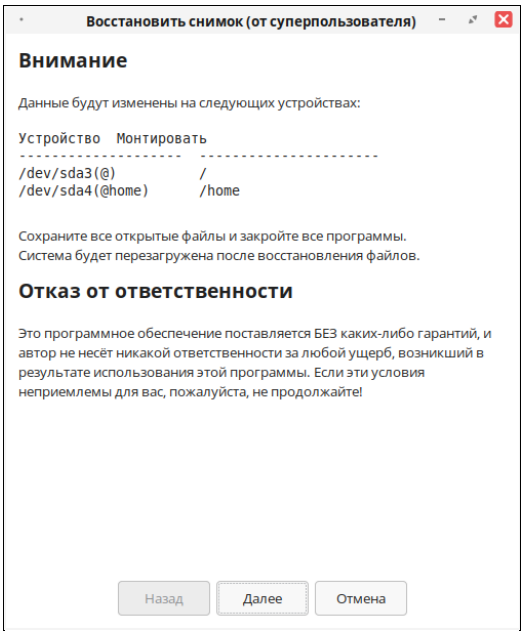
Для восстановления снимка ОС необходимо выбрать нужный снимок ОС и нажать кнопку «**Восстановить**».



Если также необходимо восстановить домашний каталог пользователя, установите соответствующий флаг в открывшемся окне.



После этого будет выведена информация о восстанавливаемых дисках. Нажмите «**Далее**» для запуска процесса восстановления снимка.



После перезагрузки ОС ПК будет работать на выбранном вами снимке ОС.

Работа с timeshift в командной строке

Работа с **timeshift** выполняется с правами администратора системы или суперпользователя root.

Вывод справки о команде осуществляется командой (возможно выполнение с правами локального пользователя):

```
timeshift
```

Если параметры не указаны, например, при создании снимка, значения по умолчанию будут загружены из конфигурации приложения.

Просмотр списка снимков:

```
timeshift --list

/dev/sda3 is mounted at: /run/timeshift/backup, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

/dev/sda4 is mounted at: /run/timeshift/backup-home, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

Device : /dev/sda3
UUID   : f58e67fe-03f2-44e9-8251-f3c7db87b6bf
Path   : /run/timeshift/backup
Mode   : BTRFS
Status : OK
2 snapshots, 19.0 GB free

Num     Name                 Tags  Description
------------------------------------------------------------------------------
0    >  2022-12-23_15-07-35  O
1    >  2022-12-23_15-59-19  O
```

Создание снимка:

```
timeshift --create

Using system disk as snapshot device for creating snapshots in BTRFS mode

/dev/sda3 is mounted at: /run/timeshift/backup, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

/dev/sda4 is mounted at: /run/timeshift/backup-home, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

Creating new backup...(BTRFS)
Saving to device: /dev/sda3, mounted at path: /run/timeshift/backup
Saving to device: /dev/sda4, mounted at path: /run/timeshift/backup-home
Created directory: /run/timeshift/backup/timeshift-btrfs/snapshots/2022-12-23_16-00-31
```

```
Created subvolume snapshot: /run/timeshift/backup/timeshift-btrfs/snapshots/2022-12-23_16-00-31/@
Created directory: /run/timeshift/backup-home/timeshift-btrfs/snapshots/2022-12-23_16-00-31
Created subvolume snapshot: /run/timeshift/backup-home/timeshift-btrfs/snapshots/2022-12-23_16-00-31/@home
Created control file: /run/timeshift/backup/timeshift-btrfs/snapshots/2022-12-23_16-00-31/info.json
BTRFS Snapshot saved successfully (0s)
Tagged snapshot '2022-12-23_16-00-31': ondemand ----------------------------------------------------------------------
```

Создание снимка, если он запланирован (есть в расписании):

```
timeshift --check
```

Восстановить снимок (параметры будут запрошены в интерактивном режиме):

```
timeshift --restore
```

Восстановить снимок:

```
timeshift --restore --snapshot '2022-12-23_16-00-31'
```

Восстановить определенный снимок в необходимый раздел (для **rsync**):

```
timeshift --restore --snapshot 1 --target /dev/sda2
```

Удалить снимок:

```
timeshift --delete --snapshot '2022-12-23_16-00-31'
```

SyncThing — утилита для синхронизации файлов

Установка
Синтаксис
Команды
Опции
Пример работы

Окружение

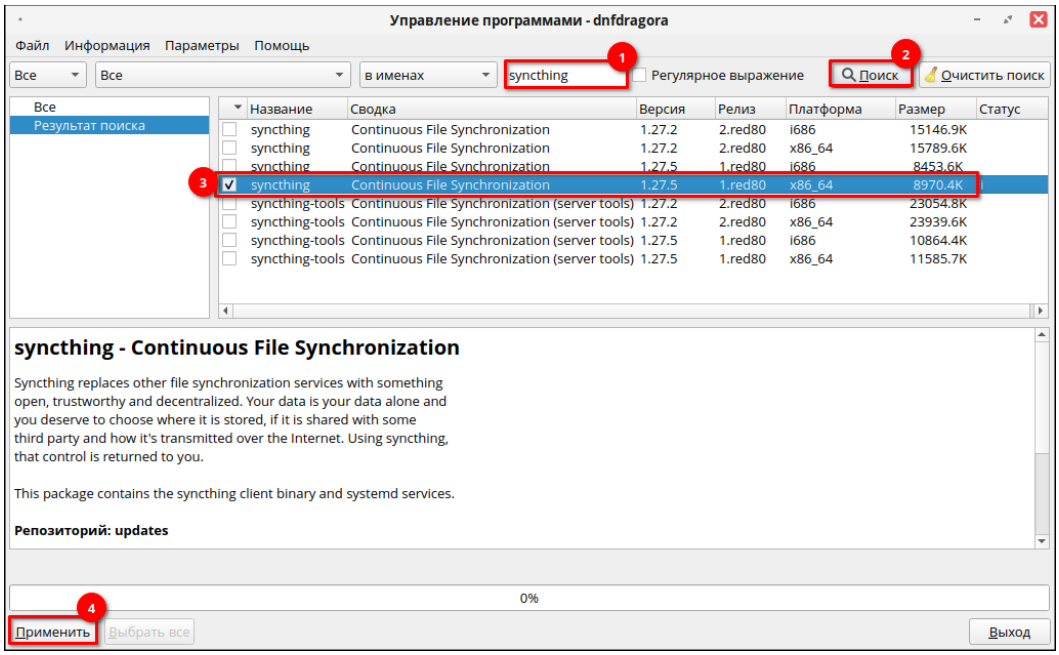
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: syncthing-1.27.5-1

Syncthing позволяет синхронизировать файлы в двух направлениях на нескольких устройствах. Создание, изменение или удаление файлов на одном компьютере будет автоматически реплицировано на другие устройства. **Syncthing** обменивается данными между компьютерами, когда они одновременно подключаются к сети.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**syncthing**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install syncthing
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
syncthing [<команда>] [<опции>]
```

Команды

Основные команды утилиты:

- **serve** — запустить синхронизацию;
- **generate** — сгенерировать ключ и конфигурацию, затем выйти;
- **decrypt** — расшифровать или проверить зашифрованную папку;
- **cli** — интерфейс командной строки для синхронизации;
- **install-completions** — печать команд для установки дополнений оболочки.

Опции

Основные опции утилиты:

- **--allow-newer-config** — загрузить конфигурационный файл с более новой версией программы;
- **--audit** — записать события в файл аудита с отметками времени в формате ГГГГММДД-ЧЧММСС.log;
- **--auditfile=<file|-|-->** — использовать файл или поток для событий аудита;
- **--browser-only** — открыть веб-интерфейс в браузере для работающего экземпляра syncthing;
- **--device-id** — вывести идентификатор устройства;
- **--generate=<dir>** — сгенерировать ключ и конфигурацию в указанном каталоге;
- **--gui-address=<address>** — переопределить адрес прослушивания графического интерфейса;
- **--gui-apikey=<string>** — переопределить ключ API, необходимого для доступа к GUI/REST API;
- **--gui-password=<password|->** — установить новый пароль аутентификации графического интерфейса для обновления файла конфигурации;
- **--gui-user=<username>** — установить новое имя пользователя для аутентификации графического интерфейса для обновления файла конфигурации;
- **--help, -h** — вывести справку;
- **--home=<dir>** — установить новую конфигурацию и каталог данных;
- **--config=<dir>** — установить каталог конфигурации;
- **--data=<dir>** — установить каталог данных;
- **--logfile=<filename>** — задать имя файла назначения для регистрации;
- **--logflags=<flags>** — выбрать информацию в префиксе строки журнала;
- **--log-max-old-files=<num>** — количество старых файлов, которые нужно сохранить;
- **--log-max-size=<num>** — задать максимальный размер любого файла журнала;
- **--no-browser** — запустить браузер;
- **--no-console** — консольное окно;
- **--no-default-folder** — не создавать папку по умолчанию при создании начальной конфигурации/первом запуске;
- **--no-restart** — не перезапускать syncthing после его закрытия;
- **--no-upgrade** — отключить автоматическое обновление;
- **--paths** — распечатать пути, используемые для конфигурации, ключей, базы данных, переопределений графического интерфейса, папки синхронизации по умолчанию и файла журнала;
- **--paused** — запуск устройства и пауза;
- **--reset-database** — удалить все данные из базы данных и возвратить ее к исходному состоянию, выполнив полное повторное сканирование и повторную синхронизацию;
- **--reset-deltas** — сбросить все изменения или обновления, которые были внесены в систему с момента последнего сброса;
- **--skip-port-probing** — пропустить сканирование портов при выполнении операций;
- **--unpaused** — запустить или выполнить действие без ожидания;
- **--upgrade** — обновить программу до новой версии;
- **--upgrade-check** — проверить наличие обновлений или новых версий;
- **--upgrade-to=<url>** — обновить до указанного URL;
- **--verbose** — выводить подробные сообщения или логи для отладки;
- **--version** — показать текущую версию syncthing;
- **--to=<dir>** — указать каталог или директорию для перемещения или копирования;
- **--verify-only** — выполнять только проверку или верификацию, без выполнения операции;
- **--password=<pw>** — установить пароль для аутентификации или доступа;
- **--folder-id=<id>** — указать идентификатор папки для операции;
- **--token-path=<file>** — указать путь к файлу токена для доступа или аутентификации;
- **--continue** — продолжить выполнение операции или действия без прерывания.

Пример работы

Для запуска сервера выполните следующий алгоритм действий:

1. Создайте файл /etc/systemd/system/syncthing@.service (потребуются права **администратора**):

```
nano /etc/systemd/system/syncthing@.service
```

2. Заполните файл следующим содержанием и сохраните его:

```
[Unit]
Description=Syncthing - Open Source Continuous File Synchronization for %I
Documentation=man:syncthing(1)
```

```
After=network.target

[Service]
User=%i
ExecStart=/usr/bin/syncthing -no-browser -gui-address="0.0.0.0:8384" -no-restart -logflags=0
Restart=on-failure
SuccessExitStatus=3 4
RestartForceExitStatus=3 4

# Hardening
ProtectSystem=full
PrivateTmp=true
SystemCallArchitectures=native
MemoryDenyWriteExecute=true
NoNewPrivileges=true

[Install]
WantedBy=multi-user.target
```

3. Перезагрузите список служб systemd:

```
sudo systemctl daemon-reload
```

4. Запустите службу синхронизации (если запуск службы необходимо разрешить только определенному пользователю, замените $USER на имя пользователя):

```
sudo systemctl start syncthing@$USER
```

5. Добавьте службу синхронизации в автозагрузку:

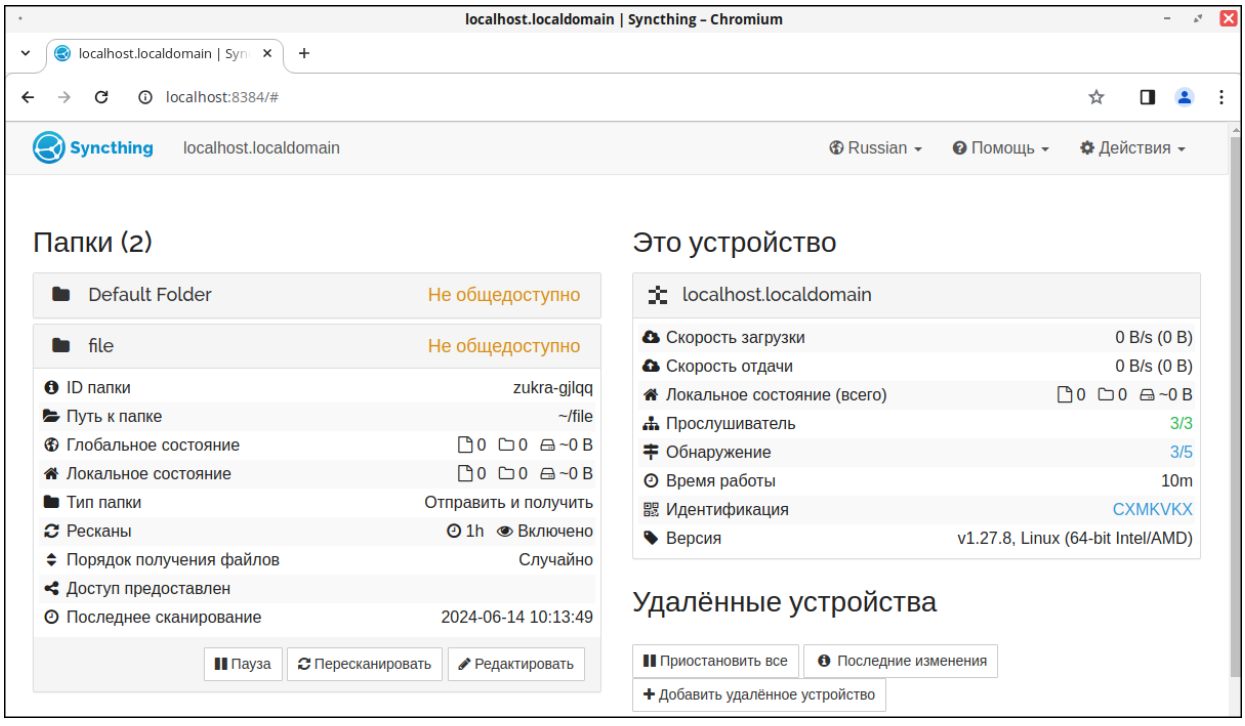
```
sudo systemctl enable syncthing@$USER
```

6. Проверьте работу службы синхронизации:

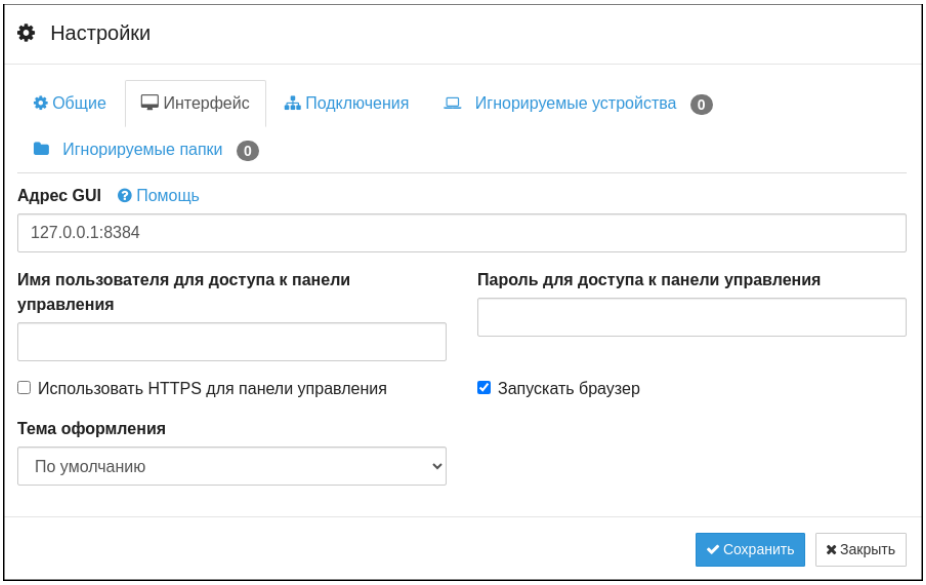
```
sudo systemctl status syncthing@$USER
```

В статусе должно отображаться active (running).

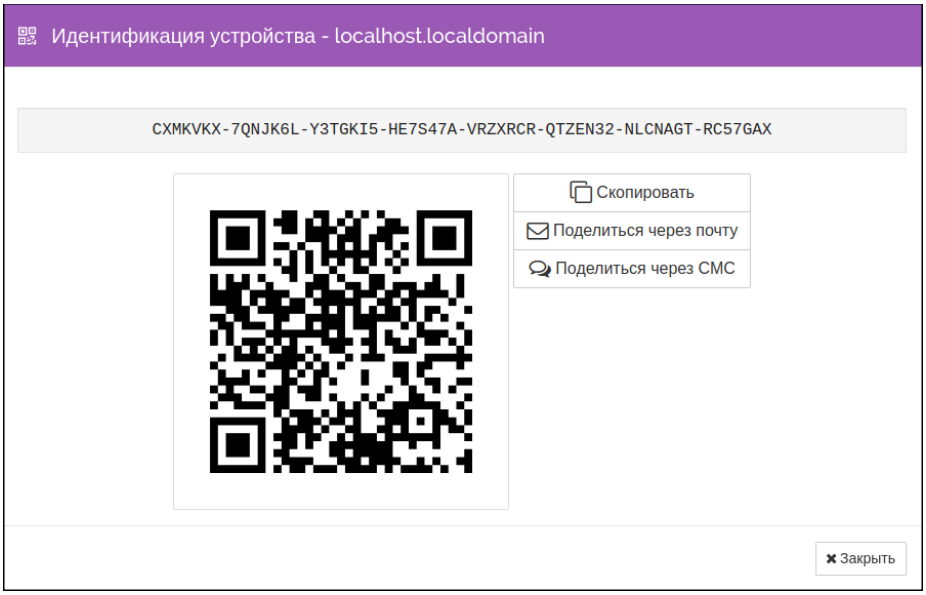
7. Перейдите в браузер. По умолчанию служба доступна по адресу: localhost:8384.



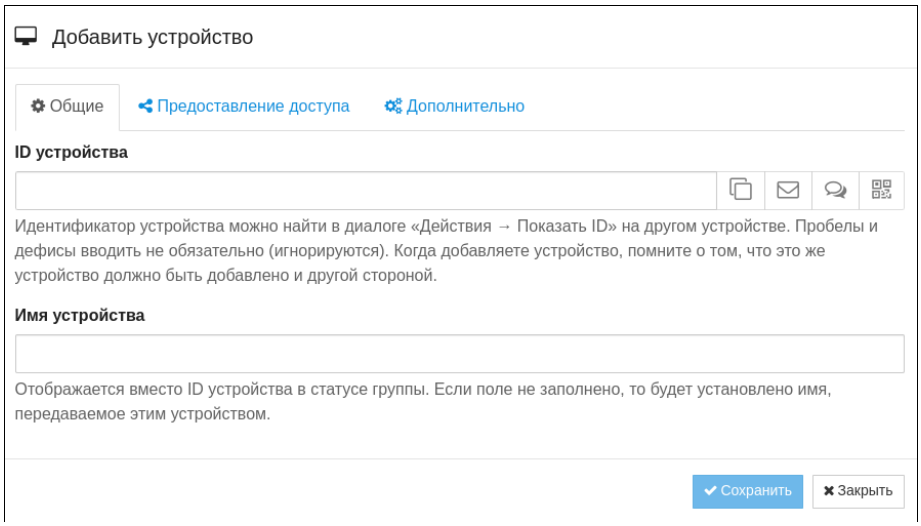
8. В целях безопасности обязательно установите имя пользователя и пароль для доступа к панели управления: «**Действия**» — «**Настройки**» — «**Интерфейс**».



9. Для добавления удаленного устройства определите его ID. Для этого на удаленном компьютере нажмите: «**Действия**» — «**Показать ID**».

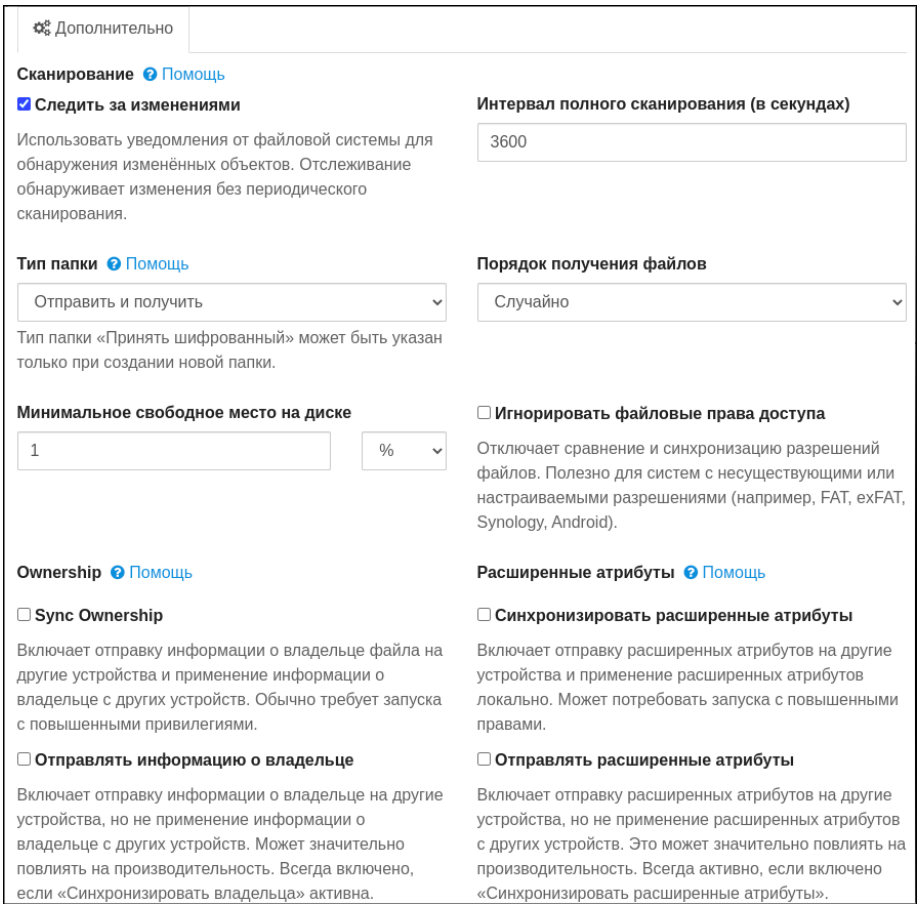


10. Укажите данные нового устройства в соответствующих полях на сервере и нажмите «**Сохранить**». После этого на удаленном устройстве появится запрос на добавление. Для связки двух устройств примите запрос.



По умолчанию создается общая папка ~/Sync. Для папок можно настроить разграничение доступа, управление версиями, шаблоны игнорирования, режим синхронизации (только принимать/отправлять или всё вместе) и другие. Программа способна сама найти кратчайший путь до удаленного устройства. Она может выполнять поиск в глобальной сети с помощью релеев или в локальной сети.

Можно настроить свой релей и не связываться с публичными серверами.



Burp - программа резервного копирования

Возможности
Установка
Синтаксис
Опции сервера
Опции клиента
Конфигурационные файлы
Запуск сервера
Создание и настройка клиента
Отключение клиента
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: burp-server-3.1.4-2, burp-client-3.1.4-2

Burp — это программа сетевого резервного копирования и восстановления данных. Она экономит сетевой трафик и объем пространства, используемого каждой резервной копией, с помощью *librsync*. Программа имеет клиент-серверную архитектуру. Сервер в **burp** представляет собой центральное хранилище резервных копий, а клиенты выполняют резервное копирование и восстановление данных через сервер.

С документацией можно ознакомиться на официальном сайте.

Возможности

Основные возможности **burp**:

- серверный режим;
- клиентский режим;
- дельта-дифференцирование с помощью *librsync*;
- сетевые резервные копии;
- ограничение скорости работы сети;
- создание резервных копий и восстановление файлов, каталогов, символических ссылок, жёстких ссылок, fifos, узлов, разрешений и временных меток;
- сжатие хранилища и сети с использованием zlib;
- возможность продолжения прерванного резервного копирования;
- шифрование связи между клиентом и сервером с помощью SSL;
- автоматическая подпись центра сертификации SSL и клиентского сертификата;
- шифрование файлов на стороне клиента;
- планирование;
- уведомления об успешном/неудачном резервном копировании по электронной почте;
- оперативный мониторинг ncurses на сервере;
- поддержка чтения/записи Fifo;
- клиентские скрипты до/после резервного копирования/восстановления;
- несколько периодов хранения;
- дедупликация данных хранилища;
- автоматическое обновление клиента.

Установка

Установить burp можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**burp**» и отметьте флагом пакеты **burp-client** и **burp-server** последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.

Для установки **burp-client** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install burp-client
```

Для установки **burp-server** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install burp-server
```

Установите зависимости:

```
sudo dnf install uthash-devel make gcc librsync-devel openssl-devel libacl-devel ncurses-devel zlib-devel autoconf automake libtool
```

Синтаксис

Программа доступна для запуска через терминал при помощи команды следующего вида:

```
burp [<опции>]
```

Опции сервера

Основные опции сервера:

- **-c <path>** — указать путь к файлу конфигурации (по умолчанию используется **/etc/burp/burp.conf)**;
- **-d <path>** — указать путь к клиенту в мониторе состояния;
- **-o <option>** — переопределить указанную конфигурационную опцию;
- **-F** — запустить сервер в режиме переднего плана (сервер перейдет в фоновый режим, если не указывать эту опцию);
- **-g** — сгенерировать исходные сертификаты центра сертификации и завершить работу;
- **-h** — вывести справку;
- **-i** — вывести индекс символов и завершить работу;
- **-n** — не создавать дочерних процессов (подразумевает -F);
- **-Q** — не выводить журналирование в stdout;
- **-t** — запустить проверку синтаксиса файла конфигурации (тестовый запуск);
- **-v** — вывести записи журнала в *stdout*;
- **-V** — вывести версию.

При использовании опции ''**-a c**'':

- **-C <client>** — запустить сервер, разделенный через подключение от клиента.

Опции клиента

Основные опции клиента:

- **-a <action>** — выбрать дополнительные действия:
    - **b** — создать резервную копию;
    - **delete** — удалить;
    - **d** — показать различия;
    - **e** — провести оценку;
    - **l** — показать список;
    - **L** — показать длинный список;
    - **m** — провести мониторинг интерфейса;
    - **p** — показать список в формате для парсинга;
    - **r** — восстановить;
    - **R** — восстановить (с учетом порядка путей из стандартного потока ввода);
    - **s** — монитор состояния;
    - **S** — снимок монитора состояния;
    - **t** — резервное копирование по времени;
    - **T** — проверить таймер резервного копирования;
    - **v** — проверить;
    - **V** — проверить (с учетом порядка путей из стандартного потока ввода);
- **-b <number>** — указать номер резервной копии, по умолчанию используется последняя;
- **-c <path>** — указать путь к файлу конфигурации, стандартно /etc/burp/burp.conf;
- **-d <directory>** — установить директорию для восстановления или просмотра;
- **-o <option>** — установить переопределение опции конфигурации;
- **-f** — установить разрешение на перезапись файлов при восстановлении;
- **-h** — вывести справку;
- **-i** — вывести индекс символов;
- **-q <max secs>** — установить задержку перед началом запланированного резервного копирования;
- **-Q** — отключить логирования в stdout;
- **-r|-R <regex>** — указать регулярное выражение для выбора файлов;

- **-s <number>** — удалить пути для использования при восстановлении;
- **-t** — проверить синтаксис файла конфигурации;
- **-V** — вывести версию программы;
- **-v** — вывести логи на стандартный вывод.

Дополнительные опции для использования с ''**-a S**'':

- **-C <client>** — отобразить информацию о клиенте;
- **-b <number>** — просмотреть файлы, доступные для списка в определенной резервной копии;
- **-d <path>** — просмотреть путь в резервной копии;
- **-l <path>** — файл лога для монитора статуса;
- **-z <file>** — вывести файл лога из резервной копии.

Конфигурационные файлы

Конфигурационные файлы и директории для программы **burp** играют ключевую роль в настройке процесса резервного копирования и восстановления.

В конфигурационном файле **/etc/burp/burp-server.conf** содержатся настройки сервера, такие как порт сервера, пути к директориям для хранения резервных копий и политики резервного копирования.

В папке **/etc/burp/clientconfdir/*** содержатся настройки резервного копирования для каждого клиента.

В конфигурационном файле **/etc/burp/burp.conf** содержатся настройки клиента для подключения к серверу. Директории для резервной копии указываются с помощью команды **include** в конфигурационном файле клиента: **/etc/burp/burp.conf**.

Резервные копии хранятся в папке **/var/spool/burp**.

Запуск сервера

Сервер **burp** используется для хранения резервных копий данных. Для запуска burp-сервера используйте команду (можно указывать свои конфигурационные файлы):

```
sudo burp -c /etc/burp/burp-server.conf
```

После выполнения команды сервер готов к подключению клиентов. Клиенты и сервер могут находиться как на одной машине, так и на разных.

Создание и настройка клиента

Клиенты отправляют свои данные на сервер для создания резервных копий и для восстановления информации в случае потери данных или необходимости восстановления системы.

Для создания клиента выполните следующий алгоритм действий:

1. Каждый клиент представлен файлом в каталоге **/etc/burp/clientconfdir** на сервере. Для добавления клиента с именем <имя_клиента> необходимо создать на сервере файл с именем **/etc/burp/clientconfdir/<имя_клиента>**.

```
nano /etc/burp/clientconfdir/<имя_клиента>
```

2. Задайте пароль клиенту в этом файле, добавив строку:

```
password = <пароль>
```

3. У клиента в файле **/etc/burp/burp.conf** в параметре **cname** укажите имя клиента, в параметре **password** — пароль, в параметре **server** — адрес сервера.

```
server = localhost:4971 password = <пароль> cname = <имя_клиента>
```

4. При первом подключении нового клиента к серверу он выполнит обмен SSL-сертификатами.

Отключение клиента

Для отключения клиента от сервера удалите файл **/etc/burp/clientconfdir/<имя_клиента>**:

```
rm /etc/burp/clientconfdir/<имя_клиента>
```

Примеры использования

1. Запустить резервное копирование:

```
sudo burp -a b
```

2. Вывести список резервных копий с датами:

```
sudo burp -a l
```

3. Показать файлы второй резервной копии:

```
sudo burp -a l -b 2
```

4. Восстановить все файлы из второй резервной копии в корневую папку:

```
sudo burp -a r -b 2 -d /
```

5. Восстановить файлы второй резервной копии, принудительно перезаписывая одноимённые файлы, в корневую папку:

```
sudo burp -a r -b 2 -d / -f
```

6. Восстановить файлы, которые соответствуют регулярному выражению "a_*" (начинаются на «a_»), из второй резервной копии в корневую папку:

```
sudo burp -a r -b 2 -r a_* -d /
```

7. Настройки резервного копирования очень разнообразные, можно исключать из резервной копии файлы, у которых путь соответствует регулярному выражению, или исключать файлы с заданными расширениями.

Можно настроить резервное копирование по расписанию с помощью crontab:

```
MAILTO="" 0,20,40 * * * * root /usr/sbin/burp -a b
```

После настройки каждые 20 минут будет производиться резервное копирование и отправляться сообщение владельцу файла *crontab*.

Создание бэкапов с помощью Butterfly Backup

Возможности
Установка
Синтаксис
Команды
Опции
Пример использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО**: butterfly-backup-1.12-2

Butterfly Backup — это инструмент для резервного копирования (РК), который использует **rsync** для синхронизации и сохранения файлов на сервере. Он обеспечивает гибкость в настройке заданий РК.

Butterfly Backup позволяет выполнять полные и инкрементные резервные копии, а также предоставляет возможность восстановления данных.

Возможности

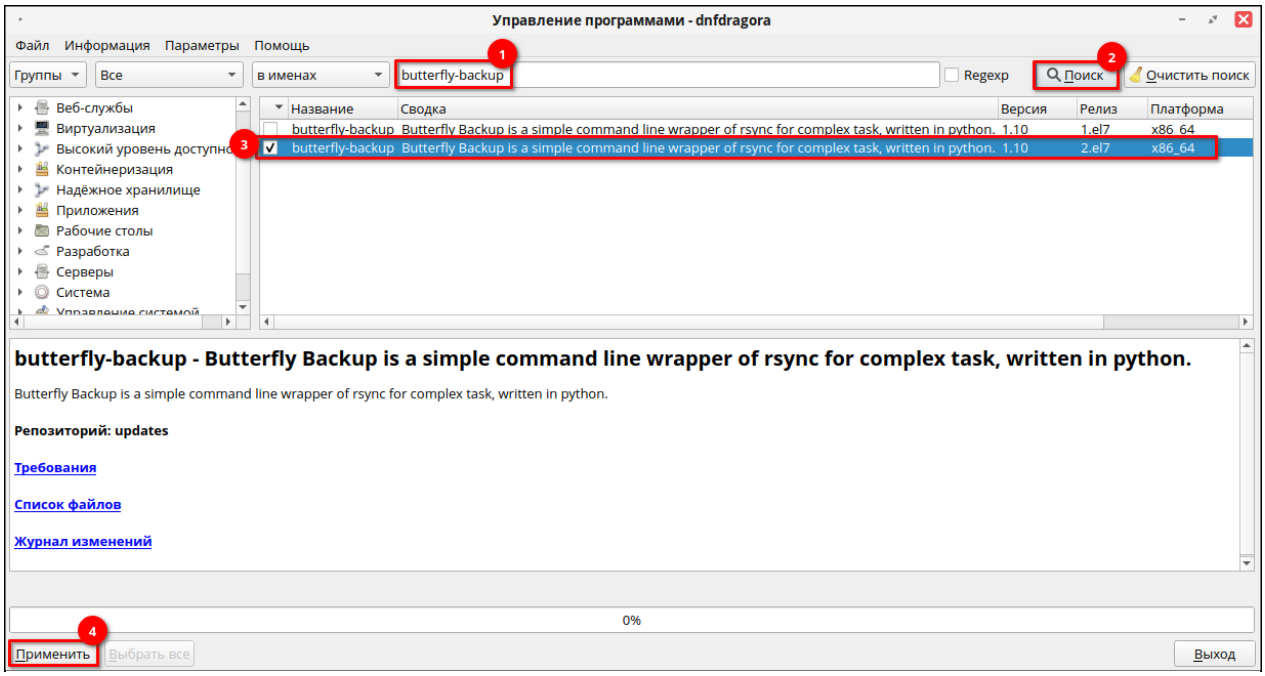
Основные возможности:

- **автоматизация заданий** — позволяет настроить автоматическое выполнение РК в определённое время с использованием cron или других планировщиков заданий;
- **управление версиями** — сохраняет историю изменений файлов, что позволяет восстановить предыдущие версии файлов при необходимости;
- **фильтрация данных** — предоставляет возможность исключать из РК определённые файлы или директории с помощью фильтров;
- **логирование** — записывает подробные логи операций, что облегчает отслеживание процесса РК и устранение возможных проблем;
- **централизованное хранение** — использует центральный сервер для сбора и хранения резервных копий от различных клиентов;
- **резервное копирование и восстановление системы** — позволяет выполнять РК всей системы и её восстановление на другом оборудовании или виртуальной машине;
- **просмотр содержимого резервных копий** — предоставляет возможность детально просматривать содержимое каждой резервной копии;
- **шифрование** — обеспечивает безопасность данных путём шифрования резервных копий перед их передачей на сервер или хранением.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**butterfly-backup**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install butterfly-backup
```

Для вывода справочной информации о доступных опциях и аргументах **butterfly-backup** воспользуйтесь командой:

```
bb --help
```

Для получения документации через man воспользуйтесь командой:

```
man bb
```

Синтаксис

Программа доступна для запуска через терминал при помощи команды следующего вида:

```
bb [<команды>] [<опции>]
```

Команды

Основные команды:

- **config** — настройка параметров конфигурации;
- **backup** — запуск процесса РК;
- **restore** — восстановление данных из резервной копии;
- **archive** — архивация, сжатие и упаковка данных для долгосрочного хранения;
- **list** — список доступных резервных копий или архивов;
- **export** — экспорт данных или настроек.

Опции

Опции команды config

Основные опции команды **config**:

Инициализация конфигурации:

- **--new, -n** — сгенерировать новую конфигурацию;
- **--remove, -r** — удалить существующую конфигурацию;
- **--init <каталог>, -i <каталог>** — изменить местоположение резервных копий;
- **--delete-host <каталог>, -D <каталог>** — удалить все записи для конкретного хоста в каталоге;
- **--clean <каталог>, -c <каталог>** — очистить каталог, если он поврежден, установив значения по умолчанию;
- **--delete-backup -b** — удалить определенный идентификатор РК из каталога.

Развертывание конфигурации:

- **--deploy <хост>, -d <хост>** — развернуть конфигурацию на удаленном хосте, указав его имя или IP-адрес;
- **--user <имя_пользователя>, -u <имя_пользователя>** — указать пользователя удаленного хоста.

Опции команды backup

Основные опции команды **backup**:

- **--computer <хост>, -c <хост>** — имя хоста или IP-адрес для РК;
- **--list <список>, -L <список>** — файл со списком удаленных хостов или IP-адресов для резервного копирования;
- **--destination <каталог>, -d <каталог>** — каталог назначения для РК;
- **--mode <значение>** — режим РК. Возможные значения:
  - **full** — полное резервное копирование;
  - **incremental** — добавочное РК выполняется на основе последней резервной копии;
  - **differential** — добавочное РК выполняется на основе последней полной резервной копии;
  - **mirror** — режим зеркалирования, при котором структура каталогов источника будет точно воспроизведена в пункте назначения.
- **--data <значение>, -D <значение>** — тип данных для РК. Возможные значения:
  - **user** — пользовательские данные;
  - **config** — конфигурационные файлы;
  - **log** — журналы;
  - **application** — данные приложений;
  - **system** — система.
- **--custom-data <путь>, -D <путь>** — пользовательский каталог для РК;
- **--user <имя_пользователя>, -u <имя_пользователя>** — имя пользователя для авторизации на удаленном хосте;
- **--type <тип_ОС>, -t <тип_ОС>** — тип операционной системы для РК. Возможные значения:
  - **unix** — все ос UNIX (Linux, BSD, Solaris);
  - **windows** — Windows Vista или более поздней версии;
  - **macos** — MacOSX 10.8 или выше.
- **--compress, -z** — сжимать данные;
- **--retention [<дни> [<количество>], -r [<дни> [<количество>]** — период хранения резервных копий (в днях) и минимальное количество хранимых резервных копий;
- **--parallel <количество>, -p <количество>** — количество параллельных заданий;
- **--timeout <значение>**, **-T <значение>** — задержка ввода/вывода в секундах;
- **--skip-error**, **-e** — пропускать ошибки;
- **--rsync-path <путь>, -R <путь>** — пользовательский путь для РК;
- **--bwlimit, -b** — ограничение пропускной способности в КБ/с;
- **--ssh-port, -P** — пользовательский SSH-порт;
- **--exclude <шаблон>, -E <шаблон>** — шаблон для исключения файлов;

- **--start-from <ID>, -s <ID>** — новая резервная копия на основании другой резервной копии по ее ID.

Опции команды restore

Основные опции команды **restore**:

- **--catalog <каталог>, -C <каталог>** — указать каталог, где хранятся резервные копии;
- **--backup-id <ID>, -i <ID>** — указать ID резервной копии для восстановления;
- **--last, -L** — использовать последнюю доступную резервную копию;
- **--user <имя_пользователя>, -u <имя_пользователя>** — имя пользователя для авторизации на удаленном хосте, где происходит восстановление;
- **--computer <имя_хоста>, -c <имя_хоста>** — указать имя хоста или IP-адрес для выполнения восстановления;
- **--type <тип_ОС>** — указать тип операционной системы для выполнения восстановления: Unix, Windows или MacOS;
- **--timeout <значение>, -T <значение>** — указать задержку ввода/вывода в секундах;
- **--mirror, -m** — режим зеркалирования, при котором структура каталогов источника будет точно воспроизведена в пункте назначения;
- **--skip-error, -e** — пропускать ошибки;
- **--rsync-path <путь>, -R <путь>** — пользовательский путь к резервной копии;
- **--bwlimit, -b** — ограничение пропускной способности в КБ/с;
- **--ssh-port, -P** — указать пользовательский SSH-порт;
- **--exclude <шаблон>, -E <шаблон>** — указать шаблон для исключения файлов;
- **--files <файлы>, -f <файлы>** — восстанавливать только указанные файлы.

Опции команды archive

Основные опции команды **archive:**

- **--catalog <каталог>, -C <каталог>** — каталог с резервной копией;
- **--days <дни>, -D <дни>** — количество дней для хранения архива;
- **--destination <каталог>, -d <каталог>** — каталог назначения для архива.

Опции команды list

Основные опции команды **list**:

- **--catalog <каталог>, -C <каталог>** — отобразить список резервных копий из указанного каталога;
- **--backup-id <ID>, -i <ID>** — выводить ID резервной копии;
- **--archived, -a** — показывать только архивированные резервные копии;
- **--cleaned, -c** — отобразить только очищенные резервные копии;
- **--computer <имя_хоста>, -H <имя_хоста>** — выводить только совпадающие имена хоста или IP-адреса;
- **--detail <ID>, -d <ID>** — отобразить подробную информацию о файлах и папках для указанного ID резервной копии;
- **--oneline, -o** — выводить информацию в одной строке.

Опции команды export

Основные опции команды **export:**

- **--catalog <каталог>, -C <каталог>** — каталог с резервной копией;
- **--backup-id <ID>, -i <ID>** — идентификатор конкретной резервной копии для экспорта;
- **--all, -A** — экспортирует все резервные копии;
- **--destination <каталог>, -d <каталог>** — каталог назначения, куда будут экспортированы данные;

- **--mirror, -m** — режим зеркалирования, при котором структура каталогов источника будет точно воспроизведена в пункте назначения;
- **--cut, -c** — удалить исходные данные после экспорта;
  --include <шаблон>, -I <шаблон> — паттерны включения определенных файлов или каталогов в экспорт;
- **--exclude <шаблон>, -E <шаблон>** — паттерны исключения определенных файлов или каталогов из экспорта;
- **--timeout <значение> , -T <значение>** — задержка ввода/вывода в секундах;
- **--skip-error, -e** — пропускать ошибки во время экспорта;
- **--rsync-path <путь>, -R <путь>** — пользовательский путь для экспорта;
- **--bwlimit, -b** — ограничение пропускной способности в КБ/с;
- **--ssh-port, -P** — пользовательский порт SSH для подключения.

Дополнительные опции

Дополнительные опции:

- **-h, --help** — отобразить справку;
- **--verbose, -v** — включить подробный режим;
- **--log, -l** — создать журналы логов;
- **--dry-run, -N** — режим предварительного запуска;
- **-version, -V** — показать версию.

Пример использования

Рассмотрим настройку сервера и удаленного хоста для создания РК с помощью **bb**.

1. Генерация SSH ключей. Сгенерируйте пару ключей:

```
ssh-keygen -t rsa Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa
Your public key has been saved in /home/user/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:7L7L6TLN6Lqj6L7PLkLVLPL/LDLFL/iaLA9Bc user@localhost.localdomain
```

В процессе генерации SSH ключей будут заданы следующие вопросы:

- **Enter file in which to save the key (/home/user/.ssh/id_rsa)**: укажите, куда сохранить файл закрытого ключа. По умолчанию он будет сохранен в папку **~/.ssh** с именем **id_rsa**. Имя файла можно изменить.
- **Enter passphrase (empty for no passphrase)**: установите пароль для ключа. Пароль используется для дополнительной защиты ключа. Если пароль не требуется, нажмите Enter.
- **Enter same passphrase again**: если пароль был задан, его необходимо повторить, чтобы избежать возможных опечаток.

2. Передача **SSH-ключей на удаленный хост.** После генерации ключей необходимо передать открытый ключ на удаленный хост. Для этого выполните команду вида:

```
bb config --deploy <IP-адрес> --user <имя_пользователя>
```

где:

<IP-адрес> — IP-адрес удаленного хоста;

<имя_пользователя> — имя пользователя, с правами которого будет выполняться РК.

```
 bb config --deploy 192.168.2.15 --user userCopying configuration to 192.168.2.15; write the password:
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/id_rsa.pub"
The authenticity of host ' 192.168.2.15 (192.168.2.15)' can't be established.
ED25519 key fingerprint is SHA256:PK4OB5HgQpPel67ag9bvi2YgVpD1xalayo/A.
```

```
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
user@192.168.2.15's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'user@192.168.2.15'"
and check to make sure that only the key(s) you wanted were added.success: Configuration copied successfully on 192.168.2.15!
```

3. Резервное копирование домашнего каталога пользователя. В качестве примера создайте резервную копию каталога /home на удаленном хосте <IP-адрес> от имени пользователя user. Убедитесь, что каталог ~/backups существует, или создайте его перед выполнением команды.

```
bb backup --computer 192.168.2.15 --data user --type unix --destination ~/backups --user user# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
Start backup  192.168.2.15success: Command rsync -ah --no-links user@192.168.2.15:/home /backups/192.168.2.15/2024_08_27__15_54
```

4. Просмотр списка резервных копий. Для просмотра списка резервных копий используйте следующую команду, заменив ~/backups на фактический путь к папке резервных копий:

```
bb list --catalog ~/backups BUTTERFLY BACKUP CATALOG

Backup id: f0e0b12c-656d-11ef-beea-080027d4cbd8
Hostname or ip:  192.168.2.15
Timestamp: 2024-08-28 21:47:13

Backup id: 0f442602-656f-11ef-83c6-080027d4cbd8
Hostname or ip:  192.168.2.15
Timestamp: 2024-08-28 21:55:14

(END)
```

5. Для получения подробной информации о резервной копии используйте команду:

```
bb list --catalog ~/backups --backup-id f0e0b12c-656d-11ef-beea-080027d4cbd8 Backup id: f0e0b12c-656d-11ef-beea-080027d4cbd8
Hostname or ip:  192.168.2.15
Type: full
Timestamp: 2024-08-28 21:47:13
Start: 2024-08-28 21:47:13
Finish: 2024-08-28 21:47:28
OS: unix
ExitCode: 0
Path: /home/user/backups/ 192.168.2.15/2024_08_28__21_47
List: home
```

где:

- f0e0b12c-656d-11ef-beea-080027d4cbd8 — это идентификатор РК, который был получен на предыдущем шаге.

6. Для просмотра файлов в конкретной РК используйте команду:

```
bb list --catalog ~/backups --detail f0e0b12c-656d-11ef-beea-080027d4cbd8
```

7. Для восстановления файлов из определённой резервной копии, используйте команду:

```
bb restore --catalog ~/backups --last --user user --computer 192.168.2.15 --type unix--verbose debug: Build a rsync command
debug: Command flags are: rsync -ahu --no-perms --no-owner --no-group -vP --log-file=/home/user/backups/
192.168.2.15/2024_08_28__21_47/restore.log
Want to do restore path /home/user/backups/192.168.2.15/2024_08_28__21_47/home/*?
To continue? [y/N] y
Start restore  192.168.2.15
debug: rsync command: rsync -ahu --no-perms --no-owner --no-group -vP --log-
file=/home/user/backups/192.168.2.15/2024_08_28__21_47/restore.log /home/user/backups/192.168.2.15/2024_08_28__21_47/home/*
```

```
user@192.168.2.15:/home
 sending incremental file list
 user/.cache/
 user/.config/
 user/.local/share/

 sent 269,43K bytes  received 711 bytes  180,09K bytes/sec
 total size is 891,06M  speedup is 3.298,53
 success: Command rsync -ahu --no-perms --no-owner --no-group -vP --log-
file=/home/user/backups/192.168.2.15/2024_08_28__21_47/restore.log /home/user/backups/192.168.2.15/2024_08_28__21_47/home/* user@
192.168.2.15:/home
```

8. Для архивации старых резервных копий, которые старше определённого количества дней, используйте:

```
bb archive --catalog ~/backups --days 365 --destination
```

9. Для копирования всех резервные копий в другую папку используйте:

```
bb export --catalog <каталог_с_РК> --all --destination <каталог_для_экспорта> Start export all_backup success: Command rsync -
ahu --no-perms --no-owner --no-group --safe-links /home/user/backups/ /home/user/backups1
```

Rescuezilla - программа для создания и восстановления резервных копий

Установка
Создание резервной копии
Восстановление резервной копии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: rescuezilla-2.4.2-64bit

Rescuezilla – программное обеспечение для резервного копирования и восстановления случайно удалённых файлов в разделах операционной системы. Поддерживает выполнение автоматического поиска и подключения сетевых разделов, которые можно использовать для размещения резервных копий.

Графический интерфейс программы основан на оболочке **LXDE**. Формат создаваемых резервных копий полностью совместим с дистрибутивом Clonezilla.

При восстановлении поддерживается работа с образами *Clonezilla*, *Redo Rescue*, *Foxclone* и *FSArchiver*.

Установка

Скачайте образ **Rescuezilla** командой:

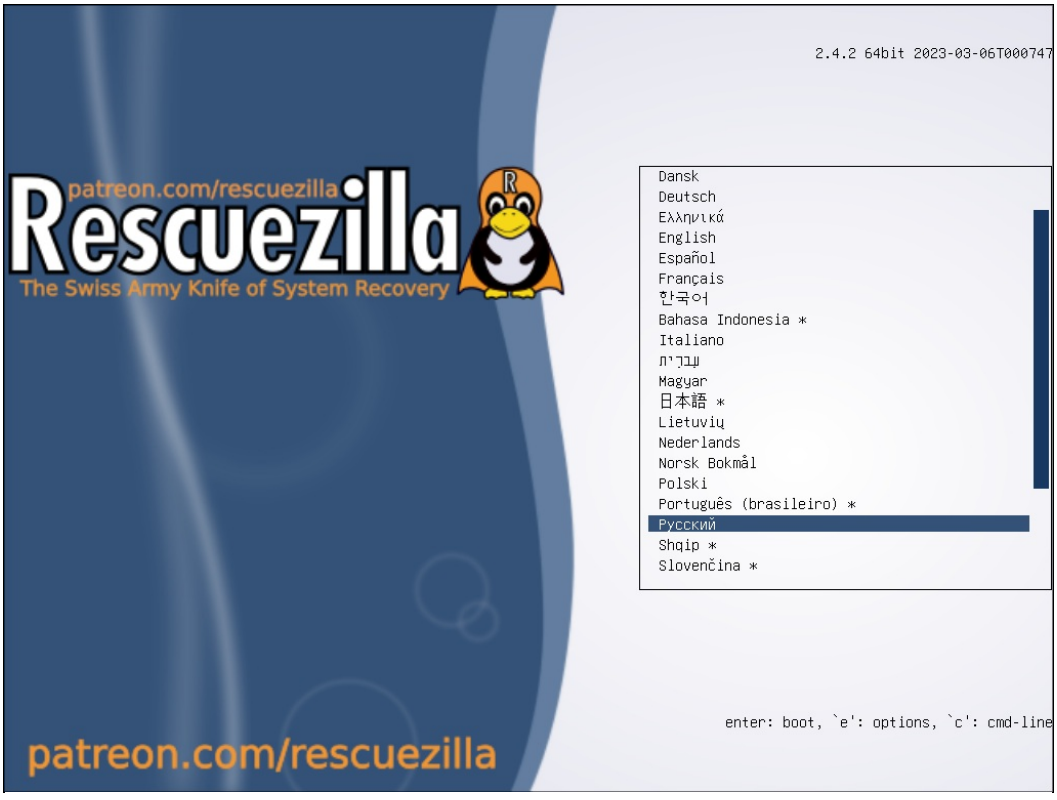
```
wget https://github.com/rescuezilla/rescuezilla/releases/download/2.4.2/rescuezilla-2.4.2-64bit.jammy.iso
```

Запишите образ на носитель. Рекомендуется использовать balenaEtcher.

Создание резервной копии

Загрузитесь с носителя, на который был записан образ **Rescuezilla**.

Выберите необходимый язык интерфейса.

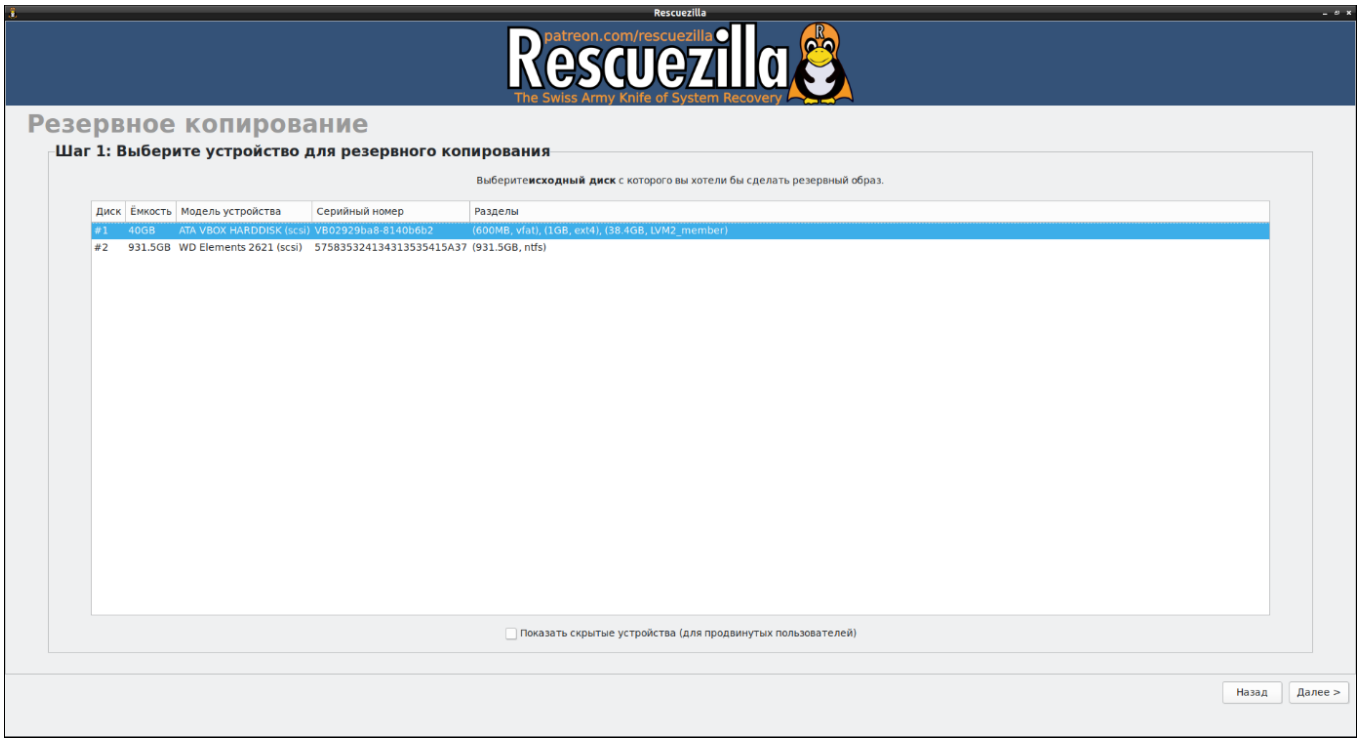


Сразу после загрузки рабочего стола откроется программа **Rescuezilla**.



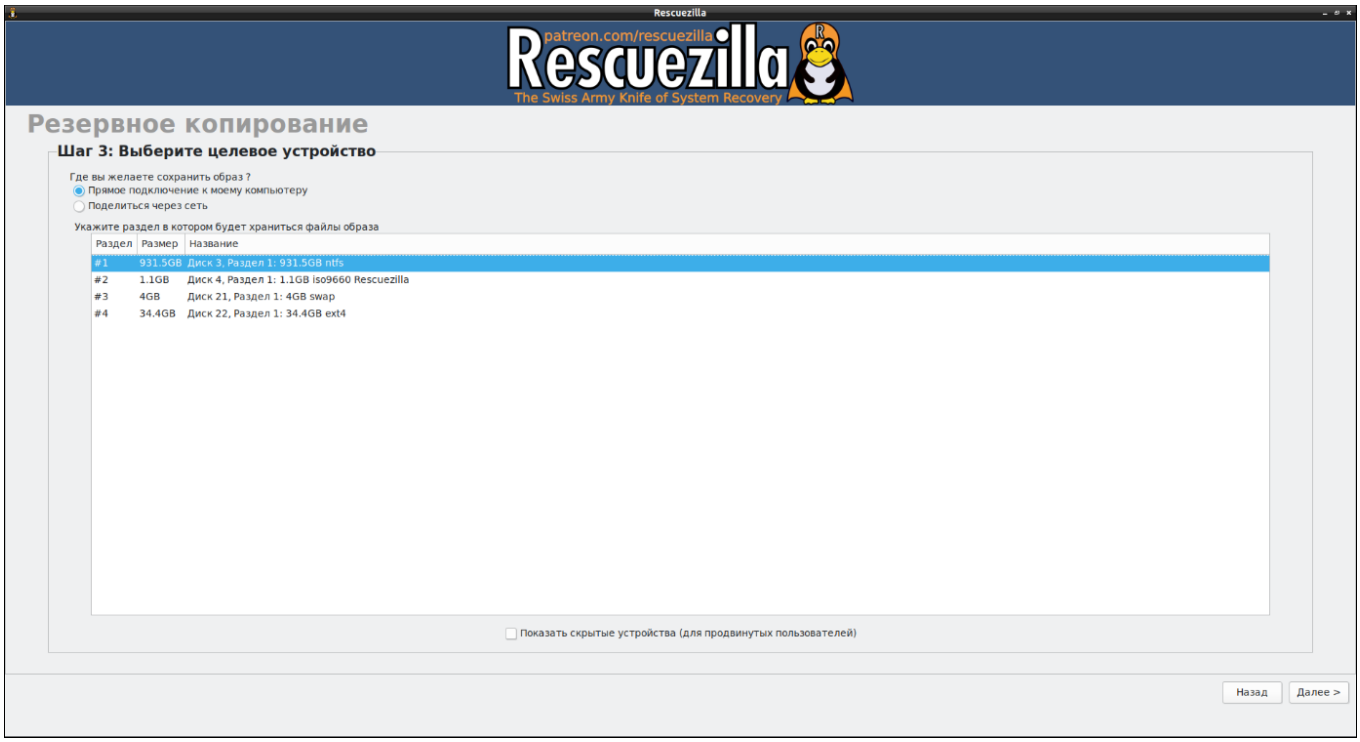
Для создания резервной копии нажмите «**Резервное копирование**».

Выберите диск и разделы на нем, которые необходимо включить в резервную копию.





Выберите диск, на который будет сохранена резервная копия.



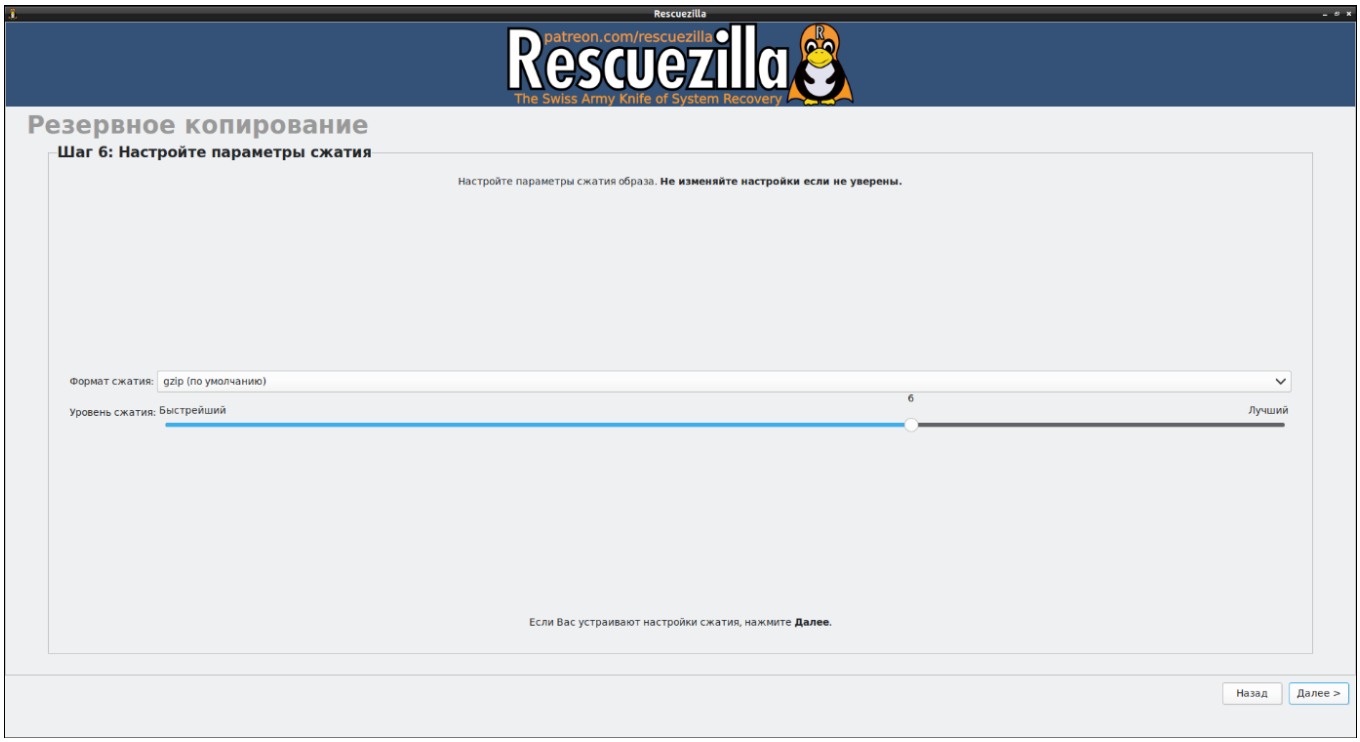
Укажите каталог хранения резервной копии.



Укажите название создаваемой резервной копии.



Определите параметры сжатия. Можно оставить настройки по умолчанию.



Проверьте указанные параметры и, если все указано верно, подтвердите изменения, нажав «**Далее**». В противном случае нажмите «**Назад**» для редактирования необходимых параметров.

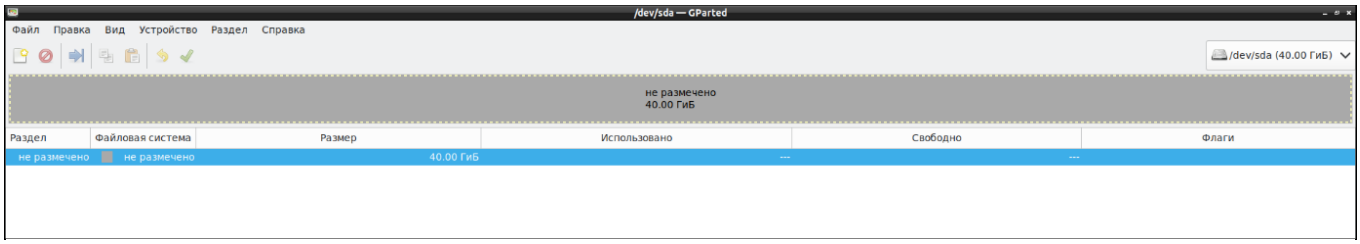


Начнется процесс резервного копирования. По завершении создания резервной копии будет выведено соответствующее сообщение.



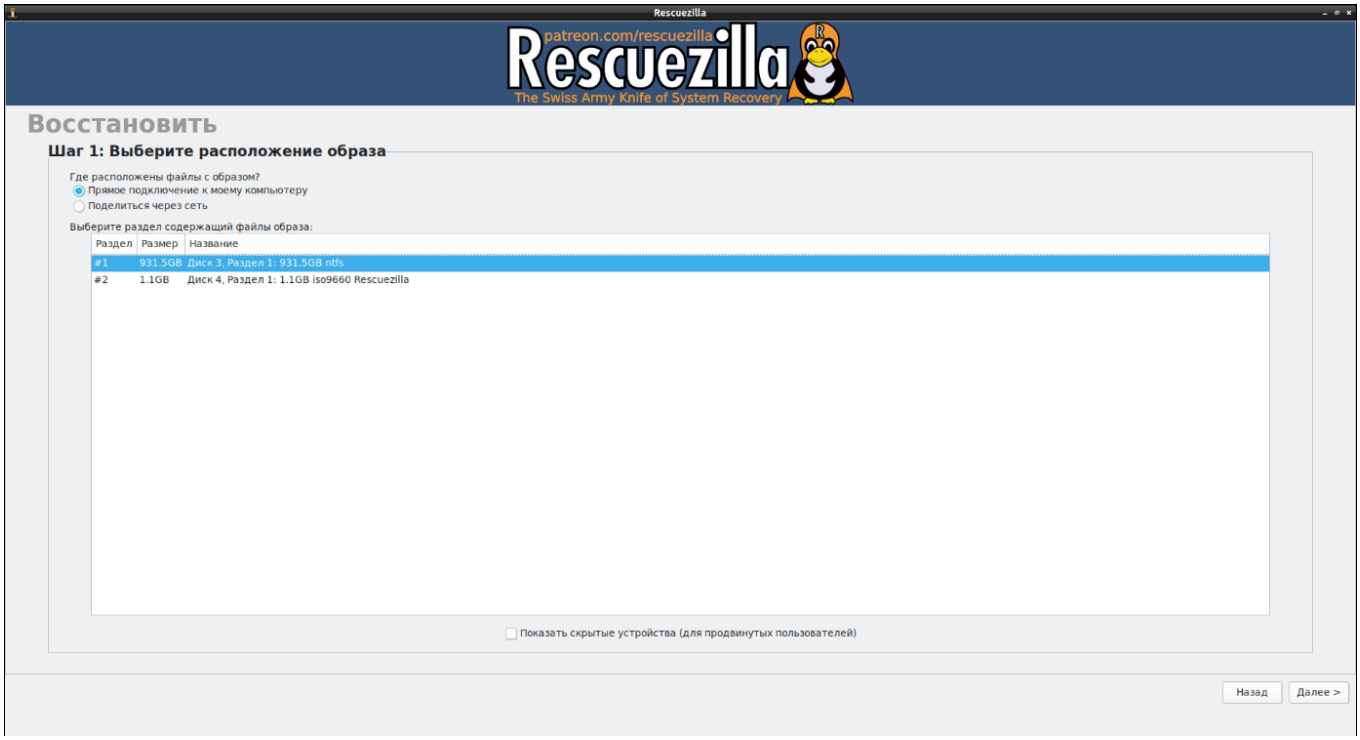
Восстановление резервной копии

Для примера будут удалены все разделы на системном диске через GParted.

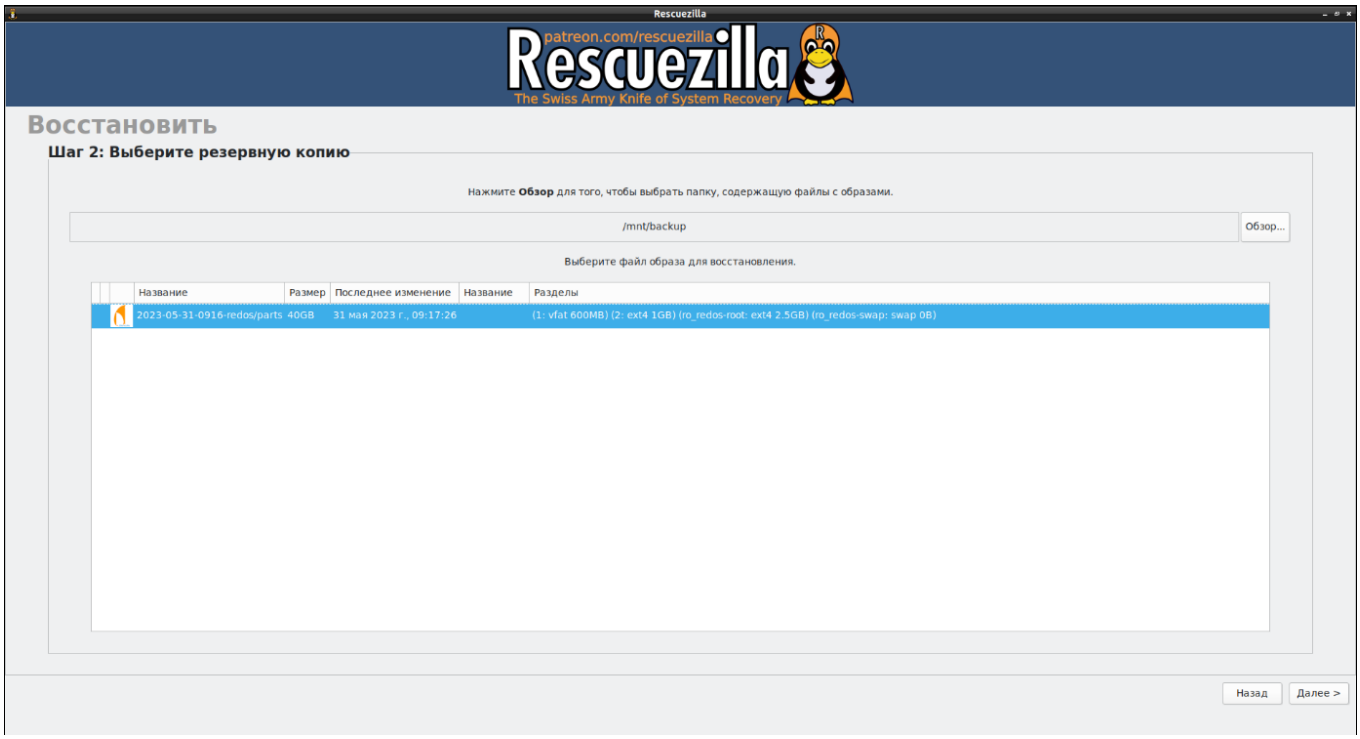


Откройте программу **Rescuezilla** и нажмите «**Восстановить**».

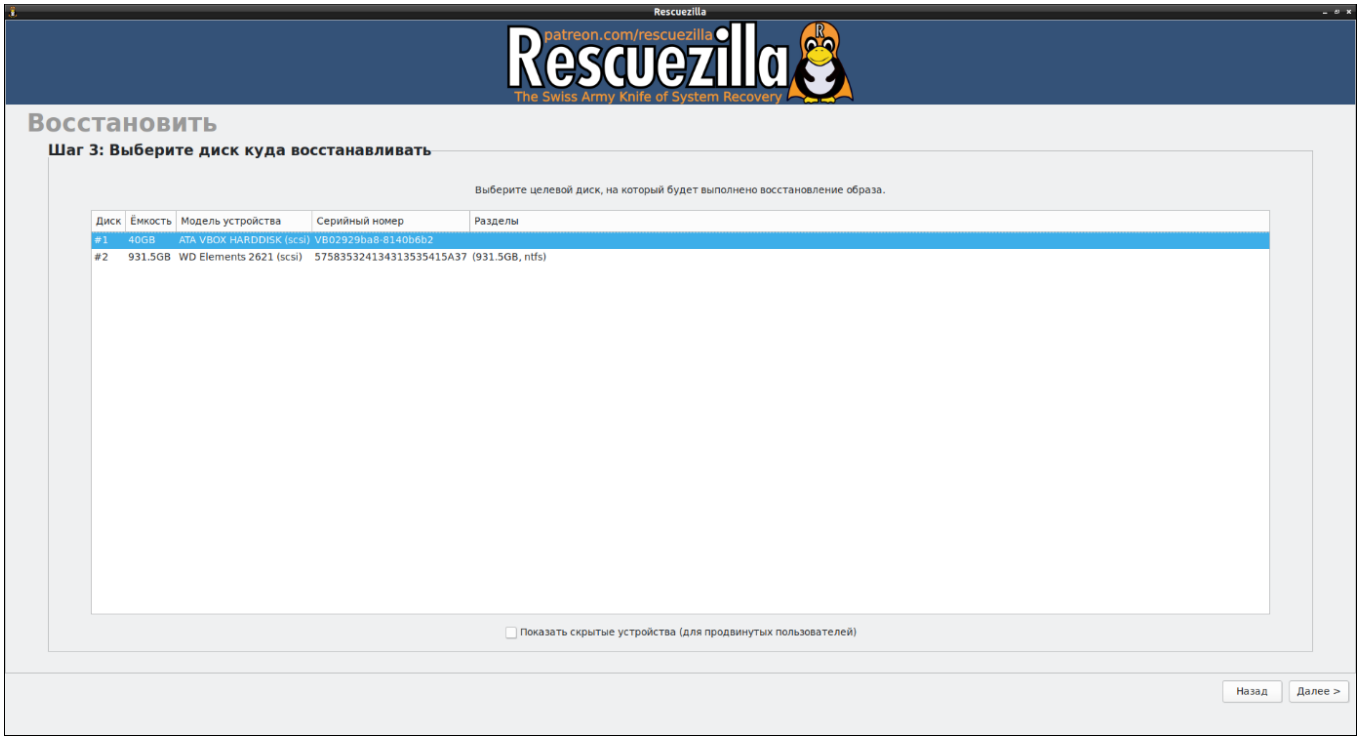
Укажите раздел, содержащий резервную копию.



Укажите каталог с сохраненной резервной копией и выберите ее.



Укажите диск, на который необходимо восстановить данные.



Укажите разделы, которые необходимо восстановить, и требуется ли перезаписать таблицу разделов.



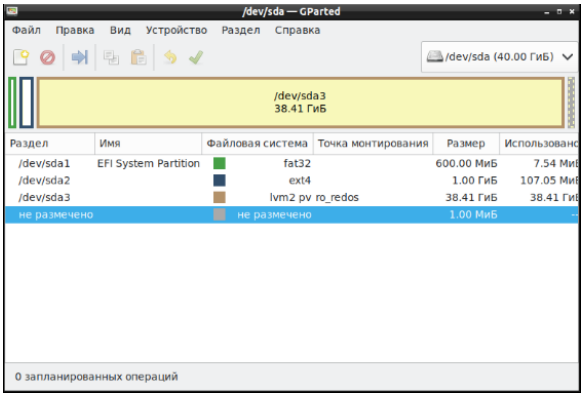
Проверьте указанные параметры и, если все указано верно, подтвердите изменения, нажав «**Далее**». В противном случае нажмите «**Назад**» для редактирования необходимых параметров.



Начнется процесс восстановления резервной копии. По завершении восстановления резервной копии будет выведено соответствующее сообщение.



Для проверки восстановления удаленных разделов откройте **GParted**.

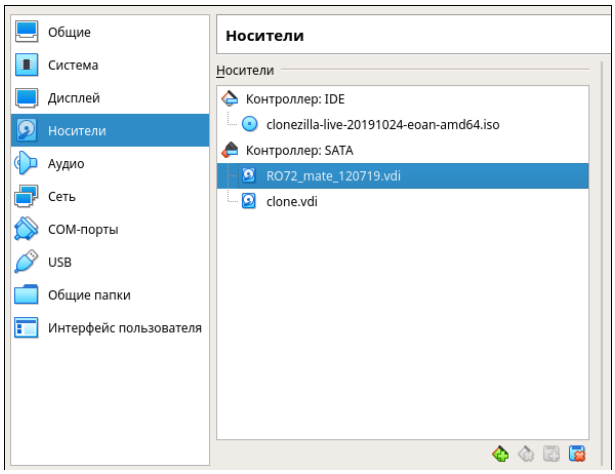


Системный диск успешно восстановлен.

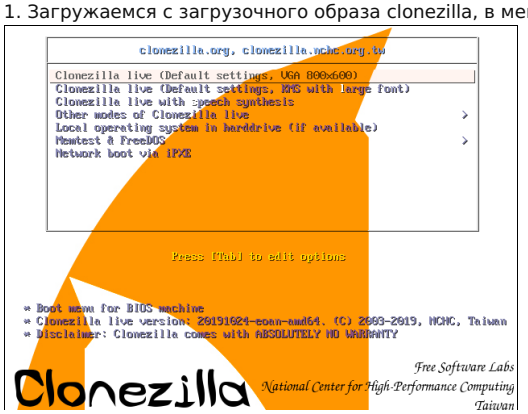
Локальное клонирование жесткого диска

СОЗДАНИЕ ОБРАЗА СИСТЕМЫ

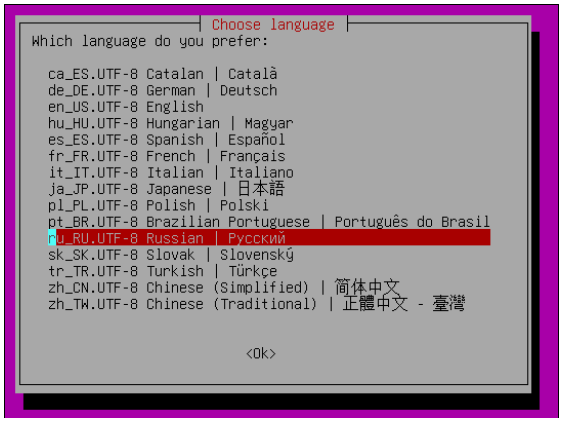
Для примера в VirtaulBox создан дополнительный диск clone.vdi на которой будет сохранен образ системы с помощью clonezilla для последующего восстановления. Вместо этого диска можно использовать Flash-накопитель.



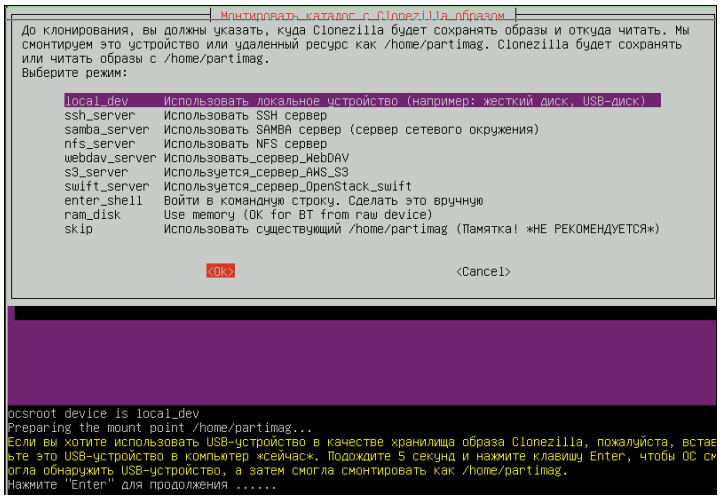
1. Загружаемся с загрузочного образа clonezilla, в меню загрузки выбрав первый пункт.



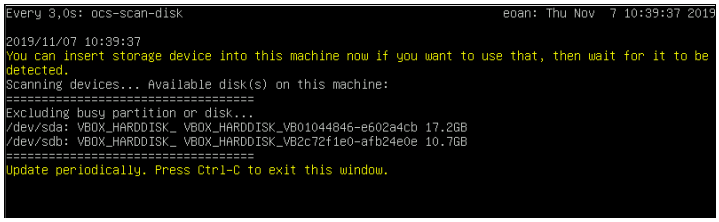
Программа предложит выбрать язык интерфейса



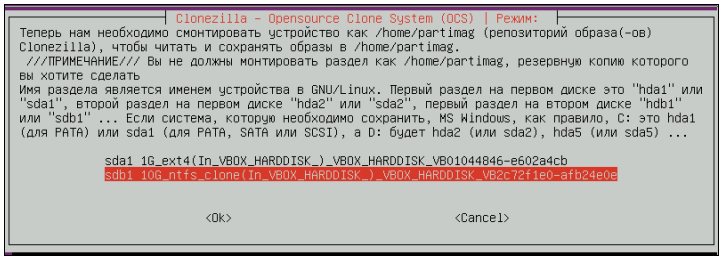
Выбираем место куда будет сохранен образ системы.
Выбираем режим для работы с диском.



Для продолжения нажмите Enter. Далее нажмите ctrl+c



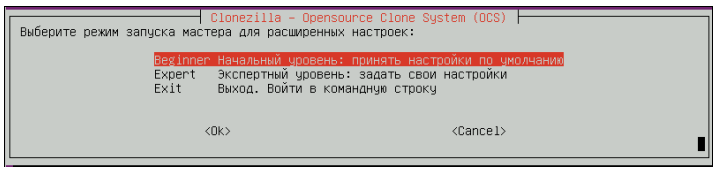
Выбираем диск на который будет сохранен образ, в нашем случае это второй подключенный диск.



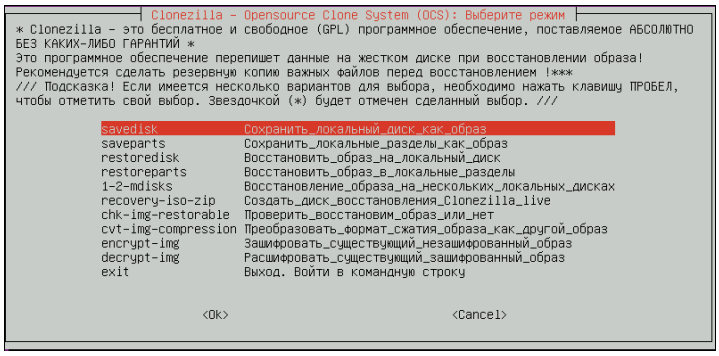
Здесь происходит выбор директории для сохранения образа, т.к диск пустой, сохраним образ в корень.



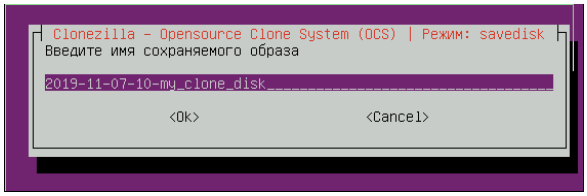
Нажмите «Done»
Режим мастера клонирования, оставим Beginner.



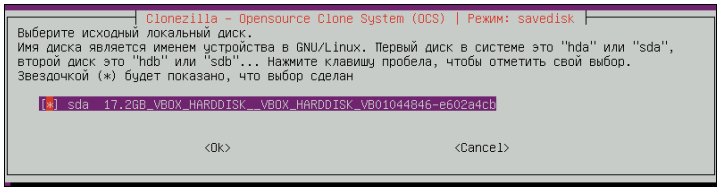
Выбираем необходимое действие, нас интересует «Сохранить локальный диск как образ»



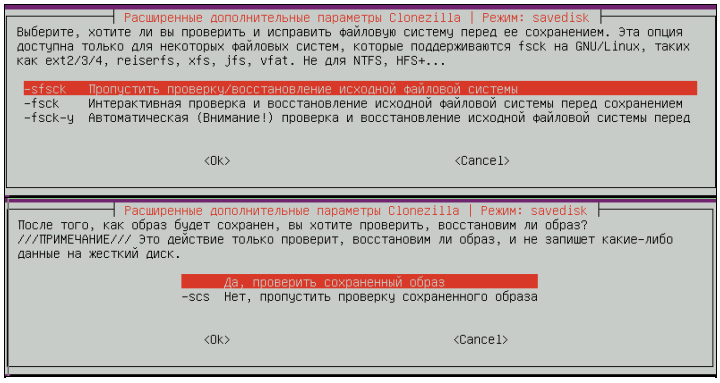
Далее предлагается ввести имя образу диска



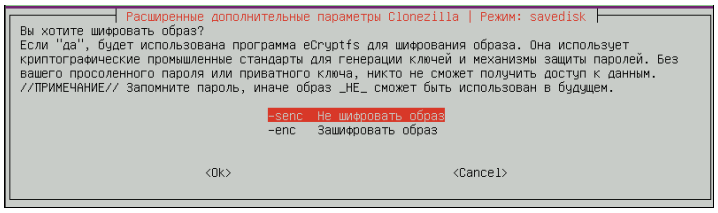
Укажите диск для клонирования



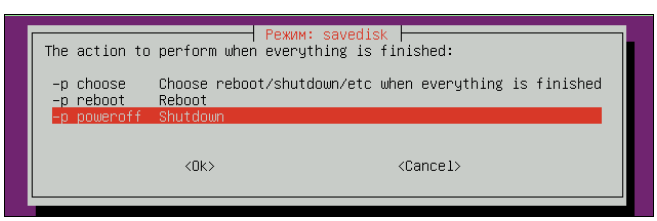
Далее предлагается проверить и исправить файловую систему перед началом клонирования диска.



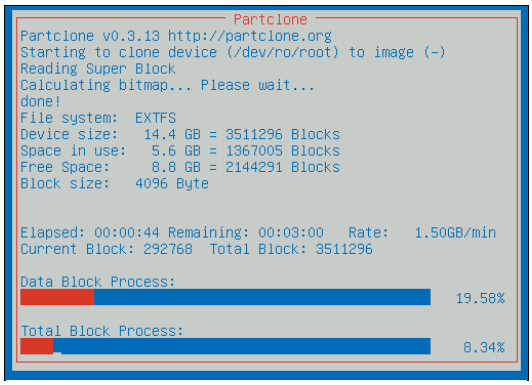
Имеется возможность зашифровать образ.



На следующем шаге предлагается запланировать действие после завершения клонирования, выберете необходимое

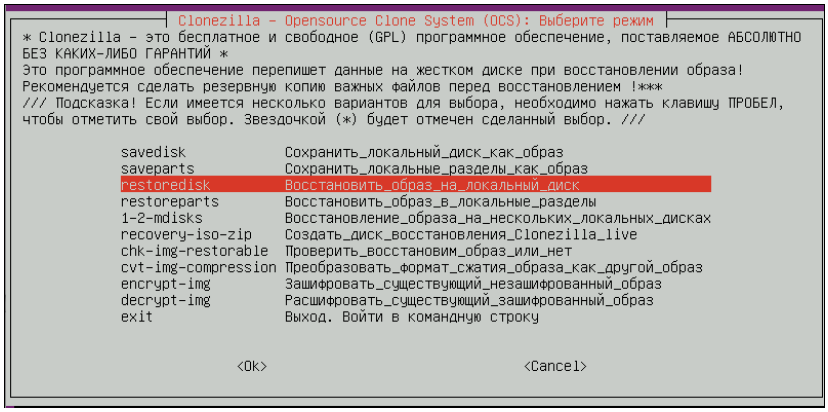


После этого начнется процесс клонирования

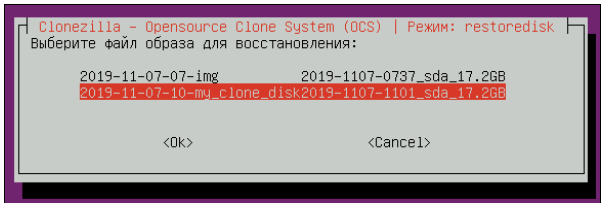


ВОССТАНОВЛЕНИЕ ОБРАЗА СИСТЕМЫ

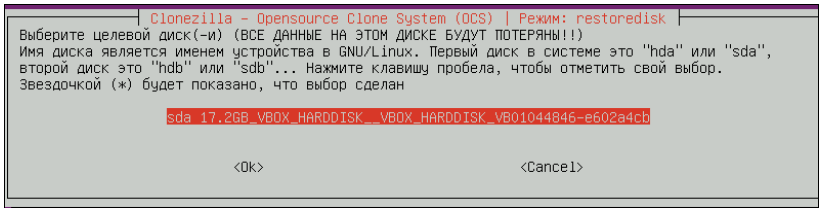
Для восстановления необходимо пройти те же шаги как и в начале клонирования, но дойдя до пункта, где выбирается сохранение и восстановление образов необходимо выбрать «Восстановить образ на локальный диск»



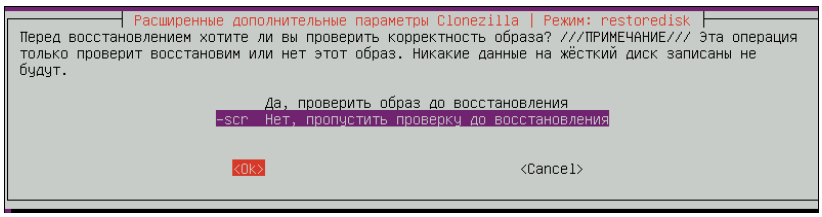
Выбираем файл образа для восстановления



Указываем физический диск на который будет разворачиваться образ



Предлагается проверить образ на ошибки



После этого начнется восстановление образа на диск.
После того, как система восстановится, загрузите РЕД ОС и выполните команду от пользователя root:

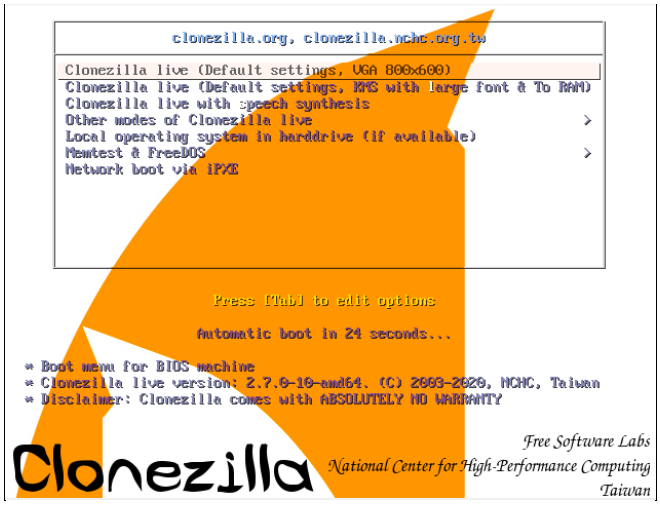
```
dracut -f -v
```

это необходимо для того, чтобы избежать возможных ошибок при использовании функции спящего режима в РЕД ОС.

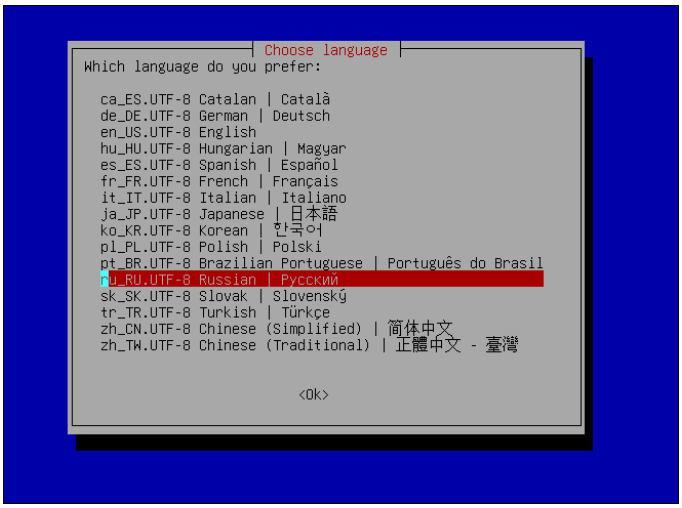
Клонирование жесткого диска на SAMBA-сервер

Создание образа системы

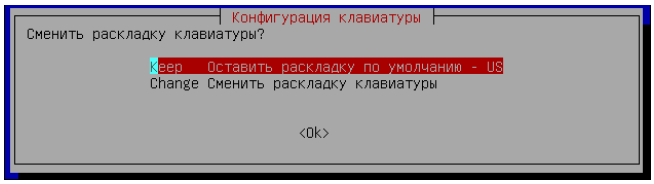
1. Необходимо загрузиться с загрузочного образа **clonezilla**. На экране появится окно загрузчика. В нем необходимо выбрать первый пункт. Для подтверждения выбора следует нажать «**Enter**».



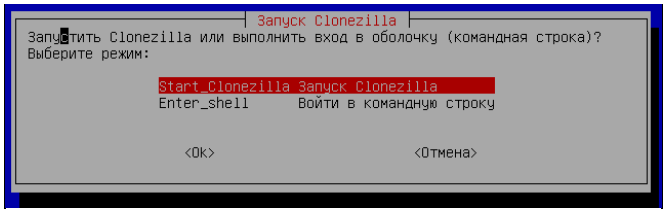
2. Затем программа предложит выбрать язык интерфейса.



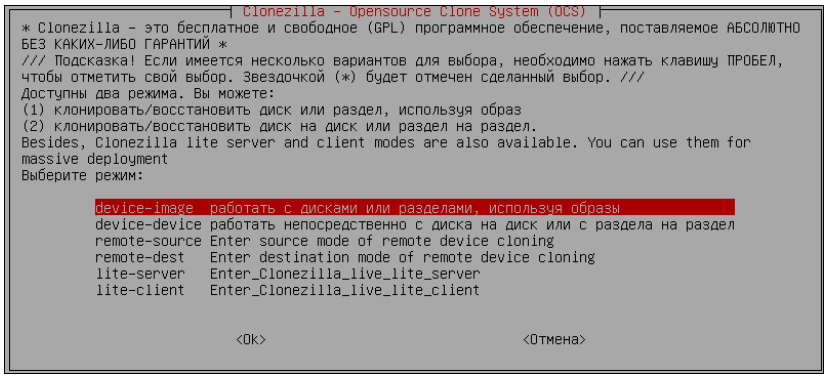
3. Далее программа предлагает сменить раскладку клавиатуры.



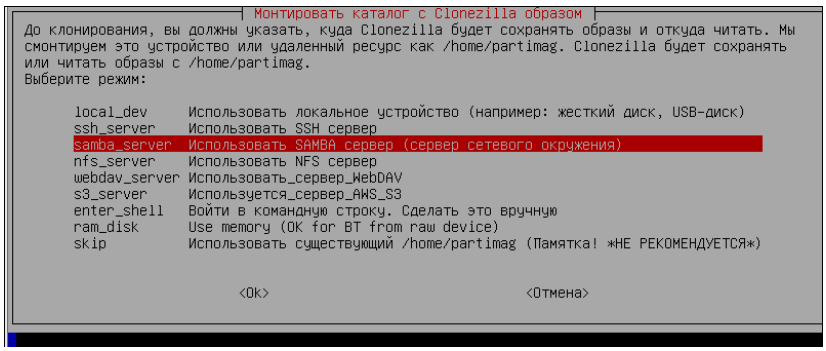
4. В следующем окне предлагается запустить **Clonezilla** или перейти в командную строку. Выберите вариант «**Start_Clonezilla**».



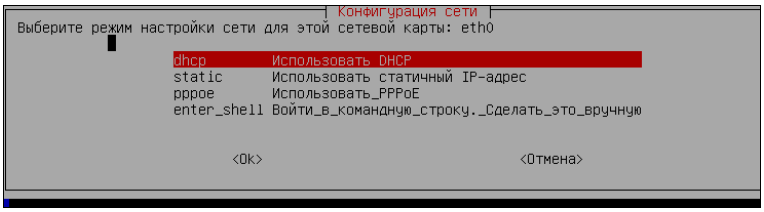
5. Затем необходимо настроить режим для работы с диском. Выберите пункт «**device-image**».



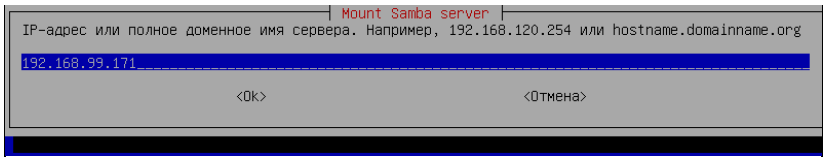
6. Местом сохранения образа в данном случае выберите «**samba_сервер**».



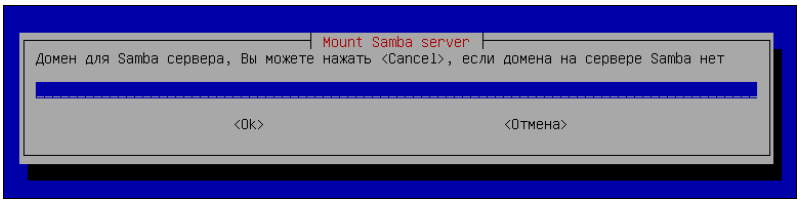
7. Далее выберите режим настройки сети — «**dhcp**».



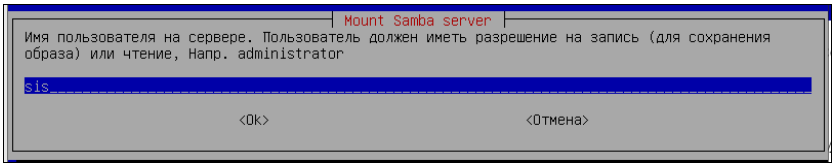
8. После выбора режима сети необходимо ввести *IP-адрес* или *полное имя* Samba-сервера.



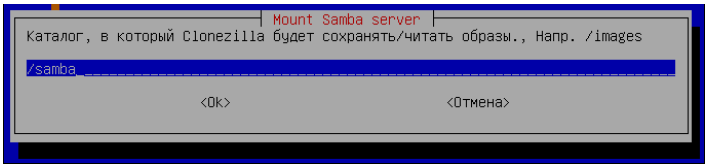
9. Затем требуется ввести домен для Samba-сервера. Однако если домена нет, нужно нажать «**Отмена**».



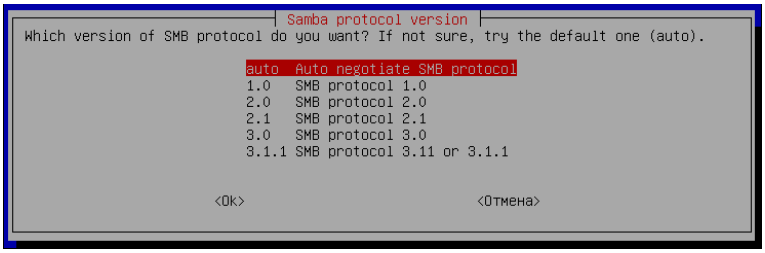
10. Далее нужно ввести *имя пользователя* Samba-сервера.



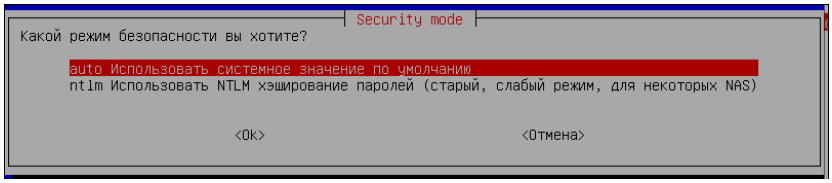
11. Определите *каталог*, в который будете сохранять/читать образы, введите его *название*.



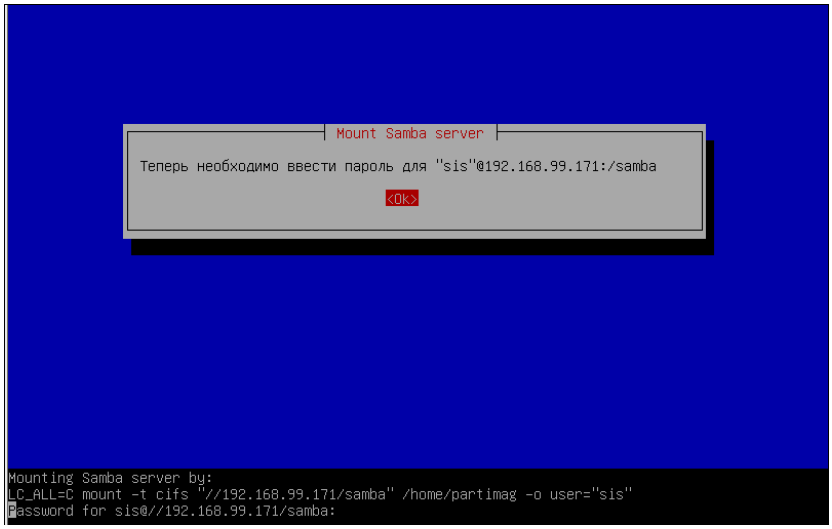
12. Затем необходимо выбрать версию протокола **SMB**.



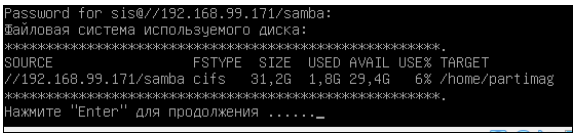
13. Режим безопасности установите «**auto**».



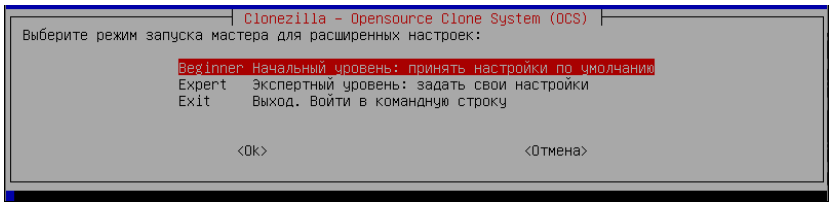
14. Введите пароль пользователя Samba-сервера.



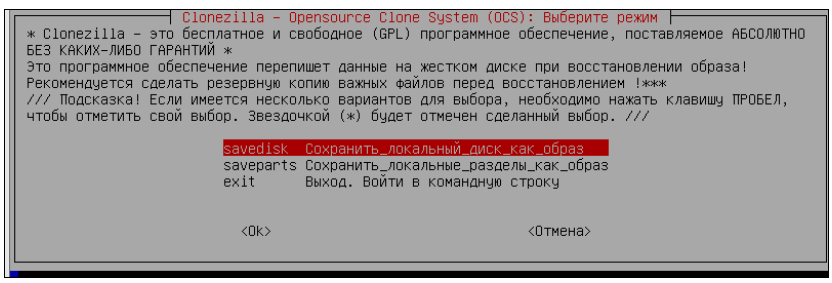
15. Подтвердите свой выбор нажатием «**Enter**».



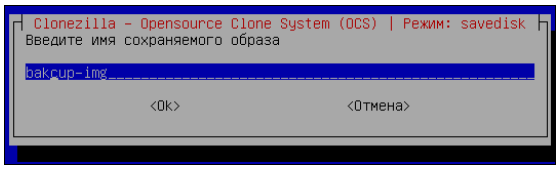
16. Затем нужно выбрать режим запуска мастера для расширенных настроек.



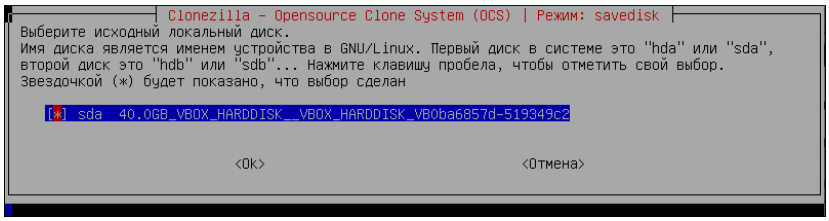
17. В нем необходимо выбрать пункт «**savedisk — Сохранить локальный диск как образ**».



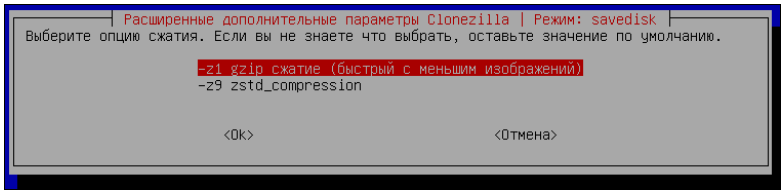
18. Затем введите *имя* сохраняемого *образа*.



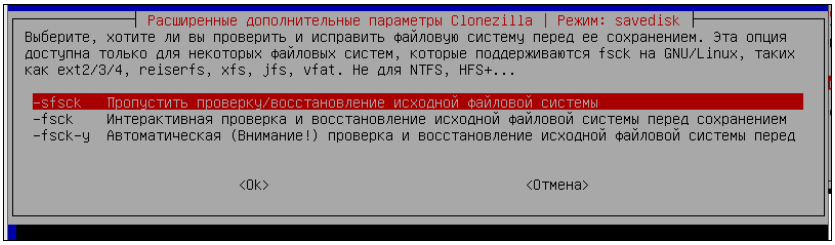
19. Выберите *диск*, который хотите сохранить.



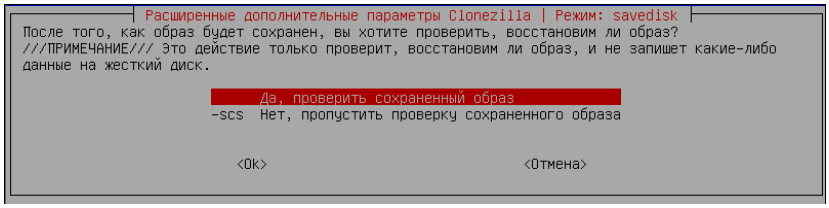
20. Далее предлагается выбрать опцию сжатия данных. Можно оставить *значение по умолчанию*.



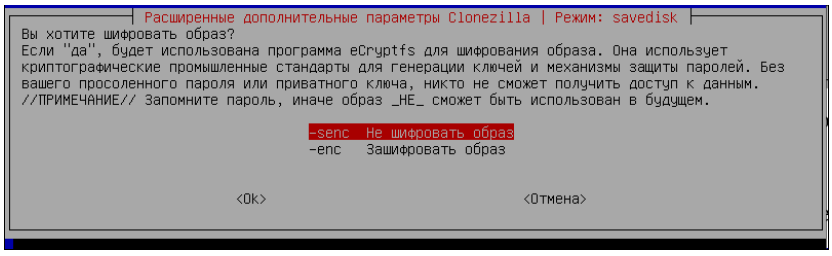
21. Затем требуется указать, нужно ли проверять файл перед сохранением.



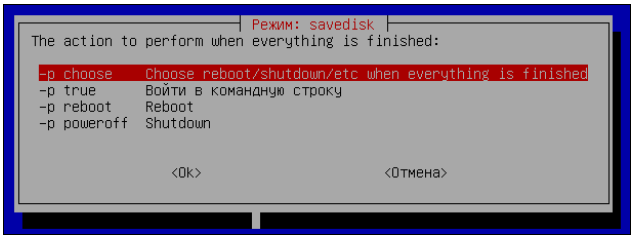
22. Следующее окно предлагает выбрать, хотите ли вы включить проверку сохраненного образа на восстановление. Выберите пункт «**Да, проверить сохраненный образ**».



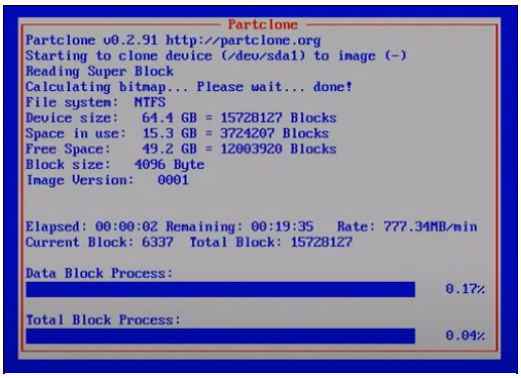
23. Выберите, нужно ли шифровать ваш образ.



24. Затем необходимо выбрать *дальнейшее действие* после завершения клонирования.



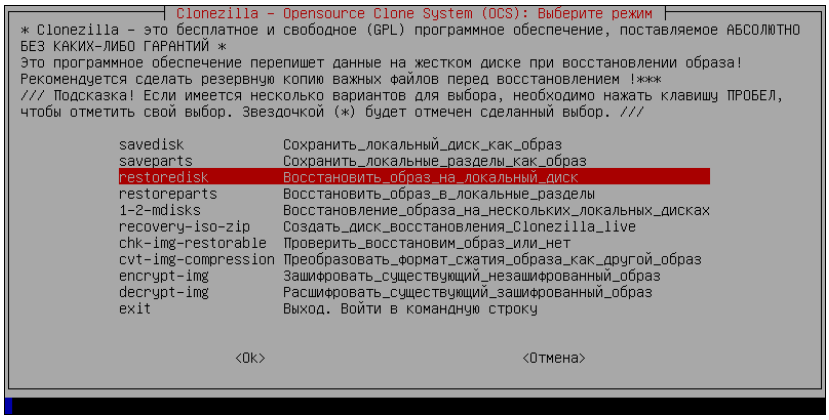
После выполнения всех вышеуказанных действий **образ диска на Samba-сервере** будет успешно **создан**.



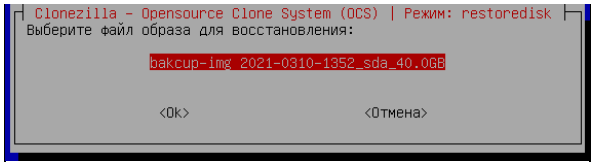
Восстановление диска

Для восстановления диска необходимо проделать описанные выше пункты **1-16**.

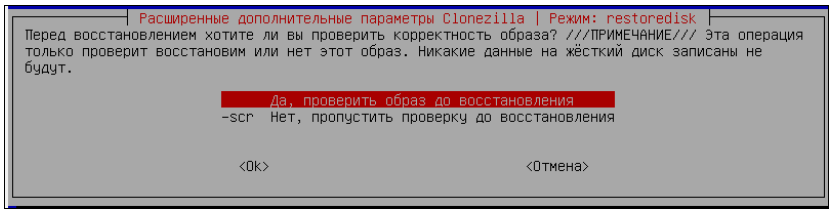
После этого необходимо выбрать действие с диском «**restoredisk — Восстановить образ на локальный диск**».



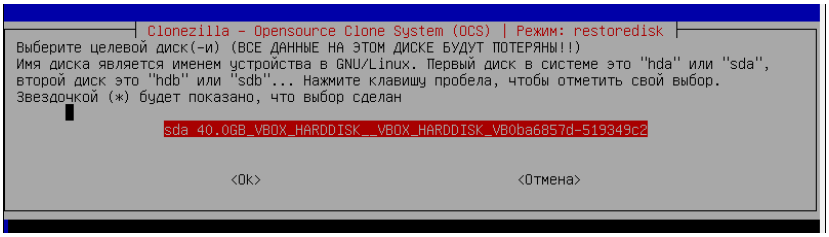
Выберите нужный *файл образа*.



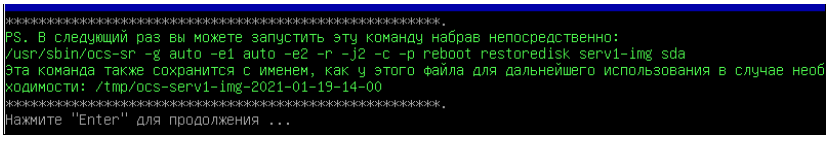
Включите *проверку образа* перед восстановлением.



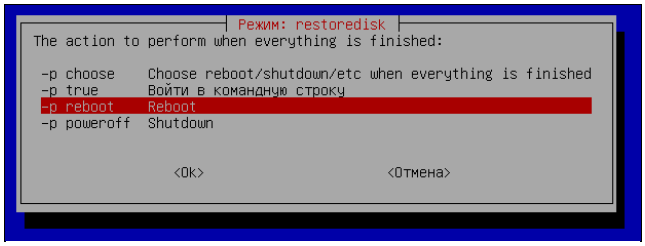
Затем выберите *диск*, на который будет установлен образ.



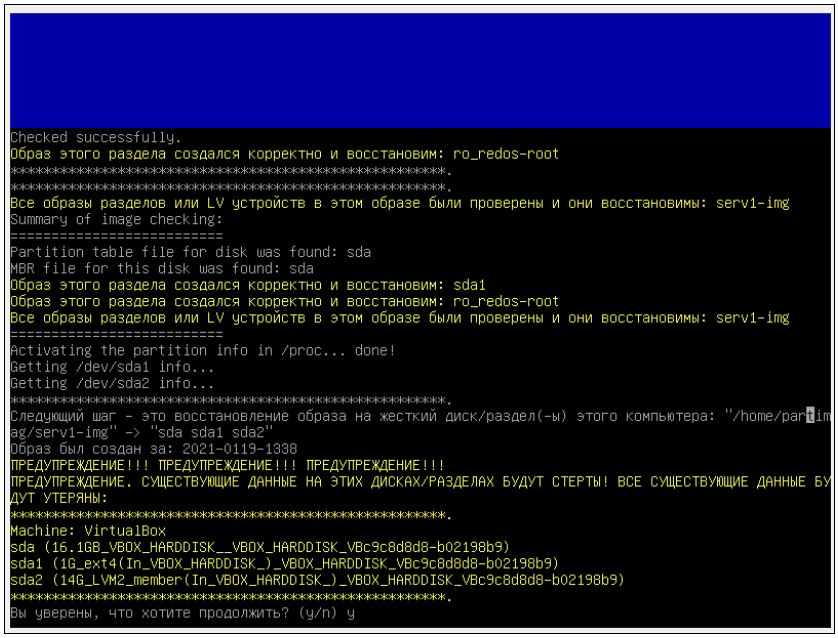
Подтвердите действия нажатием «**Enter**».



Далее выберите *действие после завершения* восстановления диска.



Будет выполнена проверка возможности восстановления диска и представлены данные о нем. Для подтверждения действия необходимо будет нажать «**y**». После этого пойдет процесс восстановления и диск будет восстановлен.



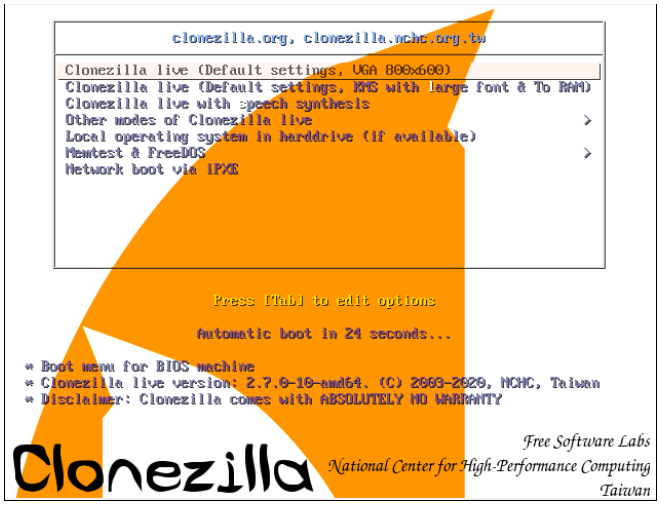
Клонирование жесткого диска на SSH-сервер

Окружение

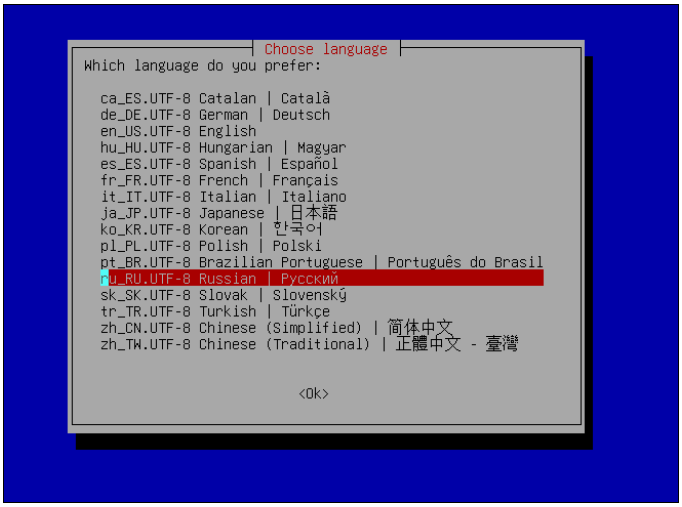
- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:**: Clonezilla 3.0.1-8

Создание образа системы

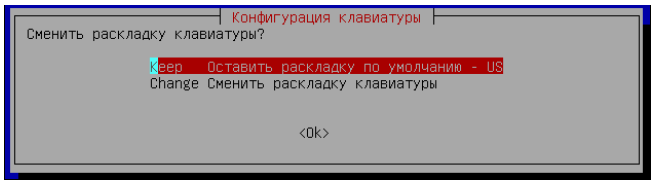
1. Необходимо загрузиться с загрузочного образа **clonezilla**. На экране появится окно загрузчика. В нем необходимо выбрать первый пункт. Для подтверждения выбора следует нажать «**Enter**».



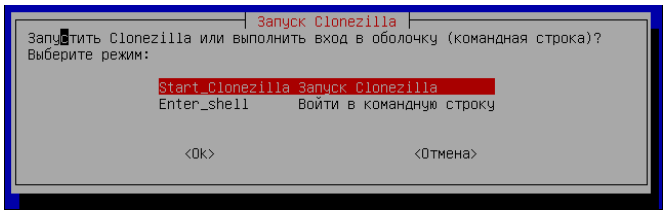
2. Затем программа предложит выбрать *язык интерфейса*.



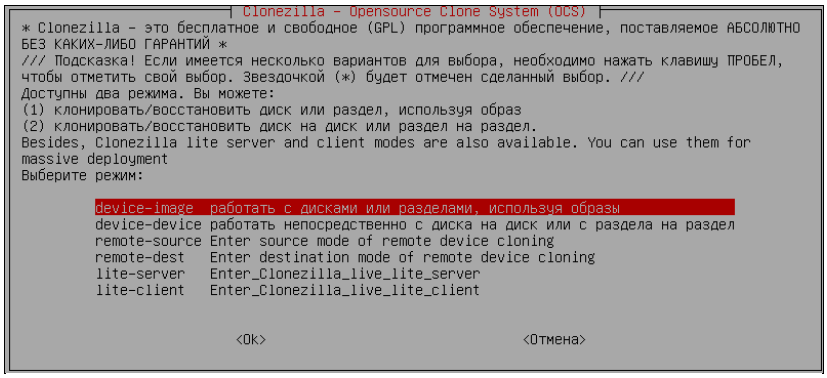
3. Далее программа предлагает сменить *раскладку* клавиатуры.



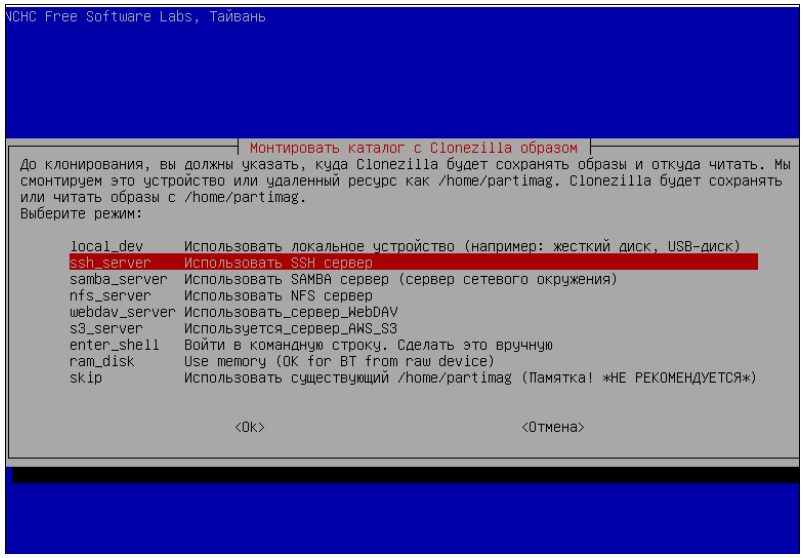
4. В следующем окне предлагается запустить **Clonezilla** или перейти в командную строку. Выберите вариант «**Start_Clonezilla**».



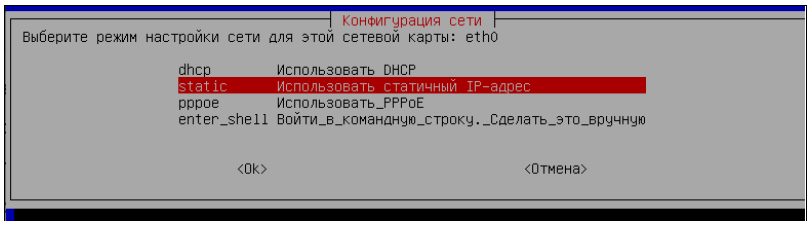
5. Затем необходимо настроить режим для работы с диском. Выберите пункт «**device-image**».



6. *Местом* сохранения образа в данном случае выберите «**ssh_сервер**».

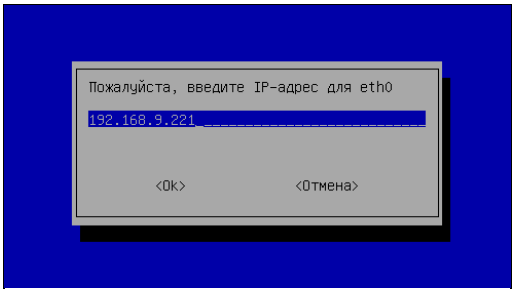


7. Далее выберите *режим* настройки сети — «**static**».

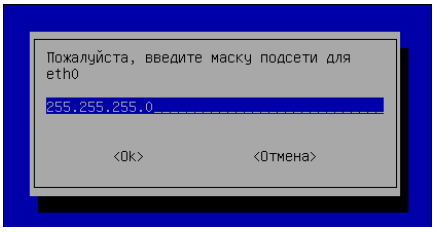


Так как было выбрано использовать *статический* ip-адрес, необходимо его прописать.

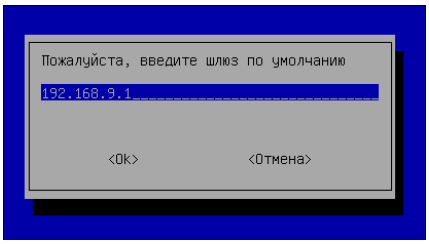
8. Введите *IP-адрес* устройства, с которого клонируется диск.



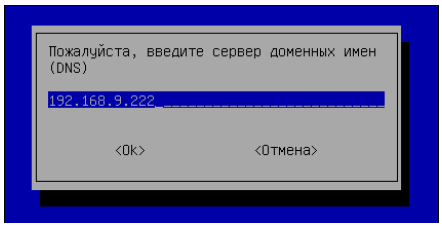
9. Введите *маску* подсети.



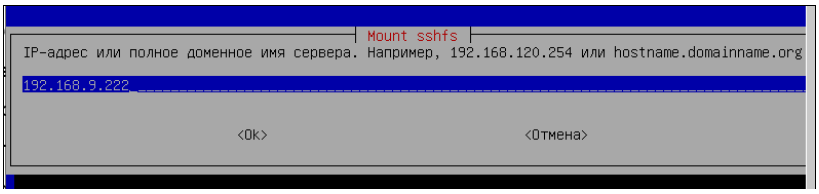
10. Затем введите *шлюз* по умолчанию.



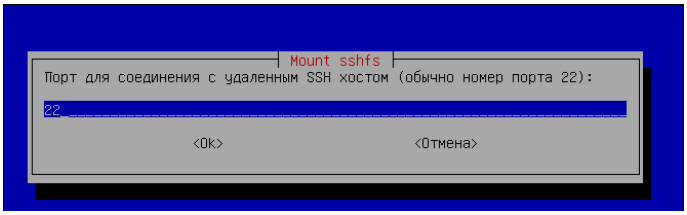
11. А также *IP-адрес DNS*.



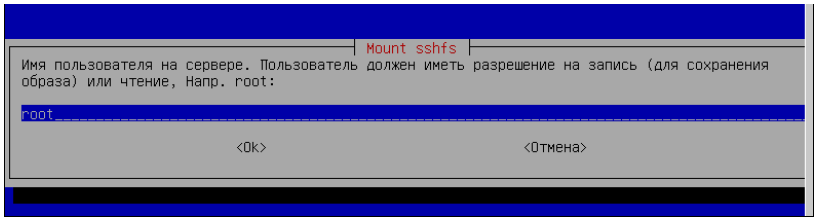
12. Затем введите *IP-адрес* или *полное имя* SSH сервера.



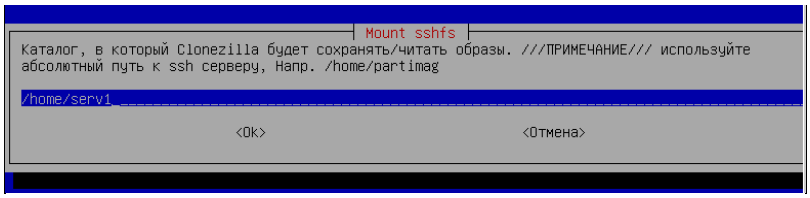
13. Введите используемый *порт* для соединения с удаленным хостом.



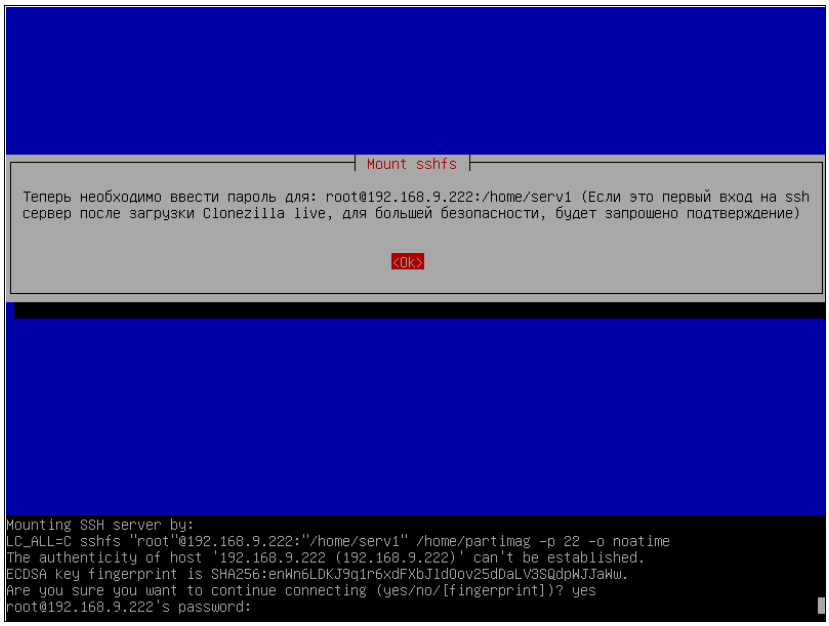
14. Далее нужно ввести *имя пользователя* SSH сервера.



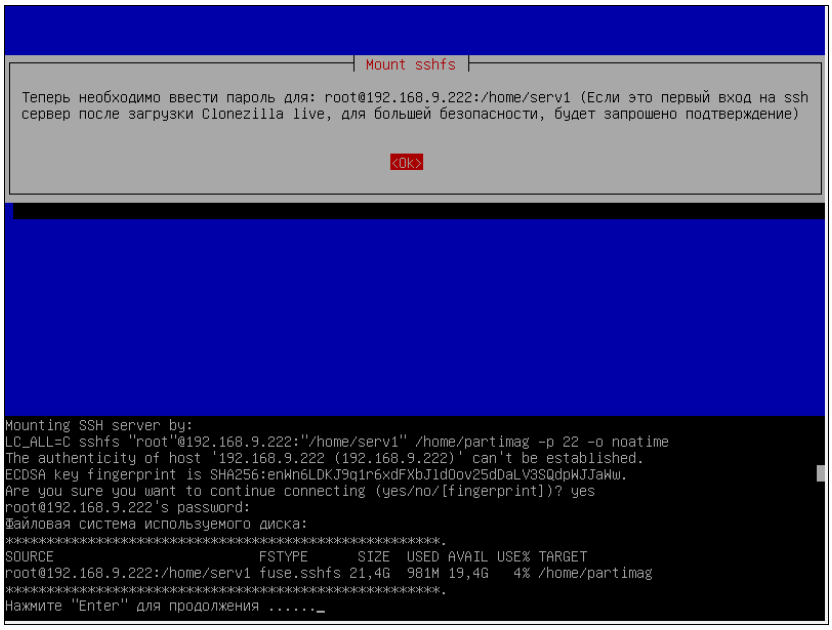
15. Определите *каталог*, в который будете сохранять/читать образы, введите *его название*.



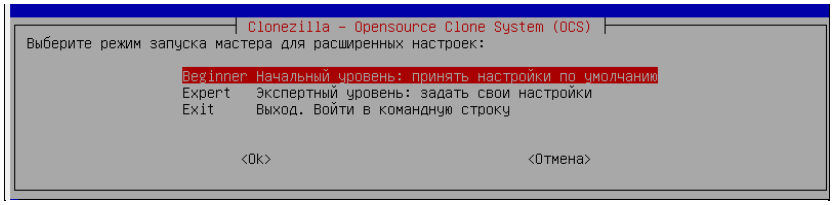
16. Введите *пароль пользователя*.



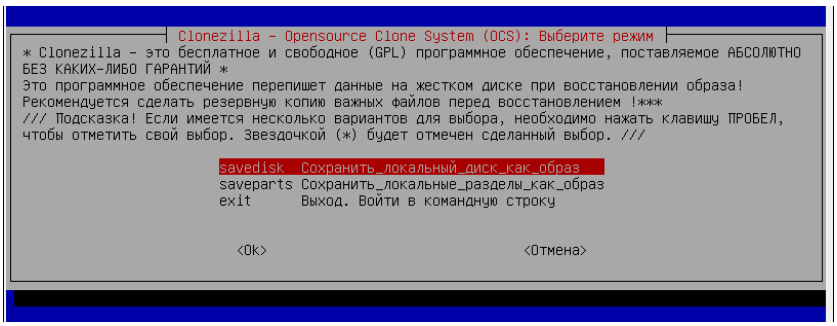
17. Подтвердите свой выбор нажатием «**Enter**».



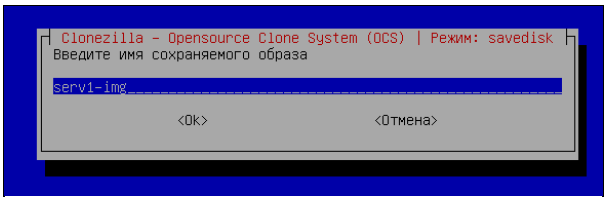
18. Затем нужно выбрать *режим запуска* мастера для расширенных настроек.



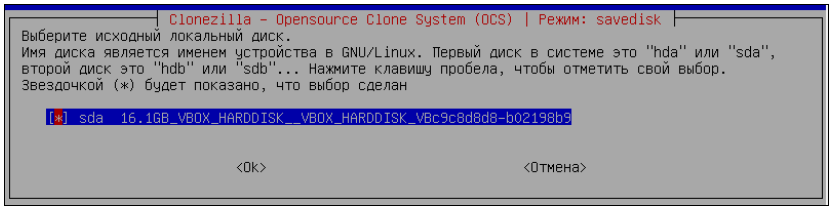
19. В нем необходимо выбрать пункт «**savedisk — Сохранить локальный диск как образ**».



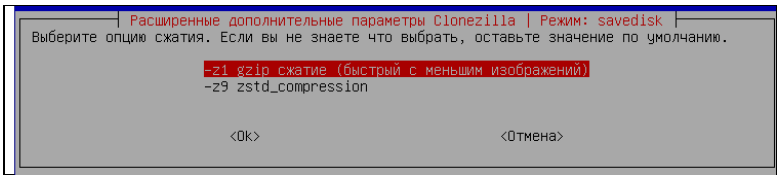
20. Затем введите *имя* сохраняемого *образа*.



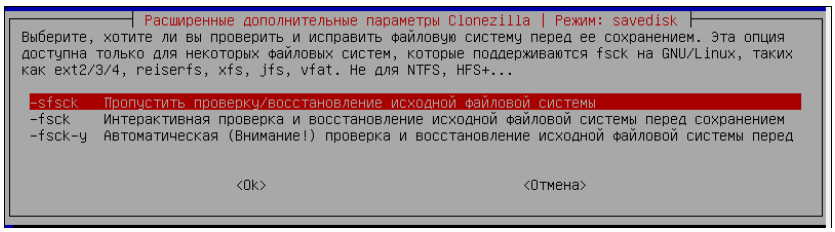
21. Выберите *диск*, который хотите сохранить.



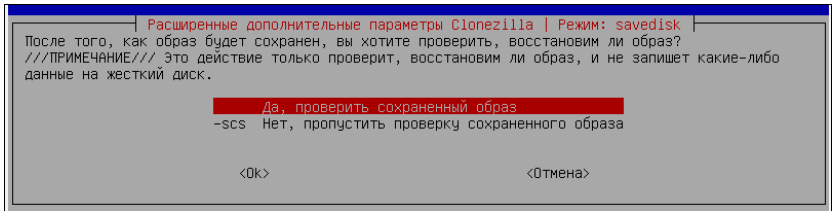
22. Далее предлагается выбрать *опцию сжатия* данных. Можно оставить значение *по умолчанию*.



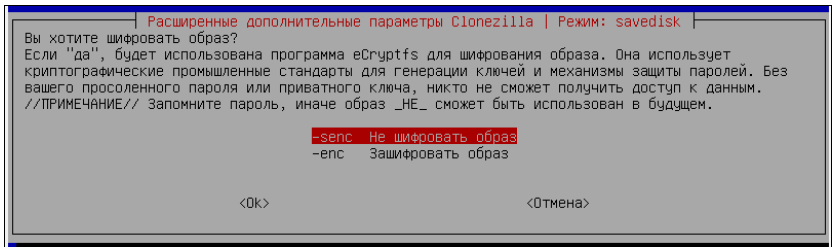
23. Затем требуется указать, нужно ли *проверять* файл перед сохранением.



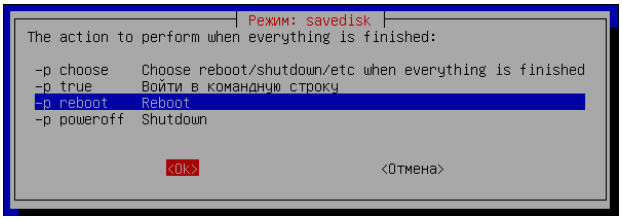
24. Следующее окно предлагает выбрать, хотите ли вы включить *проверку* сохраненного *образа* на восстановление. Выберите пункт «**Да, проверить сохраненный образ**».



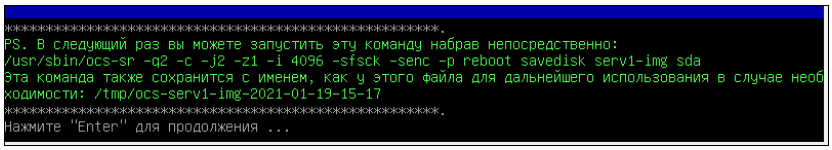
25. Выберите, нужно ли *шифровать* ваш образ.



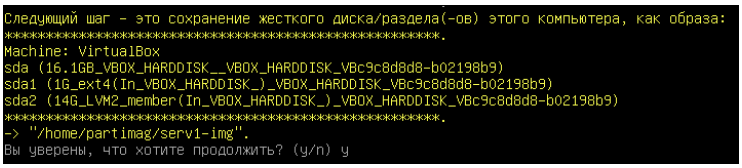
26. Затем необходимо выбрать *дальнейшее действие* после завершения клонирования.



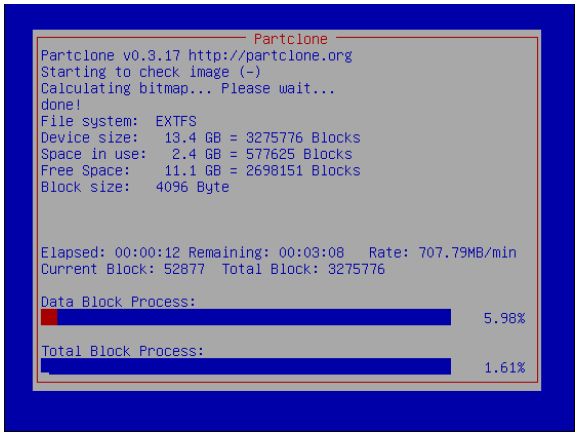
27. Подтвердите свой выбор нажатием «**Enter**».



28. Затем необходимо подтвердить сохранение диска, как образа.



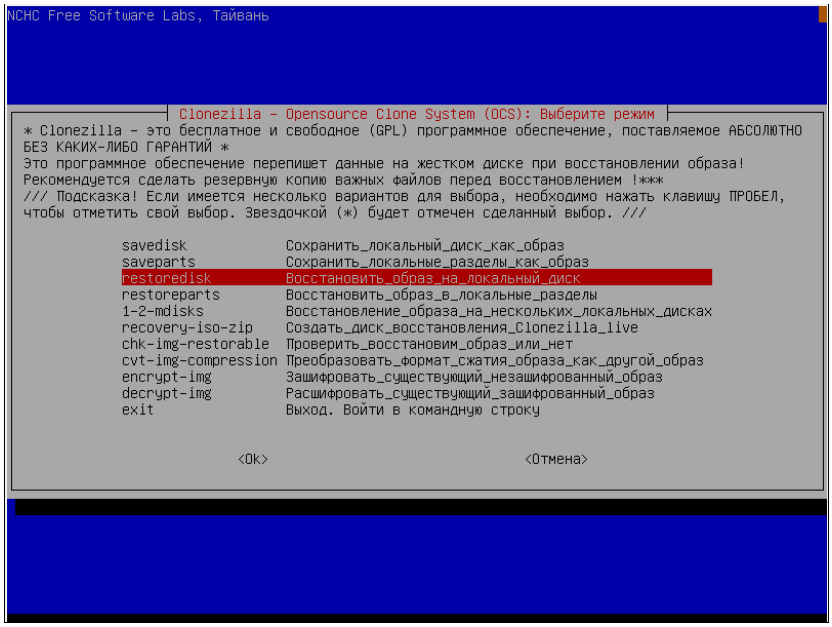
После выполнения всех перечисленных выше действий образ диска на SSH сервере создан.



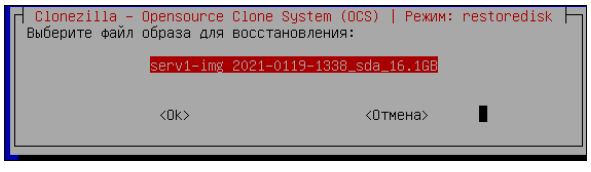
Восстановление диска

Для восстановления диска необходимо проделать описанные выше пункты **1-18**.

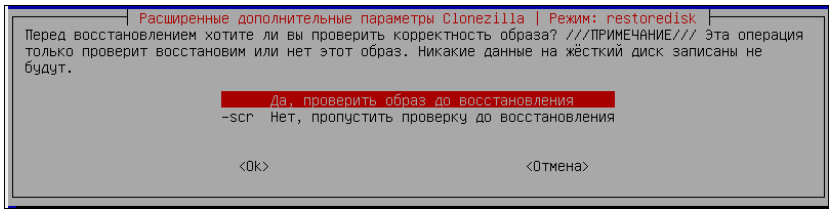
После этого необходимо выбрать действие с диском «**restoredisk — Восстановить образ на локальный диск**». Данный пункт будет доступен, если Clonezilla обнаружит сохраненный ранее образ на SSH-сервере.



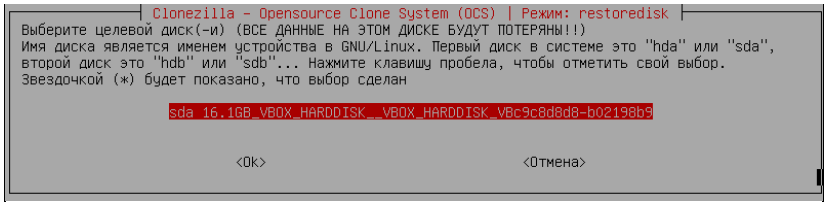
Выберите нужный *файл образа*.



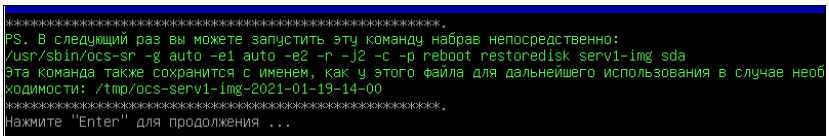
Включите *проверку образа* перед восстановлением.



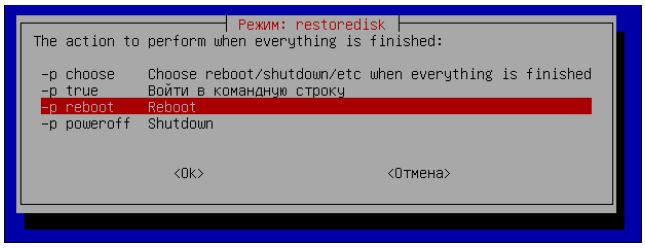
Затем выберите *диск*, на который будет установлен образ.



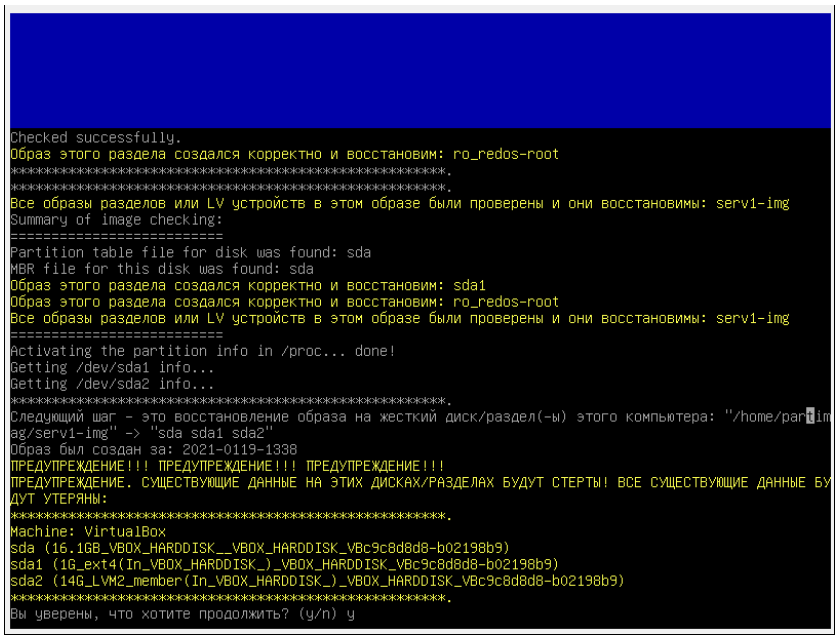
Подтвердите действия нажатием «**Enter**».



Далее выберите *действие после завершения* восстановления диска.



Будет выполнена проверка возможности восстановления диска и представлены данные о нем. Для подтверждения действия необходимо будет нажать «**y**». После этого пойдет процесс восстановления и диск будет восстановлен.



Создание резервных копий в Кибер Бекап

Обзор
Установка
Установка сервера управления
Установка агента
Создание плана выполнения резервной копии

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический
- **Версия ПО:** CyberBackup_15

Обзор

Кибер Бэкап — коммерческое программное обеспечение, предназначенное для создания резервного копирования и восстановления данных. Скачать пробную версию или приобрести продукт можно на официальном сайте компании Киберпротект.

Управление утилитой осуществляется из web-формы. Через нее можно задать расписание, по которому будет выполняться резервное копирование, просматривать доступные резервные копии, просматривать уведомления и отчеты о прошедших операциях, добавлять или удалять хранилища. Для первого подключения к web-форме нужен пароль от учетной записи суперпользователя. Впоследствии можно добавить других пользователей.

Установка

Для корректной установки **CyberBackup** необходимо установить ряд дополнительных пакетов. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду (для РЕД ОС 7.3 и старше):

```
dnf install kernel-lt-headers kernel-lt-devel gcc make dkms elfutils-libelf-devel
```

Здесь и далее работа с программой будет выполняться с правами пользователя **root**, если не указано иное.

Перейдите в директорию, куда был скачан файл, и назначьте ему права на исполнение:

```
cd /<путь_до_папки_с_файлом>/
chmod +x CyberBackup_15_64-bit.x86_64
```

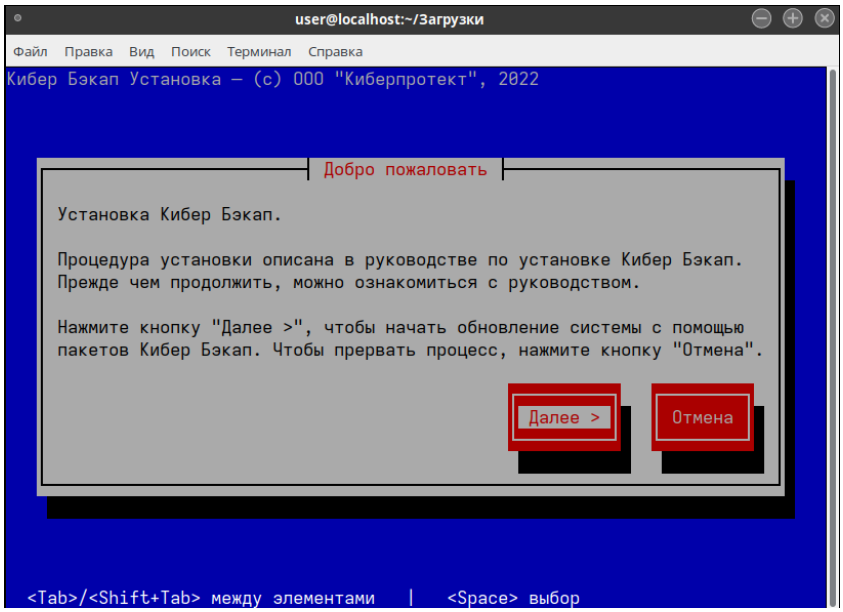
Выполните команду для запуска утилиты:

```
./CyberBackup_15_64-bit.x86_64
```

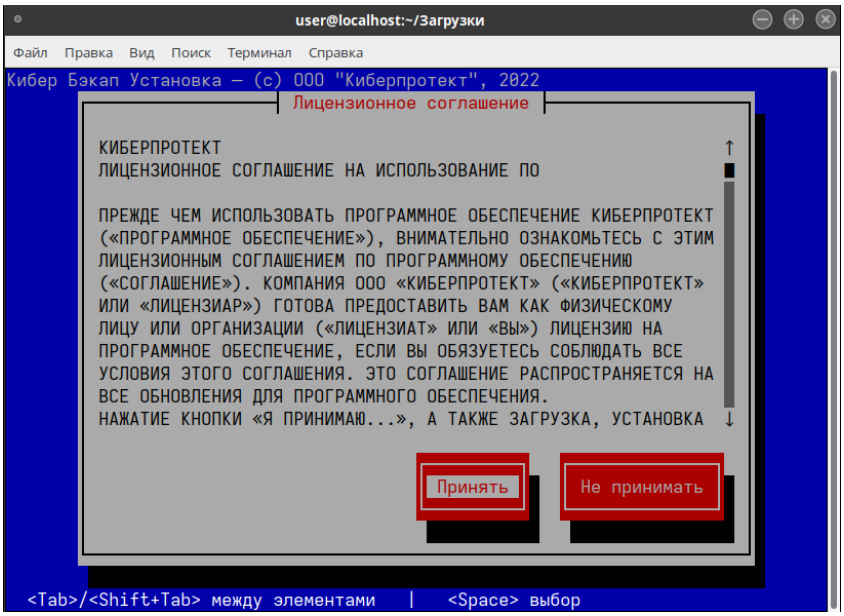
Дальнейшие действия выполняются в установщике программы.

Установка сервера управления

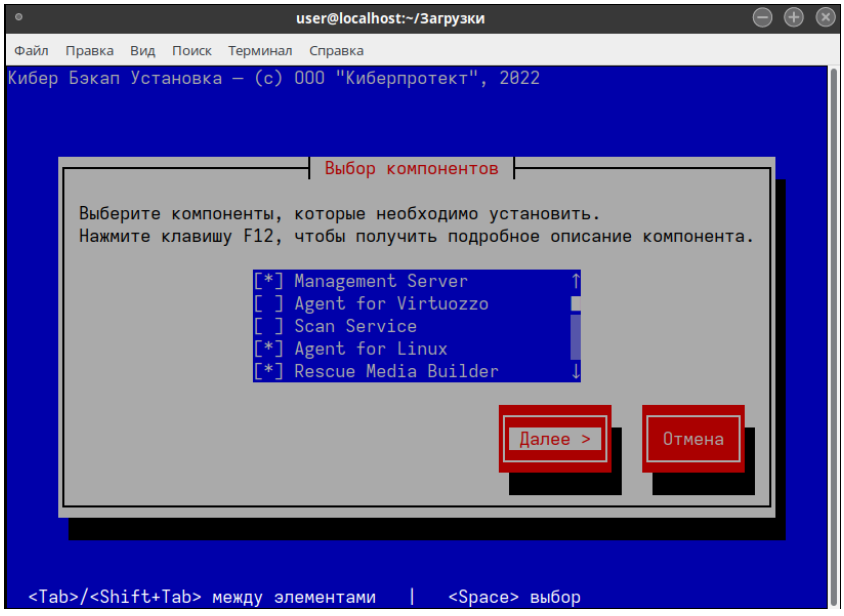
После запуска установки будет открыто окно установщика. Нажмите **Далее**.



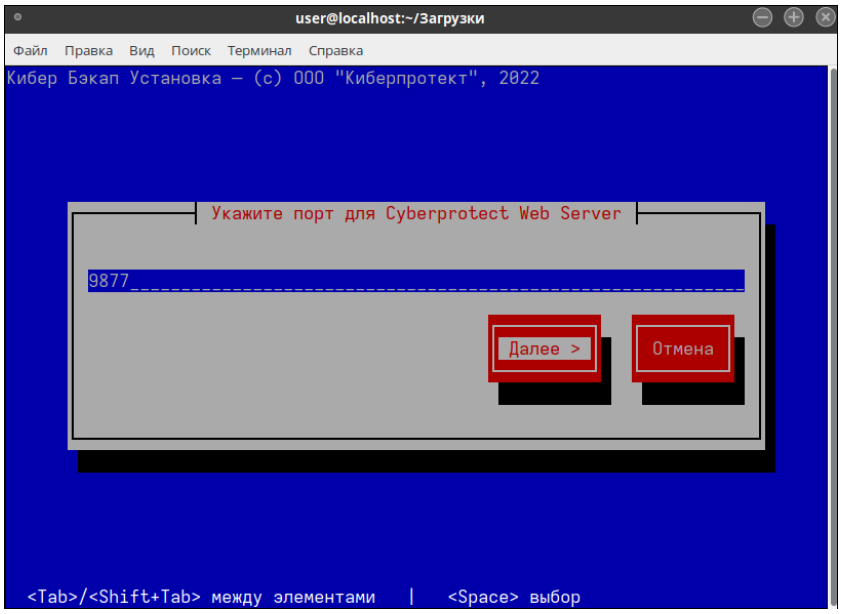
Ознакомьтесь и примите лицензионное соглашение.



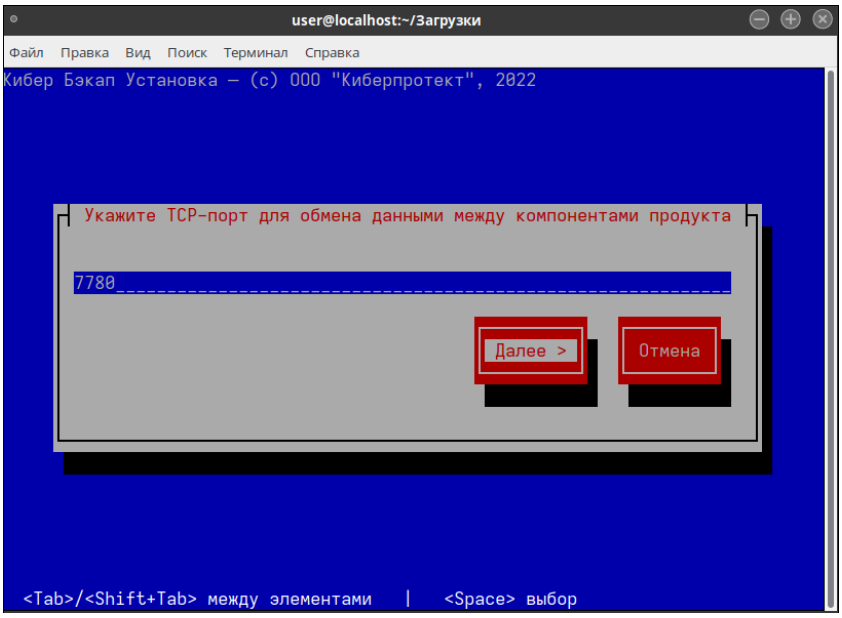
Выберите компоненты для установки.



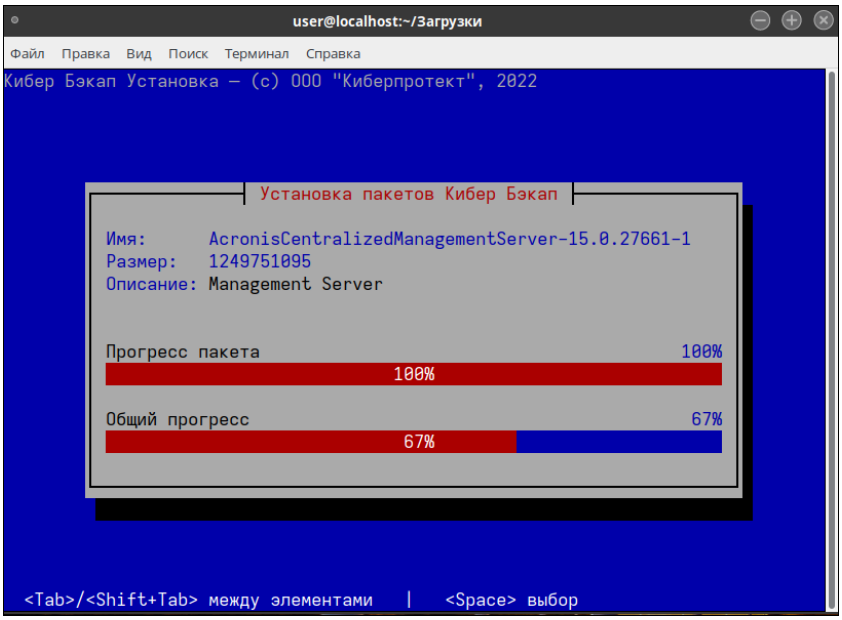
Укажите порт для **Cyberprotect Web Server**.



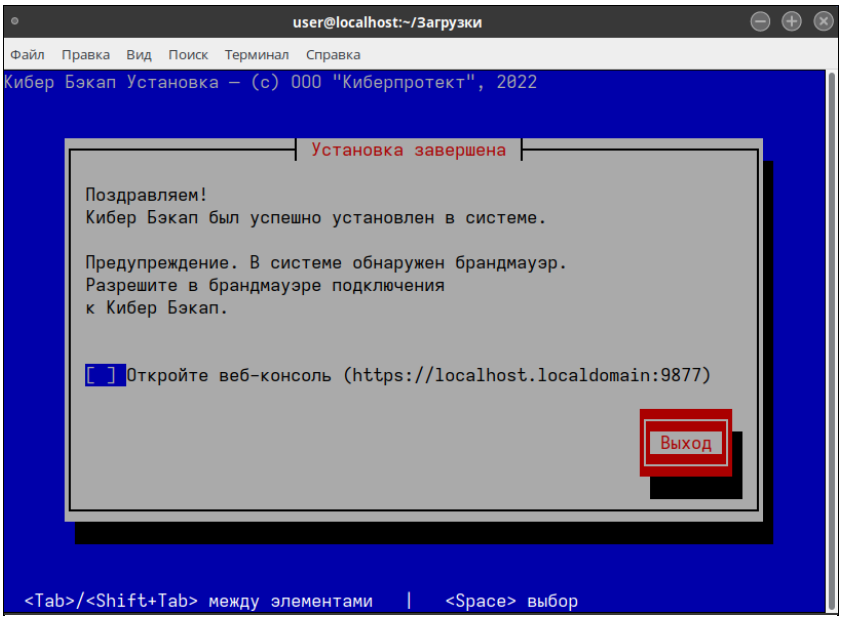
Укажите TCP-порт для обмена данными между компонентами продукта.



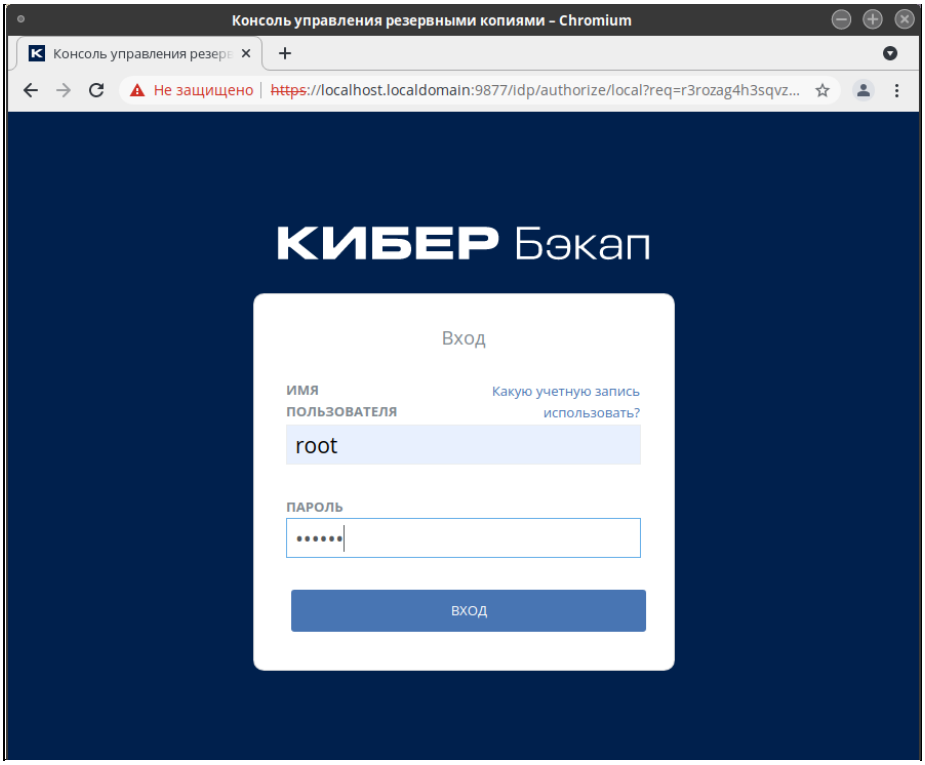
Затем будет запущен процесс установки пакетов.



После завершения установки можно выбрать пункт «**Откройте веб-консоль**», а затем нажать **Выход**. В таком случае, веб-консоль **Cyber Protect** откроется в вашем веб-браузере, установленном по умолчанию.



Вы также можете самостоятельно открыть нужный браузер и перейти по адресу https://localhost.localdomain:9877. Для входа введите имя пользователя и пароль.



Проведите проверку работы модуля командой, в выводе которой должны отобразиться диски, разделы, массивы и тома LVM, выполнив команду:

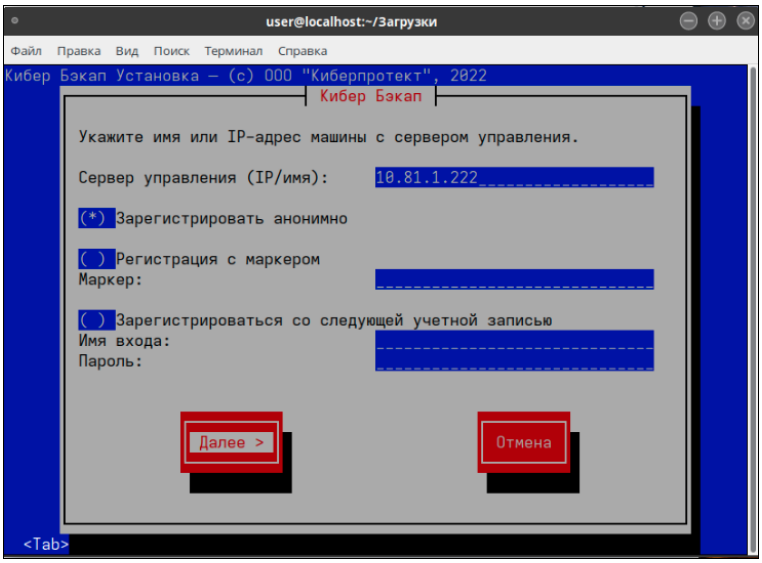
```
/usr/lib/Acronis/BackupAndRecovery/dsk_supp_test
```

Установка агента

Агенты устанавливаются на локальных машинах и должны быть подключены к серверу управления для создания резервных копий.

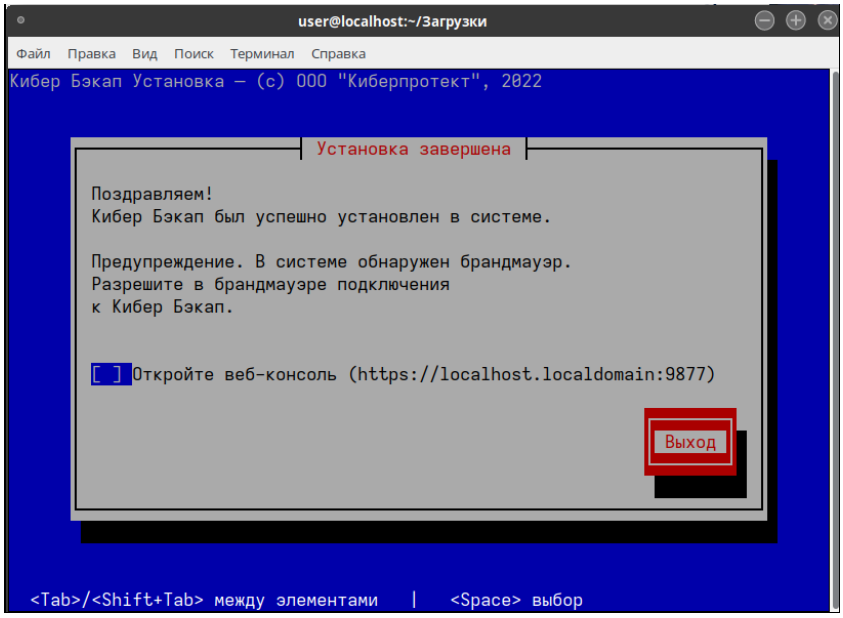
Для установки **CyberBackup Агент** выберите соответствующий компонент на этапе выбора компонентов.

Далее необходимо настроить подключение, указав **имя** или **IP-адрес** машины с установленным сервером управления.

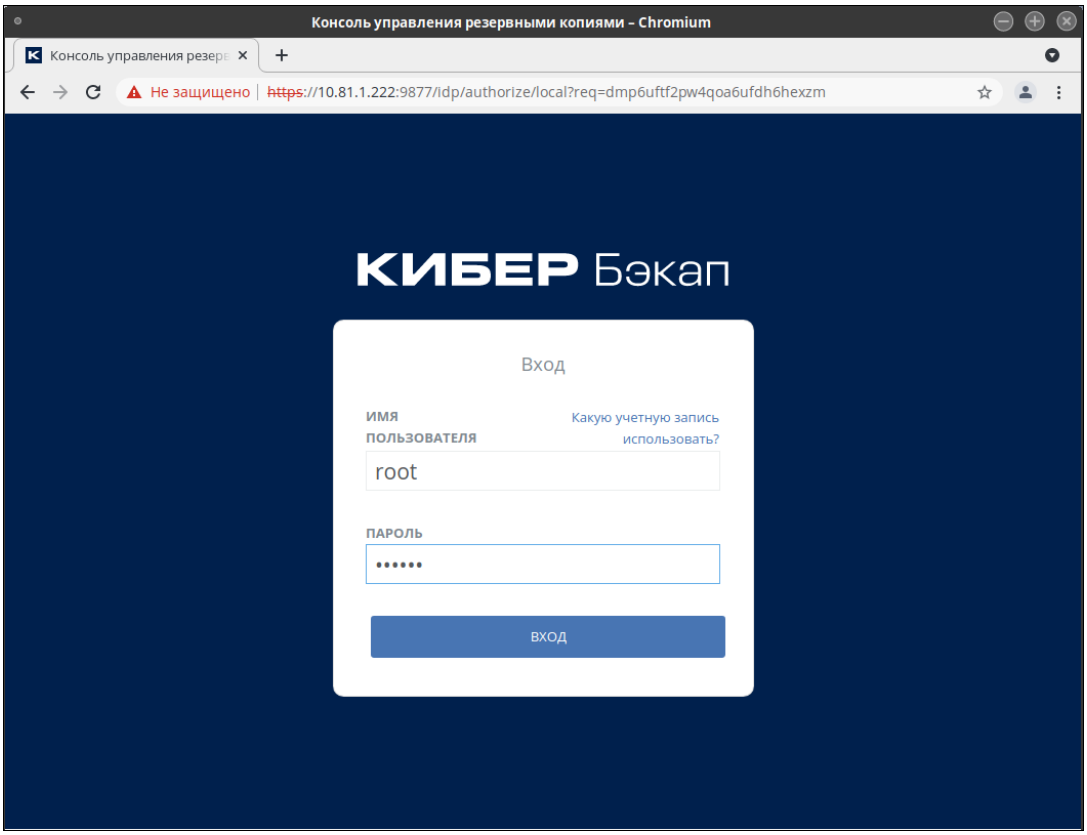


При нажатии на кнопку **Далее** начнется процесс установки агента.

После завершения установки можно выбрать пункт «**Откройте веб-консоль**», а затем нажать **Выход**. В таком случае, веб-консоль **Cyber Protect** откроется в вашем веб-браузере, установленном по умолчанию.



Вы также можете самостоятельно открыть нужный браузер и перейти по адресу https://10.81.1.222:9877. Для входа введите имя пользователя и пароль.



Создание плана выполнения резервной копии

Прежде чем создавать план, нужно добавить хранилище. Для этого выберите пункт **«Резервные копии» → «Добавить хранилище»**. Выберите и настройте один из предложенных вариантов.

Далее создайте план, выбрав в правом меню пункт **«Планы»**. Их может быть несколько типов:

- **«Резервное копирование»** - отвечает за создание резервной копии;
- **«Репликация резервной копии»** - создание дополнительной копии синхронизированной с основной для восстановления в случае, если исходная копия недоступна или повреждена.
- **«Проверка»** - план проверок созданных резервных копий
- **«Очистка»** - план удаления ранних резервных копий для освобождения места под новые.
- **«Преобразование в ВМ»** - перевод созданной резервной копии диска в виртуальную машину.
- **«Репликация ВМ»** - создание дополнительной виртуальной машины синхронизированной с основной для повышения надежности хранения.

Выберите **«Резервное копирование»** и нажмите **«Создать план».** Настройте план, указав расписание его выполнения, устройства, с которых будет создаваться резервная копия, место хранения (ранее добавленное хранилище) и срок его хранения. Дополнительно можно указать использование шифрования. Указав вышеперечисленные данные — нажмите **«Создать»**. Созданный сразу появится в списке выбора. Его можно запустить сразу, изменить его параметры или посмотреть историю его выполнения, где отображается результат его работы.

Дополнительную документацию по программе и более подробное описание функций можно посмотреть в официальной документации, нажав на знак вопроса в правом верхнем углу и выбрав пункт **«Документация».**

Для использования функциональных возможностей **CyberBackup** необходимо приобрести лицензию.

ПО для образовательного процесса – redos-education

Установка утилиты
Возможности утилиты
Информация о пакетах

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: redos-education-1.4.10-1

Redos-education – программное обеспечение для образовательного процесса, созданное компанией РЕД СОФТ для удобного управления рядом пакетов из репозитория РЕД ОС.

Вы можете подробнее ознакомиться с установкой и работой утилиты **redos-education**, просмотрев наши обучающие видео:

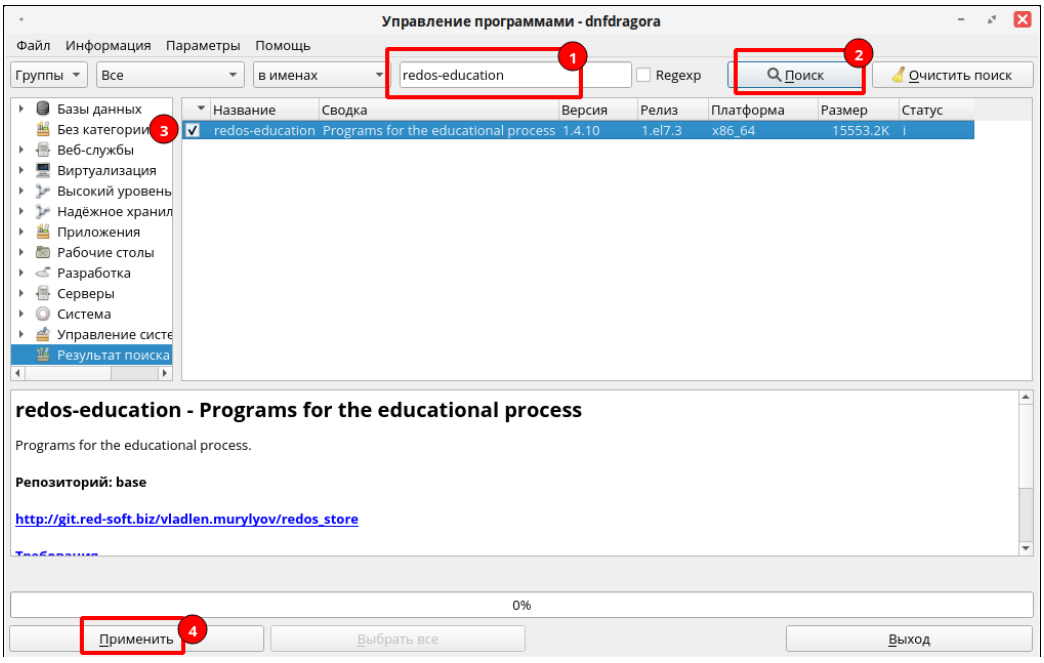
- на **RuTube** — ПО для образовательного процесса в РЕД ОС;
- в **Яндекс.Дзен** — ПО для образовательного процесса в РЕД ОС;
- в **VK Видео** — ПО для образовательного процесса в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка утилиты

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**redos-education**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

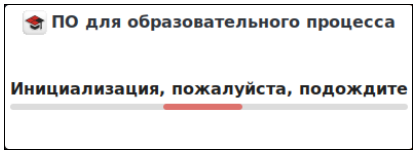
и выполните команду:

```
dnf install redos-education
```

Дальнейшая работа в программе выполняется от локального пользователя.

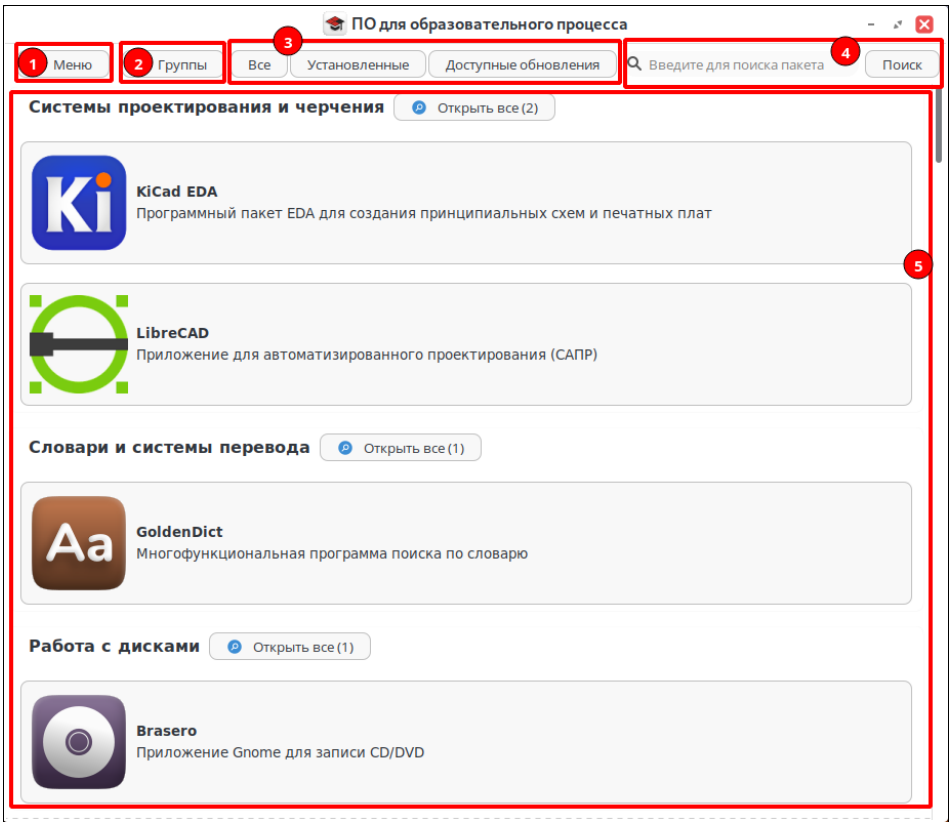
После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**ПО для образовательного процесса**».

При запуске утилиты будет открыто окно инициализации.



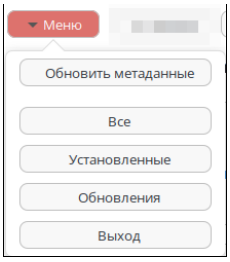
Возможности утилиты

Окно программы выглядит следующим образом:



1. **Меню программы** — представляет собой выпадающий список, здесь доступны такие действия, как:

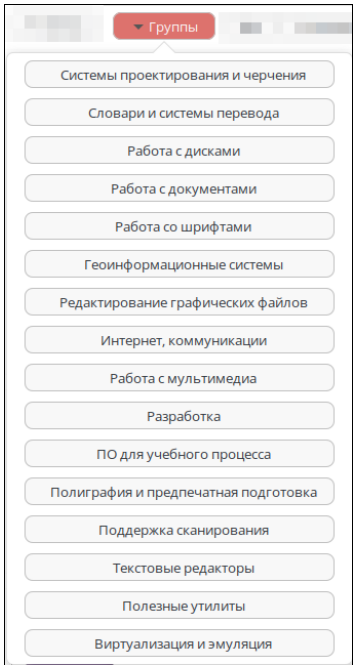
- обновление метаданных;
- отображение всех доступных утилит;
- отображение только установленных пакетов;
- отображение пакетов, требующих обновления;
- выход из программы.



2 . **Группы** — представляет собой выпадающий список доступных групп, в которые объединены утилиты, список служит навигационным меню для быстрого перехода между группами приложений:

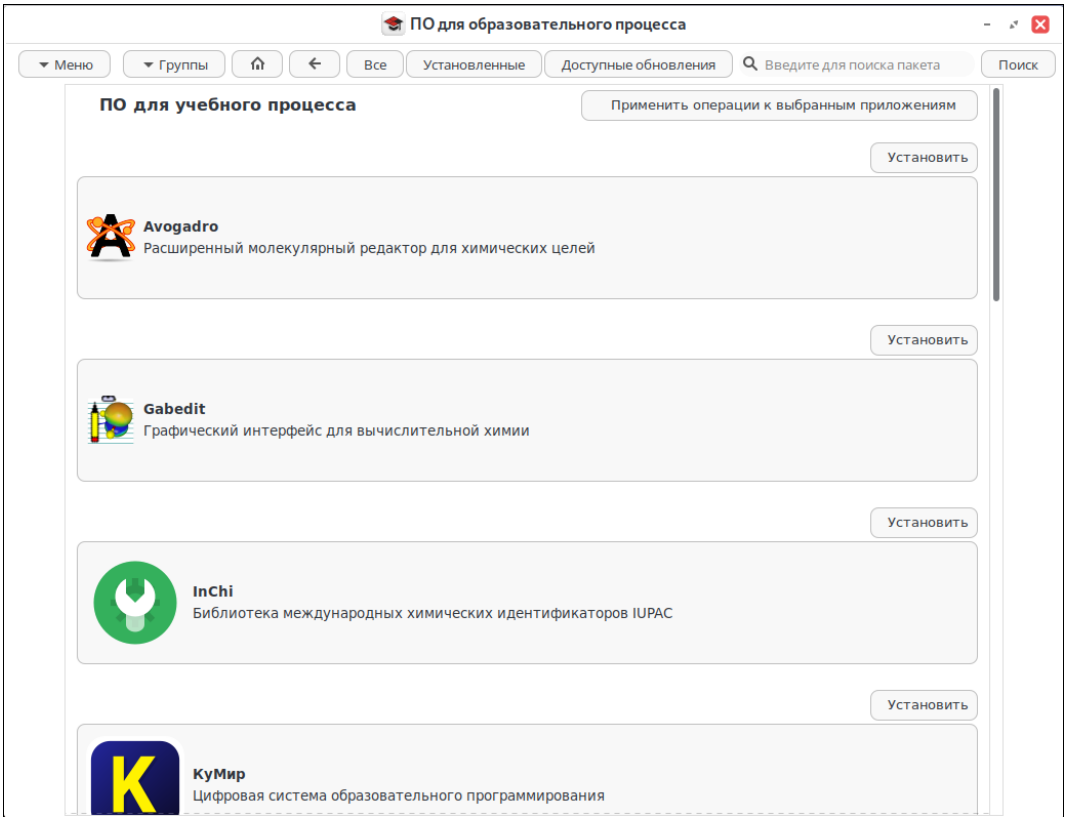
- системы проектирования и черчения;
- словари и системы перевода;
- работа с дисками;
- работа с документами;

- работа со шрифтами и т.д.



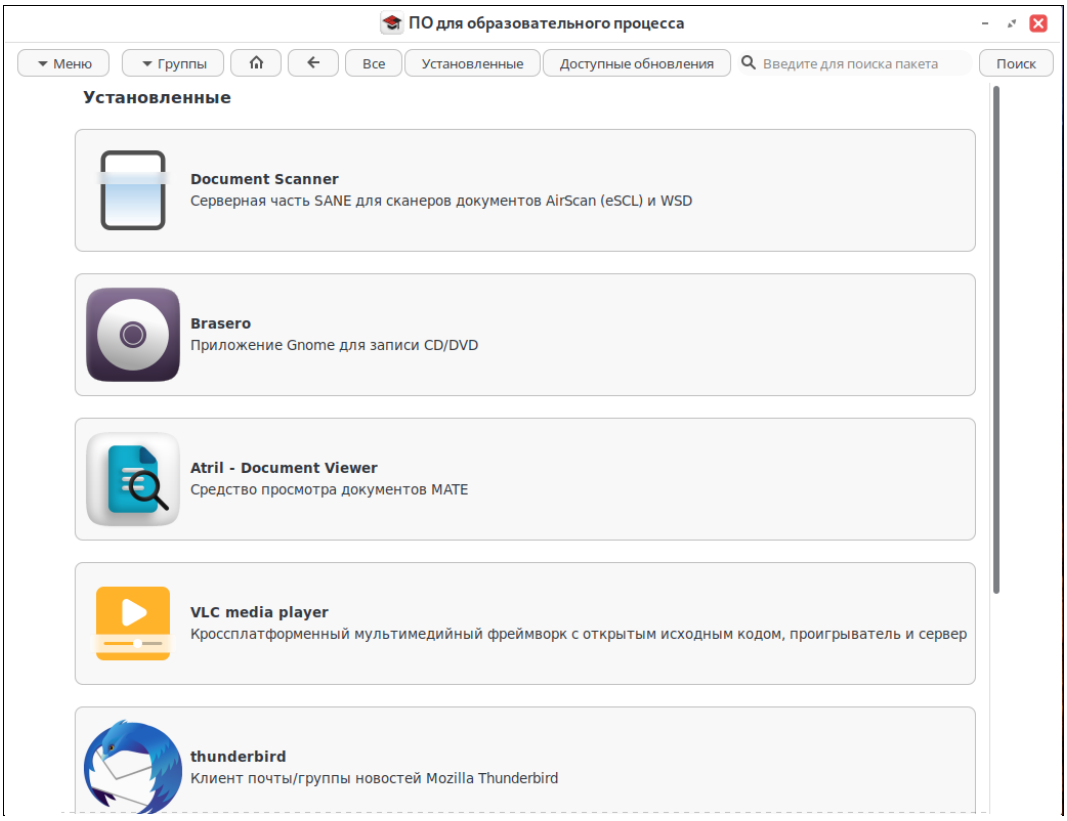
При выборе любого из пунктов будет открыта соответствующая ему страница приложения с перечнем утилит, которые входят в данную группу.

Пример отображения содержимого группы «**ПО для учебного процесса**»:

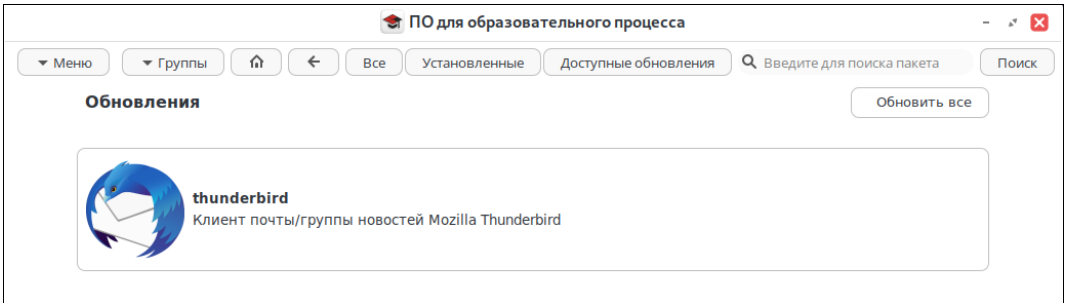


3. **Секции приложений** — отображение всех доступных утилит, отображение только установленных утилит или отображение утилит, требующих обновлений.

Отображение установленных утилит выглядит следующим образом:



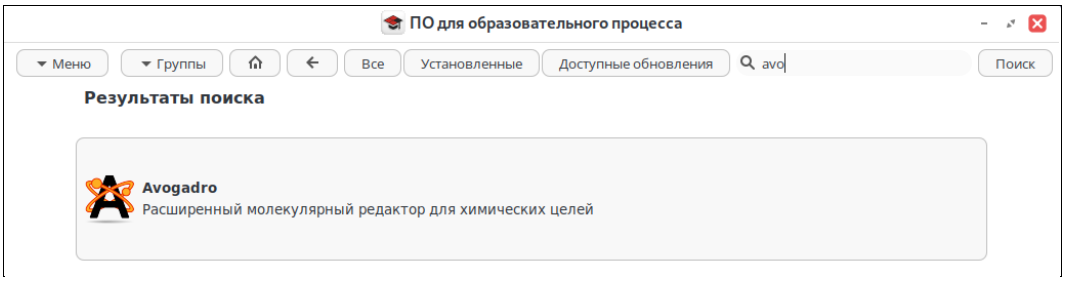
Отображение утилит, требующих обновлений, выглядит следующим образом:



В случае отсутствия доступных обновлений будет выведено сообщение:

---

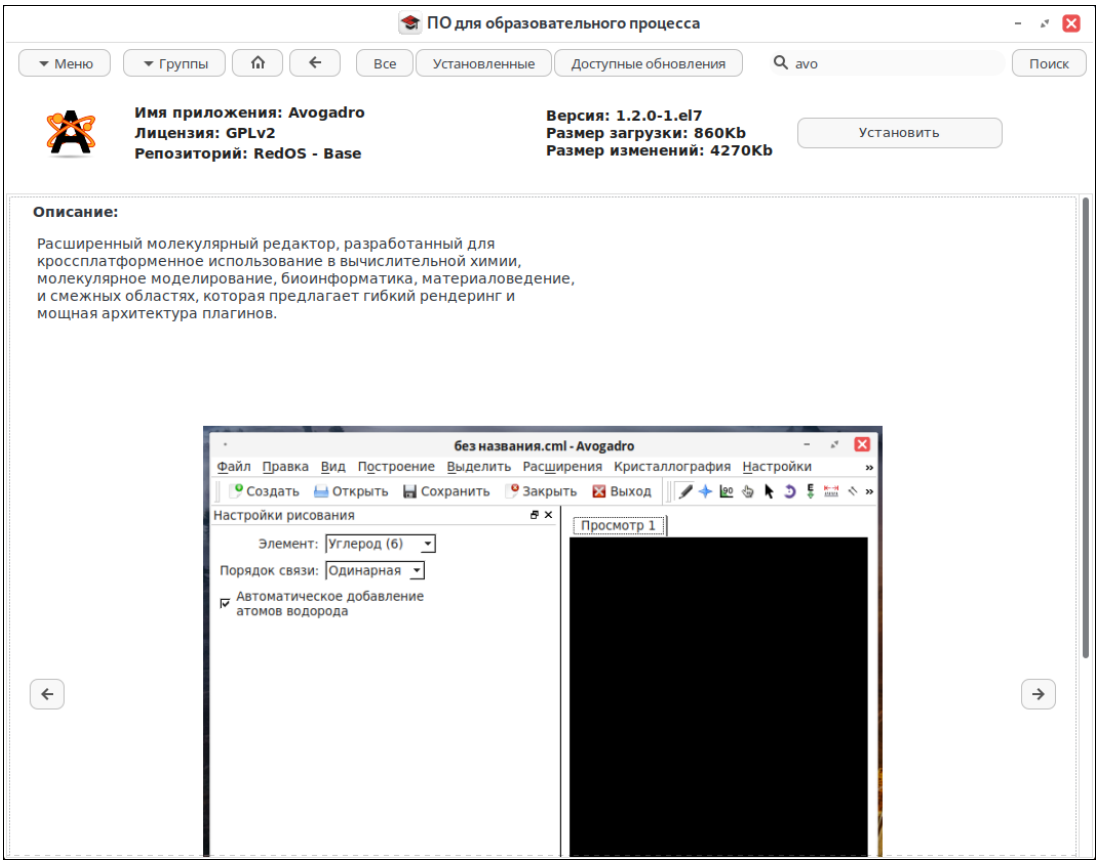
4. **Поиск утилит** — в строке поиска необходимо ввести название программы и нажать кнопку «**Поиск**».



5. **Поле** для непосредственного **отображения утилит** и информационных сообщений.

Информация о пакетах

Для открытия справочной информации, описания и список изменений определенного приложения необходимо просто кликнуть по нужной утилите.



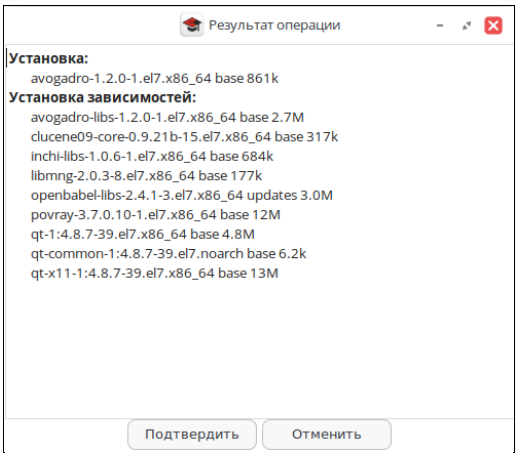
На данной странице можно ознакомиться со следующей информацией:

- имя rpm-пакета;
- лицензия, под которой распространяется данная утилита;
- имя репозитория, который предоставляет данный пакет;
- версия утилиты;
- размер загрузки и изменений в ОС после установки;
- описание утилиты;
- скриншоты работы в утилите;
- список изменений.

Список команд, которые можно выполнить с выбранной утилитой:

- установка утилиты;
- удаление утилиты;
- обновление утилиты;
- запуск утилиты после установки в ОС.

При выборе команды установки, удаления или обновления появится окно транзакции, которое оповещает пользователя о затрагиваемых зависимостях. Стоит обращать внимание на то, какие зависимости выдаются в данном окне транзакции. Если пользователь согласен с изменениями, которые будут внесены в ОС, то следует согласиться с результатами транзакции, в ином случае — отклонить.


Результат операции
Установка:
avogadro-1.2.0-1.el7.x86_64 base 861k
Установка зависимостей:
avogadro-libs-1.2.0-1.el7.x86_64 base 2.7M
clucene09-core-0.9.21b-15.el7.x86_64 base 317k
inchi-libs-1.0.6-1.el7.x86_64 base 684k
libmng-2.0.3-8.el7.x86_64 base 177k
openbabel-libs-2.4.1-3.el7.x86_64 updates 3.0M
povray-3.7.0.10-1.el7.x86_64 base 12M
qt-1:4.8.7-39.el7.x86_64 base 4.8M
qt-common-1:4.8.7-39.el7.noarch base 6.2k
qt-x11-1:4.8.7-39.el7.x86_64 base 13M
Подтвердить
Отменить

OpenBoard - программа для работы с интерактивными досками

Установка
Обзор программы
Запись экрана

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: OpenBoard-1.6.1-1

OpenBoard – кроссплатформенное приложение для интерактивной доски с открытым исходным кодом. Приложение может быть использовано как с интерактивными досками, так и с сенсорным или дополнительным экраном либо проектором.

Вы можете подробнее ознакомиться с работой программы **OpenBoard**, просмотрев наши обучающие видео:

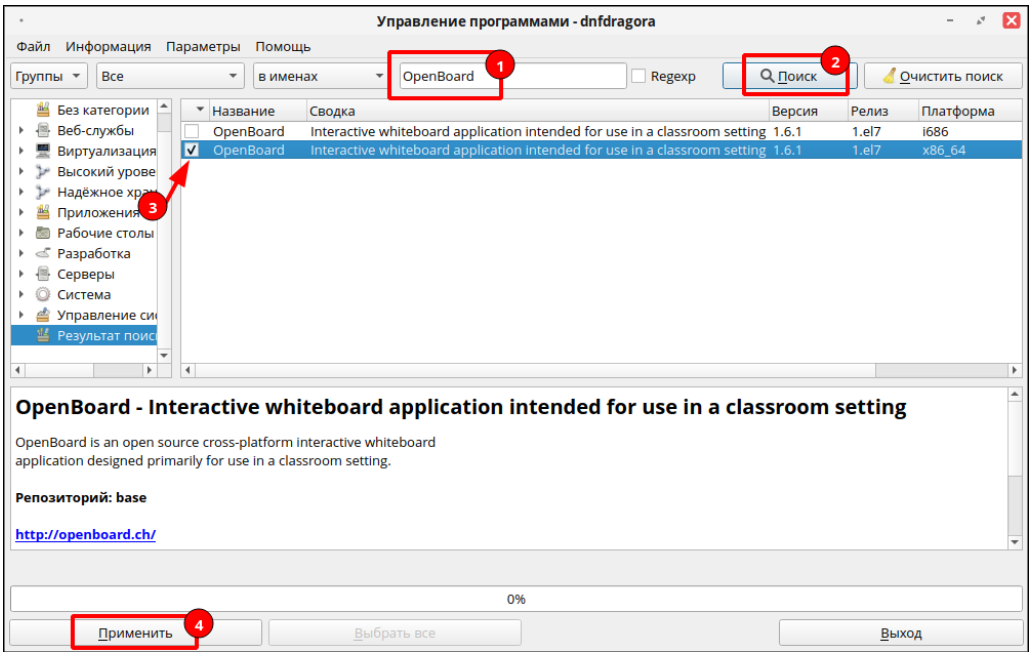
- на **RuTube** — Работа с интерактивными досками в РЕД ОС. OpenBoard;
- в **Яндекс.Дзен** — Работа с интерактивными досками в РЕД ОС. OpenBoard;
- в **VK Видео** — Работа с интерактивными досками в РЕД ОС. OpenBoard.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**OpenBoard**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

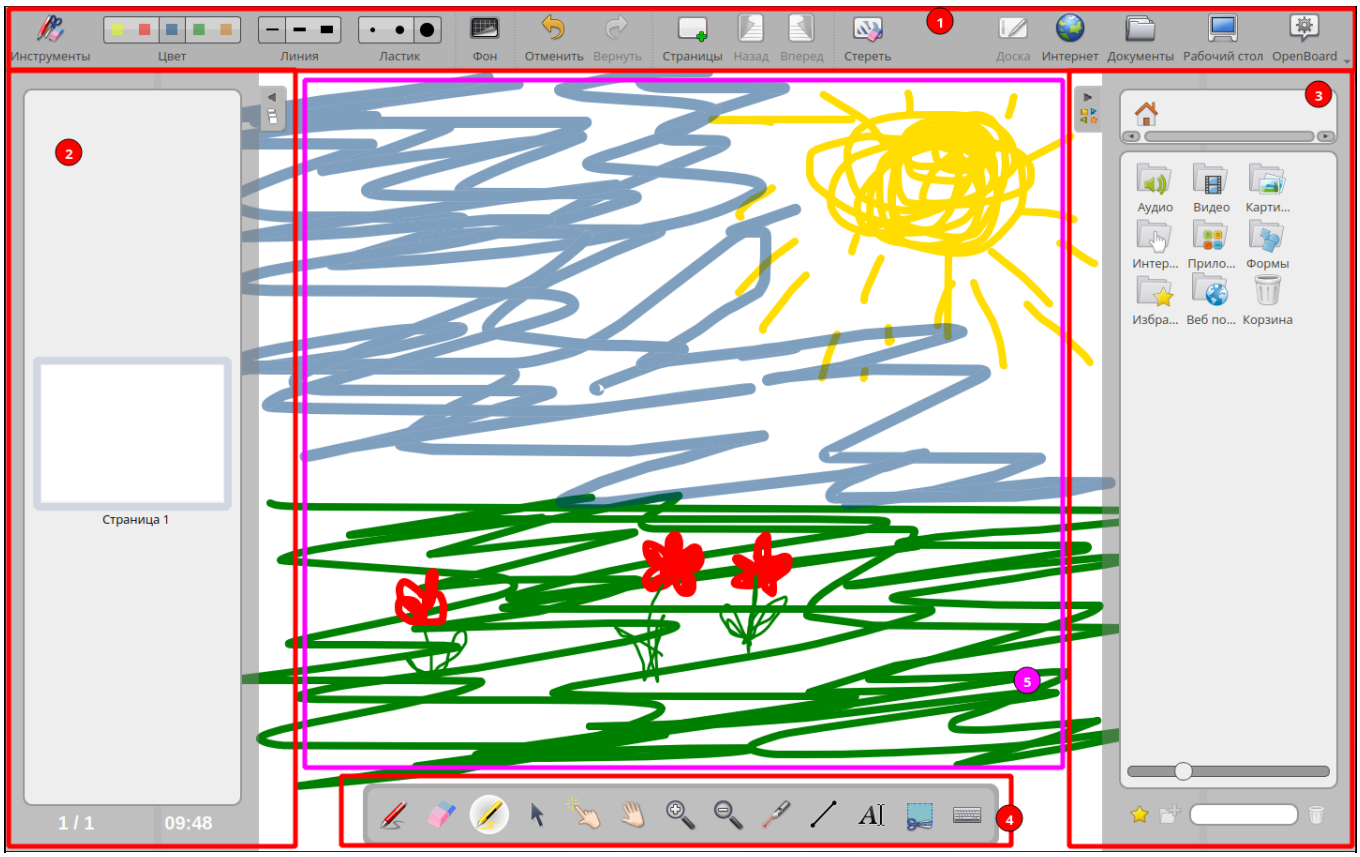
```
dnf install OpenBoard
```

Дальнейшая работа в программе выполняется от локального пользователя.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**OpenBoard**».

Описание программы

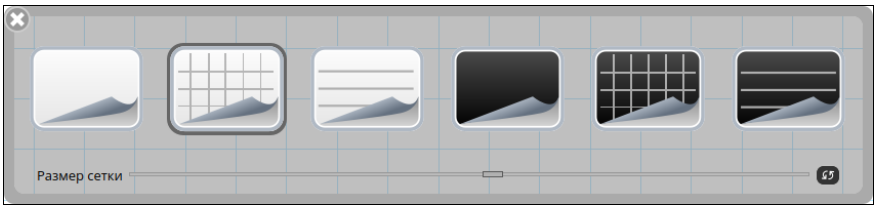
Интерфейс программы довольно прост и разделён на несколько типовых элементов. По умолчанию **OpenBoard** открывается в режиме доски на весь экран.



1. *Панель управления* – здесь доступны основные действия для быстрой работы с программой.

Можно сменить цвет линии, толщину линии, размер ластика.

Доступна смена фона – пустой белый или темный фон, фон с горизонтальными линиями, фон с сеткой, также можно изменить размер сетки.



Далее доступны кнопки для *отмены* или *возврата* выполненных действий, добавление новой пустой страницы и кнопки навигации по страницам (*Назад* и *Вперед*).

Кнопка «**Стереть**» очищает все рабочее пространство.

Далее представлены следующие кнопки:

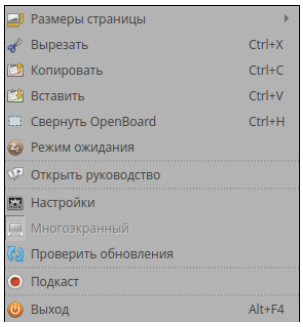
- *Интернет* – встроенный в **OpenBoard** браузер;
- *Документы* – для навигации по документам. Можно загрузить готовую презентацию и, для наглядности, выделять важные моменты и рисовать на слайдах.

  Поддерживаемые форматы программы **OpenBoard**:

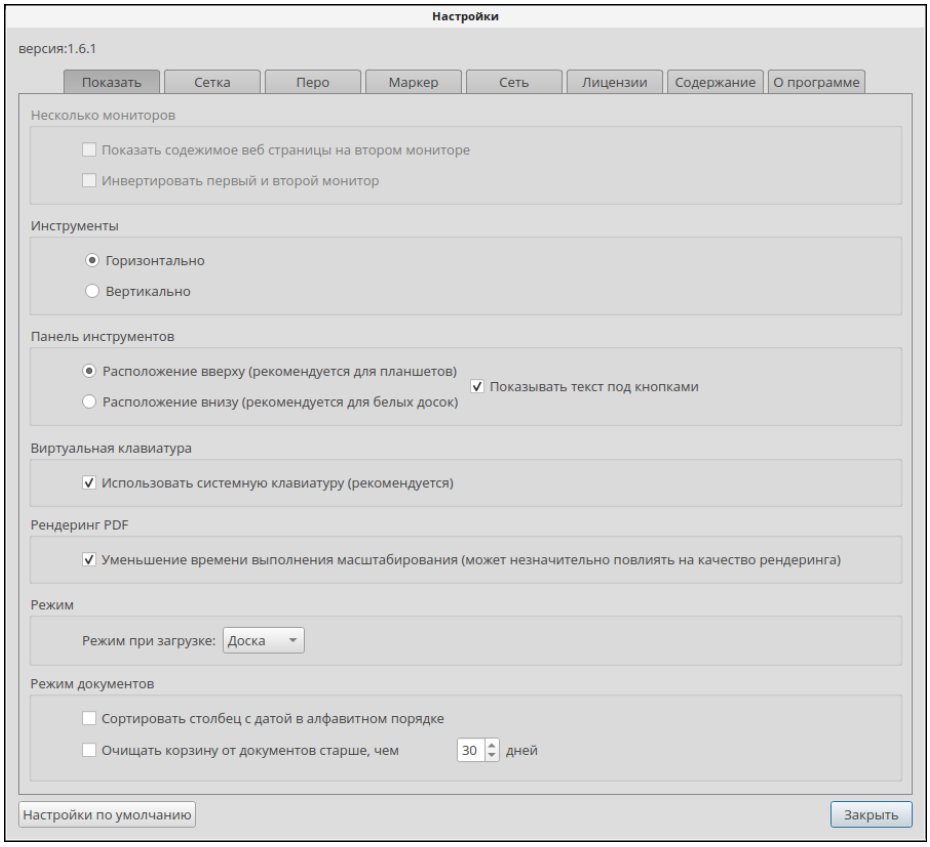
  - файлы, созданные в OpenBoard;
  - файлы в формате **PDF**;
  - изображения в формате **PNG** и **JPG**.

- *Рабочий стол* – кнопка переключения на рабочий стол. В таком режиме панель инструментов **OpenBoard** будет доступна в левой части экрана. Для демонстрации можно открыть браузер или собственный документ и использовать все необходимые инструменты.

- *OpenBoard* – контекстное меню программы с некоторыми дополнительными действиями, такими как выбор размеров страницы, вырезать, копировать, вставить, свернуть программу, перейти в режим ожидания, открыть руководство по программе, пункт настроек программы, проверка обновлений, запись подкаста и выход из программы.

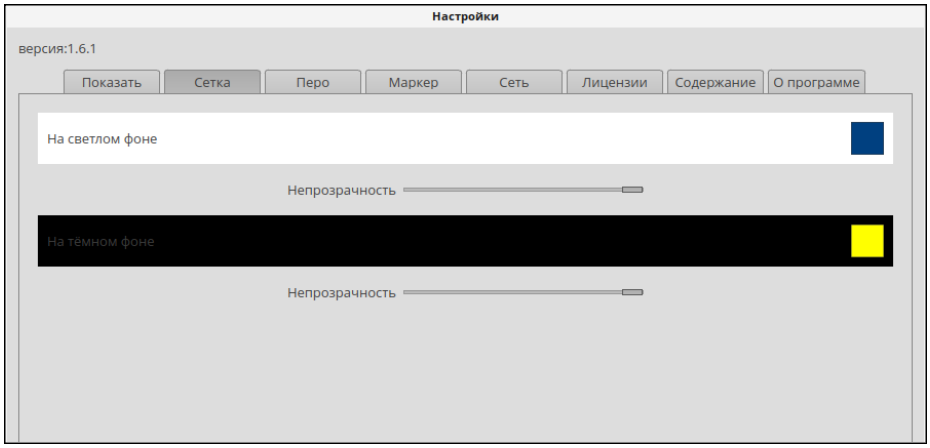


Для детальной настройки программы необходимо открыть пункт меню «**Настройки**».



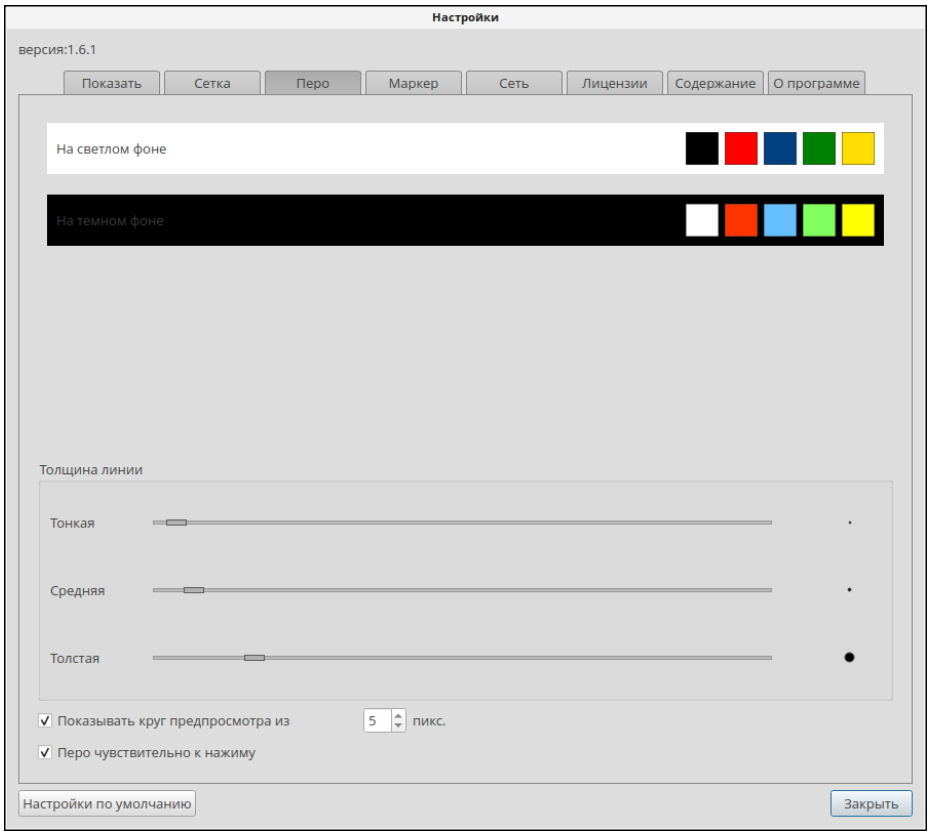
На вкладке «**Показать**» можно изменить отображение инструментов с горизонтального на вертикальное. Если доска висит высоко, полезной функцией будет смена положения панели инструментов. Если требуется компактность, можно убрать текст под кнопками панели инструментов. Далее расположены настройки *системной клавиатуры* и *рендеринг PDF*. Затем можно выбрать режим при загрузке – доска или десктоп.

На вкладке «**Сетка**» доступны настройки линий сетки на белом и темном фоне – непрозрачность и цвет линий.

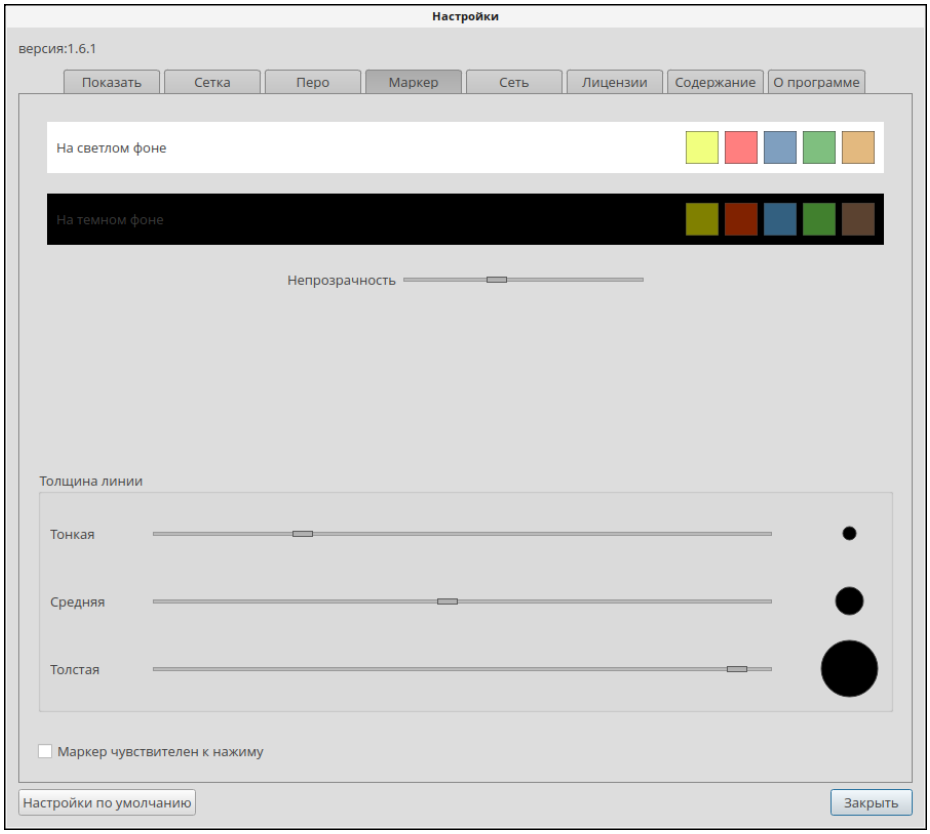


На вкладке «**Перо**» можно настроить доступные в панели инструментов цвета пера на белом и темном фоне, а также задать толщину

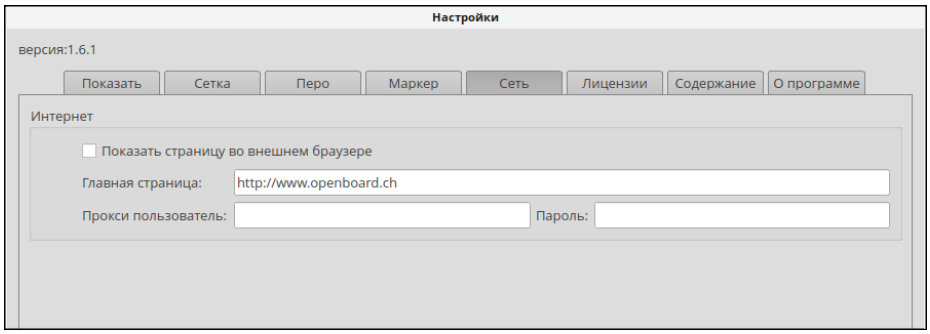
линии для вариантов *тонкая*, *средняя* и *толстая*.



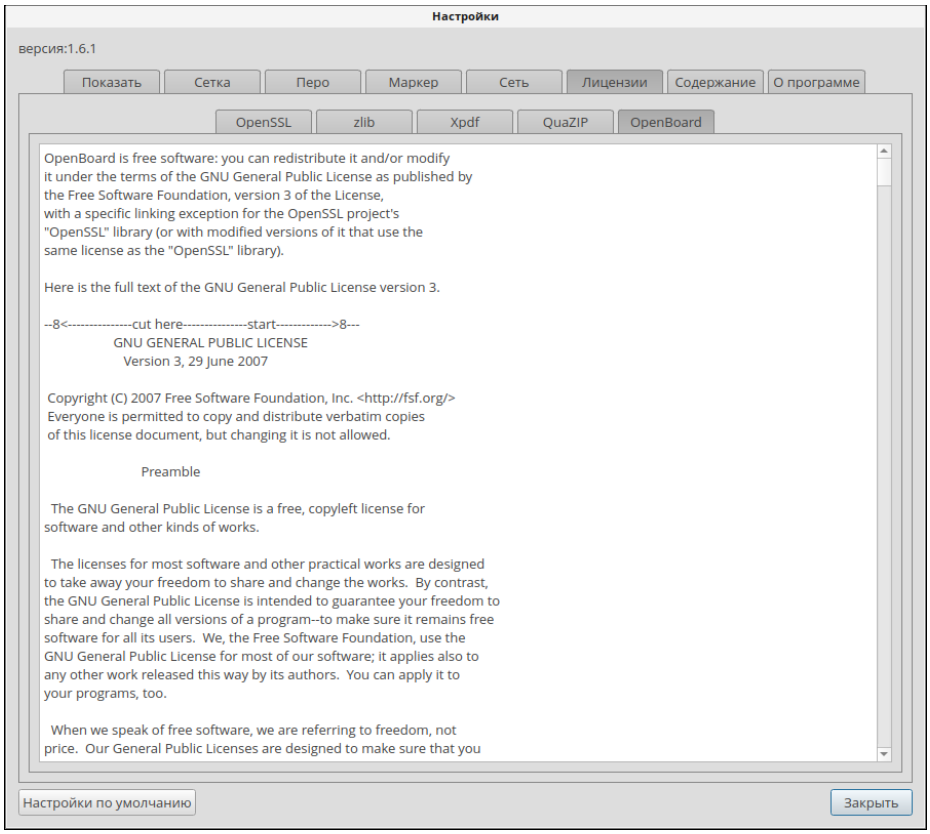
На вкладке «**Маркер**» производится настройка маркера – доступные цвета на светлом и темном фоне доски, непрозрачность, а также задается толщина линии для вариантов *тонкая*, *средняя* и *толстая*.



На вкладке «**Сеть**» задается адрес главной страницы, возможность открытия страниц во внешнем браузере, а также прокси пользователь и его пароль при наличии.



На вкладке «**Лицензии**» доступны необходимые лицензионные соглашения.



На вкладках «**Содержание**» и «**О программе**» приведены благодарности команде и общие сведения о программе.

При нажатии на кнопку «**Настройки по умолчанию**» будут отменены все установленные тонкие настройки и возвращены значения настроек по умолчанию.

2 . *Панель навигации* – здесь отображаются миниатюры открытых страниц. Для перехода к странице выберите соответствующую миниатюру. При наведении указателя на миниатюру страницы появятся кнопки «**Удалить**» и «**Копировать**».

3. *Библиотека встроенных материалов* – объекты распределены по каталогам в соответствии с форматом и тематикой. Для добавления объекта из библиотеки материалов необходимо открыть каталог и выбрать любой нужный объект, затем перенести его с помощью мыши на рабочую область.

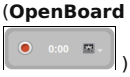
4. *Панель с инструментами для работы в режиме доски* – панель не закреплена, поэтому ее можно перенести в любое удобное место. Доступные инструменты:

- **Карандаш** — отвечает за добавление рукописного объекта;
- **Ластик** — удаление объектов с рабочей области. Размер ластика можно регулировать;
- **Маркер** для выделения — полупрозрачный маркер для выделения текста или другого объекта;
- **Курсор** — позволяет выделить отдельную область, элемент или группу элементов. При нажатии курсором по объекту будут открыты дополнительные настройки, например, изменение размера объекта, изменение положения, растягивание или поворот.
- **Взаимодействие с элементами** (палец) — перемещение объекта по рабочему полю;
- **Ладонь** — прокручивание страницы;
- **Масштаб** — увеличение или уменьшение масштаба рабочей области;

- **Указка** — указывание на объект без перемещения и выделения;
- **Отрезок** — создание отрезка любой длины и цвета;
- **Текст** — ввод текста с клавиатуры;
- **Выделение области** — выделение области для копирования на текущую или новую страницу. Работает аналогично скриншоту. Выделенную область также можно сохранить как файл в библиотеке;
- **Экранная клавиатура** — вызов экранной клавиатуры для ввода текста и навигации. Данный инструмент полезен в режиме рабочего стола.

5. *Основная рабочая область*.

Запись экрана

Полезной опцией для работы также является запись экрана (**OpenBoard** — **Подкаст**). При активации подкаста рядом с нижней панелью инструментов появится инструмент для записи видео (

).

При нажатии на кнопку конфигурирования записи подкаста () будет открыто контекстное меню с выбором использования микрофона при записи экрана, публикация видео в интранете или на Youtube.

Для записи видео необходимо нажать на кнопку «**Начать запись экрана**» ().

Для завершения записи необходимо нажать на кнопку «**Завершить запись экрана**» (). По умолчанию видеозаписи сохраняются на рабочий стол.

Veyon - программа управления компьютерным классом

Настройка сервера
Настройка клиента
Проверка работоспособности

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: veyon-4.5.7

Veyon - это программа для мониторинга и управления компьютерами. Она в основном используется в учебных заведениях для виртуальных тренингов или удаленной поддержки.

Вы можете подробнее ознакомиться с работой утилиты **veyon**, просмотрев наши обучающие видео:

- на **RuTube** — Veyon - программа управления компьютерным классом;
- в **Яндекс.Дзен** — Veyon - программа управления компьютерным классом;
- в **VK Видео** — Veyon - программа управления компьютерным классом.

На наших каналах вы также сможете найти много другой полезной информации.

Veyon предлагает множество функций, которые позволяют вам контролировать и получать доступ к компьютерам. Все функции доступны через кнопки на панели инструментов, а также из контекстного меню отдельных компьютеров.

Функции программы:

Функция	Описание
Режим мониторинга	По умолчанию **Veyon** работает в режиме мониторинга. В этом режиме у вас есть обзор всех компьютеров и содержимого их экранов в виде миниатюр. Содержимое экрана обновляется практически в режиме реального времени, поэтому вы можете отслеживать всю активность на выбранных компьютерах. Пока нет подключения, вместо содержимого экрана отображается значок компьютера. После запуска программы значок изначально окрашен в серый цвет. Как только программа обнаруживает, что компьютер недоступен или доступ запрещен, цвет меняется на красный.
Демонстрационный режим	Вы можете использовать демонстрационный режим, чтобы начать презентацию. В этом режиме содержимое вашего экрана или экрана учащегося транслируется на все компьютеры и отображается в режиме реального времени. Вы можете выбрать между полноэкранной и оконной демонстрацией.
Блокировка экранов	Еще один способ привлечь внимание студентов - использовать функцию блокировки экрана. Как и во время полноэкранного показа, все устройства ввода на компьютерах учеников заблокированы. Компьютеры больше не могут быть использованы учениками. Кроме того, отображается символ блокировки, чтобы не отвлекать внимание от открытых приложений.
Удалённый просмотр и удаленное управление	Функции удаленный просмотр и удаленное управление очень похожи. В обоих режимах доступа экран удаленного компьютера отображается в полном размере в отдельном окне. В отличие от режима мониторинга, вы можете детально наблюдать за действиями на компьютере в отдельном окне или вмешиваться самостоятельно.
Включение, перезагрузка и выключение компьютеров	Функции включения, перезагрузки и выключения питания полезны как для административных целей, так и для подготовки и последующего прохождения курсов и экзаменов. Используя эти функции, вы можете удаленно включать, перезагружать или выключать компьютеры.
Вход в систему	Функция входа в систему позволяет удаленно входить в систему определенному пользователю на всех компьютерах.
Послать текстовое сообщение	Еще одна возможность взаимодействия с пользователем - отправить текстовое сообщение отдельным или всем участникам курса. Текстовое сообщение отображается на компьютерах в виде окна сообщения.
Запустить программу	Если определенная программа должна быть запущена на всех компьютерах, вы можете использовать функцию «Запуск программы» на панели инструментов.
Открыть веб-сайт	Если вы хотите, чтобы все учащиеся открывали определенный веб-сайт, вы можете автоматически разрешить открытие этого веб-сайта на всех компьютерах.
Передача файлов	Используя функцию передачи файлов, вы можете легко передавать файлы всем учащимся и, при необходимости, открывать переданные файлы впоследствии.
Скриншот	Veyon позволяет сохранять текущее содержимое экрана одного или всех компьютеров в файлах изображений.

Настройка сервера

Для установки veyon перейдите в сеанс пользователя root:

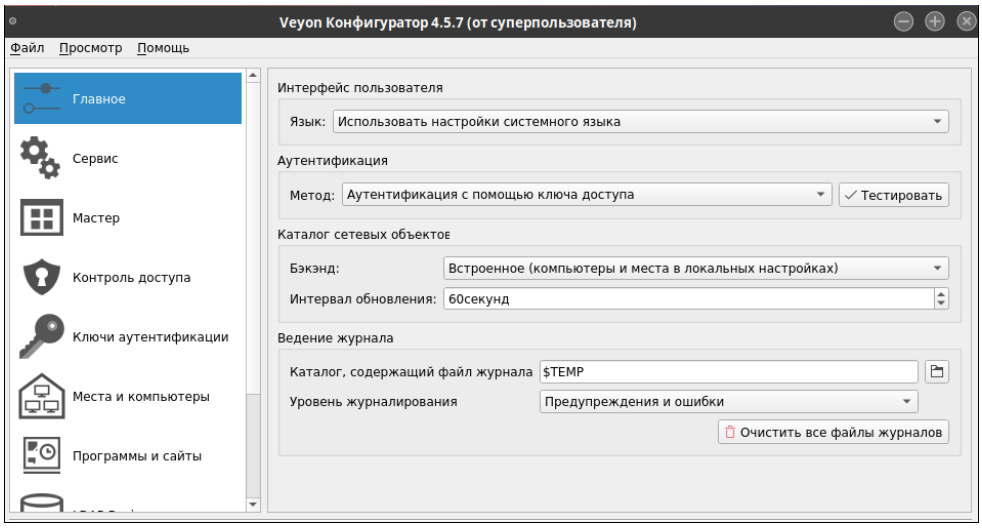
```
su -
```

и выполните команду:

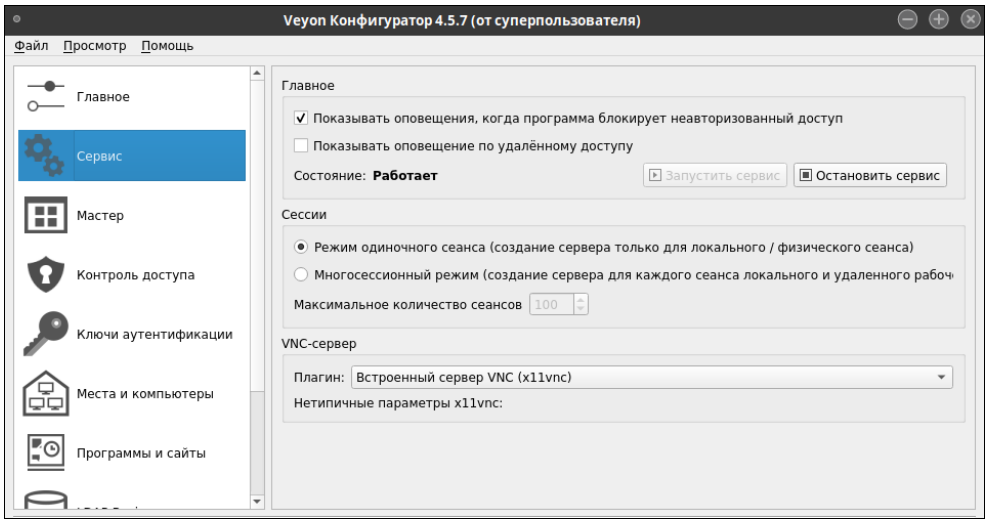
```
dnf install veyon
```

После завершения установки откройте конфигуратор **veyon**. Его можно найти в «**Главном меню**» - «**Администрирование**» - «**Настройка Veyon**».

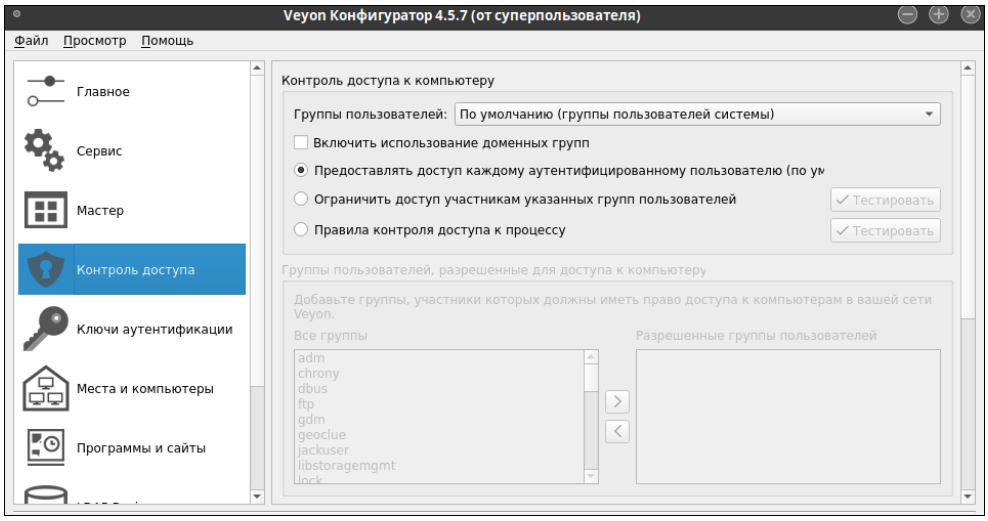
Приступим к настройке. На вкладке «**Главное**» выберите метод аутентификации: «**Аутентификация с помощью ключа доступа**», бэкэнд: «**Встроенное**».



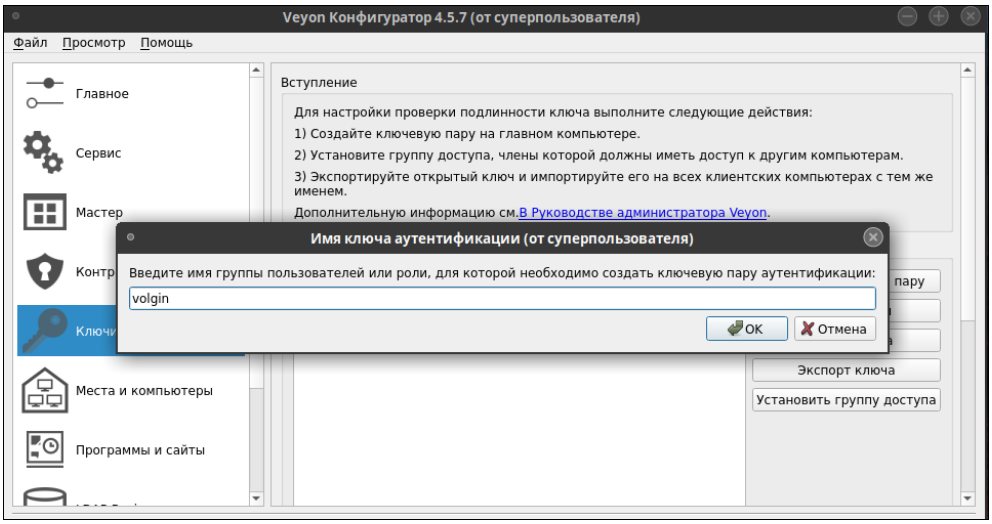
Перейдите во вкладку «**Сервис**», переключите сессии в «**Режим одиночного сеанса**» и запустите сервис.



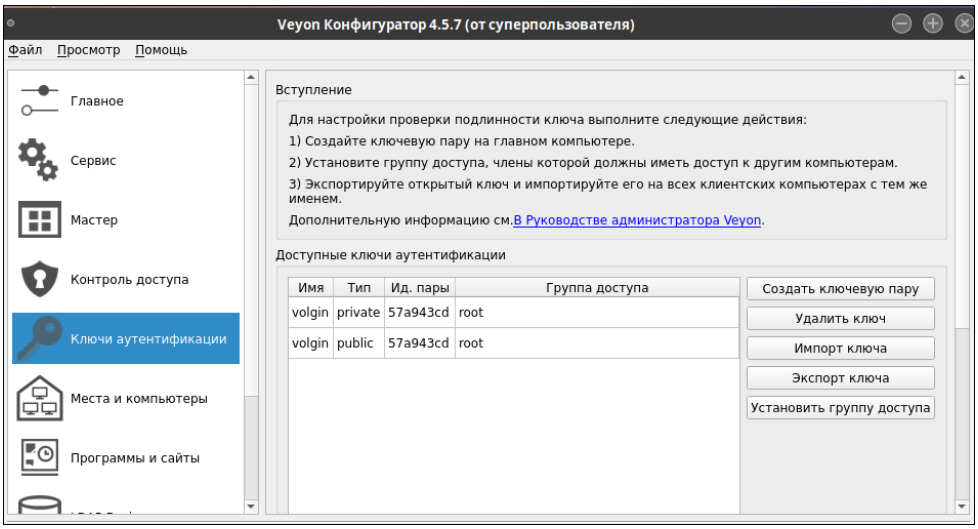
Далее на вкладке «**Контроль доступа**» выставьте группы пользователей: «**По умолчанию**».



На вкладке «**Ключи аутентификации**» нажмите на кнопку «**Создать ключевую пару**» и введите её название.



Будет создано 2 ключа с типом **private** и **public**. Необходимо экспортировать ключ с типом **public** на внешний накопитель. Это нужно для того, чтобы можно было подключиться к клиентскому компьютеру.



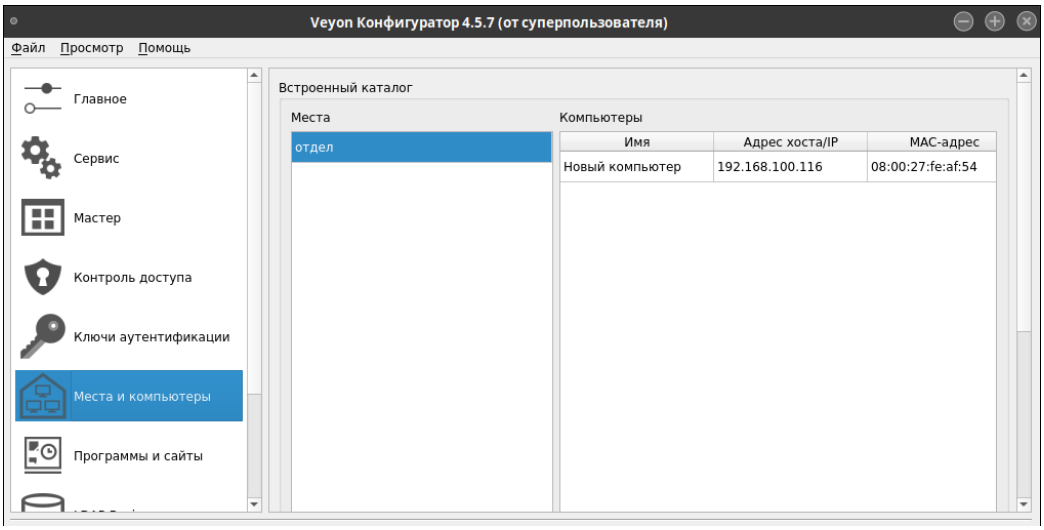
Примечание.

По умолчанию открытый и закрытый ключ будут доступны на чтение всем пользователям (все пользователи будут иметь возможность запускать *Veyon Master*). Чтобы ограничить доступ, необходимо установить группу доступа для закрытого ключа. Пользователи, которым разрешен доступ к компьютерам с помощью *Veyon Master*, должны быть членами группы доступа, заданной для закрытых ключей. Открытый ключ должен быть доступен для чтения всем пользователям.

Для изменения группы доступа следует выбрать ключ и нажать кнопку «**Установить группу доступа**». В открывшемся окне выбрать/указать группу пользователей.

Далее перейдите во вкладку «**Места и компьютеры**». Создайте новое место, дайте ему название, для этого с низу страницы нажмите на «**+**».

Далее добавьте то количество компьютеров клиентов, которое вам требуется. Задайте им имя и укажите **ip**- и **MAC**-адреса.



После этого примените настройки.

Настройка клиента

Для установки veyon перейдите в сеанс пользователя **root**:

```
su -
```

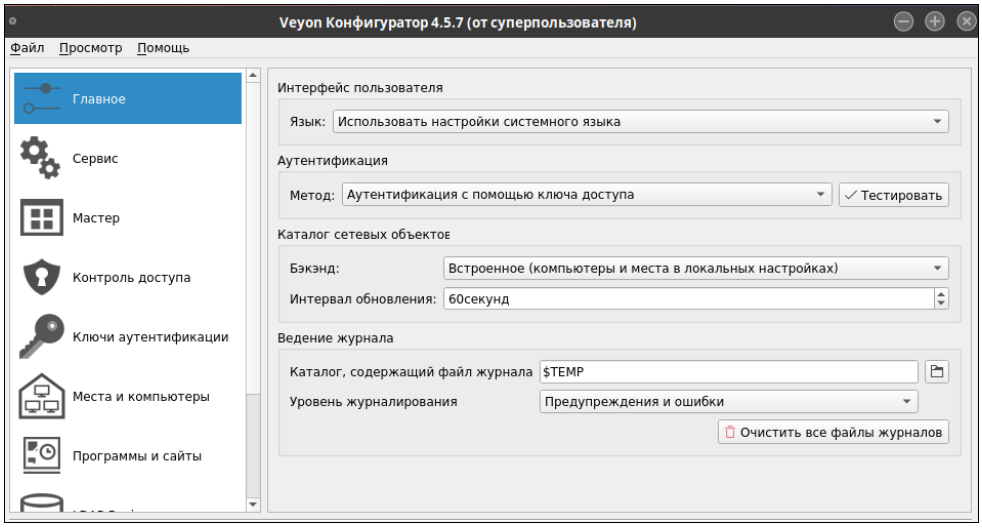
и выполните команду:

```
dnf install veyon
```

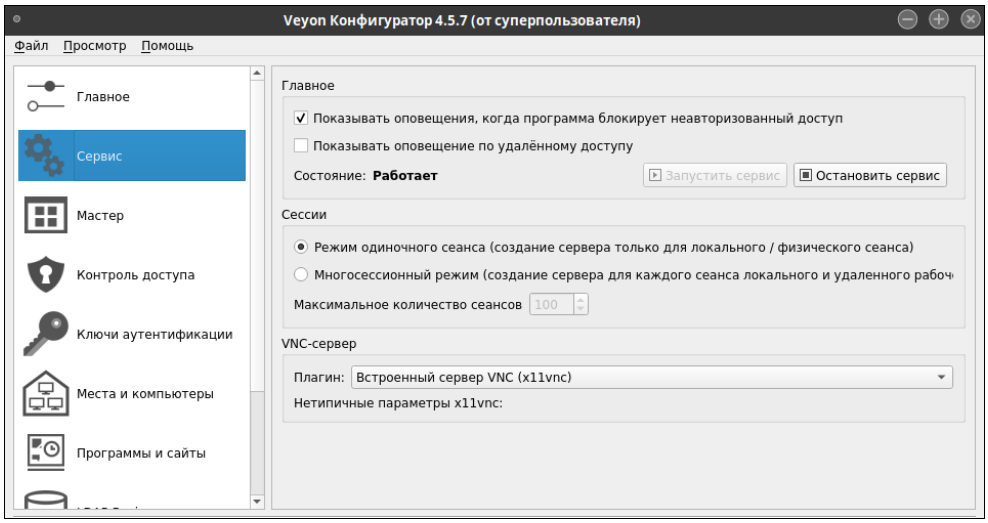
После завершения установки откройте конфигуратор **veyon**. Его можно найти в «**Главном меню**» - «**Администрирование**» - «**Настройка Veyon**».

Откройте «**Настройки Veyon**» и начните настройку программы.

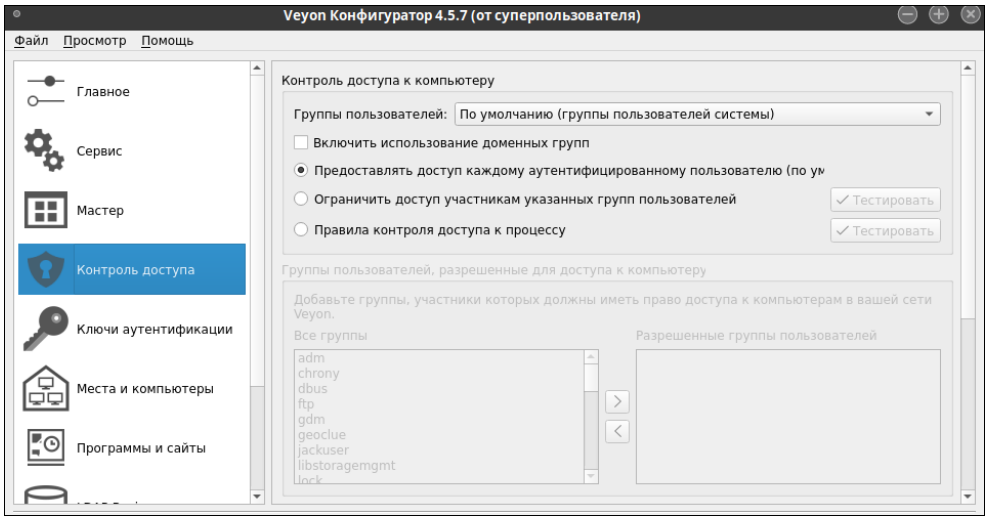
Приступим к настройке. На вкладке «**Главное**» выберите метод аутентификации: «**Аутентификация с помощью ключа доступа**», бэкэнд: «**Встроенное**».



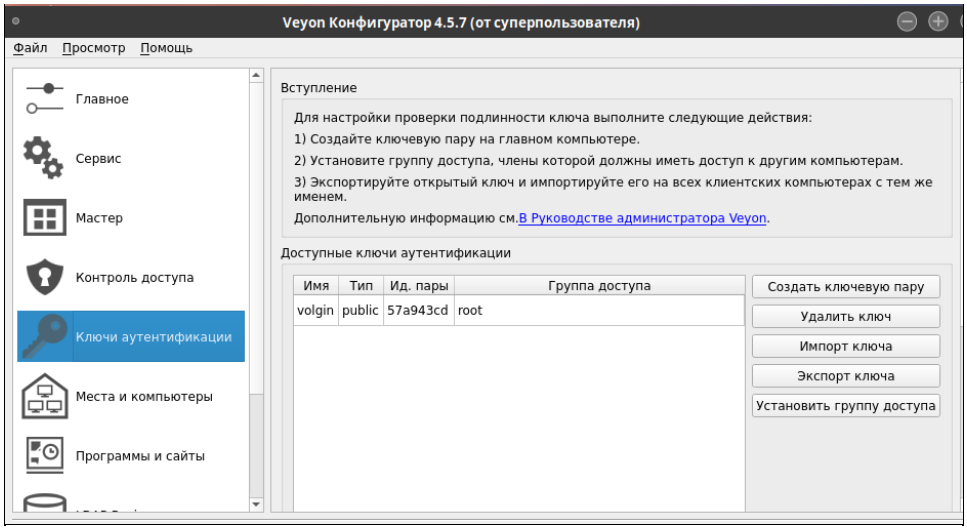
Перейдите во вкладку «**Сервис**», переключите сессии в «**Режим одиночного сеанса**» и запустите сервис.



Далее на вкладке «**Контроль доступа**» выставите группы пользователей: «**По умолчанию**».



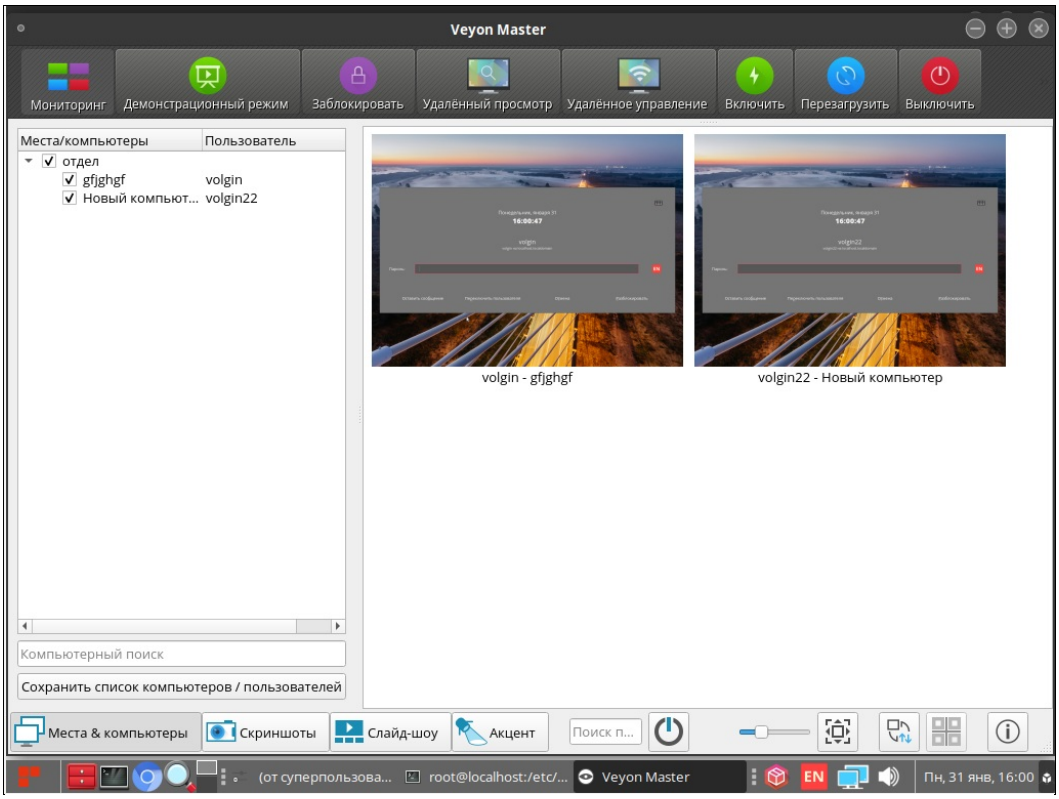
Затем перейдите во вкладку «**Ключи аутентификации**» и импортируйте ключ с внешнего носителя, который вы сгенерировали на сервере.



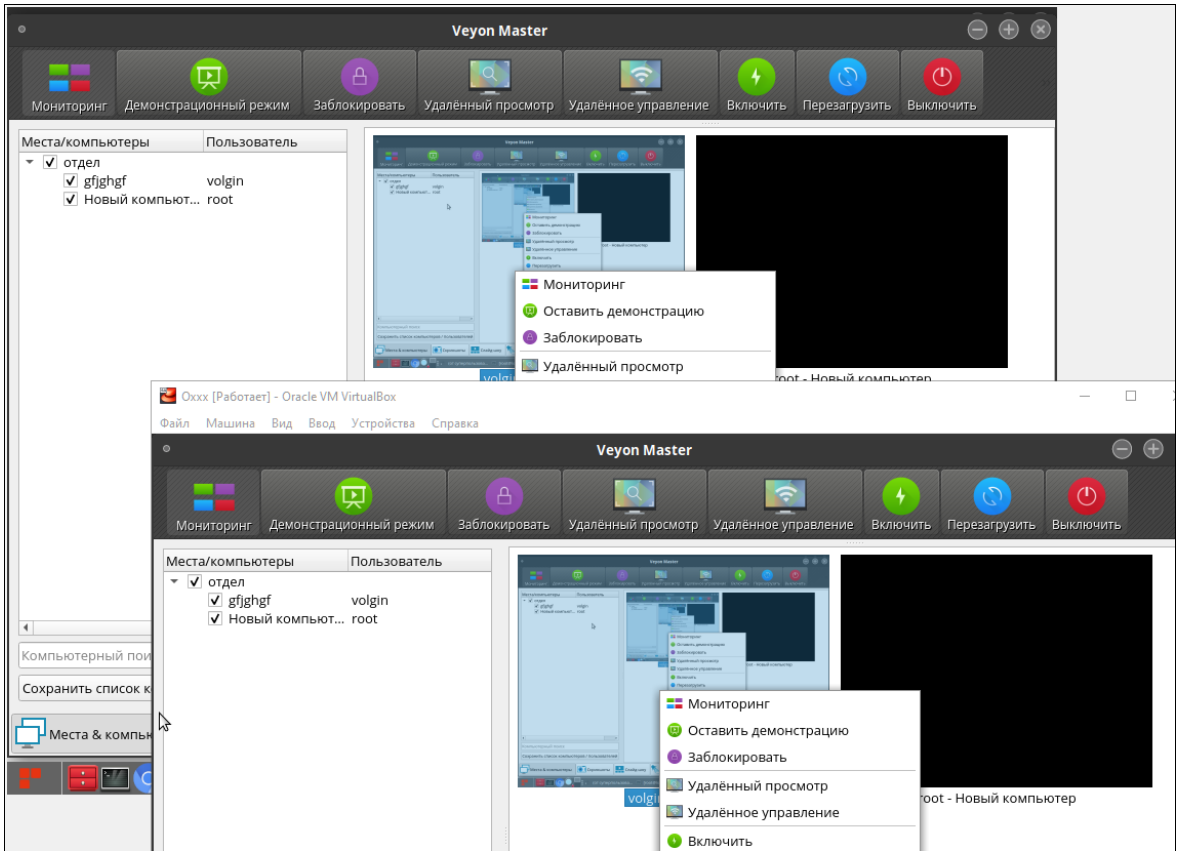
Примените настройки. На этом настройка клиента **veyon** заканчивается.

Проверка работоспособности

Теперь, когда всё настроено, войдите на сервере в «**Монитор Veyon**». Он располагается в «**Главном меню**» - «**Образовательные**» - «**Монитор Veyon**». На вкладке «**Мониторинг**» должны появиться клиентские рабочие места, если компьютеры включены, и всё настроено правильно.



Проверим работоспособность, включив демонстрационный режим.



OpenBabel – программа для работы с химическими структурами и молекулярными системами

Установка OpenBabel
Интерфейс программы и ее основные элементы
Конвертация химических форматов файлов
Разработка на языках программирования C++ и Python
Рекомендации по использованию программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openbabel-2.4.1-3

OpenBabel — экспертная система анализа химических данных, предоставляющая набор инструментов для преобразования многих форматов химических данных. Она позволяет пользователям искать, преобразовывать, хранить и анализировать данные молекулярного моделирования, химии, твердотельных материалов, биохимии или смежных областей.

OpenBabel имеет функции чтения, записи и преобразования более 110 форматов химических файлов, что делает ее универсальным инструментом для работы с молекулярными данными. Она интегрируется с другими программами для химической инженерии и моделирования, такими как Avogadro, GROMACS, XDrawChem, JMol и другими.

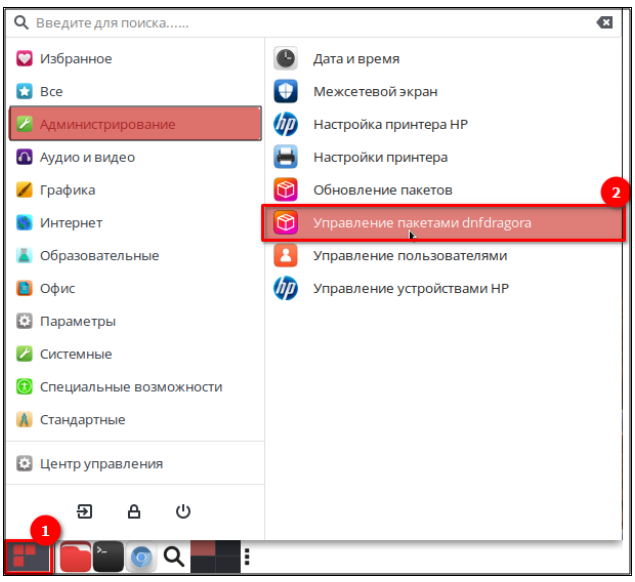
Основные возможности **OpenBabel**:

- конвертация файлов между различными форматами;
- визуализация молекул в 2D и 3D;
- расчет молекулярных свойств, таких как энергия, энтальпия, свободная энергия и т.д.;
- преобразование координат молекул из одной системы в другую;
- интеграция с другими программами и инструментами для химической инженерии;
- поддержка различных типов атомов и связей;
- работа с большими молекулярными сетями;
- поддержка работы с квантово-механическими методами;
- разработка на языках программирования C++ и Python.

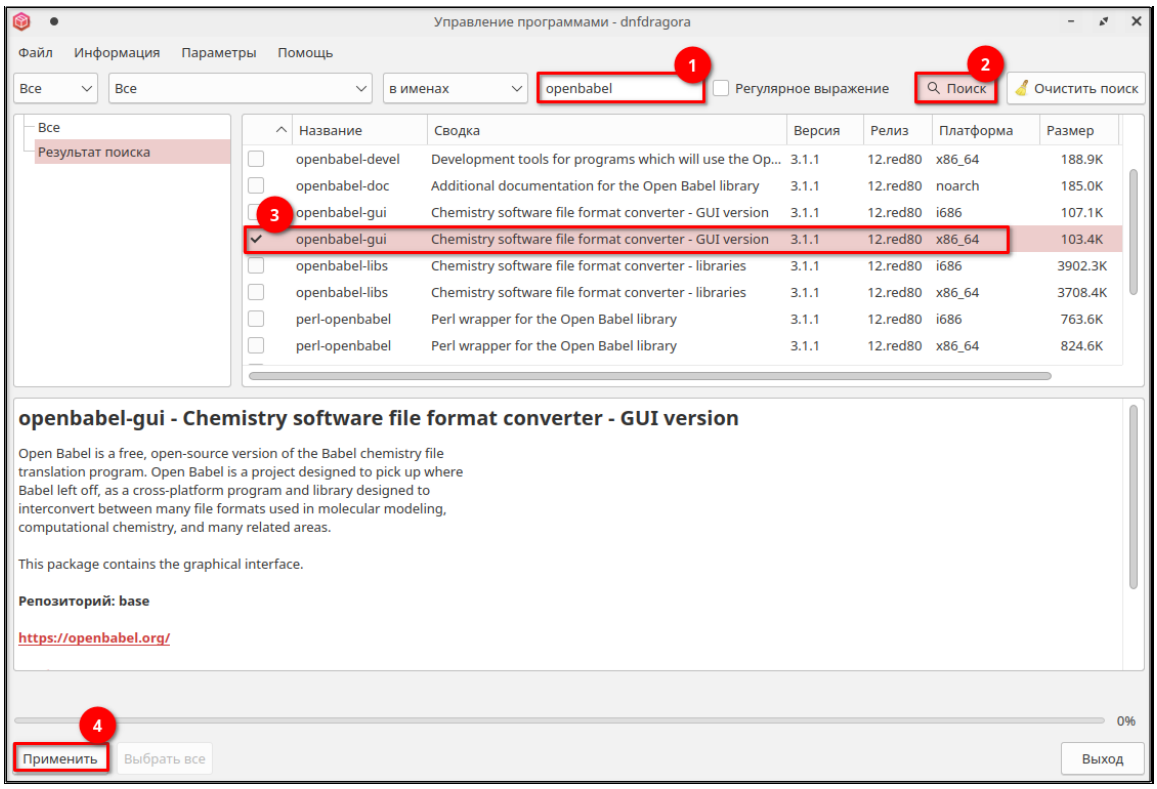
Установка OpenBabel

Программу можно установить через графический менеджер пакетов (**dnfdragora**) или с помощью команд в терминале.

Для установки программы через графический менеджер пакетов перейдите в «**Главное меню**» (1) — «**Администрирование**» — «**Управление пакетами dnfdragora**» (2).



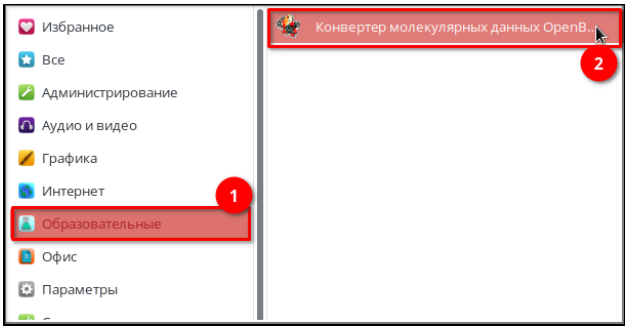
В поисковой строке менеджера пакетов введите ключевое слово «**openbabel**» (1), нажмите кнопку «**Поиск**» (2), выберите пакет «**openbabel-gui**» последней версии для платформы **x86_64**, отметьте флагом (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



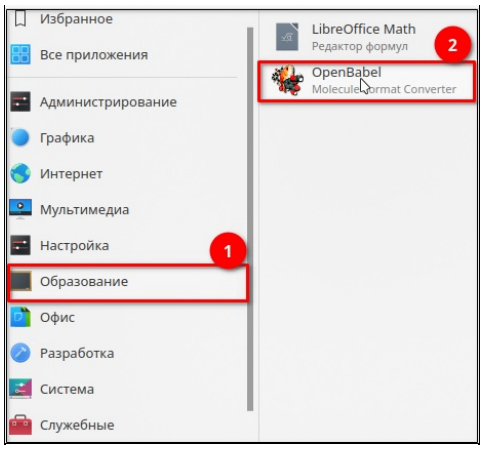
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install openbabel-gui
```

После установки программа будет доступна из «**Главного меню**» – «**Образовательные**» (1) – «**Конвертер молекулярных данных OpenBabel**» (2). (РЕД ОС 7.3)

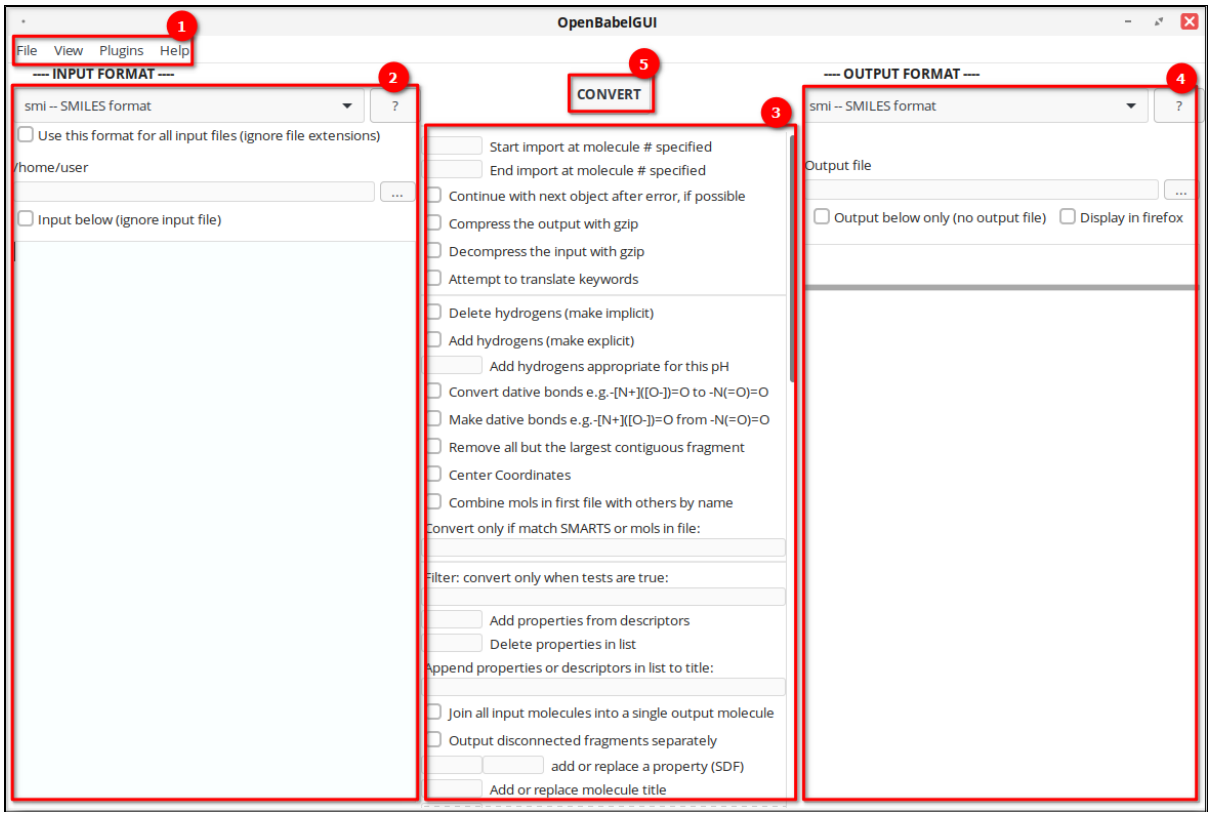


После установки программа будет доступна из «**Главного меню**» – «**Образование**» (1) – «**OpenBabel**» (2). (РЕД ОС 8)



Интерфейс программы и ее основные элементы

Программа **OpenBabel** имеет простой и понятный интерфейс. Главное окно программы содержит следующие элементы: главное меню (1), область формата входных данных (2), область выбора параметров (3), область формата выходных данных (4), кнопка конвертирования (5).



1. Главное меню включает:

- меню «**File**» («**Файл**») - здесь можно копировать, конвертировать, сохранить данные или конфигурацию экрана;
- меню «**View**» («**Вид**») - настраивает вид области для выбора параметров, можно отключить или подключить панели выбора параметров;
- меню «**Plugins**» («**Плагины**») - можно подключать дополнительные функции (например, различные методы определения частичных или парциальных зарядов, индексацию линейных фрагментов, канонически закрепить порядок атомов, генерирование двумерных и трехмерных координат);
- меню «**Help**» («**Помощь**») - позволяет просмотреть информацию о программе.

2. Область формата входных данных «**INPUT FORMAT**».

Выберите тип типа входного файла из раскрывающегося списка (например, **SD**, **SMILES**, **VMOL**, **XML**, **SDF**, **PNG**, **MPC**, **MRV**, **PDB** или другие форматы)

Нажмите кнопку ... и выберите файл, который необходимо конвертировать.

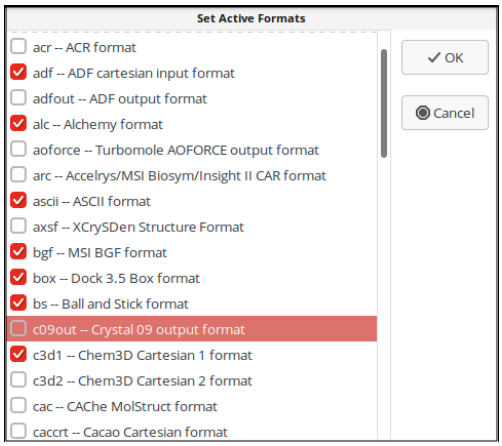
Вы можете выбрать несколько входных файлов в диалоговом окне.

Содержимое файла отобразится в текстовом поле ниже.

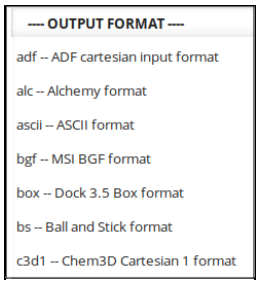
3. Область формата выходных данных «**OUTPUT FORMAT**».

Аналогичным образом выберите выходной формат и файл, в который необходимо преобразовать данные.

Если необходимо использовать только часть большого количества форматов, поддерживаемых **OpenBabel**, вы можете ограничить выбор, предлагаемый в раскрывающихся списках, что упрощает рутинный выбор. В раскрывающемся меню «**View**» нажмите кнопку «**Select set of formats**» («**Выбрать набор форматов**») для изменения отображаемых форматов. Отметьте флагами нужные форматы.



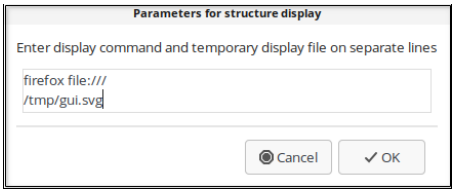
Впоследствии нажатие кнопки «**Use restricted set of formats**» («**Использовать ограниченный набор форматов**») в меню «**View**» включает и выключает эту функцию. Выбранные форматы отобразятся в областях входных и выходных данных.



Включив подстановочный знак * в имена входных и выходных файлов, вы можете выполнить пакетное преобразование (например, ***.smi**, ***.mol** и др.). Если имя выходного файла было **File_*.mol**, то выходные файлы будут иметь имя **File_first.mol** и т. д.

Вы можете отобразить выходные данные ниже в рабочей области, не выбирая при этом выходной файл. Для этого нужно установить флаг «**Output below only (no output file)**».

Преобразуемые химические структуры могут отображаться (в формате **SVG**) во внешней программе. По умолчанию используется **Firefox**, но его можно изменить в пункте меню « **View**» - «**Configure structure display**» (например, на **Opera** или **Chrome**).



Если установлен флаг «**Display in firefox**»» (под именем выходного файла), структуры будут отображаться на новой вкладке **Firefox**.

При наличии нескольких молекул изображение можно масштабировать (с помощью колеса мыши) и панорамировать (перетаскиванием нажатой левой кнопкой мыши). Довольно быстро обрабатывается до 100 молекул одновременно, при большем количестве молекул система конвертации работает медленнее.

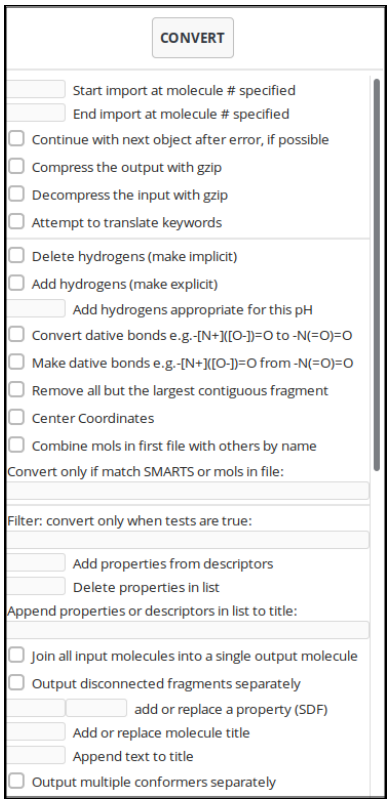
Генерация также может производиться медленнее при вычислении двумерных координат атомов. Новая вкладка браузера **Firefox** будет открываться каждый раз при нажатии кнопки «**CONVERT**» («**Преобразовать**»).

4. Область выбора параметров.

Опции параметров соответствуют типу преобразуемого химического объекта (молекула или реакция), а также форматам ввода и вывода. Вы можете отключить отображение любого из различных типов параметров с помощью меню «**View**».

Можно задать дополнительные параметры:

- сжать данные с помощью **zip**;
- распаковать данные;
- удалить или добавить водород;
- удалить самые крупные смежные фрагменты;
- отцентрировать координаты соединения;
- добавить или заменить название молекулы;
- добавить заголовок или текст;
- сгенерировать трехмерные или двухмерные координаты.



5. Кнопка «**CONVERT**» конвертирует данные выбранных форматов.

В окне сообщений под кнопкой будет указано количество преобразованных молекул, а также отобразится содержимое выходного файла.

По умолчанию все молекулы во входном файле преобразуются, если выходной формат допускает несколько молекул.

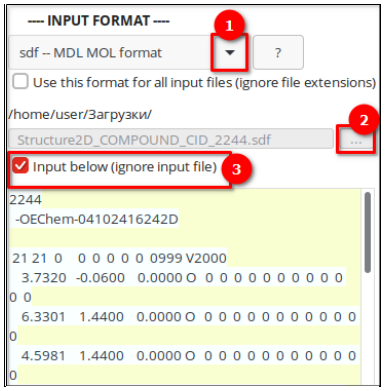
Конвертация химических форматов файлов

Наиболее распространенным применением **Open Babel** является преобразование химических форматов файлов. Ниже приведены примеры использования данной функции. Предварительно файлы для преобразования необходимо загрузить из банка данных химических веществ (например, **Pubchem**) или программ редактирования молекул (**Avogadro**, **GROMACS**, **XDrawChem** и др.).

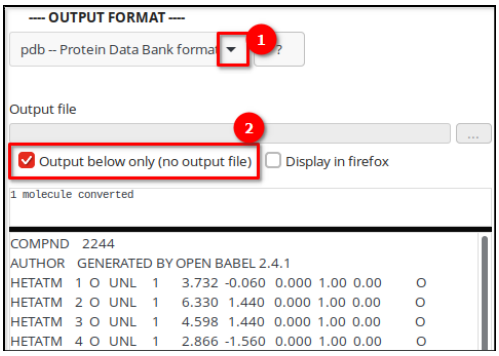
ПРИМЕР 1

Для конвертации файла формата **SDF** в формат **PDB** выполните следующие действия:

1. Установите формат входного файла **SDF** (1), загрузите файл (2), установите флаг «**Input below (ignore input file)**» (3) для считывания входных данных.



2. Установите формат выходного файла **PDB** (1) – формат банка данных трехмерных структур белков и нуклеиновых кислот. Установите флаг «**Output below only (no output file)**» (2) для вывода информации о преобразовании в поле ниже.



3. Установите дополнительные параметры при необходимости.

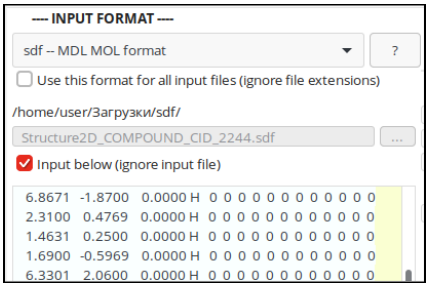
4. Выполните конвертирование, нажав «**CONVERT**».

ПРИМЕР 2

Рассмотрим пример конвертации файла формата **SDF** в **SMI** формат:

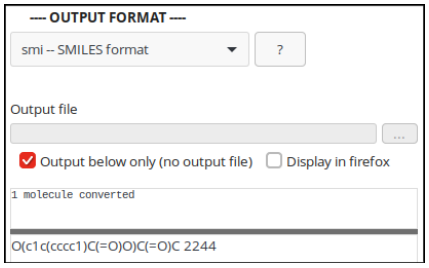
1. В области «**INPUT FORMAT**» выберите формат **SDF,** далее укажите путь к файлу.

2. Установите флаг «**Input below (ignore input file)**» для считывания входных данных.



3. В области «**OUTPUT FORMAT**» в качестве выходного формата выберите «**SMI — SMILES format**» и отметьте флагом параметр для вывода информации о преобразовании в поле ниже «**Output below only (no output file)**».

4. В информационном поле отобразится описание состава и структуры молекулы.



Разработка на языках программирования C++ и Python

Если у вас есть опыт программирования на **C++** или **Python**, вы можете использовать **OpenBabel** как основу для создания своих приложений или скриптов.

Интерфейс **Python** для **OpenBabel** предоставляет два модуля, которые можно использовать для доступа к функциональности набора инструментов:

1. Модуль **OpenBabel** - он содержит стандартные привязки **Python**, автоматически созданные из **API C++**.

2. Модуль **Pybel** - это оболочка классов и методов модуля **openbabel**. Pybel предоставляет более удобные способы доступа к набору инструментов **Open Babel**.

Для отображения 2D-форматов с помощью **Pybel** необходимо установить библиотеки **Pillow** (python3-pillow) и **Tkinter** (python3-tkinter). Обычно данные библиотеки установлены по умолчанию. В случае если они были отключены, их можно подключить через менеджер пакетов **dnfdragora** или через **терминал**.

Для установки библиотеки **Pillow** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install python3-pillow
```

Для установки библиотеки **Tkinter** выполните команду:

```
sudo dnf install python3-tkinter
```

Модуль openbabel обеспечивает прямой доступ к библиотеке **C++ Open Babel** из **Python**. Такая привязка создается с помощью пакета **SWIG** и обеспечивает доступ практически ко всем интерфейсам **Open Babel** через **Python**, включая базовые классы **OBMol**, **OBAtom**, **OBBond** и **OBResidue**, а также платформу преобразования **OBConversion**.

Рекомендации по использованию программы

1. Большинство параметров интерфейса, таких как выбранный формат, размер и положение окна, сохраняются между сеансами.
2. Конвертацию можно проводить без файлов. Вместо использования входных и выходных файлов можно вставить содержимое химического формата файла в поле ввода и просмотреть результаты преобразования в поле вывода.
3. При работе с другими программами рекомендуется интегрировать OpenBabel для удобства использования и получения более точных результатов.
4. При работе с большими молекулярными сетями необходимо учитывать ограничения программы и использовать дополнительные инструменты для оптимизации работы.
5. Рекомендуется регулярно обновлять программу, чтобы получить доступ к новым функциям и улучшениям.

XDrawChem – программа для рисования и анализа химических структур и реакций

Установка XDrawChem
Описание программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** XDrawChem-1.10.2

XDrawChem — это графическое приложение для рисования и анализа химических веществ, схем реакций. Программа предоставляет возможность редактирования химических структур в 2D-формате, а также анализа и хранения химических данных молекулярного моделирования, биохимии, твердотельных материалов или смежных областей. **XDrawChem** позволяет создавать химические структуры с фиксированными длинами связей и углами, автоматически рисует кольцевые системы, выравнивает структуры в реакциях и генерирует структурные диаграммы.

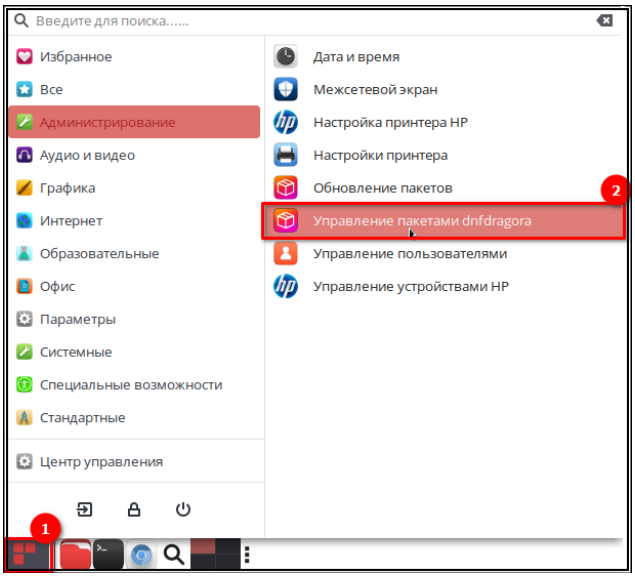
XDrawChem может работать с собственным файловым форматом, совместим с файлами **Chemdraw** и форматами, поддерживаемыми пакетом **OpenBabel** (***.cml**, ***.mdl**, ***.cif**, ***.mol**, ***.sd**, ***.sdf** и **др.**), а также позволяет экспортировать изображения в форматы: **PNG**, **BMP**, **EPS** и **SVG**.

XDrawChem предоставляет *прогнозы 13C-ЯМР* и *1H-ЯМР*, простое *ИК-прогнозирование*, простую *оценку pKa*, оценку *коэффициента распределения октанол-вода*, а также проводить *анализ реакций*, включая оценку изменения *энтальпии в газовой фазе* и сравнение *ЯМР 1H* и *ЯМР 13C*.

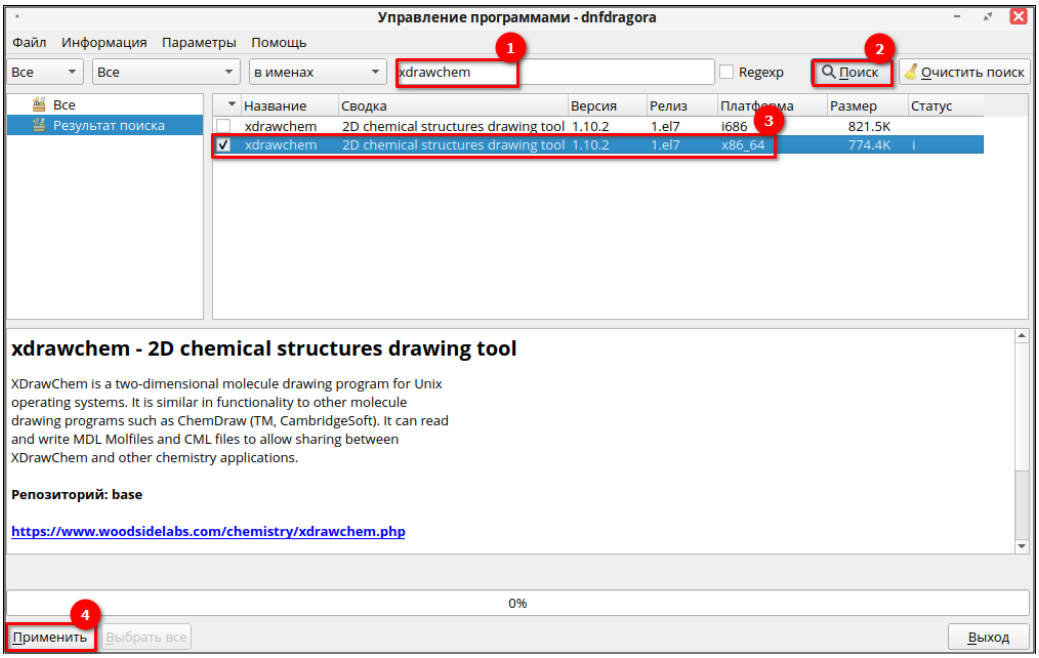
Установка XDrawChem

Программу можно установить через графический менеджер пакетов (**dnfdragora**) или с помощью команд в терминале.

Для установки программы через графический менеджер пакетов перейдите в «**Главное меню**» (1) — «**Администрирование**» — «**Управление пакетами dnfdragora**» (2).



В поисковой строке менеджера пакетов введите ключевое слово «**xdrawchem**» (1), нажмите кнопку «**Поиск**» (2) и отметьте флагом пакет последней версии для платформы **x86_64** (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



Для установки программы через **терминал** (**Ctrl+Alt+T**) перейдите в сеанс пользователя **root**:

```
su -
```

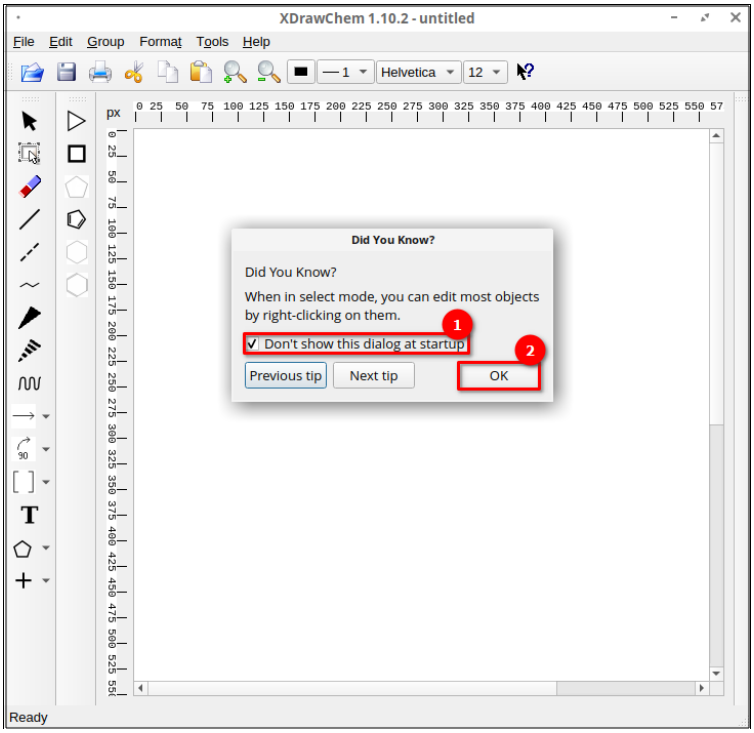
Далее выполните команду установки:

```
dnf install xdrawchem
```

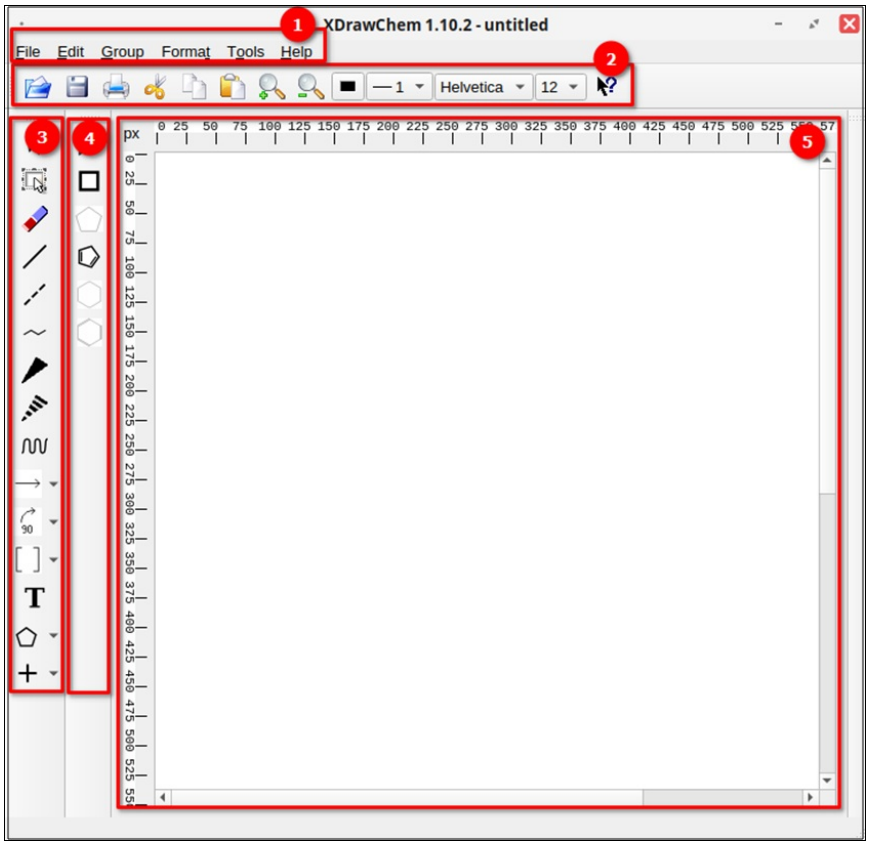
После установки программа будет доступна из «**Главного меню**» – «**Образовательные**» – «**Рисование хим. формул**».

Описание программы

При первом запуске появляется окно с различными подсказками по использованию программы. Для отключения данного окна при запуске программы поставьте флаг рядом с надписью «**Не показывать это диалоговое окно**» (1) и нажмите кнопку «**OK**» (2).



Окно программы выглядит следующим образом:



Интерфейс программы **XDrawChem** представлен в стандартном виде и состоит из следующих основных элементов:

1. Основное меню программы: содержит различные команды и опции, позволяющие управлять функциями программы, открывать и сохранять файлы, настраивать параметры и многое другое. Главные пункты меню включают:

- **Файл** (File): создание, открытие, поиск в интернете, сохранение, экспорт, настройка страницы, печать, закрытие, выход.
- **Редактирование** (Edit): отмена, вырезать, копировать, вставить, удалить, отменить выбор, повернуть, масштабировать.
- **Группа** (Group): выбор реактанта, выбор продукта реакции, очистка одной или всех групп.
- **Формат** (Format): установка цвета фона, настройки рисования, переключение сетки, отрисовка с фиксированными длинами отрезков и углами, настройки XDC.
- **Инструменты** (Tools): информация о молекуле, автоматическое распределение, *прогнозы 13C-* и *1H-ЯМР*, *простое ИК-прогнозирование*, простая оценка pKa, оценка коэффициента распределения октанол-вода, анализ реакций.
- **Помощь** (Help): дополнительная информация о программе.

2. Панель инструментов: стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы, таким как создать, сохранить, напечатать, вырезать, копировать, вставить и др.

3. Панель инструментов для рисования:

 Инструмент «Выбрать» (Select) предназначен для выбора и перемещения элементов внутри рамки. Можно выбрать несколько элементов, вырезать, копировать, перемещать и вращать их.

 Инструмент для создания лассо (Lasso) используется для выбора и перемещения элементов, рисуя петлю вокруг них. Доступны к выбору также несколько элементов.

 Инструмент «Стереть» (Erase) предназначен для удаления отдельных элементов.

 Линейный инструмент (Draw Line) используется для рисования связей. Обведите существующие связи, чтобы создать двойные и тройные связи.

 Инструмент «Пунктирная линия» (Draw dashed line) позволяет провести поверх существующих связей пунктирные линии.

 Инструмент «Цепи» (Draw aliphatic chain) дает возможность нарисовать ациклические (или алифатические) соединения.

 Инструмент для создания стереофонической восходящей линии (Draw stereo-up line) позволяет нарисовать дополнительные линии.

 Инструмент для создания стереофонической нисходящей линии (Draw stereo-down line) используется для отображения нисходящих линий.

Инструмент для создания волнистых линий (Draw wavy bond).

Инструмент «Стрелка» (Regular Arrow) позволяет рисовать простые стрелки. При нажатии и удержании можно выбирать из списка доступные стрелки.

Инструмент для рисования изогнутых стрелок используется для создания изогнутых стрелок и кубической кривой Безье.

«Квадратная скобка» (Square bracket) позволяет добавлять квадратные скобки к химическим структурам.

«Надпись» (Draw or edit text) предоставляет возможность создавать или редактировать текстовые блоки в редакторе химических структур.

Инструмент химических элементов (Chemical elements) предназначен для добавления или редактирования химических элементов.

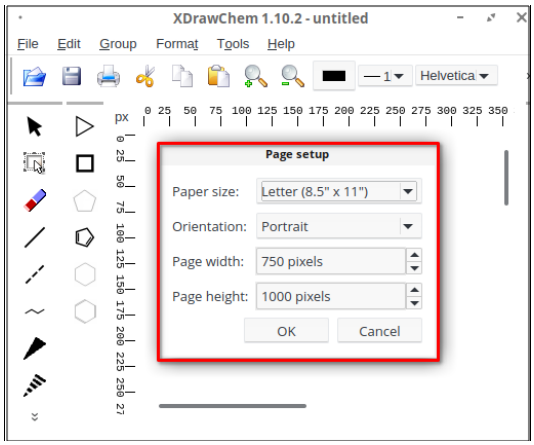
Инструмент для создания символов (Symbol tool) используется для добавления различных символов к химическим структурам.

4. Дополнительная панель инструментов: содержит инструменты для создания и редактирования химических структур.

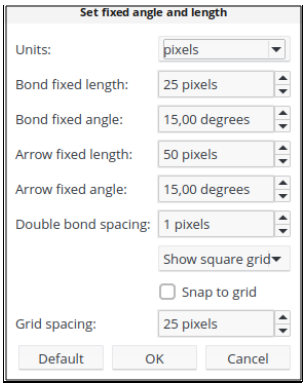
5. Рабочая область: здесь отображается сама химическая структура, которую вы создаете или редактируете, а также другие графические объекты.

XDrawChem обладает гибким пользовательским интерфейсом, который позволяет перемещать и отключать панели инструментов.

Для настройки страницы перейдите в «**File**» - «**Page setup**» и выберите необходимые опции.

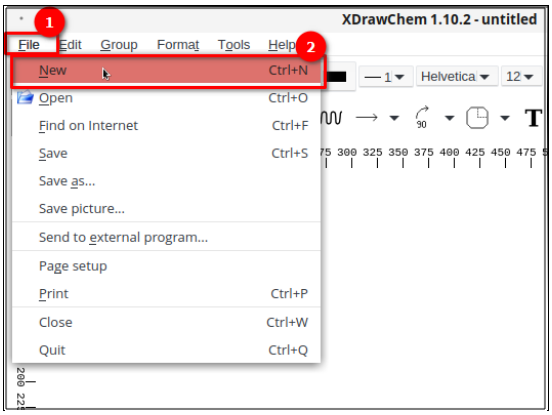


Для настройки рисования перейдите в «**Format**» - «**Drawing settings...**» и установите фиксированный угол и длину отрезка.



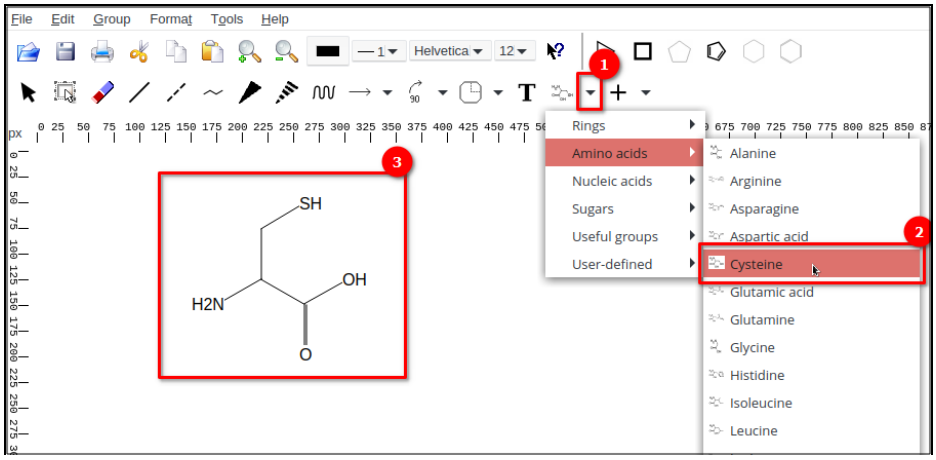
Пример работы

1. Для создания нового проекта необходимо перейти в основное меню программы в «**File**» (1) - «**New**» (2) или воспользоваться комбинацией клавиш «**Ctrl + N**».

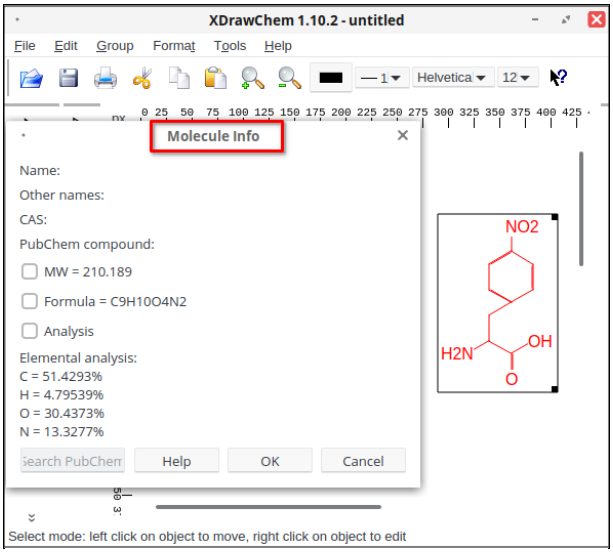


2. Взаимодействие с инструментами.

В **XDrawChem** доступны все стандартные аминокислоты и нуклеиновые кислоты во встроенной библиотеке. Например, для того чтобы разместить в рабочей области схему аминокислоты цистеина, необходимо открыть выпадающий список химических веществ (1), выбрать «**Amino acids**» - «**Cysteine**» (2), кликнуть ЛКМ в рабочей области (3). Изображение можно увеличить, повернуть и переместить.

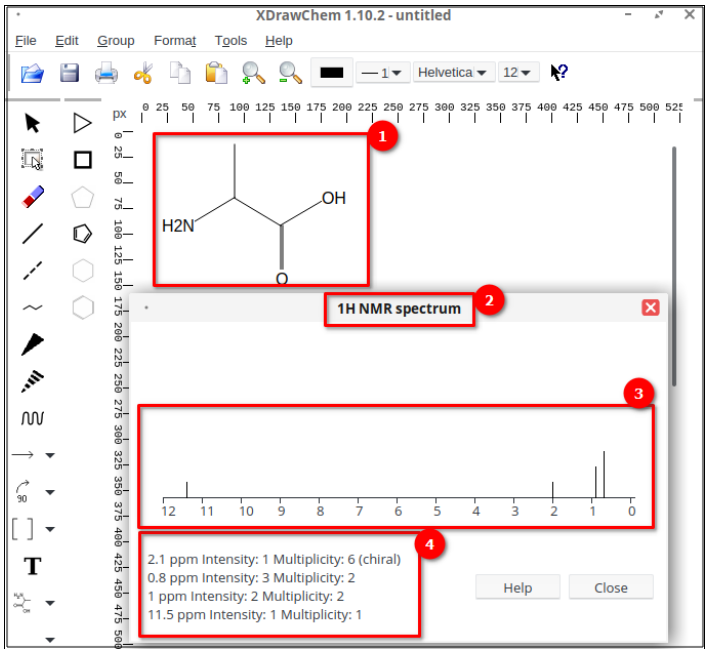


Для получения детальной информации о любом веществе в рабочей области необходимо его выделить, перейти в меню «**Tools**» - «**Molecule information...**» или воспользоваться сочетанием клавиш (**Ctrl + I**). Отобразится информация о средневесовой молекулярной массе (**MW**), формула вещества, элементарный анализ.

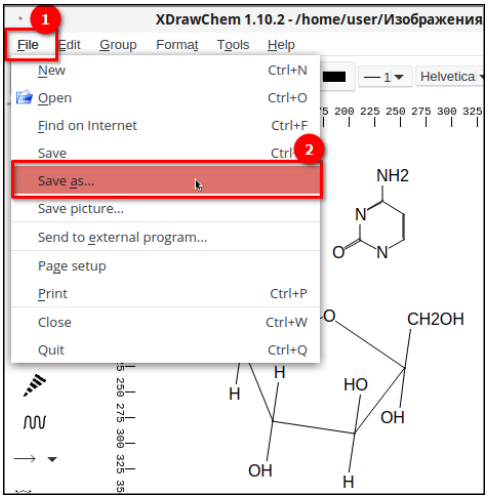


Для получения *1H ЯМР* анализа перейдите в главное меню в «**Tools**» - «**Predict 1H NMR**» и выделите соединение в рабочей области (1). Инструмент *1H NMR spectrum* (2) выведет спектр (3) и структуру соединения (4).

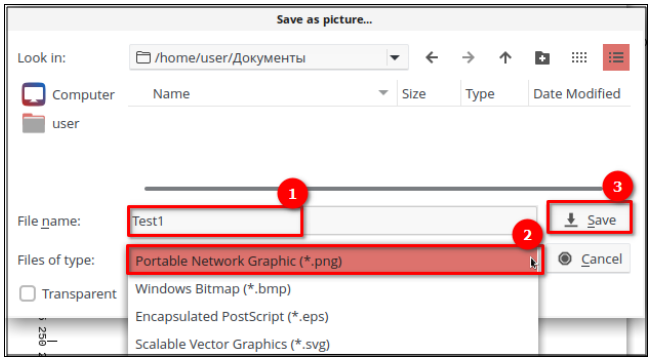
Например, спектр *1H ЯМР* аланина представляет собой 4 сигнала с химическими сдвигами 0.8, 1, 2.1 и 11.5 м. д.:



3. Для сохранения проекта необходимо перейти в пункт меню «**File**» (1) - «**Save as...**» (2). В диалоговом окне ввести имя, выбрать тип файла, директорию для сохранения.



Для сохранения изображения перейдите в пункт меню «**File**» - «**Save picture...**». Укажите имя файла (1), выберите один из доступных форматов: **PNG**, **BMP**, **EPS** и **SVG** (2), нажмите «**Save**» (3).



Kalzium - периодическая система химических элементов

Установка

Описание программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** kalzium-19.12.1-2

Kalzium — удобное графическое приложение для работы с *Периодической системой химических элементов*.

Периодическая система химических элементов имени Дмитрия Ивановича Менделеева (периодическая система, таблица Менделеева) — классификация химических элементов, устанавливающая зависимость различных свойств элементов от заряда атомного ядра. Система является графическим выражением периодического закона, открытого в 1869 году русским учёным энциклопедистом Дмитрием Ивановичем Менделеевым.

Kalzium прост в использовании, ориентирован на учащихся любого возраста в качестве маленькой и быстрой базы данных. Приложение можно использовать для изучения сведений о периодической системе.

Вы можете подробнее ознакомиться с возможностями работы программы **Kalzium**, просмотрев наши обучающие видео:

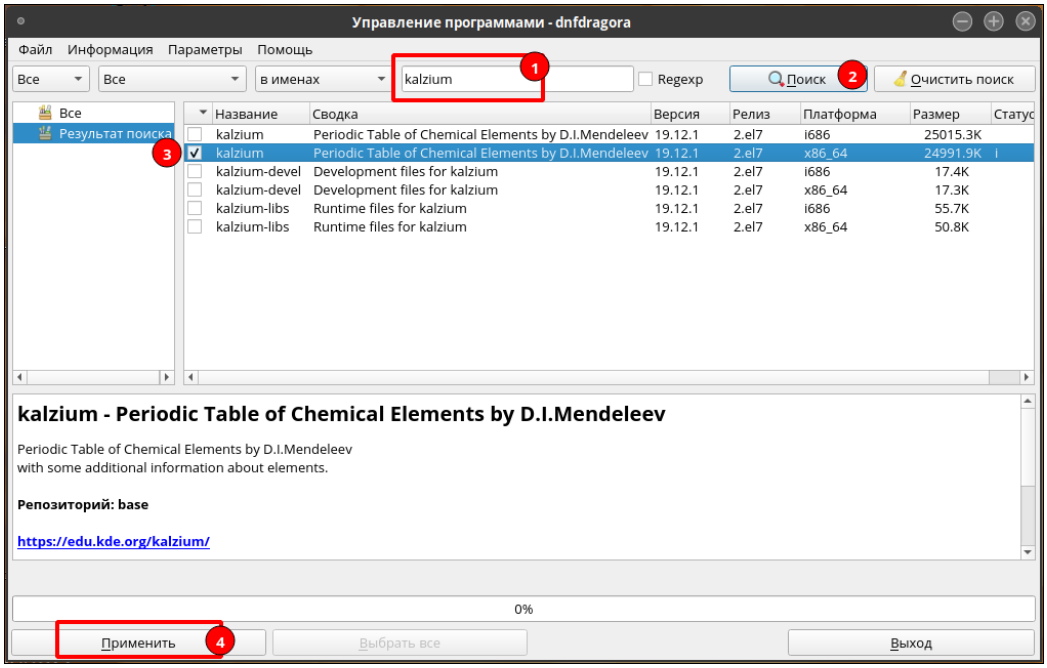
- на **RuTube** — Kalzium. Периодическая система химических элементов;
- в **Яндекс.Дзен** — Kalzium. Периодическая система химических элементов;
- в **VK Видео** — Kalzium. Периодическая система химических элементов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kalzium**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install kalzium
```

Выйдите из сеанса пользователя **root**:

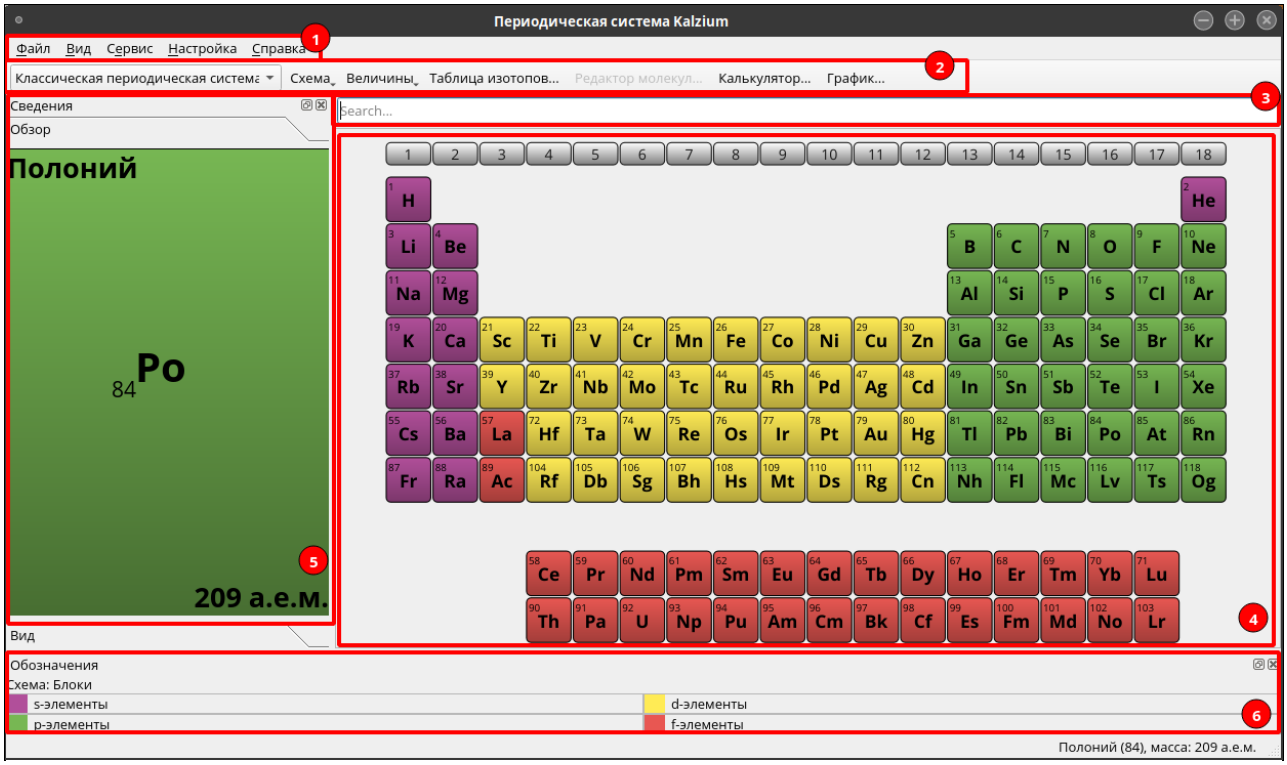
```
exit
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**Периодическая система Kalzium**».

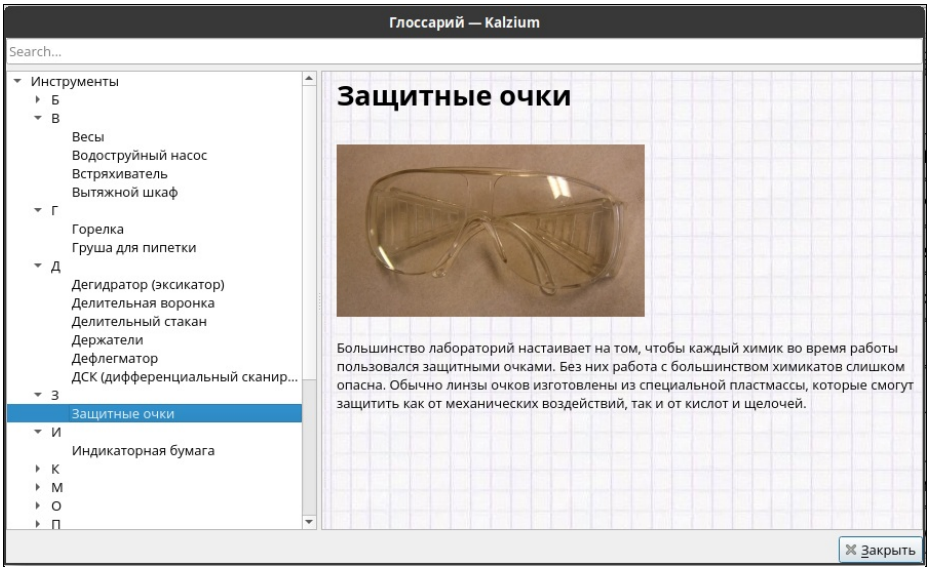
Описание программы

Интерфейс программы довольно прост и разделён на несколько типовых элементов.

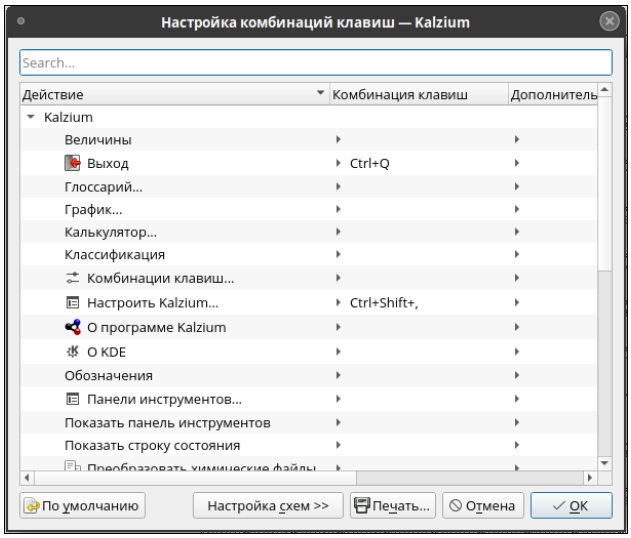


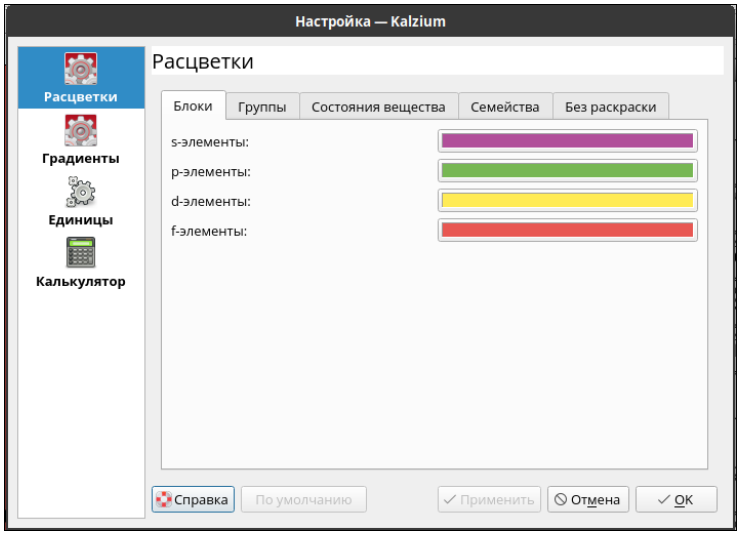
1. *Основное меню* – здесь доступны основные возможности программы.

Одним из наиболее интересных пунктов является «**Сервис**» - «**Глоссарий**», в котором собраны пояснения для большинства химических терминов, а также названия инструментов и краткое описание к ним.

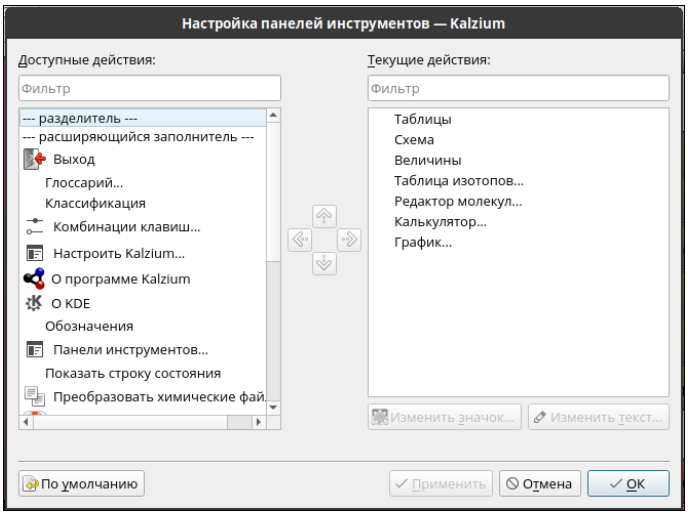


В пункте меню «**Настройка**» доступно изменение внешнего вида программы, языка интерфейса, а также просмотр и настройка используемых горячих клавиш.





2. *Панель инструментов* – нужна для быстрого доступа к основным возможностям программы. Кнопки этой панели можно настраивать через пункт меню «**Настройка**» — «**Панели инструментов**».

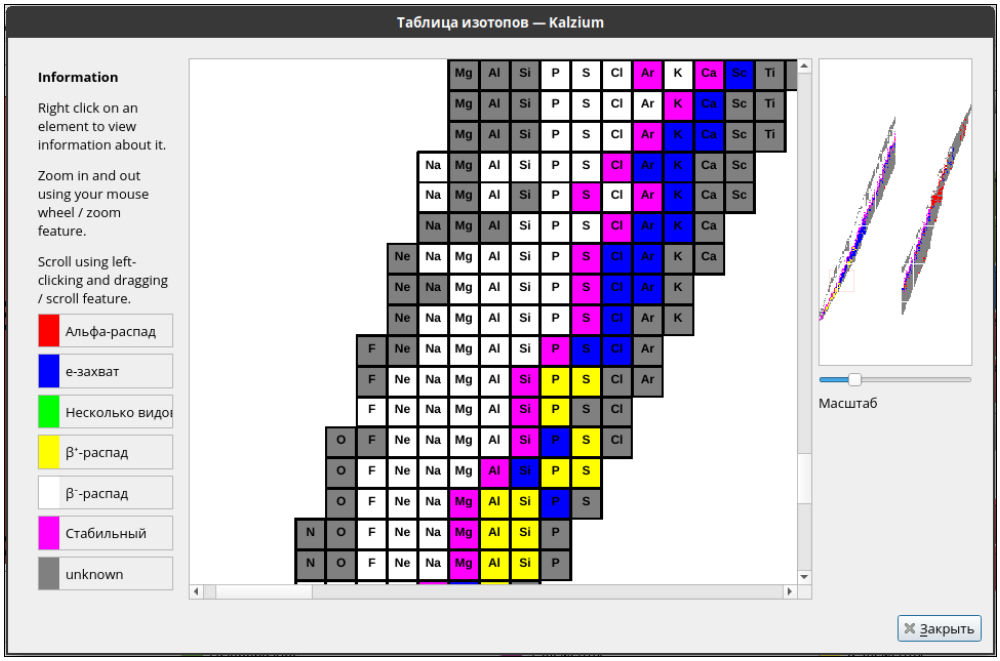


В панели инструментов также имеются некоторые дополнительные инструменты, такие как:

- *Таблица изотопов*;
- *Калькулятор*;
- *График*.

Таблица изотопов

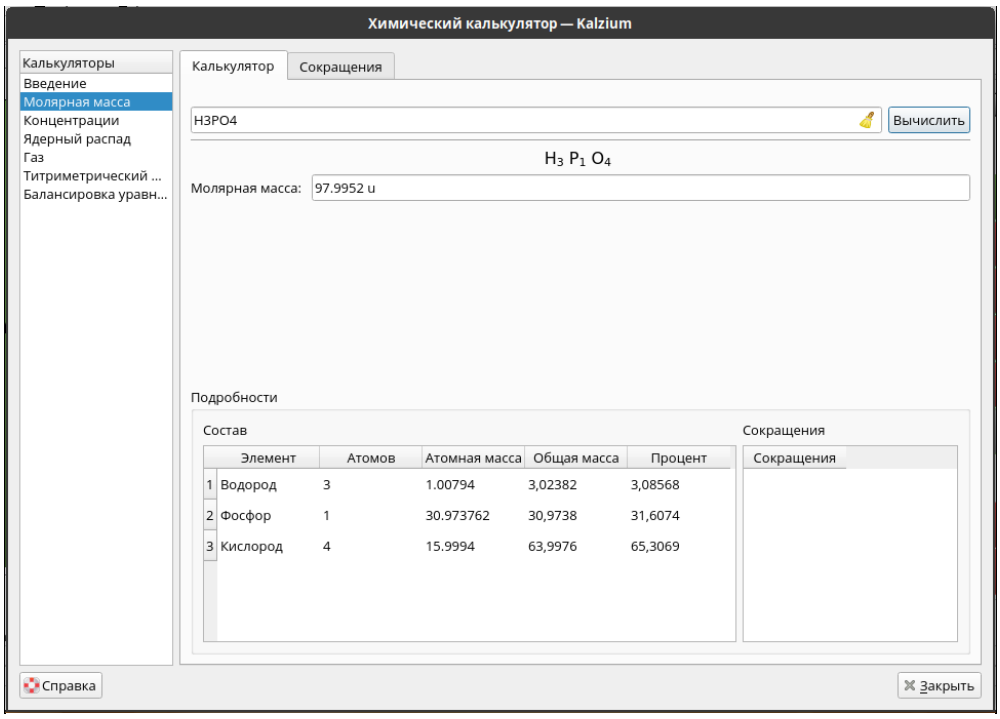
В таблице отображается информация об изотопах всех химических элементов.



Калькулятор

Химический калькулятор для расчёта значений различных свойств:

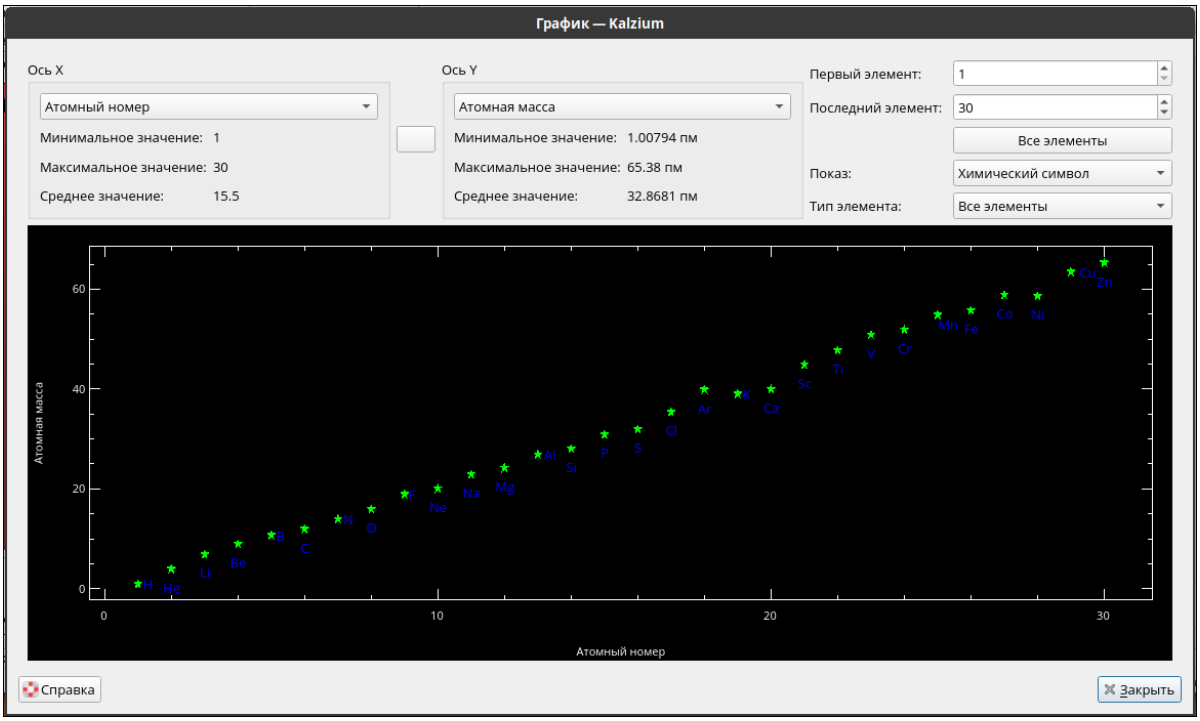
- молярной массы молекул;
- концентраций;
- титриметрического анализа;
- ядерных распадов;
- газов;
- балансировки химических уравнений.



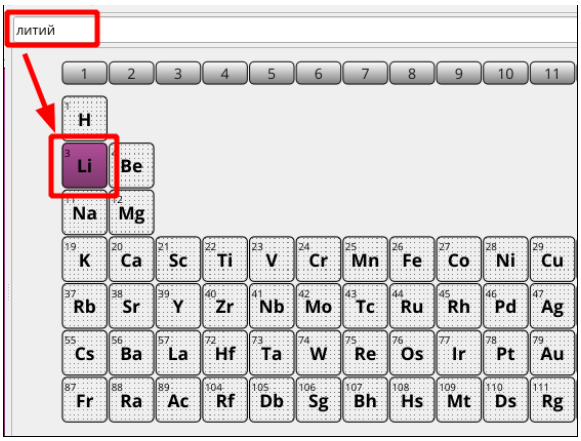
График

Kalzium позволяет построить график диапазона элементов по различным свойствам (температура кипения, атомная масса и др.). Такие

графики можно использовать, например, при наглядном отображении *закона Мозли*.



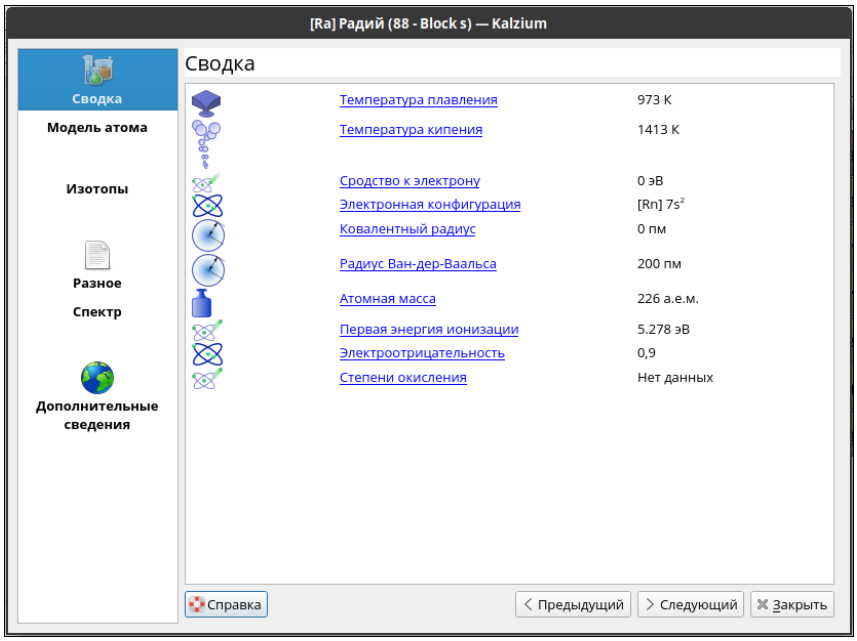
3. *Панель быстрого поиска элементов*. При поиске цветом выделяется только искомый элемент, остальные элементы становятся прозрачными.



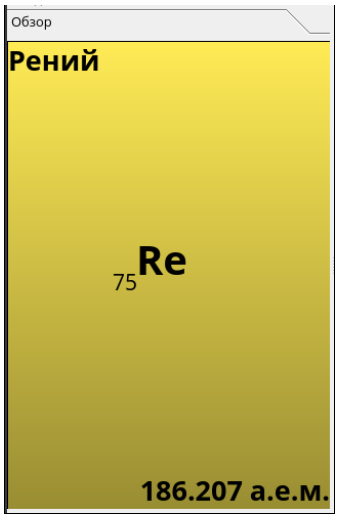
4. *Таблица элементов*. Внешний вид таблицы можно изменять через основное меню программы или через кнопки на панели инструментов (**2**).

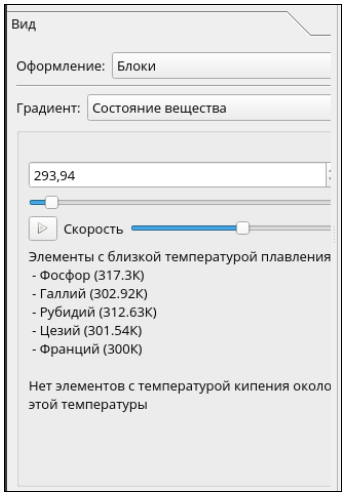
Kalzium может отображать периодическую таблицу различными способами (группами, блоками и семействами) и изменять её вид на короткую или длинную, можно также использовать различные схемы классификации, показывать элементы, сгруппированные по ряду свойств, например, кристаллической структуре и т.д.

В таблице отображаются краткое название химического элемента и его атомный номер. Для получения дополнительной информации о конкретном элементе нужно выбрать его в таблице. В открывшемся окне будет предоставлена расширенная информация о выбранном элементе: температура плавления, температура кипения, конфигурация электронных оболочек, электроотрицательность, ссылка на статью об элементе, краткая история открытия элемента, список его изотопов и модель атома.

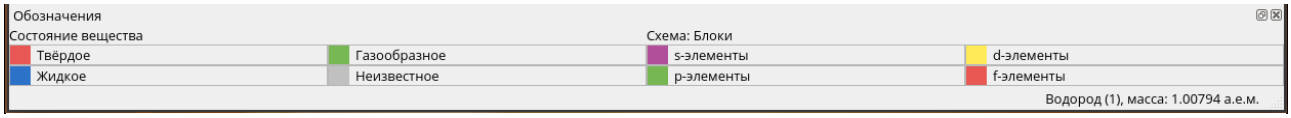


5. *Панель отображения дополнительной информации о выбранном элементе*. Тут можно показать либо обзор элемента, либо настройку общего вида таблицы.





6. *Панель легенды* с пояснениями цветовых обозначений элементов.



Kalzium может быть успешно использован как на уроках, так и при самостоятельном изучении химии.

Avogadro - программа просмотра и редактирования молекул

Установка
Описание программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** avogadro-1.2.0-1

Avogadro — редактор и визуализатор молекул, предназначенный для кроссплатформенного использования в вычислительной химии, молекулярном моделировании, биоинформатике, материаловедении и смежных областях. Функционал программы можно расширить с помощью плагинов.

С помощью **Avogadro** можно легко построить или изменить структуру молекулы, при этом программа обеспечивает отличное качество отображения молекул и белковых структур. Приложением поддерживается просмотр и редактирование трёхмерных структур большинства наиболее популярных в вычислительной химии форматов (таких как ***.cml**, ***.cif**, ***.mol**, ***.sd**, ***.sdf**, ***.pdb**, ***.ent**, ***.vis**, ***.xyz** и пр).

Вы можете подробнее ознакомиться с работой программы **avogadro**, просмотрев наши обучающие видео:

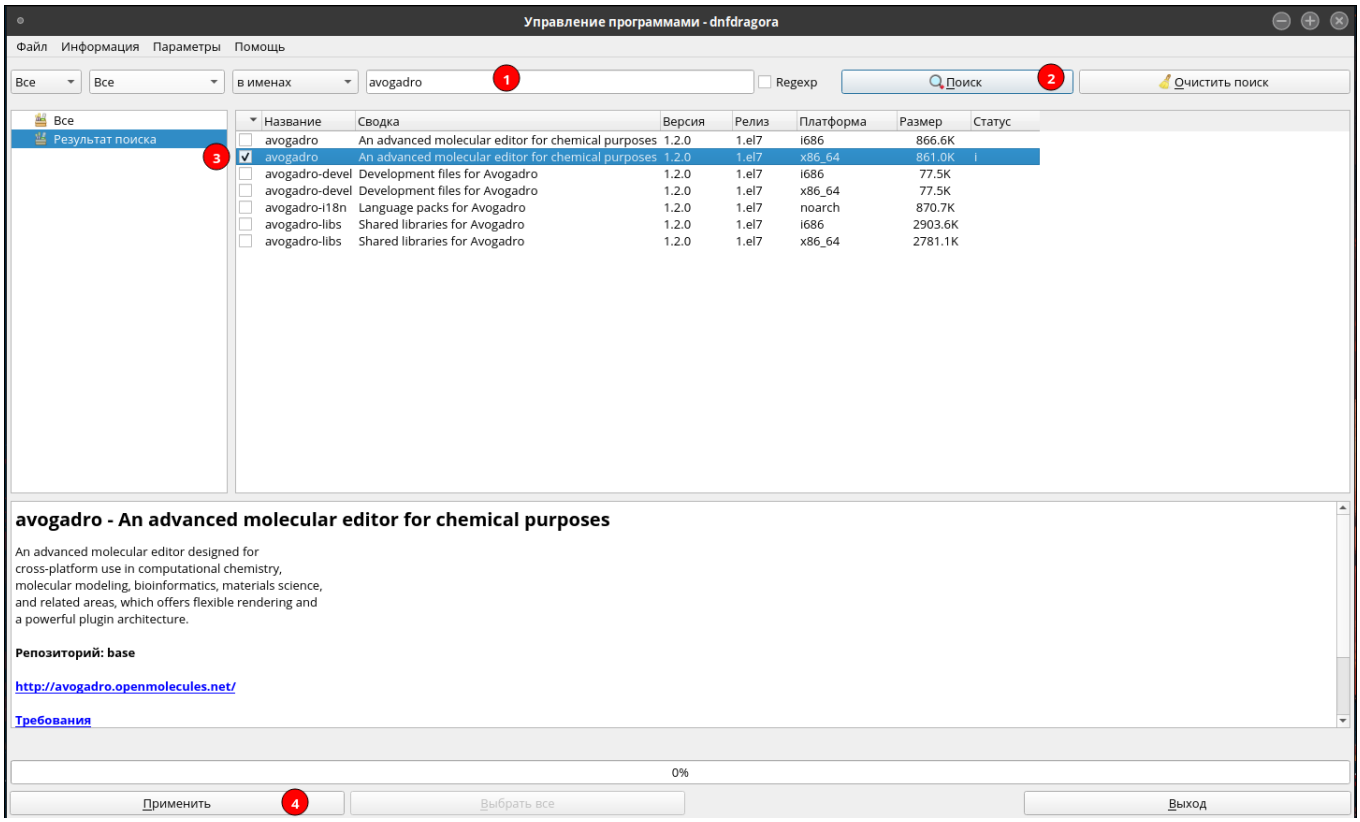
- на **RuTube** — Avogadro. Программа 3D моделирования молекул;
- в **Яндекс.Дзен** — Avogadro. Программа 3D моделирования молекул;
- в **VK Видео** — Avogadro. Программа 3D моделирования молекул.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**avogadro**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

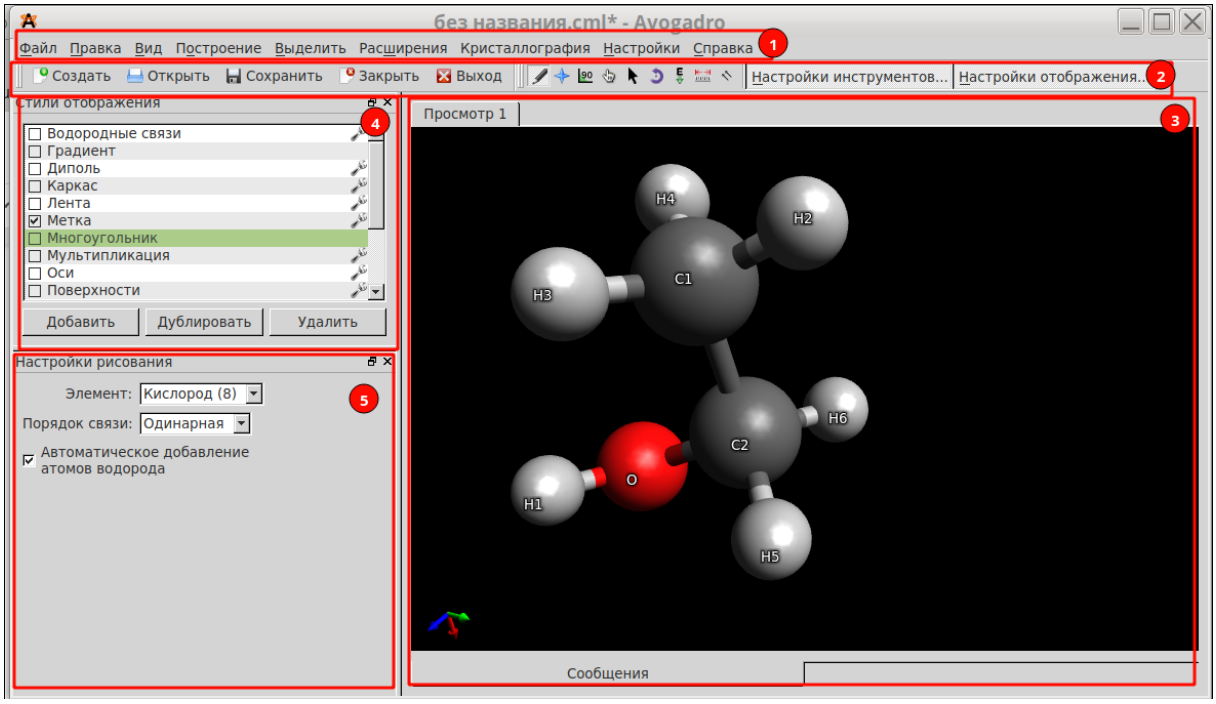
```
sudo dnf install avogadro
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**Моделирование молекул Avogadro**».

Описание программы

Интерфейс программы стандартный и состоит из нескольких типовых частей.



1. **Основное меню** программы. Позволяет выполнять различные действия с создаваемым документом, а также настраивать как саму программу, так и панель инструментов.

2. **Панель инструментов**. Это стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы. Эти панели можно скрывать и отображать через основное меню. По умолчанию отображается **Главная панель** и **Инструменты**.

В меню настройки доступно много панелей, но они нужны при более глубоком изучении приложения.

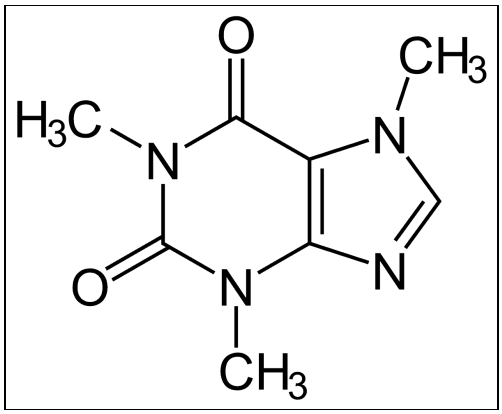
3. **Основное рабочее поле**. В данном поле происходит весь процесс рисования и анимации моделей молекул.

4. **Меню стиля отображения модели**. Эта панель инструментов позволяет менять способ отображения молекулы.

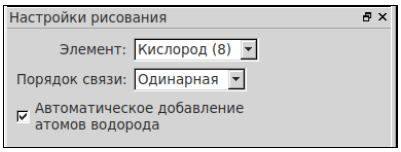
5 . **Меню рисования**. Здесь отображаются опции и действия, которые относятся к выбранному в данный момент инструменту. Инструменты можно выбирать через панель инструментов.

Пример работы

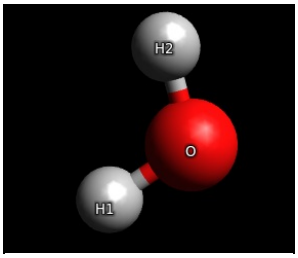
Рассмотрим создание молекулы на примере молекулы кофеина, которая имеет формулу $\mathbf{C_8H_{10}N_4O_2}$ и имеет структуру следующего вида:



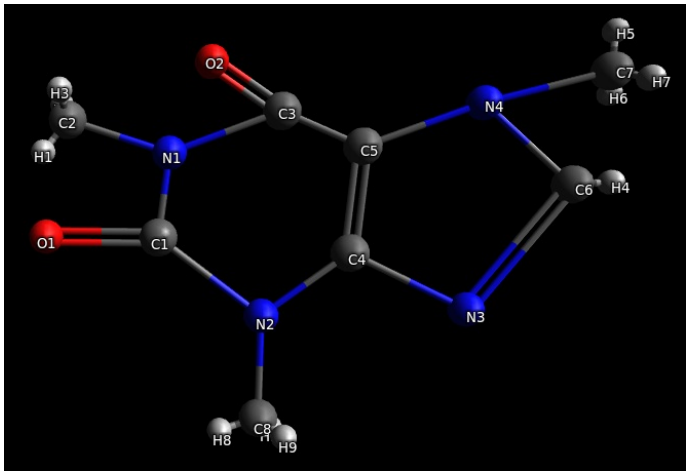
Сначала выберите атом кислорода и оставьте одинарную связь. Связи в процессе можно добавлять.



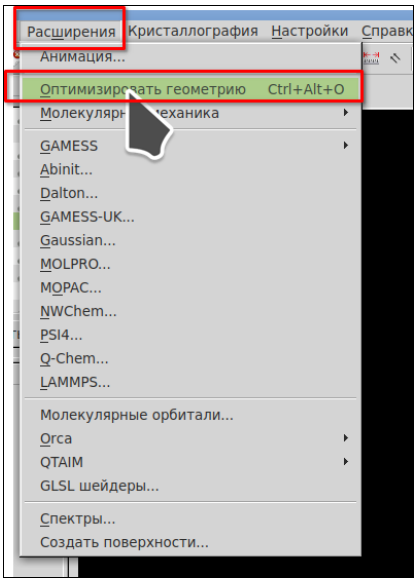
Выставьте атом на поле. В соответствии с настройками по умолчанию выстраивается молекула воды (**H_2O**).



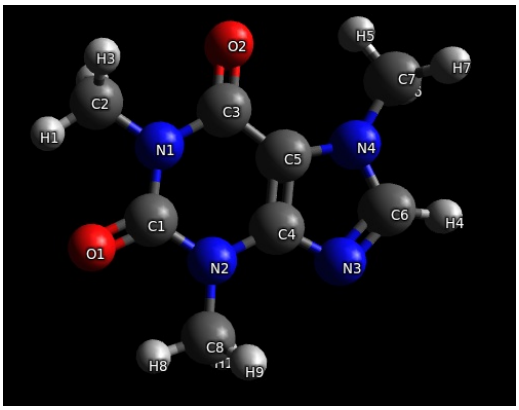
Добавьте по очереди остальные атомы. В результате получается молекула такого вида:



Необходимо оптимизировать длины и углы связей. Для этого выбираем соответствующий пункт «**Расширения**» - «**Оптимизировать геометрию**» в основном меню.

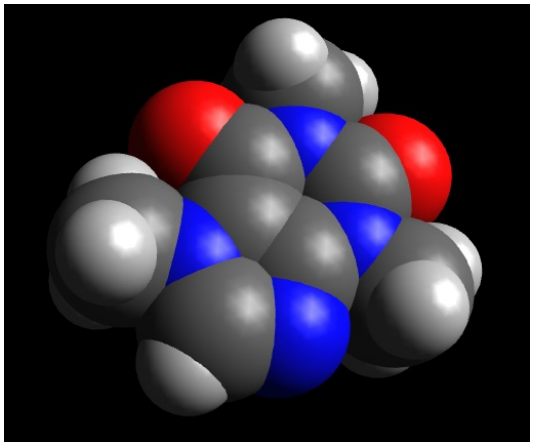


После молекула выглядит правильно, поскольку расстояние между атомами и углы между связями установлены в соответствии со справочными данными.

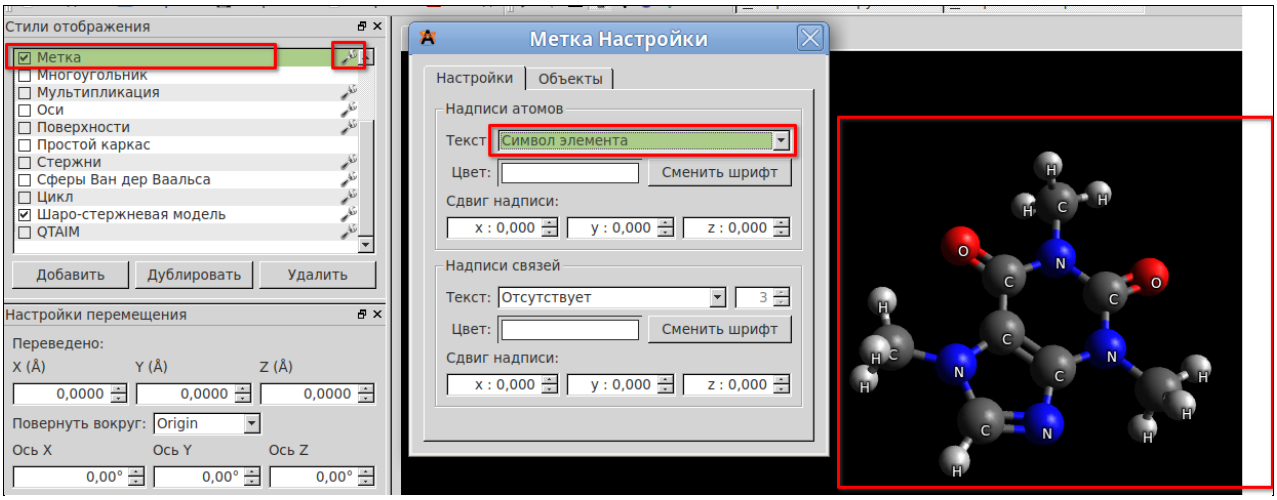


В **Настройках перемещения** можно рассмотреть молекулу со всех сторон.

Используя **Стили отображения**, также существует возможность, например, отобразить *сферы Ван-дер-Ваальса*.



Каждый стиль можно настроить, для этого существуют кнопки настроек. Например, в **настройках меток** можно добавить в созданную молекулу подписи использующихся химических элементов.



На этом создание молекулы завершено.

InChI — химический идентификатор на основе молекулярной структуры

Установка
Синтаксис
Опции
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: inchi-1.0.6

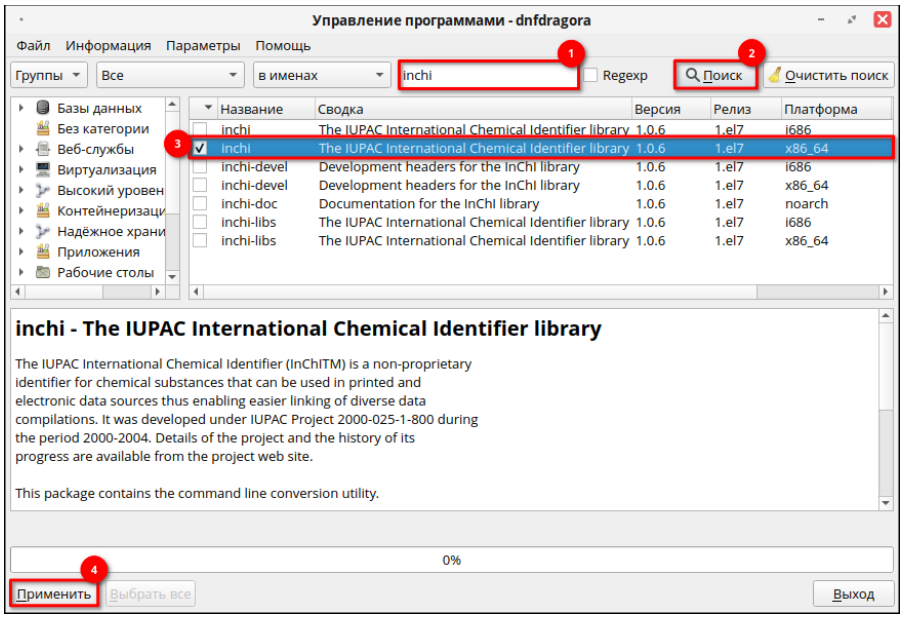
InChI — международный текстовый химический идентификатор. Предназначен для однозначного обозначения молекул. Он обеспечивает универсальный метод для облегчения поиска молекулярной информации в различных базах данных и в Интернете.

InChI и его компактная форма, **InChIKey**, являются открытыми стандартами, не ограниченными патентами. Эти идентификаторы преобразуют химические структуры в строки, которые могут быть использованы для описания, систематизации и поиска химических соединений.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**inchi**» и отметьте флагом пакет последней версии. Далее нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install inchi
```

Данный пакет предоставляет утилиту для командной строки **inchi-1**. Утилита применяется для пакетной обработки нескольких структурированных файлов, в первую очередь файлов SDF. Список опций утилиты можно вывести, запустив её без аргументов:

```
inchi-1
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
inchi-1 inputFile [outputFile [logFile [problemFile]]] [-option[ -option ...]]
```

где:

- **inchi-1** — название утилиты;
- **inputFile** — путь к входному файлу с химическими структурами, который нужно конвертировать;
- **outputFile** (необязательно) — путь к файлу, куда будет сохранён результат конвертации;
- **logFile** (необязательно) — путь к файлу логов, где будут записаны сообщения о ходе выполнения;
- **problemFile** (необязательно) — путь к файлу, куда будут записаны проблемные случаи;
- **[-option[-option ...]]** — одна или несколько опций, модифицирующих процесс конвертации.

```
inchi-1 inputFiles... -AMI [-option[ -option...]]
```

где:

- **inputFiles...** — список входных файлов для обработки;
- **-AMI** — опция, указывающая на использование дополнительного режима или модуля;
- **[-option[-option...]]** — дополнительные опции, настраивающие процесс.

Опции

Основные опции утилиты:

1. Опции ввода.

- **STDIO** — использовать стандартные потоки ввода/вывода;
- **InpAux** — ввод структур в формате дополнительной информации inchi;
- **SDF:DataHeader** — читать из входного SD-файла идентификатор под этим заголовком данных;
- **START:n** — начать с n-й входной структуры;
- **END:n** — остановиться после n-й входной структуры;
- **RECORD:n** — обработать только n-ю входную структуру;
- **AMI** — разрешить множественные входные файлы (поддержка шаблонов);
- **AMIOutStd** — записывать вывод в стандартный поток вывода (в режиме AMI);
- **AMILogStd** — записывать логи в стандартный поток ошибок (в режиме AMI);
- **AMIPrbNone** — подавить создание файлов с проблемами (в режиме AMI).

2. Опции вывода.

- **NoLabels** — не включать номер структуры, DataHeader и ID в вывод inchi;
- **NoWarnings** — подавить все предупреждающие сообщения;
- **AuxNone** — не включать дополнительную информацию;
- **SaveOpt** — сохранить пользовательские опции создания inchi (нестандартный inchi);
- **Tabbed** — разделить номер структуры, inchi и AuxInfo с помощью табуляции;
- **MergeHash** — объединить inchikey с дополнительными хешами, если они присутствуют;
- **NoInChI** — не печатать саму строку inchi;
- **OutErrInChI** — при ошибке печатать пустую строку inchi (по умолчанию ничего);
- **OutputSDF** — преобразовать inchi, созданный с дополнительной информацией по умолчанию, в SD-файл;
- **SdfAtomsDT** — выводить изотопы водорода в SD-файле как атомы D и T.

3. Опции структуры.

- **SNon** — исключить стереохимию (по умолчанию включить абсолютные стереохимические свойства);
- **NEWPSOFF** — оба конца клина указывают на стереоцентры;
- **LooseTSACheck** — ослабить критерии неоднозначного рисунка для тетраэдрической стереохимии в кольце;
- **DoNotAddH** — все атомы водорода являются явными (по умолчанию добавлять H в соответствии с обычными валентностями).

4. Модификаторы восприятия стереохимических свойств (нестандартный inchi).

- **SRel** — относительная стереохимия;
- **SRac** — рацемическая стереохимия;
- **SUCF** — использовать флаг хиральности: включено означает абсолютную стереохимию, выключено — относительную стереохимию.

5. Опции настройки создания inchi (нестандартный inchi).

- **SUU** — всегда включать опущенные неизвестные/неопределённые стереохимические свойства;
- **SLUUD** — делать метки для неизвестных и неопределённых стереохимических свойств различными;
- **RecMet** — включать результаты с реконнектированными металлами;
- **FixedH** — включать слой фиксированного водорода;
- **KET** — учитывать кето-енольный таутомеризм (экспериментально);
- **15T** — учитывать 1,5-таутомеризм (экспериментально).

6. Опции генерации.

- **Wnumber** — установить тайм-аут на структуру в секундах (W0 означает неограниченно);
- **WMnumber** — установить тайм-аут на структуру в миллисекундах (WM0 означает неограниченно);
- **LargeMolecules** — обрабатывать молекулы до 32766 атомов (экспериментально);
- **WarnOnEmptyStructure** — предупреждать и производить пустой inchi для пустой структуры;
- **Polymers** — разрешить обработку полимеров (экспериментально);
- **Polymers105** — разрешить обработку полимеров (экспериментально, устаревший режим версии 1.05);
- **FoldCRU** — складывать CRU-полимера, если внутри повторяются;
- **NoFrameShift** — отключить сдвиг рамки CRU-полимера;
- **NoEdits** — отключить сдвиг рамки и складывание CRU-полимера;
- **NPZz** — разрешить Zz-атомы, не связанные с полимерами (псевдоэлементы-заполнители);
- **SAtZz** — разрешить стереохимию у атомов, связанных с Zz (по умолчанию отключено);
- **Key** — генерировать inchikey;
- **XHash1** — генерировать расширение хеша (до 256 бит) для первого блока inchikey;
- **XHash2** — генерировать расширение хеша (до 256 бит) для второго блока inchikey.

7. Опции преобразования.

- **InChI2Struct** — преобразовать строку inchi обратно в структуру молекулы, восстановить исходную структуру молекулы из ее уникального идентификатора **inchi**;
- **InChI2InChI** — преобразовать строку inchi в другую строку inchi с использованием разных опций или стандартов, необходимо для сравнения и анализа различных представлений одной и той же молекулы.

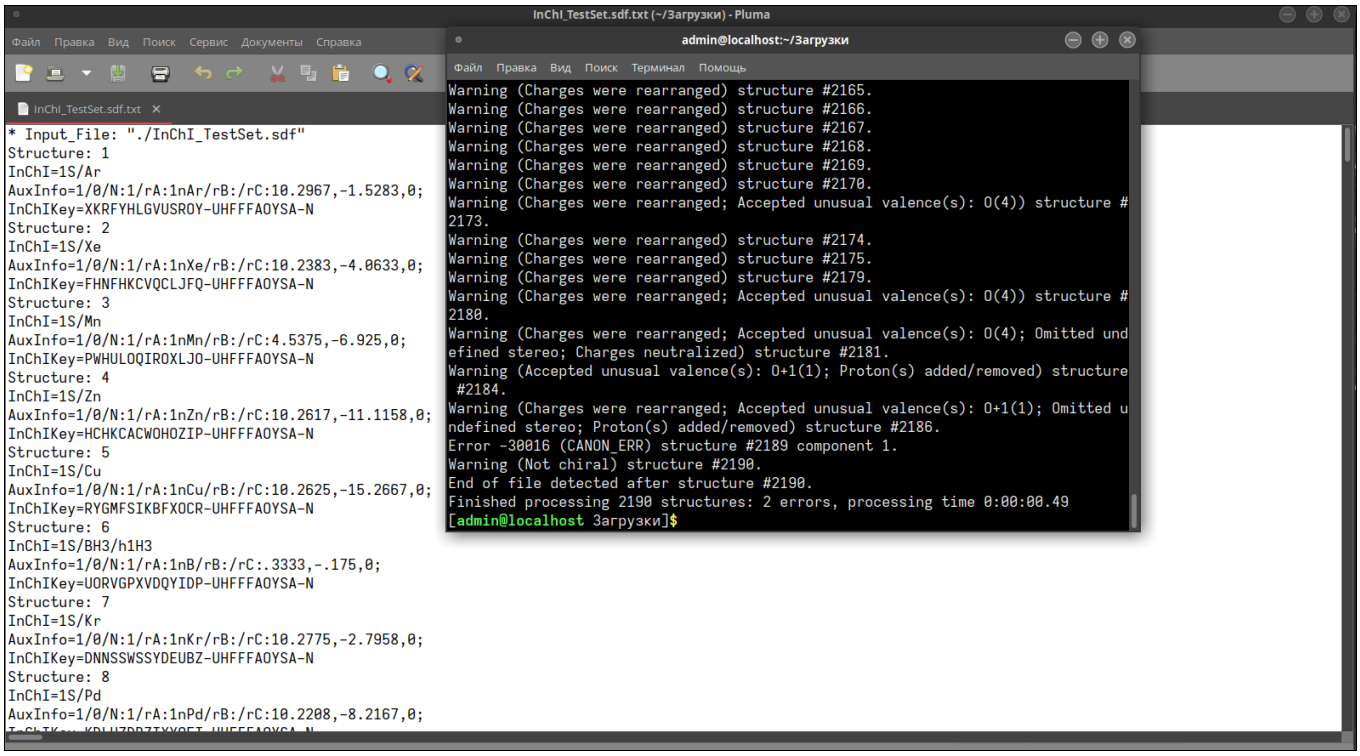
Примеры использования

Перед выполнением данных примеров создайте файл **InChI_TestSet.sdf**, содержащий необходимые химические структуры для преобразования.

> **Примечание.**
>
> Для создания и редактирования sdf-файлов можно использовать молекулярные редакторы, например:
>
> Avogadro - программа просмотра и редактирования молекул.
>
> XDrawChem – программа для рисования и анализа химических структур и реакций .

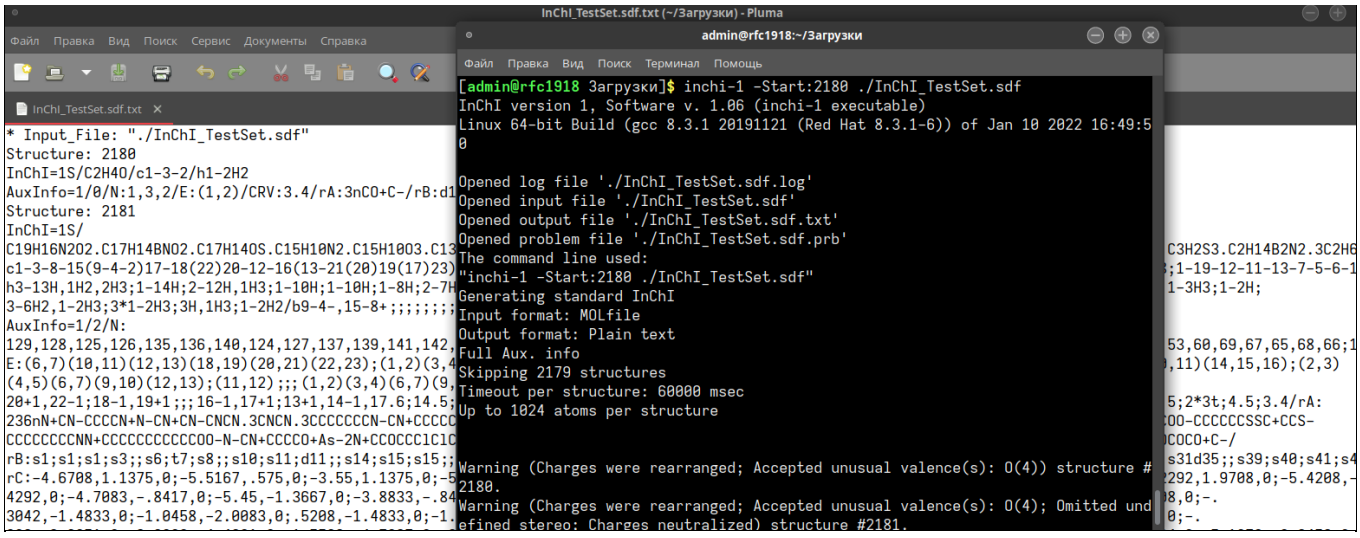
1. Преобразование sdf-файла в txt-файл со строками inchi и inchikey с использованием опции **-Key**:

```
inchi-1 -Key ./InChI_TestSet.sdf
```



2. Опции **-Start:n**, **-End:n**, **Record:n** позволяют обрабатывать структуры в файле, начиная с определённой структуры, либо заканчивая или обрабатывая только её.

```
inchi-1 -Start:2180 ./InChI_TestSet.sdf
```



OpenMolcas — программа для квантовой химии

Установка
Синтаксис
Опции
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: OpenMolcas-21.10-2

OpenMolcas — это утилита для квантовой химии, которая используется для моделирования и анализа молекулярных систем. Она предназначена для выполнения расчетов в различных областях теоретической и вычислительной химии, включая молекулярную структуру, термодинамику, спектроскопию и фотохимические процессы. Ее ключевой особенностью является мультиконфигурационный подход с использованием таких методов, как **CASSCF** (*Complete Active Space Self-Consistent Field* — метод полного самосогласованного поля активного пространства) и **CASPT2** (*Complete Active Space Perturbation Theory to second order* — полная теория возмущений активного пространства второго порядка).

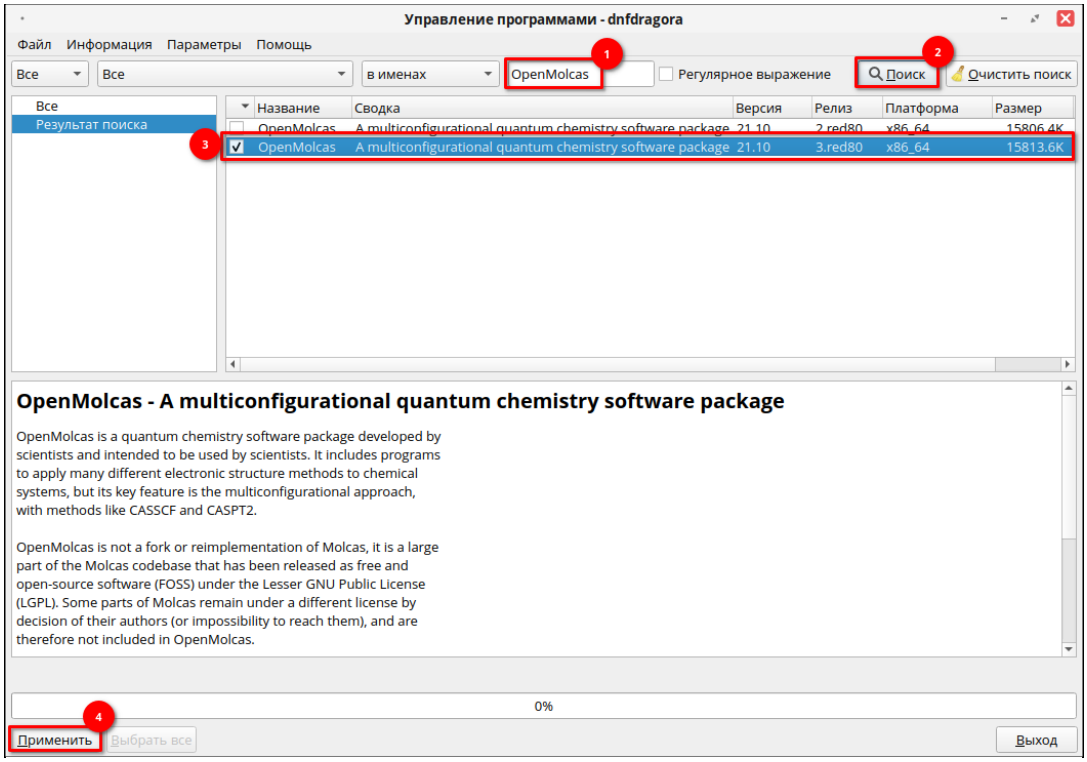
OpenMolcas предоставляет широкий спектр функций для проведения квантово-химических расчётов:

- **расчёт электронной структуры молекул** — позволяет рассчитывать электронную структуру молекул с использованием различных методов, таких как метод Хартри-Фока, метод функционала плотности и другие;
- **расчёт свойств молекул** — позволяет рассчитывать различные свойства молекул, такие как энергии, дипольные моменты, магнитные моменты и другие;
- **оптимизация геометрии молекул** — позволяет оптимизировать геометрию молекул с целью достижения минимума энергии;
- **изучение реакционной способности молекул** — позволяет изучать реакционную способность молекул с использованием методов теории возмущений.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**OpenMolcas**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install OpenMolcas
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
pymolcas [<опции>] [<входной_файл> | <сценарий>]
```

Опции

Основные опции утилиты:

- **<входной_файл> | <сценарий>** — входной файл сценария или сценарий;
- **-h, --help** — показать справку;
- **-s, --setup** — настроить molcas;
- **-env, --environment** — отобразить информацию о расположении molcas;
- **-clean, --clean_scratch** — очистить рабочую область после расчета;
- **-new, --new_scratch** — очистить рабочую область перед расчетом;
- **-old, --old_scratch** — повторно использовать рабочую область;
- **-ign, --ignore_environment** — запустить, игнорируя файлы ресурсов;
- **-val, --validate** — проверить только ввод;
- **-np [<количество_процессов>], --nprocs [<количество_процессов>]** — указать количество параллельных (MPI) процессов;
- **-v, --version** — вывести версию;
- **-o [<файл>], --output [<файл>]** — перенаправить выходной поток в указанный файл;
- **-e [<файл>], --error [<файл>]** — перенаправить поток ошибок в указанный файл;
- **-oe [<файл>], -eo [<файл>], --outputerror [<файл>]** — перенаправить потоки вывода и ошибок в указанный файл;
- **-f, --files** — перенаправить потоки вывода/ошибок в стандартные файлы (***.log** и ***.err**);
- **-b [<размер_буффера>], --buffer [<размер_буффера>]** — указать размер буфера для файлов ввода/ошибок;
- **--banner** — вывод информативного баннера;
- **--not-here** — не пытаться найти molcas в текущем каталоге (и родительских).

Пример работы

Для примера будет выполнен полный расчёт поля реакции с использованием модели Кирквуда. **SCF** будет вычислять поле реакции, в то время как **MRCI** — добавлять эффект в виде постоянного возмущения.

Для этого будет создан файл **example.input** с настройками для вычисления квантовой химии:

```
nano example.input
```

```
&GATEWAY
 Title = HF molecule
 Symmetry
 X Y
 Basis set
 F.ANO-S...3S2P.
 F 0.00000 0.00000 1.73300
 End of basis
 Basis set
 H.ANO-S...2S.
 H 0.00000 0.00000 0.00000
 End of basis
 Well integrals
 4
 1.0 5.0 6.75
 1.0 3.5 7.75
 1.0 2.0 9.75
 1.0 1.4 11.75
```

```
RF-Input
Reaction field
80.0 4.75 4
End of RF-Input

&SEWARD

&SCF
Occupied = 3 1 1 0

&MOTRA
LumOrb
Frozen = 1 0 0 0
RFPert

&GUGA
Electrons = 8
Spin = 1
Inactive = 2 1 1 0
Active = 0 0 0 0
CiAll = 1

&MRCI
SDCI
```

где:

1. **&GATEWAY** — блок используется для задания различных параметров и опций, которые определяют расчет базисного набора, тип расчета и настройки реакционного поля. *Параметры:*

- **Title = HF molecule** — заголовок расчёта указывает на то, что рассматривается молекула фтороводорода (**HF**);
- **Basis set** — определение базисного набора для каждого типа атома в молекуле, для водорода используется набор **ANOS-S...2S**, а для фтора — **ANOS-S...3S2P**;
- **Well integrals** — настройки для вычисления интегралов, связанные с потенциальной энергией и волновыми функциями в пространственной области;
- **RF-Input** — используется для определения различных параметров реакционного поля (**RF**), которые могут быть использованы в расчетах.

2. **&SCF** — настройка для **SCF-метода** (**Self-Consistent Field**). *Настройка включает:*

- **Occupied = 3 1 1 0** — определение занятых орбиталей, где 3 означает три занятые орбитали в первом представлении, 1 — одну занятую орбиталь во втором и третьем представлениях, и 0 указывает на отсутствие занятых орбиталей в четвертом представлении.

3. **&MOTRA** — настройки для многоконфигурационных методов. *Параметры:*

- **LumOrb** — учет люминесцентных свойств молекулярных орбиталей;
- **Frozen = 1 0 0 0** — включение только первого порядка теории возмущений для коррекции энергии и волновых функций, отключая все более высокие порядки возмущения;
- **RFPert** — учет эффектов спин-орбитального взаимодействия и других релятивистских эффектов.

4. **&GUGA** — настройки для **GVB-метода**. *Параметры:*

- **Electrons = 8** — общее количество электронов;
- **Spin = 1** — общее количество спиновых орбиталей;
- **Inactive = 2 1 1 0** — определение неактивных орбиталей;
- **Active = 0 0 0 0** — определение активных орбиталей;
- **CiAll = 1** — включение полного конфигурационного смешения (**Full Configuration Interaction**).

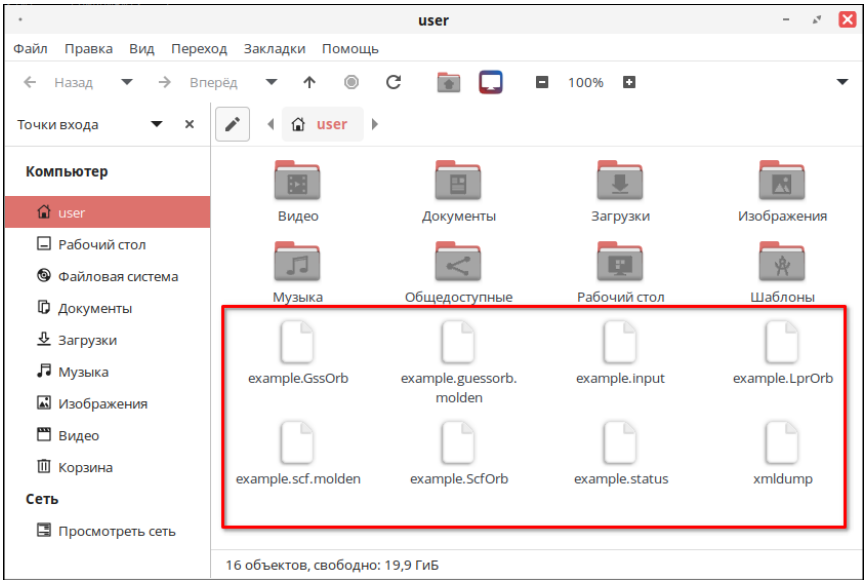
5. **&MRCI** — настройки для метода точного описания электронной структуры молекул с сильными корреляционными эффектами (**Multi-Reference Configuration Interaction**). *Настройка включает:*

- **SDCI** — расчёт с использованием **SDCI** (**Singles and Doubles Configuration Interaction**) метода в рамках блока настроек **&MRCI**.

Для запуска расчета используется команда:

```
pymolcas '/home/user/example.input'
```

Результаты работы можно посмотреть в каталоге **/home/user/**:



Более подробную информацию и расширенные возможности программы см. в официальном руководстве.

Работа со словарями

GoldenDict
StarDict
Translate-shell

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** stardict-3.0.6-1, goldendict-1.5-0.1, translate-shell-0.9.6.12-1

Словарями называют справочные издания, которые содержат упорядоченный перечень языковых единиц (слов, словосочетаний, фраз, терминов, знаков с краткими характеристиками или переводом на другой язык).

Вы можете подробнее ознакомиться с работой словарей и переводчиков в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Словари и переводчики в РЕД ОС;
- в **Яндекс.Дзен** — Словари и переводчики в РЕД ОС;
- в **VK Видео** — Словари и переводчики в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

GoldenDict

GoldenDict — оболочка для электронных словарей, поддерживающая форматы программ-словарей *ABBYY Lingvo*, *StarDict*, *Babylon*, *Dictd*.

Особенности:

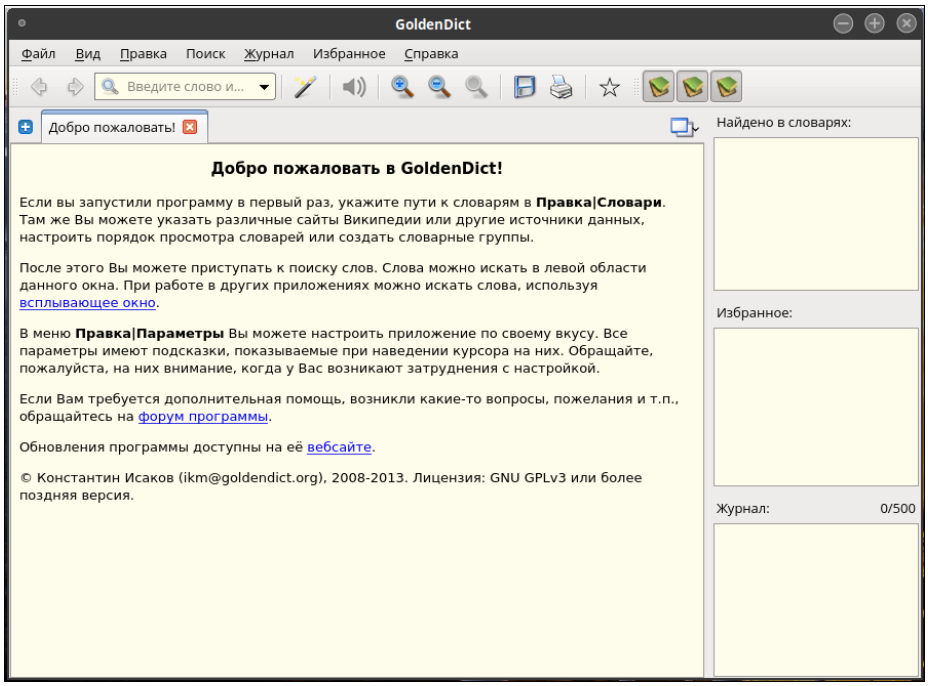
1. Вывод отформатированных статей со ссылками и картинками с помощью движка **WebKit**;
2. При поиске слов с ошибками используется система морфологии на основе свободной программы для проверки орфографии **Hunspell**;
3. Индексирование каталогов со звуковыми файлами для формирования словарей с произношением слов;
4. При поиске перевода пробелы, знаки пунктуации, диакритические знаки и регистр символов, содержащиеся в поисковой фразе, не учитываются;
5. После выделения текста появляется всплывающее окно, содержащее перевод выделенного текста;
6. Программа может показывать статьи с веб-сайтов, работающих на движке **MediaWiki** (таких как Википедия, Викисловарь и др.).

На сайте программы можно скачать русско-английский и англо-русский словари, а также словарь произношения английских слов.

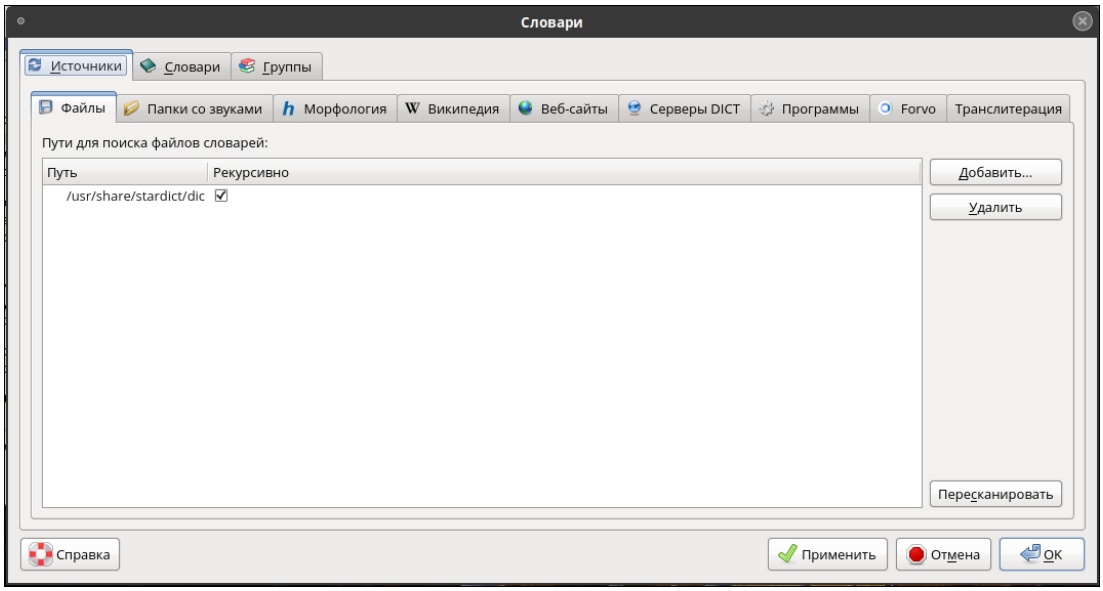
Режим всплывающего перевода

Вы можете получать перевод интересующего слова, не выходя из приложения, в котором работаете. Это осуществимо благодаря возможности программы работать в режиме *всплывающего перевода*. Чтобы посмотреть перевод интересующего слова, необходимо вызвать всплывающий перевод способом, установленным в настройках словаря. Другие способы вызова всплывающего перевода можно настроить в пункте меню «**Правка**» - «**Параметры**» - «**Всплывающее окно**».

GoldenDict по умолчанию установлен в РЕД ОС и находится в « **Главном меню**» - «**Офис**» - «**Мультиязычный словарь**».



Вы можете скачать любой словарь с официального сайта **GoldenDict**. Чтобы добавить новый словарь, распакуйте содержимое скачанного архива в **/usr/share/stardict/dic** либо укажите собственный каталог на вкладке «**Правка**» - «**Словари**» - «**Источники**». Нажмите «**Пересканировать**» и «**Применить**», все скачанные словари будут добавлены в **GodenDict**.



StarDict

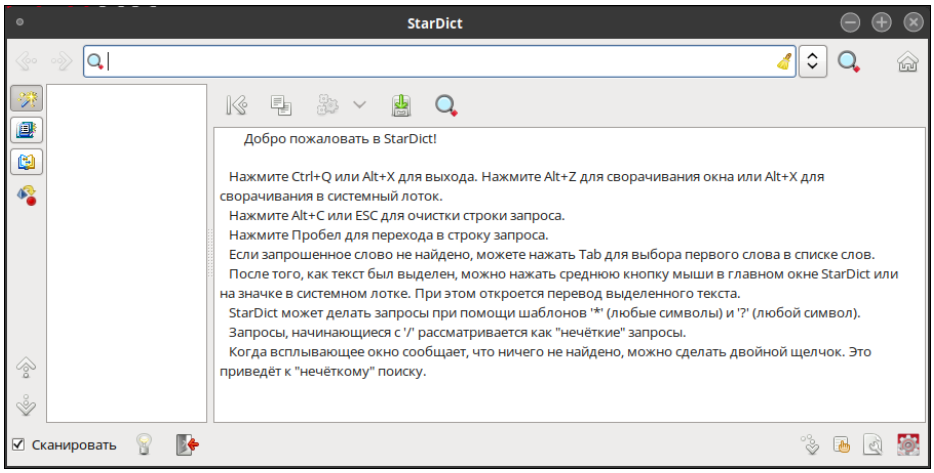
StarDict — свободная оболочка для электронных словарей с открытым исходным кодом, способная, кроме вывода статей, осуществлять перевод, озвучивать слова, использовать нечёткие запросы и шаблоны, поиск в онлайновых словарях.

Для установки **StarDict** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install stardict
```



После установки **StarDict** можно запустить из «**Главного меню**» - «**Офис**» - «**Словарь-переводчик StarDict**».

Translate-shell

Translate-shell - переводчик командной строки через **Google Translate** (по умолчанию), **Bing Translator**, **Яндекс.Переводчик** и **Apertium**. Данный инструмент позволяет получить доступ к одной из этих систем перевода прямо из терминала.

Для установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install translate-shell
```

Для перевода откройте терминал, напишите команду **trans** и необходимое для перевода слово. Данный инструмент может автоматически определять язык исходного текста. По умолчанию он переводит исходный текст на русский язык.

```
 trans dictionary

dictionary
/'dikSHə,nerē/толковый словарь
(tolkovyy slovarʹ)

dictionary – определения
[ English -> Русский ]

имя существительное
   словарь
      dictionary, vocabulary, glossary, lexicon, thesaurus, wordbook

dictionary
   толковый словарь, Словарь, словарик
```

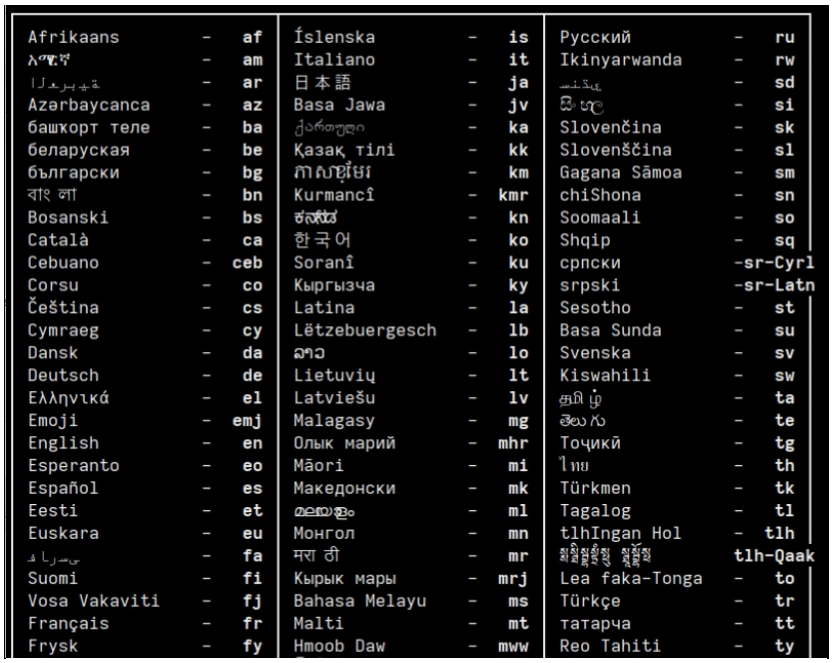
Чтобы перевести слово на другой язык надо явно указать идентификатор языка после команды **trans**, например:

```
 trans :de dictionary

dictionary
/'dikSHə,nerē/Wörterbuch

dictionary – определения
[ English -> Deutsch ]

имя существительное
   (das) Wörterbuch
      dictionary, lexicon, thesaurus
   (das) Lexikon
      lexicon, encyclopedia, dictionary, encyclopaedia
   (der) Diktionär
      dictionary
```

```
dictionary
   Wörterbuch, Lexikon
```

Для просмотра доступных языков добавьте опцию **-T** после **trans**:

```
trans -T
```



Afrikaans	-	af	Íslenska	-	is	Русский	-	ru
አማርኛ	-	am	Italiano	-	it	Ikinyarwanda	-	rw
العربية	-	ar	日本語	-	ja	سنڌي	-	sd
Azərbaycanca	-	az	Basa Jawa	-	jv	සිංහල	-	si
башкорт теле	-	ba	ქართული	-	ka	Slovenčina	-	sk
беларуская	-	be	Қазақ тілі	-	kk	Slovenščina	-	sl
български	-	bg	ភាសាខ្មែរ	-	km	Gagana Sāmoa	-	sm
বাংলা	-	bn	Kurmancî	-	kmr	chiShona	-	sn
Bosanski	-	bs	ಕನ್ನಡ	-	kn	Soomaali	-	so
Català	-	ca	한국어	-	ko	Shqip	-	sq
Cebuano	-	ceb	Soranî	-	ku	српски	-sr-Cyrl
Corsu	-	co	Кыргызча	-	ky	srpski	-sr-Latn
Čeština	-	cs	Latina	-	la	Sesotho	-	st
Cymraeg	-	cy	Lëtzebuergesch	-	lb	Basa Sunda	-	su
Dansk	-	da	ລາວ	-	lo	Svenska	-	sv
Deutsch	-	de	Lietuvių	-	lt	Kiswahili	-	sw
Ελληνικά	-	el	Latviešu	-	lv	தமிழ்	-	ta
Emoji	-	emj	Malagasy	-	mg	తెలుగు	-	te
English	-	en	Олык марий	-	mhr	Тоҷикӣ	-	tg
Esperanto	-	eo	Māori	-	mi	ไทย	-	th
Español	-	es	Македонски	-	mk	Türkmen	-	tk
Eesti	-	et	മലയാളം	-	ml	Tagalog	-	tl
Euskara	-	eu	Монгол	-	mn	tlhIngan Hol	-	tlh
فارسی	-	fa	मराठी	-	mr	𓀀𓁐𓂋𓏏 𓅱𓄿𓏏	tlh-Qaak
Suomi	-	fi	Кырык мары	-	mrj	Lea faka-Tonga	-	to
Vosa Vakaviti	-	fj	Bahasa Melayu	-	ms	Türkçe	-	tr
Français	-	fr	Malti	-	mt	татарча	-	tt
Frysk	-	fy	Hmoob Daw	-	mww	Reo Tahiti	-	ty

Для перевода слов на несколько языков, все необходимые языки указываются через «+», например:

```
 trans :de+fr dictionary

dictionary
/'dikSHə,nerē/Wörterbuchdictionary – определения
[ English -> Deutsch ]

имя существительное
   (das) Wörterbuch
      dictionary, lexicon, thesaurus
   (das) Lexikon
      lexicon, encyclopedia, dictionary, encyclopaedia
   (der) Diktionär
      dictionary

dictionary
   Wörterbuch, Lexikon

dictionary
/'dikSHə,nerē/dictionnaire

dictionary – определения
[ English -> Français ]

имя существительное
   (le) dictionnaire
      dictionary, thesaurus

dictionary
   dictionnaire
```

Для того чтобы перевести фразу, её необходимо прописывать в кавычках:

```
trans “Who ate my sandwich?”
```

Также есть возможность перевода файла. Команда в таком случае будет выглядеть следующим образом:

```
trans file:///home/user/text.txt
```

Чтобы определить язык введённого слова, требуется указать ключ **-identify**:

```
trans -identify dictionary

English
Name                English
Family              Indo-European
Writing system      Latin
Code                en
ISO 639-3           eng
SIL                 https://iso639-3.sil.org/code/eng
Glottolog           https://glottolog.org/resource/languoid/id/stan1293
Wikipedia           https://en.wikipedia.org/wiki/ISO_639:eng
```

Перевод слова или фразы также можно прослушать, указав ключ **-p**:

```
trans -p "Welcome to RED OS, we wish You productive work!"

Welcome to RED OS, we wish You productive work!

Добро пожаловать в РЕД ОС, желаем Вам плодотворной работы!
(Dobro pozhalovatʹ v RED OS, zhelayem Vam plodotvornoy raboty!)

Welcome to RED OS, we wish You productive work!: варианты перевода
[ English -> Русский ]

Welcome to RED OS, we wish You productive work!
    Добро пожаловать в РЕД ОС, желаем Вам плодотворной работы!, Добро пожаловать в РЕД ОС, желаем Вам продуктивной работы!
```

ПО для машинного перевода документов Promt Translation Server и PROMT Agent

Конфигурация веб-сервиса Nginx
Установка PROMT Agent

ВНИМАНИЕ!

Для установки утилиты необходимы дополнительные пакеты:

```
sudo dnf install coreutils tar gzip curl glibc libgcc libstdc++ libcurl libuuid zlib nginx mono-core mono-data fcgi
```

Promt Translation Server (PTS) — проприетарное программное обеспечение машинного перевода текста. Для использования **PTS** необходимо получить и активировать лицензию, отослав службе поддержки компании ПРОМТ идентификатор компьютера.

Для получения идентификатора, перейдите в каталог с **run-файлом** и выполните команду:

```
sh ptsu36.run +h
```

Создайте папки **ptsu_bin** и **ptsu_data** и распакуйте в них содержимое архивов:

```
sudo mkdir -p <путь_к_папке>/ptsu_bin
sudo mkdir -p <путь_к_папке>/ptsu_data
tar zxvf ptsu_bin.tar.gz -C <путь_к_папке>
tar zxvf ptsu_data.tar.gz -C <путь_к_папке>
```

После получения файла лицензии, его необходимо скопировать в корень папки с исполняемыми файлами:

```
cp <файл_лицензии> <путь_к_папке_ptsu_bin>
```

В файле настроек укажите путь до папки **ptsu_data** и до **FastCGI** сокета:

```
SocketPath=<путь_до_fcgisocket>
DataPath=<путь_до_папки_ptsu_data>
```

Конфигурация веб-сервиса Nginx

Перед конфигурацией **веб-сервиса** создайте две папки:

```
sudo mkdir /etc/nginx/sites-enabled /etc/nginx/sites-available
```

Следом создайте в папке **/etc/nginx/sites-available** конфигурационный файл виртуального хоста:

```
touch pts.conf
```

Заполните его следующем содержимом:

```
server {  listen 80;  server_name ptsu;  access_log /var/log/nginx/ptsu.access.log;  error_log /var/log/nginx/ptsu.error.log;  root /var/www/ptsu_bin/ui/;  rewrite ^/$ /pts redirect; client_max_body_size 1024m;  location /pts { root /var/www/ptsu_bin/ui/;  location /pts/service {  rewrite /pts/service/(.*) /pts/translator/$1 break;  proxy_pass http://127.0.0.1:9001;  proxy_connect_timeout 12000;  proxy_read_timeout 3600;  proxy_set_header Host $host;  }  location /pts/translator { fastcgi_pass unix:/home/test/fcgisocket;  fastcgi_connect_timeout 3600;  fastcgi_read_timeout 3600;  include fastcgi_params;  fastcgi_param HOST $host;  }}}
```

После чего создайте **символьную ссылку** на файл в каталог **/etc/nginx/sites-enabled**:

```
ln -s /etc/nginx/sites-available/pts.conf /etc/nginx/sites-enabled/pts.conf
```

Переместите каталог **ptsu_bin** в **/var/www/**

Сотрите все содержимое файла **/etc/nginx/nginx.conf** и вставьте туда следующее:

```
include /etc/nginx/modules-enabled.d/*.conf; include /etc/nginx/conf-enabled.d/*.conf; worker_processes 10; events { worker_connections 1024;  } http {  error_log /var/log/nginx/error.log warn;  access_log /var/log/nginx/access.log; include /etc/nginx/mime.types; include /etc/nginx/sites-enabled/*.conf; default_type application/octet-stream; sendfile on; gzip on; gzip_types text/plain text/css text/xml application/x-javascript application/atom+xml; }
```

Окончив конфигурацию веб-сервиса — запустите сервисы **PTS**, перейдя в папку **/var/www/ptsu_bin/bin64**:

```
./dcs -d
./transfcgid -d
./transfcgid -b -d
```

После запуска сервисов, веб-интерфейс будет доступен по адресу: http://localhost/pts

А сам веб-сервис: http://localhost/pts/service

Установка PROMT Agent

Для установки **PROMT Agent** распакуйте архив и запустите исполняемый файл командами:

```
tar -zxvf ptsu_agent.tar.gz
cd ptsu_agent
chmod +x PromtAgent.run
./PromtAgent.run
```

По умолчанию, **PROMT Agent** использует адрес подключения к серверу http://localhost/pts/service. Его можно изменить в настройках программы.

QGIS — геоинформационная система

Просмотр данных
Исследование данных и создание карт
Управление данными
Анализ данных
Публикация карт в сети Интернет
Внешние модули
Установка

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** qgis-3.18.1-10

Quantum GIS (**QGIS**)— свободная кроссплатформенная геоинформационная система, состоящая из настольной и серверной части:

- **QGIS Desktop** — настольная ГИС для создания, редактирования, визуализации, анализа и публикации геопространственной информации. Под «*QGIS*» часто имеют в виду именно *QGIS Desktop*.
- **QGIS Server** и **QGIS Web Client** — серверные приложения для публикации в сети проектов, созданных в *QGIS Desktop*, через сервисы, совместимые с OGC-стандартами (например, *WMS* и *WFS*).

QGIS позволяет использовать большое количество распространенных ГИС функций, обеспечиваемых встроенными инструментами и модулями. Основные возможности рассмотрим ниже.

Просмотр данных

Можно просматривать и накладывать друг на друга векторные и растровые данные в различных форматах и проекциях без преобразования во внутренний или общий формат.

Поддерживаются следующие основные форматы:

- пространственные таблицы и представления *PostGIS, SpatiaLite* и *MSSQL Spatial*, векторные форматы, поддерживаемые установленной библиотекой *OGR*, включая *shape*-файлы *ESRI, MapInfo, SDTS (Spatial Data Transfer Standard), GML (Geography Markup Language)* и многие другие;
- форматы растров и графики, поддерживаемые библиотекой *GDAL* (Geospatial Data Abstraction Library), такие, как *GeoTIFF, Erdas IMG, ArcInfo ASCII Grid, JPEG, PNG* и многие другие;
- растровый и векторный форматы GRASS (область/набор данных);
- пространственные данные, публикуемые в сети Интернет с помощью *OGC*-совместимых (Open Geospatial Consortium) сервисов *Web Map Service* (WMS) или *Web Feature Service* (WFS);
- данные *OpenStreetMap* (OSM).

Исследование данных и создание карт

С помощью удобного графического интерфейса можно создавать карты и исследовать пространственные данные. Графический интерфейс включает в себя множество полезных инструментов, например:

- браузер QGIS;
- перепроецирование «на лету»;
- компоновщик карт;
- панель обзора;
- пространственные закладки;
- определение/выборка объектов;
- редактирование/просмотр/поиск атрибутов;
- подписывание объектов;
- изменение символики векторных и растровых слоев;
- добавление слоя координатной сетки — средствами расширения *fTools* и в виде элемента оформления;
- добавление к макету карты стрелки севера, линейки масштаба и знака авторского права;
- сохранение и загрузка проектов.

Управление данными: создание, редактирование и экспорт

В QGIS можно создавать и редактировать векторные данные, а также экспортировать их в разные форматы. Чтобы иметь возможность редактировать и экпортировать в другие форматы растровые данные, необходимо сначала импортировать их в GRASS.

QGIS предоставляет следующие возможности работы с данными, в частности:

- инструменты оцифровки для форматов, поддерживаемых библиотекой OGR, и векторных слоев GRASS;
- создание и редактирование shape-файлов и векторных слоев GRASS;
- геокодирование изображений с помощью модуля пространственной привязки;
- инструменты GPS для импорта и экспорта данных в формате **GPX**, преобразования прочих форматов GPS в формат **GPX** или скачивание/загрузка непосредственно в прибор GPS;
- визуализация и редактирование данных *OpenStreetMap*;
- создание слоёв PostGIS из shape-файлов с помощью плагина **SPIT**;
- обработка слоёв PostGIS;
- управление атрибутами векторных данных с помощью новой таблицы атрибутов или модуля *Table Manager*;
- сохранение снимков экрана как изображений с пространственной привязкой.

Анализ данных

Вы можете анализировать векторные пространственные данные в PostgreSQL / PostGIS и других форматах, поддерживаемых OGR, используя модуль *fTools*, написанный на языке программирования Python.

В настоящее время QGIS предоставляет возможность использовать инструменты анализа, выборки, геопроцессинга, управления геометрией и базами данных. Также можно использовать интегрированные инструменты GRASS, которые включают в себя функциональность более чем 400 модулей GRASS.

Публикация карт в сети Интернет

QGIS может использоваться для экспорта данных в **map**-файл и публикации его в сети Интернет, используя установленный веб-сервер **Mapserver**.

Кроме того, QGIS может использоваться как клиент WMS, WMS-C, WFS и WFS-T и как сервер WMS или WFS.

Внешние модули

QGIS может быть адаптирована к особым потребностям благодаря расширяемой модульной архитектуре.

QGIS предоставляет библиотеки, которые могут использоваться для создания модулей. Можно создавать отдельные приложения, используя языки программирования *C++* или *Python*.

Основные модули:

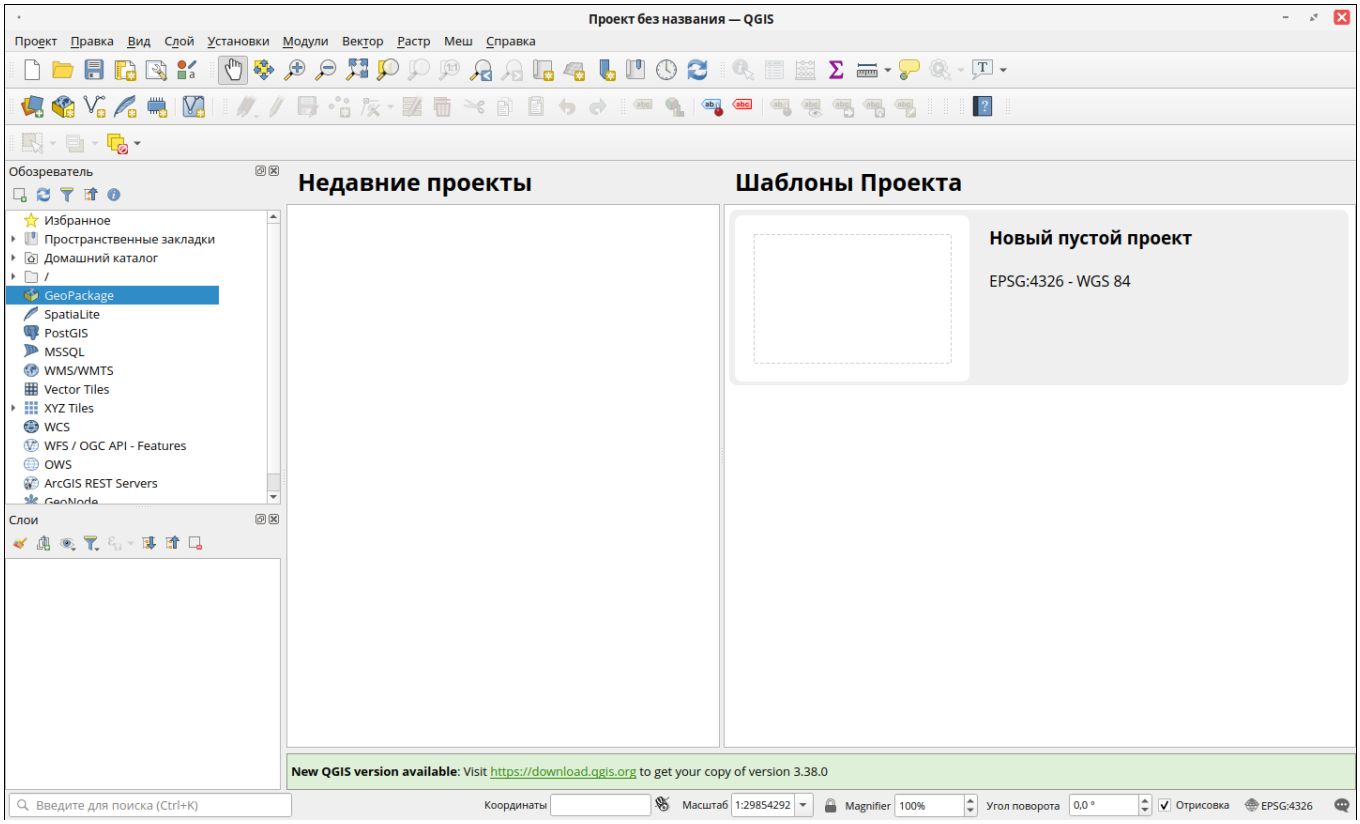
1. *Добавить слой* из текста с разделителями - загружает и выводит текстовые файлы, содержащие координаты x, y.
2. *Захват координат* - получает координаты мыши в различных системах координат.
3. *DB Manager* - импорт/экспорт, редактирование и просмотр слоёв и таблиц, выполнение SQL-запросов.
4. *Наложение диаграмм* - наложение диаграмм на векторные слои.
5. *Преобразователь Dxf2Shp* - преобразование файлов DXF в shape-файлы.
6. *Инструменты GPS* - загрузка и импорт данных GPS.
7. *GRASS* - поддержка ГИС GRASS.
8. *Инструменты GDAL* - интеграция инструментов GDAL в QGIS.
9. *Привязка растров GDAL* - географическая привязка растров.
10. *Теплокарта* - создание растровой теплокарты из точечных данных.
11. *Модуль интерполяции* - интерполяция векторных данных.
12. *Экспорт в Mapserver* - экспорт проекта QGIS в map-файл Mapserver.
13. *Оффлайновое редактирование* - оффлайновое редактирование слоёв и синхронизация с базами данных.
14. *Модуль OpenStreetMap* - просмотр и редактирование данных OpenStreetMap.
15. Доступ к данным *Oracle Spatial GeoRaster*.
16. *Установщик модулей Python* - загрузка и установка модулей QGIS.
17. *Морфометрический анализ* - морфометрический анализ растровых слоев.
18. *Road graph* - поиск кратчайшего маршрута.
19. *SPIT* - инструмент импорта shape-файлов в PostgreSQL/PostGIS.
20. *SQL Anywhere* - работа с векторными слоями в БД SQL Anywhere.
21. *Зональная статистика* - расчет количества, суммы, среднего значения ячеек растра в пределах заданных полигонов.
22. *Пространственные запросы* - пространственные запросы для векторных слоёв.
23. *eVIS* - инструмент визуализации событий — показ изображений, связанных с векторными объектами.
24. *fTools* - инструменты для управления векторными данными и их анализа.

Установка

Установка программы в РЕД ОС осуществляется командой:

```
dnf install qgis
```

Стартовое окно программы выглядит следующим образом:



Подробную информацию о работе в QGIS см. в официальной документации.

Weasis — программа просмотра диагностических изображений в формате DICOM

Установка Weasis
Смена языка интерфейса
Открытие изображений

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: weasis-4.0.3-1

Примечание.

Данная статья актуальна **только** для РЕД ОС **Стандартной редакции**.

Weasis — средство для просмотра диагностических изображений в формате **DICOM** (**.dcm**), которые используются в здравоохранении.

Является бесплатным программным обеспечением с открытым исходным кодом. Weasis поддерживает многопоточность, что позволяет выполнять высококачественный рендеринг с высокой производительностью за счет **OpenCV**-библиотеки.

Также программа имеет удобный пользовательский интерфейс и работает на экранах с высоким разрешением.

Основные особенности, заявленные разработчиками программы:

- отображение всех типов файлов DICOM (включая многокадровые, расширенные, *MPEG-2*, *MPEG-4*, *SR*, *PR*, *KOS*, *AU*, *RT* и *ЭКГ*);
- средство просмотра распространенных форматов изображений (*TIFF*, *BMP*, *GIF*, *JPEG*, *PNG*, *RAS*, *HDR* и *PNM*);
- манипуляции с изображением (панорамирование, масштабирование, управление окнами, вращение, отражение, прокрутка);
- отображение и поиск по всем атрибутам *DICOM*;
- отображение поперечных линий;
- инструменты измерения и аннотации;
- гистограмма значений модальности;
- сохранение измерений и аннотаций в файле *DICOM PR* или *XML*;
- импорт CD/DVD и локальных файлов *DICOM*;
- экспорт *DICOM* с несколькими вариантами (*DICOMDIR*, *ZIP*, файл образа *ISO*, создание новых *UID*, транскодирование, *TIFF*, *JPEG*, *PNG*...);
- стеклянная лупа с расширенными параметрами отображения;
- печать и печать *DICOM*;
- чтение изображения *DICOM*, содержащего плавающие или двойные данные (параметрическая карта);
- программа просмотра *ЭКГ DICOM*;
- модуль **Dicomizer** для преобразования стандартных изображений в формат *DICOM*.

Вы можете подробнее ознакомиться с настройкой и работой утилиты **weasis**, просмотрев наши обучающие видео:

- на **RuTube** — Weasis — программа просмотра диагностических изображений в формате DICOM;
- в **Яндекс.Дзен** — Weasis — программа просмотра диагностических изображений в формате DICOM;
- в **VK Видео** — Weasis — программа просмотра диагностических изображений в формате DICOM.

На наших каналах вы также сможете найти много другой полезной информации.

Установка Weasis

Перейдите в сеанс пользователя **root**:

```
su -
```

Сначала необходимо подключить репозиторий **redos-3rdparty-weasis** командой:

```
dnf install redos-3rdparty-weasis
```

Далее выполните команду установки **Weasis**:

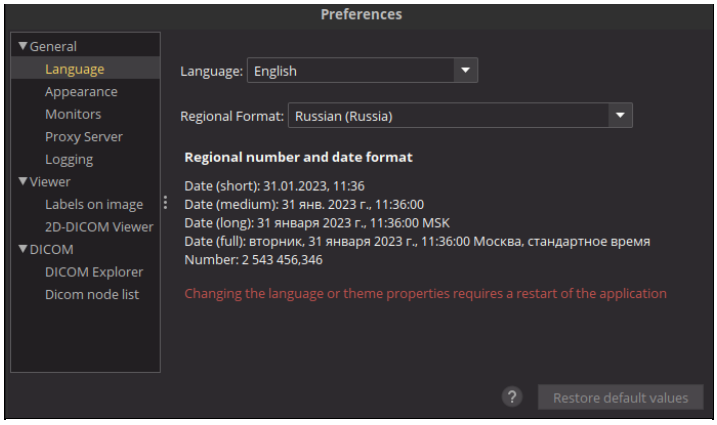
```
dnf install weasis
```

После установки программа доступна из «**Главного меню**» – «**Графика**» – «**Weasis**».

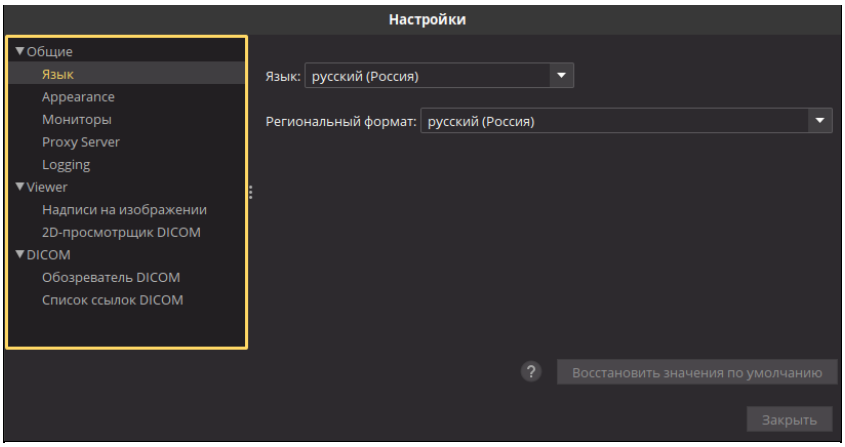
Смена языка интерфейса

Для смены языка программы выберите пункт меню «**File**» - «**Preferences...**», в открывшемся окне настроек откройте пункт **General** – **Language** и выберите из списка необходимый язык.

Интерфейс настроек на английском языке выглядит следующим образом:

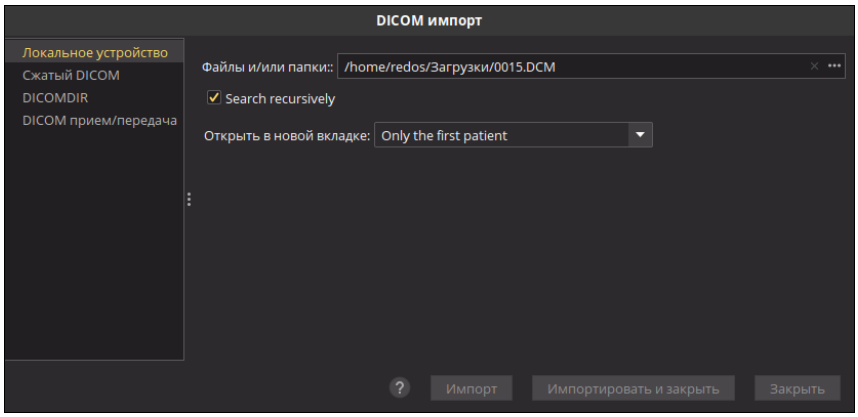


Интерфейс настроек на русском языке выглядит следующим образом (для изменения языка интерфейса необходимо перезапустить программу):

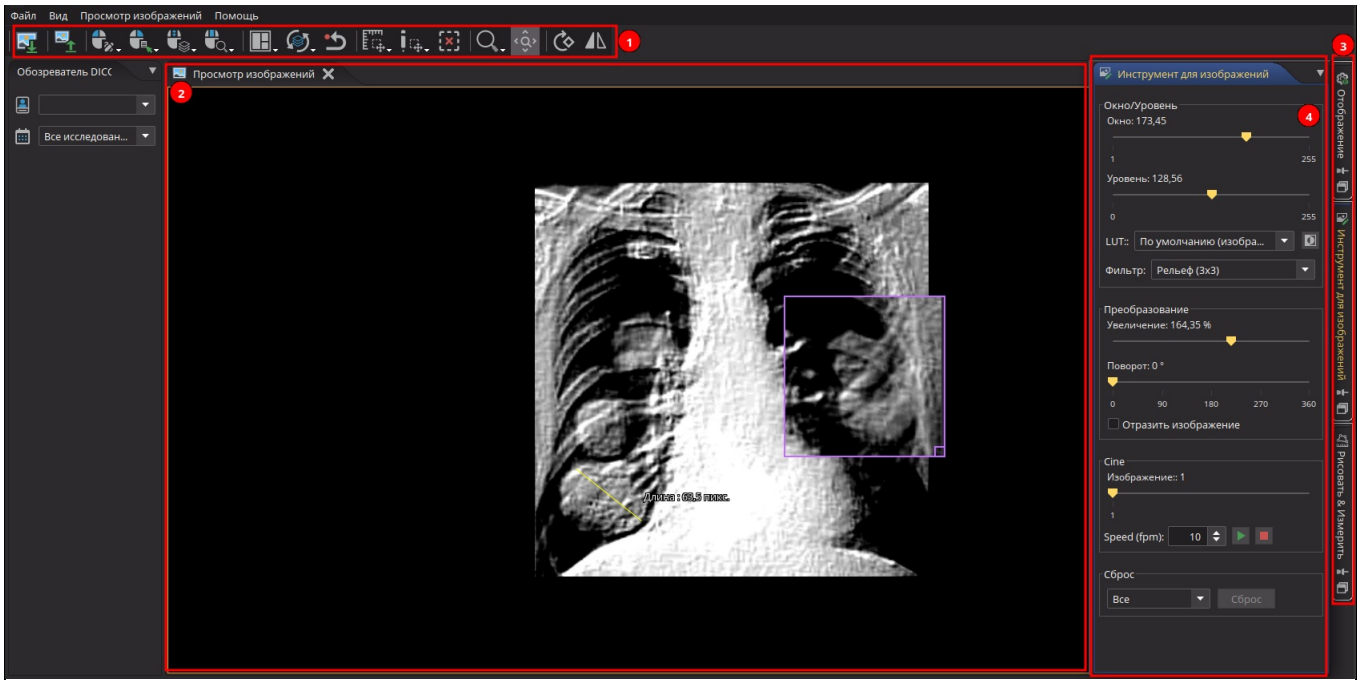


Открытие изображений

Для открытия DICOM-файла в меню программы выберите **Файл** – **Импорт** – **Dicom**.



Диагностическое изображение будет загружено в программу и доступно для детального изучения:



После загрузки изображения станут доступны инструменты для работы. Рассмотрим их подробнее:

1. Панели инструментов.

Здесь располагаются основные инструменты для работы с изображением, такие как *Импорт*, *Экспорт*, *Панель настраиваемых функций мыши*, *Панель расположения изображений*, *Панель инструментов увеличения изображения*, *Панель инструментов вращения* и т. д.

2. Основное окно программы для просмотра изображений.

3. Панель вкладок дополнительных инструментов.

Здесь сгруппированы инструменты *Отображения*, *Измерения* и *Обработки изображений*.

4. Подробное отображение дополнительных инструментов.

При выборе определенной вкладки дополнительных инструментов будет открыта их детальная настройка.

Клавиатурный тренажер KTouch

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ktouch-19.12.2-1

Клавиатура является наиболее часто используемым устройством ввода на любом компьютере. Большинство задач, которые пользователи выполняют с помощью мыши или трекпада, можно выполнить намного быстрее с помощью клавиатуры и некоторых сочетаний клавиш и сенсорного ввода.

Сенсорный ввод текста - это техника, которая помогает печатать тесты быстрее, помещая пальцы на определенные части клавиатуры и нажимая на клавиши, не глядя на клавиатуру.

Несколько причин для освоения навыка сенсорного ввода:

- уменьшение усталости пальцев, поскольку все клавиши находятся рядом;
- повышенная точность по мере развития мышечной памяти;
- улучшение осанки, поскольку не нужно смотреть на клавиатуру;
- быстрое исправление ошибок.

KTouch — это тренажёр для обучения методу слепой печати текста. Он предоставляет текст для тренировки и подстраивается под разные уровни навыков пользователя. Программа отображает клавиатуру и указывает, какую клавишу следует нажать следующей и какой палец при этом использовать.

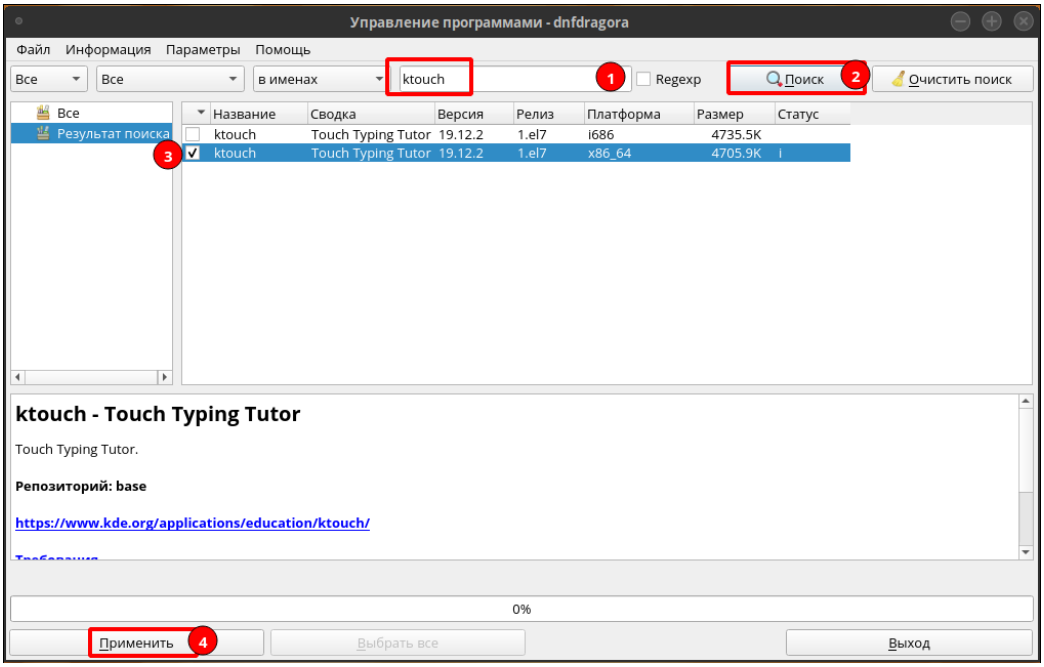
Вы можете подробнее ознакомиться с работой на тренажере **Ktouch**, просмотрев наши обучающие видео:

- на **RuTube** — Клавиатурный тренажер KTouch;
- в **Яндекс.Дзен** — Клавиатурный тренажер KTouch;
- в **VK Видео** — Клавиатурный тренажер KTouch.

На наших каналах вы также сможете найти много другой полезной информации.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**ktouch**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

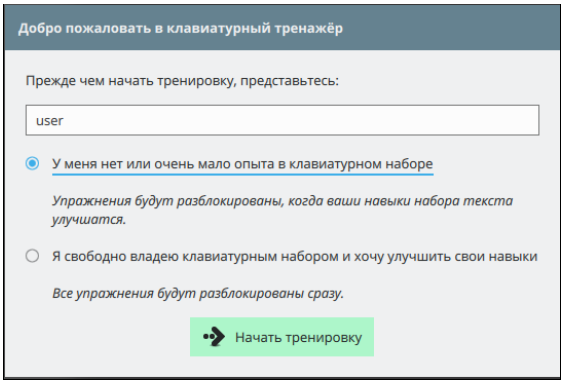
и выполните команду:

```
dnf install ktouch
```

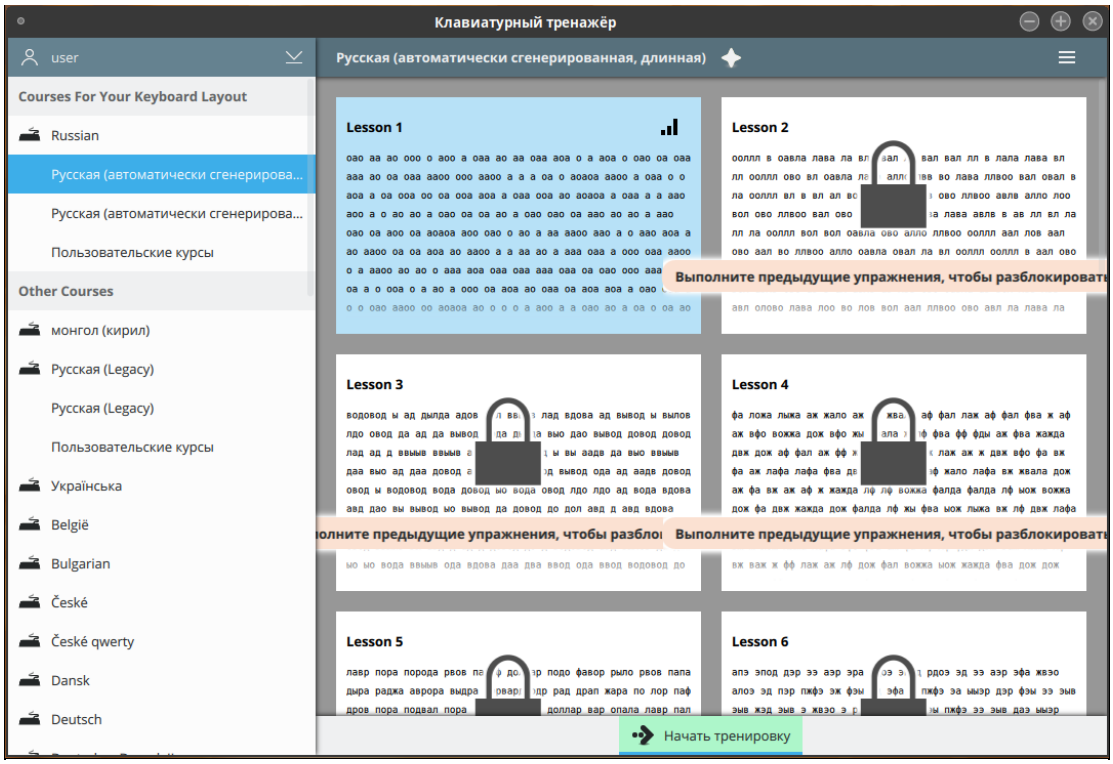
Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**Ktouch**».

При первом запуске программы будет предложено ввести имя пользователя и выбрать уровень владения клавиатурным набором.

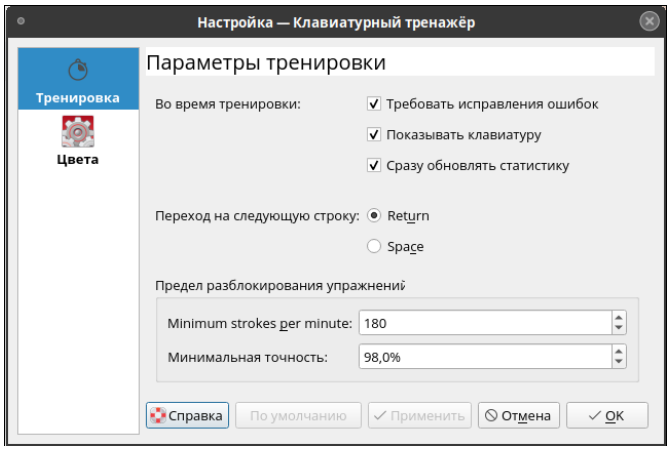


При выборе *начального уровня* — задания будут разблокированы по мере выполнения, при выборе *профессионального уровня* — все упражнения будут разблокированы сразу.



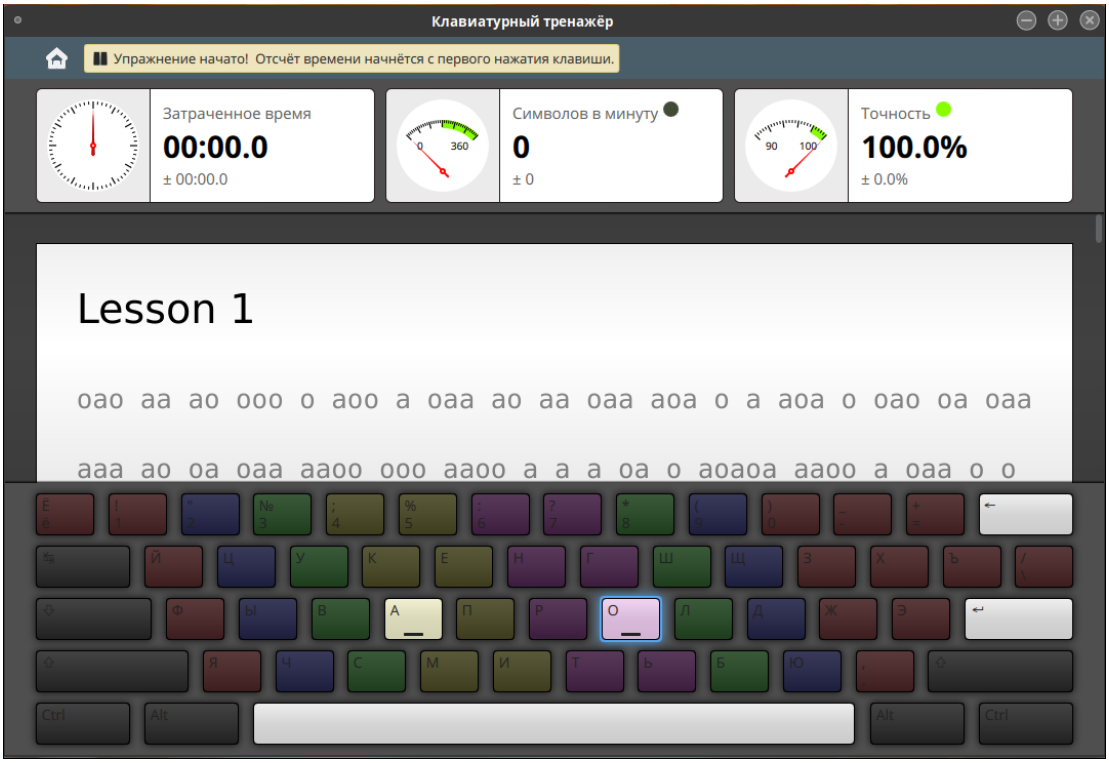
В списке слева можно выбрать любой язык для тренировок.

В **Настройках** есть возможность задать параметры тренировки — требовать ли исправления ошибок, указать минимальную точность и скорость печати в минуту. Также есть возможность задать параметры цвета. Во время упражнений перед Вами будет располагаться клавиатура с соответствующими цветами для подсказки.

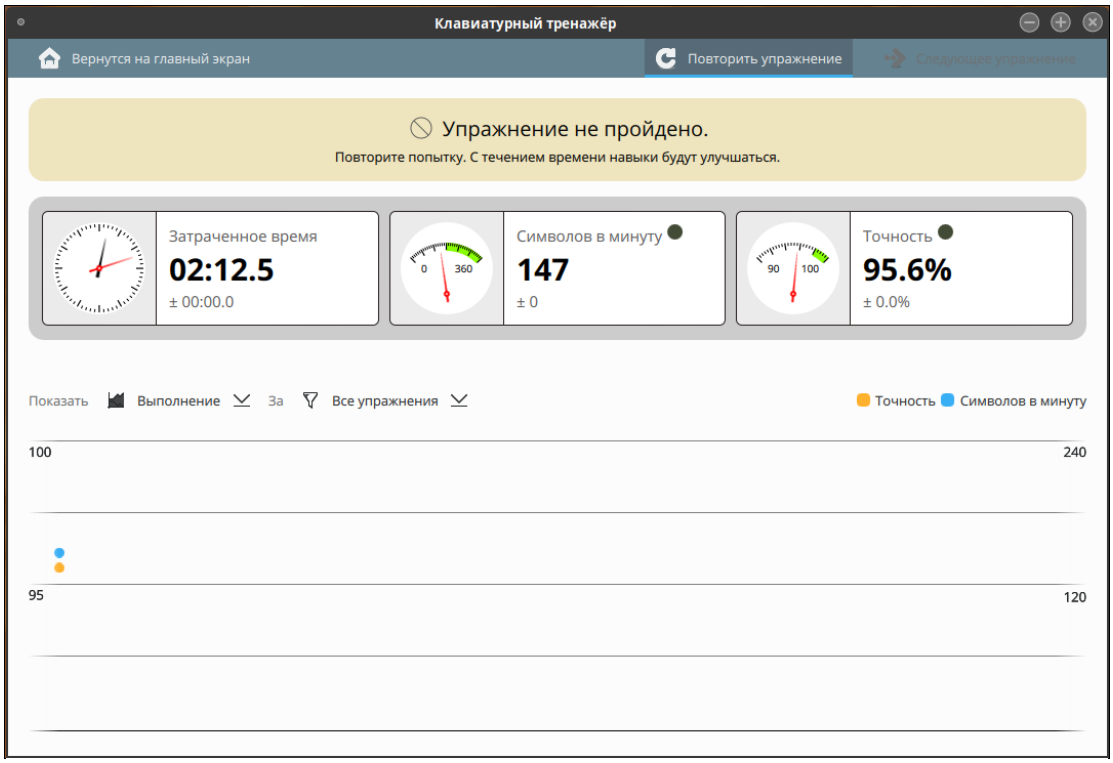


Выберите первый урок и нажмите «**Начать тренировку**».

Каждый урок длится несколько минут и представляет вам различные комбинации клавиш. По мере выполнения, если будут встречаться ошибки, *ktouch* подчеркнет их красным цветом. Добравшись до конца строки, не забудьте нажать **Enter**, а если допустили ошибку - используйте клавишу **Bakspase**.



В конце каждого урока *KTouch* представляет отчет о проделанной работе и статус — **Пройденный** или **Неудачный**.


Клавиатурный тренажёр
Вернутся на главный экран
Повторить упражнение
Следующее упражнение
Упражнение не пройдено.
Повторите попытку. С течением времени навыки будут улучшаться.
Затраченное время
02:12.5
± 00:00.0
0
360
Символов в минуту
147
± 0
90
100
Точность
95.6%
± 0.0%
Показать
Выполнение
За
Все упражнения
Точность
Символов в минуту
100
240
95
120

LibreCAD

Установка LibreCAD

Описание программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: librecad-2.2.0-0.11

LibreCAD – это мощный и бесплатный проект с открытым исходным кодом для проектирования 2D-технологий. Он предлагает широкий набор инструментов, позволяющих создавать высококачественные чертежи. Этот инструмент имеет простой и интуитивно понятный пользовательский интерфейс, что делает его идеальным выбором для начинающих пользователей, которые хотят освоить искусство компьютерного проектирования, а также для профессионалов, которым нужен надежный инструмент для работы с 2D-моделями.

Особенности **LibreCAD**:

- Кроссплатформенность – **LibreCAD** доступен на операционных системах Windows, macOS и Linux, что делает его универсальным инструментом для пользователей всех типов систем.
- Интерфейс и инструменты – программа предлагает широкий набор инструментов для создания точных чертежей. Он включает в себя создание линий, окружностей, дуг, текста, а также специализированные инструменты для работы с размерами и слоями.
- Поддержка форматов – **LibreCAD** поддерживает широкий спектр форматов файлов, включая **DXF**, поэтому пользователи могут легко импортировать и экспортировать свои чертежи в/из других CAD-систем.
- Сообщество и поддержка – благодаря своему статусу OpenSource-проекта, **LibreCAD** имеет активное сообщество пользователей и разработчиков, что обеспечивает постоянное обновление и улучшение программы.

LibreCAD нашел широкое применение в различных областях, включая архитектуру, инженерное дело, и даже в образовательных целях. Программа позволяет пользователям создавать точные чертежи различной сложности, начиная от простых эскизов и заканчивая более сложными техническими чертежами.

Установка LibreCAD

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

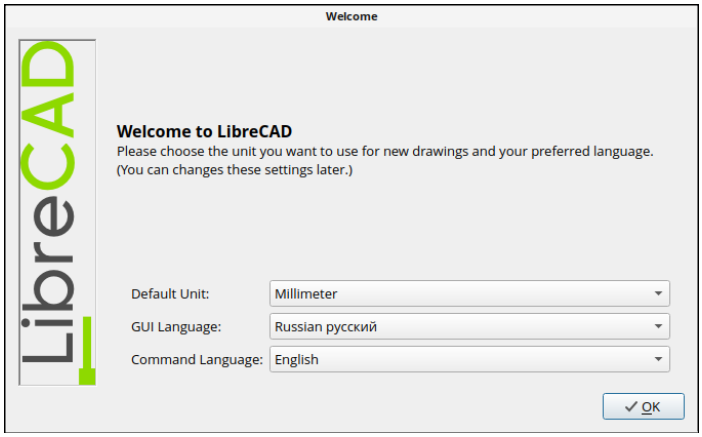
и выполните команду:

```
dnf install librecad
```

Запуск программы доступен из «**Главного меню**» – «**Графика**» – «**LibreCAD**».

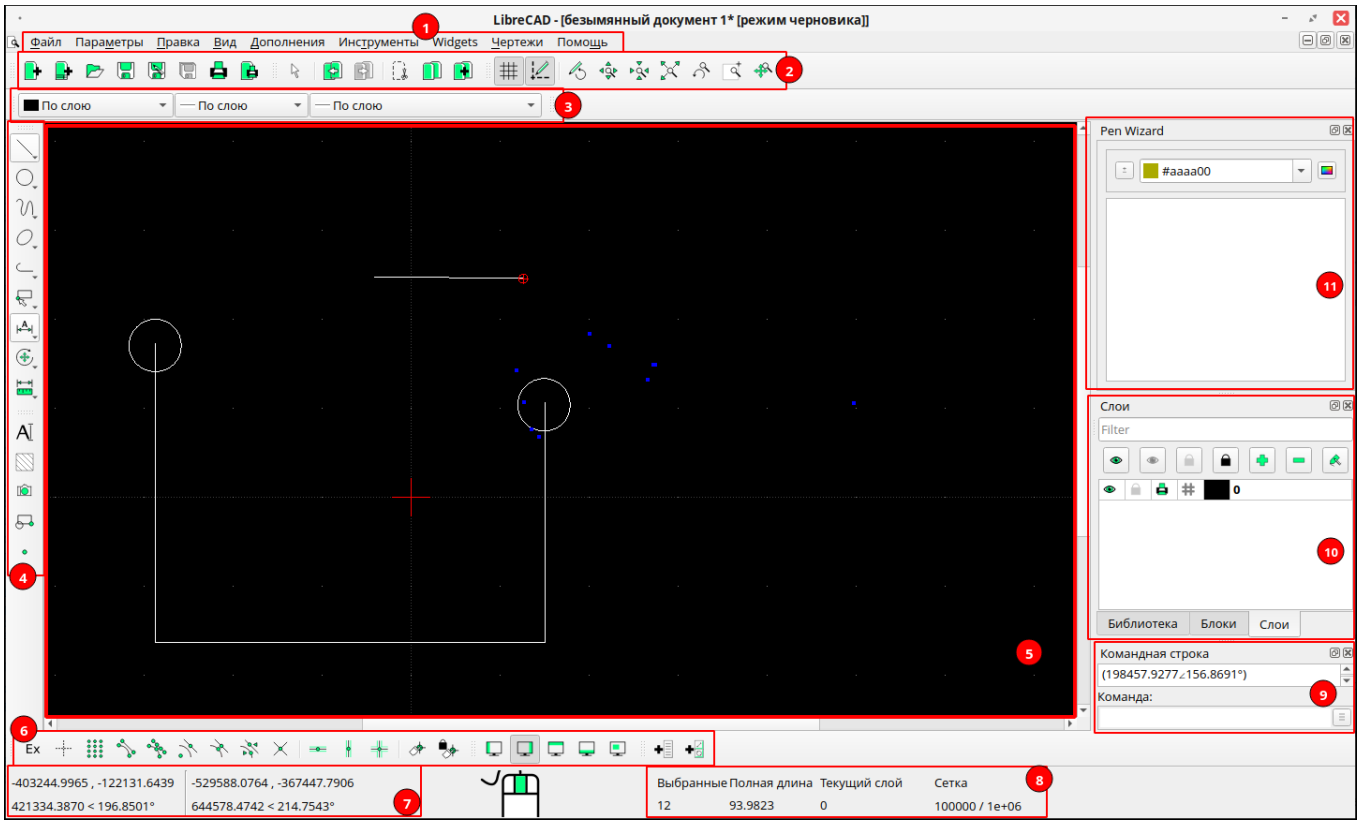
При первом запуске необходимо выбрать систему измерения по умолчанию, язык интерфейса и язык команд.

Выберите необходимые параметры и нажмите «**OK**».



Описание программы

Главное окно программы выглядит следующим образом:



1. *Основное меню* программы, где доступны все действия по настройке и работе программы.

2. *Панель инструментов* – здесь доступны основные действия над проектом, такие как создание нового проекта, сохранение проекта, печать проекта, масштабирование, добавление сетки для удобства и пр.

3. *Панель настройки линий* – цвет, ширина, тип.

4. *Боковая панель* инструментов с основными инструментами для создания проекта, такими как создание линий, окружностей, кривых, измерение расстояния, выбор блоков, добавление текста и пр.

5. *Рабочая область*, где создается проект.

6. *Нижняя панель* – здесь настраивается привязка объектов, ограничения, положение относительного нуля, отображение панелей и добавление нового меню и новых панелей инструментов.

7. *Координаты* положения курсора.

8. *Данные* о выбранных точках (объектах).

9. *Командная строка* – здесь доступно выполнение каких-либо команд над объектом.

10. *Панель слоев* – здесь можно отображать/скрывать слои для удобства работы, а также защищать от модификации объекты чертежа.

11. *Панель* для задания *цвета* выбранному объекту.

Программа имеет интуитивно понятный интерфейс. В случае если возникают какие-либо сложности в работе, доступна онлайн-справка по работе. Для ее вызова в основном меню программы выберите «**Помощь**» – «**Онлайн**».

NanoCAD 24.1

Модульный состав программы
Системные требования
Установка NanoCAD
Установка Платформы nanoCAD из репозитория
Установка Платформы nanoCAD из установочных пакетов
Лицензионное соглашение
Активация локальной лицензии
Запрос и активация локальной лицензии онлайн
Активация локальной лицензии оффлайн при помощи сохранения лицензионного запроса
Активация локальной лицензии оффлайн при помощи файла лицензии
Сервер лицензий
Установка сервера лицензий Нанософт из репозитория
Установка сервера лицензий Нанософт из установочного пакета
Активация сетевой лицензии оффлайн при помощи файла сетевой лицензии
Запрос и активация сетевой лицензии онлайн
Подключение к серверу лицензий
Состояние лицензии
Проверка подключения к локальным базам данных PostgreSQL СПДС и Механика
Установка Сервера лицензий в РЕД ОС конфигурации Сервер минимальный
Установка баз данных PostgreSQL СПДС и Механика на сервер
Дополнительная информация

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: NanoCAD-24.1-x86_64

NanoCAD представляет собой универсальный векторный редактор, а также графическую платформу для целого ряда вертикальных приложений – систем автоматизированного проектирования (САПР) в различных областях проектирования.

NanoCAD предоставляет проектировщикам полный набор современных инструментов для создания и редактирования векторных примитивов, трехмерных объектов, блоков, размеров, таблиц как в пространстве модели, так и в пространстве листа посредством видовых экранов, а также для подготовки, оформления и выпуска графической технической документации.

NanoCAD предназначается как для работы индивидуального пользователя, так и для работы проектных коллективов, с использованием функционала внешних ссылок и возможностью интеграции в системы инженерного документооборота, в том числе в системы **PDM/PLM**.

NanoCAD поддерживает импорт и экспорт векторных данных в различные 3D и 2D форматы.

Модульный состав программы

Помимо основного функционала, платформа **nanoCAD** включает в себя несколько независимо лицензируемых встроенных модулей:

- **Модуль СПДС**. Модуль позволяет быстро и точно оформлять проектно-конструкторскую документацию по общетехническим требованиям нормативных документов, применяемых в строительной отрасли. Планы, фасады, разрезы, сечения, виды, узлы и другие чертежи выполняются «на лету» с помощью инструментов, создающих динамические «умные» чертежи.
- **Модуль Механика**. Модуль предназначен для проектирования машиностроительных изделий и оформления конструкторской и технологической документации в полном соответствии с требованиями ГОСТ (ЕСКД и ЕСТД) и основными зарубежными стандартами. Наличие параметрических объектов и средств автоматизированного проектирования среднего уровня делают это программное решение одним из самых удобных инструментов создания и оформления чертежей.
- **Модуль Растр** расширяет возможности работы платформы с различными растровыми изображениями, включая сканированные документы – чертежи, планы, схемы и т.п. Базовая конфигурация платформы *nanoCAD* предоставляет возможность использовать такого рода данные лишь в качестве подложки, сопровождая это набором из нескольких инструментов по 4-х точечной коррекции, выравниванию, обрезке и настройке параметров отображения растровых изображений. В состав модуля **Растровое редактирование** входит широкий набор инструментов по улучшению качества изображений, их преобразованию, интеллектуальному анализу и редактированию, извлечению семантической информации (векторизации), полуавтоматической трассировке векторных примитивов и распознаванию текстов, а также растеризации произвольного вида данных, поддерживаемых *nanoCAD*.
- **Модуль 3D на ядре C3D**, включающий в себя функционал **2D** и **3D Зависимостей**. Модуль позволяет при помощи инструментов трехмерного проектирования формировать сложные трехмерные сцены любой геометрической формы. С помощью функции создания сечений можно получать автоматически обновляемые двумерные виды.

- **Модуль Организация** – централизованное управление настройками рабочих мест *nanoCAD* на предприятии.
- **Модуль Топоплан** предназначен для создания цифровой модели местности и подготовки чертежа к выпуску топографических планов. В модуль включена поддержка объектов **Civil 3D**. Если открыть чертёж, содержащий такие объекты, то они будут отображаться как объекты чертежа (а не в виде прокси-графики), будет доступно отображение их свойств, переключение стилей, управление элементами стилей.

На время триального (пробного) периода все модули доступны. По окончании триального периода для активации любого модуля необходимо получить соответствующую лицензию.

Существует три варианта платформ *nanoCAD*:

- платформа ***nanoCAD*** с бесплатным пробным периодом 30 дней;
- платформа ***nanoCAD Standart*** для представителей малого и среднего бизнеса;
- платформа ***nanoCAD Pro*** с максимальной конфигурацией для крупных и корпоративных клиентов.

Актуальные цены на платформы *nanoCAD* приведены на официальном сайте разработчика ПО.

Системные требования

Перед установкой *NanoCAD* убедитесь, что ваша система выполняет условия минимальных системных требований.

Оптимальная производительность и более высокая стабильность работы *NanoCAD* может быть достигнута, когда используемая операционная система выполняет условия рекомендуемых системных требований.

	Минимальные требования	**Рекомендуемые требования**
Процессор	2 ГГц	3 ГГц и выше
Оперативная память	4 Гб	16 Гб и выше
Видеоадаптер	Графический процессор с поддержкой 3D-ускорения, объемом видеопамяти 1 Гб	Графический процессор с поддержкой 3D-ускорения, объемом видеопамяти 4 Гб (поддерживающий OpenGL 2.1)
Разрешение экрана	1920 x 1080	до 3840 x 2160
Свободное место на диске	7 Гб и более	
Сеть	На сервере лицензий и всех рабочих станциях, где будут работать приложения, использующие сетевое лицензирование, должен быть запущен протокол **TCP/IP.**	
Интерфейсы	Видеовыход **HDMI** или **Displayport**, устройство для чтения DVD-дисков или USB-порт	

Установка NanoCAD

Установка Платформы nanoCAD из репозитория

Предварительно необходимо подключить репозиторий платформы при помощи скрипта:

```
sudo wget -qO- https://repo.nanodev.ru/r24.1/get_ncad.sh | sudo bash
```

Для автоматической установки платформы NanoCAD совместно с локальным сервером БД Механика и СПДС на запрос скрипта «Желаете установить nanoCAD? [д/Н]:» ответьте yes. Если установка и настройка будет производиться вручную, ответьте no.

Для ручной установки платформы БЕЗ локального сервера PostgreSQL баз данных СПДС и Механика выполните команды:

```
sudo dnf check-update
sudo dnf install ncad24-1
```

Затем выполните настройку сервера и подключения к серверу PostgreSQL на клиенте согласно п. «Установка баз данных PostgreSQL СПДС и Механика на сервер».

Для ручной установки СОВМЕСТНО с локальным сервером PostgreSQL баз данных СПДС и Механика выполните команды:

```
sudo dnf check-update
sudo dnf install ncad-pgsql
sudo dnf install ncad24-1
```

Подключение к локальному серверу баз данных СПДС и Механики будет настроено автоматически. При необходимости, выполните проверку подключения к локальному серверу баз данных PostgreSQL СПДС и Механика согласно п. «Проверка подключения к локальным базам данных PostgreSQL СПДС и Механика».

Если пакет `ncad-data24-1` был установлен раньше, чем `ncad-pgsql`, для установки и настройки баз необходимо выполнить:

```
ncad-db-install24-1
```

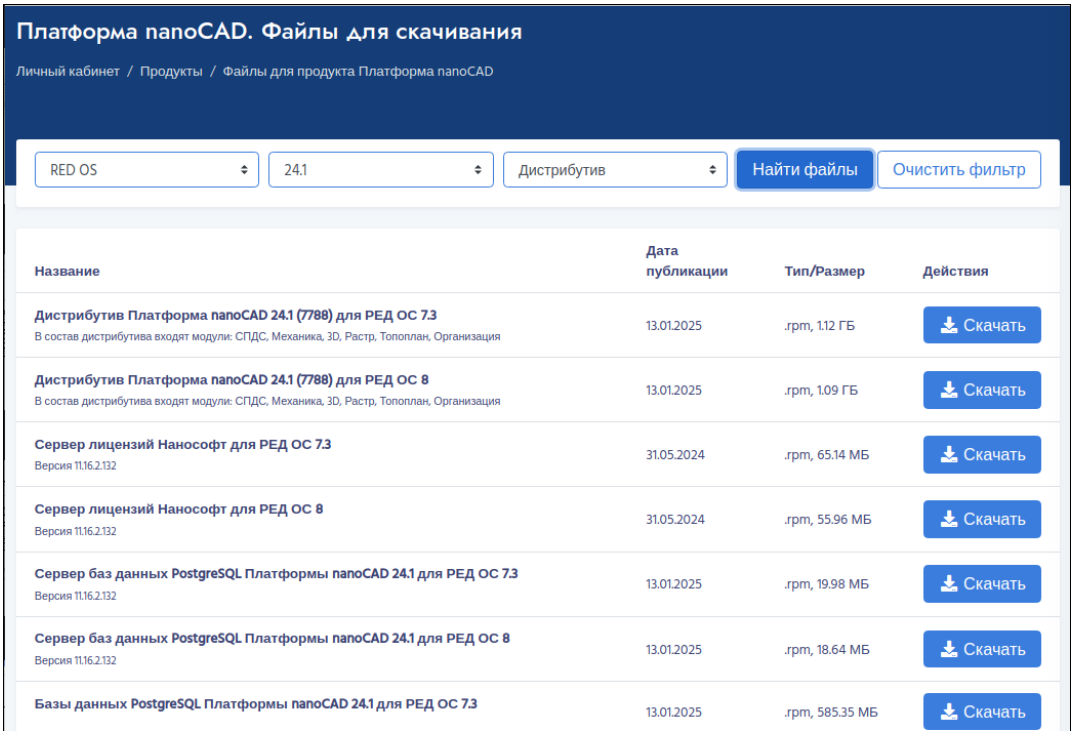
Установка Платформы nanoCAD из установочных пакетов

ВАЖНО!

Для доступа к загрузке дистрибутивов необходимо предварительно зарегистрироваться или авторизоваться в Личном кабинете.

Для загрузки инсталляционных пакетов перейдите по ссылке. На странице задайте фильтр для списка доступных дистрибутивов:

- выберите ОС – **RED OS**;
- выберите версию продукта – **24.1**;
- выберите тип файлов – **дистрибутив**.



Загрузите необходимые пакеты, нажав «**Скачать**».

Для установки БЕЗ локального сервера БД Механика и СПДС загрузите:

- Базы данных платформы NanoCAD для РЕД ОС 7.3 – ncad-data24-1.el7.x86_64.rpm;
- Платформа NanoCAD для РЕД ОС 7.3 – ncad24-1.el7.x86_64.rpm.

Для установки СОВМЕСТНО с локальным сервером БД Механикка и СПДС загрузите:

- Сервер БД платформы NanoCAD для РЕД ОС 7.3 – ncad-pgsql.el7.x86_64.rpm;
- Базы данных платформы NanoCAD для РЕД ОС 7.3 – ncad-data24-1.el7.x86_64.rpm;
- Платформа NanoCAD для РЕД ОС 7.3 – ncad24-1.el7.x86_64.rpm.

Затем перейдите в каталог со скачанными файлами – «**Загрузки**» (по умолчанию).

Для установки локальных БД и сервера БД **Механика** и **СПДС** выберите соответствующие инсталляционные пакеты (согласно указанной последовательности установки) и запустите их выполнение двойным кликом ЛКМ. В открывшемся окне «**Аутентификация**» введите пароль администратора. Нажмите **Аутентификация**.

В окне «**Результат транзакции**» будет выведен список устанавливаемых пакетов, нажмите **Хорошо** для продолжения установки.

По окончании установки нажмите **Выход**.

Повторите те же действия для пакета платформы NanoCAD **ncad24.1_x86_64.rpm**.

Примечание.

В случае если по каким-либо причинам пакет **ncad-data24-1.el7.x86_64.rpm** был установлен раньше, чем пакет **ncad-pgsql.el7.x86_64.rpm**, для установки и настройки баз необходимо выполнить:

```
ncad-db-install24-1
```

После успешной установки ярлыки будут созданы в «**Главном меню**» – «**NanoCAD 24.1**». При необходимости, можно создать ярлыки приложений на рабочем столе через контекстное меню. Для этого нажмите ПКМ на нужном приложении и выберите **Поместить на Рабочий стол**.

Лицензионное соглашение

Для дальнейшей работы в программе *NanoCAD* необходимо принять условия Лицензионного соглашения. Для этого из **Главного меню** запустите **Мастер регистрации** или **Платформу nanoCAD 24.1**.

В появившемся окне «**Установка Платформа nanoCAD x64 24.1 — Лицензионное соглашение**» внизу окна установите флаг «**Я принимаю условия Лицензионного соглашения**». Нажмите **Да**.



Активация локальной лицензии

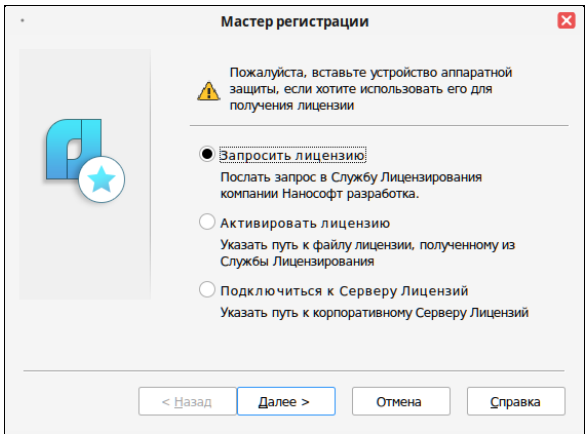
Доступно несколько способов активации лицензии:

- запрос и активация лицензии онлайн;
- активация лицензии оффлайн при помощи сохранения лицензионного запроса;
- активация лицензии оффлайн при помощи файла лицензии.

Для активации лицензии запустите **Мастер регистрации**, который доступен из «**Главного меню**» — «**nanoCAD 24.1**».

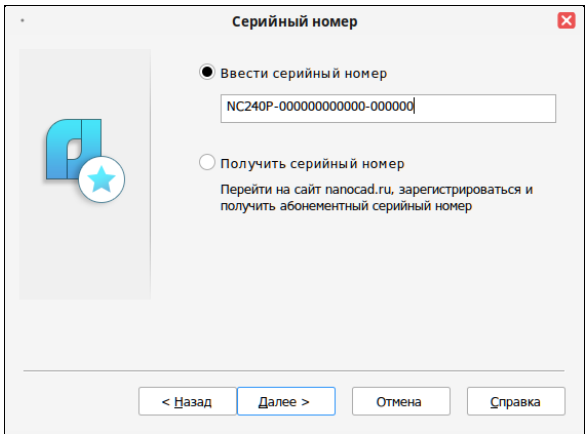
Запрос и активация локальной лицензии онлайн

После запуска **Мастера регистрации** выберите «**Запросить лицензию**» и нажмите **Далее**.



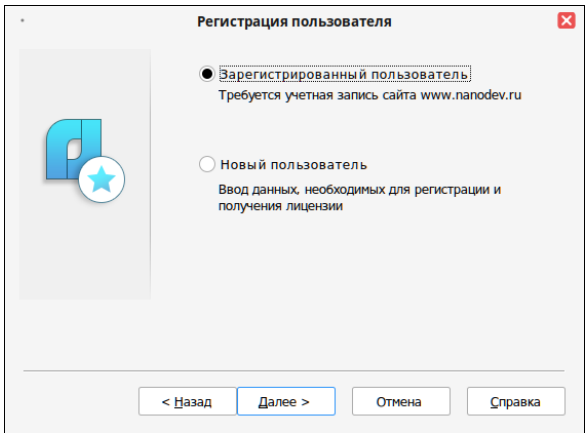
В открывшемся окне «**Серийный номер**» введите серийный номер (если у вас нет серийного номера, выберите пункт « **Получить серийный номер**»). Серийный номер имеет вид *NC240P-000000000000-000000*.

Нажмите **Далее**.



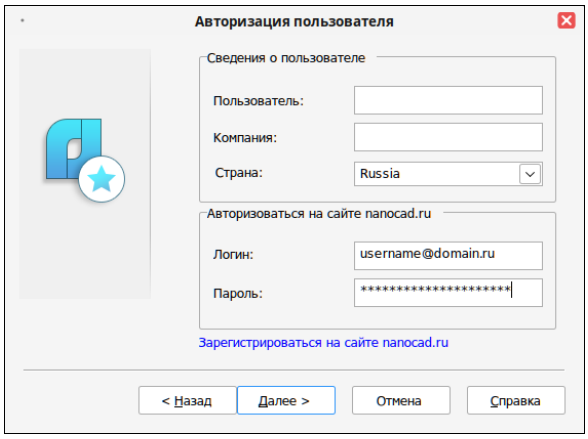
Будет открыто окно «**Регистрация пользователя**».

Если у вас уже есть учетная запись в личном кабинете на сайте https://lk.nanocad.ru, выберите пункт **Зарегистрированный пользователь**. В противном случае, необходимо зарегистрироваться в личном кабинете на сайте https://lk.nanocad.ru перед продолжением процедуры запроса лицензии.



В окне «**Авторизация пользователя**» поля **Логин** и **Пароль** следует заполнять теми значениями, которые были использованы при регистрации в личном кабинете на сайте https://lk.nanocad.ru.

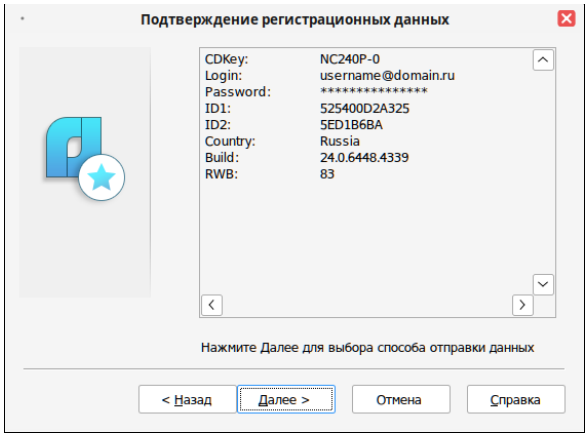
Если вы не зарегистрированы в личном кабинете на сайте https://lk.nanocad.ru, нажмите на ссылку **Зарегистрироваться на сайте www.nanodev.ru**. После регистрации введите ваши регистрационные данные в полях **Логин** и **Пароль**.



Опционально можно заполнить поля **Пользователь** и **Компания**. Информация из этих полей будет отображаться при запуске программного обеспечения.

Заполните необходимые поля и нажмите **Далее**.

В окне подтверждения регистрационных данных отображаются данные, которые будут отправлены в **ООО «Нанософт разработка»** для получения локальной лицензии.

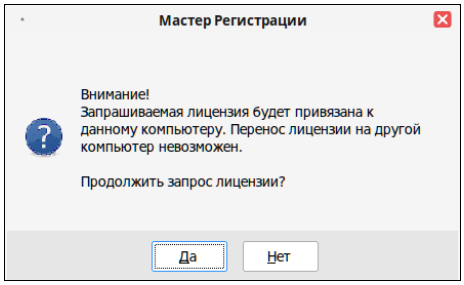


Проверьте введенные данные и подтвердите их нажатием кнопки **Далее**. В случае обнаружения ошибки нажмите **Назад** и исправьте информацию в тех полях, где это необходимо.

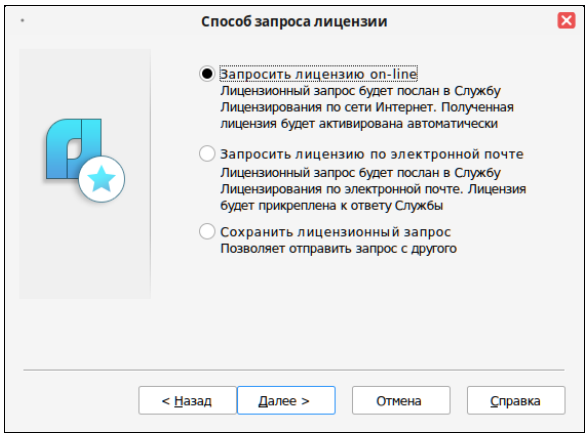
ВАЖНО!

Внимательно проверяйте указанные регистрационные данные. При неверном заполнении регистрационных полей разработчик программного обеспечения **ООО «Нанософт разработка»** может отказать в выдаче лицензии.

Подтвердите привязку лицензии к компьютеру, нажав **Да** в появившемся запросе **Мастера регистрации**.

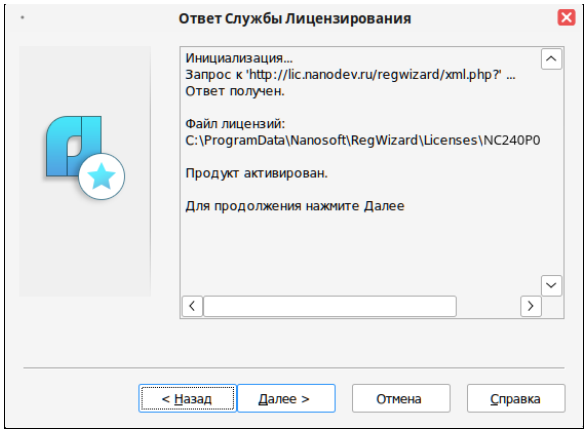


После подтверждения запроса лицензии будет открыто окно «**Способ запроса лицензии**».



Запрос лицензии онлайн производится только с компьютера, имеющего выход в сеть Интернет.

При запросе лицензии онлайн **Мастер регистрации** автоматически соединится с **Сервером лицензий**, сохранит и активирует лицензию.



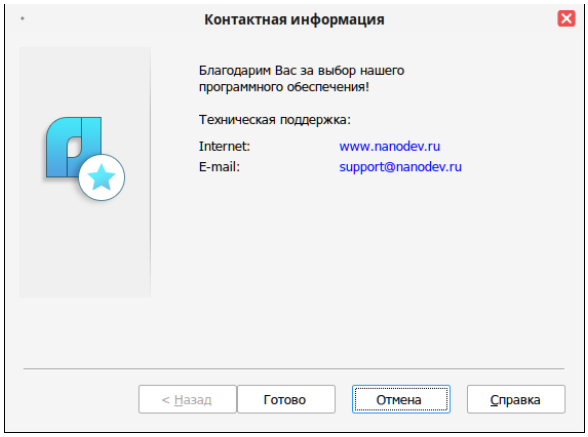
Примечание.

Все файлы лицензий, полученные таким способом, помещаются в следующую директорию **/home/<username>/.ncad_24.1x64/drive_c/ProgramData/Nanosoft/RegWizard/Licenses**.

Результатом запроса лицензии онлайн может быть:

- успешное получение лицензии;
- отказ в выдаче лицензии;
- неудачное соединение.

В случае *успешного* завершения нажмите **Далее** и в следующем окне, содержащем контактную информацию, нажмите **Готово**.



На этом процесс лицензирования продукта **ООО «Нанософт разработка»** успешно завершен. Никаких других действий по лицензированию установленного продукта производить не требуется.

Запустите **Платформу nanoCAD**.

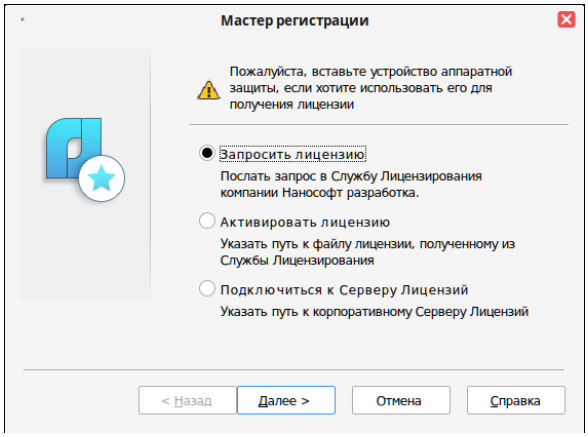
Если по той или иной причине **Сервер** отказал в выдаче локальной лицензии, нажмите **Далее** и в следующем окне, содержащем контактную информацию, нажмите **Готово**, завершив работу.

В случае неудачного соединения с **Сервером**, а также при невозможности получить локальную лицензию выбранным способом нажмите **Далее** и, вернувшись в окно «**Способ запроса лицензии**», выберите другой вариант осуществления запроса.

Дождитесь ответа службы лицензирования.

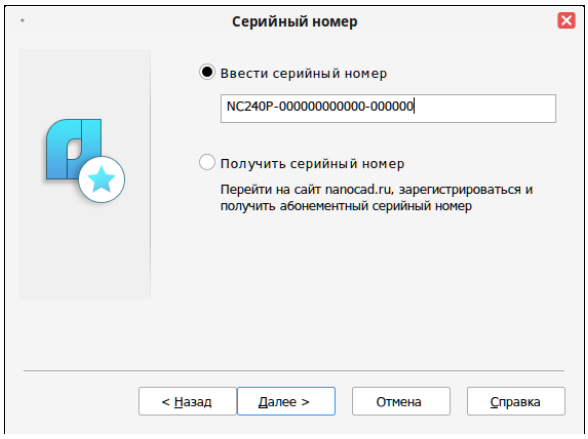
Активация локальной лицензии оффлайн при помощи сохранения лицензионного запроса

После запуска **Мастера лицензий** выберите «**Запросить лицензию**» и нажмите **Далее**.



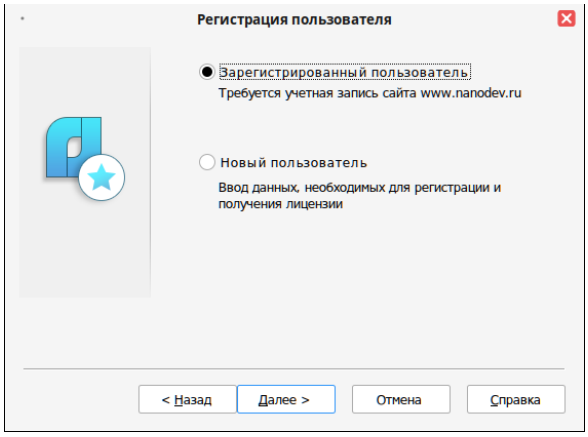
В открывшемся окне «**Серийный номер**» введите серийный номер (если у вас нет серийного номера, выберите пункт « **Получить серийный номер**»). Серийный номер имеет вид *NC240P-000000000000-000000*.

Нажмите **Далее**.



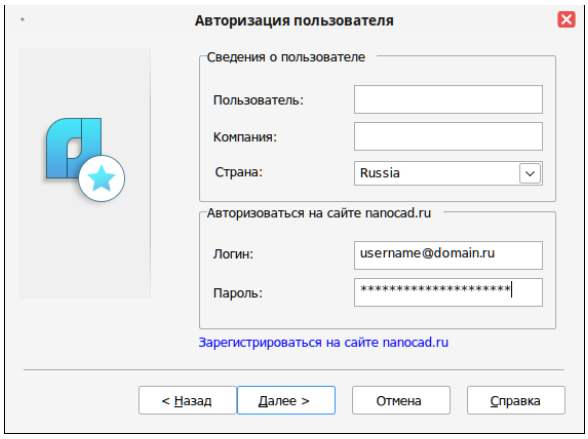
Будет открыто окно «**Регистрация пользователя**».

Если у вас уже есть учетная запись в личном кабинете на сайте https://lk.nanocad.ru, выберите пункт **Зарегистрированный пользователь**. В противном случае, необходимо зарегистрироваться в личном кабинете на сайте https://lk.nanocad.ru перед продолжением процедуры запроса лицензии.



В окне «**Авторизация пользователя**» поля **Логин** и **Пароль** следует заполнять теми значениями, которые были использованы при регистрации в личном кабинете на сайте https://lk.nanocad.ru.

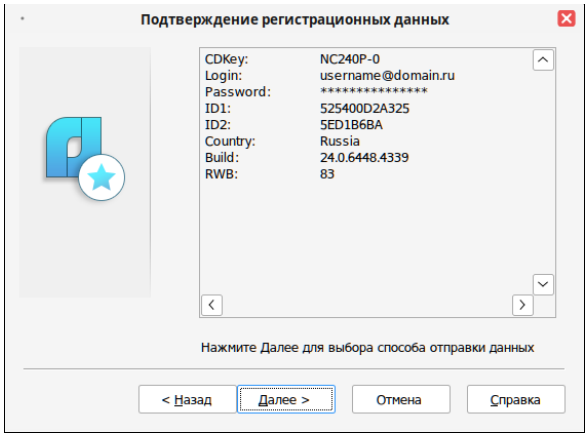
Если вы не зарегистрированы в личном кабинете на сайте https://lk.nanocad.ru, нажмите на ссылку **Зарегистрироваться на сайте www.nanodev.ru**. После регистрации введите ваши регистрационные данные в полях **Логин** и **Пароль**.



Опционально можно заполнить поля **Пользователь** и **Компания**. Информация из этих полей будет отображаться при запуске программного обеспечения.

Заполните необходимые поля и нажмите **Далее**.

В окне подтверждения регистрационных данных отображаются данные, которые будут отправлены в **ООО «Нанософт разработка»** для получения локальной лицензии.

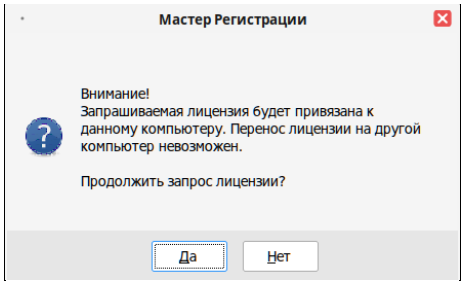


Проверьте введенные данные и подтвердите их нажатием кнопки **Далее**. В случае обнаружения ошибки нажмите **Назад** и исправьте информацию в тех полях, где это необходимо.

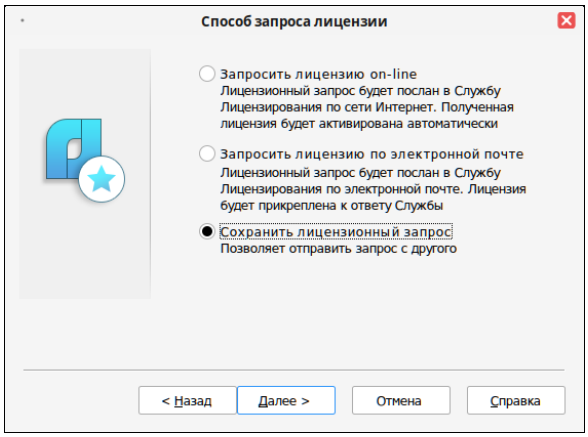
ВАЖНО!

Внимательно проверяйте указанные регистрационные данные. При неверном заполнении регистрационных полей разработчик программного обеспечения **ООО «Нанософт разработка»** может отказать в выдаче лицензии.

Подтвердите привязку лицензии к компьютеру, нажав **Да** в появившемся запросе **Мастера регистрации**.



После подтверждения запроса лицензии будет открыто окно «**Способ запроса лицензии**».



Если компьютер, с которого производится запрос лицензии, не подключен к сети Интернет, необходимо выбрать пункт **Сохранить лицензионный запрос**.

При выборе этого пункта программа автоматически создаст шаблон электронного письма.

Для продолжения процедуры лицензирования необходимо отправить сформированное письмо с компьютера, имеющего выход в сеть Интернет, в службу лицензирования **ООО «Нанософт разработка»**.

ВАЖНО!

Не изменяйте тему и содержимое сохранённого лицензионного запроса при отправке письма. Изменение содержимого может привести к отказу в выдаче лицензионного файла.

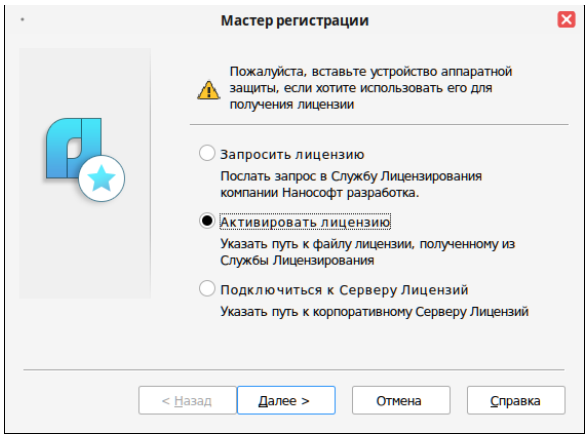
Результатом запроса лицензии при помощи электронной почты будет ответ службы лицензирования с файлом лицензии. Для активации **Платформы nanoCAD** при помощи файла локальной лицензии перейдите к пункту «Активация локальной лицензии оффлайн при помощи файла лицензии».

Активация локальной лицензии оффлайн при помощи файла лицензии

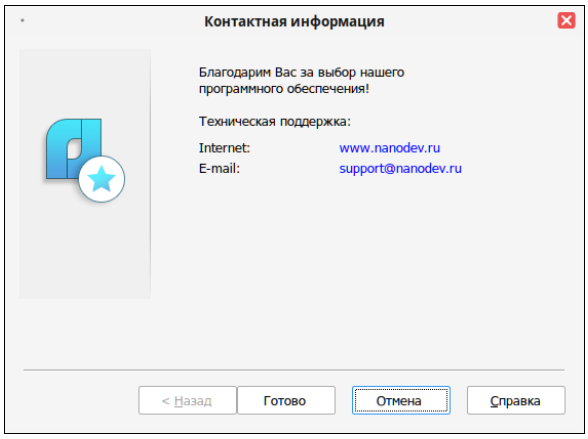
Скопируйте полученный от службы лицензирования **ООО «Нанософт разработка»** файл лицензии на компьютер, где установлен программный продукт, требующий лицензирования.

Запустите Мастер регистрации, который доступен из «**Главного меню**» — «**nanoCAD 24.1**».

В открывшемся окне **Мастера регистрации** программного обеспечения выберите пункт **Активировать лицензию** и нажмите **Далее**.



Укажите путь к файлу лицензии, нажав «**Обзор...**». Нажмите **Далее**.



На этом процесс лицензирования продукта **ООО «Нанософт разработка»** успешно завершен. Никаких других действий по лицензированию установленного продукта производить не требуется.

Запустите **Платформу nanoCAD**.

Сервер лицензий

Установка сервера лицензий Нанософт из репозитория

Примечание.

В случае если ранее платформа **NanoCAD** была автоматически установлена с помощью скрипта согласно пункту «Установка Платформы nanoCAD из репозитория» данный шаг следует пропустить.

Предварительно необходимо подключить репозиторий при помощи скрипта:

```
sudo wget -qO- https://repo.nanodev.ru/r24.1/get_ncad.sh | sudo bash
```

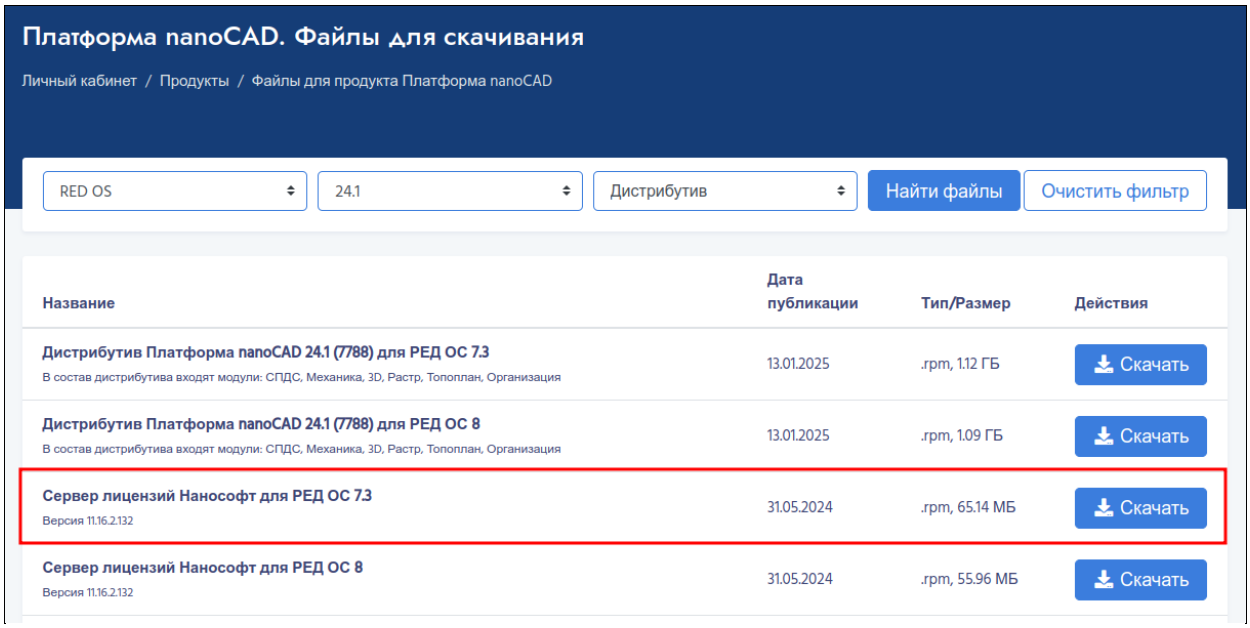
Выполните установку сервера лицензий Нанософт:

```
sudo dnf check-update
sudo dnf install ncad-licsrv
```

Установка сервера лицензий Нанософт из установочного пакета

Для загрузки инсталляционных пакетов перейдите по ссылке. На странице задайте фильтр для списка доступных дистрибутивов:

- выберите ОС – **RED OS**;
- выберите версию продукта – **24.1**;
- выберите тип файлов – **дистрибутив**.



Загрузите **Сервер лицензий Нанософт для РЕД ОС 7.3**, нажав «**Скачать**». Затем перейдите в каталог со скачанным файлом – «**Загрузки**» (по умолчанию).

Для установки **Сервера лицензий** выберите инсталляционный пакет **ncad-licsrv.rpm** и запустите его выполнение двойным кликом ЛКМ. В открывшемся окне **Аутентификация** введите пароль администратора. Нажмите **Аутентификация**.

В открывшемся окне **Результат транзакции** будет выведен список устанавливаемых пакетов, нажмите **Хорошо** для продолжения установки.

По окончании установки нажмите **Выход**.

Активация сетевой лицензии оффлайн при помощи файла сетевой лицензии

Примечание.

Если служба лицензирования уже запущена, перед добавлением лицензии остановите службу следующей командой (потребуются права **администратора** системы):

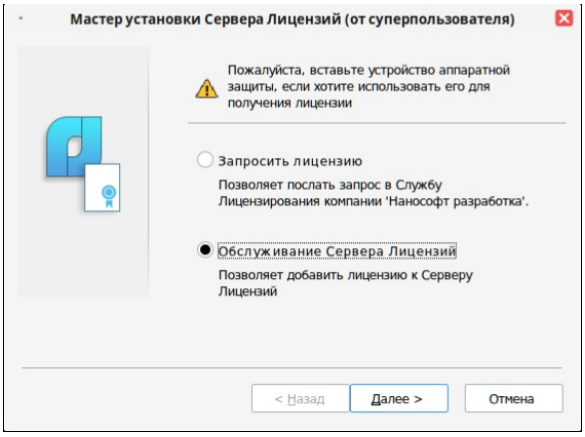
```
sudo systemctl stop ncad-licsrv
```

Если это первый запуск **Мастера установки Сервера лицензий**, пропустите данное предупреждение.

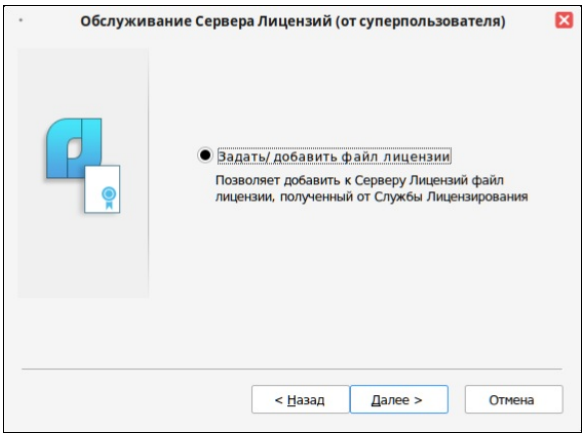
Откройте терминал и запустите **Мастер установки Сервера Лицензий** с правами **администратора** системы:

```
sudo ncad-licreq
```

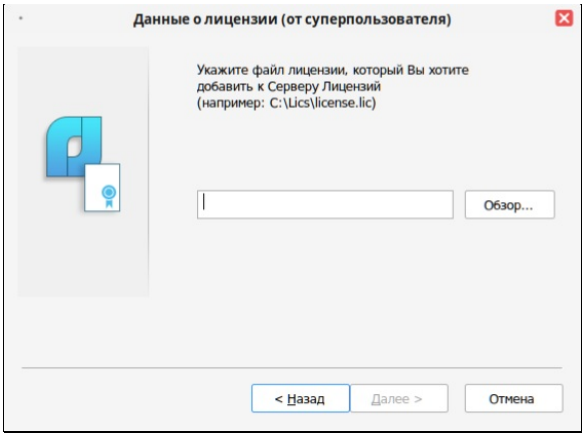
В открывшемся окне выберите «**Обслуживание Сервера Лицензий**». Нажмите **Далее**.



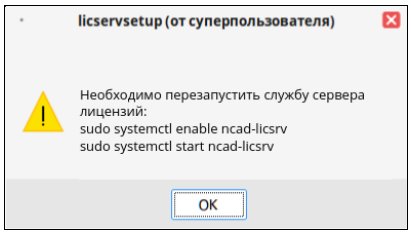
В следующем окне выберите «**Задать/добавить файл лицензии**» и нажмите **Далее**.



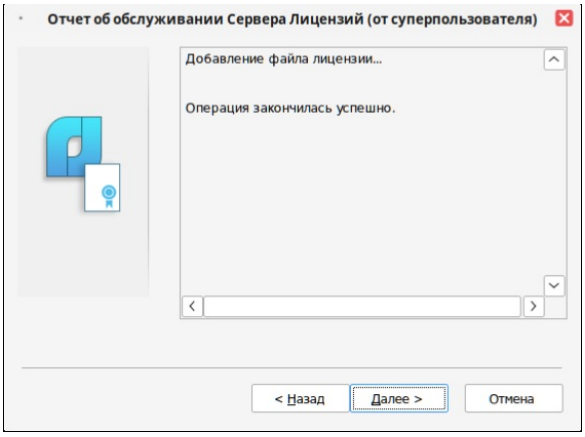
Укажите путь к файлу лицензии с расширением **.lic**, нажав «**Обзор...**». Затем нажмите **Далее**.



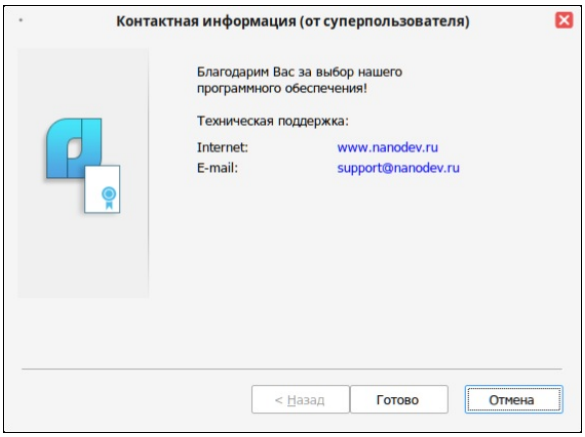
После добавления файла лицензии будет отображено информационное окно с командой запуска службы лицензирования. Нажмите **ОК**.



В случае успешного добавления файла лицензии в окне **Отчета об обслуживании Сервера Лицензий** отображается информация об успешном окончании операции. Нажмите Далее.



В окне «**Контактная информация**» нажмите **Готово**.



Откройте терминал и запустите службу лицензирования с правами суперпользователя:

```
systemctl start ncad-licsrv
```

Проверьте работу службы лицензирования командой:

```
systemctl status ncad-licsrv
```

В случае если все шаги по установке и настройке были выполнены верно, в статусе службы лицензирования будет отображаться **active (running)**.

Запрос и активация сетевой лицензии онлайн

Примечание.

Если служба лицензирования уже запущена, перед добавлением лицензии остановите службу следующей командой (потребуются права администратора системы):

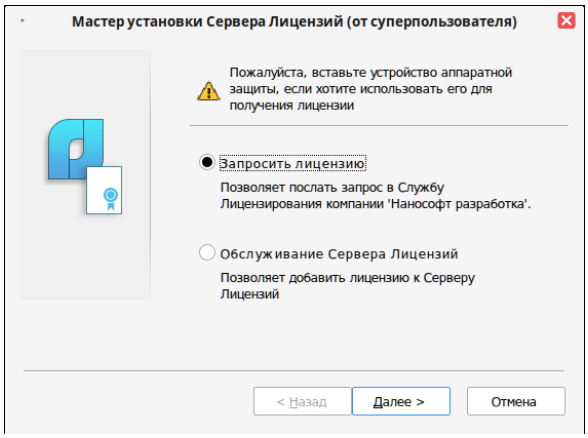
```
sudo systemctl stop ncad-licsrv
```

Если это первый запуск **Мастера установки Сервера лицензий**, пропустите данное предупреждение.

Откройте терминал и запустите **Мастер установки Сервера Лицензий** с правами администратора системы:

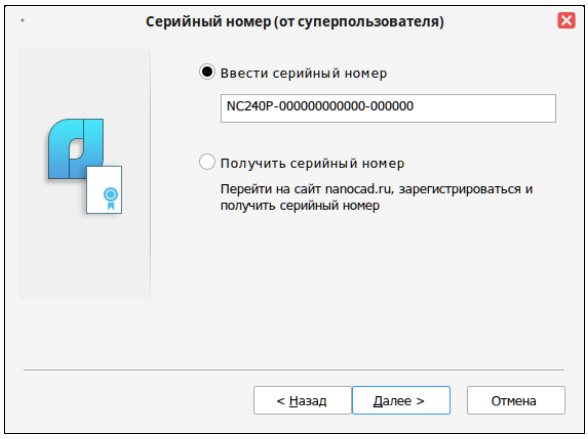
```
sudo ncad-licreq
```

После запуска **Мастера установки Сервера Лицензий** выберите «**Запросить лицензию**» и нажмите **Далее**.



В открывшемся окне «**Серийный номер**» введите серийный номер (если у вас нет серийного номера, выберите пункт « **Получить серийный номер**»). Серийный номер имеет вид *NC240P-000000000000-000000*.

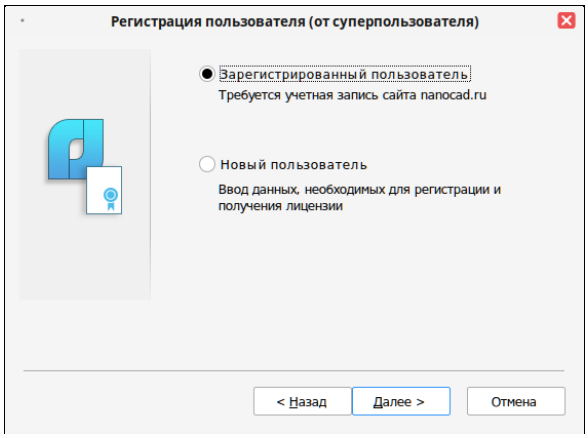
Нажмите **Далее**.



Будет открыто окно «**Регистрация пользователя**».

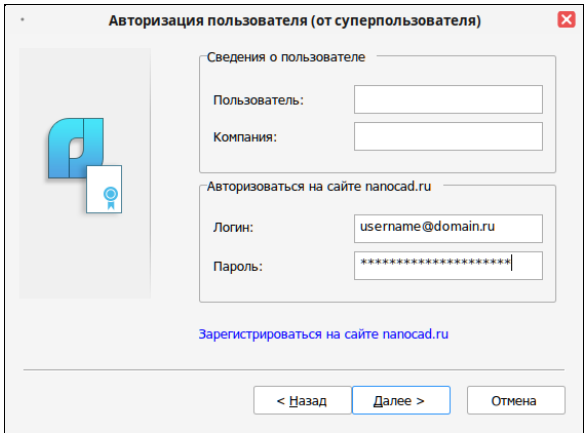
Если у вас уже есть учетная запись в личном кабинете на сайте https://lk.nanocad.ru, выберите пункт **Зарегистрированный пользователь**.

В противном случае выберите пункт «**Новый пользователь**». Сервер лицензий позволяет зарегистрироваться в качестве нового пользователя.



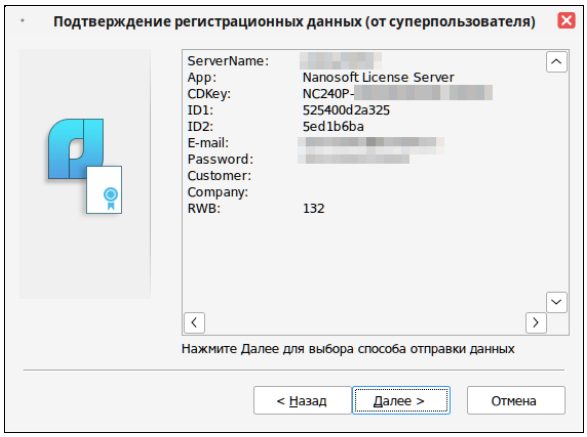
В окне «**Авторизация пользователя**» поля **Логин** и **Пароль** следует заполнять теми значениями, которые были использованы при регистрации в личном кабинете на сайте https://lk.nanocad.ru.

Если вы не зарегистрированы в личном кабинете на сайте https://lk.nanocad.ru, нажмите на ссылку **Зарегистрироваться на сайте www.nanodev.ru**. После регистрации введите ваши регистрационные данные в полях **Логин** и **Пароль**.



Опционально можно заполнить поля **Пользователь** и **Компания**. Нажмите **Далее**.

В окне подтверждения регистрационных данных отображаются данные, которые будут отправлены в **ООО «Нанософт разработка»** для получения сетевой лицензии.

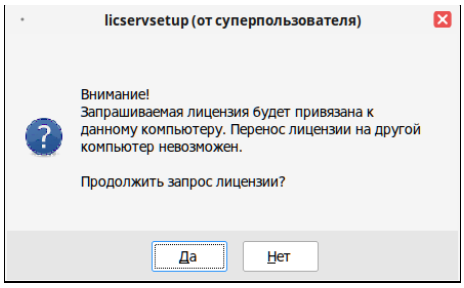


Проверьте введенные данные и подтвердите их нажатием кнопки **Далее**. В случае обнаружения ошибки нажмите **Назад** и исправьте информацию в тех полях, где это необходимо.

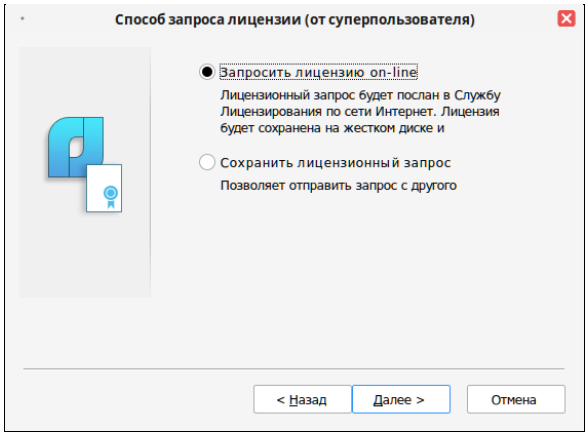
ВАЖНО!

Внимательно проверяйте указанные регистрационные данные. При неверном заполнении регистрационных полей разработчик программного обеспечения **ООО «Нанософт разработка»** может отказать в выдаче лицензии.

Подтвердите привязку лицензии к серверу, нажав **Да** в появившемся запросе **Мастера установки Сервера Лицензий**.

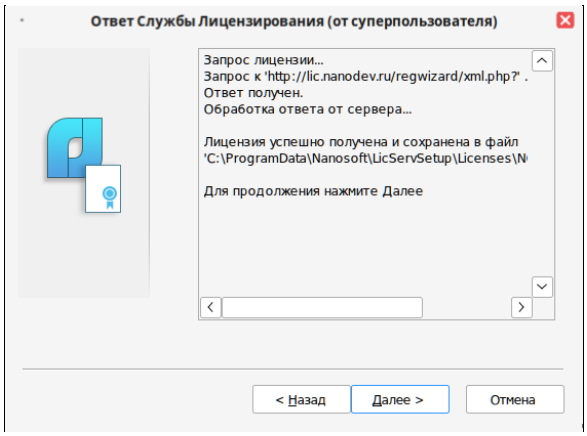


После подтверждения запроса лицензии будет открыто окно «**Способ запроса лицензии**».



Запрос лицензии онлайн производится только с компьютера, имеющего выход в сеть Интернет.

При запросе лицензии онлайн **Мастер установки Сервера Лицензий** автоматически соединится с **Сервером лицензий**, сохранит и активирует лицензию.



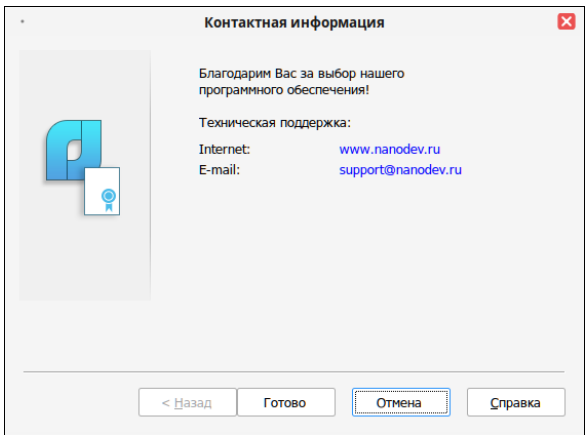
Примечание.

Все файлы лицензий, полученные таким способом, помещаются в директорию **/opt/nanosoft/licsrv/xnhome/drive_c/ProgramData/Nanosoft/LicServSetup/Licenses/**.

Результатом запроса лицензии онлайн может быть:

- успешное получение лицензии;
- отказ в выдаче лицензии;
- неудачное соединение.

В случае успешного завершения нажмите **Далее** и в следующем окне, содержащем контактную информацию, нажмите **Готово**.



Откройте терминал и запустите службу лицензирования с правами **суперпользователя**:

```
systemctl restart ncad-licsrv
```

Проверьте статус службы лицензирования командой:

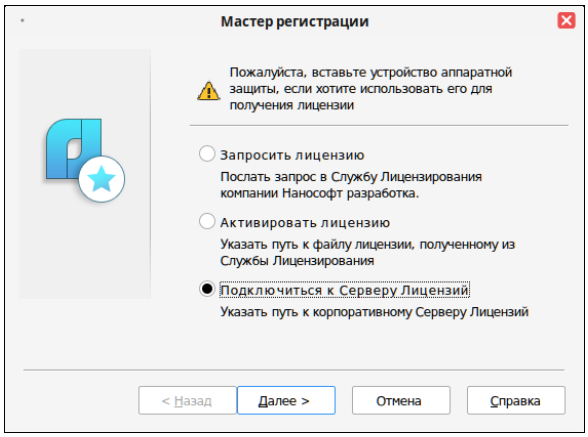
```
systemctl status ncad-licsrv
```

В случае если все шаги по установке и настройке были выполнены верно, в статусе службы лицензирования будет отображаться **active (running)**.

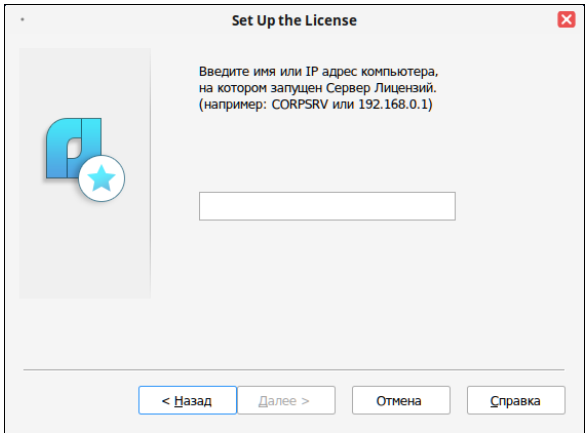
Подключение к серверу лицензий

Для подключения к **Серверу лицензий** с целью активации программного обеспечения *NanoCAD* запустите **Мастер регистрации** из «**Главного меню**» – «**nanocad 24.1**».

В открывшемся окне **Мастера регистрации** программного обеспечения выберите пункт «**Подключиться к серверу лицензий**» и нажмите **Далее**.

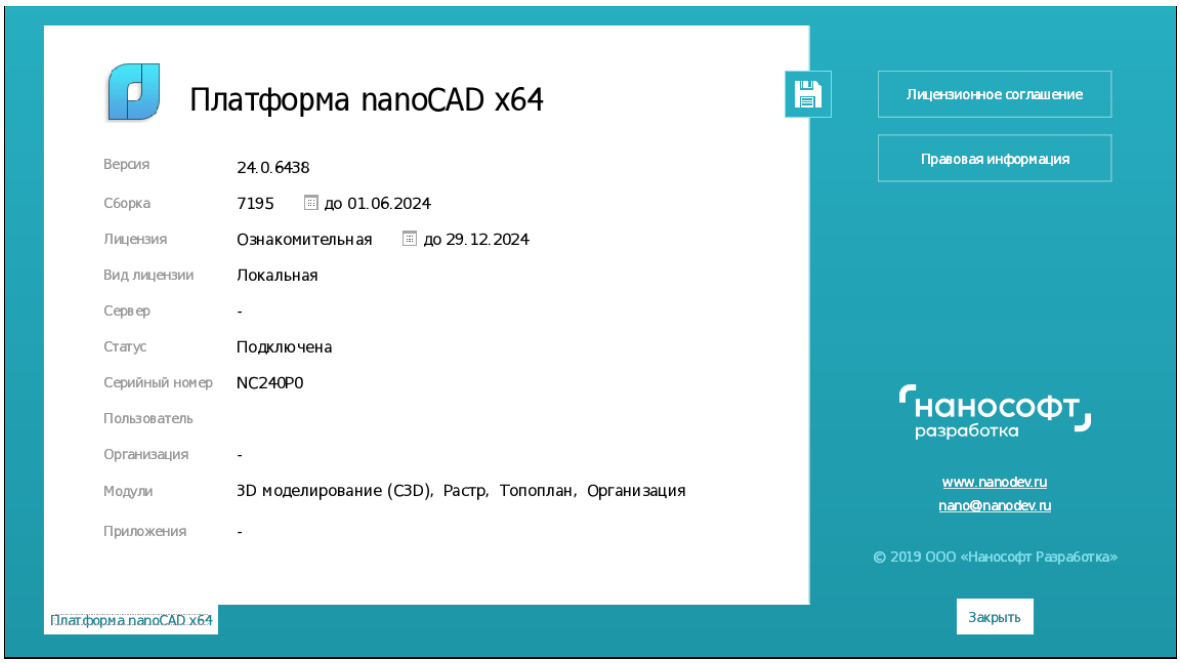


На следующем шаге введите IP-адрес компьютера, на котором установлен **Сервер лицензий** (например, *192.168.0.1*), или укажите NetBIOS-имя машины (например, *CORPSRV*). Если для подключений используются нестандартные порты, укажите запись следующего вида `<порт>@<имя_сервера>` (например, *270010@CORPSRV*).



Состояние лицензии

Уточнить информацию о состоянии имеющейся лицензии можно в меню «**Справка**» – «**О программе**».



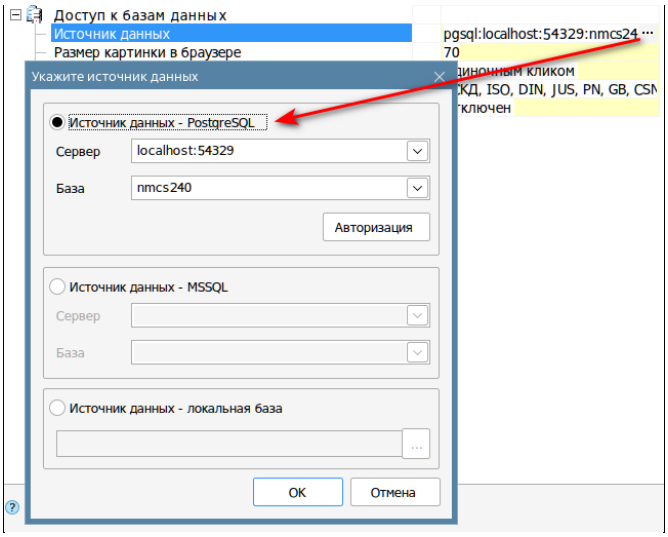
Проверка подключения к локальным базам данных PostgreSQL СПДС и Механика

Для проверки подключения запустите модуль из «**Главного меню**» – «**nanoCAD 24.1**» – «**Механика 24.1**».

В командной строке выполните:

```
params
```

Перейдите в раздел **Источник данных** и настройте локальную БД.



где:

- localhost:54329 – сервер БД:
  - localhost – имя сервера (в примере – локальный сервер);
  - 54329 – номер порта, на котором работает БД;
- имя БД:
  - nmcs240 – имя БД (для модуля Механика);
  - nspds240 – имя БД (для модуля СПДС).

Для авторизации используются следующие данные:

- логин – mclogin;
- пароль – mclogin.

Проверьте доступность порта 54329, т. к. **postgresql** работает на порту 54329:

```
ss -tulpn | grep 54329

tcp   LISTEN   0  244  127.0.0.1:54329   0.0.0.0:*
tcp   LISTEN   0  244      [::1]:54329      [::]:*
```

Для проверки статуса службы БД PostgreSQL выполните:

```
systemctl status ncad-pgsql
```

В статусе должно отображаться **active (running)**.

Установка Сервера лицензий в РЕД ОС конфигурации Сервер минимальный

Предварительная подготовка

1. Убедитесь, что на клиенте используется X11-сервер (*Wayland* или *Xorg*), выполнив команду:

```
echo $XDG_SESSION_TYPE
```

2. На сервере установите и настройте SSH-сервер. Подробную информацию об установке и настройке см. в нашей статье «Работа с клиентом и сервером SSH».

3. На сервере установите **xauth** (потребуются права **администратора**):

```
sudo dnf install xorg-x11-xauth
```

4. На сервере в файле **/etc/ssh/sshd_config** должен быть активен параметр для включения туннелирования X11 при аутентификации – X11Forwarding. Подробную информацию о параметрах конфигурационного файла **/etc/ssh/sshd_config** см. в нашей статье «Конфигурационный файл SSHD_CONFIG».

5. Пользователь, для которого настраивается аутентификация, должен быть включен в группу **wheel** (*sudoers*):

```
usermod -a -G wheel <имя_пользователя>
```

Подключение к серверу

Примечание.

Нижеприведенные действия необходимо выполнять при каждом подключении к серверу.

1. Выполните переподключение к серверу с помощью команды вида:

```
ssh -Y <имя_пользователя>@<IP-адрес_сервера>
```

2. Получите данные авторизации дисплея **X11**:

```
xauth list $DISPLAY
```

3. Авторизуйте дисплей для сессии пользователя:

```
sudo xauth add <вывод_предыдущей_команды>
```

Установка и настройка Сервера лицензий Нанософт

Предварительно загрузите на сервер файл дистрибутива **Сервера лицензий** командой:

```
wget https://download.nanodev.ru/products/nanocad_platform/24.1/ncad-licsrv-11.16.2.132-51+1735141935.el7.x86_64.rpm
```

Для установки Сервера лицензий Нанософт выполните команду (команда выполняется после подключения к серверу по **SSH** с правами **администратора** системы):

```
sudo dnf install ./ncad-licsrv-11.16.2.132-51+1735141935.el7.x86_64.rpm
```

Примечание.

Если служба лицензирования уже запущена, перед добавлением лицензии остановите службу следующей командой (потребуются права **администратора** системы):

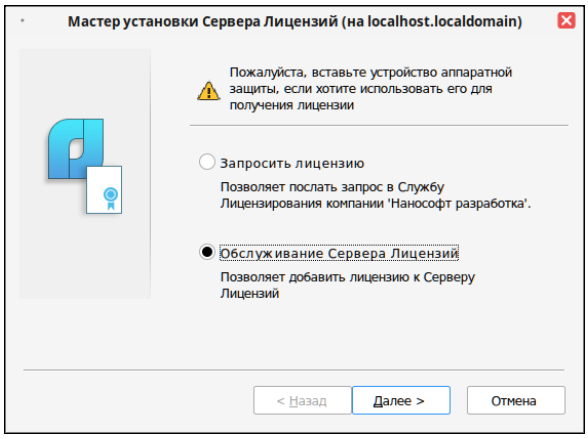
```
sudo systemctl stop ncad-licsrv
```

Если это первый запуск **Мастера установки Сервера лицензий**, пропустите данное предупреждение.

Затем запустите **Мастер установки Сервера Лицензий** с правами **администратора** системы:

```
sudo ncad-licreq
```

Будет открыто окно мастера установки Сервера лицензий:



Дальнейшая настройка и управление **Сервером лицензий** Нанософт осуществляется согласно описанным в разделе «Сервер лицензий» процедурам.

Установка баз данных PostgreSQL СПДС и Механика на сервер

Настройка сервера

На сервере выполните установку **базы данных (БД) модулей Механика и СПДС**, предварительно загрузив пакет с официального сайта разработчика:

```
wget https://download.nanodev.ru/products/nanocad_platform/24.1/ncad-pgsql-12.18-25+1729178738.el7.x86_64.rpm
```

```
sudo dnf install ./ncad-pgsql-12.18-25+1729178738.el7.x86_64.rpm
```

Для настройки подключения **к серверу PostgreSQL** необходимо выполнить следующий алгоритм действий:

1. Разрешить удаленные подключения к серверу. Для этого откройте файл **pg_hba.conf**:

```
sudo nano /opt/nanosoft/postgresql/ncad-database/ncad-data/pg_hba.conf
```

и добавьте в него строку:

```
host all all 0.0.0.0/0 trust
```

2. Разрешить прослушивание запросов на всех IP-адресах (*). Для этого откройте файл **postgresql.conf**:

```
sudo nano /opt/nanosoft/postgresql/ncad-database/ncad-data/postgresql.conf
```

и добавьте в него строку:

```
listen_addresses = '*'
```

3. Для применения настроек перезапустить службу **ncad-pgsql**:

```
sudo systemctl restart ncad-pgsql
```

4. Проверьте статус службы **ncad-pgsql**:

```
sudo systemctl status ncad-pgsql
```

В статусе должно отображаться **active (running)**.

5. Проверить доступность порта 54329, т. к. **postgresql** работает на порту 54329:

```
ss -tulpn | grep 54329

tcp   LISTEN   0  244  127.0.0.1:54329   0.0.0.0:*
tcp   LISTEN   0  244      [::1]:54329      [::]:*
```

Настройка клиента

На клиенте запустите модуль **Механика** из «**Главного меню**» – «**nanoCAD 24.1**».

Перейдите в пункт меню **Механика** – **Настройки** или выполните в командной строке:

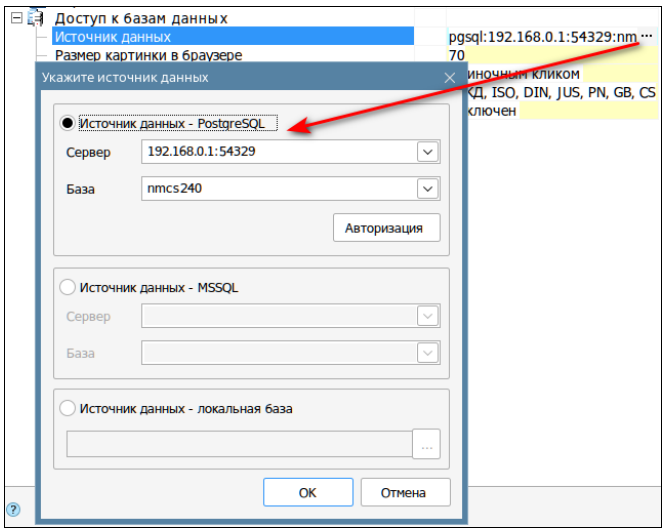
```
mcparams
```

На вкладке «**Главное настройки**» раскройте список «**Доступ к базам данных**» и выберите **Источник данных**.

В разделе **Источник данных** — **PostgreSQL** укажите сервер в формате `<IP-адрес_сервера>:<порт>` и имя базы:

- `nmcs240` – имя БД (для модуля Механика);
- `nspds240` – имя БД (для модуля СПДС).

Для сохранения настроек нажмите **OK**.



Дополнительная информация

В случае возникновения дополнительных вопросов по настройке платформы **NanoCAD** рекомендуется обращаться к официальной документации разработчика продукта, задав на странице загрузок фильтр:

- выберите ОС – **RED OS**;
- выберите версию продукта – **24.1**;
- выберите тип файлов – **инструкции**.

FreeCAD

Окружение

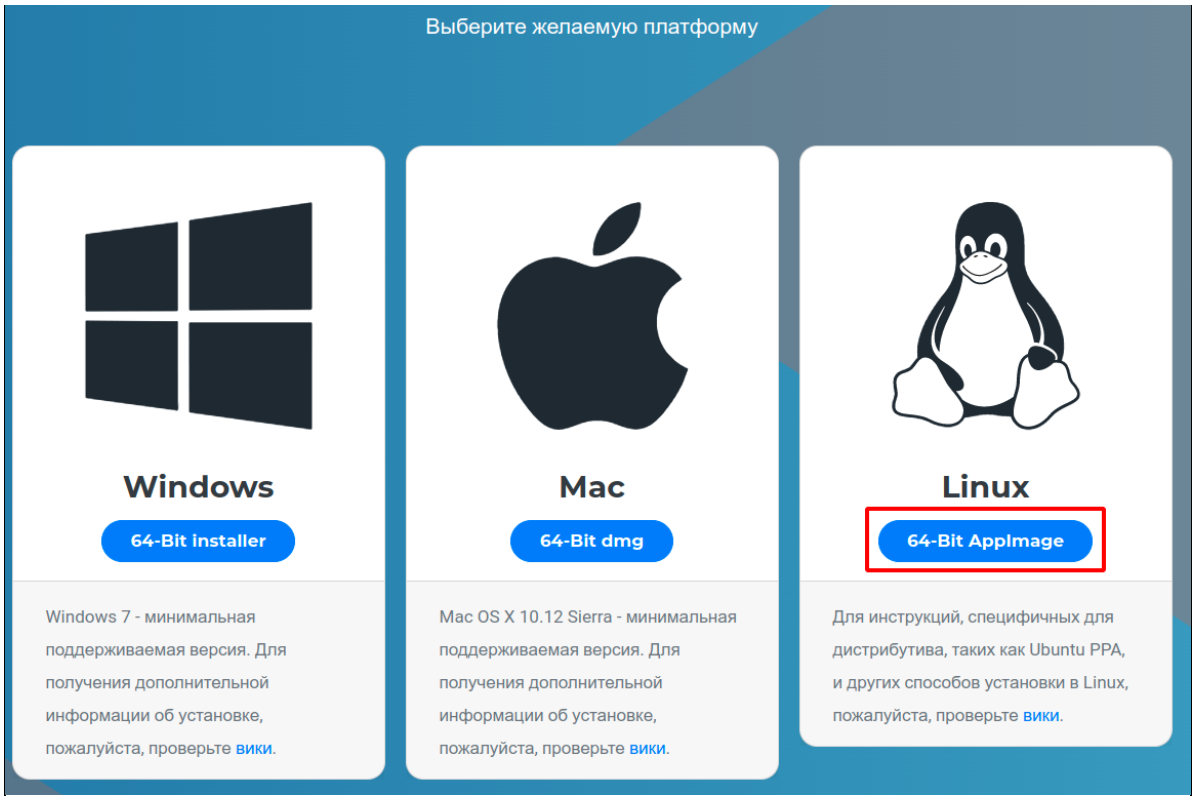
- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** FreeCAD - 0.20.1

FreeCAD - это программа параметрического трёхмерного моделирования, предназначенная прежде всего для проектирования объектов реального мира любого размера.

Параметрическое моделирование позволяет легко изменять дизайн, возвращаясь к истории модели и изменяя её параметры.

Основой геометрического моделирования твёрдых тел в **FreeCAD** является принцип граничного представления, в то же время имеется поддержка полигональных сеток.

Для загрузки **FreeCAD** перейдите на официальный сайт и выберите дистрибутив **64-bit Applimage** для **Linux**.



Перейдите в папку «Загрузки» (в примере /home/user/):

```
cd /home/user/Загрузки/
```

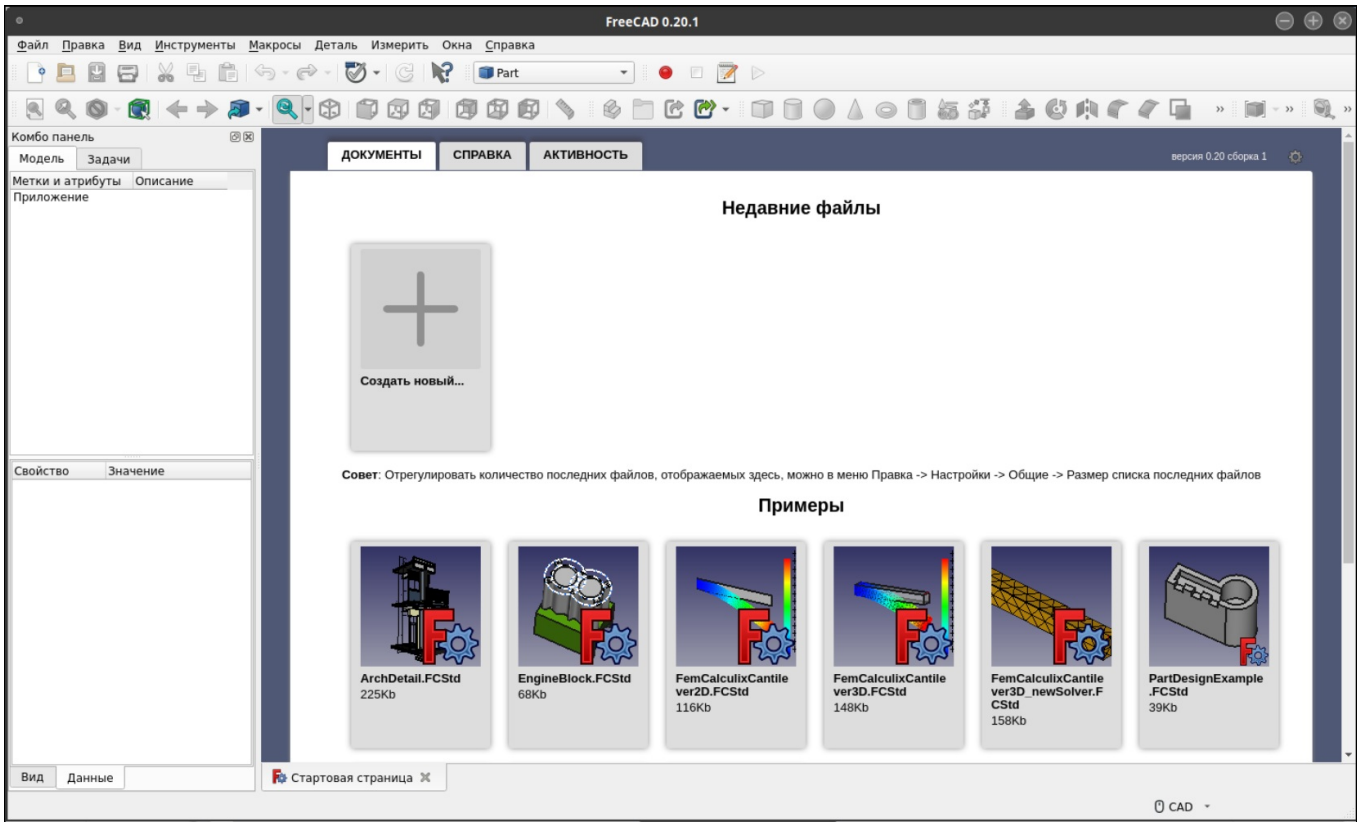
Установите права на запуск:

```
chmod +x FreeCAD_0.20-1-2022-08-20-conda-Linux-x86_64-py310.AppImage
```

После этого программу можно будет запустить двойным кликом по файлу либо командой в терминале от **локального** пользователя:

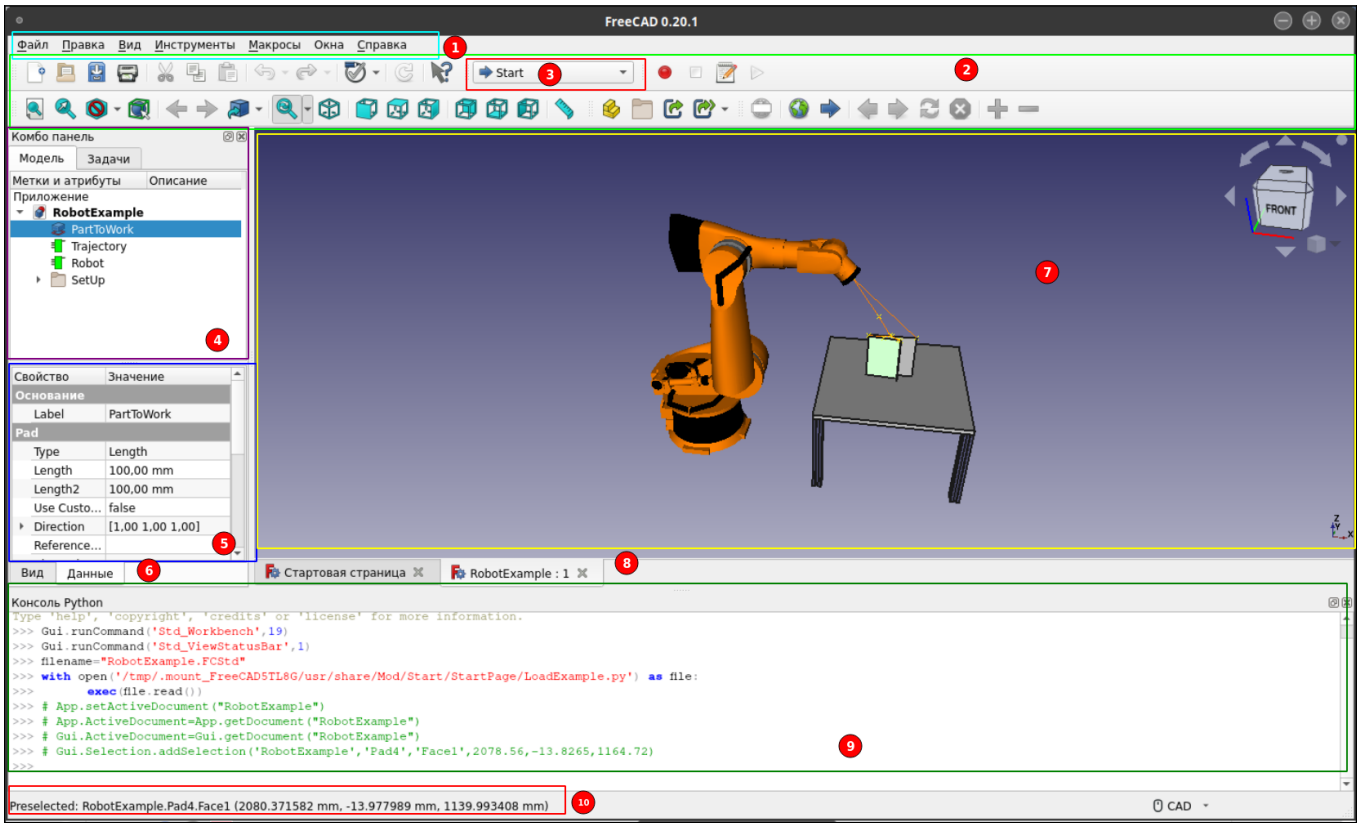
```
./FreeCAD_0.20-1-2022-08-20-conda-Linux-x86_64-py310.AppImage
```

Стартовая страница программы выглядит следующим образом.



Она позволяет вам быстро перейти к одной из наиболее распространенных рабочих сред, открыть один из последних файлов или просмотреть последние новости из мира **FreeCAD**. Вы можете изменить рабочую среду по умолчанию в настройках.

Рассмотрим стандартный интерфейс при работе в программе.



1. Стандартное меню, в котором реализованы основные операции программы.

2. Область панели инструментов, где закреплены панели инструментов.

3. Переключатель **workbench**, в котором вы выбираете активную рабочую среду.

Workbench - это набор инструментов, подходящих для конкретной задачи, такой как работа с сетками, рисование 2D-объектов или ограниченных эскизов. Вы можете переключать текущую рабочую среду с помощью переключателя workbench. Вы можете настроить инструменты, включенные в каждый workbench, добавить инструменты из других workbench или даже самостоятельно созданные инструменты, которые мы называем макросами.

Широко используемыми отправными точками являются **PartDesign Workbench** и **Part Workbench**.

4. Древовидное представление (часть комбинированного представления), показывающее иерархию и историю построения объектов в документе; оно также может отображать панель задач для активных команд

5. Редактор свойств (часть комбинированного представления), который позволяет просматривать и изменять свойства выбранных объектов.

6. Вид выделения, который указывает объекты или подэлементы объектов (вершины, ребра, грани), которые выбраны.

7. 3D-вид, показывающий геометрические объекты в документе.

8. Основная область просмотра, которая может содержать различные окна с вкладками, в основном 3D-вид.

9. Консоль Python, где печатаются все выполняемые команды и где вы можете ввести код Python.

10. Строка состояния, в которой отображаются сообщения некоторых и Остававшиеся подсказки.

КОМПАС-3D

Установка WINE@Etersoft
Установка КОМПАС-3D

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** KOMPAS-3D_v21

КОМПАС-3D – это российская импортонезависимая система трехмерного проектирования.

КОМПАС-3D широко используется для проектирования изделий основного и вспомогательного производств в таких отраслях промышленности, как машиностроение (транспортное, сельскохозяйственное, энергетическое, нефтегазовое, химическое и т.д.), приборостроение, авиастроение, судостроение, станкостроение, вагоностроение, металлургия, промышленное и гражданское строительство, товары народного потребления и т. д.

В настоящее время использование *КОМПАС-3D* возможно в связке с приложением **WINE@Etersoft** от компании Этерсофт. Данный программный продукт обеспечивает полную поддержку работы *КОМПАС-3D* в РЕД ОС.

Вы можете подробнее ознакомиться с настройкой и работой **КОМПАС-3D**, просмотрев наши обучающие видео:

- на **RuTube** — Установка КОМПАС-3D в РЕД ОС 7.3;
- в **Яндекс.Дзен** — Установка КОМПАС-3D в РЕД ОС 7.3;
- в **VK Видео** — Установка КОМПАС-3D в РЕД ОС 7.3.

На наших каналах вы также сможете найти много другой полезной информации.

Установка WINE@Etersoft

Программный продукт *WINE@Etersoft* позволяет использовать Windows-приложения в операционных системах семейства GNU/Linux.

Продукт *WINE@Etersoft* основан на коде свободного проекта **Wine**. Компания *Etersoft* занимается доработкой *Wine*, чтобы обеспечить полноценную работу в Linux наиболее востребованных в России приложений для бизнеса.

Для установки *WINE@Etersoft* необходимо запросить дистрибутив с официального сайта разработчика. Продукт представлен в двух версиях — **Enterprise** (для корпоративных клиентов) и **Local** (для частного использования).

После запроса продукта на электронную почту будет отправлено письмо с указанием индивидуальных ссылок для скачивания установочных пакетов. Найдите ссылку для скачивания скрипта установки **wine-etersoft-install.sh** и загрузите его на компьютер.

После загрузки откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

Перейдите в каталог со скачанным скриптом установки (в примере **/home/user/Загрузки/**) программы и запустите установку:

```
cd /home/user/Загрузки/
bash wine-etersoft-install.sh
```

Скрипт автоматически установит все необходимые для работы пакеты.

После установки *WINE@Etersoft* выйдите из сеанса суперпользователя:

```
exit
```

Установка КОМПАС-3D

Для установки *КОМПАС-3D* необходимо запросить дистрибутив на официальном сайте разработчика. Для ознакомления с программным обеспечением доступно использование бесплатной пробной версии, работающей без ограничения функционала в течение 30 дней.

После запроса продукта на электронную почту будет отправлено письмо с указанием индивидуальной ссылки для скачивания архива.

После загрузки архива распакуйте его командой в терминале (в примере **/home/user/Загрузки/**):

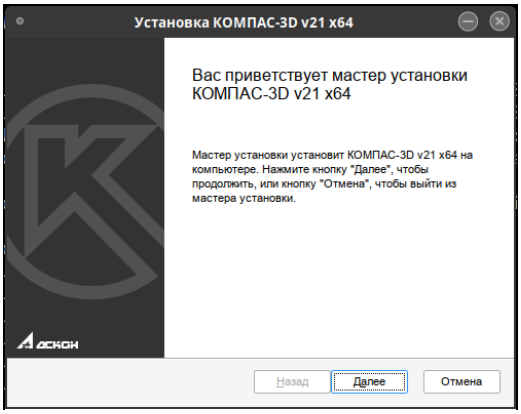
```
unzip -d /home/user/Загрузки/KOMPAS-3D_v21_x64.zip
```

Когда архив будет распакован, перейдите в каталог с дистрибутивом *КОМПАС-3D* и выполните команду (с правами **локального пользователя**):

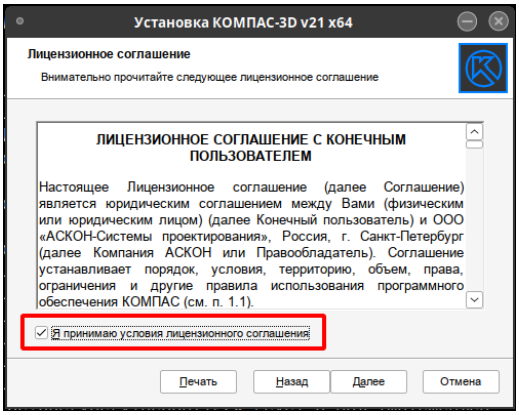
```
cd /home/user/Загрузки/KOMPAS-3D_v21_x64
wine_install_kompas
```

Будет запущен скрипт подготовки окружения для работы ПО, а затем мастер установки.

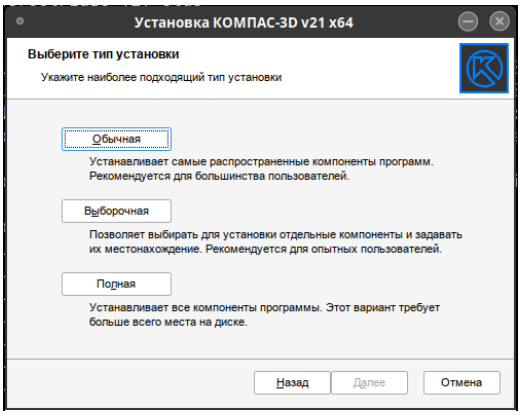
В приветственном окне нажмите «**Далее**».



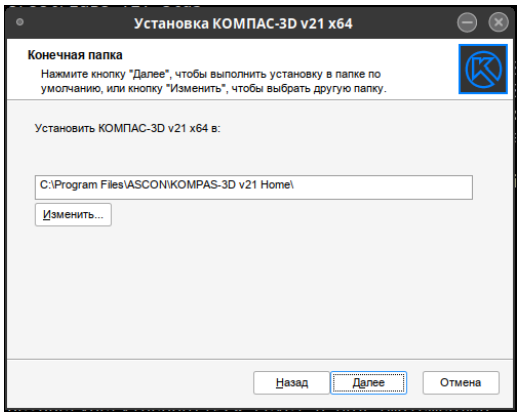
Ознакомьтесь и примите условия лицензионного соглашения, нажмите «**Далее**».



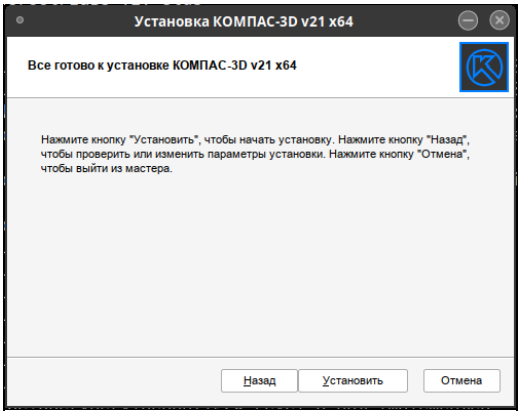
Выберите тип установки.



Выберите папку для установки программы (в примере оставлена папка по умолчанию), нажмите «**Далее**».

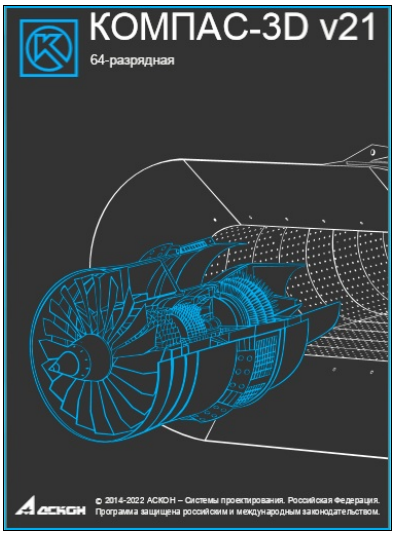


Подтвердите начало установки, нажав кнопку «**Установить**».

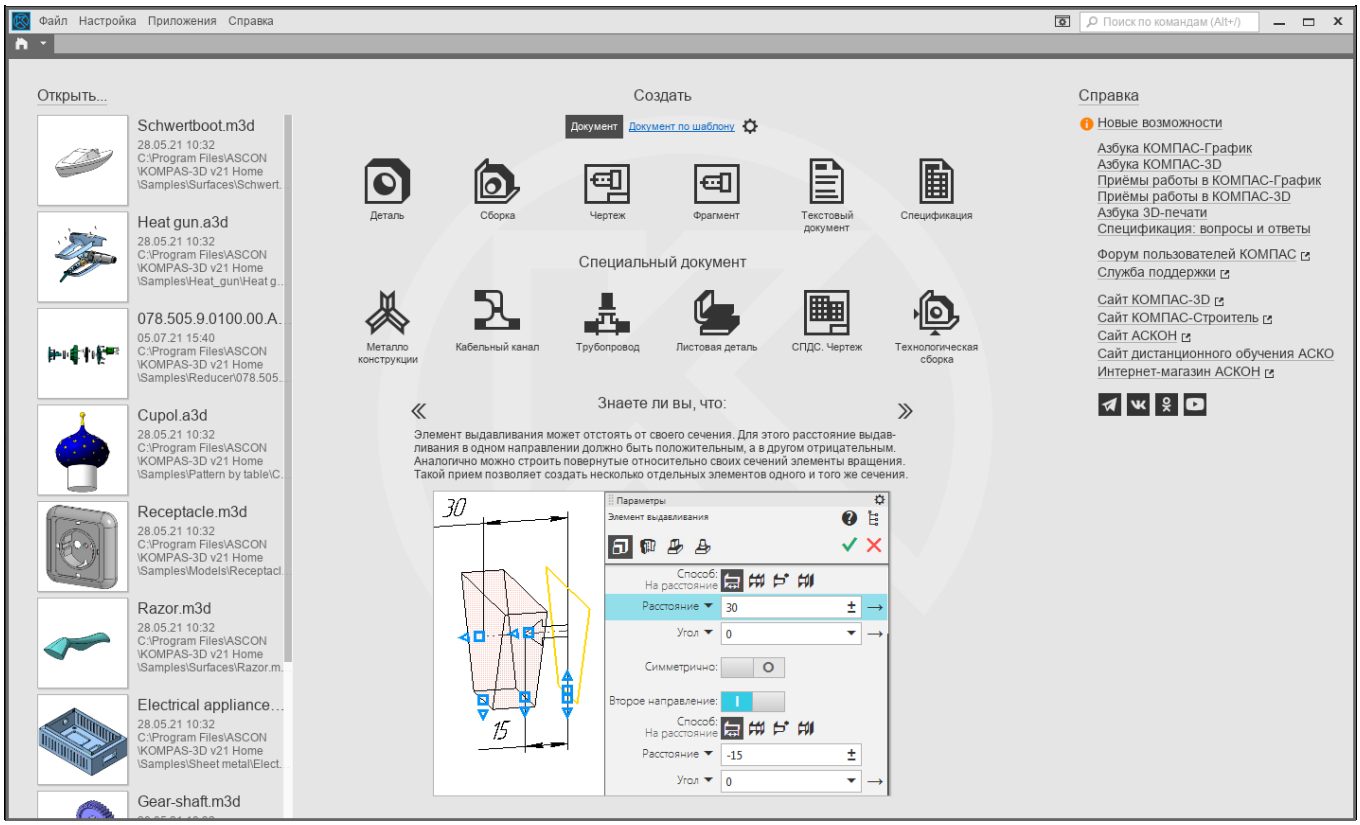


После установки ПО будет доступно из «**Главного меню**» - «**Wine**» - «**КОМПАС-3D v21**», а также появится ярлык на **Рабочем столе**.

Запуск программы выглядит следующим образом:



Главное окно программы выглядит следующим образом:


Файл Настройка Приложения Справка
Поиск по командам (Alt+/)
Открыть...
Schwertboot.m3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Surfaces\Schwert...
Heat gun.a3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Heat_gun\Heat g...
078.505.9.0100.00.A...
05.07.21 15:40
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Reducer\078.505...
Cupol.a3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Pattern by table\C...
Receptacle.m3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Models\Receptacl...
Razor.m3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Surfaces\Razor.m...
Electrical appliance...
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Sheet metal\Elect...
Gear-shaft.m3d
Создать
Документ
Документ по шаблону
Деталь
Сборка
Чертеж
Фрагмент
Текстовый документ
Спецификация
Специальный документ
Металло конструкции
Кабельный канал
Трубопровод
Листовая деталь
СПДС. Чертеж
Технологическая сборка
Знаете ли вы, что:
Элемент выдавливания может отстоять от своего сечения. Для этого расстояние выдавливания в одном направлении должно быть положительным, а в другом отрицательным. Аналогично можно строить повернутые относительно своих сечений элементы вращения. Такой прием позволяет создать несколько отдельных элементов одного и того же сечения.
30
15
Параметры
Элемент выдавливания
Способ:
На расстояние
Расстояние
30
Угол
0
Симметрично:
Второе направление:
Способ:
На расстояние
Расстояние
-15
Угол
0
Справка
Новые возможности
Азбука КОМПАС-График
Азбука КОМПАС-3D
Приёмы работы в КОМПАС-График
Приёмы работы в КОМПАС-3D
Азбука 3D-печати
Спецификация: вопросы и ответы
Форум пользователей КОМПАС
Служба поддержки
Сайт КОМПАС-3D
Сайт КОМПАС-Строитель
Сайт АСКОН
Сайт дистанционного обучения АСКО
Интернет-магазин АСКОН

Marble — виртуальный глобус

Основные функции
Установка
Описание программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: marble-19.08.3-1

Marble — это удобное программное обеспечение, представляющее виртуальный глобус, который позволяет масштабировать карту и исследовать Землю или Луну с разных позиций.

Marble предлагает огромное количество возможностей для исследования различных географических объектов, таких как горы, реки, океаны и т.д. Также пользователи могут путешествовать по различным планетам, изучая их поверхность и географию.

Основные функции

Основные функции **marble** включают:

1. **Просмотр карт —** marble предоставляет возможность просмотра и исследования различных видов карт, включая физическую карту, политическую карту, облачную карту и другие;

2. **Интерактивность** — пользователи могут вращать глобус, изменять масштаб и перемещаться по карте, что делает процесс обучения более интересным и наглядным;

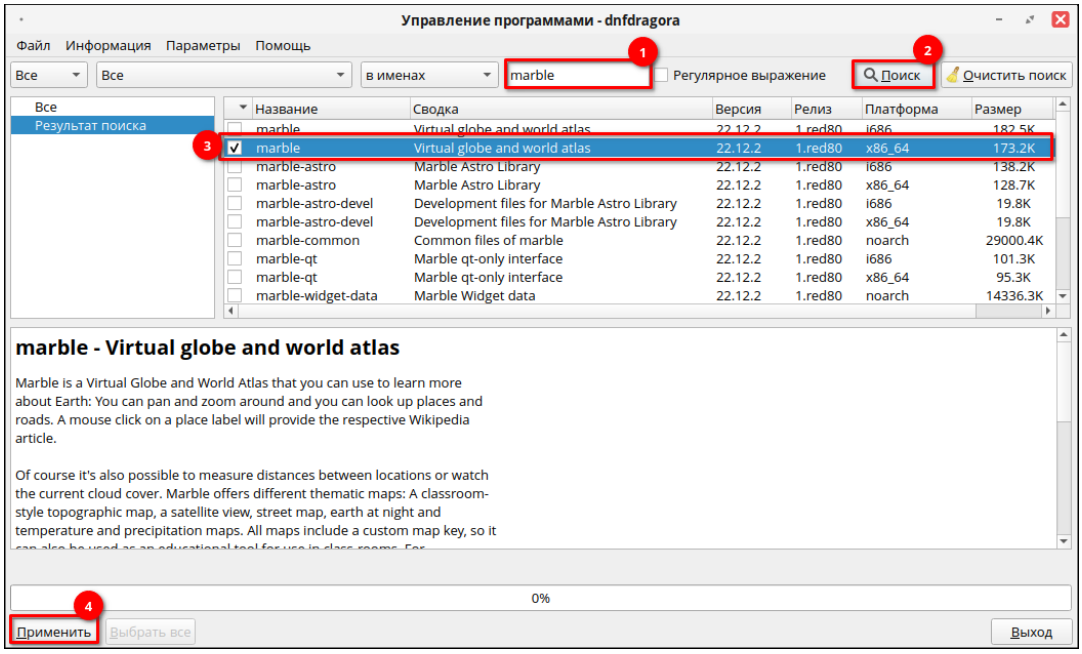
3 . **3D-моделирование —** marble использует технологию 3D-моделирования для создания высококачественных изображений поверхности планет, спутников и других небесных объектов;

4. **Информацию о географических объектах —** marble предлагает подробную информацию о различных географических объектах, таких как горы, океаны, реки, столицы и многое другое.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**marble**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install marble
```

После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**KDE Marble**».

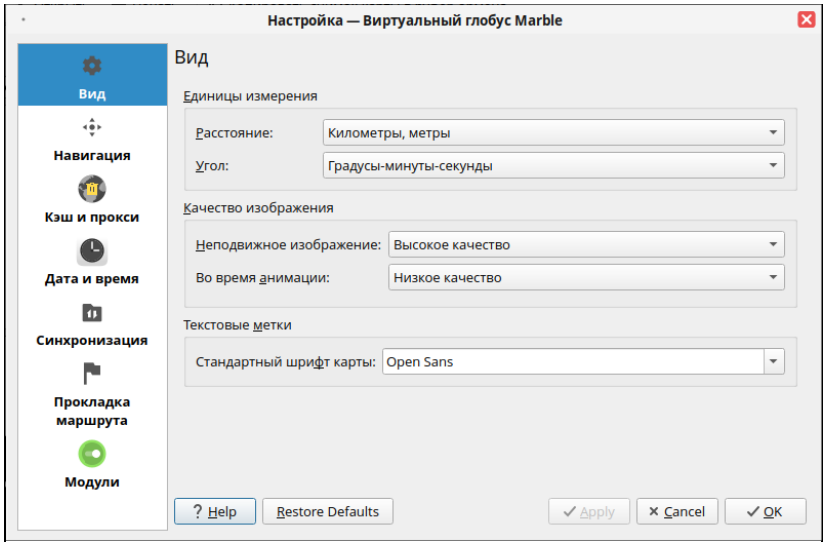
Описание программы

Интерфейс программы стандартный и состоит из нескольких типовых частей.



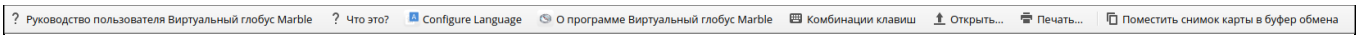
1. **Основное меню программы.** Позволяет выполнять различные действия с картой, а также настраивать как саму программу, так и панель инструментов.

Одним из наиболее важных пунктов является «**Настройка**» — «**Настроить Виртуальный глобус Marble...**», который позволяет настраивать внешний вид глобуса и его основные параметры, чтобы оптимизировать визуализацию и функциональность глобуса.

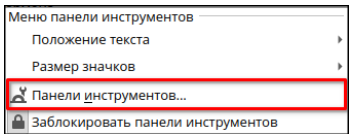


В пункте меню «**Справка**» — «**Руководство пользователя Виртуальный глобус Marble**» можно ознакомиться с более подробной пользовательской инструкцией.

2. **Основная панель инструментов.** Это панель инструментов с кнопками быстрого доступа к основным возможностям программы. Содержит кнопки справочной информации о программе, открытия файла, печати, копирования снимка, выбора языка.



Кнопки можно скрывать и отображать через контекстное меню, щёлкнув ПКМ по области панели и выбрав пункт «**Панели инструментов...**»



3. **Панель поиска.** Позволяет искать места и объекты на выбранной карте.

4. **Панель выбора карты.** Даёт возможность выбирать различные карты. По умолчанию marble предлагает 15 вариантов просмотра:

- атлас;
- OpenStreetMap;
- вид со спутника;
- Земля ночью;
- глобус Бехайма 1492 года;
- спутниковая карта Sentinel-2;
- историческая карта 1689 года;
- политическая карта;
- обычная карта;
- осадки в декабре;
- осадки в июле;
- температура в декабре;
- температура в июле;
- векторная карта OSM;
- Луна.

Также есть возможность создать новую карту и загрузить карту.

5. **Основное рабочее поле.** Основная область интерфейса, где отображается карта или глобус.

Для лучшей ориентации в левом нижнем углу рабочего поля находится масштабная линейка.



В правом верхнем углу рабочего поля находится компас.



Для навигации и управления видом возможно использовать инструменты панели навигации в правой части рабочего поля.



Используйте стрелки вправо и влево для вращения Земли вокруг оси и стрелки вверх и вниз для наклона оси Земли назад или вперёд.

Масштабирование производится перемещением ползунка вверх и вниз. В зависимости от масштаба будут отображаться различные детали.

Для возврата к первоначальным настройкам нажмите на значок  .

6. **Строка состояния.** Отображается информация о расположении, высоте, текущем уровне масштаба тайлов, индикатор выполнения загрузки данных карт. Щелчок ПКМ по строке состояния открывает контекстное меню, в котором возможно изменить её внешний вид.

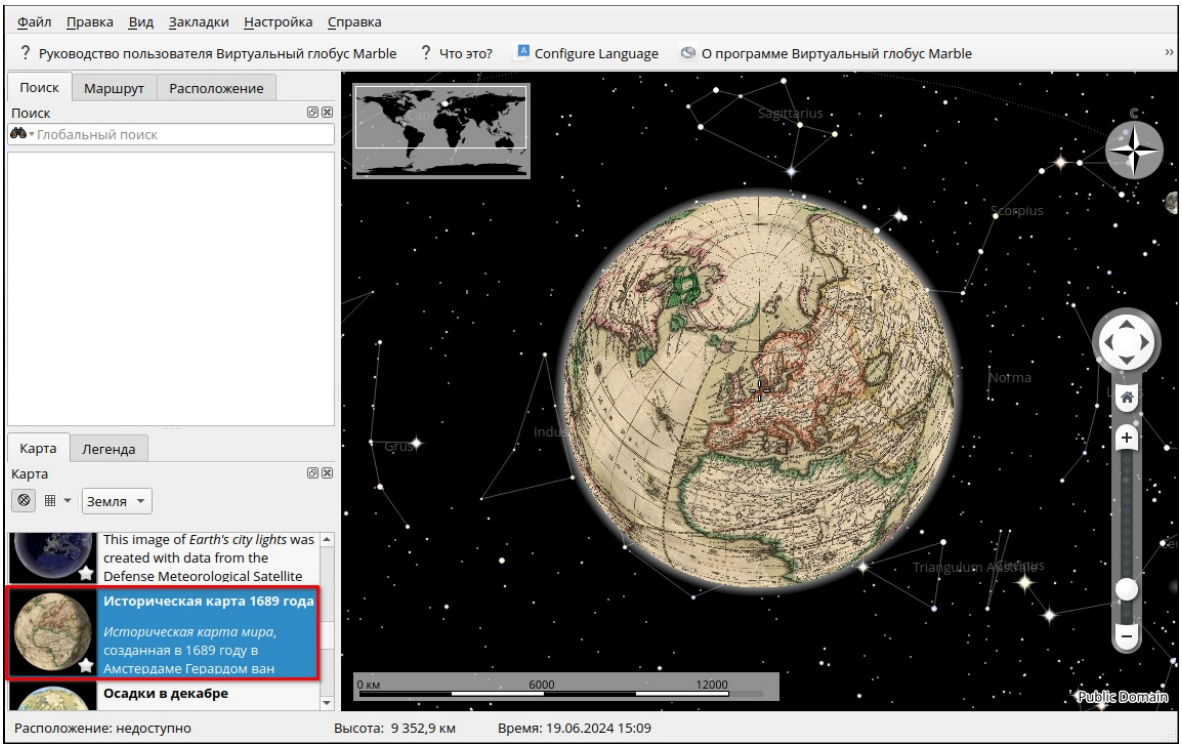
Пример работы

Для поиска информации о географическом объекте воспользуйтесь следующим алгоритмом действий:

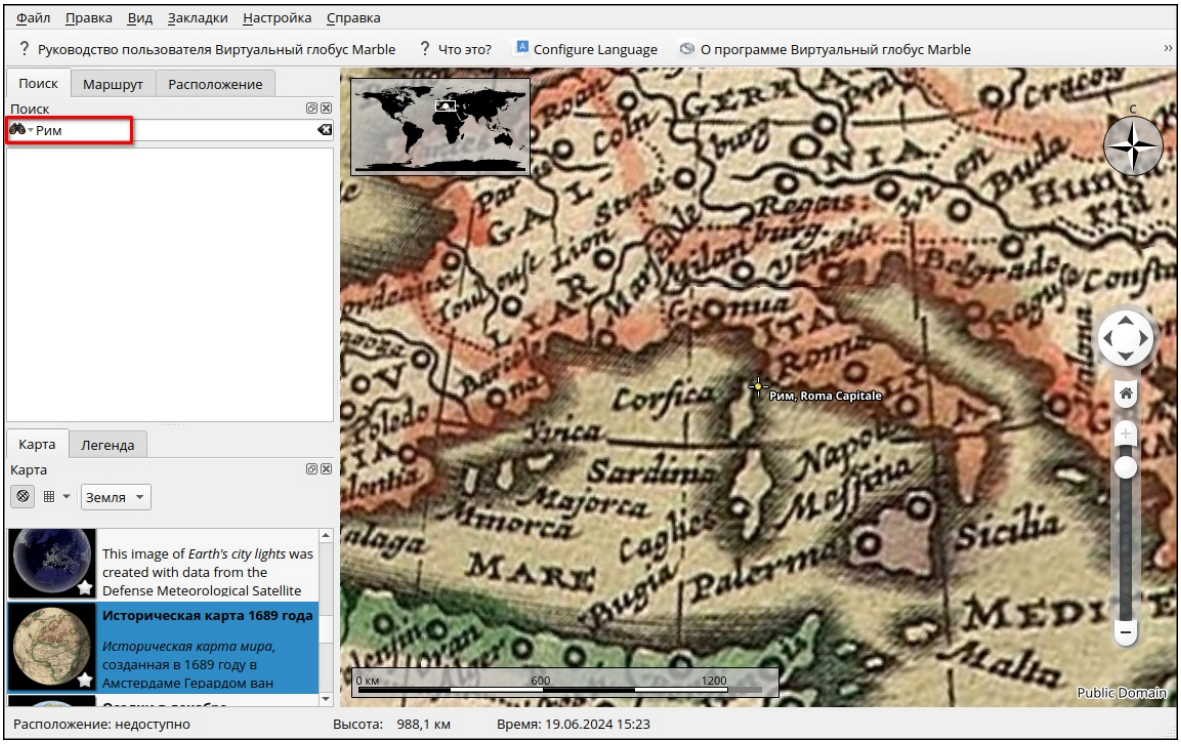
1. На панели выбора карты выберите вид глобуса или выберите режим просмотра, который хотите использовать (например, на плоскости).



2. Выберите карту. Например, историческая карта мира 1689 года.



3. Используйте панель поиска для ввода названия интересующего географического объекта. При нажатии клавиши Enter будет выполнен поиск для вывода более подробной информации.



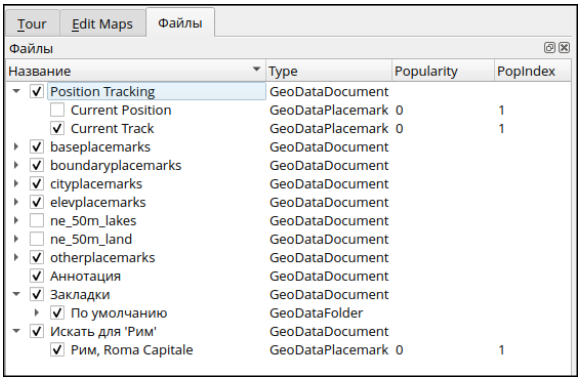
4. После того, как объект найден, используйте мышь или панель инструментов для навигации — увеличения, уменьшения или перемещения по карте.



5. Кликните по объекту, чтобы открыть панель информации, где можно узнать больше о выбранном месте.



6. Активируйте различные слои на панели слоёв, чтобы увидеть дополнительную информацию, такую как погодные условия, физическая география или спутниковые снимки.

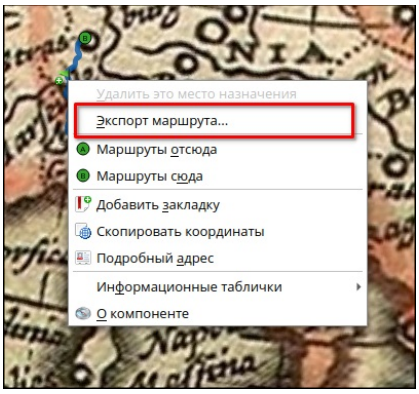


7. Проложите маршрут. Для выбора начальной точки маршрута щёлкните по желаемому местоположению ПКМ и выберите из контекстного меню «**Маршруты отсюда**». Для выбора конечной точки щёлкните по другому местоположению ПКМ и выберите «**Маршруты сюда**».

После выполненных действий маршрут отобразится на карте:



8. Возможно сохранять маршруты в формате **.kml** (Keyhole Markup Language) и загружать их на том же самом или на другом компьютере с установленным приложением Marble. Для сохранения маршрута в файл с расширением **.kml** используйте функцию экспорта маршрута в файл через контекстное меню, щёлкнув ПКМ по маршруту. Открывшийся диалог сохранения позволит указать имя сохраняемого файла.



Система программирования КуМир

Установка
Конфигурации
Описание конфигурации «Кумир»
Исполнитель «Робот»
Установка стартовой обстановки
Окно наблюдения
Ручное управление
Исполнитель «Чертежник»
Исполнитель «Кузнечик»
Описание конфигураций «Кумир для учителей» и «Кумир-Про»
Примеры работы
Пример 1 (вычисление факториала)
Пример 2 (исполнитель «Робот»)
Пример 3 (исполнитель «Чертежник»)
Пример 4 (исполнитель «Кузнечик»)

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kumir2-2.1.0

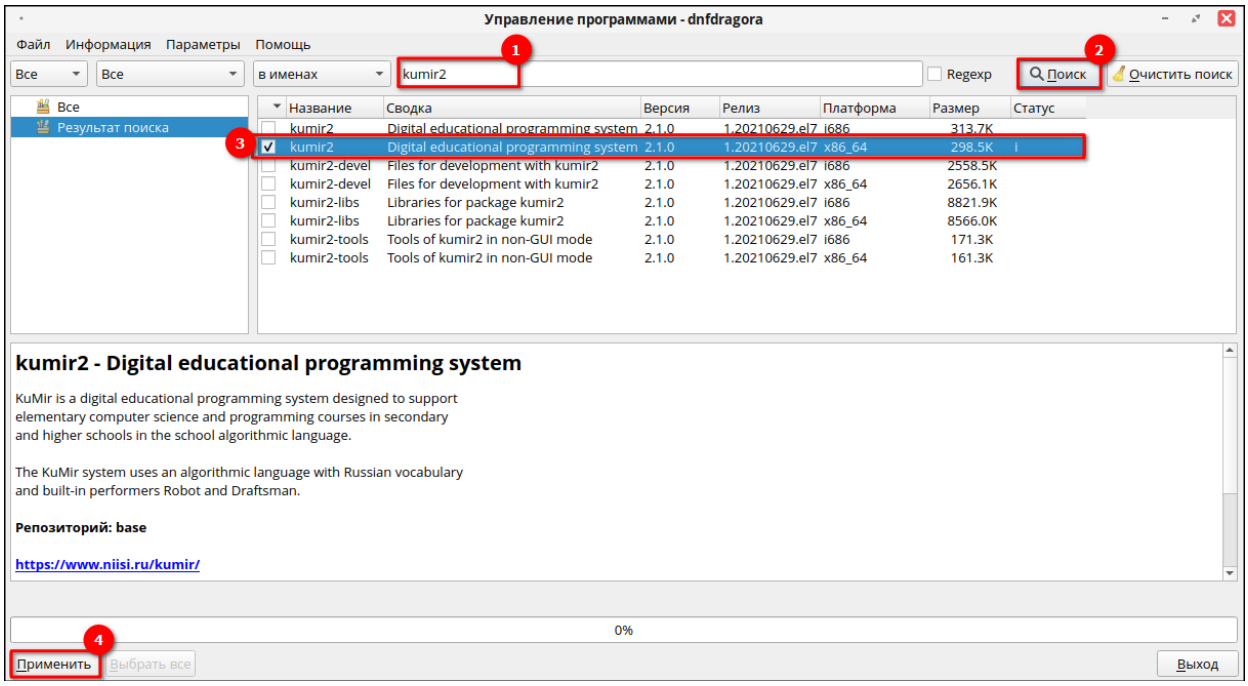
КуМир (Комплект Учебных МИРов) — это цифровая образовательная система программирования, предназначенная для поддержки начальных курсов информатики и программирования в средних и высших школах на школьном алгоритмическом языке.

Система **КуМир** использует алгоритмический язык с русской лексикой и встроенными исполнителями.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kumir2**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



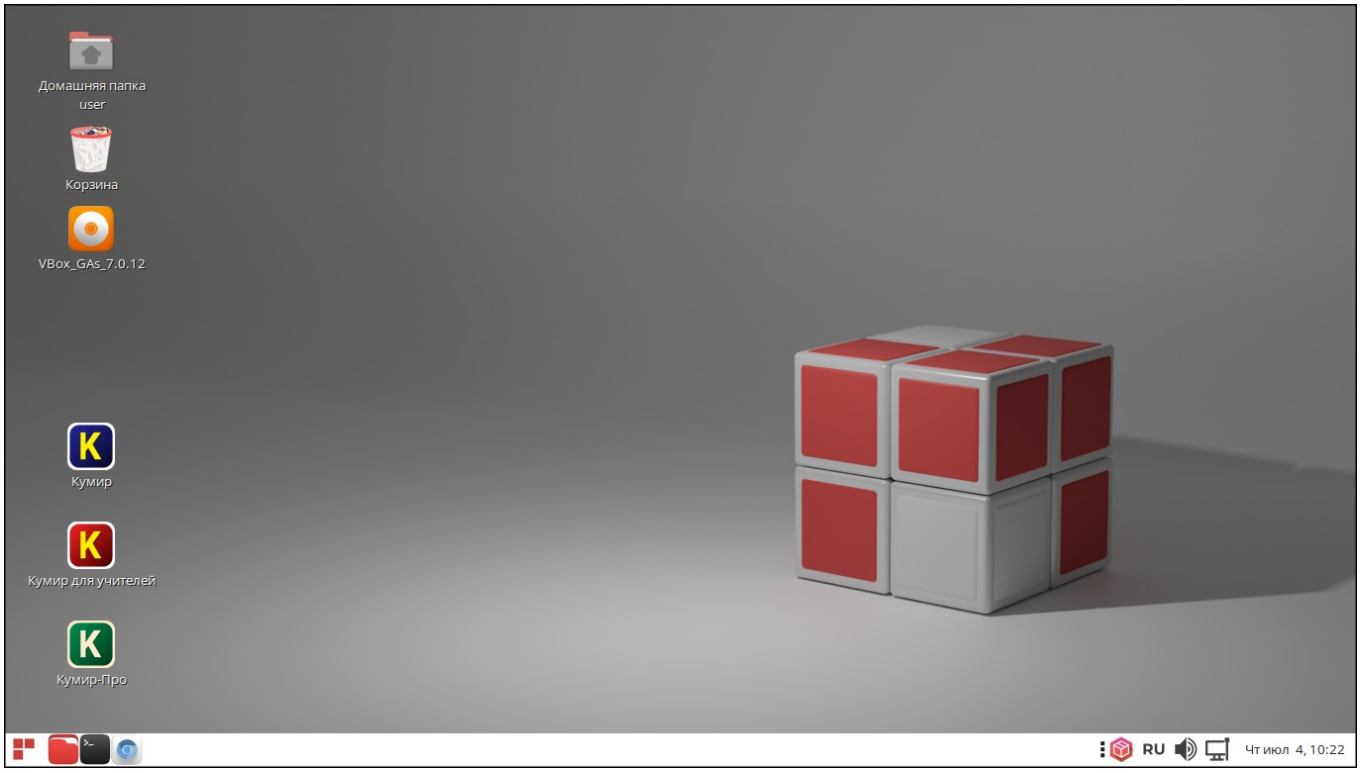
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install kumir2
```

После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**Кумир**» («**Кумир для учителей**»,

«**Кумир-Про**»).

Для размещения значка программы **Кумир** на рабочем столе наведите мышь на программу в «**Главном меню**» и, нажав ПКМ, выберите в контекстном меню «**Поместить на Рабочий стол**». Теперь значок **Кумир** доступен для быстрого запуска.



Конфигурации

Выбор между доступными конфигурациями зависит от целей и задач.

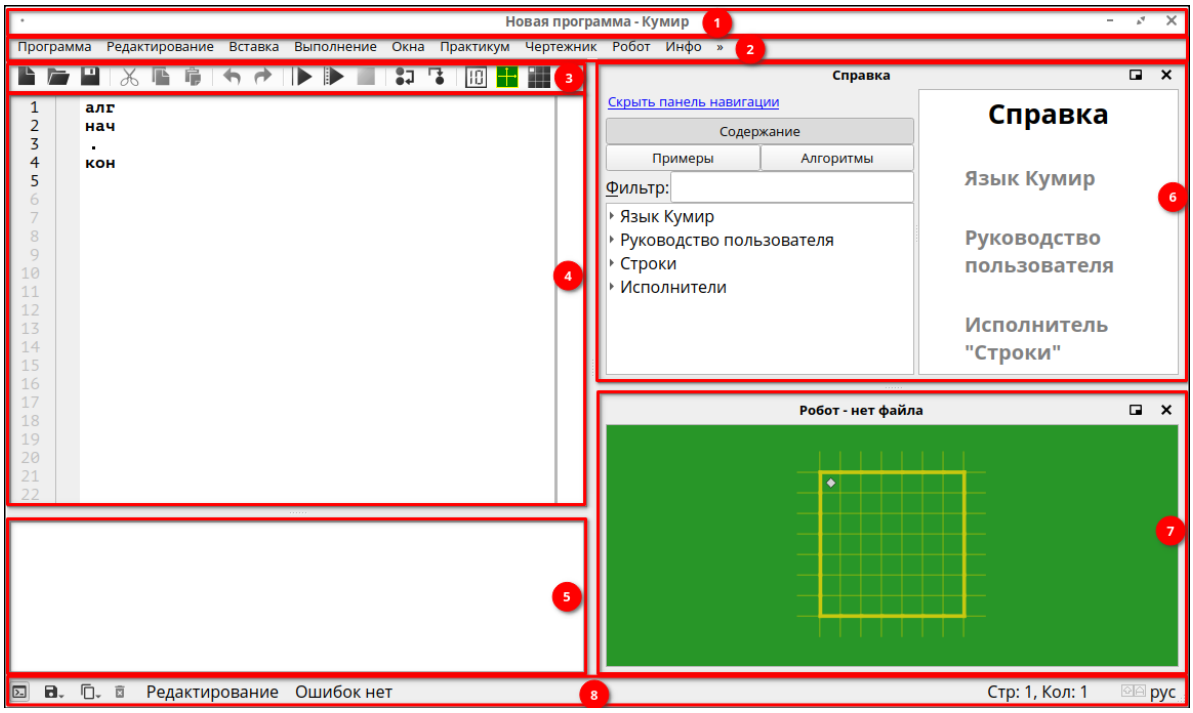
1. Конфигурация «**Кумир**» — предназначена для первичного школьного обучения.

2. Конфигурация «**Кумир для учителей**» — предназначена для подготовки заданий и практикумов.

3. Конфигурация «**Кумир-Про**» — профессиональная версия, предназначенная для более глубокой работы с программированием и разработки сложных проектов.

Описание конфигурации «Кумир»

После запуска программы в конфигурации для учащихся на экране появляется главное окно системы Кумир:



Интерфейс программы стандартный и состоит из нескольких типовых частей.

1. **Системный заголовок главного окна** — отображает название программы.

2. **Главное меню** — содержит семь основных пунктов и несколько дополнительных пунктов.

3. **Панель инструментов** — стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы.

4. **Рабочая область** — область для написания и редактирования кода. Она поддерживает подсветку синтаксиса и имеет номера строк для удобства навигации.

5. **Область ввода-вывода программы** — отображаются результаты выполнения программы, а также можно вводить данные, если программа этого требует.

6. **Справочные руководства** — раздел, где можно найти информацию о языке программирования, функциях системы **Кумир** и примеры кода (Меню «**Инфо**» — «**Справочные руководства**» или горячая клавиша **F1**).

7. **Окно исполнителя** — визуализирует выполнение программы, если она включает графический или анимационный вывод.

8. **Строка состояния** — отображает информацию об ошибках.

Главное меню

Главное меню системы содержит несколько пунктов.

Меню «**Программа**» содержит действия для работы с файлами, имеющими формат ***.kum***. С его помощью можно создать новую программу, новый текст, загрузить, сохранить файлы, закрыть рабочую вкладку.

Меню «**Редактирование**» обеспечивает стандартные средства редактирования текстов, например, ввод символов в режиме вставки или замены, удаление символов, выделение/копирование/вставку/удаление фрагмента текста, отмену/возврат последних действий, поиск по тексту.

Меню «**Вставка**» содержит операции вставки конструкций используемого языка программирования / операции выполнения записанных ранее последовательностей нажатий клавиш.

Элементами меню «**Выполнение**» являются действия по запуску и остановке выполнения текущей программы.

Меню «**Окна**» содержит действия отображения дополнительных окон, которые реализуются исполнителями, отображает или скрывает нижнюю часть главного окна с областью ввода-вывода, отображает дополнительное окно практикума.

Меню «**Практикум**» позволяет загрузить курс, открыть список тетрадей/курсов, запустить проверку заданий, сохранить тетрадь, вернуть исполнителей к исходному состоянию.

Модуль поддержки практикумов позволяет учителю создавать, а ученику выполнять учебные курсы по информатике на базе системы **Кумир**.

Курсы представляют:

- систему заданий, которую должен выполнить ученик;
- методику, которая описывает рекомендованный порядок выполнения заданий.

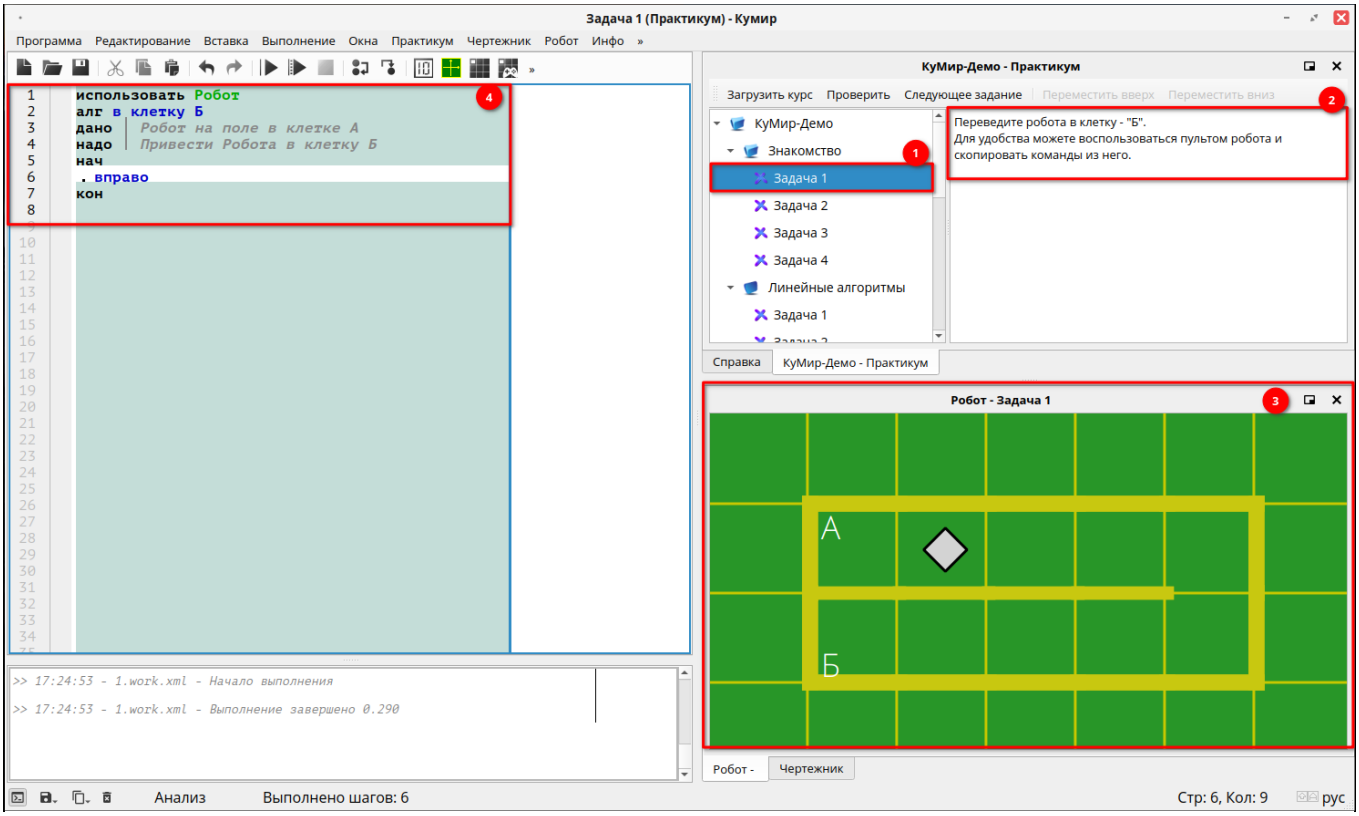
Задание предлагает ученику написать программу. Задание включает в себя:

- текстовое описание задания;
- шаблон программы и, если нужно, обстановку исполнителя;
- программу тестирования, обстановки, используемые при тестировании.

В меню «**Практикум»** ученик выбирает пункт «**Загрузить курс**» или выбирает «**Недавние тетради/курсы...**».

В исходном состоянии ученику доступно только одно действие – загрузить курс. После того, как курс выбран, ученику предлагается создать тетрадь, в которой будут сохраняться результаты его работы. В левой части окна показывается *список заданий* (1).

Ученик поочерёдно выбирает задачу в списке заданий, открывая ветви дерева, нажимая на  . После выбора задачи появляется словесное *описание текущего задания* (2), а в поле программы окна системы **Кумир** устанавливается окно исполнителей (3) и начальный текст программы (4). Результаты выполненных заданий автоматически сохраняются в тетрадь.



Различные исполнители системы Кумир могут иметь свои одноимённые меню, которые располагаются в главном окне между меню «**Практикум**» и «**Инфо**».

В среде программирования **Кумир** существует множество различных исполнителей, каждый из которых предназначен для выполнения определённых задач:

1. Исполнитель «Робот» — выполняет команды по перемещению и манипуляции объектами в лабиринте.

2. Исполнитель «Чертежник» — рисует геометрические фигуры и линии на плоскости.

3. Исполнитель «Кузнечик» — перемещается по клетчатому полю, прыгая через заданное количество клеток.

4. Исполнитель «Вертун» — вращается вокруг своей оси и выполняет команды, связанные с поворотами.

5. Исполнитель «Клавиатура» — обрабатывает ввод с клавиатуры и выполняет команды на основе введённых данных.

6. Исполнитель «Водолей» — перемещает воду между сосудами, выполняя задачи по переливанию.

7. Исполнитель «Рисователь» — создаёт рисунки и изображения на экране.

8. Исполнитель «Черепаха» — рисует линии и фигуры, перемещаясь по экрану.

Меню «**Инфо**» (сокращение от «Информация») содержит элементы, вызов которых приводит к отображению информационных окон.

Панель инструментов

Сверху от редактора находится панель инструментов, которая дублирует часто используемые действия главного меню:

 — создаёт новый файл программы;

 — открывает существующий файл программы;

 — сохраняет текущий файл программы;

 — удаляет выделенный текст и помещает его в буфер обмена;

 — копирует выделенный текст в буфер обмена;

 — вставляет текст из буфера обмена в текущее место курсора;

 — отменяет последнее изменение в тексте программы;

 — повторяет последнее отменённое изменение;

 — выполняет программу без отображения дополнительной информации на полях;

 — запускает выполнение программы в обычном режиме;

 — прерывает выполнение программы;

 — выполняет один шаг программы;

 — выполняет программу шаг за шагом;

 — открывает окно с заданиями и упражнениями;

 — запускает исполнителя «Чертежник», с помощью которого можно программировать движения виртуального рисовальщика для создания графических изображений;

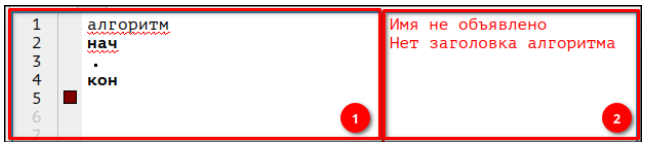
 — запускает исполнителя «Робот», позволяет программировать виртуального робота;

 — открывает пульт управления Роботом, что даёт возможность управлять роботом в режиме реального времени, а не через предварительно написанный код;

 — открывает окно, в котором можно выбрать, какие кнопки показывать в строке, а какие — скрыть.

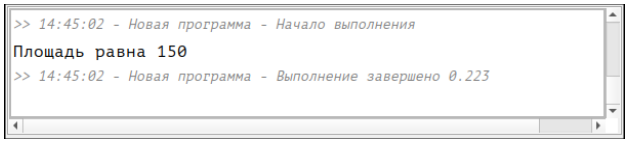
Рабочая область

Рабочая область программы делится на две части: *область редактирования текста программы* (1) и *поле редактора* (2).



Область ввода-вывода программы

Область ввода/вывода автоматически появляется при выполнении операторов или во время выполнения программы. Она может быть полностью скрыта.



Справочные руководства

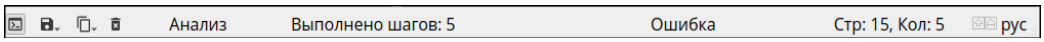
Справочные руководства представляют собой документацию, которая помогает пользователям понять основы работы с программой, её функции и язык программирования. Руководства содержат примеры кода, объяснения команд и методики решения типичных задач.

Окно исполнителя

В окне исполнителя отображается процесс выполнения программы. Здесь пользователи могут наблюдать за выполнением команд и взаимодействием программы с виртуальными объектами, такими как «**Чертежник**» или «**Робот**».

Строка состояния

Строка состояния отображает информацию о текущем состоянии программы, данные о номере выполняемой строки, статусе исполнения и сообщения об ошибках. Это помогает пользователям отслеживать процесс выполнения программы и быстро находить и исправлять ошибки.



В левой части строки состояния находятся следующие кнопки:

 – отображает область ввода/вывода;

 – отображает всплывающее меню сохранения содержимого окна ввода-вывода;

 – отображает всплывающее меню копирования содержимого окна ввода-вывода в буфер обмена;

 – эта кнопка становится доступной только при наличии текста в области ввода-вывода, её нажатие приводит к очистке данной области.

Исполнитель «Робот»

Среда исполнителя «**Робот**» — прямоугольное клетчатое поле, между клетками которого могут стоять стены. Окно «**Робота**» выглядит следующим образом:



Робот находится в **текущей обстановке**, которая изменяется при выполнении команд Робота. Выполнение программы начинается со **стартовой обстановки**.

Обстановка «**Робота**» представляет собой прямоугольное поле, окружённое забором и разбитое на клетки.

Обстановка описывается следующими величинами:

- размеры обстановки — количество строк (1–128) и количество столбцов (1–255);
- характеристики каждой клетки:
    - наличие стен вокруг клетки;
    - признак закрашенности;
    - уровень радиации (может принимать любое вещественное значение от 0 до 99 у. е.);
    - температура (может принимать любое целое значение от -273 до +233 градусах Цельсия).

«**Робот**» изображается в клетке  . «**Робот**» может измерить температуру и радиацию, но не может распознать символы в клетках. Для изменения масштаба изображения окружающей обстановки перейдите в окно наблюдения за «**Роботом**» и используйте колёсико мыши.

Команды исполнителя Робот

Основными командами исполнителя «**Робот**» являются:

- **стартовая команда** — программа, управляющая «Роботом», должна начинаться со строки `использовать «Робот»`. При выполнении этой строки **Кумир** помещает «Робота» в стартовую обстановку.
- **команды-действия** — влево, вправо, вверх, вниз, закрасить;

  Пример:

```
использовать Робот
 алг
 нач
 вправо
```

```
 вниз
 влево
 вверх
 закрасить
кон
```

- **команды проверки условий** — сверху стена/свободно, снизу стена/свободно, слева стена/свободно, справа стена/свободно, закрашена, чистая;

  Пример:

```
алг лог справа стена
```

- **команды измерения** — измеряет температуру, радиацию в клетке, где находится «Робот».

  Пример:

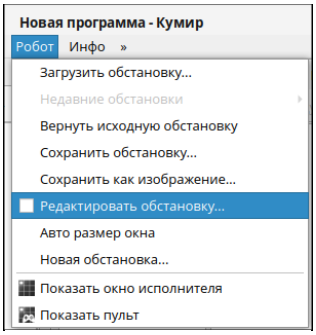
```
алг вещ радиация
 алг вещ температура
```

Исполнитель «**Робот**» двигается по клеткам. Получая простую команду, «**Робот**» выполняет движение на одну клетку и ждёт следующей команды.

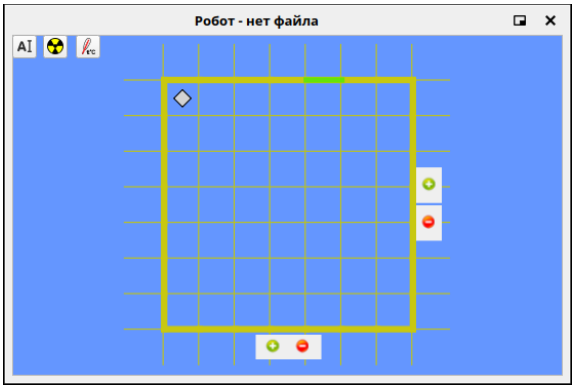
С принципами работы остальных исполнителей можно ознакомиться в меню «**Инфо**» — «**Справочные руководства**».

Установка стартовой обстановки

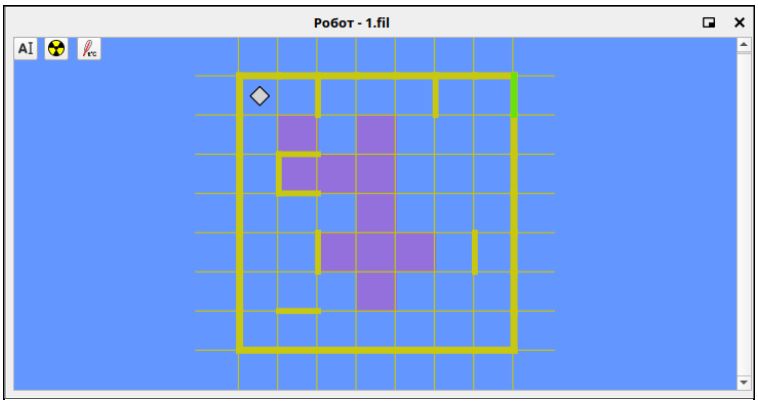
В системе **Кумир** есть средства, с помощью которых можно задать нужную стартовую обстановку. Для этого откройте меню « **Робот**» — «**Редактировать обстановку...**».



Диалоговое окно обстановки «**Робот**» становится синего цвета, также появляются кнопки управления, с помощью которых можно добавить или убрать клетки поля.

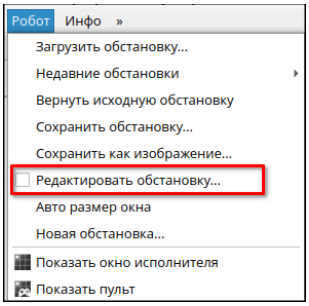


Затем, щёлкая ЛКМ, выставите препятствия для «**Робота**» или закрасьте клетки.



Для сохранения обстановки перейдите в меню «**Робот**» — «**Сохранить обстановку...**». В открывшемся диалоговом окне задайте параметры сохранения файла и сохраните его.

Для выхода из режима редактирования перейдите в меню «**Робот**» и снимите флаг с пункта «**Редактировать обстановку...**».



Для загрузки обстановки перейдите в меню «**Робот**» — «**Загрузить обстановку...**». Нажмите «**Open**».

Окно наблюдения

Окно наблюдения за «Роботом» создаётся в момент начала сеанса работы системы **Кумир** и доступно до окончания сеанса. Во время сеанса работы окно может находиться в одном из двух состояний — видимо или скрыто.

Для отображения окна наблюдения можно нажать на кнопку  или выбрать пункт в меню «**Окна**» — «**Робот**».

Окно наблюдения появится автоматически при запуске программы, содержащей команду:

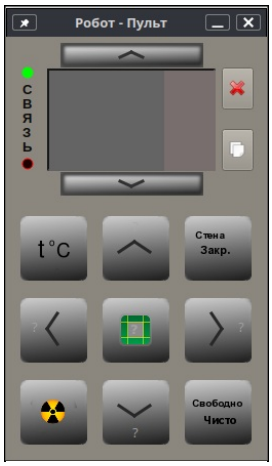
```
использовать Робот
```

Окно наблюдения за «Роботом» может находится в двух режимах:

- **обычном** – применяется при наблюдении за Роботом во время исполнения программ или управлении с пульта,
- **редактирования** – применяется при редактировании стартовой обстановки Робота.

Ручное управление

Окно пульта ручного управления «Роботом» выглядит следующим образом:



Пульт позволяет вручную управлять «Роботом» – выдавать команды, входящие в систему команд «Робота». Использовать пульт можно в интервал времени, когда выполнение программы приостановлено. Перейти к управлению через пульт можно из меню «**Окна**» — «**Робот-Пульт**» или, нажав на панели инструментов кнопку  .

Исполнитель «Чертежник»

Функции «**Чертежника**» не являются частью языка программирования. Для его использования необходимо в программе явно указать использование данного исполнителя:

```
использовать Чертежник
```

В программе отобразится поле исполнителя:

Команды исполнителя «Чертежник»

Основными командами исполнителя «**Чертежник**» являются:

1. **Опустить перо** — опускает перо и при дальнейшем перемещении оставляет след.

Синтаксис:

```
алг опустить перо
```

2. **Поднять перо** — поднимает перо и при дальнейшем перемещении не оставляет след.

Синтаксис:

```
алг поднять перо
```

3. **Выбрать чернила** — устанавливает цвет чернил (цвет *a*).

Синтаксис:

```
алг выбрать чернила(цвет a)
```

4. Сместиться в точку — смещает перо в заданную точку:

- x — абсцисса точки,
- y — её ордината.

Синтаксис:

```
алг сместиться в точку(вещ x, вещ y)
```

5. **Сместиться на вектор** — смещает перо на вектор (dx, dy). Иными словами, если до выполнения команды перо находилось в точке (x, y), то после её выполнения, оно будет находиться в точке (x + dx, y + dy).

Синтаксис:

```
алг сместиться на вектор(вещ dx, вещ dy)
```

6. **Написать** — пишет строку, растянутую или сжатую до заданной ширины:

- ширина — ширина строки,
- текст — текст строки.

Синтаксис:

```
алг написать(вещ ширина, лит текст)
```

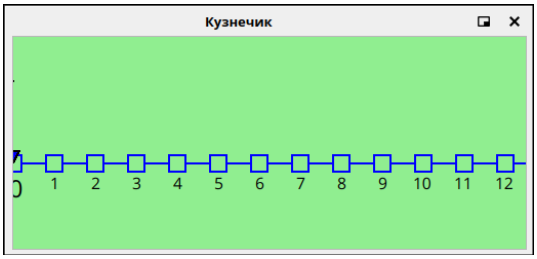
Исполнитель «Кузнечик»

«**Кузнечик**» живёт на числовой прямой и обозначается синим треугольником.

Для использования исполнителя «**Кузнечик**» необходимо в программе явно указать его использование:

```
использовать Кузнечик
```

В программе отобразится поле исполнителя:



Команды исполнителя «Кузнечик»

Основными командами исполнителя «**Кузнечик**» являются:

1. **Вперёд** — сделать прыжок длины **x** вперёд.

Синтаксис:

```
алг вперед x
```

2. **Назад** — сделать прыжок длины **x** назад.

Синтаксис:

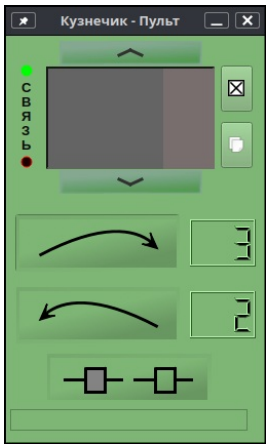
```
алг назад x
```

3. **Перекрасить** — меняет цвет клетки, в которой в данный момент находится «Кузнечик». Если клетка была чистая, закрашивает её. Если закрашена — снимает закраску.

Синтаксис:

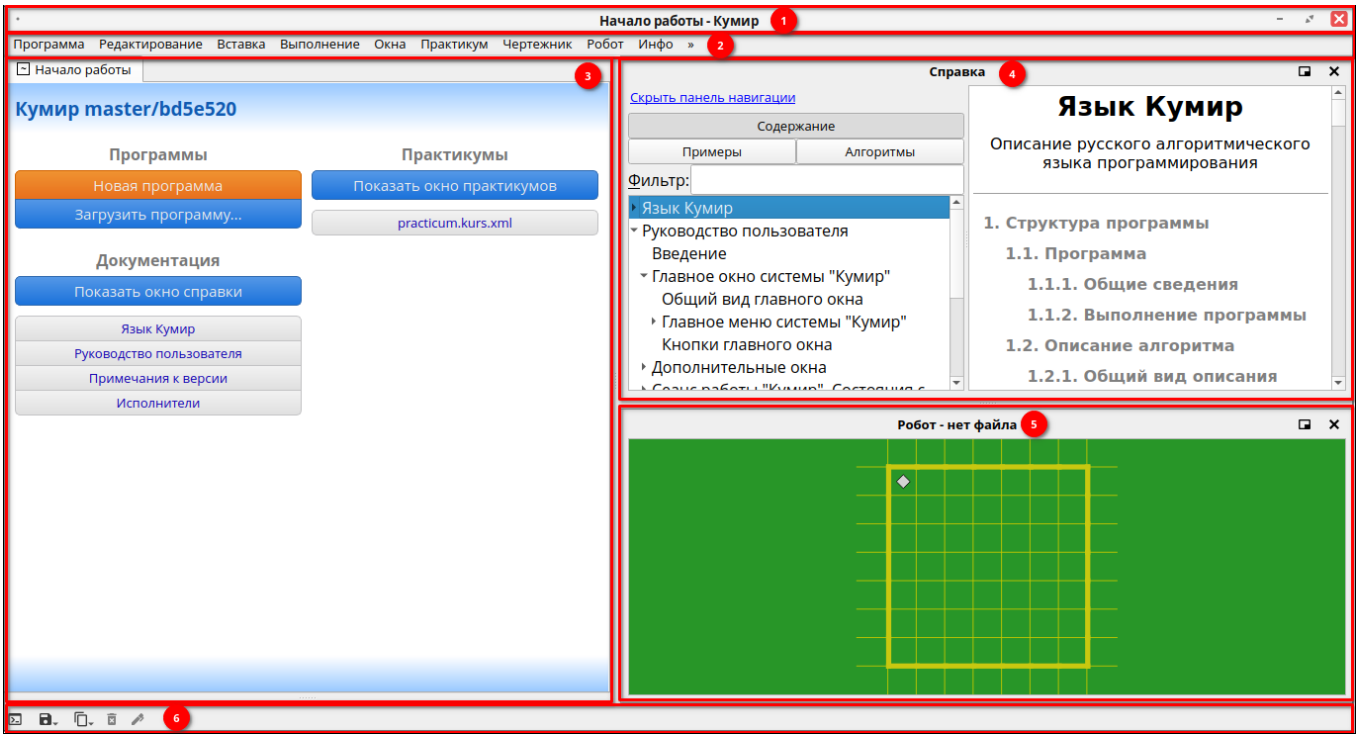
```
алг перекрасить
```

Программу для исполнителя «**Кузнечик**» можно писать также через пульт. Для управления исполнителем «**Кузнечик**» перейдите в меню «**Окна**» — «**Кузнечик-Пульт**»:



Описание конфигураций «Кумир для учителей» и «Кумир-Про»

Главное окно программы в конфигурациях «**Кумир для учителей**» и «**Кумир-Про**» выглядит следующим образом:



Интерфейс программы стандартный и состоит из нескольких типовых частей:

1. **Системный заголовок главного окна** — отображает название программы.

2. **Главное меню** — содержит семь основных пунктов и несколько дополнительных пунктов.

3. **Стартовая страница «Начало работы»** — расположены кнопки доступа к программам, практикумам, документации.

4 . **Справочные руководства** — раздел, где можно найти информацию о языке программирования, функциях системы **Кумир** и примеры кода (Меню «**Инфо**» — «**Справочные руководства**» или горячая клавиша **F1**).

5. **Окно исполнителя** — визуализирует выполнение программы, если она включает графический или анимационный вывод.

6. **Строка состояния** — отображает информацию об ошибках.

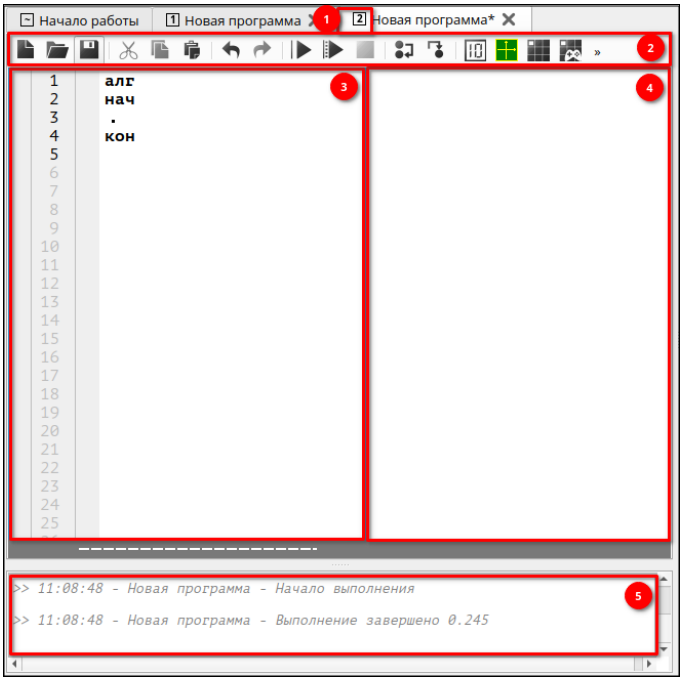
После запуска отображается стартовая страница «**Начало работы**», на которой отображаются ссылки для быстрого доступа к последним файлам, практикумам, книгам справочной системы, а также крупные кнопки, дублирующие некоторые пункты меню программы. Начальную вкладку закрыть нельзя.

Для начала работы с системой необходимо создать или загрузить существующую программу либо открыть практикум.

Слева от заголовка вкладки (1) отображается номер от 1 до 9 для быстрого доступа с помощью клавиатурного сочетания: CTRL+1..9 , где 1..9 – это номер вкладки. Доступ к стартовой странице обеспечивается комбинацией клавиш CTRL+~ .

Программа имеет две основные области: *рабочую область* и *область ввода-вывода* (4).

Рабочая область делится на две части: *область редактирования текста программы* (2) и *поле редактора* (3).



Система Кумир поддерживает преподавание по учебникам:

1. Основы информатики и вычислительной техники: Пробный учеб. для средних учебных заведений / А. П. Ершов, А. Г. Кушниренко, Г. В. Лебедев, А. Л. Семенов, А. Х. Шень. — М.: Просвещение, 1998. — 207 с.

2. Основы информатики и вычислительной техники: Учеб. для 10-11 кл. общеобразоват. учреждений / А. Г. Кушниренко, Г. В. Лебедев, Р. А. Сворень. — 4-е изд. — М.: Просвещение, 1996. — 223 с.

3. Информатика: 7-9 кл.: Учеб. для общеобразоват. учр. / А. Г. Кушниренко, Г. В. Лебедев, Я. Н. Зайдельман. — 4-е изд., стер. — М.: Дрофа, 2003. — 335 с.

4. Информационная культура. Кодирование информации. Информационные модели: 9-10 кл.: Учеб. для общеобразоват. учр. / А. Г. Кушниренко, А. Г. Леонов, М. Г. Эпиктетов и др. — 6-е изд., стер. — М.: Дрофа, 2003. — 199 с.

5. Информатика: алгоритмика: Учеб. для 6 кл. общеобразоват. учр. / А. К. Звонкин, С. К. Ландо, А. Л. Семенов. — М.: Просвещение, 2006. — 237 с.

6. Информатика: алгоритмика: Учеб. для 7 кл. общеобразоват. учр. / С. К. Ландо, А. Л. Семенов, М. Н. Вялый. — М.: Просвещение, 2008. — 207 с.

7. Информатика. 10 класс. Углубленный уровень: Учебник. в 2 частях / К. Ю. Поляков, Е. А. Еремин. — М.: Бином, 2013. — 648 с.

8. Информатика. 11 класс. Углубленный уровень: Учебник. в 2 частях / К. Ю. Поляков, Е. А. Еремин. — М.: Бином, 2013. — 532 с.

Система **Кумир** поддерживает также разработку практикумов по программированию с автоматизированной проверкой.

Примеры работы

Пример 1 (вычисление факториала)

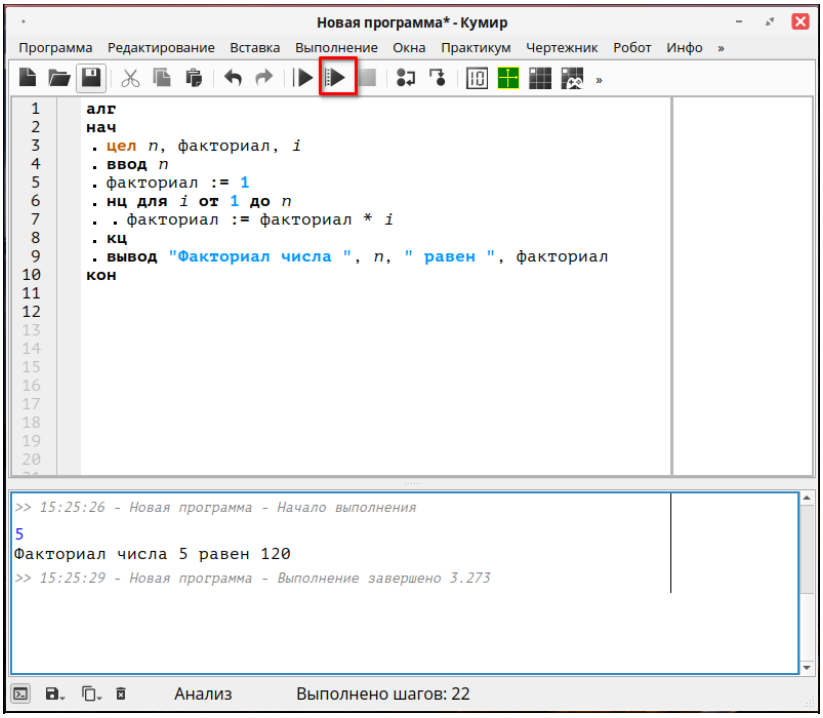
Для вычисления факториала числа, введённого пользователем, введите код в рабочей области:

```
алг
 нач
 цел n, факториал, i
 ввод n
 факториал := 1
 нц для i от 1 до n
 факториал := факториал * i
 кц
 вывод "Факториал числа ", n, " равен ", факториал
 кон
```

Алгоритм работы программы:

- Сначала программа запрашивает у пользователя число n.
- Затем она инициализирует переменную факториал значением 1.
- После этого программа входит в цикл от 1 до n, на каждом шаге умножая текущее значение факториала на номер итерации i.
- В конце программа выводит результат вычисления факториала.

Запустите код, нажав «**Обычное выполнение**». В области ввода-вывода введите любое число, далее отобразится результат выполнения программы.

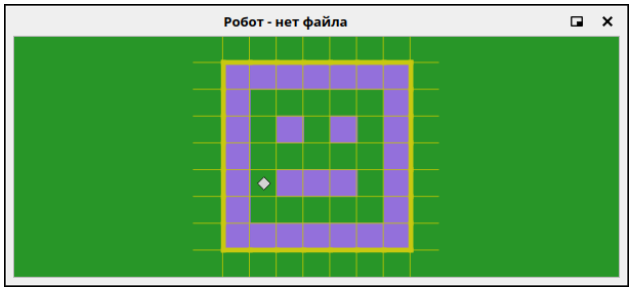


Пример 2 (исполнитель «Робот»)

Для выполнения задачи рисования на виртуальном поле с использованием «**Робота**» введите в рабочей области следующий код:

```
использовать Робот
алг
нач
нц пока справа свободно
закрасить; вправо
кц
нц пока снизу свободно
закрасить; вниз
кц
нц пока слева свободно
закрасить; влево
кц
нц пока сверху свободно
закрасить; вверх
кц
вниз; вниз; вправо; вправо
закрасить
вправо; вправо
закрасить
вниз; вниз
нц 3 раз
закрасить; влево
кц
кон
```

Результат выполнения:

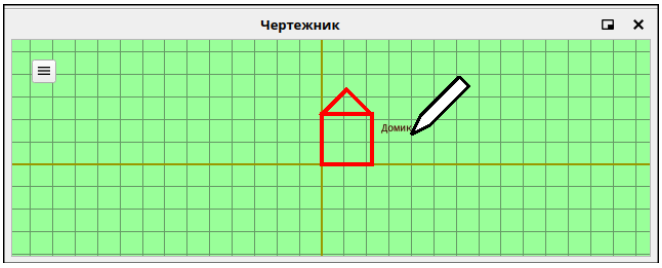


Пример 3 (исполнитель «Чертежник»)

Для выполнения задачи рисования на виртуальном поле с использованием «Чертежника» введите в рабочей области следующий код:

```
использовать Чертежник
 алг
 нач
 выбрать чернила(красный)
  опустить перо
  сместиться на вектор(0, 5)
  сместиться на вектор(5, 0)
  сместиться на вектор(0, -5)
  сместиться на вектор(-5, 0)
  поднять перо
  сместиться на вектор(5, 5)
  опустить перо
  сместиться на вектор(-2.5, 2.5)
  сместиться на вектор(-2.5, -2.5)
  поднять перо
  сместиться в точку(0, 0)
  сместиться на вектор(6, 3)
  написать(3, "Домик")
 кон
```

Результат выполнения:



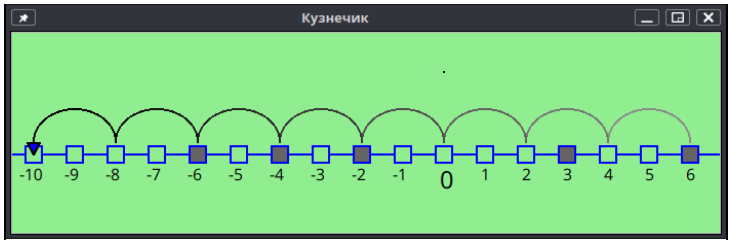
Пример 4 (исполнитель «Кузнечик»)

Для выполнения задачи перемещения «Кузнечика» с перекрашиванием клеток с использованием «Кузнечика» введите в рабочей области следующий код:

```
использовать Кузнечик
 алг
 нач
 вперед 3
   перекрасить
   вперед 3
   перекрасить
```

```
  назад 2
  назад 2
  назад 2
  назад 2
  перекрасить
  назад 2
  перекрасить
  назад 2
  перекрасить
  назад 2
  назад 2
кон
```

Результат выполнения:



GNU Octave — программа для математических вычислений

Установка
Описание программы
Начало работы
Примеры использования

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: octave-6:6.3.0

GNU Octave — свободная программная система для математических вычислений, использующая совместимый с MATLAB язык высокого уровня, предназначенный для решения задач вычислительной математики.

GNU Octave представляет удобный интерактивный командный интерфейс для решения линейных и нелинейных математических задач и для выполнения других численных экспериментов.

Язык Octave оперирует арифметикой вещественных и комплексных скаляров и матриц, имеет расширения для:

- решения линейных алгебраических задач;
- нахождения корней систем нелинейных алгебраических уравнений;
- работы с полиномами;
- решения различных дифференциальных уравнений;
- интегрирования систем дифференциальных и дифференциально-алгебраических уравнений первого порядка;
- интегрирования функций на конечных и бесконечных интервалах.

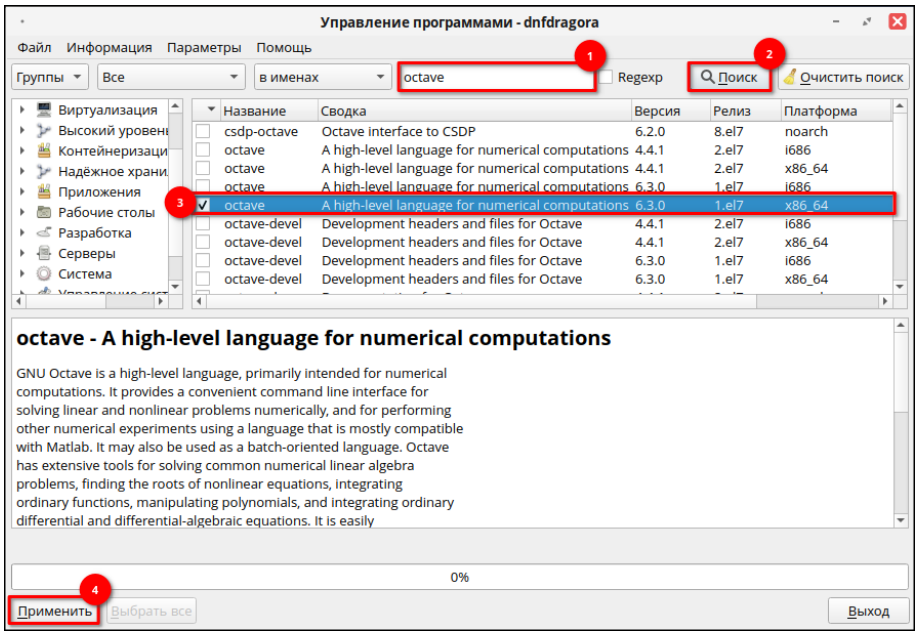
Характеристики:

- GNU Octave написана на языке C++ с использованием библиотеки STL;
- для запуска скриптов octave используется интерпретатор;
- GNU Octave можно дополнять динамически подгружаемыми модулями;
- GNU Octave является кроссплатформенной;
- существуют онлайн-сервисы, позволяющие выполнять скрипты octave и отображать полученные результаты в браузере.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**octave**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install octave
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Для запуска программы через терминал введите команду:

```
octave
```

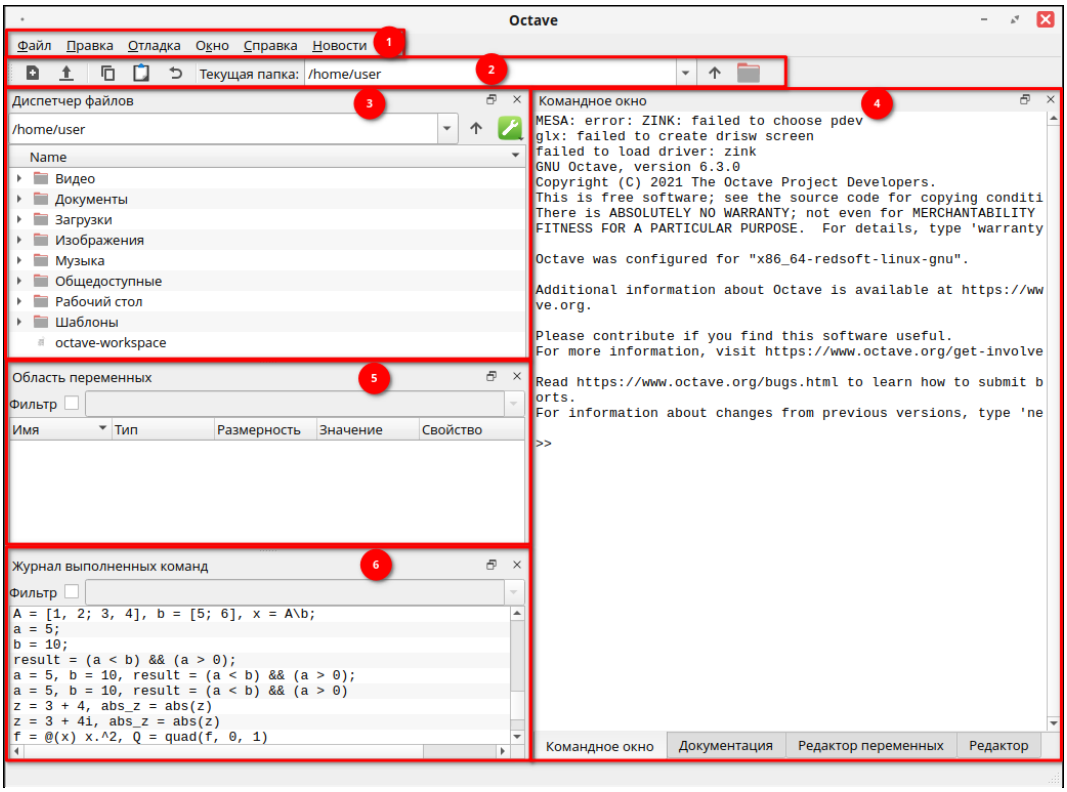
Для выхода из Octave введите **quit** или **exit** в командной строке. После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**GNU Octave**».

Можно запустить программу также с помощью кнопки запуска на рабочем столе. Для размещения кнопки запуска программы на рабочем столе в «**Главном меню**» — «**Образовательные**» щелкните ПКМ на **GNU Octave** и выберите в контекстном меню «**Поместить на Рабочий стол**».



Описание программы

Главное окно программы выглядит следующим образом:



1. **Основное меню** содержит различные функции для управления файлами, редактирования кода, настройки интерфейса и доступа к справочной информации. Основное меню включает:

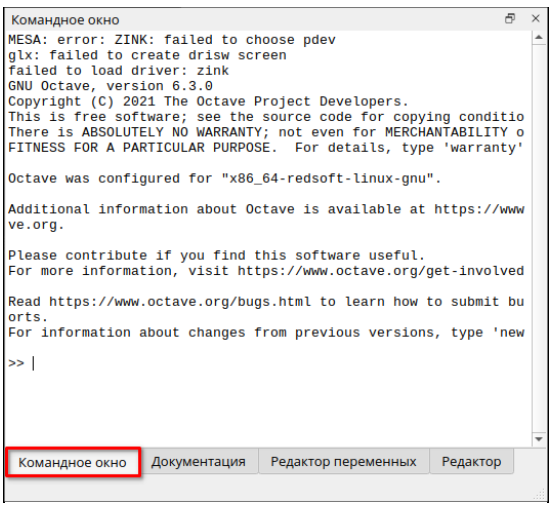
- **Файл** — работа с файлами и областью переменных;
- **Правка** — инструменты редактирования документа и операции с буфером обмена;
- **Отладка** — средство отладки кода;
- **Окно** — управление интерфейсом пользователя;
- **Справка** — доступ к справочной системе;
- **Новости** — примечания к выпуску и последние обновления.

2 . **Панель инструментов** содержит кнопки для быстрого доступа к часто используемым командам, таким как создать сценарий, открыть существующий файл в редакторе, копировать, вставить.

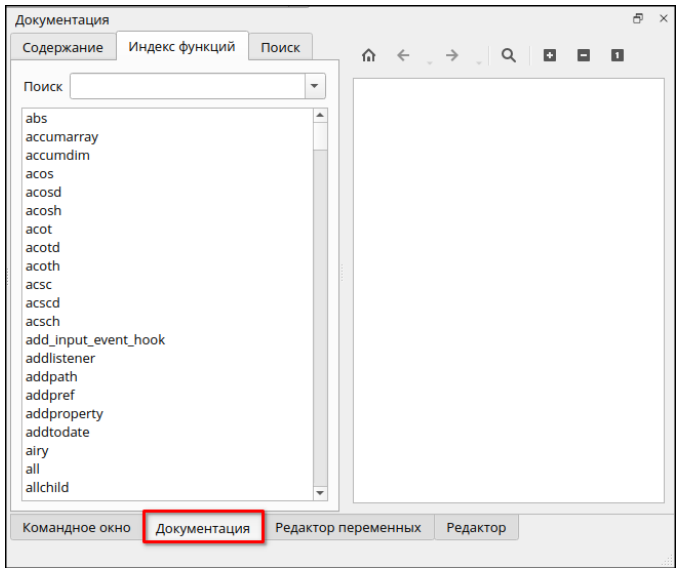
3 . **Диспетчер файлов** позволяет управлять файлами и каталогами на компьютере пользователя. Можно использовать его для открытия, сохранения, перемещения и копирования файлов, а также для просмотра содержимого файлов.

4. **Рабочая область** имеет четыре вкладки, каждая из которых выполняет определённую функцию. Переключение между вкладками позволяет управлять просмотром документации, редактированием переменных или написанием кода.

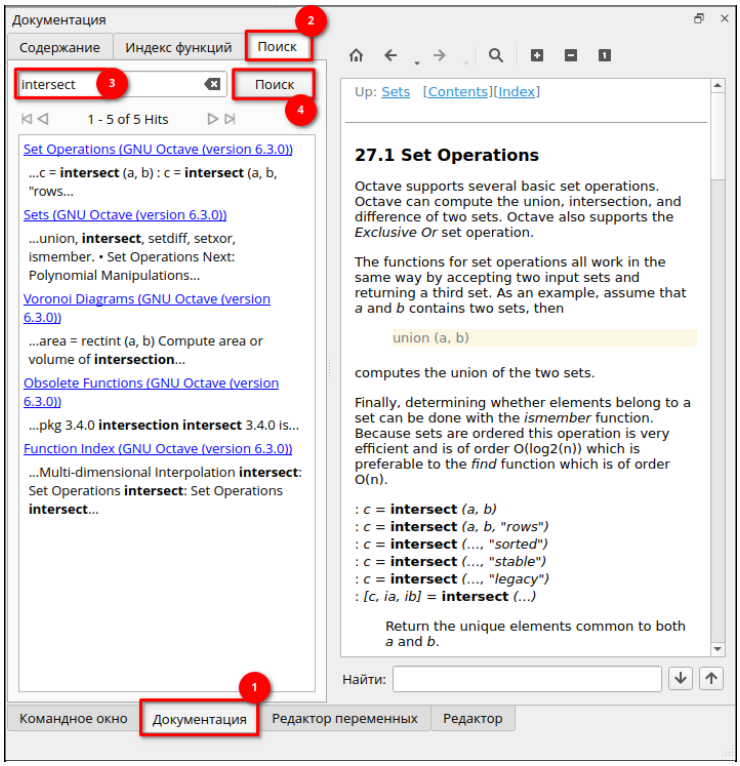
- **Командное окно** вкладка является активной по умолчанию и представляет собой панель ввода, где можно вводить команды и выражения, а также просматривать результаты их выполнения. Командное окно отображает сообщения об ошибках, если они возникают при выполнении команд.



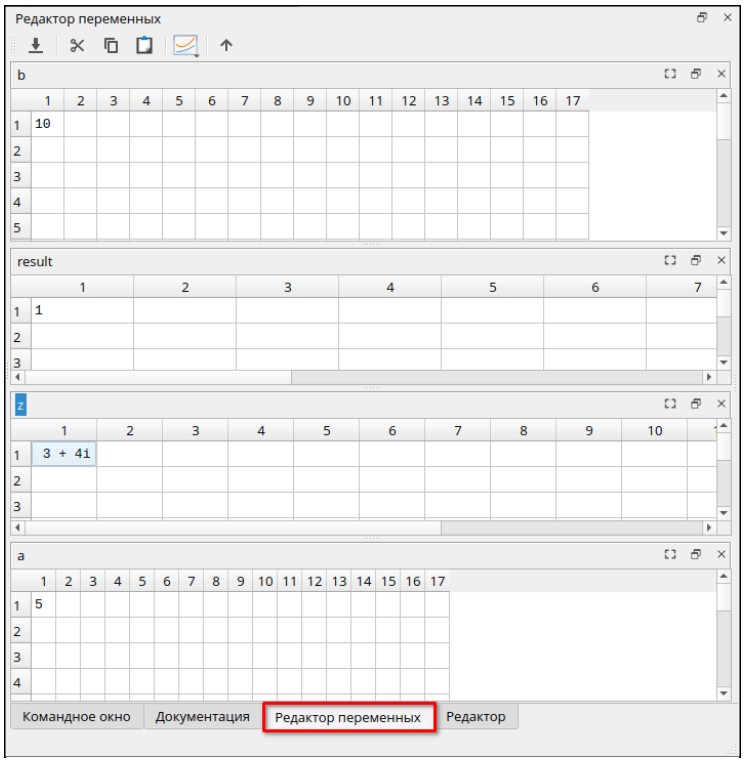
- **Документация** отображает справочную информацию о функциях, переменных и других объектах в **Octave**.



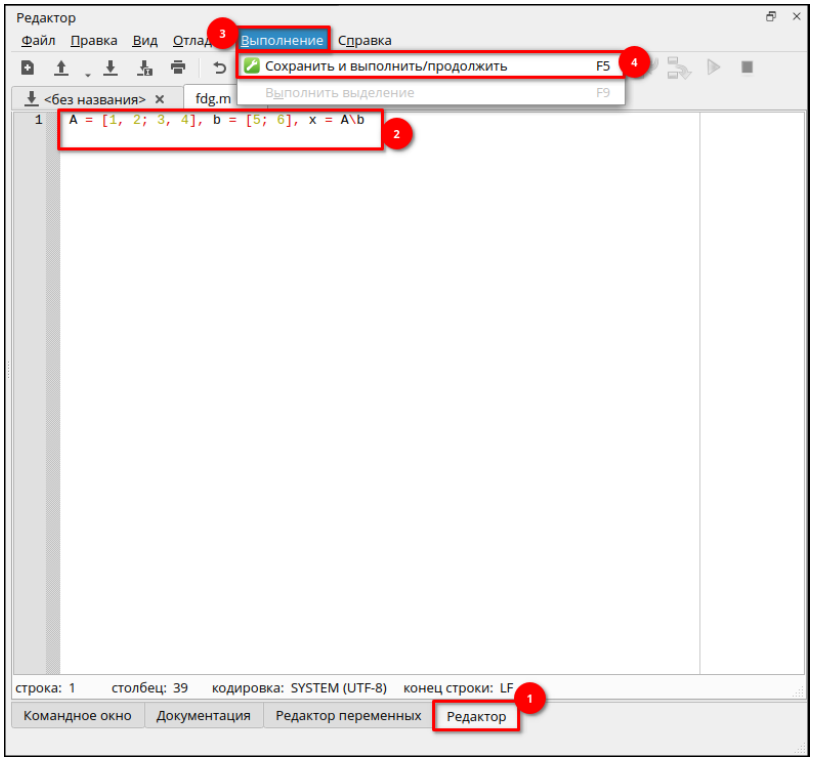
Для просмотра документации по определённому объекту перейдите на вкладку «**Документация**» (1) — «**Поиск**» (2). Введите в строке поиска нужный объект (3) и выполните поиск (4).



- **Редактор переменных** позволяет просмотреть и изменить значения переменных в текущей сессии Octave без повторного ввода всей команды, создающей переменную. После ввода команды, создающей переменную, можно переключиться на вкладку «**Редактор переменных**» и увидеть список текущих переменных. Щёлкнув по имени переменной, можно отредактировать её значение. Для отображения выбранных данных на графике доступен инструмент  .



- **Редактор** (1) позволяет работать в программном режиме. Он представляет собой текстовый редактор, в котором можно писать и редактировать скрипты и программы на языке **Octave**. Скрипты доступны для сохранения и загрузки для дальнейшей работы. После редактирования кода в редакторе (2) можно выполнить его, перейдя в меню «**Выполнение**» (3) — «**Сохранить и выполнить/продолжить**» (4) или используя горячую клавишу **F5**.



В редакторе присутствует дополнительная панель инструментов:



5 . **Область переменных** отображает текущие переменные в текущей сессии Octave. Можно просмотреть, изменить или удалить переменные из этой области.

6. **Журнал выполненных команд** отображает историю введённых команд и результатов их выполнения. Журнал также может быть сохранен как файл для дальнейшего использования или обмена с другими пользователями.

Начало работы

В **Octave** существуют два режима работы.

1 . **Терминальный режим** позволяет пользователю вводить команды в диалоговом режиме, система выполняет их и выводит результаты на экран.

2. **Программный режим** позволяет создавать текстовые файлы с расширением ***.m** и запускать файлы в среде **Octave**. Для работы в программном режиме перейдите на вкладку «**Редактор**».

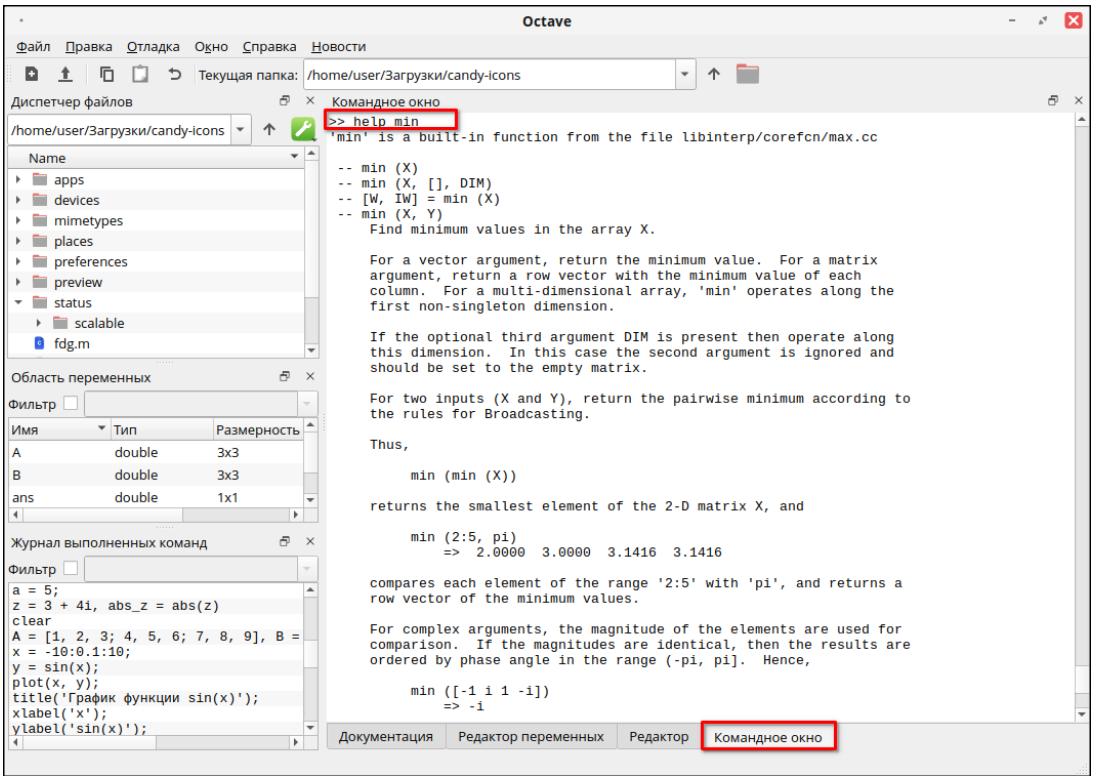
В настройках можно изменить параметры интерфейса командного окна, редактора и устанавливать комбинации клавиш.

Признаком начала работы является наличие знака **>>** в командном окне.

Octave имеет справочную базу на английском языке. Документация доступна из командной строки в онлайн-режиме и печатном варианте.

Для получения справочной информации в командном окне введите **help** и <название_команды>. Например, для вызова справки о функции **min()** введите команду:

```
help min
```



При работе в командном окне нажатие клавиши **Enter** инициирует выполнение введённой команды и выводит результат на экран.

Во время выполнения сложных вычислений, когда не требуется выводить промежуточные результаты, чтобы отменить вывод результата на экран, можно поставить символ "**;**" в конце строки после команды. В противном случае, если символ "**;**" не указан, результаты будут выведены на экран.

Сообщения об ошибке при выполнении кода помогают пользователю проследить, на каком этапе он допустил ошибку.

Octave можно использовать для базовых числовых расчётов. **Octave** поддерживает арифметические операции (**+**, **-**, ***, /**), возведение в степень (**^**), натуральные логарифмы и показатели (**log**, **exp**), тригонометрические функции (**sin**, **cos** и т.д.). **Octave** работает с действительными или мнимыми числами (**i**, **j**). Некоторые математические константы, например, основание натурального логарифма (**e**) и отношение длины окружности к её диаметру (**pi**), также заранее определены в **Octave**.

Примеры использования

Пример 1. Для выполнения арифметических операций введите в командном окне последовательность команд и нажмите **Enter**:

```
a=43;
b=2;
sum= a + b,
diff = a - b,
prod = a * b,
quot = a / b,
```

```
rem = a % b,
pow = a ^ bsum = 45
diff = 41
prod = 86
quot = 21.500
rem = 43
pow = 1849
```

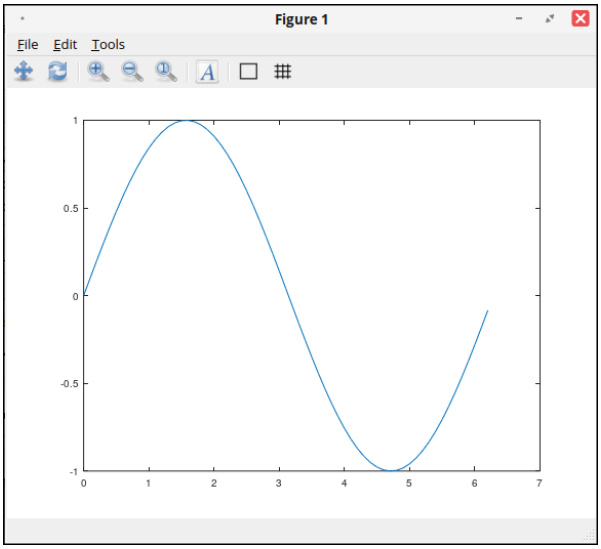
где:

- **sum = a + b** — складывает значения **a**, **b** и сохраняет результат в переменной **sum**;
- **diff = a - b** — вычитает значение **b** из значения **a** и сохраняет результат в переменной **diff**;
- **prod = a * b** — перемножает значения **a**, **b** и сохраняет результат в переменной **prod**;
- **quot = a / b** — делит значение **a** на значение **b** и сохраняет результат в переменной **quot**;
- **rem = a % b** — вычисляет остаток от деления значения **a** на значение **b** и сохраняет результат в переменной **rem**;
- **pow = a ^ b** — возводит значение **a** в степень **b** и сохраняет результат в переменной **pow**.

Пример 2. Для построения графика синусоиды введите следующую команду:

```
t = 0:0.1:2*pi;
y = sin(t);
plot(t, y)
```

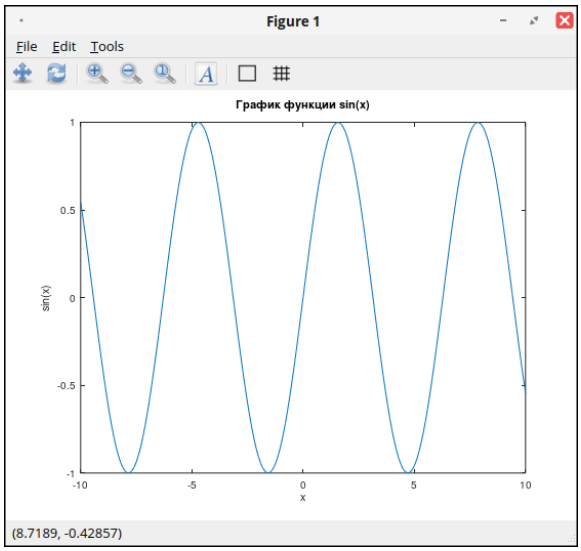
Отобразится окно с графиком.



Пример 3. Для построения графика функции создайте вектор **x** от **-10** до **10** с шагом **0.1**, затем вычислите соответствующие значения функции **sin(x)**:

```
x = -10:0.1:10;
y = sin(x);
plot(x, y);
title('График функции sin(x)');
xlabel('x');
ylabel('sin(x)');
```

Отобразится график:



Пример 4. Введите следующую команду для создания матрицы A и умножения каждого элемента на 2:

```
A = [1, 2, 3; 4, 5, 6; 7, 8, 9], B = A * 2A =
   1   2   3
   4   5   6
   7   8   9

B =
    2    4    6
    8   10   12
   14   16   18
```

Пример 5. Введите матрицу коэффициентов **A**, вектор свободных членов **b** и найдите решение системы линейных уравнений **x** с помощью обратной матрицы **A**:

```
A = [1, 2; 3, 4], b = [5; 6], x = A\bA =
   1   2
   3   4
b =
   5
   6
x =
  -4.0000
   4.5000
```

Пример 6. Введите переменные **a**, **b** и выполните логические операции:

```
a = 5, b = 10, result = (a < b) && (a > 0)a = 5
b = 10
result = 1
```

Пример 7. Введите комплексное число **z** и найдите его модуль:

```
z = 3 + 4i, abs_z = abs(z)z =  3 + 4i
abs_z = 5
```

Пример 8. Определите функцию **f** и найдите площадь под кривой **f(x) = x^2** от **0** до **1** с помощью функции **quad**:

```
f = @(x) x.^2, Q = quad(f, 0, 1)f =
@(x) x .^ 2
Q = 0.3333
```

Установка Geany

Установка
Замена терминала
Простая программа на языке pascal

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: geany-1.36

Geany — среда разработки программного обеспечения, написанная на языке **C** с использованием библиотеки **GTK+**. Отличие **Geany** в том, что это быстрая и легкая среда разработки.

Geany совмещает в себе редактор исходного кода, который поддерживает подсветку синтаксиса большого числа языков и базовые возможности по автодополнению ключевых слов, инструменты для компиляции и запуска программ.

Работать с ней очень удобно и приятно, к тому же она не ограничивает пользователя только одним языком. Всего поддерживается более **60 языков** программирования.

Вы можете подробнее ознакомиться с работой **Geany**, просмотрев наши обучающие видео:

- на **RuTube** — Geany - программировать просто. Первая программа на Pascal;
- в **Яндекс.Дзен** — Geany - программировать просто. Первая программа на Pascal;
- в **VK Видео** — Geany - программировать просто. Первая программа на Pascal.

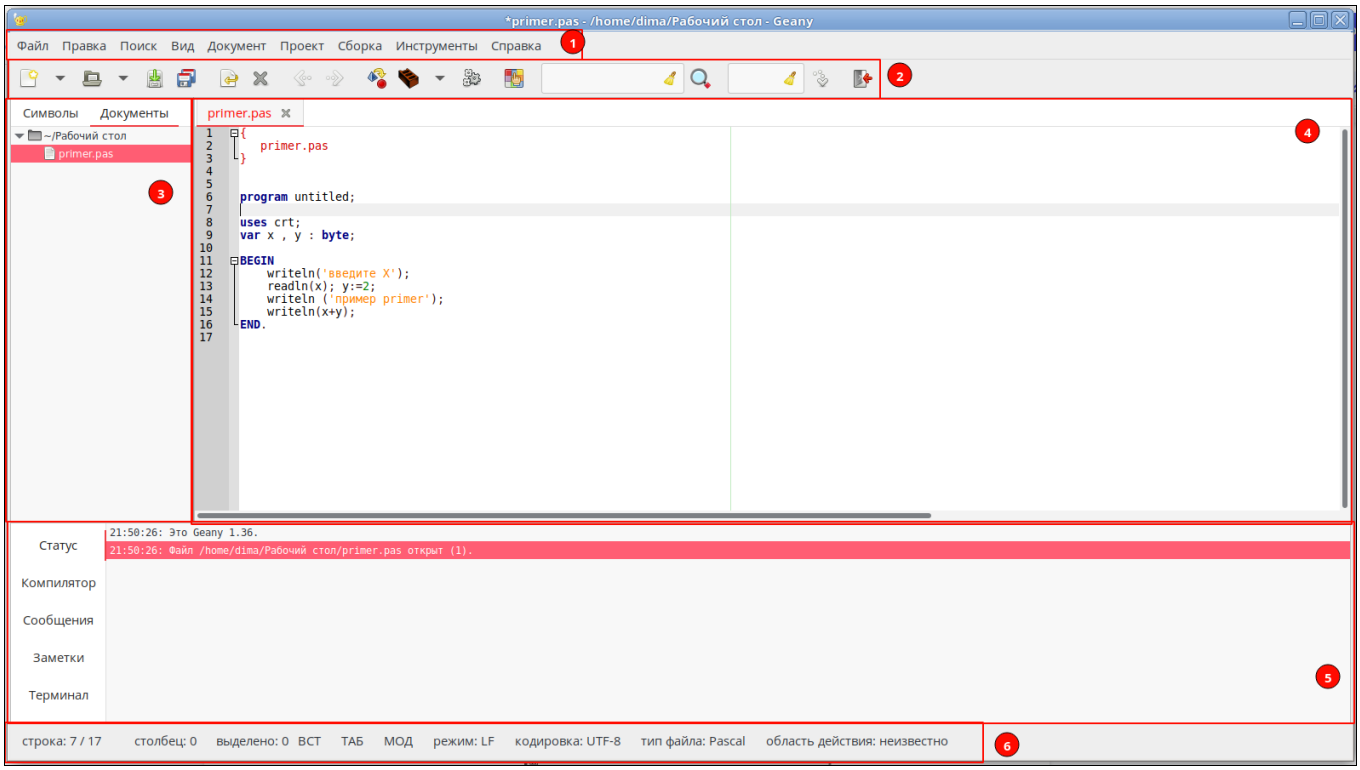
На наших каналах вы также сможете найти много другой полезной информации.

Основные функции **Geany**:

- подсветка синтаксиса;
- поддержка большого количества кодировок;
- сворачивание блоков кода;
- автозавершение имён;
- работа со сниппетами (фрагментами кода);
- автоматическое закрытие тегов *xml* и *html*;
- поддержка языков *c*, *java*, *php*, *html*, *python*, *perl*, *pascal* и других;
- списки имен;
- навигация по коду;
- отладка (требуется плагин **geanygdb**);
- использование контекстной документации **man**, **devhelp**;
- сборка — система для компиляции и исполнения кода;
- простое управление проектом;
- интерфейс для модулей.

Основное окно редактора состоит из *6 основных блоков*:

1. Строка основного меню.
2. Панель инструментов с кнопками.
3. Боковая панель.
4. Основное поле редактора.
5. Панель сообщений.
6. Панель состояний.



Установка

Для установки необходимо перейти в сеанс пользователя root:

```
su -
```

и выполнить команду:

```
dnf install geany
```

также необходимо установить компилятор языка Pascal:

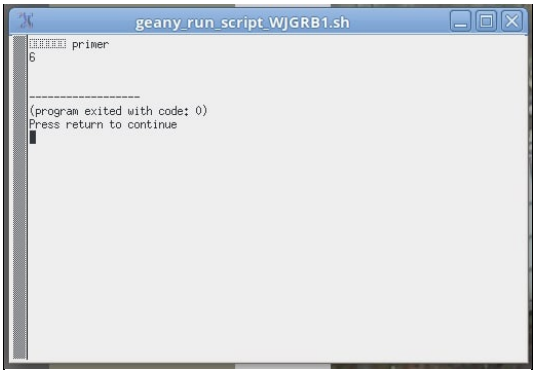
```
dnf install fpc
```

Запуск доступен из «**Меню**» - «**Программирование**» - «**Среда разработки Geany**».

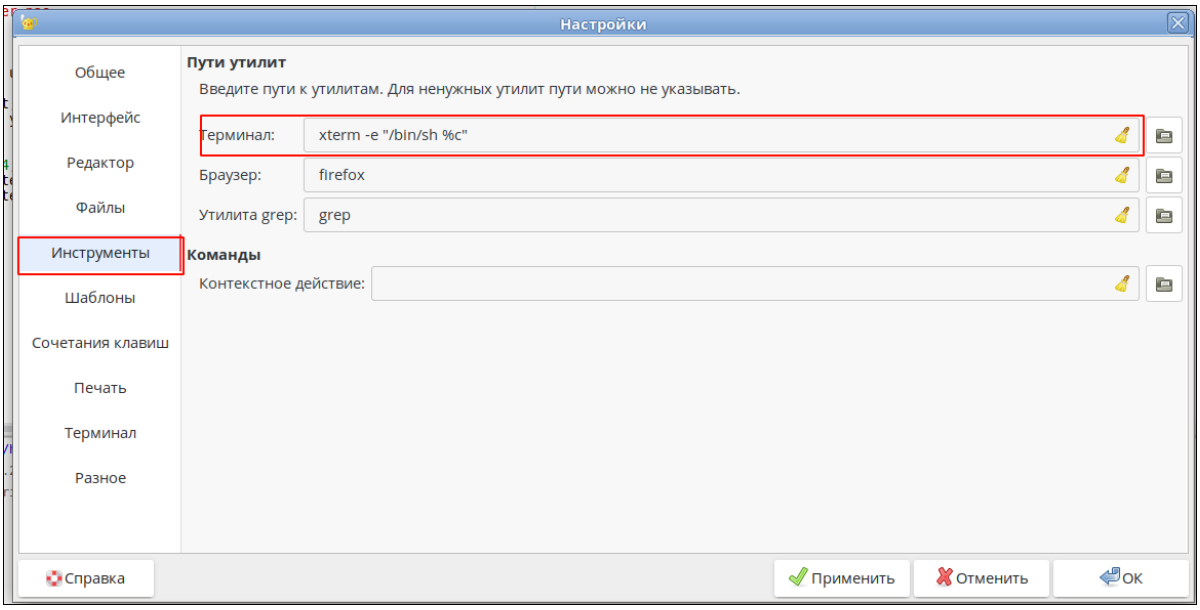
Замена терминала

По умолчанию для запуска скомпилированной программы используется программа **xterm**. Если она не установлена, это можно сделать командой:

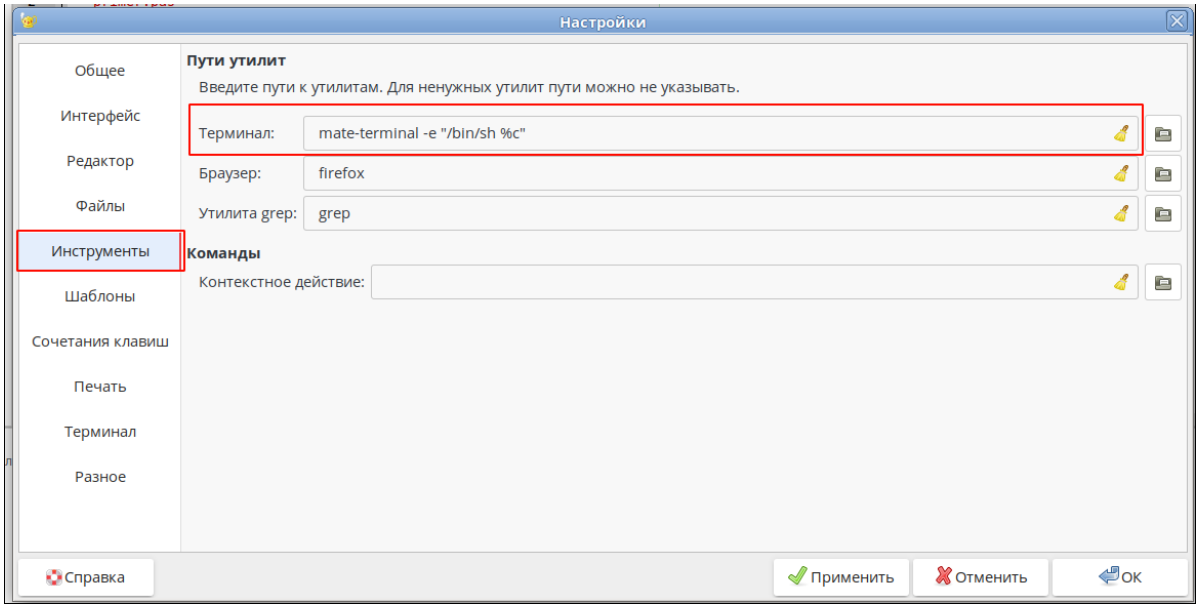
```
dnf install xterm
```



Терминал можно заменить на стандартный. Для этого необходимо перейти в **Настройки** («**Правка**» - «**Настройки**»). В появившемся окне в пункте «**Инструменты**», в поле «**Терминал**» необходимо заменить **xterm** на **mate-terminal**.

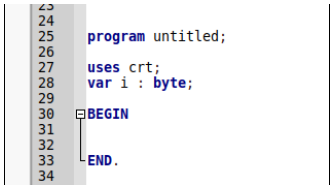


После сохранения внесенных изменений программа по умолчанию будет запускаться в стандартном для **MATE** терминале.



Простая программа на языке pascal

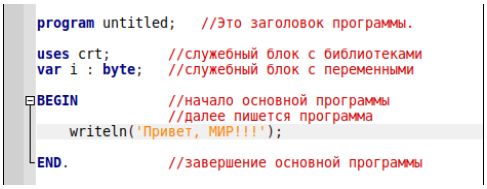
Для создания новой программы в **Geany** необходимо выбрать пункт меню «**Файл**» - «**Создать из шаблона**» - «**program.pas**». Откроется шаблон для написания кода:



```
24
25  program untitled;
26
27  uses crt;
28  var i : byte;
29
30  BEGIN
31
32
33  END.
34
```

Затем необходимо сохранить файл программы («**Файл**» - «**Сохранить**»).

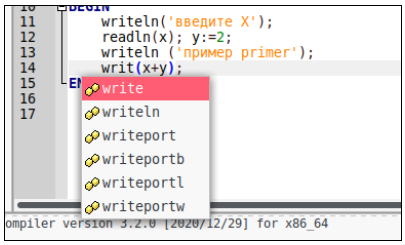
Далее следует написать основной код программы. Т.к. рассматривается простейшая программа, можно использовать в качестве основного кода программы вывод текстовой строки «*Привет, МИР!!!*» в терминал.



```
program untitled;   //Это заголовок программы.

uses crt;           //служебный блок с библиотеками
var i : byte;       //служебный блок с переменными

BEGIN               //начало основной программы
                    //далее пишется программа
    writeln('Привет, МИР!!!');

END.                //завершение основной программы
```

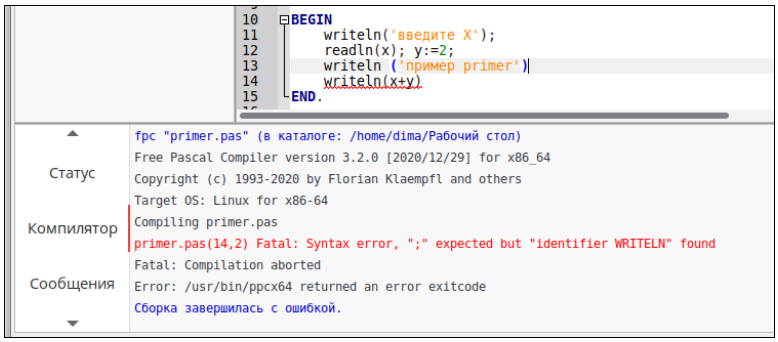
В процессе написания текста программы постоянно отображаются подсказки. Если необходимая команда есть в подсказке, можно

выбрать её двойным нажатием *ЛКМ* или клавишами *вверх/вниз + Enter*.



После того как программа написана, необходимо ее преобразовать в понятный процессору набор команд. Для этого существует компилятор. Одновременно с компиляцией происходит проверка текста программы на наличие ошибок. Компиляция запускается в пункте меню «**Сборка**» - «**Скомпилировать**».

Если в тексте программы есть синтаксические ошибки, компилятор сообщит об этом и подчеркнет строку с ошибкой красной линией.



Ошибку необходимо исправить и повторить компиляцию. Данные действия выполняются до тех пор, пока все ошибки не будут исправлены и компиляция не будет завершена успешно.

После успешной компиляции можно проверить работу программы. Запустите её на исполнение «**Сборка**» - «**Выполнить**».

Откроется окно терминала и программа начнет выполняться. Останется только проконтролировать правильность выполнения написанной программы, при необходимости исправить и повторить компиляцию.

Установка Lazarus

Установка
Обзор программы
Пример работы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: lazarus-2.2.2

Lazarus – это интегрированная среда разработки (IDE) и компилятор для языка программирования **Pascal**, который строится на основе библиотеки компонентов Free Pascal (FPC).

Особенности **Lazarus**:

- **Кроссплатформенность**. *Lazarus* позволяет разрабатывать приложения, которые могут работать в различных операционных системах, таких как *Windows*, *Linux*, *macOS* и других без изменений в исходном коде. Данная возможность поддерживается благодаря использованию *Free Pascal Compiler*.
- **Визуальное программирование**. *Lazarus* предоставляет визуальный редактор форм, который позволяет разработчикам создавать интерфейс приложения методом перетаскивания. Этот подход значительно упрощает создание пользовательских интерфейсов и улучшает процесс разработки.
- **Компонентная модель**. *Lazarus* предоставляет богатую библиотеку компонентов, которые можно использовать для создания различных элементов интерфейса и функциональности приложения. Компоненты могут быть переиспользованы, что способствует повышению производительности и уменьшению объема кода.
- **Отладка**. *Lazarus* предоставляет возможности для отладки кода, что помогает выявлять и устранять ошибки в процессе разработки.
- **Поддержка множества стандартов**. *Lazarus* соответствует различным стандартам *Pascal*, включая **Turbo Pascal** и **Delphi**, что делает его подходящим для разработчиков, знакомых с данными окружениями.

Lazarus популярен среди разработчиков, которые хотят использовать язык **Pascal** для создания кроссплатформенных приложений с удобным визуальным редактором форм и богатыми возможностями компонентной модели. Он особенно популярен среди разработчиков, знакомых с **Borland Delphi**, так как предоставляет схожий опыт разработки и привычный интерфейс.

Установка

Для установки **Lazarus** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install lazarus
```

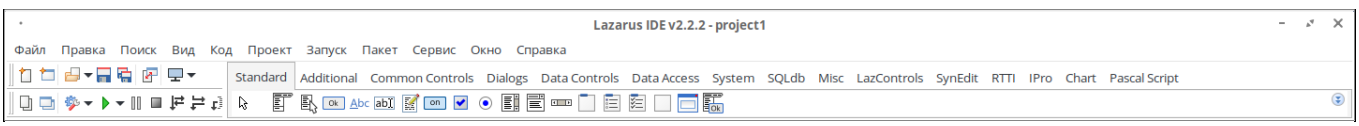
После установки запуск программы доступен из «**Главного меню**» — «**Программирование**» — «**Lazarus**» или через терминал (с правами **непривилегированного** пользователя) командой:

```
startlazarus
```

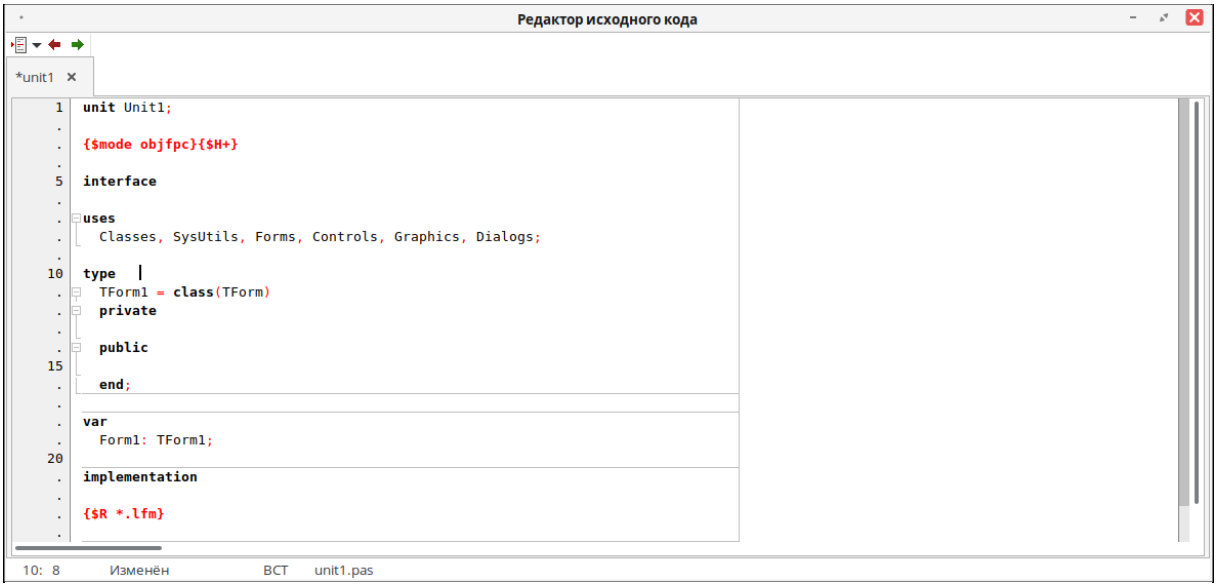
Обзор программы

Программа состоит из нескольких основных компонент:

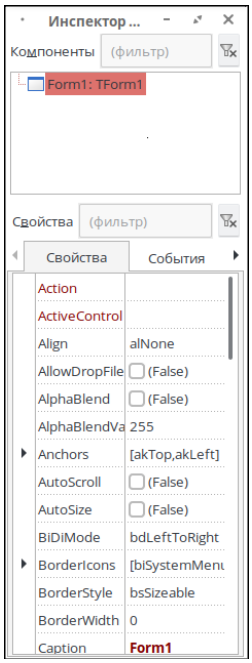
1. **Главное меню** – содержит основное меню, панели инструментов и область для работы с проектами и файлами кода. Здесь можно создавать, открывать и редактировать проекты, а также управлять компонентами и кодом приложения.



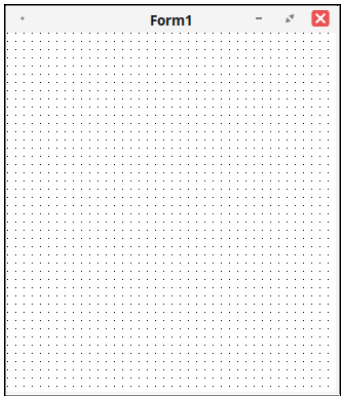
2 . **Редактор кода** – предназначен для написания и редактирования исходного кода приложения. Он обеспечивает подсветку синтаксиса, автозавершение и другие функции для облегчения работы с кодом.



3 . **Инспектор объектов** (панель объектов) – предоставляет доступ к свойствам и событиям выбранного компонента. Здесь можно настраивать свойства компонентов и устанавливать обработчики событий.

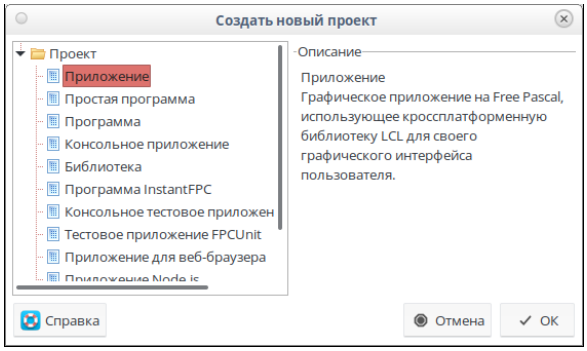


4. **Окно форм** – позволяет создавать и редактировать пользовательские формы, на которых размещаются графические компоненты для создания интерфейса приложения.



Пример работы

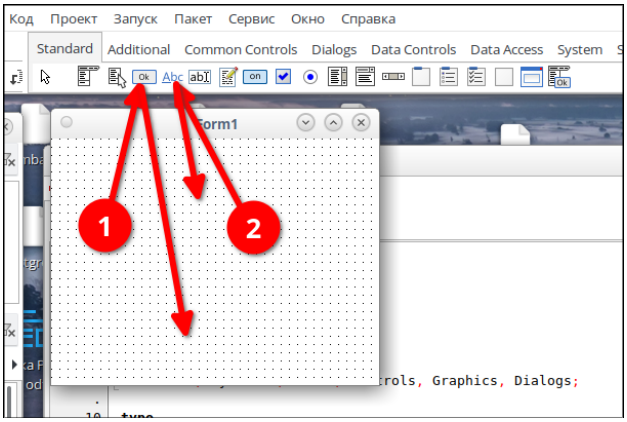
Для создания нового проекта в главном меню выберите «**Проект**» – «**Создать проект**». Появится окно, в котором предлагается выбрать тип проекта.



Для создания графического приложения выберите «**Приложение**» и нажмите «**OK**».

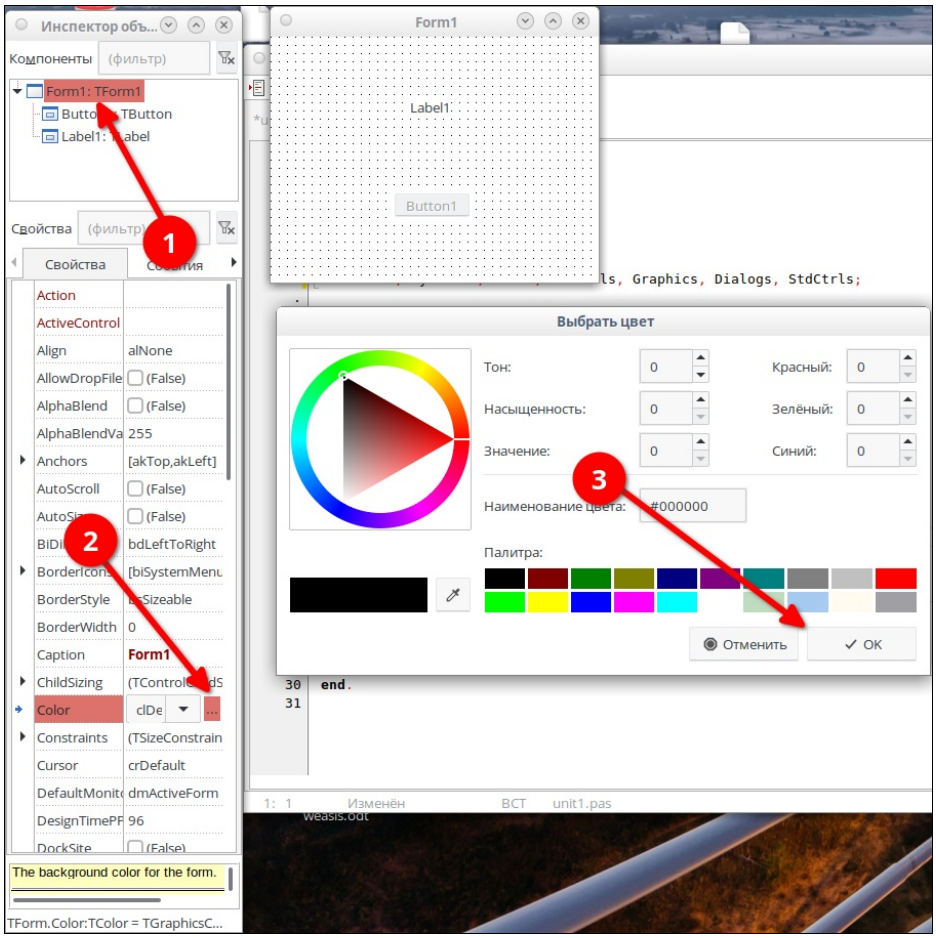
В меню с объектами выберите необходимые объекты:

- 1 – кнопка (*button*);
- 2 – текстовое поле для вывода информации (*label*).

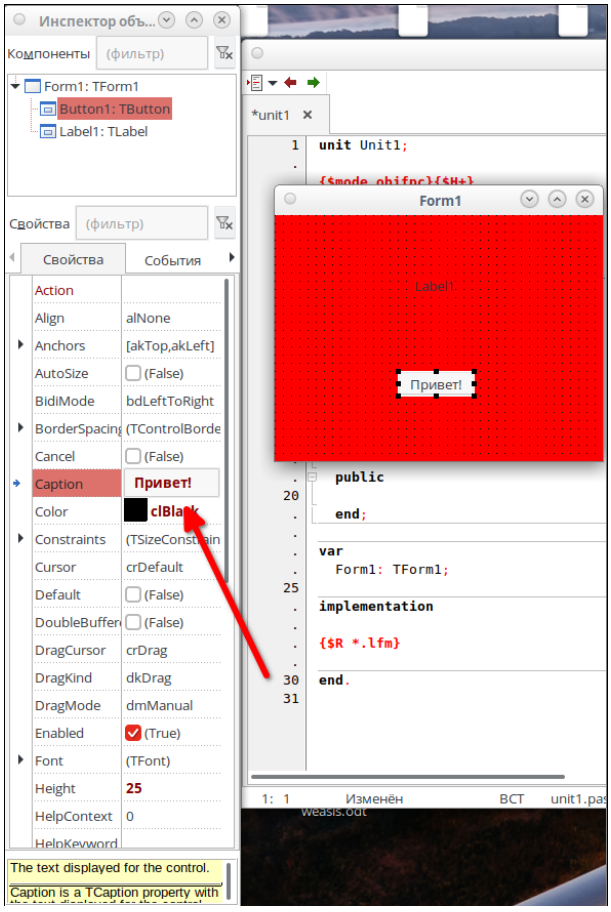


Доступно изменение размера и положения объектов.

В инспекторе объектов можно определить различные настройки для объектов, в примере будет изменен цвет фона. Для этого в окне инспектора объектов в дереве объектов выберите **Form1**, для параметра **Color** выберите необходимый цвет.



Измените надпись на кнопке. В окне инспектора объектов выберите **Button1** и в разделе «**Свойства**» укажите собственное название кнопки в параметре **Caption**.

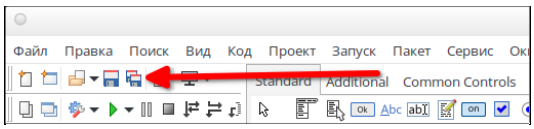


Для **Label1** удалите содержимое параметра **Caption**.

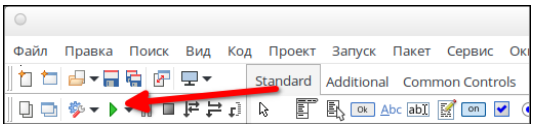
После этого можно создать код для кнопки – дважды щелкните по кнопке, откроется редактор кода. Напишите программный код для действия, например:

```
procedure TForm1.Button1Click(Sender: TObject);
begin
 Label1.Caption:='Привет мир!';
end;
```

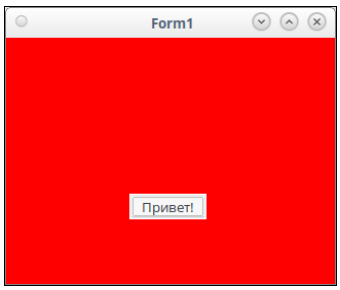
Сохраните проект – в главном меню нажмите «**Сохранить все**» или комбинацию клавиш **Shift+Ctrl+S**. Проект рекомендуется сохранять в отдельный каталог.



Запустите программу – в главном меню нажмите «**Запуск**» или клавишу **F9**.



При удачной компиляции будет открыто окно созданной программы.



Нажмите на кнопку – результат работы отобразится на экране.

В данном примере было рассмотрено создание простейшей программы для начала работы пользователя с **Lazarus**.

С помощью **Lazarus** можно разрабатывать разнообразные приложения – от простых оконных до сложных программ с графическим интерфейсом.

Установка QT Creator

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Qt Creator - 6.0.2

Qt Creator — кроссплатформенная свободная *IDE* для разработки на **C**, **C++**, **QML** и **python**. Разработана **Trolltech** для работы с фреймворком **Qt**.

Включает в себя графический интерфейс отладчика и визуальные средства разработки интерфейса как с использованием **QtWidgets**, так и **QML**.

Для установки **qtcreator** перейдите в сеанс пользователя root:

```
su -
```

Установка **qtcreator** в РЕД ОС осуществляется следующей командой:

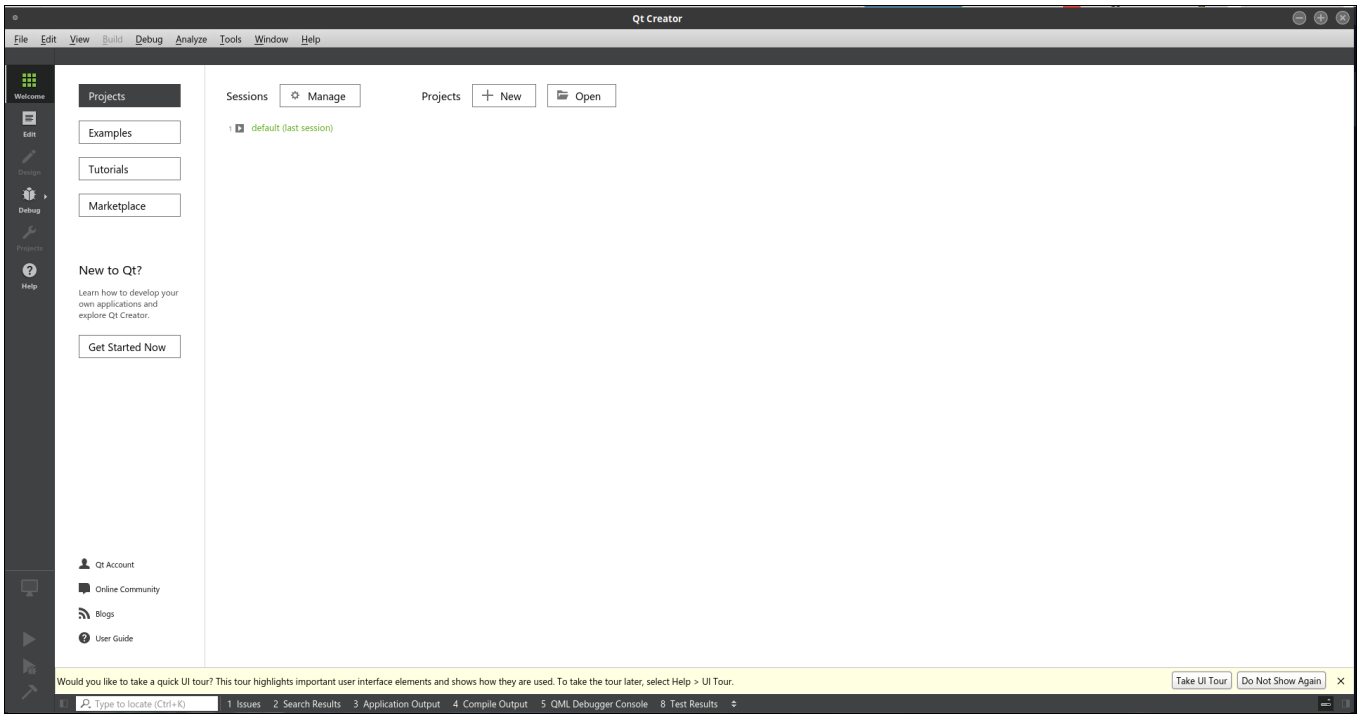
```
dnf install qt-creator libdrm
```

Для использования **QML** необходимо установить дополнительные библиотеки следующей командой:

```
dnf install qt5-qtquickcontrols2 qt5-qtquickcontrols2-devel
```

Запуск *IDE* доступен из «**Меню**» - «**Программирование**» - «**Qt Creator**» или выполнить команду от локального пользователя:

```
qtcreator
```

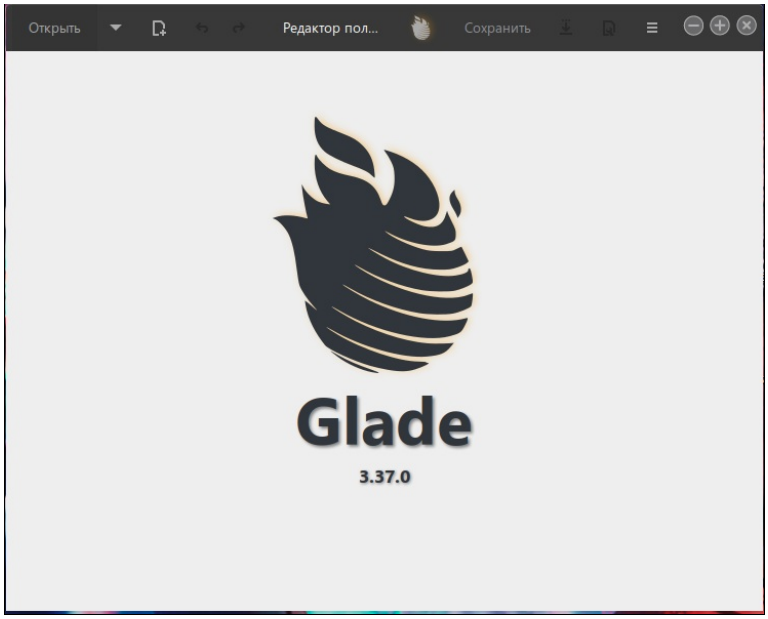


Установка Glade

Glade - это приложение для визуального создания графических интерфейсов на **GTK+**.

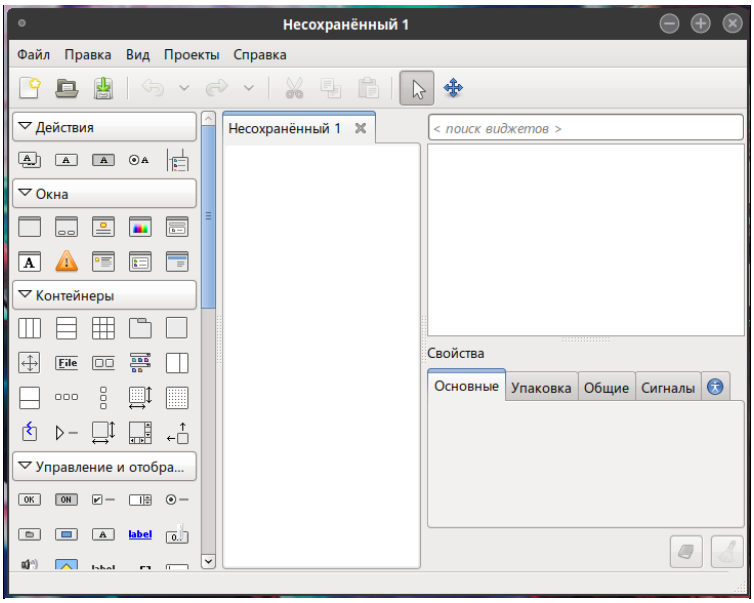
Установка производится командой:

```
dnf install glade
```



Также для поддержки старого типа **ui** файлов **GTK2** в РЕД ОС есть возможность поставить **glade** следующей командой:

```
dnf install glade3
```



Запуск доступен из «**Меню**» - «**Программирование**» - «**Glade**».

Установка Code::Blocks

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Codeblocks - 20.03

Code::Blocks — свободная кроссплатформенная среда разработки.

Code::Blocks написана на **C++** и использует библиотеку **wxWidgets**. Имея открытую архитектуру, может масштабироваться за счёт подключаемых модулей. Поддерживает языки программирования **C**, **C++**, **D**, **Fortran**.

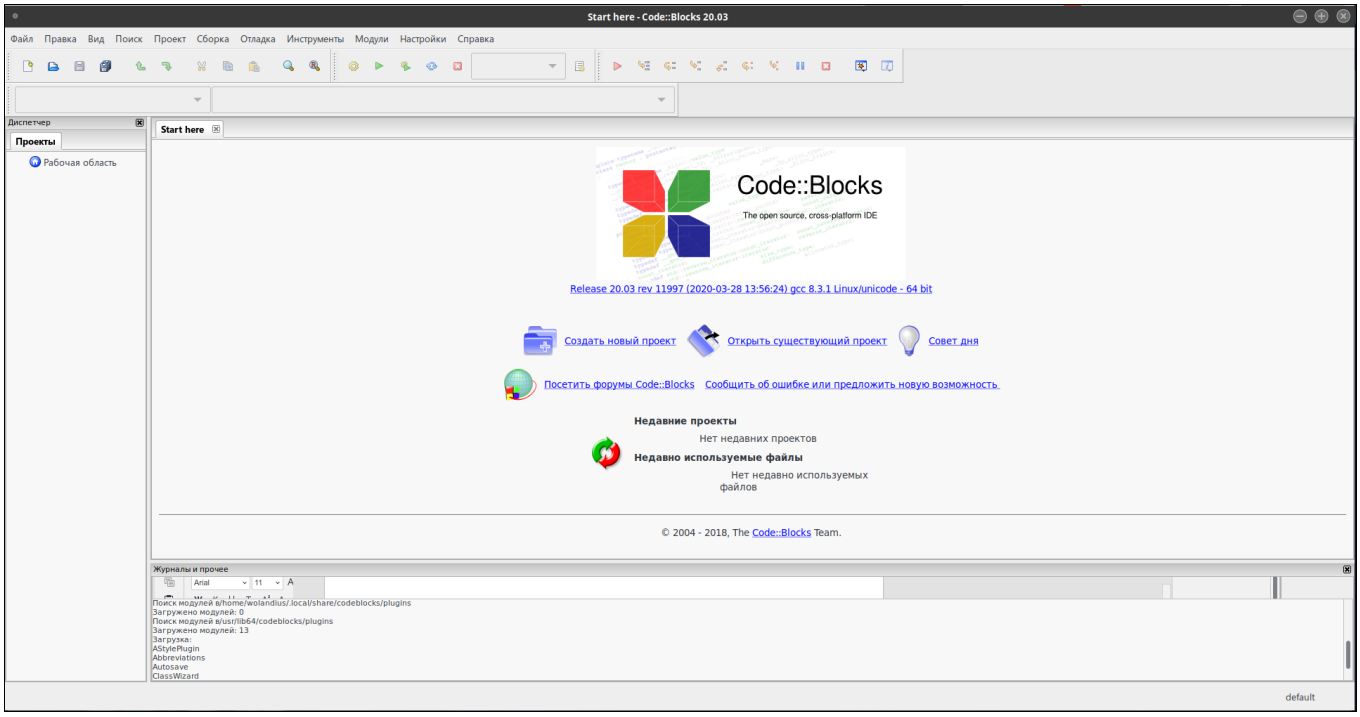
Для установки программы перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

```
dnf install codeblocks
```

Запуск *IDE* доступен из «**Меню**» - «**Программирование**» - «**Среда разработки Code::Blocks**».



Установка Visual Studio Code

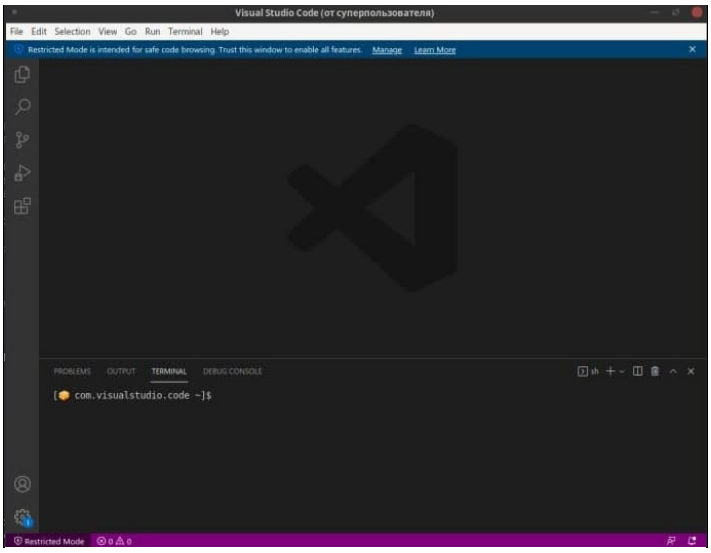
Для установки данной многофункциональной среды разработки потребуется установить **flatpak** в соответствии с инструкцией «Flatpak - изолированная среда для запуска приложений» и добавить репозиторий **flathub** с помощью команды, указанной в п. «Добавление репозиториев».

Следующим шагом является установка **vscode**, для этого потребуется выполнить следующее действие:

```
flatpak install flathub com.visualstudio.code
```

Дождитесь завершения загрузки и запустите **vscode** из «**Меню**» - «**Программирование**» либо запустите программу, выполнив команду в терминале:

```
flatpak run com.visualstudio.code
```



Установка VSCodium

Установка
Изменение языка интерфейса
Установка плагинов

Окружение

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Codium 1.66.1

VSCodium - это ответвление популярного редактора кода **Microsoft Visual Studio**. Он построен с использованием наработок проекта **Atom** и платформы **Electron**, основанной на кодовой базе **Chromium** и **Node.js**. Редактор предоставляет встроенный отладчик, инструменты для работы с **Git**, средства рефакторинга, навигации по коду, автодополнения типовых конструкций и контекстной подсказки. Поддерживается более 100 языков программирования и технологий. Для расширения функциональности **Visual Studio Codium** предоставляется возможность установки дополнений.

Вы можете подробнее ознакомиться с установкой и работой в **VSCodium**, просмотрев наши обучающие видео:

- на **RuTube** — Установка IDE VSCodium в РЕД ОС;
- в **Яндекс.Дзен** — Установка IDE VSCodium в РЕД ОС;
- в **VK Видео** — Установка IDE VSCodium в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **vscodium** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install codium
```

После установки запуск программы доступен из «**Меню**» — «**Программирование**» — «**VSCodium**» или через терминал (с правами локального пользователя) командой:

```
codium
```

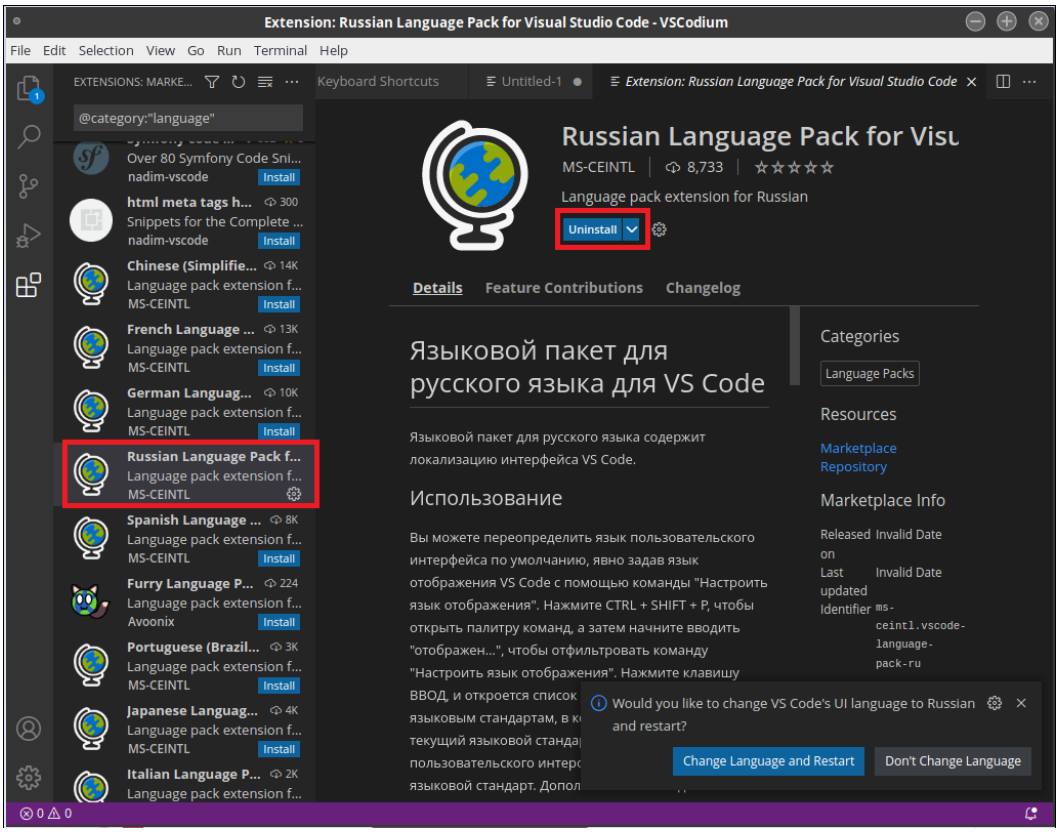
При первом запуске появится окно настройки оформления.

Изменение языка интерфейса

Для изменения языка интерфейса откройте меню **Command Palette** на вкладке **View** и введите **Configure Display Language**.

В появившемся списке выберите нужный пакет языков. Если он отсутствует, нажмите **Install additional languages**.

В строке поиска введите название языкового пакета, например «**Russian Language Pack**» и нажмите **install**.



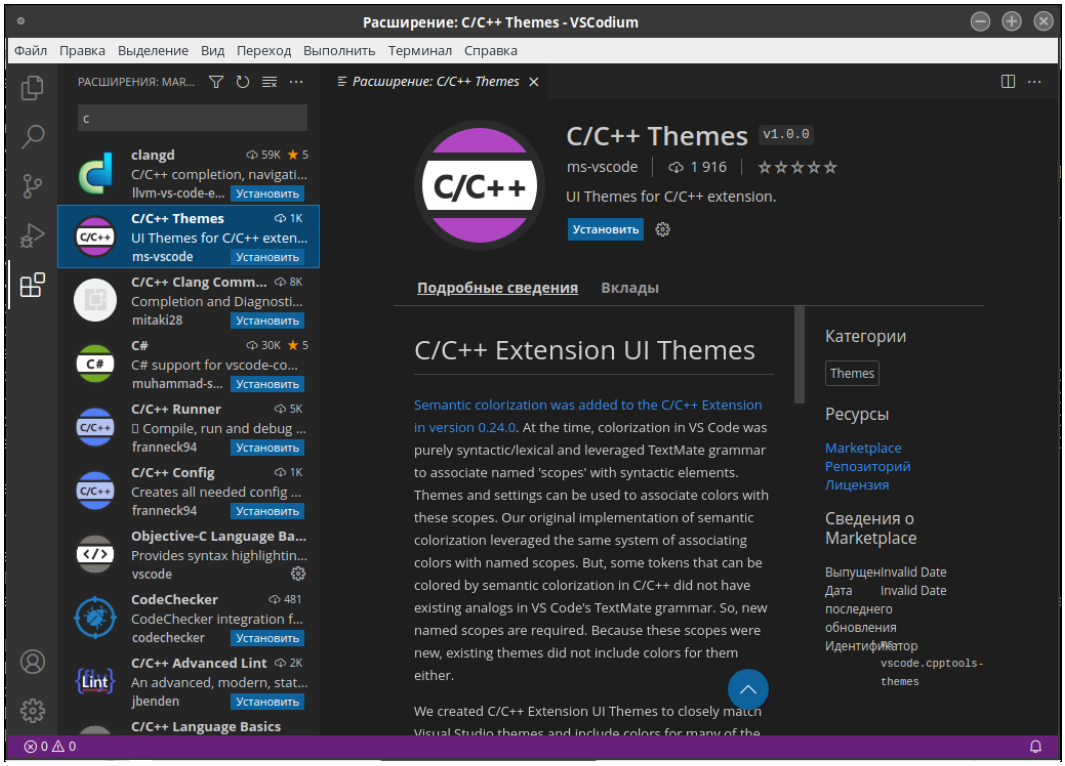
После завершения установки нажмите на кнопку **Change Language and Restart**, чтобы перезапустить **VSCodium**. После перезагрузки программы будет применён выбранный язык.

Установка плагинов

Для установки и просмотра плагинов выберите пункт **Расширения** на панели слева или нажмите сочетание клавиш **Ctrl+Shift+X**.

Введите название плагина в строке поиска, выберите дополнение и нажмите **install**.

Каждое расширение в списке включает краткое описание, имя издателя, количество загрузок и пятизвездочный рейтинг.



Установка Atom

Настройки Atom
Command Palette
Открытие, изменение и сохранение файла
Подсветка синтаксиса
Подсветка ошибок
Контроль версий
Автоматическое форматирование
Префиксы в CSS

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** atom-1.59.0-2

ВАЖНО!

С 15 декабря 2022 г. поддержка текстового редактора Atom прекращена. Основной функционал редактора по-прежнему доступен за исключением скачивания и установки дополнительных расширений.

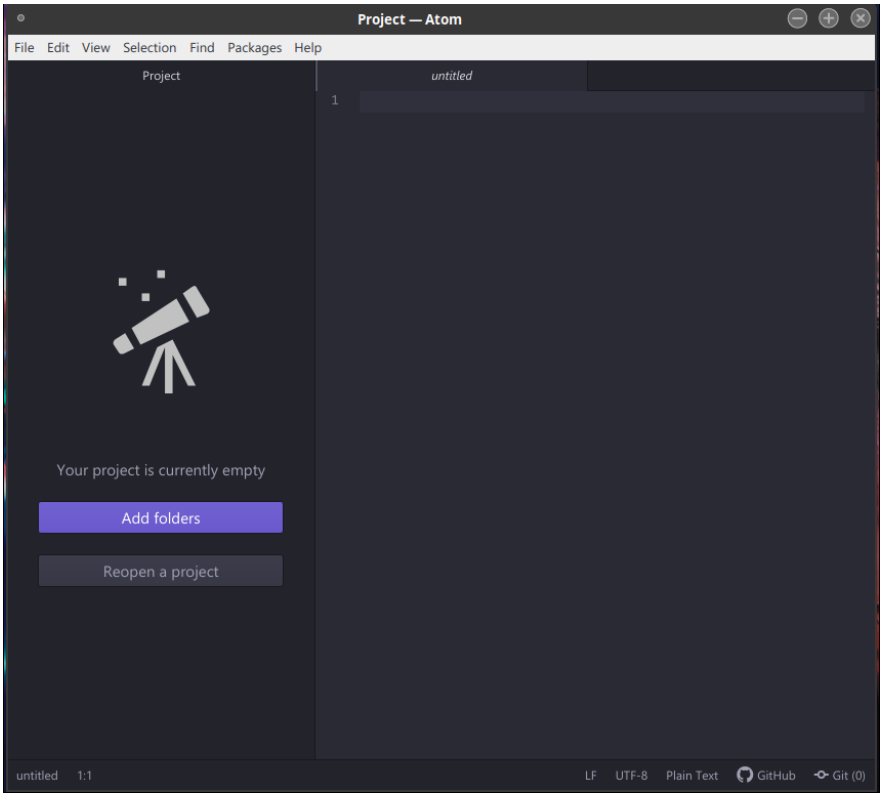
Atom — бесплатный текстовый редактор с открытым исходным кодом для **Linux**, **macOS**, **Windows** с поддержкой плагинов, написанных на **JavaScript** и встраиваемых под управлением **Git**.

Большинство плагинов имеют статус свободного программного обеспечения, разрабатываются и поддерживаются сообществом.

Установка в РЕД ОС 7.3 доступна следующей командой (с правами пользователя **root**):

```
dnf install atom
```

Запуск доступен из «**Меню**» - «**Стандартные**» - «**Atom**».

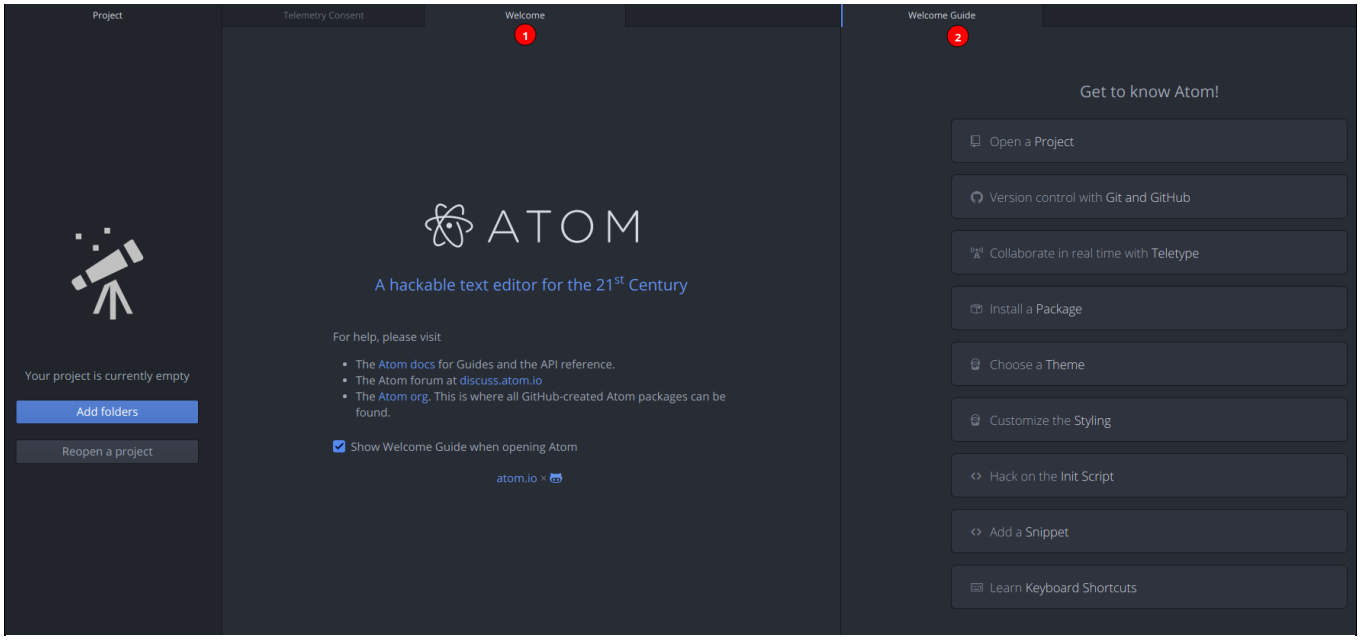


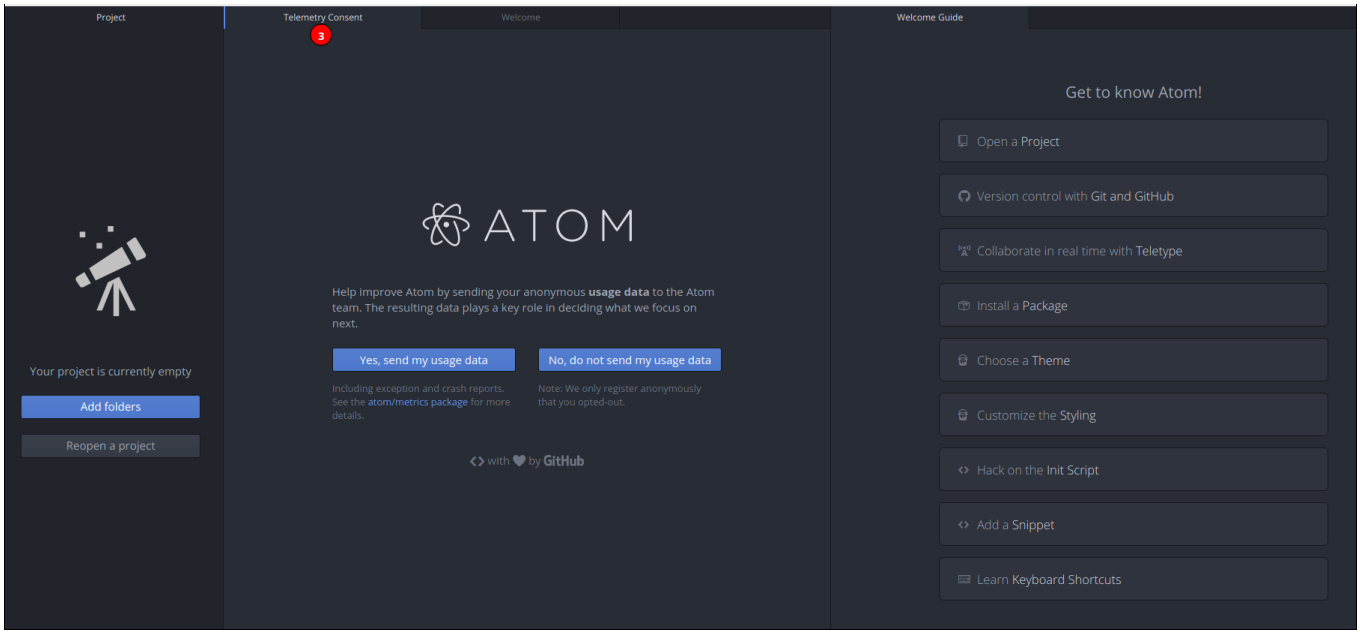
Преимущества **Atom**:

- наличие большого количества бесплатных плагинов, которые можно загружать прямо из интерфейса программы;
- редактор совместим со всеми распространенными языками программирования;

- автоматическая подсветка синтаксиса;
- удобные инструменты для совместного режима работы.

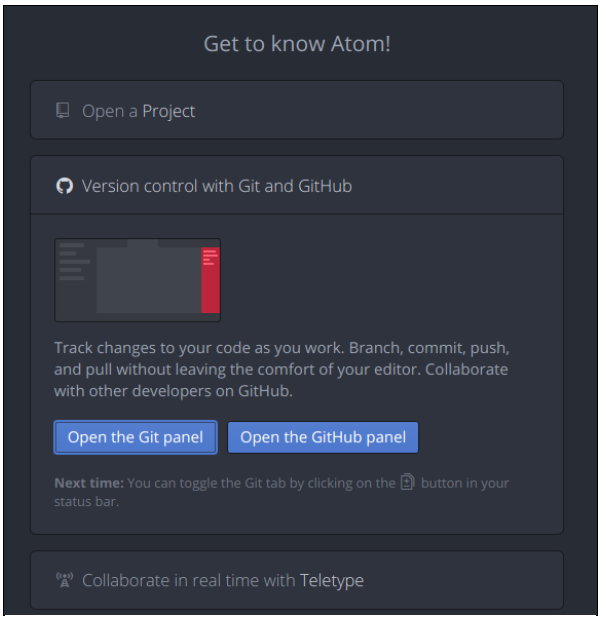
При запуске **Atom** сразу открываются три вкладки «**Welcome**», «**Welcome Guide**» и «**Telemetry Consent**».





На вкладке «**Welcome**» указаны ссылки на официальный сайт разработчика, документацию и публикацию проектов на **github.com**.

Вкладка «**Welcome Guide**» содержит перечень подсказок по функционалу редактора в виде панелей, разворачивающихся при нажатии. Фактически эти панели являются быстрым инструментом для настройки программы.



Внутри каждой панели находится краткое описание функции с кнопками для быстрого перехода к настройке, а также указан альтернативный способ перехода к ней.

Настройки Atom

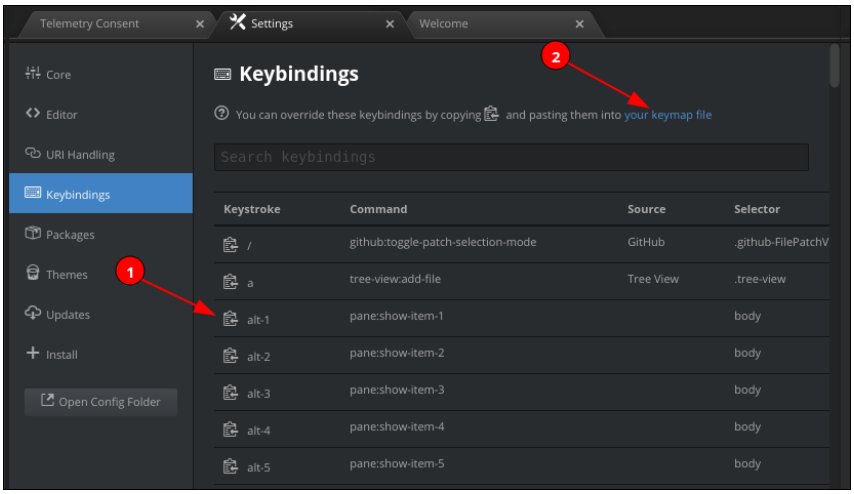
Настройки редактора **Atom** открываются через пункт меню программы «**Edit**» - «**Preferences**» - «**Settings**». В них доступны разделы *Core*, *Editor*, *URl Handling*, *Keybindings*, *Packages*, *Themes*, *Updates*, *Install*.

Core - основные настройки. Здесь настраиваются параметры пользовательского интерфейса: звуковые сигналы, закрытие пустых панелей и пустых окон, кодировка, используемая по-умолчанию для записи и чтения файлов, автоматическое обновление программы и прочее.

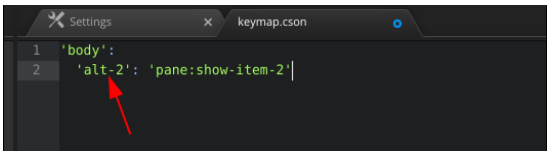
В **Editor** настраиваются шрифты, отступы, длина отступа, длина строки, чувствительность прокрутки, способ переноса и всё, что связано с редактированием текста.

URI Handling - обработка специальных URI, запускаемых системой.

Keybindings - горячие клавиши или сочетания клавиш. Если необходимо изменить сочетание клавиш для выполнения какого-либо действия, нажмите на иконку «**Скопировать**» () в строке нужной комбинации, перейдите по ссылке «**your keymap file**».



Вставьте строки из буфера обмена и пропишите желаемое сочетание клавиш.



Packages - установленные пакеты (расширения).

Themes - выбор тем пользовательского интерфейса **Theme UI** и тем подсветки синтаксиса **Theme Syntax**, по умолчанию доступны

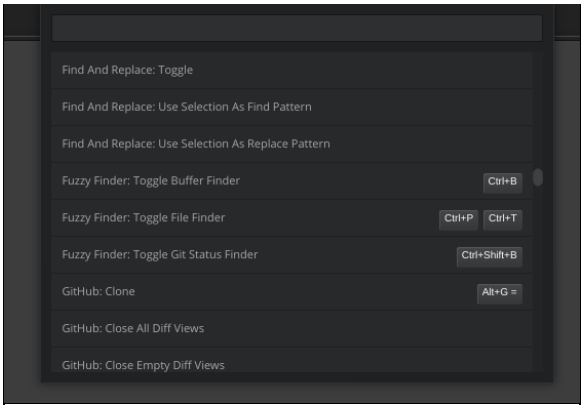
светлая и тёмная.

Updates - проверка обновлений.

Install - установка расширений и тем интерфейса.

Command Palette

Одной из самых важных команд **Atom** является **Палитра команд** (*Command Palette*), она представляет собой поисковое меню, позволяющее осуществлять быстрый переход к настройкам редактора и выполнять большинство его функций. Вызывается нажатием сочетаний клавиш «*Ctrl + Shift + P*» в области редактора. Палитра команд также показывает, есть ли связанные клавиши у запрашиваемой команды.



Открытие, изменение и сохранение файла

Для открытия файла доступен пункт основного меню «**File**» - «**Open file...**» или комбинация клавиш «*Ctrl + O*».

Чтобы сохранить файл, вы можете выбрать пункт меню «**File**» - «**Save**» или нажать «*Ctrl + S*».

Сохранить текущий контент в своем редакторе под другим именем файла можно в «**File**» - «**Save as**» или нажав «*Ctrl + Shift + S*».

Сохранить все открытые файлы в **Atom** можно в «**File**» - «**Save All**».

Поскольку, чаще всего работа производится сразу с несколькими файлами, объединенными в проект, **Atom** предоставляет возможность открытия каталога с файлами в «**File**» - «**Open Folder**». Чтобы добавить несколько каталогов в текущее окно, нужно выбрать «**File**» - «**Add Project Folder**» или нажать сочетание клавиш «*Ctrl + Shift + A*».

В открытом проекте можно легко найти и открыть любой файл с помощью связок клавиш «*Ctrl + T*» или «*Ctrl + P*», в результате чего вверху появится строка поиска. Поиск только по открытым в данный момент файлам осуществляется сочетанием клавиш «*Ctrl + B*».

Подсветка синтаксиса

Для большинства языков программирования, таких как *PHP*, *HTML*, *Json*, *SQL*, *XML*, *CSS*, *CoffeeScript*, *JavaScript*, Java, *C/C++*, *Go* подсветка синтаксиса включена по умолчанию. Для некоторых других языков может потребоваться установка дополнения atom-twig.

Подсветка ошибок

В **Atom** для подсветки ошибок на лету используется интерфейс линтеров. Есть общий пакет **Linter**, а также реализация проверки для разных языков. Для подсветки ошибок в *PHP*, *CSS*, *JSON* и *HTML* необходимо установить следующие пакеты: linter, linter-ui-default, linter-php, linter-csslint, linter-json-lint, linter-htmllint.

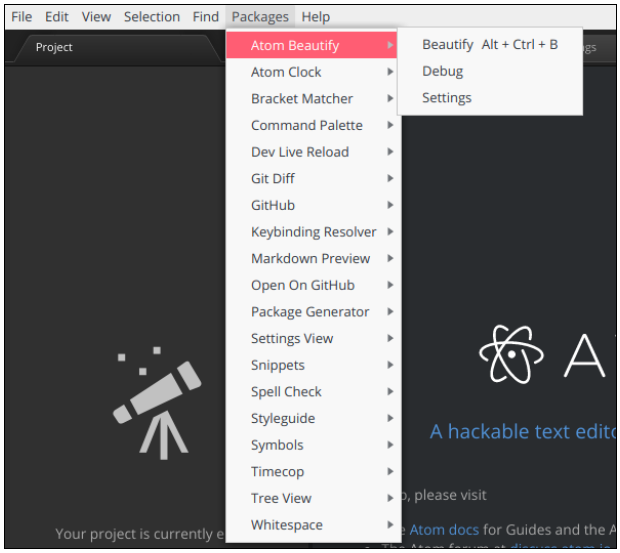
Контроль версий

В **Atom** можно интегрировать контроль версий **Git**, установив пакет git-plus. Если в каталоге проекта есть Git-репозиторий, вы будете видеть внесенные изменения, а также их текущее состояние. Для внесения изменений в проект нажмите на кнопку «**Git**», затем выберите измененные файлы, напишите комментарий и нажмите выполните «**Commit to <имя_ветки>**». Рядом с кнопкой **Git** находятся кнопки, предназначенные для переключения между ветками и публикации изменений в удаленный репозиторий.

Автоматическое форматирование

Очень удобная функция в популярных средах обработки. Позволяет исправить форматирование кода нажатием одной клавиши. В Atom автоматическое форматирование доступно при установке пакета atom-beautify. Существуют также другие пакеты для этой функции, например, php-cs-fixer.

После установки они будут доступны в меню «**Packages**».



Префиксы в CSS

Префиксы в CSS позволяют обращаться к определенному браузеру и задавать свойства, именуемые только для него (**-webkit**, **-moz**, **-ms**). **Atom** позволяет автоматизировать расстановку префиксов в CSS для разных браузеров, используя пакет autoprefixer.

После установки этого пакета необходимо выделить нужный фрагмент кода, открыть меню «**Packages**» - «**Command Palette**» - «**Toggle**». Далее набрать в строке поиска **autoprefixer** и нажать **Enter**. После этого префиксы в CSS **Atom** будут автоматически установлены.

Установка Arduino IDE

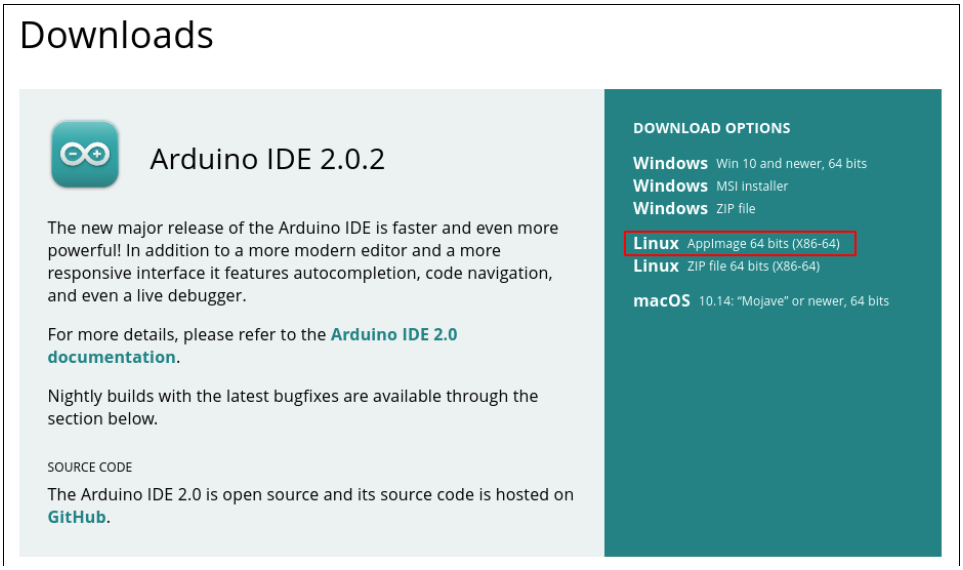
Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** arduino IDE 2.0.2

Arduino IDE — интегрированная среда разработки, предназначенная для создания и загрузки программ на платформу **Arduino**.

Для установки **Arduino IDE** перейдите на официальный сайт разработчика.

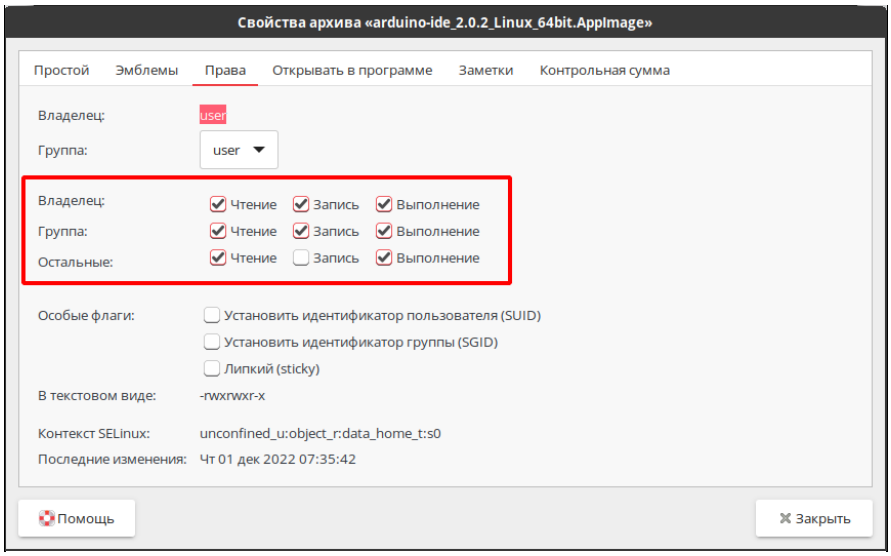
В разделе **Downloads** выберите «**Linux AppImage 64 bits (x86-64)**» и скачайте приложение.



Для запуска приложений в формате *Applimage* необходимо назначить файлу права на исполнение. Сделать это можно двумя способами:

1. Через графический интерфейс.

Перейдите в папку с загруженным файлом, вызовате контекстное меню, нажав по файлу ПКМ, выберите пункт «**Свойства**». После этого во вкладке «**Права**» активируйте флаг пункта «**Выполнение**» для необходимых пользователей и групп.



2. Через командную строку (потребуются права администратора или суперпользователя системы).

В терминале перейдите в папку с загруженным файлом (в примере **/home/user/Загрузки/**):

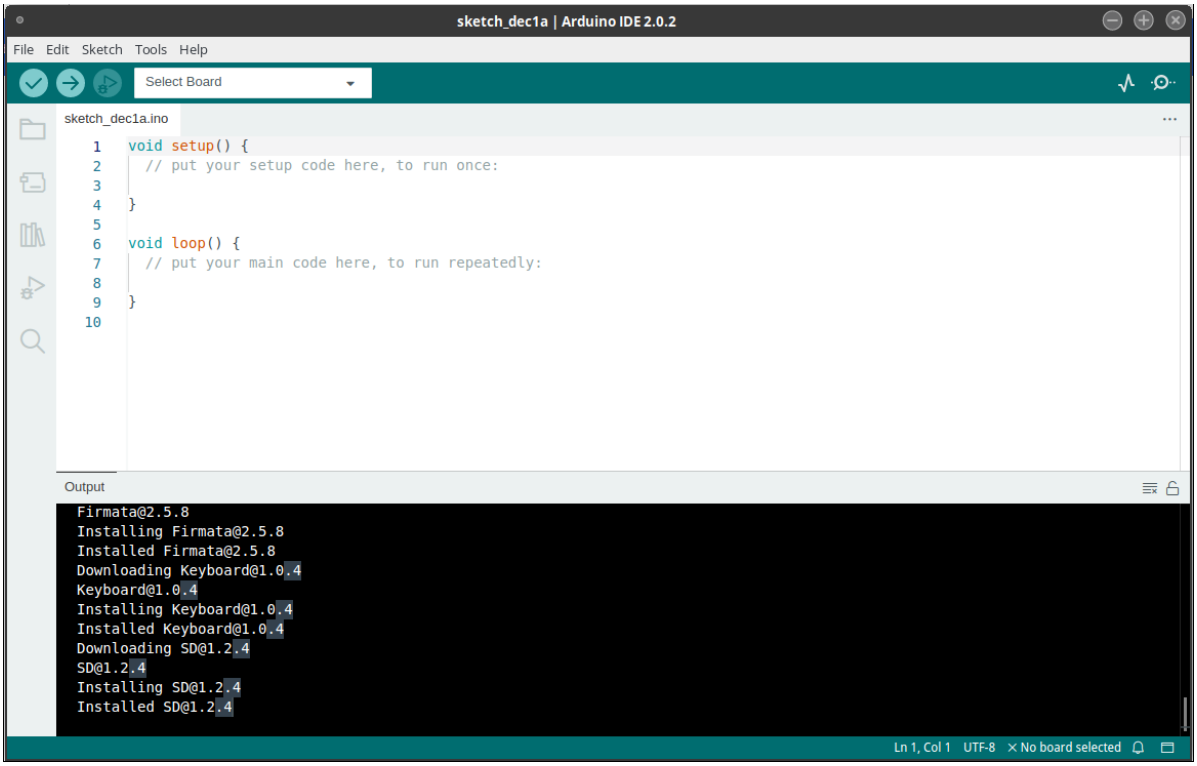
```
cd /home/user/Загрузки/
```

и выполните команду:

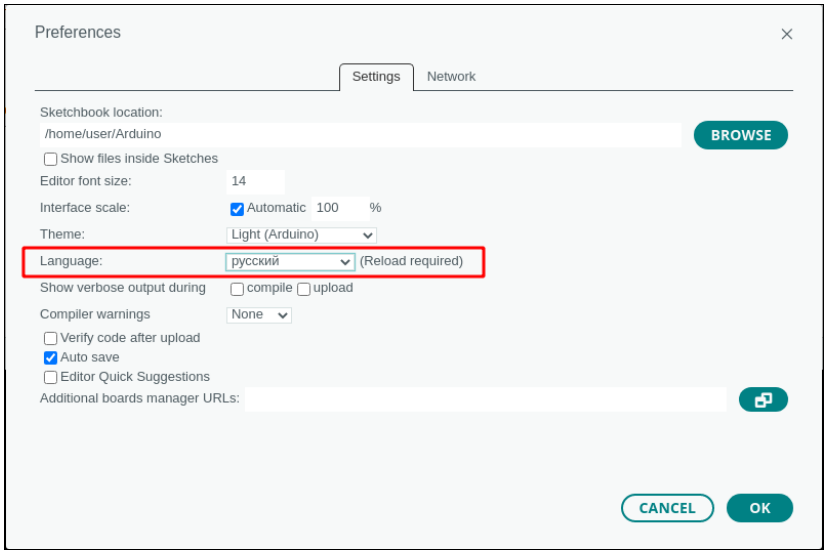
```
chmod +x arduino-ide_2.0.2_Linux_64bit.AppImage
```

Теперь приложение можно запустить, кликнув ЛКМ по файлу формата **.Applimage** или набрав в командной строке (с правами локального пользователя):

```
./arduino-ide_2.0.2_Linux_64bit.AppImage
```



Для смены языка программы выберите пункт меню «**File**» - «**Preferences...**», в открывшемся окне настроек выберите из списка необходимый язык (параметр **Language**).

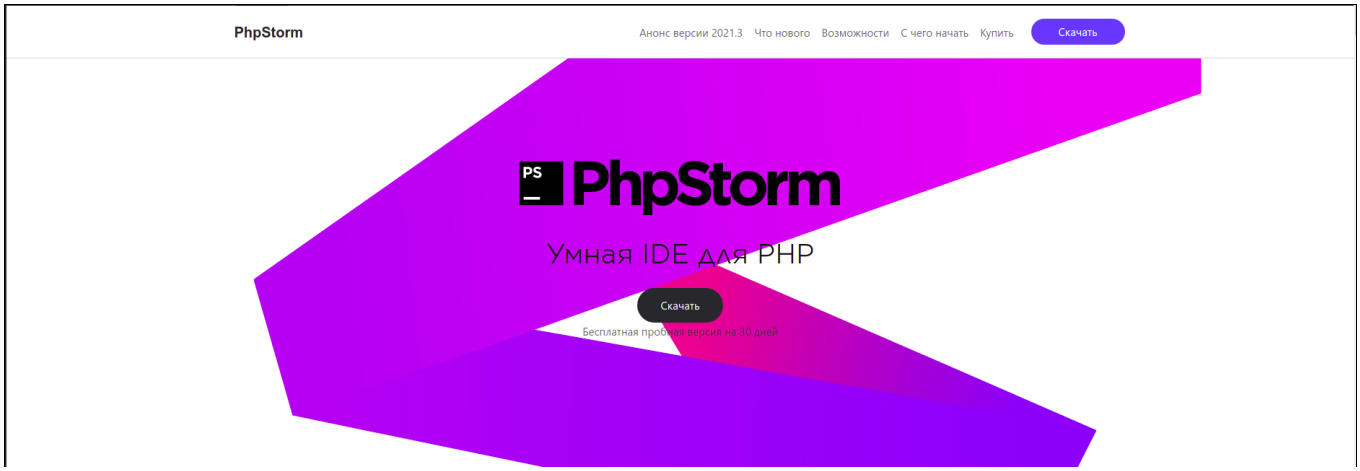


Здесь также доступны общие настройки интерфейса программы.

Установка PhpStorm

PhpStorm — коммерческая кросс-платформенная интегрированная среда разработки для **PHP**. Разрабатывается компанией **JetBrains** на основе платформы **IntelliJ IDEA**.

Скачать данную *IDE* можно по ссылке с официального сайта.



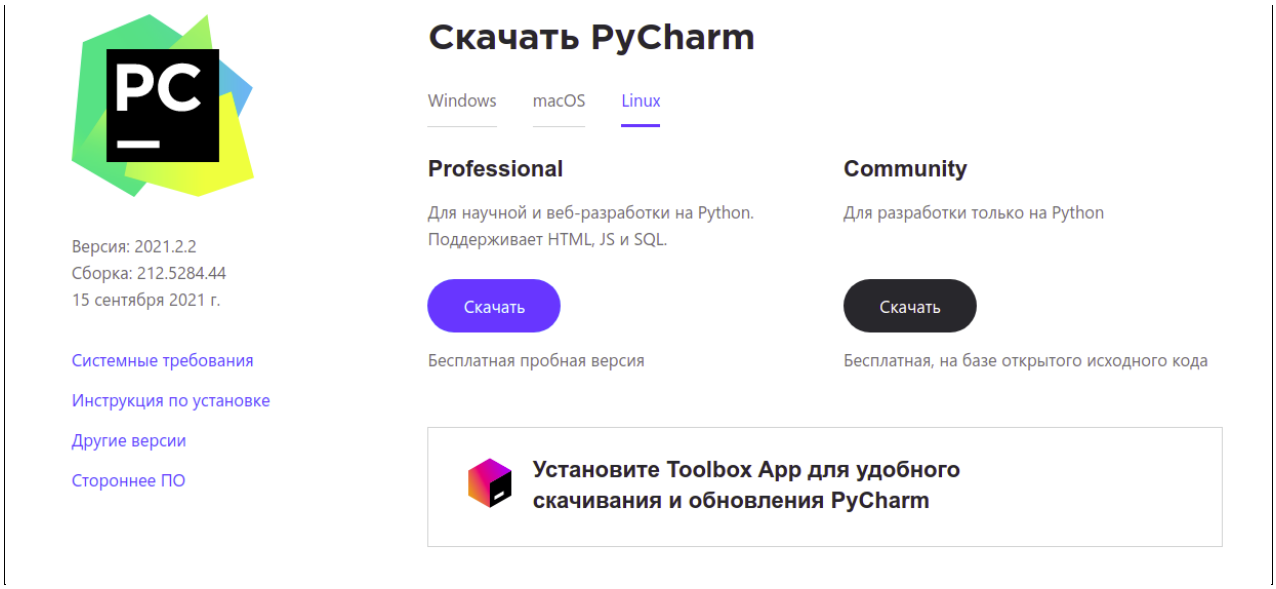
После скачивания необходимо распаковать архив **PhpStorm-202x.x.x.tar.gz**.

Для запуска перейдите в папку **PhpStorm-21xxx/bin** и запустите файл **phpstorm.sh**.

Установка PyCharm

Для установки данной многофункциональной среды разработки вам потребуется перейти на сайт разработчика данного ПО.

Выберите **community** или **professional** версию, нажмите кнопку «**Скачать**» и дождитесь завершения загрузки **tar.gz** архива.



Затем распакуйте архив в удобную для вас директорию.

Перейдите по пути **<путь_к_директории>/pycharm-202x.x/bin** в файловом менеджере или в терминале с помощью команды, например:

```
cd /home/user/Загрузки/pycharm-community-2022.1.3/bin/
```

Для начала установки вам потребуется запустить файл **pycharm.sh**:

```
./pycharm.sh
```

BlueFish - ПО для создания и редактирования интернет-приложений

Установка
Описание программы
Пример работы
Настройка CSS

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** bluefish-2.2.12-1

BlueFish — это текстовый редактор, представляющий собой интегрированную среду разработки (IDE). **BlueFish** основан на программе **KompoZer**, которую выпускало сообщество Mozilla как редактор для создания HTML-страниц или статичных сайтов. **BlueFish** стал полнофункциональным редактором для разработчиков программного обеспечения с поддержкой **HTML**, **CSS**, **JavaScript**, **PHP**, а также **C**, **C++** и ещё ряда языков программирования, однако, в первую очередь, он нацелен на создание веб-контента.

Основные возможности и достоинства **BlueFish**:

- поддержка большого количества открытых вкладок и документов;
- поддержка менеджмента проектов;
- мощный поиск и замена, позволяющие использовать регулярные выражения;
- неограниченное количество отмены и возврата совершенных действий;
- настраиваемая подсветка синтаксиса с поддержкой как пользовательских шаблонов, так и предустановленных шаблонов подсветки для **HTML**, **JavaScript**, **PHP**, **CSS**, **SQL**, **XML**, **Ruby**, **Python** и многих других языков;
- поддержка различных кодировок, по умолчанию работает в **UTF8**;
- хороший мастер для HTML-документов: таблицы, слои, фреймы и пр.;
- подсказки для HTML- и CSS-тегов со всеми их атрибутами;
- функциональные диалоги вставки различных объектов в документы;
- генератор большого количества превью для быстрого создания фотоальбомов или скриншотов страниц;
- настраиваемая пользователем панель инструментов для быстрого доступа к часто используемым функциям;
- автозакрытие тегов для HTML и XML-документов.

Вы можете подробнее ознакомиться с работой редактора **BlueFish**, просмотрев наши обучающие видео:

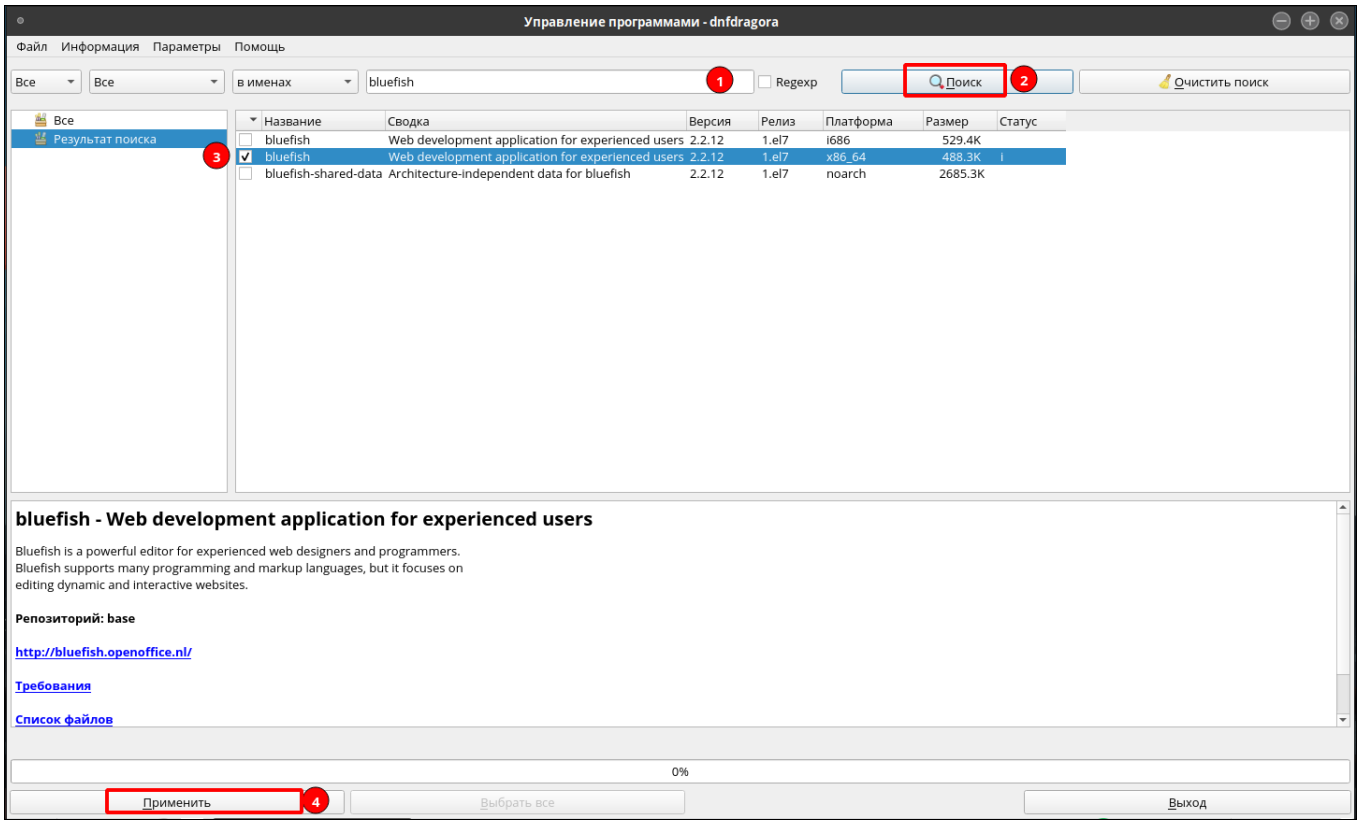
- на **RuTube** — Визуальный редактор для веб-страниц и простых сайтов BlueFish;
- в **Яндекс.Дзен** — Визуальный редактор для веб-страниц и простых сайтов BlueFish;
- в **VK Видео** — Визуальный редактор для веб-страниц и простых сайтов BlueFish.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**bluefish**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install bluefish
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

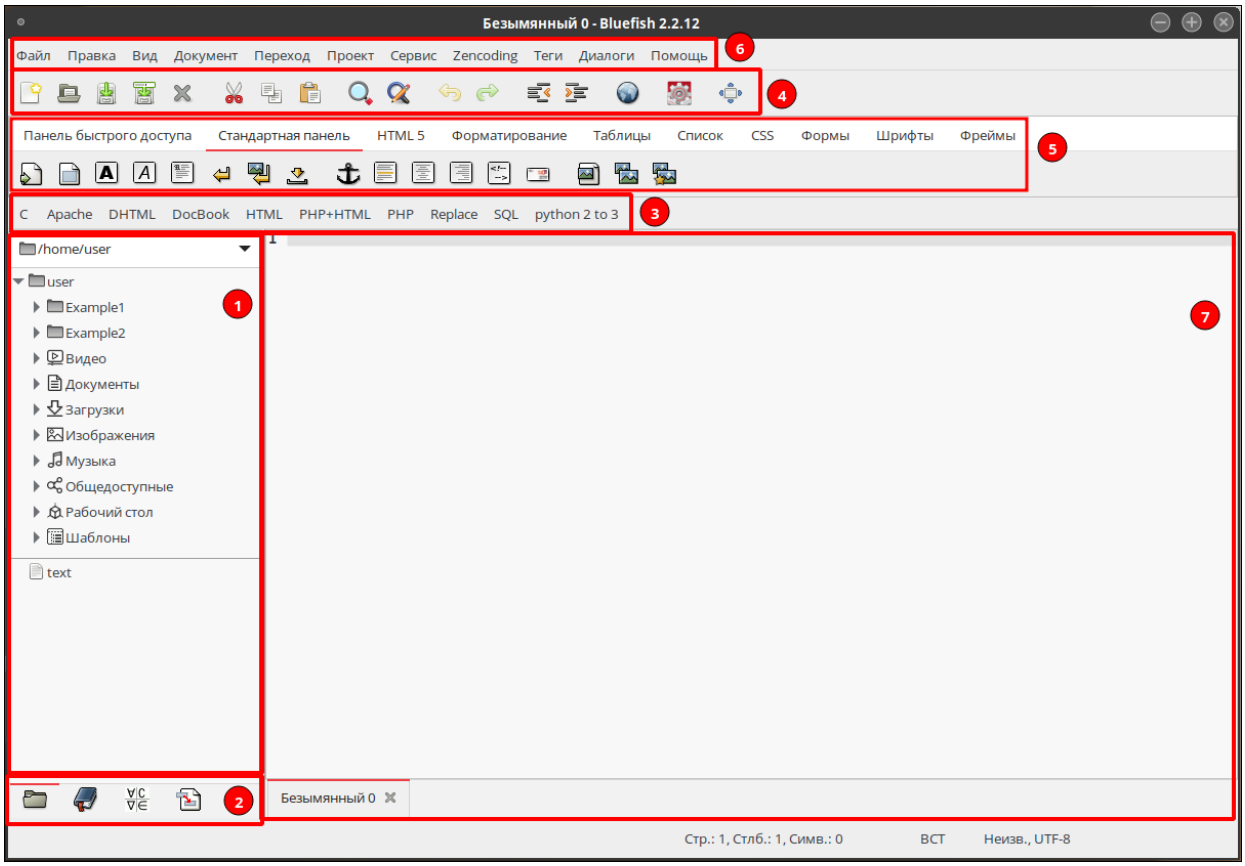
Завершите сеанс пользователя **root**:

```
exit
```

После установки программа будет доступна из «**Главного меню**» - «**Программирование**» - «**Веб-редактор BlueFish**». Если по каким-либо причинам раздел «**Программирование**» не появился в «**Главном меню**», перезагрузите систему.

Описание программы

Главное окно программы выглядит следующим образом:



1 - быстрый доступ к ряду возможностей программы, переключаемых вкладками панели **2**.

2 - панель, позволяющая переключать содержимое блока:

- панель обеспечения быстрого доступа к файловой системе для работы с файлами и каталогами (открывается по умолчанию);
- панель поиска;
- панель визуального выбора символов;
- панель выбора наиболее часто использующихся операций (дублируется на панели **3**).

3 - панель выбора наиболее часто использующихся операций;

4 - главная панель приложения;

5 - панель пиктограмм для определенных действий. В основном действия на данной панели относятся именно к созданию веб-страниц, как статических (на HTML), так и динамических (на PHP и/или JavaScript).

6 - главное меню программы, в котором собраны практически все возможности. Можно убрать показ всех верхних панелей, оставив только главное меню, и осуществлять доступ к каким-либо действиям или возможностям только через него - это может пригодиться в качестве альтернативы полноэкранному режиму - места на экране под текст больше, но и быстрый доступ ко всему функционалу программы остаётся.

7 - рабочая область программы, в котором отображается содержимое файлов проекта, с которым производится работа, и в котором и происходят основные события.

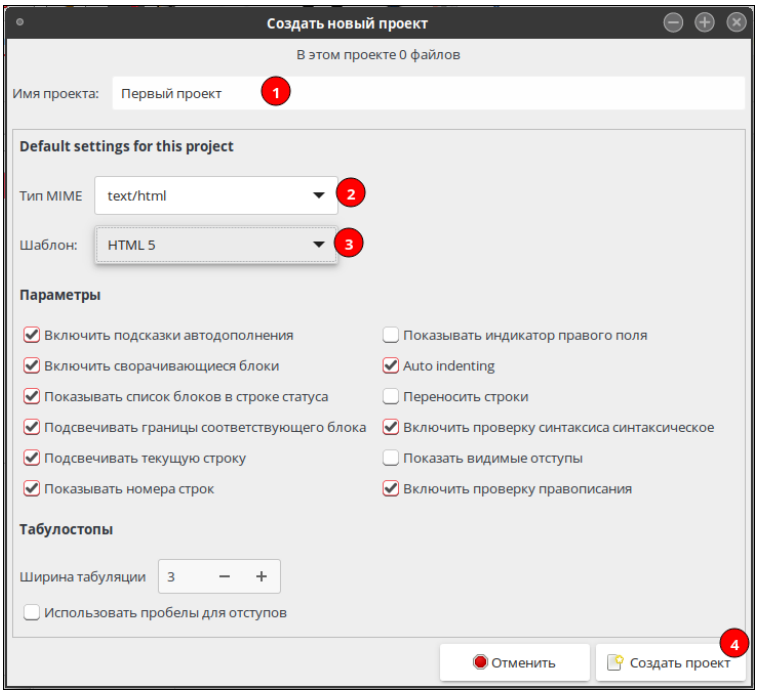
Пример работы

В качестве примера будет рассмотрено создание простейшего проекта с элементарной веб-страницей.

Для создания нового проекта в главном меню выберите «**Проект**» - «**Новый проект**». Откроется окно с базовыми параметрами нового проекта, в котором для HTML-страницы необходимо будет задать некоторые начальные значения:

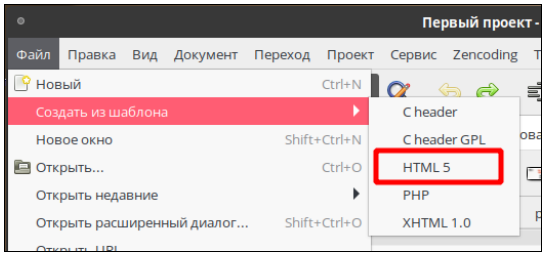
- в поле **Имя проекта** необходимо установить название для проекта;
- в поле **Тип MIME** - выбрать тип создаваемой страницы, в примере **text/html**;
- в поле **Шаблон** - выбрать тип шаблона для страницы, в примере **HTML5**;
- остальные параметры пока оставьте по умолчанию.

После этого нажмите **Создать проект**.

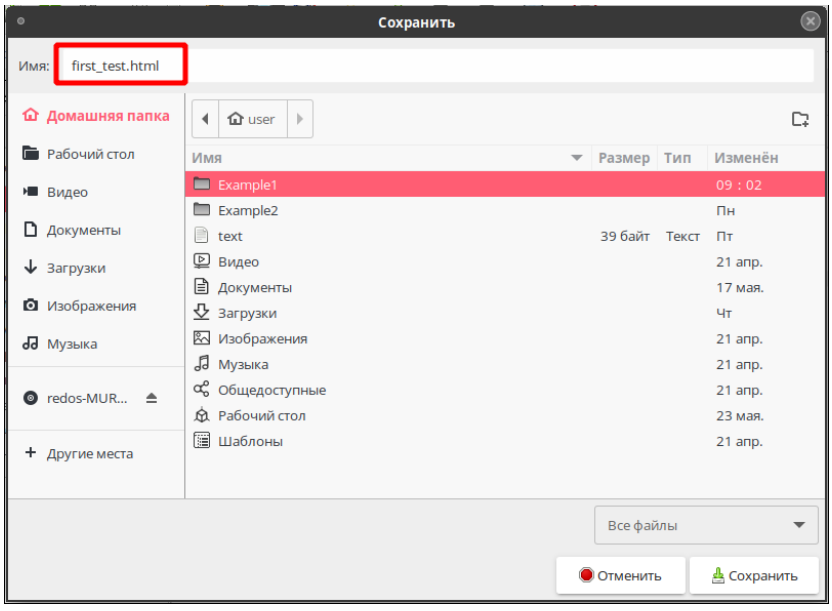


Откроется диалоговое окно с запросом имени файла — программа предлагает сразу сохранить проект. Можно оставить имя, заданное в настройках проекта, можно указать другое имя, также можно выбрать определённый каталог для проекта. После выбора каталога и имени нажмите **Сохранить**. Файл проекта будет иметь расширение **.bfproject**.

Затем в созданный проект необходимо добавить файл, для чего в главном меню выберите «**Файл**» - «**Создать из шаблона**» - «**HTML 5**».



Далее нужно сохранить () созданный файл, явно указав суффикс **.html**, поскольку редактор автоматически не присваивает расширения.



После всех выполненных действий перед вами будет открыта заготовка будущей веб-страницы. Графического способа создания веб-страниц данный редактор не имеет, поэтому работа с **BlueFish** требует хотя бы базовых знаний языка разметки HTML. В остальном редактор будет выводить всплывающие подсказки и описания тех или иных тегов.

Название страницы указывается в тегах `<title>` **Имя страницы** `</title>`.

Основное содержание страницы прописывается в тегах <body> **Содержание страницы** </body>.

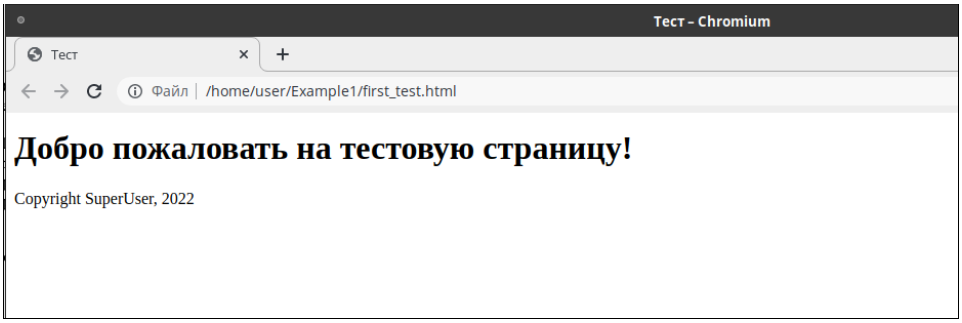
Для примера на страницу будет добавлен заголовок (теги <h1> **Заголовок** </h1>) и некоторый текст (**Текст**), а также авторские права (<footer> **Текст** </footer>).

Теги можно как прописать вручную, так и проставить, используя пункт главного меню «**Теги**» или вкладку **HTML** панели выбора наиболее часто использующихся операций.

Итоговый код страницы будет выглядеть следующим образом:

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title> Тест </title>
</head>
<body>
<h1> Добро пожаловать на тестовую страницу! </h1>
</body>
<footer> Copyright SuperUser, 2022 </footer>
</html>
```

Чтобы проверить, как страница выглядит в браузере, необходимо сначала сохранить внесенные в HTML-файл изменения, а затем в главном меню выбрать «**Сервис**» - «**Команды**» - «**Chromium**» (можно выбрать любой другой установленный в системе браузер).



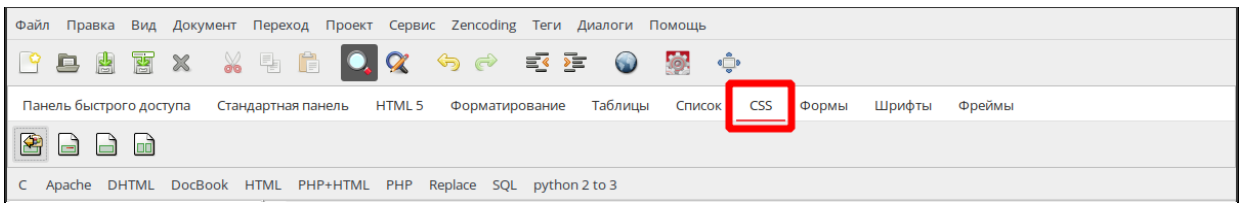
Настройка CSS

Для оформления страницы также можно применять различные стили. Для этого необходимо подключить таблицу стилей. Таблица стилей будет иметь расширение **.css**.

В качестве примера будет рассмотрено создание цветного фона для текста с авторскими правами (*Copyright SuperUser, 2022*).

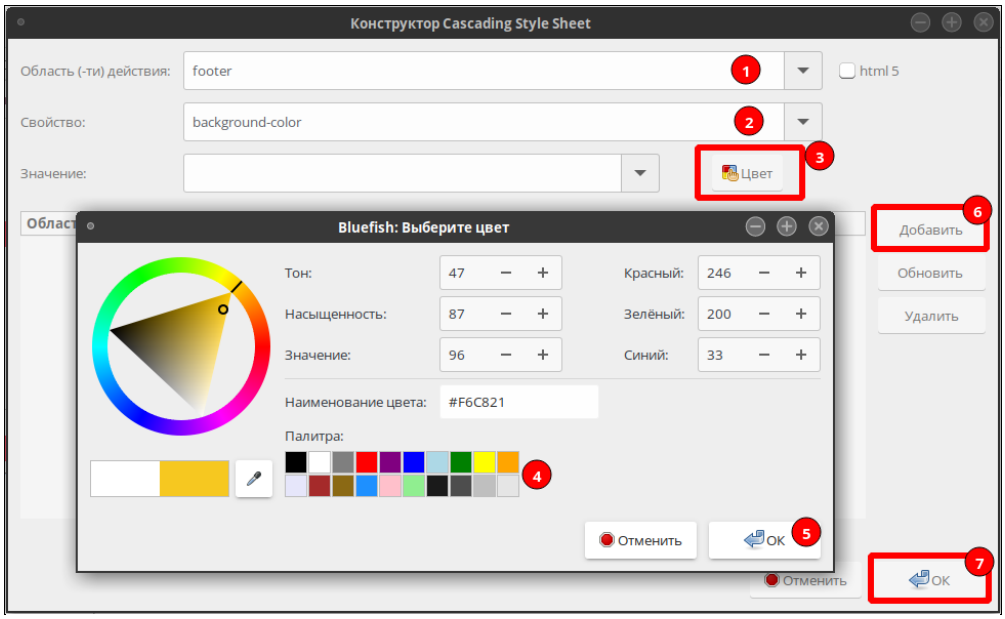
Для этого необходимо создать новый файл в проекте («**Файл**» - «**Новый**») и сохранить его с именем, например, **test.css**. Создание нового безымянного файла происходит сразу из HTML-шаблона, поэтому шаблонное содержимое можно просто удалить.

Для создания цвета фона для тега <footer> в панели быстрого доступа переключитесь на вкладку « **CSS**».



На панели выберите первую пиктограмму «**Создать таблицу стилей**» (), после чего откроется окно создания таблицы.

Укажите в «**Области действия**» тег footer, в поле «**Свойство**» из выпадающего списка выберите background-color, кнопка «**Цвет**» станет активной. Нажмите на кнопку «**Цвет**» для удобного выбора нужного цвета из палитры.



Нажмите«**ОК**». Заполнив все поля в окне, нажмите на кнопку « **Добавить**», затем «**ОК**».

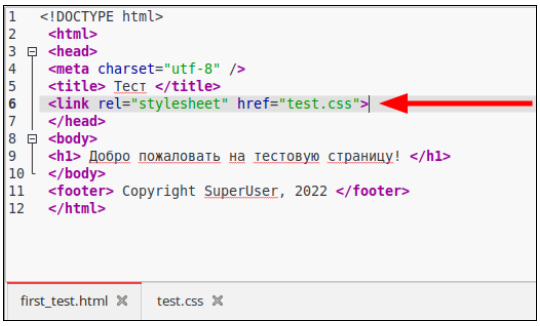
После этого в файл с таблицей стилей будет добавлена запись.

```
footer {
background-color: #F6C820;
}
```

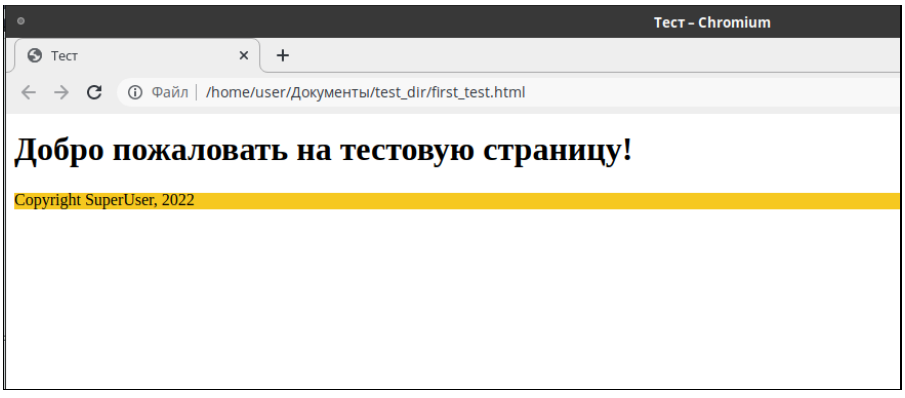
Сохраните CSS-файл.

Для того чтобы созданный стиль применился для созданного ранее HTML-файла, необходимо указать внешнюю таблицу в свойствах гипертекстового документа. Для этого переключитесь на вкладку с файлом HTML и в блоке head добавьте новую строку со следующим содержимым:

```
<link rel="stylesheet" href="test.css">
```



Сохраните документ, перейдите в браузер и обновите веб-страницу.



Основные понятия

Менеджер пакетов **RPM** (**RPM Package Manager**) — это система управления пакетами программного обеспечения, используемая в ряде операционных систем семейства GNU/Linux.

Пакет RPM состоит из архива **cpio**, содержащего файлы, и заголовка RPM, содержащего метаданные о пакете. Менеджер пакетов RPM использует эти метаданные для определения зависимостей, места установки файлов и другой информации.

Заголовок файла RPM имеет следующие записи:

- идентификатор файла как RPM-архива,
- цифровая подпись для проверки целостности и подлинности,
- данные о пакете (версия, архитектура, список файлов и т. д.).

После всего этого идёт сам архив с файлами пакета.

Архиватор **cpio** может использовать различные алгоритмы сжатия из имеющихся в системе, например: **lzma**, **xz**, **zstd**.

Существует два типа пакетов RPM:

- исходный пакет (**source RPM**, **SRPM**);
- двоичный пакет (**binary RPM**).

SRPM и двоичный RPM имеют общий формат файла и инструментарий, но имеют разное содержимое и служат разным целям:

- SRPM содержит исходный код, исправления (**patches**) к нему при необходимости и файл спецификации, в котором описывается, как построить (собрать) из исходного кода двоичный пакет;
- двоичный RPM содержит двоичные файлы, созданные из исходных текстов и патчей согласно спецификации. Именно в двоичных пакетах распространяется готовое программное обеспечение среди пользователей.

Файл спецификации (spec-файл) в русскоязычной ИТ-литературе также называют сценарием сборки пакета.

Для работы с пакетами в РЕД ОС используются следующие пакетные менеджеры:

- универсальная утилита **rpm**,
- пакетный менеджер **dnf**.

Преимущества RPM

RPM упрощает распространение, управление и обновление программного обеспечения, созданного для РЕД ОС. Многие поставщики программного обеспечения распространяют своё ПО с помощью обычного архивного файла (например, **tar**-файла). Тем не менее, есть несколько преимуществ в упаковке программного обеспечения в пакеты RPM:

1) *Установка, переустановка, удаление, обновление и проверка пакетов.*

Пользователи могут использовать стандартные инструменты управления пакетами для установки, переустановки, удаления, обновления и проверки пакетов.

2) *Использование базы данных установленных пакетов.*

Поскольку RPM поддерживает базу данных установленных пакетов и их файлов, пользователи могут легко запрашивать информацию и проверять пакеты в своей системе.

3) *Использование метаданных.*

Каждый пакет RPM содержит метаданные, описывающие компоненты пакета, версию, релиз, размер, URL проекта, инструкции по установке и так далее.

4) *Упаковка исходных текстов программного обеспечения в исходные и двоичные пакеты*.

RPM позволяет брать исходные тексты из источников программного обеспечения и упаковывать их в исходные и двоичные пакеты для пользователей. В исходных пакетах имеются нетронутые исходные тексты вместе с любыми патчами (если таковые требуются и применяются при сборке), а также полные инструкции по сборке. Такая конструкция облегчает обслуживание пакетов по мере выпуска новых версий программного обеспечения.

5) *Добавление пакетов в репозитории.*

Можно добавить свой пакет в репозиторий, который позволит клиентам легко находить, развёртывать и обновлять программное обеспечение.

6) *Цифровая подпись ваших пакетов.*

Используя ключ подписи **GPG**, можно подписать пакет цифровой подписью, чтобы пользователи могли проверить подлинность программного обеспечения.

Поименование пакетов

Каждый пакет имеет своё собственное уникальное имя, которое складывается из нескольких составляющих (полей) строго в соответствии со следующими принципами:

1) Разделителем полей является символ «**-**» (минус);

2) Первое поле — имя или название (**Name**) программного обеспечения, может совпадать с названием проекта, но возможно задавать и собственное имя, если это обусловлено какими-либо корпоративными принципами или во избежание совпадений имён с уже существующими пакетами в репозитории дистрибутива.

Окончанием имени в названии файла пакета считается первый символ «**-**», за которым следует цифра. Например (здесь имя выделено зеленым цветом):

```
openssl-1.0.2-5.el7
openssl10-1.0.2+git26ab4c78-4.el7
openssl_1_0-1.0.2-1.el7
```

3) Второе поле — версия (**Version**) программного обеспечения. Окончанием значения данного поля является первый символ «**-**». Например (здесь версия выделена зеленым цветом):

```
openssl-1.0.2-5.el7
openssl10-1.0.2+git26ab4c78-4.el7
openssl_1_0-1.0.2-1.el7
```

Как видно из примеров, в репозитории могут находиться пакеты с различным названием, но содержащие в себе программное обеспечение с одной и той же версией;

4) Третье поле — релиз (**Release**) пакета. Например (здесь поле релиза выделено зеленым цветом):

```
openssl-1.0.2-5.el7
openssl10-1.0.2+git26ab4c78-4.el7
openssl_1_0-1.0.2-1.el7
```

Цифра до точки задаётся сборщиком пакета. Значение после первой точки в релизе называют суффиксом релиза (в данных примерах — **el7**), который показывает принадлежность пакета к какому-то семейству дистрибутивов. Суффикс релиза можно опускать, хотя это и нежелательно.

Первые три поля названия пакета (имя–версия–релиз) в документации и технической литературе для краткости часто обозначают первыми буквами английских терминов — **NVR** (Name–Version–Release).

Полное имя файла пакета завершается строго определённой строкой:

- для исходных пакетов — **.src.rpm**. Например:

```
openssl-1.0.2-5.el7.src.rpm
openssl10-1.0.2-4.el7.src.rpm
```

- для бинарных пакетов — **.<ARCH>.rpm**, где **<ARCH>** — обозначение архитектуры, под которую собран пакет, т. е. скомпилирован бинарный код, содержащихся в пакете файлов. Различают большой ряд архитектур, из которых наиболее часто используются в РЕД ОС следующие:

```
i686, x86_64, aarch64, noarch
```

В случае **noarch**-пакетов в них располагаются архитектурно-независимые файлы, такие как документация, скрипты, изображения и пр.

Например:

```
openssl-1.0.2-5.el7.i686.rpm
openssl10-1.0.2+git26ab4c78-4.el7.x86_64.rpm
openssl10-docs-1.0.2+git26ab4c78-4.el7.noarch.rpm
```

Значения всех параметров, заносимых в поля имени пакета, определяются в файле спецификации.

Сборочное окружение

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Прежде чем приступать к написанию спецификации и дальнейшей сборке пакета необходимо убедиться, что в системе установлены следующие пакеты:

```
rpm-build rpm-sign rpmdevtools diffutils patch make python-srpm-macros
```

являющие собой минимально необходимый набор, требуемый для обработки сценариев сборки.

Конечно, для сборки реальных проектов могут потребоваться и набор компиляторов **gcc**, и интерпретаторы **python** или **perl**, и многие другие инструменты разработчика, а также дополнительные утилиты по обслуживанию пакетов, в том числе и репозитория. Потребность в дополнительных пакетах определяется или самим разработчиком проекта (если собирается пакет программного обеспечения собственного написания), или согласно документации к программному обеспечению.

ВАЖНО!

Собирая пакеты, **не работайте** под учётными записями с повышенными привилегиями, особенно администратора **root**!

Первым шагом на пути создания пакета RPM является создание структуры каталогов, в которых будут находиться файлы проекта, для чего необходимо выполнить команду:

```
rpmdev-setuptree
tree ~/rpmbuild/

/home/user/rpmbuild/
|-- BUILD
|-- RPMS
|-- SOURCES
|-- SPECS
`-- SRPMS

5 directories, 0 files
```

В результате чего получим в домашней директории пользователя необходимое дерево каталогов. Во время запуска сборки пакета будет создан ещё один подкаталог в этом дереве — **BUILDROOT**. Каждый подкаталог в сборочной директории имеет своё предназначение.

Каталог	Предназначение
BUILD	Директория сборочных каталогов, их содержимое бывает полезно при расследовании неудачной сборки, если выходные данные журналов не содержат достаточной информации.
BUILDROOT	В данной директории формируются псевдо-корневые каталоги, в которые происходит установка скомпилированного ПО для дальнейшего формирования двоичного пакета.
RPMS	Собранные двоичные RPM записываются в подкаталогах для разных архитектур данного каталога.
SOURCES	В данном каталоге размещаются архивы исходного кода, патчи и другие файлы, необходимые для сборки.
SPECS	Каталог для файлов спецификаций.
SRPMS	В данный каталог сохраняются собранные исходные пакеты.

Файл спецификации

Преамбула
Тело спецификации

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Файл спецификации можно рассматривать как «рецепт», согласно которому утилита **rpmbuild** создаёт готовый пакет. В спецификации задаются команды для системы сборки, определяются инструкции в ряде разделов. Фактически спецификация представляет собой сценарий, выраженный языком макросов. Написание спецификации является важнейшим этапом при создании двоичных пакетов программного обеспечения.

Макрос RPM — это прямая текстовая подстановка, осуществляемая на основе раскрытия заданных выражений и условий, реализованная на базе встроенной функциональности сборочной системы. Иными словами, макросы являются псевдонимами для часто используемых фрагментов текста, применение которых сокращает не только объём ввода, но и делает спецификацию легче читаемой и воспринимаемой. Имена макросов начинаются с символа «**%**».

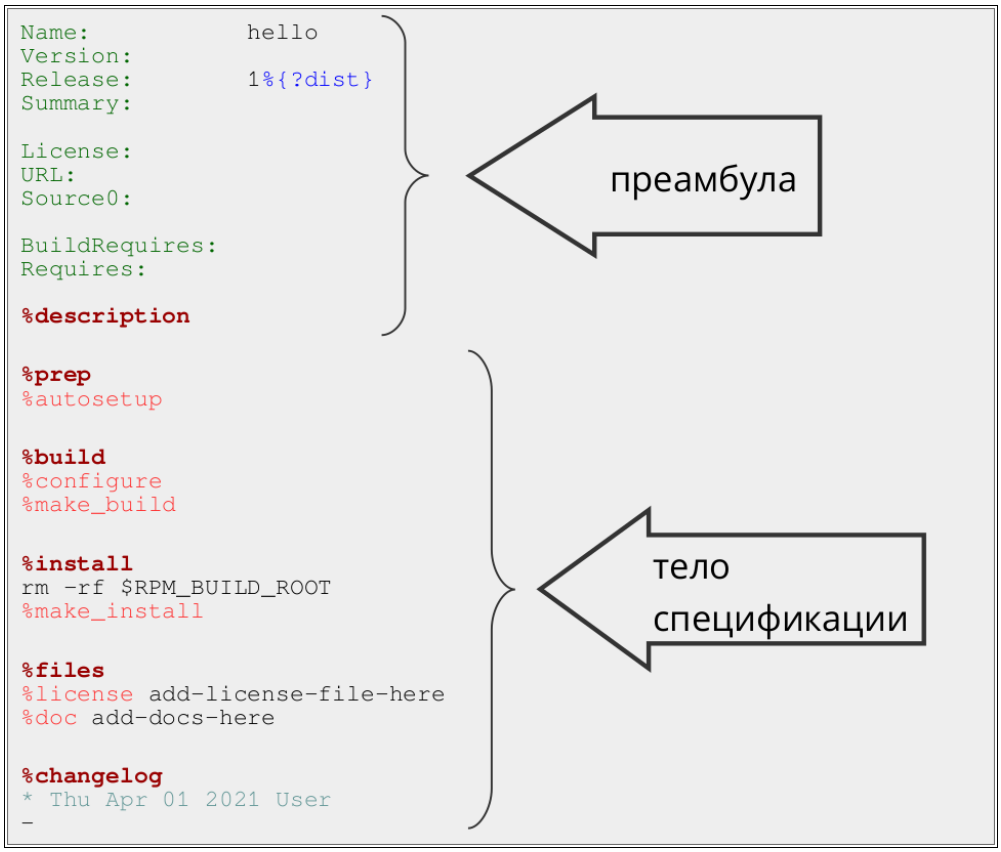
Файл спецификации разделяют на **преамбулу**, содержащую ряд элементов метаданных, которые используются в дальнейшем тексте, и **текст (тело) спецификации**, в котором содержится основная часть инструкций. В русскоязычных источниках преамбулу также называют заголовком спецификации.

Каждый из этих двух разделов сценария сборки содержит как обязательные, так и опциональные подразделы и элементы.

В случае написания спецификации «с нуля» можно создать её заготовку с типовыми блоками с помощью утилиты **rpmdev-newspec**, которой в качестве аргумента указывается имя нового проекта:

```
rpmdev-newspec hello
hello.spec created; type minimal, rpm version >= 4.13.
```

Созданный файл **hello.spec** будет иметь следующее содержимое:



Преамбула

В нижеприведенной таблице перечислены элементы, используемые в преамбуле файла спецификации RPM, которые называются **директивами** или **тэгами**. В таблице жирным шрифтом выделены **обязательные** директивы.

Директивы	Определение
Name	Базовое имя пакета, которое должно совпадать с именем файла спецификации
Version	Номер версии программного обеспечения
Release	Количество раз, когда данная версия программного продукта была собрана. Как правило, при первой сборке конкретной версии пакета значение устанавливается равным 1 и увеличивается на единицу с каждой новой сборкой пакета. После цифры указывают суффикс макросом **%{?dist}**
Epoch	Способ определения взвешенных зависимостей на основе номеров версий. Если директива явно не задана, то значение по умолчанию равно 0. Данный параметр влияет на полную версию пакета при построении зависимостей в базе данных RPM или в репозитории Полная версия выглядит как **Epoch:Version-Release**
Summary	Краткое, однострочное описание пакета
License	Лицензия на упаковываемое программное обеспечение
URL	Полный URL (адрес) для получения дополнительной информации о программе. Обычно это веб-сайт проекта для упаковываемого программного обеспечения
Source[X]	Путь (абсолютный или относительный) или URL-адрес к исходным файлам проекта. Директива может указывать как на сжатые архивы исходных кодов, так и на отдельные файлы. Проект может содержать несколько исходных файлов, тогда для их нумерации вместо **[X]** указывается цифра, например: **Source3**. Если имеется только один исходный файл, то нумерацию можно опустить, указав просто **Source**.
Patch[X]	Файлы патчей, которые при необходимости будут применены к исходному коду. Проект может содержать несколько патчей, тогда вместо **[X]** указывают их номер, например: **Patch2**. Если патч единственный, то номер можно не присваивать (**Patch**)
BuildArch	Явное указание архитектуры, под которую собирается двоичный пакет. Если параметр не задан, то пакет автоматически наследует архитектуру машины, на которой он собран. В случае с архитектурно-независимыми пакетами указание данной директивы обязательно: **BuildArch: noarch**
ExcludeArch	Если программное обеспечение, для которого собирается двоичный пакет, не может работать на определённой архитектуре процессора, то можно исключить эту архитектуру данной директивой
BuildRequires	Список пакетов, разделённых запятыми или пробелами либо указанных по одному в строке с данной директивой, необходимых для компиляции/создания программы или формирования пакета
Requires	Список пакетов, разделённых запятыми или пробелами, необходимых программному обеспечению для запуска после установки. В файле спецификации может быть несколько записей **Requires**, каждая из которых находится в отдельной строке

Provides	Указание дополнительных имён, библиотек или иных сущностей, которые предоставляет данный пакет. Используется для создания псевдонимов пакета, которые можно использовать как в тэгах спецификаций при сборке других пакетов, так и для установки пакета через пакетный менеджер
Obsoletes	Перечисление имён пакетов, которые данный пакет делает устаревшими. При установке данного пакета устаревшие пакеты будут автоматически удалены из системы пакетным менеджером
Confilcts	Перечисление имён пакетов, с которыми конфликтует данный пакет, т. е. все эти пакеты не могут быть одновременно установлены в системе

ВАЖНО!

Каждая директива обязательно разделяется от её значения символом «**:**», между директивой и двоеточием **не должно быть пробелов**!

Например:

```
Name: openssl
Version: 1.0.2
Release: 4%{?dist}
```

Завершается преамбула обязательным блоком описания назначения пакета, идущим после тэга **%description**, в котором, в отличие от директивы **Summary**, даётся развёрнутая информация о пакете. Описание может занимать любое количество строк и быть разбито на абзацы по желанию автора спецификации.

ВАЖНО!

В **одном** файле спецификации может быть описано **несколько** двоичных пакетов!

В таком случае один проект будет представлен несколькими двоичными RPM-файлами. Заголовки других пакетов в подобной спецификации должны начинаться с макроса **%package <ИМЯ_ПАКЕТА>**, причём имя другого пакета тэгом **Name** задавать не нужно — оно будет сформировано из опций указанного макроса. Также можно не указывать версию и релиз, если они совпадают (или должны совпадать по задумке автора спецификации) со значениями таковых же директив всего проекта. Например:

```
Name: superproj
Version: 1.0
Release: 1%{?dist}
Summary: Super Project
...
%description
This is the Super Project from our Company for all people.

%package devel
Summary: Development files for Super Project
...
%descrtiption devel
This package contains libraries and header files for development
with Super Project.
...
```

В результате успешного завершения сборки согласно данной спецификации будут получены два пакета, например (для архитектуры **x86_64**):

```
superproj-1.0-1.el7.x86_64.rpm  и  superproj-devel-1.0-1.el7.x86_64.rpm
```

Тело спецификации

В таблице ниже перечислены основные блоки, используемые в тексте (теле) спецификации, причём **все** они, **кроме %check**, **являются обязательными**.

Важно заметить, что сколько бы двоичных пакетов не было описано в спецификации, **все** ниже приведённые директивы, **кроме**

%files, фигурируют в тексте **только один раз** — разделение на разные двоичные RPM происходит именно в блоках **%files** согласно преамбуле.

Блоки	Определение
%prep	Команды для подготовки программного обеспечения к сборке, например, распаковка архива, указанного в **Source** или **Source0**.
%build	Команды для фактической сборки программного обеспечения в машинный код (для компилируемых языков) или байт-код (для некоторых интерпретируемых языков)
%install	Команды установки/копирования файлов из сборочного каталога в псевдо-корневую директорию
%check	Команды для тестирования программного обеспечения. Данный блок обычно включают в себя модульные тесты
%files	Список файлов для каждого двоичного пакета (если их создаётся несколько по одной спецификации), которые будут установлены в системе конечного пользователя
%changelog	Список изменений, произошедших в пакете между сборками разных версий или релизов

Командами внутри блоков могут быть как макросы сборочной системы RPM, так и вызовы внешних приложений, включая сценарии оболочки.

Если при сборке какого-либо пакета нет необходимости в каком-то блоке, всё равно его название необходимо указать в спецификации. Например, упаковывается тема пиктограмм и компилировать просто нечего при сборке двоичного пакета, то в спецификации такого пакета блок **%build** будет пустым.

Основные макросы

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Как уже говорилось ранее, **макрос RPM** — это прямая текстовая подстановка. Имеется ряд основных макросов, как явно заданных в установленной сборочной системе, так и задаваемых по мере обработки спецификации.

Получить значение заданного в сборочной системе макроса можно с помощью команды

```
rpm --eval %{<ИМЯ_МАКРОСА>}
```

Например, получим значение уже упомянутого выше макроса **%{?dist}**:

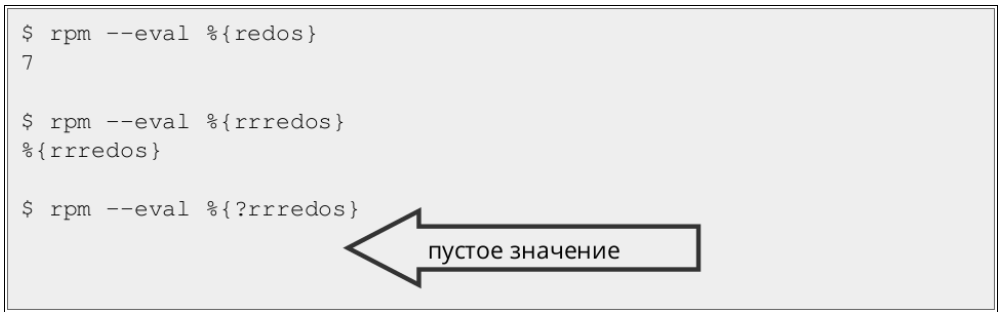
```
rpm --eval %{?dist}

.el7
```

ВАЖНО!

Тип значения макроса как переменной считается строковым (по аналогии с переменными в сценариях оболочки)!

С целью избежания нештатных ситуаций в случаях, когда макрос не определён, рекомендуется в конструкциях, где он используется как переменная, содержащая какое-либо значение, после открывающей скобки его имени ставить символ «**?**». Такая форма обращения к не определённому макросу при подстановке возвратит пустое значение, без знака вопроса — строку с именем данного макроса.

Например:



Макросы можно использовать внутри других макросов. Так, например, если название архива исходных текстов проекта формируется из его имени и версии (директивы **Name** и **Version** транслируются в определённые макросы, о чём будет рассказано ниже), то директива задания пути к файлу может выглядеть следующим образом:

```
Source0: %{name}-%{version}.tar.gz
```

Пути к системным каталогам и каталогам сборочного окружения могут быть получены в спецификации через заданные макросы, представленные в таблицах ниже.

Таблица 1. Макросы путей системных каталогов

Макрос	Определение
%{_sysconfdir}	/etc
%{_lib}	lib64 (для 64-битных платформ) lib (для 32-битных платформ)

%{_prefix}	/usr
%{_includedir}	%{_prefix}/include = /usr/include
%{_bindir}	%{_prefix}/bin = /usr/bin
%{_libdir}	%{_prefix}/%{_lib} = /usr/%{_lib}
%{_libexecdir}	%{_prefix}/libexec = /usr/lubexec
%{_sbindir}	%{_prefix}/sbin = /usr/sbin
%{_datadir}	%{_prefix}/share = /usr/share
%{_infodir}	%{_datadir}/info = /usr/share/info
%{_mandir}	%{_datadir}/man = /usr/share/man
%{_docdir}	%{_datadir}/doc = /usr/share/doc
%{_rundir}	/run
%{_localstatedir}	/var
%{_sharedstatedir}	/var/lib

Таблица 2. Макросы путей каталогов сборочного окружения

Макрос	Определение
%{_topdir}	%{getenv:HOME}/rpmbuild
%{_buildrootdir}	%{_topdir}/BUILDROOT
%{buildroot}	%{_buildrootdir}/%{name}-%{version}-%{release}.%{_arch}
%{_builddir}	%{_topdir}/BUILD
%{_rpmdir}	%{_topdir}/RPMS
%{_sourcedir}	%{_topdir}/SOURCES
%{_specdir}	%{_topdir}/SPECS
%{_srcrpmdir}	%{_topdir}/SRPMS

Значения, определяемые директивами преамбулы, транслируются для данной сборки в стандартные макросы. Связь директив и макросов дана в следующей таблице.

Таблица 3. Связь директив преамбулы и некоторых макросов

Директива	Соответствующий макрос
Name	%{name}
Version	%{version}
Release	%{release}
Epoch	%{epoch}
URL	%{url}
SourceX	%{SOURCEX} или %{S:X}

С целью сокращения написания часто требуемых команд при сборке пакета в блоках тела спецификации существует ряд полезных встроенных макросов:

1) **%setup** — используется в блоке **%prep** и выполняет следующие действия:

- переходит в дерево сборки;
- распаковывает архив с исходным кодом (с ключом **-q** подавляет подробный вывод при распаковке архива);
- изменяет владельца и права доступа к файлам с исходным кодом;
- переходит в распакованный каталог.

По умолчанию распаковывается первый архив с исходным кодом (т. е. который имеет номер 0), для любых других необходимо

использовать дополнительный параметр **-a X**, где **X** — номер, совпадающий с таковым у **Source**.

По умолчанию считается, что рабочим каталогом сборки в **BUILD** является тот, у которого имя совпадает с именем архива без суффикса (**.tar.gz** и пр.), если каталог с исходными текстами имеет другое название, то его указывают с ключом **-n** (например: **%setup -n %{name}-master**).

2) **%patch[X]** — используется в блоке **%prep** и выполняет применение указанного патча (здесь **X** — номер патча, такой же, как и при их описании в преамбуле, если патчей несколько). Применение патчей производится от текущего сборочного каталога, при необходимости обрезать часть пути к изменяемому файлу, можно использовать ключ **-p** (как и у самой утилиты **patch**). Например:

```
%patch3 -p1
```

3) **%autopatch** — применение всех патчей в порядке возрастания их номера в имени. Макрос также поддерживает использование ключа **-p**.

4) **%autosetup** — макрос, объединяющий функционал **%setup** и **%autopatch**; поддерживает все ключи, применимые в этих двум макросах.

5) **%configure** — применяется в блоке **%build** для выполнения сценария **configure** с подстановкой преднастроенных значений (обычно имён каталогов). Макрос принимает любые аргументы, которые при его раскрытии будут переданы скрипту **configure**.

6) **%make_build** — используется в блоке **%build** для выполнения команды **make** с установленными значениями **%{?_smp_mflags} %{_make_verbose}**. Здесь **%{?_smp_mflags}** раскрывается в **-j <ЧИСЛО_ПОТОКОВ>** и **%{_make_verbose}** — в **V=1 VERBOSE=1**.

Данный макрос также может принимать любые аргументы, которые при его раскрытии будут переданы утилите **make**.

7) **%make_install** — применяется в блоке **%install**, и представляет собой запуск утилиты **make** с ключом **install**, указанием каталога для установки (**DESTDIR=%{buildroot}**) и рядом других ключей.

Макрос также может принимать любые аргументы, которые при его раскрытии будут переданы утилите **make**.

8) **%dir** — макрос, используемый в блоке **%files**, указывающий, что путь является каталогом, который должен принадлежать этому RPM. Это указание важно для того, чтобы манифест файла RPM точно знал, какие каталоги нужно очистить при удалении пакета;

9) **%doc** — макрос, используемый в блоке **%files**, обеспечивающий создание каталога документации (**%{_docdir}/%{name}-%{version}**) и копирование в него указанных в качестве аргументов файлов. Пути к файлам строятся относительно каталога сборки проекта.

Например: **%doc README docs/Changelog**

10) **%license** — макрос, применяемый в блоке **%files**, аналогичный **%doc**, но копирует файлы лицензий в соответствующий каталог.

Скриптлеты

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

В спецификации RPM существует ряд директив, которые можно использовать для внесения необходимых или желаемых изменений в систему во время установки или удаления пакета. Такие директивы называются **скриптлетами**.

Некоторыми из основных примеров того, когда это может понадобиться, являются:

- установка пакетом системной службы, которая предоставляет файл модуля **systemd**, после чего нужно будет уведомить **systemd** о появлении нового модуля, возможно и запустить его. Обратная ситуация: при удалении пакета, содержащего модуль **systemd**, необходимо остановить выполнение сервиса и проинформировать **systemd** об удалении модуля;
- установка или удаление библиотек с последующей перестройкой их кэша;
- установка или удаление элементов графического интерфейса или схем **GLib**, после чего необходимо перестраивать кэши или перекомпилировать схемы;
- создание или удаление системных пользователей и/или групп при установке или удалении пакетов.

Количество стандартных (встроенных) скриптлетов весьма невелико, все они похожи на блоки тела спецификации, такие как **%build** или **%install**, в том, что определяются многострочными сегментами кода, представляющим собой стандартный сценарий оболочки (но могут быть использованы и некоторые скриптовые языки, например, Lua).

В своём роде, скриптлеты являют собой дополнительные блоки в теле спецификации, предоставляющие расширенные возможности при работе уже с двоичными пакетами.

Далее приведены встроенные скриптлеты сборочной системы в РЕД ОС.

Скриптлеты поддерживают специальный флаг **-p**, который позволяет напрямую вызывать одну указанную программу, а не создавать сеанс оболочки для вызова программ (например, **%post -p /sbin/ldconfig**):

- **%pretrans** - выполняется до начала любых операций по установке пакета;
- **%pre** - выполняется непосредственно перед установкой файлов из пакета;
- **%post** - выполняется сразу после завершения установки файлов из пакета;
- **%preun** - выполняется непосредственно перед удалением пакета;
- **%postun** - выполняется после завершения удаления файлов пакета;
- **%posttrans** - выполняется после завершения всех операций при удалении пакета.

При вызове скриптлетов им всегда передаётся аргумент, доступ к которому осуществляется через переменную **$1** (для сценариев оболочки), — это количество пакетов с этим именем, которые останутся в системе после завершения действия.

Скриптлет	Установка (install)	Обновление (upgrade)	Удаление (uninstall)
%pretrans	$1 == 0	$1 == 0	(N/A)
%pre	$1 == 1	$1 == 2	(N/A)
%post	$1 == 1	$1 == 2	(N/A)
%preun	(N/A)	$1 == 1	$1 == 0
%postun	(N/A)	$1 == 1	$1 == 0
%posttrans	$1 == 0	$1 == 0	(N/A)

Таким образом, анализируя аргумент внутри скриптлета, можно точно идентифицировать действие, которое выполняется в системе, а также определить, имеются ли в системе пакеты с таким же именем, что бывает необходимо знать при обновлении с целью

сохранения имеющихся настроек, а не их перезаписью.

Условные операторы

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Условные операторы сборочной системы RPM позволяют включать различные разделы файла спецификации в зависимости от указанных условий.

Чаще всего условные операции имеют дело с:

- разделами, относящиеся к версиям пакетов или операционной системы;
- разделами, относящиеся к архитектуре;
- существованием и определением макросов.

Синтаксис условного оператора следующий:

```
%if <УСЛОВИЕ>
...
%else
...
%endif
```

В случае необходимости выполнить только действия с истинным условием, можно использовать сокращённый вариант оператора:

```
%if <УСЛОВИЕ>
...
%endif
```

Существует форма записи данного оператора для случая проверки архитектуры, под которую собирается пакет:

```
%ifarch <АРХИТЕКТУРА>
...
%endif
```

Также имеется вариант, который проверяет условие «**если НЕ указанная архитектура**»:

```
%ifnarch <АРХИТЕКТУРА>
...
%endif
```

Например, задание переменной окружения **CFLAGS** в зависимости от архитектуры сборки пакета:

```
%ifarch %ix86 x86_64
export CFLAGS="$CFLAGS -msse2 -mfpmath=sse"
%endif
```

Чтобы избежать нештатных ситуаций при обработке условия, когда переменная (макрос) не определена, рекомендуется перед именем макроса ставить, например, символ «**0**»:

```
%if 0%{?redos} == 7
Requires: clang-devel
%endif
```

В директивах преамбулы **BuildRequires** и **Requires** для указания ограничений на версию требуемого пакета допускается краткое написание условного оператора, например:

```
BuildRequires: ffmpeg-devel >= 4.0
...
Requires: ffmpeg >= 4.0
```

Здесь в логической конструкции важно указывать такое же количество позиций у версии, как и у используемого пакета, то есть нельзя взять, например, только мажорную версию или добавить ещё одну цифру в конце.

Сборка исходных и двоичных пакетов

Сборка исходных пакетов
Сборка двоичных пакетов

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Пакеты RPM создаются с помощью утилиты **rpmbuild**. Различные сценарии и желаемые результаты сборки пакетов требуют различных комбинаций аргументов для **rpmbuild**. В этом разделе описаны два основных сценария:

- построение исходного пакета;
- построение двоичного пакета.

Команда **rpmbuild** работает с определённой структурой каталогов и файлов, которая была рассмотрена в нашей статье « Сборочное окружение». Таким образом, приступать к сборке пакетов можно при наличии всех требуемых исходных файлов, патчей к ним (в случае необходимости) и файла спецификации, размещённых в дереве каталогов сборочного окружения.

Построение двоичного пакета можно осуществить и без настроенной сборочного структуры каталогов и файлов, если имеется исходный пакет.

Сборка исходных пакетов

Основными задачами создания исходных пакетов (**SRPM**) являются:

- сохранение точного источника, включающего в себя точный файл спецификации, исходный код и все соответствующие исправления. Наличие **SRPM** бывает полезно для просмотра истории изменений и для отладки;
- возможность создавать двоичный пакет на другой аппаратной платформе или архитектуре.

Создание исходного пакета выполняется с помощью команды:

```
rpmbuild -bs <SPECFILE>
```

где <**SPECFILE**> — имя файла спецификации; ключ **-bs** является сокращением от словосочетания «**build source**». Имя файла может быть как абсолютным, так и относительным путём.

В результате безошибочного выполнения команды сборки исходного пакета в папке **~/rpmbuilds/SRPMS** появится SRPM-файл.

Сборка двоичных пакетов

Существует два метода построения двоичных пакетов:

- перестроить его из **SRPM** с помощью команды **rpmbuild --rebuild**;
- создать его из файла спецификации с помощью команды **rpmbuild -bb**. Опция **-bb** расшифровывается как «**build binary**».

Если имеется исходный пакет, то для получения двоичного необходимо выполнить команду:

```
rpmbuild --rebuild <ИМЯ>.src.rpm
```

В случае выполнения указанной команды будут реализованы следующие шаги:

1) создание сборочной структуры каталогов **~/rpmbuild** и установка в них содержимого исходного пакета;

2) сборка двоичного пакета согласно спецификации. Полученные файлы пакетов будут размещены в **~/rpmbuild/RPMS** в подкаталогах по именам архитектуры;

3) очистка содержимого каталогов **SPECS** и **SOURCES** в сборочном окружении.

Исходный пакет можно установить:

```
rpm -i <ИМЯ>.src.rpm
```

и после чего осуществить сборку двоичного пакета командой:

```
rpmbuild -bb <SPEC-ФАЙЛ>
```

Имя файла спецификации может быть как абсолютным, так и относительным путём.

С помощью последней команды можно собрать пакет, если имеется развёрнутое сборочное окружение со всеми необходимыми каталогами и файлами.

Цифровая подпись пакета

> Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Подписание пакета — это способ защитить пакет для конечного пользователя, чтобы убедиться, что никакая третья сторона не изменяла его содержимое при передаче от автора к пользователю.

В большинстве случаев пакеты создаются без подписи, которая уже позже добавляется непосредственно перед размещением файлов RPM в репозитории или ином способе передачи пользователям.

Чтобы добавить подпись к пакету, используется опция **--addsign** утилиты **rpm**. Например:

```
rpm --addsign superproj-1.0-1.el7.x86_64.rpm

 Enter pass phrase:

Pass phrase is good.
superproj-1.0-1.el7.x86_64.rpm:
```

Пакет может быть подписан несколькими различными подписями — наличие нескольких подписей позволяет отслеживать путь владения пакетом от разработчика до конечного пользователя.

Чтобы изменить открытый ключ у пакета, который уже подписан другой подписью, используется опция **--resign**:

```
rpm --resign superproj-1.0-1.el7.x86_64.rpm

 Enter pass phrase:

Pass phrase is good.
superproj-1.0-1.el7.x86_64.rpm:
```

Чтобы подписать пакет во время сборки, используется команда **rpmbuild** с параметром **--sign**, причём парольная фраза запрашивается перед сборкой пакета, а не по её окончании:

```
rpmbuild -bb --sign superproj.spec

 Enter pass phrase:

Pass phrase is good.
* Package: superproj
...
Binary Packaging: superproj-1.0-1
Finding dependencies...
...
Generating signature: 1002
Wrote: /home/user/rpmbuild/RPMS/x86_64/superproj-1.0-1.el7.x86_64.rpm
```

Сборка пакета стороннего ПО

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Рассмотрим сборку пакета на примере проекта **libfakekey**.

1) Получите исходные тексты программы, скачав архив актуальной версии по следующей ссылке.

2) Получив исходный архив, распакуйте его командой:

```
tar -xf libfakekey-0.3.tar.gz
```

3) В полученном дереве исходного кода найдите файл **INSTALL**, в случае его отсутствия — **README**. В них, как правило, описаны инструкции по сборке проекта.

В данном случае файл **INSTALL** отсутствует, а **README** имеет нулевую длину, но имеется сценарий **autogen.sh** со следующим содержимым:

```
#! /bin/sh
autoreconf -v --install || exit 1
./configure --enable-maintainer-mode "$@"
```

Значит, необходимые файлы могут быть сгенерированы с помощью утилиты **autoreconf**, для чего необходимо установить в систему пакеты **autoconf** и **automake**, если они отсутствуют. Находясь в каталоге исходных текстов, выполните следующую команду:

```
autoreconf -fiv
```

4) Поскольку в РЕД ОС сборка бинарных файлов осуществляется с использованием динамического связывания, то можно для сценария конфигурации использовать опцию отключения сборки статической версии (**--disable-static**). Также нужно указать, что при сборке проекта скомпилированные библиотеки необходимо компоновать с библиотеками X Window, для чего утилите **make** передайте указание на это (**AM_LDFLAGS=-lX11**).

5) Затем следует определиться с пакетами, необходимыми для сборки. Откройте файл **fakekey/fakekey.h**, в котором будет интересовать секция **#include**, находящаяся в его начале:

```
#ifndef _HAVE_LIBFAKEKEY_H
#define _HAVE_LIBFAKEKEY_H

#include <stdio.h>
#include <stdlib.h>
#include <X11/X.h>
#include <X11/Xlib.h>
#include <X11/Xlibint.h>
#include <X11/Xutil.h>
#include <X11/cursorfont.h>
#include <X11/keysymdef.h>
#include <X11/keysym.h>
#include <X11/extensions/XTest.h>
#include <X11/Xos.h>
#include <X11/Xproto.h>

#ifdef __cplusplus
extern "C" {
```

```
#endif
```

Здесь представляют интерес заголовочные файлы системы **X11**. Проверьте, какими пакетами они поставляются, для чего выполните операцию поиска по репозиторию, например:

```
dnf provides "*X11/Xlib.h"
```

Использование джокерного символа «*» обязательно, поскольку в метаданных пакета может храниться полный путь к файлу, а утилита **dnf** выводит результаты поиска при условии полного совпадения строк.

Таким образом, проверив все **.h**-файлы, будет выведен список из следующих пакетов:

```
libX11-devel, libXi-devel, libXtst-devel, xorg-x11-proto-devel
```

6) Имея полученную информацию, перед тем как приступить к написанию спецификации пакета, создайте структуру сборочных каталогов (см. статью «Сборочное окружение»):

```
rpmdev-setuptree
```

В каталог **SOURCES** скопируйте исходный архив, затем перейдите в директорию **SPECS** и создайте в нём заготовку спецификации (см. статью «Файл спецификации»):

```
rpmdev-newspec libfakekey libfakekey.spec created; type minimal, rpm version >= 4.13.
```

7) Откройте на редактирование файл **libfakekey.spec** в любом текстовом редакторе и начните заполнять преамбулу. Учтите, что пакет устанавливает в систему не только двоичные компоненты, но и файлы, необходимые для разработки программного обеспечения. Считается «хорошим тоном» файлы для разработчиков выносить в отдельный двоичный пакет — отразите это в спецификации.

```
0 # spec file for package libfakekey
1 Name: libfakekey
2 Version: 0.3
3 Release: 1%{?dist}
4 Summary: Library for converting characters to X key-presses
5 License: LGPLv2+
6 URL: http://projects.o-hand.com/matchbox/
7 Source0: %{name}-%{version}.tar.gz
8 BuildRequires: gcc
9 BuildRequires: make
10 BuildRequires: autoconf
11 BuildRequires: automake
12 BuildRequires: libX11-devel
13 BuildRequires: libXi-devel
14 BuildRequires: libXtst-devel
15 BuildRequires: xorg-x11-proto-devel
16 BuildRequires: pkgconfig
17
18 %description
19 libfakekey is a simple library for converting UTF-8 characters
20 into 'fake' X key-presses.
21
22 %package devel
23 Summary: Development files for %{name}
24 Requires: %{name} = %{version}-%{release}
25 Requires: libX11-devel
26 Requires: libXi-devel
27 Requires: libXtst-devel
28 Requires: xorg-x11-proto-devel
29 Requires: pkgconfig
30
31 %description devel
32 The %{name}-devel package contains libraries and header files for
```

```
33 developing applications that use %{name}.
34
```

Здесь в строке **№ 0** находится комментарий. В спецификации к таковым относится вся символьная последовательность от «**#**» до конца строки.

В строке **№ 4** даётся краткое описание, а в строках **18–20** — развёрнутое описание пакета, которые можно взять, например, с сайта проекта.

Имя исходного архива в строке **№ 7** задаётся через макросы (как показывалось в статье «Основные макросы»), что будет удобным при обновлении пакета до новой версии, так как директиву **Source0** исправлять не придётся — достаточно будет изменить только версию пакета в директиве **Version** в начале файла.

В строках **с 8 по 16** находится перечисление пакетов по одному в строке, которые необходимы для сборки данного пакета. Здесь пакет **pkgconfig** необходим для обработки файла **libfakekey.pc.in**, имеющегося в дереве исходного кода проекта.

С 22 по 33 строки производится описание второго двоичного пакета, который получит имя **libfakekey-devel**, с файлами для разработчиков. В секции его описания дополнительно указываются те пакеты, которые будут необходимы для его использования при разработке программного обеспечения — они заданы директивами **Requires**. Содержимое **%description** определяются самостоятельно, исходя из общего описания в предыдущей подобной директивы, с указанием на то, что здесь содержатся файлы для разработки.

8) Далее перейдем к телу спецификации (нумерация строк сквозная, с продолжением после преамбулы):

```
35 %prep
36 %setup -q
37
38 %build
39 autoreconf -fiv
40 %configure --disable-static
41 %make_build AM_LDFLAGS=-lX11
42
43 %install
44 %make_install
45 rm -f %{buildroot}%{_libdir}/libfakekey.la
46
47 %ldconfig_scriptlets
48
49 %files
50 %license COPYING
51 %{_libdir}/libfakekey.so.*
52
53 %files devel
54 %{_includedir}/fakekey/
55 %{_libdir}/libfakekey.so
56 %{_libdir}/pkgconfig/libfakekey.pc
57
58 %changelog
59 * Tue Jan 19 2021 Rodion Alexeev - 0:0.3-1
60 - Initial build
70
```

Со строки **№ 35** начинается блок подготовки к сборке, в нём с помощью макроса **%setup** производится распаковка архива с подавлением вывода на экран информации об извлечение файлов.

Со строки **№ 38** следует блок сборки проекта. Согласно файлу **autogen.sh**, требуется выполнить **autoreconf**, а после него — сгенерированный **configure**. Необходимо выполнить данные действия, но лучше это сделать не запуском сценария, а явным указанием этих команд в спецификации, поэтому в строке **№ 39** осуществляется выполнение утилиты **autoconf**, а в строке **№ 40** — **configure** посредством соответствующего макроса. После всего этого выполните сборку проекта утилитой **make** также посредством макроса (строка **№ 41**).

Собранный проект необходимо установить, т. е. инсталлировать, за что отвечает блок **%install** со строки **№ 43**. Типовая установка (**make install**) осуществляется посредством соответствующего макроса (строка **№ 44**), а затем из дерева установки удаляется файл **Libtool Archive** (**.la**) за ненадобностью. Обращаем внимание, что все пути указаны как абсолютные и с помощью макросов!

Поскольку в пакете будет поставляться динамическая библиотека, то при её установке или удалении необходимо перестраивать кэш

библиотек утилитой **ldconfig** — данные действия осуществляются с помощью скриптлетов **%post** и **%postun**, соответственно. Можно это оформить в следующем виде:

```
%post -p /sbin/ldconfig
%postun -p /sbin/ldconfig
```

В РЕД ОС имеется скриптлет, объединяющий вышеуказанные действия, он использован в строке **№ 47**.

Затем следуют блоки описания файлов, размещаемых в двоичных пакетах. Поскольку необходимо разделить проект на два RPM-файла, то и блоков **%files** у нас тоже два — со строки **№ 49** для **libfakekey**, со строки **№ 53** - для **libfakekey-devel**. В строке **№ 50** используется макрос для копирования и описания файла лицензии, в остальных строках (**№ 51, 54–56**) идёт перечисление файлов, которые будут принадлежать тому или иному пакету.

В данном примере количество двоичных файлов не велико и их названия и расположение можно посмотреть в **Makefile**, но в случае больших проектов это, скорее всего, не поможет в заполнении данного блока.

При написании спецификации «с нуля» можно поступить следующим образом - блоки **%files** оставить пустыми, перейти к заполнению следующего раздела, после выполнить первую сборку пакета. В конце сборки будет показано сообщение об ошибке, что имеются неупакованные в RPM файлы с выводом их полного списка. Из данного списка уже можно взять имена файлов и их местоположение и внести в блок **%files**, не забывая заменять реальные имена каталогов на макросы, их обозначающие.

Последний раздел тела спецификации — журнал изменений (**%changelog**) — начинается со строки **№ 58**. Здесь указаны дата сборки пакета, автор сборки, а также список изменений (оно в данном примере одно — **Initial build**). Допускается (и считается «хорошим тоном») после имени автора указывать его адрес электронной почты в виде **<box@domain.tld>**.

Обратите внимание на окончание строки **№ 59: 0:0.3-1**. Первая цифра до двоеточия — это эпоха (**Epoch**), которая явно в преамбуле не задана, и по умолчанию принимается равной 0. После двоеточия до символа «-» идёт указание версии пакета (**Version**), а после минуса — релиза (**Release**) без суффикса. Часто опускают указание эпохи, если она нулевая. Можно опустить и всю данную цифровую конструкцию, но не рекомендуется этого делать, поскольку становится не понятным, к какой конкретно сборке относится запись в журнале изменений.

9) Завершив редактирование файла спецификации, приступаем к сборке двоичного пакета командой:

```
rpmbuild -bb libfakekey.spec
```

Вывод информации на экран при работе данной команды весьма обширный, приведём только некоторые выдержки из него:

- начало сборки, выполнение блока **%prep**:

```
rpmbuild -bb libfakekey.spec

Выполняется(%prep): /bin/sh -e /var/tmp/rpm-tmp.yqu3Ha
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd /home/user/rpmbuild/BUILD
+ rm -rf libfakekey-0.3
+ /usr/bin/gzip -dc /home/user/rpmbuild/SOURCES/libfakekey-0.3.tar.gz
+ /usr/bin/tar -xof -
+ STATUS=0
+ '[' 0 -ne 0 ']'
+ cd libfakekey-0.3
+ /usr/bin/chmod -Rf a+rX,u+w,g-w,o-w .
+ exit 0
...
```

- начало блока **%build**:

```
Выполняется(%build): /bin/sh -e /var/tmp/rpm-tmp.lm8Y8n
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd libfakekey-0.3
+ autoreconf -fiv
...
```

продолжение **%build** — запуск макроса **%configure**:

```
...
+ ./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix= --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64 --libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/share/man --infodir=/usr/share/info --disable-static
```

запуск макроса **%make_build** и завершение блока **%build**:

```
+ make -j2 AM_LDFLAGS=-lX11
make  all-recursive
make[1]: Entering directory '/home/user/rpmbuild/BUILD/libfakekey-0.3'
...
+ exit 0
...
```

- начало блока **%install**:

```
Выполняется(%install): /bin/sh -e /var/tmp/rpm-tmp.Y0WCvw
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ '[' /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64 '!=' / ']'
+ rm -rf /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
++ dirname /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
+ mkdir -p /home/user/rpmbuild/BUILDROOT
+ mkdir /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
+ cd libfakekey-0.3
+ make install DESTDIR=/home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
Making install in fakekey
make[1]: Entering directory '/home/user/rpmbuild/BUILD/libfakekey-0.3/fakekey'
...
```

- блок **%files**:

```
Processing files: libfakekey-0.3-1.el7.x86_64
Выполняется(%license): /bin/sh -e /var/tmp/rpm-tmp.W2BVTI
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd libfakekey-0.3
+ LICENSEDIR=/home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64/usr/share/licenses/libfakekey
+ export LC_ALL=C
+ LC_ALL=C
+ export LICENSEDIR
+ /usr/bin/mkdir -p /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64/usr/share/licenses/libfakekey
+ cp -pr COPYING /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64/usr/share/licenses/libfakekey
+ exit 0
...
```

- после завершения всех действий, заданных в спецификации, сборочная система начинает анализировать полученные в ходе сборки файлы на предмет определения зависимостей (**Requires**), которые будут добавлены в метаданные пакета, чтобы пакетные менеджеры при установке данных RPM знали, что должно присутствовать в системе к моменту установки пакета, а в случае отсутствия — установить из репозитория. Также на данном этапе записывается в метаданные информация о компонентах, которые предоставляет пакет (**Provides**):

```
Provides: libfakekey = 0.3-1.el7 libfakekey(x86-64) = 0.3-1.el7 libfakekey.so.0()(64bit)
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Requires: libX11.so.6()(64bit) libXtst.so.6()(64bit) libc.so.6()(64bit) libc.so.6(GLIBC_2.2.5)(64bit) libc.so.6(GLIBC_2.4)(64bit) rtld(GNU_HASH)
Processing files: libfakekey-devel-0.3-1.el7.x86_64
Provides: libfakekey-devel = 0.3-1.el7 libfakekey-devel(x86-64) = 0.3-1.el7 pkgconfig(libfakekey) = 0.3
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Requires: /usr/bin/pkg-config
Processing files: libfakekey-debuginfo-0.3-1.el7.x86_64
Provides: libfakekey-debuginfo = 0.3-1.el7 libfakekey-debuginfo(x86-64) = 0.3-1.el7
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Проверка на неупакованный(е) файл(ы): /usr/lib/rpm/check-files /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
Записан: /home/user/rpmbuild/RPMS/x86_64/libfakekey-0.3-1.el7.x86_64.rpm
Записан: /home/user/rpmbuild/RPMS/x86_64/libfakekey-devel-0.3-1.el7.x86_64.rpm
Записан: /home/user/rpmbuild/RPMS/x86_64/libfakekey-debuginfo-0.3-1.el7.x86_64.rpm
...
```

- успешное завершение сборки пакета:

```
...
Выполняется(%clean): /bin/sh -e /var/tmp/rpm-tmp.hIC2sW
+ umask 022
+ cd /home/user/rpmbuild/BUILD
```

```
+ cd libfakekey-0.3
+ /usr/bin/rm -rf /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
+ exit 0
```

В случае успешного завершения сборки в каталоге **~/rpmbuild/RPMS** будут созданы подкаталоги с именами архитектур, под которые собрались RPM-файлы. В этих подкаталогах будут размещены двоичные пакеты:

```
ls -1Rp ~/rpmbuild/RPMS

/home/user/rpmbuild/RPMS:
x86_64/

/home/user/rpmbuild/RPMS/x86_64:
libfakekey-0.3-1.el7.x86_64.rpm
libfakekey-debuginfo-0.3-1.el7.x86_64.rpm
libfakekey-devel-0.3-1.el7.x86_64.rpm
```

Здесь видно, что собрано три пакета, хотя в спецификации описывалось два. Дело в том, что перед упаковкой файлов в архив **cpio** сборочная система извлекает из двоичных файлов отладочную информацию, которая затем помещается в отдельный файл RPM, что отражается в его названии:

```
libfakekey-debuginfo-0.3-1.el7.x86_64.rpm
```

Данные пакеты не нужны рядовым пользователям, они востребованы разработчиками для отладки работы программного обеспечения.

10) После успешного завершения сборки двоичных пакетов необходимо собрать исходный пакет:

```
rpmbuild -bs libfakekey.spec

Записан: /home/user/rpmbuild/SRPMS/libfakekey-0.3-1.el7.src.rpm
```

На этом процесс сборки проекта **libfakekey** завершён — в результате созданы как исходный, так и двоичные пакеты. Двоичные RPM можно передавать кому-либо для использования/установки, перед этим желательно подписать их своей цифровой подписью.

Сборка мета-пакета

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Определим, что такое «мета-пакет», хотя однозначного, стандартизованного толкования данного понятия не существует. В общих словах, мета-пакет — это «пустой» пакет. Под термином «пустой» понимают как отсутствие исходных файлов при сборке пакета (в спецификации нет директив **Source**), так и отсутствие файлов в архиве **cpio** двоичного пакета (блок **%files** пустой).

Может возникнуть вопрос: зачем такой пакет, который ничего не устанавливает в систему? Дело в том, что ценность пакета может быть не только в файлах, в нём содержащихся, но и в его метаданных. Иными словами, после инсталляции мета-пакета в базе данных установленных пакетов появляются записи относительно каких-то новых имён, зависимостей и прочего, имеющих значение в целом для системы.

В каких случаях это может понадобиться? Например, имеется программный проект, представленный большим числом RPM файлов, каждый из которых устанавливает в систему какой-то логически законченный набор файлов. Полная установка всего этого ПО потребует устанавливать все эти пакеты — для упрощения данной процедуры можно создать мета-пакет, который при установке всего лишь потребует от пакетного менеджера установить весь перечень пакетов этого программного проекта.

Например, имеется следующий список двоичных пакетов:

```
superproj-libs-1.0-1.el7
superproj-devel-1.0-1.el7
superproj-bin-1.0-1.el7
superproj-server-1.0-1.el7
superproj-client-1.0-1.el7
superproj-tools-1.0-1.el7
superproj-docs-1.0-1.el7
```

Создадим мета-пакет для установки всех этих пакетов. Спецификация для такого пакета будет выглядеть следующим образом:

```
1 %define debug_package %{nil}
2 Name: superproj-all
3 Version: 1.0
4 Release: 1%{?dist}
5 Summary: Meta-package for SuperProj
6 License: GPL2+
7 URL: https://super.proj/
8 Requires: superproj-libs = %{version}-%{release}
9 Requires: superproj-devel = %{version}-%{release}
10 Requires: superproj-bin = %{version}-%{release}
11 Requires: superproj-server = %{version}-%{release}
12 Requires: superproj-client = %{version}-%{release}
13 Requires: superproj-tools = %{version}-%{release}
14 Requires: superproj-docs = %{version}-%{release}
15
16 %description
17 Meta-package for installing all packages of SuperProj.
18
19 %prep
20
21 %build
22
23 %install
```

```
24
25 %files
26
27 %changelog
28 * Tue Jan 19 2021 Rodion Alexeev - 0:1.0-1
29 - Initial build
```

Здесь надо обратить внимание на строку **№ 1:** **%define** в общем случае задаёт значение макроса, а в данном случае — переопределяет значение стандартного макроса **debug_package**, устанавливая его в пустое значение (**%nil**). Такая конструкция говорит сборочной системе, что не надо извлекать отладочную информацию из конечных файлов (в данном мета-пакете извлекать нечего и не из чего!) и не формировать **debuginfo**-пакет.

Блоки **%prep**, **%build**, **%install**, **%files** в данной спецификации пустые, но они всё равно должны быть явно обозначены.

После выполнения команды **rpmbuild** будет создан пакет под заданную архитектуру, который сам в виде файлов ничего не будет поставлять в систему, но потребует от пакетного менеджера установить все пакеты, которые у него перечислены в зависимостях (директивы **Requires**).

Установка .NET

Установка
Работа в программе
Создание простого консольного приложения
Создание простого веб-приложения

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dotnet-sdk-6.0-6.0.105-1

.NET (ранее известна как *.NET Core*) — бесплатная модульная платформа с открытым исходным кодом для разработки программного обеспечения. Поддерживает следующие языки программирования:

- **C#** — это современный, объектно-ориентированный и типобезопасный язык программирования. Он имеет свои корни в семействе языков C – *C*, *C++*, *Java* и *JavaScript*.
- **F#** — это язык программирования взаимодействия для написания краткого, надежного и эффективного кода. Программирование **F#** ориентировано на данные, где код включает преобразование данных с помощью функций.
- **Visual Basic** использует более подробный синтаксис, который близок к обычному человеческому языку. Это наиболее простой язык для начинающих программистов.

Платформа **.NET** основана на высокопроизводительной среде выполнения, которая используется в рабочей среде многими высокомасштабируемыми приложениями.

Установка

Платформа **.NET** в РЕД ОС включает в себя следующие пакеты:

- **dotnet-sdk** – пакет SDK позволяет разрабатывать приложения с помощью **.NET**;
- **aspnetcore-runtime** – среда выполнения **ASP.NET Core** позволяет запускать веб-приложения, включает в себя пакет **dotnet-runtime**;
- **dotnet-runtime** – альтернатива среде выполнения **ASP.NET Core**, позволяет запускать **.NET**-приложения.

В рамках текущей статьи будет рассмотрена установка **.NET** в составе пакета **dotnet-sdk**, т.к. он включает в себя сразу всю платформу.

Перед началом установки перейдите в сеанс пользователя **root**:

```
su -
```

Далее выполните команду установки платформы:

```
dnf install dotnet-sdk-6.0
```

Для проверки установленных **SDK** воспользуйтесь следующей командой:

```
dotnet --list-sdks

6.0.105 [/usr/lib64/dotnet/sdk]
```

Для проверки установленных сред выполнения воспользуйтесь командой:

```
dotnet --list-runtimes

Microsoft.AspNetCore.App 6.0.5 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
Microsoft.NETCore.App 6.0.5 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]
```

Подробную информацию о доступных опциях и командах выполните команду:

```
dotnet --help
```

Работа в программе

Для проверки работы будут созданы два приложения – консольное и веб-приложение.

Создание простого консольного приложения

Создайте отдельный каталог для проектов (в примере **Projects**) и перейдите в созданный каталог:

```
mkdir Projects
cd Projects
```

Создайте новое консольное приложение (в примере **TestApp**) и перейдите в каталог приложения:

```
dotnet new console -o TestApp

Шаблон "Консольное приложение" успешно создан.

Идет обработка действий после создания...
Выполнение "dotnet restore" для /home/user/Projects/TestApp/TestApp.csproj...
  Determining projects to restore...
  Restored /home/user/Projects/TestApp/TestApp.csproj (in 309 ms).
 cd TestApp
```

Затем скомпилируйте или запустите скомпилированное приложение – в выводе должно отобразиться «Hello, world!».

```
dotnet run
Hello, World!
 dotnet bin/Debug/net6.0/TestApp.dll
Hello, World!
```

Создание простого веб-приложения

Создайте отдельный каталог для проектов (в примере **Projects**) и перейдите в созданный каталог:

```
mkdir Projects
cd Projects
```

Создайте новое веб-приложение (**TestWebApp**) и перейдите в каталог приложения:

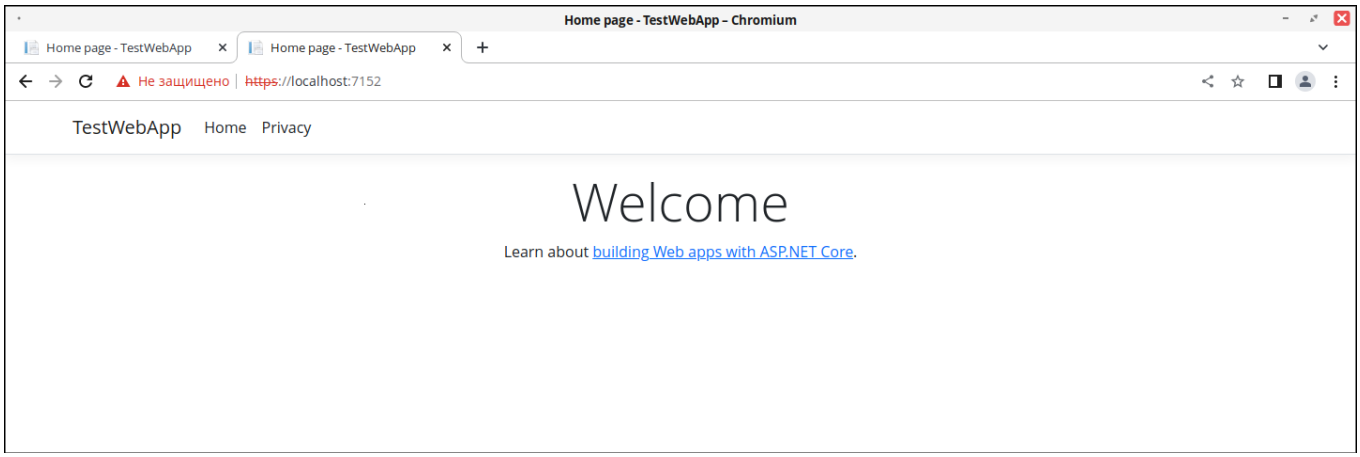
```
dotnet new webapp -o TestWebApp

Шаблон "ASP.NET Core Web App" успешно создан.
Этот шаблон содержит технологии сторонних производителей, кроме Майкрософт. Дополнительные сведения см. в разделе
https://aka.ms/aspnetcore/6.0-third-party-notices.

Идет обработка действий после создания...
Выполнение "dotnet restore" для /home/user/Projects/TestWebApp/TestWebApp.csproj...
  Determining projects to restore...
  Restored /home/user/Projects/TestWebApp/TestWebApp.csproj (in 289 ms).
Восстановление выполнено.cd TestWebApp
```

Затем скомпилируйте или запустите скомпилированное приложение.

```
dotnet run

Сборка...
info: Microsoft.Hosting.Lifetime[14]
      Now listening on: https://localhost:7152
info: Microsoft.Hosting.Lifetime[14]
      Now listening on: http://localhost:5274
info: Microsoft.Hosting.Lifetime[0]
      Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
```

```
      Hosting environment: Development
info: Microsoft.Hosting.Lifetime[0]
      Content root path: /home/user/Projects/TestWebApp/
```

В результате будет сформировано 2 адреса – для *HTTP*- и *HTTPS*-соединений. Запустите браузер и в адресной строке введите любой из указанных адресов – созданное веб-приложение должно быть доступно.



FPC – компилятор для разработки программ на языке Pascal

Установка
Создание и редактирование исходного кода
Создание простейшей программы на Pascal
Пример работы программы

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: fpc-3.2.0-1

FPC (*Free Pascal Compiler*) – это бесплатный компилятор программного обеспечения, предназначенный для языка программирования **Pascal**. *FPC* предоставляет возможность создания кроссплатформенных приложений – это означает, что можно написать программу один раз и скомпилировать ее для различных операционных систем, таких как *Windows*, *Linux*, *macOS* и даже для некоторых встраиваемых платформ.

Основные особенности *FPC*:

- **Поддержка платформ**. *FPC* поддерживает широкий спектр платформ, включая **x86**, **x86-64**, **ARM**, **PowerPC**, **SPARC** и многие другие. Это позволяет разрабатывать приложения для различных архитектур и операционных систем.
- **Полная совместимость с Turbo Pascal**. *FPC* стремится быть полностью совместимым с **Turbo Pascal** и поддерживает множество синтаксических расширений и возможностей языка.
- **Объектно-ориентированное программирование**. *FPC* поддерживает объектно-ориентированное программирование (ООП) и предоставляет возможности для создания классов, наследования, полиморфизма и инкапсуляции.
- **Модульность**. FPC позволяет разбивать программы на модули, что упрощает организацию и структурирование кода.
- **Расширения для системного программирования**. *FPC* предоставляет возможность обращения к низкоуровневым функциям и библиотекам операционной системы, что делает его подходящим для системного программирования.
- **Поддержка множества стандартов**. *FPC* соответствует многим стандартам, включая **ISO Pascal**, **Borland Pascal**, **Delphi**, **Mac Pascal** и другие.

FPC широко используется для разработки приложений, особенно в сообществах, где **Pascal** остается популярным языком программирования, таких как образование и некоторые научные области. Он также применяется для создания кроссплатформенных приложений, программирования микроконтроллеров и встроенных систем.

Установка

Для установки **fpc** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fpc
```

После установки компилятор не требует дополнительной настройки. Работа с компилятором производится с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

Синтаксис утилиты имеет вид:

```
fpc [<опции>] <файл> [<опции>]
```

Полезные опции:

- `-a` – не удалять файл ассемблера;
- `-al` – включить строки исходного кода в файл ассемблера в качестве комментариев;

- `-Cs<n>[<,m>]` – `<n>` задает минимальный размер кучи (стека данных) в байтах (от 1023 до 67107840), `[<,m>]` – максимальный размер кучи (необязательный параметр);
- `-Ct` – сгенерировать код проверки стека;
- `-s` – не вызывать ассемблер и компоновщик; вместо этого компилятор генерирует сценарий **ppas.sh**, который затем может быть выполнен для создания исполняемого файла;
- `-sh` – компилятор генерирует сценарий, который можно использовать для сборки и компоновки на хосте.

Для получения подробной информации о работе *FPC* выполните:

```
fpc -h
```

Создание и редактирование исходного кода

Перед началом работы создайте новый текстовый файл с расширением **.pas** и откройте его в любом удобном текстовом редакторе, например, nano. В этом файле будет располагаться исходный код программы на языке **Pascal**.

```
nano <имя_файла>.pas
```

> **Примечание.**
>
> Здесь и далее **<имя_файла>** замените на имя вашего файла.

Создание простейшей программы на Pascal

В примере будет написан и сохранен простейший код программы на языке **Pascal**.

Пример файла:

```
program Hello_world;
 begin
 writeln ('Hello World');
 end.
```

Компиляция программы

Теперь, когда есть исходный код, можно скомпилировать его с помощью **fpc**. Перейдите в каталог, где сохранен исходный файл, и выполните следующую команду:

```
fpc <имя_файла>.pas
```

В процессе выполнения компилятор создаст исполняемый файл с таким же именем, но без расширения **.pas**.

Запуск программы

После успешной компиляции программу можно запустить, указав в терминале имя исполняемого файла.

```
./<имя_файла>
```

Теперь программа должна запуститься и выполняться в соответствии с созданным исходным кодом.

Обратите внимание, что это базовая информация о том, как начать работать с *Free Pascal*.

Pascal – это мощный язык программирования с богатыми возможностями. Разработчик может использовать различные функции языка и библиотеки для создания разнообразных приложений. При желании, можно изучить дополнительные ресурсы и примеры для более продвинутого использования языка **Pascal** и компилятора *Free Pascal*.

Пример работы программы

Создадим исходный код программы:

```
nano test.pas
```

```
program ProgramTest;
 var a,i,n: integer;
 begin
  writeln('Введите высоту башни:');
  readln(a);
  for i:=1 to a do
  begin
   writeln();
   for n:=1 to I do
   write('*');
  end;
 writeln();
 end.
```

Выполним компиляцию программы:

```
fpc test.pas

Free Pascal Compiler version 3.2.0 [2020/12/29] for x86_64
Copyright (c) 1993-2020 by Florian Klaempfl and others
Target OS: Linux for x86-64
Compiling test.pas
Linking test
13 lines compiled, 0.1 sec
```

Запустим программу:

```
./test

Введите высоту башни:9

*
**
***
****
*****
******
*******
********
*********
```

Установка Julia

Установка
Работа в программе

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: julia-1.5.3-1

Julia – это высокоуровневый, динамический, функциональный и высокоэффективный язык программирования, который был разработан для научных вычислений и общего назначения. Он был представлен в 2012 году и стал популярным среди исследователей, инженеров, аналитиков данных и разработчиков благодаря своим мощным возможностям и простому синтаксису.

Некоторые ключевые особенности и характеристики языка программирования **Julia**:

- *Производительность*. **Julia** известен своей выдающейся производительностью. Он использует **Just-In-Time** (JIT) компиляцию, что позволяет достигать скорость, близкую к языкам низкого уровня, таким как **C** или **Fortran**. Это делает его отличным выбором для научных вычислений и других задач, где требуется высокая производительность.
- *Простота синтаксиса*. Синтаксис **Julia** интуитивен и легко читаем. Он похож на синтаксис **Matlab** и **Python**, что упрощает процесс изучения и использования языка.
- *Многопоточность*. **Julia** поддерживает параллельное программирование с помощью многопоточности. Это позволяет эффективно использовать многопроцессорные системы и ускорять выполнение вычислений.
- *Встроенная поддержка для распределенных вычислений*. Julia предоставляет удобные средства для распределенных вычислений на кластерах и удаленных системах, что делает его привлекательным для задач с высокой степенью параллелизма.
- *Обширная библиотека*. **Julia** имеет обширную библиотеку пакетов, включая инструменты для работы с матрицами, статистическими данными, машинным обучением, визуализацией данных и многое другое. Это облегчает решение различных задач без необходимости переходить к другим языкам программирования.
- *Открытый исходный код*. **Julia** является языком с открытым исходным кодом, что позволяет пользователям адаптировать его под свои потребности и вносить вклад в развитие языка.

Julia представляет собой мощный и гибкий язык программирования, который может быть использован для различных задач, особенно в области научных исследований, вычислений и анализа данных.

Установка

Для установки **Julia** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install julia
```

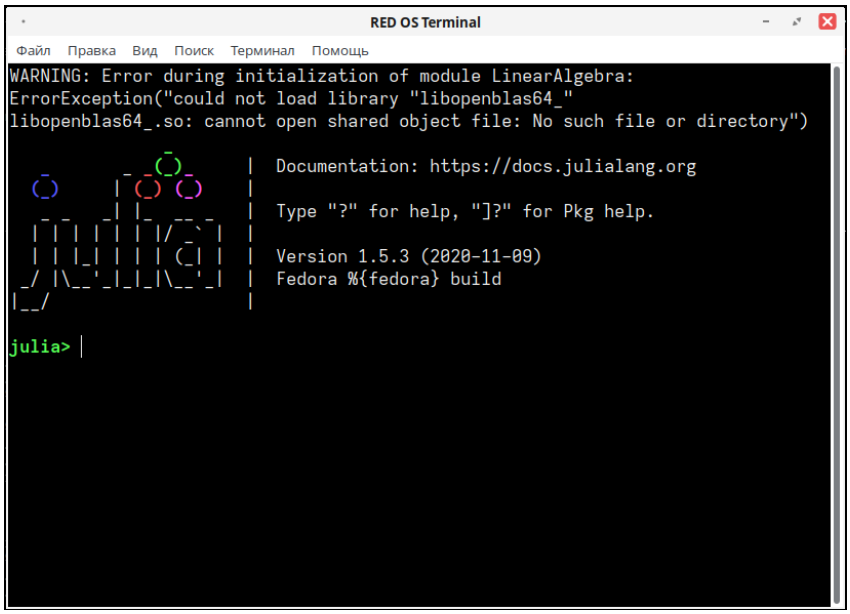
Дальнейшая работа в программе производится с правами непривилегированного пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

После установки запуск программы доступен из «**Главного меню**» — «**Программирование**» — «**Julia**» или через терминал (с правами непривилегированного пользователя) командой:

```
julia
```

При запуске программы открывается привычный терминал РЕД ОС:



Для выхода используйте сочетание клавиш **Ctrl+D**.

Работа в программе

В **Julia** нет прямого аналога команды man, как в некоторых других языках программирования или в операционных системах Unix/Linux. Однако в **Julia** доступна встроенная функция help?, которая предоставляет доступ к справке и информации о функциях и объектах в **REPL** (Read-Eval-Print Loop – интерактивная среда командной строки **Julia**).

Чтобы получить справку по функции, объекту или пакету в **Julia**, введите символ вопроса ? и имя функции или объекта, о котором необходимо получить информацию.

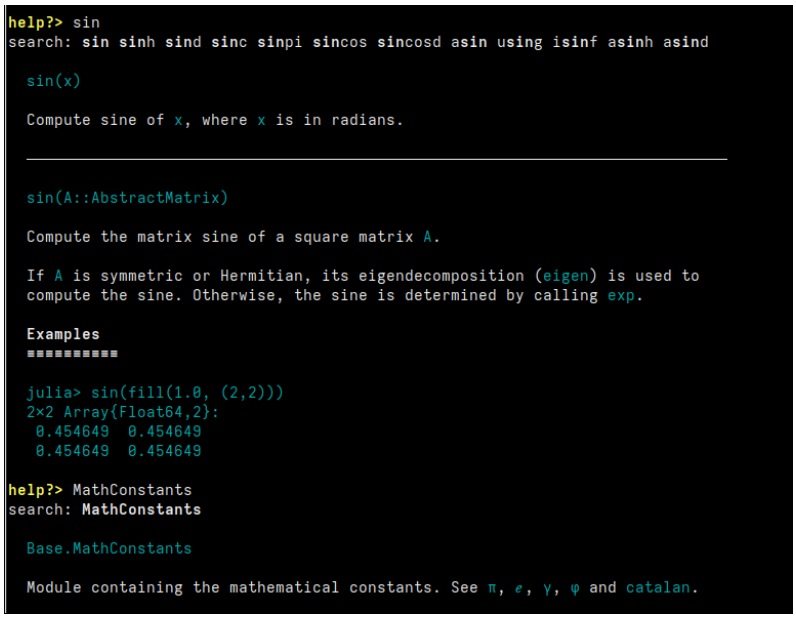
Например, для вывода справки о функции sin(), которая вычисляет синус угла, выполните:

```
?help?> sin
```

Для вывода справки о пакете или модуле также используется help?:

```
?help?> MathConstants
```

Пример вывода справки:



Справочную информацию о функции или пакете можно также получить с помощью @doc.

@doc – это макрос, который позволяет получить справку о функции, модуле или другом объекте. Для использования макроса введите команду вида:

```
@doc <имя_функции_или_объекта>
```

Например:

```
@doc sin
```

```
julia> @doc sin
  sin(x)

  Compute sine of x, where x is in radians.

  sin(A::AbstractMatrix)

  Compute the matrix sine of a square matrix A.

  If A is symmetric or Hermitian, its eigendecomposition (eigen) is used to compute the sine. Otherwise, the sine is determined by calling exp.

  Examples
  ==========

  julia> sin(fill(1.0, (2,2)))
  2×2 Array{Float64,2}:
   0.454649  0.454649
   0.454649  0.454649
```

Пример написания простого кода в программе и результаты его выполнения:

```
[user@localhost ~]$ julia
WARNING: Error during initialization of module LinearAlgebra:
ErrorException("could not load library "libopenblas64_"
libopenblas64_.so: cannot open shared object file: No such file or directory")
               _
   _       _ _(_)_     |  Documentation: https://docs.julialang.org
  (_)     | (_) (_)    |
   _ _   _| |_  __ _   |  Type "?" for help, "]?" for Pkg help.
  | | | | | | |/ _` |  |
  | | |_| | | | (_| |  |  Version 1.5.3 (2020-11-09)
 _/ |\__'_|_|_|\__'_|  |  Fedora %{fedora} build
|__/                   |

julia> bar() = (x = "Hello, Mars!"; return x)
bar (generic function with 1 method)

julia> function foo()
                    x = "Hello, "; x *= "World!"
                    return x
                end
foo (generic function with 1 method)

julia> foo()
"Hello, World!"

julia> bar()
"Hello, Mars!"
```

Tarantool — оптимизированный интерпретатор Lua

Возможности
Установка tarantool
Основные каталоги и файлы конфигурации
Интерактивная консоль
Создание базы данных с использованием Lua
Пример запуска Lua-скрипта в консоли tarantool
Пример работы с SQL
Управление экземплярами с помощью tarantoolctl
Исправление ошибок

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: tarantool-2.11.1-2

Tarantool — это одновременно резидентная база данных (размещаемая в оперативной памяти) и сервер приложений с поддержкой языка Lua.

Tarantool позволяет хранить и обрабатывать данные, разрабатывать приложения и ускорять работу системы. **Tarantool** можно использовать для работы с данными любого типа, копировать, сегментировать, распределяя большие объёмы данных по нескольким серверам и сочетая результаты, полученные от них, для создания отказоустойчивых кластеров. **Tarantool** подходит для серверов очередей, кешей, веб-приложений с отслеживанием состояния.

Возможности

Основные возможности сервера приложений:

- оптимизированный интерпретатор Lua, поддерживающий быстрый отслеживающий JIT-компилятор;
- совместная многозадачность, неблокирующий ввод-вывод;
- встроенная поддержка очередей задач;
- сегментирование данных и задач;
- встроенные средства для управления кластерами и развертывания приложений;
- коннекторы для взаимодействия с внешними базами данных;
- набор встроенных и автономных модулей.

Основные возможности базы данных:

- формат данных MessagePack и протокол клиент-сервер;
- два механизма хранения данных: хранение в оперативной памяти с полной сохраняемостью и собственная реализация LSM-tree, которая оптимизирована для работы с большими объёмами данных;
- несколько типов индексов: HASH, TREE, RTREE, BITSET;
- индексы путей в формате JSON;
- асинхронная и синхронная репликация;
- автоматическое избрание лидера с использованием алгоритма RAFT;
- аутентификация и контроль доступа;
- поддержка ANSI SQL;
- коннекторы для различных языков программирования.

Установка tarantool

Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install tarantool
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Основные каталоги и файлы конфигурации

По умолчанию создаются каталоги:

- **/etc/tarantool** — каталог для хранения всей конфигурации;
- **/var/log/tarantool** — каталог для хранения журналов;
- **/var/lib/tarantool** — каталог для хранения данных, которые распределяются между экземплярами.
- **/etc/tarantool/instances.available/*.lua** — файл инициализации **tarantool** по умолчанию с простыми в использовании примерами конфигурации, включая репликацию, сегментирование и все основные функции.

Интерактивная консоль

Для запуска интерактивной консоли **tarantool** введите команду:

```
tarantool
```

Примерный вывод:

```
Tarantool 2.4.2-68-g17621b0
type 'help' for interactive help
tarantool>
```

В консоли можно работать с языком Lua и SQL.

Создание базы данных с использованием Lua

1. Настройка конфигурации. Выполните настройку сервера с базовыми параметрами:

```
box.cfg{
    listen = 3301,  -- порт для подключения клиентов     memtx_memory = 1024 * 1024 * 256  -- размер памяти для хранения данных
(256 МБ) }
```

Результат:

```
2024-08-09 09:51:46.499 [6465] main/103/interactive C> Tarantool 2.4.2-68-g17621b0
2024-08-09 09:51:46.500 [6465] main/103/interactive C> log level 5
2024-08-09 09:51:46.501 [6465] main/103/interactive I> mapping 268435456 bytes for memtx tuple arena...
2024-08-09 09:51:46.504 [6465] main/103/interactive I> mapping 134217728 bytes for vinyl tuple arena...
2024-08-09 09:51:46.514 [6465] main/103/interactive I> instance uuid e753c2aa-3d14-4a8e-9c03-7b4412a87011
2024-08-09 09:51:46.514 [6465] iproto/101/main I> binary: bound to 0.0.0.0:3301
2024-08-09 09:51:46.514 [6465] main/103/interactive I> initializing an empty data directory
2024-08-09 09:51:46.570 [6465] main/103/interactive I> assigned id 1 to replica e753c2aa-3d14-4a8e-9c03-7b4412a87011
2024-08-09 09:51:46.570 [6465] main/103/interactive I> cluster uuid 21f5b9e0-775c-467e-9872-e3be40b06f0a
2024-08-09 09:51:46.572 [6465] snapshot/101/main I> saving snapshot `./00000000000000000000.snap.inprogress'
2024-08-09 09:51:46.589 [6465] snapshot/101/main I> done
2024-08-09 09:51:46.589 [6465] main/103/interactive I> ready to accept requests
2024-08-09 09:51:46.589 [6465] main/105/checkpoint_daemon I> scheduled next checkpoint for Fri Aug  9 11:08:02 2024
2024-08-09 09:51:46.590 [6465] main/103/interactive I> set 'listen' configuration option to "3301" ---
...
```

После выполнения команды сервер будет инициализирован.

2. Создание нового пространства имён:

```
box.schema.space.create('my_space')
```

где:

- my_space - это имя вашей первой базы данных.

Вывод:

```
---
- engine: memtx
  before_replace: 'function: 0x40736f18'
  on_replace: 'function: 0x40736ef0'
  ck_constraint: []
  field_count: 0
```

```
  temporary: false
  index: []
  is_local: false
  enabled: false
  name: my_space
  id: 514
- created
...
```

где:

- **engine: memtx** - движок хранения (memtx), используемый для этого пространства;
- **before_replace** и **on_replace** - функции, которые вызываются перед и после замены данных в этом пространстве;
- **ck_constraint** - ограничения, накладываемые на данные в этом пространстве (в данном случае пустой список);
- **field_count** - количество полей в этом пространстве (0);
- **temporary** - флаг, указывающий, является ли это пространство временным;
- **index** - список индексов, созданных для этого пространства;
- **is_local** - флаг, указывающий, является ли это пространство локальным;
- **enabled** - флаг, указывающий, включено ли это пространство;
- **name** - имя пространства ("my_space");
- **id** - идентификатор пространства (514);
- **- created** - подтверждает, что пространство успешно создано.

3. Создание индекса с именем primary для базы данных:

```
box.space.my_space:create_index('primary', {
    type = 'tree',
    parts = {1, 'unsigned'}
})
```

Результат:

```
---
- unique: true
  parts:
  - type: unsigned
    is_nullable: false
    fieldno: 1
  id: 0
  space_id: 512
  type: TREE
  name: primary
...
```

4. Добавление данных в базу данных:

```
box.space.my_space:insert{1, 'example data'}
```

Результат:

```
---
- [1, 'example data']
...
```

5. Выбор данных:

```
local result = box.space.my_space:select{}
for _, row in ipairs(result) do
    print(row[1], row[2])
end
```

Результат:

```
---
- [1, 'example data']
...
```

6. Удаление записи из пространства имен:

```
box.space.my_space:delete{1}
```

Результат:

```
---
- [1, 'example data']
...
```

Пример запуска Lua-скрипта в консоли tarantool

1. В терминале создайте файл **app.lua** с помощью текстового редактора:

```
nano app.lua
```

2. Напишите код Lua-скрипта в файле:

```lua
-- app.lua

-- Настройка конфигурации
box.cfg{
listen = 3301,
memtx_memory = 1024 * 1024 * 256
}

-- Проверка существования пространства и создание, если оно не существует
local space_name = 'example_space'
local space = box.space[space_name]

if not space then
space = box.schema.space.create(space_name)
space:create_index('primary', { type = 'tree', parts = {1, 'unsigned'} })
print('Space and index created.')
else
print('Space already exists.')
end

-- Добавление данных, если они ещё не существуют
local count = space:count()
if count == 0 then
space:insert{1, 'Hello, Tarantool!'}
print('Data inserted.')
else
print('Data already exists.')
end

-- Выбор данных и вывод
local result = space:select{}
print('Selected data:')
for _, row in ipairs(result) do
print(row[1], row[2])
end
```

Сохраните файл и закройте редактор. Для этого нажмите **Ctrl + O**, затем **Enter** для сохранения, и **Ctrl + X** для выхода.

3. Запустите консоль **tarantool**:

```
tarantool
```

4. В консоли **tarantool** выполните Lua-скрипт:

```
dofile('app.lua')
```

Результат:

```
Hello, Tarantool!
```

Пример работы с SQL

Tarantool поддерживает SQL-запросы. Для использования функций SQL, используя tarantool в качестве клиента, выполните:

1. Включение SQL-режима:

```
box.cfg{listen = 3301}
```

2. Для создания таблицы используйте команду **CREATE TABLE**:

```
box.execute('CREATE TABLE employees (id INTEGER PRIMARY KEY, name TEXT)')
```

Если SQL-запрос был выполнен успешно и затронул одну строку **- row_count: 1**, то таблица была успешно создана.

3. Чтобы вставить данные в таблицу, выполните команду **INSERT INTO**:

```
box.execute('INSERT INTO employees (id, name) VALUES (1, \'John Doe\')')
box.execute('INSERT INTO employees (id, name) VALUES (2, \'Jane Smith\')')
box.execute('INSERT INTO employees (id, name) VALUES (3, \'Alice Johnson\')')
```

Вывод **--- ...** после выполнения команды **box.execute()** в консоли **tarantool** указывает на то, что запрос был выполнен успешно, но подробная информация о результате не отображается в текущем выводе.

4. Для выбора данных из таблицы используйте команду **SELECT**:

```
local result = box.execute('SELECT * FROM employees')
for _, row in ipairs(result.rows) do
  print(row[1], row[2])
end
```

Вывод:

```
1	John Doe
2	Jane Smith
3	Alice Johnson
```

Для выхода из консоли используйте команду:

```
os.exit()
```

Управление экземплярами с помощью tarantoolctl

Tarantoolctl позволяет управлять экземплярами **tarantool**, выполнять команды SQL, подключаться к удаленным серверам и др.

Основные команды и опции, которые можно использовать с **tarantoolctl** для управления экземплярами **tarantool**:

1. Запуск экземпляра **tarantool** (example - замените на любое имя экземпляра):

```
sudo tarantoolctl start example
```

2. Остановка экземпляра **tarantool**:

```
sudo tarantoolctl stop example
```

3. Проверка состояния сервера:

```
sudo tarantoolctl status example
```

4. Перезапуск экземпляра:

```
sudo tarantoolctl restart example
```

5. Ротация логов:

```
tarantoolctl logrotate example
```

6. Проверка экземпляра:

```
tarantoolctl check example
```

7. Вход в командную строку интерфейса **tarantool**:

```
tarantoolctl enter example [--language=<language>]
```

8. Выполнение Lua-скрипта:

```
tarantoolctl eval example <FILE>
```

9. Выполнение команд через стандартный ввод:

```
<команда> | tarantoolctl eval example
```

10. Подключение к серверу **tarantool** по адресу example.com и порту 3301:

```
tarantoolctl connect tcp://example.com:3301
```

11. Передача команд через стандартный ввод на удаленный экземпляр:

Например, у вас есть сервер **tarantool**, работающий на хосте example.com и порту 3301. Вы хотите выполнить команду SQL, которая добавляет запись в таблицу, и затем получить результат.

```
echo "box.execute('INSERT INTO employees (id, name) VALUES (4, \'Jane Doe\')')" | tarantoolctl connect tcp://example.com:3301
```

12. Для получения информации об установленном **tarantoolctl** выполните:

```
tarantoolctl --help
```

13. Для определения списка запущенных на узле экземпляров класса **tarantool** используйте:

```
ls /etc/tarantool/instances.available
```

Исправление ошибок

При возникновении ошибки:

```
can't initialize storage: Failed to lock WAL directory . and hot_standby mode is off
```

В терминале выполните поиск запущенных процессов tarantool. Утилита **pgrep** работает следующим образом: вы задаете имя процесса, а утилита показывает его идентификатор:

```
sudo pgrep -f tarantool
```

Примерный вывод:

```
4143 5046 5181 5190
```

Принудительно завершить процессы можно, используя команду **kill -9**:

```
sudo kill -9 4143 sudo kill -9 5046 sudo kill -9 5181 sudo kill -9 5190
```

Java OpenJDK в РЕД ОС

В репозитории РЕД ОС доступно использование нескольких версий **Java OpenJDK**. Даже если у вас установлена последняя актуальная версия, некоторые программы могут устанавливать в качестве зависимостей другие (например, более старые) версии **JDK**, поэтому существует возможность иметь несколько версий **JDK** без возникновения конфликтов.

В РЕД ОС по умолчанию уже установлена **OpenJDK** версии **8**. Проверить это можно командой:

```
java -version

openjdk version "1.8.0_275"
OpenJDK Runtime Environment (build 1.8.0_275-b01)
OpenJDK 64-Bit Server VM (build 25.275-b01, mixed mode)
```

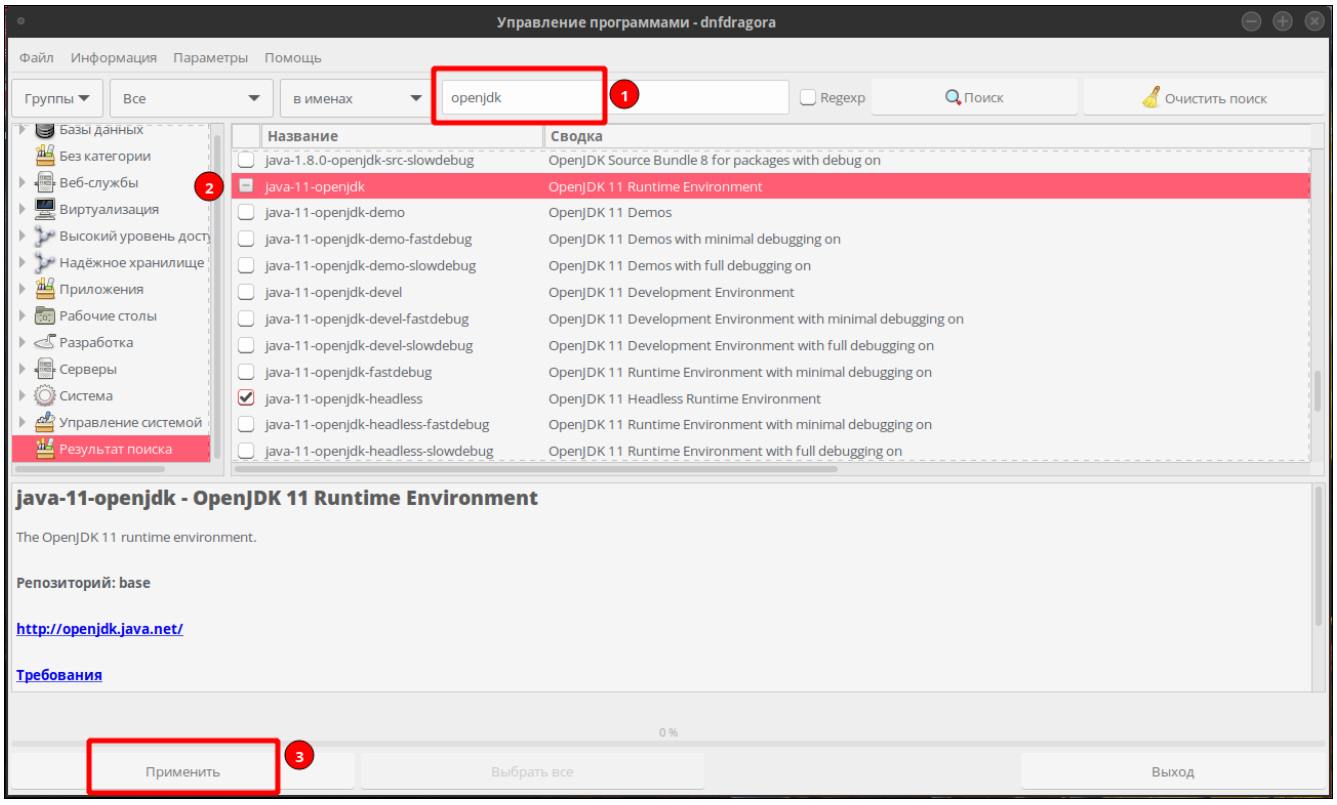
При необходимости можно установить более новую версию **Java**. В качестве примера установим **Java 11**. Сделать это можно двумя способами:

- 1 способ — через графический менеджер пакетов **dnfdragora**.

В «**Главном меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**» выполните поиск необходимых пакетов по ключевому слову «**openjdk**» и отметьте галочками пакеты:

- **java-11-openjdk**;
- **java-11-openjdk-headless**.

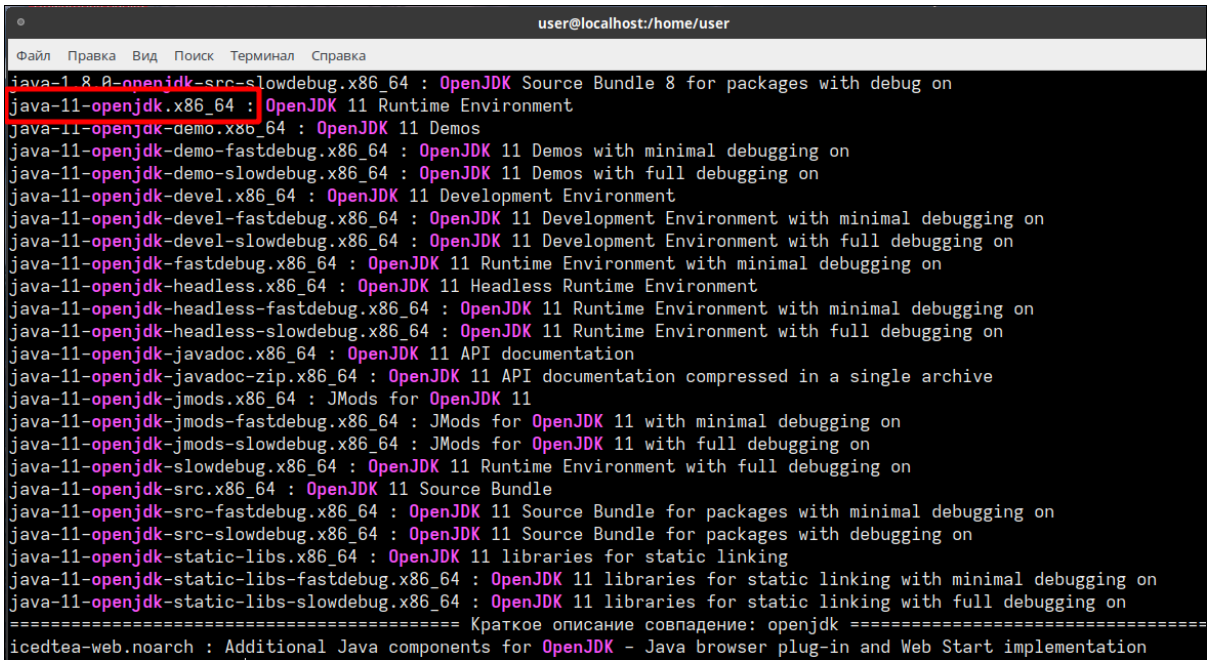
После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



- 2 способ — через терминал.

Для этого необходимо проверить доступные для установки пакеты с помощью команды:

```
dnf search openjdk
```



Затем из полученного списка нужно установить файл вида «**java-<версия>-openjdk**».

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install java-11-openjdk
```

После установки новой версии по умолчанию будет использоваться именно она. Проверить используемую версию можно следующей командой:

```
java -version

openjdk version "11.0.10" 2021-01-19 LTS
OpenJDK Runtime Environment 18.9 (build 11.0.10+9-LTS)
OpenJDK 64-Bit Server VM 18.9 (build 11.0.10+9-LTS, mixed mode, sharing)
```

Для того чтобы при необходимости переключаться на ту или иную версию **OpenJDK**, выполните команду:

```
alternatives --config java

Имеется 2 программ, которые предоставляют 'java'.

  Выбор    Команда
-----------------------------------------------
   1           java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.275.b01-1.el7.x86_64/jre/bin/java)
*+ 2           java-11-openjdk.x86_64 (/usr/lib/jvm/java-11-openjdk-11.0.10.0.9-1.el7.x86_64/bin/java)

Enter - сохранить текущий выбор[+], или укажите номер: 1
```

Знаком «**+**» выделена версия, используемая по умолчанию. Для переключения на необходимую для работы версию следует указать ее порядковый номер или нажать **Enter**, если нужная версия выбрана.

Проверим установленный выбор командой:

```
java -version

openjdk version "1.8.0_275"
OpenJDK Runtime Environment (build 1.8.0_275-b01)
OpenJDK 64-Bit Server VM (build 25.275-b01, mixed mode)
```

PHP 8.X на РЕД ОС

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: php81-release, php82-release, php83-release

Пакеты **PHP** версии **8.1, 8.2, 8.3** располагаются в подключаемых репозиториях, поэтому порядок обновления несколько отличается от обычного.

Установка и обновление пакетов **PHP** до версии **8.X** на **РЕД ОС** производится с помощью следующих команд (потребуются права пользователя **root**):

```
dnf install php8X-release
dnf clean all
dnf makecache
dnf update php*
```

где X — номер необходимой для установки версии.

Сбор диагностической информации о РЕД ОС (loginfo)

Графический интерфейс
Консольный вариант

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО:** loginfo-0.15-1

loginfo – утилита сбора технической информации о РЕД ОС для технической поддержки.

Вы можете подробнее ознакомиться с работой утилиты **loginfo**, просмотрев наши обучающие видео:

- на **RuTube** — Сбор диагностической информации о РЕД ОС;
- в **Яндекс.Дзен** — Сбор диагностической информации о РЕД ОС;
- в **VK Видео** — Сбор диагностической информации о РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

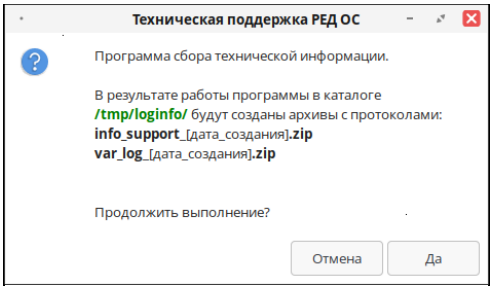
и выполните команду:

```
dnf install loginfo
```

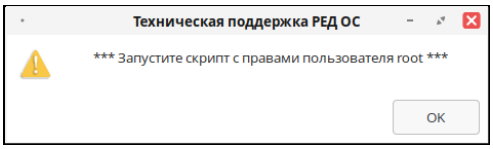
Графический интерфейс

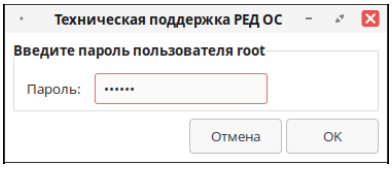
Запуск утилиты доступен из «**Главного меню**» - «**Системные**» - «**Сбор информации о системе**».

При инициализации утилиты вы увидите следующее диалоговое окно:

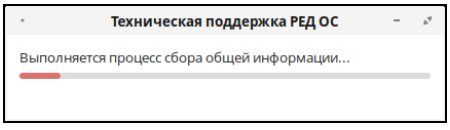


Т.к. для работы в программе необходимы права пользователя **root**, будет выведено следующее предупреждение и произведен запрос на ввод пароля пользователя **root**.



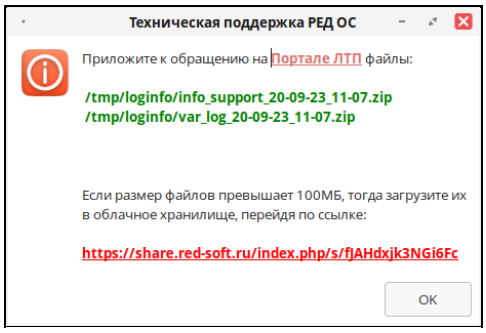


Будет запущен процесс сбора информации.



После сбора информации будет выведено информационное сообщение с контактами для отправки собранных данных в техническую поддержку.

Архивные файлы будут сформированы по пути **/tmp/loginfo**.



Консольный вариант

Для работы с утилитой необходимы права пользователя **root**:

```
su -
```

Для запуска процесса сбора информации выполните:

```
loginfo.sh
```

Loginfo также поддерживает дополнительный функционал, для просмотра выполните:

```
loginfo.sh --help
```

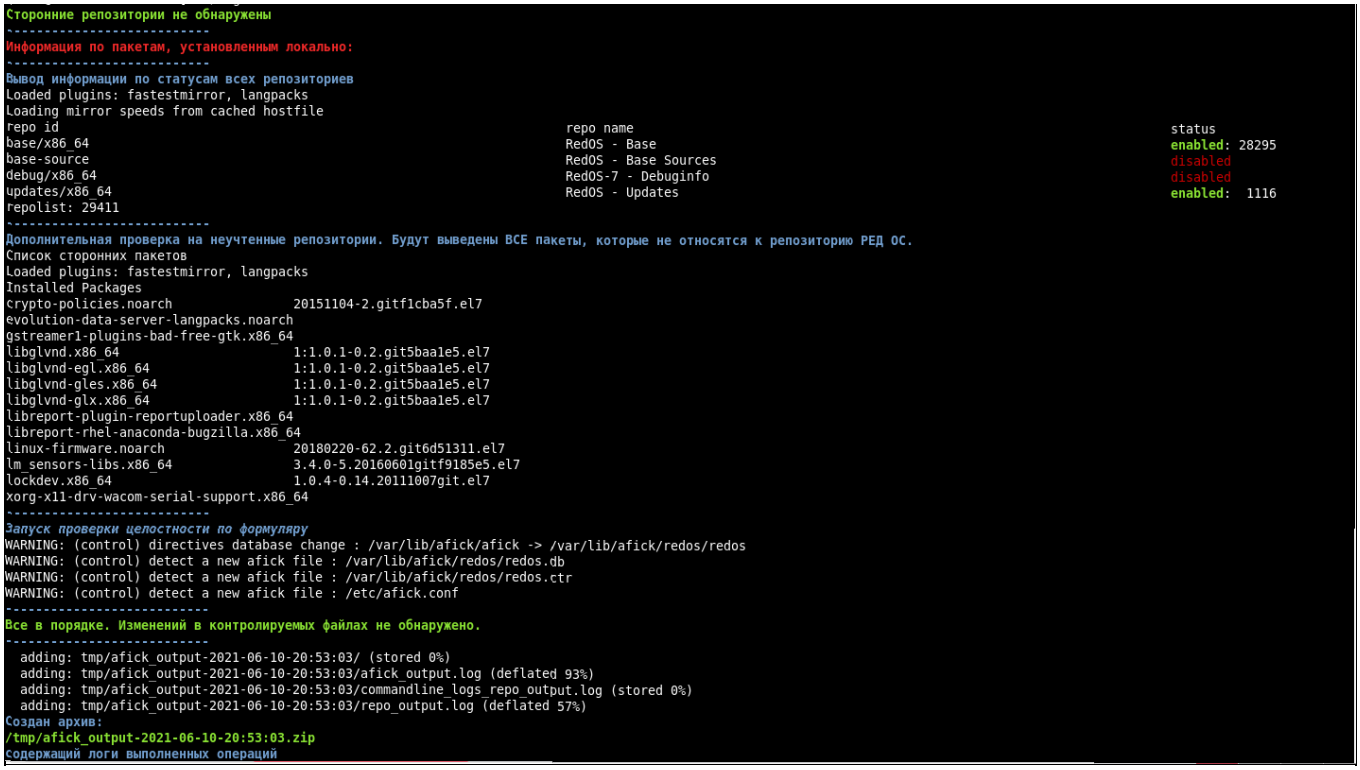
Для примера выполним дополнительную диагностику ОС.

Создание краткой сводки по аппаратным характеристикам:

```
loginfo.sh --hw-id

Создан файл /tmp/loginfo/hw-id-2022-06-21-11-50-35.txt
```

Проверка целостности сертифицированной редакции РЕД ОС:

```
loginfo.sh --afick
```



Контроль целостности системы РЕД ОС также осуществляется с помощью утилиты **afick**. Подробнее см. в нашей статье «Afick - утилита контроля целостности системы».

Проверка файловой системы на наличие ошибок

Параметры fsck
Пример проверки диска на ошибки с помощью fsck
Запуск автоматической проверки и исправления найденных ошибок
Ручное добавление параметров в меню GRUB при загрузке ОС
Добавление параметров в меню GRUB с помощью утилиты grubby
Создание файла /forcefsck
Запуск проверки в ручном режиме
Использование загрузочного диска/flash для проверки файловой системы на ошибки
Проверка LVM-разделов с помощью утилиты fsck

В определенных случаях (в результате сбоя или некорректного завершения работы) на файловой системе могут накапливаться ошибки. В РЕД ОС для проверки файловой системы и исправления ошибок имеется утилита **fsck** ("file system consistency check").

Инструмент fsck обладает следующим функционалом:

- проверка файловой системы при возникновении проблем (не загружается система/поврежденные файлы) или в качестве профилактического обслуживания;
- диагностика состояния внешних накопителей, таких как SD-карты или USB-накопители.

Базовый синтаксис соответствует следующему шаблону:

```
fsck <опции> <файловая_система>
```

В качестве *файловой системы* может быть устройство, точка монтирования или раздел, в том числе LVM.

Вы можете подробнее ознакомиться с возможностями проверки файловой системы на наличие ошибок, просмотрев наши обучающие видео:

- на **RuTube** — Проверка файловой системы на наличие ошибок;
- в **Яндекс.Дзен** — Проверка файловой системы на наличие ошибок;
- в **VK Видео** — Проверка файловой системы на наличие ошибок.

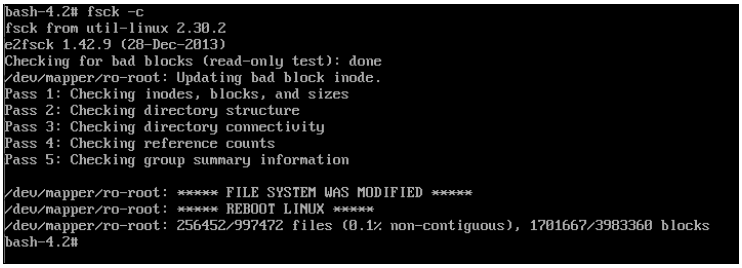
На наших каналах вы также сможете найти много другой полезной информации.

Параметры fsck

fsck -p – утилита автоматически исправит найденные ошибки.

Вывод аналогичен простой проверке.

fsck -c – проверка файловой системы на поврежденные сектора.



Для получения списка команд наберите **fsck --help** или **fsck -h.**

Опция	Описание
-a	Устаревшая опция. Указывает исправлять все найденные ошибки без одобрения пользователя.
-r	Применяется для файловых систем ext. Указывает fsck спрашивать пользователя перед исправлением каждой ошибки
-n	Выполняет только проверку ФС, без исправления ошибок. Используется также для получения информации о ФС
-c	Применяется для файловых систем ext3/4. Помечает все повреждённые блоки для исключения последующей записи в них
-f	Принудительно проверяет ФС, даже если ФС исправна
-y	Автоматически подтверждает запросы к пользователю

-b	Задаёт адрес суперблока
-p	Автоматически исправлять найденные ошибки. Заменяет устаревшую опцию -a
-A	Проверяет все ФС
-C [<fd>]	Показывает статус выполнения. Здесь fd – дескриптор файла при отображении через графический интерфейс
-l	Блокирует устройство для исключительного доступа
-M	Запрещает проверять примонтированные ФС
-N	Показывает имитацию выполнения, без запуска реальной проверки
-P	Проверять вместе с корневой ФС
-R	Пропускает проверку корневой ФС. Может использоваться только совместно с опцией -A
-r [<fd>]	Выводит статистику для каждого проверенного устройства
-T	Не показывать заголовок при запуске
-t <тип>	Задаёт ФС для проверки. Можно задавать несколько ФС, перечисляя через запятую
-V	Выводит подробное описание выполняемых действий

Пример проверки диска на ошибки с помощью fsck

Запуск автоматической проверки и исправления найденных ошибок

Существует несколько способов запуска автоматической проверки на ошибки:

1. Ручное добавление параметров в меню **GRUB** при загрузке ОС.

2. Добавление параметров в меню **GRUB** с помощью утилиты **grubby**.

3. Создание файла **/forcefsck**.

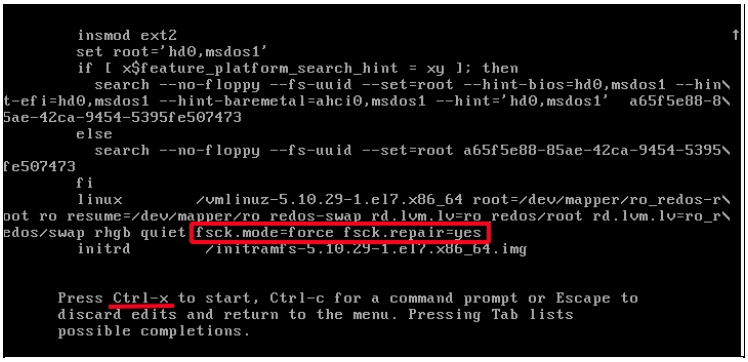
1. Ручное добавление параметров в меню GRUB при загрузке ОС

Первый вариант проверки и исправления ошибок на разделах жесткого диска.

В меню **GRUB** перейдите в режим редактирования загрузочной строки, нажав при этом клавишу **e**. Добавьте параметры:

```
fsck.mode=force fsck.repair=yes
```

в конец предпоследней строки.



Нажмите **Ctrl+X** для запуска ОС с этими параметрами, во время запуска будет произведена проверка разделов диска, и при наличии ошибок произведено их исправление.

2. Добавление параметров в меню GRUB с помощью утилиты grubby

Существует еще один способ добавления параметров ядра для принудительной проверки файловой системы на ошибки и их исправления. Добавить параметры можно командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --args="fsck.mode=force fsck.repair=yes"
```

Удалить установленные параметры можно следующей командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --remove-args="fsck.mode=force fsck.repair=yes"
```

3. Создание файла /forcefsck

Бывают ситуации, когда систему необходимо проверить на наличие ошибок в *незапланированный* момент. Для этого можно **принудительно** запустить утилиту **fsck** для проверки при следующей перезагрузке. Запуск осуществляется командой:

```
sudo touch /forcefsck
```

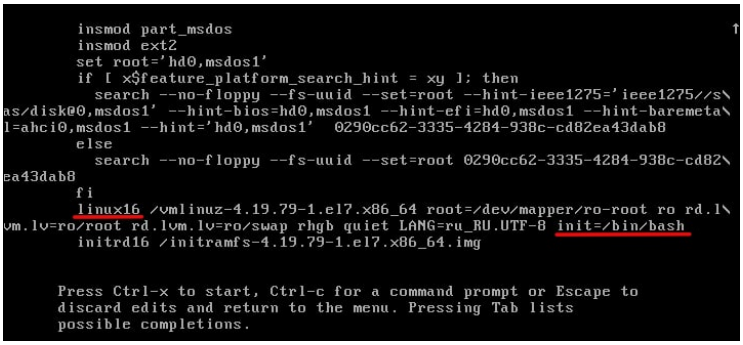
Команда **sudo** (после ввода пароля) предоставит права для создания с помощью **touch** пустого файла в корне диска **/forcefsck**, который послужит сигналом (флагом) для **fsck**, что нужно проверить диски.

Останется только перезагрузить компьютер и **fsck** начнет проверять все жесткие диски, указанные в **/etc/fstab**.

Запуск проверки в ручном режиме

Следующий метод относится к проверке диска, когда операционная система загружена в режиме **single mode**.

1. Запустим ОС в single mode, для этого пропишите в меню загрузки grub параметр init=/bin/bash в конце строки, которая начинается на linux16, см. рисунок.



Также данная строка может начинаться с linuxefi, этот параметр характерен для систем с загрузкой в UEFI. Нажмите **"ctrl+x"** для запуска с этим параметром(init=/bin/bash).

2. Запустите проверку выполнив команду:

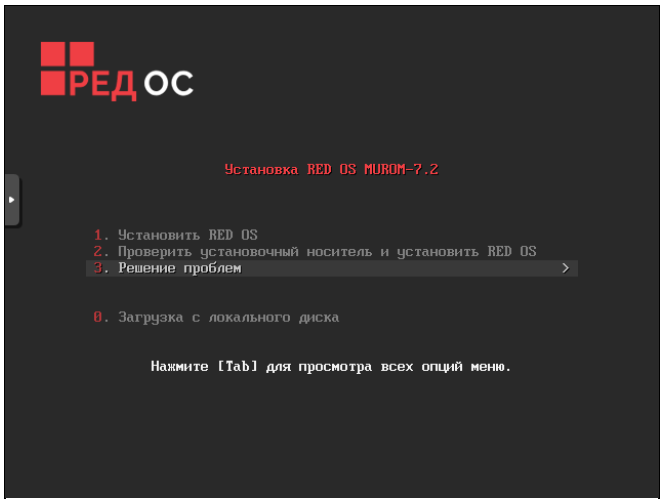
```
/usr/sbin/fsck -ACVfyv
```

Во время проверки на экране появится отчет о выполненных операциях, если отчет длинный, то можно его можно пролистать вверх сочетанием клавиш shift+PageUp. После проверки дисков перезагрузите компьютер, нажав на кнопку на системном блоке.

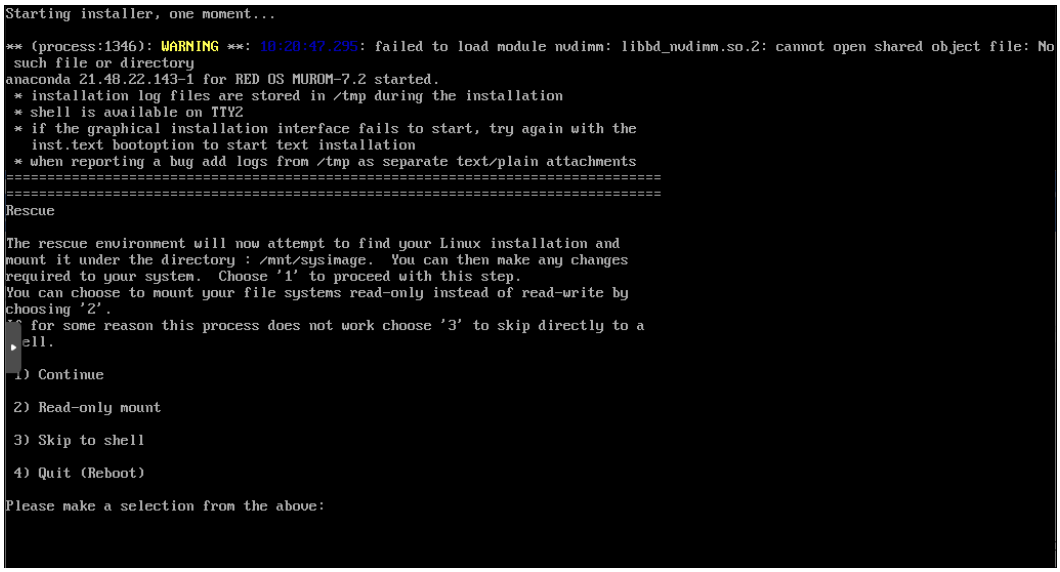
Наглядное видео примера проверки диска на ошибки:

Использование загрузочного диска/flash для проверки файловой системы на ошибки.

Загрузившись в режим восстановления операционной системы РЕД ОС с помощью загрузочного диска или съемного накопителя с установленным образом операционной системы РЕД ОС. Выберите пункт: **«Решение проблем» -> «Исправить установленную RED OS»**.



Система перезагрузится в режим восстановления. Введите «**2**» и нажмите 2 раза **Enter**. Так вы смонтируете операционную систему в режим «**Только для чтения**»



Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Потом введите команду:

```
# chroot /mnt/sysimage
```

После этого можете вводить **fsck**:

```
# fsck -ACVfyv
```

Если проверка завершится с такой ошибкой:

```
[путь_к_файловой_системе] is mounted
```

Введите:

```
umount [путь_к_файловой_системе]
```

И еще раз запустите утилиту **fsck**:

```
# fsck -ACVfyv
fsck from util-linux 2.30.2
...
```

Если система не выявит ошибок, то получится такой вывод:

```
[путь_к_файловой_системе] clean …
```

Чтобы выйти из режима восстановления, вы должны смонтировать все разделы, которые были отмонтированы командой **umount**, с помощью команды **mount**, нажать сочетание клавиш **ctrl+d**, а затем ввести команду **reboot**, которая перезапустит вашу операционную систему.

```
# reboot
```

По умолчанию, утилита **fsck** при проверке будет использовать разделы, указанные в **/etc/fstab/**, сформированные при установке операционной системы РЕД ОС.

Проверка LVM-разделов с помощью утилиты fsck

Перед проведением проверки необходимо найти устройство и размонтировать его.

Для просмотра всех подключенных устройств и проверки расположения диска выполните команду:

```
lsblk

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 20G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 19G 0 part
├─ro_redos-root 253:0 0 17G 0 lvm /
└─ro_redos-swap 253:1 0 2G 0 lvm [SWAP]
sr0 11:0 1 4,3G 0 rom /run/media/user/redos-MUROM-7.3.1 x86_64
```

При попытке запустить проверку на смонтированном диске или разделе в консоли появляется предупреждение о том, что невозможно продолжить проверку, так как диск смонтирован.

```
fsck -nf /dev/ro_redos/root

fsck из util-linux 2.37.3
e2fsck 1.44.6 (5-Mar-2019)
Warning! /dev/mapper/ro_redos-root is mounted.
```

Для того чтобы размонтировать диск, следует использовать команду:

```
umount <файловая_система>
```

Однако попытка выполнить данную процедуру на работающей ОС ни к чему не приведет.

```
umount /dev/ro_redos/root

umount: /: target is busy.
```

Также проблемой при попытке проверить LVM-разделы может быть и то, что они являются не активными. Для проверки следует использовать команду:

```
lvscan

ACTIVE '/dev/ro_redos/swap' [2,00 GiB] inherit
ACTIVE '/dev/ro_redos/root' [<17,00 GiB] inherit
```

Для активации раздела служит команда:

```
vgchange –ay <раздел>
```

Таким образом, можно сделать вывод, что проверка LVM-разделов через консоль с использованием утилиты **fsck** невозможна. Но это не значит, что LVM-разделы совсем не подлежат проверке. Существует как минимум два способа, позволяющие провести диагностику LVM-разделов.

Первым способом является проведение проверки через консоль загрузчика операционной системы **GRUB**.

А вторым - запуск утилиты **fsck** в **live-сессии** системы.

Очевидным плюсом при проверке дисковых пространств, в том числе LVM-разделов, через live-сессию является то, что разделы там по умолчанию являются не смонтированными. Поэтому проверка LVM-раздела будет выполнена с первого раза.

```
[root@redos ~]# fsck /dev/ro_redos/root
fsck из util-linux 2.34
e2fsck 1.44.6 (5-Mar-2019)
/dev/mapper/ro_redos-root: recovering journal
Clearing orphaned inode 423398 (uid=0, gid=0, mode=0100644, size=229605)
Clearing orphaned inode 172559 (uid=0, gid=0, mode=0100644, size=24992)
Clearing orphaned inode 387 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 386 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 384 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 296594 (uid=1000, gid=1000, mode=0100644, size=9059)
Setting free inodes count to 890417 (was 890569)
Setting free blocks count to 2578845 (was 2585477)
/dev/mapper/ro_redos-root: clean, 223695/1114112 files, 1876579/4455424 blocks
```

Проверка состояния жесткого диска

Smartmontools
Gsmartcontrol
Gnome disk utility
BadBlocks

Smartmontools

Smartmontools — утилита, предназначенная для проверки состояния жесткого диска. Чтобы посмотреть количество установленных жестких дисков наберите команду:

```
$ sudo smartctl --scan
```

На запрос пароля привилегированного пользователя, введите пароль локального пользователя с правами администратора.

Чтобы посмотреть информацию о жестком диске, а также узнать, поддерживает ли он технологию анализа SMART и включена ли она, наберите команду:

```
smartctl -i /dev/sda

smartctl 6.6 2018-08-10 r4748 [x86_64-linux-4.19.56-2.el7.x86_64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org
=== START OF INFORMATION SECTION ===
Model Family: Seagate Barracuda 3.5
Device Model: ST1000DM010-2EP102
Serial Number: ZN179JYJ
LU WWN Device Id: 5 000c50 0b6491aa4
Firmware Version: CC43
User Capacity: 1 000 204 886 016 bytes [1,00 TB]
Sector Sizes: 512 bytes logical, 4096 bytes physical
Rotation Rate: 7200 rpm
Form Factor: 3.5 inches
Device is: In smartctl database [for details use: -P show]
ATA Version is: ATA8-ACS T13/1699-D revision 4
SATA Version is: SATA 3.0, 6.0 Gb/s (current: 3.0 Gb/s)
Local Time is: Thu Aug 22 14:01:23 2019 MSK
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

В данном выводе указана информация о вашем жестком диске.

SMART support is: Available - device has SMART capability — жесткий диск поддерживает технологию анализа SMART. Если технология не поддерживается, вместо слова **Available** будет **Unavailable**.

SMART support is: Enabled — технология анализа SMART включена. Если она выключена у вас, то для включения введите:

```
smartctl -s on /dev/sda
```

Для выключения:

```
smartctl -s off /dev/sda
```

Для вывода атрибутов SMART введите:

```
smartctl -A /dev/sda
```

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 10
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000f   080   072   006    Pre-fail  Always       -       110427890
  3 Spin_Up_Time            0x0003   097   097   000    Pre-fail  Always       -       0
  4 Start_Stop_Count        0x0032   100   100   020    Old_age   Always       -       25
  5 Reallocated_Sector_Ct   0x0033   100   100   010    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000f   100   253   045    Pre-fail  Always       -       716102
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       42
 10 Spin_Retry_Count        0x0013   100   100   097    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   020    Old_age   Always       -       25
183 Runtime_Bad_Block       0x0032   100   100   000    Old_age   Always       -       0
184 End-to-End_Error        0x0032   100   100   099    Old_age   Always       -       0
187 Reported_Uncorrect      0x0032   100   100   000    Old_age   Always       -       0
188 Command_Timeout         0x0032   100   100   000    Old_age   Always       -       0 0 0
189 High_Fly_Writes         0x003a   100   100   000    Old_age   Always       -       0
190 Airflow_Temperature_Cel 0x0022   070   059   040    Old_age   Always       -       30 (Min/Max 24/30)
193 Load_Cycle_Count        0x0032   100   100   000    Old_age   Always       -       25
194 Temperature_Celsius     0x0022   030   021   000    Old_age   Always       -       30 (0 21 0 0 0)
195 Hardware_ECC_Recovered  0x001a   003   003   000    Old_age   Always       -       110427890
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   200   200   000    Old_age   Always       -       0
240 Head_Flying_Hours       0x0000   100   253   000    Old_age   Offline      -       42h+36m+02.609s
241 Total_LBAs_Written      0x0000   100   253   000    Old_age   Offline      -       85113048
242 Total_LBAs_Read         0x0000   100   253   000    Old_age   Offline      -       25314842
```

В данном выводе стоит смотреть на значения в колонке **RAW_VALUE**.

Наиболее важные атрибуты отмечены как **pre_fail** в колонке **TYPE**.
1 Raw_Read_Error_Rate — количество ошибок чтения. На дисках Seagate и Samsung большие значения - норма.

2 Spin_Up_Time — время раскрутки диска из состояния покоя до рабочей скорости. Растет при износе диска.

5 Rellocated Sector Count — количество переназначенных секторов. Если диск обнаружил ошибку чтения/записи он перенесет сектор в резерв. Чем меньше значение, тем лучше.

7 Seek Error Rate — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики или поверхности жёсткого диска.

196 Rellocation Event Count - число операций переназначения. **Raw Value** хранит общее число попыток переноса информации с переназначенных секторов в резервную область как успешных так и провальных.
Более подробную информацию можно найти на странице википедии.

Для того, чтобы провести тест самодиагностики, наберите команду:

```
smartctl -t <тип_теста> /dev/sda
```

Тип теста может быть:

- **long** — расширенный;
- **short** — короткий;
- **conveyance** — тест на выявления ошибок при записи/чтении.

Тесты выполняются в фоновом режиме. Чтобы просмотреть результат, наберите:

```
smartctl -l selftest /dev/sda

=== START OF READ SMART DATA SECTION ===
SMART Self-test log structure revision number 1
Num Test_Description Status Remaining LifeTime(hours) LBA_of_first_error
# 1 Conveyance offline Self-test routine in progress 60% 43 -
# 2 Short offline Completed without error 00% 42 -
# 3 Short offline Aborted by host 90% 42 -
# 4 Short captive Completed without error 00% 41 -
# 5 Short offline Completed without error 00% 41 -
```

Completed without error означает, что тест завершился без ошибок.

Для просмотра полной информации, включающей в себя показатели атрибутов SMART, информацию о жестком диске и результаты диагностических тестов, наберите:

```
$ sudo smartctl -a /dev/sda
```

Gsmartcontrol

Gsmartcontrol — это графическая утилита к **smartctl**, позволяющая оценивать состояние и работоспособность жёсткого диска или

твердотельного накопителя по показаниям S.M.A.R.T.

Основными возможностями программы являются:

- вывод информации об ошибках работы дисков;
- отображение информации о дисках, атрибутов, статистики;
- включение/выключение автоматического сбора данных о состоянии дисков;
- выполнение тестов «SMART self-tests»;
- включение/выключение SMART;
- создание отчетов по проведенным тестам.

Вы можете подробнее ознакомиться с информацией о проверке состояния жесткого диска, просмотрев наши обучающие видео:

- на **RuTube** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **Яндекс.Дзен** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **VK Видео** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install gsmartcontrol
```

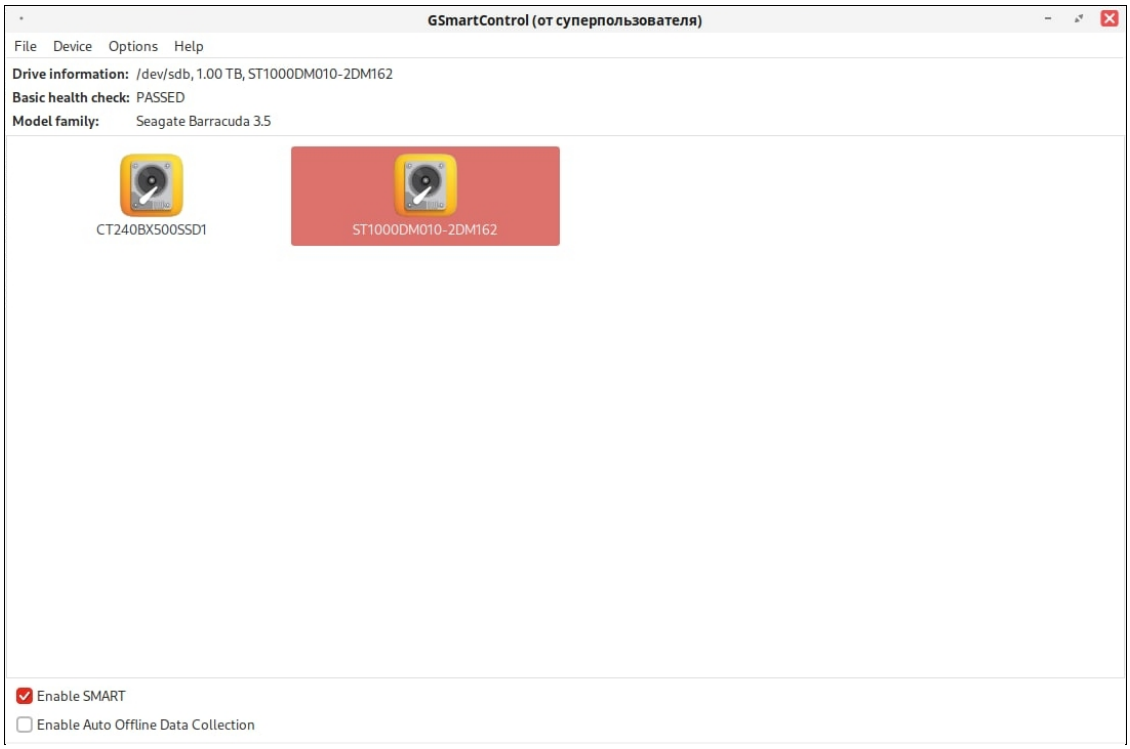
После установки программа будет доступна из «**Главного меню**» - «**Системные**» - «**Контроль S.M.A.R.T.**» или при помощи команды в терминале:

```
gsmartcontrol
```

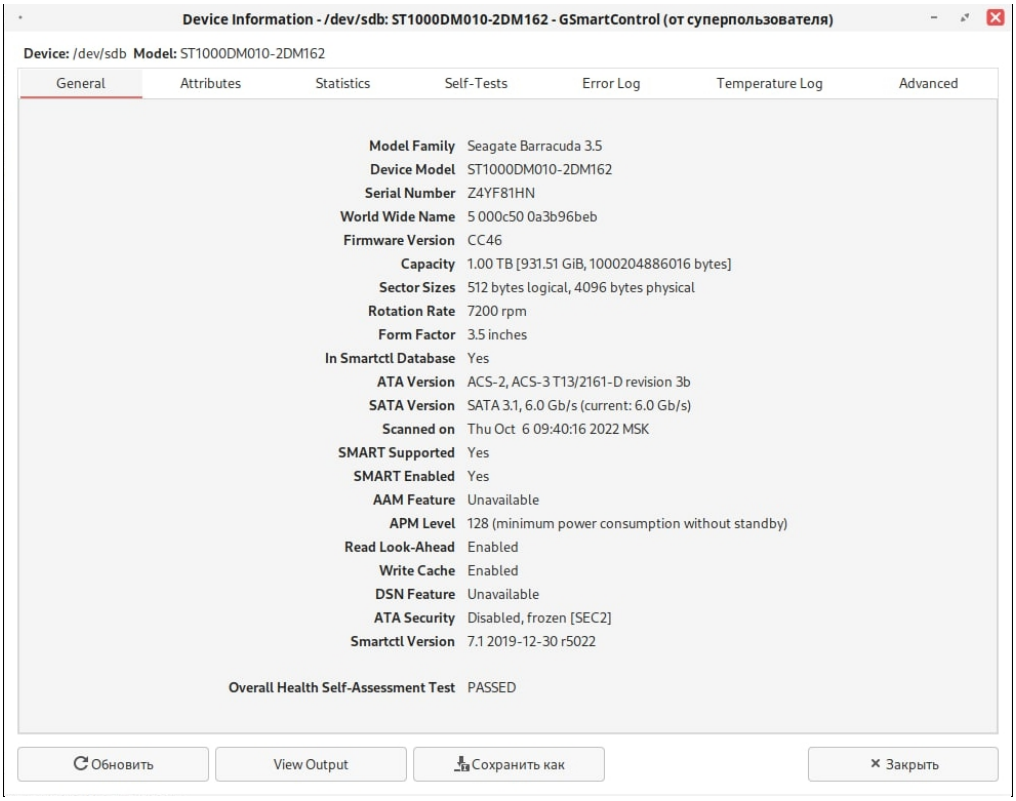
Обратите внимание, что для работы с утилитой необходимы права администратора или суперпользователя (**root**) системы.

Работа с утилитой

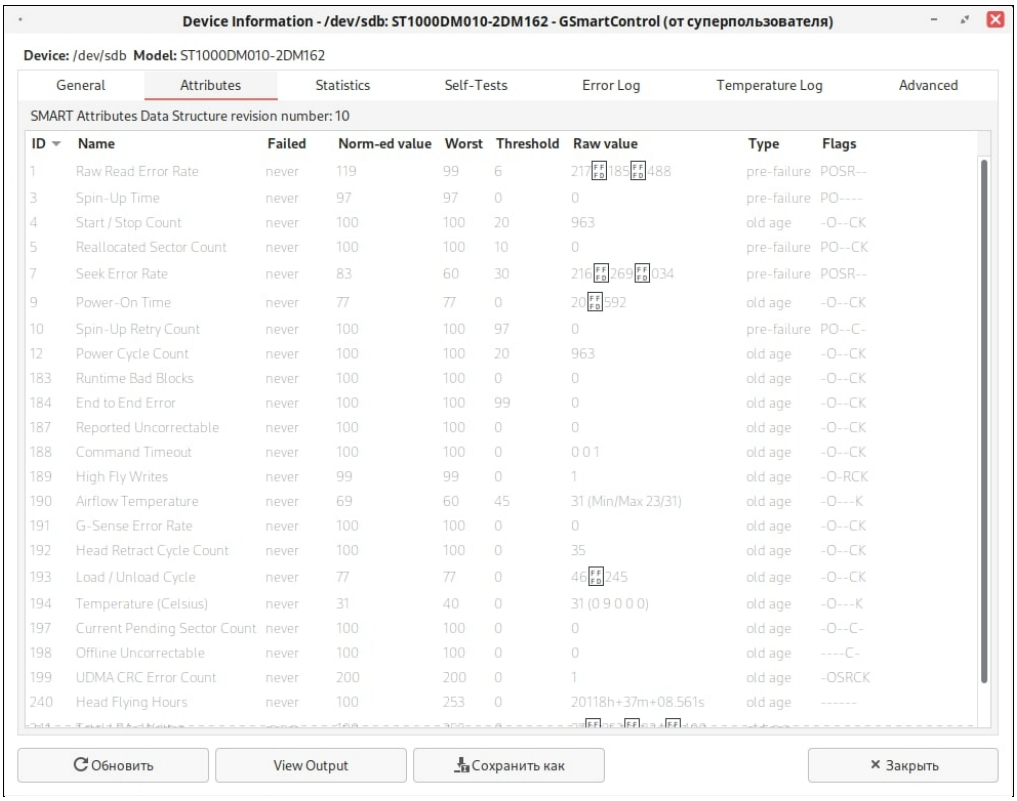
При запуске программа выглядит следующим образом:



Здесь отображены все диски, доступные для сканирования. При нажатии ПКМ на нужный диск выберите «**View details**», на вкладке «**General**» будет выведена вся информация о диске.



На вкладке «**Attributes**» указаны атрибуты проверки, нормальное, плохое и пороговое значение для каждого атрибута для удобного ориентирования по выявленным значениям в ходе проверок диска.



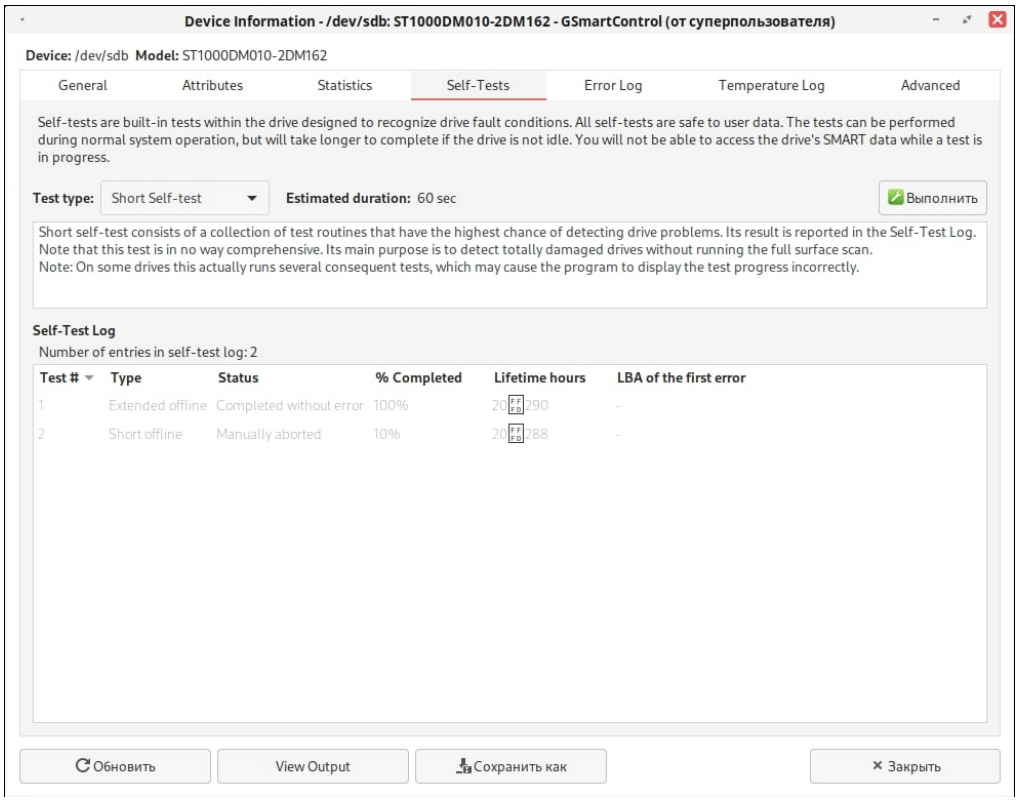
Часто используемые атрибуты:

- **Raw Read Error Rate** — частота ошибок при чтении данных с диска, происхождение которых обусловлено аппаратной частью диска, если значение большое, значит ошибки встречаются редко;
- **Spin-Up Time** — время раскрутки пакета дисков из состояния покоя до рабочей скорости, значение возрастает при износе диска;
- **Start/Stop Count** — полное число циклов запуск-остановка шпинделя. У дисков некоторых производителей (например, Seagate) — счётчик включения режима энергосбережения. В поле raw value хранится общее количество запусков/остановок диска;
- **Reallocated Sectors Count** — число операций переназначения секторов. Когда диск обнаруживает ошибку чтения/записи, он помечает сектор «переназначенным» и переносит данные в специально отведённую резервную область. Чем больше значение, тем хуже состояние поверхности дисков. Поле raw value содержит общее количество переназначенных секторов;
- **Seek Error Rat**e — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики и/или поверхности жёсткого диска;
- **Power-On Time** — число часов (минут, секунд — в зависимости от производителя), проведённых во включенном состоянии;
- **Spin-Up Retry Count** — число повторных попыток раскрутки дисков до рабочей скорости в случае, если первая попытка была неудачной. Если значение атрибута увеличивается, то велика вероятность неполадок с механической частью;
- **Power Cycle Count** — количество полных циклов включения-выключения диска;
- **End-to-End error** — данный атрибут - часть технологии HP SMART IV - означает, что после передачи данных через кэш-память чётность данных между хостом и жестким диском не совпадает;
- **Reported Uncorrectable** — ошибки, которые не могли быть восстановлены, используя методы устранения ошибки аппаратными средствами;
- **Command Timeout** — количество прерванных операций в связи с HDD тайм-аут. Обычно это значение атрибута должно быть равно нулю, и, если значение гораздо выше нуля, то, скорее всего, там будут какие-то серьезные проблемы с питанием или окисленные кабели для передачи данных;
- **Airflow Temperature** — температура воздуха внутри корпуса жёсткого диска;
- **G-sense Error Rate** — количество ошибок, возникающих в результате ударных нагрузок. Атрибут хранит показания встроенного акселерометра, который фиксирует все удары, толчки, падения и даже неаккуратную установку диска в корпус компьютера;
- **Load/Unload Cycle** — количество циклов перемещения блока магнитных головок в парковочную зону / в рабочее положение;
- **Temperature** — температура жёсткого диска;
- **Current Pending Sector Count** — число секторов, являющихся кандидатами на замену. Они пока не определены как плохие, но считывание с них отличается от чтения стабильного сектора, это так называемые подозрительные или нестабильные сектора;
- **Head flying hours** — время позиционирования головок.

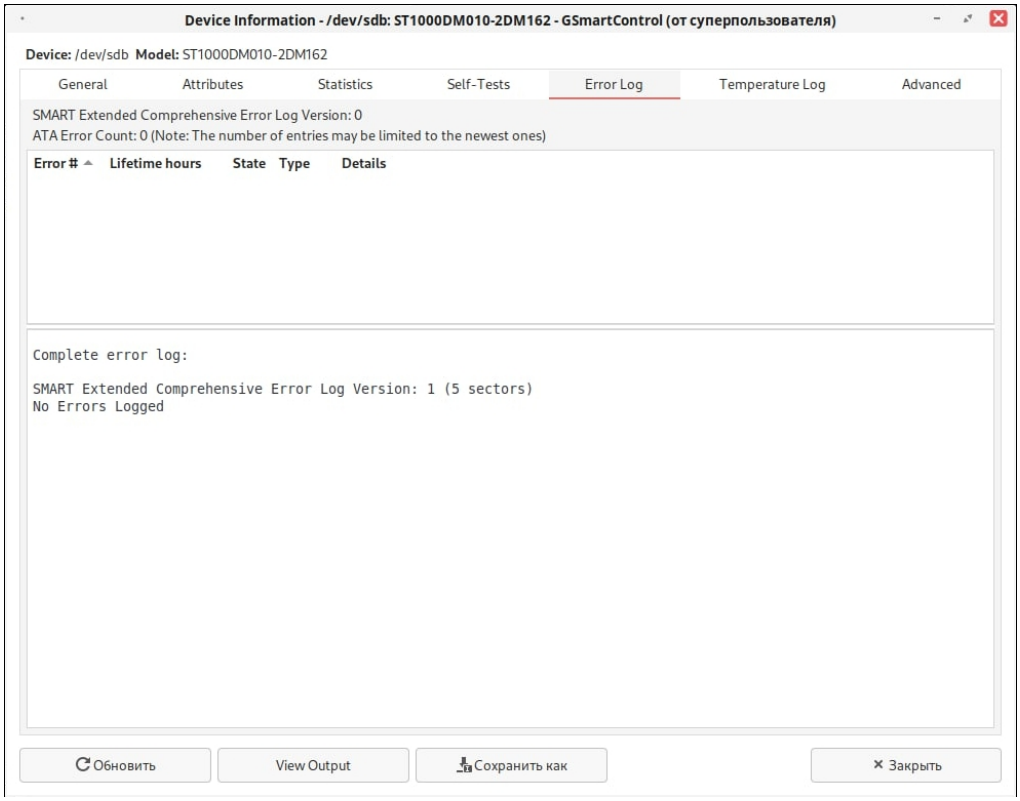
На вкладке «**Statistics**» выводится статистика использования диска.

На вкладке «**Self-Tests**» можно выполнять проверки жесткого диска. Доступно три варианта проверки:

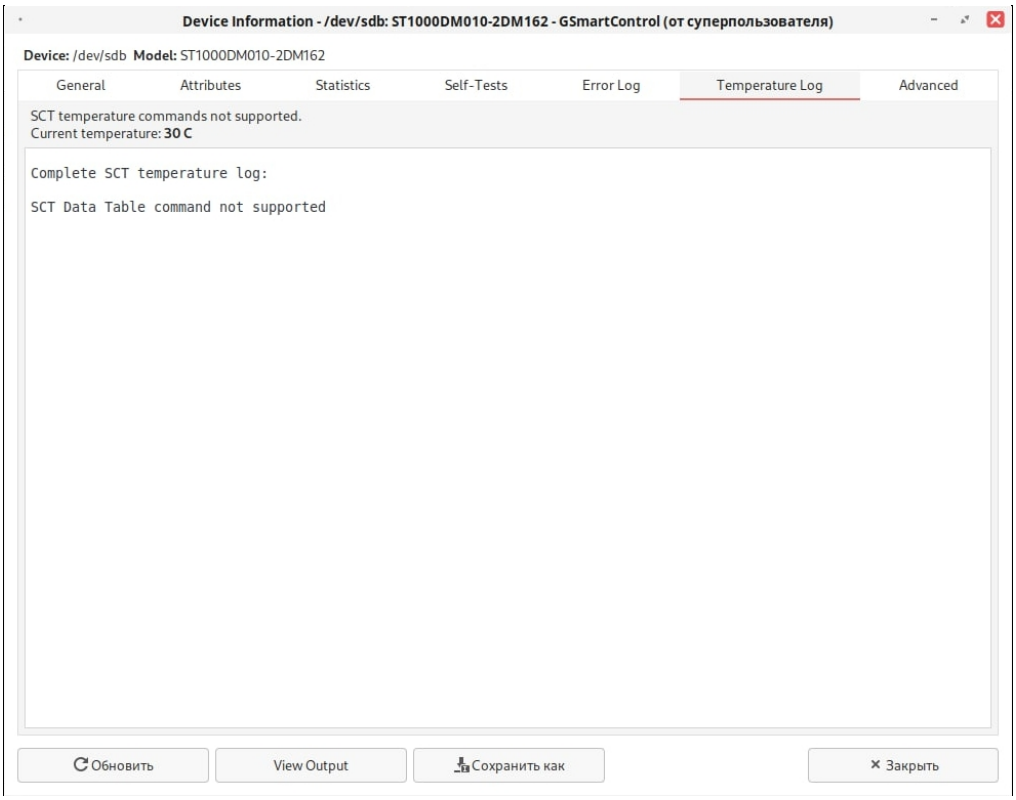
- **Быстрый тест** — продолжительностью 1 мин.
- **Расширенный тест** — продолжительностью более 1 часа, полный тест с процедурами проверки и пр.
- **Тест передачи** — продолжительностью 2 мин., тест подходит для обнаружения физических сбоев.



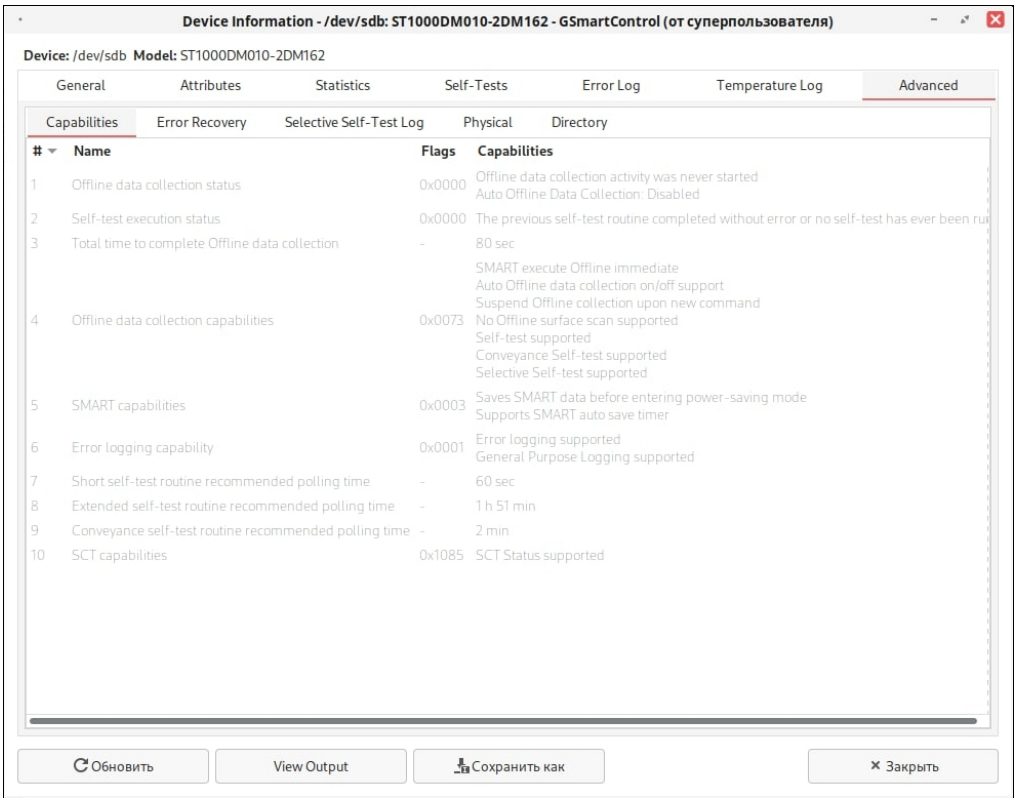
На вкладке «**Error Log**» ведется журнал ошибок с указанием деталей и подробным описанием при выборе любой из выявленных ошибок.



На вкладке «**Temperature Log**» ведется учет температурного режима используемого диска (если поддерживается).



На вкладке «**Advanced**» отображаются дополнительные параметры.



Все представленные утилитой результаты проверок можно сохранить в текстовом формате, например, для передачи информации о состоянии диска в сервисные центры или техническую поддержу.

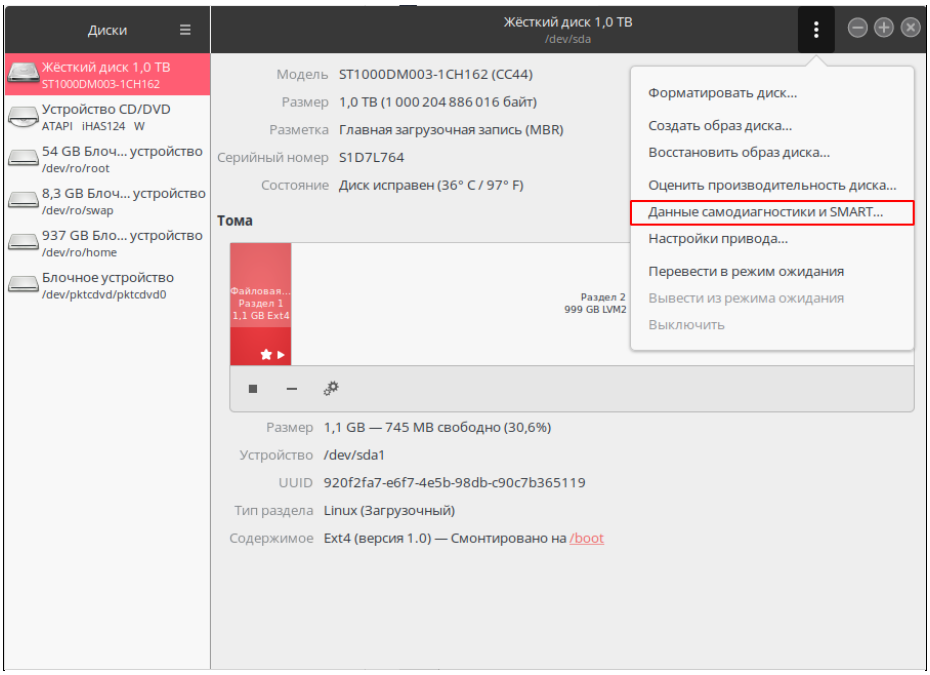
Gnome disk utility

Gnome disk utility — утилита с графической оболочкой для просмотра информации атрибутов SMART и тестирования диска. Для установки воспользуйтесь утилитой **yum** или **dnf** в зависимости от используемой версии РЕД ОС.

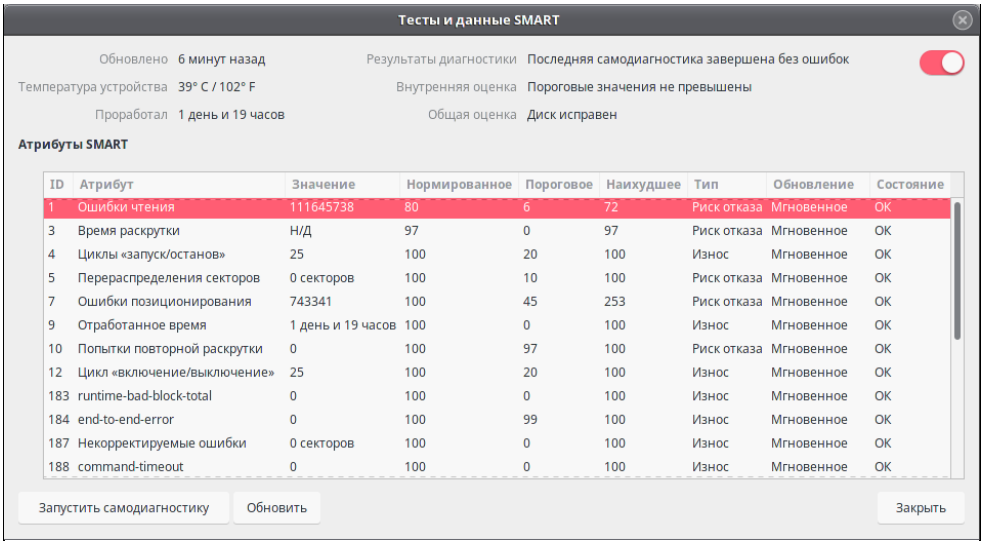
```
dnf install gnome-disk-utility
```

После установки утилита находится в **«Меню» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой Cinnamon и в **«Приложения» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой MATE.

После запуска приложения, выберите жесткий диск на панели справа, и нажмите на значок дополнительного меню, там выберите данные самодиагностики SMART.



В открывшемся окне вы можете просмотреть значения атрибутов SMART, температуры жесткого диска, результат последнего теста самодиагностики и запустить новый тест. Доступные тесты аналогичные таковым из утилиты **smartmontools**.



BadBlocks

Утилита **badblocks** используется для поиска сбойных блоков на устройстве (в разделе диска, например, */dev/sda1*).

Синтаксис утилиты:

```
badblocks [-<параметры>] <устройство> [<конечный_блок>] [<начальный_блок>]
```

Параметры [**<конечный_блок>**], [**<начальный_блок>**] являются необязательными и указывают диапазон проверяемых блоков. Если они не указаны, тогда (по умолчанию) проверке подлежат все блоки, начиная с самого первого блока и заканчивая самым последним блоком, которые используются на устройстве.

Основные параметры:

- **-b** - размер блока (в байтах);

- **-c** - порция блоков (по умолчанию 64 блока);
- **-f** - принудительный запуск теста с помощью чтения/записи;
- **-i** - входной файл (читает список уже существующих сбойных блоков);
- **-o** - исходящий файл (сохраняет список сбойных блоков в указанный файл);
- **-p** - число раз поиска (по умолчанию только одна проверка);
- **-n** - принудительное использование режима чтения-записи (только в размонтированной системе);
- **-s** - отображение хода процесса проверки;
- **-v** - подробные сообщения о проверке;
- **-w** - использование режима реальной записи (приводит к уничтожению информации на диске).

Пример использования утилиты

1. Выберите раздел жесткого диска для проверки. Для просмотра всех подключенных устройств и проверки расположения диска можно воспользоваться командой:

```
fdisk -l <имя_раздела>

  или

lsblk
```

2. Запустите проверки с помощью утилиты:

```
badblocks -v /dev/sda1Checking blocks 0 to 1048575
Checking for bad blocks (read-only test): done

Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Из вывода консоли видно, что проверка происходит только для чтения. При попытке использовать параметр **-n** (проверка чтения/записи) возникает следующее предупреждение:

```
/dev/ro_redos/root is mounted; it's not safe to run badblocks!
```

Поэтому для проверки дисков на чтение/запись рекомендуется использовать **live-сессию**.

```
badblocks -v /dev/sda1

Checking for bad blocks in non-destructive read-write mode
From block 0 to 1048575
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

```
badblocks -v /dev/ro_redos/root

Checking for bad blocks in non-destructive read-write mode
From block 0 to 17821695
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Восстановление загрузчика GRUB2

Восстановление загрузчика для систем, использующих BIOS
Восстановление загрузчика для систем, использующих UEFI

Вы можете подробнее ознакомиться с восстановлением загрузчика **grub2** и восстановлением для систем, просмотрев наши обучающие видео:

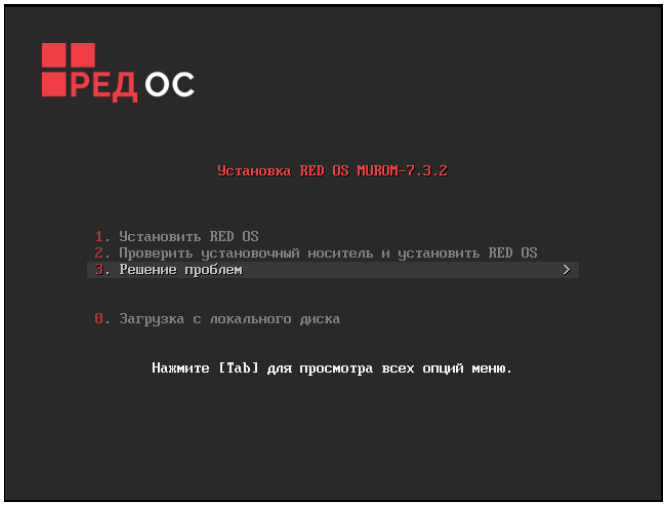
- на **RuTube** — Восстановление загрузчика GRUB2;
- в **Яндекс.Дзен** — Восстановление загрузчика GRUB2;
- в **VK Видео** — Восстановление загрузчика GRUB2.

На наших каналах вы также сможете найти много другой полезной информации.

Для восстановления необходимо загрузиться с установочного образа вашей версии РЕД ОС, поставив ваш носитель первым в списке предпочтения загрузки.

Восстановление загрузчика для систем, использующих BIOS

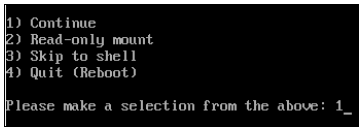
В появившемся меню следует выбрать пункт «**Решение проблем**».



Далее нужно выбрать пункт «**Исправить установленную RED OS**»:



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***:



Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Для определения диска, на котором установлена система, можно использовать следующую команду:

```
lsblk
```

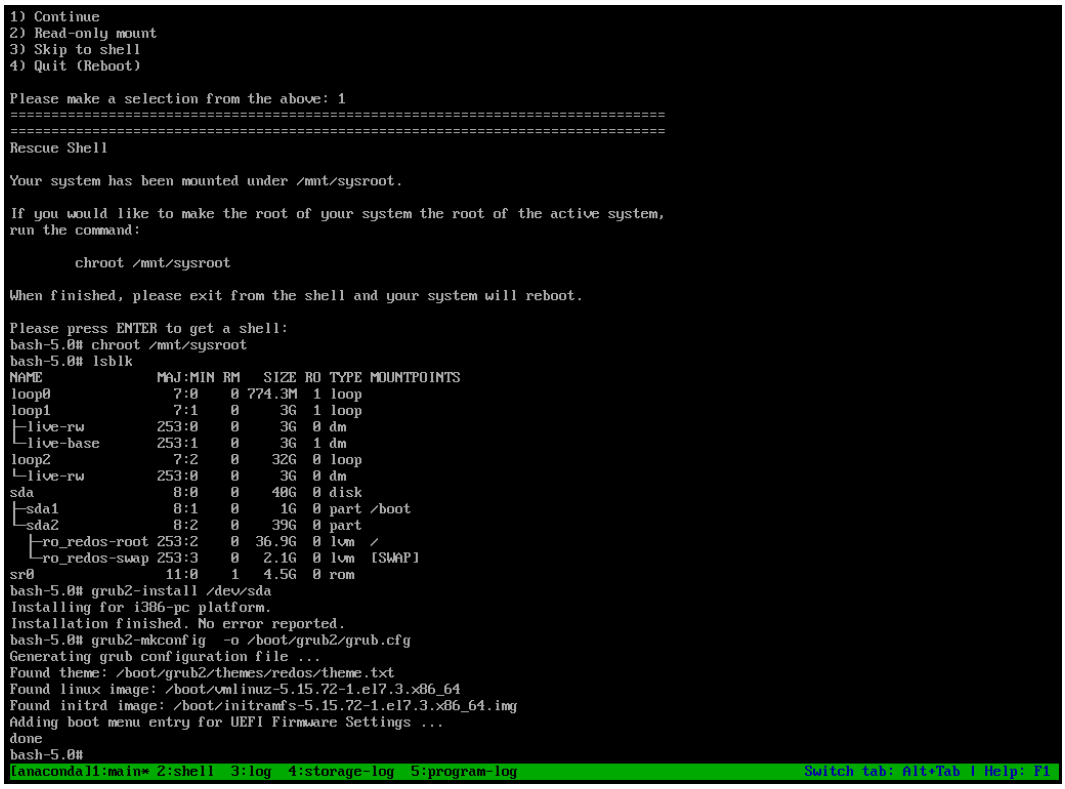
Далее выполните установку загрузчика командой (в конце указывается нужный диск):

```
grub2-install /dev/sda
```

Теперь создайте новый конфигурационный файл загрузчика с помощью команды:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Восстановление загрузчика для систем, использующих UEFI

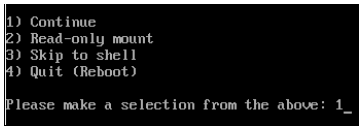
В появившемся меню следует выбрать пункт «**Troobleshooting**».



Далее нужно выбрать пункт «**Rescue a RED OS system**».



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***.



Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

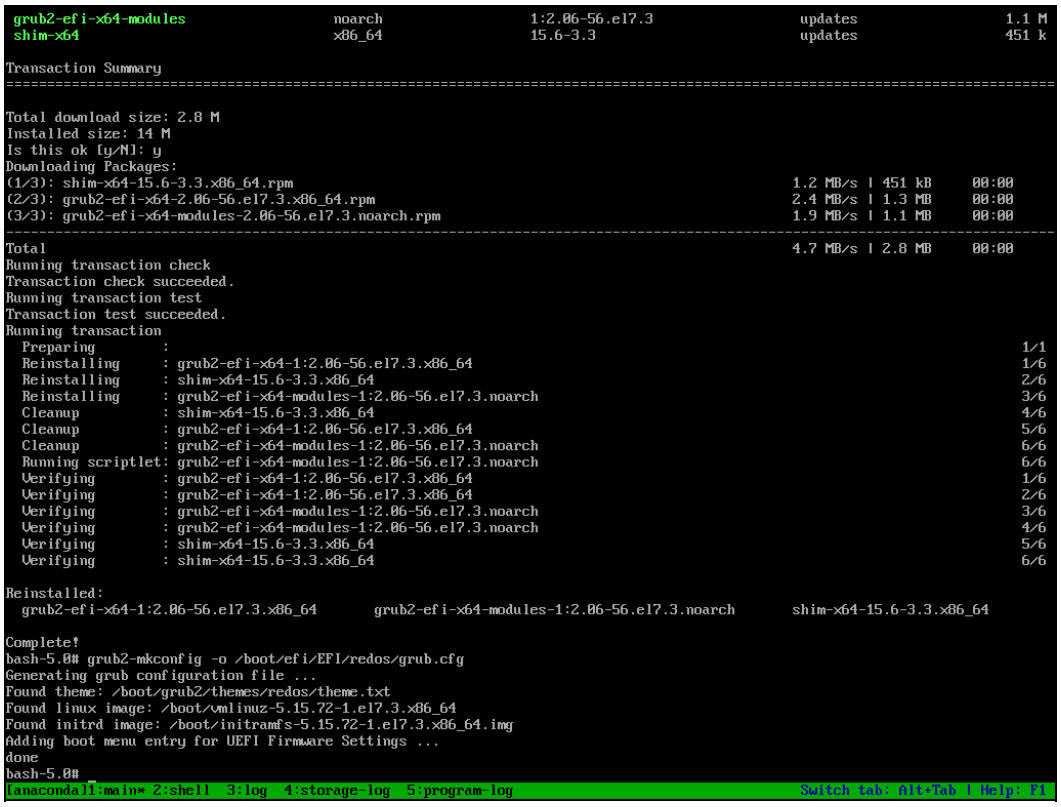
Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Затем потребуется обновить конфигурацию загрузчика с помощью команд:

```
dnf reinstall grub2-efi-x64  shim-x64 grub2-efi-x64-modules
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Проблемы с монтированием домашнего каталога /home

Суть данной проблемы заключается в том, что система вместо получения авторизации переходит в **emergency mode**, графический менеджер GDM не запускается.

```
Warning: dev/mapper/ro-root does not exist
Warning: dev/ro/root does not exist
Warning: dev/ro/swap does not exist

Generating “/run/initramfs/rdsosreport.txt“


Entering emergency mode. Exit the shell to continue.
Type “journalctl“ to view system logs.
You might want to save “/run/initramfs/rdsosreport.txt“ to a USB stick or /boot after mounting then and attach it to a bug report.
```

Проверим вывод команды `dmesg`. В выводе должны присутствовать ошибки вида «`/dev/sda3, run e2fsck manually`», где **/dev/sda3** - home-раздел. Для того чтобы узнать, за каким разделом закреплен **home**, необходимо проверить файл **/etc/fstab**. Проверка файловой системы осуществляется через утилиту **fsck**.

Запуск автоматической проверки `fsck -a /dev/sda3`, где ключ **-a** отвечает за автоматическую коррекцию ошибок файловой системы.

После успешной проверки необходимо перезагрузить компьютер. После этого графический менеджер GDM должен запуститься, и пользователь должен увидеть окно авторизации.

Пользователь забыл свой пароль и пароль root

Решением данной проблемы является сброс пароля **root**, согласно инструкции. Инструкцию предоставляет техническая поддержка, обратиться за инструкцией вы можете по ссылке.

Система не монтирует корневой раздел

Решение проблемы. Загрузка из более старого ядра
Неверное имя корневого раздела GRUB

Проблема монтирования корневого раздела выглядит следующим образом:

```
[ 1.719701] Hardware name: ECS IC780M-A2/IC780M-A2, BIOS 080015 11/03/2010
[ 1.719749] 0000000000000000 ffff88022c0b7df0 ffffffff8176cf38 ffffffff81a65048
[ 1.719951 0000000000008001 ffff88022c0b7e68 ffffffff81765306 ffffffff00000010
[ 1.720152] ffff88022c0b7e78 ffff88022c0b7e18 ffffffff81765e74 ffff88022c0b7e88
[ 1.720353] Call Trace:
[ 1.720402] [] dump_stack+0x64/0x82
[ 1.720449] [] panic+0xc8/0x206
[ 1.720494] [] ? printk+0x67/0x69
[ 1.720541] [] mount_block_root+0x225/0x2b0
[ 1.720587] [] mount_root+0x53/0x56
[ 1.720633] [] prepare_namespace+0x16c/0x1a4
[ 1.720679] [] kernel_init_freeable+0x1e1/0x1ee
[ 1.720725] [] ? initcall_blacklist+0xba/0xba
[ 1.720771] [] ? rest_init+0x80/0x80
[ 1.720817] [] kernel_init+0xe/0xf0
[ 1.720862] [] rest_from_fork+058/0x90
[ 1.720908] [] ? rest_init+0x80/0x80
[ 1.720974] Kernel Offset: 0x0 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 1.721043] ---[ end Kernel panic — not syncing: VFS: Unable to mount root fs on unknown-block (0,0)
_
```

Сообщение об ошибке «vfs unable to mount root fs on unknown block» может встречается во время загрузки Linux. Оно означает, что ядро не может примонтировать корневую файловую систему, и, следовательно, дальнейшая загрузка невозможна. Ошибка довольно серьёзная и, не исправив её, вы не сможете полноценно работать в своей операционной системе.

Все ситуации, в которых может появиться сообщение «error: vfs unable to mount root fs» можно разделить на два вида:

- Загрузка с жёсткого диска — вы загружаете свою основную операционную систему после внесения изменений в таблицу разделов, обновления или других действий, которые могли задеть диски;
- Вы загружаете LiveCD-систему с оптического диска или флешки.

Второй вариант сразу же отбросим. Здесь исправлять нечего. Ошибка означает, что либо образ был битый, либо он был неверно записан на диск. А вот первый случай интереснее, рассмотрим основные причины, которые могут его вызывать:

- Корневой раздел был переименован и теперь называется по-другому;
- Повреждена **initramfs**;
- Ядро не поддерживает файловую систему корневого раздела;
- Ошибка в конфигурации загрузчика, например, из-за недостаточного количества свободного места в папке **/boot**;
- Файловая система корневого раздела повреждена.

Рассмотрим возможные пути решения проблемы.

Решение проблемы. Загрузка из более старого ядра

После того, как система выдаст эту ошибку, случится **Kernel Panic** и компьютер перезагрузится. Вы снова окажетесь в меню загрузчика **GRUB**. Сначала следует попытаться загрузиться с помощью более старого ядра. Для этого выберите пункт «**Дополнительные параметры**» и выберите одно из более старых ядер.

Если система в этом случае загрузится, то можно сделать вывод, что не работает только новое ядро. Если вы собирали его сами, то, возможно, вы не включили в него все необходимые для работы файловые системы. Если это ядро из репозиториев, и система загрузилась с более старым ядром, то можно предположить, что у вас повреждена **initramfs** для нового ядра. Это тоже могло произойти из-за недостатка памяти при обновлении системы. Чтобы всё исправить, вам достаточно освободить место в каталоге **/boot/** и создать новую **initramfs**. Проверьте и освободите место в папке **/boot**, если его там мало:

```
df -h | grep boot
```

```
[root@localhost ~]# df -h | grep boot
/dev/sda2                974M          56M  851M            7% /boot
/dev/sda1                599M         6,4M  593M            2% /boot/efi
[root@localhost ~]#
```

На данном скриншоте занято только 7%, если будет 100% — надо освобождать. Для создания **initramfs** необходимо выполнить следующие действия:

```
cp -p /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak
dracut -f -v --regenerate-all
ls /boot
```

```
[root@localhost ~]# ls /boot
config-5.15.10-1.el7.x86_64
config-5.15.72-1.el7.3.x86_64
efi
grub
grub2
initramfs-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86.img
initramfs-5.10.29-3.el7.x86_64.img
initramfs-5.15.10-1.el7.x86_64.img
initramfs-5.15.72-1.el7.3.x86_64.img.bak
loader
lost+found
symvers-5.15.10-1.el7.x86_64.gz
symvers-5.15.72-1.el7.3.x86_64.gz
System.map-5.15.10-1.el7.x86_64
System.map-5.15.72-1.el7.3.x86_64
vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
vmlinuz-5.15.10-1.el7.x86_64
vmlinuz-5.15.72-1.el7.3.x86_64
```

Обновите конфигурацию загрузчика **grub**:

- если используется **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- если используется **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

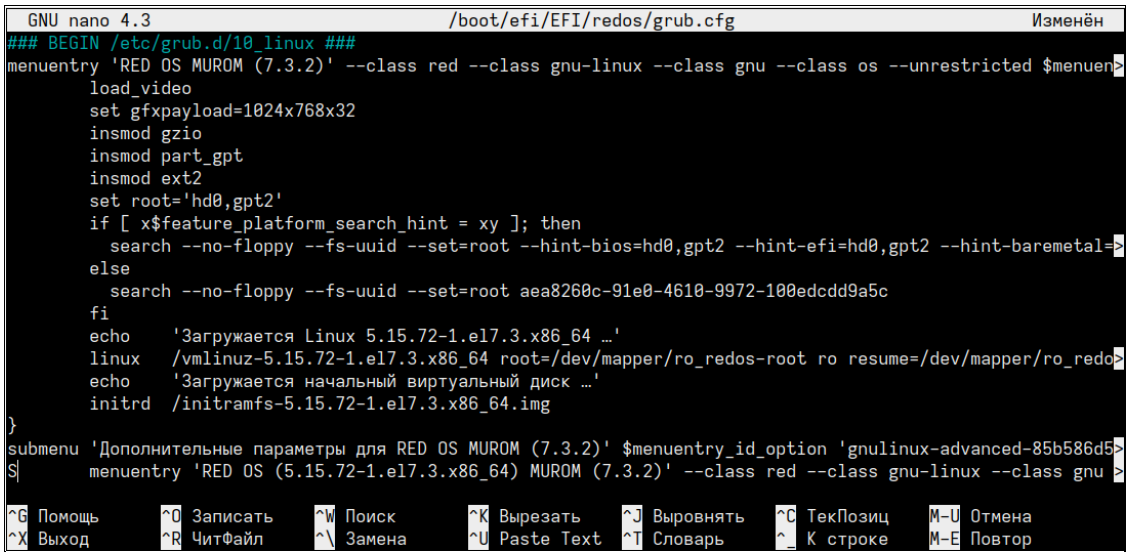
Если вы думаете, что проблема именно в свободном пространстве и **initramfs**, но загрузиться с помощью более старого ядра не можете, то попробуйте другой **LiveCD**-дистрибутив и попытайтесь всё исправить в *chroot*-окружении.

Неверное имя корневого раздела GRUB

Сейчас, в большинстве дистрибутивов, в конфигурационном файле **GRUB** имя корневого раздела передается ядру в формате **UUID**. И с этим обстоятельством есть одна проблема. Если вы каким-либо образом измените корневой раздел, например, измените его размер, то **UUID** изменится. И если вы выполните перезагрузку, не обновив конфигурацию **GRUB**, то система больше не загрузится, потому что ядро попросту не сможет найти нужного раздела.

Но попытаться решить проблему можно. Если вы точно знаете, на каком разделе у вас находится корень, то можно непосредственно в меню **GRUB** исправить конфигурацию. Для этого в меню выберете стрелками вверх и вниз нужный пункт, а затем нажмите кнопку **E**. Откроется редактор конфигурации. Вам нужно найти строчку, похожую на следующую:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro quiet splash
```



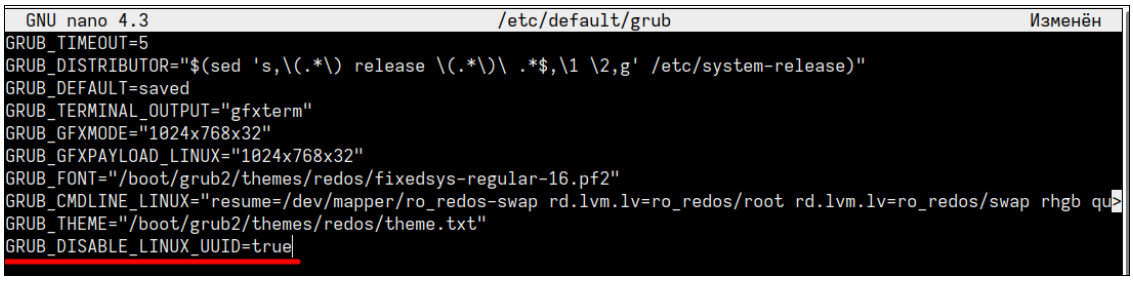
В ней надо заменить UUID=9d8d92de-74a6-4e64-8281-b8548c690e0c на обычное имя вашего корневого раздела, например, **/dev/sda2**. Для начала загрузки нажмите **F10**. Если система загрузится, значит проблема была именно в этом. В дальнейшем, можно просто обновить конфигурацию **GRUB**:

```
grub2-mkconfig
```

Или даже попросить **GRUB** больше не использовать **UUID** для обозначения корневого раздела:

```
nano /etc/default/grub
```

```
GRUB_DISABLE_LINUX_UUID=true
```



Далее необходимо снова обновить конфигурацию **GRUB**, используя команду **grub2-mkconfig**.

Если ошибка исчезла, но система всё ещё не загружается, обратите внимание, что **systemd** всё ещё использует файл **/etc/fstab** для монтирования файловых систем. И если корневая файловая система (и не корневая тоже) там указана неверно, система не загрузится. Для исправления этой проблемы можно использовать режим восстановления. Здесь тоже надо заменить **UUID** на обычную запись или же на правильный **UUID**. Такая проблема очень часто становится причиной медленной загрузки Linux.

В этом же режиме можно проверить корневой раздел на ошибки, но для проверки диска лучше использовать **LiveCD**.

Если файловая система корневого раздела повреждена, её необходимо проверить, исправить согласно инструкции «Проверка файловой системы на наличие ошибок».

ОС запускается, но зависает на экране загрузки

Скорее всего данное поведение может быть связано с некорректным поведением X-сервера и графических драйверов. Для диагностики ситуации и сбора информации с ПК вы можете запустить ПК в консольном режиме. Для этого вам потребуется перезагрузить ПК и на этапе выбора ядра для загрузки нажать «**e**».

Далее необходимо найти примерно такую строку (см. скриншот) и добавить в конец «**3**».



После этого для продолжения загрузки необходимо нажать сочетание клавиш «**Ctrl+X**», ОС будет запущена в текстовом режиме.

Следующим этапом потребуется собрать отладочную информацию через утилиту loginfo для дальнейшего изучения проблемы.

Не загружается РЕД ОС из-за неправильного UUID раздела SWAP

Диагностика проблемы
Устранение проблемы

Проблема характеризуется тем, что во время загрузки операционной системы РЕД ОС на экране появляется ошибка вида:

```
A start job is running for /dev/disk/by-uuid/03a83c83-3827-4fa3-8352-bdfb4d99a15b (10min 6s / no limit)
```

Загрузить операционную систему в безопасном режиме также не удается.

Диагностика проблемы

Ошибка «A start job is running for /dev/disk/by-uuid/...» связанна с разделом диска, который используется в системе. Операционная система не может подключить раздел, который имеет номер **UUID**, указанный в ошибке.

Для того чтобы узнать, с каким именно разделом имеются проблемы при загрузке, требуется проверить параметры загрузчика системы **grub**.

Чтобы увидеть параметры загрузки grub, нужно на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> quiet splash
```

В строке видно, что в параметре resume=UUID= записан тот номер **UUID**, из-за которого возникает проблема с запуском системы.



Параметр resume отвечает за указание файла подкачки (раздел **SWAP**) для возобновления работы системы после перехода в спящий режим. Из этого можно сделать вывод, что проблема связана с разделом **SWAP**.

Необходимо узнать, совпадает ли номер **UUID** раздела **SWAP**, который указан в параметрах grub, с его актуальным на данный момент **UUID**-номером.

Номер **UUID** всех разделов диска можно узнать с помощью команды:

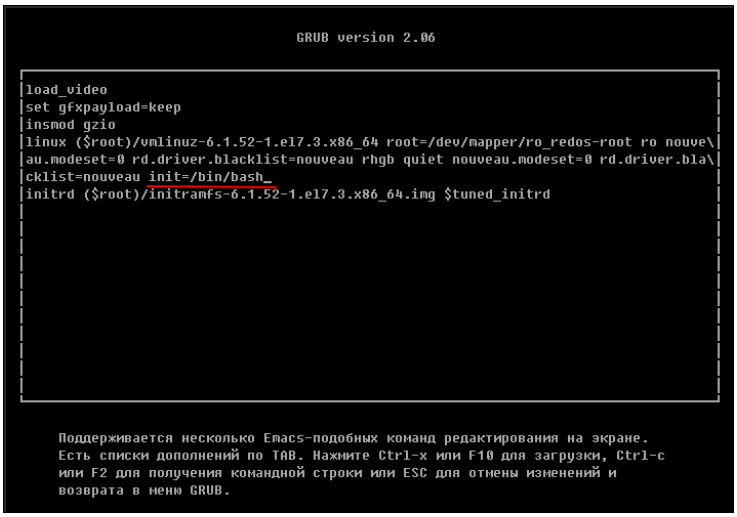
```
lsblk -o +uuid,name
```

Но т. к. операционная система РЕД ОС не может быть загружена ни в обычном, ни в безопасном режиме, то нужно выполнить загрузку системы сразу в командный интерпретатор **/bin/bash**.

Для этого необходимо открыть параметры загрузки **grub** — на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=номер_uuid ro resume=UUID=<номер_uuid> quiet splash
```

В строке необходимо удалить полностью параметр resume=UUID=<номер_uuid> и добавить параметр init=/bin/bash:



Для продолжения загрузки с введенными параметрами необходимо нажать сочетание клавиш **Ctrl+x** или **F10**.

Система сразу загрузится в командную оболочку **bash**.

Авторизуйтесь с правами пользователя **root** командой:

```
su root
```

Далее выполните монтирование корневого раздела командой:

```
mount -o remount,rw /
```

Нужно узнать **UUID**-номер, который имеет раздел **SWAP** в данный момент. Для этого необходимо выполнить команду:

```
lsblk -o +uuid,name
```

Вывод команды должен быть примерно следующим:

```
nvme0n1
│   259:0    0 476,9G  0 disk                                  nvme0n1
├─nvme0n1p1
│   259:1    0   600M  0 part /boot/efi   050C-89A6                    nvme0n1p1
├─nvme0n1p2
│   259:2    0     1G  0 part /boot      bef54c6a-a584-4147-9178-4218be5daedc   nvme0n1p2
└─nvme0n1p3
    259:3    0 475,4G  0 part          IA0CXd-ZuHw-7mqu-uhkH-igMU-c7wt-QBESxa nvme0n1p3
  ├─ro_redos-root
  │ 253:0    0    70G  0 lvm  /        832a877b-0293-4eec-a5f0-6a8d080aac03   ro_redos-srv-root
  ├─ro_redos-swap
  │ 253:1    0   7,5G  0 lvm  [SWAP]     fc46bf73-2759-4d70-a2d3-ab1f664ebf12   ro_redos-srv-swap
  └─ro_redos-home
    253:2    0 397,8G  0 lvm  /home      e5411e74-97de-4b84-aecd-e7f86e16ad5e   ro_redos-home
```

В данном примере раздел **SWAP** имеет **UUID - fc46bf73-2759-4d70-a2d3-ab1f664ebf12**.

Таким образом, можно сделать вывод, что номер **UUID** раздела **SWAP**, который записан в параметрах загрузки grub, и его актуальный **UUID** номер отличаются.

Устранение проблемы

Для устранения проблемы необходимо заменить неактуальный **UUID**-номер в параметрах загрузки **grub** на его актуальный номер, который был получен в результате диагностики.

Изменение параметра resume загрузчика GRUB

1. На этапе выбора ядра нажмите клавишу «**e**». Будут открыты параметры загрузки **grub**.

2. Замените старый номер **UUID**, прописанный в параметре `resume=UUID=`, на актуальный, который был получен в результате

диагностики командой `lsblk -o +uuid,name`.

В строке:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> quiet splash
```

3. Для продолжения загрузки с введенными параметрами нажмите сочетание клавиш **Ctrl+x** или **F10**.

Система должна загрузиться без ошибок.

Сохранение конфигурации загрузчика GRUB

При таком способе редактирования параметров загрузки **grub** введенные параметры не будут сохранены при следующей загрузке. Для сохранения внесенных изменений на постоянной основе измените параметр `resume=UUID=` в файле **/etc/default/grub**.

Для запуска терминала необходимо использовать сочетание клавиш **Ctrl+Alt+T** или запустить утилиту из **Главного меню** – **Системные** – **Терминал**.

Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

Откройте файл **/etc/default/gru**b с помощью текстового редактора командой:

```
nano /etc/default/grub
```

Найдите строку следующего вида:

```
GRUB_CMDLINE_LINUX="resume=UUID=..."
```

Номер **UUID** параметра `resume=UUID=` должен быть заменен на актуальный, с помощью которого удалось запустить систему.

Далее обновите файл загрузчика **grub** командой:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

После выполнения этих действий параметры загрузи **grub** будут сохранены для постоянного использования.

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

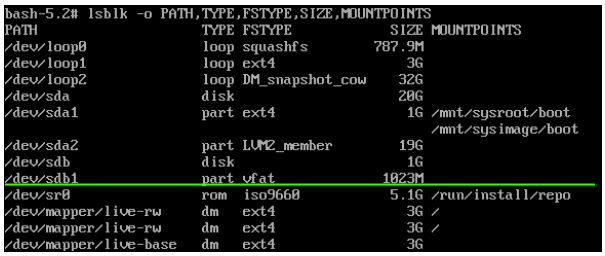
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

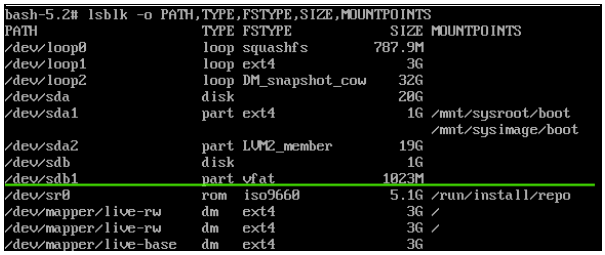
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

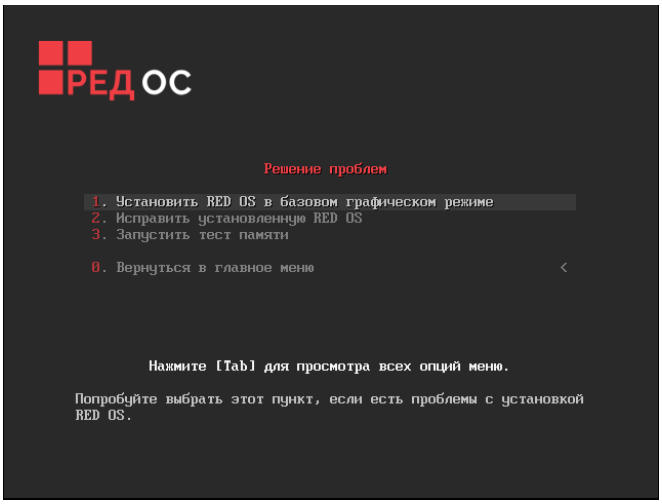
Проблемы при установке ОС

Установка ОС зависает на начальном этапе
ОС не запускается после установки с LiveUSB

Установка ОС зависает на начальном этапе

Бывают случаи, когда установка ОС зависает на этапе первичной загрузки до запуска окна *Anaconda*. В таких случаях рекомендуется произвести установку ОС в **базовом графическом режиме**, который также называется **nomodeset**.

Для загрузки ОС в режиме **nomodeset**, использующих **BIOS**, выберите пункт «**Решение проблем**» – «**Установить RED OS в базовом графическом режиме**».



Для загрузки ОС в режиме **nomodeset**, использующих **UEFI**, выберите пункт «**Troubleshooting**» – «**Install RED OS Murom-7.3.4 in basic graphics mode**».



ОС не запускается после установки с LiveUSB

Иногда бывают случаи, что после установки ОС с *LiveUSB* не происходит загрузка установленной ОС. Для таких случаев необходимо загрузиться обратно в Live-сессию и скопировать файл **initramfs** с установочного носителя на диск с ОС. Для этого выполните следующий алгоритм действий:

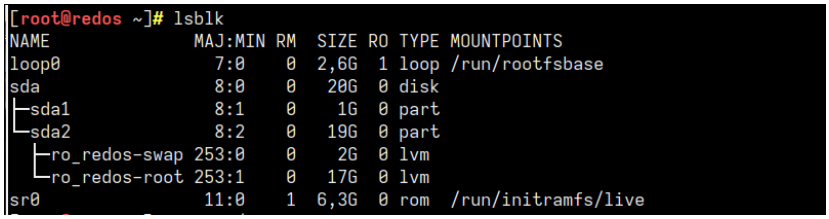
1. Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

2. Проверьте названия разделов установленной ОС командой:

```
lsblk
```

В ответе команды будут указаны разделы ОС и загрузчика, в данном случае — **/dev/ro_redos/root** и **/dev/sda1**.



3. Примонтируйте разделы установленной ОС следующими командами:

```
mkdir /OS
mount /dev/ro_redos/root /OS
mount /dev/sda1 /OS/boot
cp /run/initramfs/live/images/pxeboot/initrd.img /OS/boot/initramfs-5.15.72-1.el7.3.x86_64.img
```

4. Назначьте необходимые права:

```
chmod 600 /OS/boot/initramfs-5.15.72-1.el7.3.x86_64.img
chown root. /OS/boot/initramfs-5.15.72-1.el7.3.x86_64.img
```

5. Отмонтируйте разделы установленной ОС:

```
umount /OS/boot
umount /OS
```

6. Перезагрузите ПК в установленную ОС:

```
reboot
```

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

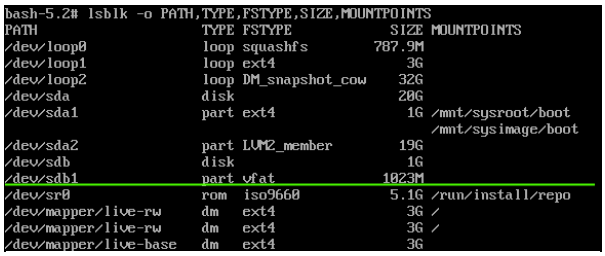
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

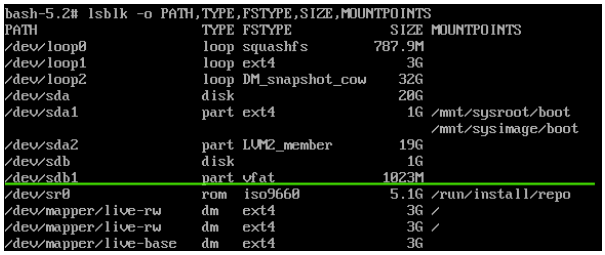
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

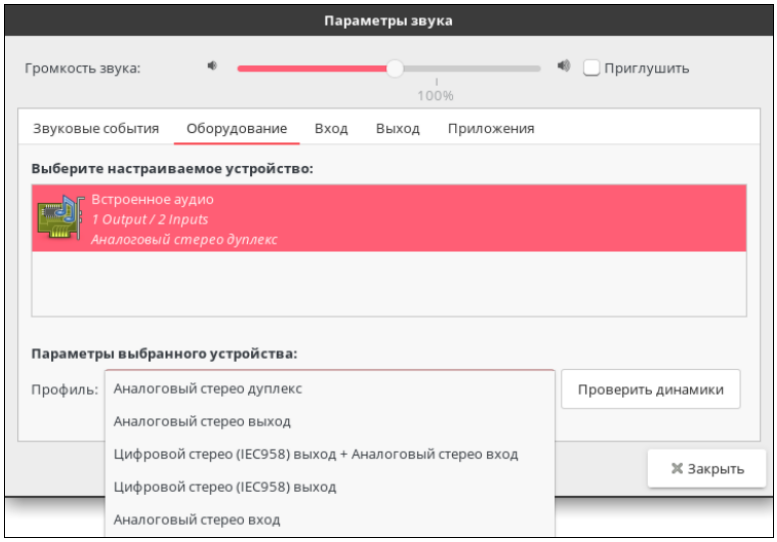
Решение проблем со звуком

Выбор оборудования
Отсутствует оборудование в списке доступных
Выбор оборудования через alsamixer
Проверка поддержки устройства ядром
Отсутствует звук у доменного пользователя

При возникновении проблем, связанных со звуком, существует несколько вариантов их решения.

Выбор оборудования

Бывают ситуации, когда необходимо вручную выбрать, какое именно устройство должно использоваться в ОС для ввода и вывода аудио-информации. Для этого выберите устройство в списке оборудования и установите для него необходимые параметры.

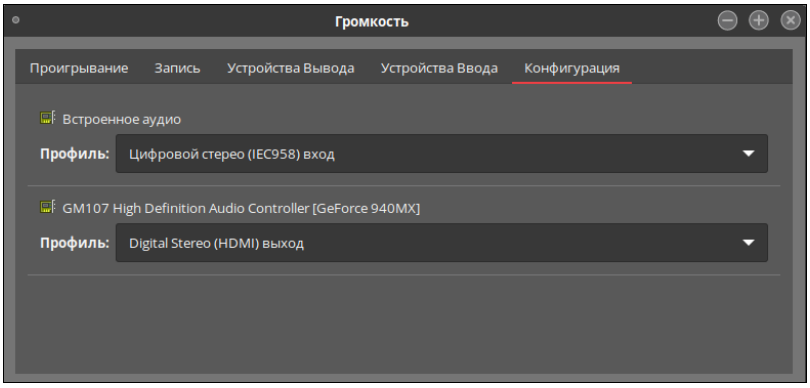


Отсутствует оборудование в списке доступных

Для решения данной проблемы на некоторых моделях ПК может подойти установка дополнительного пакета (потребуются права администратора):

```
dnf install alsa-sof-force
```

После установки необходимо перезагрузить ПК и проверить наличие аудиовыходов в параметрах звука.



Также не стоит забывать о системных обновлениях, соответственно, необходимо проверить работу оборудования на актуальных пакетах ОС. Для этого выполните следующие команды (потребуются права администратора):

```
dnf makecache
dnf update
dracut -f -v --regenerate-all
```

Затем для корректной загрузки необходимо обновить конфигурацию **GRUB**:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

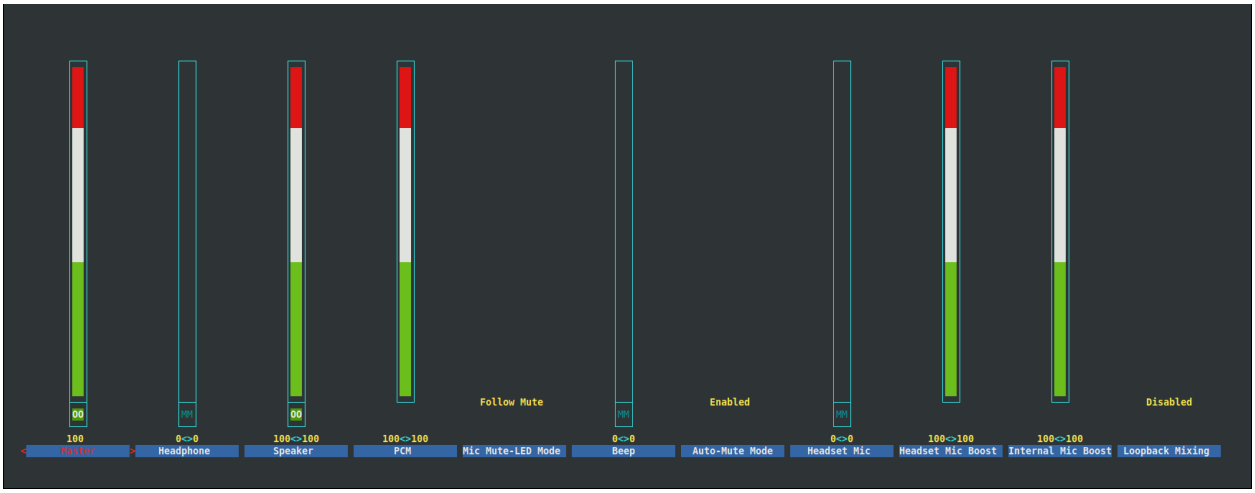
```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Для применения настроек потребуется перезагрузить ПК:

```
reboot
```

Выбор оборудования через alsamixer

В решении проблем со звуком также может помочь вариант с выбором звуковой карты из консоли через утилиту **alsamixer**.



С помощью клавиши **F6** можно выбрать необходимую звуковую карту.

Проверка поддержки устройства ядром

С выходом нового оборудования при возникновении проблем стоит обратить внимание на поддержку такого оборудования ядром. Проверить поддержку можно по нашей инструкции «Поддержка звука».

Отсутствует звук у доменного пользователя

Если звук отсутствует у доменного пользователя, в первую очередь необходимо проверить наличие файла **/var/lib/AccountsService/users/<доменный_пользователь>**. Если файл отсутствует, его необходимо создать по примеру файла локального пользователя.

Также попробуйте добавить пользователя в группу *audio*:

```
usermod -aG audio <доменный_пользователь>@<домен>
```

Если предложенные рекомендации не помогли с решением проблемы, необходимо собрать диагностическую информацию с помощью утилиты loginfo для дальнейшего ее изучения.

Realtek RTL8821CE

Для решения возможной проблемы с wi-fi адаптерами на базе микроконтроллера **Realtek RTL8821CE**, убедитесь в том, что у вас именно такой адаптер. Для этого выполните команду:

```
lspci | grep Network02:00.0 Network controller: Realtek Semiconductor Co., Ltd. RTL8821CE 802.11ac PCIe Wireless Network Adapter
```

Есть вероятность, что система использует драйверы **rtw88_***. Проверка производится командой:

```
lsmod | grep rtw
```

Если вывод команды показал, что используются именно эти драйверы, то нужно внести их в черный список (подробнее см. по ссылке) модулей ядра. Для этого необходимо создать конфигурационный файл:

```
nano /etc/modprobe.d/wifi.conf
```

и запретить загрузку «ненужных» модулей ядра (драйверов):

```
blacklist rtw88_8821ce /bin/true
blacklist rtw88_8821c /bin/true
blacklist rtw88_pci /bin/true
blacklist rtw88_core /bin/true
modprobe rtl8821ce
```

Обратите внимание на последнюю строку, в ней предопределяется модуль для загрузки, входящий в пакет, который еще не установлен. Установите пакет с работоспособным модулем (драйвером):

- для РЕД ОС версии 7.3 и старше выполните команду:

```
dnf install rtl8821ce_$(uname -r)
```

После этого нужно произвести перезагрузку системы командой:

```
reboot
```

После выполнения вышеуказанных действий проблема с wi-fi адаптерами на базе микроконтроллера **Realtek RTL8821CE** должна исчезнуть.

Intel i915

Ошибка в журнале сообщений ядра
Мерцание экрана
Отключение аппаратного ускорения
Включение поддержки графики
Зависания компьютера

Для решения возможной проблемы, связанной со встроенной графикой **Intel** последних поколений, требуется указать ядру дополнительные параметры, чтобы драйвер **i915** был применен принудительно к определенным версиям графического контроллера.

Ниже представлены примеры принудительного применения параметров для ядра. Применить параметры можно на этапе загрузки ОС для разового использования, т.е. на этапе выбора ядра необходимо нажать клавишу «**e**» и в строку примерно следующего вида:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro quiet splash
```

и вписать параметры в **GRUB**:

- для **UHD Graphics 730**:

```
i915.force_probe=4692 i915.modeset=1
```

- для **UHD Graphics 750**:

```
i915.force_probe=4c8b i915.modeset=1
```

- для **UHD Graphics 770**:

```
i915.force_probe=4680 i915.modeset=1
```

В итоге должна получиться примерно следующая строка загрузки:



Стоит обратить внимание, что некоторые ID железа могут отличаться и уточнить их следует, как показано в инструкции «Поддержка железа».

Если указанные параметры помогли в решении проблемы, их можно добавить в ядро для постоянного использования. Для этого необходимо прописать параметры в файл **/etc/default/grub** в строку, начинающуюся со слов:

```
GRUB_CMDLINE_LINUX=
```

В конец строки дописываются **ваши** параметры.

Далее обновите файлы загрузчика:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Примеры использования

При возникновении таких проблем, как:

- мерцание экрана монитора,
- произвольные выключения монитора на небольшие промежутки времени,
- произвольные выключения монитора на большие промежутки времени (при этом во всех случаях система продолжает работать, экран монитора через какое-то время восстанавливается в работе),

необходимо в конфигурационный файл **grub** внести соответствующие изменения. Далее будут рассмотрены основные возникающие проблемы и способы их решения.

Ошибка в журнале сообщений ядра

При отображении в выводе журнала сообщений ядра ОС ошибки примерно следующего вида:

```
dmesg | grep i915

i915 0000:00:02.0: [drm] *ERROR* CPU pipe A FIFO underrun
```

необходимо открыть конфигурационный файл **grub**:

```
nano /etc/default/grub
```

и добавить в строку **GRUB_CMDLINE_LINUX** следующие значения:

```
...
 GRUB_CMDLINE_LINUX="resume=/dev/mapper/ro_redos-swap rd.lvm.lv=ro_redos/root rd.lvm.lv=ro_redos/swap rhgb quiet
i915.enable_psr=0 intel_idle.max_cstate=2"
 ...
```

Мерцание экрана

Для исправления проблем с мерцанием экрана в файл **/etc/default/grub** в строку, начинающуюся со слов:

```
GRUB_CMDLINE_LINUX="..."
```

в конце допишите:

```
i915.enable_psr=0 intel_idle.max_cstate=4 i915.enable_dc=0 i915.enable_fbc=0
```

Далее выставите иной режим энергосбережения:

```
tuned-adm profile latency-performance
```

Обновите файлы загрузчика:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Перезагрузите систему и проверьте работу.

Отключение аппаратного ускорения

Для отключения аппаратного ускорения используются следующие параметры (в зависимости от производителя):

Вендор	Параметр
Intel	`i915.modeset=0` или `nomodeset`
AMD	`radeon.modeset=0` или `amdgpu.dc=0` (для новых ядер)
Nvidia	`nomodeset` (или `nouveau.modeset=0`)

Пример отключения аппаратного ускорения для **Intel**:

```
grubby --update-kernel ALL --args="nomodeset"
```

Для удаления параметра выполните:

```
grubby --update-kernel ALL --remove-args nomodeset
```

Дополнительные опции:

- `text` — загрузка в текстовом режиме;
- `xforcevesa` — загрузка видеодрайвера **vesa**.

Также настройку можно выполнить через редактирование файла **/etc/default/grub**, добавив соответствующий параметр в конец строки **GRUB_CMDLINE_LINUX=**, после этого потребуется обновить конфигурацию **grub**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Включение поддержки графики

Через ID

Для загрузки графики и возможности выбора любого поддерживаемого разрешения используется опция загрузчика — `i915.force_probe=<ID_видеокарты>`.

Например:

```
i915.force_probe=9a49
 i915.force_probe=4c8a
 i915.force_probe=4e71
 i915.force_probe=9a78
```

Стоит обратить внимание, что некоторые ID железа могут отличаться и уточнить их следует, как показано в инструкции «Поддержка железа».

Также для включения поддержки графики можно использовать конфигурационный файл **/etc/modprobe.d/i915.conf**.

Параметры прописываются следующим образом:

```
options i915 force_probe=4c8a
```

С помощью активации альфа-драйвера

Запустите ОС, перейдите в консольный режим с помощью сочетания клавиш *Ctrl+Alt+F2*.

Выполните команду:

```
grubby --update-kernel ALL --args i915.alpha_support=1
```

Включение через опцию modeset

Поддержку графики также можно активировать с помощью опции **modeset**. Для этого выполните команду:

```
grubby --update-kernel ALL --args modeset=1
```

Зависания компьютера

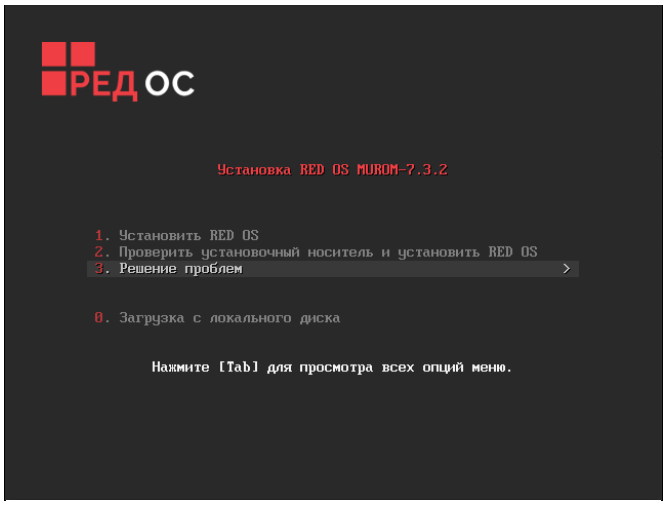
Если происходят периодические зависания компьютера без видимых причин, можно попробовать добавить параметр ядру `intel_idle.max_cstate=1` командой:

```
grubby --update-kernel ALL --args intel_idle.max_cstate=1
```

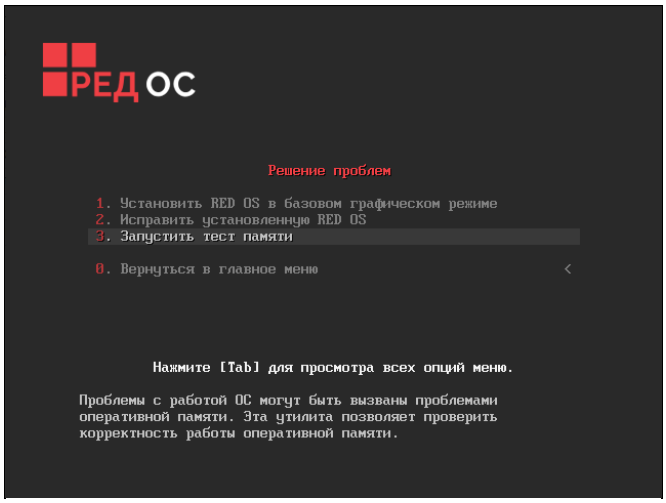
Тестирование оперативной памяти

Чтобы протестировать оперативную память на ошибки нужно запустить ОС с загрузочной флешки или диска.

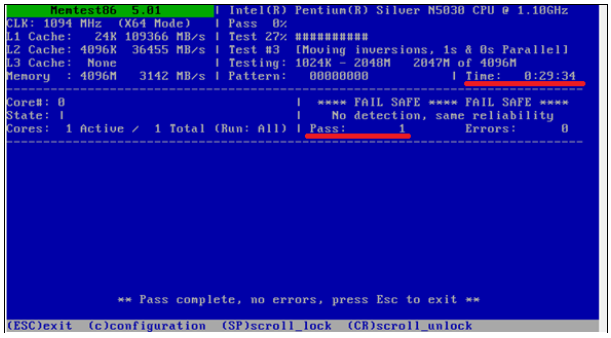
В открывшемся меню необходимо выбрать третий пункт «**Решение проблем**».



Затем выбрать третий пункт «**Запустить тест памяти**».



Запустится тест памяти.



Данный процесс будет выполняться бесконечно, пока вы не остановите его. Вам нужно дождаться окончания хотя бы одного цикла проверки (значение **Pass** должно быть **>= 1**). В случае обнаружения ошибки она отобразится в списке.

Поддержка оборудования в ядре ОС

Поддержка железа
Поддержка звука
Поддержка сети

Некоторые модели поддерживаемого оборудования указаны в разделе «Оборудование, совместимое с РЕД ОС».

Вопрос поддержки оборудования ядром и драйверами актуален всегда. Для того чтобы понять, как именно осуществляется проверка поддержки, рассмотрим основные инструменты и ссылки.

Для получения краткой сводки о комплектующих вашего ПК выполните команду:

```
loginfo.sh --hw-id
```

Предварительно **loginfo** должен быть обновлен до актуальной версии:

```
dnf update loginfo
```

Поддержка железа

Одним из популярных сайтов, в котором собраны ID устройств, является https://linux-hardware.org.

Однако, чтобы определить, какие **Vendor ID** (**VID**) и **Device ID** (**DID**) требуется вводить для понимания поддержки, воспользуйтесь утилитой **inxi**.

```
inxi -F -v 8
```

пример ID для **USB Bluetooth** / **USB Wi-Fi,** которые потребуются для эксперимента:

```
...

Device-2: 1-4:2 info: Realtek Bluetooth Radio type: Bluetooth driver: rtk_btusb interfaces: 2 rev: 1.1
speed: 12 Mb/s chip ID: 0bda:8771 serial: 00E04C239987
Device-3: 1-6:3 info: Realtek RTL8188EUS 802.11n Wireless Network Adapter type: Network driver: 8188eu
interfaces: 1 rev: 2.0 speed: 480 Mb/s chip ID: 0bda:8179 serial: 00E04C0001

...
```

В выводе отображаются 2 интересующих нас ID:

- Bluetooth - **0bda:8771**;
- Wi-Fi - **0bda:8179**.

Также рассмотрим альтернативу *linux-hardware.org* — **https://cateee.net**

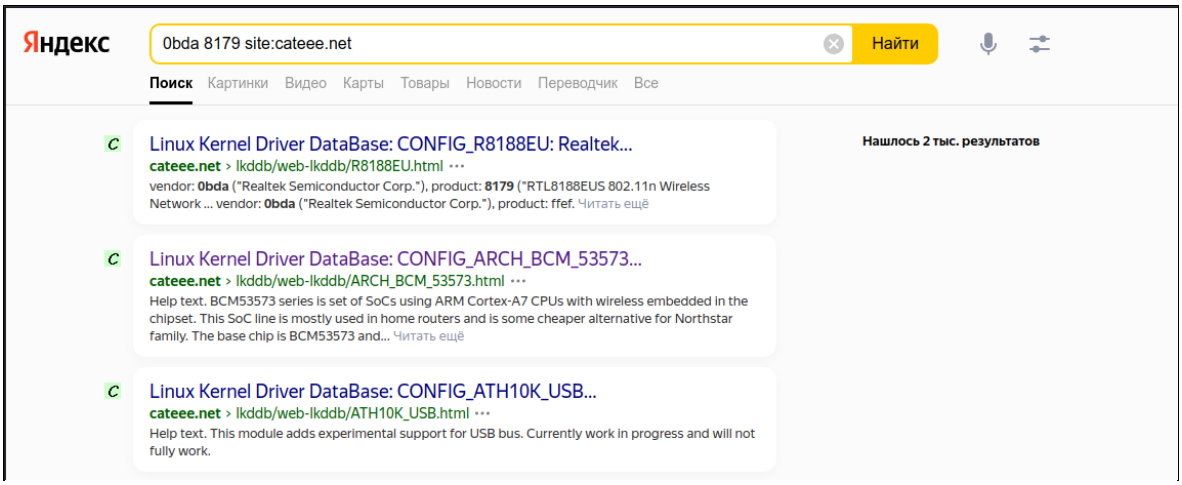
Данный сайт осуществляет поиск аналогично по ID. Для этого в поисковой строке требуется задать запрос вида:

<VID> <DID> site:cateee.net

или по одному из нужных ID.

Попробуем найти **0bda 8179** (**Wi-Fi**).

Имеется ряд результатов, в которых описывается, какой именно драйвер требует устройство:



Стоит упомянуть еще пару полезных ссылок для определения поддержки железа ядром:

- https://wireless.wiki.kernel.org/en/users/drivers
- https://h-node.org/hardware/catalogue/en

Также обращаем внимание на пункт **Driver** в выводе **inxi** - если он имеет значение отличное от **n/a**, значит у вас имеется поддержка устройства драйвером. Что это означает? Это значит, что вы можете найти данное устройство в заявленных драйвером через **modinfo**.

Bluetooth:

```
modinfo rtk_btusb | grep -i 0BDA

alias: usb:v0BDAp*d*dc*dsc*dp*icE0isc01ip01in*
```

В выводе показано, что есть метка **alias (алиас)**, являющаяся маской, по которой драйвер применяется к тому или иному устройству.

Аналогичную картину можно наблюдать для **Wi-Fi** адаптера:

```
modinfo 8188eu | grep -i 0BDA

alias: usb:v0BDAp8179d*dc*dsc*dp*ic*isc*ip*in*
```

Теперь рассмотрим проверку ядра на наличие интересующего драйвера.

Сначала проверим, установлен ли уже драйвер:

```
find /lib/modules/$(uname -r) -name *.ko | grep -i 8188eu

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/net/wireless/8188eu.ko
/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/staging/r8188eu/r8188eu.ko

find /lib/modules/$(uname -r) -name *.ko | grep -i rtk_btusb

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/bluetooth/rtk_btusb.ko
```

Как видно из вывода консоли, для ядра **5.15.10-3** данные драйвера имеются.

Существует также способ просмотра параметров ядра, с которыми оно было собрано. Для проверки того, какие были выбраны опции для драйвера, выполните команду:

```
cat /boot/config-$(uname -r) | grep -i 8188

CONFIG_RTL8188EE=m
CONFIG_R8188EU=m
```

А вот для bluetooth-драйвера вывод может выглядеть сомнительно:

```
cat /boot/config-$(uname -r) | grep -i BTUSB
```

```
CONFIG_BT_HCIBTUSB=m
CONFIG_BT_HCIBTUSB_AUTOSUSPEND=y
CONFIG_BT_HCIBTUSB_BCM=y
# CONFIG_BT_HCIBTUSB_MTK is not se t
CONFIG_BT_HCIBTUSB_RTL=y
```

Для того чтобы развеять сомнения, имеется ли драйвер - проверим его наличие следующим образом:

```
dnf provides *rtk_btusb.ko
```

Из полученного списка необходимо выбрать драйвер под свое ядро:

```
rtl8761b_5.15.10-3.el7.x86_64-1.0-8.el7.3.x86_64 : Kernel module for RTL8761B
Репозиторий        : kernels
Совпадения с:
Другое       : *rtk_btusb.ko
```

В случае, если драйвер отсутствует и в ядре, и в репозитории, существует вариант поиска необходимого драйвера на **github**.

Для этого необходимо в поиске по репозиториям **github** знать название нужного драйвера и попробовать найти интересующий. Так, к примеру, драйвер **8188eu** имеет множество разветвлений, которые охватывают широкий спектр устройств - примеры двух популярных вариаций драйвера:

- https://github.com/drygdryg/rtl8188eus;
- https://github.com/lwfinger/rtl8188eu.

Поддержка звука

Для проверки поддержки звука необходимо выполнить команду:

```
inxi -a -A

Audio:
 Device-1: NVIDIA vendor: ASUSTeK driver: snd_hda_intel v: kernel
 bus ID: 01:00.1 chip ID: 10de:10fa
 Device-2: AMD Family 17h HD Audio vendor: ASUSTeK driver: snd_hda_intel
 v: kernel bus ID: 05:00.6 chip ID: 1022:15e3
 Sound Server: ALSA v: k5.15.35-1.el7.3.x86_64

modinfo snd_hda_intel | grep -i 10de

alias:          pci:v0000 10DEd*sv*sd*bc04sc03i00*
```

Также можно попробовать поиск через легкое регулярное выражение, когда «**:**» заменяется на «**.***», что означает любые символы.

```
modinfo snd_hda_intel | grep -i 1022.*15e3

alias:          pci:v0000 1022d000015E3sv*sd*bc*sc*i*
```

Поддержка сети

Для проверки поддержки сети выполните команду:

```
inxi -a -N

Network:
 Device-1: Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet
 vendor: ASUSTeK driver: r8169 v: kernel port: e000 bus ID: 02:00.0
 chip ID: 10ec:8168
 Device-2: Realtek RTL8821CE 802.11ac PCIe Wireless Network Adapter
 vendor: AzureWave driver: rtw_8821ce v: N/A modules: rtw88_8821ce
 port: d000 bus ID: 04:00.0 chip ID: 10ec:c821

modinfo r8169 | grep -iE 10ec.*8168
```

```
alias:          pci:v000010ECd00008168sv*sd*bc*sc*i*
```

Бывают случаи, когда поле **driver** не определено (driver = N/A), но присутствует поле **module**, тогда стоит производить проверку по данному полю:

```
modinfo rtw88_8821ce | grep -iE 10ec.*c821

alias:          pci:v000010ECd0000C821sv*sd*bc*sc*i*
```

Настройка systemd-coredump для автоматического сбора дампов в РЕД ОС 7.3

Настройка сбора дампов
Изменение места сохранения дампов
Проверка работоспособности создания дампа
Чтение дампов ядра
Настройка сбора дампов в СУБД Ред База Данных

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция
- **Версия ПО**: systemd-246.10-16

Дамп памяти (*core dump*) — содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы, например, значения регистров процессора и содержимое стека. Многие операционные системы позволяют сохранять дамп памяти для отладки программы. Как правило, дамп памяти процесса сохраняется автоматически, когда процесс завершается из-за критической ошибки (например, из-за ошибки сегментации). Дамп также можно сохранить вручную через отладчик или любую другую специальную программу.

Настройка сбора дампов

В РЕД ОС 7.3 для автоматического сбора дампов используется обработчик дампов **systemd-coredump** — он собирает информацию о процессе при аварийном завершении программы. Для проверки сбора дампов выполните команду:

```
cat /proc/sys/kernel/core_pattern
|/usr/lib/systemd/systemd-coredump %P %u %g %s %t %c %h
```

Размер дампов определяется в файле конфигурации **/etc/systemd/coredump.conf**. Для изменения размера дампов в секции [Coredump] необходимо раскомментировать следующие параметры:

```
Compress=yes
ProcessSizeMax=<максимальный_размер_дампов>
ExternalSizeMax=<максимальный_размер_сжатого_дампа>
```

Далее будут подробнее рассмотрены параметры конфигурационного файла:

- Storage — определяет место хранения дампа процесса, может принимать одно из значений: *none*, *external*, *journal*.
  - *none* — дампы ядра записываются (включая обратную трассировку, если возможно), но не сохраняются;
  - *external* — значение по умолчанию, дампы сохраняются в каталоге **/var/lib/systemd/coredump/**;
  - *journal* — дампы будут храниться в журнале и перезаписываться в соответствии со стандартными принципами ротации журналов.
- Compress — используется для сжатия дампов ядра. Принимает логический аргумент — *yes* или *no*:
  - *yes* — дампы сжимаются при сохранении (значение по умолчанию);
  - *no* — дампы сохраняются без сжатия.
- ProcessSizeMax — определяет максимальный размер дампа процесса, который может быть сохранен. Если размер дампа превышает значение этого параметра, то дамп сохранен не будет. Это позволяет ограничить размер дампов и избежать переполнения дискового пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *до 1ГБ* — в 32-битных системах, *32ГБ* — в 64-битных системах. Параметры Storage=none и ProcessSizeMax=0 отключает всю обработку дампа памяти, за исключением записи журнала.
- ExternalSizeMax и JournalSizeMax — определяет максимальный (сжатый или несжатый) размер дампа процесса, который будет сохранен на диске (по умолчанию *1 ГБ* — в 32-разрядных системах, *2 ГБ* — в 64-разрядных системах), или в журнале системы (по умолчанию 10M).
- MaxUse — определяет максимальный объем общего дискового пространства, который может быть использован для хранения дампов процессов. Если общий размер всех дампов превышает значение этого параметра, старые дампы будут удаляться для освобождения места для новых. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию ограничение равно *10% от общего размера диска*.
- KeepFree — определяет минимальный объем свободного дискового пространства, который должен оставаться на диске при хранении дампов. Если свободного места на диске становится меньше указанного значения, новые дампы не будут создаваться

до тех пор, пока не будет предоставлено достаточного объема свободного пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *15% от общего размера диска* должно оставаться свободным. Старые дампы ядра также удаляются в зависимости от времени с помощью **systemd-tmpfiles**.

Изменение места сохранения дампов

Дампы по умолчанию будут создаваться в каталоге **/var/lib/systemd/coredump**. Служба **systemd-coredump** не имеет параметра конфигурации для изменения каталога, в котором будут храниться дампы.

Для смены каталога создания дампов необходимо использовать **bind-mount**:

1. В файле **/etc/fstab** пропишите монтирование нужной директории для сохранения дампов следующим образом:

```
/каталог/для/дампов /var/lib/systemd/coredump none defaults,bind 0 0
```

2. Примонтируйте каталог:

```
mount /var/lib/systemd/coredump
```

3. Перезапустите службу **systemd** для применения изменений:

```
systemctl daemon-reload
```

Проверка работоспособности создания дампа

Для проверки создания дампа необходимо выполнить в терминале:

```
sleep 3600 &
kill -11 %1
```

Проверьте создание дампа с помощью утилиты **coredumpctl**:

```
coredumpctl
```

Рассмотрим дополнительные опции **coredumpctl**:

- **list** — список доступных дампов ядра;
- **info <PID>** — вывод подробной информации об указанном дампе ядра;
- **gdb <файл>** — запускает отладчик **gdb** (GNU Debugger) для анализа дампа ядра;
- **dump <PID>** — создает дамп ядра с указанным идентификатором (PID). Дамп ядра будет передан на стандартный вывод, если не указан выходной файл с помощью **--output=**;
- **debug <PID>** — запуск процесса с указанным PID в режиме отладки. По умолчанию используется **gdb**. Отладчик может быть изменен с помощью параметра **--debugger=** или переменной среды **$SYSTEM_DEBUGGER**. Для передачи отладчику дополнительных аргументов командной строки используется параметр **--debugger-arguments=**.

Чтение дампов ядра

Сводную информацию о дампе ядра, соответствующем определенному процессу, в котором произошел сбой, можно получить, выполнив команду:

```
coredumpctl info _PID=<PID_процесса,по_которому_создан_дамп>
```

```
[user@localhost ~]$ coredumpctl info _PID=2772
           PID: 2759 (bash)
           UID: 1000 (user)
           GID: 1000 (user)
        Signal: 6 (ABRT)
     Timestamp: Fri 2023-03-31 11:46:40 MSK (20min ago)
  Command Line: bash 1212.sh
    Executable: /usr/bin/bash
 Control Group: /user.slice/user-1000.slice/session-2.scope
          Unit: session-2.scope
         Slice: user-1000.slice
       Session: 2
     Owner UID: 1000 (user)
       Boot ID: df6eee73274847bf9b977b2b77d47391
    Machine ID: 1e8ddb949cf549d8a2785068c77b85cd
      Hostname: localhost.localdomain
       Storage: /var/lib/systemd/coredump/core.bash.1000.df6eee73274847bf9b977b2b77d47391.2759.16802
       Message: Process 2759 (bash) of user 1000 dumped core.

                Stack trace of thread 2759:
                #0  0x00007fe88a6e715b __waitpid (libc.so.6 + 0xcc15b)
                #1  0x0000000000451619 waitchld.isra.12 (bash + 0x51619)
                #2  0x000000000052dfa wait_for (bash + 0x52dfa)
                #3  0x000000000043fbd7 execute_command_internal (bash + 0x3fbd7)
                #4  0x000000000043fe76 execute_command (bash + 0x3fe76)
                #5  0x0000000000426a21 reader_loop (bash + 0x26a21)
                #6  0x0000000000425144 main (bash + 0x25144)
                #7  0x00007fe88a642413 __libc_start_main (libc.so.6 + 0x27413)
                #8  0x00000000004256ce _start (bash + 0x256ce)
lines 1-28/28 (END)
```

Для полного чтения дампа необходимо установить утилиту **gdb**, выполнив команду (с правами суперпользователя **root** или администратора системы):

```
dnf install gdb
```

Запустите анализ дампа, выполнив команду:

```
coredumpctl gdb _PID=<PID_процесса,по_которому_создан_дамп>
```

```
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/bash...

warning: Unable to open "librpm.so.8" (librpm.so.8: cannot open shared object file: No such file or d
irectory), missing debuginfos notifications will not be displayed
Missing separate debuginfo for /usr/bin/bash
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/58/dbe494d53a3772d3e6f32b6c97e5b573
228ef.debug
Reading symbols from .gnu_debugdata for /usr/bin/bash...
(No debugging symbols found in .gnu_debugdata for /usr/bin/bash)
[New LWP 2759]
Missing separate debuginfo for /lib64/libiniparser.so.1
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/8c/f382586277a70f91a9befa609e0e1393
4ee12.debug
Missing separate debuginfo for /lib64/libtinfo.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/b7/b929fb355f28f374b5054d3191fc05a7
b5802.debug
Missing separate debuginfo for /lib64/libdl.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/e7/e6d7db0bca11a7f7da45896c9165d369
d14ab.debug
Missing separate debuginfo for /lib64/libc.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/75/b55efed6938ccb77e0e40fff7571aae0
ffcc0.debug
Missing separate debuginfo for /lib64/ld-linux-x86-64.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/73/db0afd7ec02589302cf7bd90ae12d482
6a6e3.debug
Core was generated by `bash 1212.sh'.
Program terminated with signal SIGABRT, Aborted.
#0  0x00007fe88a6e715b in waitpid () from /lib64/libc.so.6
(gdb)
```

Настройка сбора дампов в СУБД Ред База Данных

Для сбора дампов *СУБД Ред База Данных* необходимо в файл службы **/usr/lib/systemd/system/firebird.service** в секцию [Service] добавить строку:

```
LimitCORE=infinity
```

Для этого необходимо воспользоваться редактированием модуля юнита с помощью команды:

```
systemctl edit firebird
```

И добавить следующие строки:

```
[Service]
LimitCORE=infinity
```

После сохранения сформируется файл **/etc/systemd/system/firebird.service.d/override.conf**.

При загрузке модуля **systemd** в памяти соединит фрагмент сформированного файла (**/etc/systemd/system/firebird.service.d/override.conf**) с полным файлом модуля (**/usr/lib/systemd/system/firebird.service**). Директивы фрагмента получат приоритет над найденными директивами в оригинальном файле модуля. Для проверки всех подгружаемых фрагментов необходимо выполнить:

```
systemctl cat firebird
```

Если СУБД при работе потребляет большой объем памяти (настроен большой страничный кэш), то создание дампа на диске после падения может продолжаться некоторое время. В конфигурационном файле службы **coredump** может быть настроен таймаут работы, после которого она будет остановлена. Для того чтобы времени на создание дампа было достаточно, необходимо увеличить таймаут, например, до 30 минут, изменив значение параметра `RuntimeMaxSec` в файле **/usr/lib/systemd/system/systemd-coredump@.service**:

```
RuntimeMaxSec=30min
```

ВАЖНО!

Дампы ядра полезны для устранения неполадок, однако могут являться причиной “утечки” конфиденциальных данных. Рекомендуется отключать дампы ядра и включать их только тогда, когда это действительно необходимо.

Для отключения сбора дампов ядра необходимо остановить службу **systemd-coredump**:

```
systemctl disable systemd-coredump
systemctl stop systemd-coredump
```

kdump — инструмент для анализа причин сбоев ядра

Минимальные требования
Настройка Selinux
Запуск служб и проверка работы

Kdump — это стандартный механизм для создания дампа содержимого памяти компьютера при сбое ядра.

Минимальные требования

Минимальные требования к окружению:

- версия ядра системы – **kernel-lt-5.15.131** и выше;
- набор инструментов dracut – **dracut-056-9** и выше;
- механизм kexec – **kexec-tools-2.0.27** и выше.

Если в системе используются пакеты более ранних версий, обновите их:

```
dnf update
```

Если в системе пакеты не установлены, выполните команду:

```
dnf install dracut kexec-tools
```

Перезагрузите систему:

```
reboot
```

Затем задайте размер для дампа ядра (в примере выделено **256 Мб** памяти). Для этого в файле **/etc/default/grub** добавьте в конец строки `GRUB_CMDLINE_LINUX=` параметр `crashkernel=256M` как показано в примере:

```
GRUB_CMDLINE_LINUX="rhgb quiet crashkernel=256M"
```

Настройка Selinux

Переведите **SELinux** в режим **permissive**. Для этого откройте файл **/etc/selinux/config**:

```
nano /etc/selinux/config
```

и замените строку `SELINUX=enforcing` на `SELINUX=permissive`.

Перезагрузите систему:

```
reboot
```

Запуск служб и проверка работы

В **dmesg** проверьте, что выделенная под дампы ядра память была зарезервирована:

```
dmesg | grep crashkernel

[    0.002111] Reserving 256MB of memory at 3312MB for crashkernel (System RAM: 4095MB)

kdumpctl status

Kdump: Kdump is not operational
```

Для оценки выделенной памяти используйте команду:

```
kdumpctl estimate
```

Далее запустите службу **kdump**и добавьте ее в автозагрузку:

```
kdumpctl start
systemctl enable kdump.service --now
```

Проверьте статус службы:

```
kdumpctl status
systemctl status kdump.service
```

В выводе должно быть **active (running)**.

Для проверки работы можно выполнить команду вызова паники ядра:

```
echo c > /proc/sysrq-trigger
```

Если настройка выполнена верно, в каталоге **/var/crash/<timestamp>** будут располагаться файлы дампов **kexec-dmesg.log**, **vmcore** и **vmcore-dmesg.txt**.

Рекомендации по анализу журналов и дампов

1. Системные журналы событий ОС находятся в каталоге **/var/log/**, также можно использовать утилиту **journalctl** для просмотра журналов.

Подробную информацию по работе с утилитой **journalctl** см. в нашей статье «Работа с логами (утилита journalctl)».

Пример фильтрации содержимого журнала по типу ошибок:

```
journalctl -p err
journalctl -p alert
```

2. При анализе логов следует обращать внимание на ключевые слова, которые фигурируют в строках журналов:

- **failed** – обычно указывает на неудачное выполнение какой-либо операции или задачи. Например, сообщение вида authentication failed означает, что аутентификация завершилась неудачно;
- **error** – указывает на наличие ошибки. Далее может быть расшифровка ошибки и представлен ее код;
- **panic** – может появиться в записях, связанных с *Kernel Panic*, ошибками ядра Linux;
- **exception** – указывает на исключения (нештатную ситуацию или ошибку, которую программа или ядро не может обработать) в приложениях или ядре;
- **segfault** – ошибка сегментации, указывает на попытку доступа к памяти, к которой нет разрешения;
- **denied** – указывает на отказ в доступе, например, сообщение вида permission denied может быть связано с проблемами в правах доступа;
- **unable** – такие записи могут указывать на неспособность системы выполнить какое-либо определенное действие;
- **timeout** – задержки и таймауты могут указывать на проблемы с сетью или системными ресурсами;
- **crash** – аварийное завершение приложений или служб;
- **warning** – предупреждение о потенциальных проблемах, которые не вызывают сбоев, но требуют внимания;
- **critical** – критические события;
- **fatal** – критическая ошибка, которая приводит к сбою;
- **corruption** – обычно указывает на повреждение данных или файлов.

3. После определения кода или названия ошибки, которая связана со сбоем, уточняется ее более подробное описание, возможные причины возникновения, способы устранения. Поиск осуществляется в общедоступных поисковых системах, в системах отслеживания ошибок (*Bug tracking system*) по исследуемому компоненту или программе, а также соответствующим запросом в Техническую Поддержку программного продукта, в котором произошел инцидент.

4. Инструкция по работе с **coredump** — «Настройка systemd-coredump для автоматического сбора дампов».

5. Инструменты для анализа логов:

- средство просмотра файлов журналов **lnav** — «Средство просмотра журналов Log File Navigator (LNAV)»;
- веб-приложение для просмотра логов **loganalyzer** — «LogAnalyzer – веб-приложение для просмотра системных журналов».

Проверка работоспособности DNS с помощью nslookup

Синтаксис утилиты
Примеры использования утилиты
Получение IP-адреса
Обратное преобразование
Запись NS
Запись MX

nslookup – утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе **DNS**. Позволяет задавать различные типы запросов и опрашивать произвольно указываемые серверы для проверки работоспособности **DNS**, просмотра IP-адреса сервера, скорости его работы и т.д.

С помощью данной утилиты также можно не только получить IP-адрес по доменному имени, но и выполнить обратное преобразование, а также проверить необходимые записи **DNS**.

По умолчанию утилита **nslookup** предустановлена в РЕД ОС.

Синтаксис утилиты

Синтаксис утилиты имеет следующий вид:

```
nslookup [-опции] [домен] [сервер]
```

Основные опции **nslookup**:

- **-type** – тип информации, которую требуется получить, возможные типы: *txt*, *soa*, *ptr*, *ns*, *mx*, *mr*, *minfo*, *mg*, *mb*, *hinfo*, *gid*, *cname*, *a*, *any*;
- **-port** – использовать другой порт DNS-сервера (порт по умолчанию **53**);
- **-recurse** – рекурсивный запрос (информация запрашивается у других серверов, если она недоступна или отсутствует на указанном сервере);
- **-retry** – количество попыток опроса сервера;
- **-timeout** – время ожидания ответа от сервера (в секундах);
- **-fail** – опросить другой сервер имен, если указанный вернул ошибку.

Примеры использования утилиты

Получение IP-адреса

Для определения IP-адреса сервера по его доменному имени необходимо выполнить команду вида:

```
nslookup <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
Name: ya.ru
Address: 77.88.55.242
Name: ya.ru
Address: 5.255.255.242
Name: ya.ru
Address: 2a02:6b8::2:242
```

В строке **Server** выводится IP-адрес сервера, в строке **Address** – IP-адрес сервера и порт, с которого был отправлен запрос к **ya.ru**.

Далее отображается информация о запросе. В строке **Name** выводится доменное имя сервера, на который был отправлен запрос. В строке **Address** выводится IP-адрес, который принадлежит доменному имени сервера. Из примера видно, что доменному имени может

принадлежать несколько IP-адресов.

Обратное преобразование

Также с помощью утилиты **nslookup** может быть выполнено обратное преобразование IP-адреса в доменное имя. Для этого используется команда вида:

```
nslookup <IP-адрес>
```

Пример команды и ее вывода:

```
nslookup 77.88.55.242

242.55.88.77.in-addr.arpa name = ya.ru.

Authoritative answers can be found from:
55.88.77.in-addr.apra nameserver = ns3.yandex.ru.
55.88.77.in-addr.apra nameserver = ns4.yandex.ru.
ns3.yandex.ru internet address = 87.250.250.1
ns3.yandex.ru has AAAA address = 2a02:6b8::1001
ns4.yandex.ru internet address = 77.88.21.1
ns4.yandex.ru has AAAA address = 2a02:6b8:0:1::1:1
```

Запись NS

Первоисточником информации о домене являются его **NS**-серверы. Получить их можно, используя опцию `-type=ns` в команде следующего вида:

```
nslookup -type=ns <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=ns ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru nameserver = ns2.yandex.ru.
ya.ru nameserver = ns1.yandex.ru.

Authoritative answers can be found from:
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

Команда выведет список используемых серверов имен, в приведенном примере это **ns1.yandex.ru**.

Запись MX

Также можно получить **MX**-запись для домена, установив тип запроса **mx** в команде следующего вида:

```
nslookup -type=mx <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=mx ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru mail exchanger = 10 mx.yandex.ru.
```

```
Authoritative answers can be found from:
ya.ru nameserver = ns1.yandex.ru.
ya.ru nameserver = ns2.yandex.ru.
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

В выводе команды будут отображены все настроенные почтовые серверы, у каждого сервера есть свой приоритет – 15, 10 или 5. Чем меньше число, тем выше приоритет адреса. В приведенном примере почтовый сервер – **mx.yandex.ru** имеет приоритет **10**.

Системные требования

В данной статье приведены минимальные системные требования для установки операционной системы **РЕД ОС** в конфигурациях «**Рабочая станция**» и «**Сервер**» для версии **7.3 и 8**.

Системные требования для **РЕД ОС 7.3** и **8**:

Конфигурация	Рабочая станция	Сервер	Сервер минимальный
Процессор	X86_64 1.6 ГГц 2 ядра	X86_64 1.6 ГГц 2 ядра	X86_64 1.6 ГГц 1 ядро
Объем оперативной памяти	2 Гб	2 Гб	1 Гб
Объем свободного дискового пространства	20 Гб	20 Гб	8 Гб
Видеоадаптер	Поддержка режима SVGA800x600	Поддержка режима SVGA800x600	Поддержка режима SVGA800x600

Создание загрузочных носителей

Определение схемы разделов жёстких дисков
balenaEtcher
MultiWriter
dd
kindd
Rufus для Windows
Brasero
win32 disk imager для Windows
rawrite32 для Windows

Вы можете подробнее ознакомиться с возможностью создания загрузочных носителей и записи ISO-образов, просмотрев наши обучающие видео:

- на **RuTube**:
  - Запись iso-образа РЕД ОС и установка рядом с Windows;
  - Создание загрузочных носителей flash, cd, dvd.
- в **Яндекс.Дзен**:
  - Запись iso-образа РЕД ОС и установка рядом с Windows;
  - Создание загрузочных носителей flash, cd, dvd.
- в **VK Видео**:
  - Запись iso-образа РЕД ОС и установка рядом с Windows;
  - Создание загрузочных носителей flash, cd, dvd.

На наших каналах вы также сможете найти много другой полезной информации.

Определение схемы разделов жёстких дисков

Прежде чем приступить к установке РЕД ОС и начать работу с разделами жёсткого диска, необходимо определить, какая схема разделов на нём использована. Возможны 2 варианта схемы разделов:

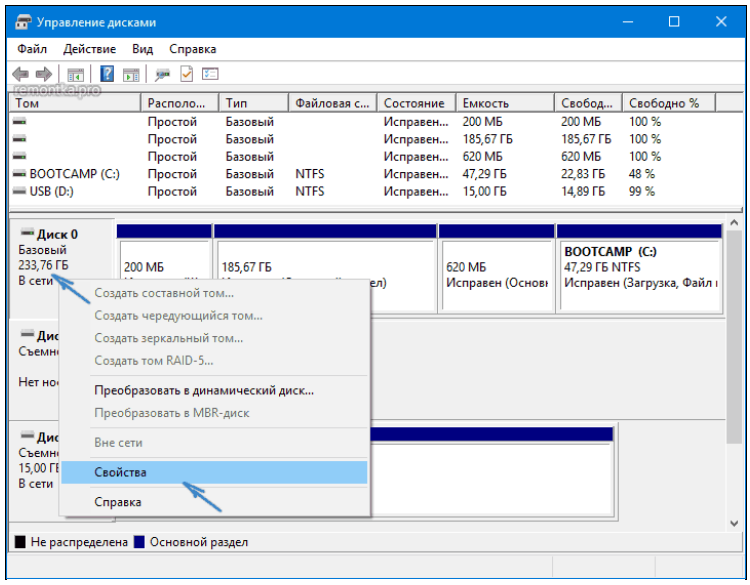
- **MBR** (Главная загрузочная запись);
- **GPT** (Таблица разделов GUID).

Они представляют собой два различных способа хранения информации о разделах диска. Сюда входят данные о начале и конце разделов, чтобы система знала, к какому разделу принадлежит каждый сектор, и какой раздел является загрузочным.

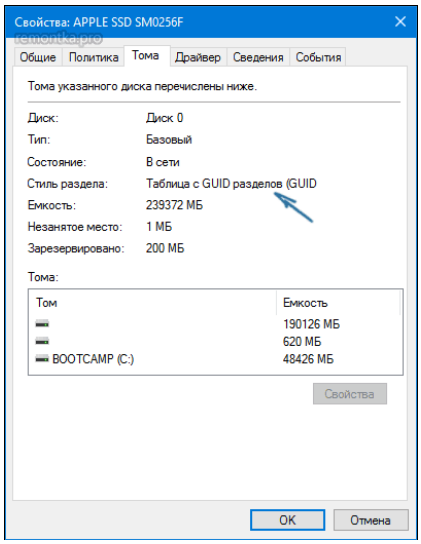
Верное определение схемы разделов жёсткого диска имеет значение для правильной подготовки загрузочного носителя. Несовпадение схем разделов жёсткого диска, на который устанавливается система, со схемой разделов загрузочного носителя, может привести к невозможности загрузки установщика.

Чтобы определить стиль схемы разделов Windows, запустите утилиту «**Управление дисками**» нажмите клавиши **Win+R**, введите **diskmgmt.msc** и нажмите **Enter**.

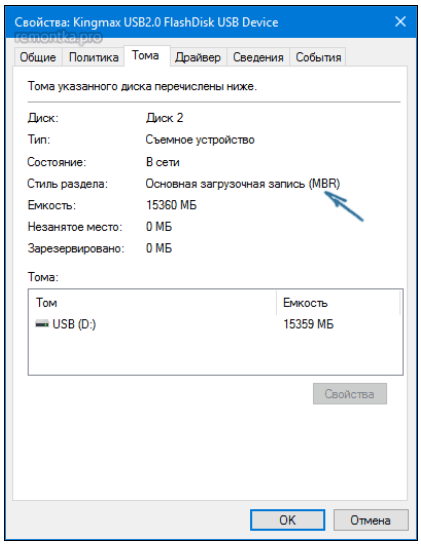
1.В нижней части утилиты «**Управление дисками**» кликните по имени диска правой кнопкой мыши и выберите пункт меню «**Свойства**».



2.В свойствах откройте вкладку «**Тома**». Если в пункте «**Стиль раздела**» указано «**Таблица с GUID разделов**» — у вас GPT-диск.



Если в этом же пункте указано «**Основная загрузочная запись (MBR)**» — у вас MBR-диск.



1 способ - balenaEtcher

balenaEtcher — свободное программное обеспечение с открытым исходным кодом, предназначенное для записи файлов образов дисков, таких как **.iso** и **.img**, а также архивов для создания LiveUSB флэш-накопителей. Скачать утилиту можно по ссылке. Существуют версии для Linux, Windows и macOS. Процедура записи образа аналогична для всех видов ОС.

Для Windows можно скачать и установить программу или запустить версию **portable** (без установки).

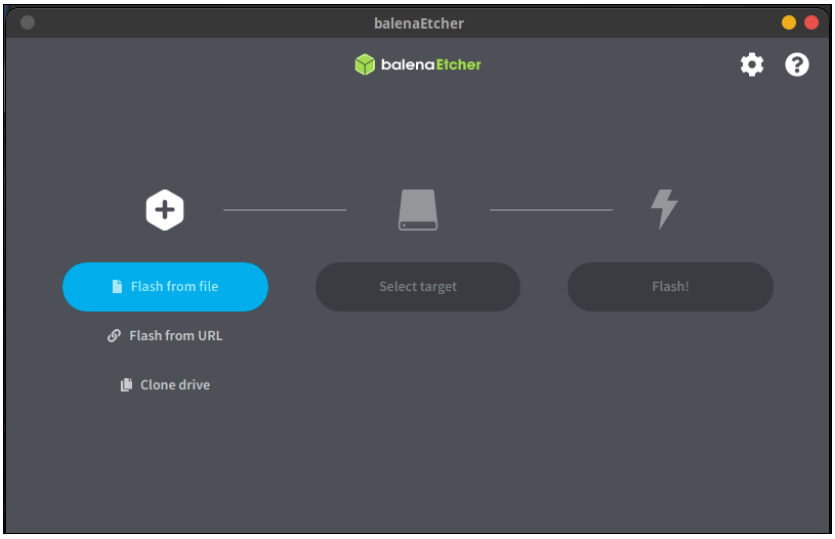
Для Linux - программа распространяется в формате **AppImage**. После ее загрузки перейдите в папку с файлом и предоставьте права на исполнение для полученного файла:

```
chmod +x balenaEtcher-1.18.11-x64.AppImage
```

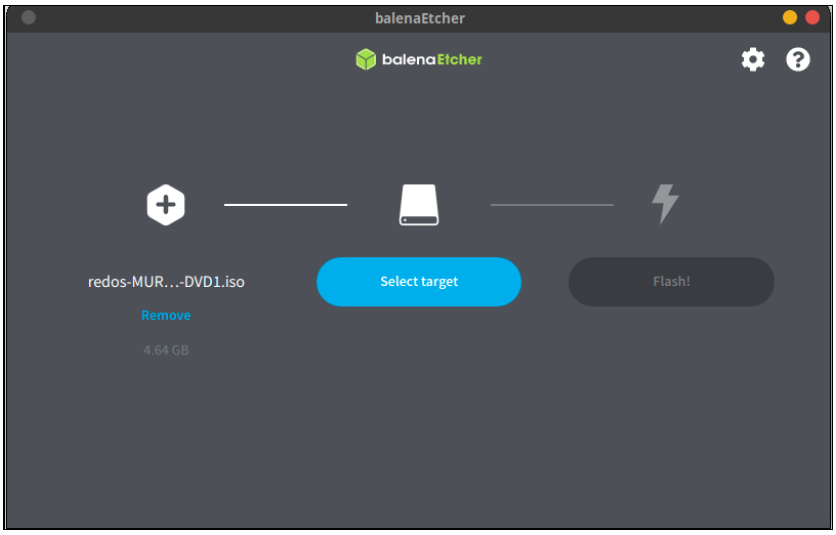
Запустить программу можно двойным кликом по файлу, либо выполнив команду в терминале:

```
./balenaEtcher-1.18.11-x64.AppImage
```

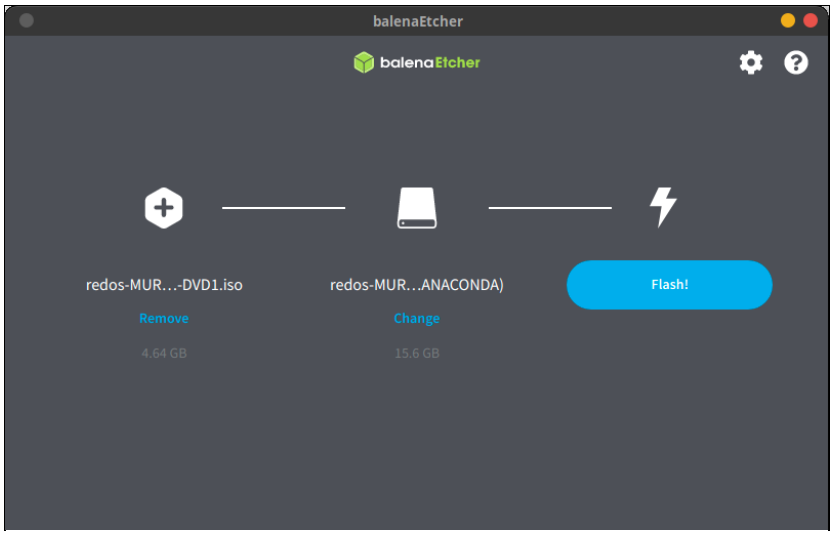
Для записи образа выберите файл, нажав на «**Flash form file**»:



Далее выберите устройство, на которое будет записан образ:



После выбора устройства нажмите «**Flash!**»:



Далее будет запрошен пароль администратора, после успешной аутентификации начнется запись образа.

2 способ - MultiWriter

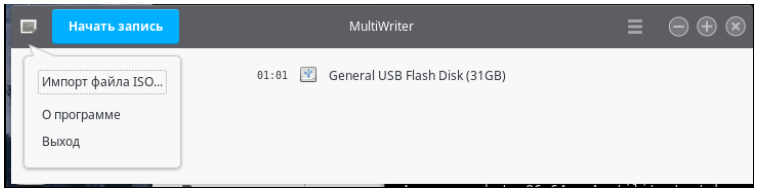
Для записи iso-образов на USB-флеш-накопитель воспользуйтесь приложением **MultiWriter**.

Установка **MultiWriter**:

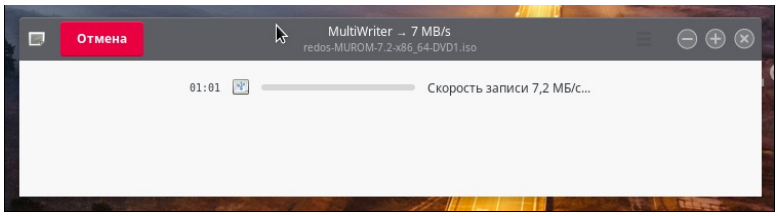
```
dnf install gnome-multi-writer
```

Откройте программу через «**Меню**» - «**Администрирование**» - «**MultiWriter**».

Импортируйте файл iso-образа:



Нажмите на кнопку «**Запись**», в результате начнется запись iso-образа на flash-носитель.



3 способ - dd

Определить имя flash-носителя, например, **sd[x]**:

```
sudo fdisk -l
```

Перейдите в консоли в каталог с iso-образом:

```
cd /путь/до/образа
```

Запись iso-образа:

```
dd if=redos-MUROM-7.2-20190523.0-Everything-x86_64-DVD1.iso of=/dev/sd[x] bs=8MB status=progress oflag=direct
```

ВАЖНО!

Вместо sd[x] укажите свое имя носителя.
При этом будут стерты все данные на USB накопителе и записаны новые!

Для систем с **UEFI** и таблицей разделов **GPT** следует подготовить flash-носитель, выполнив список команд:

```
parted -s /dev/sd[x] mklabel gpt
parted -s --align=optimal /dev/sd[x] mkpart REDOS fat32 1MiB 100%
parted -s /dev/sd[x] set 1 boot on
mkfs.vfat -F 32 /dev/sd[x]
```

Запись iso-образа:

```
dd if=redos-MUROM-7.2-20190523.0-Everything-x86_64-DVD1.iso of=/dev/sd[x] bs=8MB status=progress oflag=direct
```

4 способ - kindd (gui для dd)

Kindd — графический (gui) интерфейс для команды **dd**, бесплатный инструмент с открытым исходным кодом, написанный на **Qt**. Данный инструмент может быть очень полезен новичкам для записи образов дисков.

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

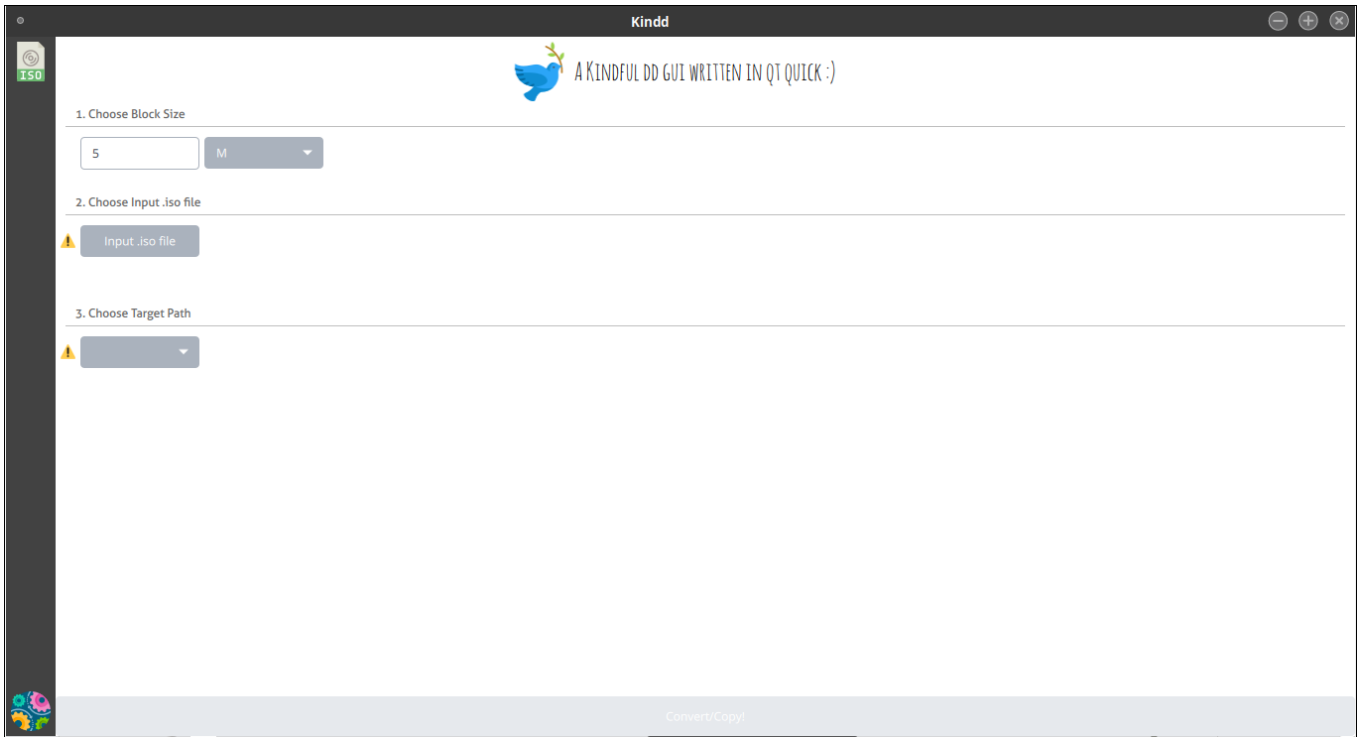
и выполните команду:

```
dnf install kindd
```

После установки запуск утилиты доступен из «**Главного меню**» - «**Стандартные**» - «**Графическая оболочка для dd**» или через терминал командой:

```
kindd
```

После запуска откроется окно утилиты:



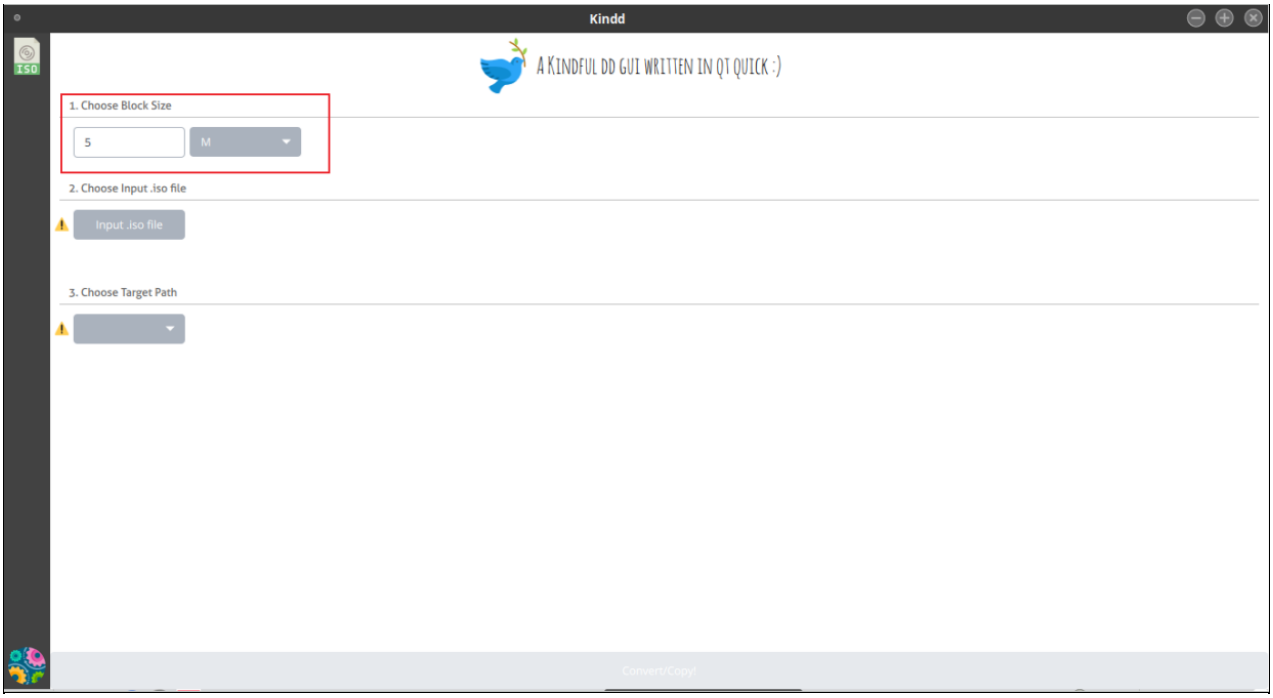
Алгоритм работы с kindd

Интерфейс **kindd** состоит из двух разделов: «**Создать загрузочный .iso**» (открывается по умолчанию) и «**Настройки**». На вкладке «**Настройки**» устанавливаются параметры внешнего вида программы.

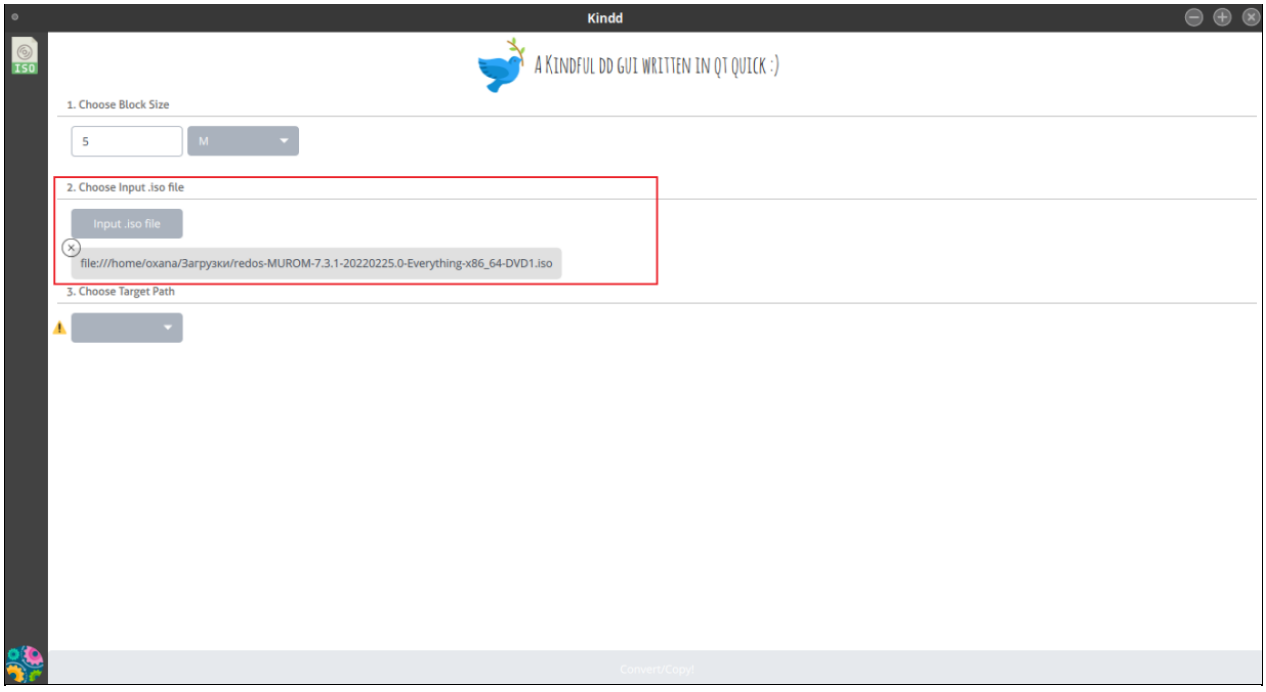
Для работы с утилитой понадобится USB-накопитель и ISO-файл.

Чтобы создать загрузочный USB-накопитель из ISO, подключите USB-накопитель, а затем запустите **kindd**.

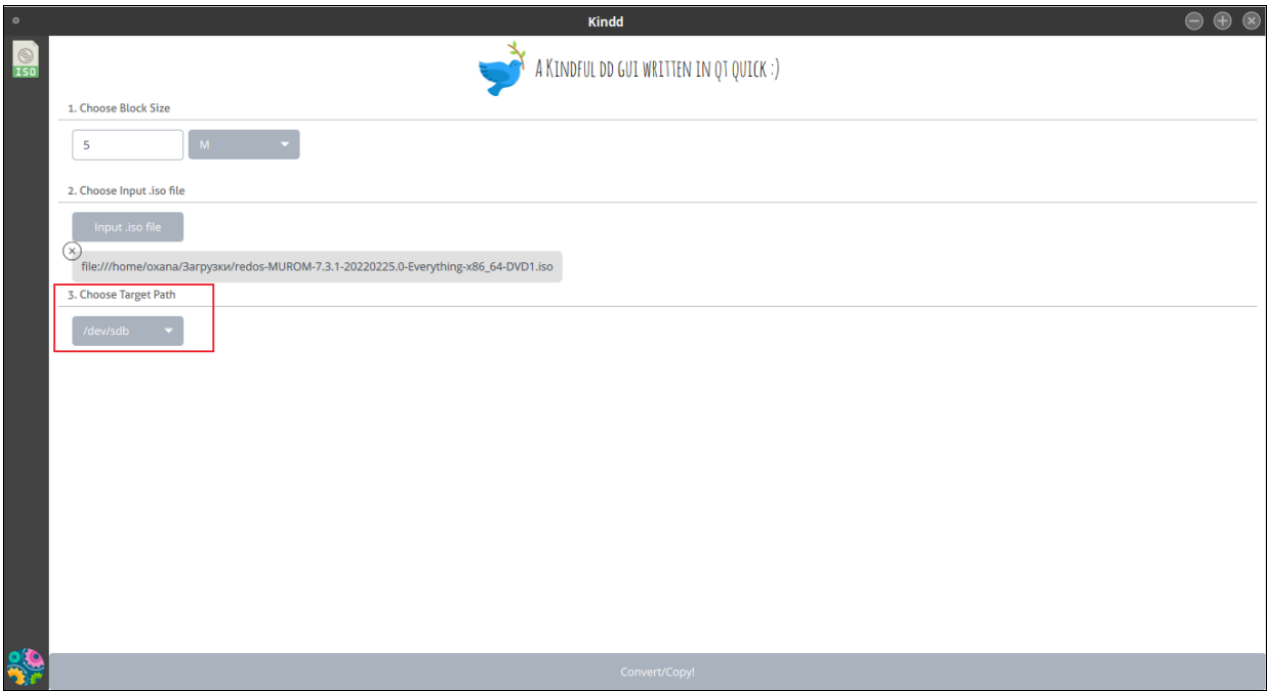
1. Укажите размер блока записи (можно оставить по умолчанию).



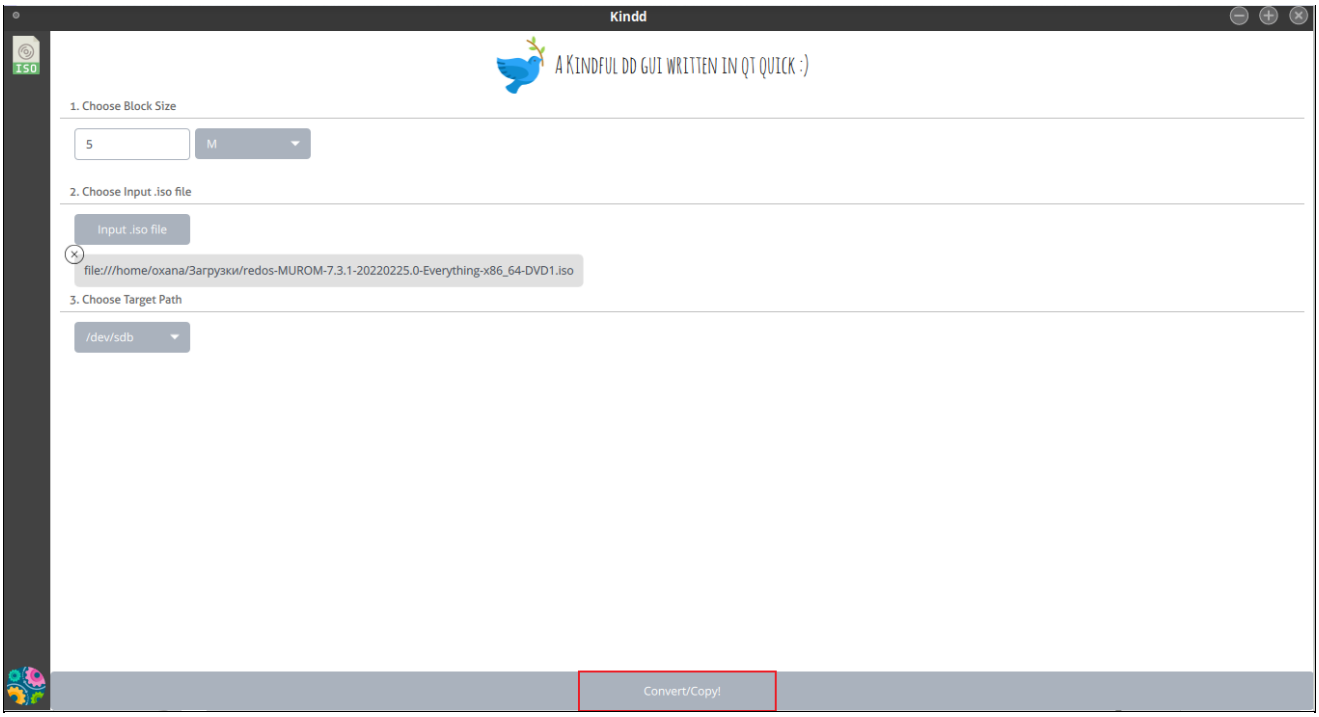
2. Выберите путь к файлу ISO.



3. Выберите устройство для записи.



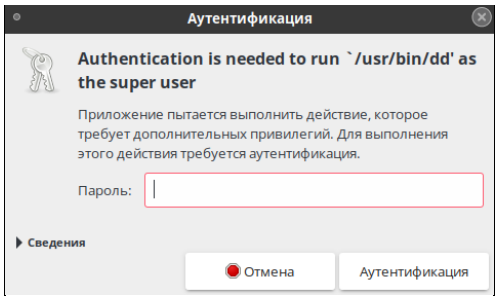
4. Нажмите кнопку **Convert/Copy**, чтобы начать создание загрузочного ISO.



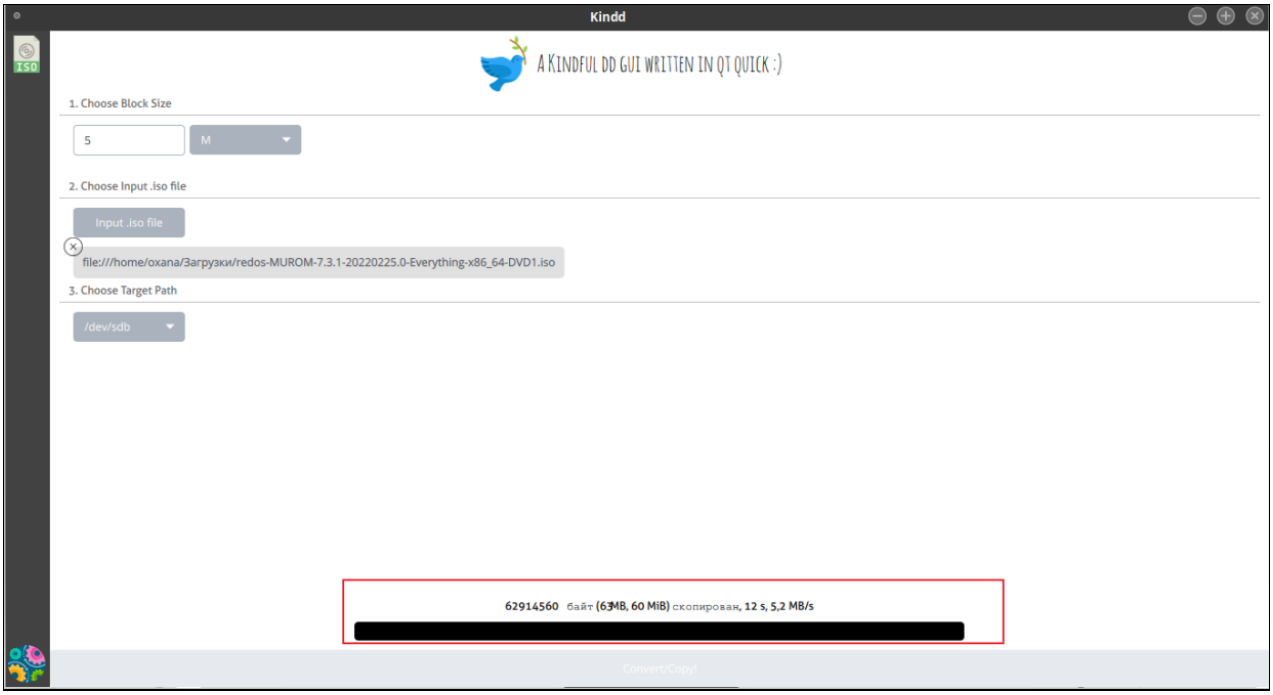
5. Появится сообщение: «**Вы уверены, что хотите продолжить?**» Нажмите «**Yes, i'm sure**».



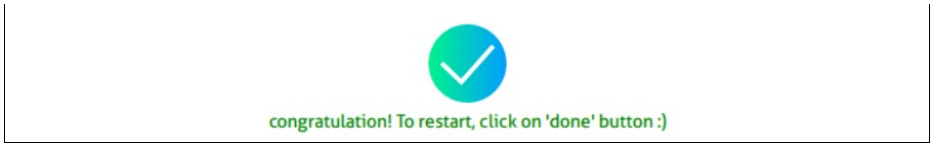
6. Далее необходимо ввести пароль суперпользователя.



7. После успешной аутентификации начнется загрузка:



8. При успешном завершении записи вы увидите следующее сообщение:



После этого можно проверить загрузку системы с USB-устройства.

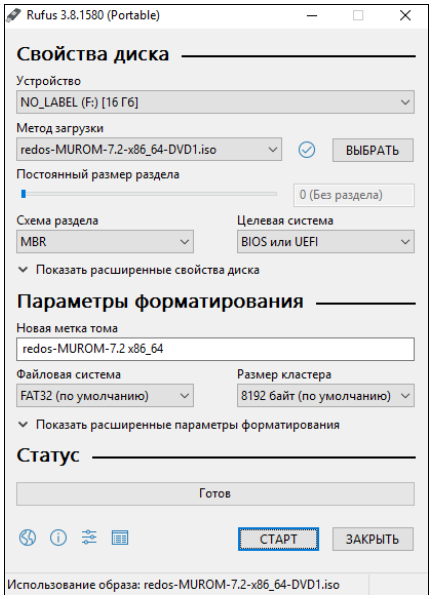
5 способ - Rufus для Windows

Примечание.

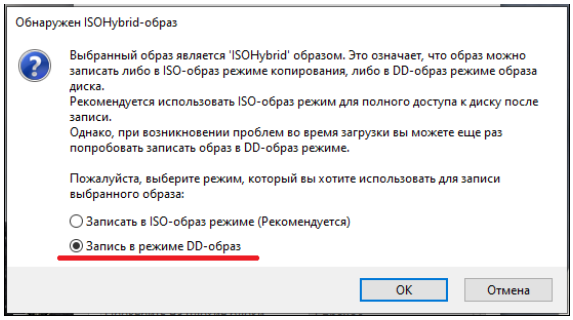
Если для установки РЕД ОС планируется использовать образ **live-usb**, то запись установочного образа с использованием ПО **Rufus** нужно производить в режиме **ISO**.

Для записи iso-образов в **Windows** на flash-накопитель можно воспользоваться утилитой **Rufus**, которая доступна по ссылке.

Из списка «**Устройство**» необходимо выбрать ваше устройство, затем нажать кнопку «**Выбрать**».

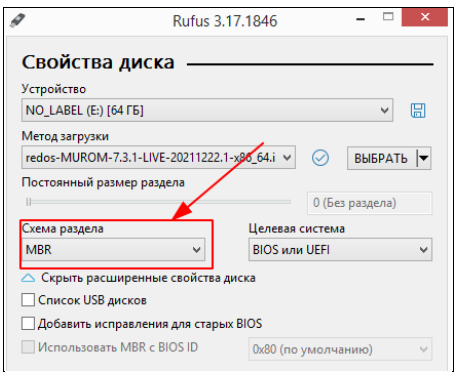


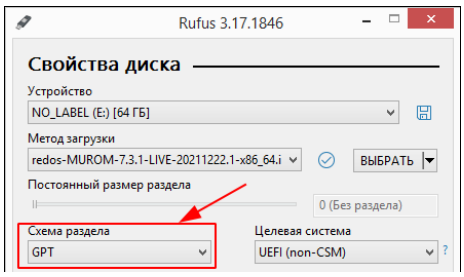
При записи образа РЕД ОС через Rufus, необходимо выбрать режим **DD**. Окно с запросом о выборе режима появляется после нажатия кнопки «**СТАРТ**».



Также при создании загрузочного носителя обратите внимание, что схема разделов загрузочного носителя должна совпадать со схемой разделов жёсткого диска вашего ПК.

Если на жёстком диске вашего ПК используется схема разделов **MBR**, то при создании образа в пункте «**Схема раздела**» необходимо выставить параметр «**MBR**». Соответственно, если вы используете ПК со схемой разделов жёсткого диска с **GPT**, то при создании образа в пункте «**Схема раздела**» необходимо выставить параметр «**GPT**».





6 способ - Brasero

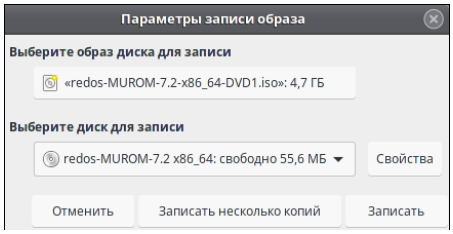
Для записи iso-образов на CD/DVD используйте приложение «**Brasero**». Если **Brasero** не установлено, его можно установить командой:

```
dnf install brasero
```

Приложение открывается из «**Меню**» - «**Аудио и видео**» - «**Brasero**».

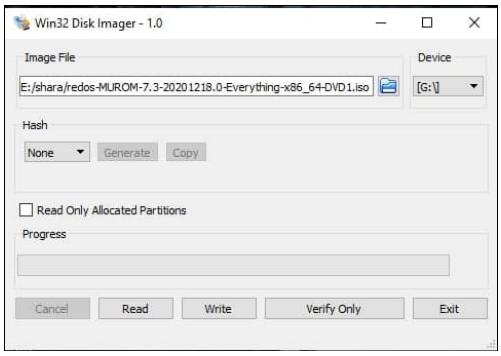
В приложении выберите пункт записать образ.

В открывшемся окне выберите iso-образ и диск.



7 способ - win32 disk imager для Windows

Для записи iso-образов в **Windows** на flash можно также воспользоваться утилитой **win32 disk imager**, которая доступна по ссылке.

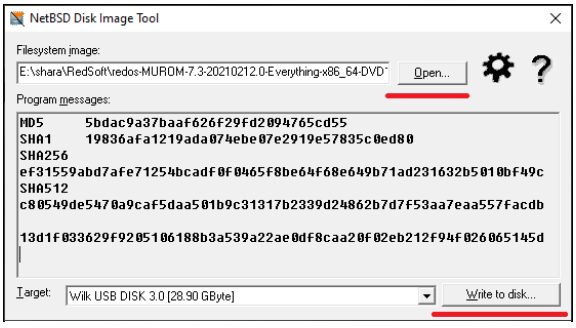


В открывшемся окне выберите iso-образ, flash-накопитель (в поле **Device**) и нажмите кнопку «**Write**».

8 способ - rawrite32 для Windows

Еще один способ для записи iso-образов в **Windows** на flash - использование утилиты **rawrite32**, которая доступна по ссылке.

Все что нужно сделать, это выбрать образ, flash-накопитель (в поле **Target**) и нажать «**Write to disk**».



Последовательность установки

До того, как будет произведена установка РЕД ОС на жесткий диск СВТ, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования СВТ завершилась успешно, будет запущен псевдографический интерфейс программы-установщика (**anaconda**). Процесс установки реализован в виде «мастера» установки, который представляет из себя интерактивный графический интерфейс, в котором пользователю предлагается отвечать на вопросы и указывать необходимые опции РЕД ОС. Мастер установки разделен на шаги, каждый шаг посвящен настройке или установке определенного сервиса системы. Шаги нужно проходить последовательно, переход к следующему шагу происходит по нажатию кнопки «**Далее**». При помощи кнопки «**Назад**», при необходимости, можно вернуться к уже пройденному шагу и изменить настройки. На некоторых этапах установки возможность перехода к предыдущему шагу ограничена теми шагами, где нет зависимости от данных, введенных ранее.

Если по каким-то причинам возникла необходимость прекратить установку, нажмите ***Reset*** на системном блоке компьютера. Помните, что совершенно *безопасно* прекращать установку только до шага «**Подготовка диска**», поскольку до этого момента не производится никаких изменений на жестком диске. Если прервать установку между шагами «**Подготовка диска**» и «**Установка загрузчика**», вероятно, что после этого с жесткого диска не сможет загрузиться ни одна из установленных систем.

Технические сведения о ходе установки можно посмотреть, нажав *«Ctrl+Alt+F1»*, вернуться к программе установки - *«Ctrl+Alt+F6»*. По нажатию *«Ctrl+Alt+F2»* откроется отладочная виртуальная консоль.

Во время установки РЕД ОС выполняются следующие шаги:

- Выбор типа накопителя СВТ;
- Присвоение имени компьютера в сети и настройка сетевых интерфейсов;
- Выбор часового пояса;
- Задание пароля администратора системы;
- Подготовка разделов диска;
- Выбор типа установки: сервер или рабочая станция;
- Установка системы;
- Установка загрузчика;
- Перезагрузка системы;
- Лицензионный договор;
- Создание системного пользователя;
- Установка даты и времени;
- Сохранение настроек;
- Завершение установки.

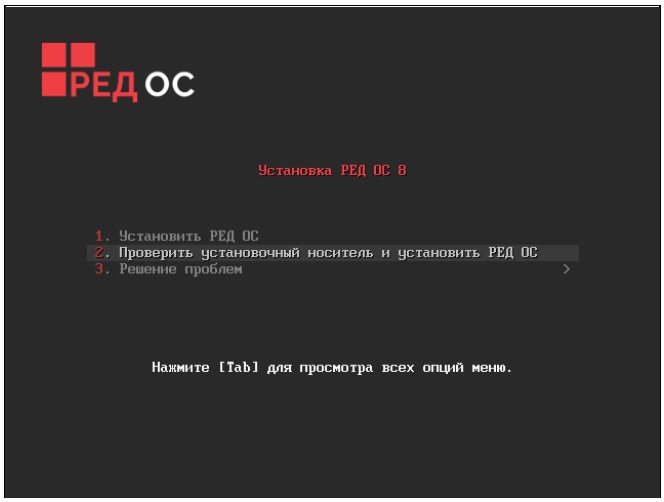
Начало установки

Системные требования

Системные требования к составу технических средств приведены в нашей статье «Системные требования».

Начало установки

Перед началом установки РЕД ОС необходимо настроить BIOS рабочей станции на загрузку с носителя информации (DVD-диска или флеш-накопителя), куда записан дистрибутив. Способ входа в меню BIOS и расположение конкретных настроек может сильно отличаться, в зависимости от используемой материнской платы оборудования рабочей станции. Чаще всего для входа в BIOS необходимо нажать функциональную клавишу *Delete* на стационарных рабочих станциях или функциональную клавишу *F1 (F9)* на мобильных рабочих станциях (ноутбуках) в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.



Загрузка с установочного носителя начинается с меню, в котором перечислено несколько вариантов загрузки, причем установка системы - это только одна из возможностей. Из данного меню можно:

- запустить тестирование носителя данных и только после этого перейти к процедурам установки ОС;
- используя меню «**Решение проблем**», запустить проверку памяти и диагностику оборудования;
- запустить уже установленную ОС на жестком диске;
- загрузить ОС в аварийном режиме.

Манипулятор графической информации (мышь) на этом этапе установки не поддерживается, поэтому для выбора различных вариантов и опций установки необходимо воспользоваться функциональными клавишами клавиатуры - стрелками. Можно скорректировать параметры запуска любого пункта начального меню установки РЕД ОС, нажав функциональную клавишу клавиатуры *TAB.*

Установка РЕД ОС автоматически осуществляется в графическом режиме с выводом текстовой информации на выбранном в начале процесса установки языке.

По умолчанию при установке используется графический видеорежим (разрешение экрана) 800x600. При возникновении проблем запуска установки в графическом режиме существует возможность альтернативной установки системы - не графический (текстовый) режим. Подробнее об установке РЕД ОС в текстовом режиме см. в нашей статье «Установка РЕД ОС в текстовом режиме».

Чтобы начать процесс установки, нужно клавишами перемещения курсора «вверх»/«вниз» выбрать пункт меню «**Установить RED OS**» и нажать *Enter.* В начальном загрузчике установлено небольшое время ожидания продолжительностью 1 минута. Если в этот момент не предпринимать никаких действий, то будет загружена установка системы с проверкой установочного носителя. Если пропущен нужный момент, нужно перезагрузить компьютер и до истечения установленного времени ожидания выбрать нужный пункт в меню загрузчика.

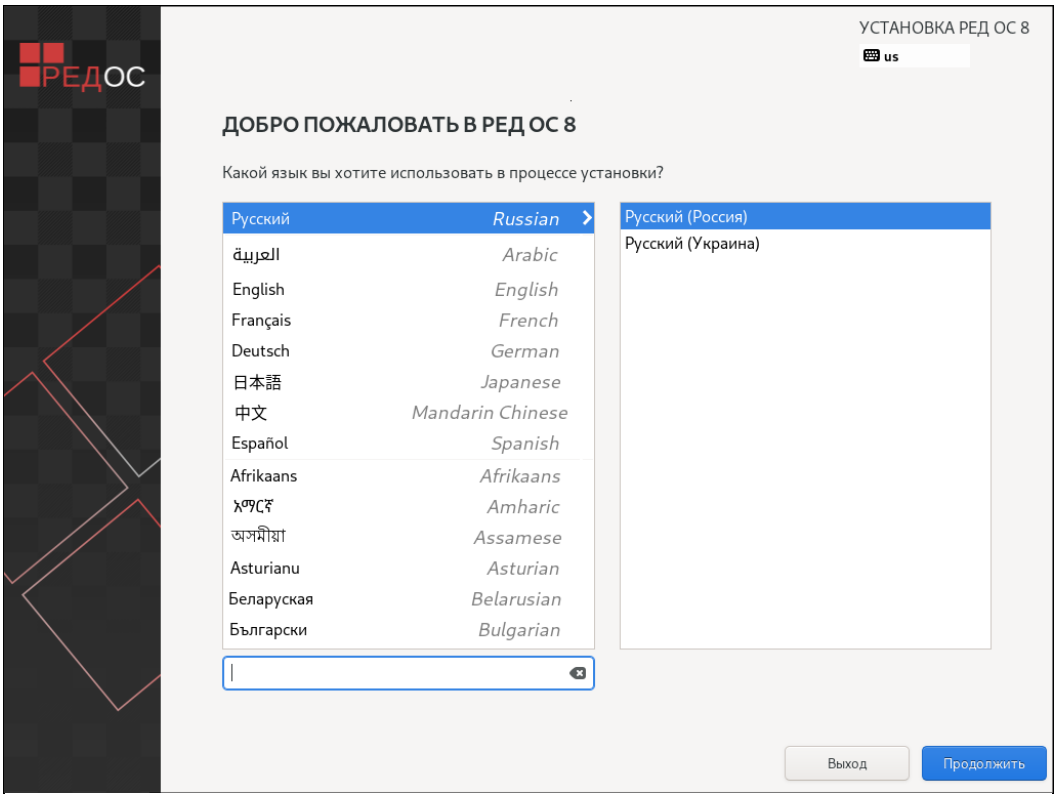
Начальный этап установки не требует вмешательства пользователя: происходит автоматическое определение оборудования и запуск компонентов программы установки. Прервать начальный этап установки и вернуться в начальное меню установки РЕД ОС можно, нажав клавишу *ESC.*

Язык интерфейса программы установки

Язык интерфейса программы установки можно выбрать на самом первом этапе процесса установки. Язык устанавливаемой РЕД ОС будет русским, если был выбран русский язык, или английским, если был выбран любой другой язык.

Дополнительным языком РЕД ОС является английский язык. Другие дополнительные языковые пакеты можно установить из репозитория после завершения установки РЕД ОС.

Переключение раскладки клавиатуры при установке РЕД ОС и в графическом интерфейсе РЕД ОС выполняется нажатием комбинации функциональных клавиш *«Alt+Shift»*.



Обзор установки

Дата и время
Клавиатура
Языковая поддержка
Источник установки
Выбор программ
Место установки
Сеть и имя узла
Создание пароля администратора

Окружение

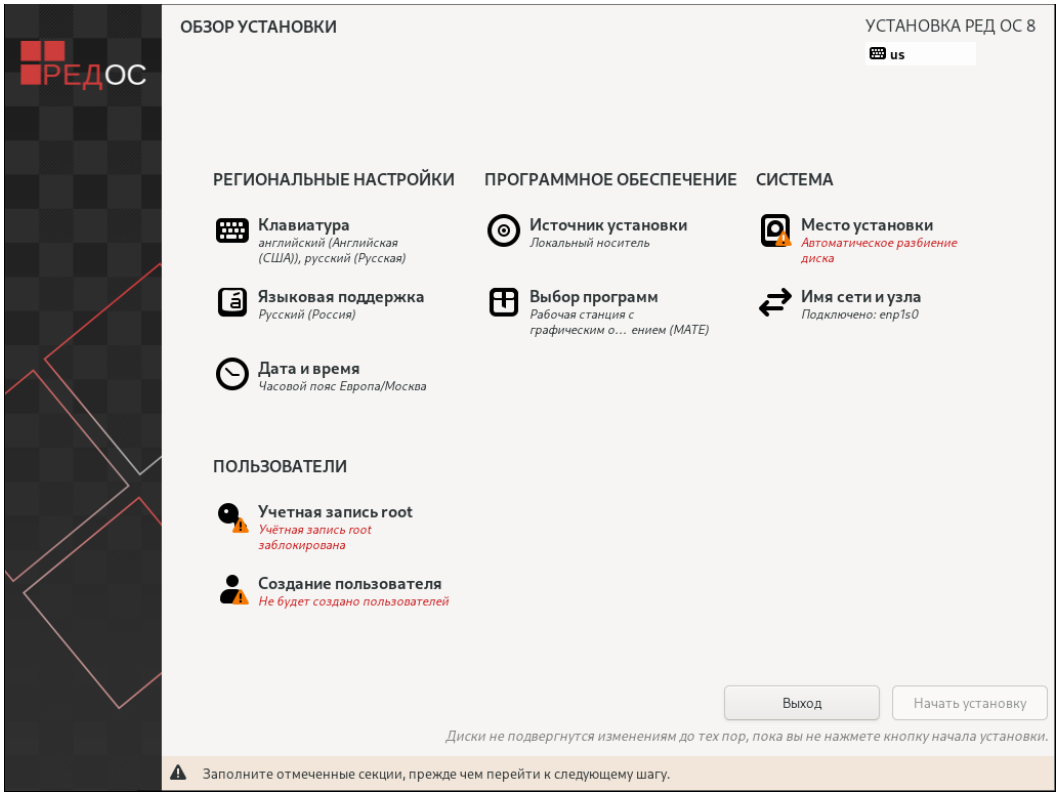
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный

Вы можете подробнее ознакомиться с каждым этапом установки системы, просмотрев наши обучающие видео:

- на **RuTube** — Установка РЕД ОС;
- в **Яндекс.Дзен** — Установка РЕД ОС;
- в **VK Видео** — Установка РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

После выбора языка необходимо произвести первоначальную конфигурацию установщика и параметров будущей системы.

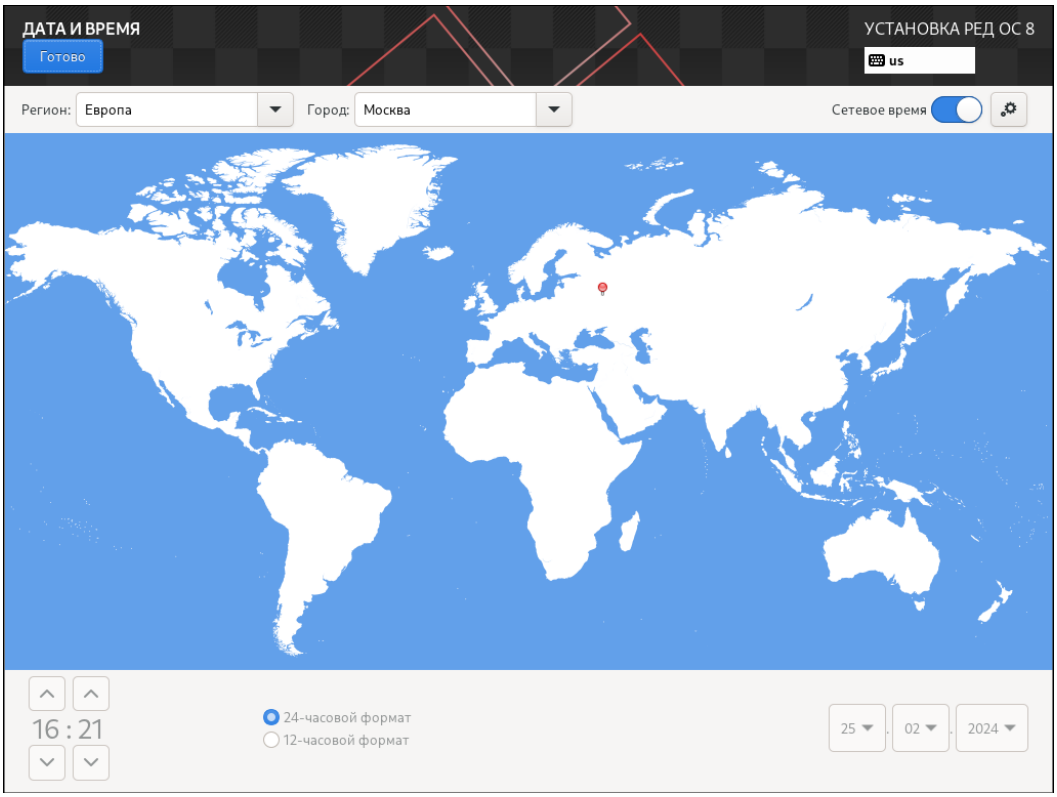


В этом окне необходимо задать региональные настройки, состав программного обеспечения и системные настройки. Здесь и в последующих окнах установщика красным цветом выводятся подсказки у тех вкладок, которые должны быть обязательно заполнены до перехода к следующему шагу установки.

Рассмотрим подробнее каждую вкладку окна.

Дата и время

В окне настройки даты и времени можно выбрать текущий регион и город и установить используемое локальное время, дату и формат времени.



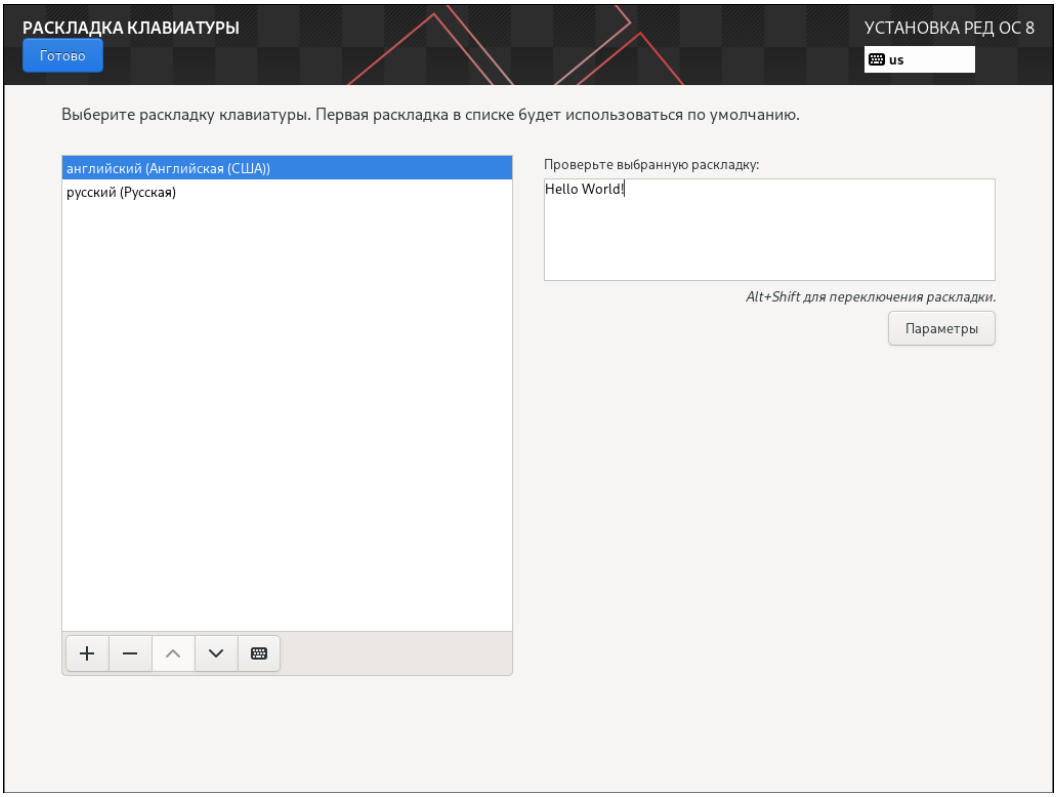
Если установлена сеть, и есть доступ к глобальной сети, можно разрешить автоматическую настройку времени с помощью службы **ntp** — сетевое время.

Данную настройку можно изменить после завершения установки РЕД ОС. По умолчанию устанавливается часовой пояс UTC+03:00 (Европа/Москва).

Здесь и далее возврат в предыдущее меню осуществляется с помощью кнопки «Готово».

Клавиатура

В окне настройки клавиатуры можно выбрать используемые в ОС раскладки.

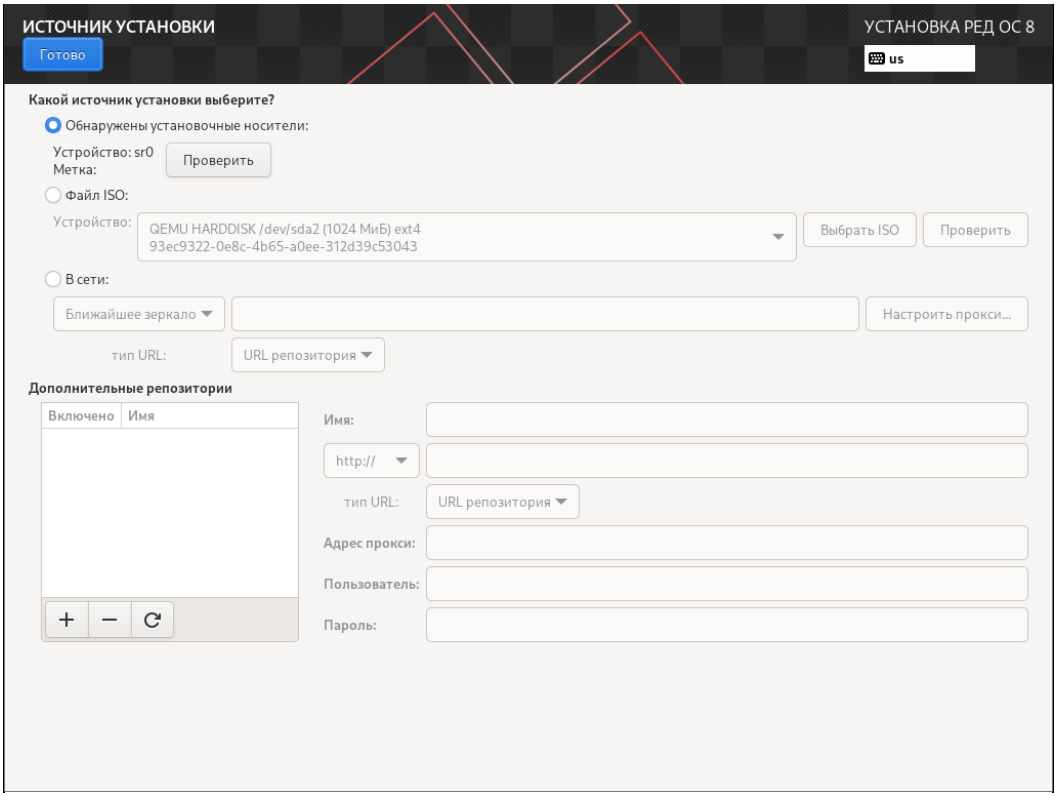


В отдельном поле ввода можно проверить корректность отображения вводимых символов.

Первая раскладка в списке будет использоваться по умолчанию.

Источник установки

В меню выбора источников установки можно задать, откуда система будет получать пакеты в процессе установки.

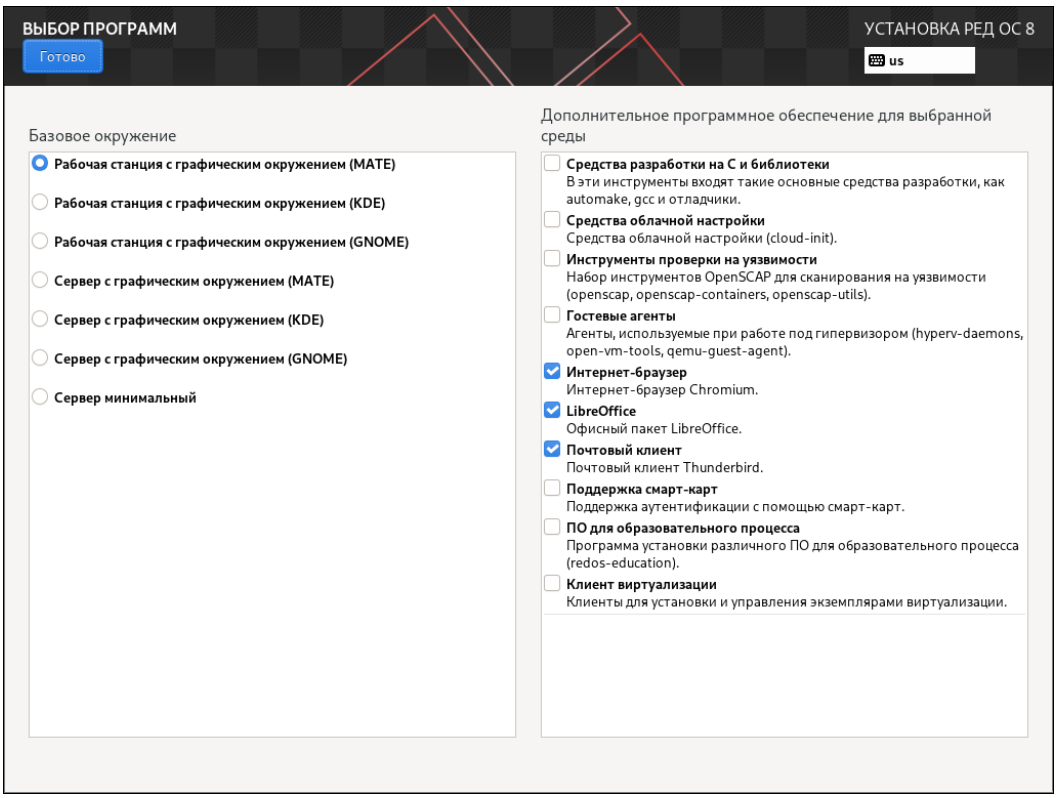


Источниками установки могут быть локальные носители или сетевые источники.

Выбор программ

В меню выбора программ можно задать, какая конфигурация из числа базового окружения будет установлена:

- рабочая станция,
- сервер минимальный,
- сервер с графическим интерфейсом.



Дополнительно для каждой из выбранных конфигураций можно настроить группы пакетов, которые будут установлены.

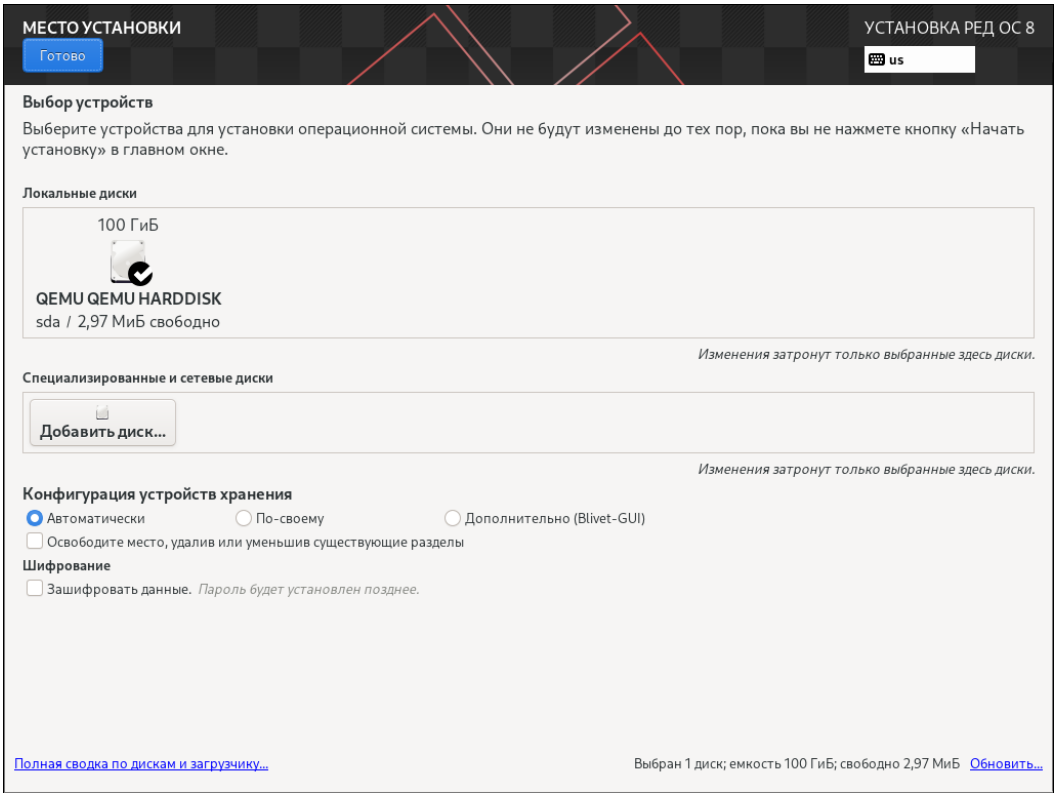
В любом дистрибутиве Linux доступно значительное количество программ (до нескольких тысяч), часть из которых составляет саму ОС, а все остальные - это прикладные программы и утилиты.

В РЕД ОС все операции установки и удаления производятся над пакетами - отдельными компонентами системы. Пакет и программа соотносятся неоднозначно: иногда одна программа состоит из нескольких пакетов, иногда один пакет включает несколько программ.

В процессе установки РЕД ОС обычно не требуется детализированный выбор компонентов на уровне пакетов - это требует слишком много времени и знаний от проводящего установку. Тем более, что комплектация дистрибутива подбирается таким образом, чтобы из имеющихся программ можно было составить полноценную рабочую среду для соответствующей аудитории пользователей. Поэтому в процессе установки РЕД ОС пользователю предлагается выбрать из небольшого списка конфигураций, объединяющих пакеты, необходимые для решения наиболее распространённых задач.

Место установки

В меню выбора расположения установки можно выбрать устройство для установки операционной системы.



Переход к этому шагу может занять некоторое время. Время ожидания может быть разным и зависит от производительности компьютера, объёма и типов используемых накопителей, количества существующих разделов на них.

На этом этапе подготавливается площадка для установки РЕД ОС, в первую очередь - выделяется свободное место на диске.

Можно выбрать и использовать профили разбиения диска. Профиль - это шаблон распределения места на диске для установки РЕД ОС.

Можно выбрать:

- автоматически;
- по-своему;
- дополнительно (Blivet-GUI).

Первый профиль предполагает *автоматическое* разбиение диска. Будет выбрано оптимальное расположение ОС. Необратимые изменения разделов на жёстком диске требуют подтверждения со стороны пользователя. После подтверждения внесённые изменения сохраняются на жестком диске/дисках СВТ. При выборе автоматического разбиения ОС будет установлена на диск со схемой разбиения «**Стандартный раздел**».

Если для применения одного из профилей автоматической разметки доступного места окажется недостаточно, будет выведено сообщение о невозможности выполнения операции разбиения диска.

При необходимости можно освободить часть дискового пространства, для этого следует воспользоваться профилем разбиения *вручную*. Можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «Готово» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке «Файловая система».

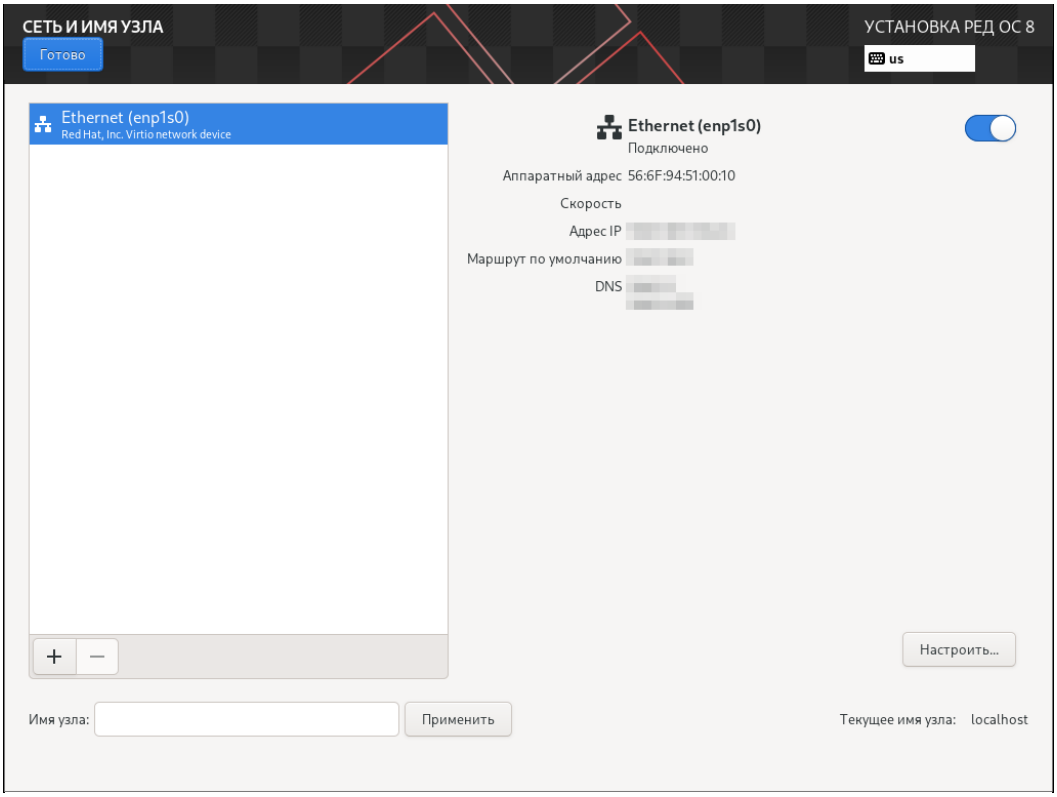
ВАЖНО!

Не следует форматировать разделы с теми данными, которые необходимо сохранить, например, с пользовательскими данными (/home) или с другими операционными системами. С другой стороны, отформатировать можно любой раздел, который необходимо «очистить» (т.е. удалить все данные).

Blivet-gui является обособленной реализацией механизмов управления разделами и дисками, снабжённой привычным интерфейсом в стиле **GParted**. Программа поддерживает управление дисковыми разделами и хранилищами **LVM2** (включая шифрованные разделы LUKS, логические тома и группы томов). Так же как и в **GParted**, изменения в **blivet-gui** применяются не сразу, а после подтверждения внесённого набора изменений.

Сеть и имя узла

В меню выбора настройки сети можно активировать соединение с сетью и задать имя узла.



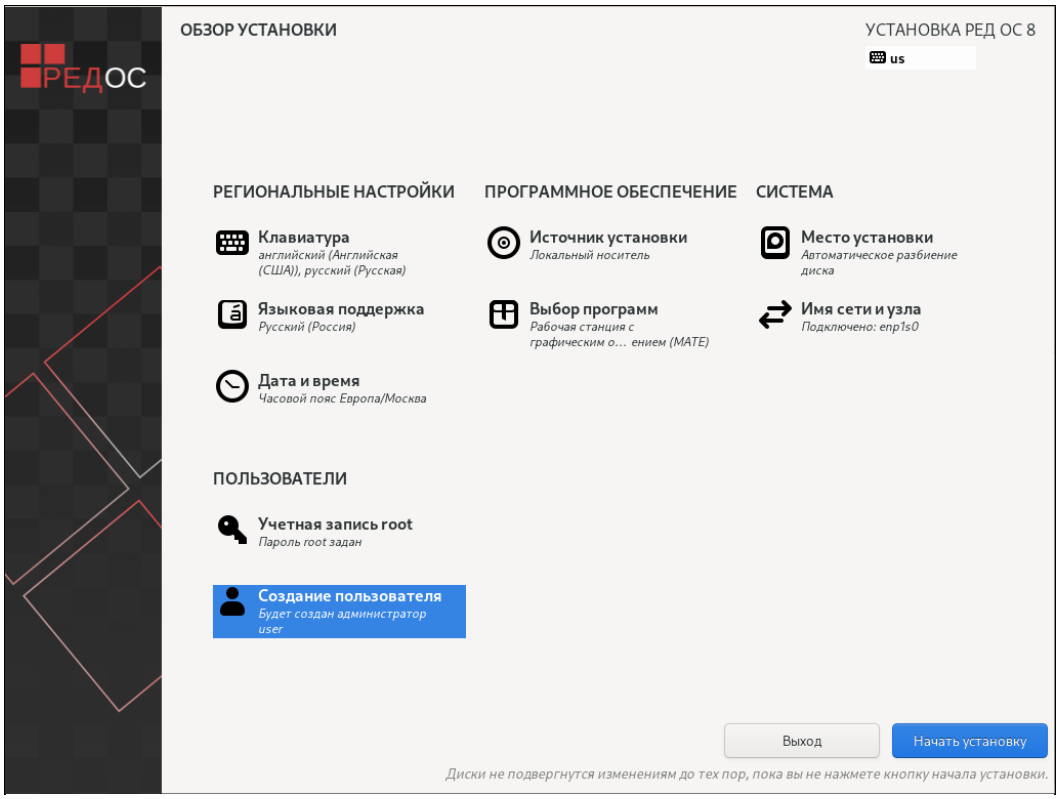
На данном этапе необходимо задать имя компьютера в сети (хоста). При наличии сети имя компьютера используется для однозначного определения каждого компьютера. Имя компьютера состоит непосредственно из имени компьютера и имени домена в сети, к которому принадлежит компьютер. Имя компьютера и имя домена разделяются знаком «.» . При наличии домена сети имя должно даваться полностью. При отсутствии сети домену также может быть дано произвольное имя.

В качестве букв в имени компьютера разрешаются только буквы латиницы. В имени компьютера не допускается использование заглавных букв, пробелов и специальных символов.

Также на данном этапе можно сконфигурировать параметры настройки сетевых интерфейсов: автоматическое включение интерфейсов, MAC-адреса сетевых интерфейсов, параметры сетевых протоколов.

Создание пароля администратора

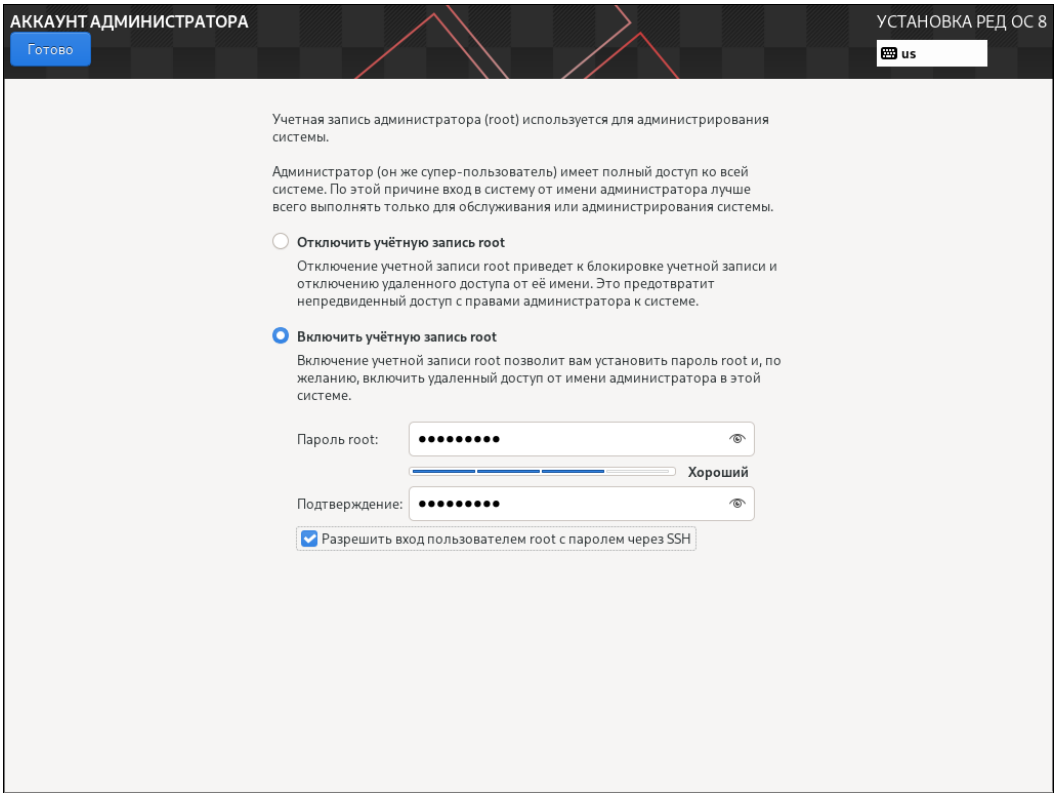
После того как предварительная настройка системы завершена, начинается непосредственная установка системы. Параллельно с установкой необходимо настроить пароль администратора **root** и, при необходимости, создать учетные записи пользователей.



РЕД ОС - это многопользовательская операционная система. На практике это означает, что для работы в системе нужно в ней *зарегистрироваться*, т.е. дать понять системе, кто именно находится за монитором и клавиатурой. Наиболее распространённый способ регистрации на сегодняшний день - использование системных имён (**login name**) и паролей. Это надёжное средство убедиться, что с системой работает тот, кто нужно, если пользователи хранят свои пароли в секрете и если пароль достаточно сложен и не слишком короток (иначе его легко угадать или подобрать).

В любой системе Linux всегда присутствует один специальный пользователь - администратор, он же суперпользователь или администратор РЕД ОС, для него зарезервировано стандартное системное имя - **root**.

Необходимо запомнить пароль **root** - его нужно будет вводить, чтобы получить право изменять настройки системы с помощью стандартных средств настройки РЕД ОС.

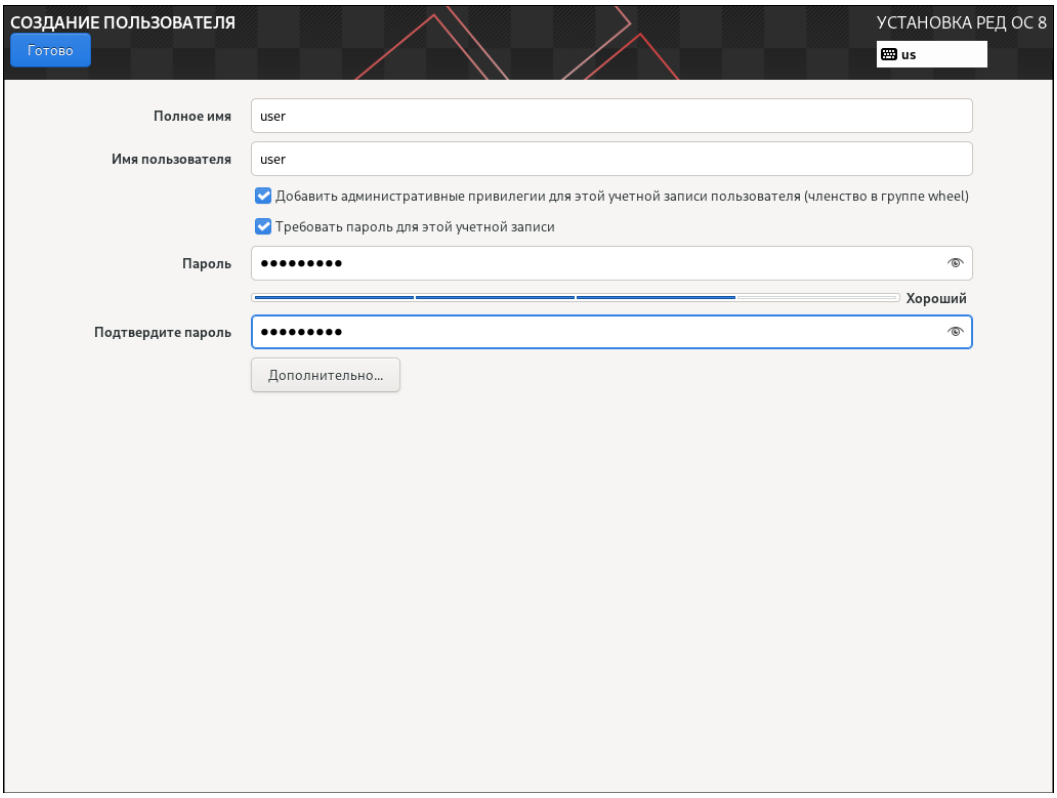


Ввод пароля защищен, при наборе пароля вместо символов на экране отображаются специальные символы. Чтобы избежать опечатки при вводе пароля, его предлагается ввести дважды. К введенному паролю в режиме реального времени применяется политика сложности пароля, т.е. производится его проверка, и при слишком простом пароле или совпадении пароля с парольной последовательностью из словаря паролей системой будет предложено произвести смену пароля администратора РЕД ОС.

Администратор отличается от всех прочих пользователей тем, что ему позволено производить любые, в том числе самые разрушительные, изменения в системе. Поэтому выбор пароля администратора РЕД ОС - очень важный момент для безопасности: любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе. Даже ваши собственные неосторожные действия от имени **root** могут иметь катастрофические последствия для всей системы.

Помимо администратора РЕД ОС (**root**) в систему необходимо добавить, по меньшей мере, одного обычного пользователя. Работа от имени администратора РЕД ОС считается опасной (можно по неосторожности повредить систему), поэтому повседневную работу в РЕД ОС следует выполнять от имени обычного пользователя, полномочия которого ограничены.

При добавлении пользователя предлагается ввести имя учётной записи (login name) пользователя. Имя учётной записи всегда представляет собой одно слово, состоящее только из строчных латинских букв (заглавные запрещены), цифр и символа подчёркивания «_» (причём цифра и символ «_» не могут стоять в начале слова). Чтобы исключить опечатки, пароль пользователя вводится дважды. Так же, как при выборе пароля администратора РЕД ОС (**root**), действуют требования по сложности пароля.



В процессе установки предлагается создать только одну учётную запись обычного пользователя - чтобы от его имени системный администратор РЕД ОС мог выполнять задачи, которые не требуют привилегий суперпользователя.

Учётные записи для всех прочих пользователей системы можно будет создать в любой момент после её установки.

Ручная разметка диска

Общая информация
Схемы разметки дисков
Создание разделов, описание интерфейса разметки
Как создать и зачем выделять home?
Разделы swap, boot, home
Пример с размещением home на отдельном диске
Сохранение раздела /home

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический

Общая информация

Прежде чем приступить к разметке дисковой подсистемы при установке ОС, вспомним про устройство файловой системы РЕД ОС.

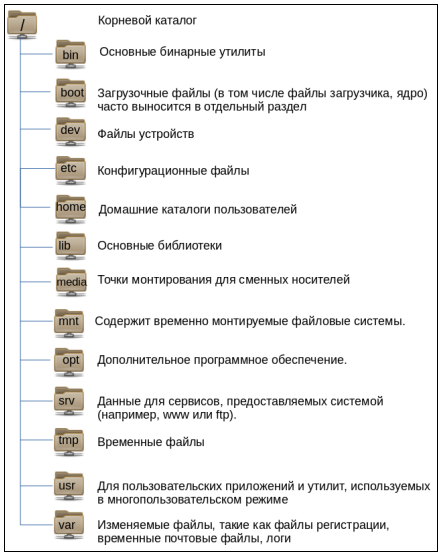


Рисунок 1 - Описание иерархии каталогов

Как мы можем видеть из рисунка, каждый каталог используется под определенные задачи. При установке РЕД ОС в ручном режиме разметки диска можно определенным образом организовать дисковое пространство под ОС, например, для основного корневого раздела **/** , директорий **/home**, **/boot** или **/var** выделить отдельные разделы диска или вообще вынести какой-либо каталог на отдельный диск.

Такое разбиение изолирует их один от другого, что может быть полезным в случае, например, если на домашнем (**/home**) каталоге, вынесенном на отдельный раздел, закончится место, то система все еще сможет нормально работать, потому что это никак не касается корневого раздела. Также, в целях удобства, выделение для **home** отдельного раздела позволит переустановить операционную систему, сохранив пользовательские данные. Таким образом, каталоги могут быть разграничены не только по задачам, но и по своему местонахождению: на разных разделах одного диска или разделах других дисков. Кроме того, ручная разметка дает возможность создавать программный **RAID** и более гибко настраивать файловую подсистему, чем в автоматическом режиме.

Вы можете подробнее ознакомиться с информацией по ручной разметке диска, просмотрев наши обучающие видео:

- на **RuTube** — Ручная разметка диска;
- в **Яндекс.Дзен** — Ручная разметка диска.
- в **VK Видео** — Ручная разметка диска.

На наших каналах вы также сможете найти много другой полезной информации.

Приступаем к разметке диска. В мастере установки ОС выберем жесткие диски для установки РЕД ОС. В нижнем правом углу виден признак количества выбранных дисков. Укажите «**Я настрою разделы**». В результате мы перейдем к ручной разметке дисков.

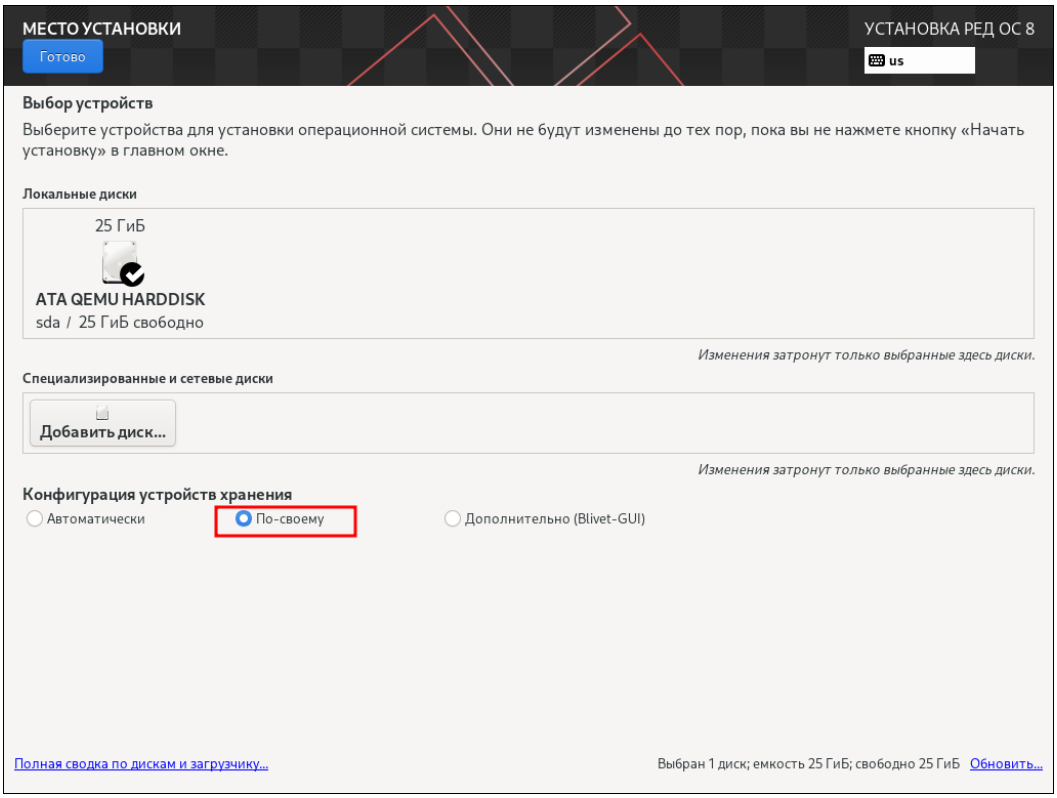


Рисунок 2 — Выбор дисков

На следующем шаге предлагается выбирать схему разбиения диска.

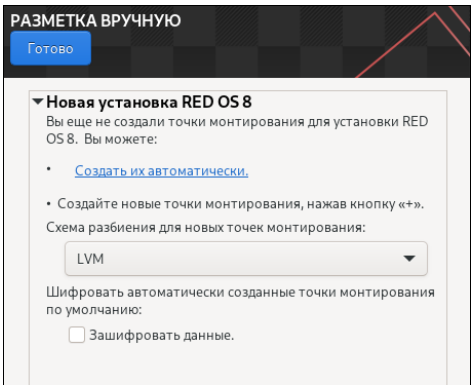


Рисунок 3 — Выбор схемы разбиения диска

Схемы разметки дисков

Стандартный раздел - позволяет создать обычные дисковые разделы, простые в управлении.

Btrfs (можно произносить как «*Butter FS*», «*Better FS*» или «*B-Tree FS*») - файловая система, которая может работать с большим числом файлов, файлами и томами гораздо большего размера, по сравнению с **ext2**, **ext3** и **ext4**, имеется поддержка снапшотов, сжатие и подтома.

Минусы: хотя **btrfs** активно развивается и перешла уже в статус стабильной, у пользователей все еще встречаются проблемы, приводящие к потере данных, а также высокая подверженность фрагментации.

LVM - позволяет создавать логические группы и тома хранения данных без непосредственной переразметки жесткого диска. Например, если у вас используется несколько жестких дисков, то при использовании LVM-разметки можно создать несколько или одну логическую группу, а в ней уже логические тома, которые в дальнейшем можно разбить на разделы и отформатировать под необходимую вам файловую систему — **ext4**, **ext3**, **ntfs** и другие.

Возможности:

- способность объединять диски в один логический том;
- изменение размера файловых систем, легкость при добавлении дисков в то время, когда система активна;
- использование RAID (чередование и зеркалирование);
- поддержка моментальных снимков;

Недостатки:

- сложность управления (предъявляются довольно высокие требования по администрированию файловой системы);
- трудный процесс восстановления данных в случае сбоя LVM из-за более сложных структур на диске;
- снимки сложны в использовании, медленны и содержат ошибки.

Динамический LVM - перераспределяет свободное пространство между устройствами в зависимости от требований программ и при необходимости пул пространства может наращиваться динамически.

Пример схемы LVM-разметки 4-х физических дисков, из которых, в свою очередь, создаются два физических тома, а из них одна большая логическая группа объемом, равным объему всех физ. дисков. В дальнейшем из группы VG создаются логические тома с точками монтирования см. Рисунок 4.

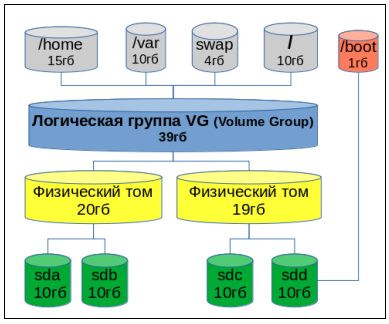


Рисунок 4 - Пример LVM-разметки дисков

Создание разделов, описание интерфейса разметки

Выберем схему со стандартной разметкой диска, которая является более простой, как в плане понимания, так и в сопровождении по сравнению с LVM.

Для обычных пользователей РЕД ОС рекомендуем создавать следующие разделы:

- **swap** (раздел для подкачки ОЗУ);
- **/boot** (загрузочный раздел);
- **/home** (данные пользователей);
- **/** (корневой раздел).

Выбираем схему разбиения «**Стандартный раздел**»,

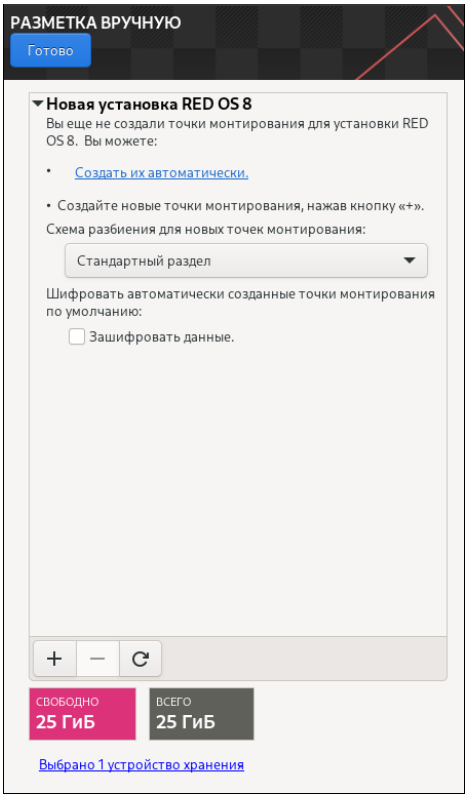


Рисунок 5 - Схема разбиения

далее можно создать все разделы вручную — кнопка плюс (**+**), кнопка минус (**-**) удаляет выбранный раздел.

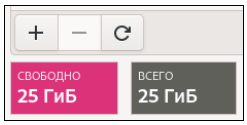


Рисунок 6 - Добавление разделов

Но если нажать на кнопку «**Создать их автоматически**», то в результате будут созданы все необходимые разделы для установки ОС: **boot**, **swap**, **/** и нам не придется их создавать, а останется выделить только раздел **/home** для домашнего каталога.

Как создать и зачем выделять home?

Как видим, корневой раздел / самый большой, поэтому возьмем от него часть для домашнего раздела **/home**. Уменьшаем размер, указав в окне «**Требуемый размер**» размер раздела, указываем меньше, чем сейчас есть, нажимаем кнопку «**Применить**». Заметим, при разметке диска нужно учитывать, что и для корневого раздела нужно оставить свободное место, минимально допустимый размер для корня / - не менее 10 ГБ.

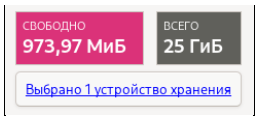
Далее нажмите на плюс (+), выберите точку монтирования **/home**, размер оставляем пустым (но можно и указать необходимый). Таким образом, под **/home** выделится все остальное свободное место, которое мы забрали у корневого **/**. Тип файловой системы оставим по умолчанию — **ext4**, как более технологически продвинутую, но также в окне инсталлятора представлены и другие файловые системы.

Рисунок 7.1 — Стандартная разметка диска

Рисунок 7.2 — Стандартная разметка диска

Другие параметры диалога разметки диска:

- Точка монтирования: указывается директория для подключения будущего раздела;
- Требуемый размер: указывается размер раздела;
- Устройство: выбирается физическое устройство, на котором будет располагаться раздел;
- Тип устройства: стандартный раздел, LVM, динамический LVM, RAID, btrfs;
- Файловая система: выбирается файловая система для раздела;
- Метка: назначается имя разделу под понятным вам именем, не обязательный параметр;
- Имя: имя раздела;
- В нижнем левом углу показывается оставшееся свободное и израсходованное место под разметку.



Разделы swap, boot, home

Рассмотрим для чего предназначен каждый из созданных разделов.

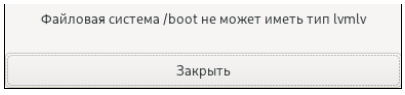
Раздел swap используется для поддержки виртуальной памяти. Данные попадают в раздел подкачки, когда системе не хватает оперативной памяти для их обработки.

Размер раздела для **swap** - минимум половина от ОЗУ, это если пользователь не собирается использовать режим глубокого сна (гибернации). При гибернации вся оперативная память перемещается в **swap**, в этом случае его размер должен быть не меньше размера оперативной памяти!

Раздел /boot содержит ядро операционной системы и файлы начальной загрузки **grub2** 1024 МБ (1 ГБ) будет достаточно для данного раздела. Раздел **boot** лучше создать вне группы томов, а создавать его как отдельный стандартный раздел.

Ряд ограничений, по которым **boot** выделяется в отдельный стандартный раздел:

- раздел **boot** не может располагаться на шифрованных разделах;
- раздел **boot** не может находиться на разделах, файловая система которых не поддерживается загрузчиком **grub2**;
- загрузчик быстрее обнаружит свои файлы, если они находятся на небольшом разделе в начале диска;
- файловая система раздела **/boot** не может иметь тип LVM (для случая, когда используется LVM-разметка диска).



Раздел /home используется для хранения профилей пользователя, настроек рабочего окружения и документов. Как мы уже говорили, выделение отдельного раздела для каталога **/home** позволяет отделить пространство хранения пользовательских данных от

системных. Пользовательские данные, размещенные на отдельном разделе, не пострадают при переустановке системы, а также надежнее защищены от ошибок пользователя во время переноса данных. При переполнении домашнего каталога видео, музыкой и прочим, это не скажется на работе системы в целом, как если бы **home** был на одном разделе с корневой файловой системой, в результате чего закончилось бы все дисковое пространство.

В корневом разделе / будут находиться все системные файлы и к нему будут монтироваться (подключаться) все выше созданные разделы. Минимальный рекомендуемый размер раздела - **10 ГБ**.

Пример с размещением home на отдельном диске

Если в компьютере имеется несколько жестких дисков, то для надежности и, в дальнейшем, простоты администрирования можно, например, точку монтирования **/home** разместить на **отдельном диске**, тем самым изолировав ее от основной файловой системы. Давайте разместим каталог пользователя (**home**) на диске sdb, размер которого в нашем примере 10 Гб. Это легко сделать, выбрав для точки монтирования **/home** нужный диск. Раздел «**Устройство**» - «**Изменить**». Для сохранения настроек нажмите «**Применить**».

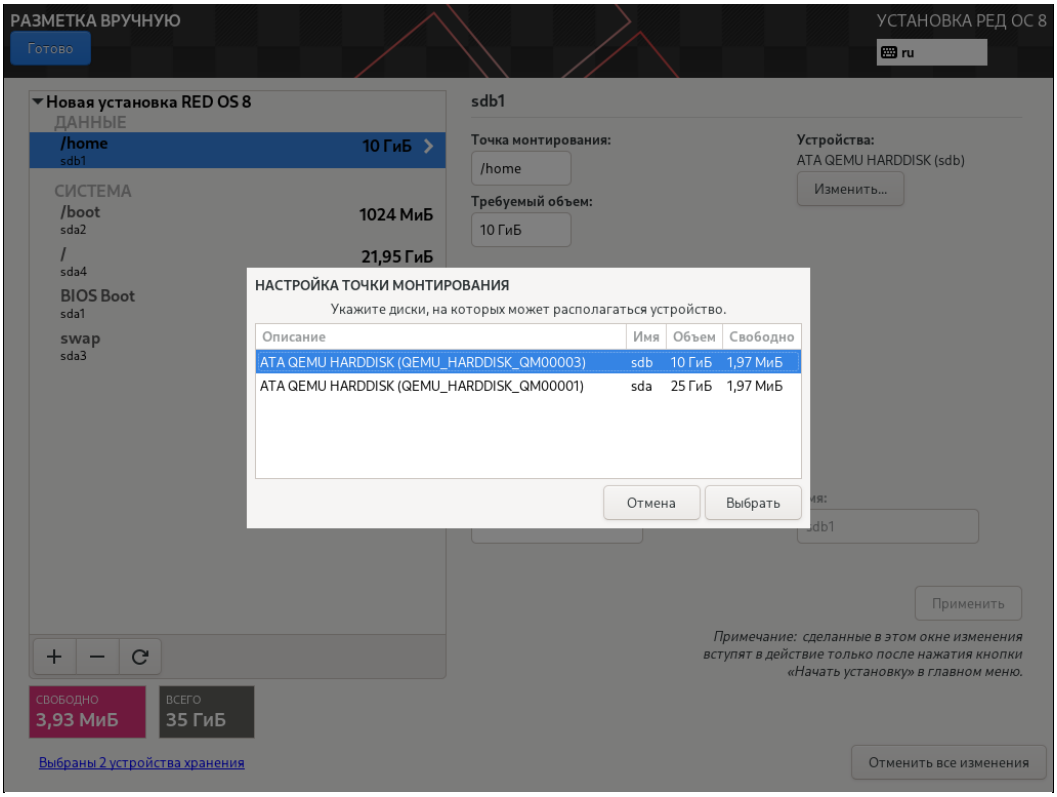
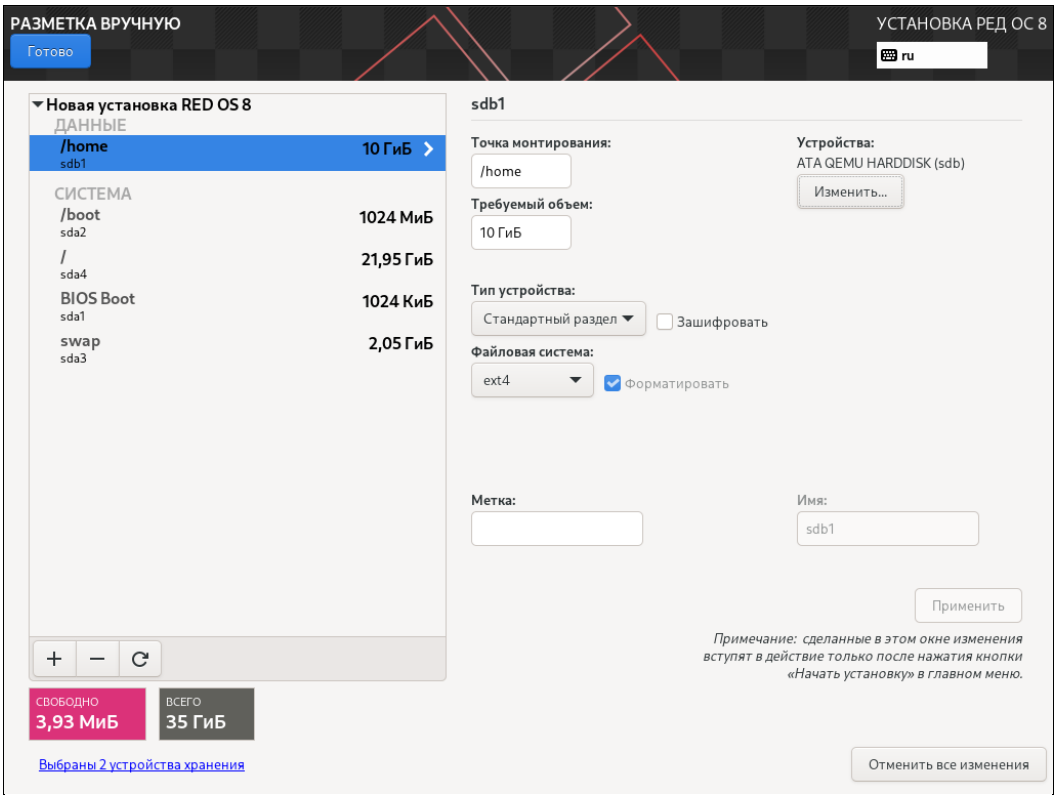


Рисунок 8 — Выбранные диски

Таким образом, под **/home** (домашний каталог профилей пользователей) был выделен отдельный физический диск **sdb** размером **10 Гб**. Остальные разделы **boot** (sda1), **swap** (sda3) и корень (sda2) мы разместили на другом физическом диске **sda** размером **25 Гб**.

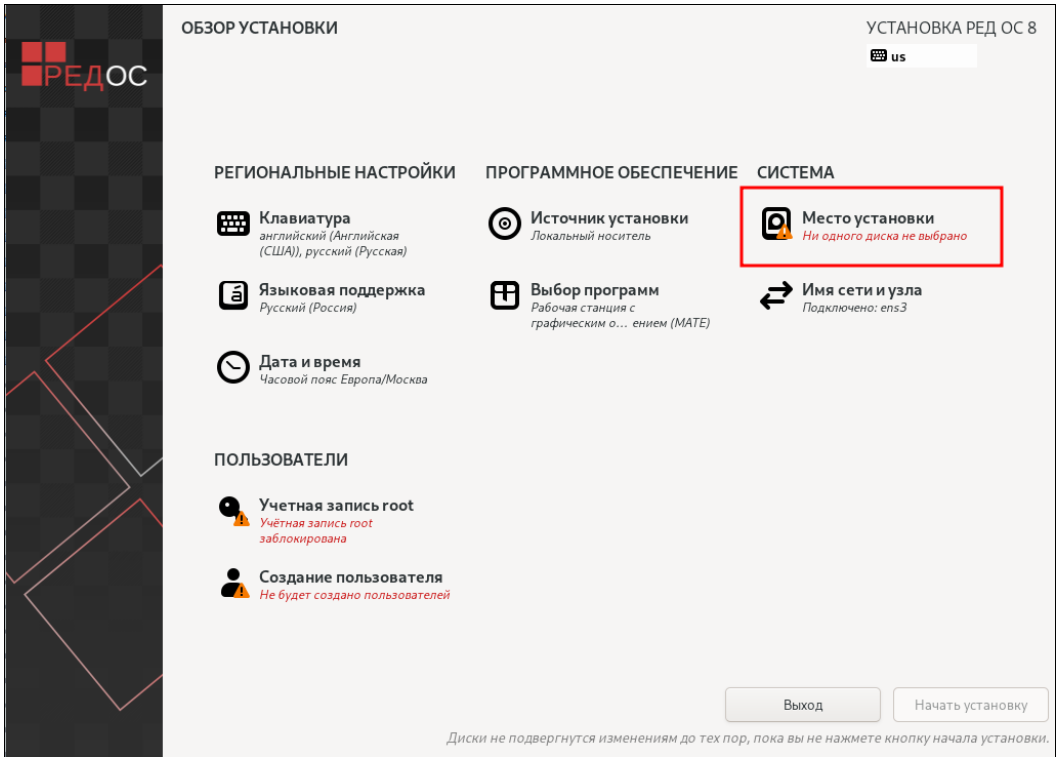


Нажимаем на кнопку «**Готово**» и приступаем к дальнейшим шагам установки РЕД ОС.

Сохранение раздела /home

Далее рассмотрим порядок настройки диска для сохранения (без изменения или удаления) домашнего раздела (**/home**) при переустановке РЕД ОС.

Запустите новую установку РЕД ОС, в мастере установки ОС перейдите в пункт «**Место установки**». Выберите конфигурацию для разметки диска «**По-своему**».

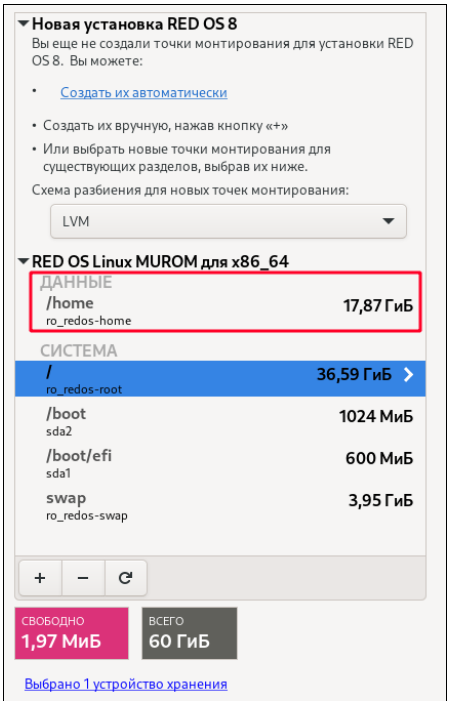


Убедитесь, что на диске присутствует отдельный раздел **/home**.

Примечание.

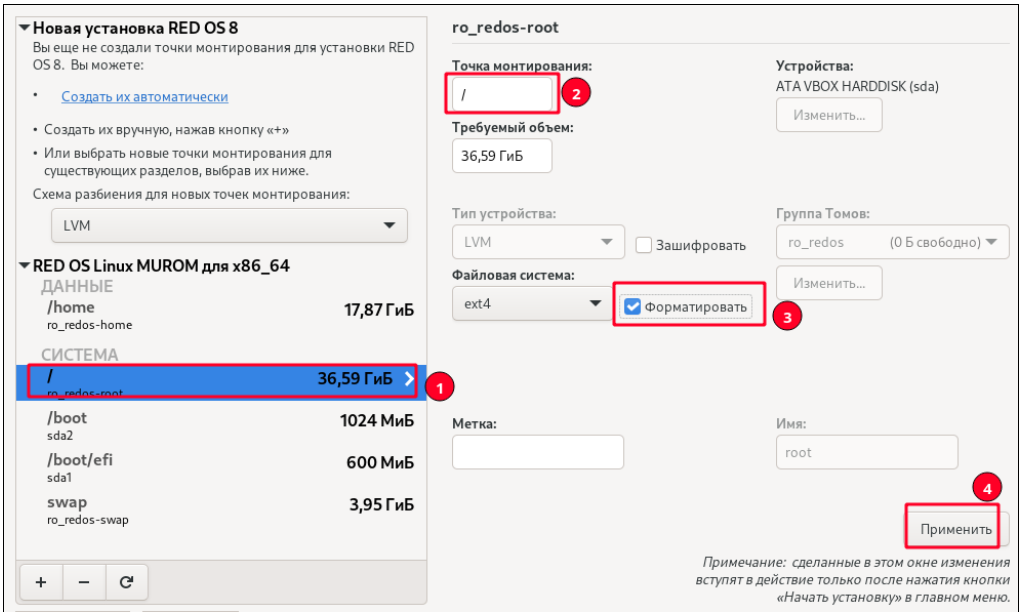
Данный раздел может отсутствовать, если ранее ОС установили с использованием автоматической разметки на жесткий диск,

размер которого был **менее 50 ГБ**, в этом варианте домашний каталог (**/home**) размещается в корневом разделе (/), а не на отдельном. В результате при переустановке ОС корневой раздел будет неизбежно отформатирован вместе с домашним каталогом пользователя. В этом случае, перед установкой необходимо сделать резервную копию **/home** и после установки ОС восстановить данные.



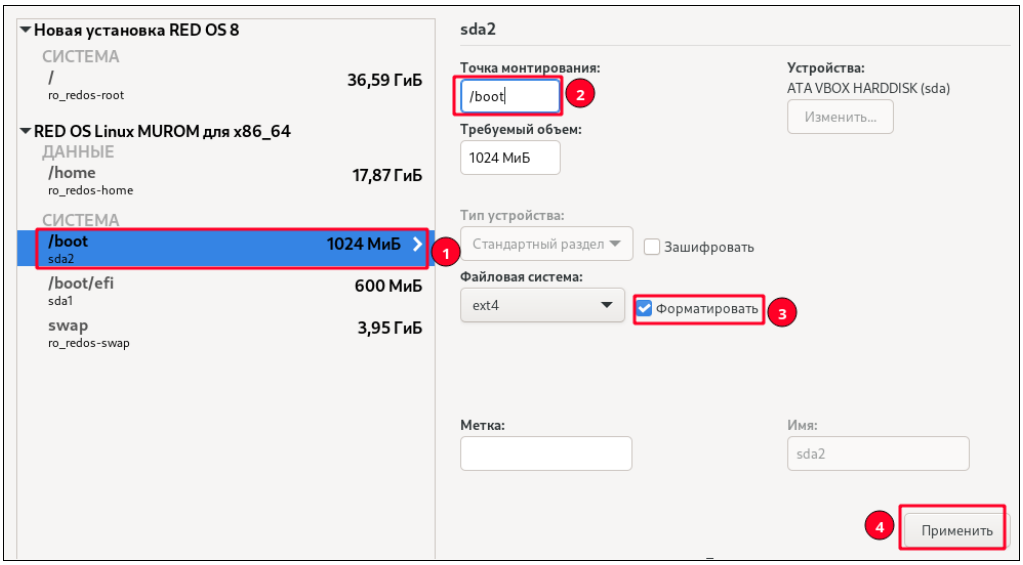
Именно этот раздел (**/home**), содержащий профили пользователей с их данными, **не будет отформатирован**. Остальные разделы необходимо настроить.

Для корневого раздела укажите точку монтирования «**/**», файловую систему **ext4**, а также установите флаг «**Форматировать**», далее нажмите кнопку «**Применить**».

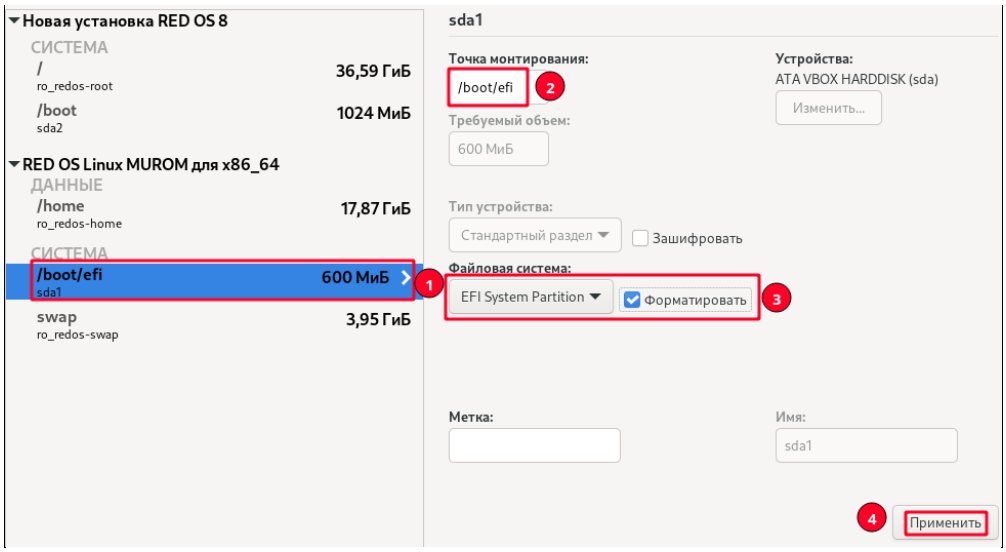


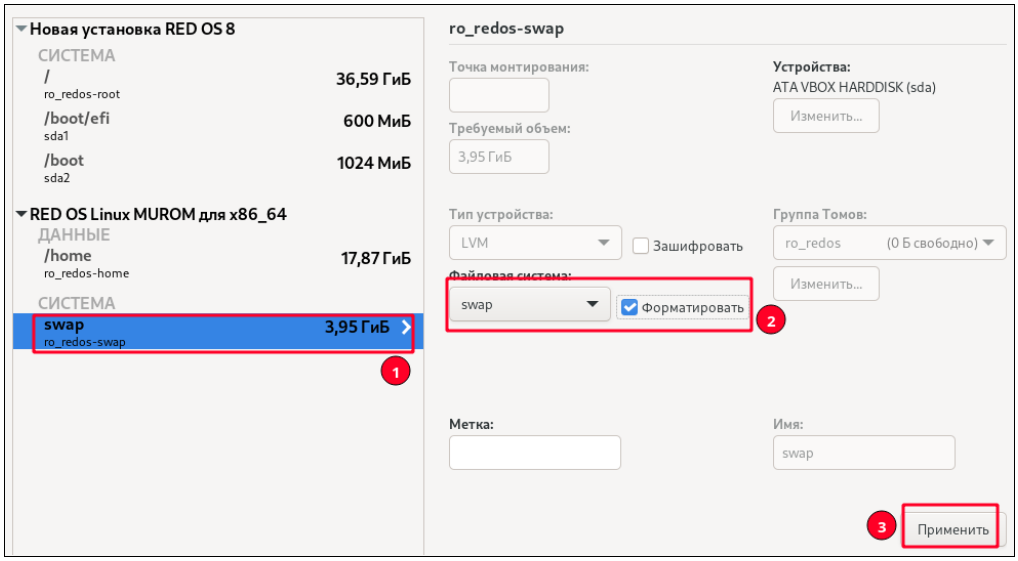
Результат изменения появится в разделе «**Новая установка RED OS 8**».

Следующим шагом выберите раздел **/boot** и присвойте ему точку монтирования **/boot**, файловую систему **ext4** и установите флаг «**Форматировать**», нажмите «**Применить**».



Аналогичные действия выполните для раздела **/boot/efi** и **swap** так, как это показано на нижеприведенных рисунках.





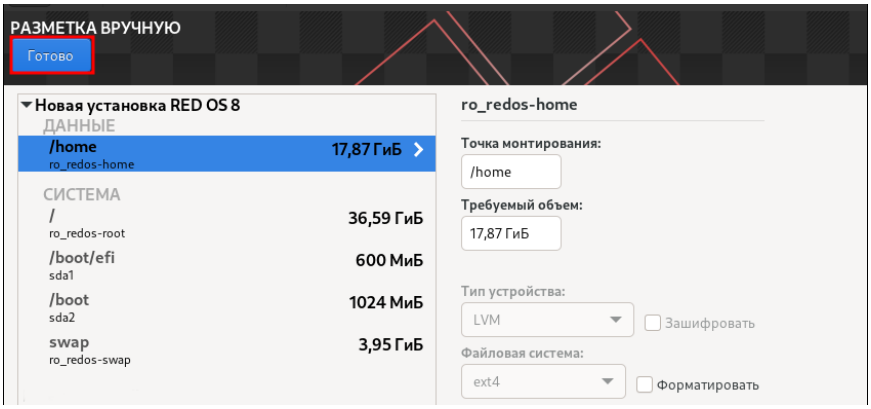
ВАЖНО!

Остался раздел, на котором ранее был размещен **/home**. Для него укажите точку монтирования **/home**, но флаг «**Форматировать**» не устанавливайте. Нажмите кнопку «**Применить**».

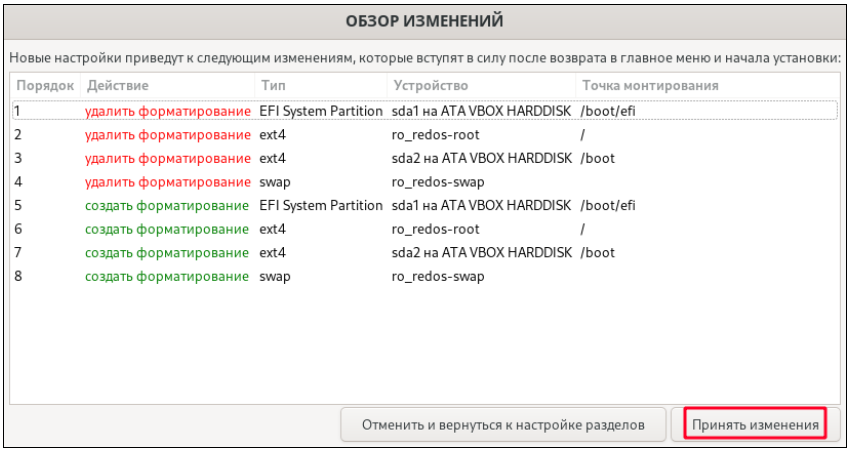
Готовая конфигурация разметки диска показана на рисунке ниже.

Обратите внимание, что для раздела **/home** не был установлен признак форматирования. Но для корневого раздела (**/**), а также для

/boot/efi, **/boot** и **swap** признак «**Форматировать**» был присвоен, т.е. все данные перед установкой на этих разделах будет удалены. Нажмите на кнопку «**Готово**» для продолжения.



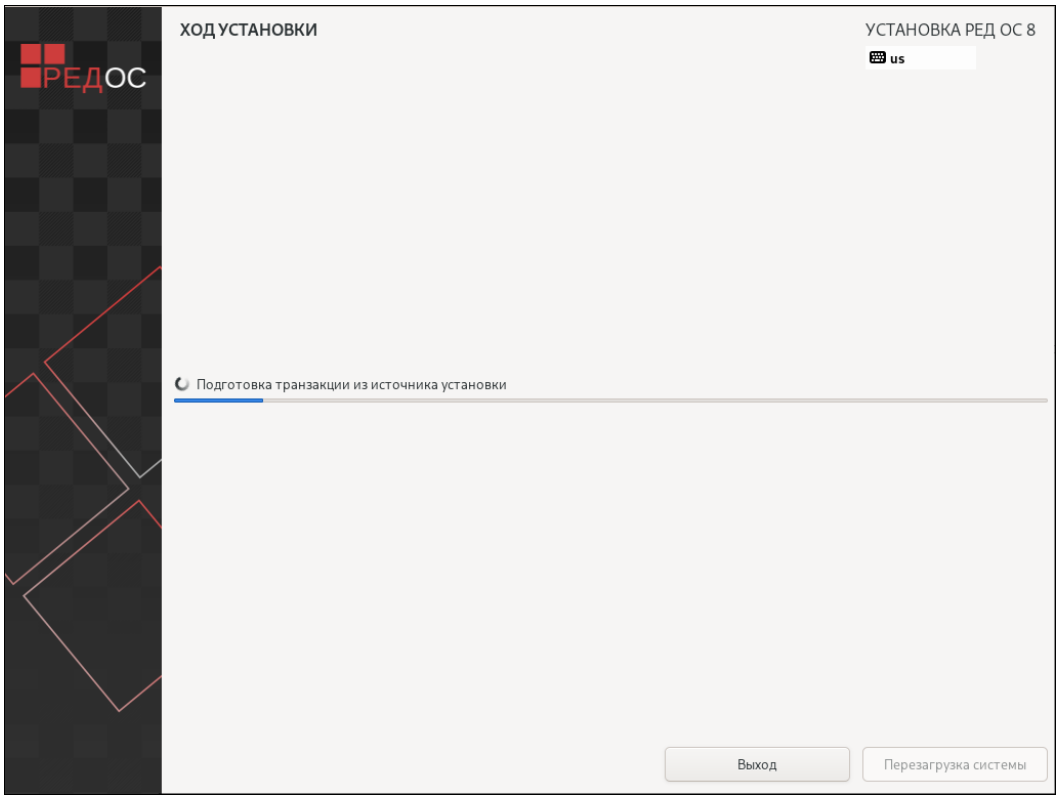
В результате появится итоговая таблица изменений, которые будут выполнены перед установкой ОС.



Примените изменения и продолжите настройку других параметров для установки РЕД ОС.

Установка системы

Этап установки представляет собой установку набора программ, необходимых для работы системы.



Получение пакетов осуществляется с источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу **FTP** и/или **HTTP**) время выполнения этого шага будет зависеть от скорости соединения и может быть значительно большим, чем при установке с дистрибутивного DVD-диска.

Начиная с этого шага, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включённых в дистрибутив.

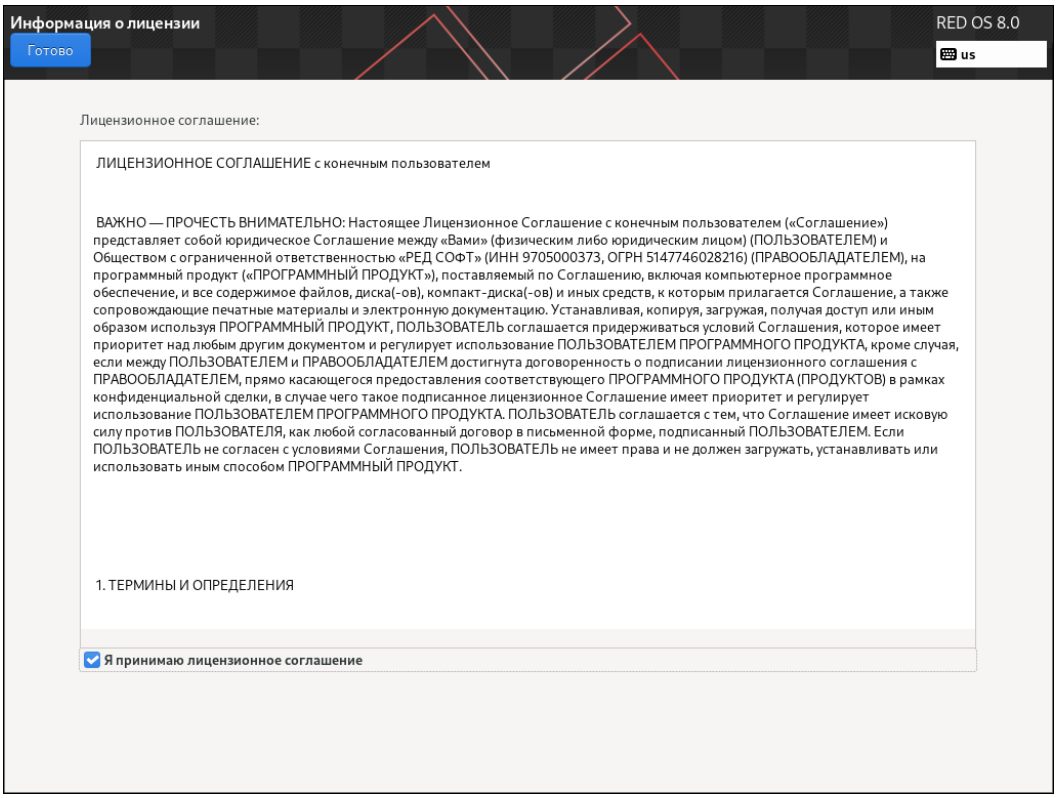
Загрузчик Linux — программа, которая позволяет загружать Linux и другие операционные системы. При автоматическом разбиении разделов накопителя на жестких дисках средства вычислительной техники загрузчик автоматически устанавливается в начальный раздел диска.

Если же планируется использовать и другие операционные системы, уже установленные на этом компьютере, тогда имеет значение, на каком жестком диске или разделе будет расположен загрузчик. В большинстве случаев программа установки правильно подберет расположение загрузчика.

После выполнения копирования файлов РЕД ОС и установки загрузчика пользователю предлагается произвести перезагрузку РЕД ОС кнопкой «**Перезагрузить**».

Соглашение пользователя и Лицензионный договор

После успешной перезагрузки и перед продолжением установки следует внимательно прочитать условия пользовательского соглашения.



В лицензии говорится о правах распространения и гарантиях производителя.

При приобретении дистрибутива данное лицензионное соглашение прилагается в печатном виде к копии дистрибутива на вкладыше комплекта дистрибутива. Лицензия относится ко всему дистрибутиву РЕД ОС.

Завершение установки

После сохранения настроек и перезапуска системы пользователю предоставляется экран приветствия и приглашения к авторизации. На этом установка и настройка РЕД ОС завершена, и РЕД ОС полностью готова к использованию.

Действия после установки ОС

После установки РЕД ОС не все функции безопасности включены по умолчанию. Администратор должен определить функциональную роль установленной копии ОС, перечень решаемых задач, и, в соответствии с действующими политиками безопасности организации, произвести активацию необходимых служб, сервисов и приложений. А именно:

- сконфигурировать перечень отслеживаемых событий безопасности;
- настроить действия в случае обнаружения критически важных событий безопасности;
- настроить действия для предотвращения потери данных аудита;
- настроить защищенную передачу данных аудита;
- создать необходимое количество пользователей, групп, ролей и связать пользователей с группами и ролями, исходя из необходимых им полномочий;
- установить права доступа на создаваемые вновь каталоги и файлы;
- определить правила установки программ и правила запуска компонентов программного обеспечения;
- определить и настроить используемые механизмы идентификации и аутентификации, сроки действия учетных записей и паролей, требования, предъявляемые к аутентификационным данным;
- создать необходимые резервные копии данных и системных настроек и проводить периодическое их тестирование;
- настроить доверенные сервера точного времени;
- проверить целостность важных данных и системных файлов;
- организовать отказоустойчивый кластер при необходимости обеспечения повышенной отказоустойчивости;
- определить квоты и приоритеты, выделяемые пользователям;
- установить необходимые ограничения на сеансы пользователей;
- установить продолжительность бездействия пользовательского сеанса, после которого сеанс будет заблокирован или завершен.

Общие понятия

Для штатной установки дистрибутива РЕД ОС используется загрузочный оптический носитель информации - DVD-диск из комплекта поставки дистрибутива РЕД ОС.

Установка с оптического носителя информации (DVD-диска) - это лишь один из возможных способов установки РЕД ОС. Он подходит для большинства случаев, но не работает, например, в случае отсутствия на компьютере накопителя на оптических носителях информации - DVD-привода. Для таких случаев поддерживаются альтернативные методы установки. Важно понимать, что для начала установки необходимо иметь две вещи: возможность загрузить компьютер и доступ к установочным файлам. В случае установочного дистрибутивного DVD-диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все необходимые для установки файлы. Однако вполне допустим и такой вариант: первоначальная загрузка происходит со специально подготовленного flash-диска, а установочные файлы берутся с FTP-сервера сети.

Таким образом, для установки дистрибутива необходимо:

- Выбрать способ первоначальной загрузки компьютера;
- Выбрать источник установки.

Для загрузки компьютера с целью установки операционной системы необходимо воспользоваться носителем, содержащим начальный загрузчик. Таким носителем может быть, как сам загрузочный оптический диск, так и, например, flash-накопитель, который можно сделать загрузочным, воспользовавшись одним из способов, описанных в нашей статье «Создание загрузочных носителей».

После первоначальной загрузки с одного из поддерживаемых носителей можно выбрать *источник установки* - место, откуда программа установки будет брать все необходимые при установке данные (прежде всего, устанавливаемое ПО). Так как установка системы возможна не только с лазерного диска, то можно выбрать один из поддерживаемых альтернативных источников установки.

Источники установки:

- Сетевые:
  - FTP-сервер;
  - NFS-сервер;
  - HTTP-сервер.

- Локальные:
  - Загрузочный флеш-диск.

Условием для всех способов установки является доступность дерева файлов, аналогичного содержимому установочного диска.

Установка РЕД ОС в текстовом режиме

Установка в текстовом режиме предлагает интерактивный, не графический интерфейс для установки РЕД ОС. Это может быть полезно в системах без графических возможностей. Однако необходимо учитывать ограничения, накладываемые на текстовый режим, и рассмотреть иные доступные альтернативы перед началом текстовой установки.

Для установки РЕД ОС в текстовом режиме необходимо:

1. После появления загрузчика инсталлятора (Рисунок 1) выбрать пункт меню «Установить RED OS» и нажать *«TAB»* на клавиатуре.

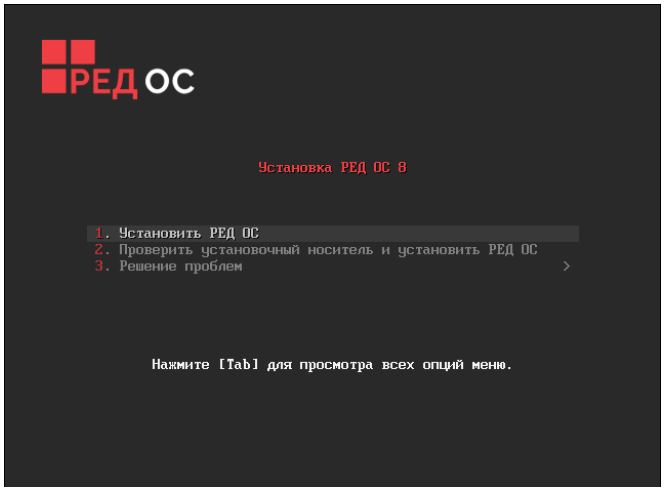


Рисунок 1 – Стартовое окно установки

2. В появившейся нижней части экрана в командной строке загрузчика (Рисунок 2) добавить текст:

```
inst.text
```

и нажать клавишу *«Enter»*.

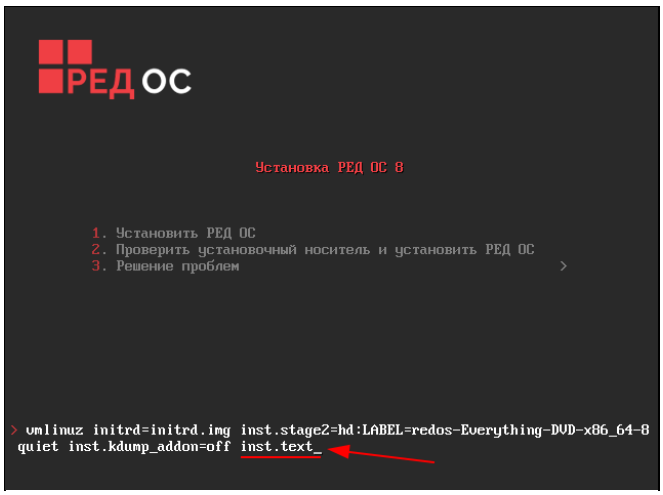


Рисунок 2 – Командная строка загрузчика

Установка в текстовом режиме (Рисунок 3) происходит по схеме, аналогичной графической установке: нет единого фиксированного порядка настройки. Пользователь может настроить все доступные параметры в любом порядке, используя главный экран инсталлятора.



Рисунок 3 – Настройка параметров

Экраны, которые уже были настроены автоматически или корректно настроены самим пользователем, помечаются как **[x]**, а экраны, которые требуют обязательной настройки до начала установки, помечаются как **[!]**. Доступные команды отображаются под списком доступных опций. Выбор пункта меню осуществляется в строке ввода нажатием соответствующей цифровой клавиши.
Например, чтобы в меню, показанном на Рисунке 3, назначить пароль для администратора root, необходимо нажать на клавиатуре последовательно цифру *«7»* и *«Enter»*.
По умолчанию используются следующие клавиши:

- *q* – для выхода из текущего меню;
- *r* – для обновления содержимого;
- *b* – для начала процесса установки в главном меню;
- *c* – для подтверждения действия.

Примечание.
При выполнении связанных фоновых задач некоторые пункты меню могут быть временно недоступны или отображать «Processing...». Чтобы обновить текущее состояние элементов текстового меню, используйте команду «r» в приглашении текстового режима.

В нижней части экрана в текстовом режиме (Рисунок 3) отображается зеленая полоса с пятью вариантами меню. Эти параметры представляют собой различные экраны в мультиплексоре терминала **tmux** (по умолчанию пользователь запускается на экране 1). Пользователь может использовать сочетания клавиш для переключения на другие экраны, которые содержат журналы и интерактивную командную строку.

ВАЖНО!

Ограничения установки интерактивного текстового режима включают в себя:

- установщик всегда будет использовать английский язык и английскую раскладку клавиатуры. Пользователь может настроить язык и параметры клавиатуры, но эти параметры будут применяться только к установленной системе, а не к самой установке;
- пользователь не может настроить какие-либо расширенные методы хранения (LVM, программный RAID, FCoE, zFCP и iSCSI);
- настроить пользовательское разбиение на разделы невозможно – необходимо использовать один из параметров автоматического разбиения на разделы. Пользователю также недоступна настройка места, куда будет установлен загрузчик;
- пользователь не может установить дополнительные пакеты, они должны быть добавлены после завершения установки с помощью диспетчера пакетов DNF.

Для конфигураций "Рабочая станция" и "Сервер с графикой", после полного завершения установки ОС и входа под пользователем в терминальном режиме требуется выполнить команду:

```
systemctl set-default graphical.target
```

И выполните перезагрузку:

```
reboot
```

Обзорная инструкция про RAID

Определение RAID
Виды RAID. RAID 0
Виды RAID. RAID 1
Виды RAID. RAID 2
Виды RAID. RAID 5
Виды RAID. RAID 6
Виды RAID. RAID 10
Аппаратные RAID-контроллеры
Программный RAID

Определение RAID

RAID — это дисковый массив из нескольких жестких дисков. Он используется для повышения надежности хранения данных или для увеличения скорости чтения/записи.

Разные типы этих конфигураций как раз и отмечаются разными номерами: **1**, **2**, **3**, **4** и, соответственно, выполняют разные функции.

- **RAID 0** — дисковый массив повышенной производительности с чередованием без отказоустойчивости;
- **RAID 1** — зеркальный дисковый массив;
- **RAID 2** — зарезервирован для массивов, которые применяют код Хемминга;
- **RAID 3** — дисковый массив с выделенным диском чётности;
- **RAID 4** — дисковый массив с чередованием и выделенным диском чётности;
- **RAID 5** — дисковый массив с чередованием, в том числе данных чётности;
- **RAID 6** — дисковый массив с чередованием, использующий две контрольные суммы, вычисляемые двумя независимыми способами;
- **RAID 10** — массив **RAID 0**, построенный из массивов **RAID 1**.

Вы можете подробнее ознакомиться с дисковыми массивами **RAID**, просмотрев наши обучающие видео:

- на **RuTube** — Создание программного RAID массива на РЕД ОС;
- в **Яндекс.Дзен** — Создание программного RAID массива на РЕД ОС;
- в **VK Видео** — Создание программного RAID массива на РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Виды RAID

RAID 0

RAID 0 (чередование дисков) — на данном уровне задействован процесс разделения массива данных на блоки с последующим их распределением по нескольким устройствам хранения, объединенных в одну совокупную группу. Блоки распределяются последовательно и содержат каждый свою часть данных на отдельном диске.

Распределение данных в RAID-массиве нулевого уровня происходит без данных четности и не имеет избыточности или отказоустойчивости. Это означает, что в случае сбоя какого-то одного диска происходит разрушение всего дискового массива, и восстановить информацию в полном объеме не получится без использования данных с неисправного накопителя.

Системы хранения выполняют чередование дисков по-разному. Система может чередовать данные на уровне байтов, блоков или разделов, либо одновременно на всех или отдельных дисках кластера.

RAID 0 лучше всего использовать для хранилища, наличие защиты от потери данных в котором не критично, но требуется поддержка высокоскоростного режима чтения и записи. Например, это могут быть задачи по обработке потокового видео в реальном времени и редактирование файлов медиа-формата, хранение временных данных.

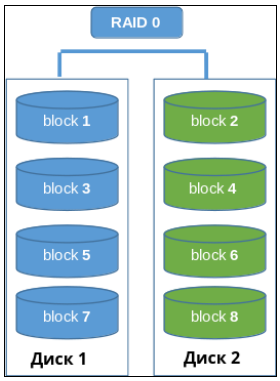
Преимущества **RAID 0**:

- Повышенная производительность чтения и записи;
- Использование полной мощности накопителей;
- Легко реализуется.

Недостатки RAID 0:

- Отсутствует отказоустойчивость.

Наглядная схема **RAID 0** состоящая из двух дисков представлена на рисунке.



RAID 1

RAID 1 — массив из двух (или более) дисков, являющихся полными копиями друг друга. Самая простая система **RAID**-массивов из всех возможных. Представляет собой параллельную запись информации с основного диска на другие — дублирующие. Повышение производительности происходит только при чтении данных, за счёт распараллеливания запросов. Зеркальное копирование дисков особенно полезно для сценариев аварийного восстановления, поскольку обеспечивает мгновенное восстановление требуемых, для критически важных приложений, данных сразу после отказа диска. Если первичные диски в массиве повреждены или не могут быть использованы, произойдет переключение на вторичные или зеркальные резервные диски, обладающие работоспособными копиями, и функционирование приложений, обращающихся к востребованным данным, не будет нарушено.

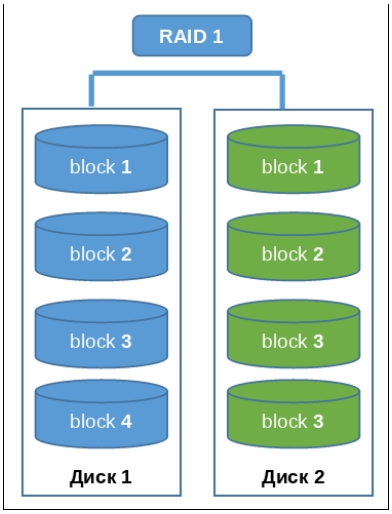
Достоинства:

- Обеспечивает приемлемую скорость записи и выигрыш по скорости чтения при распараллеливании запросов.
- Имеет высокую надёжность — работает до тех пор, пока функционирует хотя бы один диск в массиве. Вероятность выхода из строя сразу двух дисков равна произведению вероятностей отказа каждого диска, то есть значительно ниже вероятности выхода из строя отдельного диска.

Недостатки:

- По цене двух жестких дисков пользователь получает объём одного.

Наглядная схема **RAID 1**.



RAID 2

Массивы такого типа основаны на использовании кода Хэмминга. Но поскольку современные жесткие диски также используют самоконтролирующийся код Хэмминга, то уровень «**RAID 2**» теперь считается устаревшим. Чтобы получить **RAID** данного типа, создаются две группы дисков — одна для хранения данных, другая — для кодов исправления ошибок.

Данный код исправления ошибок позволяет производить анализ данных, которые считываются или пересылаются, и, при необходимости, исправлять их непосредственно во время процесса передачи.

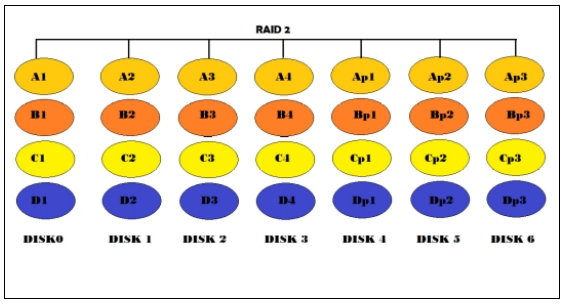
Достоинства:

- Быстрое исправление ошибок, без снижения скорости передачи данных между дисковым массивом и процессором.

Недостатки:

- Минимальное количество дисков 7, только начиная с этого количества для него требуется меньше дисков, чем для **RAID 1** (4 диска с данными, 3 диска с кодами коррекции ошибок), в дальнейшем избыточность уменьшается по экспоненте.

Наглядная схема **RAID 2**.



RAID 5

RAID 5 — дисковый массив с чередованием блоков данных и контролем чётности.

Схож по своему принципу работы с **RAID 1**. Только теперь потребуется минимум 3 накопителя, на одном из которых будет храниться продублированная информация. Избыточный массив конфигурации независимых дисков подобного формата основан в соответствии с принципом чередования на уровне блоков четности. Данные и информация о четности распределяются равномерно по всем дискам, что влечет за собой снижение критичной уязвимости отдельного запоминающего накопителя из организованного объединения, и позволяет массиву «**RAID 5**» функционировать даже в случае сбоя какого-нибудь одного диска, а также даже восстановить данные за счёт чередования, утраченные с проблемного устройства.

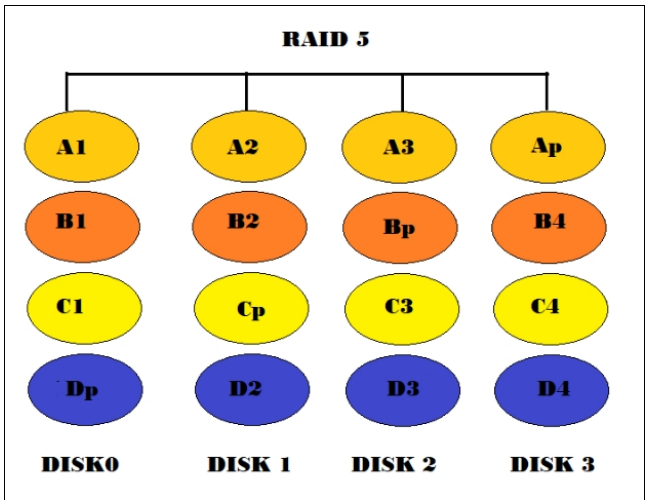
Достоинства:

- **RAID 5** получил широкое распространение, в первую очередь благодаря своей экономичности. С увеличением количества дисков в массиве экономия (по сравнению с другими уровнями **RAID**, обладающими отказоустойчивостью) продолжает увеличиваться.
- **RAID 5** обеспечивает высокую скорость чтения — выигрыш достигается за счёт независимых потоков данных с нескольких дисков массива, которые могут обрабатываться параллельно.

Недостатки:

- Производительность **RAID 5** заметно ниже на операциях записи в произвольном порядке, при которых производительность падает на 10-25 % от производительности **RAID 0** (или **RAID 10**), так как требует большего количества операций с дисками. Каждая операция записи заменяется на контроллере **RAID** на четыре — две операции чтения и две операции записи.

Наглядная схема **RAID 5**.



RAID 6

RAID 6 — массив из четырёх или более дисков, обеспечивающий двойной контроль четности хранимой информации. Разработанный для защиты от потери данных при выходе из строя сразу двух жестких дисков в массиве. За счёт двух дисков избыточности он имеет более высокую степень надёжности. Среди дисковых массивов **RAID 6** — самый надёжный, но и самый медленный. Архитектурное построение «**RAID 6**» представляет собой одну из нескольких схем «**RAID**», которая функционирует, размещая данные на нескольких дисках и позволяя операциям ввода/вывода («I/O») перекрываться сбалансированным образом. Использование дополнительной четности позволяет массиву продолжать свое функционирование, даже если два диска выходят из строя одновременно

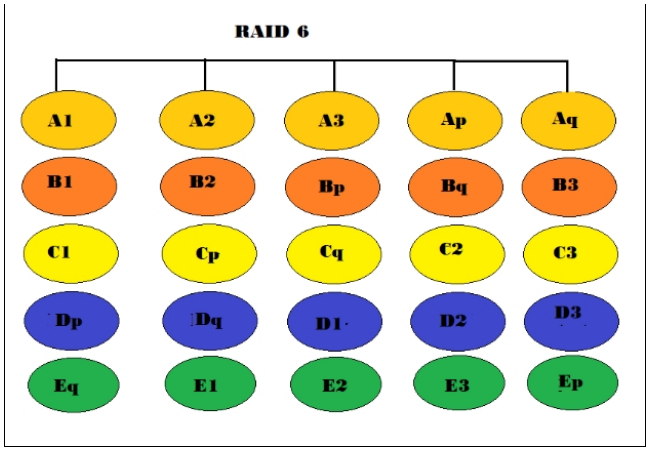
Достоинства:

- Надёжность — она максимальна из всех массивов данных **RAID**.
- Если два диска выйдут из строя, и их придется заменить, вы все равно будете иметь доступ ко всем данным.

Недостатки:

- Отказы дисков влияют на производительность массива;
- Операции записи медленнее, чем в **RAID 5**, из-за дополнительных блоков четности, принимающих участие в вычислениях.

Наглядная схема **RAID 6**.



RAID 10

RAID 10 (RAID 1+0) — зеркалированный массив, данные в котором записываются последовательно на несколько дисков, как в **RAID 0**. Диски вложенного массива объединяются в «зеркала» **RAID 1**. Эти зеркальные пары затем преобразуются в общий массив с использованием чередования **RAID 0**. Вам потребуется минимум 4 носителя, и их количество всегда должно быть четным. В данном массиве вы получаете высокую производительность и высокую надежность. Однако, как в случае и с **RAID 1**, вам будет доступна лишь половина от общего объема всей системы.

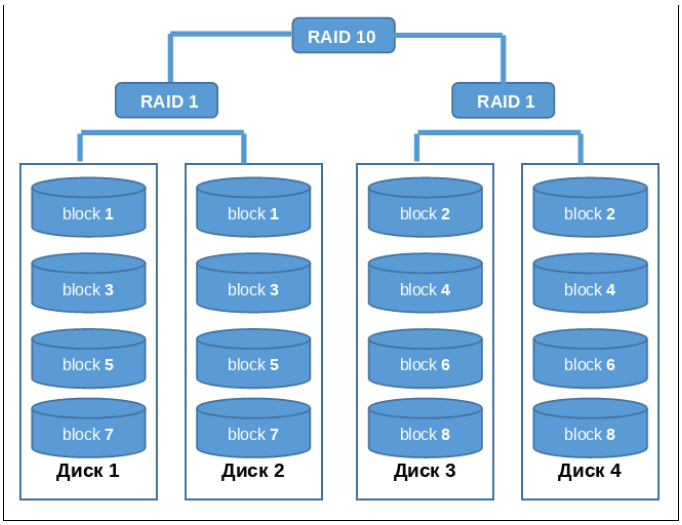
Достоинства:

- **RAID 10** объединяет в себе высокую отказоустойчивость и производительность.
- **RAID 10** является достаточно надёжным вариантом для хранения данных в связи с тем, что весь массив **RAID 10** будет выведен из строя только после выхода из строя всех накопителей в одном и том же массиве **RAID 1**.

Недостатки:

- Эффективность дискового пространства 50%.

Наглядная схема **RAID 10**.



Аппаратные RAID-контроллеры

Представляют собой плату расширения либо размещаются вне сервера (например, в составе внешней дисковой подсистемы либо **NAS**). Имеют собственный процессор, многие имеют кэш-память для ускорения работы. При значительной нагрузке на систему дисков, которая требует от сервера обработки больших объемов данных, может работать только отдельное оборудование **RAID**-контроллера.

Он подключается через разъем **PCI** к материнской плате и самостоятельно решает задачи управления массивом жестких дисков.

Для подключения дисков контроллер может иметь внутренние либо внешние порты, либо и те, и другие.

Контроллеры различных производителей, как правило, не совместимы и не взаимозаменяемы между собой — это следует иметь в виду в случае выхода из строя платы контроллера. Информация о конфигурации **RAID**-массива хранится на дисках, но прочитать её, даже с полностью исправных дисков, и воссоздать массив сможет только контроллер того же производителя. Программные **RAID**-массивы также лишены этого недостатка.

Программный RAID

Дисковый массив, который создается в операционной системе, называется программным **RAID**. Для реализации **RAID** можно применять не только аппаратные средства, но и полностью программные компоненты (драйверы). Управлять **RAID**-устройствами в РЕД ОС можно с помощью утилиты **mdadm**.

Главное преимущество программной реализации — невысокая стоимость.

Недостатки — низкая производительность и постоянная дополнительная нагрузка на процессор.

Получается, программная реализация лучше всего проявляет себя в работе с теми массивами дисков, которые не требуют объемных вычислений.

Создание программного массива уровня RAID0 и RAID1

Подготовка к созданию RAID-массива
Создание программного массива уровня RAID 0
Создание программного массива уровня RAID1
Создание автоматического монтирования RAID 0

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Подготовка к созданию RAID-массива

В примере для создания RAID-массива **нулевого уровня** будем использовать **два диска** объемом **10 Гб**. Описание и особенности работы **RAID0** можно найти по ссылке.

Для выполнения дальнейших действий требуется перейти в сеанс пользователя **root**:

```
su -
```

Для того чтобы посмотреть текущую информацию об устройствах хранения, выполните команду:

```
lsblk
```

```
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   40G  0 disk
├─sda1   8:1    0    1M  0 part
├─sda2   8:2    0    1G  0 part /boot
├─sda3   8:3    0    2G  0 part [SWAP]
└─sda4   8:4    0 36,9G  0 part /
sdb      8:16   0   10G  0 disk
sdc      8:32   0   10G  0 disk
sr0     11:0    1 1024M  0 rom
zram0  252:0    0  1,9G  0 disk [SWAP]
```

Здесь **sdb**, **sdc** – это те диски, которые мы будем использовать для создания **RAID 0**.

Далее необходимо создать разделы на каждом из дисков **sdb** и **sdc**, для этого воспользуемся утилитой fdisk. Создадим таблицу разделов для диска **/dev/sdb**:

```
fdisk /dev/sdb
```

```
[root@localhost ~]# fdisk /dev/sdb

Добро пожаловать в fdisk (util-linux 2.38.1).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.

Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0xa63e8f88.

Команда (m для справки): n
Тип раздела
   p   основной (0 primary, 0 extended, 4 free)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p
Номер раздела (1-4, default 1): 1
Первый сектор (2048-20971519, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-20971519, default 20971519):

Создан новый раздел 1 с типом 'Linux' и размером 10 GiB.

Команда (m для справки): t
Выбранный раздел 1
Hex code or alias (type L to list all): fd
Тип раздела 'Linux' изменен на 'Linux raid autodetect'.

Команда (m для справки): w
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

Последовательность указания ключей **fdisk** при создании разделов и их описание:

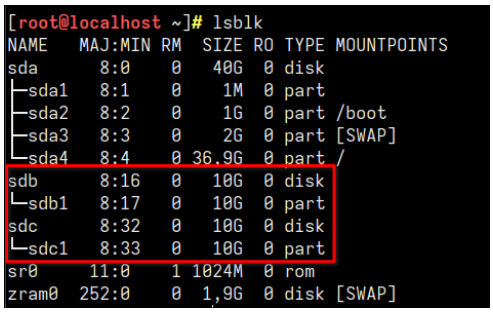
- создание раздела (**n**);
- тип раздела primary (**p**);
- номер раздела (**1**).
- начальный и конечный блоки;
- изменение id раздела (**t**);
- установка id раздела в Linux raid autodetect (**fd**);
- применение изменений и выход (**w**).

Аналогично создаем таблицу разделов для диска **/dev/sdc**.

```
fdisk /dev/sdc
```

Выведем информацию о разделах:

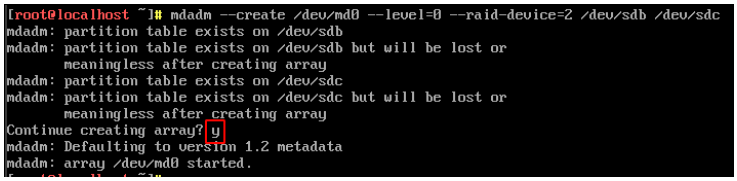
```
lsblk
```



Создание программного массива уровня RAID 0

Для создания программного RAID-массива в РЕД ОС используется утилита mdadm.

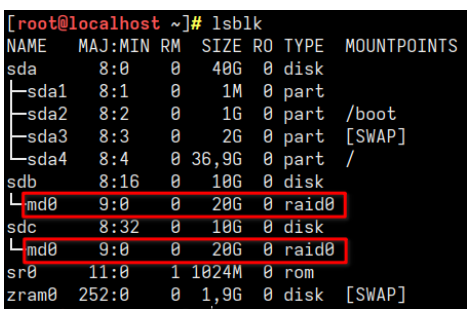
```
mdadm --create /dev/md0 --level=0 --raid-device=2 /dev/sdb /dev/sdc
```



Описание параметров **mdadm**:

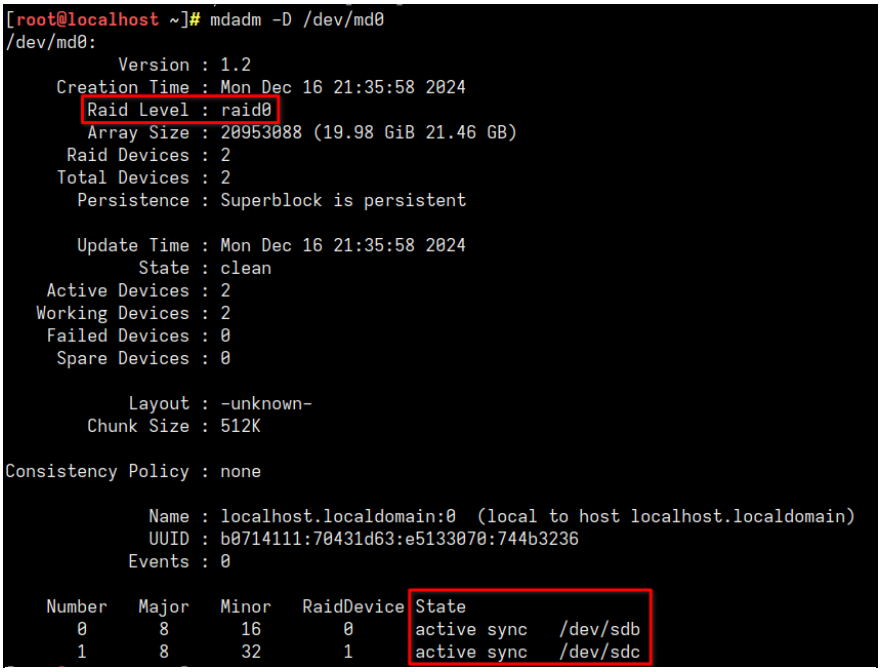
- **/dev/md0** – имя устройства **RAID**;
- **--level=0** – уровень **RAID**;
- **--raid-devices=2** – количество дисков, которые участвуют в сборке **RAID**;
- **/dev/sdb, /dev/sdc** – имена дисков, участвующих в сборке массива.

Снова выполните команду lsblk, теперь в выводе видно, что создано устройство **md0** с типом **RAID0**.



Следующая команда покажет детальную информацию о массиве:

```
mdadm -D /dev/md0
```



Создание программного массива уровня RAID1

Для создания **RAID 1** необходимо выполнить аналогичные действия, которые производились для создания программного массива **RAID 0**, различие лишь в том, что необходимо указать первый класс (**--level=1**) массива данных в параметрах утилиты `mdadm`:

```
mdadm --create /dev/md1 --level=1 --raid-device=2 /dev/sdb /dev/sdc
```

Создание автоматического монтирования RAID 0

Создадим файловую систему **ext4** на RAID-устройстве **/dev/md0** и смонтируем массив в каталог **/mnt/raid0/**.

```
mkfs.ext4 /dev/md0
mkdir /mnt/raid0
mount /dev/md0 /mnt/raid0
ls -l /mnt/raid0/
```

Для автоматического подключения **RAID** добавим запись в конец файла **/etc/fstab**, для этого в терминале выполните команду:

```
echo "/dev/md0 /mnt/raid0 ext4 defaults 0 0" >> /etc/fstab
```

Сохраните конфигурацию **RAID**, чтобы во время загрузки системы происходило ее считывание.

```
mdadm --detail --scan --verbose >> /etc/mdadm.conf
```

Создание программного массива уровня RAID 6

Подготовка к созданию RAID-массива
Создание RAID-массива
Создание автоматического монтирования RAID

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Подготовка к созданию RAID-массива

В данной инструкции рассмотрено создание программного RAID-массива из **4 дисков**, размером в **1 ГБ**. Это минимально возможное количество дисков, которое требуется для создания RAID-массива класса 6.

Для выполнения дальнейших действий требуется перейти в сеанс пользователя **root**:

```
su -
```

Для того чтобы посмотреть текущую информацию об устройствах хранения, выполните команду:

```
lsblk
```

```
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   40G  0 disk
├─sda1   8:1    0    1M  0 part
├─sda2   8:2    0    1G  0 part /boot
├─sda3   8:3    0    2G  0 part [SWAP]
└─sda4   8:4    0 36,9G  0 part /
sdb      8:16   0    1G  0 disk
sdc      8:32   0    1G  0 disk
sdd      8:48   0    1G  0 disk
sde      8:64   0    1G  0 disk
sr0     11:0    1 1024M  0 rom
zram0  252:0    0  1,9G  0 disk [SWAP]
```

Здесь **sdb**, **sdc**, **sdd** и **sde** – диски, из которых будет собран программный **RAID 6**.

Проверим подключенные диски на отсутствие метаданных **RAID**.

```
mdadm -E /dev/sd[b-e]
```

```
[root@localhost ~]# mdadm -E /dev/sd[b-e]
mdadm: No md superblock detected on /dev/sdb.
mdadm: No md superblock detected on /dev/sdc.
mdadm: No md superblock detected on /dev/sdd.
mdadm: No md superblock detected on /dev/sde.
```

Из вывода команды видно, что признаки **RAID** на дисках отсутствуют.

Создадим на каждом диске раздел с помощью следующей команды:

```
fdisk /dev/sdd
```

```
[root@localhost ~]# fdisk /dev/sdd

Добро пожаловать в fdisk (util-linux 2.38.1).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.

Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0xceba92f3.

Команда (m для справки): n
Тип раздела
   p   основной (0 primary, 0 extended, 4 free)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p
Номер раздела (1-4, default 1): 1
Первый сектор (2048-2097151, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-2097151, default 2097151):

Создан новый раздел 1 с типом 'Linux' и размером 1023 MiB.

Команда (m для справки): t
Выбранный раздел 1
Hex code or alias (type L to list all): fd
Тип раздела 'Linux' изменен на 'Linux raid autodetect'.

Команда (m для справки): w
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

В консоли **fdisk** выберите:

- Создание раздела (**n**);
- Тип раздела primary (**p**);
- Номер раздела (**1**).
- Начальный и конечный блоки (**Enter**);
- Для изменения типа раздела (**t**);
- Шестнадцатеричный код (**fd**);
- Применение изменений и выход (**w**).

Создание RAID-массива

Для создания программного **RAID**-массива в РЕД ОС используется утилита **mdadm**.

```
mdadm --create /dev/md0 --level=6 --raid-devices=4 /dev/sd[b-e]1
```

Здесь:
/dev/md0 – имя устройства **RAID**;
--level=6 – уровень **RAID**;
--raid-devices=4 – количество дисков, участвующих в сборке массива;
/dev/sd[b-e]1 – имена дисков участвующих в сборке массива.

```
[root@localhost ~]# mdadm --create /dev/md0 --level=6 --raid-devices=4 /dev/sd[b-e]1
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
```

Проверим состояние созданного RAID-массива:

```
cat /proc/mdstat
```

```
[root@localhost ~]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid6 sde1[3] sdd1[2] sdc1[1] sdb1[0]
      2091008 blocks super 1.2 level 6, 512k chunk, algorithm 2 [4/4] [UUUU]

unused devices: <none>
```

Создание автоматического монтирования RAID

Создадим файловую систему **ext4** на **RAID**-устройстве **/dev/md0** и смонтируем массив в каталог **/mnt/raid6/**.

```
mkfs.ext4 /dev/md0
mkdir /mnt/raid6
mount /dev/md0 /mnt/raid6
```

Для автоматического монтирования **RAID** добавим запись:

```
/dev/md0   /mnt/raid6    ext4  defaults   0 0
```

в **/etc/fstab**.

```
 GNU nano 7.2                                                                 /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Nov  4 20:22:40 2024
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=2f23dcb4-ca21-41db-bee4-849df2c674d6 /                       ext4    defaults        1 1
UUID=040b195b-c58c-46d7-96f7-da469f947596 /boot                   ext4    defaults        1 2
UUID=afa7e8a6-84ae-4684-8014-35192b657a34 none                    swap    defaults        0 0
/dev/md0                       /mnt/raid6                         ext4    defaults        0 0
```

А также необходимо сохранить конфигурацию **RAID**, чтобы во время загрузки системы происходило ее считывание.

```
mdadm --detail --scan --verbose > /etc/mdadm.conf
```

Выполним команду **lsblk**, при этом в ее выводе будет видно, что тип дисков изменился на **RAID6**.

```
[root@localhost ~]# lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda       8:0    0   40G  0 disk
├─sda1    8:1    0    1M  0 part
├─sda2    8:2    0    1G  0 part  /boot
├─sda3    8:3    0    2G  0 part  [SWAP]
└─sda4    8:4    0 36,9G  0 part  /
sdb       8:16   0    1G  0 disk
└─sdb1    8:17   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid6 /mnt/raid6
sdc       8:32   0    1G  0 disk
└─sdc1    8:33   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid6 /mnt/raid6
sdd       8:48   0    1G  0 disk
└─sdd1    8:49   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid6 /mnt/raid6
sde       8:64   0    1G  0 disk
└─sde1    8:65   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid6 /mnt/raid6
sr0      11:0    1 1024M  0 rom
zram0   252:0    0  1,9G  0 disk  [SWAP]
```

Создание программного массива уровня RAID 10

Подготовка к созданию RAID-массива
Создание RAID-массива
Создание автоматического монтирования RAID
Замена неисправного диска при сбое, добавление запасного диска
Удаление диска из массива
Расширение массива

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Подготовка к созданию RAID-массива

В инструкции рассмотрено создание программного RAID-массива из **4 дисков**, размером в **1 ГБ**. Это минимально возможное количество дисков, которое требуется для создания RAID-массива уровня 10. Массив показывает высокую производительность и высокую надежность. Однако, как в случае и с RAID 1 эффективность использования дискового пространства составляет 50%.

Для выполнения дальнейших действий требуется перейти в сеанс пользователя **root**:

```
su -
```

Чтобы посмотреть текущую информацию об устройствах хранения, выполните команду:

```
lsblk
```

```
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   20G  0 disk
├─sda1   8:1    0  600M  0 part /boot/efi
├─sda2   8:2    0    1G  0 part /boot
├─sda3   8:3    0    2G  0 part [SWAP]
└─sda4   8:4    0 16,4G  0 part /
sdb      8:16   0    1G  0 disk
sdc      8:32   0    1G  0 disk
sdd      8:48   0    1G  0 disk
sde      8:64   0    1G  0 disk
sr0     11:0    1  4,4G  0 rom  /run/media/user/redos-Everything-DVD-x86_64-8
zram0  252:0    0  1,9G  0 disk [SWAP]
```

Здесь **sdb**, **sdc**, **sdd** и **sde** – диски, из которых будет собран программный **RAID 10**.

Убедимся, что на подключенных дисках отсутствуют метаданных типа RAID. Это можно сделать командой.

```
mdadm -E /dev/sd[b-e]
```

```
[root@localhost ~]# mdadm -E /dev/sd[b-e]
mdadm: No md superblock detected on /dev/sdb.
mdadm: No md superblock detected on /dev/sdc.
mdadm: No md superblock detected on /dev/sdd.
mdadm: No md superblock detected on /dev/sde.
```

mdadm – специальная утилита для управления программными RAID-массивами. В РЕД ОС уже предустановлена по умолчанию. В выводе команды видим сообщение ***«No md superblock detected»*** это означает, что признаки RAID на дисках отсутствуют.

Приступим к предварительной подготовке, а именно создадим на каждом диске раздел с помощью утилиты **fdisk**:

```
fdisk /dev/sdb
```

В консоли **fdisk** выберите:

- Создание раздела (**n**);
- Тип раздела primary (**p**);
- Номер раздела (**1**);
- Начальный и конечный блоки (**Enter**);
- Для изменения типа раздела (**t**);
- Шестнадцатеричный код раздела (**fd**);
- Применение изменений и выход (**w**).

Подобные действия повторяем и для оставшихся дисков: **/dev/sdb**, **/dev/sdc**, **/dev/sde**.

Создание RAID-массива

Для создания программного **RAID**-массива в РЕД ОС используется утилита **mdadm**.

```
mdadm --create /dev/md0 --level=10 --raid-devices=4 /dev/sd[b-e]1
```

Здесь:

- **/dev/md0** – имя устройства **RAID**;
- **--level=10** – уровень **RAID**;
- **--raid-devices=4** – количество дисков, участвующих в сборке массива;
- **/dev/sd[b-e]1** – имена дисков, участвующих в сборке массива.

```
[root@localhost ~]# mdadm --create /dev/md0 --level=10 --raid-devices=4 /dev/sd[b-e]1
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
```

Проверим состояние созданного RAID-массива:

```
cat /proc/mdstat
```

```
[root@localhost ~]# cat /proc/mdstat
Personalities : [raid10]
md0 : active raid10 sde1[3] sdd1[2] sdc1[1] sdb1[0]
      2091008 blocks super 1.2 512K chunks 2 near-copies [4/4] [UUUU]

unused devices: <none>
```

Кроме этого следующая команда покажет более детальную информацию о созданном RAID массиве:

```
mdadm -D /dev/md0
```

Создание автоматического монтирования RAID

Создадим файловую систему **ext4** на **RAID**-устройстве **/dev/md0** и смонтируем массив в каталог **/mnt/raid10/**.

```
mkfs.ext4 /dev/md0
mkdir /mnt/raid10
mount /dev/md0 /mnt/raid10
ls -l /mnt/raid10/
```

Для автоматического подключения **RAID** добавим запись в конец файла /etc/fstab, для этого в терминале выполните команду:

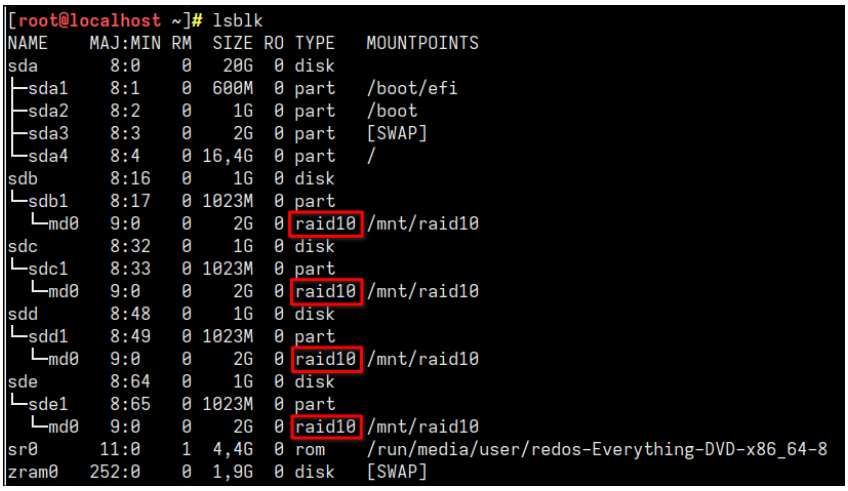
```
echo "/dev/md0 /mnt/raid10 ext4 defaults 0 0" >> /etc/fstab
```

```
 GNU nano 7.2                                /etc/fstab                                Изменён

#
# /etc/fstab
# Created by anaconda on Tue Dec 10 12:05:50 2024
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=535fd0ea-032f-41cd-91c0-b86aebb7e5ba /                       ext4    defaults        1 1
UUID=9029730e-8aba-4605-b50e-edd7539f2b15 /boot                   ext4    defaults        1 2
UUID=E9A9-4D65          /boot/efi               vfat    umask=0077,shortname=winnt 0 2
UUID=a76a7430-b504-4ada-a66d-8be332d11db4 none                    swap    defaults        0 0
/dev/md0                /mnt/raid10                               ext4    defaults        0 0
```

А также сохраним конфигурацию **RAID**, чтобы во время загрузки системы происходило ее считывание.

```
mdadm --detail --scan --verbose >> /etc/mdadm.conf
```

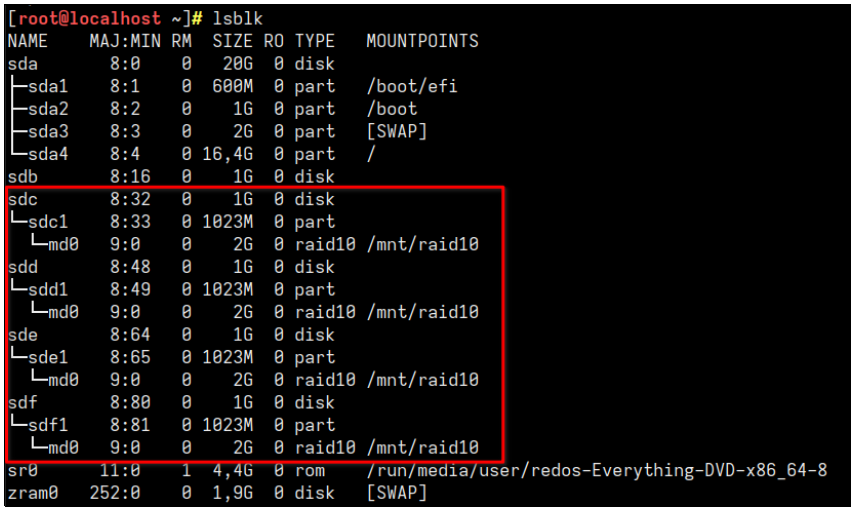
Команда **lsblk** покажет, что тип дисков изменился на **RAID10**.



Замена неисправного диска при сбое, добавление запасного диска

В RAID-массиве уровня 10 имеется возможность добавления запасного диска для быстрой замены при выходе из строя одного из основных устройств хранения.

Рассмотрим RAID-массив, состоящий из дисков **/dev/sdc**, **/dev/sdd**, **/dev/sde**, **/dev/sdf**.



В примере диск **/dev/sdc** будет выведен из строя, а для его замены будет подключен новый диск **/dev/sdb**.

Проверим присутствие на диске метаданных RAID с помощью утилиты **mdadm**:

```
mdadm -E /dev/sdb
mdadm: No md superblock detected on /dev/sdb
```

Сообщение в выводе команды означает, что признаки RAID на диске отсутствуют.

Создадим на диске раздел с помощью утилиты **fdisk**:

```
fdisk /dev/sdb
```

Далее повторно проверим раздел, добавим диск **/dev/sdb1** в массив **md0** и проверим добавление запасного диска в RAID-устройство:

```
mdadm --examine /dev/sdb1
mdadm: No md superblock detected on /dev/sdb1.
 mdadm --add /dev/md0 /dev/sdb1
mdadm: added /dev/sdb1
```

Для отображения детальной информации о созданном RAID-массиве выполните:

```
mdadm --detail /dev/md0/dev/md0:
        Version : 1.2
  Creation Time : Tue Dec 17 10:25:04 2024
```

```
        Raid Level : raid10
        Array Size : 2091008 (2042.00 MiB 2141.19 MB)
     Used Dev Size : 1045504 (1021.00 MiB 1070.60 MB)
      Raid Devices : 5
     Total Devices : 5
       Persistence : Superblock is persistent

       Update Time : Tue Dec 17 11:31:04 2024
             State : clean
    Active Devices : 5
   Working Devices : 5
    Failed Devices : 0
     Spare Devices : 0

            Layout : near=2
        Chunk Size : 512K

Consistency Policy : resync

              Name : localhost.localdomain:0  (local to host localhost.localdomain)
              UUID : eb4005dd:15ecc750:b6fac596:81e0fe64
            Events : 20
```

Пометим диск **/dev/sdc1** в массиве **/dev/md0** как сбойный и проверим статус:

```
mdadm --manage --fail /dev/md0 /dev/sdc1
mdadm: set /dev/sdc1 faulty in /dev/md0
 mdadm --detail /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Tue Dec 17 10:25:04 2024
        Raid Level : raid10
        Array Size : 2091008 (2042.00 MiB 2141.19 MB)
     Used Dev Size : 1045504 (1021.00 MiB 1070.60 MB)
      Raid Devices : 5
     Total Devices : 5
       Persistence : Superblock is persistent

       Update Time : Tue Dec 17 11:33:07 2024
             State : clean
    Active Devices : 4
   Working Devices : 4
    Failed Devices : 1
     Spare Devices : 0

            Layout : near=2
        Chunk Size : 512K

Consistency Policy : resync

              Name : localhost.localdomain:0  (local to host localhost.localdomain)
              UUID : eb4005dd:15ecc750:b6fac596:81e0fe64
            Events : 39cat /proc/mdstat
```

После завершения процесса синхронизации статус будет изменен на **[UU]**. Для дисков большого размера процесс синхронизации может занять длительное время.

Удаление диска из массива

Утилита **mdadm** с ключом **--remove** удалит из массива указанный команде диск. Удалим диск **/dev/sdc1** из **/dev/md0**, который ранее был помечен как сбойный и проверим статус:

```
mdadm --remove /dev/md0 /dev/sdc1
mdadm: hot removed /dev/sdc1 from /dev/md0
 cat /proc/mdstat
Personalities : [raid10]
md0 : active raid10  sdb1[4]  sdf1[3]  sde1[2]  sdd1[1]
      2091008 blocks super 1/2  512K chunks  2  near-copies [4/4] [UUUU]
```

```
unused devices: <none>
```

Расширение массива

Проверим отображение нового подключенного диска (**/dev/sdg**) с помощью **lsblk**.

```
lsblkNAME    MAJ:MIN RM  SIZE RO TYPE   MOUNTPOINTS
sda       8:0    0   20G  0 disk
├─sda1    8:1    0  600M  0 part   /boot/efi
├─sda2    8:2    0    1G  0 part   /boot
├─sda3    8:3    0    2G  0 part   [SWAP]
└─sda4    8:4    0 16,4G  0 part   /
sdb       8:16   0    1G  0 disk
└─sdb1    8:17   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid10 /mnt/raid10
sdc       8:32   0    1G  0 disk
└─sdc1    8:33   0 1023M  0 part
sdd       8:48   0    1G  0 disk
└─sdd1    8:49   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid10 /mnt/raid10
sde       8:64   0    1G  0 disk
└─sde1    8:65   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid10 /mnt/raid10
sdf       8:80   0    1G  0 disk
└─sdf1    8:81   0 1023M  0 part
  └─md0   9:0    0    2G  0 raid10 /mnt/raid10
sdg       8:96   0    1G  0 disk
sr0      11:0    1  4,4G  0 rom    /run/media/user/redos-Everything-DVD-x86_64-8
zram0   252:0    0  1,9G  0 disk   [SWAP]
```

Затем добавим диск в массив, увеличим размер массива и проверим статус RAID следующими командами:

```
mdadm --add /dev/md0 /dev/sdg1
mdadm --grow --raid-devices=5 /dev/md0
mdadm --detail /dev/md0
cat /proc/mdstat
```

Сохраним конфигурацию RAID в **/etc/mdadm.conf** командой:

```
mdadm --detail --scan >> /etc/mdadm.conf
```

Установка РЕД ОС на программный массив RAID1 и RAID10

Установка РЕД ОС на программный массив уровня RAID 1 для систем с UEFI
Решение проблемы недоступности одного из дисков
Установка РЕД ОС на программный массив уровня RAID 10

Особенности программного RAID-массива:

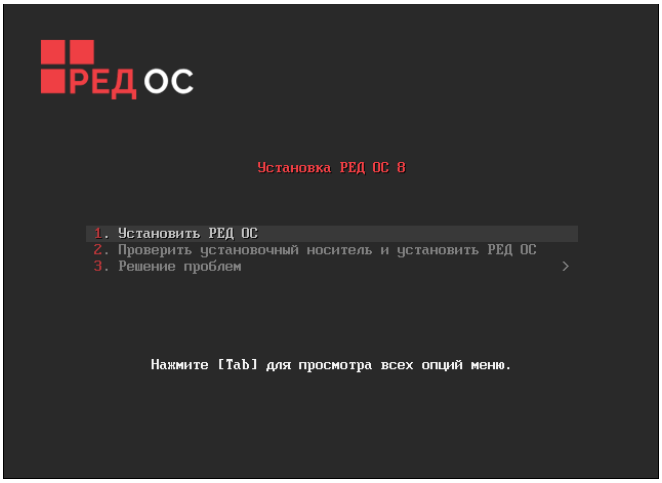
- *Гибкость*: управление RAID происходит с помощью операционной системы, поэтому такой массив можно настроить из работающей системы без перенастройки оборудования.
- *Открытый исходный код*: реализация программного RAID-массива основана открытом программном коде.
- *Никаких дополнительных расходов*: программный RAID не требует специального аппаратного обеспечения и не привязан к конкретному оборудованию.
- *Ресурсные затраты*: в течение всего срока существования программный RAID критикуют за повышенное использование аппаратных ресурсов. Такие программные реализации как mdadm практически полностью устраняют эту проблему на современном оборудовании.

Установка РЕД ОС на программный массив уровня RAID 1 для систем с UEFI

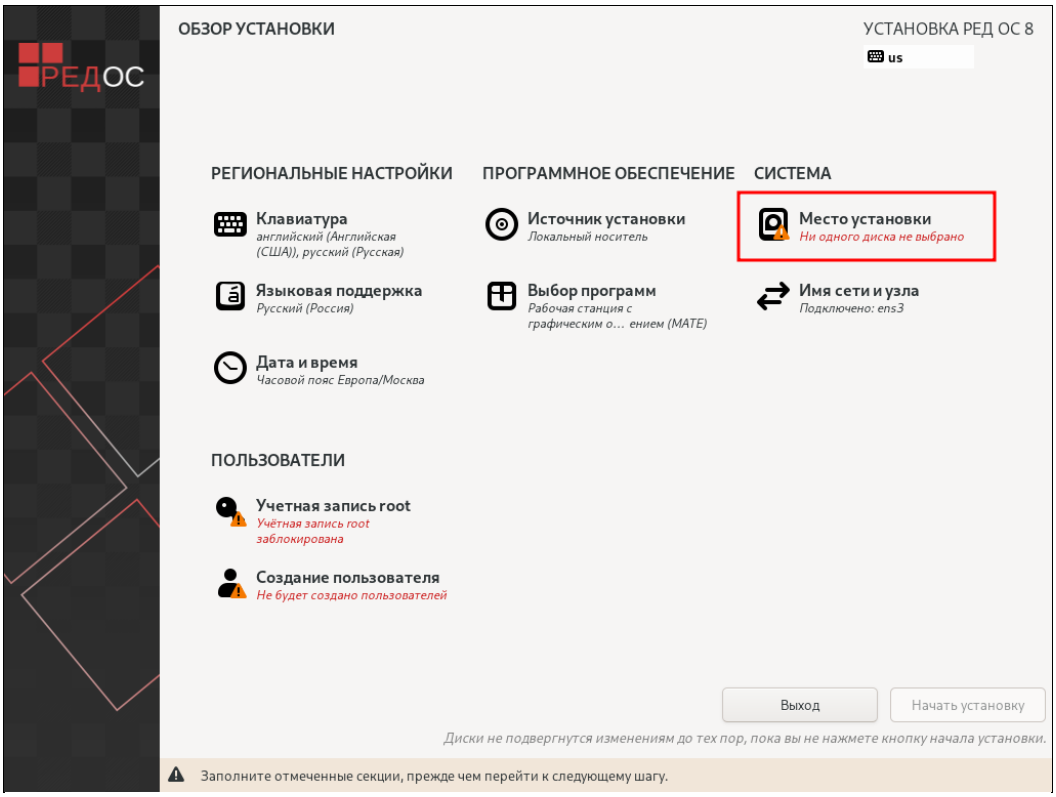
RAID 1 состоит из так называемого «зеркалирования» данных без их контроля четности и чередования. В такой реализации данные записываются идентично на два или более дисков, тем самым создавая «зеркальный набор» дисков. Таким образом, все диски в массиве являются полными копиями друг друга, что обеспечивает высокую надежность, но в то же время появляется избыточность данных.

Для установки РЕД ОС на **RAID 1** выполните следующие действия:

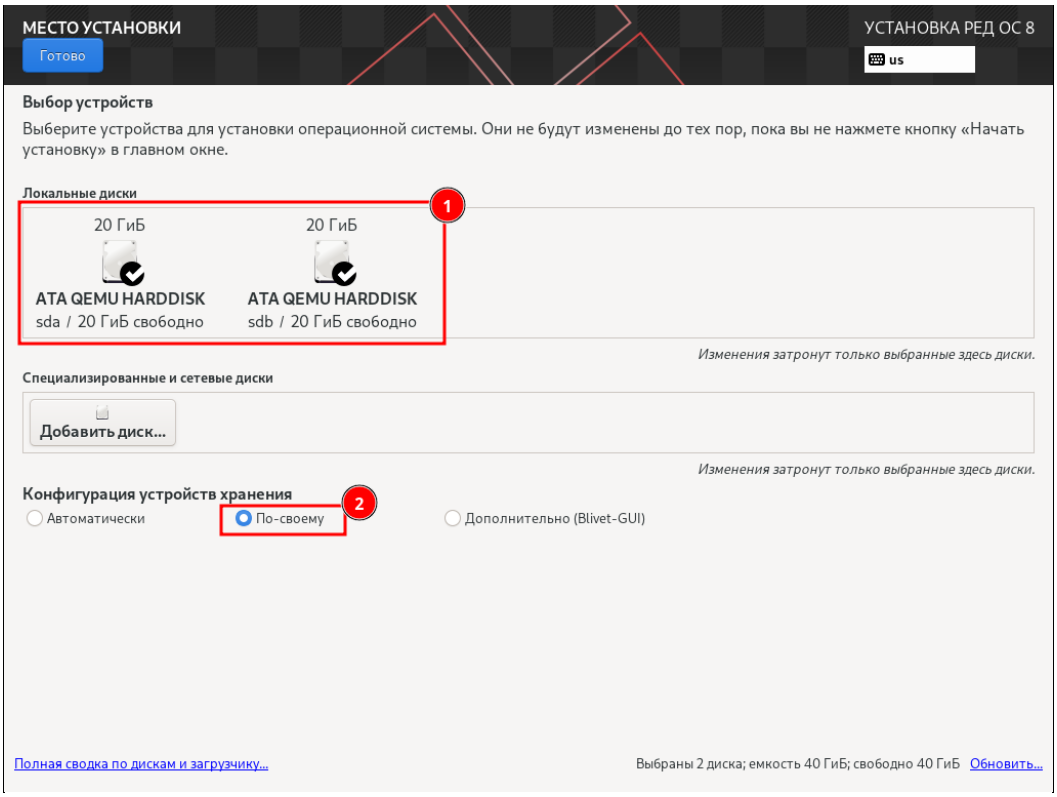
1. Выберите первый пункт «**Установить RED OS**».



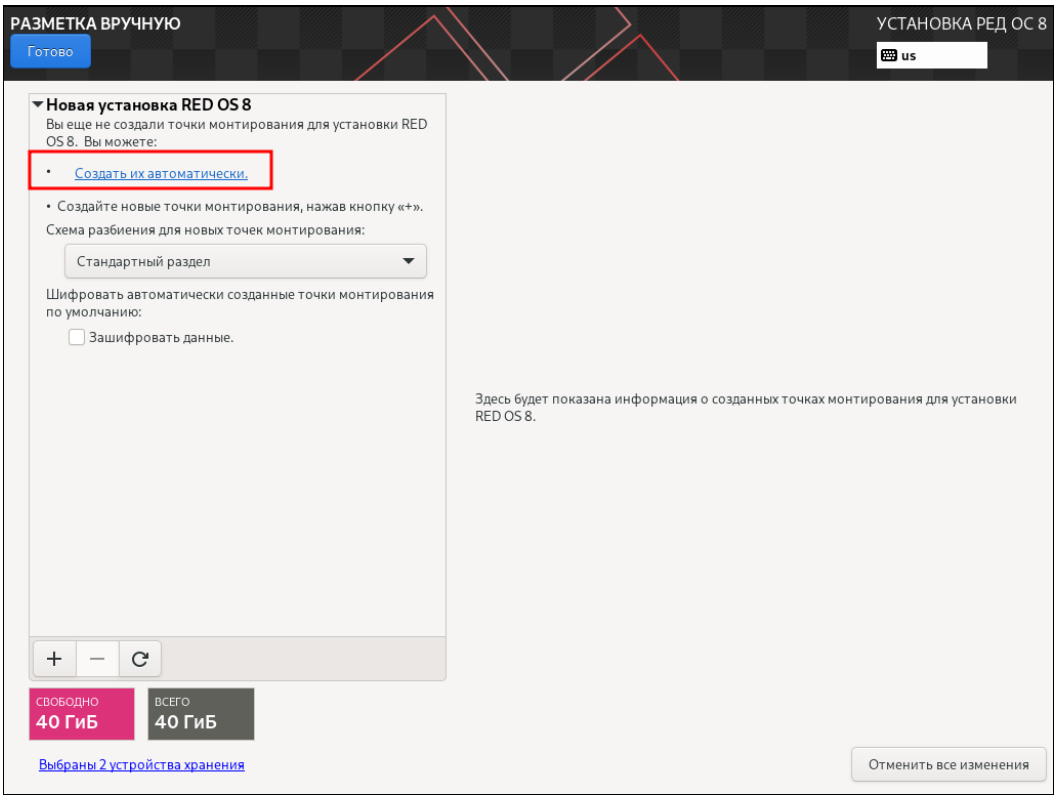
2. Перейдите в раздел для разметки дисков, выбрав пункт «**Место установки**».



3. В окне «**Место установки**» выберите необходимые для разметки диски (в примере отмечены два диска по 20 ГБ), активируйте чекбокс для варианта «**По-своему**», а затем нажмите «**Готово**».



4. Создайте необходимые разделы, нажав «**Создать их автоматически**».

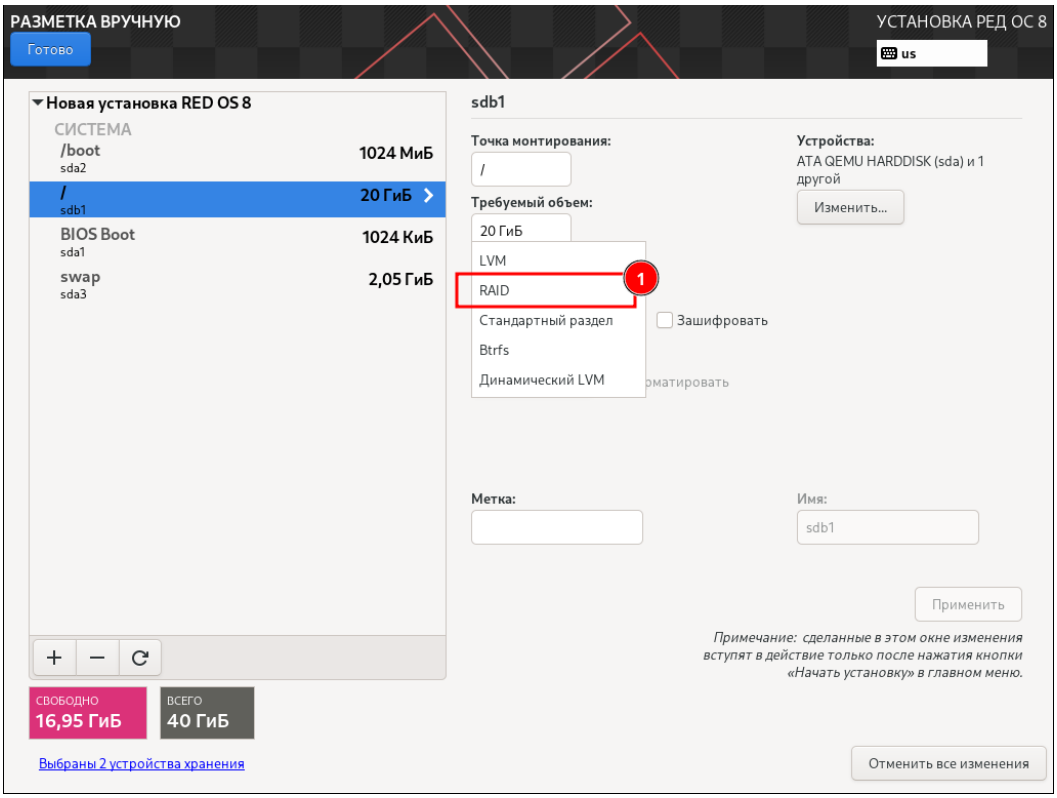


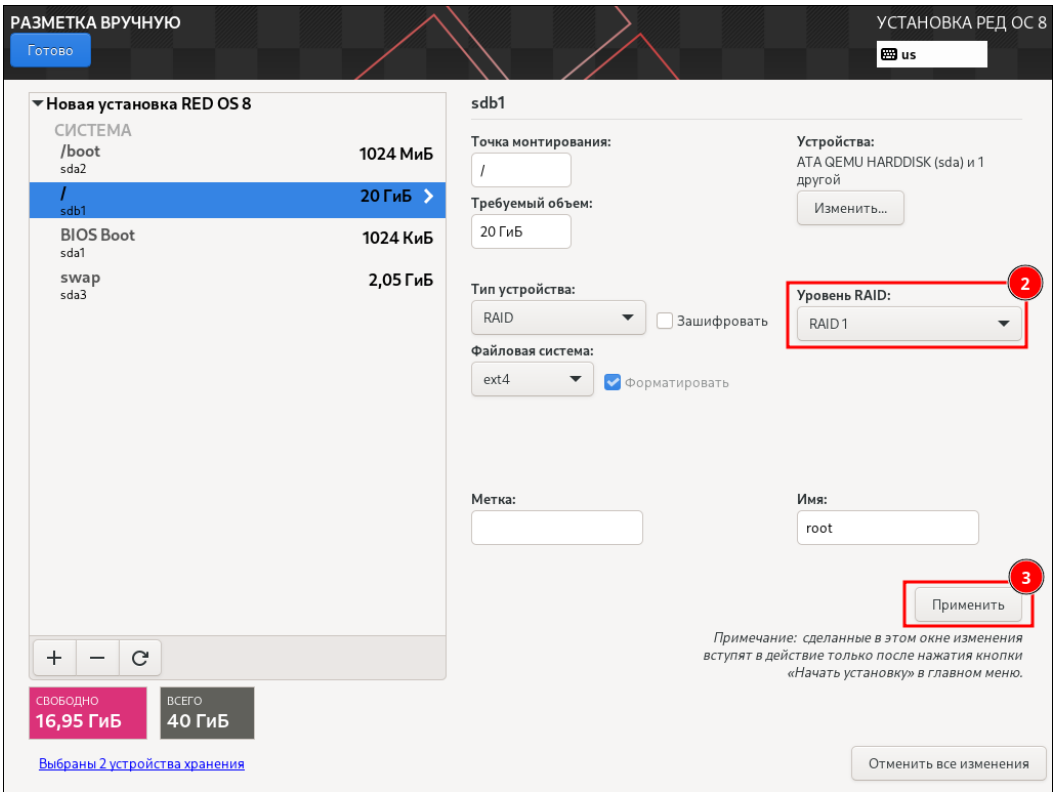
5. После разметки в правой части окна выполните следующие действия:

5.1 Выбрать «**Тип устройства**» — **RAID**.

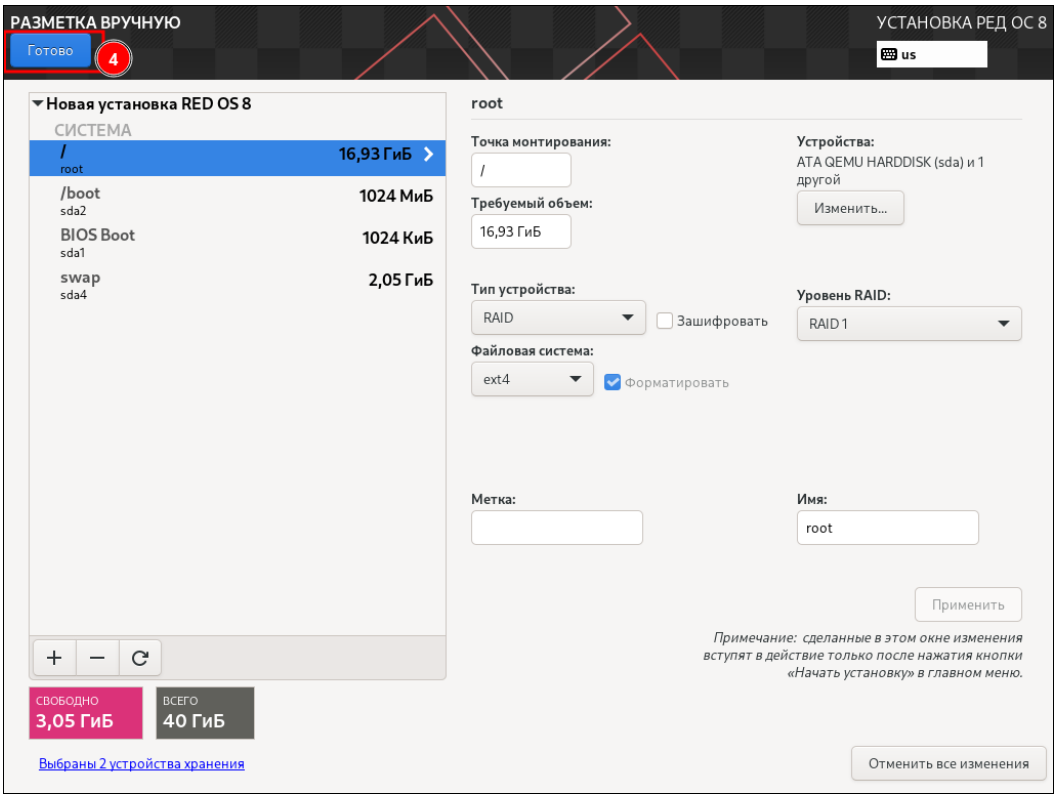
5.2 В группе «**Уровень RAID**» — указать необходимый тип RAID-массива (в примере выбран **RAID1**).

5.3 Нажмите кнопку «**Применить**».





6. Повторите операцию выбора типа устройства (**RAID**) и уровня **RAID** для всех остальных разделов: **/boot/efi**, **/boot**, **swap**.



7. По нажатии кнопки «**Готово**» будет открыто окно с итоговой таблицей разметки – при необходимости проверьте установленные параметры и, если все настроено верно, нажмите «**Принять изменения**».

8. Далее установите ОС в штатном режиме.

Решение проблемы недоступности одного из дисков

Для подготовки разделов диска на случай, если один из дисков будет недоступен, необходимо:

1. Вывести и запомнить идентификаторы (**UUID**) дисков командой:

```
lsblk -fs
```

2. Изменить **UUID** для **sdb1** и **sdb2** из вывода команды `lsblk -fs`:

```
mkdosfs -i <UUID_sda1> /dev/sdb1
e2fsck -f /dev/sdb2
tune2fs /dev/sdb2 -U <UUID_sda2>
```



3. Скопировать данные на **/dev/sdb1** для EFI-раздела:

```
mount /dev/sdb1 /mnt
cp -R /boot/efi/EFI/ /mnt
```

После чего отмонтировать раздел:

```
umount /dev/sdb1
```

4. Скопировать на **/dev/sdb2** данные из **/dev/sda2** для **boot**-раздела:

```
mount /dev/sda2 /media
mount /dev/sdb2 /mnt
```

```
cp -R /media/* /mnt/
umount /media /mnt
```

После этого система с **UEFI** сможет найти загрузчик на любом из дисков, который будет доступен.

В случае если система с **UEFI** не смогла самостоятельно обнаружить загрузочную запись, можно прописать ее самостоятельно. Для этого:

1. Загрузитесь в rescue с USB/DVD-диска:

```
chroot /mnt/sysroot
```

2. Переведите SELinux в режим permissive:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

3. Выведите информацию о загрузочных записях:

```
efibootmgr -v
```

4. Пропишите загрузчик командой:

```
efibootmgr -c -d /dev/sdb -p 1 -L "RED OS 2" -l "\EFI\redos\shimx64.efi"
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

```
[root@localhost ~]# efibootmgr -v
BootCurrent: 0005
Timeout: 0 seconds
BootOrder: 0008,0005,0000,0001,0002,0003,0004,0006
Boot0000* UiApp FvVol(7cb8bdc9-f8eb-4f34-aaea-3ee4af6516a1)/FvFile(462caa21-7614-4503-836e-8ab6f4662331)
Boot0001* UEFI VBOX CD-ROM VB2-01700376         PciRoot(0x0)/Pci(0x1,0x1)/Ata(1,0,0)N.....YM....R,Y.
Boot0002* UEFI VBOX HARDDISK VB4eb3ffe3-127cf754        PciRoot(0x0)/Pci(0xd,0x0)/Sata(0,65535,0)N.....YM....R,Y.
Boot0003* UEFI VBOX HARDDISK VB241a0996-68ce5c4d        PciRoot(0x0)/Pci(0xd,0x0)/Sata(1,65535,0)N.....YM....R,Y.
Boot0004* EFI Internal Shell    FvVol(7cb8bdc9-f8eb-4f34-aaea-3ee4af6516a1)/FvFile(7c04a583-9e3e-4f1c-ad65-e05268d0b4d1)
Boot0005* RED OS        HD(1,GPT,ec410ecf-c449-4fd1-b696-e38825b1dd91,0x800,0x12c000)/File(\EFI\redos\shimx64.efi)
Boot0006* UEFI PXEv4 (MAC:080027388CEE) PciRoot(0x0)/Pci(0x3,0x0)/MAC(080027388cee,1)/IPv4(0.0.0.00.0.0.0,0,0)N.....YM....R,Y.
Boot0008* RED OS 2      HD(1,GPT,390bc59e-4ecc-4262-9f98-155a2a826e1a,0x800,0x12c000)/File(\EFI\redos\shimx64.efi)
[root@localhost ~]#
```

Если потребуется удалить запись, выполните команду:

```
efibootmgr -b 6 -B
```

где:

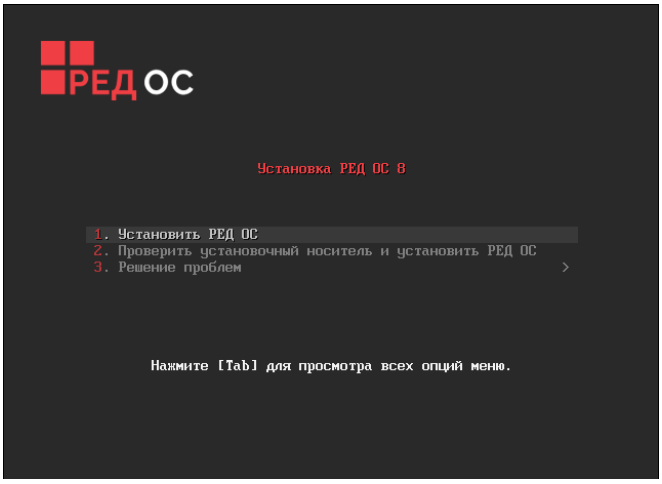
- **-b** (**--bootnum**) – указывает на номер записи;
- **-B** (**--delete-bootnum**) – указывает удалить запись.

Установка РЕД ОС на программный массив уровня RAID 10

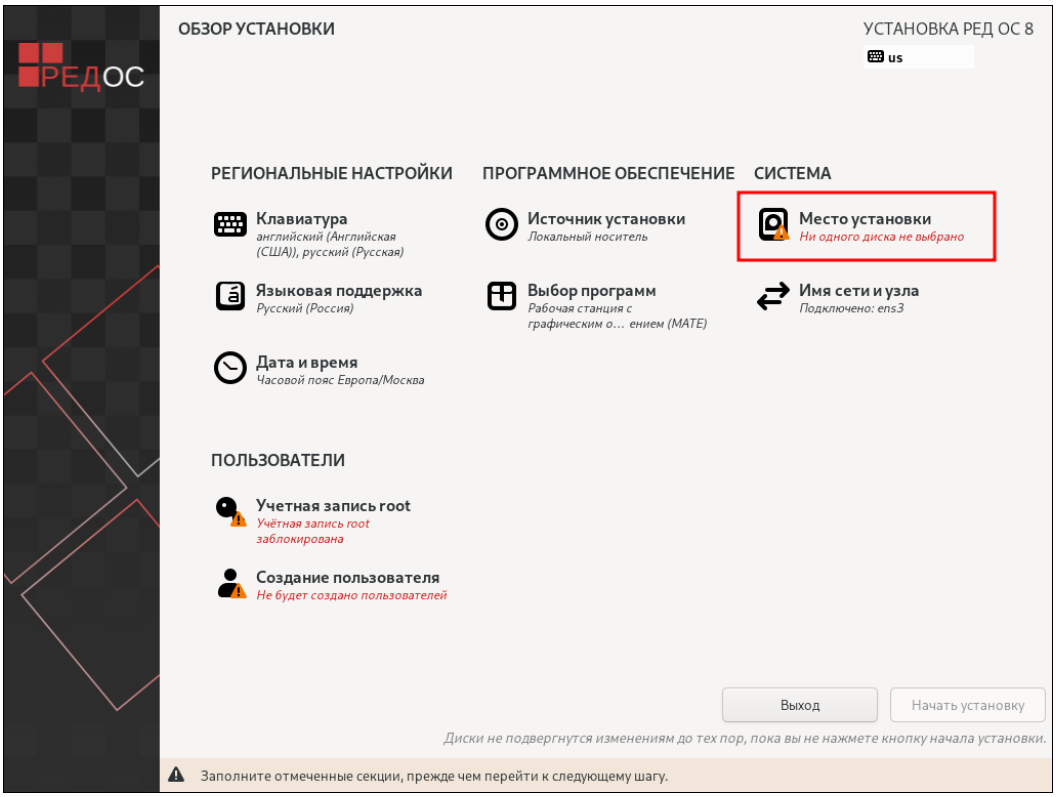
RAID 10 представляет собой объединение массивов **RAID 1** и **RAID 0**. Для создания **RAID 10** требуется **минимум четыре диска**, в которых данные чередуются на зеркальных парах. Пока один диск в каждой зеркальной паре функционирует, данные могут быть извлечены. В случае сбоя двух дисков в одной зеркальной паре все данные будут потеряны из-за отсутствия четности в чередующихся наборах.

Для установки РЕД ОС на **RAID 10** выполните следующие действия:

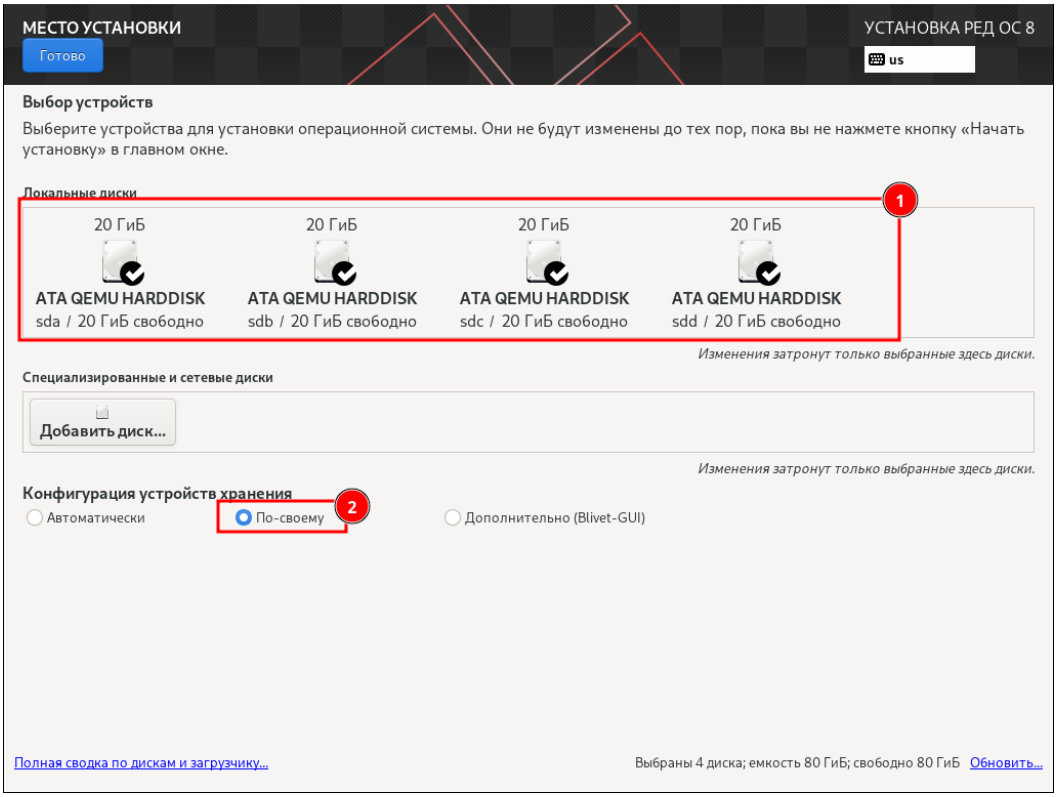
1. Выберите первый пункт «**Установить RED OS**».



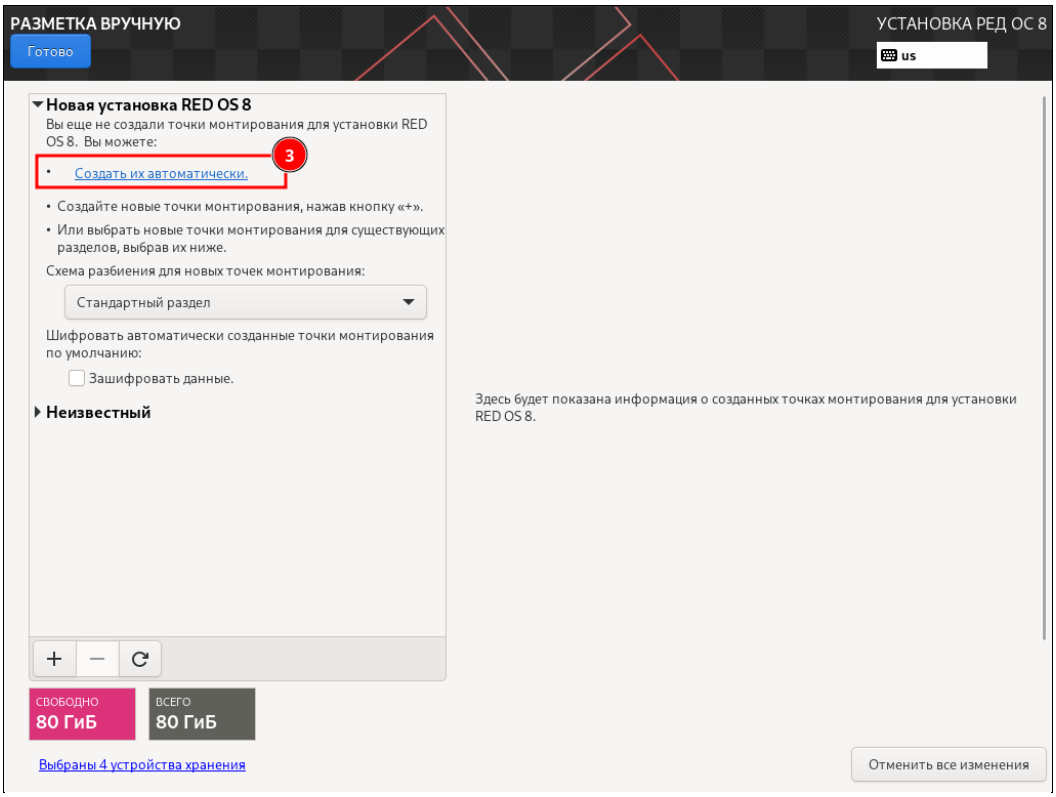
2. Перейдите в раздел для разметки дисков (пункт «**Место установки**»).



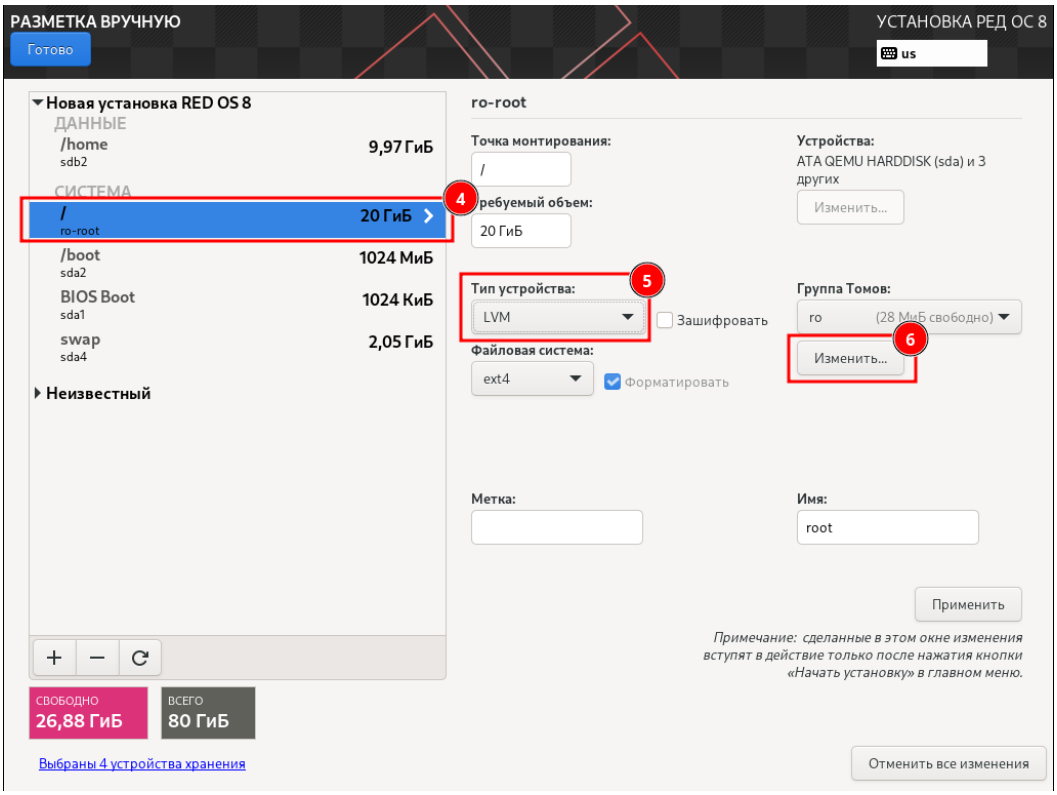
3. В данном окне отметьте все локальные диски, нажмите кнопку «**По-своему**», а затем «**Готово**».



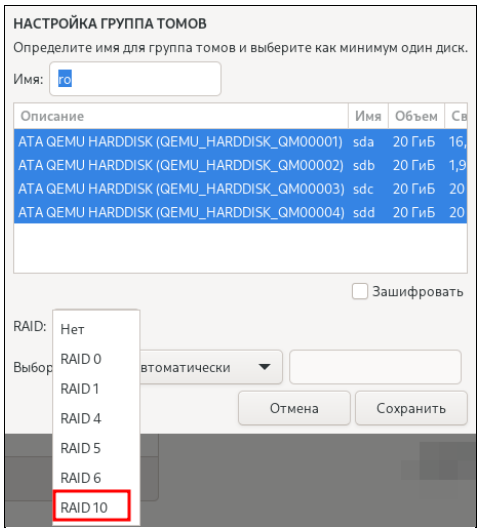
4. Нажмите на пункт «**Создать их автоматически**».



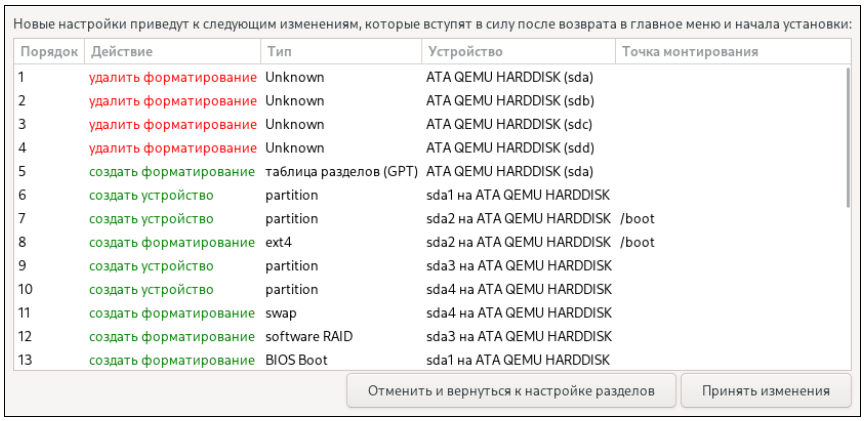
5. В конфигураторе разметки дисков определите нужный размер для корневого и домашнего раздела через параметр «**Требуемый объем**». После этого выберите корневой раздел и в группе томов нажмите на кнопку « **Изменить**».



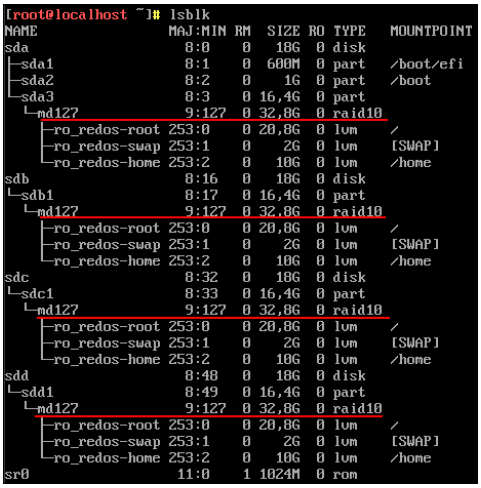
6. В окне настройки группы томов из списка **RAID** выберите «**RAID 10**».



7. Итоговая таблица разметки:

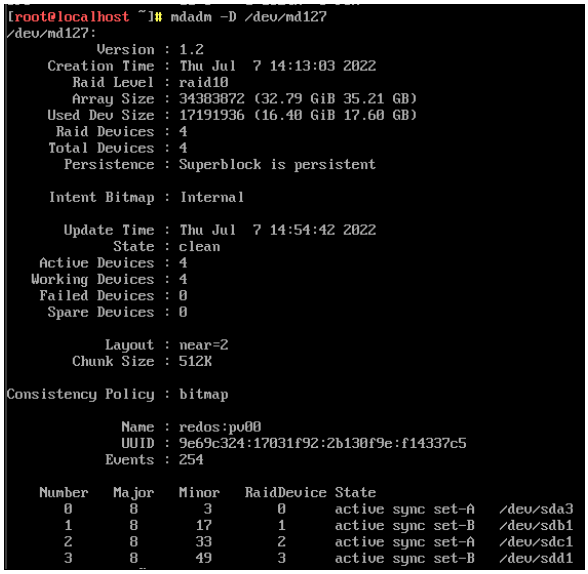


8. После установки можно просмотреть информацию о разделах на **RAID 10**:



Команда `lsblk` показывает, что **md127** – это **RAID 10**. Также видно, что на каждом из дисков **sda**, **sdb**, **sdc**, **sdd** созданы разделы с точками монтирования **swap**, **home** и **корень** (/), которые являются точными копиями друг друга. В RAID-массиве десятого уровня данные делятся на блоки и дублируются на паре дисков.

Команда `mdadm -D /dev/md127` выведет на экран детальную информацию о RAID-массиве.


[root@localhost ~]# mdadm -D /dev/md127
/dev/md127:
Version : 1.2
Creation Time : Thu Jul 7 14:13:03 2022
Raid Level : raid10
Array Size : 34383872 (32.79 GiB 35.21 GB)
Used Dev Size : 17191936 (16.40 GiB 17.60 GB)
Raid Devices : 4
Total Devices : 4
Persistence : Superblock is persistent
Intent Bitmap : Internal
Update Time : Thu Jul 7 14:54:42 2022
State : clean
Active Devices : 4
Working Devices : 4
Failed Devices : 0
Spare Devices : 0
Layout : near=2
Chunk Size : 512K
Consistency Policy : bitmap
Name : redos:pv00
UUID : 9e69c324:17031f92:2b130f9e:f14337c5
Events : 254
Number Major Minor RaidDevice State
0 8 3 0 active sync set-A /dev/sda3
1 8 17 1 active sync set-B /dev/sdb1
2 8 33 2 active sync set-A /dev/sdc1
3 8 49 3 active sync set-B /dev/sdd1

Автоматизация развертывания (kickstart)

Порядок установки
Создание файла кикстарта
Проверка файла кикстарт
Расположение файла кикстарта
Создание загрузочного диска
Начало установки
Запуск установки вручную
Автоматический запуск установки
Синтаксис кикстарта
Команды и интерпретаторы
Секция %packages
Секция %pre
Секция %post
Пример файла конфигурации

Процесс установки операционной системы можно автоматизировать, определив все необходимые данные (список пакетов, схемы разделов, часовой пояс, языковые настройки и т. д.) в одном файле — файле **kickstart**. Файлы кикстарта могут располагаться на отдельном сервере и подгружаться во время установки.

Данный способ очень удобен и является наиболее предпочтительным для сетевых и системных администраторов, т.к. один файл может использоваться для одновременной установки системы на нескольких компьютерах.

Сценарии и журналы кикстарта хранятся в каталоге **/tmp** для помощи в диагностике ошибок при установке.

Порядок установки

Автоматизированная установка может быть запущена с локального жесткого диска, DVD или с сервера NFS, FTP, HTTP, HTTPS.

Для этого необходимо:

1. Создать файл кикстарта.

2. Записать файл на локальный или удаленный носитель.

3. Создать загрузочный диск, с которого будет запускаться установка.

4. Предоставить доступ к установочной структуре.

5. Начать процесс установки.

Создание файла кикстарта

Файл кикстарта представляет собой обычный текстовый файл, содержащий параметры установки, каждый из которых определяется ключевым словом. Файл можно создать самостоятельно в любом текстовом редакторе, способном сохранять файлы в формате ASCII, например, в vim, либо модифицировать готовый шаблон, который автоматически создается в ходе установки системы, исходя из выбранных параметров. Файл (шаблон) **anaconda-ks.cfg** можно найти в каталоге **/root/**.

При создании файла кикстарта следует придерживаться нескольких рекомендаций:

- Секции файла должны быть упорядочены. Элементы внутри секций могут располагаться в любом порядке. Порядок секций следующий:
    - Раздел команд (обязательные параметры должны быть определены);
    - Раздел **%packages**;
    - Разделы **%pre** и **%post**, которые могут следовать в любом порядке и обязательными не являются.

ВАЖНО!

Секции **%packages**, **%post** и **%pre** должны завершаться директивой **%end**. В противном случае файл не будет обработан.

- Элементы, не отмеченные как обязательные, могут быть опущены;
- Если обязательный параметр не определен, программа установки предложит его ввести так же, как и во время обычной

установки. После получения ответа установка будет продолжена без вмешательства пользователя (если снова не столкнется с отсутствующим параметром);

- Строки, начинающиеся с символа **#**, интерпретируются как комментарии и игнорируются.

Проверка файла кикстарт

После создания файла кикстарта рекомендуется проверить его формат. Для этого в репозитории РЕД ОС имеется программа **ksvalidator** в составе пакета **pykickstart**.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install pykickstart
```

Для проверки формата файла выполните команду (с правами локального пользователя):

```
ksvalidator /<путь_к_файлу>/kickstart.ks
```

В параметре <путь_к_файлу> укажите свой актуальный путь.

Подробную информацию по использованию **ksvalidator** см. в справке `man ksvalidator`.

Примечание.

Возможности такой проверки **ограничены**. Структура файла может быть достаточно сложной и, несмотря на то, что **ksvalidator** проверит синтаксис файла и поможет убедиться в отсутствии устаревших параметров, это **не гарантирует** успех установки. Более того, секции *%pre*, *%post* и *%packages* **не проверяются**.

Расположение файла кикстарта

Файл кикстарта может быть расположен:

- на съемном носителе (DVD, USB);
- на локальном жестком диске;
- на доступном сетевом ресурсе.

Размещение файла кикстарта в сети используется чаще — для автоматизации установки в системах, подключенных к сети. Сначала устанавливаемая система загружается с PXE-сервера, затем файл кикстарта загружается с удаленного диска, а перечисленные в файле пакеты в дальнейшем будут установлены в системе.

Доступ программы установки к файлу кикстарта необходимо обеспечить аналогично тому, как это делается для установочных образов.

Создание загрузочного диска

Подробную информацию о создании загрузочных носителей и записи iso-образов см. в нашей инструкции «Создание загрузочных носителей».

Начало установки

Для запуска кикстарт-установки используется параметр `inst.ks=`.

Также установку можно запустить с PXE-сервера. В файл конфигурации загрузчика можно добавить параметр автоматического запуска установки. Этот подход позволяет полностью автоматизировать процесс загрузки.

Приведенные ниже инструкции являются общими и могут отличаться в зависимости от архитектуры.

Запуск установки вручную

Ручной запуск установки подразумевает некоторую степень взаимодействия с пользователем, например, добавление параметров в строке `boot:`.

Для запуска установки необходимо выполнить следующие действия:

1. Загрузить систему с локального носителя (CD, DVD, USB).

2. В строке приглашения загрузки добавить параметр **inst.ks=<путь_к_файлу>/kickstart.ks**, где вместо <путь_к_файлу> укажите свой путь. Если файл расположен на другом компьютере в сети, дополнительно потребуется определить параметр `ip=`. Обычно также требуется указать расположение пакетов с помощью `inst.repo=`.

3. Подтвердите выбранные параметры и начните установку.

Если файл кикстарта не содержит ошибок, процесс установки сможет завершиться без необходимости ввода каких-либо данных.

Автоматический запуск установки

Для автоматического запуска установки необходимо выполнить следующие действия:

1. Открыть файл конфигурации загрузчика на PXE-сервере и добавить параметр `inst.ks=`.

- для систем с **BIOS** можно использовать файл **default** или путь, определяемый с помощью IP-адреса. В конец строки **append** необходимо добавить параметр `inst.ks=`:

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
...
APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp method=http://192.168.1.38/images/REDOS/
devfs=nomount inst.ks=http://192.168.1.38/ks.cfg
...
```

- для систем с **UEFI** параметр `inst.ks=` добавляется к строке **kernel** в файле **grub.cfg**:

```
kernel vmlinuz inst.ks=http://192.168.1.38/ks.cfg
```

Пример grub.cfg:

```
function load_video {
insmod efi_gop
insmod efi_uga
insmod video_bochs
insmod video_cirrus
insmod all_video
}
load_video
set gfxpayload=keep
insmod gzio
menuentry 'REDOS 7.3' {
linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp kernel vmlinuz inst.repo=http://192.168.1.38/images/REDOS/
inst.ks=http://192.168.1.38/ks.cfg
initrd images/REDOS/images/pxeboot/initrd.img
}
```

2. Загрузить программу установки с сервера PXE.

Если файл кикстарта не содержит ошибок, процесс установки сможет завершиться без необходимости ввода каких-либо данных.

Синтаксис кикстарта

Примечание.

Если за параметром следует знак равенства, необходимо определить его значение. В приведенных примерах параметры в квадратных скобках (**[ ]**) не являются обязательными.

Ниже будут рассмотрены основные необходимые команды для создания файла кикстарта.

Команды и интерпретаторы

bootloader

bootloader (обязательный) — определяет порядок установки загрузчика.

Параметры:

- **--append=** — содержит список параметров ядра (указываются через запятую), например:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

Параметры **rhgb** и **quiet** используются по умолчанию, даже если они явно не заданы, или строка `--append=` вовсе не определена.

- **--boot-drive=** — диск, на который будет записан загрузчик и с которого будет загружаться система.
- **--driveorder** — определяет порядок загрузки в BIOS, например:

```
bootloader --driveorder=sda,hda
```

- **--location=** — место расположения загрузочной записи. Допустимые значения:
  - *mbr* (используется по умолчанию) - его поведение определяется наличием MBR или GPT;
  - *partition* — установка загрузчика в первый сектор раздела, содержащего ядро;
  - *none* — не устанавливать загрузчик.

В большинстве случаев этот параметр можно не определять.

- **--password=** — пароль GRUB2. Рекомендуется установить пароль для ограничения доступа к оболочке GRUB2 во избежание несанкционированной передачи параметров ядру.

Если пароль задан, будет предложено ввести имя пользователя. По умолчанию будет выбран пользователь **root**.

- **--iscrypted** — разрешает использование зашифрованного пароля, который изначально был создан помощью параметра `--password=`. В противном случае пароль хранится в открытой форме.

Пароль можно зашифровать с помощью команды `grub2-mkpasswd-pbkdf2`. Скопируйте код из строки вывода, начинающейся с `grub.pbkdf2`, и сохраните его в файл кикстарта. Пример записи с зашифрованным паролем:

```
bootloader --iscrypted --
password=grub.pbkdf2.sha512.10000.5520C6C9832F3AC3D149AC0B24BE69E2D4FB0DBEEDBD2<...>95CA4BA4381F8550510B75E8E0BB2938990.
C688B6F0EF935701FF9BD1A8EC7FE5B<...>EA3384E56EB38A2E39102F5334C47405E
```

- **--timeout=** — время ожидания в секундах, по истечении которого начнется загрузка в соответствии с параметром `--default=`.
- **--default=** — определяет загрузочный образ, который будет использоваться по умолчанию.

clearpart

clearpart (дополнительный) — удаляет разделы с диска, прежде чем создавать новые. По умолчанию разделы не удаляются.

Параметры:

- **--all** — удаляет все разделы.
- **--drives=** — удаляет разделы на заданных дисках:

```
clearpart --drives=hda,hdb --all
```

- **--list=** — список разделов для удаления. Допускается выбор разделов на разных дисках. Этот параметр переопределяет **--all** и **--linux**.

```
clearpart --list=sda2,sda3,sdb1
```

- **--initlabel** — метка диска, которая будет выбираться по умолчанию для заданной архитектуры (например, msdos для x86).

Используется вместе с **--all**.

- **--linux** — удаляет разделы Linux.
- **--none** (по умолчанию) — не удалять разделы.

keyboard

keyboard (дополнительный) — выбор раскладки клавиатуры.

Параметры:

- **--vckeymap=** — определяет раскладку VConsole. В качестве значения можно выбирать имена файлов из **/usr/lib/kbd/keymaps/*** без расширения **.map.gz**.
- **--xlayouts=** — список раскладок X через запятую без пробелов. Значения можно определить в форме `<раскладка>` (например, cz) или `<раскладка_(вариант)>` (например, cz (qwerty)).

Полный список раскладок можно найти на справочной странице `xkeyboard-config(7)`, в секции **Layouts**.

- **--switch=** — комбинации клавиш для переключения между раскладками. Несколько значений разделяются запятыми без пробелов. Например, переключение раскладки клавиатуры сочетанием «*Alt+Shift*» выглядит следующим образом:

```
keyboard --xlayouts=us,ru --switch=grp:alt_shift_toggle
```

Описание дополнительных параметров можно найти на справочной странице `xkeyboard-config(7)`, в секции **Options**.

ВАЖНО!

Опции **--vckeymap=** и **--xlayouts=** не должны использоваться вместе.

lang

lang (обязательный) — определяет язык, который будет использоваться в ходе установки и по умолчанию — в установленной системе. Пример выбора английского языка:

```
lang en_US
```

Список кодов языков приведен в файле **/usr/share/system-config-language/locale-list**, в первом столбце.

Некоторые языки, в частности китайский, японский, корейский и языки индийской группы, не поддерживаются в текстовом режиме установки. Если такого рода язык задан с помощью команды **lang**, установка будет продолжена на английском, а указанный язык будет включен в готовой системе.

Параметры:

- **--addsupport=** — список дополнительных языков через запятую без пробелов.

```
lang en_US --addsupport=ru_RU,de_DE
```

logvol

logvol (дополнительный) — помогает создать логический том LVM.

Формат команды:

```
logvol <точка_монтирования> --vgname=<имя_группы> --size=<размер> --name=<имя> [<параметры>]
```

Параметры:

- **--noformat** — использует существующий логический том без форматирования.
- **--useexisting** — использует существующий логический том и повторно его форматирует.
- **--fstype=** — тип файловой системы: xfs, ext2, ext3, ext4, swap или vfat.
- **--fsoptions=** — строка параметров монтирования файловой системы, заключенная в кавычки. В готовой системе эта строка будет

записана в **/etc/fstab**.

- **--label=** — метка логического тома.
- **--grow** — увеличить размер логического тома до заданной величины или заполнить все свободное место.
- **--size=** — минимальный размер тома в мегабайтах.
- **--maxsize=** — максимально допустимый размер тома в мегабайтах. Укажите целое значение без единиц, например 500.
- **--resize** — изменение размера тома. Также надо будет определить параметры **--useexisting** и **--size**.
- **--percent=** — размер увеличения логического тома в процентной доле от доступного места в группе томов. Используется вместе с **--size** и **--grow**.

Сначала необходимо создать раздел, затем группу логических томов, а уже потом — логический том:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

network

network (дополнительный) — настройка сетевого окружения. По умолчанию будет включено первое указанное в команде устройство. Активацию конкретного устройства можно явно запросить с помощью **--activate**.

Параметры:

- **--activate** — отвечает за активацию устройства.

Если этот параметр указан применительно к уже активному устройству, будет выполнена его повторная активация согласно настройкам в файле кикстарта.

- **--nodefroute** — запрещает использовать стандартный маршрут.
- **--bootproto=** — может принимать одно из следующих значений: *dhcp* (используется по умолчанию), *bootp*, *static*.

В режиме DHCP для получения сетевых настроек используется DHCP-сервер. Как можно догадаться, в случае с BOOTP для получения сетевых настроек подобным образом используется сервер BOOTP. Чтобы настроить функции DHCP, добавьте:

```
network --bootproto=dhcp
```

Чтобы настроить получение сетевой конфигурации с помощью BOOTP, добавьте в файл кикстарта:

```
network --bootproto=bootp
```

Для метода **static** в файле кикстарта необходимо определить *IP*, *маску сети*, *шлюз* и *сервер имен*. Эти данные не изменяются и используются во время и после установки.

Все данные статической конфигурации должны быть указаны в одной строке.

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 --gateway=10.0.2.254 --nameserver=10.0.2.1
```

- **--device=** — сетевое устройство.

Если в первом вхождении команды network не указан параметр `--device=`, по умолчанию будет использоваться значение параметра загрузки `ksdevice=`. Это поведение считается устаревшим, поэтому рекомендуется явно определить значение `--device=`.

Для всех последующих команд **network** необходимо явно определить `--device=`.

Устройства могут быть заданы:

- по *имени* интерфейса, например eth0,
- по *MAC-адресу*, например 01:23:45:67:89:ab,
- по ключевому слову *link*, которое определяет первый интерфейс со статусом up.
- по ключевому слову *bootif* с целью наследования адреса MAC из переменной BOOTIF. Чтобы pxelinux смог определить переменную BOOTIF, включите **IPAPPEND 2** в файл **pxelinux.cfg**.

Например:

```
network --bootproto=dhcp --device=em1
```

- **--ip=** — адрес устройства.
- **--ipv6=** — IPv6-адрес устройства в формате `<адрес>[/<префикс> <длина>]`, например **3ffe:ffff:0:1::1/128**. Если префикс не задан, по умолчанию будет использоваться 64. Другие допустимые значения включают *auto* (автоматическая конфигурация) и *dhcp* (DHCPv6).
- **--gateway=** — IPv4-адрес шлюза.
- **--ipv6gateway=** — IPv6-адрес шлюза.
- **--nodefroute** — определяет, что выбранный интерфейс не может использоваться по умолчанию. Обычно устанавливается при активации дополнительных устройств с помощью `--activate=` — например для сетевой карты в другой подсети или цели iSCSI.
- **--nameserver=** — IP-адрес сервера имен. Несколько серверов разделяются запятыми.
- **--nodns** — не настраивать DNS-сервер.
- **--netmask=** — маска сети.
- **--hostname=** — имя устанавливаемой системы.
- **--wepkey=** — ключ WEP беспроводной сети.
- **--wpakey=** — ключ WPA беспроводной сети.
- **--onboot=** — активация устройства при загрузке.
- **--dhcpclass=** — класс DHCP.
- **--noipv4** — отключает IPv4.
- **--noipv6** — отключает IPv6.

part, partition

part, partition (обязательный) — отвечает за создание раздела.

> **ВАЖНО!**
>
> Если параметры **--noformat** и **--onpart** не определены, создаваемые разделы будут форматироваться в процессе установки.

Формат команды:

```
part|partition <точка_монтирования> --name=<имя> --device=<устройство> --rule=<правило> [<параметры>]
```

Параметры:

- параметр `<точка_монтирования>` может принимать следующие значения:
  - **/<путь>** - например: /, /usr, /home.
  - **swap** — раздел подкачки. Чтобы автоматически выбрать размер раздела подкачки, добавьте аргумент **--recommended**:

```
swap --recommended
```

Будет выбран подходящий, но не обязательно оптимальный размер.

  - **raid.id** — программный RAID-массив.
  - **pv.id** — раздел LVM.
  - **biosboot** — загрузочный раздел BIOS. На платформах с BIOS, использующих таблицу разделов GPT, необходимо создать загрузочный раздел размером 1 МБ. Именно в этот раздел будет установлен загрузчик. В системах с UEFI этот раздел не требуется. Подробную информацию см. в описании команды bootloader.
  - **efi** — системный раздел EFI. На платформах с UEFI необходимо создать раздел с минимальным размером 50 МБ (рекомендуется 200 МБ). В системах с BIOS этот раздел не требуется. Подробную информацию см. в описании команды `bootloader`.
- **--size=** — минимальный размер раздела в мегабайтах. Введите целое значение без указания единиц, например 500.

ВАЖНО!

Если значение **--size** недостаточно велико, установка будет прекращена.

- **--grow** — увеличить размер раздела до заданной величины или заполнить все свободное место.

Примечание.

Если для раздела подкачки определен параметр **--grow=** без **--maxsize=**, Anaconda ограничит его максимальный размер, руководствуясь следующими правилами: в системах с физической памятью **<2 ГБ** максимальный размер будет равен двойному объему памяти, а в системах с памятью **>2 ГБ** максимальный размер будет равен объему памяти плюс 2 ГБ.

- **--maxsize=** — максимальный размер раздела в мегабайтах. Укажите целое значение без единиц, например 500.
- **--noformat** — использует существующий логический том без форматирования. Используется вместе с **--onpart**.
- **--onpart=** или **--usepart=** — устройство, где будет создан раздел.

```
partition /home --onpart=hda1
```

Эта команда создаст раздел **/home** на **/dev/hda1**.

Пример создания раздела в пределах логического тома:

```
partition pv.1 --onpart=hda2
```

Устройство уже должно существовать.

- **--fsprofile** — определяет профиль для передачи программе создания файловой системы. Профиль содержит набор параметров файловой системы. Этот аргумент требует наличия файла конфигурации. Так, в файловых системах ext2, ext3, ext4 файл расположен в /etc/mke2fs.conf.
- **--fstype=** — тип файловой системы: xfs, ext2, ext3, ext4, swap, vfat, efi, biosboot.
- **--fsoptions=** — строка параметров монтирования файловой системы, заключенная в кавычки. В готовой системе эта строка будет записана в **/etc/fstab**.
- **--label=** — метка раздела.

rootpw

rootpw (обязательный) — позволяет установить пароль **root**.

Формат команды:

```
rootpw [--iscrypted|--plaintext] [--lock] <пароль>
```

Параметры:

- **--iscrypted** — сообщает, что пароль зашифрован. Параметры **--plaintext** и **--iscrypted** являются взаимоисключающими. Зашифровать пароль можно следующим образом:

```
python -c 'import crypt; print(crypt.crypt("my_password", crypt.mksalt(crypt.METHOD_SHA512)))'
```

Эта команда создаст шифр SHA512 с использованием заданной случайной строки.

- **--plaintext** — сообщает, что пароль определен в открытом виде. Параметры **--plaintext** и **--iscrypted** являются взаимоисключающими.
- **--lock** — блокирует учетную запись. Авторизация пользователя root из консоли будет недоступна.

timezone

timezone (обязательный) — устанавливает часовой пояс. Для просмотра полного списка часовых поясов выполните:

```
timedatectl list-timezones
```

Формат команды:

```
timezone <часовой_пояс> [<параметры>]
```

Параметры:

- **--utc** — если задан, подразумевается, что системные часы установлены по Гринвичу.
- **--nontp** — отключает автоматический запуск NTP.
- **--ntpservers** — список NTP-серверов через запятую без пробелов.

user

user (дополнительный) — создание пользователя.

Формат команды:

```
user --name=<пользователь> [<параметры>]
```

Параметры:

- **--username=** — обязательное имя пользователя.
- **--gecos=** — строка параметров GECOS через запятую. Типичные параметры включают полное имя пользователя, номер офиса, и т.п. Подробную информацию можно найти на справочной странице passwd(5).
- **--groups=** — список групп пользователя, разделенных запятой. Список должен содержать существующие группы (см. описание команды **group**).
- **--homedir=** — домашний каталог пользователя. По умолчанию используется /home/пользователь.
- **--lock** — блокирует учетную запись, то есть пользователи не смогут авторизоваться из консоли.
- **--password=** — пароль пользователя. Если не задан, учетная запись будет заблокирована.
- **--shell=** — оболочка пользователя. По умолчанию используются системные настройки.

volgroup

volgroup (дополнительный) — создание группы LVM.

Формат команды:

```
volgroup <имя> <раздел> [<параметры>]
```

Параметры:

- **--noformat** — использует существующую группу томов без форматирования.
- **--useexisting** — использует существующую группу томов и повторно ее форматирует.
- **--pesize=** — размер физических экстентов.
- **--reserved-space**= — размер пространства в мегабайтах, которое должно быть зарезервировано в группе томов. Применимо только к новым группам томов.
- **--reserved-percent=** — процентная доля пространства, зарезервированного в группе томов.

Пример создания раздела, группы логических томов и отдельного тома:

```
part pv.01 --size 10000
volgroup volgrp pv.01
logvol / --vgname=volgrp --size=2000 --name=root
```

xconfig

xconfig (дополнительный) — настраивает X Window System. Если в файле кикстарта есть запись для установки X, но нет команды **xconfig**, настройки X потребуется определить вручную.

Не следует добавлять эту команду в файл кикстарта, если вы не планируете устанавливать X Window System.

Параметры:

- **--defaultdesktop=** — рабочее окружение. Чтобы выбрать графическое окружение, необходимо, чтобы они также присутствовали в секции **%packages**.
- **--startxonboot** — графическая авторизация в установленной системе.

Секция %packages

Команда **%packages** отмечает начало секции устанавливаемых пакетов.

В этой секции можно указать отдельный пакет, группу или целое окружение.

Список групп и окружений можно найти в файле **repodata/*-comps-Everything.<архитектура>.xml** на установочном образе РЕД ОС.

В ***-comps-Everything.<архитектура>.xml** окружения отмечены тегом **<environment>**, а группы — тегом <group>. Каждая запись имеет свой идентификатор, признак отображения для пользователей, название, описание и список пакетов. Пакеты, отмеченные в как обязательные (mandatory), будут всегда устанавливаться при установке группы, пакеты **default** автоматически выбираются при выборе группы, а пакеты **optional** должны быть заданы явно.

Группы и окружения можно выбрать по имени (тег **<name>**) и идентификатору (тег **<id>**).

ВАЖНО!

Если в процессе установки не была установлена X Window System и не включены возможности графической авторизации, то после перезагрузки этап первоначальной настройки будет пропущен, и только пользователь root сможет авторизоваться в системе. Чтобы создать другие учетные записи, то прежде чем приступить к установке других систем, добавьте параметр user в файл кикстарта или авторизуйтесь как root в виртуальной консоли и добавьте пользователей вручную с помощью команды adduser.

Секция **%packages** должна завершаться директивой **%end**.

Выбор окружения

Секция **%packages** может содержать не только пакеты, но и целые окружения.

```
%packages
@^desktop-environment
%end
```

Данный фрагмент установит окружение desktop-environment - рабочая станция с графическим окружением **Mate**. Файл кикстарта должен содержать только одно окружение.

Выбор групп

В каждой строке определяется по одной группе, начиная со знака **@**. Имена групп должны соответствовать записям в файле ***-comps-Everything.<архитектура>.xml**.

```
%packages
@X Window System
@Development Tools
@Smart Card Support
%end
```

Основные группы пакетов будут выбраны по умолчанию, поэтому их не надо указывать в разделе **%packages**.

Выбор отдельных пакетов

Отдельные пакеты вводятся по одному в строке. Допускается использование шаблонов (*), например:

```
%packages
sqlite
curl
```

```
aspell
docbook*
%end
```

В примере запись **docbook*** охватывает пакеты **docbook-dtds**, **docbook-simple**, **docbook-slides** и т.п.

Исключение окружений, групп и пакетов

Добавление дефиса перед именем пакетов и групп исключает их из списка установки:

```
%packages
-@Graphical Internet
-autofs
-ipa*fonts
%end
```

ВАЖНО!

Установка всех доступных пакетов с использованием только символа * в файле кикстарта **не допускается**.

Поведение секции **%packages** можно контролировать с помощью параметров.

Общие параметры выбора пакетов

Ниже перечислены параметры секции **%packages**. Параметры добавляются в конец заголовка секции, например:

```
%packages --multilib --ignoremissing
```

Параметры:

- **--nobase** — не устанавливает группу **@base**. Используется, если целью является создание компактной системы.
- **--ignoremissing** — игнорирует недостающие пакеты вместо того, чтобы приостановить установку и ожидать подтверждения продолжения.
- **--excludedocs** — исключает документацию пакетов. В большинстве случаев это означает исключение файлов из **/usr/share/doc***.
- **--multilib** — разрешает установку 32-битных пакетов в 64-битных системах.

Обычно на платформах AMD64 и Intel 64 по умолчанию устанавливаются пакеты, предназначенные для заданной архитектуры (например, **x86_64**) и стандартные пакеты (**noarch**). Однако данный параметр разрешает установку 32-битных пакетов (**i686**).

Этот подход применим только к пакетам в секции **%packages**. Если же пакет участвует в решении зависимостей, будет установлена только необходимая версия.

Параметры для отдельных групп

Чтобы определить параметры для конкретной группы пакетов, надо добавить их после названия группы.

```
%packages
@Internet Applications --optional
%end
```

Параметры:

- **--nodefaults** — устанавливает только обязательные пакеты, а не стандартный набор.
- **--optional** — установка дополнительных пакетов группы согласно списку в ***-comps-Everything.<архитектура>.xml**.

Секция %pre

В секции **%pre** определяются команды, которые будут выполняться сразу после обработки файла кикстарта, но до начала установки.

Секция должна располагаться ближе к концу файла, начинаться с директивы **%pre** и заканчиваться директивой **%end**. Порядок

секций **%pre** и **%post** не имеет значения.

В секции **%pre** можно обращаться к сети, но так как на данном этапе служба имен еще не настроена, следует использовать IP-адреса.

> **Примечание.**
>
> Сценарий **%pre** не выполняется в окружении **chroot** в отличие от **%post**.

Ниже перечислены параметры **%pre**. Они добавляются в конец заголовка секции:

```
%pre --interpreter=/usr/bin/bash
--- <исполняемый_скрипт> --
%end
```

Параметры:

- **--interpreter=** — язык сценариев, например **/usr/bin/sh**, **/usr/bin/bash** или **/usr/bin/python**.
- **--erroronfail** — при сбое сценария показывает сообщение об ошибке и прерывает установку.
- **--log**= — вывод сообщений сценария в заданный файл:

```
%pre --log=/mnt/sysimage/root/ks-pre.log
```

Секция %post

В секции **%post** определяются команды, которые будут выполняться после установки, но до перезагрузки системы. Эта секция должна располагаться после секции команд ближе к концу файла, начинаться с директивы **%post** и заканчиваться директивой **%end**. Порядок секций **%pre** и **%post** не имеет значения.

В этой секции можно установить дополнительные программы или настроить сервер имен. Сценарий **%post** выполняется в окружении **chroot**, поэтому некоторые задачи (такие как копирование сценариев и пакетов с установочных носителей) выполнить не удастся. Это поведение можно изменить с помощью **--nochroot**.

> **ВАЖНО!**
>
> Если вы используете статическую настройку IP, в секции **%post** можно обращаться к сети с разрешением IP-адресов. Если используется DHCP, файл **/etc/resolv.conf** еще не будет сформирован к моменту обработки **%post**, поэтому при обращении к сети необходимо использовать IP-адреса.

Ниже перечислены параметры **%post**. Параметры добавляются в конец заголовка секции:

```
%post --interpreter=/usr/bin/bash
--- <исполняемый_скрипт> ---
%end
```

Параметры:

- **--interpreter=** — определяет язык сценариев, например **bash**.

```
%post --interpreter=/usr/bin/python
```

Здесь можно указать любой установленный язык, например **/usr/bin/sh**, **/usr/bin/bash** или **/usr/bin/python**.

- **--nochroot** - позволяет определить команды для выполнения вне окружения **chroot**.

В следующем примере файл **/etc/resolv.conf** будет скопирован в созданную файловую систему.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
%end
```

- **--erroronfail** — при сбое сценария показывает сообщение об ошибке и прерывает установку.
- **--log=** — сохраняет протокол выполнения сценария в файл. Путь должен учитывать наличие **--nochroot**. Пример без **--nochroot**:

```
%post --log=/root/ks-post.log
```

Пример с **--nochroot**:

```
%post --nochroot --log=/mnt/sysimage/root/ks-post.log
```

Пример файла конфигурации

Стандартный файл кикстарта (шаблон) имеет следующее содержимое:

```
# Generated by Anaconda 33.25.4
# Generated by pykickstart v3.30
# Use graphical install
graphical


%packages --multilib
@^desktop-environment

%end

# Keyboard layouts
keyboard --xlayouts='us','ru' --switch='grp:alt_shift_toggle'
# System language
lang ru_RU.UTF-8

# Network information
network  --bootproto=dhcp --device=ens18 --ipv6=auto --activate
network  --hostname=localhost.localdomain

# Use CDROM installation media
cdrom

# Run the Setup Agent on first boot
firstboot --enable

# Generated using Blivet version 3.3.0
ignoredisk --only-use=sda
autopart
# Partition clearing information
clearpart --none --initlabel

# System timezone
timezone Europe/Moscow --utc

# Root password
rootpw --iscrypted
$6$3zZ3MWYmRB5UU2Nb$f7ZKDB1tQJ/9Q4VRoRVvFfqK8DBjO8.HO9AZ8nTOvhPeJ3JNBKBJ7lO.UFqH4fWykCE.Emiie1JHCvIq1Nhgu1
user --groups=wheel --name=user --
password=$6$AywHyJ1Jw8ffZbCs$642L93KbjyltoS79aJs1Vng8IjMs.UlBcnzoC0TaBxMs4/ULbYOTRLejpPXDiW20/c5xIs7JwYwIi.ep2P7Yi/ --
iscrypted --gecos="user"
```

Подготовка PXE-сервера для развертывания РЕД ОС с загрузкой в UEFI или Legacy в РЕД ОС 8

Вы можете подробнее ознакомиться с информацией по установке и настройке PXE-сервера, просмотрев наши обучающие видео:

- на **RuTube** — Настройка PXE с аутентификацией и KICKSTART;
- в **Яндекс.Дзен** — Настройка PXE с аутентификацией и KICKSTART;
- в **VK Видео** — Настройка PXE с аутентификацией и KICKSTART.

На наших каналах вы также сможете найти много другой полезной информации.

1. Сначала установите необходимые пакеты на сервер. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install dhcp-server tftp-server syslinux httpd dnf-plugins-core
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

2. Создайте следующие каталоги:

```
mkdir /var/lib/tftpboot/pxelinux.cfg
mkdir /var/lib/tftpboot/uefi
mkdir -p /var/lib/tftpboot/images/REDOS
```

3. Следующей командой скопируйте файлы для запуска установки РЕД ОС в режиме **legacy** через **PXE**:

```
cp /usr/share/syslinux/{chain.c32,mboot.c32,memdisk,menu.c32,pxelinux.0,ldlinux.c32,libutil.c32} /var/lib/tftpboot/
chmod 777 /var/lib/tftpboot/pxelinux.0
```

4. Скопируйте файлы для **UEFI** режима установки РЕД ОС в каталог **/var/lib/tftpboot/uefi**.

Для этого выполните последовательность команд:

```
dnf download shim-x64 grub2-efi-x64 --downloaddir=/root/
cd /root/
rpm2cpio shim-x64-*.rpm | cpio -dimv
rpm2cpio grub2-efi-x64-*.rpm | cpio -dimv
cp ./boot/efi/EFI/BOOT/BOOTX64.EFI /var/lib/tftpboot/uefi
cp ./boot/efi/EFI/redos/grubx64.efi /var/lib/tftpboot/uefi

chmod 777 /var/lib/tftpboot/uefi/*.*
```

5. Подключите загрузочный USB-носитель с РЕД ОС 8 и скопируйте его содержимое в каталог **/var/lib/tftpboot/images/REDOS**:

```
cp -vR "/run/media/user/redos-Everything-DVD-x86_64-8/." /var/lib/tftpboot/images/REDOS
```

Также возможен вариант копирования из iso-образа.

Смонтируйте образ:

```
mount -t iso9660 -o loop redos-MUROM-8-Everything-x86_64-DVD1.iso /mnt/
```

Скопируйте все содержимое в каталог **/var/lib/tftpboot/images/REDOS/**:

```
cp -vR /mnt/* /var/lib/tftpboot/images/REDOS/
```

Размонтируйте образ:

```
umount /mnt/
```

6. Конфигурирование DHCP-сервера.

В файле **/etc/dhcp/dhcpd.conf** укажите свои значение для вашей подсети, а именно шлюз и выдаваемый диапазон IP-адресов. Параметру next-server назначается IP-адрес DHCP-сервера.

Зеленым цветом выделены сетевые параметры для изменения под вашу конфигурацию сети.

```
nano /etc/dhcp/dhcpd.conf
```

```
non-authoritative;
 allow bootp;
 option space pxelinux;
 option pxelinux.magic code 208 = string;
 option pxelinux.configfile code 209 = text;
 option pxelinux.pathprefix code 210 = text;
 option pxelinux.reboottime code 211 = unsigned integer 32;
 option architecture-type code 93 = unsigned integer 16;
 subnet 192.168.2.0 netmask 255.255.255.0 {
 option routers 192.168.2.1;
 range 192.168.2.70 192.168.2.80;
 class "pxeclients" {
 match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
 next-server 192.168.2.10;
 if option architecture-type = 00:07 {
 filename "uefi/grubx64.efi";
 }
 else {
 filename "pxelinux.0";
 }
 }
 }
```

Запустите службу **dhcpd**:

```
systemctl enable dhcpd --now
```

7.1 Создайте загрузочное меню для установки в режиме **legacy** с использованием **PXE**:

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
default menu.c32
 PROMPT 0
 TIMEOUT 150
 MENU TITLE PXE Menu
 LABEL REDOS 8
 MENU LABEL REDOS 8
 KERNEL images/REDOS/images/pxeboot/vmlinuz
 APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp inst.repo=http://192.168.2.10/images/REDOS/
```

7.2 Создайте загрузочное меню для установки в режиме **UEFI** с использованием **PXE**:

```
nano /var/lib/tftpboot/uefi/grub.cfg
```

```
function load_video {
 insmod efi_gop
 insmod efi_uga
 insmod video_bochs
 insmod video_cirrus
 insmod all_video
 }
 load_video
 set gfxpayload=keep
 insmod gzio
 menuentry 'REDOS 8' {
```

```
linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp inst.repo=http://192.168.2.10/images/REDOS/
initrd images/REDOS/images/pxeboot/initrd.img
}
```

8. Конфигурирование web-сервера **httpd**.

WEB-сервер используется для публикации файлов дистрибутива РЕД ОС в локальной сети.

Создайте файл:

```
nano /etc/httpd/conf.d/pxeboot.conf
```

```
Alias /images /var/lib/tftpboot/images
 <Directory /var/lib/tftpboot/images>
 Options Indexes FollowSymLinks
 Require ip 127.0.0.1 192.168.2.0/24
 </Directory>
```

Настройте SELinux:

```
chcon -R -t httpd_sys_content_t /var/lib/tftpboot/images
```

Запустите службу **httpd**:

```
systemctl enable httpd --now
```

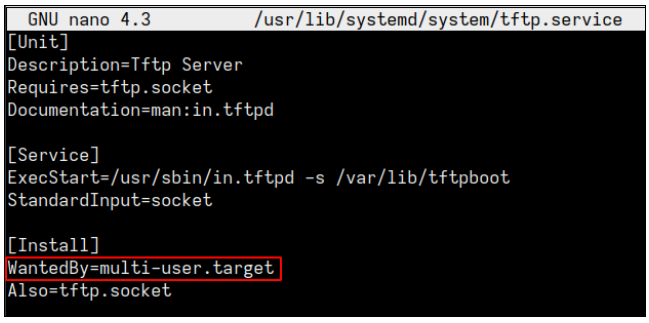
9. Настройка и запуск службы **tftp**.

Откройте файл:

```
nano /usr/lib/systemd/system/tftp.service
```

и добавьте строку в секцию [**Install**]:

```
WantedBy=multi-user.target
```



Откройте файл:

```
nano /usr/lib/systemd/system/tftp.socket
```

измените строку `ListenDatagram=69` на `ListenDatagram=0.0.0.0:69`, чтобы запустить **tftp** на **69** порту по IPv4-протоколу. По умолчанию порт публикуется на IPv6.

```
[Unit]
 Description=Tftp Server Activation Socket

 [Socket]
 ListenDatagram=0.0.0.0:69

 [Install]
 WantedBy=sockets.target
```

После изменения модулей **systemd** их нужно инициализировать:

```
systemctl daemon-reload
```

Добавьте службу **tftp** в автозапуск:

```
systemctl enable tftp --now
```

Если в системе используется **firewalld**, дополнительно необходимо выполнить его настройку:

```
firewall-cmd --add-service=tftp
firewall-cmd --add-service=http
firewall-cmd --runtime-to-permanent
```

Настройка установки РЕД ОС по PXE через VNC в РЕД ОС 8

Подготовка рабочей станции

Для установки ОС на рабочей станции выбираем загрузку по сети: «**Network Boot Agent**» или «**PXE boot**».

> **ВАЖНО!**
>
> Необходимо, чтобы загрузка по PXE была активирована в **BIOS**. Настройка может называться по-разному, в зависимости от версии BIOS и производителя материнской платы. Необходимо ознакомиться со спецификацией на конкретную материнскую плату.

Настройка установки РЕД ОС по PXE через VNC

Создайте файл меню со следующим содержимым:

- для систем, использующих **BIOS**:

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
default menu.c32
 PROMPT 0
 TIMEOUT 150
 MENU TITLE PXE Menu
 LABEL REDOS 7.3
 MENU LABEL REDOS 7.3
 MENU PASSWD $1$15opgKTx$dP/IaLNiCbfECiC2KPkDC0
 KERNEL images/REDOS/images/pxeboot/vmlinuz
 APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp inst.repo=http://192.168.1.38/images/REDOS/
devfs=nomount inst.vnc inst.vncpassword=password
```

- для систем, использующих **UEFI**:

```
nano /var/lib/tftpboot/uefi/grub.cfg
```

```
function load_video {
 insmod efi_gop
 insmod efi_uga
 insmod video_bochs
 insmod video_cirrus
 insmod all_video
 }
 load_video
 set gfxpayload=keep
 insmod gzio
 menuentry 'REDOS 8' {
 linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp inst.repo=http://192.168.2.10/images/REDOS/ inst.vnc inst.vncpassword=password
 initrd images/REDOS/images/pxeboot/initrd.img
 }
```

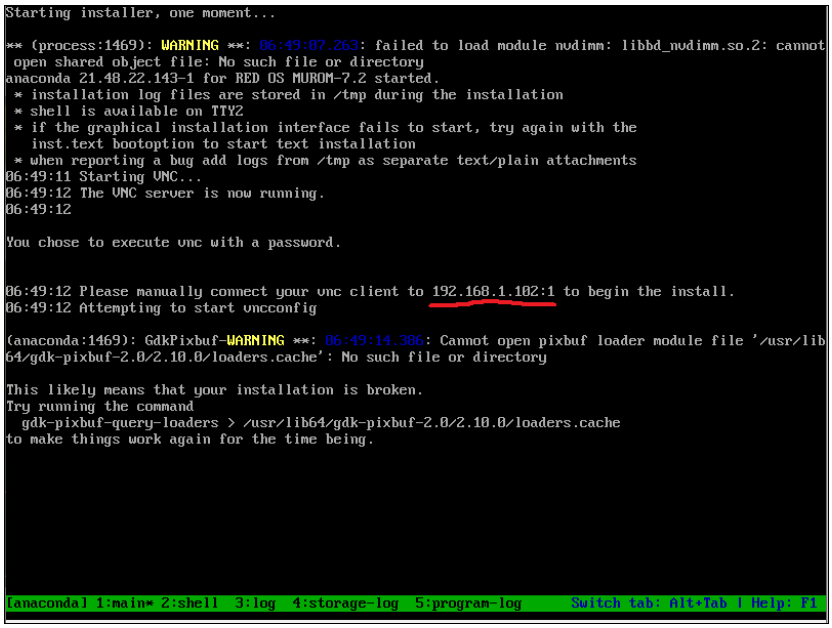
В данном файле конфигурации параметр **TIMEOUT 150** - счётчик времени, после которого будет запущена установка автоматически.

Параметры в конце строки **APPEND**:

```
inst.vnc inst.vncpassword=password
```

дают возможность подключиться по протоколу **VNC**, для удалённой настройки установки РЕД ОС, зная IP-адрес машины, порт и заданный пароль.

IP-адрес можно увидеть после того, как произойдёт первичная загрузка сервисов после меню:

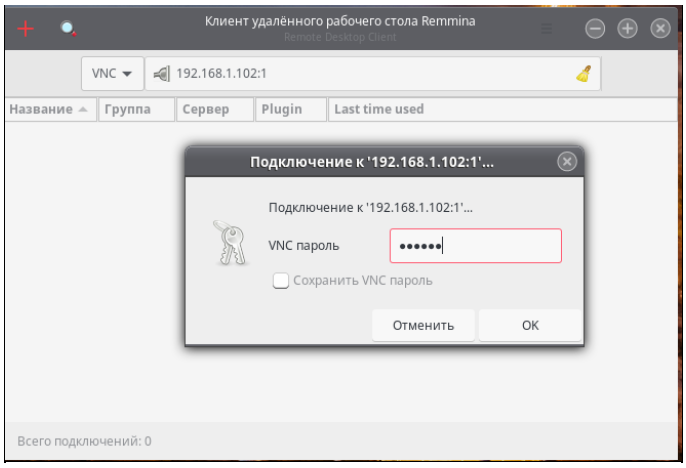


Вместо этих параметров можно указать:

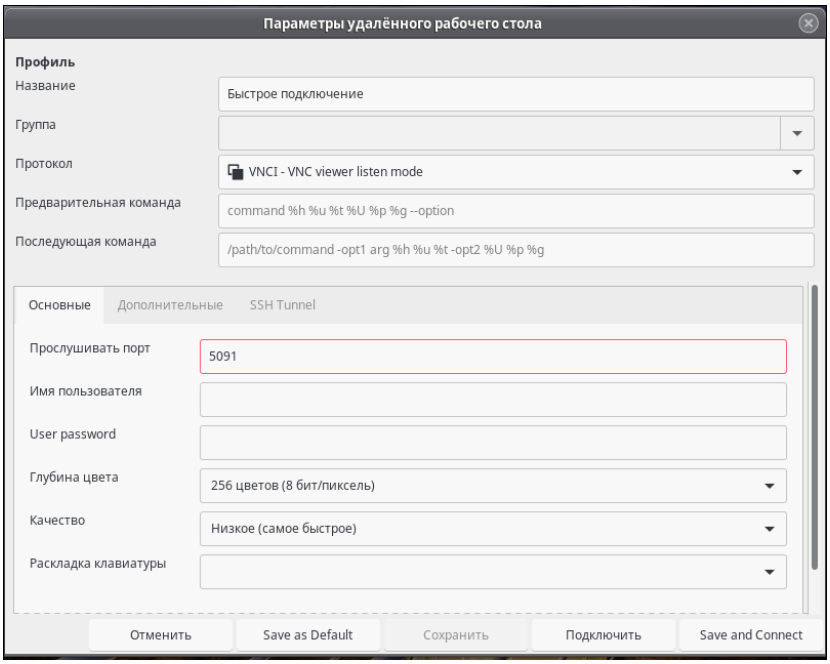
```
inst.vnc inst.vncconnect=<узел>:<порт>
```

Где **<узел>**:**<порт>** - это заранее известные ip-адрес и порт машины, с которой будет производиться настройка установки.

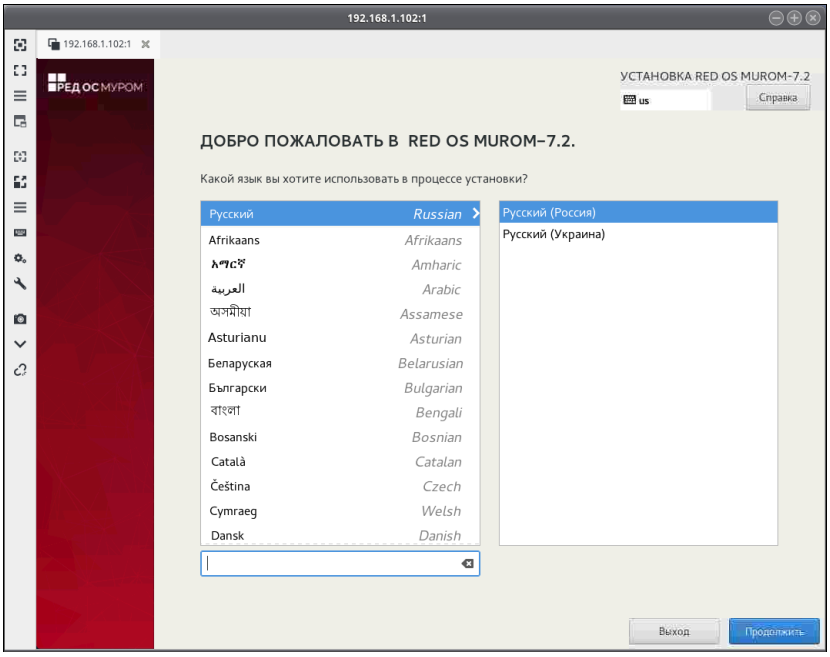
После того, как эти параметры заданы, на удалённой машине нужно запустить VNC-клиент «**Меню**» - «**Интернет**» - «**Remmina**», выбрать тип подключения **VNC** и ввести <**IP-адрес**>:<**порт**>. После этого придёт запрос пароля:



В случае, когда был настроен конкретный удалённый компьютер для контроля установки, в *Remmina* нажмите на кнопку «**Плюс**» слева вверху и введите настройки порта, на котором он будет ждать запрос:



Если всё настроено верно, то в итоге мы получим возможность удалённой настройки подключившись по **vnc**:



ВАЖНО!

РЕД ОС, установленная через VNC, по умолчанию запускается в текстовом режиме. Для включения графического режима воспользуйтесь нашей инструкцией «Установка графической оболочки в РЕД ОС 8».

Установка РЕД ОС на один диск с ОС Windows (dual-boot)

Выделение дискового пространства
Настройка BIOS

Примечание.

Данная инструкция носит исключительно рекомендательный характер. Данная инструкция описывает общую процедуру установки РЕД ОС 8 рядом с ОС Windows 10, без учёта различий возможных конфигураций аппаратного и программного обеспечения ПК, а также вносимых ими изменений, способных повлиять на работоспособность систем.

ВАЖНО!

В некоторых случаях для установки и работы РЕД ОС необходимо обновление **BIOS/UEFI** компьютера.

Вы можете подробнее ознакомиться с возможностью установки РЕД ОС на один диск с ОС Windows, просмотрев наши обучающие видео:

- на **RuTube** — Запись iso-образа РЕД ОС и установка рядом с Windows;
- в **Яндекс.Дзен** — Запись iso-образа РЕД ОС и установка рядом с Windows;
- в **VK Видео** — Запись iso-образа РЕД ОС и установка рядом с Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Выделение дискового пространства

ВАЖНО!

Перед началом работы с разделами жёстких дисков создайте резервную копию важных данных. При работе с несистемным разделом, например, D, E, F и т. д., достаточно просто скопировать файлы оттуда.

При необходимости наличия двух операционных систем (Windows и Linux) на компьютере пользователя, необходимо выделить отдельный раздел на жёстком диске для установки РЕД ОС.

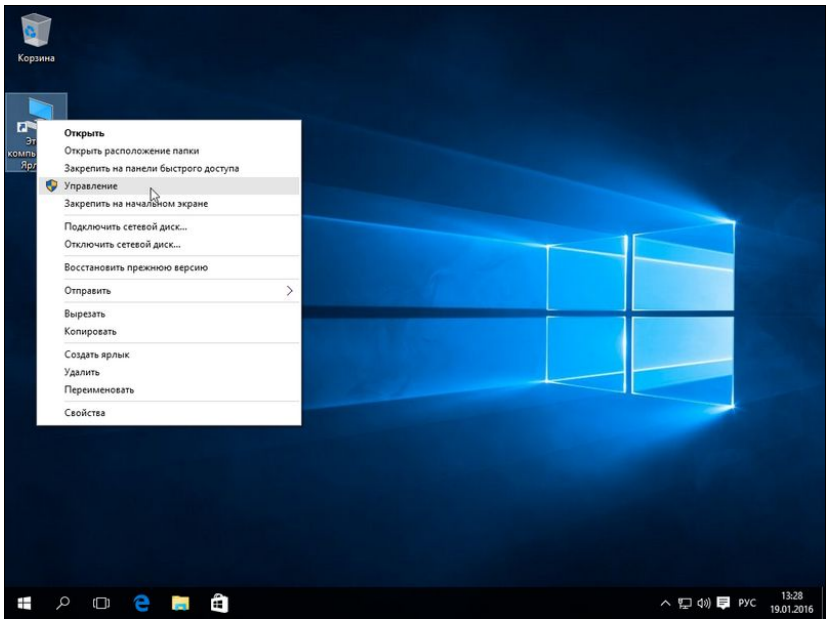
ВАЖНО!

Более корректным вариантом для организации **dual-boot** является использование отдельного жёсткого диска для установки РЕД ОС.

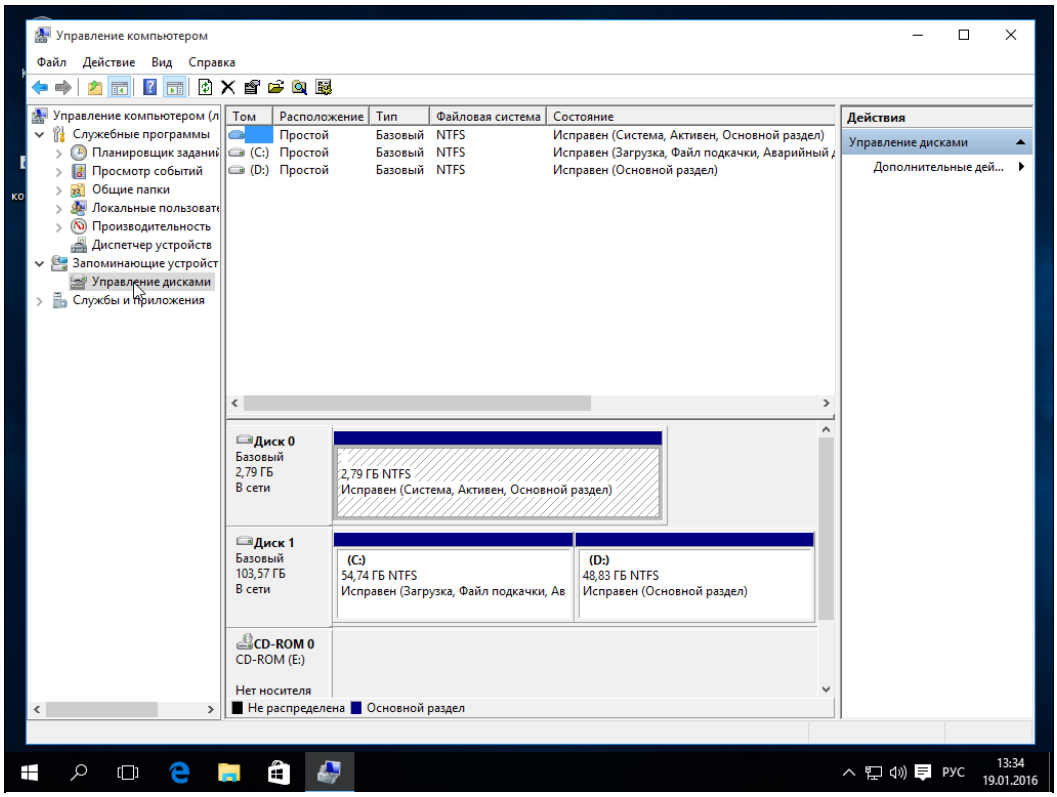
Имеется много вариантов для работы с разделами жёстких дисков (создание, удаление, форматирование). Это можно реализовать, как средствами специализированного ПО, так и средствами утилиты «**Управление дисками**» в составе операционной системы Windows.

В данной инструкции будет рассмотрен метод создания отдельного раздела на жёстком диске средствами утилиты «**Управление дисками**».

Кликните правой кнопкой мыши по значку «**Этот компьютер**» на рабочем столе и откройте пункт меню « **Управление**».

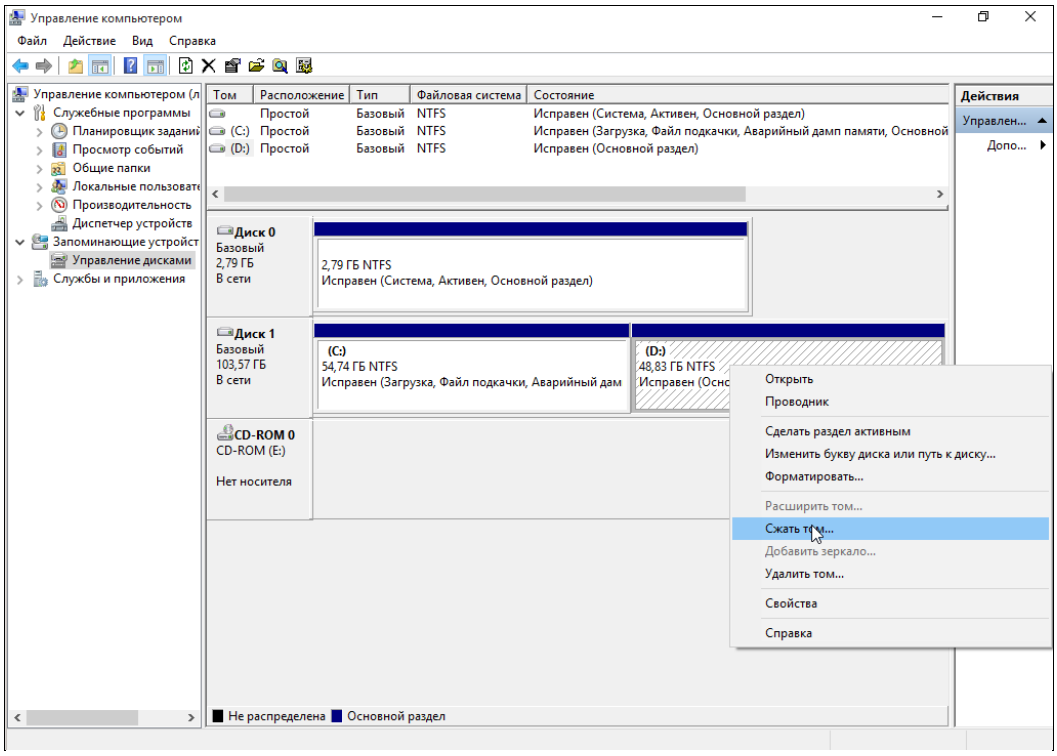


Далее работа производится в утилите «**Управление дисками**».

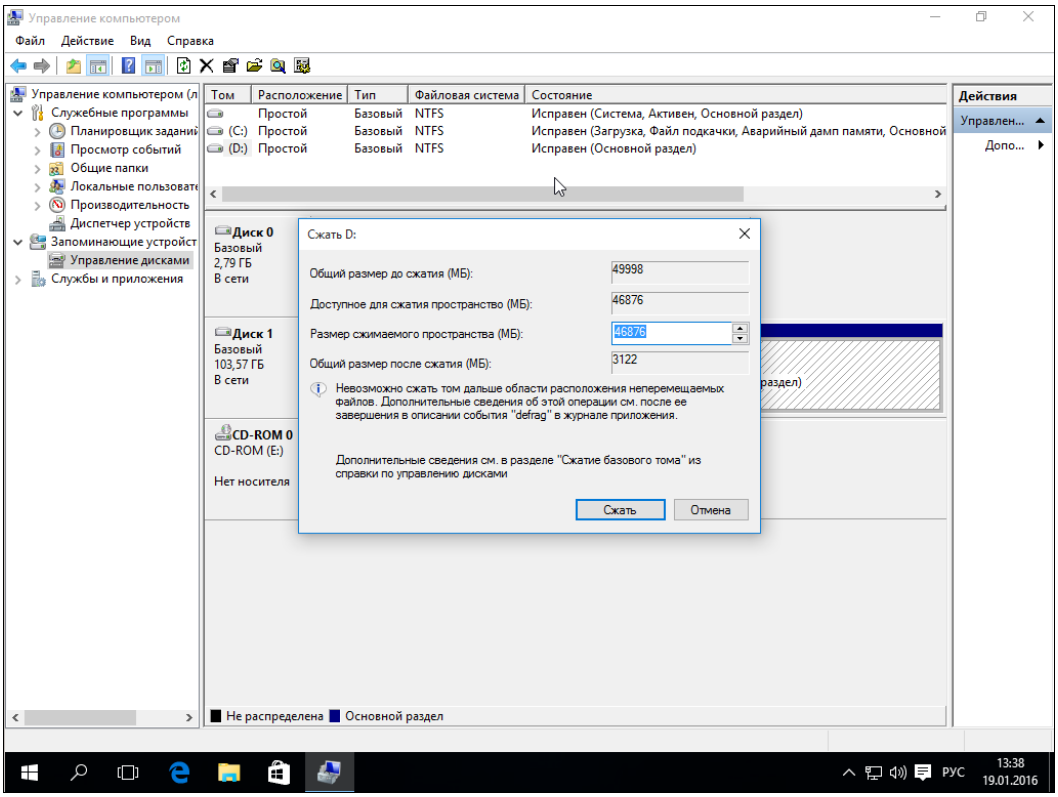


Внизу окна есть два диска: **C** (системный) и **D**. Рассмотрим пример изменения размера диска **D**.

Кликните по нужному диску правой кнопкой мыши и выберите опцию «**Сжать том**».

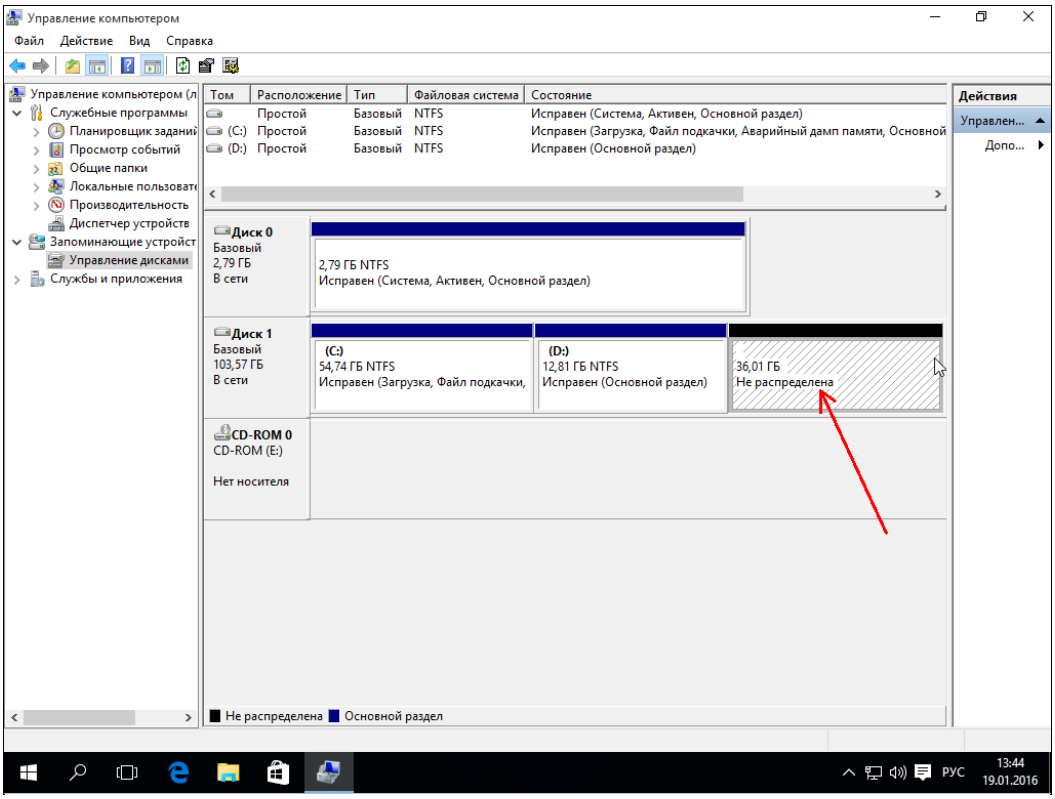


Откроется окно, в котором необходимо ввести размер создаваемого тома в поле «**Размер сжимаемого пространства**».



Обратите внимание, что вы не можете указать размер нового раздела больше, чем количество свободного места на диске.

Нажмите на кнопку «**Сжать**». После этого появится неразмеченное пространство, которое можно будет использовать для установки РЕД ОС.



Настройка BIOS

Перед установкой РЕД ОС необходимо настроить **BIOS** рабочей станции, на которую производится установка ОС, на загрузку с подготовленного флеш-накопителя. Для этого необходимо включить в **BIOS** рабочей станции опцию загрузки с CD/DVD-привода. Способ входа в меню **BIOS** и расположение конкретных настроек может отличаться, в зависимости от используемой материнской платы. Чаще всего для входа в **BIOS** необходимо нажать функциональную клавишу **Delete** на стационарных рабочих станциях или функциональную клавишу **F1** (**F9**) на мобильных рабочих станциях (ноутбуках) в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.

Также предварительно отключите в **BIOS** параметр **Secure Boot**, т. к. он может помешать нормальной установке и загрузке РЕД ОС.

Установка системы производится в штатном режиме согласно «Обзор установки».

Обратите внимание, что в меню выбора расположения установки РЕД ОС необходимо выбрать выделенный раздел диска или дополнительно выделенный диск.

При выборе разметки диска «**По-своему**», раздел с установленной ОС Windows будет отображаться как «**Неизвестный**» раздел. Не рекомендуется производить над данным разделом какие-либо действия посредством установщика РЕД ОС, т. к. это может привести к проблемам загрузки или полной неработоспособности установленной ОС Windows.

После завершения установки выберите в настройках **BIOS** основным загрузочным устройством жёсткий диск вашего ПК и загрузите его.

Иногда (в зависимости от производителя ПК и используемом в нём **BIOS/UEFI**) возникает необходимость в самостоятельном указании в **BIOS/UEFI** компьютера загрузчика РЕД ОС в качестве загрузчика по умолчанию, т. к. **Windows Boot Manager**, оставшись загрузчиком по умолчанию, автоматически запустит ОС Windows, не предоставив возможности выбора загрузки необходимой ОС.

На этом установка и настройка РЕД ОС завершена, и система полностью готова к использованию.

ВАЖНО!

Если вы планируете установку ОС Windows **после** установки РЕД ОС, учтите, что перезапись загрузчика **Windows Boot Manager** приведёт к нарушению корректной работы загрузчика **GRUB** и невозможности загрузки РЕД ОС.

Для решения данной проблемы необходимо восстановить **GRUB**. Подробную информацию о восстановлении загрузчика **GRUB** см. в нашей статье «**Восстановление загрузчика GRUB2**».

Загрузка РЕД ОС в SecureBoot-режиме

Для запуска РЕД ОС в **SecureBoot**-режиме необходимо произвести импорт сертификата в **BIOS**.

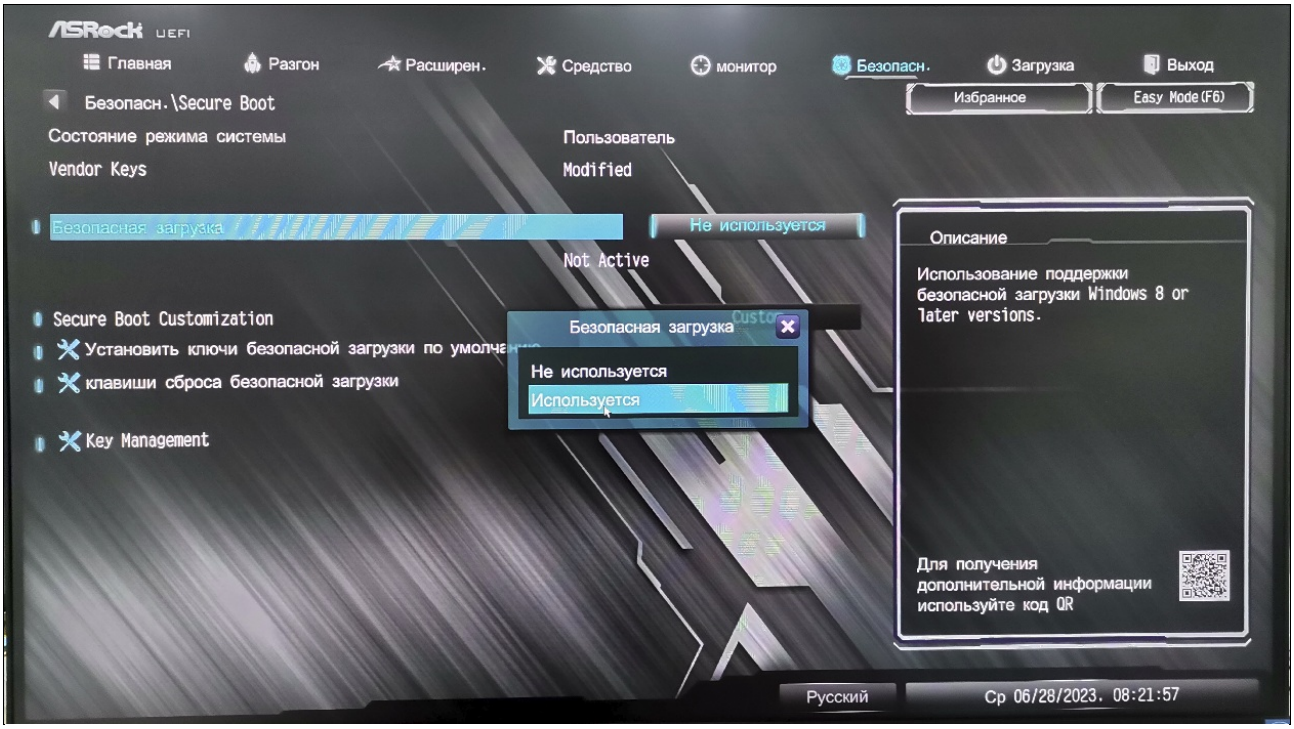
В данной статье рассмотрен общий случай настройки **BIOS**, т.к. настройка **BIOS** для разных производителей материнских плат может отличаться.

Запустите **BIOS**. Чаще всего для входа в **BIOS** необходимо нажать функциональную клавишу **Delete** на стационарных рабочих станциях или функциональную клавишу **F1** (**F9**) на мобильных рабочих станциях (ноутбуках) в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.

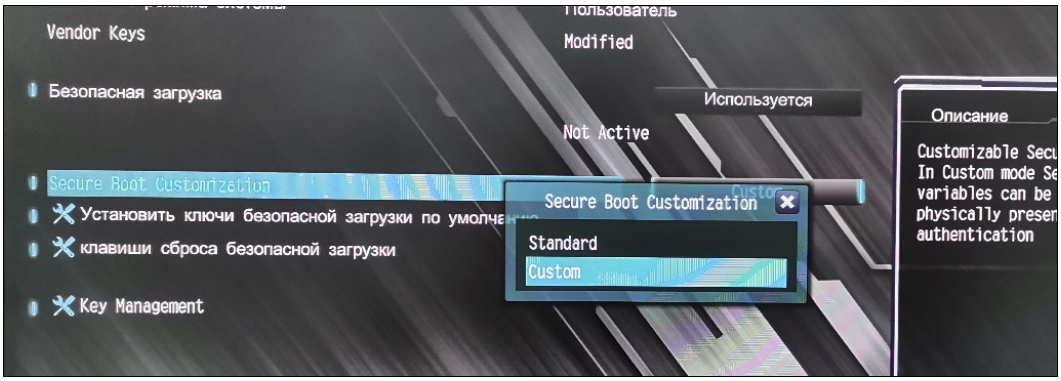
Перейдите в **Расширенный режим BIOS** (**Advanced Mode**).



В секции **Безопасность** необходимо активировать **SecureBoot**, если он выключен.



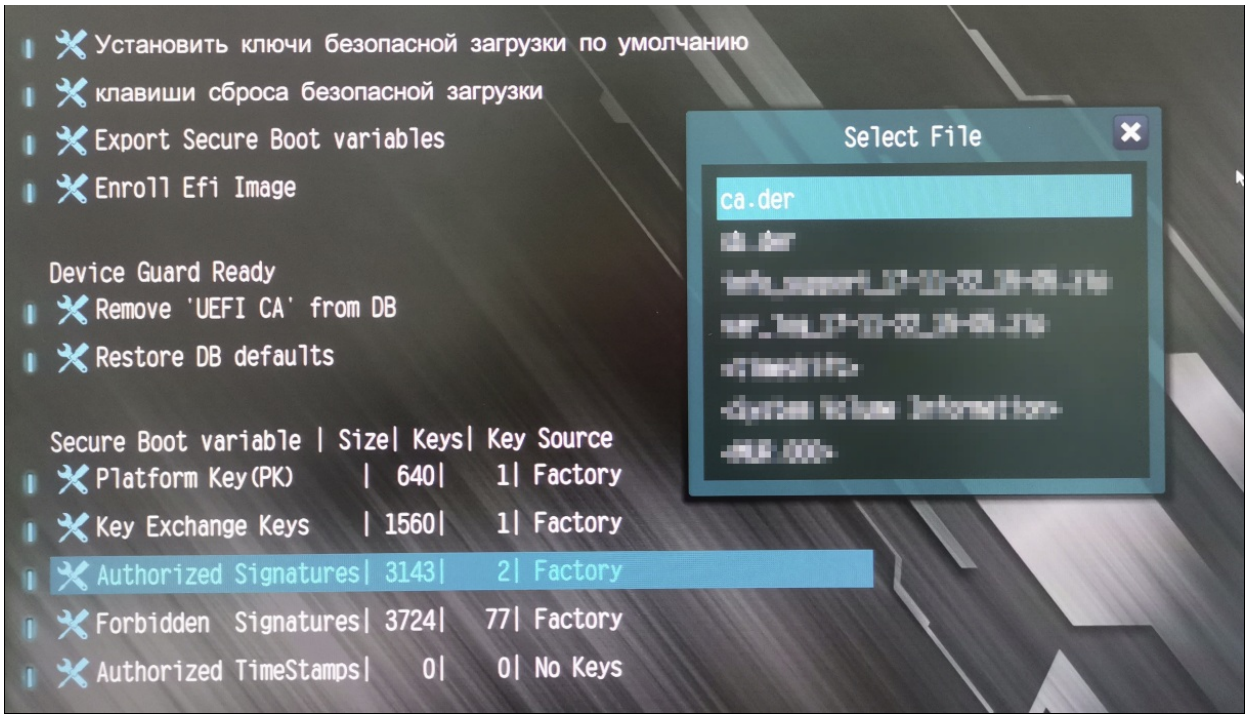
Далее необходимо переключить значение параметра **Secure Boot Customization** в **custom**, для того чтобы **BIOS** при загрузке считывал не только стандартные сертификаты.



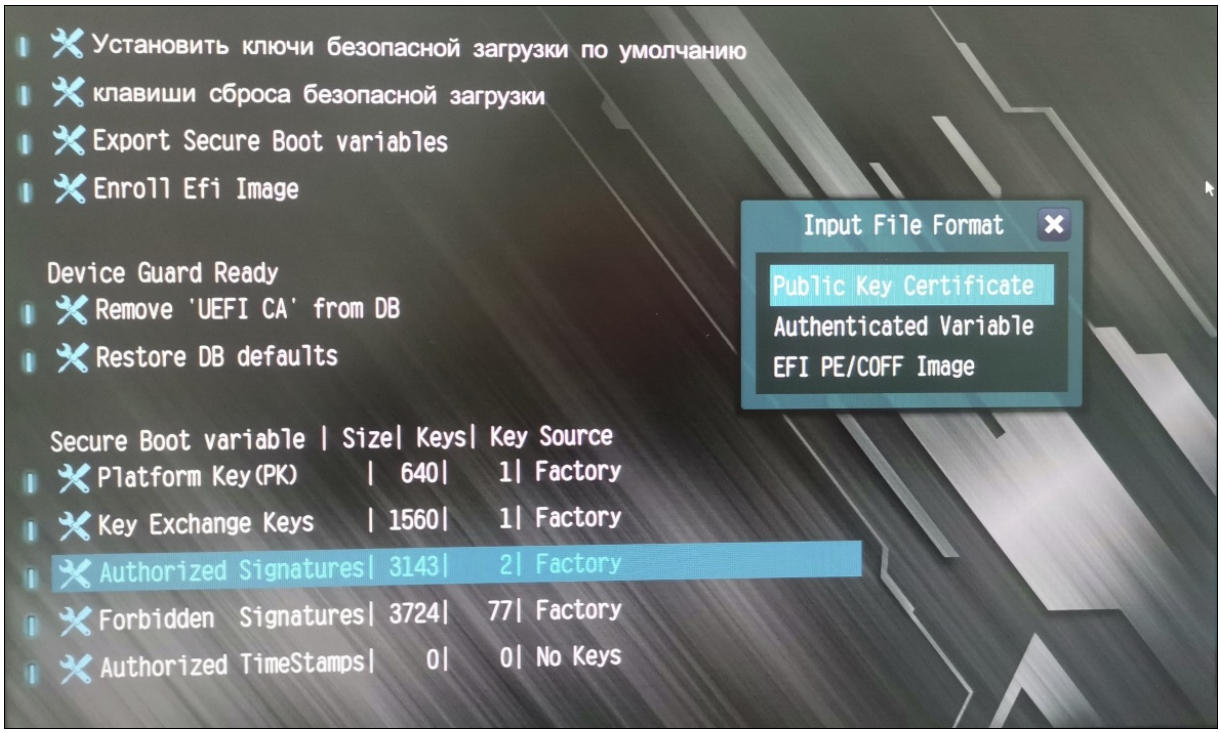
Затем необходимо установить сертификат. Для этого потребуется usb-flash накопитель с файловой системой **FAT32**, на который должен быть скопирован сертификат **ca.der**.

Выберите пункт **Authorized Signatures** – **Append**, чтобы добавить к уже существующим сертификатам новый.

После определения вашего устройства необходимо выбрать сам сертификат.



Тип необходимо указать **Public Key Certificate**.



На данном этапе настройка **BIOS** завершена – примените изменения и перезагрузите ПК.

В РЕД ОС проверить, активирован ли **SecureBoot**, можно командой:

```
mokutil --sb-state

SecureBoot enabled
```

Работа с РЕД ОС в сессии LiveUSB

Загрузочный экран LiveUSB
Графические программы LiveUSB
Консольные программы LiveUSB
Дополнительная информация

ISO-образ LiveUSB — представляет собой образ операционной системы, который можно записать на съёмный носитель (USB flash-накопитель) и ознакомиться с её функциональными возможностями без установки на жесткий диск ПК.

На текущий момент в РЕД ОС существует **ISO-образ LiveUSB**, который доступен к загрузке по ссылке.

Наименование **ISO-образа LiveUSB** производится в следующем формате:

```
redos—MUROM—<версия_ОС>—<архитектура>—LIVE.iso
```

Примечание.

Обратите внимание, что это именно **ознакомительный формат** ОС. Все изменения, которые производятся при работе с данным ISO-образом, **будут сброшены** после перезагрузки, за исключением изменений, которые производились на других носителях (не на том носителе, куда записан ISO-образ).

ISO-образ LiveUSB записывается на носитель идентично обычному образу.

Вы можете подробнее ознакомиться с работой системы РЕД ОС в сессии LiveUSB, просмотрев наши обучающие видео:

- на **RuTube** — Работа с РЕД ОС в сессии LiveUSB;
- в **Яндекс.Дзен** — Работа с РЕД ОС в сессии LiveUSB;
- в **VK Видео** — Работа с РЕД ОС в сессии LiveUSB.

На наших каналах вы также сможете найти много другой полезной информации.

Загрузочный экран LiveUSB

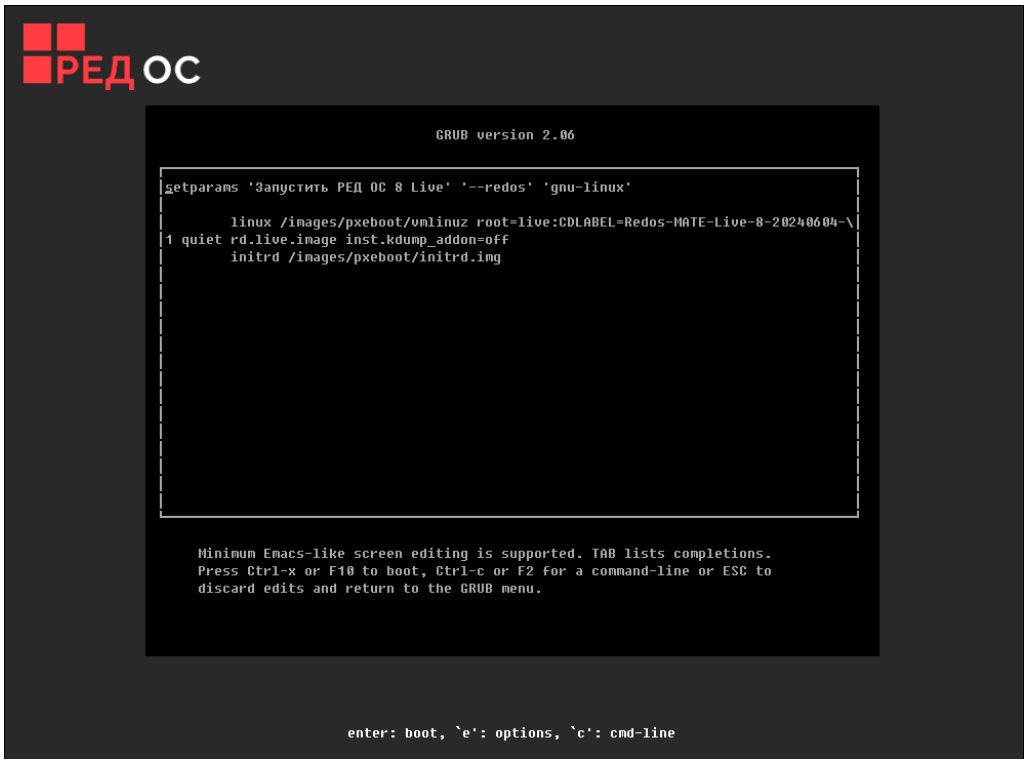
Загрузочный экран **LiveUSB** выглядит следующим образом:



Он предоставляет 2 варианта для выбора:

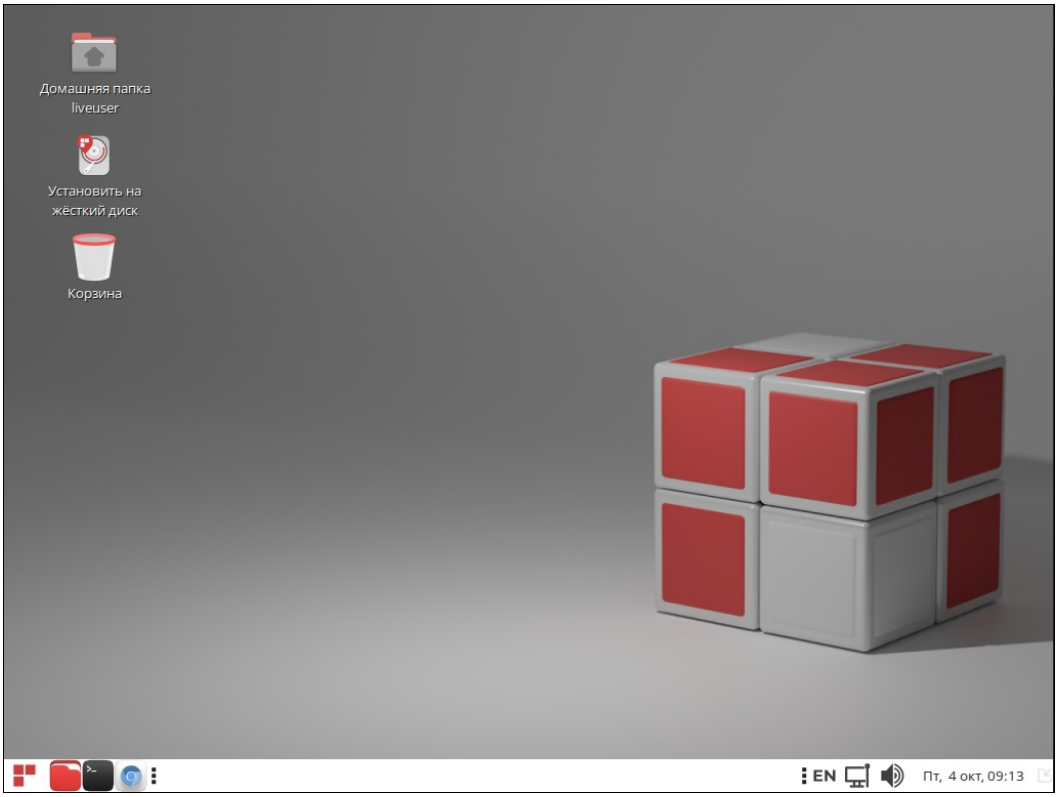
- произвести непосредственное ознакомление с ОС;
- проверить установленный носитель и запустить ознакомительную сессию.

Также вы можете изменить параметры загрузки ОС, если нажмете **e**.



Благодаря **ISO-образу LiveUSB** можно проводить тест на совместимость ваших комплектующих ПК с драйверами РЕД ОС. К примеру, в случае успешной работы драйвера и вашей видеокарты, вы увидите рабочий стол и сможете проверить через inxi -G, что ваша видеокарта нашла нужный ей видеодрайвер.

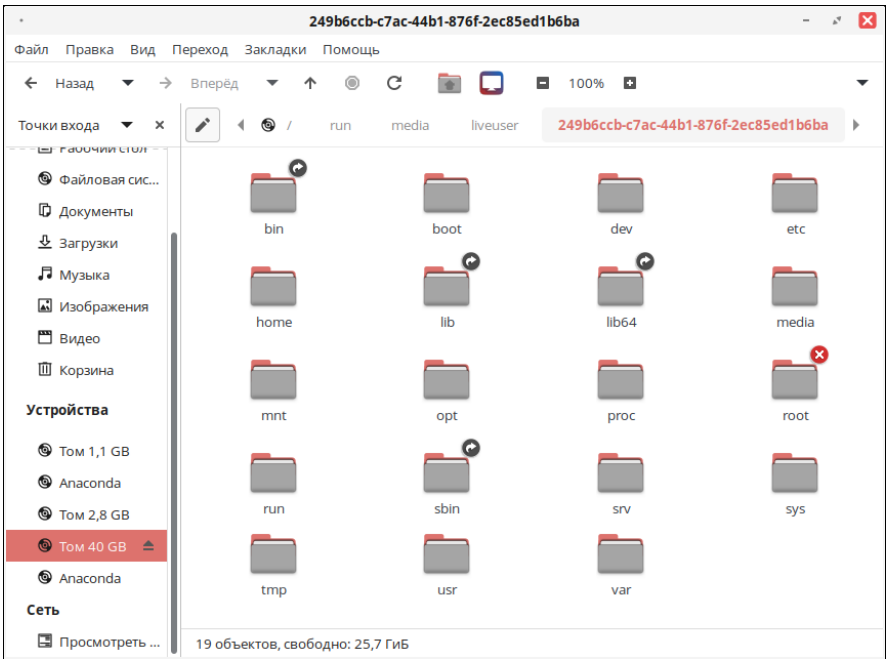
Рабочий стол **LiveUSB** выглядит так:



С него вы можете осуществить непосредственно установку ОС, нажав на ярлык «**Установить на жесткий диск**».

Если на ПК уже есть другая ОС, вы можете примонтировать ее «**Домашнюю папку**» для чтения/записи.

Если выбрать определенный диск из доступных, то он также будет примонтирован. Его содержимое можно будет скопировать или изменить.



Графические программы LiveUSB

Основной список доступных графических программ доступен в «**Главном меню**».

Список утилит, которые могут позволить восстановить работоспособность ОС, помочь записать диск или изменить разделы:

- Утилита **записи ISO-образов на USB-накопитель** - **MultiWriter** - подробная информация по ссылке;
- Утилита для работы **с дисковыми разделами** - **Gparted** - подробная информация по ссылке;
- Утилиты для **резервного копирования и восстановления данных** - подробная информация по ссылке;
- Утилита **сбора информации о системе** - **loginfo** - подробная информация по ссылке.

Консольные программы LiveUSB

Список основных доступных консольных команд:

- Утилита для отображения информации о системе и об аппаратной части ПК - **inxi** - подробная информация по ссылке;
- Утилита для проверки файловой системы и исправления ошибок - **fsck** - подробная информация по ссылке;
- Утилита для проверки контрольных сумм файлов - **md5sum** - подробная информация по ссылке;
- Утилита для отображения информации о модуле - **modinfo** - подробная информация по ссылке;
- Восстановление загрузчика **grub2** - подробная информация о командах по ссылке;
- И многие другие полезные программы как для анализа работы ОС, так и для различных других задач.

Дополнительная информация

Вы также можете просмотреть содержимое репозиториев РЕД ОС и проверить работу того или иного выбранного вами пакета. Главное - не забывать о том, что все внесенные вами изменения **будут сброшены** после перезагрузки ОС.

Ознакомиться с содержимым репозиториев вы можете как консольно, так и графически, через утилиты:

- Система управления пакетами - **dnf** - подробная информация по ссылке;
- Менеджер пакетов - **dnfdragora**.

Для восстановления работоспособности ОС, которая установлена на основном ПК, можно воспользоваться следующей информацией.

Проблемы с монтированием домашнего каталога /home

Рассмотрим проблему, из-за которой система не запускает графический менеджер **GDM** и вместо этого переходит в режим **emergency mode**. Суть данной проблемы заключается в том, что происходит сбой при монтировании домашнего каталога **/home**. При загрузке системы можно увидеть следующие предупреждения:

```
Warning: dev/mapper/ro-root does not exist
Warning: dev/ro/root does not exist
Warning: dev/ro/swap does not exist
```

В результате система входит в **emergency mode**. При входе будет предложено воспользоваться командной оболочкой для диагностики проблемы:

```
Entering emergency mode. Exit the shell to continue.
Type “journalctl“ to view system logs.
You might want to save “/run/initramfs/rdsosreport.txt“ to a USB stick or /boot after mounting then and attach it to a bug report.
```

Можно просмотреть журналы системы, введя команду:

```
journalctl
```

Запустите следующую команду, чтобы увидеть ошибки, связанные с домашним каталогом:

```
dmesg
```

В выводе должны присутствовать ошибки вида:

```
/dev/sda3, run e2fsck manually
```

где **/dev/sda3** - home-раздел.

Для того чтобы узнать, за каким разделом закреплен **/home**, необходимо проверить файл **/etc/fstab**. Найдите строчку, относящуюся к **/home**, чтобы определить, за каким устройством он закреплен.

```
cat /etc/fstab
```

Проверка файловой системы осуществляется через утилиту **fsck**. Запустите **fsck** для автоматической проверки (замените /dev/sda3 на ваш корректный раздел):

```
fsck -a /dev/sda3
```

где ключ **-a** отвечает за автоматическую коррекцию ошибок файловой системы.

Следуйте инструкциям. Если утилита сообщает о наличии ошибок, позвольте ей исправить их. Если некоторые ошибки не могут быть исправлены автоматически, утилита предложит вам выполнить их исправление вручную. После успешной проверки необходимо перезагрузить компьютер.

```
reboot
```

После этого графический менеджер GDM должен запуститься, и пользователь должен увидеть окно авторизации.

Пользователь забыл свой пароль и пароль root

Решением данной проблемы является сброс пароля **root**, согласно инструкции. Инструкцию предоставляет техническая поддержка, обратиться за инструкцией вы можете по ссылке.

Система не монтирует корневой раздел

Решение проблемы. Загрузка из более старого ядра
Неверное имя корневого раздела GRUB

Проблема монтирования корневого раздела выглядит следующим образом:

```
[ 1.719701] Hardware name: ECS IC780M-A2/IC780M-A2, BIOS 080015 11/03/2010
[ 1.719749] 0000000000000000 ffff88022c0b7df0 ffffffff8176cf38 ffffffff81a65048
[ 1.719951 0000000000008001 ffff88022c0b7e68 ffffffff81765306 ffffffff00000010
[ 1.720152] ffff88022c0b7e78 ffff88022c0b7e18 ffffffff81765e74 ffff88022c0b7e88
[ 1.720353] Call Trace:
[ 1.720402] [] dump_stack+0x64/0x82
[ 1.720449] [] panic+0xc8/0x206
[ 1.720494] [] ? printk+0x67/0x69
[ 1.720541] [] mount_block_root+0x225/0x2b0
[ 1.720587] [] mount_root+0x53/0x56
[ 1.720633] [] prepare_namespace+0x16c/0x1a4
[ 1.720679] [] kernel_init_freeable+0x1e1/0x1ee
[ 1.720725] [] ? initcall_blacklist+0xba/0xba
[ 1.720771] [] ? rest_init+0x80/0x80
[ 1.720817] [] kernel_init+0xe/0xf0
[ 1.720862] [] rest_from_fork+058/0x90
[ 1.720908] [] ? rest_init+0x80/0x80
[ 1.720974] Kernel Offset: 0x0 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 1.721043] ---[ end Kernel panic — not syncing: VFS: Unable to mount root fs on unknown-block (0,0)
_
```

Сообщение об ошибке «vfs unable to mount root fs on unknown block» может встречается во время загрузки Linux. Оно означает, что ядро не может примонтировать корневую файловую систему, и, следовательно, дальнейшая загрузка невозможна. Ошибка довольно серьёзная и, не исправив её, вы не сможете полноценно работать в своей операционной системе.

Все ситуации, в которых может появиться сообщение «error: vfs unable to mount root fs» можно разделить на два вида:

- Загрузка с жёсткого диска — вы загружаете свою основную операционную систему после внесения изменений в таблицу разделов, обновления или других действий, которые могли задеть диски;
- Вы загружаете LiveCD-систему с оптического диска или флешки.

Второй вариант сразу же отбросим. Здесь исправлять нечего. Ошибка означает, что либо образ был битый, либо он был неверно записан на диск. А вот первый случай интереснее, рассмотрим основные причины, которые могут его вызывать:

- Корневой раздел был переименован и теперь называется по-другому;
- Повреждена **initramfs**;
- Ядро не поддерживает файловую систему корневого раздела;
- Ошибка в конфигурации загрузчика, например, из-за недостаточного количества свободного места в папке **/boot**;
- Файловая система корневого раздела повреждена.

Рассмотрим возможные пути решения проблемы.

Решение проблемы. Загрузка из более старого ядра

После того, как система выдаст эту ошибку, случится **Kernel Panic** и компьютер перезагрузится. Вы снова окажетесь в меню загрузчика **GRUB**. Сначала следует попытаться загрузиться с помощью более старого ядра. Для этого выберите пункт «**Дополнительные параметры**» и выберите одно из более старых ядер.

Если система в этом случае загрузится, то можно сделать вывод, что не работает только новое ядро. Если вы собирали его сами, то, возможно, вы не включили в него все необходимые для работы файловые системы. Если это ядро из репозиториев, и система загрузилась с более старым ядром, то можно предположить, что у вас повреждена **initramfs** для нового ядра. Это тоже могло произойти из-за недостатка памяти при обновлении системы. Чтобы всё исправить, вам достаточно освободить место в каталоге **/boot/** и создать новую **initramfs**. Проверьте и освободите место в папке **/boot**, если его там мало:

```
df -h | grep boot
```

```
[root@localhost ~]# df -h | grep boot
/dev/sda2                974M          56M  851M            7% /boot
/dev/sda1                599M         6,4M  593M            2% /boot/efi
[root@localhost ~]#
```

На данном скриншоте занято только 7%, если будет 100% — надо освобождать. Для создания **initramfs** необходимо выполнить следующие действия:

```
cp -p /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak
dracut -f -v --regenerate-all
ls /boot
```

```
[root@localhost ~]# ls /boot
config-5.15.10-1.el7.x86_64
config-5.15.72-1.el7.3.x86_64
efi
grub
grub2
initramfs-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86.img
initramfs-5.10.29-3.el7.x86_64.img
initramfs-5.15.10-1.el7.x86_64.img
initramfs-5.15.72-1.el7.3.x86_64.img.bak
loader
lost+found
symvers-5.15.10-1.el7.x86_64.gz
symvers-5.15.72-1.el7.3.x86_64.gz
System.map-5.15.10-1.el7.x86_64
System.map-5.15.72-1.el7.3.x86_64
vmlinuz-0-rescue-5bcf621e66ba4fe4a75d2f4079182c86
vmlinuz-5.15.10-1.el7.x86_64
vmlinuz-5.15.72-1.el7.3.x86_64
```

Обновите конфигурацию загрузчика **grub**:

- если используется **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- если используется **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

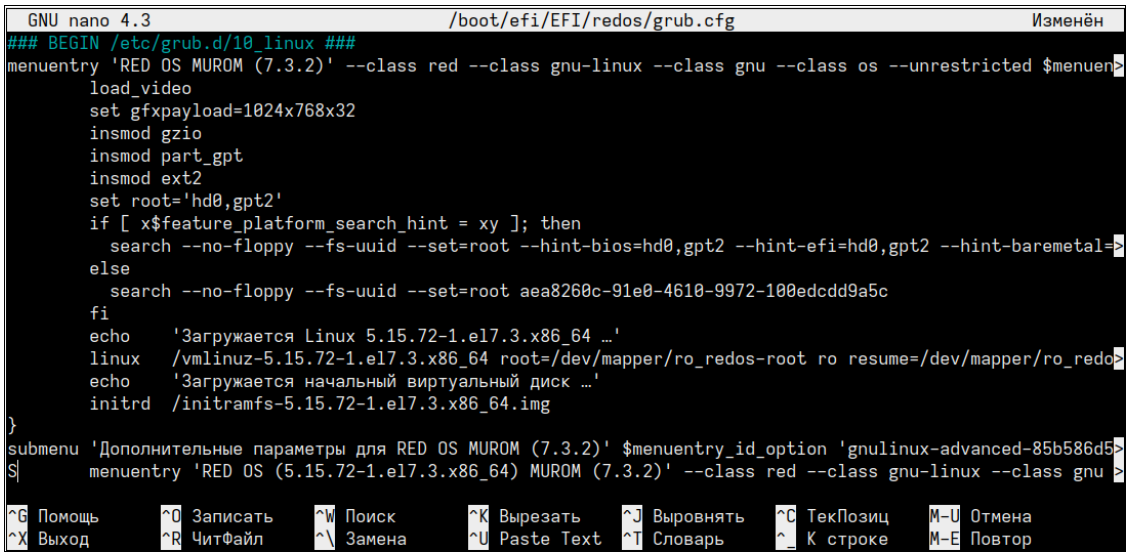
Если вы думаете, что проблема именно в свободном пространстве и **initramfs**, но загрузиться с помощью более старого ядра не можете, то попробуйте другой **LiveCD**-дистрибутив и попытайтесь всё исправить в *chroot*-окружении.

Неверное имя корневого раздела GRUB

Сейчас, в большинстве дистрибутивов, в конфигурационном файле **GRUB** имя корневого раздела передается ядру в формате **UUID**. И с этим обстоятельством есть одна проблема. Если вы каким-либо образом измените корневой раздел, например, измените его размер, то **UUID** изменится. И если вы выполните перезагрузку, не обновив конфигурацию **GRUB**, то система больше не загрузится, потому что ядро попросту не сможет найти нужного раздела.

Но попытаться решить проблему можно. Если вы точно знаете, на каком разделе у вас находится корень, то можно непосредственно в меню **GRUB** исправить конфигурацию. Для этого в меню выберете стрелками вверх и вниз нужный пункт, а затем нажмите кнопку **E**. Откроется редактор конфигурации. Вам нужно найти строчку, похожую на следующую:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro quiet splash
```



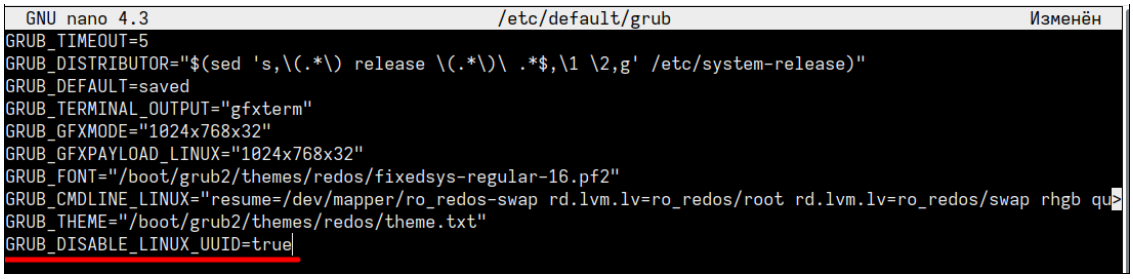
В ней надо заменить UUID=9d8d92de-74a6-4e64-8281-b8548c690e0c на обычное имя вашего корневого раздела, например, **/dev/sda2**. Для начала загрузки нажмите **F10**. Если система загрузится, значит проблема была именно в этом. В дальнейшем, можно просто обновить конфигурацию **GRUB**:

```
grub2-mkconfig
```

Или даже попросить **GRUB** больше не использовать **UUID** для обозначения корневого раздела:

```
nano /etc/default/grub
```

```
GRUB_DISABLE_LINUX_UUID=true
```



Далее необходимо снова обновить конфигурацию **GRUB**, используя команду **grub2-mkconfig**.

Если ошибка исчезла, но система всё ещё не загружается, обратите внимание, что **systemd** всё ещё использует файл **/etc/fstab** для монтирования файловых систем. И если корневая файловая система (и не корневая тоже) там указана неверно, система не загрузится. Для исправления этой проблемы можно использовать режим восстановления. Здесь тоже надо заменить **UUID** на обычную запись или же на правильный **UUID**. Такая проблема очень часто становится причиной медленной загрузки Linux.

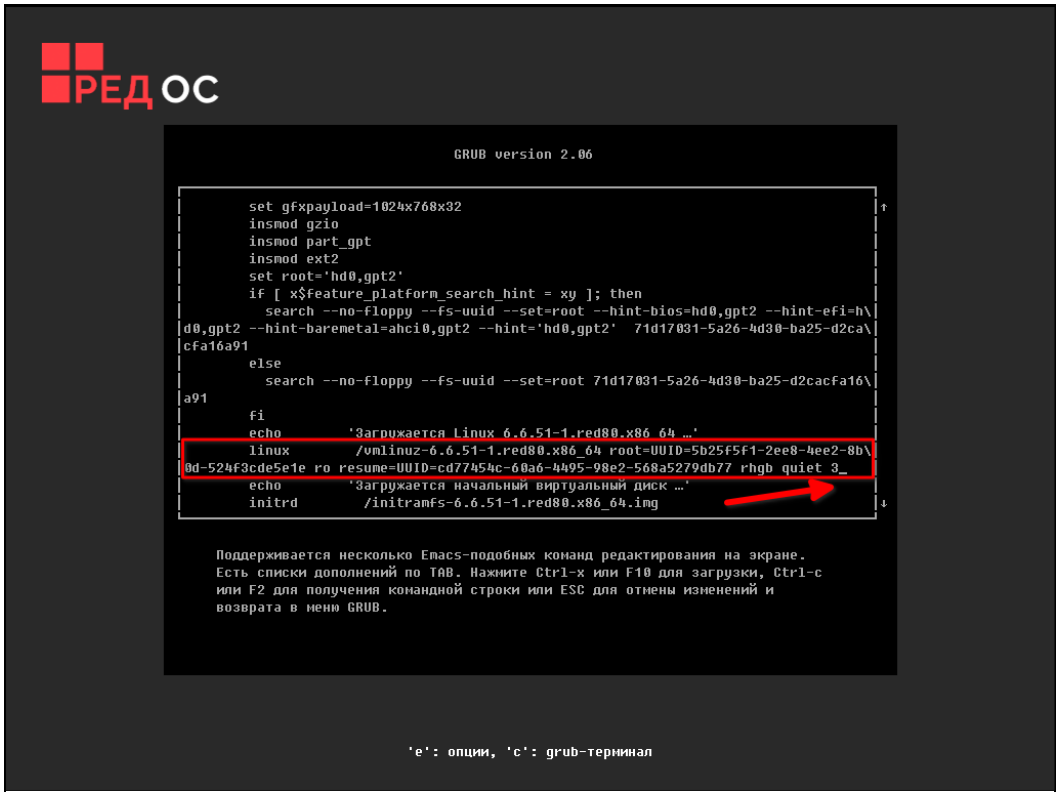
В этом же режиме можно проверить корневой раздел на ошибки, но для проверки диска лучше использовать **LiveCD**.

Если файловая система корневого раздела повреждена, её необходимо проверить, исправить согласно инструкции «Проверка файловой системы на наличие ошибок».

ОС запускается, но зависает на экране загрузки

Скорее всего данное поведение может быть связано с некорректным поведением X-сервера и графических драйверов. Для диагностики ситуации и сбора информации с ПК вы можете запустить ПК в консольном режиме. Для этого вам потребуется перезагрузить ПК и на этапе выбора ядра для загрузки нажать «**e**».

Далее необходимо найти примерно такую строку (см. скриншот) и добавить в конец «**3**».



После этого для продолжения загрузки необходимо нажать сочетание клавиш «**Ctrl+X**», ОС будет запущена в текстовом режиме.

Следующим этапом потребуется собрать отладочную информацию через утилиту loginfo для дальнейшего изучения проблемы.

Не загружается РЕД ОС из-за неправильного UUID раздела SWAP

Диагностика проблемы
Устранение проблемы

Проблема характеризуется тем, что во время загрузки операционной системы РЕД ОС на экране появляется ошибка вида:

```
A start job is running for /dev/disk/by-uuid/03a83c83-3827-4fa3-8352-bdfb4d99a15b (10min 6s / no limit)
```

Загрузить операционную систему в безопасном режиме также не удается.

Диагностика проблемы

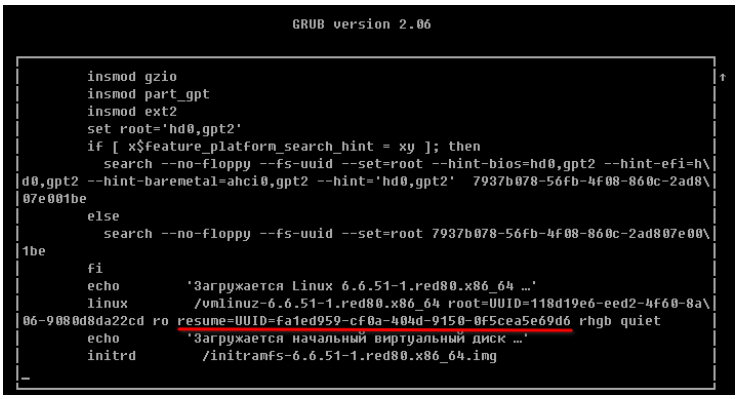
Ошибка «A start job is running for /dev/disk/by-uuid/...» связанна с разделом диска, который используется в системе. Операционная система не может подключить раздел, который имеет номер **UUID**, указанный в ошибке.

Для того чтобы узнать, с каким именно разделом имеются проблемы при загрузке, требуется проверить параметры загрузчика системы **grub**.

Чтобы увидеть параметры загрузки grub, нужно на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /vmlinuz-6.6.51-1.red80.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> rhgb quiet
```

В строке видно, что в параметре resume=UUID= записан тот номер **UUID**, из-за которого возникает проблема с запуском системы.



Параметр resume отвечает за указание файла подкачки (раздел **SWAP**) для возобновления работы системы после перехода в спящий режим. Из этого можно сделать вывод, что проблема связана с разделом **SWAP**.

Необходимо узнать, совпадает ли номер **UUID** раздела **SWAP**, который указан в параметрах grub, с его актуальным на данный момент **UUID**-номером.

Номер **UUID** всех разделов диска можно узнать с помощью команды:

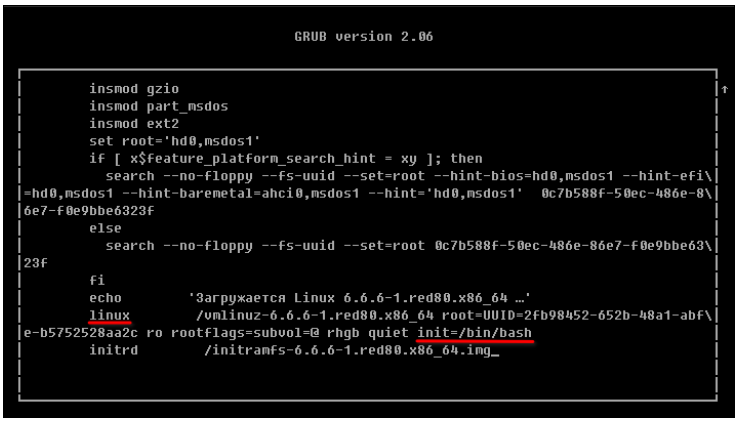
```
lsblk -o +uuid,name
```

Но т. к. операционная система РЕД ОС не может быть загружена ни в обычном, ни в безопасном режиме, то нужно выполнить загрузку системы сразу в командный интерпретатор **/bin/bash**.

Для этого необходимо открыть параметры загрузки **grub** — на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /vmlinuz-6.6.51-1.red80.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> rhgb quiet
```

В строке необходимо удалить полностью параметр resume=UUID=<номер_uuid> и добавить параметр init=/bin/bash:



Для продолжения загрузки с введенными параметрами необходимо нажать сочетание клавиш **Ctrl+x** или **F10**.

Система сразу загрузится в командную оболочку **bash**.

Авторизуйтесь с правами пользователя **root** командой:

```
su root
```

Далее выполните монтирование корневого раздела командой:

```
mount -o remount,rw /
```

Нужно узнать **UUID**-номер, который имеет раздел **SWAP** в данный момент. Для этого необходимо выполнить команду:

```
lsblk -o +uuid,name
```

Вывод команды должен быть примерно следующим:

```
nvme0n1
│   259:0    0 476,9G  0 disk                                  nvme0n1
├─nvme0n1p1
│   259:1    0   600M  0 part /boot/efi   050C-89A6                    nvme0n1p1
├─nvme0n1p2
│   259:2    0     1G  0 part /boot      bef54c6a-a584-4147-9178-4218be5daedc   nvme0n1p2
└─nvme0n1p3
   259:3    0 475,4G  0 part           lA0CXd-ZuHw-7mqu-uhkH-igMU-c7wt-QBESxa nvme0n1p3
  ├─ro_redos-root
  │ 253:0    0    70G  0 lvm  /        832a877b-0293-4eec-a5f0-6a8d080aac03   ro_redos-srv-root
  ├─ro_redos-swap
  │ 253:1    0   7,5G  0 lvm  [SWAP]     fc46bf73-2759-4d70-a2d3-ab1f664ebf12   ro_redos-srv-swap
  └─ro_redos-home
    253:2    0 397,8G  0 lvm  /home      e5411e74-97de-4b84-aecd-e7f86e16ad5e   ro_redos-home
```

В данном примере раздел **SWAP** имеет **UUID - fc46bf73-2759-4d70-a2d3-ab1f664ebf12**.

Таким образом, можно сделать вывод, что номер **UUID** раздела **SWAP**, который записан в параметрах загрузки grub, и его актуальный **UUID** номер отличаются.

Устранение проблемы

Для устранения проблемы необходимо заменить неактуальный **UUID**-номер в параметрах загрузки **grub** на его актуальный номер, который был получен в результате диагностики.

Изменение параметра resume загрузчика GRUB

1. На этапе выбора ядра нажмите клавишу «**e**». Будут открыты параметры загрузки **grub**.

2. Замените старый номер **UUID**, прописанный в параметре `resume=UUID=`, на актуальный, который был получен в результате диагностики командой `lsblk -o +uuid,name`.

В строке:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> quiet splash
```

3. Для продолжения загрузки с введенными параметрами нажмите сочетание клавиш **Ctrl+x** или **F10**.

Система должна загрузиться без ошибок.

Сохранение конфигурации загрузчика GRUB

При таком способе редактирования параметров загрузки **grub** введенные параметры не будут сохранены при следующей загрузке. Для сохранения внесенных изменений на постоянной основе измените параметр `resume=UUID=` в файле **/etc/default/grub**.

Для запуска терминала необходимо использовать сочетание клавиш **Ctrl+Alt+T** или запустить утилиту из **Главного меню** – **Системные** – **Терминал**.

Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

Откройте файл **/etc/default/gru**b с помощью текстового редактора командой:

```
nano /etc/default/grub
```

Найдите строку следующего вида:

```
GRUB_CMDLINE_LINUX="resume=UUID=..."
```

Номер **UUID** параметра `resume=UUID=` должен быть заменен на актуальный, с помощью которого удалось запустить систему.

Далее обновите файл загрузчика **grub** командой:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

После выполнения этих действий параметры загрузи **grub** будут сохранены для постоянного использования.

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

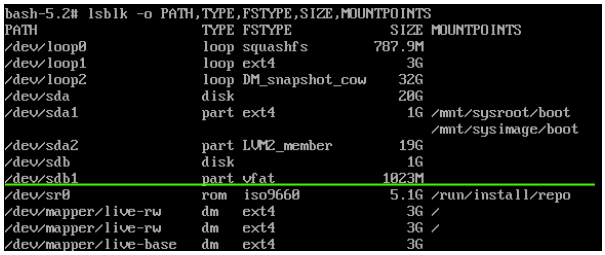
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

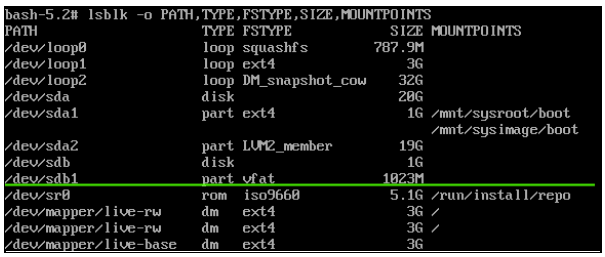
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

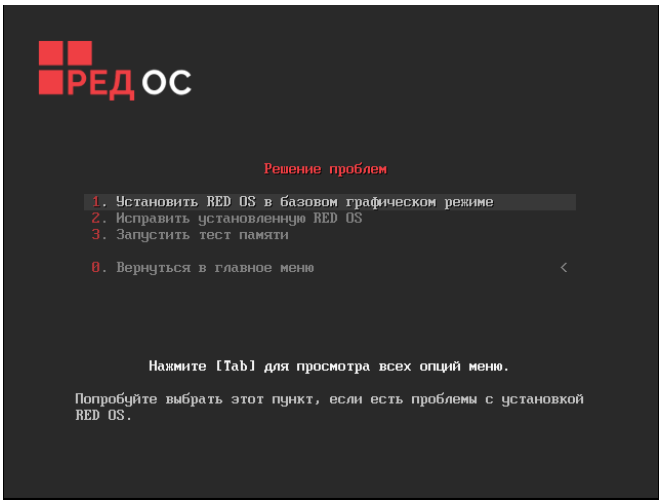
Проблемы при установке ОС

Установка ОС зависает на начальном этапе
ОС не запускается после установки с LiveUSB

Установка ОС зависает на начальном этапе

Бывают случаи, когда установка ОС зависает на этапе первичной загрузки до запуска окна *Anaconda*. В таких случаях рекомендуется произвести установку ОС в **базовом графическом режиме**, который также называется **nomodeset**.

Для загрузки ОС в режиме **nomodeset**, использующих **BIOS**, выберите пункт «**Решение проблем**» – «**Установить RED OS в базовом графическом режиме**».



Для загрузки ОС в режиме **nomodeset**, использующих **UEFI**, выберите пункт «**Решение проблем**» – «**Установить РЕД ОС в базовом графическом режиме**».



ОС не запускается после установки с LiveUSB

Иногда бывают случаи, что после установки ОС с *LiveUSB* не происходит загрузка установленной ОС. Для таких случаев необходимо загрузиться обратно в Live-сессию и скопировать файл **initramfs** с установочного носителя на диск с ОС. Для этого выполните следующий алгоритм действий:

1. Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

2. Проверьте названия разделов установленной ОС командой:

```
lsblk
```

В ответе команды будут указаны разделы ОС и загрузчика.

```
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   40G  0 disk
├─sda1   8:1    0    1M  0 part
├─sda2   8:2    0    1G  0 part /boot
├─sda3   8:3    0    2G  0 part [SWAP]
└─sda4   8:4    0 36,9G  0 part /
sr0     11:0    1  6,3G  0 rom  /run/initramfs/live
```

3. Примонтируйте разделы установленной ОС следующими командами:

```
mkdir /newboot
mount /dev/sda2 /newboot
```

4. Скопируйте образ **initrd.img** с **liveUsb** на раздел **/boot** диска с установленной системой:

```
cp /run/initramfs/live/images/pxeboot/initrd.img /newboot/initramfs-6.6.51-1.red80.x86_64.img
```

5. Назначьте необходимые права:

```
chmod 600 /newboot/initramfs-6.6.51-1.red80.x86_64.img
chown root. /newboot/initramfs-6.6.51-1.red80.x86_64.img
```

6. Отмонтируйте разделы установленной ОС:

```
umount /newboot
```

7. Перезагрузите ПК в установленную ОС:

```
reboot
```

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

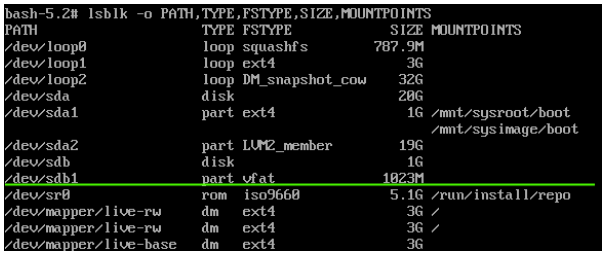
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

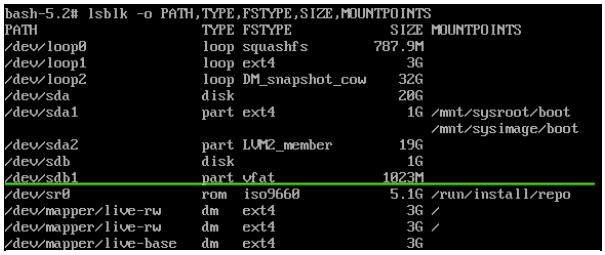
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Общие положения

Перед началом работы с РЕД ОС пользователю необходимо изучить руководство администратора и руководство пользователя, поставляемые с техническими средствами ПК в составе оборудования рабочего места пользователя. Также пользователь должен пройти инструктаж по технике безопасности при работе с электроприборами и ПК.

Для начала работы в РЕД ОС пользователю необходимо убедиться в работоспособности ПК своего рабочего места. После проверки и подготовки рабочего места пользователь для начала работы с РЕД ОС должен произвести включение оборудования ПК рабочего места.

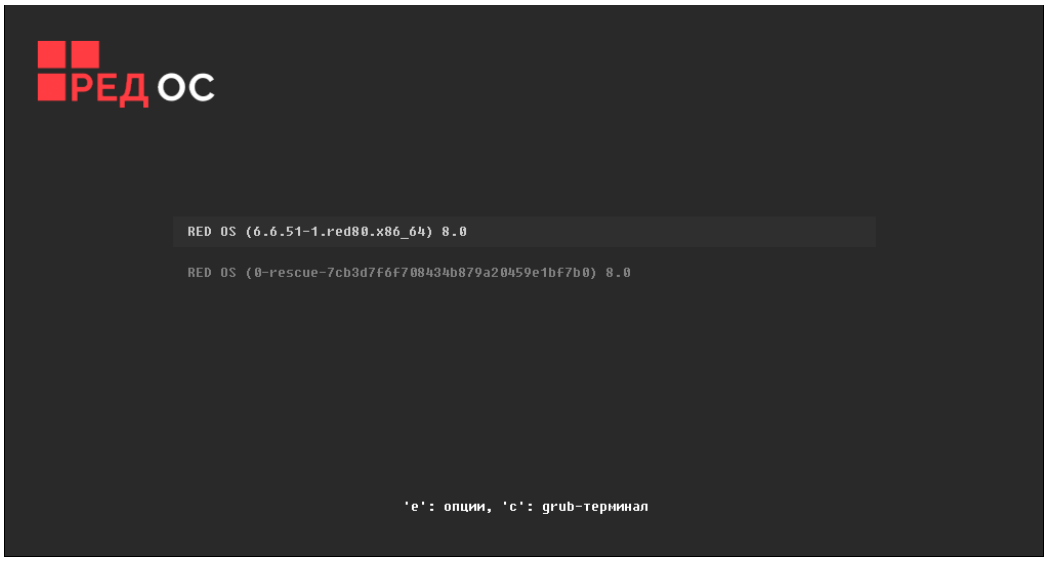
Базовая система ввода/вывода (BIOS) персонального компьютера пользователя должна быть настроена на автоматическую загрузку операционной системы с локального накопителя жестких дисков.

После включения питания ПК и выполнения загрузки BIOS производится запуск РЕД ОС. При запуске РЕД ОС в течение заданного интервала времени предоставляет пользователю возможность выбора варианта загрузки ОС, с которым будет произведена загрузка и работа РЕД ОС.



По умолчанию система загружается в штатном режиме, также доступен выбор дополнительных параметров загрузки.

При выборе дополнительных параметров будет предложено 2 варианта: обычная загрузка в штатном режиме и загрузка ОС в режиме восстановления с минимальным числом настроек для возможности восстановления системы после сбоя.



Если в течение заданного интервала времени пользователь не выбрал вариант загрузки клавишами «вверх/вниз», то операционная система производит автоматическую загрузку варианта заданного по умолчанию.

Далее производится загрузка РЕД ОС, которая визуально для пользователя может проходить двумя способами:

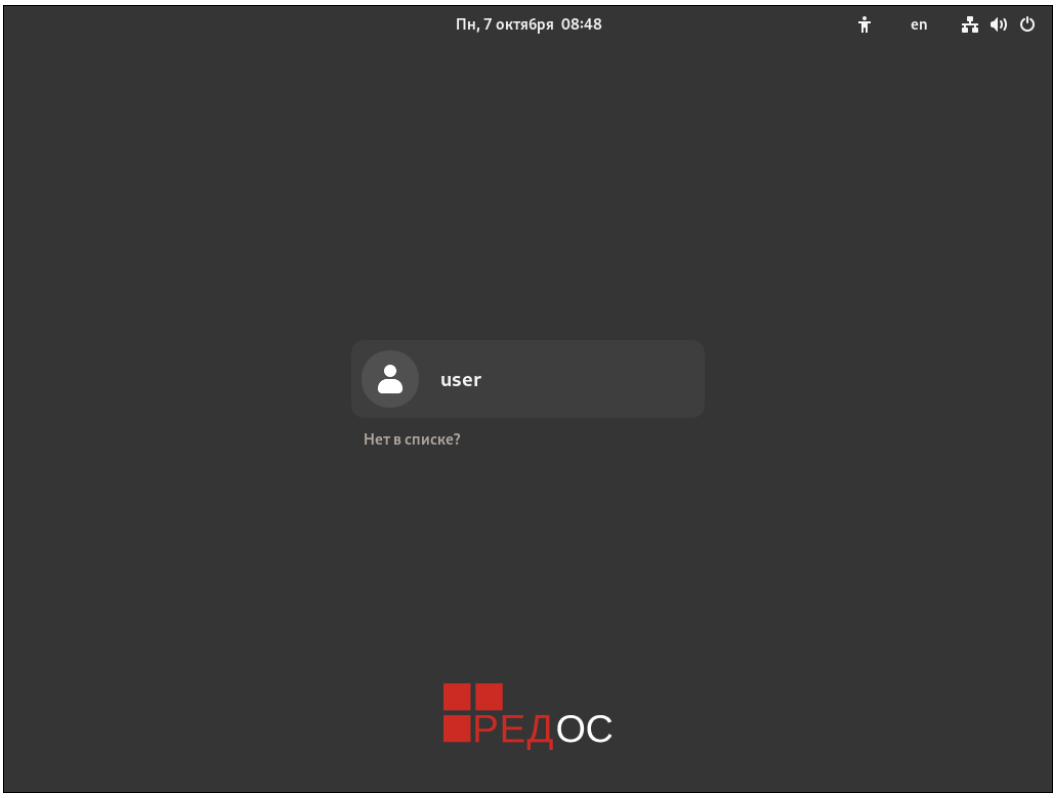
- **в текстовом режиме** с выводом лога загрузки, который отражает статус загрузки и старта модулей РЕД ОС. Текстовый режим загрузки производится до момента инициализации и старта графического сервера операционной системы. После старта графического сервера операционной системы загрузка РЕД ОС переходит в графический режим. При отказе оборудования или программного обеспечения, приводящем к невозможности старта графического сервера системы, загрузка ОС продолжается в текстовом режиме.
- **в графическом режиме**, в котором пользователю отображается графический экран загрузки ОС. Данный режим загрузки

скрывает от пользователя текстовый лог загрузки ОС и выводит на экран анимированный прогресс-индикатор.

При зависании процесса загрузки ОС, выражающемся в сообщениях о сбоях в текстовом режиме загрузки или замирании на долгое время прогресс-индикатора загрузки, пользователю необходимо произвести выключение ПК, проверку подключенных к ПК периферийных устройств и произвести повторный запуск ОС. При повторном зависании загрузки пользователь должен выключить электрическое питание ПК и периферийных устройств и обратиться к администратору для устранения неисправности.

Аутентификация пользователя

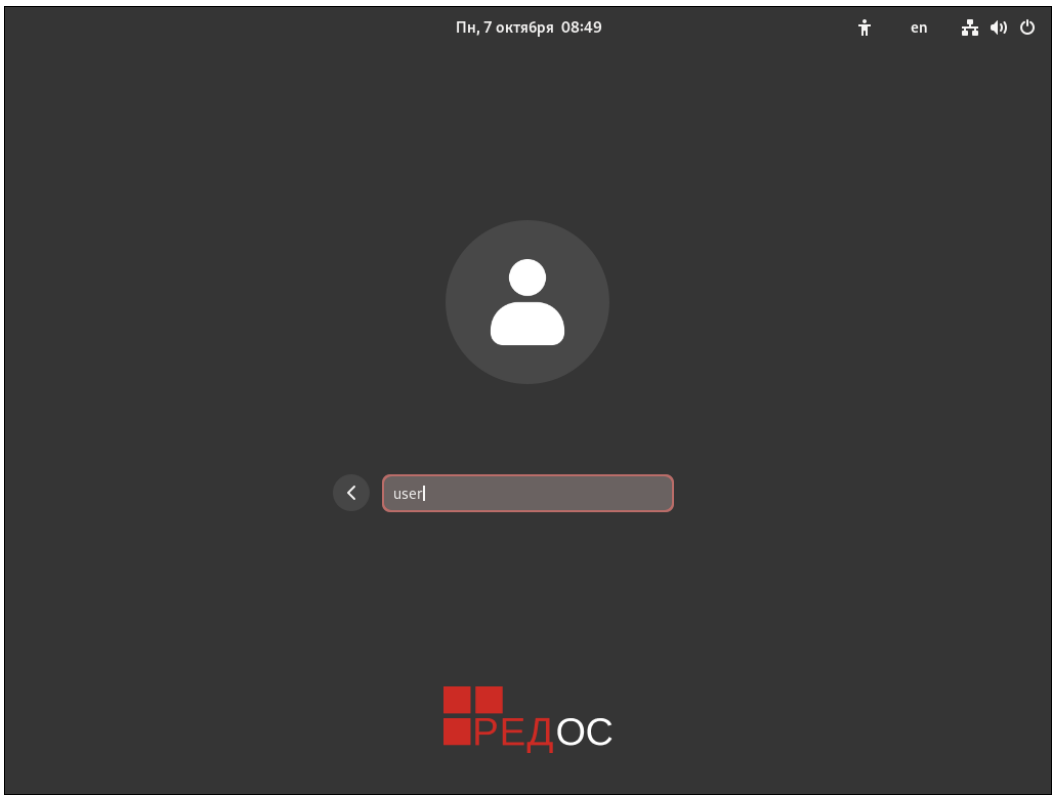
По окончании загрузки РЕД ОС пользователю отображается экран приветствия и приглашения к аутентификации, приведенный на рисунке ниже.



В РЕД ОС база данных пользователей может быть как локальной для операционной системы, так и являться частью единого пространства пользователей (ЕПП), функционирующего на основе протокола LDAP.

Если ЕПП не используется, аутентификация осуществляется с помощью локальной БД пользователей. При использовании ЕПП аутентификация пользователей осуществляется централизованно по протоколу LDAP. В ЕПП в качестве источника данных для идентификации и аутентификации пользователей применяются службы каталогов openldap.

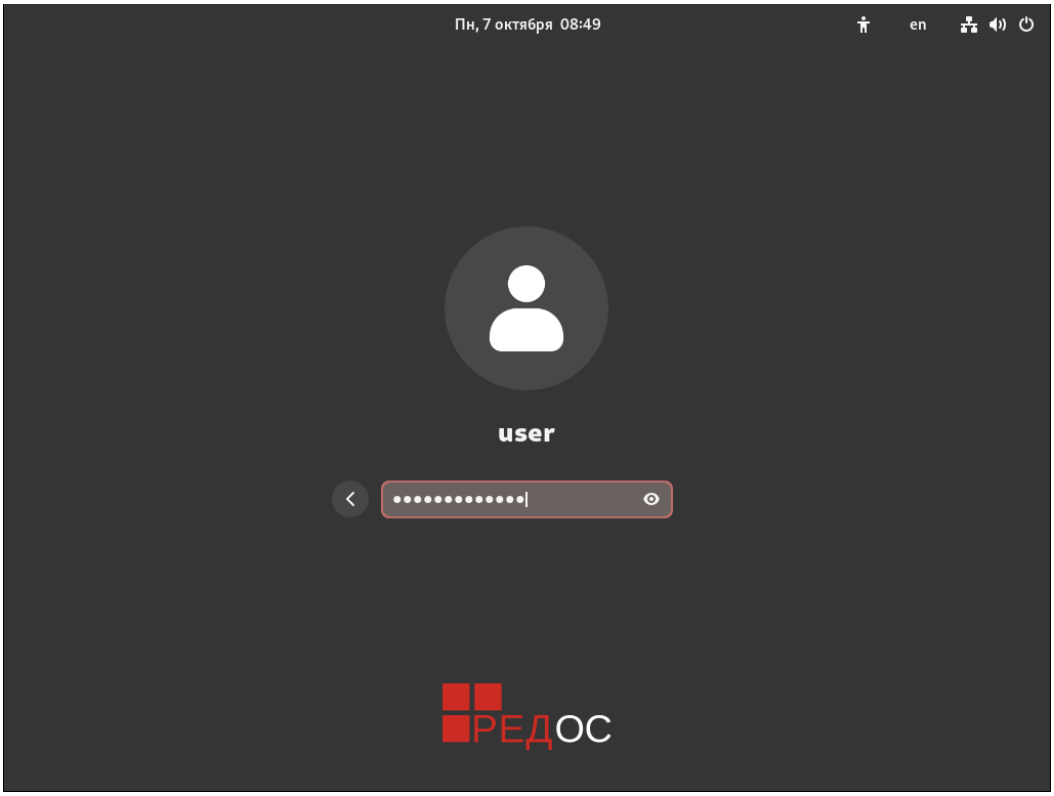
Для аутентификации в операционной системе по локальной БД пользователей, в окне запроса аутентификационных данных необходимо выбрать соответствующего пользователя в списке пользователей или ввести имя пользователя (логин пользователя) в поле «**Имя пользователя**» нажав кнопку «**Нет в списке?**», ввести пароль учетной записи и нажать клавишу «**Enter**».



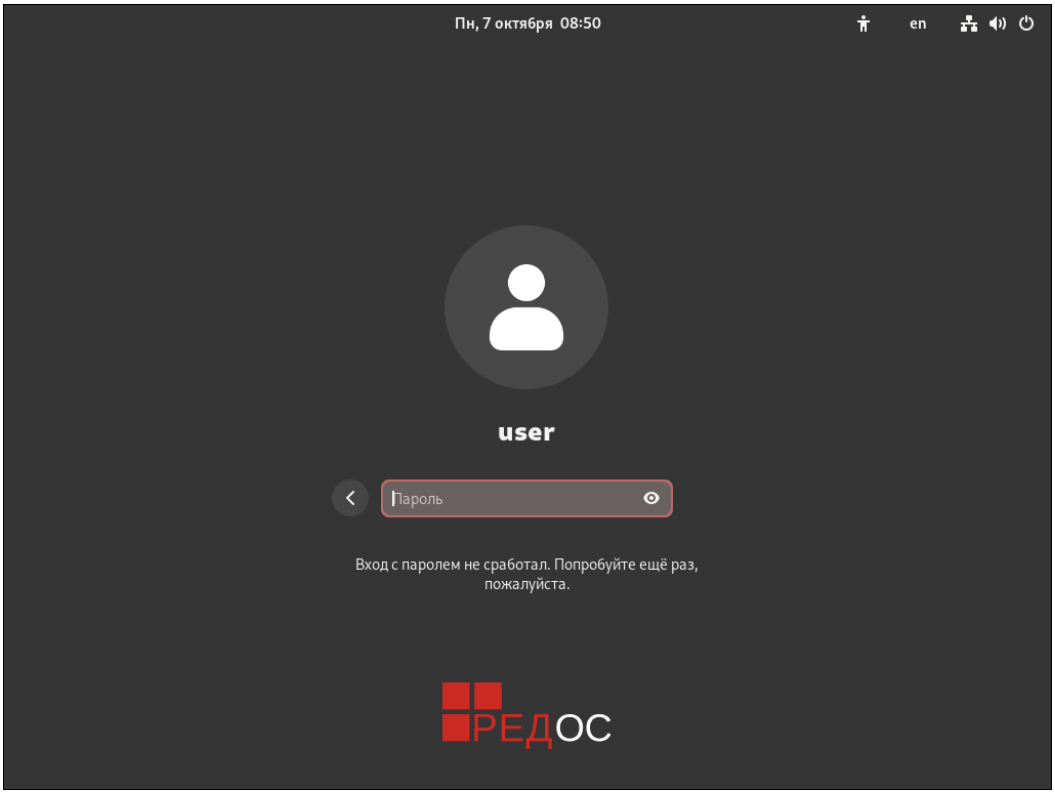
Если используется многофакторная аутентификация необходимо использовать дополнительные факторы аутентификации

предоставленные администратором системы.

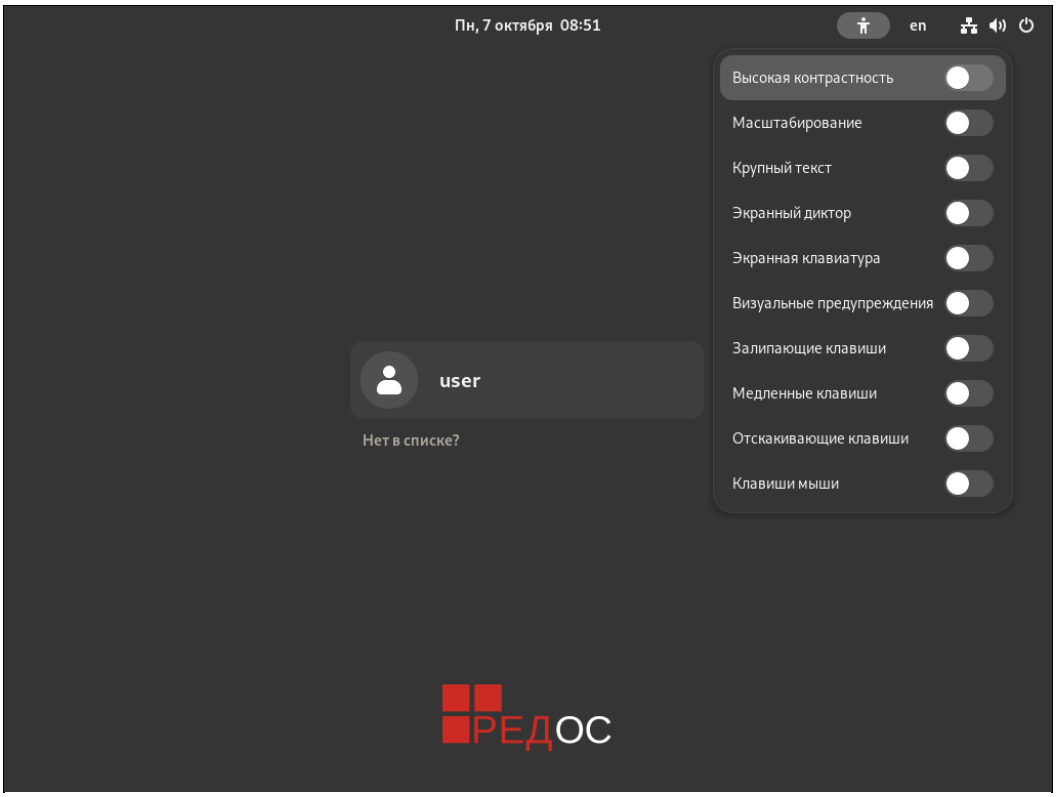
После ввода имени пользователя необходимо ввести пароль пользователя и нажать клавишу «**Enter**».



При неправильно указанных атрибутах пользователя (логин и/или пароль) РЕД ОС выводит предупреждение о сбое во время проверки данных. После этого РЕД ОС предлагает пользователю повторно ввести аутентификационную информацию.

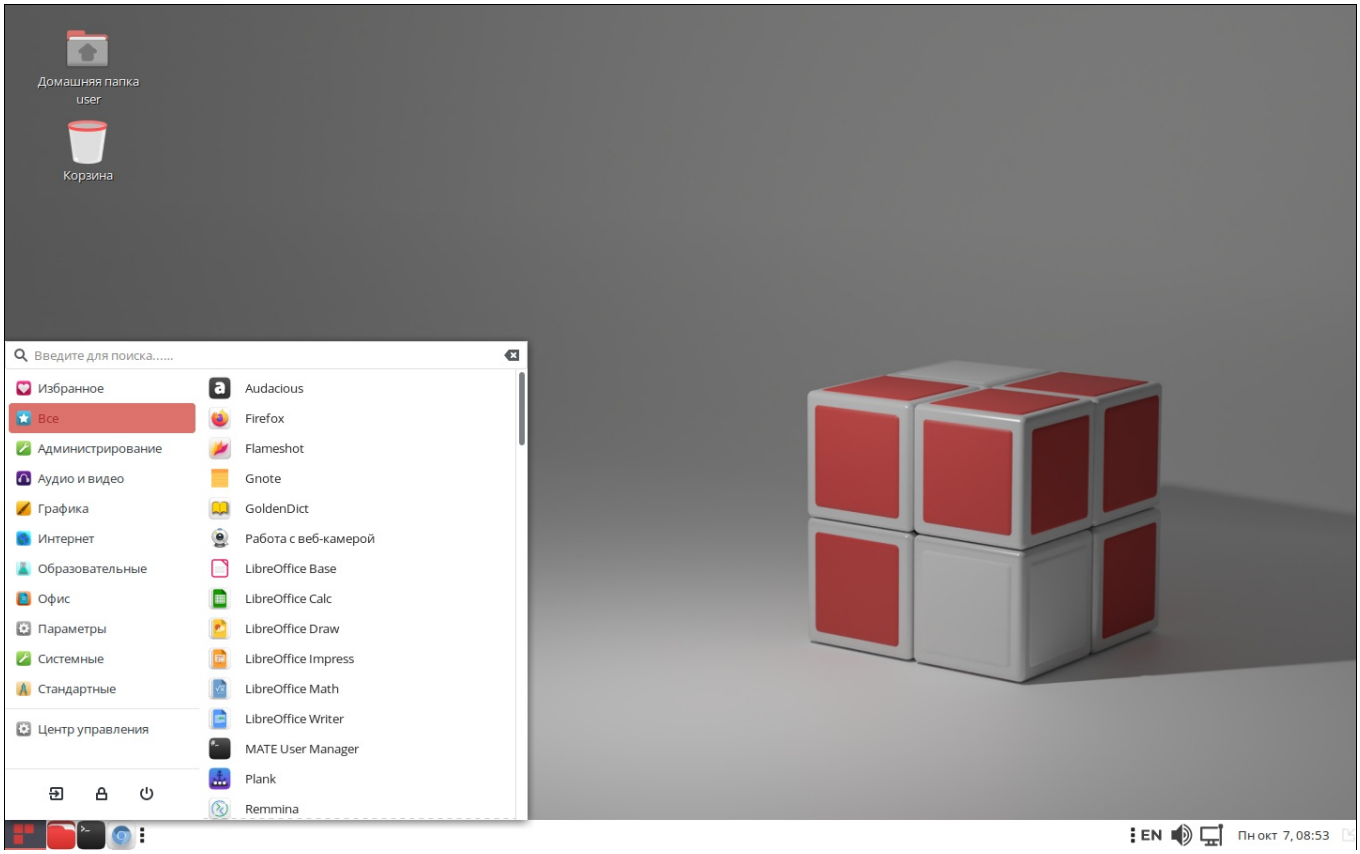


РЕД ОС при аутентификации предоставляет пользователям с ограниченными возможностями набор средств для облегчения процесса работы в ОС: экранная клавиатура; контрастные цветовые схемы; крупный экранный шрифт и т.д.



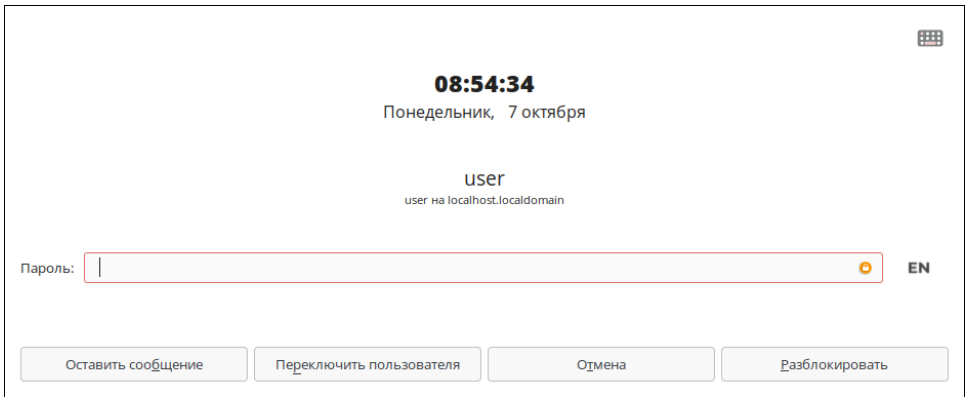
После того, как пользователь ввел корректные аутентификационные данные, РЕД ОС загружает рабочий стол пользователя.

После этого происходит окончательная загрузка графического окружения пользователя.

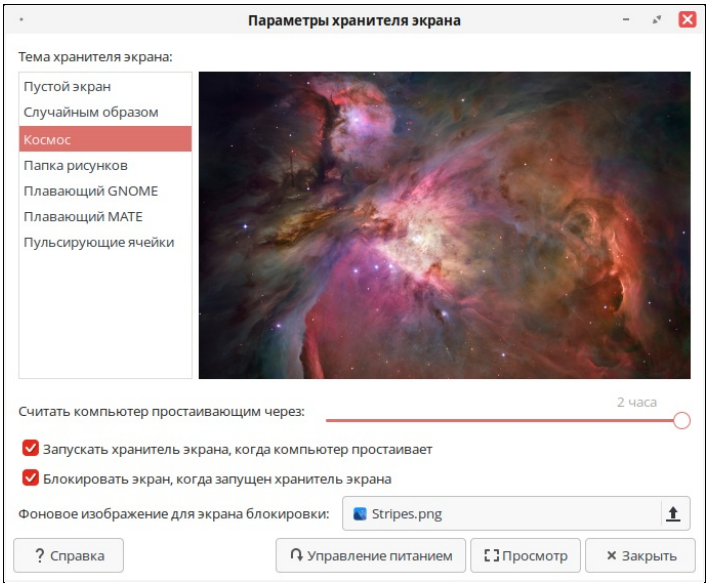


В правом нижнем углу рабочего стола отображается текущая дата и время, иконка с возможностью быстрого доступа к настройкам сетевого подключения и регулятор громкости. В левом нижнем углу вызывается меню приложения, осуществляется переход по каталогам файловой системы и доступ к утилитам системной настройки. Далее следуют иконки быстрого запуска наиболее часто используемых приложений.

При продолжительном бездействии пользователя рабочий стол пользователя блокируется, и для возобновления работы пользователю требуется провести повторную аутентификацию в РЕД ОС.



Значение продолжительности бездействия пользователя, после которого произойдет блокировка рабочего стола, определяется утилитой «**Хранитель экрана**». Данная утилита находится в «**Главном меню**» - «**Параметры**». Внешний вид утилиты управления хранителем экрана приведен на рисунке ниже.



Все действия пользователя при аутентификации, успешные и неуспешные попытки аутентификации фиксируются в системном журнале РЕД ОС.

Окно настройки РЕД ОС

Вкладка «Настройка системы»
Вкладка «Сторонние приложения»
Вкладка «Документация и Помощь»
Вкладка «О РЕД ОС»

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** redoswelcome-1.13.2-1

Вы можете подробнее ознакомиться с проведением первой настройки РЕД ОС, просмотрев наши обучающие видео:

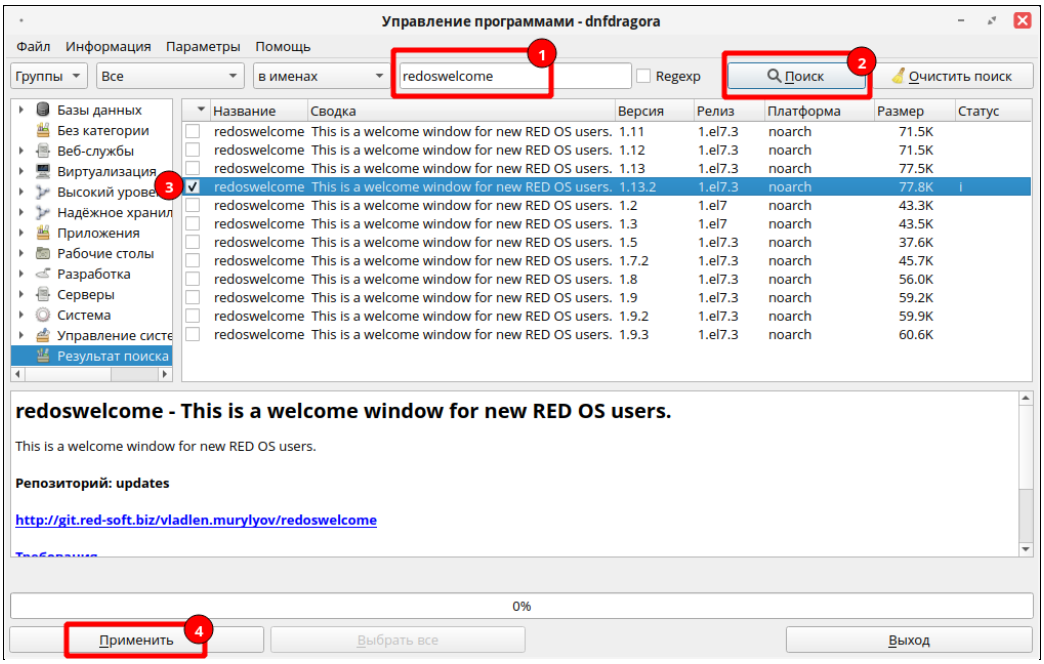
- на **RuTube** — Окно настройки РЕД ОС;
- в **Яндекс.Дзен** — Окно настройки РЕД ОС;
- в **VK Видео** — Окно настройки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

В репозитории РЕД ОС существует утилита «**Окно настройки РЕД ОС**», позволяющая пользователям ознакомиться с базовым функционалом ОС перед началом работы.

В более поздних версиях ОС данная утилита установлена по умолчанию.

Установка утилиты доступна через менеджер пакетов dnfdragora. Откройте «**Главное меню**» - «**Администрирование**» - «**Управление пакетами dnfdragora**», в строке поиска впишите название пакета **redoswelcome**, нажмите «**Поиск**». В окне результатов выберите последнюю из доступных версий пакета и нажмите кнопку «**Применить**».



Также доступен консольный вариант установки утилиты, для этого перейдите в сеанс пользователя **root**:

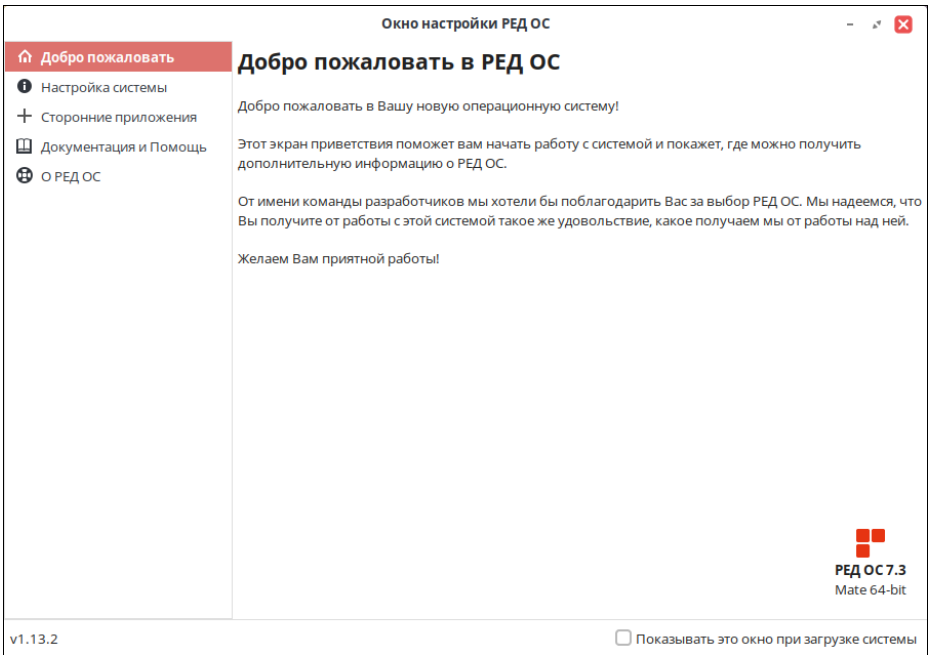
```
su -
```

и выполните команду:

```
dnf install redoswelcome
```

После установки программа будет доступна из «**Главного меню**» - «**Параметры**» - «**Окно настройки РЕД ОС**».

При первой авторизации пользователя в системе будет автоматически открыто следующее окно:



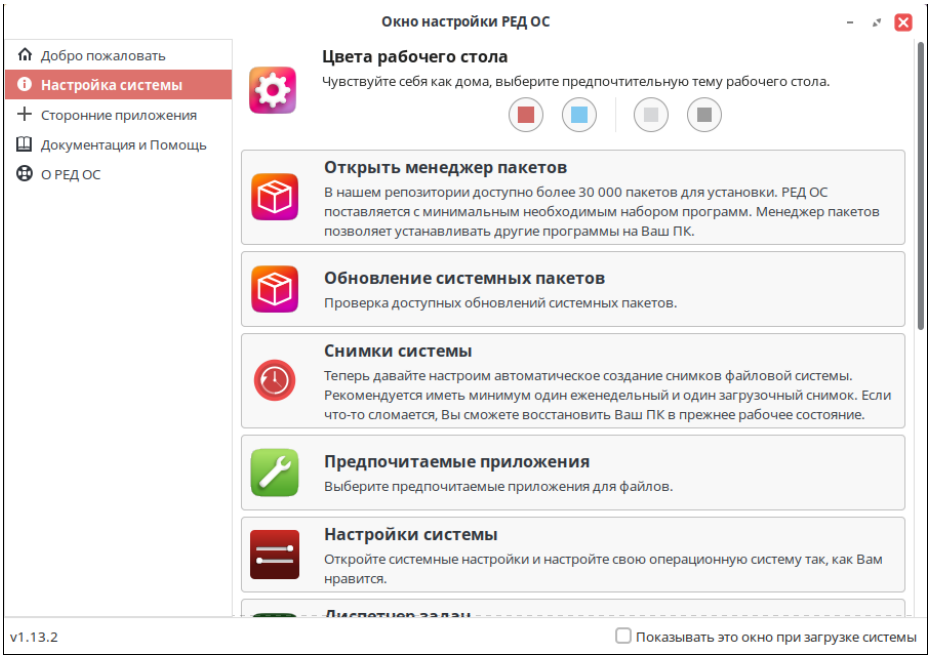
Стартовая страница утилиты позволяет пользователю:

- Ознакомиться с приветственным обращением от команды РЕД ОС;
- Включить или отключить возможность показа данной утилиты после авторизации пользователя;
- Переключаться между вкладками.

Вкладка «Настройка системы»

Функционал, доступный пользователю на данной странице:

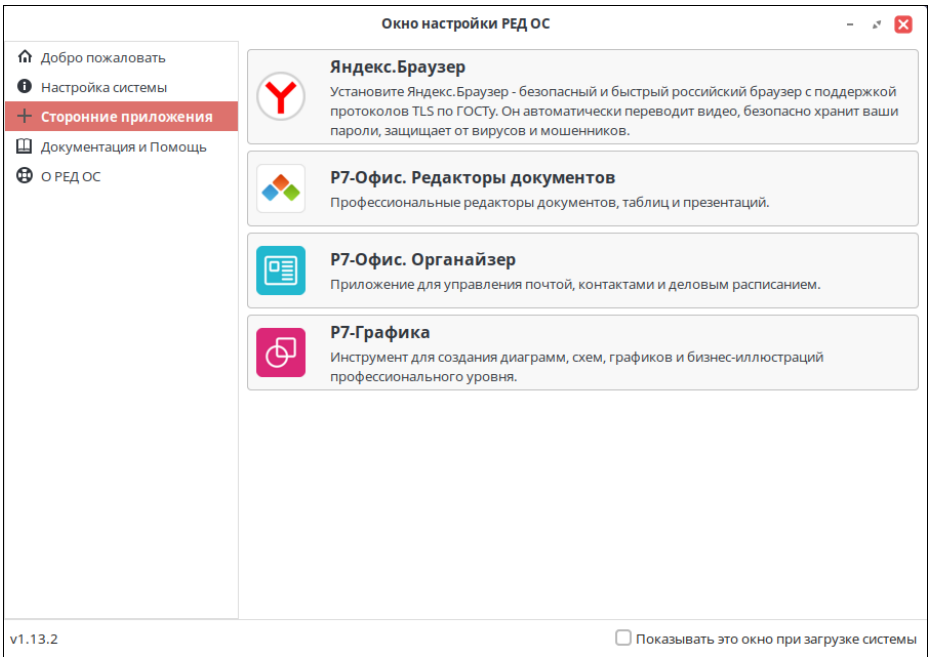
- Переключение оформления ОС между стандартными темами;
- Запуск для ознакомления предустановленного ряда программ (пакетов), перечисленных в списке.



Вкладка «Сторонние приложения»

На данной вкладке для установки доступны некоторые сторонние программы, такие как:

- Яндекс.Браузер;
- Р7-Офис. Редакторы документов;
- Р7-Офис. Органайзер;
- Р7-Графика.



Вкладка «Документация и Помощь»

Вкладка «**Документация и Помощь**» будет полезна как новичкам, так и администраторам. Здесь представлены публичные ресурсы компании, справочная информация о системе, а также существует возможность ознакомиться с другими продуктами компании.

Перечень основных ресурсов для поиска необходимой информации о работе в системе:

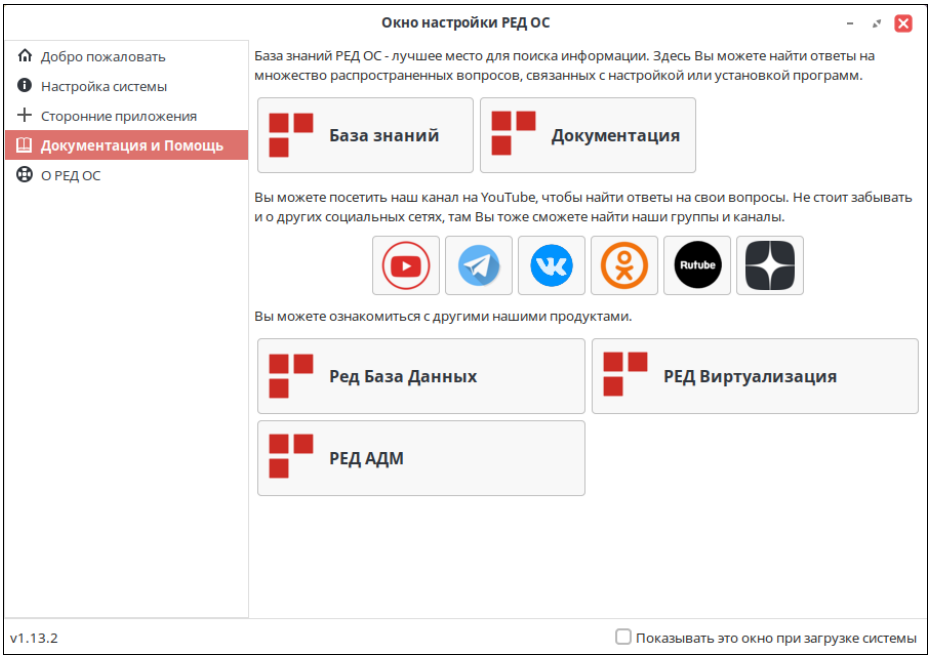
- База знаний;
- Документация.

Перечень доступных для посещения каналов, расположенных на следующих ресурсах:

- Telegram;
- ВКонтакте;
- Одноклассники;
- Rutube;
- Яндекс.Дзен.

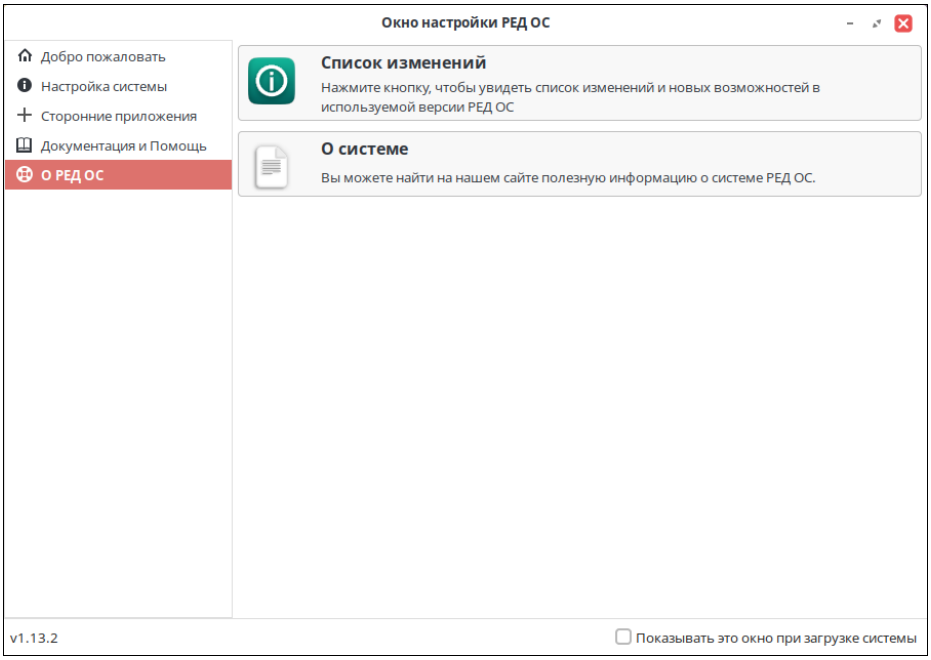
Другие продукты компании РЕД СОФТ, такие как:

- РЕД База Данных;
- РЕД Виртуализация;
- РЕД АДМ.



Вкладка «О РЕД ОС»

Здесь можно получить информацию о новых возможностях системы и перейти на сайт РЕД ОС.



Графическое окружение MATE

Апплеты
Настройка фона рабочего стола
Настройка системной панели
Настройка внешнего вида графического интерфейса РЕД ОС
Настройка шрифтов графического интерфейса РЕД ОС
Настройка хранителя экрана, блокировки и режима энергосбережения
Управление окнами графического интерфейса
Настройка рабочих областей
Работа с файловым менеджером
Автоматический запуск приложений
Настройка смены раскладки клавиатуры

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

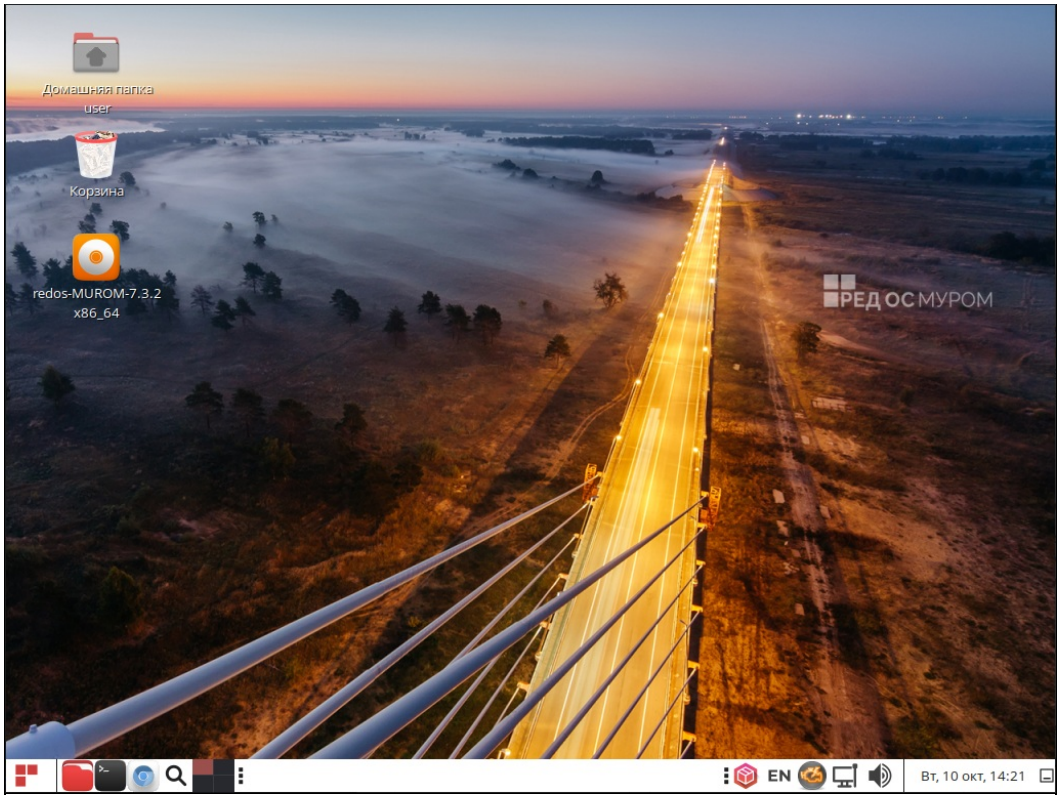
MATE – интегрированное графическое окружение рабочего стола в РЕД ОС.

Вы можете подробнее ознакомиться с возможностями графического окружения **MATE**, просмотрев наши обучающие видео:

- на **RuTube** — Основы работы с DE Mate;
- в **Яндекс.Дзен** — Основы работы с DE Mate.

На наших каналах вы также сможете найти много другой полезной информации.

Графическое окружение **MATE** выглядит следующим образом:

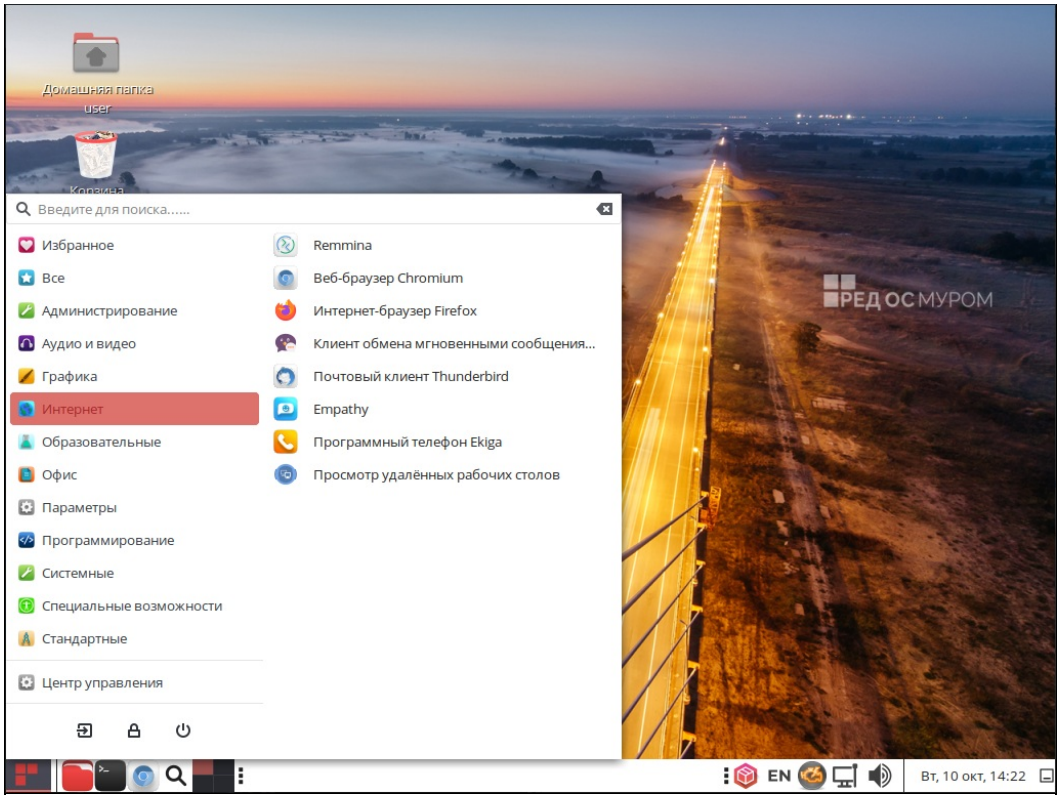


Главным элементом рабочего стола является системная панель, которая расположена в нижней части экрана и условно разделена на три основные части:

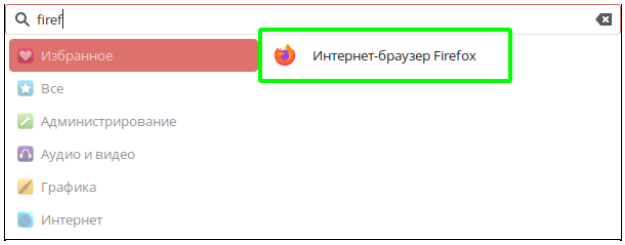
- Главное меню;
- Панель приложений;
- Панель апплетов.

Главное меню — представляет собой список установленных программ, разделенных на несколько категорий, таких как «Аудио и

видео», «Графика», «Интернет», «Офис» и т. д.

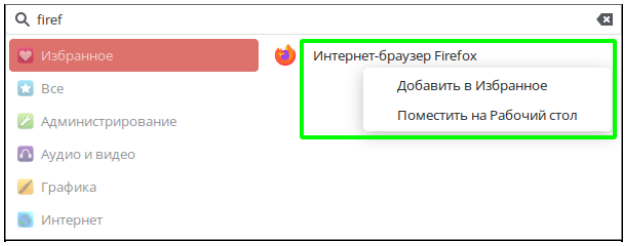


Поисковая строка здесь предназначена для поиска установленных приложений. Начните вводить ключевое слово, чтобы получить список только тех компонентов меню, которые его содержат.



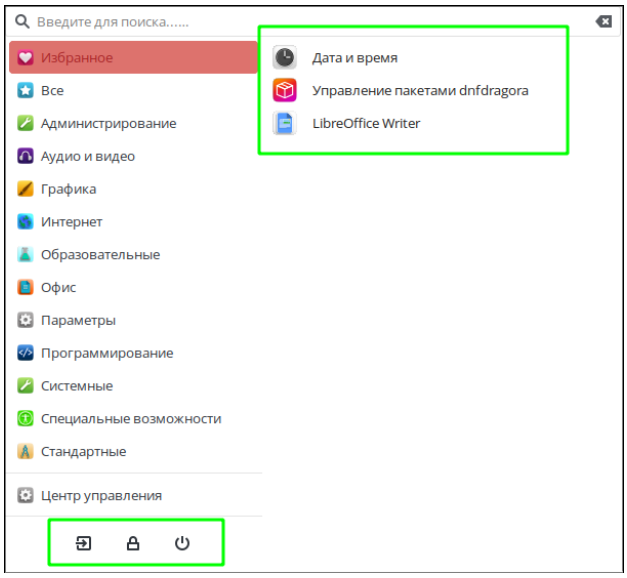
При нажатии ПКМ по какому-либо приложению можно выбрать несколько действий:

- добавить приложение на рабочий стол;
- добавить приложение в избранное.



Список избранного изначально пуст.

Также здесь доступны кнопки блокировки экрана, выхода из сеанса и завершения работы.



Панель приложений представляет собой управляющую панель, которая по умолчанию располагается в нижней части экрана. Управляющая панель включает в себя следующие компоненты:

- кнопка Главного меню ( ) ;
- область запуска приложений — Panel Launcher ( );
- область открытых приложений — Window list (Видео user@localhost:~);
- область системных сообщений — Notifications (1);
- системный лоток (трей) — System Tray, куда помещаются пиктограммы некоторых работающих в фоне приложений ( );
- несколько пиктограмм разного назначения — модуль сетевых соединений, регулятор громкости, часы, индикатор раскладки клавиатуры и т. д. (EN Вт, 10 окт, 14:31).

Апплеты

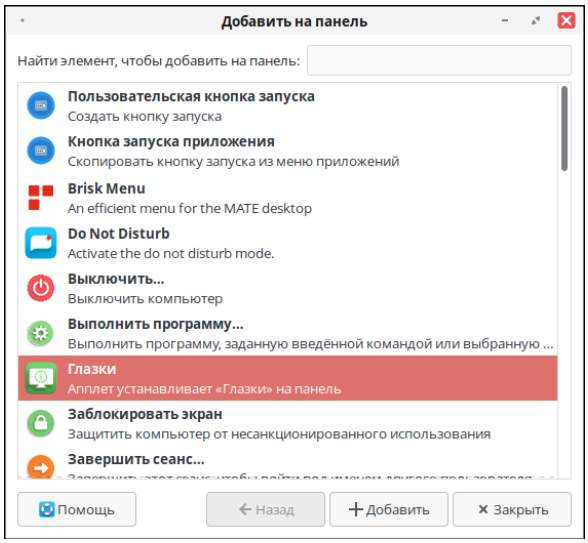
Все области и кнопки панели представляют собой так называемые апплеты – небольшие программы. Апплеты могут как добавляться на панель, так и удаляться с неё. Главное меню, системный лоток, менеджер сети, настройки пользователя — всё это апплеты.

Для добавления новых апплетов на панель нажмите ПКМ по системной панели и в появившемся контекстном меню выберите пункт «Добавить на панель...».

В открывшемся окне можно настроить доступные апплеты.

При выборе какого-либо установленного апплета становится активной строка управления, с помощью которой можно добавить апплет на панель (+ Добавить) или закрыть окно апплетов (× Закрыть).

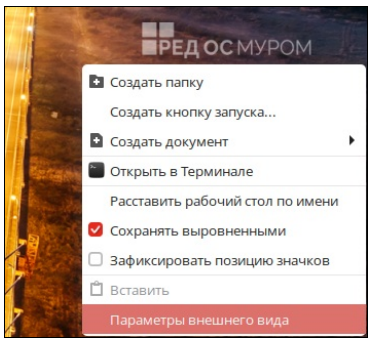
Кнопка «Помощь» вызывает справку по добавлению объектов на системную панель.



Настройка фона рабочего стола

Для смены изображения рабочего стола существует два варианта.

Вариант 1. Для смены фона рабочего стола необходимо в свободной части рабочего стола вызвать контекстное меню (нажав ПКМ). В открывшемся контекстном меню необходимо выбрать пункт «Параметры внешнего вида».

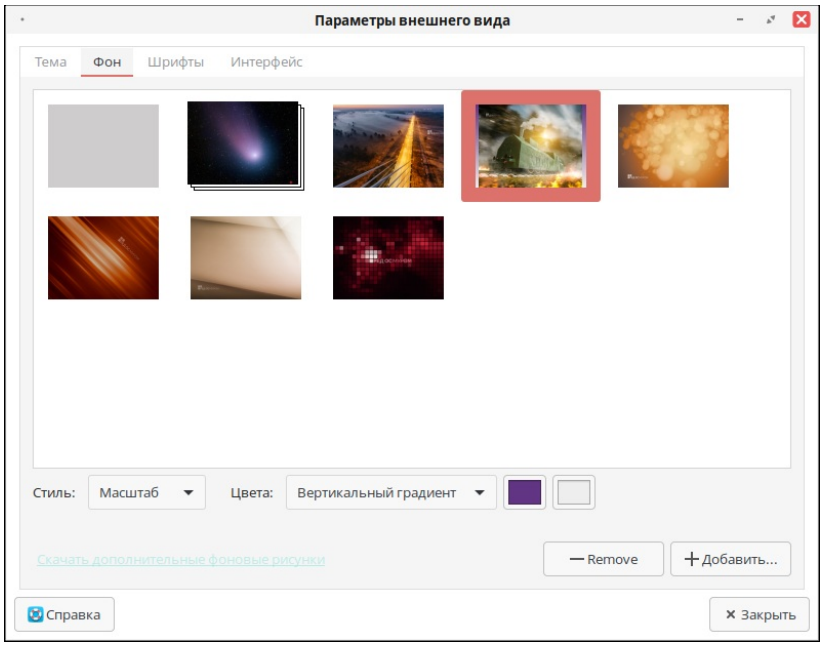


Вариант 2. Для смены фона рабочего стола пользователю необходимо в системной панели выбрать пункт «Главное меню» - «Параметры» - «Внешний вид».

На вкладке «Фон» можно выбрать изображение из имеющихся или добавить собственное, нажав кнопку «Добавить...».

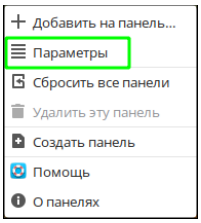
Ненужные изображения можно удалить, нажав «Remove».

Дополнительно можно выбрать стиль отображения фонового рисунка на рабочем столе — мозаика, масштаб, размещение по центру или растягивание, и выбрать вариант заполнения экрана и его цвет.



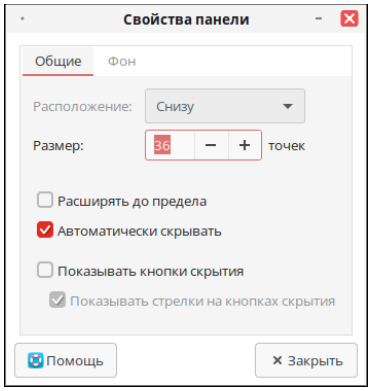
Настройка системной панели

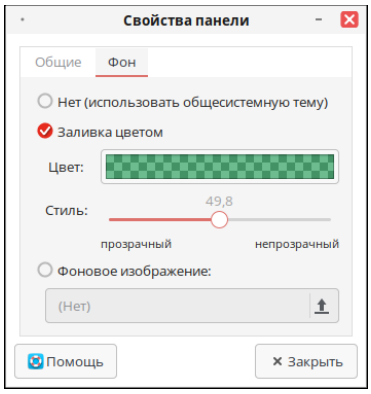
Для изменения параметров панели задач графической оболочки РЕД ОС **MATE** также нужно с помощью клика ПКМ по панели вызвать контекстное меню и выбрать соответствующий пункт меню.



При выборе пункта меню «Параметры» будет открыто окно, в котором на вкладке «Общие» доступны такие настройки, как расположение панели (сверху или снизу), размер панели, внешний вид панели (расширение панели до предела, автоматическое скрытие панели, отображение кнопок скрытия панели).

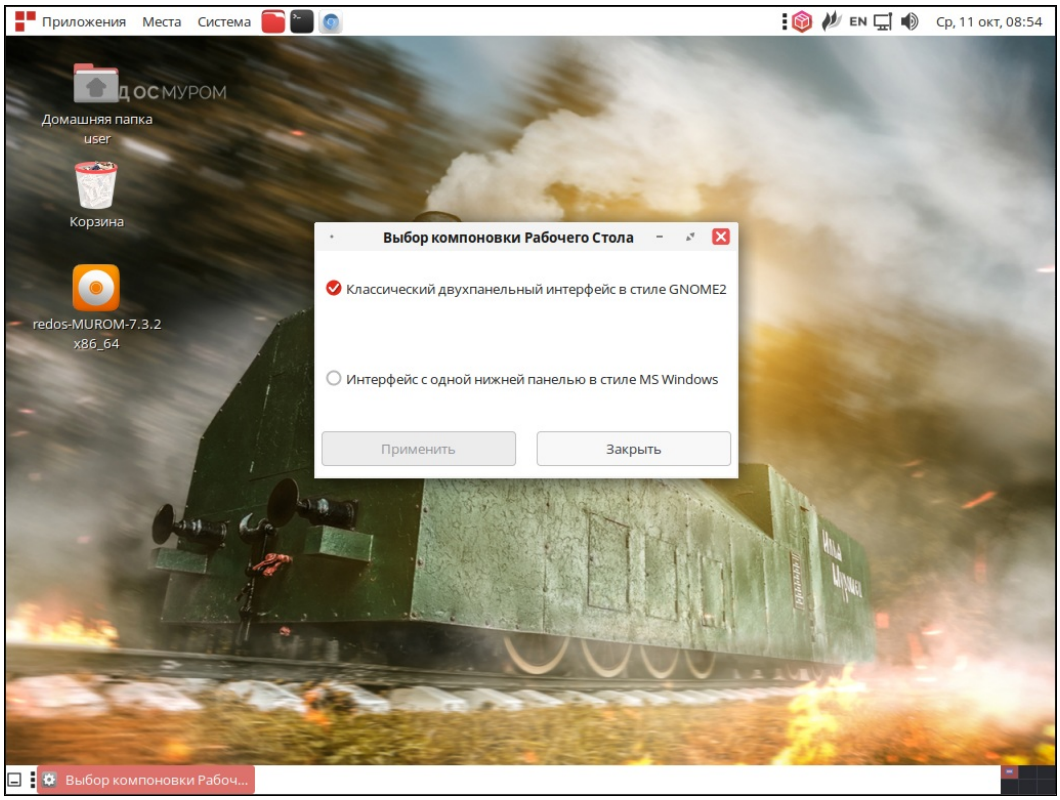
На вкладке «Фон» производится настройка фона системной панели — можно сделать сплошную заливку цветом или выбрать собственное изображение фона панели, а также задать прозрачность.





По умолчанию в графическом окружении **MATE** для удобства пользователей применяется интерфейс с одной нижней панелью, но можно настроить классический двухпанельный интерфейс MATE, открыв «Главное меню» - «Параметры» - «Компоновка панелей» и установив соответствующий параметр.

После применения настроек рабочий стол будет выглядеть следующим образом:



На верхней панели **Главное меню** разделяется на пункт «Приложения», где доступны установленные программы, и пункт «Система», где доступны настройки системы и кнопки выключения питания, завершения сеанса и блокировки экрана.

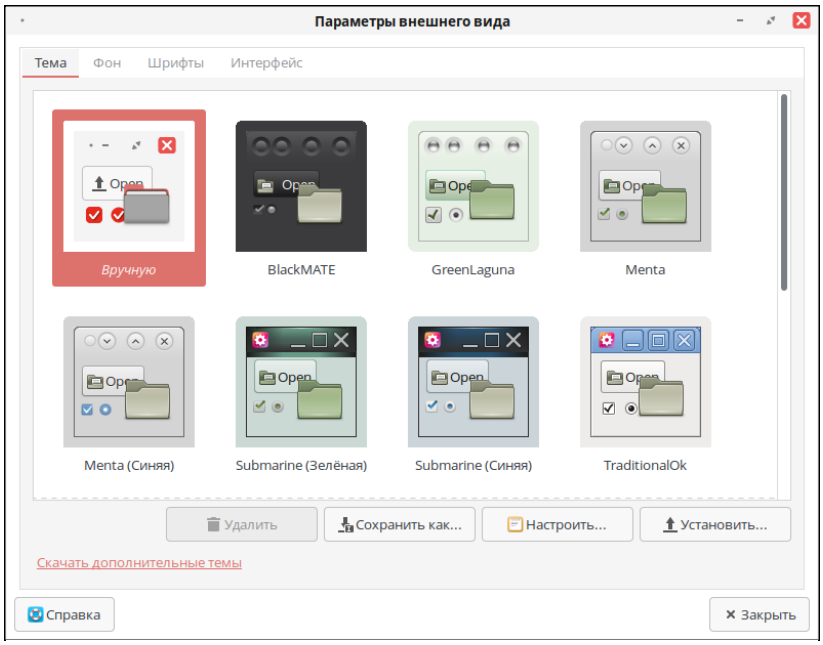
В пункте «Места» расположены доступные пользователю каталоги, настройка сети, инструмент поиска и недавние документы.

Также здесь отображаются закрепленные для быстрого доступа приложения и системный трей.

На нижней панели располагается кнопка для сворачивания всех открытых окон и открытия рабочего стола, список открытых окон и переключатель рабочих областей.

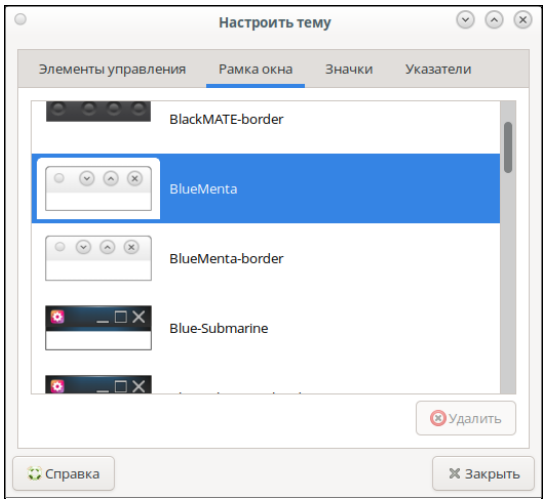
Настройка внешнего вида графического интерфейса РЕД ОС

Для смены внешнего вида окон графической оболочки РЕД ОС пользователю необходимо на свободной области рабочего стола вызвать контекстное меню (нажав ПКМ), выбрать пункт меню «Параметры внешнего вида» и перейти на вкладку «Тема».



Здесь можно обратиться к коллекции доступных тем. Для установки понравившейся темы нажмите «Установить».

Также можно задать стилевое оформление отдельных элементов интерфейса, полностью независимое друг от друга и от темы рабочего стола, нажав кнопку «Настроить».

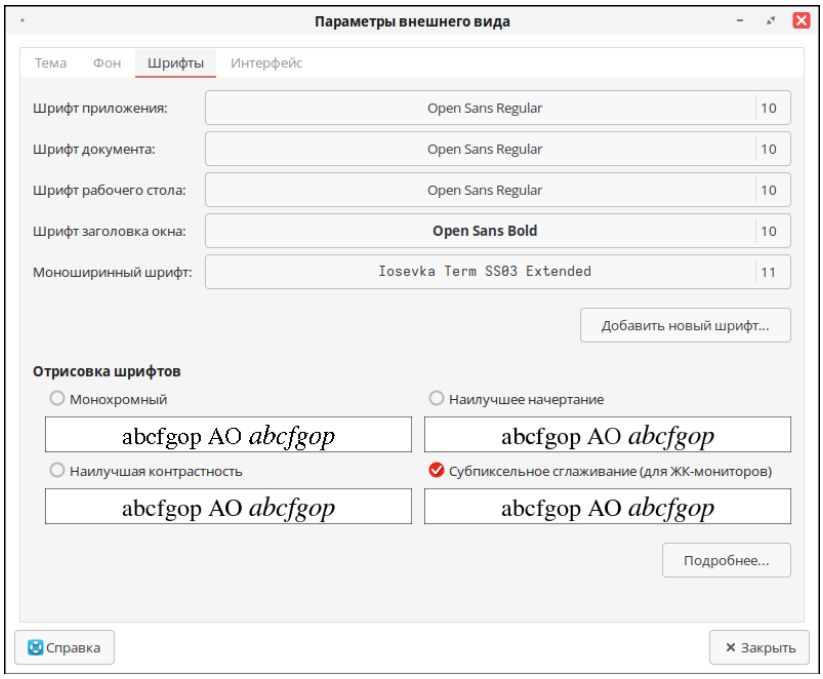


Большое количество доступных вариантов позволяют комбинировать элементы оформления интерфейса в широких пределах, достигая максимального визуального эффекта. Это имеет практическое значение, особенно для людей с плохим зрением или нарушением цветовосприятия.

Настройка шрифтов графического интерфейса РЕД ОС

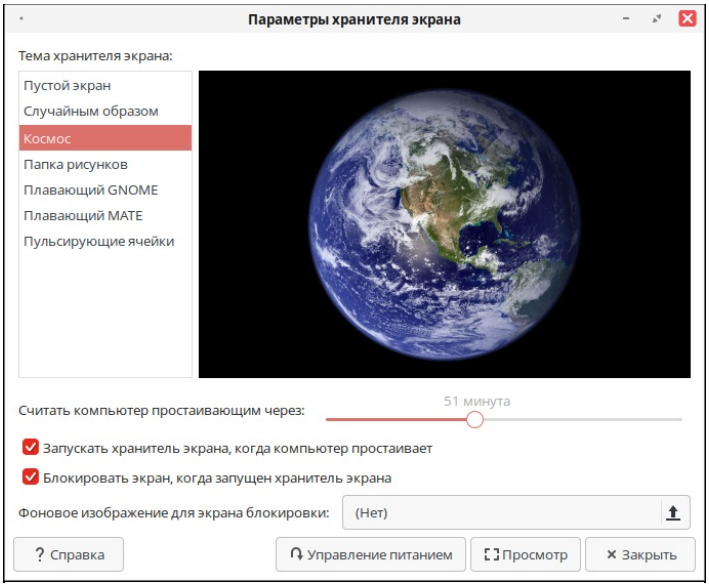
Для изменения используемых шрифтов графической оболочки РЕД ОС пользователю необходимо на свободной области рабочего стола вызвать контекстное меню (нажав ПКМ), выбрать пункт меню «Параметры внешнего вида» и перейти на вкладку «Шрифты».

В окне можно настроить шрифты как для заголовков окон, так и для документов.

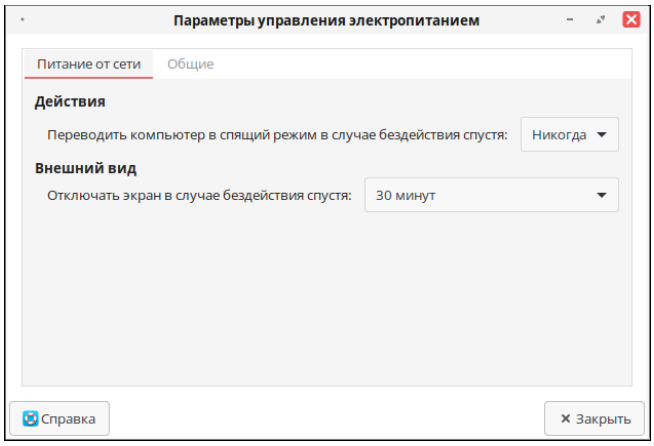


Настройка хранителя экрана, блокировки и режима энергосбережения

Настройка времени блокировки рабочего стола, настройка хранителя экрана, а также управление режимом энергосбережения определяется утилитой «Хранитель экрана». Данная утилита находится в «Главном меню» - «Параметры».



Утилита позволяет пользователю определить время, по истечении которого, при бездействии пользователя, рабочий стол системы будет заблокирован, выбрать тему хранителя экрана и определить режимы управления питанием.

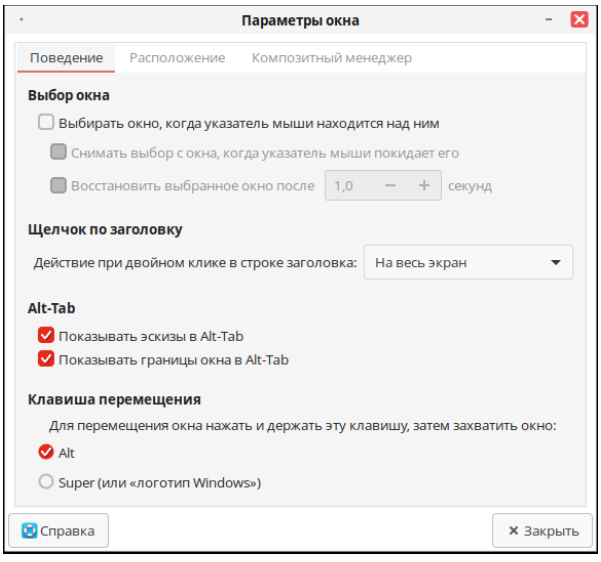


Управление окнами графического интерфейса

Управление окнами подразумевает в первую очередь переключение между ними.

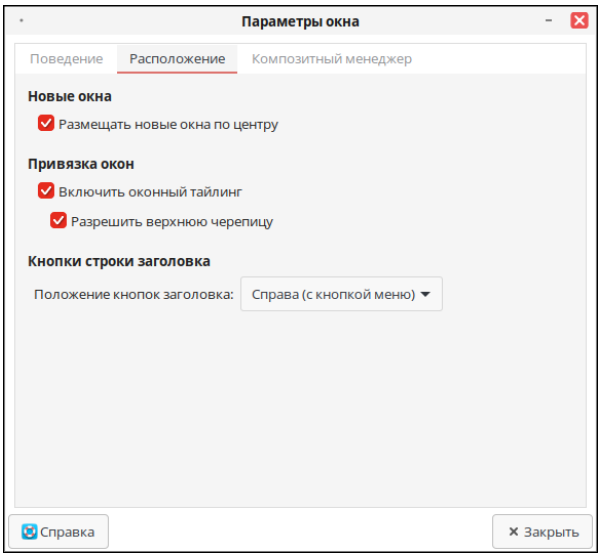
Для настройки параметров окон необходимо открыть «Главное меню» - «Параметры» - «Окна».

На вкладке «Поведение» можно настроить отклик окон на поведение мыши, а также настроить переключение между окнами при помощи комбинации клавиш **Alt+Tab**.

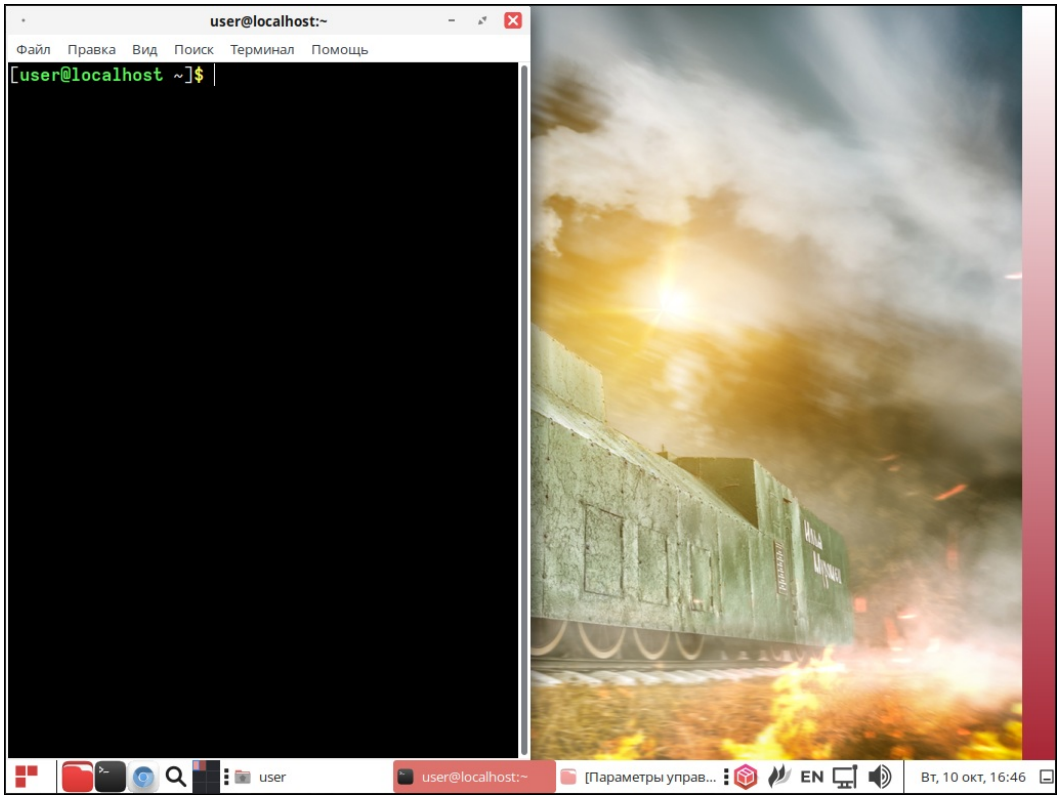


На вкладке «Расположение» настраивается положение новых окон и оконный тайлинг (привязка окна к какой-либо части экрана).

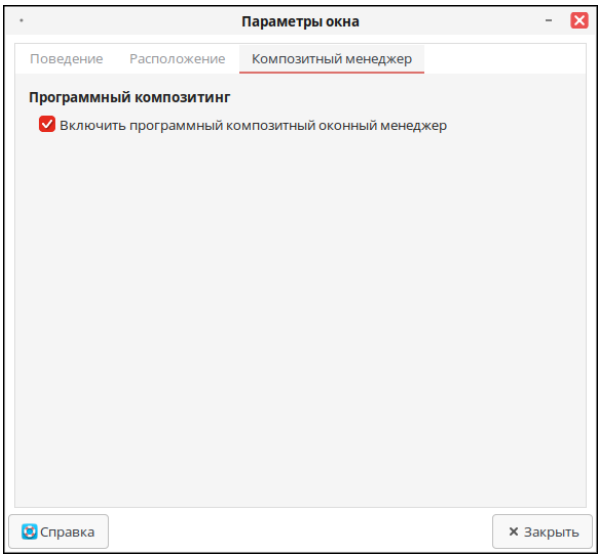
Также здесь можно сменить расположение кнопок заголовка — слева или справа.



При перетаскивании окна мышью к верхней границе экрана оно занимает верхнюю его половину. Аналогичное движение к нижней границе экрана разворачивает окно на нижнюю его половину. Перемещение окна к боковой стороне экрана (левой или правой) прикрепляет его на левую или правую половины, в зависимости от стороны перетаскивания.



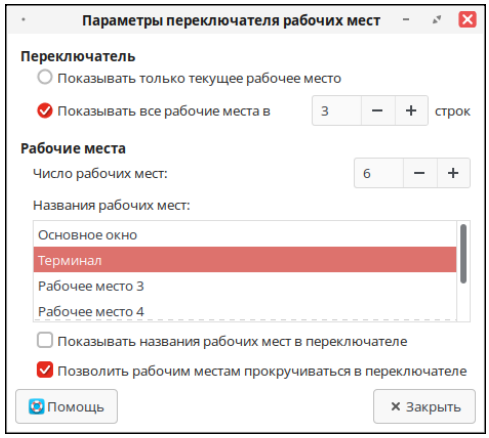
На вкладке «Композитный менеджер» включается или отключается использование композитного оконного менеджера.



Настройка рабочих областей

В **MATE** существуют дополнительные рабочие пространства, по умолчанию доступно 4 рабочие области. При нажатии клавиш **Ctrl+Alt+Up** (стрелка вверх) на экран выводятся все доступные рабочие области. Здесь можно легко переключиться на необходимую рабочую область. Для быстрого переключения между областями воспользуйтесь клавишами **Ctrl+Alt + Right** (стрелка вправо) или **Left** (стрелка влево).

Переключатель рабочих областей находится на системной панели. Задать нужные настройки, создать новые рабочие области и переименовать имеющиеся можно, кликнув ПКМ по апплету переключателя рабочих областей и выбрав в появившемся контекстном меню пункт «Настройка».



Работа с файловым менеджером

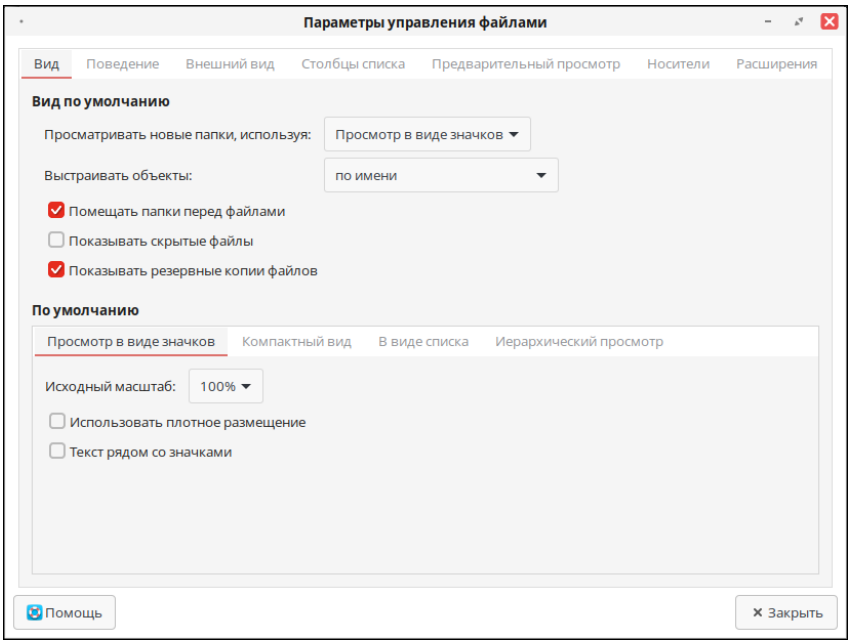
По умолчанию в **MATE** используется файловый менеджер **Caja**. Далее будут рассмотрены некоторые основные возможности файлового менеджера.

При нажатии клавиши **F3** можно разделить рабочую зону на две части.

При помощи сочетания клавиш **Ctrl+1**, **Ctrl+2**, **Ctrl+3** можно изменить вид отображения каталогов и файлов — значки, список или компактный вид.

Через пункт панели инструментов «Закладки» можно создавать новые закладки, прикреплять новые каталоги в быстрый доступ и т.д.

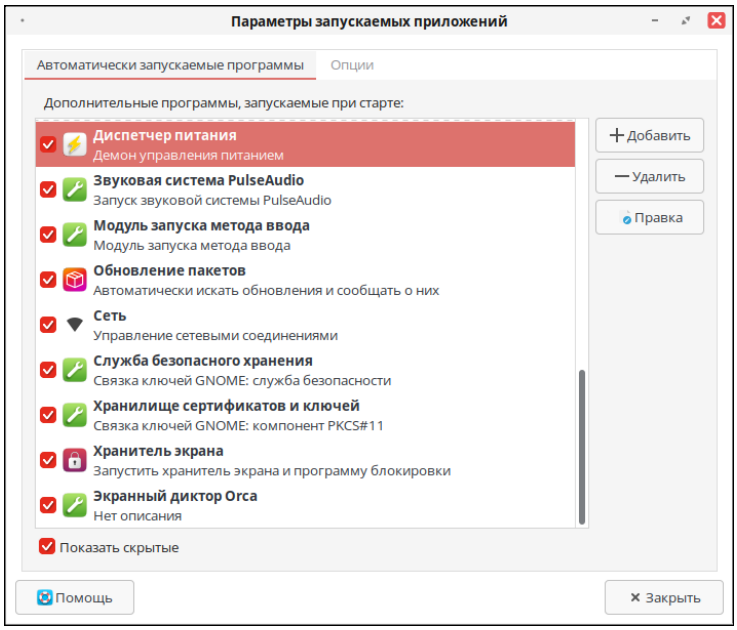
Для тонкой настройки отображения каталогов и их содержимого, поведения мыши, внешнего вида, списков, предварительного просмотра, внешних носителей и дополнительных расширений необходимо выбрать на панели инструментов пункт меню «Правка» - «Параметры».



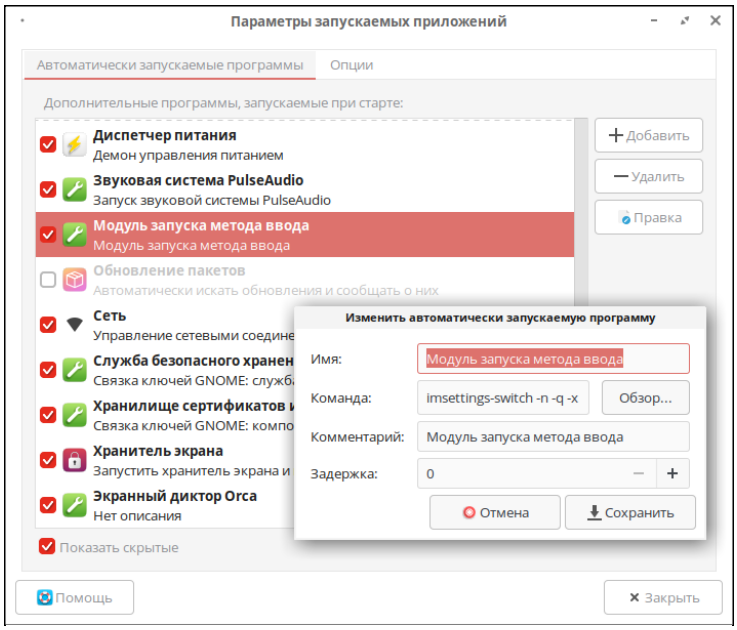
Также есть множество других настроек, которые позволят комфортно работать с файловым менеджером.

Автоматический запуск приложений

В «Главном меню» - «Параметры» - «Запускаемые приложения» доступна настройка автоматически запускаемых программ при старте системы.

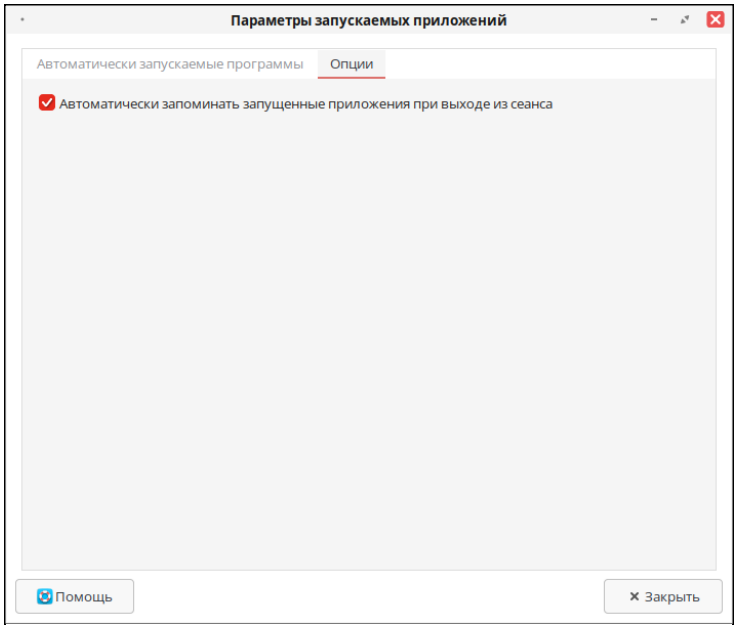


На вкладке «Автоматически запускаемые программы» можно отключить ненужные для запуска приложения, сняв флаг, установленный рядом с ним. Можно внести изменения в настроенные и включенные программы или просмотреть подробные сведения, нажав кнопку «Правка».



Также можно добавить новые необходимые для запуска программы или удалить из списка имеющиеся, нажав соответственно «Добавить» или «Удалить».

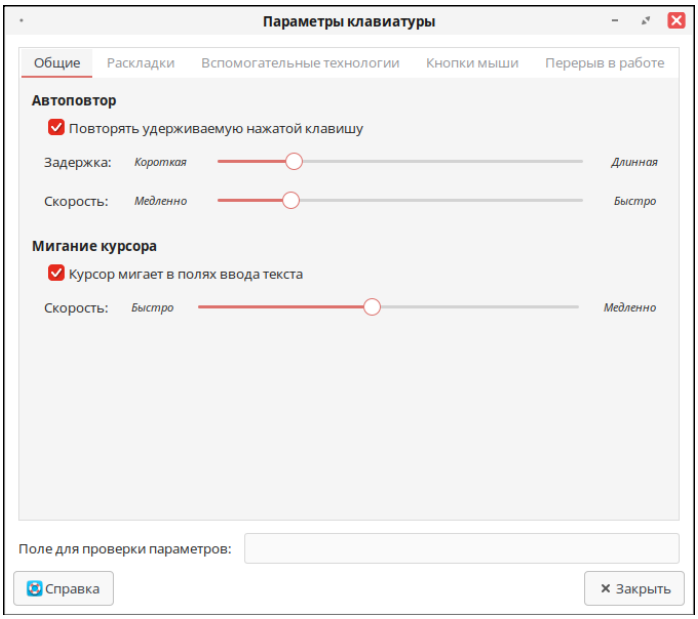
На вкладке «Опции» доступна настройка запоминания запущенных приложений при выходе из сеанса, т. е. при следующем старте системы открытые ранее программы будут автоматически запущены.



Настройка смены раскладки клавиатуры

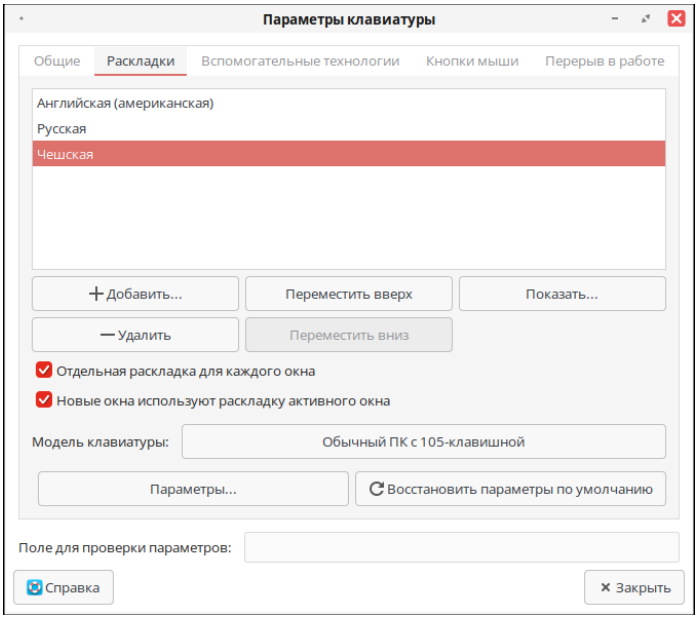
В РЕД ОС по умолчанию смена раскладки клавиатуры (языка ввода) осуществляется при одновременном нажатии функциональных клавиш клавиатуры **Shift+Alt** одновременно. Для изменения сочетания функциональных клавиш, применяемых для смены раскладки клавиатуры, необходимо в системной панели перейти в «Главное меню» - «Параметры» - «Клавиатура».

На вкладке «Общие» задается автоповтор нажатых клавиш и скорость мигания курсора в полях ввода.

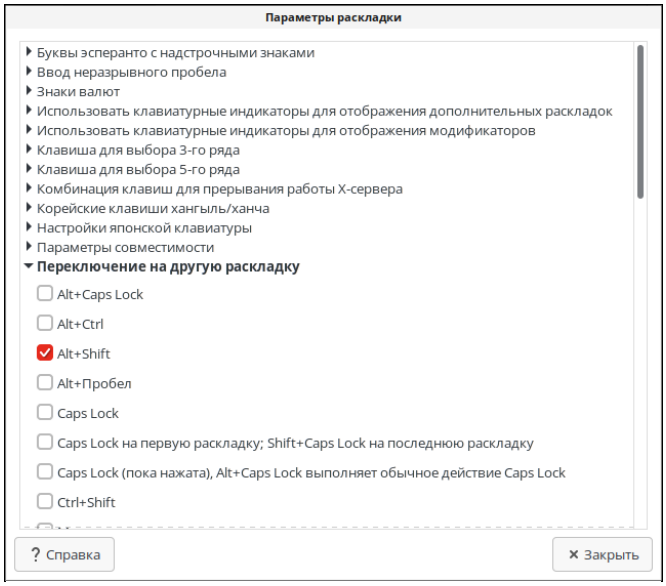


На вкладке «Раскладки» задается порядок раскладки клавиатуры, также можно добавить новые языки, переместить выбранную раскладку выше или ниже в списке, удалить ненужную раскладку.

Дополнительно можно выбрать модель клавиатуры, определить раскладки клавиатуры для других рабочих областей.

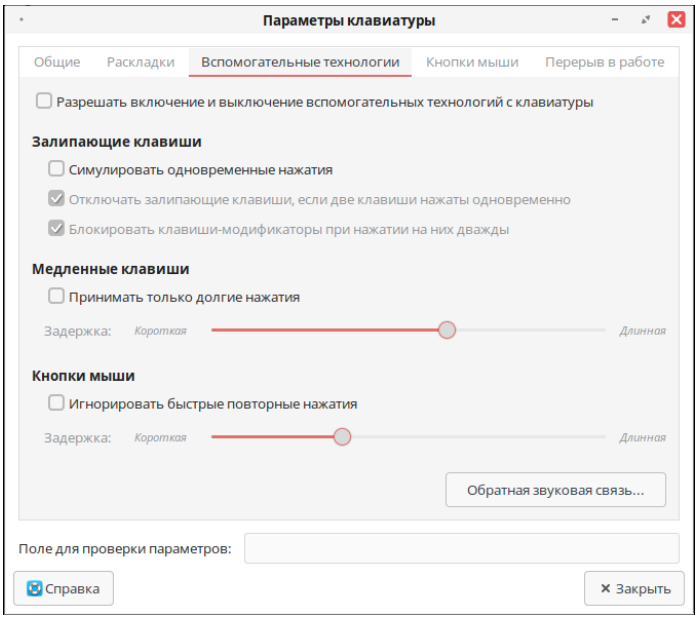


При нажатии на кнопку «Параметры» можно изменить сочетания клавиш клавиатуры по умолчанию.

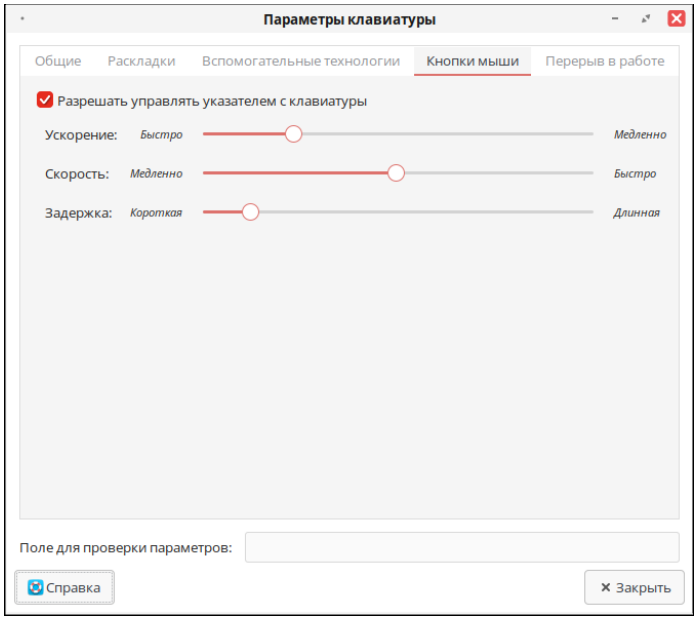


На вкладке «Вспомогательные возможности» определяется необходимость использования вспомогательных технологий с клавиатуры,

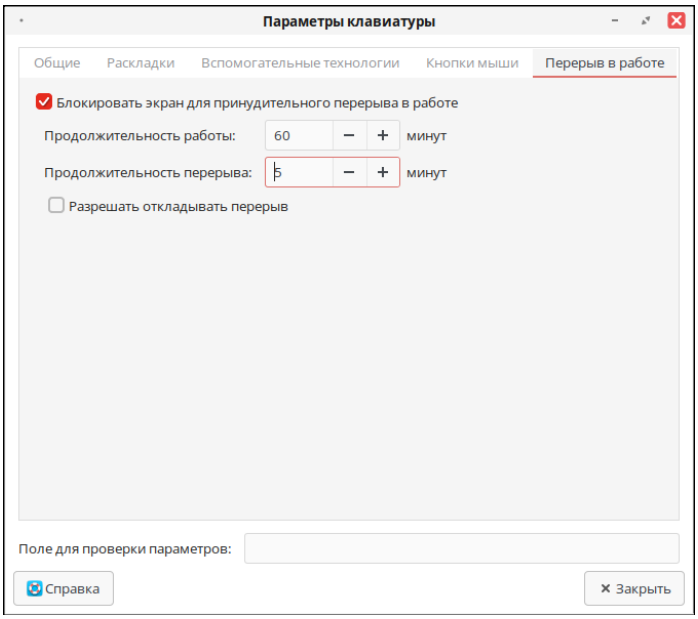
задается поведение залипающих клавиш, медленные нажатия и реагирование на кнопки мыши. Также можно настроить обратную звуковую связь, например, при активном **Caps Lock** и нажатии какой-либо клавиши будет подаваться звуковой сигнал.



На вкладке «Кнопки мыши» задается разрешение на управление курсором мыши с клавиатуры.



На вкладке «Перерыв в работе» можно задать продолжительность работы и перерыва. При достижении указанной продолжительности работы экран будет заблокирован.


Параметры клавиатуры
Общие
Раскладки
Вспомогательные технологии
Кнопки мыши
Перерыв в работе
Блокировать экран для принудительного перерыва в работе
Продолжительность работы:
60
минут
Продолжительность перерыва:
5
минут
Разрешать откладывать перерыв
Поле для проверки параметров:
Справка
Закрыть

Графическое окружение KDE Plasma

Общая информация
Информация об учётной записи
Настройка фона рабочего стола пользователя РЕД ОС
Настройка внешнего вида графического интерфейса РЕД ОС
Настройка шрифтов графического интерфейса РЕД ОС
Настройка хранителя экрана, блокировки и режима энергосбережения
Настройка смены раскладки клавиатуры
Управление элементами панели

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

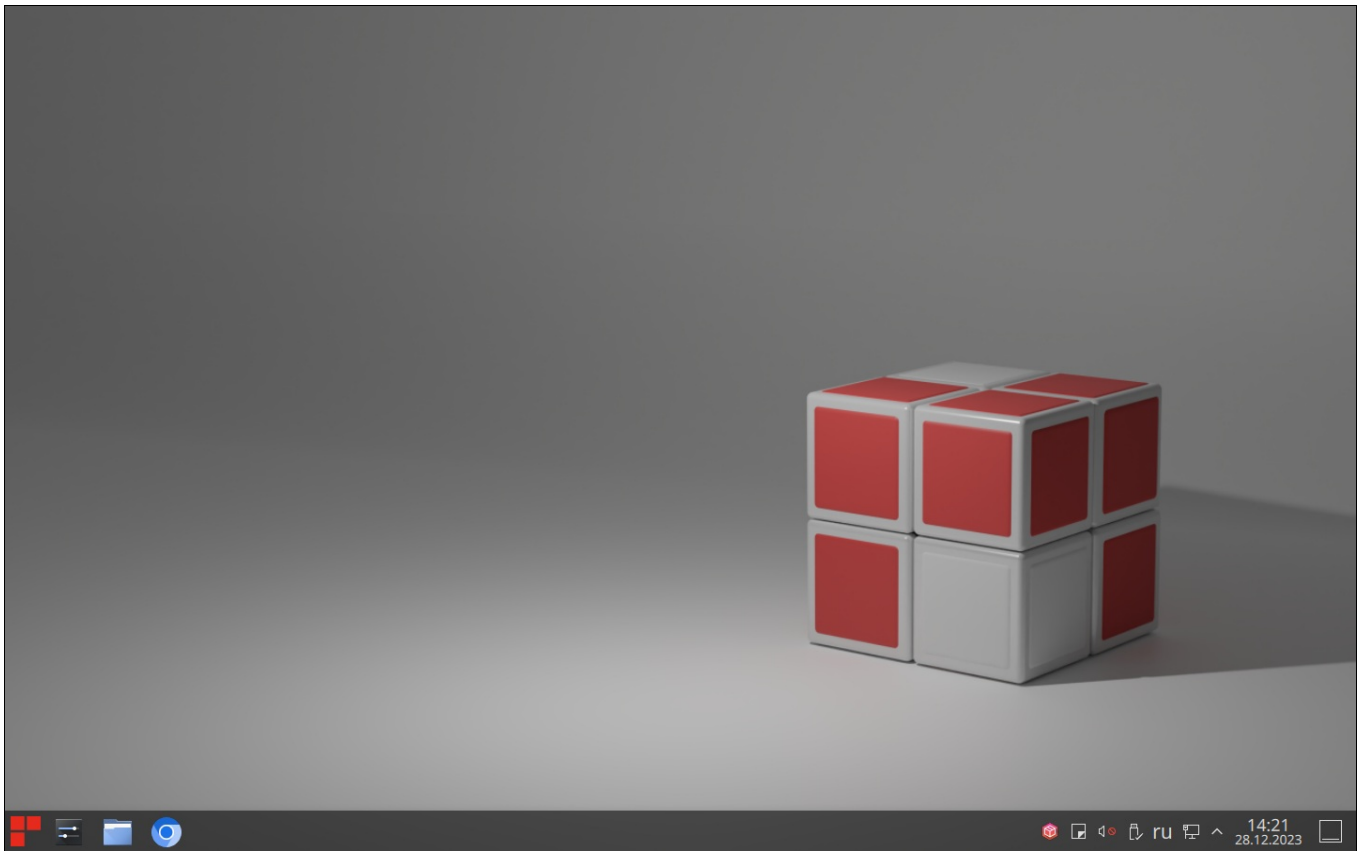
KDE Plasma — это среда рабочего стола, созданная сообществом **KDE**. **Plasma** предоставляет пользователю современное настраиваемое окружение рабочего стола для работы с приложениями и доступа к необходимой информации. К основным отличительным свойствам рабочего стола **Plasma** относятся улучшенное управление окнами и эффектами рабочего стола, поддержка виджетов **KDE Plasma**, интегрированный поиск, управление аппаратными средствами и высокая степень настраиваемости.

Вы можете подробнее ознакомиться с возможностями графического окружения **KDE Plasma**, просмотрев наши обучающие видео:

- на **RuTube** — Обзор графического окружения KDE Plasma;
- в **Яндекс.Дзен** — Обзор графического окружения KDE Plasma;
- в **VK Видео** — Обзор графического окружения KDE Plasma.

На наших каналах вы также сможете найти много другой полезной информации.

Графическое окружение **KDE Plasma** выглядит следующим образом:



Навигационное пространство рабочего стола РЕД ОС состоит из двух зон управления:

- **Системная панель** – панель, расположенная по умолчанию в нижней части экрана. Системная панель обеспечивает доступ пользователя к главному меню запуска всех установленных программ, содержит апплеты и элементы управления работой РЕД ОС;
- **Рабочее пространство** – все свободное пространство рабочего стола, предназначенное для расположения файлов данных и ярлыков часто используемых программ. Рабочее пространство может быть оформлено фоном рабочего стола.

Управление графическим интерфейсом РЕД ОС пользователь может осуществлять при помощи мыши или клавиатуры. Правая клавиша мыши (ПКМ) по умолчанию используется для вызова контекстных свойств любого графически представленного в интерфейсе РЕД ОС объекта. Левая клавиша мыши (ЛКМ) по умолчанию используется для инициации действий с любым графическим объектом в интерфейсе РЕД ОС.

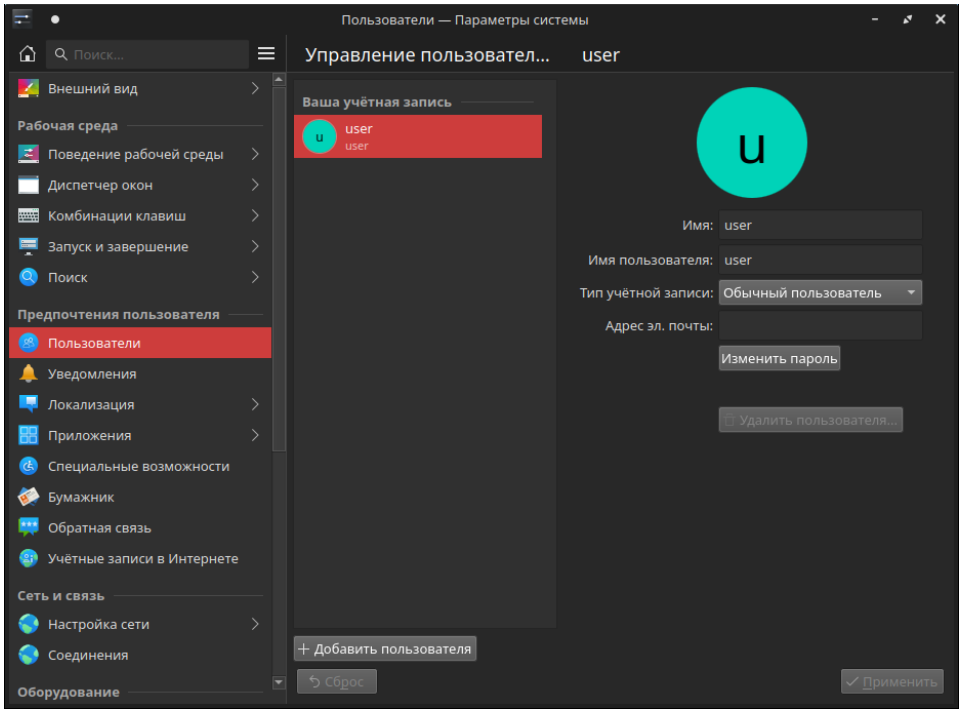
Общие методы работы пользователя с графическим интерфейсом РЕД ОС являются общепринятыми методами работы пользователей с графическими интерфейсами операционных систем. Основными элементами графического интерфейса РЕД ОС являются окна, панели, кнопки, меню, поля ввода, списки выбора, апплеты, радиокнопки, скроллеры и т.д.

Общая информация

Набор утилит управления РЕД ОС находится в «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**». Некоторые утилиты управления и конфигурирования РЕД ОС могут потребовать привилегий администратора РЕД ОС.

Информация об учётной записи

В РЕД ОС (среда **KDE Plasma**) пользователю доступна настройка реквизитов учётной записи пользователя. Настройка производится из «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» в подразделе «**Пользователи**».



Управление пользователями позволяет производить изменения следующих групп реквизитов учётной записи:

- полное имя пользователя, отображаемое в системе и окне выбора пользователя загрузчика;
- тип учетной записи — обычный пользователь или администратор (для повышения привилегий обычного пользователя до администратора потребуются права суперпользователя);
- адрес электронной почты.

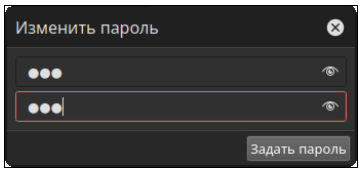
Указанная пользователем информация сохраняется в локальной БД пользователей РЕД ОС.

Пользователю доступно редактирование информации только о своей учётной записи, которая использовалась для аутентификации в РЕД ОС.

Также пользователь может отредактировать используемую пиктограмму, ассоциируемую с учётной записью, и изменить текущий пароль.

В ОС могут быть заданы политики сложности, предъявляемые к используемым паролям.

При выполнении процедуры смены пароля пользователь сразу задает новый пароль и подтверждает его повторным вводом в соответствующих полях. Для смены пароля пользователя необходимы права администратора ОС.



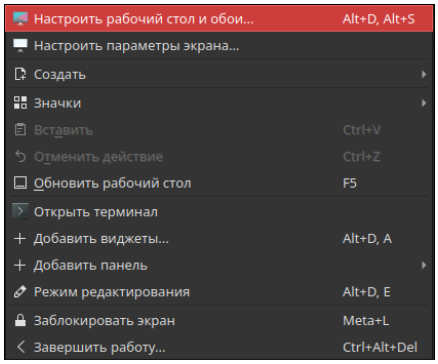
Если введённый пользователем новый пароль нарушает параметры требований к паролям, то РЕД ОС выводит текст предупреждения о нарушении политик с описанием требования, которому новый пароль не соответствует.

На любом этапе операции смены пароля пользователь может прервать смену пароля при помощи кнопки «**Закрыть**».

По окончании операции смены пароля РЕД ОС выводит пользователю сообщение об успешном изменении атрибутов безопасности пользователя.

Настройка фона рабочего стола пользователя РЕД ОС

Для смены фона рабочего стола необходимо в свободной части рабочего стола вызвать контекстное меню (нажав ПКМ). В открывшемся контекстном меню необходимо выбрать пункт «**Настроить рабочий стол и обои...**».

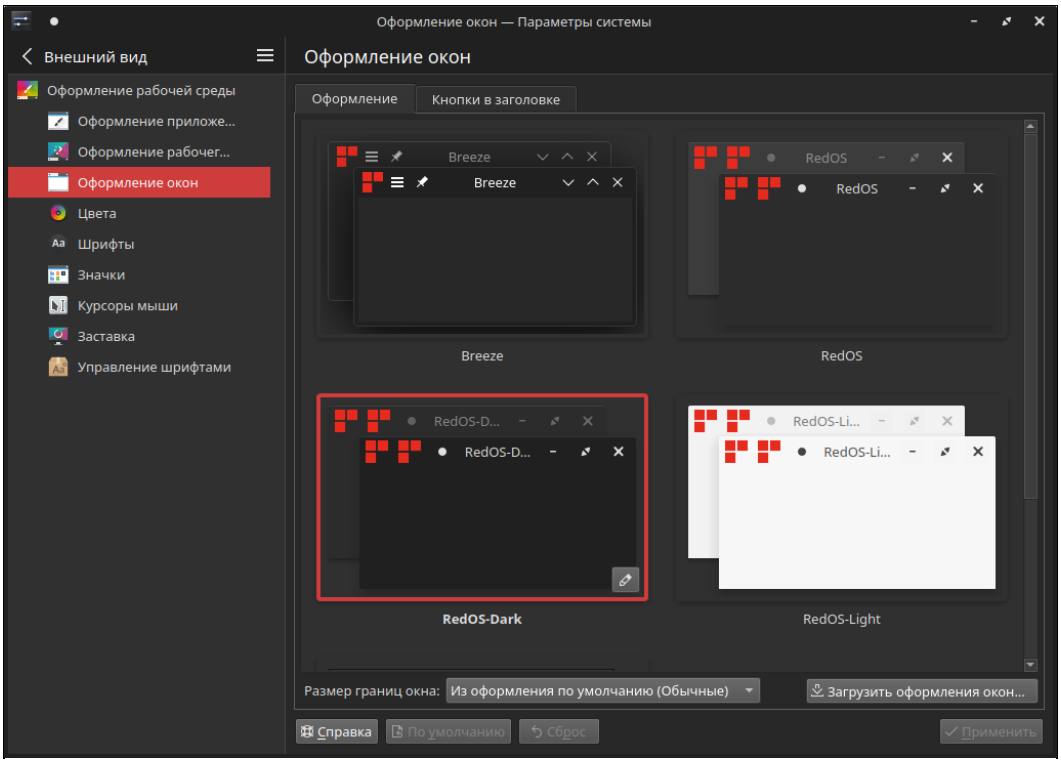


Дополнительно можно выбрать стиль отображения фонового рисунка на рабочем столе — масштабирование с кадрированием, на весь рабочий стол, по центру пропорционально, по центру, черепицей.

Также доступен выбор типа обоев — одноцветные обои, изображение, слайд-шоу, изображение дня и дополнительные модули. Доступна загрузка новых модулей и изображений.

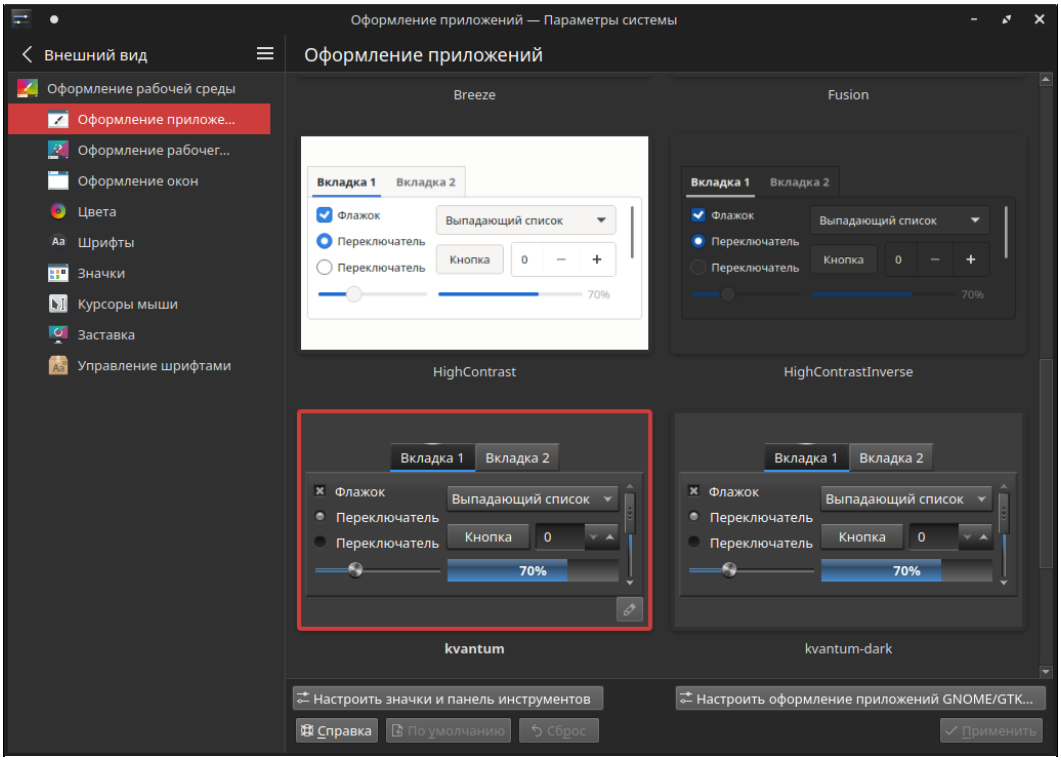
Настройка внешнего вида графического интерфейса РЕД ОС

Для смены внешнего вида окон графической оболочки РЕД ОС пользователю необходимо открыть «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» и выбрать раздел «**Внешний вид**», в открывшемся окне необходимо перейти во вкладку «**Оформление окон**».



Здесь можно обратиться к коллекции доступных тем. Для установки понравившейся темы необходимо выбрать ее и нажать «**Применить**». Дополнительно можно настроить размеры границ окон и загрузить новые оформления окон.

Также можно задать стилевое оформление отдельных элементов интерфейса, полностью независимое друг от друга и от темы рабочего стола. Для этого необходимо перейти во вкладку «**Оформление приложений**».

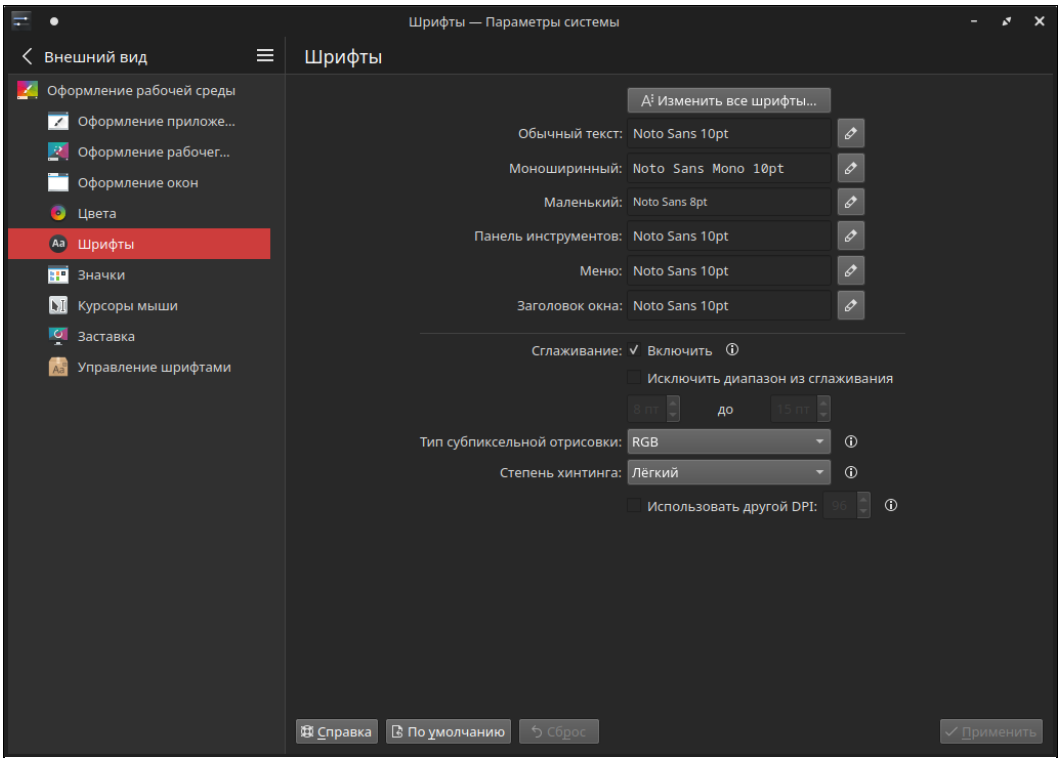


Дополнительно есть возможность настройки значков и панели инструментов, а также отображения приложений **GNOME/GTK**.

Настройка шрифтов графического интерфейса РЕД ОС

Для изменения используемых шрифтов графической оболочки РЕД ОС пользователю необходимо открыть «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» и выбрать раздел «**Внешний вид**», в открывшемся окне необходимо перейти во вкладку «**Шрифты**».

В окне можно настроить шрифты как для заголовков окон, так и для документов.



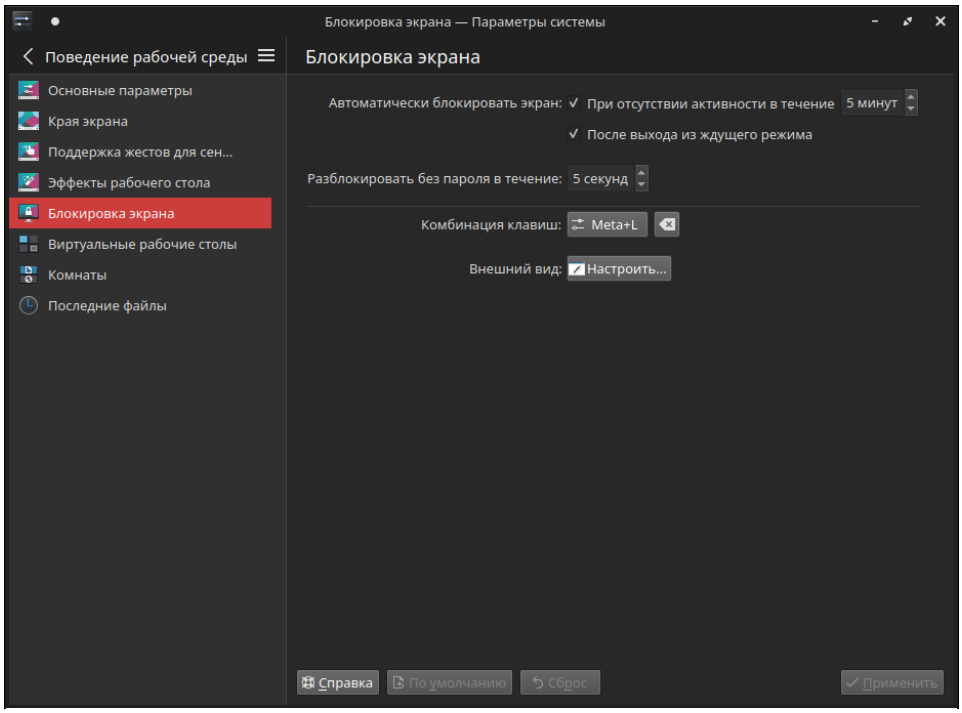
В открывшемся окне пользователь может настроить шрифты, которые будут использованы по умолчанию в системных утилитах, документах и в оформлении окружения.

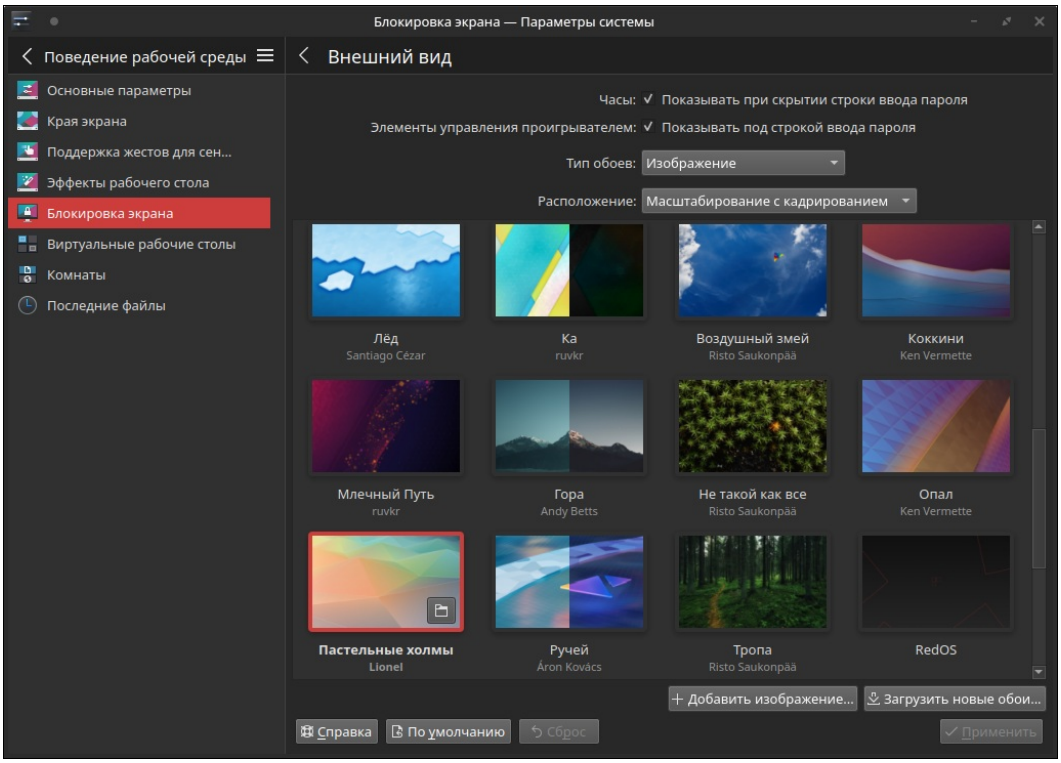
Для подтверждения настройки необходимо нажать «**Применить**».

Настройка хранителя экрана, блокировки и режима энергосбережения

Настройка времени блокировки рабочего стола определяется утилитой настройки поведения рабочей среды. Для настройки необходимо открыть «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» и выбрать подраздел «**Поведение рабочей среды**». В открывшемся окне необходимо перейти во вкладку «**Блокировка экрана**».

Утилита позволяет пользователю определить время, по истечении которого, при бездействии пользователя, рабочий стол РЕД ОС будет заблокирован, задать комбинацию клавиш для быстрой блокировки рабочего стола и настроить графическое оформление блокировки экрана.

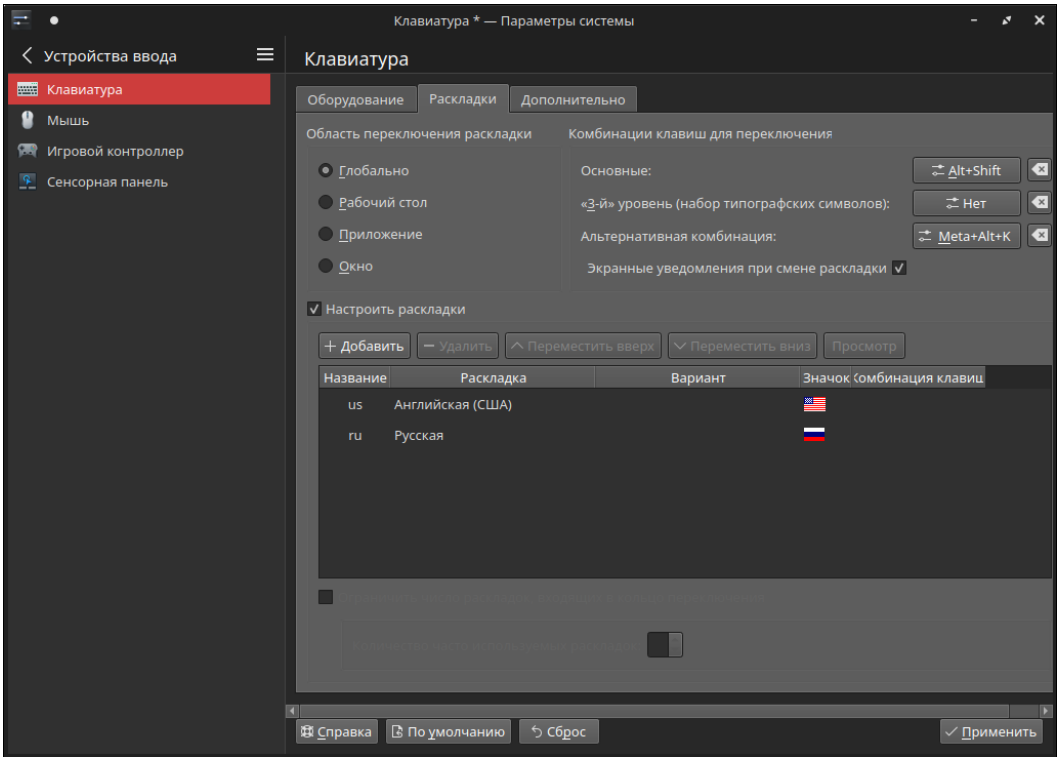




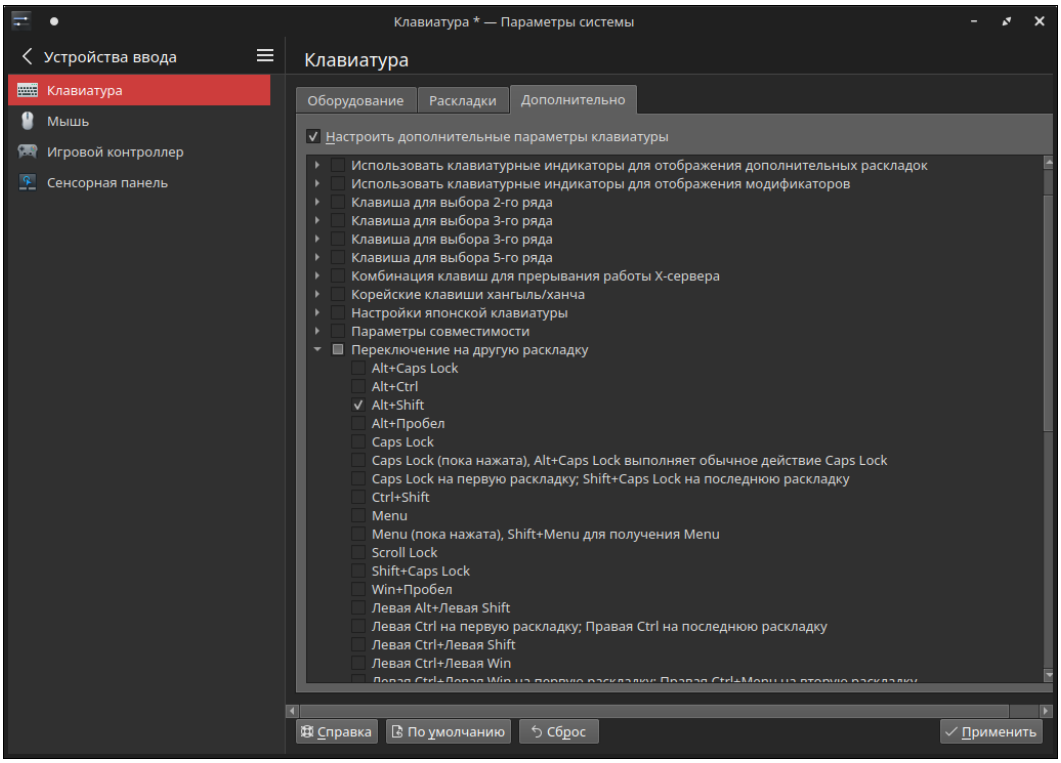
Настройка смены раскладки клавиатуры

В РЕД ОС по умолчанию смена раскладки клавиатуры (языка ввода) осуществляется при одновременном нажатии функциональных клавиш клавиатуры **Shift+Alt**.

Для настройки раскладок клавиатуры необходимо открыть «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**», выбрать подраздел «**Устройства ввода**» и перейти во вкладку «**Клавиатура**» — «**Раскладки**».



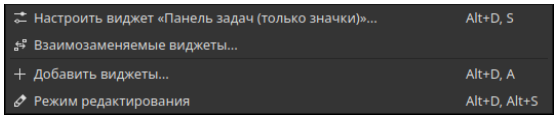
Для изменения установленных по умолчанию комбинаций клавиш смены раскладки клавиатуры пользователю необходимо открыть вкладку «**Дополнительно**» и указать из списка выбора «**Переключение на другую раскладку**» необходимые клавиши для смены раскладки клавиатуры.



Подтверждение произведённых изменений пользователь осуществляет кнопкой «**Применить**».

Управление элементами панели

Для выбора в системной панели рабочего стола необходимых элементов пользователю необходимо на системной панели нажать ПКМ и в появившемся контекстном меню выбрать действие «**Добавить виджеты...**».



В открывшемся окне пользователь может выбрать из перечня доступных виджетов нужный и добавить его на панель нажатием ЛКМ. Если виджет уже добавлен на панель, в левом верхнем углу отображается счетчик копий добавленных виджетов.



В результате действий пользователя на системной панели должен появиться соответствующий приложению индикатор.

Графическое окружение GNOME

Общая информация
Информация об учётной записи
Настройка фона рабочего стола пользователя РЕД ОС
Настройка внешнего вида графического интерфейса РЕД ОС
Настройка шрифтов графического интерфейса РЕД ОС
Настройка смены раскладки клавиатуры
Управление элементами панели

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

GNOME — это интегрированное графическое окружение рабочего стола в РЕД ОС. **GNOME** предоставляет пользователям интуитивно понятную рабочую среду, а также платформу разработки — обширный каркас для создания приложений, интегрируемых с рабочей средой.

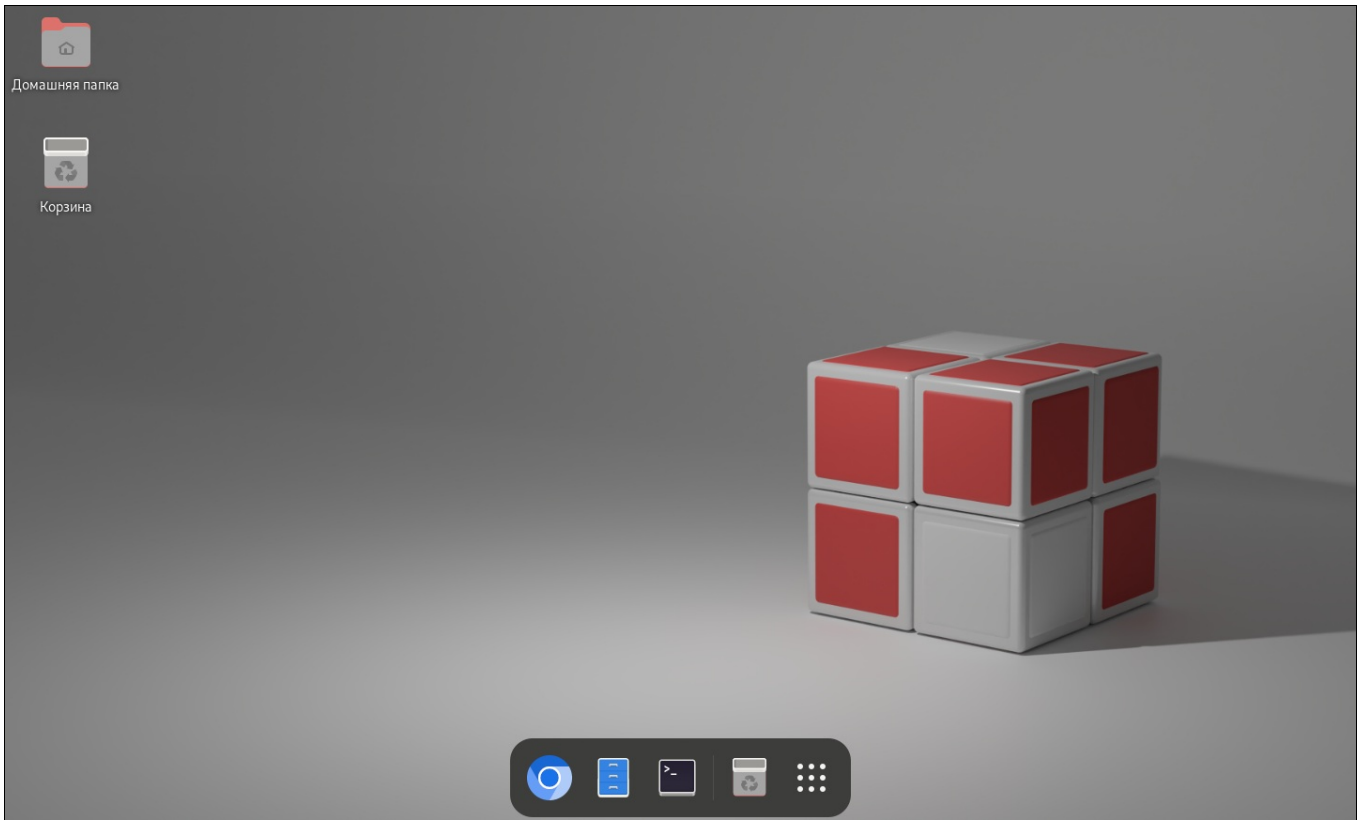
Функциональность **GNOME Shell** может быть расширена с помощью дополнительных расширений, которые могут быть написаны с помощью **JavaScript**. Помимо создания сценариев поведения элементов **GNOME Shell**, возможно изменять внешний вид среды рабочего стола при помощи изменения **CSS**-файлов.

Вы можете подробнее ознакомиться с возможностями графического окружения **GNOME**, просмотрев наши обучающие видео:

- на **RuTube** — Обзор графического окружения GNOME в РЕД ОС 8;
- в **Яндекс.Дзен** — Обзор графического окружения GNOME в РЕД ОС 8;
- в **VK Видео** — Обзор графического окружения GNOME в РЕД ОС 8.

На наших каналах вы также сможете найти много другой полезной информации.

Графическое окружение **GNOME** выглядит следующим образом:



Основным режимом работы пользователя в РЕД ОС является графический режим. Работа пользователя в графическом режиме производится на рабочем столе пользователя РЕД ОС. Рабочий стол каждого пользователя индивидуален, так как настраивается отдельно для каждого пользователя. Настройки рабочего стола пользователя хранятся в домашней папке пользователя.

Навигационное пространство рабочего стола РЕД ОС состоит из трех зон управления:

- **Системная панель** – панель, расположенная по умолчанию в нижней части экрана. Системная панель обеспечивает доступ

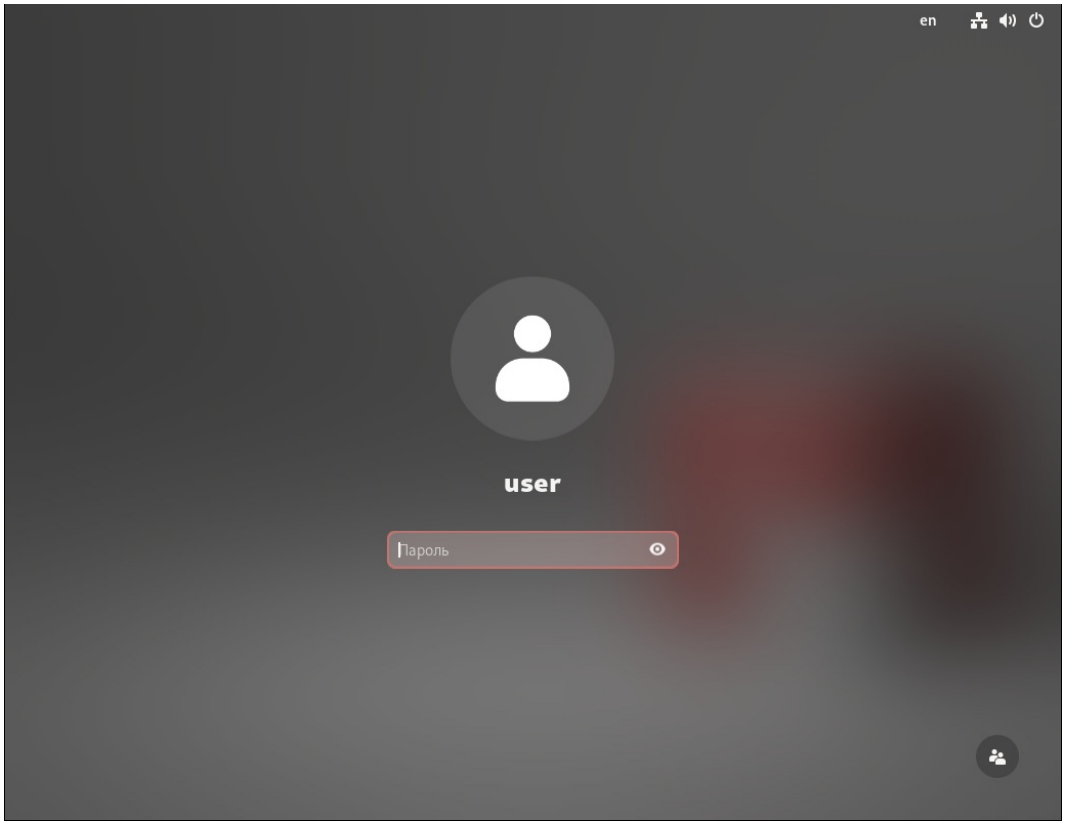
пользователя к меню запуска всех установленных программ, а также иконки уже запущенных программ;

- **Рабочее пространство** – все свободное пространство рабочего стола, предназначенное для расположения файлов данных и ярлыков часто используемых программ. Рабочее пространство может быть оформлено фоном рабочего стола;
- **Верхняя панель** – панель, расположенная по умолчанию в верхней части экрана. В этой панели отображаются кнопка « **Обзор**» для переключения между виртуальными рабочими столами, текущие дата и время, раскладка клавиатуры и системное меню для управления звуком, сетевыми соединениями и питанием системы. Также на панели отображается наименование активного окна.

Управление графическим интерфейсом РЕД ОС пользователь может осуществляться при помощи мыши или клавиатуры. Правая клавиша мыши (ПКМ) по умолчанию используется для вызова контекстных свойств любого графически представленного в интерфейсе РЕД ОС объекта. Левая клавиша мыши (ЛКМ) по умолчанию используется для инициации действий с любым графическим объектом в интерфейсе РЕД ОС.

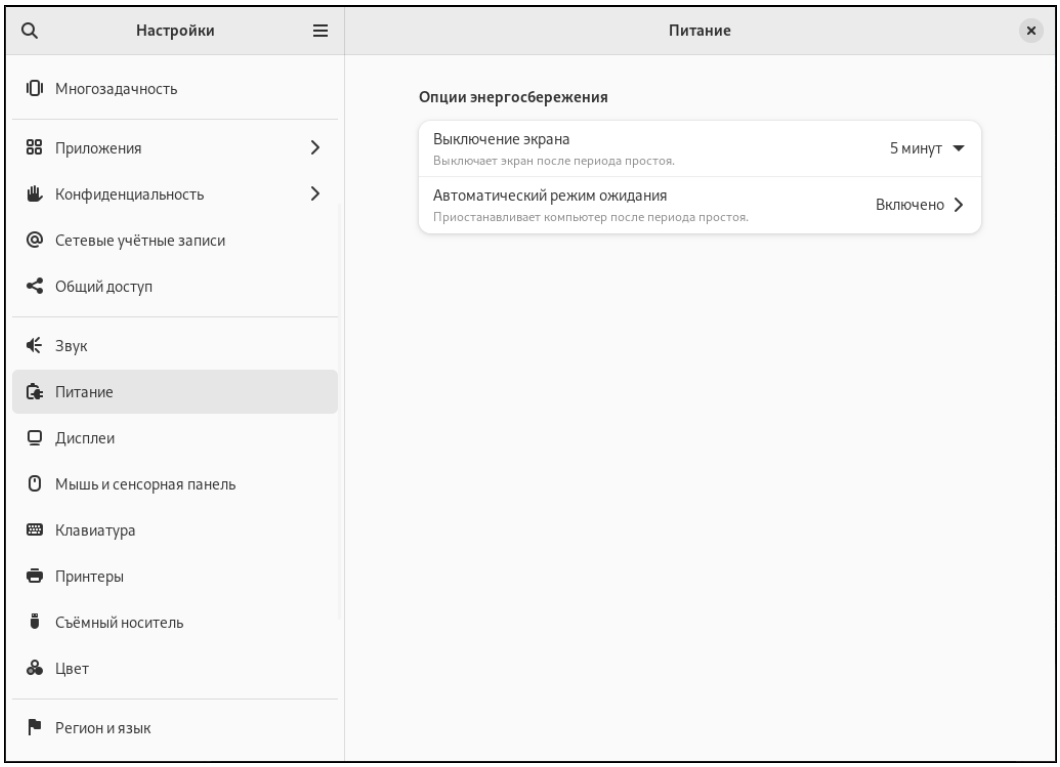
Общие методы работы пользователя с графическим интерфейсом РЕД ОС являются общепринятыми методами работы пользователей с графическими интерфейсами операционных систем. Основными элементами графического интерфейса РЕД ОС являются окна, панели, кнопки, меню, поля ввода, списки выбора, апплеты, радиокнопки, скроллеры и т.д.

При продолжительном бездействии пользователя рабочий стол пользователя блокируется, и для возобновления работы пользователю требуется провести повторную аутентификацию в РЕД ОС.



Значение продолжительности бездействия пользователя, после которого произойдёт блокировка рабочего стола, определяется настройкой питания системы. Настройка питания находится в меню «**Показать приложения**» — «**Настройки**» в подразделе «**Питание**».

Внешний вид настройки параметров блокировки экрана:



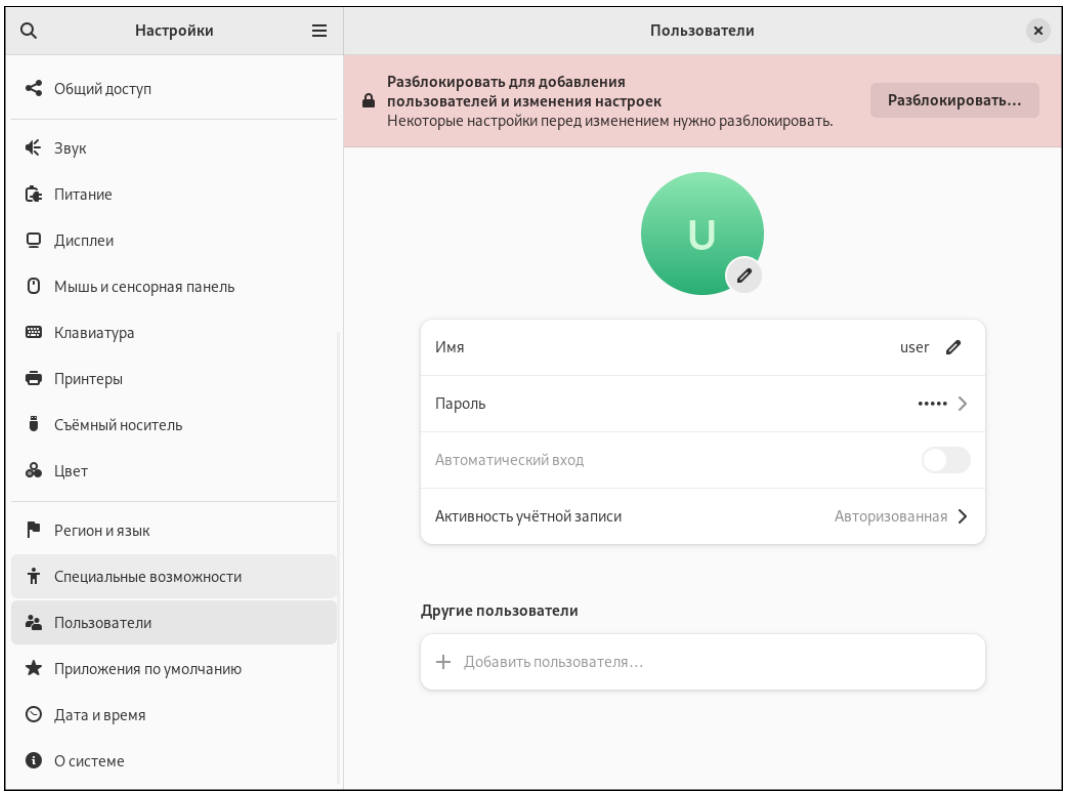
Все действия пользователя при аутентификации, успешные и неуспешные попытки аутентификации фиксируются в системном журнале РЕД ОС.

Общая информация

Набор утилит управления РЕД ОС находится в меню «**Показать приложения**» — «**Настройки**». Большинство параметров управления и конфигурирования РЕД ОС требуют привилегий администратора РЕД ОС.

Информация об учётной записи

В РЕД ОС (среда **GNOME**) пользователю доступна настройка реквизитов учётной записи пользователя. Настройка производится в меню «**Показать приложения**» — «**Настройки**» в подразделе «**Пользователи**».



В подразделе «**Пользователи**» можно производить изменения следующих групп реквизитов учётной записи:

- имя пользователя, отображаемое в системе и окне выбора пользователя загрузчика;
- пароль учетной записи;
- использование автоматического входа в систему.

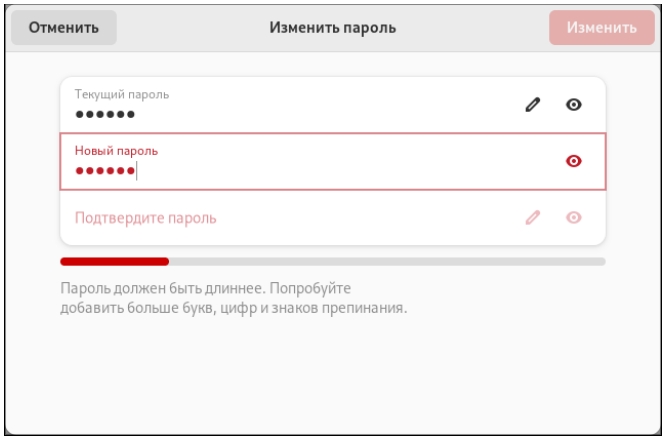
Указанная пользователем информация сохраняется в локальной БД пользователей РЕД ОС.

Пользователю доступно редактирование информации только о своей учётной записи, которая использовалась для аутентификации в РЕД ОС.

С помощью данной настройки пользователь может отредактировать используемую пиктограмму, ассоциируемую с учётной записью, и изменить текущий пароль.

В ОС могут быть заданы политики сложности, предъявляемые к используемым паролям.

При выполнении процедуры смены пароля, пользователю необходимо сначала ввести действующий пароль, а затем дважды ввести новый пароль в соответствующих полях.



Если введённый пользователем новый пароль нарушает параметры требований к паролям, то РЕД ОС выводит текст предупреждения о нарушении политик с описанием требования, которому новый пароль не соответствует.

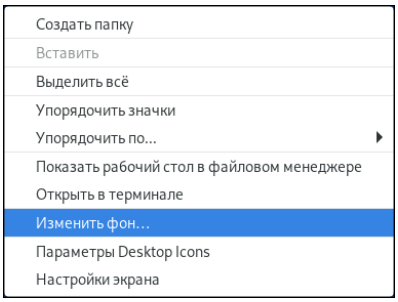
На любом этапе операции смены пароля пользователь может прервать смену пароля при помощи кнопки «**Отменить**».

По окончании операции смены пароля РЕД ОС выводит пользователю сообщение об успешном изменении атрибутов безопасности пользователя.

Настройка фона рабочего стола пользователя РЕД ОС

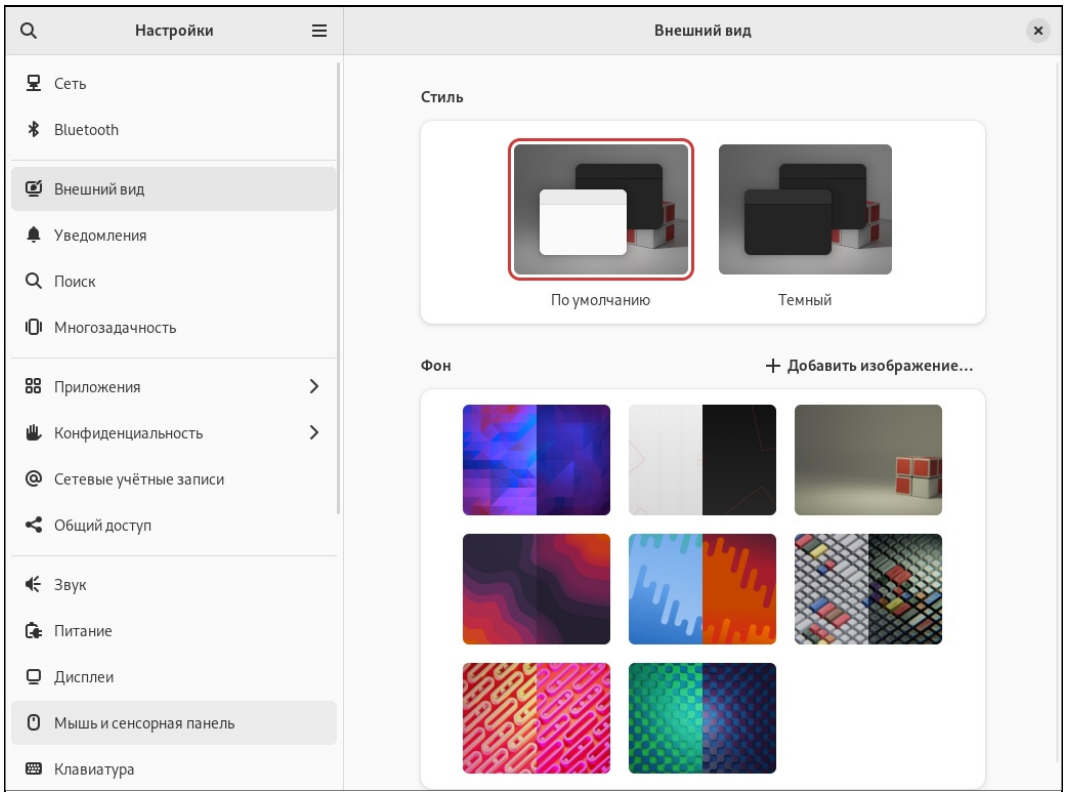
Для смены изображения рабочего стола существует два варианта.

Вариант 1. Для смены фона рабочего стола необходимо в свободной части рабочего стола вызвать контекстное меню (нажав ПКМ). В открывшемся контекстном меню необходимо выбрать пункт «**Изменить фон...**».



Вариант 2. Для смены фона рабочего стола пользователю необходимо в меню «**Показать приложения**» — «**Настройки**» открыть подраздел «**Внешний вид**».

В блоке «**Фон**» можно выбрать изображение из имеющихся или добавить собственное, нажав кнопку «**Добавить изображение...**».

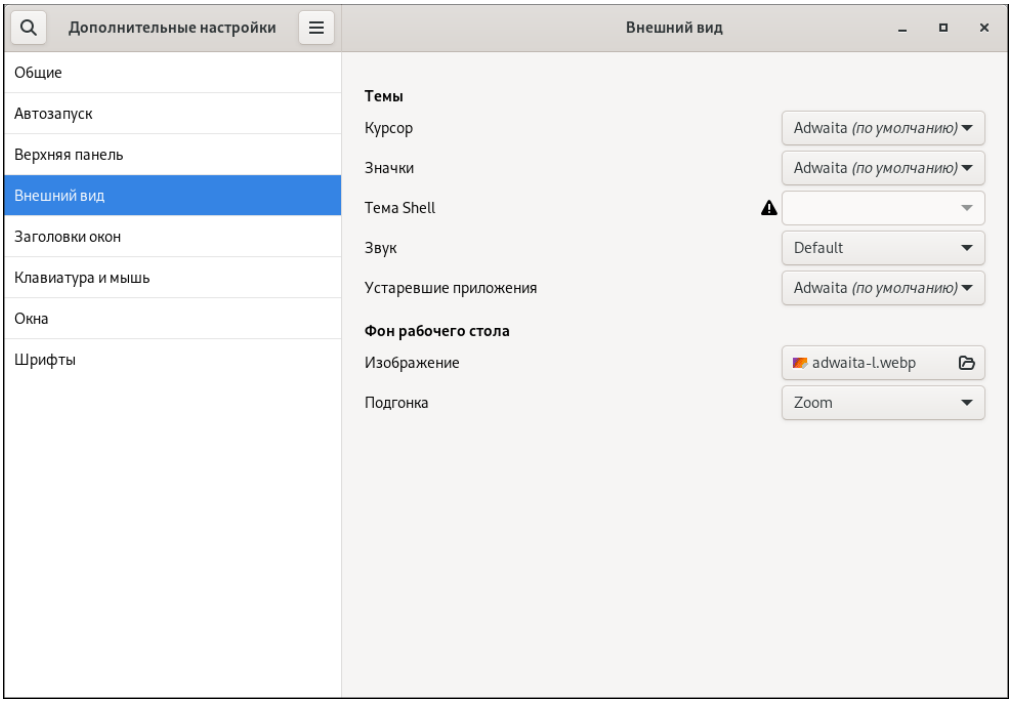


Дополнительно можно выбрать стиль отображения фонового рисунка в зависимоси от используемой темы оформления окон — светлый или темный.

Настройка внешнего вида графического интерфейса РЕД ОС

Для смены внешнего вида окон графической оболочки РЕД ОС пользователю необходимо перейти в меню «**Показать приложения**» — «**Доп.настройки GNOME**».

В открывшемся окне необходимо перейти в раздел «**Внешний вид**» и в блоке «**Темы**» определить собственные значения стилевого оформления отдельных элементов интерфейса, полностью независимое друг от друга и от темы рабочего стола, таких как указатель мыши, иконки приложений, тема shell, звук и окна устаревших приложений. При выборе какого-либо значения его применение производится автоматически.

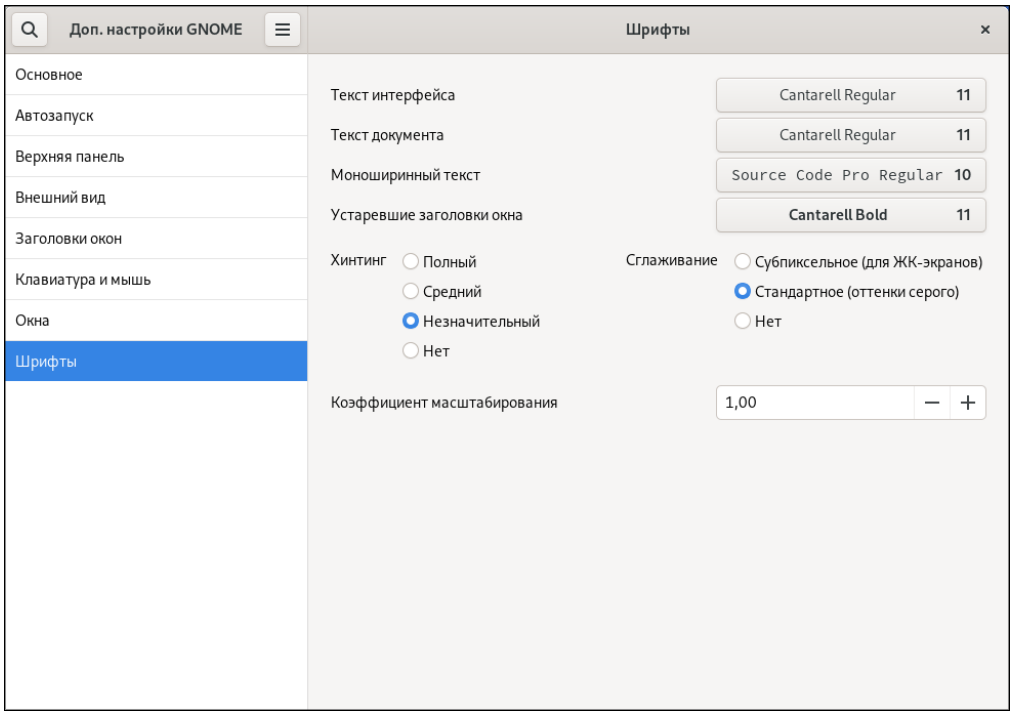


Здесь также можно загрузить и установить собственное изображение рабочего стола и выбрать способ подгонки изображения.

Настройка шрифтов графического интерфейса РЕД ОС

Для изменения используемых шрифтов графической оболочки РЕД ОС пользователю необходимо открыть меню «**Показать приложения**» — «**Доп.настройки GNOME**», затем перейти в раздел «**Шрифты**».

В окне можно настроить шрифты как для заголовков окон, так и для документов.



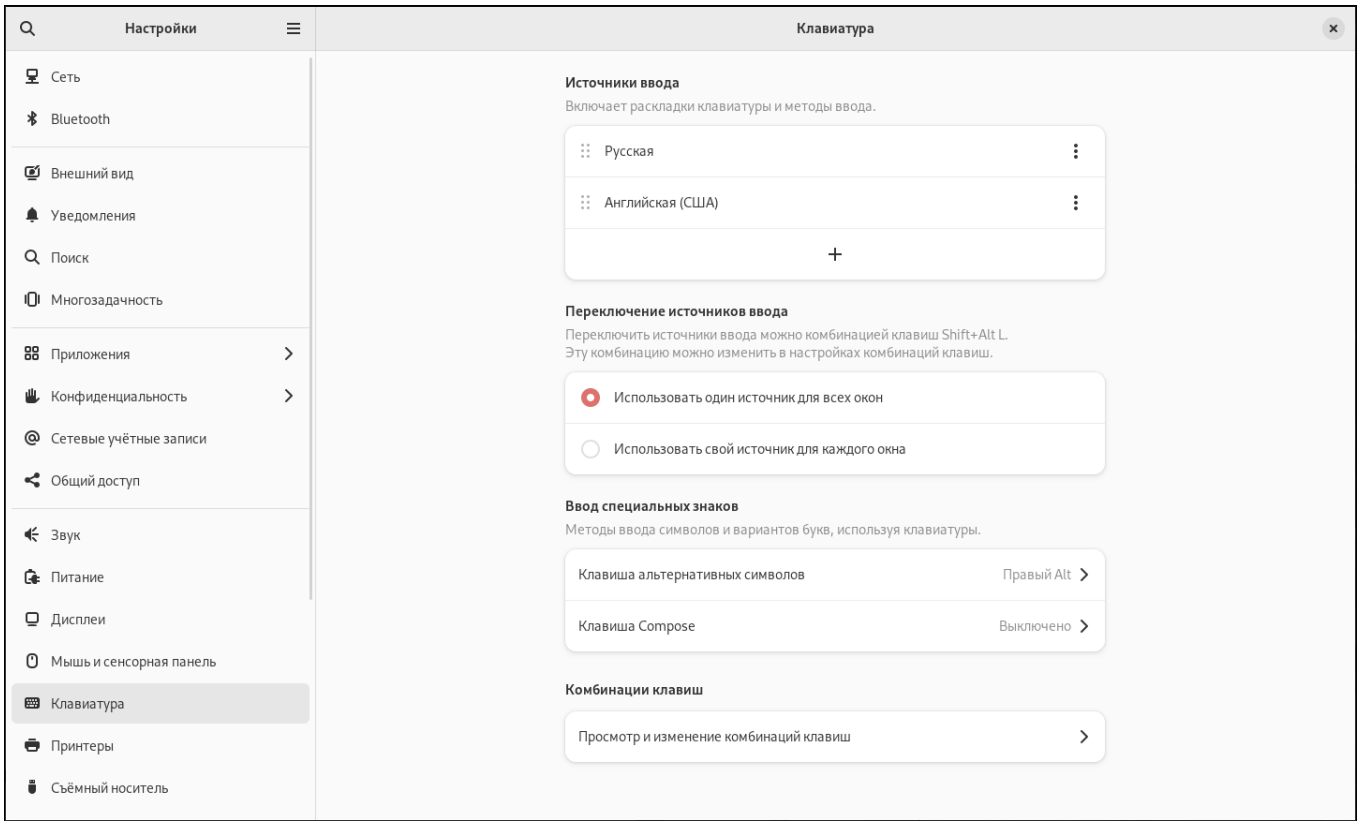
В открывшемся окне пользователь может настроить шрифты, которые будут использованы по умолчанию в системных утилитах, документах и в оформлении окружения.

Пользователю необходимо выбрать из представленных примеров шрифтов необходимый, настройки будут применены автоматически.

Настройка смены раскладки клавиатуры

В РЕД ОС по умолчанию смена раскладки клавиатуры (языка ввода) осуществляется при одновременном нажатии функциональных клавиш клавиатуры **Shift+Alt**.

Для изменения сочетания функциональных клавиш, применяемых для смены раскладки клавиатуры, необходимо в меню «**Показать приложения**» — «**Настройки**» открыть подраздел «**Клавиатура**», перейти в блок «**Комбинации клавиш**» и нажать «**Просмотр и изменение комбинаций клавиш**».



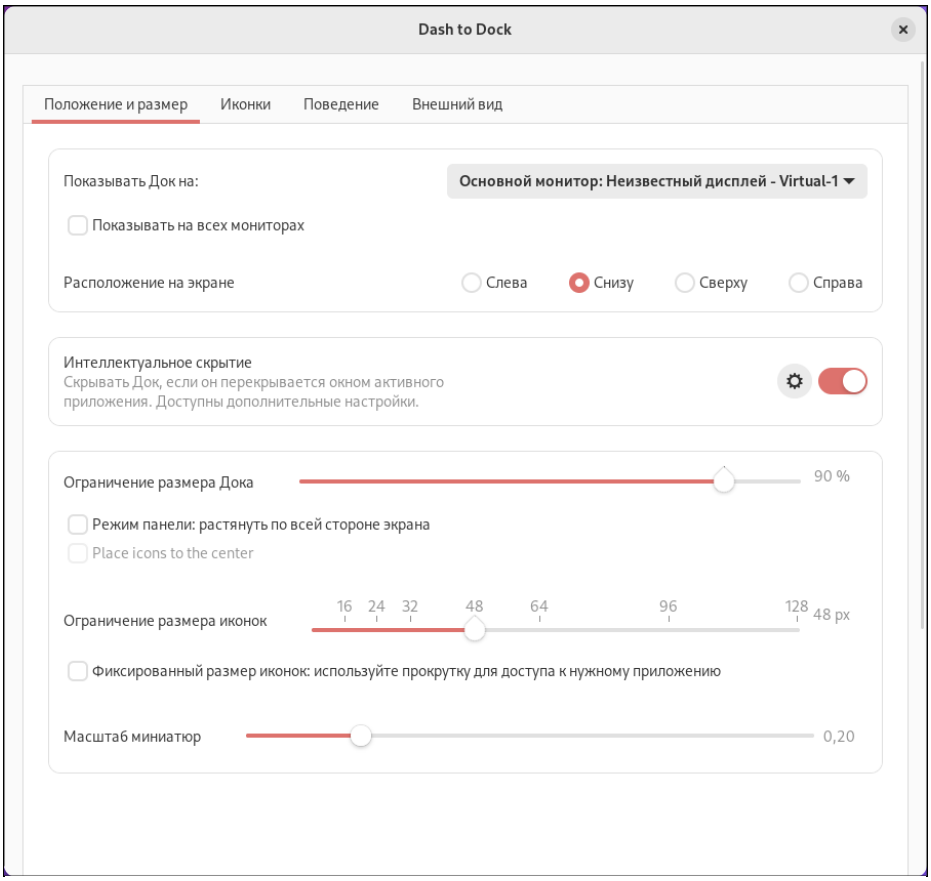
В открывшемся окне пользователю необходимо выбрать параметр «**Ввод текста**» и задать собственные комбинации клавиш для параметров «**Переключиться на предыдущий источник ввода**» и «**Переключиться на следующий источник ввода**».



При нажатии пользователем необходимой комбинации клавиш ее сохранение производится автоматически.

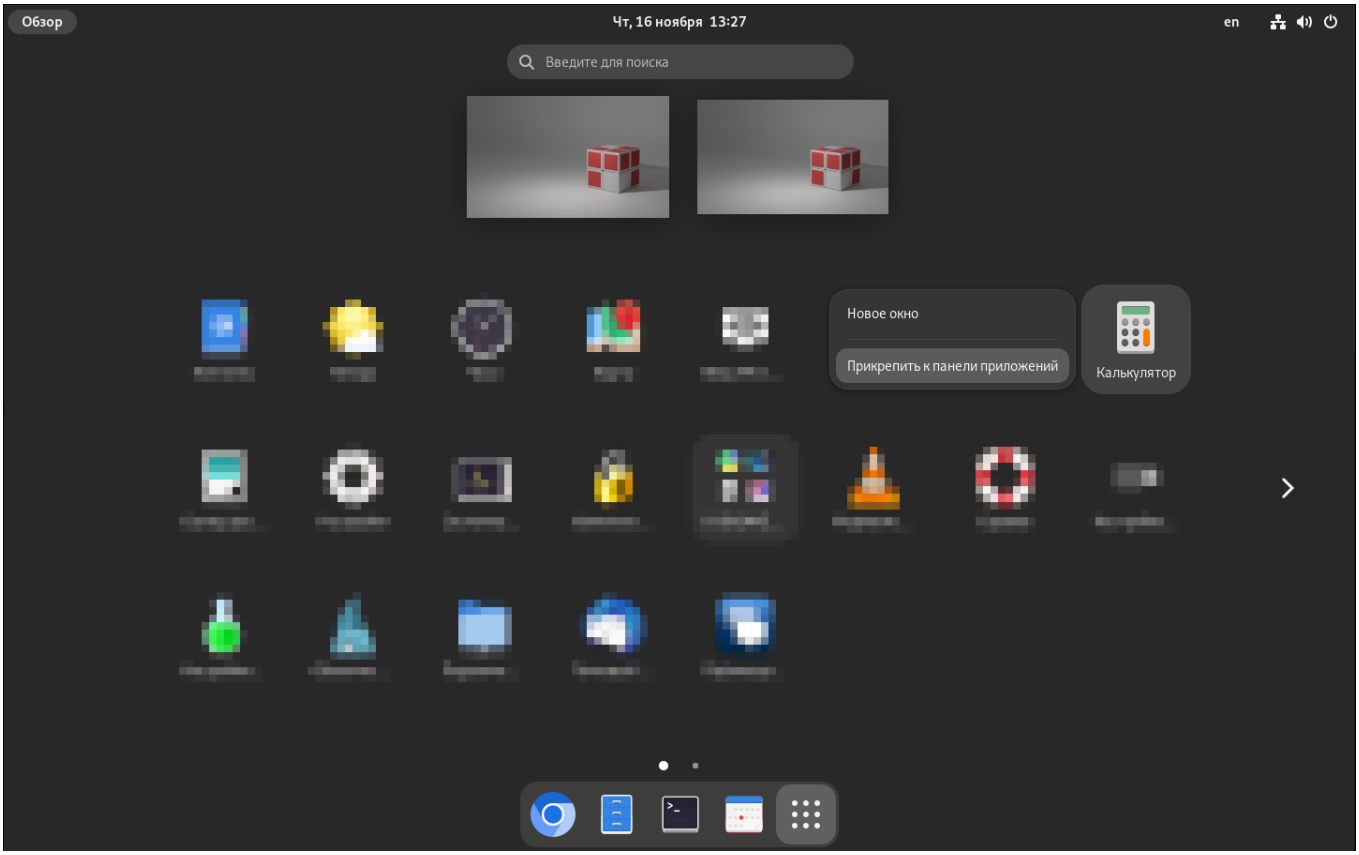
Управление элементами панели

Для настройки параметров системной панели рабочего стола пользователю необходимо нажать ПКМ по меню «**Показать приложения**» и в открывшемся контекстном меню выбрать действие «**Dash to Dock Настройки**».



В открывшемся окне пользователь может настроить расположение и режим панели, интеллектуальное скрытие панели, масштаб миниатюр, настроить иконки приложений, действия по нажатию как кнопок мыши, так и клавиш клавиатуры, а также внешний вид панели.

Для добавления на панель каких-либо программ необходимо открыть меню «**Показать приложения**» и нажать ПКМ по выбранной программе и в появившемся контекстном меню выбрать пункт «**Прикрепить к панели приложений**».



В результате действий пользователя на системной панели должен появиться соответствующий приложению индикатор.

Оконный менеджер Openbox

Установка openbox
Настройка openbox
Файл rc.xml
Файл menu.xml
Автозапуск приложений
Файл environment
Настройка тем (внешнего оформления)
Применение настроек
Настройка сочетания клавиш
Добавление панелей

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openbox-3.6.1-20

Openbox – это легкий и настраиваемый оконный менеджер, который предоставляет пользователю максимальную гибкость в управлении окнами на экране.

Openbox можно использовать как отдельный оконный менеджер или в качестве замены стандартного оконного менеджера своей среды рабочего стола. Он обеспечивает достаточную функциональность для работы на его основе, но также позволяет настроить большую часть своих функций и использовать плагины для улучшения его возможностей.

Основные возможности **Openbox** включают:

- настраиваемые горячие клавиши (клавиши быстрого доступа);
- поддержку декоративных элементов окон, включая кнопки закрытия и переключения виртуальных рабочих столов;
- поддержку управления окнами с помощью мыши;
- DAO-режим, который позволяет управлять поведением окон при открытии приложений;
- поддержку стандартов среды рабочего стола (**KDE**, **Xfce**).

К основным настройкам относятся:

- настройка переключения окон с помощью мыши или клавиатуры;
- настройка внешнего вида границ окон и их декорирование;
- настройка горячих клавиш для быстрого запуска приложений или выполнения команд;
- настройка виртуальных рабочих столов для организации рабочего пространства;
- установка и использование плагинов для расширения функциональности оконного менеджера.

Openbox имеет довольно простой и интуитивно понятный интерфейс, который делает его удобным для использования как начинающими, так и опытными пользователями.

Установка openbox

Для установки **openbox** перейдите в сеанс пользователя **root**:

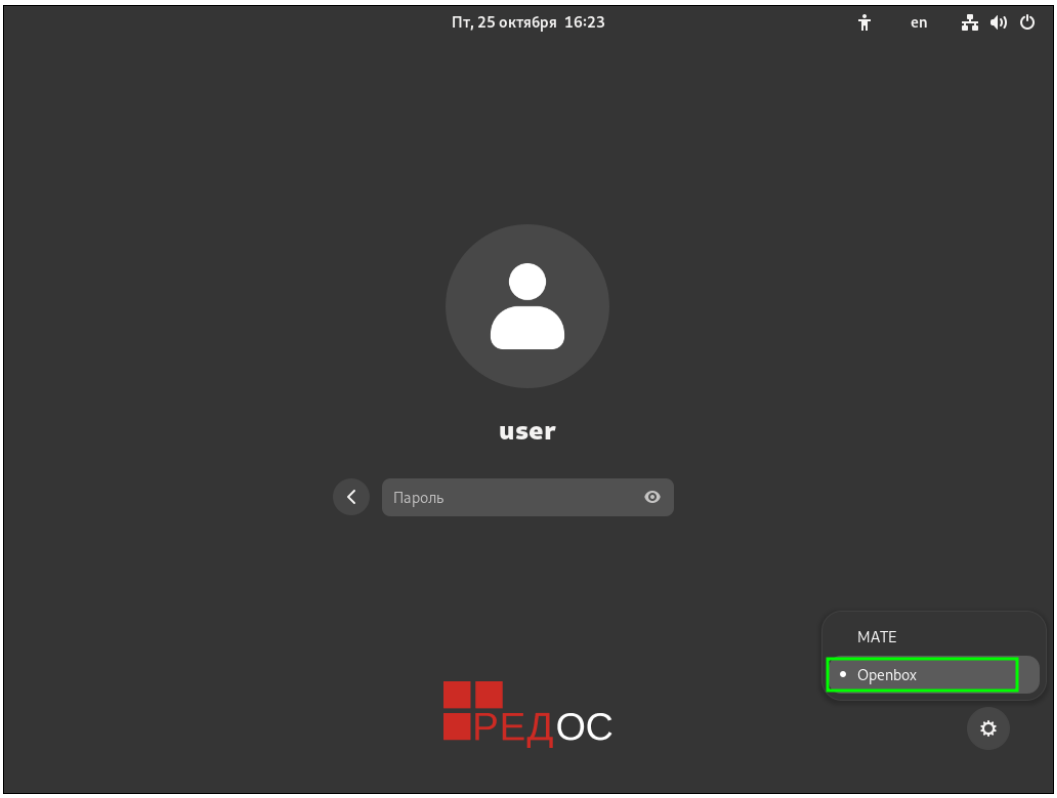
```
su -
```

и выполните команду:

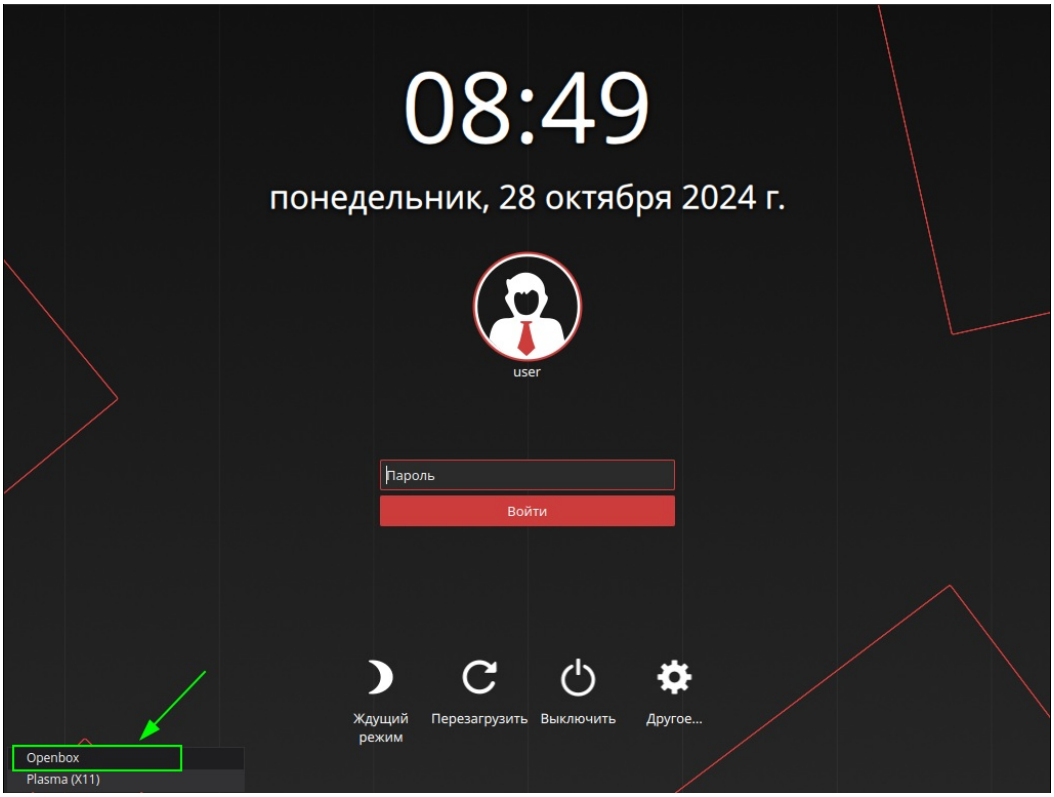
```
dnf install openbox
```

Для загрузки в новом оконном менеджере необходимо выйти из текущего сеанса пользователя, выбрав в «**Главном меню**» пункт «**Завершить текущий сеанс**» – «**Завершить сеанс**».

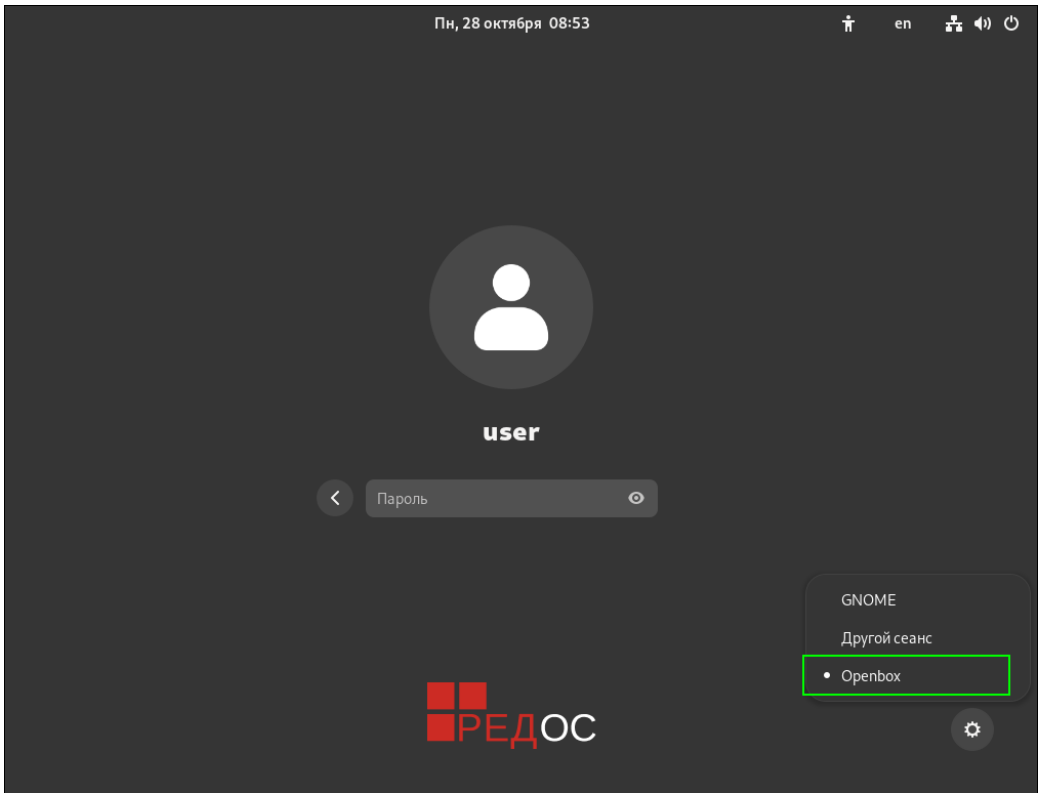
При использовании графического окружения **MATE** в окне выбора пользователей выберите нужного пользователя, в правом нижнем углу нажмите на значок шестеренки и выберите из списка **Openbox**, введите пароль пользователя и авторизуйтесь в системе.



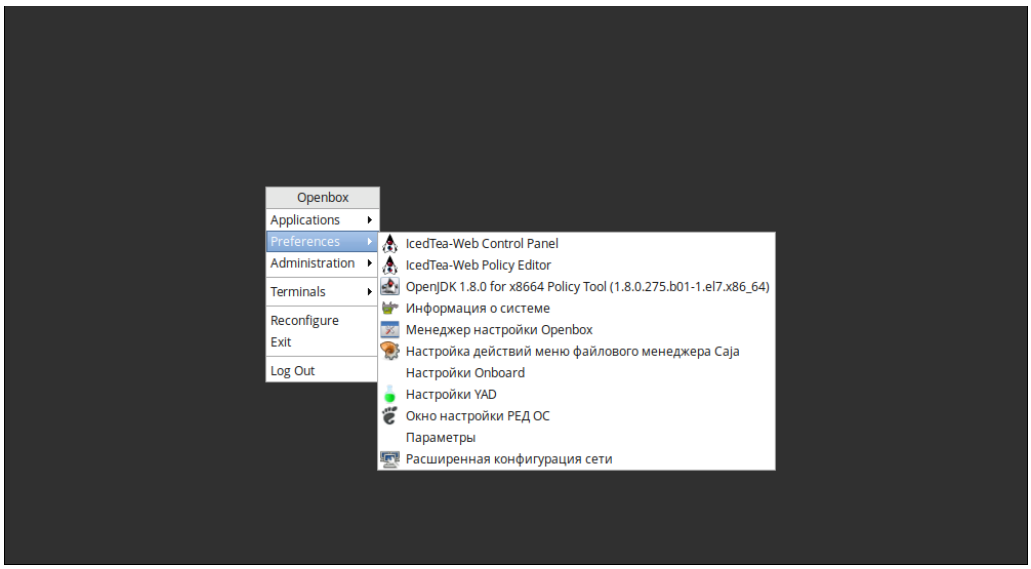
При использовании графического окружения **KDE** в окне выбора пользователей выберите нужного пользователя, в левом нижнем углу нажмите на строку выбора окружения и выберите из списка **Openbox**, введите пароль пользователя и авторизуйтесь в системе.



При использовании графического окружения **GNOME** в окне выбора пользователей выберите нужного пользователя, в правом нижнем углу нажмите на значок шестеренки и выберите из списка **Openbox**, введите пароль пользователя и авторизуйтесь в системе.



После запуска будет отображаться просто серый экран. Нажмите правую кнопку мыши по экрану — это вызовет меню **Openbox** и продемонстрирует, что всё успешно запустилось и работает.



Настройка openbox

Примечание.

Локальные файлы конфигурации имеют приоритет выше, чем глобальные.

Основу конфигурации openbox составляют четыре конфигурационных файла, каждый из которых выполняет свою роль: **rc.xml**, **menu.xml**, **autostart** и **environment**.

Перед настройкой рекомендуется создать локальный профиль **openbox** (специфичный для вашей учётной записи). Это можно сделать путём копирования глобального профиля **/etc/xdg/openbox** (который применяется для всех пользователей) в свой каталог настроек:

```
mkdir -p ~/.config/openbox
cp -a /etc/xdg/openbox/ ~/.config/
```

Файл rc.xml

> **Примечание.**
>
> Пользовательские сочетания клавиш должны добавляться в раздел `<keyboard>` этого файла и под заголовком `<!-- Keybindings for running aplications -->`

~/.config/openbox/rc.xml — это основной файл конфигурации, отвечающий за определение поведения и настроек всего сеанса, в том числе:

- сочетания клавиш (например, запуск приложений, регулировка громкости);
- темы оформления;
- настройки рабочего стола и виртуального рабочего стола;
- настройки окна приложения.

Файл имеет прописанные настройки по умолчанию, поэтому достаточно добавить необходимые изменения в соответствии с личными предпочтениями.

> **Примечание.**
>
> Настройки для каждого приложения, относящиеся к фиксированному размещению приложений на мониторе, будут работать только в том случае, если также были определены положения *x* и *y*.

Файл menu.xml

~/.config/openbox/menu.xml определяет поведение меню, открывающегося по нажатии ПКМ по рабочему столу. По умолчанию предоставляется статическое меню (которое не обновляется автоматически при установке новых приложений), но можно также использовать динамическое меню, которое будет обновляться автоматически.

Автозапуск приложений

openbox-session имеет два механизма автозапуска:

- **XDG Autostart** – работает, если установлен пакет **python-pyxdg**;
- свой собственный механизм.

Собственный механизм:

- считывает переменные из **/etc/xdg/openbox/environment**;
- считывает переменные из **~/.config/openbox/environment**;
- запускает **/etc/xdg/openbox/autostart**;
- запускает **~/.config/openbox/autostart**.

При возникновении проблем, связанных с выполнением команд в **~/.config/openbox/autostart** (команды выполняются не последовательно или наблюдается пропуск выполнения некоторых команд), рекомендуется добавить небольшие задержки. Например:

```
xset -b
(sleep 3s && nm-applet) &
(sleep 3s && conky) &
```

Файл environment

Файл **~/.config/openbox/environment** можно использовать для добавления связанных переменных окружения, например:

- определить новые пути при выполнении команд, которые требуют указания абсолютных путей до файлов;
- изменить языковые настройки;
- определить другие переменные, которые будут использоваться (например, здесь можно указать исправление для тем **GTK**).

Настройка тем (внешнего оформления)

Примечание.

Рекомендуется скопировать тему в домашний каталог пользователя вместо того, чтобы редактировать её напрямую в /usr/share/themes/. Это позволит оставить оригинал нетронутым, а также не удалит внесенные изменения при обновлении пакетов.

Стандартной утилитой для настройки внешнего вида **openbox** является **obconf**.

Для её установки перейдите в сеанс пользователя **root**:

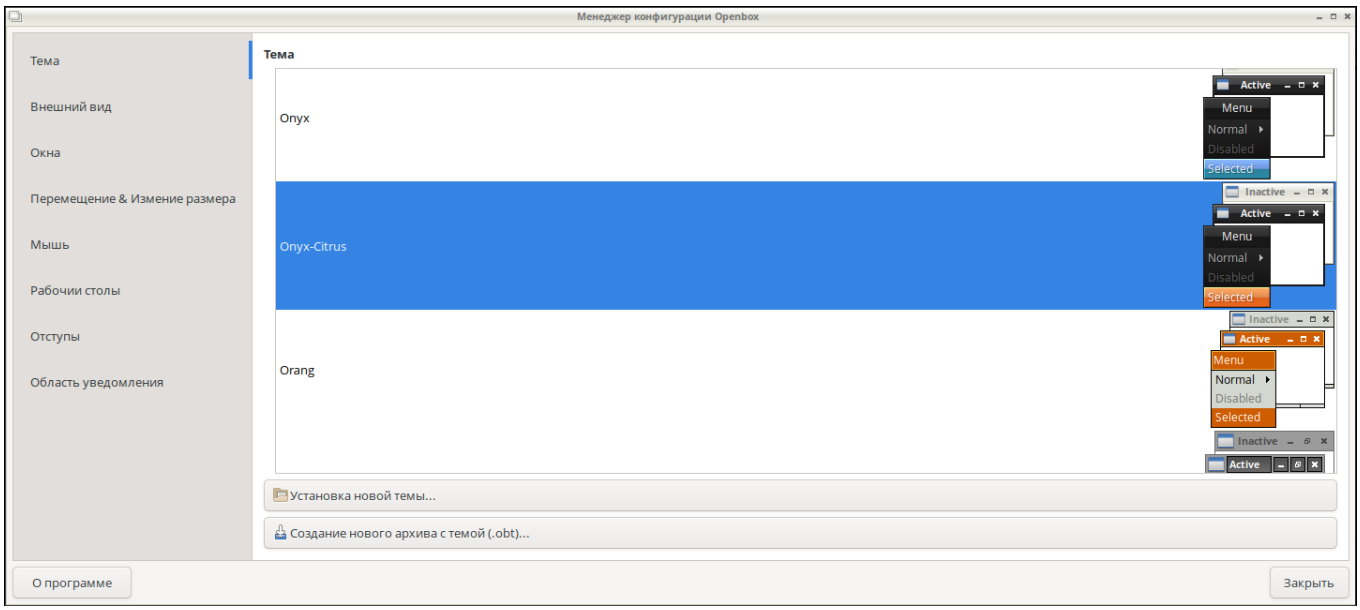
```
su -
```

и выполните команду:

```
dnf install obconf
```

Запуск утилиты доступен из «**Меню**» – «**Preferences**» – «**Менеджер настройки Openbox**».

В менеджере можно изменить тему интерфейса, шрифты, размеры окон и пр.



Применение настроек

Openbox не всегда автоматически применяет изменения, внесённые в его файлы конфигурации в течение сеанса. Как следствие, необходимо вручную перезагрузить эти файлы после того, как они были изменены. Для этого выполните следующую команду:

```
openbox --reconfigure
```

Настройка сочетания клавиш

Все сочетания клавиш добавляются в файл **~/.config/openbox/rc.xml** под заголовком `<!-- Keybindings for running aplications -->`.

Для добавления собственных сочетаний клавиш откройте конфигурационный файл **rc.xml** с помощью команды:

```
nano ~/.config/openbox/rc.xml
```

и в конец файла добавьте следующие строки:

- для добавления сочетания клавиш:

```
<keybind key="новое_сочетание_клавиш">
  <action name="новое_действие">
    ...
  </action>
 </keybind>
```

- для выполнения внешней команды (используется действие execute):

```
<keybind key="новое_сочетание_клавиш">
  <action name="Execute">
    <command>новая_команда</command>
  </action>
 </keybind>
```

Добавление панелей

Openbox не содержит панелей, но их можно установить самостоятельно, например, с помощью утилиты **tint2**.

Для установки утилиты перейдите в сеанс пользователя **root**:

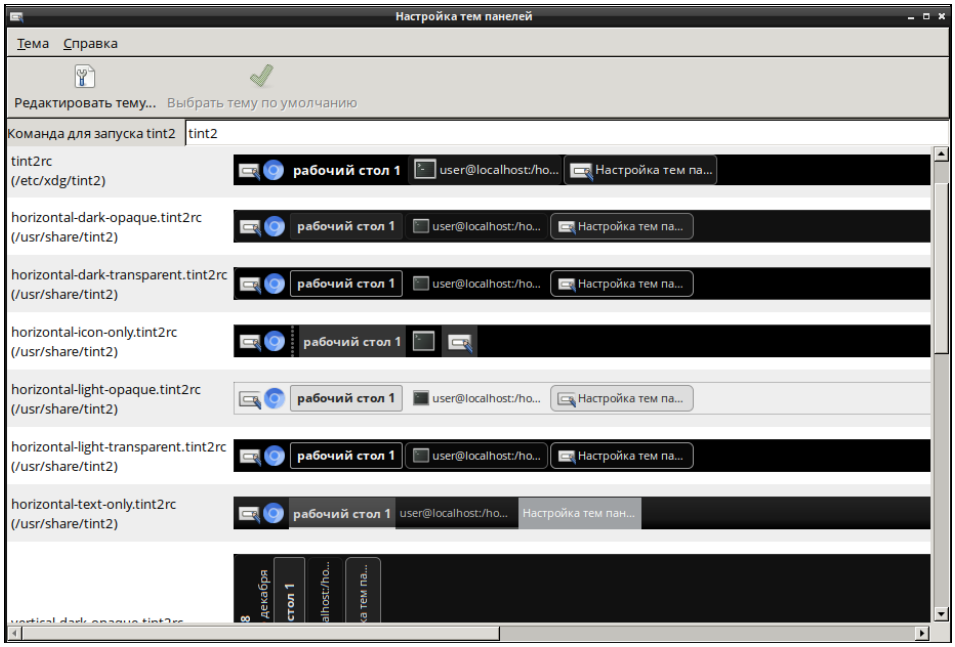
```
su -
```

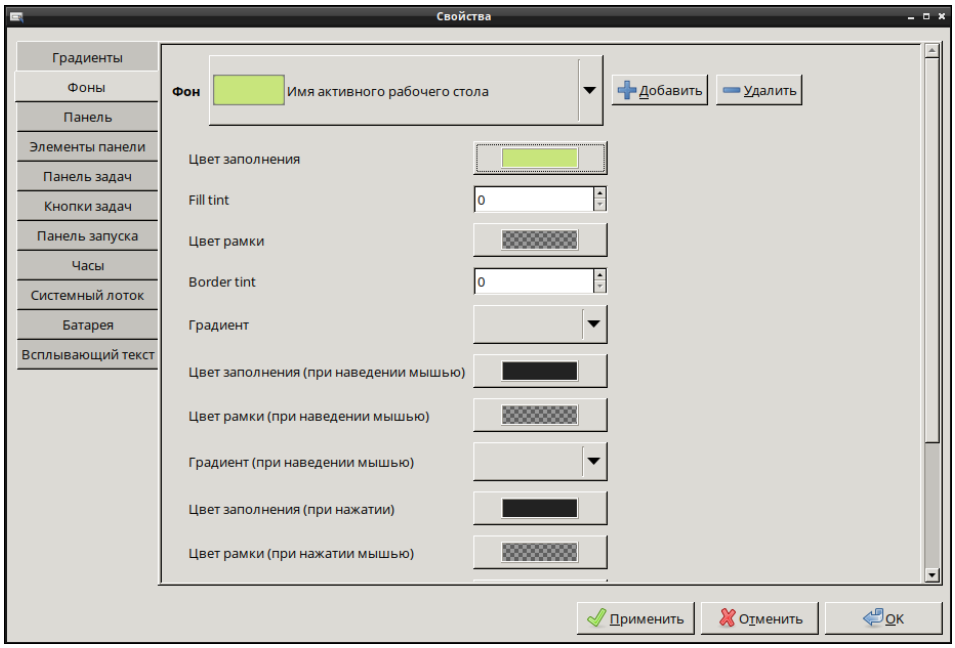
и выполните команду:

```
dnf install tint2
```

Запуск утилиты доступен из «**Меню**» – «**Preferences**» – «**Настройки tint2**».

Далее можно выбрать любую подходящую тему и редактировать её при необходимости.





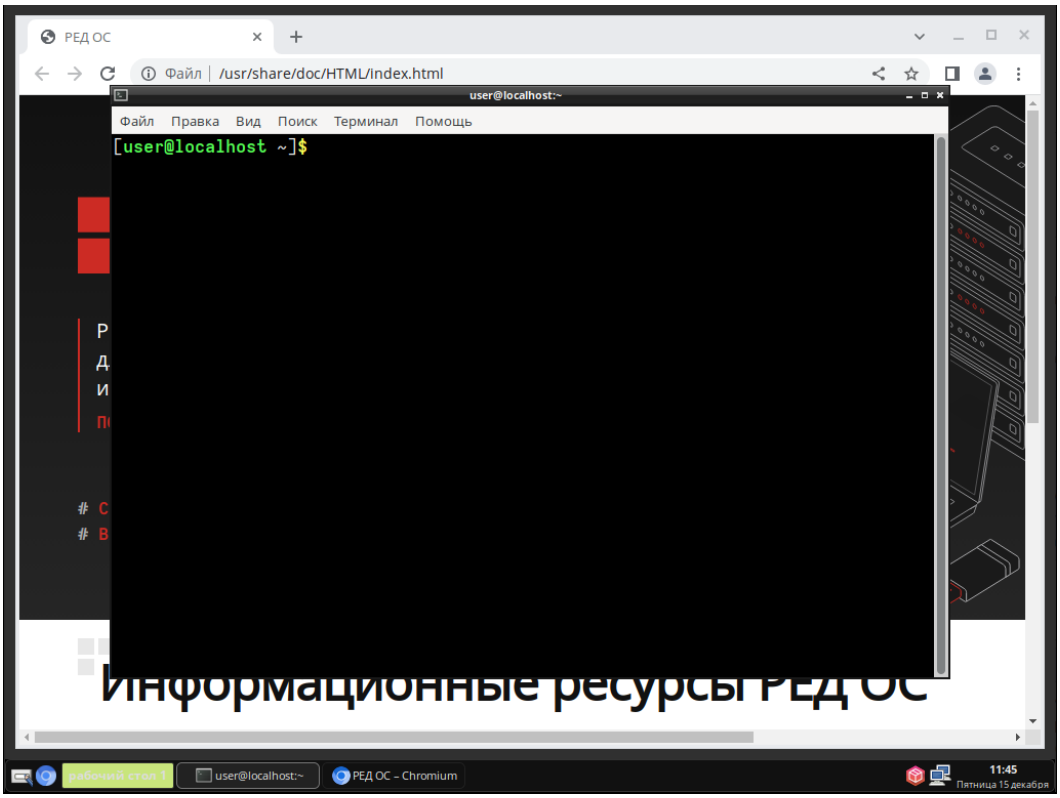
Для применения изменений необходимо в файле конфигурации **~/.config/openbox/autostart** указать **tint2**:

```
nano ~/.config/openbox/autostart
```

```
tint2 &
```

а затем перезагрузить систему:

```
reboot
```



Графический сервер Wayland

Установка Wayland в GNOME
Установка Wayland в KDE

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: gnome-session-wayland-session-44.0-1, plasma-workspace-wayland-5.27.3-4

Wayland – протокол для организации графического сервера в РЕД ОС и других UNIX-подобных операционных системах.

По умолчанию в РЕД ОС 8 используется графический сервер **Xorg**. Однако в репозитории доступен **Wayland**, который можно установить и использовать вместо **Xorg** в графических оболочках **GNOME** и **KDE**.

Кардинальное отличие от **Xorg** заключается в том, что **Wayland** лишь управляет буферами (плоскостями) окон и возлагает всю отрисовку их содержимого на инструментальные пакеты (GTK, Qt). API рисования (drawing API) полностью отсутствует. Все версии протокола строго определены, а сама система определения версий отлично продумана.

У **Xorg** есть серьёзная проблема с версиями разных расширений, часто пересекающимися или дополняющимися, вместо того чтобы быть самодостаточными и исключающими.

Функцию композиции буферов осуществляет референтный композитный менеджер **Weston**, использующий как OpenGL ES, так и программную отрисовку. В состав **Wayland** также входит унифицированный протокол устройств ввода, предоставляющий одну виртуальную клавиатуру, одну виртуальную мышь и один экранно-сенсорный интерфейс — разделяемые всеми приложениями. **Wayland** знает о состояниях устройств ввода и способен запоминать их. **Xorg** напротив – не сохраняет состояния устройств (stateless-протокол), но может быть настроен через файлы конфигурации.

Вы можете подробнее ознакомиться с установкой и возможностями графического сервера **Wayland**, просмотрев наши обучающие видео:

- на **RuTube** — Графический сервер Wayland. Установка Wayland в GNOME и KDE;
- в **Яндекс.Дзен** — Графический сервер Wayland. Установка Wayland в GNOME и KDE;
- в **VK Видео** — Графический сервер Wayland. Установка Wayland в GNOME и KDE.

На наших каналах вы также сможете найти много другой полезной информации.

Установка Wayland в GNOME

Для установки **Wayland** в графической оболочке **GNOME** откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

выполните команду:

```
dnf install gnome-session-wayland-session
```

В файле конфигурации **/etc/gdm/custom.conf** установите значение параметра `WaylandEnable` в `true`:

```
WaylandEnable=true
```

Сохраните внесенные изменения и закройте файл.

Выйдите из сеанса пользователя **root**:

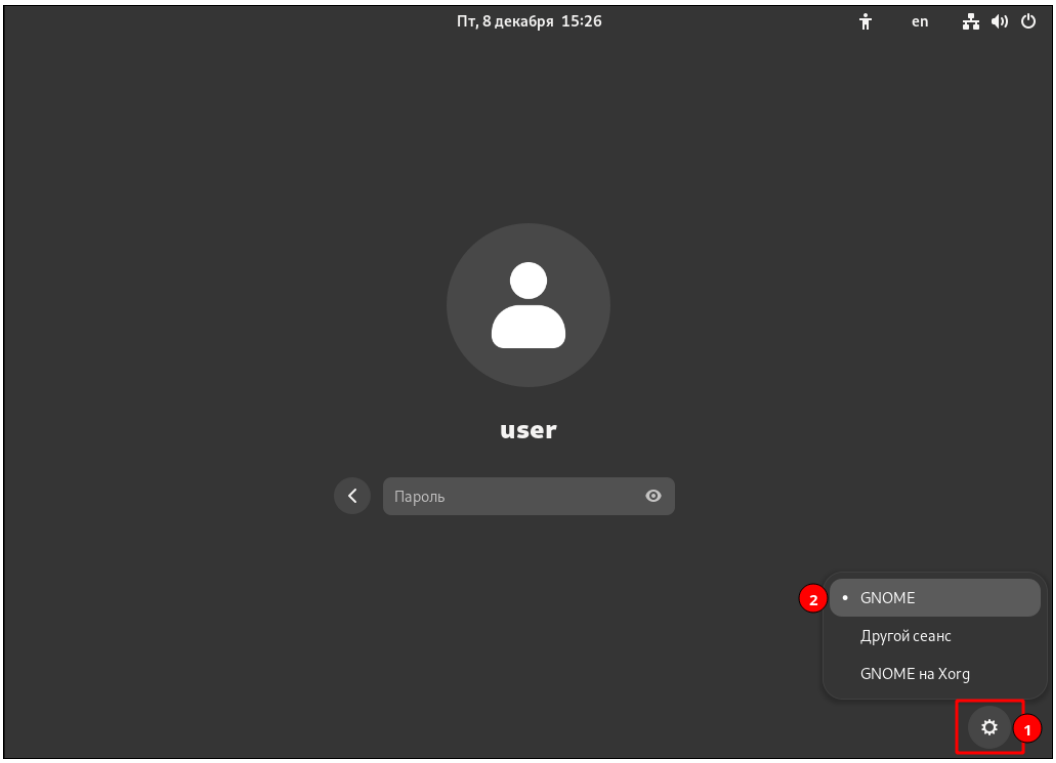
```
exit
```

Перезагрузите систему для применения внесенных изменений:

```
reboot
```

После перезапуска в окне авторизации выберите необходимого пользователя для входа в систему. В окне ввода пароля в правом нижнем углу нажмите на знак шестеренки. В списке графических оболочек выберите один из вариантов:

- *GNOME* – для запуска сессии с использованием **Wayland**;
- *GNOME на Xorg* – для запуска сессии с использованием **Xorg**.



Для проверки использования на машине X11-сервера (*Wayland* или *Xorg*) выполните команду:

```
echo $XDG_SESSION_TYPE

wayland
```

Установка Wayland в KDE

Для установки **Wayland** в графической оболочке **KDE** откройте терминал и перейдите в сеанс пользователя **root**:

```
su
```

выполните команду:

```
dnf install plasma-workspace-wayland
```

Выйдите из сеанса пользователя **root**:

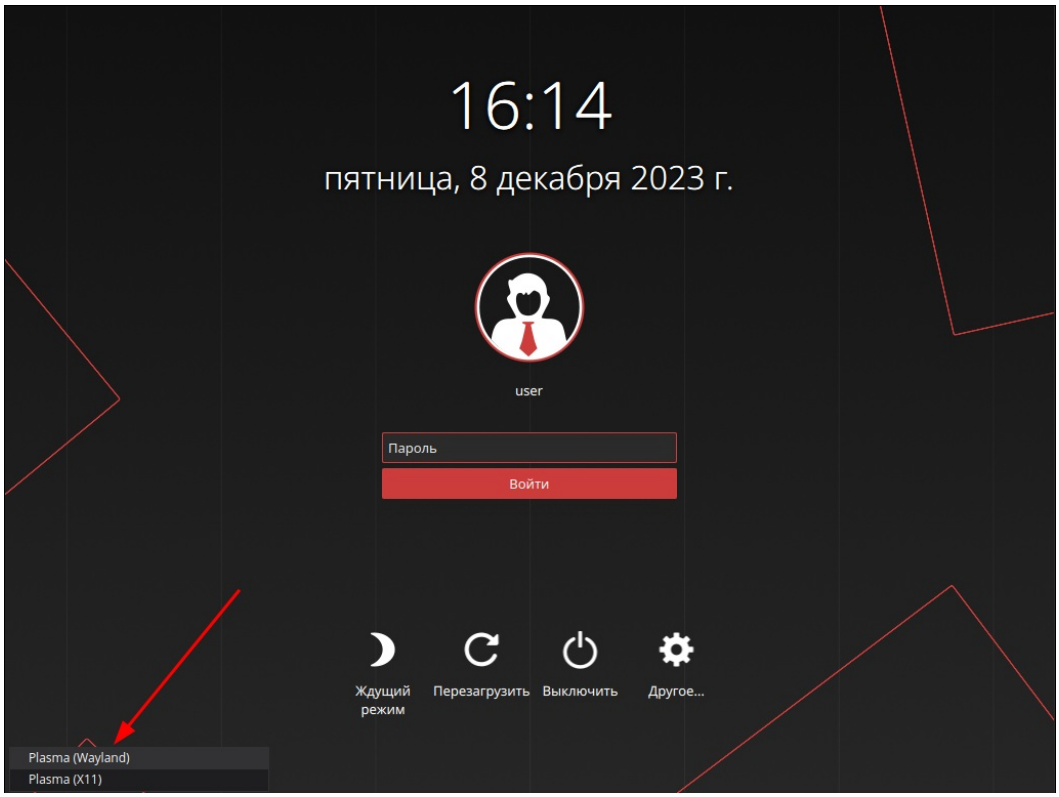
```
exit
```

Перезагрузите систему для применения внесенных изменений:

```
reboot
```

После перезапуска в окне авторизации выберите необходимого пользователя для входа в систему, в левом нижнем углу в списке графических оболочек выберите один из вариантов:

- *Plasma (Wayland)* – для запуска сессии с использованием **Wayland**;
- *Plasma (X11)* – для запуска сессии с использованием **Xorg**.



Для проверки использования на машине X11-сервера (*Wayland* или *Xorg*) выполните команду:

```
echo $XDG_SESSION_TYPE

wayland
```

Установка графической оболочки в РЕД ОС 8

Mate
KDE Plasma
GNOME
Графический режим работы
Удаление графической оболочки в РЕД ОС 8

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический

Вы можете подробнее ознакомиться с информацией по установке графических оболочек, просмотрев наши обучающие видео:

- на **RuTube** — Установка графической оболочки в РЕД ОС 8;
- в **Яндекс.Дзен** — Установка графической оболочки в РЕД ОС 8;
- в **VK Видео** — Установка графической оболочки в РЕД ОС 8.

На наших каналах вы также сможете найти много другой полезной информации.

ВАЖНО!

В РЕД ОС 8 не рекомендуется использовать несколько графических оболочек на одной рабочей машине из-за возможности возникновения конфликтов пакетов. Такие конфликты могут вызвать сбои в работе системы, и некоторые функции могут стать для пользователя недоступны.

Mate

Для установки **MATE** в **РЕД ОС 8** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install @MATE --allowerasing
```

KDE Plasma

Для установки **KDE Plasma** в **РЕД ОС 8** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install @KDE --allowerasing
```

GNOME

Для установки **GNOME** в **РЕД ОС 8** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install @GNOME --allowerasing
```

Графический режим работы

Для включения графического режима работы на сервере по умолчанию выполните команду (потребуются права **администратора**):

```
sudo systemctl set-default graphical.target
```

Перезагрузите сервер:

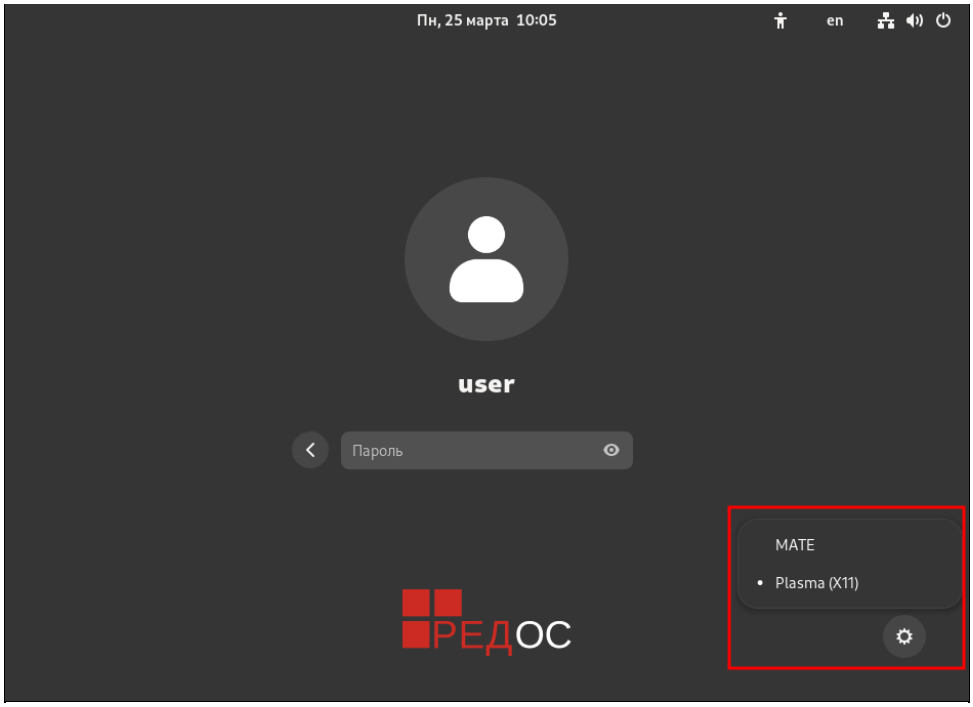
```
reboot
```

Удаление графической оболочки

В случае, если на одной рабочей машине установлено несколько графических оболочек, неиспользуемые графические оболочки рекомендуется удалить.

Для удаления неиспользуемой графической оболочки необходимо:

1. Перед входом в систему на этапе ввода пароля учетной записи выбрать нужную графическую оболочку, нажав в правом нижнем углу на значок шестеренки.



2. После авторизации в системе с нужной графической оболочкой выполните одну из следующих команд для удаления неиспользуемых графических оболочек:

- для **MATE**:

```
sudo dnf remove @MATE
```

- для **KDE Plasma**:

```
sudo dnf remove @KDE
```

- для **GNOME**:

```
sudo dnf remove @GNOME
```

Специальные возможности в графическом окружении MATE

Экранный диктор
Виртуальная клавиатура
Экранная лупа
Высококонтрастные темы

Тифлотехника — это отрасль приборостроения специального назначения, относящаяся к разработке технических средств для обучения, политехнической или производственной подготовки, трудовой деятельности и культурно-бытового обслуживания слепых, слабовидящих и слепоглухих, а также для коррекции, развития и восстановления зрения.

Основными задачами тифлотехники являются:

- уменьшение ограниченности в ориентировании слепых в пространстве, вызванной полной или частичной потерей зрения;
- создание необходимых технических условий для разностороннего развития и получения дополнительного необходимого образования;
- расширение возможности применения труда незрячих на современных механизированных производствах;
- облегчение ориентированности слепых в быту, создание возможности организации культурного отдыха и досуга.

В РЕД ОС доступно несколько специальных программ для облегчения работы слабовидящих в системе.

Вы можете подробнее ознакомиться с программами специального назначения, просмотрев наши обучающие видео:

- на **RuTube** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **Яндекс.Дзен** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **VK Видео** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника.

На наших каналах вы также сможете найти много другой полезной информации.

Экранный диктор

Средством для чтения текста (синтезатор речи) с экрана в РЕД ОС является **Orca**. Программа предоставляет доступ к рабочему столу для слабовидящих пользователей.

По умолчанию данная программа предустановлена в системе. Подробнее о работе экранного диктора **Orca** см. в нашей статье «Экранный диктор».

Виртуальная клавиатура

В РЕД ОС по умолчанию используется виртуальная клавиатура **Onboard**.

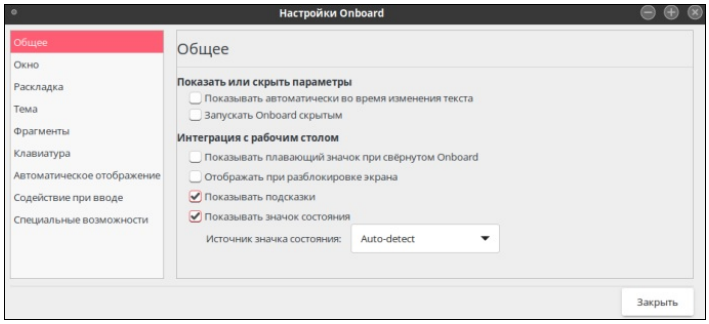
Если виртуальная клавиатура не установлена, перейдите в сеанс пользователя **root**:

```
su -
```

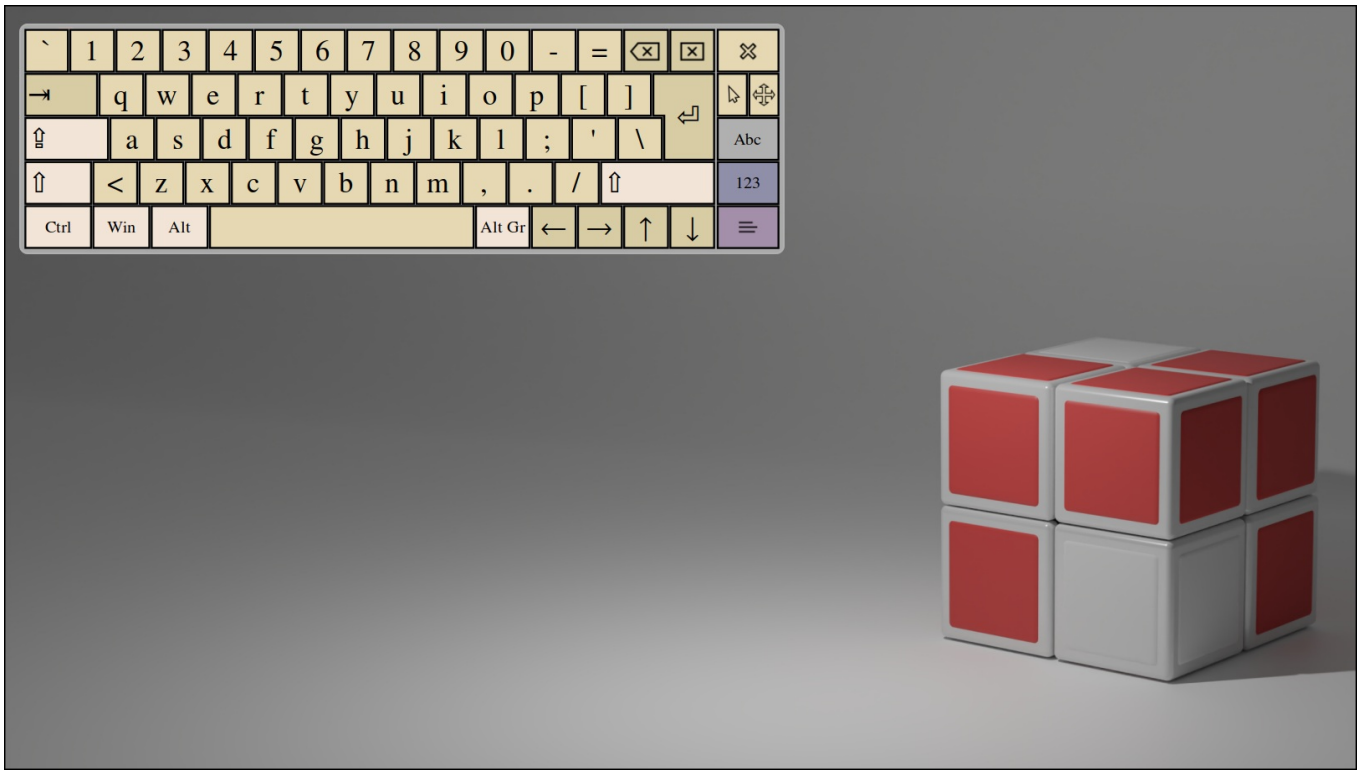
и выполните команду:

```
dnf install onboard
```

Для настройки клавиатуры перейдите в «**Главное меню**» — «**Параметры**» — «**Настройка Onboard**».



Для запуска виртуальной клавиатуры перейдите в «**Главное меню**» — «**Специальные возможности**» — «**Onboard**».



Клавиатуру можно свернуть, раскрыть или закрыть, нажав ПКМ на значок клавиатуры в системном трее, и выбрав в контекстном меню соответствующий пункт.

Экранная лупа

Также немаловажны инструменты для работы с изучением мелкого текста или фотографий.

Для данной цели существует приложение **KMagnifier** (**kmag**).

Для установки данного инструмента перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install kdeaccessibility
```

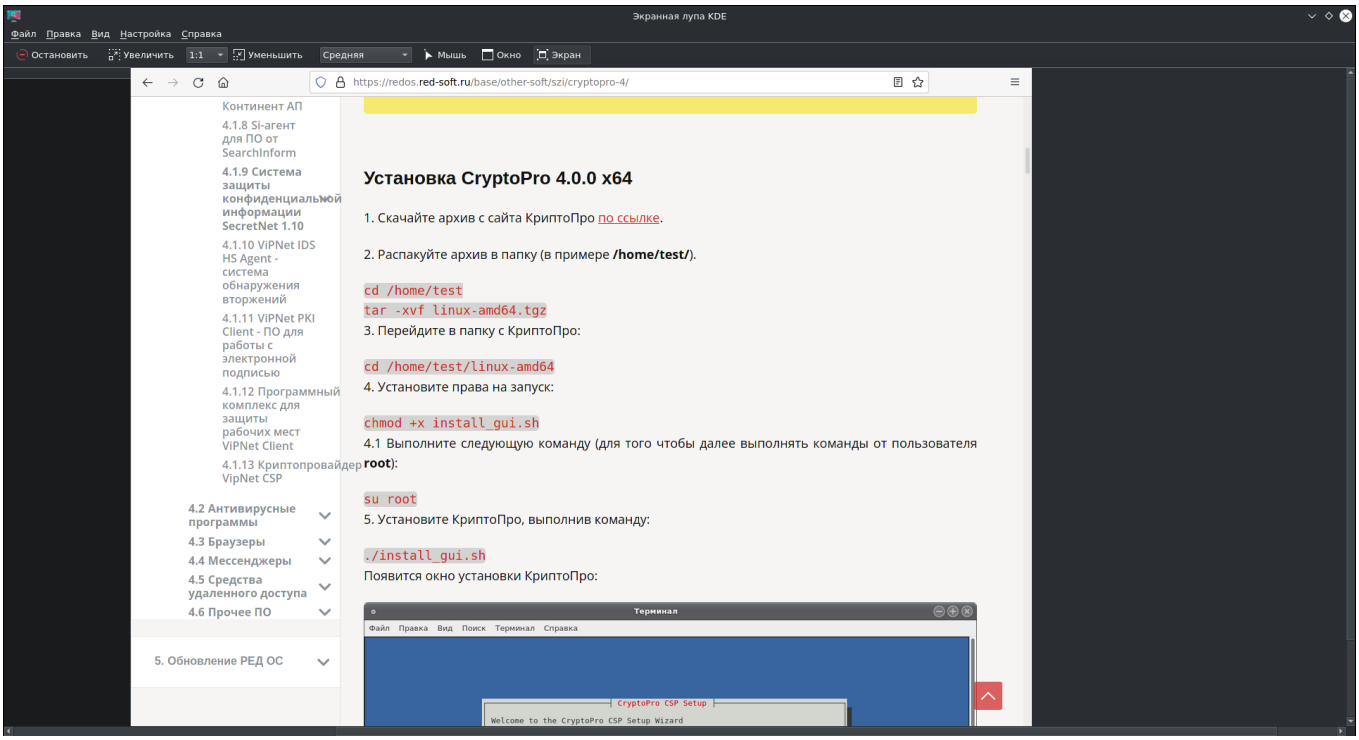
Для запуска **Kmagnifier** в графическом режиме перейдите в «**Главное меню**» — «**Специальные возможности**» — «**KMag**».

Данная программа поможет рассмотреть необходимый файл и сохранить увеличенный фрагмент на диск.

Рассмотрим, как можно воспользоваться данной программой.

Допустим, необходимо увеличить текст на странице браузера.

Для этого потребуется открыть нужный объект, который необходимо увеличить, затем перенести туда окно с экранной лупой.



Для сохранения увеличенного изображения необходимо нажать на «**Файл**» — «**Сохранить как**» и выбрать формат файла.

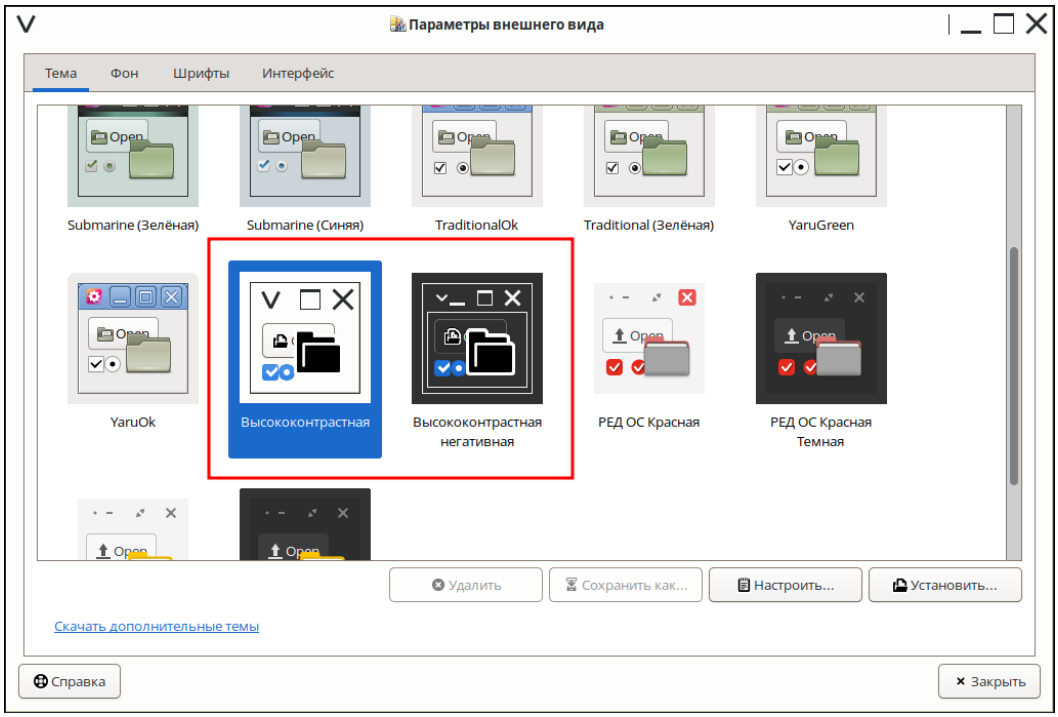
Высококонтрастные темы

Для пользователей с проблемами зрения в **MATE** предусмотрены высококонтрасные темы оформления рабочей среды. С помощью таких тем повышается контрастность окон и кнопок, чтобы их было лучше видно.

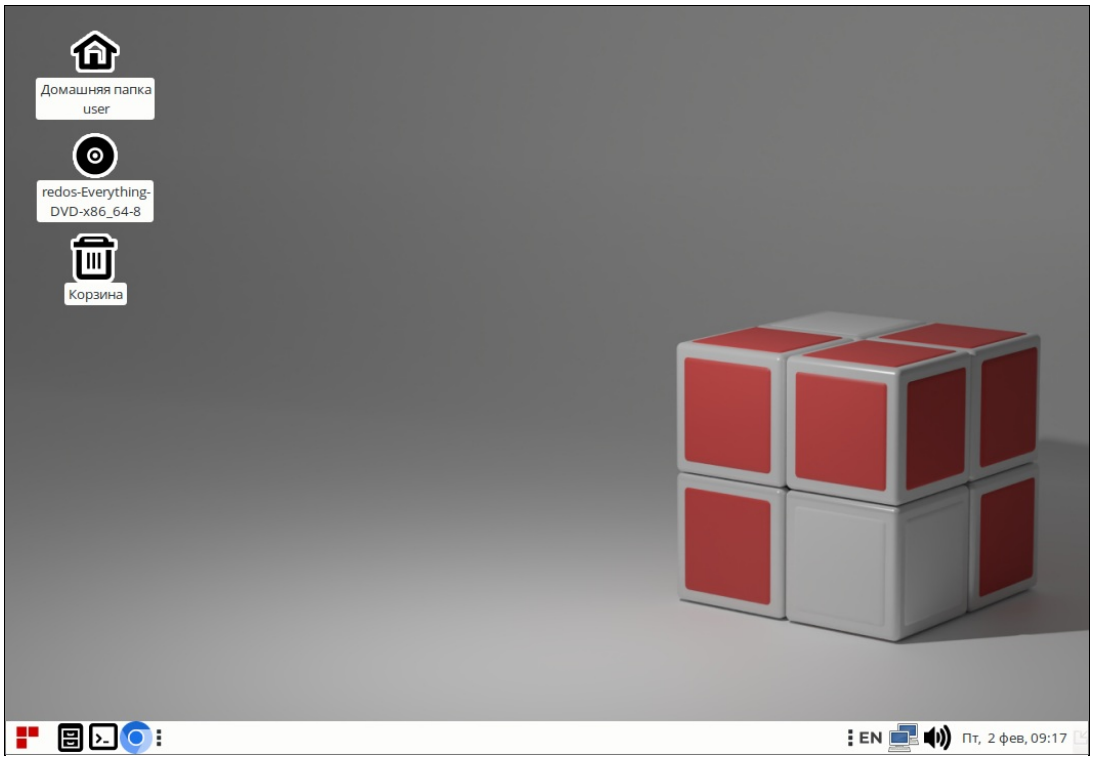
При применении высококонтрастной темы оформления иконки на рабочем столе заменяются черно-белыми аналогами, тема интерфейса приобретает монотонные цвета.

Для установки контрастной темы рабочей среды перейдите в «**Главное меню**» — «**Параметры**» — «**Внешний вид**» и на вкладке темы выберите предпочитаемую тему:

- Высококонтрастная (светлое оформление);
- Высококонтрастная негативная (темное оформление).



Внешний вид рабочего стола пользователя после применения высококонтрастной темы:


Домашняя папка
user
redos-Everything-
DVD-x86_64-8
Корзина
EN
Пт, 2 фев, 09:17

Специальные возможности в графическом окружении KDE

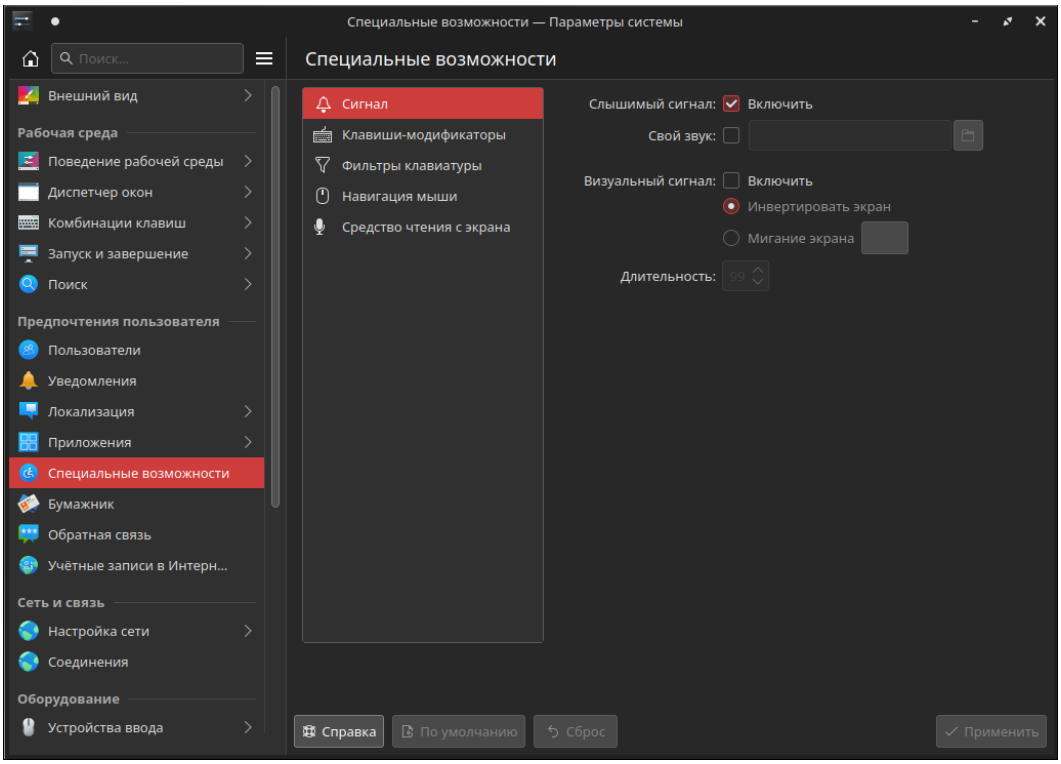
Сигнал
Клавиши-модификаторы
Фильтры клавиатуры
Замедленные клавиши
"Прыгающие" клавиши
Навигация мыши
Управление курсором мыши с цифрового блока клавиатуры
Средство чтения с экрана
Высококонтрастные темы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

В графическом окружении **KDE Plasma** реализованы специальные возможности для облегчения работы за компьютером людям с ограниченными возможностями здоровья по зрению и/или слуху.

Соответствующие настройки доступны из «**Меню запуска приложений**» – «**Настройка**» – «**Параметры системы**» в разделе «**Специальные возможности**».

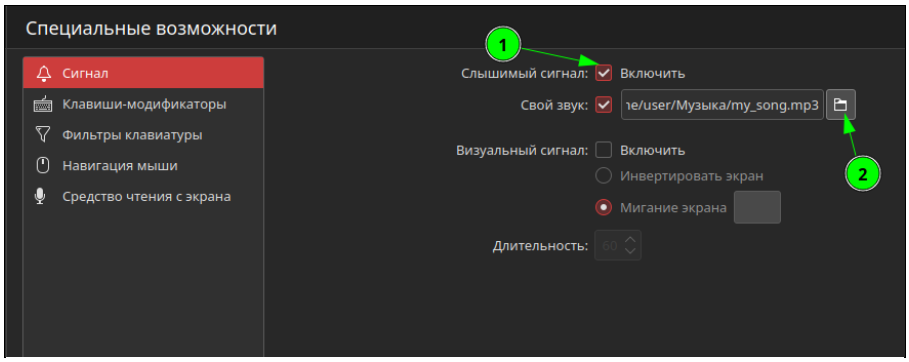


Сигнал

Вкладка «**Сигнал**» содержит разделы «**Слышимый сигнал**» и «**Визуальный сигнал**».

Установленный флаг для параметра «**Включить**» в разделе «**Слышимый сигнал**» определяет, будет ли слышен системный динамик. Если флаг не установлен, системный динамик слышно не будет.

Для дублирования или замены звука системного динамика можно назначить воспроизведение выбранного звукового файла. Для этого установите флаг «**Свой звук**» и с помощью кнопки «**Обзор...**» в открытом диалоговом окне выберите нужный файл.

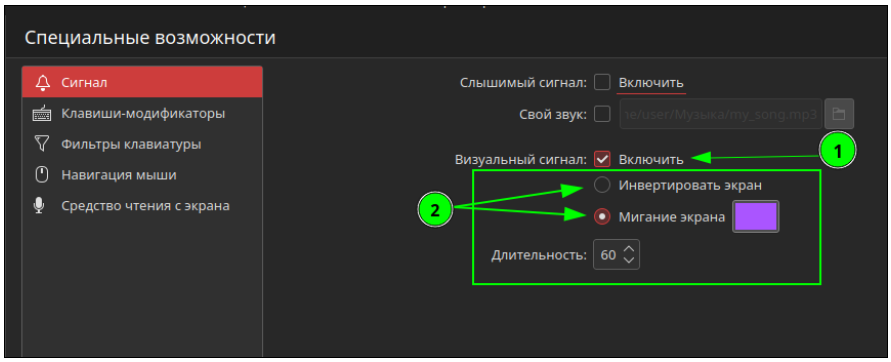


Пользователи, которые плохо слышат системные звуковые сигналы, и те, кто пользуется компьютером в беззвучном режиме, могут использовать «**Визуальный сигнал**». При его использовании вместо звукового сигнала будет воспроизводиться видимый сигнал (на выбор: *инвертирование экрана* или *мигание*).

Чтобы включить визуальный сигнал, установите флаг «**Визуальный сигнал**».

Затем следует выбрать режим визуализации системного звукового сигнала: «**Инвертировать экран**» или «**Мигание экрана**». В первом случае для вывода оповещения будут инвертированы цвета экрана, во втором – экран будет мигать цветом, который возможно выбрать, используя кнопку, расположенную справа.

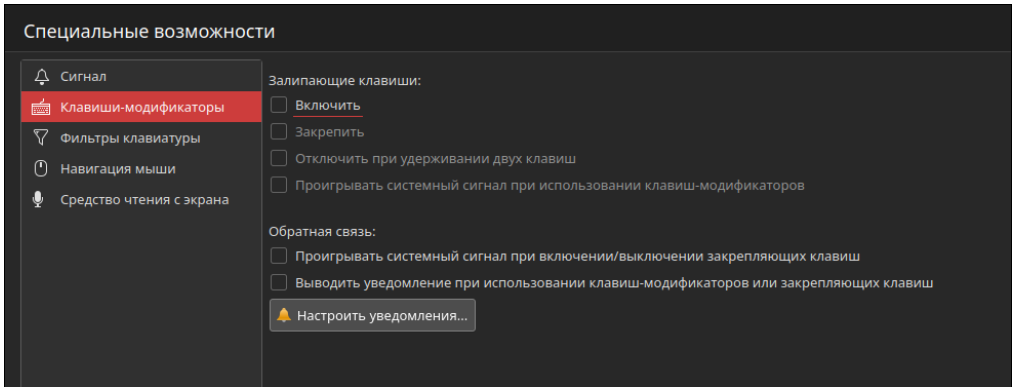
Длительность визуального сигнала регулируется с помощью соответствующего поля, по умолчанию установлена длительность **99 мс**.



Клавиши-модификаторы

Вкладка «**Клавиши-модификаторы**» позволяет настраивать поведение функций залипания клавиш. *Залипание клавиш* – это функция операционных систем, позволяющая нажимать комбинацию клавиш клавиатуры не одновременно, а последовательно.

На вкладке доступны разделы «**Залипающие клавиши**» и «**Обратная связь**».



При включении функции «**Залипающие клавиши**» для использования комбинации клавиш достаточно нажать и отпустить **Shift**, **Alt** и/или **Ctrl** и затем нажать необходимую клавишу. Например, комбинация **Ctrl+Alt+Del** может быть выполнена последовательным нажатием **Ctrl**, потом **Alt** и затем **Del**.

В этом разделе расположен флаг «**Закрепить**». Если он установлен, клавиши **Alt**, **Ctrl** и **Shift** остаются «нажатыми» до повторного нажатия на них.

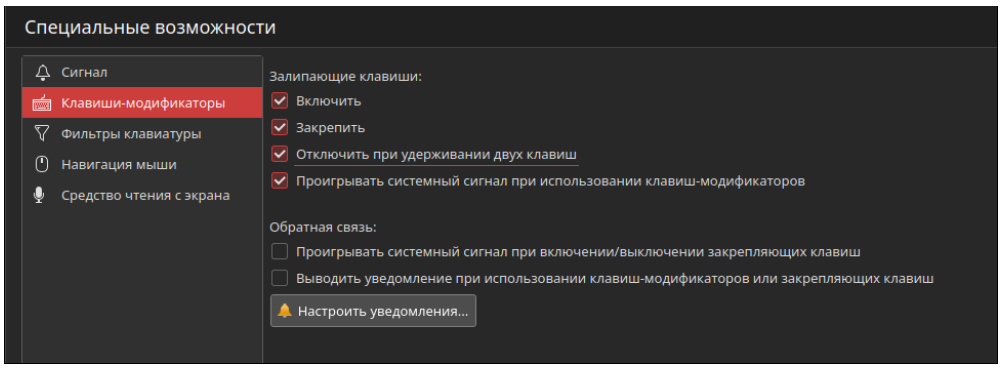
Например:

- флаг «*Закрепить*» **снят** – последовательное нажатие клавиш **Shift** и **F** компьютер будет воспринимать как нажатие комбинации **Shift+F**. Если затем нажать клавишу **P**, компьютер воспримет это как строчную букву «**p**» (без **Shift**).

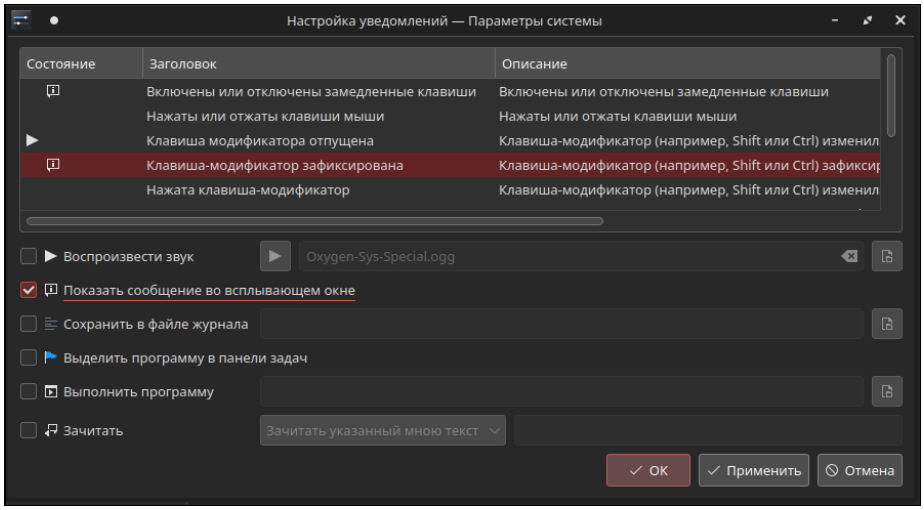
- флаг «*Закрепить*» **установлен** – двойное нажатие клавиши **Shift** и нажатие клавиши F компьютер будет воспринимать как комбинацию **Shift+F**. Если после этого нажать клавишу **P**, компьютер воспримет это как прописную букву «**P**» (**Shift+P**). Чтобы отменить залипание клавиши **Shift**, нужно нажать её ещё раз.

Активация флага «**Отключить при удерживании двух клавиш**» позволяет избежать случайного набора комбинаций и отключает уже нажатые залипшие клавиши.

Активация флага «**Проигрывать системный сигнал при использовании клавиш-модификаторов**» позволяет извещать пользователя звуковым сигналом при нажатии клавиши-модификатора.



В разделе «**Обратная связь**» пользователь может настроить оповещения от операционной системы об использовании (включении/выключении) закрепляющих клавиш, а также определить собственные уведомления для определенного действия с клавишами-модификаторами, нажав «**Настроить уведомления...**».

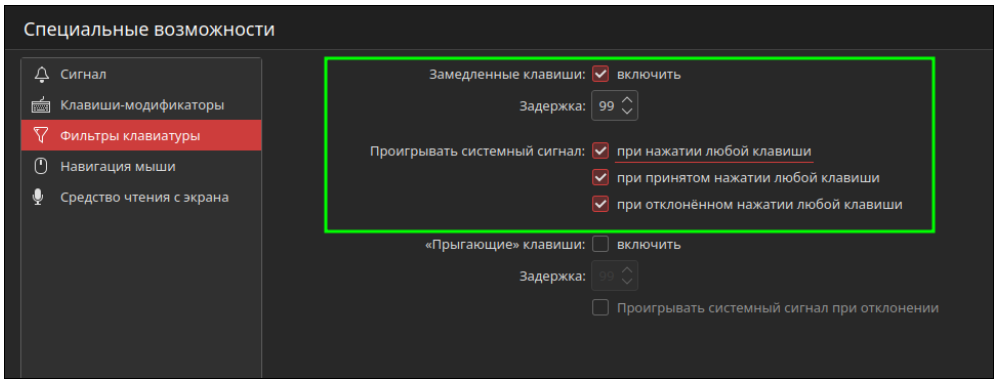


Фильтры клавиатуры

Вкладка «**Фильтры клавиатуры**» содержит два раздела – **Замедленные клавиши** и **"Прыгающие" клавиши**.

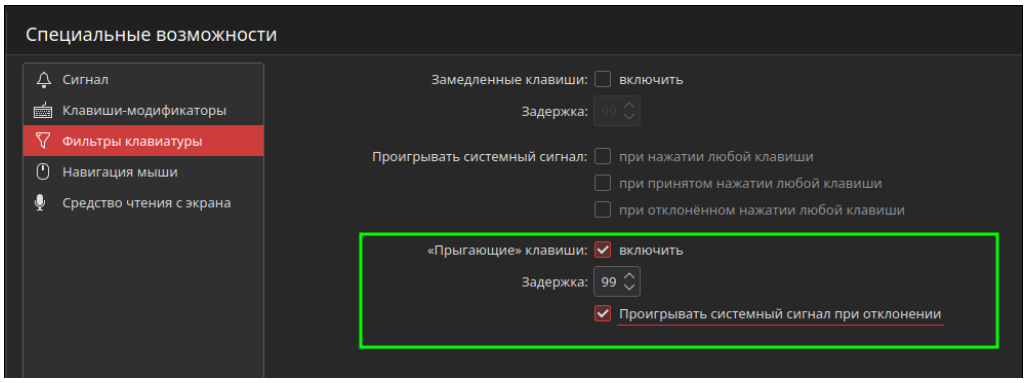
Замедленные клавиши

Если параметр включен, пользователь должен держать клавишу нажатой определённое время (настраивается с помощью соответствующего поля), чтобы она была воспринята, как нажатая. Это помогает избежать негативных последствий от случайного нажатия клавиш. Также можно выбрать, когда будет проигрываться системный сигнал – при нажатии любой клавиши, при принятом нажатии любой клавиши, при отклонённом нажатии любой клавиши.



"Прыгающие" клавиши

При включении этого параметра между нажатиями двух клавиш должно пройти определённое время (которое устанавливается при помощи счётчика), чтобы следующая клавиша была воспринята. Это помогает избежать негативных последствий от случайного нажатия сразу нескольких клавиш. Дополнительно можно включить системный сигнал, который будет проигрываться при отклонении.

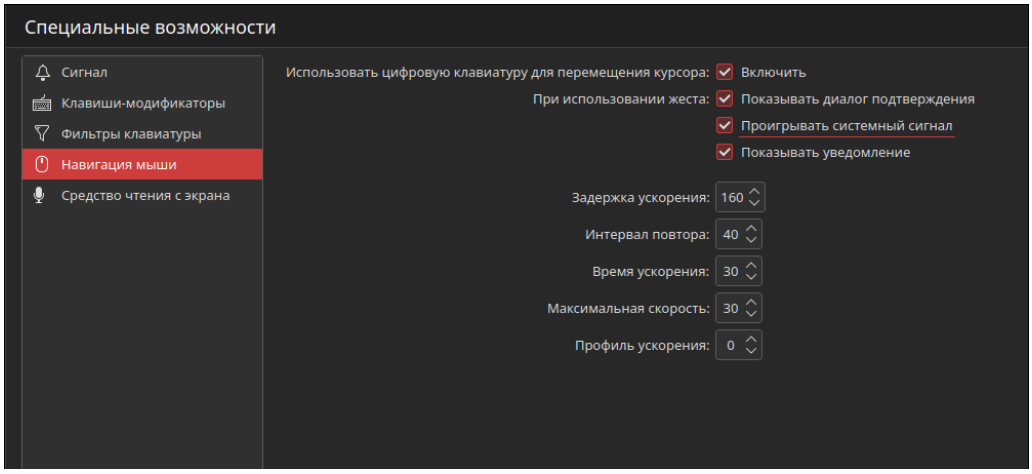


Навигация мыши

Вкладка «**Навигация мыши**» позволяет настроить цифровую клавиатуру для управления курсором мыши. Это может быть полезно при работе на компьютере без другого устройства указания или в тех случаях, когда цифровая клавиатура больше никак не используется.

Управление курсором мыши с цифрового блока клавиатуры

Для включения режима управления курсором мыши с клавиатуры необходимо установить флаг «**Использовать цифровую клавиатуру для перемещения курсора**». После этого станут доступны остальные параметры управления курсором с помощью клавиатуры, при необходимости их можно будет настроить.



Нажатие различных клавиш на цифровой клавиатуре приводит к перемещению в ожидаемом направлении. Обратите внимание, что указатель можно перемещать как по диагонали, так и по горизонтали/вертикали. Клавиша **5** эмулирует щелчок устройства указания, обычно *левой кнопки мыши*. Эмулируемую клавишу можно выбрать с помощью клавиши **/** (что сделает её левой кнопкой мыши), клавиши ***** (что сделает её средней кнопкой мыши) и клавиши **–** (что сделает её правой кнопкой мыши). Клавиша **+** эмулирует двойной щелчок выбранной кнопки устройства указания. С помощью клавиши **0** можно эмулировать удержание в нажатом состоянии

выбранной кнопки устройства указания (для облегчения перетаскивания), и затем использовать клавишу **.** для эмуляции отпускания кнопки устройства указания.

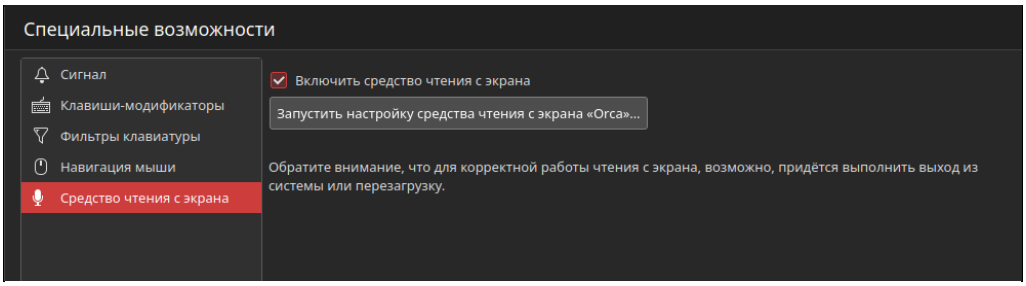
При использовании какого-либо эмулируемого жеста можно настроить оповещения, установив соответствующий флаг – «**Показать диалог подтверждения**», «**Проигрывать системный сигнал**» или «**Показывать уведомление**».

Параметры, определяющие скорость движения указателя:

- **Задержка ускорения** – время (в миллисекундах), которое проходит между нажатием клавиши и первым повторением события движения при ускорении передвижения.
- **Интервал повтора** – время (в миллисекундах) между повторами события передвижения при ускорении передвижения.
- **Время ускорения** – время (в миллисекундах), за которое указатель достигает максимальной скорости за счёт ускорения.
- **Максимальная скорость** – максимальная скорость (в пикселах в секунду), которую указатель мыши может достичь за счёт ускорения.
- **Профиль ускорения** – наклон кривой ускорения при ускорении передвижения курсора.

Средство чтения с экрана

Вкладка «**Средство чтения с экрана**» позволяет настроить специализированную утилиту **Orca**.



Для настройки утилиты нажмите кнопку «**Запустить настройку средства чтения с экрана «Orca»...**».

Подробнее о настройке экранного диктора **Orca** см. в нашей статье «Экранный диктор».

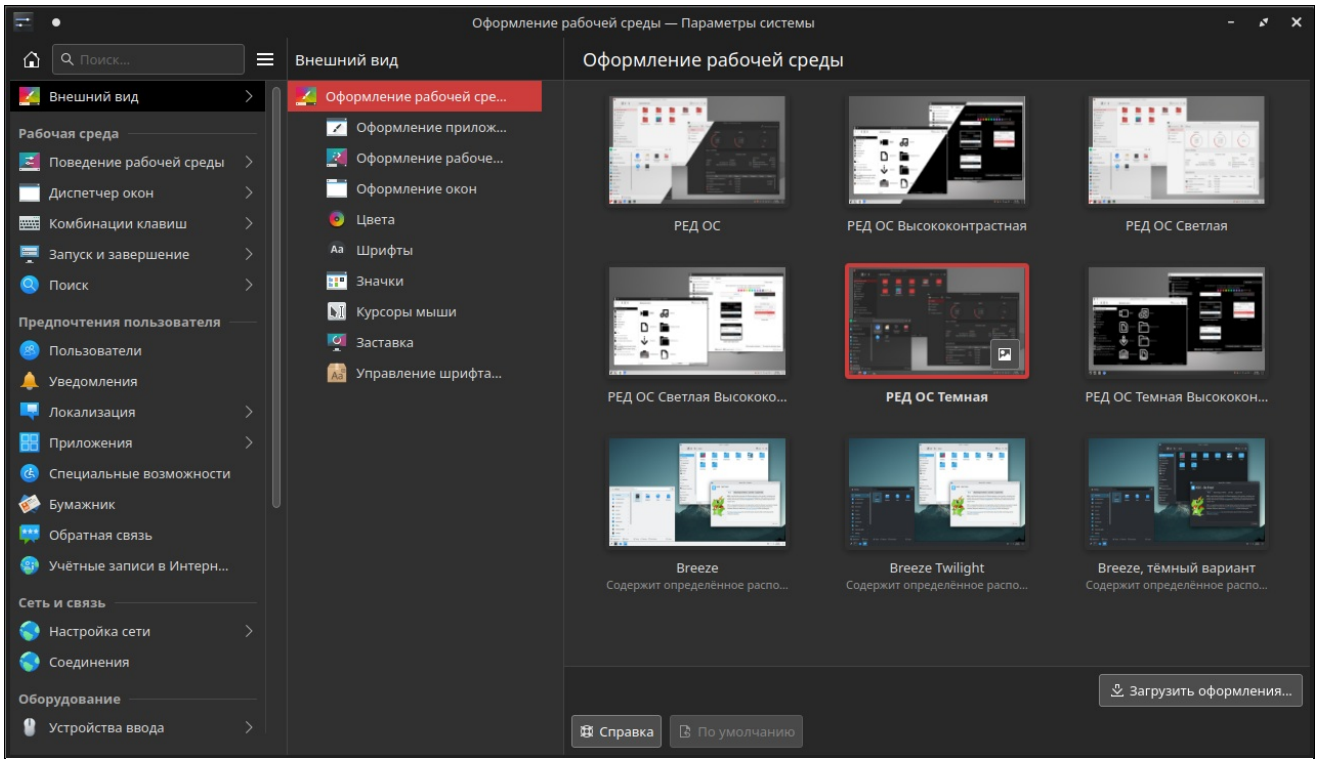
Для корректной работы средства чтения с экрана необходимо активировать флажок «**Включить средство чтения с экрана**», выйти из системы и перезапустить сеанс рабочего стола.

Высококонтрастные темы

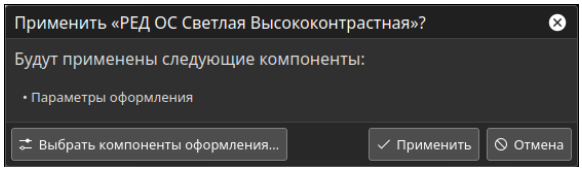
Для людей с проблемами зрения доступна установка высококонтрастных тем оформления рабочей среды. Для применения высококонтрастной темы перейдите в «**Меню запуска приложений**» – «**Настройка**» – «**Параметры системы**», откройте раздел «**Внешний вид**» – «**Оформление рабочей среды**».

На выбор доступны 2 темы:

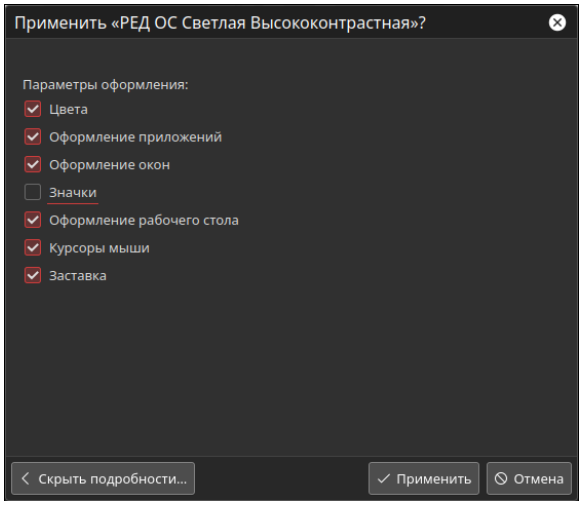
- РЕД ОС Светлая Высококонтрастная;
- РЕД ОС Высококонтрастная (темная).



Выберите нужную тему оформления и в появившемся диалоговом окне нажмите «**Применить**» для применения оформления рабочей среды.



Также пользователю доступен выбор компонентов оформления. Для выбора необходимых компонентов нажмите соответствующую кнопку диалогового окна и определите параметры, к которым необходимо применить новое оформление.



Специальные возможности в графическом окружении GNOME

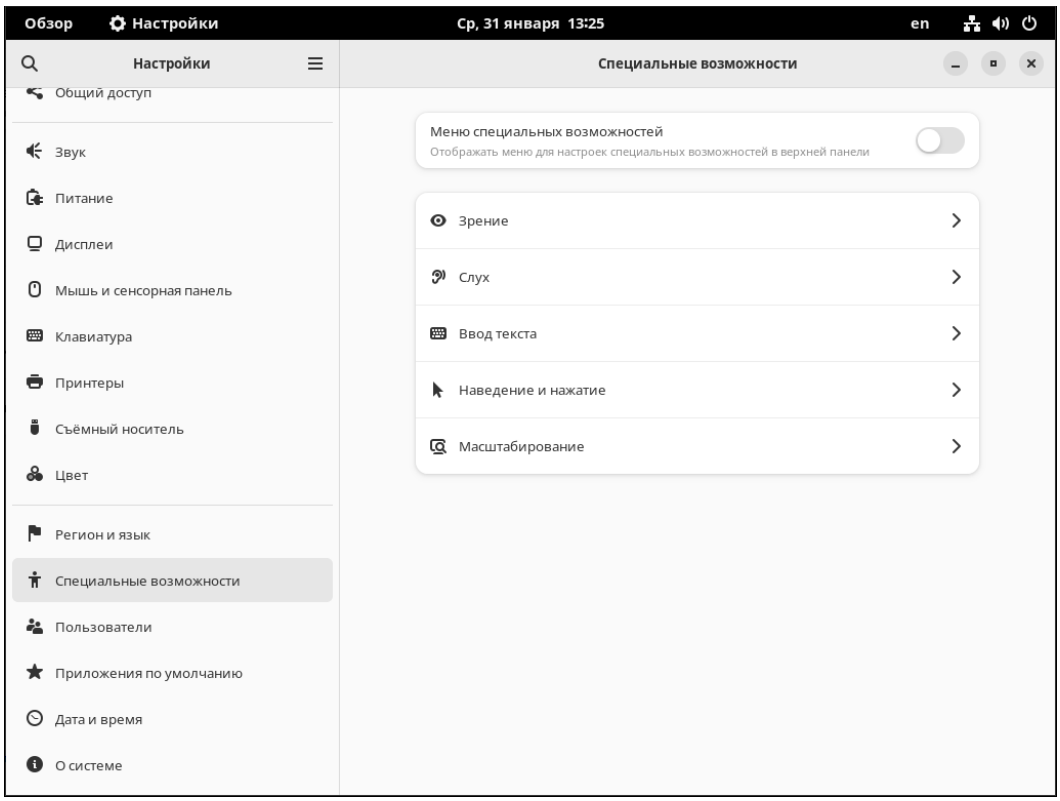
Зрение
Чтение с экрана
Слух
Ввод текста
Наведение и нажатие
Масштабирование

Окружение

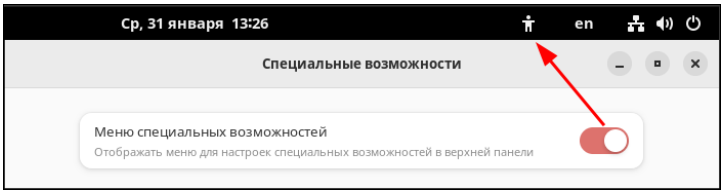
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

В графическом окружении **GNOME** реализованы специальные возможности для облегчения работы за компьютером людям с ограниченными возможностями здоровья по зрению и/или слуху.

Соответствующие настройки доступны из меню «**Показать приложения**» – «**Настройки**» в разделе «**Специальные возможности**».



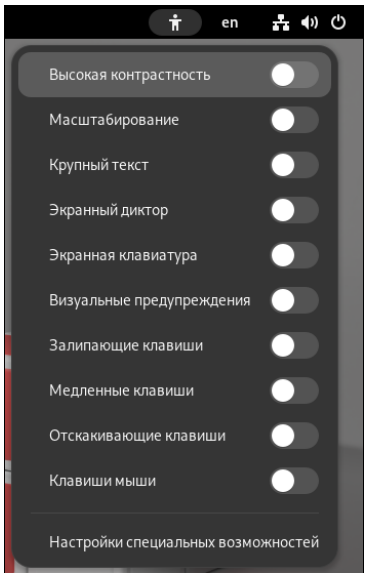
При активации меню специальных возможностей в системной панели отображается соответствующая иконка.



Меню специальных возможностей позволяет включать и отключать различные настройки специальных возможностей.

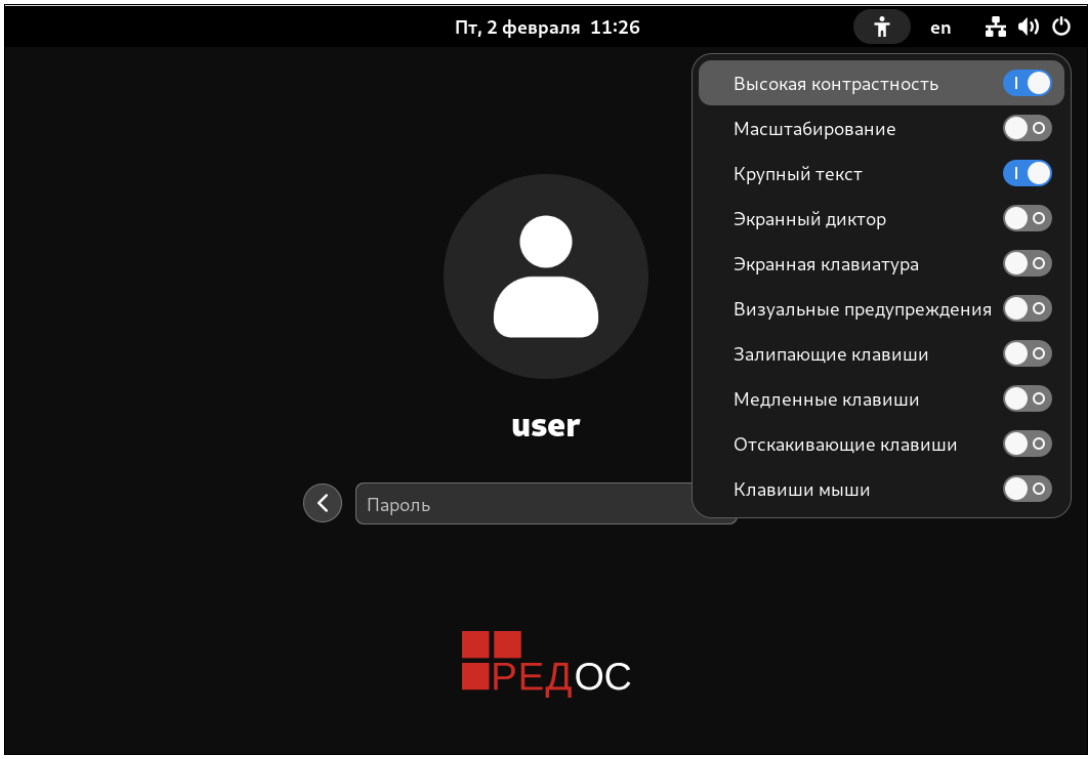
Чтобы получить доступ к этому меню с помощью клавиатуры, нажмите **Ctrl+Alt+Tab** для перемещения фокуса клавиатуры на верхнюю панель. Под кнопкой **Обзор** появится белая полоса, показывающая, какой элемент верхней панели выбран.

С помощью клавиш со стрелками переместите белую полосу под меню специальных возможностей и нажмите **Enter**, чтобы открыть меню. Для выбора пунктов меню используйте клавиши со стрелками вверх и вниз. Чтобы переключить выбранный пункт меню, нажмите **Enter**.



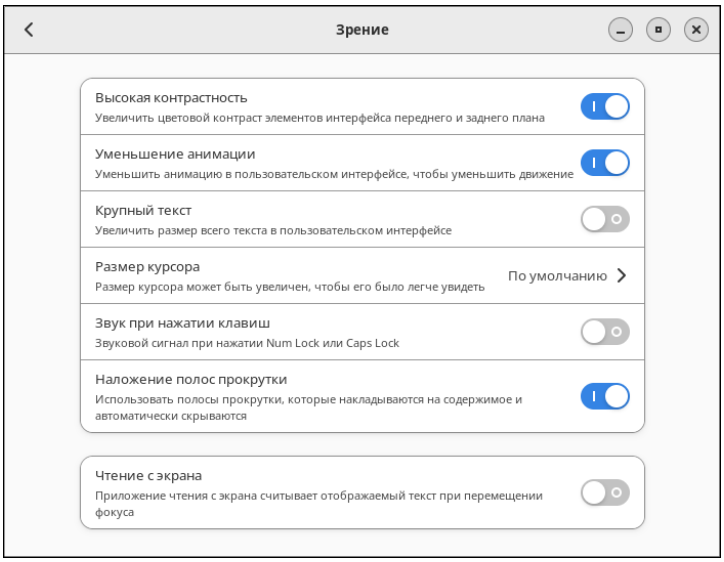
В графическом менеджере входа в систему (**GDM**) *меню специальных возможностей* доступно по умолчанию и имеет те же параметры:

- *высокая контрастность* – включение высококонтрастной темы оформления рабочей среды;
- *масштабирование* – увеличение определенной части рабочей области;
- *крупный текст* – увеличение размера текста на экране;
- *экранный диктор* – озвучивание элементов пользовательского интерфейса;
- *экранная клавиатура* – использование экранной клавиатуры вместо обычной;
- *визуальные предупреждения* – включение мигания экрана при наступлении определенных событий;
- *залипающие клавиши* – включение функции залипающих клавиш;
- *медленные клавиши* – включение функции медленных клавиш;
- *отскакивающие клавиши* – включение функции отскакивающих клавиш;
- *клавиши мыши* – управление указателем мыши с помощью клавиатуры.



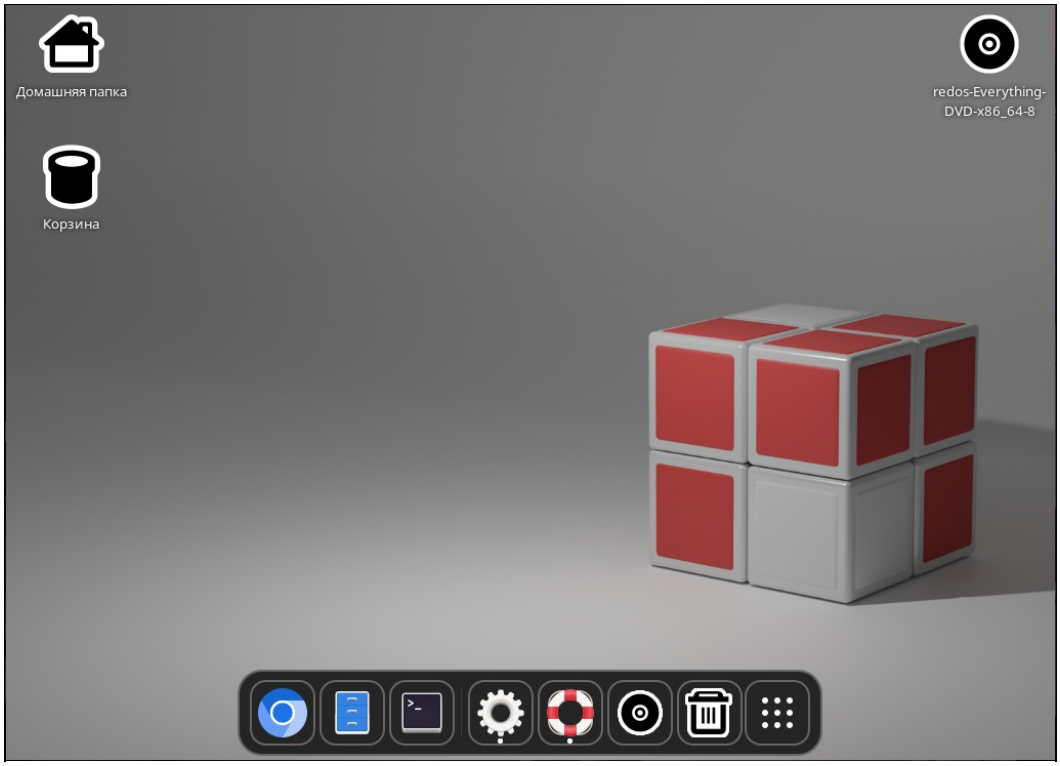
Зрение

В разделе «**Зрение**» доступны визуальные настройки пользовательского интерфейса.



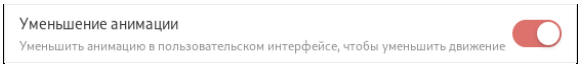
Высокая контрастность

При включении функции «**Высокая контрастность**» можно настроить контрастность окон и кнопок, чтобы их было лучше видно. Функция не относится к изменению яркости всего экрана, изменяются только отдельные элементы пользовательского интерфейса. Иконки на рабочем столе заменяются черно-белыми аналогами, тема интерфейса приобретает монотонные цвета.



Уменьшение анимации

При включении функции «**Уменьшение анимации**» настроенные эффекты окон (восстановление, скрытие, переключение, наведение курсора мыши) будут отключены.



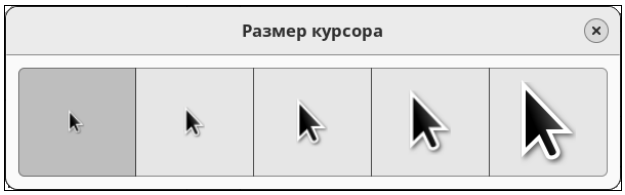
Крупный текст

При включении функции «**Крупный текст**» увеличивается размер шрифта в пользовательском интерфейсе.



Размер курсора

Выбирая «**Размер курсора**», можно увеличить видимость указателя мыши.



Звук при нажатии клавиш

Если «**Звук при нажатии клавиш**» включен, то каждый раз при нажатии клавиш **Num Lock** или **Caps Lock** будет воспроизводиться системный сигнал.

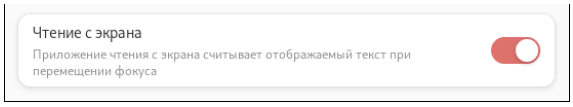
Наложение полос прокрутки

При включении «**Наложения полос прокрутки**» дополнительно накладываются полосы прокрутки поверх содержимого на экране, которые автоматически скрываются.

Чтение с экрана

Также для пользователей с нарушением зрения **GNOME** предоставляет экранный диктор **Orca**. Если параметр «**Чтение с экрана**» включен, любой элемент пользовательского интерфейса или текст, на который наведен фокус клавиатуры, читается вслух. Подробнее о работе экранного диктора **Orca** см. в нашей статье «Экранный диктор».

Для быстрого запуска экранного диктора можно использовать сочетание клавиш **Super+Alt+S** или нажать на значок специальных возможностей в верхней панели и выбрать пункт **Экранный диктор**.

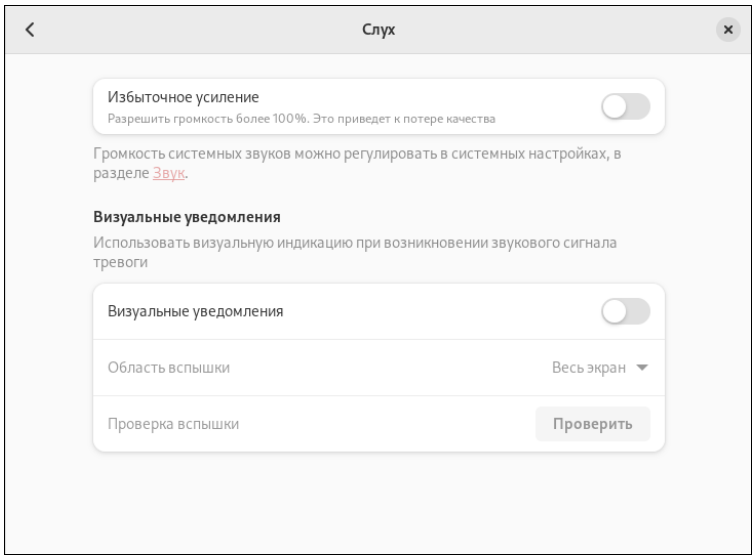


Слух

Для пользователей с нарушением слуха доступна настройка увеличения громкости сверх предела в 100% – «**Избыточное усиление**». Однако слишком высокая громкость приведет к значительному снижению качества звука.

Для некоторых типов сообщений и событий воспроизводятся звуковые уведомления. Если пользователю трудно их услышать, можно настроить визуальные уведомления – при воспроизведении уведомлений мигает либо весь экран, либо текущее окно.

При нажатии «**Проверить**» можно ознакомиться с поведением данной функции.

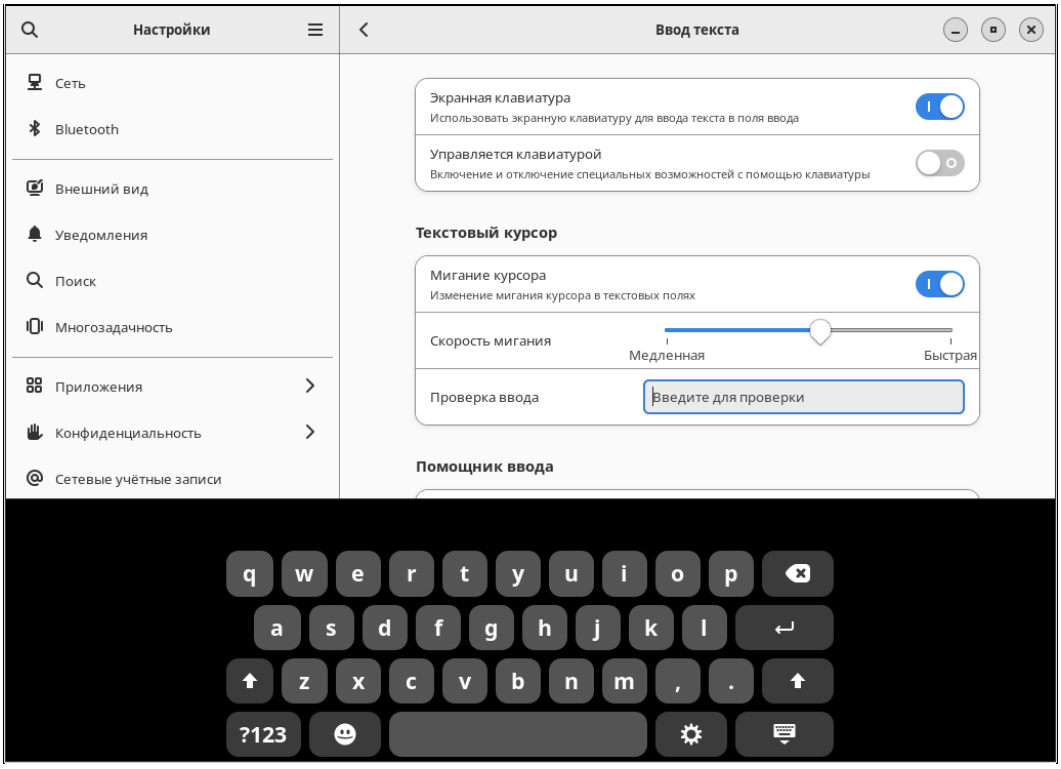


Ввод текста

Экранная клавиатура

Если к компьютеру не подключена клавиатура, или пользователь предпочитает её не использовать, в **GNOME** доступен ввод текста с помощью экранной клавиатуры. Для этого следует активировать функцию «**Экранная клавиатура**».

В следующий раз, когда пользователю потребуется вводить текст, экранная клавиатура появится в нижней части экрана.



Для ввода цифр и символов нажмите кнопку **?123**. Дополнительные символы будут доступны при нажатии кнопки **=/<**. Чтобы снова вернуться к алфавитной клавиатуре, нажмите кнопку **ABC**.

Если экранная клавиатура больше не нужна, нажмите кнопку  , чтобы временно скрыть клавиатуру. Клавиатура снова автоматически появится, когда пользователь установит курсор мыши в поле ввода.

Управление с помощью клавиатуры

При включении функции «**Управляется клавиатурой**» можно получить доступ к использованию компьютера без мыши или другого указательного устройства.

Далее приведены комбинации клавиш для людей, которые не могут использовать мышь или другое указательное устройство, или

хотят больше пользоваться клавиатурой.

Навигация по пользовательскому интерфейсу

Комбинации клавиш	Назначение
Tab, **Ctrl+Tab**	Перемещение фокуса клавиатуры между различными элементами управления. **Ctrl+Tab** перемещает между группами элементов, например, с боковой панели в основную область окна. **Ctrl+Tab** также позволяет выйти из элемента управления, который сам использует **Tab**, такого как текстовая область. Удерживайте нажатой **Shift** для перемещения фокуса в обратном порядке.
Клавиши со стрелками	Перемещение выбора между частями одного элемента управления или группы взаимосвязанных элементов. Используйте клавиши со стрелками для выбора кнопки на панели инструментов, объектов при просмотре в режиме списка или значков, а также кнопки из группы радиокнопок.
Ctrl+клавиши со стрелками	В режиме списка или значков – перемещение фокуса клавиатуры на другой объект, не снимая выделение с ранее выделенного объекта.
Shift+клавиши со стрелками	В режиме списка или значков – выделение группы объектов, начиная с текущего выделенного объекта, и заканчивая вновь выбранным объектом. В режиме древовидной структуры элементов, имеющие дочерние элементы, можно развернуть или свернуть, чтобы отобразить или скрыть их: развернуть, нажав **Shift+→**, и свернуть, нажав **Shift+←**.
Пробел	Активация обладающего фокусом объекта, такого как кнопка, флаг или элемент списка.
Ctrl+пробел	В режиме списка или значков – выделение или снятие выделения с обладающего фокусом объекта, не снимая выделение с других объектов.
Alt	Удерживайте клавишу **Alt** для показа горячих клавиш: подчёркнутых букв в командах меню, на кнопках и других элементах управления. Нажмите Alt и подчёркнутую букву, чтобы активировать элемент управления, как если бы вы нажали на него мышью.
Esc	Выход из меню, всплывающего окна, переключателя или диалогового окна.
F10	Открывает первое меню в строке меню окна. Используйте клавиши со стрелками для перемещения по меню.
Super+F10	Открывает меню приложения в верхней панели.
Shift+F10, **Меню**	Всплывающее контекстное меню для выбранного объекта, как при нажатии правой кнопкой.
Ctrl+F10	В менеджере файлов всплывающее контекстное меню для текущей папки, как при нажатии правой кнопкой на пустом месте в папке.
Ctrl+PageUp, **Ctrl+PageDown**	В интерфейсе со вкладками переключение на вкладку слева или справа.

Навигация по рабочему столу

Комбинации клавиш	Назначение
Alt+F1, **клавиша Super**	Переключение между **Обзором** и **рабочим столом**. Чтобы быстро найти нужное приложение, контакт или документ, просто начните вводить его имя в **Обзоре**.
Super+Tab	Быстрое переключение между окнами. Удерживайте клавишу **Shift** для переключения в обратном порядке.
Super+`	Переключение между окнами приложения или приложения, выбранного нажатием **Super+Tab**. В этой комбинации используется клавиша `, расположенная над клавишей **Tab**. Если на вашей клавиатуре нет клавиши `, используйте **Super** и клавишу, находящуюся над клавишей **Tab**.
Ctrl+Alt+Tab	Передаёт фокус верхней панели. В **Обзоре** переключает фокус клавиатуры между верхней панелью, панелью задач, обзором окон, списком приложений и полем поиска. Для навигации используйте клавиши со стрелками.
Super+Page Up, **Super+Page Down**	Переключение между рабочими местами.
Alt+F6	Циклическое переключение между окнами одного приложения. Удерживайте **Alt** и нажимайте **F6**, пока не выделится подсветкой нужное окно, затем отпустите **Alt**. Это действие подобно комбинации **Alt+`**.
Alt+Esc	Циклическое переключение между всеми окнами на рабочем месте.
Super+V	Открывает панель сообщений. Нажмите **Esc**, чтобы закрыть панель.

Управление окнами

Комбинации клавиш	Назначение
Alt+F4	Закрывает текущее окно.
Alt+F, Super+↓	Восстановление исходных размеров окна. Используйте **Alt+F10** для разворачивания окна. Повторное нажатие **Alt+F10** восстановит предыдущие размеры окна.
Alt+F7	Перемещение текущего окна. Нажмите **Alt+F7**, затем используйте клавиши со стрелками для перемещения окна. Нажмите **Enter**, чтобы завершить перемещение окна, или **Esc** для возврата окна в исходную позицию.
Alt+F8	Изменение размера текущего окна. Нажмите **Alt+F8**, затем используйте клавиши со стрелками для изменения размера окна. Нажмите **Enter**, чтобы завершить изменение размера, или **Esc**, чтобы вернуть окну исходный размер.
Shift+Super+Page Up , **Shift+Super+Page Down**	Перемещение текущего окна на другое рабочее место.
Shift+Super+←	Переместить текущее окно на один монитор влево.
Shift+Super+→	Переместить текущее окно на один монитор вправо.
Alt+F10, Super+↑	Разворачивание окна. Чтобы восстановить размер окна до прежних размеров, нажмите **Alt+F10** или **Super+↓**.
Super+H	Свернуть окно.
Super+←	Разворачивание окна вертикально вдоль левого края экрана. Нажмите снова, чтобы восстановить предыдущий размер окна. Нажмите **Super+→** для смены краёв экрана.
Super+→	Разворачивание окна вертикально вдоль правого края экрана. Нажмите снова, чтобы восстановить предыдущий размер окна. Нажмите **Super+←** для смены краёв экрана.
Alt+пробел	Открывает меню окна, как при нажатии правой кнопкой по заголовку окна.

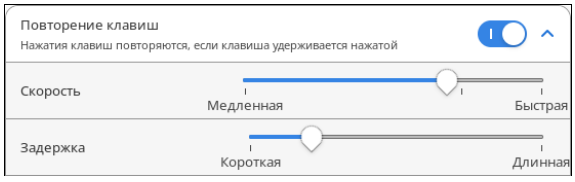
Текстовый курсор

В случае если пользователю трудно рассмотреть курсор в поле ввода текста, можно сделать его мигающим. В пункте «**Мигание курсора**» измените частоту мерцания указателя.

Помощник ввода

В разделе «**Помощник ввода**» доступны следующие вспомогательные параметры:

- **Повторение клавиш**. По умолчанию при удержании клавиши нажатой буква или символ печатаются повторно до тех пор, пока пользователь не отпустит клавишу. Если пользователю трудно быстро поднимать пальцы, можно отключить эту функцию или изменить время до начала повторения после нажатия клавиши, также можно настроить скорость повторения нажатых клавиш.



- **Залипающие клавиши**. Залипающие клавиши позволяют вводить комбинации клавиш не одновременным нажатием всех клавиш, а нажимая их по одной последовательно. Например, для переключения между окнами используется комбинация клавиш **Super+Tab**. Если «залипающие клавиши» отключены, нужно нажать обе клавиши одновременно, если включены — можно нажать сначала **Super** и затем **Tab**.

«**Залипающие клавиши**» могут быть полезны, если пользователю трудно удерживать нажатыми несколько клавиш одновременно.

Быстрое включение и отключение «залипающих клавиш».

Измените положение переключателя **Управляется клавиатурой**, чтобы включить или выключить залипание клавиш на клавиатуре. Если этот параметр включен, можно нажать **Shift** пять раз подряд, чтобы включить или отключить залипание клавиш.

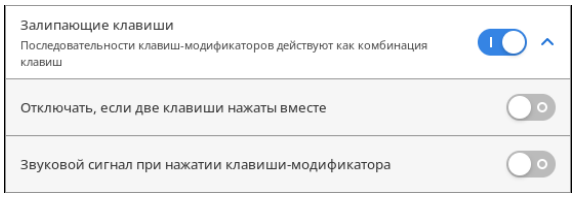
Чтобы включить или отключить залипающие клавиши, можно также нажать на значок специальных возможностей в верхней панели и выбрать **Залипающие клавиши**. Значок специальных возможностей становится виден в том случае, если один или более параметров были включены в разделе **Специальные возможности**.

Если нажать две клавиши одновременно, «залипающие клавиши» временно отключатся, чтобы пользователь мог ввести комбинацию клавиш «обычным» способом.

Например, если залипающие клавиши включены, но пользователь нажал **Super** и **Tab** одновременно, залипающие клавиши не будут ждать нажатия ещё одной клавиши. Однако они будут ожидать следующего нажатия, если пользователь нажал только одну клавишу из нужной комбинации. Это полезно, если пользователь может нажимать некоторые сочетания клавиш одновременно (например, клавиши, которые находятся рядом друг с другом).

Для включения этой возможности выберите **Отключать, если две клавиши нажаты вместе**.

Можно сделать так, чтобы компьютер подавал звуковой сигнал, если пользователь начинает набор на клавиатуре при включённых «залипающих клавишах». Это полезно, если пользователю необходимо знать, когда «залипающие клавиши» ожидают нажатия комбинации клавиш и следующее нажатие будет интерпретироваться, как часть этой комбинации. Для включения этой возможности выберите **Звуковой сигнал при нажатии клавиши-модификатора**.



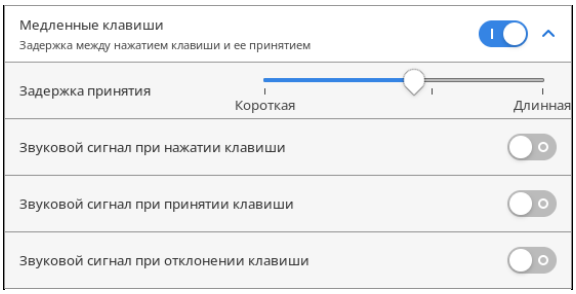
- **Медленные клавиши**. Включите «медленные клавиши», если необходимо, чтобы между нажатием клавиши и появлением символа на экране была задержка. Для набора каждого символа в таком случае нужно будет некоторое время удерживать соответствующую клавишу нажатой. Полезно использовать «медленные клавиши», если при наборе пользователь часто случайно нажимает несколько клавиш одновременно.

Быстрое включение и отключение «медленных клавиш» .

Измените положение переключателя **Управляется с клавиатуры**, чтобы включить или выключить «медленные» клавиши с клавиатуры. Если этот параметр включён, то, нажав и удерживая клавишу **Shift** в течение **восьми секунд**, можно включать и отключать «медленные» клавиши. Для включения или отключения «медленных клавиш» можно также нажать на значок специальных возможностей в верхней панели и выбрать **«Медленные» клавиши**. Значок специальных возможностей становится виден на панели, если один или более параметров были включены в разделе **Специальные возможности**.

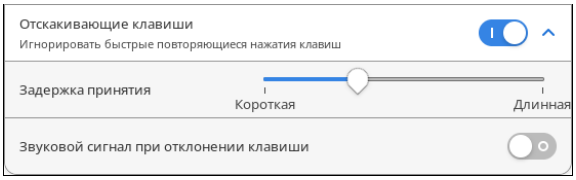
Используйте ползунок **Задержка принятия** для настройки времени, в течение которого нужно удерживать клавишу для регистрации её нажатия.

Можно сделать так, чтобы компьютер подавал звуковой сигнал при нажатии клавиши, когда нажатие принято, или если нажатие проигнорировано из-за того, что клавиша удерживалась нажатой недостаточно долго.



- **Отскакивающие клавиши**. Включите «отскакивающие клавиши», чтобы игнорировать быстро повторяющиеся нажатия. Это может быть полезно, например, если из-за дрожания рук вместо однократного нажатия клавиши пользователь нажимает её несколько раз.

Используйте ползунок **Задержка принятия**, чтобы изменить время, в течение которого «отскакивающие клавиши» ожидают регистрации повторного нажатия после нажатия клавиши в первый раз. Включите **Звуковой сигнал при отклонении клавиш**, если хотите, чтобы компьютер подавал звуковой сигнал каждый раз, когда нажатие клавиши игнорируется из-за того, что она нажата слишком рано после предыдущего её нажатия.



Наведение и нажатие

В разделе «**Наведение и нажатие**» выполняется настройка имитации поведения мыши с помощью клавиатуры.

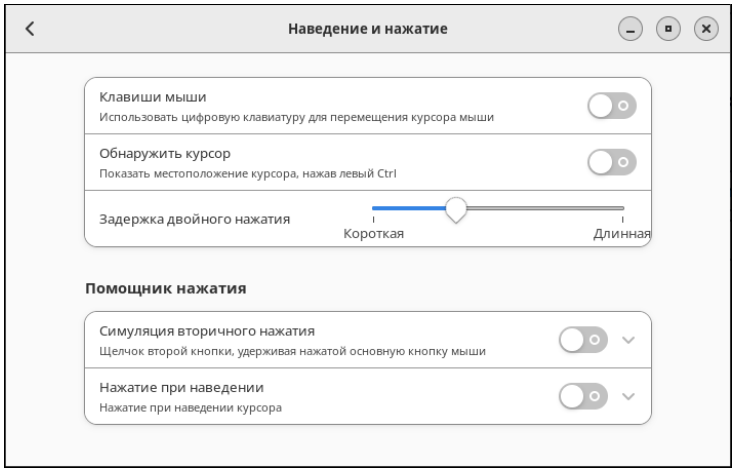
Если пользователю трудно управлять мышью или другим указывающим устройством, можно управлять указателем мыши с помощью клавиш цифрового блока клавиатуры. Для этого доступна функция «**Клавиши мыши**».

Каждая клавиша с номером в цифровом блоке соответствует направлению. Например, нажатие клавиши **8** переместит указатель вверх, а нажатие клавиши **2** — вниз. Чтобы выполнить нажатие мышью, нажмите **5**, а для двойного нажатия быстро нажмите эту же клавишу дважды.

Примечание.

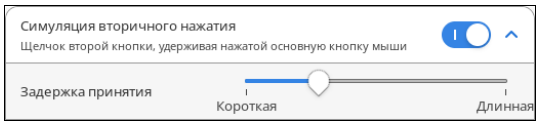
Обычные клавиши с цифрами, находящиеся в верхнем ряду клавиатуры, не могут управлять указателем мыши. Для этого можно использовать только клавиши цифрового блока.

Убедитесь, что индикатор **Num Lock** отключен. Помните, что при включённом **Num Lock** управлять указателем мыши с помощью цифрового блока клавиатуры невозможно.



Симуляция вторичного нажатия

Также можно выполнять нажатия правой кнопкой мыши, удерживая нажатой её левую кнопку. Это может быть полезно, если пользователю трудно двигать пальцами руки по отдельности, или если указывающее устройство имеет только одну кнопку. Данная функция активируется с помощью включения параметра «**Симуляция вторичного нажатия**». Дополнительно можно изменить время, в течение которого нужно удерживать нажатой левую кнопку мыши, чтобы было зарегистрировано нажатие правой кнопки.



Чтобы выполнить нажатие правой кнопкой с помощью имитации вторичного нажатия, удерживайте нажатой левую кнопку мыши там, где обычно выполняете нажатие правой кнопкой, затем отпустите её. Пока левая кнопка мыши удерживается нажатой, указатель постепенно меняет свой цвет. Как только он полностью изменит цвет, отпустите кнопку мыши, чтобы было выполнено нажатие правой кнопкой.

Нажатие при наведении

Можно выполнять нажатия или перетаскивание, просто удерживая указатель мыши над элементом интерфейса или объектом на экране. Это удобно, если пользователю трудно одновременно перемещать мышь и выполнять нажатие. Данная функция активируется с помощью включения параметра **Нажатие при наведении**.

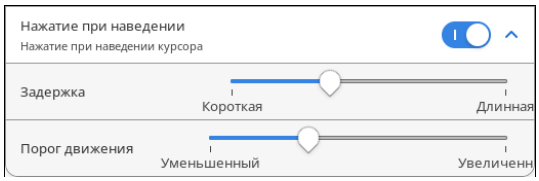
Если **Нажатие при наведении** включено, достаточно навести указатель мыши на кнопку, снять руку с мыши и затем подождать некоторое время. Нажатие кнопки будет выполнено автоматически.

Если навести указатель мыши на кнопку и держать его неподвижно, его цвет будет постепенно меняться. Когда указатель полностью сменит цвет, будет выполнено нажатие на кнопку.

Настройте параметр **Задержка**, чтобы изменить время, в течение которого нужно удерживать указатель мыши неподвижно, чтобы произошло нажатие.

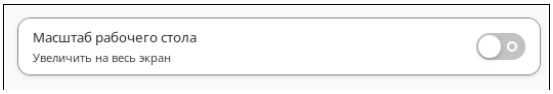
Необязательно удерживать мышь абсолютно неподвижно во время выполнения «нажатия по наведению». Нажатие будет выполнено, даже если курсор немного сместится. Однако, если он сместится слишком сильно, нажатия не произойдёт.

Настройте параметр **Порог движения**, чтобы указать, насколько может смещаться курсор, чтобы всё равно считаться неподвижным.



Масштабирование

Масштабирование — это не то же самое, что увеличение размера текста. Данная функция похожа на увеличительное стекло, которое можно перемещать по экрану и увеличивать отдельные его части.



Для активации функции масштабирования активируйте параметр «**Масштаб рабочего стола**». Теперь, перемещая мышь, можно передвигать «увеличительное стекло» в различных направлениях, чтобы рассмотреть нужную область экрана.

Примечание.

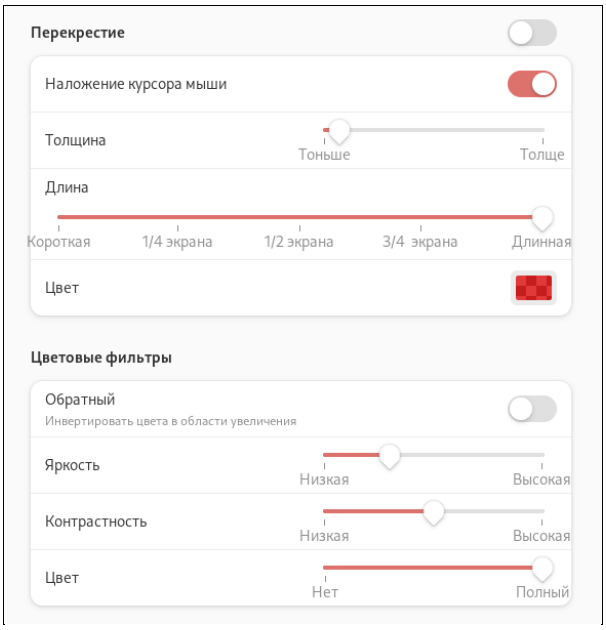
Чтобы быстро включить или отключить увеличение экрана, можно нажать на значок специальных возможностей в верхней панели и изменить положение переключателя **Масштабирование**.

Коэффициент увеличения, режим слежения за мышью и позицию увеличиваемой области на экране можно изменять. Настройте эти параметры в разделе **Увеличитель**.



Для упрощения поиска курсора мыши или сенсорной панели, можно включить **Перекрестия**. Включите функцию и настройте длину, цвет и толщину.

В разделе **Цветовые фильтры** можно инвертировать цвета области увеличения и настроить яркость, контрастность и параметры оттенков серого для увеличителя. Сочетание этих параметров требуются людям со слабым зрением, любой степенью светобоязни или просто при использовании компьютера в условиях неблагоприятного освещения.


Перекрестие
Наложение курсора мыши
Толщина
Тоньше
Толще
Длина
Короткая
1/4 экрана
1/2 экрана
3/4 экрана
Длинная
Цвет
Цветовые фильтры
Обратный
Инвертировать цвета в области увеличения
Яркость
Низкая
Высокая
Контрастность
Низкая
Высокая
Цвет
Нет
Полный

Экранный диктор

Экранный диктор Orca
Синтезатор речи RHVoice

Экранный диктор позволяет полноценно работать в системе пользователям с ограниченными возможностями по зрению путем озвучивания отдельных элементов пользовательского интерфейса.

Вы можете подробнее ознакомиться с программами специального назначения, просмотрев наши обучающие видео:

- на **RuTube** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **Яндекс.Дзен** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника;
- в **VK Видео** — Специальные возможности и вспомогательные технологии в РЕД ОС. Тифлотехника.

На наших каналах вы также сможете найти много другой полезной информации.

Экранный диктор Orca

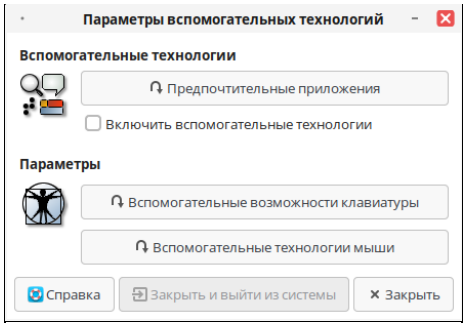
Orca в РЕД ОС является средством для чтения текста (синтезатор речи) с экрана, программа предоставляет доступ к рабочему столу для слабовидящих пользователей.

По умолчанию данная программа уже установлена в системе.

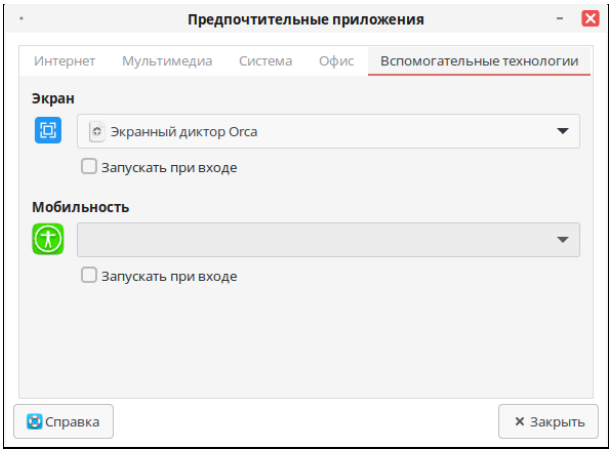
Графический режим

Для запуска экранного диктора в графическом режиме перейдите в «**Главное меню**» - «**Центр управления**» - «**Вспомогательные технологии**».

Необходимо активировать переключатель «**Включить вспомогательные технологии**» и нажать кнопку «**Предпочтительные приложения**».



В открывшемся окне можно выбрать приложение и настроить запуск программы при входе в систему.



Консольный режим

Справку по синтаксису утилиты можно увидеть через команду от *локального* пользователя:

```
orca --help
```

Использование:

```
orca [-h] [-v] [-r] [-s] [-l] [-e <параметр>] [-d <параметр>] [-p <имя>] [-u <каталог>] [--debug-file <файл>] [--debug]
```

Ключ	Описание
-h, --help	Показать данное справочное сообщение и выйти
-v, --version	Отобразить текущую версию
-r, --replace	Заменить уже работающий экземпляр экранного диктора
-s, --setup	Задать параметры пользователя (графическая версия)
-l, --list-apps	Вывести список известных запущенных приложений
-e <параметр>, --enable <параметр>	Принудительно использовать параметр
-d <параметр>, --disable <параметр>	Исключить использование параметра
-p <имя>, --profile <имя>	Загрузить профиль
-u <каталог>, --user-prefs <каталог>	Использовать другой каталог с параметрами пользователя
--debug-file <файл>	Записывать отладочные данные в указанный файл
--debug	Записывать отладочные данные в debug-<ГГГГ-ММ-ДД-ЧЧ:ММ:СС>.out

Синтезатор речи RHVoice

RHVoice — российский синтезатор речи с открытым исходным кодом, использование которого доступно на компьютере или телефоне любого пользователя с ограниченными возможностями зрения.

RHVoice использует статистический параметрический синтез. Он опирается на уже существующие речевые технологии с открытым исходным кодом (прежде всего **HTS** и связанные компоненты).

Голоса создаются на основе записей естественной человеческой речи. Они компактны, так как на компьютере пользователей хранятся только статистические модели.

Изначально **RHVoice** поддерживал только русский язык. Теперь он также поддерживает английский, бразильский португальский, эсперанто, грузинский, украинский, киргизский и татарский языки.

Для установки **RHVoice** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install RHVoice
```

Перезапустите систему:

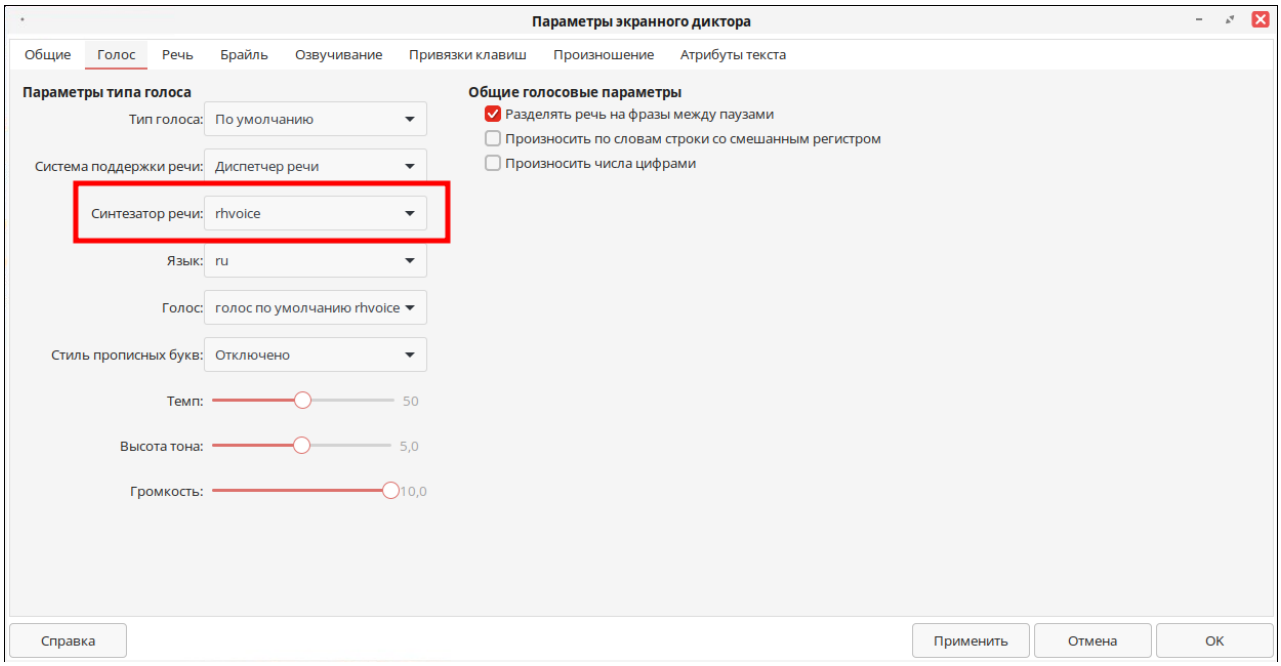
```
reboot
```

После перезапуска для настройки **RHVoice** в качестве синтезатора речи по умолчанию в терминале выполните команду (от *локального* пользователя):

```
orca -s
```

В окне параметров перейдите на вкладку «**Голос**».

В пункте «**Синтезатор речи**» выберите «**rhvoice**».

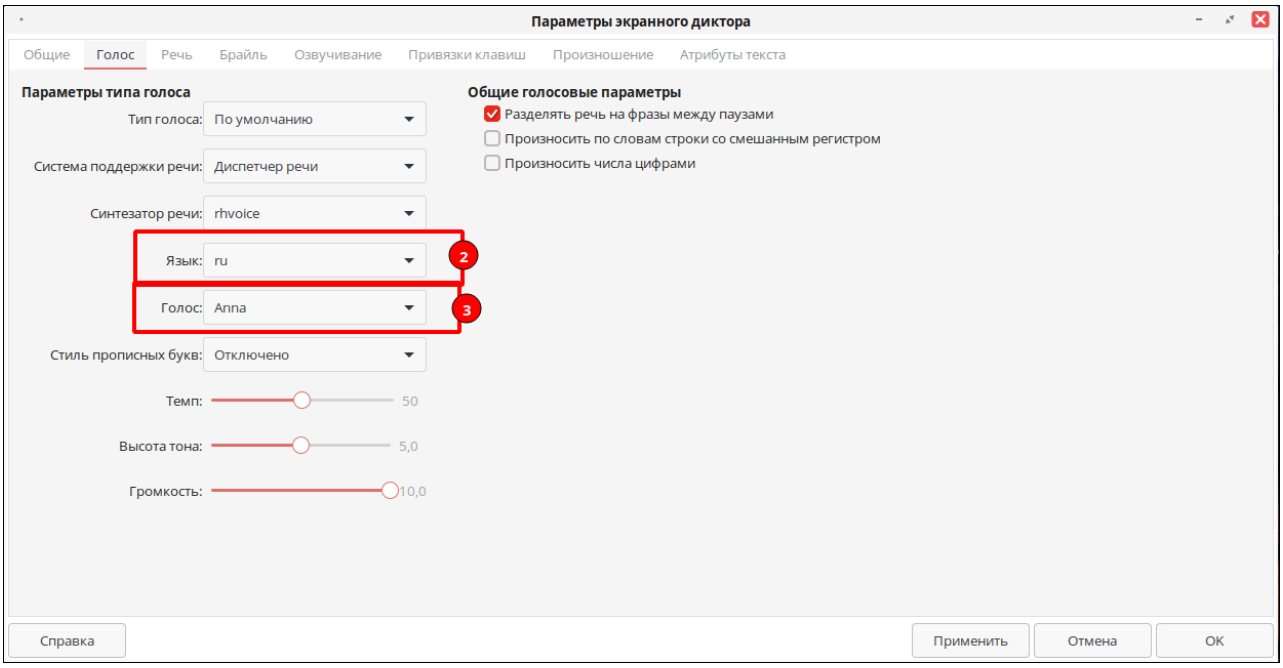


Нажмите «**OK**» и перезагрузите систему.

После перезагрузки с правами *локального* пользователя снова откройте параметры экранного диктора с помощью команды:

```
orca -s
```

На вкладке «**Голос**» в соответствующих пунктах выберите необходимый *язык* (**2**) и *голос озвучки* (**3**). Также в данном окне можно настроить все необходимые параметры для озвучки. Для применения изменений нажмите «**Применить**» и «**OK**».



Установка дополнительных шрифтов

Предварительная подготовка
Установка популярных шрифтов Windows
Установка шрифтов Bitmap Fonts для использования в терминале
Установка шрифта Inconsolata (доступно для РЕД ОС 8)
Установка шрифта Droid Sans Mono
Установка шрифта DejaVu Sans Mono
Установка сторонних шрифтов
Установка одиночного шрифта
Установка архива шрифтов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: msttcore-fonts-installer-2.6, bitmap-fonts-compat-0.3, levien-inconsolata-fonts-3.0, google-droid-sans-mono-fonts-20200215, dejavu-lgc-sans-mono-fonts-2.37

По умолчанию в РЕД ОС предустановлено несколько основных шрифтов. Однако не все шрифты, используемые в ОС Windows, доступны в РЕД ОС. Необходимые шрифты можно доустановить. В рамках данной инструкции будет рассмотрено несколько способов добавления новых шрифтов в РЕД ОС.

Предварительная подготовка

Перед установкой шрифтов ОС Windows необходимо убедиться, что в системе доступны необходимые инструменты, такие как:

- **curl** – для загрузки файлов;
- **cabextract** – для извлечения файлов шрифтов Windows;
- **xorg-x11-font-utils** – для установки, преобразования и генерации шрифтов;
- **fontconfig** – для управления и настройки доступа к шрифтам.

В РЕД ОС они установлены по умолчанию, но рекомендуется проверить и установить недостающие пакеты.

Используйте нижеприведенную команду для установки (потребуются права **администратора**):

```
sudo dnf install curl cabextract xorg-x11-font-utils fontconfig
```

Установка популярных шрифтов Windows

В состав дистрибутива РЕД ОС входит пакет `msttcore-fonts-installer`, который содержит основные шрифты Microsoft:

- Andale Mono;
- Arial;
- Arial black;
- Calabri;
- Cambria;
- Candara;
- Consolas;
- Constantia;
- Corbel;
- Comic;
- Courier New;
- Impact;
- Tahoma;
- Times New Roman;
- Trebuchet;
- Verdana;
- Webdings.

Для установки пакета *msttcore-fonts-installer* выполните команду (потребуются права **администратора**):

```
sudo dnf install msttcore-fonts-installer
```

В результате будут установлены основные *шрифты Windows*.

Установка шрифтов Bitmap Fonts для использования в терминале

Bitmap Fonts — семейство растровых шрифтов. **Bitmap Fonts** содержит шрифты, предназначенные для использования в терминале. Формат шрифта основан на группе глифов, нарисованных внутри текстовых файлов, и наборе файлов конфигурации **JSON** для установки их параметров.

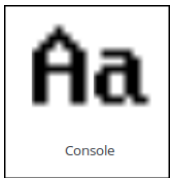
Моноширинные шрифты для использования в терминале можно установить из официального репозитория РЕД ОС с помощью пакета *bitmap-fonts-compat*.

Для добавления нового шрифта используется пакет *bitmap-fonts-compat*.

Для установки пакета *bitmap-fonts-compat* выполните команду (потребуются права **администратора**):

```
sudo dnf install bitmap-fonts-compat
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

```
sudo dnf remove bitmap-fonts-compat
```

Установка шрифта Inconsolata (доступно для РЕД ОС 8)

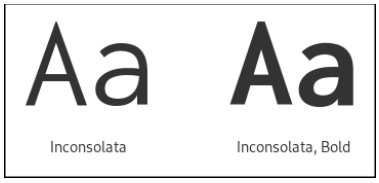
Inconsolata часто используется пользователями для работы в терминале — это четкий и легко читаемый моноширинный шрифт, разработанный Рафаэлем Левиеном. Шрифт имеет символ перечеркнутого нуля, чтобы отличить этот символ от заглавной буквы O, а также легко различимые символы для строчной буквы L и цифры 1.

Для добавления нового шрифта используется пакет *levien-inconsolata-fonts*.

Для установки пакета *levien-inconsolata-fonts* выполните команду (потребуются права **администратора**):

```
sudo dnf install levien-inconsolata-fonts
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

```
sudo dnf remove levien-inconsolata-fonts
```

Установка шрифта Droid Sans Mono

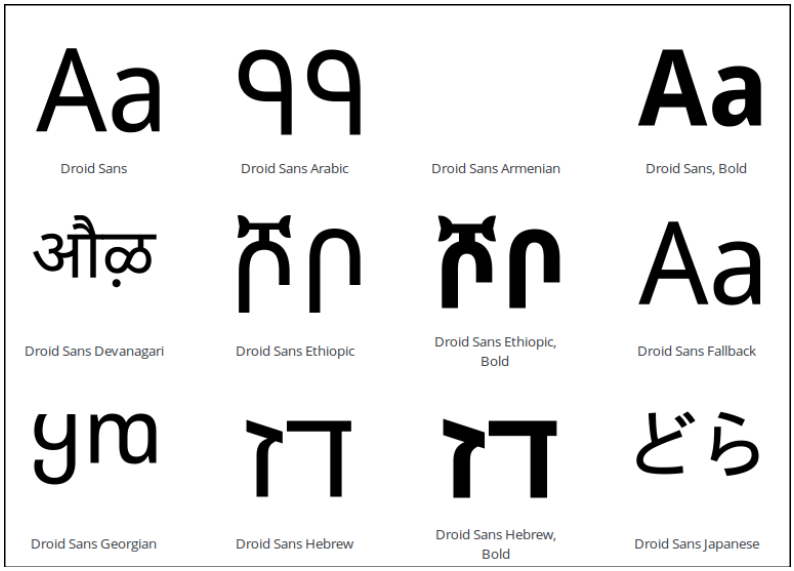
Droid Sans Mono — часть шрифтов семейства **Droid**, созданных компанией **Google**. Недостатком этого шрифта является отсутствие нуля с точками или косой чертой, из-за чего глиф нуля трудно отличить от заглавной буквы O.

Для добавления нового шрифта используется пакет *google-droid-sans-mono-fonts*.

Для установки пакета *google-droid-sans-mono-fonts* выполните команду (потребуются права **администратора**):

```
sudo dnf install google-droid-sans-mono-fonts
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

```
sudo dnf remove google-droid-sans-mono-fonts
```

Установка шрифта DejaVu Sans Mono

DejaVu Sans Mono — это шрифт, который относится к семейству шрифтов **DejaVu**. **DejaVu** — проект, целью которого является полное покрытие алфавитных сценариев, абджадов и символов всеми символами, которые являются частью подмножеств **Unicode MES-1**, **MES-2** и **MES-3**.

Для добавления нового шрифта используется пакет *dejavu-lgc-sans-mono-fonts*.

Для установки пакета *dejavu-lgc-sans-mono-fonts* выполните команду (потребуются права **администратора**):

```
sudo dnf install dejavu-lgc-sans-mono-fonts
```

После установки шрифт будет доступен к использованию.



Для удаления пакета с набором шрифтов используйте следующую команду:

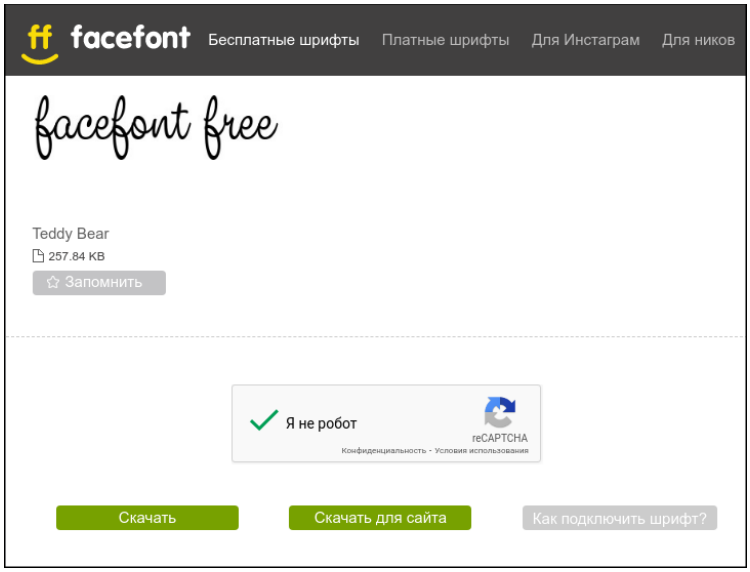
```
sudo dnf remove dejavu-lgc-sans-mono-fonts
```

Установка сторонних шрифтов

Установка одиночного шрифта

Для установки какого-либо определенного шрифта выполните следующий алгоритм действий:

1. Загрузите из сети Интернет файл нужного шрифта (в примере загружен шрифт **Teddy Bear**).



2. Скопируйте файл шрифта из каталога загрузок (в примере */home/user/Загрузки/*) в каталог хранения шрифтов */usr/share/fonts*:

```
cp /home/user/Загрузки/teddy-bear.ttf /usr/share/fonts
```

После этого новый шрифт будет доступен к использованию.



Установка архива шрифтов

Для установки какого-либо набора шрифтов выполните следующий алгоритм действий:

1. Загрузите из сети Интернет архив нужного шрифта (в примере с официального сайта **JetBrains** скачан архив шрифтов **JetBrains Mono**).

2. Перейдите в терминал и выполните команду для перехода в каталог с загруженными шрифтами (в примере */home/user/Загрузки/*):

```
cd /home/user/Загрузки/
```

3. Убедитесь, что установлен пакет для работы с архивами **unzip** (потребуются права **администратора**):

```
sudo dnf install unzip
```

4. Распакуйте архив с загруженными шрифтами с помощью команды:

```
unzip ./JetBrainsMono-2.304.zip
```

5. Скопируйте каталог шрифтов в каталог хранения шрифтов */usr/share/fonts/* (потребуются права **администратора**):

```
sudo cp -r ./fonts /usr/share/fonts/
```



Установка прочих шрифтов в РЕД ОС аналогична вариантам, приведенным выше.

Настройка внешнего вида графического окружения MATE в РЕД ОС 8

Настройка темы графической оболочки MATE
Установка темы через менеджер пакетов dnfdragora
Установка темы через терминал
Установка дополнительных тем
Создание собственных тем
Установка новых курсоров мыши
Установка новых тем значков (иконок)
Установка нового фона рабочего стола
Удаление параметра темы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с настройкой внешнего вида графического окружения **MATE**, просмотрев наши обучающие видео:

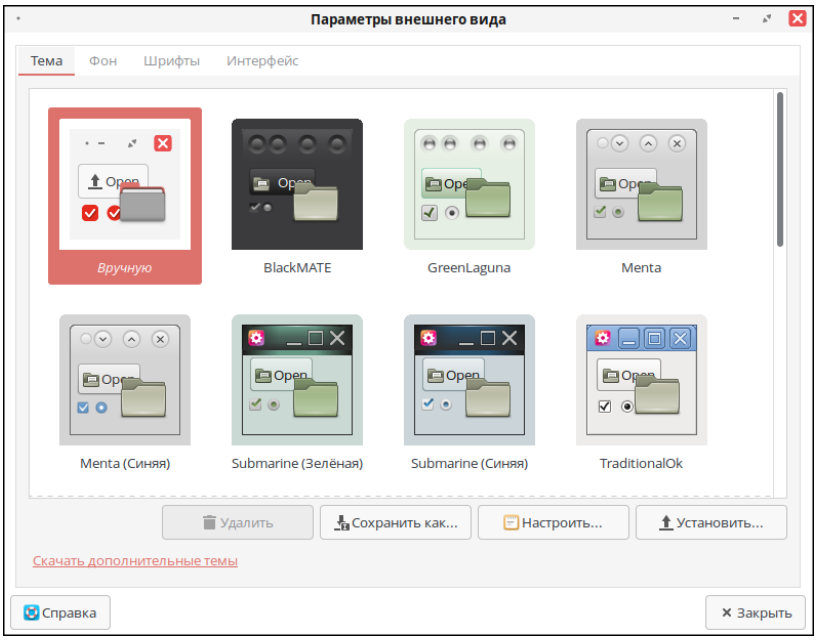
- на **RuTube** — Настройка внешнего вида графического окружения MATE в РЕД ОС 8;
- в **Яндекс.Дзен** — Настройка внешнего вида графического окружения MATE в РЕД ОС 8;
- в **VK Видео** — Настройка внешнего вида графического окружения MATE в РЕД ОС 8.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка темы графической оболочки MATE

Тема — это группа параметров, влияющих на визуальное представление частей рабочего стола. Тема влияет на различные параметры: элементы управления, цвета, рамку окна, значки, указатели.

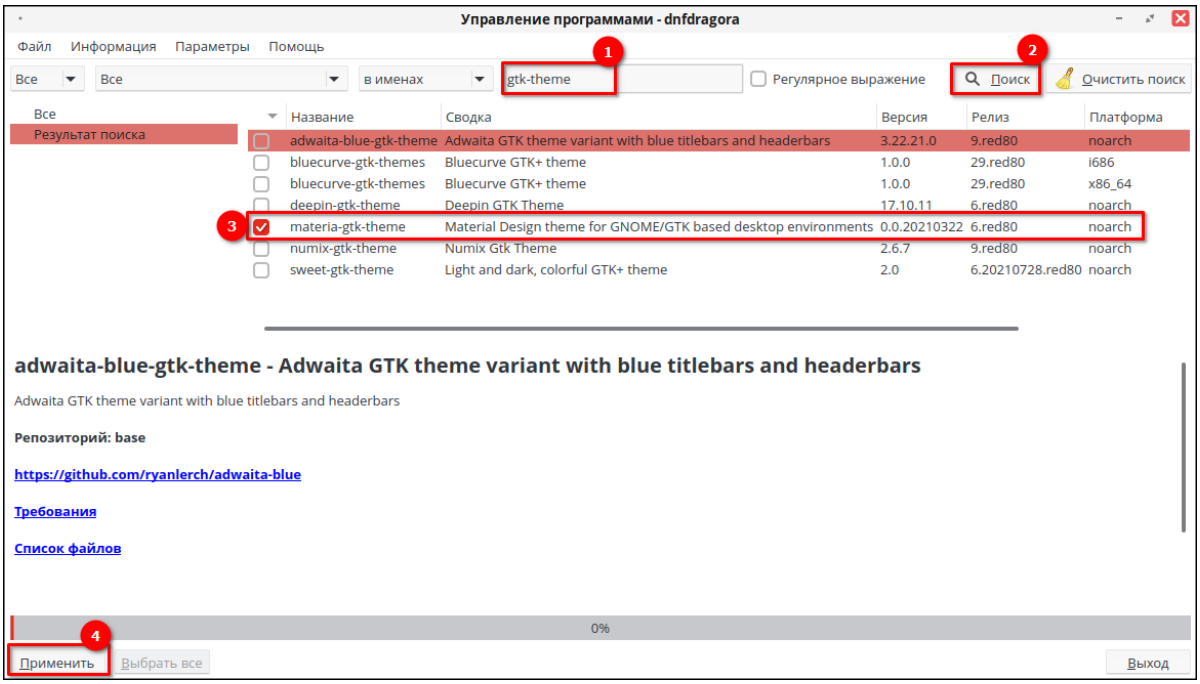
Для смены внешнего вида графической оболочки MATE в РЕД ОС необходимо вызвать контекстное меню, нажав ПКМ по свободной области рабочего стола, и выбрать пункт меню «**Параметры внешнего вида**», а затем вкладку «**Тема**».



Здесь можно обратиться к коллекции доступных встроенных тем. Для установки понравившейся темы щелкните по ней ЛКМ. Оформление темы будет применено автоматически.

Установка темы через менеджер пакетов dnfdragora

Для установки темы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову (например, «**gtk-theme**») и отметьте флагом нужный пакет. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Установка темы через терминал

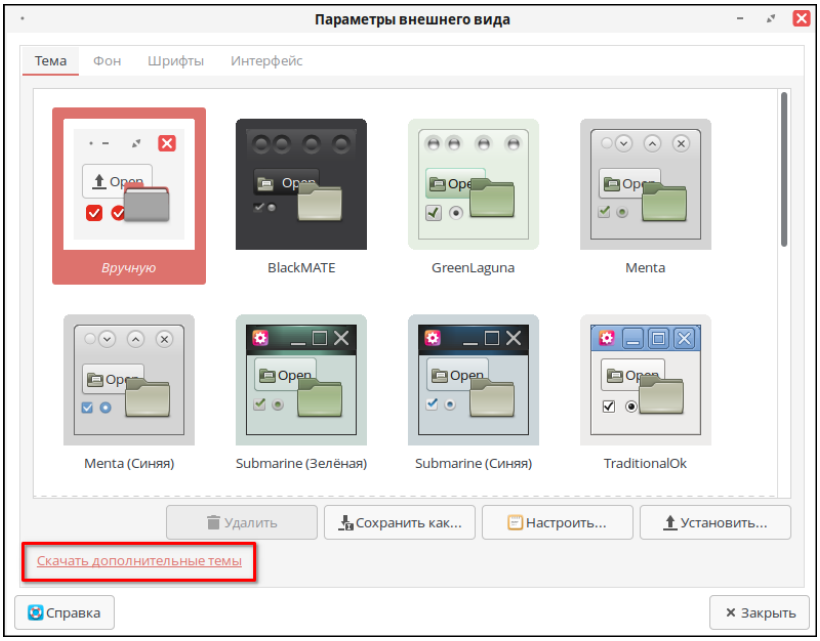
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install material-gtk-theme
```

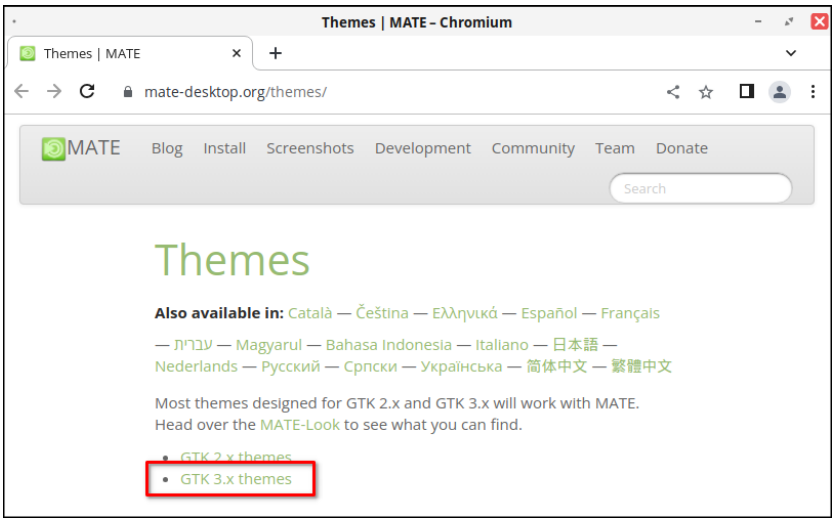
Установка дополнительных тем

Для установки сторонней темы и добавления ее в список доступных выполните следующий алгоритм действий:

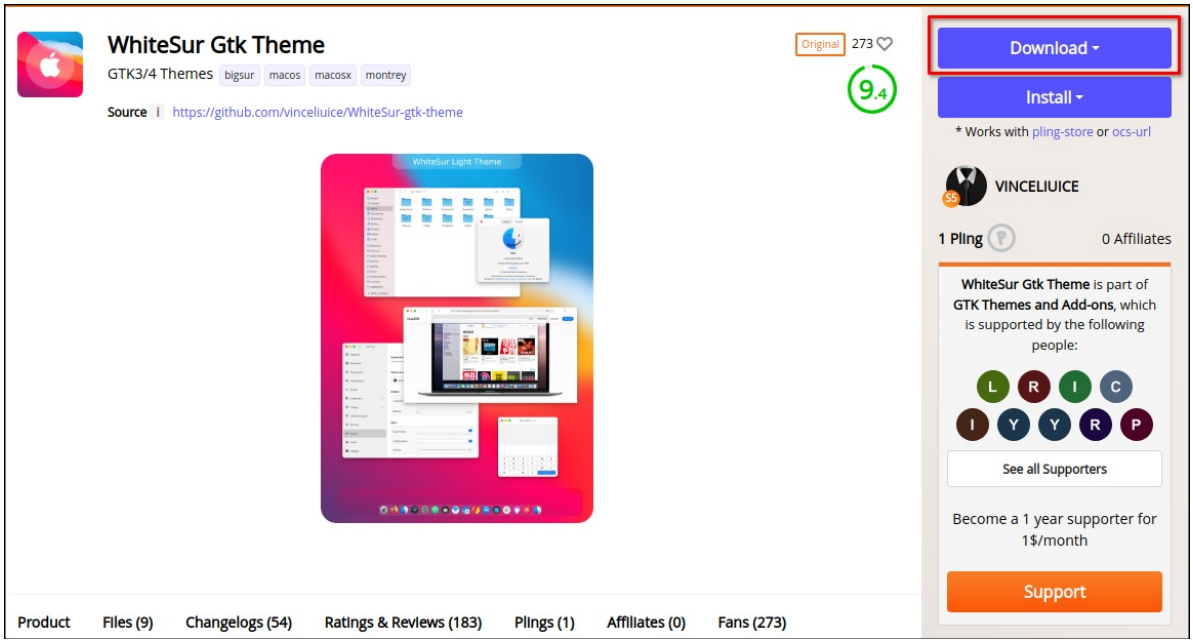
1. В «**Параметрах внешнего вида**» на вкладке темы нажмите «**Скачать дополнительные темы**».



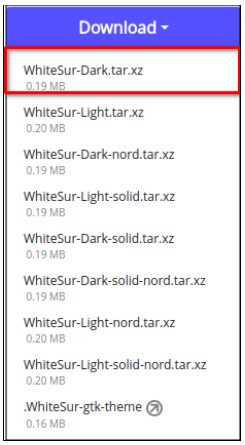
2. Будет выполнено автоматическое перенаправление на страницу с темами. На загруженной странице выберите «**GTK 3.x themes**».



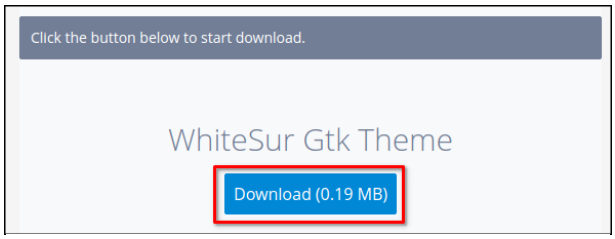
3. Выберите из списка понравившуюся тему и нажмите на нее. Будет открыто подробное описание темы. Для загрузки нажмите «**Download**».



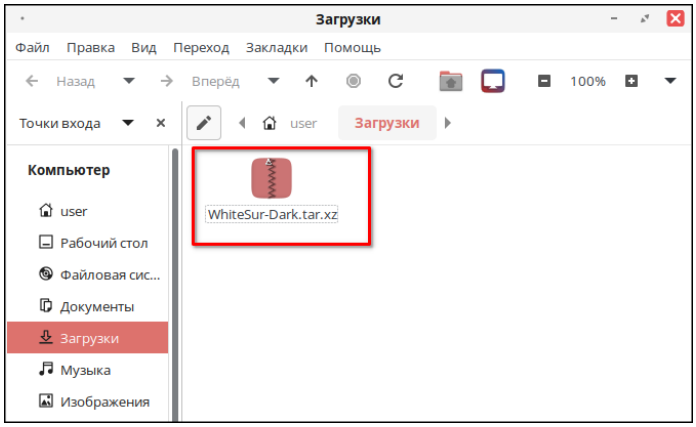
4. По нажатии на кнопку «**Download**» будет открыт список с доступным цветовым оформлением. Выберите любое цветовое оформление.



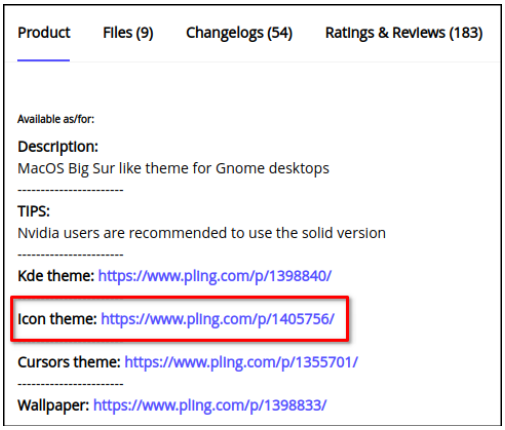
5. Начнется подготовка архива к скачиванию. Когда архив станет доступен для скачивания, нажмите на активную кнопку «**Download**».



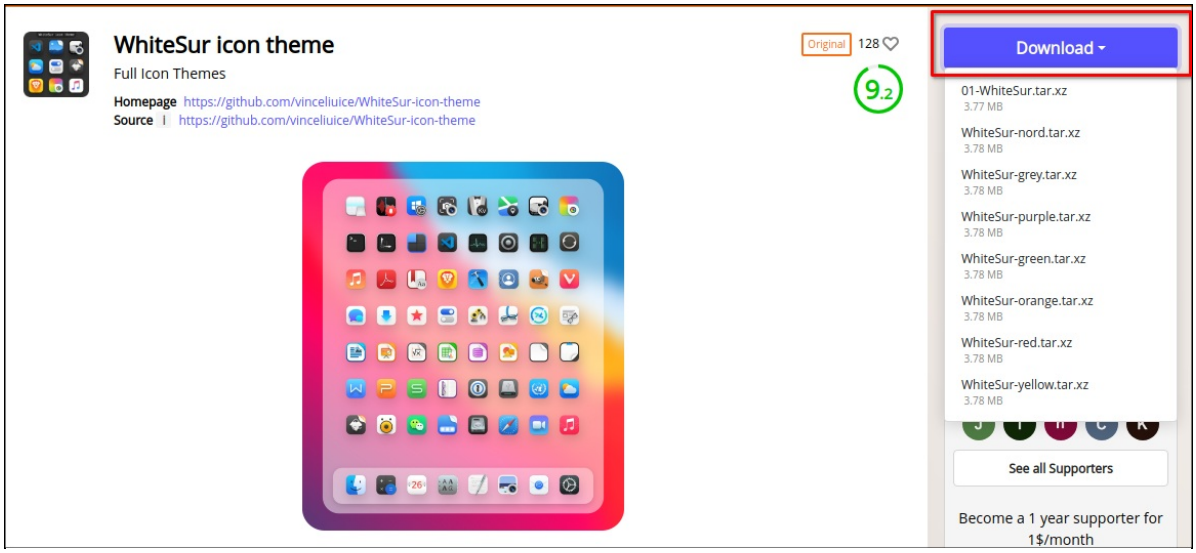
6. Архив будет сохранен в каталог загрузок (в примере /home/user/Загрузки).



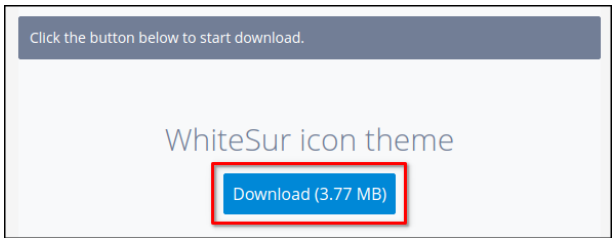
7. Далее необходимо дополнительно скачать оформление иконок для выбранной темы. Для этого пролистайте вниз до ссылки на иконки и перейдите по указанной ссылке.



8. Для скачивания набора иконок нажмите кнопку «**Download**» и выберите цветовое оформление из списка.



9. Дождитесь подготовки архива и нажмите на кнопку «**Download**».



10. Перейдите в терминал и выполните команду для перехода в каталог с загруженными архивами тем (в примере /home/user/Загрузки/):

```
cd /home/user/Загрузки/
```

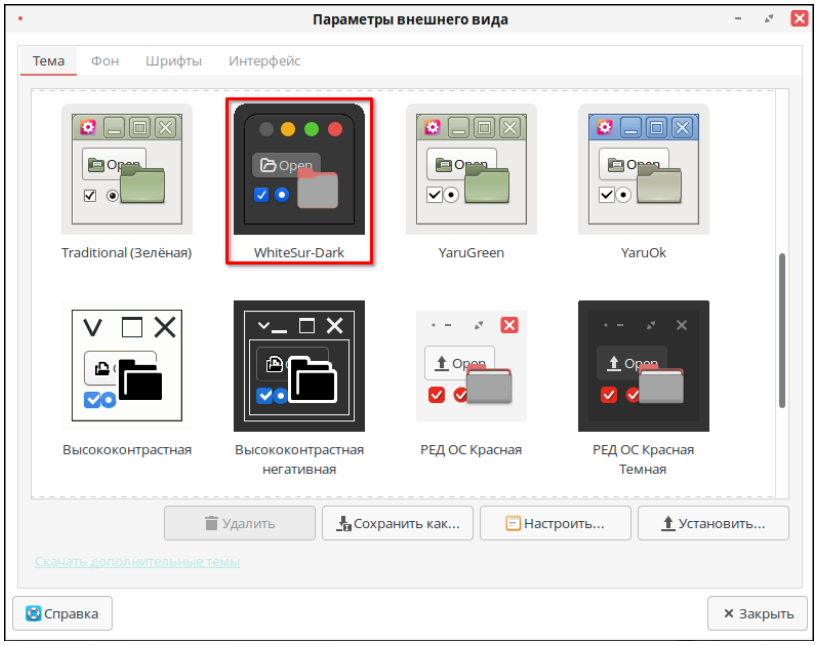
Распакуйте архив с основной темой с помощью команды:

```
tar -xvf ./WhiteSur-Dark.tar.xz
```

Скопируйте распакованный каталог темы в /usr/share/themes/ (потребуются права **администратора**):

```
sudo cp -r ./WhiteSur-Dark /usr/share/themes/
```

11. Закройте терминал и перейдите в «**Параметры внешнего вида**» — «**Тема**».



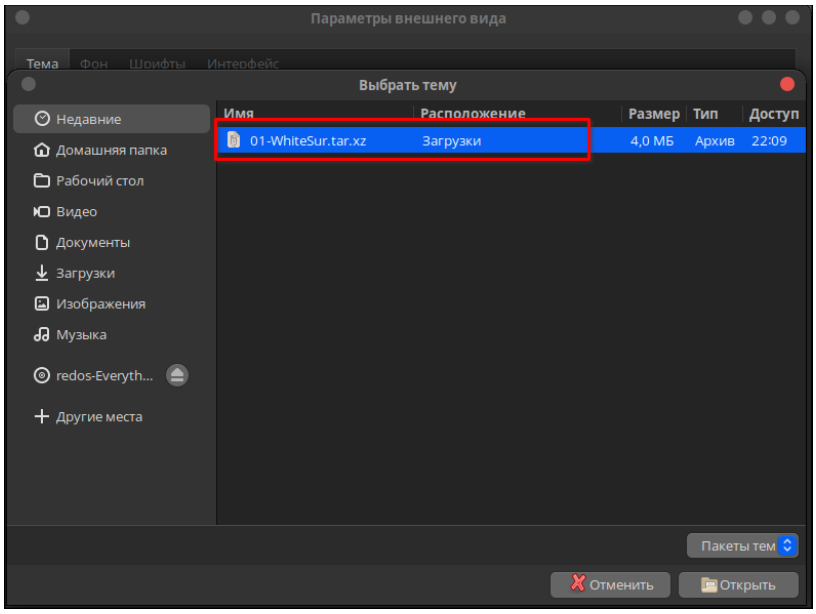
12. При выборе загруженной темы появится уведомление вида: «*Эта тема не будет выглядеть так, как задумано, потому что требуемая тема значков <название_темы> не установлена*».



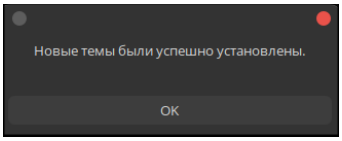
13. Для установки требуемой темы значков нажмите «**Установить...**».

---

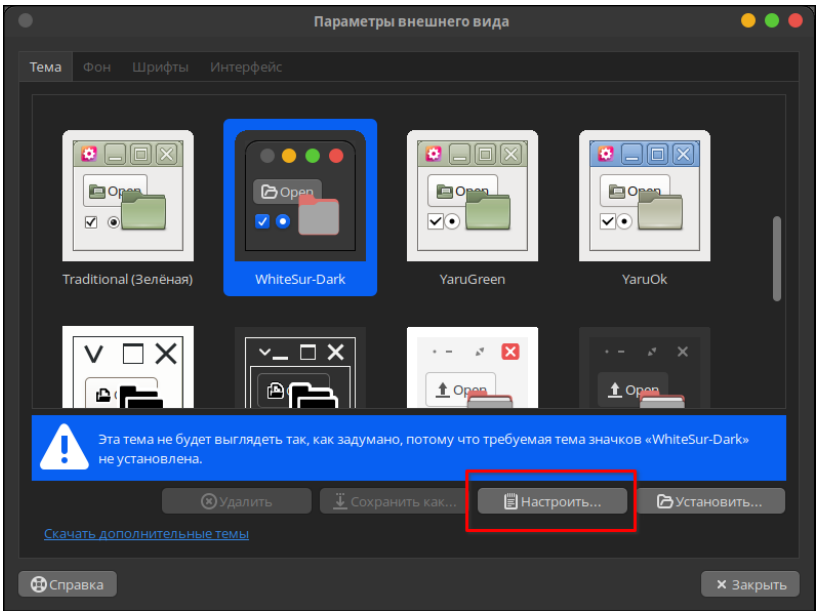
14. В открывшемся диалоговом окне двойным щелчком ЛКМ выберите тему оформления значков.



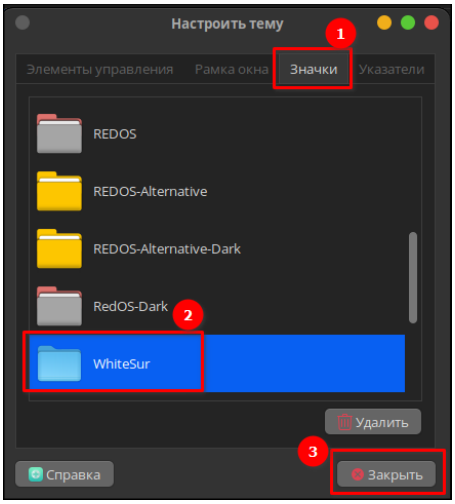
15. Появится сообщение о том, что темы были успешно установлены. Нажмите «**OK**».



16. Далее нажмите «**Настроить...**» и перейдите на вкладку «**Значки**».



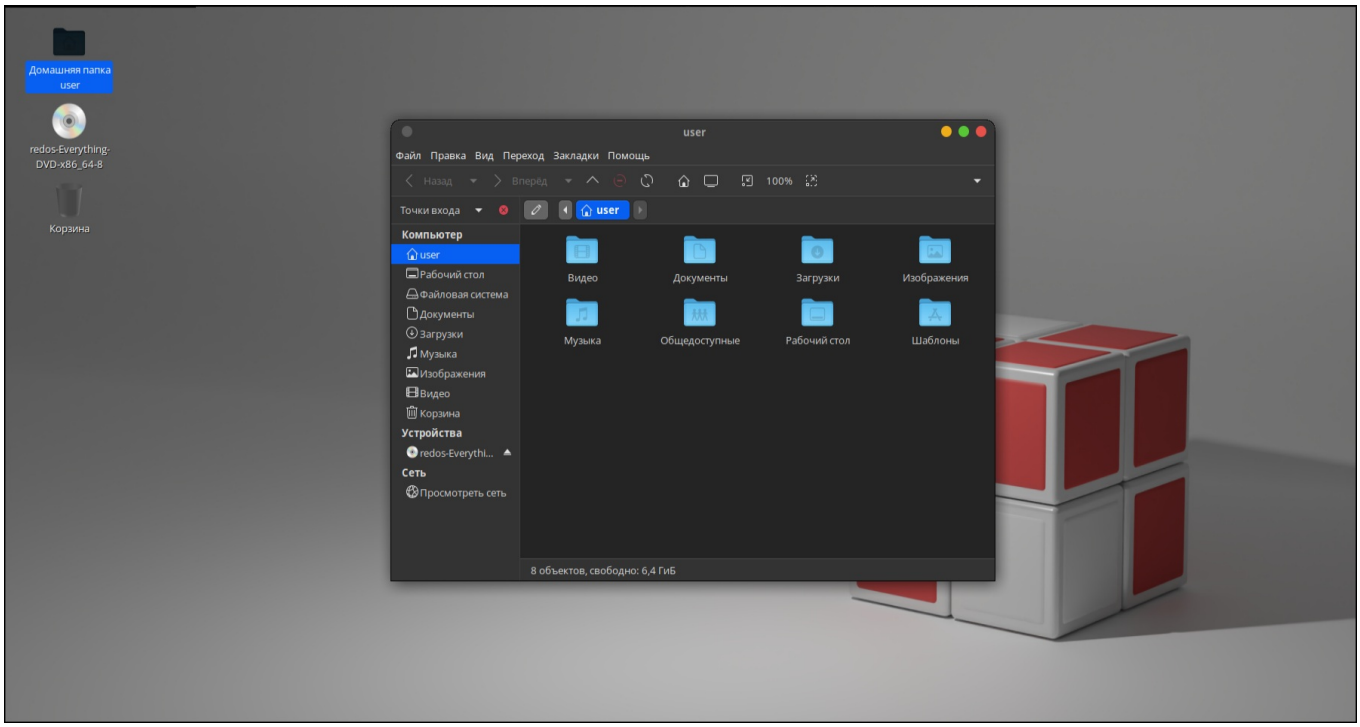
17. Выберите значки установленной темы (в примере **WhiteSur**) и нажмите «**Закрыть**».



18. Закройте диалоговое окно «**Параметры внешнего вида**».



Новая тема будет успешно применена к системе.



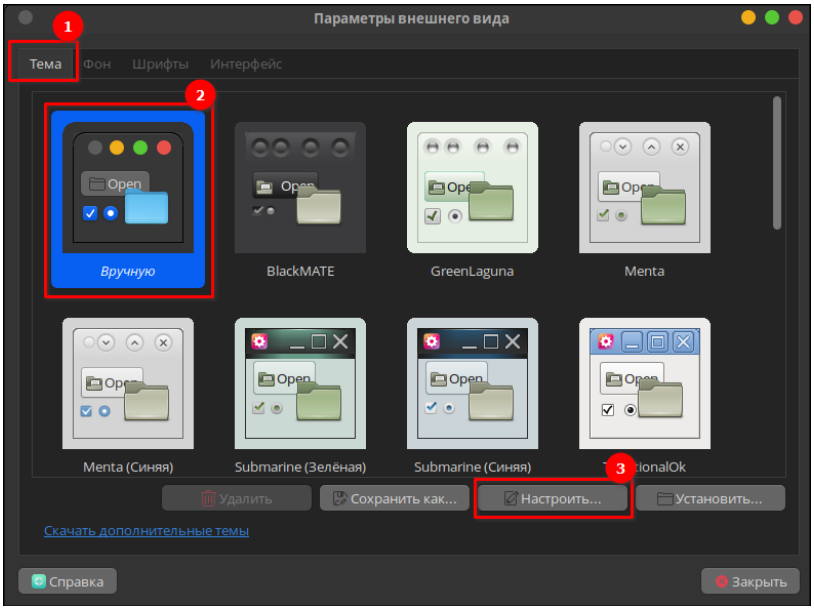
Создание собственных тем

Темы представляют собой различные комбинации параметров элементов управления. Вы можете создать собственную тему, в которой будет использоваться другая комбинация параметров элементов управления.

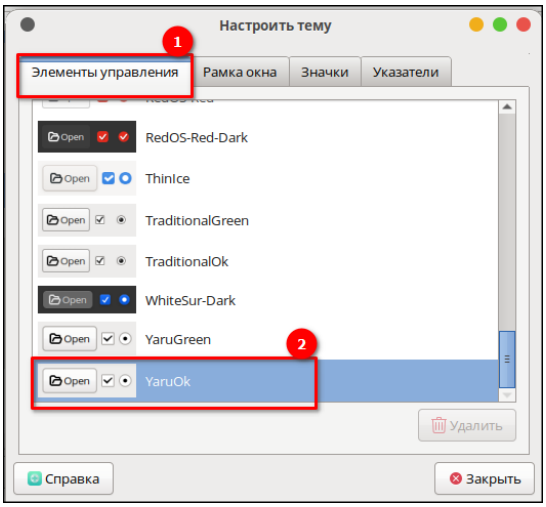
Для создания собственной темы выполните следующие действия:

1. Запустите инструмент «**Внешний вид**». Откройте вкладку «**Тема**» (1).

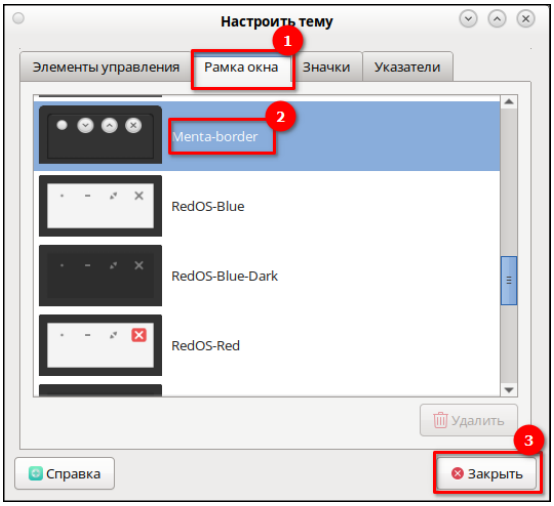
2. Выберите тему из списка (2) и нажмите кнопку «**Настроить**» (3).



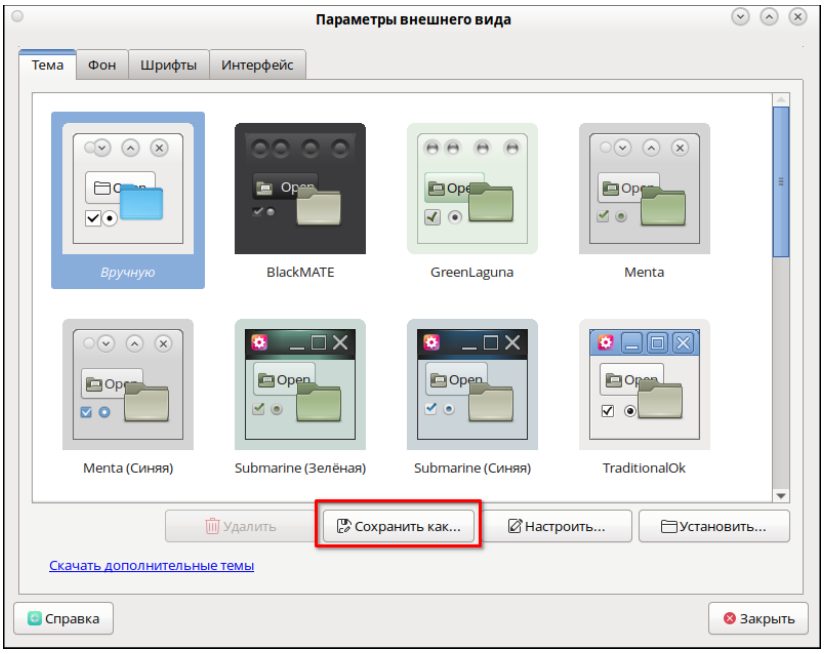
3. В появившемся диалоговом окне на вкладке «**Элементы управления**» (1) выберите параметр элементов управления (2), который необходимо использовать в теме.



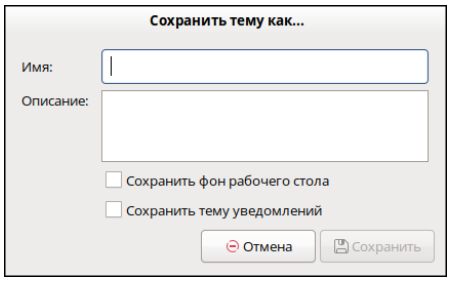
4. Щелкните по вкладке «**Рамка окна**» (1), выберите параметры рамки окна (2), который следует использовать в вашей собственной теме. Нажмите закрыть (3).



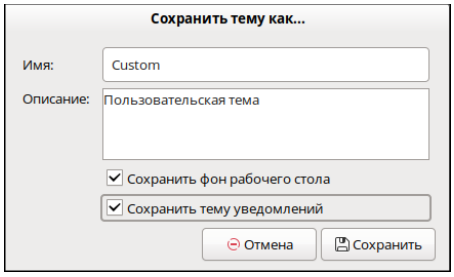
5. В инструменте настройки «**Внешний вид**» нажмите кнопку «**Сохранить как...**».



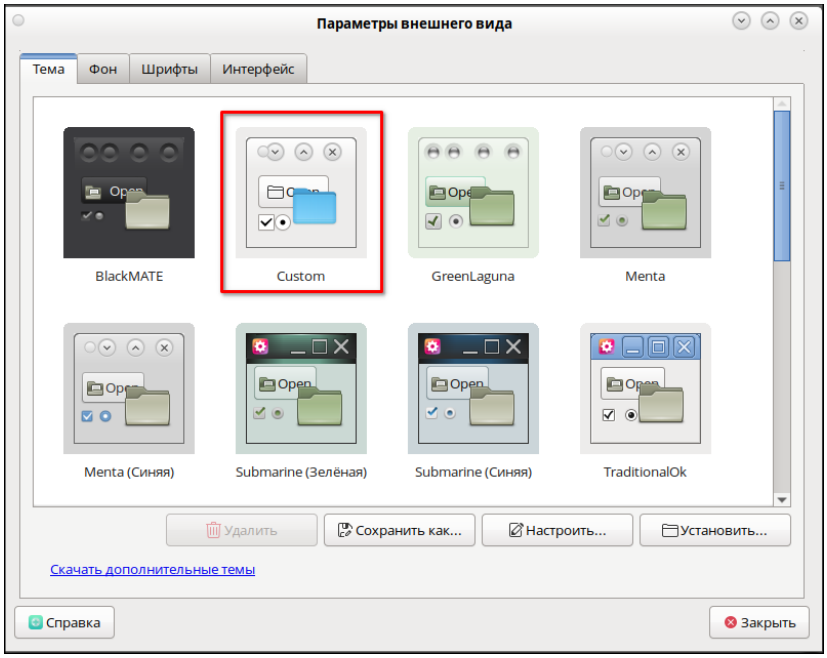
Появится диалоговое окно «**Сохранить тему как...**».



6. Введите в диалоговом окне название и краткое описание собственной темы, затем нажмите кнопку «**Сохранить**».



Тема появится в списке доступных тем.



Установка новых курсоров мыши

Для добавления новых курсоров (указателей мыши) можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**,

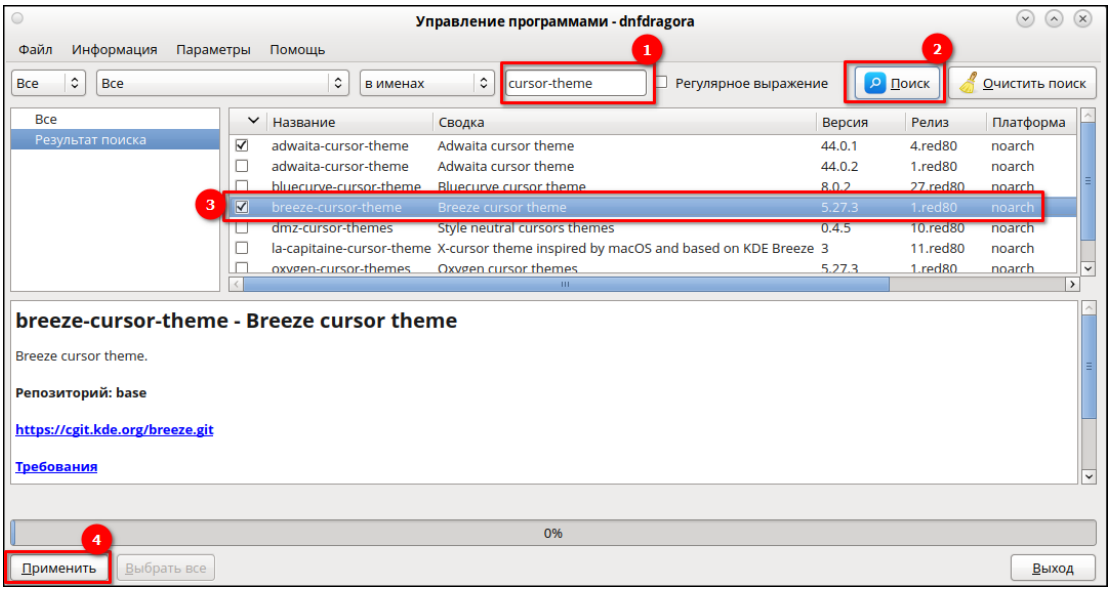
Для поиска новых курсоров через терминал выполните команду:

```
dnf search *-cursor-theme
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы курсора (потребуются права **администратора**), например:

```
dnf install breeze-cursor-theme
```

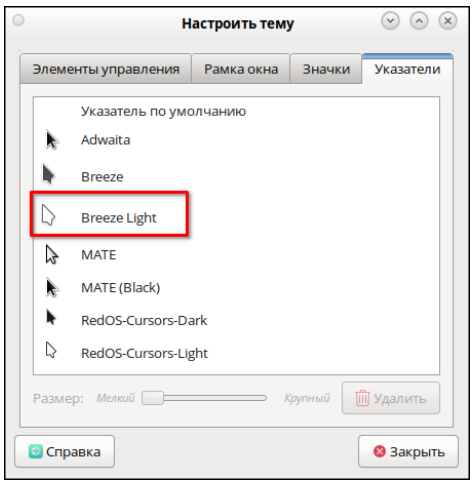
Для установки новой темы оформления указателя мыши через менеджер пакетов **dnfdragora** по шаблону — «**cursor-theme**» (1) выполните поиск темы (2), отметьте флагом необходимую тему (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



Для применения новой темы оформления курсора мыши перейдите в «**Параметры внешнего вида**» — «**Тема**» — «**Настроить**» — «**Указатели**».

Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.



Установка новых тем значков (иконок)

Для добавления новых значков (иконок) рабочего стола можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов dnfdragora.

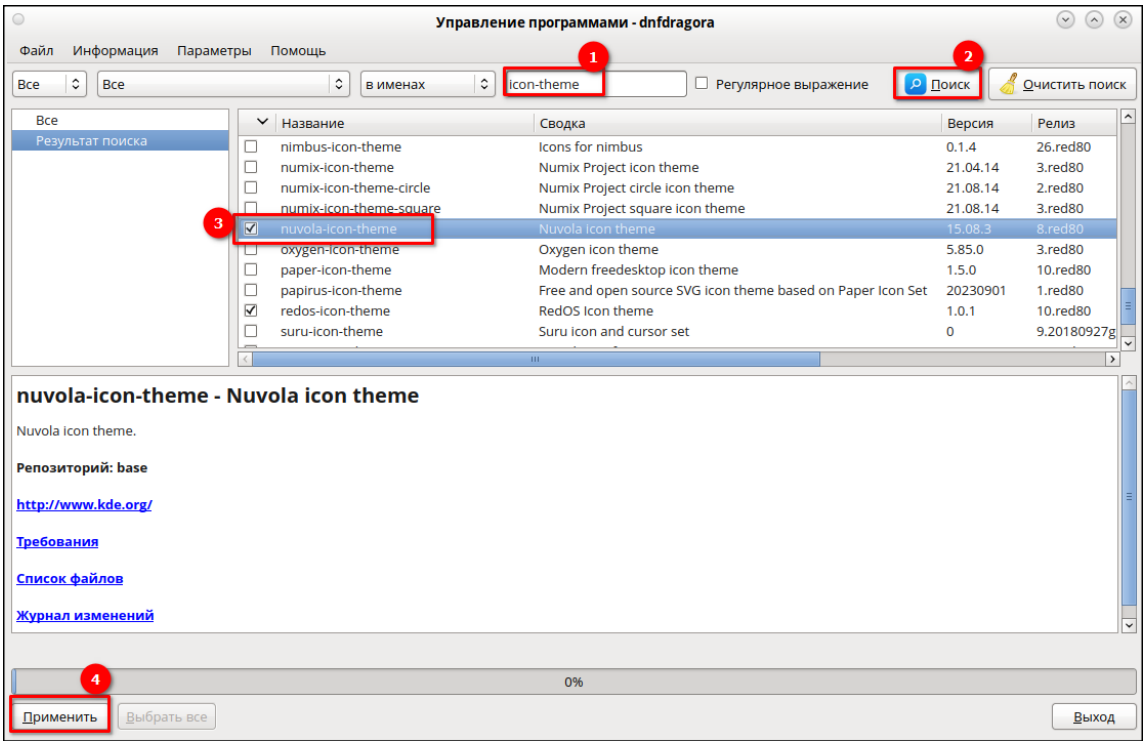
Для поиска новых тем значков через терминал выполните команду:

```
dnf search icon-theme
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы значков (потребуются права **администратора**), например:

```
dnf install nuvola-icon-theme
```

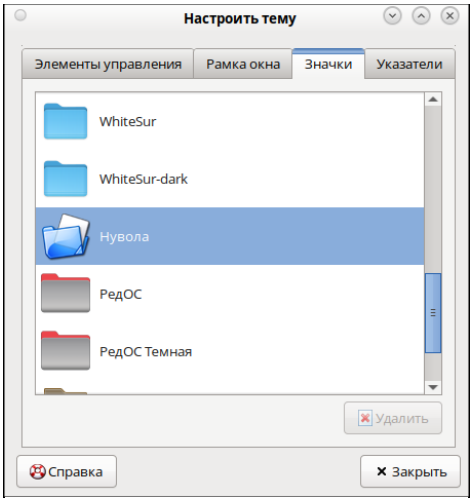
Для установки новой темы оформления значков рабочего стола через менеджер пакетов dnfdragora выполните поиск темы по шаблону — «**icon-theme**», выберите из списка актуальную версию пакета и нажмите кнопку « **Применить**».



Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

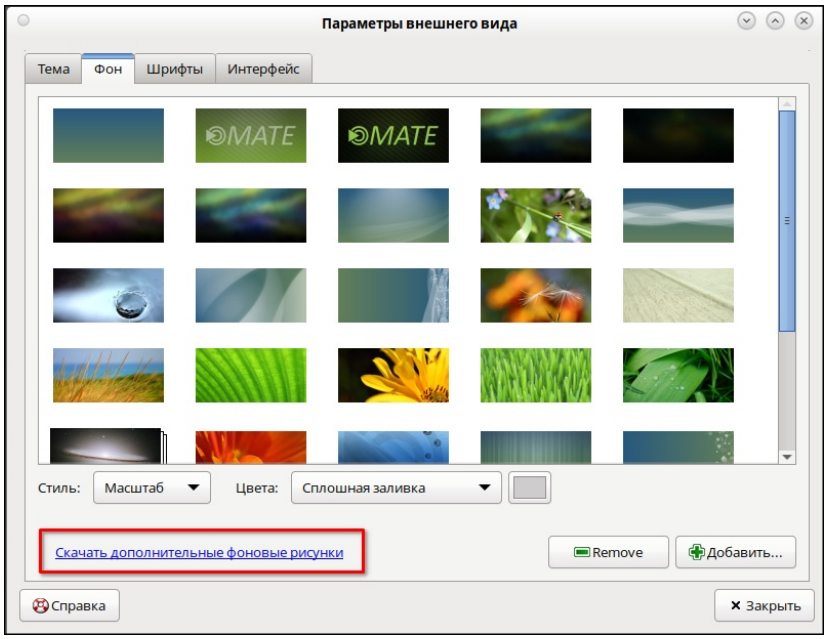
Для применения новой темы оформления значков рабочего стола перейдите в «**Параметры внешнего вида**» — «**Тема**» — «**Настроить**» — «**Значки**».



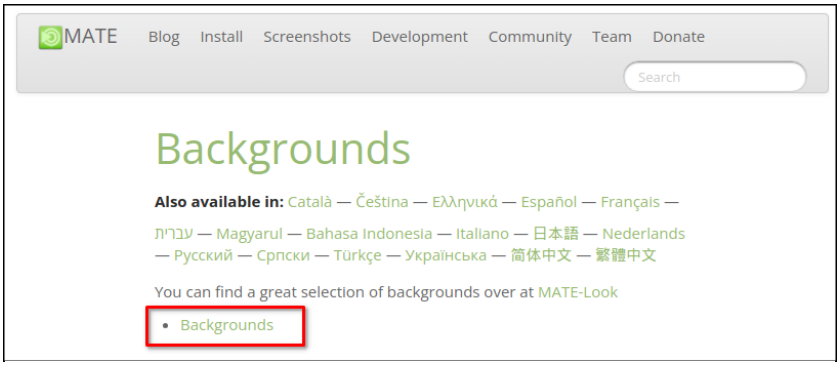
Установка нового фона рабочего стола

Для смены фона рабочего стола пользователю необходимо в системной панели выбрать пункт «**Главное меню**» — «**Параметры**» — «**Внешний вид**».

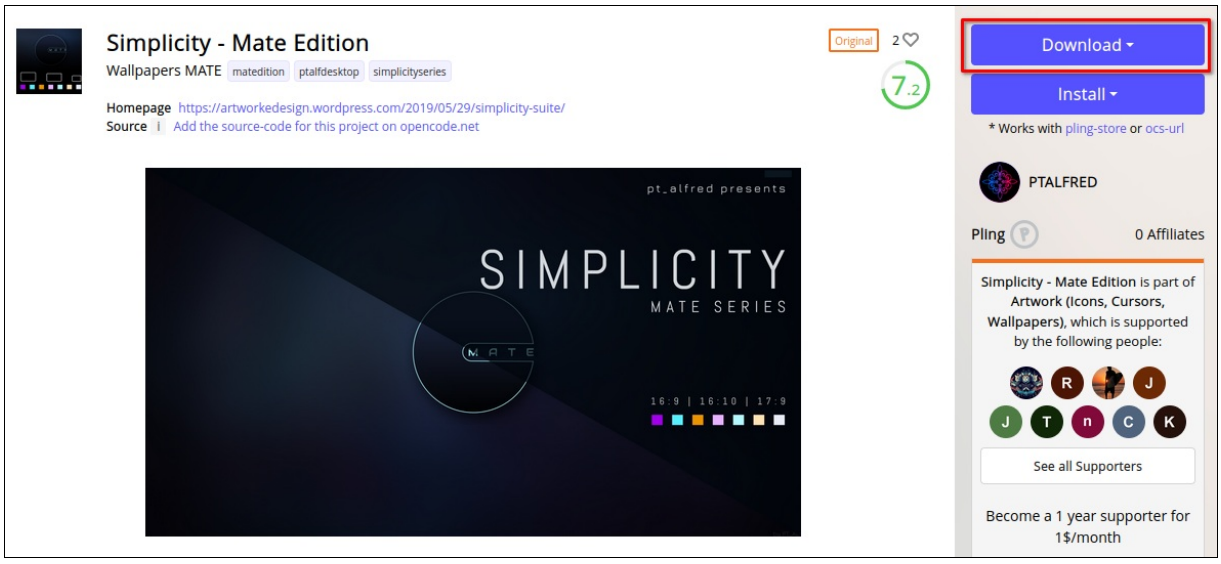
На вкладке «**Фон**» можно выбрать доступное изображение или добавить собственное, нажав кнопку «**Скачать дополнительные фоновые рисунки**».



Будет выполнено автоматическое перенаправление на страницу с изображениями рабочего стола. На загруженной странице выберите «**Backgrounds**».



Выберите из списка понравившееся изображение и нажмите на него. Будет открыто подробное описание изображения. Для загрузки нажмите «**Download**».

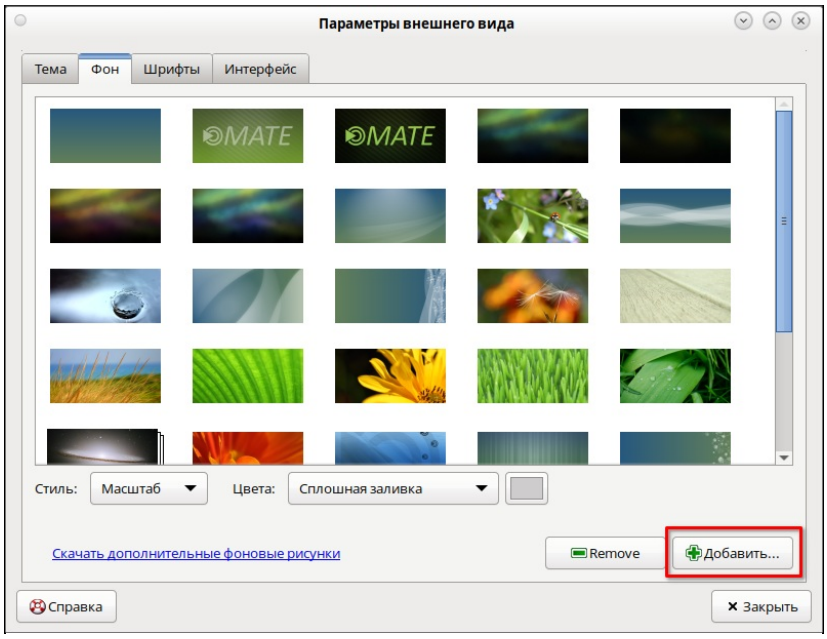


По нажатии на кнопку «**Download**» будет открыт список с доступными форматами изображения.

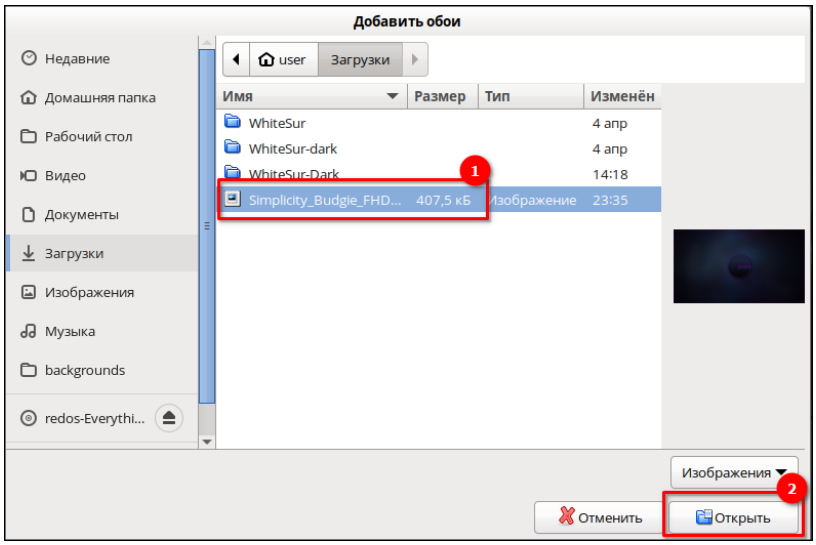
Начнется подготовка файла к скачиванию. Когда файл станет доступен для скачивания, нажмите на активную кнопку «**Download**».



Далее перейдите в «**Параметры внешнего вида**» и нажмите на кнопку «**Добавить**».



Выберите загруженное изображение для фона рабочего стола (1). Нажмите на кнопку «Открыть» (2).



Выбранное изображение автоматически будет установлено в качестве фона рабочего стола.

Удаление параметра темы

Можно удалять параметры элементов управления, рамок окна и значков. Для удаления какого-либо параметра выполните следующие действия:

1. Запустите инструмент «**Внешний вид**» — «**Тема**».

2. Нажмите «**Настроить**». Отобразится диалоговое окно «**Настроить тему**».

3. Щелкните по вкладке с параметром, который необходимо удалить и выберите параметр для удаления.

4. Нажмите кнопку «**Удалить**». Выбранный параметр будет удален.

Настройка внешнего вида графического окружения KDE Plasma

Настройка темы графической оболочки KDE Plasma
Установка темы через менеджер пакетов dnfdragora
Установка темы через терминал
Настройка новой темы
Настройка внешнего вида графического интерфейса РЕД ОС
Установка дополнительных тем
Установка новых курсоров мыши
Установка дополнительных курсоров мыши
Установка новых тем значков (иконок)
Установка нового фона рабочего стола

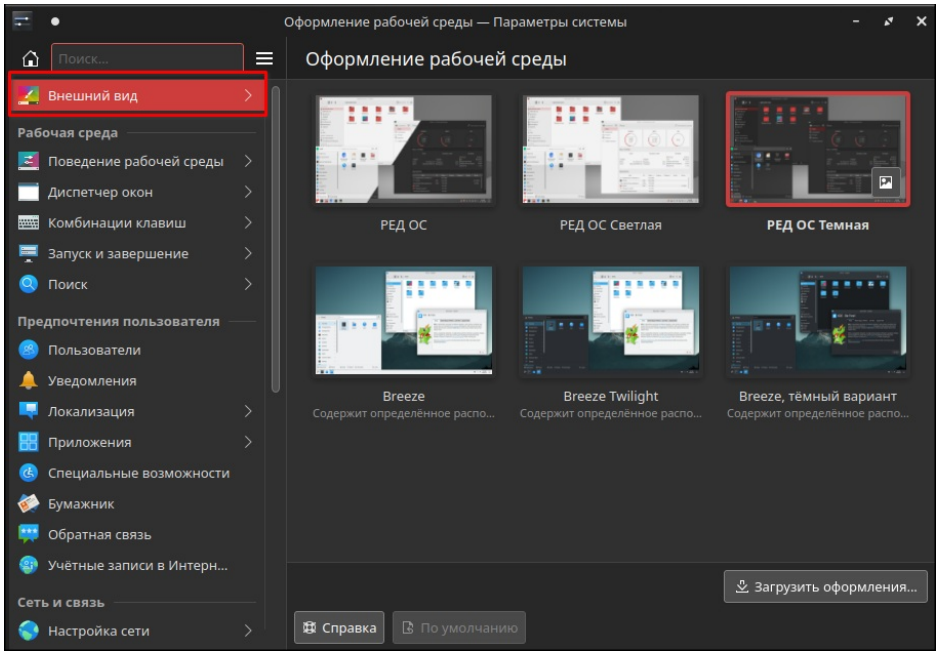
Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

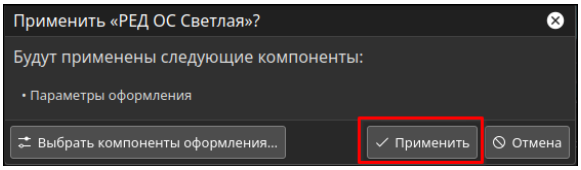
Настройка темы графической оболочки KDE Plasma

Тема — это группа параметров, влияющих на визуальное представление частей рабочего стола. Тема влияет на различные параметры: элементы управления, цвета, рамку окна, значки, указатели.

Настройка внешнего вида графической оболочки KDE Plasma производится из «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» в подразделе «**Внешний вид**».

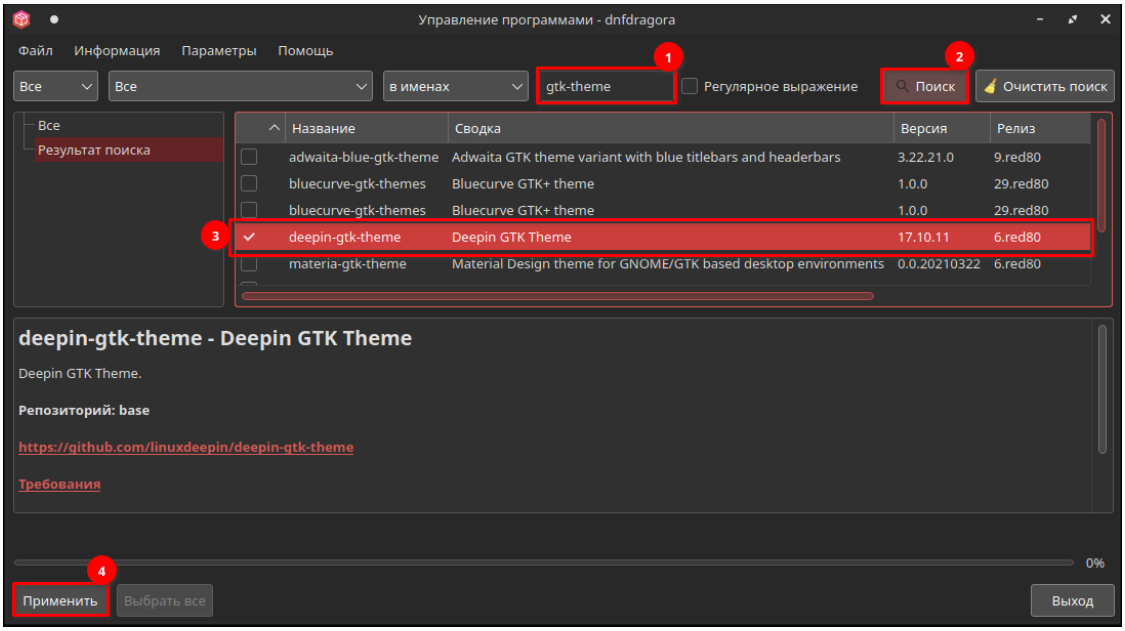


Здесь можно обратиться к коллекции доступных встроенных тем. Для установки понравившейся темы щелкните по ней ЛКМ. В открывшемся окне есть возможность выбора компонентов оформления, можно отключить/включить параметры оформления: цвета, оформление приложений, оформление окон, значки, оформление рабочего стола, курсоры мыши, заставку. Если выбирать компоненты оформления нет необходимости, нажмите «**Применить**».



Установка темы через менеджер пакетов dnfdragora

Для установки темы через графический менеджер пакетов dnfdragora перейдите в «**Меню запуска приложений**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову (например, «**gtk-theme**») и отметьте флагом нужный пакет. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



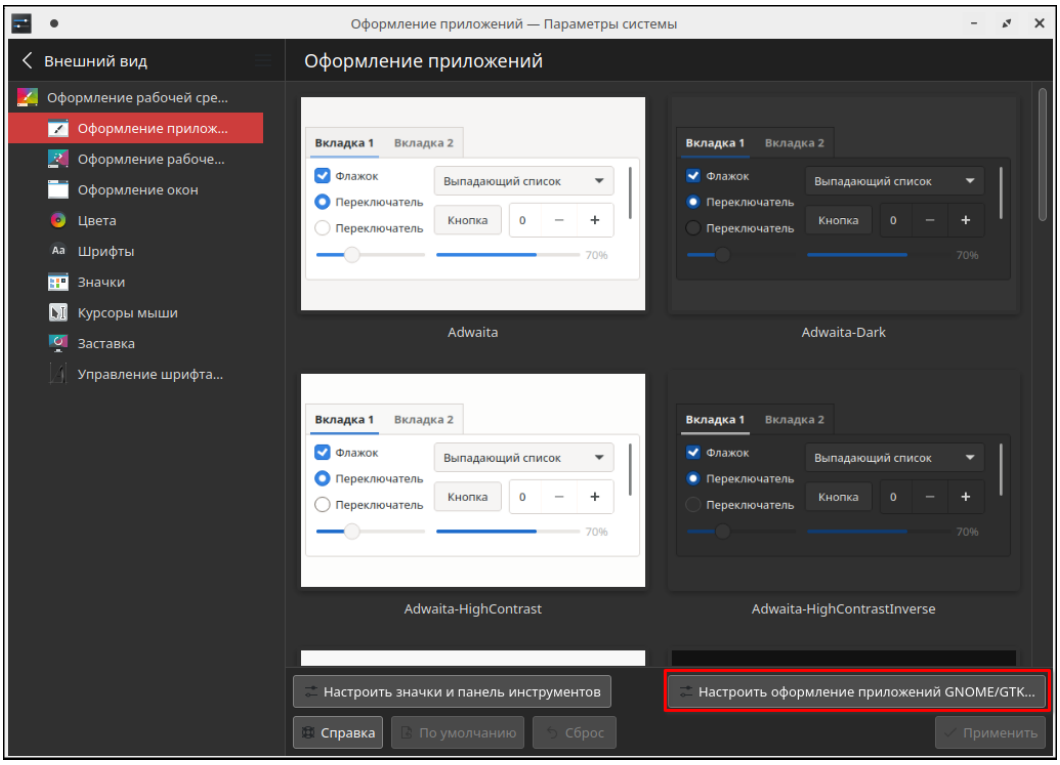
Установка темы через терминал

Для установки программы через терминал выполните команду (потребуются права **администратора**):

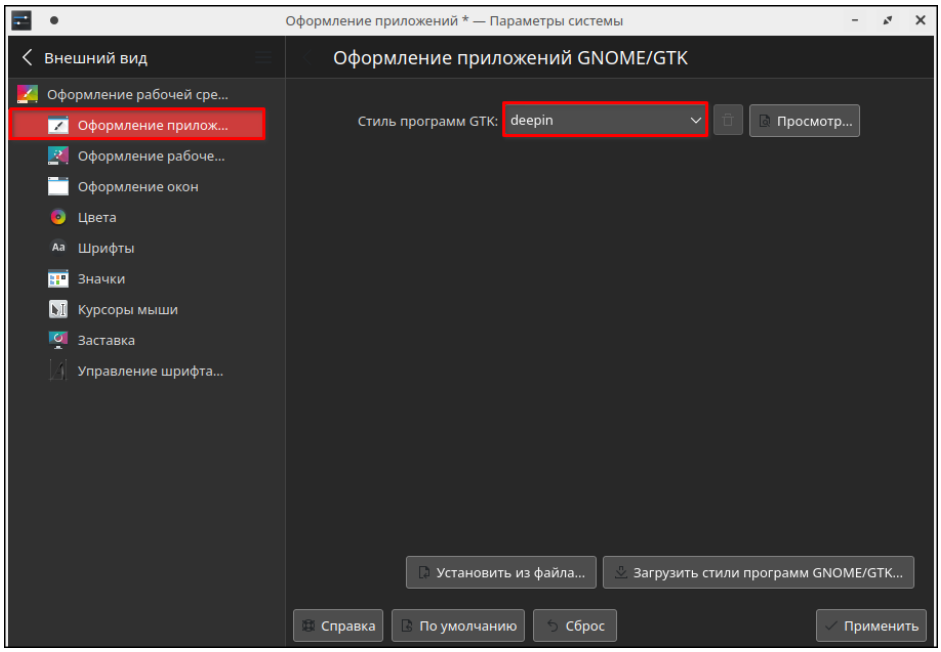
```
sudo dnf install deepin-gtk-theme
```

Настройка новой темы

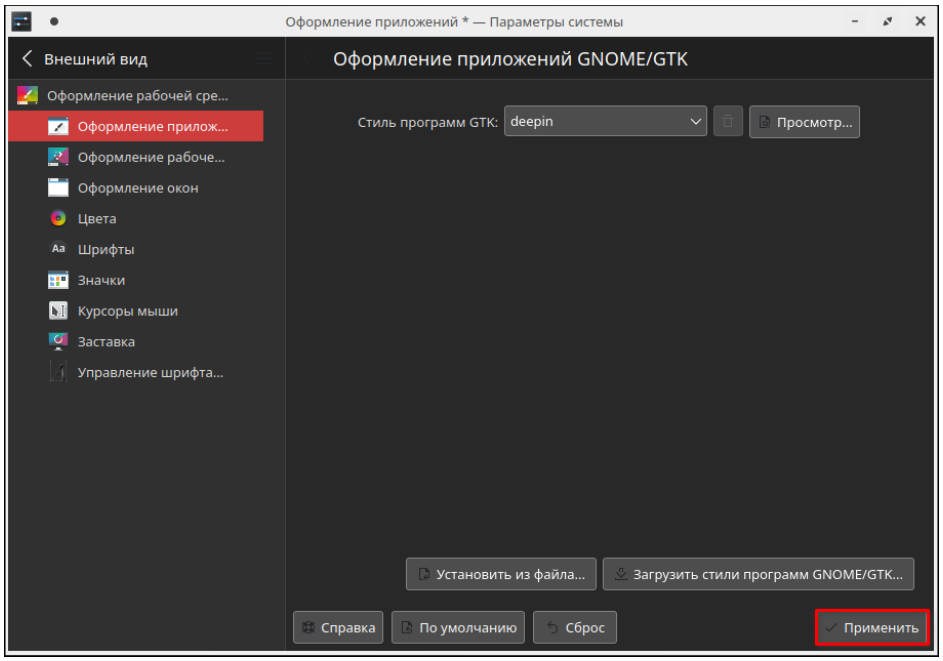
Для применения установленной темы пользователю необходимо открыть «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» и выбрать раздел «**Внешний вид**», в открывшемся окне необходимо перейти в подраздел «**Оформление приложений**» и нажать «**Настроить оформление приложений GNOME/GTK...**»



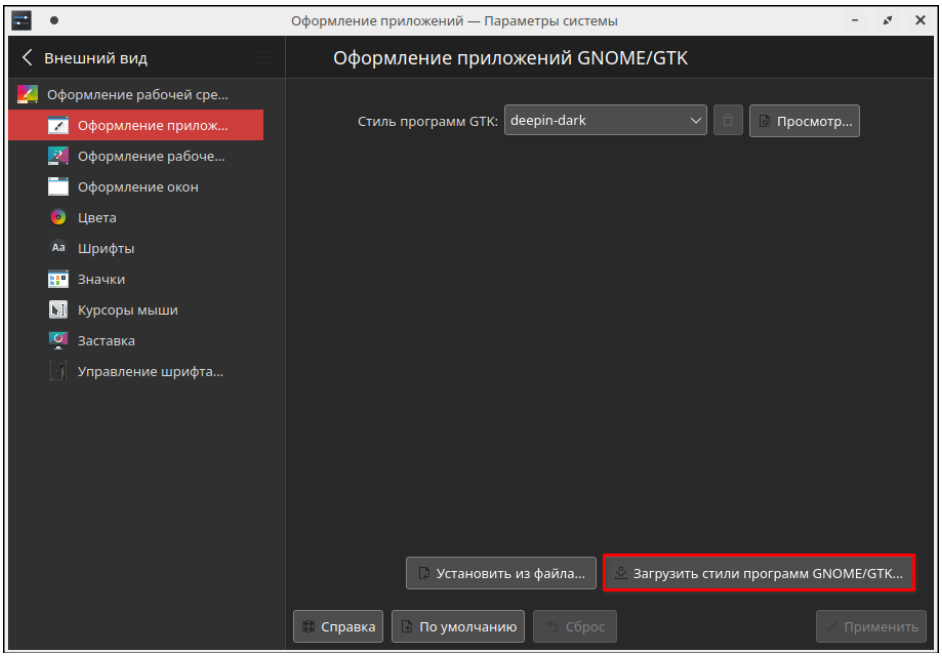
Выберите стиль программ GTK, нажав на выпадающий список и пролистав его до нужной темы.



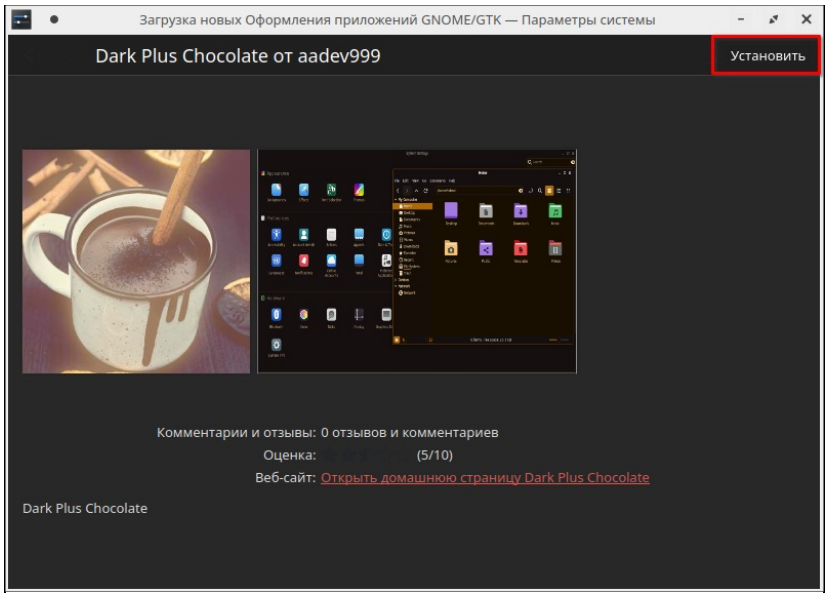
После выбора стиля нажмите «**Применить**» для изменения текущего стиля.



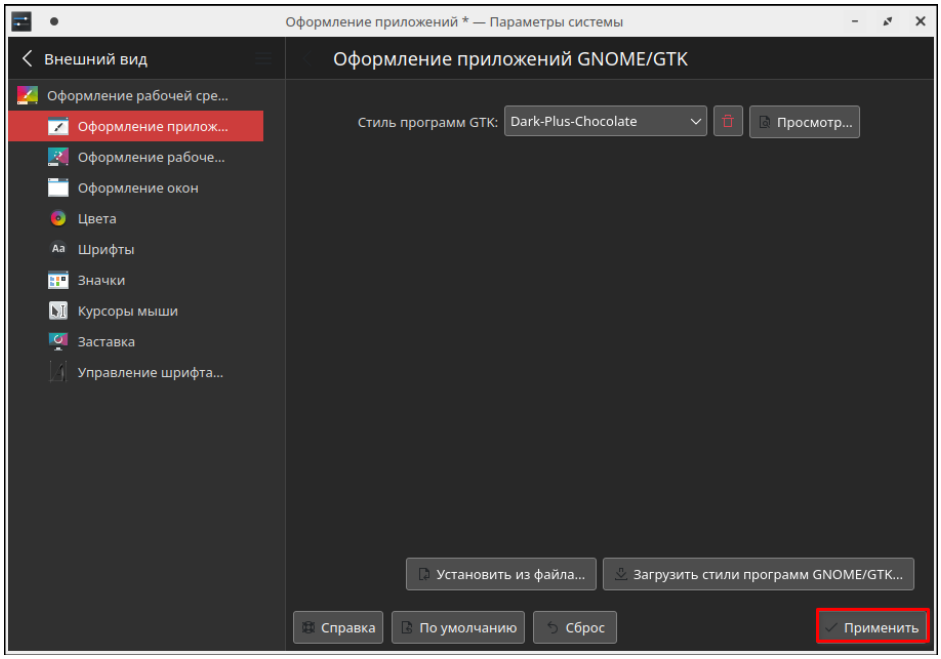
Можно загрузить дополнительные стили программ. Для этого нажмите на кнопку «**Загрузить стили программ GNOME/GTK...**».



В появившемся окне из списка тем можно выбрать понравившуюся тему, нажав на нее ЛКМ. Затем в окне с описанием выбранной темы в правом верхнем углу нажмите «**Установить**».

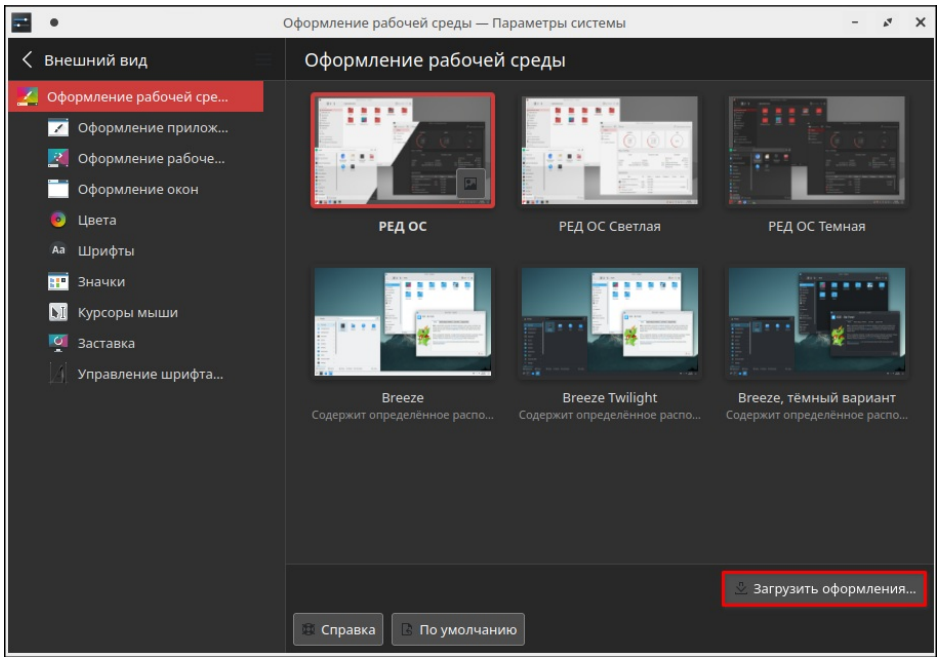


В разделе «**Стиль программ GTK**» выберите установленный стиль приложений. Далее нажмите «**Применить**».

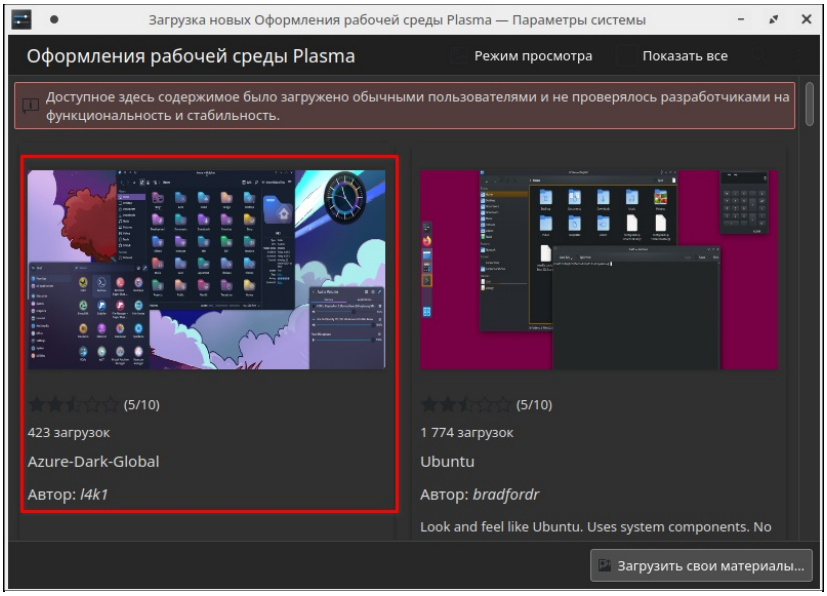


Настройка внешнего вида графического интерфейса РЕД ОС

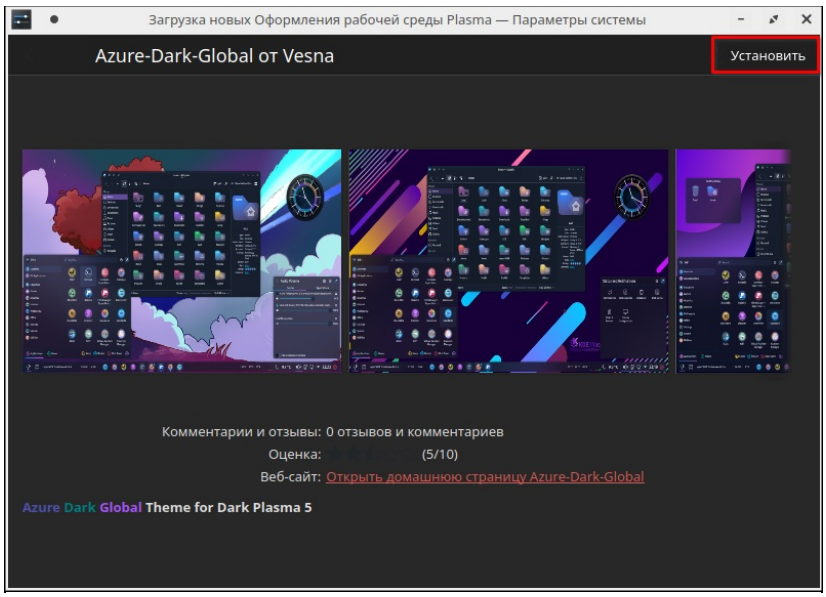
Для смены оформления рабочей среды пользователю необходимо открыть «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» и выбрать раздел «**Внешний вид**». Откроется раздел «**Оформление рабочей среды**». Для загрузки нового оформления нажмите «**Загрузить оформления...**».



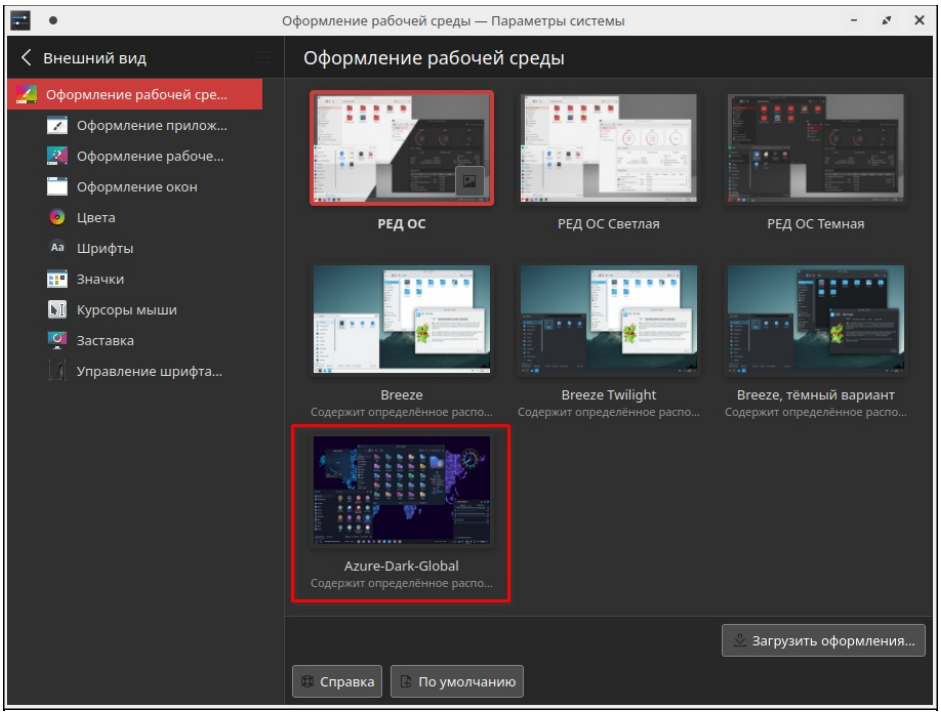
Появится окно загрузки новых тем оформления рабочей среды. Выберите из списка понравившуюся тему, щелкнув по ней ЛКМ.



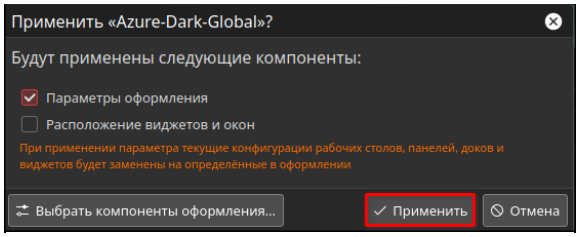
Загрузится окно с информацией о данной теме. Нажмите кнопку «**Установить**».



Если в теме несколько вариантов цветового оформления, то будет предложено выбрать вариант оформления для установки. Если вариант один, то загрузка начнется сразу. Далее дождитесь окончания обработки выбранного компонента.

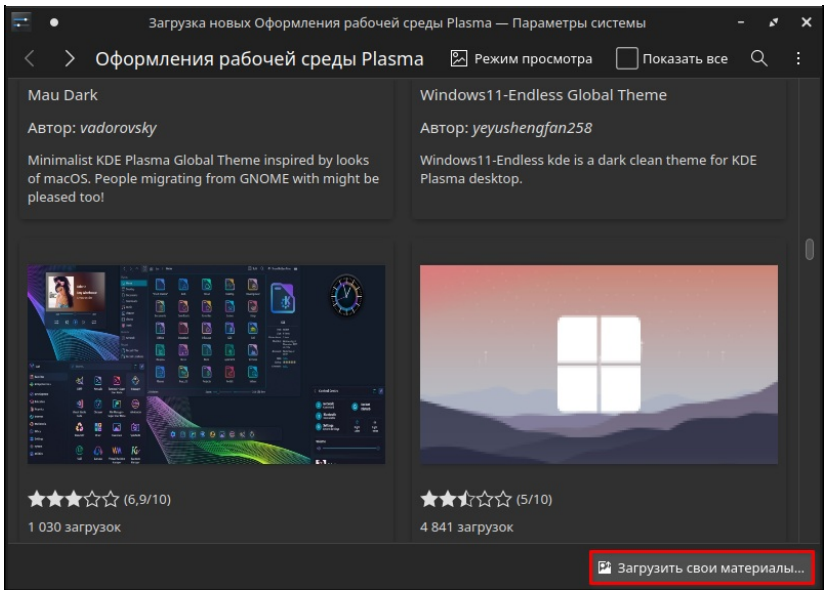


Щелкните ЛКМ по загруженной теме оформления рабочей среды. Если не требуется выбрать компоненты оформления, нажмите «**Применить**» (компоненты оформления будут выбраны по умолчанию).

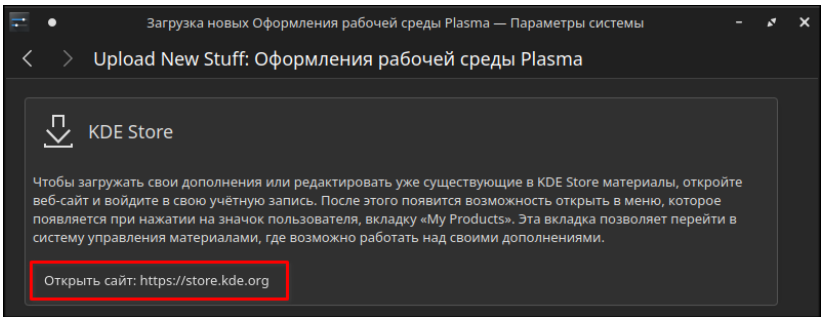


Установка дополнительных тем

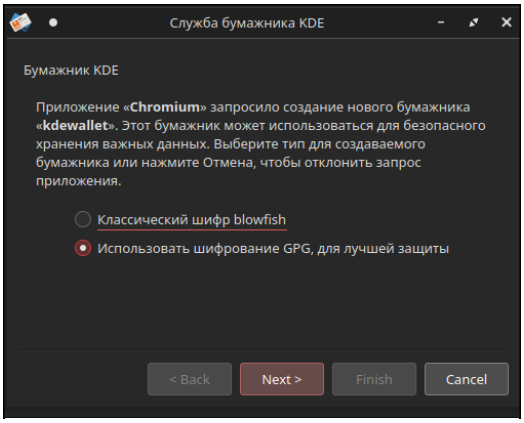
Можно также загружать свои дополнения и редактировать уже существующие темы оформления в **KDE Store**. Для загрузки пользовательских тем оформления нажмите «**Загрузить оформления...**» и в появившемся окне выберите «**Загрузить свои материалы...**».



Появится информационное окно с информацией о необходимых действиях для загрузки своих дополнений или редактирования уже существующих в **KDE Store** материалов. Далее нажмите «**Открыть сайт https://store.kde.org**».



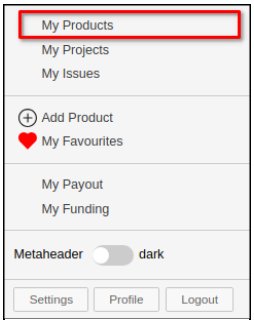
Следуя инструкциям, можно выбрать создание бумажника KDE.



Если создание бумажника не требуется, нажмите «**Cancel**».

KWallet (Бумажник KDE) — приложение для управления паролями в среде KDE, обеспечивающее пользователям централизованный способ хранения паролей.

После открытия веб-сайта войдите в свою учетную запись. После входа в учетную запись появится возможность открыть в меню вкладку «**My Products**». В этой вкладке можно работать со своими материалами.



Установка новых курсоров мыши

Для добавления новых курсоров (указателей мыши) можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**,

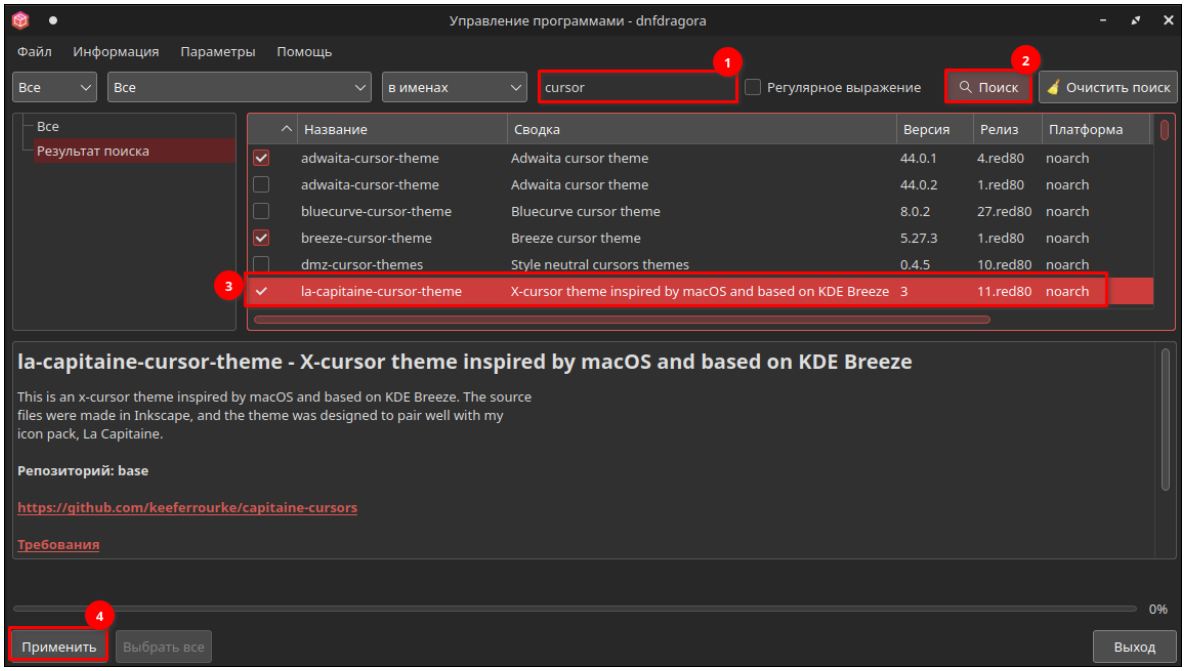
Для поиска новых курсоров через терминал выполните команду:

```
dnf search *-cursor*
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы курсора (потребуются права **администратора**), например:

```
dnf install la-capitaine-cursor-theme
```

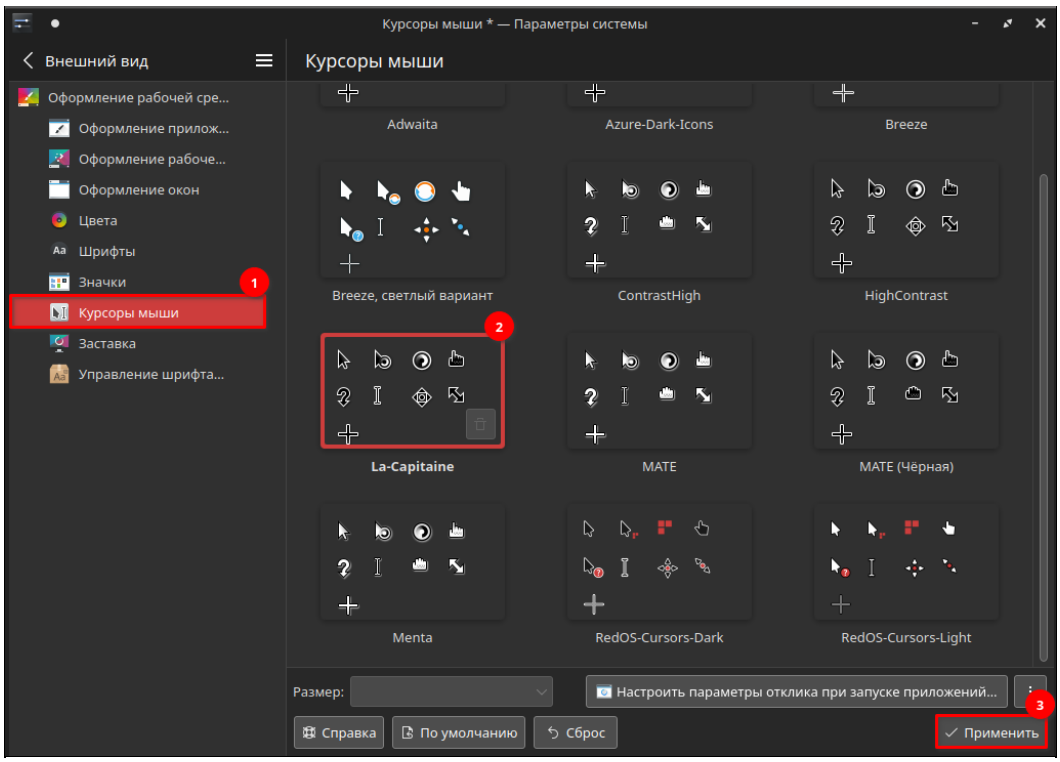
Для установки новой темы оформления указателя мыши через менеджер пакетов **dnfdragora** по шаблону — «**cursor**» (1) выполните поиск темы (2), отметьте флагом необходимую тему курсора (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



Для применения новой темы оформления курсора мыши перейдите в «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**»— «**Внешний вид**» — «**Курсоры мыши**» (1). Выберите установленную тему курсора (2) и нажмите «**Применить**» (3).

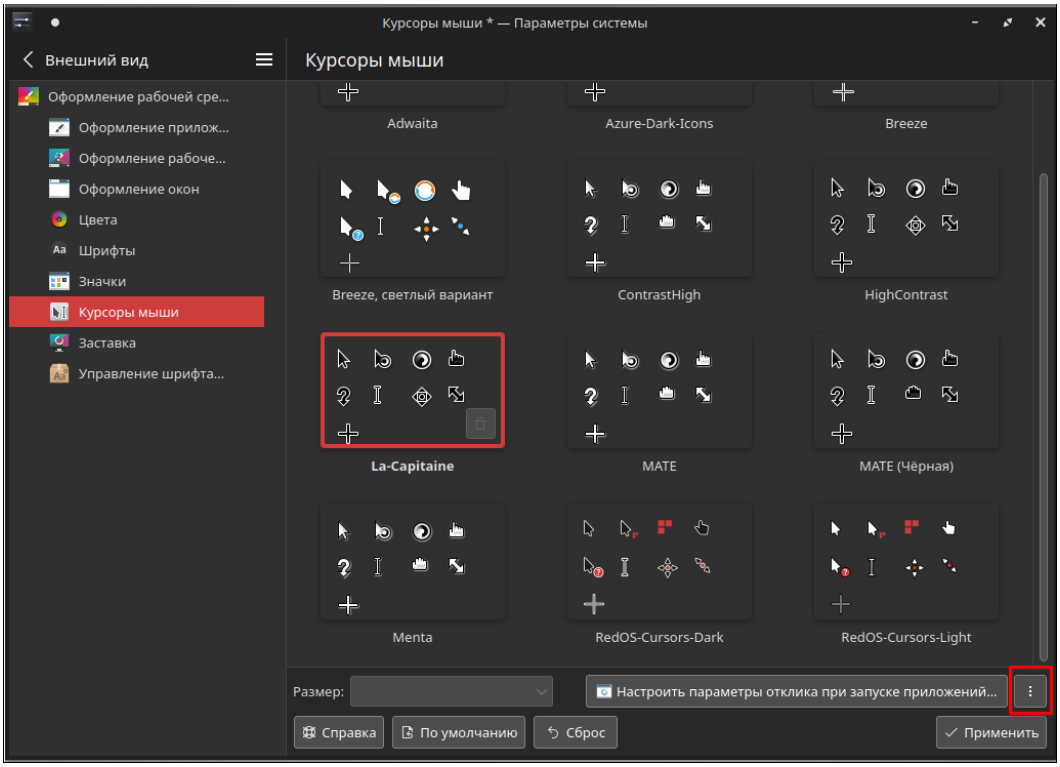
Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

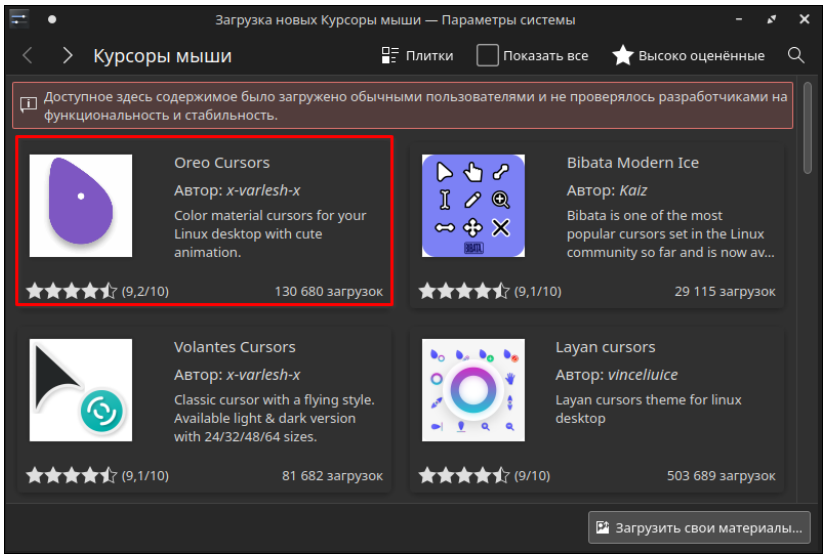


Установка дополнительных курсоров мыши

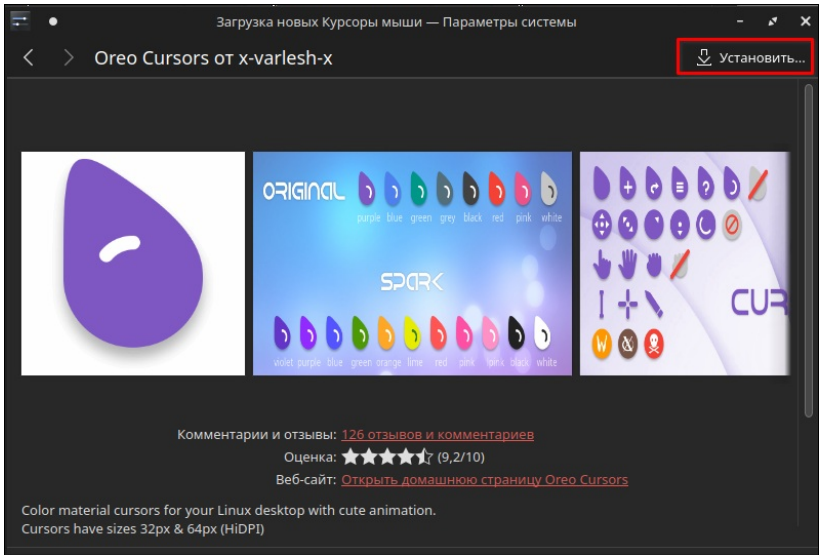
Можно также загрузить дополнительные темы курсоров мыши. Для загрузки пользовательских тем оформления нажмите в правом нижнем углу «**Больше действий**» ( ) и выберите «**Загрузить наборы курсоров...**».



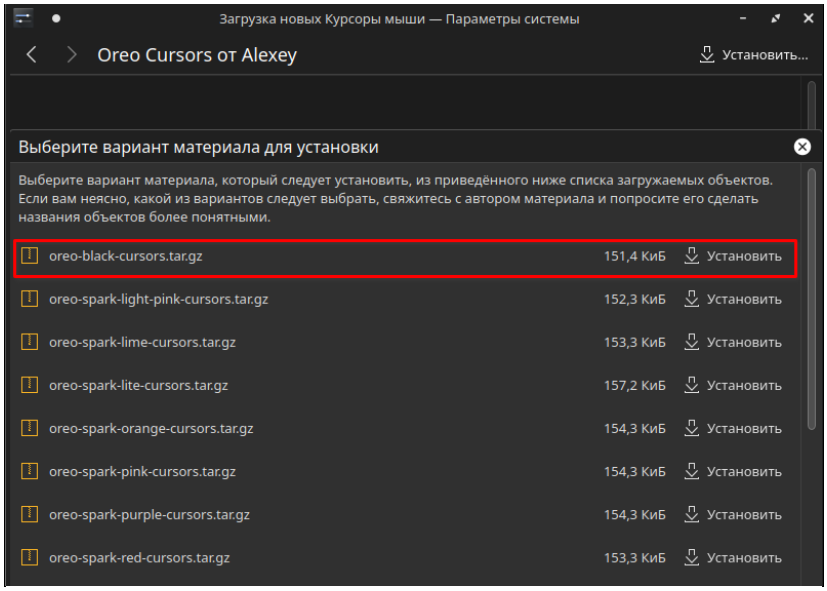
Откроется окно загрузки новых курсоров мыши.



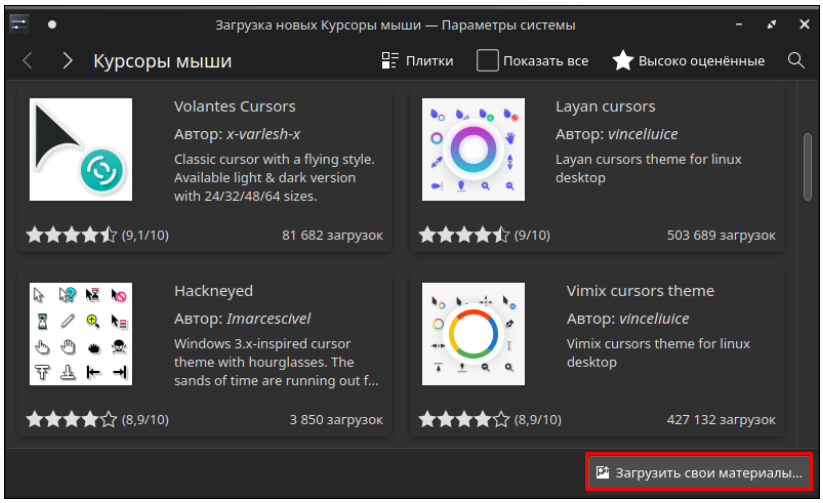
Выберите понравившуюся тему курсора и нажмите «**Установить...**».



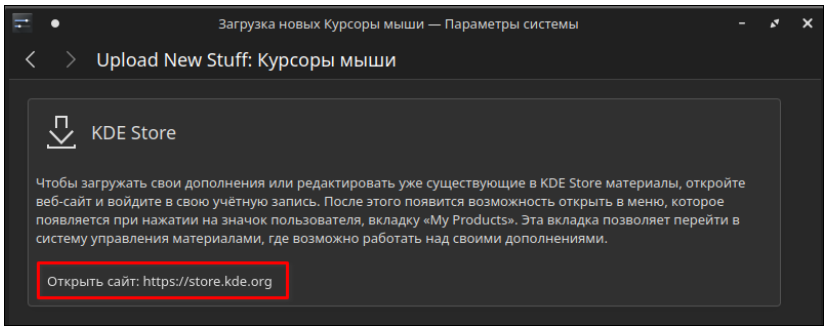
Если в теме несколько вариантов цветового оформления, то будет предложено выбрать вариант материала для установки. Рядом с выбранным материалом нажмите «**Установить**».



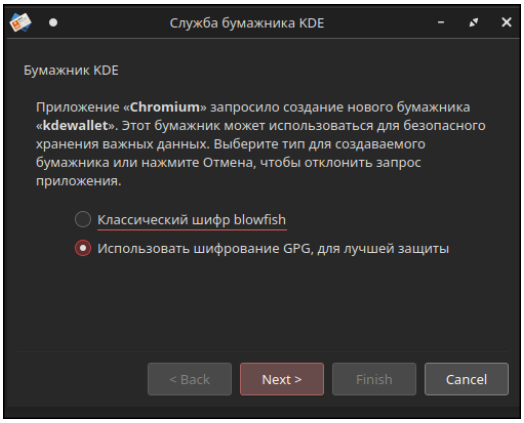
Можно также загружать свои дополнения или редактировать уже существующие в **KDE Store** материалы.



Появится информационное окно, сообщающее, какие действия необходимо выполнить для загрузки своих дополнений или редактирования имеющихся материалов. Далее нажмите «**Открыть сайт** **https://store.kde.org**».

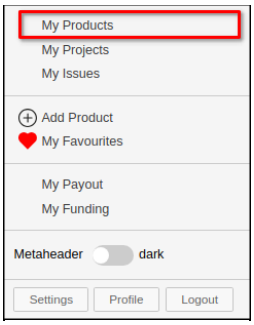


Следуя инструкциям, можно выбрать создание нового бумажника «**kdewallet**».



Если создание бумажника не требуется, нажмите «**Cancel**». Откроется выбранный сайт.

После открытия веб-сайта войдите в свою учетную запись. После входа в учетную запись появится возможность открыть в меню вкладку «**My Products**». В этой вкладке можно работать со своими материалами.



Установка новых тем значков (иконок)

Для добавления новых значков (иконок) рабочего стола можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**.

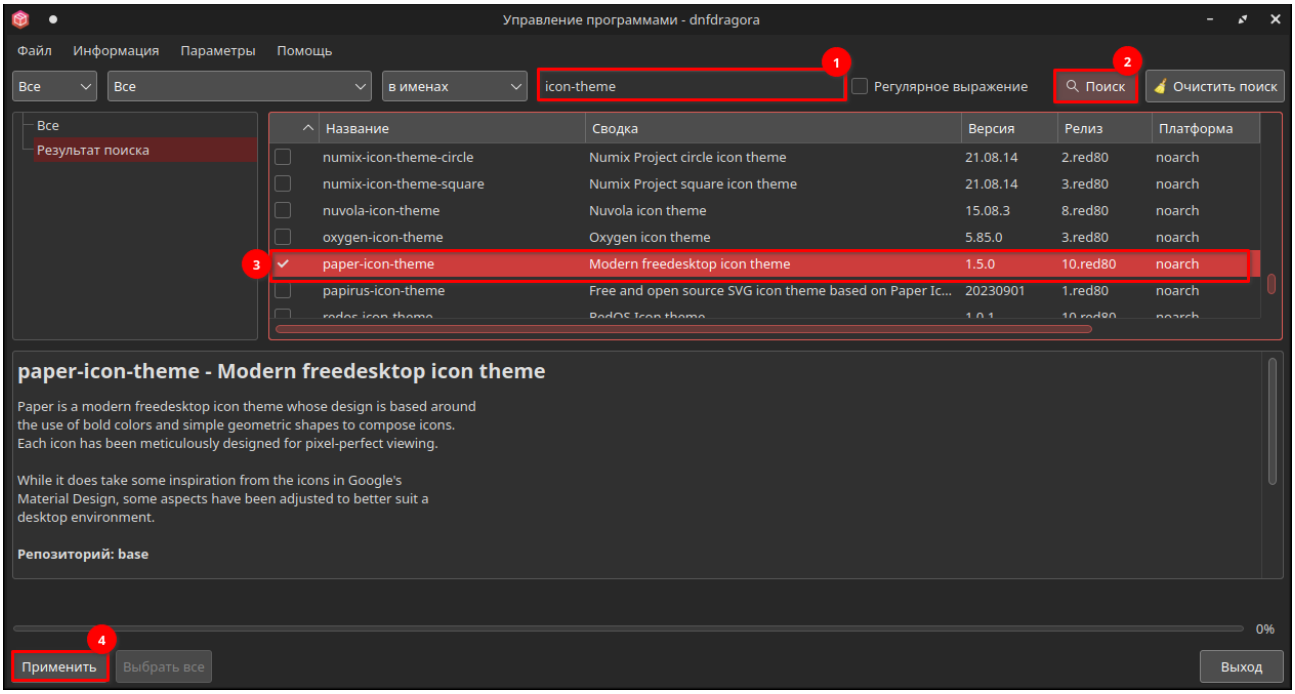
Для поиска новых тем значков через терминал выполните команду:

```
dnf search icon-theme
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы значков (потребуются права **администратора**), например:

```
dnf install paper-icon-theme
```

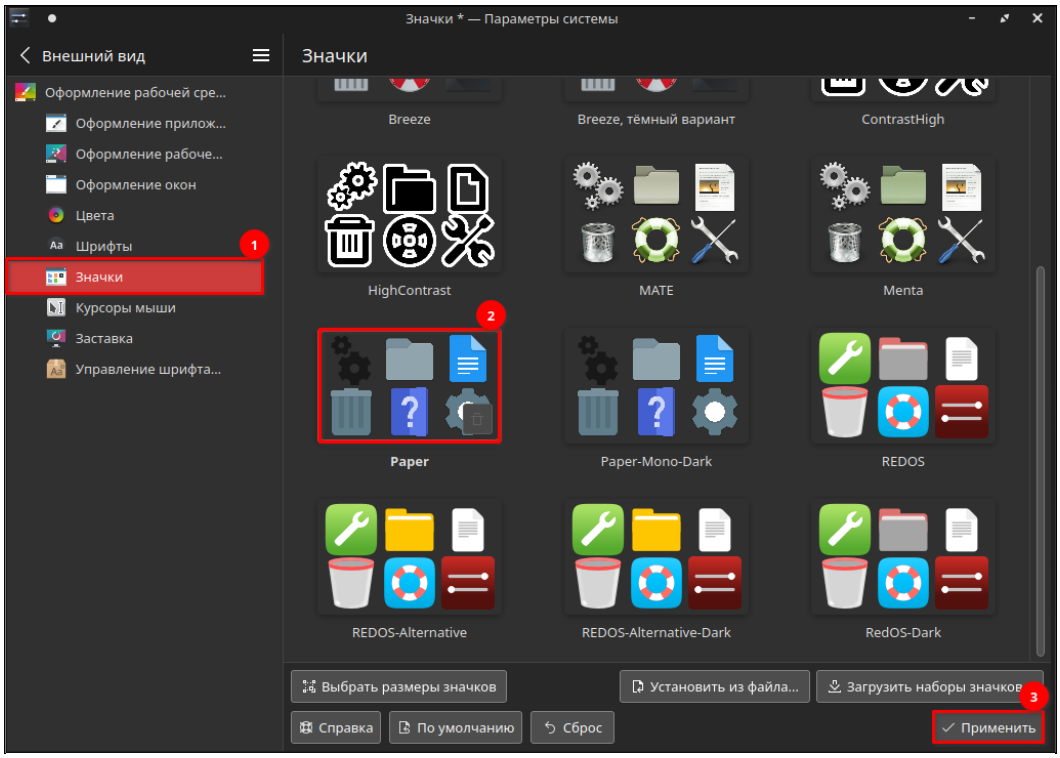
Для установки новой темы оформления значков рабочего стола через менеджер пакетов **dnfdragora** выполните поиск темы по шаблону — «**icon-theme**», выберите из списка актуальную версию пакета и нажмите кнопку « **Применить**».



Примечание.

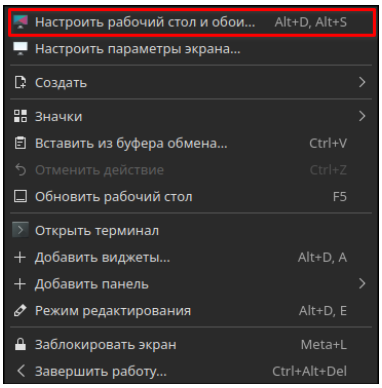
После установки новых тем оформления может потребоваться перезагрузка системы.

Для применения новой темы оформления значков перейдите в «**Меню запуска приложений**» — «**Настройка**» — «**Параметры системы**» — «**Внешний вид**» — «**Значки**» (1). Выберите установленную тему значков (2) и нажмите «**Применить**» (3).

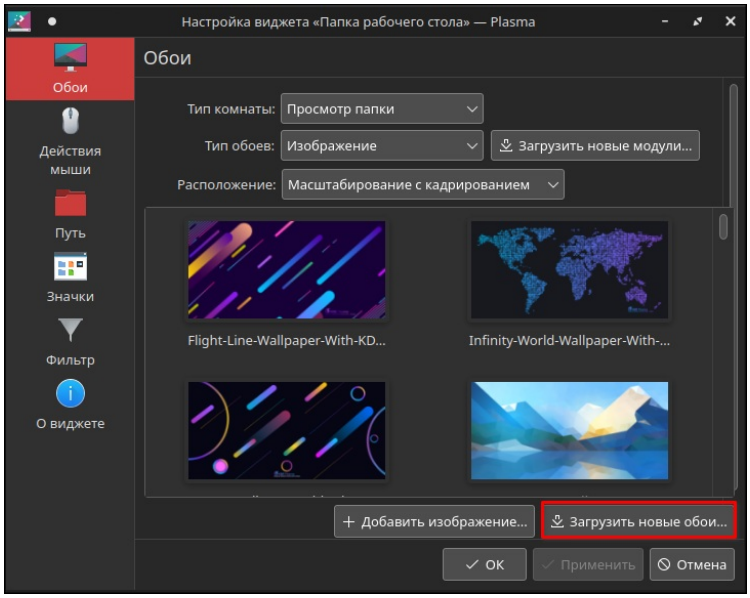


Установка нового фона рабочего стола

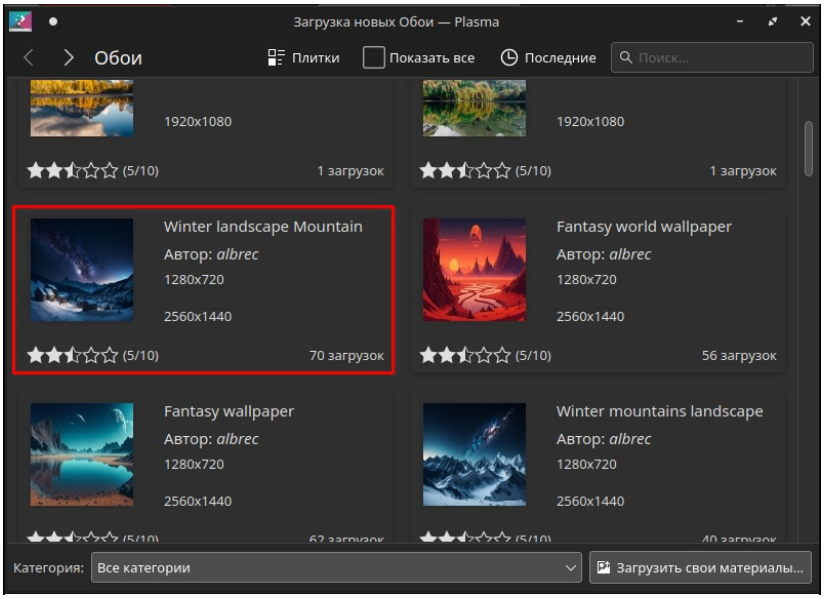
Для установки нового фона рабочего стола необходимо в свободной части рабочего стола вызвать контекстное меню, нажав ПКМ. В открывшемся контекстном меню необходимо выбрать пункт «**Настроить рабочий стол и обои...**».



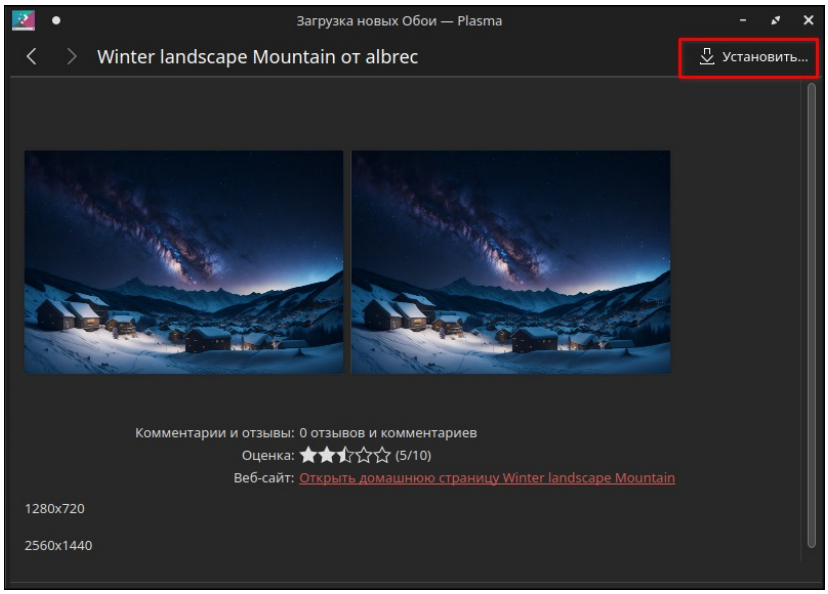
На вкладке «**Обои**» можно выбрать доступное изображение или добавить собственное, нажав кнопку « **Загрузить новые обои...**».



В окне выбора загрузки новых обоев выберите понравившиеся обои из предложенных вариантов. Обои можно вывести списком, значками или крупными миниатюрами, сортировать по алфавиту, по времени, по рейтингу, по популярности.

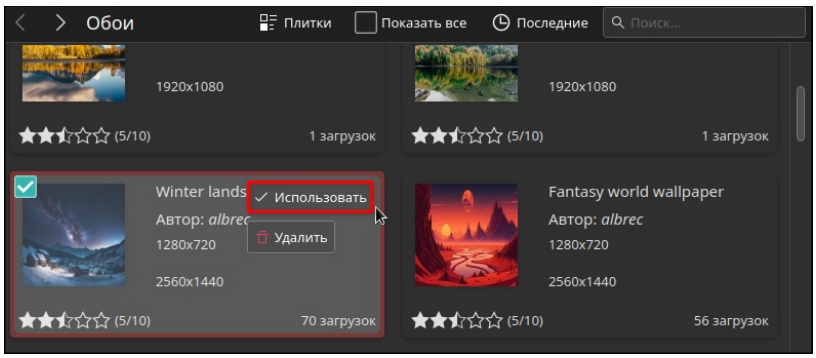


Далее отобразится информация об обоях, которые можно установить. Выберите «**Установить...**».



Если будет выведено окно и предложены варианты для выбора, выберите вариант материала для установки и нажмите «**Установить**».

При наведении курсора мыши на область новых обоев доступно две опции: «**Использовать**» и «**Удалить**». Для применения новых обоев нажмите «**Использовать**».



Настройка внешнего вида графического окружения GNOME

Настройка темы графической оболочки GNOME
Установка темы через менеджер пакетов dnfdragora
Установка темы через терминал
Устранение неполадок: не удается выбрать тему GNOME Shell
Установка дополнительных тем
Установка новых курсоров мыши
Установка дополнительных тем курсоров мыши
Установка новых тем значков (иконок)
Установка дополнительных тем значков (иконок)
Установка нового фона рабочего стола

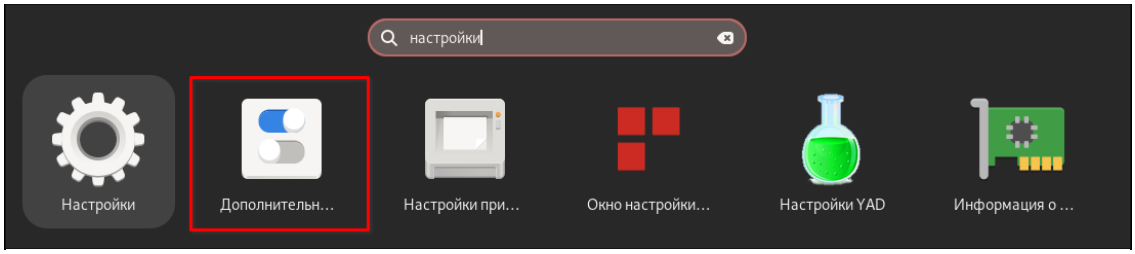
Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

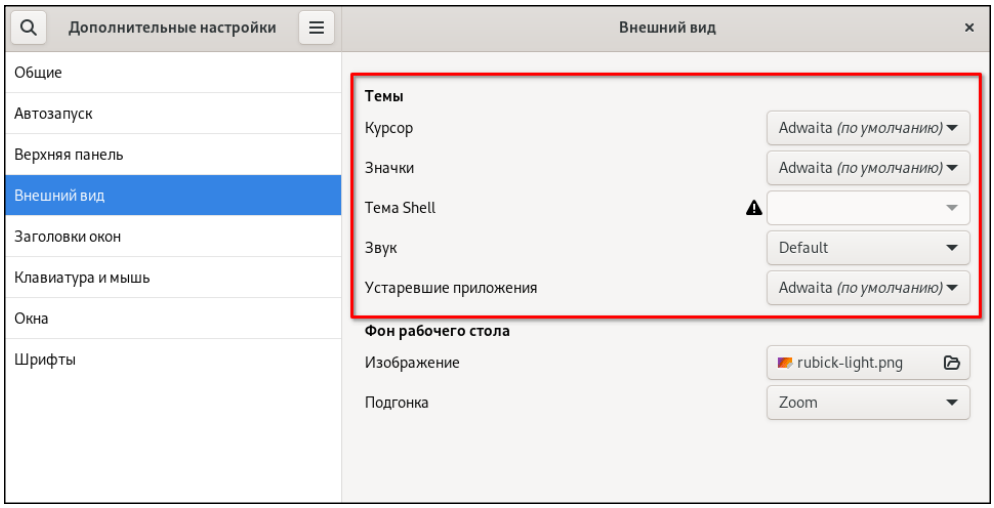
Настройка темы графической оболочки GNOME

Тема — это группа параметров, влияющих на визуальное представление частей рабочего стола. Тема влияет на различные параметры: элементы управления, цвета, рамку окна, значки, указатели.

Для смены внешнего вида окон графической оболочки РЕД ОС пользователю необходимо перейти в меню «**Показать приложения**», ввести в поисковой строке «*настройки*», выбрать «**Дополнительные настройки GNOME**».

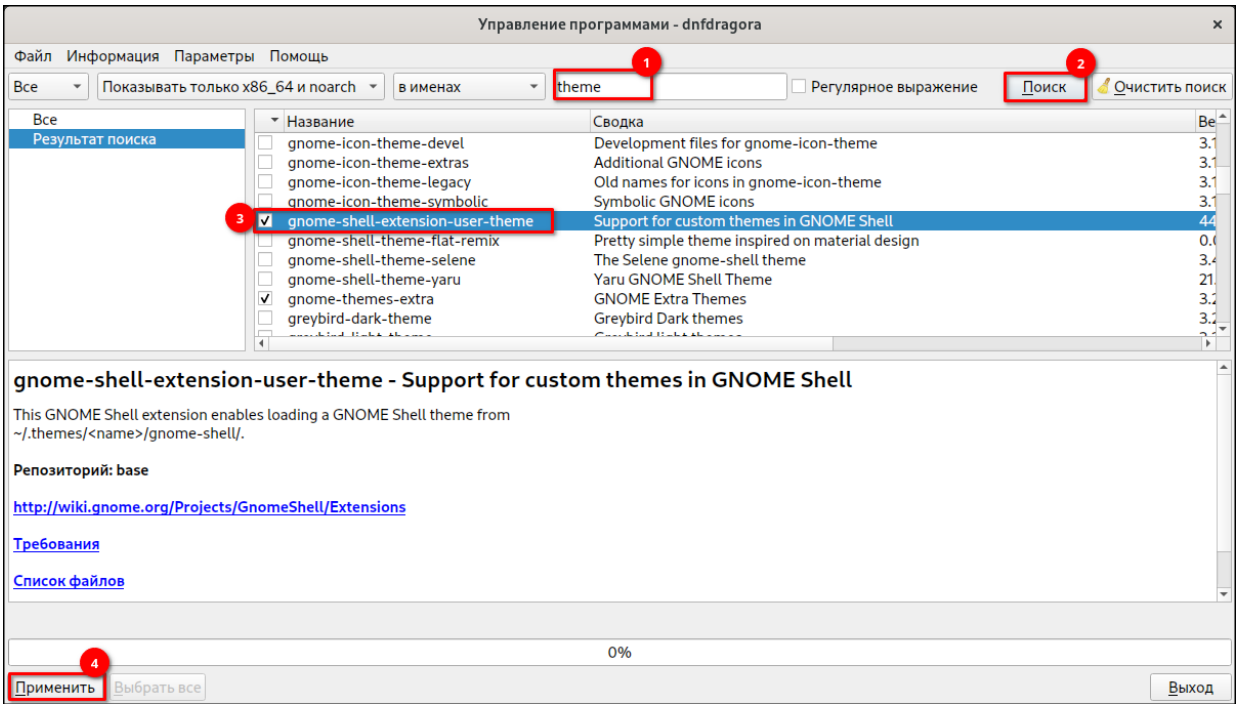


В открывшемся окне необходимо перейти в раздел «**Внешний вид**» и в блоке «**Темы**» определить собственные значения стилевого оформления отдельных элементов интерфейса, полностью независимые друг от друга и от темы рабочего стола, такие как указатель мыши, значки приложений, тема shell, звук и окна устаревших приложений. При выборе какого-либо значения его применение производится автоматически.



Установка темы через менеджер пакетов dnfdragora

Для установки темы через графический менеджер пакетов **dnfdragora** перейдите в «**Показать приложения**» — «**Управление программами dnfdragora**», выполните поиск необходимого пакета по ключевому слову (например, «**theme**») и отметьте флагом нужный пакет. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



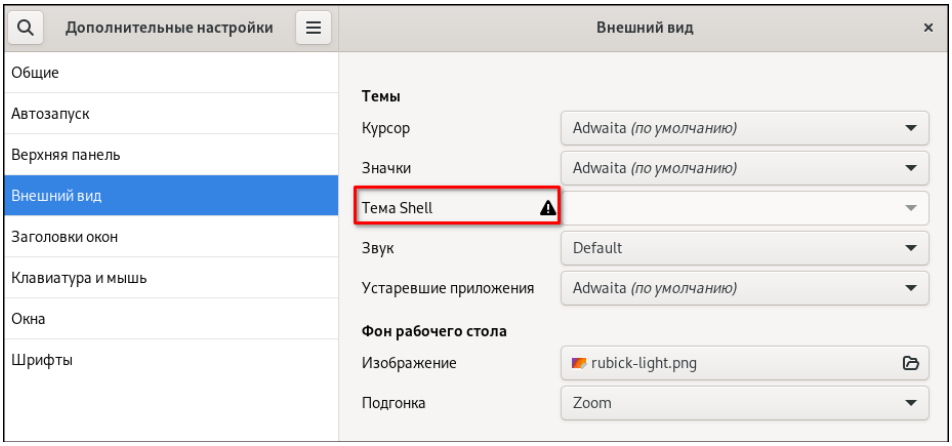
Установка темы через терминал

Для установки программы через терминал выполните команду (потребуются права **администратора**):

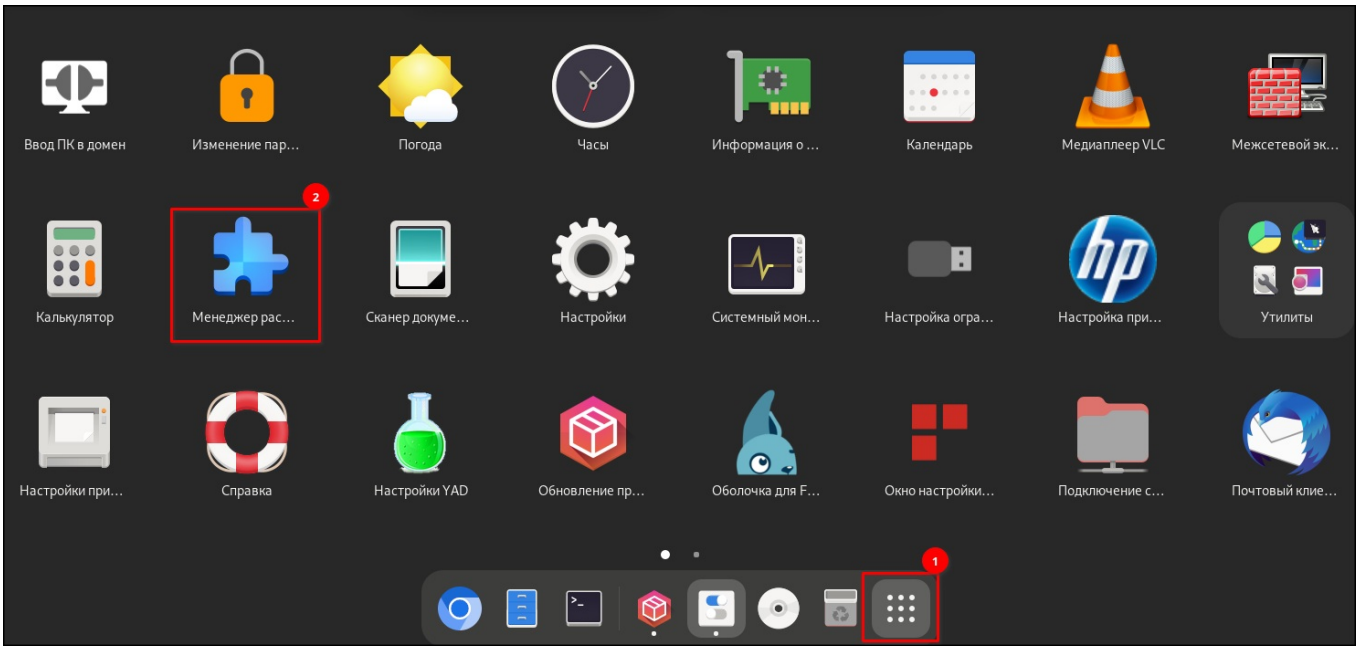
```
sudo dnf install adwaita-blue-gtk-theme
```

Устранение неполадок: не удается выбрать тему GNOME Shell

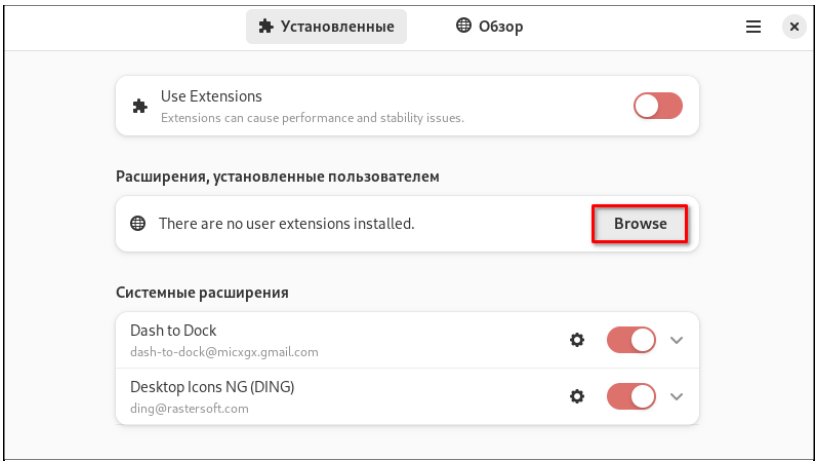
В дополнительных настройках перейдите в раздел «**Внешний вид**». Если в блоке «**Темы**» перед темой Shell есть предупреждающий знак, для устранения проблемы необходимо установить расширения GNOME Shell.



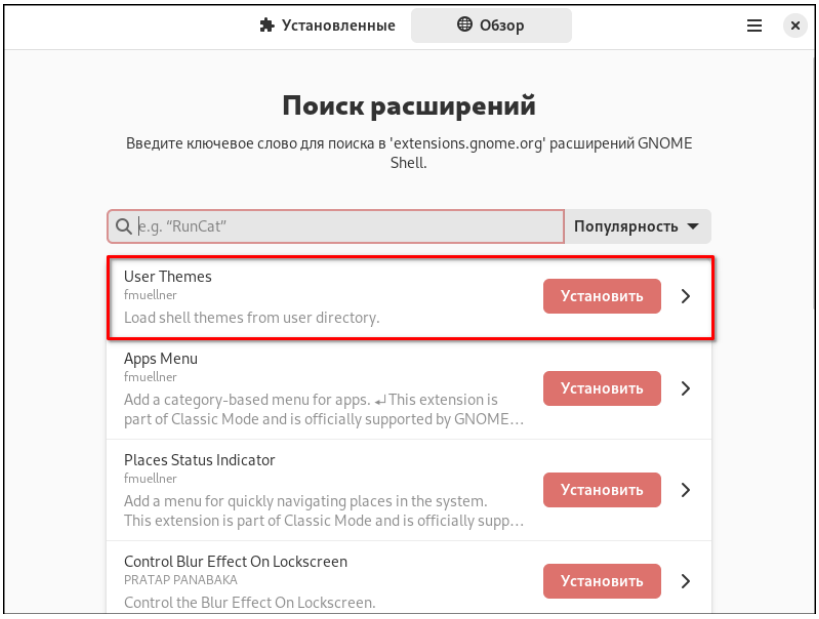
Перейдите в меню «**Показать приложения**» — «**Менеджер расширений**».



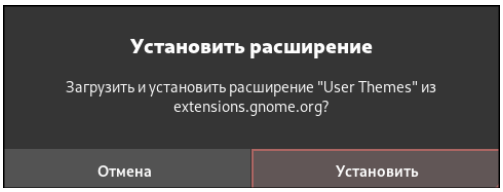
Для перехода в расширения, установленные пользователем, щелкните ЛКМ кнопку «**Browse**».



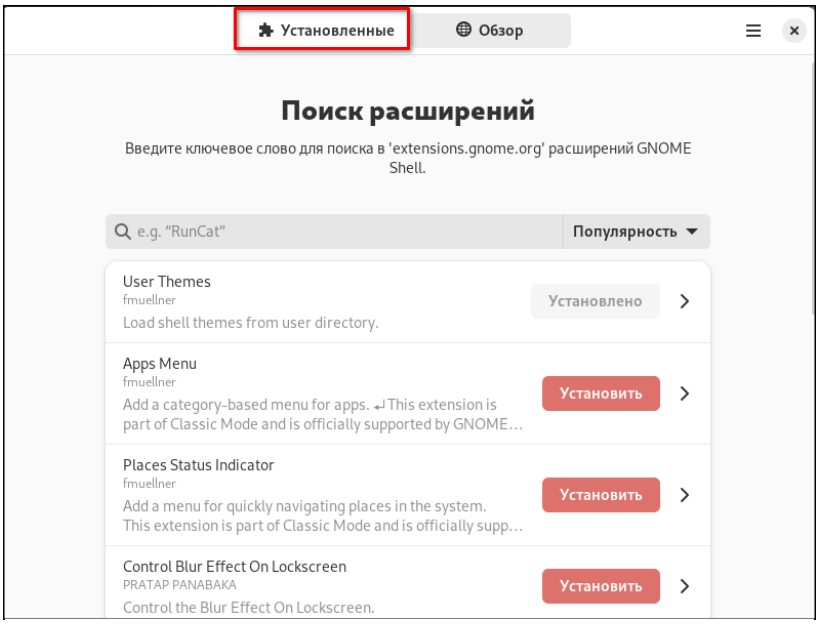
Откроется окно с расширениями GNOME Shell. Найдите в списке «**User Themes**» и нажмите «**Установить**».



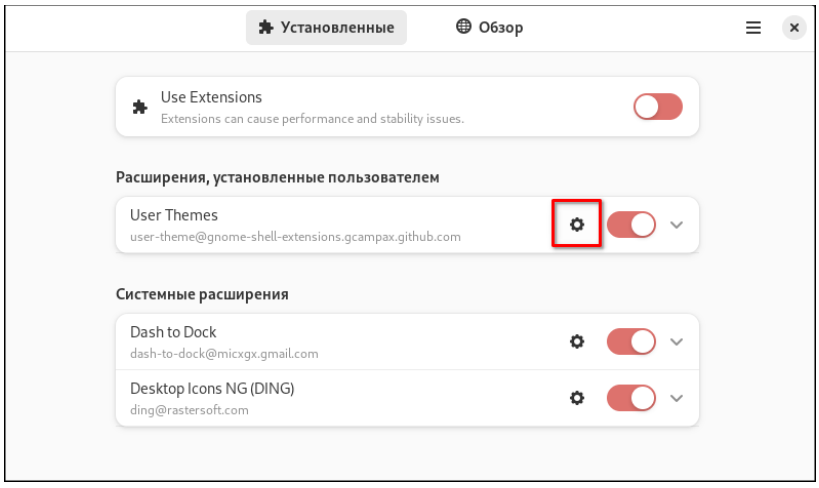
Далее появится диалоговое окно для загрузки и установки расширения «**User Themes**». Нажмите «**Установить**».



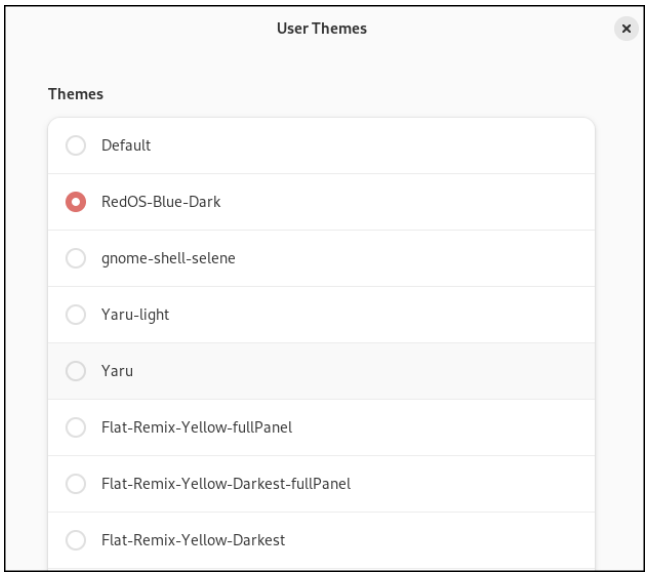
После установки пользовательских тем перейдите во вкладку «**Установленные**».



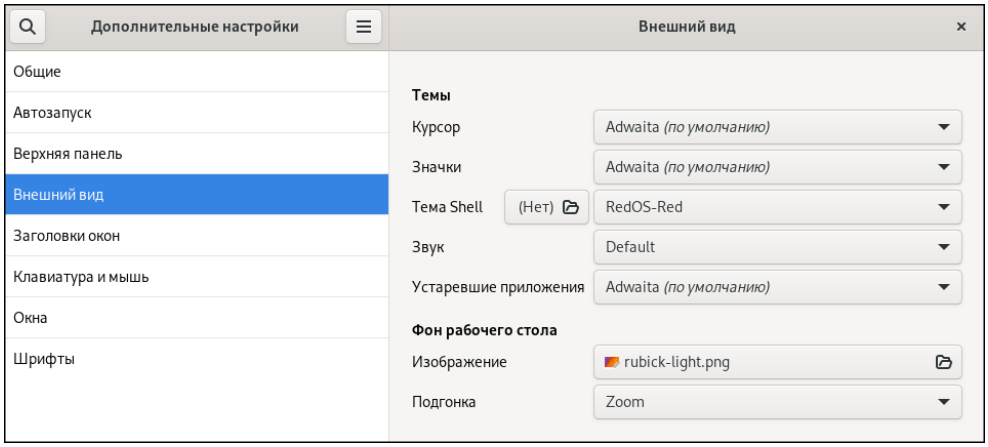
На вкладке «**Установленные**» в разделе «**Расширения, установленные пользователем**» по нажатии на значок шестеренки откроется список установленных тем.



Список установленных тем может меняться в зависимости от того, какие пакеты устанавливаются или удаляются. Если щелкнуть по выбранной теме, она будет автоматически применена.



После установки тем в дополнительных настройках в инструменте «**Внешний вид**» тему Shell можно изменить.

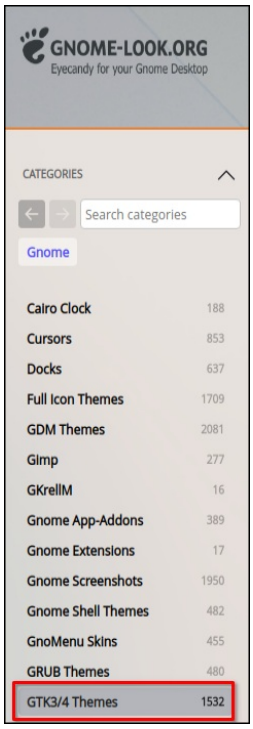


Установка дополнительных тем

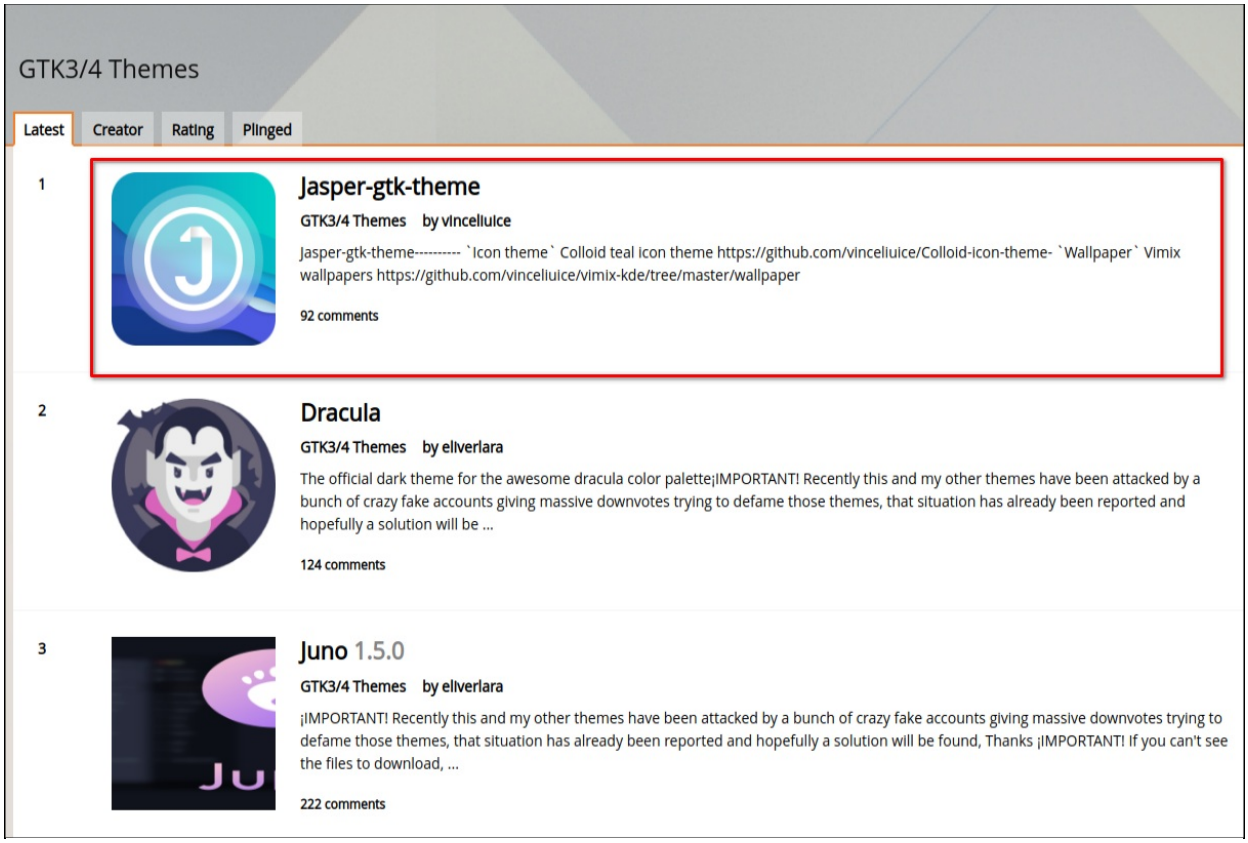
Для установки сторонней темы и добавления ее в список доступных выполните следующий алгоритм действий:

1. Перейдите на сайт https://www.gnome-look.org.

2. На левой боковой панели выберите категорию тем «**GTK3/4 Themes**».



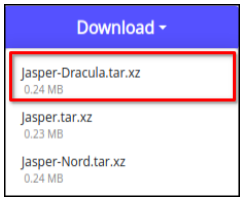
3. Выберите из списка понравившуюся тему и щелкните по ней ЛКМ.



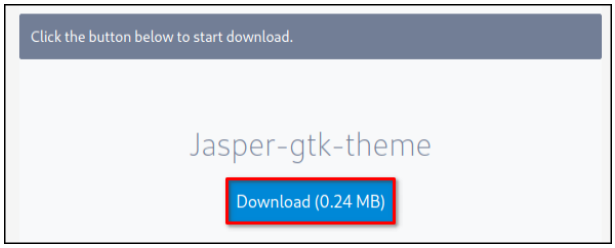
4. Для загрузки в правой боковой панели нажмите «**Download**».



5. По нажатии на кнопку «**Download**» будет открыт список с доступным цветовым оформлением. Выберите любое цветовое оформление.



6. Начнется подготовка архива к скачиванию. Когда архив станет доступен для скачивания, нажмите на активную кнопку «**Download**». Архив по умолчанию сохранится в каталог /home/user/Загрузки/.



7. Откройте терминал и перейдите в каталог с загруженными архивами тем (в примере /home/user/Загрузки/):

```
cd /home/user/Загрузки/
```

8. Распакуйте архив с основной темой с помощью команды:

```
tar -xvf ./Jasper-Dracula.tar.xz
```

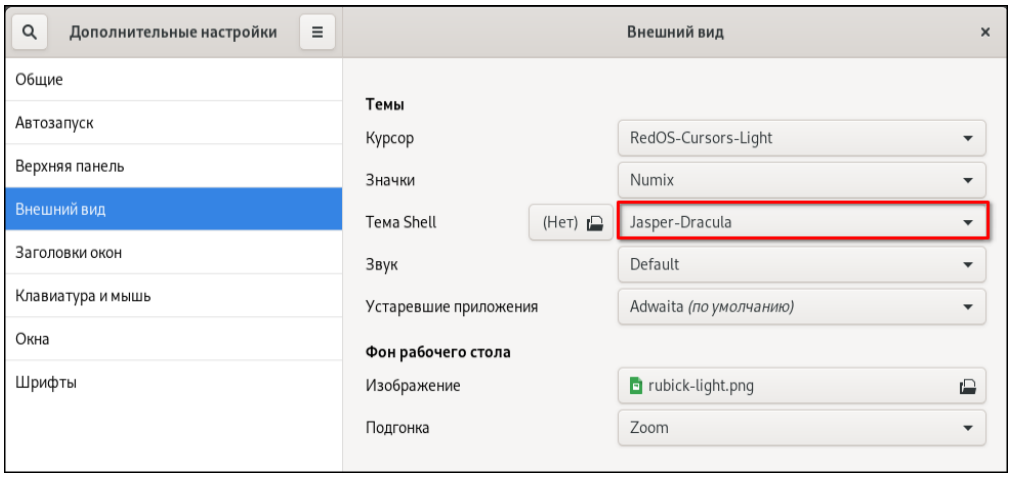
9. Скопируйте распакованный каталог темы в **/usr/share/themes/** (потребуются права **администратора**):

```
sudo cp -r ./Jasper-Dracula /usr/share/themes/
```

Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

10. Закройте терминал и перейдите в «**Дополнительные настройки**» — «**Внешний вид**». Выберите установленную тему. Новая тема будет применена автоматически.



Установка новых курсоров мыши

Для добавления новых курсоров (указателей мыши) можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**,

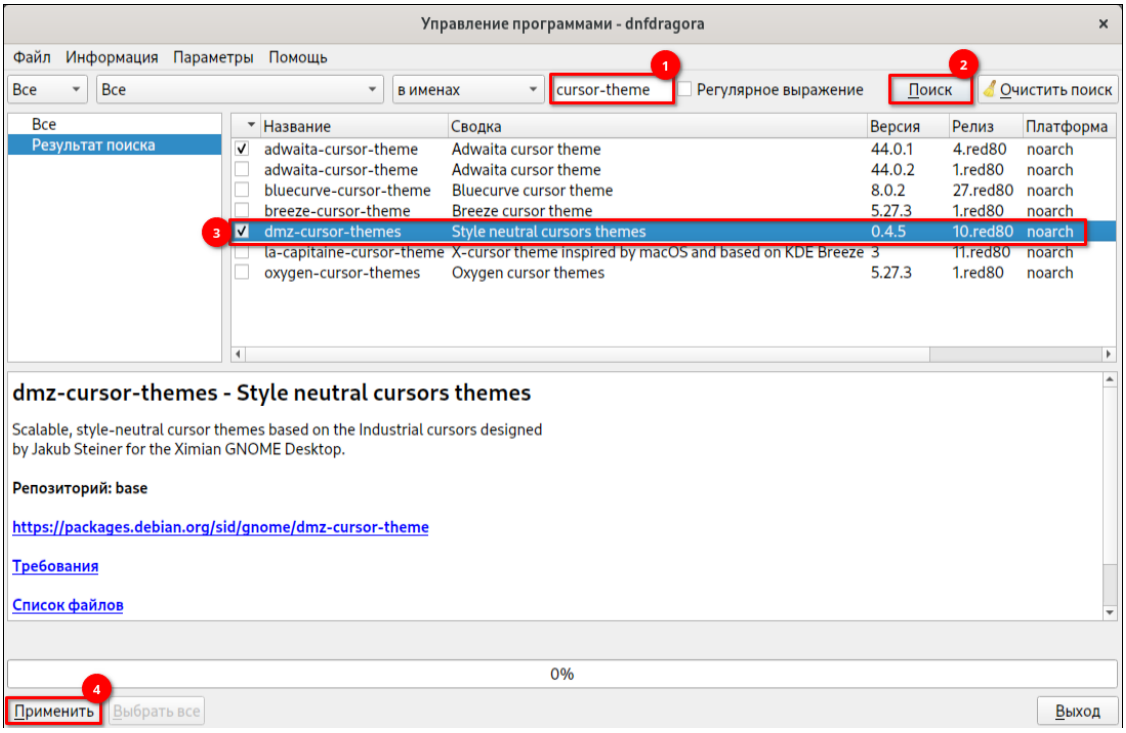
Для поиска новых курсоров через терминал выполните команду:

```
dnf search *-cursor-theme
```

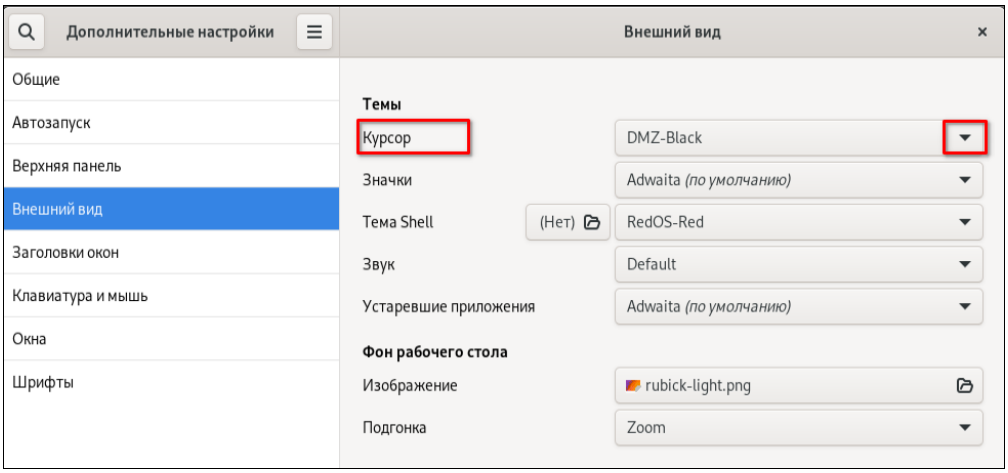
Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы курсора (потребуются права **администратора**), например:

```
dnf install dmz-cursor-theme
```

Для установки новой темы оформления указателя мыши через менеджер пакетов **dnfdragora** по шаблону — «**cursor-theme**» (1) выполните поиск темы (2), отметьте флагом необходимую тему (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



Для применения новой темы оформления курсора мыши перейдите в «**Дополнительные настройки**» — «**Внешний вид**». В блоке «**Темы**» из выпадающего списка курсоров выберите установленную тему курсора. Выбранная тема курсора будет применена автоматически.



Примечание.

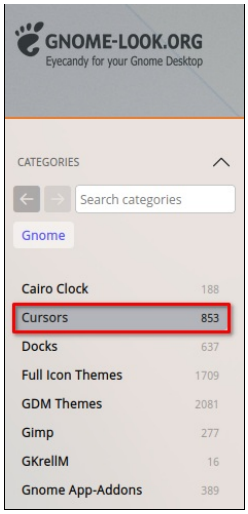
После установки новых тем оформления может потребоваться перезагрузка системы.

Установка дополнительных тем курсоров мыши

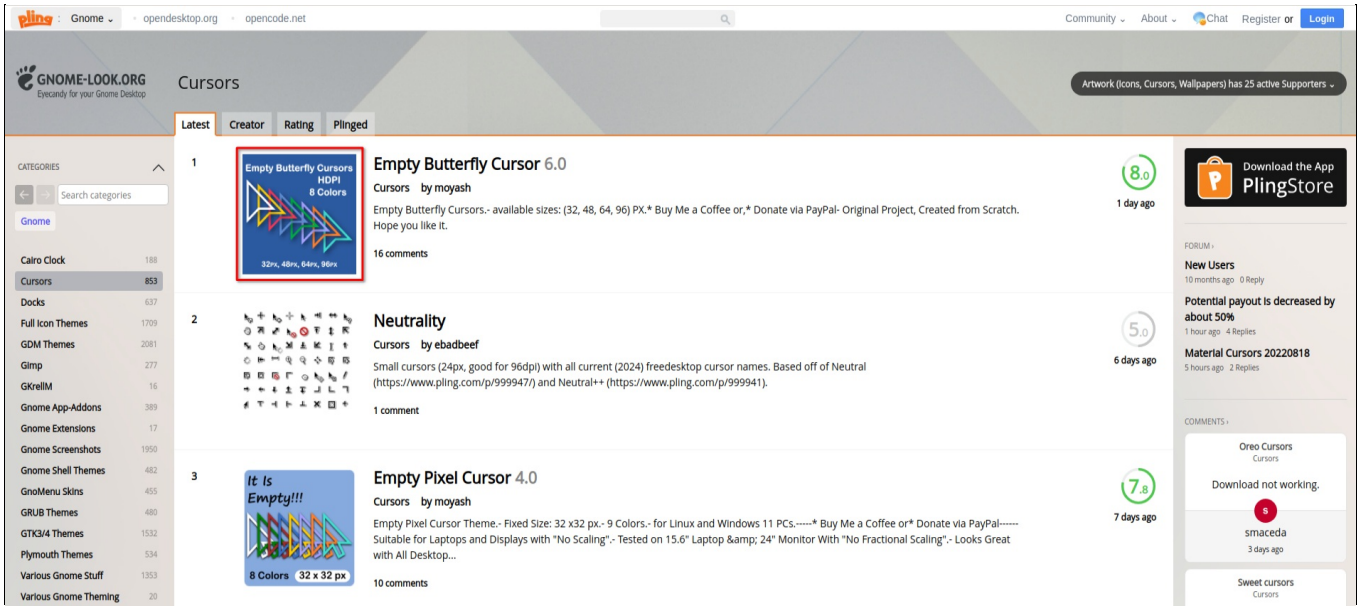
Для установки сторонней темы и добавления ее в список доступных выполните следующий алгоритм действий:

1. Перейдите на сайт https://www.gnome-look.org.

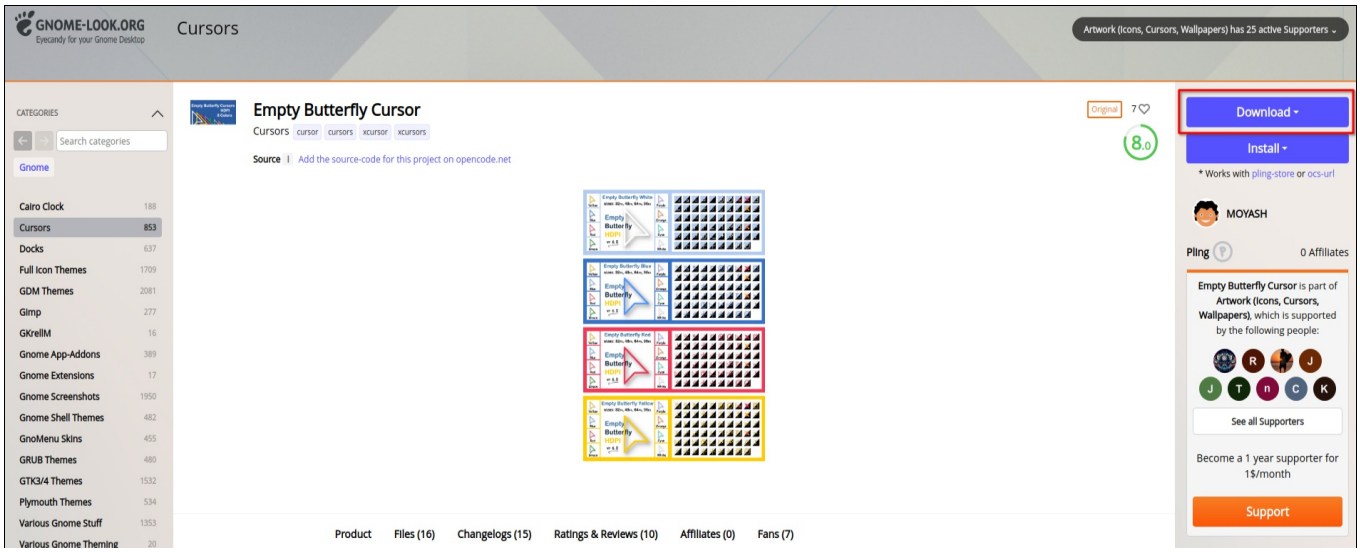
2. На левой боковой панели выберите категорию «**Курсоры**».



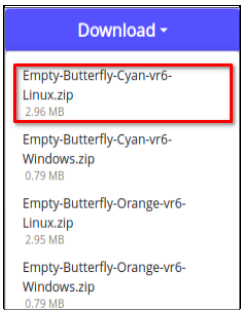
3. Выберите из списка понравившуюся тему и щелкните ЛКМ по ней.



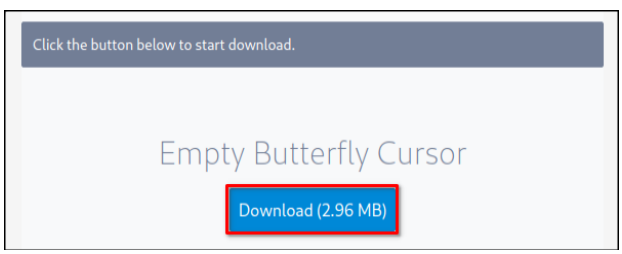
4. Для загрузки нажмите «**Download**».



5. По нажатии на кнопку «**Download**» будет открыт список с доступным цветовым оформлением. Выберите любое цветовое оформление.



6. Начнется подготовка архива к скачиванию. Когда архив станет доступен для скачивания, нажмите на активную кнопку «**Download**». Архив будет сохранен в каталог загрузок (в примере /home/user/Загрузки/).



7. Откройте терминал и перейдите в каталог с загруженными архивами тем (в примере /home/user/Загрузки/):

```
cd /home/user/Загрузки/
```

8. Убедитесь, что установлен пакет для работы с архивами **unzip** (потребуются права **администратора**):

```
sudo dnf install unzip
```

9. Распакуйте архив с основной темой с помощью команды:

```
unzip ./Empty-Butterfly-Cyan-vr6-Linux.zip
```

Примечание.

Все файлы на сайте упакованы в архивы и после извлечения файлы окажутся в дополнительной папке с именем архива. Удалите лишнюю папку с именем архива.

10. Перейдите в каталог с распакованной темой курсора.

```
cd ./Empty-Butterfly-Cyan-vr6-Linux
```

11. Просмотрите содержимое каталога, внутри будет еще один каталог, который нужно скопировать.

```
ls
```

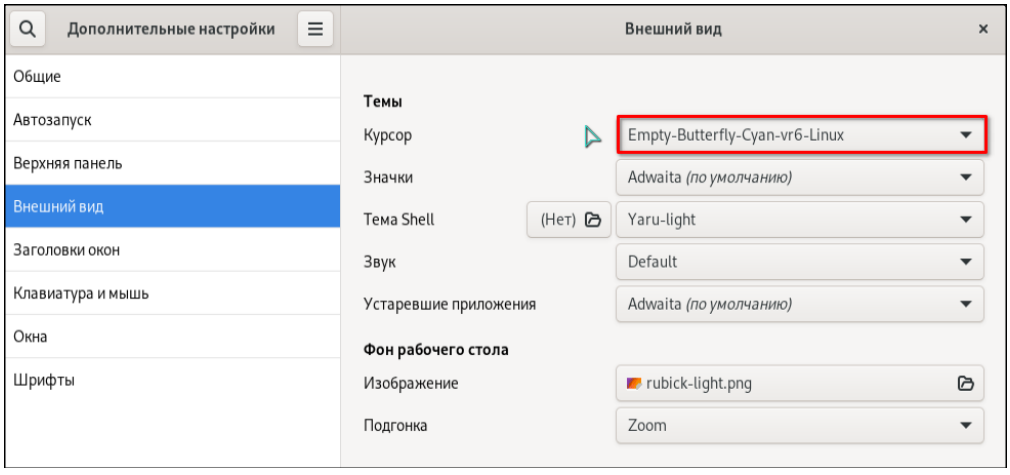
12. Скопируйте каталог темы курсора в /usr/share/icons/ (потребуются права **администратора**). Папка /**icons** предназначена для тем иконок и курсоров.

```
sudo cp -r ./Empty-Butterfly-Cyan-vr6 /usr/share/icons/
```

Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

13. Закройте терминал и перейдите в «**Дополнительные настройки**» — «**Внешний вид**». Выберите установленную тему курсора. Новая тема будет применена автоматически.



Установка новых тем значков (иконок)

Для добавления новых значков (иконок) рабочего стола можно установить доступные в репозитории пакеты через терминал или через менеджер пакетов **dnfdragora**.

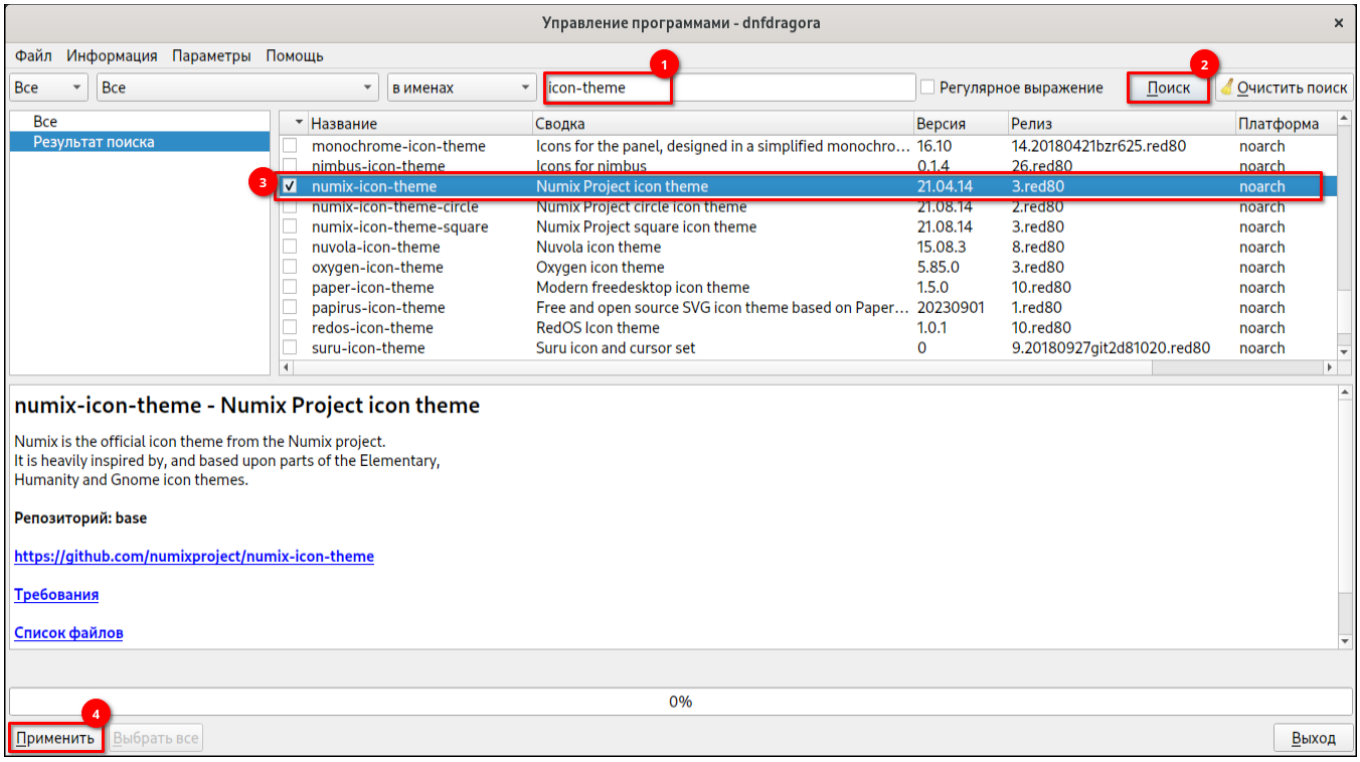
Для поиска новых тем значков через терминал выполните команду:

```
dnf search icon-theme
```

Из появившегося списка выберите нужную тему и воспользуйтесь командой для установки новой темы значков (потребуются права **администратора**), например:

```
dnf install numix-icon-theme
```

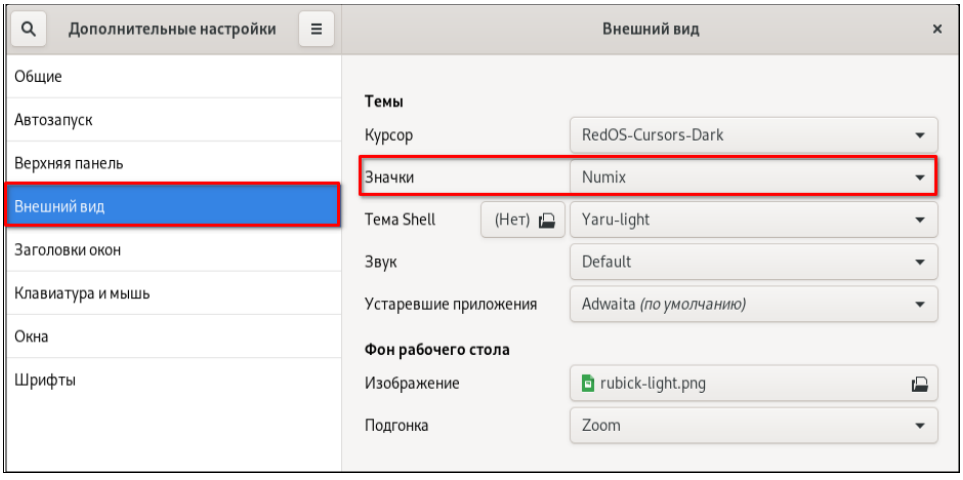
Для установки новой темы оформления значков рабочего стола через менеджер пакетов **dnfdragora** выполните поиск темы по шаблону — «**icon-theme**», выберите из списка актуальную версию пакета и нажмите кнопку « **Применить**».



Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

Для применения новой темы оформления значков рабочего стола перейдите в «**Дополнительные настройки**» — «**Внешний вид**». Выберите установленную тему значков. Новая тема будет применена автоматически.

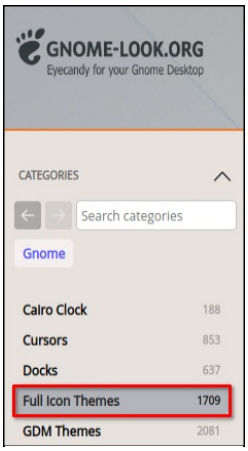


Установка дополнительных тем значков (иконок)

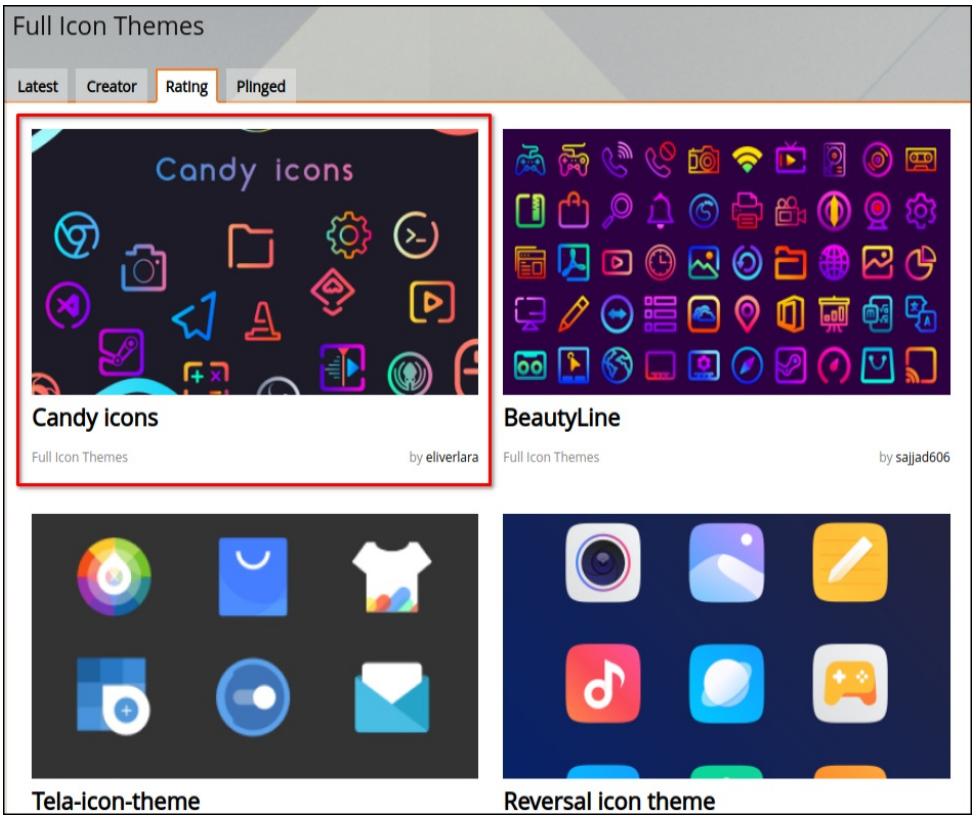
Для установки сторонней темы и добавления ее в список доступных выполните следующий алгоритм действий:

1. Перейдите на сайт https://www.gnome-look.org.

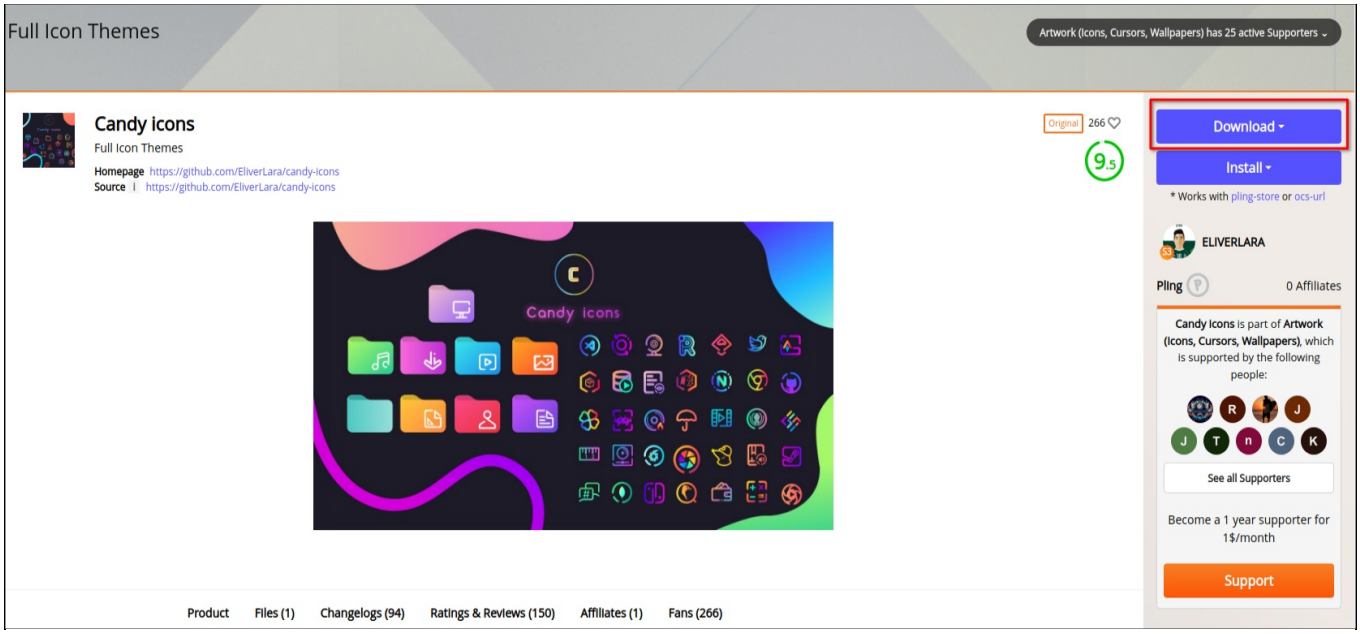
2. На левой боковой панели выберите категорию иконок «**Full Icon Themes**».



3. Выберите из списка понравившуюся тему значков и щелкните ЛКМ по ней.

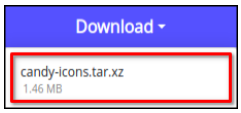


4. Для загрузки понравившейся темы иконок нажмите «**Download**».

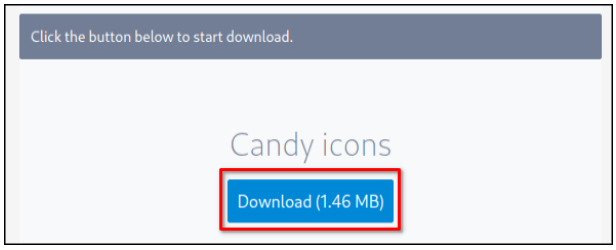


5. По нажатии на кнопку «**Download**» будет открыт список с доступным цветовым оформлением. Выберите любое цветовое

оформление.



6. Начнется подготовка архива к скачиванию. Когда архив станет доступен для скачивания, нажмите на активную кнопку «**Download**». Архив будет сохранен в каталог загрузок (в примере /home/user/Загрузки/).



7. Откройте терминал и перейдите в каталог с загруженными архивами тем (в примере /home/user/Загрузки/):

```
cd /home/user/Загрузки/
```

8. Распакуйте архив с основной темой с помощью команды:

```
tar -xvf ./candy-icons.tar.xz
```

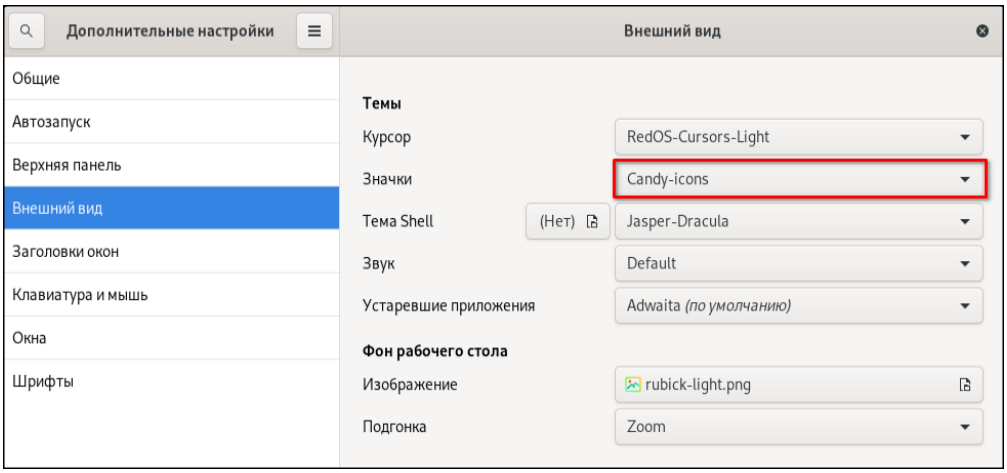
9. Скопируйте распакованный каталог темы в /usr/share/icons/ (потребуются права **администратора**):

```
sudo cp -r ./candy-icons /usr/share/icons/
```

Примечание.

После установки новых тем оформления может потребоваться перезагрузка системы.

10. Закройте терминал и перейдите в «**Дополнительные настройки**» — «**Внешний вид**». Выберите установленную тему значков.

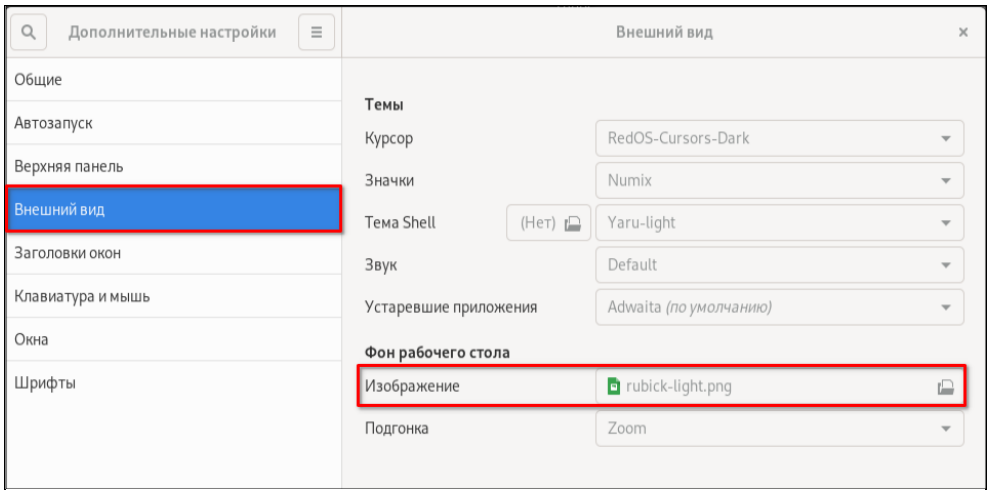


Новая тема будет применена автоматически.

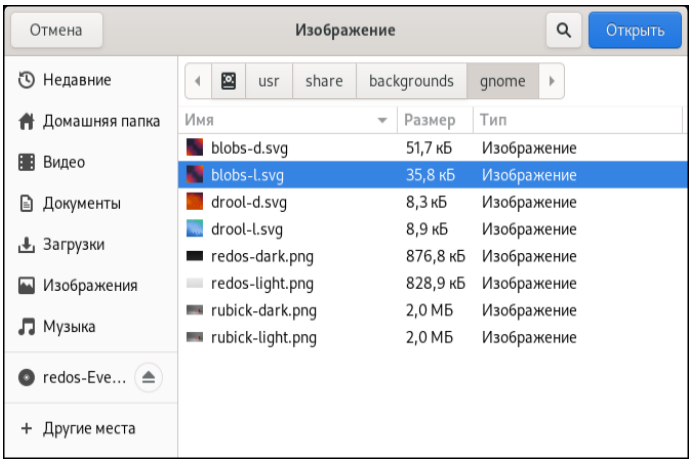


Установка нового фона рабочего стола

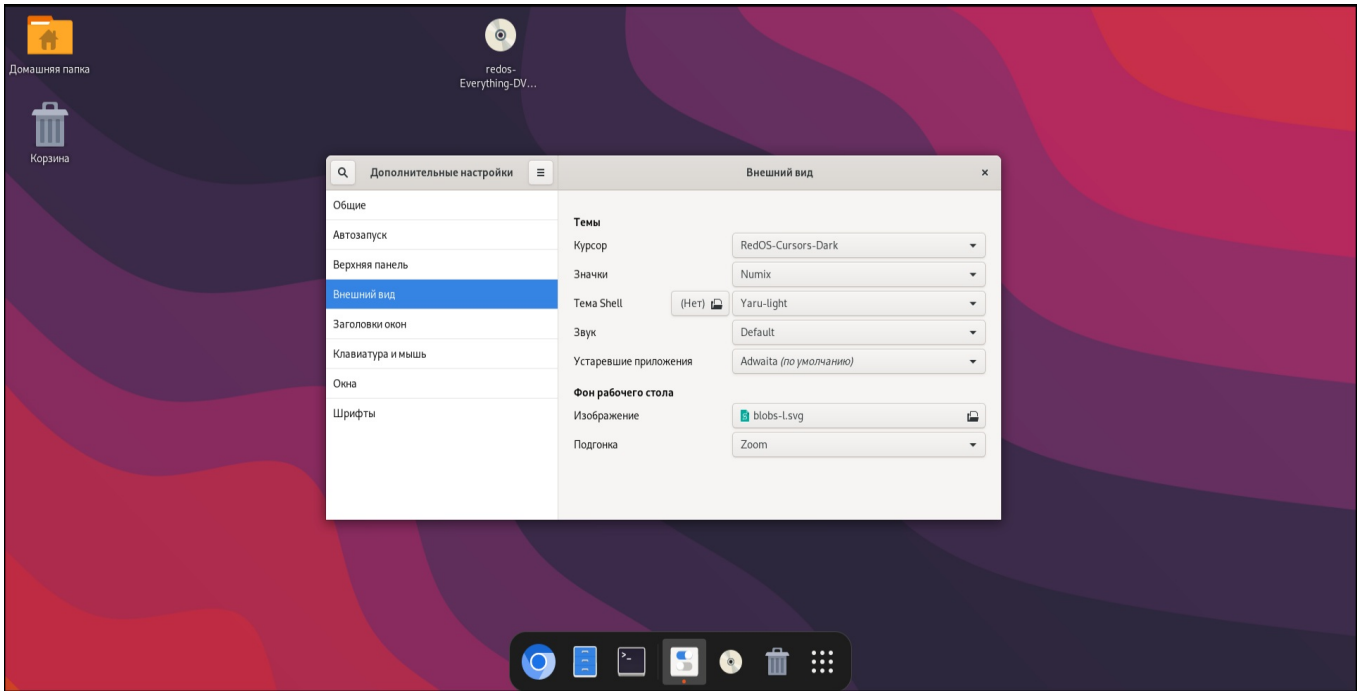
Для смены фона рабочего стола пользователю необходимо перейти в «**Дополнительные настройки**» — «**Внешний вид**». В блоке «**Фон рабочего стола**» можно выбрать изображение из имеющихся или скачать и установить новое.



Изображения для фона рабочего стола хранятся в папке **/usr/share/backgrounds/gnome/**.



Выбранное изображение автоматически будет установлено в качестве фона рабочего стола.



Тема оформления рабочего стола WindowsLike

Установка
Переключение на WindowsLike
Возвращение настроек по умолчанию
Переключение на WindowsLike со стандартной темы РЕД ОС
Переключение на WindowsLike с предварительно настроенной темы РЕД ОС
Переключение на стандартную тему РЕД ОС
Возвращение настроек по умолчанию
Переключение на РЕД ОС со стандартной темы WindowsLike
Переключение на РЕД ОС с предварительно настроенной темы WindowsLike

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: redos-wintheme-switcher-0.2.0-1

Для удобства и быстрой адаптации пользователей при переходе на РЕД ОС была разработана новая тема оформления рабочего стола – **WindowsLike**. Стиль новой темы оформления схож со стилем темы оформления ОС Windows 11.

Для корректного применения новой темы оформления дополнительно была разработана специальная утилита – **redos-wintheme-switcher**, которая позволяет переключать стандартный стиль темы оформления **РЕД ОС** на новую тему оформления **WindowsLike** и обратно. Под стандартным стилем темы оформления РЕД ОС подразумевается настраиваемая по умолчанию при установке РЕД ОС 8 с графическим окружением KDE тема оформления.

Примечание.

Утилита **redos-wintheme-switcher** может быть установлена только в **РЕД ОС 8** с графическим окружением **KDE**.

Вы можете подробнее ознакомиться с возможностью переключения на новую тему оформления **WindowsLike**, просмотрев наши обучающие видео:

- на **RuTube** — Установка темы оформления WindowsLike в РЕД ОС 8 KDE;
- в **Яндекс.Дзен** — Установка темы оформления WindowsLike в РЕД ОС 8 KDE;
- в **VK Видео** — Установка темы оформления WindowsLike в РЕД ОС 8 KDE.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

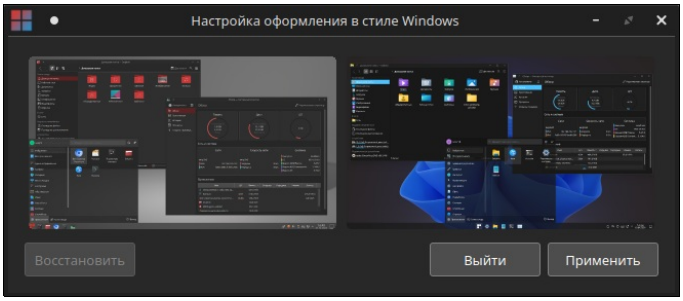
Для установки утилиты настройки оформления в стиле Windows выполните команду (потребуются права **администратора**):

```
sudo dnf install redos-wintheme-switcher
```

Дальнейшая работа с утилитой производится с правами обычного (непривилегированного) пользователя.

После установки запуск утилиты доступен из «**Меню запуска приложений**» – «**Настройка**» – «**Настройка оформления в стиле Windows**».

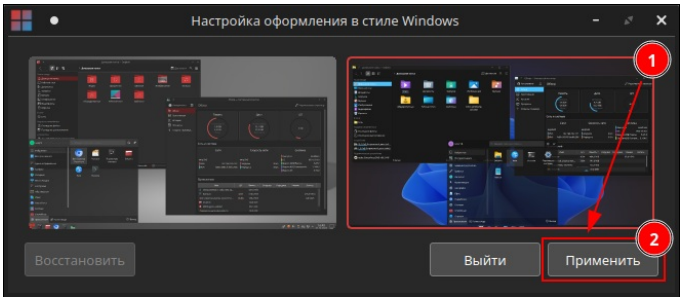
Окно утилиты настройки оформления в стиле Windows выглядит следующим образом:



Переключение на WindowsLike

В окне утилиты настройки оформления в стиле Windows справа расположена кнопка выбора новой темы оформления **WindowsLike**.

Для применения новой темы **WindowsLike** выберите соответствующий вариант (1) и нажмите кнопку «**Применить**» (2).



Переключение на новую тему оформления **WindowsLike** возможно в следующих случаях:

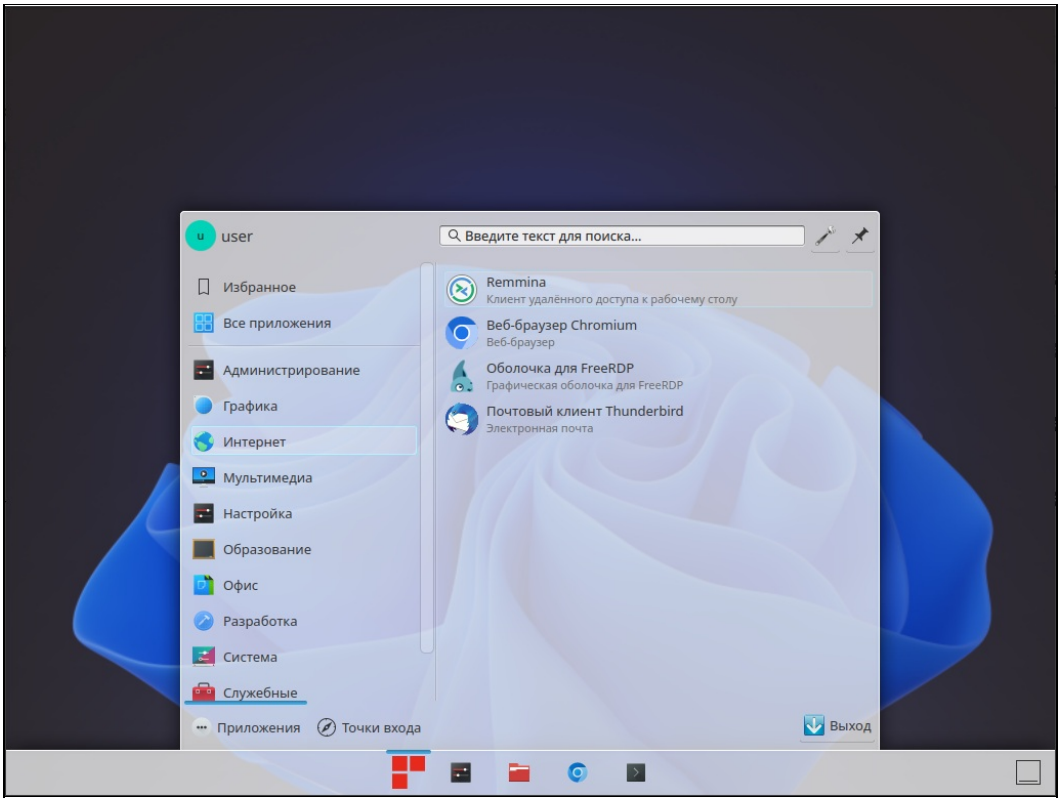
- возвращение настроек по умолчанию для измененной пользователем темы оформления **WindowsLike**;
- переключение на стандартную тему оформления **WindowsLike** со стандартной темы оформления **РЕД ОС**;
- переключение на стандартную тему оформления **WindowsLike** с измененной пользователем темы оформления **РЕД ОС**.

Далее будут рассмотрены указанные варианты переключения на стандартную тему оформления **WindowsLike**.

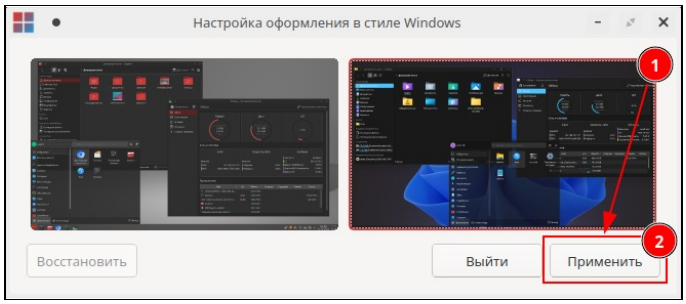
Возвращение настроек по умолчанию

В рассматриваемом примере были внесены следующие изменения в оформление среды рабочего стола:

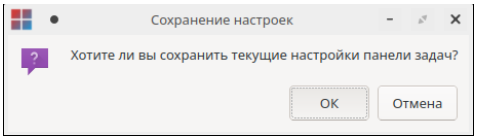
- оформление рабочей среды изменено на «**РЕД ОС Светлая**» (по умолчанию используется «**WindowsLike Темная**»);
- оформление приложений изменено на «**Adwaita**» (по умолчанию используется «**Lightly**»);
- оформление рабочего стола изменено на «**Air**» (по умолчанию используется «**WindowsLikeDark**»);
- с системной панели удалены некоторые виджеты.



Для возвращения темы оформления рабочего стола к настройкам по умолчанию откройте утилиту «**Настройка оформления в стиле Windows**», выберите стандартную тему оформления **WindowsLike** и нажмите «**Применить**».



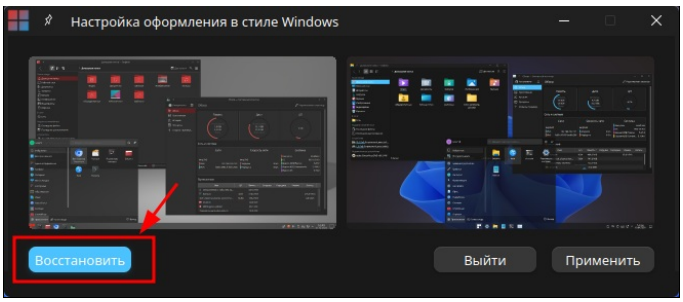
При этом будет выведен запрос на сохранение текущих настроек системной панели. Для сохранения настроек нажмите «**OK**», в противном случае нажмите «**Отмена**».



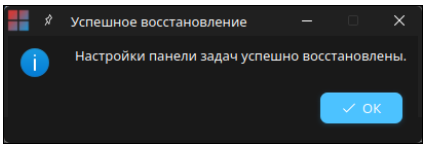
Тема оформления будет возвращена к настройкам по умолчанию.



В случае если настройки панели задач были предварительно сохранены, их можно восстановить в установленной теме оформления. Для этого откройте утилиту «**Настройка оформления в стиле Windows**» и нажмите на активную кнопку «**Восстановить**».



Будет запущен процесс восстановления настроек системной панели. По завершении восстановления настроек будет выведено соответствующее информационное сообщение. Нажмите «**OK**», чтобы закрыть окно.

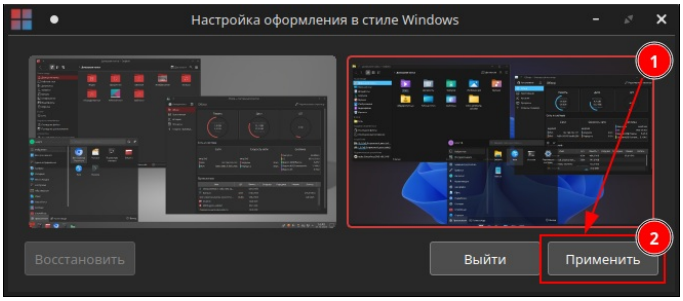


Оформление системной панели успешно восстановлено.

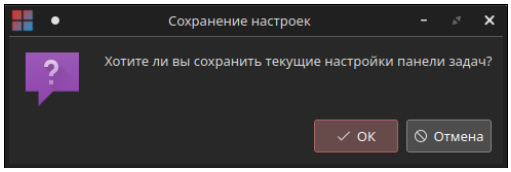


Переключение на WindowsLike со стандартной темы РЕД ОС

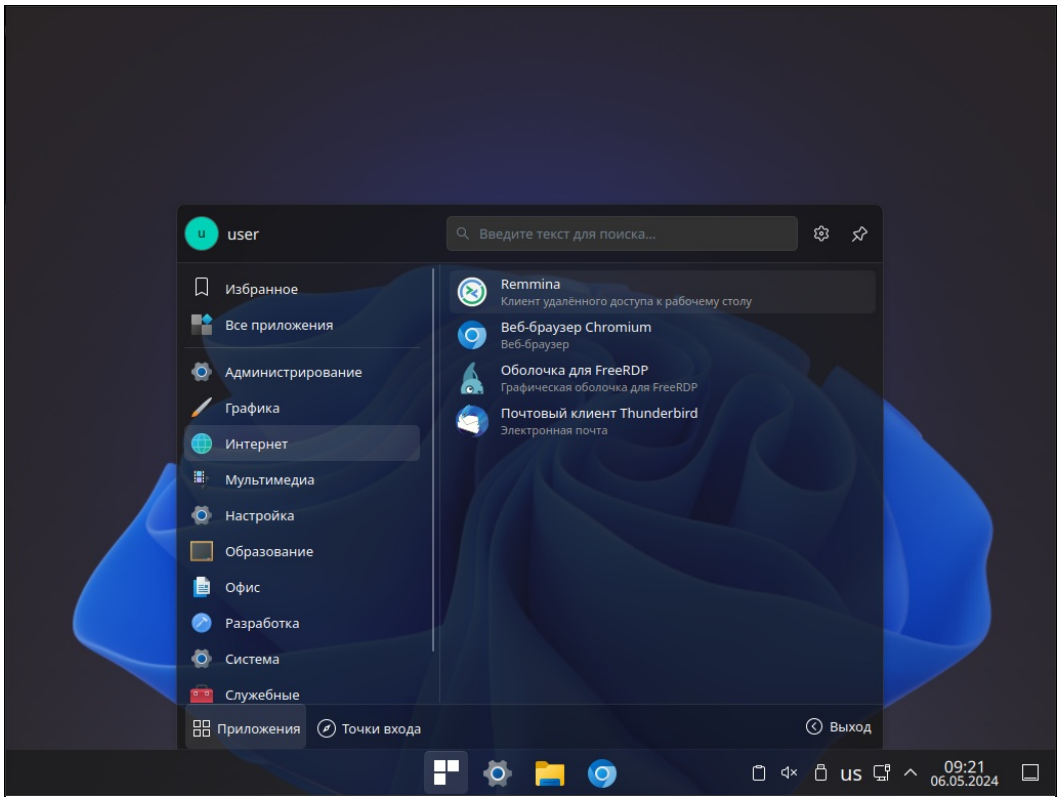
Для переключения на новую тему оформления WindowsLike со стандартной (не измененной пользователем) темы оформления РЕД ОС откройте утилиту «**Настройка оформления в стиле Windows**», выберите новую тему оформления (1) и нажмите «**Применить**» (2).



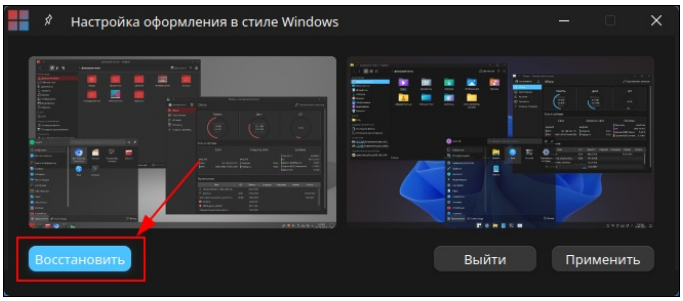
При этом будет выведен запрос на сохранение текущих настроек системной панели. Для сохранения настроек нажмите «**OK**», в противном случае нажмите «**Отмена**».



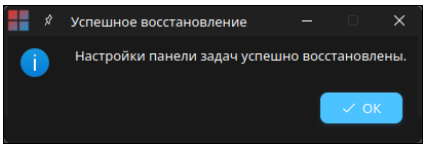
Новая тема оформления рабочего стола будет успешно применена.



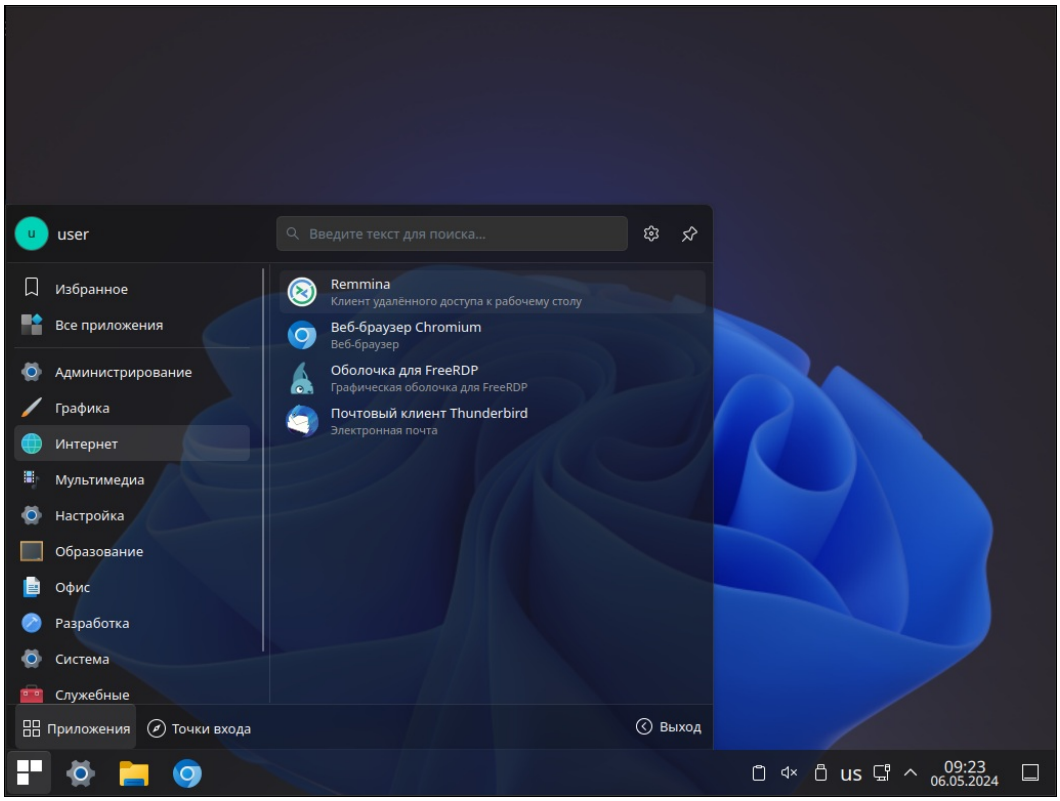
В случае если настройки панели задач были предварительно сохранены, их можно восстановить в установленной теме оформления. Для этого откройте утилиту «**Настройка оформления в стиле Windows**» и нажмите на активную кнопку «**Восстановить**».



Будет запущен процесс восстановления настроек системной панели. По завершении восстановления настроек будет выведено соответствующее информационное сообщение. Нажмите «**OK**», чтобы закрыть окно.



Оформление системной панели успешно восстановлено.

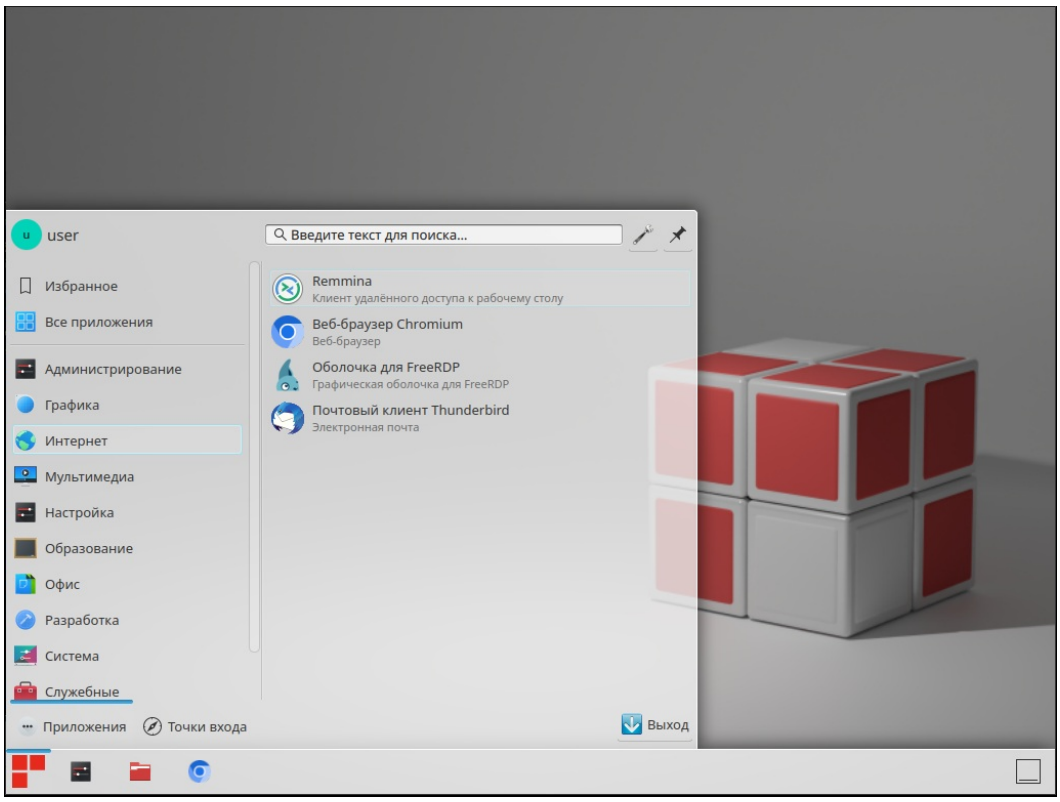


Переключение на WindowsLike с предварительно настроенной темы РЕД ОС

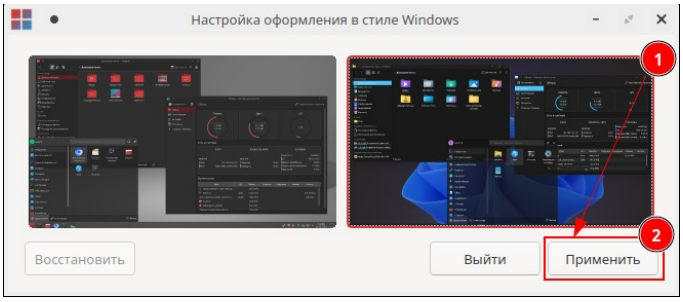
При переключении предварительно настроенной пользователем темы оформления рабочего стола **РЕД ОС** на стандартную тему **WindowsLike** будут восстановлены настройки по умолчанию.

В рассматриваемом примере были внесены следующие изменения в оформление среды рабочего стола:

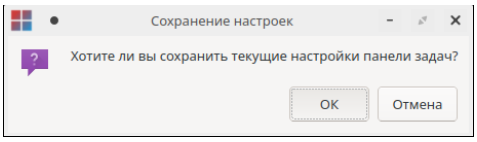
- оформление рабочей среды изменено на «**РЕД ОС Светлая**» (по умолчанию используется «**WindowsLike Темная**»);
- оформление приложений изменено на «**Adwaita**» (по умолчанию используется «**Lightly**»);
- оформление рабочего стола изменено на «**Air**» (по умолчанию используется «**WindowsLikeDark**»);
- с системной панели удалены некоторые виджеты.



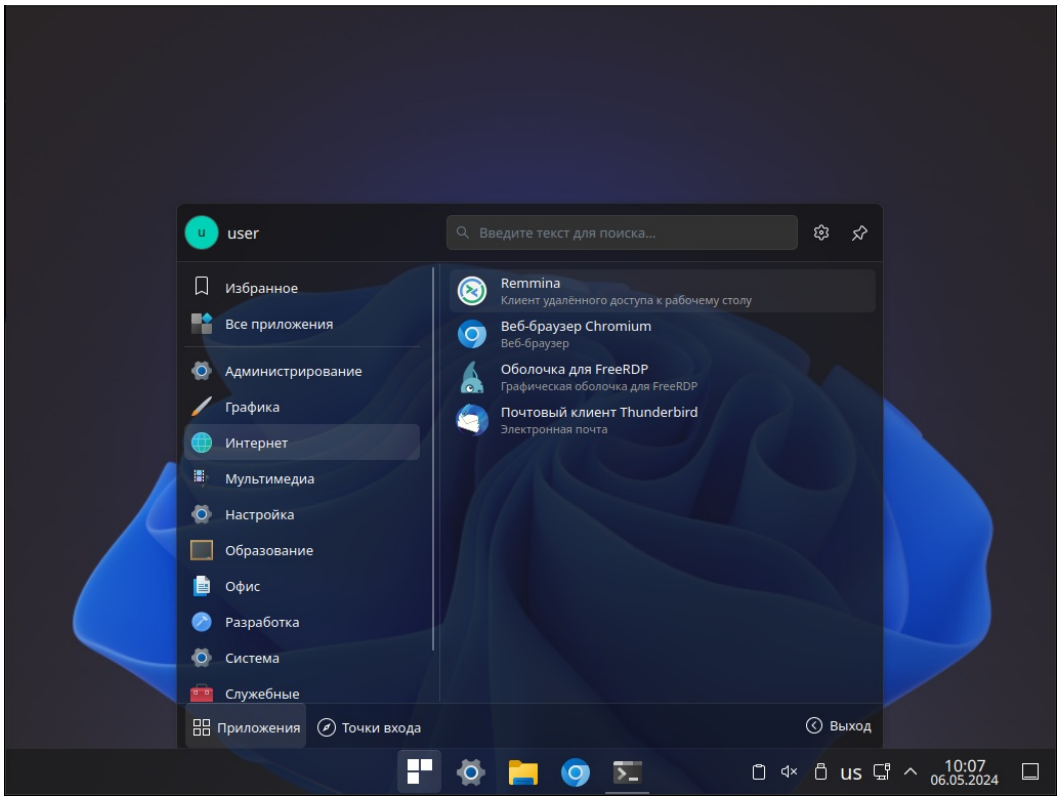
Для переключения на новую тему оформления **WindowsLike** с настроенной пользователем темы оформления РЕД ОС откройте утилиту «**Настройка оформления в стиле Windows**», выберите новую тему оформления **WindowsLike** (1) и нажмите «**Применить**» (2).



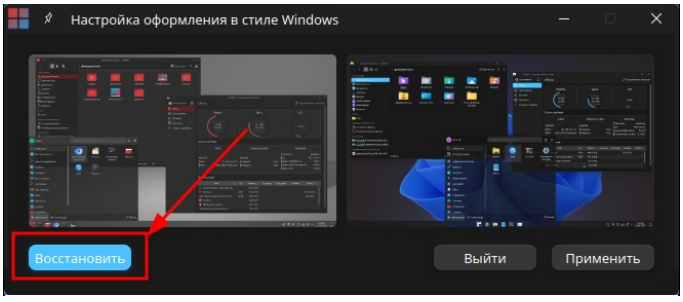
При этом будет выведен запрос на сохранение текущих настроек системной панели. Для сохранения настроек нажмите «**OK**», в противном случае нажмите «**Отмена**».



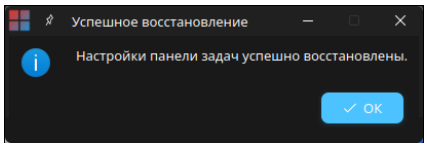
В процессе применения новой темы оформления **WindowsLike** все предыдущие настройки будут сброшены. Тема оформления будет успешно применена.



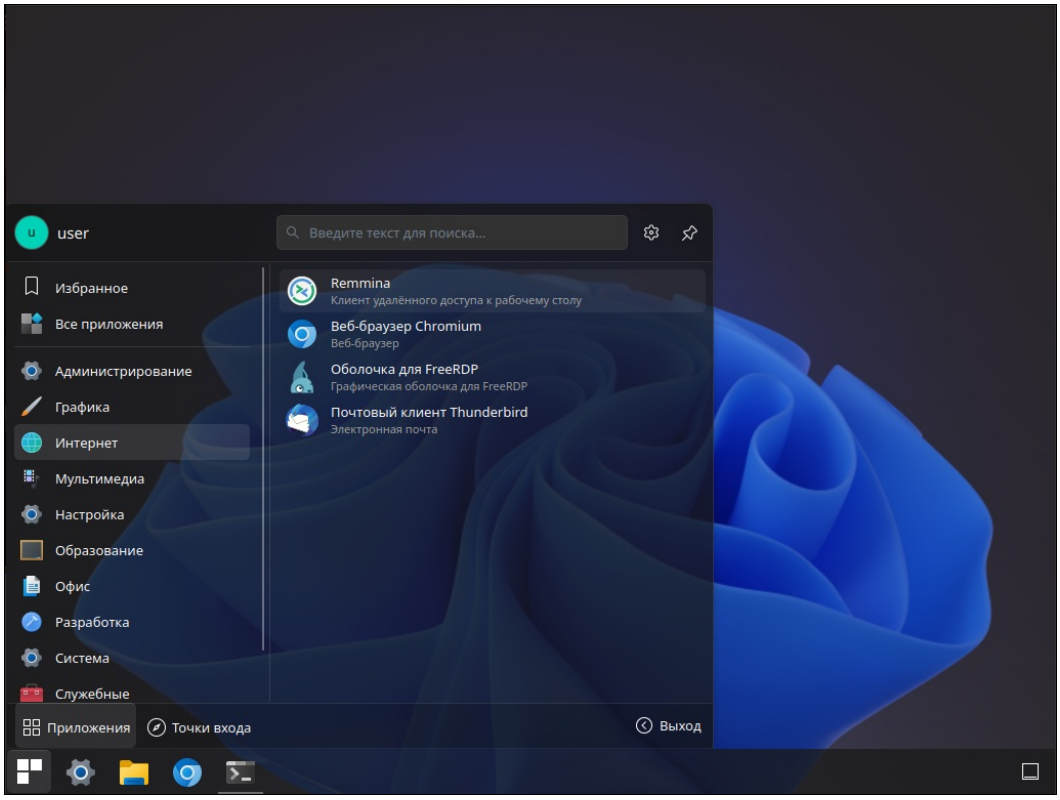
В случае если настройки панели задач были предварительно сохранены, их можно восстановить в установленной теме оформления. Для этого откройте утилиту «**Настройка оформления в стиле Windows**» и нажмите на активную кнопку «**Восстановить**».



Будет запущен процесс восстановления настроек системной панели. По завершении восстановления настроек будет выведено соответствующее информационное сообщение. Нажмите «**OK**», чтобы закрыть окно.



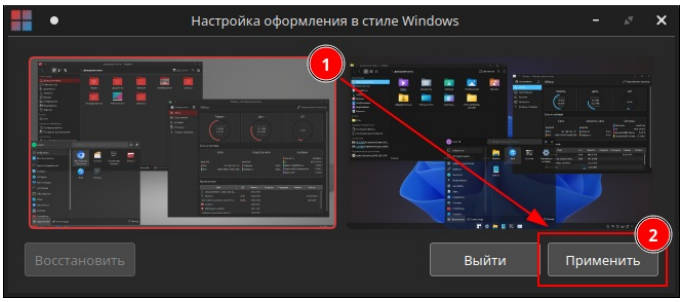
Оформление системной панели успешно восстановлено.



Переключение на стандартную тему РЕД ОС

В окне утилиты настройки оформления в стиле Windows слева расположена кнопка выбора стандартной темы РЕД ОС.

Для применения стандартной темы РЕД ОС выберите соответствующий вариант (1) и нажмите кнопку «**Применить**» (2).



Переключение на стандартную тему оформления РЕД ОС возможно в следующих ситуациях:

- возвращение настроек по умолчанию для измененной пользователем темы оформления РЕД ОС;
- переключение на стандартную тему оформления РЕД ОС со стандартной темы оформления *WindowsLike*;
- переключение на стандартную тему оформления РЕД ОС с измененной пользователем темы оформления *WindowsLike*.

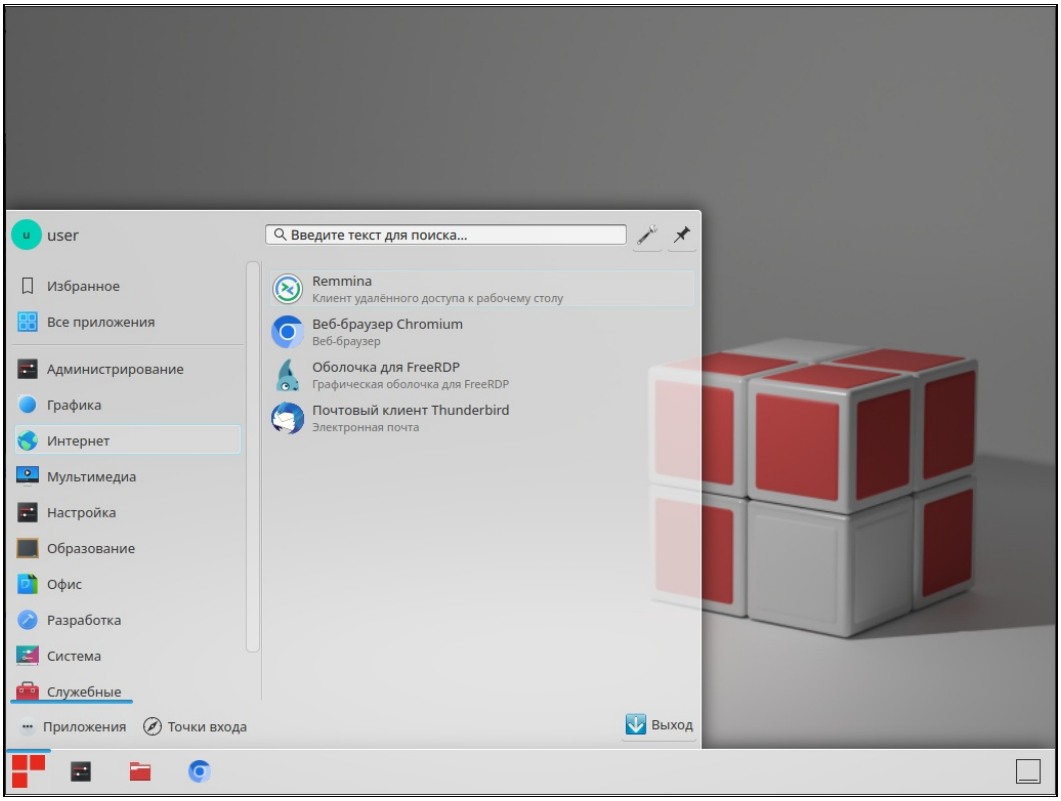
Далее будут рассмотрены указанные варианты переключения на стандартную тему оформления РЕД ОС.

Возвращение настроек по умолчанию

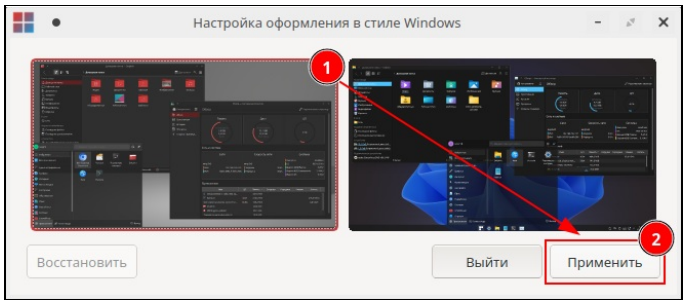
В рассматриваемом примере были внесены следующие изменения в оформление среды рабочего стола:

- оформление рабочей среды изменено на «**РЕД ОС Светлая**» (по умолчанию используется «**РЕД ОС Темная**»);
- оформление приложений изменено на «**Adwaita**» (по умолчанию используется «**Breeze**»);

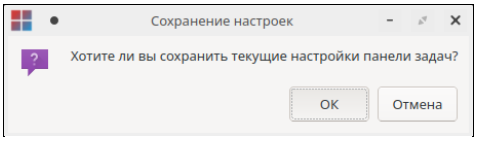
- оформление рабочего стола изменено на «**Air**» (по умолчанию используется «**РЕД ОС**»);
- с системной панели удалены некоторые виджеты.



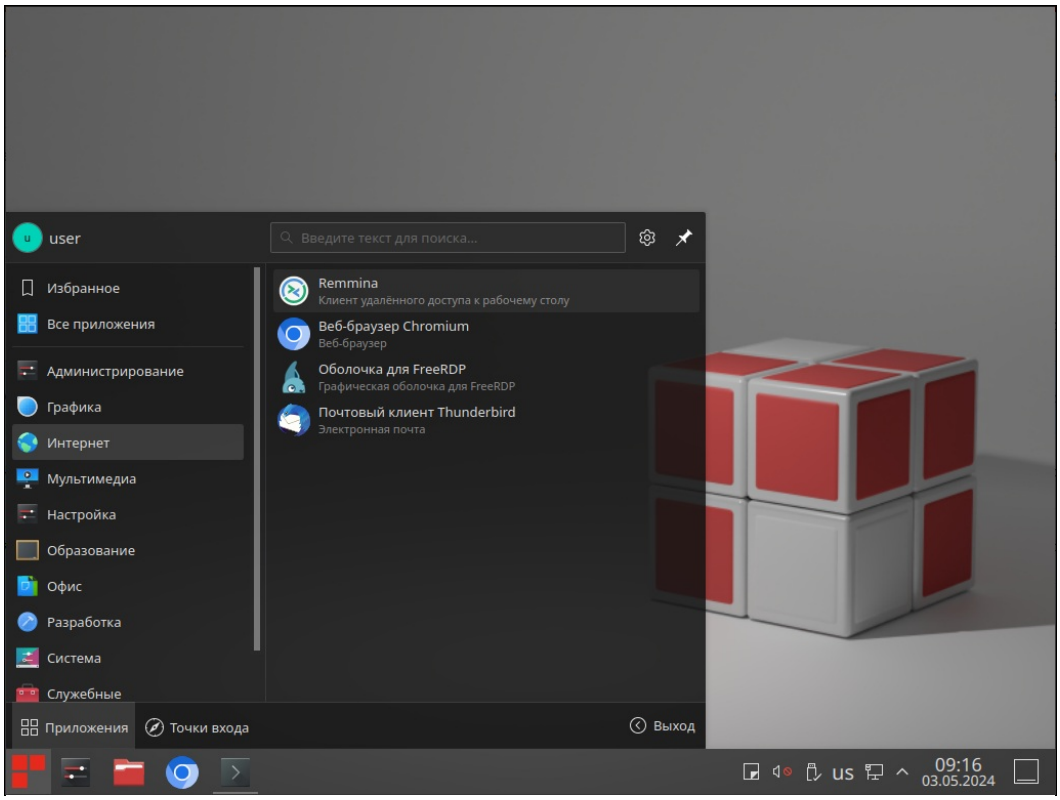
Для возвращения темы оформления рабочего стола к настройкам по умолчанию откройте утилиту «**Настройка оформления в стиле Windows**», выберите стандартную тему оформления РЕД ОС и нажмите « **Применить**».



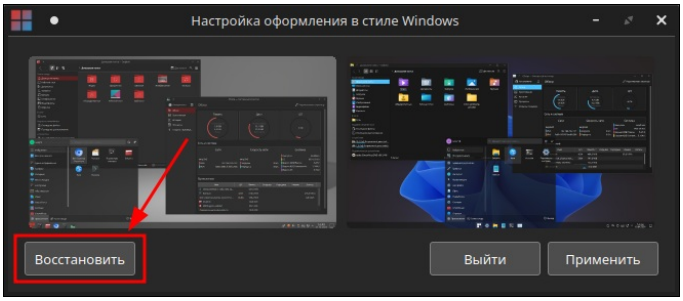
При этом будет выведен запрос на сохранение текущих настроек системной панели. Для сохранения настроек нажмите «**OK**», в противном случае нажмите «**Отмена**».



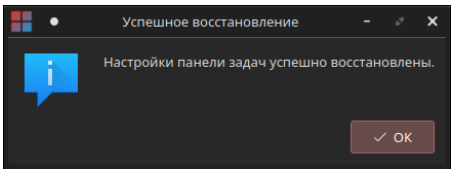
Тема оформления будет возвращена к настройкам по умолчанию.



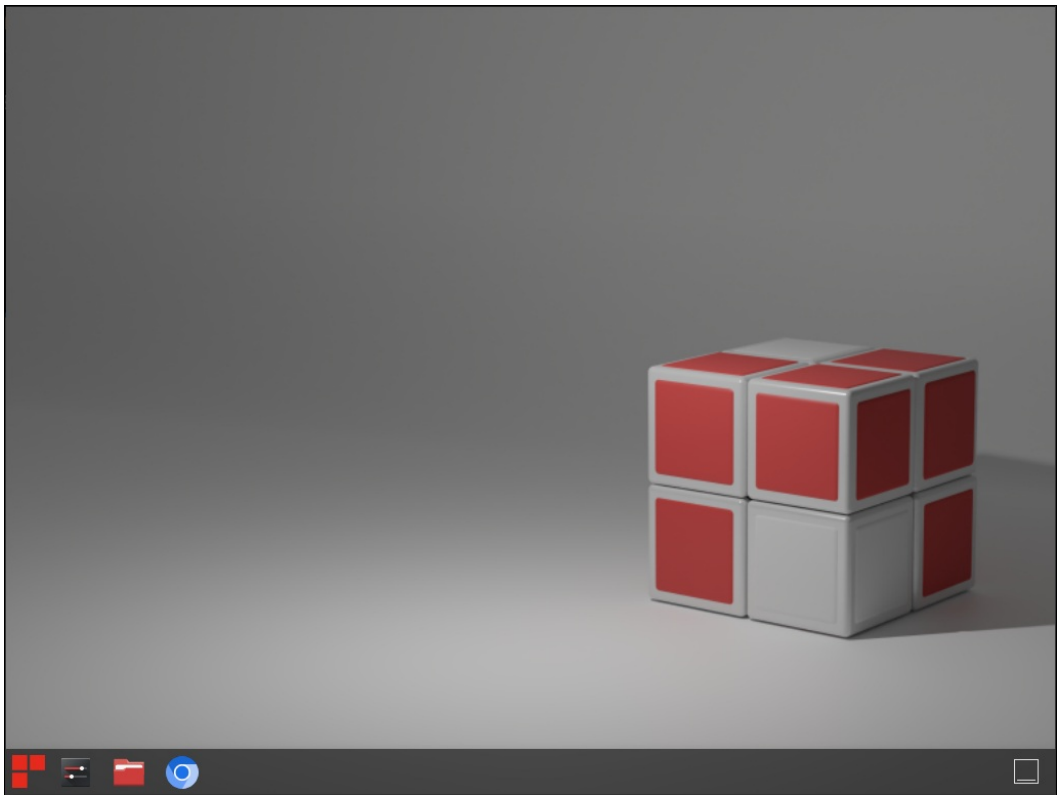
В случае, если настройки панели задач были предварительно сохранены, их можно восстановить в установленной теме оформления. Для этого откройте утилиту «**Настройка оформления в стиле Windows**» и нажмите на активную кнопку «**Восстановить**».



Будет запущен процесс восстановления настроек системной панели. По завершении восстановления настроек будет выведено соответствующее информационное сообщение. Нажмите «**OK**», чтобы закрыть окно.

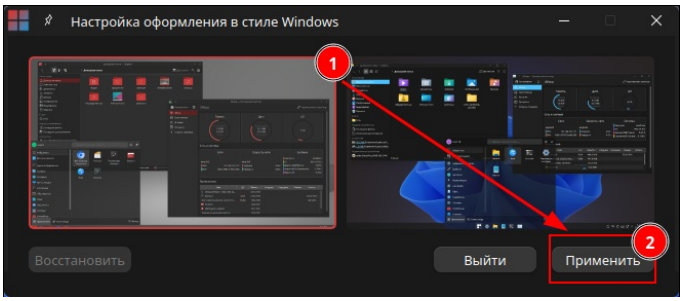


Оформление системной панели успешно восстановлено.

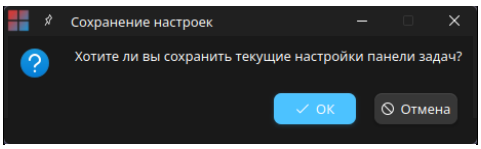


Переключение на РЕД ОС со стандартной темы WindowsLike

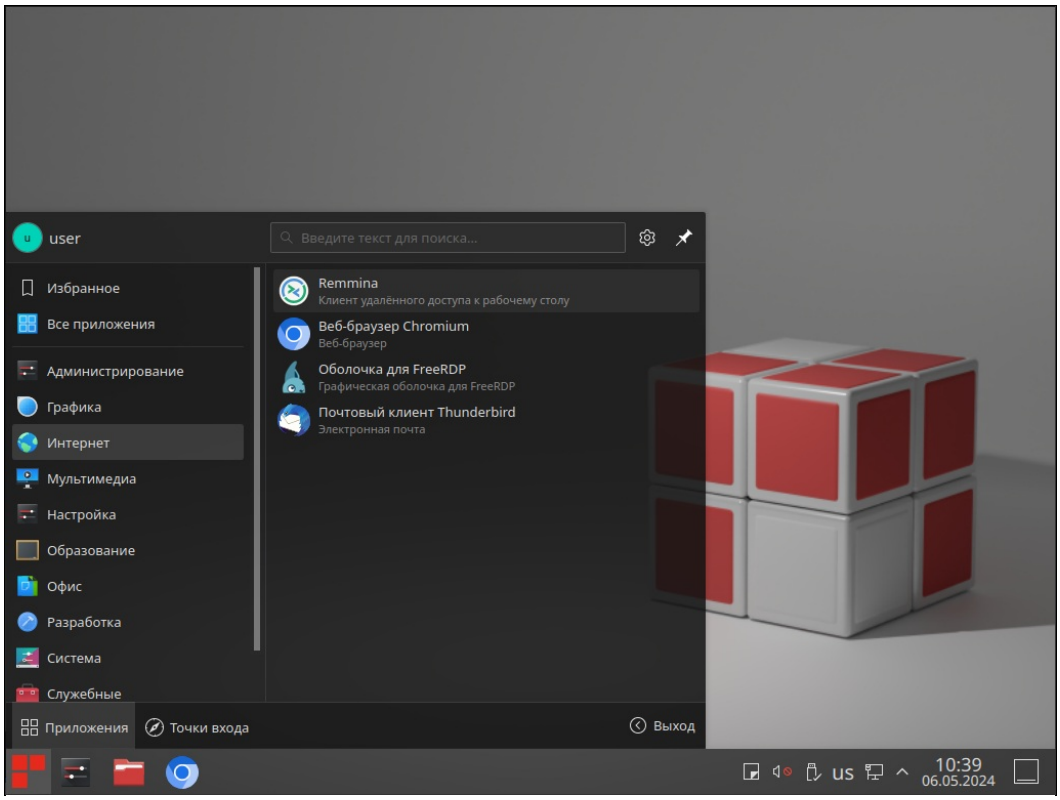
Для переключения на стандартную тему оформления РЕД ОС со стандартной (не измененной пользователем) темы оформления WindowsLike откройте утилиту «**Настройка оформления в стиле Windows**», выберите тему оформления РЕД ОС (1) и нажмите «**Применить**» (2).



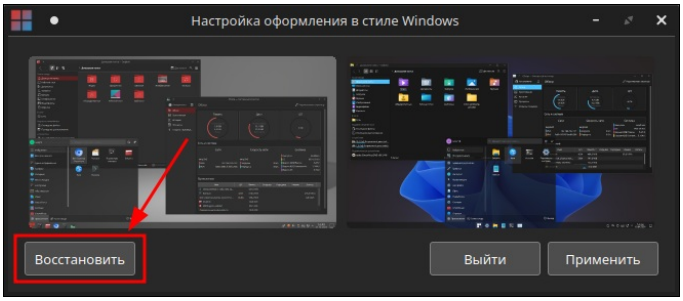
При этом будет выведен запрос на сохранение текущих настроек системной панели. Для сохранения настроек нажмите «**ОК**», в противном случае нажмите «**Отмена**».



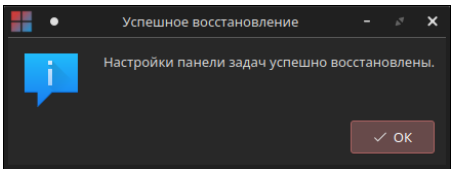
Стандартная тема оформления рабочего стола **РЕД ОС** будет успешно применена.



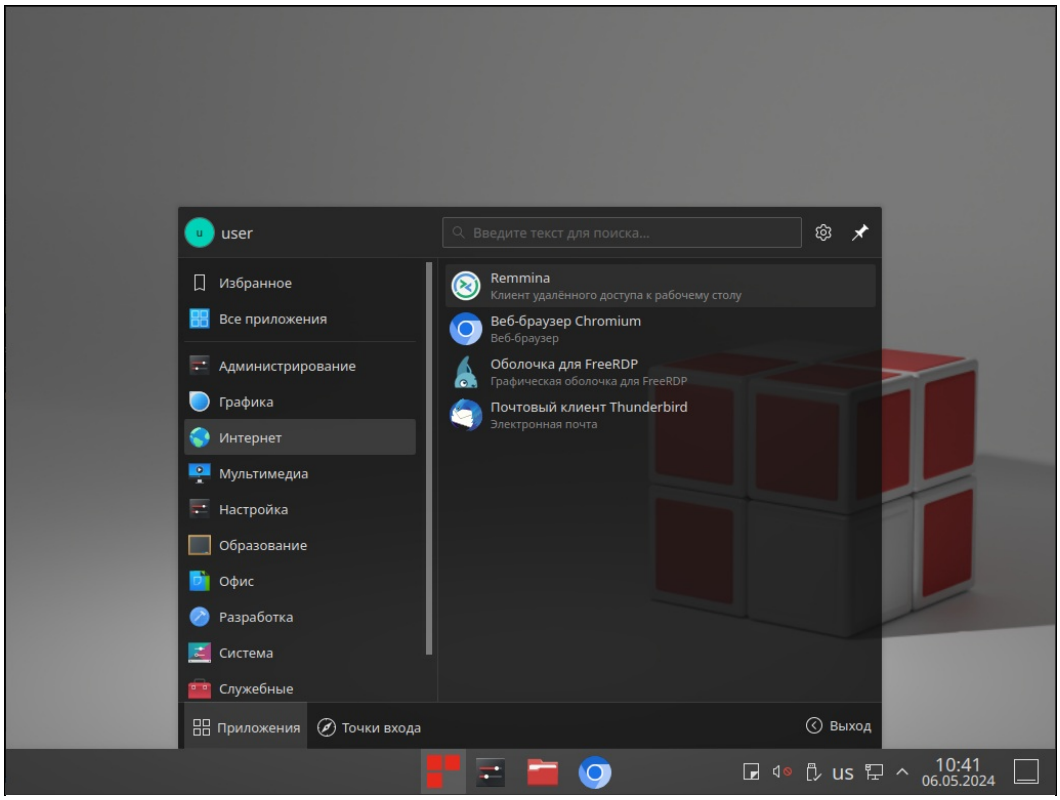
В случае, если настройки панели задач были предварительно сохранены, их можно восстановить в установленной теме оформления. Для этого откройте утилиту «**Настройка оформления в стиле Windows**» и нажмите на активную кнопку «**Восстановить**».



Будет запущен процесс восстановления настроек системной панели. По завершении восстановления настроек будет выведено соответствующее информационное сообщение. Нажмите «**OK**», чтобы закрыть окно.



Оформление системной панели успешно восстановлено.

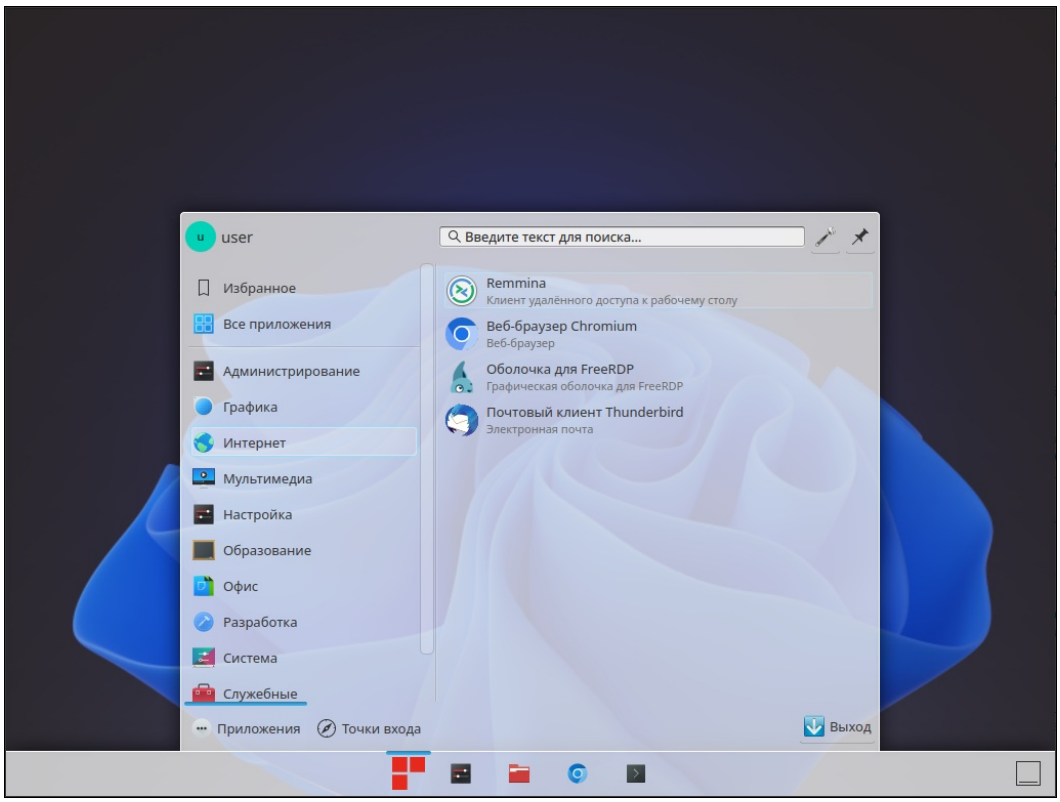


Переключение на РЕД ОС с предварительно настроенной темы WindowsLike

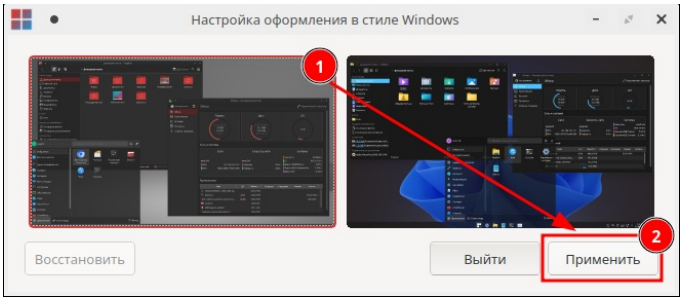
При переключении предварительно настроенной пользователем темы оформления рабочего стола **WindowsLike** на стандартную тему **РЕД ОС** будут восстановлены настройки по умолчанию.

В рассматриваемом примере были внесены следующие изменения в оформление среды рабочего стола:

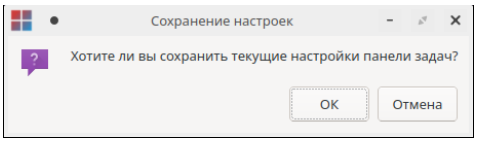
- оформление рабочей среды изменено на «**РЕД ОС Светлая**» (по умолчанию используется «**WindowsLike Темная**»);
- оформление приложений изменено на «**Adwaita**» (по умолчанию используется «**Lightly**»);
- оформление рабочего стола изменено на «**Air**» (по умолчанию используется «**WindowsLikeDark**»);
- с системной панели удалены некоторые виджеты.



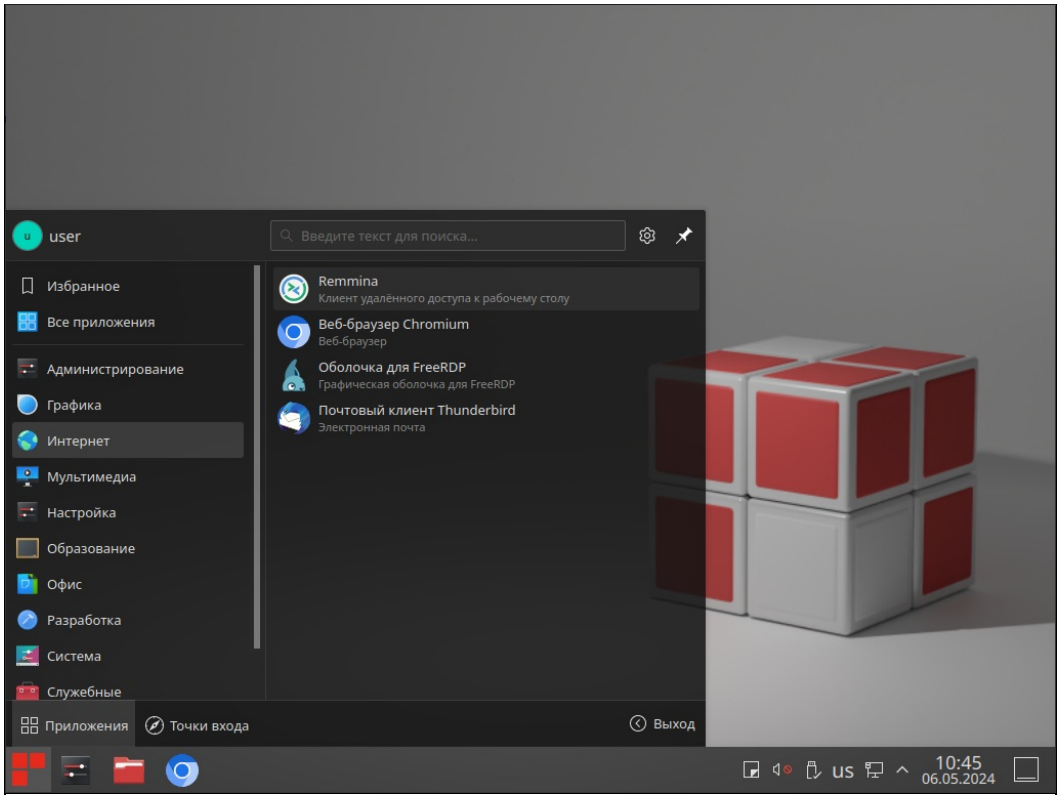
Для переключения темы оформления рабочего стола на стандартную тему **РЕД ОС** откройте утилиту «**Настройка оформления в стиле Windows**», выберите стандартную тему оформления **РЕД ОС** и нажмите «**Применить**».



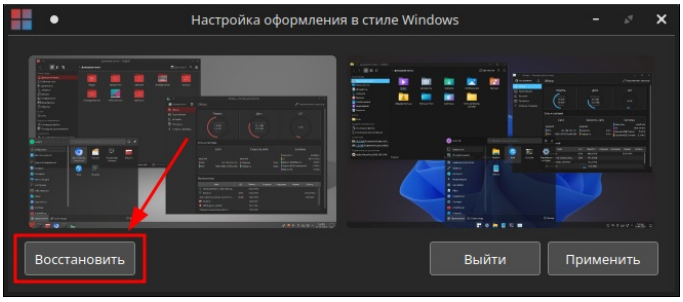
При этом будет выведен запрос на сохранение текущих настроек системной панели. Для сохранения настроек нажмите «**OK**», в противном случае нажмите «**Отмена**».



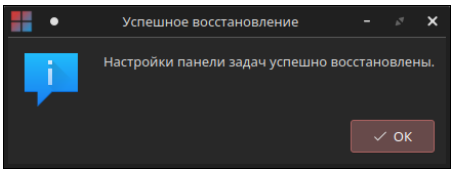
Тема оформления будет успешно применена.



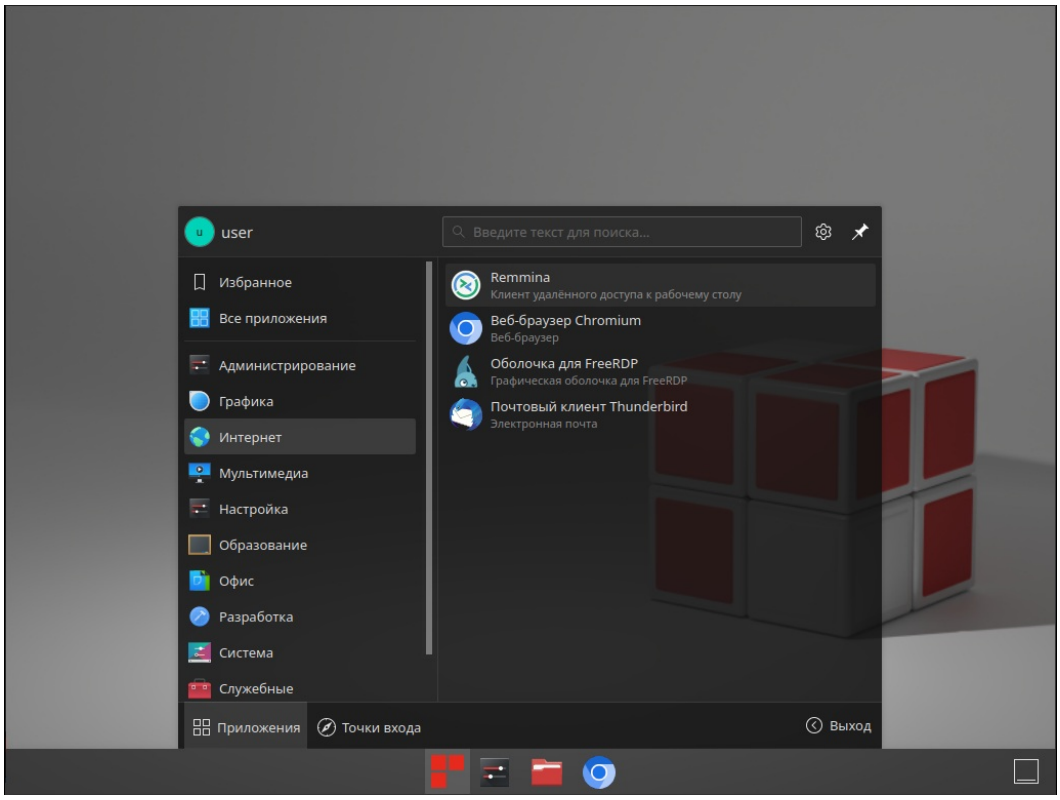
В случае, если настройки панели задач были предварительно сохранены, их можно восстановить в установленной теме оформления. Для этого откройте утилиту «**Настройка оформления в стиле Windows**» и нажмите на активную кнопку «**Восстановить**».



Будет запущен процесс восстановления настроек системной панели. По завершении восстановления настроек будет выведено соответствующее информационное сообщение. Нажмите «**OK**», чтобы закрыть окно.



Оформление системной панели успешно восстановлено.



Работа пользователя в РЕД ОС

Общие положения
Домашняя папка пользователя
Работа с папками и файлами
Пакет офисных приложений по работе с документами
Работа с мультимедиа
Средства коммуникации
Справочная система РЕД ОС

Вы можете подробнее ознакомиться с работой в системе, просмотрев наши обучающие видео:

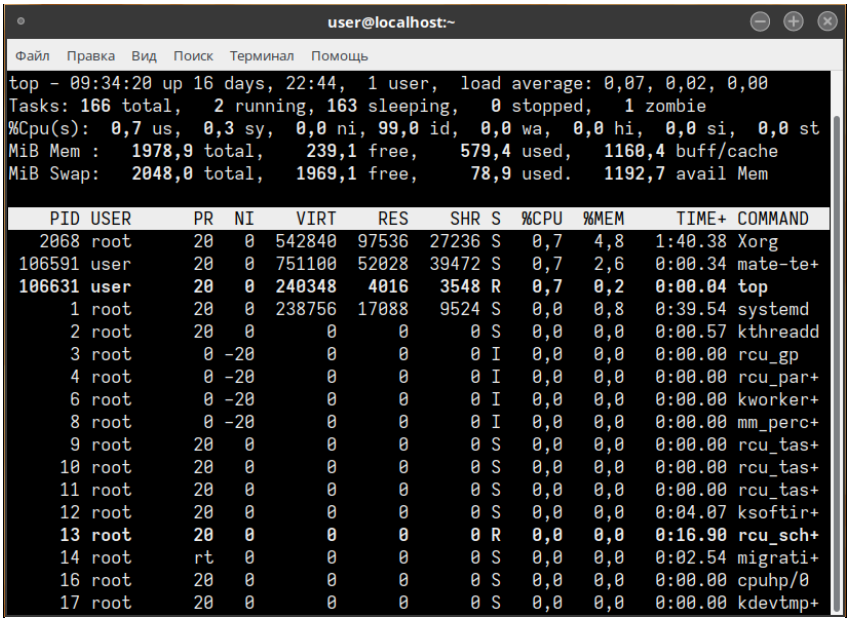
- на **RuTube** — РЕД ОС “Рабочая станция” в повседневных задачах;
- в **Яндекс.Дзен** — РЕД ОС “Рабочая станция” в повседневных задачах;
- в **VK Видео** — РЕД ОС “Рабочая станция” в повседневных задачах.

На наших каналах вы также сможете найти много другой полезной информации.

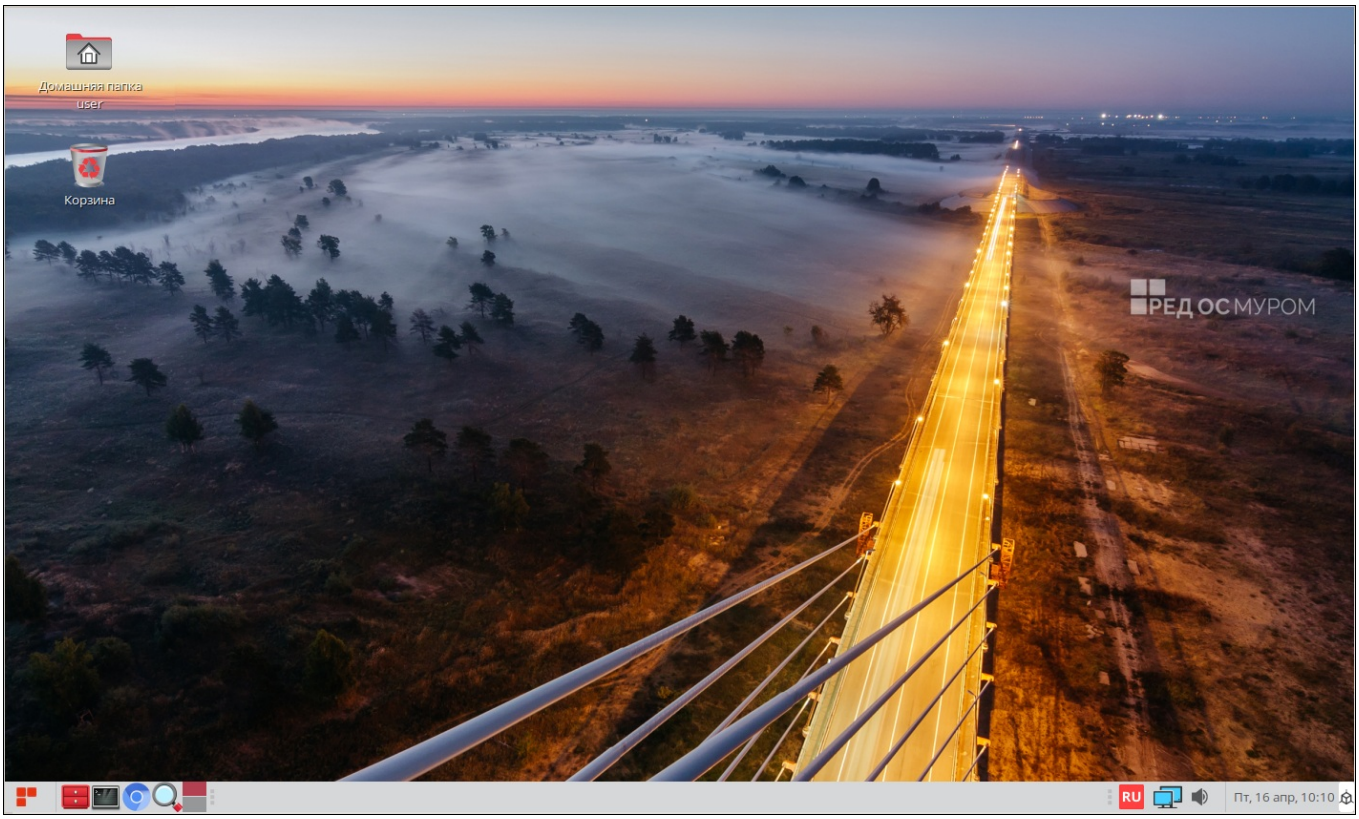
Общие положения

Работа пользователя в РЕД ОС может осуществляться в двух режимах: консольный режим и графический режим.

Консольный режим применяется в ограниченных случаях использования устаревшего программного обеспечения, конфигурирования РЕД ОС или невозможности старта графического сервера из-за сбоев РЕД ОС. Для консольного режима основным средством управления РЕД ОС является командная строка, в которой пользователь может вводить команды управления РЕД ОС. Результаты выполнения команд выводятся в консоли в виде текстовых или псевдографических сообщений.



Основным режимом работы пользователя в РЕД ОС является **графический** режим. Работа пользователя в графическом режиме производится на рабочем столе. Рабочий стол для каждого пользователя настраивается индивидуально. Настройки рабочего стола хранятся в **домашней папке** пользователя.



Навигационное пространство рабочего стола РЕД ОС состоит из трёх зон управления:

- **Системная панель** – панель, расположенная по умолчанию в нижней части экрана. Системная панель обеспечивает доступ пользователя к глобальному меню запуска всех установленных программ, содержит апплеты и элементы управления работой РЕД ОС;
- **Рабочее пространство** – все свободное пространство рабочего стола, предназначенное для расположения файлов данных и ярлыков часто используемых программ. Рабочее пространство может быть оформлено фоном рабочего стола;
- **Панель программ Mate** – панель, расположенная по умолчанию в нижней части экрана. В этой панели отображаются иконки уже запущенных программ, а также апплеты рабочих столов и корзины файлов и документов.

Управление графическим интерфейсом РЕД ОС пользователь может осуществлять при помощи мыши или клавиатуры. Правая клавиша мыши по умолчанию используется для вызова контекстных свойств любого графически представленного в интерфейсе РЕД ОС объекта. Левая клавиша мыши по умолчанию используется для инициации действий с любым графическим объектом в интерфейсе РЕД ОС.

Общие методы работы пользователя с графическим интерфейсом РЕД ОС являются общепринятыми методами работы пользователей с графическими интерфейсами операционных систем. Основными элементами графического интерфейса РЕД ОС являются окна, панели, кнопки, меню, поля ввода, списки выбора, апплеты, радиокнопки, скроллеры и т.д.

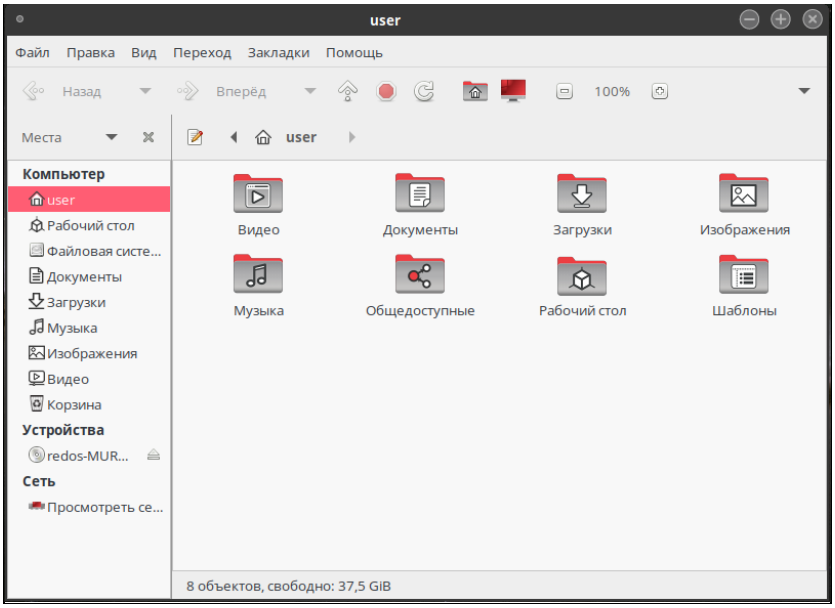
Вы можете подробнее ознакомиться с возможностями графического окружения **MATE**, просмотрев наши обучающие видео:

- на **RuTube** — Основы работы с DE Mate;
- в **Яндекс.Дзен** — Основы работы с DE Mate.

На наших каналах вы также сможете найти много другой полезной информации.

Домашняя папка пользователя

Для каждого пользователя в РЕД ОС автоматически формируется домашняя папка пользователя, которая содержит файлы и папки с данными пользователя.



Домашняя папка содержит пользовательские конфигурационные данные (профили) сервисов и функций РЕД ОС. Имена папок, начинающихся с точки и имеют атрибут «**скрытый**». Например:

/home/ivanov/.cups
/home/ivanov/.config

В домашней папке для пользователя автоматически создаются папки для хранения различных широко распространённых типов файлов. Например: «**Документы**», «**Изображения**», «**Музыка**», «**Видео**».

Все домашние папки пользователей расположены в едином каталоге пользователей **/home**.

Имена домашних папок пользователей совпадают с именами (логинами) пользователей в системе. Например:

/home/ivanov/
/home/sorokina/
/home/kiselev/

Пользователь может перейти в домашнюю папку по ссылке (ярлыку) на рабочем столе.

Все программы в РЕД ОС по умолчанию сохраняют редактируемые пользователем файлы в домашнюю папку пользователя.

Пользователь имеет полный доступ к файлам и папкам в своём домашнем каталоге. Однако пользователь имеет ограниченный доступ к домашним папкам и файлам в них других пользователей.

Работа с папками и файлами

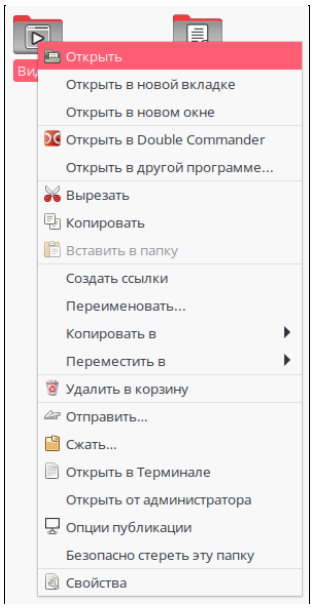
Помимо домашней папки пользователь может работать с файлами и папками в файловой системе РЕД ОС. Возможность работы с файлами и папками РЕД ОС определяется правами доступа пользователя, устанавливаемыми администратором РЕД ОС.

Пользователь может осуществлять работу с папками и файлами в РЕД ОС несколькими способами:

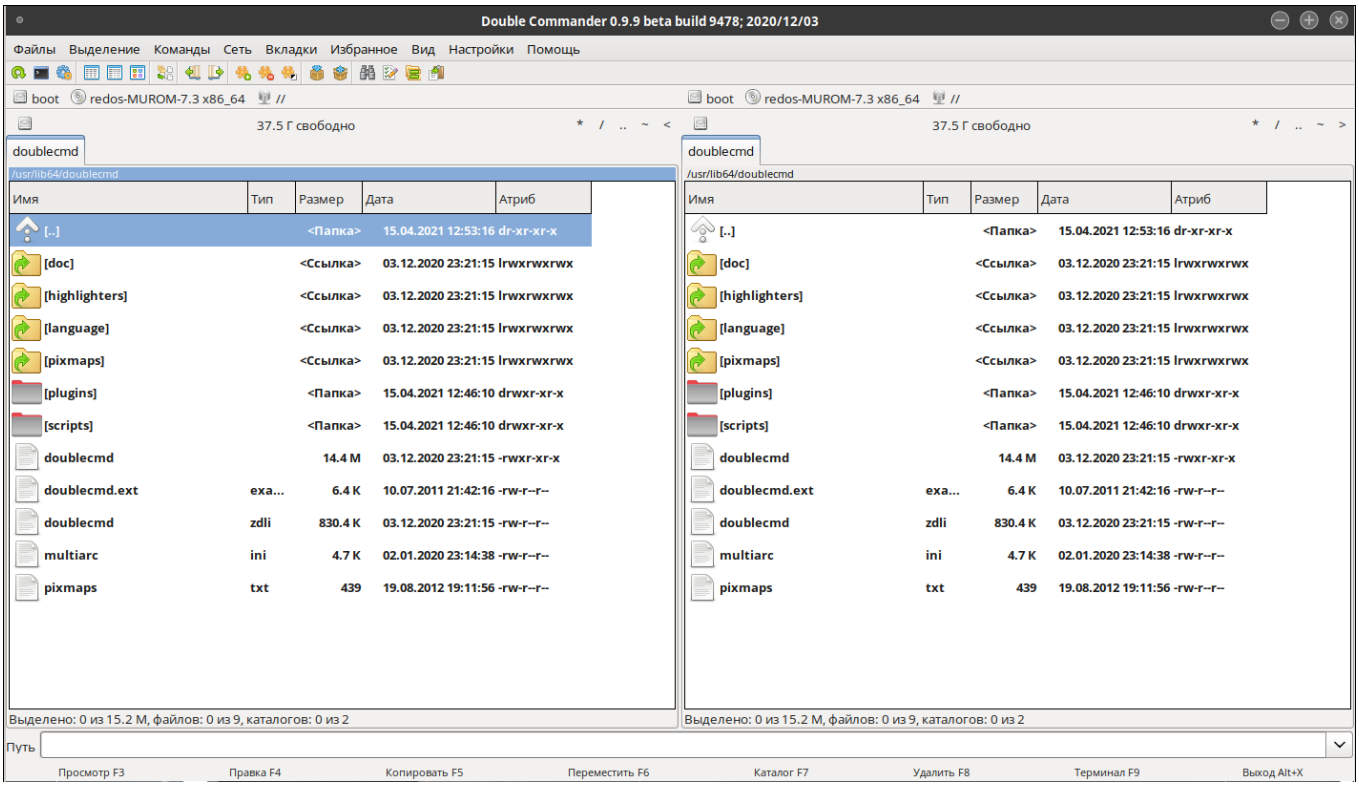
- при помощи стандартного менеджера файлов графического окружения;
- при помощи специализированных программ, например **MidnightCommander**.

После запуска менеджера файлов откроется окно, в котором пользователь может в графическом режиме перемещаться по файловой системе РЕД ОС и выполнять доступные операции с папками и файлами.

Действия с папками и файлами в стандартном обозревателе файлов выполняются при помощи мыши и клавиатуры. Стандартный обозреватель поддерживает технологию перетаскивания «мышью» (drag and drop). Доступные пользователю операции с файлами и папками можно увидеть в контекстном меню графического объекта при активации его правой функциональной клавишей мыши.

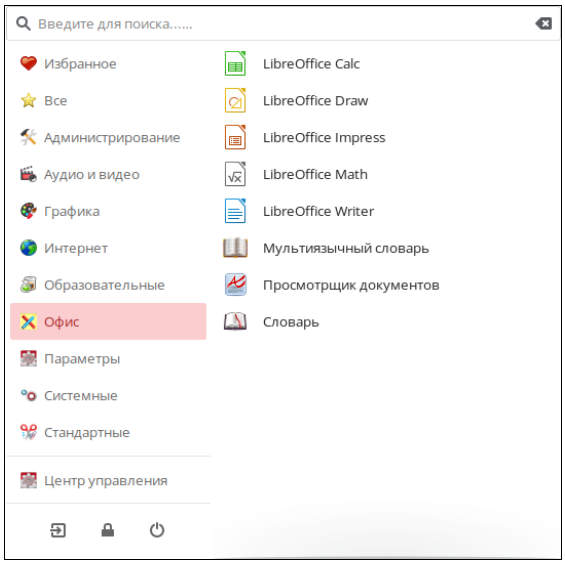


Управление файлами и папками пользователь также может совершать при помощи двухпанельных файловых менеджеров, таких как **MidnightCommander** или **Double Commander**.



Пакет офисных приложений по работе с документами

В качестве средств работы с текстовыми и табличными документами пользователю доступен пакет офисных приложений **LibreOffice**. Пакет офисных приложений доступен пользователю в «**Главном меню**» - «**Офис**».



В состав пакета включены следующие программные средства:

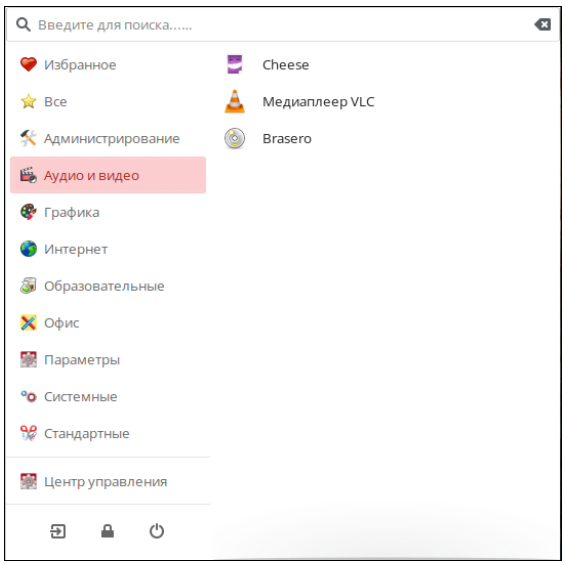
- *LibreOffice Calc* - табличный процессор;
- *LibreOffice Draw* - векторный графический редактор;
- *LibreOffice Impress* - программа подготовки презентаций;
- *LibreOffice Writer* - текстовый редактор и визуальный редактор HTML.

Пакет интегрирован в графическую оболочку РЕД ОС и автоматически открывается в случае, если пользователь производит запуск файла соответствующего формата.

Пакет полностью русифицирован и обеспечивает поддержку документов, созданных средствами различных текстовых и табличных редакторов, в том числе документы *Microsoft Word*.

Работа с мультимедиа

Пользователю в РЕД ОС для работы с мультимедиа-файлами доступен набор программ, который расположен в «**Главном меню**» - «**Аудио и видео**».



В состав пакетов для работы с мультимедиа-форматами по умолчанию включены следующие программные средства:

- приложение для записи дисков Brasero, который обеспечивает запись мультимедийных дисков и дисков с данными на оптические носители информации CD/DVD;
- фото-, видео-будка Cheese, которая обеспечивает работу с веб-камерами;
- утилита настройки звука.

Пакеты для работы с мультимедиа интегрированы в графическую оболочку РЕД ОС, и соответствующие приложения автоматически открываются в случае, если пользователь производит запуск файла определённого мультимедийного формата.

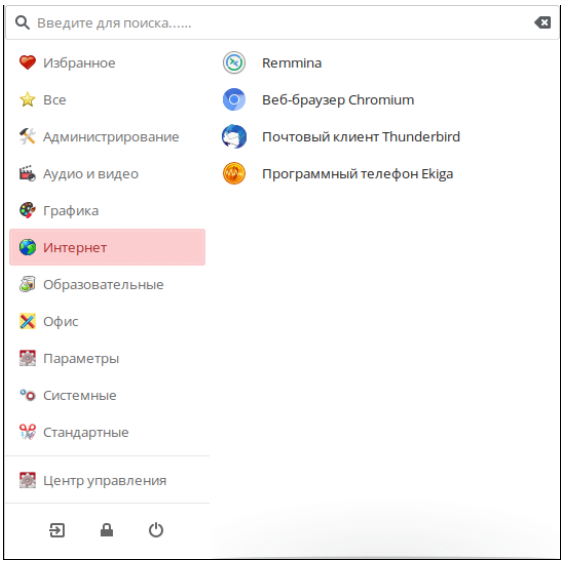
Для обеспечения возможности работы с некоторыми форматами требуется дополнительная установка кодеков мультимедийных

форматов. Установка дополнительных кодеков требует административных полномочий администратора РЕД ОС.

Описанные программные средства имеют интуитивно понятный интерфейс и снабжены контекстной справочной системой.

Средства коммуникации

Для обеспечения комфортной работы в сети Интернет в состав РЕД ОС включен набор необходимых приложений, доступный в «**Главном меню**» - «**Интернет**».



Remmina — это свободный клиент удаленного рабочего стола для компьютерных операционных систем. Он поддерживает протокол удаленного рабочего стола (RDP), протоколы VNC, NX, XDMCP, SPICE и SSH.

Chromium — веб-браузер с открытым исходным кодом, разрабатываемый сообществом The Chromium Authors, компанией Google и некоторыми другими компаниями. Chromium предназначен для предоставления пользователям быстрого, безопасного и надёжного доступа в Интернет, а также удобной платформы для веб-приложений.

Почтовый клиент **Thunderbird** — бесплатная кроссплатформенная свободно распространяемая программа для работы с электронной почтой и группами новостей, а при установке расширения Lightning - с календарём. Поддерживает протоколы: SMTP, POP3, IMAP, NNTP, RSS.

Ekiga — приложение для IP-телефонии и проведения видеоконференций, которое ранее называлось *GnomeMeeting*. **Ekiga** поддерживает протоколы **SIP** и **H.323** (с помощью **penH323**) и способна взаимодействовать с другими **SIP** и **H.323**-совместимыми клиентами, а также с *Microsoft NetMeeting*. Поддерживает множество аудио- и видеокодеков высокого качества.

Примечание.

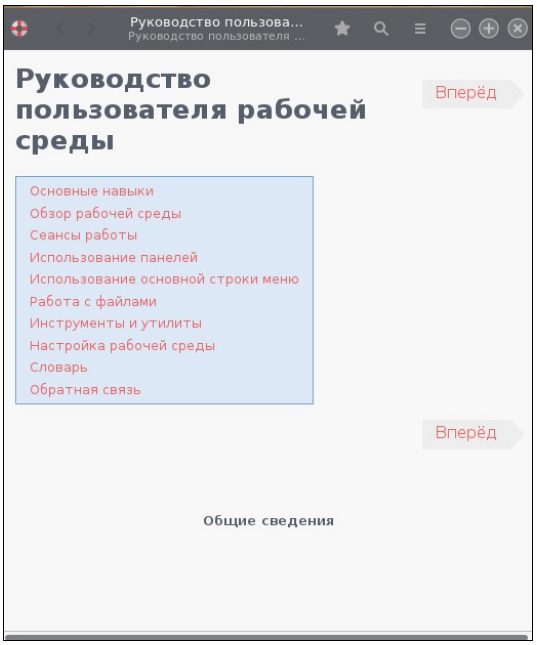
В **РЕД ОС 8** поддержка **Ekiga** прекращена. Для организации видеоконференций и звонков рекомендуется использовать кроссплатформенный программный клиент IP-телефонии **Linphone** или систему интернет-телефонии и мгновенного обмена сообщениями **Jitsi**.

Справочная система РЕД ОС

В РЕД ОС интегрирована расширенная справочная система, которая позволяет пользователю найти более подробную информацию по функциям и возможностям системы.

Доступ к справочной системе пользователю предоставляется при нажатии

правой кнопки мыши на системной панели и выборе пункта «Справка».


Руководство пользова...
Руководство пользователя ...
Руководство пользователя рабочей среды
Вперёд
Основные навыки
Обзор рабочей среды
Сеансы работы
Использование панелей
Использование основной строки меню
Работа с файлами
Инструменты и утилиты
Настройка рабочей среды
Словарь
Обратная связь
Вперёд
Общие сведения

Настройка среды рабочего стола

Установка
Работа с утилитой
Рабочий стол
Панель
Окна

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** mate-tweak 20.04.0-1

mate-tweak – утилита для точной настройки среды рабочего стола.

С ее помощью можно управлять значками рабочего стола и изменять настройки интерфейса для значков, контекстных меню или панелей инструментов.

Установка

Для установки перейдите в сеанс пользователя **root**:

```
su -
```

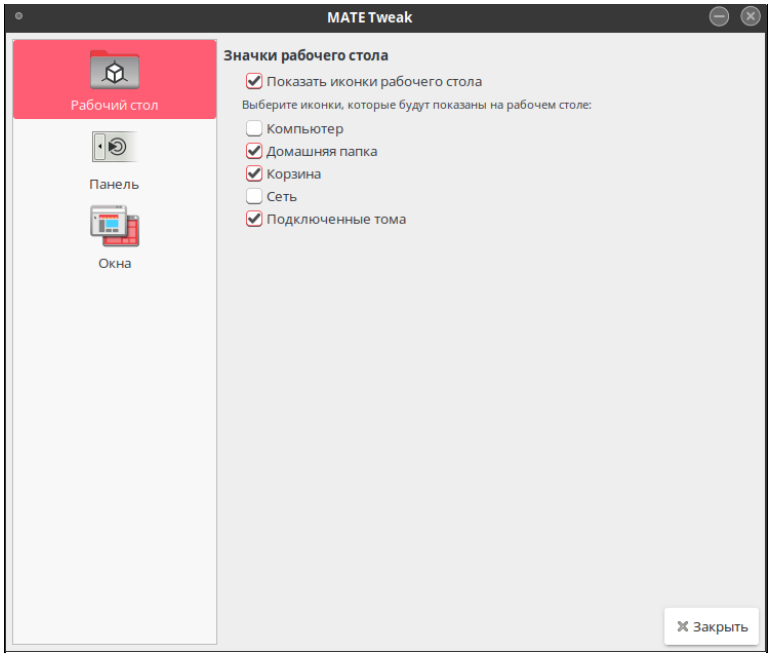
и выполните команду:

```
dnf install mate-tweak
```

После установки утилита доступна из «**Главного меню**» - «**Параметры**» - «**MATE Tweak**».

Работа с утилитой

Окно программы выглядит следующим образом:

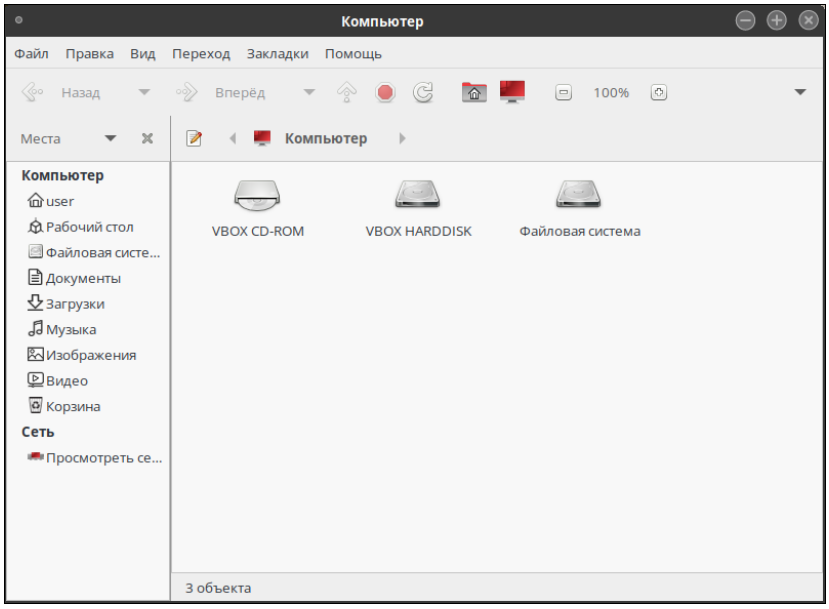


В программе имеется три вкладки: **Рабочий стол**, **Панель** и **Окна**.

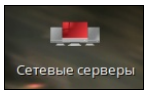
Рабочий стол

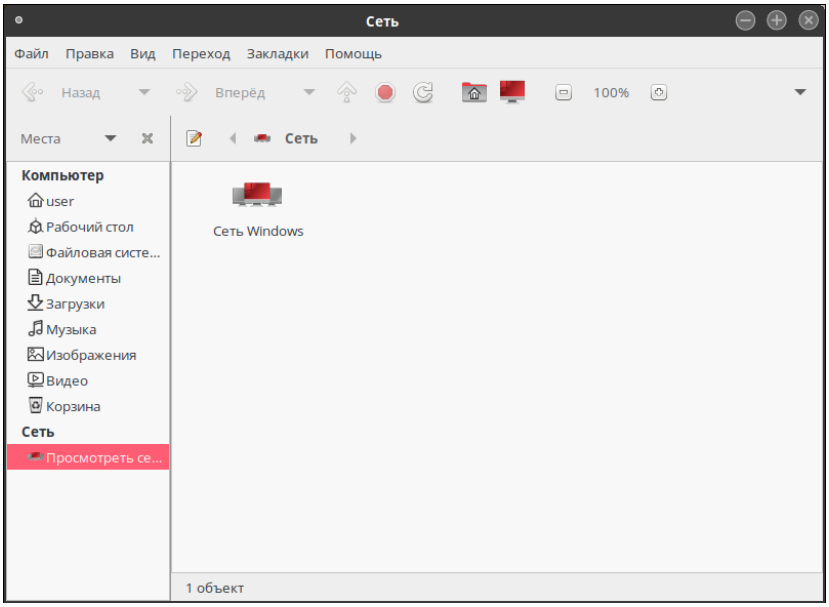
На вкладке **Рабочий стол** можно редактировать рабочий стол MATE, включать или отключать отображение иконок, отвечающих за различные функции. По умолчанию включены иконки **Домашняя папка**, **Корзина** и **Подключенные тома**. По желанию можно включить иконку **Компьютер**, которая будет отображать все подключенные к компьютеру носители.





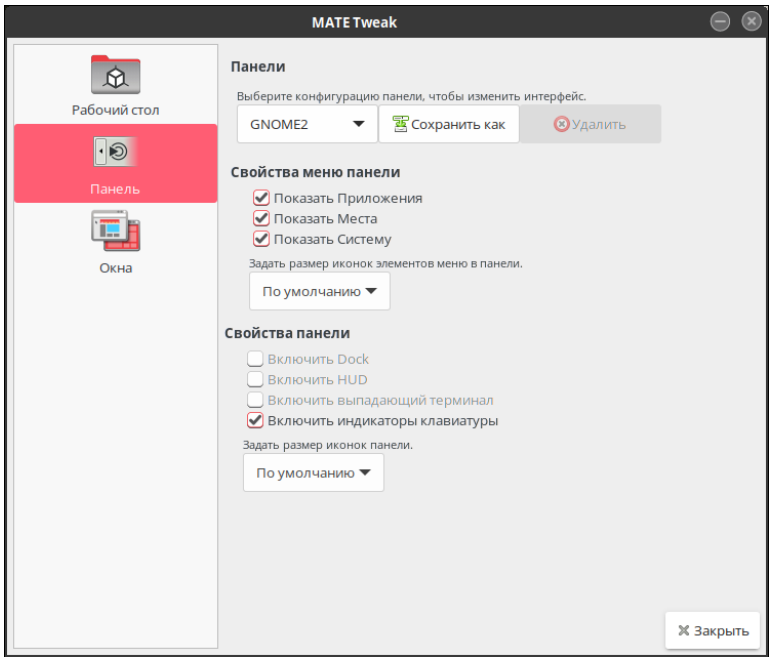
Также можно включить иконку **Сеть**, которая будет отображать сетевое окружение машины.





Панель

На вкладке **Панель** можно настроить нижнюю панель: включить или отключить отображение различных элементов панели, изменить их размеры, а также размеры самих иконок. Выполненные изменения можно сохранить в отдельный профиль и присвоить ему название.



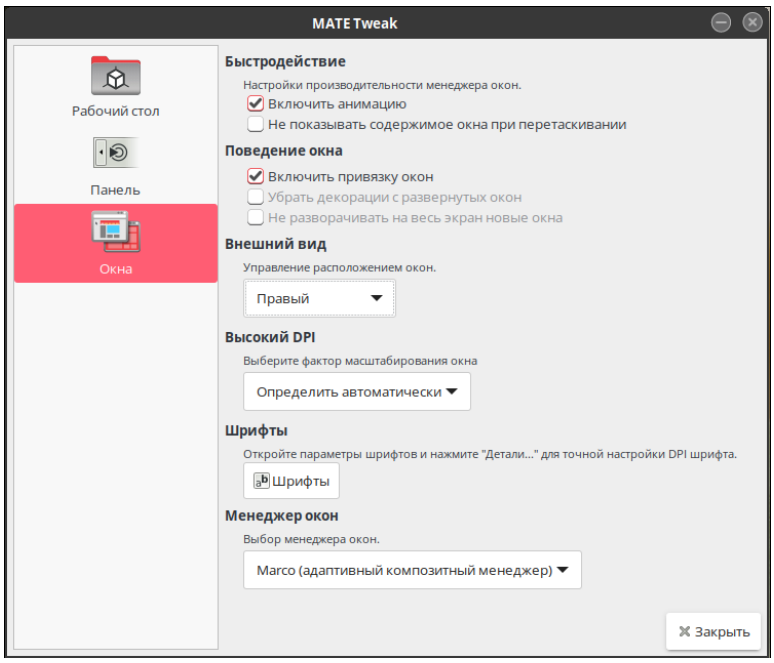
Также можно включить индикатор клавиатуры, он будет расположен в правой части панели. Он позволит увидеть состояния клавиатуры: включен ли **Scroll Lock**, **Num Lock** или **Caps Lock**.



Белый цвет означает неактивное состояние, красный – активное.

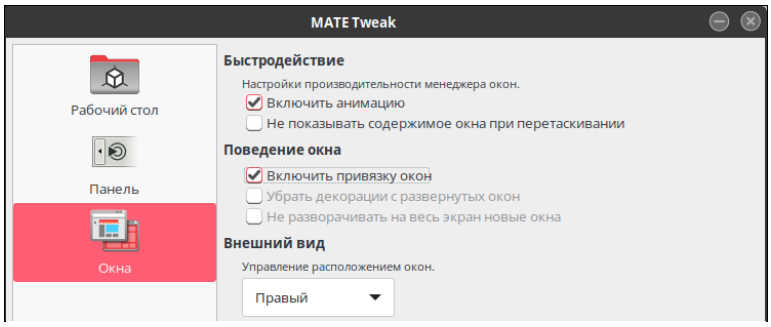
Окна

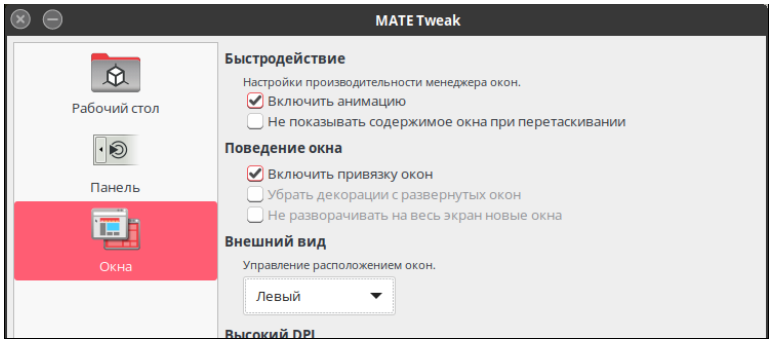
На вкладке **Окна** можно настроить свойства окон: отображение анимации свертывания и развертывания, содержимое окон при перетаскивании.



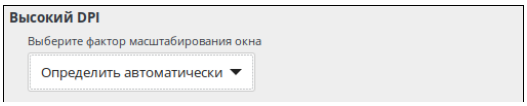
Надстройка **Включить привязку окон** позволяет при перетаскивании окна к краю экрана растянуть его по вертикали и покрыть половину рабочего пространства. По желанию, эту надстройку можно отключить.

Также можно изменить положение самого окна – привычное правое или левое.

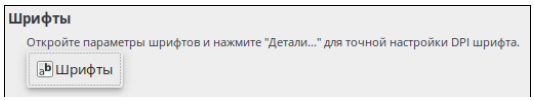




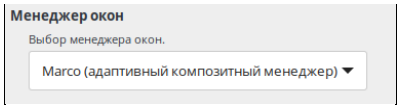
Надстройка **Высокий DPI** позволяет увеличивать размер всех окон, панелей, виджетов, шрифтов и прочего для дисплеев с высокими значениями DPI. По умолчанию данное значение выбирается автоматически.



Надстройка **Шрифты** позволяет поменять шрифты в системе и изменить их размер.



Надстройка **Менеджер окон** позволяет изменить менеджер окна, используемого в системе. По умолчанию установлен менеджер окна **Marco**.



Привилегии и root

Вы можете подробнее ознакомиться с привилегиями пользователя **root** и их использованием в работе, просмотрев наши обучающие видео:

- на **RuTube** — Привилегии и root;
- в **Яндекс.Дзен** — Привилегии и root;
- в **VK Видео** — Привилегии и root.

На наших каналах вы также сможете найти много другой полезной информации.

Правила хорошего тона при работе

Правило 1.

Никогда не выполняйте под правами администратора пользовательскую работу! Бороздить бескрайние просторы интернета, читать и отправлять почту, набирать текстовые документы и рисовать изображения — всё это можно и нужно делать под правами обычного пользователя!

Правило 2.

При необходимости выполнить действия, требующие администраторских прав, не регистрируйтесь в системе как **root**, а используйте утилиты **sudo** или **su**! Если Вам потребовалось установить какой-либо пакет или внести изменения в системные настройки, то воспользуйтесь данными утилитами как в терминальном окне, так и в полном консольном режиме. Применяя утилиту **su** (повышение привилегий) в интерактивном режиме (то есть фактически создавая отдельный терминальный сеанс), не забывайте после выполнения требуемых задач завершать работу данного сеанса, а не оставлять его «висящим» в системе на всякий случай.

Правило 3.

Запуская службы, старайтесь по возможности давать им пониженные права! Это верно как для уже готовых пакетов, когда имя пользователя, с чьими правами будет работать служба, задаётся в файлах конфигурации, так и для программного обеспечения, которое Вы пишите самостоятельно. Каким бы важным не был сервис (веб-сервер, служба DNS или почтовый сервис), ему нет необходимости работать с эффективными правами пользователя **root** — достаточно и прав порою даже меньше, чем у «обычного» пользователя.

Правило 4.

Можно не входить в систему как **root** и даже не использовать утилиты **sudo** или **su** — достаточно на часто запускаемые файлы установить бит **SUID**, и тогда пользователю, запускающему эти программы многое станет доступно без поднятия привилегий. Ни в коем случае так нельзя делать! Использование битов **SUID/SGID** должно быть под полным запретом в Вашей практике!

Утилиты su и sudo

sudo - это программа, разработанная в помощь системному администратору и позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы. Основная идея - дать пользователям как можно меньше прав, но при этом ровно столько, сколько необходимо для решения поставленных задач.

Команда **sudo** предоставляет возможность пользователям выполнять команды от имени *root* или других пользователей. Правила, используемые **sudo** для принятия решения о предоставлении доступа, находятся в файле **/etc/sudoers**. Кроме того, пример правил, предоставляющих пользователям, являющимися членами группы **rpm**, возможность устанавливать, обновлять и удалять пакеты в системе, приведен в файле **/usr/share/doc/sudo-/sample.sudoers**.

Для редактирования файла **/etc/sudoers** следует использовать программу **visudo**, которая проверяет синтаксис и, тем самым, позволяет избежать ошибок в правилах.

В большинстве случаев, грамотная настройка **sudo** делает работу от имени суперпользователя ненужной.

Команда **su** позволяет изменить привилегии на любого имеющегося в системе пользователя, в связи с чем синтаксис команды следующий:

```
su <имя_пользователя> <опции>
```

Если не указать имя пользователя, то по умолчанию считается, что это — **root**, то есть выполнение команды без аргументов «**su**» означает «**su root**».

Из опций наиболее значимой является:

«**-c**» — позволяет выполнить команду, указанную после данного ключа в кавычках, и завершить работу утилиты.

Например:

```
su -c "dnf update"
```

«-» или «**-l**» — при получении привилегий другого пользователя запускается отдельная оболочка со значениями переменных окружения того пользователя, чьи привилегии мы получаем.

То есть, выполнив из-под пользователя ivanov команду «**su**», мы останемся в том же рабочем окружении, что и были (то есть получив права супер-администратора, всё равно нашим домашним каталогом останется **/home/ivanov**, а также все переменные рабочего окружения оболочки).

Следовательно, если какая-то программа или команда захочет что-то записать в домашнюю папку, то она сделает это в каталоге /home/ivanov, но владельцем файла установит уже пользователя **root**, что потом при работе с правами пользователя ivanov не позволит этот файл редактировать, удалить и т. д. Совсем плохо, если этим файлом окажется какой-то из файлов конфигурации.

Поэтому, запомните как ещё одно правило:

Правило 5.

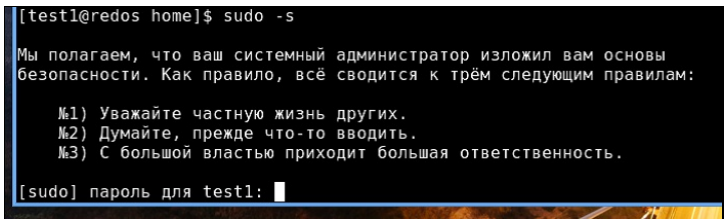
Используя команду **su**, обязательно выполняйте её с аргументом «**-**»:

```
su -
```

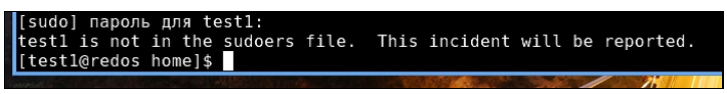
Пример, демонстрирующий различие в переменных окружения между **su** и **su -** :



При первом использовании команды **sudo** на экран будет выведено следующее предупреждение:



И после ввода пароля пользователя может быть выдано следующее сообщение:



Это означает, что при установке РЕД ОС на шаге создания пользователя Вы не установили флажок «**Сделать этого пользователя администратором**». Но это поправимо! Достаточно внести нашего пользователя в группу **wheel**, для чего нужно из-под администратора **root** выполнить следующую команду:

```
usermod -aG wheel <имя_пользователя>
```

Если пользователь, которому менялось членство в группах, находился в системе, то необходимо завершить сеанс работы и войти в систему заново. После этого использование утилиты **sudo** станет возможным. Соответственно, если необходимо убрать у пользователя право пользоваться командой **sudo**, то достаточно удалить его из группы **wheel**.

Ниже приведена таблица различий использования команд **su** и **sudo**.

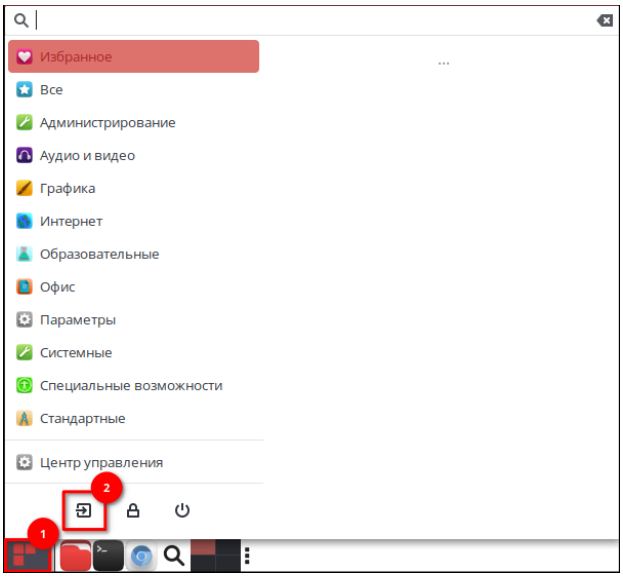
Команда	Описание	Текущий каталог (pwd)	$HOME	$LOGNAME	$USER	$USERNAME	$PATH	DESKTOP_SESSION (export | grep mate)	Комментарий
su	При вызове **su** без аргументов по умолчанию запускается shell пользователя root, но сохраняется прежняя среда	не изменяется	/root	user	user	user	/home/user/.local/bin:/home/user/bin: /usr/share/Modules/bin:/usr/local/bin: /usr/bin:/usr/local/sbin:/usr/sbin	DESKTOP_SESSION="mate"	
su - или su -l	Запустить shell в его начальной среде, как если бы root действительно зарегистрировался в системе. Оболочка получает правильный environment. **Чистая сессия root**	изменяется на /root	/root	root	root	пусто	/usr/share/Modules/bin:/usr/local/sbin: /usr/local/bin:/usr/sbin:/usr/bin:/root/bin	пусто	Рекомендовано к использованию
su root	Аналогично команде su	не изменяется	/root	user	user	user	/home/user/.local/bin:/home/user/bin: /usr/share/Modules/bin:/usr/local/bin: /usr/bin:/usr/local/sbin:/usr/sbin	DESKTOP_SESSION="mate"	
su - root	Аналогично su -l или su -	изменяется на /root	/root	root	root	пусто	/usr/share/Modules/bin:/usr/local/sbin: /usr/local/bin:/usr/sbin:/usr/bin:/root/bin	пусто	Рекомендовано к использованию
su root -	Аналогично команде su или su root	не изменяется	/root	user	user	user	/home/user/.local/bin:/home/user/bin: /usr/share/Modules/bin:/usr/local/bin: /usr/bin:/usr/local/sbin:/usr/sbin	DESKTOP_SESSION="mate"	
sudo -i	Получить оболочку root и его environment. Разрешено, если пользователь добавлен в /etc/sudoers	изменяется на /root	/root	root	root	user	/usr/share/Modules/bin:/usr/local/sbin: /usr/local/bin:/usr/sbin:/usr/bin:/root/bin	пусто	Рекомендовано к использованию
sudo su	Получить оболочку root и его environment. Разрешено, если пользователь добавлен в sudoers	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	пусто	
sudo -s	Команда запускает shell пользователя root, но без смены текущего каталога, при этом не импортируются некторые переменные окружения	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	пусто	
sudo <команда>	Команда исполняется от пользователя root	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	пусто	
sudo -E	Выполнение команд от root с сохранением переменных окружения пользователя	не изменился /home/user	/root	root	root	user	/usr/share/Modules/bin:/sbin:/bin:/usr/sbin: /usr/bin	DESKTOP_SESSION="mate"	

Блокирование сеанса и завершение работы с РЕД ОС

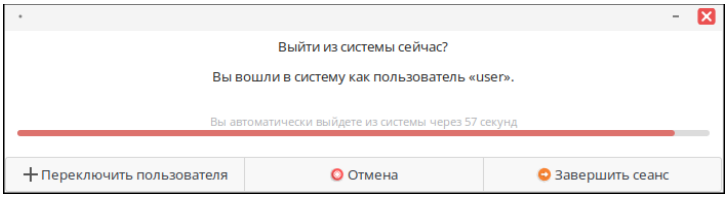
Завершение сеанса в MATE
Блокирование сеанса в MATE
Завершение работы в MATE
Завершение сеанса в KDE Plasma
Блокирование сеанса в KDE Plasma
Завершение работы в KDE Plasma
Завершение сеанса в GNOME
Блокирование сеанса в GNOME
Завершение работы в GNOME

Завершение сеанса в MATE

Если необходимо полностью завершить сеанс, пользователь должен перейти в «**Главное меню**» (1) — «**Завершить текущий сеанс**» (2).



Система перейдет в окно выбора пользователей.

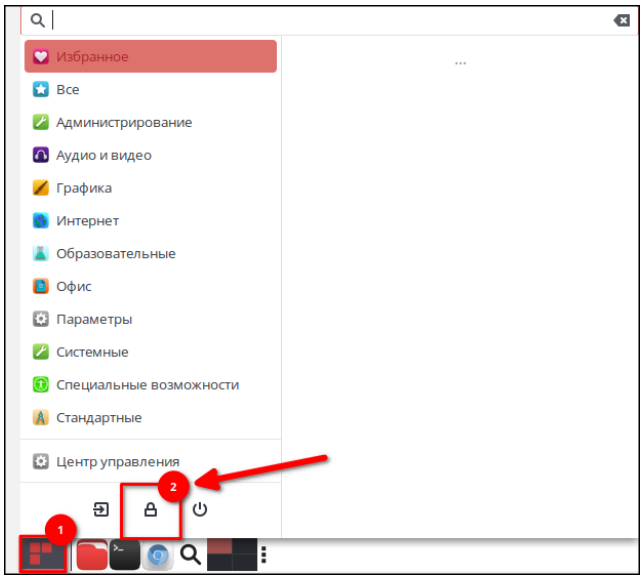


В открывшемся окне пользователь должен выбрать требуемое действие:

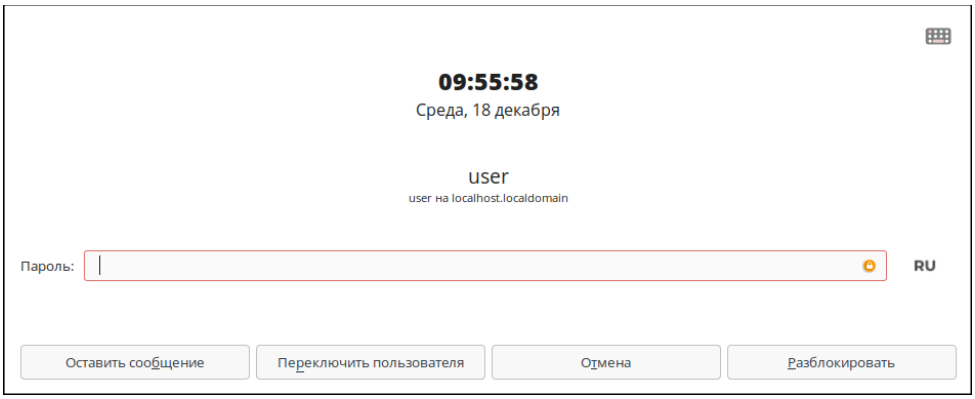
- **Переключить пользователя** — система сохраняет текущее состояние сеанса пользователя (открытые окна, запущенные программы), но переводит устройство в режим выбора пользователей;
- **Отмена** — отменяет операции выхода из системы;
- **Завершить сеанс** — система завершает текущий сеанс пользователя, закрывает все открытые приложения и документы, а также полностью выходит из учетной записи.

Блокирование сеанса в MATE

Для блокирования сеанса пользователя можно использовать сочетание клавиш «**Win + L**», «**Ctrl + Alt + L**» или перейти в «**Главное меню**» (1) — «**Заблокировать экран**» (2).



В результате выполненных действий сеанс пользователя будет приостановлен, на экране появится хранитель экрана, дальнейшая работа возможна только после разблокировки экрана с вводом пароля пользователя.

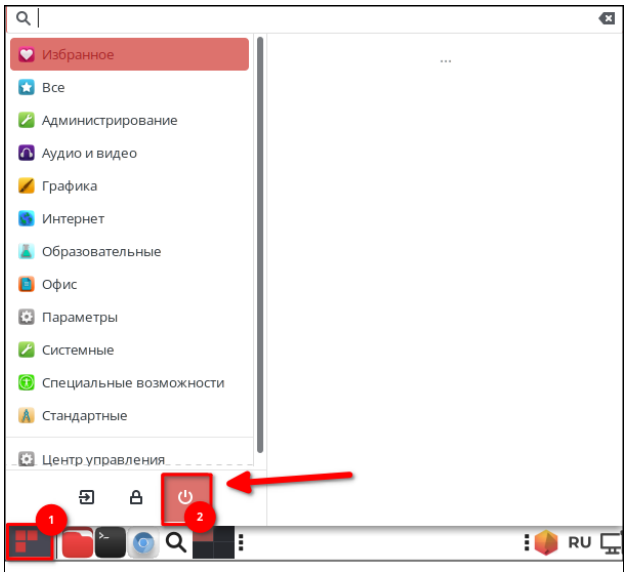


В открывшемся окне пользователь должен выбрать требуемое действие:

- **Оставить сообщение** — эта кнопка позволяет оставить текстовое сообщение для пользователя, который войдет в систему после разблокировки экрана;
- **Переключить пользователя** — этот вариант позволяет быстро сменить активного пользователя, не закрывая текущие приложения и программы;
- **Отмена** — кнопка отмены возвращает пользователя обратно в хранитель экрана, если он после ввода пароля передумал разблокировать экран;
- **Разблокировать** — после ввода пароля эта кнопка снимает блокировку экрана.

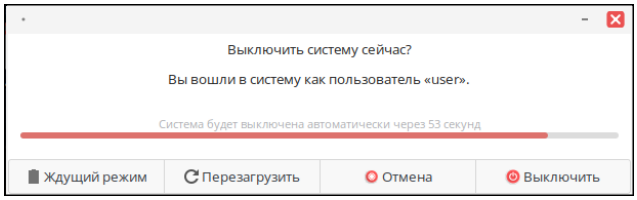
Завершение работы в MATE

Для завершения работы **в MATE** и выключения компьютера пользователю необходимо перейти в «**Главное меню**» (1) — «**Выключить устройство**» (2).



В открывшемся окне пользователь должен выбрать требуемое действие:

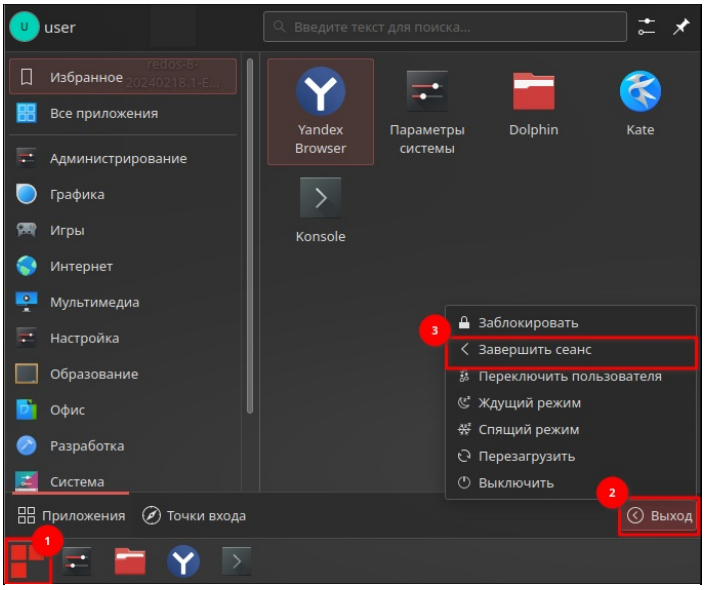
- **Ждущий режим** — энергосберегающий режим работы компьютерного оборудования. Назначение режима — уменьшение потребления энергии устройством во время простоя. Для ждущего режима требуется аппаратная поддержка со стороны оборудования;
- **Перезагрузить** — выполняется перезагрузка и возвращение РЕД ОС в рабочее состояние;
- **Отмена** — отменяет операции завершения работы с РЕД ОС;
- **Выключить** — действие производит корректное выключение РЕД ОС с остановкой всех служб и последующим автоматическим выключением питания СВТ.



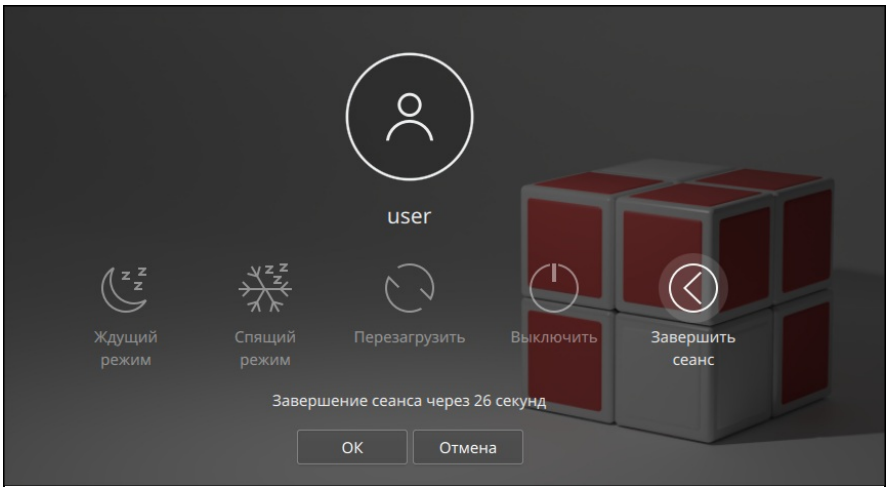
Для корректного завершения работы ОС (перезагрузки) во время ее работы **ЗАПРЕЩАЕТСЯ** выключать питание или нажимать на кнопку «**Reset**». Перед окончанием работы с ОС пользователь должен завершить все работающие программы.

Завершение сеанса в KDE Plasma

Если необходимо полностью завершить сеанс, пользователь должен перейти в «**Главное меню**» (1) — «**Выход**» (2) — «**Завершить сеанс**» (3).



Система перейдет в окно выбора режима.

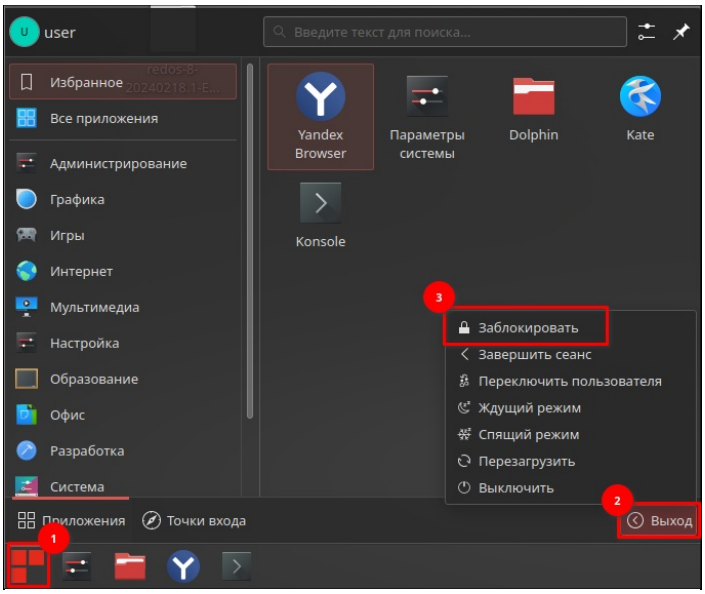


В открывшемся окне пользователь должен выбрать требуемое действие:

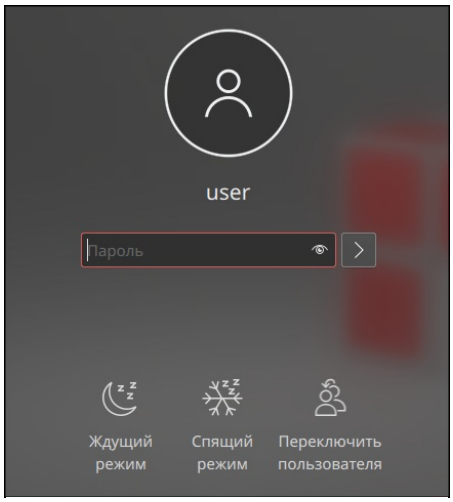
- **Ждущий режим** — энергосберегающий режим работы компьютерного оборудования. Назначение режима — уменьшение потребления энергии устройством во время простоя. Для ждущего режима требуется аппаратная поддержка со стороны оборудования;
- **Спящий режим** — режим, при котором большинство компонентов переводится в состояние пониженного энергопотребления, однако вся информация о текущем состоянии системы сохраняется в оперативной памяти;
- **Перезагрузить** — выполняется перезагрузка и возвращение РЕД ОС в рабочее состояние;
- **Выключить** — действие производит корректное выключение РЕД ОС с остановкой всех служб и последующим автоматическим выключением питания СВТ;
- **Завершить сеанс** — система завершает текущий сеанс пользователя, закрывает все открытые приложения и документы, а также полностью выходит из учетной записи.

Блокирование сеанса в KDE Plasma

Для блокирования сеанса пользователя можно использовать сочетание клавиш «**Win + L**», «**Ctrl + Alt + L**» или перейти в «**Главное меню**» (1) — «**Выход**» (2) — «**Заблокировать**» (3) .



В результате выполненных действий сеанс пользователя будет приостановлен, на экране появится хранитель экрана, дальнейшая работа возможна только после разблокировки экрана с вводом пароля пользователя.

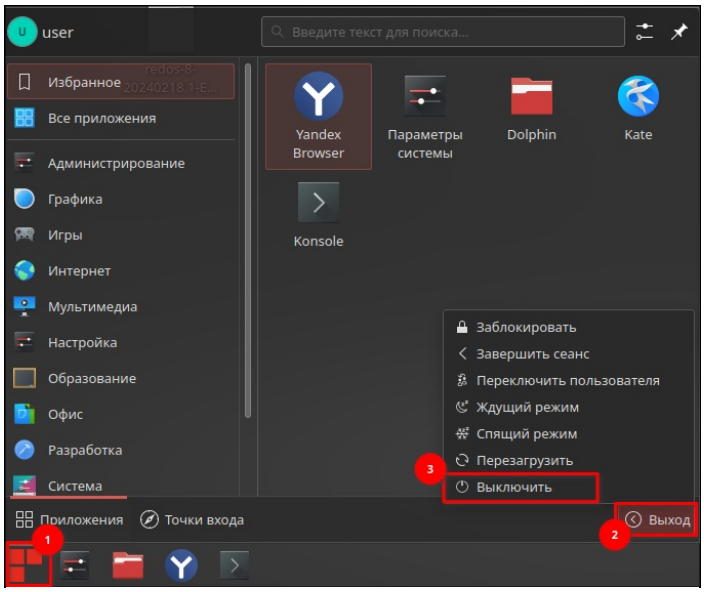


В открывшемся окне пользователь должен выбрать требуемое действие:

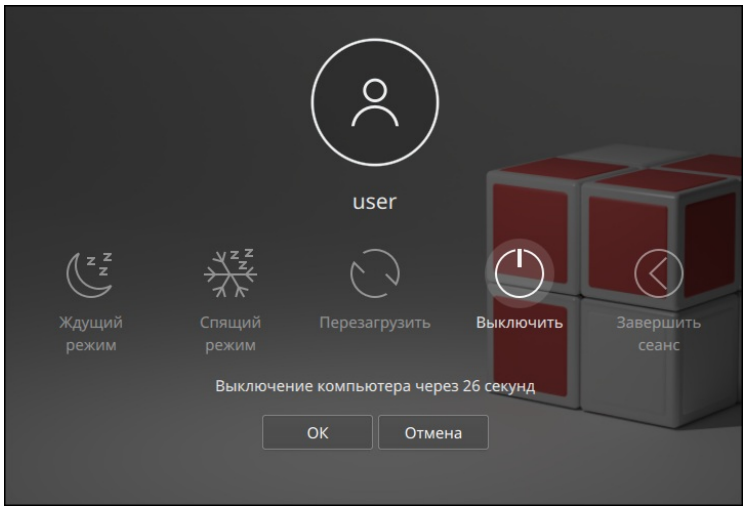
- **Ждущий режим** — энергосберегающий режим работы компьютерного оборудования. Назначение режима — уменьшение потребления энергии устройством во время простоя. Для ждущего режима требуется аппаратная поддержка со стороны оборудования;
- **Спящий режим** — режим, при котором большинство компонентов переводится в состояние пониженного энергопотребления, однако вся информация о текущем состоянии системы сохраняется в оперативной памяти;
- **Переключить пользователя** — этот вариант позволяет быстро сменить активного пользователя, не закрывая текущие приложения и программы.

Завершение работы в KDE Plasma

Для завершения работы **в KDE Plasma** и выключения компьютера пользователю необходимо перейти в «**Главное меню**» (1) — «**Выход**» (2) — «**Выключить устройство**» (3).



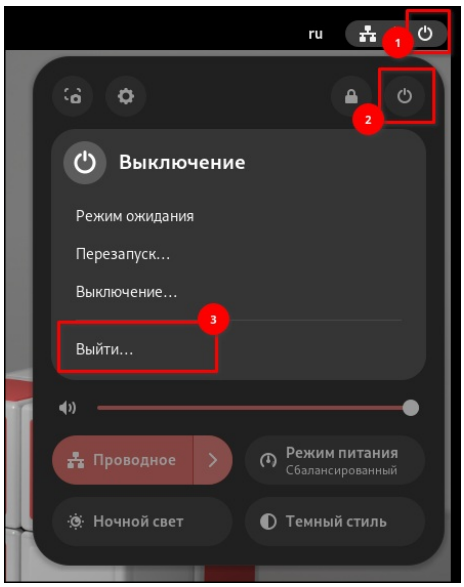
В открывшемся окне пользователь должен выбрать требуемое действие.



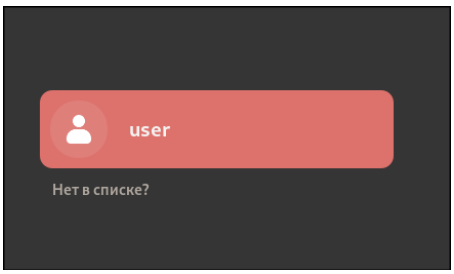
Для корректного завершения работы ОС во время ее работы **ЗАПРЕЩАЕТСЯ** выключать питание или нажимать на кнопку «**Reset**». Перед окончанием работы с ОС пользователь должен завершить все работающие программы.

Завершение сеанса в GNOME

Завершение сеанса **в GNOME** включает в себя выход из текущей учетной записи пользователя и закрытие всех активных приложений и процессов. Для завершения сеанса **в GNOME** пользователь должен открыть меню в правом верхнем углу (1), выбрать «**Завершить работу**» (2) — «**Выйти...**» (3).



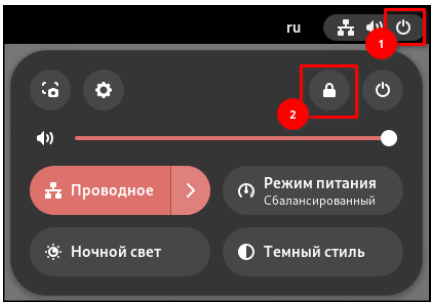
Далее в появившемся окне нажать «**Выйти**». После завершения сеанса пользователь будет возвращен к экрану входа в систему, где сможет либо войти в другую учетную запись, либо перезагрузить или выключить компьютер.



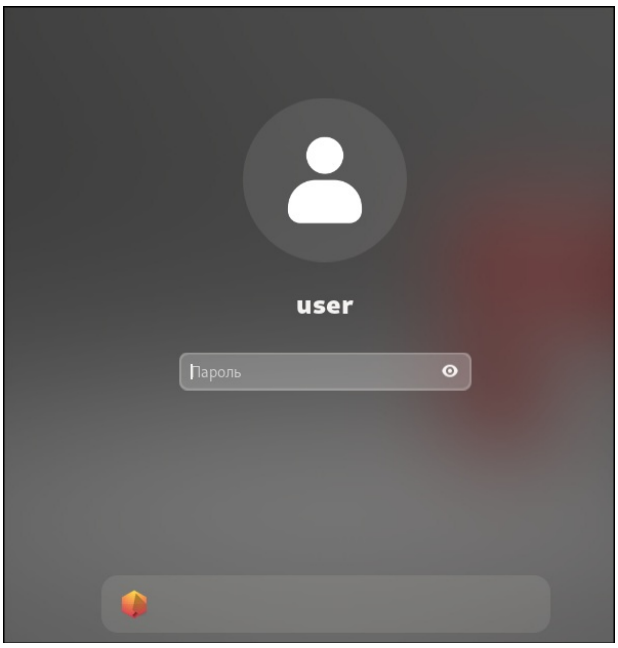
Блокирование сеанса в GNOME

Блокирование сеанса **в GNOME** позволяет защитить учетную запись и данные, пока пользователь временно отсутствует за компьютером. При блокировке сеанса экран становится недоступным до тех пор, пока пользователь не введет свой пароль для разблокировки.

Для блокирования экрана **в GNOME** можно использовать сочетание клавиш «**Win + L**», «**Ctrl + Alt + L**» или открыть меню в правом верхнем углу (1), затем выбрать «**Заблокировать экран**» (2).

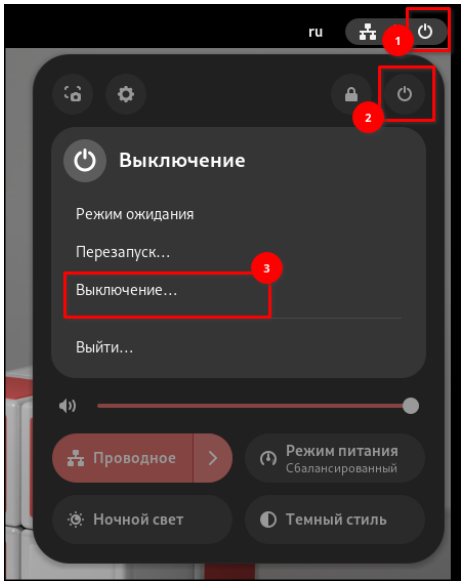


В результате выполненных действий сеанс пользователя будет приостановлен, на экране появится хранитель экрана, дальнейшая работа возможна только после разблокировки экрана с вводом пароля пользователя.



Завершение работы в GNOME

Для завершения работы **в GNOME** и выключения компьютера пользователю необходимо **в GNOME** пользователь должен открыть меню в правом верхнем углу (1), выбрать «**Завершить работу**» (2) — «**Выключение...**» (3).



Для корректного завершения работы ОС (перезагрузки) во время ее работы **ЗАПРЕЩАЕТСЯ** выключать питание или нажимать на кнопку «**Reset**». Перед окончанием работы с ОС пользователь должен завершить все работающие программы.

Ядро ОС

Ядро является основным компонентом операционной системы (ОС) и основным интерфейсом между аппаратным обеспечением компьютера и его процессами. Оно обеспечивает взаимодействие между этими двумя системами, максимально эффективно управляя ресурсами.

Ядро существует в операционной системе и управляет всеми основными функциями аппаратного обеспечения.

Ядро выполняет 5 основных функций:

1. *Управление памятью* – отслеживает объемы памяти для хранения тех или иных объектов и освобождает оперативную память. Ядро следит за доступом к памяти и позволяет процессам использовать адресное пространство, превышающее физическую память, гарантируя, что данные не будут случайно перезаписаны.

2. *Управление процессами* – управляет созданием, планированием и завершением процессов, обеспечивая механизм многозадачности, позволяя нескольким процессам выполняться практически одновременно.

3. *Взаимодействие драйверов устройств* – ядро управляет взаимодействием с устройствами, такими как жесткие диски, клавиатуры, мыши, сетевые интерфейсы.

4 . *Управление файловой системой* – управляет структурой хранения данных на диске и обеспечивает безопасность файлов и каталогов.

5. *Сетевое взаимодействие* – управляет сетевыми соединениями и реализует сетевые протоколы.

Ядро, если оно реализовано должным образом, невидимо для пользователя и работает в собственном разделе системы, известном как пространство ядра, где оно выделяет память и отслеживает, где что хранится. То, что видит пользователь — например, веб-браузеры и файлы – называется *пользовательским пространством*. Эти приложения взаимодействуют с ядром через интерфейс системных вызовов (SCI).

Ядро операционной системы обеспечивает взаимодействие между аппаратным обеспечением и программным обеспечением. Оно выполняет множество функций, включая управление процессами, памятью, файловыми системами и сетями. Понимание работы ядра и различных его архитектур помогает разработчикам и системным администраторам более эффективно использовать ресурсы компьютера и разрабатывать надежные приложения.

Загрузчик ОС

После включения питания компьютера запускается процедура самотестирования (Power On Self Test, POST), проверяющая основные компоненты системы: видеокарту, оперативную память, жесткие диски и т. д. Затем начинается загрузка операционной системы. Компьютер при этом выполняет поиск на жестком диске (и других носителях) программы-загрузчика операционной системы. Если такая программа найдена, ей передается управление; если же такая программа не найдена ни на одном из носителей, выдается сообщение с запросом на подключение загрузочного диска.

В настоящее время актуален только один загрузчик: GRUB2 — он используется по умолчанию в большинстве дистрибутивов и после установки РЕД ОС начальным загрузчиком будет именно он.

Задача загрузчика — предоставить пользователю возможность выбрать нужную операционную систему (для случаев, когда кроме РЕД ОС на компьютере установлены дополнительные операционные системы) и передать ей управление. В случае с РЕД ОС загрузчик загружает ядро операционной системы и передает управление ему. Все последующие действия по загрузке системы: монтирование корневой файловой системы, запуск программы инициализации — выполняет ядро ОС.

Файловая система в РЕД ОС

Журналируемые и нежурналируемые файловые системы
Файлы
Устройства
Монтирование устройств
Каталоги файловой системы РЕД ОС
Основные команды для работы с файлами и файловой системой
Навигация
Операции с файлами
Операции с каталогами
Мягкие и жесткие ссылки
Примеры создания ссылок

Файл — это поименованная область памяти. Если память «долгосрочная» и информация в ней хранится на дисковых или подобных им носителях (например, USB-накопители), то поименованными областями являются имеющиеся на них файлы.

Упрощённо можно сказать, что совокупность файлов, структурированная в соответствии с унифицированными требованиями на физическом носителе, представляет собой **файловую систему** (**ФС**). Файловая система определяет порядок/способ хранения данных на носителях, допустимый размер имён файлов и каталогов, формат, количество и объём метаданных.

Метаданные — это дополнительная информация о файле, то, что в повседневном использовании называется «свойства файла».

Вы можете подробнее ознакомиться с поддерживаемыми файловыми системами в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Файловая система в РЕД ОС;
- в **Яндекс.Дзен** — Файловая система в РЕД ОС;
- в **VK Видео** — Файловая система в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Журналируемые и нежурналируемые файловые системы

Файловые системы можно классифицировать по различным признакам, далее будет рассмотрен вариант классификации на журналируемые и нежурналируемые файловые системы.

К **журналируемым** файловым системам относятся те, которые сохраняют список изменений, осуществляемых с файловой системой, перед фактическим их применением. Такие записи хранятся в отдельной части файловой системы, называемой журналом. Как только изменения файловой системы внесены в журнал, она применяет изменения к файлам или метаданным, а затем удаляет эти записи из журнала.

К **нежурналируемым** файловым системам относятся **ext2** и **FAT** (*FAT12, FAT16, FAT32*). Ядро ОС их также поддерживает.

При перезагрузке компьютера программа монтирования может гарантировать целостность журналируемой файловой системы простой проверкой журнала на наличие ожидаемых, но не произведённых изменений и последующей записью их в файловую систему. Т.е. при наличии журнала в большинстве случаев системе не нужно проводить проверку целостности файловой системы. Соответственно, шансы потери данных в связи с проблемами в файловой системе значительно снижаются.

Для рабочих станций в РЕД ОС используется журналируемая файловая система **ext4** — логическое продолжение **ext3**, которая является журналируемым вариантом системы **ext2** — «материнской» файловой системы Linux.

В зависимости от указанных администратором настроек файловая система **ext4** может работать в любом из трёх известных для журналируемых систем режиме:

- в режиме обратной связи — журналируются только метаданные;
- упорядочивание — журналируются только метаданные синхронно относительно данных;
- в режиме данных — журналируются как метаданные, так и данные.

Для серверного варианта РЕД ОС рекомендуется использовать файловую систему **XFS**, которая также является журналируемой.

Обе файловые системы — **ext4** и **XFS** — являются не только журналируемыми, но и:

- поддерживают большие объёмы дисковых накопителей (до 2^{60} байт);
- поддерживают файлы большого размера (до 2^{44} байт);
- используют механизм пространственной записи файлов, уменьшающий фрагментацию и повышающий производительность. Суть механизма заключается в том, что новая информация добавляется в конец области диска, выделенной заранее рядом с

областью, занятой содержимым файла.

Важными отличиями представленных файловых систем является то, что **XFS**:

- может производить дефргаментацию «на лету»;
- имеет API ввода-вывода реального времени (для приложений жёсткого или мягкого реального времени, например, для работы с потоковым видео);
- имеет малые «накладные расходы» — размер служебных структур данных.

Ext4 в отличие от **XFS** менее агрессивно использует оперативную память при работе с файлами на носителе, поэтому её оптимально применять на вычислительных системах с небольшим объёмом ОЗУ.

При выборе файловой системы при создании/форматировании раздела рекомендуется определить, для чего будет использоваться этот раздел. Также следует обратить внимание на параметры процессора и оперативной памяти компьютера, и на основании этого принимать решение о необходимости выбора той или иной ФС.

РЕД ОС поддерживает и другие файловые системы, такие как **FAT**, **NTFS**, а также **ISO-9660** для оптических накопителей, сетевые файловые системы.

Файлы

У всех файловых систем в РЕД ОС есть одно принципиальное отличие от файловых систем Windows — имена файлов регистрозависимы, т.е «заявление.odt», «Заявление.odt» и «ЗАЯВЛЕНИЕ.odt» — это три разных файла. Необходимо обращать на это внимание, если вы только начинаете миграцию на РЕД ОС с других операционных систем. Особенно следует быть внимательными, когда такие файлы копируются на USB-накопитель — **FAT** и **NTFS** не разборчивы в символах, поэтому при выполнении данной операции возникнет ошибка.

Другим принципиальным отличием файловых систем Linux от файловых систем Windows является разделитель в именах каталогов — в РЕД ОС им служит «слэш» (или «прямой слэш») — «**/**», а в Windows применяется «обратный слэш» — «\». Например:

- **/var/log/boot.log** — путь к файлу в РЕД ОС;
- **C:\Windows\System32\example.exe** — путь к файлу в Windows.

В РЕД ОС (как и вообще в Linux) нет как такового понятия «расширение файла», поскольку точки интерпретируются как часть названия, а не как разделитель. Но прикладные программы и файловые менеджеры анализируют имя файла после последней точки и могут выполнять определённые действия над файлами с теми или иными «окончаниями» (например, двойной клик по файлу с окончанием **.odt** в файловом менеджере приведёт к запуску LibreOffice и открытию файла в нём).

Существует еще одно отличие в организации файловых систем — чтобы в РЕД ОС сделать файл скрытым — надо первым символом его имени указать символ точки «**.**». «Скрытость» файла в РЕД ОС — не метаданные, а непосредственное имя файла, т. е. для того чтобы сделать файл скрытым, его нужно переименовать, поставив первым символом имени «**.**»

Устройства

Следует особенно отметить, что в Unix-подобных операционных системах существует парадигма, относящаяся к идеологии UNIX, называемой **UNIX-Way**. Формулируется она как «Всё — есть файл». То есть всё, до чего «дотягивается» операционная система, можно представить в виде файла, будь то клавиатура, монитор, процессор, веб-камера и т. д.

То, что обычно считается файлом (текст или бинарный файл) называется простым (или регулярным) файлом, а файлы, связанные с каким-либо оборудованием (включая виртуальное) — файлом устройства. Например:

- **/dev/sda** — файл первого «жесткого» диска;
- **/dev/sda1** — файл устройства раздела на первом «жестком» диске;
- **/dev/dvd** — файл привода DVD;
- **/dev/lp0** — файл первого (по подключению) печатающего устройства (принтера).

В свою очередь, файлы устройств бывают двух типов — **блочные** и **символьные**. Обмен информации с блочными устройствами, например, с «жёстким» диском, осуществляется блоками информации, а с символьными — отдельными символами. Примеры символьных устройств: последовательный порт, клавиатура. С символьными файлами можно работать так же, как и с регулярными файлами, т.е. с помощью тех же утилит.

Также не стоит забывать и про каталоги — это специализированные файлы, которые содержат в себе список других файлов.

Файловая система РЕД ОС (как и у любого Linux), в отличие от операционных систем семейства Windows, не разделена по томам (дискам, устройствам), а имеет единую древовидную структуру. **Корневой каталог** — это уровень файловой системы, выше которого по дереву каталогов подняться невозможно. В РЕД ОС корневой каталог обозначается как «**/**».

Монтирование устройств

Для подключения любого устройства к файловой системе — монтирования — используется так называемая точка монтирования — каталог, все вложенные уровни которого являются файловой системой на устройстве-носителе. Например, если подключить флэш-носитель к USB-порту, РЕД ОС автоматически смонтирует устройство в каталог **/var/run/<имя_пользователя>/media**, и все папки и файлы, находящиеся после монтирования в данном каталоге, на самом деле будут располагаться на флэш-накопителе. Для монтирования файловых ресурсов и внешних устройств используется утилита mount. Общий синтаксис команды имеет следующий вид:

```
mount -t <тип_ФС> <имя_устройства> <точка монтирования>
```

Каталоги файловой системы РЕД ОС

У структуры файловой системы РЕД ОС есть ещё одна особенность: пользователям выделяется в ней домашний каталог — специальная папка, необходимая для хранения пользовательских данных. При входе пользователя в систему, он сразу оказывается в своём домашнем каталоге. Обычно права доступа к домашней папке устанавливаются таким образом, что доступ к ней имеют только пользователь и администратор (**root**). В других папках системы пользователю, как правило, разрешен только просмотр содержимого.

Файловая система РЕД ОС содержит следующие каталоги:

- **/** — корневой каталог;
- **/bin** — каталог основных исполняемых файлов, необходимых для функционирования системы;
- **/boot** — каталог загрузчика, содержит образы ядра и Initrd, может содержать конфигурационные и вспомогательные файлы загрузчика;
- **/dev** — содержит файлы устройств;
- **/etc** — конфигурационные файлы системы и основные файлы настроек системных приложений;
- **/home** — папка для домашних каталогов пользователей;
- **/lib** — содержит основные библиотеки и модули, необходимые для работы системы;
- **/lib64** — то же, что и **/lib**, для 64-битных систем;
- **/media** — обычно используется для вручную смонтированных «внешних» носителей;
- **/mnt** — обычно содержит точки монтирования сетевых и файловых ресурсов (смонтированных ISO-файлов);
- **/opt** — альтернатива **/usr** для проприетарного ПО или ПО, не входящего в основной дистрибутив;
- **/proc** — содержит виртуальную файловую систему proc, создаваемую «на лету», а также общую информацию о системе и о каждом процессе;
- **/root** — каталог администратора (суперпользователя) **root**;
- **/run** – каталог для хранения данных, которые были запущены приложениями, требующимися в процессе работы (к ним относятся службы, запускаемые самой системой, и программы, которые запускаются пользователем вручную). Каталог также представляет собой смонтированную виртуальную ФС, чтобы при выключении/перезагрузке ПК вся текущая информация в данном каталоге (информация является временной) удалялась и не занимала пространство на диске;
- **/sbin** — каталог системных утилит, выполнять которые имеет право пользователь root;
- **/srv** – содержит файлы серверов и сервисов. Например, могут содержаться файлы веб-сервера **apache**.
- **/sys** — содержит виртуальную файловую систему, а также подробную информацию о процессах;
- **/tmp** — каталог для временных файлов;
- **/usr** — программы, библиотеки, документация пользовательских приложений, также может содержать исходные коды программ и ядра;
- **/var**— постоянно изменяющиеся данные системы, например, очереди системы печати, протоколы и т. д.

Основные команды для работы с файлами и файловой системой

Навигация

Для навигации по содержимому файловой системы используются следующие команды:

- `ls` — вывод содержимого текущей или явно указанной папки;

- `pwd` — вывод полного имени текущего каталога;
- `cd` — изменение текущего каталога на указанный. Если аргумент не указан или указан как «**~**», то смена происходит на домашний каталог текущего пользователя. Аргумент «**..**» меняет каталог на вышестоящий в иерархии дерева каталогов;
- `pushd`, `popd` — команды работают в связке. Команда **pushd** изменяет каталог на указанный, история запоминается в стек и потом может быть использована для быстрой обратной навигации с помощью команды **popd**.

Операции с файлами

Для операций с файлами используются следующие команды:

- `touch <файл>` — создание пустого файла.
- `cat <файл>` — вывод текстового файла на экран.
- `tac <файла>` — вывод содержимого текстового файла в обратном порядке, т. е. сначала выводится последняя строка файла, потом предпоследняя и т. д.
- `cp <файл1> <файл2>` — копирование файла **<файл1>** в **<файл2>**. Если **<файл2>** существует, программа спросит разрешение на перезапись.
- `mv <файл1> <файл2>` — перемещение файла **<файл1>** в **<файл2 >**. Эту же команду можно использовать для переименования файла.
- `rm <файл>` — удаление файла (с ключом **-i** выводит запрос на разрешение удаления, ключ **-f** подавляет все запросы).
- `locate <файл>` — быстрый поиск файла.
- `which <программа>` — вывод каталога, в котором находится программа, если она установлена. Поиск производится в каталогах, указанных в переменной окружения **path** (путь поиска программ).
- `less <файл>` — удобный просмотр файла с возможностью постраничной прокрутки с использованием клавиш навигации.

Операции с каталогами

Для операций с каталогами используются следующие команды:

- `mkdir <каталог>` — создание каталога;
- `rmdir <каталог>` — удаление пустого каталога;
- `rm -r <каталог>` — рекурсивное удаление каталога;
- `cp -r <каталог1> <каталог2>` — копирование **<каталога1>** в каталог с именем **<каталог2>**, причём **<каталог1>** должен быть пустым. Если каталог требуется скопировать со всем содержимым, то необходимо указать ключ **-r**;
- `mv <каталог1> <каталог2>` — переименование каталогов. Для переноса каталога с именем **<каталог1>** в каталог с именем **<каталог2>** необходимо указать ключ **-r**.

Мягкие и жесткие ссылки

В РЕД ОС имеются также дополнительные файлы и называются они ссылками. Ссылки бывают двух типов - «мягкие» ссылки (*softlink*) и «жёсткие» ссылки (*hardlink*). «Мягкие» ссылки являются указателями на имеющиеся файлы и каталоги. «Жёсткие» ссылки являются ещё одним именем файла.

Создаются ссылки с помощью утилиты **ln**. Для создания «мягких» ссылок необходимо передавать команде ключ **-s**.

Общий синтаксис команды имеет следующий вид:

```
ln [ -s ] <имя_файла_или_каталога> <имя_ссылки>
```

Примеры создания ссылок

Мягкие ссылки

```
cd ~
mkdir FirstDir
ls
```

```
 FirstDir  test-ca.conf  Видео  Документы  Загрузки Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
 ln -s FirstDir SecondDir
ls

 FirstDir  SecondDir  test-ca.conf  Видео  Документы Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол' Шаблоны
 cd SecondDir
touch file1.txt
ls ~/FirstDir

file1.txt
```

При создании пустого файла в каталоге **SecondDir** на самом деле действие производится в каталоге **FirstDir**, что подтверждает последний листинг.

Если удалить исходный файл или каталог, на который ссылается «мягкая» ссылка, то она становится недействительной, т.е. как файл она продолжит существовать, но уже ни на что указывать не будет, и операции с ней (просмотр и т.д.) будут завершаться с ошибкой.

```
cd ~
rm -rf ~/FirstDir
ls SecondDir  test-ca.conf  Видео  Документы  Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
```

Жёсткие ссылки

В примере будет создан текстовый файл путём перенаправления в него вывода строки и жёсткая ссылка на него:

```
cd ~
echo "One small test..." > File1.txt
ls

 File1.txt  test-ca.conf  Видео  Документы Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол' Шаблоныln File1.txt
File2.txt
```

Затем будут внесены изменения в файл **File2.txt** и просмотрено содержимое файла **File1.txt**:

```
echo "Second string..." >> File2.txt
cat File1.txt

One small test...
Second string...
 cat File2.txt

One small test...
Second string...
```

Файлы содержат одну и ту же информацию, поскольку указывают на одну и ту же область памяти на диске. После удаления первого файла область информации на диске остаётся, поскольку остаётся «жёсткая» ссылка, которая становится единственным именем данного файла:

```
rm -f File1.txt
ls

 File2.txt  test-ca.conf  Видео  Документы Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол' Шаблоны
 cat File2.txt

One small test...
Second string...
```

Введение: пакеты, зависимости и репозитории

В РЕД ОС огромное число общих ресурсов, которыми пользуются сразу несколько программ: разделяемых библиотек, содержащих стандартные функции, исполняемых файлов, сценариев и стандартных утилит и т.д. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или даже вывести из строя всю систему. В контексте системного администрирования проблемы такого рода называют нарушением *целостности системы*. Задача администратора - обеспечить наличие в системе согласованных версий всех необходимых программных компонентов (обеспечение целостности системы).

Для установки, удаления и обновления программ и поддержания целостности системы используются *менеджеры пакетов*. С точки зрения менеджера пакетов программное обеспечение представляет собой набор компонентов - программных *пакетов*. Такие компоненты содержат в себе набор исполняемых программ и вспомогательных файлов, необходимых для корректной работы программного обеспечения. Менеджеры пакетов облегчают установку программ: они позволяют проверить наличие необходимых для работы устанавливаемой программы компонент подходящей версии непосредственно в момент установки, а также производят необходимые процедуры для регистрации программы во всех операционных средах пользователя: сразу после установки программа может быть доступна пользователю из командной строки и - если это предусмотрено - появляется в меню всех графических оболочек.

ВАЖНО!

Благодаря менеджерам пакетов, пользователю обычно не требуется непосредственно обращаться к установочным процедурам отдельных программ или непосредственно работать с каталогами, в которых установлены исполняемые файлы и компоненты программ (обычно это **/usr/bin**, **/usr/share/имя_пакета**) - всю работу делает менеджер пакетов. Поэтому установку, обновление и удаление программ обычно называют управлением пакетами.

Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставляемого пакетом A, необходимо установить пакет B. В таком случае говорят, что пакет A *зависит* от пакета B или что между пакетами A и B существует *зависимость*.

Отслеживание зависимостей между такими пакетами представляет собой серьезную задачу для любого дистрибутива - некоторые компоненты могут быть взаимозаменяемыми: может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Задача контроля целостности и непротиворечивости установленного в системе ПО еще сложнее. Представим, что некие программы A и B требуют наличия в системе компоненты C версии 1.0. Обновление версии пакета A, требующее обновления компоненты C до новой, использующей новый интерфейс доступа, версии (скажем, до версии 2.0), влечет за собой обязательное обновление и программы B.

Однако менеджеры пакетов оказались неспособны предотвратить все возможные коллизии при установке или удалении программ, а тем более эффективно устранить нарушения целостности системы. Особенно сильно этот недостаток сказывается при обновлении систем из централизованного *репозитория пакетов*, в котором последние могут непрерывно обновляться, дробиться на более мелкие и т. п. Этот недостаток и стимулировал создание систем управления программными пакетами и поддержания целостности системы.

Для автоматизации этого процесса в РЕД ОС применяется система управления программными пакетами **DNF**.

Вы можете подробнее ознакомиться с информацией о работе с программными пакетами, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Назначение DNF

Фактически, **dnf** представляет собой оболочку для **rpm**, обеспечивающую работу с репозиториями.

Утилита **dnf** - это менеджер пакетов, который умеет запрашивать информацию о пакетах, получать пакеты из репозиториев, устанавливать и удалять их, используя автоматическое разрешение зависимостей, а также обновлять целиком систему до последних версий пакетов. **DNF** выполняет автоматическое разрешение зависимостей для пакетов, которые обновляются, устанавливаются или удаляются, и, таким образом, позволяют автоматически определять, получать и устанавливать все доступные по зависимостям пакеты. Для **DNF** можно настроить новые, дополнительные репозитории, или, по-другому, источники пакетов, кроме того, для него доступны многие дополнения, которые улучшают и расширяют его возможности. **DNF** позволяет выполнять многие из задач, которые выполняет **RPM.** Многие из опций командной строки у него также подобны опциям **RPM**. Утилита **DNF** обеспечивает простое и легкое управление пакетами на одной машине или же на группе машин.

DNF обеспечивает безопасное управление пакетами, используя проверку GPG-сигнатур для пакетов, подписанных с помощью GPG, для всех репозиториев пакетов или для отдельных репозиториев. Если проверка сигнатур активирована, **DNF** откажется устанавливать любые пакеты, не подписанные корректным ключом для данного репозитория. Это означает, что можно доверять пакетам **RPM**, которые скачиваются и устанавливаются на машине в том случае, если они получены из доверенных источников и не были изменены в процессе передачи.

DNF также позволяет легко создавать собственные репозитории RPM-пакетов для скачивания и установки их на других машинах.

Основные команды DNF и утилиты dnf repoquery

Основные команды **DNF** приведены в таблице.

Команда	Описание
dnf install <имя_пакета>	Установка пакета с заданным именем
dnf reinstall <имя_пакета>	Переустановка пакета
dnf remove <имя_пакета>	Удаление пакета
dnf autoremove	Удаляет все пакеты, которые не нужны системе, если они не используются другими приложениями
dnf info <имя_пакета>	Показать информацию о пакете
dnf search <имя_пакета>	Поиск пакета по имени в репозитории
dnf list	Вывод имен всех доступных и установленных пакетов
dnf list installed	Вывод списка всех установленных пакетов
dnf list available	Вывод списка всех доступных пакетов
dnf repolist all	Вывод списка всех репозиториев
dnf repoinfo <имя_репозитория>	Информация о репозитории
dnf config-manager --set-disabled <имя_репозитория>	Отключение репозитория
dnf config-manager --set-enabled <имя_репозитория>	Включение репозитория
dnf clean all	Удаление всех метаданных, кешированных пакетов и заголовков
dnf makecache	Загружает и кэширует метаданные для всех известных репозиториев
dnf history	Вывод истории об использования dnf
dnf groupinstall <имя_группы>	Установка всех пакетов из группы с заданным именем
dnf groupupdate <имя_группы>	Обновление всех пакетов из группы с заданным именем
dnf groupremove <имя_группы>	Удаление всех пакетов из группы с заданным именем
dnf groupinfo <имя_группы>	Получить список пакетов, относящихся к группе
dnf grouplist	Вывод имен всех существующих групп пакетов
dnf provides <имя_файла или пакета>	Поиск пакета, к которому принадлежит определенный файл/подпакет
dnf update	Обновить все пакеты в системе
dnf download <имя_пакета>	Загружает из репозитория пакет
dnf repoquery --requires <имя_пакета>	Получить список зависимостей неустановленного пакета
dnf repoquery --requires --resolve <имя_пакета>	Вывод списка пакетов, которые необходимы для удовлетворения зависимостей
dnf downgrade <имя_пакета><версия>	Понижает текущую версию пакета до предыдущей (по возможности). Если указана версия пакета (ниже установленной), выполняется понижение до целевой версии пакета
dnf download --resolve <имя_пакета> --downloaddir /<путь_к_каталогу>	Позволяет загружать rpm-пакет вместе со всеми зависимостями в указанный каталог

Вы можете подробнее ознакомиться с менеджером пакетов DNF, просмотрев наши обучающие видео:

- на **RuTube** — Менеджер пакетов DNF в РЕД ОС 7.3 ;
- в **Яндекс.Дзен** — Менеджер пакетов DNF в РЕД ОС 7.3 ;
- в **VK Видео** — Менеджер пакетов DNF в РЕД ОС 7.3 .

На наших каналах вы также сможете найти много другой полезной информации.

Утилита **dnf repoquery** предоставляет широкий набор инструментов для работы с репозиториями и пакетами, что делает ее мощным инструментом для управления пакетами в системе. В таблице приведены некоторые из основных возможностей **dnf repoquery**.

Команда	Описание
dnf repoquery <название_пакета>	Находит пакет в установленных репозиториях по его названию.
dnf repoquery --info <название_пакета>	Предоставляет подробную информацию о пакете, включая версию, размер, описание и другие атрибуты.
dnf repoquery --whatprovides <путь_к_файлу>	Находит пакет, который содержит указанный файл.

dnf repoquery --requires <название_пакета>	Показывает список зависимостей, необходимых для установки указанного пакета.
dnf repoquery --whatrequires <название_пакета>	Находит другие пакеты, которые зависят от указанного пакета.
dnf repoquery --group <название_группы>	Находит все пакеты, входящие в указанную группу пакетов.
dnf repoquery --requires <название_пакета>	Показывает список зависимостей, которые должны быть удовлетворены для установки указанного пакета.
dnf repoquery --all	Показывает список всех пакетов, доступных в репозиториях.
dnf repoquery --unneeded	Показывает только те пакеты, которые могут быть удалены командой "dnf autoremove".
dnf repoquery --installed	Показывает список всех установленных пакетов.
dnf repoquery -h	Вывести список всех доступных команд.

Работа с историей DNF

Просмотр истории транзакций
Отмена транзакции
Повтор транзакции
Откат к предыдущей транзакции
Просмотр недавно добавленных пакетов

Для отслеживания изменений по установке, обновлению и удалению пакетов в системе используется история DNF, которая дает представление о транзакциях в хронологическом порядке.

Благодаря истории транзакций можно отменить ту или иную транзакцию, сделать откат к предыдущей транзакции (при этом отменятся все выполненные транзакции после указанной), повторить отмененную транзакцию, а также просмотреть недавно добавленные транзакции.

Просмотр истории транзакций

Для просмотра транзакций используется следующая команда:

```
dnf history
```

```
[root@localhost user]# dnf history
Иденти | Командная строка          | Дата и время     | Действия       | Изменен
-------------------------------------------------------------------------------
    38 | install gscan2pdf-2.8.0-1 | 2022-01-11 12:43 | Install        |   62
    37 | install flatpak           | 2022-01-11 12:42 | Install        |    4 EE
    36 | install redshift          | 2022-01-11 12:42 | Install        |    1
    35 | install shotwell-0.31.2-1 | 2022-01-11 12:41 | Install        |   50
    34 | install cherrytree-0.38.1 | 2022-01-11 12:41 | Install        |    8
    33 | install gimp              | 2022-01-11 12:39 | Install        |    7
```

Отмена транзакции

Отмена какой-либо транзакции выполняется с помощью следующей команды:

```
dnf history undo <идентификатор_транзакции>
```

```
[root@localhost user]# dnf history undo 36
Последняя проверка окончания срока действия метаданных: 2:26:35 назад, Вт 11 янв 2022 10:19:18.
Откат транзакции 36, с Вт 11 янв 2022 12:42:14
    Установка redshift-1.12-2.el7.x86_64 @base
Зависимости разрешены.
================================================================================
 Пакет                Архитектура         Версия                    Репозиторий        Размер
================================================================================
Удаление:
 redshift             x86_64              1.12-2.el7                @base              561 k

Результат транзакции
================================================================================
Удаление  1 Пакет

Освобожденное место: 561 k
Продолжить? [д/Н]: y
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```

Повтор транзакции

Отмененную транзакцию можно повторить (необходимо указать ID отмененной транзакции):

```
dnf history redo <идентификатор_транзакции>
```

```
[root@localhost user]# dnf history redo 36
Последняя проверка окончания срока действия метаданных: 2:30:33 назад, Вт 11 янв 2022 10:19:18.
Repeating transaction 36, from Вт 11 янв 2022 12:42:14
    Установка redshift-1.12-2.el7.x86_64 @base
================================================================================================
 Пакет                  Архитектура          Версия                   Репозиторий        Размер
================================================================================================
Установка:
 redshift               x86_64               1.12-2.el7               base               149 k

Результат транзакции
================================================================================================
Установка  1 Пакет

Объем загрузки: 149 k
Объем изменений: 561 k
Продолжить? [д/Н]: y
Загрузка пакетов:
redshift-1.12-2.el7.x86_64.rpm                                  1.2 MB/s | 149 kB     00:00
------------------------------------------------------------------------------------------------
Общий размер                                                    1.2 MB/s | 149 kB     00:00
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```

Откат к предыдущей транзакции

Для отката к предыдущей версии транзакции используется следующая команда:

```
dnf history rollback <идентификатор_транзакции>
```

```
[root@localhost user]# dnf history rollback 35
Последняя проверка окончания срока действия метаданных: 2:35:38 назад, Вт 11 янв 2022 10:19:18.
Rollback to transaction 35, from Вт 11 янв 2022 12:41:25
  Undoing the following transactions: 36, 37, 38, 39, 40
    Установка ImageMagick-perl-6.9.11.27-1.el7.x86_64           @base
    Установка flatpak-selinux-1.6.3-2.el7.noarch                @base
    Установка flatpak-session-helper-1.6.3-2.el7.x86_64         @base
    Установка flatpak-1.6.3-2.el7.x86_64                        @base
    Установка goocanvas2-2.0.2-4.el7.x86_64                     @base
    Установка gscan2pdf-2.8.0-1.el7.noarch                      @base
                                        ...
 perl-namespace-autoclean              noarch        0.29-2.el7            @base         41 k
 perl-namespace-clean                  noarch        0.27-12.el7           @base         39 k
 perltidy                              noarch        20190915-1.el7        @base        2.1 M
 redshift                              x86_64        1.12-2.el7            @base        561 k
 sane-frontends                        x86_64        1.0.14-22.el7         @base        135 k

Результат транзакции
================================================================================================
Удаление  67 Пакетов

Освобожденное место: 53 M
Продолжить? [д/Н]: y
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
```

Обратите внимание, что **транзакции**, выполненные **после** той, к которой выполняется откат, **будут отменены**.

Просмотр недавно добавленных пакетов

Для просмотра недавно добавленных пакетов используется следующая команда:

```
dnf list recent
```

```
[root@localhost user]# dnf list recent
RedOS - Base                                    66 kB/s | 3.6 kB     00:00
RedOS - Base                                    11 MB/s |  38 MB     00:03
RedOS - Updates                                 80 kB/s | 2.9 kB     00:00
RedOS - Updates                                9.6 MB/s | 7.3 MB     00:00
Последняя проверка окончания срока действия метаданных: 2:38:49 назад, Вт 11 янв
 2022 10:19:18.
Недавно добавленные пакеты
anaconda.i686                          33.25.4-6.3.el7              updates
anaconda.x86_64                        33.25.4-6.3.el7              updates
anaconda-core.i686                     33.25.4-6.3.el7              updates
anaconda-core.x86_64                   33.25.4-6.3.el7              updates
anaconda-dracut.i686                   33.25.4-6.3.el7              updates
anaconda-dracut.x86_64                 33.25.4-6.3.el7              updates
anaconda-gui.i686                      33.25.4-6.3.el7              updates
anaconda-gui.x86_64                    33.25.4-6.3.el7              updates
anaconda-install-env-deps.i686         33.25.4-6.3.el7              updates
anaconda-install-env-deps.x86_64       33.25.4-6.3.el7              updates
anaconda-live.i686                     33.25.4-6.3.el7              updates
anaconda-live.x86_64                   33.25.4-6.3.el7              updates
anaconda-tui.i686                      33.25.4-6.3.el7              updates
anaconda-tui.x86_64                    33.25.4-6.3.el7              updates
```

Источники программ (репозитории)

Создание репозитория
Подключение репозиториев
ПО в репозитории
Доступные репозитории РЕД ОС

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный

Репозитории, с которыми работает **DNF**, отличаются от обычного набора пакетов наличием метаинформации - индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, **DNF** достаточно получить его индексы. **DNF** может работать с любым количеством репозиториев одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов **DNF** обращает внимание только на название пакета, его версию и зависимости, а расположение в том или ином репозитории не имеет значения. Если потребуется, **DNF** в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

ВАЖНО!

При использовании РЕД ОС (стандартной и сертифицированной редакции), в целях предотвращения нарушения целостности системы, **ЗАПРЕЩАЕТСЯ** настройка служб автоматического обновления на использование внешних **сторонних** репозиториев операционных систем.

Подключение репозитория **сторонней** ОС влечет за собой **нарушение** зависимостей в устанавливаемых пакетах. Принудительная установка пакетов из репозитория сторонней ОС может привести к **неработоспособности** как отдельных компонентов системы, так и ОС в целом.

Если для обеспечения рабочих процессов пользователя нужен пакет (программа, утилита), которого нет в РЕД ОС (и/или требуется обновление версий пакетов, которые уже есть в репозитории РЕД ОС), необходимо обратиться в техническую поддержку с запросом на добавление нового пакета или обновление версии пакетов РЕД ОС.

DNF позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные - **HTTP** и **FTP**, однако существуют и некоторые дополнительные методы. Для того чтобы **DNF** мог использовать тот или иной репозиторий, информацию о нем необходимо поместить в папку **/etc/yum.repos.d/**. После того как отредактирован список репозиториев в **/etc/yum.repos.d/**, необходимо обновить локальную базу данных **DNF** о доступных пакетах:

```
dnf repolist
```

При выборе пакетов для установки **DNF** руководствуется *всеми* доступными репозиториями вне зависимости от способа доступа к ним. Так, если в репозитории, доступном по сети Интернет, обнаружена более новая версия программы, чем на компакт-диске, то **DNF** начнёт загружать данный пакет из сети Интернет.

Создание репозитория

Для создания репозитория выполните следующие действия:

1. Установите пакет **createrepo**.

   ```
   dnf install createrepo
   ```

2. Скопируйте все пакеты в один каталог, например: **/mnt/local_repo**.

3. Создайте репозиторий, используя следующую команду и указав созданный каталог:

   ```
   createrepo --database /mnt/local_repo
   ```

Для установки пакетов из созданного локального репозитория создайте конфигурационный файл в каталоге **/etc/yum.repos.d/**.

Например:

```
nano /etc/yum.repos.d/my-rpm.repo
```

Содержимое файла:

```
[my-rpm]
 name=my-rpm
 baseurl=file:///mnt/local_repo
 gpgcheck=0
```

Подключение репозиториев

Для подключения репозитория на постоянной основе необходимо выполнить (в примере используется репозиторий **foo-bar**):

```
dnf config-manager --set-enabled foo-bar
```

Для отключения репозитория на постоянной основе необходимо выполнить:

```
dnf config-manager --set-disabled foo-bar
```

Для временного подключения репозитория и установка пакета из него необходимо выполнить:

```
dnf install --refresh foo-bar --enablerepo=foo-bar
```

Необязательный параметр `--refresh` добавляется для принудительного обновления кеша **dnf**.

ПО в репозитории

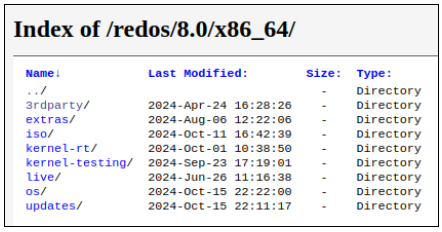
Ознакомиться со списком доступного в репозитории программного обеспечения можно по ссылке.

Доступные репозитории РЕД ОС

Для РЕД ОС существуют два типа репозиториев - для *стандартной* редакции и для *сертифицированной* редакции ОС.

Репозитории стандартной редакции развиваются (обновляются) быстрее.

Далее в качестве примера будут рассмотрены репозитории стандартной редакции РЕД ОС и их назначение. Для просмотра доступных репозиториев перейдите по ссылке.



Index of /redos/8.0/x86_64/

Name↓	Last Modified:	Size:	Type:
../		-	Directory
3rdparty/	2024-Apr-24 16:28:26	-	Directory
extras/	2024-Aug-06 12:22:06	-	Directory
iso/	2024-Oct-11 16:42:39	-	Directory
kernel-rt/	2024-Oct-01 10:38:50	-	Directory
kernel-testing/	2024-Sep-23 17:19:01	-	Directory
live/	2024-Jun-26 11:16:38	-	Directory
os/	2024-Oct-15 22:22:00	-	Directory
updates/	2024-Oct-15 22:11:17	-	Directory

Репозитории для образов:

- **iso/** – место расположения ISO-образов;
- **live/** – место расположения LIVE-образов;
- **oem/** – место расположения OEM-образов.

По умолчанию в РЕД ОС подключены следующие репозитории:

- **os/** – базовый репозиторий;
- **updates/** – репозиторий обновлений.

Дополнительные ветки репозиториев:

- **kernel/** – репозиторий для новых версий ядра;
- **kernel-rt/** – репозиторий для realtime-ядра;
- **kernel-testing/** – репозиторий для предрелизной публикации обновлений ядра;
- **testing/** – репозиторий для предрелизной публикации обновлений некоторых пакетов;

- **extras/** – пакеты, дополняющие базовый репозиторий;
- **3rdparty/** – пакеты сторонних разработчиков.

Синтаксис команды имеет следующий вид:

```
dnf install <название_пакета>
```

Для просмотра подключенных репозиториев в каталог **/etc/yum.repos.d/** выполните команду:

```
ls -lah /etc/yum.repos.d/
```

Для просмотра подключенных репозиториев в каталог **/etc/distro.repos.d/** выполните команду:

```
ls -lah /etc/distro.repos.d/
```

```
[root@localhost ~]# ls -lah /etc/yum.repos.d/
итого 44K
drwxr-xr-x.   2 root root 4,0K авг 11 09:36 .
drwxr-xr-x. 161 root root  12K авг 10 16:05 ..
-rw-r--r--.   1 root root  385 ноя  7  2022 RedOS-ansible6.repo
-rw-r--r--.   1 root root  251 мая  4 12:11 RedOS-Base.repo
-rw-r--r--.   1 root root  316 мар 31 16:39 RedOS-kernels6.repo
-rw-r--r--.   1 root root  287 янв 13  2022 RedOS-kernels.repo
-rw-r--r--.   1 root root  369 авг 22  2022 RedOS-php81.repo
-rw-r--r--.   1 root root  260 мая 11  2022 RedOS-postgresql14.repo
-rw-r--r--.   1 root root  272 мая  4 12:11 RedOS-Updates.repo
[root@localhost ~]# ls -lah /etc/distro.repos.d/
итого 36K
drwxr-xr-x.   2 root root 4,0K авг 10 16:17 .
drwxr-xr-x. 161 root root  12K авг 10 16:05 ..
-rw-r--r--.   1 root root  289 дек 29  2022 RedOS-3rdparty-clickhouse.
repo
-rw-r--r--.   1 root root  269 июн 28 10:43 RedOS-3rdparty-gitlab.repo
-rw-r--r--.   1 root root  331 июн 27 10:12 RedOS-3rdparty-keycloak.re
po
-rw-r--r--.   1 root root  269 июн 28 10:48 RedOS-3rdparty-pantum.repo
-rw-r--r--.   1 root root  269 янв 17  2023 RedOS-3rdparty-weasis.repo
[root@localhost ~]#
```

Для просмотра всех подключенных репозиториев выполните команду:

```
dnf repolist
```

```
[root@localhost ~]# dnf repolist
идентификатор репозитория     имя репозитория
3rdparty-clickhouse           Repositories for 3rdparty-clickhouse
3rdparty-gitlab               Repositories for 3rdparty-gitlab
3rdparty-keycloak             Repositories for 3rdparty-keycloak
3rdparty-pantum               Repositories for 3rdparty-pantum
3rdparty-weasis               Repositories for 3rdparty-weasis
PostgreSQL14                  PostgreSQL14 for RED OS 7.3
ansible6                      Ansible 6 Repository for RED OS 7.3
base                          RedOS - Base
kernels                       Kernels updates for RED OS 7.3
kernels6                      Repositories for kernels6
php81                         PHP 8.1 Repository for RED OS 7.3
updates                       RedOS - Updates
```

Управление пакетами

Поиск пакетов
Установка или обновление пакетов
Удаление установленных пакетов
Обновление ОС
Удаление из системы пакетов старых ядер
Просмотр списка установленных ядер
Установка очередности загрузки ядра в ОС
Графическая утилита kernel-manager
Настройка DNF для работы через proxy

Поиск пакетов

Если пользователь не знает точного названия пакета, для его поиска можно воспользоваться утилитой **dnf search**, которая позволяет искать не только по имени пакета, но и по его описанию.

Вы можете подробнее ознакомиться с информацией о поиске программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Команда вида:

```
dnf search <подстрока>
```

Позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Например:

```
dnf search gdm

========================= Имя точное соответствие: gdm =========================gdm.x86_64 : The
GNOME Display Managergdm.i686 : The GNOME Display Manager
==================== Имя и Краткое описание совпадение: gdm ====================gdm-devel.i686 :
Development files for gdmgdm-devel.x86_64 : Development files for gdmgdm-pam-extensions-devel.i686 : Macros for developing GDM
extensions to PAMgdm-pam-extensions-devel.x86_64 : Macros for developing GDM extensions to PAMgdm-presession-clean.noarch : RedOS
addons for gdmgdm-settings.noarch : GDM Settings
gschemas-gdm-redos.noarch : Brand gsettings for GDMovirt-guest-agent-gdm-plugin.noarch : Files for the GDM plug-in of the oVirt
                          : Guest Agent
root-gdml.i686 : GDML import/export for ROOT geometries
root-gdml.x86_64 : GDML import/export for ROOT geometries
```

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой **dnf info**, которая покажет информацию о пакете из репозитория. Пример использования команды:

```
dnf info gdm-devel

Имеющиеся пакеты
Имя         : gdm-develЭпоха       : 1
Версия      : 45.0.1
Выпуск      : 3.red80
Архитектура  : i686
Размер      : 25 k
Источник    : gdm-45.0.1-3.red80.src.rpm
Репозиторий  : updates
Краткое опис : Development files for gdm
URL         : https://wiki.gnome.org/Projects/GDM
Лицензия    : GPL-2.0-or-later
Описание    : The gdm-devel package contains headers and other
            : files needed to build custom greeters.

Имя         : gdm-develЭпоха       : 1
Версия      : 45.0.1
Выпуск      : 3.red80
Архитектура  : x86_64
Размер      : 25 k
Источник    : gdm-45.0.1-3.red80.src.rpm
Репозиторий  : updates
```

```
Краткое опис : Development files for gdm
URL          : https://wiki.gnome.org/Projects/GDM
Лицензия     : GPL-2.0-or-later
Описание     : The gdm-devel package contains headers and other
             : files needed to build custom greeters.
```

Установка или обновление пакетов

Примечание.

В связи с размещением в репозитории двух версий ядра — **LT** и **ML** — изменён принцип именования пакетов с модулями: **теперь непосредственно в имя пакета входит полная версия сборки ядра, которая может быть определена как uname -r**. Данный подход был реализован для возможности установки в системе нескольких пакетов с модулями под каждую из версий ядра, имеющихся в системе, с целью исключения конфликтов имён пакетов.

Более подробную информацию о принципах именования пакетов с модулями ядра можно посмотреть в данной статье.

Вы можете подробнее ознакомиться с информацией по установке и обновлению программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка пакета выполняется командой:

```
dnf install <имя_пакета>
```

DNF позволяет устанавливать в систему пакеты, требующие для работы другие, пока ещё не установленные. В этом случае они определяют, какие пакеты необходимо установить, и устанавливают их, пользуясь всеми доступными репозиториями.

Пример установки пакета **vsftpd**:

```
dnf install vsftpd

================================================================================
 Пакет         Архитектура     Версия              Репозиторий    Размер
================================================================================
Установка:
 vsftpd        x86_64        3.0.5-1.red80          base         157 k

Результат транзакции
================================================================================
Установка  1 Пакет

Объем загрузки: 157 k
Объем изменений: 348 k
Продолжить? [д/Н]: д
Загрузка пакетов:
vsftpd-3.0.5-1.red80.x86_64.rpm                298 kB/s | 157 kB     00:00
--------------------------------------------------------------------------------
Общий размер                                   294 kB/s | 157 kB     00:00
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
  Подготовка       :                                        1/1
  Установка        : vsftpd-3.0.5-1.red80.x86_64            1/1
  Запуск скриптлета: vsftpd-3.0.5-1.red80.x86_64            1/1
  Проверка         : vsftpd-3.0.5-1.red80.x86_64            1/1

Установлен:
  vsftpd-3.0.5-1.red80.x86_64

Выполнено!
```

Команда **dnf install <имя_пакета>** используется также для обновления уже установленного пакета или группы пакетов. В этом случае **dnf** дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи менеджера пакетов можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториев (например, полученный из Интернет). Для этого достаточно выполнить команду:

```
dnf install <путь_к_файлу.rpm>
```

При этом **DNF** проводит стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

Удаление установленных пакетов

Для удаления пакета используется следующая команда:

```
dnf remove <имя_пакета>
```

Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого: если отсутствует необходимый для работы приложения компонент (например, библиотека), то само приложение становится бесполезным.

Вы можете подробнее ознакомиться с информацией об удалении программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Обновление ОС

Для обновления всей системы рекомендуется использовать следующую команду:

```
dnf update
```

Она позволяет обновить те и только те установленные пакеты, для которых в репозиториях, перечисленных в **/etc/yum.repos.d**, имеются новые версии; при этом из системы не будут принудительно удалены никакие другие пакеты. Этот способ полезен при работе со стабильными пакетами приложений, относительно которых известно, что они при смене версии изменяются несущественно.

В случае обновления всего дистрибутива **DNF** проведёт сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, а также отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Всё, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчёте **dnf**, которым **DNF** соответственно предварит само обновление.

Вы можете подробнее ознакомиться с информацией об обновлении программных пакетов, просмотрев наши обучающие видео:

- на **RuTube** — Работа с пакетами в РЕД ОС;
- в **Яндекс.Дзен** — Работа с пакетами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Удаление из системы пакетов старых ядер

Вы можете подробнее ознакомиться с информацией об удалении из системы пакетов старых ядер, просмотрев наши обучающие видео:

- на **RuTube** — Удаление старых ядер из системы;
- в **Яндекс.Дзен** — Удаление старых ядер из системы;
- в **VK Видео** — Удаление старых ядер из системы.

На наших каналах вы также сможете найти много другой полезной информации.

Просмотр списка установленных ядер

1) Для того чтобы посмотреть установленные в системе пакеты ядра, можно воспользоваться консольной командой:

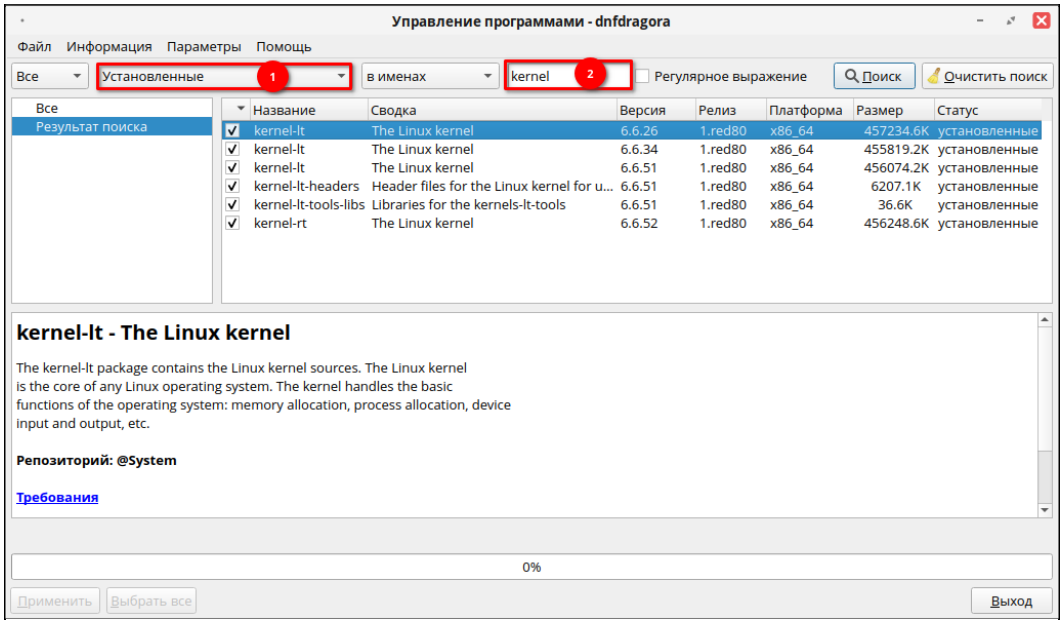
```
rpm -qa kernel-*
```

Для удаления можно воспользоваться утилитой **yum** или **dnf** в зависимости от используемой версии РЕД ОС.

```
dnf remove <имя_старого_пакета_ядра>
```

2) Также можно воспользоваться графической программой **dnfdragora**, расположенной по адресу **«Меню» - «Администрирование» - «dnfdragora»**. При запросе пароля привилегированного пользователя нужно ввести пароль локального пользователя с правами администратора.

Для отображения всех установленных пакетов ядер, наберите в поиске «**kernel**», предварительно выбрав пункт **«Установленные»**.



После этого снимите галочку напротив того пакета, который вы хотите удалить, и нажмите **«Применить»**. В открывшемся окне нажмите **«ОК»** и дождитесь конца операции.

3) Вы также можете воспользоваться командой с регулярным выражением:

- для BIOS:

```
awk -F\' '$1=="menuentry " {print i++ " : " $2}' /etc/grub2.cfg
```

- для EFI:

```
awk -F\' '$1=="menuentry " {print i++ " : " $2}' /etc/grub2-efi.cfg
```

Она выведет все установленные в системе ядра:

```
0 : RED OS (8.0)
```

Установка очередности загрузки ядра в ОС

Для установки очередности загрузки используется команда **grubby --set-default**.

Следующей командой укажите необходимый порядковый номер, под которым вы будете загружаться:

```
grubby --set-default 0
```

здесь **0** - это порядковый номер очередности загрузки, т.е. будет по умолчанию загружаться - **0 : RED OS (8.0)**.

Таким образом, если рядом стоит windows, то можно выбрать порядок загрузки ОС.

Графическая утилита kernel-manager

В репозитории РЕД ОС доступна специальная утилита для управления ядрами операционной системы - **kernel-manager**.

Подробнее о работе с утилитой см. в нашей статье «kernel-manager - утилита управления ядрами».

Настройка DNF для работы через proxy

По умолчанию **dnf** получает данные с HTTP-сервера. Все соединения **dnf** с **HTTP** происходят с использованием **HTTP / 1.1** протокола и совместимых с ним веб прокси-серверов.

Если вам необходимо разрешить доступ к **dnf** через proxy-сервер для всех пользователей, используйте файл **/etc/dnf/dnf.conf** и внесите в раздел [main] данные прокси и данные для аутентификации:

```
[main]
proxy=http://proxy.mydomain.com:3128
proxy_username=user_proxy
proxy_password=pass_user_proxy
```

В данном примере параметры:

- **proxy.mydomain.com** — адрес вашего proxy-сервера **:порт**;
- **proxy_username** — имя пользователя;
- **proxy_password** — пароль пользователя.

В результате файл **/etc/dnf/dnf.conf** примет следующий вид:



Здесь на скриншоте, в красном блоке, выделены строки, которые отвечают за настройку proxy для пакетного менеджера.

Если ваш proxy-сервер не использует авторизацию, достаточно прописать только:

```
proxy=http://proxy.mydomain.com:3128
```

Таким образом, файл /etc/dnf/dnf.conf требуется для настройки работы **dnf** через прокси для всех пользователей.

Чтобы разрешить доступ **dnf** через proxy-сервер для конкретного пользователя, вам необходимо использовать файл профиля пользователя. По умолчанию это **~/.bash_profile** в домашнем каталоге пользователя. Внесите в него следующие строки:

```
http_proxy="http://mycache.mydomain.com:3128"
export http_proxy
```

Если для работы proxy сервера необходимо использовать логин-пароль, то добавьте их в строку **http_proxy**:

```
http_proxy="http://user_proxy:pass_user_proxy@proxy.mydomain.com:3128"
```

Менеджер пакетов Dnfdragora

Установка
Обзор программы
Установка/удаление пакетов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** dnfdragora-2.1.6-1

Менеджер пакетов – это утилита, обеспечивающая поиск и установку пакетов из репозитория, а также обновление и удаление уже установленных пакетов на машине.

Для более удобной работы с пакетным менеджером в ОС установлена графическая утилита **dnfdragora**.

Установка

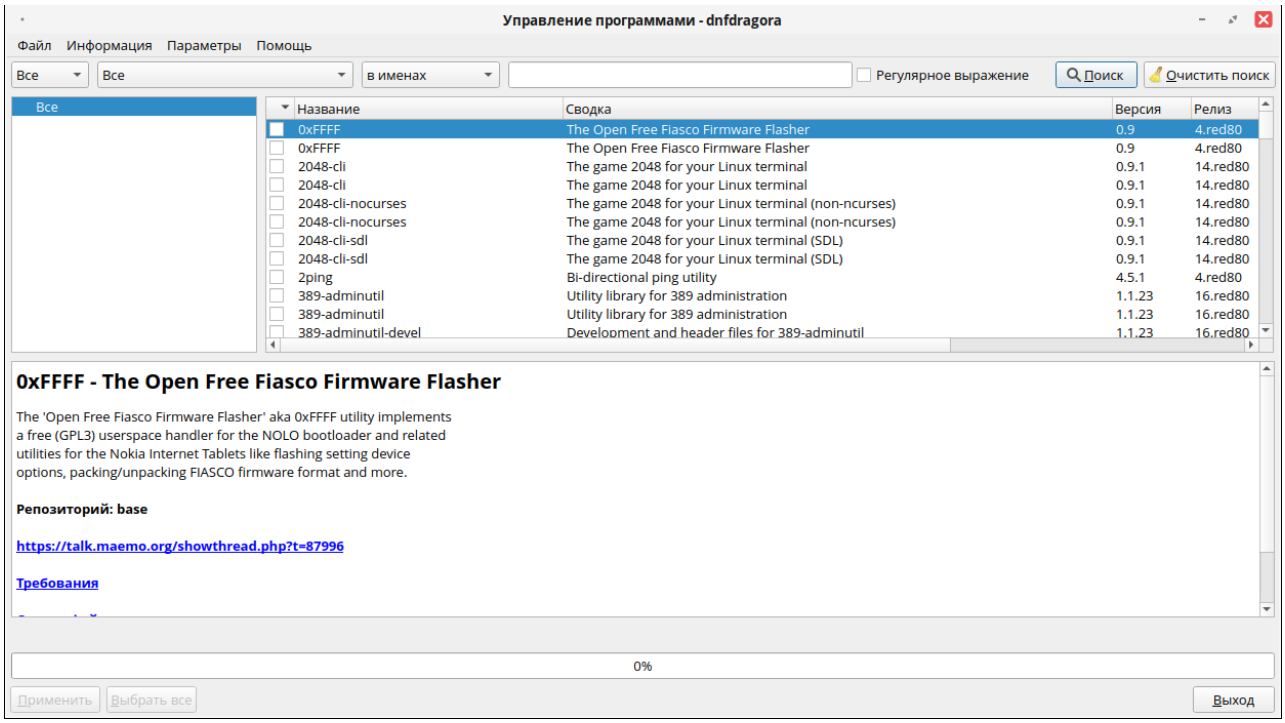
Dnfdragora установлена в РЕД ОС 8 по умолчанию. Если по какой-либо причине *dnfdragora* была удалена, установить ее можно через терминал **с правами администратора** системы командой:

```
dnf install dnfdragora
```

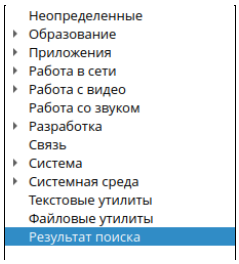
Запустить утилиту можно из «**Главного меню**» - «**Администрирование**» - «**Управление пакетами dnfdragora**».

Обзор программы

Окно программы выглядит следующим образом:



В левой части интерфейса утилиты располагается перечень групп пакетов, находящихся в репозиториях.

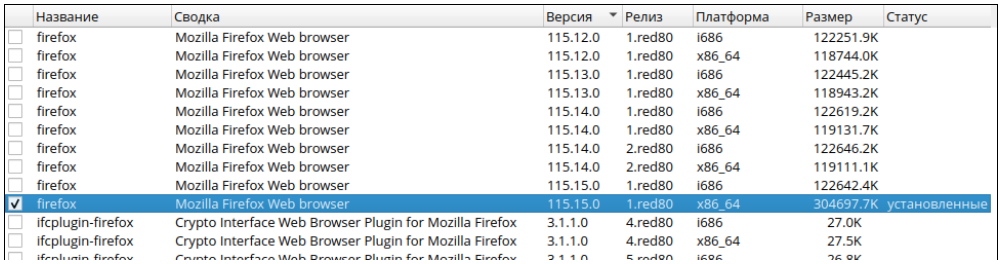


В верхней части расположена поисковая строка (**4**) и параметры поиска, отвечающие за:

- группировку пакетов (**1**);
- отображение пакетов в зависимости от их статуса или указанной архитектуры пакета (**2**);
- места поиска — в имени, описании или файлах внутри пакета (**3**).



В центральной части утилиты расположена область, где отображается результат поиска пакетов и некоторая информация о них. Здесь можно просмотреть полное название пакета, краткую сводку о нем, версию, номер релиза, платформу, размер, статус.



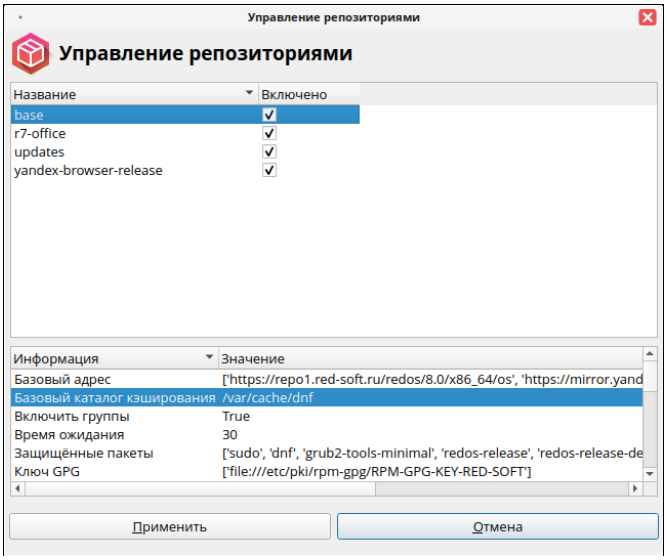
Название	Сводка	Версия	Релиз	Платформа	Размер	Статус
firefox	Mozilla Firefox Web browser	115.12.0	1.red80	i686	122251.9K	
firefox	Mozilla Firefox Web browser	115.12.0	1.red80	x86_64	118744.0K	
firefox	Mozilla Firefox Web browser	115.13.0	1.red80	i686	122445.2K	
firefox	Mozilla Firefox Web browser	115.13.0	1.red80	x86_64	118943.2K	
firefox	Mozilla Firefox Web browser	115.14.0	1.red80	i686	122619.2K	
firefox	Mozilla Firefox Web browser	115.14.0	1.red80	x86_64	119131.7K	
firefox	Mozilla Firefox Web browser	115.14.0	2.red80	i686	122646.2K	
firefox	Mozilla Firefox Web browser	115.14.0	2.red80	x86_64	119111.1K	
firefox	Mozilla Firefox Web browser	115.15.0	1.red80	i686	122642.4K	
firefox	Mozilla Firefox Web browser	115.15.0	1.red80	x86_64	304697.7K	установленные
ifcplugin-firefox	Crypto Interface Web Browser Plugin for Mozilla Firefox	3.1.1.0	4.red80	i686	27.0K	
ifcplugin-firefox	Crypto Interface Web Browser Plugin for Mozilla Firefox	3.1.1.0	4.red80	x86_64	27.5K	

В нижней части утилиты располагается информация о выбранном пакете. Здесь указано его название, описание, имя источника установки или репозитория, из которого его можно установить, сайт разработчика, требования к системе, список файлов в пакете, журнал изменений.

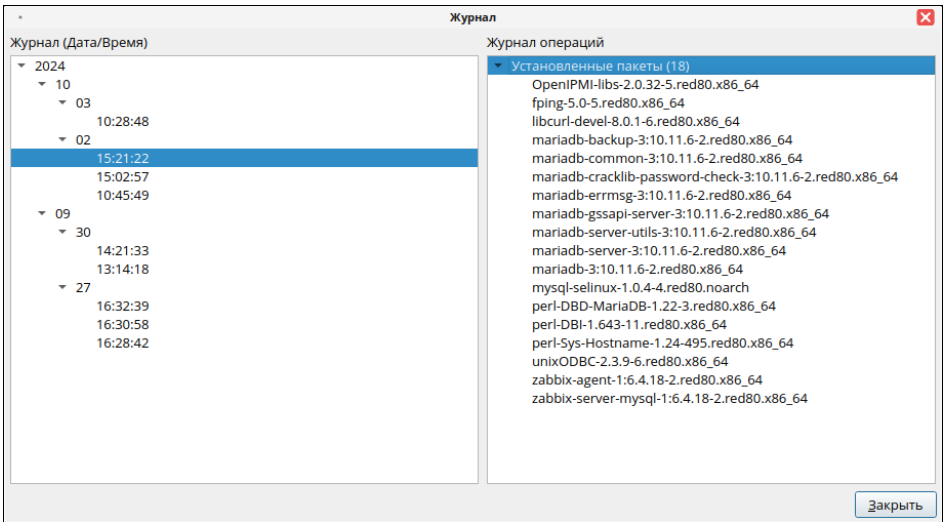


Во вкладке «**Файл**» - «**Обновить метаданные**» можно запустить обновление метаданных.

Во вкладке «**Файл**» - «**Репозитории**» можно просмотреть используемые репозитории и отключить или активировать их при необходимости.

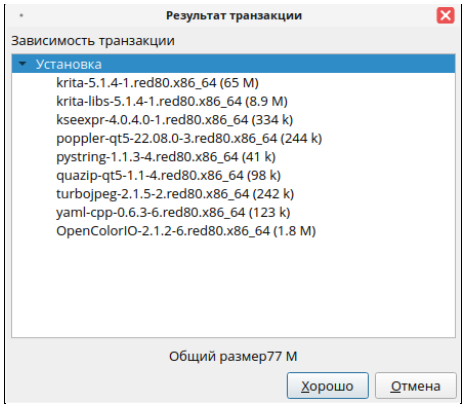


Во вкладке «**Информация**» - «**Журнал**» можно просмотреть историю операций в менеджере.



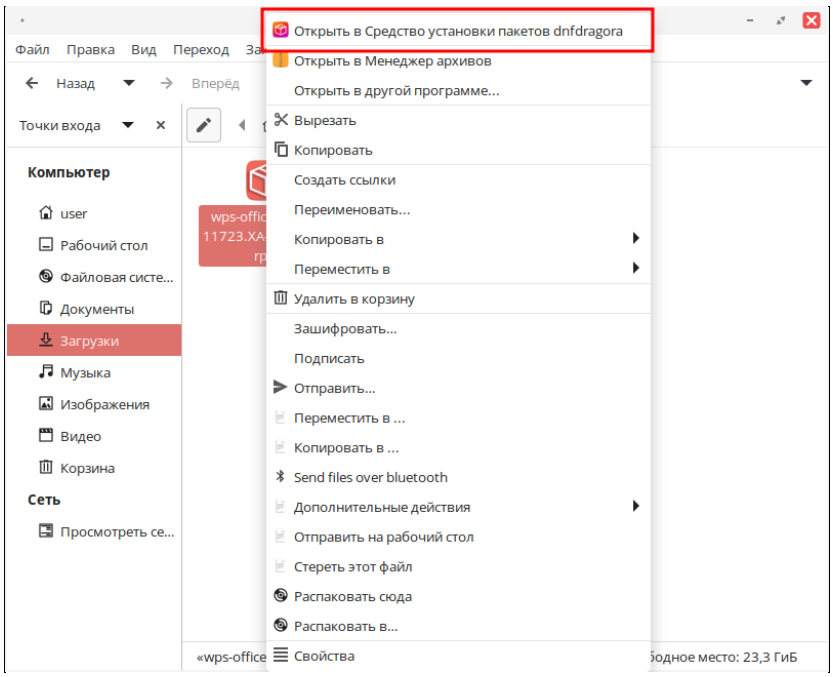
Установка/удаление пакетов

Для установки пакетов необходимо проставить признак выбора у нужного пакета (☑). Одновременно может быть выбрано несколько пакетов. После выбора пакетов нажмите «**Применить**» в левом нижнем углу. Будет выведен список транзакций, нажмите кнопку «**Хорошо**» в правом нижнем углу появившегося окна.

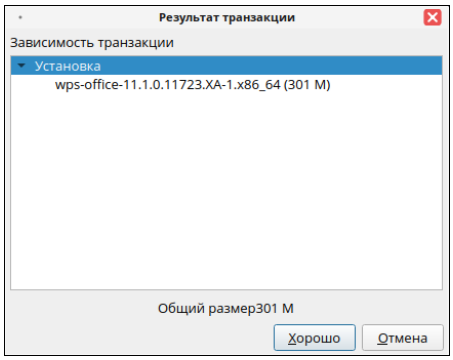


Для подтверждения выполнения операции необходимо ввести пароль (установка и удаление пакетов требует прав администратора). При успешной аутентификации начнется процесс скачивания и установки пакетов.

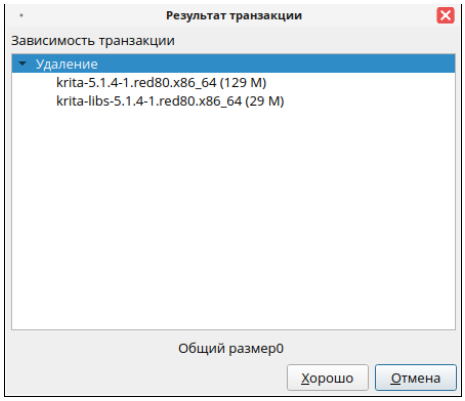
Также с помощью *dnfdragora* можно запускать установку **rpm**-пакетов с локального диска. Для этого достаточно открыть **rpm**-пакет с помощью *dnfdragora*.



Для запуска установки потребуется ввести пароль администратора, после чего начнется установка пакета.



Для удаления пакетов необходимо найти их в перечне установленных, убрать признак выбора, после чего нажать кнопку «**Применить**».



Назначение RPM

RPM – это менеджер пакетов, который может быть использован для сборки, установки, запроса, проверки, обновления и удаления отдельных программных пакетов.

Пакеты содержат архив с файлами и метаданные, используемые для установки и удаления файлов архива. Метаданные включают сценарии, атрибуты файлов и информацию с описанием конкретного пакета.

Пакеты бывают двух типов: двоичные пакеты, используемые для объединения устанавливаемых программ, и пакеты с исходными кодами, включающие исходные коды и описание способа формирования двоичного пакета.

База данных **RPM** ведётся в каталоге **/var/lib/rpm**. Она состоит из одиночной базы данных (**Packages**), в которой хранится вся информация о пакетах, и множества маленьких баз (**__db.001**, **__db.002** и т. д.), которые служат для индексации и содержат в себе сведения о том, какие файлы менялись и создавались при установке и удалении пакетов.

Если база данных повреждена (что может произойти, если процесс установки или удаления был принудительно завершен или закончилось место на разделе), то её можно восстановить, выполнив команду `rpm --rebuilddb`.

Если база была уничтожена — рекомендуется восстановить заранее созданную резервную копию.

Каждый пакет **RPM** имеет название, которое состоит из нескольких частей:

- название программы;
- версия программы;
- номер выпущенной версии (количество раз пересборки программы одной и той же версии);
- архитектура, под которую собран пакет (i386, ppc и т. д.)

Собранный пакет обычно имеет такой формат названия:

```
<название>-<версия>-<выпуск>.<архитектура>.rpm
```

Например:

```
nano-0.98-2.i386.rpm
```

Иногда в пакет входят исходные коды. Такие пакеты не содержат информации об архитектуре, она заменяется на **src**. Например:

```
libgnomeuimm2.0-2.0.0-3.src.rpm
```

Библиотеки чаще всего распространяются в двух отдельных пакетах. Первый содержит собранный код, второй (обычно к нему добавляют **-devel**) содержит заголовочные файлы и другие файлы, необходимые разработчикам. Необходимо следить за тем, чтобы версии этих двух пакетов совпадали, иначе библиотеки могут работать некорректно. Пакеты с расширением **noarch.rpm** не зависят от конкретной архитектуры компьютера. Обычно они содержат графику и тексты, используемые другими программами.

Основной список команд RPM

Если необходимо удалить определенный пакет, назовем его rpm_some_package, то нужно выполнить команду:

```
rpm -e rpm_some_package
```

Если необходимо показать список всех установленных rpm пакетов, используйте:

```
rpm -qa
```

PS: Можно отобрать нужные пакеты (со всех установленный) и показать список, например для nginx:

```
rpm -qa | grep nginx
```

Допустим, вам нужно просмотреть некоторую информацию о конкретном пакете (допустим — это rpm_some_package):

```
rpm -qi rpm_some_package
```

Если необходимо установить определенный пакет, назовем его rpm_some_package с выводом на экран и с прогресс-баром то нужно выполнить команду:

```
rpm -ivh rpm_some_package.rpm
```

Если необходимо обновить некий пакет rpm_some_package, но без всяких изменений в конфигурационных файлов (если отсутствует пакет, то он будет установлен):

```
rpm -Uvh rpm_some_package.rpm
```

Чтобы установить пакет rpm_some_package с выводом всех действий на экран и без контроля всех зависимостей, используйте:

```
rpm -ivh --nodeps rpm_some_package.rpm
```

Чтобы обновить пакет rpm_some_package (если он установлен), используйте:

```
rpm -F rpm_some_package.rpm
```

Чтобы показать список функциональностей которые предоставляются, выполните:

```
rpm -qip rpm_some_package --whatprovides
```

Показать историю ревизий данного пакета rpm_some_package:

```
rpm -qip rpm_some_package --changelog
```

Вывести скрипты, которые запускаются при установке/удалении пакета rpm_some_package:

```
rpm -qip rpm_some_package --scripts
```

Выполнить проверку (узнать какому пакету относится указанный файл), то нужно прописать полный путь к файлу:

```
rpm -qf /путь/к/файлу
```

Показать список файлов конфигурации которые входят в пакет rpm_some_package:

```
rpm -qc rpm_some_package
```

Показать весь список файлов которые входят в пакет rpm_some_package:

```
rpm -qlp rpm_some_package
```

Показать список всех пакетов, которые необходимы для установки данного пакета rpm_some_package по его зависимостям:

```
rpm -q rpm_some_package --whatrequires
```

Вывести список файлов, которые входят в пакет, но ещё не установленны в систему:

```
rpm -qp rpm_some_package.rpm -l
```

Команда что ниже выводит список всех rpm зависимостей:

```
rpm -qpR rpm_some_package.rpm
```

Если вы случайно обновили rpm до новой версии, вы можете вернуть все как было, используя команду:

```
rpm -Uvh --oldpackage rpm_some_package-<old-version>.rpm
```

Вывести содержимое всех пакетов которые установлены на ОС:

```
rpm -Va
```

Выполнить установку пакета, который собранный из исходных кода:

```
rpm -ivh /usr/src/redhat/RPMS/`arch`/rpm_some_package.rpm
```

Выполнить проверку пакета, который ещё не установлен на сервере:

```
rpm -Vp rpm_some_package.rpm
```

Извлечь из пакета файлы которые содержат в своём имени bin:

```
rpm2cpio rpm_some_package.rpm | cpio --extract --make-directories *bin*
```

Выполнить импорт публичный (public) ключа с цифровой подписью:

```
rpm --import /media/cdrom/RPM-GPG-KEY
```

Выполнить проверку подписи пакета rpm_some_package:

```
rpm --checksig rpm_some_package.rpm
```

Выполнить проверку на целостность установленного содержимого пакета:

```
rpm -qa gpg-pubkey
```

Показать какой размер, полномочия, тип, владельца, группу, а так же MD5 сумму и дату последнего изменения пакета rpm_some_package:

```
rpm -V rpm_some_package
```

Выполнить сборку пакета rpm_some_package из исходного кода:

```
rpmbuild --rebuild rpm_some_package.src.rpm
```

Для более детального ознакомления, используйте:

```
rpm --help
```

Преобразование форматов систем управления пакетами с помощью alien

Преобразование .deb в .rpm
Преобразование .rpm в .deb
Ключи и атрибуты alien

Alien – полезная утилита, созданная для преобразования форматов различных систем управления пакетами Linux.

Поддерживается преобразование между пакетами: Linux Standard Base (**.lsb**), Redhat (**.rpm**), Debian (**.deb**), Stampede (**.slp**), Solaris (**.pkg**) и Slackware (**.tgz**).

Для установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install alien
```

Преобразование .deb в .rpm

> Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Для преобразования файла **.deb** в файл **.rpm** с изменением стандартных для Debian-пакета инсталляционных скриптов используется опция **-r**. На выходе получится RPM-пакет.

В следующем примере файл *libreoffice-writer_7.0.5-0ubuntu0.20.10.1_amd64.deb* преобразуется в файл *libreoffice-writer-7.0.5-1.x86_64.rpm*:

```
alien -r --scripts libreoffice-writer_7.0.5-0ubuntu0.20.10.1_amd64.deb

libreoffice-writer-7.0.5-1.x86_64.rpm generated
```

Преобразование .rpm в .deb

Для преобразования файла **.rpm** в файл **.deb** используется опция **-d**. На выходе получится DEB-пакет:

```
alien -d --scripts libreoffice-writer-7.0.5-1.x86_64.rpm

libreoffice-writer_7.0.5-2_amd64.deb generated
```

Для того чтобы сгенерировать дерево, не создавая пакет, используется опция **-g**:

```
alien -g -c libreoffice-writer-7.0.5-1.x86_64.rpm

Directories  libreoffice-writer-7.0.5 and  libreoffice-writer-7.0.5.orig prepared
```

В корневом каталоге создались два подкаталога, не конвертируя пакет.

Alien позволяет преобразовывать сразу несколько файлов, для этого нужно последовательно прописать название двух или более пакетов:

```
alien -r -c firefox_89.0+build2-0ubuntu0.20.04.2_amd64.deb chromium-browser_85.0.4183.83-0ubuntu0.20.04.2_amd64.deb

firefox-89.0+build2-1.x86_64 generated
chromium-browser-85.0.4183.83-1.x86_64.rpm generated
```

Вы также можете использовать alien для преобразования файлов в пакет Stampede **.slp**, пакет LSB и пакет Slackware **.tgz**. Выполните **alien -h**, чтобы увидеть доступные параметры.

Ключи и атрибуты alien

- *file [...]* – задать список файлов пакета для конвертирования;
- *-to-deb, -d* – конвертировать в deb (используется приложением "по умолчанию");
- *-to-rpm, -r* – конвертировать в rpm;
- *-to-tgz, -t* – создать tgz-пакет;
- *-to-slp* – создать Stampede slp пакет;
- *-to-lsb, -l* – создать LSB пакет;
- *-to-pkg, -p* – создать Solaris pkg пакет;
- *-i* – автоматически установить все сгенерированные пакеты и после этого удалить сам файл пакета;
- *-g* – сгенерировать дерево построения, не создавая пакет;
- *-c* – включить скрипты в пакет;
- *-v* – отображать каждую команду, которую выполняет alien;
- *-k* – не менять версию генерируемых пакетов;
- *-V* – показать номер версии alien;
- *-h* – показать справку.

Процессы в РЕД ОС

Работа с процессами
Список запущенных процессов
Завершение процесса

Практически в любом контексте можно заменить слово «**процесс**» терминами «*программа*», «*команда*» или «*задача*». Внутри Linux-подобных систем нет принципиальных отличий между программой и командой. Обычно программы с текстовым выводом информации, например, **ls**, часто называются «*командами*».

Чтобы создать процесс, необходимо запустить на выполнение какой-либо исполняемый файл, то есть файл, у которого установлен атрибут «*исполняемый*». Иногда говорят, что надо «*выполнить файл*» или «*выполнить команду*».

После того как содержимое запущенного файла будет считано и помещено в оперативную память, а также будут размещены необходимые для работы программы данные, процесс начнет своё существование. Такой «*живой*» процесс иногда называют «*задачей*». Отсюда можно сформулировать определение: **процесс** — это совокупность программного кода и данных, загруженных в память вычислительного устройства.

Процесс может находиться в различных состояниях, обычно выделяют три основных состояния:

- ***работающий процесс*** — в данный момент времени код процесса выполняется, т.е. процесс занимает определенную часть ресурсов центрального процессора (процессорного времени);
- ***спящий процесс*** — в данный момент времени код процесса не выполняется, находясь в ожидании какого-либо события (например, нажатия клавиш на клавиатуре, поступление данных по сети и т.д.);
- ***процесс-«зомби»*** — состояние, когда сам процесс уже не существует, его код и данные выгружены из оперативной памяти, но запись в таблице процессов остаётся по тем или иным причинам.

Запустить программу или породить процесс можно двумя способами:

1) вводом имени команды в терминале и нажатием «*Enter*»;

2) нажатием ЛКМ по пиктограмме приложения в **Главном меню** или на **Рабочем столе**.

Вы можете подробнее ознакомиться с процессами, просмотрев наши обучающие видео:

- на **RuTube** — Процессы в среде РЕД ОС;
- в **Яндекс.Дзен** — Процессы в среде РЕД ОС;
- в **VK Видео** — Процессы в среде РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Работа с процессами

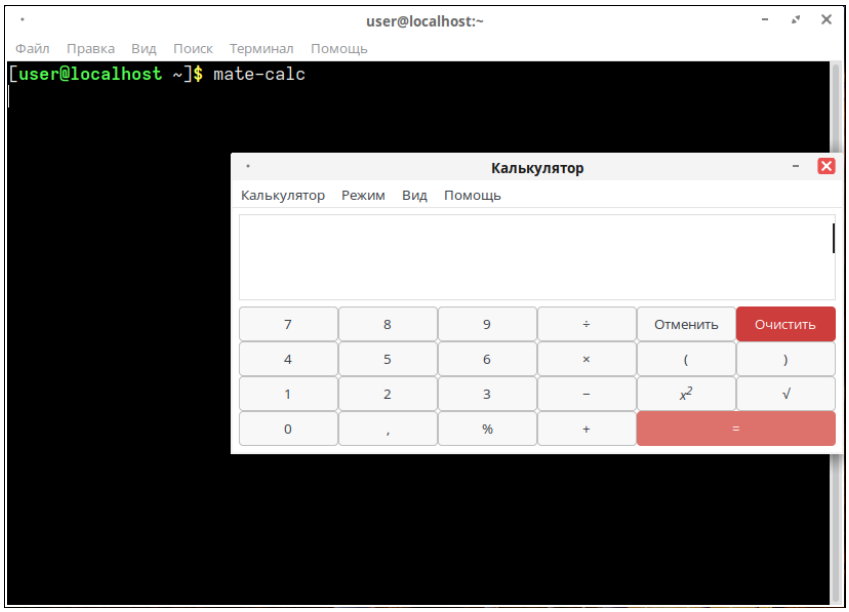
В качестве примера запустим приложение «**Калькулятор**» из командной строки, для чего необходимо открыть окно терминала и выполнить команду:

- для **MATE** и **KDE Plasma**:

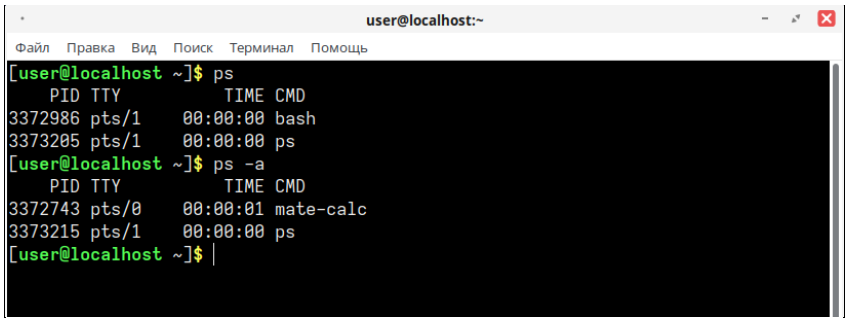
```
mate-calc
```

- для **GNOME**:

```
gnome-calculator
```



Затем откроем второе окно терминала и выполним последовательно команды `ps` и `ps -a`:



Вывод команд отличается.

Команда **ps** (*proccesses*) — это утилита командной строки, позволяющая работать со списком процессов в системе. Вызванная без параметров, она выводит список процессов, запущенных в данном терминале — в выводе показано, что были запущены командная оболочка **bash** и сама утилита **ps**.

Ключ **-a** позволяет вывести все интерактивные процессы, запущенные данным пользователем — в выводе команды отображается mate-calc, который был выполнен из другого терминального окна.

При закрытии окна терминала, из которого запускался калькулятор, будет закрыто и само приложение «Калькулятор». Обычно процессы связаны с терминалом, из которого они запускались. Такой терминал называется управляющим терминалом для процесса.

Именно названия терминалов были указаны в колонке **TTY** вывода запущенных ранее команд `ps` и `ps -a` — **pts/0** и **pts/1**.

```
[user@localhost ~]$ ps -a
    PID TTY          TIME CMD
3372743 pts/0    00:00:01 mate-calc
3373215 pts/1    00:00:00 ps
```

Важно также отметить, что калькулятор после запуска занял терминал — командная строка не появилась и процесс интерактивной работы с консолью в этом окне стал невозможным.

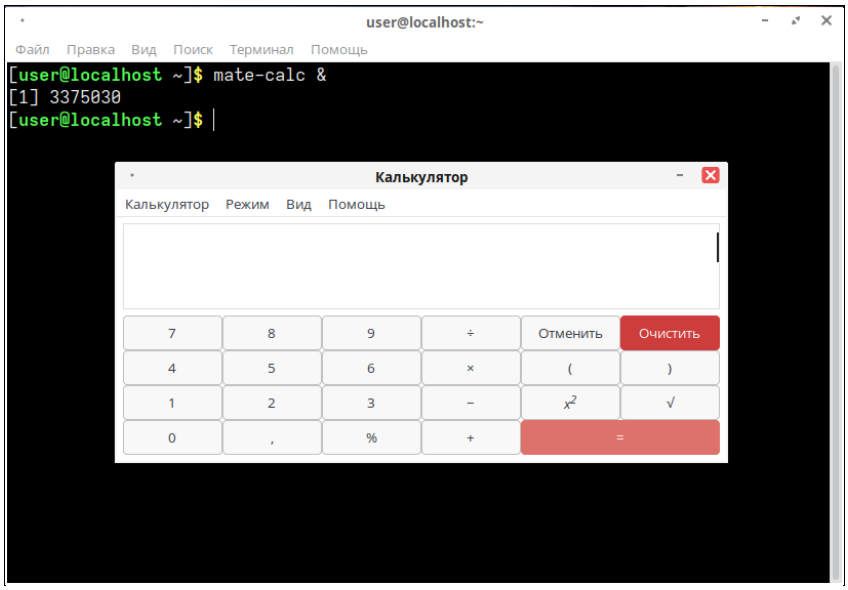
Когда необходимо выполнить программу так, чтобы она не занимала терминальное окно, следует запустить процесс как демон. Для этого в качестве последнего аргумента командной строки указывается символ «**&**»:

- для **MATE** и **KDE Plasma**:

```
mate-calc &
```

- для **GNOME**:

```
gnome-calculator &
```



Калькулятор запускается, а терминал доступен для дальнейшей работы. Однако, если снова закрыть окно терминала, калькулятор также прекратит работу. То есть управляющий терминал, даже если он предоставляет возможность дальнейшей работы с ним, всё равно является важным звеном в работе порождённого процесса.

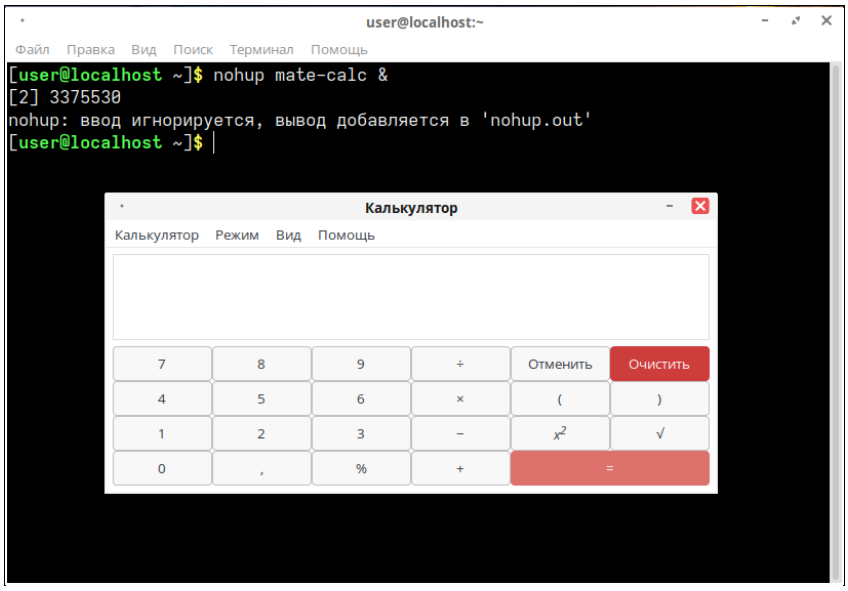
В случае, когда необходимо освободить терминал для работы и сделать запущенный процесс независимым, используется команда `nohup`, которая отвязывает процесс от управляющего терминала:

- для **MATE** и **KDE Plasma**:

```
nohup mate-calc &
```

- для **GNOME**:

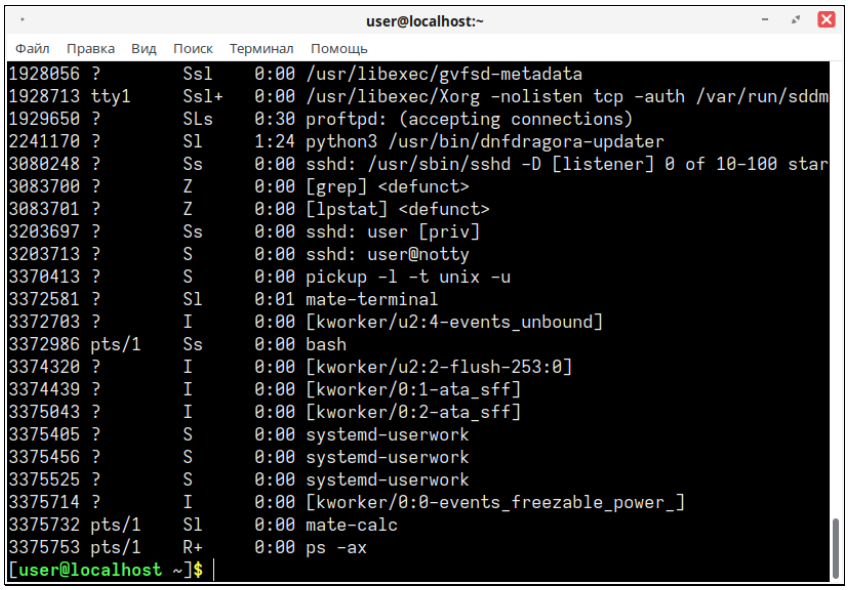
```
nohup gnome-calculator &
```



Теперь можно закрыть терминальное окно, а калькулятор продолжит свою работу. Причём в выводе команды `ps` данный процесс уже не будет отображен.

Список запущенных процессов

Чтобы увидеть весь список процессов, запущенных пользователем, включая не имеющие управляющего терминала, следует добавить ключ **-x** (`ps -ax`):



В *первом столбце* списка процессов отображаются некоторые числовые значения — это идентификаторы процессов — **PID** (***P****roccess* ***ID****entificator*), являющиеся «именами», по которым ядро операционной системы общается с процессами.

В *третьем столбце* списка запущенных процессов (**STAT**) находятся сокращённые обозначения состояния процесса:

- **R** — процесс выполняется в данный момент времени;
- **I** — простаивающий процесс;
- **D** — процесс выполняется, но ожидает ввода/вывода;
- **S** — спящий процесс;
- **T** — процесс остановлен, но пока не удалён из списка процессов и не выгружен его код из памяти;
- **X** — процесс мёртв, то есть код и данные находятся в памяти, но процесс не отзывается;
- **Z** — процесс-«зомби».

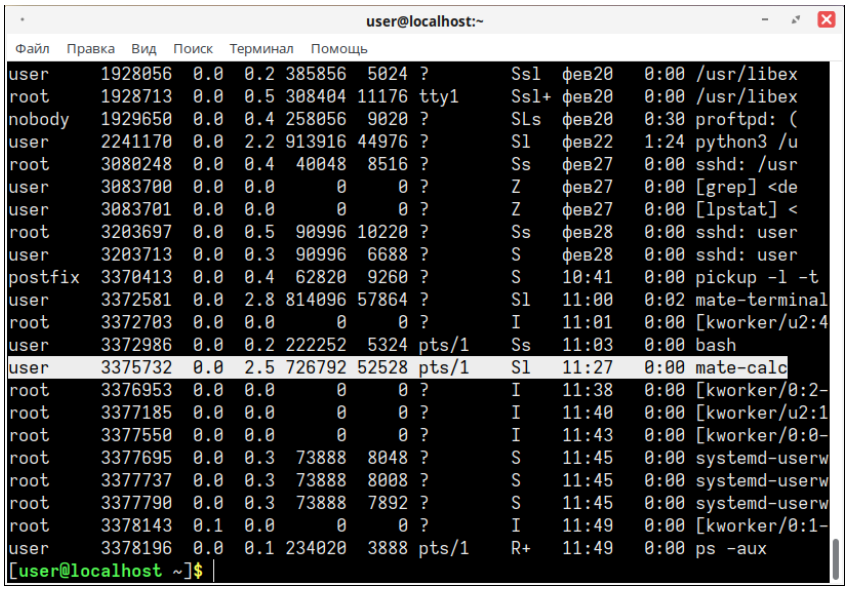
Каждый процесс инициализируется в сеансе какого-либо пользователя, и этот пользователь становится владельцем процесса. Если управляющий терминал можно убрать, то владельца у процесса изъять невозможно, однако его можно сменить на другого пользователя.

Таким образом, все файловые операции, которые будет выполнять процесс (если в программе это заложено), будут реализовываться в соответствии с правами доступа пользователя — владельца процесса.

Для просмотра владельца процесса утилитой ps используется ключ **-u**. Выполните команду:

```
ps -aux
```

В *первом столбце* списка процессов теперь будут отображены имена пользователей — владельцев процесса.



Например, при попытке сохранить файл *LibreOffice Writer* в каталоге **/etc** — будет выведено сообщение об ошибке, информирующее о

том, что сохранение невозможно из-за недостатка прав. Такая ситуация возникает, потому что процесс редактора *LibreOffice Writer* запускается с правами локального пользователя, а права на запись в паку **/etc** имеет **только** суперпользователь **root** (в чём можно убедиться в выводе команды `ls -l /etc`)!

Завершение процесса

Для завершения какого-либо запущенного процесса используется утилита **kill**. В качестве аргумента утилите необходимо передать **PID** процесса, который можно уточнить с помощью описанных выше команд. Подробную информацию об использовании утилиты **kill** см. в нашей статье «Основные утилиты в консоли РЕД ОС».

Следует обратить внимание на то, что пользователь может завершить только тот процесс, для которого он является владельцем. Администратор **root** может посылать любые сигналы любому процессу в системе, следовательно, может и прекратить работу любого процесса.

Получение сведений о процессах в РЕД ОС

Содержимое каталога /proc
Назначение файлов в каталогах процессов /proc/<PID>
Структура каталога /proc/sys

Процесс — это экземпляр запущенной программы. Каждый раз, когда в терминале выполняется какая-либо команда, система создает новый процесс. Процессы в операционной системе имеют числовой идентификатор, называемый **PID**.

Программы пространства пользователя в РЕД ОС не могут обращаться к ядру системы напрямую. Однако для получения информации от ядра были созданы некоторые специальные каталоги, с помощью которых любая программа или пользователь может получить данные о состоянии компьютера и ядра – это каталоги **/proc** и **/sys**.

Вы можете подробнее ознакомиться с назначением каталога **/proc** и файловой системы **procfs**, просмотрев наши обучающие видео:

- на **RuTube** — Файловая система procfs;
- в **Яндекс.Дзен** — Файловая система procfs.
- в **VK Видео** — Файловая система procfs.

На наших каналах вы также сможете найти много другой полезной информации.

С дополнительной информацией о работе с процессами можно ознакомиться в нашей статье «Процессы в РЕД ОС».

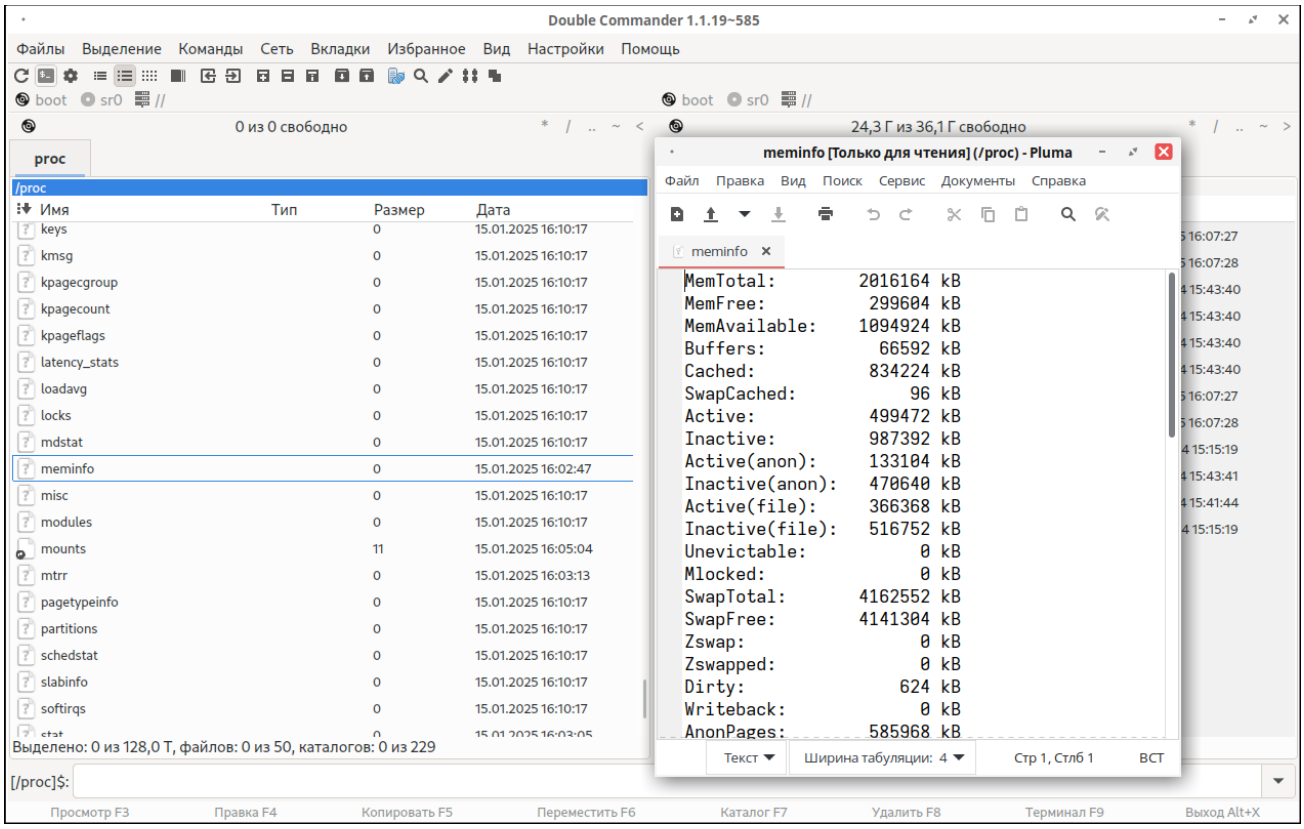
В рамках текущей статьи будет рассмотрен механизм получения сведений о процессах, на котором основаны все программы, позволяющие работать с процессами – работа с каталогом **/proc**.

В каталог **/proc** монтируется специальная файловая система **procfs**.

procfs — специальная файловая система, используемая в UNIX-подобных операционных системах, позволяющая получить доступ к информации из ядра о системных процессах, необходима для выполнения таких команд, как ps, w, top.

На самом деле каталог **/proc** – это не обычный каталог. Все подкаталоги, файлы и хранящаяся в них информация генерируются ядром «на лету», как только пользователь ее запрашивает. Работа построена таким образом, что пользователь может не заметить разницы между обычной файловой системой и **proc**, если откроет ее с помощью файлового менеджера.

Каталог **/proc** содержит файлы нулевого размера, у каждого файла отображается текущая дата создания. Например, файл **/proc/meminfo** будет содержать разные данные при каждом открытии, поскольку использование памяти постоянно изменяется.



С помощью такого механизма разработчики придерживаются главной концепции Unix: «Всё – есть файл». Все файлы доступны для изменения любым редактором, и все они представлены в простом текстовом формате, но для того чтобы проанализировать весь

каталог, необходимы права суперпользователя (**root**).

Большинство файлов в каталоге **/proc** доступны только для чтения, с их помощью можно только просмотреть информацию. Однако существуют и доступные для записи файлы, в частности – каталог **/proc/sys**, с помощью которого можно настраивать различные параметры ядра.

Содержимое каталога /proc

/proc/buddyinfo – файл отображает информацию о фрагментации памяти в ядре системы. Чаще всего используется для диагностики проблем с фрагментацией памяти.

```
cat /proc/buddyinfo
Node 0, zone      DMA      3      2      3      4      4      4      4      2      3      1      0
Node 0, zone    DMA32   3091   2531   1857    728    273    119     59     25      6      3      8
```

/proc/cmdline – файл отображает информацию о параметрах, которые были указаны в строке запуска ядра загрузчиком **grub**. Может быть полезно при поиске и устранении проблем с загрузкой ядра или в случае необходимости выявления файла, использованного для загрузки.

```
cat /proc/cmdline
BOOT_IMAGE=/vmlinuz-6.6.51-1.red80.x86_64 root=UUID=5b25f5f1-2ee8-4ee2-8b0d-524f3cde5e1e ro resume=UUID=cd77454c-60a6-4495-98e2-568a5279db77 rhgb quiet
```

/proc/consoles – файл отображает информацию о зарегистрированных в ядре символических устройствах для системной консоли **/dev/console**.

```
cat /proc/consoles
tty0                 -WU (EC p  )    4:2
```

/proc/cpuinfo – файл отображает очень подробную информацию о процессоре. Здесь можно просмотреть производителя, количество ядер, объем кеша, активные ядра, частоту, поддерживаемые расширения и многое другое. Ту же информацию можно получить с помощью специальных команд, однако все скрипты, выводящие информацию о процессоре, берут ее из каталога **/proc**.

```
cat /proc/cpuinfoprocessor : 0
vendor_id : GenuineIntel
cpu family : 6
model  : 158
model name : Intel(R) Core(TM) i5-9400 CPU @ 2.90GHz
stepping : 13
microcode : 0xea
cpu MHz  : 2903.998
cache size : 16384 KB
physical id : 0
siblings : 1
core id  : 0
cpu cores : 1
apicid  : 0
initial apicid : 0
fpu  : yes
fpu_exception : yes
cpuid level : 22
wp  : yes
[...]
```

/proc/devices – файл отображает информацию о различных блочных и символических устройствах, подключенных к системе, кроме тех, для которых не загружены модули ядра. Устройства разделены на *символические* и *блочные*. У символических устройств нет буфера хранения, поэтому они отправляют ядру данные определенного размера. Блочные устройства имеют буфер для данных и предназначены для сохранения информации, например, на жесткие диски.

```
cat /proc/devicesCharacter devices:
  1 mem
  2 pty
  3 ttyp
  4 /dev/vc/0
  4 tty
  4 ttyS
  5 /dev/tty
  5 /dev/console
```

```
  5 /dev/ptmx
  7 vcs
 10 misc
 13 input
 14 sound
 21 sg
 29 fb
116 alsa
128 ptm
136 pts
180 usb
188 ttyUSB
[...]
```

/proc/fb – файл отображает информацию об устройствах фреймбуфера (экраны), а также используемые графические драйверы. Файл является одним из способов просмотра используемого драйвера видеокарты.

```
cat /proc/fb
0 qxldrmfb
```

/proc/filesystems – файл содержит список файловых систем, которые на данный момент поддерживаются ядром. Значение **nodev** показывает, что это файловая система специального назначения, и она не используется для хранения данных на носителях.

```
cat /proc/filesystems
nodev sysfs
nodev tmpfs
nodev bdev
nodev proc
nodev cgroup
nodev cgroup2
nodev cpuset
nodev devtmpfs
nodev configfs
nodev debugfs
nodev tracefs
nodev securityfs
nodev sockfs
nodev bpf
nodev pipefs
nodev ramfs
nodev hugetlbfs
nodev devpts
 ext3
 ext2
 ext4
[...]
```

/proc/kcore – это все содержимое оперативной памяти, представленное в одном файле. В отличие от других у этого файла есть размер – объем ОЗУ плюс 4 Кб. Для доступа к файлу необходимы права суперпользователя (**root**). Перед работой с файлом его необходимо скопировать в другой каталог, а затем выполнять требуемые действия.

```
cat /proc/kcore
[...]
PAGESIZE=4096
SYMBOL(init_uts_ns)=ffffffff862b4fe0
OFFSET(uts_namespace.name)=0
SYMBOL(node_online_map)=ffffffff8631a3c0
SYMBOL(swapper_pg_dir)=ffffffff8601c000
SYMBOL(_stext)=ffffffff84000000
SYMBOL(vmap_area_list)=ffffffff861c8f30
SYMBOL(mem_section)=ffff9c9f7ffb1000
LENGTH(mem_section)=2048
SIZE(mem_section)=16
OFFSET(mem_section.section_mem_map)=0
NUMBER(SECTION_SIZE_BITS)=27
NUMBER(MAX_PHYSMEM_BITS)=46
SIZE(page)=64
SIZE(pglist_data)=175424
SIZE(zone)=1728
SIZE(free_area)=104
SIZE(list_head)=16
```

```
SIZE(nodemask_t)=128
OFFSET(page.flags)=0
OFFSET(page._refcount)=52
[...]
```

/proc/kmsg – файл накапливает и сохраняет сообщения ядра. Сообщения можно посмотреть также с помощью утилиты **dmesg**. Для доступа к файлу потребуются права суперпользователя (**root**).

```
cat /proc/kmsg
[...]
<6>[    1.469422] Freeing unused decrypted memory: 2028K
<6>[    1.471034] Freeing unused kernel image (initmem) memory: 4392K
<6>[    1.471067] Write protecting the kernel read-only data: 32768k
<6>[    1.472590] Freeing unused kernel image (rodata/data gap) memory: 1548K
<6>[    1.504398] x86/mm: Checked W+X mappings: passed, no W+X pages found.
<6>[    1.504415] rodata_test: all tests were successful
<6>[    1.504430] Run /init as init process
<7>[    1.504434]   with arguments:
<7>[    1.504436]     /init
<7>[    1.504437]     rhgb
<7>[    1.504438]   with environment:
<7>[    1.504439]     HOME=/
<7>[    1.504440]     TERM=linux
<7>[    1.504441]     BOOT_IMAGE=/vmlinuz-6.6.51-1.red80.x86_64
[...]
```

/proc/loadavg – файл позволяет оценить среднюю нагрузку на систему. Первые три цифры показывают нагрузку на процессор в данный момент времени, 5 минут назад и 15 минут назад, следующие два столбца показывают количество активных процессов и общее количество запущенных процессов. Последняя цифра — это идентификатор последнего процесса (**PID**).

```
cat /proc/loadavg
0.04 0.19 0.56 1/487 5764
```

/proc/meminfo – файл отображает всю доступную информацию об оперативной памяти и пространстве подкачки.

```
cat /proc/meminfo
MemTotal:        2016164 kB
MemFree:           88360 kB
MemAvailable:     181764 kB
Buffers:            7920 kB
Cached:           206472 kB
SwapCached:         6240 kB
Active:           972320 kB
Inactive:         595760 kB
Active(anon):     814268 kB
Inactive(anon):   553056 kB
Active(file):     158052 kB
Inactive(file):    42704 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:       4162552 kB
SwapFree:        3227384 kB
Zswap:                 0 kB
Zswapped:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:       1350020 kB
Mapped:            95860 kB
Shmem:             13636 kB
```

/proc/modules – файл содержит список всех загруженных модулей ядра. Ту же информацию можно увидеть, выполнив команду **lsmod**.

```
cat /proc/modules
uinput 20480 1 - Live 0x0000000000000000
snd_seq_dummy 12288 0 - Live 0x0000000000000000
snd_hrtimer 12288 1 - Live 0x0000000000000000
qrtr 49152 2 - Live 0x0000000000000000
rfkill 28672 3 - Live 0x0000000000000000
sunrpc 839680 1 - Live 0x0000000000000000
snd_hda_codec_generic 110592 1 - Live 0x0000000000000000
```

```
ledtrig_audio 12288 1 snd_hda_codec_generic, Live 0x0000000000000000
snd_hda_intel 61440 2 - Live 0x0000000000000000
intel_rapl_msr 20480 0 - Live 0x0000000000000000
intel_rapl_common 36864 1 intel_rapl_msr, Live 0x0000000000000000
snd_intel_dspcfg 36864 1 snd_hda_intel, Live 0x0000000000000000
snd_intel_sdw_acpi 16384 1 snd_intel_dspcfg, Live 0x0000000000000000
snd_hda_codec 204800 2 snd_hda_codec_generic,snd_hda_intel, Live 0x0000000000000000
snd_hda_core 135168 3 snd_hda_codec_generic,snd_hda_intel,snd_hda_codec, Live 0x0000000000000000
kvm_intel 409600 0 - Live 0x0000000000000000
snd_hwdep 16384 1 snd_hda_codec, Live 0x0000000000000000
kvm 1302528 1 kvm_intel, Live 0x0000000000000000
[...]
```

/proc/mounts – файл содержит все точки монтирования и все подключенные файловые системы.

```
cat /proc/mountsproc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
sysfs /sys sysfs rw,seclabel,nosuid,nodev,noexec,relatime 0 0
devtmpfs /dev devtmpfs rw,seclabel,nosuid,size=4096k,nr_inodes=1048576,mode=755,inode64 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,seclabel,nosuid,nodev,inode64 0 0
devpts /dev/pts devpts rw,seclabel,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,seclabel,nosuid,nodev,size=403236k,nr_inodes=819200,mode=755,inode64 0 0
cgroup2 /sys/fs/cgroup cgroup2 rw,seclabel,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,seclabel,nosuid,nodev,noexec,relatime 0 0
bpf /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
/dev/sda4 / ext4 rw,seclabel,relatime 0 0
[...]
```

/proc/partitions – в файле отображены все подключенные к системе разделы жестких дисков или других запоминающих устройств.

```
cat /proc/partitions
major minor  #blocks  name

   8        0   41943040 sda
   8        1       1024 sda1
   8        2    1048576 sda2
   8        3    2147328 sda3
   8        4   38744064 sda4
  11        0    1048575 sr0
 252        0    2015232 zram0
```

Назначение файлов в каталогах процессов /proc/<PID>

Для отображения файлов какого-либо процесса следует открыть каталог с номером необходимого процесса. В каждом каталоге более 50 файлов.

Далее будет рассмотрено назначение некоторых файлов:

- **cmdline** – содержит команду, с помощью которой был запущен процесс, а также переданные ей параметры;
- **cwd** – символическая ссылка на текущий рабочий каталог процесса;
- **exe** – ссылка на исполняемый файл;
- **root** – ссылка на каталог суперпользователя (**root**);
- **environ** – переменные окружения, доступные для процесса;
- **fd** – содержит файловые дескрипторы, файлы и устройства, которые использует процесс;
- **maps**, **statm**, и **mem** – информация о памяти процесса;
- **stat**, **status** – состояние процесса.

Структура каталога /proc/sys

Каталог **/proc/sys** содержит файлы с параметрами ядра. Файлы доступны не только для чтения, но и для редактирования с целью передачи ядру ОС новых значений параметров.

Каталог содержит подкаталоги, разделённые по типам хранимых параметров. Далее будет рассмотрено назначение некоторых

файлов:

- **debug** – содержит отладочную информацию, она будет полезна для разработчиков ядра;
- **dev** – содержит параметры различных устройств, подключенных к системе;
- **fs** – содержит всю информацию о файловой системе;
- **kernel** – позволяет напрямую настраивать ядро;
- **net** – позволяет настраивать различные параметры сети;
- **vm** – содержит ряд файлов и подкаталогов, соответствующих переменным ядра с подсистемой виртуальной памяти.

Более подробную информацию о каталоге **/proc** также можно просмотреть, выполнив команду:

```
man proc
```

Журналирование событий в РЕД ОС

Журнал пространства ядра
Журналы пользовательского пространства
Основные файлы журналов
Службы журналов

Журналы являются неотъемлемой частью любой ОС. В журналы записывается хронология событий, происходящих в используемой ОС, ее приложениях и службах.

Журналы являются полезным инструментом при возникновении различного рода неполадок системы и позволяют точно определять проблемы путем изучения предупреждений и сообщений об ошибках. Журналы событий используются для выявления инцидентов безопасности, диагностики проблем с производительностью, а также для обеспечения соответствия требованиям и аудита.

Журнал пространства ядра

Ядро ОС использует кольцевой буфер для хранения сообщений журнала, начиная с процесса загрузки системы. Этот буфер имеет фиксированный размер. После заполнения буфера новые сообщения будут перезаписывать старые. Все сообщения ядра записываются в кольцевой буфер с помощью функции `printk()`. Далее сообщения из кольцевого буфера ядра сохраняются в файлах журнала в постоянном хранилище системы – **/var/log/kern.log**. Параметр конфигурации ядра `CONFIG_PRINTK` позволяет вести журнал пространства ядра через `printk()`. Если он не установлен, системные вызовы ядра возвращают ошибку `ENOSYS`.

Сообщения ядра имеют собственные уровни (приоритеты), которые определяются ядром ОС для выявления серьезности конкретного сообщения.

Далее приведены доступные уровни (приоритеты) сообщений ядра:

- `KERN_EMERG` — экстренные сообщения (наивысший приоритет);
- `KERN_ALERT` — ошибка, требующая немедленного внимания;
- `KERN_CRIT` — критическая ошибка (аппаратная или программная);
- `KERN_ERR` — ошибка;
- `KERN_WARNING` — предупреждение;
- `KERN_NOTICE` — замечание;
- `KERN_INFO` — информационное сообщение;
- `KERN_DEBUG` — отладочные сообщения;
- `KERN_DEFAULT` — уровень ведения журнала ядра по умолчанию;
- `KERN_CONT` — продолжение ведения журнала (низший приоритет).

Все сообщения функции `printk()` записываются в кольцевой буфер ядра. Кольцевой буфер является файлом символьного устройства – **/dev/kmsg**. Устройство **/dev/kmsg** является абстракцией, предназначенной для чтения и записи в кольцевой буфер ядра.

Для управления кольцевым буфером ядра или его печати в стандартный вывод в консоли используется команда `dmesg`.

```
dmesg

[    3.330401] PM: Image not found (code -22)
[    5.508468] kauditd_printk_skb: 4 callbacks suppressed
[    5.508471] audit: type=1130 audit(1719211645.071:15): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=kernel
msg='unit=systemd-fsck-root comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
[    5.539630] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Quota mode: none.
[    5.592869] audit: type=1334 audit(1719211645.157:16): prog-id=8 op=UNLOAD
[    5.592980] audit: type=1334 audit(1719211645.157:17): prog-id=7 op=UNLOAD
```

Журналы пользовательского пространства

Журналирование может осуществляться как на локальной системе, так и в сети.

Ведение журналов пользовательского пространства основано на протоколе **rsyslog**. **Rsyslog** — это быстрый, расширяемый сервис для управления журналами с большим количеством возможностей. Среди его возможностей можно отметить поддержку фильтрации контента, а также передачу журналов по сети.

В конфигурационном файле **/etc/rsyslog.conf** возможна тонкая регулировка уровня журналирования. Журналирование

осуществляется при помощи службы **rsyslog.service**, которая обычно получает входную информацию при помощи сокета **/dev/log** (локально) или с **UDP**-порта **514** (с удаленных машин).

Сообщения журналов пространства пользователя имеют собственные уровни (приоритеты) событий. Приоритеты системного журнала указывают на серьезность зафиксированного сообщения. Значения приоритетов сообщений варьируются от **0** до **7**, где **0** является наиболее *критическим* уровнем.

Далее приведены приоритеты сообщений и их описание:

Приоритет	Ключевое слово	Серьезность инцидента	Описание
0	emerg	Экстренная ошибка	Система не может использоваться.
1	alert	Важное предупреждение	Необходимо немедленно принять меры.
2	crit	Критическая ошибка	Описание критической ошибки.
3	err	Ошибка	Описание ошибки.
4	warning	Предупреждение	Описание предупреждения.
5	notice	Уведомление	Важные сообщения.
6	info	Информация	Информационные сообщения.
7	debug	Отладка	Отладочные сообщения.

Важным значением в сообщениях журнала также является категория программы, которая сформировала данное сообщение. Значение категории программы варьируется от **0** до **23**.

Далее приведены категории программ:

Приоритет	Ключевое слово	Описание
0	kern	Сообщения ядра ОС.
1	user	Сообщения на уровне пользователя.
2	mail	Сообщения почтовых систем.
3	daemon	Сообщения от прочих системных служб.
4	auth	Сообщения безопасности или аутентификации, генерируемые системами авторизации или программами, которые запрашивают имена пользователей и пароли. Например, **su**, **login**, **ftpd**.
5	syslog	Внутренние сообщения **syslog**.
6	lpr	Сообщения, связанные с системой печати.
7	news	Сообщения подсистемы сетевых новостей (**nntp**).
8	uucp	Сообщения подсистемы **UUID**.
9	cron	Сообщения от подсистемы **cron**.
10	authpriv	Сообщения безопасности или аутентификации, аналогичен **auth**.
11	ftp	Сообщения службы **FTP**.
12	ntp	Сообщения подсистемы сетевого времени (**ntp**).
13	security	Журнал аудита.
14	console	Журнал оповещений.
15	solaris-cron	Сообщения службы планирования заданий.
16-23	local0-local7	Зарезервировано для локального использования.

Основные файлы журналов

По умолчанию события журналируются в каталог **/var/log/**. В нем хранится множество различных файлов с расширением ***.log**, содержащих события от различных источников в текстовом виде.

К основным файлам журналов относятся:

- **/var/log/rsyslog** или **/var/log/messages** — глобальный системный журнал, где хранятся события, произошедшие с момента запуска системы от различных компонентов ОС — ядра, служб, устройств и т. д.;
- **/var/log/kern.log** — содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок, произошедших при работе пользовательских модулей, встроенных в ядро;

- **/var/log/auth.log** или **/var/log/secure** — наиболее интересны для службы безопасности, так как содержат информацию об авторизации пользователей, т.е. попытки успешных/неуспешных входов в систему и методов аутентификации;
- **/var/log/dmesg** – в файле фиксируются ошибки работы драйверов и оборудования;
- **/var/log/anaconda.log** – в файле находятся события установки системы;
- **/var/log/boot.log** – в файле находятся логи загрузки системы;
- **/var/log/audit** — лог службы **auditd**;
- **/var/log/cron** — содержит результаты выполнения различных событий планировщика задач cron.

Также в зависимости от установленных приложений в **/var/log/** могут находиться журналы БД MySQL или веб-серверов Apache/Nginx.

Службы журналов

Служба **rsyslog** обеспечивает расширенную фильтрацию, различные параметры конфигурации, ретрансляцию сообщений с защитой от шифрования, модули ввода и вывода, а также поддержку транспортировки по протоколам **TCP** или **UDP**.

Помимо **rsyslog** файлами журналов также может управлять системная служба ведения журналов **journald** (компонент **systemd**). Служба **journald** собирает сообщения системного журнала, сообщения журнала ядра, сообщения о начальной загрузке с диска RAM и сообщения о ранней загрузке, а также сообщения, записанные в стандартный вывод и стандартный вывод ошибок всех служб, индексирует их и делает доступными для пользователя.

Основное различие между **rsyslog** и **journald** заключается в том, что файлы журналов, создаваемые **journald**, по умолчанию не являются постоянными. Файлы журналов хранятся только в памяти или небольшом кольцевом буфере в каталоге **/run/log/journal/**. **Rsyslog**, в свою очередь, хранит журналы в файлах журналов, доступных по адресу **/var/log/**.

Для просмотра содержимого журналов службы **journald** необходимо использовать команду:

```
journalctl
```

Для вывода справки по использованию утилиты выполните:

```
journalctl -h
```

Все настройки **journald** находятся в файле **/etc/systemd/journald.conf** и других конфигурационных файлах из директории **/etc/systemd/journald.conf.d**. По умолчанию все параметры в файле **/etc/systemd/journald.conf** закомментированы — они сообщают, какие значения используются по умолчанию. Значения параметров, установленных в файле **/etc/systemd/journald.conf** могут быть переопределены в одном из файлов в директории **/etc/systemd/journald.conf.d**.

Общая информация

РЕД ОС, как и любой UNIX – многопользовательская операционная система. Также имеются группы пользователей, основное предназначение которых - облегчить управление большим количеством пользователей, а также более точно распределить права доступа к различным объектам системы. Пользователи и группы внутри системы обозначаются цифровыми идентификаторами - UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод ее может быть примерно следующим:

```
id

uid=1000(test) gid=1000(test) группы=1000(test),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 1000) входит в группы *test* и *wheel*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Вы можете подробнее ознакомиться с информацией по управлению пользователями в системе, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

ВНИМАНИЕ!

В связи с тем, что в дистрибутивах РЕД ОС большинство привилегированных системных утилит имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

Роли пользователей

Роль sysadm - администратор системы
Роль — пользователь системы

В ОС пользователи по умолчанию сопоставляются SELinux-пользователю <**unconfined_u**>. SELinux-пользователь <**unconfined_u**>, в свою очередь, сопоставлен ролям <**unconfined_r**> и <**system_r**>.

Обе роли <**unconfined_r**> и <**system_r**> сопоставляются доменам безопасности SELinux. Домены безопасности SELinux - это определённые окружения безопасности для процессов.

Неограниченный домен безопасности <**unconfined_t**> - зарезервированное окружение для процессов, которые в значительной степени освобождены от ограничений SELinux. Роль <**system_r**> сопоставляется доменам безопасности для системных процессов.

SELinux-пользователь <**unconfined_u**> имеет доступ к роли <**system_r**>, чтобы иметь возможность запускать системные процессы в своих доменах безопасности. SELinux-пользователь <**unconfined_u**> работает в домене безопасности <**unconfined_t**> через роль <**unconfined_r**>, которой он сопоставлен.

Команда «semanage» позволяет добавлять, изменять и удалять сопоставления между ОС- и SELinux-пользователями, так же как и другие настройки, касающиеся управления SELinux.

Чтобы с помощью команды «semanage» посмотреть какому SELinux- пользователю по умолчанию сопоставлены пользователи ОС, наберите:

```
semanage login -l | grep default
```

В примере выше пользователи по умолчанию сопоставлены SELinux- пользователю <**unconfined_u**>.

Чтобы изменить это и сопоставить пользователей по умолчанию ограниченному SELinux-пользователю с именем <**user_u**>, просто наберите:

```
semanage login -m -s user_u "__default__"
```

В результате все новые пользователи будут по умолчанию сопоставляться ограниченному SELinux-пользователю <**user_u**>.

Вы можете переопределить данное сопоставление при добавлении пользователей командой «**useradd**» используя опцию «**-Z**». Эта опция определяет, какому SELinux-пользователю должен быть сопоставлен пользователь ОС.

Например, наберите:

```
useradd -Z guest_u joe
```

В результате будет создан новый пользователь с именем **joe**, который будет сопоставлен SELinux-пользователю <**guest_u**>, вместо определённого по умолчанию SELinux-пользователя.

Также для изменения сопоставления между пользователем и SELinux-пользователем может быть использована команда «**usermod**» с опцией «**-Z**».

Существует несколько предопределённых профилей SELinux-пользователей. Список данных профилей можно вывести командой «**semanage**», наберите:

```
semanage user -l
```

SELinux-пользователь <**unconfined_u**> - это среда, в которой по умолчанию работают все пользователи. Этот пользователь в значительной степени освобождён от ограничений, накладываемых SELinux. Если Вы хотите повысить безопасность вашей системы, тогда не следует сопоставлять реальных пользователей, не пользователя root, SELinux-пользователю <**unconfined_u**>.

Вход пользователя root должен быть запрещён. Root должен иметь возможность войти с терминала только в случае крайней необходимости. Чтобы повысить безопасность использования root, можно сопоставить пользователя root SELinux-пользователю <**sysadm_u**>.

Ролевой доступ SELinux используется для обеспечения возможности назначения нескольких ограниченных окружений SELinux одному SELinux-пользователю.

В SELinux роли пользователя (*User Roles*) - это домены пользователя или пользовательские домены (*User Domains*). Когда упоминаются роли, часто имеется в виду дополнительный (*secondary*) пользовательский домен пользователя SELinux. Часто роли, предназначенные для использования в качестве дополнительных доменов пользователя, отличаются от основных (*primary*) доменов. Это объясняется тем, что пользователи ОС фактически не используют для входа в систему роли, созданные как дополнительные домены пользователя. Вместо этого пользователи Linux, используя команду «**sudo**» или комбинацию команд «**su**» и «**newrole**», осуществляют переключение домена или доменный переход (*Domain Transition*) к их дополнительной роли.

Роль sysadm - администратор системы

Пример роли, предназначенной для использования в качестве основного домена пользователя. SELinux пользователь <**sysadm_u**> сопоставлен роли <**sysadm_r**>. Это сопоставление можно увидеть, выполнив команду:

```
semanage user -l | grep sysadm_u
```

По умолчанию пользователи ОС, сопоставленные пользователю SELinux <**sysadm_u**>, работают с ролью <**sysadm_r**>. В этом случае <**sysadm_r**> — это основной домен пользователя.

SELinux пользователь <**staff_u**> также сопоставлен роли <**sysadm_r**>. Основным пользовательским доменом пользователя SELinux <**staff_u**> является (роль) <**staff_r**>. Контексты по умолчанию, обозначенные в **/etc/selinux/targeted/contexts/users/staff_u**, определяют, с какими пользовательскими доменами пользователи будут подключаться по умолчанию и с какими пользовательскими доменами пользователи могут войти, указав домен пользователя при входе.

По умолчанию SELinux пользователь <**staff_u**> входит в систему в домен пользователя <**staff_t**>. Роль <**sysadm_r**>, предназначенная для использования в качестве основного домена пользователя, может быть использована при входе, например, следующим образом:

```
ssh joe/sysadm_r@localhost.localdomain.tld
```

Также роль <**sysadm_r**> может быть использована при переходе домена выполнением команд «**sudo**» и «**su**» вместе с «**newrole**», как это предусмотрено для дополнительных доменов пользователей.

Пользовательский домен <**sysadm_t**> является окружением по умолчанию для SELinux-пользователя <**sysadm_u**> и предназначен для использования в качестве дополнительного окружения для SELinux-пользователя <**staff_u**>, хотя даже SElinux-пользователь <**staff_u**> может настроить подключаемый модуль аутентификации (*Pluggable Authentication Module*) <**pam_selinux**> для использования <**sysadm_t**> в качестве его основного домена пользователя.

Роль <user_r> — пользователь системы

Пользовательский домен, используемый только в качестве основного. Описание пользователя SELinux <**user_u**> приведено ранее.

Какие-то домены пользователей могут использоваться пользователями для входа в систему, потому что эти домены, например, имеют полномочия по доступу к домашней директории пользователя. Такие домены в предыдущей части назывались основными (*primary*) пользовательскими доменами. Другие домены созданы в качестве дополнительных. Пользователи, используя команды «**sudo**» или «**su**» вместе с «**newrole**», могут осуществить доменный переход (*Domain Transition*) к этим дополнительным доменам.

Дополнительные домены не могут использоваться для входа в систему. Далее будет продемонстрировано как создаётся такой дополнительный пользовательский домен. Целью является реализовать привилегированную роль SELinux, которой предоставлены полномочия по управлению DNS службой Bind.

Начнём с создания нового дополнительного домена пользователя с названием «**bindadm**», основанного на предустановленном домене SELinux <**webadm_t**>. Новый домен пользователя основан на двух файлах с исходным текстом политики SELinux (SELinux Source Policy):

- webadm.te;
- webadm.if.

Файлы исходных текстов политики SELinux с расширением "**.te**" называются Type Enforcement файлы. Файлы с расширением "**.if**" называются интерфейсными (Interface files). Файлы *Type Enforcement* содержат описания (*Declarations*) и политику (*Policy*), персональные или локальные для данного домена (*Domain*). Интерфейсные файлы содержат описания и политики, общие для этого домена и других доменов, желающими взаимодействовать с данным доменом.

```
mkdir ~/bindadm; cd ~/bindadm
echo "policy_module(bindadm, 0.0.1)" >> bindadm.te
echo "role bindadm_r" >> bindadm.te
echo "userdom_base_user_template(bindadm)" >> bindadm.te
echo "allow bindadm_t self:capability { dac_override dac_read_search kill sys_ptrace sys_nice" >> bindadm.te
echo "files_dontaudit_search_all_dirs(bindadm_t)" >> bindadm.te
echo "files_manage_generic_locks(bindadm_t)" >> bindadm.te
echo "files_list_var(bindadm_t)" >> bindadm.te
echo "selinux_get_enforce_mode(bindadm_t)" >> bindadm.te
echo "seutil_domtrans_setfiles(bindadm_t)" >> bindadm.te
echo "logging_send_syslog_msg(bindadm_t)" >> bindadm.te
echo "userdom_dontaudit_search_user_home_dirs(bindadm_t)" >> bindadm.te
```

Это основное содержимое для привилегированного дополнительного домена пользователя. Исключена политика, специфичная для управления службой Apache.

Теперь добавим политику, специфичную для управления службой Bind. Можно позаимствовать эту политику из исходных текстов политики для Bind. Как уже отмечалось, общая политика располагается в интерфейсных файлах. Это значит, что если мы хотим включить общую политику, относящуюся к Bind, можно посмотреть в соответствующем файле политики **bind.if**. Для включения этой политики в наш Type Enforcement файл требуется всего лишь добавить вызов этого интерфейса:

```
echo "bind_admin(bindadm_t, bindadm_r)" >> bindadm.te
```

На этом Type Enforcement файл bindadm заканчивается. Далее необходимо обеспечить другим доменам возможность взаимодействия с нашим доменом <**bindadm_t**>. Реализуем эту часть политики, взяв за основу файл **webadm.if**.

```
echo "## Bind administrator role" > bindadm.if
echo "########################################" >> bindadm.if
echo "##" >> bindadm.if
echo "## Change to the bind administrator role." >> bindadm.if
echo "##" >> bindadm.if
echo '##' >> bindadm.if
echo "##" >> bindadm.if
echo "## Role allowed access." >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "#" >> bindadm.if
echo "interface(\`bindadm_role_change',\`" >> bindadm.if
echo " gen_require(\`" >> bindadm.if
echo " role bindadm_r;" >> bindadm.if
echo " ')" >> bindadm.if
echo " allow  $1 bindadm_r;" >> bindadm.if
echo "')" >> bindadm.if
```

Позже общая политика администратора **Bind** (Bind Administrator Shared policy) будет использоваться в нашем основном специально созданном пользовательском домене SELinux.

Следующим шагом будет создание специализированного пользовательского домена SELinux для обслуживания Bind, разрешающего данному домену осуществлять переход к роли <**bindadm_r**> вызовом интерфейса <**bindadm_role_change**>. Создаваемый домен SELinux будет основан на пользовательском домене <**staff_t**>, описание политики смотрим в файле **staff.te**.

```
echo "policy_module(bindguy, 0.0.1)" > bindguy.te
echo "role bindguy_r;" >> bindguy.te
echo "userdom_unpriv_user_template(bindguy)" >> bindguy.te
echo "sudo_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "ssh_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "kernel_read_ring_buffer(bindguy_t)" >> bindguy.te
echo "kernel_getattr_core_if(bindguy_t)" >> bindguy.te
echo "kernel_getattr_message_if(bindguy_t)" >> bindguy.te
echo "kernel_read_software_raid_state(bindguy_t)" >> bindguy.te
echo "auth_domtrans_pam_console(bindguy_t)" >> bindguy.te
echo "libs_manage_shared_libs(bindguy_t)" >> bindguy.te
echo "seutil_run_newrole(bindguy_t, bindguy_r)" >> bindguy.te
echo "netutils_run_ping(bindguy_t, bindguy_r)" >> bindguy.te
echo "domain_read_all_domains_state(bindguy_t)" >> bindguy.te
echo "domain_getattr_all_domains(bindguy_t)" >> bindguy.te
echo "domain_obj_id_change_exemption(bindguy_t)" >> bindguy.te
echo "files_read_kernel_modules(bindguy_t)" >> bindguy.te
echo "kernel_read_fs_sysctls(bindguy_t)" >> bindguy.te
echo "modutils_read_module_config(bindguy_t)" >> bindguy.te
echo "modutils_read_module_deps(bindguy_t)" >> bindguy.te
echo "miscfiles_read_hwdata(bindguy_t)" >> bindguy.te
echo "term_use_unallocated_ttys(bindguy_t)" >> bindguy.te
```

Чтобы разрешить домену <**bindguy_t**> осуществлять переход в ограниченное окружение SELinux <**bindadm_t**>, добавим вызов интерфейса <**bindadm_role_change**>, определённого в нашем интерфейсном файле **bindadm.if**:

```
echo "bindadm_role_change(bindguy_r)" >> bindguy.te
```

Можно также автоматически создать сопоставление пользователя SELinux с именем <**bindguy_u**> ролям <**bindguy_r**>, <**bindadm_r**> и <**system_r**>. Роль <**system_r**> включается, чтобы <**bindadm_t**> мог остановить, запустить и перезапустить системную службу **bind**.

```
echo "gen_user(bindguy_u, user, bindguy_r system_r bindadm_r, s0,  s0 - mls_systemhigh,
mcs_allcats)" >> bindguy.te
```

Чтобы программы входа знали, что bindguy допустимый пользователь, добавим контексты по умолчанию для этого пользователя, взяв за основу контексты по умолчанию пользователя <**staff_u**>:

```
cp /etc/selinux/targeted/contexts/users/staff_u
/etc/selinux/targeted/contexts/users/bindguy_u
sed -i 's/staff/bindguy/g'
/etc/selinux/targeted/contexts/users/bindguy_u
```

Теперь можно собрать и установить обе политики bindguy и bindadm:

```
make -f /usr/share/selinux/devel/Makefile
semodule -i bindguy.pp bindadm.pp
```

Далее командой «**useradd**», опцией «**-Z**» и параметром <**bindguy_u**> можно создать нового пользователя Linux:

```
useradd -Z bindguy_u bindguy
```

Для того чтобы разрешить пользователю *bindguy* использовать команду «**sudo**» для автоматического перехода к пользователю root и SELinux-домену <**bindadm_t**>, добавим в **/etc/sudoers**:

```
echo "bindguy ALL=(ALL) ROLE=bindadm_r TYPE=bindadm_t ALL" » /etc/sudoers
```

При входе пользователя bindguy в систему он оказывается в пользовательском домене <**bindguy_t**>, основанном на домене <**staff_t**>. Домен <**bindguy_t**> может осуществлять переход в домен <**bindadm_t**>, используемый с правами root и позволяющий управлять службой Bind.

Например, выполнив следующую команду, пользователь bindguy сможет перезапустить службу bind:

```
systemctl restart named
```

Также пользователю *bindguy* разрешается редактировать различные конфигурационные файлы и файлы информационного наполнения Bind. При этом, например, пользователь *bindguy* не имеет прав изменить пароль пользователя root.

Подведём итог. Процессы и файлы маркируются метками - контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально). Когда SELinux включён, вся эта информация используется для принятия решения о предоставлении доступа.

В контексте SELinux используется следующий синтаксис SELinux:

```
<user>:<role>:<type>:<level>:<пользователь_SELinux>
```

<**Пользователь_SELinux**> - это сущность, определённая в политике, которая отвечает за определённый набор ролей и за определённый набор MLS-уровней. Каждый пользователь ОС сопоставлен пользователю SELinux посредством политики SELinux. Это позволяет пользователям наследовать ограничения, установленные на пользователей SELinux. Сопоставленные сущности пользователей SELinux используются в контексте SELinux для процессов в сессии, в порядке определения, для каких ролей и уровней они применимы.

Роль - это часть модели безопасности Ролевого управления доступом **Role-Based Access Control** (RBAC). Роль - это атрибут RBAC. Пользователи SELinux авторитетны для ролей, а роль авторитетна для доменов. Каждая конкретная роль определяет, какие домены могут быть доступны для пользователей с этой ролью. Роль служит промежуточным звеном между доменами и пользователями SELinux. Роль, которой обладает пользователь, определяет, в какие домены может попасть пользователь - фактически, этот механизм управляет доступностью объектов. Таким образом, уменьшается риск, связанный с уязвимостью повышения привилегий в системе. По умолчанию пользователям назначена неопределённая роль, не накладывающая ограничений на пользователя. Но есть и предопределённые роли пользователя и администратора системы, которые могут быть назначены администратором для повышения безопасности системы.

Тип - это атрибут *Type Enforcement*. Тип определяет домен для процессов и тип для файлов. Правила политики SELinux определяют, как типы взаимодействуют друг с другом, является ли тип доменом, получающим доступ к типу, или доменом, получающим доступ к другому домену. Доступ разрешается, только если существует определённое правило политики SELinux, позволяющее данное действие.

Контекст безопасности записывается в атрибуты файла (в файловой системе) и создаётся при установке SELinux (операция **labeling**). Уже присвоенный контекст безопасности может быть впоследствии изменён - операцией «**transition**».

Командные оболочки (интерпретаторы)

Для управления ОС используется командные интерпретаторы (shell). Зайдя в систему, пользователь увидит приглашение - строку, содержащую символ «$» (далее этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора - передавать команды пользователя операционной системе. При помощи командных интерпретаторов можно писать небольшие программы - сценарии (скрипты). Оболочкой по умолчанию в РЕД ОС является «**Bash**» (Bourne Again Shell) Чтобы проверить, какая оболочка используется, необходимо выполнить команду:

```
echo $SHELL
```

Вы можете подробнее ознакомиться с возможностями работы **bash**, просмотрев наши обучающие видео:

- на **RuTube**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **Яндекс.Дзен**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **VK Видео**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.

На наших каналах вы также сможете найти много другой полезной информации.

Командная оболочка Bash

В bash имеется несколько приемов для работы со строкой команд. Например, используя клавиатуру, можно:

- **Ctrl + A** - перейти на начало строки;
- **Ctrl + U** - удалить текущую строку;
- **Ctrl + C** - остановить текущую задачу.

Можно использовать «;» для того, чтобы ввести несколько команд одной строкой. Клавиши «вверх» и «вниз», позволяют вам перемещаться по истории команд.

Для того чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, необходимо набрать:

Ctrl + R

Команды, присутствующие в истории, отображаются в списке пронумерованными. Для того, чтобы запустить конкретную команду, наберите:

```
! <номер_команды>
```

если ввести:

```
!!
```

запустится последняя из набранных команд. Иногда имена программ и команд слишком длинны. Bash сам может завершать имена. Нажав клавишу [TAB], можно завершить имя команды, программы или каталога. Например, предположим, что необходимо использовать программу декомпрессии bunzip2. Для этого нужно набрать:

```
bu
```

затем нажать [TAB]. Если ничего не происходит, то, вероятно, существует несколько возможных вариантов завершения команды.

Нажав клавишу [TAB] еще раз, пользователь получит список имен, начинающихся с «bu». Например, может быть:

```
bu buildhash builtin bunzip2
```

Если далее добавить:

n

(bunzip - это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу [TAB], оболочка дополнит имя и остается лишь нажать «Enter», чтобы запустить команду. Программу, вызываемую из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH.

По умолчанию, в этот перечень каталогов не входит текущий каталог, обозначаемый «./» (точка слэш), поэтому для запуска программы **prog** из текущего каталога, надо дать команду:

```
./prog
```

Базовые команды оболочки Bash

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации используйте команду **man.**Пример:

```
man ls
```

Команда su

Позволяет получить права администратора. Когда пользователь набирает su, оболочка запрашивает пароль суперпользователя (root). Необходимо ввести пароль и нажать **Enter**. Чтобы вернуться к правам основного пользователя, необходимо набрать **exit**.

Команда cd

Позволяет сменить каталог. Она работает как с абсолютными, так и с относительными путями. Предположим, что, находясь в своем домашнем каталоге, пользователь хочет перейти в его подкаталог **docs/**. Для этого нужно ввести относительный путь:

```
cd docs/
```

Чтобы перейти в каталог **/usr/bin** , нужно набрать (абсолютный путь):

```
cd /usr/bin/
```

Некоторые варианты команды:

```
cd ..
```

позволяет сделать текущим родительский каталог,

```
cd -
```

позволяет вернуться в предыдущий каталог. Команда cd без параметров переводит в домашний каталог.

Команда ls

ls (list) выдает список файлов в текущем каталоге. Синтаксис:

```
ls
```

Две основные опции:

- -a - просмотр всех файлов, включая скрытые,
- -l - отображение более подробной информации.

Команда rm

Эта команда используется для удаления файлов. Синтаксис:

```
rm <имя_файла>
```

У данной программы существует ряд параметров. Самые часто используемые:

- -i - запрос на удаление файла,
- -r - рекурсивное удаление (т.е. удаление, включая подкаталоги и скрытые файлы).

Команды mkdir и rmdir

Команда **mkdir** позволяет создать каталог, тогда как **rmdir** удаляет каталог, при условии, что он пуст. Синтаксис:

```
mkdir <имя_каталога>
```

```
rmdir <имя_каталога>
```

Команда **rmdir** часто заменяется командой **rm-rf** , которая позволяет удалять каталоги, даже если они не пусты.

Команда less

less позволяет постранично просматривать текст.

Синтаксис:

```
less <имя_файла>
```

Для выхода нужно нажать q.

Команда grep

Данная команда имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep <шаблон_поиска> <файл>
```

Команда ps

Отображает список текущих процессов. Колонка команд указывает имя процесса, колонка PID (идентификатор процесса) - номер процесса (этот номер используется для операций с процессом, например чтобы «убить» его командой **kill**).

Синтаксис:

```
ps <аргументы>
```

Аргумент -u предоставляет больше информации, а -x позволяет просмотреть те процессы, которые не принадлежат пользователю (такие как те, что были запущены во время процесса загрузки).

Команда kill

Если программа перестала отвечать или зависла, необходимо использовать данную команду, чтобы её завершить.

Синтаксис:

```
kill <PID_номер>
```

Иногда необходимо будет использовать **kill -9** (когда обычная команда **kill** не дает желательного эффекта). Номер PID выясняется при помощи команды **ps**.

Горячие комбинации клавиш в Bash

Для удобства запоминания сочетания клавиш сгруппированы по действию. Обратите внимание, что **в комбинациях следует использовать левую клавишу Alt**, т.к. правая Alt Gr используется как клавиша Compose (специальная клавиша, позволяющая вводить символы с помощью определённых комбинаций клавиш).

Перемещение по тексту

Сочетание	Действие
Ctrl+a, Home	Переместить курсор в начало командной строки
Ctrl+e, End	Переместить курсор в конец командной строки
Ctrl+b, ←	Переход на один символ назад от курсора
Ctrl+f, →	Переход на один символ вперёд от курсора
Alt+b, Esc+b	Переместить курсор назад на одно слово
Alt+f, Esc+f	Переместить курсор вперёд на одно слово
Ctrl+xx	Переход от курсора в начало строки и обратно

Редактирование строки

Сочетание	Действие
Alt+?, Tab+Tab	Автодополнение команды или имени файла
Ctrl+u	Удалить все символы от курсора до начала командной строки
Ctrl+k	Удалить все символы от курсора до конца командной строки
Ctrl+w	Удалить символы от курсора до пробела слева
Alt+Backspace	Удалить символы от курсора до начала слова
Alt+d, Esc+d	Удалить символы от курсора до конца слова
Ctrl+y	Вставить символ, слово или текст, которые были удалены при помощи сочетаний клавиш, приведенных выше
Alt+y	Просмотреть буфер удалённых слов и вставить интересующее. Работает после нажатия Ctrl+y
Ctrl+h	Удалить перед курсором один символ
Ctrl+d	Удалить под курсором один символ
Alt+	Удалить любое количество пробелов вокруг курсора
Ctrl+_	Откатить редактирование
Alt+r, Esc+r	Отменить все изменения содержимого строки
Alt+c	Заменяет под курсором букву на заглавную и переводит курсор в конец слова
Alt+u	Переводит все буквы от курсора и до конца слова в заглавные
Alt+l	Переводит все буквы от курсора и до конца слова в нижний регистр
Alt+t	Замена текущего слова под курсором на предыдущее слово
Ctrl+t	Замена символа перед курсором на предыдущий символ

История команд

Сочетание	Действие
Ctrl+r	Искать команду по истории

Ctrl+g	Выйти из режима поиска в истории
Ctrl+p, ↑	Предыдущая команда в истории
Ctrl+n, ↓	Следующая команда в истории
Alt+<	Переход к первой команде в буфере истории
Alt+., Esc+.	Вставить последний аргумент предыдущей команды
Ctrl+o	Выполняет введённую команду и оставляет её же в командной строке

Выполнение и вывод на экран

Сочетание	Действие
Ctrl+l	Очистка экрана
Ctrl+s	Остановить вывод на экран
Ctrl+q	Возобновить вывод на экран, если он был приостановлен указанной выше командой
Ctrl+c	Прервать выполнение текущей команды
Ctrl+z	Приостановить выполнение текущей команды (для возобновления выполните fg)
Ctrl+d	Выйти из командной оболочки Bash

Информационный вывод

Сочетание	Действие
***+Alt+?, *+Tab+Tab**	Показать каталоги, кроме скрытых
$+Alt+?, $+Tab+Tab	Показать все системные переменные

Специальные клавиши

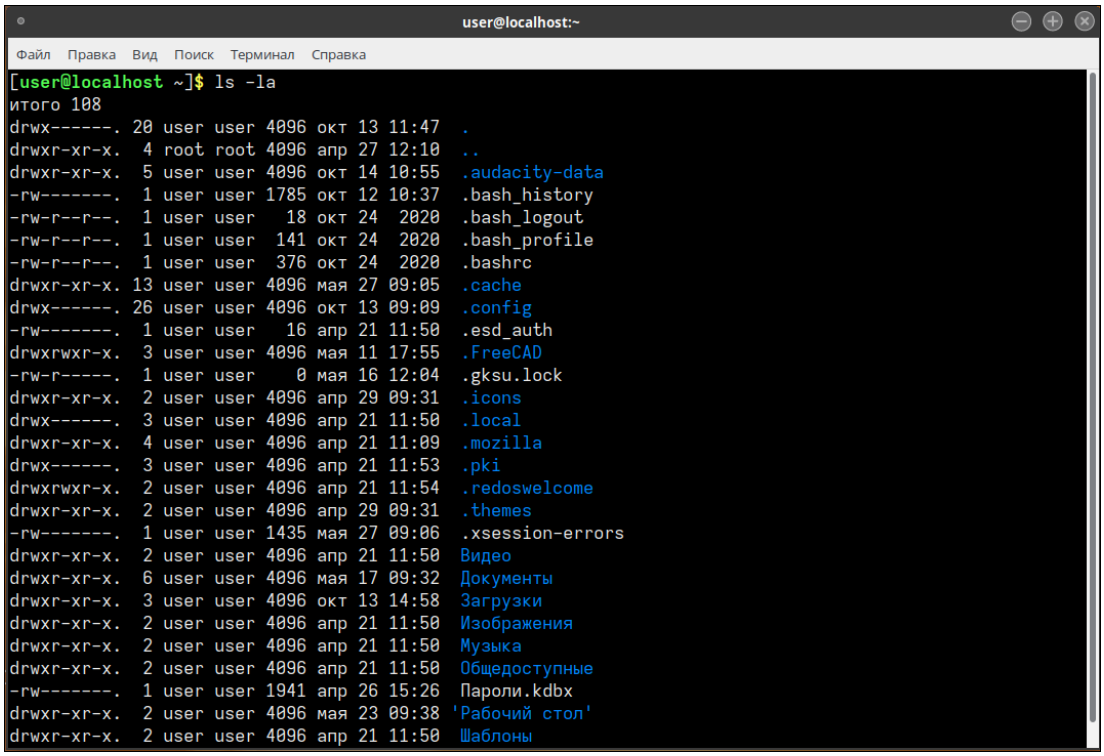
Сочетание	Действие
Ctrl+i	Tab
Ctrl+m	Enter
Ctrl+[	Esc

Основные утилиты в консоли РЕД ОС

ls

Утилита для просмотра содержимого каталогов. По умолчанию показывает содержимое текущего каталога. Если в параметрах указан путь к каталогу, она перечислит содержимое конечного каталога. Полезные опции:

- **-l** (list) - форматирует вывод в виде списка с более подробной информацией;
- **-a** (--all) - включает показ скрытых файлов;
- **--help** - вывести справку по использованию утилиты.

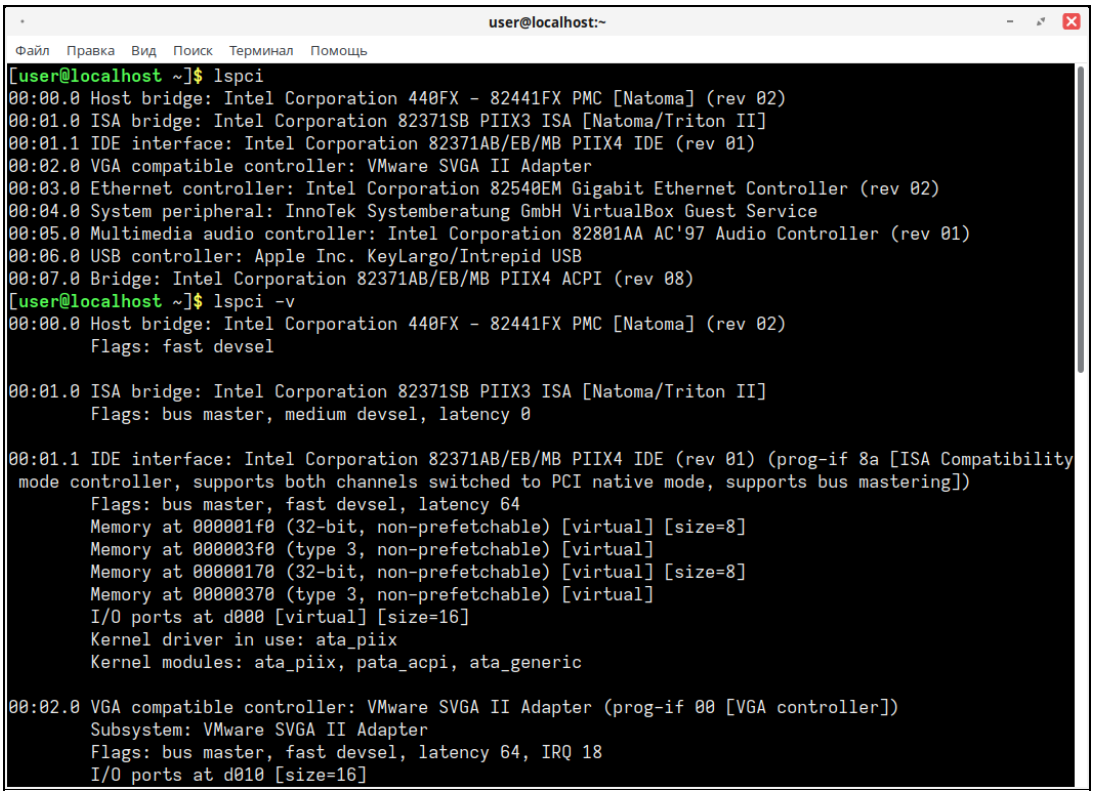


lspci

Команда **lspci** позволяет задействовать одноименную утилиту, предназначенную для вывода информации о PCI-шинах и подключенных к ним устройствах. Она поддерживает все разновидности PCI-шин: классическую шину **PCI** (Peripheral Component Interconnect), ее серверный вариант **PCI-X** и ее современный вариант **PCIe** (PCI-Express). Обычно к данной шине подключаются такие устройства, как графические, звуковые и сетевые карты, Wi-Fi и Bluetooth-адаптеры, SSD-накопители, а также множество других устройств.

Наиболее полезные опции:

- **-m** и **-mm** — для вывода установленных производителем идентификаторов устройств;
- **-t** — для вывода информации в древовидном формате;
- **-v** — для вывода подробной информации об устройствах;
- **-n** — для вывода идентификаторов устройств;
- **-s** и **-d** — для вывода информации об устройствах в заданных слотах и с заданными идентификаторами соответственно.



lsusb

Команда lsusb позволяет задействовать одноименную утилиту, предназначенную для вывода информации о USB-шинах и подключенных к ним устройствах. Каждое из устройств имеет пару 16-битных идентификаторов: идентификатор производителя (**Vendor ID**) и идентификатор устройства (**Device ID**), которые следует использовать для идентификации устройств и поиска драйверов в случае их отсутствия в ядре ОС, а также несколько дополнительных идентификаторов, устанавливаемых производителем.

```
[user@localhost ~]$ lsusb
Bus 002 Device 003: ID 062a:4101 MosArt Semiconductor Corp. Wireless Keyboard/Mouse
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
[user@localhost ~]$
```

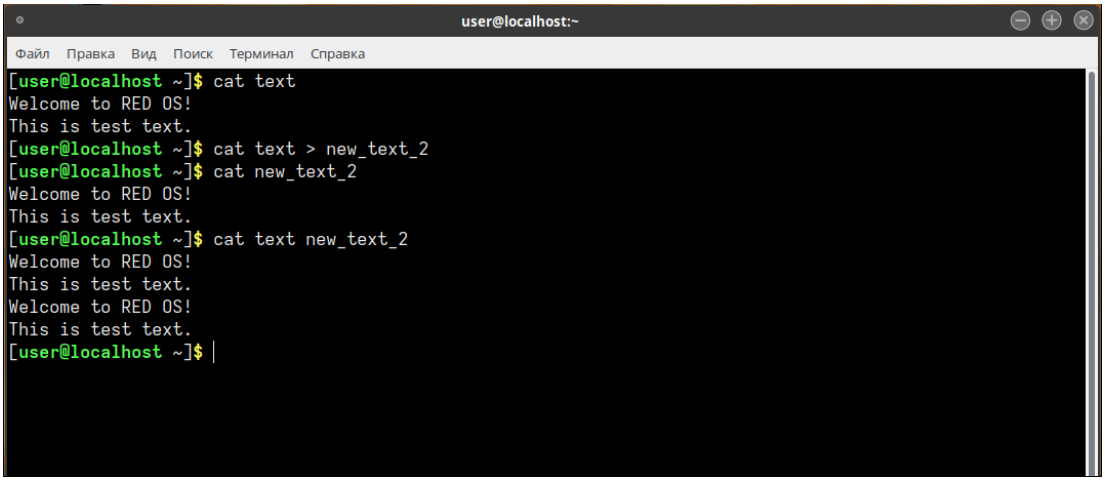
lsmod

Команда **lsmod** показывает, какие модули ядра загружены в системе в данный момент.

```
[user@localhost ~]$ lsmod
Module                  Size  Used by
snd_hrtimer            16384  1
nf_conntrack_netlink    53248  0
xt_addrtype            16384  2
br_netfilter           32768  0
xt_conntrack           16384  3
ipt_REJECT             16384  4
nf_reject_ipv4         16384  1 ipt_REJECT
nft_compat             20480  18
nft_chain_nat          16384  4
nf_tables             294912  337 nft_compat,nft_chain_nat
nfnetlink              20480  4 nft_compat,nf_conntrack_netlink,nf_tables
xt_CHECKSUM            16384  3
iptable_mangle         16384  1
xt_MASQUERADE          20480  8
xt_comment             16384  8
iptable_nat            16384  1
nf_nat                 57344  3 nft_chain_nat,iptable_nat,xt_MASQUERADE
nf_conntrack          167936  4 xt_conntrack,nf_nat,nf_conntrack_netlink,xt_MASQUERADE
nf_defrag_ipv6         24576  1 nf_conntrack
nf_defrag_ipv4         16384  1 nf_conntrack
bridge                360448  1 br_netfilter
stp                    16384  1 bridge
```

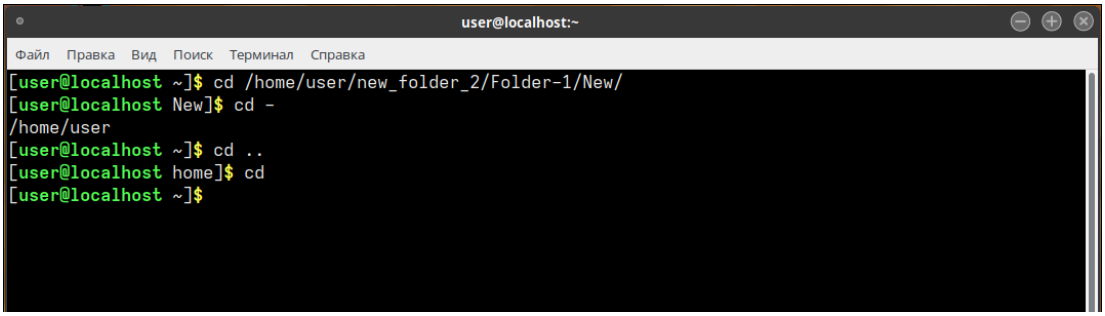
cat

Печатает содержимое файла, переданного в параметре, в стандартный вывод. Если передать несколько файлов, команда объединит их. Также можно перенаправить вывод в ещё один файл с помощью символа « **>** ».



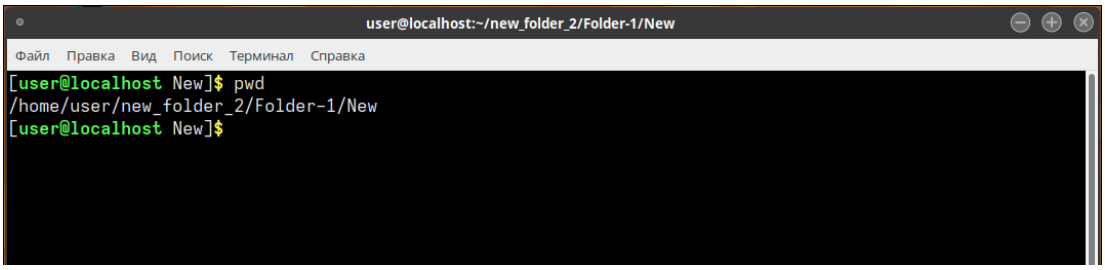
cd

Позволяет перейти из текущего каталога в указанный. Если запустить без параметров - возвращает в домашний каталог. Вызов с двумя точками (**cd ..**) - возвращает на уровень выше относительно текущего каталога. Вызов с тире (**cd -**) возвращает к предыдущему каталогу.



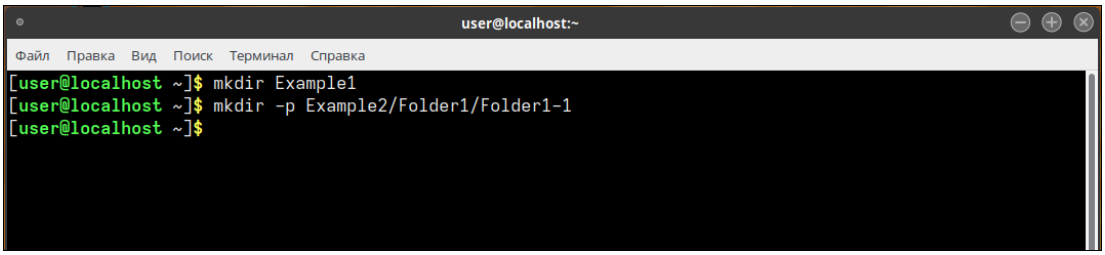
pwd

Выводит полный путь к текущему/рабочему каталогу.



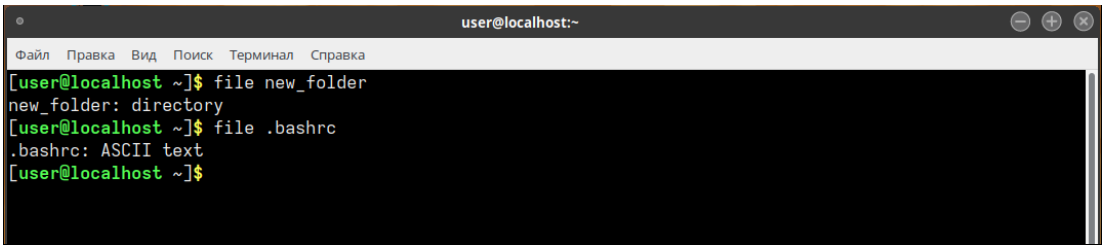
mkdir

Создание новых каталогов. Наиболее удобная опция **-p** (parents), позволяет создать всю структуру подкаталогов одной командой, даже если они ещё не существуют.



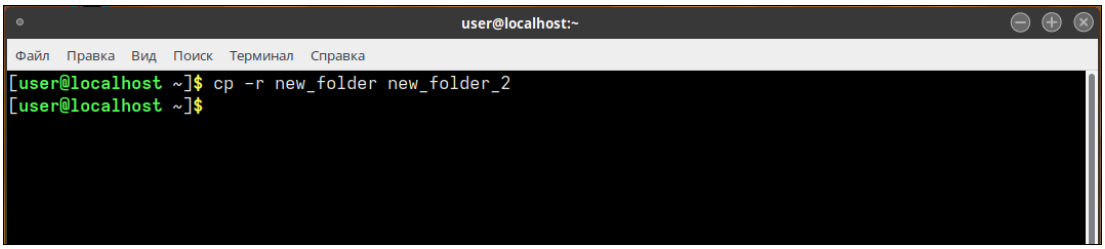
file

Показывает тип файла. В Linux файлы не обязаны всегда иметь расширения для того, чтобы с ними работать. Поэтому пользователю иногда трудно определить, какой именно перед ним файл. Данная утилита решает такую проблему.



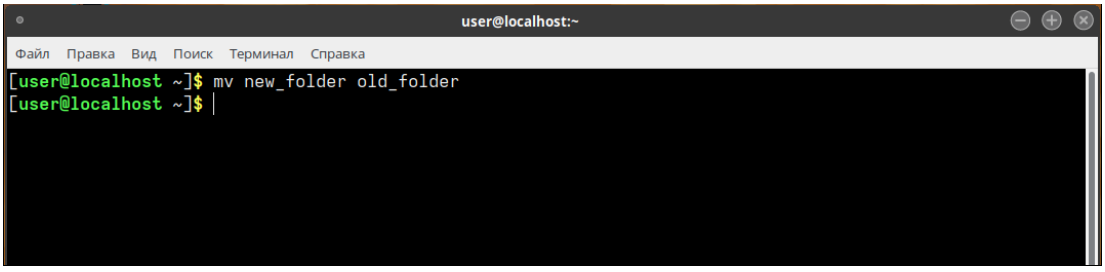
cp

Копирование файлов и каталогов. Утилита по умолчанию не копирует каталоги рекурсивно, поэтому необходимо добавить опцию **-r** (recursive) или **-a** (archive). Последняя включает режим сохранения атрибутов, владельца и временного штампа в дополнение к рекурсивному копированию.



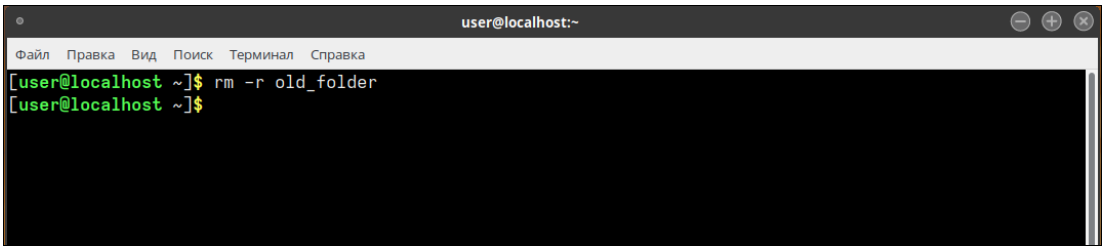
mv

Перемещение или переименование файлов и каталогов. В Linux это одна и та же операция. Переименование - это перемещение файла в ту же папку с другим именем.



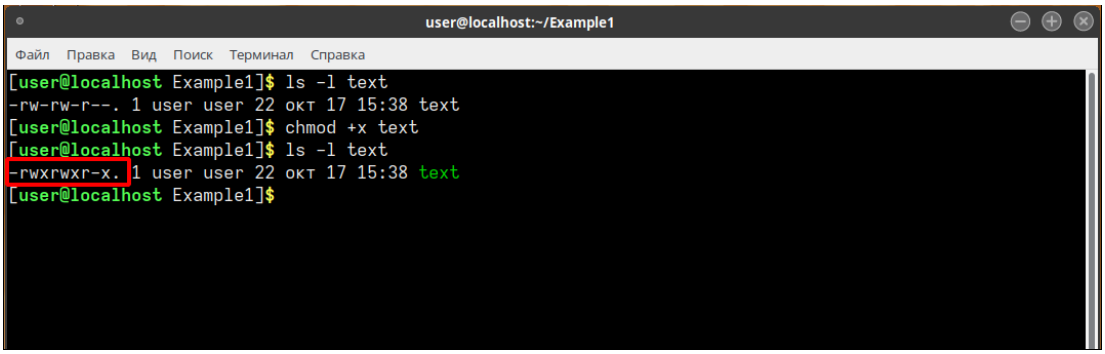
rm

Удаляет файлы и папки. Если нужно рекурсивное удаление, используйте опцию **-r**. **Rm** удаляет файлы не в корзину, из которой потом данные можно будет восстановить, а полностью их стирает. Действия оператора **rm** необратимы.



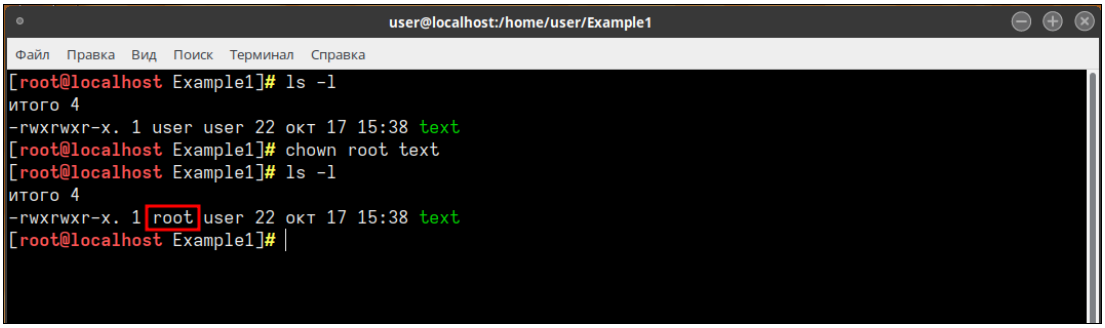
chmod

Изменяет права доступа к файлу - чтение, запись и выполнение. Каждый пользователь может изменять права для своих файлов.



chown

Изменяет владельца файла. Только суперпользователь может изменять владельцев. Для рекурсивного изменения используйте опцию **-R**.

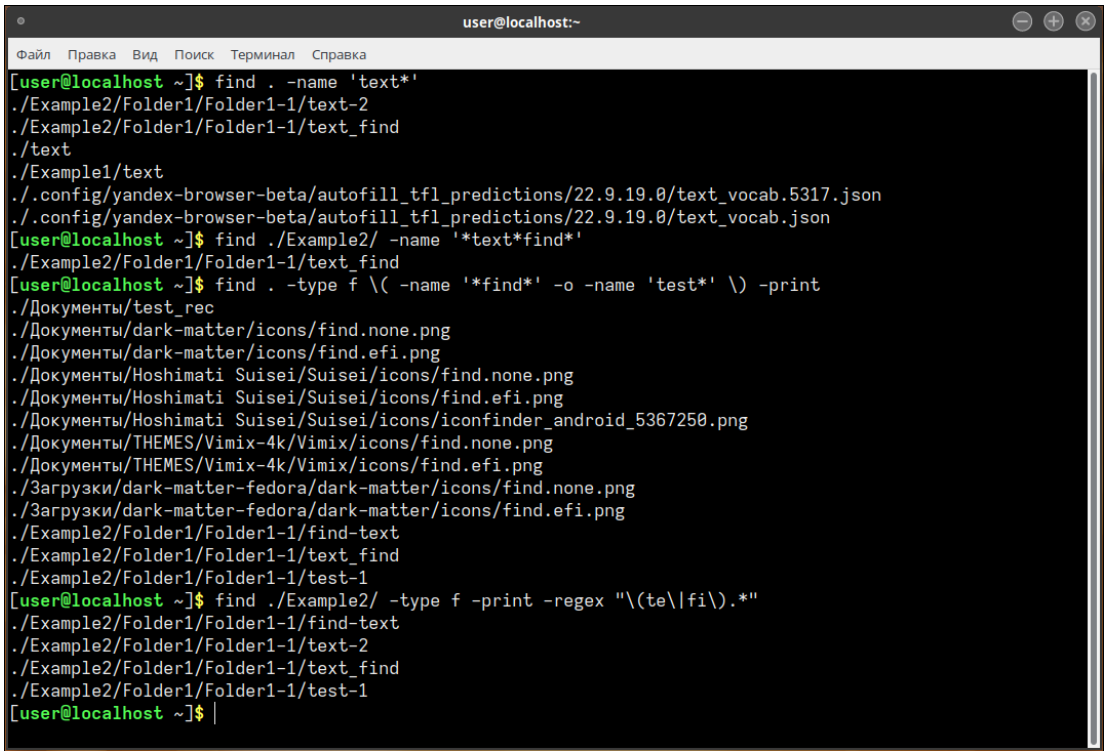


find

Очень гибкая и мощная команда Linux не только из-за своих способностей удобного поиска, но и благодаря возможности выполнять произвольные команды для найденных файлов. Поиск может осуществляться как в одном, так и в нескольких каталогах, имеется поддержка регулярных выражений для более точного поиска.

Основные опции:

- **-type** [f=файл, d=каталог (directory), l=ссылка (link), p=канал (pipe), s=сокет] - поиск по типу файла;
- **-name** '<имя_файла>' - поиск по имени файла, можно использовать как полное имя, так и его часть ('text' или 'te*');
- **-regex** "<регулярное_выражение>" - поиск файлов по регулярному выражению;
- **-print** - показать на экране найденные файлы.

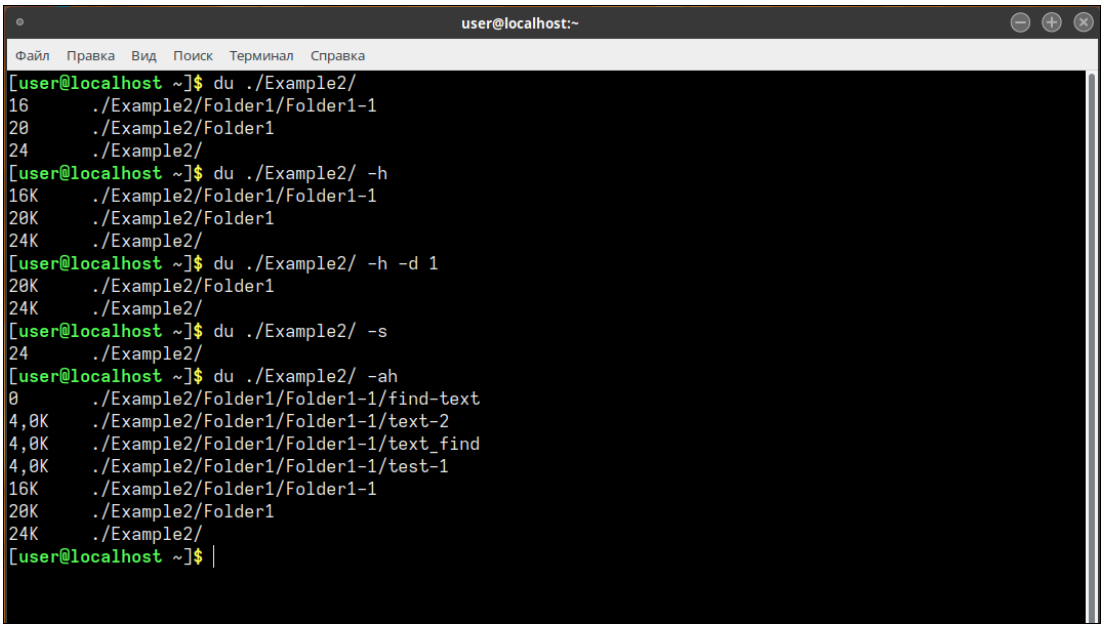


du

Показывает размер файла или каталога для оценки занимаемого файлового пространства.

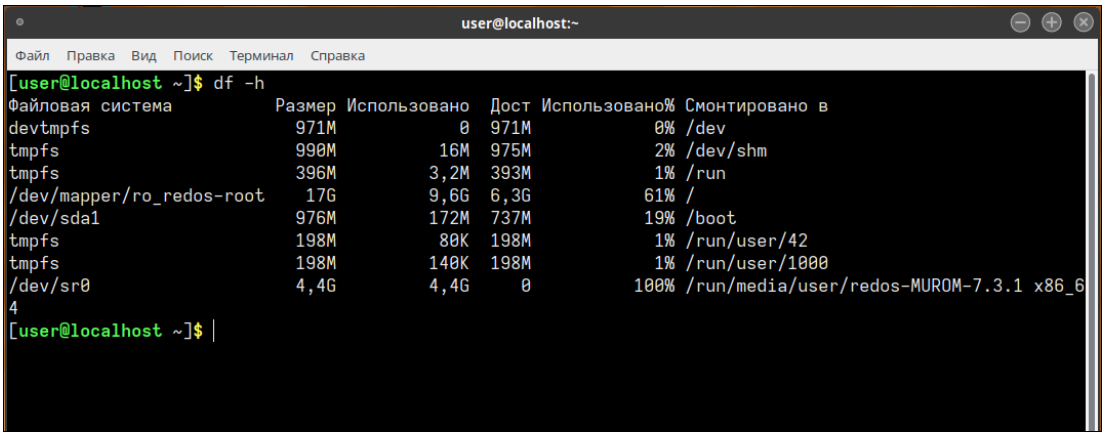
Полезные опции:

- **-a** (--all) - выводить размер для всех файлов, а не только для директорий, по умолчанию размер выводится только для папок;
- **-d** (--max-depth) - максимальная глубина вложенности директорий;
- **-h** (--human-readable) - преобразует размеры файлов в удобный формат;
- **-s** (--summarize) - выводит минимум данных.



df

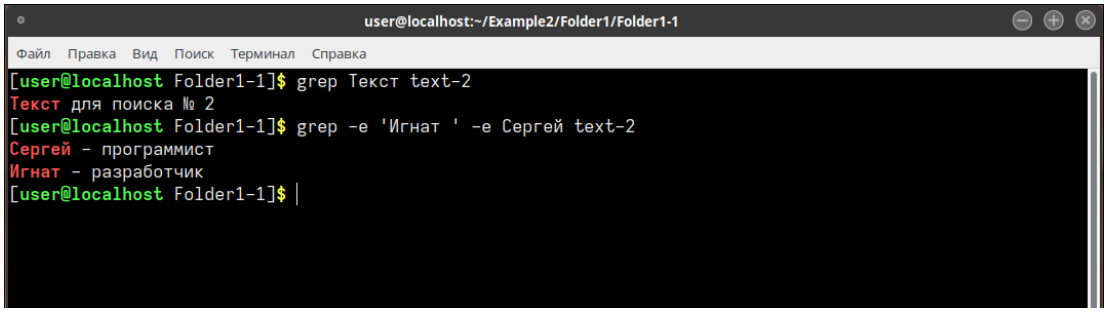
Используется для получения полной сводной информации о доступном и используемом дисковом пространстве файловой системы. По умолчанию вывод достаточно подробный: перечислены все файловые системы, их размер, количество использованного и свободного пространства. Для удобства можно использовать опцию **-h**, которая отобразит размеры удобными для чтения.



grep

Утилита **grep** ищет заданный шаблон или регулярное выражение из стандартного ввода или файла и печатает соответствующие заданным критериям строки. Утилита может вывести как полностью совпадающие, так и частично совпадающие строки и их контекст.

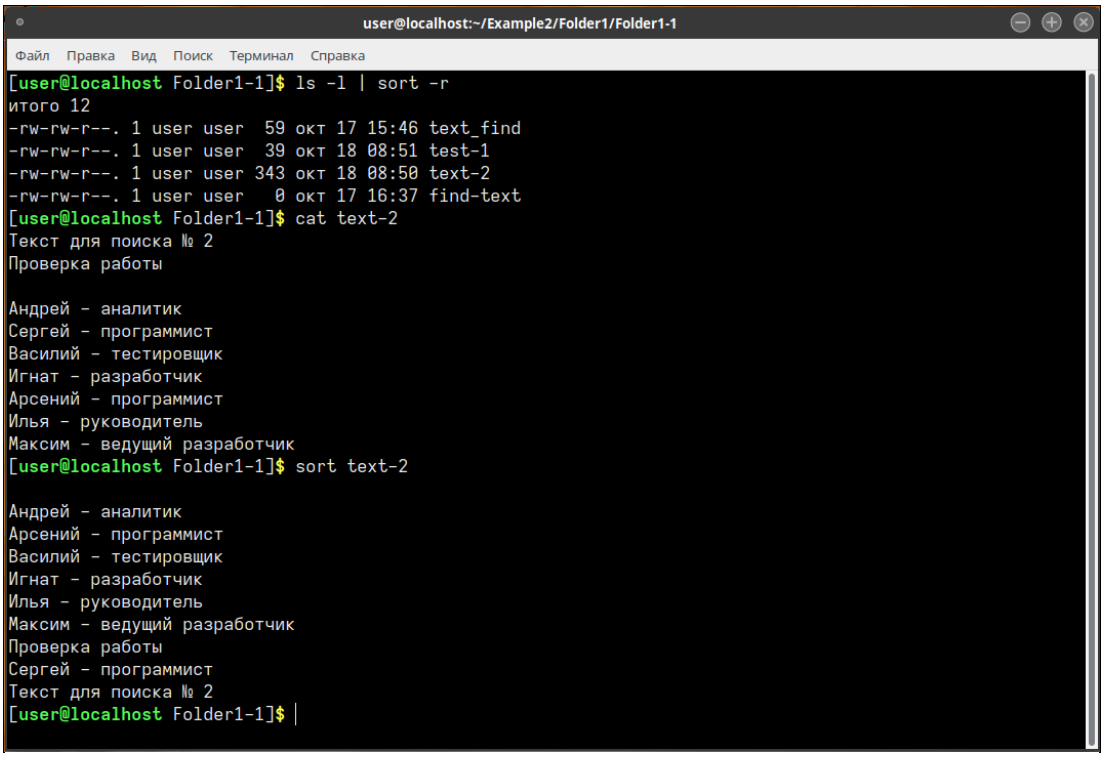
Команде **grep** также можно передавать и несколько параметров. Для этого перед каждым аргументом пишется ключ **-e**. Эту команду система понимает, как "или-или" и выводит все вхождения указанных слов. Кавычками выделяются только строки, содержащие пробел.

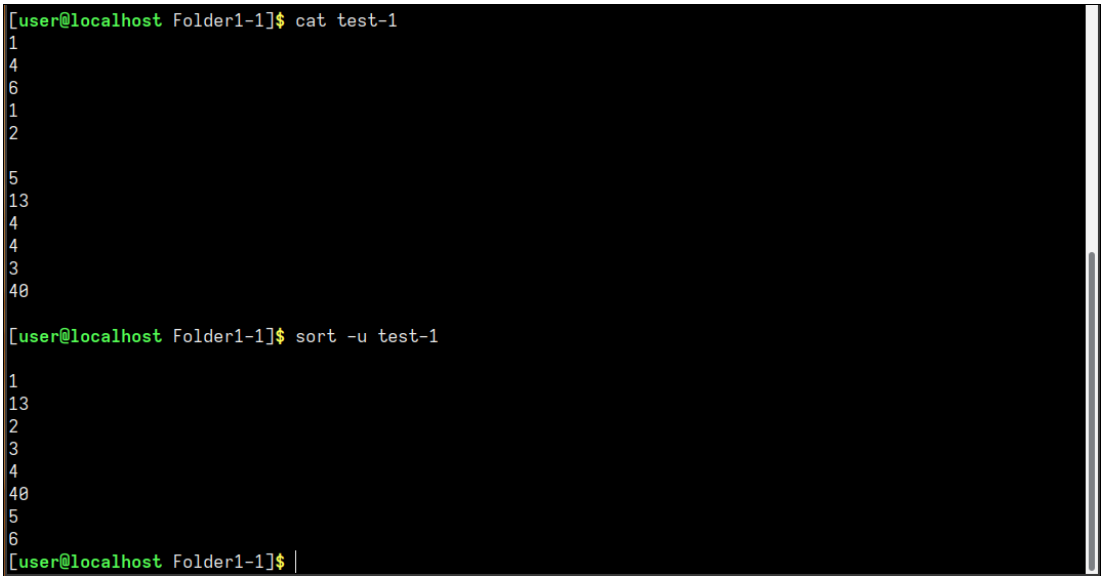


sort

Сортировка строк текста из одного или нескольких файлов по различным критериям, также может быть выполнена сортировка для вывода какой-либо команды. Наиболее полезные опции:

- **-b** - не учитывать пробелы;
- **-c** - проверить был ли отсортирован файл;
- **-n** (numeric) - сортирует по числовому значению;
- **-o** - вывести результат в файл;
- **-u** - игнорировать повторяющиеся строки
- **-r** (reverse) - сортирует в обратном порядке.



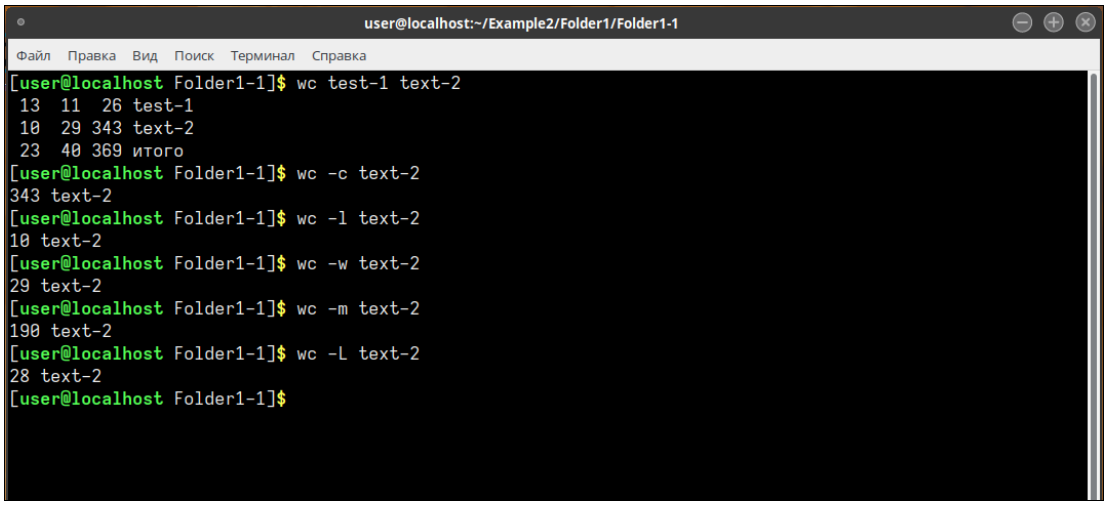


wc

Выводит число переводов строк, слов и байт для каждого указанного файла и итоговую строку, если было задано несколько файлов.

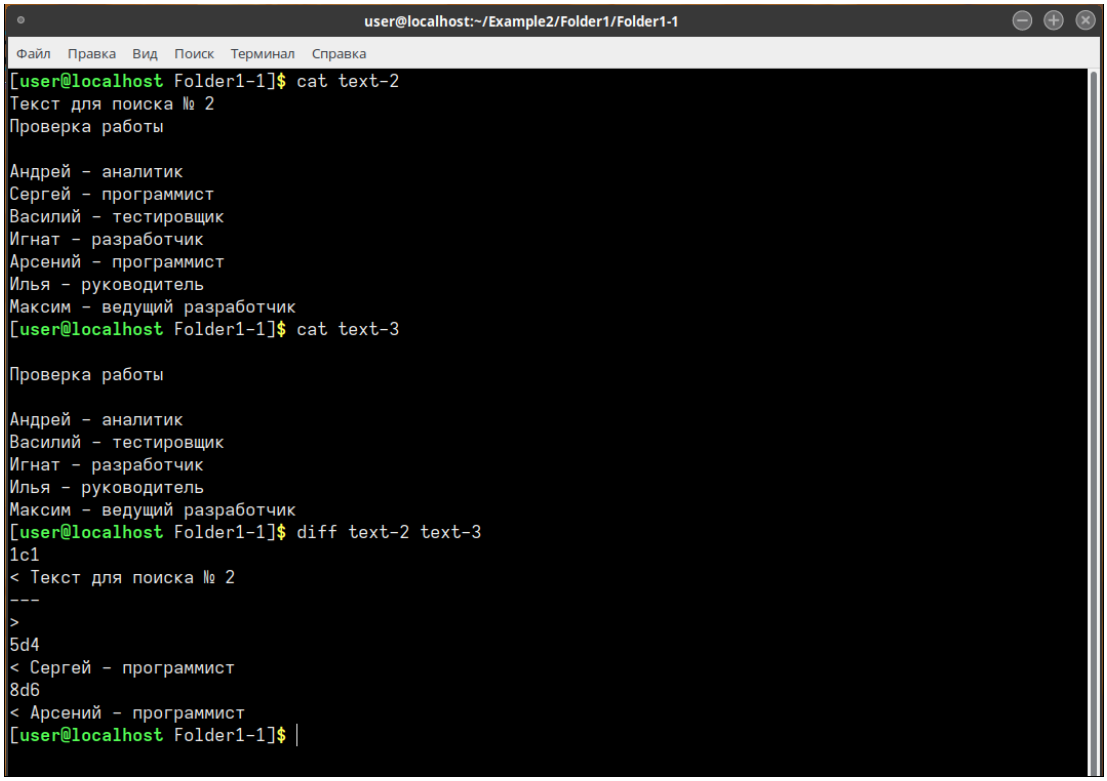
Основные опции:

- **-c**, **--bytes** – вывод размера файла в байтах;
- **-m**, **--chars** – вывод числа символов в файле;
- **-l**, **--lines** – вывод числа строк в файле;
- **-L**, **--max-line-length** – вывод максимальной длины строки в файле;
- **-w**, **--words** – вывод числа слов в файле.

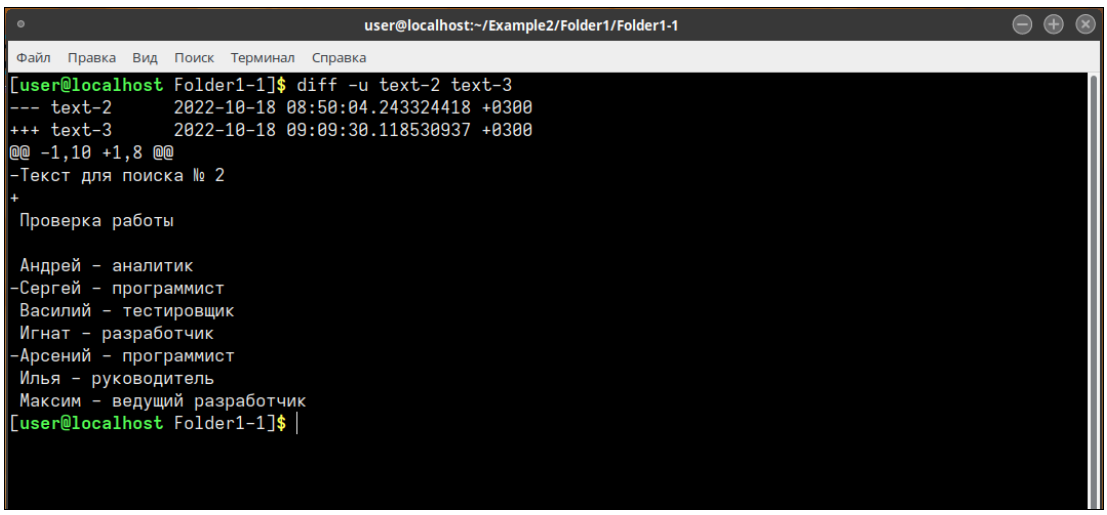


diff

Показывает различия между двумя файлами в построчном сравнении. Причём выводятся только строки, в которых обнаружены отличия. Измененные строки отмечаются символом «**c**», удаленные - «**d**», а новые - «**a**». Добавленные и удаленные строки обозначаются с помощью символов **>** и **<** соответственно.



Для вывода информации о различиях в унифицированном формате можно использовать опцию **-u**:



ps / pgrep

Предназначена для просмотра списка процессов. Чтобы завершить/приостановить какой-либо процесс, необходим его идентификатор. Один из способов получить его - утилита **ps**. Для отображения всех запущенных процессов можно использовать опцию **a**. Следует обратить внимание, что это только снимок состояния на момент вызова, информация не будет обновляться.

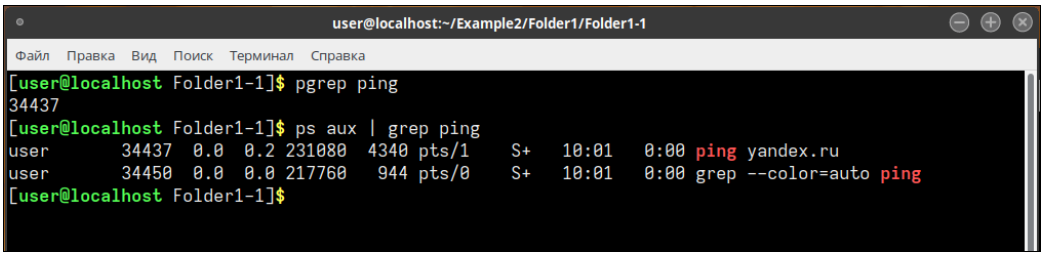
Для получения полной информации о процессах и определения идентификатора процесса (**PID**) выполните команду:

```
ps aux
```

Для конкретизации поиска определенного процесса рекомендуется использовать утилиту grep, например:

```
ps aux | grep ping
```

Утилита **pgrep** работает следующим образом: вы задаете имя процесса, а утилита показывает его идентификатор.



kill / xkill / pkill / killall

Данные команды служат для завершения процессов, однако они принимают различные параметры для идентификации процессов. **Kill** - нужен PID процесса, **xkill** - достаточно кликнуть по окну, чтобы закрыть его, **killall** и **pkill** - принимают имя процесса. Можно использовать любую из утилит, которая будет удобна в определенной ситуации.

Для определения идентификатора процесса (**PID**) воспользуйтесь утилитами ps или pgep, описанными выше.

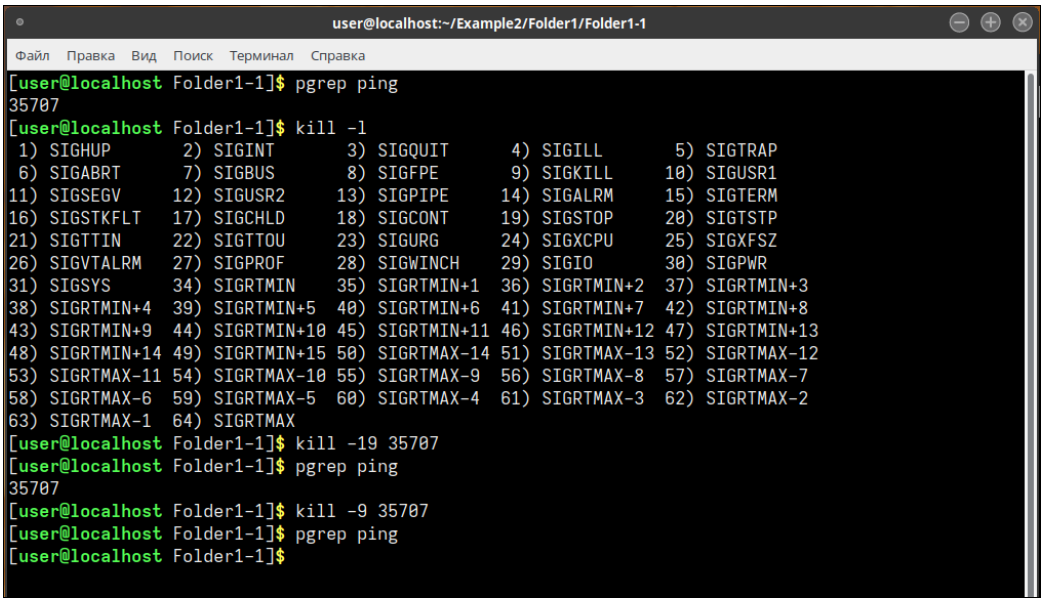
Для утилит kill и killall доступно несколько сигналов, которые также можно использовать для прерывания, завершения или приостановки процессов:

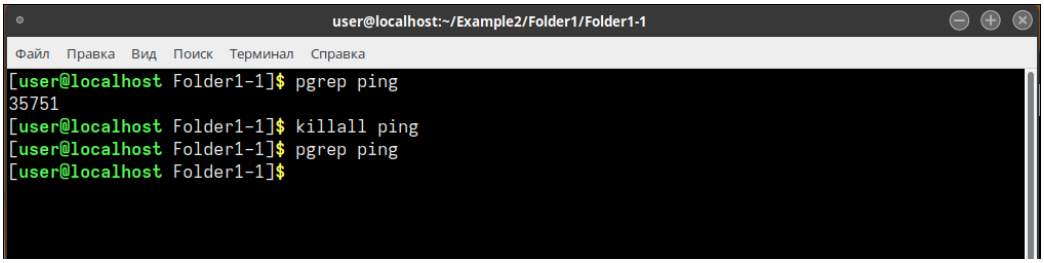
```
kill -l
killall -l
```

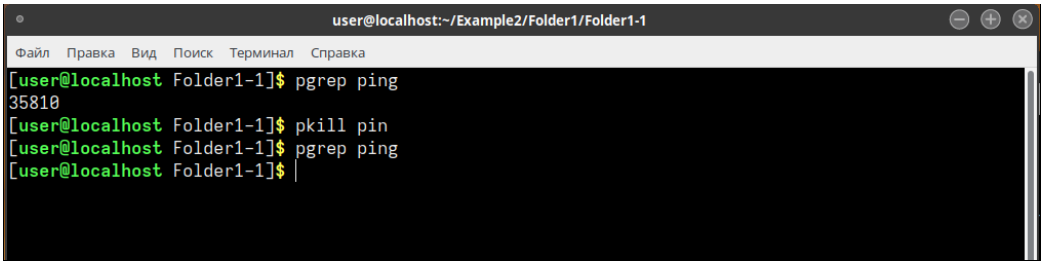
Принудительно завершить процесс можно, используя команды:

```
kill <PID_процесса>
killall <имя_процесса>
pkill <шаблон>
```

Утилита pkill может использовать как полное имя процесса для его завершения, так и часть имени. Утилита сопоставляет переданное ей имя процесса и может по ошибке завершить процесс с похожим именем, поэтому работу с утилитой следует проводить с осторожностью.

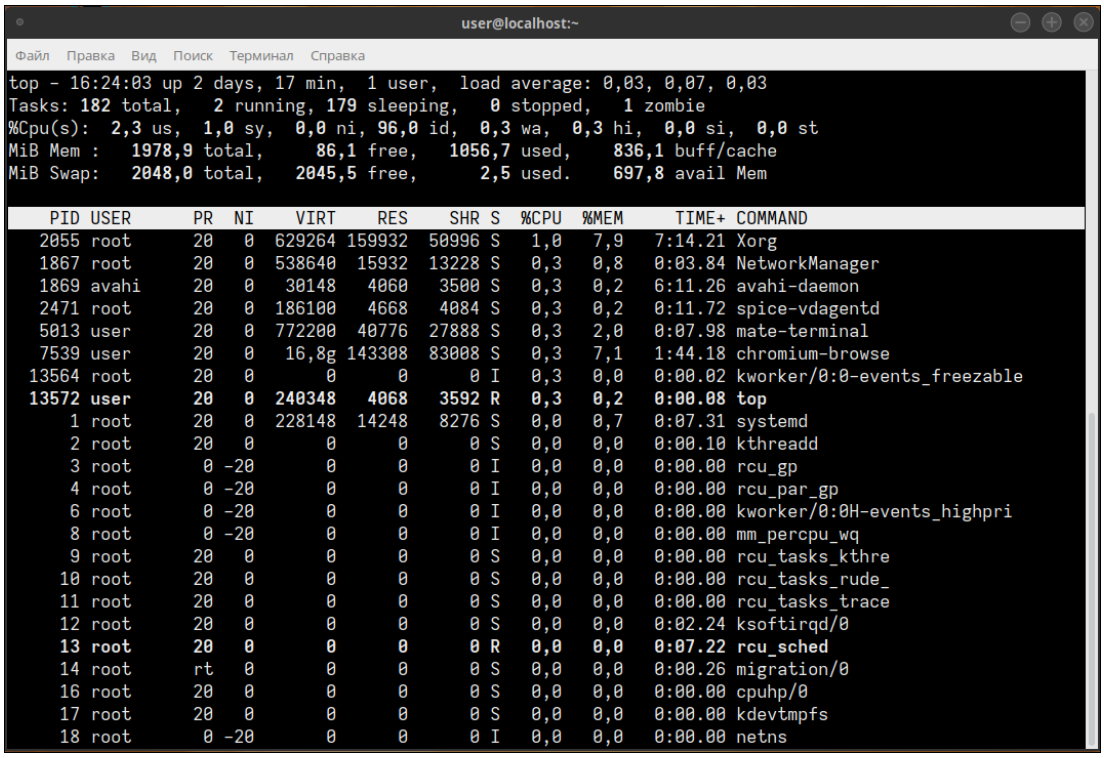






top / htop

Обе команды похожи, обе отображают процессы и могут быть использованы как консольные системные мониторы. **htop** - это улучшенная версия **top**. Вы сможете не только просматривать, но и контролировать процессы через его интерактивный интерфейс.



date

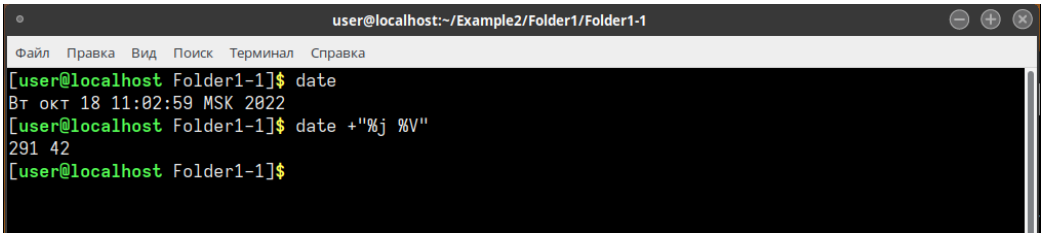
В отличие от **time**, выводит текущую дату и время в различных форматах и позволяет устанавливать системное время. Его можно форматировать в зависимости от ваших потребностей: вывести год, месяц, день, установить 12-ти или 24-ти часовой формат, получить наносекунды или номер недели. Например, **date +"%j %V"** выведет день в году и номер недели в формате ISO.

Установка системных даты и времени производится с правами администратора или суперпользователя (**root**) системы командой:

```
date ММДДччмм[[ВВ]ГГ][.сс]
```

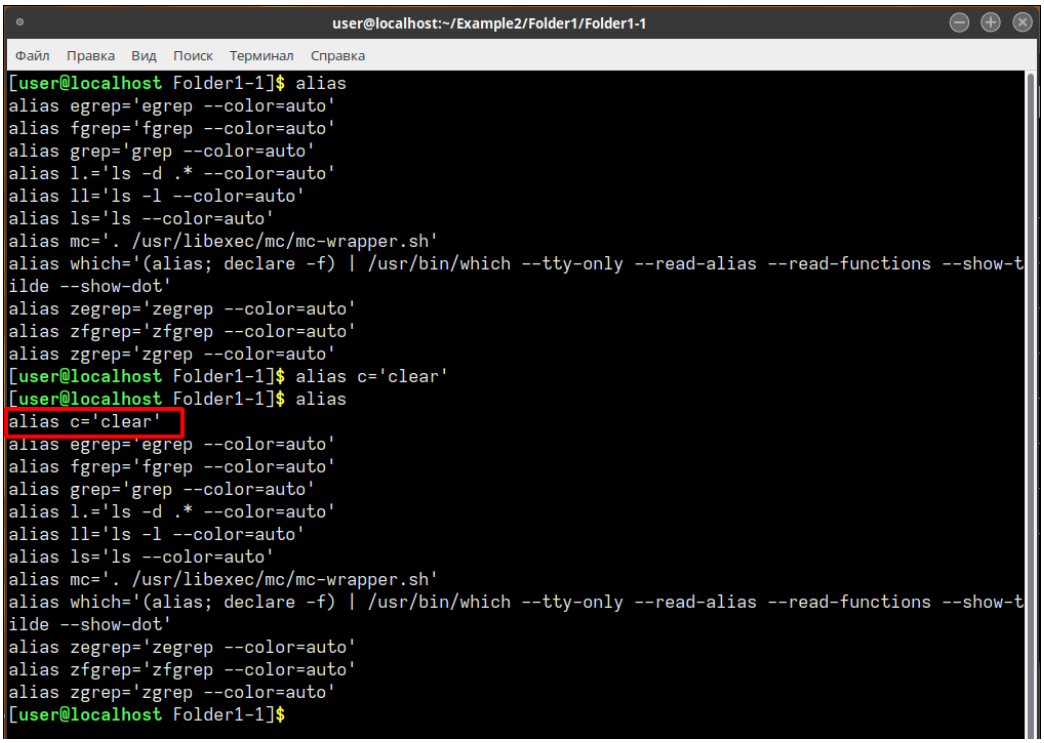
где:

- ММ - Месяц (от 01 до 12);
- ДД - День (от 01 до 28, 29, 30 или 31 в зависимости от месяца);
- чч - Часы (от 00 до 24);
- мм - Минуты (от 00 до 59);
- ГГ - Две последние цифры года (от 00 до 99, не обязательно);
- ВВ - Век (от 00 до 99, используется вместе с предыдущим элементом, не обязательно);
- .сс - Секунды (от 00 до 59 с символом точки, не обязательно).



alias

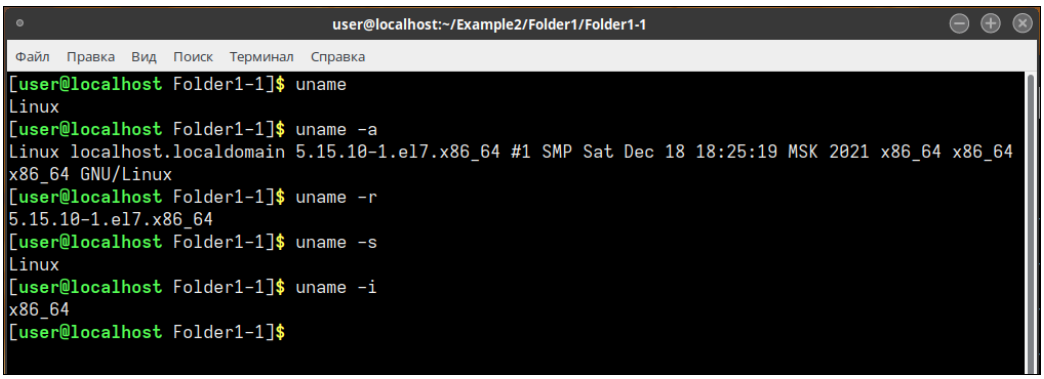
Команда создаёт синонимы для других команд Linux. То есть вы можете создать новые команды или группы команд, а также переименовывать существующие. Это очень удобно для сокращения длинных названий команд, которые вы часто используете, или создания более понятных имен для команд, которые вы используете нечасто или не можете запомнить.



uname

Выводит основную информацию о системе. Основные опции:

- **-a** (all) - информация о ядре, имени хоста и архитектуре процессора;
- **-i** - имя аппаратной реализации (платформы);
- **-r** - информация о релизе системы;
- **-s** - имя операционной системы, опция используется по умолчанию.

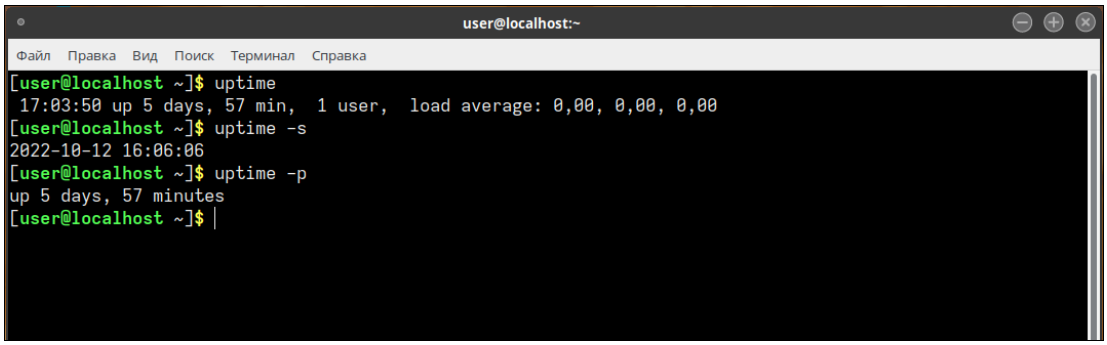


uptime

Выводит время работы системы, количество текущих в данный момент пользователей и среднюю загрузку системы за последние 1, 5 и 15 минут.

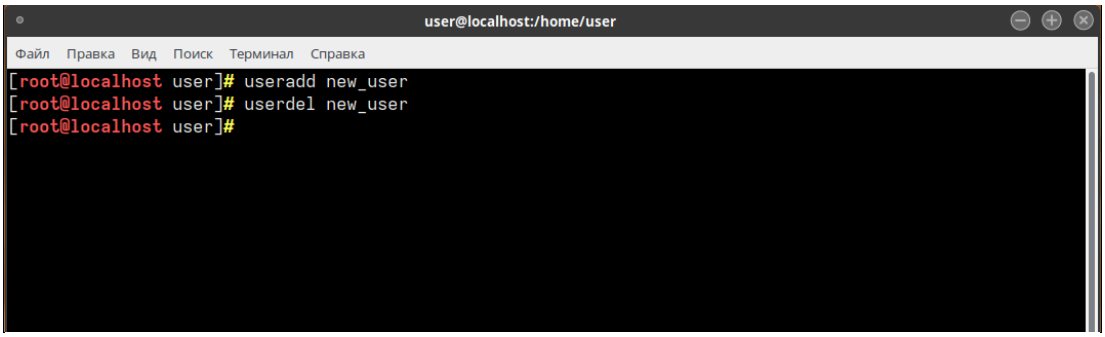
Можно использовать опции:

- **-s** (--since) - вывести время запуска системы. Это время, начиная с которого, отсчитывается время работы системы. Время выводится в формате YYYY-MM-DD HH:MM:SS;
- **-p** (--pretty) - вывести только время работы системы.



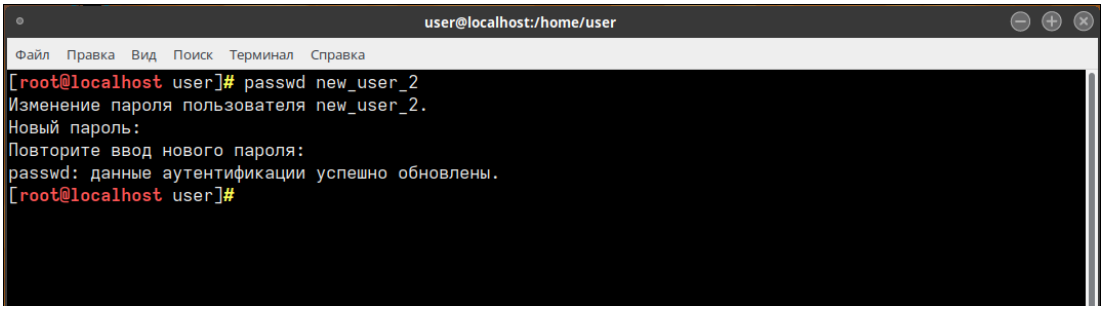
useradd / userdel / usermod

Эти команды позволяют добавлять, удалять и изменять учетные записи пользователей, для использования команд необходимы права администратора или суперпользователя (**root**) системы.



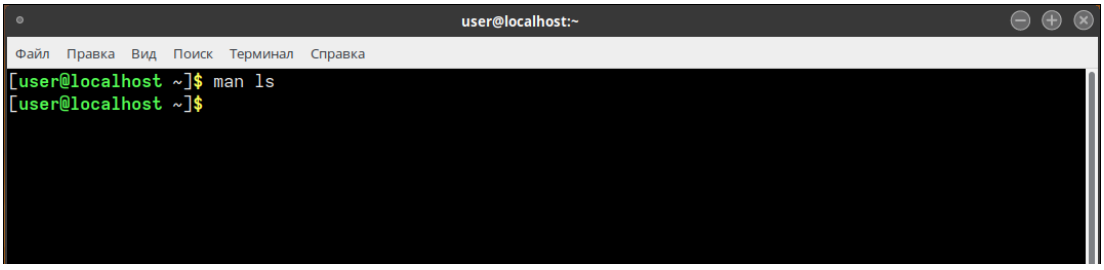
passwd

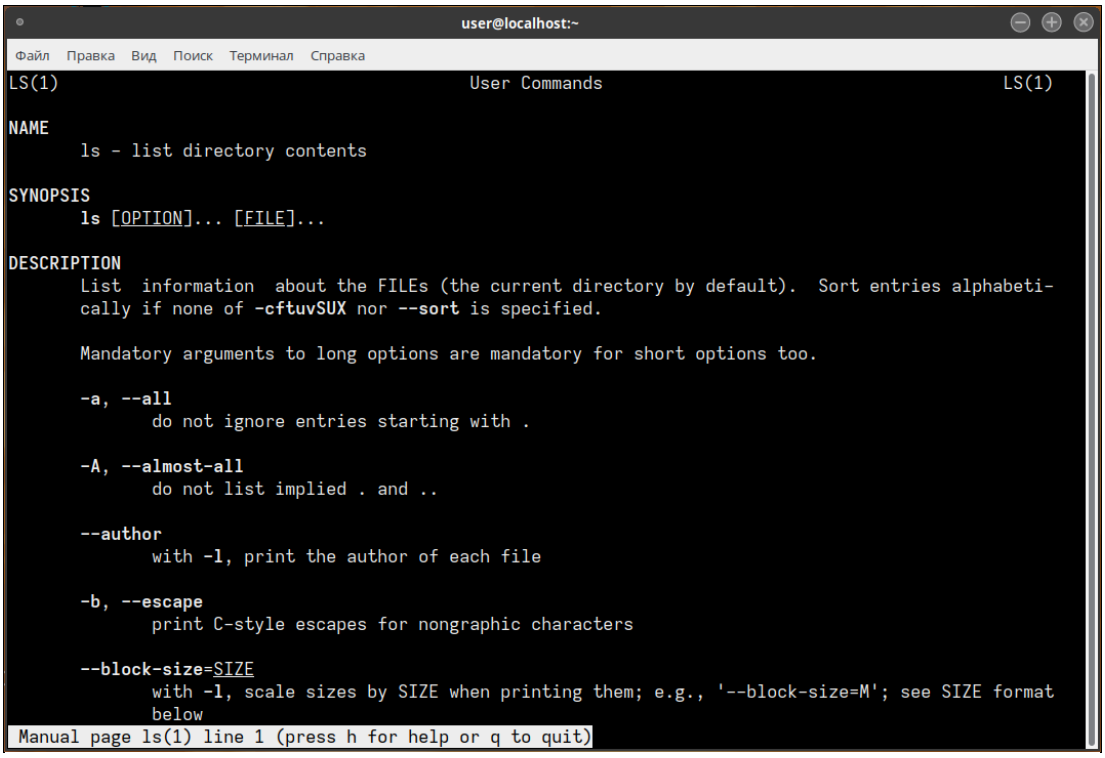
Эта команда позволяет изменить пароль учетной записи пользователя. Для использования команды необходимы права администратора или суперпользователя (**root**) системы.

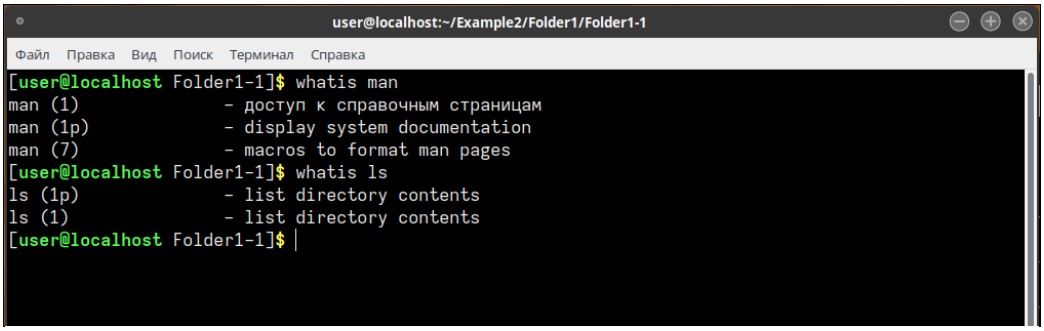


man / whatis

Команда **man** открывает руководство по определённой команде. Для всех основных команд Linux есть **man**-страницы. **Whatis** показывает, какие разделы руководств есть для данной команды.

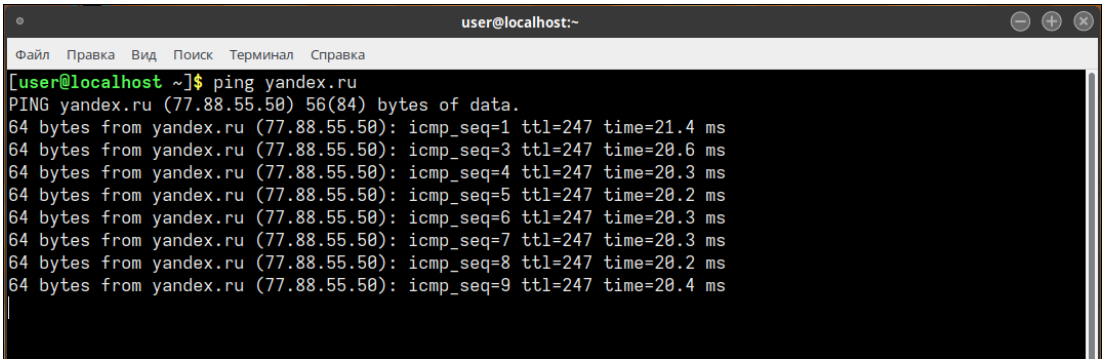






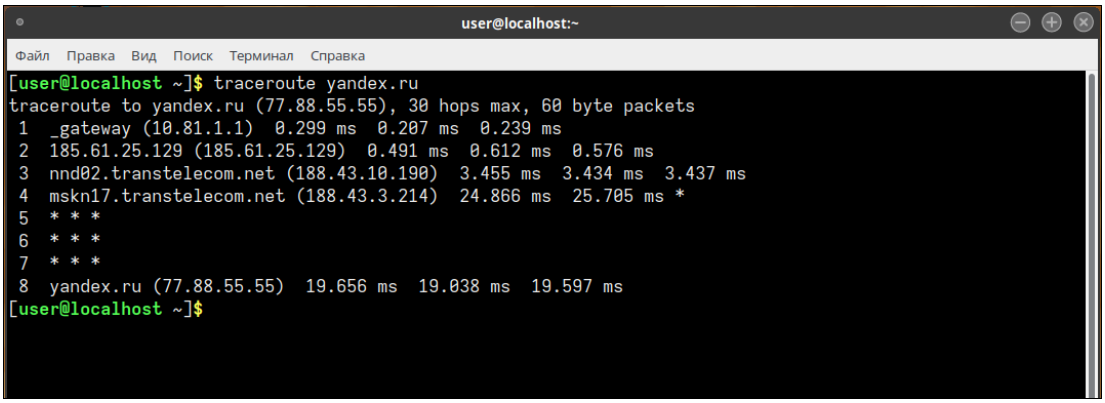
ping

Утилита **ping** может быть очень полезным диагностическим инструментом. Она поможет быстро проверить, подключены ли вы к маршрутизатору или к интернету, и дает некоторое представление о качестве этой связи.



traceroute

Это усовершенствованная версия **ping**. Мы можем увидеть не только полный маршрут сетевых пакетов, но и доступность узла, а также время доставки этих пакетов на каждый из узлов.



journalctl

journald — системная служба, отвечающая за сбор, хранение и управление данными журналов в ОС, также выполняет ротацию, сжатие и индексацию лог-файлов. **journalctl** позволяет просматривать и фильтровать данные, собираемых службой **journald**.

Полезные опции:

- **-f** — показать последние записи журнала и продолжить вывод новых записей при добавлении их в журнал;
- **-xb** — вывод записей журнала с момента запуска текущей сессии с расшифровкой ошибок.

```
[user@localhost ~]$ journalctl -f
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-tmpfiles-setup.service: Suc
ceeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped Create User's Volatile File
s and Directories.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus-broker.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped D-Bus User Message Bus.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus.socket: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Closed D-Bus User Message Bus Socke
t.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Shutdown.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-exit.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Finished Exit the Session.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Exit the Session.
```

ip

ip — утилита командной строки из пакета **iproute2**, которая позволяет выполнять настройку сетевой подсистемы и является заменой таких утилит, как *ifconfig*, *route*, *arp*.

```
[user@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group d
efault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    altname enp0s25
    inet [redacted] brd [redacted] scope global dynamic noprefixroute eno1
       valid_lft 90149sec preferred_lft 90149sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever
4: anbox0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group de
fault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet [redacted] scope global anbox0
       valid_lft forever preferred_lft forever
```

netstat

netstat — утилита командной строки, выводящая состояние TCP-соединений (как входящих, так и исходящих), таблицы

маршрутизации, число сетевых интерфейсов и сетевую статистику по протоколам.

```
[root@localhost user]# netstat --inet -pl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:46825         0.0.0.0:*               LISTEN      1088/containerd
tcp        0      0 0.0.0.0:ideafarm-door   0.0.0.0:*               LISTEN      1055/vmware-authdla
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      1086/sshd: /usr/sbi
tcp        0      0 localhost:54329         0.0.0.0:*               LISTEN      1113/postgres
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2133/dnsmasq
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      1078/cupsd
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN      1258/master
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2180/dnsmasq
udp        0      0 0.0.0.0:40848           0.0.0.0:*                           791/avahi-daemon: r
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2180/dnsmasq
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2180/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*                           1/systemd
udp        0      0 localhost:323           0.0.0.0:*                           848/chronyd
```

df

Утилита **df** — консольная утилита, которая позволяет проверить использование дискового пространства в операционной системе. Эта команда отображает информацию об общем, свободном и используемом объеме памяти файловых систем. Утилита **df** предоставляет множество опций, которые позволяют настроить ее вывод.

```
[root@localhost user]# df
Файловая система 1K-блоков Использовано  Доступно Использовано% Смонтировано в
devtmpfs              4096            0      4096            0% /dev
tmpfs              4011852       608496   3403356           16% /dev/shm
tmpfs              1604744         3632   1601112            1% /run
/dev/sdb1        234213368    181416340  40826880           82% /
/dev/sda4        530945160    134478724 369422392           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1          106496       106496         0          100% /var/lib/snapd/snap/core/16928
/dev/loop0          108032       108032         0          100% /var/lib/snapd/snap/core/16574
/dev/loop2           57088        57088         0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3           57088        57088         0          100% /var/lib/snapd/snap/core18/2812
/dev/loop4           73088        73088         0          100% /var/lib/snapd/snap/webinar/7
/dev/loop6             128          128         0          100% /var/lib/snapd/snap/bare/5
/dev/loop7          168832       168832         0          100% /var/lib/snapd/snap/gnome-3-28-1804/198
/dev/loop5          382848       382848         0          100% /var/lib/snapd/snap/anbox/186
/dev/loop8           93952        93952         0          100% /var/lib/snapd/snap/gtk-common-themes/1535
/dev/loop9           72960        72960         0          100% /var/lib/snapd/snap/webinar/6
tmpfs               802368          160    802208            1% /run/user/1000
[root@localhost user]# df -h
Файловая система Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs           4,0M            0  4,0M            0% /dev
tmpfs              3,9G          595M  3,3G           16% /dev/shm
tmpfs              1,6G          3,6M  1,6G            1% /run
/dev/sdb1          224G          174G   39G           82% /
/dev/sda4          507G          129G  353G           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1         104M          104M     0          100% /var/lib/snapd/snap/core/16928
/dev/loop0         106M          106M     0          100% /var/lib/snapd/snap/core/16574
/dev/loop2          56M           56M     0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3          56M           56M     0          100% /var/lib/snapd/snap/core18/2812
```

free

Команда **free** предоставляет информацию об общем объеме физической памяти и памяти подкачки, а также о свободной и используемой памяти.

```
[user@localhost ~]$ free
               total        used        free      shared  buff/cache   available
Mem:         8023704     6372008      367168      575088     1284528      781116
Swap:        5122228     4663944      458284
[user@localhost ~]$ free -m
               total        used        free      shared  buff/cache   available
Mem:            7835        6225         355         561        1254         760
Swap:           5002        4554         447
[user@localhost ~]$ free -h
               total        used        free      shared  buff/cache   available
Mem:           7,7Gi       6,1Gi       355Mi       565Mi       1,2Gi       759Mi
Swap:          4,9Gi       4,4Gi       447Mi
[user@localhost ~]$
```

Получение справочной информации об использовании утилит с помощью man

Установка
Навигация
Разделы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО:** man-db-2.9.4-4, man-pages-5.12-4

man — утилита, предназначенная для форматирования и вывода справочных страниц. Каждая страница справки является самостоятельным документом и пишется разработчиками соответствующего программного обеспечения.

Установка

В РЕД ОС по умолчанию утилита уже установлена. Однако, если по каким-либо причинам она отсутствует, ее можно установить. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install man man-pages
```

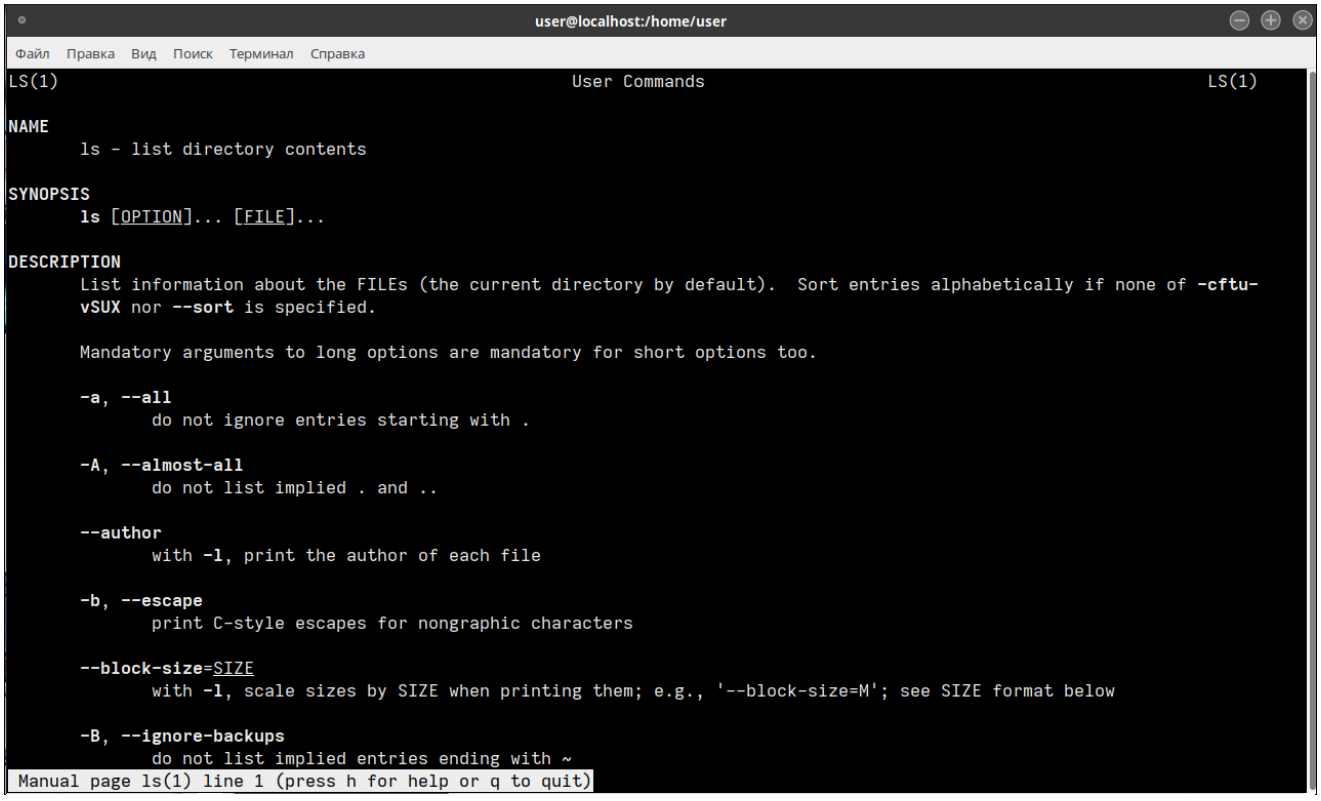
Далее команды будут выполняться с правами **локального пользователя**, если не указано иное.

Для вывода справочного руководства по какой-либо команде или пакету с возможностью запуска в терминале необходимо выполнить команду вида:

```
man <команда>
```

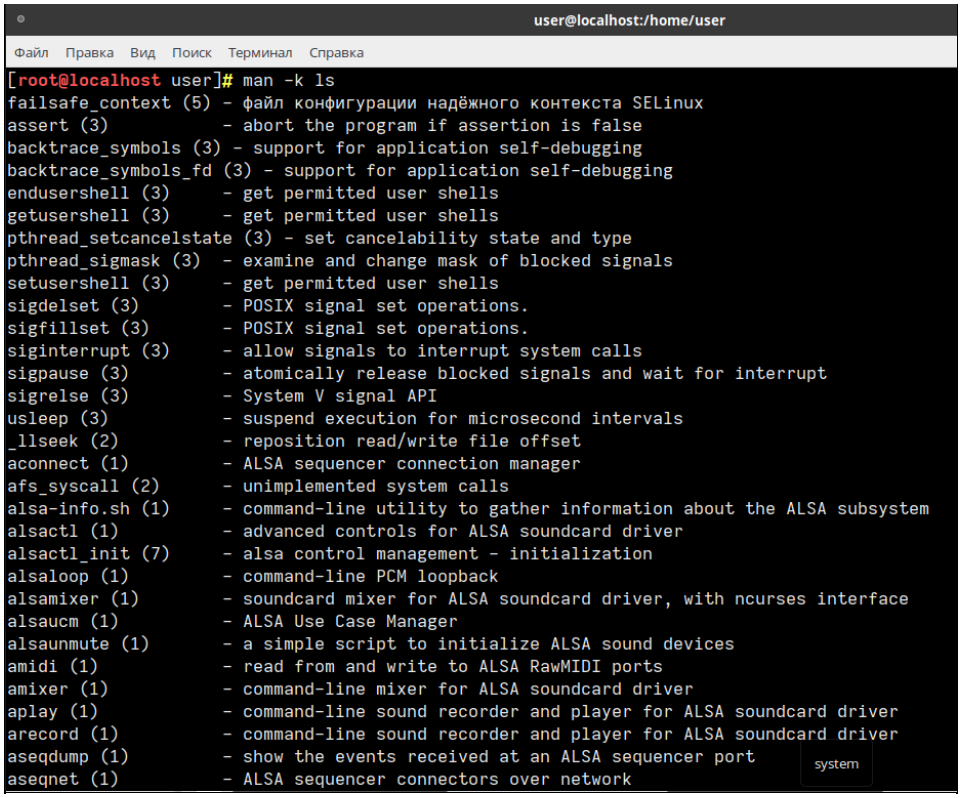
Например:

```
man ls
```



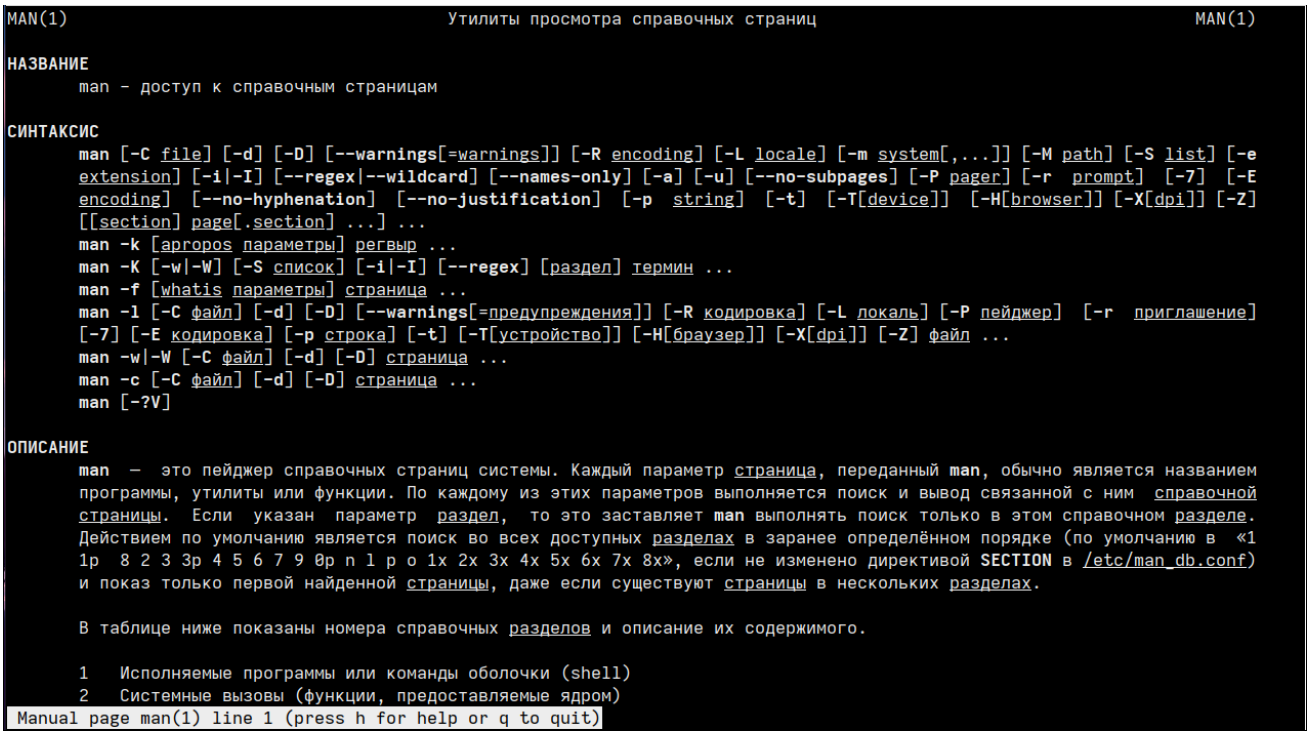
Опция **-k** выполняет поиск и выводит список man-страниц, в которых встречается искомый запрос.

```
man -k ls
```



Другие полезные опции утилиты **man** можно посмотреть командой:

```
man man
```



Навигация

Для навигации по страницам руководства используются следующие сочетания клавиш:

- ↑ и ↓ — для построчного перехода по руководству;
- **PgUp** и **PgDown** — для постраничного перехода по руководству;

- **/** — поиск по странице; введите **/** и искомое слово, затем нажмите **Enter**;
- **?** — поиск в обратном направлении (снизу вверх); введите **?** и искомое слово, затем нажмите **Enter**;
- **n** — переход к следующему подсвеченному вхождению;
- **Shift+n** — переход к предыдущему подсвеченному вхождению;
- **&** — поиск внутри страницы; выводятся только строки, где было найдено искомое слово;
- **h** — открыть справку по командам и горячим клавишам, для закрытия справки нажмите **q**;
- **q** — закрыть man-страницу.

Разделы

Справочные страницы поделены на 8 стандартных разделов и один дополнительный. Каждый из разделов соответствует той или иной тематике.

Раздел	Краткое описание
1	Прикладные программы и команды оболочки
2	Системные вызовы ядра (функции языка Си)
3	Библиотечные вызовы (функции различных библиотек, установленных в систему)
4	Специальные файлы (находящиеся обычно в каталоге **/dev**)
5	Форматы файлов и соглашения
6	Игры
7	Различные описания, соглашения и прочее
8	Команды администрирования системы, которые обычно запускаются от имени суперпользователя
9	Ядро операционной системы (нестандартный раздел)

Номер раздела в команде **man** указывается вторым аргументом, перед названием справочной страницы. Если номер раздела опущен, то поиск справочной страницы ведётся по всем разделам по порядку.

```
man kill  # раздел 1
man 1 kill  # раздел 1
man 2 kill  # раздел 2
```

Общие рекомендации

В целях соблюдения безопасности рекомендуется:

- не использовать пароли, попытка установки которых приводит к предостережению от утилиты **passwd**;
- не работать привилегированным пользователем;
- не запускать те сервисы, которыми никто не будет пользоваться, и отключать временно неиспользуемые;
- следовать основным правилам сетевой безопасности:
    - настроить **firewall** между компьютером и остальной сетью, а также между корпоративной сетью и Интернет;
    - использовать защищенные протоколы для передачи данных, такие как **IPSEC** (IP Security) и **SSH** (Secure Shell);

- не использовать электронную почту для передачи конфиденциальной информации; если использование электронной почты для этих целей абсолютно необходимо, например, ввиду отсутствия технической возможности применения защищенных протоколов передачи данных, то воспользуйтесь **GnuPG** для подписи и шифрования почтовых сообщений;
- использовать различные пароли к локальным ресурсам и ресурсам, расположенным на удаленных серверах, чтобы пароли к локальным ресурсам не покидали пределов локальной сети.

В РЕД ОС настройки для пользователя *root* определяются спецификой его задач, а потому не приспособлены для повседневной работы и лишь ограниченно локализованы.

Аудит в РЕД ОС

Журналирование
Аудит системных вызовов
Файлы и утилиты аудита РЕД ОС
Описание auditd.conf
Служба аудита — auditd
Утилита auditctl
Примеры базовых правил и конструкций утилиты auditctl
Утилита aureport
Утилита ausearch
Утилита autrace

Основными целями при разработке системных вызовов для подсистемы аудита были:

- максимально низкая нагрузка на производительность;
- отсутствие подобной функциональности в SELinux (и/или в любой другой подсистеме безопасности).

Инструментарий аудита будет работать без внедренных компонент безопасности, но он не может быть использован вместо них, например, он не будет предоставлять функциональные возможности без действующих подсистем безопасности.

Есть две основные части: одна работает всегда (базовое журналирование в **audit.c**), а другой можно управлять во время загрузки или работы сервера (аудит системных вызовов в **auditsc.c**). Патч включает в себя изменения в **security/selinux/avc.c** в качестве примера, как системные вызовы аудита могут быть использованы совместно с другим кодом, определяющим события для аудита.

Журналирование

Использует сетевой сокет для связи с пользовательским пространством. Если служба запущена - все сообщения журналируются через этот сетевой сокет. Иначе, сообщения журналируются через **printk** посредством службы **syslog** (по умолчанию).

Сообщения могут не журналироваться (настраивается отдельно) в зависимости от настроек аудита, скорости генерации сообщений или загруженности памяти.

Когда какая-то часть ядра генерирует часть сообщения аудита, эта часть будет немедленно послана в пользовательское пространство, и автоматически выставится флаг, указывающий, что этот системный вызов находится под аудитом. Таким образом, при выходе из системного вызова будет сформирована дополнительная информация (если включен аудит системных вызовов).

Аудит системных вызовов

Во время создания процесса формируется контекст аудита и привязывается к структуре, описывающей процесс.

Во время входа в системный вызов, заполняется следующая информация в контексте аудита, если он есть: номер системного вызова, дата и время, но не аргументы.

В ходе работы системного вызова перехватываются обращения к **getname()** и **path_lookup()**. Эти процедуры вызываются, когда ядро действительно собирается искать информацию для принятия решения, будет ли системный вызов успешно выполнен или нет. Перехватывать вызовы нужно для того, чтобы не допустить копирование информации, которую генерирует **getname**, поскольку **getname** уже сделал приватную (для ядра) копию этой информации.

Сохранение копий всех аргументов системного вызова усложняет реализацию и требует увеличения расхода ресурсов, что, наиболее вероятно, не нужно. С этим патчем, к примеру, если пользователь непривилегированный, то **chroot** ("foo") будет завершен с ошибкой - "foo" не будет отражено в записи аудита, потому что ядро определяет еще перед поиском "foo", что работа системного вызова не может быть продолжена. Этот подход предотвращает сохранение пользовательской информации, которая может быть ложной или ненадежной (например, из-за атаки на совместно используемую память) в отличие от истинной информации, фактически используемой ядром.

Во время выхода их системного вызова генерируется та часть сообщения аудита, которая ответственна за информацию о системном вызове, включая имена файлов и номера **inode** (если доступны). Сообщение о системном вызове генерируется, только если выставлен флаг, указывающий, что системный вызов находится под аудитом (он выставляется, например, когда SELinux генерирует ***avc*** сообщение или когда другая часть ядра определяет, что должно формироваться сообщение для аудита). Следует заметить, что полное сообщение аудита приходит в пользовательское пространство по частям, это позволяет не хранить сообщения неопределенный срок внутри ядра.

Во время завершения процесса контекст аудита уничтожается.

Во время генерации сообщения аудита может быть выполнена простая фильтрация (например, для увеличения производительности - отключение аудита системных вызовов, выполняемых от имени пользователя, работающего с базой данных). Фильтрация может быть, как простой, так и сложной. В основном, инструментарий аудита использует компоненты ядра (например, SELinux), чтобы принимать

решение о том, что необходимо подвергать аудиту, а что нет.

Файлы и утилиты аудита РЕД ОС

Описание auditd.conf

В файле **/etc/audit/auditd.conf** определяются параметры службы аудита. На одной строке может быть не больше одной директивы. Директива состоит из ключевого слова (названия параметра), знака равенства и соответствующих ему данных (значения параметра). Допустимые ключевые слова:

log_file, log_format, flush, freq, num_logs, max_log_file, max_log_file_action, space_left, action_mail_acct, space_left_action, admin_space_left, admin_space_left_action, disk_full_action и disk_error_action.

Далее даётся описание каждого из них.

Ключ	**Значение ключа**
log_file	Полное имя файла, в который следует записывать протокол.
log_format	Оформление данных в протоколе. Допустимы два значения: *raw* и *nolog*. При указании **RAW**, данные будут записываться в том виде, в котором они получаются от ядра. Значение **NOLOG** отключает запись данных об аудите. Этот параметр не влияет на обработку данных диспетчером событий системы аудита.
priority_boost	Неотрицательное число, определяющее повышение приоритета выполнения службы аудита. Значение по умолчанию: **3**. Для того чтобы не изменять приоритет, укажите **0**.
flush	Стратегия работы с дисковым буфером. Допустимые значения: *none*, *incremental*, *data* и *sync*. Вариант **none**, отключает какие-либо дополнительные действия со стороны службы по синхронизации буфера с диском. При значении **incremental**, запросы на перенос данных из буфера на диск выполняются с частотой задаваемой параметром **freq**. При значении **data** данные файла синхронизируются немедленно. Значение **sync** указывает на необходимость немедленной синхронизации как данных, так и метаданных файла при записи на диск.
freq	Максимальное число записей протокола, которые могут храниться в буфере. При достижении этого числа производится запись буферированных данных на диск. Данный параметр допустим, только если **flush** имеет значение **incremental**.
num_logs	Максимальное число файлов с протоколами. Используется, если параметр **max_log_file_action** имеет значение **rotate**. Если указано число меньше 2, при достижении ограничения на размер файла он обнуляется. Значение параметра не должно превышать **99**. Значение по умолчанию: **0**. При указании большого числа может потребоваться увеличить ограничение на количество ожидающих запросов. Это можно сделать в файле **/etc/audit/rules.d/audit.rules**.
dispatcher	Диспетчер - программа, которой (на стандартный ввод) будут передаваться копии сообщений о событиях аудита. Она запускается (с правами администратора) службой аудита при загрузке последней.
disp_qos	Разрешить ли блокирование при взаимодействии с диспетчером. Для передачи информации диспетчеру используется буфер размером 128 Кб. Это значение является оптимальным для большинства случаев. Если блокирование запрещено (**lossy**), то все сообщения, поступающие при полном буфере, не будут доходить до диспетчера (записи о них по-прежнему будут вноситься в файл на диске, если только **log_format** не равно **nolog**). В случае, если блокирование разрешено (**lossless**), служба аудита будет ожидать появления свободного места в очереди, передавать сообщение диспетчеру и только потом записывать его на диск. Допустимые значения: **lossy** и **lossless**. Значение по умолчанию - **lossy**.
max_log_file	Ограничение на размер файла протокола в мегабайтах. Действие, выполняемое при достижении размера файла указанного значения, можно настроить с помощью следующего параметра.
max_log_file_action	Действие, предпринимаемое при достижении размером файла протокола максимального значения. Допустимые значения: *ignore*, *syslog*, *suspend*, *rotate* и *keep_logs*. Вариант **ignore** отключает контроль над размером файла. При значении **syslog** в системный протокол будет внесено соответствующее сообщение. При значении **suspend** дальнейшее ведение протокола будет прекращено. Служба по-прежнему будет работать. При значении **rotate** текущий файл будет переименован и для протокола будет создан новый файл. Имя предыдущего протокола будет дополнено числом **1**, а номера других протоколов (если они имеются) будут увеличены на единицу. Таким образом, чем больше номер у протокола, тем он старше. Максимальное число файлов определяется параметром **num_logs** (естественно, соответствие ему достигается за счёт удаления самых старых протоколов). Такое поведение аналогично поведению утилиты **logrotate**. Вариант **keep_logs** аналогичен предыдущему, но число файлов не ограничено.
action_mail_acct	Адрес электронной почты. Значение по умолчанию: root. Если адрес не локальный по отношению к данной системе, необходимо чтобы в ней был настроен механизм отправки почты. В частности, требуется наличие программы **/usr/lib/sendmail**.
space_left	Минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое следующим параметром.
space_left_action	Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного минимума. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается программа по указанному пути. Передача параметров не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.
admin_space_left	Критический минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое следующим параметром. Данное действие следует рассматривать как последнюю меру, предпринимаемую перед тем, как закончится место на диске. Значение настоящего параметра должно быть меньше значения **space_left**.

Ключ	Значение ключа
admin_space_left_action	Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного критического минимума. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении **email** по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается программа по указанному пути. Передача параметров не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.
disk_full_action	Действие, предпринимаемое при обнаружении отсутствия свободного пространства на диске. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается сценарий по указанному пути. Передача параметров сценарию не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.
disk_error_action	Действие, предпринимаемое при возникновении ошибки в работе с диском. Допустимые значения - *ignore*, *syslog*, *email*, *exec*, *suspend*, *single* и *halt*. При значении **ignore** никаких действий не производится. При значении **syslog** в системный протокол добавляется соответствующая запись. При значении **email** по адресу, указанному в **action_mail_acct**, отправляется уведомление. При значении **exec** запускается сценарий по указанному пути. Передача параметров сценарию не поддерживается. При значении **suspend** служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание **single** приведёт к переводу компьютера в однопользовательский режим. Указание **halt** приведёт к выключению компьютера.

ВАЖНО!

В среде CAPP (Controlled Access Protection Profile - контролируемый профиль защиты доступа) ведение протоколов настолько важно, что невозможность его продолжения может служить основанием отказа в доступе к ресурсам. Поэтому рекомендуется выделять для файла **/var/log/audit** специальный раздел. Кроме того, параметру **flush** следует присвоить значение **sync** или **data**.

Для обеспечения полного использования раздела параметрам **max_log_file** и **num_logs** следует присвоить соответствующие значения. Учитывайте, что чем больше файлов создаётся на диске (и, соответственно, переименовывается), тем больше времени будет уходить на обработку событий при достижении размером очередного файла максимума. Параметру **max_log_file_action** рекомендуется присвоить значение **keep_logs**.

Значение **space_left** должно быть таким, которое позволит администратору вовремя среагировать на предупреждение. Обычно в число действий, выполняемых администратором, входит запуск **aureport -t** и архивирование самых старых протоколов. Значение **space_left** зависит от системы, в частности от частоты поступления сообщений о событиях. Значение **space_left_action** рекомендуется установить в **email**. Если требуется отправка сообщения **snmp trap**, укажите вариант **exec**.

Установите значение **admin_space_left** таким образом, чтобы хватило свободного места для сохранения записей о последующих действиях администратора. Значение параметра **admin_space_left_action** следует установить в **single**, ограничив, таким образом, способы взаимодействия с системной консолью.

Действие, указанное в **disk_full_action**, выполняется, когда в разделе уже не осталось свободного места. Доступ к ресурсам машины должен быть полностью прекращён, т.к. нет возможности контролировать работу системы. Это можно сделать, указав значение **single** или **halt**.

Значение **disk_error_action** следует установить в **syslog**, **single**, либо **halt** в зависимости от соглашения относительно обращения со сбойным аппаратным обеспечением.

Служба аудита - auditd

Служба **auditd** - это прикладной компонент системы аудита Linux. Он ведёт протокол аудита на диске. Для просмотра протоколов предназначены команды **ausearch** и **aureport**. Команда **auditctl** позволяет настраивать правила аудита. Кроме того, при загрузке загружаются правила из файла **/etc/audit/rules.d/audit.rules**. Некоторые параметры самой службы можно изменить в файле **auditd.conf**.

Синтаксис:

```
auditd [-f] [-l] [-n]
```

Опции:

Опция	Значение опции
-f	Не переходить в фоновый режим (для отладки). Сообщения программы будут направляться в стандартный вывод для ошибок (**stderr**), а не в файл.
-l	Включить следование по символическим ссылкам при поиске конфигурационных файлов.

Опция	Значение опции
-n	Не создавать дочерний процесс. Для запуска из **inittab**.

Сигналы:

Сигнал	Значение сигнала
SIGHUP	Перезагрузить конфигурацию - загрузить файл конфигурации с диска. Если в файле не окажется синтаксических ошибок, внесенные в него изменения вступят в силу. При этом в протокол будет добавлена запись о событии **DAEMON_CONFIG**. В противном случае действия службы будут зависеть от параметров **space_left_action**, **admin_space_left_action**, **disk_full_action**, **disk_error_action** файла **auditd.conf**.
SIGTERM	Прекратить обработку событий аудита и завершить работу, о чём предварительно занести запись в протокол.
SIGUSR1	Создать новый файл для протокола, перенумеровав старые файлы или удалив часть из них, в зависимости от параметра **max_log_size_action**.

ВАЖНО!

Для того чтобы сделать возможным аудит всех процессов, запущенных до службы аудита, добавьте в строку параметров ядра (в конфигурации загрузчика) **audit=1**. В противном случае аудит некоторых процессов будет невозможен.

Утилита auditctl

Утилита **auditctl** используется для контроля поведения, получения состояния и добавления/удаления правил аудита, предоставляемого Linux ядром.

Опции:

Опция	Значение опции
-b *<лимит>*	Установить максимальное количество доступных для аудита буферов, ожидающих обработки (значение в ядре по умолчанию - 64). Если все буфера заняты, то флаг сбоя будет выставлен ядром для его дальнейшей обработки.
-e [0..2]	Установить флаг блокировки. **0** позволит на время отключить аудит, включить его обратно можно, передав **1** как параметр. Если установлено значение опции **2**, то защитить конфигурацию аудита от изменений. Каждый, кто захочет воспользоваться этой возможностью, может поставить эту команду последней в **audit.rules**. После этой команды все попытки изменить конфигурацию будут отвергнуты с уведомлением в журналах аудита. В этом случае, чтобы задействовать новую конфигурацию аудита, необходимо перезагрузить систему аудита.
-f [0..2]	Установить способ обработки для флага сбоя. **0**=silent **1**=printk **2**=panic. Эта опция позволяет определить, каким образом ядро будет обрабатывать критические ошибки. Например, флаг сбоя выставляется при следующих условиях: ошибки передачи в пространство службы аудита, превышение лимита буферов, ожидающих обработки, выход за пределы памяти ядра, превышение лимита скорости выдачи сообщений. Значение по умолчанию: **1**. Для систем с повышенными требованиями к безопасности, значение **2** может быть более предпочтительно.
-h	Краткая помощь по аргументам командной строки.
-i	Игнорировать ошибки при чтении правил из файла.
-l	Вывести список всех правил по одному правилу в строке.
-k *<ключ>*	Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше *31 символа*. Ключ помогает уникально идентифицировать записи, генерируемые в ходе аудита за точкой наблюдения.
-m *<текст>*	Послать в систему аудита пользовательское сообщение. Это может быть сделано только из-под учетной записи **root**.
-p [r|w|x|a]	Установить фильтр прав доступа для точки наблюдения. **r**=чтение, **w**=запись, **x**=исполнение, **a**=изменение атрибута. Не путайте эти права доступа с обычными правами доступа к файлу - они определяют типы системных вызовов, которые выполняют данные действия. Заметьте, системные вызовы **read** и **write** не включены в этот набор, поскольку логи аудита были бы перегружены информацией о работе этих вызовов.
-r *<частота>*	Установить ограничение скорости выдачи сообщений в секунду (**0** - нет ограничения). Если эта частота не нулевая и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: **0**.
-R *<файл>*	Читать правила из *файла*. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Следующие ограничения накладываются на файл: владельцем должен быть **root** и доступ на чтение должен быть только у него. Файл может содержать комментарии, начинающиеся с символа «**#**». Правила, расположенные в файле, идентичны тем, что набираются в командной строке, без указания «**auditctl**».
-s	Получить статус аудита.

Опция	Значение опции
-a *<список, действие>*	Добавить правило с указанным *действием* к концу *списка*. Заметьте, что запятая разделяет эти два значения. Отсутствие запятой вызовет ошибку. Ниже описаны имена доступных списков: • **task** - добавить правило к списку, отвечающему за процессы. Этот список правил используется только во время создания процесса - когда родительский процесс вызывает **fork()** или **clone()**. При использовании этого списка вы можете использовать только те поля, которые известны во время создания процесса: **uid**, **gid** и т.д. • **entry** - добавить правило к списку, отвечающему за точки входа системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам входа системных вызовов. • **exit** - добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов. • **user** - добавить правило, отвечающее за список фильтрации пользовательских сообщений. Этот список используется ядром, чтобы отфильтровать события приходящие из пользовательского пространства перед тем, как они будут переданы службе аудита. Необходимо отметить, что только следующие поля могут быть использованы: **uid**, **auid**, **gid** и **pid**. Все остальные поля будут обработаны, как если бы они не совпали. • **exclude** - добавить правило к списку, отвечающему за фильтрацию событий определенного типа. Этот список используется, чтобы отфильтровывать ненужные события. Например, если вы не хотите видеть *avc* сообщения, вы должны использовать этот список. Тип сообщения задается в поле **msgtype**.

Ниже описаны доступные *действия* для правил:

Действие	Описание действия
never	Аудит не будет генерировать никаких записей. Это может быть использовано для подавления генерации событий. Обычно необходимо подавлять генерацию вверху списка, а не внизу, т.к. событие инициируется на первом совпавшем правиле.
always	Установить контекст аудита. Всегда заполнять его во время входа в системный вызов и всегда генерировать запись во время выхода из системного вызова.
-A *<список, действие>*	Добавить правило с указанным действием в начало списка.
-d *<список, действие>*	Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали и имя системного вызова, и поля сравнения.
-D	Удалить все правила и точки наблюдения.
-S *<имя или номер системного вызова>*/[**all**]	Любой номер или имя системного вызова может быть использован. Также возможно использование ключевого слова **all**. Если какой-либо процесс выполняет указанный системный вызов, то аудит генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов - это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил.

Действие	Описание действия
-F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v]	Задать поле сравнения для правила. Атрибуты поля следующие: *объект*, *операция*, *значение*. Вы можете задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с **-F**. Аудит будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: *равно*, *не равно*, *меньше*, *больше*, *меньше либо равно*, *больше либо равно*, *битовая маска* (**n&v**) и *битовая проверка* (**n&=v**). Битовая проверка выполняет операцию «**and**» над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию «**and**». Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы. Поля сравнения могут быть заданы для следующих объектов: • **a0, a1, a2, a3** - четыре первых аргумента, переданных системному вызову. Строковые аргументы не поддерживаются. Это связано с тем, что ядро должно получать указатель на строку, а проверка поля по значению адреса указателя не желательна. Таким образом, вы должны использовать только цифровые значения. • **arch** - архитектура процессора, на котором выполняется системный вызов. Используйте '**uname -m**', чтобы определить архитектуру. Если вы не знаете архитектуру вашей машины, но хотите использовать таблицу 32-х битных системных вызовов, и ваша машина поддерживает 32 бита, вы можете использовать **b32**. Подобно этому **b64** может быть использовано для использования таблицы 64-х битных системных вызовов. • **auid** - это аббревиатура: *audit uid* - идентификатор пользователя, использованный для входа в систему. • **devmajor** - главный номер устройства (Device Major Number). • **devminor** - вспомогательный номер устройства (Device Minor Number). • **egid** - действительный идентификатор группы; • **euid** - действительный идентификатор пользователя; • **exit** - значение, возвращаемое системным вызовом при выходе; • **fsgid** - идентификатор группы, применяемый к файловой системе; • **fsuid** - идентификатор пользователя, применяемый к файловой системе; • **gid** - идентификатор группы; • **inode** - номер *inode*; • **key** - альтернативный способ установить ключ фильтрации. Смотри выше описание опции **-k**; • **msgtype** - используется для проверки совпадения с числом, описывающим тип сообщения. Может быть использован только в списке **exclude**; • **obj_user** - имя пользователя-владельца ресурса (в контексте SELinux); • **obj_role** - роль ресурса (в контексте SELinux); • **obj_type** - тип ресурса (в контексте SELinux); • **obj_lev_low** - нижний уровень ресурса (в контексте SELinux); • **obj_lev_high** - верхний уровень ресурса (в контексте SELinux); • **path** - полный путь к файлу для точки наблюдения. Смотри ниже описание опции "**-w**". Может быть использован только в списке **exit**; • **perm** - фильтр прав доступа для файловых операций. Смотри выше описание опции "**-p**". Может быть использован только в списке **exit**; • **pers** - персональный номер операционной системы; • **pid** - идентификатор процесса; • **ppid** - идентификатор родительского процесса; • **subj_user** - имя пользователя-владельца процесса (в контексте SELinux); • **subj_role** - роль процесса (в контексте SELinux); • **subj_type** - тип процесса (в контексте SELinux); • **subj_sen** - чувствительность процесса (в контексте SELinux); • **subj_clr** - допуск процесса (в контексте SELinux); • **sgid** - установленный идентификатор группы; • **success** - если значение, возвращаемое системным вызовом, больше либо равно **0**, данный объект будет равен "**true**/**yes**", иначе "**false**/**no**". При создании правила используйте **1** вместо "**true**/**yes**" и **0** вместо "**false**/**no**"; • **suid** - установленный идентификатор пользователя; • **uid** - идентификатор пользователя.
-w *<путь>*	Добавить точку наблюдения за файловым объектом, находящемуся по указанному *пути*. Вы не можете добавлять точку наблюдения к каталогу верхнего уровня - это запрещено ядром. Групповые символы (wildcards) также не могут быть использованы, попытки их использования будут генерировать предупреждающее сообщение. Внутренне точки наблюдения реализованы как слежение за inode. Таким образом, если вы установите точку наблюдения за каталогом, вы увидите файловые события, которые в действительности будут означать обновления метаданных этой inode, и вы можете не увидеть событий, непосредственно связанных с файлами. Если вам необходимо следить за всеми файлами в каталоге, рекомендуется создавать индивидуальную точку наблюдения для каждого файла. В противоположность к правилам аудита системных вызовов, точки наблюдения не оказывают влияния на производительность, связанную с количеством правил посылаемых в ядро.
-W *<путь>*	Удалить точку наблюдения за файловым объектом, находящемуся по указанному *пути*.

Примеры базовых правил и конструкций

ВАЖНО!

Приведенные ниже команды будут выполняться только в ходе работы одного сеанса ОС, если вы хотите сделать это правило постоянным, добавьте его в конец файла **/etc/audit/rules.d/audit.rules** следующим образом:

```
-w /var/log/audit/ -p wra -k auditlog
```

Самоаудит

Отображение успешных и неудачных попыток чтения информации из записей аудита:

```
auditctl -w /var/log/audit/ -p wra -k auditlog
```

Отображение изменения конфигурации аудита, происходящей во время работы функций журналирования:

```
auditctl -w /etc/audit/ -p wra -k auditconfig
auditctl -w /etc/libaudit.conf -p wra -k auditconfig
```

Отслеживание использования инструментов управления аудитом:

```
auditctl -w /sbin/auditctl -p x -k audittools
auditctl -w /sbin/auditd -p x -k audittools
auditctl -w /usr/sbin/auditd -p x -k audittools
auditctl -w /usr/sbin/augenrules -p x -k audittoolss
```

Отслеживание доступа к прочим утилитам службы аудирования:

```
auditctl -a always,exit -F path=/usr/sbin/ausearch -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/aureport -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/aulast -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/aulastlogin -F perm=x -k auditreport
auditctl -a always,exit -F path=/usr/sbin/auvirt -F perm=x -k auditreport
```

Фильтры

Игнорирование событий **SELinux**:

```
auditctl -a always,exclude -F msgtype=AVC
```

Игнорирование событий с меткой рабочей директории:

```
auditctl -a always,exclude -F msgtype=CWD
```

Игнорирование событий с меткой идентификатора криптографического ключа, используемого в криптографических целях:

```
auditctl -a always,exclude -F msgtype=CRYPTO_KEY_USER
```

Игнорирование событий **cron**:

```
auditctl -a never,user -F subj_type=crond_t
auditctl -a exit,never -F subj_type=crond_t
```

Игнорирование событий **chrony**:

```
auditctl -a never,exit -F arch=b32 -S adjtimex -F auid=unset -F uid=chrony -F subj_type=chronyd_t
auditctl -a never,exit -F arch=b64 -S adjtimex -F auid=unset -F uid=chrony -F subj_type=chronyd_t
```

Игнорирование сообщений, связанных с инструментами виртуальной машины:

```
###Игнорирование ошибок VMware tools

auditctl -a never,exit -F arch=b32 -S fork -F success=0 -F path=/usr/lib/vmware-tools -F subj_type=initrc_t -F exit=-2
auditctl -a never,exit -F arch=b64 -S fork -F success=0 -F path=/usr/lib/vmware-tools -F subj_type=initrc_t -F exit=-2
auditctl -a exit,never -F arch=b32 -S all -F exe=/usr/bin/vmtoolsd
auditctl -a exit,never -F arch=b64 -S all -F exe=/usr/bin/vmtoolsd
```

Фильтр событий большого объема:

```
### Игнорирование событий, связанных с работой shm и lvm

auditctl -a never,exit -F arch=b32 -F dir=/dev/shm -k sharedmemaccess
auditctl -a never,exit -F arch=b64 -F dir=/dev/shm -k sharedmemaccess
auditctl -a never,exit -F arch=b32 -F dir=/var/lock/lvm -k locklvm
auditctl -a never,exit -F arch=b64 -F dir=/var/lock/lvm -k locklvm
```

Игнорирование событий с меткой объекта **FileBeat**:

```
auditctl -a never,exit -F arch=b32 -F path=/opt/filebeat -k filebeat
auditctl -a never,exit -F arch=b64 -F path=/opt/filebeat -k filebeat
```

Базовые правила

Отслеживание изменений параметров **Kernel**:

```
auditctl -w /etc/sysctl.conf -p wa -k sysctl
auditctl -w /etc/sysctl.d -p wa -k sysctl
```

Отслеживание удачной и неудачной загрузки **Kernel module**:

```
auditctl -a always,exit -F perm=x -F auid!=-1 -F path=/sbin/insmod -k modules
auditctl -a always,exit -F perm=x -F auid!=-1 -F path=/sbin/modprobe -k modules
auditctl -a always,exit -F perm=x -F auid!=-1 -F path=/sbin/rmmod -k modules
auditctl -a always,exit -F arch=b64 -S finit_module -S init_module -S delete_module -F auid!=-1 -k modules
auditctl -a always,exit -F arch=b32 -S finit_module -S init_module -S delete_module -F auid!=-1 -k modules
```

Отслеживание изменений конфигурации **Modprobe**:

```
auditctl -w /etc/modprobe.conf -p wa -k modprobe
auditctl -w /etc/modprobe.d -p wa -k modprobe
```

Отслеживание использования **KExec**:

```
auditctl -a always,exit -F arch=b64 -S kexec_load -k KEXEC
auditctl -a always,exit -F arch=b32 -S sys_kexec_load -k KEXEC
```

Отслеживание использования специальных файлов (утилита **mknod**):

```
auditctl -a always,exit -F arch=b32 -S mknod -S mknodat -k specialfiles
auditctl -a always,exit -F arch=b64 -S mknod -S mknodat -k specialfiles
```

Отслеживание использования утилиты **mount**:

```
auditctl -a always,exit -F arch=b64 -S mount -S umount2 -F auid!=-1 -k mount
auditctl -a always,exit -F arch=b32 -S mount -S umount -S umount2 -F auid!=-1 -k mount
```

Отслеживание использования утилиты **swap**:

```
auditctl -a always,exit -F arch=b64 -S swapon -S swapoff -F auid!=-1 -k swap
auditctl -a always,exit -F arch=b32 -S swapon -S swapoff -F auid!=-1 -k swap
```

Отслеживание изменения времени:

```
auditctl -a always,exit -F arch=b32 -F uid!=ntp -S adjtimex -S settimeofday -S clock_settime -k time
auditctl -a always,exit -F arch=b64 -F uid!=ntp -S adjtimex -S settimeofday -S clock_settime -k time
```

Отслеживание изменения локального времени:

```
auditctl -w /etc/localtime -p wa -k localtime
```

Отслеживание использования утилиты **stunnel**:

```
auditctl -w /usr/sbin/stunnel -p x -k stunnel
auditctl -w /usr/bin/stunnel -p x -k stunnel
```

Отслеживание изменения файлов конфигурации **cron** и запланированных заданий:

```
auditctl -w /etc/cron.allow -p wa -k cron
auditctl -w /etc/cron.deny -p wa -k cron
auditctl -w /etc/cron.d/ -p wa -k cron
auditctl -w /etc/cron.daily/ -p wa -k cron
```

```
auditctl -w /etc/cron.hourly/ -p wa -k cron
auditctl -w /etc/cron.monthly/ -p wa -k cron
auditctl -w /etc/cron.weekly/ -p wa -k cron
auditctl -w /etc/crontab -p wa -k cron
auditctl -w /var/spool/cron/ -k cron
```

Отслеживание изменения баз пользователей, групп, паролей:

```
auditctl -w /etc/group -p wa -k etcgroup
auditctl -w /etc/passwd -p wa -k etcpasswd
auditctl -w /etc/gshadow -k etcgroup
auditctl -w /etc/shadow -k etcpasswd
auditctl -w /etc/security/opasswd -k opasswd
```

Отслеживание изменения файлов **sudo**:

```
auditctl -w /etc/sudoers -p wa -k actions
auditctl -w /etc/sudoers.d/ -p wa -k actions
```

Отслеживание использования **passwd**:

```
auditctl -w /usr/bin/passwd -p x -k passwd_modification
```

Отслеживание использования инструментов изменения идентификаторов группы:

```
auditctl -w /usr/sbin/groupadd -p x -k group_modification
auditctl -w /usr/sbin/groupmod -p x -k group_modification
auditctl -w /usr/sbin/addgroup -p x -k group_modification
auditctl -w /usr/sbin/useradd -p x -k user_modification
auditctl -w /usr/sbin/userdel -p x -k user_modification
auditctl -w /usr/sbin/usermod -p x -k user_modification
auditctl -w /usr/sbin/adduser -p x -k user_modification
```

Отслеживание изменения информации и конфигурации **login**:

```
auditctl -w /etc/login.defs -p wa -k login
auditctl -w /etc/securetty -p wa -k login
auditctl -w /var/log/faillog -p wa -k login
auditctl -w /var/log/lastlog -p wa -k login
auditctl -w /var/log/tallylog -p wa -k login
```

Правила сетевого окружения

Отслеживание изменения **hostname**:

```
auditctl -a always,exit -F arch=b32 -S sethostname -S setdomainname -k network_modifications
auditctl -a always,exit -F arch=b64 -S sethostname -S setdomainname -k network_modifications
```

Отслеживание удачных попыток подключения **IPv4**:

```
auditctl -a always,exit -F arch=b64 -S connect -F a2=16 -F success=1 -F key=network_connect_4
auditctl -a always,exit -F arch=b32 -S connect -F a2=16 -F success=1 -F key=network_connect_4
```

Отслеживание удачных попыток подключения **IPv6**:

```
auditctl -a always,exit -F arch=b64 -S connect -F a2=28 -F success=1 -F key=network_connect_6
auditctl -a always,exit -F arch=b32 -S connect -F a2=28 -F success=1 -F key=network_connect_6
```

Отслеживание изменения файлов конфигурации сетевых настроек:

```
auditctl -w /etc/hosts -p wa -k network_modifications
auditctl -w /etc/sysconfig/network -p wa -k network_modifications
auditctl -w /etc/sysconfig/network-scripts -p w -k network_modifications
auditctl -w /etc/network/ -p wa -k network
auditctl -a always,exit -F dir=/etc/NetworkManager/ -F perm=wa -k network_modifications
```

Отслеживание изменения файлов **issue**:

```
auditctl -w /etc/issue -p wa -k etcissue
auditctl -w /etc/issue.net -p wa -k etcissue
```

Отслеживание изменения скриптов при запуске ОС:

```
auditctl -w /etc/inittab -p wa -k init
auditctl -w /etc/init.d/ -p wa -k init
auditctl -w /etc/init/ -p wa -k init
```

Отслеживание изменения файлов **libpath**:

```
auditctl -w /etc/ld.so.conf -p wa -k libpath
auditctl -w /etc/ld.so.conf.d -p wa -k libpath
```

Отслеживание изменения предварительной загрузки общесистемной библиотеки (**LD_PRELOAD**):

```
auditctl -w /etc/ld.so.preload -p wa -k systemwide_preloads
```

Отслеживание изменения конфигурации **PAM** и связанных с ним файлов:

```
auditctl -w /etc/pam.d/ -p wa -k pam
auditctl -w /etc/security/limits.conf -p wa -k pam
auditctl -w /etc/security/limits.d -p wa -k pam
auditctl -w /etc/security/pam_env.conf -p wa -k pam
auditctl -w /etc/security/namespace.conf -p wa -k pam
auditctl -w /etc/security/namespace.d -p wa -k pam
auditctl -w /etc/security/namespace.init -p wa -k pam
```

Отслеживание изменения конфигурации **mail**:

```
auditctl -w /etc/aliases -p wa -k mail
auditctl -w /etc/postfix/ -p wa -k mail
auditctl -w /etc/exim4/ -p wa -k mail
```

Отслеживание изменения конфигурации **ssh**:

```
auditctl -w /etc/ssh/sshd_config -k sshd
auditctl -w /etc/ssh/sshd_config.d -k sshd
```

Отслеживание изменения подделки ключа **ssh**:

```
auditctl -w /root/.ssh -p wa -k rootkey
```

Правила служб

Отслеживание изменения и использования файлов **systemd**:

```
auditctl -w /bin/systemctl -p x -k systemd
auditctl -w /etc/systemd/ -p wa -k systemd
auditctl -w /usr/lib/systemd -p wa -k systemd
```

Отслеживание событий **SELinux**, которые изменяют систему мандатного управления доступом:

```
auditctl -w /etc/selinux/ -p wa -k mac_policy
```

Отслеживание событий сбоя доступа к критическим элементам:

```
auditctl -a always,exit -F arch=b64 -S open -F dir=/etc -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/bin -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/sbin -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/usr/bin -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/usr/sbin -F success=0 -k unauthedfileaccess
```

```
auditctl -a always,exit -F arch=b64 -S open -F dir=/var -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/home -F success=0 -k unauthedfileaccess
auditctl -a always,exit -F arch=b64 -S open -F dir=/srv -F success=0 -k unauthedfileaccess
```

Отслеживание использования приложений для изменения идентификатора процесса (переключение учетных записей):

```
auditctl -w /bin/su -p x -k priv_esc
auditctl -w /usr/bin/sudo -p x -k priv_esc
auditctl -w /etc/sudoers -p rw -k priv_esc
auditctl -w /etc/sudoers.d -p rw -k priv_esc
```

Отслеживание использования приложений, изменяющих состояние питания:

```
auditctl -w /sbin/shutdown -p x -k power
auditctl -w /sbin/poweroff -p x -k power
auditctl -w /sbin/reboot -p x -k power
auditctl -w /sbin/halt -p x -k power
```

Отслеживание изменения информации об инициации сеанса:

```
auditctl -w /var/run/utmp -p wa -k session
auditctl -w /var/log/btmp -p wa -k session
auditctl -w /var/log/wtmp -p wa -k session
```

Отслеживание модификации дискреционного контроля доступа:

```
auditctl -a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=-1 -k perm_mod
auditctl -a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=-1 -k perm_mod
```

Специальные правила

Отслеживание запросов на получение информации о пользователе:

```
auditctl -w /usr/bin/whoami -p x -k recon
auditctl -w /usr/bin/id -p x -k recon
auditctl -w /bin/hostname -p x -k recon
auditctl -w /bin/uname -p x -k recon
auditctl -w /etc/issue -p r -k recon
auditctl -w /etc/hostname -p r -k recon
```

Отслеживание подозрительной деятельности:

```
### Подразумевается, что использование специализированных утилит, связанных с работой с/в
```

```
### внутренней/внешней сетью, может быть отслежено и зажурналировано.
auditctl -w /usr/bin/wget -p x -k susp_activity
auditctl -w /usr/bin/curl -p x -k susp_activity
auditctl -w /usr/bin/base64 -p x -k susp_activity
auditctl -w /bin/nc -p x -k susp_activity
auditctl -w /bin/netcat -p x -k susp_activity
auditctl -w /usr/bin/ncat -p x -k susp_activity
auditctl -w /usr/bin/ss -p x -k susp_activity
auditctl -w /usr/bin/netstat -p x -k susp_activity
auditctl -w /usr/bin/ssh -p x -k susp_activity
auditctl -w /usr/bin/scp -p x -k susp_activity
auditctl -w /usr/bin/sftp -p x -k susp_activity
auditctl -w /usr/bin/ftp -p x -k susp_activity
auditctl -w /usr/bin/socat -p x -k susp_activity
auditctl -w /usr/bin/wireshark -p x -k susp_activity
auditctl -w /usr/bin/tshark -p x -k susp_activity
auditctl -w /usr/bin/rawshark -p x -k susp_activity
auditctl -w /usr/bin/rdesktop -p x -k Remote_Access_Tools
auditctl -w /usr/local/bin/rdesktop -p x -k Remote_Access_Tools
auditctl -w /usr/bin/wlfreerdp -p x -k susp_activity
auditctl -w /usr/bin/xfreerdp -p x -k Remote_Access_Tools
auditctl -w /usr/local/bin/xfreerdp -p x -k Remote_Access_Tools
auditctl -w /usr/bin/nmap -p x -k susp_activity
```

Отслеживание использования утилит архивации и сжатия данных:

```
auditctl -w /usr/bin/zip -p x -k Data_Compressed
auditctl -w /usr/bin/gzip -p x -k Data_Compressed
auditctl -w /usr/bin/tar -p x -k Data_Compressed
auditctl -w /usr/bin/bzip2 -p x -k Data_Compressed
auditctl -w /usr/bin/lzip -p x -k Data_Compressed
auditctl -w /usr/local/bin/lzip -p x -k Data_Compressed
auditctl -w /usr/bin/lz4 -p x -k Data_Compressed
auditctl -w /usr/local/bin/lz4 -p x -k Data_Compressed
auditctl -w /usr/bin/lzop -p x -k Data_Compressed
auditctl -w /usr/local/bin/lzop -p x -k Data_Compressed
auditctl -w /usr/bin/plzip -p x -k Data_Compressed
auditctl -w /usr/local/bin/plzip -p x -k Data_Compressed
auditctl -w /usr/bin/pbzip2 -p x -k Data_Compressed
auditctl -w /usr/local/bin/pbzip2 -p x -k Data_Compressed
auditctl -w /usr/bin/lbzip2 -p x -k Data_Compressed
auditctl -w /usr/local/bin/lbzip2 -p x -k Data_Compressed
auditctl -w /usr/bin/pixz -p x -k Data_Compressed
auditctl -w /usr/local/bin/pixz -p x -k Data_Compressed
auditctl -w /usr/bin/pigz -p x -k Data_Compressed
auditctl -w /usr/local/bin/pigz -p x -k Data_Compressed
auditctl -w /usr/bin/unpigz -p x -k Data_Compressed
auditctl -w /usr/local/bin/unpigz -p x -k Data_Compressed
auditctl -w /usr/bin/zstd -p x -k Data_Compressed
auditctl -w /usr/local/bin/zstd -p x -k Data_Compressed
```

Отслеживание подозрительной активности в **sbin**:

```
### Подразумевается, что использование специализированных утилит  может быть отслежено и
### зажурналировано.
auditctl -w /sbin/iptables -p x -k sbin_susp
auditctl -w /sbin/ip6tables -p x -k sbin_susp
auditctl -w /sbin/ifconfig -p x -k sbin_susp
auditctl -w /usr/sbin/arptables -p x -k sbin_susp
auditctl -w /usr/sbin/ebtables -p x -k sbin_susp
auditctl -w /sbin/xtables-nft-multi -p x -k sbin_susp
auditctl -w /usr/sbin/nft -p x -k sbin_susp
auditctl -w /usr/sbin/tcpdump -p x -k sbin_susp
auditctl -w /usr/sbin/traceroute -p x -k sbin_susp
auditctl -w /usr/sbin/ufw -p x -k sbin_susp
```

Отслеживание отправки вызовов **dbus**:

```
### Может указывать на повышение привилегий CVE-2021-3560
auditctl -w /usr/bin/dbus-send -p x -k dbus_send
auditctl -w /usr/bin/gdbus -p x -k gdubs_call
```

Отслеживание вызовов **pkexec**:

```
### Может указывать на повышение привилегий CVE-2021-4034
auditctl -w /usr/bin/pkexec -p x -k pkexec
```

Отслеживание подозрительной активности, связанной с **shell**:

```
auditctl -w /bin/ash -p x -k susp_shell
auditctl -w /bin/bash -p x -k susp_shell
auditctl -w /bin/csh -p x -k susp_shell
auditctl -w /bin/dash -p x -k susp_shell
auditctl -w /bin/busybox -p x -k susp_shell
auditctl -w /bin/ksh -p x -k susp_shell
auditctl -w /bin/fish -p x -k susp_shell
auditctl -w /bin/tcsh -p x -k susp_shell
auditctl -w /bin/tclsh -p x -k susp_shell
auditctl -w /bin/zsh -p x -k susp_shell
auditctl -w /bin/xonsh -p x -k susp_shell
auditctl -w /usr/local/bin/xonsh -p x -k susp_shell
auditctl -w /bin/open -p x -k susp_shell
auditctl -w /bin/sh -p x -k susp_shell
auditctl -w /bin/rbash -p x -k susp_shell
```

Отслеживание изменения конфигурации **Shell/profile configurations**:

```
auditctl -w /etc/profile.d/ -p wa -k shell_profiles
auditctl -w /etc/profile -p wa -k shell_profiles
auditctl -w /etc/shells -p wa -k shell_profiles
auditctl -w /etc/bashrc -p wa -k shell_profiles
auditctl -w /etc/csh.cshrc -p wa -k shell_profiles
auditctl -w /etc/csh.login -p wa -k shell_profiles
auditctl -w /etc/fish/ -p wa -k shell_profiles
auditctl -w /etc/zsh/ -p wa -k shell_profiles
```

Отслеживание злоупотребления привилегиями:

```
### Целью этого правила является обнаружение случаев, когда администратор злоупотребляет полномочиями,
### путем просмотра домашнего каталога пользователя.
auditctl -a always,exit -F dir=/home -F uid=0 -F auid>=1000 -F auid!=-1 -C auid!=obj_uid -k power_abuse
```

Отслеживание создания сокетов:

```
### Отслеживает как IPv4, так и IPv6
auditctl -a always,exit -F arch=b32 -S socket -F a0=2  -k Exfiltration_Over_Other_Network_Medium
auditctl -a always,exit -F arch=b64 -S socket -F a0=2  -k Exfiltration_Over_Other_Network_Medium
auditctl -a always,exit -F arch=b32 -S socket -F a0=10 -k Exfiltration_Over_Other_Network_Medium
auditctl -a always,exit -F arch=b64 -S socket -F a0=10 -k Exfiltration_Over_Other_Network_Medium
```

Отслеживание создания анонимного файла:

```
### Эти правила следят за использованием memfd_create, "memfd_create" создает анонимный файл и возвращает
### дескриптор файла для доступа к нему
auditctl -a always,exit -F arch=b64 -S memfd_create -F key=anon_file_create
auditctl -a always,exit -F arch=b32 -S memfd_create -F key=anon_file_create
```

Правила управления ПО

Отслеживание использования **rpm/yum**:

```
auditctl -w /usr/bin/rpm -p x -k software_mgmt
auditctl -w /usr/bin/yum -p x -k software_mgmt
```

Отслеживание использования **dnf**:

```
auditctl -w /usr/bin/dnf -p x -k software_mgmt
```

Отслеживание использования **pip**:

```
auditctl -w /usr/bin/pip -p x -k third_party_software
auditctl -w /usr/local/bin/pip -p x -k third_party_software
auditctl -w /usr/bin/pip3 -p x -k third_party_software
auditctl -w /usr/local/bin/pip3 -p x -k third_party_software
```

Отслеживание использования **npm**:

```
auditctl -w /usr/bin/npm -p x -k third_party_software
```

Отслеживание использования **CPAN** (*Comprehensive Perl Archive Network*):

```
auditctl -w /usr/bin/cpan -p x -k third_party_software
```

Отслеживание использования **ruby** (*RubyGems*):

```
auditctl -w /usr/bin/gem -p x -k third_party_software
```

Отслеживание использования **Lua**:

```
auditctl -w /usr/bin/luarocks -p x -k third_party_software
```

Правила управления специальным ПО

Отслеживание изменений файлов **puppet**:

```
auditctl -w /etc/puppet/ssl -p wa -k puppet_ssl
```

Отслеживание изменений файлов **chef**:

```
auditctl -w /etc/chef -p wa -k soft_chef
```

Отслеживание изменений файлов **otter**:

```
auditctl -w /etc/otter -p wa -k soft_otter
```

Отслеживание использования утилиты **grep**:

```
auditctl -w /usr/bin/grep -p x -k T1081_Credentials_In_Files
auditctl -w /usr/bin/egrep -p x -k T1081_Credentials_In_Files
auditctl -w /usr/bin/ugrep -p x -k T1081_Credentials_In_Files
```

Отслеживание использования и изменения файлов конфигурации **docker**:

```
auditctl -w /usr/bin/dockerd -k docker
auditctl -w /usr/bin/docker -k docker
auditctl -w /usr/bin/docker-containerd -k docker
auditctl -w /usr/bin/docker-runc -k docker
auditctl -w /var/lib/docker -k docker
auditctl -w /etc/docker -k docker
auditctl -w /etc/sysconfig/docker -k docker
auditctl -w /etc/sysconfig/docker-storage -k docker
auditctl -w /usr/lib/systemd/system/docker.service -k docker
auditctl -w /usr/lib/systemd/system/docker.socket -k docker
```

Отслеживание использования систем виртуализации:

```
auditctl -w /usr/bin/qemu-system-x86_64 -p x -k qemu-system-x86_64
auditctl -w /usr/bin/qemu-img -p x -k qemu-img
auditctl -w /usr/bin/qemu-kvm -p x -k qemu-kvm
auditctl -w /usr/bin/qemu -p x -k qemu
auditctl -w /usr/bin/virtualbox -p x -k virtualbox
```

```
auditctl -w /usr/bin/virt-manager -p x -k virt-manager
auditctl -w /usr/bin/VBoxManage -p x -k VBoxManage
```

Отслеживание использования утилиты **kubelet** (*Kubernetes*):

```
auditctl -w /usr/bin/kubelet -k kubelet
```

«Тяжелые» события

> **Примечание.**
>
> Правила, представленные ниже, требуют большого объема свободного пространства в среде.

Отслеживание применения команд с правами пользователя **root**:

```
auditctl -a always,exit -F arch=b64 -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k rootcmd
auditctl -a always,exit -F arch=b32 -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k rootcmd
```

Отслеживание события удаления файлов пользователем:

```
auditctl -a always,exit -F arch=b32 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=-1 -k delete
auditctl -a always,exit -F arch=b64 -S rmdir -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=-1 -k delete
```

Отслеживание события неудачного доступа к файлу:

```
auditctl -a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
auditctl -a always,exit -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access
auditctl -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
auditctl -a always,exit -F arch=b64 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access
```

Отслеживание события неудачного создания:

```
auditctl -a always,exit -F arch=b32 -S creat,link,mknod,mkdir,symlink,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
auditctl -a always,exit -F arch=b64 -S mkdir,creat,link,symlink,mknod,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
auditctl -a always,exit -F arch=b32 -S link,mkdir,symlink,mkdirat -F exit=-EPERM -k file_creation
auditctl -a always,exit -F arch=b64 -S mkdir,link,symlink,mkdirat -F exit=-EPERM -k file_creation
```

Отслеживание события неудачной модификации:

```
auditctl -a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
auditctl -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
auditctl -a always,exit -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
auditctl -a always,exit -F arch=b64 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
```

Отслеживание события использования 32-битного API для 64-битной системы:

```
### Это правило обнаружит любое использование 32-битных системных вызовов, потому как это может быть
### признаком использования уязвимости 32-битного API.
auditctl -a always,exit -F arch=b32 -S all -k 32bit_api
```

Утилита aureport

Утилита **aureport** - это инструмент, который генерирует итоговые отчеты на основе логов службы аудита. **aureport** может также принимать данные со стандартного ввода (*stdin*) до тех пор, пока на входе будут необработанные данные логов. В шапке каждого

отчета для каждого столбца есть заголовок - это облегчает понимание данных. Все отчеты, кроме основного итогового отчета, содержат номера событий аудита. Используя их, вы можете найти полные данные о событии с помощью **ausearch -a** . Если в отчете слишком много данных, можно задать время начала и время окончания для уточнения временного промежутка. Отчеты, генерируемые **aureport**, могут быть использованы как исходный материал для получения более развернутых отчетов.

Опции:

Опция	Значение опции
-au, --auth	Отчет обо всех попытках аутентификации.
-a, --avc	Отчет обо всех avc сообщениях.
-c, --config	Отчет об изменениях конфигурации.
-cr, --crypto	Отчет о событиях, связанных с шифрованием.
-e, --event	Отчет о событиях.
-f, --file	Отчет о файлах.
--failed	Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются и удачные, и неудачные события.
-h, --host	Отчет о хостах.
-i, --interpret	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен aureport. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, --input файл	Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-l, --login	Отчет о попытках входа в систему.
-m, --mods	Отчет об изменениях пользовательских учетных записей.
-ma, --mac	Отчет о событиях в системе, обеспечивающей мандатное управление доступом - Mandatory Access Control (MAC).
-p, --pid	Отчет о процессах.
-r, --response	Отчет о реакциях на аномальные события.
-s, --syscall	Отчеты о системных вызовах.
--success	Для обработки в отчетах выбирать только удачные события. По умолчанию показываются и удачные, и неудачные события.
--summary	Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете. Такой режим есть не у всех отчетов.
-t, --log	Этот параметр генерирует отчет о временных рамках каждого отчета.
-te, --end	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается текущий момент (now). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, --terminal	Отчет о терминалах.
-ts, --start	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается полночь (midnight). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-u, --user	Отчет о пользователях.
-v, --version	Вывести версию программы и выйти.

Утилита ausearch

Программа **ausearch** является инструментом поиска по журналу аудита. Утилита **ausearch** может также принимать данные со стандартного ввода (*stdin*) до тех пор, пока на входе будут необработанные данные логов. Все условия, указанные в параметрах, объединяются логическим «**И**». К примеру, при указании **- m** и **-ui** в качестве параметров будут показаны события, соответствующие заданному типу и идентификатору пользователя.

Стоит отметить, что каждый системный вызов ядра из пользовательского пространства и возвращение данных в пользовательское

пространство имеет один уникальный (для каждого системного вызова) идентификатор события.

Различные части ядра могут добавлять дополнительные записи. Например, в событие аудита для системного вызова «**open**» добавляется запись *PATH* с именем файла. **ausearch** показывает все записи события вместе. Это означает, что при запросе определенных записей результат может содержать записи *SYSCALL*.

Также помните, что не все типы записей содержат указанную информацию. Например, запись *PATH* не содержит имя узла или *loginuid*.

Опции:

Опция	Значение опции
-a, --event audit-event-id	Искать события с заданным идентификатором события. Сообщения обычно начинаются примерно так: msg=audit(1116360555.329:2401771). Идентификатор события - это число после «:». Все события аудита, связанные с одним системным вызовом имеют одинаковый идентификатор.
-c, --comm comm-name	Искать события с заданным comm name. comm name - имя исполняемого файла задачи.
-f, --file file-name	Искать события с заданным именем файла.
-ga, --gid-all all-group-id	Искать события с заданным эффективным или обычным идентификатором группы.
-ge, --gid-effective effective-group-id	Искать события с заданным эффективным идентификатором группы или именем группы.
-gi, --gidgroup-id	Искать события с заданным идентификатором группы или именем группы.
-h, --help	Справка.
-hn, --host host-name	Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен ausearch. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, --input file-name	Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов.
-k, --key key-string	Искать события с заданным ключевым словом.
-m, --message message-type | comma-sep-message-type-list	Искать события с заданным типом. Вы можете указать список значений, разделенных запятыми. Можно указать несуществующий в событиях тип ALL, который позволяет получить все сообщения системы аудита. Список допустимых типов большой и будет показан, если указать эту опцию без значения. Тип сообщения может быть строкой или числом. В списке значений этого параметра в качестве разделителя используются запятые и пробелы недопустимы.
-o, --object SE-Linux-context-string	Искать события с заданным контекстом (объектом).
-p, --pid process-id	Искать события с заданным идентификатором процесса.
-pp, --ppid parent-process-id	Искать события с заданным идентификатором родительского процесса.
-r, --raw	Необработанный вывод. Используется для извлечения записей для дальнейшего анализа.
-sc, --success syscall-name-or-value	Искать события с заданным системным вызовом. Вы можете указать его номер или имя. Если вы указали имя, оно будет проверено на машине, где запущен ausearch.
-se, --context SE-Linux-context-string	Искать события с заданным контекстом SELinux (stcontext/subject или tcontext/object).
-su, --subject SE-Linux-context-string	Искать события с заданным контекстом SELinux - scontext (subject).
-sv, --success success-value	Искать события с заданным флагом успешного выполнения. Допустимые значения: yes (успешно) и no(неудачно).
-te, --end [end-date] [end-time]	Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается текущий момент (now). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. localtime). this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-ts, --start [start-date] [start-time]	Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается полночь (midnight). Используйте 24-часовую нотацию времени, а не AM/PM. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00. Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.
-tm, --terminal terminal	Искать события с заданным терминалом. Некоторые службы (такие как cron и atd) используют имя службы как имя терминала.
-ua, --uid-all all-user-id	Искать события, у которых любой из идентификатора пользователя, эффективного идентификатора пользователя или loginuid (auid) совпадают с заданным идентификатором пользователя.

Опция	Значение опции
-ue, --uid-effective effective-user-id	Искать события с заданным эффективным идентификатором пользователя.
-ui, --uid user-id	Искать события с заданным идентификатором пользователя.
-ul, --loginuid login-id	Искать события с заданным идентификатором пользователя. Все программы, которые его используют, должны использовать pam_loginuid.
-v, --verbose	Показать версию и выйти.
-w, --word	Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux.
-x, --executable executable	Искать события с заданным именем исполняемой программы.

Утилита autrace

Утилита **autrace** - это программа, которая добавляет правила аудита для того, чтобы следить за использованием системных вызовов в указанном процессе подобно тому, как это делает **strace**. После добавления правил она запускает процесс с указанными аргументами. Результаты аудита будут либо в логах аудита (если служба аудита запущена), либо в системных логах. Внутри **autrace** устроена так, что удаляет все предыдущие правила аудита, перед тем как запустить указанный процесс и после его завершения. Поэтому, в качестве дополнительной меры предосторожности, программа не запустится, если перед ее использованием правила не будут удалены с помощью **audtictl** - предупреждающее сообщение известит об этом.

Опции:

Опция	Значение опции
-r	Ограничить сбор информации о системных вызовах только теми, которые необходимы для анализа использования ресурсов. Это может быть полезно при моделировании внештатных ситуаций, к тому же позволяет уменьшить нагрузку на логи.

Примеры:

Ниже представлен пример обычного использования программы:

```
autrace /bin/ls /tmp
ausearch --start recent -p 2442 -i
```

Еще один пример для режима ограниченного сбора информации:

```
autrace -r /bin/ls
ausearch --start recent -p 2450 --raw | aureport --file –summary
ausearch --start recent -p 2450 --raw | aureport --host –summary
```

Расчет контрольных сумм файлов

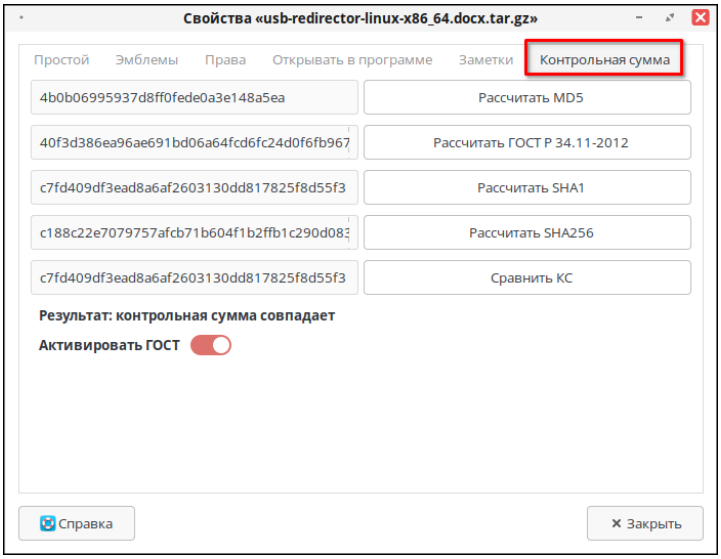
Контрольная сумма (**КС**) вычисляется на основе содержимого файла и уникальна для каждого файла. Даже небольшое изменение в файле приведет к значительному изменению контрольной суммы.

Контрольные суммы выполняют **две основные задачи**:

1. **Проверка корректности загрузки.** При загрузке больших файлов всегда есть риск получить поврежденный файл из-за ошибок в процессе передачи. **КС** позволяют проверить, был ли файл загружен корректно, сравнивая вычисленную контрольную сумму загруженного файла с контрольной суммой оригинала.

2. **Обнаружение несанкционированных изменений. КС** также могут использоваться для обнаружения любых несанкционированных изменений в файле, которые могут быть внесены злоумышленниками. Если контрольная сумма файла изменилась, это может указывать на то, что файл был изменен, и его содержимое больше не является оригинальным.

Для расчета и сравнения контрольных сумм файлов необходимо нажать ПКМ на файл, выбрать пункт «**Свойства**» и перейти на вкладку «**Контрольная сумма**». После чего вы можете выбрать один из алгоритмов вычисления контрольных сумм, а затем сравнить **КС**.



Обратите внимание, что расчет контрольных сумм по **ГОСТ** производится при включенной функции «**Активировать ГОСТ**» и настроенном **openssl-gost-engine**.

В графической оболочке **GNOME** не поддерживается встроенный расчет контрольных сумм файлов в свойствах файла. Чтобы вычислить контрольную сумму файла в **GNOME**, используйте другие средства, такие как командная строка или сторонние утилиты.

Например, можно использовать команду **sha256sum** в терминале, чтобы вычислить контрольную сумму файла с использованием алгоритма **SHA-256**.

```
sha256sum <myfile>
```

где <myfile> - имя файла, контрольную сумму которого нужно вычислить.

Замкнутая программная среда

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: ima-manage-0.2-1, dracut-056-9

Для контроля целостности компонентов ОС используется **IMA**. Компонент архитектуры измерения целостности (**IMA**) производит проверки целостности во время выполнения файлов с использованием хэшей, сравнивая их со списком допустимых хэшей.

Примечание.

Работает, начиная с версии **ядра 5.15.78** из репозитория РЕД ОС.

Для проведения контроля целостности необходимо перейти в сеанс пользователя **root**:

```
su -
```

и выполнить следующие действия:

1. Установить пакеты для работы с **IMA**:

```
dnf install ima-manage openssl-gost-engine keyutils
```

2. Обновить пакет **dracut**:

```
dnf update dracut
```

ВАЖНО!

Для корректного осуществления контроля целостности компонентов ОС необходимо, чтобы в системе были установлены актуальные версии пакетов - **dracut** версии **056-6 и выше**, **ima-manage** версии **0.2-1 и выше**.

3. Включить ГОСТ в **openssl**:

```
openssl-switch-config gost
```

4. Сгенерировать пару ключей.

а) Создать файл **test-ca.conf**:

```
nano test-ca.conf
```

В **test-ca.conf** добавить содержимое:

```
[ req ]
 distinguished_name = req_distinguished_name
 prompt = no
 string_mask = utf8only
 x509_extensions = v3_ca
 [ req_distinguished_name ]
 O = IMA-CA
 CN = IMA/EVM certificate signing key
 emailAddress = ca@ima-ca
 [ v3_ca ]
 basicConstraints=CA:TRUE
 subjectKeyIdentifier=hash
 authorityKeyIdentifier=keyid:always,issuer
```

Значения полей **O**, **CN**, **emailAddress** являются произвольными, можно заменить их на свои. Место расположения файла не играет роли, он нужен только для создания пары ключей один раз.

Для сохранения и выхода из текстового редактора **nano** использовать: `CTRL + O` -> `Enter` -> `Ctrl + X`.

б) Сгенерировать приватный ключ:

```
openssl genpkey -algorithm gost2012_512 -pkeyopt paramset:A -out privkey_evm.pem
```

в) Создать запрос:

```
openssl req -new -config test-ca.conf -md_gost12_512 -key privkey_evm.pem -out cert.req
```

г) Отправить файл запроса в Техническую поддержку РЕД СОФТ. Получить публичный ключ (например, **x509_evm.der**). В случае получения сертификата в **CRT**-формате, его можно перевести в формат **DER** следующим образом:

```
openssl x509 -outform der -in pub.crt -out x509_evm.der
```

5. Создать папку **/etc/keys/ima/** и скопировать в нее открытый ключ **x509_evm.der**.

```
mkdir /etc/keys/ima/
cp x509_evm.der /etc/keys/ima/x509_evm.der
```

Секретный ключ «**privkey_evm.pem**» сохранить в каталоге, недоступном для всех пользователей, кроме администратора **root**, например:

```
mv privkey_evm.pem /root/privkey_evm.pem
```

6. Запустить утилиту **ima-manage** с ключом **init**:

```
ima-manage init
```

7. В файле **/etc/ima-manage.conf** изменить значение **HASHALGO="sha256"** на **HASHALGO="streebog512"**.

ВАЖНО!

Значение битности параметра **HASHALGO** должно совпадать с битностью сгенерированных ключей. Например, если приватный ключ был сгенерирован с параметром **gost2012_256**, то значение параметра **HASHALGO** в таком случае будет равен **streebog256**.

8. Запустить утилиту «**ima-manage**» с ключом «**signfs**» и указанием пути размещения секретного ключа:

```
ima-manage signfs /root/privkey_evm.pem
```

9. Запустить утилиту **ima-manage** с ключом «**enforce**»:

```
ima-manage enforce
```

Дождаться завершения работы утилиты и предложения перезагрузки. Дать согласие на перезагрузку системы.

Примечание.

После обновления/редактирования файлов, которые ранее были подписаны **IMA**, их рекомендуется **переподписать**, выполнив действия, указанные в *п. 8-9*.

В противном случае корректное поведение системы при следующем запуске **не гарантируется**.

Для проверки работы защиты от запуска неподписанных исполняемых файлов создайте копию существующего исполняемого файла, например:

```
cp /bin/ls ls.copy
```

Попробуйте его запустить, будет выведена ошибка:

```
./ls.copy

bash: ./ls.copy: Permission denied
```

При этом в логе аудита появится запись о запрете запуска неподписанного файла:

```
grep -i ima /var/log/audit/audit.log | tail -n 1

type=INTEGRITY_DATA msg=audit(1638974599.231:11315): pid=2800 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op=appraise_data cause=IMA-signature-required comm="bash"
name="/home/user/ls.copy" dev="dm-0" ino=946370 res=0 errno=0UID="user" AUID="user"
```

Для запуска сторонних файлов, не имеющих подписи, необходимо **от имени администратора** подписать файл:

```
evmctl ima_sign --hashalgo md_gost12_512 --key <путь_к_приватному_ключу_privkey_evm.pem> <путь_к_файлу>
```

Например:

```
evmctl ima_sign --hashalgo md_gost12_512 --key /root/privkey_evm.pem /home/user/ls.copy
```

Для включения режима журналирования (система не будет запрещать запуск неподписанных файлов, но будет записывать попытки их запуска) необходимо в файле **/etc/default/grub** изменить параметр **ima_appraise=enforce** на **ima_appraise=log**.

После этого обновите конфигурацию загрузчика ОС, для этого выполните в терминале команду:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Проверка контрольной суммы ISO-образа

Проверка контрольных сумм через файловый менеджер caja
Проверка контрольных сумм через файловый менеджер dolphin
Проверка контрольных сумм через Double Commander
Проверка при помощи встроенных утилит
Проверка с помощью дополнительных утилит

Образ ISO представляет собой полную копию всего, что хранится на физическом оптическом диске, таком как *CD*, *DVD* или *Blu-ray*, включая собственную файловую систему.

Большинство операционных систем и многие «утилиты» также позволяют монтировать **образ ISO** как виртуальный диск. В этом случае, все приложения обрабатывают его таким же образом, как если бы это был реальный оптический диск, вставленный в привод персонального компьютера.

Контрольная сумма - некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении.

Контрольная сумма является результатом хеш-функции, используемой для вычисления контрольного кода — небольшого количества бит внутри большого блока данных, например, сетевого пакета или блока компьютерного файла, применяемого для обнаружения ошибок при передаче или хранении информации. Значение контрольной суммы добавляется в конец блока данных непосредственно перед началом передачи или записи данных на какой-либо носитель информации. Впоследствии оно проверяется для подтверждения целостности данных.

Популярность использования контрольных сумм для проверки целостности данных обусловлена тем, что подобная проверка просто реализуема в двоичном цифровом оборудовании, легко анализируется и хорошо подходит для обнаружения общих ошибок, вызванных наличием шума в каналах передачи данных.

Вы можете подробнее ознакомиться с возможностью проверки контрольной суммы iso-образа, просмотрев наши обучающие видео:

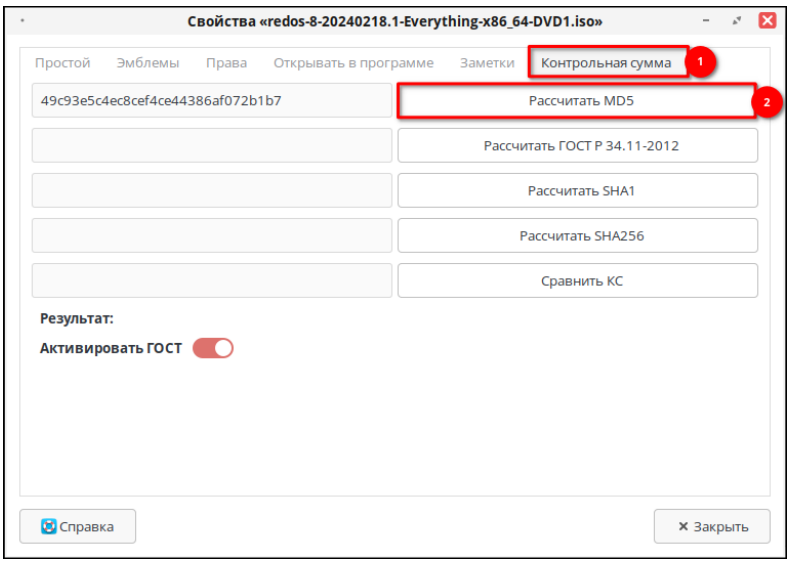
- на **RuTube** — Проверка контрольной суммы iso-образа;
- в **Яндекс.Дзен** — Проверка контрольной суммы iso-образа;
- в **VK Видео** — Проверка контрольной суммы iso-образа.

На наших каналах вы также сможете найти много другой полезной информации.

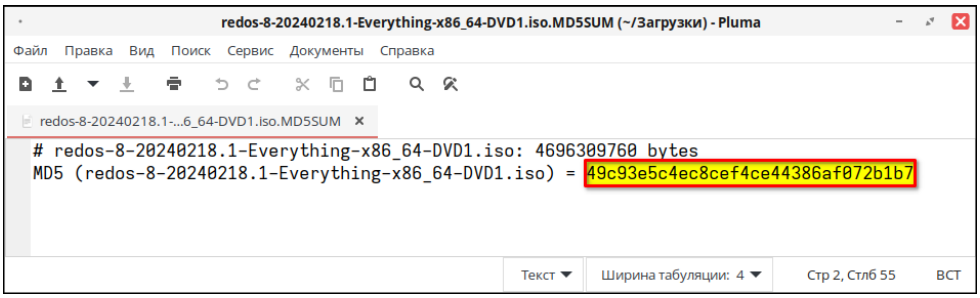
Проверка контрольных сумм через файловый менеджер caja

Для расчета контрольной суммы файла (хеш-суммы) через файловый менеджер **caja** необходимо выделить файл и нажать правую кнопку мыши. В контекстном меню выбрать пункт «**Свойства**» - «**Контрольная сумма**» (1).

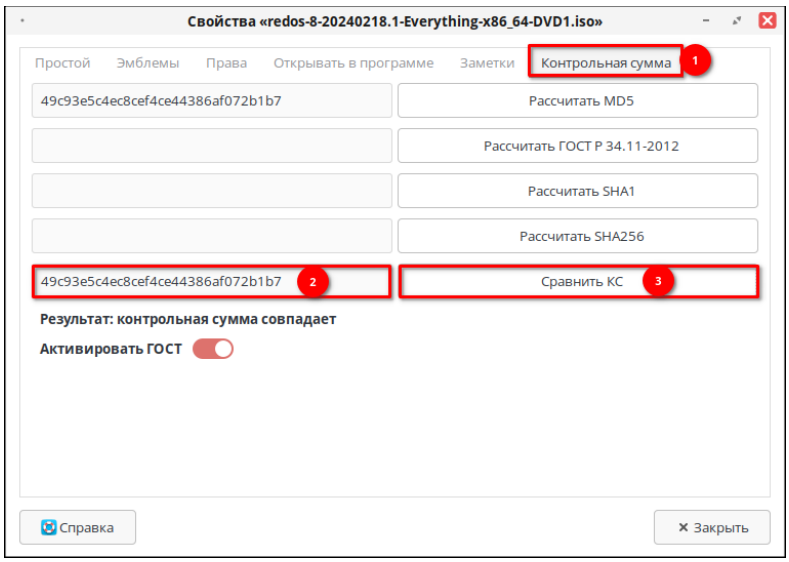
Далее требуется нажать кнопку «**Расчитать MD5**» (2).



На официальном сайте необходимо скачать файл с хеш-суммой. Из файла **redos-8-20240218.1-Everything-x86_64-DVD1.iso.MD5SUM** требуется скопировать эталонную хэш-сумму образа.



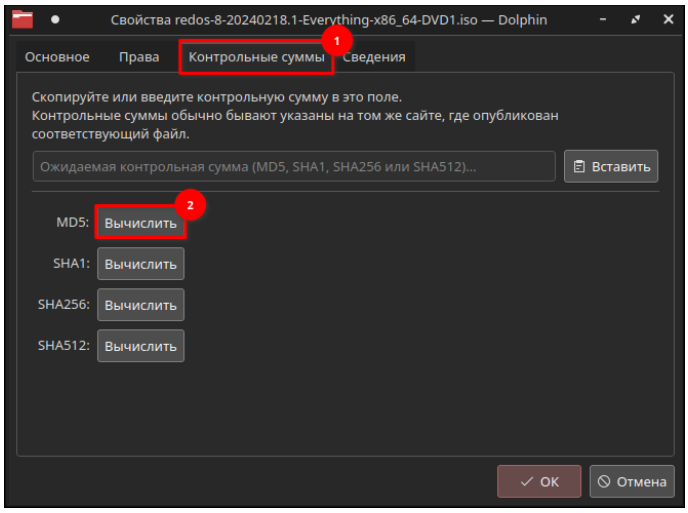
Далее перейти в пункт «**Свойства**» - «**Контрольная сумма**» (1), вставить хеш-сумму в поле (2) и нажать кнопку «**Сравнить КС**» (3).



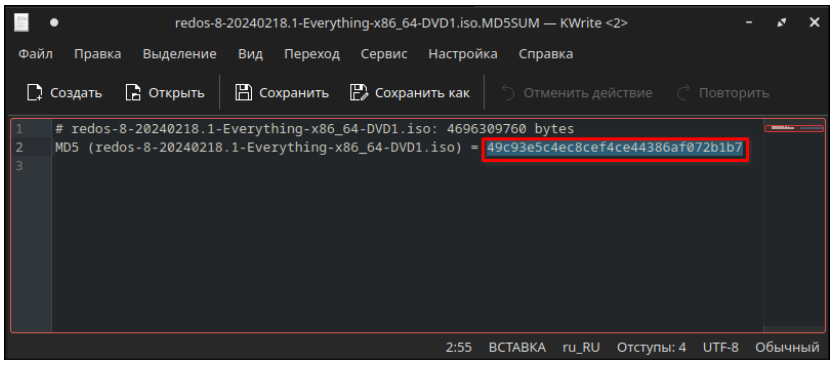
Проверка контрольных сумм через файловый менеджер dolphin

Для расчета контрольной суммы файла (хеш-суммы) через файловый менеджер **dolphin** необходимо выделить файл и нажать правую кнопку мыши. В контекстном меню выбрать пункт «**Свойства**» - «**Контрольные суммы**» (1).

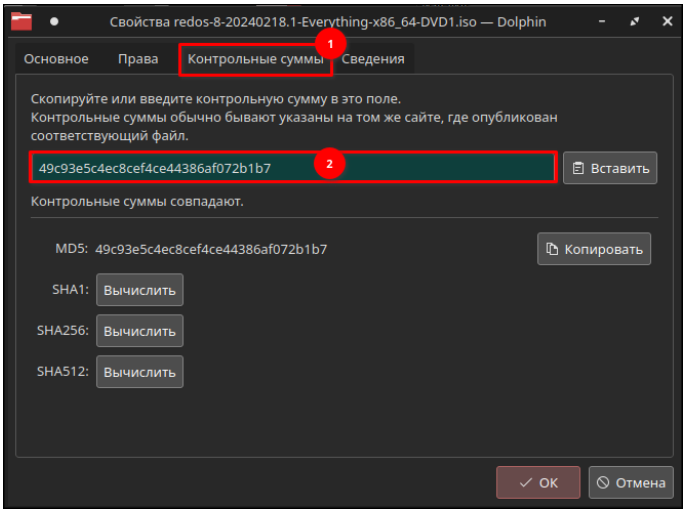
Далее требуется нажать кнопку рядом с пунктом MD5 «**Вычислить**» (2).



На официальном сайте необходимо скачать файл с хеш-суммой. Из файла **redos-8-20240218.1-Everything-x86_64-DVD1.iso.MD5SUM** требуется скопировать эталонную хэш-сумму образа.

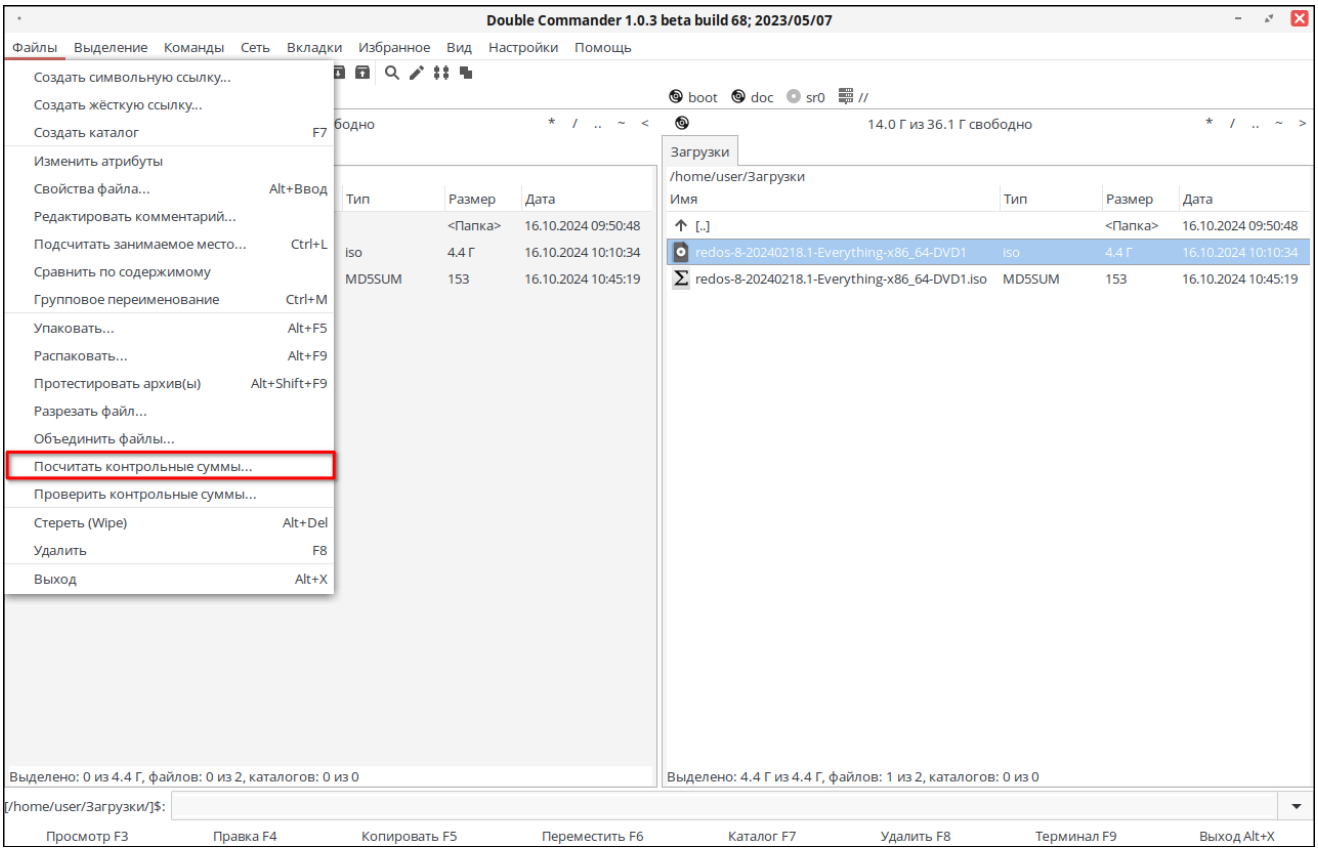


Далее перейти в пункт «**Свойства**» - «**Контрольные суммы**» (1), вставить хеш-сумму в поле для сравнения (2).

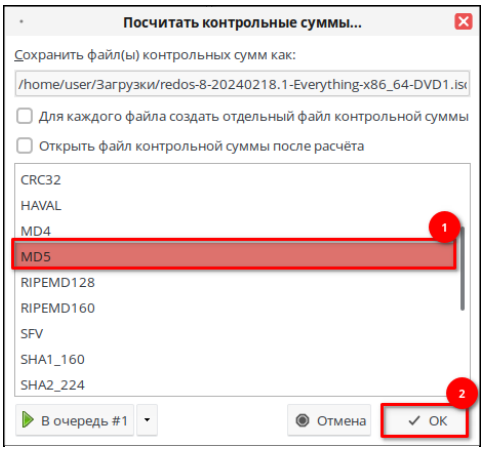


Проверка контрольных сумм через Double Commander

Для расчета контрольной суммы файла (хеш-суммы) через **Double Commander** необходимо выделить файлы и выбрать пункт меню «**Файлы**» - «**Посчитать контрольные суммы...**».

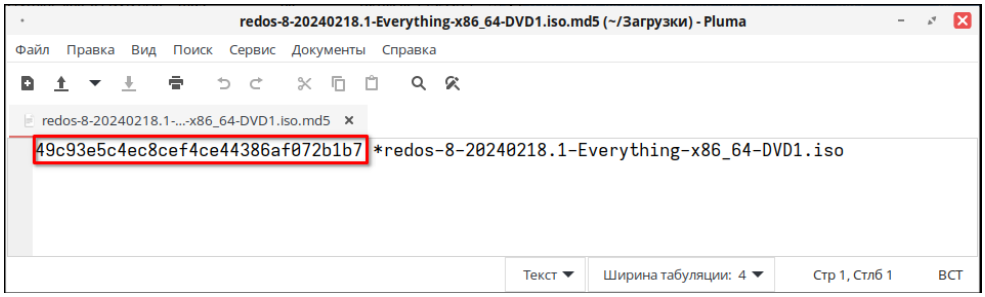


Далее в меню расчета контрольной суммы нужно выбрать требуемый алгоритм (хеш-фукцию) и нажать кнопку «**OK**».

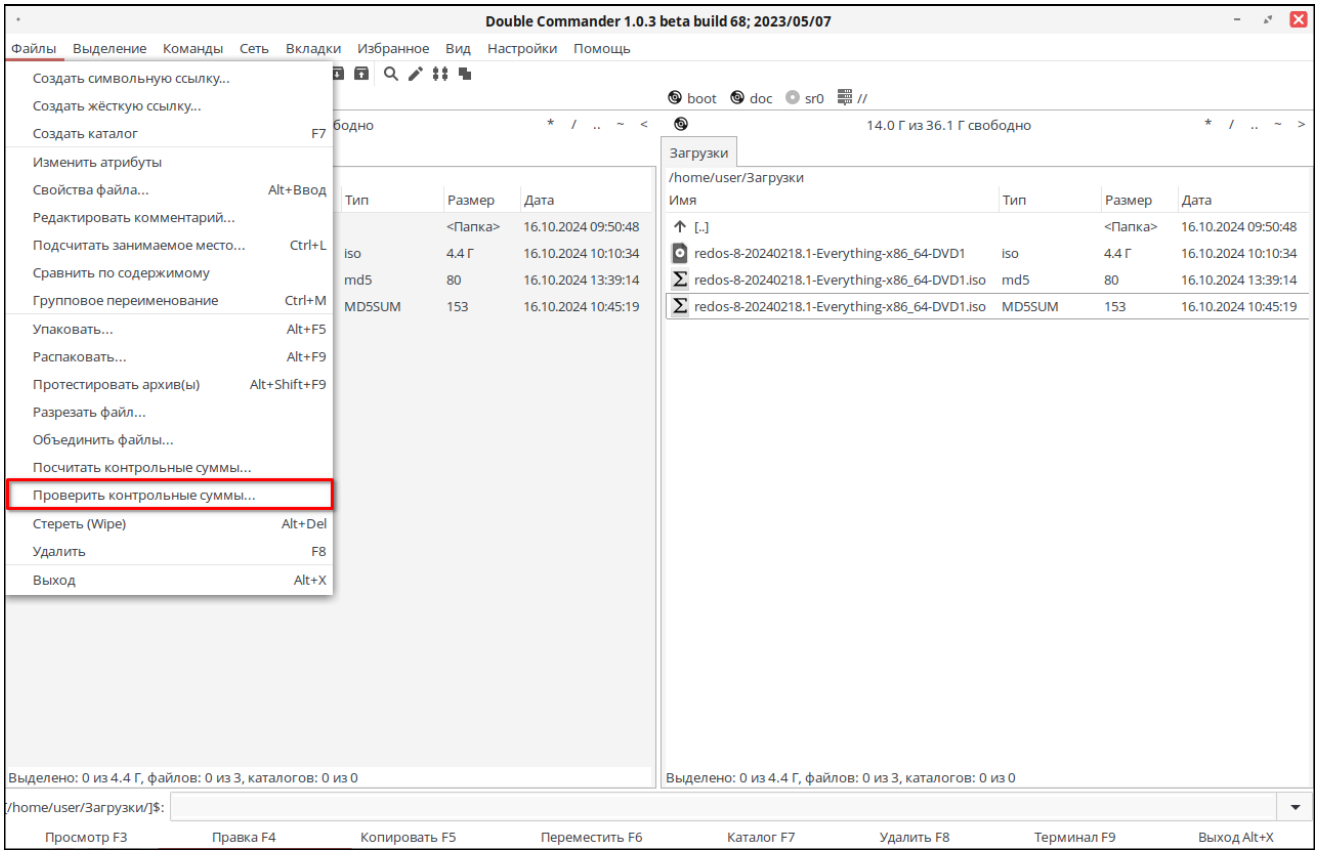


Результат расчета помещается в файл с расширением, соответствующим алгоритму хеширования.

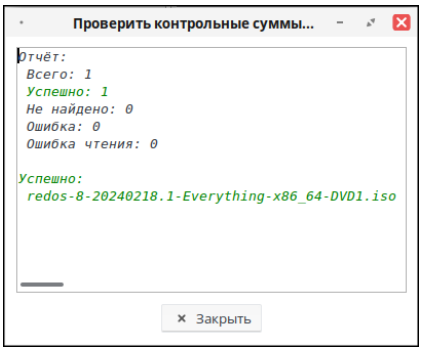
Строка результата для каждого файла представляет собой его *контрольную сумму* и его **название*.



Можно, наоборот, рядом с проверяемым файлом создать файл его контрольной суммы указанного выше формата с тем же именем и соответствующим хеш-алгоритму расширением. Затем выделить этот файл контрольной суммы и из меню «**Файлы**» - «**Проверить контрольные суммы...**» запустить проверку.



После расчета будет выведен результат проверки.



Проверка при помощи встроенных утилит

РЕД ОС имеет встроенные утилиты, с помощью которых проверяются хеши файлов:

- **md5sum** для алгоритма **md5**;
- **shasum** для проверки алгоритма **sha**.

Проверка с помощью утилиты md5sum

Запустите терминал и введите команду:

```
md5sum <имя_файла>
```

В данном случае рассмотрим файл с именем «**redos-8-20240218.1-Everything-x86_64-DVD1.iso**».

```
md5sum redos-8-20240218.1-Everything-x86_64-DVD1.iso

49c93e5c4ec8cef4ce44386af072b1b7  redos-8-20240218.1-Everything-x86_64-DVD1.iso
```

где **49c93e5c4ec8cef4ce44386af072b1b7** – контрольная сумма файла.

Также, помимо нахождения контрольной суммы, можно проверить правдивость указанных в источнике контрольных сумм.

Для этого понадобится файл контрольной суммы из источника с нужным расширением и команда:

```
md5sum -c <имя_файла>
```

В данном случае ответ будет следующим:

```
md5sum -c redos-8-20240218.1-Everything-x86_64-DVD1.iso.md5
redos-8-20240218.1-Everything-x86_64-DVD1.iso: ЦЕЛ
```

Помимо опции «**-c**», отвечающей за проверку контрольной суммы файла, есть и другие опции:

- **-b** - работать в двоичном формате;
- **-t** - работать в текстовом формате;
- **-w** - выводить предупреждения о неверно отформатированном файле сумм;
- **--quiet** - не выводить сообщения об успешных проверках.

Проверка с помощью утилиты shasum

При использовании алгоритма **sha** нужно дополнить команду в зависимости от битности алгоритма **1-**, **256-**, **384-** или **512-**битного.

Команда примет вид:

```
sha1sum <имя_файла>
```

Проверим наш образ:

```
sha1sum redos-8-20240218.1-Everything-x86_64-DVD1.iso
```

```
6a77b64e7ece51227275504c219e5867a76231c8  redos-8-20240218.1-Everything-x86_64-DVD1.iso
```

где **6a77b64e7ece51227275504c219e5867a76231c8** - контрольная сумма файла.

Проверка с помощью дополнительных утилит

Помимо традиционных методов нахождения контрольных сумм через встроенные утилиты также существует аналогичный метод, который используется реже. Дело в том, что контрольная сумма ISO-образа может быть встроена непосредственно в ISO-файл.

Встроить **MD5** в файл поможет утилита **implantisomd5**, входящая в набор программ **isomd5sum**.

Проверку соответствия содержимого образа по встроенной в него контрольной сумме можно осуществить при помощи утилиты **checkisomd5** из того же пакета.

Для установки пакета введите команду (потребуются права **администратора**):

```
sudo dnf install isomd5sum
```

Сначала утилита извлекает **md5** контрольную сумму, далее идет проверка диска.

Контрольная сумма должна быть предварительно внедрена в образ диска, с которого происходит запись, командой:

```
implantisomd5 --force <имя_файла>
```

> **Примечание.**
>
> Сначала создаются образы дисков, затем внедряется контрольная сумма, и только потом записывается на диск. Только после этого можно пользоваться программой **checkisomd5**.

Пример:

```
implantisomd5 --force /home/user/Загрузки/redos-8-20240218.1-Everything-x86_64-DVD1.iso
Inserting md5sum into iso image...
md5 = 79c5725dda1ea581a797b219b85c93c8
Inserting fragment md5sums into iso image...
fragmd5 = 9f5dda2b973b3ac79a2321d458e8124c6a9ebd4d36d283dd976268bc39cf
frags = 20
Setting supported flag to 0
checkisomd5 /home/user/Загрузки/redos-8-20240218.1-Everything-x86_64-DVD1.iso
Press [Esc] to abort check.

The media check is complete, the result is: PASS.

It is OK to use this media.
```

Для того чтобы узнать значение внедренной контрольной суммы, введите команду:

```
checkisomd5  --verbose <имя_файла>
```

Например:

```
checkisomd5  --verbose /home/user/Загрузки/redos-8-20240218.1-Everything-x86_64-DVD1.iso
/home/user/Загрузки/redos-8-20240218.1-Everything-x86_64-DVD1.iso:   79c5725dda1ea581a797b219b85c93c8
Fragment sums: 9f5dda2b973b3ac79a2321d458e8124c6a9ebd4d36d283dd976268bc39cf
Fragment count: 20
Supported ISO: no
Press [Esc] to abort check.
Checking: 100.0%

The media check is complete, the result is: PASS.

It is OK to use this media.
```

SELinux - система принудительного контроля доступа

Введение
Установка
Утилита audit2allow
Утилита secon
Утилита audit2why

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя. Далее описываются основные принципы, на которых построена работа SELinux, а также их реализация в РЕД ОС.

Введение

В большинстве операционных систем имеются средства управления доступом, которые определяют, может ли определенный объект (пользователь или программа) получить доступ к определенному ресурсу. В системах UNIX применяется разграничительный контроль доступа (discretionary access control, DAC). Этот метод позволяет ограничить доступ к объектам на основе групп, к которым они принадлежат. Например, в GNU/Linux для каждого файла определены владелец, группа, а также указаны права доступа к этому файлу. Правами доступа определяется, кто может получить доступ к файлу, кто может открыть его для чтения, кто может внести в него изменения, кто может запустить этот файл на выполнение. Права доступа определены для трех категорий: пользователь (владелец файла), группа (все пользователи, которые являются членами группы) и другие (все пользователи, которые не являются ни владельцем файла, ни членами группы).

Такое разграничение прав доступа может привести к возникновению ряда проблем из-за того, что программа, в которой может быть обнаружена уязвимость, наследует все права доступа пользователя. Следовательно, она может выполнять действия с тем же уровнем привилегий, какой есть у пользователя (*что нежелательно*). Вместо того чтобы определять ограничения подобным образом, более безопасно использовать принцип наименьшего уровня привилегий (*principle of least privilege*), согласно которому программы могут делать только то, что им необходимо для выполнения своих задач, и не более того. Таким образом, даже если в программе будет обнаружена уязвимость, то возможности доступа данной программы будут жестко ограничены. Такой тип контроля называется принудительным управлением доступом (*mandatory access control*, MAC).

Другим методом управления доступом является управление доступом на основе ролей (role-based access control, RBAC). При использовании RBAC права доступа предоставляются на основе ролей, выдаваемых системой безопасности. Отличие концепции ролей от традиционных групп состоит в том, что группа представляет одного или нескольких пользователей, в то время как роль, хотя она также может быть применена к нескольким пользователям, представляет совокупность полномочий на выполнение определенных действий.

SELinux добавляет в операционную систему GNU/Linux поддержку как MAC, так и RBAC.

Установка

Для установки SELinux требуется установить пакет selinux-policy. Это можно сделать, например, воспользовавшись командной строкой с привилегиями root-пользователя:

```
dnf install selinux-policy
```

После перезагрузки SELinux проиндексирует содержимое жёсткого диска, это может занять некоторое время.

Для настройки SELinux можно использовать различные текстовые редакторы чтобы настроить вручную его файл конфигурации:

/etc/selinux/config.

Утилиты

Утилита audit2allow

Утилита audit2allow создает разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций.

Эта утилита сканирует журналы в поиске сообщений, появляющихся, когда система не дает разрешения на операцию. Далее утилита генерирует ряд правил, которые, будучи загруженными в политику, могли бы разрешить эти операции. Однако, данная утилита генерирует только разрешающие правила Type Enforcement (TE). Некоторые отказы в использовании разрешений могут потребовать других изменений политики. Например, добавление атрибута в определение типа, для разрешения существующего ограничения (constraint), добавления разрешающего правила для роли или модификации ограничения (constraint). В случае сомнений для диагностики можно попробовать использовать утилиту audit2why.

Следует с осторожностью работать с выводом данной утилиты, убедившись, что разрешаемые операции не представляют угрозы безопасности. Обычно бывает лучше определить новый домен и/или тип или произвести другие структурные изменения. Лучше избирательно разрешить оптимальный набор операций вместо того, чтобы вслепую применить иногда слишком широкие разрешения, рекомендованные этой утилитой. Некоторые запреты на использование разрешений бывают не принципиальны для приложения. В таких случаях вместо использования разрешительного правила («allow» rule) лучше просто подавить журналирование этих запретов при помощи правила «dontaudit».

Синтаксис:

```
audit2allow
```

Опция	Значение опции
-a | --all	Прочесть входную информацию из журналов message и audit. Не используется вместе с опцией -i
-d | --dmesg	Прочесть входную информацию из вывода команды /bin/dmesg. Обратите внимание, что когда работает auditd, не все сообщения аудита доступны через dmesg. Вместо этого используйте "ausearch -m avc | audit2allow " или "-a".
-f | --fcfile <File Context File>	Добавить Файл Контекстов в генерируемый пакет модуля. Требует опцию -M.
-h | --help	Вывести краткую справку по использованию
-i <inputfile> | --input <inputfile>	Прочесть входную информацию из <inputfile>
-l | --lastreload	Прочесть только часть входной информации, начиная с момента последней перезагрузки политики
-m <modulename> | --module <modulename>	Генерировать модуль. Требуется вывод <modulename>
-M <modulename>	Генерировать загружаемый пакет модуля. Опция конфликтует с -o
-o <outputfile> | --output <outputfile>	Дописать вывод в <outputfile>
-r | --requires	Генерировать вывод в синтаксисе загружаемого модуля.
-R | --reference	Генерировать эталонную политику (reference policy), используя установленные макросы. Требуется пакет selinux-policy-devel.
-t | --tefile	Указывает, что выходной файл является te-файлом (type enforcement). Может использоваться для конвертации старого формата политик в новый формат.
-v | --verbose	Включить подробный вывод

Пример:
Этот пример подходит для системы, использующей пакет *audit*. Если вы не используете пакет audit, сообщения AVC будут появляться в **/var/log/messages**. В этом случае замените **/var/log/audit/audit.log**, используемый в примере, на **/var/log/messages.**
Использование *audit2allow* для генерации монолитной (не модульной) политики.

```
cd /etc/selinux/$ SELINUXTYPE/src/policycat /var/log/audit/audit.log | audit2allow >> domains/misc/local.tecat
domains/misc/local.teallow cupsd_config_t unconfined_t:fifo_file { getattr ioctl };
```

Просмотрите **domains/misc/local.te** и измените его

```
make load
```

Использование audit2allow для генерации модульной политики:

```
cat /var/log/audit/audit.log | audit2allow -m local > local.te
cat local.te

module local 1.0;
require {
role system_r;
class fifo_file { getattr ioctl }; type cupsd_config_t; type unconfined_t;};
allow cupsd_config_t unconfined_t:fifo_file { getattr ioctl };
```

Просмотрите **local.te** и измените его.

Создание модуля политики вручную:

Скомпилируйте модуль:

```
checkmodule -M -m -o local.mod local.te
```

Создайте пакет:

```
semodule_package -o local.pp -m local.mod
```

Загрузите модуль в ядро:

```
semodule -i local.pp
```

Использование audit2allow для генерации и создания модуля политики:

```
cat /var/log/audit/audit.log | audit2allow -M local
```

Создается новый type enforcment файл: local.te.

Компиляция политики:

```
checkmodule -M -m -o local.mod local.te
```

Создание пакета:

```
semodule_package -o local.pp -m local.mod
```

Для того чтобы загрузить только что созданный пакет политики в ядро, вам необходимо выполнить команду:

```
semodule -i local.pp.
```

Утилита secon

Утилита secon - просмотреть контекст SELinux для файла, программы или ввода пользователя.

Просматривает часть контекста. Контекст берется из файла, идентификатора процесса, ввода пользователя или контекста, в котором была запущена утилита secon.

Синтаксис:

```
secon [-hVurtscmPRfLp] [CONTEXT] [--file] FILE [--link] FILE [--pid] PID
```

Опции:

Опция	>**Значение опции**
-V, --version	Посмотреть текущую версию secon
-h, --help	Вывести информацию по использованию secon
-P, --prompt	Вывести данные в формате, подходящем для подсказки
-u, --user	Показать пользователя контекста безопасности
-r, --role	Показать роль контекста безопасности
-t, --type	Показать тип контекста безопасности
-s, --sensitivity	Показать уровень чувствительности (sensitivity level) контекста безопасности
-c, --clearance	Показать уровень допуска (clearance level) контекста безопасности
-m, --mls-range	Показать для контекста безопасности в виде диапазона уровень чувствительности (sensitivity level) и уровень допуска (clearance)
-R, --raw	Вывести уровень чувствительности (sensitivity level) и уровень допуска (clearance) в формате без трансляции
-f, --file	Получить контекст заданного файла FILE
-L, --link	Получить контекст заданного файла FILE (не следовать по символическим ссылкам)
-p, --pid	Получить контекст заданного процесса по идентификатору PID
--pid-exec	Получить exec контекст заданного процесса по идентификатору PID

Опция	>Значение опции
--pid-fs	Получить fscreate контекст заданного процесса по идентификатору PID
--current, --self	Получить контекст из текущего процесса
--current-exec, --self-exec	Получить exec контекст из текущего процесса
--current-fs, --self-fs	Получить fscreate контекст из текущего процесса
--parent	Получить контекст из родительского процесса текущего процесса
--parent-exec	Получить exec контекст из родительского процесса текущего процесса
--parent-fs	Получить fscreate контекст из родительского процесса текущего процесса

Если не было задано опций, то для того, чтобы secon получил контекст из другого источника, может быть задан дополнительный аргумент CONTEXT. Если этим аргументом является знак дефиса (-), то контекст будет прочитан из стандартного ввода. Если аргументов не было заданно, то secon будет пытаться прочитать контекст со стандартного ввода, но только в том случае, если стандартный ввод не терминал (tty). В этом случае secon будет вести себя как будто была передана опция --self .

Если не задана ни одна опция из --user, --role, --type, --level или --mls-range, то все они будут использованы.

Утилита audit2why

Утилита audit2why - определит из сообщения аудита SELinux причину запрета доступа.

Эта утилита обрабатывает сообщения аудита SELinux, принятые со стандартного ввода, и сообщает, какой компонент политики вызвал каждый из запретов. Если задана опция -p, то используется указанная этой опцией политика, в противном случае используется активная политика. Есть три возможные причины запрета доступа:

- отсутствует или отключено разрешительное TE правило (TE allow rule);
- нарушение ограничения (a constraint violation);
- отсутствует разрешительное правило для роли (role allow rule).

В первом случае разрешительное TE правило может присутствовать в политике, но было отключено через булевы атрибуты. Если же разрешительного правила не было, то оно может быть создано при помощи утилиты audit2allow.

Во втором случае могло произойти нарушение ограничения. Просмотрите policy/constraints или policy/mls для того, чтобы определить искомое ограничение. Обычно, проблема может быть решена добавлением атрибута типа к домену.

В третьем случае была произведена попытка сменить роль, при том что не существует разрешительного правила для участвующей при этом пары ролей. Проблема может быть решена добавлением в политику разрешительного правила для этой пары ролей.

Синтаксис:

```
audit2why
```

Опция	Значение опции
--help	Вывести короткую подсказку
-p <policyfile>	Указать альтернативный файл политики.

Пример:

```
/usr/sbin/audit2why < /var/log/audit/audit.logtype=KERNEL msg=audit(1115316408.926:336418): avc: denied { getattr } for
path=/home/ sds   dev=hda5   ino=1175041   scontext=root:secadm_r: secadm_t:s0-s9:c0.c127
tcontext=user_u:object_r:user_home_dir_t:s0 tclass=dir
```

Причина: Отсутствует или отключено разрешительное TE правило. Разрешительное TE правило может присутствовать в политике, но было отключено через булевы переключатели; проверьте булевы переключатели. Вы можете посмотреть необходимые разрешительные правила, запустив audit2allow и подав это сообщение аудита на ввод.

```
type=KERNEL msg=audit(1115320071.648:606858): avc: denied { append } for name=.bash_history dev=hda5 ino=1175047
scontext=user_u:user_r:user_t:s1-s9:c0.c127 tcontext=user_u:object_r:user_home_t:s0 tclass=file
```

Причина: Нарушение ограничения. Проверьте *policy/constraints*. Обычно, для разрешения ограничения необходимо добавить в

домен атрибут типа.

Отключение SELINUX

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

SELinux имеет три режима работы, по умолчанию установлен режим `Enforcing`.

Enforcing: Все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: Информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Disabled: Полное отключение системы принудительного контроля доступа.

1. Для перевода **SELinux** в режим уведомлений в файле `/etc/selinux/config` замените строку `SELINUX=enforcing` на `SELINUX=permissive`. **SELinux** при этом перейдет в режим уведомлений. Откройте файл конфигурации в редакторе `nano` от пользователя **root** или от пользователя с правами **администратора**.

```
sudo nano /etc/selinux/config
```

В файле замените текст `SELINUX=enforcing` на `SELINUX=permissive`.

Изменения будут применены **только после перезагрузки ОС**.

Вместо ручной правки конфигурационного файла можно выполнить следующую команду в консоли от пользователя с правами администратора (после выполнения команды нужно перезагрузить ПК, перезагрузку можно запустить из консоли командой `reboot`):

```
sudo sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

Параметр `SELINUXTYPE=targeted` **изменять не нужно**.

2. Мгновенный перевод режима SELinux `Enforcing` на `Permissive`:

```
sudo setenforce 0
```

После перезагрузки SELinux будет запущен в режиме, который указан в файле **/etc/selinux/config**.

ВАЖНО!

Крайне **не рекомендуется** устанавливать для **SELinux** режим **Disabled**.

Подключаемые модули аутентификации (PAM). Общие сведения

PAM или Pluggable Authentication Modules (подключаемые модули аутентификации) — это модульный подход к системе аутентификации. Они позволяют сторонним службам предоставлять модуль аутентификации для обеспечения доступа к службе для систем с поддержкой PAM. Службы, использующие PAM для аутентификации, могут использовать их сразу же, без необходимости дополнительной пересборки.

На сервере Linux PAM (Pluggable Authentication Modules) могут использоваться для управления аутентификацией (как часть управления предоставления доступа). При использовании PAM сервисам нет необходимости поддерживать собственную систему аутентификации. Вместо этого они полагаются на модули PAM, доступные в системе. Любой сервис при необходимости может использовать собственную конфигурацию PAM, хотя в большинстве случаев аутентификация выполняется одинаково во множестве сервисов. Вызывая модули PAM, сервисы могут поддерживать двухфакторную аутентификацию «из коробки», сразу же использовать централизованные хранилища аутентификационных средств и многое другое.

PAM предоставляют гибкую модульную архитектуру для следующих сервисов:

- Управление аутентификацией - проверяет, существует ли пользователь, под которым пытаются зайти.
- Управление учётными записями - проверяет, что пароль пользователя не истёк или имеет ли пользователь право обращаться к определённому сервису.
- Управление сеансами - выполняет определённые задачи во время входа или выхода пользователя из системы (аудит, монтирование файловых систем и так далее).
- Управление паролями - предлагает интерфейс для сброса пароля и тому подобное.

При работе с PAM администраторы очень быстро поймут принципы, по которым функционирует PAM.

Во-первых, это «независимость от бэк-энда». Приложениям, поддерживающим PAM, нет необходимости учитывать низкоуровневую логику, чтобы работать с бэк-эндами, например, базами данных, службой LDAP, файлами паролей, веб-службами с поддержкой WS-Security или другими ещё не изобретёнными бэк-эндами. Используя PAM, приложения отделяют логику работы бэк-энда от своей. Всё, что им нужно сделать — это вызвать функцию PAM.

Другим принципом является «независимость от конфигурации». Администраторам не нужно знать, как настраивать десятки различных приложений, чтобы заставить их поддерживать аутентификацию через LDAP-сервер. Вместо этого им достаточно воспользоваться одной конфигурационной структурой, предоставляемой PAM.

Последним принципом, являющимся также частью названия PAM, является «подключаемая архитектура». Когда необходимо интегрировать новый бэк-энд, всё, что нужно сделать администратору — это установить библиотеку для этого бэк-энда (большинство модулей используют один файл настроек). Начиная с этого момента, модуль становится доступен для использования приложениями. Администраторы могут настроить аутентификацию для использования этого бэк-энда и просто перезапустить приложение.

Приложения, для которых необходимо использование PAM, линкуются с библиотекой PAM (libpam) и могут вызывать нужные функции работы с указанными выше службами. Кроме этого, в приложении не нужно реализовывать ничего специфичного для работы с этими сервисами, так как эту задачу на себя берёт PAM. И когда пользователь захочет аутентифицироваться, скажем, в веб-приложении, то это приложение вызывает PAM (передавая ему идентификатор и, возможно, пароль или запрос) и проверяет возвращаемые данные, чтобы принять решение, аутентифицировался ли пользователь и имеет ли он доступ к приложению. Внутренней задачей PAM является определение, где необходимо аутентифицировать пользователя (например, в центральной базе данных или на LDAP-сервере).

Сильной стороной PAM является то, что любой желающий может создать модули PAM для интеграции с любым поддерживающим PAM-сервисом или приложением. Если какая-нибудь компания выпускает новый сервис для аутентификации, всё, что нужно будет сделать, — это предоставить для взаимодействия с этим сервисом модуль PAM, после чего любое использующее PAM приложение сможет незамедлительно работать с этим сервисом: нет необходимости что-то пересобирать или улучшать.

Другой важной особенностью PAM является то, что они поддерживают объединение в цепочки нескольких модулей. Пример конфигурационного файла PAM для некоего сервиса:

```
# Аутентификация
auth        required      pam_env.so
auth        required      pam_ldap.so
# Управление учётными записями
account     required      pam_ldap.so
# Управление паролями
password    required      pam_ldap.so
# Управление сеансами
session     optional      pam_loginuid.so
session     required      pam_selinux.so close
session     required      pam_env.so
session     required      pam_log.so level=audit
session     required      pam_selinux.so open multiple
session     optional      pam_mail.so
```

Видно, что конфигурационный файл разделён на четыре области сервисов, которые поддерживают PAM: аутентификация, управление учётными записями, управление паролями и управление сеансами.

Каждый из этих разделов в файле вызывает один или несколько модулей PAM. Например, **pam_env.so** устанавливает переменные среды, которые могут быть использованы последующими модулями. Код, возвращаемый модулем PAM, вместе с управляющими

директивами (в данном примере — *required* или *optional*) позволяет PAM решать, что делать дальше.

PAM поддерживают следующие управляющие директивы:

- **required** - Указанный модуль PAM должен вернуть код успеха для того, чтобы весь сервис (например, аутентификация) был успешен. Если модуль PAM вернёт код неудачи, остальные модули будут всё равно вызваны (хотя уже точно известно, что сам сервис будет недоступен).
- **requisite** - Указанный модуль PAM должен вернуть код успеха для того, чтобы весь сервис был доступен. В отличие от *required*, если модуль PAM вернёт код неудачи, директива сразу же завершится, и сам сервис будет недоступен.
- **sufficient** - Если указанный модуль PAM вернёт код успеха, весь сервис будет разрешен. Оставшиеся модули PAM не будут проверяться. Однако, если модуль PAM вернёт код неудачи, оставшиеся модули пройдут проверку, а неудача данного модуля не будет приниматься во внимание.
- **optional** - Код успеха или неудачи указанного модуля PAM будет иметь значение, если это единственный модуль в стеке.

Цепочки модулей позволяют выполнить множественную аутентификацию, выполнить несколько задач в процессе создания сеанса и тому подобное.

Так как конфигурационные файлы PAM управляют процессом аутентификации в приложении, очень важно правильно с ними взаимодействовать. Файлы обычно располагаются в каталоге **/etc/pam.d/**.

В больших организациях или в требовательных к безопасности системах любая модификация конфигурационных файлов PAM должна подвергаться соответствующему аудиту.

Это же относится к тому месту, где располагаются модули PAM (**/lib/security** или **/lib64/security**).

Помимо файлов-сценариев для некоторых модулей могут использоваться дополнительные файлы конфигурации. Все они расположены в каталоге **/etc/security** и каждый файл предназначен для конкретной группы настроек.

- **time.conf** - Здесь вы сможете ограничить время доступа пользователей с различных терминалов к различным сервисам. Например, запретить входить в систему с первой виртуальной консоли администратору во время выходных. Эти настройки обслуживает модуль pam_time и, соответственно, если вы желаете, чтобы ваши ограничения возымели действие модуль должен быть прописан в соответствующем сценарии.
- **pam_env.conf** - Здесь можно ограничить возможности в изменении отдельных переменных среды пользователями. Работает под руководством модуля pam_env.
- **limits.conf** - Здесь можно индивидуально или для группы ограничить: размер core-файла, максимальный допустимый размер файла, максимальное количество открытых файлов, запущенных процессов, сколько раз можно одновременно зайти в систему и т.д. Руководящий модуль pam_limits.
- **access.conf** - играет важную роль, поскольку PAM предоставляет средства аутентификации по сети. Подобные настройки оказываются полезными, поскольку контролируется не только, кто может войти, но и откуда. Для осуществления такого контроля используется pam_access.
- **group.conf** - Можно указать какой группе будет принадлежать служба запущенная определенным пользователем в определенное время с определенного терминала. Контролируется pam_time и pam_group.
- **console.perms** - Несколько выбивается своим названием, но не функциями. Здесь определяются права, получаемые привилегированными пользователями к консоли во время входа в систему и возвращаемые при выходе. Модуль pam_console.

Список модулей:

- **pam_cracklib**: Тип password. Проверяет ваш пароль на стойкость, не является ли он, например, палиндромом (примечание - это не обязательно при использовании модуля pam_unix). Полезен для программ, задающих пароли. Полезные параметры:
  retry=N - дается N попыток на исправление ошибки,
  diffok=N - должно быть изменено минимум N символов при смене пароля,
  minlen=N - минимальный размер пароля,
  dcredit=N ucredit=N lcredit=N ocredit=N - в пароле должно присутствовать минимум N цифр, строчных, прописных букв и других символов.
- **pam_deny**: Тип любой. Всегда перекрывает доступ.
- **pam_env**: Тип auth. Контролирует сохранность переменных среды. Полезный параметр *conffile=S* - задает альтернативное название файла конфигурации.
- **pam_ftp**: Тип auth. Предназначен для организации анонимного доступа. То есть, получив имя пользователя «anonymous», ждет в качестве пароля что-то похожее на его почтовый адрес. Полезные параметры:
  ignore - не обращать внимание похож ли пароль на почтовый адрес,
  users=XXX,YYY - позволяет анонимный вход для пользователей из этого списка.
- **pam_group**: Тип auth. Предназначение ясно из описания конфигурационного файла group.conf.
- **pam_lastlog**: Тип session. Сообщает о времени и месте входа в систему. Обновляет /var/log/wtmp файл. Полезные параметры:
  nodate, noterm, nohost, silent - не выводить в сообщении даты, терминала, машины или вообще ничего,
  never - если пользователь никогда ранее не появлялся, то его приветствуют.
- **pam_limits**: Тип session. Предназначение указано выше при описании файла limits.conf. Полезный параметр:
  conf=S - альтернативное имя конфигурационного файла.
- **pam_listfile**: Тип auth. Предназначен для организации доступа на основе конфигурационных файлов-списков например /etc/ftpaccess. Для примера смотрите соответствующие файлы сценариев. Возможные параметры: *on err=succeed|fail; sence=allow|deny; file=filename; item=user|tty|rhost|ruser|group|shell apply=user|@group*. Первый параметр задает возвращаемое значение в случае неудачного поиска. Второй - в случае удачного поиска. Третий - имя файла со списком. Четвертый - тип элемента в списке. Последний вносит дополнительные ограничения, если тип объявлен tty, rhost или shell.
- **pam_mail**: Тип auth. Сообщается о наличии почты, если таковая имеется. Полезные параметры:
  dir=S - путь к каталогу почтовых очередей,

noenv - не устанавливать переменную среды MAIL,
close - сообщать, если есть почта у пользователей с аннулированными бюджетами,
nopen - не печатать какой-либо почтовой информации, если пользовательский бюджет только что заведен.

- **pam_nologin**: Тип auth. Стандартная реакция на наличие файла /etc/nologin. Когда он присутствует, в систему может зайти только root, а остальным будет выдано на экран содержимое этого файла.
- **pam_permit**: Тип любой. Использование данного модуля **ОПАСНО** и применимо только в критических ситуациях. Всегда дает допуск.
- **pam_pwdb**: Тип любой. Замещает модули серии pam_unix... . Использует интерфейс библиотеки libpwdb (пользовательские базы данных), что повышает независимость системы аутентификации от способа хранения пользовательских данных (NIS или passwd или shadow). Полезные параметры:
  nullok - можно использовать пустые пароли,
  md5, shadow, bigcrypt - различные способы шифрования пароля.
- **pam_radius**: Тип session. Позволяет осуществлять аутентификацию через RADIUS сервер.
- **pam_rhosts_auth**: Тип auth. Механизм работы этого модуля основывается на анализе содержимого файлов hosts.equiv и .rhosts, используемых для аутентификации таких служб как rlogin и rsh. Полезные параметры:
  no_hosts_equiv - игнорировать содержимое файла hosts.equiv,
  no_rhosts - игнорировать содержимое файлов .rhosts,
  suppres s - охраняет системные журналы от потока малозначимых сообщений, в частности когда используется контрольный флаг sufficient.
- **pam_rootok**: Тип auth. Используется в случае, когда администратору необходимо получать доступ к сервису без введения пароля. Этот модуль допускает пользователя к сервису, только если его uid равен 0.
- **pam_securetty**: Включает в проверку файл /etc/securitty. Суперпользователь сможет зайти только на указанных там терминалах.
- **pam_time**: Тип account. Смотри описание устройства конфигурационного файла time.conf.
- **pam_warn**: Тип auth, session и password. Просто ведет записи в системных журналах, например, при смене пароля.
- **pam_wheel**: Тип auth и account. Права суперпользователя может использовать только пользователь группы wheel (группа root в Linux). Полезные параметры:
  group=XXX - использовать указанную группу вместо стандартной нулевой,
  deny - инвертирование действия алгоритма, запрещается получать права суперпользователя пользователям указанной группы, используется вместе с предыдущим параметром,
  trust - избавляет пользователей группы wheel от необходимости вводить пароль при смене uid на 0.

Настройка двухфакторной аутентификации с помощью модуля pam_usb

Для двухфакторной аутентификации используется модуль «**pam_usb**». Чтобы использовать *FLASH*-накопитель в качестве токена аутентификации, необходимо подключить к ЭВМ *FLASH*-накопитель и убедиться, что ОС успешно его подмонтировала.

Вы можете подробнее ознакомиться с возможностью настройки двухфакторной аутентификации, просмотрев наши обучающие видео:

- на **RuTube** — Модуль PAM USB - двухфакторная аутентификация;
- в **Яндекс.Дзен** — Модуль PAM USB - двухфакторная аутентификация;
- в **VK Видео** — Модуль PAM USB - двухфакторная аутентификация.

На наших каналах вы также сможете найти много другой полезной информации.

Добавить *FLASH*-накопитель, который будет использоваться как токен для аутентификации:

```
pamusb-conf --add-device <Auth-Stick>
```

где **<Auth-Stick>** - произвольное имя, присваиваемое токену.

Далее необходимо выбрать устройство из числа обнаруженных:

```
Please select the device you wish to add.
* Using "JetFlash TS128MJF2A (JetFlash_TS128MJF2A-0:0)" (only option)
Which volume would you like to use for storing data ?
```

И подтвердить его использование:

```
 * Using "/dev/sdc1 (UUID: 1CD6-B3F1)" (only option)
Name  : Auth-Stick
Vendor  : JetFlash
Model  : TS128MJF2A
Serial  : JetFlash_TS128MJF2A-0:0
UUID  : 1CD6-B3F1
```

Подтвердить сохранение параметров:

```
Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

Далее необходимо добавить пользователей, которые могут использовать этот токен:

```
pamusb-conf --add-user='petrov'

Which device would you like to use for authentication ?
* Using "Auth-Stick" (only option)
User
: petrov
Device
: Auth-Stick
Save to /etc/pamusb.conf ?
[Y/n] y
Done.
```

В файлах **/etc/pam.d/system-auth** и **/etc/pam.d/password-auth** нужно в начало файла добавить строку, отвечающую за загрузку модуля, и установить уровень управляющей директивы, как было описано ранее:

```
auth sufficient pam_usb.so
```

Локальная аутентификация с использованием Рутокен MFA

Настройка второго фактора
Настройка связки PIN-код + касание

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pam-u2f-1.2.1-1, pamu2fcfg-1.2.1-1, ido2-tools-1.10.0-1

Рутокен MFA — линейка токенов для аутентификации в веб-сервисах, работающих по протоколу **FIDO2** (CTAP2). Устройства линейки **Рутокен MFA** выступают в качестве единого средства защиты учетных записей веб-сервисов с использованием двухфакторной аутентификации.

Для настройки локальной аутентификации по **Рутокен MFA** установите следующие пакеты (потребуются права администратора системы или суперпользователя **root**):

```
dnf install fido2-tools pam-u2f pamu2fcfg
```

После установки пакетов подключите **Рутокен MFA**.

Для проверки корректности подключения **Рутокена MFA** выведите список подключенных устройств:

```
fido2-token -L
```

Вывод команды должен иметь примерно следующий вид (если к машине подключено только одно **FIDO2**-устройство):

```
/dev/hidraw1: vendor=0x0a89, product=0x0093 (Aktiv Co. FIDO)
```

Установите новый *PIN-код* на токен с помощью команды:

```
fido2-token -S /dev/hidraw1
```

Дважды введите новый *PIN-код*:

```
Enter new PIN for /dev/hidraw1:<новый_PIN>
Enter the same PIN again:<повторите_новый_PIN>
```

Примечание.

Особенности политики *PIN-кода*:

- *PIN-код* по умолчанию не задан;
- заданный *PIN-код* можно изменить, но нельзя удалить без сброса устройства;
- длина *PIN-кода* должна составлять от 4 до 63 символов;
- если *PIN-код* введен неправильно 8 раз подряд, Рутокен блокируется – потребуется сброс устройства.

Рутокен MFA позволяет аутентифицировать пользователя при входе в ОС в следующих сценариях:

- локальная аутентификация пользователя в ОС с использованием **Рутокен MFA** с нажатием кнопки в качестве второго фактора;
- локальная аутентификация пользователя в ОС с использованием **Рутокен MFA** с вводом PIN-кода и нажатием кнопки;
- доступ к хостам по **SSH** с использованием **Рутокен MFA** с нажатием кнопки в качестве второго фактора.

Настройка второго фактора

Для настройки второго фактора аутентификации создайте каталог командой:

```
mkdir -p ~/.config/aktivco
```

Подключите **Рутокен MFA** к машине и выполните настройку модуля с помощью утилиты pamu2fcfg. По завершении выполнения команды вывод утилиты будет записан в файл **u2f_keys**.

ВАЖНО!

Команда должна быть выполнена под пользователем, для которого настраивается аутентификация.

```
pamu2fcfg > ~/.config/aktivco/u2f_keys
```

В процессе выполнения команды необходимо будет прикоснуться к устройству **Рутокен MFA**.

Для повышения безопасности переместите сформированный конфигурационный файл **u2f_keys** в каталог **/etc** следующими командами:

```
sudo mkdir -p /etc/aktivco
sudo mv ~/.config/aktivco/u2f_keys /etc/aktivco/u2f_keys
```

Настройте файлы модуля **PAM** – отредактируйте файл **/etc/pam.d/common-auth**, который обрабатывает общие настройки аутентификации для всех сервисов:

```
sudo nano /etc/pam.d/common-auth
```

После модуля **pam_fprintd.so** добавьте следующую строку:

```
auth sufficient pam_u2f.so authfile=/etc/aktivco/u2f_keys cue nouserok
```

где:

- cue – выводит сообщение с запросом на касание устройства **Рутокен MFA**;
- nouserok – позволяет войти в систему с вводом данных логин/пароль, в случае если пользователь не найден в файле аутентификации или файл аутентификации неверно сформирован. После успешной настройки опцию можно удалить.

```
[root@localhost user]# cat /etc/pam.d/system-auth
# Generated by authselect on Tue Jan  9 13:48:03 2024
# Do not modify this file manually.

auth        required                                    pam_env.so
auth        required                                    pam_faildelay.so delay=2000000
auth        sufficient                                  pam_fprintd.so
auth        sufficient                                  pam_u2f.so authfile=/etc/aktivco/u2f_keys cue nouserok
```

Проверьте, что касание запрашивается в момент входа пользователя, выполнив команду (например, для пользователя **user**):

```
su user

Please touch the device.
```

Настройка связки PIN-код + касание

Для настройки связки *PIN-код + касание* выполните настройку модуля помощью утилиты pamu2fcfg. По завершении выполнения команды вывод утилиты будет записан в файл **u2f_mappings**.

ВАЖНО!

Команда должна быть выполнена под пользователем, для которого настраивается аутентификация.

```
pamu2fcfg -u <username> > /tmp/u2f_mappings
```

Примечание.

В случае выполнения команды без параметра `<username>` файл конфигурации будет создан для текущего пользователя.

В процессе выполнения команды необходимо будет прикоснуться к устройству **Рутокен MFA**.

Содержимое файла **u2f_mappings** должно иметь примерно следующий вид:

```
cat /tmp/u2f_mappings

user: hOzdi1ekgoVWLEzQH20uWJmoA3Dwno53zd2WCvlApHwfMVp/zz3+awUbeCL0E3pe,
jzL+t6w7vhBgR2wwO+61/g8aliGNbDUpYZj6mxLXain4F1bQB0rvnwzP3n+n/GIXUp5Oiui0Du7/aKP/pE27PQ==, es256, +presence
```

Для повышения безопасности переместите сформированный конфигурационный файл u2f_mappings в каталог /etc следующей командой:

```
sudo mv /tmp/u2f_mappings /etc/u2f_mappings
```

Настройте файлы модуля PAM – отредактируйте файл /etc/pam.d/common-auth, который обрабатывает общие настройки аутентификации для всех сервисов:

```
sudo nano /etc/pam.d/common-auth
```

После модуля pam_fprintd.so добавьте следующую строку:

```
auth sufficient pam_u2f.so authfile=/etc/u2f_mappings cue pinverification=1
```

где:

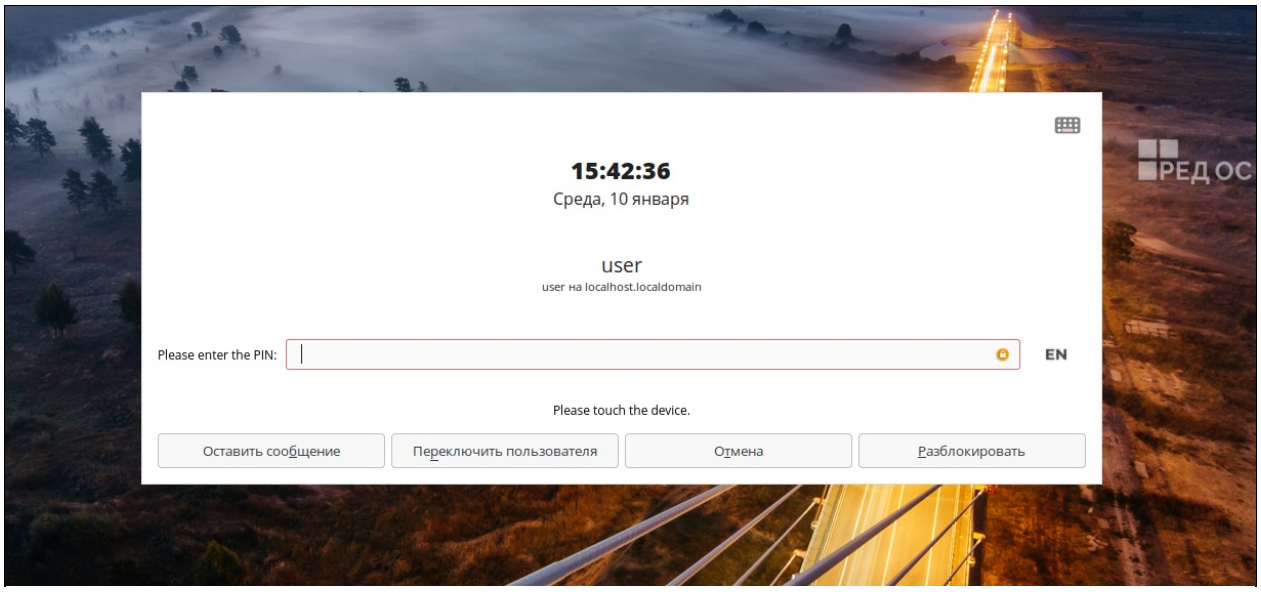
- `cue` – выводит сообщение с запросом на касание устройства **Рутокен MFA**;
- `pinverification=1` – выводит запрос на ввод *PIN-кода* Рутокена.

```
[root@localhost user]# cat /etc/pam.d/system-auth
# Generated by authselect on Tue Jan  9 13:48:03 2024
# Do not modify this file manually.

auth        required                                     pam_env.so
auth        required                                     pam_faildelay.so delay=2000000
auth        sufficient                                   pam_fprintd.so
auth        sufficient                                   pam_u2f.so authfile=/etc/u2f_mappings cue pinverification=1
```

Проверьте, что *PIN-код и касание* запрашиваются в момент входа пользователя, выполнив команду (например, для пользователя **user**):

```
su user

Please enter the PIN: Please touch the device.
```

При входе пользователя в графическую оболочку ОС также будет запрашиваться *PIN-код и касание* кнопки **Рутокен MFA**.


15:42:36
Среда, 10 января
user
user на localhost.localdomain
Please enter the PIN:
EN
Please touch the device.
Оставить сообщение
Переключить пользователя
Отмена
Разблокировать
РЕД ОС

Разблокировка связки ключей в MATE

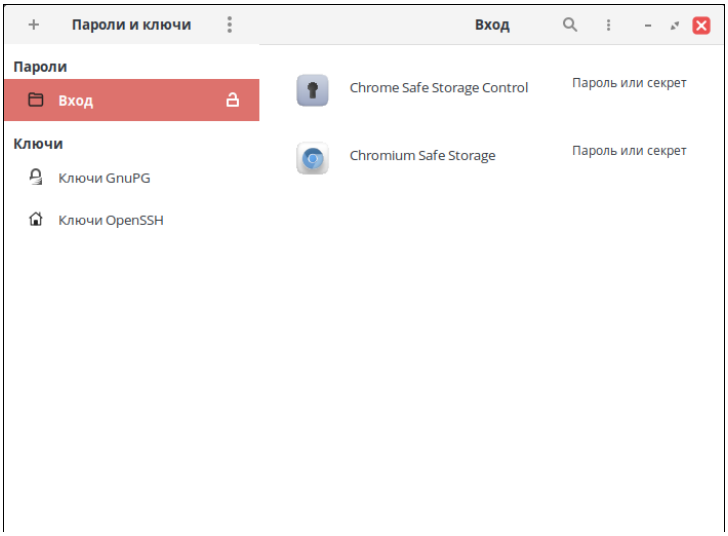
Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Графическое окружение**: MATE

Связка ключей — это зашифрованный контейнер, в котором безопасно хранятся пароли, логины и другие данные для подключения, например, к внешним сетевым ресурсам.

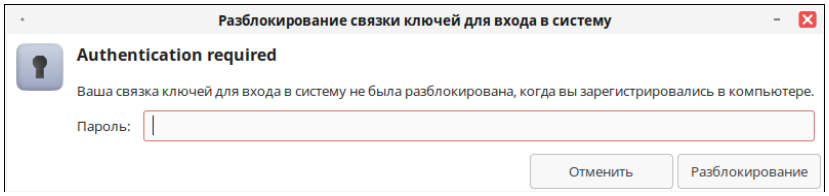
Это хранилище по умолчанию зашифровано и открывается с помощью пароля пользователя при входе в систему.

У каждого пользователя (как локального, так и доменного) на компьютере есть связка ключей входа.



Например, в файловом менеджере был настроен доступ к сетевому ресурсу с параметрами доступа: логин и пароль пользователя (если доменная учетная запись, то указывается и домен) с параметром «**Запомнить навсегда**».

Если вы измените пароль пользователя, появится окно «**Разблокирование связки ключей для входа в систему**».



Но если Вы не желаете вводить каждый раз пароль пользователя для подключения к каким-то ресурсам, то можно сделать пароль в «**Связке ключей**» пустым и тогда данный запрос больше не будет вас беспокоить.

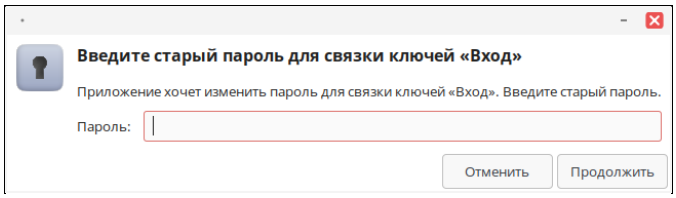
Есть 3 варианта, как сделать пароль в «**Связке ключей**».

1 вариант

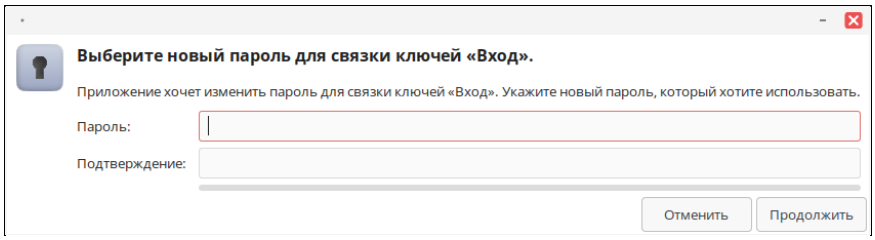
1. Откройте «**Меню**» - «**Стандартные**» - «**Пароли и ключи**».

2. Щелкните правой кнопкой мыши на «**Вход**» и выберите «**Изменить пароль**».

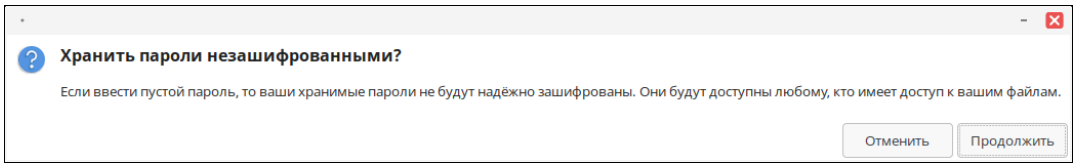
3. Введите старый пароль (пароль пользователя).



4. При вводе нового пароля, оставьте поля пустыми, таким образом он будет не назначен.



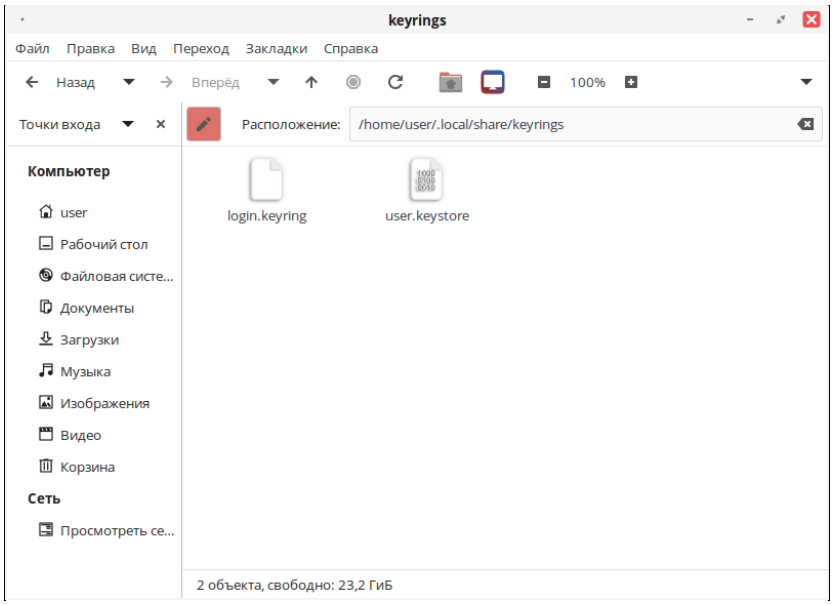
5. На данный запрос выберите «**Продолжить**».



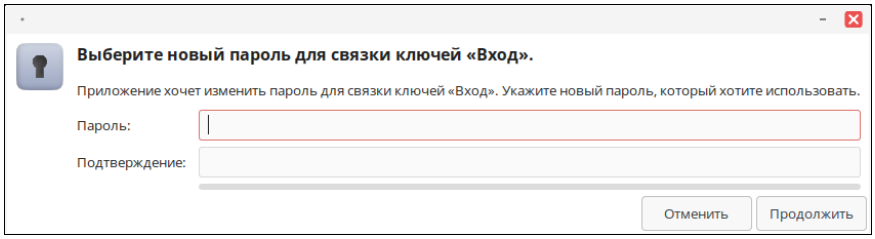
После проделанных действий запрос на ввод пароля для разблокировки связки ключей не должен появиться.

2 вариант

Необходимо через файловый менеджер удалить содержимое скрытого каталога **/home/user/.local/share/keyrings/**. Убедитесь, что включена опция отображения скрытых файлов. Для включения показа скрытых файлов откройте файловый менеджер, перейдите в меню «**Вид**» и установите флаг «**Показывать скрытые файлы**». Затем перейдите в указанный каталог и удалите все файлы внутри него.



Далее выполните перезагрузку компьютера, появится окно, в котором необходимо установить новый пароль.

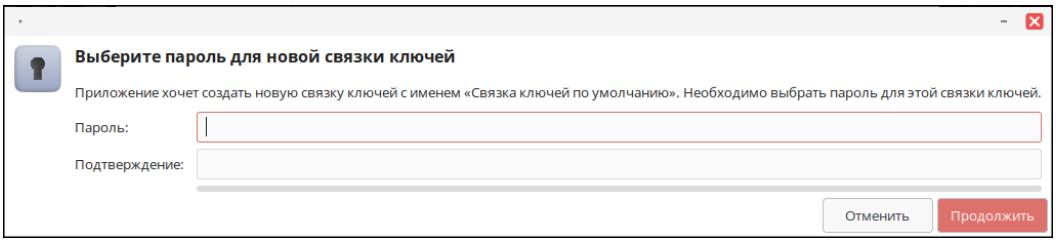


3 вариант

Для сброса настроек (удаление всех паролей и создание новой цепочки ключей) откройте терминал и введите команду:

```
rm ~/.local/share/keyrings/*
```

После перезапуска приложения будет запрошен новый пароль.


Выберите пароль для новой связки ключей
Приложение хочет создать новую связку ключей с именем «Связка ключей по умолчанию». Необходимо выбрать пароль для этой связки ключей.
Пароль:
Подтверждение:
Отменить
Продолжить

Управление паролями в KDE Plasma

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Графическое окружение**: KDE Plasma

KWallet (KDE Бумажник) — это встроенное приложение в **KDE Plasma**, которое служит для безопасного хранения паролей и другой конфиденциальной информации. По умолчанию все данные хранятся в одном бумажнике под названием **kdewallet**, который защищен тем же паролем, что и учетная запись пользователя, и автоматически открывается при входе в систему. Однако пользователи могут создавать несколько отдельных бумажников, каждый из которых может быть защищен своим уникальным паролем. Это позволяет управлять доступом к различным категориям данных, например, разделять рабочие и личные пароли.

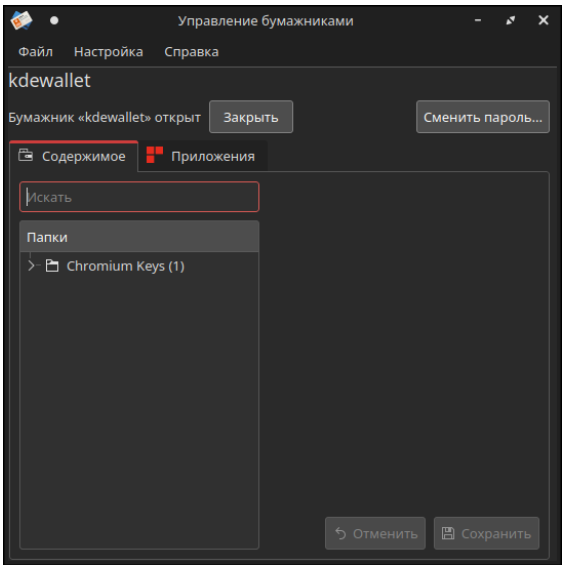
Существует три способа изменения пароля для бумажника **kdewallet.**

1 вариант - Использование KWalletManager

Для управления бумажниками в **KDE Plasma** используется приложение **KWalletManager**, которое запускается через «**Меню**» — «**Система**» — «**KWalletManager**».

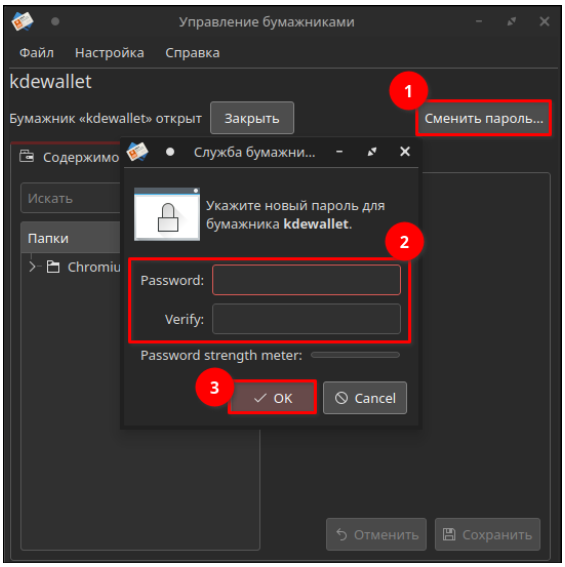
Запустить приложение также можно, выполнив в консоли команду:

```
kwalletmanager5
```



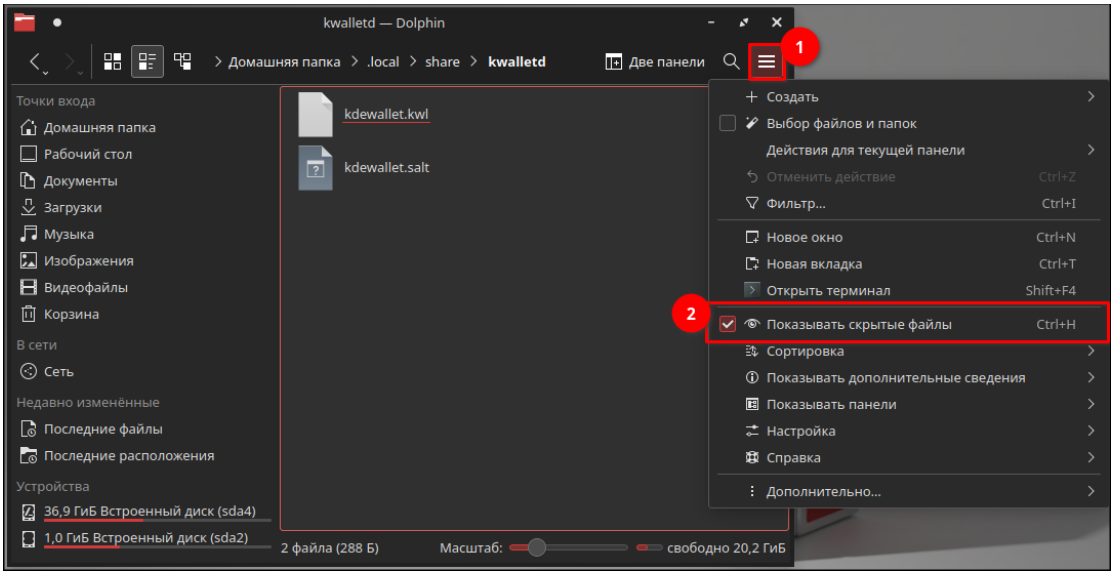
Если пароль бумажника совпадает с паролем пользователя, то при входе в систему он открывается автоматически, без дополнительного запроса. Однако при изменении пароля пользователя пароль бумажника не обновляется автоматически. Поэтому после смены пароля пользователя система будет запрашивать пароль бумажника отдельно до тех пор, пока его пароль не будет изменен вручную на новый.

Для изменения пароля после запуска **KWalletManager** выберите нужный бумажник, нажмите кнопку «**Сменить пароль...**» и в открывшемся окне введите новый пароль:

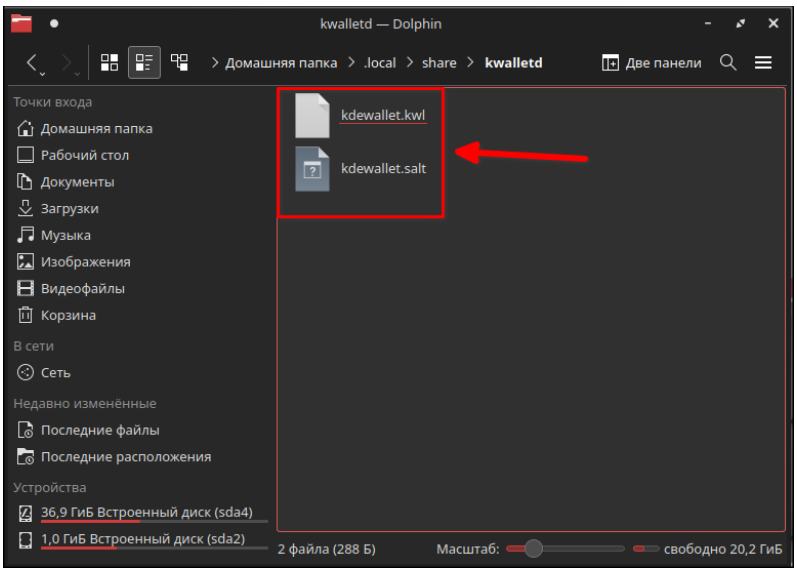


2 вариант - Изменение пароля

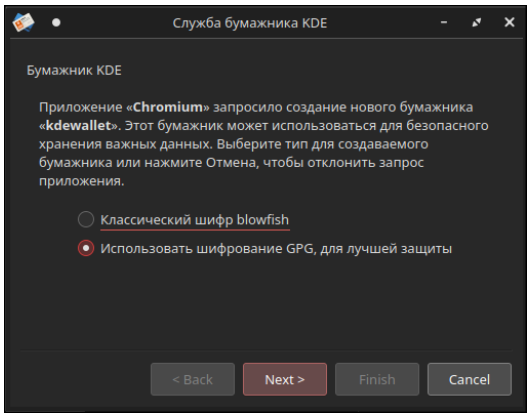
Файлы бумажников находятся в скрытой директории **~/.local/share/kwalletd/**. Убедитесь, что включена опция отображения скрытых файлов. Для включения показа скрытых файлов откройте файловый менеджер, перейдите в дополнительное меню (1) и установите флаг рядом с пунктом «**Показывать скрытые файлы**» (2).



Перейдите в каталог **~/.local/share/kwalletd/** и удалите все файлы внутри него:



При следующем запуске любого приложения, использующего **KWallet**, будет предложено создать новый бумажник. В открывшемся диалоговом окне нужно выбрать модуль шифрования, после чего будет создан бумажник.



3 вариант - Сброс настроек через консоль

Для сброса настроек **KWallet** откройте консоль и введите команду:

```
rm ~/.local/share/kwalletd/*
```

После выполнения команды перезапустите приложение, которое использует **KWallet**. Будет предложено создать новый бумажник и задать новый пароль.

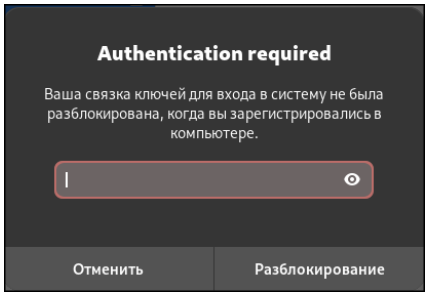
Разблокировка связки ключей в GNOME

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Графическое окружение**: GNOME

Связка ключей — это зашифрованный контейнер, в котором безопасно хранятся пароли, логины и другие данные для подключения, например, к внешним сетевым ресурсам. Это хранилище по умолчанию зашифровано и открывается с помощью пароля пользователя при входе в систему.

У каждого пользователя (как локального, так и доменного) на компьютере есть связка ключей входа. Например, в файловом менеджере был настроен доступ к сетевому ресурсу с параметрами доступа: логин и пароль пользователя (если доменная учетная запись, то указывается и домен) с параметром «**Запомнить навсегда**». Если вы измените пароль пользователя, появится окно разблокирования связки ключей для входа в систему.



Если пользователь не желает вводить каждый раз пароль для подключения к каким-то ресурсам, то можно сделать пароль в «**Связке ключей**» пустым и тогда данный запрос больше не будет беспокоить.

Есть 3 варианта, как сделать пароль в «**Связке ключей**».

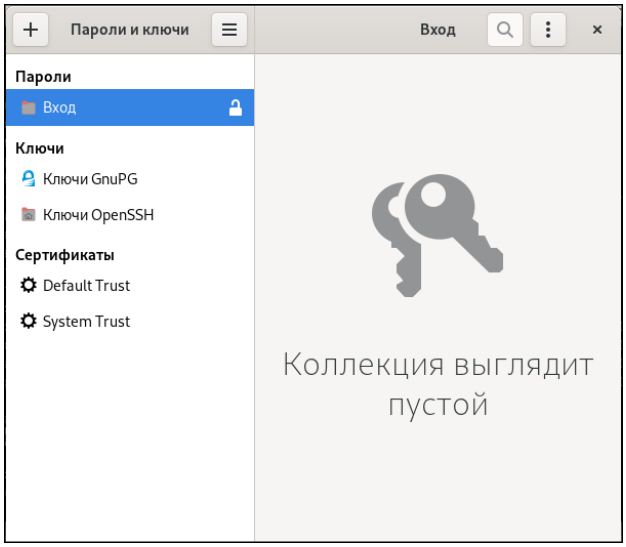
1 вариант

1. **Seahorse** — графическое приложение для управления PGP и SSH-ключами. Для установки пакета введите в терминале команду:

```
sudo dnf install seahorse
```

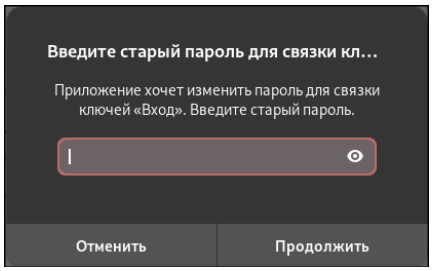
2. Запустите приложение с помощью команды:

```
seahorse
```

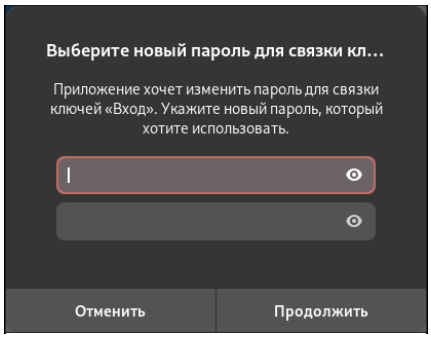


3. Щелкните правой кнопкой мыши на «**Вход**» и выберите «**Изменить пароль**».

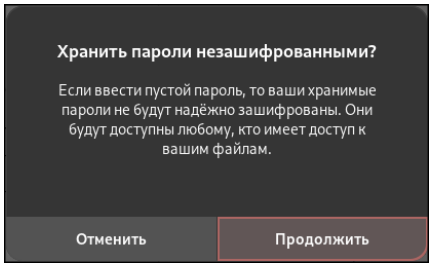
4. Введите старый пароль пользователя для связки ключей.



5. При вводе нового пароля оставьте поля пустыми. Таким образом, он не будет назначен.



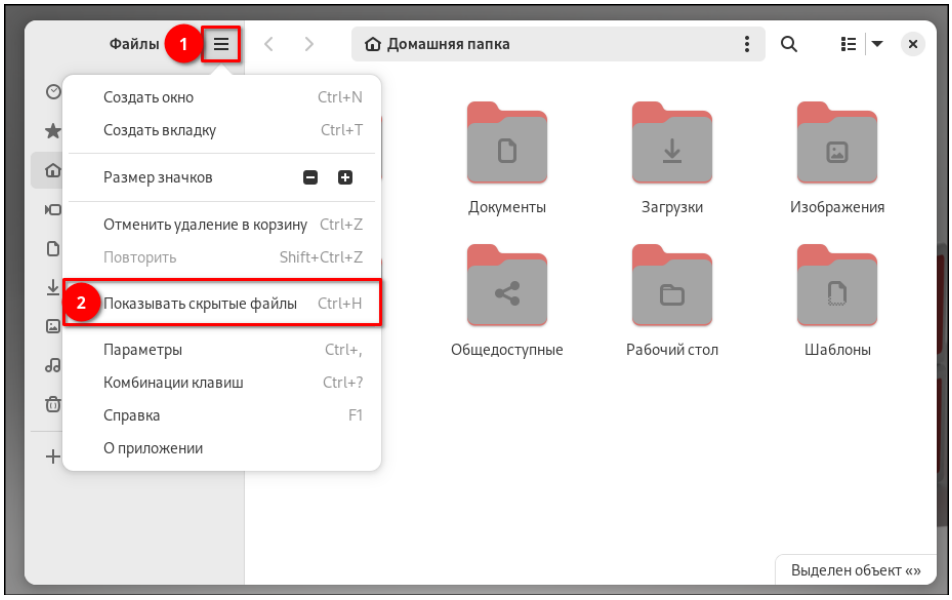
6. На данный запрос выберите «**Продолжить**».



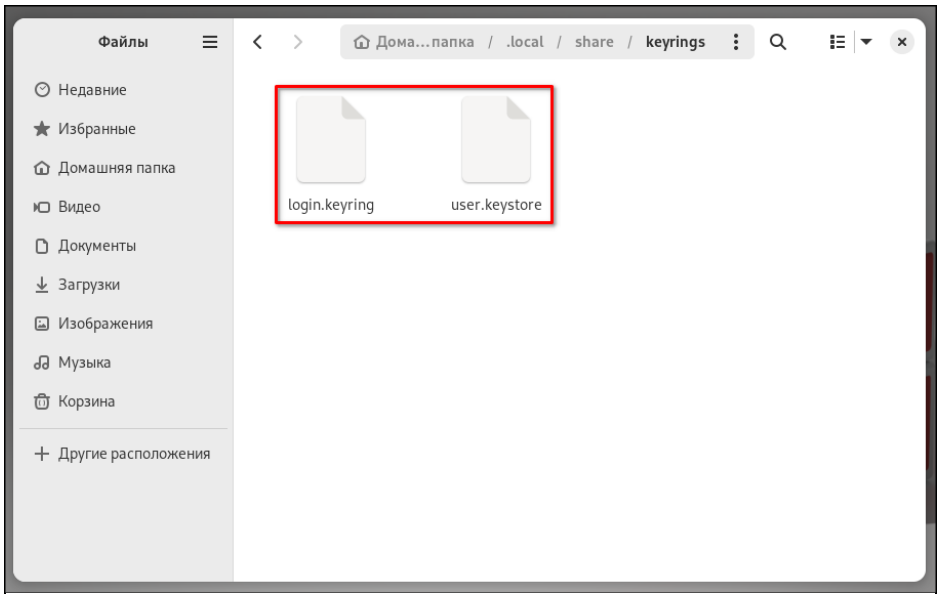
После проделанных действий запрос на ввод пароля для разблокировки связки ключей не должен появиться.

2 вариант

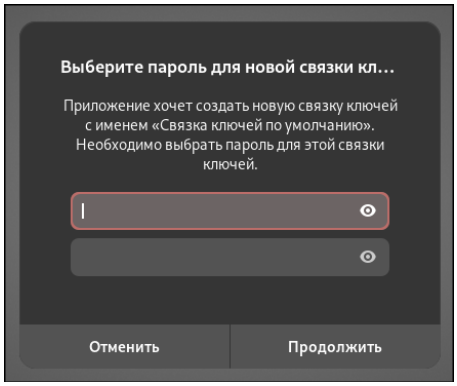
1. Необходимо удалить содержимое скрытого каталога через файловый менеджер **~/.local/share/keyrings/**. Убедитесь, что включена опция отображения скрытых файлов. Для включения показа скрытых файлов откройте файловый менеджер, перейдите в дополнительное меню (1) и установите флаг рядом с пунктом «**Показывать скрытые файлы**» (2).



2. Перейдите в указанный каталог и удалите файлы.



3. Далее выполните перезагрузку приложения, которое использует **связку ключей.** Появится окно, в котором необходимо установить новый пароль.

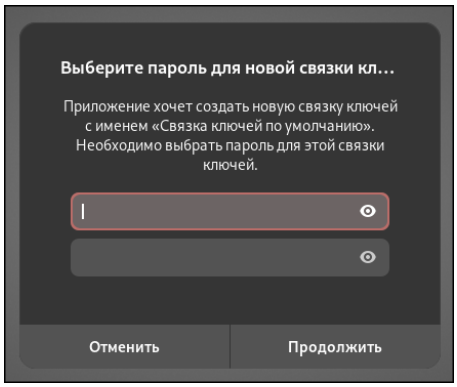


3 вариант

Для сброса паролей откройте консоль и введите команду:

```
rm ~/.local/share/keyrings/*
```

После выполнения команды запустите приложение, которое использует **связку ключей**. Вам будет предложено создать новую связку ключей.



Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012 в РЕД ОС 8

Задание хешей паролей в системах, использующих authconfig
Задание хешей паролей в системах, использующих authselect

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Задание хешей паролей в системах, использующих authconfig

Для настройки задания хешей паролей в соответствии с **ГОСТ Р 34.11-2012** в системах, использующих **authconfig**, необходимо установить пакет **gost-switch-passhash**. Для этого перейдите в сеанс суперпользователя **root**:

```
su -
```

и выполните команду:

```
dnf install gost-switch-passhash
```

Дальнейшая работа с утилитой должна производиться с правами суперпользователя **root**, если не указано иное.

После установки для указания алгоритма хеша пароля выполните команду:

```
gost-switch-passhash gost
```

Для проверки настройки установите новый пароль пользователю:

```
passwd <username>
```

Затем проверьте алгоритм хеша пароля командой:

```
passwd -S <username>
```

В выводе консоли видно, что до внесения настроек алгоритм определялся «**SHA512**», после — «**gost-yescrypt**» (**ГОСТ Р 34.11-2012**):

```
passwd -S user

user PS 2022-03-04 0 99999 7 -1 (Пароль задан, шифр SHA512)

gost-switch-passhash gost
passwd user

Изменение пароля пользователя user.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.

passwd -S user

user PS 2022-03-04 0 99999 7 -1 (Пароль задан, шифр gost-yescrypt)
```

Для того чтобы установить для паролей алгоритм хеширования «**SHA512**», как было в настройках по умолчанию, выполните команду:

```
gost-switch-passhash default
```

Задание хешей паролей в системах, использующих authselect

Проверьте текущий метод шифрования:

```
passwd -S <username>
```

```
<username> PS 2023-11-13 0 99999 7 -1 (Пароль задан, шифр Yescrypt)
```

Проверьте текущий профиль и включенные функции:

```
authselect current

Идентификатор профиля: sssd
Включенные функции:
- with-fingerprint
- with-silent-lastlog
```

Проверьте текущий метод шифрования в текущем профиле:

```
authselect test sssd | grep -e '^password.*pam_unix.so'

password    sufficient      pam_unix.so yescrypt shadow nullok use_authtok
password    sufficient      pam_unix.so yescrypt shadow nullok use_authtok
```

Создайте новый профиль на базе текущего с именем, например, **gost-yescrypt**:

```
authselect create-profile gost-yescrypt --base-on=sssd

Новый профиль создан в /etc/authselect/custom/gost-yescrypt
```

Измените в новом профиле метод шифрования паролей пользователей на **gost_yescrypt**:

```
sed -i 's/\byescrypt\b/gost_yescrypt/' /etc/authselect/custom/gost-yescrypt/password-auth
sed -i 's/\byescrypt\b/gost_yescrypt/' /etc/authselect/custom/gost-yescrypt/system-auth
```

Выберите новый профиль с функциями, которые были в предыдущем профиле:

```
authselect select custom/gost-yescrypt with-fingerprint with-silent-lastlog

Выбран профиль «custom/gost-yescrypt».
Следующие карты nsswitch перезаписаны профилем:
- passwd
- group
- netgroup
- automount
- services

Make sure that SSSD service is configured and enabled. See SSSD documentation for more information.

- with-fingerprint is selected, make sure fprintd service is configured and enabled
```

Примените внесенные изменения:

```
authselect apply-changes

Изменения успешно применены.
```

Проверьте установленные параметры:

```
authselect current

Идентификатор профиля: custom/gost-yescrypt
Включенные функции:
- with-fingerprint
- with-silent-lastlog

authselect test custom/gost-yescrypt | grep -e '^password.*pam_unix.so'

password    sufficient      pam_unix.so gost_yescrypt shadow nullok use_authtok
password    sufficient      pam_unix.so gost_yescrypt shadow nullok use_authtok
```

Задайте пароль пользователю:

```
passwd <username>

Изменение пароля пользователя <username>.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Проверьте метод шифрования:

```
passwd -S <username>

<username> PS 2023-11-13 0 99999 7 -1 (Пароль задан, шифр GOST Yescrypt)
```

Для возврата к профилю по умолчанию выберите прежний профиль с функциями:

```
authselect select sssd with-fingerprint with-silent-lastlog

Выбран профиль «sssd».
Следующие карты nsswitch перезаписаны профилем:
- passwd
- group
- netgroup
- automount
- services

Make sure that SSSD service is configured and enabled. See SSSD documentation for more information.

- with-fingerprint is selected, make sure fprintd service is configured and enabled
```

И примените изменения:

```
authselect apply-changes

Изменения успешно применены.
```

Новые пароли будут шифроваться в соответствии с выбранным профилем.

Менеджер паролей keepassxc

Установка
Создание новой базы данных
Добавление учетных данных
Настройки приложения
Включение SSH-агента в KeePassXC
Добавление RSA-ключа в базу KeePassXC
Проверка работы приложения

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** keepassxc-2.7.6-3

Keepassxc - это современный, безопасный менеджер паролей с открытым исходным кодом, который хранит и управляет вашей конфиденциальной информацией. Он сохраняет множество различных типов информации, таких как имена пользователей, пароли, URL-адреса, вложения и заметки в автономном зашифрованном файле, который может храниться в любом месте, включая частные и общедоступные облачные решения.

Вы можете подробнее ознакомиться с работой менеджера паролей **keepassxc**, просмотрев наши обучающие видео:

- на **RuTube** — Менеджер паролей KeePassXC;
- в **Яндекс.Дзен** — Менеджер паролей KeePassXC;
- в **VK Видео** — Менеджер паролей KeePassXC.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

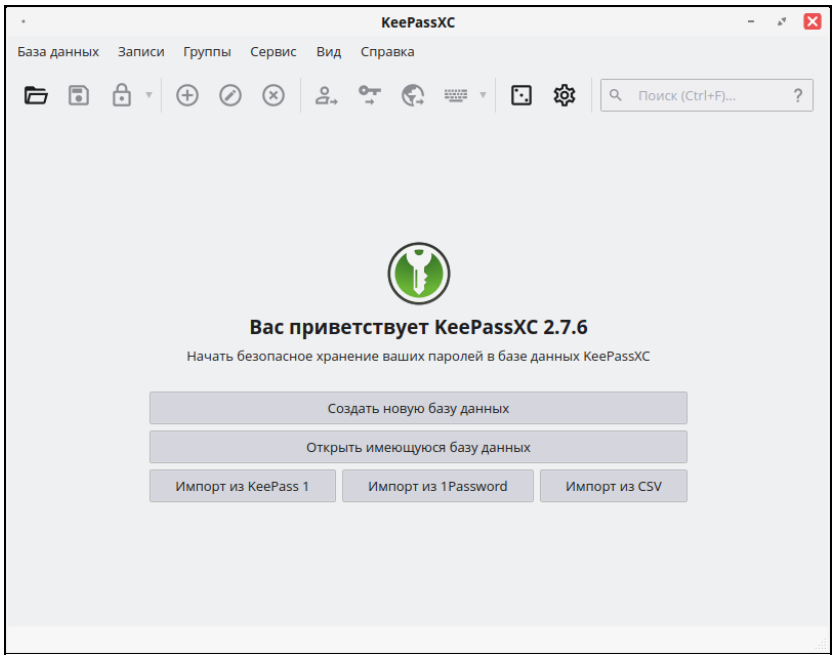
и выполните команду:

```
dnf install keepassxc
```

После установки приложение можно запустить из «**Главного меню**» — «**Стандартные**» — «**KeePassXC**» либо выполнив в терминале команду:

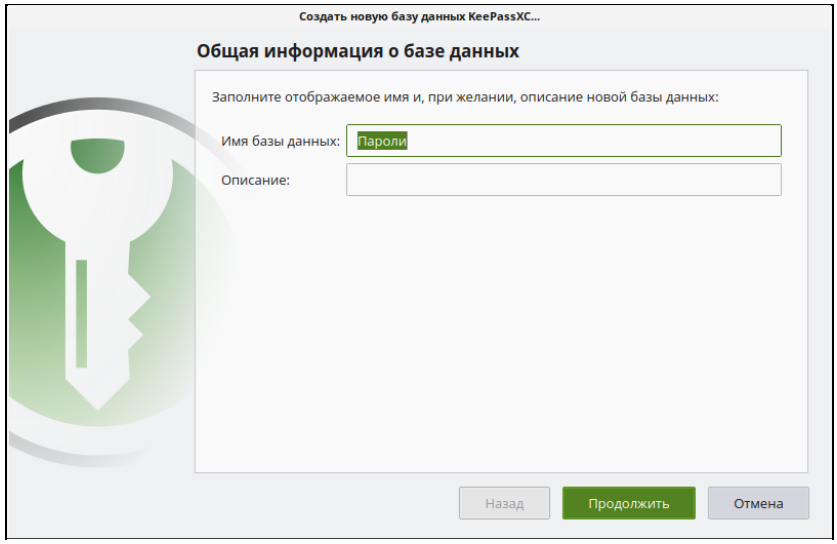
```
keepassxc
```

Главное окно программы выглядит следующим образом:

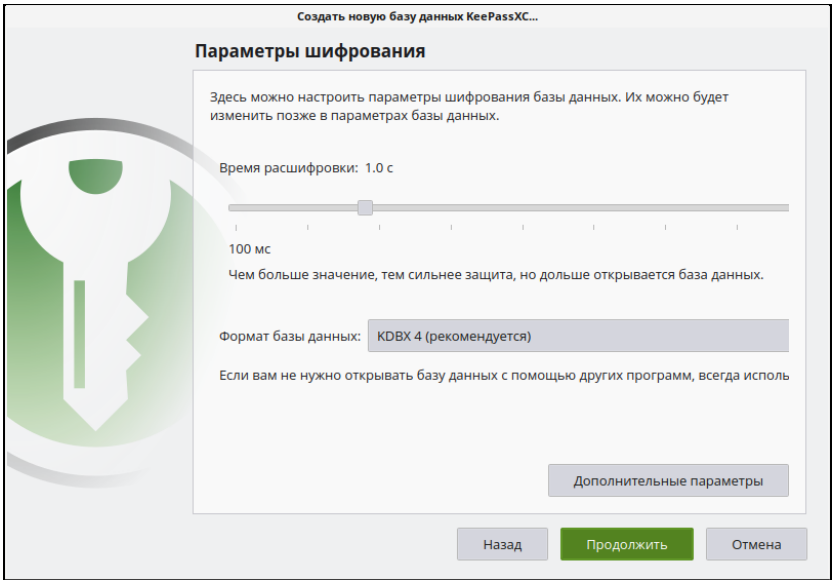


Создание новой базы данных

В окне «**Создать новую базу данных**» предлагается ввести название базы данных и ее описание.

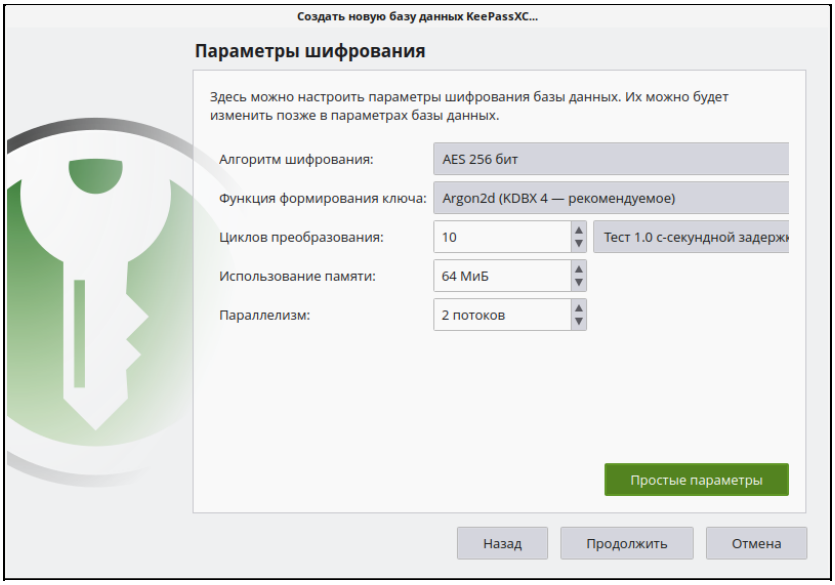


Далее в «**Параметрах шифрования**» можно задать время расшифровки. В дальнейшем, после создания базы, можно будет изменить данные параметры.

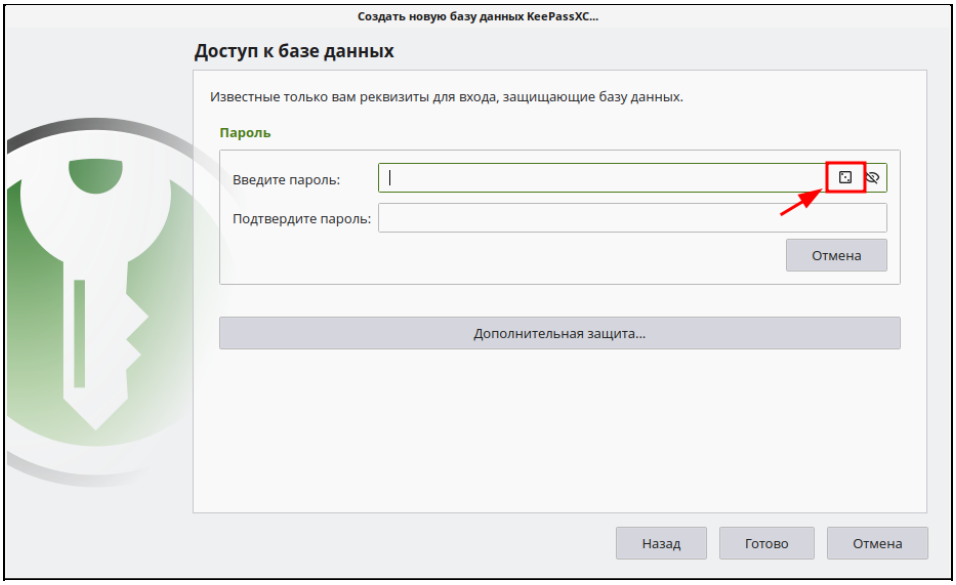


Также можно изменить формат шифрования базы данных, если это необходимо для совместимости с другими приложениями.

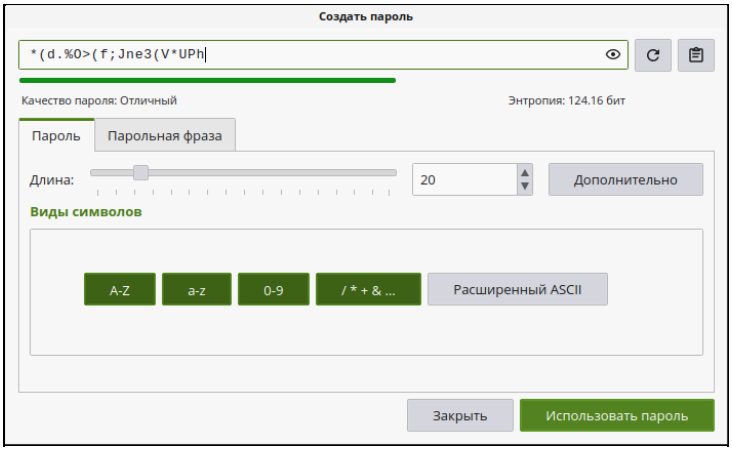
В «**Дополнительных параметрах**» можно усложнить настройки шифрования с помощью предложенных функций:



После установки параметров шифрования необходимо задать пароль для создаваемой базы. Можно как придумать собственный пароль, так и сгенерировать надежный пароль, нажав на кнопку генерации паролей.



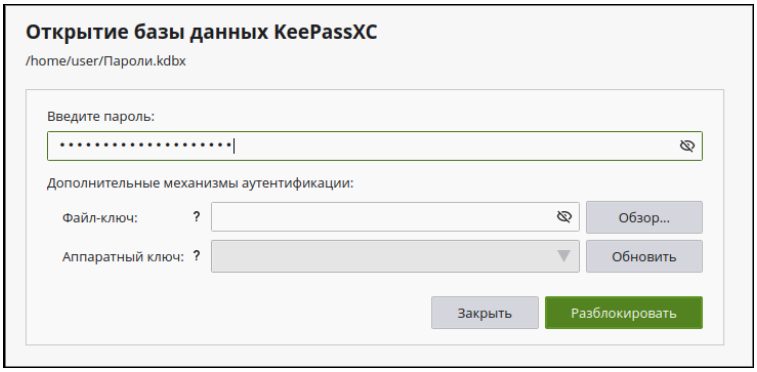
При использовании генератора паролей можно включить и выключить виды используемых символов и задать длину пароля.



ВАЖНО!

Не потеряйте пароль для базы данных. Потеря пароля может привести к невозможности разблокировать вашу базу данных, вы не сможете получить информацию, хранящуюся в ней.

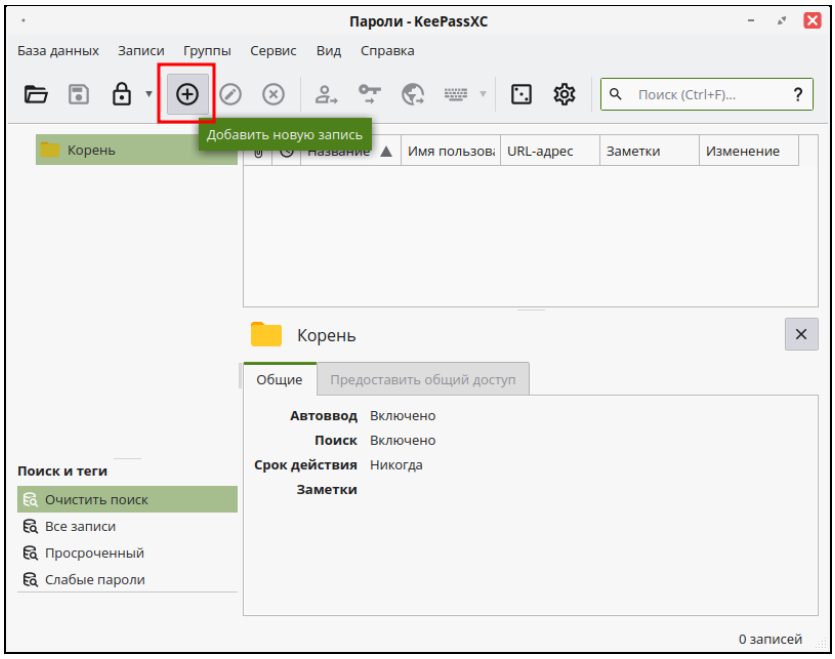
После создания базы можно открыть ее с помощью созданного пароля.



Открыв окно с базой данных, можно создать запись с учетными данными.

Добавление учетных данных

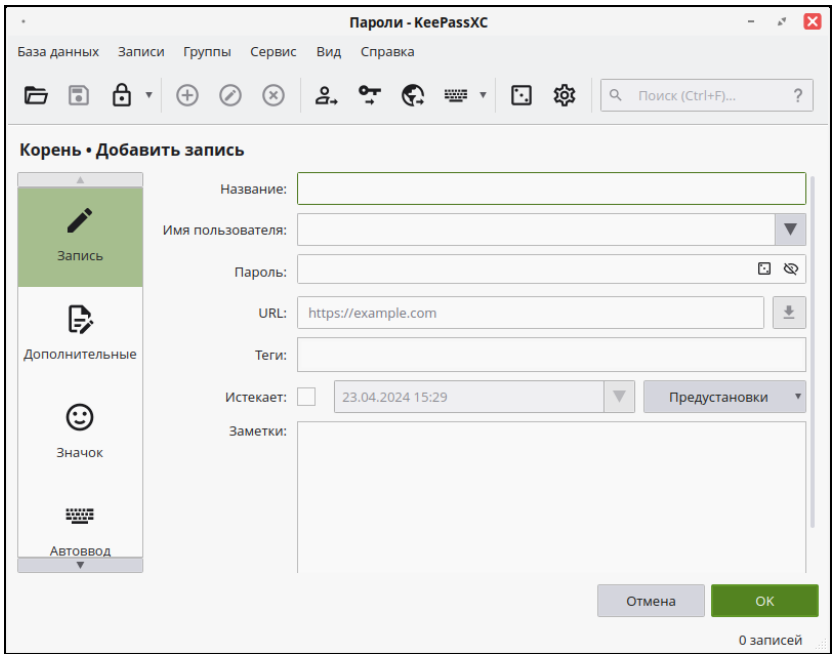
Для того чтобы создать новую запись, нажмите «**Добавить новую запись**» на панели инструментов:



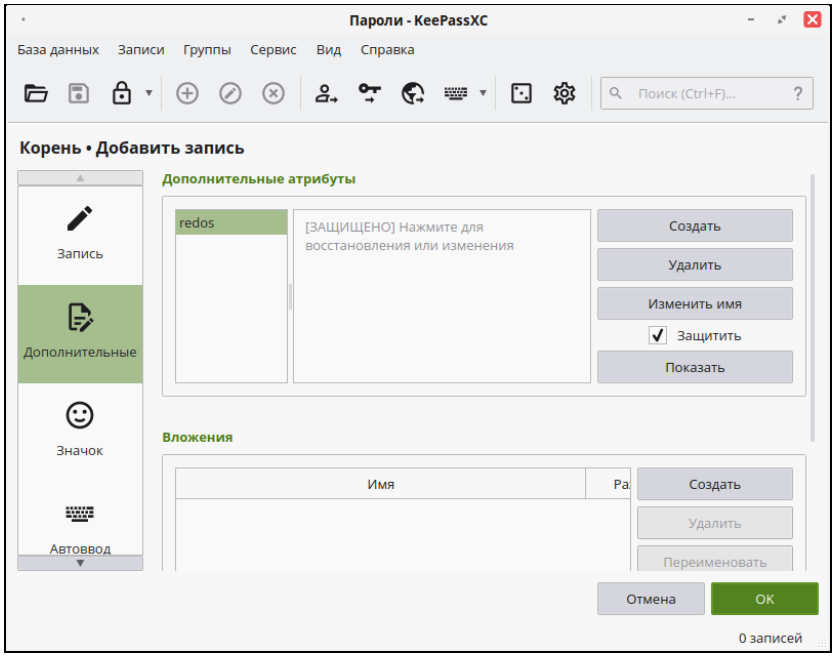
В разделе «**Запись**» указываются название приложения или сайта, где будут использоваться данные, имя пользователя, пароль и URL-адрес ресурса.

В поле «**Пароль**» можно указать собственный пароль или воспользоваться генератором.

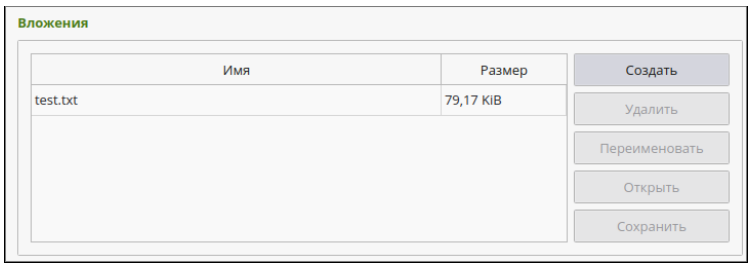
Также можно задать срок окончания действия записи и оставить примечания.



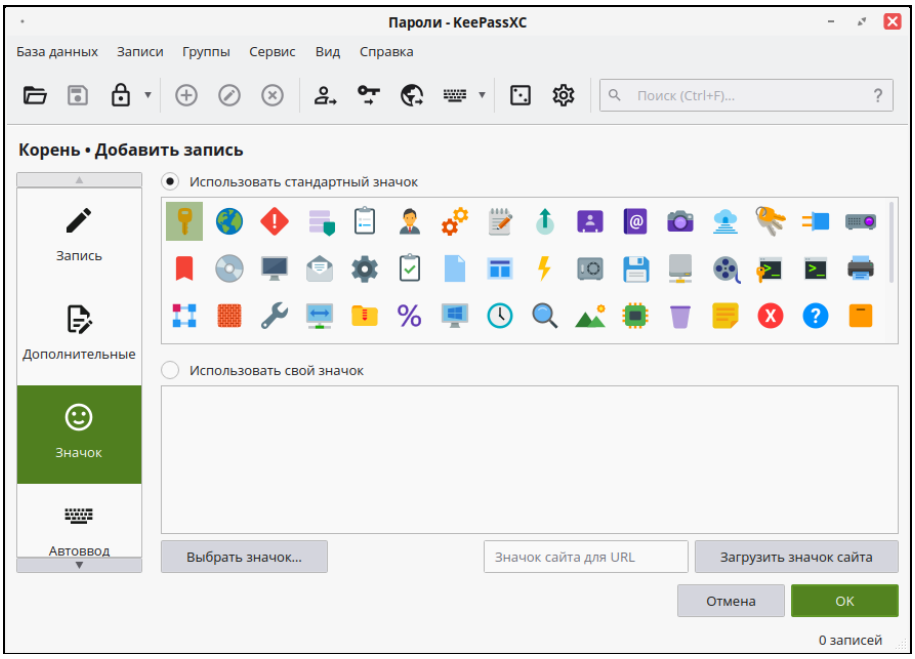
В разделе «**Дополнительные**» можно добавить информацию об учетной записи. Например, ответ на контрольный вопрос для восстановления пароля или любую другую произвольную информацию, которую можно скопировать в буфер обмена или использовать вместе с автовводом.



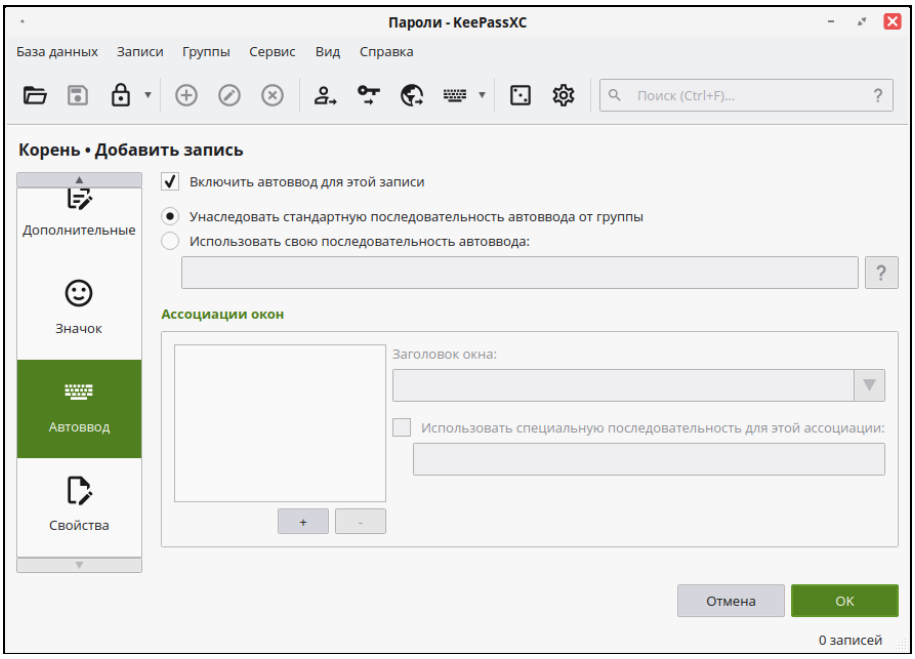
Также в данном разделе можно прикрепить файлы к записи. Эти файлы добавляются в базу данных и хранятся как зашифрованные бинарные файлы. Файлы можно открыть из этого же меню.



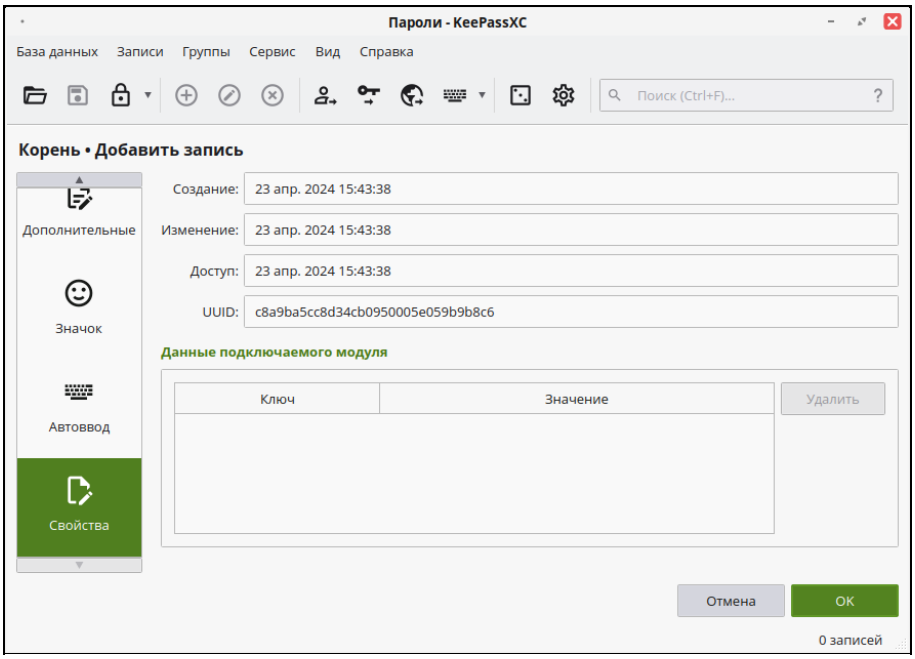
В разделе «**Значок**» можно выбрать значок для вашей записи из стандартных либо добавить свой:



Для каждой созданной записи можно включить автоввод данных. Для этого необходимо перейти в раздел «**Автоввод**» и установить соответствующий флажок:



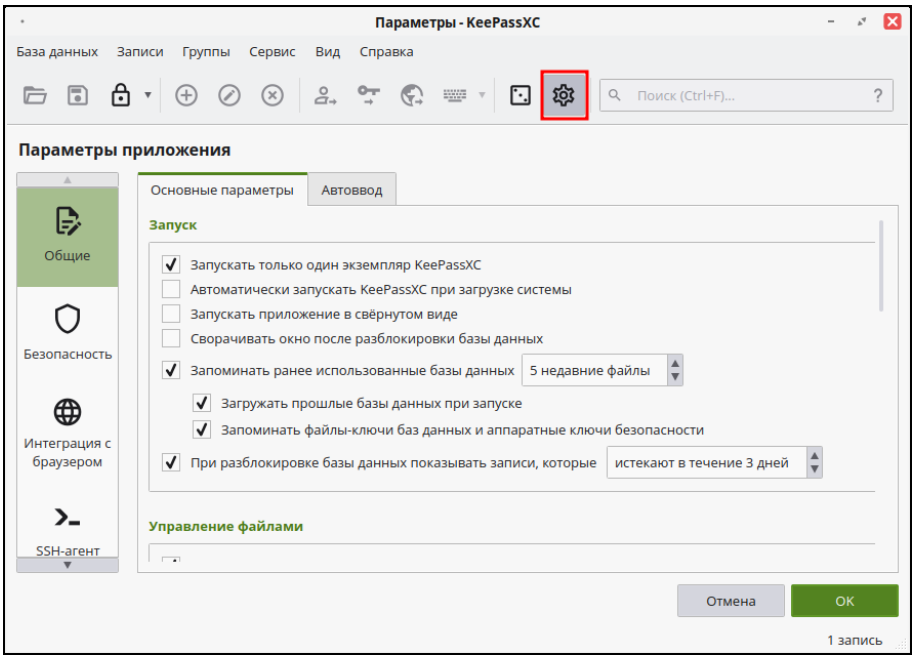
На вкладке «**Параметры**» отображаются дата и время создания, изменения и последнего просмотра этой записи, а также ее уникальный идентификатор.



После ввода всех необходимых данных нажмите кнопку «**OK**», и запись будет создана.

Настройки приложения

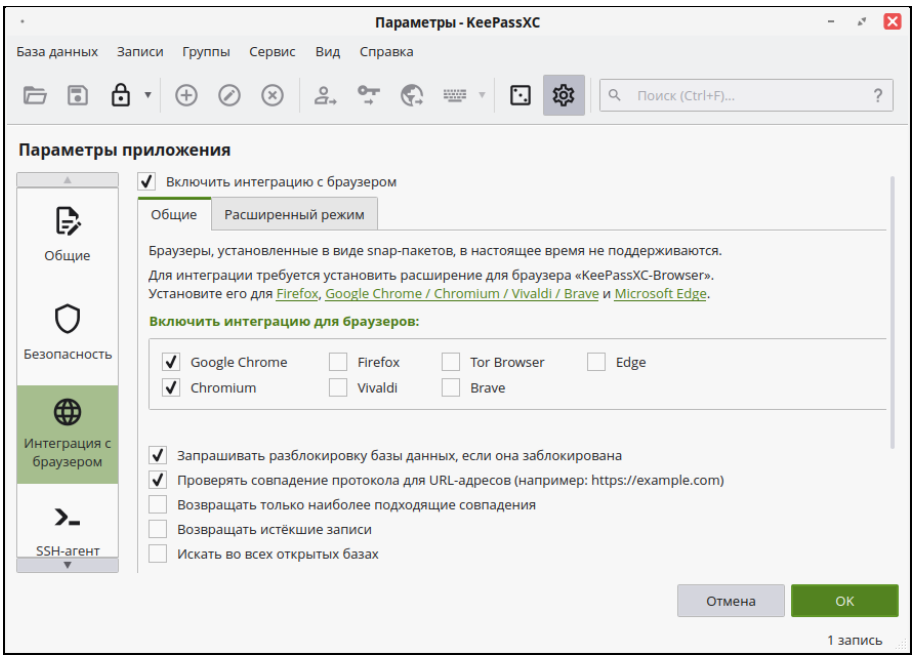
Теперь перейдем в настройки приложения с помощью кнопки «**Параметры**» на верхней панели инструментов и рассмотрим основные опции.



На вкладке «**Общее**» настраиваются параметры запуска приложения, управления файлами и записями, а также настройки интерфейса. Также здесь расположены дополнительные настройки автоввода.

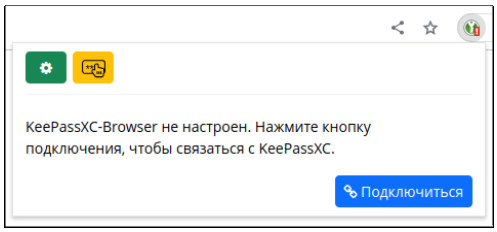
Вкладка «**Безопасность**» содержит настройки блокировки базы данных в различных ситуациях. Например, блокировка сессии пользователя или сворачивания окна.

Следующая вкладка позволяет настроить интеграцию с браузерами.

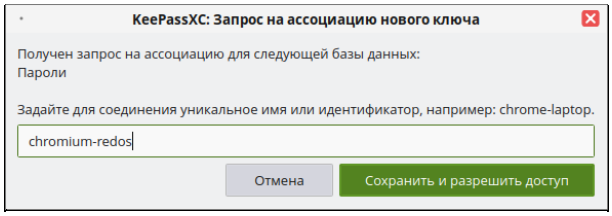


Для этого необходимо проставить соответствующие флажки и установить расширение **KeePassXC-Browser**, ссылки на который находятся в этом же окне.

После установки расширения в браузер необходимо связать его с программой **KeePassXC**. Нажмите кнопку «**Подключиться**».



После этого задайте имя для ключа соединения:



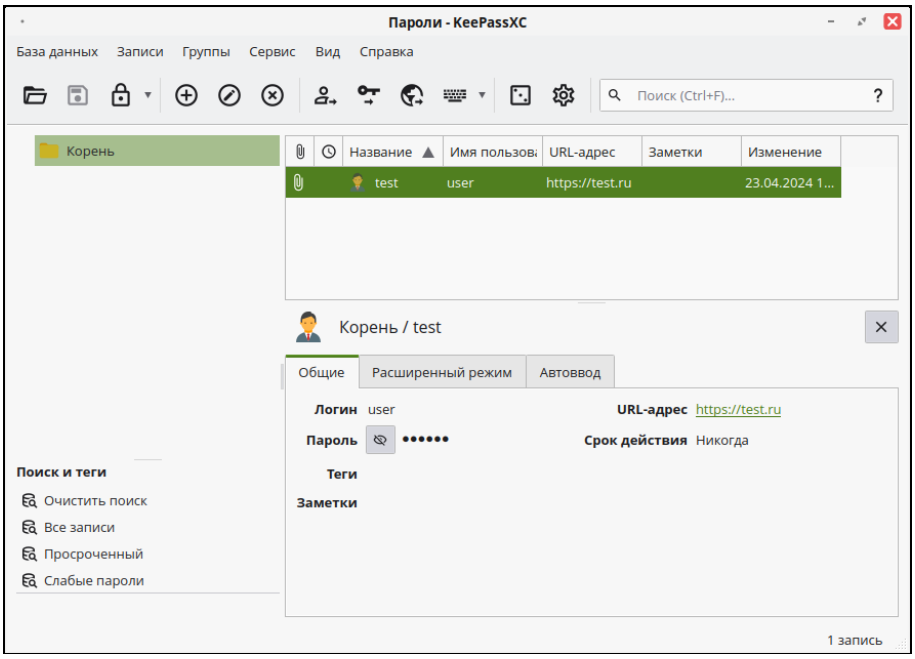
Основные элементы для работы с сохраненными данными находятся на верхней панели инструментов:

1. Скопировать логин в буфер обмена.

2. Скопировать пароль в буфер обмена.

3. Скопировать URL-адрес в буфер обмена.

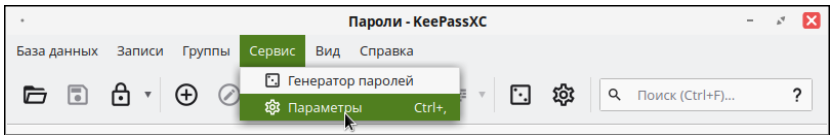
4. Выполнить автоввод.



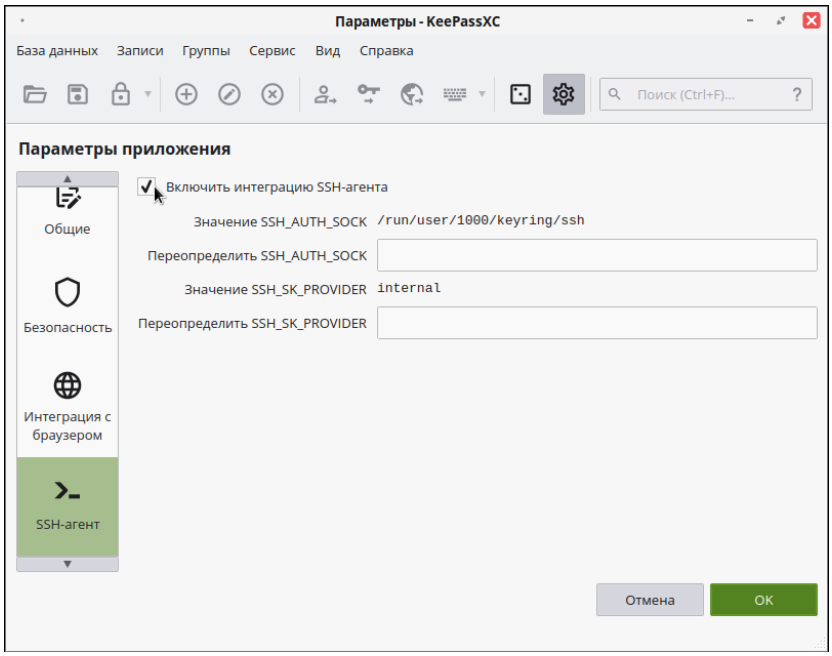
При использовании автоввода логин и пароль будут подставлены в предыдущем открытом приложении в соответствии с настройками автоввода. По умолчанию это последовательность `{USERNAME}{TAB}{PASSWORD}{ENTER}`.

Включение SSH-агента в KeePassXC

В панели инструментов нажмите «**Сервис**» и в контекстном меню выберете «**Параметры**».

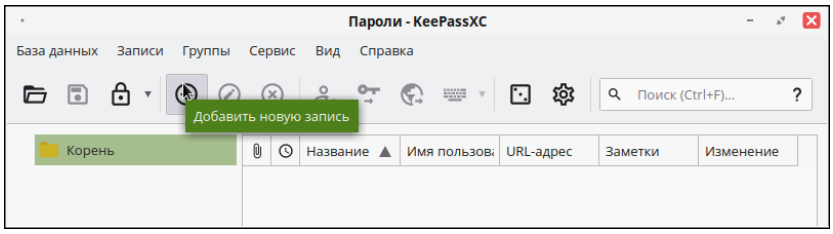


Перейдите на складку «**SSH-агент**», установите флаг «**Включить интеграцию SSH-агента**» и подтвердите настройки нажатием кнопки «**OK**».

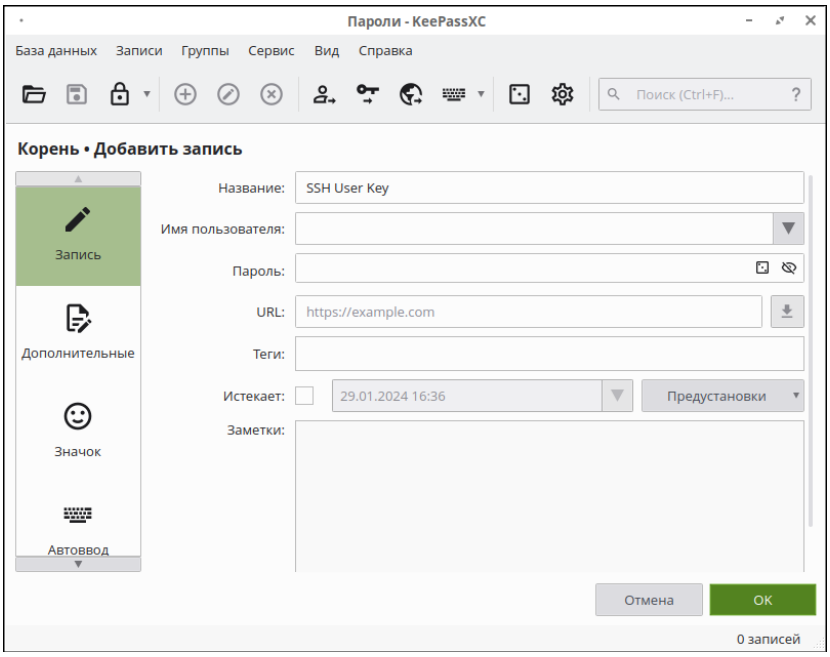


Добавление RSA-ключа в базу KeePassXC

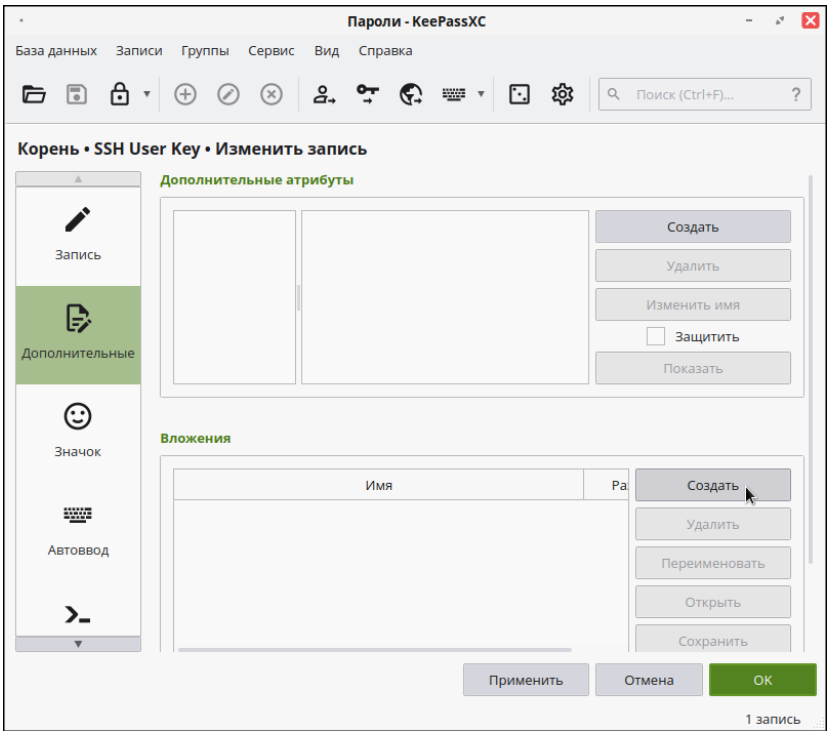
Для добавления новой записи в панели инструментов нажмите на кнопку «**+**».



Укажите название записи и пароль. Если пароль ранее не создавался, оставьте поле пустым.



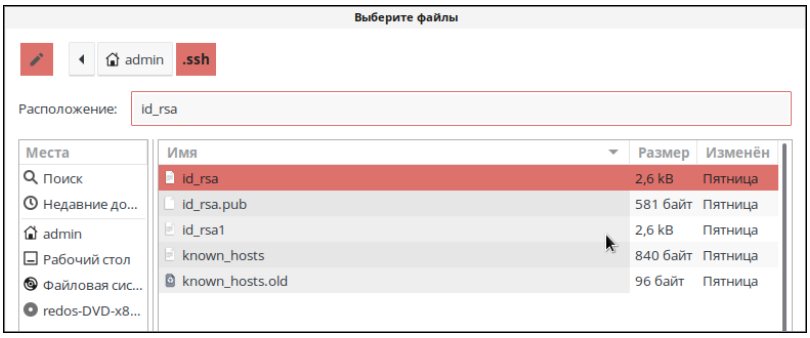
Далее перейдите на вкладку «**Дополнительные**» и в секции «**Вложения**» нажмите «**Создать**».



В открывшемся диалоговом окне укажите путь до закрытой части ключа.

ВАЖНО!

В РЕД ОС каталоги, начинающиеся с точки (**/.ssh**, **/.local** и пр.) определяются графическими оболочками как скрытые. Закрытый ключ по умолчанию расположен в каталоге **/.ssh**. Для отображения скрытых элементов нажмите ПКМ по пустому месту поля выбора файла и установите флаг для параметра «**Показывать скрытые файлы**».

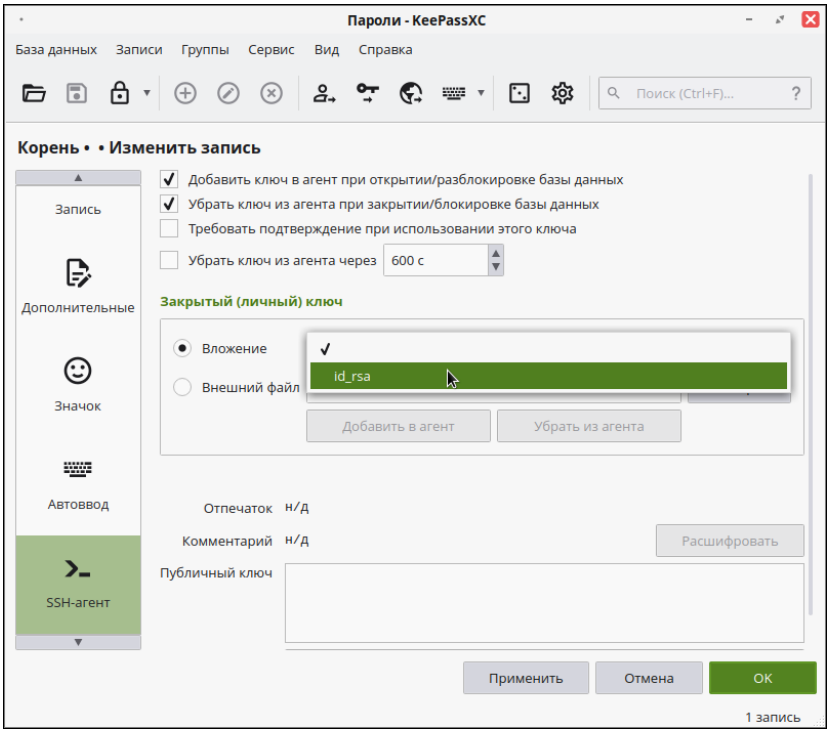


После загрузки закрытого ключа перейдите на вкладку «**SSH-агент**» и в секции «**Закрытый (личный) ключ**» отметьте параметр «**Вложения**». В списке выберите загруженный закрытый ключ.

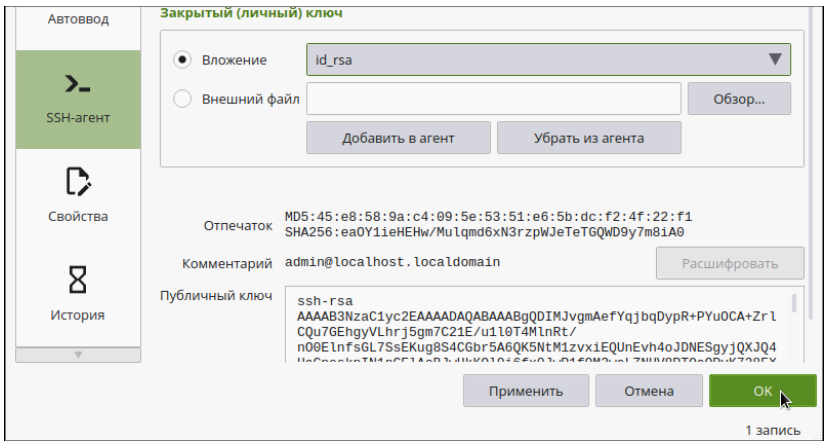
Дополнительно необходимо установить флаги для параметров «**Добавить ключ в агент при открытии/разблокировке базы данных**» и «**Убрать ключ из агента при закрытии/блокировке базы данных**».

Параметр «**Добавить ключ в агент при открытии/разблокировке базы данных**» отвечает за доступность закрытого ключа при запуске приложения. Если параметр не активен, ключ будет недоступен.

Параметр «**Убрать ключ из агента при закрытии/блокировке базы данных**» отвечает за доступность закрытого ключа после закрытия приложения. Если параметр не активен, ключ будет доступен даже после закрытия приложения до выхода из сеанса.



Ниже будет выведена информация о ключе. Для применения изменений нажмите «**OK**» и перезапустите приложение.



Ключ будет сохранен в базе данных **KeePassXC**. В дальнейшем **при запущенном приложении** можно будет осуществлять SSH-подключения вне зависимости от наличия и состояния оригинального файла ключа.

Проверка работы приложения

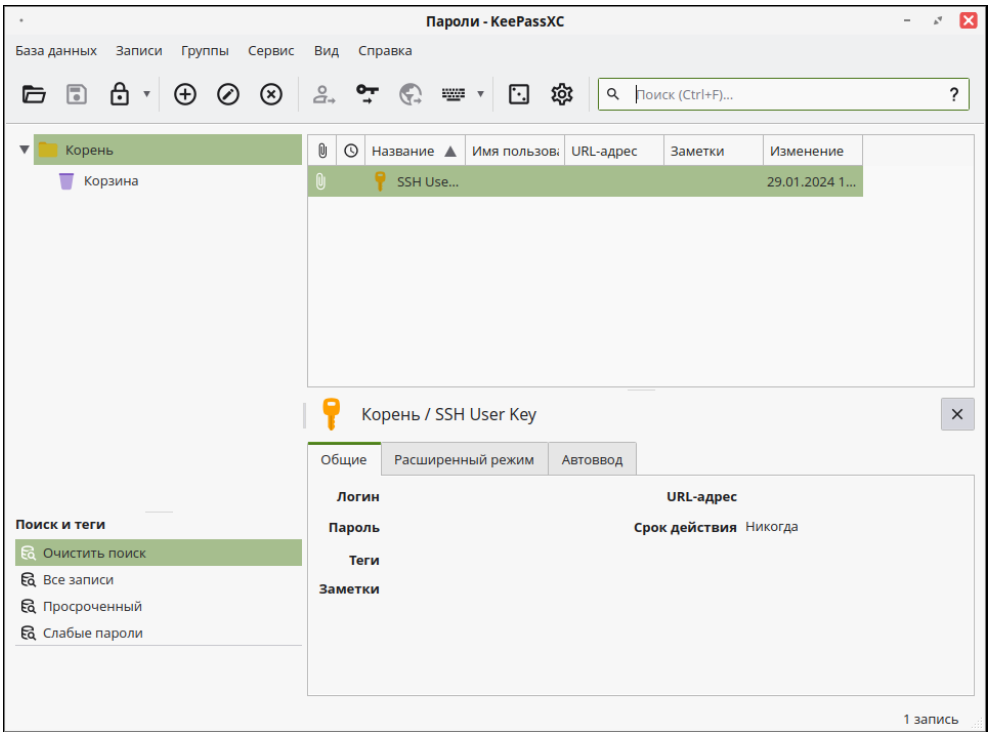
Для проверки работы командой mv переименуйте приватную часть ключа на клиентской машине (устройство, которое инициирует подключение):

```
mv ~/.ssh/id_rsa ~/.ssh/id_rsa1
```

Выполните подключение. При попытке подключения клиент SSH не находит переименованный ранее ключ, вследствие чего сервер предлагает авторизоваться по паролю.

```
ssh user@192.168.100.61

user@192.168.100.61's password:
```

Запустите **KeePassXC** и введите ранее установленный пароль приложения.



Выполните подключение. Обратите внимание на *имя пользователя* и *имя хоста* в командной строке. Если параметры изменились и соответствуют параметрам подключения, аутентификация прошла удачно. Приложение настроено верно.

```
[admin@localhost ~]$ ssh user@192.168.100.61
Last login: Mon Feb  5 11:47:11 2024 from 192.168.100.60
[user@server ~]$
```

Также стоит учитывать, что уже открытые SSH-соединения продолжат работу даже после закрытия приложения.

Работа с политиками Polkit

Polkit
Политики polkit
Правила polkit
Журналирование действий polkit
Примеры
Монтирование раздела и создание нового подключения без запроса пароля
Монтирование устройств с запросом пароля
Разрешение монтирования определённых usb-flash-накопителей
Изменение Network Manager для администратора
Polkit-правило разрешающее вносить изменения в утилиту управления принтерами без запроса пароля

Polkit

Polkit (прежнее название: PolicyKit) — библиотека для UNIX-подобных операционных систем. API библиотеки используется для предоставления непривилегированным процессам возможности выполнения действий, требующих прав администратора. Использование Polkit противопоставляется использованию таких систем, как *sudo*, но не наделяет процесс пользователя правами администратора, а позволяет точно контролировать, что разрешено, а что запрещено.

Вы можете подробнее ознакомиться с работой политик **Polkit**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с политиками Polkit;
- в **Яндекс.Дзен** — Работа с политиками Polkit;
- в **VK Видео** — Работа с политиками Polkit.

На наших каналах вы также сможете найти много другой полезной информации.

Политики polkit

Все политики находятся в ***/usr/share/polkit-1/actions/*** в формате **.policy*. Каждая политика представляет собой xml-файл, в котором описываются запросы к *polkit*. Каждый запрос имеет три условия, прописанных в секции *defaults*:

1. Запрос от любого пользователя. Тег *<allow_any>*;
2. Запрос от неактивного (заблокированного при создании) пользователя. Тег *<allow_inactive>*;
3. Запрос от активного пользователя *<allow_active>*.

Внутри каждого тега прописывается возвращаемое значение. Используются следующие варианты значений:

- **yes** - предоставить разрешения;
- **no** - заблокировать разрешения;
- **auth_self** - пользователь должен ввести свой пароль для аутентификации;
- **auth_self_keep** - пользователь должен ввести свой пароль для аутентификации один раз за сессию, разрешение предоставляется для всей сессии;
- **auth_admin** - пользователь должен ввести пароль *admin* при каждом запросе;
- **auth_admin_keep** - пользователь должен ввести пароль *admin*, разрешение предоставляется для всей сессии.

admin - в РЕД ОС определён в правиле **/etc/polkit-1/rules.d/50-default.rules**:

```
polkit.addAdminRule(function(action, subject)
{
return ["unix-user:root"];
});
```

Правила polkit

Менять напрямую политики нельзя, так как при обновлении системы они будут удалены. Необходимо создавать собственные правила в **/etc/polkit-1/rules.d/** в формате ***.rules**. Правила выполняются в порядке названия по алфавиту, поэтому вначале пишутся цифры, чтобы указать приоритет правила. Алгоритм создания правила (все действия выполняются с правами пользователя **root**):

1. Сначала определяем, какую политику мы хотим изменить, для этого находим в */usr/share/polkit-1/actions/* требуемую.
2. Редактируем новый файл с политикой:

```
nano /etc/polkit-1/rules.d/99-vashe_pravilo.rules
```

3. Вставляем следующий текст:

```
polkit.addRule(function(action, subject)
{
if (action.id == "policy" && <ваше_условие>)
{
return polkit.Result.YES;
};
});
```

где

- вместо ***99*** подставляем нужное число (файлы с политиками просматриваются в лексикографическом порядке, 99 будет последним правилом);
- вместо ***policy*** пишем название политики, поведение которой нужно изменить;
- вместо ***<ваше_условие>***:
  - если необходимо изменить поведение политики для одного конкретного пользователя, пропишите `subject.user == "<имя_пользователя>"`,
  - если необходимо изменить поведение политики для нескольких пользователей, входящих в одну группу как локальную, так и доменную, пропишите `subject.isInGroup("<название_группы>")`.

    Например, для локальной группы **local**, в которую входят пользователи *user1*, *user2* и *user3*, указывается правило вида `subject.isInGroup("**local**")`; для доменной группы, в которую входят пользователи *dom_user1*, *dom_user2* и *dom_user3*, указывается правило вида `subject.isInGroup("**пользователи домена**")`. По желанию для конкретных пользователей домена, которым необходимо настроить доступ или правило, можно создать отдельную группу и поместить в неё нужных пользователей, в таком случае в правиле следует прописать `subject.isInGroup("<название_новой_отдельной_группы_доменных_пользователей>")`.

- ***Result.YES*** означает, что политика при выполнении условия правила будет предоставлять разрешение.

Журналирование действий polkit

Используя правила polkit, можно также делать записи в системный журнал. Метод **log()** записывает сообщение в системный журнал. Пример:

```
polkit.addRule(function(action, subject)
{
if (action.id == "действие")
{
polkit.log("action=" + action);
polkit.log("subject=" + subject);
};
});
```

В параметре *action* передается объект с информацией о совершенном процессе и связанные с этим действием параметры (например, если запрошенное действие - *монтирование съемного диска*, то в параметре **action** будут переданы *серийный номер* диска, его *id*, *файловая система* и т.д.).

В параметре *subject* передается объект с информацией о пользователе, запустившем процесс. Этот объект имеет следующие атрибуты:

- **id** – идентификатор процесса;
- **user** – имя пользователя;
- **groups** – список групп, в которые входит пользователь;
- **seat** – местонахождение субъекта (пустое значение, если местонахождение не локальное);
- **session** – сессия субъекта;
- **local** – true, только если местонахождение имеет локальный характер;
- **active** – true, только если сеанс активен.

Примеры

Пользователи часто сталкиваются с необходимостью вводить пароль при монтировании разделов в файловом менеджере и создании нового подключения в NetworkManager, а также невозможностью извлечения usb-flash-накопителей или лотка оптического привода. За эти разрешения отвечают схемы, в которых описаны определенные доступные действия, предустановленные разработчиком ПО:

- *org.freedesktop.udisks2.filesystem-mount-system* — разрешение на монтирование файловых систем системных устройств;

- *org.freedesktop.udisks2.filesystem-mount-other-seat* — разрешение на монтирование файловых систем с устройств, подключенных в другое место;
- *org.freedesktop.udisks2.eject-media-other-seat* — разрешение на извлечение лотка оптического привода;
- *org.freedesktop.udisks2.power-off-drive-other-seat* — разрешение на извлечение usb-flash;
- *org.freedesktop.NetworkManager.settings.modify.system* — разрешение на создание и модификацию системных сетевых соединений.

Монтирование раздела и создание нового подключения без запроса пароля

Настроим правила для пользователя, находящегося в системной группе **xgrp**, таким образом, чтобы запросы пароля не выполнялись для монтирования раздела и создания нового подключения. Для этого необходимо выполнить следующий алгоритм действий (все действия выполняются с правами пользователя **root**):

1. Наполним **/etc/polkit-1/rules.d/99-udisk2_mount.rules** следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (
(action.id == "org.freedesktop.udisks2.filesystem-mount-system" ||
action.id == "org.freedesktop.udisks2.filesystem-mount-other-seat" ||
action.id == "org.freedesktop.udisks2.eject-media-other-seat" ||
action.id == "org.freedesktop.udisks2.power-off-drive-other-seat")
&& subject.isInGroup("xgrp")
)
{
return polkit.Result.YES;
};
});
```

Указанная в созданном правиле группа **xgrp** используется в качестве примера. При настройке правила необходимо указать название **вашей** группы или имени пользователя в зависимости от требований:

- если необходимо изменить поведение политики для одного конкретного пользователя, пропишите `subject.user == "<имя_пользователя>"`,
- если необходимо изменить поведение политики для нескольких пользователей, входящих в одну группу как локальную, так и доменную, пропишите `subject.isInGroup("<название_группы>")`.

  Например, для локальной группы **local**, в которую входят пользователи *user1*, *user2* и *user3*, указывается правило вида `subject.isInGroup("local")`; для доменной группы, в которую входят пользователи *dom_user1*, *dom_user2* и *dom_user3*, указывается правило вида `subject.isInGroup("пользователи домена")`. По желанию для конкретных пользователей домена, которым необходимо настроить доступ или правило, можно создать отдельную группу и поместить в неё нужных пользователей, в таком случае в правиле следует прописать `subject.isInGroup("<название_новой_отдельной_группы_доменных_пользователей>")`.

2. Наполним **/etc/polkit-1/rules.d/99-networkmanager.rules** следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (action.id == "org.freedesktop.NetworkManager.settings.modify.system" && subject.isInGroup("xgrp"))
{ return polkit.Result.YES; };
});
```

3. Создадим системную группу **xgrp** (если её ещё нет):

```
groupadd -r xgrp
```

4. Добавим пользователя в группу **xgrp**:

```
gpasswd -a <имя_пользователя> xgrp
```

5. Перезапустим политики *Polkit*:

```
systemctl restart polkit
```

Монтирование устройств с запросом пароля

Рассмотрим пример создания правила, разрешающего пользователю выполнять монтирование и извлечение устройств с запросом пароля (при указании **polkit.Result.AUTH_SELF** — будет запрошен пароль текущего пользователя, **polkit.Result.AUTH_ADMIN** — администратора). Также рассмотрим добавление записи в системный журнал при подключении съемного устройства о том, какое устройство было подключено и каким пользователем.

1. Наполним **/etc/polkit-1/rules.d/99-udisk2_mount.rules** следующим содержимым:

```
polkit.addRule(function(action, subject)
{
polkit.log("action "+ action);
polkit.log("subject "+ subject);
if (action.id == "org.freedesktop.udisks2.filesystem-mount-system")
{
return polkit.Result.AUTH_SELF;
};
if (action.id == "org.freedesktop.udisks2.filesystem-mount")
{
return polkit.Result.AUTH_SELF;
};
if (action.id == "org.freedesktop.udisks2.filesystem-mount-other-seats")
{
return polkit.Result.AUTH_SELF;
};
});
```

2. Перезапустим политики Polkit:

```
systemctl restart polkit
```

При монтировании USB-диска в системном журнале появятся записи:

```
action [Action id='org.freedesktop.udisks2.filesystem-mount' device='/dev/sdb1' polkit.message='Authentication is required to mount
$(drive)' partition.type='0x0b' partition.flags='0x00000000' drive='Kingston DataTraveler 3.0 (/dev/sdb1)' drive.revision='PMAP'
partition.number='1' partition.uuid='cc06b6d9-01' drive.serial='E0D55EA574BEE52129D21523' id.type='vfat' id.version='FAT32'
polkit.gettext_domain='udisks2' id.uuid='9BFA-18D3' drive.removable.media='thumb' drive.vendor='Kingston' drive.removable='true'
id.usage='filesystem' drive.removable.bus='usb' drive.model='DataTraveler 3.0']
```

Таким образом, в системном журнале зарегистрировано, что usb-диск с серийным номером *E0D55EA574BEE52129D21523* был подключен пользователем test.

Просмотреть факты подключения конкретного носителя можно, выполнив команду:

```
journalctl | grep "drive.serial='E0D55EA574BEE52129D21523'"
```

Разрешение монтирования определённых usb-flash накопителей

Создаём файл **/etc/polkit-1/rules.d/30-mount.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject) {
polkit.log("action "+ action);
if (action.id == "org.freedesktop.udisks2.filesystem-mount")
{
if (action.lookup("drive.serial") == "04GS1F3LBIBDWU05" || action.lookup("drive.serial") == "E0D55EA574BEE52129D21523 ")
return polkit.Result.YES;
else return polkit.Result.NO;
};
});
```

Во втором правиле можно указать:

- **AUTH_ADMIN** – разрешено с вводом пароля администратора;
- **NO** – не разрешено вообще.

В данном примере разрешается монтирование usb-flash-накопителей с файловой системой "**FAT32**" или серийным номером "**E0D55EA574BEE52129D21523**".

Основной список доступных параметров вы можете получить при подключении usb-flash-накопителя и просмотре содержимого журнала:

```
journalctl |grep "org.freedesktop.udisks2.filesystem-mount-system"
```

Или в статусе сервиса политик *Polkit*:

```
systemctl status polkit
```

Изменение Network Manager только для администратора

Создаём файл **/etc/polkit-1/rules.d/60-sysvinit-nm.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject) {
if (action.id=="org.freedesktop.NetworkManager.settings.modify.system")
{
return polkit.Result.AUTH_ADMIN;
}
});
```

Polkit-правило разрешающее вносить изменения в утилиту управления принтерами без запроса пароля

Создайте файл **/etc/polkit-1/rules.d/40-allow-printers.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (action.id == "org.opensuse.cupspkhelper.mechanism.all-edit") {
return polkit.Result.YES;
}
});
```

Ниже рассмотрено создание polkit-правила для **группы пользователей**, которое разрешает пользователям указанной группы вносить изменения в настройки утилиты по управлению принтерами (system-config-printer).
Создайте файл **/etc/polkit-1/rules.d/40-allow-changing-printers.rules** со следующим содержимым:

```
polkit.addRule(function(action, subject)
{
if (action.id == "org.opensuse.cupspkhelper.mechanism.all-edit" && subject.isInGroup("users"))
{
return polkit.Result.YES;
}
});
```

Указанная в созданном правиле группа **users** используется в качестве примера. При настройке правила необходимо указать название **вашей** группы или имени пользователя в зависимости от требований:

- если необходимо изменить поведение политики для одного конкретного пользователя, пропишите `subject.user == "<имя_пользователя>"`,
- если необходимо изменить поведение политики для нескольких пользователей, входящих в одну группу как локальную, так и доменную, пропишите `subject.isInGroup("<название_группы>")`.

  Например, для локальной группы **local**, в которую входят пользователи *user1*, *user2* и *user3*, указывается правило вида `subject.isInGroup("local")`; для доменной группы, в которую входят пользователи *dom_user1*, *dom_user2* и *dom_user3*, указывается правило вида `subject.isInGroup("пользователи домена")`. По желанию для конкретных пользователей домена, которым необходимо настроить доступ или правило, можно создать отдельную группу и поместить в неё нужных пользователей, в таком

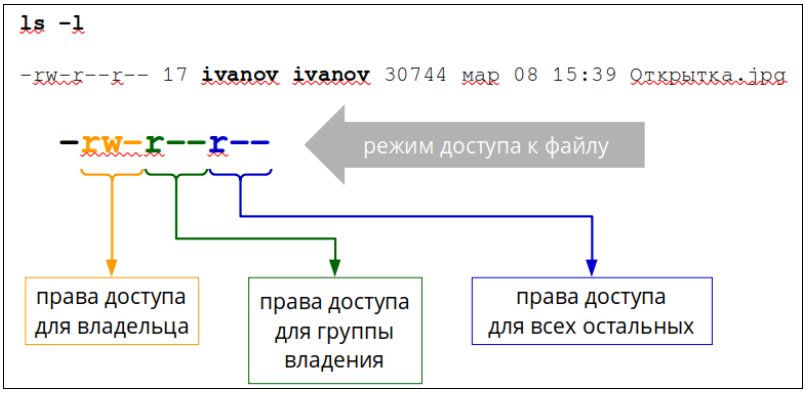
случае в правиле следует прописать `subject.isInGroup("<название_новой_отдельной_группы_доменных_пользователей>")`.

Списки контроля доступа ACL

Списки контроля доступа
Настройка списков доступа
Маска эффективных прав

Для того чтобы получить доступ к файлам в РЕД ОС, используются разрешения, которые назначаются трем объектам — *владельцу*, *группе* и *другим пользователям*.

Просмотреть текущие права доступа можно, используя команду `ls -l`. Она выведет таблицу файлов в каталоге с некоторыми параметрами.



Управление обычными правами доступа возможно как из графического интерфейса, так и через консоль. Но есть расширенные права доступа, которые через графический интерфейс недоступны.

Списки контроля доступа

Для реализации сложных структур прав доступа на файловых системах в РЕД ОС используются расширенные права — **ACL** (*access control list* — списки контроля доступа), которые дают бóльшую гибкость, чем стандартный набор полномочий.

Поддержка **ACL** на файловых системах **ext4** и **XFS** включена по умолчанию. При необходимости можно отключить поддержку списков доступа, указав для выбранной файловой системы опцию «**noacl**» в файле **/etc/fstab**.

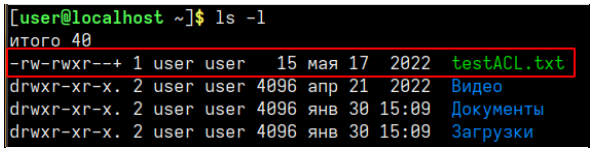
Система списков доступа **ACL** предоставляет дополнительные функциональные возможности ОС. **НО** у нее есть один недостаток — не все утилиты ее поддерживают. Следовательно, можно потерять настройки **ACL** при копировании или перемещении файлов, а программное обеспечение для резервного копирования может не выполнить резервное копирование настроек **ACL**.

Вы можете подробнее ознакомиться с настройкой списков контроля доступа **ACL**, просмотрев наши обучающие видео:

- на **RuTube** — Списки контроля доступа ACL (Access Control List);
- в **Яндекс.Дзен** — Списки контроля доступа ACL (Access Control List);
- в **VK Видео** — Списки контроля доступа ACL (Access Control List).

На наших каналах вы также сможете найти много другой полезной информации.

Если у файла или каталога установлены **ACL**, то в листинге будет отображаться знак «**+**». Команда `ls -l` не показывает никаких существующих **ACL**, она просто показывает «**+**» после списка разрешений, который указывает, что списки **ACL** применяются и к файлу.



Попробуем сделать копию файла и убедимся, что настройки **ACL** при этом не копируются:

```
cp testACL.txt testACLcopy.txt
ls -l
```

```
[user@localhost ~]$ cp testACL.txt testACLcopy.txt
[user@localhost ~]$ ls -l
итого 44
-rw-rwxr--. 1 user user   15 янв 30 16:07  testACLcopy.txt
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACL.txt
drwxr-xr-x. 2 user user 4096 апр 21  2022  Видео
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Документы
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Загрузки
```

При работе с ACL нужно быть внимательнее, т.к. не все программы могут использовать ACL. Заметим, что для копирования файла с сохранением ACL необходимо использовать ключ **-p** для команды `cp`:

```
cp -p testACL.txt testACLcopy2.txt
```

```
[user@localhost ~]$ cp -p testACL.txt testACLcopy2.txt
[user@localhost ~]$ ls -l
итого 52
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACLcopy2.txt
-rw-rwxr--. 1 user user   15 янв 30 16:07  testACLcopy.txt
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACL.txt
drwxr-xr-x. 2 user user 4096 апр 21  2022  Видео
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Документы
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Загрузки
```

Чтобы увидеть текущие настройки ACL, потребуется команда `getfacl`. Просмотрим установленные настройки на файле без ACL и сравним вывод с командой `ls -l`:

```
getfacl testACLcopy.txt
ls -l testACLcopy.txt
```

```
[user@localhost ~]$ getfacl testACLcopy.txt
# file: testACLcopy.txt
# owner: user
# group: user
user::rw-
group::rwx
other::r--

[user@localhost ~]$ ls -l testACLcopy.txt
-rw-rwxr--. 1 user user 15 янв 30 16:07 testACLcopy.txt
```

Права доступа отображаются по-разному, но значения соответствующих полей одинаковы.

Попробуем посмотреть настройки ACL-файла с установленными списками доступа, сравним вывод с командой `ls -l`:

```
getfacl testACL.txt
ls -l testACL.txt
```

```
[user@localhost ~]$ getfacl testACL.txt
# file: testACL.txt
# owner: user
# group: user
user::rw-
user:test:r-x
group::rw-
mask::rwx
other::r--

[user@localhost ~]$ ls -l testACL.txt
-rw-rwxr--+ 1 user user 15 мая 17  2022 testACL.txt
```

Команда `ls` не выводит имя второго владельца файла и его права доступа к файлу, хотя второй владелец присутствует, как показывает команда `getfacl`. Также для файла теперь присутствует поле `mask`, которое определяет максимальные права для добавляемых полей. В данном примере видно, что можно установить права на чтение, запись и выполнение.

Настройка списков доступа

Для установки и настройки списков доступа предназначена команда `setfacl`. Она имеет простой формат.

Синтаксис команды:

```
setfacl [<опции>] <ключ> <список_правил> <объект>
```

Опции:

- **-b** — удаляет все ACL права с объекта, сохраняя основные права;
- **-k** — удаляет с объекта ACL по умолчанию;
- **-d** — устанавливает ACL по умолчанию на объект, т. е. наследуемых прав;
- **-R** — рекурсивное назначение (удаление) прав.

Ключи:

- **--set** — устанавливает новые указанные права, удаляя все существующие;
- **-m** — изменяет указанные ACL на объекте, сохраняя существующие;
- **-x** — удаляет указанные ACL с объекта, стандартные права не изменяются.

Ниже приведено несколько примеров списков правил, устанавливаемых командой setfacl:

- **u:<uid>:<права>** — назначение ACL для доступа заданному пользователю (здесь можно указать имя или UID пользователя);
- **g:<gid>:<права>** — назначение ACL для доступа заданной группе (здесь можно указать имя или GID группы);
- **o:<права>** — назначение ACL для доступа пользователям, не включённым в группу владельцев файлового объекта («все остальные»);
- **m:<права>** — назначение маски эффективных прав.

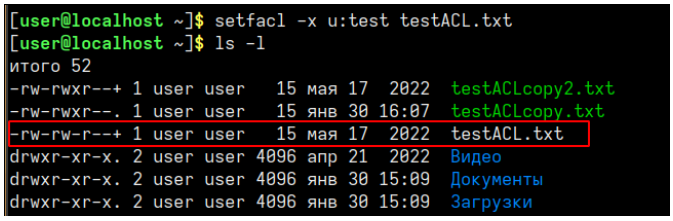
Например, команда setfacl -m u:test:r-x testACL.txt дает разрешения пользователю **test** для файла **testACL.txt**, не делая его владельцем и не изменяя назначение текущего владельца. Иначе говоря, пользователь **test** будет иметь права на этот файл как владелец, только со своими особенными правами доступа.

Команда удаления ACL для пользователя выглядит следующим образом:

```
setfacl -x u:test testACL.txt
```

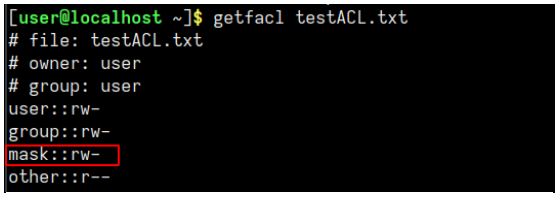
Проверим, удалились ли сведения ACL:

```
ls -l
```



Знак «**+**» все еще отображается, значит сведения ACL ещё действуют. Проверим, какие сведения ACL привязаны к файлу, выполнив команду:

```
getfacl testACL.txt
```



Вывод команды показывает, что применен параметр mask, удалим его командой:

```
setfacl -x m testACL.txt
```

Проверяем, осталась ли запись ACL у файла:

```
ls -l
```

```
[user@localhost ~]$ setfacl -x m testACL.txt
[user@localhost ~]$ ls -l
итого 48
-rw-rwxr--+ 1 user user   15 мая 17  2022  testACLcopy2.txt
-rw-rwxr--. 1 user user   15 янв 30 16:07  testACLcopy.txt
-rw-rw-r--. 1 user user   15 мая 17  2022  testACL.txt
drwxr-xr-x. 2 user user 4096 апр 21  2022  Видео
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Документы
drwxr-xr-x. 2 user user 4096 янв 30 15:09  Загрузки
```

Знак «**+**» у файла **testACL.txt** теперь отсутствует, значит сведения ACL удалены полностью.

Маска эффективных прав

Маска эффективных прав задает максимальные права доступа для всех пользователей, за исключением владельца и групп. Установка маски представляет собой самый быстрый путь изменения фактических (эффективных) прав доступа всех пользователей и групп. Например, маска (**r - -**) показывает, что пользователи и группы не могут иметь больших прав, чем просто чтение, даже если им назначены права доступа на чтение и запись.

Рассмотрим пример, где установим максимальные права для пользователя **test**:

```
setfacl -m u:test:rwx testACL.txt
```

Затем зададим маску эффективных прав:

```
setfacl -m m:r-- testACL.txt
```

Права на файл устанавливаются в соответствии с выполняемой командой, но маска, установленная как **r--**, лишает разрешения на запись и запуск всех владельцев, кроме основного. Это и отображает появившаяся запись:

```
[user@localhost ~]$ setfacl -m u:test:rwx testACL.txt
[user@localhost ~]$ setfacl -m m:r-- testACL.txt
[user@localhost ~]$ getfacl testACL.txt
# file: testACL.txt
# owner: user
# group: user
user::rw-
user:test:rwx                   #effective:r--
group::rw-                      #effective:r--
mask::r--
other::r--
```

Для отмены маски ее следует установить в значение **rwx**.

Для удаления параметров ACL необходимо выполнить команду:

```
setfacl -b testACL.txt
```

```
[user@localhost ~]$ setfacl -b testACL.txt
[user@localhost ~]$ getfacl testACL.txt
# file: testACL.txt
# owner: user
# group: user
user::rw-
group::r--
other::r--
```

Теперь вы можете использовать списки доступа ACL для более гибких настроек прав доступа к вашим данным.

Ограничение полномочий пользователей по использованию виртуальных терминалов

Ограничение полномочий пользователей по использованию виртуальных терминалов можно настроить следующим образом:

Перейдите в сеанс пользователя **root**:

```
su -
```

и добавьте строку в файл **/etc/security/limits.conf**:

```
petrov hard maxlogins 2
```

Добавить строку можно следующей командой:

```
echo "petrov hard maxlogins 2" >> /etc/security/limits.conf
```

где **petrov** - имя пользователя, которому необходимо ограничить число запускаемых виртуальных терминалов.

Затем для ограничения количества запускаемых виртуальных терминалов **для группы пользователей** добавьте в файл **/etc/security/limits.conf** следующую строку:

```
@users hard maxlogins 2
```

где **@users**- это название группы пользователей (для обозначения группы перед её названием используется символ '**@**').

После добавления правила, ограничивающего число сеансов для пользователя *petrov* равным 2, при попытке открыть 3 сеанс в виртуальном терминале возникает ошибка вида:

```
Too many logins for 'petrov'.

Permission denied
```

Для ограничения количества допустимых **tty** (в том числе и отключение их) для всех пользователей, следует изменить содержимое файла **/etc/systemd/logind.conf**:

```
nano  /etc/systemd/logind.conf
```

раскомментировать строку и указать число 1:

```
NAutoVTs=1
```

после перезагрузки доступ к остальным **tty** будет закрыт, вы увидите только черный экран.

Шифрование дисков и отдельных файлов

Шифрование дисков с помощью cryptsetup
Шифрование файлов средствами gpg

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с возможностью шифрования дисков и отдельных файлов, просмотрев наши обучающие видео:

- на **RuTube** — Шифрование дисков и отдельных файлов;
- в **Яндекс.Дзен** — Шифрование дисков и отдельных файлов;
- в **VK Видео** — Шифрование дисков и отдельных файлов.

На наших каналах вы также сможете найти много другой полезной информации.

Шифрование дисков с помощью cryptsetup

Создается файл размером 20 Гб (размер указывается под нужды пользователя) под зашифрованный диск - на примере домашней директории пользователя *user*:

```
truncate -s 20G /home/.user
chown user:user /home/.user
```

Создайте loop-устройство:

```
losetup /dev/loop0 /home/.user
```

Инициализируем зашифрованный диск (потребуется дважды ввести пароль):

```
cryptsetup -h sha256 -c aes-xts-plain64 -s 512 luksFormat /dev/loop0
```

Обязательно - указать соглашение в верхнем регистре **YES**.

```
Are you sure? (Type uppercase yes): YESEnter passphrase:
Verify passphrase:
```

Откройте зашифрованный диск:

```
cryptsetup luksOpen /dev/loop0 user_home
```

В результате появится устройство **/dev/mapper/user_home**. Создаем на нем ФС:

```
mkfs.ext4 /dev/mapper/user_home
```

Примонтируйте зашифрованный диск:

```
mount /dev/mapper/user_home /mnt
```

Измените права на файловой системе:

```
chown -R user:user /mnt
```

Скопируйте содержимое домашнего каталога. Затем отмонтируйте зашифрованный диск:

```
umount /mnt
```

Закройте зашифрованный диск:

```
cryptsetup luksClose user_home
```

Отсоедините loop-устройство:

```
losetup -d /dev/loop0
```

Теперь производится архивация и удаление содержимого **/home/user**, затем монтирование в него зашифрованного диска. Если все работает нормально — бэкап удаляется.

Скрипт **/home/mount.sh** для автоматизации монтирования:

```
#!/bin/sh
set -e
losetup /dev/loop0 /home/.user
cryptsetup luksOpen /dev/loop0 user_home
mount /dev/mapper/user_home /home/user
```

Сделайте скрипт исполняемым:

```
chmod +x /home/mount.sh
```

Выполните скрипт:

```
/home/mount.sh
```

Скрипт **/home/umount.sh**, выполняющий обратные действия:

```
#!/bin/sh
set -e
umount /home/user
cryptsetup luksClose user_home
losetup -d /dev/loop0
```

Сделайте скрипт исполняемым:

```
chmod +x /home/umount.sh
```

Выполните скрипт:

```
/home/umount.sh
```

Когда оригинальных данных на диске не осталось, можно заполнить свободное место мусором (процесс долгий):

```
cd /home
dd if=/dev/urandom of=./random.tmp bs=10M count=6300
sync
rm random.tmp
```

Наконец, чтобы временные файлы (те же черновики электронных писем) писались на зашифрованный раздел, в **/home/user/.bashrc** следует дописать:

```
export TMPDIR=/home/user/temp
mkdir -p $TMPDIR
```

Шифрование файлов средствами gpg

Сгенерируйте свой личный ключ для шифрования файлов:

```
gpg --gen-key
```

От вас потребуется ввести имя пользователя, почту и придумать пароль.

Просмотр списка ключей доступен командами:

```
gpg --list-keys
gpg --list-secret-keys
```

Проверка отпечатка, что вы правильно сможете обратиться к ключу:

```
gpg --fingerprint 'user_name'
```

Зашифровывание содержимого каталога при помощи ключа:

```
tar -c -f- /home/user/Документы/* | gpg -e -c -r 'user_name'> file.tar.gpg
```

Расшифровывание - потребуется ввести пароль ключа:

```
gpg -d -o ./file.tar ./file.tar.gpg
```

Защитное преобразование файлов и каталогов по ГОСТ Р 34.12–2015

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** caja-extension-actions-0.9-1

Для шифрования файлов по ГОСТ необходимо наличие в системе пакета **caja-extension-actions** последней версии.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

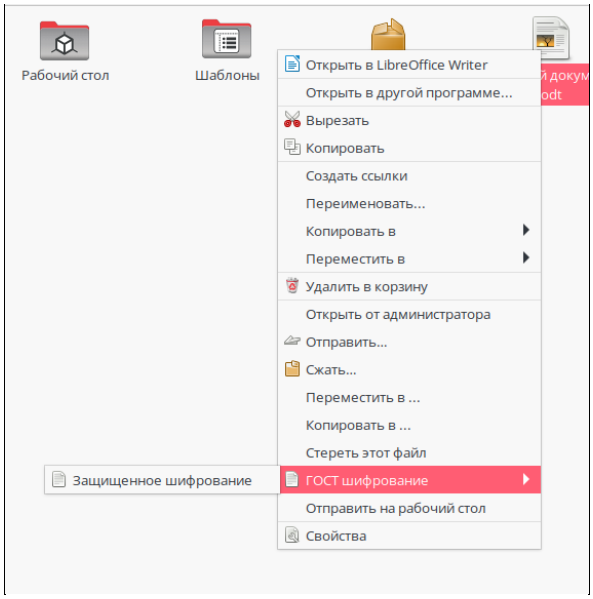
```
dnf install caja-extension-actions
```

Затем выполните:

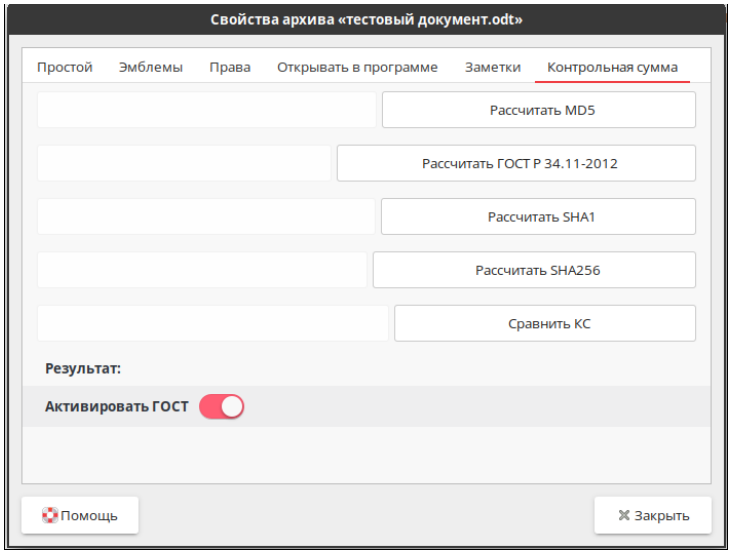
```
caja -q
```

Следующим шагом необходимо проверить активированное ГОСТ шифрование.

Если в контекстном меню файла появилось поле «**ГОСТ шифрование**», тогда дополнительных действий делать не нужно.



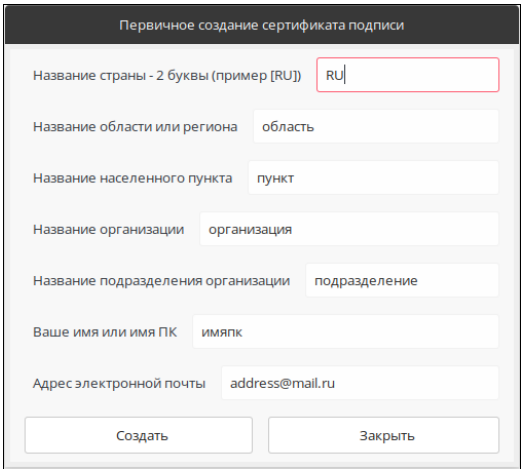
Если данное поле отсутствует, необходимо выбрать «**Свойства**» файла, перейти на вкладку «**Контрольная сумма**» и активировать ГОСТ при помощи тумблера.



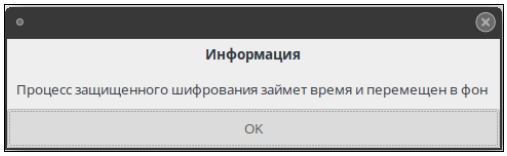
После этого необходимо создать сертификат подписи.

Данный сертификат будет расположен по пути **~/.gost**, и для расшифровывания файлов данный каталог должен быть выгружен другому пользователю.

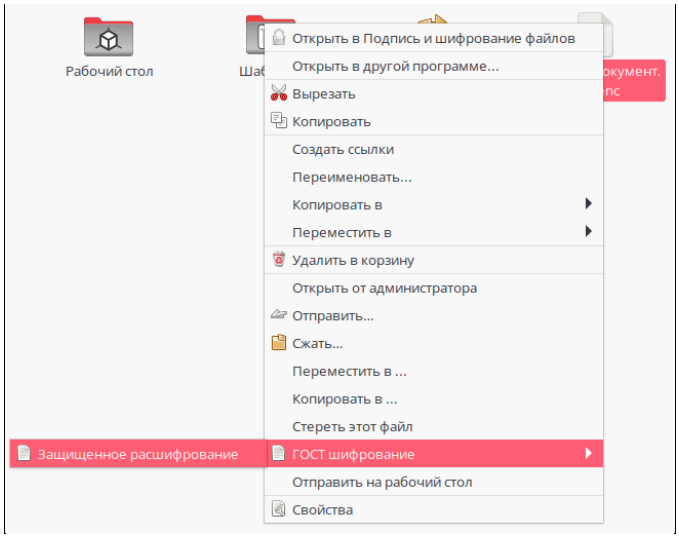
В ином случае будет выполнена реинициализация создания сертификата, который будет не приемлем для расшифровывания.



Далее вы увидите уведомляющее окно, дождитесь завершения процесса и у вас появится зашифрованный файл с расширением **.enc**.



Для расшифрования файла вам потребуется вызвать ПКМ контекстное меню файла с расширением **.enc** и, соответственно, выбрать пункт «**ГОСТ шифрование**» – «**Защищенное расшифрование**».



При успешном завершении операции вы увидите ваш расшифрованный файл.

Безопасное удаление файлов

shred

wipe

Дополнительные утилиты

srm

sfill

sswap

Удаление файлов и каталогов с помощью команд **rm** и **find** не гарантирует того, что удаленные объекты не могут быть восстановлены. Для безопасного гарантированного удаления файлов и каталогов без возможности восстановления необходимо использовать утилиты **shred** и **wipe**.

Вы можете подробнее ознакомиться с работой утилит, предназначенных для безопасного удаления файлов, просмотрев наши обучающие видео:

- на **RuTube** — Полное и необратимое удаление данных с дисков;
- в **Яндекс.Дзен** — Полное и необратимое удаление данных с дисков;
- в **VK Видео** — Полное и необратимое удаление данных с дисков.

На наших каналах вы также сможете найти много другой полезной информации.

shred

shred — переписывает несколько раз указанные файлы для того, чтобы сделать более сложным восстановление.

Синтаксис:

```
shred [<КЛЮЧ>] <ФАЙЛ>
```

Ключи:

- `-f`, `--force` — изменять права, разрешая запись, если необходимо;
- `-n`, `--iterations=N` — выполнить **N** циклов перезаписи содержимого (по умолчанию **3**). На современных устройствах хранения одного цикла перезаписи (`N=1`) должно быть достаточно, однако минимально рекомендуемое количество циклов перезаписи - **3**. При `N > 25` все внутренние шаблоны перезаписи будут использованы хотя бы один раз;
- `--random-source=<ФАЙЛ>` — получать случайные числа из **<ФАЙЛА>** (по умолчанию **/dev/urandom**);
- `-s`, `--size=N` — очистить **N** байт (возможны суффиксы вида **K**, **M**, **G**);
- `-u` — освобождать и удалять файл после перезаписи;
- `--remove[=<способ_удаления>]` — подобно `-u`, но задаётся способ удаления;
- `-v`, `--verbose` — показывать ход выполнения;
- `-x`, `--exact` — не округлять размеры файлов до следующего целого блока;
- `-z`, `--zero` — перезаписать в конце нулями, чтобы скрыть измельчение;
- `--help` — показать справку и выйти;
- `--version` — показать информацию о версии и выйти.

wipe

wipe — это небольшая программа для безопасного стирания файлов с магнитных носителей.

Синтаксис:

```
wipe [<опции>] файлы...
```

Опции:

- `-a` — прервать при ошибке;
- `-b <buffer-size-lg2>` — установить размер индивидуального буфера ввода/вывода указав его логарифм по основанию 2. Могут быть выделены до 30 этих буферов;

- `-c` — делать `chmod()` на защищённых от записи файлах;
- `-D` — следовать символическим ссылкам (конфликтует с `-r`);
- `-e` — использовать точный размер файла: не округлять размер файла для стирания возможного мусора, остающегося на последнем блоке;
- `-f` — форсировать, т. е. не спрашивать подтверждения;
- `-F` — не пытаться стирать имена файлов;
- `-h` — показать справку;
- `-i` — информативный (подробный) режим;
- `-k` — сохранить файлы, т. е. не удалять их после перезаписи,
- `-l <длина>` — установить длину стирания на `<длину>` байт, где `<длина>` — это целое число, за которым следует **K** (Kilo:1024), **M** (Mega:K^2) или **G** (Giga:K^3);
- `-M (l|r)` — установить алгоритм `PRNG` для заполнения блоков (и порядка проходов):
  - `l` — использовать вызов библиотеки `random()`;
  - `a` — использовать алгоритм шифрования `arcfour`.
- `-o <сдвиг>` — установить сдвиг очистки на `<сдвиг>`, где `<сдвиг>` имеет тот же формат, что и `<длина>`;
- `-P <проходы>` — установить количество проходов для очистки имени файла. По умолчанию **1**;
- `-Q <количество>` — установить количество проходов для быстрой очистки;
- `-q` — быстрая очистка, менее безопасная, по умолчанию **4 случайных** прохода;
- `-r` — рекурсия по каталогам — по символическим ссылкам не будет переходов;
- `-R` — установить устройство рандомизации (или команду сидов рандомизации `-S c`);
- `-S (r|c|p)` — метод рандомизации сидов:
  - `r` — считывать с устройства рандомизации (надёжно);
  - `c` — считывать из вывода команды рандомизации сидов;
  - `p` — использовать `pid()`, `clock()` и т.д. (самый слабый вариант).
- `-s` — тихий режим — подавлять весь вывод;
- `-T <попытки>` — установить максимальное число попыток для свободного поиска имени файла, по умолчанию **10**;
- `-v` — показать информацию о версии;
- `-Z` — не пытаться стирать имя файла.

Дополнительные утилиты

Также для безопасного удаления данных можно использовать утилиты пакета **secure-delete**: **srm**, **sfill**, **sswap**, которые безопасно очищают файлы, диски, раздел подкачки и память.

srm

srm выполняет безопасную перезапись/переименование/удаление целевого файла(ов).

Синтаксис:

```
srm [<опции>] <файл_1> <файл_2> ...
```

Опции:

- `-d` — игнорировать специальные файлы "." и "..";
- `-f` — быстрый (и небезопасный режим): без **/dev/urandom**, без режима синхронизации;
- `-r`, `-R`, `--recursive` — рекурсивный режим, удаляет содержимое директорий;
- `-v` — подробный режим;
- `-V` — показать информацию о версии.

sfill

sfill выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов (**inode**) указанного каталога.

Синтаксис:

```
sfill [-fillvz] <каталог>
```

Опции:

- `-f` — быстрый (и небезопасный режим): без **/dev/urandom**, без режима синхронизации;
- `-i` — стирает только индексные дескрипторы в указанной директории;
- `-l` — стирает только пространство, без индексных дескрипторов;
- `-l` — снижение уровня безопасности (используйте дважды для включения небезопасного режима);
- `-v` — подробный режим;
- `-z` — последний проход заполняет нулями вместо рандомных данных.

sswap

sswap делает безопасную перезапись раздела подкачки.

Синтаксис:

```
sswap [-flvz] [-j start] /dev/of_swap_device
```

Опции:

- `-f` — быстрый (и небезопасный режим): без **/dev/urandom**, без режима синхронизации;
- `-j` — при очистке перепрыгнуть через это количество первых байт (по умолчанию **4096**);
- `-l` — снижение уровня безопасности (используйте дважды для включения небезопасного режима);
- `-v` — подробный режим;
- `-z` — последний проход заполняет нулями вместо рандомных данных.

Отключение CD-ROM

Запрет монтирования CD-ROM

Чтобы отключить **CD-ROM**, вам необходимо создать файл **/etc/modprobe.d/usb-storage.conf** и отредактировать его с помощью текстового редактора.

```
sudo nano /etc/modprobe.d/usb-storage.conf
```

Введите следующие строки в файл:

```
install usb-storage /bin/true
```

Вышеупомянутый файл ***.conf** отражает фальшивую установку **CD-ROM**. Сохраните файл с помощью `Ctrl + O`, затем нажмите `Enter`, и выйдите из редактора с помощью `Ctrl + X`.

Запретите чтение/запись/выполнение всем пользователям, кроме **root**, на каталог, в который монтируются **CD-ROM**.

```
sudo chmod -R 700 /run/media
```

Для вступления изменений в силу перезагрузите компьютер.

Возврат возможности подключения

Для того чтобы вернуть возможность монтирования, выполните следующие команды

```
sudo rm -f /etc/modprobe.d/usb-storage.conf
sudo chmod -R 755 /run/media
```

Перезагрузите компьютер.

Ограничение доступа к USB-накопителям

Примеры выбора устройств по определенным свойствам
Запрет автомонтирования с параметром UDISKS_IGNORE
Создание белого списка с параметром UDISKS_IGNORE
Запрет автомонтирования с параметром authorized
Создание белого списка с параметром authorized

Алгоритм создания белого списка USB-флеш-накопителей состоит из 2 этапов:

Вариант 1:

1. Запрет монтирования всех USB-флеш-накопителей
2. Разрешение монтирования некоторых устройств

Вариант 2:

1. Разрешение монтирования некоторых устройств
2. Запрет монтирования всех иных USB-флеш-накопителей

Вы можете подробнее ознакомиться с информацией по ограничению доступа к USB-накопителям, просмотрев наши обучающие видео:

- на **RuTube** — Ограничение доступа к USB-накопителям;
- в **Яндекс.Дзен** — Ограничение доступа к USB-накопителям;
- в **VK Видео** — Ограничение доступа к USB-накопителям.

На наших каналах вы также сможете найти много другой полезной информации.

Примеры выбора устройств по определенным свойствам

Для создания белого списка USB-флеш-накопителей необходимо знать атрибуты накопителя.

1) Определите ваш флеш-накопитель:

```
 ls -l /dev/sd*

brw-rw---- 1 root disk 8, 0 июн 30 12:59 /dev/sda
brw-rw---- 1 root disk 8, 1 июл 22 12:59 /dev/sda1
brw-rw---- 1 root disk 8, 2 июл 22 12:59 /dev/sda2
brw-rw---- 1 root disk 8, 3 июн 30 12:59 /dev/sda3
brw-rw---- 1 root disk 8, 16 июл 22 13:43/dev/sdb # нужная нам строка
brw-rw---- 1 root disk 8, 17 июн 30 13:43 /dev/sdb1
```

2) Проверьте атрибуты (символы после **sd*** должны вводиться в соответствии с вашим выводом команды `ls -l /dev/sd*`):

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром UDISKS_IGNORE

Для отключения автомонтирования USB-флеш-накопителей необходимо создать правило для **udev**.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
```

Флаг `ENV{UDISKS_IGNORE}` отвечает за игнорирование устройства:

- «0» – false;
- «1» - true.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром UDISKS_IGNORE

Выборка разрешения доступа по трем параметрам:

- серийному номеру устройства;
- модели;
- максимальному потребления тока.

Для их определения выполните поочередно команды:

```
udevadm info -a -p /sys/block/sdb | grep serial
udevadm info -a -p /sys/block/sdb | grep product
udevadm info -a -p /sys/block/sdb | grep bMaxPower
```

в выводе будет отображен серийный номер, модель и значение максимального потребления тока:

```
ATTRS{serial}=="04GS1F3LBIBDWU05"
 ATTRS{model}=="Silicon-Power8G "
 ATTRS{bMaxPower}=="200mA"
```

Запишите эти значения в файл правил в качестве разрешающих.

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
 ATTRS{serial}=="04GS1F3LBIBDWU05",ENV{UDISKS_IGNORE}="0"
 ATTRS{product}=="DataTraveler 3.0",ENV{UDISKS_IGNORE}="0"
 ATTRS{bMaxPower}=="200mA",ENV{UDISKS_IGNORE}="0"
```

Здесь:

- **1** - заблокировать все usb-накопители;
- **0** - разрешить накопитель по определенным свойствам.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, находится в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром authorized

Для отключения автомонтирования USB-флеш-накопителей необходимо будет создать правило для **udev** и исполняемый скрипт запрета монтирования USB-флеш-накопителей.

Создайте скрипт:

```
nano /usr/bin/remove_usb.sh
```

```
#!/bin/bash
var=$1
var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
echo 0 > '/sys/bus/usb/devices'$var2'authorized'
```

Измените права на скрипт:

```
chmod +x /usr/bin/remove_usb.sh
```

Параметр **authorized** отвечает за монтирование USB-флеш-накопителя в момент подключения к ПК.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
```

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром authorized

Выборка по серийному номеру устройства:

```
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
```

Выборка по названию модели. Точное название смотрите в выводе команды:

```
 udevadm info -a -p /sys/block/sdb

ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
```

Для удобства, когда полный список параметров устройства известен, можно производить отбор по конкретному параметру:

```
udevadm info -a -p /sys/block/sdb | grep "ATTRS{serial}"
udevadm info -a -p /sys/block/sdb | grep "ATTRS{product}"
```

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ACTION!="add", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}=="usb-storage", RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
LABEL="dont_remove_usb"
```

Логика данного правила отлична от первого варианта. В первом варианте происходила блокировка сразу всех usb флеш-накопителей, а только потом осуществлялось добавление устройств в белый список. В данном (втором) варианте сначала происходит добавление устройств в белый список, а только потом блокирование устройств (добавление в черный список). Такое действие связано с тем, что параметр **authorized** появляется в момент монтирования и, если его значение установить в **0**, то для дальнейшей работы он становится недоступен. Соответственно, сначала требуется проверить, входит ли флеш-накопитель в белый список, и если входит, то разрешить его монтирование.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, отображается в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Настройка протоколирования событий подключения USB-накопителей

Создаем правила для **udev**:

```
nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды

```
#log mount/unmount
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo unmount $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

После выполнения данных действий будут фиксироваться все факты подключения/отключения usb-накопителей.

Настройка принадлежности USB-накопителей

В данной статье будет рассмотрен пример разграничения правил для разных пользователей.

Сначала необходимо создать udev-правило, содержащее разрешения на определенные usb-устройства, по выбранным пользователем параметрам.

```
nano /etc/udev/rules.d/80-alloweduserlist1.rules
```

```
ACTION!="add", GOTO="dont_remove_usb"
 ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
 ATTRS{product}=="USB DISK 2.0",GOTO="dont_remove_usb"
 ENV{DRIVER}=="usb-storage",RUN+="/bin/python3 /usr/local/bin/remove_usb.py $devpath"
 LABEL="dont_remove_usb"
 ENV{DRIVER}=="usb-storage", ENV{UDISKS_AUTO}="0"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="add", RUN+="/bin/systemctl start usb-mount-list1@%k.service"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="remove", RUN+="/bin/systemctl stop usb-mount-list1@%k.service"
```

Затем необходимо создать скрипт для запрета монтирования устройств со следующим содержимым:

```
nano /usr/local/bin/remove_usb.py
```

```
#!/usr/bin/python3
 import os
 import sys
 var = sys.argv[1].strip()
 var2 = os.popen(f"echo {var} | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//'").readlines()[0]
 os.system(f"echo 0 > '/sys/bus/usb/devices{var2.strip()}authorized'")
```

Далее создайте сервис, отвечающий за запуск скрипта, проверяющего список доступных пользователей для данного udev-правила.

```
nano /etc/systemd/system/usb-mount-list1@.service
```

```
[Unit]
 Description=Mount USB Drive on %i

 [Service]
 RemainAfterExit=true
 Type=oneshot
 ExecStart=/usr/bin/python3 /usr/local/bin/usb-mount.py add %i /etc/udev/rules.d/80-alloweduserlist1.rules
 ExecStop=/usr/bin/python3 /usr/local/bin/usb-mount.py remove %i /etc/udev/rules.d/80-alloweduserlist1.rule
```

Следующим этапом формируется список разрешенных пользователей.

Допустимые значения **umask**:

- 0 - rwx - полные права; rw - чтение/запись;
- 2 - r - чтение.

Создайте список разрешенных пользователей (в примере **user1** с правами на чтение) без проверки на группы:

```
mkdir /etc/udevlist
nano /etc/udevlist/userlist1.json
```

```
{"user1": 2}
```

Если необходимо указать несколько пользователей, список указывается в виде `{"user1": 2, "user2": 0, ...}`.

Затем создайте файл соответствия udev-правила со списком разрешенных пользователей:

```
nano /etc/udevlist/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/userlist1.json"}
```

Создайте список разрешенных групп:

```
mkdir /etc/udevlist/group/
nano /etc/udevlist/group/grouplist1.json
```

```
{}
```

Если в правиле необходимо использовать разграничение по группам, список указывается в виде `{"name_group1": 0, "name_group2": 2}`.

После этого создайте файл соответствия udev-правила со списком разрешенных групп:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/group/grouplist1.json"}
```

Создайте файл для других списков, если используются:

```
mkdir /etc/udevlist/otherlists/
nano /etc/udevlist/otherlists/otherlists1.json
```

с содержимым вида:

```
{"others": 7}
```

После этого создайте файл соответствия udev-правила с новым списком:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/otherlists/otherlists1.json"}
```

Затем загрузите скрипт проверки доступа пользователей и монтирования устройств, распакуйте архив и переместите файл скрипта в каталог **/usr/local/bin/**:

```
wget https://redos.red-soft.ru/upload/usb-mount.zip
unzip ./usb-mount.zip -d /usr/local/bin/
```

Для применения настроек перезапустите службы командой:

```
systemctl daemon-reload
```

Настройка учета USB-накопителей

Создаем правила для **udev**:

```
sudo nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды (в примере показан учет **USB** на основе серийного номера):

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add",RUN+="/bin/sh /mnt/logs.sh $devnode %E{ID_SERIAL}"
```

Создаем скрипт для ведения лог файла. Если указать путь **/root/log.txt**, то доступ к файлу лога будет только у пользователя **root**.

```
nano /mnt/logs.sh
```

```
path=$1
 serial=$2
 File="/root/log.txt"
 if ! grep -q "$serial" "$File";
 then
 echo $path $serial $(date)>> /root/log.txt
 fi
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

Ограничение доступа USB-устройств по defines class code

Существует большое количество устройств, имеющих разный *USB defines class code*. Для того чтобы разрешить подключение определенного класса устройств, потребуется применить следующий алгоритм:

1) Создать правило, в котором прописаны разрешенные устройства, а остальные блокируются:

```
nano /etc/udev/rules.d/99-usb-bInterfaceClass.rules
```

Содержимое правила на примере классов для **token**, **HID**, **audio** и **video** устройств:

```
# Allow all TOKEN devices
 ATTR{bInterfaceClass}=="0b",ACTION=="add",GOTO="usb_rules_end"
 # Allow all c
 ATTR{bInterfaceClass}=="03",ACTION=="add",GOTO="usb_rules_end"
 # Allow all AUDIO devices
 ATTR{bInterfaceClass}=="01",ACTION=="add",GOTO="usb_rules_end"
 # Allow all VIDEO devices
 ATTR{bInterfaceClass}=="0e",ACTION=="add",GOTO="usb_rules_end"
 SUBSYSTEM=="usb",ACTION=="add",RUN+="/bin/sh -c '/usr/bin/reject_usb_bInterfaceClass.sh $devpath'"
 LABEL="usb_rules_end"
```

2) Создать скрипт, изменяющий атрибут **authorized** для определенного устройства:

```
nano /usr/bin/reject_usb_bInterfaceClass.sh
```

Содержимое скрипта:

```
#!/bin/bash
 var=$1
 var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
 var3=$(echo $var2 | grep '^/[0-9]-[0-9]$')
 var4=$(echo $var2 | grep '^/[0-9]-[0-9].[0-9]$')
 if [ -z "$var3" ] && [ -z "$var4" ]; then
 echo 0 > '/sys/bus/usb/devices'$var2'/authorized'
 fi
```

Сделайте скрипт исполняемым:

```
chmod +x /usr/bin/reject_usb_bInterfaceClass.sh
```

Перезапустите правила **udev**:

```
sudo udevadm control --reload-rules
```

HUB устройства

Есть устройства, которые системой определяются как **HUB**. В момент редактирования правил и перезагрузки **udev** на **HUB**-устройства, которые находятся в системном блоке/кейсе, влияние оказано не будет, так как они не переподключаются. Зато при перезагрузке ОС они заблокируются и в итоге все подключенные к ним устройства ниже по дереву тоже будут заблокированы. Для корректного редактирования устройств подключенных через **HUB** требуется в правилах разрешить:

```
DRIVER=="hub",ACTION=="add",GOTO="end_usb_rules"
```

либо:

```
ATTR{bInterfaceClass}=="09",ACTION=="add",GOTO="usb_rules_end"
```

Перезапустить правила:

```
udevadm control --reload-rules
```

Утилита по созданию правил для монтирования USB-накопителей

Установка
Полная блокировка всех usb
Назначение личной привязки к UDEV-правилу
Протоколирование событий usb-flash накопителей

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** usb_rules-2.1-1

Утилита **usb_rules** основана на работе с правилами **udev** и системными сервисами **systemd**.

Вы можете подробнее ознакомиться с работой утилиты **usb_rules**, просмотрев наши обучающие видео:

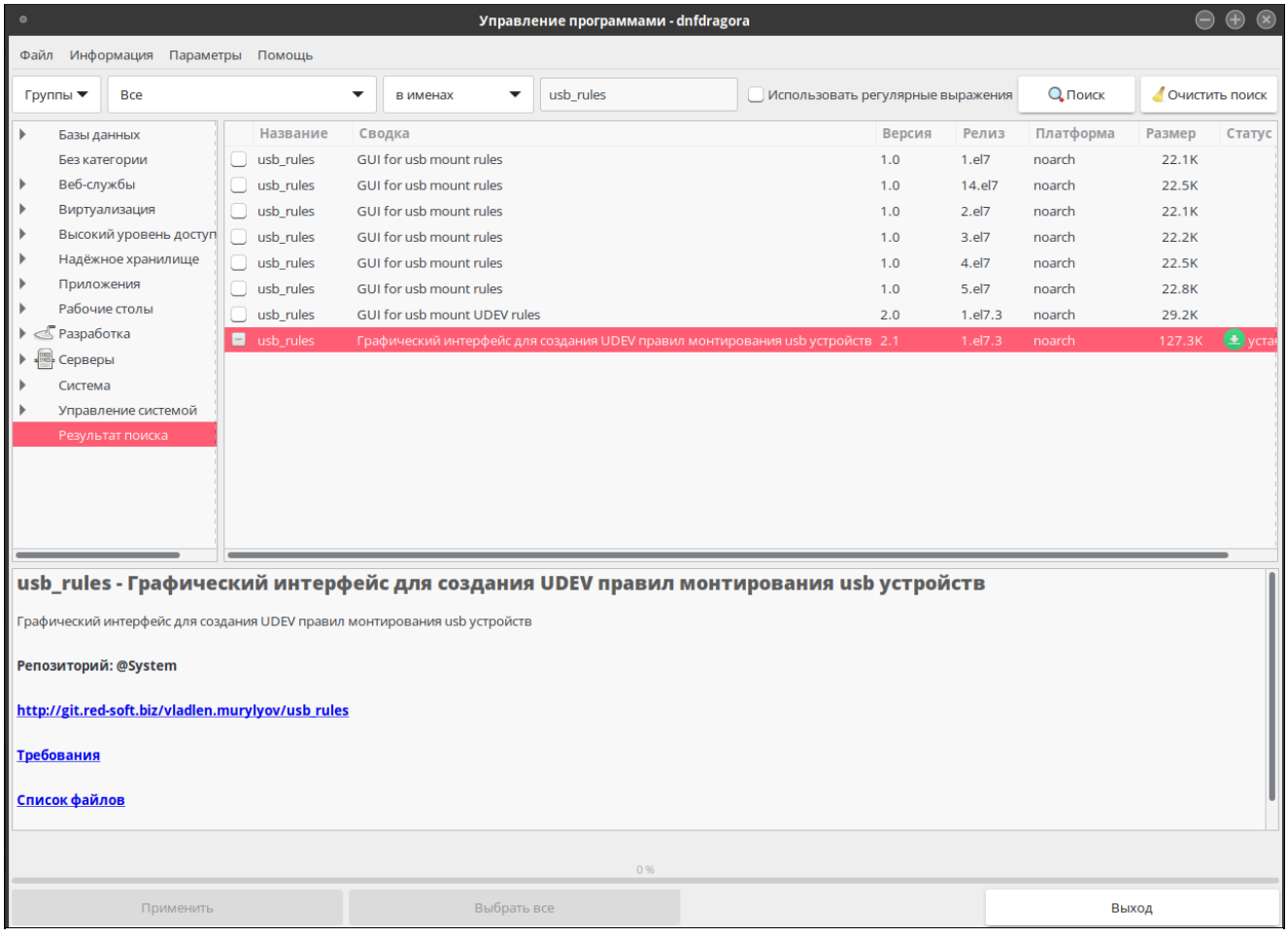
- на **RuTube** — Утилита по созданию правил для монтирования usb-flash накопителей ;
- в **Яндекс.Дзен** — Утилита по созданию правил для монтирования usb-flash накопителей ;
- в **VK Видео** — Утилита по созданию правил для монтирования usb-flash накопителей .

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установка утилиты доступна через пакетный менеджер *dnfdragora* («**Главное меню**» - «**Администрирование**» -«**Управление пакетами dnfdragora**»).

В поисковой строке пакетного менеджера введите название утилиты «**usb_rules**», нажмите «**Enter**» для поиска. Из списка результатов выберите последнюю версию утилиты и нажмите кнопку «**Применить**».



Будет выполнена установка пакета.

Также установка утилиты доступна из терминала. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

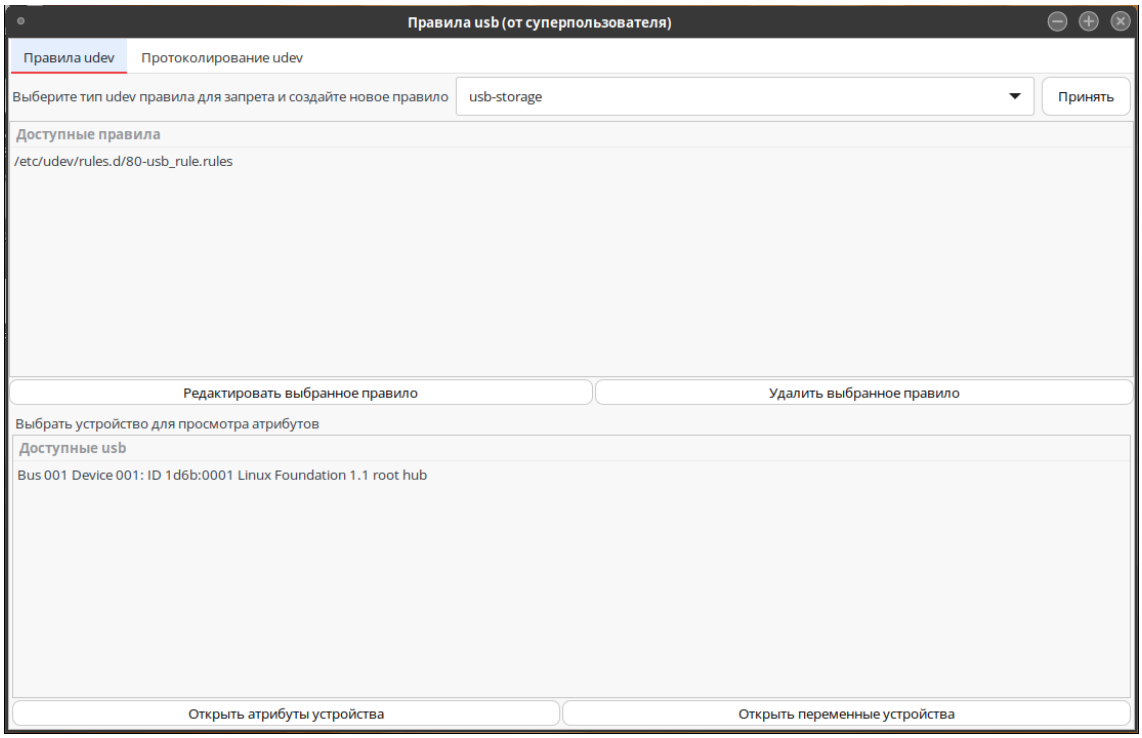
и выполните команду:

```
dnf install usb_rules
```

После установки запуск утилиты доступен с правами пользователя **root** из «**Главного меню**» - «**Параметры**» - «**Настройка ограничения монтирования**» или через терминал с помощью команды:

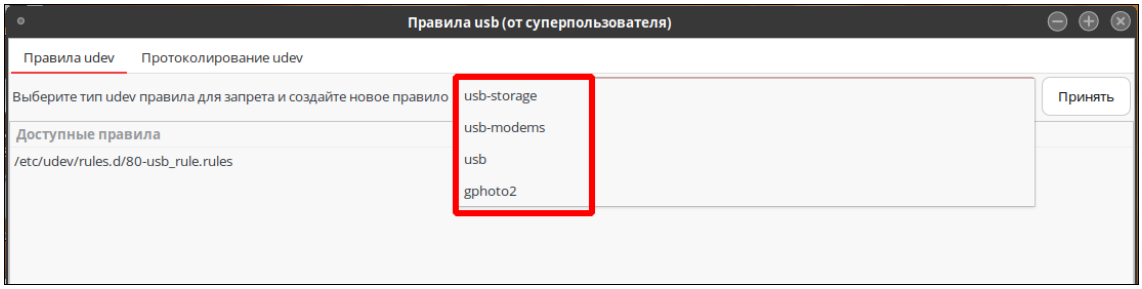
```
usb-rules
```

Стартовое окно утилиты позволяет пользователю ознакомиться с подключенными usb-устройствами и со списком уже созданных правил.



При формировании нового правила пользователю доступны 4 шаблона:

- **usb-storage**;
- **usb-modems**;
- **usb**;
- **gphoto2**.



Каждое из правил отвечает за полную блокировку тех или иных устройств.

Полная блокировка всех usb

Ниже представлено содержимое шаблонов для каждого правила:

```
#type:usb-storage
```

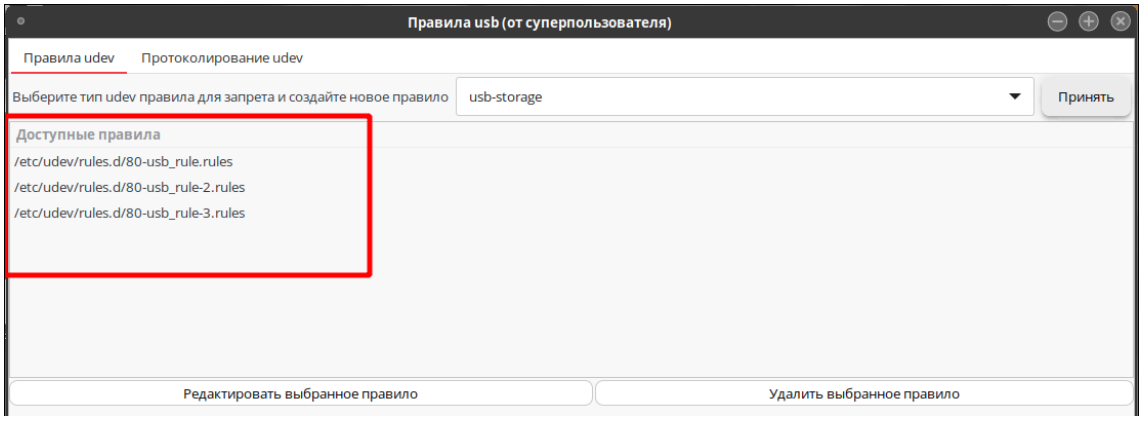
```
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:usb-modems
ACTION!="add", GOTO="dont_remove_usb"
DRIVER!="rndis_host", GOTO="dont_remove_usb"
DRIVER=="rndis_host", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

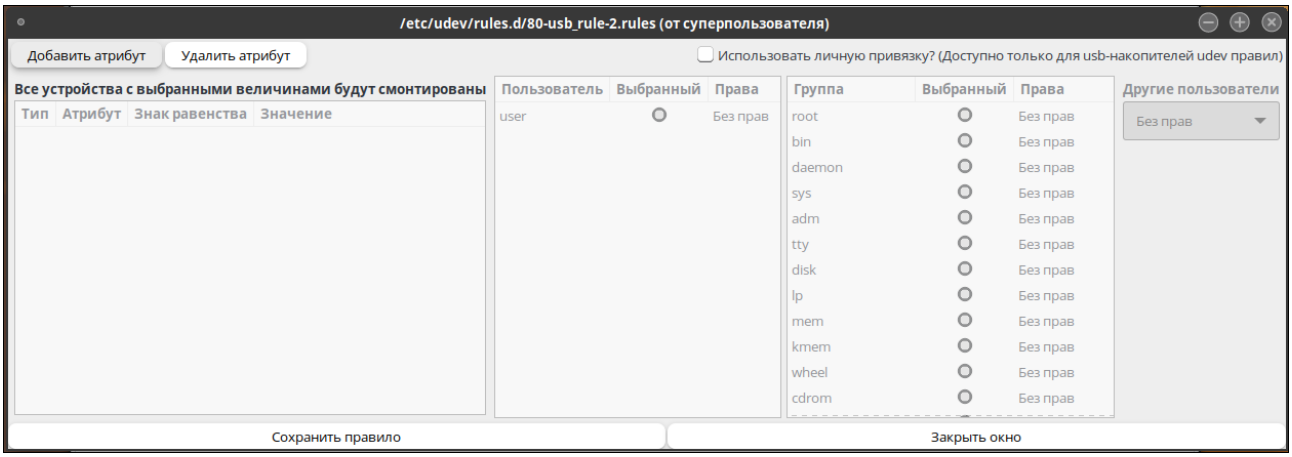
```
#type:usb
ACTION!="add", GOTO="dont_remove_usb"
SUBSYSTEM!="usb", GOTO="dont_remove_usb"
SUBSYSTEM=="usb", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:gphoto2
ACTION!="add", GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}!="PTP",GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}=="PTP",ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

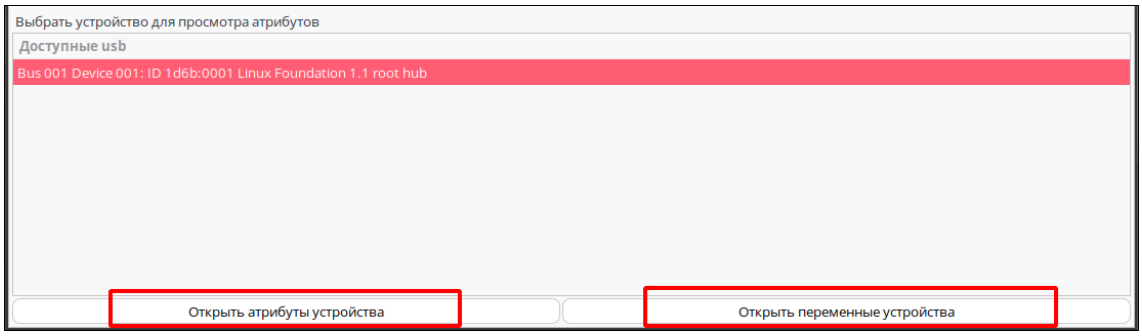
При формировании правила из шаблонного в окне утилиты появляется строка, соответствующая сформированному правилу.



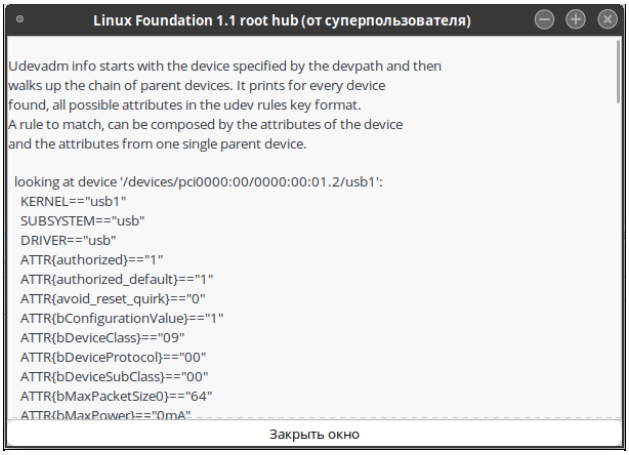
Далее потребуется создать разрешающие монтирование параметры. Для этого необходимо добавить атрибут, который в новом правиле будет отвечать за исключение из блокировки устройств, подходящих под данный параметр. Добавление или удаление таких атрибутов доступно после выбора интересующего правила и нажатия кнопки «**Редактировать правило**».

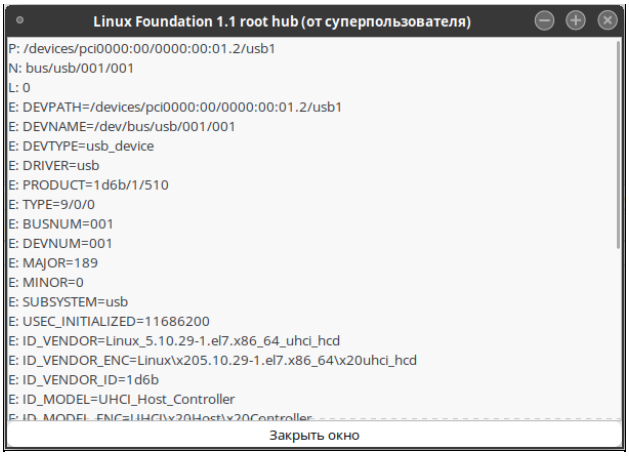


В полях «**Атрибут**» и «**Значение**» необходимо подобрать значения из доступных устройств. Просмотр доступных значений можно осуществить следующим образом:



В результате будут открыты следующие окна:

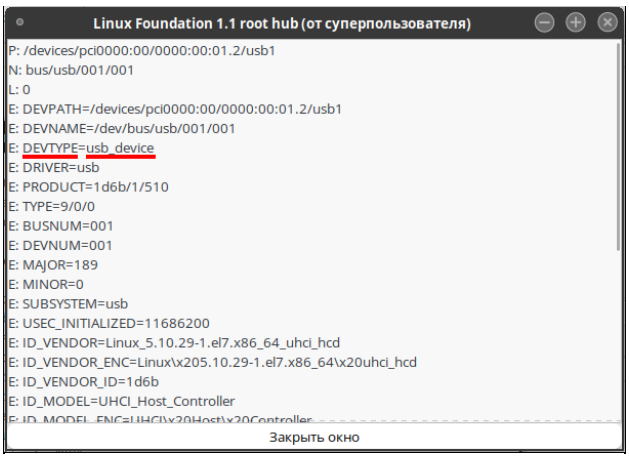




При добавлении пункта **ATTR** следует прописать значение и величины соответствующие:

Значения указываются, соответственно, без фигурных скобок **{}** и без кавычек **""**.

Для указания величин **ENV** следует выбирать величины:

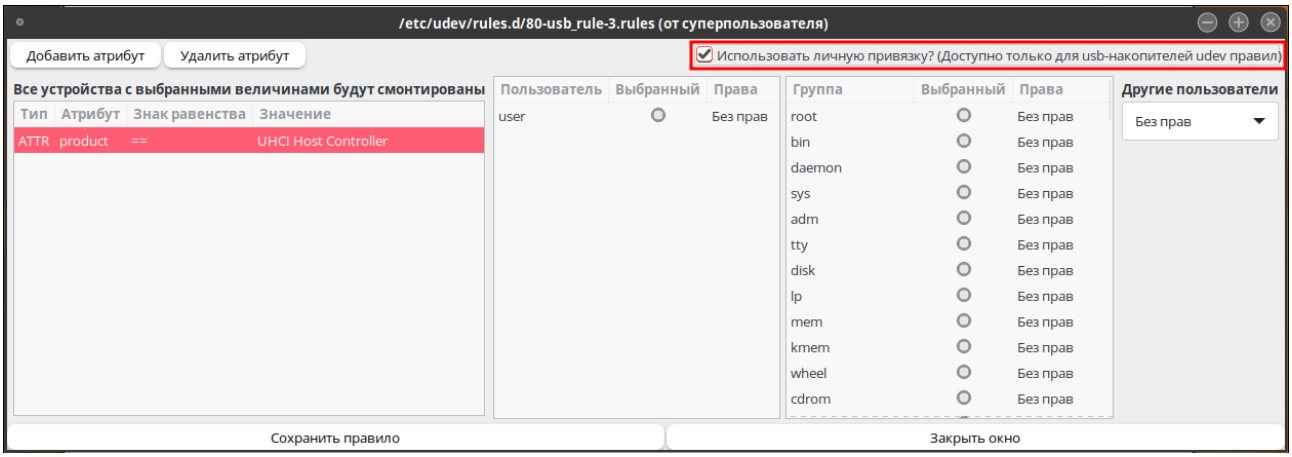


В результате будет сформировано примерно следующее правило **/etc/udev/rules.d/80-usb_rule.rules**:

```
#type:usb-storage
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTR{product}==UHCI Host Controller, GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

Назначение личной привязки к UDEV-правилу

За назначение привязки отвечает поле, которое активируется соответствующим флагом:



По умолчанию все пользователи не имеют прав. Соответственно, потребуется выбрать необходимых пользователей и задать им права «**чтения**», «**чтения и записи**» или «**все права**».

При формировании личной привязки будет создаваться **systemd**-сервис, который будет работать в связке с отведенным под него udev-правилом.

```
nano /etc/systemd/system/usb-mount@.service
```

```
[Unit]
Description=Mount USB Drive on %i

[Service]
RemainAfterExit=true
Type=oneshot
ExecStart=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py add %i /etc/udev/rules.d/80-usb_rule.rules
ExecStop=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py remove %i /etc/udev/rules.d/80-usb_rule.rules
```

Протоколирование событий usb-flash накопителей

Вкладка «**Протоколирование udev**» позволяет протоколировать события, связанные с **usb-flash** накопителями по выбранным пользователем атрибутам. Синтаксис добавления идентичен добавлению **ENV**-атрибутов.

В результате формирования правила для протоколирования будет создан файл **/etc/udev/rules.d/98-usb_logs.rules** со следующим примерным содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo disconnected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
```

USBIP - утилита для подключения удаленных USB-устройств

Настройка на сервере
Настройка на клиенте
Графическая утилита usbip-gui

USBIP — это утилита, направленная на предоставление в общий доступ USB-устройств через IP-сеть для совместного использования. Чтобы совместно использовать USB-устройства между компьютерами с их полной функциональностью, *USBIP* преобразует «сообщения ввода-вывода USB» в полезные данные **TCP/IP** и передает их между компьютерами. Оригинальные драйверы и приложения для USB-устройств также могут использоваться для удаленных USB-устройств без их модификации. Компьютер может использовать удаленные USB-устройства, как если бы они были напрямую подключены.

Устройства, которые можно подключить через утилиту:

- запоминающие устройства USB: флешки, внешние жесткие диски и картридеры;
- периферийные устройства ввода: USB-клавиатуры, мыши;
- мультимедийные устройства (например, веб-камеры);
- оборудование для печати и сканирования.

Вы можете подробнее ознакомиться с установкой и настройкой утилиты **USBIP**, просмотрев наши обучающие видео:

- на **RuTube** — Подключение удаленных USB устройств. USBIP;
- в **Яндекс.Дзен** — Подключение удаленных USB устройств. USBIP;
- в **VK Видео** — Подключение удаленных USB устройств. USBIP.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка на сервере

Сервер предназначен для публикации **USB-устройств**, которые могут быть удаленно доступны с клиентской стороны. Он выполняет роль хоста, предоставляя подключенные к нему **USB-устройства** (например, флеш-накопители, принтеры, сканеры) для использования через сеть. Это позволяет клиентам взаимодействовать с устройствами так, как если бы они были подключены локально.

Для начала работы необходимо установить утилиту *USBIP* командой (потребуются права **администратора**):

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe usbip-host
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 usbip-host
 vhci-hcd
```

Сохраните изменения и закройте редактор. Чтобы обеспечить автоматический запуск **usbipd** при старте системы, его можно оформить в виде системного юнита:

```
nano /etc/systemd/system/usbipd.service
```

Добавьте в файл следующие строки:

```
[Unit]
 Description=USBIPd
```

```
[Service]
ExecStart=/usr/sbin/usbipd -D
Type=oneshot
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

После создания или изменения системного юнита необходимо перезагрузить настройки менеджера системных служб и включить автоматический запуск службы usbipd, чтобы она запускалась сразу после загрузки системы. Для этого выполните следующие команды:

```
sudo systemctl daemon-reload
sudo systemctl enable usbipd --now
```

Перед тем как открыть доступ к какому-либо usb-устройству, нужно узнать его ID. Сделать это можно командой:

```
usbip list -l
```

Доступ к устройству открывается с помощью команды:

```
sudo usbip bind --busid=1-1
```

где **1-1** - это ID устройства.

Проверить, что устройство успешно привязано и доступно для использования, можно выполнив на сервере команду:

```
usbip list -r localhost
```

Для закрытия доступа к устройству необходимо ввести команду:

```
sudo usbip unbind -b 1-1
```

Настройка на клиенте

Клиент предназначен для подключения **USB-устройств**, опубликованных на сервере. Через клиента устройства, находящиеся на сервере, становятся доступными для локального использования, как если бы они были подключены непосредственно к клиентскому компьютеру.

Для начала работы необходимо установить утилиту *USBIP* командой:

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 vhci-hcd
```

Сохраните изменения и закройте редактор.

Проверить доступность USB-устройств, подключенных к серверу, можно выполнив на клиенте команду:

```
sudo usbip list -r <IP-адрес-сервера>
```

Для подключения открытого в общий доступ устройства на сервере к компьютеру-клиенту надо знать его ID и IP-адрес сервера. Для этого необходимо выполнить команду:

```
sudo usbip attach --remote=<IP-адрес-сервера> --busid=1-1
```

где:

- **1-1** — это ID устройства,
- **<IP-адрес-сервера>** — это IP-адрес сервера в формате **xx.xx.xx.xx**.

После подключения USB-устройства оно должно отображаться после выполнения команды:

```
lsusb
```

Для того чтобы отключить устройство из общего доступа, необходимо узнать его порт:

```
sudo usbip port
```

После того, как порт определен, можно отсоединить устройство:

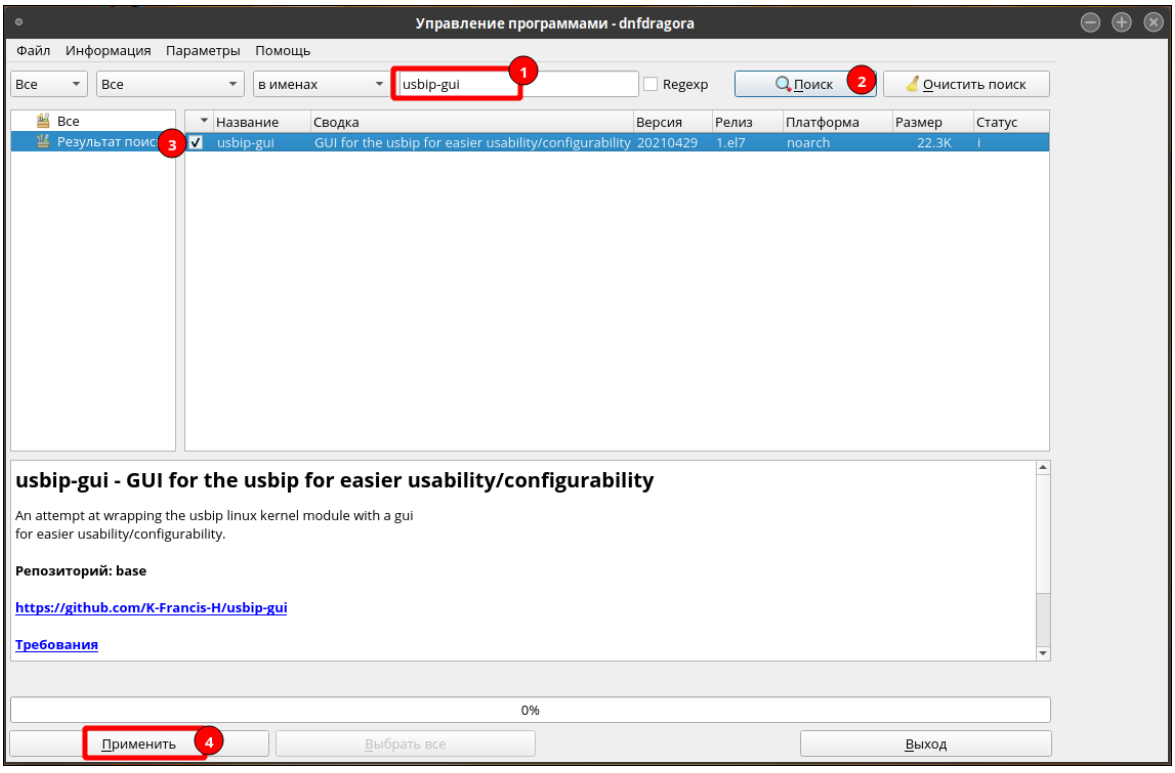
```
sudo usbip detach --port=0
```

Графическая утилита usbip-gui

В РЕД ОС также существует графическая утилита для предоставления в общий доступ USB-устройств через IP-сеть — **usbip-gui**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**usbip-gui**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.

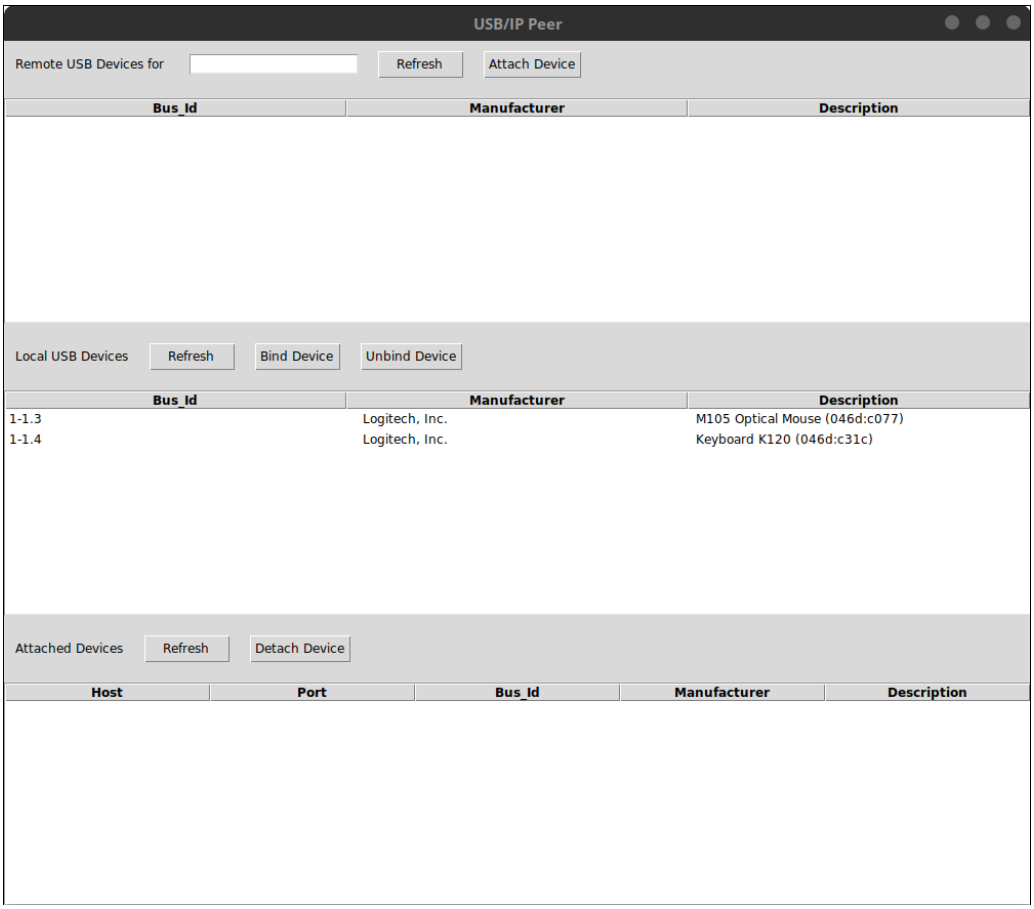


Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

```
sudo dnf install usbip-gui
```

После установки программа будет доступна из «**Главного меню**» — «**Администрирование**» — «**Управление USBIP**». Обратите

внимание, что для работы с программой необходимы права администратора или суперпользователя системы.



Тестирование аппаратного обеспечения

amtu — утилита тестирования абстрактной машины (Abstract Machine Test Utility — AMTU). Она проверяет, соблюдаются ли основные механизмы защиты аппаратного обеспечения.

AMTU выполняет следующие тесты:

- **память**: произвольно записывает данные в области памяти, затем считывает память, чтобы гарантировать, что записанные значения остаются неизменными;
- **разделение памяти**: обеспечивает, чтобы программы пользовательского пространства не могли читать и записывать в области памяти, используемые такими элементами, как видеопамять и код ядра;
- **контроллер ввода/вывода — сеть**: проверяет, что переданные случайные данные также являются данными, полученными для каждого настроенного сетевого устройства. Проверяет только настроенные устройства Ethernet и Token Ring. Не проверяет асинхронные устройства;
- **контроллер ввода/вывода — диск**: проверяет, что случайные данные, записанные на диски, остаются неизменными. Проверяются только контроллеры IDE и SCI, связанные с установленными файловыми системами. Контроллеры дисков с файловыми системами, доступными только для чтения, не проверяются;
- **инструкции режима супервизора**: проверяет, что принудительное использование свойств привилегированных инструкций в режиме супервизора, по-прежнему действует. Набор привилегированных инструкций, проверенных для подтверждения этого, зависит от архитектуры.

Для установки программы выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install amtu
```

Синтаксис:

```
amtu [ -dmsinph ]
```

Для команды **amtu** доступны следующие параметры:

- **-d** — выводить отладочные сообщения;
- **-m** — выполнить проверку памяти;
- **-s** — выполните проверку разделения памяти;
- **-i** — выполнить тест контроллера ввода-вывода;
- **-n** — выполнить - сетевой тест;
- **-p** — выполнить проверку инструкций режима супервизора;
- **-h** — показать справку.

Команда **amtu** выдает следующие коды возврата при выполнении:

- **-1** — ошибка выполнения;
- **0** — успех.

Исследование сети с помощью консольной утилиты nmap

Установка
Примеры работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** nmap-2:7.80-4

NMAP — инструмент с открытым исходным кодом для исследования сети и аудита безопасности. Он был разработан для быстрого сканирования больших сетей, но также отлично подходит для отдельных хостов в сети.

Nmap способен определить, какие хосты доступны в сети и какие сервисы они предоставляют, версии операционных систем, используемые типы фильтров пакетов/брандмауэров и десятки других характеристик.

Обычно **nmap** используется для аудита безопасности, но многие системные и сетевые администраторы находят его полезным для рутинных задач, таких как инвентаризация сети, управление графиками обновления службы и мониторинг работоспособности хостов или служб.

Установка

Для установки **nmap** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install nmap
```

Дальнейшая работа с утилитой производится с правами локального пользователя.

Примеры работы

1. Проверка доступности порта:

```
nmap 10.81.1.144 -p 22
```

```
[~]$ sudo nmap 10.81.1.144 -p 22
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-13 15:36 MSK
Nmap scan report for 10.81.1.144
Host is up (0.00091s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[~]$
```

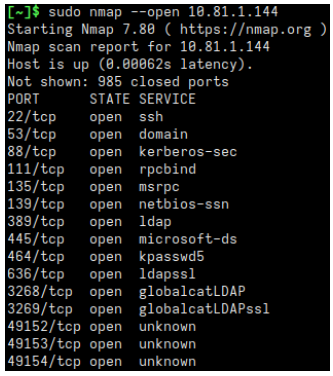
2. Показать все открытые порты на сетевом узле:

```
nmap -sV 10.81.1.144 -p 1-65535 | grep open
```

```
[~]$ sudo nmap -sV 10.81.1.144 -p 1-65535 | grep open
22/tcp    open  ssh          OpenSSH 8.2 (protocol 2.0)
53/tcp    open  domain       (generic dns response: NOTIMP)
88/tcp    open  kerberos-sec (server time: 2022-07-13 12:42:35Z)
111/tcp   open  rpcbind      2-4 (RPC #100000)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
389/tcp   open  ldap         (Anonymous bind OK)
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
464/tcp   open  kpasswd5?
636/tcp   open  ssl/ldap     (Anonymous bind OK)
3268/tcp  open  ldap         (Anonymous bind OK)
3269/tcp  open  ssl/ldap     (Anonymous bind OK)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
```

Возможен вариант с указанием параметра **--open**:

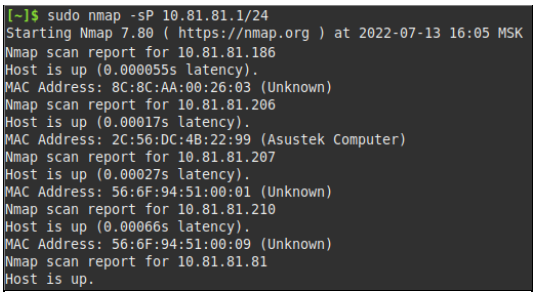
```
nmap --open 10.81.1.144
```



3. Сканировать сеть методом **ping** для обнаружения активных узлов:

```
nmap -sn 10.81.81.1/24
```

При этом в выводе команды будут отображаться IP и MAC-адреса.

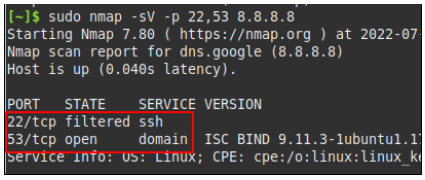


4. Информация о сетевом узле:

```
nmap -sV 10.81.1.144
```

5. Сканирование определенных портов, в примере указаны 22 (**ssh**) и 53 (**dns**):

```
nmap -sV -p 22,53 8.8.8.8
```



Также можно определить диапазон адресов для сканирования:

```
nmap -sV -p 22,53 10.81.1.1-50
```

6. Сканирование всей подсети:

```
nmap 192.168.1.0/24
```

7. Исключение нескольких хостов по их IP-адресам:

```
nmap 192.168.1.0/24 --exclude 192.168.1.10,192.168.1.154
```

8. Для быстрого сканирования используется опция **-F**:

```
nmap -F 10.81.1.1-10
```

9. Быстрое сканирование открытых портов на всех хостах подсети:

```
nmap -T5 192.168.1.1/24
```

10. Сканирование с определением версии ОС:

```
nmap -O -v --osscan-guess 192.168.1.1
```

11. Сканирование подсети с помощью **UDP ping**:

```
nmap -PU 192.168.1.1/24
```

12. Сканирование с использованием подмены MAC-адреса, в данном случае одно устройство/приложение маскируется под другое, указывая его MAC-адрес:

```
nmap -v -sT -PN --spoof-mac 0 192.168.1.1
```

В данном примере «**0**» означает, что **nmap** выберет случайный MAC-адрес.

Исследование сети с помощью графической утилиты zenmap

Установка
Описание программы
Профили сканирования
Пользовательские профили

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: nmap-zenmap-3:7.94-3

Zenmap — это мультиплатформенный графический интерфейс утилиты **nmap** и средство просмотра результатов анализа. **Zenmap** стремится сделать **nmap** простым в использовании для новичков, а опытным пользователям он предоставляет расширенные возможности.

Вы можете подробнее ознакомиться с работой утилиты **Zenmap**, просмотрев наши обучающие видео:

- на **RuTube** — Zenmap - графическая утилита исследования сети;
- в **Яндекс.Дзен** — Zenmap - графическая утилита исследования сети;
- в **VK Видео** — Zenmap - графическая утилита исследования сети.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **zenmap** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

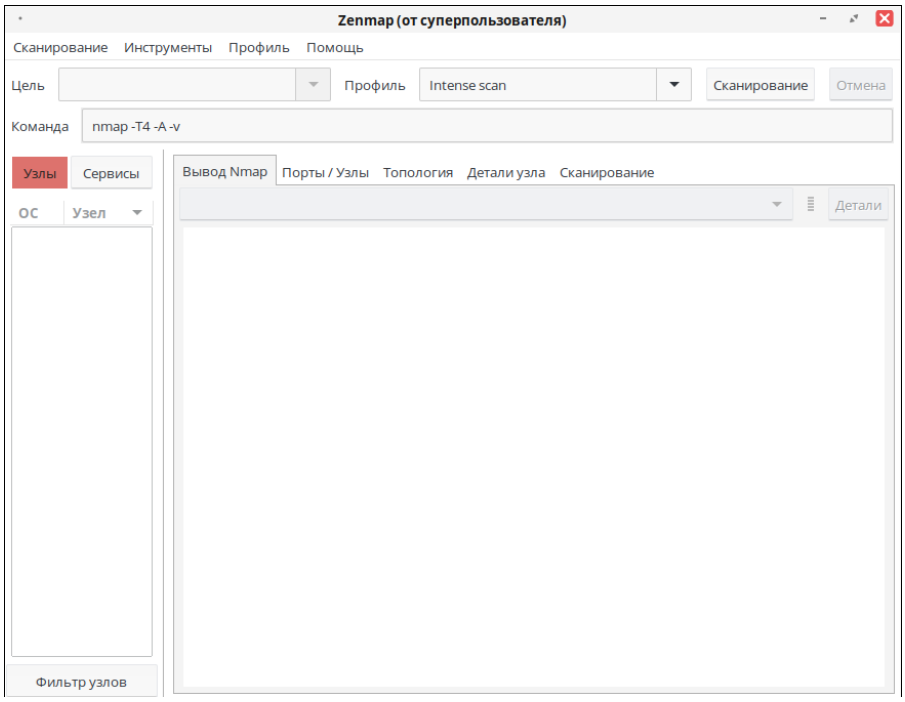
```
dnf install nmap-zenmap
```

Запуск программы доступен через «**Главное меню**» — «**Интернет**» — «**Zenmap**» или через терминал командой:

```
zenmap
```

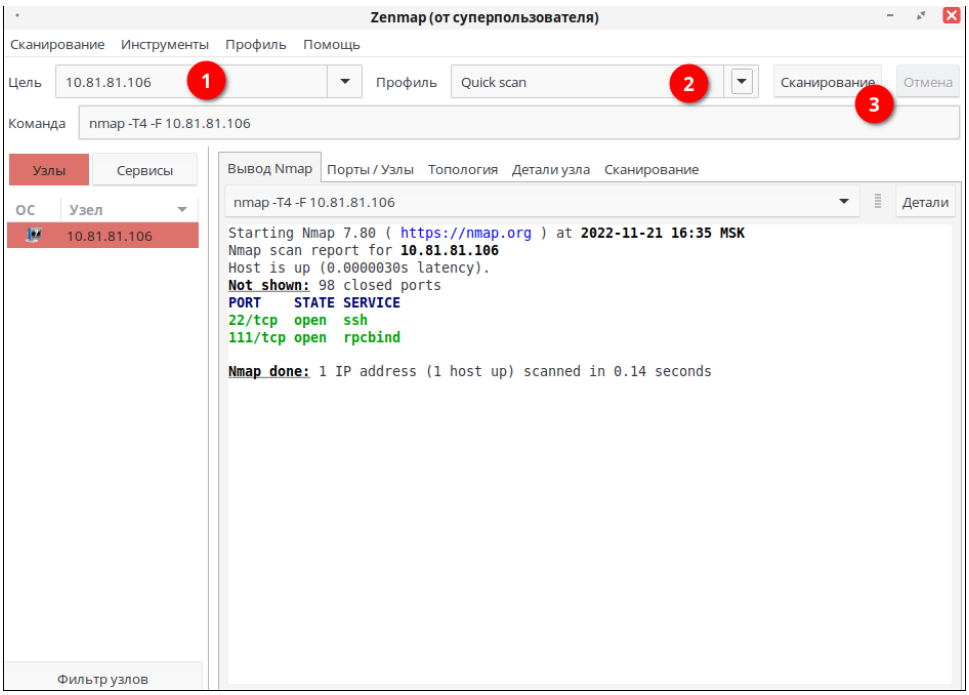
Для работы в программе **необходимы права** суперпользователя **root**.

Основное окно программы выглядит следующим образом:



Описание программы

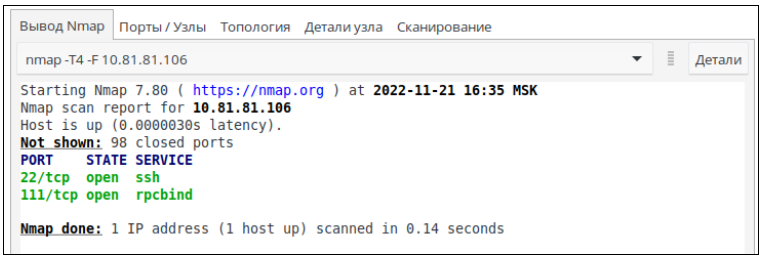
Перед началом сканирования необходимо указать в поле «**Цель**» (**1**) IP-адрес, имя домена, диапазон IP-адресов или подсеть для сканирования, а во вкладке «**Профиль**» (**2**) выбрать профиль сканирования. Запуск сканирования осуществляется нажатием кнопки «**Сканирование**» (**3**).



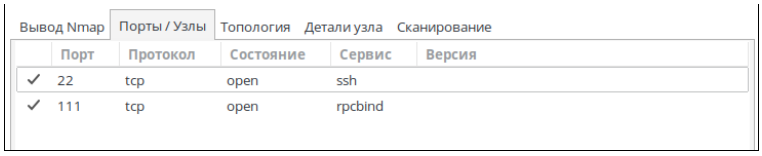
Ниже расположены следующие вкладки:

- Вывод Nmap;
- Порты/Узлы;
- Топология;
- Детали узла;
- Сканирование.

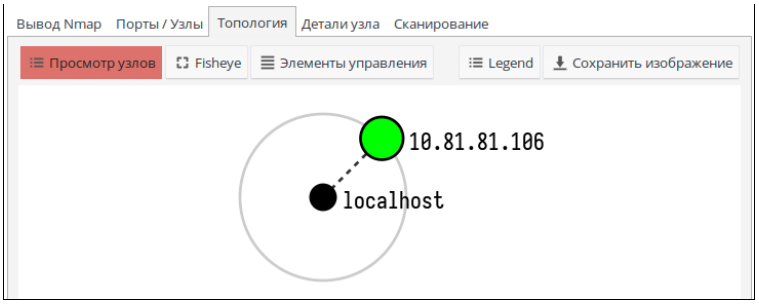
Вкладка «**Вывод Nmap**» показывает стандартный вывод информации **nmap**.



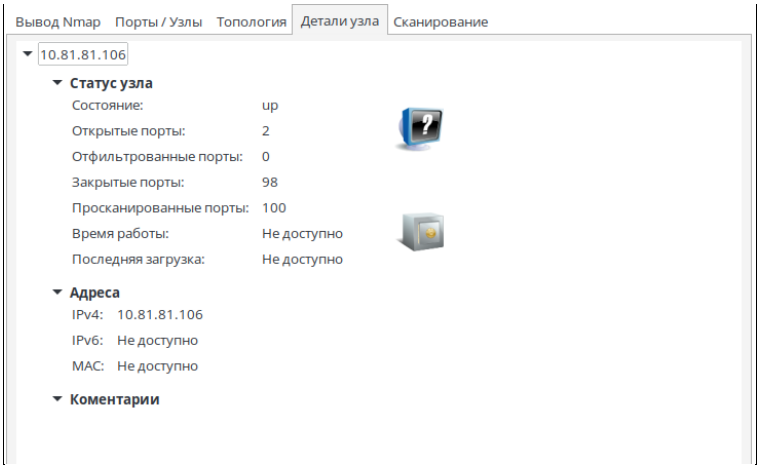
Вкладка «**Порты/Узлы**» выводит службы или порты с дополнительной информацией, отсортированной по узлам. Если выбран один узел, отображается статус сканированных портов.



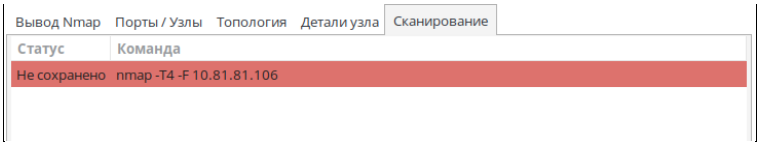
Вкладка «**Топология**» показывает топологию сети цели в графическом режиме.



Вкладка «**Детали узла**» демонстрирует информацию об отсканированном узле, которая включает в себя имя узла, состояние сканированных портов, время безотказной работы, адреса подключения и др.



Вкладка «**Сканирование**» отображает историю всех выполненных проверок, включая запущенные проверки. Также можно добавить проверки, импортировав файл кнопкой «**Добавить отчет**».



Профили сканирования

В **zenmap** существует несколько профилей сканирования:

- **Intense scan** — интенсивное сканирование;
- **Intense scan plus UDP** — интенсивное сканирование плюс UDP;
- **Intense scan, all TCP ports** — интенсивное сканирование, со всеми TCP-портами;
- **Intense scan, no ping** — интенсивное сканирование, без пинга;

- **Ping scan** — пинг-сканирование;
- **Quick scan** — быстрое сканирование;
- **Quick scan plus** — быстрое сканирование плюс;
- **Quick traceroute** — быстрая трассировка;
- **Regular scan** — обычное сканирование;
- **Slow comprehensive scan** — медленное комплексное сканирование.

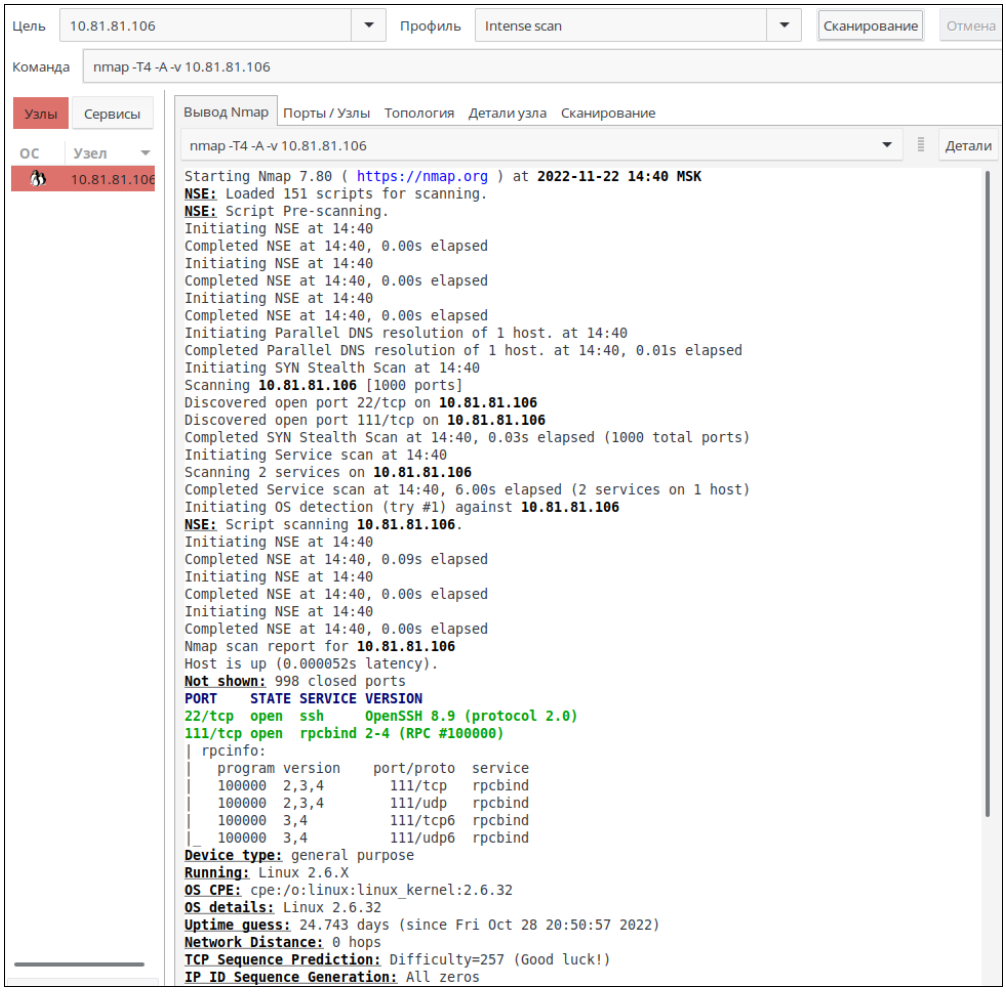
1. **Intense scan** — этот профиль быстро сканирует наиболее распространенные TCP-порты, а также определяет тип ОС, её службы и версии.

Команда:

```
nmap -T4 -A -v <цель>
```

где:

- **-T4** — временной параметр, который находится в диапазоне от 0 до 5, где 0 — самый медленный тип сканирования, а 5 — самый быстрый тип сканирования;
- **-A** — параметр, определяющий тип ОС и ее версии;
- **-v** — параметр, который отображает подробную информацию и детали сканирования, чтобы пользователь знал текущее состояние сканирования.



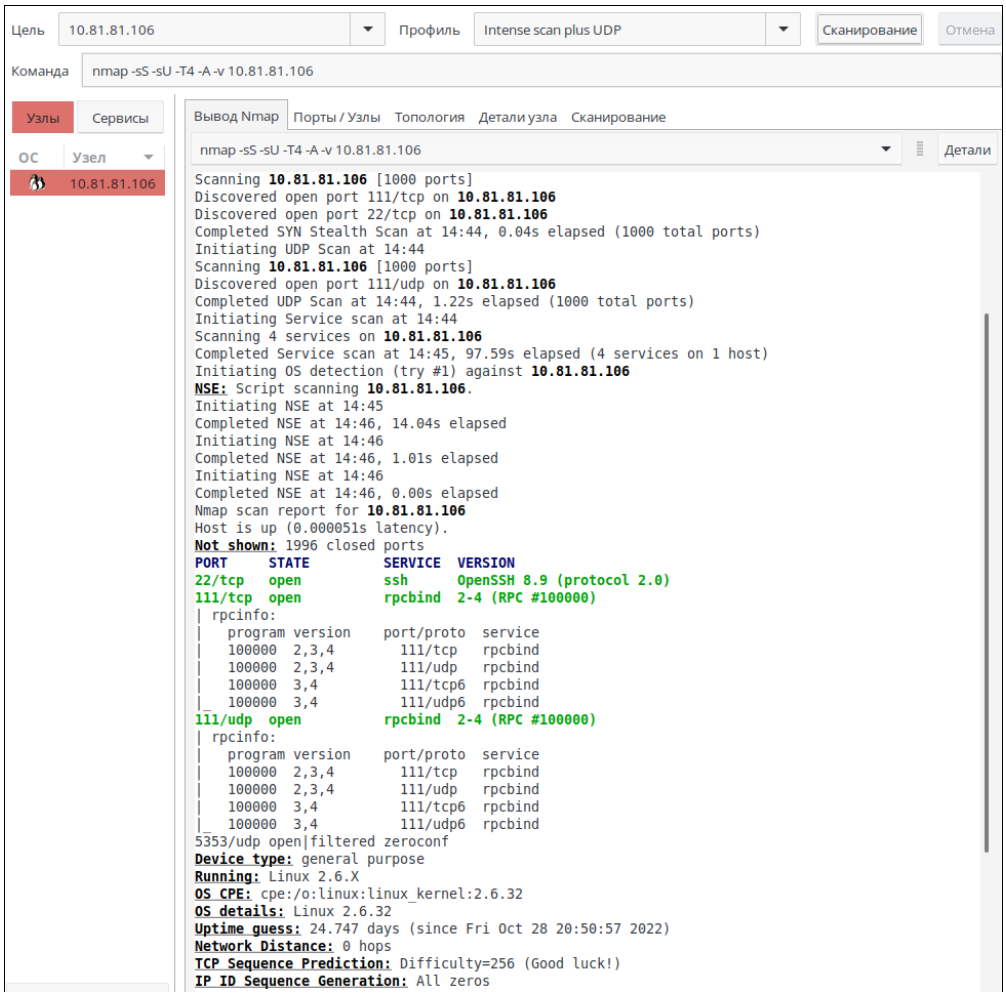
2. **Intense scan plus UDP** — работает как обычное интенсивное сканирование, однако дополнительно сканирует порты UDP.

Команда:

```
nmap -sS -sU -T4 -A -v <цель>
```

где:

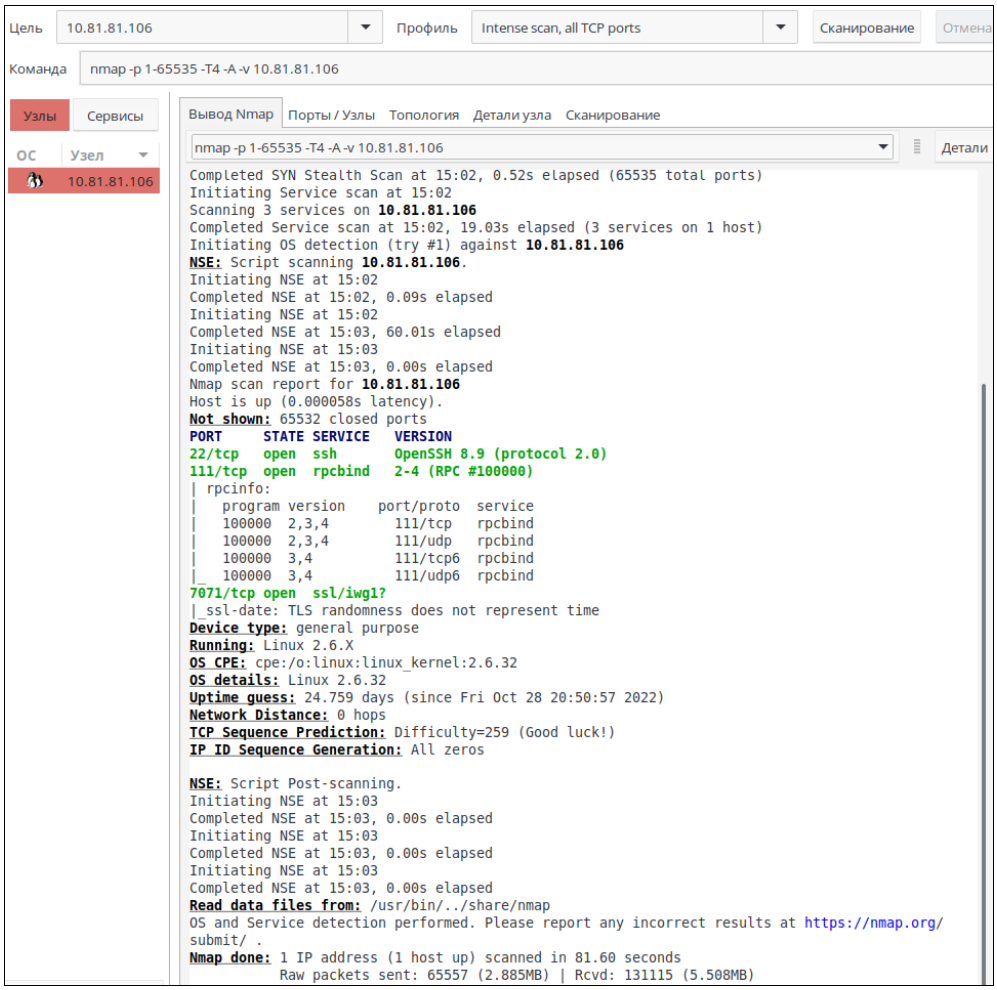
- **-sS** — указывает nmap сканировать порты TCP с помощью пакетов SYN;
- **-sU** — параметр, отвечающий за сканирование UDP-портов.

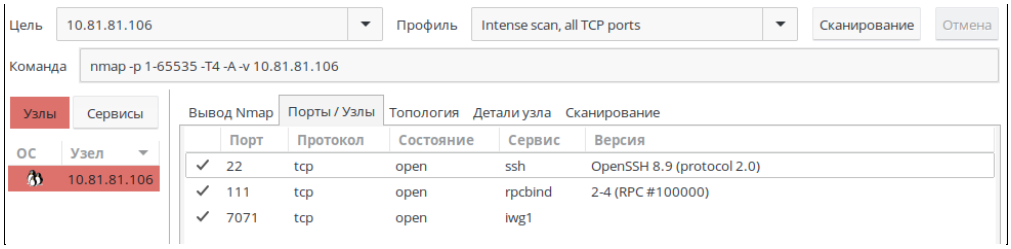


3. **Intense scan, all TCP ports** — поскольку для сканирования всех портов требуется время, **nmap** обычно сканирует 1000 самых распространённых портов. При *Интенсивном сканировании* проверка **nmap** идёт по всем портам от 1 до 65535 (макс.).

Команда:

```
nmap -p 1-65535 -T4 -A -v <цель>
```





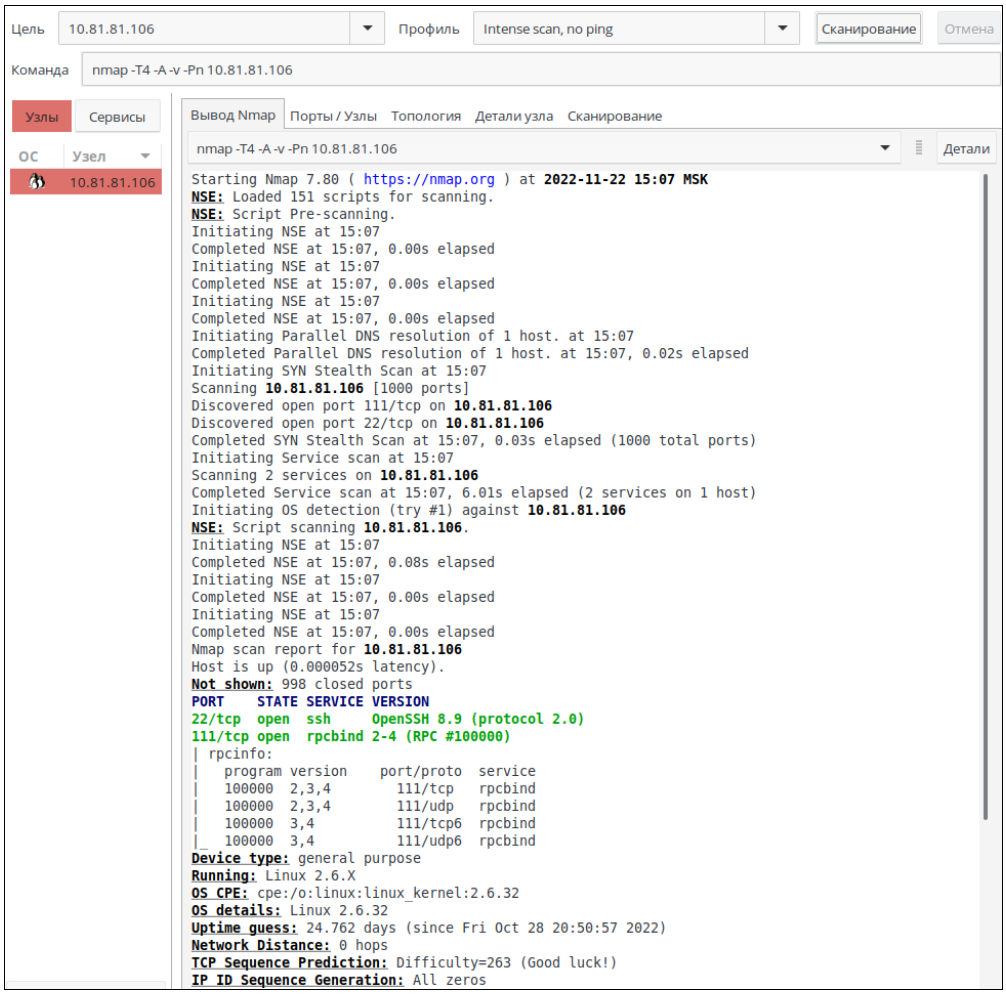
4. **Intense scan, no ping** — работает точно так же, как и другие интенсивные сканирования. Данный тип сканирования полезен, когда целевой хост блокирует запрос **ping**, но вы знаете, что он активен.

Команда:

```
nmap -T4 -A -v -Pn <цель>
```

где:

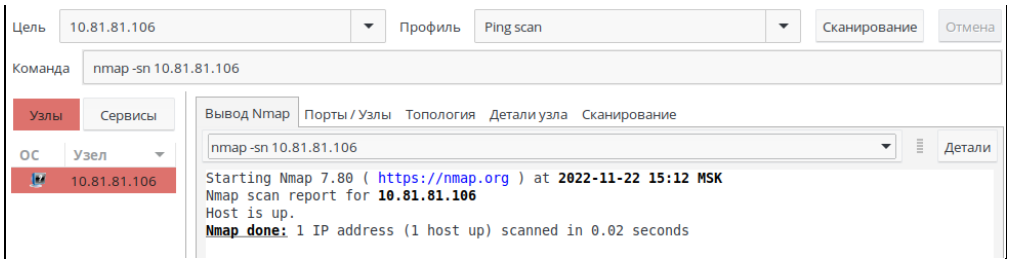
- **-Pn** — параметр предполагает, что хост работает.



5. **Ping scan** — выполняет только пинг цели, не сканируя порты.

Команда:

```
nmap -sn <цель>
```



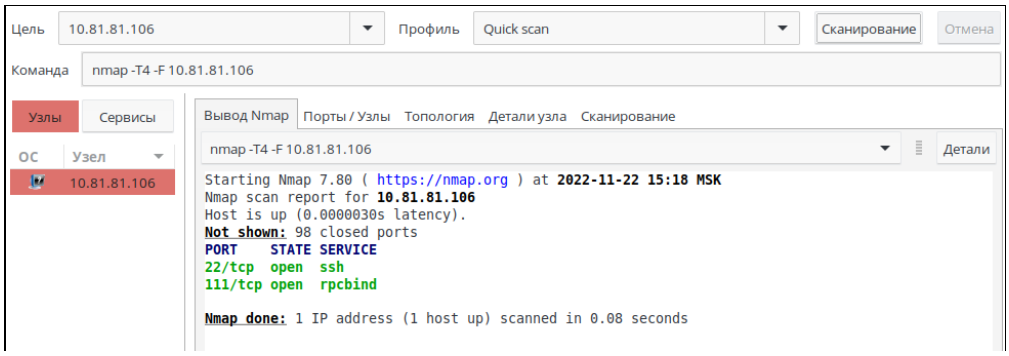
6. **Quick scan** — сканирует только ограниченное количество портов TCP, т.е. 100 самых распространенных портов **TCP**.

Команда:

```
nmap -T4 -F <цель>
```

где:

- **-F** — параметр для быстрого сканирования. Вместо того чтобы сканировать все порты, сканируется только несколько портов.



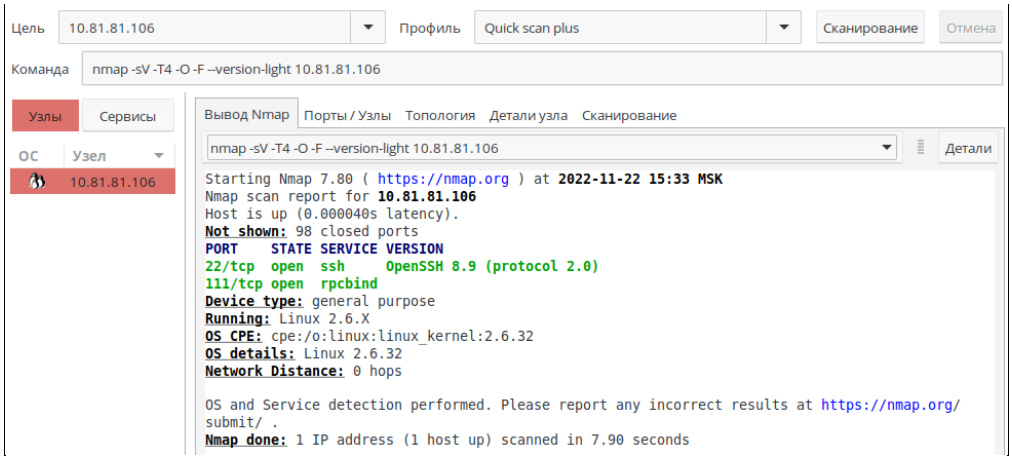
7. **Quick scan plus** — помимо быстрого сканирования определяет также операционную систему сканируемого хоста и определяет версии служб, за которыми закреплены сканируемые порты.

Команда:

```
nmap -sV -T4 -O -F --version-light <цель>
```

где:

- **-O** — параметр, который определяет тип ОС, а затем выполняет легкое сканирование.



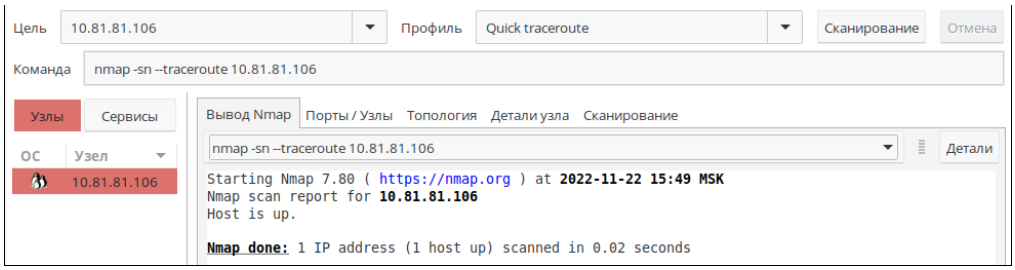
8. **Quick traceroute** — отслеживает и выполняет пинг всех хостов, определенных в цели.

Команда:

```
nmap -sn --traceroute <цель>
```

где:

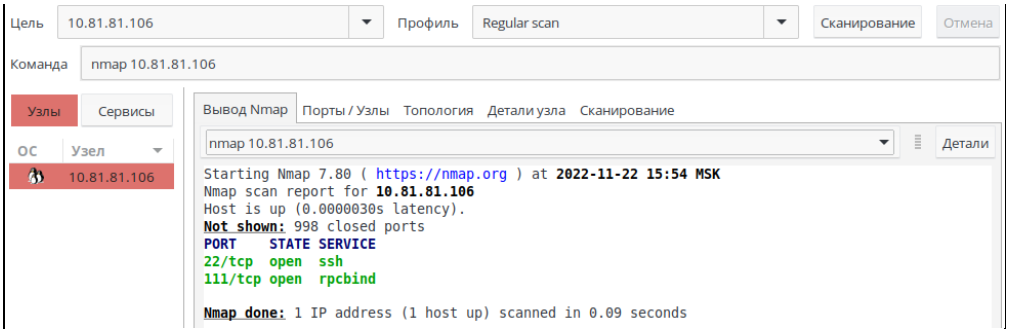
- **--traceroute** — программа, которая записывает маршрут между вашим компьютером и определенным пунктом назначения через Интернет.



9. **Regular scan** — выполняет сканирование TCP SYN для 1000 наиболее распространенных портов, используя запрос ping для обнаружения хоста.

Команда:

```
nmap <цель>
```



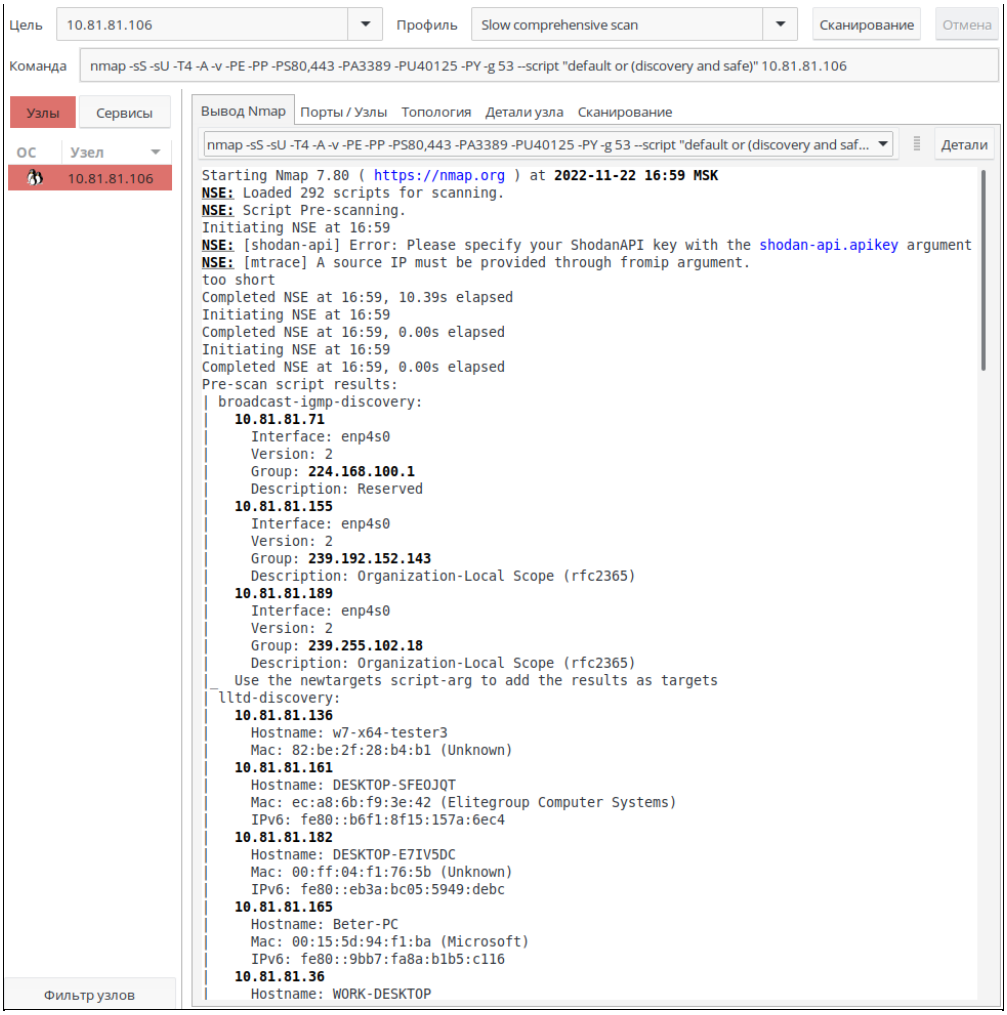
10. **Slow comprehensive scan** — профиль обладает большим количеством параметров, которые позволяют провести комплексное сканирование сети.

Команда:

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" <цель>
```

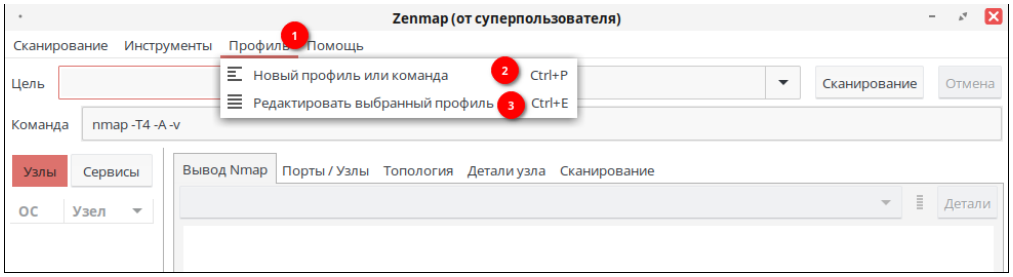
где:

- **-PE** — пинг с использованием ICMP-эхо запросов;
- **-PP** — пинг с использованием запросов временной метки;
- **-PS<№_порта>** — TCP SYN-пинг заданных хостов;
- **-PA<№_порта>** — TCP ACK-пинг заданных хостов;
- **-PU<№_порта>** — UDP-пинг заданных хостов;
- **-PY** — похоже на сканирование TCP SYN, только вместо этого используется SCTP;
- **-g** — указывается, какой исходный порт вы хотите использовать. Используется при попытке обойти систему обнаружения вторжений (IDS);
- **--script** — сканирование с использованием скриптов.

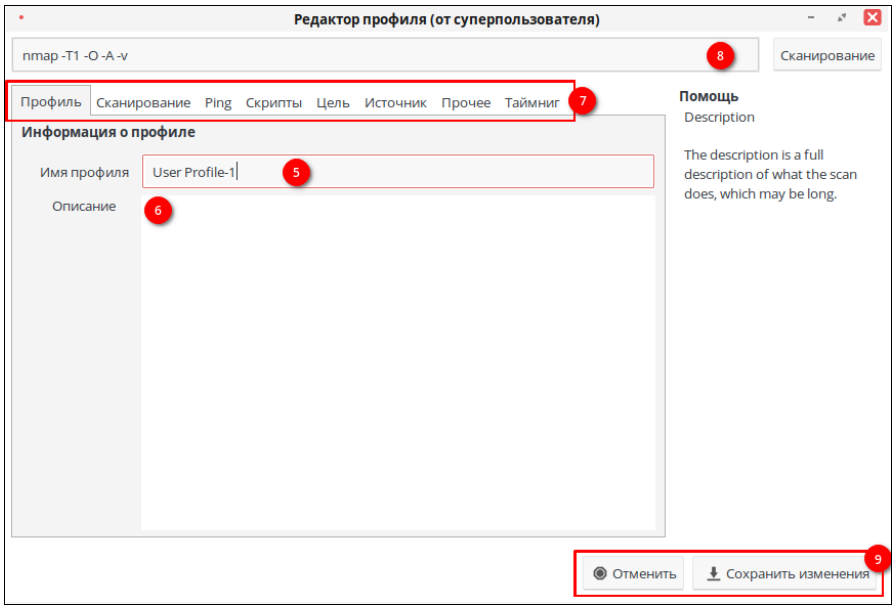


Пользовательские профили

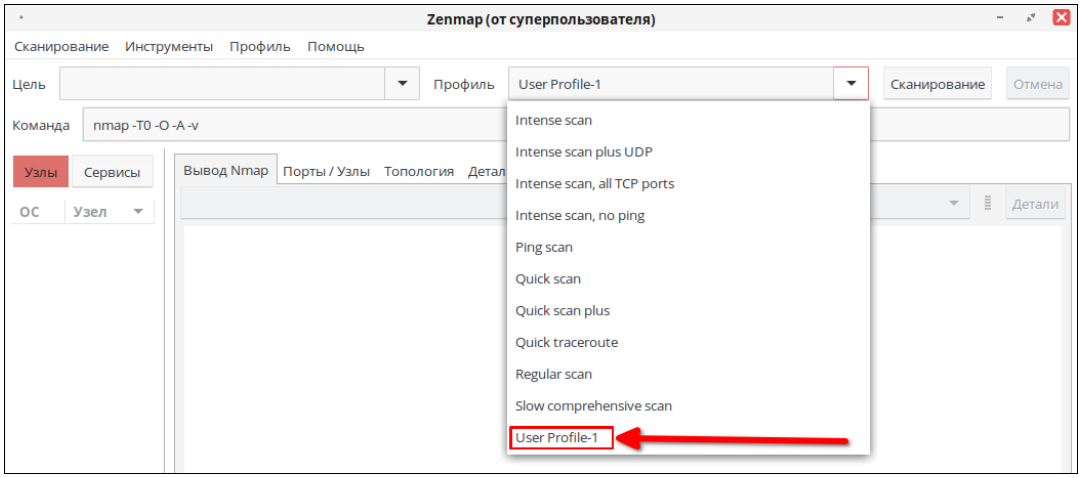
В **zenmap** есть возможность создавать и редактировать пользовательские профили. Для этого необходимо выбрать во вкладке «**Профиль**» (**1**) соответствующий пункт меню: «**Новый профиль или команда**» (**2**) или «**Редактировать выбранный профиль**» (**3**).



В окне редактора указывается *имя профиля* (**5**). Пользователь может при необходимости добавить *описание* к своему профилю (**6**). После указания всех необходимых *параметров* настройки (**7**) в отдельном поле (**8**) формируется *команда* для последующего сканирования сети. В этом же поле можно сразу указать нужную команду для выполнения сканирования без последовательной настройки. После настройки можно *сохранить* полученный профиль или *отменить* все изменения (**9**).



Во вкладке «**Профиль**» можно выбрать сохранённый профиль сканирования.



Настройка SSL для веб-серверов

Предварительная подготовка
Установка веб-серверов nginx и apache
Генерация сертификата
Настройка веб-серверов nginx и apache с сертификатами

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Редакция**: Стандартная
- **Версия ПО**: nginx-1:1.25.4-1, httpd-2.4.58-1, mod_ssl-1:2.4.58-1

Предварительная подготовка

Необходимо внести DNS-запись с наименованием веб-сервера в файл **/etc/hosts** (необходимы права пользователя **root**):

```
echo <ip-адрес> <название сайта> > /etc/hosts
```

Например:

```
echo 127.0.0.1 redsite.ru > /etc/hosts
```

Установка веб-серверов nginx и apache

Примечание.

Все команды, используемые в данном разделе, выполняются **с правами пользователя root**, если не указано иное.

Nginx

Выполните установку пакетов:

```
dnf install nginx
```

Запустите службу **nginx** и добавьте ее в автозагрузку:

```
systemctl enable nginx --now
```

Apache

Выполните установку пакетов:

```
dnf install httpd
```

Запустите службу **apache** и добавьте ее в автозагрузку:

```
systemctl enable httpd --now
```

Генерация сертификата

В качестве примера будет использоваться домен - **redsite.ru**.

В данном разделе будет рассмотрен выпуск самоподписанных сертификатов для тестовых или внутренних серверов.

В качестве утилиты генерации сертификатов будет использоваться openssl, который по умолчанию предустановлен в РЕД ОС.

Примечание.

Работа с командами утилиты **openssl** осуществляется **с правами непривилегированного пользователя** и не требует прав администратора.

Примечание.

Данный раздел является общим для веб-серверов **nginx** и **apache**.

1. Создайте корневой закрытый ключ:

```
openssl genpkey -algorithm RSA -out rootCA.key -aes-128-cbc
```

где:

- genpkey – команда создания закрытого ключа;
- algorithm RSA – алгоритм асинхронного шифрования, именно он используется для выделения открытого ключа из этого закрытого;
- out rootCA.key – получаемый файл закрытого ключа;
- aes-128-cbc – алгоритм симметричного шифрования, которым зашифровывается файл закрытого ключа с помощью пароля. Пароль необходимо ввести.

Вывод команды будет иметь примерно следующий вид:

```
.......+++++
...+++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

2. Создайте открытый ключ:

```
openssl req -x509 -new -key rootCA.key -sha256 -days 365 -out rootCA.crt
```

где:

- req – команда создания сертификатов или запросов на сертификаты;
- -x509 – создание именно сертификата, а не запроса;
- -new – новый сертификат (потребуется ввести значения некоторых полей в сертификате);
- -key rootCA.key – используемый закрытый ключ, из которого следует создать открытый;
- -sha256 – алгоритм хеширования для создания подписи ключа;
- -days 365 – выпуск сертификата на 1 год;
- -out rootCA.crt – получаемый сертификат.

Пример вывода команды:

```
Enter pass phrase for rootCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Murom
Locality Name (eg, city) [Default City]:Murom
Organization Name (eg, company) [Default Company Ltd]:RS
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:redsite.ru
```

```
Email Address []:admin@redsite.ru
```

3. Создайте файл порядковых номеров для выпуска сертификатов, в нем следует указать два нуля:

```
echo 00 > rootCA.srl
```

4. В **openssl** нет возможности добавлять некоторые поля, например, такие как subjectAltName. Для этого создайте конфигурационный файл с необходимыми параметрами:

```
nano redsite.cnf
```

Содержимое файла следующее:

```
[ req ]
 default_bits = 2048
 distinguished_name = req_distinguished_name
 req_extensions = req_ext
 [ req_distinguished_name ]
 countryName = Country Name (2 letter code)
 countryName_default = RU
 stateOrProvinceName = State or Province Name (full name)
 stateOrProvinceName_default = Murom
 localityName = Locality Name (eg, city)
 localityName_default = Murom
 organizationName = Organization Name (eg, company)
 organizationName_default = RS
 commonName = Common Name (eg, YOUR name or FQDN)
 commonName_max = 64
 commonName_default = redsite.ru
 [ req_ext ]
 basicConstraints = CA:FALSE
 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 subjectAltName = DNS:redsite.ru
```

здесь:

- раздел [req]:
  - default_bits = 2048 – длина ключа по умолчанию;
  - distinguished_name = req_distinguished_name – это поля в сертификате, например, **Common Name**, **organizationName** и др. Для этих полей создается блок req_distinguished_name ниже;
  - req_extensions = req_ext – расширение для req, в котором можно добавить дополнительные поля в сертификат. В данном параметре указывается наличие ниже блока req_ext с дополнительными полями;
- раздел [req_distinguished_name] – параметры для конфигурации сертификата;
- раздел [req_ext] – расширенные параметры для конфигурации сертификата:
  - basicConstraints = CA:FALSE – полученные сертификаты нельзя использовать как центр сертификации;
  - keyUsage = nonRepudiation, digitalSignature, keyEncipherment – созданный ключ будет иметь следующие свойства: неотрекаемость, цифровая подпись (сертификат можно использовать в качестве цифровой подписи), шифрование ключей;
  - subjectAltName = DNS:redsite.ru – здесь указывается поле **subjectAltName** и его значение.

5. Создайте закрытый ключ для домена:

```
openssl genpkey -algorithm RSA -out redsite.key
```

Вывод команды будет иметь примерно следующий вид:

```
.....+++++
.....+++++
```

6. Создайте с закрытым ключом файл запроса на сертификат. После выполнения команды на всех полях необходимо нажать *Enter*, т.к. данные используются из конфигурационного файла **nginx.cnf**, который был создан ранее:

```
openssl req -new -key redsite.key -config redsite.cnf -reqexts req_ext -out redsite.csr
```

Пример вывода команды:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:RU
State or Province Name (full name) [Murom]: Murom
Locality Name (eg, city) [Murom]: Murom
Organization Name (eg, company) [RS]: RS
Common Name (eg, YOUR name or FQDN) [redsite.ru]: redsite.ru
```

7. Сгенерируйте сертификат для домена:

```
openssl x509 -req -days 365 -CA rootCA.crt -CAkey rootCA.key -extfile redsite.cnf -extensions req_ext -in redsite.csr -out redsite.crt
```

где:

- `x509` – создание сертификата методом подписания;
- `-req` – если производится подпись файла запроса, необходимо использовать эту опцию;
- `-days 365` – срок сертификата 1 год;
- `-CA rootCA.crt -CAkey rootCA.key` – корневая пара ключей;
- `-extfile redsite.cnf` – файл, содержащий расширения сертификатов;
- `-in redsite.csr -out redsite.crt` – файл запроса и файл сертификата.

Пример вывода команды:

```
Signature ok
subject=C = RU, ST = Murom, L = Murom, O = RS, CN = redsite.ru, Getting CA Private Key
Enter pass phrase for rootCA.key:
```

8. Проверьте наличие сертификатов:

```
 ls -l

итого 60
-rw-rw-r--. 1 user user  801 июн 13 22:23  redsite.cnf
-rw-rw-r--. 1 user user 1245 июн 13 22:26  redsite.crt
-rw-rw-r--. 1 user user 1058 июн 13 22:25  redsite.csr
-rw-------. 1 user user 1704 июн 13 22:23  redsite.key
-rw-rw-r--. 1 user user 1363 июн 13 22:20  rootCA.crt
-rw-------. 1 user user 1874 июн 13 22:18  rootCA.key
-rw-rw-r--. 1 user user    3 июн 13 22:26  rootCA.srl
```

9. Затем необходимо поместить сертификаты в директории **/etc/ssl/certs** и **/etc/ssl/private** следующим образом:

```
sudo mkdir /etc/ssl/private
sudo cp  rootCA.crt redsite.crt  /etc/ssl/certs
sudo cp redsite.key /etc/ssl/private
```

10. Добавьте сертификат в системное хранилище. Для этого скопируйте сертификаты в каталог **/etc/pki/ca-trust/source/anchors/**:

```
sudo cp  rootCA.crt redsite.crt /etc/pki/ca-trust/source/anchors/
```

Затем выполните команды обновления (с правами пользователя **root**):

```
update-ca-trust
update-ca-trust extract
```

Настройка веб-серверов nginx и apache с сертификатами

> **Примечание.**
>
> Все команды, используемые в данном разделе, выполняются **с правами пользователя root**, если не указано иное.

Nginx

1. Приведите раздел **Settings for a TLS enabled server** файла **/etc/nginx/nginx.conf** к следующему виду:

```
nano /etc/nginx/nginx.conf
```

```
# Settings for a TLS enabled server.
#
server {    # раскомментируйте строку
listen 443 ssl default_server;    # раскомментируйте строку и замените http2 на default_server
listen [::]:443 ssl default_server;    # раскомментируйте строку и замените http2 на default_server
server_name redsite;    #укажите имя сервера без доменной области
# root /usr/share/nginx/html;
#
ssl_certificate "/etc/ssl/certs/redsite.crt";
ssl_certificate_key "/etc/ssl/private/redsite.key";
# ssl_session_cache shared:SSL:1m;
# ssl_session_timeout 10m;
# ssl_ciphers HIGH:!aNULL:!MD5;
# ssl_prefer_server_ciphers on;
#
# # Load configuration files for the default server block.
# include /etc/nginx/default.d/*.conf;
#
# error_page 404 /404.html;
# location = /404.html {
# }
#
# error_page 500 502 503 504 /50x.html;
# location = /50x.html {
# }
}    # раскомментируйте строку


}
```

В конце файла необходимо добавить фигурную скобку «**}**», чтобы избежать ошибок синтаксиса от **nginx**.

2. Выполните проверку настроек **nginx**:

```
nginx -t
```

Вывод команды должен иметь примерно следующий вид:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Выполните перезапуск службы **nginx**:

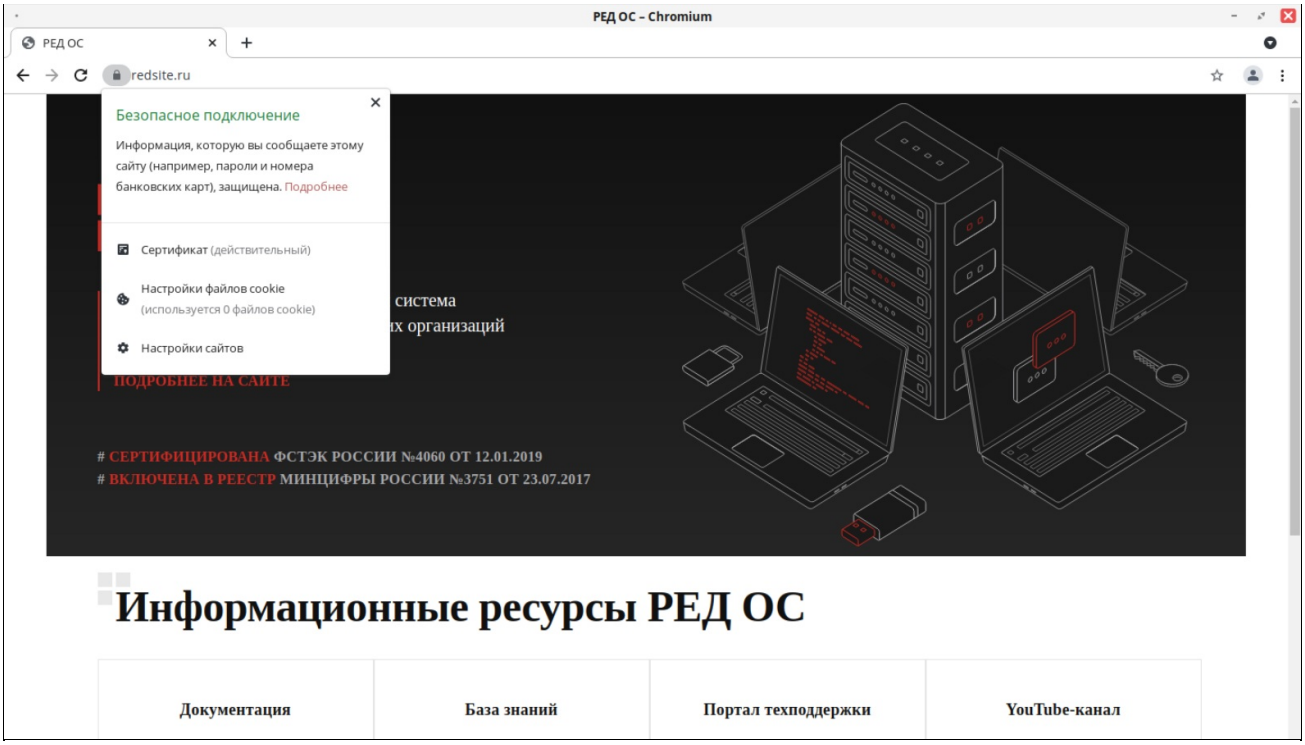
```
systemctl restart nginx
```

Примените правило *SELinux* для разрешения подключений:

```
setsebool -P httpd_read_user_content 1
```

Для проверки перейдите в браузере по ссылке `https://<ваш_сайт>`.

Например:



Apache

1. Для работы **SSL** необходимо установить следующий пакет:

```
dnf install mod_ssl
```

2. Приведите файл **/etc/httpd/conf/httpd.conf** к виду:

```
ServerName redsite.ru    # раскомментировать строку и указать имя сервера
 LoadModule ssl_module modules/mod_ssl.so    # добавить строку в конец файла
```

3. В **/etc/httpd/conf.d/ssl.conf** укажите путь до сертификатов:

```
SSLCertificateFile /etc/ssl/certs/redsite.crt    # укажите путь до сертификата (открытая часть)
 SSLCertificateKeyFile /etc/ssl/private/redsite.key    # укажите путь до сертификата (закрытая часть)
```

4. Проверьте настройки **httpd**:

```
apachectl configtest
```

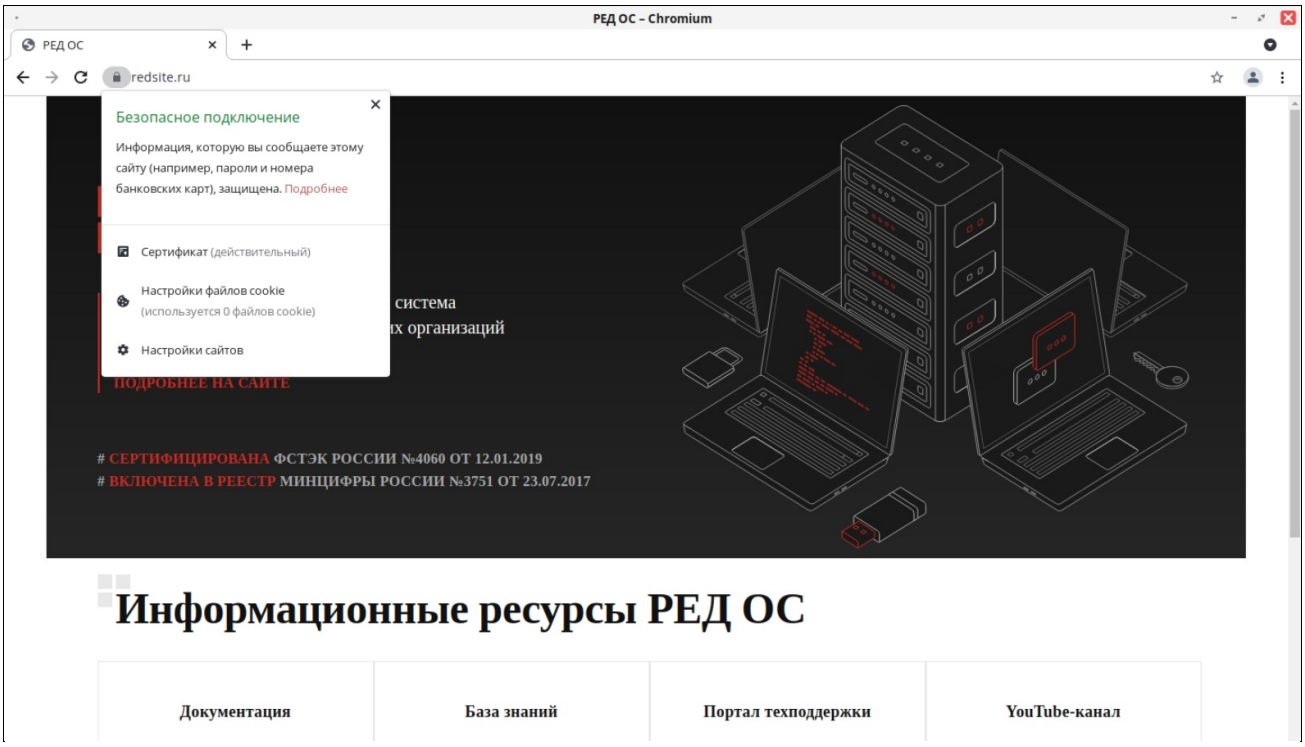
Вывод команды должен иметь примерно следующий вид:

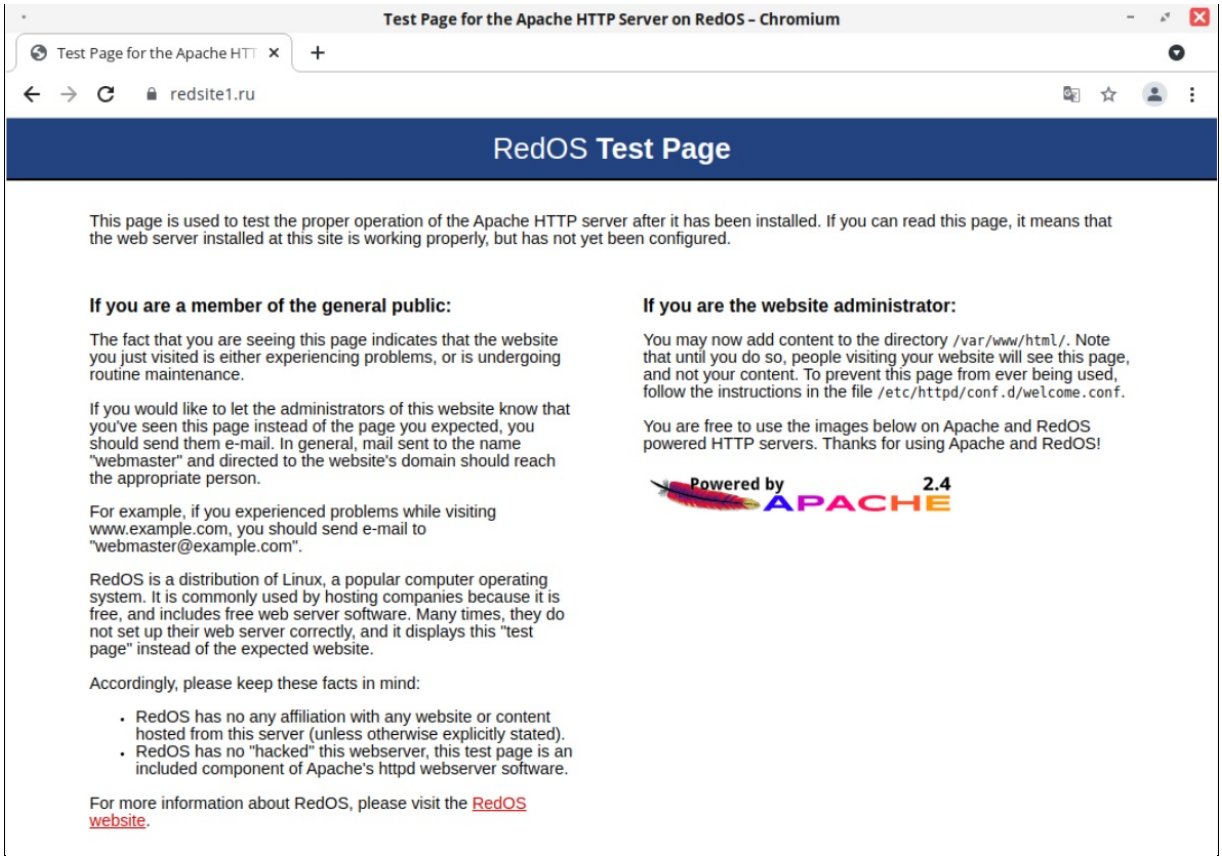
```
Syntax OK
```

5. Для применения изменений перезапустите службу **httpd**:

```
systemctl restart httpd
```

6. Для проверки перейдите в браузере по ссылке `https://<ваш_сайт>`. Например:


РЕД ОС – Chromium
РЕД ОС
redsite.ru
Безопасное подключение
Информация, которую вы сообщаете этому сайту (например, пароли и номера банковских карт), защищена. Подробнее
Сертификат (действительный)
Настройки файлов cookie
(используется 0 файлов cookie)
Настройки сайтов
ПОДРОБНЕЕ НА САЙТЕ
СЕРТИФИЦИРОВАНА ФСТЭК РОССИИ №4060 ОТ 12.01.2019
ВКЛЮЧЕНА В РЕЕСТР МИНЦИФРЫ РОССИИ №3751 ОТ 23.07.2017
Информационные ресурсы РЕД ОС
Документация
База знаний
Портал техподдержки
YouTube-канал


Test Page for the Apache HTTP Server on RedOS – Chromium
Test Page for the Apache HTT
redsite1.ru
RedOS Test Page
This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.
If you are a member of the general public:
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.
If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.
For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".
RedOS is a distribution of Linux, a popular computer operating system. It is commonly used by hosting companies because it is free, and includes free web server software. Many times, they do not set up their web server correctly, and it displays this "test page" instead of the expected website.
Accordingly, please keep these facts in mind:
RedOS has no any affiliation with any website or content hosted from this server (unless otherwise explicitly stated).
RedOS has no "hacked" this webserver, this test page is an included component of Apache's httpd webserver software.
For more information about RedOS, please visit the RedOS website.
If you are the website administrator:
You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf.d/welcome.conf.
You are free to use the images below on Apache and RedOS powered HTTP servers. Thanks for using Apache and RedOS!
Powered by APACHE 2.4

Поддержка российских сертификатов безопасности

Сертификаты ТЦИ
Настройка цепочки доверия TLS-сертификатов ГОСТ

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: ca-certificates-ru-2022-8

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. **SSL** (**Secure Sockets Layer**) – это протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.

Компаниям необходимо добавлять SSL-сертификаты на веб-сайты для обеспечения конфиденциальности и безопасности клиентских данных.

В РЕД ОС обеспечена поддержка российских сертификатов безопасности, предоставленных удостоверяющим центром сертификации Минцифры России. Пакет ca-certificates-ru, содержащий комплект корневых сертификатов ЦС России, по умолчанию предустановлен в РЕД ОС. Привязка сертификатов в браузерах **Chromium**, **Firefox**, **Яндекс.Браузер** происходит **автоматически**.

Вы можете подробнее ознакомиться с установкой и настройкой сертификатов безопасности, просмотрев наши обучающие видео:

- на **RuTube** — Поддержка российских SSL-сертификатов в РЕД ОС;
- в **Яндекс.Дзен** — Поддержка российских SSL-сертификатов в РЕД ОС;
- в **VK Видео** — Поддержка российских SSL-сертификатов в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сертификаты ТЦИ

В состав пакета ca-certificates-ru также входят корневые сертификаты *Центра сертификации ТЦИ*.

Центр сертификации ТЦИ — это организация, которая выпускает TLS-сертификаты для веб-ресурсов (сайтов, платформ и т.п.).

TLS-сертификаты являются важным инструментом, обеспечивающим безопасность пользователей сети Интернет. Они представляют собой аналог цифровой подписи для веб-ресурса, т.е. подтверждают его подлинность и позволяют организовать доверенный, защищённый канал обмена данными, обеспечивая их сохранность и невозможность перехвата.

Центр сертификации ТЦИ выпускает сертификаты с методами шифрования **ECDSA** и **ГОСТ**. Оба метода очень похожи между собой и имеют более высокую скорость шифрования по сравнению с *RSA*, но технически имеют различия в математической модели криптографических параметров. **ECDSA**-сертификаты можно использовать при типовых настройках без изменений на сервере и клиенте, а **ГОСТ**-сертификаты популяризируют отечественную криптографию.

Настройка цепочки доверия TLS-сертификатов ГОСТ

Для настройки использования в РЕД ОС **TLS**-сертификатов с методом шифрования по **ГОСТ** выполните следующие действия:

1. Обновите пакет ca-certificates-ru:

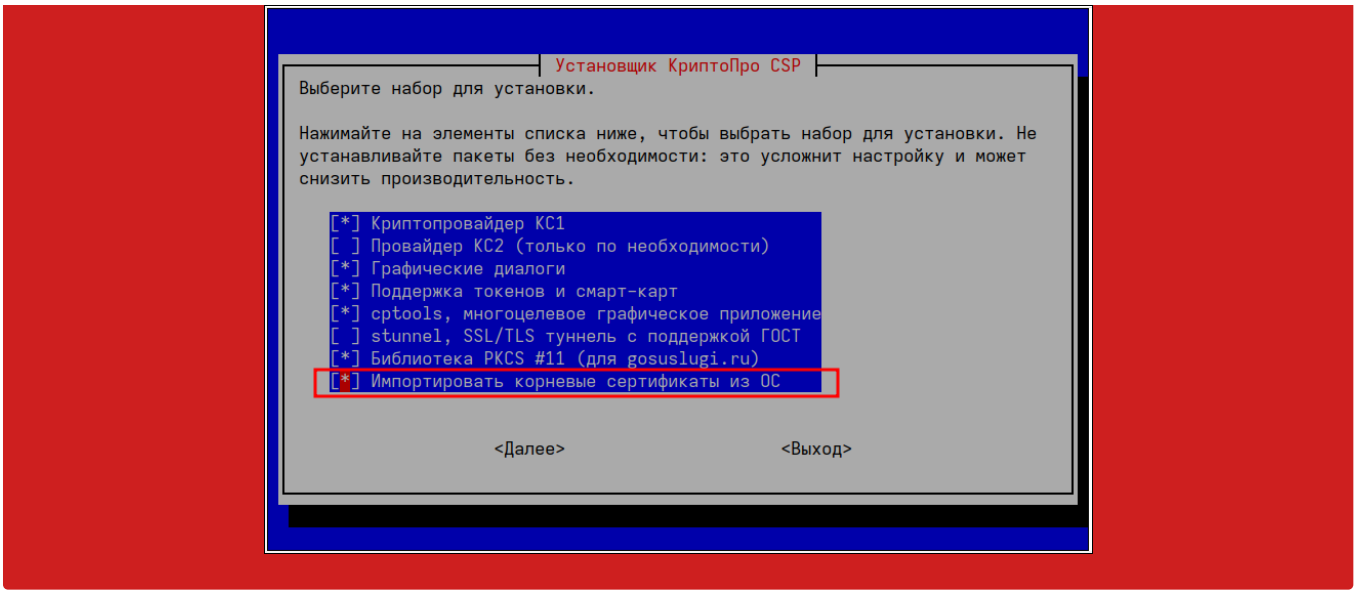
```
dnf update ca-certificates-ru
```

2. Установите криптопровайдер **КриптоПро CSP 5.0** согласно нашей инструкции «Установка КриптоПро CSP 5.0».

ВАЖНО!

Обратите внимание, что на втором шаге при определении набора установки необходимо выбрать пункт «**Импортировать корневые сертификаты ОС**», т.к. *КриптоПро CSP* по умолчанию **НЕ использует** хранилище корневых сертификатов из ОС.

Без установки указанного параметра «**Импортировать корневые сертификаты ОС**» ГОСТ-сертификат ТЦИ работать **не будет**!



Для доступа к сайтам с ГОСТ-сертификатом можно пользоваться штатным браузером **Chromium** или **Яндекс**.

Проверка работоспособности

Для проверки корректной работы сертификатов Минцифры в ОС можно перейти по ссылке https://fias.egisz.rosminzdrav.ru/. Если сайт открыт без предупреждений о небезопасном соединении, значит все настроено верно.

Проверку корректной настройки TLS-сертификата с методом шифрования ГОСТ можно осуществить на тестовой странице ТЦИ https://gost.tlscc.ru/.

Настройка ГОСТ в OpenSSL в РЕД ОС 8

Установка пакетов
Включение поддержки алгоритмов шифрования ГОСТ
Проверка поддержки ГОСТ в OpenSSL
Пример генерации ключей
Возврат настроек по умолчанию

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openssl-gost-engine-3.0.1-8

В состав дистрибутива РЕД ОС входит пакет библиотек, поддерживающих методы защитного преобразования по алгоритмам ГОСТ, **openssl-gost-engine**.

Пакет **openssl-gost-engine** включает в себя реализацию следующих алгоритмов ГОСТ:

- ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 — алгоритмы электронной цифровой подписи.
- ГОСТ Р 34.11-2012 — криптографический алгоритм вычисления хеш-функции “Стрибог” с размером блока входных данных 512 бит и размером хеш-кода 256 или 512 бит.
- ГОСТ 28147-89 — симметричное шифрование с 256-битным ключом. Доступны режимы CBC, CFB и CNT. Для усложнения статистического анализа поддерживается «key meshing» (подробнее см. RFC 4357).
- VKO ГОСТ Р 34.10 2001 и VKO ГОСТ Р 34.10 2012 – алгоритмы согласования ключей.
- ГОСТ Р 34.12-2018 – симметричный алгоритм блочного шифрования “Магма”, построенный по типу сети Фейстеля, с размером секретного ключа 256 бит, размером входного сообщения 64 бита и 32 раундами шифрования.
- ГОСТ Р 34.12-2018 — симметричный алгоритм блочного шифрования “Кузнечик” с размером блока 128 бит и длиной ключа 256 бит, использующий для генерации раундовых ключей SP-сеть.

Методы шифрования ГОСТ применяются к используемой в системе политике шифрования.

Общесистемные политики шифрования — это системный компонент, который настраивает основные криптографические подсистемы, включая протоколы TLS, IPsec, SSH, DNSSec и Kerberos. Он предоставляет небольшой набор политик, которые может выбрать администратор.

При использовании в системе общесистемных политик программы следуют настроенным правилам и не используют в своей работе алгоритмы и протоколы, которые не соответствуют настроенной политике (за исключением случаев, когда администратор явно указывает программе выполнить данное действие). Это значит, что политика применяется к поведению программ по умолчанию при работе с предоставленной системой конфигурацией, но при необходимости ее можно переопределить.

В системе поддерживаются следующие предопределенные политики:

- **DEFAULT** – уровень общесистемной криптографической политики по умолчанию предлагает безопасные настройки для текущих моделей угроз. Он поддерживает протоколы TLS 1.2 и 1.3, а также протоколы IKEv2 и SSH2. Ключи RSA и параметры Диффи-Хеллмана принимаются, если их длина не менее 2048 бит.
- **LEGACY** – совместим с более ранними системами и менее безопасен из-за увеличенной поверхности атаки. Помимо алгоритмов и протоколов уровня DEFAULT, он включает поддержку протоколов TLS 1.0 и 1.1. Алгоритмы DSA, 3DES и RC4 разрешены, а ключи RSA и параметры Диффи-Хеллмана принимаются, если их длина не менее 1023 бит.
- **FUTURE** – более строгий уровень безопасности, предназначенный для тестирования возможной будущей политики. Политика не позволяет использовать SHA-1 в алгоритмах подписи. Он поддерживает протоколы TLS 1.2 и 1.3, а также протоколы IKEv2 и SSH2. Ключи RSA и параметры Диффи-Хеллмана принимаются, если их длина не менее 3072 бит. Если система имеет доступ в Интернет, есть вероятность столкнуться с проблемами совместимости.

Подробную информацию о криптографических политиках системы см. в нашей статье «Общесистемные криптографические политики».

Установка пакетов

Пакет **openssl-gost-engine**, обеспечивающий поддержку алгоритмов ГОСТ, по умолчанию предустановлен в РЕД ОС. Однако если по каким-либо причинам в вашей системе пакет отсутствует, для его установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install openssl-gost-engine
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Включение поддержки алгоритмов шифрования ГОСТ

Для активации поддержки ГОСТ в **openssl** выполните:

```
openssl-switch-config gost
```

Для проверки используемой в системе политики шифрования выполните:

```
update-crypto-policies --show
```

Затем примените модуль политики, определяющий используемые методы шифрования ГОСТ:

- для поддержки *стандартных* типов шифрования выполните команду:

```
update-crypto-policies --set <политика_шифрования>:GOST
```

- для поддержки *расширенных* типов шифрования выполните:

```
update-crypto-policies --set <политика_шифрования>:TLS-GOST
```

Модуль политики **GOST**, поддерживающий *стандартные* типы шифрования, добавляет поддержку:

- алгоритмов электронной цифровой подписи (ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012).
- алгоритмов вычисления хеш-функции “Стрибог” (ГОСТ Р 34.11-2012).
- алгоритмов симметричного шифрования (ГОСТ 28147-89).
- алгоритмов согласования ключей (VKO ГОСТ Р 34.10 2001, VKO ГОСТ Р 34.10 2012).

Модуль политики **TLS-GOST**, поддерживающий *расширенные* типы шифрования, добавляет к стандартному набору типов шифрования поддержку следующих алгоритмов:

- алгоритм блочного шифрования “Магма” (ГОСТ Р 34.12-2018).
- алгоритм блочного шифрования “Кузнечик” (ГОСТ Р 34.12-2018).

Также данный модуль исключает тип шифрования **3DES** и способы обмена ключами **RSA**, **PSK** и **DHE_DSS**.

Проверка поддержки ГОСТ в OpenSSL

После проведения настройки проверьте, видит ли **OpenSSL** алгоритмы ГОСТ, командой:

```
openssl ciphers | tr ":" "\n" | grep GOST

GOST2012-MAGMA-MAGMAOMAC
GOST2012-KUZNYECHIK-KUZNYECHIKOMAC
LEGACY-GOST2012-GOST8912-GOST8912
IANA-GOST2012-GOST8912-GOST8912
GOST2001-GOST89-GOST89
```

Пример генерации ключей

Генерация закрытого ключа и создание сертификата с подписью ГОСТ производится следующей командой:

```
openssl req -x509 -newkey gost2012_256 -pkeyopt paramset:A -nodes -keyout key.pem -out cert.pem -md_gost12_256
```

Для проверки сертификата выполните команду:

```
openssl x509 -in cert.pem -text -noout

Certificate:
    Dat a:
        Version: 3 (0x2)
        Serial Number:
            17:86:3c:c0:8c:62:36:af:88:3c:19:01:34:bb:19:92:61:38:5a:37
        Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
        Issuer: C = ru, ST = Russia, L = Moscow, O = red-soft, OU = drsp, CN = root, emailAddress = root
        Validity
            Not Before: Mar 15 11:24:48 2022 GMT
            Not After : Apr 14 11:24:48 2022 GMT
        Subject: C = ru, ST = Russia, L = Moscow, O = red-soft, OU = drsp, CN = root, emailAddress = root
        Subject Public Key Info:
            Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus
                Public key:
                    X:27F4547D48EFAAE904FDCDCD190EB702858B77A796600E175FDEDA8BA35E3C1A
                    Y:35D4E769099EDBC4461A8E67510897D98FD59C4F4D34F08F722899EAD7ABEF81
                Parameter set: id-GostR3410-2001-CryptoPro-A-ParamSet
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                4B:E5:69:DE:B5:00:AE:01:71:56:97:C8:C5:30:8C:B1:5F:5E:AF:AF
            X509v3 Authority Key Identifier:
                keyid:4B:E5:69:DE:B5:00:AE:01:71:56:97:C8:C5:30:8C:B1:5F:5E:AF:AF

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
        3e:94:02:7d:82:7a:52:5c:4d:09:8b:ae:c9:51:c1:19:2a:0f:
        c9:ce:39:39:89:27:89:87:e2:e7:bf:f7:9a:b3:be:bd:56:ea:
        27:bf:56:d8:99:a9:96:09:62:a5:49:04:69:d1:ea:b3:0f:fa:
        92:04:6a:da:27:79:49:ac:79:bd
```

Возврат настроек по умолчанию

Для возврата к настройкам по умолчанию выключите поддержку ГОСТ в **openssl** командой:

```
openssl-switch-config default
```

и примените необходимую общесистемную политику шифрования:

```
update-crypto-policies --set <политика_шифрования>
```

Fail2Ban - сервис блокировки хостов

Установка и запуск
Основные настройки и примеры использования
Параметры конфигурационного файла
Настройка защиты SSH
Блокировка нежелательного трафика
Настройка блокировки для Asterisk
Работа со списком заблокированных адресов
Пример работы fail2ban

Fail2Ban – это сервис для блокировки хостов, вызывающих множественные ошибки при попытках аутентификации.

Fail2Ban работает путем мониторинга файлов журналов (например, **/var/log/auth.log**, **/var/log/apache/access.log** и др.) для выбранных записей и запуска сценариев на их основе. Чаще всего это используется для блокировки выбранных IP-адресов, которые могут принадлежать хостам, пытающимся нарушить безопасность системы. Он может запретить любой IP-адрес хоста, который делает слишком много попыток входа в систему или выполняет любые другие нежелательные действия в течение периода времени, определенного администратором. Включает поддержку как **IPv4**, так и **IPv6**. Опционально более длительные запреты могут быть настроены специально для нарушителей, которые продолжают возвращаться.

Fail2Ban обычно настраивается на разблокировку заблокированного хоста в течение определенного периода времени, чтобы не "блокировать" любые подлинные соединения, которые могли быть временно неправильно сконфигурированы. Время блокировки нежелательных хостов в несколько минут, обычно является достаточным, чтобы снизить вероятность сетевой атаки или атаки подбора пароля по словарю, например, при подключении по **ssh**.

Стандартная конфигурация *Fail2Ban* поставляется с фильтрами для *Apache, Lighttpd, sshd, vsftpd, qmail*. Фильтры определяются регулярными выражениями Python, которые могут быть удобно настроены администратором, знакомым с регулярными выражениями. С помощью фильтров можно блокировать попытки доступа от вредоносного хоста к определенным сетевым службам.

Fail2Ban можно настроить для мониторинга любой службы, которая записывает попытки аутентификации в файл журнала. Для блокировки IP-адресов нежелательных хостов *Fail2Ban* использует правила *iptables*.

Установка и запуск Fail2Ban

Установка производится командой:

```
dnf install fail2ban
systemctl start fail2ban
systemctl enable fail2ban
```

Основные настройки и примеры использования приложения Fail2Ban

Все конфигурационные файлы программы находятся в каталоге **/etc/fail2ban**. Для установки собственных настроек необходимо создать файл с таким же именем и расширением **.local**.

Основные параметры конфигурационного файла jail.conf

Конфигурационный файл **jail.conf** используется для создания ограничивающих правил для различных программ и имеет параметры, которые описаны ниже:

- *action* — действие, которое будет выполняться, если *Fail2ban* обнаружит активность, соответствующую критериям поиска;
- *ignoreip* — задает список IP-адресов, которые нужно исключить из алгоритмов Fail2ban. К ним не будут применяться ограничения, так что выбирайте их аккуратно. Диапазоны и IP-адреса стоит разделить пробелом. Сюда можно добавить локальный IP, а также IP-адрес, с которого вы будете подключаться сами, чтобы у вас не возникло проблем при входе;
- *bantime* — время в секундах, на которое клиенту будет закрыт доступ к серверу, если он не сможет авторизоваться;
- *maxretry* — указывает количество попыток перед тем, как доступ будет заблокирован;
- *findtime* — время в секундах, на протяжении которого рассчитывается *maxretry*.

Настройка защиты SSH

Сначала копируем содержимое **jail.conf** в **jail.local**:

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

По умолчанию **jail.local** работает только для *SSH*. Примерная настройка файла **jail.local** для *SSH*:

```
[sshd]
enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
logpath  = /var/log/auth.log
findtime    = 600
maxretry    = 3
bantime     = 21600
```

Блокировка нежелательного трафика к определенному URL для NGINX

Откроем файл конфигурации:

```
nano /etc/fail2ban/jail.local
```

И добавим в конец:

```
[nginx-req-limit]
enabled = true
filter = nginx-req-limit
action = iptables-multiport[name=ReqLimit, port="http,https", protocol=tcp]
logpath = /var/log/nginx/*error.log
findtime = 600
bantime = 7200
maxretry = 10
```

Настройка блокировки для Asterisk

Добавляем в конец файла **jail.local**:

```
[asterisk]
 enabled = true
 action = iptables-allports[name=asterisk, protocol=all]
 logpath = /var/log/asterisk/messages
 bantime = 86400
```

Работа со списком заблокированных адресов

- Получить статистику заблокированных адресов можно следующей командой:

```
fail2ban-client status <имя_правила>
```

- Для удаления адреса из списка вводим:

```
fail2ban-client set <имя правила> unbanip
```

- Получить список правил можно командой:

```
fail2ban-client status
```

- После необходимо перечитать правила:

```
firewall-cmd --reload
```

- После каких либо изменений в конфигурационных файлах перезапустите *faile2ban* командой:

```
systemctl restart fail2ban
```

Пример работы fail2ban

Пример блокировки подключения к ssh-серверу после нескольких неудачных попыток авторизоваться. Для примера было взято правило для *ssh*. В примере пользователь попытался 3 раза ввести пароль для доступа к ssh-серверу, и после неудачных попыток последующие соединения с IP-адреса клиента были заблокированы.

Попытка пользователя авторизоваться на ssh-сервере:

После неудачных попыток ввода пароля, дальнейшие соединения к ssh-серверу были отказаны.

XCA - программа для управления асимметричными ключами

Установка XCA
Обзор простейших функций XCA
Начало работы с XCA
Примеры работы с XCA
Создание корневого сертификата

X Certificate and Key management (**XCA**) - это программа, предоставляющая интерфейс для управления асимметричными ключами *RSA, DSA and EC private keys, Smartcards and CRLs*. Программа может использоваться для создания и подписания сертификатов в рамках небольшого **ЦС** (**CA**) и создать собственную инфраструктуру открытых ключей (**PKI**).

Возможности:

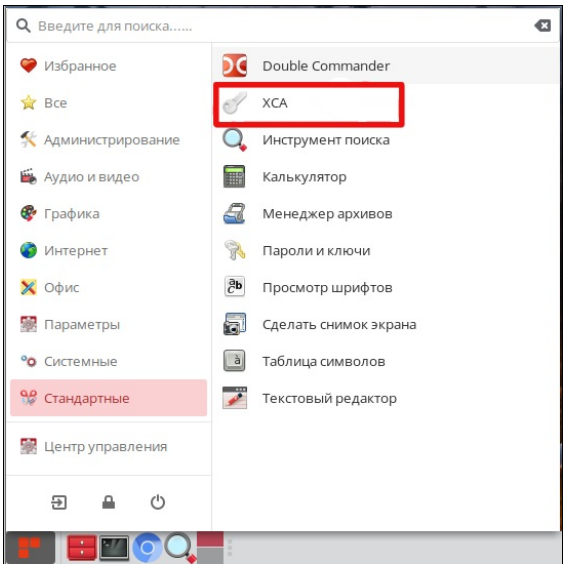
1. Создание собственного **PKI**, закрытых ключей, сертификатов, запросов или CRL. 2. Экспорт и импорт ключей в форматах: **PEM, DER, PKCS#7, PKCS#12**. 3. Управления смарт-картами через интерфейс **PKCS#11**. 4. Функция экспорта сертификатов и запросов в виде конфигурационного файла **OpenSSL**. 5. Создание шаблонов для сертификатов, а также создание шаблонов на основе готовых сертификатов. 6. Преобразование существующих сертификатов или запросов в шаблоны. 7. Получение широкой поддержки расширений **x509v3** таких же гибких, как OpenSSL, но более удобных для пользователя. 8. Запись сертификатов на токен.

Установка XCA

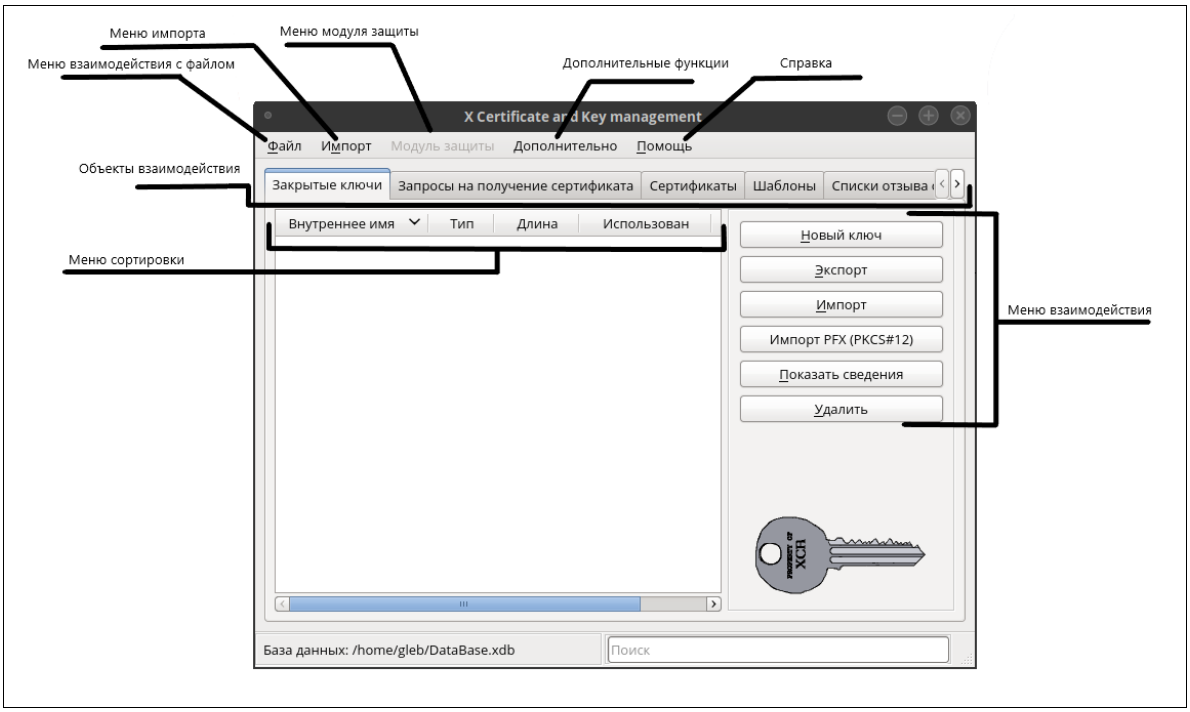
Для установки XCA выполните команду:

```
dnf install xca
```

После установки программу можно будет найти в **"Меню" – "Стандартные"**.



Обзор простейших функций XCA



Меню «*Файл*» позволяет создать или открыть уже существующую базу данных, а так же настроить язык всей XCA и настроить саму XCA. Меню «*Импорт*» позволяет импортировать уже имеющиеся ключи, запросы, сертификаты и др. в базу данных. Меню «*Модуль защиты*» позволяет настроить защиту базы данных. Меню «*Дополнительно*» имеет дополнительные функции для взаимодействия с базой данных, такие как экспорт списка сертификатов или генерация параметров Диффи – Хэллмана.

Начало работы с XCA

Для начала работы с приложением создайте базу данных. Для этого необходимо выбрать в меню **«Файл» - «Новая база данных»**.

Работа с токенами/смарт-картами:

1. Для того чтобы в XCA начать работать с токенами, нужно подключить библиотеку **PKCS#11** данного токена. Библиотеку PKCS#11 под РЕД ОС с поддержкой RSA для *Актив Рутокен ЭЦП* можно скачать по ссылке: https://www.rutoken.ru/support/download/pkcs/. Установите командой:

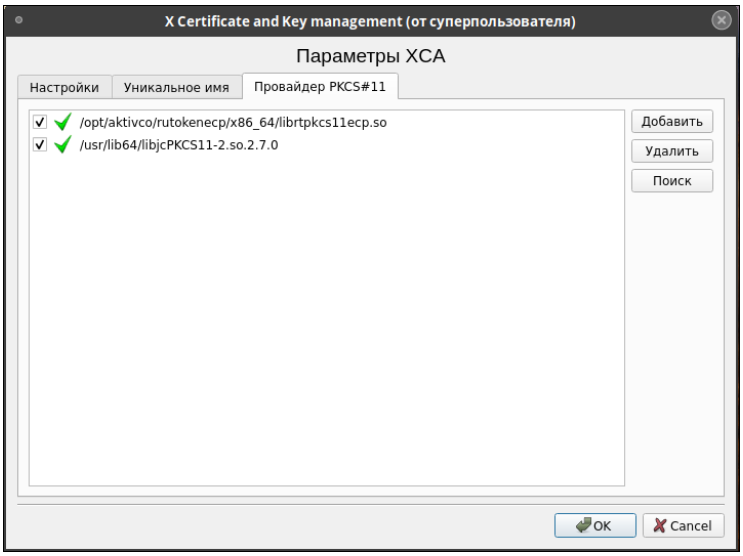
```
dnf localinstall librtpkcs11ecp-2.0.11.0-1.x86_64.rpm
```

Библиотеку PKCS#11 под РЕД ОС с поддержкой RSA для *Аладдин JaCarta PKI/GOST* можно скачать по ссылке: https://www.aladdin-rd.ru/support/downloads/jacarta. Сначала необходимо разархивировать все файлы, затем установить командой:

```
dnf localinstall jcpkcs11-2_2.7.0.443_x64.rpm
dnf localinstall jacartauc_2.13.0.3084_ro7.2_x64.rpm
```

2. Переходим в меню **«Файл» - «Настройки» - «Провайдер PKCS#11»**. 3. Нажимаем «*Добавить*» и ищем файл «**libjcPKCS11-2.so**» и «**librtpkcs11ecp.so**». Они могут находиться в директории **/usr/lib** или **/usr/lib64**. Если вы не можете найти этот файл, зайдите в терминал и найдите его с помощью команды:

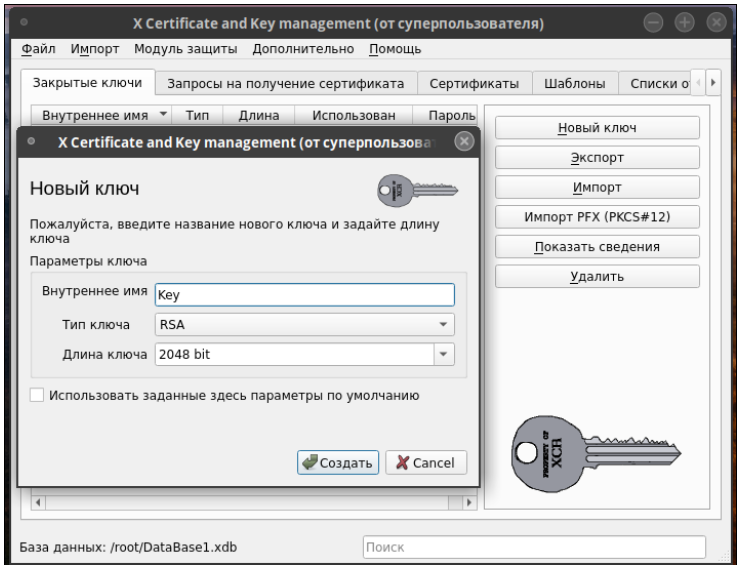
```
sudo find /usr -iname '*pkcs11*'
```



Примеры работы с XCA

Создание ключа SSH

1. Для начала перейдите на вкладку «*Закрытые ключи*». 2. Нажмите на кнопку «*Новый ключ*». 3. В поле «*Тип ключа*» выберите **RSA**. В поле «*Длина ключа*» выберите **2048 bit**. Имя ключу дайте на свое усмотрение.



Экспорт ключей

Для экспорта **открытого** ключа необходимо выполнить следующие действия:

1. Перейти на вкладку «*Закрытые ключи*» ; 2. Выбрать нужный «*Сертификат клиента*» ; 3. Нажать кнопку «*Экспорт*» ; 4. В появившемся окне в поле «*Формат сертификата*» нужно выбрать **Открытый ключ SSH2 (*.pub)** и указать путь к файлу, затем нажать «*OK*».

Для экспорта **закрытого** ключа необходимо выполнить следующие действия:

1. Перейти на вкладку «*Закрытые ключи*» ; 2. Выбрать нужный закрытый ключ сервера; 3. Нажать кнопку «*Экспорт*» ; 4. В появившемся окне в поле «*Формат для экспорта*» нужно выбрать **Закрытый ключ PEM (*.pem)**, указать путь к файлу, затем нажать «*OK*».

Для экспорта **закрытого ключа, зашифрованного паролем**, необходимо выполнить следующие действия:

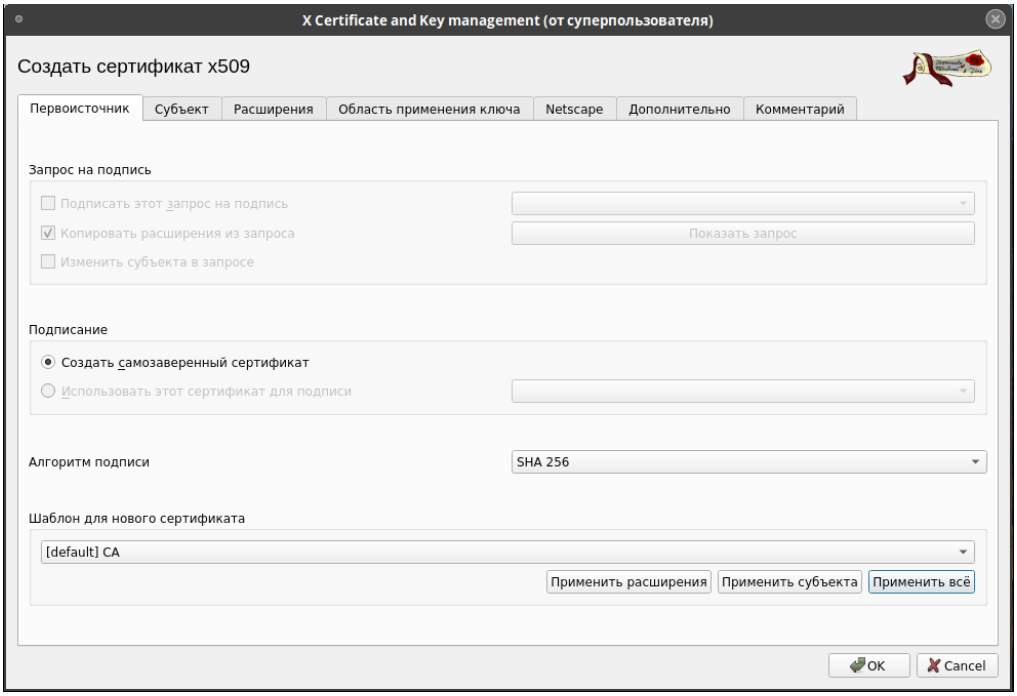
1. Перейти на вкладку «*Закрытые ключи*» ; 2. Выбрать нужный закрытый ключ сервера; 3. Нажать кнопку «*Экспорт*» ; 4. В появившемся окне в поле «*Формат для экспорта*» нужно выбрать **Зашифрованный ключ PEM (*.pem)**, указать путь к файлу, затем нажать «*OK*»; 5. В появившемся окне *Certificate and Key management* нужно ввести пароль, который будет требоваться для доступа к этому ключу.

Создание корневого сертификата

Корневой сертификат (**CA**) — часть ключа, которым центры сертификации подписывают выпущенные *SSL*-сертификаты. Выдавая корневой сертификат, каждый такой центр гарантирует, что пользователи или организации, запросившие SSL, верифицированы и действия с доменом легальны.

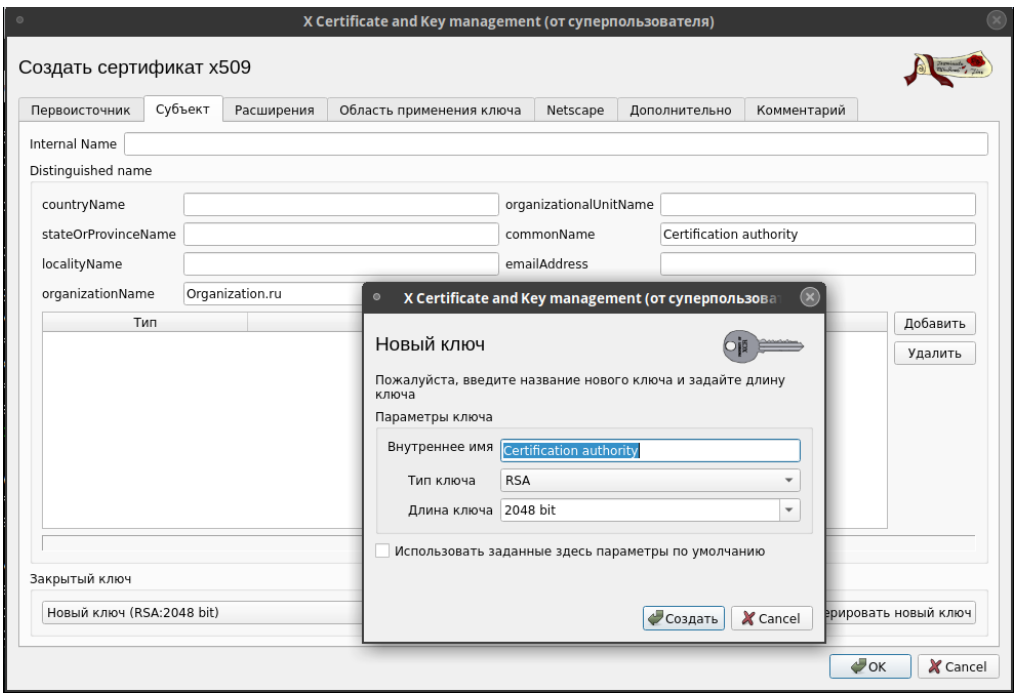
Для создания такого сертификата необходимо выполнить следующие действия:

1. Перейти на вкладку «*Сертификаты*» и выбрать «**Новый сертификат**» ; 2. Поставить галочку на пункт «*Создать самоподписанный сертификат...*»; 3. Выбрать «*Шаблон для нового сертификата*» - «**[Default] CA**»; 4. Нажать кнопку «**Применить всё**»;

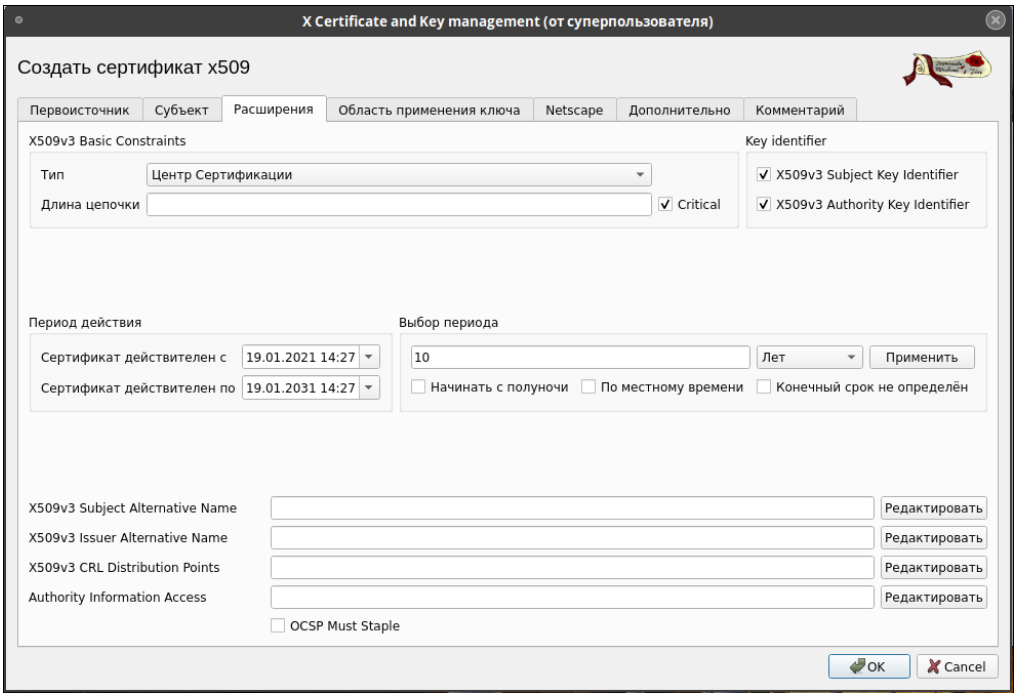


5. Перейти на вкладку «*Субъект*» («*Владелец*») ; 6. В поле «*organizatioName*» указать имя вашего домена; 7. В поле «*commonName*» указать имя «**Certification authority**» ; 8. По необходимости заполнить остальные поля;праитарна 9. Выбрать «*Создать новый ключ*»:

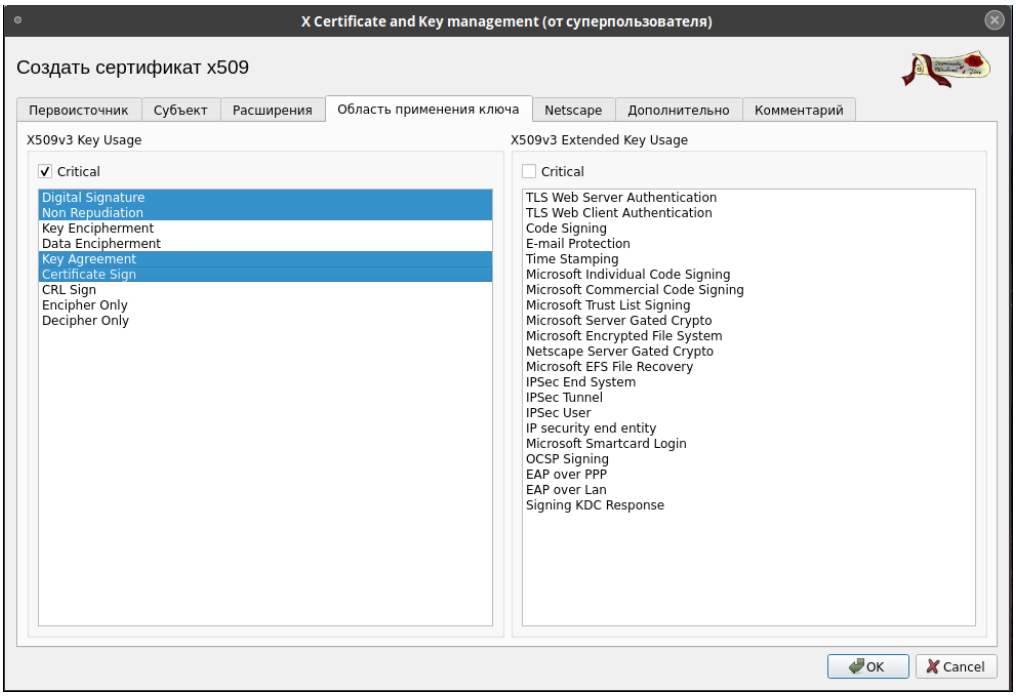
- В поле «Имя ключа» указать имя ключа, например «**Certification authority**»;
- Нажать «**Создать**»;



10. Перейти на вкладку «*Расширения*» ; 11. Убедиться, что выбран «*Тип*» «**Центр Сертификации**» ; 12. Отметить пункты «*Critical*», «*Subject Key identifier*», «*Authority key Identifier*»; 13. Определить срок действия сертификата: «*Временной диапазон*» => **10 (лет)**;



14. Перейти на вкладку «*Область применения ключа*»; 15. Отметить пункт «*Critical*», выбрать функции «**Digital Signature**», «**Non repudation**», «**Certificate Sign**», «**CRL Sign**»; 16. Сохранить созданный сертификат: «*Применить*» - «*Да*».



Блокировка макросов в LibreOffice

Макрос — это записанный пользователем программный алгоритм, позволяющий автоматизировать шаблонные действия при создании или редактировании документов.

Благодаря макросам пользователь может увеличить эффективность работы с приложением, а также гораздо быстрее выполнять определенные задачи: производить обработку внешних файлов, загрузку и передачу файлов и данных через интернет, чтение и изменение настроек операционной системы.

Однако не все макросы могут приносить пользу. Для повышения безопасности пользователя и предотвращения непреднамеренного открытия файлов, включающих активное содержимое, для офисных пакетов в РЕД ОС предусмотрена утилита с функцией блокировки макросов.

Данная функция помогает решить две основные задачи - защита от выполнения вредоносного кода при открытии документов и запрет исполнения произвольного кода через механизм макросов.

Для установки утилиты блокировки макросов перейдите в сеанс пользователя **root**:

```
su -
```

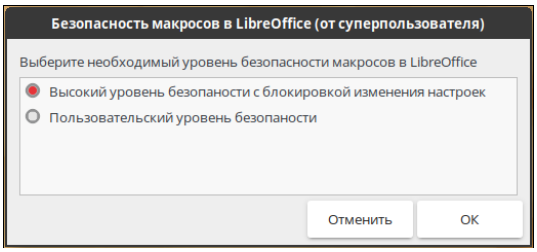
и выполните команду:

```
dnf install lo-macros-lock
```

После установки программа будет доступна из «**Главного меню**» - «**Администрирование**» - «**Безопасность макросов в LibreOffice**».

Для работы в программе необходимы привилегии пользователя **root**, поэтому при запуске необходимо ввести пароль суперпользователя.

После успешной аутентификации будет предложено выбрать необходимый уровень защиты:



После выбора нажмите «**OK**», чтобы изменения вступили в силу.

Для установки необходимого уровня защиты можно использовать консольный вариант работы с утилитой.

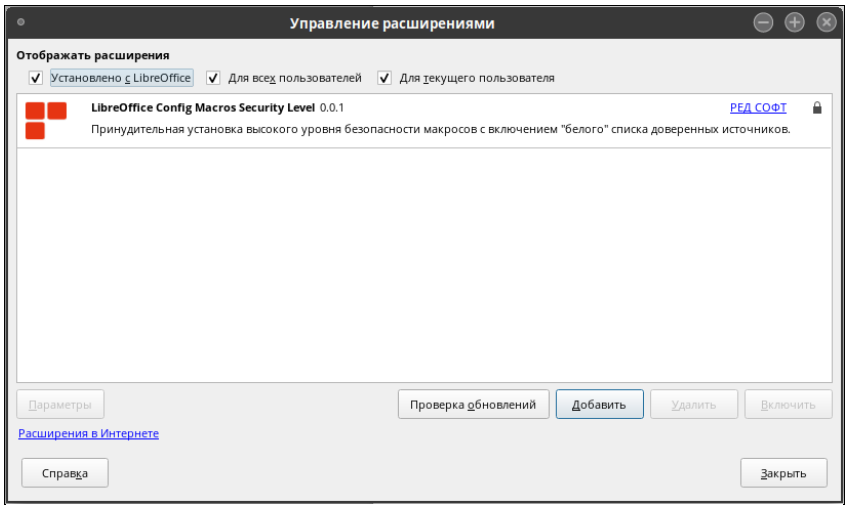
Для выбора «**Высокого уровня безопасности**» выполните:

```
lo-macros-lock -1
```

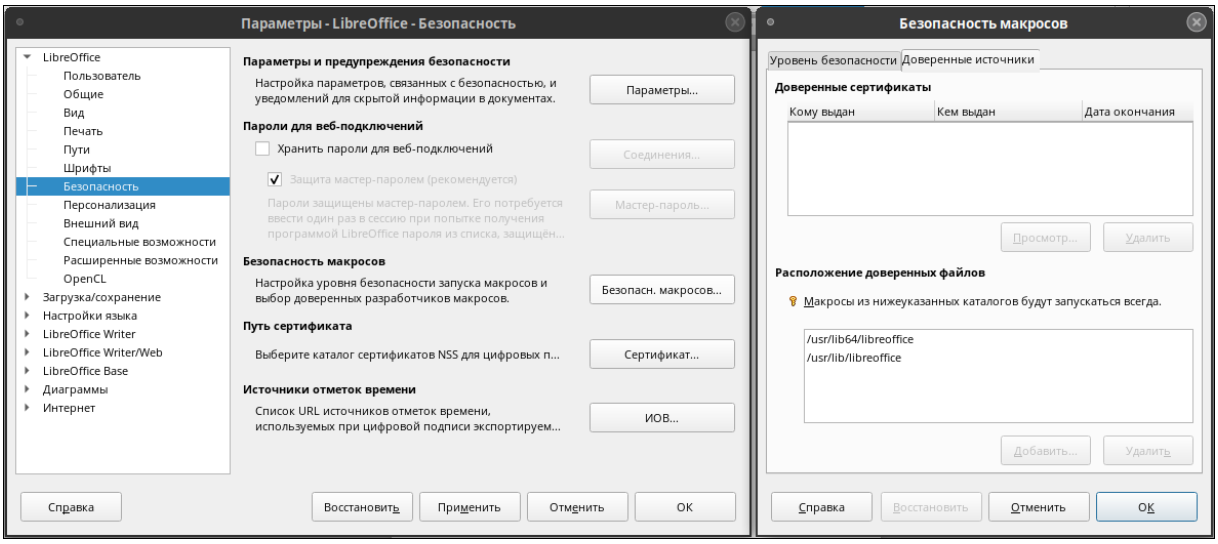
Для выбора «**Пользовательского уровня безопасности**» выполните:

```
lo-macros-lock -0
```

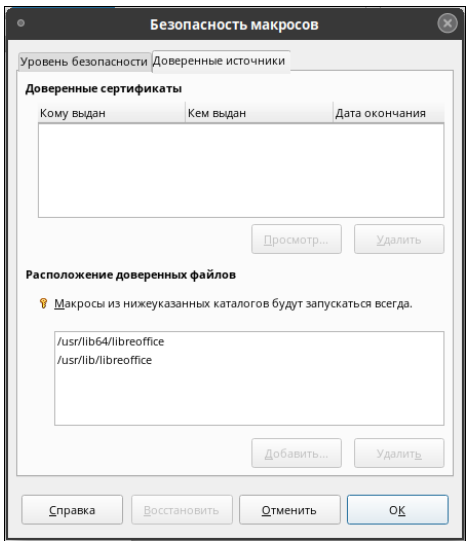
При выборе высокого уровня безопасности в папку системных расширений LibreOffice устанавливается блокирующее расширение, отображаемое при запуске любого офисного приложения.



В «**Параметрах**» LibreOffice при этом будет заблокирована возможность изменения режимов безопасности, а уровень безопасности будет установлен «**Очень высокий**».



В список «**Доверенных источников**» будут внесены системные каталоги LibreOffice без права пользователю их изменять.



ВАЖНО!

Будьте внимательны, запускайте макросы только из **надежных** источников!

Установка КриптоПро CSP 4.0

Установка CryptoPro CSP 4.0.0
Проверка лицензии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** CryptoPro 4.0.0 x64

КриптоПро — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами, организации структуры PKI и т.д.

Сайт: http://www.cryptopro.ru/

Примечание.

Для корректной работоспособности электронной подписи в информационных системах необходимо выполнить установку в последовательности:

1. Установить программное обеспечение для работы с корневыми и личными сертификатами по инструкции.
2. Установить браузер Chromiuim.
3. Установить плагин Госуслуг и КриптоПро, в зависимости от системных требований к информационной системе.

Вы можете подробнее ознакомиться с примером установки и настройки криптопровайдера CryptoPro, просмотрев наши обучающие видео:

- на **RuTube** — Установка КриптоПро CSP в РЕД ОС;
- в **Яндекс.Дзен** — Установка КриптоПро CSP в РЕД ОС;
- в **VK Видео** — Установка КриптоПро CSP в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка CryptoPro 4.0.0 x64

1. Скачайте архив с сайта КриптоПро по ссылке.

2. Распакуйте архив в папку (в примере **/home/test/**).

```
cd /home/test
tar -xvf linux-amd64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-amd64
```

4. Установите права на запуск:

```
chmod +x install_gui.sh
```

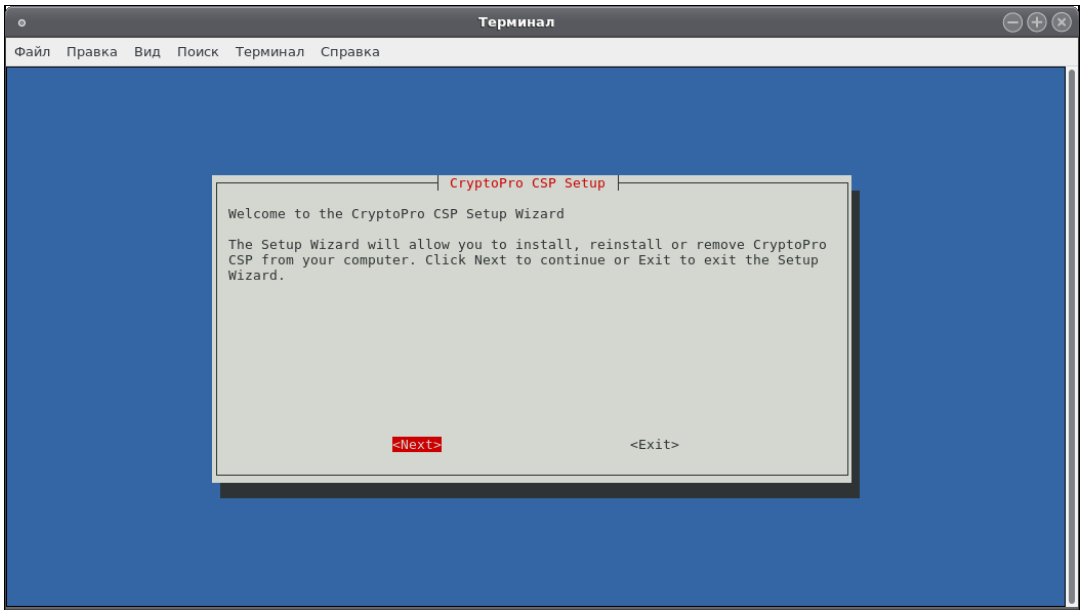
4.1 Выполните следующую команду (для того чтобы далее выполнять команды от пользователя **root**):

```
su root
```

5. Установите КриптоПро, выполнив команду:

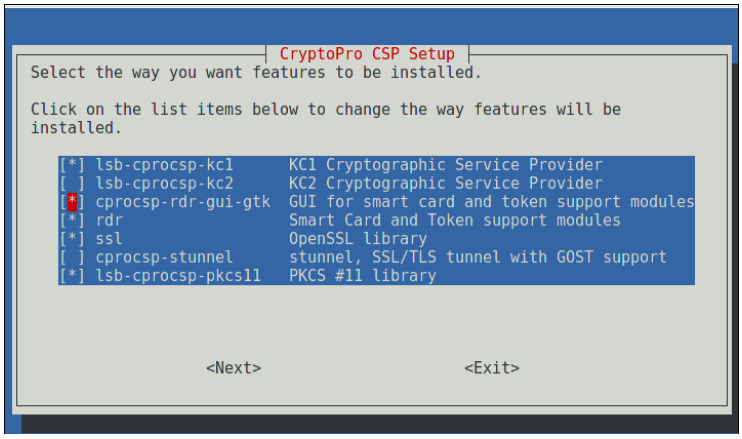
```
./install_gui.sh
```

Появится окно установки КриптоПро:

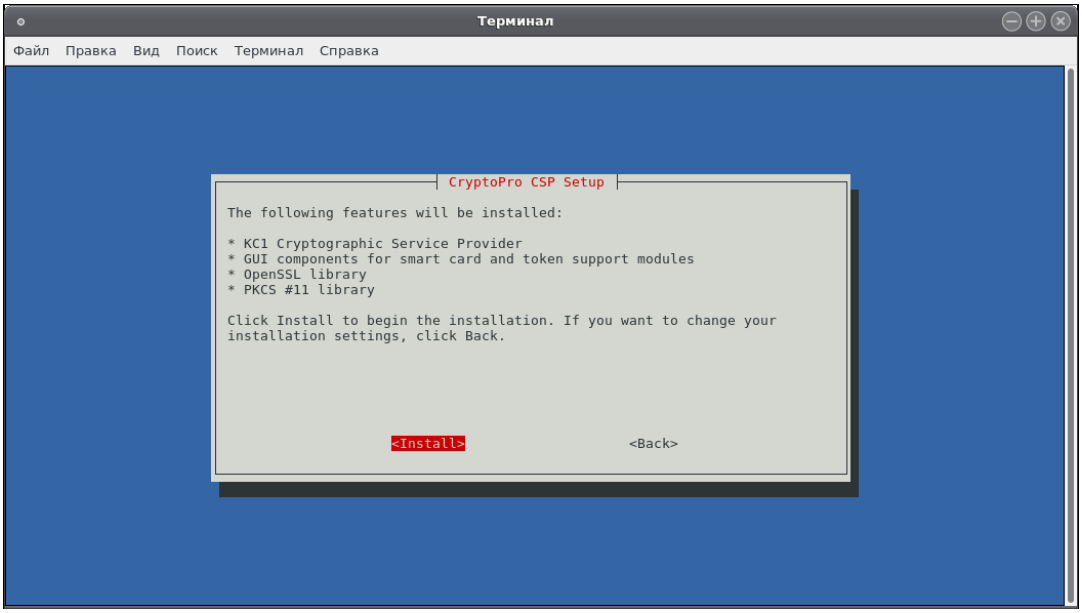


Нажмите кнопку «**Next**» для продолжения установки.

В следующем окне выберите пакеты, указанные на скриншоте:



Нажмите кнопку «**Next**» для продолжения установки:



Нажмите «**Install**» для установки пакетов.

6. Установите дополнительные пакеты и драйверы.

6.1 Установка драйверов и библиотек для работы **Рутокен S**, **Рутокен ЭЦП 2.0**, **Рутокен ЭЦП 3.0**.

Загрузите с официального сайта библиотеку **PKCS#11** с поддержкой RSA для Актив Рутокен ЭЦП. Перейдите в каталог с загруженным файлом (в примере ***/home/user/Загрузки***):

```
cd /home/user/Загрузки
```

Установите библиотеку командой:

```
dnf localinstall ./librtpkcs11ecp-2.15.1.0-1.x86_64.rpm
```

где **librtpkcs11ecp-2.15.1.0-1.x86_64.rpm** замените на актуальную версию.

Установите утилиту для обнаружения внешних устройств:

```
dnf install pcsc-tools
```

Для работы **Рутокен S** установите драйвер:

```
dnf install ifd-rutokens
```

6.2 Установка драйверов для токенов **Jacarta**:

Перейдите в папку:

```
cd /home/test/linux-amd64
```

Выполните команду установки:

```
dnf install cprocsp-rdr-jacarta*.rpm
```

Проверка лицензии

Вывод серийного номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

Ввод номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

Установка КриптоПро CSP 5.0

Установка CryptoPro CSP 5.0.0
Проверка лицензии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** CryptoPro 5.0.0 x64

КриптоПро — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами, организации структуры PKI и т.д.

Сайт: http://www.cryptopro.ru/

Примечание.

Для корректной работоспособности электронной подписи в информационных системах необходимо выполнить установку в последовательности:

1. Установить программное обеспечение для работы с корневыми и личными сертификатами по инструкции.
2. Установить браузер Chromiuim.
3. Установить плагин Госуслуг и КриптоПро, в зависимости от системных требований к информационной системе.

Вы можете подробнее ознакомиться с примером установки и настройки криптопровайдера CryptoPro, просмотрев наши обучающие видео:

- на **RuTube** — Установка КриптоПро CSP в РЕД ОС;
- в **Яндекс.Дзен** — Установка КриптоПро CSP в РЕД ОС;
- в **VK Видео** — Установка КриптоПро CSP в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка CryptoPro 5.0.0 x64

1. Скачайте архив с сайта КриптоПро по ссылке.

2. Распакуйте архив в папку (в примере **/home/test/**).

```
cd /home/test
tar -xvf linux-amd64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-amd64
```

4. Установите права на запуск:

```
chmod +x install_gui.sh
```

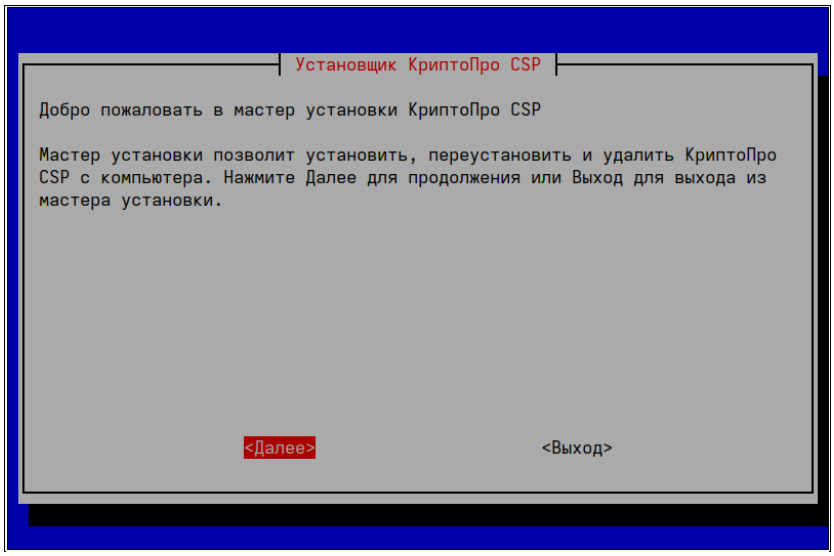
4.1 Выполните следующую команду (для того чтобы далее выполнять команды от пользователя **root**):

```
su root
```

5. Установите КриптоПро, выполнив команду:

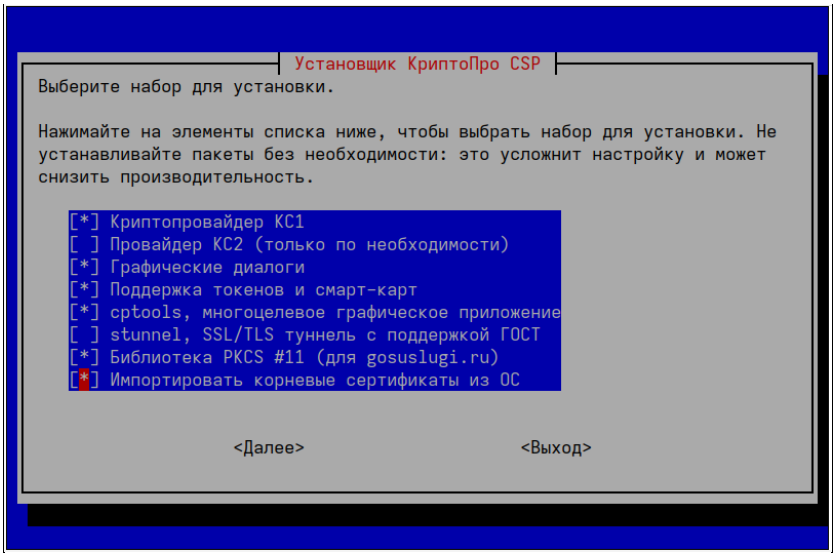
```
./install_gui.sh
```

Появится окно установки КриптоПро:

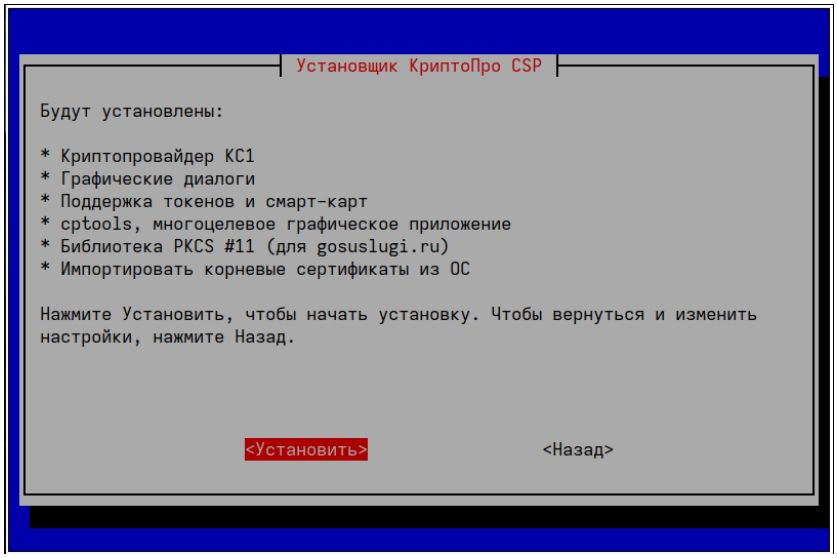


Нажмите кнопку «**Далее**» для продолжения установки.

В следующем окне выберите пакеты, указанные на скриншоте:



Нажмите кнопку «**Далее**» для продолжения установки:



Нажмите «**Установить**» для установки пакетов.

6. Установите дополнительные пакеты и драйверы.

6.1 Установка драйверов и библиотек для работы **Рутокен S**, **Рутокен ЭЦП 2.0**, **Рутокен ЭЦП 3.0**.

Загрузите с официального сайта библиотеку **PKCS#11** с поддержкой RSA для Актив Рутокен ЭЦП. Перейдите в каталог с загруженным файлом (в примере ***/home/user/Загрузки***):

```
cd /home/user/Загрузки
```

Установите библиотеку командой:

```
dnf localinstall ./librtpkcs11ecp-2.15.1.0-1.x86_64.rpm
```

где **librtpkcs11ecp-2.15.1.0-1.x86_64.rpm** замените на актуальную версию.

Установите утилиту для обнаружения внешних устройств:

```
dnf install pcsc-tools
```

Для работы **Рутокен S** установите драйвер:

```
dnf install ifd-rutokens
```

6.2 Установка драйверов для токенов **Jacarta**:

Перейдите в папку:

```
cd /home/test/linux-amd64
```

Выполните команду установки:

```
dnf install cprocsp-rdr-jacarta*.rpm
```

Проверка лицензии

Вывод серийного номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

Ввод номера лицензии:

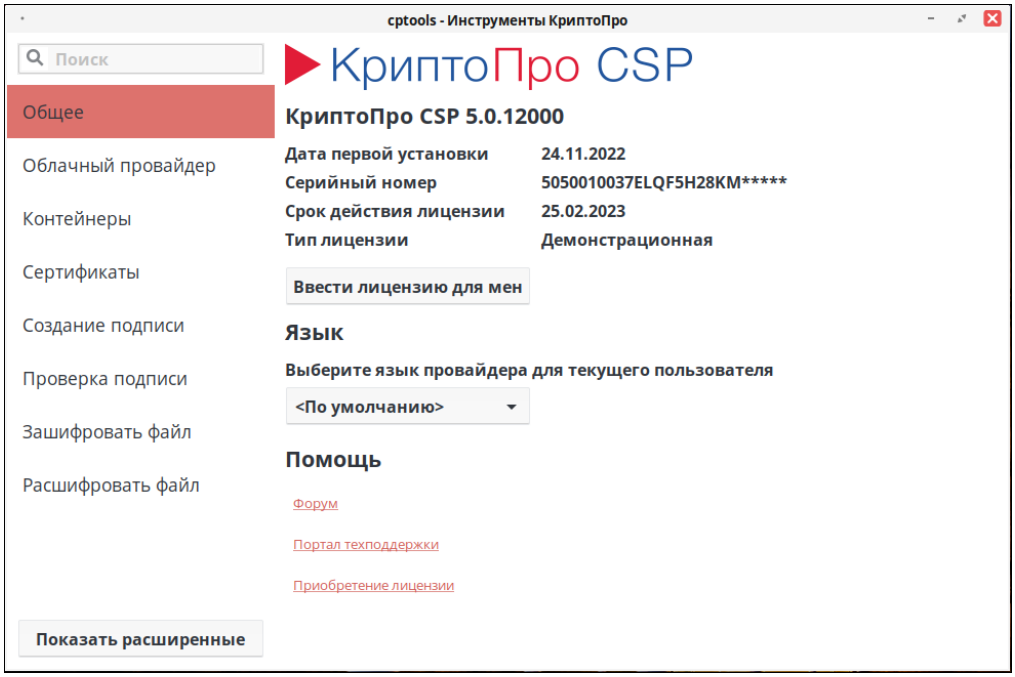
```
/opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

Графические утилиты для работы с КриптоПро CSP

Инструменты КриптоПро
Установка программного обеспечения для работы с сертификатами
Ключевые носители и сертификаты
GOST-CRYPTO-GUI
Подпись документов в LibreOffice

Инструменты КриптоПро

В **КриптоПро** версии **5.0** появилась графическая утилита для работы с сертификатами - **cptools**. Запуск утилиты доступен из «**Главного меню**» – «**Параметры**» – «**Инструменты КриптоПро**».



Запуск из терминала:

```
cptools

или

/opt/cprocsp/bin/*/cptools
```

Установка программного обеспечения для работы с сертификатами

1. Установка средства управления сертификатами **token-manager**:

```
dnf install token-manager python3-chardet
```

1.2 Доступен формат запуска приложения без установки в ОС. Для этого скачайте AppImage и сделайте его исполняемым:

```
wget $(curl -s https://api.github.com/repos/wolandius/token-manager/releases/latest | grep browser_download_url | cut -d\" -f4 | grep 'ro73')
```

- Запуск:

```
chmod +x ./token-manager-*-x86_64.AppImage
./token-manager-*-x86_64.AppImage
```

2. Установка программного обеспечения для подписи файлов **gostcrypto**.

```
dnf install gostcryptogui
```

2.2 Доступен формат запуска приложения без установки в ОС. Для этого скачайте AppImage и сделайте его исполняемым:

```
wget $(curl -s https://api.github.com/repos/wolandius/gost-crypto-gui/releases/latest | grep browser_download_url | cut -d\" -f4 | grep 'ro73')
```

- Запуск:

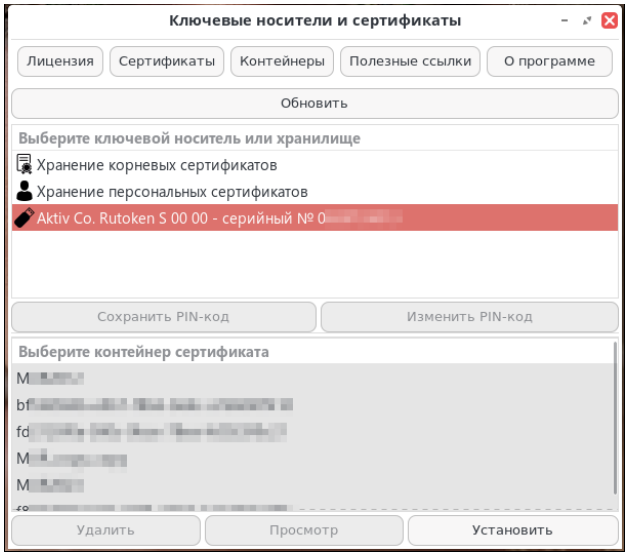
```
chmod +x ./gost-crypto-gui-*-x86_64.AppImage
./gost-crypto-gui-*-x86_64.AppImage
```

Работа с ключевыми носителями и сертификатами

Ключевые носители и сертификаты

Для работы с ключевыми носителями и сертификатами используется утилита «**Ключевые носители и сертификаты**», которую мы установили ранее. Найти его можно в «**Главном меню**» - «**Администрирование**» - «**Ключевые носители и сертификаты**».

Окно программы выглядит следующим образом:



В меню «**Операции**» можно выполнить:

- Ввод лицензии КриптоПро CSP;
- Просмотр лицензии;

- Установка корневых сертификатов;
- Установка списка отозванных сертификатов;
- Запись сертификата в контейнер;
- Экспортировать сертификат из контейнера;
- Связать сертификат с контейнером;
- Просмотр корневых сертификатов;
- Просмотр списков отозванных сертификатов;

- Скопировать контейнер с токена;
- Скопировать контейнер с **usb-flash** накопителя;
- Скопировать токен из HDIMAGE на токен.

Рассмотрим более подробно копирование контейнера с **usb-flash** накопителя.

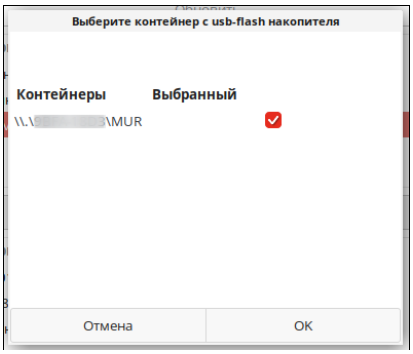
1. Необходимо с **RuToken** скопировать закрытую часть электронной подписи (ЭП) на *usb-flash* накопитель, выполнить это необходимо на КриптоПро в ОС Windows.

Инструкция для Windows находится по ссылке.

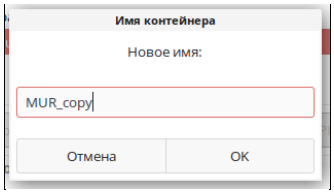
2. Вставьте *usb-flash* накопитель в компьютер и запустите утилиту **Ключевые носители и сертификаты**.

3. Перейдите в меню «**Операции**» и выберите «**Скопировать контейнер с *usb-flash* накопителя**».

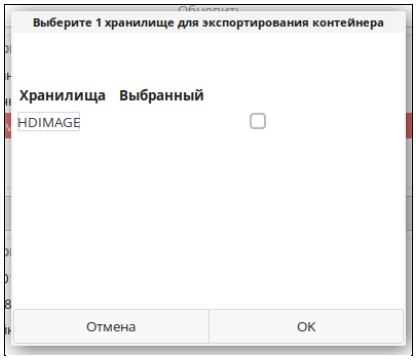
4. Появится окно с выбором контейнера. Выберите необходимый контейнер, отметив чекбокс в поле «**Выбранный**».



5. Задайте имя контейнеру.

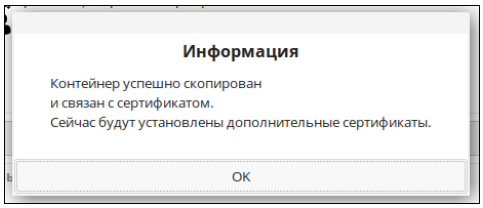


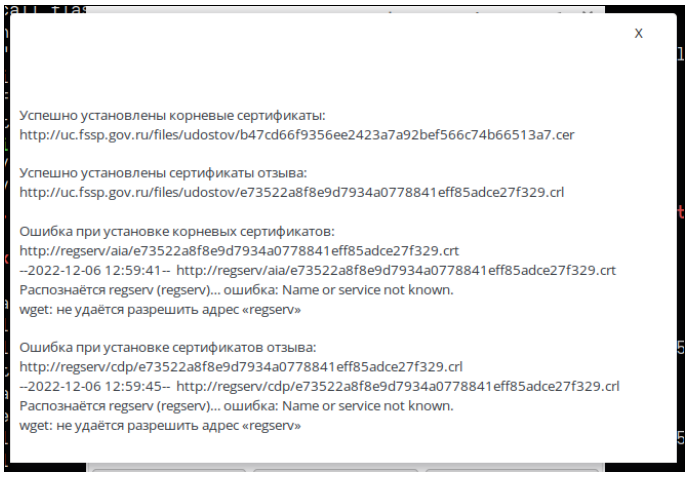
6. Выберите контейнер, в который требуется скопировать.



7. Далее потребуется ввести PIN-код контейнеров.

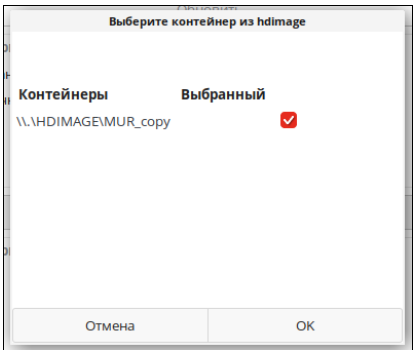
8. Появится окно с успешной привязкой контейнера с сертификата. Сертификат отобразится в «**Личном хранилище сертификатов**».





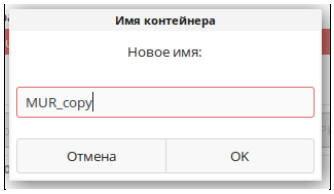
Работа по копированию контейнеров с токена или из **HDIMAGE** имеет схожую логику.

1. Для выбора необходимого контейнера требуется выбрать галочкой необходимый.

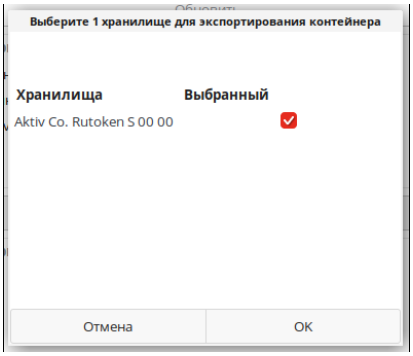


2. Следующим этапом необходимо выбрать пункт назначения копирования.

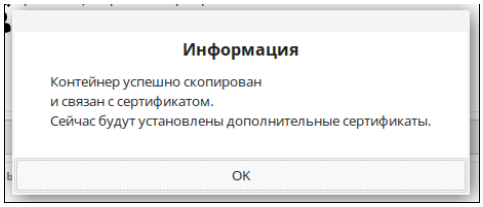
Пользователю предоставляется возможность задать новое имя копируемого контейнера (настоятельно рекомендуем использовать латиницу).

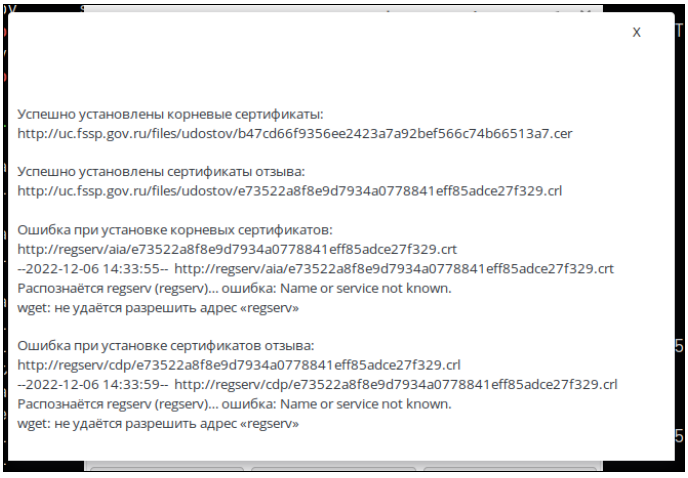


3. Далее выбирается токен или **HDIMAGE**.

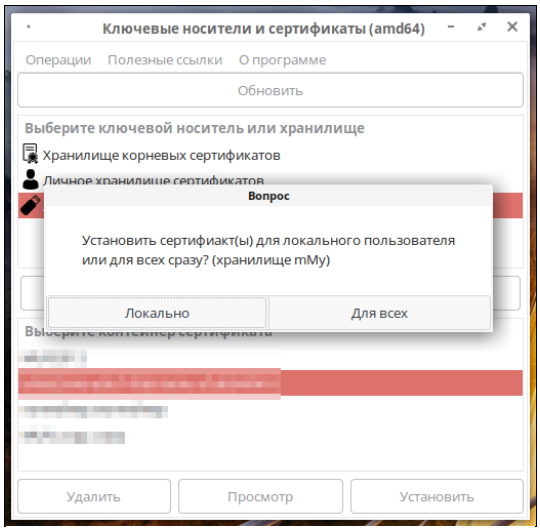


4. После ввода PIN-кодов, в случае успеха, вы увидите сообщение:





Стоит обратить внимание на диалоговое окно, которое добавлено для работы с КриптоПро версии 5 и новее. Данное диалоговое окно позволяет устанавливать сертификаты в машинное хранилище ПК или в личное хранилище пользователя. Вызов диалогового окна происходит при попытке установки из локального файла сертификата или с токена.



В последних версиях **token-manager** была добавлена возможность консольного запуска утилиты с использованием ряда ключей:

```
token-manager.py --help

Подсказки по использованию ключей в token-manager:
В данной реализации token-manager поддерживает явное указание архитектуры КриптоПро, вместо автоматического.
 --amd64         вызов 64-битной версии КриптоПро;
 --ia32          вызов 32-битной версии КриптоПро;
 --aarch64       вызов aarch64 версии КриптоПро;
 --e2k64         вызов e2k64 версии КриптоПро;
 --version       вывод номера версии token-manager;
 --debug-output  пробный вызов основных функций утилиты;
 --debug-output --amd64 пробный вызов основных функций утилиты для архитектуры amd64;
 --debug-output --ia32 пробный вызов основных функций утилиты для архитектуры ia32;
 --debug-output --aarch64 пробный вызов основных функций утилиты для архитектуры aarch64;
 --debug-output --e2k64 пробный вызов основных функций утилиты для архитектуры e2k64;
```

Пример вывода версии утилиты:

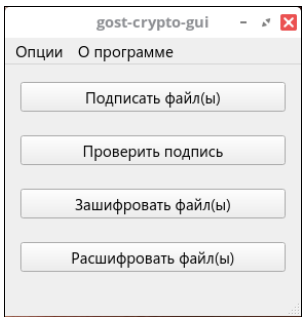
```
token-manager.py --version

token-manager версия 5.2.2
```

GOST-CRYPTO-GUI

Формат подписи может настраиваться в графической утилите **gostcryptogui**, которую мы рассмотрим далее.

Запуск утилиты производится из «**Главного меню**» - «**Администрирование**» - «**Подпись и шифрование файлов**».

Окно программы выглядит следующим образом:

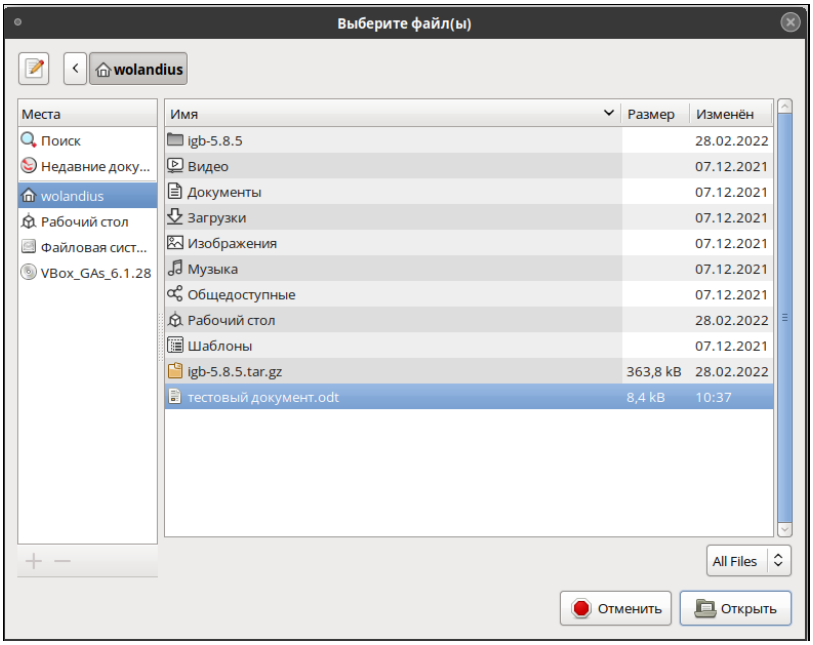


Доступны следующие опции:

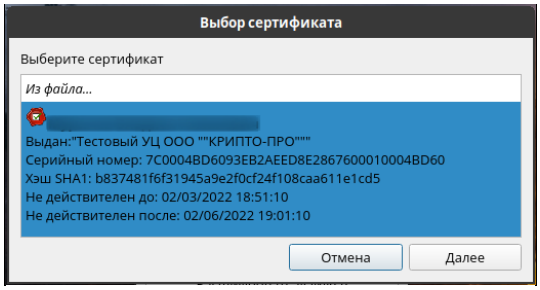
- Криптопровайдер;
- Кодировка файлов;
- Авт. проверка подписи;
- Отсоединённая подпись.

Для примера зашифруйте файл, но с использованием другого сертификата, размещённого на ключевом носителе **Rutoken**.

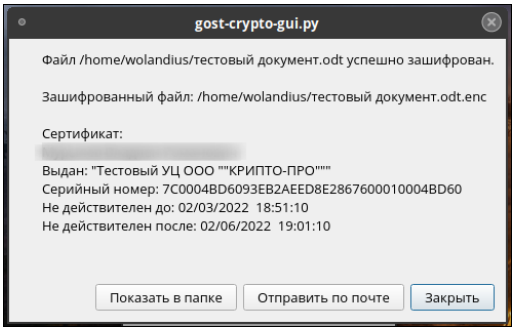
Выберите необходимый файл:



Затем укажите ваш сертификат:

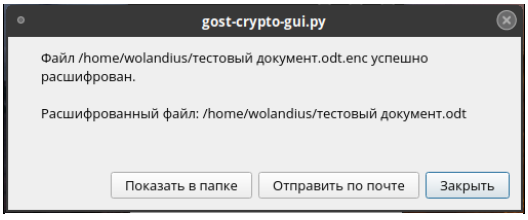


Зашифрованный файл формируется с тем же именем и расширением **.enc**.



После этого попробуйте его расшифровать.

Нажмите «**Расшифровать файл(ы)**», выберите зашифрованный файл, затем сертификат, которым был зашифрован наш файл.



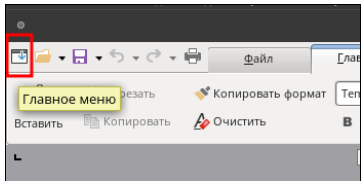
Подпись документов в LibreOffice

Для активации подписания документов потребуется установить плагин:

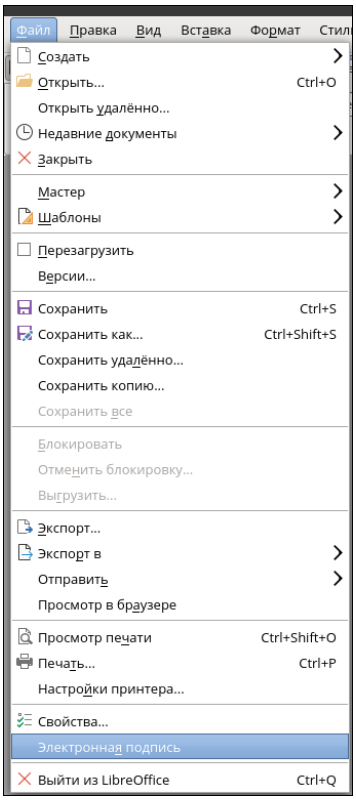
```
dnf install LibreOffice-plugin-altcsp
```

Для активации подписи требуется нажать кнопку «**Файл**». Если меню «**Файл**» недоступно, нажмите предварительно кнопку,

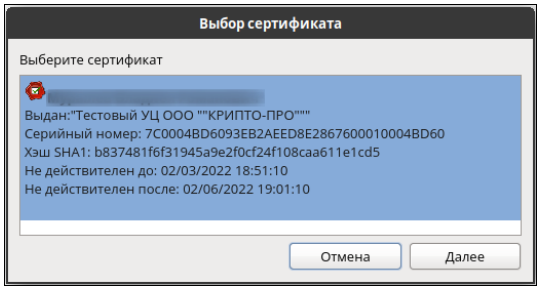
выделенную на скриншоте:



Нажмите кнопку «**Электронная подпись**»:



Для подписи вам будет предложен выбор сертификата:

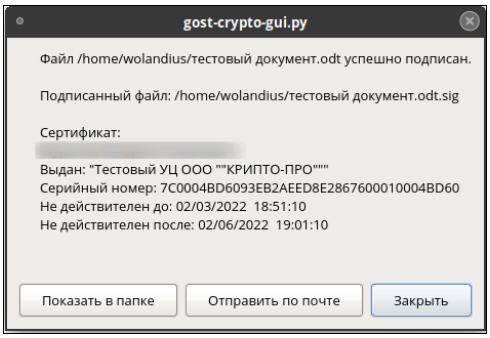


Также не забудьте проверить, что для выбранного сертификата у вас установлены все необходимые корневые и отозванные сертификаты. Пример необходимых сертификатов можно проверить командой:

```
certmgr -list -store uMy

***
CA cert URL : http://testgost2012.cryptopro.ru/CertEnroll/root2018.crt
CDP : http://testgost2012.cryptopro.ru/CertEnroll/!0422!0435!0441!0442!043e!0432!044b!0439%20!0423!0426%20...
CDP : http://testgost2012.cryptopro.ru/CertEnroll/testgost2012(1).crl
***
```

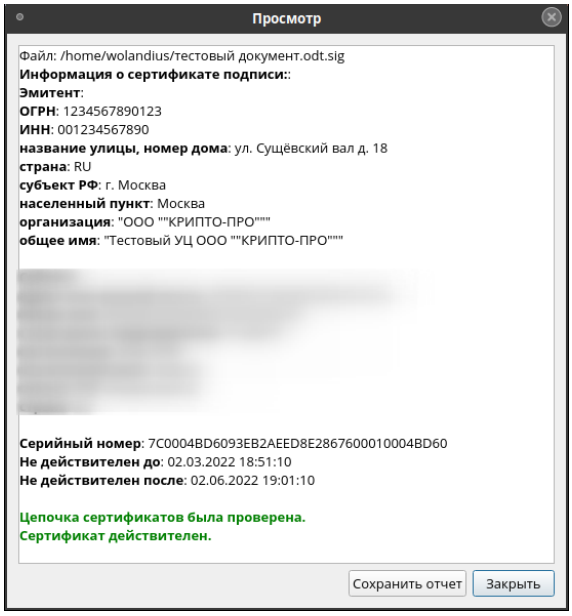
Как показано в примере, необходимо доставить **3 сертификата.** Выполнить это можно через **token-manager** и установку сертификатов из утилиты.

В случае успешной подписи вы увидите следующее уведомление:



Проверить подпись можно из «**gostcryptogui**» - «**Проверить подпись**».

После выбора документа вы увидите следующую информацию:



Работа с сертификатами КриптоПро

Работа с криптоконтейнерами
Решение проблемы отсутствия контейнеров в КриптоПро в домене
Установка личных сертификатов
Установка корневых сертификатов
Установка сертификатов pfx
Просмотр сертификатов
Удаление сертификатов
Перенос контейнера с flash-носителя в локальное хранилище ПК
Просмотр цепочки сертификата

Для удобства использования утилит КриптоПро создадим на них символьные ссылки, для этого выполните:

```
ln -s /opt/cprocsp/bin/amd64/certmgr /usr/bin/certmgr
ln -s /opt/cprocsp/bin/amd64/csptest /usr/bin/csptest
ln -s /opt/cprocsp/sbin/amd64/cpconfig /usr/bin/cpconfig
```

Просмотр версии КриптоПро:

```
csptest -enum -info
```

или

```
cat /etc/opt/cprocsp/release
```

Проверка лицензии:

```
cpconfig -license -view
```

Для установки лицензии выполните (с правами **root**):

```
# cpconfig -license -set <серийный_номер>
```

При использовании токенов сервис **pcscd** должен быть запущен. Проверка статуса **pcscd**:

```
systemctl status pcscd
```

если он выключен, то включите его:

```
systemctl start pcscd
systemctl enable pcscd
```

Вывод сообщений журнала службы **pcscd**:

```
pcscd -dffff
```

Узнать модель подключенного токена:

```
csptest -card -enum -v -v
pcsc_scan
```

Работа с криптоконтейнерами

1. Проверить наличие доступных контейнеров:

```
csptest -keyset -enum_cont -fqcn -verifyc | iconv -f cp1251

CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 16778675
\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4
\\.\FLASH\bob
```

```
\\.\HDIMAGE\bob
OK.
Total: SYS: 0,010 sec USR: 0,110 sec UTC: 6,240 sec
[ErrorCode: 0x00000000]
```

Имена контейнеров используются для установки личных сертификатов.

- Считыватель **HDIMAGE** размещается в **/var/opt/cprocsp/keys/<имя пользователя>/** т.е в данном случае используется жесткий диск для хранения ключей.
- Считыватель **FLASH** означает, что используется флешка для хранения приватных ключей.
- Также считывателем может выступать токен.

2. Имена контейнеров могут содержать символы на кириллице, поэтому чтобы корректно отобразить контейнеры используйте следующую команду:

```
csptest -keyset -enum_cont -fqcn -verifyc | iconv -f cp1251
```

Для дальнейшего использования имен контейнеров содержащих кодировку **cp1251**, выведем список контейнеров с уникальными именами:

```
csptest -keyset -enum_cont -fqcn -verifyc -uniq

CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 23397811
\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4 | \\.\Aladdin R.D. JaCarta 00
00\SCARD\JACARTA_6082028344937676\CC00\E412
OK.
Total: SYS: 0,000 sec USR: 0,110 sec UTC: 6,230 sec
[ErrorCode: 0x00000000]
```

3. Просмотр подробной информации о контейнере:

```
csptest -keyset -container '\\.\HDIMAGE\bob' -info
```

4. Перечисление контейнеров пользователя:

```
csptest -keyset -enum_cont -verifycontext -fqcn
```

5. Перечисление контейнеров компьютера:

```
csptest -keyset -enum_cont -verifycontext -fqcn -machinekeys
```

6. Открыть(проверить) контейнер пользователя:

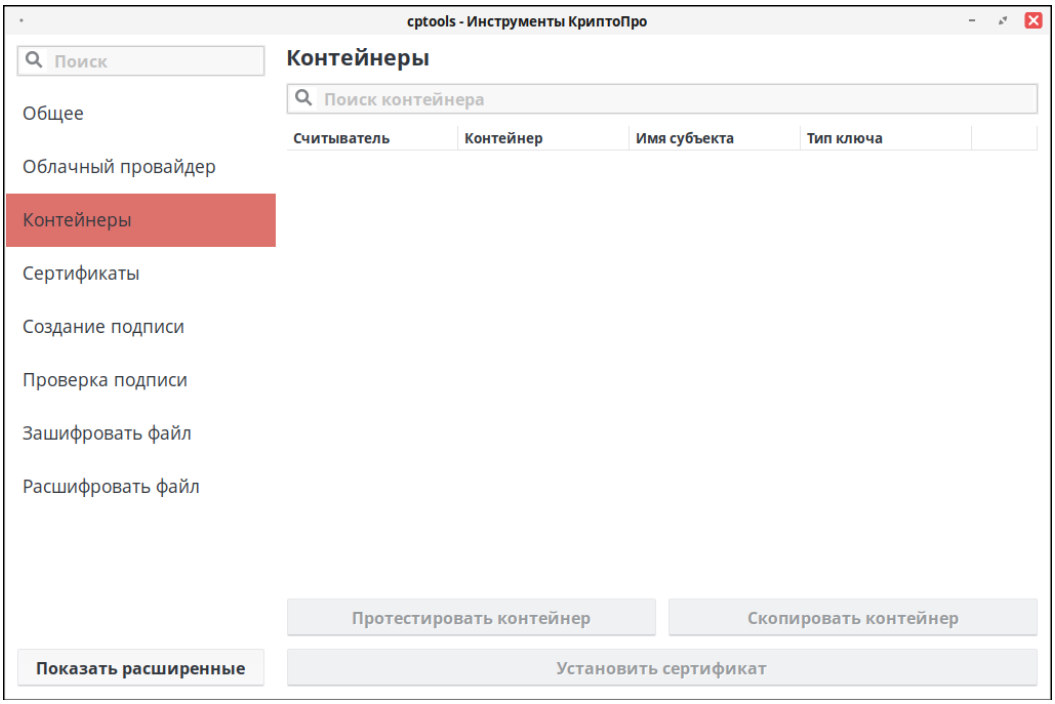
```
csptest -keyset -check -cont '\\.\имя считывателя\имя контейнера'
```

7. Открыть(проверить) контейнер компьютера:

```
csptest -keyset -check -cont '\\.\имя считывателя\имя контейнера' -machinekeyset
```

Решение проблемы отсутствия контейнеров в КриптоПро в домене

В некоторых случаях, если компьютер введен в домен, может возникнуть проблема отсутствия контейнеров под доменным пользователем.



Для решения данной проблемы необходимо выполнить ряд действий:

1. Создать **udev**-правило командой:

```
nano /etc/udev/rules.d/87-domain_usb.rules
```

Добавить в него следующее содержимое:

```
ENV{ID_FS_USAGE}=="filesystem|other|crypto", ENV{UDISKS_FILESYSTEM_SHARED}="1"
```

2. Выполнить перезапуск **udev**-правил:

```
udevadm control --reload
```

3. Проверить наличие файла **/var/lib/AccountsService/users/<имя_пользователя>**, где **<имя_пользователя>** – имя вашего доменного пользователя.

Если файла нет, его необходимо создать по примеру существующего.

Пример содержимого файла можно просмотреть в том же каталоге в файле локального пользователя:

```
cat /var/lib/AccountsService/users/user

[User]
Language=
XSession=
Icon=/home/user/.face
SystemAccount=false
```

Перезагрузите систему для применения внесенных изменений.

Если вышеприведенное решение не помогло, следует переустановить КриптоПро, запустив скрипт **uninstall.sh** (скрипт находится в архиве с установщиком КриптоПро):

```
./uninstall.sh
```

Затем удалить оставшиеся каталоги:

```
rm -rf /opt/cprocsp /etc/opt/cprocsp /var/opt/cprocsp
```

После полного удаления потребуется произвести установку КриптоПро с **udev**-правилом, приведенным в п. 1.

Установка личных сертификатов

1. Установка сертификата без привязки к ключам:

```
certmgr -inst -file cert_bob.cer
```

2. Установка личного сертификата cert_bob.cer, сертификат при этом попадает в пользовательское хранилище **uMy**. Приватный ключ находится на флешке.

```
certmgr -inst -file cert_bob.cer -store uMy -cont '\\.\FLASH\bob'
```

в команде указывается сертификат cert_bob.cer, который ассоциируется с приватным контейнером **\\.\FLASH\bob'**

3. Установка сертификата с токена (в конце команды указывается контейнер)

```
/opt/cprocsp/bin/amd64/certmgr -inst -store uMy -cont '\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4'
```

Установка корневых сертификатов

При установке корневых сертификатов достаточно указать хранилище **uRoot**. При указании **mRo o t** (при наличии прав администратора) корневой сертификат будет доступен всем пользователям системы.

1. Установка в хранилище КриптоПро**:**

```
certmgr -inst -store uRoot -file <название-файла>.cer
```

2. Установка в хранилище ПК:

```
certmgr -inst -store mRoot -file <название-файла>cer
```

3. Установка списка отозванных сертификатов **crl**:

```
certmgr -inst -crl -file <название-файла>.crl
```

Установка сертификатов pfx

1. Необходимо установить пакет **cprocsp-rsa**, который находится в составе дистрибутива КриптоПро (**linux-amd64**).

2. Выполним команду от **локального** (доменного) пользователя:

```
/opt/cprocsp/bin/amd64/certmgr -inst -store uMy -pfx -pin <пинкод> -file 'путь до pfx'
```

Цепочка сертификатов будет отображаться в утилите «**Ключевые носители и сертификаты**» в «**Личное хранилище сертификатов**».

Просмотр сертификатов

1. Просмотр установленных сертификатов:

```
certmgr -list
```

2. Просмотр установленных сертификатов в локальном хранилище **uMy**:

```
certmgr -list -store uMy
```

3. Просмотр сертификатов в хранилище ПК (обычно сюда устанавливаются корневых сертификаты):

```
$ certmgr -list -store uRoot
```

4. Просмотр сертификатов в контейнере:

```
certmgr -list -container '\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4'
```

5. Просмотр промежуточных сертификатов:

```
certmgr -list -store uca
```

Удаление сертификатов

1. Удалить сертификат из личного хранилища сертификатов

Просмотрите установленные сертификаты:

```
certmgr -list
```

Изучите список всех установленных сертификатов (в общем списке отображаются абсолютно все сертификаты).

Для удаления следует выполнить команду в Терминале:

```
certmgr -delete -store uMy
```

Если установлено более одного сертификата, то будет предложено указать номер удаляемого сертификата.

2. Удалить сертификаты, установленные в хранилище КриптоПро:

```
certmgr -delete -store uRoot
```

Если установлено более одного сертификата, то будет предложено указать номер удаляемого сертификата.

3. Удалить все сертификаты, установленные в хранилище КриптоПро:

```
certmgr -delete -all -store uRoot
```

4. Удалить все сертификаты, установленные в хранилище ПК:

```
certmgr -delete -store mRoot
```

Перенос контейнера с flash-носителя в локальное хранилище ПК

1. Активируем хранилище **HDIMAGE**:

```
cpconfig -hardware reader -add HDIMAGE store

Adding new reader:
Nick name: HDIMAGE
Succeeded, code:0x0
```

2. Посмотрим, какие контейнеры доступны на флешке:

```
csptest -keyset -enum_cont -fqcn -verifyc

CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 32114099
\\.\FLASH\bob
OK.
Total: SYS: 0,020 sec USR: 0,080 sec UTC: 0,190 sec
[ErrorCode: 0x00000000]
```

3. Перейдите на Flash-носитель и скопируйте этот контейнер — каталог **bob.000** с приватными (закрытыми) ключами в **/var/opt/cprocsp/keys/user** - в этом каталоге находится локальное хранилище **HDIMAGE**

4. Посмотрим доступные контейнеры:

```
csptest -keyset -enum_cont -fqcn -verifyc
```

```
CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 36951475
\\.\FLASH\bob
\\.\HDIMAGE\bob
OK.
Total: SYS: 0,000 sec USR: 0,070 sec UTC: 0,160 sec
[ErrorCode: 0x00000000]
```

Как видим, появился новый контейнер `\\.\HDIMAGE\bob`
Теперь flash-носитель можно отключить, он нам больше не понадобится.

5. Установим пользовательский сертификат с привязкой к закрытому контейнеру `\\.\HDIMAGE\bob`

```
certmgr -inst -file cert-bob.cer -cont '\\.\HDIMAGE\bob'
```

Просмотр цепочки сертификата

Просмотр необходимых корневых сертификатов и сертификатов отзыва вы можете посмотреть следующей командой:

1) Для сертификатов, хранящихся в личном хранилище:

```
certmgr -list -store uMy
```

Интересующие строки, информирующие о необходимом сертификате начинаются со слов

```
URL сертификата УЦ
URL списка отзыва
```

Или в английском варианте:

```
CA cert URL
CDP
```

2) Для просмотра цепочки на токене выполните следующую команду:

```
certmgr -list -cont '<CONTAINER>'
```

Где вместо '<CONTAINER>' укажите ваш контейнер, к примеру '\\.\Aladdin R.D. JaCarta 00 00\8df47e71-18ae-49c1-8738-9b4b0944dcd4'

3. Просмотр цепочки из файла сертификата:

```
certmgr -list -file 'путь_к_файлу'
```

Установка плагинов Госуслуг и КриптоПро в браузерах Chromium, Яндекс.Браузер, Firefox

Установка КриптоПро для работы с корневыми и личными сертификатами
Настройка браузера Chromium
Настройка Яндекс.Браузера
Настройка браузера Firefox
Установка КриптоПро «CryptoPro Extension for CAdES Browser Plug-in»
Добавление сайта в список доверенных сайтов плагина
Вход на сайт Госуслуги через Chromium

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: cryptopro-4.0, cryptopro-5.0

Установка КриптоПро для работы с корневыми и личными сертификатами

Для установки **КриптоПро 4.0** перейдите по ссылке.

Для установки **КриптоПро 5.0** перейдите по ссылке.

Настройка браузера Chromium

Установка браузера Chromium

В РЕД ОС браузер **Chromium** установлен по-умолчанию и доступен из «**Главного меню**» - «**Интернет**» - «**Веб-браузер Chromium**».

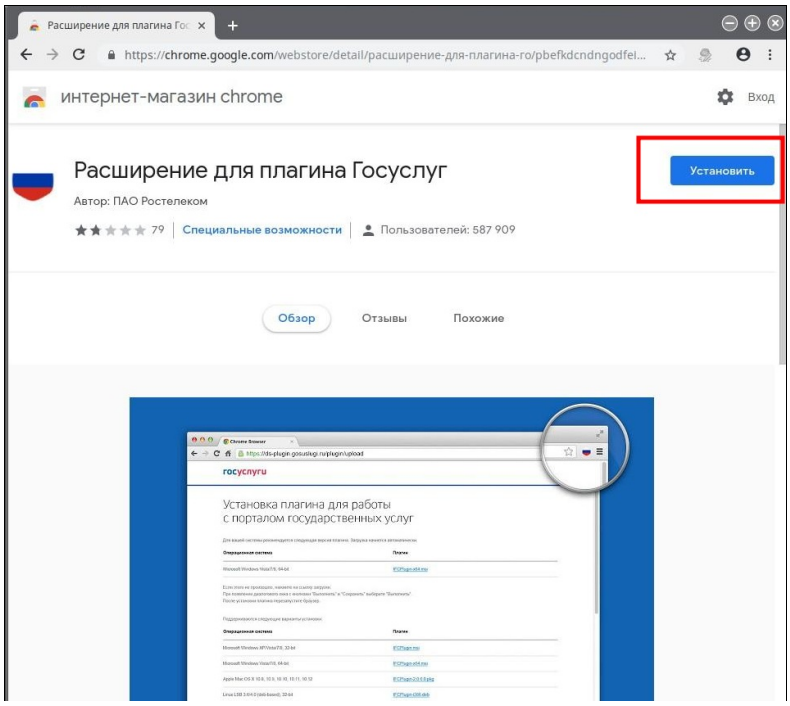
Установка расширения для плагина Госуслуг (ЕПГУ)

Выполните команду для установки расширений для браузера **Chromium** с правами администратора:

```
sudo dnf install ifcplugin-chromium
```

2. Установите расширение для плагина Госуслуг (ЕПГУ).

Перейдите по ссылке и нажмите кнопку «**Установить**».



Добавьте сайт https://esia.gosuslugi.ru в **Доверенные сайты** согласно Добавление сайта в список доверенных сайтов плагина.

Настройка Яндекс.Браузера

Установка Яндекс.Браузера

Для установки Яндекс.Браузера перейдите по ссылке.

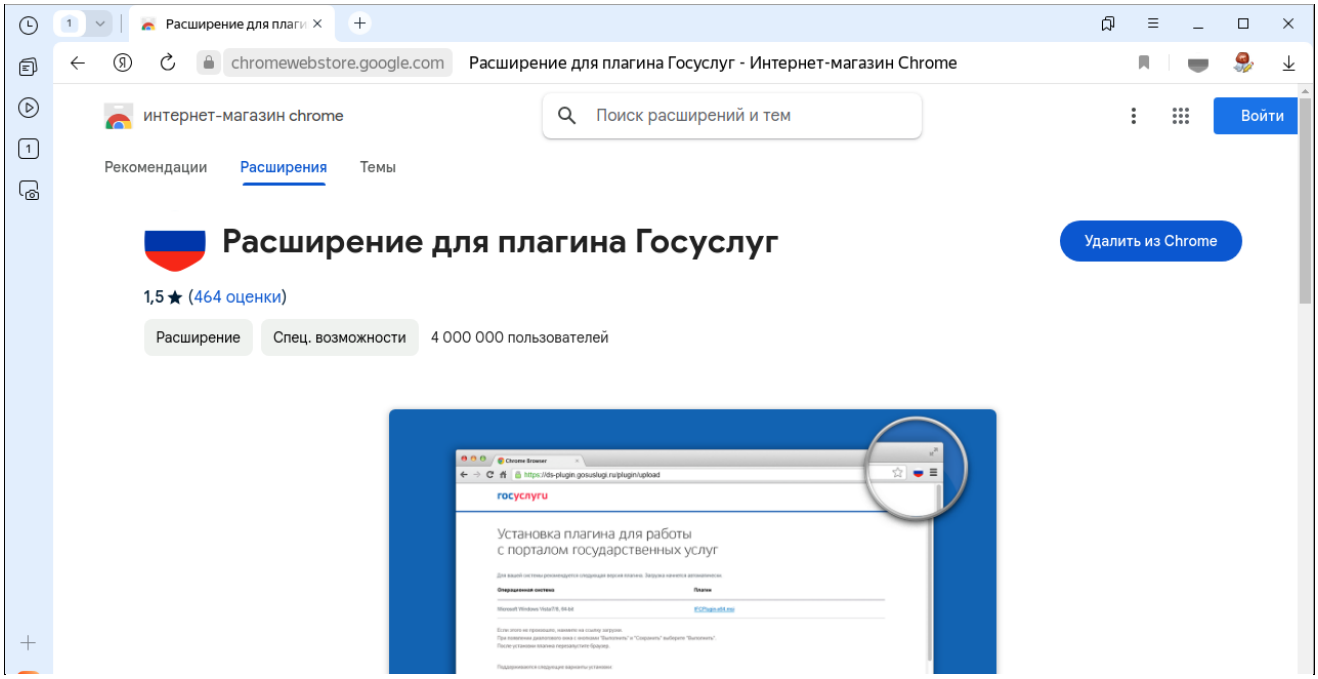
Установка расширения для плагина Госуслуг (ЕПГУ)

Выполните команду для установки расширений для браузеров **Chromium** и **Яндекс.Браузер** с правами администратора:

```
sudo dnf install ifcplugin-chromium
```

Установите расширение для плагина Госуслуг (ЕПГУ).

Перейдите по ссылке и нажмите кнопку «**Установить**».



Добавьте сайт https://esia.gosuslugi.ru в **Доверенные сайты** согласно Добавление сайта в список доверенных сайтов плагина.

Настройка браузера Firefox

Установка браузера Firefox

Для установки браузера Firefox перейдите по ссылке.

Установка расширения для плагина Госуслуг (ЕПГУ)

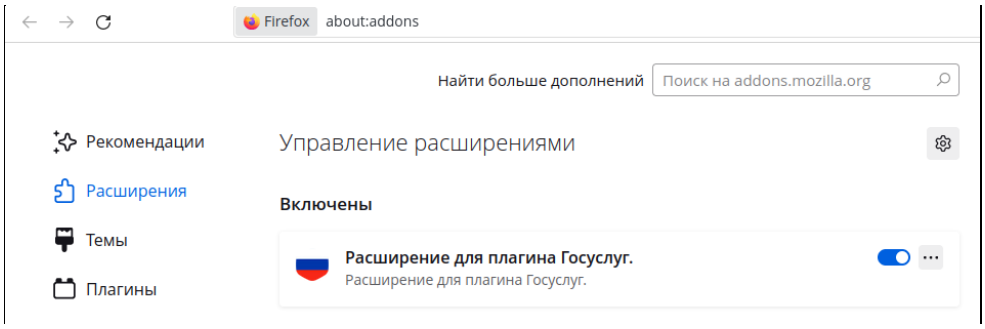
Выполните команду для установки расширений для браузера Firefox с правами администратора:

```
sudo dnf install ifcplugin-firefox
```

Установите расширение для плагина Госуслуг (ЕПГУ).

Для браузера **Firefox** необходимо вручную установить расширение для работы с Плагином Госуслуг. Для этого перейдите по ссылке и выберите удобный формат установки – через RPM-пакет или автоматически.

После установки расширение будет доступно в списке расширений браузера.



Добавьте сайт https://esia.gosuslugi.ru в **Доверенные сайты** согласно Добавление сайта в список доверенных сайтов плагина.

Установка КриптоПро «CryptoPro Extension for CAdES Browser Plug-in»

Пункты 1-3 данного раздела следует выполнять, только если у вас установлен КриптоПро CSP ниже версии 5.0.12500.

1. Скачайте плагин, перейдя по ссылке.

2. Распакуйте скачанный архив:

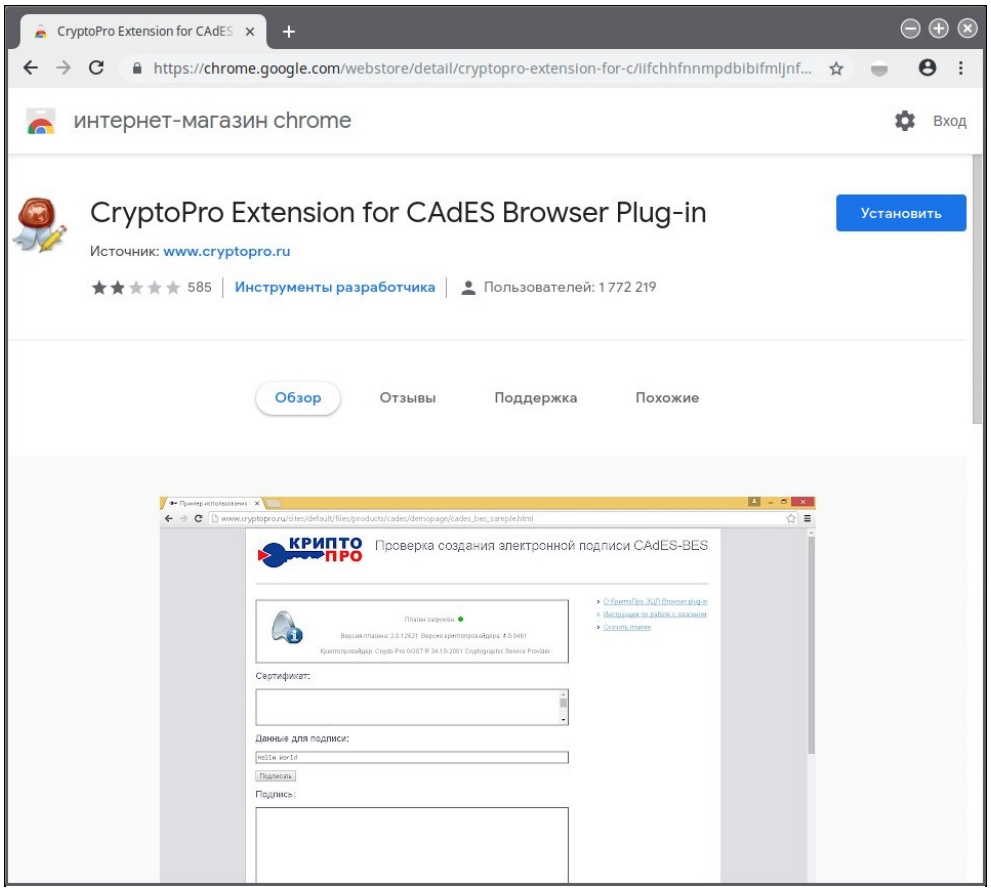
```
$ tar -xvf cades-linux-amd64.tar.gz
```

3. Перейдите в папку с распакованным архивом и установите следующие пакеты:

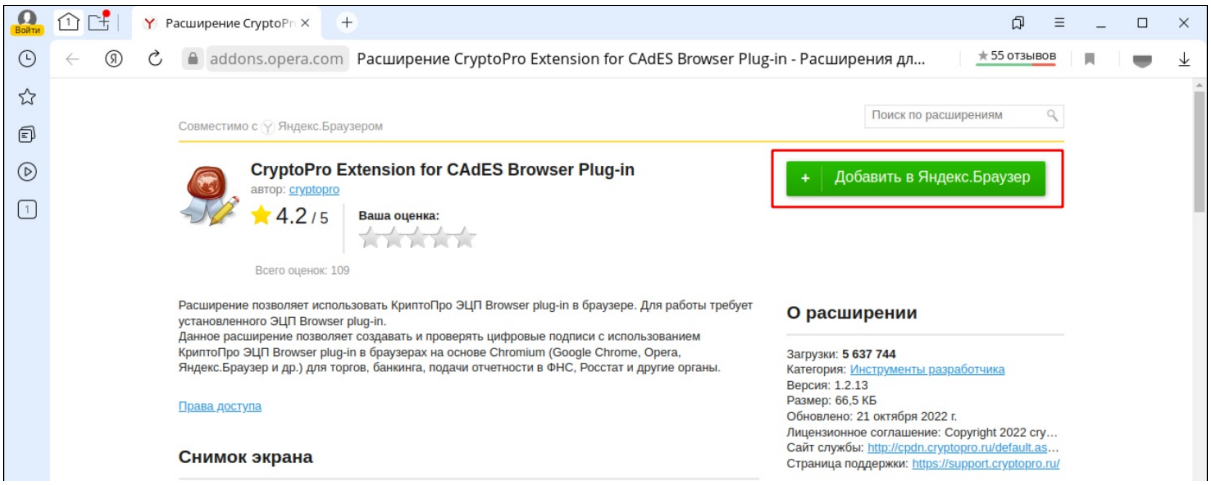
```
dnf install ./cprocsp-pki*rpm
```

4. Установите плагин **CryptoPro Extension for CAdES Browser Plug-in**:

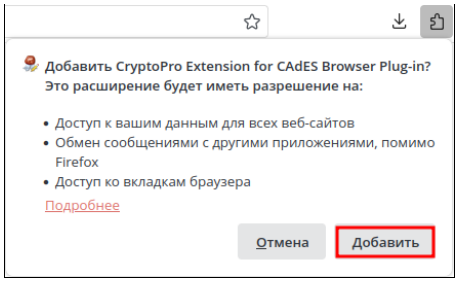
- для **Chromium** - перейдите по ссылке и нажмите кнопку «**Установить**»:



- для **Яндекс.Браузера** - перейдите по ссылке и нажмите кнопку «**Добавить в Яндекс.Браузер**»:



- для **Firefox**– скачайте расширение по ссылке и установите в браузер самостоятельно.



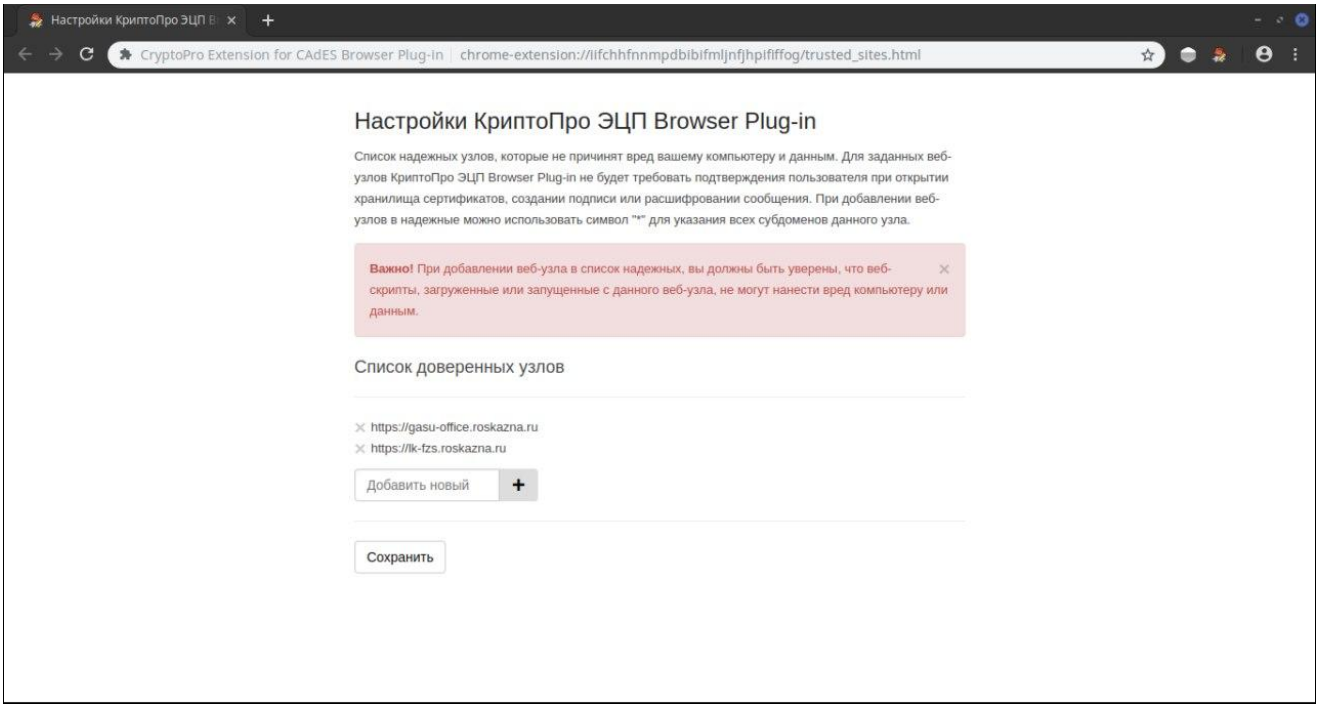
Проверить работу плагина можно по ссылке.

Добавление сайта в список доверенных сайтов плагина

Для добавления сайта откройте меню плагина и выберите пункт «**Настройка доверенных сайтов**».

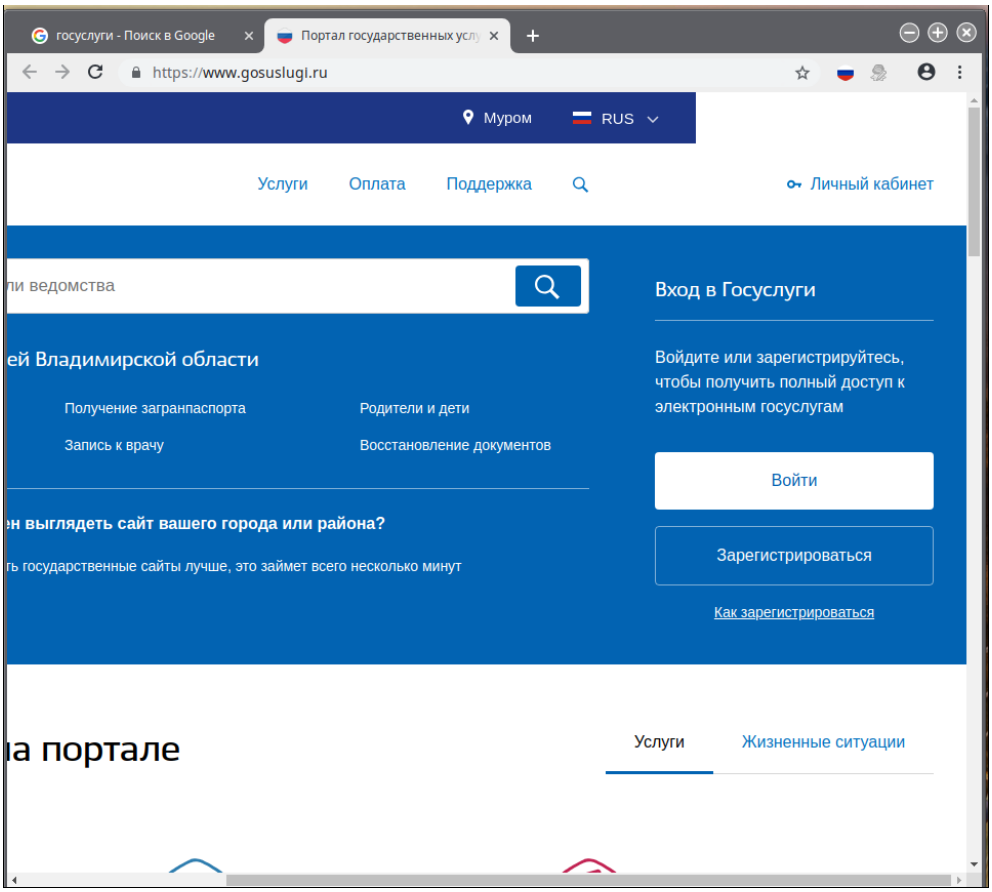


Далее откроется страница, на которой можно произвести добавление сайтов:

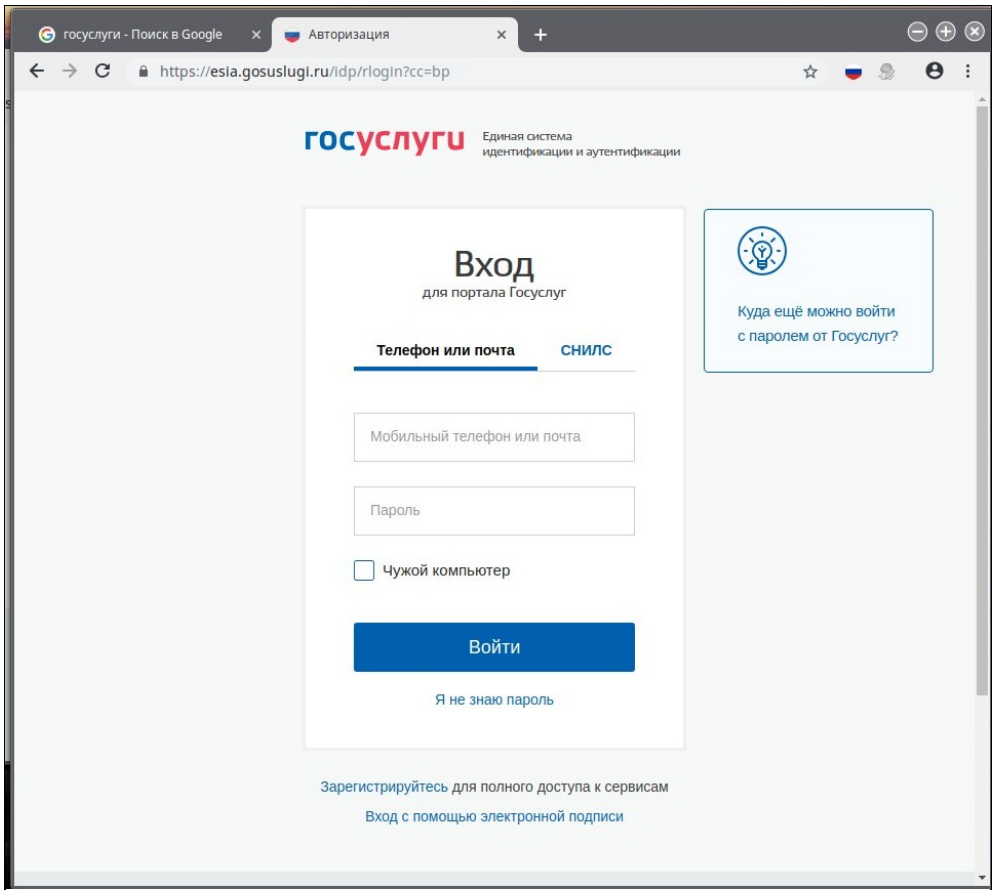


Вход на сайт Госуслуги

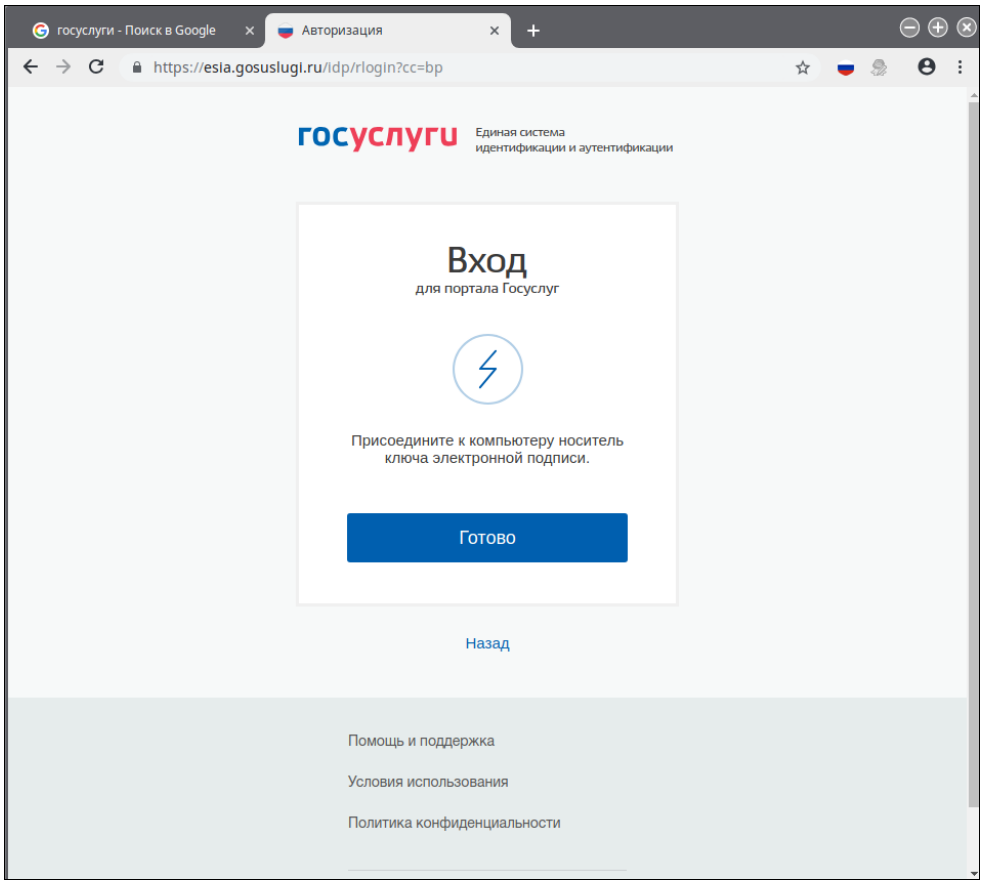
1. В браузере перейдите по ссылке и нажмите кнопку «**Вход**».



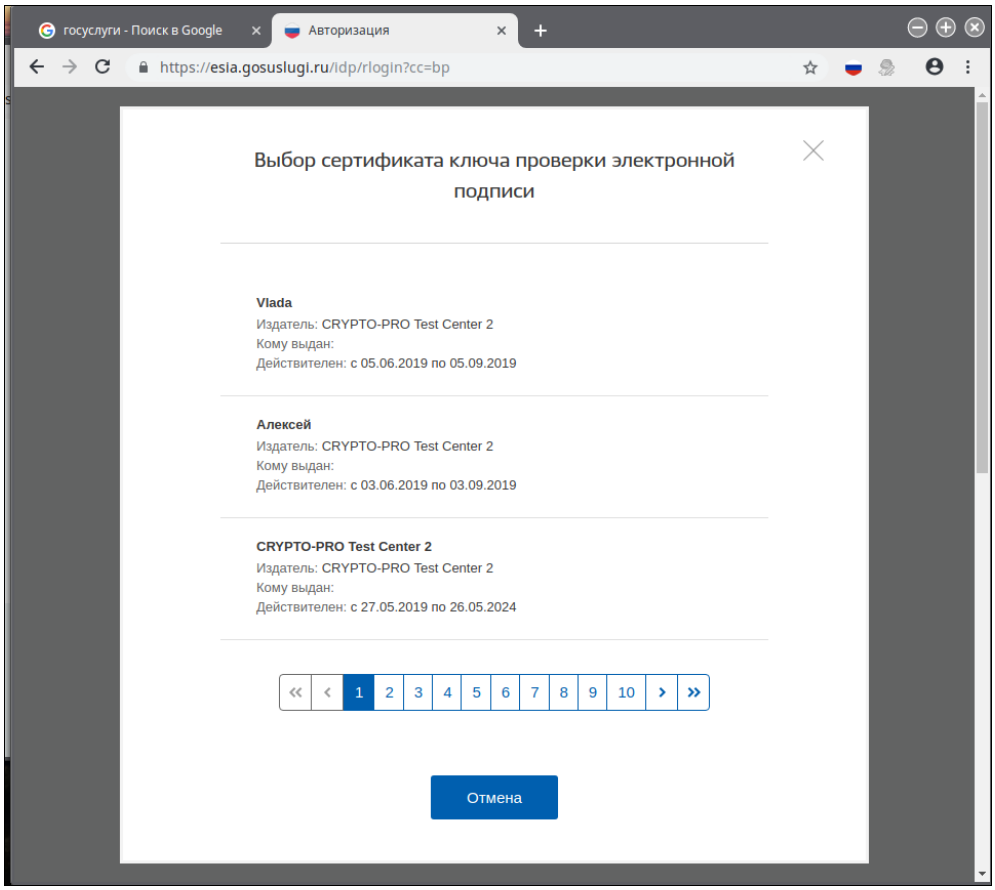
2. На открывшейся странице нажмите на «**Вход**» с помощью электронной подписи.



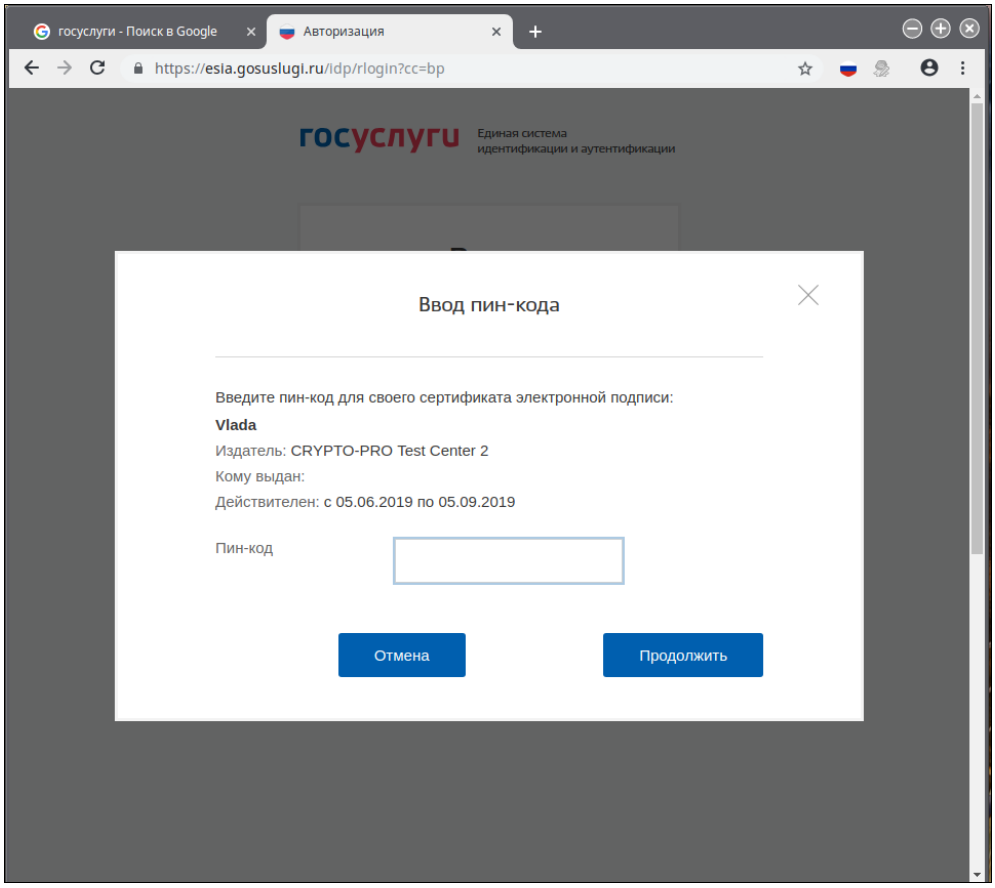
3. Подключите токен с ключом к компьютеру и нажмите кнопку «**Готово**».



4. Выберите сертификат ключа проверки электронной подписи, щёлкнув левой кнопкой мыши по строке с сертификатом.



5. Введите ПИН-код пользователя и нажмите кнопку «**Продолжить**».



ViPNet IDS HS Agent - система обнаружения вторжений

ViPNet IDS HS — программный комплекс, осуществляющий обнаружение сетевых атак и вторжений внутри хоста, изменения в реестре или в ключевых логах. В этой статье будет рассмотрена установка **linux-агента** и проверка его работоспособности.

Установка

1. Скачайте **rpm-пакет** и запустите установку:

   ```
   sudo dnf install vipnet-ids-hs-agent-1.4.1-2.rpm
   ```

2. Добавьте IP-адрес машины, на которой запущена серверная часть комплекса, в файл **/var/idshs/idshs_agent.conf**:

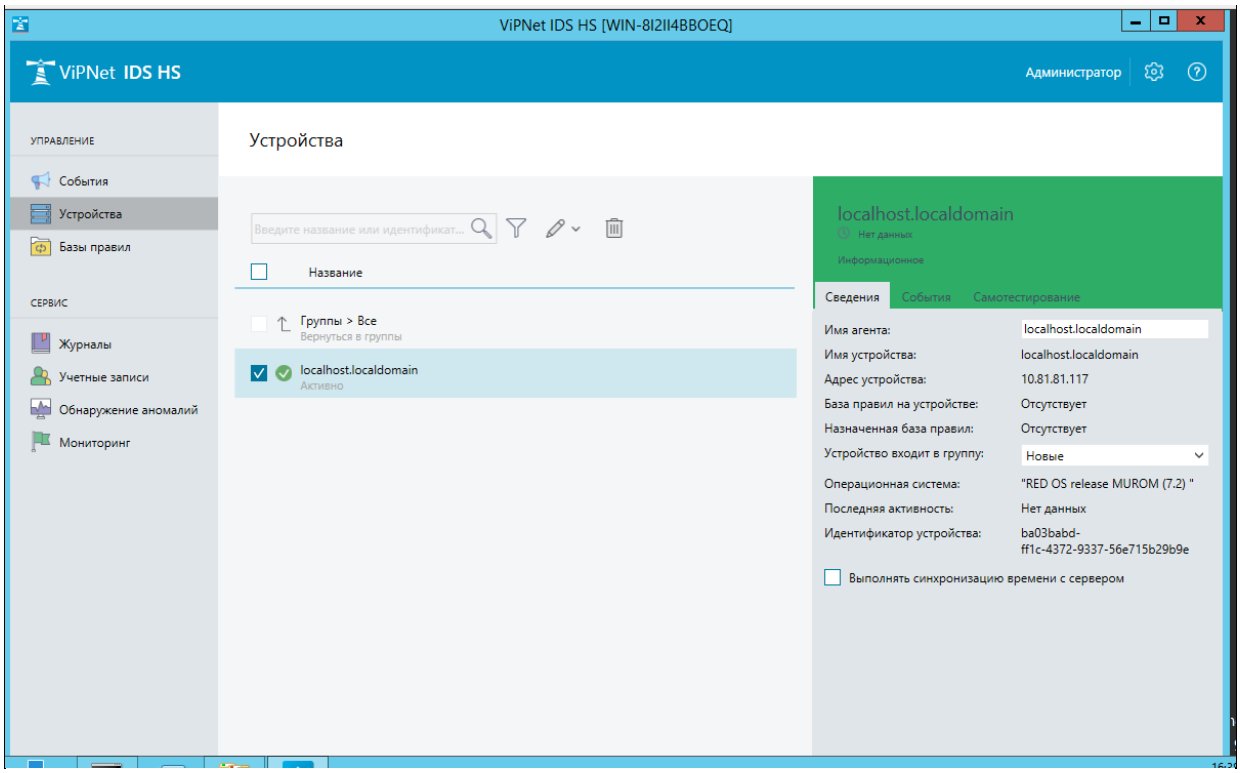
   ```
   sudo sh -c "echo 'server_address : <ip_адрес_сервера>' >> /var/idshs/idshs_agent.conf"
   ```

3. Перезагрузите компьютер.
4. Отправьте запрос на подключение серверу:

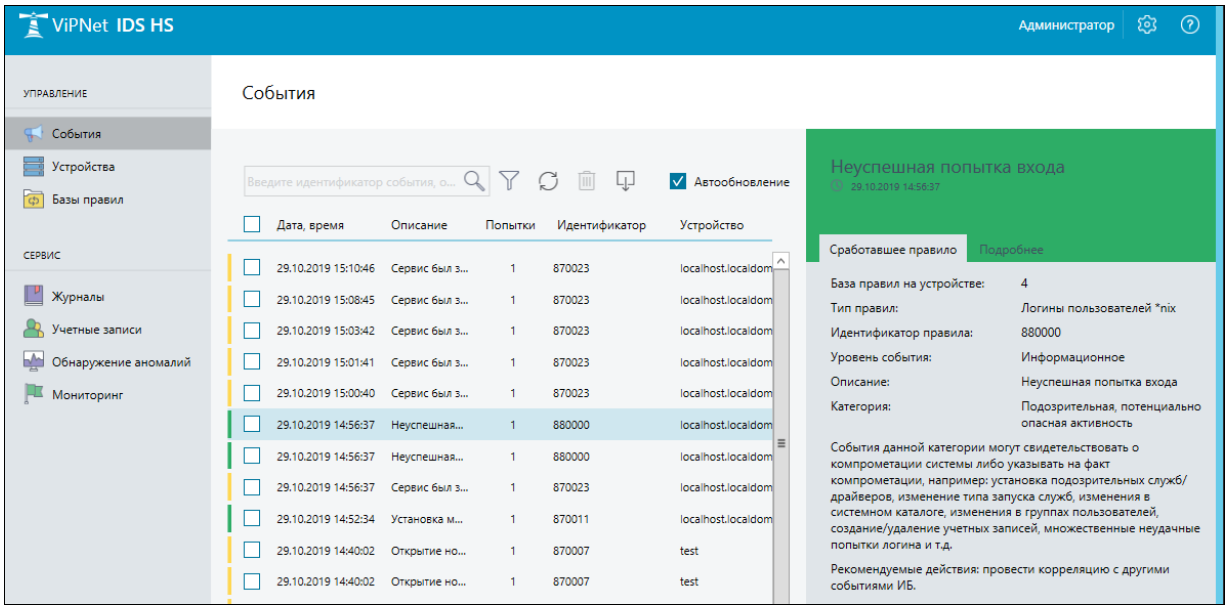
   ```
   idshs-agent <ip-адрес сервера>
   ```

Проверка работоспособности

Запустите приложение **ViPNet IDS HS** на сервере. Перейдите на вкладку **«Устройства»** и проверьте что машина, на которой был установлен агент, появилась в списке:



На вкладке **«События»** показаны отслеживаемые в реальном времени события информационной безопасности, которые были зафиксированы агентом:


ViPNet IDS HS
Администратор
УПРАВЛЕНИЕ
События
Устройства
Базы правил
СЕРВИС
Журналы
Учетные записи
Обнаружение аномалий
Мониторинг
События
Введите идентификатор события, о...
Автообновление
Дата, время
Описание
Попытки
Идентификатор
Устройство
29.10.2019 15:10:46 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:08:45 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:03:42 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:01:41 Сервис был з... 1 870023 localhost.localdom
29.10.2019 15:00:40 Сервис был з... 1 870023 localhost.localdom
29.10.2019 14:56:37 Неуспешная... 1 880000 localhost.localdom
29.10.2019 14:56:37 Неуспешная... 1 880000 localhost.localdom
29.10.2019 14:56:37 Сервис был з... 1 870023 localhost.localdom
29.10.2019 14:52:34 Установка м... 1 870011 localhost.localdom
29.10.2019 14:40:02 Открытие но... 1 870007 test
29.10.2019 14:40:02 Открытие но... 1 870007 test
Неуспешная попытка входа
29.10.2019 14:56:37
Сработавшее правило
Подробнее
База правил на устройстве: 4
Тип правил: Логины пользователей *nix
Идентификатор правила: 880000
Уровень события: Информационное
Описание: Неуспешная попытка входа
Категория: Подозрительная, потенциально опасная активность
События данной категории могут свидетельствовать о компрометации системы либо указывать на факт компрометации, например: установка подозрительных служб/драйверов, изменение типа запуска служб, изменения в системном каталоге, изменения в группах пользователей, создание/удаление учетных записей, множественные неудачные попытки логина и т.д.
Рекомендуемые действия: провести корреляцию с другими событиями ИБ.

ViPNet PKI Client - ПО для работы с электронной подписью

Установка программы
Работа с сертификатами
Генерация запроса на сертификат
Установка сертификата
Экспорт сертификатов

Окружение:

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** VipNet PKI Client - 1.6.0.1688, VipNet CSP - 4.4.0.11431

ViPNet PKI Client — проприетарное программное обеспечение разработанное компанией ИнфоТеКС для работы с электронной подписью и построении защищенных TLS-соединений.

Установка программы

Скачайте и распакуйте архив с пакетами для установки в домашний каталог от **локального пользователя** (в примере /home/user):

```
cd /home/user/
```

```
tar xvf pki_client_linux-x86_64-dist.tar.bz2
```

Поместите файл лицензии в распакованный каталог. Затем перейдите в каталог и запустите скрипт установки:

```
cd pki_client_linux/rpm
```

```
sudo ./install.sh
```

Дождитесь завершения процедуры установки.

Запустите VipNet PKI Client в **"Главное меню"** - **"Стандартные"** - **"Vipnet PKI Client".**

Работа с сертификатами

Генерация запроса на сертификат

Для генерации запроса на сертификат необходимо перейти в раздел **«Сертификаты»**, заполнить поля необходимой информацией и нажать кнопку **«Создать запрос»**. После этого, запрос будет передан в удостоверяющий центр.

Установка сертификата

Для добавления сертификата в локальное хранилище перейдите в раздел **«Сертификаты»**, выберите **«Добавить сертификат или CRL»** и укажите путь к файлу сертификата.

Экспорт сертификатов

Для экспорта сертификатов пользователей в файлы формата **X.509** сделайте следующее:

1. Выберите раздел **«Сертификаты»**;
2. Нажмите на кнопку напротив необходимого сертификата и выберите необходимый пункт;
3. В открывшемся окне выберите папку для сохранения файла.

Криптопровайдер VipNet CSP

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VipNet CSP - 4.4

ВАЖНО!

Для работы графических утилит на РЕД ОС предварительно установите зависимости командой с правами **пользователя root:**

```
dnf install qt qt-common qt-settings qt-x11
```

Вы можете подробнее ознакомиться с примером установки и настройки криптопровайдера VipNet, просмотрев наши обучающие видео:

- на **RuTube** — Установка ViPNet CSP в РЕД ОС;
- в **Яндекс.Дзен** — Установка ViPNet CSP в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка VipNetCSP 4.4

Токены типа **Рутокен S** и **Рутокен Lite** исключены из поддержки с версии **ViPNet CSP 4.2.11**.

Скачайте архив и распакуйте его содержимое в корне домашней папки пользователя (с правами **локального** пользователя):

```
cd /home/<имя_пользователя>
```

```
unzip CSP_44_RedOS.zip
```

Перейдите в папку с установочным скриптом командой (с правами **локального** пользователя):

```
cd /home/<имя_пользователя>/CSP_44_RedOS/SOFT/scripts/
```

Предоставьте права на запуск файла в папке **scripts** командой (с правами **локального** пользователя):

```
chmod 777 vipnetcsp_pkg_manager.sh
```

Запустите скрипт установки командой:

```
./vipnetcsp_pkg_manager.sh install --package rpm --platform <архитектура_процессора> --profile <конфигурация_приложения> --dist /home/<имя_пользователя>/rpm/
```

Архитектура процессора:

- **x86_64** — для 64 или 32 битной версии РЕД ОС.
- **i686** — для версии РЕД ОС на архитектуре i686.

Чтобы посмотреть информацию об архитектуре процессора, введите команду:

```
uname -m
```

Конфигурация приложения:

- **vipnet_csp** - для установки приложения без графического интерфейса.
- **vipnet_csp_gui** - для установки приложения с графическим интерфейсом.
- **all** - то же, что и предыдущий параметр.

Пример команды:

```
./vipnetcsp_pkg_manager.sh install --package rpm --platform x86_64 --profile vipnet_csp_gui --dist
/home/user/CSP_44_RedOS/SOFT/LSB_x86/rpm
```

Или просто запустите скрипт установки с указанным путем до каталога с устанавливаемыми пакетами. Все остальные параметры определятся автоматически:

```
./vipnetcsp_pkg_manager.sh install --dist /home/<имя_пользователя>/CSP_44_RedOS/SOFT/LSB_x86/rpm/
```

После установки все исполняемые файлы приложения будут находится по пути **/opt/itcs/bin/**.

Для установки примеров использования функций в *Vipnet CSP* и заголовочных файлов, перейдите в папку **rpm**:

```
cd /home/user/CSP_44_RedOS/SOFT/LSB_x86/rpm
```

и установите пакет **itcs-csp-dev-4.4.0.732-1.noarch.rpm**.

```
dnf localinstall itcs-csp-dev-4.4.0.732-1.noarch.rpm
```

Примеры использования будут хранится по пути **/opt/itcs/share/samples**, а заголовочные файлы **/opt/itcs/include/**.

Для удаления приложения замените параметр **install** в установочном скрипте на **uninstall**.

```
./vipnetcsp_pkg_manager.sh uninstall
```

Для подробного разбора функций и примеров использования приложения, просмотрите официальную документацию по продукту на сайте infotecs.

СКЗИ Континент АП

Установка программного обеспечения
Работа с сертификатами
Создание запроса на сертификат
Регистрация сертификатов
Список доверенных серверов доступа
Настройка подключений
Создание нового профиля подключения
Подключение к серверу доступа
Автоматическое подключение к серверу доступа
Разрыв соединения с сервером доступа

СКЗИ Континет АП - специализированное программное обеспечения, предназначенное для установки на местах удаленных пользователей. **Абонентский пункт** (ап) отвечает за подключение к корпоративным ресурсам и обмен информацией в зашифрованном виде.

Установочный комплекс содержит 4 каталога:

1. **TS** — установочные пакеты ПО абонентского пункта;
2. **Sable** — ПО для поддержки совместной работы с ПАК «Соболь»;
3. **third_party** — стороннее ПО, необходимое для работы абонентского пункта;
4. **token_libs** — стороннее ПО, необходимое для работы с ключевыми носителями.

Установка программного обеспечения

1. Для установки стороннего ПО, необходимого для работы абонентского пункта, нужно установить пакеты, находящиеся в каталоге **third_party**. Для этого перейдите в каталог **third_party**, далее перейдите в подкаталог с номером версии используемой ОС и выполните команду:

```
sudo dnf localinstall *.rpm --disablerepo=*
```

2. Для установки стороннего ПО, необходимого для работы с ключевыми носителями, нужно установить пакеты, находящиеся в каталоге **token_libs**. Для этого перейдите в каталог **token_libs**, далее перейдите в подкаталог с номером версии используемой ОС и установите пакеты, содержащиеся в подкаталоге.

3. Если программное обеспечение абонентского пункта должно соответствовать среднему уровню безопасности, необходимо перейти в каталог **Sable/v.3.0/**, далее — в подкаталог с номером версии используемой операционной системы и установить пакет, содержащийся в подкаталоге.

4. Для установки абонентского пункта необходимо перейти в папку **TS**, далее в подкаталог с номером версии используемой операционной системы и установить пакет, соответствующий требуемому уровню безопасности.

Низкий уровень безопасности:

```
sudo dnf localinstall cts-3.7.6-70.ks1.redos7.1.x86_64.rpm --disablerepo=*
```

Средний уровень безопасности:

```
sudo dnf localinstall cts-3.7.6-70.ks2.redos7.1.x86_64.rpm --disablerepo=*
```

Для удаления программного обеспечение абонентского пункта выполните команду:

```
sudo dnf remove cts
```

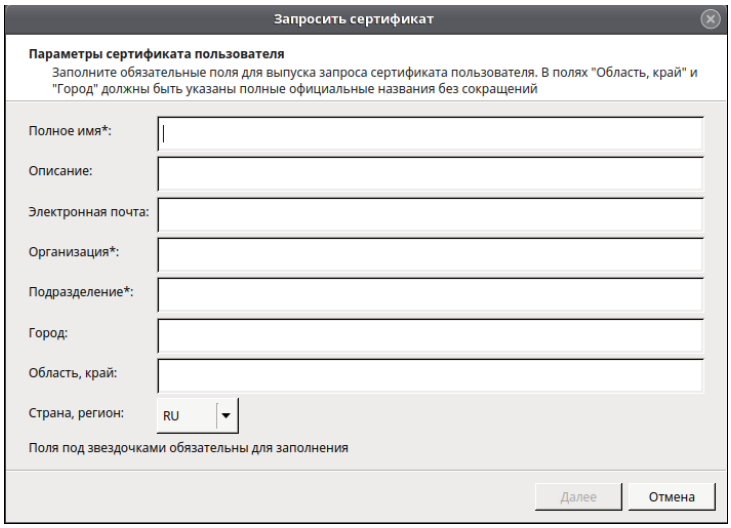
Для запуска абонентского пункта необходимо перезапустить службу **cts**. Для этого выполните команду:

```
sudo systemctl restart cts
```

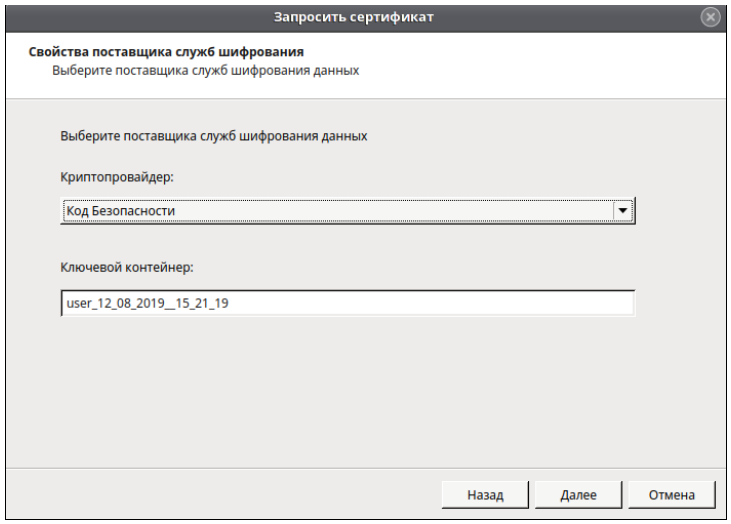
Работа с сертификатами

Создание запроса на сертификат

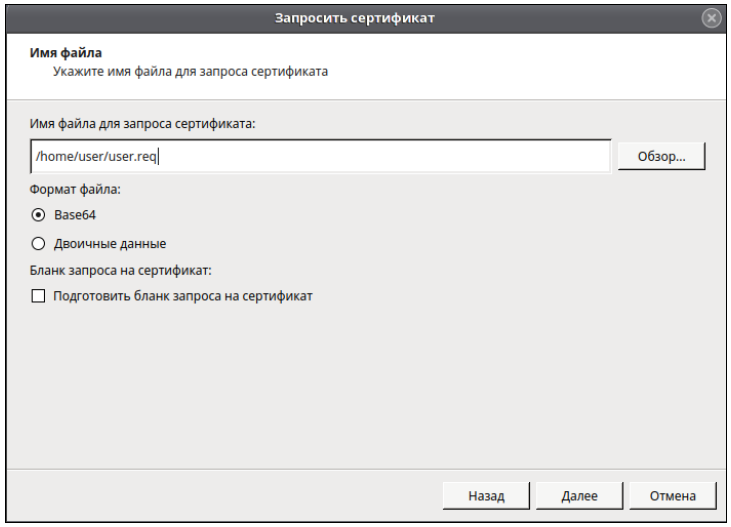
Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду **"Настройка → Запросить новый сертификат..."**.



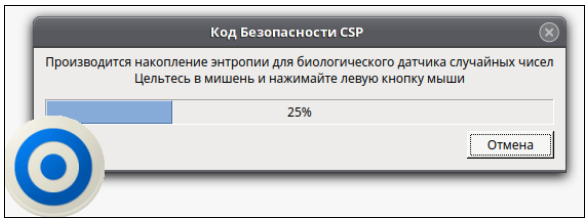
Заполните необходимые поля и нажмите кнопку **"Далее"**.



Выберите поставщика служб шифрования данных и, если необходимо, задайте имя ключевого контейнера и нажмите кнопку **"Далее"**.

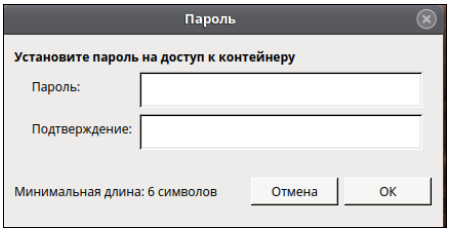


Укажите нужные сведения и нажмите кнопку **"Далее"**. На экране появится завершающее окно мастера запроса сертификата, содержащий введенные сведения. Проверьте указанные сведения и нажмите кнопку **"Готово"**. Если версия ПО абонентского пункта соответствует низкому уровню безопасности, на экране появится окно, предназначенное для накопления энтропии.

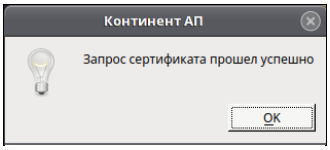


Если версия ПО абонентского пункта соответствует среднему уровню безопасности, на экране появится окно выбора ключевого носителя.

Выберите ключевой носитель и нажмите кнопку **"ОК"**. На экране появится окно задания пароля для доступа к ключевому контейнеру. Задайте пароль и нажмите кнопку **"ОК"**.



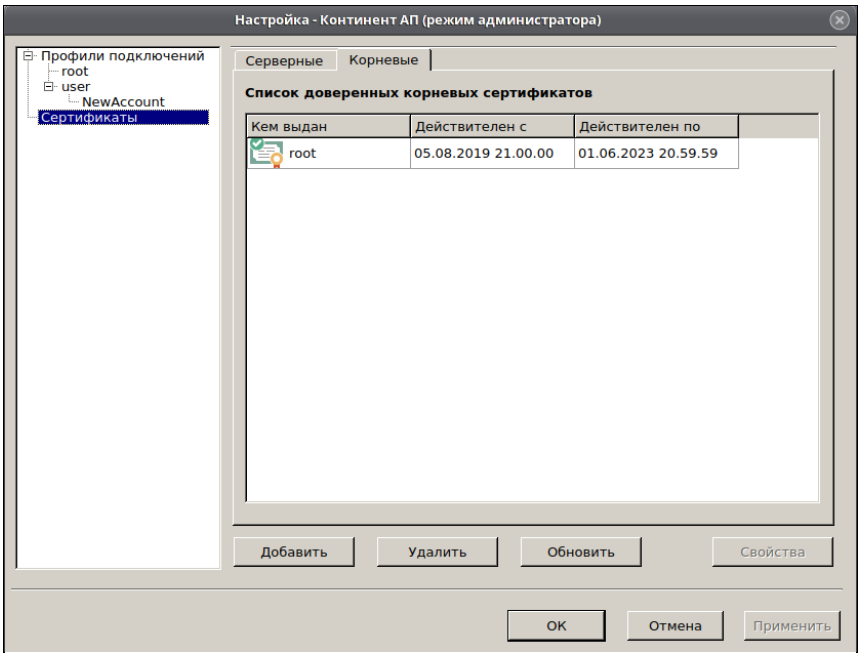
После на экране появится сообщение об успешном завершении создания запроса. Нажмите кнопку **"ОК"** в окне сообщения, извлеките ключевой носитель и передайте файл запроса администратору.



Регистрация сертификатов

На основании запроса, администратор сервера доступа создает и передает пользователю в виде файлов **user.cer**, **root.p7b** и **serv.cer** сертификат пользователя, корневой сертификат и серверный сертификат.

Регистрация корневого сертификата может быть выполнена пользователем в режиме администратора. Для этого необходимо войти в режим администратора и ввести пароль суперпользователя. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду **"Режим администратора → Параметры"**. Для входа в режим администратора введите пароль суперпользователя и на экране появится окно в соответствии с выбранным пунктом меню. Выберите в меню пункт **"Сертификаты"** и перейдите на вкладку **"Корневые"**. На вкладке отобразятся зарегистрированные корневые сертификаты.

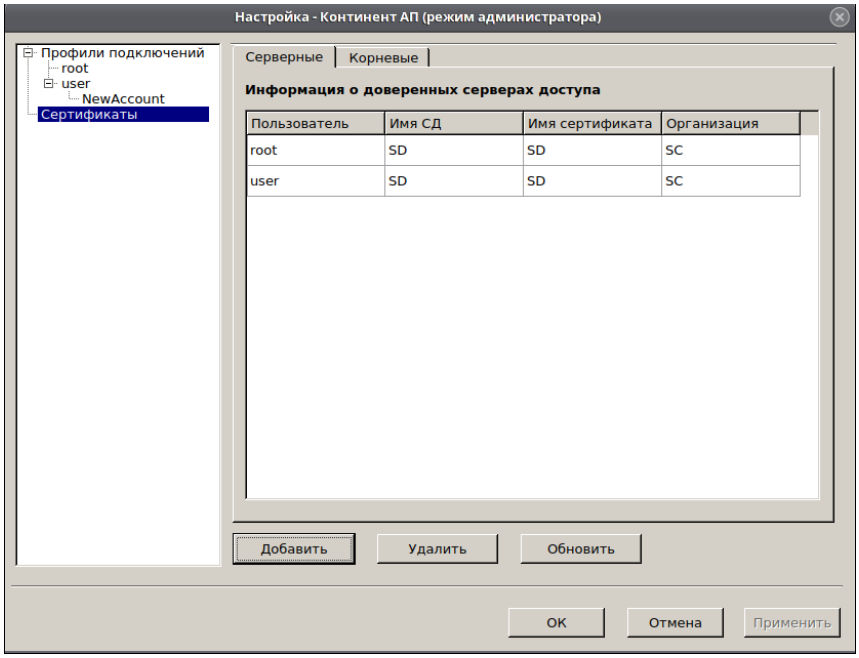


Для регистрации корневого сертификата нажмите кнопку **"Добавить"**. На экране появится окно для выбора файла. Откройте нужную папку, выберите файл сертификата и нажмите кнопку **"Открыть"**. Сертификат появится в списке.

Список доверенных серверов доступа

Для установления соединения сервер доступа, к которому осуществляется подключение, должен входить в **список доверенных серверов**.

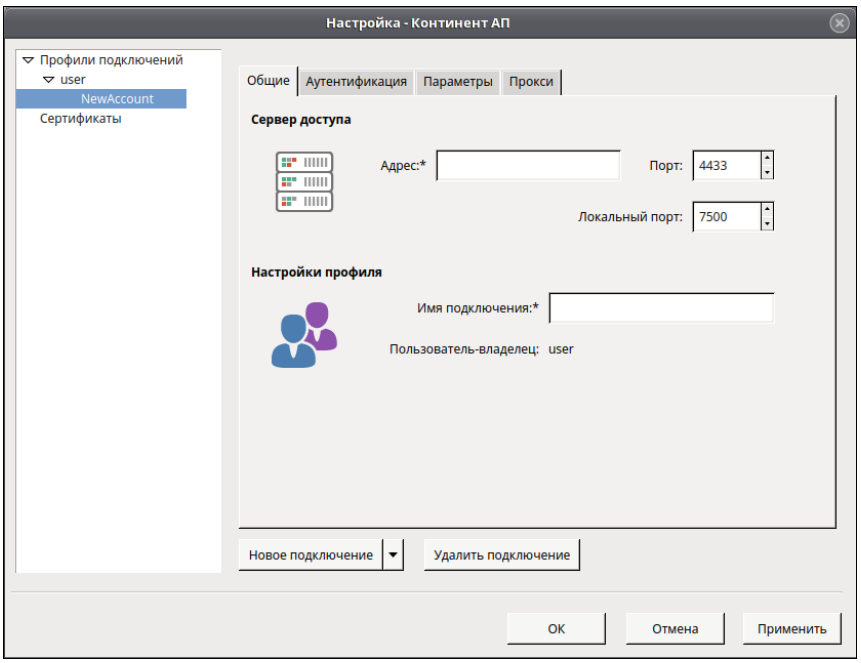
Откройте окно настроек абонентского пункта, выберите меню **"Сертификаты"** и перейдите на вкладку **"Серверные"**. Для регистрации серверного сертификата нажмите кнопку **"Добавить"**. На экране появится окно для выбора файла. Откройте нужную папку, выберите файл сертификата и нажмите кнопку **"Открыть"**.



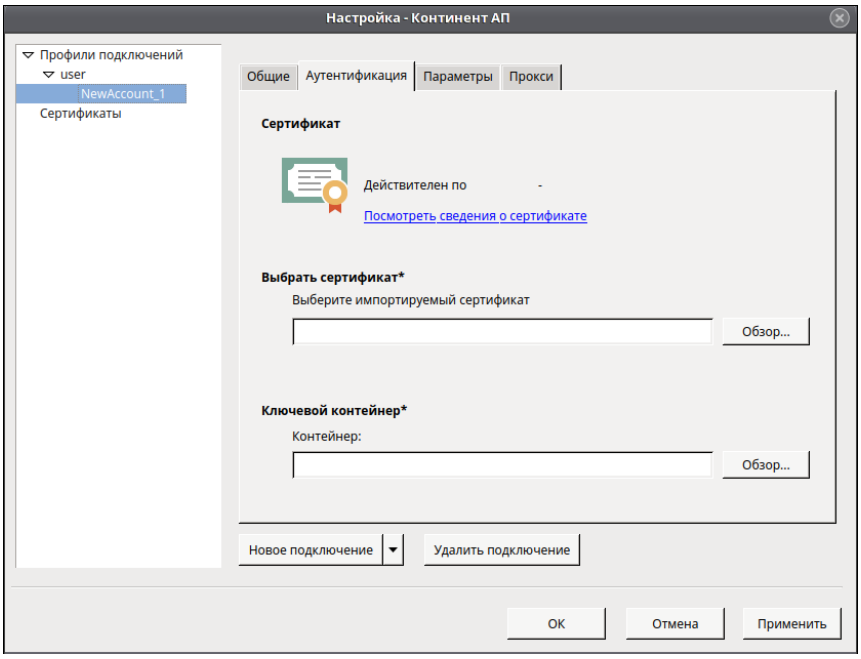
Настройка подключений

Создание нового профиля подключения

Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и активируйте команду **"Настройка → Параметры"**. На экране появится окно в соответствии с выбранным пунктом меню. В меню **"Профили"** подключений выберите нужного пользователя. В нижней части окна нажмите кнопку **"Новое подключение"**.



На вкладке **"Общие"** введите имя нового подключения, укажите нужные значения параметров и перейдите на вкладку **"Аутентификация"**.



Укажите сертификат пользователя и имя связанного с ним ключевого контейнера. Для этого используйте кнопку **"Обзор"**.

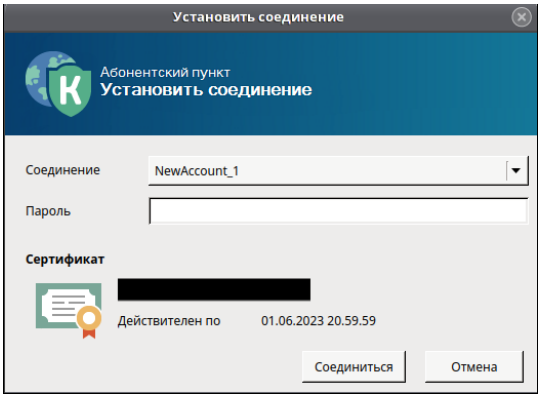
Перейдите на вкладку **"Параметры"**, проверьте значения, установленные по умолчанию, и при необходимости введите нужные значения.

При необходимости использовать **прокси-сервер** перейдите на вкладку **"Прокси"** и выполните настройку. **По умолчанию прокси-сервер не используется.**

Для сохранения установленных значений параметров нажмите кнопку **"Применить"**.

Подключение к серверу доступа

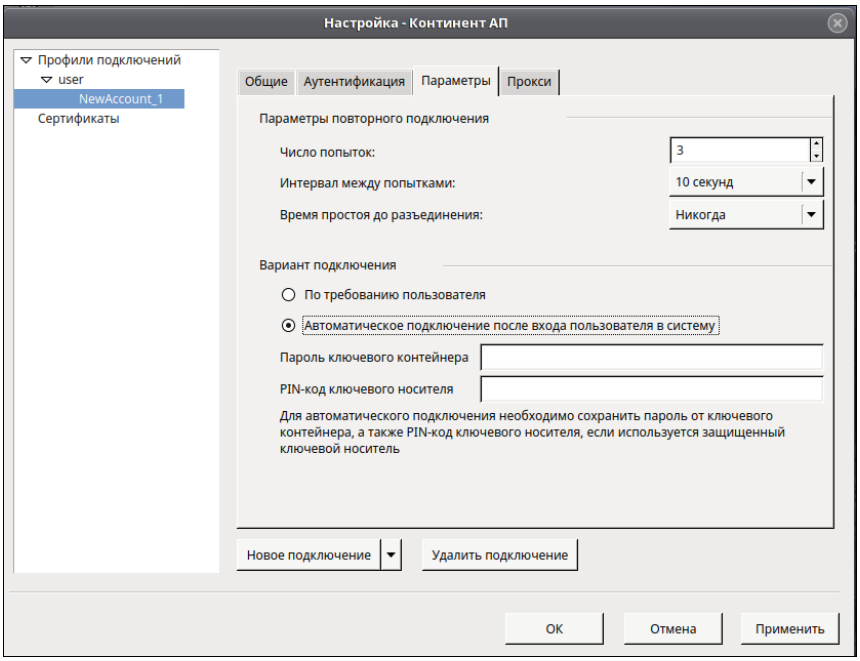
Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач, и выберите команду **"Подключить"**. На экране появится окно **"Установить соединение"**.



В поле **"Соединение"** укажите профиль подключения. Введите пароль доступа к ключевому контейнеру и нажмите кнопку **"Соединиться"**.

Автоматическое подключение к серверу доступа

Вызовите окно настроек абонентского пункта. Откройте меню **"Профили подключений"** и выберите в списке нужное подключение. Перейдите на вкладку **"Параметры"** и у параметра **"Вариант активации подключения"** установите значение **"Автоматическое подключение после входа пользователя в систему"**.



Введите пароль ключевого контейнера и **PIN-код** ключевого носителя и нажмите кнопку **"Применить"**.

Разрыв соединения с сервером доступа

Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач. В контекстном меню активируйте команду **"Разорвать. Соединение"** с сервером доступа будет разорвано. При этом пиктограмма абонентского пункта на панели задач примет вид **"Отключено"**.

Криптографический комплекс КАРМА

Установка КриптоПро CSP 5.0
Установка плагина CryptoPro Extension for CAdES Browser Plug-in
Установка личных и корневых сертификатов
Установка дополнительных пакетов
Установка КАРМА
Работа с программой

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** carma-56.2.435

Криптографический комплекс КАРМА — программное решение для использования криптографических функций, таких как шифрование, установка и проверка электронной цифровой подписи, в прикладных функциональных системах.

КАРМА позволяет применять в прикладном программном обеспечении криптографические методы защиты информации, используя высокоуровневый интерфейс, не требующий специальных знаний в области криптографии, учёта особенностей использования различных криптографических провайдеров и оперирования специальными криптографическими объектами, такими как ключевые контейнеры, хэш-функции и прочее.

Визуальная оболочка позволяет использовать *КАРМА* в качестве персонального АРМ для криптографической обработки файлов.

Установка КриптоПро CSP 5.0

Установка **КриптоПро CSP 5.0** выполняется согласно инструкции «Установка КриптоПро CSP 5.0».

Установка плагина «CryptoPro Extension for CAdES Browser Plug-in»

Установка **плагина КриптоПро** выполняется согласно инструкции «Установка КриптоПро «CryptoPro Extension for CAdES Browser Plug-in»».

Установка личных и корневых сертификатов

Установка *корневых и личных сертификатов* производится согласно инструкции «Графические утилиты для работы с КриптоПро CSP».

Установка дополнительных пакетов

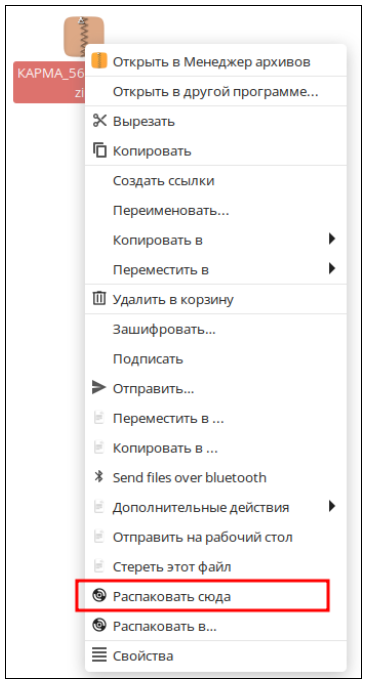
Для корректной установки криптографического комплекса *КАРМА* необходимо установить дополнительные пакеты. Для этого выполните команду (с правами администратора или суперпользователя системы):

```
dnf install libmicrohttpd libcurl tinyxml qt5-qtbase qt5-qtbase-gui
```

Установка КАРМА

Перейдите на официальный сайт разработчика и получите дистрибутив программы.

Затем перейдите в каталог с загруженным архивом, нажмите правой кнопкой мыши по архиву и выберите в контекстном меню «**Распаковать сюда**».



Далее перейдите в директорию с распакованными файлами и выполните команду установки:

```
cd /home/user/Загрузки/KAPMA_56.2.442-R5/Linux/
dnf install carma-common-56.2.442-redos8.x86_64.rpm carma-capilite-56.2.442-redos8.x86_64.rpm carma-dev-56.2.442-redos8.x86_64.rpm
```

По умолчанию КАРМА устанавливается в режиме пользовательского графического приложения. Для запуска криптографического модуля в графическом режиме откройте «**Главное меню**» — «**Прочие**» — «**Карма**».

Для запуска приложения в режиме демона (от *текущего* пользователя) необходимо указать ключ запуска:

```
/usr/local/carma/EosCryptoSvc -d
```

Для установки в виде **systemd**-сервиса необходимо выполнить скрипт **./carma.service_install.sh** из комплекта поставки, предварительно указав *имя пользователя* и *группу* в файле **./carma.service**:

```
[Service]
...
User=user
Group=user
```

> **Примечание.**
>
> Перед повторной регистрацией сервиса и установкой под *другим* пользователем необходимо выполнить скрипт **uninstall_daemon.sh**.

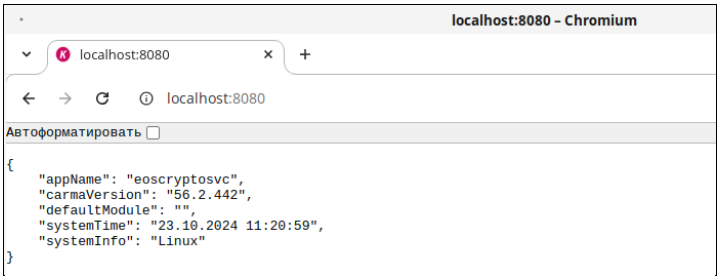
На этом установка и предварительная настройка сервиса *KAPMA* завершена.

Работа с программой

Для проверки работоспособности в терминале выполните команду `curl http://localhost:8080`. Если настройка выполнена верно, вывод команды будет иметь следующий вид:

```
{
  "appName": "eoscryptosvc",
  "carmaVersion": "56.2.442",
  "defaultModule": "",
  "systemTime": "23.10.2024 11:21:18",
  "systemInfo": "Linux"
}
```

Проверку работоспособности также можно выполнить в браузере. Для этого в адресной строке введите http://localhost:8080.



Также в браузере будут доступны следующие предопределенные страницы:

- localhost:8080 — страница доступа к веб-сервису;
- localhost:8080/test — страница тестирования функций сервиса;
- http://localhost:8080/settings — страница редактирования настроек сервиса.

Установка Kaspersky Endpoint Security

Установка «Kaspersky Endpoint Security 11.3 и новее для Linux»
Установка агента антивируса «Kaspersky Endpoint Security 11 для Linux»
Установка графической составляющей для «Kaspersky Endpoint Security 11.3 и новее для Linux»
Запуск и остановка Kaspersky
Дополнительные настройки

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: Kaspersky Endpoint Security 11 для Linux - 11.3.0.7441

Вы можете подробнее ознакомиться с установкой и настройкой **Kaspersky**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Kaspersky Endpoint Security;
- в **Яндекс.Дзен** — Установка Kaspersky Endpoint Security;
- в **VK Видео** — Установка Kaspersky Endpoint Security.

На наших каналах вы также сможете найти много другой полезной информации.

Установка «Kaspersky Endpoint Security 11.3 и новее для Linux»

Откройте в браузере страницу для скачивания установочных файлов «**Kaspersky Endpoint Security 11 для Linux**».

Скачайте установочный файл дистрибутива **RPM** (x64) kesl-11.3.0-7441.x86_64.rpm.

Перейдите в каталог с загруженным файлом дистрибутива (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
```

Далее в терминале выполните следующие команды (потребуются права администратора):

```
sudo -E dnf install kesl-11.3.0-7441.x86_64.rpm perl-Getopt-Long perl-File-Copy
```

Запустите скрипт настройки **Kaspersky Endpoint Security**:

```
sudo -E /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Выберите локаль (параметры региона) для антивируса (для использования системной локали нажмите **Enter**):

```
Setting up the Anti-Virus Service default locale
List of available locales:
- ru_RU.UTF-8
- de_DE.UTF-8
- en_US.UTF-8
- fr_FR.UTF-8
- ja_JP.UTF-8
- zh_CN.UTF-8
[ru_RU.UTF-8]:
```

Для ознакомления с пользовательским соглашением нажмите **Enter**. После этого введите «**y**»:

```
Accepting the End User License Agreement (EULA) and Privacy Policy
Press ENTER to display the EULA and Privacy Policy:
I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement [y/n]: y
```

Введите «**y**» для согласия с политикой конфиденциальности:

```
I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy [y/n]: y
```

Для соглашения с положением о **Kaspersky Security Network** введите «**y**»:

```
Configuring KSN
I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement (KSN Statement is available here: '/opt/kaspersky/kesl/doc/ksn_license.ru') [y/n]: y
```

Введите имя пользователя, которому будут предоставлены права администратора для антивируса:

```
Granting the Administrator role
Only users with the Administrator role have full access to Kaspersky Endpoint Security management by command line and GUI.
Specify user to grant the 'admin' role to (leave empty to skip): user
```

Настройка SELinux – введите «**y**»:

```
SELinux configuration
Do you want to configure SELinux automatically? [y]: y
```

Введите адрес сервера для загрузки обновлений (нажмите **Enter** для использования серверов Лаборатории Касперского по умолчанию):

```
Configuring the update source
Specify the update source. Possible values: KLServers|SCServer|<url>:[KLServers]:
```

При необходимости, введите данные для использования прокси сервера. Для пропуска настройки нажмите **Enter**:

```
If you use an HTTP proxy server to access the Internet, please enter the address in one of the following formats: proxyIP:port or user:pass@proxyIP:port, or enter 'no' [n]: n
```

Для загрузки актуальной базы данных антивируса нажмите **Enter**:

```
Do you want to download the latest databases now? [y]:
```

Для активации запланированных обновлений нажмите **Enter** (по умолчанию проверка обновлений будет выполняться каждый час):

```
Do you want to enable scheduled updates? [y]:
Scheduled updates are enabled.
The application databases are scheduled to be updated hourly.
```

Введите ключ активации либо нажмите **Enter** для использования пробного ключа на 30 дней:

```
Activate the application
You must activate the application to use it.
To activate the application now, enter the path to your key file or an activation code. Enter an empty string to add the built-in trial key:
Adding the built-in trial key has completed successfully.
```

Проверьте статус задач:

```
sudo -E kesl-control --get-task-list
```

Запустите следующие задачи:

- Защита от файловых угроз:

```
sudo kesl-control --start-task 1 -W
```

- Проверка загрузочных секторов:

```
sudo kesl-control --start-task 4 -W
```

Рекомендуется запустить все задачи, которые будут применяться при использовании **Kaspersky Endpoint Security**.

Убедитесь, что в файле **audit.log** нет ошибок:

```
sudo -E grep kesl /var/log/audit/audit.log
```

Установка агента антивируса «Kaspersky Endpoint Security 11 для Linux»

На данной странице можно скачать «**Агент администрирования**» - файл RPM (x64) klnagent64-14.0.0-4646.x86_64.rpm. Для установки перейдите в каталог со скачанным файлом дистрибутива и выполните следующие команды (потребуются права администратора системы или суперпользователя **root**):

```
cd /home/user/Загрузки
dnf install klnagent64-14.0.0-4646.x86_64.rpm
/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

Ф а й л **/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl** содержит параметры настроек агента администрирования, при необходимости их можно отредактировать.

После запуска установщика(**postinstall.pl**), вам будет предложено ознакомится с лицензионным соглашением. После прочтения, закройте его, нажав на клавишу **"q"**, и подтвердите принятие условий соглашения клавишей **"y".**

Далее установщик Касперского выполнит интерактивную установку **Агента администрирования**.

Потребуется указать DNS-имя или IP-адрес сервера:

```
Please enter Administration Server DNS-name or static IP-address:
```

Далее необходимо задать порты сервера и ssl:

```
Please enter Administration Server port number [14000]:
Please enter Administration Server ssl port number [13000]:
```

При необходимости можно согласиться с использованием ssl-шифрования:

```
Please enter 'Y' to confirm that you want to use SSL encryption or enter 'N' to use non-encrypted communication [Y]:
```

Затем выберите тип конфигурирования:

```
The Network Agent being installed can be used as connection gateway. It will allow you to connect to Administration Server using the specified connection gateway.
1) Do not configure connection gateway
2) Do not use connection gateway
3) Connect to server using connection gateway
4) Use as connection gateway
Please choose connection gateway mode: [1]:
```

На этом установка **Агента администрирования** завершена.

Установка графической составляющей для «Kaspersky Endpoint Security версии 11.3 и новее для Linux»

Откройте в браузере страницу для скачивания установочных файлов «**Kaspersky Endpoint Security 11 для Linux**».

Установка графической составляющей KESL производится через **rpm**-пакет. Скачайте установочный файл дистрибутива **RPM** (x64) kesl-gui-11.3.0-7441.x86_64.rpm.

Перейдите в каталог с загруженным файлом дистрибутива.

В терминале выполните следующую команду:

```
sudo dnf install kesl-gui-11.3.0-7441.x86_64.rpm
```

Выполните перезагрузку ПК, чтобы завершить настройку.

Запуск антивируса будет доступен из «**Главного меню**» – «**Системные**» – «**Kaspersky Endpoint Security 11.3.0 для Linux**».

Запуск и остановка Kaspersky Endpoint Security

Чтобы остановить **Kaspersky Endpoint Security** в systemd-системе, выполните следующую команду:

```
systemctl stop kesl
```

Чтобы перезапустить **Kaspersky Endpoint Security** в systemd-системе, выполните следующую команду:

```
systemctl restart kesl
```

Чтобы вывести статус **Kaspersky Endpoint Security** в systemd-системе, выполните следующую команду:

```
systemctl status kesl
```

Дополнительные настройки

Если Вы по каким-либо причинам пропустили пункт настройки прав администратора для пользователя (**Specify user to grant the 'admin' role to (leave empty to skip)**), то права администратора можно назначить с помощью команды в терминале:

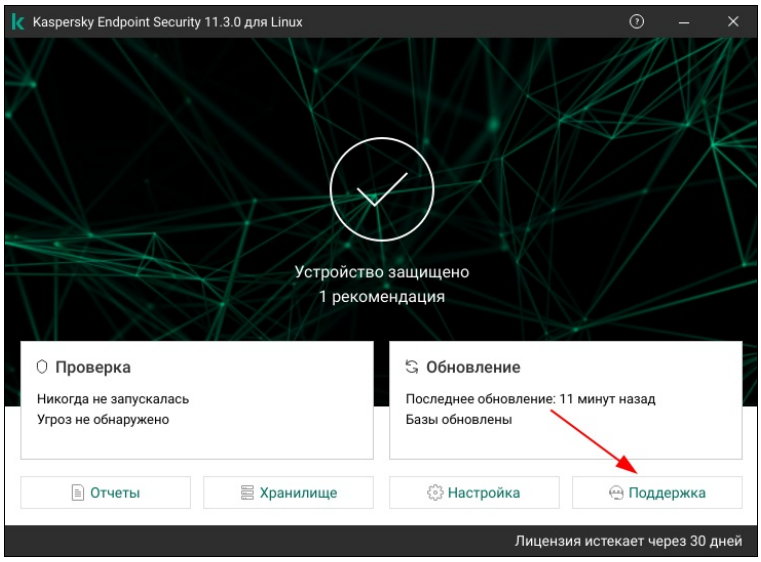
```
sudo -E kesl-control --grant-role admin user
```

где **user** - имя пользователя.

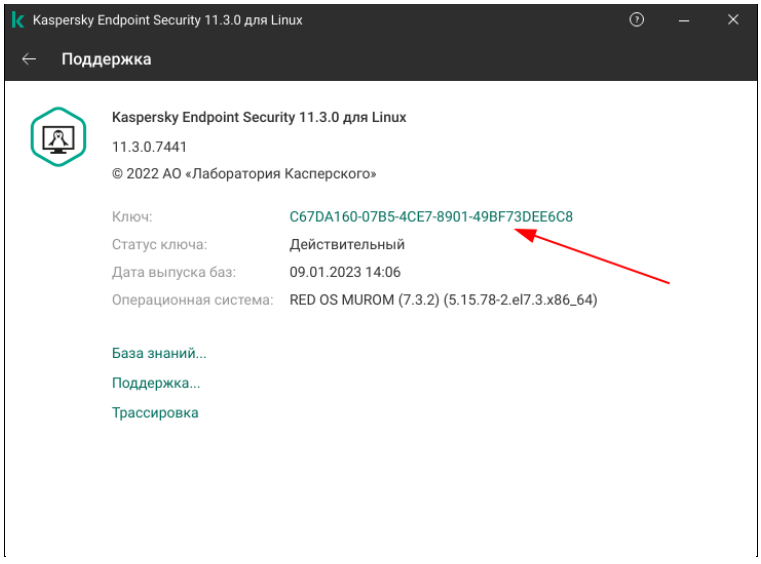
Если был пропущен этап ввода ключа активации, можно выполнить команду в терминале:

```
sudo -E kesl-control --add-active-key <код_активации_или_файл_ключа>
```

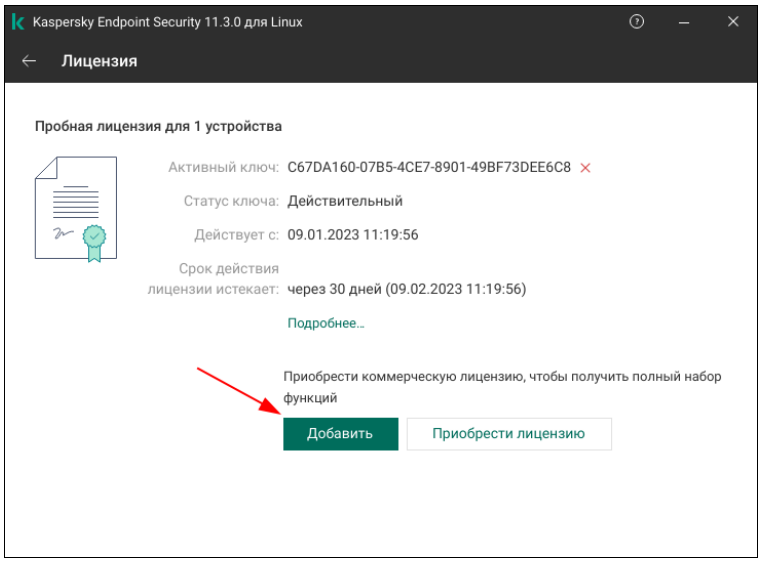
Также ввод активации ключа доступен в графическом интерфейсе. Для этого нажмите на кнопку «**Поддержка**».



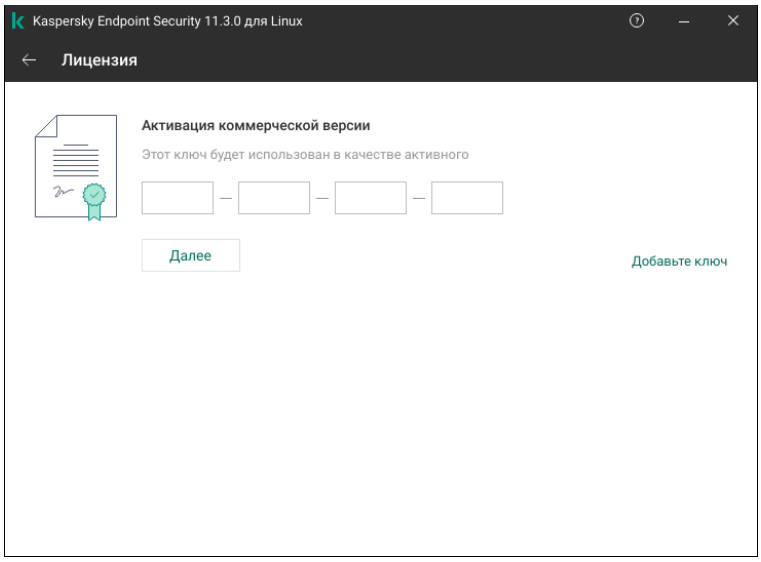
Затем кликните ЛКМ на временный (30-дневный) ключ.



Будет открыто окно, в котором необходимо нажать на кнопку «**Добавить**».



Введите ключ лицензии или укажите файл ключа.



Установка Kaspersky Security Center

Установка и настройка СУБД
Установка и настройка KSC
Установка и настройка WebConsole

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: ksc64-15.2.0, ksc-web-console-15.2.265, mariadb-3:10.11.6-3

Вы можете подробнее ознакомиться с настройкой и работой **Kaspersky**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Kaspersky Security Center и WebConsole в РЕД ОС ;
- в **Яндекс.Дзен** — Установка Kaspersky Security Center и WebConsole в РЕД ОС ;
- в **VK Видео** — Установка Kaspersky Security Center и WebConsole в РЕД ОС .

На наших каналах вы также сможете найти много другой полезной информации.

Установка и настройка СУБД

1. Выполните установку **MariaDB**:

```
sudo dnf install mariadb-server mariadb
```

2. Запустите службу и добавьте ее в автозагрузку:

```
sudo systemctl enable mariadb --now
```

Проверьте статус службы:

```
systemctl status mariadb
```

В статусе должно отображаться **active (running)**.

3. Выполните сценарий установки БД:

```
/usr/bin/mysql_secure_installation
```

Данный сценарий подробно описывает каждый шаг. Сначала он запросит пароль пользователя **root**, но т. к. после начальной установки он не задан, нажмите **Enter** и на следующем этапе задайте свой пароль.

В процессе выполнения сценария можно нажимать **Enter**. В результате будут удалены анонимные пользователи, удаленный root-логин, тестовые таблицы, а также будут перезагружены привилегии.

4. Далее необходимо настроить конфигурационный файл **/etc/my.cnf**, включив поддержку **InnoDB** и хранилища **MEMORY**, а также кодировок **UTF-8** и **UCS-2**.

```
sudo nano /etc/my.cnf
```

Пример содержимого файла:

```
[client-server]
 port = 3306
 socket = /var/run/mysqld/mysqld.sock
 [mysqld]
 basedir=/usr
 tmpdir=/tmp
 port=3306
 bind-address=0.0.0.0
```

```
local-infile=0
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
symbolic-links=0
sql_mode = ""
log-error = /var/log/mysql-error.log
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=2048M #укажите свой объем памяти в МБ
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Значение innodb_buffer_pool_size должно быть *не менее 80%* от ожидаемого размера базы данных *KAV*. Обратите внимание, что указанная память выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Если вы используете **MariaDB 10.4.3** или более раннюю версию, фактический размер выделенной памяти примерно на *10% превышает* указанный размер буфера.

5. Для применения внесенных изменений перезапустите службу:

```
systemctl restart mariadb
```

6. Проверьте статус службы:

```
systemctl status mariadb
```

В статусе должно отображаться **active (running)**.

Установка и настройка KSC

1. Создайте непривилегированную учетную запись **ksc** и группу **kladmins**. Учетная запись должна быть членом группы **kladmins**. Для этого последовательно выполните следующие команды:

```
sudo adduser ksc
```

```
sudo groupadd kladmins
```

```
sudo gpasswd -a ksc kladmins
```

```
sudo usermod -g kladmins ksc
```

2. Перейдите на официальную страницу разработчика KSC, выберите и скачайте необходимую версию продукта.

3. Запустите установку **Kaspersky Security Center**:

```
sudo dnf install /<путь_к_файлу>/ksc64-<версия>.rpm
```

4. Запустите настройку **Kaspersky Security Center**:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```



4.1 Прочтите *Лицензионное соглашение* и *Политику конфиденциальности*. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

a. Введите **y**, если вы понимаете и принимаете условия *Лицензионного соглашения*. Введите **n**, если вы не принимаете условия *Лицензионного соглашения*. Чтобы использовать *Kaspersky Security Center Linux*, необходимо принять условия *Лицензионного соглашения*.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y
```

b. Введите **y**, если вы понимаете и принимаете условия *Политики конфиденциальности* и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно *Политике конфиденциальности*. Введите **n**, если вы не принимаете условия *Политики конфиденциальности*. Чтобы использовать *Kaspersky Security Center Linux*, необходимо принять условия *Политики конфиденциальности*.

```
Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y
```

4.2 При отображении запроса введите следующие параметры:

a. Введите DNS-имя *Сервера администрирования* или статический *IP-адрес*. Для локальной установки – **127.0.0.1**.

b. Введите номер SSL-порта *Сервера администрирования*. По умолчанию номер порта – **13000**.

c. Оцените примерное количество устройств, которыми вы планируете управлять:

- если у вас от 1 до 100 сетевых устройств, введите **1**;
- если у вас от 101 до 1000 сетевых устройств, введите **2**;
- если у вас более 1000 сетевых устройств, введите **3**.

```
Enter Administration Server DNS-name or static IP-address:
127.0.0.1

Enter Administration Server SSL port number [13000]:


Define the approximate number of devices that you intend to manage:
1) 1 to 100 networked devices
2) 101 to 1 000 networked devices
3) More than 1 000 networked devices
Enter the range number (1, 2, or 3) [1]:
1
```

d. Введите имя группы безопасности для служб. По умолчанию используется группа **kladmins**.

e. Введите имя учетной записи для запуска службы *Сервера администрирования*. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись **ksc**.

f. Введите имя учетной записи, чтобы запустить другие службы. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись **ksc**.

g. Выберите СУБД, которую вы установили для работы с *Kaspersky Security Center Linux*:

- если вы установили MySQL или MariaDB, введите **1**;
- если вы установили PostgreSQL или Postgres Pro SQL, введите **2**.

h. Введите DNS-имя или IP-адрес устройства, на котором установлена база данных. Для локальной установки – **127.0.0.1**.

i. Введите номер порта базы данных. Этот порт используется для связи с *Сервером администрирования*. По умолчанию используются следующие порты:

- порт **3306** для MySQL или MariaDB;
- порт **5432** для PostgreSQL или Postgres Pro.

j. Введите имя базы данных **mariadb.**

k. Введите имя учетной записи **root** базы данных, которая используется для доступа к базе данных.

l. Введите **пароль** учетной записи **root** базы данных, которая используется для доступа к базе данных.

```
Enter the security group name for services:
kladmins

Enter the account name to start the Administration Server service. The
account must be a member of the entered security group:
ksc

Enter the account name to start other services. The account must be a
member of the entered security group:
ksc

Choose the database type to connect to:
1) MySQL
2) Postgres
Enter the range number (1 or 2):
1

Enter the database address:
127.0.0.1

Enter the database port:
3306

Enter the database name:
mariadb

Enter the database login:
root

Enter the database password:
```

Подождите, пока службы добавятся и запустятся автоматически:

- klnagent_srv;
- kladminserver_srv;
- klactprx_srv;
- klwebsrv_srv.

Создайте учетную запись, которая будет выполнять роль администратора *Сервера администрирования*. Введите имя пользователя и пароль (пароль должен содержать от 8 до 16 символов).

```
It is necessary to create an Administration Server account. This user will
act as an Administration Server administrator. The user password cannot
have less than 8 and more than 16 characters.
Enter the user name:
admin
```

Вы можете использовать следующую команду для создания пользователя:

```
sudo /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <пароль>
```

Пользователь будет добавлен, а *Kaspersky Security Center Linux* установлен.

5. Проверьте, запущены ли необходимые службы:

```
systemctl status klnagent_srv.service kladminserver_srv.service klactprx_srv.service klwebsrv_srv.service
```

В статусе должно отображаться **active (running)**.

Установка и настройка WebConsole

1. Создайте файл ответов, который содержит параметры для подключения *Kaspersky Security Center Web Console* к *Серверу администрирования*. Имя файла **ksc-web-console-setup.json**.

```
sudo nano /etc/ksc-web-console-setup.json
```

Пример файла ответов, содержащего минимальный набор параметров, адрес и порт по умолчанию:

```
{
 "address": "192.168.122.49",
 "port": 8080,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
 "acceptEula": true
 }
```

Описание параметров:

- `address` – адрес, по которому будет осуществляться доступ к консоли, статичный IP, который вы задавали ранее;
- `port` – порт, по которому будет осуществляться доступ к консоли;
- `trusted` – параметры подключения к серверу KSC, путь к сертификату KSC, имя сервера;
- `acceptEula` – принятие лицензионного соглашения.

Подробную информацию о файле см. по ссылке.

Программа *Kaspersky Security Center Web Console* не может быть обновлена с помощью того же установочного файла **.rpm**. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки программы, сначала необходимо удалить программу, а затем установить ее снова с новым файлом ответов.

2. Перейдите на официальную страницу, выберите и скачайте необходимую версию *Kaspersky Security Center Web Console*.

3. Запустите установку скачанного файла с расширением **.rpm** (необходимы права суперпользователя или администратора системы):

```
sudo dnf install ksc-web-console-[номер_сборки].x86_64.rpm
```

Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки. *Kaspersky Security Center Web Console* устанавливается в каталог **/var/opt/kaspersky/ksc-web-console**.

4. Перезапустите все службы *Kaspersky Security Center Web Console*, выполнив следующую команду:

```
sudo systemctl restart KSC*
```

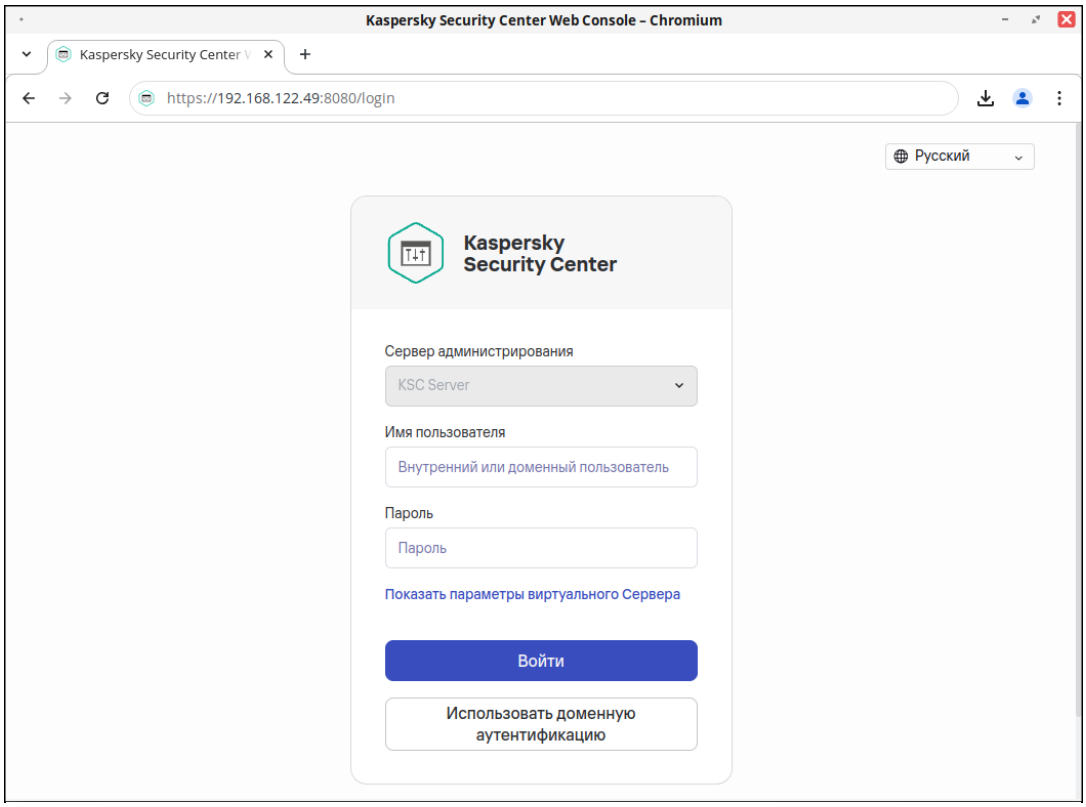
5. Проверьте статус служб:

```
systemctl status KSC*
```

В статусе должно отображаться **active (running)**.

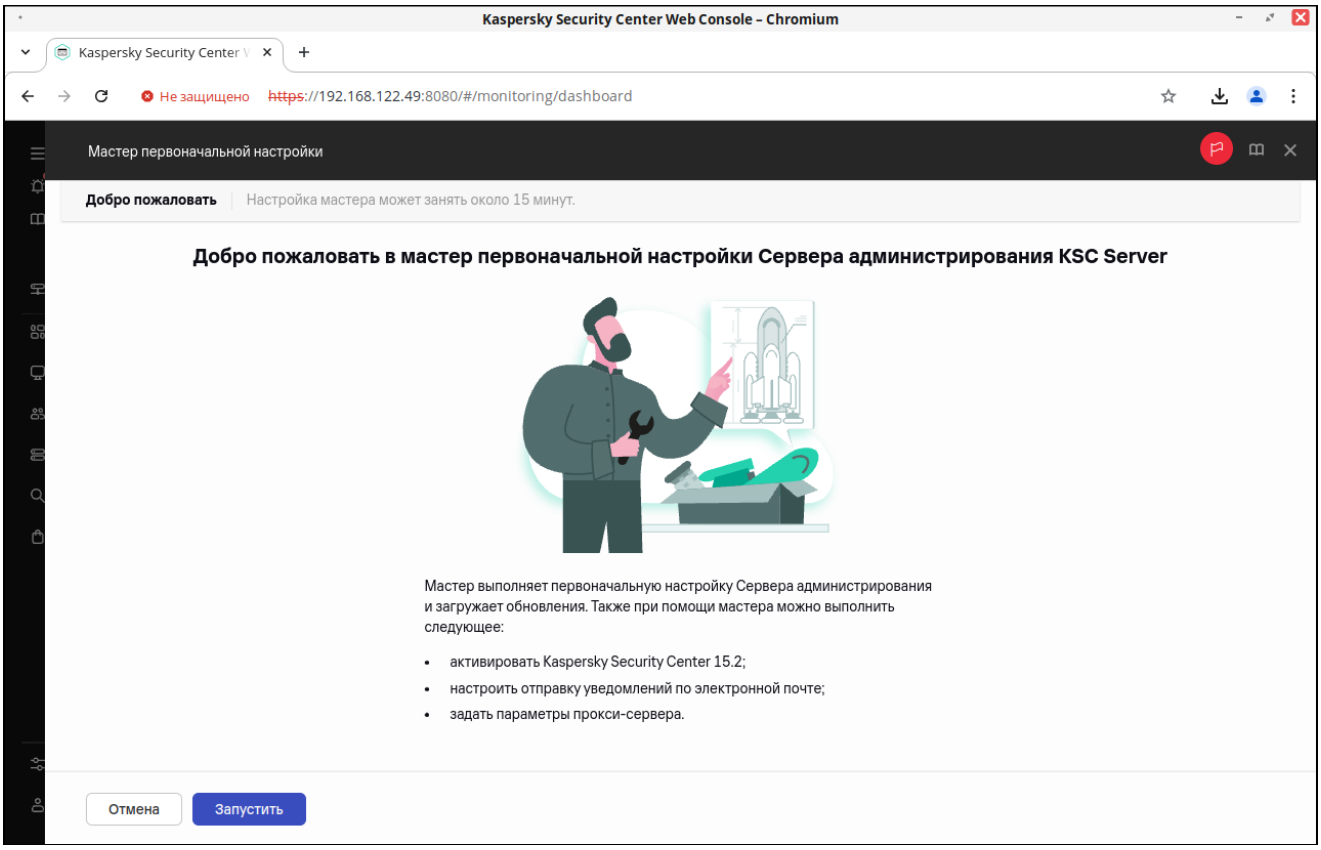
Перейдите в веб-консоль *Kaspersky Security Center Web Console*, для этого в браузере в адресную строку введите https://192.168.122.49:8080.

В вашем браузере **JavaScript** должен быть включен.



Используйте *логин* и *пароль* администратора, указанные при установке **KSC**, для доступа к инструментам администрирования.

После входа запустится мастер первоначальной настройки, с его помощью вы сможете настроить основные политики, задачи, активировать программу и пр.



Со сравнением функционала версий для *Windows* и *Linux* можно ознакомиться на данной странице.

Установка Dr.Web

Подключение репозитория Dr.Web
Установка Dr.Web

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** drweb-workstations-11.1.5

Вы можете подробнее ознакомиться с информацией по установке и настройке **Dr.Web**, просмотрев наши обучающие видео:

- на **RuTube** — Установка Dr.Web;
- в **Яндекс.Дзен** — Установка Dr.Web;
- в **VK Видео** — Установка Dr.Web.

На наших каналах вы также сможете найти много другой полезной информации.

Подключение репозитория Dr.Web

Создайте файл репозитория **drweb** командой (потребуются права **администратора**):

```
nano /etc/yum.repos.d/drweb.repo
```

Добавьте в него следующее содержимое:

```
[drweb]
 name=DrWeb - 11.1
 baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
 enabled=1
 gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Установка Dr.Web

Для установки **Dr.Web** выполните команду (потребуются права **администратора**):

```
dnf install drweb-workstations
```

После установки антивирус будет доступен из «**Главного меню**» — «**Dr.Web**» — «**Dr.Web для Linux**».



О DHCP

DHCP - Протокол динамической конфигурации хоста, представляет собой протокол сетевого управления, посредством которого сервер DHCP динамически назначает IP-адрес и другие параметры конфигурации сети для каждого устройства в сети.

Включенный в состав РЕД ОС DHCP-сервер, соответствующий RFC 2131, включает фирменные расширения BOOTP (RFC 2132). Так же поддерживает протокол конфигурации динамического хоста для IPv4 (DHCPv4), который может использоваться для обмена информацией о полном доменном имени клиента DHCPv4, описанный в RFC 4702.

Поддерживается стандарт DHCPv6, описанный в RFC 3315. Так же поддерживается контроль и настройка параметров доступа к беспроводным точкам доступа (CAPWAP) DHCP, описанные в RFC 5417.

Базовая настройка DHCP

Установка и первоначальная настройка

Устанавливаем **DHCP**:

```
dnf install dhcp-server
```

Настройки для диапазона адресов **IPv4** производятся в файле **/etc/dhcp/dhcpd.conf**. Пример данного файла можно посмотреть в файле **/usr/share/doc/dhcp-server/dhcpd6.conf.example**. Ваша версия **dhcpd** в пути может отличаться.

Вы можете подробнее ознакомиться с базовой настройкой DHCP, просмотрев наши обучающие видео:

- на **RuTube** — Базовая настройка DHCP;
- в **Яндекс.Дзен** — Базовая настройка DHCP;
- в **VK Видео** — Базовая настройка DHCP.

На наших каналах вы также сможете найти много другой полезной информации.

Теперь откроем на редактирование конфигурационный файл:

```
nano /etc/dhcp/dhcpd.conf
```

Подсети обозначаются блоками, пример такого блока представлен ниже:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.0 192.168.0.100;
  range 192.168.0.120 192.168.0.254;
  option domain-name-servers 192.168.0.10, 192.168.0.11;
  option domain-name "redos.test";
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  default-lease-time 600;
  max-lease-time 7200;
 }
```

где:

- ***subnet*** *обозначает сеть, в области которой будет работать данная группа настроек;*
- ***range*** *— диапазон, из которого будут браться IP-адреса, диапазон адресов 192.168.0.101—192.168.0.120 выдаваться не будет;*
- ***option domain-name-servers*** *— через запятую перечисленные DNS-сервера;*
- ***option domain-name*** *— суффикс доменного имени;*
- ***option routers*** *— шлюз по умолчанию;*
- ***option broadcast-address*** *— адрес сети для широковещательных запросов;*
- ***default-lease-time***, ***max-lease-time*** *— время и максимальное время в секундах, на которое клиент получит адрес, по его истечению будет выполнено продление срока.*

Добавляем правило в **firewalld** (дополнительную информацию см. в нашей инструкции "Настройка брандмауэра Firewall"):

```
firewall-cmd --permanent --add-service=dhcp
firewall-cmd --reload
```

Некоторые дополнительные параметры

option domain-name *string***;** — параметр задает доменное имя, которое клиенты используют при запросах к DNS, при разрешении имен.

option netbios-name-servers <*ip-address*> [**,** *ip-address*...]**;** — задает список серверов имен **NetBIOS** (NBNS), соответствующих **RFC 1001/1002.** Сервера должны быть перечислены в порядке предпочтительности. Сервера имен **NetBIOS** также известны как сервера **WINS**.

option netbios-dd-server <*ip-address*> [**,** *ip-address*...]**;** — опция сервера распределения данных **NetBIOS** (NBDD) указывает список серверов **RFC 1001/1002 NBDD**. Серверы должны быть перечислены в порядке предпочтения.

option netbios-node-type INT**;** — параметр позволяет сконфигурировать тип узла, т.е. способ разрешения имен клиентами **NetBIOS** поверх **TCP/IP**.

Возможные значения параметра:

- **1 B-node (Broadcast):** разрешение имен с помощью широковещательных запросов, WINS не используется;
- ***2*** **P-node (Peer):** используется только WINS;
- ***4*** **M-node (Mixed):** смешанный тип, сначала используется широковещательный запрос, затем в случае неудачи — WINS;
- ***8*** **H-node (Hybrid):** смешанный наоборот, WINS, а затем broadcast.

option netbios-scope *string***;** — опция области **NetBIOS** указывает параметр **NetBIOS** через **TCP/IP** для клиента, как указано в **RFC 1001/1002**. См. RFC1001, RFC1002 и RFC1035 для ограничения набора символов.

BOOTP

Каждый клиент **BOOTP** может быть настроен отдельно в файле **dhcpd.conf**. Самая простая конфигурация состоит из адреса сетевой карты и IP-адреса, назначаемого этому клиенту. Если клиент должен быть загружен с сервера, указывается загрузочный образ. Простая конфигурация для клиента **BOOTP** может выглядеть так:

```
host haagen {
 hardware ethernet 08:00:2b:4c:59:23;
 fixed-address 239.252.197.9;
 filename "/tftpboot/haagen.boot";
 }
```

где:

- **hardware ethernet** — MAC-адрес сетевого интерфейса клиента, используется сервером для идентификации конкретного устройства;
- **fixed-address** — указывает, какой IP-адрес должен быть назначен клиенту, адрес будет фиксированным для данного клиента, и сервер всегда будет назначать именно его этому устройству;
- **filename** — указывает путь к загрузочному образу, который клиент должен загрузить.

Дополнительные параметры.

Включение и отключение bootp

С помощью следующих директив можно управлять тем, разрешены ли BOOTP-запросы для сервера:

- **allow bootp** — разрешает серверу обрабатывать BOOTP-запросы;
- **deny bootp** — запрещает серверу обрабатывать BOOTP-запросы.

Параметр **bootp** сообщает серверу dhcp обрабатывать или нет bootp-запросы. По умолчанию bootp-запросы разрешены.

Параметр ***dynamic-bootp*** в секции **range** указывается в случае, если предполагается назначать адреса из диапазона клиентам по протоколу **BOOTP**.

Необходима хотя бы одна секция **h o s t** для каждого BOOTP-клиента, обслуживаемого сервером. Так ж е **host** может быть указана для DHCP-клиентов, хотя это и не обязательно, если только не требуется раздача адресов только определенным клиентам.

Если требуется обеспечить выдачу фиксированных адресов и конфигурацию клиентов по протоколам **DHCP** или **BOOTP** в более, чем одной подсети, то можно указать несколько адресов с помощью параметра *fixed-address* или указать несколько секций **host.**

Если клиентские параметры меняются в зависимости от сети, к которой подключен клиент, то необходимо использовать множественные записи **host.**

<имя_хоста> — имя, идентифицирующее хост. Если в описании хоста опция **hostname** не указана, то используется значение **<имя_хоста>**.

Объявления *Host* сопоставляются с реальными DHCP или BOOTP-клиентами путем сравнения опции **dhcp-client-identifier,** указанной в секции *host* со значением, предоставленным клиентом, или если клиент не предоставляет **dhcp-client-identifier**, то путем сравнения опции *hardware* и аппаратного (mac) адреса клиента. Клиенты BOOTP нормально не предоставляют *dhcp-client-identifier*, так что, при работе по протоколу BOOTP, необходимо использовать mac-адреса.

hardware <*тип_железа*> <*аппаратный_адрес*>**;**

Для того что бы BOOTP-клиент был опознан сервером, его mac-адрес должен быть объявлен с помощью параметра *hardware* в секции *host* параметр ***<тип_железа>*** — тип физического интерфейса. В настоящее время используются только **ethernet** и **token-ring** и, возможно, скоро будут реализованы другие типы, особенно **fddi**.

<аппаратный_адрес> — записывается как набор шестнадцатеричных значений (от 0 до ff), разделенных двоеточиями. Параметр *hardware* можно использовать и для DHCP-клиентов.

Параметр *dynamic-bootp-lease-cutoff*

dynamic-bootp-lease-cutoff <*дата*>**;**

Параметр ***dynamic-bootp-lease-cutoff*** устанавливает момент времени, в который все адреса, назначенные клиентам BOOTP, должны быть освобождены. Так как клиенты BOOTP не имеют возможности продлить срок использования полученных адресов и не могут определить, что срок аренды истек, то по умолчанию клиентам BOOTP адреса выделяются на неограниченный срок. Однако в некоторых случаях оказывается полезным установить параметр ***dynamic-bootp-lease-cutoff***, например в учебном заведении при окончании семестра или в ночное время, когда предприятие не работает, а все компьютеры выключены.

<дата> — срок окончания действия всех адресов, выделенных BOOTP-клиентам. Дата указывается в следующем формате: **W ГГГГ/ММ/ДД ЧЧ:ММ:СС** .

- **W** — день недели в виде числа от 0 (воскресенье) до 6 (суббота);
- **ГГГГ** — год;
- **ММ** — месяц 1..12;
- **ДД** — день месяца 1..31;
- **ЧЧ** — часы 0..23 MM — минуты 0..59;
- **СС** — секунды 0..59.

Время указывается в GMT, а не местное.

Параметр *dynamic-bootp-lease-length*

dynamic-bootp-lease-length <*время_в_секундах*>**;**

Параметр ***dynamic-bootp-lease-length*** используется для указания срока, на который выделяется адрес BOOTP-клиенту. В некоторых организациях возможна ситуация, что по прошествии определенного времени можно быть уверенным, что выделенный адрес уже не используется. Период задается числом секунд. Если клиент перезагружается в момент, когда срок, указанный в этом параметре еще не истек, то период аренды адреса заново устанавливается в указанное значение. Таким образом, часто перезагружаемые BOOTP-клиенты могут постоянно удерживать свой адрес. Необходимо заметить, что при настройке параметра следует быть осторожным.

always-reply-rfc1048 <*on/off*>**;**

Некоторые BOOTP-клиенты ожидают ответа от сервера в стиле **RFC1048**, но сами не следуют **RFC1048** при посылке запросов. Если в вашей сети имеется такой проблемный клиент, который не воспринимает параметры, передаваемые ему сервером, и если в логах появляется сообщение **"(non-rfc1048)"** , то можно воспользоваться этим параметром.

Если у вас все клиенты требуют работы в стиле **RFC1048**, то можно использовать параметр **always-reply-rfc1048**. Параметр может быть указан в любом объявлении, в этом случае - воздействует только на тех клиентов, которые соответствуют указанной зоне действия.

Резервирование ip-адреса за клиентом

Хост с именем **myhost**, у которого сетевая карта имеет MAC **08:45:32:00:00:23** должен иметь постоянный адрес **192.168.1.121**.

```
host myhost {
 hardware ethernet 08:45:32:00:00:23;
 fixed-address 192.168.1.121;
 }
```

Определенный интерфейс для работы

Если в системе присутствует несколько сетевых адаптеров, а сервер DHCP должен работать только для определенных, открываем на редактирование следующий файл:

```
nano /etc/sysconfig/dhcpd
```

И добавляем в него следующее:

```
DHCPDARGS=enp0s8
```

** в данном примере сервер будет работать только для интерфейса **enp0s8**.*

Перед запуском убедитесь, что сетевой адаптер **enp0s8** настроен для работы в создаваемой сети. Для этого создайте файл **/etc/sysconfig/network-scripts/ifcfg-enp0s8** со следующим содержимым.

```
TYPE="Ethernet"
 BOOTPROTO="none"
 DNS1="192.168.0.1"
 IPADDR0="192.168.0.1"
 PREFIX0=24
 GATEWAY0=192.168.0.1
 DEFROUTE="yes"
 PEERDNS="yes"
 PEERROUTES="yes"
 IPV4_FAILURE_FATAL="no"
 IPV6INIT="yes"
 IPV6_AUTOCONF="yes"
 IPV6_DEFROUTE="yes"
 IPV6_PEERDNS="yes"
 IPV6_PEERROUTES="yes"
 IPV6_FAILURE_FATAL="no"
 IPV6_ADDR_GEN_MODE="stable-privacy"
 NAME="enp0s8"
 DEVICE="enp0s8"
 ON BOOT="yes"
```

Разрешаем автозапуск сервиса:

```
systemctl enable dhcpd
```

и запускаем его:

```
systemctl start dhcpd
```

Настройка логов

По умолчанию, сервер **dhcp** ведет лог в файле **/var/log/messages**, что не очень удобно, так как это общий лог-файл, в котором может находиться много записей.

Для того чтобы сервер сохранял записи в отдельный файл, открываем на редактирование **rsyslog.conf**:

```
nano /etc/rsyslog.conf
```

И добавляем следующее:

```
local6.*       /var/log/dhcp.log
```

Далее открываем конфигурационный файл **dhcp**:

```
nano /etc/dhcp/dhcpd.conf
```

И добавляем:

```
log-facility local6;
```

Перезапускаем сервисы:

```
systemctl restart dhcpd
systemctl restart rsyslog
```

Настройка DHCP-сервера для работы с сервером PXE

Отредактируйте файл **/etc/dhcp/dhcpd.conf**:

```
nano /etc/dhcp/dhcpd.conf
```

Добавьте строку в конец файла до фигурной скобки.

```
filename "pxelinux.0";
 next-server <имя_сервера>;
 }
```

Параметр **next-server** используется для указания клиенту адреса сервера, с которого должен быть получен загрузочный файл (тот самый файл, что указан в параметре *filename*). <**Имя_сервера**> может быть IP-адресом или доменным именем. Если этот параметр не указан, то используется адрес DHCP-сервера.

Отказоустойчивый сервер DHCP

Подготовка серверов

Для отказоустойчивой конфигурации необходимо два сервера DHCP.

Синхронизируйте время, между серверами с помощью ntpsec или chrony. Так же можно воспользоваться командой ntpdate, которую нужно выполнить на обоих серверах к одному ntp-серверу.

```
ntpdate <адрес сервера ntp>
```

Предположим, что имеется два сервера, на которых установлен пакет dhcp и добавлен в автозапуск.

Первичный сервер: 192.168.0.1

Вторичный сервер: 192.168.0.2

Настройка первичного сервера

1. Пропишите необходимые правила для iptables, если вы используете его.

```
iptables -A INPUT -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
iptables -A INPUT -s 192.168.0.2/24 -p tcp -m state --state NEW -m tcp --dport 647 -j ACCEPT
```

2. Отредактируйте файл /etc/dhcp/dhcpd.conf.

```
nano /etc/dhcp/dhcpd.conf
```

Обратите внимание, что параметр **mclt** (максимальное время выполнения клиента) должен быть определен на главном сервере, но не должен быть определен на подчиненном сервере. Параметр **split** является еще одним параметром , который должен быть определен на первичном и опущен из конфигурации на вторичном сервере. Стоит отметить, что связь между отказоустойчивыми узлами не шифруется и не аутентифицируется.

```
failover peer "failover-dhcp" {
  primary; # Определяет главный сервер
  address 192.168.0.1; # адрес первичного сервера
  port 647;
  peer address 192.168.0.2; # адрес вторичного сервера
  peer port 647;
  max-response-delay 60;
  max-unacked-updates 10;
  mclt 3600;
  split 128;
  load balance max seconds 3;
}

authoritative;
default-lease-time 86400; # 1 день
max-lease-time 86400; # 1 день
update-static-leases on;
one-lease-per-client on;

omapi-port 7911;
omapi-key omapi_key;
key omapi_key {
     algorithm hmac-md5;
     secret a6d79e096b7055ff51e5756c77947ab5==; # сформируйте секретный ключ с помощью любого генератора, указав тип
шифрования hmac-md5
}

subnet 192.168.0.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  option routers 192.168.0.1;
  option domain-name-servers redos.test;
  option domain-search "redos.test";
  pool {
    failover peer "failover-dhcp";
    range 192.168.0.100 192.168.0.200;
  }
}
```

+ Описание параметров

name *data* просмотр

имя связи резервирования, задается в файле **dhcpd.conf**.

partner-address *data*

IP адрес резервного сервера.

local-address *data*

IP адрес текущего сервера.

partner-port *data*

порт TCP, на котором резервный сервер ожидает подключения по протоколу failover.

local-port *data*

порт TCP, на котором текущий сервер ожидает подключения по протоколу failover.

max-outstanding-updates *integer*

количество обновлений, которые могли быть важными, но остались без ответа в этой связке резервирования.

mclt *integer*

максимальное время перенаправления клиента в этой связке резервирования.

default-lease-time *integer*

срок по умолчанию для клиентов, которые не запрашивают определенный срок аренды. Срок аренды DHCP может быть назначен от нуля секунд до бесконечности.

max-lease-time *integer*

максимальный срок аренды

update-static-leases *data*

если он включен, то сервер DHCP делает обновление DNS для клиентов.

one-lease-per-client *data*

если этот флаг включен, всякий раз, когда клиент отправляет DHCPREQUEST для конкретной аренды, сервер автоматически отчищает любые другие lease записи, которыми владеет клиент.

load-balance-max-secs *integer*

максимальное значение в поле secs запроса клиента после которого будет произведена балансировка нагрузки.

load-balance-hba *data*

массив хэшей буферов для балансировки нагрузки в этой связке резервирования.

local-state *integer*

текущий статус сервера DHCP в этой связке резервирования. Возможные значения:

```
1  - партнер выключен
2  - обычная работа
3  - обмен данными прерван
4  - разрешение прервано
5  - потенциальный конфликт
6  - восстановление
7  - восстановление закончено
8  - выключение
9  - пауза
10 - запуск
11 - идет восстановление
```

В общем случае делать изменения в этом атрибуте - плохая идея. Однако в случае, когда известно, что резервный сервер выключен, бывает необходимо явно указать что резервный сервер недоступен и необходимо взять на себя выданные адреса резервного сервера как можно быстрее. Если же вы указали, что резервный сервер выключен, а он работает (но временно

недоступен), возможны конфликты назначения IP адресов.

partner-state *integer*

текущий статус резервного сервера

local-stos *integer*

время, в течение которого сервер работает в текущем статусе.

partner-stos *integer*

время, в течение которого резервный сервер работает в текущем статусе.

hierarchy *integer*

роль сервера: первичный (0) или вторичный (1) в текущей связке резервирования.

last-packet-sent *integer*

время последнего пакета синхронизации, отправленного резервному серверу в связке.

last-timestamp-received *integer*

время последнего пакета синхронизации, полученного от резервного сервера в связке.

skew *integer*

разница между часами резервного и текущего сервера

max-response-delay *integer*

время в секундах, по истечении которого если не получен ни один пакет синхронизации, определяется разрыв в соединении.

cur-unacked-updates *integer*

количество сообщений об обновлении, полученных от резервного сервера, но пока не обработанных.

3. Из за того, что хеш находится в файле, закроем к нему доступ.

```
chmod 0600 /etc/dhcp/dhcpd.conf
```

4. Проверьте конфигурационный файл

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
```

5. Перезапустите сервис

```
systemctl restart dhcpd
```

Настройка вторичного сервера

1. Пропишите настройки для iptables, если используете его

```
iptables -A INPUT -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
iptables -A INPUT -s 192.168.0.1/24 -p tcp -m state --state NEW -m tcp --dport 647 -j ACCEPT
```

2. Для вторичного (secondary) сервера:

```
failover peer "failover-dhcp" {
  secondary; # определитель вторичного сервера
  address 192.168.0.2;
  port 647;
  peer address 192.168.0.1;
  peer port 647;
  max-response-delay 60;
  max-unacked-updates 10;
  load balance max seconds 3;
}

authoritative;
default-lease-time 86400; # 1 day
```

```
max-lease-time 86400; # 1 day
update-static-leases on;
one-lease-per-client on;

omapi-port 7911;
omapi-key omapi_key;
key omapi_key {
  algorithm hmac-md5;
  secret a6d79e096b7055ff51e5756c77947ab5==; # впишите тот же секретный ключ, как и на первичном сервере
}

subnet 192.168.0.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  option routers 192.168.0.1;
  option domain-name-servers redos.test;
  option domain-search "redos.test";
  pool {
    failover peer "failover-dhcp";
    range 192.168.0.100 192.168.0.200;
  }
}
```

3. Из за того, что хеш находится в файле, закроем к нему доступ.

```
chmod 0600 /etc/dhcp/dhcpd.conf
```

4. Проверьте конфигурационный файл

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
```

5. Перезапустите сервис

```
systemctl restart dhcpd
```

О службе DNS (bind)

Если локальная сеть не подключена к сети Интернет, вполне возможно, что внутренний DNS-сервер в ней не нужен. За преобразование доменного имени в IP-адрес и обратно в Linux отвечает несколько разных механизмов, лишь один из которых базируется на службе доменных имён. В самом простом случае имена всех компьютеров вместе с их адресами можно записать в файл **/etc/hosts**. Порядок просмотра различных пространств имён указывается в файле **/etc/nsswitch.conf**. Строка **hosts: files nisplus nis dns** этого файла предписывает приложениям, пользующимся стандартной функцией **gethostbyname()** сначала заглянуть в **/etc/hosts**, затем попытаться получить таблицы **hosts** службы **nisplus** или **nis**, а только затем обращаться к DNS-серверу. Это вполне разумное правило, учитывая время выполнения запроса в каждом случае.

Если задачу преобразования имён в адреса взял на себя провайдер, собственный DNS-сервер можно тоже не заводить. В этом случае на всех компьютерах в качестве сервера имён указывается сервер провайдера (поле *nameserver* в файле **/etc/resolv.conf**), к которому и идут все запросы. Даже если внутренняя сеть организована согласно **RFC1918** (интранет) и адреса компьютеров в ней не могут отображаться в сети Интернет, DNS-запросы во внешний мир работать будут. Между собой компьютерам предлагается общаться с помощью **/etc/hosts** или IP-адресов.

Однако уже здесь очевидны две задачи, для решения которых можно организовать собственную службу доменных имён.

Первая задача - уменьшение времени ответа на DNS-запрос абонентов внутренней сети. Если канал подключения к Интернет обладает большим временем задержки (скажем, четверть секунды), то работа с данными, включающими в себя много доменных имён (например, с www-страницами) может стать весьма медленной, хотя общий объём трафика будет невелик. Система доменных имён - распределённая база данных, замечательно поддерживающая механизм кеширования запросов. Первое обращение к кеширующему DNS-серверу приводит к выполнению рекурсивного запроса: опрашивается сервер более высокого уровня, который, если не знает ответа, передаст запрос дальше. Результат запроса оседает в кеше, так что все последующие обращения именно к этой записи дальше кеширующего сервера не уйдут. Время жизни (*Time To Live, TTL*) записи в кеше определяется хозяином запрошенного доменного имени. По истечении TTL запись из кеша удаляется.

Вторая задача - именование компьютеров в интранет-сети. Это бывает важно, если среди компьютеров внутренней сети есть свои серверы (например, корпоративный WWW-сервер), к которым другие компьютеры обращаются по доменному имени. Поскольку адреса такой сети не пойдут дальше межсетевого экрана, вы можете использовать имя какого угодно, — в том числе несуществующего — домена и составить табличку в **/etc/hosts**. Однако раздавать эту табличку лучше всё-таки средствами DNS.

Обе эти задачи можно решить, воспользовавшись Bind - мощным полнофункциональным DNS-сервером (обратите внимание, пакет и сервис называются **bind**, а сама служба - **named**). При необходимости запуска bind с использованием chroot необходимо установить пакет bind-chroot. В этом случае будет использоваться каталог /var/named/chroot/.

Для того, чтобы запустить named в кеширующем режиме, достаточно раскомментировать и заполнить раздел настройки forwarders (вышестоящие серверы) в файле /var/named/chroot/etc/named.conf. Обратите внимание на возможные ограничения на право обращаться к серверу с обычными и рекурсивными запросами (настройки allow-query и allow-recursion). Можно раскомментировать находящиеся в этом файле разумные установки по умолчанию. Эти настройки открывают доступ только абонентам локальных сетей, т.е. сетей, к которым компьютер подключён непосредственно.

```
grep allow- /var/named/chroot/etc/named.conf
        allow-query     { localhost; any; };
        allow-query-cache { localhost; any; };
```

Использование Bind для полноценного именования компьютеров в локальной сети требует создания двух зон (т.е. прямой и обратной), содержащих в виде записей определённого формата информацию о доменных именах компьютеров и об их роли в этих доменах. Каждая зона должна включать запись типа SOA (State Of Authority, сведения об ответственности). В этой записи определяются основные временные и административные параметры домена, в том числе электронный адрес лица, ответственного за домен (администратора) и серийный номер зоны. Серийный номер - число в диапазоне от 0 до 4294967295 (2**32); каждое изменение, вносимое в зону, должно сопровождаться увеличением этого номера. Обнаружив увеличение серийного номера, кеширующие и вторичные серверы признают все закешированные записи из этой зоны устаревшими. Структура номера может быть любой, лишь бы он постоянно увеличивался. Удобно использовать формат «<год><месяц><число><версия>», где все числа, кроме года, двузначные, а версия может обнуляться раз в день, соответствовать времени (например, по формуле 100*(часы*60+минуты)/(60*24) или иметь сквозную нумерацию (в этом случае появляется сложность с переходом от версии 99 к версии 100, то есть 0). Даже если серийный номер генерируется автоматически, рекомендуется пользоваться этим форматом, наглядно отражающим время создания зоны. Пример зоны, не содержащей ничего, кроме записи SOA и обязательной записи типа NS, находится в файле /usr/share/doc/bind/sample/var/named/named.localhost.

Кроме записи типа SOA, в каждой зоне должна быть хотя бы одна запись типа NS (Name Server), указывающая адрес DNS-сервера, авторитетного в этом домене (как минимум - адрес сервера, на котором запущен named). Несколько зон включаются в настройку Bind автоматически (файл /var/named/chroot/etc/named.rfc1912.zones). Они нужны для обслуживания сети, привязанной к сетевой заглушке (127.0.0.1/8). Стоит обратить внимание на то, что имя домена, который обслуживается зоной, задаётся в файле настроек, а в самом файле зоны можно использовать относительную адресацию (без . в конце имени), так что операция переименования домена делается редактированием одной строки. Рекомендуется добавлять описания зон в конфигурационный файл /var/named/chroot/etc/named.rfc1912.zones.

Прямая зона нужна для преобразования доменного имени в IP-адрес - операции, необходимой многим программам постоянно. Большинство записей в прямой зоне - типа A (Address) - предназначены именно для этого. Другие часто встречающиеся типы записей - это CNAME (Canonical Name, настоящее имя), позволяющий привязать несколько дополнительных имён к одному, и MX (Mail eXchange, обмен почтой), указывающий, куда пересылать почтовые сообщения, в поле адресат которых встречается определённое доменное имя. Вот пример прямой зоны для воображаемого домена *internal.domain.net* (незначащие поля соответствующих файлов заменены на . . .):

```
# cat /var/named/chroot/etc/named.rfc1912.zones
 . . .
zone "example" IN {
        type master;
        file "internal.domain.net";
        allow-update { none; };
};
 . . .
# cat /var/named/chroot/var/named/internal.domain.net

  $TTL    1D
  @       IN      SOA server root.server (
  2004082202      ; serial
  12H             ; refresh
  1H              ; retry
  1W              ; expire
  1H              ; ncache
                  )
  IN      NS      server
  MX 10   server
  Server        A       10.10.10.1
  www           CNAME   server
  mail          CNAME   server
  jack          A       10.10.10.100
```

В этом примере совпадение имени файла и имени зоны осмысленно - так проще разбираться с содержимым каталога **/var/named/chroot/var/named/**. Используются правила умолчания: если в записи некоторое поле опущено, оно наследуется от предыдущей. Так, вместо A можно было бы всюду написать IN A, а вместо MX - @ IN MX (@ означает имя домена, указанное в конфигурационном файле). Как видно из пример, всю работу в сети делает компьютер с адресом 10.10.10.1, он же **server.internal.domain.net**, он же **www.internal.domain.net** и **mail.internal.domain.net**. Несмотря на наличие среди CNAME этого сервера имени mail, MX-запись указывает всё же не на него, а на действительный адрес - так рекомендовано RFC. Распространённая практика заводить запись типа A непосредственно на имя зоны (т. е. присваивать адрес имени internal.domain.net) приводит, помимо

незначительных выгод, к мелким, неочевидным и весьма трудно преодолимым трудностям, которые мы здесь описывать не будем, ограничившись советом не использовать этот - пусть и законный - трюк.

Для того чтобы преобразовывать IP-адреса в доменные имена, у каждой сети должна быть обратная зона. Если такой зоны нет, и в файле **/etc/hosts** тоже ничего не написано, операция не выполнится. Такое преобразование нужно гораздо реже и в основном по соображениям административным: для того, чтобы выяснить принадлежность компьютера (с которого, допустим, пытаются атаковать сервер) по его IP-адресу. Некоторые почтовые серверы проверяют, содержится ли IP-адрес машины, передающей сообщение, в обратной зоне и похоже ли полученное доменное имя на то, что указано в сообщении, и при несовпадении отказываются принимать письмо. К сожалению, поскольку неудобства, связанные с отсутствием обратной зоны, понятны лишь грамотному администратору, а таковых на просторах Интернета не слишком много, обратные зоны во множестве сетей либо отсутствуют, либо дают неверную информацию. В случае внутренней сети обратная зона необязательна, но желательна - для простоты администрирования и удовлетворения потребностей разных программных продуктов, которые ею пользуются.

Обратная зона состоит почти целиком из записей типа PTR (Pointer, указатель). Чтобы не умножать сущностей, решено было не вводить новый способ работы сервера имён и представить обратное преобразование IP-адреса как прямое преобразование доменного имени специального вида. Например, чтобы выяснить доменное имя компьютера с адресом 1.2.3.4, необходимо запросить информацию о доменном имени 4.3.2.1.in-addr.arpa. Таким образом, каждой подсети класса C (или выше) соответствует определённый домен, в котором можно найти ответ. Вот как выглядит обратная зона для нашего воображаемого домена:

```
 cat /var/named/chroot/etc/named.rfc1912.zones
zone "12.11.10.in-addr.arpa" { type master;
file "12.11.10.in-addr.arpa";
};
 cat /var/named/chroot/var/named/12.11.10.in-addr.arpa
$TTL 1D
@       IN      SOA  server.internal.domain.net.       root.server.internal.domain.net (
2004082201    ; serial
12H           ; refresh
1H            ; retry
1W            ; expire
1H            ; ncache
)
        IN      NS   server.internal.domain.net
0             PTR  internal.domain.net.
1             PTR  server.internal.domain.net
100           PTR  jack.internal.domain.net.
```

Обратите внимание, что относительные адреса, использованные в левой части записей PTR, раскрываются в полные вида **<адрес>.12.11.10.in-addr.arpa**, а в правой части используются полные (которые вполне могут указывать на имена в разных доменах).

Проверить синтаксическую правильность конфигурационного файла и файла зоны можно с помощью утилит **named-checkconf** и **named-checkzone**, входящих в пакет bind. Они же используются при запуске службы командой **service bind start**. Однако при интенсивной эксплуатации сервера, когда остановка службы нежелательна, можно попросить службу перечитать файлы настроек или определённые зоны с помощью утилиты **rndc** - вот тогда не стоит забывать о проверке синтаксиса.

Стоит иметь в виду, что, в отличие от прямых зон, обратные описывают административную принадлежность компьютеров, но сами принадлежат хозяину сети (как правило, провайдеру). Возникает особого рода затруднение, связанное с работой DNS-сервера уже не во внутренней сети, а в сети Интернет. Дело в том, что подсети класса C (т. н. сети /24, в которых сетевая маска занимает 24 бита, а адрес компьютера - 8) выдаются только организациям, способным такую подсеть освоить (в сети класса C 254 абонентских IP-адреса, один адрес сети и один широковещательный адрес). Чаще всего выдаются совсем маленькие подсети - от /30 (на два абонентских адреса) до /27 (на 30 адресов) - или другие диапазоны, сетевая маска которых не выровнена по границе байта. Таких подсетей в обратной зоне получится несколько, а возможности просто разделить её, отдав часть адресов в администрирование хозяевам, нет. Грамотный провайдер в таких случаях пользуется **RFC2317** (есть в пакете bind-docs), предписывающем в обратной зоне заводить не записи вида **PTR**, а ссылки **CNAME** на адреса в «классифицированных» обратных зонах специального вида. Обратное преобразование становится двухступенчатым, зато администрирование каждой классифицированной зоны можно отдать хозяину.

DNS-сервер, отвечающий на запросы из сети Интернет, должен быть зарегистрирован в родительском домене. В самом деле, единственный способ узнать, кто обслуживает домен **internal.domain.net** - спросить об этом у DNS-сервера домена **domain.net**. Так что о выделении поддомена необходимо договариваться с провайдером. Регистрацией в доменах первого уровня занимаются выделенные организации. Например, домен в зоне **.ru** необходимо регистрировать в компании АНО «Региональный Сетевой Информационный Центр» (RU-CENTER).

Правила требуют, чтобы при регистрации домена было указано не менее двух DNS-серверов, которые будут его обслуживать. Из всех зарегистрированных серверов (записей типа NS в родительской зоне) только одна соответствует т.н. первичному (master) серверу, а остальные - т.н. вторичным (slave). Для внешнего пользователя вторичный сервер не отличается от первичного: он столь же авторитетен в ответе на запрос об именах его домена. Отличия только в способе администрирования. Все изменения вносятся в зоны первичного сервера, а вторичный только кеширует эти зоны, целиком получая их по специальному межсерверному протоколу. Полученная зона складывается в файл, редактировать который бессмысленно: первичный сервер при изменении зоны рассылает всем своим вторичным указание скачать её заново. Право на скачивание зоны можно ограничить настройкой **allow-transfer** (как правило, в ней перечисляются адреса вторичных серверов). Вот слегка отредактированная цитата из руководства по Bind, описывающая задание вторичного сервера в файле настроек:

```
// We are a slave server for eng.example.com
zone "eng.example.com" { type slave;
file "slave/eng.example.com";
// IP address of eng.example.com master server masters { 192.168.4.12; };
};
```

Вторичный сервер хорошо размещать где-нибудь подальше от первичного, во всяком случае, в другой сети - так повышается надёжность обработки запроса (если один сервер недоступен, возможно, ответит второй) и возрастает скорость распространения записей по кешам промежуточных серверов.

Проверку работоспособности, доступности и вообще самочувствия DNS-сервера лучше всего делать утилитой **dig** из пакета **bind-utils**. Это очень мощная утилита, выдающая максимум информации о том, что происходило с запросом (запрашивая обратное преобразование, не забудьте добавить ключ **-x**). Более лаконична, но не менее мощна утилита **host** из того же пакета. Упоминаемую старыми руководствами по UNIX утилиту **nslookup** использовать не рекомендуется.

```
# dig jack.internal.domain.net
<<>> DiG 9.2.4rc5 <<>> jack.internal.domain.net
;; global options:   printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32751
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;jack.internal.domain.net.        IN     A
;; ANSWER SECTION:
jack.internal.domain.net. 86400   IN     A       10.11.12.100
;; AUTHORITY SECTION:
internal.domain.net. 86400        IN     NS      server.internal.domain.net.
;; ADDITIONAL SECTION:
server.internal.domain.net. 86400 IN     A       10.11.12.1
;; Query time: 37 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Aug 22 16:07:17 2004 ;; MSG SIZE rcvd: 95
```

Наконец, для выяснения административной принадлежности тех или иных доменов и сетей можно воспользоваться утилитой **whois**, которая обращается к специальной сетевой базе данных (не имеющей отношения к DNS).

Настройка DNS-сервера bind

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер минимальный
- **Версия bind:** bind-9.16.16

О сервере

В состав репозитория РЕД ОС включен DNS-сервер **bind**, поддерживающий стандарты **RFC 1034,1035, 2136**. Поддерживает реализацию хост-систем на базе стека протоколов **Internet**, описанных в **RFC 1123**. Поддерживает механизм инкрементального переноса зон **IXFR**, описанный в **RFC 1995** и механизм извещения ведомых серверов **NOTIFY, RFC 1996**.

Подготовка сервера

Устанавливаем все обновления:

```
dnf update
```

Установка и запуск BIND

Устанавливаем DNS-сервер следующей командой:

```
dnf install bind
```

Разрешаем автозапуск:

```
systemctl enable named --now
```

И проверяем, что он работает корректно:

```
systemctl status named
```

Базовая настройка DNS-сервера

Открываем на редактирование конфигурационный файл **bind**:

```
nano /etc/named.conf
```

и редактируем следующее в блоке **options**:

```
listen-on port 53 { 127.0.0.1; 192.168.0.1; };
listen-on-v6 port 53 { none; };
allow-query { any; };
forward first;
forwarders { 8.8.8.8; };
```

* 192.168.0.1 — IP-адрес нашего DNS-сервера, на котором он будет принимать запросы;

- **allow-query** разрешает выполнять запросы всем, но из соображений безопасности можно ограничить доступ для конкретной сети, например, вместо **any** написать **10.10.1.0/24**.
- **listen-on-v6 port 53** присвоим значение none, тем самым отключив ipv6
- **forward** с параметром **first** указывает, DNS-серверу пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders, и лишь в случае, если разрешить имя с помощью данных серверов не удалось, то будет осуществлять попытки разрешения имени самостоятельно.
- **forwarders** перенаправляем запросы, которые сами не резолвим, на днс сервер гугла.

Создание локальных зон DNS

Создайте папку с мастер зонами:

```
mkdir /var/named/master
```

Прямая DNS зона

Создайте прямую DNS-зону.

```
nano /var/named/master/example.org
```

Пример её содержимого с описанием ниже.

```
$TTL 604800     ;
example.org.    IN     SOA     ns01.example.org. root.example.org. (
                1              ; Serial
                600            ; Refresh
                3600           ; Retry
                1w             ; Expire
                360            ; Minimum TTL
                )
       IN      NS      ns01.example.org.
       IN      NS      ns02.example.org.
       IN      NS      ns03.example.org.
ns01    IN      A       192.168.10.50
ns02    IN      A       192.168.10.60
ns03    IN      A       192.168.10.70
www     IN      A       192.168.10.20
test    IN      A       192.168.10.12
```

Рассмотрим подробнее написанное:

$TTL 3600 — Time to live время жизни, по умолчанию 1 день. По достижении установленного времени, кеширующий сервер запрашивает DNS сервер, содержащий доменную зону, информацию о зоне. И при необходимости обновляет записи.
example.org IN SOA ns01.example.org. root.example.org. зона обслуживания, адрес корневого сервера для зоны, акаунт её админа. 2022112801**; Serial** - серийный номер версии таблицы dns. Самый лучший формат - ГГГГММДДNN, где NN - номер изменения таблицы за текущий день;
600; Refresh-указывает подчиненным DNS серверам как часто им обращаться, для поиска изменений к master серверу.
3600; Retry — говорит о том, сколько Slave сервер должен подождать, прежде чем повторить попытку.
1w; Expire — Максимальный срок жизни записей, после которой они потеряют актуальность (1 неделя)
300; Minimum TTL -минимальный срок жизни записи 5 мин.
NS ns01.example.org.-NS сервер который обслуживает эту зону
NS ns02.example.org.-NS сервер который обслуживает эту зону
NS ns03.example.org.-NS сервер который обслуживает эту зону
A 192.168.10.20 -если требуется попасть по адресу example.org, то клиенту будет выдан этот IP
ns01 A 192.168.10.50 — Записи для поиска наших NS серверов
ns02 A 192.168.10.60
ns03 A 192.168.10.70
test A 192.168.10.12 -Если клиент запрашивает адрес test.example.org, DNS выдаст ip 192.168.10.12?

Назначьте владельца и права.

```
chown -R root:named /var/named/master
chmod 0640 /var/named/master/*
```

В конфигурационный файл **named.conf** добавьте следующее:

```
zone "example.org" {
 type master;
 file "master/example.org";
 };
```

* где **example.org** — имя зоны, которую будет обслуживать наш DNS-сервер. Это и есть домен, для которого bind будет хранить записи. Должен совпадать по имени с файлом зоны в папке master.

Описание опций настройки зоны:

- **type** <тип зоны> (в нашем случае первичная — значит master). Другие варианты — **slave**, **stub**, **forward**.
- **file** <путь_к_файлу> с записями зоны. В данном примере указан относительный путь — то есть файл находится по пути **master/test.local**, который начинается относительно рабочей директории (по умолчанию — **/var/named/**). Таким образом, полный путь до файла — **/var/named/master/test.local**.

Для каждой зоны создайте свой блок **zone**.

Чтобы настройки применились, необходимо перезапустить службу.

```
systemctl restart named
```

Для проверки работоспособности сервера с другого компьютера сети (например, на Windows) выполняем команду:

```
> nslookup test.example.org 192.168.0.1
```

** данной командой мы пытаемся узнать IP-адреса сайта test.example.org через сервер 192.168.0.1.*

Должно получиться, примерно, следующее:

```
Server:     192.168.0.1
Address:    192.168.0.1#53

Name:       test.example.org
Address:    192.168.10.12
```

Создание обратной зоны

В конфигурационный файл **named.conf** добавьте следующее:

```
zone "10.168.192.in-addr.arpa" {
    type master;
    file "master/10.168.192.zone";
};
```

Создайте обратную DNS-зону.

```
nano /var/named/master/10.168.192.zone
```

Пример её содержимого с описанием ниже.

```
$TTL    3600
@  IN     SOA     example.org. root.example.org (
              20060204        ; Serial
              3600            ; Refresh
              900             ; Retry
              3600000         ; Expire
              3600 )          ; Minimum
@  IN     NS      localhost.
50 IN     PTR     ns01
60 IN     PTR     ns02
70 IN     PTR     ns03
20 IN     PTR     www
12 IN     PTR     test
```

Чтобы настройки применились, необходимо перезапустить службу.

```
systemctl restart named
```

Логирование Bind

Способ 1

По умолчанию, сервер **Bind** хранит логи в файле:

```
/var/named/data/named.run
```

Для его непрерывного просмотра вводим следующую команду:

```
tail -f /var/named/data/named.run
```

Степень детализации логов можно настроить в конфигурационном файле:

```
logging {
  channel default_debug {
    file "data/named.run";
  severity dynamic;
  };
};
```

* где **file** — путь к log-файлу; **severity** — уровень чувствительности к возникающим событиям.

Возможны следующие варианты для severity:

- **critical** — критические ошибки;
- **error** — ошибки и выше (critical);
- **warning** — предупреждения и выше. Предупреждения не говорят о наличии проблем в работе сервиса, однако это такие событтия, которые могут привести с ошибкам, поэтому не стоит их игнорировать;
- **notice** — уведомления и выше;
- **info** — информация;
- **debug** — отладка (подробный лог);
- **dynamic** — тот же debug.

Способ 2

Создайте каталог для логов:

```
mkdir /var/log/bind
```

В разделе **logging** задаются 2 параметра **channel** (можно и больше двух - на ваше усмотрение), эти параметры дословно можно назвать "канал" записи. Каждый канал определяет имя канала и настройки параметров записи (что записывать, а что - нет и куда писать).

Директива **category** задает какую категорию сообщений в какой канал отправлять.

Исходя из этого, мы имеем: запись стандартной информации в канал **misc**, а приходящие запросы посылаются в канал **query**. При этом, если файлы журнала достигают 4Мб (size 4m), он переименовывается добавлением к имени **.1** и начинается запись в новый журнал, числа в конце других журналов увеличиваются. Журналы с номером, более указанного в **version** (в нашем случае 4) удаляются.

Параметры **print*** определяют заносить ли в журнал время появления, важность и категорию информации. Более подробно про настройки раздела **logging** можно почитать в **man (5) named.conf**.

Добавьте конфигурацию логирования в файл **/etc/named.conf**:

```
// настройки логирования
logging {
        channel "misc" {
                file "/var/log/bind/misc.log" versions 4 size 4m;
                print-time yes;
                print-severity yes;
                print-category yes;
        };

        channel "query" {
                file "/var/log/bind/query.log" versions 4 size 4m;
                print-time yes;
                print-severity no;
                print-category no;
        };

        category default {
                "misc";
        };
```

```
        category queries {
                "query";
        };
};
```

Проверка работоспособности

Для проверки работоспособности и правильной конфигурации DNS-сервера, нужно сделать к нему несколько запросов. Для этого можно воспользоваться консольными утилитами **ping**, **dig** или **nslookup**.

ВАЖНО!

Клиент, на котором выполняются запросы должен быть настроен на использование вашего DNS сервера, подробнее смотрите в настройках сетевого адаптера.

Утилита **ping**, при указании доменного имени, резолвит его с помощью DNS. Если пинг к хосту, указанному в DNS, выполняется, то A запись данного хоста корректна.

С помощью **dig** или **nslookup** можно проверить обратные записи или иные специфические записи DNS-сервера. Например:

```
dig SRV _ldap._tcp.ad.test
```

Сделает запрос SRV-записи на сервере в домене **ad.test**. Должен вывести ip-адрес хоста с LDAP сервисом.

```
nslookup 192.168.10.50
```

Запрос должен вывести hostname для введенного **ip**. Тем самым проверив обратную (**PTR**) запись.

Настройка репликации DNS-сервера bind

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер минимальный
- **Версия bind:** bind-9.16.16

Предварительно необходимо ознакомиться и настроить DNS-сервер согласно нашей инструкции «**Настройка DNS-сервера bind**».

Подготовка master сервера

Открываем на редактирование конфигурационный файл bind:

```
nano /etc/named.conf
```

и редактируем следующее в блоке options:

```
allow-recursion { none; };
```

Находим и закомментируем строку

```
dnssec-validation yes;
```

Добавьте строки в блоки ваших локальных зон

```
allow-transfer { <ip адрес реплики>; };
allow-update { <ip адрес реплики>; };
notify yes;
```

Рассмотрим подробнее, то что мы написали:

- **allow-recursion { none; }** — Отключаем использование рекурсивных запросов т.к. это сильно снижает скорость работы, да и нее имеет смысла опрашивать вышестоящие DNS сервера по поводу зоны которую сами же и обслуживаем.
- **allow-transfer {<ip адрес реплики>;}** — разрешаем передачу данной зоны на остальные наши DNS сервера;
- **allow-update {<ip адрес реплики>;}** — разрешаем обновление;
- **notify yes** — включаем автоматическое уведомление подчиненных серверов об обновлении файла настроек DNS зоны.

Перезагрузите bind.

```
systemctl restart named
```

Настройка slave сервера.

Устанавливаем все обновления.

```
dnf update
```

Устанавливаем DNS-сервер следующей командой:

```
dnf install bind
```

Запускаем сервис и добавляем в автозапуск:

```
systemctl enable named --now
```

И проверяем, что он работает корректно:

```
systemctl status named
```

Открываем на редактирование конфигурационный файл bind:

```
nano /etc/named.conf
```

и редактируем следующее в блоке options:

```
listen-on port 53 { 127.0.0.1; <ip данного сервера>;};
listen-on-v6 port 53 { none; };
allow-query { any; };
forward first;
forwarders {8.8.8.8;};
allow-recursion { none; };
```

Находим и закомментируем строку

```
dnssec-validation yes;
```

добавляем туда запись, только на этот раз она будет немного отличаться:

```
zone "example.org" IN {
        type slave;
        file "/var/named/slaves/slave.example.org";
        masters { <ip адрес мастера>; };
        allow-transfer { "none"; };
};
```

Рассмотрим подробнее изменения:

- **type slave;** — тип зоны подчиненная
- **file /var/named/slaves/slave.example.org"** — путь к файлу с настройками, в этот раз в имени файла указано slave.example.org чтобы было понятно на каком сервере вы находитесь.
- **masters { <ip адрес мастера>; }** — IP адрес Мастер сервера, откуда будет производиться запрос файлов с настройками DNS зон.
- **allow-transfer {none;}** — Отключаем передачу зоны другим серверам, чтобы нельзя было получить все записи в домене

Впишите вышеописанные блоки для каждой зоны.

Перезагрузите DNS сервер.

```
systemctl restart named
```

Теперь должны появиться файлы DNS зон по пути, который указан.

ВАЖНО

Каждый раз, когда в настройки зоны на мастере вносятся изменения, к серийному номеру прибавляется единица, это делается для того чтобы подчиненные сервера увидели изменения в записях и приняли обновленный файл зоны, если после внесения изменений в файл, серийный номер остался прежним или уменьшился, то подчиненные DNS сервера НЕ станут подтягивать обновления считая что на мастер сервере изменений небыло!

Для редактирования серийного номера DNS зоны, откройте её файл и отредактируйте параметр serial.

Пример файла зоны:

```
...
@       IN      SOA     ns0.ipa.test. postmaster.ipa.test. (
                2018042804  ;serial
...
```

Это значение нужно увеличивать каждый раз при редактировании файла доменной зоны. Оно записано в формате YY-MM-DD + наращиваемый порядковый номер.

Для проверки работоспособности сервера с другого компьютера сети выполняем команду:

```
nslookup test.example.org <ip адрес реплики>
```

** данной командой мы пытаемся узнать IP-адреса сайта test.example.org через сервер репликации DNS.*

Должно получиться, примерно, следующее:

```
Server:      192.168.0.1
Address:     192.168.0.1#53
```

```
Name:        test.example.org
Address: 192.168.10.12
```

Настройка кеширования DNS с помощью dnsmasq

ВНИМАНИЕ

Для корректной установки и настройки dnsmasq, перейдите в сеанс суперпользователя:

```
sudo -i
```

или

```
su
```

На запрос пароля, введите пароль привилегированного пользователя или локального администратора.

DNS - кэш предназначен для ускорения загрузки страниц веб-сайтов, путем сохранения в памяти их IP-адресов. Для настройки кэширования используйте утилиту **dnsmasq**.

```
dnf install dnsmasq
```

С помощью текстового редактора vi или nano откройте файл, расположенный по адресу **/etc/dnsmasq.conf**

```
vi /etc/dnsmasq.conf
```

или

```
nano /etc/dnsmasq.conf
```

Отредактируйте следующие параметры:

```
resolv-file=/etc/resolv.dnsmasq
no-poll
listen-address=127.0.0.1
cache-size=150
conf-dir=/etc/dnsmasq.d,.rpmnew,.rpmsave,.rpmorig
```

А так же допишите следующий параметр:

```
all-servers
```

Где:

- **resolv-file** — файл с IP-адресами dns - серверов
- **no-poll** — параметр, запрещающий автоматическое применение изменений в файлах с именем resolv.
- **listen-address** — параметр, указывающий какой адрес слушать.
- **cache-size** — размер кэша. Значение по умолчанию позволяет хранить 150 хостов.
- **conf-dir** — параметр, отвечающий за дополнительный файл конфигурации.
- **all-servers** — перенаправляет dns-запрос всем доступным dns-серверам и возвращает ответ от первого откликнувшегося сервера. Параметр нужно записать вручную.

Также можно указать следующие параметры:

- **no-negcache** — не кэшировать негативные ответы от серверов.
- **bind-interfaces** — позволяет запускать копии процесса.
- **dns-forward-max** — максимальное количество dns-запросов. По умолчанию — 150. Параметр нужно записать вручную.

Теперь создайте файл **resolv.dnsmasq** с помощью текстового редактора **vi** или **nano** и запишите туда адреса dns-серверов.

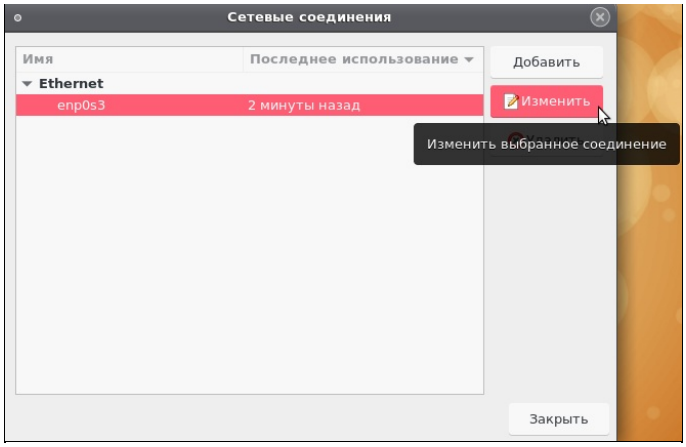
```
vi /etc/resolv.dnsmasq
```

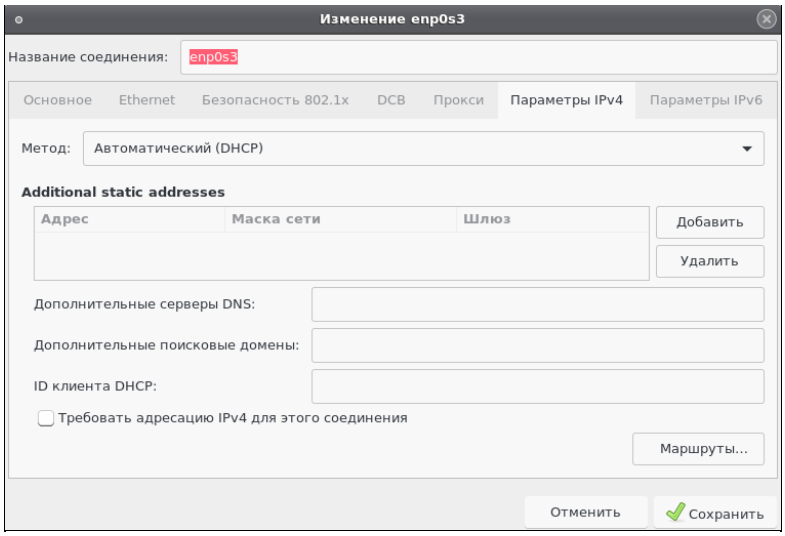
или

```
nano /etc/resolv.dnsmasq
```

Потом добавьте IP-адрес **127.0.0.1** в файл **resolv.conf**. Для этого, используйте утилиту **«Сетевые соединения»**, расположенную в **«Меню» → «Параметры» → «Сетевые соединения»** в графическом окружении **Cinnamon** или **«Система» → «Параметры» →**

«Сетевые соединения» в графическом окружении **Mate**. Выберите ваше активное подключение, нажмите кнопку **«Изменить»,** перейдите на вкладку **«Параметры IPv4»**, поменяйте **«Метод»** на **«Автоматический (DHCP, только адрес)»**, а в поле "**Дополнительные серверы DNS**" напишите адрес **127.0.0.1**, нажмите применить и перезапустите **NetworkManager.**





Редактирование файла resolv.conf с помощью текстовых редакторов не рекомендуется. Файл перезапишется со следующим перезапуском системы.

```
systemctl restart NetworkManager.service
```

Чтобы убедиться, что изменения вступили в силу, посмотрите содержимое файла **resolv.conf**:

```
cat /etc/resolv.conf
```

Содержимое должно быть таким:

```
# Generated by NetworkManager

nameserver 127.0.0.1
```

Описанные выше операции позволят перенаправлять все dns-запросы на локальную машину.

Добавьте службу **dnsmasq** в автозапуск и перезайдите в сеанс:

```
systemctl enable dnsmasq.service --now
```

Для того, чтобы сбросить кэш, просто перезапустите службу:

```
systemctl restart dnsmasq.service
```

Проверка работоспособности

Проверьте, включена ли служба:

```
systemctl status dnsmasq.service
```

Проверьте порт 53:

```
netstat -ntlp | grep :53
```

```
tcp  0  0 0.0.0.0:53  0.0.0.0:*  LISTEN 7319/dnsmasq
tcp6 0  0 :::53   :::*   LISTEN 7319/dnsmasq
```

Теперь попробуйте с помощью утилиты dig несколько раз обратиться к сайту **google.com**

```
dig google.com | grep "Query time"
```

```
;; Query time: 135 msec
```

Если кэширование dns-запросов работает, то практически во всех следующих запросах выделенная строчка **query time** будет равна нулю.

```
;; Query time: 0 msec
```

В противном случае она будет варьироваться от 0 и выше с каждым новым запросом.

В результате, основной DNS-сервер сети будет испытывать гораздо меньше нагрузки.

Настройка локального кеширующего DNS-сервера systemd-resolved

Предварительная подготовка
Настройка файла конфигурации
Режим совместимости
Откат к старому методу разрешения имен

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: systemd-251.13-2

systemd-resolved представляет собой небольшой локальный кеширующий DNS-сервер. Основной задачей кеширующего DNS-сервера является обработка DNS-запросов, которые выполняет во время своей работы операционная система, и сохранение их в памяти (кеширование).

systemd-resolved поддерживает такие стандарты, как **DNSSEC** и **DNSoverTLS** (или DoT), которые увеличивают безопасность при работе в сети Интернет.

systemd-resolved входит в состав пакета **systemd**, который установлен в РЕД ОС по умолчанию.

Предварительная подготовка

Для настройки службы **systemd-resolved** используется конфигурационный файл **/etc/systemd/resolved.conf**.

Для проверки DNS-серверов, используемых **systemd-resolved** в данный момент, выполните команду:

```
resolvectl status
```

В ответе команды должно отображаться примерно следующее:

```
Global
       Protocols: LLMNR=resolve -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (enp0s3)
    Current Scopes: DNS LLMNR/IPv4 LLMNR/IPv6
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 192.168.0.1
       DNS Servers: 192.168.0.1 192.168.0.251
        DNS Domain: example.com
```

По умолчанию **systemd-resolved** считывает стандартные настройки **DNS** в сети.

Дополнительно рекомендуется проверить параметр `hosts` в файле **/etc/nsswitch.conf**, который определяет последовательность обращений программ к системным компонентам для разрешения доменных имен. В параметре **hosts** должен быть указан **resolve**:

```
hosts: files myhostname resolve [!UNAVAIL=return] dns
```

где:

- `files` – считывание настроек из файла **/etc/hosts** (имеет наивысший приоритет);
- `myhostname` – считывание имени текущего хоста;
- `resolve [!UNAVAIL=return]` – считывание настроек с помощью локального кеширующего DNS-сервера, **systemd-resolved** поддерживает внутренний каталог с собственным файлом **resolv.conf**;
- `dns` – обращение напрямую к DNS-серверам (имеет низший приоритет).

Настройка файла конфигурации

Для настройки **DNS**, к которым необходимо обращаться для преобразования доменных имен, в файл **/etc/systemd/resolved.conf**

потребуется внести следующие изменения:

```
nano /etc/systemd/resolved.conf
```

- Указать список основных и запасных **DNS**. Для этого раскомментируйте параметры `DNS=` и `FallbackDNS=` и укажите свои значения.

  В параметре `DNS=` рекомендуется указывать IP-адрес главного маршрутизатора в локальной сети.

  В параметре `FallbackDNS=` рекомендуется указывать любые публичные DNS-серверы, например, `77.88.8.88` – бесплатный DNS-сервер от Яндекс.

- При необходимости раскомментируйте и укажите нужные значения для следующих параметров:

  - `DNSSEC=yes` – набор расширений протокола **DNS**, позволяющий минимизировать атаки, связанные с подменой IP-адреса при разрешении доменных имён;
  - `DNSOverTLS=yes` – стандартный протокол для выполнения разрешения удалённой системы **DNS** с использованием **TLS**;
  - `MulticastDNS=no` – многоадресный **DNS** для поиска устройства или службы по имени в локальной сети;
  - `LLMNR=no` – протокол стека **TCP/IP**, выполняющий разрешение имён хостов в локальной сети.

- Включите кеширование, раскомментировав параметр `Cache=` и установив значение `yes`.

После настройки конфигурационного файла выполните перезапуск службы **systemd-resolved** и проверьте её статус:

```
systemctl restart systemd-resolved
systemctl status systemd-resolved
```

В случае если по каким-либо причинам в вашей системе **systemd-resolved** не запущен, при проверке статуса будет отображаться следующее сообщение:

```
Failed to get global data: The name is not activatable
```

Для решения данной проблемы запустите и добавьте службу **systemd-resolved.service** в автозагрузку с помощью команды:

```
systemctl enable systemd-resolved.service --now
```

Режим совместимости

Для совместимости с приложениями, которые не используют библиотечные вызовы, а обращаются к DNS-серверам напрямую, получая их из **/etc/resolv.conf**, потребуется наличие символической ссылки на файл **resolv.conf**, содержимое которого автоматически генерируется, исходя из настроек, заданных в **/etc/systemd/resolved.conf**.

В РЕД ОС 8 в конфигурации **systemd-resolved** по умолчанию реальный файл **/etc/resolv.conf** заменен на ссылку к автоматически генерируемому файлу **/run/systemd/resolve/stub-resolv.conf**.

Для проверки символической ссылки выполните:

```
ls -la /etc/resolv.conf

lrwxrwxrwx. 1 root root 39 апр 15 08:34 /etc/resolv.conf -> ../run/systemd/resolve/stub-resolv.conf
```

Файл **/run/systemd/resolve/stub-resolv.conf** содержит в себе отсылку на локальный псевдо-сервер DNS (local stub) на адресе **127.0.0.53** в качестве единственного DNS-сервера, а также список доменов для поиска (параметр `search`).

Отсылка на локальный псевдо-сервер DNS связана с тем, что в конфигурации по умолчанию в **/etc/systemd/resolved.conf** активирован механизм **DNSStubListener** (`DNSStubListener=yes`), который запускает отдельные TCP/UDP-прослушиватели на адресах `127.0.0.53%lo:53` и `127.0.0.54:53`:

```
ss -tunlp | sort

tcp   LISTEN 0      4096   127.0.0.53%lo:53       0.0.0.0:*    users:(("systemd-resolve",pid=531,fd=17))
tcp   LISTEN 0      4096      127.0.0.54:53       0.0.0.0:*    users:(("systemd-resolve",pid=531,fd=19))
```

Согласно справке по **systemd-resolved.service** такой режим работы является рекомендуемым для **systemd-resolved**, так как позволяет пропустить весь поток DNS-запросов от всех типов локальных приложений через внутренний кеширующий DNS-сервер **systemd-resolved**.

Откат к старому методу разрешения имен

Для того чтобы вернуться с старому методу разрешения имён необходимо:

1. Отключить сервис **systemd-resolved**:

```
systemctl disable systemd-resolved --now
```

2. Удалить **/etc/resolv.conf** и создать его как обычный файл:

```
rm /etc/resolv.conf && touch /etc/resolv.conf
```

3. Прописать в файл все необходимые DNS-сервера, например:

```
nameserver 8.8.8.8
nameserver 77.88.8.8
```

Расширенная настройка DNS-сервера

Настройка stub-зоны на сервере bind
Зоны пересылки
Русскоязычные имена
Использование DNSSEC

Настройка stub-зоны на сервере bind

Примечание.

Данная настройка требует указания правильной цепочки доверенностей DNS серверов. Если у вас её нет, впишите следующие параметры в файл:

```
dnssec-enable no;
dnssec-validation no;
```

Static-stub позволяет указать конкретные **IP**, по которым следует обращаться для преобразования имен (**resolving**) заданных зон в обход обслуживающих данные зоны DNS-серверов.

Откройте конфигурационный файл **bind**:

```
nano /etc/named.conf
```

Настройте зону следующим образом:

```
zone "stub.test" {
type static-stub;
server-addresses { 192.168.0.1; 192.168.0.50; };
};
```

* где:

- **stub.test** — домен, для которого нужно делать перенаправление запросов;
- **192.168.0.1, 192.168.0.50** — адреса DNS-серверов, на которые перенаправлятся запросы.

Перезапустите **bind**, чтобы применить настройки:

```
systemctl restart named
```

Зоны пересылки

Примечание.

Данная настройка требует указания правильной цепочки доверенностей DNS серверов. Если у вас её нет, впишите следующие параметры в файл:

```
dnssec-enable no;
dnssec-validation no;
```

Задачу перенаправления DNS-запросов можно решить с помощью зоны типа **forward**. Настройка выполняется следующим образом:

```
zone "stub.test" {
type forward;
forwarders { 192.168.0.1; 192.168.0.30; };
};
```

Перезагрузить сервис:

```
systemctl restart named
```

Русскоязычные имена

Для записи русскоязычных имен хостов или доменов нужно узнать, как доменное имя выглядит в **Punycode**-представлении. Например, с помощью сервиса 2ip. Далее необходимо вписать имя в **punycode**-представлении в файл зоны, например:

```
xn----gtbc2bgjip    IN    A    10.81.200.222
```

Использование DNSSEC

DNSSEC описана в стандарте **RFC 4033**.

Создайте отдельный каталог для файлов с ключами:

```
mkdir -p /var/named/keys
cd /var/named/keys
```

Обычно генерируется большое количество файлов, поэтому для каждой зоны можно создать отдельную директорию с ключами.

Для работы **DNSSEC** требуется создать **master**-ключ (*KSK, Key Signing Key*), который будет использован для создания цифровых подписей для других ключей, и ключи для каждой из локальных зон (*ZSK, Zone Signing Key*).

Создайте KSK-ключ:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -n ZONE example.net

Generating key pair.....+++.....+++
Kexample.net.+005+38287
```

Создайте ZSK-ключ:

```
dnssec-keygen -a RSASHA1 -b 2048 -n ZONE example.net

Generating key pair.....+++ ..+++
Kexample.net.+005+55896
```

Для того чтобы ключи были сгенерированы, необходима рандомная составляющая. Для этого нужно перемещать указатель мыши несколько раз при генерации ключей либо выполнять команды генерации с дополнительным параметром -r /dev/urandom, например:

```
dnssec-keygen -f KSK -a RSASHA1 -b 2048 -r /dev/urandom -n ZONE example.net
```

Установите на ключи права доступа *только для чтения* процессу **named**:

```
chown named. *
```

Включите в настройках **named.conf** запись лога **DNSSEC** для упрощения анализа возможных проблем.

Подготовьте директорию для хранения лога:

```
mkdir -p /var/log/bind/
chown named. /var/log/bind/
```

В **named.conf** пропишите путь к логу, который будет ограничен максимальным размером в **20 Мб**:

```
logging {
channel dnssec_log {
```

```
file "/var/log/bind/dnssec.log" size 20m;
print-time yes;
print-category yes;
print-severity yes;
severity debug 3;
};
category dnssec {
dnssec_log;
};
};
```

Отредактируйте секцию **options**:

```
options {

...
key-directory "/var/named/keys";
sig-validity-interval 20 10;
};
```

* где:

- **key-directory** — каталог для хранения сгенерированных ключей (необходимо указать тот каталог, в котором были сформированы последние ключи командой dnssec-keygen);
- **sig-validity-interval** — период действия ключей: дней/период обновления.

Для зоны редактируем:

```
zone "example.net" {
type master;
file "master/example.net";
key-directory "keys/";
inline-signing yes;
auto-dnssec maintain;
};
```

Опция inline-signing yes включает режим прозрачного формирования подписей, не требуя внесения изменений непосредственно в файл зоны. При работе inline-signing вручную поддерживаемый файл с зоной преобразуется в динамическую зону, для которой создаётся цифровая подпись. Из-за этого выдаваемый сервером серийный номер отличается от серийного номера, прописанного в файле с зоной. Изменения **DNSSEC** производятся в **jnl**-файле с журналом изменений.

Проверьте, что у пользователя **named/bind** есть права на запись в каталог хранения зоны. При необходимости, можно изменить владельца, например:

```
chown -R named:named /var/named/master
```

Откройте на редактирование файл зоны и измените серийный номер.

Перезапустите **bind**:

```
systemctl restart named
```

После перезапуска **named** в директории **/var/named/keys** появятся следующие файлы:

- example.net;
- example.net.jbk;
- example.net.signed;
- example.net.jnl.

При запросе параметров зоны можно заметить появление нового поля **RRSIG**.

```
dig example.net +dnssec
```

```
...
example.net. 600 IN A 1.2.3.4
example.net. 600 IN RRSIG A 5 3 600 2012021356423 20120415331566 21695 net. IKeklJa314313G/xZpQ+B2313eqaDceR/VNcdsdasxV2 ...
```

Так как **DNSSEC** основан на обеспечении цепочки доверия, чтобы процесс верификации заработал, требуется, чтобы регистратор заверил созданный KSK-ключ, подтвердив своё доверие. Для этого создайте на основе KSK-ключа **DSKEY**-ключ (Delegation Signature Key)

```
dnssec-dsfromkey Kexample.net.+005+38287

example.net. IN DS 38287 5 1 E8C01C9CA1252389A9CB4E
example.net. IN DS 38287 5 2 57EC936A479A94C3232412313423452349235 9A623 39712D53
```

Скопируйте две сгенерированные строки в интерфейсе ввода **DSKEY** на сайте регистратора домена. Верификация заработает после того, как регистратор обновит параметры первичной зоны.

Для поддержки **DNSSEC**-проверки на стороне резолвера следует добавить в настройки **named.conf**:

```
options {
...
dnssec-enable yes;
dnssec-validation auto;
...
};
```

Проверка работоспособности DNS с помощью nslookup

Синтаксис утилиты
Примеры использования утилиты
Получение IP-адреса
Обратное преобразование
Запись NS
Запись MX

nslookup – утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе **DNS**. Позволяет задавать различные типы запросов и опрашивать произвольно указываемые серверы для проверки работоспособности **DNS**, просмотра IP-адреса сервера, скорости его работы и т.д.

С помощью данной утилиты также можно не только получить IP-адрес по доменному имени, но и выполнить обратное преобразование, а также проверить необходимые записи **DNS**.

По умолчанию утилита **nslookup** предустановлена в РЕД ОС.

Синтаксис утилиты

Синтаксис утилиты имеет следующий вид:

```
nslookup [-опции] [домен] [сервер]
```

Основные опции **nslookup**:

- **-type** – тип информации, которую требуется получить, возможные типы: *txt*, *soa*, *ptr*, *ns*, *mx*, *mr*, *minfo*, *mg*, *mb*, *hinfo*, *gid*, *cname*, *a*, *any*;
- **-port** – использовать другой порт DNS-сервера (порт по умолчанию **53**);
- **-recurse** – рекурсивный запрос (информация запрашивается у других серверов, если она недоступна или отсутствует на указанном сервере);
- **-retry** – количество попыток опроса сервера;
- **-timeout** – время ожидания ответа от сервера (в секундах);
- **-fail** – опросить другой сервер имен, если указанный вернул ошибку.

Примеры использования утилиты

Получение IP-адреса

Для определения IP-адреса сервера по его доменному имени необходимо выполнить команду вида:

```
nslookup <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
Name: ya.ru
Address: 77.88.55.242
Name: ya.ru
Address: 5.255.255.242
Name: ya.ru
Address: 2a02:6b8::2:242
```

В строке **Server** выводится IP-адрес сервера, в строке **Address** – IP-адрес сервера и порт, с которого был отправлен запрос к **ya.ru**.

Далее отображается информация о запросе. В строке **Name** выводится доменное имя сервера, на который был отправлен запрос. В строке **Address** выводится IP-адрес, который принадлежит доменному имени сервера. Из примера видно, что доменному имени может

принадлежать несколько IP-адресов.

Обратное преобразование

Также с помощью утилиты **nslookup** может быть выполнено обратное преобразование IP-адреса в доменное имя. Для этого используется команда вида:

```
nslookup <IP-адрес>
```

Пример команды и ее вывода:

```
nslookup 77.88.55.242

242.55.88.77.in-addr.arpa name = ya.ru.

Authoritative answers can be found from:
55.88.77.in-addr.apra nameserver = ns3.yandex.ru.
55.88.77.in-addr.apra nameserver = ns4.yandex.ru.
ns3.yandex.ru internet address = 87.250.250.1
ns3.yandex.ru has AAAA address = 2a02:6b8::1001
ns4.yandex.ru internet address = 77.88.21.1
ns4.yandex.ru has AAAA address = 2a02:6b8:0:1::1:1
```

Запись NS

Первоисточником информации о домене являются его **NS**-серверы. Получить их можно, используя опцию `-type=ns` в команде следующего вида:

```
nslookup -type=ns <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=ns ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru nameserver = ns2.yandex.ru.
ya.ru nameserver = ns1.yandex.ru.

Authoritative answers can be found from:
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

Команда выведет список используемых серверов имен, в приведенном примере это **ns1.yandex.ru**.

Запись MX

Также можно получить **MX**-запись для домена, установив тип запроса **mx** в команде следующего вида:

```
nslookup -type=mx <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=mx ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru mail exchanger = 10 mx.yandex.ru.
```

```
Authoritative answers can be found from:
ya.ru nameserver = ns1.yandex.ru.
ya.ru nameserver = ns2.yandex.ru.
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

В выводе команды будут отображены все настроенные почтовые серверы, у каждого сервера есть свой приоритет – 15, 10 или 5. Чем меньше число, тем выше приоритет адреса. В приведенном примере почтовый сервер – **mx.yandex.ru** имеет приоритет **10**.

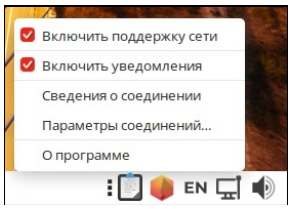
Настройка сетевого адаптера

Настройка сети в графическом сеансе
Настройка сети в терминале
Изменение конфигурационного файла текстовым редактором
Использование интерфейса nmtui
Изменение через утилиту nmcli

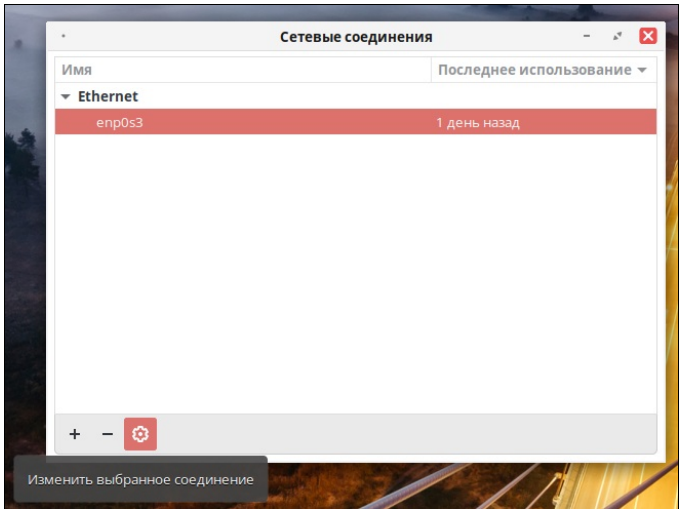
Настройку сетевого адаптера можно осуществить, используя графический интерфейс, либо через терминал.

Настройка сети в графическом сеансе

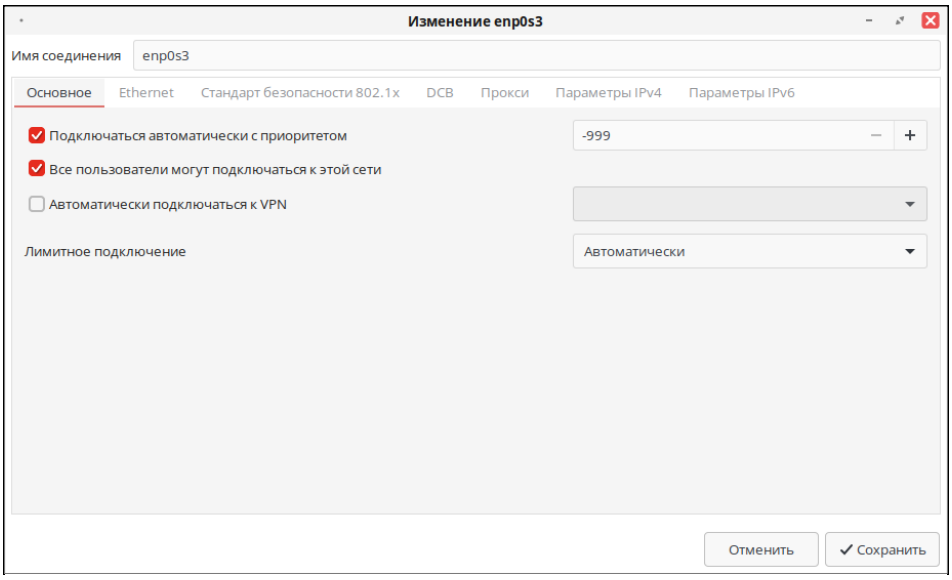
Настройка сети в РЕД ОС производится с помощью программы **NetworkManager**. Для ручной настройки сетевого адаптера необходимо в системном трее ПКМ вызвать контекстное меню, нажав на иконку сетевых соединений. В контекстном меню выберите пункт «**Параметры соединений...**».



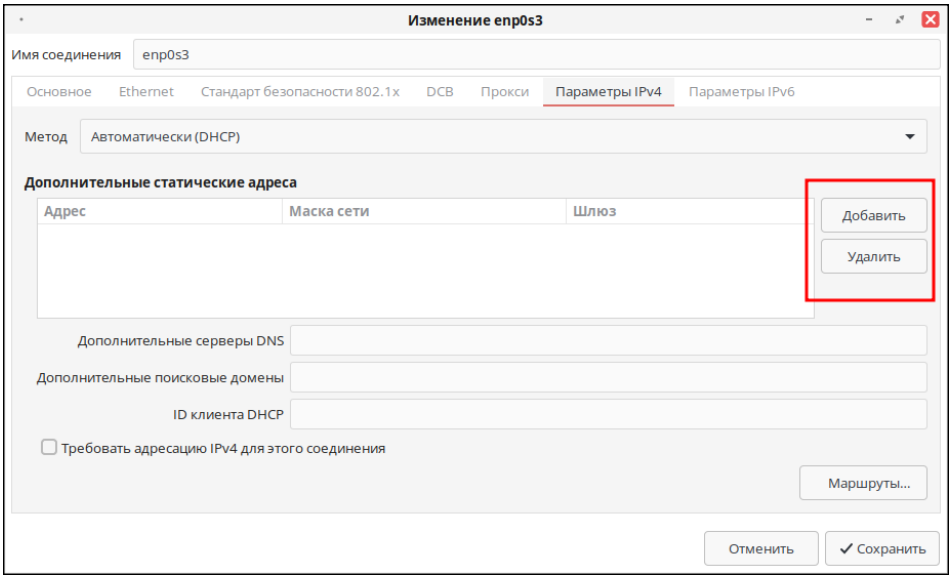
В открывшемся окне «**Сетевые соединения**» необходимо выбрать нужный сетевой адаптер и нажать кнопку «**Изменить выбранное соединение**».



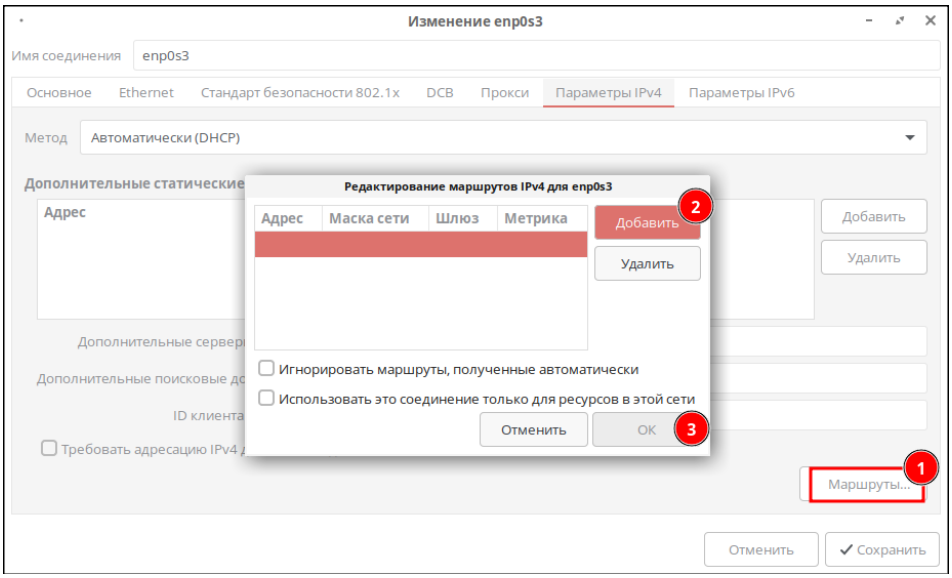
В открывшемся окне свойств сетевого адаптера на вкладке «**Основное**» можно установить свойства автоматического подключения - «**Подключаться автоматически с приоритетом**» и «**Все пользователи могут подключаться к этой сети**».



На вкладке «**Параметры IPv4**» можно задать вручную параметры сетевого подключения, нажав кнопку « **Добавить**».



Для добавления новых маршрутов необходимо нажать на кнопку «**Маршруты...**». В открывшемся диалоговом окне нажмите «**Добавить**», задайте необходимые параметры и нажмите « **OK**».



Для подтверждения изменений, внесенных в настройки сетевого адаптера, нажмите «**Сохранить**».

Настройка сети в терминале (консоли)

Для настройки сети в терминале можно использовать 3 варианта:

1. **Изменение конфигурационного файла текстовым редактором**
2. **Использование интерфейса nmtui**
3. **Изменение через утилиту nmcli**

Изменение конфигурационного файла текстовым редактором

Вы можете подробнее ознакомиться с информацией по настройке сети, просмотрев наши обучающие видео:

- на **RuTube**:
  - Сеть в РЕД ОС. Основы. Утилита ip;
  - Сеть в РЕД ОС. NetworkManager CLI.
- в **Яндекс.Дзен**:
  - Сеть в РЕД ОС. Основы. Утилита ip;
  - Сеть в РЕД ОС. NetworkManager CLI.

- в **VK Видео**:
    - Сеть в РЕД ОС. Основы. Утилита ip;
    - Сеть в РЕД ОС. NetworkManager CLI.

На наших каналах вы также сможете найти много другой полезной информации.

Для просмотра сетевых настроек выполните команду:

```
ifconfig
```

или воспользуйтесь утилитой `ip` с параметром `addr`:

```
ip addr
```

Тут можно увидеть параметры и название сетевой карты.

```
ip addr

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether be:cd:c8:c8:7a:60 brd ff:ff:ff:ff:ff:ff
inet 10.10.10.83/24 brd 10.10.10.255 scope global dynamic noprefixroute enp0s3
valid_lft 435sec preferred_lft 435sec
inet6 fe80::f42e:4ae5:4dc0:ff68/64 scope link noprefixroute
valid_lft forever preferred_lft forever+
```

По умолчанию сетевой адаптер настроен для получения IP-адреса по **DHCP**. Настройки хранятся в файле **/etc/NetworkManager/system-connections/<имя_сетевого_интерфейса>.nmconnection**. Именуются они, например, как **enp0s3** или **enp0s4**.

В данном примере сетевой интерфейс имеет имя **enp0s3**. Используя команду `cat`, можно посмотреть содержимое файла настроек:

```
cat /etc/NetworkManager/system-connections/enp0s3.nmconnection

[connection]
id=enp0s3
uuid=97def639-603a-4167-9613-edd5bd902ef8
type=ethernet
interface-name=enp0s3
timestamp=1704763284

[ethernet]

[ipv4]
method=auto

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

Для редактирования файла настроек можно использовать любой текстовый редактор (например **mcedit** или **vi**).

Для установки статического IP-адреса необходимо для параметра `method` указать значение `manual` в секции **[ipv4]**:

```
method=manual
```

Далее следует указать собственные конфигурации:

- Игнорировать **DNS** из **DHCP**:

```
ignore-auto-dns=true
```

- Указать статический **DNS**:

```
dns=8.8.8.8;
```

- Указать **IP**, **маску** и **шлюз** по умолчанию:

```
address1=192.168.1.100/24,192.168.1.1
```

Для немедленного применения изменений перезапустите сеть:

```
systemctl restart NetworkManager
```

Таким образом, при статической настройке IP-адреса, секция **[ipv4]** будет иметь следующий вид:

```
[ipv4]
address1=192.168.1.100/24,192.168.1.1
dns=8.8.8.8;
ignore-auto-dns=true
method= manual
```

В файле настройки сетевой карты можно добавить столько DNS-серверов, сколько требуется. Например:

```
dns=8.8.8.8;8.8.4.4;192.168.1.1;
```

ВАЖНО!

В работе используются максимум 3 DNS-сервера (те, что указаны первыми).

Проверить шлюз, по умолчанию установленный в системе, можно с помощью команды:

```
netstat -nr

Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 172.16.0.1 0.0.0.0 UG 0 0 0 eno16777736
172.16.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eno16777736
```

Строка `Destination 0.0.0.0` определяет адрес шлюза. Если у вас ее нет, возможно, что для параметра `Gateway` установлен неверный шлюз, это можно исправить. Установите шлюз по умолчанию:

```
route add default gw 172.16.0.1
```

Если вы не сменили при установке ОС имя сервера или вы хотите его изменить, то сделать это можно следующим образом. Сначала проверьте, какое имя сервера (`hostname`) у вас установлено:

```
hostname
```

В примере имя сервера будет изменено на `server.work` с помощью команды:

```
hostnamectl set-hostname server.work
```

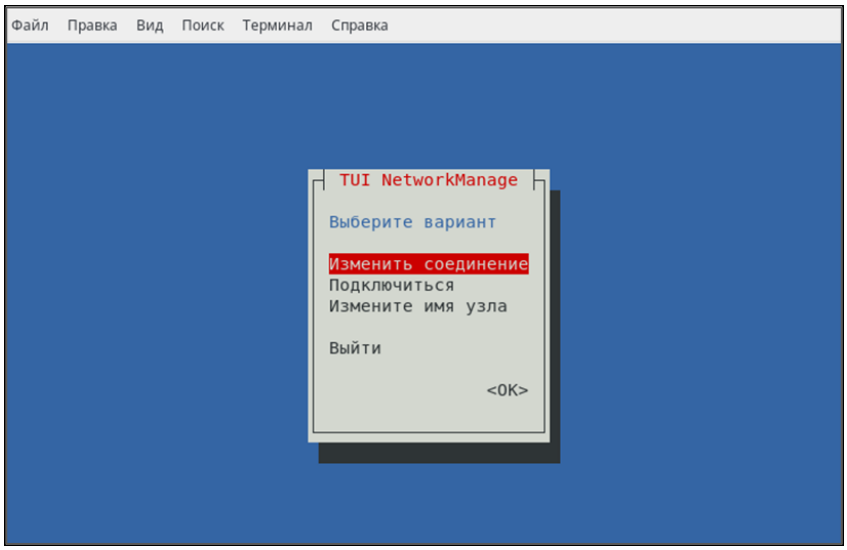
Для смены имени ПК перезагрузка не требуется.

Использование интерфейса nmtui

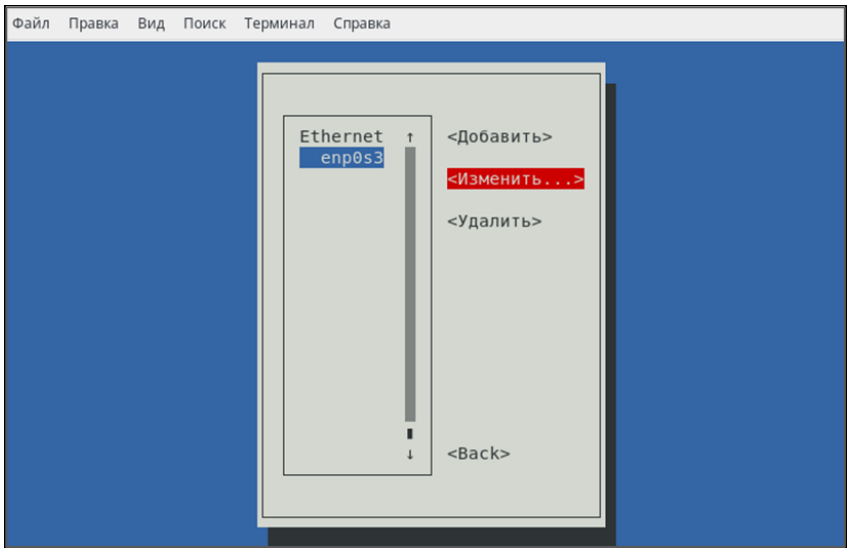
nmtui - утилита для настройки сети с интуитивно-понятным графическим интерфейсом, для ее запуска в терминале необходимо выполнить:

```
nmtui
```

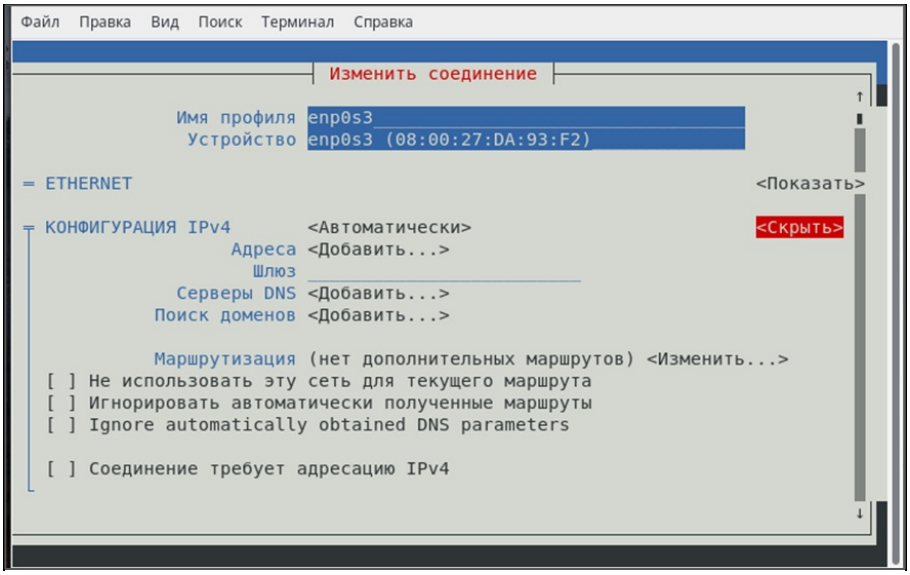
Выберите «Изменить соединение» клавишей **Enter**.



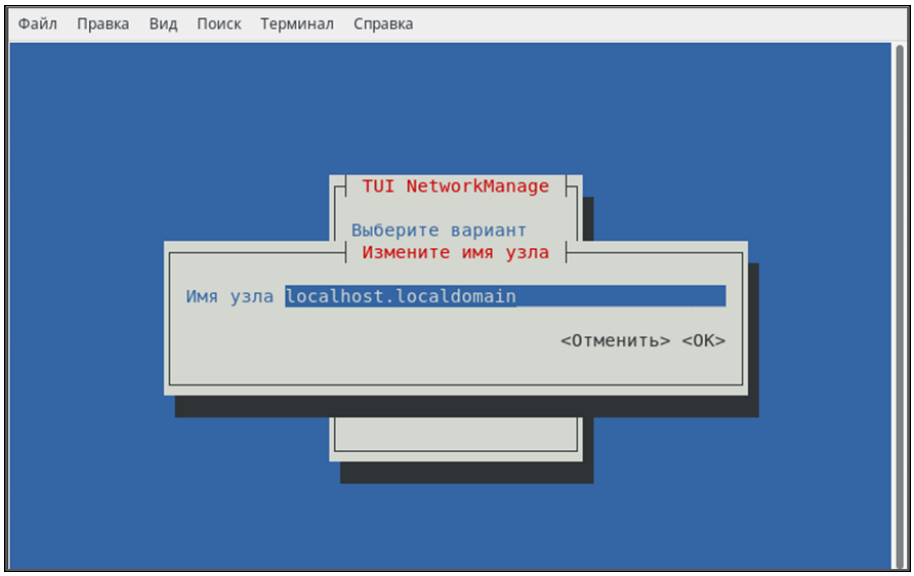
Выберите необходимый интерфейс и нажмите «Изменить...».



Определите список изменений.



Для изменения имени узла выберите «Измените имя узла». Введите новое имя и нажмите «OK».



Изменение через утилиту nmcli

nmcli - это инструмент командной строки для управления **NetworkManager** и создания отчетов о состоянии сети. Используется для создания, отображения, редактирования, удаления, активации и деактивации сетевых подключений, а также для контроля и отображения состояния сетевых устройств.

Чтобы узнать название интерфейса введите в командной строке:

```
nmcli con
```

В нашем случае интерфейс будет называться **eth0**.

```
nmcli con

NAME UUID TYPE DEVICE
eth0 3a2830fe-b8dd-45bd-b33e-387db796c8da ethernet eth0
```

Для того чтобы указать, что настройки должны быть получены от **DHCP**, используется команда:

```
nmcli con modify eth0 ipv4.method auto
```

Для использования ручных настроек необходимо ввести:

```
nmcli con modify eth0 ipv4.method static
```

Для того, чтобы указать статический адрес, используется команда:

```
nmcli con modify eth0 ipv4.address 192.168.0.1/24
```

Для того чтобы указать **dns**, используется команда:

```
nmcli connection modify eth0 ipv4.dns 202.131.124.4
```

Для того чтобы указать шлюз, используется команда:

```
nmcli connection modify eth0 IPv4.gateway 192.168.0.1
```

Чтобы настроить статический маршрут для существующего соединения **Ethernet**, используется команда:

```
nmcli connection modify eth0 +ipv4.routes "192.168.122.0/24 10.10.10.1"
```

Для остановки сетевой службы и её запуска доступны команды `nmcli networking off` и `nmcli networking on`.

Любое внесенное изменение также требует перезагрузки интерфейса для его применения.

Настройка сетевых соединений с помощью networkctl

Установка
Синтаксис
Опции
Команды
Запуск службы systemd-networkd
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: systemd-249.17-1, systemd-251.20-1

Networkctl — это инструмент для управления сетевыми устройствами и конфигурациями. Он позволяет пользователям получать информацию о состоянии сетевых интерфейсов и их конфигурации.

Установка

Для установки systemd-networkd выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install systemd-networkd
```

Запуск службы systemd-networkd

Для обеспечения корректной работы **networkctl** служба **systemd-networkd** должна быть запущена. Для запуска службы и добавления ее в автозагрузку выполните:

```
sudo systemctl enable systemd-networkd --now
```

Дальнейшая работа в программе производится с правами непривилегированного пользователя.

Проверить статус службы:

```
systemctl status systemd-networkd
```

Синтаксис

Утилита доступна для запуска через терминал с использованием команды следующего формата:

```
networkctl [<опции>] [<команды>]
```

Опции

Основные опции утилиты:

- **-h, --help** — вывод справки по использованию утилиты;
- **--version** — вывод версии утилиты;
- **--no-pager** — отключение постраничного вывода данных;
- **--no-legend** — отключение вывода условных обозначений;
- **-a, --all** — отображение всех интерфейсов, включая те, которые неактивны;
- **-s --stats** — показ статистики сетевых интерфейсов;
- **-l --full** — вывод подробной информации;

- **-n, --lines=[<число>]** — указание количества строк для отображения в журнале;
- **--json=pretty|short|off** — вывод информации в формате JSON.
  Возможные значения:
    - **pretty** — форматированный вывод;
    - **short** — сокращённый вывод;
    - **off** — отключение вывода в формате JSON.

Команды

Основные команды утилиты:

- **list [<шаблон>]** — отображает список сетевых интерфейсов и их статус;
- **status[<шаблон>]** — показывает статус сетевых каналов;
- **lldp [<шаблон>]** — отображает обнаруженных соседей по протоколу LLDP (Link Layer Discovery Protocol);
- **label** — отображает цифровые метки адресов, которые можно использовать для выбора адреса;
- **delete [<устройство>]** — удаляет виртуальные сетевые устройства;
- **up [<устройство>]** — активирует (поднимает) сетевое устройство;
- **down [<устройство>]** — выводит сетевое устройство из строя (отключает);
- **renew [<устройство>]** — обновляет динамические конфигурации устройства;
- **forcerenew [<устройство>]** — инициирует принудительную реконфигурацию устройства;
- **reconfigure [<устройство>]** — перенастраивает сетевые интерфейсы;
- **reload** — перезагружает файлы **.network** и **.netdev**, используется для применения изменений в конфигурации сети.

Примеры использования

Примечание.

Перед запуском **networkctl** убедитесь, что служба **systemd-networkd** запущена, в противном случае вы получите неполный вывод, о чем свидетельствует следующая ошибка:

```
WARNING: systemd-networkd is not running, output will be incomplete.
```

1. Отображение списка доступных сетевых соединений и их текущего состояния:

```
networkctl list
```

Команда **networkctl list** используется для отображения списка всех сетевых соединений и их соответствующих свойств, включая индекс интерфейса, состояние, тип, аппаратный адрес, драйвер и рабочее состояние.

Пример вывода:

```
IDX   LINK         TYPE           OPERATIONAL     SETUP
1     lo           loopback       carrier         unmanaged
2     enp0s3       ether          routable        unmanaged

2 links listed.
```

где:

- **IDX** — индекс сетевого интерфейса,
- **LINK** — название сетевого интерфейса,
- **TYPE** — тип сетевого интерфейса.
  Возможные значения:
    - **loopback** — интерфейс для обратной связи,
    - **ether** — Ethernet-интерфейс.
- **OPERATIONAL** — текущее рабочее состояние.
  Возможные значения:
    - **missing** — устройство отсутствует;

    - **off** — питание устройства отключено;
    - **no-carrier** — устройство включено, но ещё не подключено к оператору связи;
    - **dormant** — устройство подключено к оператору связи, но ещё не готово для передачи данных;
    - **degraded-carrier** — у главного интерфейса нет адреса, один из подчинённых сетевых устройств соединения или моста отключен;
    - **carrier** — все сетевые интерфейсы подчинены основному интерфейсу или мосту, связь установлена;
    - **degraded** — не все подчиненные сетевые интерфейсы подключены к оператору связи;
    - **enslaved** — интерфейс привязан к основному сетевому интерфейсу или мосту;
    - **routable** — интерфейс настроен и имеет главный или маршрутизируемый IP-адрес.

- **SETUP** — состояние настройки сетевого канала.
  Возможные значения:

    - **pending** — ссылка находится в процессе обработки;
    - **initialized** — ссылка успешно обработана;
    - **configuring** — ссылка настраивается;
    - **configured** — ссылка успешно настроена;
    - **unmanaged** — systemd-networkd не управляет этим интерфейсом;
    - **failed** — не удалось настроить ссылку;
    - **linger** — ссылка удалена, но ещё не удалена пользователем systemd-networkd.

2. Отображение общего состояния определённого сетевого канала:

```
networkctl status enp0s3
```

где:

- enp0s3 — название сетевого канала (интерфейса), для которого необходимо получить информацию.

Команда **networkctl status** предоставляет обзор всех сетевых каналов и связанных с ними свойств, включая активные **IP-адреса**, назначенный **DHCP-сервер**, шлюз и информацию **DNS**.

Пример вывода:

```
State: routable (unmanaged)
Address: 192.168.2.15 Gateway: 192.168.2.1
```

где:

- **State** — показывает текущее состояние сетевого канала;
- **Address** — отображает назначенный IP-адрес;
- **Gateway** — указывает шлюз по умолчанию.

3. Запуск сетевых устройств:

```
networkctl up enp0s3
```

Команда **networkctl up** используется для активации сетевого интерфейса.

4. Отключение сетевого устройства с временным выводом из эксплуатации:

```
networkctl down enp0s3
```

5. Обновление динамических конфигураций:

```
networkctl renew enp0s3
```

6. Перезагрузка файлов конфигурации:

```
networkctl reload
```

Если были внесены изменения в конфигурационные файлы сети (**.netdev** и **.network**), необходимо перезагрузить конфигурацию, чтобы изменения вступили в силу.

7. Перенастройка сетевых интерфейсов:

```
networkctl reconfigure enp0s3
```

Команда используется для применения изменений конфигурации к сетевому интерфейсу без его перезагрузки.

8. Просмотр логов службы **systemd-networkd** для диагностики и анализа проблем с сетью:

```
journalctl -u systemd-networkd.service
```

Настройка bonding с использованием инструмента nmcli

Bonding – это объединение двух и более сетевых интерфейсов в один логический для достижения отказоустойчивости или увеличения пропускной способности.

В таблице приведены возможные режимы работы утилиты **bond**.

Режим	Тип	Отказоустойчивость	Балансировка	Описание
mode=0	Round Robin	-	+	Циклический режим. Пакеты последовательно передаются и принимаются через каждый интерфейс один за другим.
mode=1	Active Backup	+	-	В этом режиме активен только один интерфейс, а все остальные интерфейсы находятся в резервном состоянии. Если активный интерфейс выходит из строя, резервный интерфейс заменяет его как единственный активный интерфейс в соединении. MAC-адрес интерфейса связи в режиме 1 виден только на одном порту на коммутаторе, что предотвращает путаницу для коммутатора.
mode=2	XOR [exclusive OR]	+	+	Один и тот же интерфейс работает с определённым получателем. MAC-адрес источника использует логику исключающего или (XOR) с MAC-адресом назначения.
mode=3	Broadcast	+	-	Широковещательный режим. Все пакеты отправляются на все интерфейсы.
mode=4	Dynamic Link Aggregation	+	+	IEEE 802.3ad, требует от коммутатора соответствующей настройки, к которому подключен объединенный интерфейс.
mode=5	Transmit Load Balancing (TLB)	+	+	Входящий трафик приходит только на активный интерфейс, а исходящий распределяется в зависимости от текущей загрузки канала каждого интерфейса. Не требует настройки коммутатора.
mode=6	Adaptive Load Balancing (ALB)	+	+	Адаптивная балансировка нагрузки. Отличается более совершенным алгоритмом балансировки нагрузки чем Mode-5. Обеспечивает балансировку нагрузки как исходящего, так и входящего трафика. Не требуется специальной поддержки и настройки со стороны коммутатора/коммутаторов.

Отобразите текущее состояние сетевых интерфейсов командой:

```
nmcli con

NAME    UUID                                  TYPE      DEVICE
enp0s3  d90e7109-6a41-3da8-b662-e8dbae914073  ethernet  enp0s3
enp0s8  17b8cbdb-df3f-31bd-bc82-cf4edb3205cd  ethernet  enp0s8
```

В выводе команды указано, что в системе присутствует две сетевые карты с именами **enp0s3** и **enp0s8**. В дальнейшем они будут связаны в один логический сетевой интерфейс (**Bond**).

Создание bond

Создайте интерфейс **bond0** с автоматическим получением адреса по **DHCP**:

```
nmcli con add type bond con-name bond0 ifname bond0 mode 802.3ad
```

Если же нужно присвоить статический адрес для **bond0**, то используйте команду:

```
nmcli con add type bond con-name bond0 ifname bond0 mode 802.3ad ip4 x.x.x.x/yy
```

где:

- **x.x.x.x** – IPv4 адрес;
- **yy** – маска сети.

Выполните настройку **bond0** и назначьте ему необходимые параметры:

```
nmcli con mod id bond0 bond.options mode=802.3ad,miimon=100,lacp_rate=fast,xmit_hash_policy=layer2+3
```

где:

- **mode=802.3ad** – назначение 4-ого режима работы **bond**;
- **miimon=100** - определяет, как часто производится мониторинг **MII** (Media Independent Interface). ***0*** – мониторинг отключён (используется по-умолчанию). Рекомендуемое значение *100 мс*;
- **lacp_rate=fast** – параметр может принимать два значения *slow* или *fast*. Данное значение определяет, через какой промежуток времени управляющие пакеты **LACPDU** отправляются по каналу **LACP**. По умолчанию значение установлено в *30 секунд* (*slow*). В

режиме *fast* – пакеты отправляются каждую секунду;

- **xmit_hash_policy=layer2+3** - определяет режим вычисления хешей при организации балансировки нагрузки между интерфейсами **bond**. Для вычисления хешей будут использоваться MAC-адреса получателей/отправителей пакета и их IP адреса, если это возможно. Значение по умолчанию для этой опции – *layer2*, что определяет вычисление хеша только по MAC-адресам.

Удаление действующих подключений

Удалите действующие соединения интерфейсов **enp0s3** и **enp0s8**:

```
nmcli con del enp0s3
nmcli con del enp0s8
```

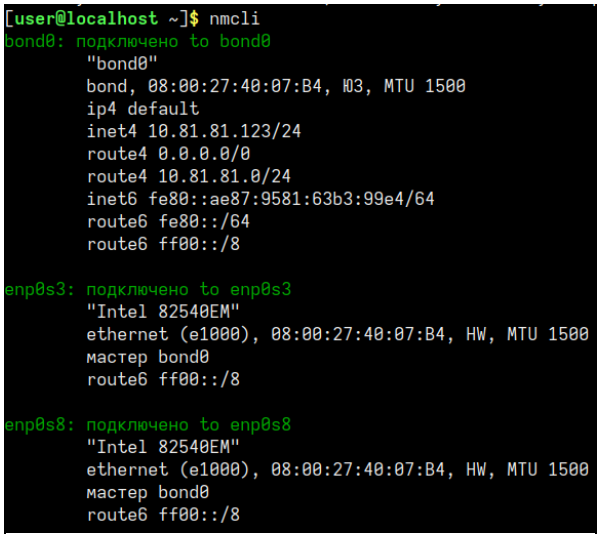
Связывание сетевых интерфейсов в bond

Выполните команды связывания сетевых интерфейсов **enp0s3** и **enp0s8** в **bond0**:

```
nmcli con add type bond-slave ifname enp0s3 con-name enp0s3 master bond0
nmcli con add type bond-slave ifname enp0s8 con-name enp0s8 master bond0
```

Информация о сетевых соединениях

Чтобы вывести результирующую информацию о сетевых настройках, выполните команду **nmcli**:



После завершения настройки проверьте, что интерфейс **bond0** активен и ошибок не обнаружено:

```
cat /proc/net/bonding/bond0

Ethernet Channel Bonding Driver: v6.6.51-1.red80.x86_64
Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
Peer Notification Delay (ms): 0

802.3ad info
LACP active: on
LACP rate: slow
Min links: 0
Aggregator selection policy (ad_select): stable
System priority: 65535
System MAC address: 08:00:27:40:07:b4
Active Aggregator Info:
Aggregator ID: 1
```

Number of ports: 1
Actor Key: 9
Partner Key: 1
Partner Mac Address: 00:00:00:00:00:00

Slave Interface: enp0s3
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:40:07:b4
Slave queue ID: 0
Aggregator ID: 1
Actor Churn State: none
Partner Churn State: churned
Actor Churned Count: 0
Partner Churned Count: 1
details actor lacp pdu:
  system priority: 65535
  system mac address: 08:00:27:40:07:b4
  port key: 9
  port priority: 255
  port number: 1
  port state: 77
details partner lacp pdu:
  system priority: 65535
  system mac address: 00:00:00:00:00:00
  oper key: 1
  port priority: 255
  port number: 1
  port state: 1

Slave Interface: enp0s8
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:21:5c:6a
Slave queue ID: 0
Aggregator ID: 2
Actor Churn State: churned
Partner Churn State: churned
Actor Churned Count: 1
Partner Churned Count: 1
details actor lacp pdu:
  system priority: 65535
  system mac address: 08:00:27:40:07:b4
  port key: 9
  port priority: 255
  port number: 2
  port state: 69
details partner lacp pdu:
  system priority: 65535
  system mac address: 00:00:00:00:00:00
  oper key: 1
  port priority: 255
  port number: 1
  port state: 1

Управление пропускной способностью сетевого интерфейса

Утилита ethtool
Установка
Синтаксис утилиты
Имя сетевого интерфейса
Настройки сетевой карты
Просмотр статистики интерфейса
Получение информации о драйвере
Изменение настроек сетевого интерфейса
Сохранение настроек
Идентификация порта сетевой карты

Утилита tc
Установка
Работа с утилитой
Ограничение скорости
Снятие ограничения скорости
Статус сетевой карты

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: ethtool-2:5.14-2, iproute-tc-6.1.0-2

Утилита ethtool

Ethtool – утилита настройки сетевых интерфейсов. Ethtool позволяет настраивать автоопределение сетевых настроек (*auto-negotiation*) сетевого интерфейса и изменять режимы (*полудуплексный*|*полнодуплексный*) из командной строки.

Автосогласование (Auto-Negotiation) – это механизм, с помощью которого устройство автоматически выбирает наиболее эффективный режим передачи на основе характеристик своих аналогов. Рекомендуется оставить автосогласование включенным, поскольку оно позволяет устройствам выбирать наиболее эффективные средства для передачи данных.

Полудуплексный режим (Half-duplex) позволяет устройству отправлять или получать пакеты по очереди. Устройство, установленное в этот режим, не может выполнять оба действия одновременно.

Когда режим устройства находится в *полнодуплексном* режиме (Full-duplex), оно может отправлять и получать пакеты одновременно.

Важно отметить, что **ethtool** работает только с физическими адаптерами, т.е. для виртуальных устройств просмотр и редактирование настроек недоступны.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ethtool
```

Синтаксис утилиты

Синтаксис утилиты имеет следующий вид:

```
ethtool [<параметры>] <имя_сетевого_интерфейса>
```

Основными параметрами утилиты являются:

- **--version** – версия утилиты;
- **-i, --driver** – информация о драйвере;

- **-P, --show-permaddr** – вывод физического MAC-адреса устройства. Может не совпадать с текущим при использовании bonding;
- **-p, --identify** – мигание светодиодом порта сетевой карты;
- **-r, --negotiate** – повторное согласование скорости передачи данных, если включено автоматическое согласование;
- **-S, --statistics** – вывод статистики;
- **-s, --change** – изменение настроек сетевого интерфейса. После перезагрузки настройки сбрасываются;
- **-k, --show-offload** – просмотр включенных технологий offload;
- **--reset** – сброс настроек различных компонентов сетевой карты, для сброса всех настроек используется all;
- **ethtool -h** – вывод справки о работе с утилитой.

Работа с утилитой

Имя сетевого интерфейса

Для получения имени сетевого интерфейса выполните:

```
ifconfig eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.122.49  netmask 255.255.255.0  broadcast 192.168.122.255
        inet6 fe80::5054:ff:fea5:5f03  prefixlen 128  scopeid 0x10<host>
        ether 00:1e:8c:f4:d0:a5  txqueuelen 1000  (Ethernet)
        RX packets 21472  bytes 31825829 (30.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        X packets 2217  bytes 182000 (177.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Настройки сетевой карты

Для получения текущих настроек сетевой карты выполните команду вида:

```
ethtool <имя_сетевого_интерфейса>
```

Например:

```
ethtool eno1

Settings for eno1:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        MDI-X: on (auto)
netlink error: Operation not permitted
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

Вывод команды показывает, что текущая скорость равна *1000 Мбит/с*, дуплекс находится в режиме «*Full*» и автосогласование *включено*.

Просмотр статистики интерфейса

Для получения статистики сетевой карты выполните команду вида:

```
ethtool -S <имя_сетевого_интерфейса>
```

Например:

```
ethtool -S eno1

NIC statistics:
     rx_packets: 8527943
     tx_packets: 6515884
     rx_bytes: 4924517588
     tx_bytes: 2746866206
     rx_broadcast: 450774
     tx_broadcast: 9
     rx_multicast: 277235
     tx_multicast: 12177
     rx_errors: 0
     tx_errors: 0
     tx_dropped: 0
     multicast: 277235
     collisions: 0
...
```

Получение информации о драйвере

Для получения имени драйвера и вывода сопутствующей информации выполните команду вида:

```
ethtool -i <имя_сетевого_интерфейса>
```

Например:

```
ethtool -i eno1

driver: r8169
version: 6.6.51-1.red80.x86_64
firmware-version: rtl8168h-2_0.0.2 02/26/15
expansion-rom-version:
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: yes
```

Изменение настроек сетевого интерфейса

Для изменения настроек сетевой карты выполните команду вида:

```
ethtool -s [<имя_сетевого_интерфейса>] speed [10/100/1000] duplex [half/full] autoneg [on/off]
```

где:

- `speed [10/100/1000]` – требуемая скорость сетевого интерфейса;
- `duplex [half/full]` – режим дуплекса (полудуплексный/полнодуплексный);
- `autoneg [on/off]` — автосогласование (включено/выключено).

Например:

```
ethtool -s eno1 speed 100 duplex half autoneg on
```

Для проверки применения установленных настроек сетевой карты выполните команду вывода текущих настроек:

```
ethtool <имя_сетевого_интерфейса>
```

Сохранение настроек

По умолчанию установленные изменения в настройках сетевой карты будут сброшены после перезагрузки системы. Для сохранения внесенных изменений на постоянной основе необходимо отредактировать конфигурационный файл интерфейса устройства.

Для этого откройте файл интерфейса:

```
nano /etc/sysconfig/network-scripts/ifcfg-<имя_сетевого_интерфейса>
```

и в конце файла добавьте строку с нужными настройками:

```
ETHTOOL_OPTS="speed [100|1000|10000] duplex [half|full] autoneg [on|off]"
```

Сохраните изменения и закройте файл.

После перезагрузки системы внесенные настройки будут автоматически применяться для выбранного сетевого интерфейса.

Идентификация порта сетевой карты

Одной из полезных функций утилиты ethtool является возможность поиска физического расположения сетевого адаптера путем мигания светодиода устройства. Например, для мигания светодиодом устройства Ethernet eno1 можно использовать команду:

```
ethtool -p eno1 15
```

где `15` – продолжительность мигания светодиода в секундах.

Утилита tc

tc – консольная утилита для просмотра и конфигурирования параметров управления сетевым трафиком. Позволяет управлять классификацией трафика, дисциплинами управления очередями для различных классов трафика либо целиком для сетевого интерфейса.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install iproute-tc
```

Затем скачайте специальный установочный файл install.sh.

Работа с утилитой

Для вывода списка сетевых карт выполните:

```
ifconfig

eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.122.49  netmask 255.255.255.0  broadcast 192.168.122.255
      inet6 fe80::5054:ff:fea5:5f03  prefixlen 128  scopeid 0x10<host>
      ether 00:1e:8c:f4:d0:a5  txqueuelen 1000  (Ethernet)
      RX packets 21472  bytes 31825829 (30.3 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
```

```
        X packets 2217  bytes 182000 (177.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Перед началом работы запустите скачанный ранее установочный файл **install.sh** для каждой сетевой карты, на которой будет регулироваться скорость, например:

```
/install.sh eno1

Для включения лимита выполните команду /sbin/eno1limiton.sh 1000 2000
Где 1000 - скорость отдачи, 2000 - скорость загрузки
Для отключения лимита выполните команду /sbin/eno1limitoff.sh
Для просмотра статуса ограничения скорости выполните команду /sbin/eno1limitstatus.sh
```

Ограничение скорости

Для включения ограничения скорости выполните команду вида:

```
/sbin/<имя_интерфейса>limiton.sh <скорость_отдачи> <скорость_загрузки>
```

Например:

```
/sbin/eno1limiton.sh 500 1000
cat /sbin/eno1limitstatus.sh

На сетевой карте eno1 установлено ограничение скорости на отдачу 500 килобит, на загрузку 1000 килобит
```

Снятие ограничения скорости

Для отключения ограничения скорости выполните команду вида:

```
/sbin/<имя_интерфейса>limitoff.sh
```

Например:

```
/sbin/eno1limitoff.sh
cat /sbin/eno1limitstatus.sh

На сетевой карте eno1 не установлено ограничение скорости
```

Статус сетевой карты

Для просмотра статуса сетевой карты выполните команду вида:

```
cat /sbin/<имя_интерфейса>limitstatus.sh
```

Например:

```
cat /sbin/eno1limitstatus.sh
```

Управление маршрутизацией

Управление маршрутизацией с помощью графической утилиты NetworkManager
Управление маршрутизацией с помощью утилиты route
Изменение таблицы маршрутизации

Окружение

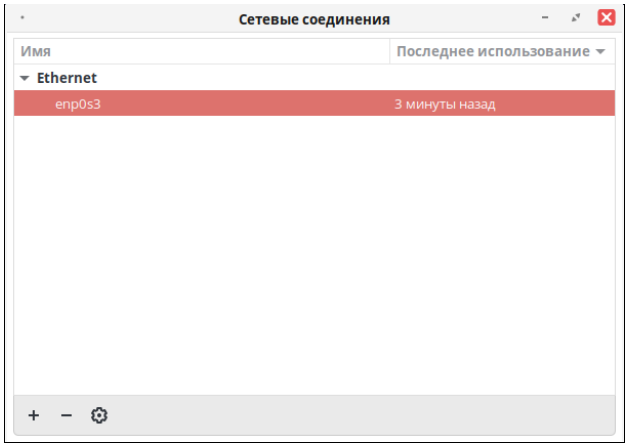
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: NetworkManager-1:1.32.12-1

Сетевые маршруты необходимы для перенаправления пакетов, передаваемых по сети, таким образом, чтобы они могли достигнуть конечной цели. Маршруты можно настраивать на уровне интерфейса или маршрутизатора.

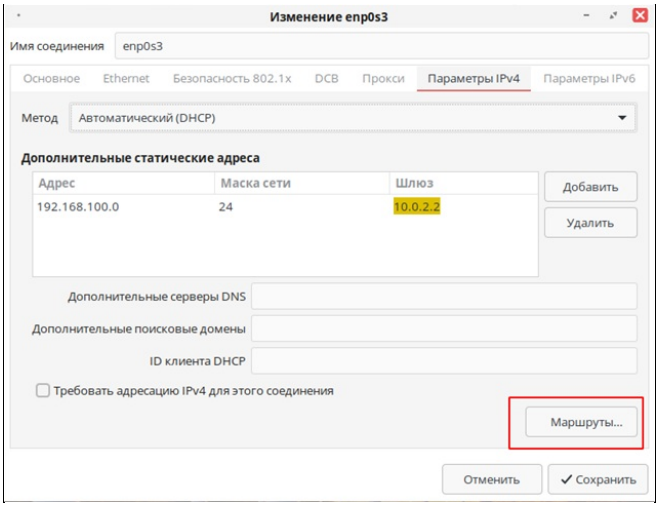
Когда компьютеру необходимо отправить пакет в сеть, он проверяет таблицу маршрутизации; в ней указаны IP-адреса пунктов назначения и адреса интерфейсов и роутеров в сети, которые могут отправить пакет по нужному адресу. Если для конечной цели маршрут не указан, используется так называемый шлюз по умолчанию или маршрут по умолчанию. Точно такой же принцип используется в роутере – устройство смотрит на IP-адрес назначения, сверяет его со своей таблицей маршрутизации и отправляет далее по маршруту.

Управление маршрутизацией с помощью графической утилиты NetworkManager

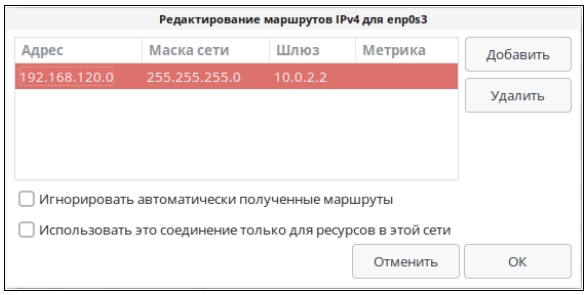
Для добавления новых маршрутов необходимо открыть панель управления сетью, для этого в системном трее нажмите ПКМ на значок сети и выберите пункт «Изменить соединение». Будет открыто окно «Сетевые соединения».



Выберите интерфейс, который необходимо настроить. Перейдите на вкладку «Параметры IPv4». На этой вкладке можно перейти к настройке маршрутов, нажав на кнопку «Маршруты».



Будет открыто окно для настройки и редактирования маршрутов. Создать новый маршрут можно с помощью кнопки «Добавить».



Управление маршрутизацией с помощью утилиты route

Утилита **route** помогает просматривать и вносить изменения в сетевые маршруты в операционной системе. Она также отображает маршруты, которые были добавлены с помощью графической утилиты **NetworkManager**.

Для того чтобы посмотреть правила маршрутизации, достаточно выполнить команду:

```
route
```

```
[user@localhost ~]$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
[user@localhost ~]$
```

Для того чтобы вывести все строки таблицы в цифровом формате, можно выполнить команду:

```
route -n
```

Изменения таблицы маршрутизации

В общем случае прототипом команды **route** является следующая запись:

```
route add [-net|-host] <IP/Net> netmask <Netmask> gw <Gateway_IP> dev <Int>
```

где:

- **-net** – используется для добавления правила для всей подсети;
- **-host** – используется для добавления правила для одного адреса;
- **<IP/Net>** – адрес объекта назначения;
- **<Netmask>** – маска объекта назначения;
- **<Gateway IP>** – адрес шлюза, через который будет проложен маршрут до объекта назначения;
- **<Int>** – интерфейс, который будет использоваться при обработке пакетов.

Примечание.

Команду для добавления маршрута необходимо выполнять с правами **администратора** системы.

Таким образом, команда для добавления маршрута для подсети будет выглядеть следующим образом:

```
route add -net 192.168.100.0 netmask 255.255.255.0 gw 192.168.122.3 dev enp0s3
```

В сокращенном виде:

```
route add -net 192.168.100.0/24 gw 192.168.122.3 dev enp3s0
```

Команда для добавления маршрута только для определенного хоста будет выглядеть следующим образом:

```
route add -host 192.168.1.122 gw 192.168.122.1 dev enp3s0
```

При добавлении правила для хоста маску можно не указывать, она автоматически будет равна **255.255.255.255**.

Для удаления маршрута можно воспользоваться следующей командой с указанием объекта назначения:

```
route del -net 192.168.100.0/24 gw 192.168.122.3 dev enp3s0
route del -host 192.168.1.122 gw 192.168.122.1 dev enp3s0
```

Добавленные с помощью утилиты **route** маршруты будут активны только до перезагрузки системы, после перезагрузки они будут автоматически удалены. Чтобы маршруты сохранились, их необходимо добавить в файл конфигурации.

Для этого потребуется добавить значения маршрута в конфигурационный файл используемого интерфейса:

```
nano /etc/NetworkManager/system-connections/<имя_интерфейса>.nmconnection
```

В секцию [ipv4] конфигурационного файла следует добавить информацию о маршруте. Например:

```
route1=192.168.1.0/24,192.168.0.4
```

Пример содержимого конфигурационного файла с добавленным маршрутом:

```
nano /etc/NetworkManager/system-connections/enp3s0.nmconnection
```

```
[connection]
id=enp3s0
uuid=800eab29-0d08-3b42-aeaf-9dc1219aca14
type=ethernet
autoconnect-priority=-999
interface-name=enp3s0
timestamp=1713466837

[ethernet]

[ipv4]
method=auto
route1=192.168.1.0/24,192.168.0.4

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

После добавления информации о маршрутах потребуется перезагрузить систему для применения внесенных изменений.

Настройка Wi-Fi в РЕД ОС

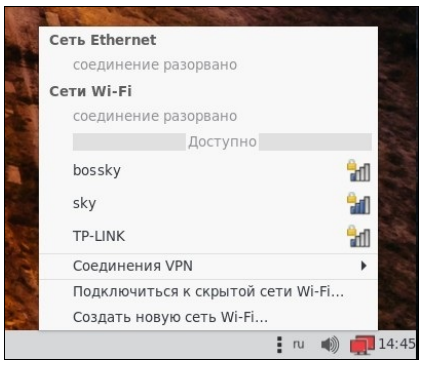
Пример подключения
Использование консольных утилит
Решение проблем с Wi-Fi
Получение информации об устройстве
Поиск и установка драйвера
Подключение к скрытой сети Wi-Fi

В данной статье будет рассмотрено подключение РЕД ОС к сети **Wi-Fi** — технологии беспроводной локальной сети.

Подключение осуществляется посредством сетевого адаптера *Wi-Fi*, который может быть установлен в вашем ноутбуке или стационарном ПК.

Для работы *Wi-Fi* адаптера требуются соответствующие драйверы. В РЕД ОС имеется поддержка большинства таких устройств.

При успешном обнаружении системой *Wi-Fi* адаптера, при нажатии на значок сетевого подключения, можно увидеть список доступных беспроводных сетей.



Здесь отображаются названия сетей и уровень сигнала точек доступа, значок замка на пиктограмме уровня сообщает, что доступ к сети защищён паролем.

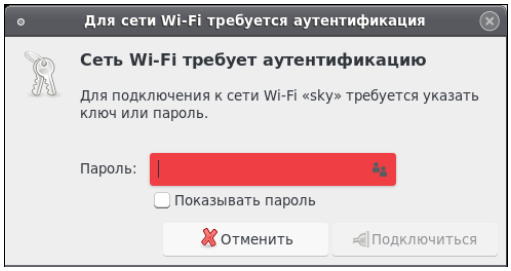
Вы можете подробнее ознакомиться с настройкой **Wi-Fi**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка Wi-Fi в РЕД ОС;
- в **Яндекс.Дзен** — Настройка Wi-Fi в РЕД ОС;
- в **VK Видео** — Настройка Wi-Fi в РЕД ОС.

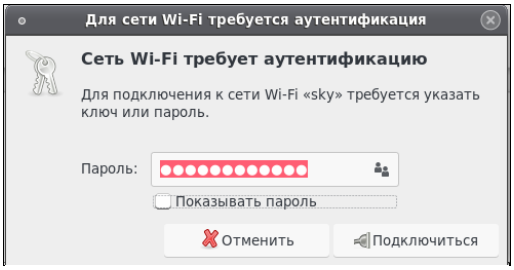
На наших каналах вы также сможете найти много другой полезной информации.

Пример подключения

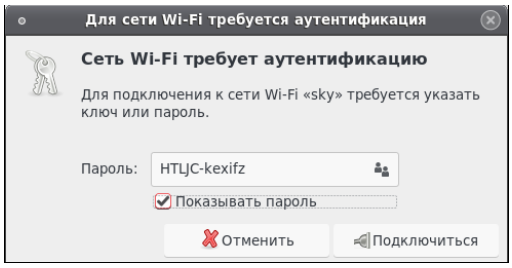
Далее будет рассмотрен пример подключения к одной из сетей.



Выберите любую из доступных сетей, введите пароль для подключения к точке доступа беспроводной сети.

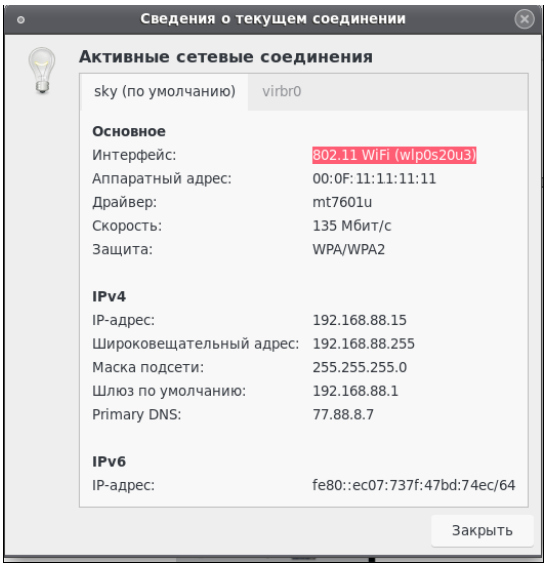


При необходимости выберите «**Показать пароль**» и проверьте правильность его написания.



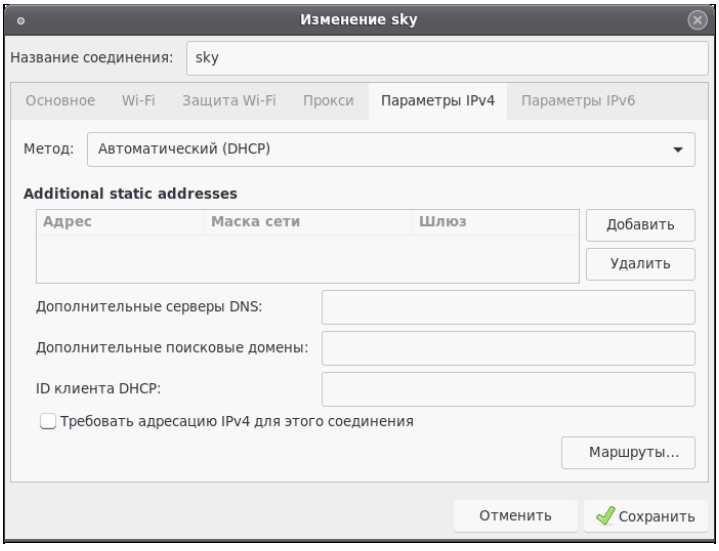
При успешном подключении в системном трее появится соответствующий значок ().

Если нажать правой кнопкой мыши по значку и выбрать в меню «**Сведения о соединении**», откроется окно, в котором будет показана информация о сетевом подключении.

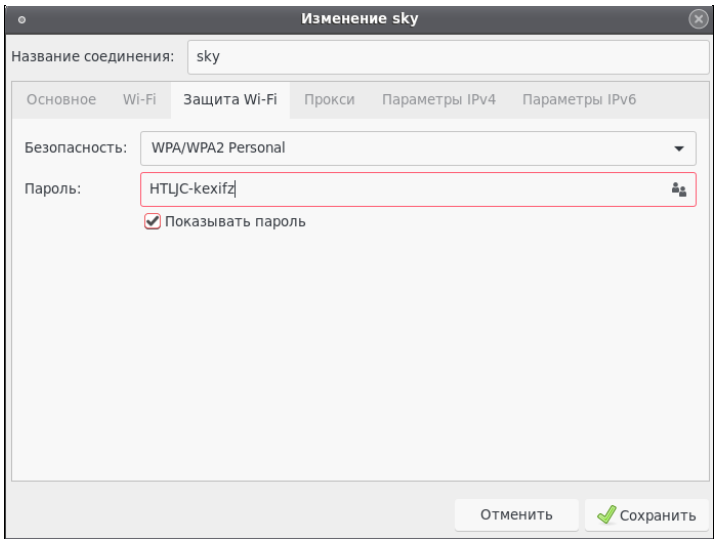


Здесь можно просмотреть такие параметры, как MAC-адрес устройства, используемый драйвер (в данном случае — это **mt7601u**), скорость подключения, тип защиты (WPA/WPA2), а также IP-адрес, сетевую маску, шлюз и прочие параметры.

Как и при проводном соединении имеется возможность редактировать различные сетевые параметры Wi-Fi соединения.



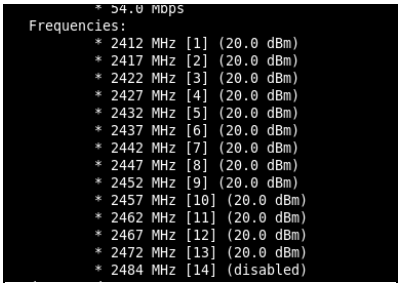
Если необходимо посмотреть пароль текущего Wi-Fi подключения, перейдите на вкладку «**Защита Wi-Fi**» и нажмите «**Показать пароль**».



Использование консольных утилит

Также информацию о сетевом Wi-Fi адаптере можно просмотреть с помощью консольных утилит. Одна из них — это утилита **iw**.

iw list — команда показывает информацию о Wi-Fi адаптере, например, радиочастоты, поддерживаемые вашей Wi-Fi картой.



В данном примере беспроводной адаптер поддерживает радиочастоты 2.4 ГГц. Существуют адаптеры, которые работают с диапазоном 5 ГГц, что позволяет заметно увеличить пропускную способность сетевой карты.

Команда iw monitor отображает, что происходит на уровне межсетевого протокола, например, как IP-адреса присваиваются сетевому интерфейсу, и какие маршруты прописываются в системе. Во время запуска программы можно попробовать подключиться к точке доступа, в выводе будут отображены результаты ваших действий.

iw event — команда выводит перечень беспроводных событий, связанных с Wi-Fi интерфейсом. Во время запуска команды можно попробовать подключиться к другой сети Wi-Fi, в выводе будут отображены результаты ваших действий.

iw dev — отображает сведения о текущем соединении, в выводе можно узнать название сети (SSID), а также номер канала и радиочастоту, на которой работает Wi-Fi. **SSID** (*Service Set Identifier*) – идентификатор беспроводной сети.

```
iw dev

phy#0
    Interface     wlp0s20u3
                ifindex 3 wdev 0x1
                addr 00:0f:11:11:11:11
                ssid sky
                type managed
                channel 9 (2452 MHz), width: 40 MHz, center1: 2462 MHz
```

Решение проблем с Wi-Fi

В некоторых ноутбуках присутствует аппаратный переключатель питания беспроводной карты и не исключается случай, когда карта может быть заблокирована ядром Linux. С помощью следующей команды проверьте текущий статус:

```
rfkill list

1: phy1:  Wireless LAN
        Soft blocked: no
```

```
        Hard blocked: no
```

В выводе указано, что аппаратная и программная блокировка не используется. Об этом свидетельствуют значения: «Soft blocked: **no**» и «Hard blocked: **no**».

Если в выводе данной команды будет отображаться «Hard blocked: **Yes**», тогда для снятия блокировки используйте аппаратную кнопку/переключатель на вашем устройстве (ноутбуке).

В случае отображения в выводе «Soft blocked: **Yes**» — выполните команду разблокировки:

```
rfkill unblock wifi
```

Если система все так же не видит доступные беспроводные сети, то существует высокая вероятность, что в ОС отсутствует Wi-Fi драйвер для данной модели устройства. Это могло произойти из-за того, что РЕД ОС установлен на компьютер с новым Wi-Fi модулем, который появился в продаже уже после выхода релиза РЕД ОС и драйвера для данной модели беспроводного устройства не были включены в ОС.

В данном случае разработчиками РЕД ОС добавляются драйвера для новых Wi-Fi чипов в репозиторий программного обеспечения РЕД ОС.

Однако может возникнуть проблема — как получить доступ к сети Интернет для загрузки нужного драйвера, если Wi-Fi не работает.

Самое простое решение — это настроить проводную сеть (при наличии). Если на ПК нет проводной сетевой карты, можно использовать смартфон, подключенный по USB, который в системе отобразится либо как USB-модем, либо как сетевой USB-адаптер.

Если никакой из перечисленных вариантов не поможет настроить доступ в Интернет, тогда необходимо узнать информацию об используемом устройстве (см. п. «Получение информации об устройстве»). Собранную информацию можно передать в ТП РЕД ОС, после ее анализа специалист ТП отправит нужный драйвер для установки.

Получение информации об устройстве

Определите модель Wi-Fi устройства и установите драйвера из репозитория РЕД ОС. Для этого используйте команду:

```
lspci -nn

00:00.0 Host bridge: Intel Corporation Device 9b63 (rev 03)
00:02.0 VGA compatible controller: Intel Corporation Device 9bc8 (rev 03)
00:12.0 Signal processing controller: Intel Corporation Device 06f9
00:14.0 USB controller: Intel Corporation Device 06ed
00:14.2 RAM memory: Intel Corporation Device 06ef
00:14.3 Network controller: Intel Corporation Device 06f0
00:16.0 Communication controller: Intel Corporation Device 06e0
00:16.3 Serial controller: Intel Corporation Device 06e3
00:17.0 SATA controller: Intel Corporation Device 06d2
00:1b.0 PCI bridge: Intel Corporation Device 06c0 (rev f0)
00:1c.0 PCI bridge: Intel Corporation Device 06bd (rev f0)
00:1f.0 ISA bridge: Intel Corporation Device 0687
00:1f.3 Multimedia audio controller: Intel Corporation Device 06c8
00:1f.4 SMBus: Intel Corporation Device 06a3
00:1f.5 Serial bus controller [0c80]: Intel Corporation Device 06a4
00:1f.6 Ethernet controller: Intel Corporation Device 0d4c
01:00.0 Non-Volatile memory controller: Device 1e0f:0001
02:00.0 Unassigned class [ff00]: Realtek Semiconductor Co., Ltd. RTS522A PCI Express Card Reader (rev 01)
```

Команда lspci выводит информацию обо всех PCI-шинах и устройствах на них.

В примере в выводе команды присутствуют две строки с текстом **Ethernet controller** и **Network controller**, это говорит о том, что в компьютере имеется две сетевые карты. Также можно заметить, что в конце строки указаны их идентификаторы (**0d4c** и **06f0**) . Данные идентификаторы будут использоваться для определения драйвера, который нужно установить.

Если используется **USB** Wi-Fi модуль, то для определения идентификатора устройства можно применить команду lsusb.

```
lsusb

Bus 002 Device 002: ID 8087:8000 Intel Corp.
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 8087:8008 Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 004: ID 148f:7601 Ralink Technology, Corp. MT7601U Wireless Adapter
```

```
Bus 003 Device 003: ID 046d:c077 Logitech, Inc. M105 Optical Mouse
```

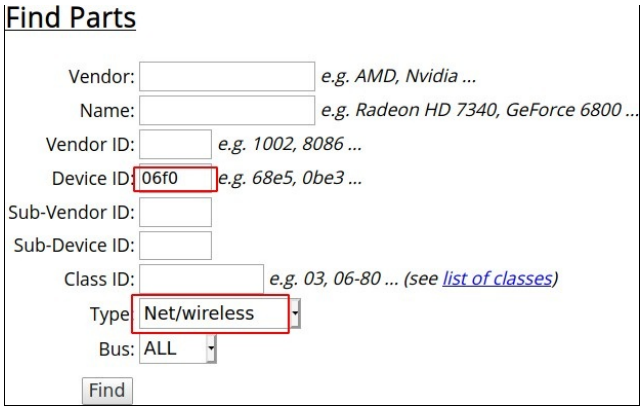
Здесь:

- **148f** — это **Vendor ID**;
- **7601** — это **Device ID**.

Поиск и установка драйвера

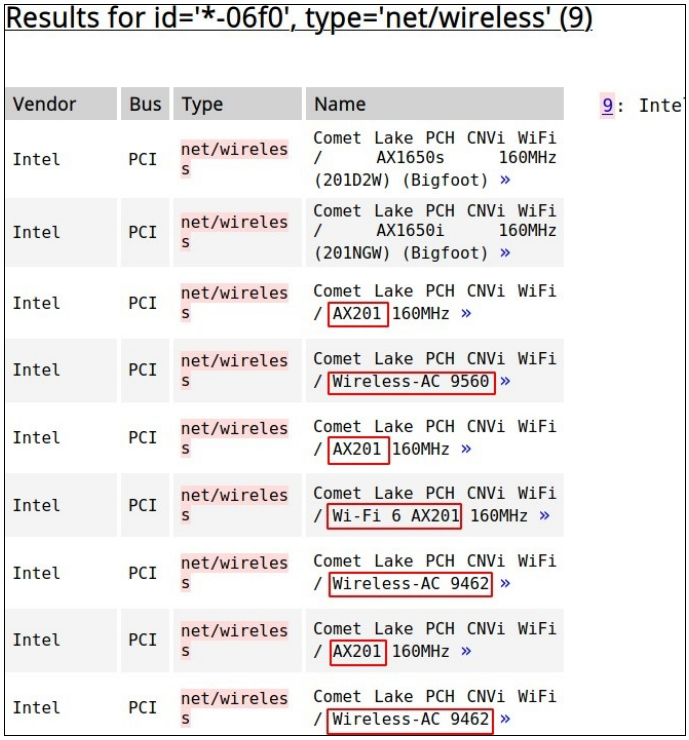
Перейдите на сайт https://linux-hardware.org — этот портал содержит информацию об оборудовании компьютеров под управлением Linux.

Откройте раздел **Find Parts**.



В поле **Device ID** укажите идентификатор первого сетевого устройства из вывода lspci.

В поле **Type** выберите «**Net / wireless**» — это означает, что поиск будет осуществляться только по устройствам с беспроводным сетевым интерфейсом (Wi-Fi). Нажмите на кнопку «**Find**», будут выведены следующие результаты поиска:



Ваш результат поиска может отличаться от приведенного в примере, он зависит от модели беспроводного устройства.

В данной таблице устройствам с идентификатором **06f0**, соответствуют Wi-Fi адаптеры производства Intel: **Wi-Fi AX201** и **Wireless-AC 9462**.

Попробуйте найти в репозитории РЕД ОС Wi-Fi устройство по имени из этой таблицы:

```
dnf search AX201
```

```
[user@rfc1918 ~]$ yum search AX201
Загружены модули: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
================================================================ N/S matched: AX201 ================================
iwl7260-firmware.noarch : Firmware for Intel(R) Wireless WiFi Link 726x/8000/9000/AX200/AX201 Series Adapters
```

Это означает, что нужно установить данный пакет. Для этого воспользуйтесь командой:

```
dnf install iwl7260-firmware
```

После установки драйвера проверьте беспроводное сетевое подключение.

Кроме этого компьютеры могут поставляться с Wi-Fi адаптерами, которые используют, например, драйвера **Realtek**. В репозитории РЕД ОС имеются драйвера и для них.

Установка драйвера производится командой:

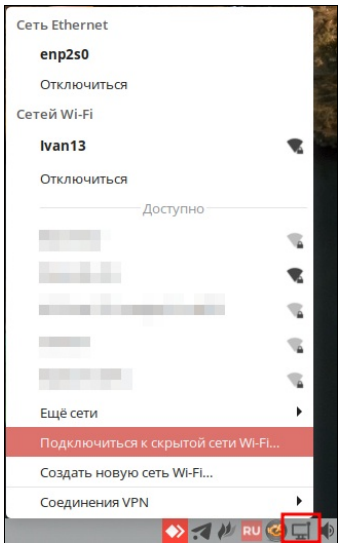
```
dnf install rtl<модель_адаптера>
```

Рассмотренный в статье метод поиска и установки Wi-Fi драйвера может быть применен не только к беспроводным модулям, но и, по аналогии, к другим устройствам.

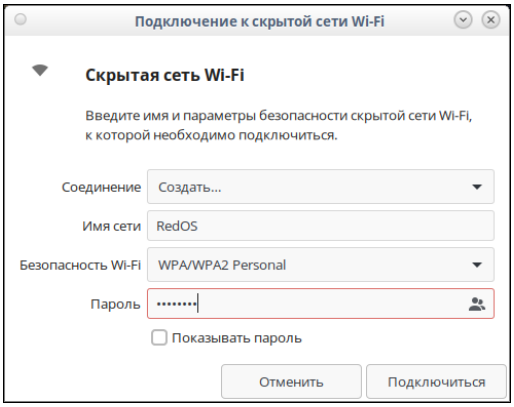
Подключение к скрытой сети Wi-Fi

Подключение к скрытой сети Wi-Fi в графической оболочке Mate

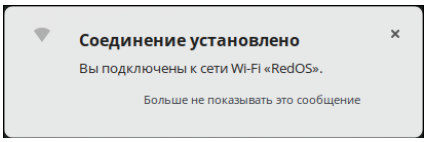
Для подключения к *скрытой сети wi-fi* в графической оболочки *Mate* нажмите ПКМ на значок сети в системном трее и выберите пункт «**Подключиться к скрытой сети Wi-Fi**».



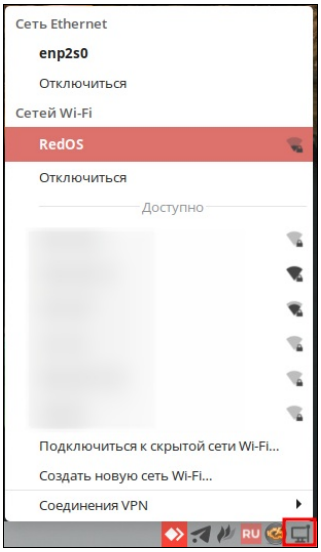
В открывшемся окне заполните поля «**Соединение**», «**Имя сети**», «**Безопасность Wi-Fi**» и «**Пароль**» и нажмите кнопку «**Подключиться**».



При успешном подключении будет выведено соответствующее сообщение.

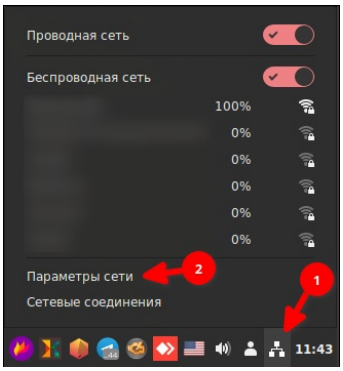


Также, нажав ПКМ на значок сети в системном трее, можно просмотреть доступные сети и текущие сетевые соединения.

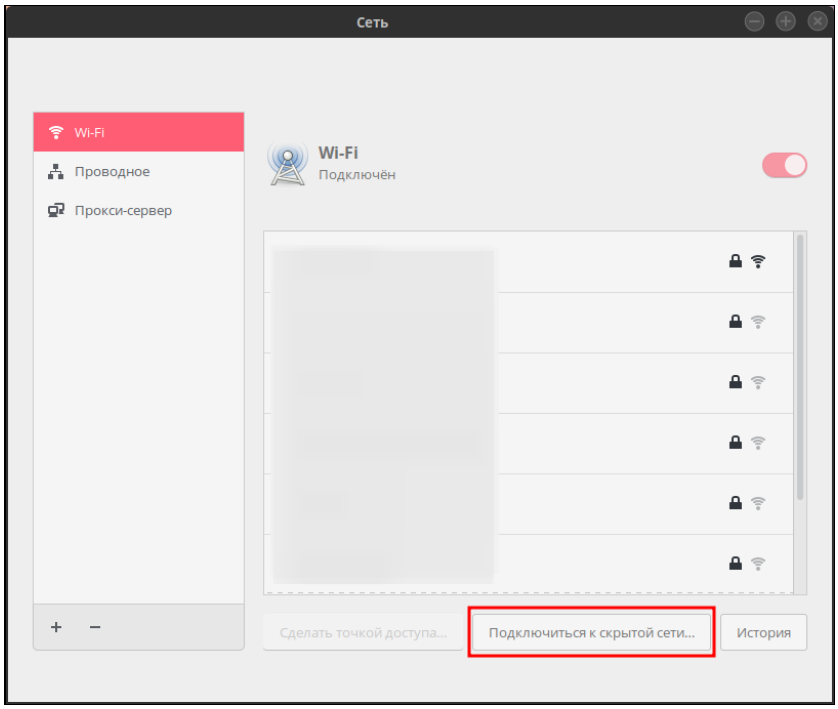


Подключение к скрытой сети Wi-Fi в графической оболочке Cinnamon

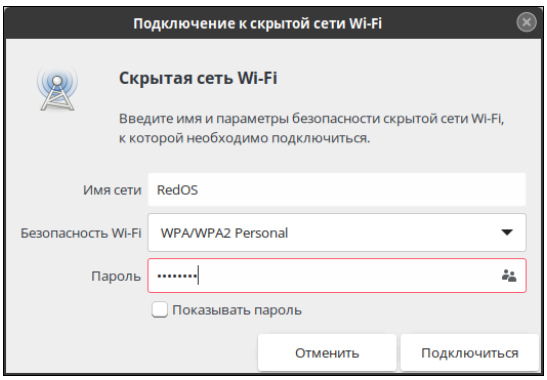
Для подключения к *скрытой сети wi-fi* в графической оболочке *Cinnamon* нажмите ЛКМ на значок сети в системном трее и выберите пункт «**Параметры сети**».



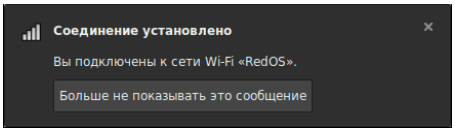
Будет открыто окно настройки сети. В разделе Wi-Fi нажмите кнопку «**Подключиться к скрытой сети...**».



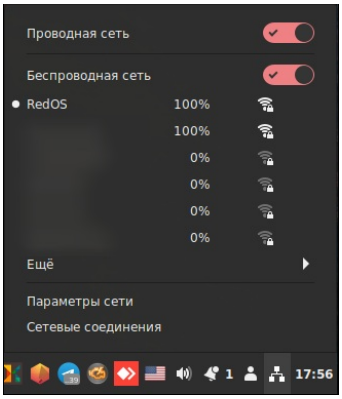
В открывшемся окне «**Подключение к скрытой сети Wi-Fi**» заполните поля «**Имя сети**», «**Безопасность Wi-Fi**» и «**Пароль**» и нажмите кнопку «**Подключиться**».



При успешном подключении будет выведено соответствующее сообщение.



Также, нажав ЛКМ на значок сети в системном трее, можно просмотреть доступные сети и текущие сетевые соединения.



Основные понятия squid

Централизованный выход в Интернет через один сервер в сети (proxy)

В корпоративных сетях является стандартной ситуация, когда, с одной стороны, множество пользователей на разных компьютерах пользуются ресурсами сети Интернет, при этом обеспечить надлежащий уровень безопасности на этих компьютерах одновременно довольно сложно. Ещё сложнее заставить пользователей соблюдать некий «корпоративный стандарт», ограничивающий возможности использования Интернет (например, запретить использование определённого типа ресурсов или закрыть доступ к некоторым адресам).

Простейшим решением будет разрешить только определённые методы доступа к Интернет (например, по протоколам HTTP и FTP) и определить права доступа абонентов на одном сервере, а самим абонентам разрешить только обращение к этому серверу по специальному прокси-протоколу (поддерживается всеми современными браузерами). Сервер же, после определения прав доступа, будет транслировать (проксировать) приходящие на него HTTP-запросы, направляя их адресату. Допустим, несколько пользователей с нескольких компьютеров внутренней сети просматривают некоторый сайт. С точки зрения этого сайта их активность представляется потоком запросов от одного и того же компьютера.

Обычный доступ

Непосредственно после установки **Squid** уже поддерживает функции прокси, но принимает соединения только с того компьютера, на который установлен. Для того, чтобы можно было воспользоваться этим сервисом с других компьютеров, необходимо изменить таблицы управления доступом (**Access Control Lists**, далее **ACL**), находящиеся, как и большинство настроек **Squid**, в файле **/etc/squid/squid.conf**. Файл содержит подробные комментарии и примеры для всех настроек, представленные в следующем формате:

```
# TAG: <настройка>
```

Таким же образом там описаны все значения, выставленные по умолчанию. В частности, для того, чтобы **Squid** принимал соединения из всей внутренней сети, необходимо раскомментировать две строки, и подставить в них действительный диапазон адресов вашей сети:

```
acl our_networks src 192.168.1.0/24 192.168.2.0/24
 http_access allow our_networks
```

При обработке запроса на доступ к **Squid** все строки **http_access** в файле **squid.conf** анализируются последовательно, начиная с верхней строки и заканчивая первой строкой, соответствующей параметрам запроса. Порядок расположения строк **http_access** имеет значение.

Анонимизирующий доступ

При использовании прокси-сервера остаётся некоторая угроза безопасности, связанная с тем, что топология внутренней сети и активность её абонентов не маскируются. Например, в протоколе HTTP используются заголовки (**headers**), значения которых заполняются браузерами при отправлении запроса. **Squid** умеет удалять опасные поля заголовка из запроса при помощи настройки **header_access** или подменять их значения на другие, заранее заданные, при помощи настройки **header_replace**. Варианты использования этих настроек приведены в squid.conf в районе **TAG: header_access** и **TAG: header_replace**, соответственно.

Имейте в виду, что из-за удаления и/или подмены полей заголовков может нарушиться связь с некоторыми системами, использующими значение этих полей для организации взаимодействия и авторизации.

«Прозрачный» доступ

Прокси-сервер можно использовать незаметно для конечных пользователей сети. Если прокси-сервер также выполняет функцию маршрутизатора, весь сетевой трафик неизбежно пройдет через него. Используя средства межсетевого экрана, можно перенаправлять все стандартные HTTP-запросы к удалённым серверам на специально настроенный порт **Squid**. С внешней стороны это будет выглядеть как обычный прокси-сервер, а для пользователей работа в сети останется привычной. Команда **iptables**, перенаправляющая HTTP-запросы к внешним серверам на порт **Squid**, может выглядеть следующим образом:

```
iptables -t NAT -A PREROUTING -d ! <адрес_самого_сервера> \
-i <внутренний_сетевой_интерфейс> -p tcp -m tcp --dport 80 \
-j REDIRECT --to-ports 3128
```

Или так:

```
iptables -t nat -A PREROUTING -p tcp -d 0/0 --dport www \
-i <внутренний_сетевой_интерфейс> -j DNAT \
--to <локальный_адрес_на_котором_слушает_прокси>:3128
```

Для настройки прозрачного проксирования в файле **squid.conf** используется обратный прокси, описанный ниже. Для организации прозрачного прокси достаточно добавить в **squid.conf** следующую строку:

```
http_port 80 intercept
```

Фильтрация доступа

Squid предоставляет гибкую систему фильтрации внешних ссылок, позволяющую закрывать доступ к определённым веб-сайтам и ресурсам, блокировать баннеры, ссылки непристойного содержания и другие нежелательные элементы. Фильтрация осуществляется с использованием **ACL** и соответствующих настроек **http_access deny**, примеры которых приведены в файле **squid.conf**.

При определении фильтруемых URL или доменов можно применять регулярные выражения, что позволяет создавать фильтры для целых классов адресов или доменных имен в одной строке. Дополнительную информацию о регулярных выражениях можно найти в руководстве **regex**.

Пример запрета доступа к домену **baddomain.com**:

```
acl Bad dstdomain baddomain.com
 http_access deny Bad
```

Необходимо учитывать, что правило **http_access deny Bad** должно располагаться перед строками вида **http_access allow**, в этом случае доступ к любому сайту домена будет закрыт безусловно.

Авторизация доступа

Squid поддерживает возможность применения различных **ACL** для отдельных пользователей или категорий пользователей. Если для определения того, какой именно пользователь подключается к серверу, недостаточно IP-адреса его компьютера, следует воспользоваться одной из многих схем авторизации, принятых в **Squid**. Авторизация конфигурируется с помощью тега **TAG: auth_param**. Посмотреть, какие схемы (программы) авторизации поддерживает **Squid**, можно в каталоге **/usr/lib/squid**.

Пример настройки авторизации через **LDAP**:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b ou=People,dc=office,dc=lan -f (uid=%s) -h ldap.office.lan auth_param basic
children 5
 auth_param basic realm Squid proxy-caching web server auth_param basic credentialsttl 2 hours
```

Дополнительную информацию по настройке выбранных программ авторизации можно найти в соответствующих руководствах.

Локальное хранение данных, которые уже запрашивались пользователями (cache)

Одним из преимуществ **Squid** является возможность кеширования данных, полученных из сети Интернет. Кешированные объекты остаются доступными для повторного использования до окончания срока их актуальности или до момента, когда они будут заменены новыми, более востребованными данными. Это значительно сокращает нагрузку на внешний канал связи и уменьшает время ожидания ответа для пользователей. Например, если несколько пользователей внутри сети одновременно обращаются к одному и тому же веб-ресурсу, общее количество запросов к внешнему источнику через **Squid** существенно снизится, так как большая часть необходимых данных уже находится в кеше.

Обычное кеширование

Сразу после установки **Squid** начинает выполнять функции кеширования. Эта функция не только экономит трафик, но и сокращает время доступа к ресурсам Интернета. Важно отметить, что снижение внешнего трафика возможно только если один и тот же ресурс был запрошен несколькими пользователями на протяжении определенного промежутка времени. Если пользовательские запросы практически не пересекаются, снижение объема внешнего трафика может оказаться минимальным.

Кроме того, кеширование неэффективно в ситуации, когда повторный запрос на большинство объектов приходит уже после того, как эти объекты вытесняются из кеша более новыми. Если анализ статистики показывает, что происходит именно это, можно попробовать увеличить объём кешируемой информации. Настройки **Squid**, отвечающие за размер кеша, приведены в файле **squid.conf** в разделе, начинающемся словами **OPTIONS WHICH AFFECT THE CACHE SIZE**.

Наконец, кеширование входящего трафика делает невозможным точное распределение оплаты трафика между разными пользователями. Например, если один пользователь посещает сайты по рекомендации другого, его трафик в значительной степени останется внутри сети, так как необходимые ресурсы уже были закешированы благодаря действиям первого пользователя.

Выборочное кеширование

Некоторые типы данных, такие как очень большие файлы, динамически генерируемые веб-страницы, аудиофайлы и прочие ресурсы, нецелесообразно кешировать, поскольку вероятность их повторного запроса в пределах установленного срока хранения невелика, при этом они занимают значительное пространство в кеше, вытесняя другие полезные объекты. С другой стороны, некоторые виды контента могут требовать обязательного кеширования для улучшения скорости доступа. Управление этими процессами осуществляется посредством **ACL** и настроек **always_direct** (для исключения кеширования) и **never_direct** (для принудительного кеширования).

Например, чтобы отключить кеширование файлов, загружаемых по протоколу **FTP** (что обычно рекомендуется), необходимо в соответствующем разделе файла **squid.conf** раскомментировать следующие строки:

```
acl FTP proto FTP
 always_direct allow FTP
```

Иерархия серверов

Если запрашиваемый ресурс не найден в локальном кеше **Squid**, система может попытаться запросить его у вышестоящих серверов (**parent peer**) или у соседей (**sibling peers**), прежде чем отправлять запрос в Интернет. В качестве вышестоящего сервера может выступать сервер провайдера, а соседними серверами могут быть устройства других абонентов, подключённых к тому же провайдеру. Подробные правила взаимодействия и построения иерархии кеширующих серверов описаны в документации **Squid**. Раздел конфигурационного файла, отвечающий за механизм обмена кешем, начинается словами **OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM**.

Важно учитывать, что обмен содержимым кеша между серверами требует обязательной авторизации доступа между серверами для предотвращения подделки данных и других видов атак. Все параметры соединений между серверами (настройка **cache_peer**) задаются в текстовой форме, включая пароли, поэтому доступ к файлу настройки **squid.conf** должен быть строго ограничен.

Обратное проксирование и кеширование внутренних серверов (accelerate)

Функции кеширования и проксирования **Squid** могут использоваться для обработки входящих запросов к внутренним серверам. Такой подход, известный как **обратное проксирование**, позволяет скрывать реальную инфраструктуру серверов и снижать нагрузку на них.

Обычное обратное проксирование (один сервер)

В режиме ускорения (**accelerate**) сервер **Squid** обрабатывает внешние HTTP-запросы, направленные на стандартный **порт 80**. Необходимо указать имя внутреннего сервера и порт, на который будут перенаправляться запросы.

Пример конфигурации:

```
http_port 80 defaultsite=internal.www.com
 cache_peer 192.168.1.1 parent 80 0 no-query originserver
```

Для ограничения доступа к внутреннему серверу можно использовать списки управления доступом (**ACL**).

Множественное проксирование

Для обратного проксирования нескольких внутренних серверов необходимо, чтобы внешние запросы на сайты с разными доменными именами попадали на вход **Squid**, который бы ставил в соответствие каждому имени действительный адрес сервера во внутренней сети и перенаправлял бы запрос туда. Делается это с помощью механизма виртуальных хостов. Вот как, например, можно организовать прокси для двух серверов, **www1.foo.bar** и **www2.foo.bar**, адреса которых в DNS указывают на машину со Squid-сервером (файл **/etc/squid/squid.conf**):

```
http_port 80 defaultsite=www1.foo.bar vhost
 hosts_file /etc/hosts
```

Настройка **defaultsite** нужна серверу для заполнения HTTP-заголовков. Соответствие доменных имён адресам серверов во внутренней сети разумно получать из стандартного файла **/etc/hosts**:

```
10.0.0.1      www1.foo.bar
```

```
10.0.0.2    www2.foo.bar
```

Множественное обратное проксирование имеет важный побочный эффект. В сетях, подключённых к Интернету постоянно, нередки случаи, когда недобросовестные администраторы внутренних сайтов регистрируют их в других доменах и используют их в качестве хостинг-платформ, часто с документами незаконного или нецензурного содержания.

Допустим, сайт **www1.foo.bar** также зарегистрирован как www.verycoolwarez.com, и по этому адресу доступны контрафактные версии программ и т. п. В обычном случае для обнаружения этого факта необходимо анализировать трафик, делать внушение администратору **www1.foo.bar** и т.д. При использовании обратного проксирования такого вообще не может произойти без договорённости с администратором **Squid**, то есть без занесения в **/etc/hosts**.

Разное

Безопасность

Squid поддерживает проксирование разнообразных протоколов, использование которых необходимо контролировать на уровне прав доступа. Если прокси-сервер - анонимизирующий, им могут воспользоваться нарушители, чтобы скрыть обратный адрес при незаконном доступе к данным или даже атаке на другие серверы.

Неправильно настроенный прокси-сервер можно использовать для массовой рассылки почты (спама), что является инцидентом информационой безопасности и может привести к отказу пользователей сети и администраторов почтовых серверов принимать почту из данного домена.

Сбор статистики и ограничение полосы доступа

В **Squid** входит утилита кеш-менеджер, которая служит для сбора статистических данных и загрузки сервера. Кеш-менеджер представляет собой cgi-приложение и должен выполняться под управлением сконфигурированного HTTP-сервера. Все настройки кеш-менеджера производятся в файле **/etc/squid/squid.conf**, строки, которые относятся к кеш-менеджеру, обычно включают **cachemgr**.

При помощи **Squid** можно ограничить полосу пропускания (толщину канала) для пользователей. За это отвечают параметры **delay_pools** и **delay_class**. Эта технология позволит вам снизить загрузку канала, например, большими по объёму медиафайлами, и отдать полосу какому-то более приоритетному трафику.

Кеширование DNS-запросов

Squid содержит встроенный минисервер для обработки **DNS-запросов**. Он выступает как посредник между **Squid** и внешними **DNS-серверами**. При запуске **Squid** выполняет проверку доступности DNS и общего подключения к Интернету. Это можно отключить, используя опцию **-D**. Время кеширования удачного DNS-запроса по умолчанию составляет шесть часов.

Установка и настройка squid

Описание Squid
Установка Squid и настройка в прозрачном режиме работы
Настройка Selinux для Squid
Настройка кэширования
Контроль доступа к сайтам
Перенаправление трафика
Настройка клиента и браузера

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** squid-6.12

Описание Squid

Squid – программа, представляющая собой кэширующий прокси-сервер для протоколов HTTP, HTTPS, FTP и других. Используется для кэширования часто запрашиваемого веб-контента, а также для фильтрации сетевого трафика.

Установка Squid и настройка в прозрачном режиме работы

Установка

Установите прокси-сервер следующей командой:

```
sudo dnf install squid
```

Подготовка сертификатов

Чтобы работал HTTPS, необходимо сгенерировать сертификаты. Для этого создаем папку для хранения сертификатов, например, в **/etc/squid/sslcert**.

```
sudo mkdir /etc/squid/sslcert
```

Переходим в эту папку:

```
cd /etc/squid/sslcert
```

Генерируем ключ:

```
sudo openssl genrsa -out /etc/squid/sslcert/squid.key
```

Создаем **csr**-запрос, используя ключ; нужно будет указать всю необходимую информацию для **csr**:

```
sudo openssl req -new -key /etc/squid/sslcert/squid.key -out /etc/squid/sslcert/squid.csr
```

Пример вывода команды:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Murom
Locality Name (eg, city) [Default City]:Murom
Organization Name (eg, company) [Default Company Ltd]:RS
```

```
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [redsite.ru]:redsite.ru
Email Address []:admin@redsite.ru
A challenge password []:
An optional company name []:
```

Подписываем сертификат самим собой:

```
sudo openssl x509 -req -days 3650 -in /etc/squid/sslcert/squid.csr -signkey /etc/squid/sslcert/squid.key -out /etc/squid/sslcert/squid.pem
```

Генерируем корневой сертификат, который нужно будет добавить в браузер:

```
sudo openssl x509 -in /etc/squid/sslcert/squid.pem -outform DER -out squid.der
```

Далее нужно будет дать права на папку с сертификатами для **squid**:

```
sudo chown -R :squid /etc/squid/sslcert
```

Описание настроек Squid.conf

Открываем файл настроек:

```
sudo nano /etc/squid/squid.conf
```

Блок настроек «**acl localnet src ...**» устанавливает правила доступа для вашей локальной сети, если в списке нет IP-адреса вашей сети, то его нужно добавить, например:

```
acl localnet src 10.9.1.0/24
```

или через файл:

```
acl localnet src "/etc/squid/acl_localnet"
```

* кавычки обязательны
** после необходимо создать файл **/etc/squid/acl_localnet** и с каждой строчки перечислить разрешенные IP-адреса.

Блок настроек **http_access** устанавливает разрешения на доступ; чтобы разрешить весь трафик, добавляем следующую строчку:

```
http_access allow all
```

* важно, чтобы выше она была запрещающей – **http_access deny all**.

Настройка Squid с HTTPS

Открываем файл конфигурации:

```
sudo nano /etc/squid/squid.conf
```

Находим строку с **http_port 3128** и под ней дописываем строки:
- создание прозрачного *HTTP-порта 3129*:

```
http_port 3129 intercept
```

- создание *порта 3130* для https-трафика с генерацией сертификатов по ключу:

```
https_port 3130 intercept ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/sslcert/squid.pem
key=/etc/squid/sslcert/squid.key
```

Отключаем проверку сертификатов:

```
sslproxy_cert_error allow all
```

Указываем, что необходимо принимать сертификаты, даже если они не прошли проверку:

```
sslproxy_flags DONT_VERIFY_PEER
```

Перенаправляем весь трафик на **squid**:

```
always_direct allow all
```

Устанавливаем безопасное соединение с сервером, затем с клиентом, используя имитированный сертификат сервера:

```
ssl_bump server-first all
```

Устанавливаем TCP-туннель, не расшифровывая прокси-трафик:

```
ssl_bump none all
```

Указываем расположение программы генерации сертификатов и устанавливаем кэширование:

```
sslcrtd_program /usr/lib64/squid/security_file_certgen -s /var/lib/ssl_db -M 4MB
```

Сохраняем и закрываем файл **/etc/squid/squid.conf**.

Дальше нужно пересоздать базу данных сертификатов:

```
rm -rf /var/lib/ssl_db
sudo /usr/lib64/squid/security_file_certgen -c -s /var/lib/ssl_db -M 4MB
```

Устанавливаем владельца **squid** на папку базы данных сертификатов:

```
sudo chown -R :squid /var/lib/ssl_db
```

Настройка Selinux для Squid

Добавляем политики:

```
sudo semanage fcontext -a -t squid_conf_t '/var/lib/ssl_db/index.txt'
sudo semanage fcontext -a -t squid_conf_t '/var/lib/ssl_db/size'
```

Применяем политики:

```
sudo /sbin/restorecon -v /var/lib/ssl_db/index.txt
sudo /sbin/restorecon -v /var/lib/ssl_db/size
```

Перезагружаем систему и запускаем squid:

```
sudo systemctl start squid
```

Проверяем работоспособность squid:

```
sudo systemctl status squid
```

При успешно выполненных настройках в статусе должно отображаться **active (running)**.

Добавляем squid в автозагрузку:

```
sudo systemctl enable squid
```

Настройка кэширования

Настройте директорию для кэша в файле **/etc/squid/squid.conf**:

```
cache_dir ufs /var/spool/squid 4096 32 256
```

где:

- **ufs** — файловая система (ufs для SQUID является самой подходящей);
- **/var/spool/squid** — директория хранения кэша;
- **4096** — объем пространства в мегабайтах, которое будет выделено под кэш;
- **32** — количество каталогов первого уровня, которое будет создано для размещения кэша;
- **256** — количество каталогов второго уровня, которое будет создано для размещения кэша.

Теперь создайте структуру папок под кэш следующей командой:

```
sudo squid -z
```

Перезапускаем *squid*:

```
sudo systemctl restart squid
```

Контроль доступа к сайтам

Открываем конфигурационный файл *squid*:

```
nano /etc/squid/squid.conf
```

После строки «**acl Safe_ports port 777**» добавляем:

```
acl CONNECT method CONNECT
acl BLOCKED url_regex -i '/etc/squid/blocklist'
```

Тем самым создается список доступа к сайтам.

Далее перед строкой «**http_access allow localnet**» для блокировки списка доступа прописываем:

```
http_access deny BLOCKED
```

Сохраняем конфигурационный файл.

Создаем файл со списком сайтов для блокировки:

```
sudo nano /etc/squid/blocklist
```

Например, с таким списком сайтов:

```
amazon.com
vk.com
music.yandex.ru
```

Сохраняем файл.

Перечитываем конфигурацию *squid*:

```
sudo systemctl reload squid
```

Блокировка сайтов настроена, осталось только перенаправить трафик на сервер *squid*.

Перенаправление трафика

Установите **iptables**, если пакет еще не установлен:

```
sudo dnf install iptables
```

Включаем **ip_forwarding** для разрешения проходящего трафика:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

Чтобы настройка **ip_forward** не сбрасывалась после перезагрузки, нужно в конце файла **/usr/lib/sysctl.d/50-default.conf** прописать:

```
net.ipv4.ip_forward = 1
```

Добавляем правила для **iptables**:

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3129
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 3130
```

Для тестирования прокси-сервера с локальным трафиком, надо перенаправлять на *Squid* весь трафик, кроме трафика от *Squid*, это можно сделать правилами:

```
sudo iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner squid --dport 80 -j REDIRECT --to-port 3129
sudo iptables -t nat -A OUTPUT -p tcp -m owner ! --uid-owner squid --dport 443 -j REDIRECT --to-port 3130
```

Если нужно сохранить правила *iptables*, чтобы после перезагрузки они не сбрасывались, необходимо ввести команду:

```
sudo service iptables save
```

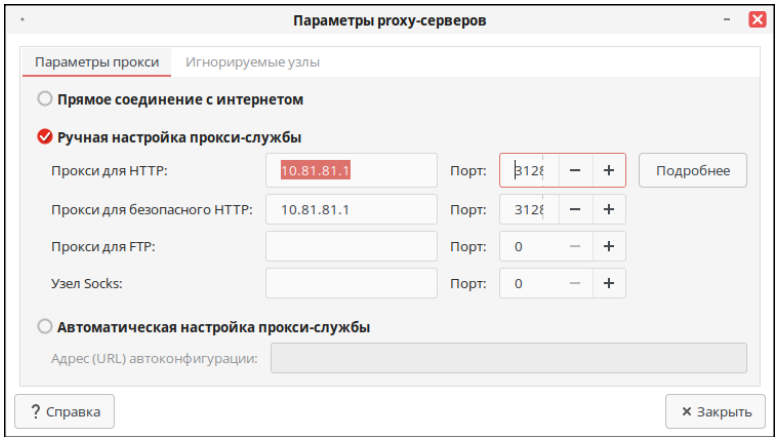
Перезапускаем *squid*:

```
sudo systemctl restart squid
```

Настройка клиента и браузера

В РЕД ОС откройте «**Главное меню**» — «**Параметры**» — «**Прокси-сервер**».

Для ручной настройки подключения к прокси заполните поля адреса сервера и порт (3128):



Настройка браузера

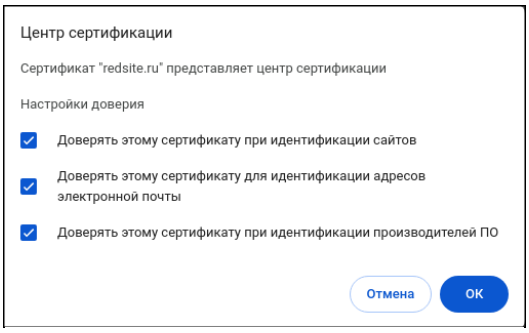
Сейчас большинство сайтов используют технологию **HSTS** для предотвращения *MiTM*-атак, поэтому если вы хотите настроить *Squid* для фильтрации трафика в своей организации, вам следует добавить сертификат **.der**. Рассмотрим на примере *Chrome*.

В меню браузера переходим по пути: **Настройки->Конфиденциальность и безопасность->Безопасность->Настроить сертификаты->Центры сертификации->Импорт**.

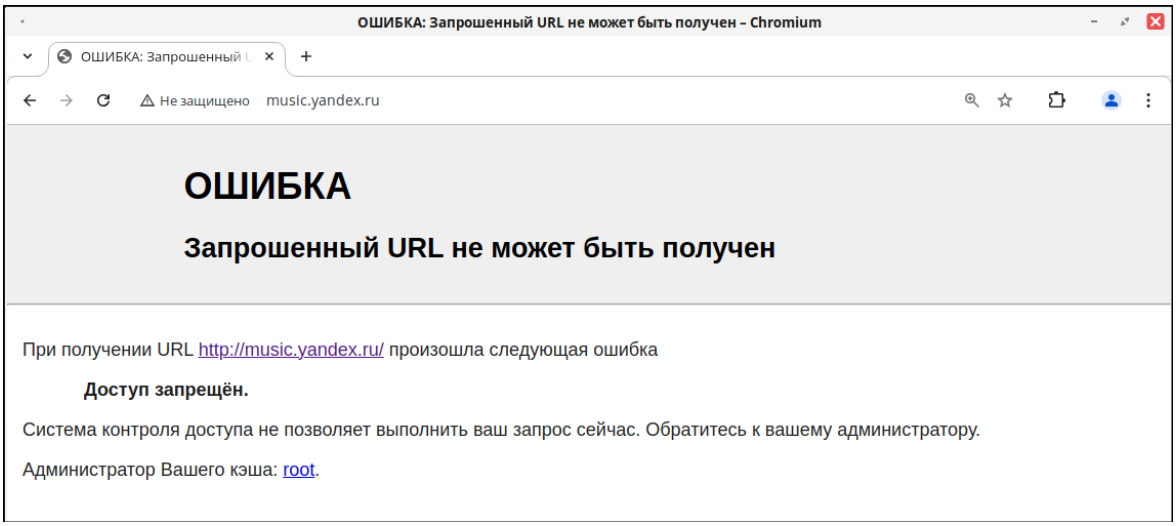
Добавляем созданный ранее сертификат для браузера по пути:

```
/etc/squid/sslcert/squid.pem
```

Устанавливаем все галочки и нажимаем «**OK**».



Если все сделано правильно, то при входе на запрещенный сайт должна отобразиться такая страница:



Настройка автоматической авторизации доменных пользователей IPA в squid

Ввод сервера squid в домен IPA:

Для ввода сервера в домен IPA выполните команду:

```
# ipa-client-install --enable-dns-updates --mkhomedir
```

ВАЖНО

Проверьте правильность записи DNS в файле /etc/resolv.conf, должен быть указан DNS контроллера домена IPA. Более подробно о вводе в домен написано в статье «Ввод клиентских машин в домен IPA».

Установка squid

Для установки squid выполните команду:

```
# dnf install squid
```

Добавьте сервис в автозагрузку, выполнив команду:

```
# systemctl enable squid
```

Настройка конфигурации squid

Отредактируйте файл /etc/squid/squid.conf любым текстовым редактором

```
# vi /etc/squid/squid.conf
```

Добавьте строки для включения авторизации через kerberos

```
auth_param negotiate program /usr/lib64/squid/negotiate_kerberos_auth -d -s HTTP/squid.example.com
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl auth proxy_auth REQUIRED
```

Закомментируйте строки

```
#http_access allow localnet
#http_access allow localhost
```

Добавьте следующие строки

```
http_access deny !auth
http_access allow auth
```

Создание kerberos keytab для доступа Squid HTTP

На сервере IPA выполните:

```
# kinit admin
Password for admin@EXAMPLE.COM:
# ipa service-add HTTP/squid.example.com
```

Вывод команды должен быть следующим:

```
----------------------------------------------------
Added service "HTTP/squid.example.com@EXAMPLE.COM"
----------------------------------------------------
```

```
  Principal: HTTP/squid.example.com@EXAMPLE.COM
  Managed by: squid.example.com
```

На сервере squid выполните:

```
# kinit admin
# ipa-getkeytab -s dc.example.com -p HTTP/squid.example.com -k /etc/squid/krb5.keytab
```

При правильном выполнении команды выведет:

```
Keytab successfully retrieved and stored in: /etc/squid/krb5.keytab
```

Измените права доступа к файлу /etc/squid/krb5.keytab

```
# chown root:squid /etc/squid/krb5.keytab
# chmod 640 /etc/squid/krb5.keytab
```

Отредактируйте файл /etc/sysconfig/squid и добавьте в него следующие строки:

```
KRB5_KTNAME=/etc/squid/krb5.keytab export KRB5_KTNAME
```

Перезапустите squid

```
#systemctl restart squid
```

Откройте порт в IPTables:

```
# iptables -I INPUT -p tcp --dport 3128 -j ACCEPT
# service iptables save
```

Настройка высокодоступного прокси-сервера HAProxy

Предварительная настройка
Отключение SELinux
Базовая настройка HAProxy
Настройка веб-серверов
Настройка сервера nginx
Настройка сервера apache2 (httpd)
Проверка работоспособности HAProxy

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический, сервер минимальный
- **Версия ПО**: haproxy-2.6.11-2

HAProxy – программное обеспечение с открытым исходным кодом, которое обеспечивает высокодоступный балансировщик нагрузки и прокси-сервер для приложений на основе **TCP** и **HTTP**, распределяющих запросы между несколькими серверами.

Предварительная настройка

Дальнейшая настройка должна выполняться с правами администратора системы (**sudo**) или суперпользователя **root** (**su**), если не указано иное. В текущей инструкции команды будут выполнены с правами суперпользователя **root**. Для перехода в сеанс суперпользователя выполните:

```
su -
```

Перед настройкой на всех машинах необходимо установить последние обновления:

```
dnf update
```

Отключение SELinux

На время установки и настройки **HAProxy** необходимо переключить SELinux в режим уведомлений.

Для этого в файле конфигурации **/etc/selinux/config** замените режим `enforcing` на `permissive` командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

Для применения изменений перезапустите систему.

Статус службы SELinux можно просмотреть командой:

```
sestatus
```

Базовая настройка HAProxy

Для установки **HAProxy** выполните команду:

```
dnf install haproxy
```

После установки **HAProxy** будет автоматически запущена служба **haproxy**. Для проверки статуса службы выполните команду:

```
systemctl status haproxy
```

В статусе должно отображаться **active (running)**.

Для автоматического запуска службы после перезагрузки сервера выполните команду:

```
systemctl enable haproxy
```

Перед началом настройки рекомендуется создать резервную копию файла конфигурации:

```
cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.bk
```

Для настройки откройте конфигурационный файл HAProxy:

```
nano /etc/haproxy/haproxy.cfg
```

Файл конфигураций состоит из следующих секций:

- `global` – содержит системные настройки и отвечает за более гибкую настройку производительности и безопасности;
- `defaults` – стандартные настройки, которые должны работать без дополнительных изменений. Также здесь находятся настройки времени ожидания и отчетов ошибок;
- `frontend` – настройки *frontend*-сервера, на котором установлен **haproxy**;
- `backend` – информация о *backend*-серверах и режиме балансировки;
- `listen` – дополнительные настройки, позволяющие включить мониторинг статистики.

Выбор режимов балансировки:

- **roundrobin** — режим, при котором **HAProxy** выбирает сервера по очереди, равномерно распределяя нагрузку;
- **leastconn** — в этом режиме запросы направляются к серверу, у которого меньше всего подключений, рекомендуется использовать для долгих сессий;
- **source** — режим выбирает сервер на основе хэша источника IP-адреса, с которого клиенты отправляют запросы, это гарантирует, что одни и те же пользователи используют один и тот же сервер.

Добавьте в секцию `frontend` следующее содержимое:

```
frontend haproxy      # имя фронтенда
 bind 192.168.1.1:80   # IP-адрес сервера с HAproxy
 stats uri /haproxy?stats    # адрес веб-интерфейса мониторинга
 default_backend webservers  # имя нужного бэкенда
```

В секцию `backend` добавьте следующее содержимое:

```
backend webservers    # имя бэкэнда
 balance roundrobin    # режим балансировки
 server web1.example.com 192.168.1.2:80    # имя и адрес веб-серверов
 server web2.example.com 192.168.1.3:80
```

Для включения статистики в секцию `listen` добавьте:

```
listen stats
 bind *:8080
 stats enable
 stats uri /
 stats refresh 5s
 stats realm Haproxy\ Stats
 stats auth Login:Password    #логин и пароль для подключения к веб-интерфейсу мониторинга
```

После сохранения изменений в файле конфигурации проверьте корректность файла, выполнив команду:

```
haproxy -f /etc/haproxy/haproxy.cfg -c
```

Если все настроено правильно, ответ должен выглядеть следующим образом:

```
Configuration file is valid
```

Для применения внесенных изменений перезапустите службу:

```
systemctl restart haproxy
```

ВАЖНО!

Если DNS-сервер не настроен, необходимо прописать веб-сервера в файл **/etc/hosts**:

```
192.168.1.1  haproxy
192.168.1.2  web1.example.com
192.168.1.3  web2.example.com
```

Настройка веб-серверов

В рамках данной статьи для проверки работы **haproxy** будет рассмотрена настройка двух серверов – **nginx** и **apache2** (**httpd**).

Настройка сервера nginx

Для установки **nginx** выполните команду:

```
dnf install nginx
```

Запустите службу **nginx** и добавьте ее в автозагрузку:

```
systemctl enable nginx --now
```

Проверьте статус службы:

```
systemctl status nginx
```

В статусе должно отображаться **active (running)**.

Для настройки сервера откройте файл конфигурации **nginx.conf**:

```
nano /etc/nginx/nginx.conf
```

В секцию server добавьте следующее содержимое:

```
server_name web1.example.com;     # укажите имя веб-сервера или IP-адрес
```

Выполните проверку настроек **nginx**:

```
nginx -t
```

Если файл конфигурации настроек верно, вывод должен иметь вид:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Для применения конфигурации перезапустите веб-сервер:

```
systemctl restart nginx
```

Настройка сервера apache2 (httpd)

Для установки **apache2** (**httpd**) выполните команду:

```
dnf install httpd
```

Запустите службу **httpd** и добавьте ее в автозагрузку:

```
systemctl enable httpd --now
```

Проверьте статус службы:

```
systemctl status httpd
```

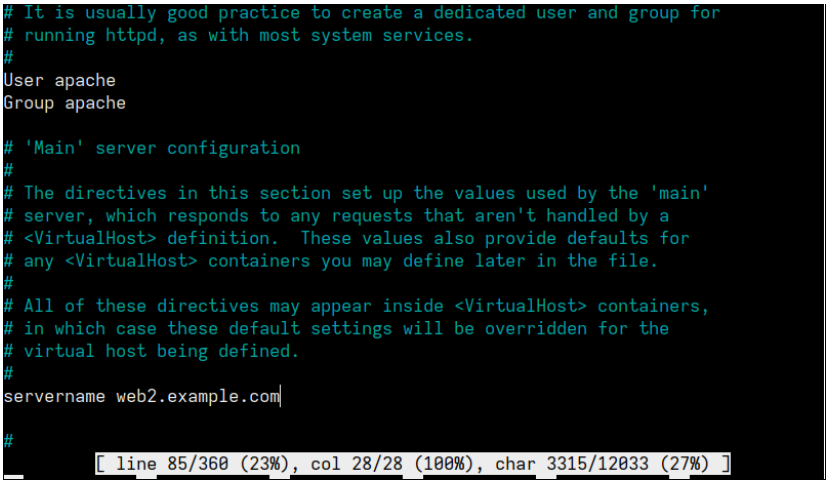
В статусе должно отображаться **active (running)**.

Для настройки сервера откройте файл конфигурации **httpd.conf**:

```
nano /etc/httpd/conf/httpd.conf
```

В секцию 'Main' server configuration добавьте следующее содержимое:

```
servername web1.example.com     # укажите имя веб-сервера или IP-адрес
```

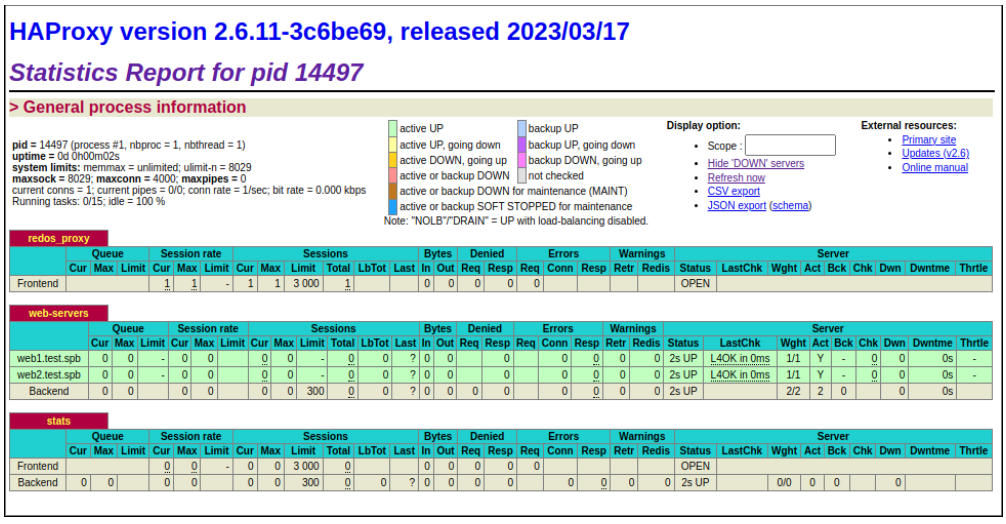


Для применения конфигурации перезапустите службу:

```
systemctl restart httpd
```

Проверка работоспособности HAProxy

Ранее был настроен сбор статистики для **HAProxy**. Для доступа к просмотру собранной статистики откройте браузер и в адресной строке введите **<IP-адрес_HAProxy>/haproxy?stats**.



Если сервер в списке подсвечен *зеленым цветом*, значит настройка была произведена корректно.

Если серверы подсвечены *красным цветом*, значит настройка была выполнена неверно либо сервер не включен. Также в статистике отображено, что весь трафик уходит на единственный рабочий сервер.

web-servers

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
web1.test.spb	0	0	-	0	257		0	5	-	1 000	1 000	11s	157 000	356 000		0		0	0	0	0	2m18s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-
web2.test.spb	0	0	-	0	0		0	0	-	0	0	?	0	0		0		0	0	0	0	2m17s DOWN	L4CON in 0ms	1/1	Y	-	1	1	2m17s	-
Backend	0	0		0	257		0	5	300	1 000	1 000	11s	157 000	356 000	0	0		0	0	0	0	2m18s UP		1/1	1	0		0	0s	

При правильной работе в режиме **roundrobin** трафик распределяется равномерно:

redos_proxy

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				41	235	-	2	29	3 000	1 006			160 624	543 753	0	0	2					OPEN								

web-servers

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
web1.test.spb	0	0	-	26	120		0	2	-	500	500	1s	78 500	178 000		0		0	0	0	0	1m36s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-
web2.test.spb	0	0	-	25	120		0	2	-	500	500	1s	78 500	178 000		0		0	0	0	0	19s UP	L4OK in 1ms	1/1	Y	-	1	1	1m16s	-
Backend	0	0		52	240		0	4	300	1 000	1 000	1s	157 000	356 000	0	0		0	0	0	0	1m36s UP		2/2	2	0		0	0s	

stats

	Queue			Session rate			Sessions						Bytes		Denied		Errors			Warnings		Server							
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
Frontend				0	0	-	0	0	3 000	0			0	0	0	0	0					OPEN								
Backend	0	0		0	0		0	0	300	0	0	?	0	0	0	0		0	0	0	0	1m36s UP		0/0	0	0		0		

Настройка прокси-сервера 3proxy

Установка и настройка
Настройка доступа

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: 3proxy-0.9.3-1

Установка и настройка

3proxy – бесплатный кроссплатформенный прокси-сервер. Не имеет графического интерфейса, настройка производится путем написания конфигурационного файла.

Основными особенностями являются:

- поддержка протоколов HTTP, HTTPS, SOCKS v4, SOCKS v4a, SOCKS v5, SMTP;
- переадресация TCP и UDP трафика;
- объединение прокси-серверов в цепочку и функции обратного соединения;
- ограничение пропускной способности канала и трафика;
- контроль доступа (ACL);
- ведение журналов;
- поддержка IPv6.

Для установки ПО перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install 3proxy
```

Далее необходимо настроить конфигурационный файл прокси-сервера. Он располагается по пути **/etc/3proxy**. Откройте файл и добавьте в него следующее содержимое:

```
nano /etc/3proxy/3proxy.cfg
```

```
#!/bin/3proxy
# DNS-сервера (указываем желаемые DNS-сервера, либо смотрим в /etc/resolv.conf)
nserver 77.8.8.8
nserver 77.8.8.1
# Режим запуска daemon
daemon
# IP-адрес внешнего интерфейса (без кавычек)
external <IP-адрес>
# IP-адрес адрес внутреннего интерфейса (без кавычек)
internal <IP-адрес>
# запуск http proxy на порту 4555
proxy -p4555 -n -a
# запуск ftp proxy на порту 4556
ftppr -p4556
# socks proxy на порту 2333
socks -p2333
# путь к логам и формат лога
log /var/log/3proxy/3proxy.log D
logformat "- +_L%t.%. %N.%p %E %U %C:%c %R:%r %O %I %h %T"
rotate 30
```

```
# Размер кэша запросов DNS. Стандартное значение, в килобайтах
nscache 65536
# Стандартные таймауты
timeouts 1 5 30 60 180 1800 15 60
```

Для упрощения работы с **3proxy** создайте для него собственный сервис для управления через **systemd**:

```
touch /etc/systemd/system/3proxy.service
chmod 664 /etc/systemd/system/3proxy.service
nano /etc/systemd/system/3proxy.service
```

Добавьте в описание сервиса следующее содержимое:

```
[Unit]
Description=3proxy Proxy Server
After=network.target
[Service]
Type=simple
ExecStart=/usr/bin/3proxy /etc/3proxy/3proxy.cfg
ExecStop=/bin/kill /usr/bin/pgrep 3proxy
RemainAfterExit=yes
Restart=on-failure
[Install]
WantedBy=multi-user.target
```

После проведенных манипуляций необходимо обновить конфигурацию **systemd** командой:

```
systemctl daemon-reload
```

Затем добавьте сервис в автозагрузку и запустите его:

```
systemctl enable 3proxy --now
```

Проверьте статус сервиса:

```
systemctl status 3proxy
```

В статусе должно быть отображено **active (exited)**.

```
● 3proxy.service - 3proxy Proxy Server
     Loaded: loaded (/etc/systemd/system/3proxy.service; enabled; vendor preset: disabled)
     Active: active (exited) since Tue 2023-01-24 16:42:34 MSK; 2s ago
    Process: 24909 ExecStart=/usr/bin/3proxy /etc/3proxy/3proxy.cfg (code=exited, status=0/SUCCESS)
   Main PID: 24909 (code=exited, status=0/SUCCESS)
        CPU: 2ms

янв 24 16:42:34 localhost.localdomain systemd[1]: Started 3proxy Proxy Server.
```

Настройка доступа

Если доступ к прокси необходимо настроить по паролю, в конфигурационном файле для этого добавьте следующие строки:

```
auth cache strong
users "user1:CL:password1"
users "user2:CR:password2"
```

Пользователи добавляются строкой `users "<имя_пользователя>:<тип_пароля>:<пароль>"`.

Существует два типа хранения пароля:

- **CL** – пароль пользователя указывается в открытом виде, непосредственно в конфигурационном файле;
- **CR** – зашифрованный пароль (**md5**), можно получить с помощью команды `openssl passwd`.

Для ограничения доступа пользователей к определенным IP-адресам в конфигурационном файле следует добавить строки:

```
deny user1 * 192.168.0.1
allow *
```

где:

- **user1** – имя пользователя, которому запрещен доступ к ресурсу;
- **192.168.0.1** – IP-адрес, к которому запрещен доступ;
- **allow *** - разрешение доступа ко всем остальным ресурсам.

Чтобы запретить всем пользователям доступ к адресу, вместо имени пользователя указывается «*».

```
deny * * 192.168.0.1
allow *
```

Настройка ЕСПД (Единая Сеть Передачи Данных от Ростелеком)

Установка корневого сертификата
Установка сертификата с использованием интернет-браузера Firefox
Установка сертификата с использованием веб-браузера Chromium
Настройка прокси-сервера

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: chromium-94.0.4606.81, firefox-102.9.0

ЕСПД (Единая Сеть Передачи Данных) — это совокупность сетей в разных регионах Российской Федерации, объединенных в единую систему с централизованным управлением и фильтрацией трафика, подключение к которой в скором времени станет обязательным для всех государственных и муниципальных учреждений и органов власти. Оператором ЕСПД является *Ростелеком* (РТ).

Настройка подразумевает установку корневого сертификата и указания прокси-сервера, через который проходит весь трафик. Сертификат можно скачать с официального сайта Ростелеком — https://espd.wifi.rt.ru/settings/cert-install.

Установка корневого сертификата

Перед установкой корневой сертификат необходимо скопировать в центры сертификации ОС. Для этого перейдите в сеанс суперпользователя **root**:

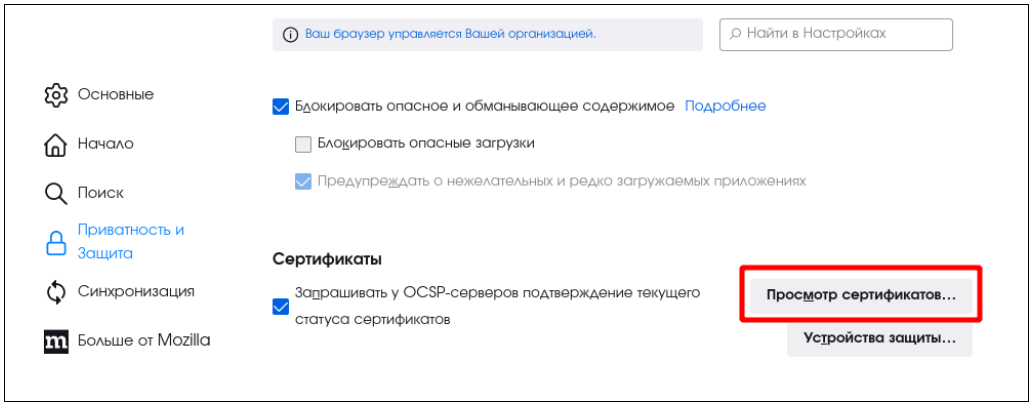
```
su -
```

и выполните следующие команды:

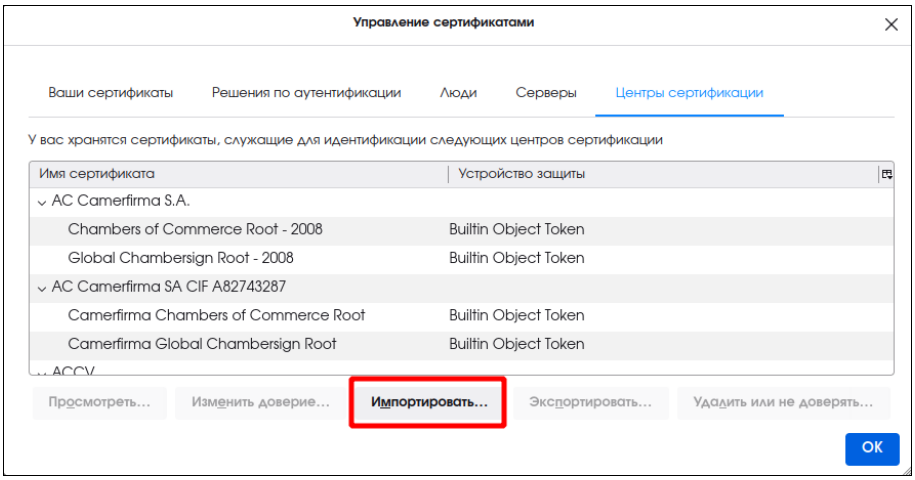
```
update-ca-trust
cp /<путь_до_сертификата>/ca-root.crt /etc/pki/ca-trust/source/anchors/
update-ca-trust extract
```

Установка сертификата с использованием интернет-браузера Firefox

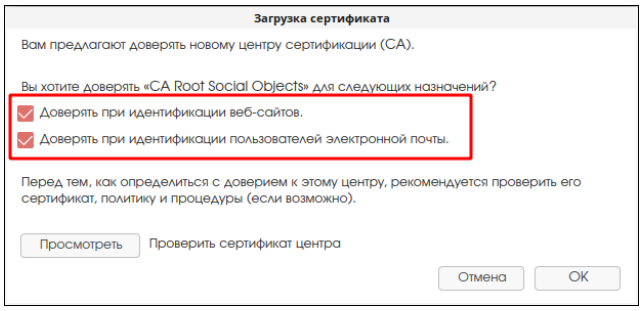
Установите сертификат Ростелекома в **Firefox**. Для этого перейдите в «**Настройки**» браузера, откройте вкладку «**Приватность и защита**», перейдите к разделу «**Сертификаты**» и нажмите «**Просмотр сертификатов...**».



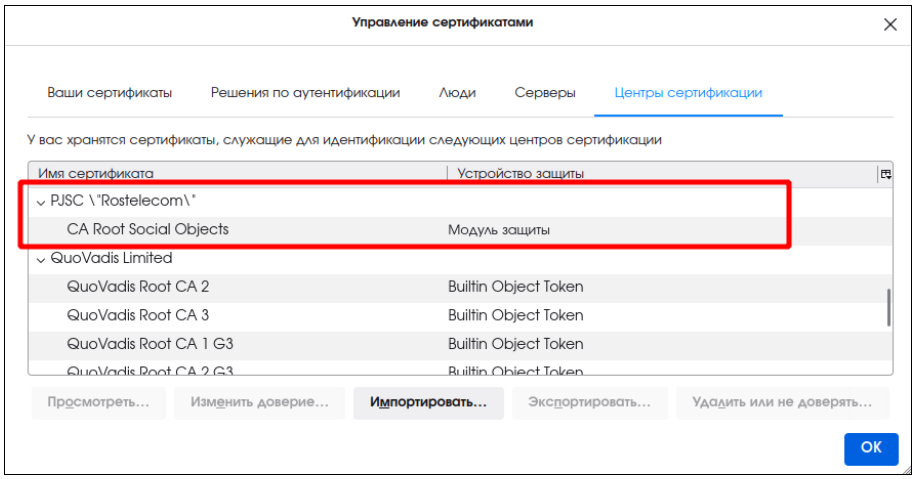
Затем откройте вкладку «**Центры сертификации**» и нажмите «**Импортировать...**».



При импорте сертификата необходимо разрешить доверие данному сертификату, установив соответствующие флаги.

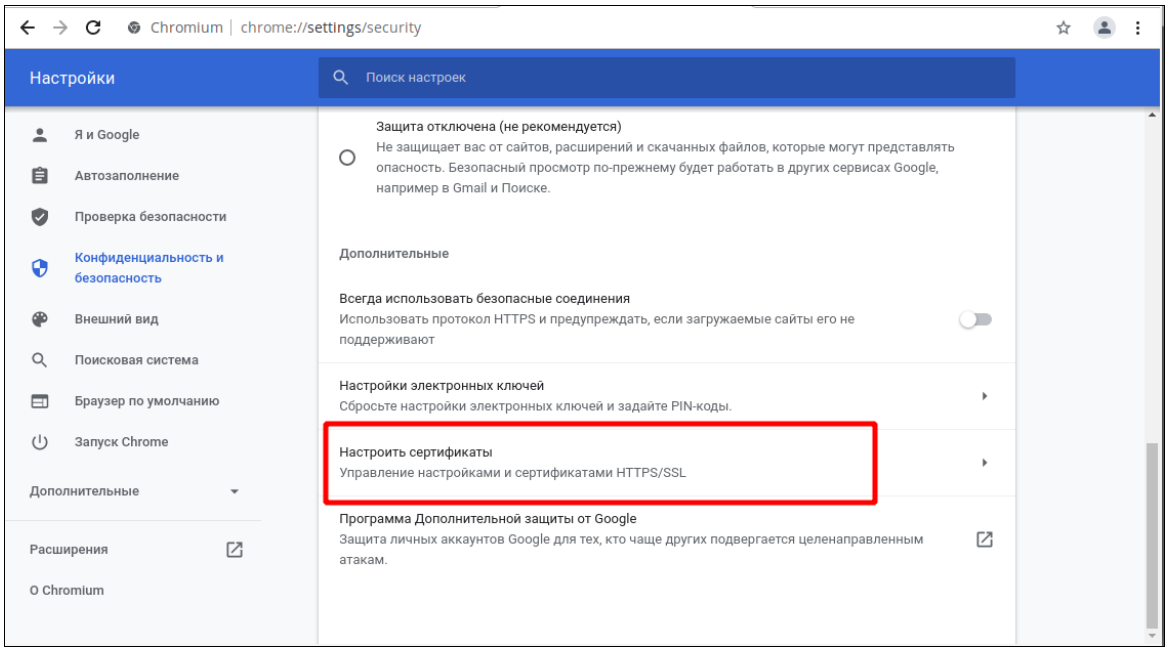


Убедитесь, что сертификат был установлен.

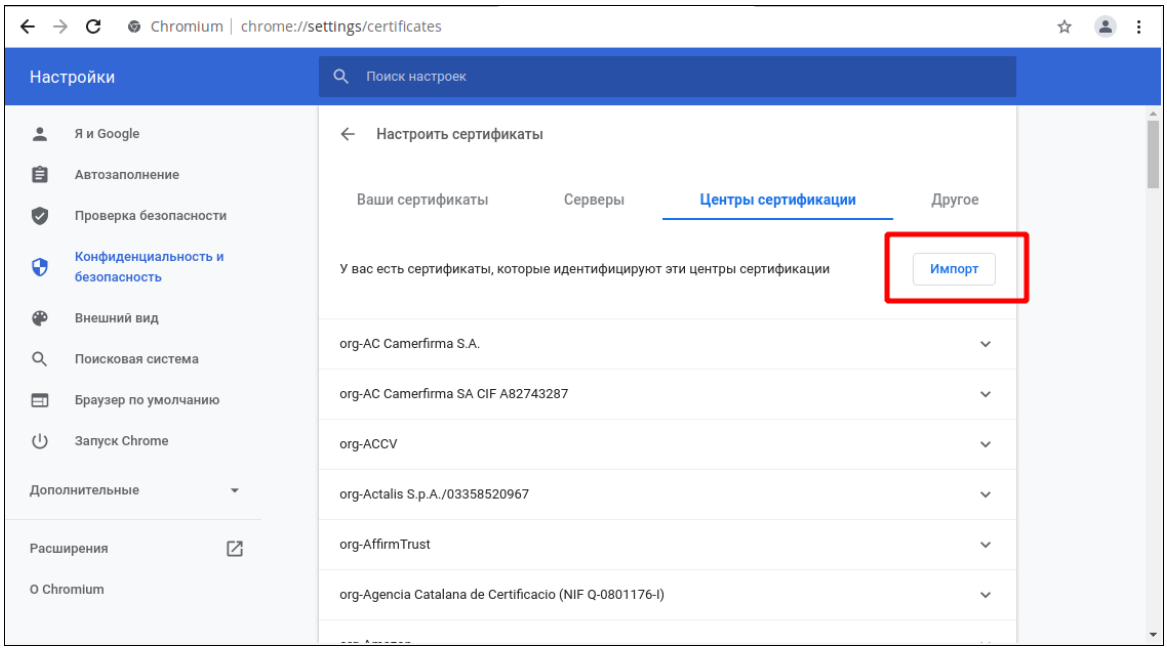


Установка сертификата с использованием веб-браузера Chromium

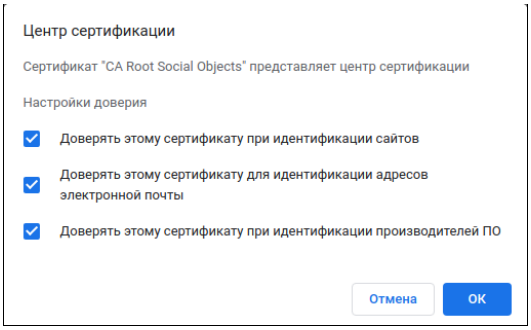
Для установки сертификата Ростелекома в **Chromium** перейдите в «**Настройки**» — «**Конфиденциальность и безопасность**», откройте раздел «**Безопасность**» и нажмите «**Настроить сертификаты**».



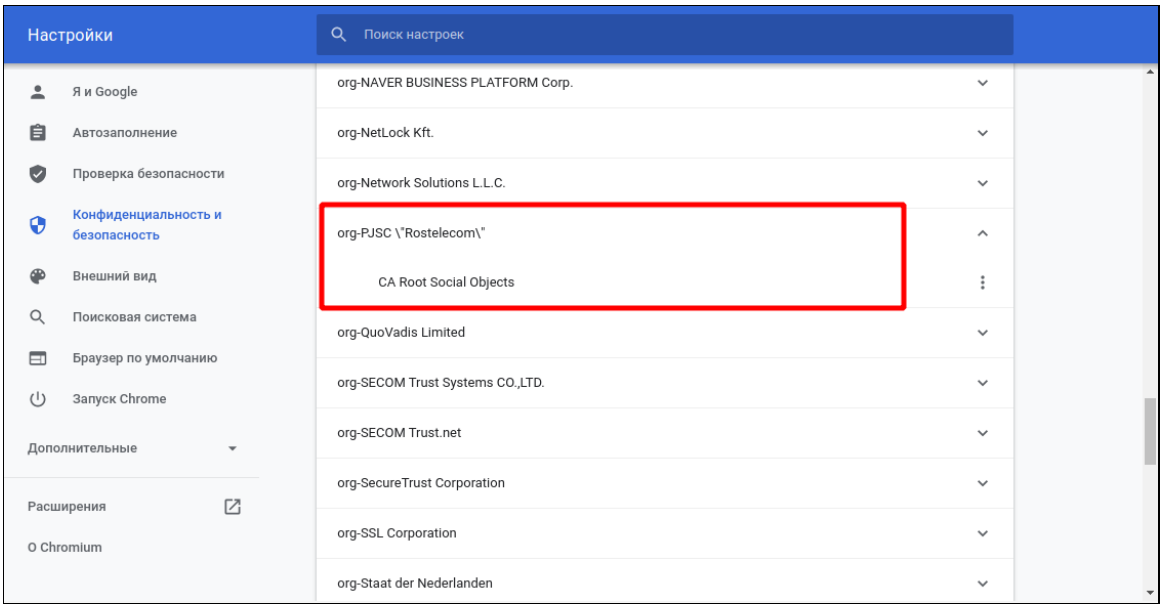
Откройте вкладку «**Центры сертификации**» и нажмите «**Импорт**».



При импорте сертификата необходимо разрешить доверие данному сертификату, установив соответствующие флаги.



Убедитесь, что сертификат был установлен.



Настройка прокси-сервера

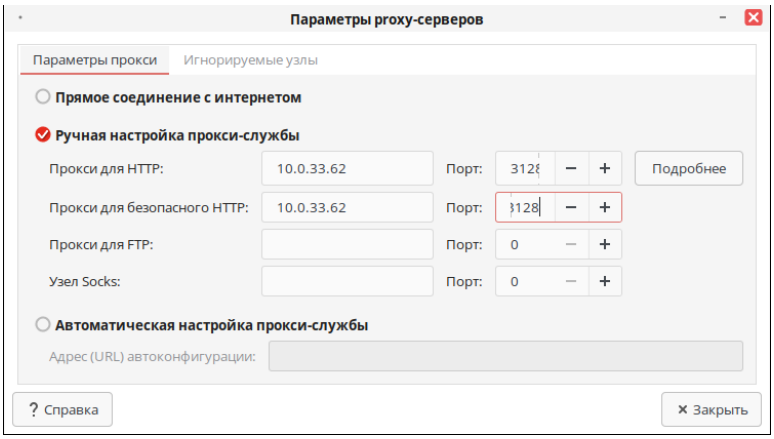
Для настройки прокси-сервера перейдите в «**Главное меню**» — «**Параметры**» — «**Прокси-сервер**».

Выберите пункт «**Ручная настройка прокси-службы**».

Укажите *адрес* и *порт* подключения прокси-сервера для параметров «**Прокси для HTTP**» и «**Прокси для безопасного HTTP**».

Примечание.

Адрес и *порт* прокси-сервера **выдаются провайдером Ростелеком**, по умолчанию используется порт **3128**.



После настройки необходимо проверить доступ к сети Интернет, если сайты загружаются успешно, значит настройка выполнена верно.

Настройка прокси на клиентских ПК

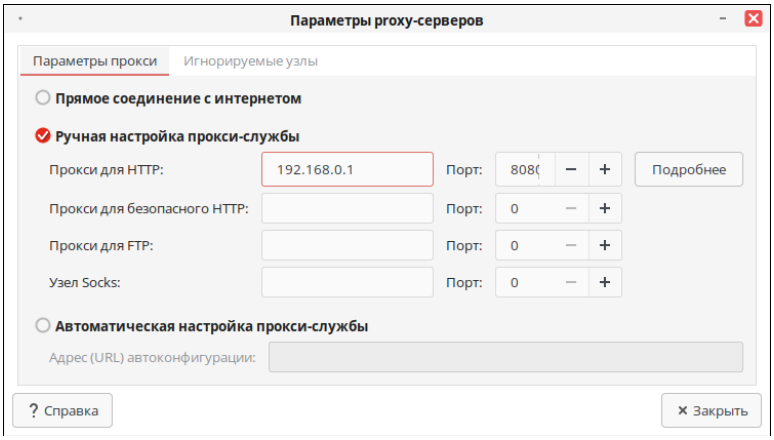
Настройка прокси для приложений графической среды
Настройка прокси в графическом интерфейсе
Настройка прокси посредством gsettings
Настройка прокси для терминальных приложений
Общесистемные настройки прокси для терминальных приложений
Настройка dnf для работы через прокси
Настройка wget для работы через прокси

Настройка прокси для приложений графической среды

Настройка прокси в графическом интерфейсе

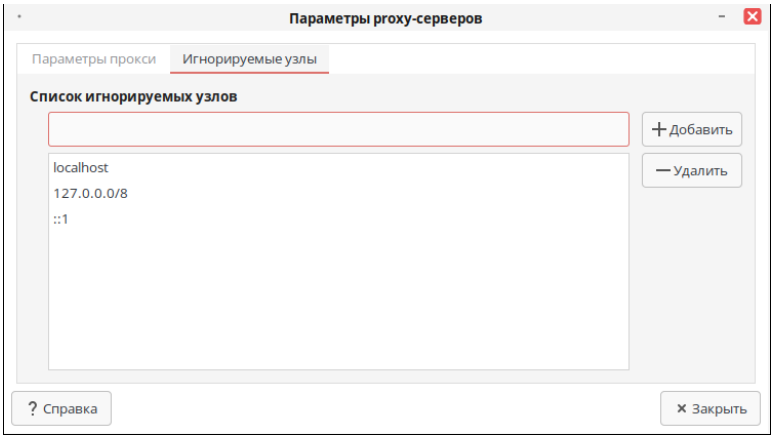
Для настройки прокси-сервера через графический интерфейс в *среде рабочего стола MATE* откройте утилиту «**Прокси-сервер**» из «**Главного меню**» - «**Параметры**».

В открывшемся окне выберите «**Ручная настройка прокси-службы**» и введите *ip-адрес* или *сетевое имя* прокси сервера и его *порт*.

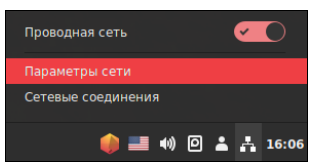


Если у вас настроена автоконфигурация на прокси-сервере, выберите пункт «**Автоматическая настройка прокси-службы**».

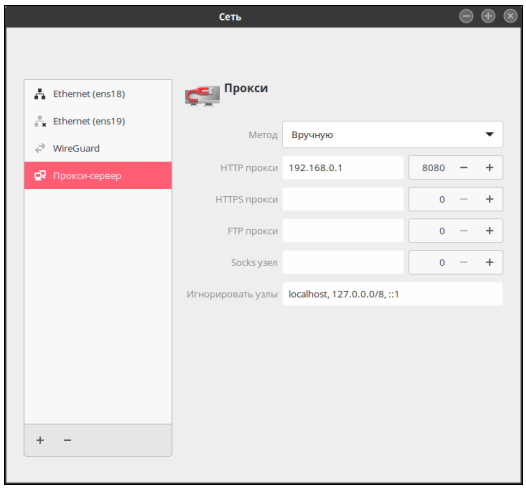
Список игнорируемых узлов на вкладке «**Игнорируемые узлы**» позволяет задать те узлы, для подключения к которым не нужно использовать прокси. Подключение к указанным в этом списке узлам будет выполняться напрямую через Интернет, без использования прокси-сервера.



Для настройки прокси-сервера через графический интерфейс в *среде рабочего стола Cinnamon* откройте «**Параметры сети**», нажав по иконке «**Сетевых соединений**» в трее.



В открывшемся окне откройте настройки для **Прокси-сервера**, выберите для поля «**Метод**» значение «**Вручную**» и укажите *IP-адрес* и *порт* для **HTTP прокси**.



Настройка прокси посредством gsettings

Для установки параметров прокси текущего пользователя из командной строки следует воспользоваться утилитой **gsettings**. Синтаксис и примеры использования приведены в нашей статье «Управление Dconf» в соответствующем разделе.

Схемы и ключи **dconf**-настроек прокси:

Схема	Ключ	Описание
org.gnome.system.proxy	**ignore-hosts**	Список узлов-исключений, которые используют подключение напрямую, а не через прокси-сервер. Пример создания списка исключений будет приведен ниже.
	mode	Режим настройки прокси. Возможные значения: “*none*” - без прокси, “*manual*” - ручная настройка, “*auto*” - автоматическая настройка.
	autoconfig-url	URL для автоматической конфигурации прокси.
org.gnome.system.proxy.http	**use-authentication**	Указание применения аутентификации (только для HTTP-протокола). Возможные значения: *true*, *false*.
	authentication-user	Имя пользователя для аутентификации по HTTP.
	authentication-password	Пароль для аутентификации по HTTP.
org.gnome.system.proxy.http (https/ftp/socks)	**host**	Имя или IP-адрес используемого прокси-сервера для указанного в схеме протокола.
	port	Числовое значение порта прокси-сервера для указанного в схеме протокола.

Пример команды для указания списка узлов-исключений:

```
gsettings set org.gnome.system.proxy ignore-hosts "['localhost', '127.0.0.0/8', '::1', 'someaddress.here', '*.localportal.work']"
```

Пример команд для указания параметров https-прокси:

```
gsettings set org.gnome.system.proxy mode 'manual'
gsettings set org.gnome.system.proxy.https host 'proxy.work'
gsettings set org.gnome.system.proxy.https port 8085
```

Сброс параметров настроек прокси до значений по умолчанию, заданных в системе:

```
gsettings reset-recursively org.gnome.system.proxy
```

Задание настроек прокси по умолчанию для всей системы производится аналогично действиям из соответствующего раздела в нашей статье «Управление Dconf». В этой же статье описана возможность принудительного применения и блокировки параметров, которая позволит установить настройки в качестве неизменяемых общесистемных (для приложений графической среды).

Примечание.

Браузеры на основе **Chrome** не используют параметры **dconf** при входе через **sddm**.

Настройка прокси для терминальных приложений

Общесистемные настройки прокси для терминальных приложений

Настройка производится установкой значений глобальных переменных окружения путем создания файла **/etc/profile.d/proxy_set.sh**:

```
sudo nano /etc/profile.d/proxy_set.sh
```

В него необходимо поместить следующие строки (**proxyserver** и **port** заменить на адрес и порт вашего прокси-сервера):

```
export {http,ftp,https,rsync}_proxy="http://proxyserver:port"
export {HTTP,FTP,HTTPS,RSYNC}_PROXY=$http_proxy
```

Настройки будут применены после перезагрузки компьютера.

Примечание.

Если необходимо настроить прокси для конкретного пользователя, то необходимо изменить файл **.bash_profile** в домашней директории пользователя, добавив в конец файла вышеприведенные строки. Примените настройки выходом/входом в систему, затем выполните:

```
source ~/.bash_profile
```

Примечание.

Если необходимо указать имя пользователя и пароль, то они указываются в следующем формате:

```
MY_PROXY_URL="http://user:password@ServerProxy:8080/"
```

Настройка dnf для работы через прокси

По умолчанию **dnf** получает данные с HTTP-сервера. Все соединения **dnf** с HTTP происходят с использованием **HTTP / 1.1** протокола и совместимых с ним веб прокси-серверов.

Если вам необходимо разрешить доступ к **dnf** через proxy-сервер для всех пользователей, используйте файл **/etc/dnf/dnf.conf** и внесите в раздел [main] данные прокси и данные для аутентификации:

```
[main]
proxy=http://proxy.mydomain.com:3128
proxy_username=user_proxy
proxy_password=pass_user_proxy
```

В данном примере параметр:

- **proxy.mydomain.com** — адрес вашего proxy-сервера **:порт**;
- **proxy_username** — имя пользователя;
- **proxy_password** — пароль пользователя.

Если ваш proxy-сервер не использует авторизацию, достаточно прописать только:

```
proxy=http://proxy.mydomain.com:3128
```

Таким образом, файл `/etc/dnf/dnf.conf` требуется для настройки работы **dnf** через прокси для всех пользователей.

Чтобы разрешить доступ **dnf** через proxy-сервер для конкретного пользователя, вам необходимо использовать файл профиля пользователя. По умолчанию это **~/.bash_profile** в домашнем каталоге пользователя. Внесите в него следующие строчки:

```
http_proxy="http://mycache.mydomain.com:3128"
export http_proxy
```

Если для работы proxy сервера необходимо использовать логин-пароль, то добавьте их в строчку **http_proxy**:

```
http_proxy="http://user_proxy:pass_user_proxy@proxy.mydomain.com:3128"
```

Настройка wget для работы через прокси

Откройте конфигурационный файл **wget**:

```
nano /etc/wgetrc
```

и добавьте следующие строки:

```
http_proxy=http://xxx.xxx.xx.xx:8080
https_proxy=http://xxx.xxx.xx.xx:8080
proxy_user=domain\user
proxy_passwd=password
```

Настройка брандмауэра Firewall

Базовые понятия брандмауэра
Базовые понятия брандмауэра. Зоны
Базовые понятия брандмауэра. Сохранение правил
Включение брандмауэра firewalld
Включение брандмауэра firewalld. Просмотр правил по умолчанию
Включение брандмауэра firewalld. Другие зоны брандмауэра
Настройка зон интерфейсов
Настройка зон интерфейсов. Изменение зоны интерфейса на одну сессию
Настройка зон интерфейсов. Изменение зоны интерфейса на постоянной основе
Настройка зон интерфейсов. Настройка зоны по умолчанию
Создание правил для приложений. Добавление сервиса в зону
Что делать, если нужный сервис недоступен?
Способ 1: Настройка порта
Способ 2: Определение сервиса
Создание зон
Автоматический запуск брандмауэра
Заключение

Базовые понятия брандмауэра

Зоны

Демон firewalld управляет группами правил при помощи так называемых зон.

Зоны – это, по сути, наборы правил, которые управляют трафиком на основе уровня доверия к той или иной сети. Зоны присваиваются сетевым интерфейсам и управляют поведением брандмауэра.

Компьютеры, которые часто подключаются к разным сетям (например, ноутбуки) могут использовать зоны, чтобы изменять наборы правил в зависимости от среды. К примеру, при подключении к общественной сети WiFi брандмауэр может применять более строгие правила, а в домашней сети ослаблять ограничения.

В firewalld существуют следующие зоны:

- **drop**: самый низкий уровень доверия сети. Весь входящий трафик сбрасывается без ответа, поддерживаются только исходящие соединения.
- **block**: эта зона похожа на предыдущую, но при этом входящие запросы сбрасываются с сообщением icmp-host-prohibited или icmp6-adm-prohibited.
- **public**: эта зона представляет публичную сеть, которой нельзя доверять, однако поддерживает входящие соединения в индивидуальном порядке.
- **external**: зона внешних сетей. Поддерживает маскировку NAT, благодаря чему внутренняя сеть остается закрытой, но с возможностью получения доступа.
- **internal**: обратная сторона зоны external, внутренние сети. Компьютерам в этой зоне можно доверять. Доступны дополнительные сервисы.
- **dmz**: используется для компьютеров, расположенных в DMZ (изолированных компьютеров, которые не будут иметь доступа к остальной части сети); поддерживает только некоторые входящие соединения.
- **work**: зона рабочей сети. Большинству машин в сети можно доверять. Доступны дополнительные сервисы.
- **home**: зона домашней сети. Окружению можно доверять, но поддерживаются только определённые пользователем входящие соединения.
- **trusted**: всем машинам в сети можно доверять.

Сохранение правил

Правила firewalld бывают постоянными и временными. Если в наборе появляется или изменяется какое-либо правило, текущее поведение брандмауэра изменяется сразу. Однако после перезагрузки все изменения будут утрачены, если их не сохранить.

Большинство команд firewall-cmd может использовать флаг --**permanent**, который сохранит правило, после чего оно будет использоваться на постоянной основе.

Включение брандмауэра firewalld

Установка firewalld в РЕД ОС производится из репозитория командой:

```
sudo dnf install firewalld
```

После инсталляции активируйте сервис **firewalld.service**:

```
sudo systemctl start firewalld.service
```

Убедитесь, что сервис запущен:

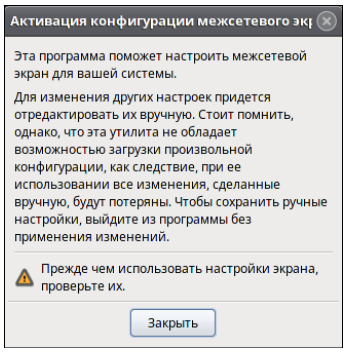
```
firewall-cmd --state
running
```

Теперь брандмауэр запущен и работает согласно конфигурации по умолчанию.

На данный момент сервис включен, но не будет запускаться автоматически вместе с сервером. Чтобы случайно не заблокировать себя на собственном сервере, сначала создайте набор правил, а затем настройте автозапуск.

Стоит сделать небольшое замечание по поводу GUI-интерфейса, он очень удобен, но совершенно не гибок в отличие от способа, если бы мы конфигурировали МЭ через консольные команды

Об этом прямо говорит справка при открытии GUI.



Просмотр правил по умолчанию

Чтобы узнать, какая зона используется по умолчанию, введите:

```
firewall-cmd --get-default-zone
public
```

На данный момент firewalld не получал никаких инструкций относительно других зон, кроме того, к другим зонам не привязан ни один интерфейс, поэтому сейчас зона public является зоной по умолчанию, а также единственной активной зоной.

Чтобы получить список активных зон, введите:

```
firewall-cmd --get-active-zones
public
interfaces: eth0 eth1
```

К зоне **public** привязаны два сетевых интерфейса: **eth0** и **eth1**. Интерфейсы, привязанные к зоне, работают согласно правилам этой зоны.

Чтобы узнать, какие правила использует зона по умолчанию, введите:

```
firewall-cmd --list-all
 public (default, active)
 interfaces: eth0 eth1
 sources:
 services: dhcpv6-client ssh
 ports:
 masquerade: no
 forward-ports:
 icmp-blocks:
 rich rules:
```

Итак, теперь вы знаете, что:

- **public** является зоной по умолчанию и единственной активной зоной.
- К ней привязаны интерфейсы **eth0** и **eth1**.
- Она поддерживает трафик **DHCP** (присваивание IP-адресов) и **SSH** (удаленное администрирование).

Другие зоны брандмауэра

Теперь следует ознакомиться с другими зонами.

Чтобы получить список всех доступных зон, введите:

```
firewall-cmd --get-zones
block dmz drop external home internal public trusted work # Чтобы получить параметры конкретной зоны, добавьте в команду флаг --zone=.

firewall-cmd --zone=home --list-all
home
interfaces:
sources:
services: dhcpv6-client ipp-client mdns samba-client ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Чтобы вывести определения всех доступных зон, добавьте опцию --**list-all-zones**. Для более удобного просмотра вывод можно передать в пейджер:

```
firewall-cmd --list-all-zones | less
```

Настройка зон интерфейсов

Изначально все сетевые интерфейсы привязаны к зоне по умолчанию.

Изменение зоны интерфейса на одну сессию

Чтобы перевести интерфейс в другую зону на одну сессию, используйте опции **--zone=** и **--change-interface=**.

Например, чтобы перевести **eth0** в зону **home**, нужно ввести:

```
sudo firewall-cmd --zone=home --change-interface=eth0
success
```

Примечание: При переводе интерфейса в другую зону нужно учитывать, что это может повлиять на работу некоторых сервисов. К примеру, зона home поддерживает SSH, поэтому соединения этого сервиса не будут сброшены. Но некоторые зоны сбрасывают все соединения, включая SSH, и тогда вы можете случайно заблокировать себе доступ к собственному серверу.

Чтобы убедиться, что интерфейс привязан к новой зоне, введите:

```
firewall-cmd --get-active-zones
home
interfaces: eth0
public
interfaces: eth1
```

После перезагрузки брандмауэра интерфейс будет снова привязан к зоне по умолчанию.

```
sudo systemctl restart firewalld.service
firewall-cmd --get-active-zones
public
interfaces: eth0 eth1
```

Изменение зоны интерфейса на постоянной основе

Если в настройках интерфейса не указана никакая другая зона, после перезапуска брандмауэра интерфейс будет снова привязан к зоне по умолчанию. В РЕД ОС такие конфигурации хранятся в каталоге **/etc/sysconfig/network-scripts**, в файлах формата **ifcfg-interface**.

Чтобы определить зону интерфейса, откройте конфигурационный файл этого интерфейса, например:

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

В конец файла добавьте переменную **ZONE=** и в качестве значения укажите другую зону, например, home:

Содержимое файла:

```
. . . DNS1=2001:4860:4860::8844 DNS2=2001:4860:4860::8888 DNS3=8.8.8.8 ZONE=home
```

Сохраните и закройте файл.

Чтобы обновить настройки, перезапустите сетевой сервис и брандмауэр:

```
sudo systemctl restart network.service

sudo systemctl restart firewalld.service
```

После перезапуска интерфейс **eth0** будет привязан к зоне **home**.

```
firewall-cmd --get-active-zones
home
interfaces: eth0
public
interfaces: eth1
```

Настройка зоны по умолчанию

Также вы можете выбрать другую зону по умолчанию.

Для этого используется параметр **--set-default-zone=**. После этого все интерфейсы будут привязаны к другой зоне:

```
sudo firewall-cmd --set-default-zone=home
home
interfaces: eth0 eth1
```

Создание правил для приложений

Добавление сервиса в зону

Проще всего добавить сервис или порт в зону, которую использует брандмауэр. Просмотрите доступные сервисы:

```
firewall-cmd
--get-services
RH-Satellite-6 amanda-client bacula bacula-client
dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https imaps
ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls
mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy pmwebapi
pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba
samba-client smtp ssh telnet tftp tftp-client transmission-client
vnc-server wbem-https
```

Примечание: Больше информации о каждом конкретном сервисе можно найти в файлах .xml в каталоге /usr/lib/firewalld/services. К пример, сведения о сервисе SSH хранятся в /usr/lib/firewalld/services/ssh.xml и выглядят так:

```
<?xml version="1.0"
encoding="utf-8"?>
```

```
<service>
<short>SSH</short>
<description>Secure
Shell (SSH) is a protocol for logging into and executing commands on
remote machines. It provides secure encrypted communications. If you
plan on accessing your machine remotely via SSH over a firewalled
interface, enable this option. You need the openssh-server package
installed for this option to be useful.</description>
<port
protocol="tcp" port="22"/>
</service>
```

Чтобы включить поддержку сервиса в той или иной зоне, используйте опцию **--add-service=**. Указать целевую зону можно с помощью опции **--zone=**. По умолчанию эти изменения будут работать в течение одной сессии. Чтобы сохранить изменения и использовать их на постоянной основе, добавьте флаг **--permanent**.

Например, чтобы запустить веб-сервер для обслуживания трафика HTTP, для начала нужно включить поддержку этого трафика в зоне **public** на одну сессию:

```
sudo firewall-cmd --zone=public --add-service=http
```

Если сервис нужно добавить в зону по умолчанию, флаг **--zone=** можно опустить.

Убедитесь, что операция выполнена успешно:

```
firewall-cmd --zone=public --list-services
dhcpv6-client http ssh
```

Протестируйте работу сервиса и брандмауэра. Если все работает правильно, можно изменить постоянный набор правил и добавить в него правило для поддержки этого сервиса.

```
sudo firewall-cmd --zone=public --permanent --add-service=http
```

Чтобы просмотреть список постоянных правил, введите:

```
sudo firewall-cmd --zone=public --permanent --list-services
dhcpv6-client http ssh
```

Теперь зона public поддерживает HTTP и порт 80 на постоянной основе. Если веб-сервер может обслуживать трафик SSL/TLS, вы также можете добавить сервис https (для одной сессии или в набор постоянных правил):

```
sudo firewall-cmd --zone=public --add-service=https
sudo firewall-cmd --zone=public --permanent --add-service=https
```

Что делать, если нужный сервис недоступен?

Брандмауэр firewalld по умолчанию включает в себя многие наиболее распространённые сервисы. Однако некоторым приложениям необходимы сервисы, поддержка которых отсутствует в firewalld. В таком случае вы можете поступить двумя способами.

Способ 1: Настройка порта

Проще всего в такой ситуации открыть порт приложения в необходимой зоне брандмауэра. Нужно просто указать порт или диапазон портов и протокол.

Например, приложение, которое использует порт 5000 и протокол **TCP**, нужно добавить в зону **public**. Чтобы включить поддержку приложения на одну сессию, используйте параметр **--add-port=** и укажите протокол **tcp** или **udp**.

```
sudo firewall-cmd --zone=public --add-port=5000/tcp
```

Убедитесь, что операция прошла успешно:

```
firewall-cmd --list-ports
5000/tcp
```

Также можно указать последовательный диапазон портов, отделив первый и последний порт диапазона с помощью тире. Например,

если приложение использует UDP-порты 4990-4999, чтобы добавить их в зону **public**, нужно ввести:

```
sudo firewall-cmd --zone=public --add-port=4990-4999/udp
```

После тестирования можно добавить эти правила в постоянные настройки брандмауэра.

```
sudo firewall-cmd --zone=public --permanent --add-port=5000/tcp
sudo firewall-cmd --zone=public --permanent --add-port=4990-4999/udp
sudo firewall-cmd --zone=public --permanent --list-ports
success
success
4990-4999/udp 5000/tcp
```

Способ 2: Определение сервиса

Добавлять порты в зоны просто, но если у вас много таких приложений, в результате будет сложно отследить, для чего предназначен тот или иной порт. Чтобы избежать такой ситуации, можно вместо портов определить сервисы.

Сервисы – это просто наборы портов с определенным именем и описанием. С помощью сервисов проще управлять настройками, но сами по себе они сложнее, чем порты.

Для начала нужно скопировать существующий сценарий из каталога **/usr/lib/firewalld/services** в каталог **/etc/firewalld/services** (здесь брандмауэр ищет нестандартные настройки).

Например, можно скопировать определение сервиса SSH и использовать его для определения условного сервиса **example**. Имя сценария должно совпадать с именем сервиса и иметь расширение **.xml**.

```
sudo cp /usr/lib/firewalld/services/service.xml /etc/firewalld/services/example.xml
```

Откорректируйте скопированный файл.

```
sudo nano /etc/firewalld/services/example.xml
```

В файле находится определение SSH:

```
<?xml version="1.0" encoding="utf-8"?> <service> <short>SSH</short> <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description> <port protocol="tcp" port="22"/> </service>
```

Большую часть определения сервиса составляют метаданные. Изменить краткое имя сервиса можно в тегах . Это человекочитаемое имя сервиса. Также нужно добавить описание сервиса. Единственное изменение, которое повлияет на работу сервиса – это изменение номера порта и протокола.

Вернёмся к сервису example; допустим, он требует открыть TCP- порт 7777 и UDP- порт 8888. Определение будет выглядеть так:

```
<?xml version="1.0" encoding="utf-8"?> <service> <short>Example Service</short> <description>This is just an example service.  It probably shouldn't be used on a real system.</description> <port protocol="tcp" port="7777"/> <port protocol="udp" port="8888"/> </service>
```

Сохраните и закройте файл.

Перезапустите брандмауэр:

```
sudo firewall-cmd --reload
```

Теперь сервис появится в списке доступных сервисов:

```
firewall-cmd
--get-services
RH-Satellite-6 amanda-client bacula bacula-client
dhcp dhcpv6 dhcpv6-client dns example ftp high-availability http
https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt
libvirt-tls mdns mountd ms-wbt mysql nfs ntp openvpn pmcd pmproxy
pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba
samba-client smtp ssh telnet tftp tftp-client transmission-client
```

```
vnc-server wbem-https
```

Создание зон

Брандмауэр предоставляет много предопределенных зон, которых в большинстве случаев достаточно для работы. Но в некоторых ситуациях возникает необходимость создать пользовательскую зону.

Например, для веб-сервера можно создать зону **publicweb**, а для DNS-сервиса – зону **privateDNS**.

Создавая зону, нужно добавить её в постоянные настройки брандмауэра.

Попробуйте создать зоны **publicweb** и **privateDNS**:

```
sudo firewall-cmd --permanent --new-zone=publicweb
sudo firewall-cmd --permanent --new-zone=privateDNS
```

Убедитесь, что зоны существуют:

```
sudo firewall-cmd --permanent --get-zones
block dmz drop external home internal privateDNS public publicweb trusted work
```

В текущей сессии новые зоны не будут доступны:

```
firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

Чтобы получить доступ к новым зонам, нужно перезапустить брандмауэр:

```
sudo firewall-cmd --reload
firewall-cmd --get-zones
block dmz drop external home internal privateDNS public publicweb trusted work
```

Теперь вы можете присвоить новым зонам требуемые сервисы и порты. К примеру, в зону **publicweb** можно добавить SSH, HTTP и HTTPS.

```
sudo firewall-cmd --zone=publicweb --add-service=ssh
sudo firewall-cmd --zone=publicweb --add-service=http
sudo firewall-cmd --zone=publicweb --add-service=https
firewall-cmd --zone=publicweb --list-all
publicweb
interfaces:
sources:
services: http https ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

В зону **privateDNS** можно добавить DNS:

```
sudo firewall-cmd --zone=privateDNS --add-service=dns
firewall-cmd --zone=privateDNS --list-all
privateDNS
interfaces:
sources:
services: dns
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Затем можно привязать сетевые интерфейсы к новым зонам:

```
sudo firewall-cmd --zone=publicweb --change-interface=eth0
sudo firewall-cmd --zone=privateDNS --change-interface=eth1
```

Теперь можно протестировать настройку. Если всё работает правильно, вы можете добавить эти правила в постоянные настройки.

```
sudo firewall-cmd --zone=publicweb --permanent --add-service=ssh
sudo firewall-cmd --zone=publicweb --permanent --add-service=http
sudo firewall-cmd --zone=publicweb --permanent --add-service=https
sudo firewall-cmd --zone=privateDNS --permanent --add-service=dns
```

После этого можно настроить сетевые интерфейсы для автоматического подключения к правильной зоне.

К примеру, **eth0** будет привязан к **publicweb**:

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

Содержимое файла:

```
. . . IPV6_AUTOCONF=no DNS1=2001:4860:4860::8844 DNS2=2001:4860:4860::8888 DNS3=8.8.8.8 ZONE=publicweb
```

А интерфейс eth1 будет привязан к privateDNS:

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth1
```

Содержимое файла:

```
. . . NETMASK=255.255.0.0 DEFROUTE='no' NM_CONTROLLED='yes' ZONE=privateDNS
```

Перезапустите сетевые сервисы и брандмауэр:

```
sudo systemctl restart network
sudo systemctl restart firewalld
```

Проверьте зоны:

```
firewall-cmd --get-active-zones
privateDNS
interfaces: eth1
publicweb
interfaces: eth0
```

Убедитесь, что в зонах работают нужные сервисы:

```
firewall-cmd --zone=publicweb --list-services
http htpps ssh
firewall-cmd --zone=privateDNS --list-services
dns
```

Пользовательские зоны полностью готовы к работе. Вы можете сделать любую из них зоной по умолчанию. Например:

```
sudo firewall-cmd --set-default-zone=publicweb
```

Автоматический запуск брандмауэра

Теперь, когда вы проверили все настройки и убедились, что все правила работают должным образом, вы можете настроить автозапуск брандмауэра.

Для этого введите:

```
sudo systemctl enable firewalld
```

Теперь брандмауэр будет запускаться вместе с сервером.

Заключение

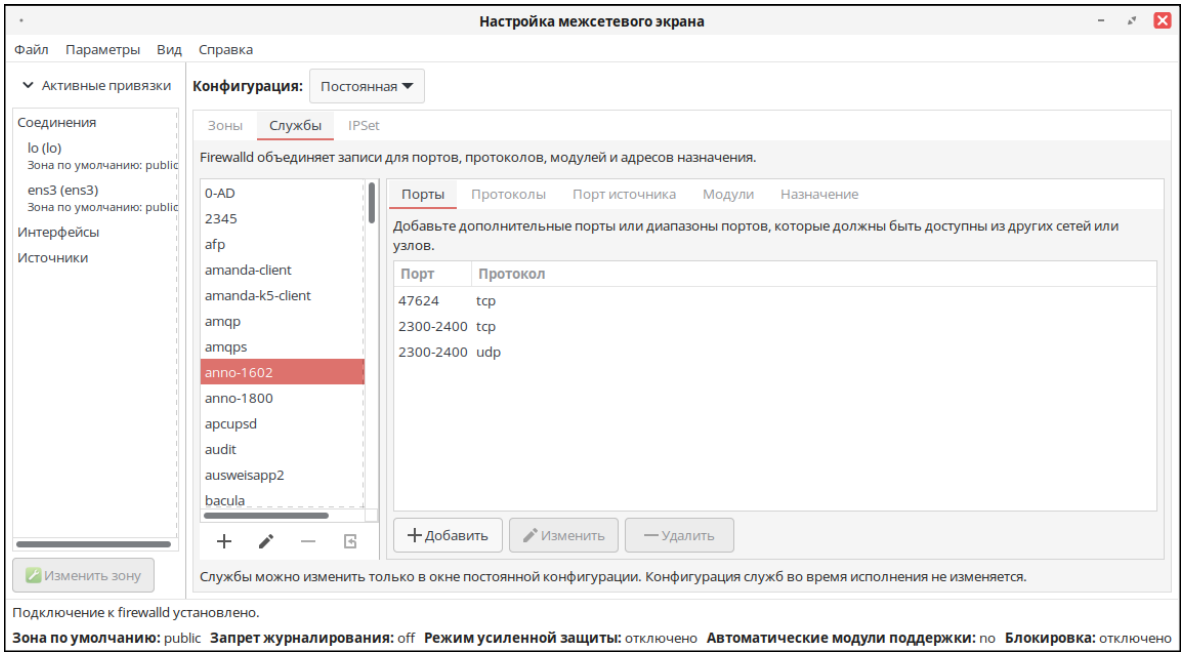
Брандмауэр firewalld — очень гибкий инструмент. Зоны позволяют быстро изменять политику брандмауэра.

Настройка iptables

Настройка в графическом режиме
Включение службы iptables
Настройка iptables при помощи консольных команд
Просмотр и удаление правил
Прием и сбрасывание трафика в цепях
Разрешение и блокировка портов
Блокирование ICMP
Предотвращение несанкционированных действий на сервере

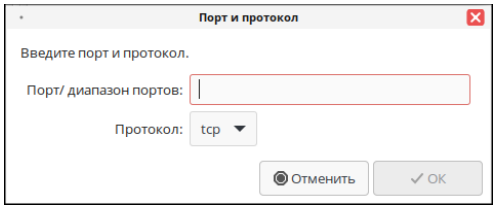
Настройка в графическом режиме

Межсетевой экран можно найти и настроить через «**Главное меню**» — «**Администрирование**» — «**Межсетевой экран**». **iptables** в графическом режиме более удобен, но менее гибок по отношению к ручной настройке.

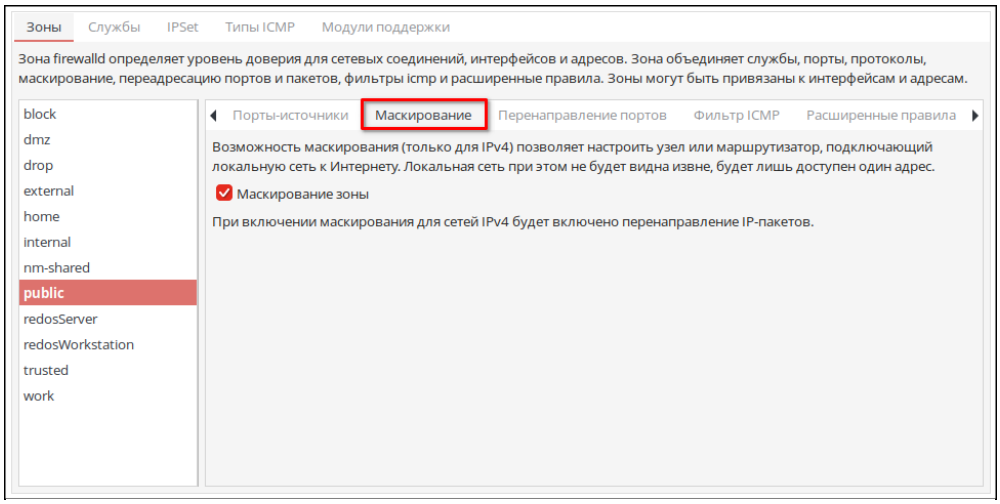


1) Здесь доступен уже предопределенный список служб, для которых можно открыть порты, по которым они работают.

2) Если нужной службы нет в списке, порты для нее можно добавить вручную. Для этого нажмите «**Добавить службу**», затем перейдите на вкладку «**Порты**» и нажмите «**Добавить**». В появившемся окне введите порт и протокол.

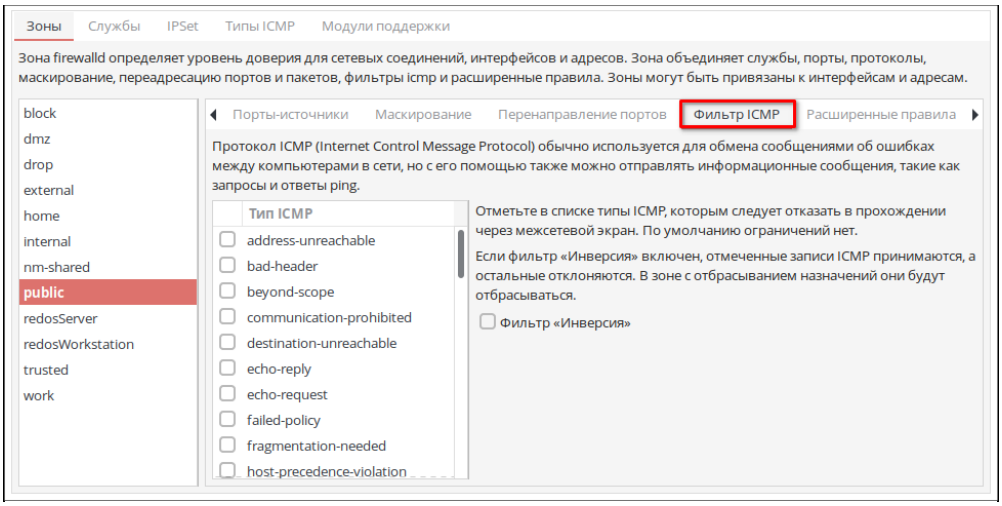


3) Вкладка «**Маскирование**» позволяет настроить узел, подключающий локальную сеть к интернету (из LAN в WAN), но при этом локальная сеть не будет видна извне, будет лишь доступен один адрес (только **IPv4**).



4) Если используется «**Маскирование**», скорее всего возникнет потребность в перенаправлении портов из одной системы в другую (только **IPv4**).

5) Можно настроить фильтр **ICMP**, который работает ниже сетевого протокола, поэтому он используется для информирования о сети. Для этого протокола можно закрыть доступ, чтобы другая сторона не была информирована о вашей сети.



6) Можно добавить собственные готовые правила, если уже готов шаблон, их можно разом добавить и применить.

Включение службы iptables

Установка службы iptables в РЕД ОС производится командой:

```
sudo dnf install iptables-services
```

После инсталляции активируйте службу **iptables-services**:

```
sudo systemctl start iptables.service
```

Убедитесь, что сервис запущен:

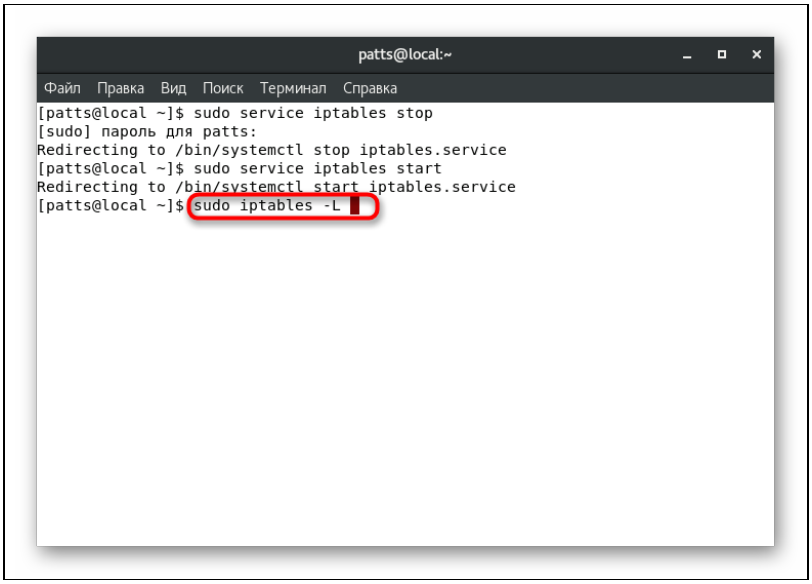
```
sudo systemctl status iptables.service
```

Настройка iptables при помощи консольных команд

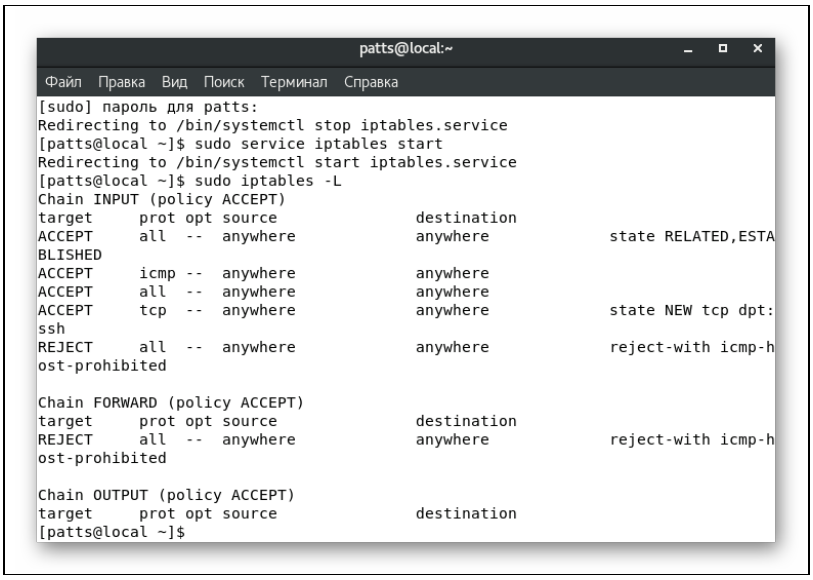
Просмотр и удаление правил

Как уже было сказано ранее, управление межсетевым экраном производится путем ручного или автоматического добавления правил. Например, некоторые дополнительные приложения могут обращаться к инструменту, изменяя определенные политики. Однако большинство подобных действий все же делается вручную. Просмотр списка всех текущих правил доступен через команду:

```
sudo iptables -L
```

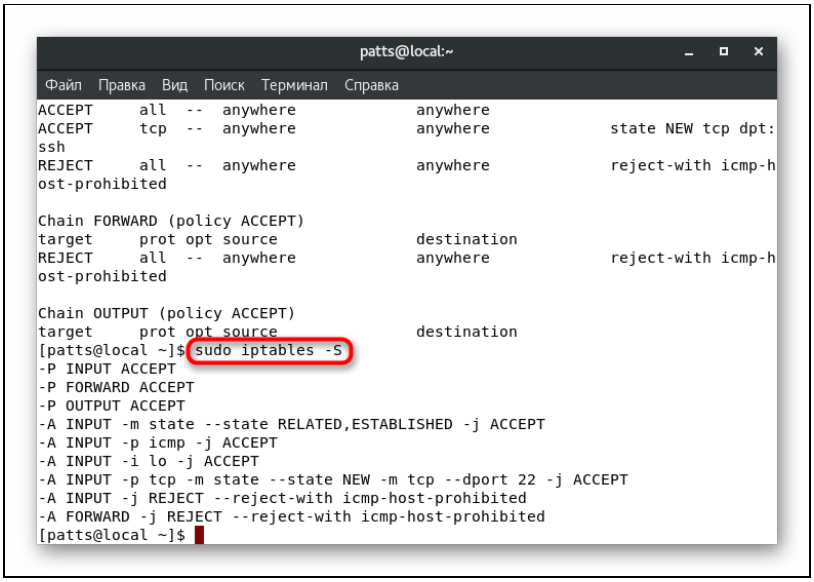


В отобразившемся результате будет информация по трем цепочкам: «**INPUT**», «**OUTPUT**» и «**FORWARD**» — входящий, исходящий и пересылаемый трафик соответственно.



Определить статус всех цепочек можно, выполнив:

```
sudo iptables -S
```



Если настроенные правила не выполняют необходимые задачи, их можно удалить. Весь список правил можно удалить с помощью команды:

```
sudo iptables -F
```

После активации правила будут стерты абсолютно для всех трех цепочек.

Когда необходимо затронуть только политики из какой-то одной цепи, к строке добавляется дополнительный аргумент:

```
sudo iptables -F INPUT
sudo iptables -F OUTPUT
sudo iptables -F FORWARD
```

Отсутствие всех правил означает, что сейчас не применяется никаких настроек фильтрации трафика ни в одну из сторон. Далее системный администратор уже самостоятельно задает новые параметры, используя всю ту же консоль, команду и различные аргументы.

Прием и сбрасывание трафика в цепях

Каждая цепь настраивается отдельно для приема или блокирования трафика. Выставив определенное значение, можно добиться того, что, например, весь входящий трафик будет блокироваться. Для этого команда должна иметь вид:

```
sudo iptables --policy INPUT DROP
```

где **INPUT** — название цепи, а **DROP** — значение сброса.

Точно такие же параметры задаются и для других цепей, например:

```
sudo iptables --policy OUTPUT DROP
```

Если же необходимо выставить значение на прием трафика, тогда **DROP** изменяется на **ACCEPT** и получается:

```
sudo iptables --policy INPUT ACCEPT
```

Разрешение и блокировка портов

Как известно, все сетевые приложения и процессы работают через определенный порт. Путем блокировки или разрешения определенных адресов можно контролировать доступ всех сетевых целей. Давайте разберем проброс порта на примере **80**. В терминале будет достаточно ввести команду:

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

где:

- **-A** — добавление нового правила;
- **INPUT** — указание цепи;
- **-p** — определение протокола, в этом случае TCP;
- **--dport** — порт назначения.

Точно такая же команда относится и к порту **22**, который используется сервисом **SSH**:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Для блокирования указанного порта применяется строка точно такого же вида, только в конце **ACCEPT** изменяется на **DROP**. В итоге получается:

```
sudo iptables -A INPUT -p tcp --dport 2450 -j DROP
```

Все эти правила заносятся в конфигурационный файл, и вы можете просмотреть их в любой момент. Напоминаем, осуществляется это через sudo iptables -L. Если вместе с портом необходимо разрешить еще и сетевой IP-адрес, строка немного видоизменяется — после **tcp** добавляется **-s** и сам адрес:

```
sudo iptables -A INPUT -p tcp -s 12.12.12.12/32 --dport 22 -j ACCEPT
```

где **12.12.12.12/32** — необходимый IP-адрес.

Блокирование происходит по тому же принципу, меняя в конце значение **ACCEPT** на **DROP**. Тогда получается;

```
sudo iptables -A INPUT -p tcp -s 12.12.12.0/24 --dport 22 -j DROP
```

Блокирование ICMP

ICMP (Internet Control Message Protocol) — протокол, который входит в состав TCP/IP и задействован для передачи сообщений об ошибках и экстренных ситуациях при работе с трафиком. Например, когда запрашиваемый сервер недоступен, именно этот инструмент выполняет сервисные функции. Утилита **iptables** позволяет заблокировать его через брандмауэр, а сделать это можно командой:

```
sudo iptables -A OUTPUT -p icmp --icmp-type 8 -j DROP
```

Она произведет блокировку запросов **от** вашего и **к** вашему серверу.

Входящие запросы блокируются немного иначе. Тогда нужно ввести:

```
sudo iptables -I INPUT -p icmp --icmp-type 8 -j DROP
```

После активации данных правил сервер не будет отвечать на **ping**-запросы.

Предотвращение несанкционированных действий на сервере

Иногда серверы подвергаются DDoS-атакам или другим несанкционированным действиям со стороны злоумышленников. Правильная настройка межсетевого экрана позволит обезопасить себя от подобного рода взломов. Для начала рекомендуется задать следующие правила:

1. Пропишите в консоли:

```
sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 20/minute --limit-burst 100 -j ACCEPT
```

где:

- `--limit 20/minute` — ограничение на частоту положительных результатов. Единицу измерения вы можете указывать самостоятельно, например, **/second**, **/minute**, **/hour**, **/day**;
- `--limit-burst <number>` — ограничение на число пропускаемых пакетов. Все значения выставляются индивидуально по предпочтениям администратора.

2. Далее можно запретить сканирование открытых портов, чтобы убрать одну из возможных причин взлома. Введите первую команду:

```
sudo iptables -N block-scan
```

3. Затем укажите:

```
sudo iptables -A block-scan -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j RETURN
```

4. Последняя команда имеет вид:

```
sudo iptables -A block-scan -j DROP
```

Выражение **block-scan** в данных случаях — название используемой цепи.

Для того чтобы новые правила вступили в силу, необходимо сохранить конфигурацию и вновь запустить службу **iptables**:

```
sudo iptables-save > /etc/sysconfig/iptables
sudo systemctl enable --now iptables.service
```

Тестирование пропускной способности сети с помощью iperf3

Iperf — кроссплатформенная консольная клиент-серверная программа — генератор TCP и UDP трафика для тестирования пропускной способности сети.

Вы можете подробнее ознакомиться с утилитами мониторинга работы сети, просмотрев наши обучающие видео:

- на **RuTube** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **Яндекс.Дзен** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **VK Видео** — Сеть в РЕД ОС. Утилиты мониторинга работы сети.

На наших каналах вы также сможете найти много другой полезной информации.

Установка утилиты происходит на 2 машинах: одна выступает в роли сервера, другая в роли клиента.

```
dnf install iperf3
```

Запуск на стороне сервера

```
iperf3 -s
```

```
[root@localhost ~]# iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 10.81.81.202, port 55840
[  5] local 10.81.1.206 port 5201 connected to 10.81.81.202 port 55842
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  82.9 MBytes   696 Mbits/sec
[  5]   1.00-2.00   sec  88.1 MBytes   739 Mbits/sec
[  5]   2.00-3.00   sec  86.2 MBytes   723 Mbits/sec
[  5]   3.00-4.00   sec  87.3 MBytes   732 Mbits/sec
[  5]   4.00-5.00   sec  86.0 MBytes   722 Mbits/sec
[  5]   5.00-6.00   sec  88.6 MBytes   743 Mbits/sec
[  5]   6.00-7.00   sec  87.8 MBytes   736 Mbits/sec
[  5]   7.00-8.00   sec  83.9 MBytes   704 Mbits/sec
[  5]   8.00-9.00   sec  90.7 MBytes   761 Mbits/sec
[  5]   9.00-10.00  sec  90.5 MBytes   759 Mbits/sec
[  5]  10.00-10.01  sec   841 KBytes   733 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.01  sec   873 MBytes   732 Mbits/sec                  receiver
-----------------------------------------------------------
```

Запуск на стороне клиента:

```
iperf3 -c server_address
```

```
[root@localhost ~]# iperf3 -c 10.81.1.206
Connecting to host 10.81.1.206, port 5201
[  5] local 10.81.81.202 port 56010 connected to 10.81.1.206 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  81.6 MBytes   684 Mbits/sec  272   1.93 MBytes
[  5]   1.00-2.00   sec  92.5 MBytes   776 Mbits/sec   66   1.03 MBytes
[  5]   2.00-3.00   sec  88.8 MBytes   744 Mbits/sec    0   1.10 MBytes
[  5]   3.00-4.00   sec  87.5 MBytes   734 Mbits/sec    0   1.15 MBytes
[  5]   4.00-5.00   sec  90.0 MBytes   755 Mbits/sec    0   1.19 MBytes
[  5]   5.00-6.00   sec  88.8 MBytes   744 Mbits/sec    0   1.25 MBytes
[  5]   6.00-7.00   sec  87.5 MBytes   734 Mbits/sec    4    938 KBytes
[  5]   7.00-8.00   sec  81.2 MBytes   682 Mbits/sec    0   1.02 MBytes
[  5]   8.00-9.00   sec  87.5 MBytes   734 Mbits/sec    0   1.10 MBytes
[  5]   9.00-10.00  sec  86.2 MBytes   724 Mbits/sec    0   1.17 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec   872 MBytes   731 Mbits/sec  342             sender
[  5]   0.00-10.01  sec   870 MBytes   729 Mbits/sec                  receiver

iperf Done.
```

В ходе выполнения команд выполняется 10 секундная передача данных, на основе которых выдается скорость сети.

Вывод подсказки о том, как использовать **iperf3**:

```
iperf3 -h
```

Вывод информации об активных сетевых соединениях с помощью iftop

Iftop - показывает информацию об активных сетевых соединениях . С её помощью можно мониторить трафик в режиме online, причем с разделением по протоколам, интерфейсам и хостам.

Вы можете подробнее ознакомиться с утилитами для получения информации об активных сетевых соединениях, просмотрев наши обучающие видео:

- на **RuTube**:
  - Информация, мониторинг и тестирование системы;
  - Сеть в РЕД ОС. Утилиты мониторинга работы сети.
- в **Яндекс.Дзен**:
  - Информация, мониторинг и тестирование системы;
  - Сеть в РЕД ОС. Утилиты мониторинга работы сети.
- в **VK Видео**:
  - Информация, мониторинг и тестирование системы;
  - Сеть в РЕД ОС. Утилиты мониторинга работы сети.

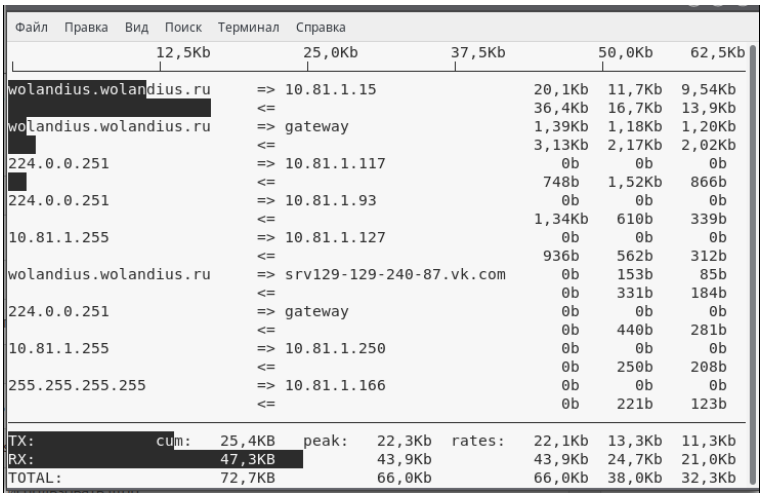
На наших каналах вы также сможете найти много другой полезной информации.

Установка:

```
dnf install iftop
```

Запуск утилиты:

```
iftop
```



Вывод трафика в байтах:

```
iftop -i eth0 -B
```

Трафик между локальным интерфейсом и хостом 8.8.8.8

```
iftop -i eth0 -f "dst 8.8.8.8"
```

Вывод подсказки, как использовать iftop:

```
iftop -h
```

Мониторинг сетевого трафика с помощью nethogs

Nethogs - это утилита, используемая для мониторинга пропускной полосы сетевого трафика в реальном времени, используемой каждым процессом или приложением.

Вы можете подробнее ознакомиться с утилитами мониторинга работы сети, просмотрев наши обучающие видео:

- на **RuTube** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **Яндекс.Дзен** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **VK Видео** — Сеть в РЕД ОС. Утилиты мониторинга работы сети.

На наших каналах вы также сможете найти много другой полезной информации.

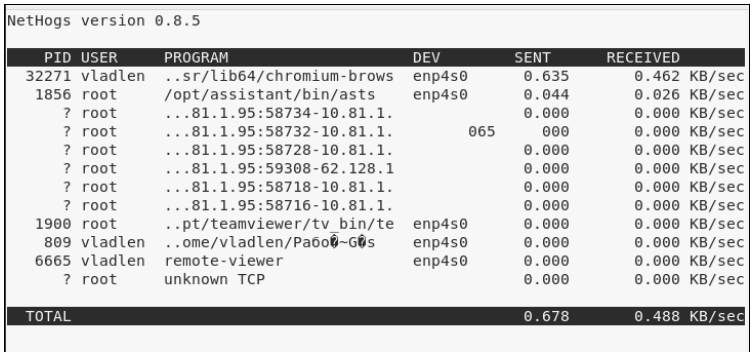
Для использования nethogs необходимы права администратора.

Установка утилиты:

```
dnf install nethogs
```

Запуск утилиты производится командой:

```
nethogs
```



Просмотр трассировки:

```
nethogs -t
```

Просмотр основного списка доступных команд:

```
nethogs -h
```

Когда nethogs запущен доступно:

```
q: выход
s: отсортировать трафик по критерию SENT
r: отсортировать трафик по критерию RECEIVE
m: переключить режимы между kb/s, m/s
```

Отображение информации о сетевых сокетах с помощью ss

Использование утилиты ss
Вывод информации по IP-адресу
Вывод информации по состоянию сокета
Вывод информации по имени сервиса или номеру порта

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: iproute2-6.1.0

ss — консольная утилита, которая предоставляет информацию о сетевых сокетах, подключениях **TCP/UDP**, маршрутизации и других сетевых статистических данных.

ss отображает информацию аналогично утилите **netstat** и при этом выводит больше информации о сетевых соединениях и их состоянии, чем какие-либо другие инструменты.

Информация о сокете выводится в виде таблицы. Каждый столбец отображает определенную информацию, относящуюся к сокету.

Описание выводимой информации в столбцах:

- `Netid` — отображает тип сокета;
- `State` — отображает состояние сокета. Может принимать следующие значения: сокет установлен — **ESTAB**, сокет не подключен — **UNCONN**, сокет прослушивается — **LISTEN**.
- `Recv-Q` — отображает количество принятых пакетов в очереди;
- `Send-Q` — отображает количество отправленных пакетов в очереди;
- `Local address:port` — показывает адрес локальной машины и порт;
- `Peer address:port` — отображает адрес удаленной машины и порт.

Использование утилиты ss

Синтаксис утилиты **ss** выглядит следующим образом:

```
ss <опции>
```

Утилита ss может принимать несколько опций:

```
ss <опция_1> <опция_2> <опция_3> ...
```

Основные опции утилиты **ss**:

- `-V, --version` — показать версию утилиты;
- `-n, --numeric` — не определять имена служб;
- `-r, --resolve` — определять сетевые имена адресов с помощью DNS;
- `-a, --all` — отобразить все сокеты (открытые соединения);
- `-l, --listening` — показать только прослушиваемые сокеты;
- `-o, --options` — показать информацию таймера;
- `-e, --extended` — выводить расширенную информацию о сокете;
- `-p, --processes` — показать процессы, использующие сокет;
- `-i, --info` — посмотреть внутреннюю информацию TCP;
- `-s, --summary` — статистика использования сокета;
- `-D, --diag=<файл>` — экспортировать текущее состояние TCP-сокетов в файл;
- `-F, --filter=<файл>` — работать с информацией, взятой из файла.

Можно выводить информацию о сокете, который использует только необходимый протокол, используя следующие опции:

- `-4, --ipv4` — только сокеты протокола IPv4;
- `-6, --ipv6` — только сокеты протокола IPv6;
- `-0, --packet` — только PACKET-сокеты;
- `-t, --tcp` — TCP-сокеты;
- `-u, --udp` — UDP-сокеты;
- `-x, --unix` — UNIX-сокеты.

Для отображения всех TCP-соединений выполните команду:

```
ss -ta
```

Для отображения всех UDP-соединений выполните команду:

```
ss -ua
```

Для вывода информации о подключенных TCP- и UDP-сокетах, а также информации о процессах, которые используют сокеты — имя процесса и его PID, выполните:

```
ss -tupn
```

Для отображения открытых TCP- и UDP-сокетов, которые ожидают соединение, выполните команду, добавив опцию -l:

```
ss -tupnl
```

Вывод информации по IP-адресу

Утилита поддерживает фильтрацию информации об установленных подключениях по адресу назначения и по адресу получения.

Для фильтрации информации по адресу назначения выполните:

```
ss dst xx.xx.xx.xx
```

Для фильтрации информации по адресу получения выполните:

```
ss src xx.xx.xx.xx
```

где xx.xx.xx.xx — IP-адрес, по которому необходимо отфильтровать информацию.

Вывод информации по состоянию сокета

Можно отфильтровать информацию по состоянию сокета. Для этого используется дополнительный ключ `state`.

Состояния, которые может принимать сокет:

- *established*;
- *listening*;
- *syn-sent*;
- *syn-recv*;
- *time-wait*;
- *closed*;
- *close-wait*;
- *last-ack*;
- *fin-wait-1*;
- *fin-wait-2*;
- *closing*.

Кроме того, ss распознаёт следующие идентификаторы состояний:

- *all* — все состояния;
- *connected* — все состояния, кроме прослушиваемых и закрытых;
- *synchronized* — все состояния, кроме *syn-sent*;
- *bucket* — состояния, представляющие собой минисокеты, например, *time-wait* или *syn-recv*;
- *big* — все состояния, кроме *bucket*.

Для отображения всех открытых TCP-портов выполните команду:

```
ss -t state listening
```

Для отображения всех успешных соединений по IPv4 выполните:

```
ss -4 state established
```

Вывод информации по имени сервиса или номеру порта

Для фильтрации информации по номеру порта или его имени утилите необходимо передать соответствующие опции:

- для порта получения:

```
ss <опции> sport = :<порт>
```

- для порта назначения:

```
ss <опции> dport = :<порт>
```

где <порт> — номер порта или имя сервиса.

Для фильтрации TCP-соединения с выводом информации об использовании только порта получателя **22** выполните:

```
ss -ta '( sport = :22 )'
```

Для фильтрации TCP-соединения с выводом информации об использовании сервиса **HTTPS** в адресе назначения выполните:

```
ss -ta '( dport = :https )'
```

Мониторинг использования сетевого канала с помощью trafshow

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** trafshow 5.2.3-1

Trafshow помогает оценить интенсивность использования канала, постоянно показывает информацию о пакетном трафике для конфигурации сетевого интерфейса и периодически сортирует и обновляет эту информацию.

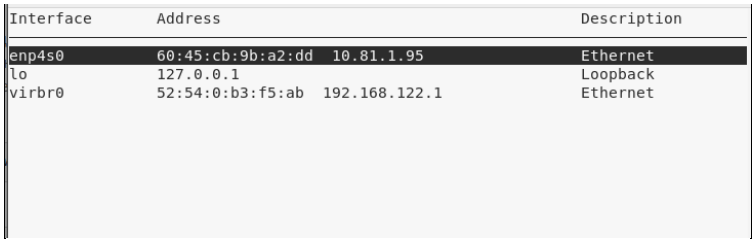
Вы можете подробнее ознакомиться с утилитами мониторинга работы сети, просмотрев наши обучающие видео:

- на **RuTube** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **Яндекс.Дзен** — Сеть в РЕД ОС. Утилиты мониторинга работы сети;
- в **VK Видео** — Сеть в РЕД ОС. Утилиты мониторинга работы сети.

На наших каналах вы также сможете найти много другой полезной информации.

Установка:

```
dnf install trafshow
```



Запуск утилиты

```
trafshow
```

Запуск с определенным интерфейсом, к примеру enp4s0

```
trafshow -i enp4s0
```

Вывод подсказки о том, как использовать trafshow:

```
trafshow -h
```

Анализ и фильтрация сетевых пакетов с помощью tcpdump

Назначение утилиты
Синтаксис утилиты
Опции утилиты
Фильтры утилиты
Примеры использования утилиты

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tcpdump-14:4.9.3-3

tcpdump – инструмент командной строки для анализа пакетов, который позволяет перехватывать сетевые пакеты на основе правил фильтрации, интерпретировать содержимое пакетов и отображать результат в удобочитаемом формате. По умолчанию утилита предустановлена в РЕД ОС.

Однако если по каким-либо причинам утилита отсутствует в системе, перейдите в сеанс пользователя **root**:

```
su -
```

и установите ее командой:

```
dnf install tcpdump
```

Для работы с утилитой необходимы права суперпользователя **root** или администратора системы (**sudo**), поэтому здесь и далее команды выполняются с правами суперпользователя **root**, если не указано иное.

Назначение утилиты

Утилита **tcpdump** помогает:

- диагностировать потерю пакетов;
- проверять производительность приложений;
- проверять маршрутизацию трафика в многосетевой среде;
- отслеживать теги VLAN;
- прослушивать трафик.

По умолчанию **tcpdump** прослушивает сетевой интерфейс с наименьшим номером в списке, поэтому сначала необходимо определить, какой интерфейс будет прослушиваться.

Синтаксис утилиты

Синтаксис команды **tcpdump** имеет следующий вид:

```
tcpdump [-опции] [фильтры]
```

Для отображения списка сетевых интерфейсов, используемых в системе, выполните команду:

```
tcpdump -D
```

```
1.wlo1 [Up, Running]
2.enp0s20f0u1 [Up, Running]
3.lo [Up, Running, Loopback]
4.any (Pseudo-device that captures on all interfaces) [Up, Running]
5.virbr0 [Up]
6.bluetooth-monitor (Bluetooth Linux Monitor) [none]
7.nflog (Linux netfilter log (NFLOG) interface) [none]
8.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
9.bluetooth0 (Bluetooth adapter number 0) [none]
10.usbmon0 (Raw USB traffic, all USB buses) [none]
11.usbmon1 (Raw USB traffic, bus number 1)
12.usbmon2 (Raw USB traffic, bus number 2)
```

Для прослушивания конкретного сетевого интерфейса необходимо использовать опцию **-i** с именем интерфейса, передаваемого в качестве параметра. Например, для интерфейса под номером 2 команда будет иметь следующий вид:

```
tcpdump -i enp0s20f0u1
```

Если необходимо захватить трафик со всех сетевых интерфейсов, например, если в системе несколько сетевых подключений, в **tcpdump** для таких случаев предусмотрен специальный параметр **any**:

```
tcpdump -i any
```

Опции утилиты

Описание некоторых опций **tcpdump**:

Опция	Описание
-a	Преобразовать сетевые и широковещательные адреса в доменные имена.
-e	Отображать данные канального уровня (MAC-адрес, протокол, длина пакета). Помимо IP-адресов будут отображены MAC-адреса компьютеров.
-N	Не добавлять доменное расширение к именам узлов. Например, отобразить **net** вместо **net.library.org**.
-n	Отображать IP-адрес вместо имени хоста.
-nn	Отображать номер порта вместо используемого протокола.
-q	Вывести минимум информации. Обычно – имя протокола, отправитель и получатель пакета, используемые порты и объем переданных данных.
-r	Прочесть трафик из файла, если он был предварительно сохранен параметром **-w**.
-S	Не обрабатывать абсолютные порядковые номера (initial sequence number — ISN) в относительные.
-t	Не отображать метку времени в каждой строке.
-tt	Отображать неформатированную метку времени в каждой строке.
-tttt	Показывать дату и время.
-v	Выводить подробную информацию (TTL; ID; общая длина заголовка, а также его параметры; производить проверку контрольных сумм IP и ICMP-заголовков).
-vv	Выводить ещё более полную информацию, в основном относится к NFS и SMB.
-vvv	Выводить максимально подробную информацию.
-w <файл>	Сохранять данные **tcpdump** в двоичном формате. Преимущества использования данного способа по сравнению с обычным перенаправлением в файл является высокая скорость записи и возможность чтения подобных данных другими программами, например, snort, но этот файл нельзя прочитать человеку.
-c <число>	Завершит работу **tcpdump** после получения указанного числа пакетов.

Описанные опции помогают отфильтровывать информативность пакетов, перенаправлять вывод в файл или прочитать уже записанный файл и т.д. Для получения более подробной информации по всем доступным опциям утилиты **tcpdump** можно воспользоваться командой:

```
man tcpdump
```

Фильтры утилиты

Для упрощения поиска пакетов и экономии времени в **tcpdump** предусмотрены фильтры. Они используются для отсеивания ненужных пакетов. Таким образом можно вывести список пакетов, полученных от какого-либо конкретного IP-адреса или подсети.

Описание фильтров для **tcpdump**:

- **host**, **net**, **port** – для фильтрации по значению соответствующего идентификатора;
- **src**, **dst** – для фильтрации по конкретному направлению передачи к и/или от идентификатора;
- **tcp**, **udp**, **icmp**, **ah** – для фильтрации по заданному сетевому протоколу.

Примеры использования утилиты

Для просмотра исходящего и входящего трафика по IP-адресу выполните команду с фильтром **host** и соответствующим аргументом:

```
tcpdump host 192.168.1.1
```

Для обнаружения пакетов, следующих из определенной сети либо в нее, используйте команду с фильтром **net**:

```
tcpdump net 192.168.1.0/24
```

Для захвата трафика, который поступает только на определенный порт, выполните команду с фильтром **port** и номером соответствующего порта в качестве аргумента:

```
tcpdump port 22
```

Для отсеивания трафика по отправителю с помощью фильтра **src**, выполните команду:

```
tcpdump src 192.168.1.1
```

Для отображения входящего трафика с IP-адреса выполните команду:

```
tcpdump dst 192.168.1.1
```

Для поиска конкретного типа трафика используются фильтры **tcp**, **udp**, **icmp**. Например, фильтр **icmp** поможет вывести на экран весь трафик, передаваемый по протоколу **ICMP**:

```
tcpdump icmp
```

Настройка сервера Port Knocking

Настройка сервера
Предварительная настройка брандмауэра
Установка и настройка службы knockd
Настройка клиента

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер минимальный, сервер графический
- **Версия ПО**: knock-server-0.8-1

Knock — программное обеспечение, осуществляющее работу с использованием механизма **Port Knocking** в среде операционной системы РЕД ОС.

Port Knocking имеет следующий принцип работы – сетевой порт является по умолчанию закрытым до тех пор, пока на него не поступит заранее определённая последовательность пакетов данных, которая «заставит» порт открыться. Например, можно сделать недоступным для внешних подключений порт SSH, но в то же время открывать его только для тех, кто знает необходимую последовательность.

Вы можете подробнее ознакомиться с настройкой сервера **Port Knocking**, просмотрев наши обучающие видео:

- на **RuTube** — Механизм защиты сервера Port Knocking;
- в **Яндекс.Дзен** — Механизм защиты сервера Port Knocking;
- в **VK Видео** — Механизм защиты сервера Port Knocking.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка сервера

Предварительная настройка брандмауэра

Для организации работы механизма **Port Knocking** в системе необходимо правильно настроить брандмауэр. Цепочка правил **INPUT**, которая отвечает за фильтрацию входящих подключений, обязательно должна начинаться с правила, разрешающего уже установленные и связанные соединения, а завершаться правилом, запрещающим любые входящие подключения. Между ними должны располагаться правила, разрешающие доступ к отдельным сервисам.

В минимальной конфигурации должны присутствовать следующие два правила, где **enp9s0** – имя внешнего интерфейса:

```
# Разрешить установленные и связанные соединения
 iptables -A INPUT -i enp9s0 -m state --state ESTABLISHED,RELATED -j ACCEPT
 # Запретить входящие соединения извне
 iptables -A INPUT -i enp9s0 -j DROP
```

Данные команды можно ввести в консоли, и они начнут действовать немедленно. Однако обратите внимание, если команды будут выполняться удаленно с подключением через внешний интерфейс, можно **полностью потерять связь** с сервером до его последующей перезагрузки. В этом случае (при удаленном подключении) необходимо добавить между двумя вышеуказанными правилами еще одно дополнительное правило и не удалять его до тех пор, пока работа **Port Knocking** не будет организована как требуется.

```
# Разрешить подключение по SSH
 iptables -A INPUT -i enp9s0 -p tcp --dport 22 -j ACCEPT
```

Если указанные выше команды выполняются в терминале, разрешающее правило для **SSH** следует вводить после правила, разрешающего установленные и связанные соединения.

После проведенных манипуляций перезапустите службу **iptables** командой:

```
systemctl restart iptables
```

Значения будут применены автоматически.

Установка и настройка службы knockd

Для реализации механизма **Port Knocking** необходимо настроить службу **knockd**, которая находится в репозитории РЕД ОС в составе пакета **knock-server**.

Для установки **knock-server** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install knock-server
```

После установки необходимо отредактировать конфигурационный файл **/etc/knockd.conf**. В нем должна остаться только секция [options], которую необходимо привести к следующему виду:

```
[options]
 UseSyslog
 Interface = enp9s0
```

где:

- UseSyslog – указывает, что события будут записываться в системный журнал;
- Interface – имя сетевого интерфейса, который будет слушать **knockd** (в примере указан интерфейс enp9s0).

После этого требуется создать секцию для доступа по **SSH**:

```
[SSH]
 sequence = 7000,9000,8000
 seq_timeout = 5
 tcpflags = syn
 start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 stot_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 cmd_timeout = 60
```

где:

- sequence – задает последовательность подключений, по умолчанию используется протокол **tcp**, но если необходимо использовать протокол **udp**, следует указать его в формате <номер_порта>:<протокол>, например:

```
[SSH]
 sequence = 7000,9000:udp,8000
```

Так, порты **7000** и **8000** будут ожидать подключения по протоколу **tcp**, а порт **9000** — по протоколу **udp**.

- seq_timeout – время в секундах, за которое клиент должен совершить всю последовательность подключений. Значение следует указать минимальным, но при этом необходимо учитывать возможные задержки каналов связи как сервера, так и клиента;
- tcpflags – определяет TCP-флаги пакетов, которые будут участвовать в последовательности. Флаг **syn** рекомендуется использовать совместно с SSH, так как SSH-трафик может мешать **knockd**, признавая последовательность недействительной.
- start_command и stop_command – определяют команды, которые должен выполнить **knockd** с интервалом, указанном в опции cmd_timeout. Принцип действия следующий – получив указанную последовательность подключений, служба выполняет команду из опции start_command, по истечении заданного таймаута – команду stop_command.

Основной задачей является предоставление доступа к порту SSH на время, достаточное для установления подключения. Поэтому в параметр start_command в качестве первого правила в цепочку **INPUT** добавляется разрешение подключения к SSH с адреса источника подключения. Обратите внимание, что для этого используется ключ -I, который без указания номера добавляет правило первой строкой, а также подстановочную конструкцию -s %IP%, которая установит в правило текущий адрес подключающегося. Вторая команда удаляет уже добавленное правило.

Таким образом, порт будет открыт на подключение только для адреса клиента и только на время, указанное в таймауте. Обратите внимание, что значение таймаута необходимо только для осуществления подключения, после успешного подключения клиента и истечения таймаута текущее соединение не разрывается, а продолжает сохраняться и переходит в состояние ESTABLISHED за счет заданного правила в цепочке **INPUT**, которое разрешает установленные и связанные подключения.

Для сохранения конфигурации и запуска службы выполните команду:

```
systemctl start knockd
```

После завершения настройки можно попробовать подключиться к серверу с клиентской машины. Однако предварительно следует проверить состояние брандмауэра командой:

```
iptables -L -vn
```

```
[root@localhost user]# iptables -L -vn
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   29  2878 ACCEPT     all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 DROP       all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 16 packets, 3383 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

В выводе отображаются действующие правила, которые сигнализируют о том, что подключение к серверу невозможно.

Теперь можно попробовать выполнить подключение к серверу. Информацию о подключении клиента к серверу см. в разделе «Настройка клиента».

Затем снова стоит проверить состояние брандмауэра:

```
iptables -L -vn
```

```
[root@localhost user]# iptables -L -vn
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       192.168.8.4          0.0.0.0/0           tcp dpt:22
  595  243K ACCEPT     all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
   23  2460 DROP       all  --  enp9s0 *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

После подключения клиента первым в цепочке **INPUT** появилось правило, разрешающее доступ к SSH с адреса клиента.

Ровно через указанное в таймауте время (в примере 60 секунд) правило исчезнет, поэтому рекомендуется устанавливать значение таймаута достаточным для выполнения необходимых действий по подключению.

Возможности **knockd** не ограничиваются одним только управлением правилами сетевого фильтра. Можно настраивать **knockd** на запуск определенных скриптов, способных выполнять практически любые действия на сервере (от создания резервных копий до полного удаления каких-либо важных данных с сервера).

Настройка клиента

Подробную информацию о подключении клиента к серверу с помощью механизма **Port Knocking** см. в нашей статье «Механизм защиты сервера Port Knocking. Подключение клиента».

Подключение клиента Port Knocking

Настройка сервера
Настройка клиента
Установка knock
Подключение к серверу

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: knock-0.8-1

Knock — программное обеспечение, осуществляющее работу с использованием механизма **Port Knocking** в среде операционной системы РЕД ОС.

Port Knocking имеет следующий принцип работы – сетевой порт является по умолчанию закрытым до тех пор, пока на него не поступит заранее определённая последовательность пакетов данных, которая «заставит» порт открыться. Например, можно сделать недоступным для внешних подключений порт SSH, но в то же время открывать его только для тех, кто знает необходимую последовательность.

Вы можете подробнее ознакомиться с возможностью подключения клиентов к серверу **Port Knocking**, просмотрев наши обучающие видео:

- на **RuTube** — Механизм защиты сервера Port Knocking;
- в **Яндекс.Дзен** — Механизм защиты сервера Port Knocking;
- в **VK Видео** — Механизм защиты сервера Port Knocking.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка сервера

Подробную информацию о настройке и защите сервера с помощью механизма **Port Knocking** см. в нашей статье «Механизм защиты сервера Port Knocking».

Настройка клиента

Установка knock

Для установки **knock** на клиенте перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install knock
```

Подключение к серверу

Для выполнения подключения к серверу посредством **knock** используется команда следующего вида:

```
knock <IP_адрес_сервера> <порты>
```

Например:

```
knock 192.168.1.153 7000:tcp 9000:udp 8000:tcp
```

Обратите внимание на формат описания номеров и типов портов. Он должен быть абсолютно таким же, как и в конфигурационном файле **/etc/knockd.conf** на сервере.

Настройка FTP-сервера

Установка и настройка сервера
Монтирование ftp-ресурса в качестве директории РЕД ОС
Ручной вариант монтирования
Автоматический вариант монтирования при помощи autofs

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** ftp-0.17-69, vsftpd-3.0.5-1

Вы можете подробнее ознакомиться с информацией по установке и настройке ftp-сервера, просмотрев наши обучающие видео:

- на **RuTube** — FTP-сервер на РЕД ОС;
- в **Яндекс.Дзен** — FTP-сервер на РЕД ОС;
- в **VK Видео** — FTP-сервер на РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и настройка сервера

Для установки через терминал перейдите в сеанс пользователя **root** с помощью команды:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Для установки выполните команду:

```
dnf install vsftpd
dnf install ftp
```

Запуск сервера и включения демона **vsftpd** в автозагрузку :

```
systemctl start vsftpd
systemctl enable vsftpd
```

Конфигурационным файлом для настройки **vsFTPd** является файл **vsftpd.conf**, который обычно находится по пути **/etc/vsftpd/vsftpd.conf**.

На всякий случай полезно перед редактированием оригинального файла настроек сделать его резервную копию:

```
cp /etc/vsftpd/vsftpd.conf vsftpd.conf.backup
```

FTP-сервер **vsFTPd** предусматривает два основных варианта работы: с анонимными и авторизованными пользователями.

Чтобы включить анонимный доступ по FTP, нужно в файле **/etc/vsftpd/vsftpd.conf** определить значение «**YES**» для соответствующей директивы:

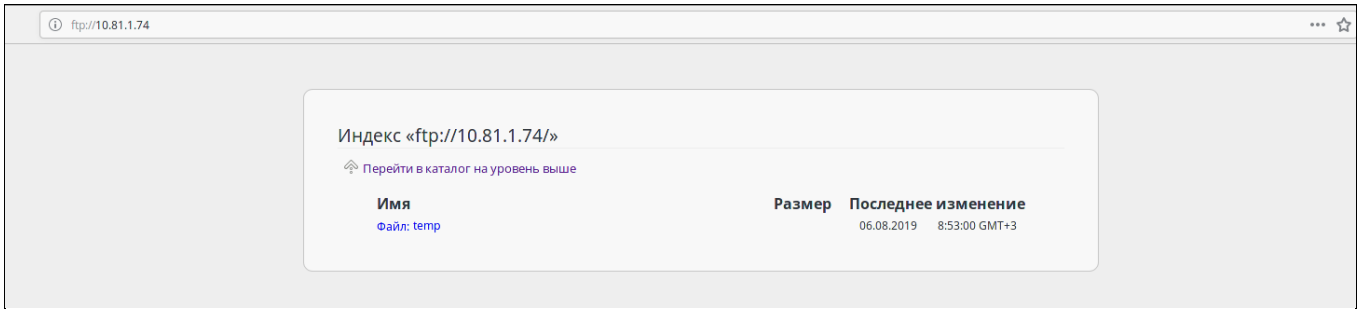
```
anonymous_enable=YES
```

Теперь для управления файлами будет использоваться определённый каталог (обычно **/var/ftp/pub**) и определённый пользователь — обычно **ftp**.

Можно определить и другое расположение файлов для анонимного доступа по FTP, т. е. изменить домашнюю директорию пользователя **ftp**:

```
mkdir -p /srv/share/ftp
usermod -d /srv/share/ftp ftp
```

Пример доступа к папке



Для авторизованного доступа проще всего включить использование локальных учётных записей на сервере. Для этого нужно привести строку в файле конфигурации **vsftpd.conf** к виду:

```
local_enable=YES
```

Примечание.

Для авторизации локальных пользователей используется пароль пользователя для локального входа в систему.

Чтобы ограничить передвижение авторизованного пользователя в рамках одной папки, используется следующий алгоритм:

1. В конфигурационный файл **vsftpd.conf** добавьте строку:

```
user_config_dir=/etc/vsftpd_user_conf
```

2. Создайте папку, в которой будет храниться правило для пользователя:

```
mkdir /etc/vsftpd_user_conf
```

3. Создайте файл, имя которого равно имени пользователя, которому требуется разрешить доступ к папке:

```
nano /etc/vsftpd_user_conf/<ИМЯ_ПОЛЬЗОВАТЕЛЯ>
```

4. Добавьте строку:

```
local_root=/serv/ftp/
```

5. Для добавления доступа другому пользователю к папке создайте новый файл **/etc/vsftpd_user_conf/<ИМЯ_ПОЛЬЗОВАТЕЛЯ>** с аналогичным содержимым.

6. Кроме этого, для ограничения перемещения по дереву каталогов вне домашней директории, в конфигурационном файле /etc/vsftpd/vsftpd.conf раскомментируйте параметр chroot_local_user:

```
# запретить выходить из домашнего каталога на верхний уровень
chroot_local_user=YES
```

а ниже добавьте параметр для разрешения пользователю права записи в домашний каталог:

```
allow_writeable_chroot=YES
```

7. Далее перезапустите **vsftpd** для активации внесенных изменений:

```
systemctl restart vsftpd
```

Монтирование ftp-ресурса в качестве директории РЕД ОС

Ручной вариант монтирования

Осуществляется при помощи утилиты **curlftpfs**. Данная утилита позволяет монтировать ftp-ресурсы в качестве локальных папок на ПК.

Установите пакеты:

```
dnf install curlftpfs autofs
```

Выполните запуск сервиса **autofs**:

```
systemctl enable autofs --now
systemctl restart vsftpd
```

Пример монтирования представлен в следующих командах:

Общий синтаксис:

```
curlftpfs ftp://SERVER /<ТОЧКА_МОНТИРОВАНИЯ>
```

1) Анонимное монтирование:

```
curlftpfs ftp://10.81.1.74 /serv/ftp
```

Если требуется разрешить доступ для всех, то добавляется параметр:

```
-o allow_other
```

2) Авторизованное монтирование:

```
curlftpfs ftp://10.81.1.74 /serv/ftp -o user=username:password
```

Если требуется разрешить доступ для всех, то к `-o user=username:password` добавляется через запятую:

```
-o user=username:password,allow_other
```

Автоматический вариант монтирования при помощи autofs

Данная утилита использует для конфигурирования шаблоны, расположенные в **/etc/**. Основной шаблон называется **auto.master**, он может указывать на один или несколько других шаблонов для конкретных типов. В данном случае будет рассмотрено монтирование **ftp**.

Создайте файл:

```
nano /etc/auto.ftp
```

Содержимое (авторизованный вариант):

```
10.81.1.74 -fstype=fuse,allow_other    :curlftpfs\#username:password@10.81.1.74
```

Содержимое (анонимный вариант):

```
10.81.1.74 -fstype=fuse,allow_other    :curlftpfs\#10.81.1.74
```

В файл **/etc/auto.master** добавьте строку:

```
/serv/ftp /etc/auto.ftp --ghost,--timeout=30
```

Настройка ProFTPD

Установка и настройка proftpd
Создание отдельных пользователей для авторизации на FTP-сервере
Настройка анонимного пользователя
Создание виртуальных пользователей
Настройка прав доступа
Настройка ProFTPd с использованием TLS

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: proftpd-1.3.6e-1

ProFTPD — это FTP-сервер, который позволяет использовать виртуальных пользователей с сопоставимыми с UID идентификаторами системных пользователей, а также настраивать анонимный доступ, ограничивать права доступа и работать через протокол FTP с поддержкой TLS для безопасной передачи данных. Преимущества ProFTPD также включают гибкость настройки, возможность установки квот на дисковое пространство, ограничение скорости передачи данных, управление правами доступа.

Установка и настройка proftpd

Для установки **proftpd** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install proftpd proftpd-utils
```

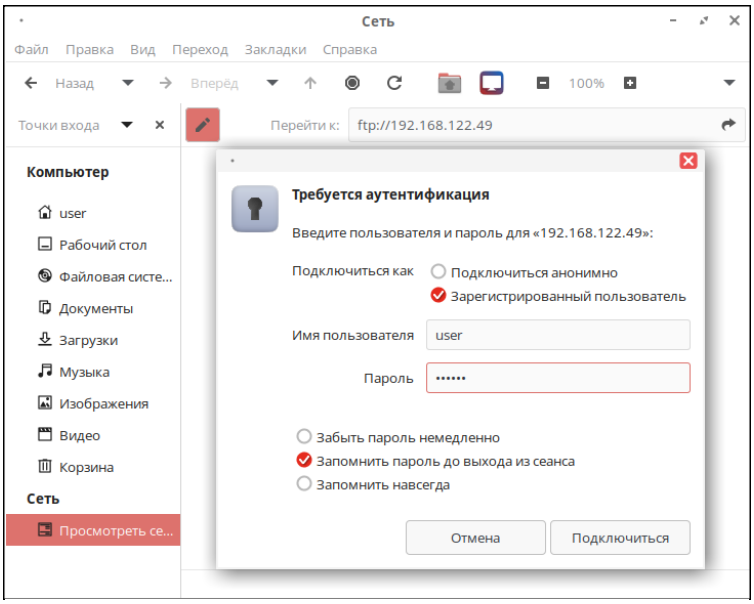
Запустите сервис **proftpd** и добавьте его в автозагрузку:

```
systemctl enable proftpd --now
```

Для проверки статуса сервиса **proftpd** выполните команду:

```
systemctl status proftpd

● proftpd.service - ProFTPD FTP Server
     Loaded: loaded (/usr/lib/systemd/system/proftpd.service; enabled; vendor preset: disabled)
     Active: active (running) since Tue 2025-01-14 14:35:47 MSK; 19h ago
    Process: 1924238 ExecStartPre=/usr/sbin/proftpd --configtest (code=exited, status=0/SUCCESS)
   Main PID: 1924243 (proftpd)
      Tasks: 1 (limit: 2329)
     Memory: 38.5M
        CPU: 1.649s
     CGroup: /system.slice/proftpd.service
             └─1924243 proftpd: (accepting connections)

янв 14 14:35:39 localhost.localdomain systemd[1]: Starting proftpd.service - ProFTPD FTP Server...
янв 14 14:35:40 localhost.localdomain proftpd[772]: Checking syntax of configuration file
янв 14 14:35:47 localhost.localdomain proftpd[860]: daemon[860]: 127.0.0.1: ProFTPD 1.3.8b (maint)
янв 14 14:35:47 localhost.localdomain systemd[1]: Starting proftpd.service - ProFTPD FTP Server...
```

После запуска службы **proftpd** FTP-сервер сразу готов предоставлять доступ с аутентификацией от имен существующих локальных пользователей данного сервера. При этом предоставляется полный доступ к домашней директории пользователя. Произвести подключение можно с помощью *файлового менеджера* или ftp-клиента **FileZilla**.



Создание отдельных пользователей для авторизации на FTP-сервере

Добавьте группу **ftpgroup** и пользователя **ftpuser**:

```
groupadd ftpgroup
useradd ftpuser -d /home/ftpuser -s /bin/false -g ftpgroup
```

Здесь:

- **ftpuser** – имя пользователя;
- **-d /home/ftpuser** – домашний каталог для пользователя ftpuser;
- **-s /bin/false** – ключ указывает, что пользователю будет отключен shell в целях безопасности;
- **ftpgroup** – группа пользователя.

Назначьте пароль для пользователя **ftpuser** командой:

```
passwd ftpuser
```

Выполните команду, которая добавит в **/etc/shells** запись **/bin/false** в качестве недействительной оболочки (shell). Это предотвратит непосредственный вход в систему пользователя **ftpusers**, но для входа по **ftp** этого будет достаточно:

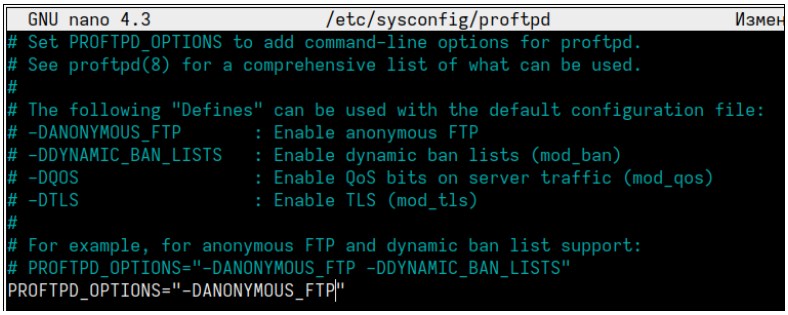
```
echo '/bin/false' >> /etc/shells
```

Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

Настройка анонимного пользователя

Для активации анонимного доступа добавьте параметр `PROFTPD_OPTIONS="-DANONYMOUS_FTP"` в файл **/etc/sysconfig/proftpd**.



Сервер **proftpd** сопоставляет анонимных клиентов (**anonymous**) с пользователем **FTP**. Пользователь с логином **FTP** имеет оболочку **/sbin/nologin**, которая на самом деле не является оболочкой (**shell**), и такому пользователю будет запрещено запускать сеанс командой строки. Однако его можно использовать в качестве пользователя на FTP-сервере.

Добавьте ложную оболочку **/sbin/nologin** в файл списка оболочек **/etc/shells**.

```
echo '/sbin/nologin' >> /etc/shells
```

Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

При подключении анонимному пользователю доступны два каталога — **pub** и **uploads**, которые находятся в корневой директории FTP-сервера **/var/ftp/**.

Директория **/pub** – общедоступный каталог FTP, который имеет права только на чтение.

Директория **/uploads** – имеет права на запись, но при этом просматривать содержимое директории запрещено.

Создание виртуальных пользователей

В качестве примера настроим доступ к FTP-серверу с возможностью авторизации под *виртуальным* пользователем. Хранить виртуальных пользователей можно в файле или базе данных.

Создайте домашний каталог для пользователя, при подключении виртуальным пользователем будет открываться именно эта директория, например:

```
mkdir /home/vftp1
```

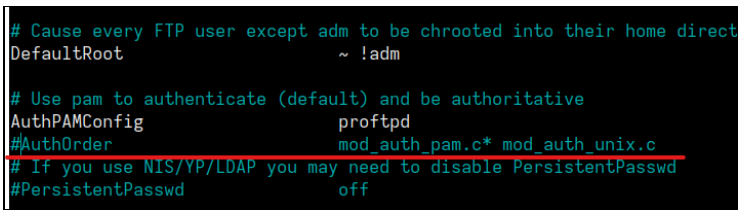
После этого создайте файл с паролями и виртуальными пользователями, которые сопоставляются с локальными учетными записями по их **UID** и **GID**:

```
ftpasswd --passwd --file=/etc/proftpd/ftpd.passwd --name=vftp1 --uid=48 --gid=48 --home=/home/vftp1 --shell=/sbin/nologin
```

Здесь:

- **/etc/proftpd/ftpd.passwd** — полный путь до файла, в котором хранятся пользователи;
- **vftp1** — имя пользователя (логин);
- **uid** и **gid** — идентификаторы пользователя и группы системной учетной записи, от которой будет выступать сервер;
- **/home/vftp1** — домашний каталог пользователя;
- **/sbin/nologin** — оболочка, запрещающая локальный вход пользователя в систему.

Откройте файл конфигурации **/etc/proftpd.conf** и закомментируйте строку, которая начинается на «**AuthOrder**».



Создайте дополнительный конфигурационный файл в каталоге **/etc/proftpd/conf.d** (в нем находятся пользовательские конфигурационные файлы) и добавьте следующие строки:

```
nano /etc/proftpd/conf.d/virtual.conf
```

```
AuthUserFile /etc/proftpd/ftpd.passwd
AuthOrder mod_auth_file.c
```

Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

Теперь можно подключится к FTP-серверу от имени виртуального пользователя **vftp1**.

Настройка прав доступа

Разберем пример, когда к одной и той же папке необходимо будет предоставить разные права — одному пользователю *только на чтение*, другому — *на чтение и запись*.

Производим изменения в конфигурационном файле **/etc/proftpd/conf.d/rights.conf**, добавив следующее содержимое:

```
<Directory /var/www>
  <Limit WRITE>
    Order deny,allow
    AllowUser vuser1
  </Limit>
  <Limit ALL>
    AllowAll
  </Limit>
 </Directory>
```

где:

- **<Directory /var/www>** — задаются права для директории /var/www;
- **AllowUser vuser1** — разрешение для **vuser1** только права на чтение, для других пользователей запись и чтение файлов доступны.

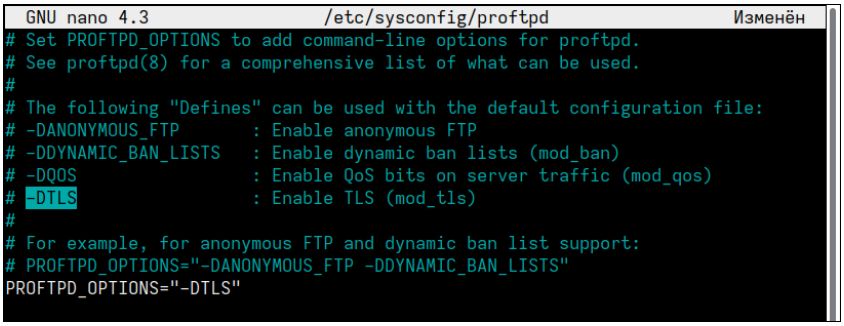
Перезапустите службу **proftpd** для применения настроек:

```
systemctl restart proftpd
```

Настройка ProFTPd с использованием TLS

Протокол TLS — криптографический протокол, который обеспечивает защищённый обмен данными между сервером и клиентом.

В файле **/etc/sysconfig/proftpd** задайте значение для опции `PROFTPD_OPTIONS: "-DTLS"`.



Создайте сертификат с помощью команды:

```
openssl req -x509 -days 1461 -nodes -newkey rsa:2048 -sha256 -keyout /etc/pki/tls/private/postfix.key -out /etc/pki/tls/certs/proftpd.pem -subj "/C=RU/ST=MSK/L=Murom/O=REDos Security/OU=IT Department/CN=192.168.1.240/CN=ftp"
```

Затем в файле **/etc/proftpd/mod_tls.conf** необходимо определить дополнительные опции и пути к сертификату, которые были указаны в генерации сертификата:

```
TLSEngine on
TLSRequired off
TLSProtocol SSLv23 TLSv1.2
TLSCertificateChainFile /etc/pki/tls/certs/proftpd.pem
TLSRSACertificateFile /etc/pki/tls/certs/proftpd.pem
TLSRSACertificateKeyFile /etc/pki/tls/private/postfix.key
```

В итоге файл **/etc/proftpd/mod_tls.conf** должен выглядеть следующим образом:

```
# TLS (http://www.castaglia.org/proftpd/modules/mod_tls.html)
<IfModule mod_tls.c>
  TLSEngine                  on
  TLSRequired                off
  TLSProtocol                SSLv23 TLSv1.2
  TLSCertificateChainFile    /etc/pki/tls/certs/proftpd.pem
  TLSRSACertificateFile      /etc/pki/tls/certs/proftpd.pem
  TLSRSACertificateKeyFile   /etc/pki/tls/private/postfix.key
  # Relax the requirement that the SSL session be re-used for data trans>
  TLSOptions                 NoSessionReuseRequired
  TLSLog                     /var/log/proftpd/tls.log
  <IfModule mod_tls_shmcache.c>
    TLSSessionCache          shm:/file=/run/proftpd/sesscache
  </IfModule>
</IfModule>
```

В файле конфигурации **/etc/proftpd.conf** необходимо прописать строку `Include /etc/proftpd/mod_tls.conf`, для того чтобы FTP-сервер использовал конкретные настройки конфигурации.

```
# A basic anonymous configuration, with an upload directory
# Enable this with PROFTPD_OPTIONS=-DANONYMOUS_FTP in /etc/sysconfig/pro>
<IfDefine ANONYMOUS_FTP>
Include /etc/proftpd/anonftp.conf
</IfDefine>

# Include other custom configuration files
Include /etc/proftpd/mod_tls.conf
```

Перезапустите службу **proftpd** для применения изменений:

```
systemctl restart proftpd
```

Настройка NFS

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** nfs-utils-2.5.2-0, nfs4-acl-tools-0.3.5-2

Если нет пакета **NFS**, его необходимо установить:

```
dnf install nfs-utils nfs4-acl-tools
```

Все настройки сервера хранятся в файле **/etc/exports**. Открываем его на редактирование

```
nano /etc/exports
```

и добавляем в конец файла строки вида (строк может быть произвольное количество):

```
/data 192.168.1.1/255.255.255.0(rw,insecure,nohide,all_squash,anonuid=1000,anongid=1000,no_subtree_check)
```

- **/data** –путь к папке, для которой раздается доступ;
- **192.168.1.1** –IP-адрес, которому раздается доступ к папке (можно указать всю сеть, тогда запись примет вид 192.168.1.0/24)
- **(rw,no_root_squash,sync)** –набор опций, опции могут быть:
  - **rw** –чтение запись(может принимать значение ro-только чтение);
  - **no_root_squash** – по умолчанию пользователь root на клиентской машине не будет иметь доступа к разделяемой директории сервера. Этой опцией мы снимаем это ограничение. В целях безопасности этого лучше не делать;
  - **nohide** - NFS автоматически не показывает нелокальные ресурсы (например, примонтированые с помощью mount –bind), эта опция включает отображение таких ресурсов;
  - **sync** – синхронный режим доступа(может принимать обратное значение- async). sync (async) - указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами. Опция async указывает серверу не ждать записи информации на диск, что повышает производительность, но понижает надежность, т.к. в случае обрыва соединения или отказа оборудования возможна потеря данных;
  - **noaccess** – запрещает доступ к указанной директории. Может быть полезной, если перед этим вы задали доступ всем пользователям сети к определенной директории, и теперь хотите ограничить доступ в поддиректории лишь некоторым пользователям.
  - **all_squash** – подразумевает, что все подключения будут выполнятся от анонимного пользователя
  - **subtree_check (no_subtree_check)** - в некоторых случаях приходится экспортировать не весь раздел, а лишь его часть. При этом сервер NFS должен выполнять дополнительную проверку обращений клиентов, чтобы убедиться в том, что они предпринимают попытку доступа лишь к файлам, находящимся в соответствующих подкаталогах. Такой контроль поддерева (subtree checks) несколько замедляет взаимодействие с клиентами, но если отказаться от него, могут возникнуть проблемы с безопасностью системы. Отменить контроль поддерева можно с помощью опции no_subtree_check. Опция subtree_check, включающая такой контроль, предполагается по умолчанию. Контроль поддерева можно не выполнять в том случае, если экспортируемый каталог совпадает с разделом диска;
  - **anonuid=1000** – привязывает анонимного пользователя к «местному» пользователю;
  - **anongid=1000** – привязывает анонимного пользователя к группе «местного» пользователя.

Чтобы запустить демон (службу) и добавить её в автозагрузку, прописываем следующие команды:

```
systemctl enable nfs-server.service --now
```

При положительном результате вы увидите, что демон запустился и функционирует

```
Redirecting to /bin/systemctl status nfs.service
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; vendor preset: disabled)
   Active: active (exited) since Вт 2019-08-06 15:23:21 MSK; 3s ago
  Process: 732 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
  Process: 729 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
Main PID: 732 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/nfs-server.service
```

Впоследствии после внесения изменений в файл **/etc/exports** не обязательно перезапускать сервер, достаточно выполнить:

```
exportfs -ra
```

Настройка iSCSI

Конфигурация хранилища
Конфигурация клиента

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** targetcli-2.1.54-6, iscsi-initiator-utils-6.2.1.4-6

Конфигурация хранилища

Создайте диск LVM на целевом сервере, чтобы использовать его в качестве общего хранилища для клиентов.

Проверьте доступные диски:

```
fdisk -l | grep -i sd

Диск /dev/sda: 200 GiB, 214748364800 байт, 419430400 секторов
/dev/sda1 * 2048 2099199 2097152 1G 83 Linux
/dev/sda2 2099200 419430399 417331200 199G 8e Linux LVM
Диск /dev/sdb: 35 GiB, 37580963840 байт, 73400320 секторов
```

Из приведенного выше примера видно, что в системе доступно 35 ГБ дискового пространства (**dev/sdb**). Создайте раздел нужного объёма. В примере, на указанном выше диске, будет задействовано 5 ГБ для LVM.

```
fdisk /dev/sdb

Добро пожаловать в fdisk (util-linux 2.37.3).
Изменения останутся только в памяти до тех пор, пока вы не решите записать их.
Будьте внимательны, используя команду write.
Устройство не содержит стандартной таблицы разделов.
Создана новая метка DOS с идентификатором 0xaee65952.
Команда (m для справки): n → Новый раздел
Тип раздела
   p   основной (0 primary, 0 extended, 4 free)
   e   расширенный (контейнер для логических разделов)
Выберите (по умолчанию - p):p → Основной раздел
Номер раздела (1-4, default 1): 1 → Номер раздела
Первый сектор (2048-73400319, default 2048):  → Нажмите Enter
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-73400319, default 73400319): +5G → Задайте размер раздела
 Создан новый раздел 1 с типом 'Linux' и размером 5 GiB.
Команда (m для справки): t → Измените метку
Выбранный раздел 1
Шестнадцатеричный код (введите L для получения списка кодов): 8e → Изменить метку на LVM
Тип раздела 'Linux' изменен на 'Linux LVM'.
Команда (m для справки): w → Сохраните
Таблица разделов была изменена.
Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
```

Создайте LVM с разделом **/dev/sdb1** (замените **/dev/sdb1** на имя вашего диска):

```
pvcreate /dev/sdb1

Physical volume "/dev/sdb1" successfully created.
```

```
vgcreate vg_iscsi /dev/sdb1

Volume group "vg_iscsi" successfully created
```

```
lvcreate -l 100%FREE -n lv_iscsi vg_iscsi

Logical volume "lv_iscsi" created.
```

Создание таргета iSCSI

Установите пакет **targetcli**:

```
dnf install targetcli
```

Добавьте службу **target** в автозагрузку и запустите:

```
systemctl enable target --now
```

Откройте **targetcli**:

```
targetcli

targetcli shell version 2.1.53
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.
/>
```

Просмотрите структуру, в виде которой представлен таргет, командой:

```
/> ls

  1. o- / ..... [...]
  2.   o- backstores ..... [...]
  3.   | o- block ..... [Storage Objects: 0]
  4.   | o- fileio ..... [Storage Objects: 0]
  5.   | o- pscsi ..... [Storage Objects: 0]
  6.   | o- ramdisk ..... [Storage Objects: 0]
  7.   o- iscsi ..... [Targets: 0]
  8.   o- loopback ..... [Targets: 0]
  9.   o- vhost ..... [Targets: 0]
```

Помощь можно вызывать в любом разделе внутри **targetcli**:

```
help
```

Перейдите в раздел **block**:

```
/> cd backstores/block
```

Создайте блочное устройство, используя ранее созданный логический том:

```
/backstores/block> create scsi_disk1 /dev/vg_iscsi/lv_iscsi

Created block storage object scsi_disk1 using /dev/vg_iscsi/lv_iscsi.
```

Создайте таргет (цель):

```
/backstores/block> cd /iscsi
/iscsi> create

Created target iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
```

Просмотреть структуру таргета можно командой:

```
/iscsi> ls

o- iscsi ..... [Targets: 1]
  o- iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625 ..... [TPGs: 1]
    o- tpg1 ..... [no-gen-acls, no-auth]
      o- acls ..... [ACLs: 0]
```

```
    o- luns ..... [LUNs: 0]
    o- portals ..... [Portals: 1]
      o- 0.0.0.0:3260 ..... [OK]
```

Здесь:

- **iqn** — имя таргета.
- **tpg1** (Target Portal Group) – список IP-адресов и TCP портов, которые будет слушать этот таргет.
- **acls** – список адресов, с которых можно будет подключиться к таргету,
- **luns** – список адресов дискового устройства в сетях хранения,
- **portals** – список IP-адресов и портов, которые будет слушать таргет.

Создайте ACL для клиентской машины. Для этого перейдите на уровень *acls*, используя команду cd и клавиши управления со стрелками «вверх» и «вниз». Затем используйте команду create и имя инициатора, которое находится в файле **/etc/iscsi/initiatorname.iscsi** на клиентской машине:

```
/iscsi/iqn.20...625/tpg1/acls> create iqn.1994-05.com.redhat:70f2a07b2daf

Created Node ACL for iqn.1994-05.com.redhat:70f2a07b2daf
Created mapped LUN 0.
Created mapped LUN 1.
```

Создайте LUN. Он должен использовать раннее созданный объект хранилища. В примере это «**scsi_disk1**». Перейдите на уровень «**luns**», используя команду cd и клавиши управления со стрелками «вверх» и «вниз». После чего используйте команду create:

```
/iscsi/iqn.20...625/tpg1/luns> create /backstores/block/scsi_disk1

Created LUN 0.
Created LUN 0->0 mapping in node ACL iqn.1994-05.com.redhat:70f2a07b2daf
```

Проверьте конфигурацию сервера:

```
/iscsi/iqn.20...625/tpg1/luns> cd /
/> ls

o- / ..... [...]
  o- backstores ..... [...]
  | o- block ..... [Storage Objects: 1]
  | | o- scsi_disk1 ..... [/dev/vg_iscsi/lv_iscsi (5.0GiB) write-thru activated]
  | |   o- alua ..... [ALUA Groups: 1]
  | |     o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
  | o- fileio ..... [Storage Objects: 0]
  | o- pscsi ..... [Storage Objects: 0]
  | o- ramdisk ..... [Storage Objects: 0]
  o- iscsi ..... [Targets: 1]
  | o- iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625 ..... [TPGs: 1]
  |   o- tpg1 ..... [no-gen-acls, no-auth]
  |     o- acls ..... [ACLs: 1]
  |     | o- iqn.1994-05.com.redhat:70f2a07b2daf ..... [Mapped LUNs: 1]
  |     |   o- mapped_lun0 ..... [lun0 block/scsi_disk1 (rw)]
  |     o- luns ..... [LUNs: 1]
  |     | o- lun0 ... [block/scsi_disk1 (/dev/vg_iscsi/lv_iscsi) (default_tg_pt_gp)]
  |     o- portals ..... [Portals: 1]
  |       o- 0.0.0.0:3260 ..... [OK]
  o- loopback ..... [Targets: 0]
  o- vhost ..... [Targets: 0]
```

Сохраните конфигурацию:

```
/> saveconfig

Last 10 configs saved in /etc/target/backup/.
Configuration saved to /etc/target/saveconfig.json
```

```
/> exit

Global pref auto_save_on_exit=true
```

```
Last 10 configs saved in /etc/target/backup/.
Configuration saved to /etc/target/saveconfig.json
```

Перезапустите сервис таргета:

```
systemctl restart target
```

Конфигурация клиента

На клиентской машине с РЕД ОС, к которой планируется подключение хранилища iSCSI, уже установлен клиент **iscsi-initiator-utils**. Если его нет в системе, необходимо установить пакет и добавить необходимые службы в автозагрузку:

```
dnf install iscsi-initiator-utils
systemctl enable iscsid iscsi --now
```

Отредактируйте файл **/etc/iscsi/initiatorname.iscsi**, если хотите изменить имя инициатора:

```
nano /etc/iscsi/initiatorname.iscsi
```

измените имя инициатора:

```
InitiatorName=iqn.1994-05.com.redhat:70f2a07b2daf
```

Найдите сервер (таргет) с помощью команды:

```
iscsiadm -m discovery -t st -p 192.168.81.190

192.168.81.190:3260,1 iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625
```

Перезапустите службы:

```
systemctl restart iscsid iscsi
```

Подключитесь к таргету (серверу):

```
iscsiadm -m node -T iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625 -p 192.168.81.190 -l

Logging in to [iface: default, target: iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625, portal: 192.168.81.190,3260]
Login to [iface: default, target: iqn.2003-01.org.linux-iscsi.ro73.x8664:sn.4a0b7ff2b625, portal: 192.168.81.190,3260] successful.
```

Проверить подключение диска можно командой:

```
fdisk -l
```

В выводе должно появиться подключенное iscsi-устройство:

```
    ...   ...   ...
    Диск /dev/sdb: 4,102 GiB, 5364514816 байт, 10477568 секторов
    Disk model: scsi_disk1
    Единицы: секторов по 1 * 512 = 512 байт
    Размер сектора (логический/физический): 512 байт / 512 байт
    Размер I/O (минимальный/оптимальный): 512 байт / 33550336 байт
```

Создайте файловую систему на диске *iscsi*.

```
mkfs.ext4 /dev/sdb

    mke2fs 1.44.6 (5-Mar-2019)
    Creating filesystem with 1309696 4k blocks and 327680 inodes
    Filesystem UUID: 5be3f332-b730-4aae-baaf-6c5e8cda0a57
    Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
```

```
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

Смонтируйте диск в систему:

```
mount /dev/sdb /mnt
```

Проверка осуществляется командой:

```
df -hT
```

```
Файловая система         Тип      Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs                 devtmpfs   1,9G          0  1,9G          0% /dev
tmpfs                    tmpfs      2,0G          0  2,0G          0% /dev/shm
tmpfs                    tmpfs      785M        3,4M  782M          1% /run
/dev/mapper/ro_redos-root ext4        26G        6,8G   18G         28% /
/dev/sda1                ext4       976M        159M  750M         18% /boot
tmpfs                    tmpfs      393M         76K  393M          1% /run/user/42
tmpfs                    tmpfs      393M        128K  393M          1% /run/user/1000
tmpfs                    tmpfs      393M         68K  393M          1% /run/user/0
/dev/sdb                 ext4       4,9G         20M  4,6G          1% /mnt
```

Настройте автоматическое монтирование хранилища. Для этого понадобится **UUID** диска *iscsi*:

```
blkid /dev/sdb
```

```
/dev/sdb: UUID="5be3f332-b730-4aae-baaf-6c5e8cda0a57" TYPE="ext4"
```

Теперь необходимо отредактировать файл **/etc/fstab**:

```
nano /etc/fstab
```

Добавив в него запись вида:

```
UUID=5be3f332-b730-4aae-baaf-6c5e8cda0a57 /mnt ext4 _netdev 0 0
```

Теперь, при перезагрузке инициатора (клиентской машины), диск *iscsi* будет подключаться к системе автоматически.

Установка и настройка веб-сервера nginx

Предварительная настройка
Установка и запуск nginx
Настройка nginx

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: nginx-1:1.26.2-1

Nginx — высокопроизводительный веб-сервер и почтовый прокси-сервер с открытым исходным кодом, обслуживающий большое количество высоконагруженных сайтов по всему миру. **Nginx** завоевал широкую популярность благодаря своей лёгкости, надёжности, масштабируемости и простоте настройки.

Предварительная настройка

Для настройки веб-сервера **nginx** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее настройка будет производиться с правами суперпользователя **root**, если не указано иное.

Внесите DNS-запись с наименованием веб-сервера в файл **/etc/hosts**:

```
echo <IP-адрес> <название_сайта> > /etc/hosts
```

Например:

```
echo 127.0.0.1 testsite.ru > /etc/hosts
```

Установка и запуск nginx

Установите **nginx** с помощью команды:

```
dnf install nginx
```

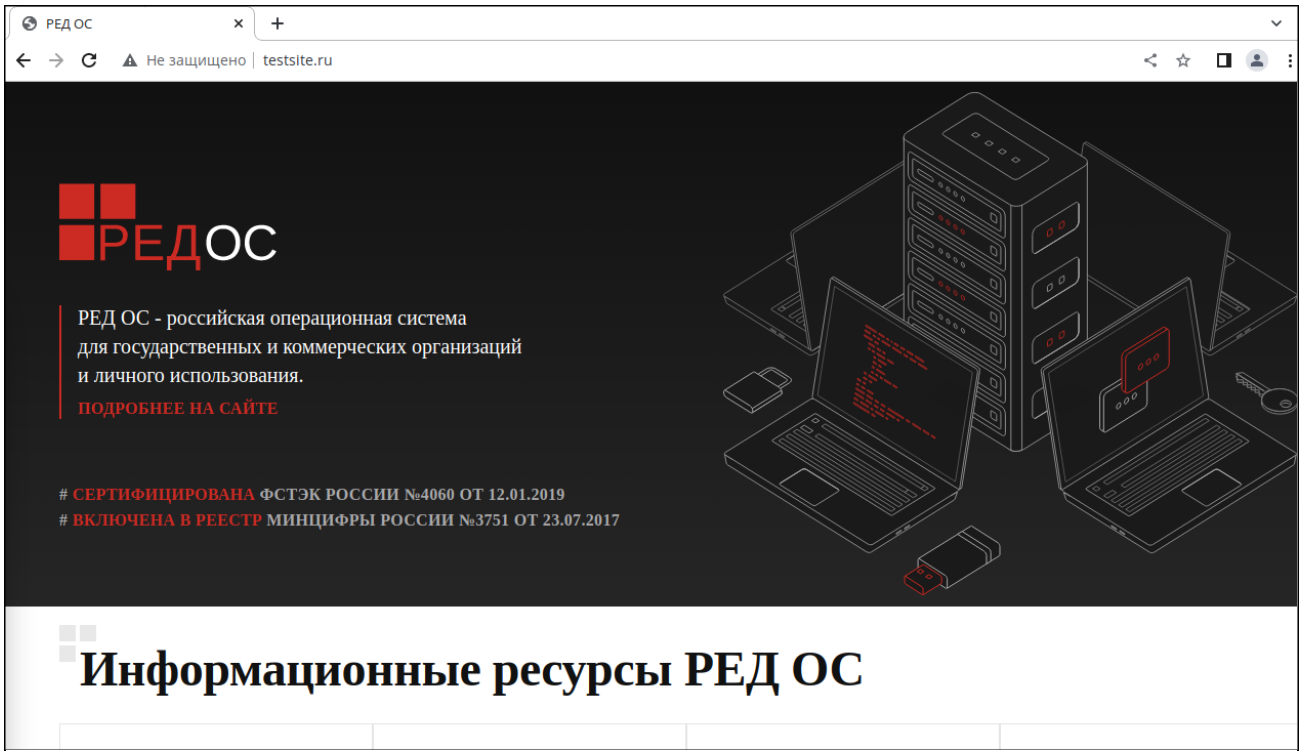
Запустите и добавьте в автозагрузку службу **nginx**:

```
systemctl enable nginx --now
```

Проверьте статус службы **nginx**:

```
systemctl status nginx

 nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
     Active: active (running) since Mon 2024-04-01 13:55:33 MSK; 2s ago
    Process: 637943 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 637950 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 637951 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 637952 (nginx)
      Tasks: 13 (limit: 18964)
     Memory: 11.3M
        CPU: 66ms
     CGroup: /system.slice/nginx.service
```

Для проверки перейдите в браузере по ссылке http://testsite.ru/.



Настройка nginx

Создайте каталог, в котором будут хранится файлы сайта:

```
mkdir -p /var/www/testsite.ru/
```

Создайте файл сайта:

```
nano /var/www/testsite.ru/index.html
```

В файл добавьте следующее содержимое, которое задаст первоначальный вид страницы:

```
<html>
  <head>
    <title>Hello!</title>
  </head>
  <body>
    <h1>Success!</h1>
  </body>
 </html>
```

Создайте каталог **vhosts** в папке **nginx**:

```
mkdir -p /etc/nginx/vhosts/
```

Далее необходимо создать конфигурационный файл, отвечающий за запросы **nginx** к файлам сайта:

```
nano /etc/nginx/vhosts/testsite.conf
```

В файле укажите следующую настройку:

```
server{
  listen 80;
  server_name testsite.ru;
  root /var/www/testsite.ru;
  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;
```

```
    index index.html;
}
```

Затем укажите запуск сервера в **/etc/nginx/nginx.conf**:

```
include /etc/nginx/vhosts/*.conf;
```

ВАЖНО!

Данную строку необходимо указывать **перед** общей настройкой секции server!

```
include /etc/nginx/conf.d/*.conf;
include /etc/nginx/vhosts/*.conf;
server {
    listen       80;
    listen       [::]:80;
    server_name  _;
    root         /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
```

Далее назначьте необходимые права для файлов, указав следующие параметры:

```
chown -R $USER:$USER /var/www/testsite.ru/index.html
chmod -R 755 /var/www/testsite.ru
```

Проверьте конфигурацию **nginx** на наличие ошибок:

```
nginx -t

 nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
 nginx: configuration file /etc/nginx/nginx.conf test is successful
```

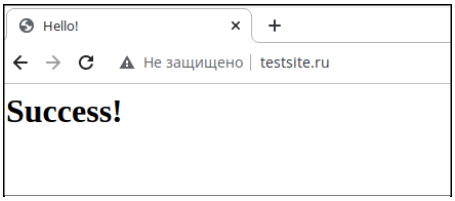
Перезапишите правила **Selinux**:

```
restorecon -Rv /var/www/testsite.ru/
```

Для применения внесенных изменений перезапустите службу **nginx**:

```
systemctl restart nginx
```

Выполните проверку работы в браузере, открыв ссылку http://testsite.ru.



Настройка прокси-сервера nginx для веб-приложений на Node.js

Предварительная настройка
Установка пакетов и запуск служб
Настройка Node.js
Настройка nginx
Настройка автозапуска systemd

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: nginx-1:1.26.2-1, nodejs-1:20.15.1-1

Nginx — высокопроизводительный веб-сервер и почтовый прокси-сервер с открытым исходным кодом, обслуживающий большое количество высоконагруженных сайтов по всему миру. **Nginx** завоевал широкую популярность благодаря своей лёгкости, надёжности, масштабируемости и простоте настройки.

Предварительная настройка

Для настройки веб-сервера **nginx** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее настройка будет производиться с правами суперпользователя **root**, если не указано иное.

Внесите DNS-запись с наименованием веб-сервера в файл **/etc/hosts**:

```
echo <IP-адрес> <название_сайта> > /etc/hosts
```

Например:

```
echo 127.0.0.1 testsite.ru > /etc/hosts
```

Установка пакетов и запуск служб

Установите **nginx** и **node.js** с помощью команды:

```
dnf install nginx nodejs
```

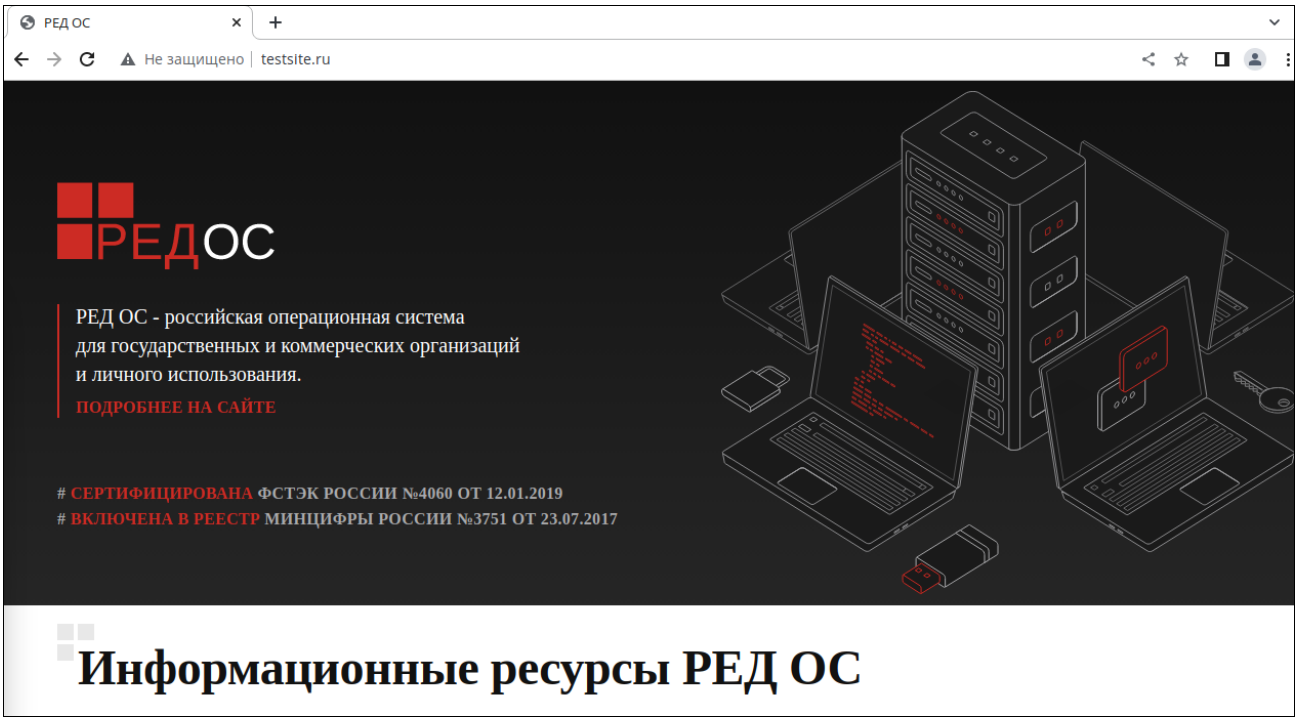
Запустите и добавьте в автозагрузку службу **nginx**:

```
systemctl enable nginx --now
```

Проверьте статус службы **nginx**:

```
systemctl status nginx

 nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
     Active: active (running) since Mon 2024-04-01 13:55:33 MSK; 2s ago
    Process: 637943 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 637950 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 637951 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 637952 (nginx)
      Tasks: 13 (limit: 18964)
     Memory: 11.3M
        CPU: 66ms
     CGroup: /system.slice/nginx.service
```

Для проверки работы в адресной строке браузера введите http://testsite.ru.



Настройка Node.js

Создайте каталог, в котором будут хранится файлы веб-приложения **Node.js**:

```
mkdir -p /var/www/testsite.ru
```

Создайте файл запуска приложения:

```
nano /var/www/testsite.ru/server.js
```

В файл **server.js** добавьте следующее содержимое:

```
const http = require('http');
 const server = http.createServer((req, res) => {

   res.writeHead(200, {
   'Content-Type': 'text/plain; charset=UTF-8'
   });
 res.end('Hello, world!');
 });

 server.listen(3000, () => {
  console.log('Start NodeJS Server on port 3000');
 });
```

Запустите приложение:

```
node /var/www/testsite.ru/server.js
```

Для проверки работы в адресной строке браузера введите http://testsite.ru:3000.



Далее назначьте необходимые права для файлов, указав следующие параметры:

```
chown -R $USER:$USER /var/www/testsite.ru/server.js
chmod -R 755 /var/www/testsite.ru
```

Настройка nginx

Создайте каталог **vhosts** в папке **nginx**:

```
mkdir -p /etc/nginx/vhosts/
```

Далее необходимо создать конфигурационный файл, отвечающий за перенаправление (проксирование) запросв **nginx** к файлам сайта:

```
nano /etc/nginx/vhosts/testsite.conf
```

В файле укажите следующую настройку:

```
server{
      listen 80;
      server_name testsite.ru;
      access_log /var/log/nginx/access.log;
      error_log /var/log/nginx/error.log;
      location / {
      proxy_pass http://127.0.0.1:3000;
      proxy_set_header Host   $host;
     }
 }
```

Затем укажите запуск сервера в **/etc/nginx/nginx.conf**:

```
include /etc/nginx/vhosts/*.conf;
```

ВАЖНО!

Данную строку необходимо указывать **перед** общей настройкой секции server!

```
include /etc/nginx/conf.d/*.conf;
include /etc/nginx/vhosts/*.conf;
server {
    listen       80;
    listen       [::]:80;
    server_name  _;
    root         /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
```

Проверьте конфигурацию **nginx** на наличие ошибок:

```
nginx -tnginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Добавьте правило **SELinux** для разрешения перенаправления запросов (проксирования):

```
setsebool -P httpd_can_network_connect 1
```

Для применения внесенных изменений перезапустите службу **nginx**:

```
systemctl restart nginx
```

Настройка автозапуска systemd

Для настройки автозапуска веб-приложения **Node.js** создайте файл **node@.service**:

```
nano /etc/systemd/system/node@.service
```

В файле укажите следующую настройку:

```
[Unit]
 Description=NodeJS Service
 After=network.target

 [Service]
 Type=simple
 ExecStart=/usr/bin/node ./server.js
 ExecReload=/bin/kill -HUP $MAINPID
 Restart=on-failure
 WorkingDirectory=/var/www/%i

 [Install]
 WantedBy=multi-user.target
```

> **Примечание.**
>
> Обратите внимание, что **%i** — это переменная, которой передается имя настраиваемого веб-приложения. Имя соответствует названию каталога, в котором хранится веб-приложение.

Для применения внесенных изменений перезапустите конфигурацию **systemd**:

```
systemctl daemon-reload
```

Запустите и добавьте в автозагрузку настраиваемое веб-приложение:

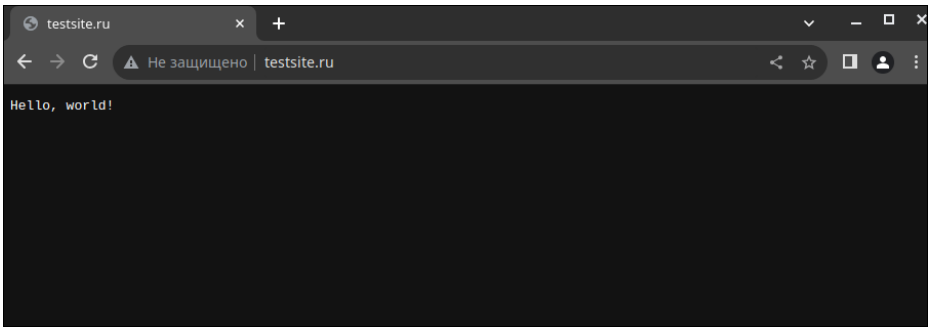
```
systemctl enable node@testsite.ru --now
```

Проверьте статус службы:

```
systemctl status node@testsite.ru
```

В статусе должно отображаться **active (running)**.

Для проверки работы перейдите в браузере по адресу настроенного сайта http://testsite.ru.


testsite.ru
Не защищено | testsite.ru
Hello, world!

Установка и настройка веб-сервера apache

Предварительная настройка
Установка и запуск Apache
Настройка виртуального хоста
Настройка разрешений в SELinux
Управление службой httpd веб-сервера Apache

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: httpd-2.4.62-2

Apache (*Apache HTTP Server*) — это открытое кросс-платформенное программное обеспечение для размещения и поддержки веб-сервера. Основными достоинствами **Apache** считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д.

Предварительная настройка

Для настройки веб-сервера **apache** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее настройка будет производиться с правами суперпользователя **root**, если не указано иное.

Внесите DNS-запись с наименованием веб-сервера в файл **/etc/hosts**:

```
echo <IP-адрес> <название_сайта> >> /etc/hosts
```

Например:

```
echo 192.168.100.185 redsite11.ru >> /etc/hosts
```

Установка и запуск Apache

Установите **Apache** с помощью команды:

```
dnf install httpd -y
```

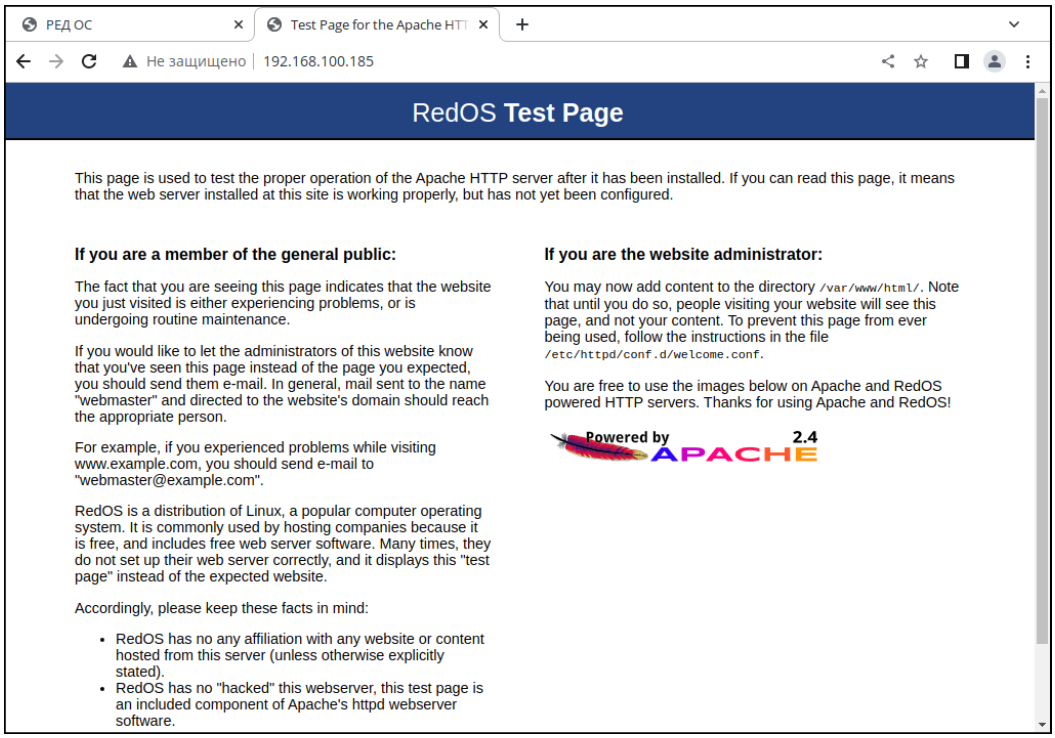
Запустите и добавьте в автозагрузку службу **httpd**:

```
systemctl enable httpd  --now
```

Проверьте статус службы **httpd** командой:

```
systemctl status httpd

tpd.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor pre>
    Active: active (running) since Mon 2024-04-01 14:56:43 MSK; 1min 1s ago
      Docs: man:httpd.service(8)
  Main PID: 813 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
     Tasks: 213 (limit: 2310)
    Memory: 21.2M
       CPU: 133ms
```

Для проверки работы веб-сервера откройте браузер и введите в адресной строке `http://<IP-адрес_вашего_сервера>`. Например, `http://192.168.100.185`.

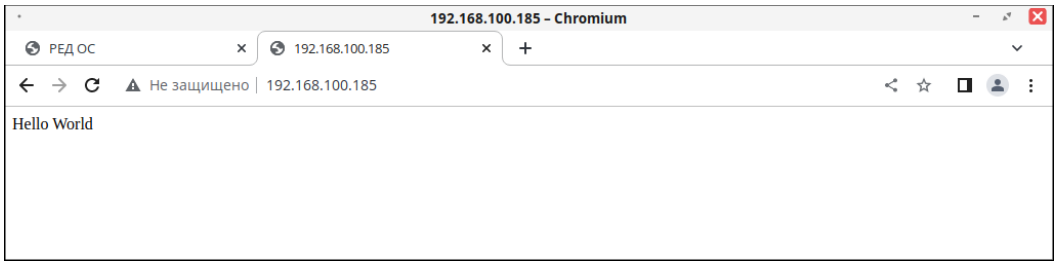


Для проверки корректности установки **Apache** можно создать тестовую страницу с любым содержимым. Для этого выполните:

```
echo "Hello World" > /var/www/html/index.html
```

Команда создаст файл **index.html** и запишет в него содержимое, в данном случае фразу Hello World.

Для просмотра тестовой страницы снова откройте браузер и введите в адресной строке http://<IP-адрес_вашего_сервера>. Например, http://192.168.100.185.



На тестовой странице отображается фраза Hello World, значит, веб-сервер **Apache** работает корректно.

Настройка виртуального хоста

ВАЖНО!

В приведенных примерах необходимо заменить **redsite11.ru** на имя **вашего** реального домена. Только в этом случае файл будет указывать веб-серверу, где найти корневой каталог сайта и куда необходимо сохранять журналы ошибок и обращений к сайту.

Создайте каталог, в котором будут хранится файлы сайта:

```
mkdir -p /var/www/redsite11.ru/html/
```

Назначьте владельца на созданный каталог командой:

```
chown -R $USER. /var/www/redsite11.ru/html/
```

Далее следует убедиться, что на каталог **/var/www/** установлены стандартные права. Для этого выполните команду:

```
chmod -R 755 /var/www/
```

Создайте файл сайта **index.html** в каталоге **/var/www/redsite11.ru/html/**:

```
nano /var/www/redsite11.ru/html/index.html
```

В файл добавьте следующее содержимое, которое задаст первоначальный вид страницы:

```
<html>
  <head>
    <title>Welcome to redsite11.ru!</title>
  </head>
  <body>
    <h1>Success! The redsite11.ru virtual host is working!</h1>
  </body>
</html>
```

Далее создайте два каталога **/sites-available** и **/sites-enabled** в **/etc/httpd**, где будут храниться файлы настроек для каждого отдельно взятого домена. Файлы настроек транслируют домены веб-серверу **Apache**, чтобы веб-сервер понимал, как обрабатывать запросы. Для создания каталогов выполните команду:

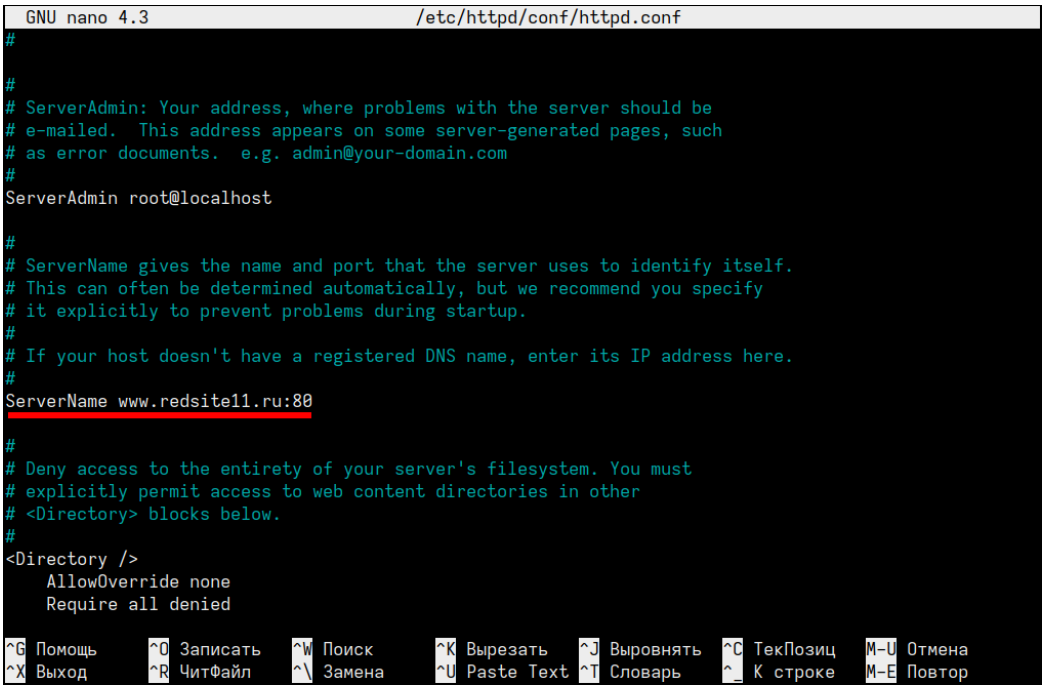
```
mkdir /etc/httpd/sites-available /etc/httpd/sites-enabled
```

Укажите веб-серверу на виртуальный хост в каталоге **/sites-enabled**. Для этого отредактируйте файл **/httpd.conf**:

```
nano /etc/httpd/conf/httpd.conf
```

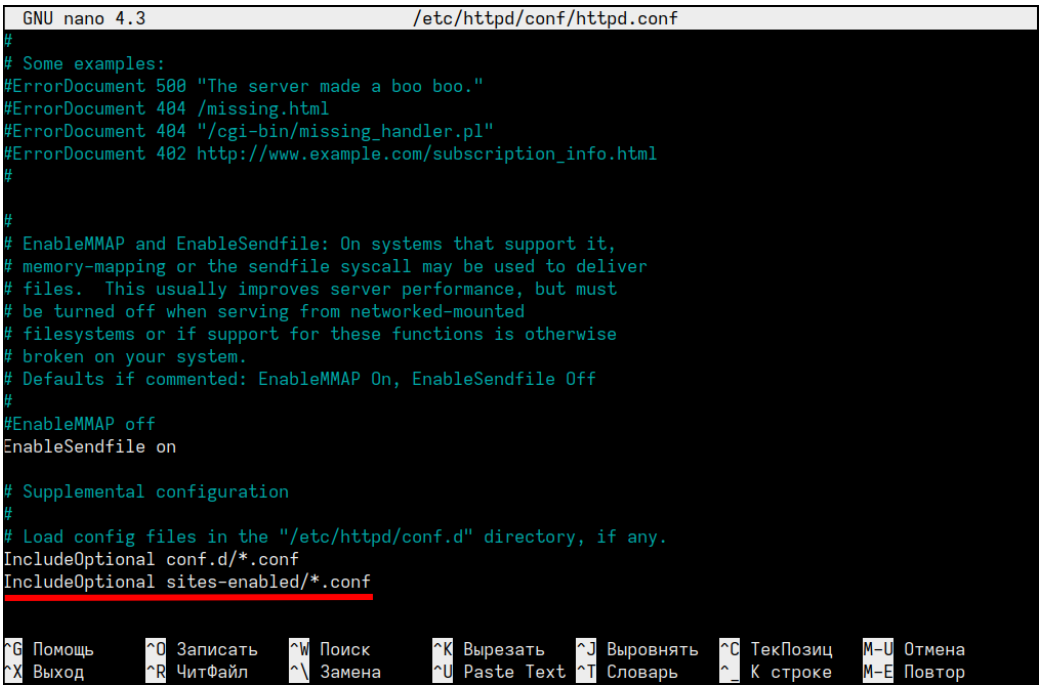
Раскомментируйте строку ServerName и укажите название **своего** сайта:

```
ServerName www.redsite11.ru:80
```



В конец файла добавьте строку:

```
IncludeOptional sites-enabled/*.conf
```



Проверьте настройки **httpd**, выполнив команду:

```
apachectl configtest
```

Если настройки указаны верно, вывод команды должен иметь следующий вид:

```
Syntax OK
```

Далее создайте файл виртуального хоста командой:

```
nano /etc/httpd/sites-available/redsite11.ru.conf
```

Поместите в него содержимое:

```
<VirtualHost *:80>
  ServerName www.redsite11.ru
  ServerAlias redsite11.ru
  DocumentRoot /var/www/redsite11.ru/html
  ErrorLog /var/www/redsite11.ru/log/error.log
  CustomLog /var/www/redsite11.ru/log/requests.log combined
 </VirtualHost>
```

Создайте отдельную папку, где будут храниться файлы журнала:

```
mkdir -p /var/www/redsite11.ru/log
```

Теперь нужно создать символическую ссылку для домена в директории /sites-enabled, чтобы активировать виртуальный хост:

```
ln -s /etc/httpd/sites-available/redsite11.ru.conf /etc/httpd/sites-enabled/redsite11.ru.conf
```

Настройка разрешений в SELinux

Чтобы при старте веб-сервера не получить ошибку запуска, примените универсальную настройку. Для этого выполните команду:

```
setsebool -P httpd_unified 1
```

Для проверки работы перейдите в браузер и в адресной строке введите адрес своего веб-сервера (в примере `http://redsite11.ru`).



Управление службой httpd веб-сервера Apache

Запуск веб-сервера осуществляется командой:

```
systemctl start httpd
```

Остановка веб-сервера осуществляется командой:

```
systemctl stop httpd
```

Перезапуск сервера осуществляется командой:

```
systemctl restart httpd
```

По умолчанию **Apache** запускается автоматически вместе с сервером. Для удаления службы из автозагрузки используется команда:

```
systemctl disable httpd
```

Для добавления **Apache** в автозагрузку, чтобы он стартовал вместе с системой, используется команда:

```
systemctl enable httpd
```

Для перезагрузки веб-сервера **Apache** во время настройки без сброса соединений:

```
systemctl reload httpd
```

Проверка статуса службы **httpd** осуществляется командой:

```
systemctl status httpd
```

Проверка информации об установленной версии **Apache** на сервере осуществляется командой:

```
httpd -v
```

WordPress - инструмент управления сайтами

Настройка Selinux
Установка и настройка веб-сервера Apache
Установка и настройка СУБД MariaDB
Установка и настройка PHP
Установка и настройка WordPress

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: httpd-2.4.62-2, mariadb-10.11.6-2, php-8.1.29-1, wordpress-6.6.2

WordPress – это свободный открытый инструмент для управления сайтами и блогами, основанный на PHP и MySQL.

Для корректной работы **WordPress** необходимо установить компилятор **php**, базу данных **MySQL** и веб-сервер **Apache**.

Примечание.

Все команды, используемые в данном разделе, выполняются с правами пользователя **root**, если не указано иное.

Настройка Selinux

Для настройки SELinux выполните:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_graceful_shutdown 1
```

Установка и настройка веб-сервера Apache

Установите веб-сервер **Apache**:

```
dnf install httpd
```

Запустите службу **apache** и добавьте ее в автозагрузку:

```
systemctl enable httpd --now
```

Для проверки запуска перейдите в браузере по ссылке **http://<IP_сервера>**.



Установка и настройка СУБД MariaDB

Установите СУБД **MariaDB**:

```
dnf install mariadb-server mariadb
```

Запустите службу **mariadb** и добавьте ее в автозагрузку:

```
systemctl enable mariadb --now
```

Создайте пользователя и базу данных с поддержкой русского языка:

```
mysql -u root -p
MariaDB[(none)] > CREATE DATABASE wordpress DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
MariaDB[(none)] > CREATE USER user_wp@localhost IDENTIFIED BY 'password';
```

Определите права для пользователя, который будет использовать базу данных **WordPress**:

```
MariaDB[(none)] > GRANT ALL ON wordpress.* TO 'user_wp'@'localhost';
```

Теперь оповестите **MySQL** о текущих изменениях:

```
MariaDB[(none)] > flush privileges;
```

Выход:

```
quit;
```

Установка и настройка PHP

Установите **php** и дополнительные расширения:

```
dnf install php php-mysqlnd php-pdo php-gd php-mbstring
```

Перезапустите **apache**-сервер:

```
systemctl restart httpd
```

Установка и настройка WordPress

Скачайте установочный архив **WordPress** по ссылке.

Перейдите в каталог, куда была выполнена загрузка, и выполните распаковку архива:

```
cd /home/user/Загрузки/
tar -xvf ./wordpress-6.3.tar.gz
```

Далее распакованные файлы необходимо скопировать в директорию **/var/www/html/**:

```
rsync -av wordpress/* /var/www/html
```

Добавьте отдельную папку для хранения файлов командой:

```
mkdir /var/www/html/wp-content/uploads
```

Предоставьте права пользователю и группе **apache** на каталог с **WordPress**:

```
chown -R apache:apache /var/www/html/*
```

Перейдите в каталог с **WordPress**:

```
cd /var/www/html
```

Главный конфигурационный файл **WordPress** называется **wp-config.php** и содержит все необходимые параметры.

Замените используемый конфигурационный файл по умолчанию на файл **wp-config.php**:

```
cp wp-config-sample.php wp-config.php
```

Внесите в файл информацию о БД:

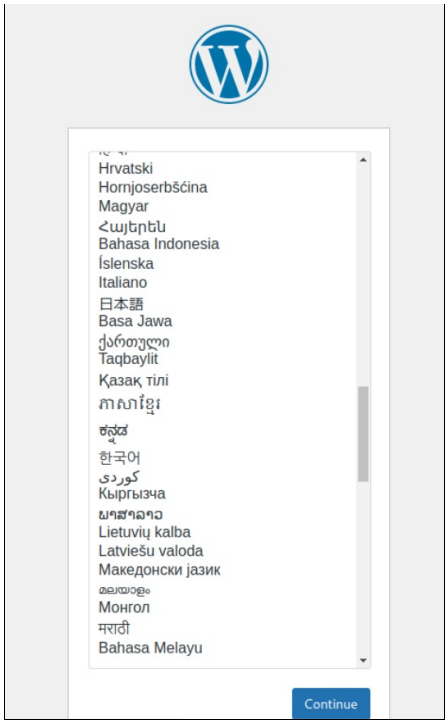
```
nano ./wp-config.php
```

Пример содержимого:

```
// ** Database settings - You can get this info from your web host ** //
 /** The name of the database for WordPress */
 define( 'DB_NAME', 'wordpress' );

 /** Database username */
 define( 'DB_USER', 'user_wp' );

 /** Database password */
 define( 'DB_PASSWORD', 'password' );

 /** Database hostname */
 define( 'DB_HOST', 'localhost' );

 /** Database charset to use in creating database tables. */
 define( 'DB_CHARSET', 'utf8' );

 /** The database collate type. Don't change this if in doubt. */
 define( 'DB_COLLATE', '' );
```

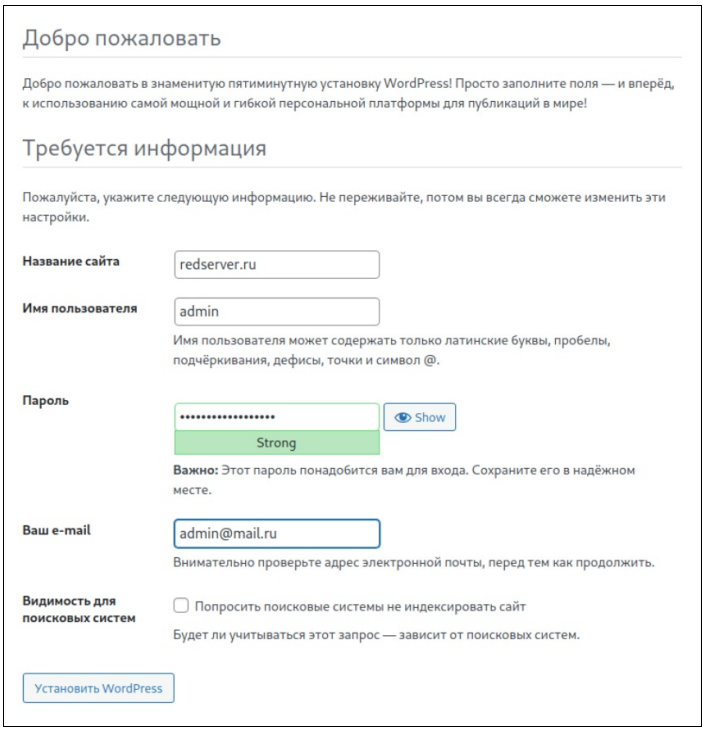
Затем перейдите в браузер по адресу **http://<IP_сервера>** для завершения установки.

WordPress предложит выбрать язык интерфейса, после выбора нажмите **Продолжить**.

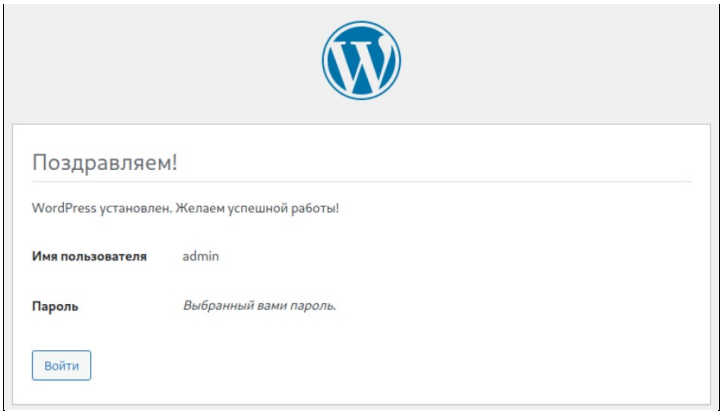


Откроется страница приветствия.

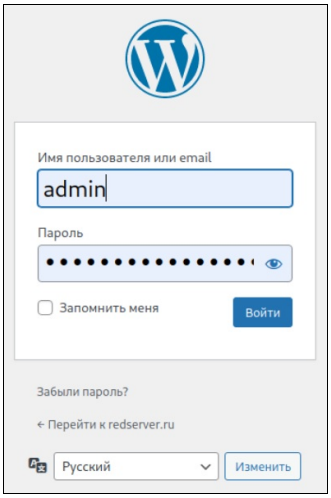
Заполните поля о вашем сайте и администраторе сайта. Например:



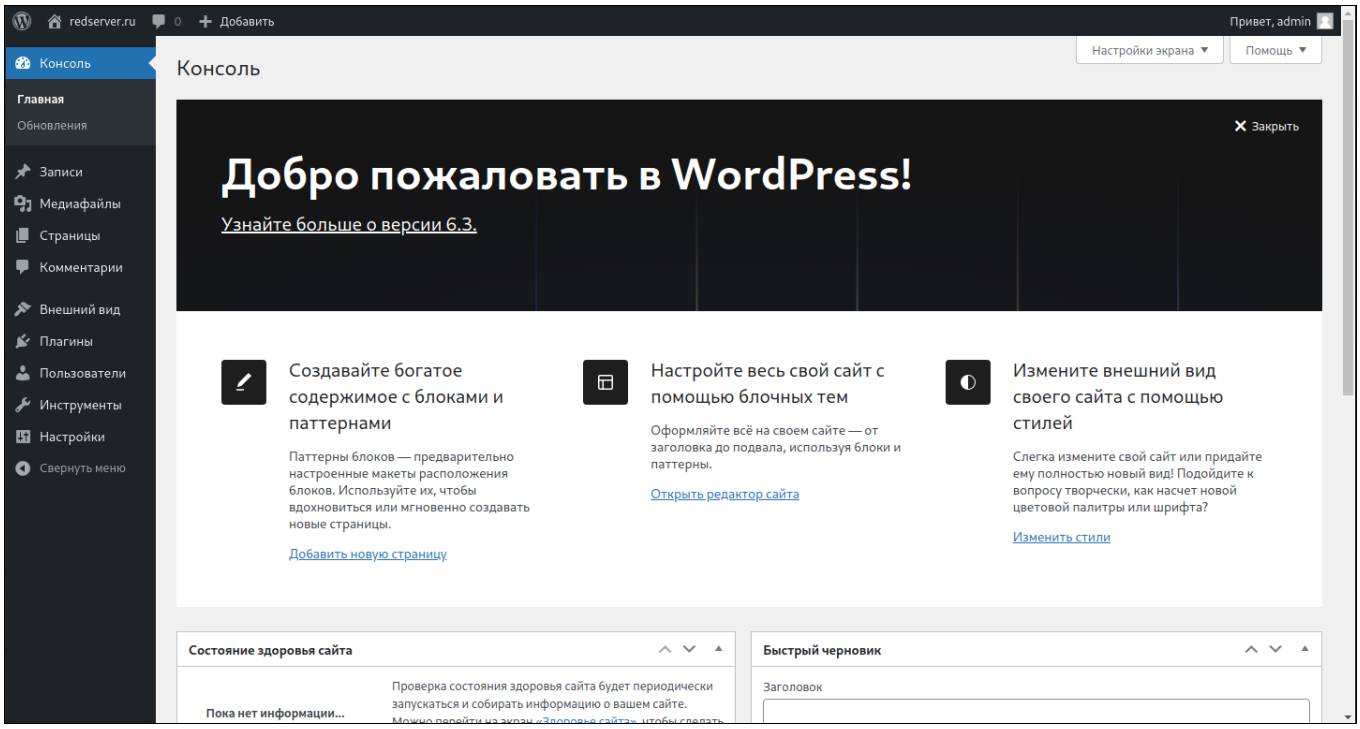
Затем появится окно с уведомлением успешной настройки.



Чтобы продолжить работу с **WordPress** введите *имя пользователя* или *email* и *пароль*.



Система управления контентом **WordPress** готова к использованию.


redserver.ru
0
Добавить
Привет, admin
Консоль
Главная
Обновления
Записи
Медиафайлы
Страницы
Комментарии
Внешний вид
Плагины
Пользователи
Инструменты
Настройки
Свернуть меню
Консоль
Настройки экрана
Помощь
Закрыть
Добро пожаловать в WordPress!
Узнайте больше о версии 6.3.
Создавайте богатое содержимое с блоками и паттернами
Паттерны блоков — предварительно настроенные макеты расположения блоков. Используйте их, чтобы вдохновиться или мгновенно создавать новые страницы.
Добавить новую страницу
Настройте весь свой сайт с помощью блочных тем
Оформляйте всё на своем сайте — от заголовка до подвала, используя блоки и паттерны.
Открыть редактор сайта
Измените внешний вид своего сайта с помощью стилей
Слегка измените свой сайт или придайте ему полностью новый вид! Подойдите к вопросу творчески, как насчет новой цветовой палитры или шрифта?
Изменить стили
Состояние здоровья сайта
Пока нет информации...
Проверка состояния здоровья сайта будет периодически запускаться и собирать информацию о вашем сайте.
Быстрый черновик
Заголовок

Общие сведения о протоколе SSH

Одна из самых распространенных задач, возникающих при работе в сети — удаленный доступ к другим компьютерам и предоставление такого доступа.

Для решения этой задачи используется ставший уже традиционным протокол ***SSH*** (Secure Shell). В отличие от устаревших протоколов, таких как **telnet** и **rsh/rlogin/rcp**, которые передают данные прямым текстом и подвержены обыкновенному прослушиванию и различным атакам, **SSH** реализует соединение с удаленным компьютером, защищающее от:

- прослушивания данных, передаваемых по этому соединению;
- манипулирования данными на пути от клиента к серверу;
- подмены клиента либо сервера путем манипулирования IP-адресами, DNS либо маршрутизацией.

В дополнение к отличным характеристикам в области обеспечения безопасного клиент-серверного соединения, **SSH** обладает следующими возможностями:

- сжатие передаваемых данных;
- туннелирование каналов внутри установленного соединения, в т.ч. соединений с X-сервером;
- широкая распространенность: существуют реализации **SSH** для самых различных аппаратных платформ и операционных систем.

OpenSSH — это входящая в дистрибутив реализация **SSH**, которая включает в себя:

- клиентские программы **ssh, scp** и **sftp** (используются для запуска программ на удаленных серверах и копирования файлов по сети);
- серверные программы **sshd, sftp-server** (используются для предоставления доступа по протоколу SSH);
- вспомогательные программы **make-ssh-known-hosts, rescp, ssh-keygen, ssh-add, ssh-agent, ssh-copy-id, ssh-keyscan**. Одна из самых распространенных задач, возникающих при работе в сети — удаленный доступ к другим компьютерам и предоставление такого доступа.

Служба SSHD

Аутентификация
Вход в систему
SSH-доступ для root
SSHRC
Формат файла authorized keys
Формат файла ssh_known_hosts
Файлы
Предостережения

OpenSSH Daemon - это программа-сервер, обслуживающая запросы программы-клиента **ssh**. Вместе эти программы заменяют **rlogin** и **rsh** и обеспечивают защищённую и зашифрованную связь между двумя непроверенными компьютерами через незащищённую сеть.

sshd - это служба, принимающая запросы на соединения от клиентов. Обычно она запускается при загрузке системы из **/etc/rc**. Для каждого нового соединения создаётся (с помощью вызова *fork*) новый экземпляр службы. Ответвлённый экземпляр обрабатывает обмен ключами, шифрование, аутентификацию, выполнение команд и обмен данными.

Параметры определяются при помощи ключей командной строки или файла конфигурации (по умолчанию - **sshd_config**). Ключи командной строки имеют больший приоритет, чем значения, указанные в файле конфигурации. При получении сигнала отбоя *SIGHUP* перечитывает свой файл конфигурации путём запуска собственной копии с тем же самым именем, с которым был запущен, например, **/usr/sbin/sshd**.

Доступны следующие ключи:

Ключ	Описание ключа
-4	Использовать только адреса IPv4.
-6	Использовать только адреса IPv6.
-b	Определяет число битов в ключе сервера протокола версии 1 (по умолчанию 768).
-D	Не переходить в фоновый режим и не становиться службой. Это упрощает слежение за экземпляром sshd.
-d	Режим отладки. Сервер посылает расширенную отладочную информацию в файл журнала событий системы и не переходит в фоновый режим работы. Также сервер не создаёт дочерних процессов и обрабатывает только одно соединение. Этот параметр предназначен только для отладки работы сервера. Несколько параметров -d, указанных один за другим, повышают уровень отладки. Максимум - это 3.
-e	Направлять вывод в консоль (stderr) вместо механизма журналирования событий системы.
-f	Определяет имя файла конфигурации. По умолчанию - это /etc/ssh/sshd_config; отказывается работать, не имея файла конфигурации.
-g	Определяет период, в течение которого клиент должен себя идентифицировать (по умолчанию - 120 секунд). Если клиент не смог идентифицировать себя в течение этого времени, экземпляр сервера прекращает свою работу. Значение, равное нулю, отменяет ограничение на время ожидания.
-h	Определяет файл, из которого будет считан ключ хоста. Этот параметр должен быть указан, если запущен не от имени суперпользователя (так как обычно стандартные файлы хоста доступны для чтения только суперпользователю). Стандартное расположение файла - /etc/ssh/ssh_host_key для протокола версии 1, и /etc/ssh/ssh_host_rsa_key и /etc/ssh/ssh_host_dsa_key для протокола версии 2. Можно иметь несколько ключей хоста для разных версий протокола и алгоритмов генерации ключей.
-i	Этот ключ позволяет уведомить программу о том, что она запускается службой inetd(8). Обычно не запускается из inetd, так как требуется генерировать ключ сервера до ответа клиенту, а это может отнять десятки секунд. Клиент будет вынужден ожидать слишком долго, если ключ будет повторно генерироваться каждый раз. Однако, при малых размерах ключа (например, 512), использование из inetd может быть оправдано.
-k	Определяет, как часто будет регенерироваться ключ сервера протокола версии 1 (по умолчанию 3600 секунд - один раз в час). Мотивацией для регенерации ключа так часто служит то, что ключ нигде не сохраняется и, по истечении примерно часа, восстановить ключ для прерванных соединений становится невозможно, даже если машина была взломана или захвачена физически. Значение «ноль» означает, что ключ никогда не будет регенерирован.
-o	Позволяет указывать директивы в формате файла конфигурации, например такие, для которых нет соответствующего ключа командной строки. Директивы файла конфигурации описаны в sshd_config(5).
-p	Порт, на котором сервер будет ожидать соединения (по умолчанию - 22). Возможно указание нескольких ключей с разными портами. Если данный ключ указан, параметр Port файла конфигурации игнорируется, однако порты, указанные в ListenAddress имеют больший приоритет, чем указанные в командной строке.
-q	Не заносить в системный журнал регистрации событий никакой информации. В обычном режиме в нём фиксируется подключение, аутентификация и разрыв каждого соединения.
-t	Режим тестирования. Выполняется только проверка соответствия файла конфигурации и готовность ключей. Полезно для проверки состояния службы после обновления, при котором были изменены файлы конфигурации.
-u	Размер поля в структуре utmp, хранящей имя удалённого хоста. Если разрешённое имя хоста превышает указанное значение, то взамен будет использовано десятичное представление IP-адреса через точку. Это позволяет уникально идентифицировать машины со слишком длинными именами. Указание -u0 включает использование в файле utmp IP-адресов во всех случаях. При этом, будет производить DNS-запросы только, если это явно требуется конфигурацией (from=pattern-list) или механизмом аутентификации (либо RhostsRSAAuthentication либо HostbasedAuthentication). Использование DNS также обязательно в случае задания параметрам AllowUsers и DenyUsers значения в формате USER@HOST.

Аутентификация

Служба **OpenSSH** SSH поддерживает версии протокола SSH 1 и 2. Запретить использование одного из протоколов можно, указав в параметре *Protocol* файла **sshd_config**. Протокол 2 поддерживает ключи *RSA и DSA*; протокол 1 поддерживает только ключи *RSA*. Независимо от протокола, каждый подключающийся хост имеет собственный (обычно 2048-битный) идентифицирующий его ключ.

Для протокола версии 1 подтверждение субъекта сервера обеспечивается 768-битным ключом, который генерируется при запуске сервера. Ключ генерируется заново каждый час, при условии его использования, и не хранится на диске. При получении запроса на подключение со стороны клиента служба посылает в ответ свой открытый ключ и свои ключи. Клиент сравнивает ключ хоста *RSA* со своими данными, чтобы убедиться в том, что это тот же сервер. Затем клиент генерирует 256-битное произвольное число, шифрует его при помощи обоих ключей (своего и сервера) и отправляет результат серверу. Это число становится ключом сеанса, и с его помощью выполняется кодирование всей последующих данных, по согласованному методу - *Blowfish* или *3DES* (клиент выбирает метод из предложенных сервером). В настоящее время по умолчанию используется **3DES**.

Для протокола версии 2 подтверждение субъекта сервера обеспечивается по схеме Диффи—Хеллмана, в результате которой также получается общий ключ сеанса. Дальнейший обмен данными шифруется *симметричным кодом, 128-битным AES, Blowfish, 3DES, CAST128, Arcfour, 192-битным AES или 256-битным AES*, который выбирает клиент из предложенных сервером. Кроме того, целостность передаваемых данных обеспечивается кодом подтверждения подлинности сообщения (hmac-sha1 или hmac-md5).

Далее сервер и клиент переходят в режим аутентификации. Клиент пытается аутентифицировать себя по своему хосту, открытому ключу, паролю или с помощью беспарольного механизма («вызов-ответ»).

Независимо от типа аутентификации, служба проверяет доступность соответствующей учётной записи в системе. Так, она может быть заблокирована посредством добавления её в параметр *DenyUsers* или её группы в *DenyGroups*. Механизм общесистемной блокировки учётной записи выполняется разными системами по-разному. Одни системы ведут собственную базу данных учётных записей (AIX), другие вносят соответствующие изменения в поля файла **passwd** («*LK*» - Solaris и UnixWare, «*» - на HP-UX, «Nologin» - Tru64, «*LOCKED*» во FreeBSD и «!!» в GNU/Linux). Для запрета только аутентификации по паролю укажите в файле *passwd* «**NP**» или «***NP***».

После успешной аутентификации себя клиентом связь переходит в режим подготовки сеанса. В этот момент клиент может запросить такие вещи, как выделение псевдо-терминала, перенаправление соединения X11, перенаправление соединения TCP/IP или перенаправление соединения агента аутентификации через защищённый канал.

Наконец, клиент запрашивает оболочку или выполнение команды, после чего стороны входят в режим сеанса. В этом режиме каждая из сторон в любой момент может пересылать данные и эти данные будут переданы оболочке или команде на стороне сервера и на пользовательский терминал соответственно.

По завершении работы пользовательской программы и закрытии всех перенаправленных X11 и других соединений сервер посылает клиенту команду со статусом выхода и сеанс завершается.

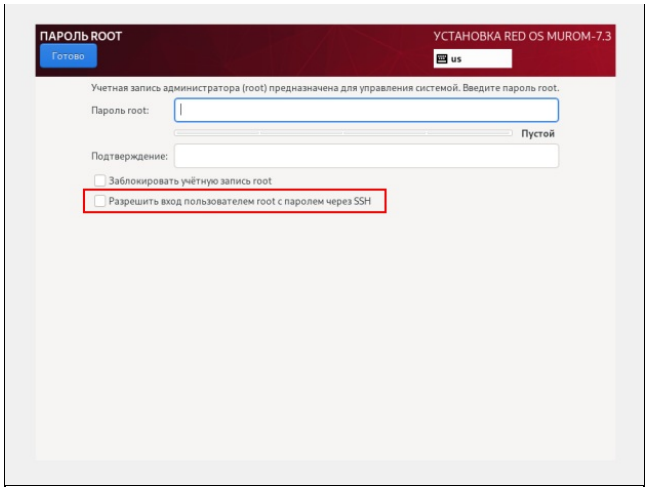
Вход в систему

После успешной аутентификации пользователя выполняются следующие действия:

- Если регистрация в системе произведена на терминале (tty) и не указана никакая команда, то отображается время последнего входа в систему и содержимое файла **/etc/motd** (если только это не отключено в файле конфигурации или **~/.hushlogin**).
- Если регистрация в системе произведена на терминале, записывается время регистрации.
- Проверяется **/etc/nologin**, если он присутствует, выводится его содержимое и завершается работа (исключение - root).
- Осуществляется переход к выполнению с правами обычного пользователя.
- Устанавливаются значения основных переменных среды.
- Интерпретируется файл **~/.ssh/environment**, если таковой имеется, и пользователям разрешено изменять среду.
- Переходит в домашний каталог пользователя.
- Если имеется файл **~/.ssh/rc**, то производится его выполнение, а если нет, но имеется **/etc/ssh/sshrc**, то выполняется он, в противном случае не выполняется ничего. Файлам «rc» на стандартный ввод передаётся протокол аутентификации **X11** и **cookie**.
- Запускается оболочка пользователя или выполняется указанная команда.

SSH-доступ для root

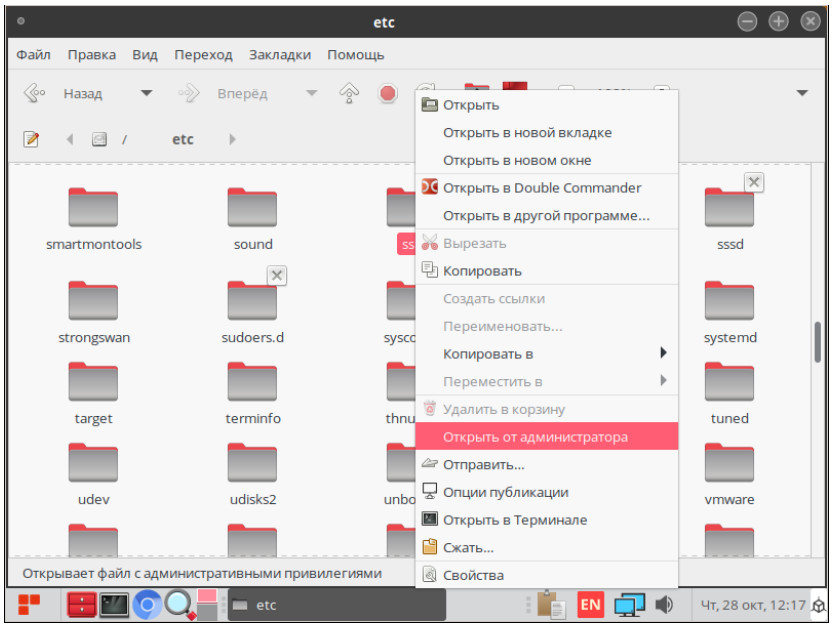
В начале установки операционной системы РЕД ОС предоставляется возможность разрешить вход пользователем root с паролем через ssh.



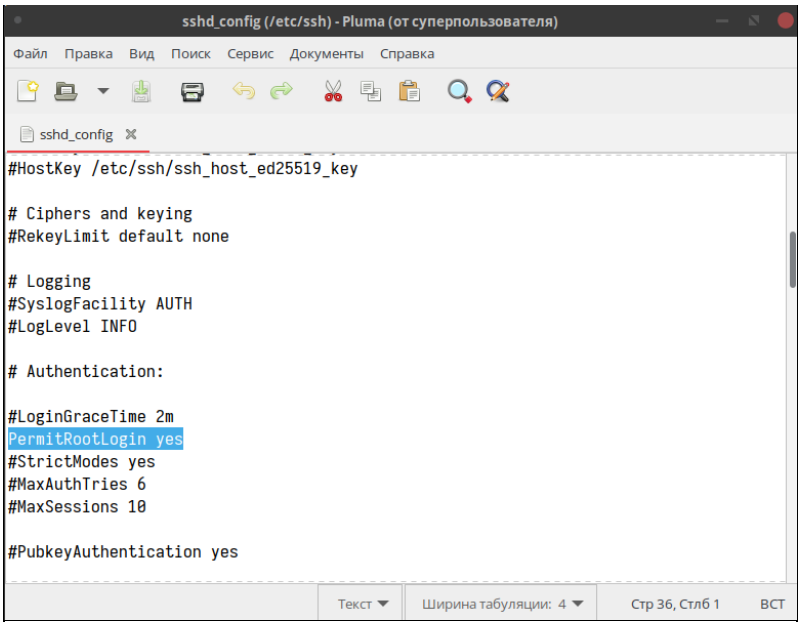
Но даже если не указывать данное разрешение при установке, его можно настроить после завершения установки системы.

Для этого на рабочем столе необходимо открыть меню и перейти в файловую систему (**/**). Затем требуется найти папку **/etc** и перейти в неё.

В папке **/etc** необходимо открыть папку **/ssh** от имени администратора.



Затем нужно найти файл **sshd_config** и отредактировать в нем строку **PermitRootLogin prohibit-password** на **PermitRootLogin yes**.



После редактирования необходимо сохранить внесенные изменения.

Далее следует открыть терминал и перезапустить ssh-сервер (перезапуск сервера необходимо делать после каждого изменения файла конфигурации для последующего применения) командой:

```
systemctl restart sshd
```

Теперь можно подключаться по **SSH** от имени суперпользователя **root**.

SSHRC

Если файл **~/.ssh/rc** существует, он будет выполняться после файлов определения переменных среды, но перед запуском оболочки пользователя или команды. Если используется подмена **X11**, то на его стандартный ввод будет передана пара «**proto cookie**», также ему будет доступна переменная среды **DISPLAY**. Сценарий должен вызывать **xauth(1)** самостоятельно для добавления **cookie X11**.

Основная цель этого файла состоит в выполнении процедур инициализации, необходимые прежде, чем станет доступным основной каталог пользователя. **AFS** - пример такой среды.

Этот файл будет, вероятно, содержать блок аналогичный следующему:

```
if read proto cookie && [ -n "$DISPLAY" ]; then
if [ 'echo $DISPLAY | cut -c1-10' = 'localhost:' ]; then
 X11UseLocalhost=yes
echo add unix:'echo $DISPLAY
| cut -c11-' $proto $cookie
else
 X11UseLocalhost=no
echo add $DISPLAY $proto $cookie
fi | xauth -q -
fi
```

Если этот файл отсутствует, то выполняется **/etc/ssh/sshrc**, а если отсутствует и он, то для добавления **cookie** используется **xauth**.

Формат файла authorized keys

Параметр файла конфигурации **AuthorizedKeysFile** определяет путь к файлу с открытыми ключами. Значение по умолчанию **—/.ssh/authorized_keys**. Каждая строка файла содержит один ключ (пустые строки или строки, начинающиеся с символа «#», считаются комментариями и игнорируются). Открытые ключи протокола 1 (RSA) состоят из следующих полей, разделённых пробелами: параметры, битность, порядок, модуль, комментарий. Открытые ключи протокола версии 2 состоят из: параметра, типа ключа, ключа в виде base64, комментария. Поля параметров необязательны; их отсутствие определяется наличием в начале строки цифры (поле параметра никогда не начинается с цифры). Поля битности, порядка, модуля и комментарии определяют ключ RSA; поле комментария не используется (но может быть удобно пользователю для отметки ключа). Для протокола версии 2 типом ключа является **ssh-dss** или **ssh-rsa**.

Примечание! Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен байт (из-за размера открытого ключа RSA) и могут достигать длины в 8 килобайт (таким образом, максимальный размер ключа DSA - 8 килобит, а RSA - 16 килобит). Очевидно, не стоит вводить их вручную. Вместо этого скопируйте файл **identity.pub, id_dsa.pub** или **id_rsa.pub** и отредактируйте их.

Минимальная длина модуля RSA независимо от протокола составляет 768 бит.

Параметры (если таковые имеются) состоят из разделённых запятой определений. Для указания пробелов следует воспользоваться двойными кавычками. Поддерживаются следующие определения параметров (регистра названий параметров не учитывается):

Параметр	Значение
command=команда	Выполнять команду при каждом использовании данного ключа для аутентификации. Команда, передаваемая пользователем, будет игнорироваться. Команда выполняется на псевдо-терминале, если последний запрашивается клиентом; в противном случае она выполняется без терминала. Если требуется «чистый» 8-битный канал, запрашивать псевдо-терминал или указывать no-pty нельзя. В команду может быть включена кавычка, предварённая обратной косой чертой. Данный параметр полезен для ограничения использования определённых RSA-ключей. Примером может служить ключ, по которому можно выполнять удалённые операции резервного копирования и ничего более. Учтите, что клиент по-прежнему может запросить перенаправление TCP и/или X11, если только это не запрещено явно. Команда, запрашиваемая клиентом, заносится в переменную SSH_ORIGINAL_COMMAND. Заметьте, что данный параметр относится к выполнению оболочки, команды или подсистемы.
environment=ПЕРЕМЕННАЯ=значение	Добавить переменную в среду (или переопределить её значение) при регистрации в системе с использованием данного ключа. Допускается указание нескольких таких директив. По умолчанию изменение переменных среды таким образом отключено. За его включение отвечает параметр PermitUserEnvironment. Этот параметр отключается автоматически при включении UseLogin.
from=список-шаблонов	Если параметр определён, то в дополнение к прохождению аутентификации по открытому ключу каноническое имя удалённого хоста должно соответствовать одному из шаблонов в списке (шаблоны указываются через запятую). Цель этого параметра - увеличение степени защиты: если частный ключ хоста каким-либо образом удастся похитить, то он позволит злоумышленнику войти в систему из любой точки мира. Этот дополнительный параметр делает использование ворованных ключей более затруднительным (кроме перехвата ключа, требуется взлом серверов имён и/или маршрутизаторов). См. секцию ШАБЛОНЫ в ssh_config(5).
no-agent-forwarding	Запретить перенаправление агента аутентификации при аутентификации данным ключом.
no-port-forwarding	Запретить перенаправление TCP/IP при аутентификации данным ключом. Любой запрос на перенаправление порта приведёт к получению клиентом сообщения об ошибке. Это может быть использовано, например, вместе с параметром command.
no-pty	Запретить назначение терминала (запросы на назначение псевдо-терминала не будут удовлетворены).
no-X11-forwarding	Запретить перенаправление X11 при аутентификации данным ключом. Любой запрос на перенаправление порта возвратит клиенту сообщение об ошибке.
permitopen=хост:порт	Для функции перенаправления данных с локального клиентского порта на порт удалённой системы (выполняемого при указании ssh -L). Ограничит набор возможных целей для перенаправления указанной машиной и портом. Для указания адресов IPv6 можно использовать альтернативный синтаксис: хост / порт. Допускается указание нескольких целей через запятую. Значение параметра не интерпретируется как шаблон (т.е. является литеральным).
tunnel=n	Принудительно использовать устройство tun(4) на сервере. Без этого параметра при запросе клиентом туннеля используется ближайшее доступное для этого устройство.

Пример файла **authorized_keys**:

```
# допустимы комментарии только на всю строку
ssh-rsa AAAAB3Nza...LiPk== user@example.net
from="*.sales.example.net,!pc.sales.example.net" ssh-rsa
AAAAB2...19Q== john@example.net
command="dump /home",no-pty,no-port-forwarding ssh-dss
AAAAC3...51R== example.net
permitopen="192.0.2.1:80",permitopen="192.0.2.2:25" ssh-dss
AAAAB5...21S==
tunnel="0",command="sh /etc/netstart tun0" ssh-rsa AAAA...==
jane@example.net
```

Формат файла ssh_known_hosts

В файлах **/etc/ssh/ssh_known_hosts** и **~/.ssh/known_hosts** хранятся открытые ключи всех машин, с которыми когда-либо устанавливалась связь.

Глобальный файл должен быть подготовлен администратором (это необязательно), пользовательский файл поддерживается автоматически: каждый раз, когда поступает запрос на соединение от неизвестной машины, её ключ автоматически заносится в пользовательский файл.

Каждая строка в этом файле содержит следующие поля: имена хостов, битность, порядок, модуль, комментарий. Поля разделены пробелами.

Имена хостов - это разделённый запятыми список шаблонов (символы подстановки - «*****» и «**?**»); каждый шаблон сопоставляется с каноническим именем машины (при аутентификации клиента) или с именем, которое указано пользователем (при аутентификации сервера). Этот шаблон может также быть предварён знаком «**!**» для обозначения отрицания: если имя машины соответствует отрицаемому шаблону, оно будет отвергнуто (этой строкой) даже если оно соответствует другому шаблону в этой же строке. Также можно, заключив имя хоста или IP-адрес в квадратные скобки «**[**» и «**]**», через «**:**» указать нестандартный порт.

Вместо имён хостов можно записывать их хэши. Это позволит скрыть их от злоумышленника в случае попадания файла в его руки. Для различия хэшей от имён хостов первые предваряются символом «|». На одной строке может быть не больше одного хэша, операция отрицания в этом случае не доступна.

Разрядность, порядок и модуль копируются из ключа хоста RSA, например, **/etc/ssh/ssh_host_key.pub**. Необязательное поле комментария занимает всю оставшуюся часть строки и игнорируется.

Комментариями также считаются пустые и строки начинающиеся с «**#**».

Идентификация машины принимается, если любая совпавшая строка содержит правильный ключ. Таким образом, можно (хотя это не рекомендуется) иметь несколько строк или различных ключей для одного и того же хоста. Это неизбежно случается при помещении в файл кратких форм имён хостов из различных доменов. В файлах может содержаться противоречивая информация. Идентификация принимается, если адекватная информация имеется в любом из них.

> **Примечание!** Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен символов и, очевидно, не стоит вводить имена хостов вручную. Вместо этого их можно сгенерировать при помощи сценария оболочки или взять из файла **/etc/ssh/ssh_host_key.pub**, добавив в начале имя хоста.

Пример файла **ssh_known_hosts**:

```
# допустимы явные комментарии только на всю строку
closenet      192.0.2.53 1024 37 159...93 closenet.example.net
cvs.example.net,192.0.2.10 ssh-rsa AAAA1234 =
# хэш имени хоста
|1|JfKTdBh7rNbXkVAQCRp4OQoPfmI=|USECr3SWf1JUPsms5AqfD5QfxkM= ssh-rsa
AAAA1234 =
```

Файлы

Файл	Назначение
-/.hushlogin	Позволяет отключить вывод времени последнего входа в систему и содержимого файла /etc/motd, если в файле конфигурации включены соответственно PrintLastLog и PrintMotd. Файл не влияет на вывод содержимого Banner.
-/.rhosts	Этот файл используется для аутентификации по хосту (см. ssh(1)). На некоторых машинах, если каталог пользователя находится на разделе NFS, для того чтобы он был доступен пользователю root, он должен быть доступен для чтения всем. Файл должен принадлежать пользователю и не должен быть доступен для записи другим. Рекомендуемый набор прав доступа в общем случае - чтение/запись для пользователя и недоступность для других.
-/.shosts	Аналогичен файлу .rhosts, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью rlogin/rsh.

Файл	Назначение
~/.ssh/authorized_keys	Содержит список открытых ключей (RSA/DSA), которые могут быть использованы для регистрации данного пользователя. Формат файла описан выше. Этот файл не очень важен для злоумышленника, но мы рекомендуем сделать его доступным только пользователю (чтение/запись). Если этот файл, каталог ~/.ssh или домашний каталог пользователя доступны для записи другим пользователям, этот файл может быть изменён или заменён любым пользователем системы, имеющим сколько угодно мало прав. В этом случае sshd не будет использовать этот файл, если только параметр StrictModes не имеет значение «no». Установить рекомендуемый набор прав доступа можно командой chmod go-w ~/ ~/.ssh ~/.ssh/authorized_keys.
~/.ssh/environment	Этот файл (при его наличии) считывается в среду при регистрации в системе. Он может содержать только пустые строки, строки комментария (начинающиеся с «#») и определения значений переменных в виде: переменная=значение. Правом на запись этого файла должен обладать только пользователь; он не должен быть доступен остальным. Задание переменных среды отключено по умолчанию, за что отвечает параметр PermitUserEnvironment.
~/.ssh/known_hosts	Список адресов, к которым когда-либо подключался пользователь и которые отсутствуют в общесистемном файле, и соответствующих им открытых ключей. Формат файла описан выше. Файл должен быть доступен для записи только владельцу и администратору. Он может также быть доступен для чтения всем остальным, но это не обязательно.
~/.ssh/rc	Сценарий инициализации, запускаемый перед запуском оболочки пользователя или команды. Этот файл должен быть доступен для записи только пользователю и не должен быть вообще доступен другим.
/etc/hosts.allow **/etc/hosts.deny**	Данные о разрешении и запрете соединений с хостами для надстроек TCP. См. hosts_access(5).
/etc/hosts.equiv	Используется для аутентификации на основе хоста (см. ssh(1)). Должен быть доступен для записи только root.
/etc/moduli	Группы для схемы Диффи—Хеллмана. Формат файла описан в moduli(5).
/etc/motd	См. motd(5).
/etc/nologin	Если существует, подключение будет разрешено только суперпользователю. Любому, кто пытается войти в систему, будет показано содержимое этого файла и запросы на регистрацию в качестве не суперпользователя будут отвергнуты. Этот файл должен быть доступен для чтения всем.
/etc/shosts.equiv	Аналогичен hosts.equiv, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью rlogin/rsh.
/etc/ssh/ssh_known_hosts	Общесистемный список известных хостов и их ключей. Этот файл должен составляться администратором. В него следует включать открытые ключи всех компьютеров организации. Формат файла описан выше. Файл должен быть доступен всем для чтения и владельцу/администратору для записи.
/etc/ssh/ssh_host_key **/etc/ssh/ssh_host_dsa_key** **/etc/ssh/ssh_host_rsa_key**	Содержат частные ключи хостов. Файлы должны принадлежать root и быть доступными только для него. Не запустится, если эти файлы доступны для чтения кому-либо кроме суперпользователя.
/etc/ssh/ssh_host_key.pub **/etc/ssh/ssh_host_dsa_key.pub** **/etc/ssh/ssh_host_rsa_key.pub**	Содержат открытые ключи хостов. Должны быть доступны всем для чтения и только суперпользователю для записи. Содержимое файлов должно соответствовать содержимому соответствующих файлов с частными ключами. Эти файлы не используются программой и предназначены для копирования пользователем в файлы known_hosts. Эти файлы создаются командой ssh-keygen(1).
/etc/ssh/sshd_config	Конфигурация службы sshd. Формат файла и параметры конфигурации описаны в sshd_config(5).
/etc/ssh/sshrc	Аналогичен ~/.ssh/rc, позволяет задавать инициализационный сценарий глобально для всех пользователей. Должен быть доступен всем для чтения и только root для записи.
/var/empty	Каталог chroot(2), используемый при отделении полномочий на предаутентификационном этапе. В папке не должно быть никаких файлов, она должна принадлежать только root и не должна быть доступна другим для записи.
/var/run/sshd.pid	Идентификатор процесса, ожидающего запросов на подключение (если одновременно работает несколько экземпляров служб для нескольких портов, в него записывается идентификатор экземпляра запущенного последним). Содержимое этого файла может не быть защищено и может быть доступно всем.

Предостережения

Использование этой службы не повысит уровень защиты системы пока **rshd, rlogind** и **rexecd** не будут **полностью отключены** в системе.

Конфигурационный файл SSHD_CONFIG

Описание файла конфигурации

Указание времени

Файлы

Описание файла конфигурации

Служба **sshd** считывает данные о конфигурации из файла **/etc/ssh/sshd_config** (или из файла. указанного в командной строке при помощи параметра **-f**). Файл содержит пары параметр-значение, по одной на строку. Пустые и строки, начинающиеся с «**#**». интерпретируются как комментарии. Если аргументы содержат пробелы, они должны быть заключены в двойные кавычки (' ').

Далее приведены описания возможных параметров (регистр имён аргументов учитывается, регистр имён параметров - нет):

Очищать ли кэш аутентификационных данных клиента при завершении сеанса. Значение по умолчанию - «yes». Данный параметр относится только к протоколу версии 2.

Параметр	Значение
AcceptEnv	Список переменных среды, которые, будучи заданы клиентом, будут копироваться в environ(7) сеанса. Соответствующая настройка на стороне клиента выполняется параметром SendEnv и описана в ssh_config(5). Переменные указываются по имени, допускаются символы подстановки «*» и «?». Несколько переменных среды можно указывать через пробелы или в нескольких параметрах AcceptEnv. Данный параметр введен для предотвращения обхода ограничений среды пользователя посредством изменения значений переменных среды. По умолчанию не принимаются никакие переменные среды.
AddressFamily	Семейство адресов, которое должна использовать служба sshd(8). Допустимые значения: «any», «inet» (только IPv4) и «inet6» (только IPv6). Значение по умолчанию - «any».
AllowGroups	Список шаблонов имён групп через пробел. Если параметр определён, регистрация в системе разрешается только пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп; числовой идентификатор группы не распознаётся. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).
AllowTcpForwarding	Определяет, будет ли разрешено перенаправление TCP. Значение по умолчанию - «yes». Имейте ввиду, что отключение пересылки TCP не увеличит уровень защищённости системы, пока пользователям не запрещён доступ к командной оболочке, так как они всегда могут установить свои собственные перенаправления.
AllowUsers	Список имён пользователей через пробел. Если параметр определён, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов. Допустимы только имена пользователей; числовой идентификатор пользователя не распознаётся. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом разрешая доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).
AuthorizedKeysFile	Файл с открытыми ключами, которые могут быть использованы для аутентификации пользователей. Допустимо указание шаблонов, они преобразуются при настройке соединения: «%%» заменяется на символ «%», «%h» заменяется на домашний каталог идентифицируемого пользователя, «%u» - на имя пользователя. После преобразования AuthorizedKeysFile интерпретируется либо как абсолютный путь, либо как путь относительно домашнего каталога пользователя. Значение по умолчанию - «.ssh/authorized_keys».
Banner	На некоторых территориях для получения защиты со стороны закона может быть необходимо послание предупредительного сообщения перед аутентификацией. Содержимое указанного файла будет отправлено удалённому пользователю прежде, чем будет разрешена аутентификация. Этот параметр доступен только с протоколом версии 2. По умолчанию не выводится никакой информации.
ChallengeResponseAuthentication	Определяет, разрешается ли беспарольная аутентификация «вызов-ответ». Поддерживаются все схемы аутентификации login.conf(5). Значение по умолчанию - «yes».
Ciphers	Допустимые для протокола версии 2 шифры. Несколько шифров указываются через запятую. Поддерживаются следующие шифры: «3des-cbc», «aes128-cbc», «aes192-cbc», «aes256-cbc», «aes128-ctr», «aes192-ctr», «aes256-ctr», «arcfour128», «arcfour256», «arcfour», «blowfish-cbc» и «cast128-cbc». Значение по умолчанию: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128, arcfour256,arcfour,aes192-cbc,aes256-cbc,aes128-ctr, aes192-ctr,aes256-ctr
ClientAliveCountMax	Количество запросов, проверяющих доступность клиента (см. ниже), которые могут оставаться без ответа. Если предел достигнут, sshd(8) отключит клиента и завершит сеанс. Имейте в виду, запросы client alive отличаются от TCPKeepAlive (см. ниже). Данные запросы отправляются через защищённый канал и поэтому не могут быть подменены. Параметр TCPKeepAlive допускает возможность подмены данных. Механизм client alive полезен, если поведение клиента или сервера зависит от активности соединения. Значение по умолчанию - 3. Если ClientAliveInterval (см. ниже) равно 15, а для ClientAliveCountMax оставлено значение по умолчанию, не отвечающие клиенты SSH будут отключаться приблизительно через 45. Данный параметр относится только к протоколу версии 2.
ClientAliveInterval	Время бездействия со стороны клиента в секундах, после которого sshd(8) отправляет через защищённый канал запрос отклика клиенту. Значение по умолчанию - 0, что означает, что клиенту не будут направляться такие запросы. Этот параметр применим только с протоколом версии 2.
Compression	Разрешить сжатие сразу, после аутентификации или вообще запретить его. Допустимые значения - «yes», «delayed» и «no». Значение по умолчанию - «delayed».
DenyGroups	Список шаблонов имён групп через пробел. Если параметр определён, регистрация в системе пользователям, чья главная или вспомогательная группа соответствуют содержащимся в списке шаблонам, не разрешается. Допустимы только имена групп; числовой идентификатор группы не распознаётся. По умолчанию регистрация в системе разрешена для всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).

Параметр	Значение
DenyUsers	Список имён пользователей через пробел. Если параметр определён, регистрация в системе пользователей, чьи имена соответствуют одному из шаблонов, будет запрещена. Допустимы только имена пользователей; числовой идентификатор пользователя не распознаётся. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом запрещается доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. См. секция ШАБЛОНЫ в ssh_config(5).
ForceCommand	Выполнять указанную команду после регистрации пользователя в системе, игнорируя команду, запрашиваемую им. Команда запускается оболочкой пользователя с ключом -c. Это относится к выполнению оболочки, команды или подсистемы. Обычно применяется внутри блока Match. Команда, запрошенная пользователем, помещается в переменную среды SSH_ORIGINAL_COMMAND.
GatewayPorts	Определяет, разрешено ли удалённым машинам подключение к портам, выделенным для туннелирования трафика клиентов. По умолчанию, sshd(8) делает доступными порты, используемые для туннелирования, инициируемого сервером, только для кольцевого (loopback) адреса, т.е. удалённые машины подключаться к перенаправляемым портам не могут. С помощью данного параметра можно исправить такое положение дел. Значение «no» разрешает туннелирование только в рамках данной системы, «yes» разрешает туннелирование для хостов, соответствующих шаблону, а «clientspecified» позволяет клиенту самостоятельно выбирать адрес для туннелирования. Значение по умолчанию - «no».
GSSAPIAuthentication	Допускать аутентификацию по GSSAPI. Значение по умолчанию - «no». Данный параметр относится только к протоколу версии 2.
GSSAPICleanupCredentials	Указывает, следует ли автоматически уничтожать кэш учетных данных пользователя при выходе из системы. Значение по умолчанию - да.
HostbasedAuthentication	Допускать аутентификацию по хостам, т.е. аутентификацию по rhosts или /etc/hosts.equiv в сочетании с открытым ключом клиента. Этот параметр схож с RhostsRSAAuthentication и применим только к протоколу версии 2. Значение по умолчанию - «no».
HostbasedUsesNameFromPacketOnly	Отключить выполнение запросов имени хоста при обработке файлов ~/.shosts, ~/.rhosts и /etc/hosts.equiv в рамках аутентификации по хосту (HostbasedAuthentication). При значении «yes» для сравнения будет использоваться имя, указанное клиентом, а не имя, которое может быть получено стандартными средствами соединения TCP. Значение по умолчанию - «no».
HostKey	Файл с частными ключами хоста. Значение по умолчанию - /etc/ssh/ssh_host_key для протокола 1, и /etc/ssh/ssh_host_rsa_key и /etc/ssh/ssh_host_dsa_key для протокола 2. Имейте в виду, что sshd(8) не будет принимать файлы частных ключей доступные для чтения всей группе или вообще всем пользователям. Можно указывать несколько файлов с ключами хоста. Ключи «rsa1» используются для протокола версии 1, ключи «dsa» и «rsa» - для версии 2 протокола SSH.
IgnoreRhosts	Не учитывать содержимое файлов .rhosts и .shosts при аутентификации RhostsRSAAuthentication и HostbasedAuthentication. При этом будут учитываться только /etc/hosts.equiv и /etc/shosts.equiv. Значение по умолчанию - «yes».
IgnoreUserKnownHosts	Не учитывать содержимое файла ~/.ssh/known_hosts при RhostsRSAAuthentication или HostbasedAuthentication. Значение по умолчанию - «no».
KerberosAuthentication	Определяет, дозволена ли аутентификация Kerberos: Проверять ли пароль, указанный пользователем для аутентификации PasswordAuthentication в Kerberos KDC. Это может быть либо в форме тикетов Kerberos или, если PasswordAuthentication установлена в «yes», пароль, предоставленный пользователем, будет утвержден через Kerberos KDC. Для использования этого параметра серверу необходима Kerberos servtab, которая разрешит проверку субъекта KDC. Значение по умолчанию - «no».
KerberosGetAFSToken	Если AFS активна, и у пользователя имеется Kerberos 5 TGT, получать талон AFS перед обращением к домашнему каталогу пользователя. Значение по умолчанию - «no».
KerberosOrLocalPasswd	В случае непринятия аутентификации посредством Kerberos, проверять пароль другими механизмами, такими как /etc/passwd. Значение по умолчанию - «yes».
KerberosTicketCleanup	Очищать ли кэш талонов пользователя при завершении сеанса. Значение по умолчанию - «yes».
KeyRegenerationInterval	В протоколе версии 1 эфемерный ключ сервера будет автоматически регенерироваться по истечении этого количества секунд (если он использовался). Цель регенерации состоит в том, чтобы предохранить шифрованные установленные сеансы от более поздних вторжений на машину и захвата ключей. Ключ нигде не сохраняется. Если установлено значение «0», то ключ не будет регенерироваться. Значение по умолчанию - 3600 (секунд).
ListenAddress	Локальные адреса, по которым sshd(8) должен ожидать соединения. Могут быть использованы следующие форматы записей:
ListenAddress	хост | адрес-IPv4 | адрес-^6
ListenAddress	хост | адрес-IPv4 : порт
ListenAddress	[хост | адрес-IPv6 : порт] Если порт не указан, sshd будет ожидать соединения на указанном адресе и на всех указанных ранее (но не после) в параметре Port портах. По умолчанию ожидается соединение на всех локальных адресах. Допустимо указание нескольких параметров.
LoginGraceTime	Сервер отключается по истечении этого времени, если пользователю не удалась регистрация в системе. Если стоит значение «0», то время ожидания не ограничено. Значение по умолчанию - 120 секунд.
LogLevel	Задает степень подробности сообщений для протоколов sshd. Допустимыми являются значения: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, и DEBUG3. Значение по умолчанию - INFO. Значения DEBUG и DEBUG1 эквивалентны. Использование значения DEBUG* нарушает конфиденциальность пользователей и потому не рекомендуется.
MACs	Допустимые алгоритмы MAC (Message Authentication Code - код установления подлинности сообщения). Они используются в протоколе версии 2 для гарантирования целостности данных. Несколько алгоритмов следует указывать через запятую. Значение по умолчанию «hmac-md5,hmac-sha1,hmac- ripemd160,hmac-sha1-96,hmac-md5-96».

Параметр	Значение
Match	Начинает условный блок. Если все критерии на строке Match удовлетворены, указанные в блоке директивы будут иметь больший приоритет, чем указанные в глобальном разделе файла конфигурации. Концом блока считается либо следующая директива Match, либо конец файла. В качестве аргументов Match принимаются пары критерий-шаблон. Допустимые критерии: User Group Host и Address. В самом блоке Match допустимо указание следующих параметров: AllowTcpForwarding Banner ForceCommand GatewayPorts GSSApiAuthentication KbdInteractiveAuthentication KerberosAuthentication PasswordAuthentication PermitOpen RhostsRSAAuthentication RSAAuthentication X11DisplayOffset X11Forwarding X11UseLocalHost.
MaxAuthTries	Ограничение на число попыток идентифицировать себя в течение одного соединения. При достижении количества неудачных попыток аутентификации записи о последующих неудачах будут вноситься в протокол. Значение по умолчанию - 6.
MaxStartups	Ограничение на число одновременных соединений, в которых не был пройден этап аутентификации. Все последующие соединения не будут приниматься, пока на уже существующем соединении не будет произведена аутентификация или не истечет время, указанное в параметре LoginGraceTime. Значение по умолчанию - 10. Как альтернатива, может быть задействован ранний случайный отказ в подключении, путем указания трёх разделённых через двоеточие значений «старт:норма:предел» (например, "10:30:60"). Соединение будет сбрасываться с вероятностью «норма/100» (30%), если имеется «старт» (10) (10) соединений с не пройденным этапом аутентификации. Вероятность возрастает линейно и постоянно попытки будут отвергаться при достижении числа «предел» (60).
PasswordAuthentication	Допускать аутентификацию по паролю. Значение по умолчанию - «yes».
PermitEmptyPasswords	Допускать использование пустых паролей при аутентификации по паролю. Значение по умолчанию - «no».
PermitOpen	Ограничить возможные конечные точки для туннелирования TCP. Допустимые формы указания точек:
PermitOpen	хост : порт
PermitOpen	адрес-IPv4 : порт
PermitOpen	[адрес-IPv6] : порт. Возможно указание нескольких конечных точек через пробел. Значение «any» снимает ограничение и является значением по умолчанию.
PermitRootLogin	Допускать вход в систему через ssh в качестве суперпользователя. Допустимые значения: «yes», «prohibit-password»,«without-password», «forced-commands-only», «no». Значение по умолчанию - «prohibit-password». Если этот параметр установлен в значение «prohibit-password» или «without-password», войти в систему в качестве суперпользователя, указав для аутентификации пароль, будет невозможно. Если этот параметр установлен в значение «forced-commands-only», будет разрешена регистрация суперпользователя в системе по открытому ключу, но только если определён параметр command команда (что может быть полезно для удалённого создания резервных копий, даже если регистрация суперпользователя в системе в обычном режиме не разрешена). Все другие методы аутентификации для суперпользователя будут отключены. При значении «no» вход в систему в качестве root будет полностью запрещён.
PermitTunnel	Допускать использование перенаправления для устройств tun(4). Допустимые значения: «yes», «point-to-point» (уровень 3), «ethernet» (уровень 2), «no». Значение «yes» эквивалентно «point-to-point» и «ethernet» одновременно. Значение по умолчанию - «no».
PermitUserEnvironment	Учитывать ли файл ~/.ssh/environment и параметры environment= в файле ~/.ssh/authorized_keys. Значение по умолчанию - «no». Посредством изменения переменных среды пользователи могут обойти ограничения своих полномочий. Например, с помощью механизма LD_PRELOAD.
PidFile	Файл, в который следует записывать идентификатор процесса службы SSH. Значение по умолчанию - /var/run/sshd.pid.
Port	Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию - 22. Допустимо указание параметра несколько раз. См. также ListenAddress.
PrintLastLog	Выводить ли время и дату предыдущего входа в систему при интерактивной регистрации пользователя в ней. Значение по умолчанию - ''yes''.
PrintMotd	Выводить ли содержимое файла /etc/motd при интерактивной регистрации пользователя в системе (в некоторых системах это выполняется оболочкой, сценарием /etc/profile или аналогичным). Значение по умолчанию - «yes».
Protocol	Версии протокола, которые следует принимать. Допустимые значения - '1' и '2'. Несколько значений указываются через запятую. Значение по умолчанию - «2,1». Порядок указания протоколов не имеет значения, т.к. протокол выбирается клиентом из списка доступных.
PubkeyAuthentication	Допускать аутентификацию по открытому ключу. Значение по умолчанию - «yes». Данный параметр относится только к протоколу версии 2.
RhostsRSAAuthentication	Допускать аутентификацию по rhosts или /etc/hosts.equiv совместно с аутентификацией по хосту RSA. Значение по умолчанию - «no». Данный параметр относится только к протоколу версии 1.
RSAAuthentication	Допускать аутентификацию только по ключу RSA. Значение по умолчанию - «yes». Данный параметр относится только к протоколу версии 1.
ServerKeyBits	Длина ключа сервера для эфемерного протокола версии 1. Минимальное значение - 512, значение по умолчанию - 768.
StrictModes	Проверять наборы прав доступа и принадлежность конфигурационных файлов и домашнего каталога пользователя перед разрешением регистрации в системе. Это рекомендуется выполнять, потому что новички иногда оставляют свои каталоги или файлы доступными для записи всем. Значение по умолчанию - «yes».
Subsystem	Позволяет настроить внешнюю подсистему (напр., службу FTP). В качестве параметров должны выступать имя подсистемы и команда, которая будет выполняться при запросе подсистемы. Команда sftp-server(8) реализует подсистему передачи файлов «sftp». По умолчанию подсистемы не определены. Данный параметр относится только к протоколу версии 2.
SyslogFacility	Код источника сообщений для протокола syslog. Допустимые значения: DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7. Значение по умолчанию - AUTH.

Параметр	Значение
TCPKeepAlive	Указывает, будет ли система посылать другой стороне контрольные сообщения для удержания соединения активным. Если они посылаются, то разрыв соединения или аварийный отказ одной из машин будут должным образом замечены. Однако, при этом временная потеря маршрута также повлечёт за собой разрыв соединения, и некоторые люди сочтут это раздражающим. С другой стороны, если контрольные сообщения не посылаются, сеанс на сервере может зависнуть, оставив после себя «пользователей-привидений» и отнимая ресурсы сервера. Значение по умолчанию - «yes» (отправлять сообщения TCP keepalive). Это позволяет избежать бесконечно долгих сеансов. Для отключения отправки сообщений TCP keepalive установите значение «no».
UseDNS	Выполнять ли запросы DNS для получения имени удалённого хоста, для того чтобы убеждаться в том, что обратное преобразование выдаёт тот же самый IP-адрес. Значение по умолчанию - «yes».
UseLogin	Использовать login(1) для интерактивных сеансов регистрации в системе. Значение по умолчанию - «no». Имейте ввиду, что login(1) никогда не используется для удалённого выполнения команд. Если этот параметр включен, функция X11Forwarding будет отключена, потому что login(1) не может обрабатывать cookie xauth(1). В случае использования разделения полномочий (UsePrivilegeSeparation) данный параметр будет отключен после прохождения аутентификации.
UsePAM	Включить интерфейс модулей аутентификации Pluggable Authentication Module. При значении «yes» аутентификация PAM будет доступна через ChallengeResponseAuthentication и PasswordAuthentication в дополнение к учётной записи PAM и обработке модулей сеансов для всех типов аутентификации. Поскольку беспарольная аутентификация PAM «вызов-ответ» служит заменой аутентификации по паролю, необходимо отключить либо PasswordAuthentication, либо ChallengeResponseAuthentication. При включенном UsePAM службу sshd(8) можно будет выполнять только с правами root. Значение по умолчанию - «no».
UsePrivilegeSeparation	Разделять полномочия посредством создания дочернего процесса с меньшими правами для обработки входящего сетевого трафика. После прохождения аутентификации для работы с клиентом будет создаваться специальный процесс, соответствующий его правам. Целью данного параметра служит предотвращение повышения полномочий злоумышленником. Значение по умолчанию - «yes».
X11DisplayOffset	Номер первого дисплея, доступного для туннелирования трафика X11 sshd(8). Позволяет избежать вмешательства sshd в работу настоящих серверов X11. Значение по умолчанию - 10.
X11Forwarding	Допускать туннелирование X11. Допустимые значения - «yes» и «no». Значение по умолчанию - «no». Если дисплей-посредник ожидает соединений от любых адресов (или по шаблону) sshd(8), включение туннелирования X11 подвергает сервер и логические дисплеи клиентов дополнительной опасности. Поэтому такое поведение не является поведением по умолчанию. Проверка и подмена аутентификационных данных при атаке выполняются на стороне клиента. При туннелировании X11 графический сервер клиента может подвергаться атаке при запросе клиентом SSH-туннелирования (см. замечания в описании параметра ForwardX11 в ssh_config(5)). Для большей защиты пользователей администратор может запретить туннелирование, установив значение «no». Обратите внимание, что даже если туннелирование X11 запрещено данным параметром, пользователи по-прежнему смогут туннелировать трафик X11 посредством настройки туннелей общего назначения. Туннелирование X11 отключается автоматически при включении UseLogin.
X11UseLocalhost	К какому адресу следует привязывать сервер туннелирования X11: к кольцевому (loopback) или адресу, указанному по шаблону. По умолчанию сервер туннелирования привязывается к кольцевому адресу, а в качестве хоста в переменную среды DISPLAY заносится «localhost». Это не позволяет удалённым хостам подключаться к дисплею-посреднику. Однако, в случае старых клиентов X11, такая конфигурация может не сработать. Установите тогда X11UseLocalhost в «no». Допустимые значения - «yes» и «no». Значение по умолчанию - «yes».
XAuthLocation	Путь к команде xauth(1). Значение по умолчанию - /usr/X11R6/bin/xauth.

Указание времени

Ключи командной строки **sshd** и параметры файлов конфигурации могут требовать указания времени. Оно должно указываться в виде последовательности таких выражений:

```
<время> <единицы>
```

, где <время> - положительное целое число, <единицы> могут принимать следующие значения:

Единица	Значение единицы
ничего	-
s | S	секунды
m | M	минуты
h | H	часы
d | D	дни
w | W	недели

Итоговое время получается в результате сложения всех выражений.

Примеры:

Единицы	Значения
600	600 секунд (10 минут)

10m	10 минут
1h30m	1час 30 минут (90 минут)

Файлы

Файл конфигурации sshd.

/etc/ssh/sshd_config

> **Примечание!** Этот файл должен быть доступен для записи только пользователю **root**, и рекомендуется делать его доступным для чтения всем.

Работа с клиентом и сервером SSH

Описание принципов работы и используемых приложений
Установка
Настройка сервера
Рекомендуемые параметры безопасности
Максимальное число попыток аутентификации
Время ожидания регистрации пользователя в системе
Списки пользователей sshd
Запрещение удаленного доступа для суперпользователя
Парольная аутентификация
Аутентификация на основе SSH2 RSA-ключей
Настройка SSH-клиента
Утилита screen
SSH aliases
SFTP
Монтирование удаленной директории с помощью sshfs
Запуск графических приложений через SSH
Копирование файлов SCP
Подключение через MC (Midnight Commander)
Диагностика проблем подключения

Данная статья посвящена клиенту и серверу защищенного терминала (secure shell) в РЕД ОС, их настройке и использованию. **SSH** — это специальный сетевой протокол, позволяющий получать удаленный доступ к компьютеру с большой степенью безопасности соединения.

Описание принципов работы и используемых приложений

В основном, SSH реализован в виде двух приложений — *SSH-сервера* и *SSH-клиента*. При подключении клиент проходит процедуру авторизации у сервера и между ними устанавливается зашифрованное соединение. OpenSSH-сервер может работать как с протоколом *ssh1*, так и с протоколом *ssh2*. В настоящее время протокол **ssh1** считается небезопасным, поэтому его использование **крайне не рекомендуется**. В этой статье мы не будем останавливаться на технических деталях работы протокола, так как основная цель руководства — описание его настройки и использования.

Вы можете подробнее ознакомиться с информацией установке и настройке клиента и сервера SSH, просмотрев наши обучающие видео:

- на **RuTube** — Работа с клиентом и сервером SSH;
- в **Яндекс.Дзен** — Работа с клиентом и сервером SSH;
- в **VK Видео** — Работа с клиентом и сервером SSH.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

По умолчанию сервер и клиент **OpenSSH** уже установлен в РЕД ОС. Однако, при необходимости, его можно установить из терминала командой:

```
sudo dnf install openssh
```

Настройка сервера

Для его остановки и запуска используйте команды:

```
sudo systemctl stop sshd
sudo systemctl start sshd
```

Основной файл конфигурации SSH-сервера — файл **/etc/ssh/sshd_config**, доступный для чтения или редактирования только суперпользователю. После каждого изменения этого файла необходимо перезапустить ssh-сервер для применения таких изменений командой:

```
sudo systemctl restart sshd
```

Рекомендуемые параметры безопасности

Сам по себе, неправильно настроенный SSH-сервер — огромная уязвимость в безопасности системы, т. к. у потенциального злоумышленника есть возможность получить практически неограниченный доступ к системе. Помимо этого, у *sshd* есть много дополнительных полезных опций, которые желательно включить для повышения удобства работы и безопасности.

```
Port, ListenAddress и AddressFamily
```

Эти три параметра определяют, на каких портах и адресах ваш сервер будет ждать входящие соединения. Во-первых, имеет смысл по возможности ограничить семейство обрабатываемых адресов реально используемыми, т. е. если вы используете только IPv4 — отключите IPv6, и наоборот. Сделать это можно при помощи параметра **AddressFamily**, например (для разрешения IPv4 и запрета IPv6):

```
AddressFamily inet
```

Во-вторых, если ваш ssh-сервер имеет выход в интернет, либо находится в незащищённой сети, желательно сменить стандартный порт (22), на котором слушает sshd. Это связано с тем, что многочисленные сетевые сканеры постоянно пытаются соединиться с 22-м портом и, как минимум, получить доступ путем перебора логинов/паролей из своей базы. Даже если у вас и отключена парольная аутентификация — эти попытки сильно засоряют журналы и (в большом количестве) могут негативно повлиять на скорость работы ssh-сервера. Если же вы по какой-либо причине не желаете изменить стандартный порт, вы можете использовать различные внешние утилиты для борьбы брутфорсерами, например *fail2ban*.
Задать порт можно как абсолютным значением для всех интерфейсов при помощи директивы **Port**, так и конкретным значением для каждого интерфейса, при помощи директивы **ListenAddress**. Например:

```
Port 2002
```

или

```
ListenAddress 192.168.0.1:2003
ListenAddress 192.168.1.1:2004
```

После того, как был задан порт, в любой из приведённых выше опций, необходимо предупредить систему безопасности операционной системы о внесённых изменениях. Если этого не сделать, то, при попытке перезапуска ssh-сервера, SELinux заблокирует его работу. Для этого используем команду:

```
sudo semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
```

Если задан порт, отличный от стандартного, строка подключения будет иметь вид:

```
ssh -p 2002 user@server
```

Максимальное число попыток аутентификации

```
MaxAuthTries
```

Прописывается в файле **/etc/ssh/sshd_config** и указывает максимальное число попыток аутентификации, разрешенное для одного соединения. Как только число неудачных попыток превысит половину заданного значения, все последующие попытки будут заноситься в журнал. При достижении максимума сеанс аутентификации разрывается.

Время ожидания регистрации пользователя в системе

```
LoginGraceTime
```

Как и предыдущий параметр, указывается в файле настройки ssh-сервера. Он задаёт время ожидания регистрации пользователя в системе. Если пользователь не успел войти в систему в течение отведенного данной директивой времени, сеанс обрывается.

Списки пользователей sshd

```
AllowUsers user
```

В файле настроек **/etc/ssh/sshd_config** может быть прописан список пользователей, разделённых пробелом, которым можно пользоваться sshd. По умолчанию — не указан = разрешено всем. Т.е. если указан хотя бы один пользователь, ssh доступ к серверу доступен только для него.

```
AllowGroups users
```

Список шаблонов имён групп через пробел. Если параметр определён, регистрация в системе разрешается только пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп; числовой

идентификатор группы не распознаётся. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups. Подробнее см. "Конфигурационный файл SSHD_CONFIG"

Дополнительную информацию см. в статье "Служба sshd - OpenSSH, сервер протокола SSH, описание"

Запрещение удаленного доступа для суперпользователя

Учетная запись root часто является целью хакеров. Доступ к учетной записи через root по протоколу SSH на сервере Linux, который работает в сети или в Интернете, может представлять серьезную угрозу безопасности.
По умолчанию root-доступ по паролю разрешён. Если есть пользователь, который имеет возможность решать все административные задачи через sudo, то рекомендуется совсем отключить root-доступ по ssh. Отключить эту опцию можно так:

```
PermitRootLogin no
```

Парольная аутентификация

Разрешенная по умолчанию парольная аутентификация является практически самым примитивным способом авторизации в **sshd**. С одной стороны, это упрощает конфигурацию и подключение новых пользователей (пользователю достаточно знать свой системный логин/пароль), с другой стороны пароль всегда можно подобрать, а пользователи часто пренебрегают созданием сложных и длинных паролей. Специальные боты постоянно сканируют доступные из интернета ssh-сервера и пытаются авторизоваться на них путем перебора логинов/паролей из своей базы. Настоятельно не рекомендуется использовать парольную аутентификацию. Отключить ее можно так:

```
PasswordAuthentication no
```

Если по каким-либо причинам вам все-таки хочется использовать парольную аутентификацию — позаботьтесь о том, чтобы никто не мог авторизоваться с пустым паролем. Для этого задайте директиву **PermitEmptyPasswords**:

```
PermitEmptyPasswords no
```

Аутентификация на основе SSH2 RSA-ключей

Наиболее предпочтительным способом авторизации является аутентификация на основе SSH2 RSA-ключей. При таком способе пользователь генерирует на своей стороне пару ключей, из которой один ключ является *приватным*, а другой *публичным*. *Публичный* ключ копируется на сервер и служит для проверки идентичности пользователя. Подробную информацию о создании пары ключей и способах их размещения на сервере см. в нашей инструкции «Аутентификация по протоколу SSH с использованием RSA-ключа».

Для включения аутентификации по публичному ключу в файле конфигурации сервера **/etc/ssh/sshd_config** для параметра PubkeyAuthentication укажите значение yes:

```
PubkeyAuthentication yes
```

Сервер должен знать, где ему следует искать публичный ключ пользователя. Для этого применяется специальный файл **authorized_keys**.

Можно указать как один общий файл с ключами, так и по одному файлу на каждого пользователя. Последний способ является более удобным и безопасным, т. к. можно, во-первых, указывать разные комбинации ключей для каждого пользователя, а во-вторых, ограничить доступ к публичному ключу пользователя. Задать файл с ключами можно при помощи директивы **AuthorizedKeysFile**:

- для схемы с общим файлом:

```
AuthorizedKeysFile /etc/ssh/authorized_keys
```

- для схемы пользователь — файл:

```
AuthorizedKeysFile .ssh/authorized_keys
```

По умолчанию SSH-клиент ищет ключи в файле **.ssh/authorized_keys**, т. е. по схеме пользователь-файл.

Настройка SSH-клиента

Наиболее безопасным считается вход по ключу, и в большинстве случаев на стороне сервера такая возможность включена, так что для её использования никаких прав суперпользователя не требуется. На клиентской машине генерируем ключ:

```
ssh-keygen -t rsa
```



Получаем предложение ввести пароль для защиты файла ключа (оказывается полезным при попадании файла в чужие руки). Если мы собираемся по SSH выполнять скрипты, то оставляем пароль пустым. Передаём публичный ключ на сервер командой:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
```

Всё, можно заходить:

```
ssh user@server
```

Когда ssh работает на нестандартном порту:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub -p port user@server
```

Если возникает ошибка, попробуйте взять параметры в кавычки:

```
ssh-copy-id '-i /home/user/.ssh/id_rsa.pub -p port user@server'
```

Завершающий этап настройки: отключение парольной аутентификации на сервере, см. «Парольная аутентификация».

Примечание.

В новых версиях **systemd** и **OpenSSH** поддержка **tcp_wrappers** будет прекращена.

tcp_wrapper выполняет управление доступом только для приложений, разработанных на основе протокола **TCP** и вызывающих библиотеку **libwrap**. После удаления зависимости **libwrap** из **openssh** перестанут действовать правила, определенные в файле **/etc/hosts.deny**. Для блокирования нежелательного трафика необходимо использовать брандмауэры **iptables/nftables** на сетевом уровне или использовать аналогичную фильтрацию на уровне приложений, поскольку они не имеют подобных ограничений.

ВАЖНО!

Мы **НЕ РЕКОМЕНДУЕМ** продолжать использовать инструмент **tcp_wrappers**. Для контроля трафика используйте брандмауэр **firewall**. Подробную информацию о настройке брандмауэра можно посмотреть по ссылке.

Если вы все же решите продолжить использовать инструмент **tcp_wrappers** для контроля сетевого трафика, функциональность данного инструмента для любой службы можно возобновить, выполнив ряд действий:

Примечание.

В случае, если используется **РЕД ОС 8**, необходимо предварительно установить пакет **tcp_wrappers** командой:

```
sudo dnf install tcp_wrappers
```

1. Отключите службу **sshd**:

```
systemctl disable sshd
```

2. Создайте каталог **/etc/systemd/system/sshd@.service.d/** для переопределения конфигурации:

```
mkdir -p /etc/systemd/system/sshd@.service.d/
```

3. Создайте переопределяющий файл конфигурации для службы SSH **/etc/systemd/system/sshd@.service.d/override.conf**:

```
nano /etc/systemd/system/sshd@.service.d/override.conf
```

```
[Unit]
ConditionFileIsExecutable=/usr/sbin/tcpd

[Service]
ExecStart=
```

4. В переопределяющий файл добавьте параметр **ExecStart** из файла конфигурации по умолчанию, добавив в значение **@-/usr/sbin/tcpd**:

```
grep '^ExecStart=' /usr/lib/systemd/system/sshd@.service | sed 's#[^\/]*\(.*\)#ExecStart=@-/usr/sbin/tcpd \1#'
>>/etc/systemd/system/sshd@.service.d/override.conf
```

Пример содержимого переопределяющего файла конфигурации:

```
cat /etc/systemd/system/sshd@.service.d/override.conf

[Unit]
ConditionFileIsExecutable=/usr/sbin/tcpd

[Service]
ExecStart=
ExecStart=@-/usr/sbin/tcpd /usr/sbin/sshd -i $OPTIONS
```

5. Измените политику SELinux для отслеживания трафика по **TCP**:

```
setsebool -P ssh_use_tcpd=1
```

6. Перезапустите конфигурацию **systemctl**:

```
systemctl daemon-reload
```

7. Запустите и добавьте в автозагрузку сокет **sshd**:

```
systemctl enable --now sshd.socket
```

8. Проверьте подключение к новой службе:

```
ssh localhost
```

Подключение должно произойти вне зависимости от содержимого файлов **/etc/hosts.allow** и **/etc/hosts.deny**.

9. Внесите изменения в файл запрещенных соединений **/etc/hosts.deny**:

```
nano /etc/hosts.deny
```

```
sshd: 127.0.0.1 [::1]
```

10. Убедитесь, что содержимое файла **/etc/hosts.deny** зафиксировано:

```
ssh localhost

kex_exchange_identification: read: Connection reset by peer
Connection reset by ::1 port 22
```

Соединение должно быть заблокировано.

11. Заблокированное соединение также должно быть зафиксировано в журнале:

```
journalctl -t sshd | grep refused
```

```
окт 17 16:19:44 localhost.localdomain sshd[4249]: refused connect from ::1 (::1)
```

Аналогичный подход можно использовать для других служб, у которых удалена зависимость **tcp_wrappers**.

Утилита screen

Screen – это приложение, позволяющее запускать несколько виртуальных терминалов в режиме сессий. После того как сессия создана, от неё можно отключиться, а позже — снова подключиться, причём с любого другого хоста, на котором установлен SSH-клиент. Процессы, запущенные в **screen**, продолжают выполняться и после того как пользователь отключается от сессии или вообще от хоста в целом.

Для установки программы **screen** на сервере выполните команду:

```
dnf install screen
```

Подключаемся к серверу:

```
ssh user@server
```

После подключения создаем новую сессию **screen** с названием **session1**:

```
screen -S session1
```

Затем выполняем на сервере необходимые действия и команды. Для примера запустим **ping** до ресурса **ya.ru**:

```
ping ya.ru
```

Для отключения от сессии нажмем сочетание «**Ctrl+a d**». При этом процесс **ping** продолжит выполнение, даже если разорвать ssh-подключение к серверу. Чтобы вернуться в нашу сессию выполним команду:

```
screen -r session1
```

Можно увидеть, что утилита **ping** все еще будет работать.

Более подробную информацию о работе с терминальными мультиплексорами описана в статье Терминальные мультиплексоры.

SSH aliases

При использовании нескольких серверов с различными параметрами доступа (нестандартный порт, длинное имя хоста, логин отличный от локального, и т.п.) приходится каждый раз вводить настройки подключения заново. Чтобы облегчить этот процесс, можно использовать псевдонимы — **aliases**.

Настройки хранятся в **~/.ssh/config** для одного пользователя и в **/etc/ssh/ssh_config** глобально для всех пользователей.

Пример конфигурации.

Открываем с помощью текстового редактора нужный нам файл настроек (для одного пользователя или глобальный) и добавляем следующие строки:

```
Host AliasName
HostName 1.2.3.4
User YourUserName
Port YourSSHPort
```

Где:

- **Host** — алиас (псевдоним) для удаленного сервера;
- **HostName** — IP-адрес или доменное имя (если работает DNS) удаленного сервера;
- **User** — имя пользователя для соединения по SSH;
- **Port** — порт SSH на удаленном сервере.

Таким образом может быть описано множество серверов.

После этого можно подключаться к серверу командой

```
ssh AliasName
```

SFTP

В sshd по умолчанию встроен SFTP-сервер. Протокол **SFTP** (**SSH File Transfer Protocol**) — SSH-протокол для передачи файлов. Он предназначен для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения. Как правило, в качестве базового протокола, обеспечивающего соединение, и используется протокол SSH2. Для того чтобы включить поддержку SFTP, добавьте в **sshd_config** строку:

```
subsystem sftp /usr/libexec/openssh/sftp-server
```

По умолчанию поддержка SFTP включена.

Монтирование удаленной директории с помощью sshfs

При постоянном использовании ресурсов ssh-сервера, для удобства возможно монтирование удаленного каталога в локальную директорию.

Установка:

```
sudo dnf install sshfs
```

Монтирование:

```
sshfs user@server:/home/userdir ~/sshfsdir
```

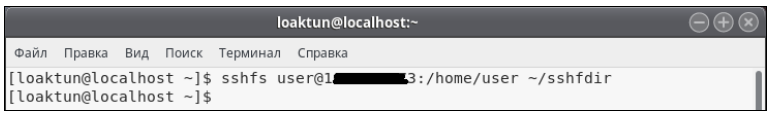
Директория, в которую производится монтирование, должна быть предварительно создана:

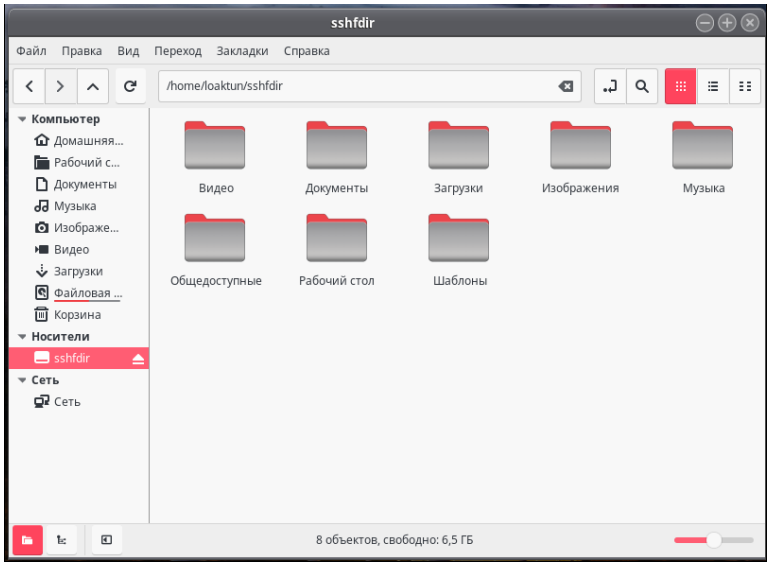
```
mkdir ~/sshfsdir
```

Размонтирование:

```
fusermount -u ~/sshfsdir
```

Пример:





Запуск графических приложений через SSH (X11Forwarding)

Настройка сервера.

В файле конфигурации **/etc/ssh/sshd_config** прописываем:

```
...
X11Forwarding yes
```

```
...
```

Перезапускаем ssh-сервер:

```
systemctl restart sshd
```

Настройка клиента.

В файле конфигурации **/etc/ssh/ssh_config** прописываем:

```
...
ForwardX11 yes
...
```

После того, как настройка закончена, заходим на удаленный хост и потом запускаем приложение, например, текстовый редактор **pluma**:

```
ssh -XC user@server
pluma
```

Чтобы сразу запустить приложение pluma:

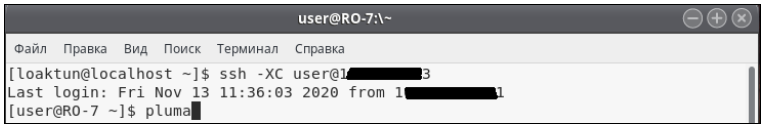
```
ssh -XC user@server "pluma"
```

Опции:

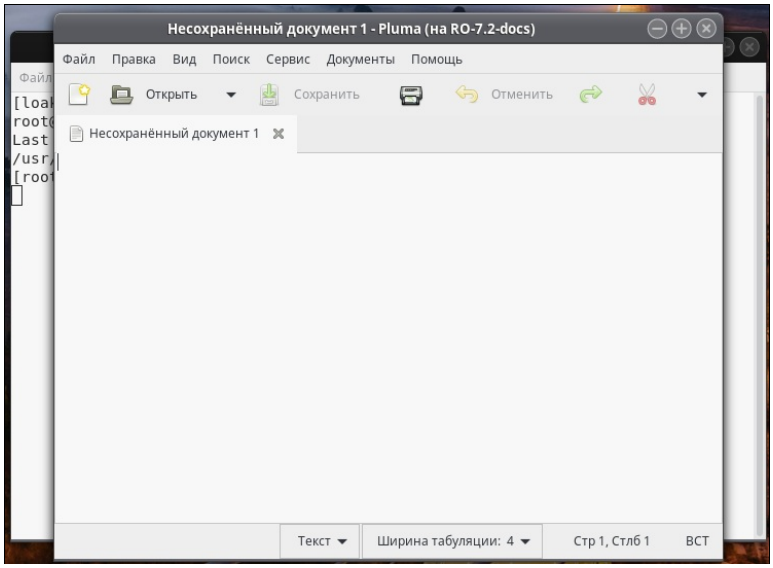
```
X : перенаправлять графический вывод
C : компрессия передаваемых данных
```

Пример.

Запуск:



Результат выполнения:



Создаваемый файл будет сохранён на удалённой машине.

Копирование файлов SCP

С помощью этой консольной утилиты можно перемещать файлы между удалённой и локальной системой.

Копирование файла на удалённую машину:

```
scp /srcfolder/file1 user@server:/destfolder/file1
```

Копирование файла на локальную машину с удалённой:

```
scp user@server:/srcfolder/file1 /destfolder/file1
```

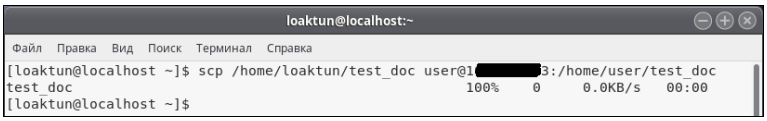
При копировании файлов нужно учитывать, что если на удалённой машине уже существует файл с таким же именем, то после выполнения команды он будет перезаписан.

Доступные опции :

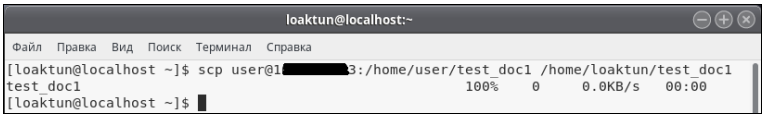
```
C : сжимать данные при их отправке на конечный компьютер.
r : рекурсивно копировать каталоги.
```

Пример.

Копирование на удалённую машину:



Копирование из удалённой системы в локальную:



Подключение через MC (Midnight Commander)

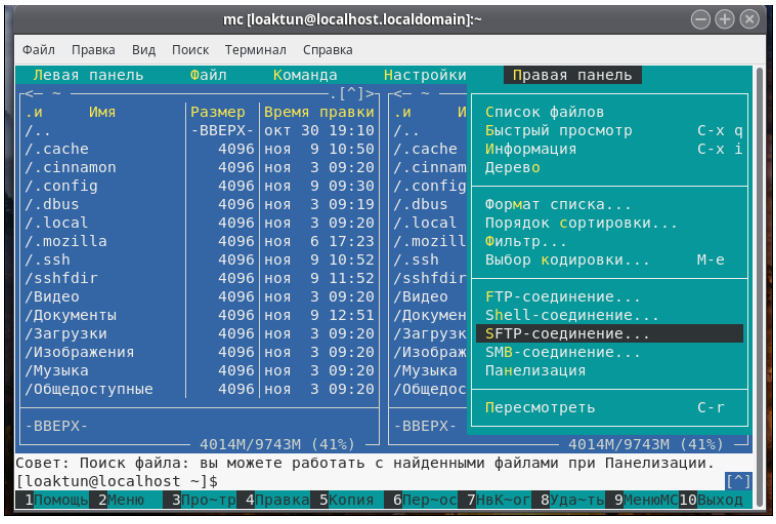
Midnight Commander (**MC**) — это визуальный файловый менеджер. Это программа, которая позволяет вам копировать, перемещать и удалять файлы и директории, производить поиск файлов и запускать на выполнение команды оболочки.

Также Midnight Commander позволяет подключиться к ssh-серверу.

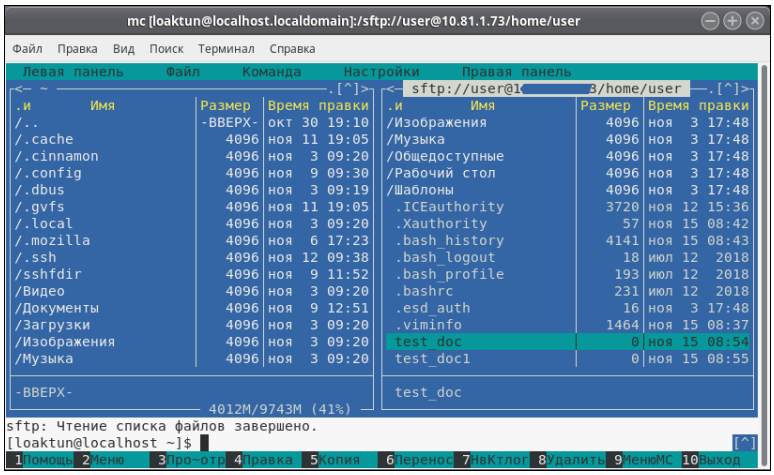
Для запуска программы в консоли вводим:

```
mc
```

После чего, клавишей **F9** активируем верхнее меню. В нём выбираем панель, левую или правую, в которой будет произведено подключение к ssh-серверу. В выпадающем меню выбираем пункт «SFTP-соединение».



После этого в появившейся строке вводим адрес сервера в формате **user@server**, и пароль, если аутентификация происходит не по ключу. В результате получим удобный и наглядный вариант для работы с файлами на сервере и возможностью производить копирование файлов как на сервер, так и с него на локальную систему.



Диагностика проблем подключения

Для анализа лога подключения используется команда:

```
ssh -vvv user@server
```

Для анализа конфигурационных файлов ssh-клиента и сервера, вам может понадобиться подробное описание параметров, значений и т. п. Для этого используйте команды вывода справки:

```
man ssh #
man sshd #
```

Muon – графический SSH-клиент

Предварительная подготовка
Установка и настройка Muon
Смена языка интерфейса
Работа с программой

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: snapd-2.65.1-1, muon-ssh-2.2.0

Muon - это графический SSH-клиент. В нем доступны такие инструменты как:

- расширенный файловый браузер **SFTP**,
- эмулятор терминала **SSH**,
- удаленный менеджер ресурсов/процессов,
- анализатор дискового пространства сервера,
- текстовый редактор,
- просмотрщик журналов, а также многие другие полезные инструменты, которые упрощают работу пользователей.

Muon предоставляет функциональность, аналогичную веб-панелям управления, но работает по протоколу **SSH** с локального компьютера, следовательно, установка на сервер не требуется.

Вы можете подробнее ознакомиться с работой графической утилиты **muon**, просмотрев наши обучающие видео:

- на **RuTube** — Muon - графический SSH-клиент;
- в **Яндекс.Дзен** — Muon - графический SSH-клиент;
- в **VK Видео** — Muon - графический SSH-клиент.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка

Muon в РЕД ОС устанавливается и запускается с помощью изолированной программной среды **snap**, поэтому перед настройкой muon требуется установить **snap**, если он еще не установлен.

Подробную информацию об установке и настройке **snap** см. в нашей статье «Snap - изолированная среда для запуска приложений».

После установки **snap** потребуется перезагрузить систему, чтобы убедиться, что пути snap были обновлены правильно.

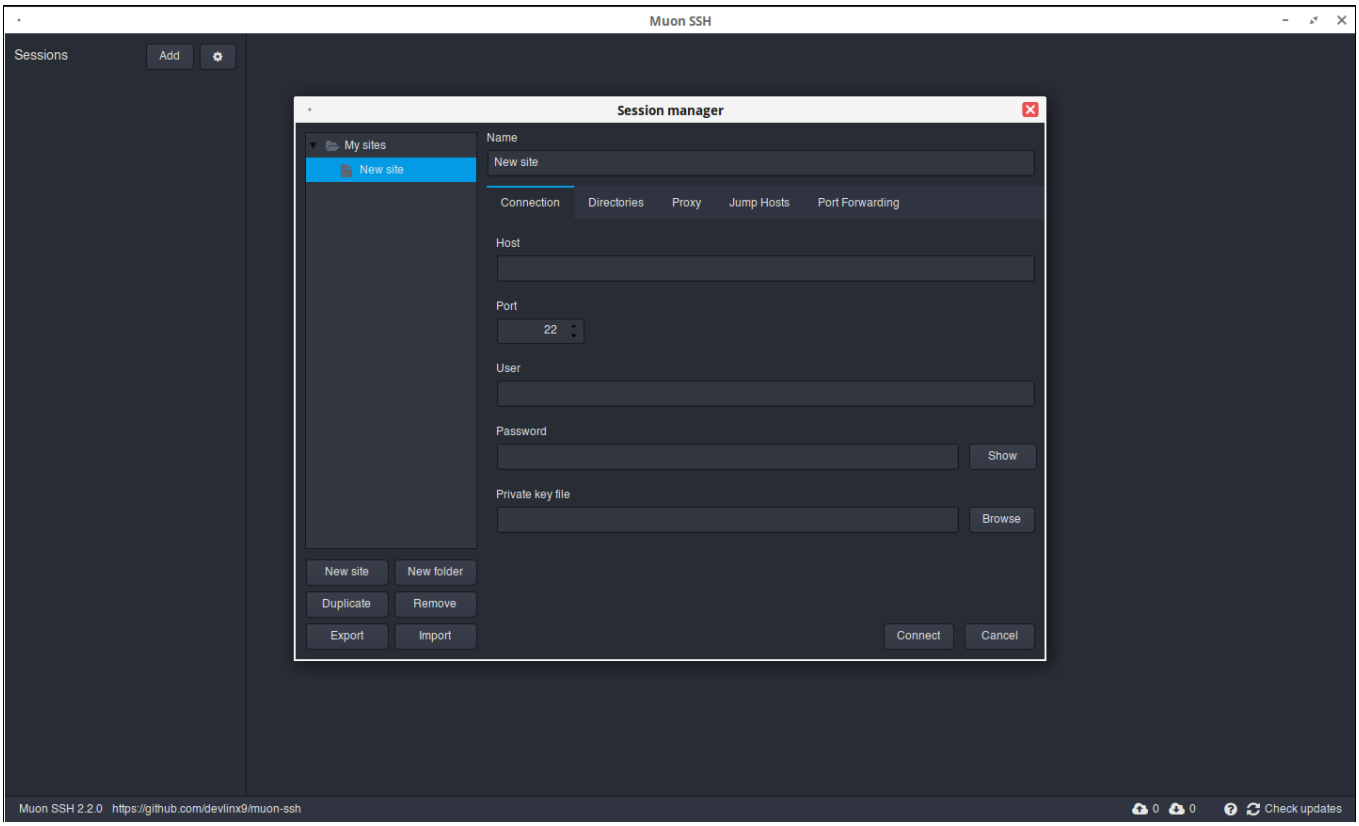
Установка и настройка Muon

Для установки **muon** выполните следующую команду:

```
sudo snap install muon-ssh --edge
```

После установки запуск программы доступен из «**Главного меню**» — «**Прочие**» — «**Muon SSH client snap**».

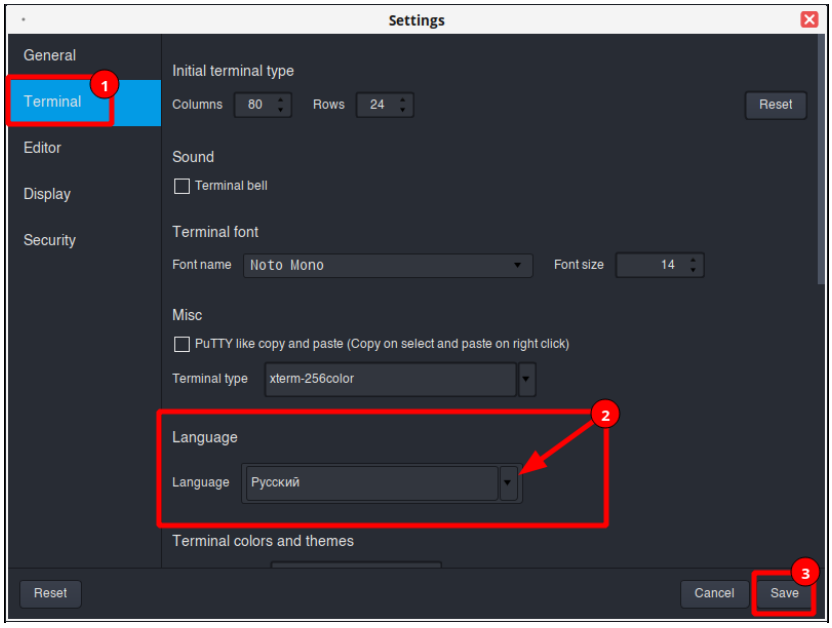
Главное окно клиента **muon** выглядит следующим образом:



Смена языка интерфейса

Для смены языка приложения откройте настройки программы, нажав на кнопку  .

На вкладке «**Terminal**» в разделе «**Language**» в выпадающем меню выберите необходимый язык (в примере выбран русский). Нажмите «**Save**».

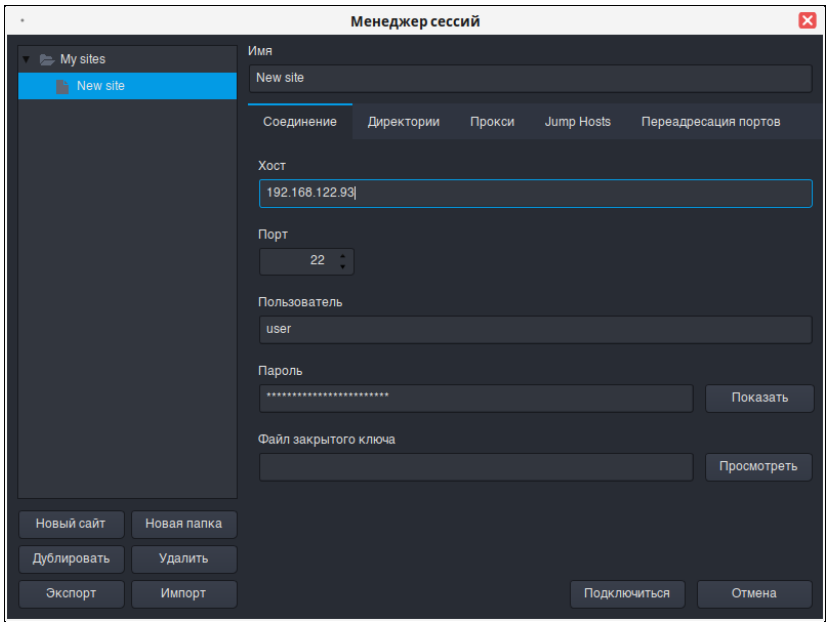


Для применения изменений перезапустите программу.

Работа с программой

Для использования **muon** необходим настроенный SSH-сервер, к которому будет производиться подключение. Информацию о настройке SSH-сервера см. в нашей статье «Работа с клиентом и сервером SSH».

Для подключения к SSH-серверу на главной странице программы нажмите кнопку «**Добавить**». Будет открыто окно настройки подключения «**Менеджер сессий**».



В поле **Хост** укажите IP-адрес сервера или имя хоста.

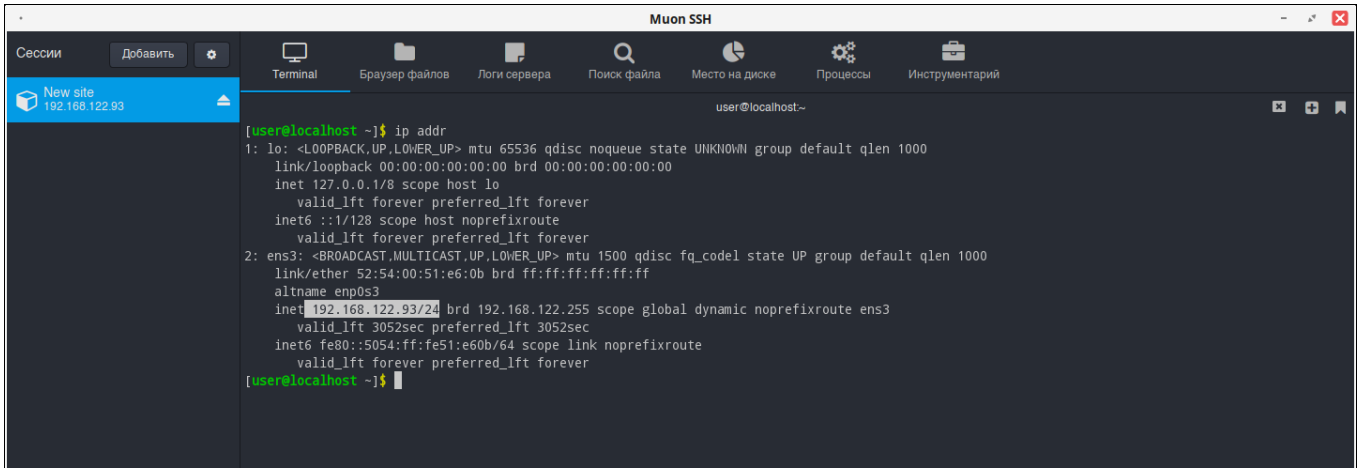
В поле **Порт** укажите нормер порта для подключения (по умолчанию используется порт 22).

В поле **Пользователь** укажите имя пользователя, к учетной записи которого необходимо подключиться.

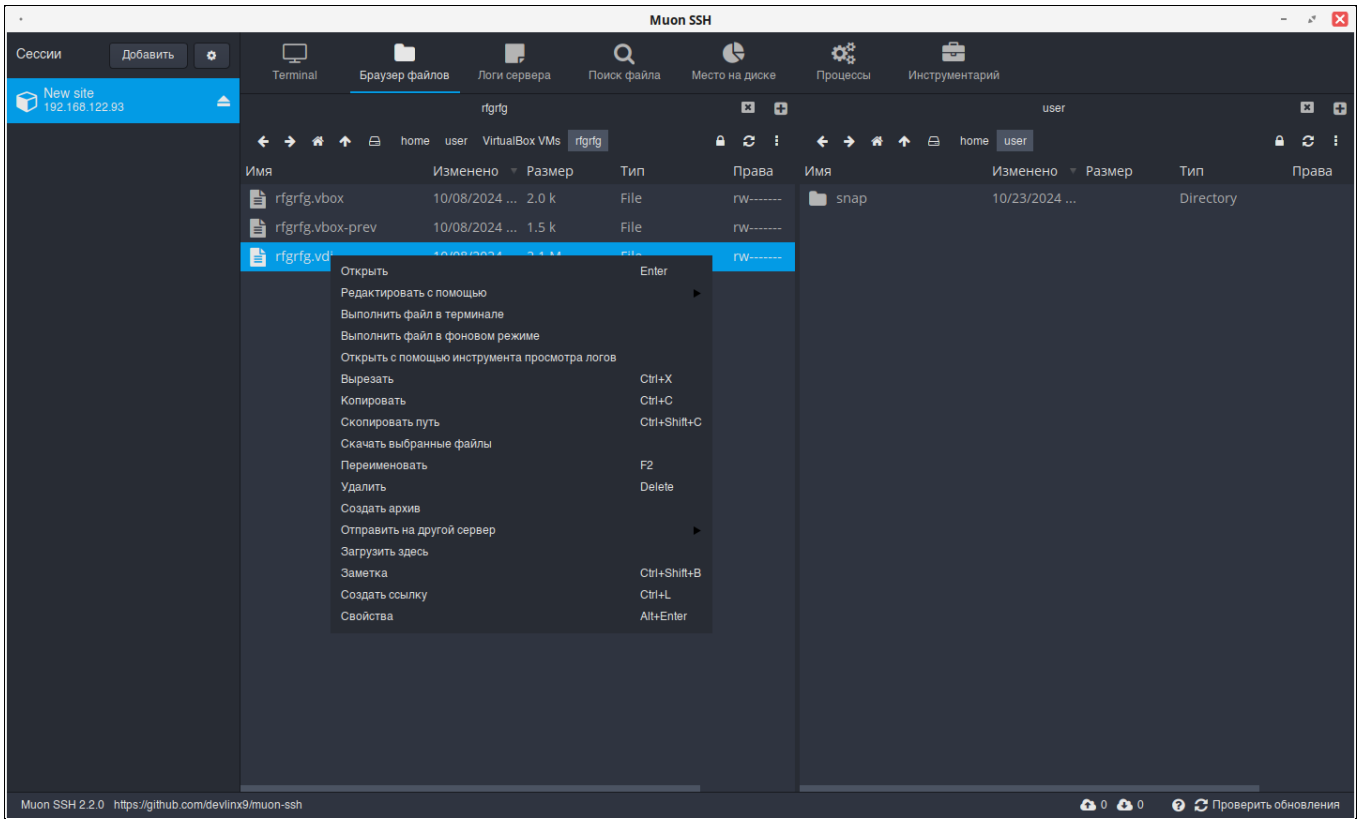
В поле **Пароль** укажите пароль от учетной записи указанного выше пользвоателя.

В поле **Файл закрытого ключа** загрузите файл из каталога, в котором хранится закрытый ключ.

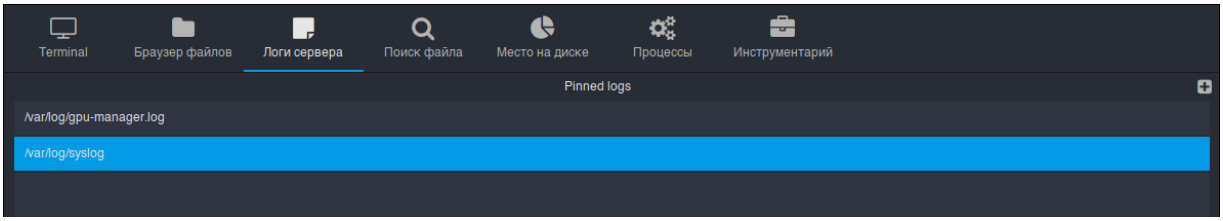
При успешном подключении будет запущен терминал удалённого хоста.



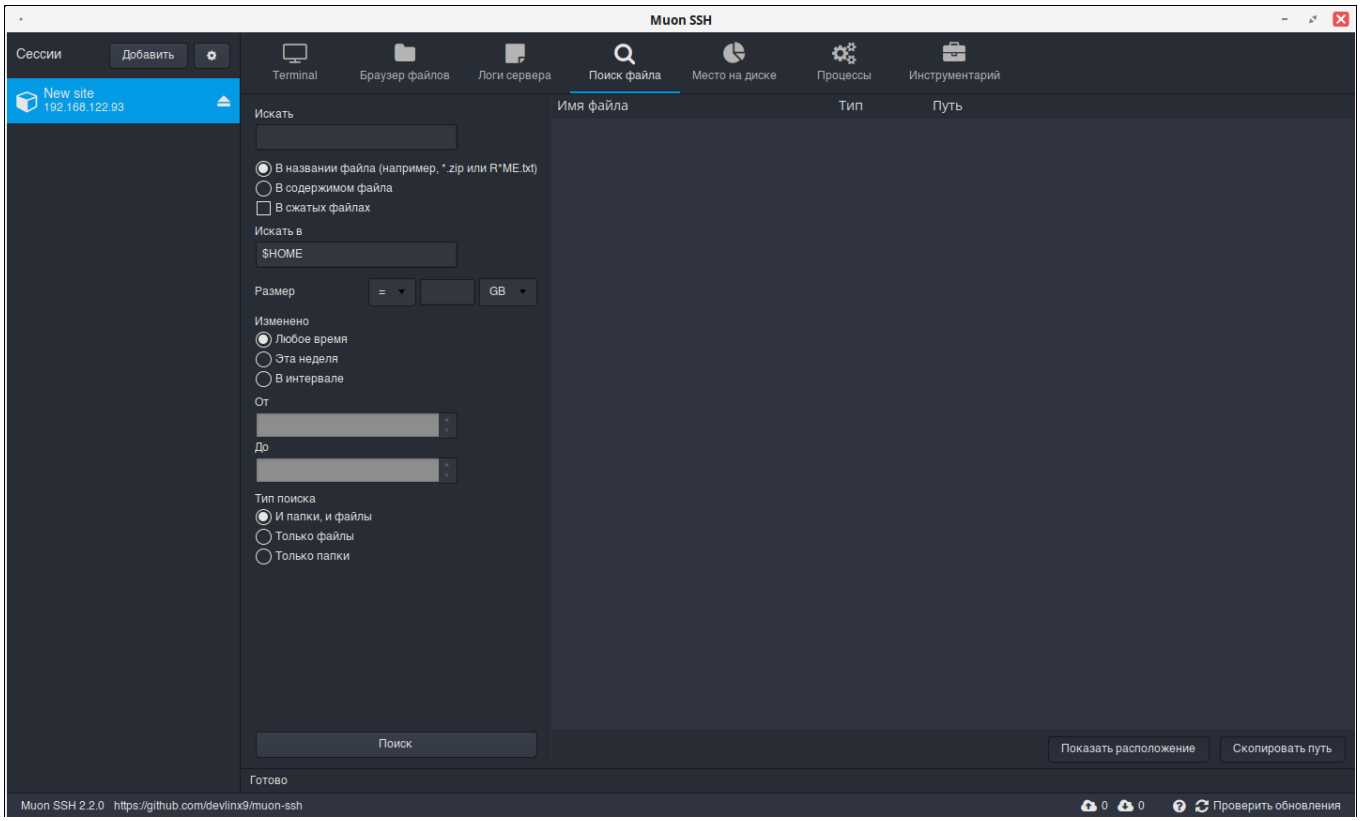
На вкладке «**Браузер файлов**» можно просмотреть содержимое каталогов, доступных пользователю. При нажатии ПКМ по какому-либо файлу или каталогу будет вызвано контекстное меню с доступными действиями.



На вкладке «**Логи сервера**» доступны системные журналы удаленного хоста.

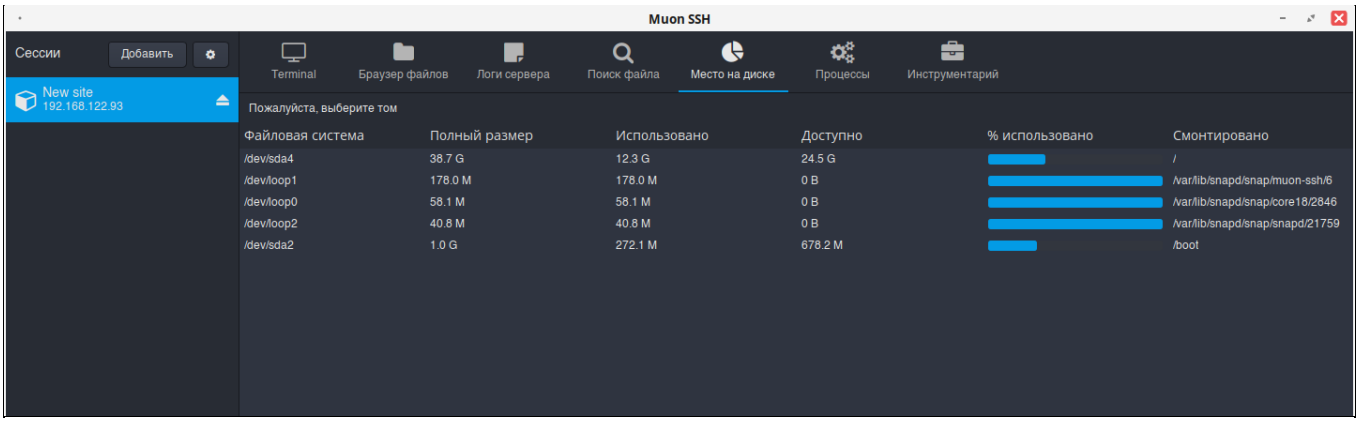


На вкладке «**Поиск файла**» доступен поиск файлов и каталогов с фильтрацией результатов поиска по различным критериям.

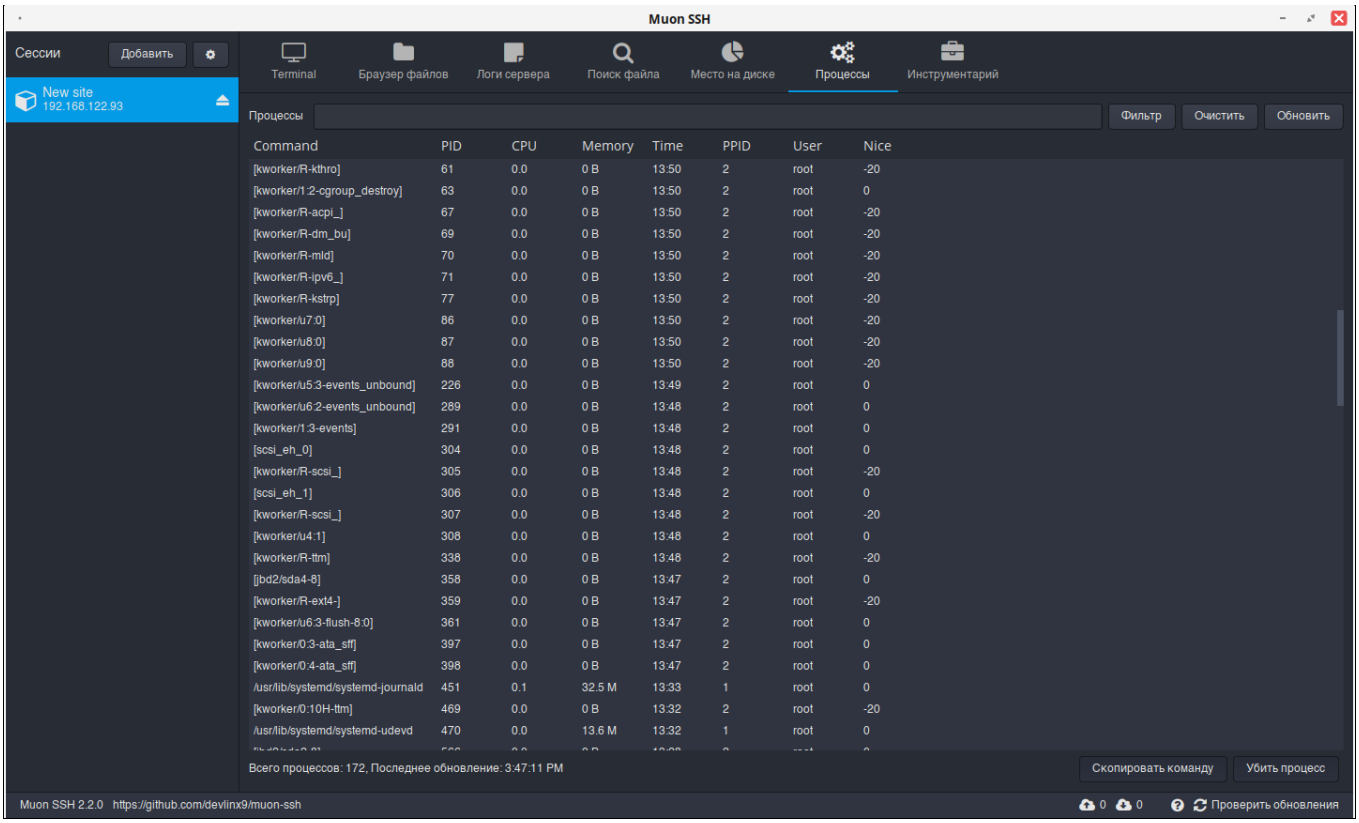


На вкладке «**Место на диске**» осуществляется оценка занятого дискового пространства. Доступен выбор анализа:

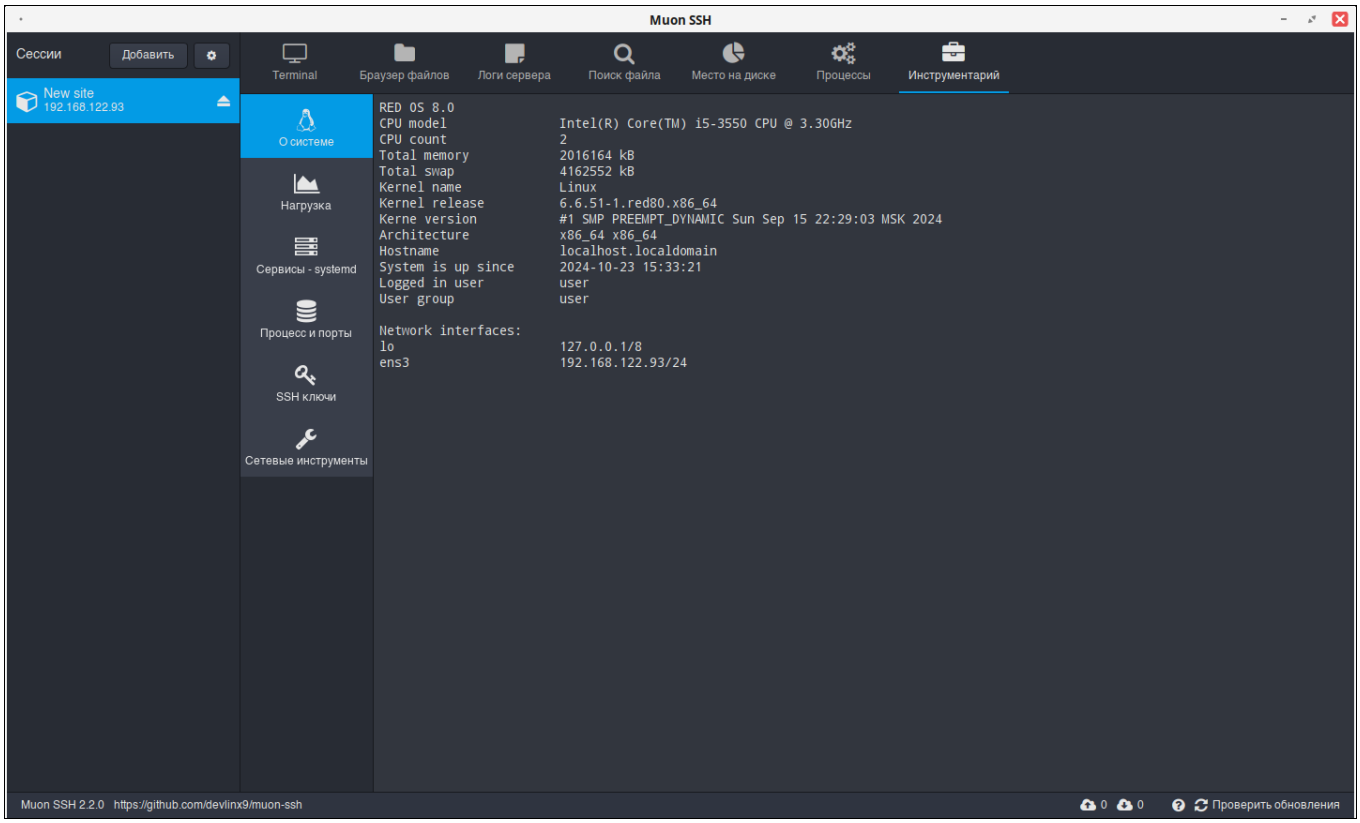
- анализировать том;
- анализировать папку.



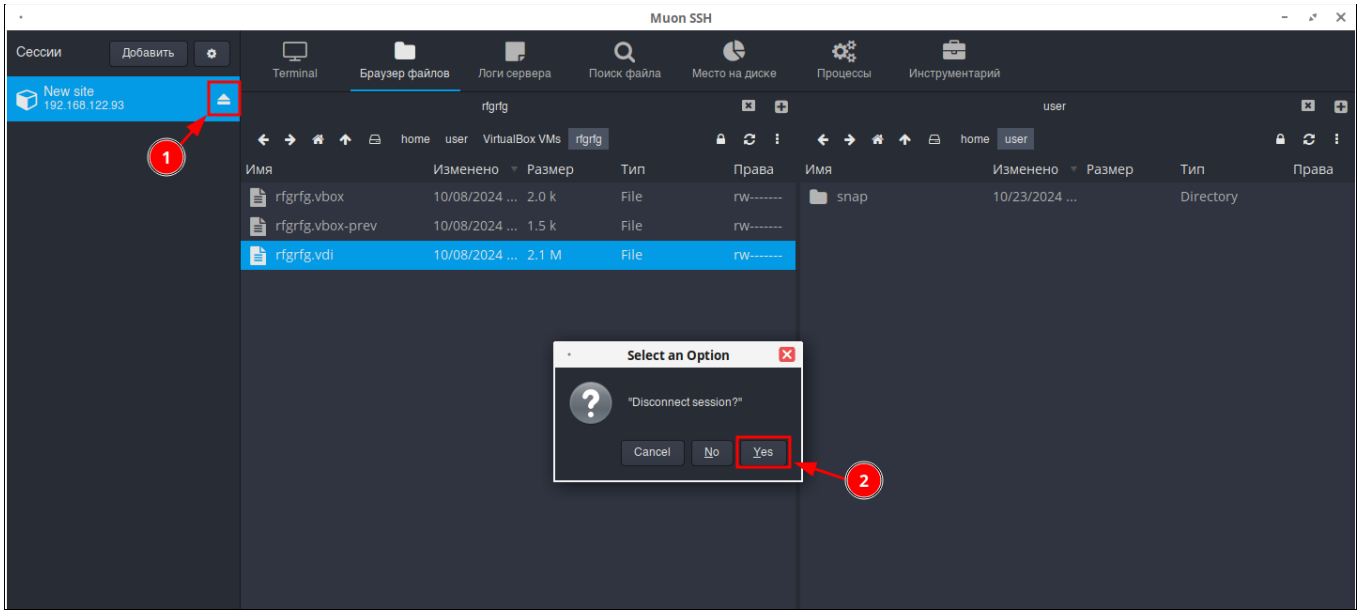
На вкладке «**Процессы**» отображается список запущенных на удаленном хосте процессов.



На вкладке «**Инструментарий**» выводится общая информация о хосте, системных службах, процессах и используемых ими портах, производится оценка нагрузки и пр.



Для отключения от сессии в списке установленных соединений нажмите кнопку  и в появившемся диалоге подтвердите завершение сессии.



Snowflake - графический SSH-клиент

Установка
Работа в программе
Возможности программы
Удаление программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: snowflake-1.0.4

Snowflake – современный SSH-клиент со встроенными графическими инструментами для простого управления серверами. **Snowflake** включает в себя менеджер соединений, файловый браузер, эмулятор терминала, диспетчер ресурсов/процессора, анализатор дискового пространства, текстовый редактор, просмотрщик журнала, поддержку аутентификации по ключу **SSH** и многие другие функции.

Просмотр файлов основан на протоколе **SFTP**, однако **Snowflake** может использовать консольные команды для эффективного выполнения операций. Например, удаление каталога с большим количеством файлов и подкаталогов может занять некоторое время при использовании **SFTP**, но с помощью команды `rm` процесс удаления производится намного быстрее.

Также **Snowflake** может выполнять операции с повышенными привилегиями (**sudo**). Для вызова **sudo** не требуется переключение на терминал.

Перемещение файлов между серверами можно осуществлять простым перетаскиванием.

Установка

Скачайте установочный файл командой:

```
wget https://github.com/subhra74/snowflake/releases/download/v1.0.4/snowflake-1.0.4-setup-amd64.bin
```

Затем предоставьте установочному файлу права на исполнение (потребуются права **администратора**):

```
sudo -E chmod +x ./snowflake-1.0.4-setup-amd64.bin
```

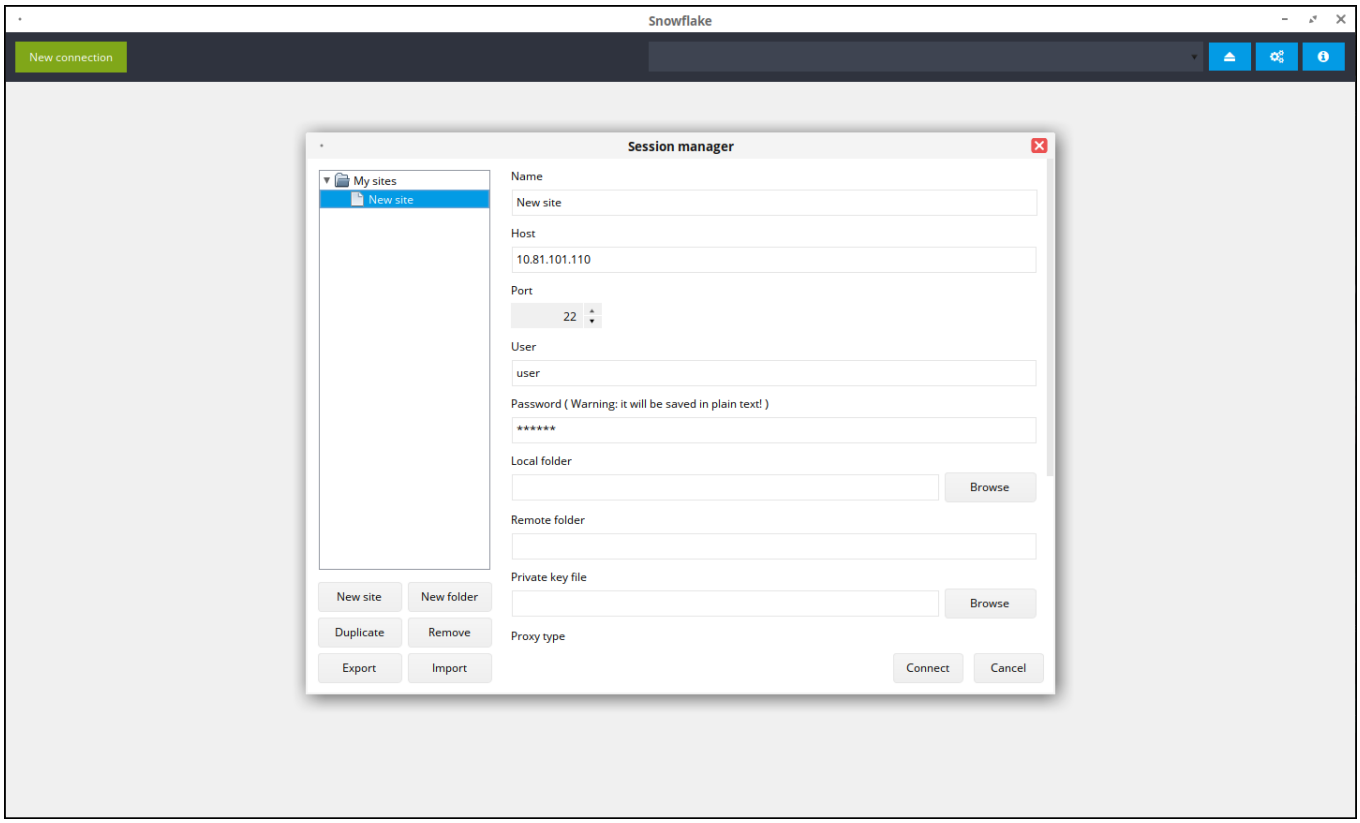
Запустите установку (потребуются права **администратора**):

```
sudo -E ./snowflake-1.0.4-setup-amd64.bin
```

После установки программа доступна из «**Главного меню**» – «**Прочие**» – «**Snowflake SSH Client**».

Работа в программе

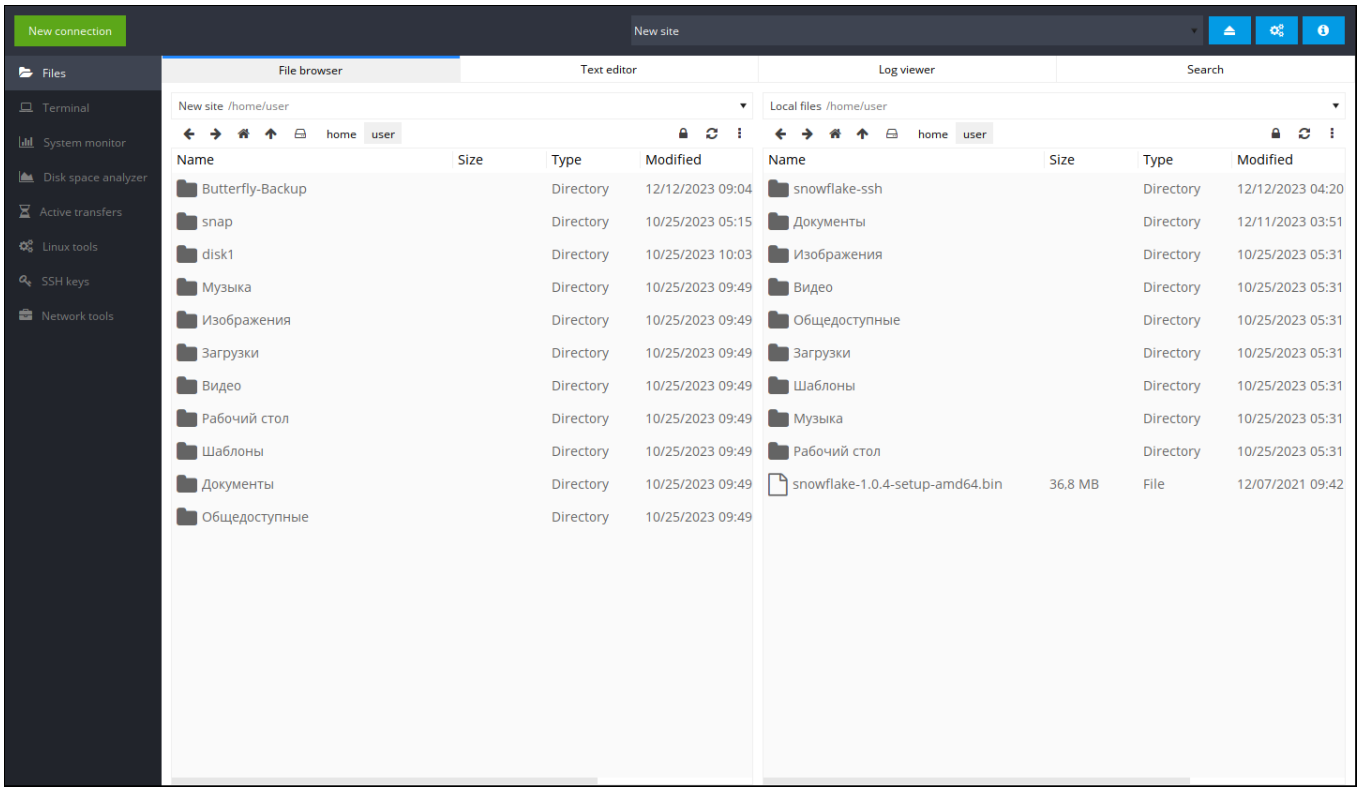
Для создания нового соединения нажмите «**New connection**». В открывшемся окне заполните данные удаленного сервера – IP-адрес, порт (по умолчанию 22), имя пользователя и пароль.



Для соединения с удаленным сервером нажмите «**Connect**».

После успешного соединения будет открыт файловый менеджер для удаленного сервера – слева, для локального – справа.

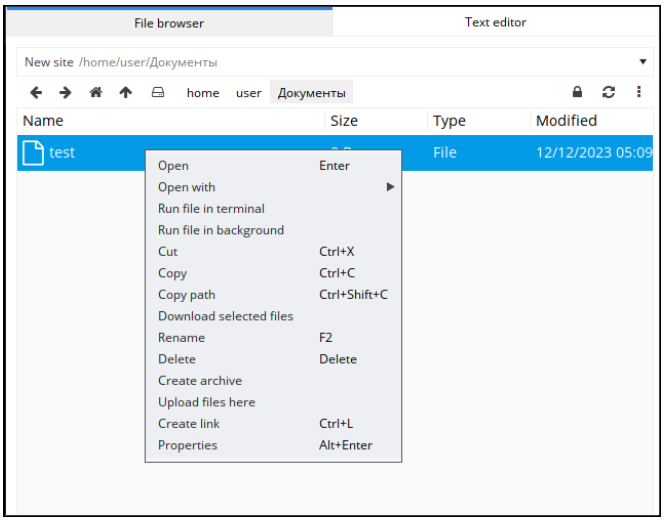
Интерфейс программы после установленного соединения выглядит следующим образом:



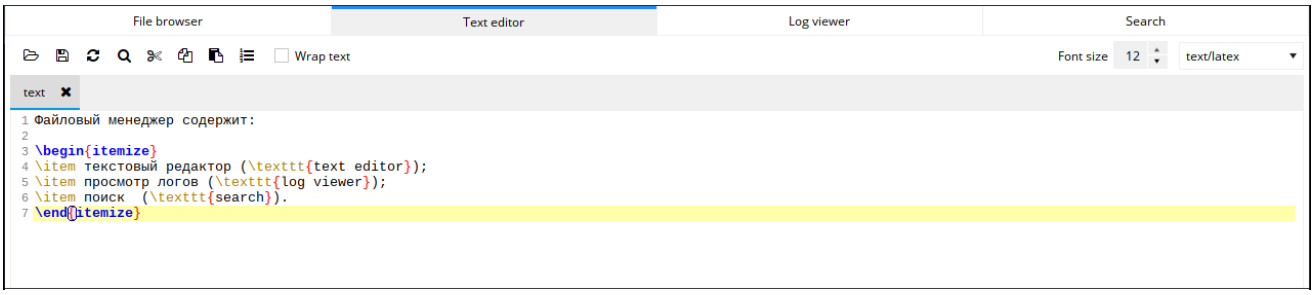
Файловый менеджер содержит текстовый редактор (*text editor*), просмотр логов (*log viewer*) и поиск (*search*).

Возможности программы

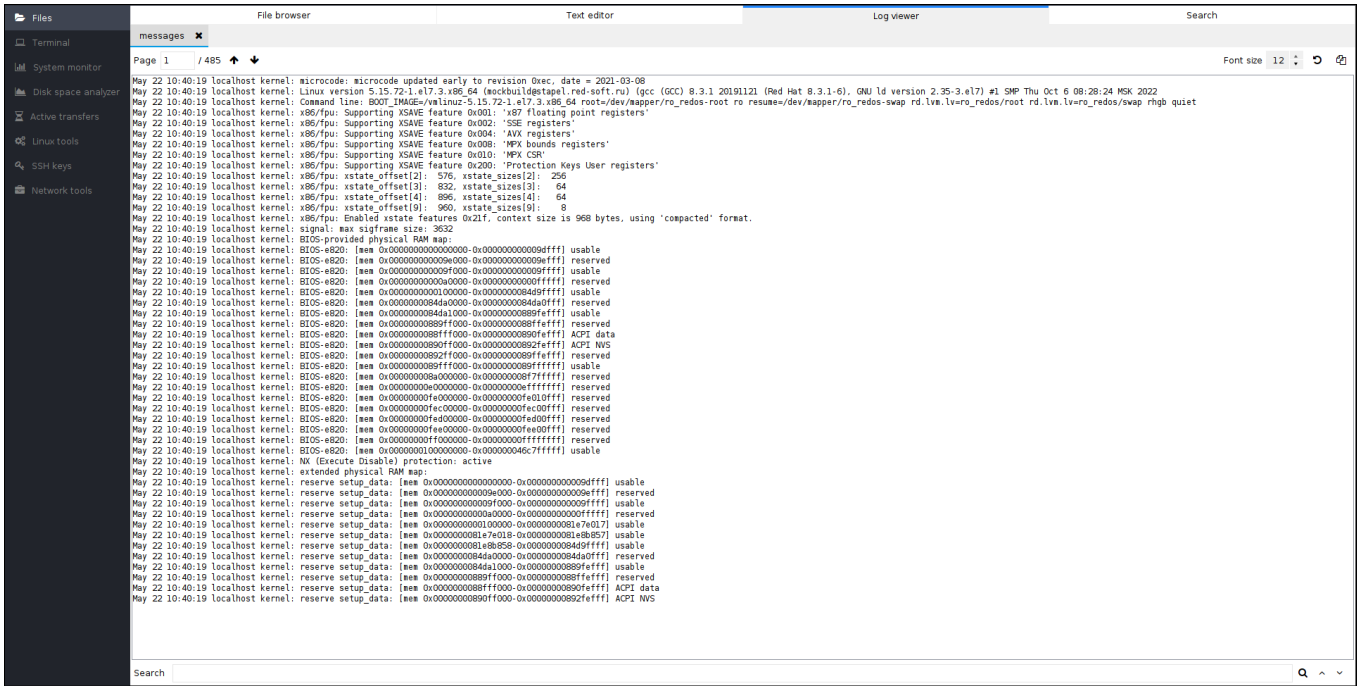
По нажатии ПКМ по какому-либо файлу вызывается контекстное меню для выбора действия – открыть, запустить в терминале, вырезать, скопировать, вставить, переименовать, удалить и пр.



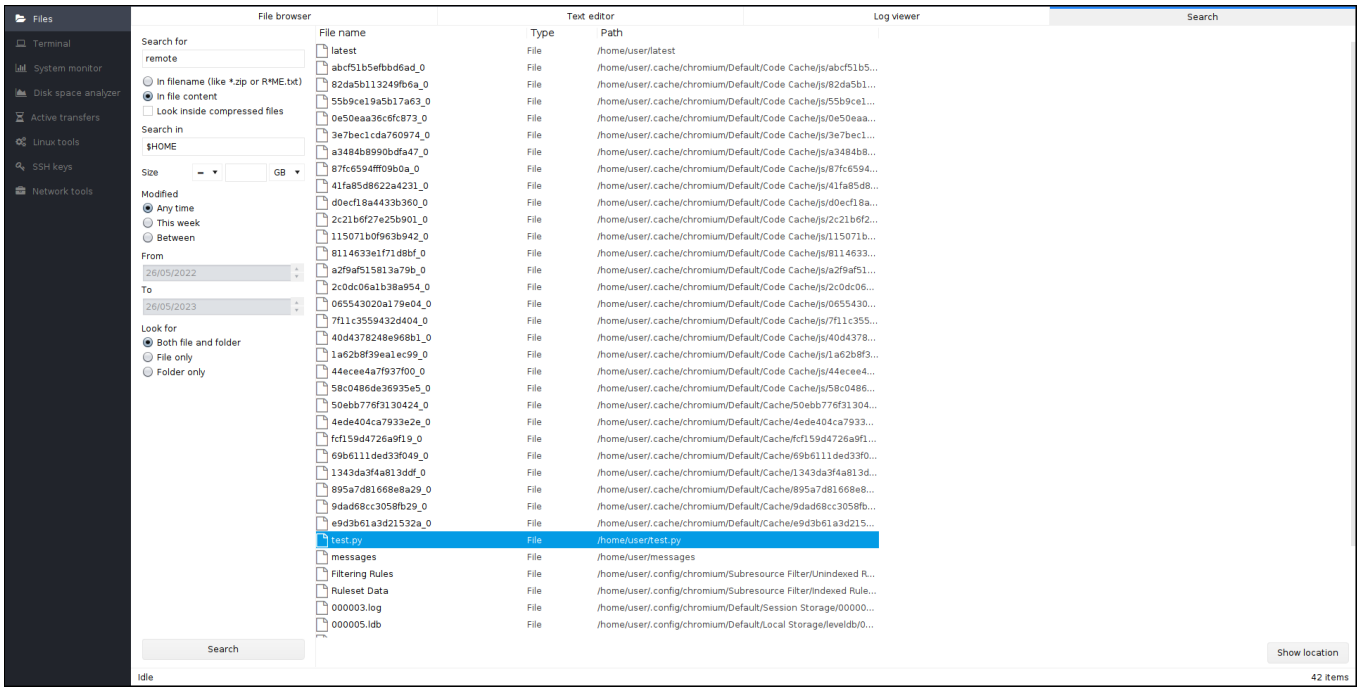
Текстовый редактор поддерживает подсветку синтаксиса, изменение размера шрифта текста, а также выбор среды программирования.



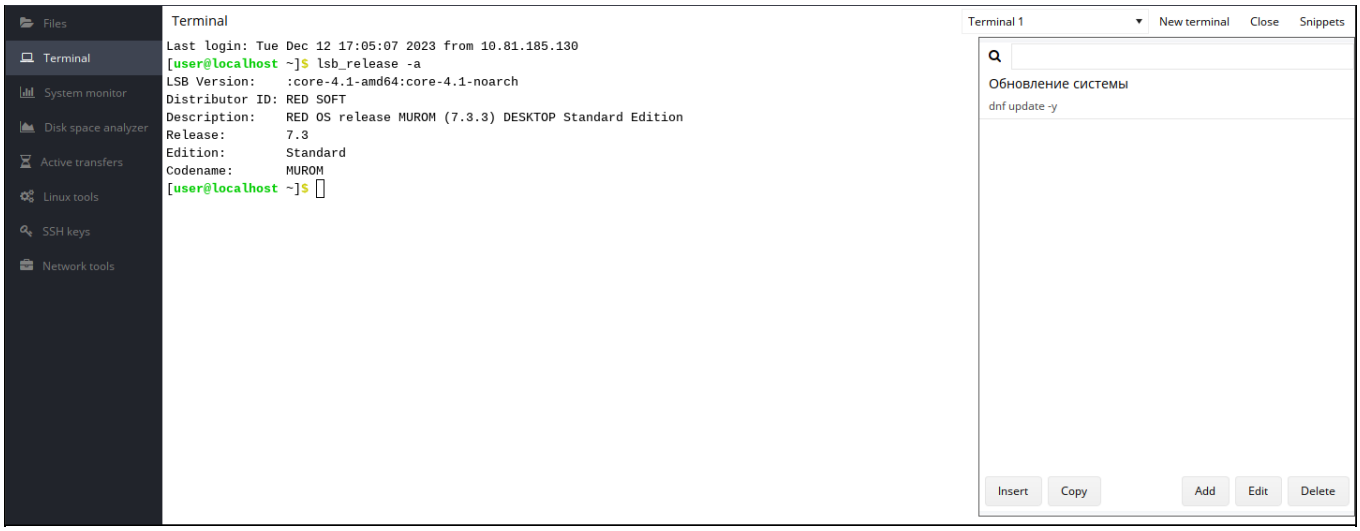
Просмотр системных журналов или больших текстовых файлов осуществляется через встроенный просмотрщик – **jiffy**.



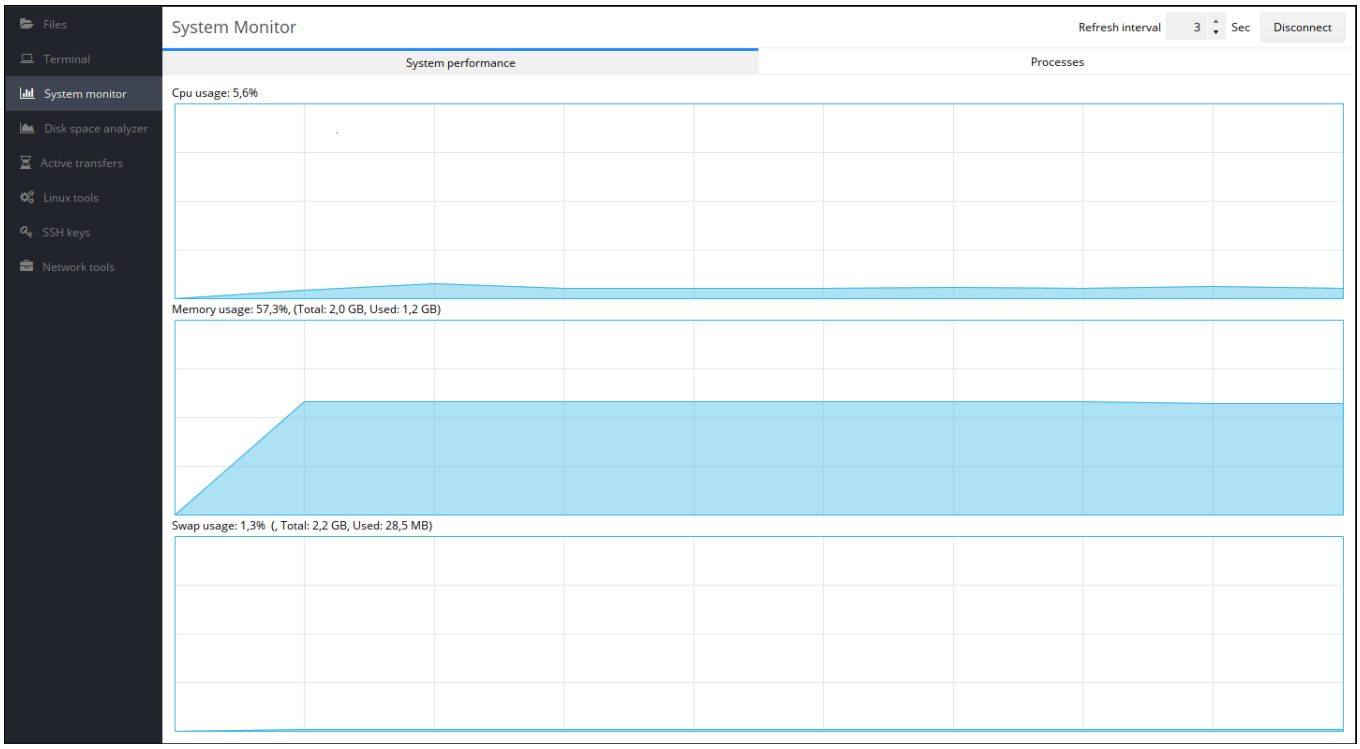
Быстрый поиск файлов основан на консольной команде find, поиск может также осуществляться в архивах **tar** и **zip**.



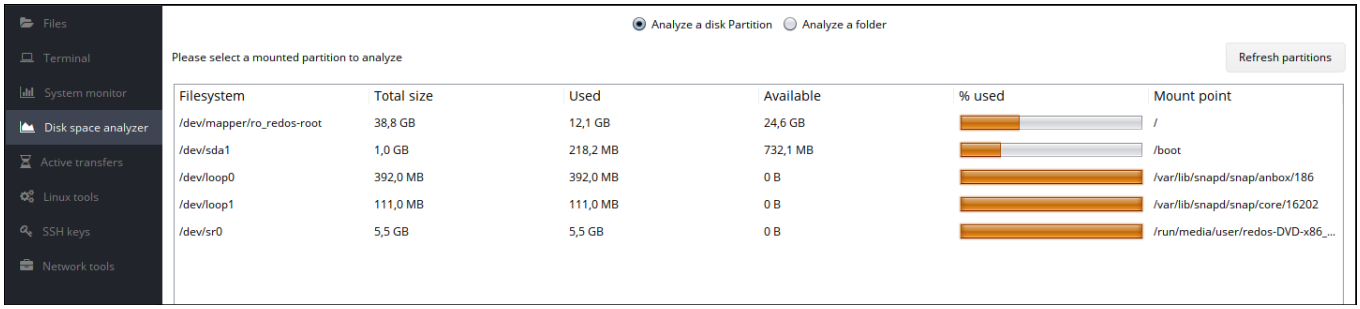
Во встроенном терминале поддерживаются *сниппеты*, с помощью которых можно сохранить часто используемые команды.



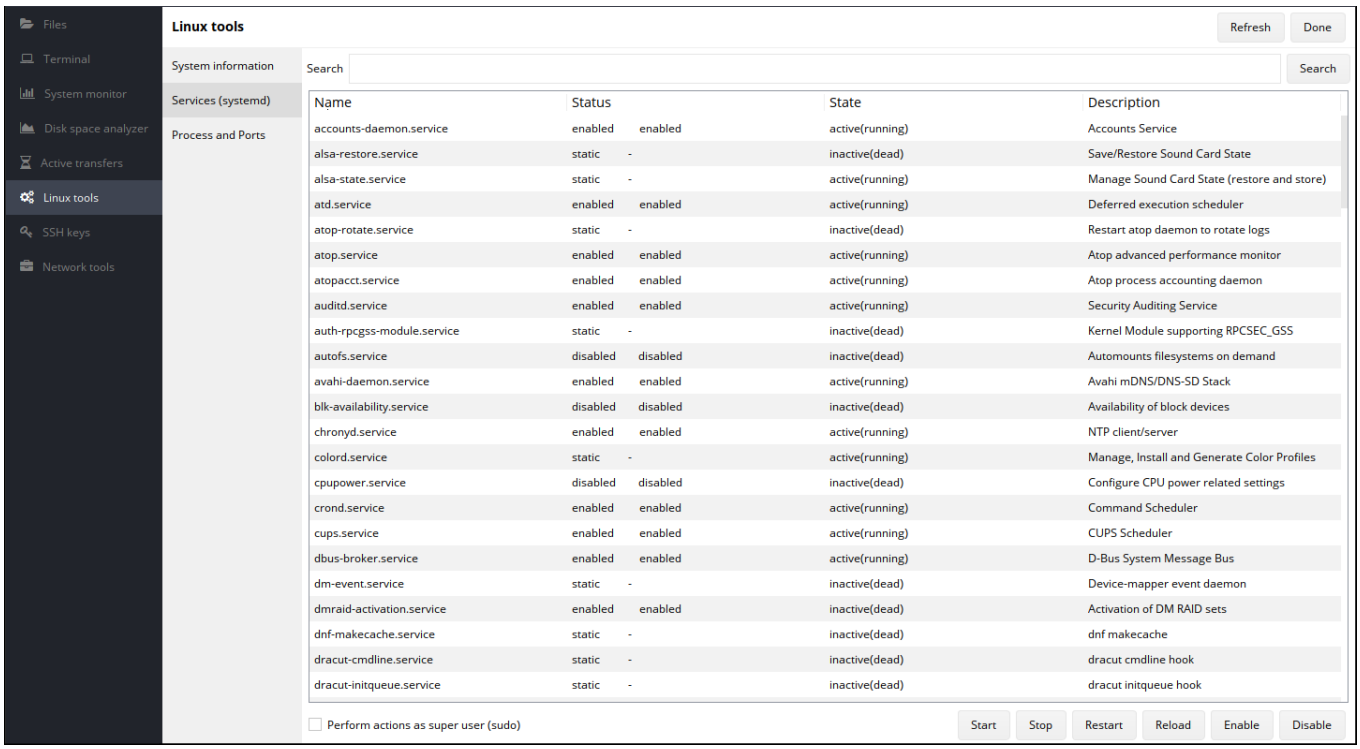
Доступен также системный монитор (аналог диспетчера задач), в котором нагрузка на процессор и использование памяти отображены в виде графика. Нагрузку по отдельным процессам можно просмотреть на вкладке **Processes**.



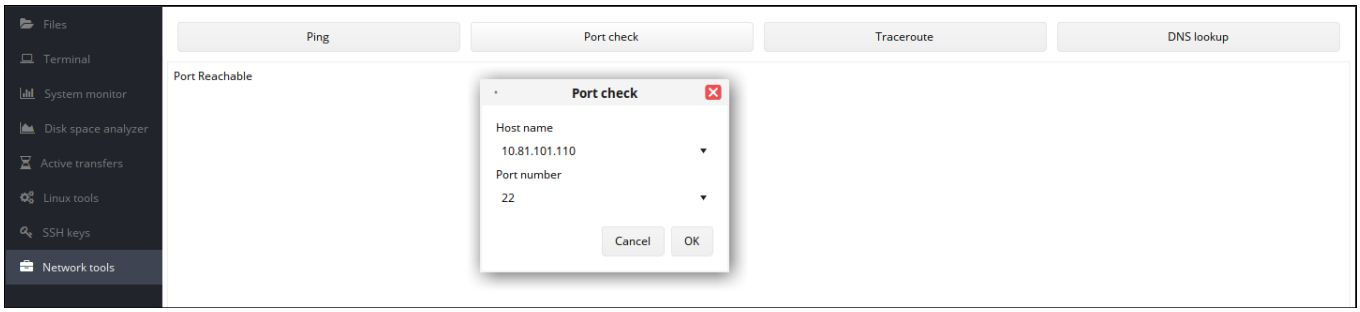
Встроенный графический анализатор места на диске показывает занятое и свободное дисковое пространство.



В разделе **Linux tools** можно получить информацию о системе, доступ к работе со службами **systemd**, а также проверить, какие порты используются процессами.



В сетевых настройках можно проверить целостность соединения с удаленным сервером, доступность портов удаленного сервера, определить сетевые маршруты, а также DNS-записи хостов.



В разделе **SSH keys** доступно управление ключами **SSH**.

Удаление программы

Для удаления **Snowflake** необходимо последовательно выполнить следующие команды (потребуются права суперпользователя **root** или **администратора** системы):

```
sudo rm -rf /opt/snowflake
sudo rm -rf /usr/bin/snowflake
sudo rm -rf /usr/share/applications/snowflake.desktop
rm -rf ~/snowflake-ssh
```

Создание SSH-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический, Сервер минимальный

Для включения поддержки шифрования ГОСТ в **openssl** необходимо установить пакеты **openssl-gost-engine** и **crypto-policies**.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install openssl-gost-engine crypto-policies
```

Более подробная информация о настройке ГОСТ в **openssl** доступна по ссылке .

Для установки пакетов **openssh-gost** необходимо выполнить следующие действия:

```
dnf swap openssh openssh-gost --allowerasing
dnf swap openssh-clients openssh-gost-clients --allowerasing
dnf swap openssh-server openssh-gost-server --allowerasing
```

Включить поддержку алгоритмов ГОСТ в **openssl** можно командой:

```
openssl-switch-config gost
```

После этого перезапустите сервис **sshd**:

```
systemctl restart sshd
```

Список поддерживаемых алгоритмов шифрования трафика можно посмотреть с помощью команды:

```
ssh -Q cipher

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
grasshopper-cbc@altlinux.org
grasshopper-ctr@altlinux.org
magma-cbc@altlinux.org
magma-ctr@altlinux.org
```

Для просмотра списка поддерживаемых **MAC** (коды аутентификации сообщений) выполните команду:

```
ssh -Q mac

hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
hmac-md5
hmac-md5-96
umac-64@openssh.com
umac-128@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
```

```
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
grasshopper-mac@altlinux.org
hmac-gostr3411-2012-256@altlinux.org
hmac-streebog-256@altlinux.org
hmac-gostr3411-2012-512@altlinux.org
hmac-streebog-512@altlinux.org
hmac-gostr3411-2012-256-etm@altlinux.org
hmac-streebog-256-etm@altlinux.org
hmac-gostr3411-2012-512-etm@altlinux.org
hmac-streebog-512-etm@altlinux.org
```

На клиенте для настройки также необходимо выполнить вышеуказанные действия.

Для подключения к серверу с использованием алгоритмов ГОСТ выполните команду:

```
ssh <пользователь>@<сервер> -oCiphers=grasshopper-ctr@altlinux.org -oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org
```

Пример подключения:

```
ssh user@192.168.1.92 -oCiphers=grasshopper-ctr@altlinux.org -oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org

The authenticity of host '192.168.1.92 (192.168.1.92)' can't be established.
ED25519 key fingerprint is SHA256:qUo//tqZCHfpp3QY9qEBqIxXcjT/8va13xGeREclvU8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.92' (ED25519) to the list of known hosts.
user@192.168.1.92's password: <пароль_сервера>
Last login: Thu Apr 21 09:47:30 2022
```

Для выхода из сессии выполните команду:

```
exit

выход
Connection to 192.168.1.92 closed.
```

Аутентификация по протоколу SSH с использованием RSA-ключа

Клиент SSH. Генерация RSA-ключа
Клиент SSH. Передача открытой части ключа на сервер
Клиент SSH. Установка ранее сгенерированного ключа
Сервер SSH. Отключение аутентификации по паролю

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openssh-9.3p1-5

Установка и настройка утилиты openssh подробно описаны нашей статье «Работа с клиентом и сервером SSH».

Использование ключа при аутентификации позволяет не только отказаться от обязательного ввода пароля при установке соединения, но и повысить защищенность соединения, автоматизировать процессы. Такие утилиты и протоколы как **scp**, **rsync**, **sftp**, которые при аутентификации ранее требовали ввода пароля, используя ключ, могут функционировать без участия пользователя.

Ключ состоит из двух частей – публичной и приватной. *Публичная часть* ключа может распространятся по открытым каналам без угрозы для безопасности соединения. *Приватная часть* должна быть защищена от несанкционированного доступа. В случае передачи приватной части ключа по незащищенным каналам или возможности несанкционированного доступа предусмотрена возможность парольной защиты ключа.

Общий принцип аутентификации с использованием ключа заключается в том, что при инициализации клиентом сеанса связи сервер шифрует открытой частью ключа случайное число и передает его клиенту. Если клиент обладает приватной частью, он сможет его расшифровать и, передав ответ обратно на сервер, подтвердить свою подлинность.

Клиент SSH. Генерация RSA-ключа

Для создания подключения с использованием ключа на стороне клиента (устройство, которое инициирует подключение) генерируется SSH-ключ, включающий в себя два файла – *приватную* и *публичную* части. *Публичная часть* ключа будет передана на сервер (устройство, с которым устанавливается связь).

Сгенерируйте ключ утилитой **ssh-keygen**:

```
ssh-keygen
```

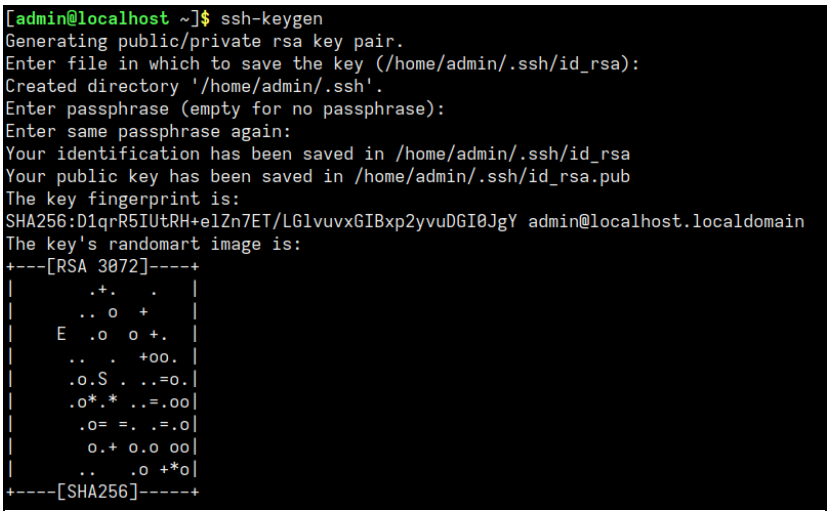
Утилита информирует о каталоге размещения сгенерированных ключей. Каталог можно изменить, указав другой путь (не рекомендуется):

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
```

Далее будет предложено установить пароль на ключ для защиты от несанкционированного доступа третьих лиц. Опция не является обязательной. Если оставить поле пустым, пароль не будет установлен:

```
Created directory '/home/admin/.ssh'.
Enter passphrase (empty for no passphrase):
```

После этого происходит генерация ключей. По завершении процесса генерации будут указаны каталоги хранения **id_rsa** (приватная часть ключа) и **id_rsa.pub** (публичная часть ключа).



Ключи успешно сгенерированы.

Клиент SSH. Передача открытой части ключа на сервер

ВАЖНО!

Обратите внимание, что при передаче ключа используется имя уже созданного на сервере пользователя. Если такого пользователя на сервере нет, его необходимо создать **до** передачи ключа. Также на сервере должна быть доступна аутентификация с применением пароля.

Открытую часть ключа передайте на сервер при помощи утилиты **ssh-copy-id** в формате вида:

```
ssh-copy-id -i <путь_до_ключа> <имя_пользователя>@<IP-адрес_сервера>
```

Например:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@192.168.100.61
```

При первом подключении к серверу будет предложено проверить отпечаток ключа ***fingerprint***. Для подтверждения наберите **yes**. Отпечаток ключа будет сохранен в файл **~/.ssh/known_hosts**.

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.100.61 (192.168.100.61)' can't be established.
ED25519 key fingerprint is SHA256:q3oeMFb4bpE4SMd39cH5QqShw3yFmMXi4Wh5VfS260g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Далее будет предложено ввести пароль пользователя, от имени которого производится подключение к серверу:

```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keysuser@192.168.100.61's
password: <пароль_пользователя>
```

После этого будет выведена информация о результатах передачи ключа:

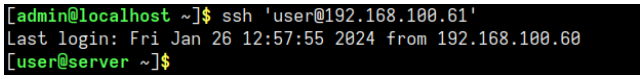
```
Number of key(s) added: 1
Now try logging into the machine, with:   "ssh 'user@192.168.100.61'"
and check to make sure that only the key(s) you wanted were added.
```

Выполните проверку подключения к серверу с помощью команды вида:

```
ssh <имя_пользователя>@<IP-адрес_сервера>
```

Например:

```
ssh user@192.168.100.61
```



Обратите внимание на *имя пользователя* и *имя хоста* в командной строке. Если параметры изменились и соответствуют параметрам подключения, аутентификация прошла удачно.

Настройка подключения завершена.

ВАЖНО!

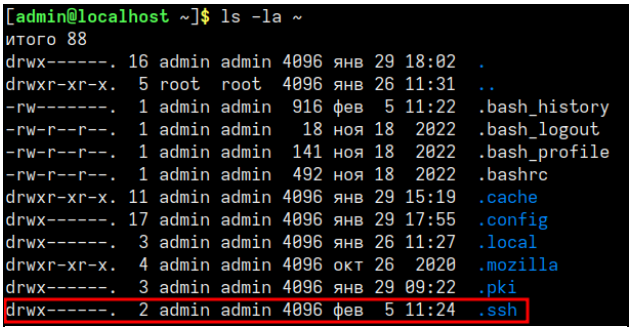
Обратите внимание, что настройка аутентификации с применением RSA-ключа не отключает возможность аутентификации по паролю. По умолчанию аутентификация с применением RSA-ключа имеет более высокий приоритет. В случае утраты ключа или несоответствия параметров, при подключении будет предложено пройти аутентификацию с использованием пароля.

Если аутентификацию с использованием пароля требуется отключить, необходимо изменить конфигурацию на стороне сервера. Подробнее об отключении аутентификации с использованием пароля см. в пункте «Сервер SSH. Отключение аутентификации по паролю».

Клиент SSH. Установка ранее сгенерированного ключа

При установке ранее сгенерированного ключа необходимо убедиться в наличии каталога **/.ssh** в домашнем каталоге и правах доступа к этому каталогу. Для этого выполните:

```
ls -la ~
```



ВАЖНО!

Обратите внимание на права доступа `drwx------` к каталогу **/.ssh**. В случае предоставления прав доступа группе или другим пользователям при попытке подключения к серверу в авторизации будет отказано.

Если каталога **/.ssh** не существует, его необходимо создать:

```
mkdir ~/.ssh
```

и предоставить необходимые права:

```
chmod 700 ~/.ssh
```

После этого полученный ключ необходимо разместить в каталоге **/.ssh**.

Сервер SSH. Отключение аутентификации по паролю

Для отключения аутентификации по паролю на сервере необходимо внести изменения в файл конфигурации SSH-сервера – **/etc/ssh/sshd_config**. Откройте файл конфигурации (потребуются права **администратора**):

```
sudo nano /etc/ssh/sshd_config
```

Найдите и раскомментируйте параметр `PasswordAuthentication`. Установите для него значение `no`.

Сохраните изменения и закройте файл.

Для применения внесенных изменений обновите конфигурацию службы командой:

```
sudo systemctl reload sshd.service
```

Аутентификация по паролю отключена.

Установка и настройка xrdp-сервера в РЕД ОС 8

Установка и настройка xrdp-сервера
Включение возможности запуска нового сеанса пользователя и устранение ошибки «Could not acquire name on session bus»

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: xrdp-1:0.10.1-1, xorgxrdp-0.10.2-1, pipewire-module-xrdp-0~git19-1

Вы можете подробнее ознакомиться с возможностью осуществления удаленного подключения **на примере РЕД ОС 7.3**, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows;
- в **VK Видео** — Организация удаленного доступа с РЕД ОС на Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и настройка xrdp-сервера

Перед установкой и настройкой сервера необходимо предварительно перейти в сеанс пользователя **root**:

```
su -
```

Дальнейшие указанные действия должны выполняться с правами пользователя **root** или **администратора** системы, если не указано иное.

1. Установите сервер **xrdp** командой:

```
dnf install xrdp xorgxrdp pipewire-module-xrdp
```

2. Настройте предпочитаемую графическую оболочку.

ВАЖНО!

В РЕД ОС 8 не рекомендуется использовать несколько графических оболочек на одной рабочей машине из-за возможности возникновения конфликтов пакетов. Такие конфликты могут вызвать сбои в работе системы, и некоторые функции могут стать для пользователя недоступны.

Создайте файл настроек рабочего стола:

```
nano /etc/sysconfig/desktop
```

и внесите соответствующие настройки для предпочитаемой графической оболочки:

- для **MATE**:

```
DESKTOP=MATE
```

- для **GNOME**:

```
DESKTOP=GNOME
```

- для **KDE**:

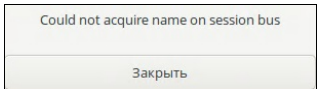
```
DESKTOP=KDE
```

3. Запустите сервер **xrdp** и добавьте его в автозапуск:

```
systemctl enable xrdp --now
```

Включение возможности запуска нового сеанса пользователя и устранение ошибки «Could not acquire name on session bus»

После авторизации пользователя при удаленном подключении к xrdp-серверу с графической оболочкой **MATE** возникает ошибка **"Could not acquire name on session bus"**.

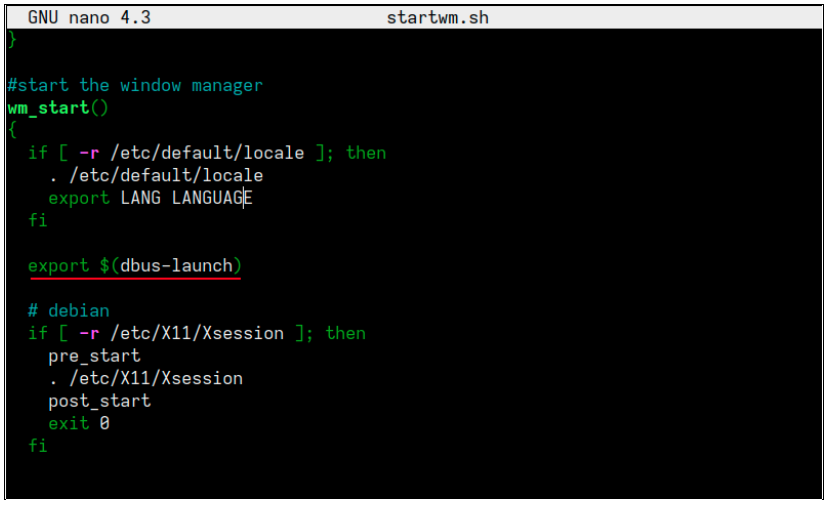


GNOME — ошибка проявляется отключением **RDP** при попытке авторизации пользователя.

KDE — после авторизации сеанс пользователя не загружается.

Для устранения данной ошибки в скрипте **/usr/libexec/xrdp/startwm.sh** в функции **wm_start** добавьте строку:

```
export $(dbus-launch)
```



после сохранения изменений перезапустите сервис **xrdp** командой в терминале:

```
systemctl restart xrdp
```

Дополнительная настройка xrdp-сервера

Проброс локального диска и принтера при подключении из Windows
Подключение на клиенте
Устранение ошибки при настройке удаленного доступа с Windows 7/XP на РЕД ОС
Аутентификация под доменным пользователем
Дополнительная настройка SELinux
Завершение всех процессов при выходе из сеанса
Оптимизация производительности
Автоматическое завершение сеанса пользователя, подключенного по xrdp
Автоматическое завершение всех графических сеансов пользователя

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с возможностью осуществления удаленного подключения **на примере РЕД ОС 7.3**, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows;
- в **VK Видео** — Организация удаленного доступа с РЕД ОС на Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Проброс локального диска и принтера при подключении из Windows

Для успешного подключения локального диска к удаленному рабочему столу необходимо убрать в настройках RDP-клиента галочку «**Принтеры**».

Проброс локального принтера текущей версией xrdp не поддерживается.

Подключение на клиенте

Для подключения из Windows используйте «**Подключение к удаленному рабочему столу**».

Для подключения из РЕД ОС используйте приложение «**Remmina**» («Главное меню» — «Интернет» — «Remmina»).

Выберите протокол **RDP**, впишите узел и нажмите клавишу **Enter**, чтобы подключиться.

Для подключения в открывшемся окне впишите имя пользователя и пароль.

Для применения настроек перезагрузите сервер **xrdp**:

```
systemctl restart xrdp
```

Устранение ошибки при настройке удаленного доступа с Windows 7/XP на РЕД ОС

При возникновении ошибки такого вида:



Откройте файл:

```
nano /etc/xrdp/xrdp.ini
```

Измените значение параметра *security_layer*:

```
security_layer=rdp
```

Для применения настроек перезагрузите сервер **xrdp**:

```
systemctl restart xrdp
```

Аутентификация под доменным пользователем

Для разрешения аутентификации доменных пользователей требуется изменить файл:

```
nano /etc/xrdp/sesman.ini
```

Закомментировав следующие строки:

```
#TerminalServerUsers=tsusers
#TerminalServerAdmins=tsadmins
```

Перезапустите сервер:

```
systemctl restart xrdp
```

Чтобы разрешить определенным доменным пользователям доступ к RDP-серверу, необходимо создать локальную в группу **tsusers** и добавить в нее доменных пользователей.

```
groupadd tsusers
```

Добавление в группу **tsusers** пользователя <**bob**> производится командой:

```
usermod -aG tsusers bob
```

где <**bob**> - это доменный пользователь,

В файл **/etc/xrdp/sesman.ini** в секцию `[Security]` необходимо добавить строки:

```
TerminalServerUsers=tsusers
AlwaysGroupCheck=true
```

Еще один вариант - в качестве локальной группы указать доменную:

```
TerminalServerUsers=rdp
```

здесь **rdp** - группа безопасности на вашем контроллере домена, в которую могут входить необходимые вам пользователи **xrdp**-сервера.

После этого перезапустите сервер:

```
systemctl restart xrdp
systemctl restart sssd
```

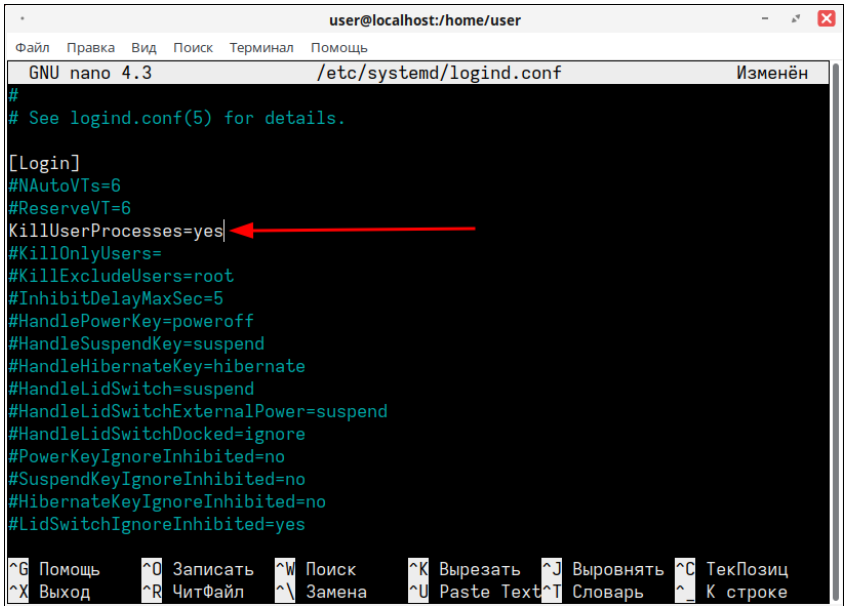
Дополнительная настройка SELinux

После тестового подключения к xrdp-серверу нужно выполнить настройку SELinux, выполните следующие команды на сервере:

```
ausearch -c 'krb5_child' --raw | audit2allow -M my-krb5child
semodule -X 300 -i my-krb5child.pp
```

Завершение всех процессов при выходе из сеанса

Для того чтобы при выходе из системы прекращались все процессы, явно или неявно запущенные от имени авторизованного пользователя, в файле **/etc/systemd/logind.conf** необходимо раскомментировать параметр KillUserProcesses и установить значение yes.



После изменения значения данного параметра необходимо либо перезагрузить компьютер, либо выполнить команду перезапуска сервиса **logind** для применения настроек:

```
systemctl restart systemd-logind
```

Оптимизация производительности

Оптимизацию использования ресурсов RDP-сервера (процессора, оперативной памяти, каналов связи) можно произвести представленными ниже изменениями конфигурации.

- при использовании **MATE**:

Для отключения композитного менеджера путем задания значения по умолчанию параметра dconf следует создать файл **/etc/dconf/db/local.d/10_mate_nocomp** со следующим содержимым (с правами пользователя **root**):

```
nano /etc/dconf/db/local.d/10_mate_nocomp
```

```
[org/mate/marco/general]
 compositing-manager=false
```

Для того чтобы ограничить возможность изменения данного параметра пользователем, то есть принудительно применить настройку, следует выполнить команду:

```
echo "/org/mate/marco/general/compositing-manager" > /etc/dconf/db/local.d/locks/10_mate_nocomp
```

Для включения композитного менеджера измените значение параметра compositing-manager с false на true.

- при использовании **KDE**:

Для отключения композитного менеджера выполните в терминале команду:

```
qdbus org.kde.KWin /Compositor suspend
```

Включить снова композитный менеджер можно с помощью команды:

```
qdbus org.kde.KWin /Compositor resume
```

- при использовании **GNOME**:

Для оптимизации производительности отключение композитного менеджера не предусмотрено.

Автоматическое завершение сеанса пользователя, подключенного по xrdp

Данный вариант подойдет для решения ситуаций, когда после удаленного входа пользователь не может войти в сеанс на локальном компьютере.

Для автоматического завершения xrdp-подключения с завершением графического сеанса пользователя в файле **/etc/xrdp/sesman.ini** раскомментируйте и укажите параметры:

```
KillDisconnected=true
 DisconnectedTimeLimit=60
 IdleTimeLimit=600
```

В этом примере конфигурационного файла RDP-соединение отключится через 10 минут (600 секунд) неактивности, с завершением сеанса пользователя через 60 секунд после отключения.

KillDisconnected - [true|false] Включение функции принудительного завершения сеанса пользователя, после отключения RDP. Данная настройка работает только для xorgxrdp-сессий.

DisconnectedTimeLimit - Время в секундах, через которое будет завершен сеанс пользователя, после отключения RDP-соединения. Минимальное значение 60. При указании меньшего, значение будет равно 60.

IdleTimeLimit - Время в секундах, через которое будет будет отключено неактивное RDP-соединение. Под неактивностью понимается отсутствие ввода с клавиатуры, отсутствие движения/нажатий мыши. Если указано 0 - неактивное соединение не отключается. Данная настройка работает только для xorgxrdp сессий.

Автоматическое завершение всех графических сеансов пользователя

Данный вариант завершает все графические сеансы пользователей, которые неактивны указанное время. Решает проблему, когда незавершенный сеанс на локальном компьютере не позволяет подключиться этому пользователю по xrdp удаленно.

Создайте скрипт:

```
nano /opt/logout.sh
```

Сделайте его исполняемым:

```
chmod +x /opt/logout.sh
```

Содержание скрипта:

```
#!/bin/bash
idle_time=30 # Время в минутах бездействия в сессии пользователя, после которого сессия будет завершена (Указать необходимое)
while true; do
# Время бездействия пользователя в миллисекундах
user_time=$(xprintidle)
if [ $user_time -ge $((idle_time*60*1000)) ]; then
# Завершаем сеанс пользователя
loginctl kill-user "$USER"
fi
sleep 1
done
```

Создайте файл автозапуска скрипта **/opt/logout.sh**:

```
nano /etc/xdg/autostart/logout.desktop
```

Содержание файла **/etc/xdg/autostart/logout.desktop**:

```
[Desktop Entry]
 Type=Application
```

```
Exec=/opt/logout.sh
Hidden=false
Name=MyLogout
```

Установка и настройка TigerVNC

Установка
Предварительная настройка
Настройка файла конфигурации
Подключение к серверу tigerVNC

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Графический сервер
- **Версия ПО**: tigervnc-server-1.13.1

TigerVNC-сервер – это программный пакет, который позволяет запускать сервер **XVNC**, а также параллельные сеансы различных окружений рабочего стола, таких как **MATE**, **GNOME** и т. д. по протоколу **VNC**.

Вы можете подробнее ознакомиться с установкой и настройкой **Tigervnc** для удаленного подключения, просмотрев наши обучающие видео:

- на **RuTube**:
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.
- в **Яндекс.Дзен:**
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.
- в **VK Видео:**
  - Организация удаленного доступа с РЕД ОС на РЕД ОС при помощи VNC;
  - Организация удаленного доступа с Windows на РЕД ОС при помощи VNC.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки сервера **tigervnc** перейдите в сеанс суперпользователя **root**:

```
su -
```

и выполните команду:

```
dnf install tigervnc-server
```

Предварительная настройка

Примечание.

Для подключения к серверу через **VNC** *не рекомендуется* использовать учетную запись суперпользователя **root**, поскольку это *небезопасно*. Кроме того, некоторые функции могут работать некорректно.

Создайте обычного пользователя для подключения к серверу **VNC** и задайте для него пароль, добавьте пользователя в группу **wheel** для назначения ему привилегий администратора (**sudo**):

```
adduser <имя_пользователя>
passwd <имя_пользователя>
usermod -aG wheel <имя_пользователя>
```

Для подключения также можно использовать существующего пользователя, имеющего права администратора.

Настройка файла конфигурации

Далее необходимо назначить для каждого пользователя индивидуальный порт для подключения. Для этого откройте файл конфигурации **vncserver.users**:

```
nano /etc/tigervnc/vncserver.users
```

В конец файла добавьте строку вида:

```
:<номер_рабочего_стола>=<имя_пользователя>
```

Например:

```
# TigerVNC User assignment
#
# This file assigns users to specific VNC display numbers.
# The syntax is =. E.g.:
#
# :2=andrew
# :3=lisa

:2=test_user
```

здесь:

- :2 – номер рабочего стола для подключения. По умолчанию каждый рабочий стол отображается на порте **5900** + **номер рабочего стола**. То есть рабочий стол **:2** будет доступен через порт **5902**. Порт для каждого пользователя должен быть уникальным;
- test_user – имя пользователя с правами администратора для подключения к серверу **VNC**.

Затем откройте файл конфигурации по умолчанию:

```
nano /etc/tigervnc/vncserver-config-defaults
```

И укажите используемую по умолчанию графическую оболочку для подключения к серверу **VNC**. Например:

```
session=mate
```

Также установить графическую оболочку по умолчанию для пользователя, под которым будет производиться подключение к серверу, можно, указав имя сессии в файле в домашней директории этого пользователя **~/.vnc/config**. Например:

```
nano /home/test_user/.vnc/config
```

```
session=mate
```

Перейдите в сеанс пользователя, под которым будет производиться подключение к серверу **VNC**:

```
su - <имя_пользователя>
```

Установите пароль для пользователя сервера **TigerVNC**:

```
vncpasswd
```

Обратите внимание, что пароль должен иметь длину **не менее 6 символов**.

> **Примечание.**
>
> При запросе установки пароля только для просмотра нажмите **n**. При нажатии **y** управление сервером будет заблокировано.

Запустите службу **vncserver** и добавьте ее в автозагрузку:

```
systemctl enable --now vncserver@:2
```

здесь:

- `:2` – номер порта для подключения к серверу пользователя **test_user**, для каждого пользователя номер порта уникален.

Подключение к серверу tigerVNC

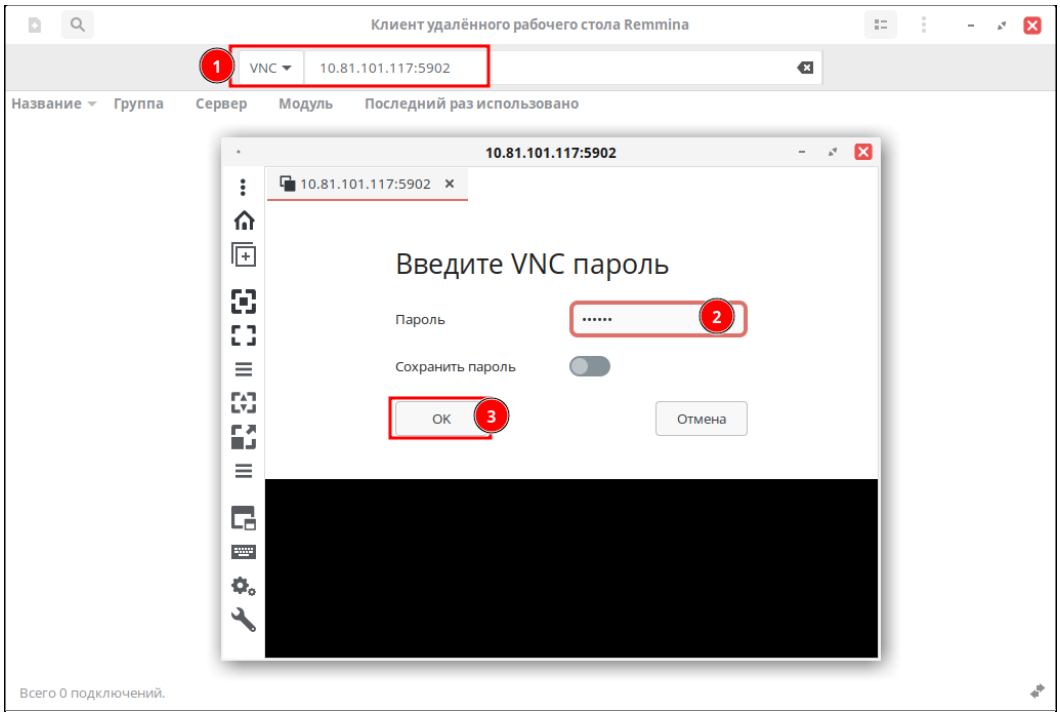
Для подключения можно использовать любое клиентское приложение **VNC**, например, **Remmina** Выберите протокол подключения – **VNC**, введите общедоступный *IP-адрес сервера* и *номер порта*, по которому будет производиться подключение (в примере используется порт **5902** для пользователя **test_user**).

ВАЖНО!

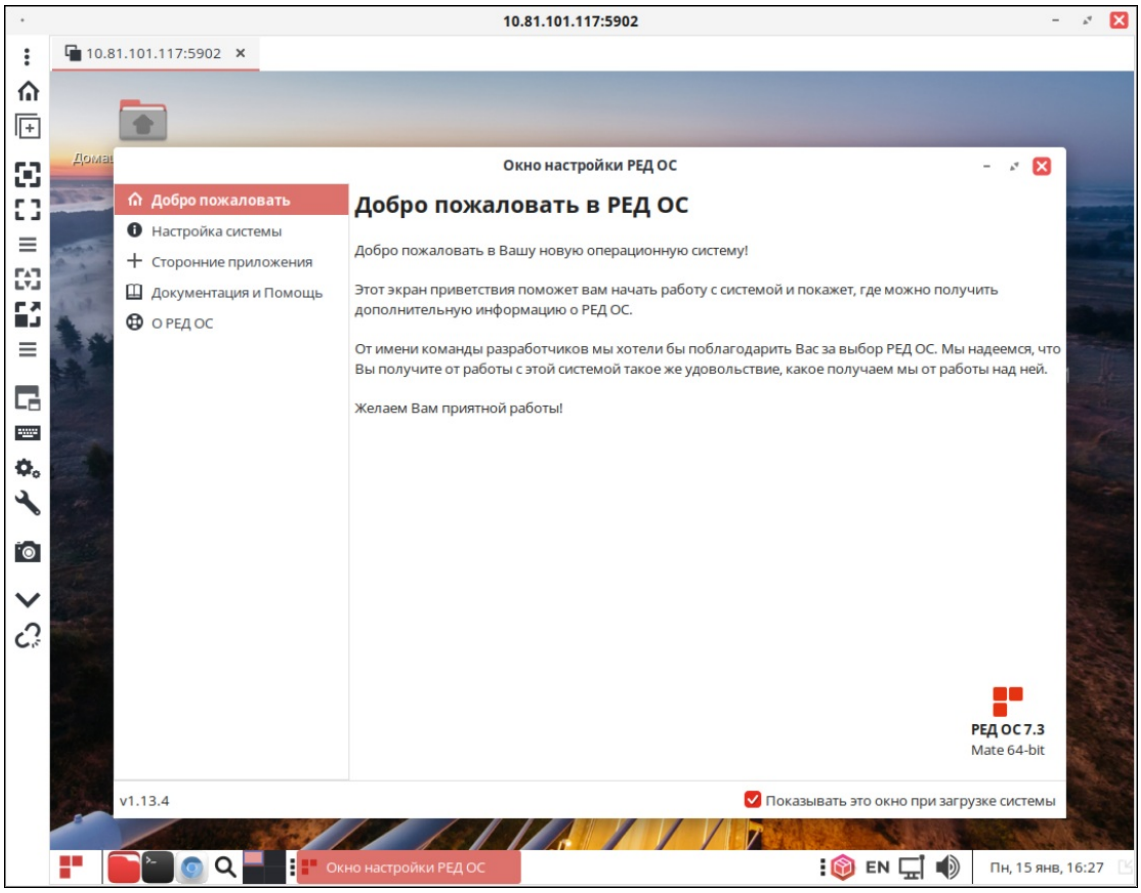
При вводе IP-адреса сервера важно правильно указать порт для подключения. В рассматриваемом примере запись будет выглядеть следующим образом:

```
10.81.101.117:5902
```

Введите пароль пользователя сервера **VNC**, который был создан ранее (см. пункт «Предварительная настройка»). После этого будет выполнено подключение к серверу и отображен удаленный рабочий стол.



Подключение к серверу прошло успешно.


10.81.101.117:5902
10.81.101.117:5902
Окно настройки РЕД ОС
Добро пожаловать
Настройка системы
Сторонние приложения
Документация и Помощь
О РЕД ОС
Добро пожаловать в РЕД ОС
Добро пожаловать в Вашу новую операционную систему!
Этот экран приветствия поможет вам начать работу с системой и покажет, где можно получить дополнительную информацию о РЕД ОС.
От имени команды разработчиков мы хотели бы поблагодарить Вас за выбор РЕД ОС. Мы надеемся, что Вы получите от работы с этой системой такое же удовольствие, какое получаем мы от работы над ней.
Желаем Вам приятной работы!
РЕД ОС 7.3
Mate 64-bit
v1.13.4
Показывать это окно при загрузке системы
Окно настройки РЕД ОС
EN
Пн, 15 янв, 16:27

Настройка X2GO

Установка x2go
Настройка клиента
Обзор клиента
Запуск определенного приложения
Проброс принтеров
Настройка трансляции токенов в сессию сервера
Завершение сессий x2go
X2Go Broker

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: x2goagent-4.1.0.3-16, x2goserver-4.1.0.3-16, x2goclient-4.1.2.2-7

X2Go — это программное обеспечение для удаленного рабочего стола с открытым исходным кодом, использующее модифицированный протокол **NX 3**. **X2Go** предоставляет удаленный доступ к графическому пользовательскому интерфейсу системы.

В данной статье раскрываются основные моменты по настройке данного варианта удаленного подключения, однако вы так же можете обратиться к официальной документации.

ВАЖНО!

Обратите внимание, что удаленные подключения посредством **x2go** к *типам сессий* **KDE 5 и выше**, **GNOME 3.12 и выше** НЕ поддерживаются!

Удаленные подключения к типу сессии **MATE** производятся корректно.

Вы можете подробнее ознакомиться с организацией удаленного доступа, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с помощью x2go. Проброс принтеров, трансляция токенов;
- в **Яндекс.Дзен** — Организация удаленного доступа с помощью x2go. Проброс принтеров, трансляция токенов;
- в **VK Видео** — Организация удаленного доступа с помощью x2go. Проброс принтеров, трансляция токенов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка x2go

Для установки **x2go** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install x2goserver-xsession x2goserver-fmbindings x2goserver-common x2goserver x2goagent x2goserver-desktopsharing
```

Здесь и далее команды будут выполняться от пользователя **root**, если не указано иное.

Для установки **x2go** на клиенте выполните команду:

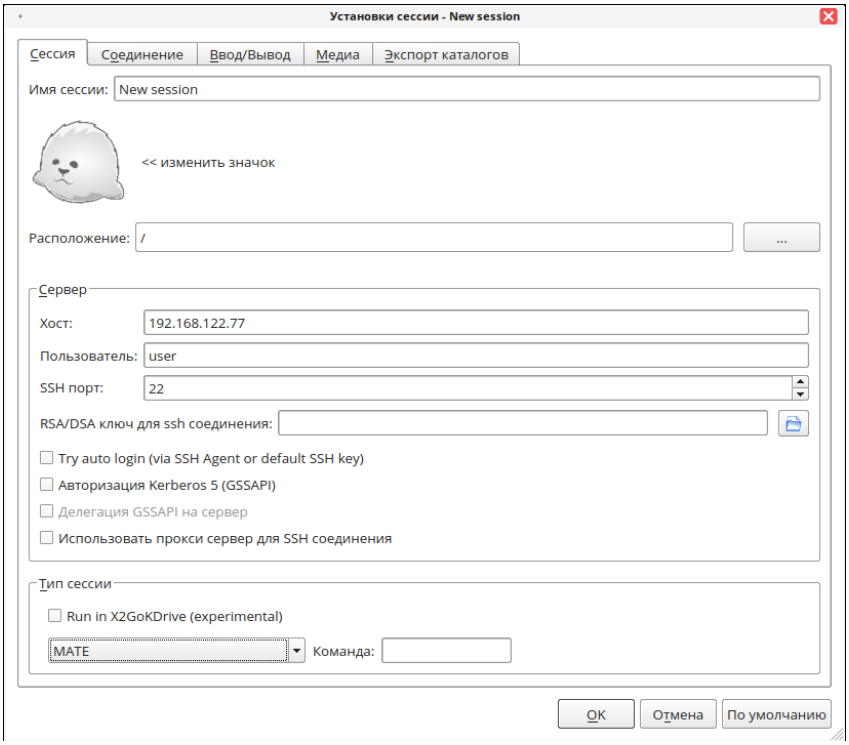
```
dnf install x2goclient
```

Настройка клиента

1. Откройте **x2go client** из «**Главного меню**» - «**Интернет**» - «**X2Go Client**».

2. После открытия потребуется настроить параметры:

- *Хост*: IP-адрес машины;
- *Пользователь*: имя учетной записи.
- *SSH-порт*: если не менялся на клиенте, оставить 22.



3. Для создания новых сессий при подключении к серверу требуется выбрать тип сессии Mate. В РЕД ОС 7.3 по умолчанию используется графическая оболочка Mate. Если же у вас используется другая DE, то тип сессии изменяется в соответствии с нужным требованием.

Если необходимо соединение с активной сессией пользователя, то выберите тип сессии «X2Go/X11 Desktop Sharing».



4. Обратите внимание, что можно настроить автоподключение, указав **RSA/DSA** ключ через выбор файла ключа.

Для этого необходимо выполнить следующие действия:

- На клиенте необходимо сгенерировать ключ SSH командой **ssh-keygen** (с правами **непривилегированного** пользователя):

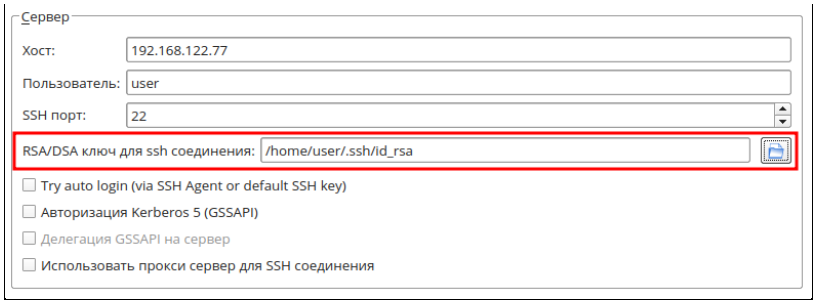
```
ssh-keygen -t rsa
  или
ssh-keygen -t dsa
```

Будет выведено предложение ввести пароль для защиты файла ключа. Если вы планируете выполнять скрипты по **SSH**, оставьте пароль пустым.

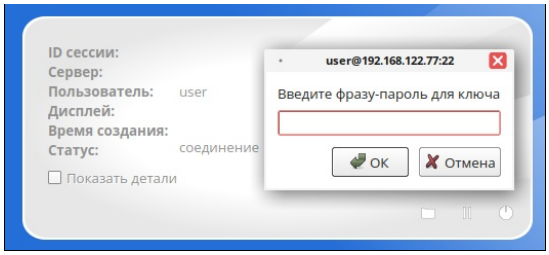
- Передайте публичный ключ на сервер командой от **непривилегированного** пользователя:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server   или ssh-copy-id -i ~/.ssh/id_dsa.pub user@server
```

- В **x2go client** выберите приватную часть ключа.



При подключении произойдет запрос фразы-пароля для ключа.



- Для того чтобы настроить автоматический вход без пароля, необходимо установить флажок в поле «**Try auto login (via SSH Agent or default SSH key)**».

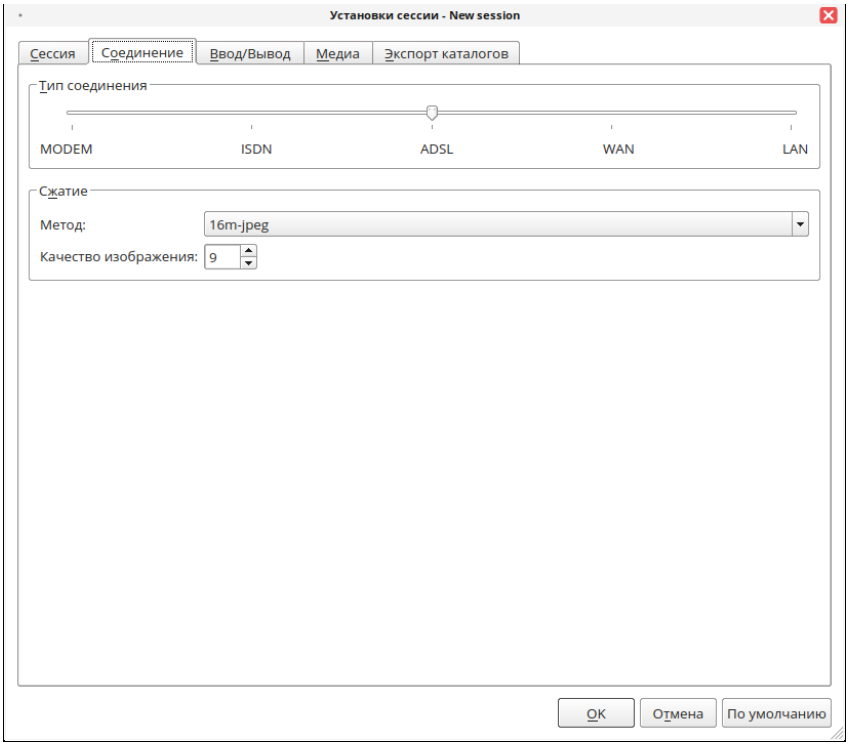
Обзор клиента

Вкладка «Соединение»

В зависимости от пропускной способности сетевого подключения вы можете выбрать предпочитаемый **тип соединения**:

- MODEM;
- ISDN;
- ADSL;
- WAN;
- LAN.

Также данная вкладка предоставляет возможность выбора типа сжатия изображения путем выбора **метода сжатия** и **качества** изображения.



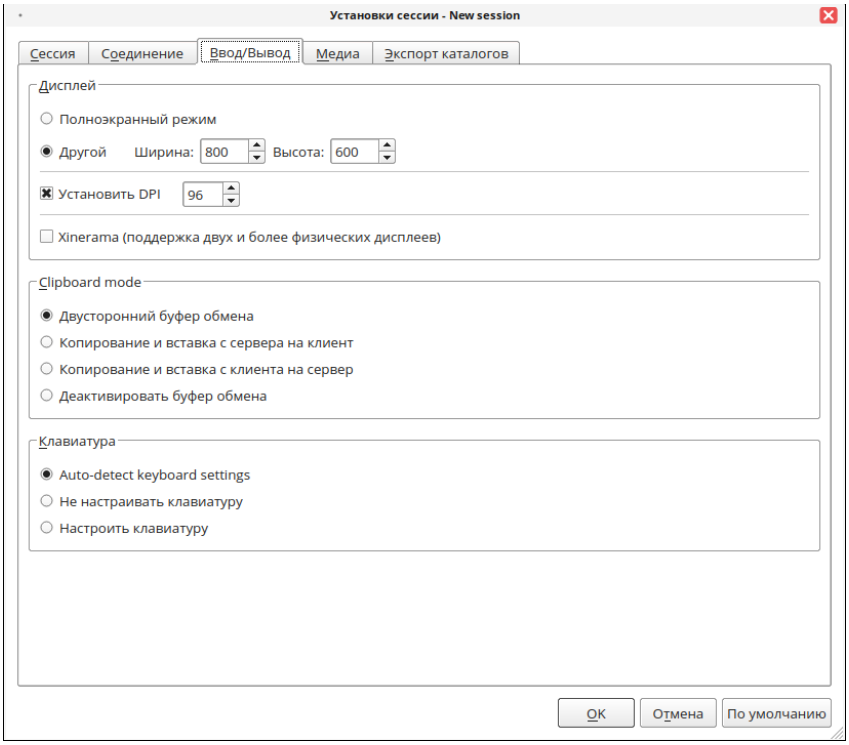
Вкладка «Ввод/Вывод»

Данная вкладка позволяет задать разрешение клиента, т.е. использовать полноэкранный режим или указать свои собственные параметры.

При наличии нескольких физических мониторов вы можете активировать опцию **Xinerama**.

Для работы с буфером обмена рекомендуется оставить настройку двустороннего буфера обмена для удобства работы.

Соответственно, настройку клавиатуры рекомендуется оставить по умолчанию, однако если есть необходимость ручной настройки, то выберите пункт ручной настройки клавиатуры.

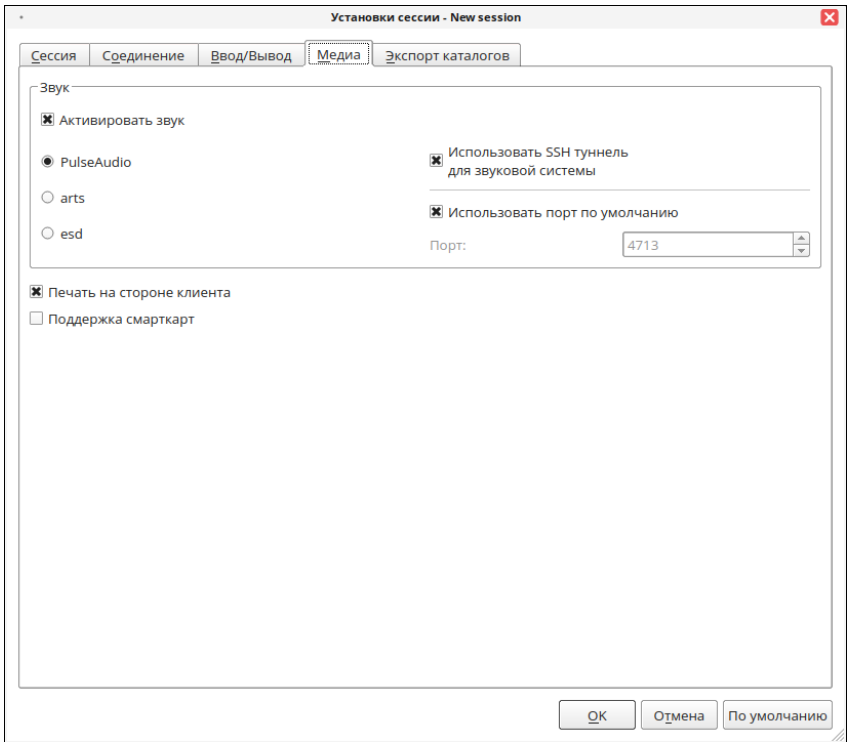


Вкладка «Медиа»

Стоит обратить внимание,что клиент **X2Go** поддерживает проброс звука, по умолчанию данная опция включена. Однако вы можете изменить свойства подключения и изменить установленное значение по умолчанию в случае необходимости.

Не рекомендуется выбирать тип звука **arts** или **esd**, т. к. они являются устаревшими. При попытке выбора любого из данных типов клиент посоветует перейти на тип **PulseAudio**.

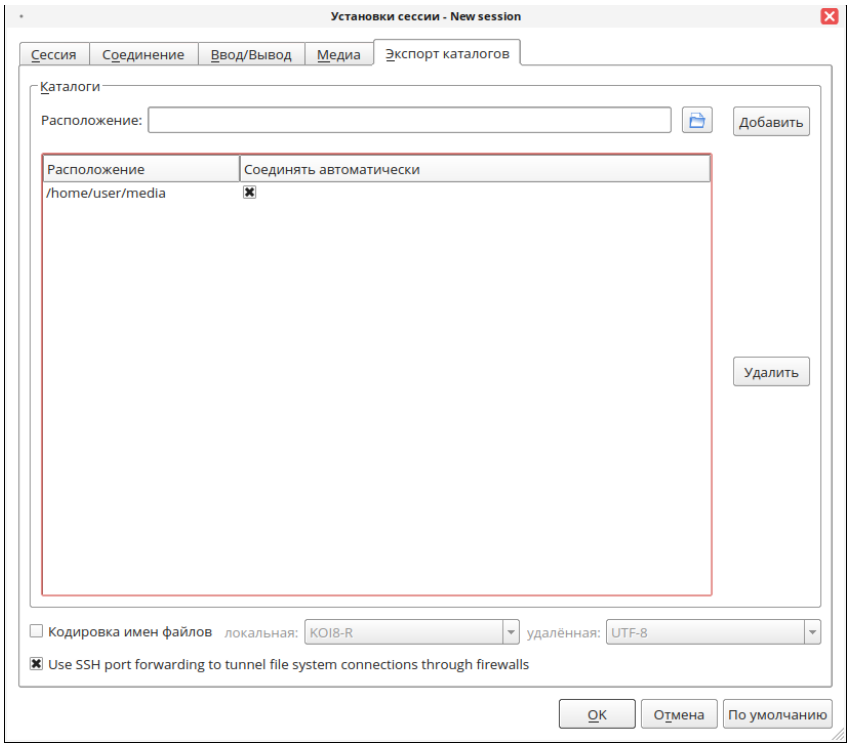
Также вы можете опционально изменить SSH-туннель и порт по умолчанию.



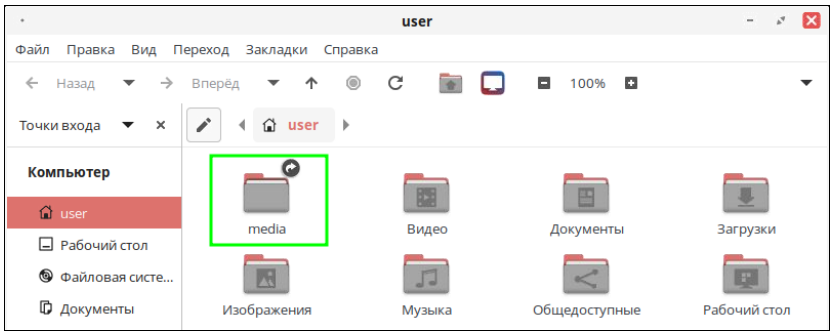
Вкладка «Экспорт каталогов»

Стоит обратить внимание на такую полезную функцию, как экспорт каталогов.

На данной вкладке вы можете выбрать, каким каталогом желаете поделиться. После выбора и добавления он отобразится в списке, где вы сможете активировать его автоматическое соединение.



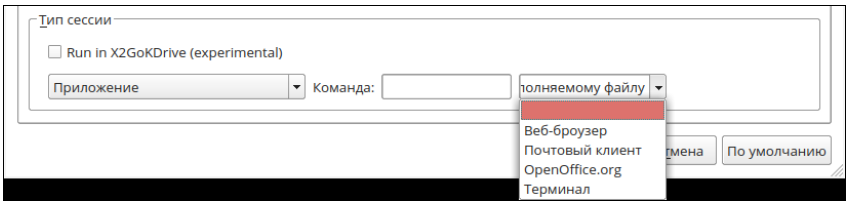
После подключения через **x2go** в домашнем каталоге пользователя будет создан каталог **media**, именно в него перенаправится каталог с клиента.



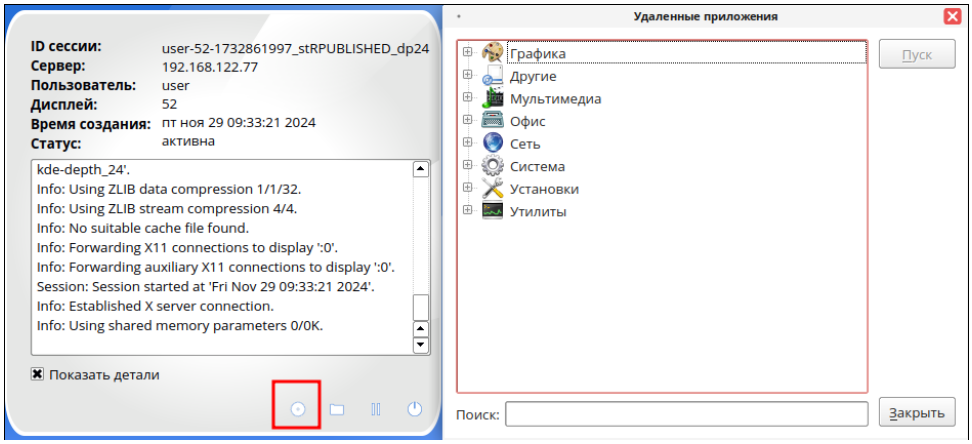
Запуск определенного приложения

Клиент **x2go** поддерживает также вариант подключения не только к полному рабочему столу сервера, но и к конкретному приложению. Реализовать данное подключение можно при помощи типа сессии «**Приложение**» или «**Удаленные приложения**».

При выборе типа сессии приложения вам будет доступен ряд предустановленных вариантов запуска:



При выборе типа сессии «**Удаленные приложения**» откроется новая сессия, где вручную потребуется выбрать то, какое приложение требуется запустить.



Проброс принтеров

1. Для корректного проброса принтера необходимо установить следующие пакеты:

- На сервере:

```
dnf install x2goserver-printing cups-x2go
```

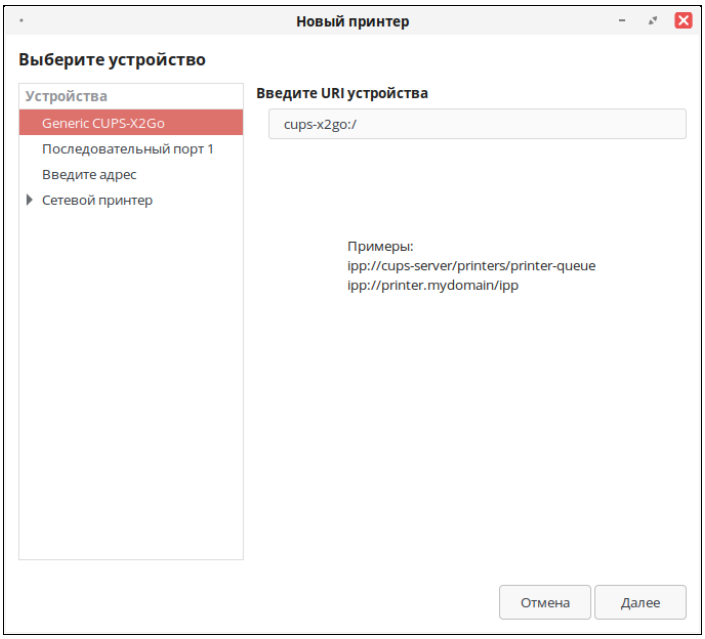
- На клиенте:

```
dnf install cups-x2go
```

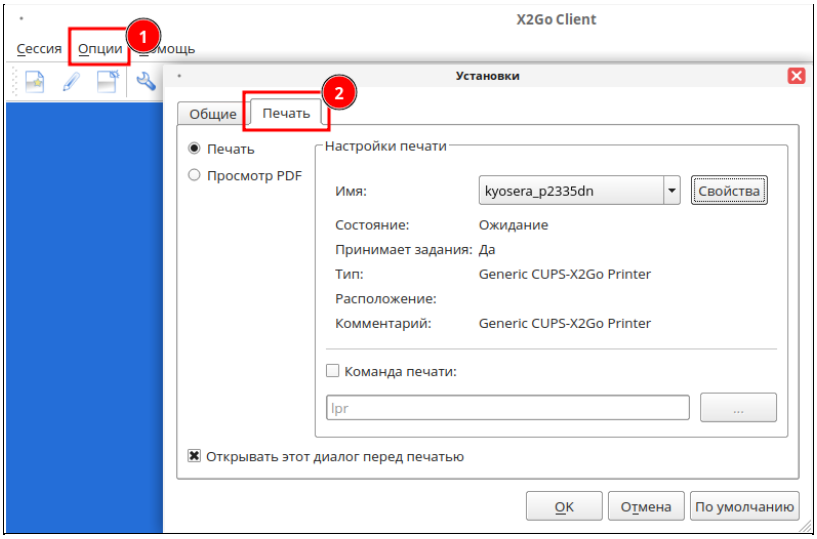
При необходимости перезапустите службу **cups**:

```
systemctl restart cups
```

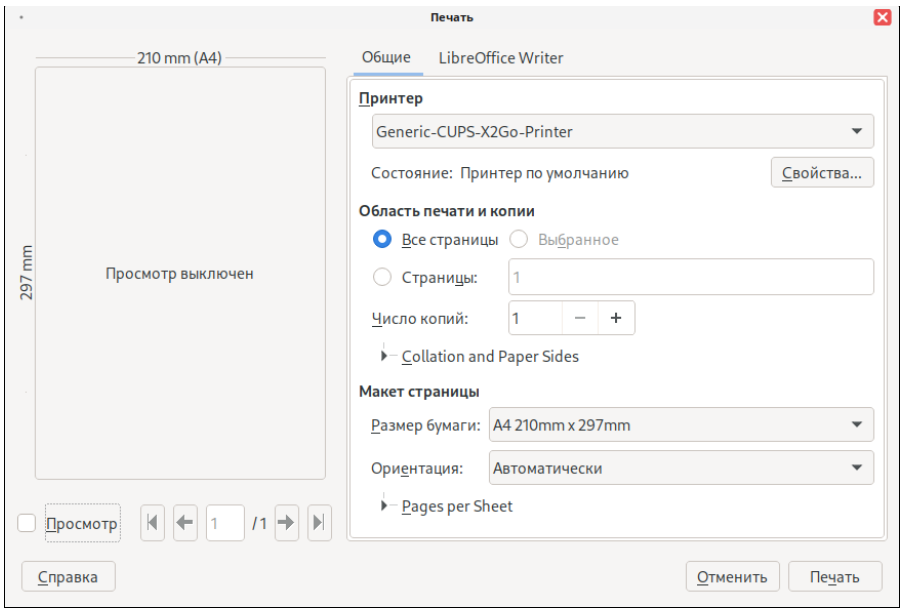
2. На сервере **X2go** добавьте принтер **Generic CUPS-X2Go** («Главное меню» - «Администрирование» - «Настройки принтера»).



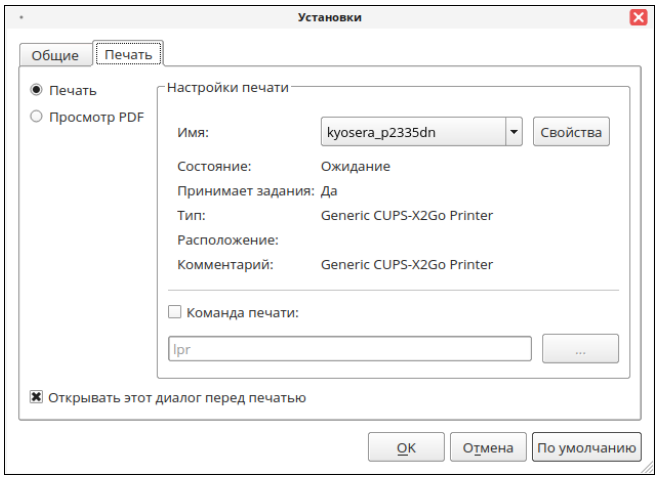
3. В **x2go**-клиенте перейдите в меню «**Опции**» - «**Установки**» - «**Печать**» и выберите принтер, который будет определн по умолчанию при печати. Установите параметр «Открывать этот диалог перед печатью».



4. При печати документа в сессии **x2go** выберите принтер «**Generic CUPS-X2Go-printer**» и нажмите «**Печать**».



После этого на вашем ПК откроется окно выбора локального принтера для печати.

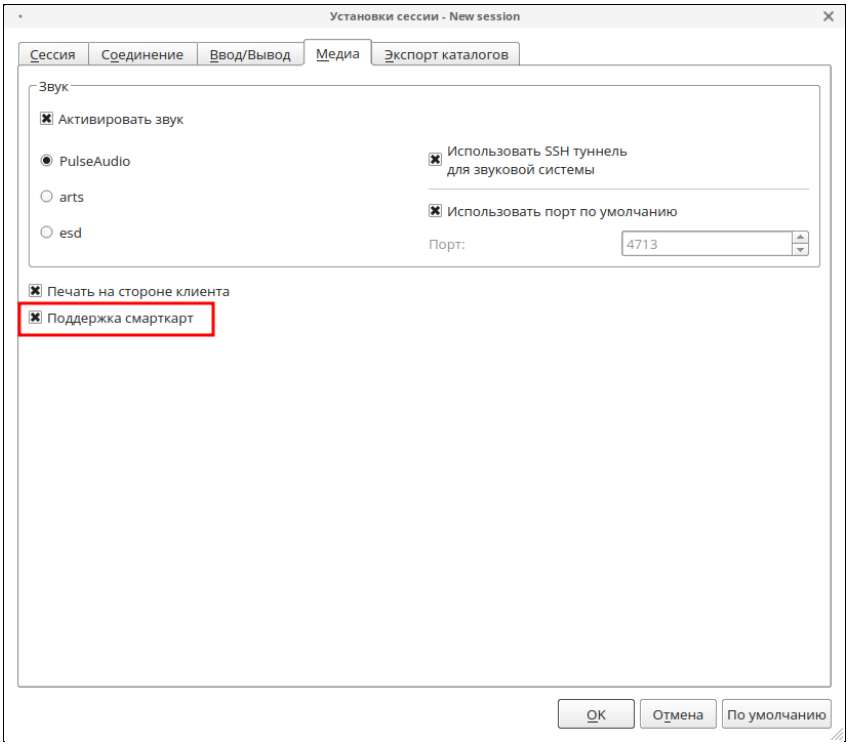


Настройка трансляции токенов в сессию сервера

1. Для настройки трансляции прежде всего требуется убедиться, что настроен **КриптоПро** и необходимые драйвера для токенов на сервере **x2go** - инструкция по настройке.

2. Проверьте работоспособность токена в утилите «**Ключевые носители и сертификаты**» и затем установите флажок в **x2go client** - **Медиа** - **Поддержка смарт-карт**.

Данная поддержка обеспечивает трансляцию как смарт-карт, так и usb-токенов.



Завершение сессий x2go

На сервере необходимо запустить команду, которая покажет все активные сессии:

```
x2golistsessions_root
```

Примерный вывод данной команды:

```
 3226 | user-50-1649312737_stDMATE_dp24 | 50 | localhost.localdomain | S | 2022-04-07T09:25:38 | 8b2f5d3433700b44b5acf5150a7d35fb | 10.81.1.132 | 36540 | 36541 | 2022-04-07T09:35:04 | user | 1839 | 36542 | -1 | -1
 7350 | user-51-1649313366_stS1XSHADuserXSHADPP50_dp24 | 51 | localhost.localdomain | R | 2022-04-07T09:36:06 | c9f4d9a24979efe9ddca96ec20e722cc | 10.81.1.132 | 56847 | 56848 | 2022-04-07T09:36:10 | user | 1211 | 56849 | -1 | -1
 7769 | user-52-1649313401_stS1XSHADuserXSHADPP0_dp24 | 52 | localhost.localdomain | R | 2022-04-07T09:36:41 | 414d5ac30224e035a46c9d7be0d4608b | 10.81.1.132 | 38461 | 38462 | 2022-04-07T09:36:43 | user | 1176 | 38463 | -1 | -1
```

Для завершения определенной сессии выполните:

```
x2goterminate-session <session_id>
```

где **<session_id>** - это идентификатор сессии.

Пример:

```
x2goterminate-session user-50-1649312737_stDMATE_dp24
```

Массовое завершение сессий

Если же на сервере требуется применить **массовую** очистку сессий, то вы можете воспользоваться одним из предложенных ниже скриптов, которые автоматизируют данный процесс.

Завершение сессии и вывод текущей даты

Пример скрипта **завершения сессий** и **вывода текущей даты** при завершении:

```
#!/bin/bash
f=$( cd "$( dirname "${BASH_SOURCE[0]}" )" && pwd )
NOWDATE=$(date '+%Y-%m-%d_%T')
echo -----$NOWDATE------
for i in $(x2golistsessions_root | cut -d "|" -f 2 | sed "s/|/ | /g")
do
echo terminate - ${i} # вывод на экран
x2goterminate-session ${i} # команда завершения пользователя
done
```

Завершение неактивных более 2 часов сессий

Пример скрипта завершения сессий, **время простоя** которых **более 2 часов**:

```
#!/bin/bash
for ll in `x2golistsessions_root`; do
SessionDate=`echo $ll | awk -F \| '{print $11}';`
CleanSessionDate=`echo ${SessionDate//T/ }`
FinalDate=`echo ${CleanSessionDate//-//}`
CurrentDate=`date +%s`
SessionDateEpoch=`date -d "$FinalDate" +%s`
DateDiff=$(($CurrentDate-$SessionDateEpoch))
Hours=$(($DateDiff/60/60))
if [[ $Hours -gt 2 ]]; then
sid=`echo $ll | awk -F \| '{print $2}'`
x2goterminate-session $sid
fi
done
```

Завершение неактивных более 1 дня сессий

Пример скрипта завершения сессий, **время простоя** которых **больше 1 дня**:

```
#!/bin/bash
LIMIT_DAYS=1
for ll in `x2golistsessions_root`; do
#Get the date of last use of the session
lastd=`echo $ll | awk -F \| '{print $11}' | awk -F T '{print $1}';`
```

```
#Date in seconds
lastsec=`date -d "$lastd" +%s`
#Current date in seconds
now=`date +%s` days=`echo $(( ($now - $lastsec) /60/60/24 ))`
if [[ $days -gt $LIMIT_DAYS ]]; then
sid=`echo $ll | awk -F \| '{print $2}'`
echo "terminating session: $sid, $days days old, lastd: $lastd, lastsec: $lastsec, now: $now" x2goterminate-session $sid
fi
done
```

Настройка автоматического завершения сессий

Также администратору сервера будет удобен вариант создания сервиса, который по определенному таймеру завершит сессии. Ниже приведен пример сервиса, который по таймеру запускает абстрактный скрипт. **Обратите внимание, что необходимо изменить путь к скрипту на ваш**.

Создайте файл:

```
nano /etc/systemd/system/x2go-sessions-killer.service
```

со следующим содержимым:

```
[Unit]
Description="X2Go service for session cleaning"
After=network.target
[Service]
Type=simple
ExecStart=/usr/bin/SCRIPT.sh # укажите ваш путь к скрипту
Restart=always
RestartSec=7200
[Install]
WantedBy=multi-user.target
```

В строке `RestartSec=7200` указано время перезапуска скрипта в секундах. В примере скрипт будет выполняться **каждые два часа**. Измените это значение на необходимое вам.

Затем в папку **/usr/bin/** добавьте ваш скрипт и назначьте ему права на исполнение:

```
chmod +x /usr/bin/SCRIPT.sh
```

После этого обновите список сервисов и добавьте сервис завершения сессий в автозагрузку:

```
systemctl daemon-reload
systemctl enable --now x2go-sessions-killer.service
```

X2Go Broker

X2Go Broker — модуль, позволяющий централизованно управлять настройками сессий клиентов. В большинстве случаев клиенты X2Go запускаются в автономном режиме, и пользователь сам настраивает одну или несколько сессий для подключения к серверам X2Go, а все настройки сохраняются на локальных компьютерах.

Данный модуль позволяет хранить настроенные профили подключения непосредственно на сервере, а для получения настроек с сервера клиент X2Go должен быть запущен в режиме **Broker Mode**, при этом локально настроенные профили игнорируются. Это решение полезно в масштабах крупных предприятий для балансировки нагрузки.

Настройка x2gobroker

Для установки пакетов **x2gobroker** перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

```
dnf install x2gobroker x2gobroker-common x2gobroker-ssh x2gobroker-daemon x2gobroker-authservice
```

Далее необходимо в файл **/etc/hosts** добавить запись о сервере:

```
echo "<ip-адрес_сервера> x2goserver" >> /etc/hosts
```

В файле **/etc/x2go/broker/x2gobroker-sessionprofiles.conf** определите следующие параметры:

```
[x2goserver-mate]
name=Test Work Mate
host=x2goserver
command=MATE
usebrokerpass=true
```

где:

- **[x2goserver-mate]** — уникальный идентификатор сессии;
- **name** — имя сессии, которое будет отображаться на клиенте;
- **command** — тип сессии (MATE, KDE и т.п.).

Затем запустите необходимые для работы сервисы:

```
systemctl enable x2gobroker-authservice --now
systemctl enable x2gobroker-daemon --now
```

Настройка x2goserver

Для настройки сервера необходимо сначала установить соответствующие пакеты командой:

```
dnf install x2goserver x2goserver-printing cups-x2go x2goserver-xsession
```

После установки в файл **/etc/hosts** следует добавить запись о брокере командой:

```
echo "<ip-адрес_брокера> x2gobroker" >> /etc/hosts
```

Запустите сервис сервера командой:

```
systemctl enable x2gocleansessions --now
```

Настройка x2goclient

Для настройки клиента необходимо установить соответствующий пакет командой:

```
dnf install x2goclient
```

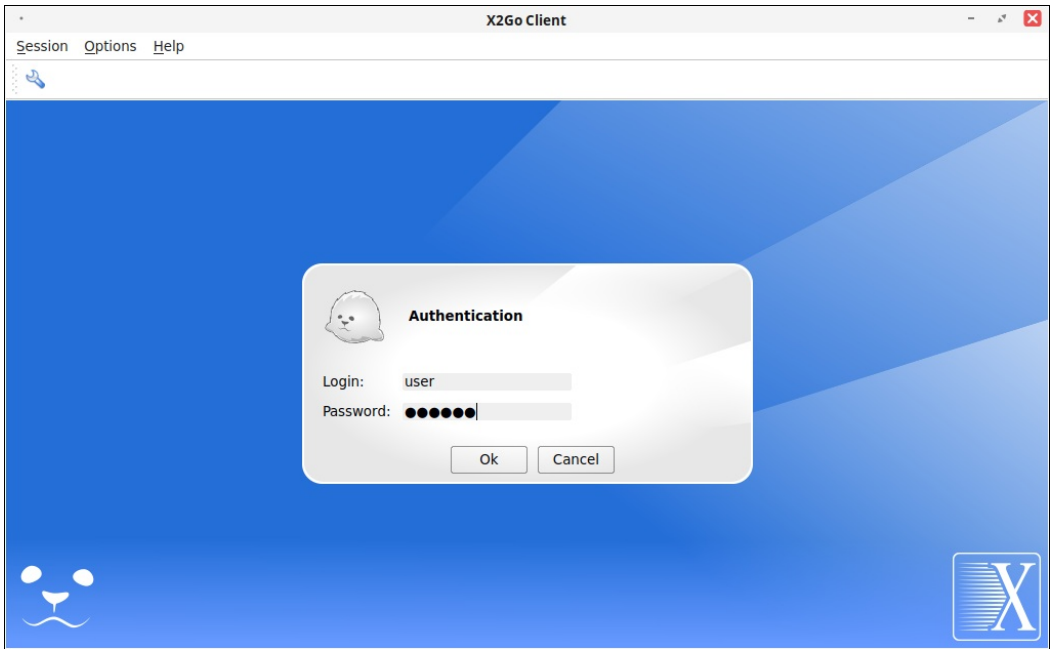
После установки клиента в файл **/etc/hosts** следует добавить запись о брокере и сервере командой:

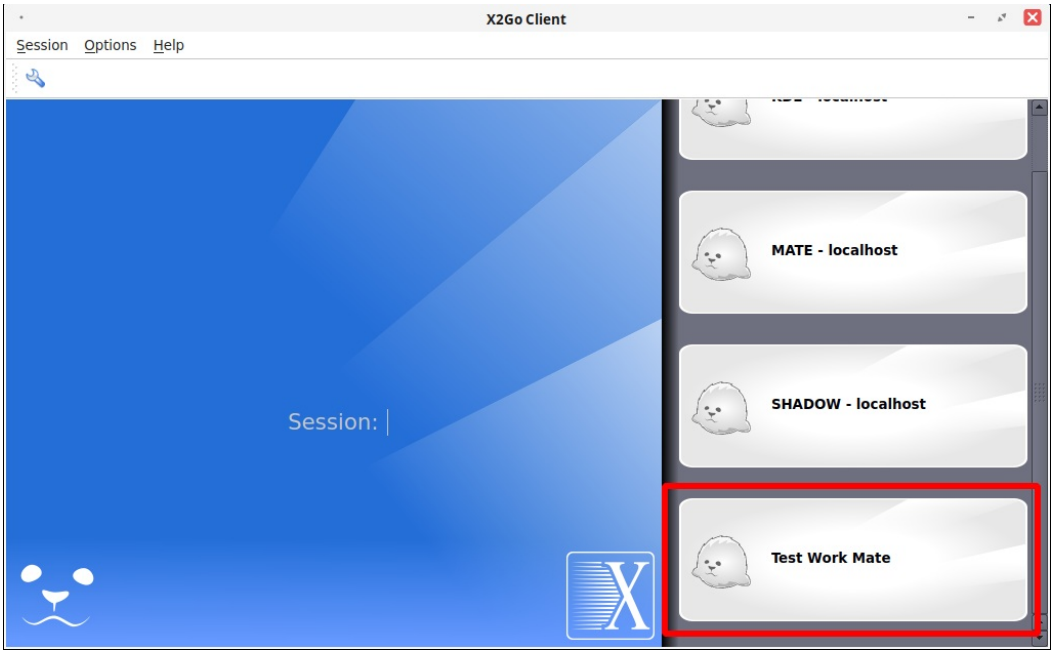
```
echo "<ip-адрес_брокера> x2gobroker" >>/etc/hosts
echo "<ip-адрес_сервера> x2goserver" >>/etc/hosts
```

Для подключения к серверу выполните команду:

```
x2goclient --broker-url=http://x2gobroker:8080/plain/
```

В окне аутентификации введите логин и пароль пользователя, с правами которого необходимо подключиться к серверу, и выберите нужную сессию (в примере *Test Work Mate*).





В активном окне сессии можно убедиться в правильности подключения, проверив IP-адрес машины. Должен быть отображен IP-адрес сервера.

Запуск отдельного графического приложения

Для запуска определенного приложения на брокере необходимо добавить конфигурацию новой сессии (файл **/etc/x2go/broker/x2gobroker-sessionprofiles.conf**):

```
[x2goserver-brasero]
name=Test Brasero
host=x2goserver
command=brasero
usebrokerpass=true
```

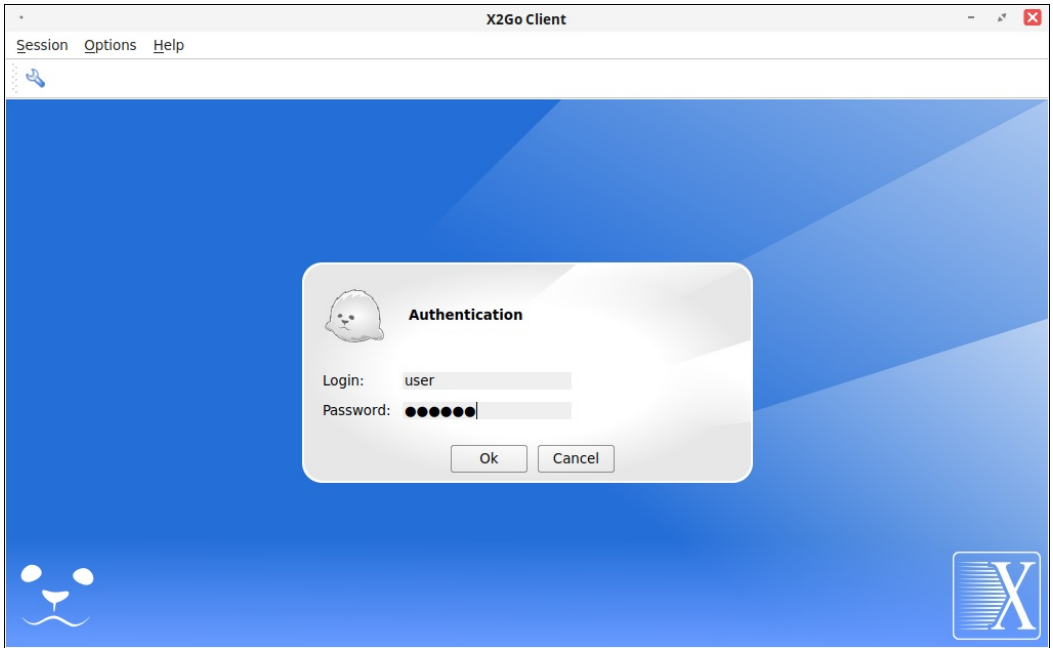
В данном случае в параметре command указывается название приложения, которое должно быть запущено вместо графической сессии.

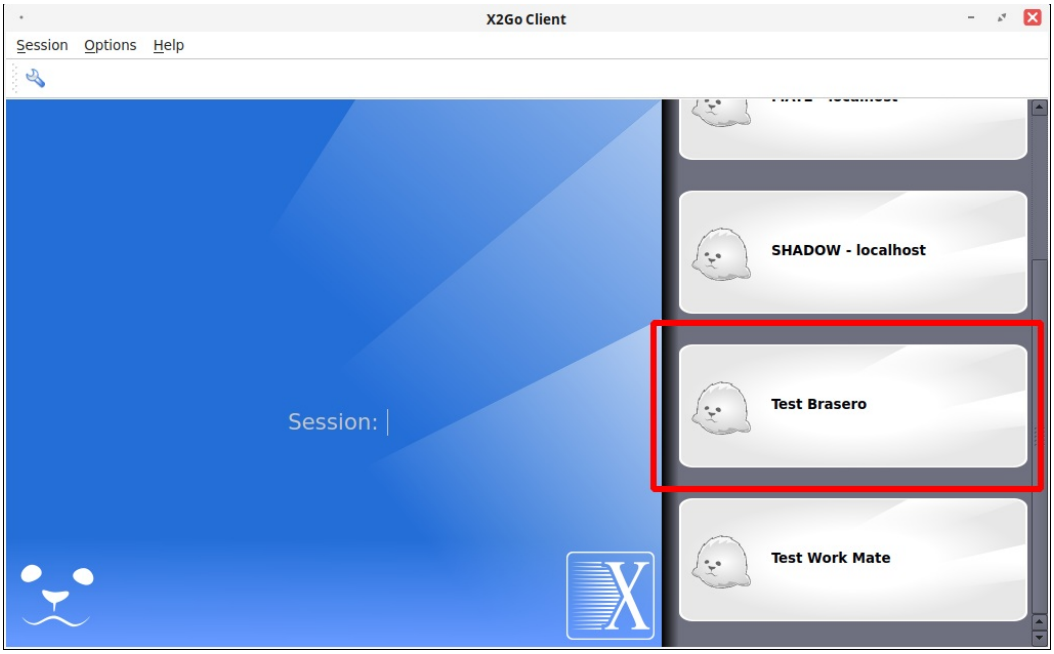
Для подключения клиента к серверу используется та же команда:

```
x2goclient --broker-url=http://x2gobroker:8080/plain/
```

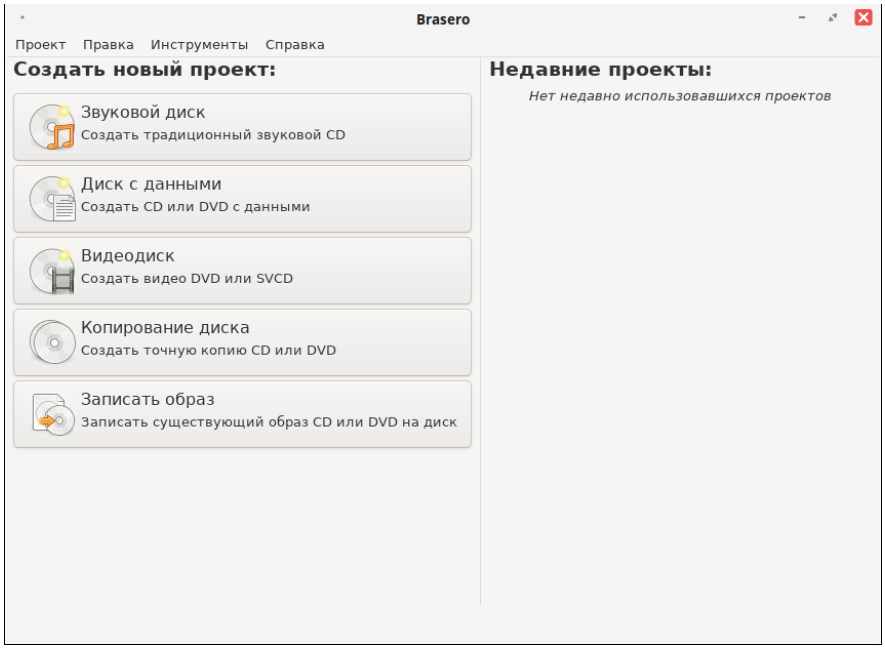
В окне аутентификации так же потребуется введите логин и пароль пользователя, с правами которого необходимо подключиться к

серверу, и выбрать сессию с запуском отдельного приложения (в примере **Test Brasero**).





После успешного подключения будет открыто окно указанной программы.



Настройка X11VNC

Установка
Настройка x11vnc
Графическая утилита X11VNC Server

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: x11vnc-0.9.16-9

Установка

Перейдите в сеанс пользователя **root**:

```
su -
```

Далее все команды будут выполняться с правами пользователя **root**, если не указано иное.

Установите пакет **x11vnc**:

```
dnf install x11vnc
```

Настройка x11vnc

> **Примечание.**
>
> Корректная работа **x11vnc** возможна **только** при использовании дисплейного менеджера **SDDM**.

Дисплейный менеджер **SDDM** по умолчанию используется в графическом окружении **KDE**. Подробную информацию об установке дисплейного менеджера **SDDM** для графических окружений **MATE** и **GNOME** см. в нашей инструкции «Менеджер входа в систему sddm».

Предварительно необходимо настроить пароль для удаленного подключения:

```
x11vnc -storepasswd "<задайте_пароль>" /etc/vncpasswd
```

Далее необходимо настроить сервер **X11VNC**. Для этого создайте файл службы `x11vnc.service`:

```
nano /usr/lib/systemd/system/x11vnc.service
```

и заполните его следующим содержимым:

```
[Unit]
Description=x11vnc server for SDDM
After=display-manager.service

[Service]
ExecStart=/bin/bash -c "/usr/bin/x11vnc -display :0 -many -shared -dontdisconnect -repeat -auth /var/run/sddm/xauth* -noxdamage -rfbauth
/etc/vncpasswd"
Restart=on-failure
RestartSec=3

[Install]
WantedBy=graphical.target
```

Перезагрузите конфигурацию **systemd**:

```
systemctl daemon-reload
```

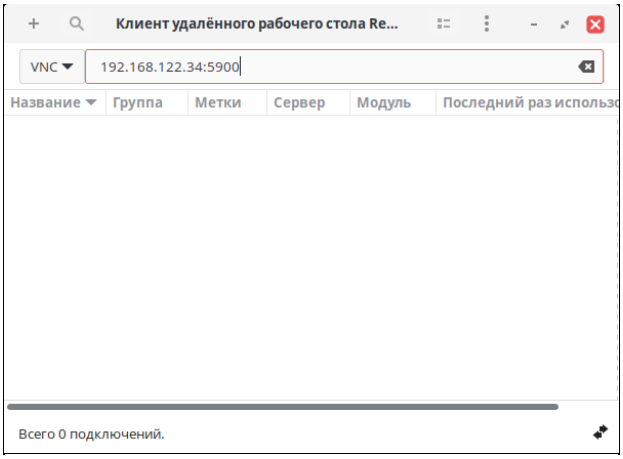
Запустите и добавьте в автозагрузку службу `x11vnc.service`:

```
systemctl enable x11vnc.service --now
```

Проверьте, запустилась ли служба (в статусе должно отображаться **active (running)**).

```
systemctl status x11vnc.service
```

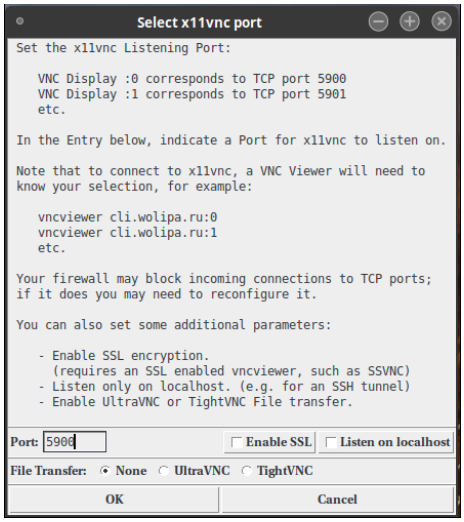
Для подключения к сессии пользователя можно воспользоваться любой утилитой удаленного подключения. В данном случае подключение будет выполнено с помощью менеджера удаленных подключений **Remmina**. Выберите тип подключения — `VNC`, в адресе подключения укажите IP-адрес удаленного хоста, дополнительно можно указать порт, на котором запущена служба `x11vnc.service` (обычно **5900**).



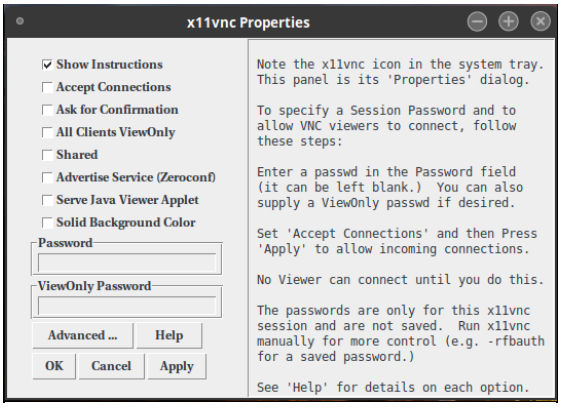
Графическая утилита X11VNC Server

Запуск графической утилиты администрирования **x11vnc** доступен из «**Главного меню**» - «**Интернет**» - «**X11VNC Server**».

Стартовое окно утилиты представлено в следующем виде:

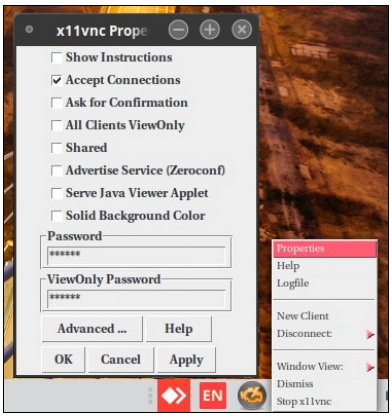


При нажатии на «**OK**» вы увидите дальнейшее окно настройки сервера:

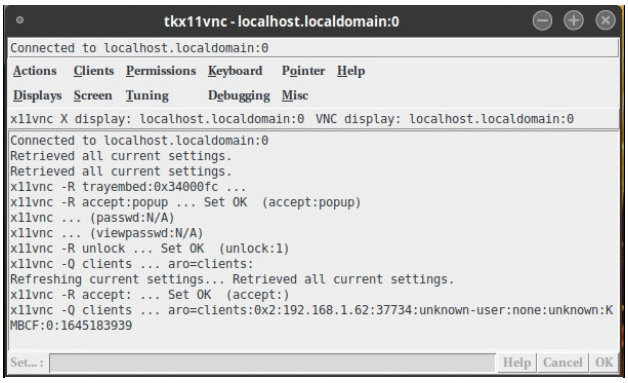


Вы можете настроить параметры подключения клиентов под себя. При нажатии кнопки «**OK**» происходит запуск службы **x11vnc**, ПК становится доступен для подключения. После запуска утилита сворачивается в системный трей.

При вызове свойств из трея вы увидите следующее окно:



При переходе в режим **Advanced** открывается более подробная информации о подключении и дополнительных параметрах настройки связи.



Работа с FreeRDP и RemoteApp

Установка freerdp
Варианты использования freerdp для подключения к удаленному рабочему столу
xfreerdp_gui - графическая оболочка для работы с freerdp
RemoteApp - запуск приложений

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический
- **Версия ПО**: freerdp-3:3.8.0-1, freerdp-gui-3.0-1

freerdp — клиент с открытым кодом для подключения к удаленному рабочему столу по протоколу **RDP**.

Установка FreeRDP

Для установки пакета выполните команду:

```
dnf install xfreerdp
```

Описание часто используемых параметров:

Параметр	Описание
/u:	Имя пользователя
/d:	Имя домена
/v:	ip-адрес или имя хоста
/p:	Пароль
/w: /h:	Значения ширины и высоты
/smartcard:	Проброс токенов
/a:printer	Подключение принтера
/cert:ignore	Игнорировать сертификат
/app:program:	Запуск удаленного приложения
/drive:	Подключение каталога
/sound:	Перенаправление звука
/microphone:	Активация микрофона

Полный список параметров представлен на официальной странице проекта **FreeRDP**.

Варианты использования FreeRDP для подключения к удаленному рабочему столу

Подключение папки

```
xfreerdp /u:bob /d:win.redos /v:192.168.1.196 /cert:ignore /sec:rdp /p:my_password /drive:folder,/home/bob@win.redos/temp
```

Подключение принтера

Названия подключенных принтеров можно вывести командой **lpstat -a**.

```
xfreerdp /u:bob /d:win.redos /v:192.168.1.196 /cert:ignore /sec:rdp /p:my_password /a:printer,"Kyocera-Kyocera-ECOSYS-P2335dn-(KPDL)"
```

Подключение токена

С помощью **pcsc_scan** узнаем имя токена, например, **Reader 0: Aladdin R.D. JaCarta 00 00** достаточно указать первое вхождение в имени **Aladdin**.

```
xfreerdp /u:user /p:my_password /smartcard:Aladdin /v:192.168.1.196
```

Перенаправление звука и микрофона в сессию

```
xfreerdp /v:192.168.1.196 /u:user /p:my_password /sound:sys:oss,dev:1,format:1 /sound:sys:alsa /microphone:sys:oss,dev:1,format:1 /microphone:sys:alsa
```

где **sys:alsa** - явное указание какой звуковой поддержки выбрать (**alsa**/**pulse**).

Подключение к сессии с явным указанием размеров окна

```
xfreerdp /v:192.168.1.196 /u:user /p:my_password /w:800 /h:600
```

Данное явное указание полезно в тех случаях, когда стандартное разрешение не умещается на мониторе.

freerdp-gui — графическая оболочка для работы с freerdp

Утилита **freerdp-gui** представляет собой графическую оболочку для работы с **FreeRDP**.

Данная утилита устанавливается следующей командой:

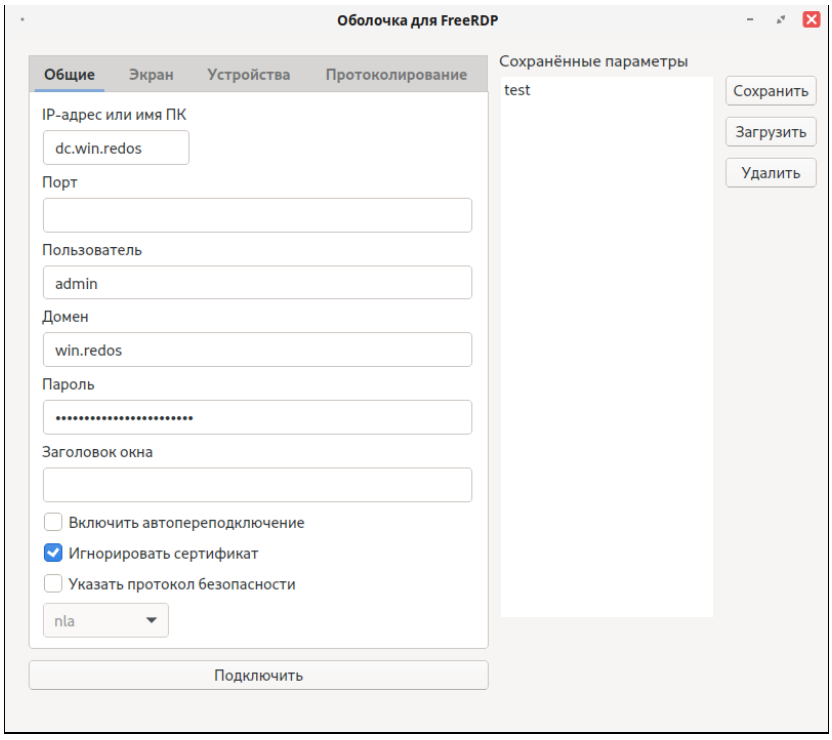
```
sudo -E dnf install freerdp-gui
```

Запуск утилиты доступен из «**Главного меню**» - «**Интернет**» - «**Оболочка для FreeRDP**» или из терминала командой:

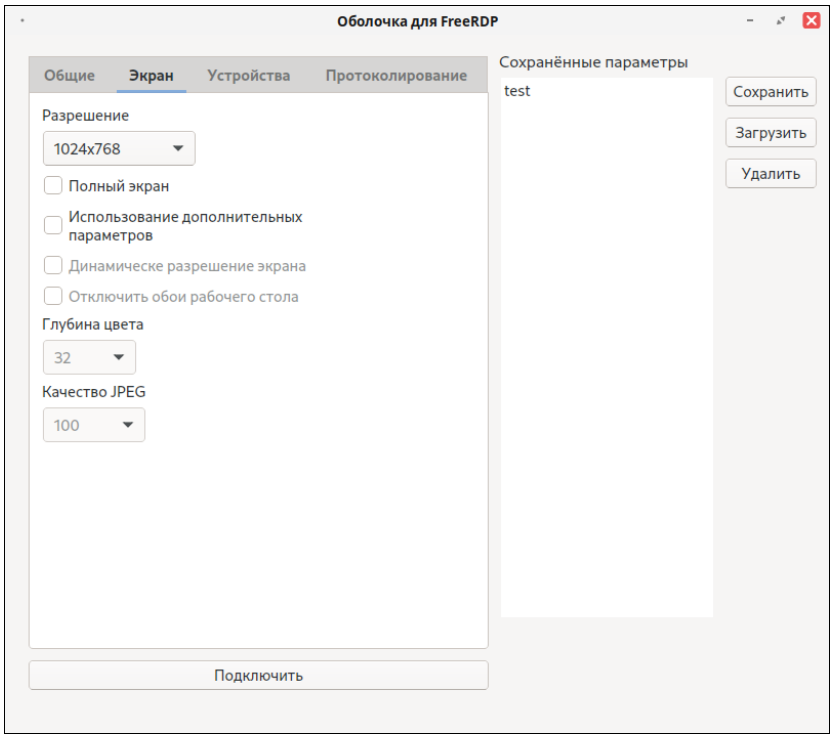
```
freerdp-gui
```

Главное окно утилиты представляет функционал по подключению к **xrdp** или Windows RDP серверу.

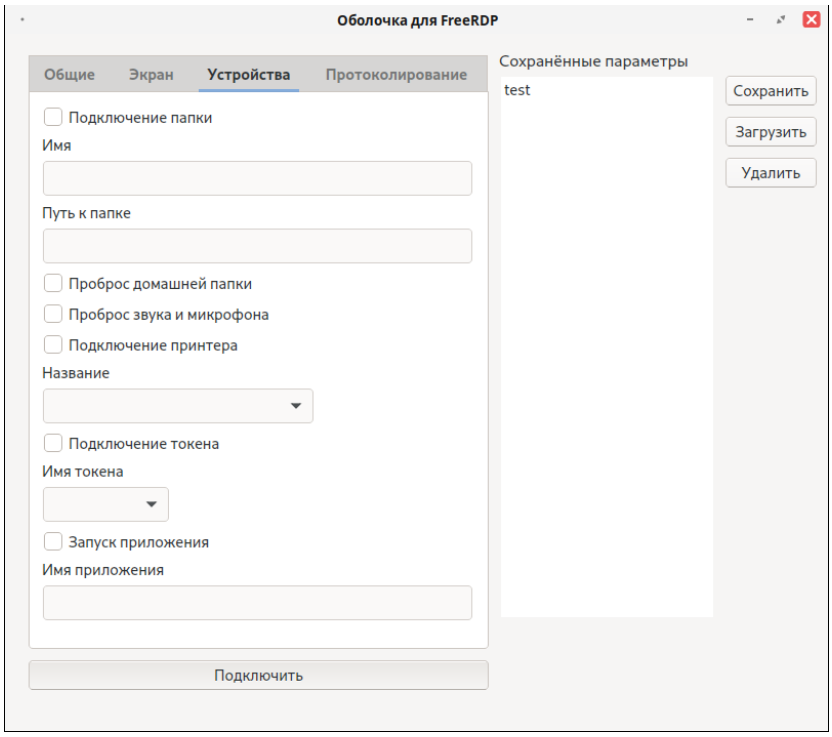
Пользователь может задать для своих целей параметры, представленные на снимке основного окна утилиты.



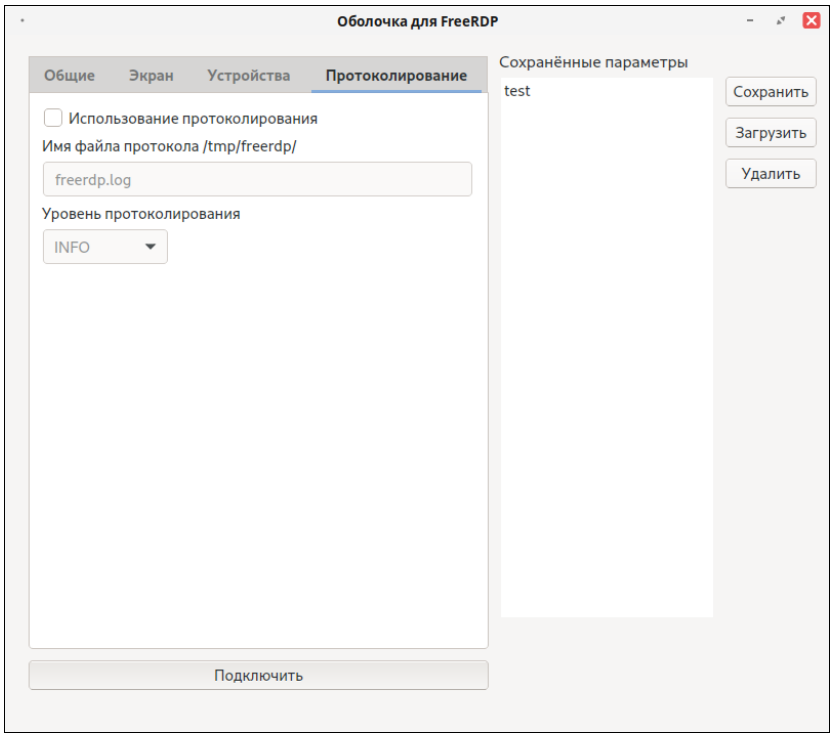
Для выбора необходимого разрешения экрана и дополнительных параметров предусмотрена вкладка «**Экран**».



Если требуется работа с пробросом папки или устройств, таких как принтер, токен или звук на серверную часть - для этого предусмотрена вкладка «**Устройства**».



Для настройки протоколирования событий предусмотрена вкладка «**Протоколирование**».



RemoteApp - запуск приложений

RemoteApp - позволяет запускать приложения по **rdp**, как если бы они были запущены на локальном компьютере пользователя, т.е пользователь запускает приложение, которое выполняется на сервере, но внешне выглядит, будто оно запущено на локальном компьютере. Для доступа к приложению, оно предварительно должно быть опубликовано на сервере **rdp**. В строке подключения укажите приложение, доступное на сервере приложений.

```
xfreerdp /u:user /d:win.redos /v:192.168.1.196 /cert:ignore /p:my_password /app:program:"||word"
```

GUI запрос пароля:

```
xfreerdp /u:user /d:win.redos /v:192.168.1.196 /cert:ignore /p:$(zenity --entry --title="Domain Password" --text="Enter your password:" --hide-text)
```

В данном примере используется **zenity** - утилита, которая позволяет выводить на экран диалоговые окна. В данном случае - это диалог ввода пароля.

Настройка guacamole

Установка
Настройка файла конфигурации
Настройка файла параметров
Настройка клиента
Веб-интерфейс

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: guacd-1.5.3-1, tomcat-1:9.0.93-1

Guacamole — бесплатная программа с открытым исходным кодом, которая предоставляет дистанционный доступ ко всем рабочим клиентским машинам через веб-интерфейс. То есть на ваш собственный компьютер, с которого вы удалённо администрируете клиентские машины, не нужно устанавливать никаких плагинов и стороннего программного обеспечения, всё работает по **HTML5**.

Установка

Установка необходимых пакетов:

```
dnf install guacd libguac-client-rdp libguac-client-ssh libguac-client-vnc libguac-client-telnet tomcat tomcat-webapps
```

Настройка файла конфигурации

Создайте директорию:

```
mkdir /etc/guacamole
```

Настройка конфигурационного файла:

```
nano /etc/guacamole/guacd.conf
```

Содержимое файла конфигурации:

```
[server]
 bind_host = 127.0.0.1
 bind_port = 4822
```

Примечание.

Файл конфигурации чувствителен к синтаксису. Необходимо добавить 2 пустых строки в конце файла.

Настройка файла параметров

Настройка файла параметров:

```
nano /etc/guacamole/guacamole.properties
```

Содержимое файла параметров:

```
guacd-hostname: localhost
 guacd-port: 4822
 user-mapping: /etc/guacamole/user-mapping.xml
 auth-provider: net.sourceforge.guacamole.net.basic.BasicFileAuthenticationProvider
```

Создайте GUACAMOLE_HOME переменную окружения:

```
echo "GUACAMOLE_HOME=/etc/guacamole" | sudo tee -a /etc/default/tomcat
```

Создайте символьную ссылку:

```
ln -s /etc/guacamole /usr/share/tomcat/.guacamole
```

Настройка клиента

Выполните настройку guacamole client:

```
wget https://dlcdn.apache.org/guacamole/1.5.5/binary/guacamole-1.5.5.war
mv guacamole-1.5.5.war /etc/guacamole/guacamole.war
ln -s /etc/guacamole/guacamole.war /usr/share/tomcat/webapps/
```

Создайте зашифрованный пароль (укажите вместо **password** ваш пароль):

```
echo -n password | openssl md5

 (stdin)= 5f4dcc3b5aa765d61d8327deb882cf99
```

Сохраните вывод зашифрованного пароля. Он пригодится при следующем этапе настройки доступных подключений:

```
nano /etc/guacamole/user-mapping.xml
```

Содержимое:

```
<user-mapping>
 <!-- Per-user authentication and config information -->

  <!-- A user using md5 to hash the password
  guacadmin user and its md5 hashed password below is used to
  login to Guacamole Web UI-->
  <authorize
   username="admin"
   password="5f4dcc3b5aa765d61d8327deb882cf99"
   encoding="md5">
  <!-- First authorized Remote connection -->
   <connection name="ssh ro73">
   <protocol>ssh</protocol>
   <param name="hostname">192.168.1.43</param>
   <param name="port">22</param>
  </connection>

  <!-- Second authorized remote connection -->
   <connection name="rdp ro73">
   <protocol>rdp</protocol>
   <param name="hostname">192.168.1.43</param>
   <param name="port">3389</param>
   <param name="username">test</param>
   <param name="ignore-cert">true</param>
  </connection>
  </authorize>
</user-mapping>
```

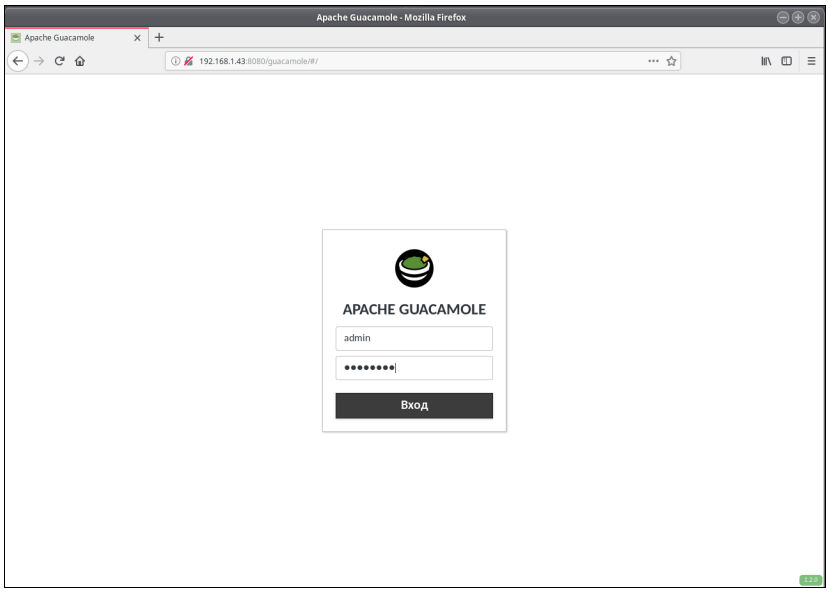
Выполните перезапуск необходимых служб:

```
systemctl restart tomcat guacd
```

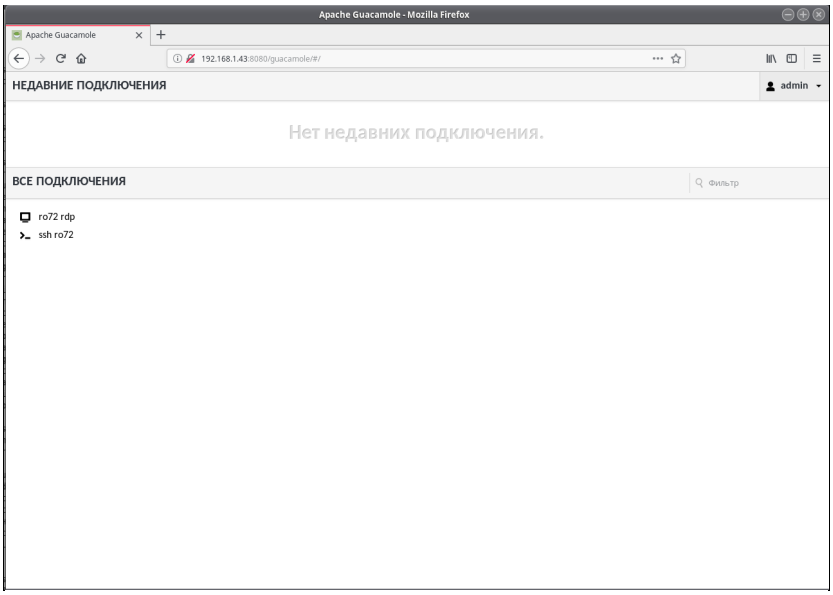
Веб-интерфейс

Для входа через веб-интерфейс в адресной строке браузера введите 192.168.1.43:8080/guacamole.

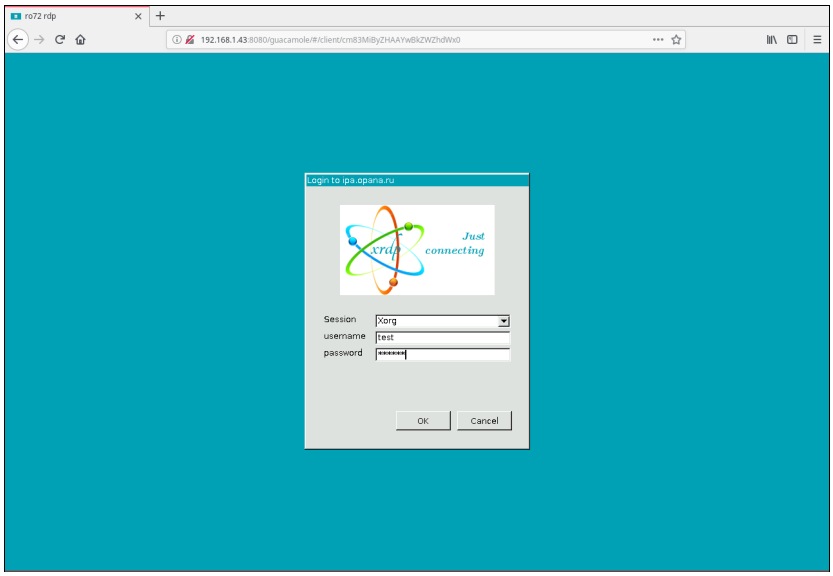
Будет открыта форма авторизации:



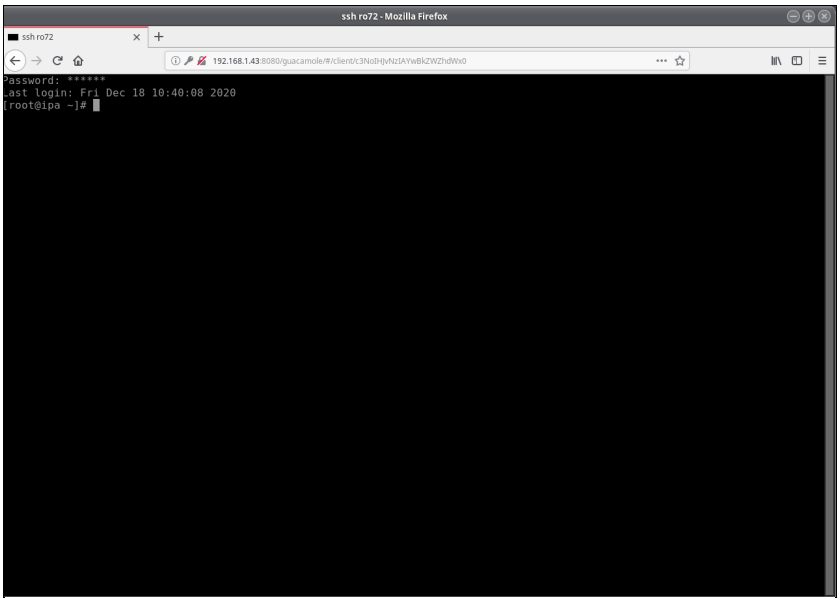
Доступные подключения:



Подключение по **RDP** (предварительно на данном ПК должен быть настроен XRDP-сервер).



Пример входа по **SSH**:



Remmina – клиент для подключения к удаленному рабочему столу

Установка Remmina и плагинов
Подключение устройств
Примеры использования Remmina
Решение возникающих проблем

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: remmina-1.4.27-4

Remmina — клиент удалённого рабочего стола, имеет лицензию *GPLv2+*.

Обычно используется для подключения к удаленному рабочему столу *Windows* (**RDP**), но также *Remmina* имеет возможности подключения с использованием следующих протоколов: **SSH, VNC, RDP, NX и XDMCP**.

Вы можете подробнее ознакомиться с возможностью осуществления удаленного подключения при помощи **Remmina**, просмотрев наши обучающие видео:

- на **RuTube** — Организация удаленного доступа с РЕД ОС на Windows;
- в **Яндекс.Дзен** — Организация удаленного доступа с РЕД ОС на Windows;
- в **VK Видео** — Организация удаленного доступа с РЕД ОС на Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Установка Remmina и плагинов

Для установки данного приложения выполните команду:

```
dnf install remmina
```

При скачивании *Remmina* будут доступны следующие плагины: **EXEC, NX, RDP, RDPF, RDPS, SFTP, SPICE, SSH, ST, VNC, VNCI, XDMCP, glibsecret**.

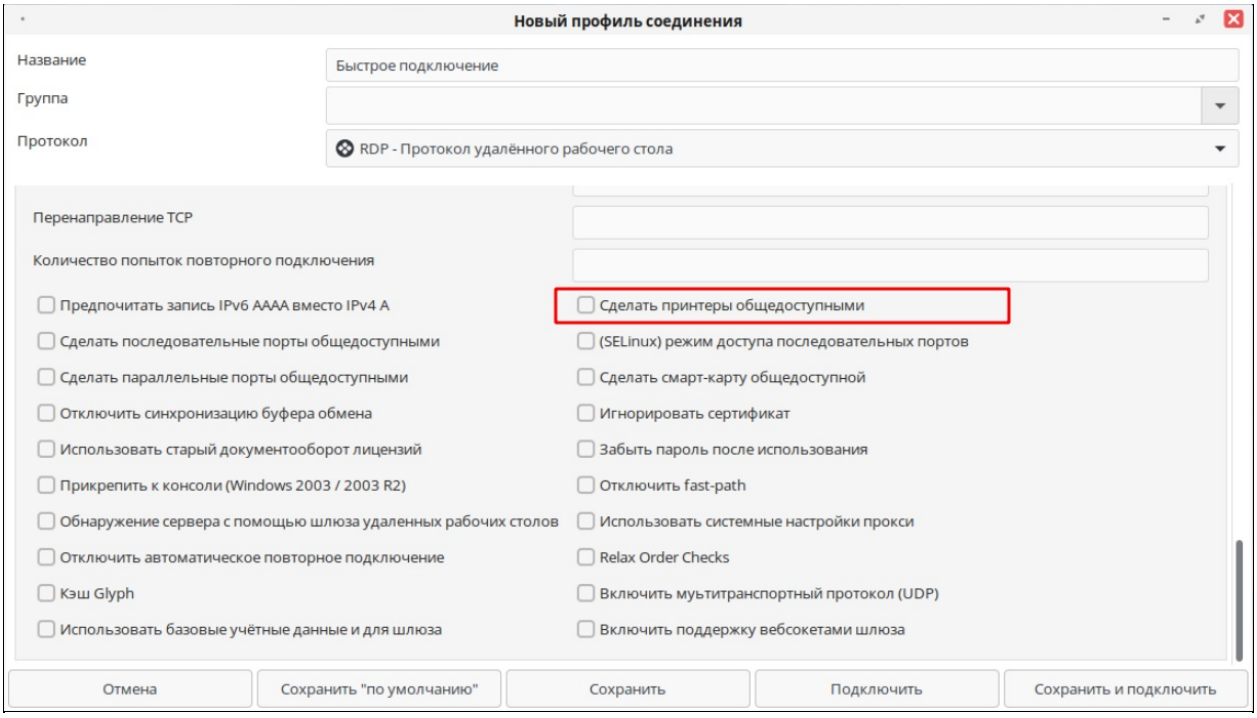
Для расширенной работы с приложением можно установить оставшиеся плагины следующей командой (с правами пользователя **root**):

```
dnf install remmina-gnome-session remmina-plugins-kwallet remmina-plugins-spice remmina-plugins-www
```

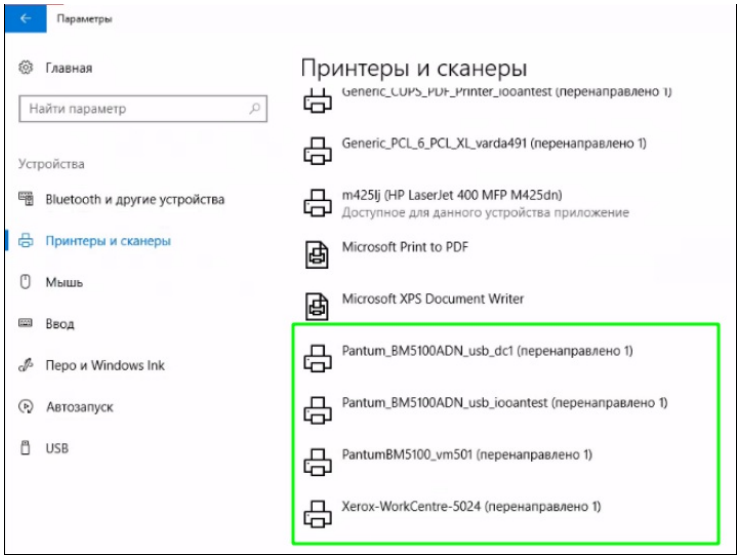
Подключение устройств

Перенаправление принтера в удаленный рабочий стол по протоколу RDP

Откройте параметры соединения, перейдите на вкладку «**Дополнительные**», установите флажок на строке «**Сделать принтеры общедоступными**».



Нажмите на кнопку «**Сохранить и подключить**», в результате локальный принтер будет перенаправлен в удаленный рабочий стол.



Вы можете подробнее ознакомиться с примером подключения локального принтера к удаленному рабочему столу, просмотрев наши обучающие видео:

- на **RuTube** — Подключение локального принтера к удаленному рабочему столу;
- в **Яндекс.Дзен** — Подключение локального принтера к удаленному рабочему столу;
- в **VK Видео** — Подключение локального принтера к удаленному рабочему столу.

На наших каналах вы также сможете найти много другой полезной информации.

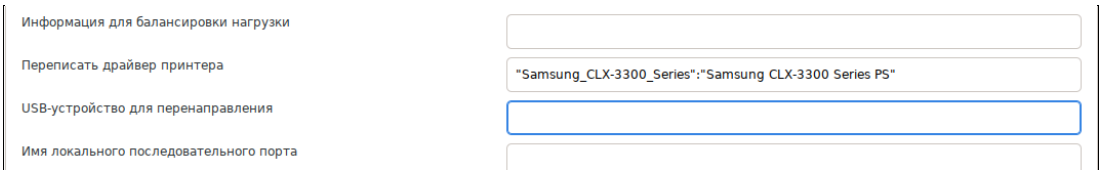
Переназначение драйвера принтера

Иногда бывает недостаточным при перенаправлении принтера выбирать параметр «**Сделать принтеры общедоступными**», в результате наблюдаются ошибки при печати или принтеру может не назначиться признак «**По умолчанию**».

В данном случае в **Remmina** на вкладке «**Дополнительно**» можно попробовать определить параметр «**Переписать драйвер принтера**».

Формат данного поля следующий: первым указывается в двойных кавычках *имя принтера* на РЕД ОС, а вторым - *драйвер* в Windows.

Пример - **"Samsung_CLX-3300_Series":"Samsung CLX-3300 Series PS"**:



Перенаправление токенов в удаленный рабочий стол по протоколу RDP

В качестве примера будут рассмотрены токены **Рутокен ЭЦП** и **Aladdin R.D. JaCarta**.

Для перенаправления устройства необходимо указать идентификатор устройства (**ID**), определить его можно с помощью команды `pcsc_scan` (выполняется с правами **локального пользователя**).

Пример вывода команды для **Рутокен ЭЦП**:

```
pcsc_scan

Using reader plug'n play mechanism
Scanning present readers...
0: Aktiv Rutoken ECP 00 00

Sun May 28 22:02:03 2023
 Reader 0: Aktiv Rutoken ECP 00 00
  Event number: 0
  Card state: Card inserted,
  ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1

ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
+ TS = 3B --> Direct Convention
+ T0 = 8B, Y(1): 1000, K: 11 (historical bytes)
  TD(1) = 01 --> Y(i+1) = 0000, Protocol T = 1
-----
+ Historical bytes: 52 75 74 6F 6B 65 6E 20 44 53 20
  Category indicator byte: 52 (proprietary format)
+ TCK = C1 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
 Aktiv Rutoken ECP
 https://www.rutoken.ru/products/all/rutoken-ecp/
```

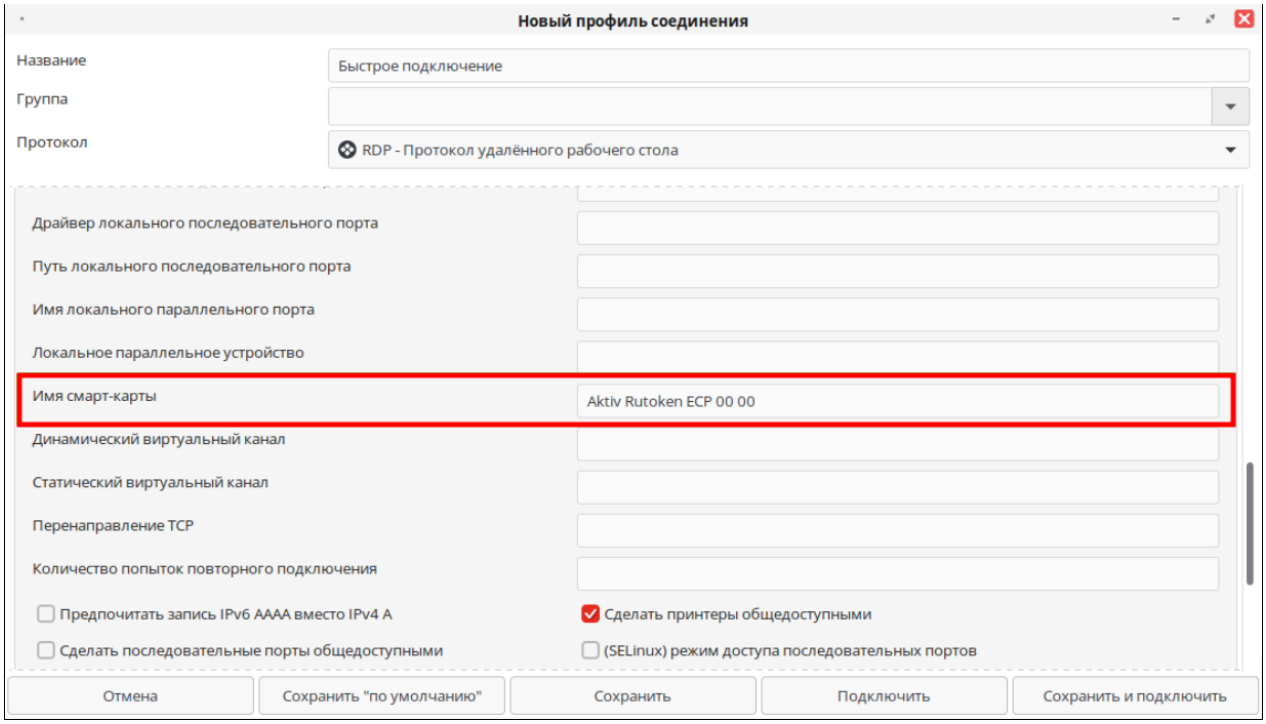
Пример вывода команды для **Aladdin R.D. JaCarta**:

```
pcsc_scan

Using reader plug'n play mechanism
Scanning present readers...
0: Aladdin R.D. JaCarta [SCR Interface] 00 00

Mon May 29 11:21:48 2023
 Reader 0: Aladdin R.D. JaCarta [SCR Interface] 00 00
  Event number: 0
  Card state: Card inserted,
  ATR: 3B DC 18 FF 81 91 FE 1F C3 80 73 C8 21 13 66 01 06 11 59 00 01 28

ATR: 3B DC 18 FF 81 91 FE 1F C3 80 73 C8 21 13 66 01 06 11 59 00 01 28
+ TS = 3B --> Direct Convention
+ T0 = DC, Y(1): 1101, K: 12 (historical bytes)
  TA(1) = 18 --> Fi=372, Di=12, 31 cycles/ETU
    129032 bits/s at 4 MHz, fMax for Fi = 5 MHz => 161290 bits/s
  TC(1) = FF --> Extra guard time: 255 (special value)
  TD(1) = 81 --> Y(i+1) = 1000, Protocol T = 1
-----
  TD(2) = 91 --> Y(i+1) = 1001, Protocol T = 1
-----
  TA(3) = FE --> IFSC: 254
  TD(3) = 1F --> Y(i+1) = 0001, Protocol T = 15 - Global interface bytes following
-----
  TA(4) = C3 --> Clock stop: no preference - Class accepted by the card: (3G) A 5V B 3V
```

```
 + Historical bytes: 80 73 C8 21 13 66 01 06 11 59 00 01
  Category indicator byte: 80 (compact TLV data object)
    Tag: 7, len: 3 (card capabilities)
      Selection methods: C8
        - DF selection by full DF name
        - DF selection by partial DF name
        - Implicit DF selection
      Data coding byte: 21
        - Behaviour of write functions: proprietary
        - Value 'FF' for the first byte of BER-TLV tag fields: invalid
        - Data unit in quartets: 2
      Command chaining, length fields and logical channels: 13
        - Logical channel number assignment: by the card
        - Maximum number of logical channels: 4
    Tag: 6, len: 6 (pre-issuing data)
      Data: 01 06 11 59 00 01
+ TCK = 28 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B DC 18 FF 81 91 FE 1F C3 80 73 C8 21 13 66 01 06 11 59 00 01 28
 JaCarta (PKI)
 http://www.aladdin-rd.ru
```

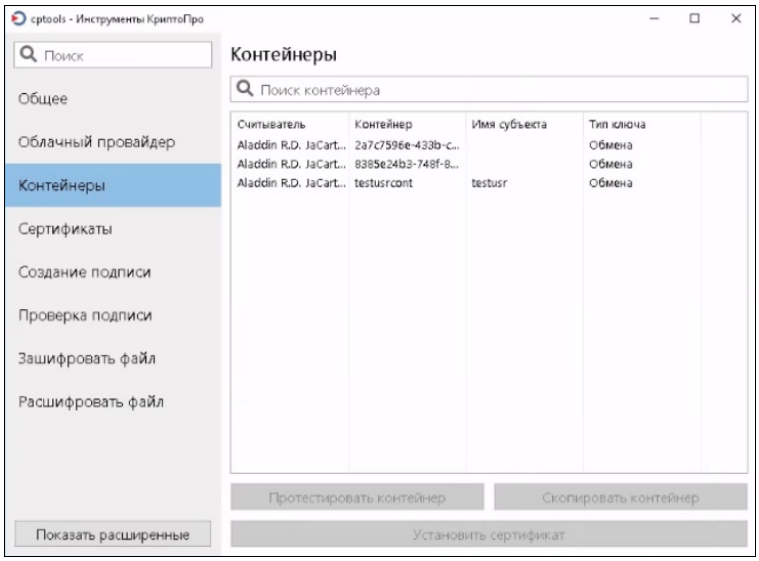
В выводе команды из строки «**Reader 0**» необходимо скопировать идентификатор устройства.

В Remmina в новом профиле соединения на вкладке «**Дополнительные**» в поле «**Имя смарт-карты**» укажите **ID** устройства из команды `pcsc_scan`.



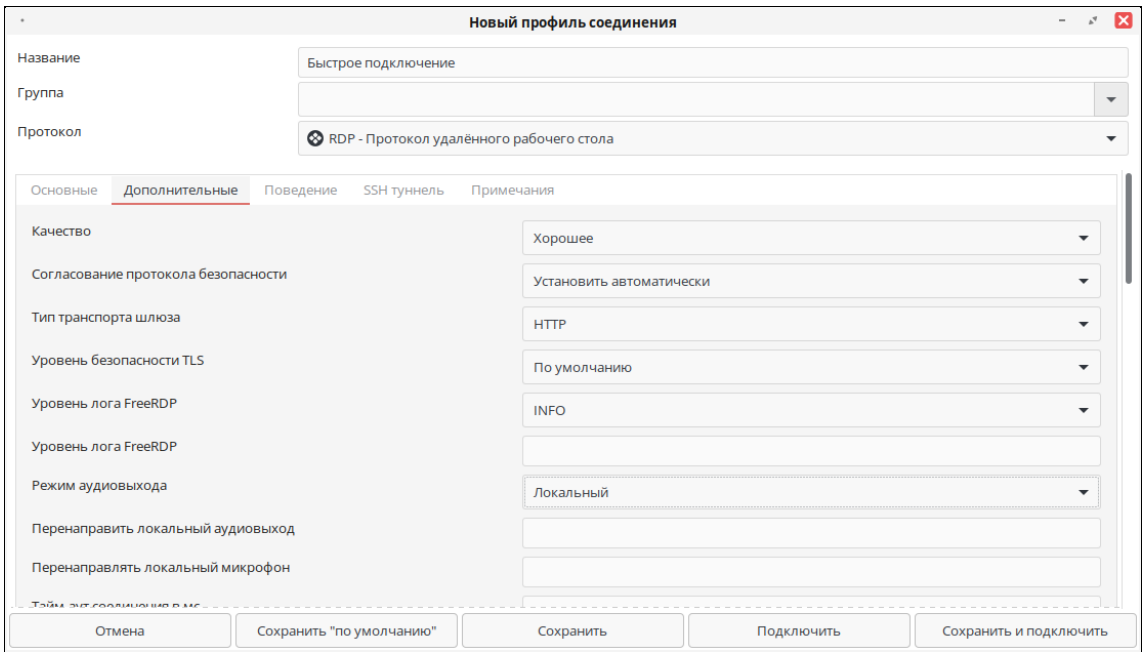
Затем нажмите на кнопку «**Сохранить**».

Пример успешного перенаправления токенов можно просмотреть в утилите «**Инструменты КриптоПРО**».



Перенаправление звука на удаленный рабочий стол

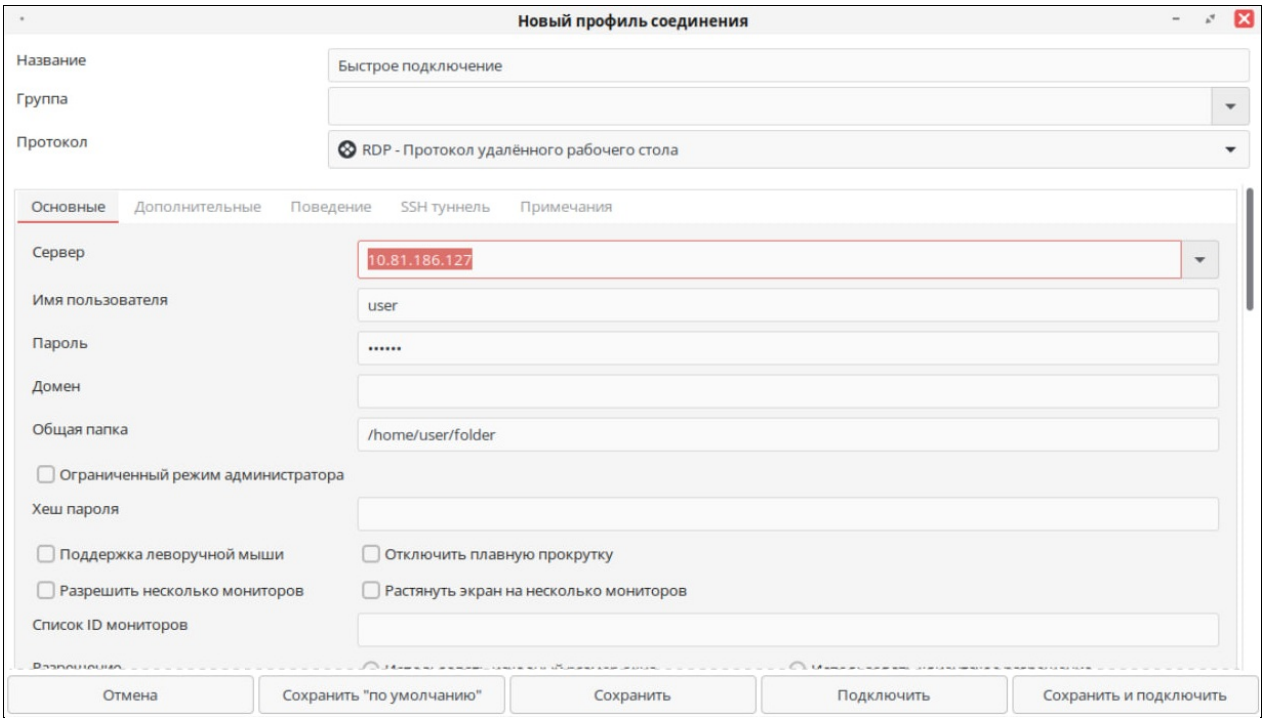
Откройте профиль соединения в «**Профиль соединения**», во вкладке «**Дополнительные**» для параметра «**Режим аудиовыхода**» в диалоговом окне выпадающего списка выберите значение «**Локальный**».



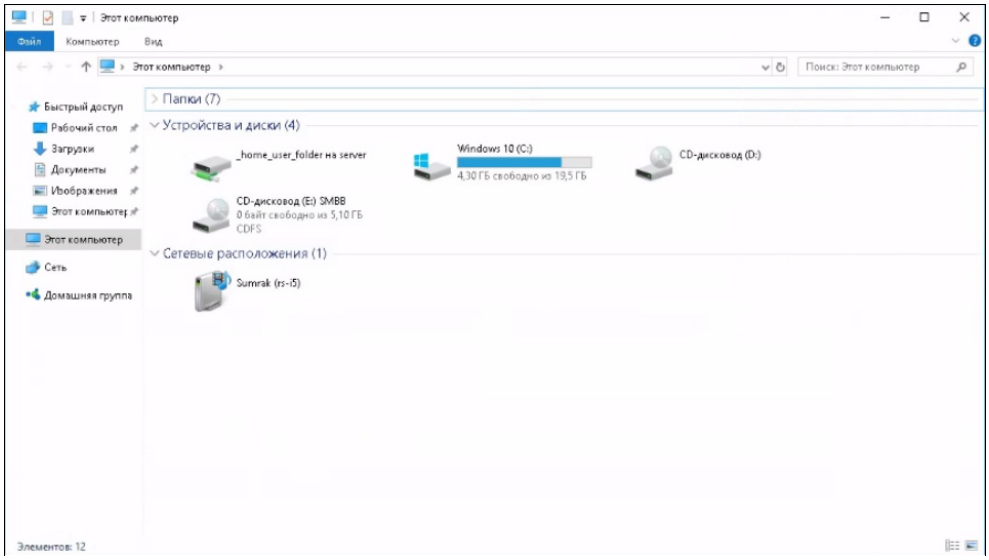
Нажмите на кнопку «**Сохранить и подключить**». Теперь звук будет передаваться на удаленный компьютер.

Общий доступ к локальным каталогам или Flash-носителю в удаленном рабочем столе

Откройте профиль соединения в «**Профиль соединения**», далее во вкладке «**Основные**» в диалоговом окне выпадающего списка директорий параметра «**Общая папка**» выберите нужный каталог или диск.



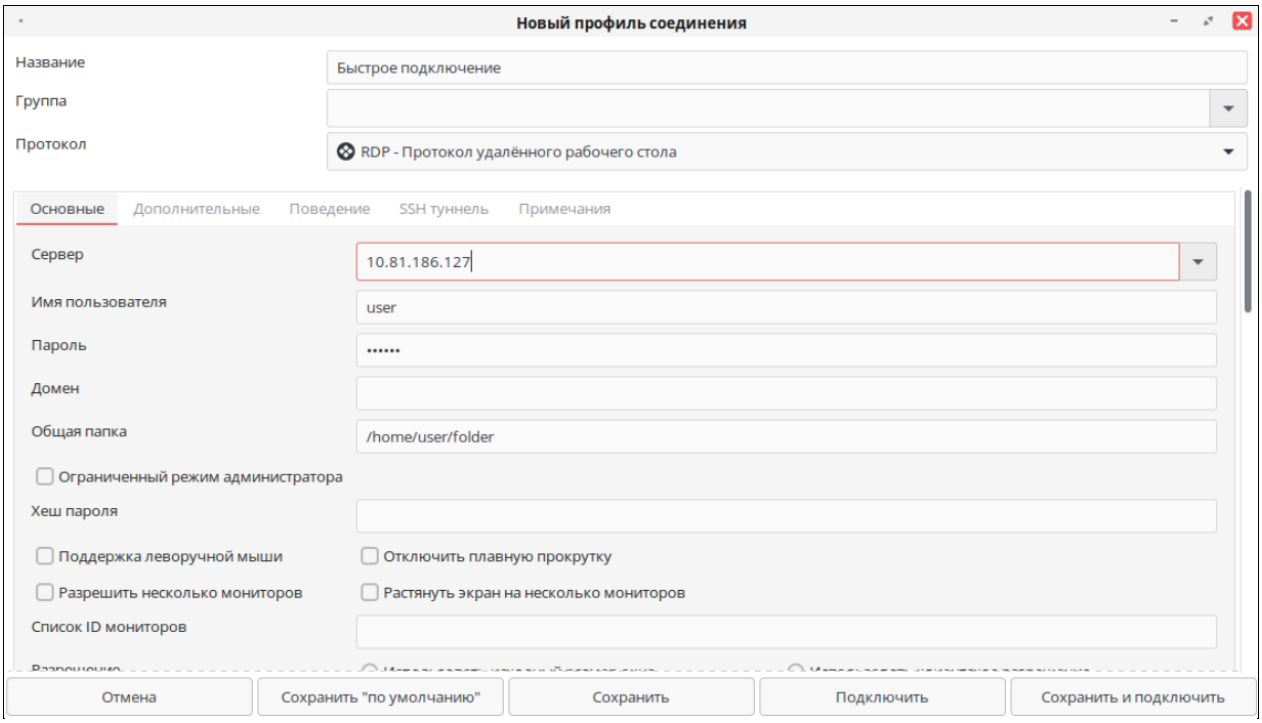
Нажмите на кнопку «**Сохранить и подключить**». Выбранная папка станет доступной для использования в удаленном рабочем столе.



Примеры использования Remmina

Установка подключения к Windows (для примера используется Windows 10 Pro)

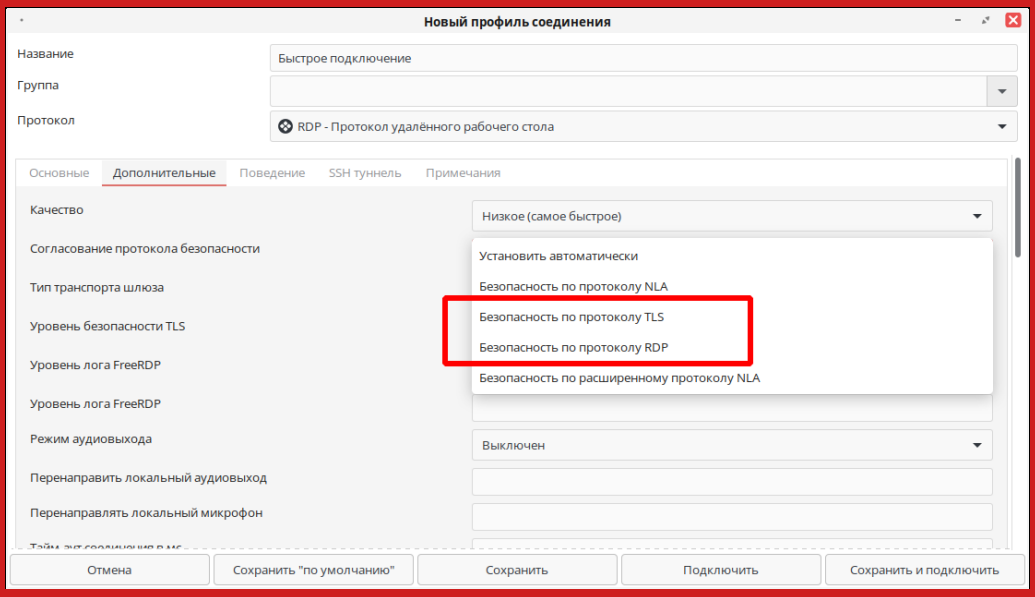
Для установки соединения нажмите на кнопку «**Добавить новый профиль соединения**». Откроется окно создания соединения, где вам нужно выбрать протокол **RDP** и заполнить поля «**Сервер**», «**Имя пользователя**» и «**Пароль**».



После заполнения полей нажмите на кнопку «**Сохранить**» - для сохранения настроек или на кнопку «**Сохранить и подключить**» - для сохранения настроек и подключения к удаленному рабочему столу.

ВАЖНО!

Если возникла проблема с закрытием **Remmina** при повторном подключении к windows-серверу по протоколу **RDP**, рекомендуется в настройках соединения на вкладке «**Дополнительные**» для параметра **Согласование протокола безопасности** использовать «**Безопасность по протоколу TLS**» или «**Безопасность по протоколу RDP**».

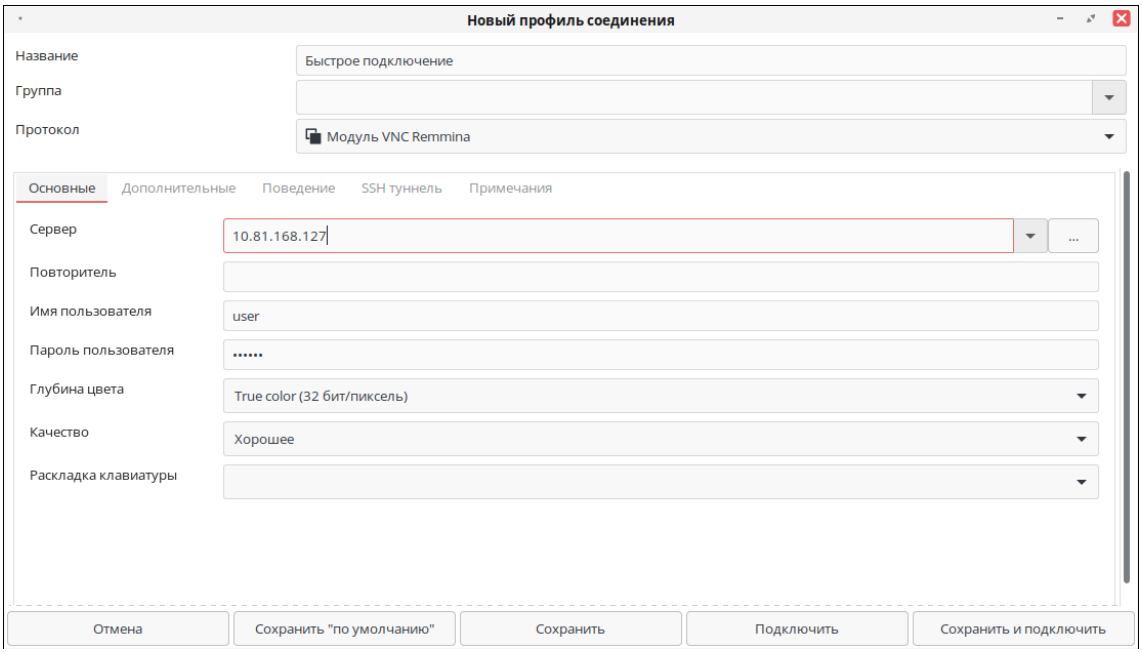


Для подключения по протоколу безопасности **TLS** может понадобится снять чекбокс «**Разрешить подключение только с компьютеров, на которых работает удалённый рабочий стол с проверкой подлинности на уровне сети**» в дополнительных параметрах windows-сервера.

Для подключения по протоколу безопасности **RDP** на windows-сервере требуется поменять регистр **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer** на **0**.

Установка подключения к x11vnc-серверу с использованием протокол VNC

В новом профиле соединения из выпадающего списка параметра «**Протокол**» выберите «**Модуль VNC Remmina**». Также заполните поля «**Имя пользователя**» и «**Пароль**». В поле «**Сервер**» впишите IP-адрес хоста вашей машины и порт VNC.



Для подключения нажмите на кнопку «**Подключить**» или «**Сохранить и подключить**».

Решение возникающих проблем

В случае возникновения ошибок в Remmina при повторном подключении к Windows-серверу необходимо проверить используемый протокол безопасности в параметре «**Согласование протокола безопасности**», скорее всего параметр имеет значение «**Безопастность по протоколу NLA**».

Для решения данной проблемы значение параметра следует установить «**Безопасность по протоколу TLS**» или «**Безопасность по протоколу RDP**».

> **Примечание.**
>
> Данные протоколы безопасности должны поддерживаться на вашем Windows-сервере.

Если использование других протоколов безопасности невозможно, рекомендуется использовать **xfreerdp-gui**. Подробную информацию о настройке подключения через **xfreerdp-gui** см. в нашей инструкции «xfreerdp_gui — графическая оболочка для работы с freerdp».

Утилита удаленного запуска графических приложений xpra

Установка
Основные возможности
Запуск приложения
Запуск новой графической сессии
Получение управления запущенной графической сессией на удаленной машине
TCP-сокеты
Графический интерфейс xpra

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** xpra-5.0.8-1

Утилита **xpra** — инструмент, который запускает программы X11, обычно на удаленном хосте, и направляет их отображение на локальный компьютер без потери состояния. Предоставляет удаленный доступ как отдельным приложениям, так и новым или существующим сеансам рабочего стола.

На сервере утилита **xpra** в режиме демона запускает программу с заданным идентификатором сеанса, а на клиенте происходит присоединение к этому сеансу с идентификатором.

Доступ к сеансам можно получить по **SSH** или через защищенные паролем обычные TCP-сокеты с SSL или без него.

Установка

Для установки утилиты **xpra** в РЕД ОС 7.3 на сервере и на клиенте перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду в терминале:

```
dnf install xpra
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Выйдите из сеанса суперпользователя **root**:

```
exit
```

После установки запуск утилиты доступен из «**Главного меню**» - «**Интернет**» - «**Xpra**» или через терминал командой:

```
xpra
```

Основные возможности

Просмотр списка запущенных xpra-серверов на текущей машине текущим пользователем осуществляется командой:

```
xpra list

Found the following xpra sessions:
/run/user/1000/xpra:
LIVE session at :0
LIVE session at :1
LIVE session at :2
LIVE session at :3
LIVE session at :4
LIVE session at :5
```

Остановка **xpra** на указанном дисплее (если сервер один, дисплей можно не указывать) осуществляется командой:

```
xpra stop :0
```

```
server requested disconnect:
server shutdown
xpra at :0 has exited.
```

Для остановки сервера на удаленной машине выполните команду:

```
xpra stop ssh://user@10.81.1.130/1

user@10.81.1.130's password:
server requested disconnect:
server shutdown
Sent shutdown command
```

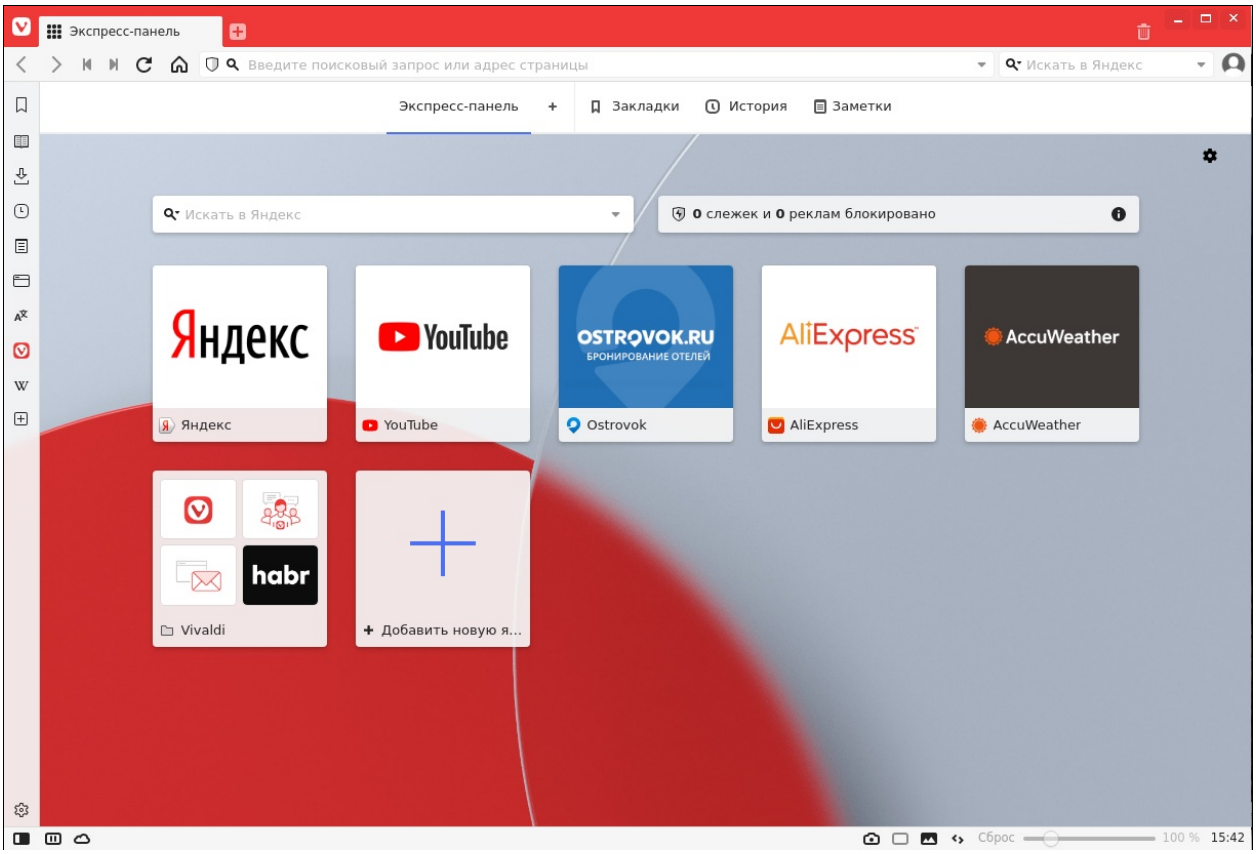
Для запуска **xpra** сервера на указанном дисплее выполните команду:

```
xpra start :1

using systemd-run to wrap 'start' server command
'systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' ':1' '--systemd-run=no'
Running scope as unit: run-rd9a968d02afd45c3b8da0197d39aea1e.scope
WARNING: low display number: 1
You are attempting to run the xpra server
against a low X11 display number: ':1'.
This is generally not what you want.
You should probably use a higher display number
just to avoid any confusion and this warning message.
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/:1.log.new
```

Запуск приложения

Для запуска приложения (на примере браузера **Vivaldi**) удалённо через **SSH** без предварительного запуска **xpra** на сервере, выполните команду:

```
xpra start ssh://user@10.81.1.130 --start="vivaldi"
```



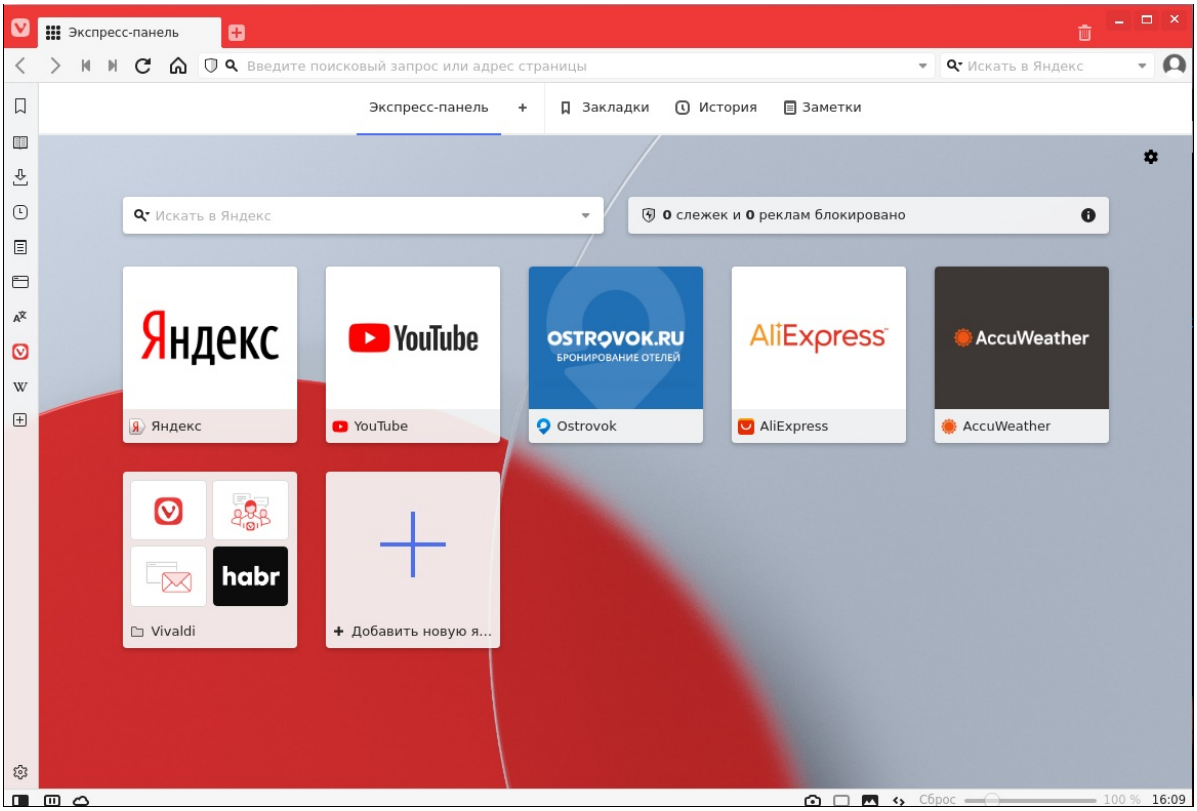
Далее будет рассмотрен запуск приложения (на примере браузера **Vivaldi**) с предварительным запуском **xpra**.

Запустите **xpra**, автоматически выберите дисплей и запустите программу:

```
xpra start --start=vivaldi

using systemd-run to wrap 'start' server command
'systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' '--start=vivaldi' '--systemd-run=no'
Running scope as unit: run-rbe185189832e44dab4cf2e624170b2b5.scope
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/S9507.log
Actual display used: :2
Actual log file name is now: /run/user/1000/xpra/:2.log
```

Подключение выполняется командой:

```
xpra attach ssh://user@10.81.1.130/2
```



Запуск новой графической сессии

Для запуска новой графической сессии на сервере необходимо запустить вложенный сервер **X11**, выполнив команду:

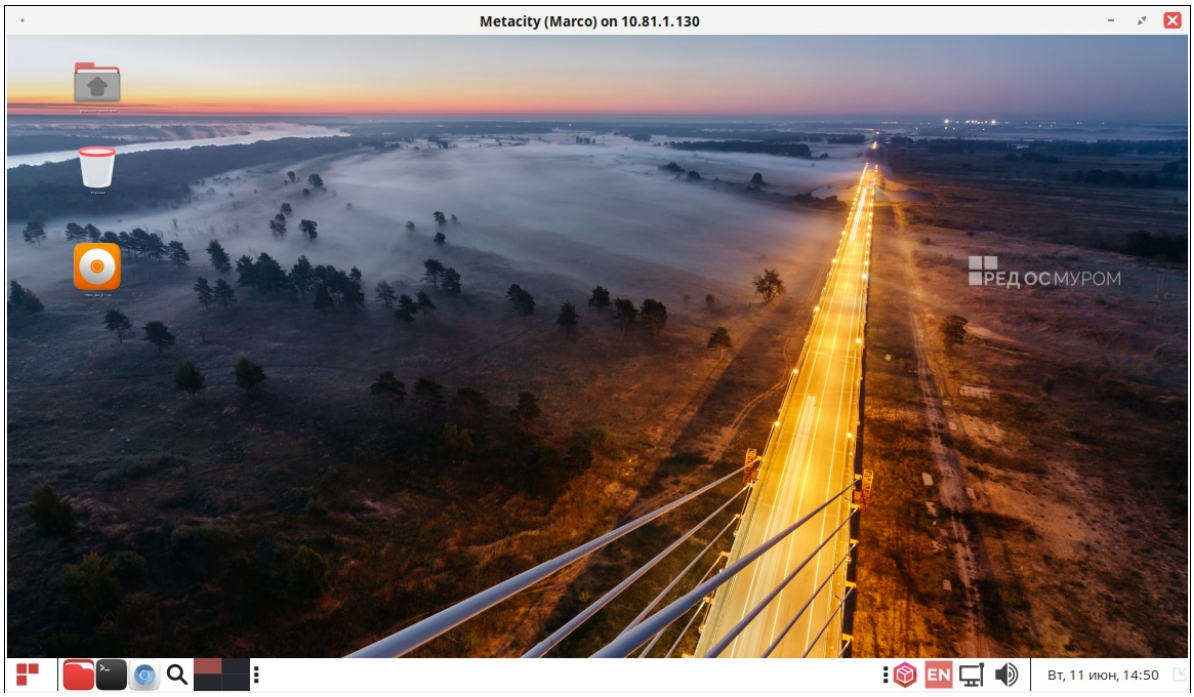
```
xpra start-desktop :1 --start-child=mate-session --exit-with-children=yes

using systemd-run to wrap 'start-desktop' server command
'systemd-run' '--description' 'xpra-start-desktop' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start-desktop' ':1' '--start-child=mate-session' '--exit-with-children=yes' '--systemd-run=no'
Running scope as unit: run-rd3c1ca4fcb5b42908297daef2392939c.scope
WARNING: low display number: 1
You are attempting to run the xpra server against a low X11 display number: ':1'.
This is generally not what you want.
You should probably use a higher display number just to avoid any confusion and this warning message.
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/:1.log.new
Actual log file name is now: /run/user/1000/xpra/:1.log
```

где:

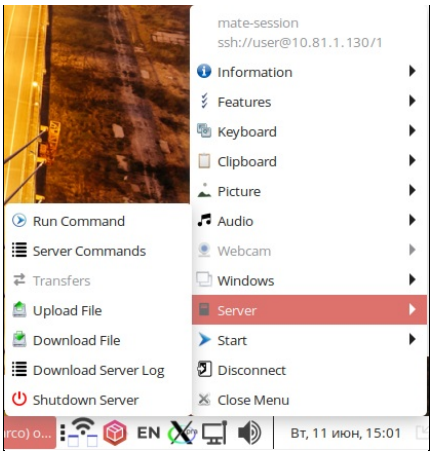
- **:1** — это номер сеанса отображения дисплея;
- **--start-child=mate-session** — запуск mate сессии как дочернего элемента на сервере **xpra**;
- **--exit-with-children=yes** — сервер будет закрыт после выхода из сессии (дочерний выход).

Подключение к графической сессии выполняется командой:

```
xpra attach ssh:user@10.81.1.130:1 --min-size=1200x800 --clipboard-direction=both --clipboard=yes
```



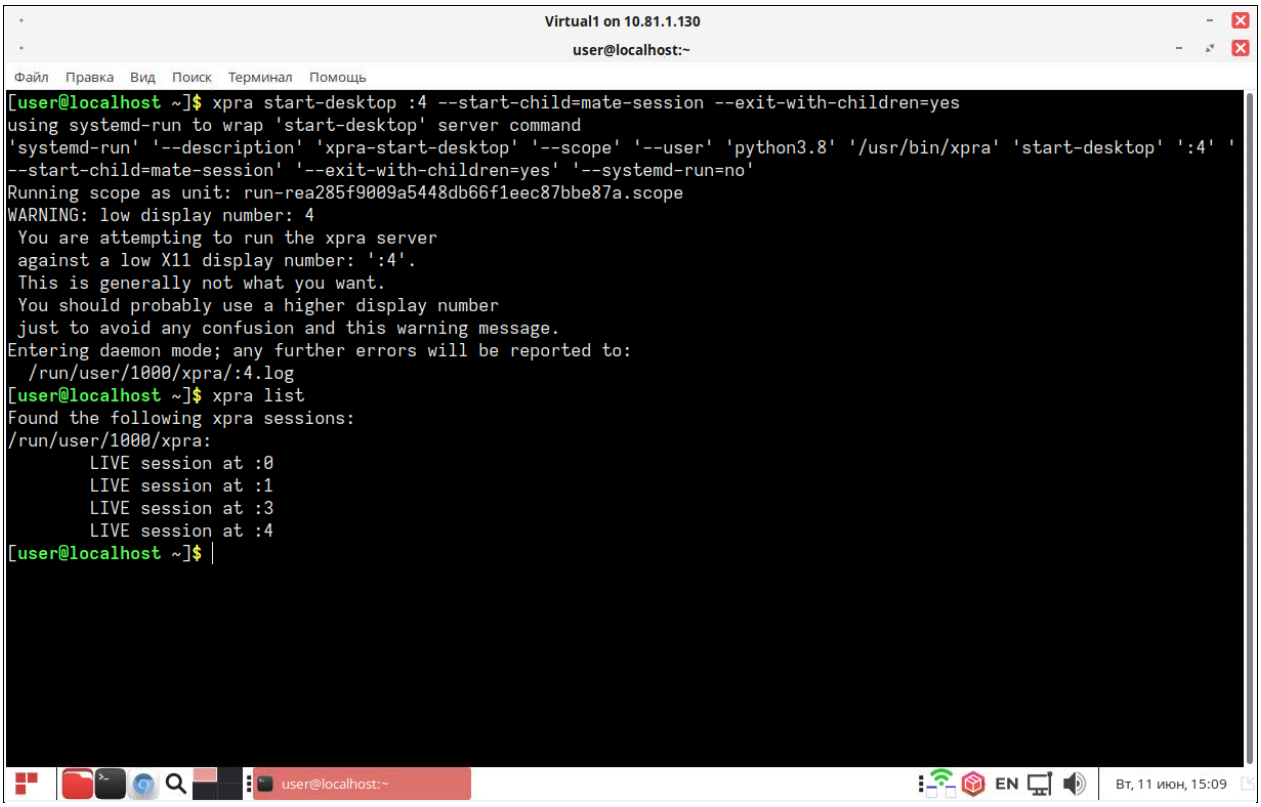
При подключении к серверу **xpra** в системном трее появится значок, где можно управлять подключением и изменять настройки.



Получение управления запущенной графической сессией на удаленной машине

Для удаленного запуска выполните команду:

```
xpra shadow --ssh=ssh ssh://user@10.81.1.130/0
```

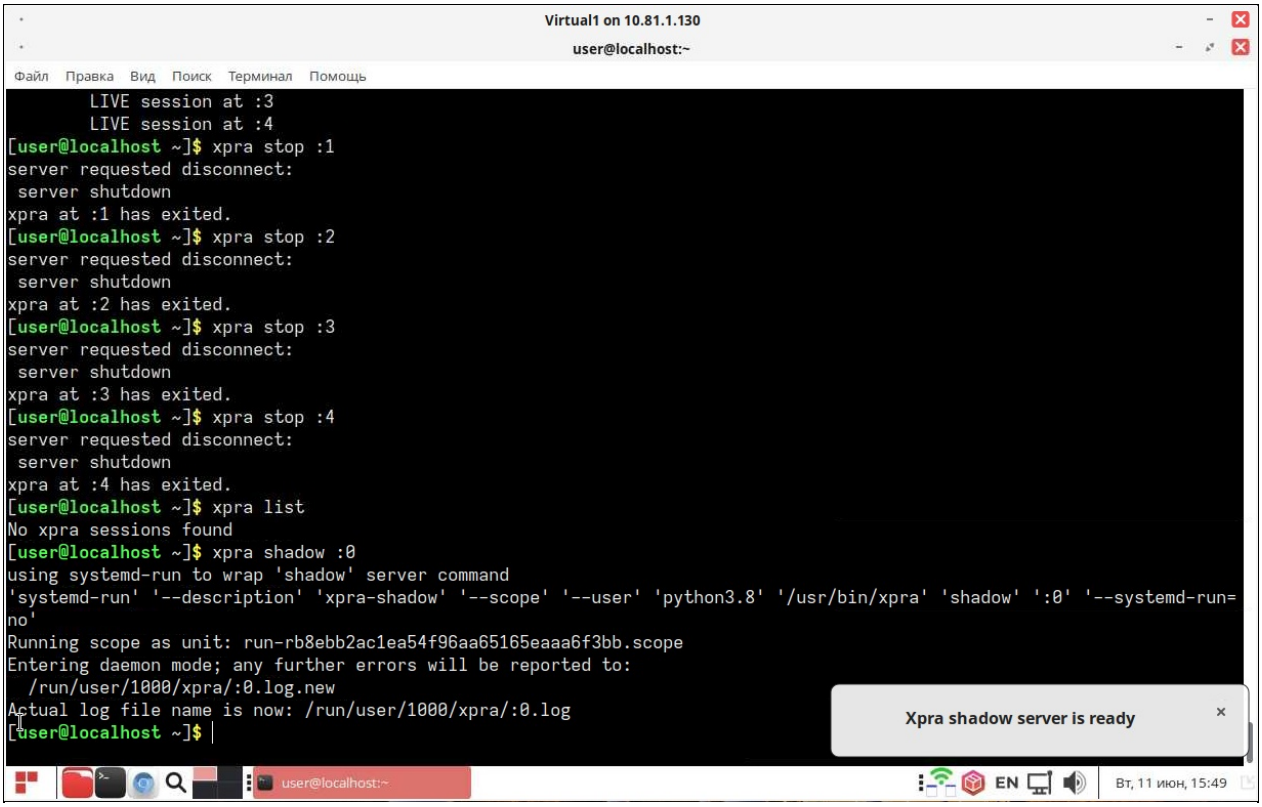


Для запуска на сервере выполните команду:

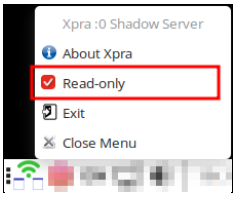
```
xpra shadow :0

using systemd-run to wrap 'shadow' server command
'systemd-run' '--description' 'xpra-shadow' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'shadow' ':0' '--systemd-run=no'
Running scope as unit: run-r711bde6c5e9143839c23798b8cdaea87.scope
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/:0.log.new
Actual log file name is now: /run/user/1000/xpra/:0.log
```

А также команду для подключения к серверу на удаленной машине:

```
xpra attach --speaker=no ssh://user@10.81.1.130
```



На сервере в трее появится значок, где «**Exit**» - остановить сервер, «**Read Only**» - запретить управление, разрешен только просмотр.



TCP-сокеты

Для запуска приложения (на примере браузера **Vivaldi**) на сервере выполните команду:

```
xpra start --start=vivaldi --bind-tcp=0.0.0.0:9878

using systemd-run to wrap 'start' server command
['systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' '--start=vivaldi' '--bind-tcp=0.0.0.0:9878' '--systemd-run=no']
Running scope as unit: run-r6a6a67cc4fb74ff18ae9e6f1dd7b16e3.scope
Entering daemon mode; any further errors will be reported to:
/run/user/1000/xpra/S12703.log
Actual display used: :1
Actual log file name is now: /run/user/1000/xpra/:1.log
```

Для управления запущенной графической сессией используется команда:

```
xpra shadow --bind-tcp=0.0.0.0:9878

using systemd-run to wrap 'shadow' server command
['systemd-run' '--description' 'xpra-shadow' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'shadow' '--bind-tcp=0.0.0.0:9878' '--systemd-run=no']
Running scope as unit: run-r2da092cb198b4764a93e72094bff097f.scope
Entering daemon mode; any further errors will be reported to:
 /run/user/1000/xpra/:0.log.new
Actual log file name is now: /run/user/1000/xpra/:0.log
```

Выполните подключение на удаленной машине командой:

```
xpra attach ws://10.81.1.130:9878
```

Адрес **10.81.1.130:9878** можно открыть в веб-браузере.

Для создания TCP-сеанса, начиная с версии **4.0.1**, с защитой паролем, выполните одну из приведенных команд:

```
XPRA_PASSWORD=<ваш_пароль> xpra start --bind-tcp=0.0.0.0:10000,auth=env
SOME_OTHER_ENV_VAR_NAME=<ваш_пароль> xpra start --bind-tcp=0.0.0.0:10000,auth=env:name=SOME_OTHER_ENV_VAR_NAME
xpra start --bind-tcp=0.0.0.0:10000,auth=password:value=<ваш_пароль>
```

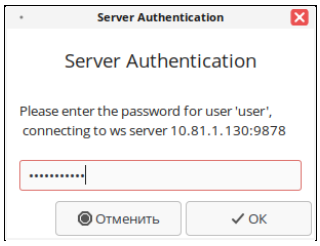
Например, команда для создания TCP-сеанса, защищенного паролем, с запуском текстового редактора **Pluma** будет выглядеть следующим образом:

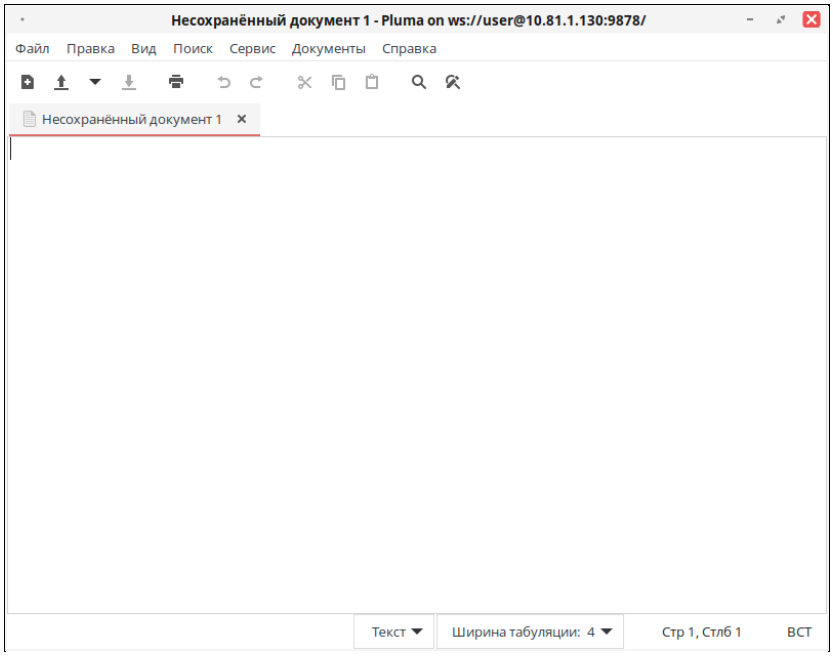
```
xpra start --start=pluma --bind-tcp=0.0.0.0:9878,auth=password:value=password123

using systemd-run to wrap 'start' server command
['systemd-run' '--description' 'xpra-start' '--scope' '--user' 'python3.8' '/usr/bin/xpra' 'start' '--start=pluma' '--bind-tcp=0.0.0.0:9878,auth=password:value=password123' '--systemd-run=no']
Running scope as unit: run-r46fa07c9510342e4a5b9938988201a52.scope
Entering daemon mode; any further errors will be reported to:
 /run/user/1000/xpra/S14277.log
Actual display used: :1
Actual log file name is now: /run/user/1000/xpra/:1.log
```

При подключении необходимо указать имя пользователя:

```
xpra attach ws:user@10.81.1.130:9878
```

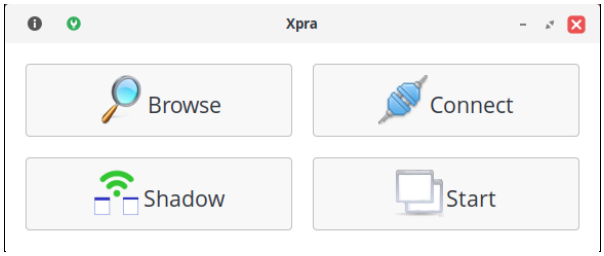
и по запросу ввести пароль:





Графический интерфейс xpra

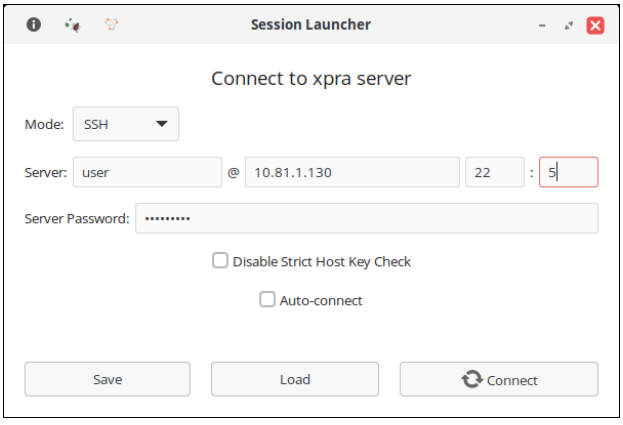
Графический интерфейс **xpra** доступен из «**Главного меню**» - «**Интернет**» - «**Xpra**».



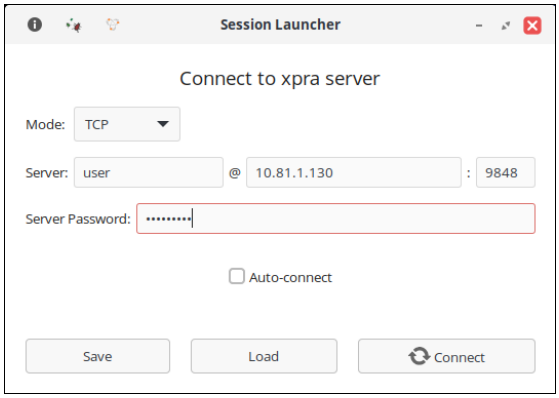
Здесь:

- «**Browse**» - просмотр списка, подключение к локальному дисплею.
- «**Shadow**» - предоставление доступа к рабочему столу.
- «**Connect**» - подключение к удаленному серверу.
- «**Start**» - запуск сервера **xpra**.

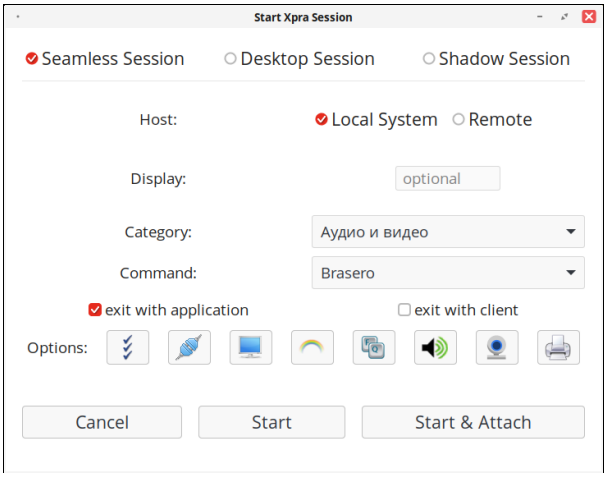
Настройка подключения по **SSH** выглядит следующим образом:



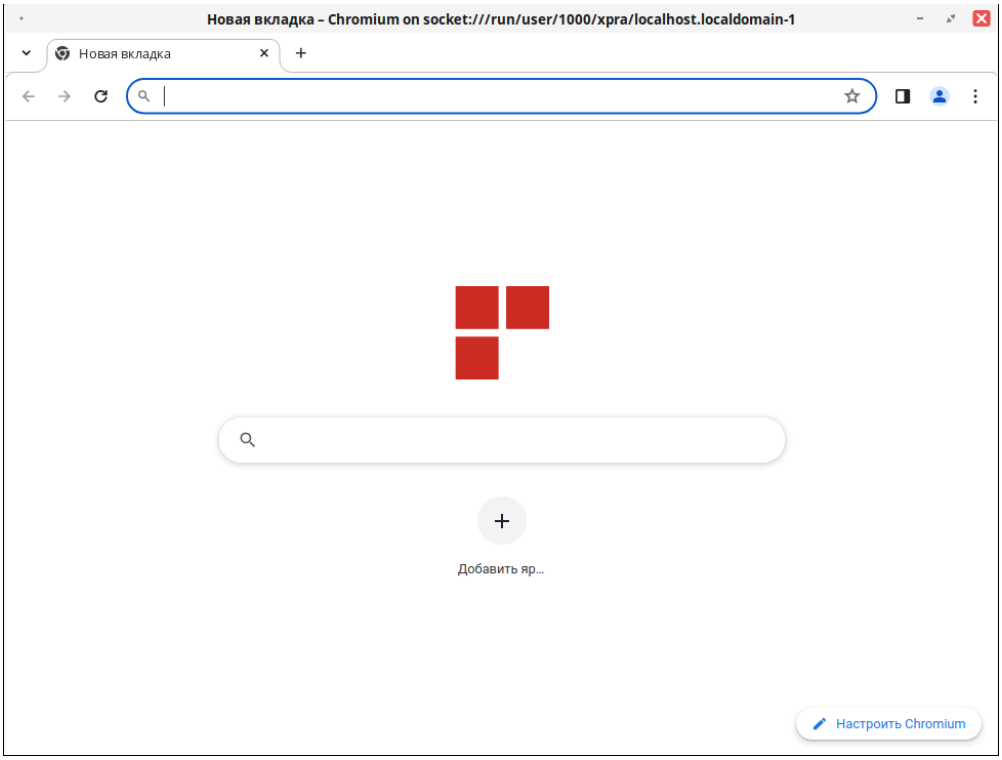
Настройка подключения по **TCP** выглядит следующим образом:



Запуск приложения в удаленной системе с отображением на локальном компьютере (на примере браузера **Chromium**):



Результат выполнения настройки:



Клиентская программа для работы с сетевыми протоколами PuTTY

Установка программы
Работа с программой
Авторизация по ключу SSH

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: putty-0.81

PuTTY — клиентская программа для удаленного подключения к серверам. **PuTTY** использует для работы такие безопасные сетевые протоколы, как *SSH*, *Telnet*, *SFTP*, *SCP* и др.

Программа применяется для администрирования удаленных машин.

К преимуществам программы можно отнести поддержку *IPv6*, поддержку аутентификации с открытым ключом и возможность работы через прокси-сервер.

Установка программы

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

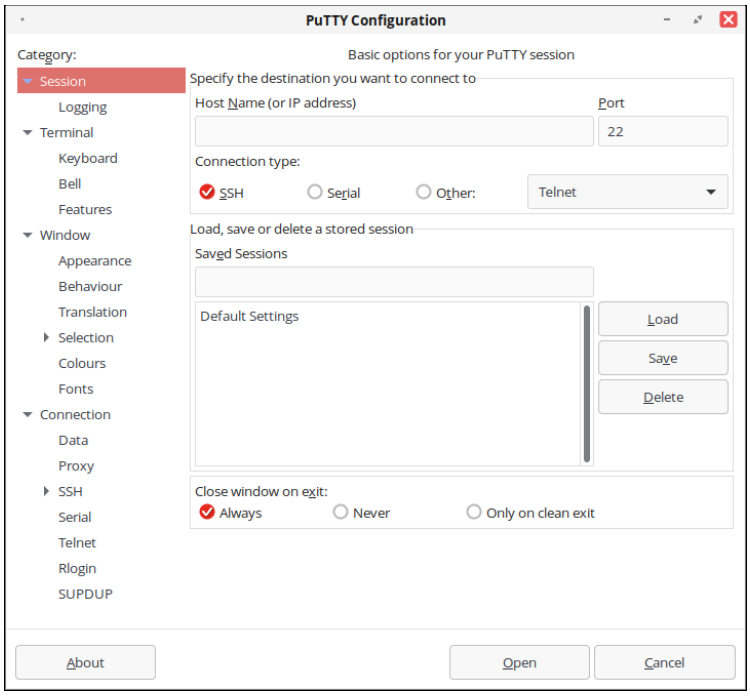
и выполните команду:

```
dnf install putty
```

После установки запуск программы доступен из «**Главного меню**» – «**Интернет**» – «**PuTTY**».

Работа в программе производится от **непривилегированного** пользователя.

Главное окно программы выглядит следующим образом:



Для настройки соединения доступны 4 основных раздела:

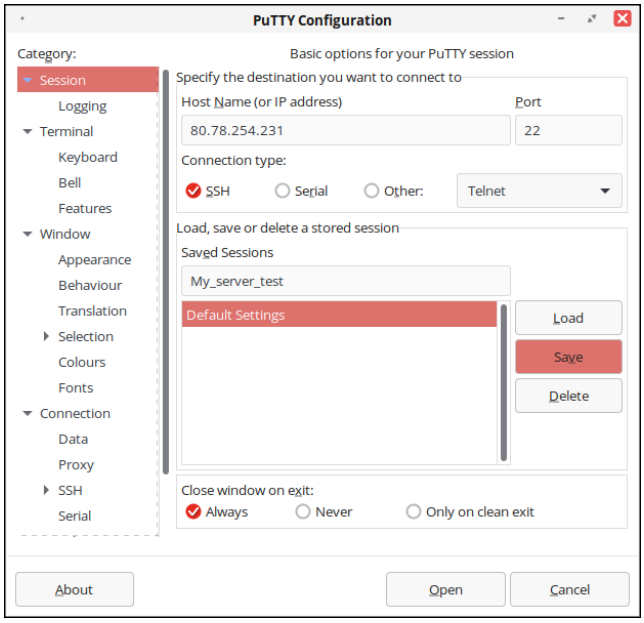
- Вкладка «**Session**» – необходима для ввода данных о подключаемом устройстве. Здесь можно указать порт, IP-адрес и другие параметры подключения. Чтобы при последующих подключениях не приходилось снова вносить информацию, ниже расположен блок, куда можно сохранить параметры текущего подключения;
- Вкладка «**Terminal**» – предназначена для включения или отключения возможностей терминала;

- Вкладка «**Window**» – предназначена для настройки визуальных параметров: облик окна, шрифт, цвет элементов и т. д.
- Вкладка «**Connection**» – предназначена для настройки параметров подключения, ключей аутентификации и других значений.

Работа с программой

В примере для подключения к удаленному серверу будет использоваться протокол **SSH** с портом по умолчанию – **22**.

Для начала сессии нажмите «**Open**».

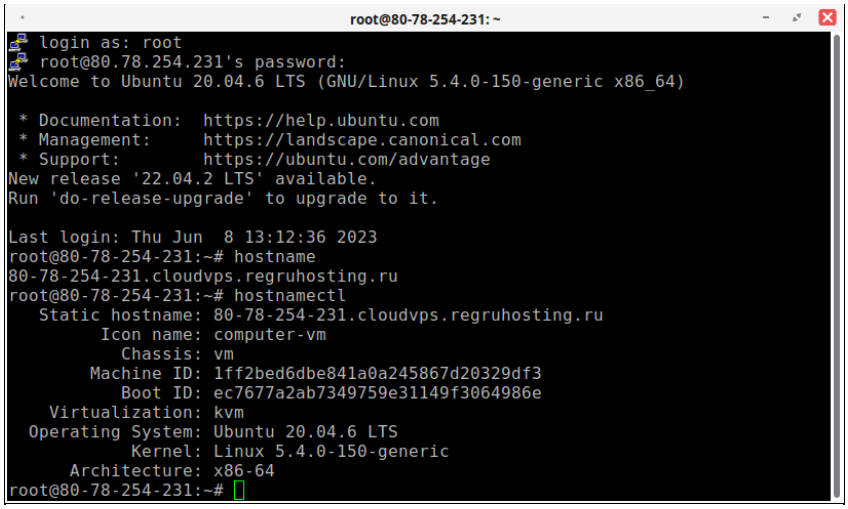


Если удаленный сервер доступен, и данные для подключения указаны корректно, откроется окно консоли, где необходимо указать *логин* и *пароль* для подключения.



После успешной авторизации можно начинать работу на удаленном сервере.

Для примера будет выполнена команда hostname для отображения информации о сервере.



Авторизация по ключу SSH

Для повышения безопасности подключения возможно настроить подключение по публичному ключу.

Для этого необходимо выпустить пару ключей – *публичный* и *приватный*, приватный будет храниться на клиентской машине, а публичный – на удаленном сервере. Важно помнить, что приватный ключ не должен передаваться третьим лицам.

Для создания ключа на клиентской машине выполните команду:

```
ssh-keygen
```

Будет выведен запрос на указание места хранения ключа, можно оставить каталог по умолчанию **~/.ssh/**. После выполнения команды будут сгенерированы два ключа – приватный **id_rsa** и публичный **id_rsa.pub**.

Приватный ключ можно защитить дополнительным шифрованием, указав пароль, однако в таком случае для его использования необходимо будет каждый раз вводить пароль, что не всегда удобно.

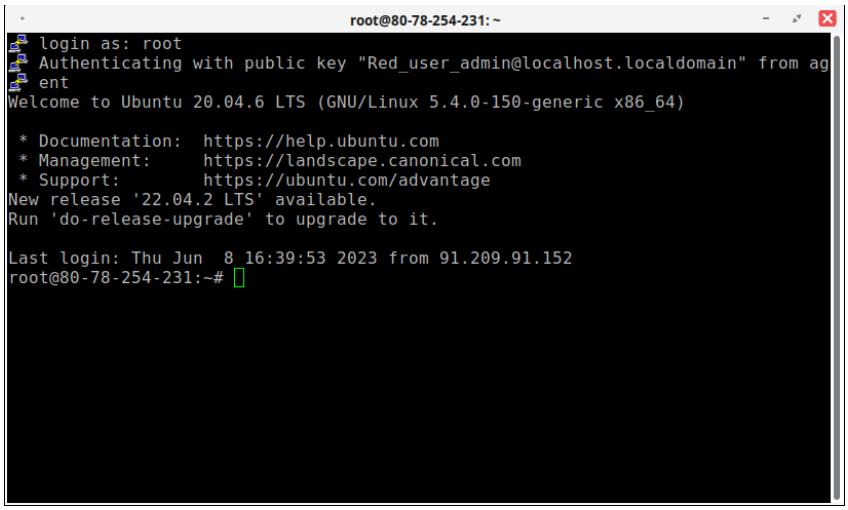
После создания ключей необходимо скопировать публичный ключ на удаленный сервер командой:

```
ssh-copy-id -i <путь_до_ключа> <имя_пользователя>@<IP-адрес_сервера>
```

Например:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@80.78.254.231
```

После этого при подключении к удаленному серверу авторизация будет проходить мгновенно.



Дополнительно для повышения безопасности подключения на удаленном сервере рекомендуется отключить авторизацию по паролю.

Для отключения авторизации по паролю на удаленном сервере откройте файл конфигурации **/etc/ssh/sshd_config** и измените значение параметра `PasswordAuthenticatin yes` на `PasswordAuthenticatin no`, сохраните файл.

Для применения изменений перезагрузите службу **sshd** на удаленном сервере:

```
systemctl reload sshd
```

AnyDesk

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: anydesk-6.3.3-1

AnyDesk предоставляет удаленный доступ к рабочим столам на базе Linux, Windows, MacOS, Android и др.

Скачать AnyDesk для личного пользования можно на официальном сайте.

Для РЕД ОС нужно перейти в «**Другие версии**» и выбрать версию **anydesk-6.3.3-1.el8.x86_64.rpm**.

Вы можете подробнее ознакомиться со средствами удаленного доступа в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Средства удалённого доступа;
- в **Яндекс.Дзен** — Средства удалённого доступа;
- в **VK Видео** — Средства удалённого доступа.

На наших каналах вы также сможете найти много другой полезной информации.

1. Перейдите в сеанс пользователя root:

```
su -
```

2. Перейдите в папку с дистрибутивом (в качестве примера /home/user/Загрузки/):

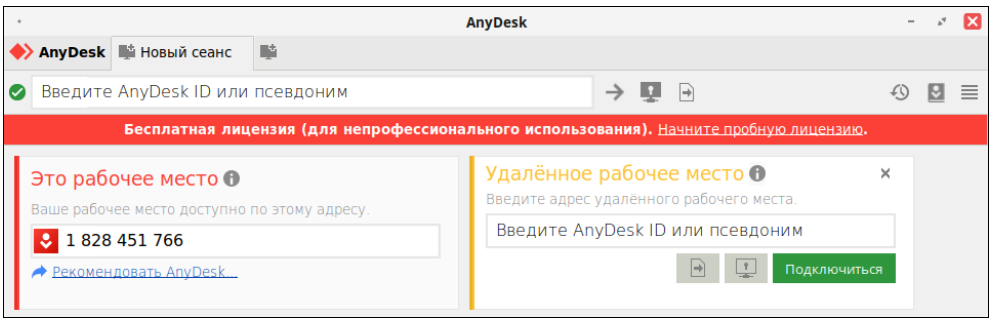
```
cd /home/user/Загрузки/
```

3. Выполните установку:

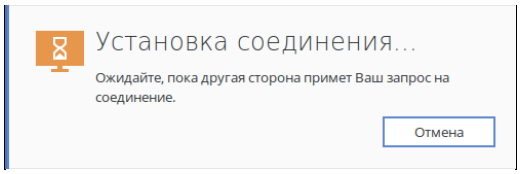
```
dnf install anydesk-6.3.3-1.el8.x86_64.rpm
```

Для запуска Anydesk откройте «**Главное меню**» — «**Интернет**» — «**Anydesk**».

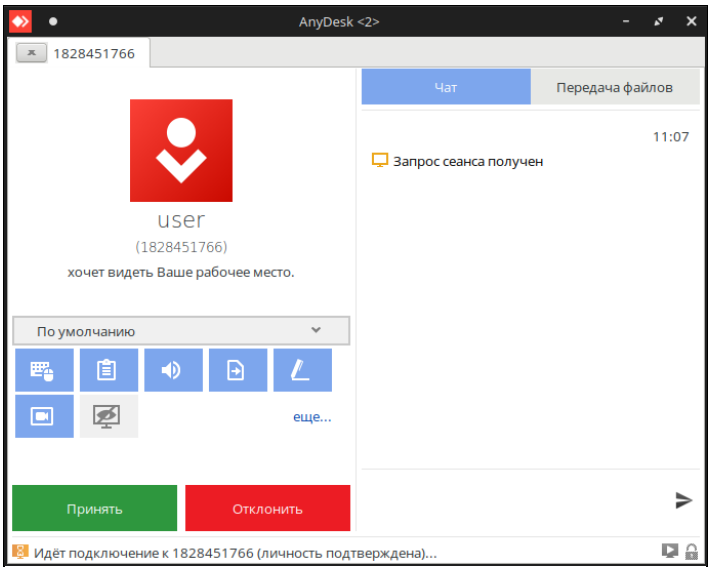
В интерфейсе AnyDesk имеется два основных пункта: адрес вашего компьютера, по которому можно подключится к вашему экрану, и поле для ввода адреса другого компьютера для подключения.



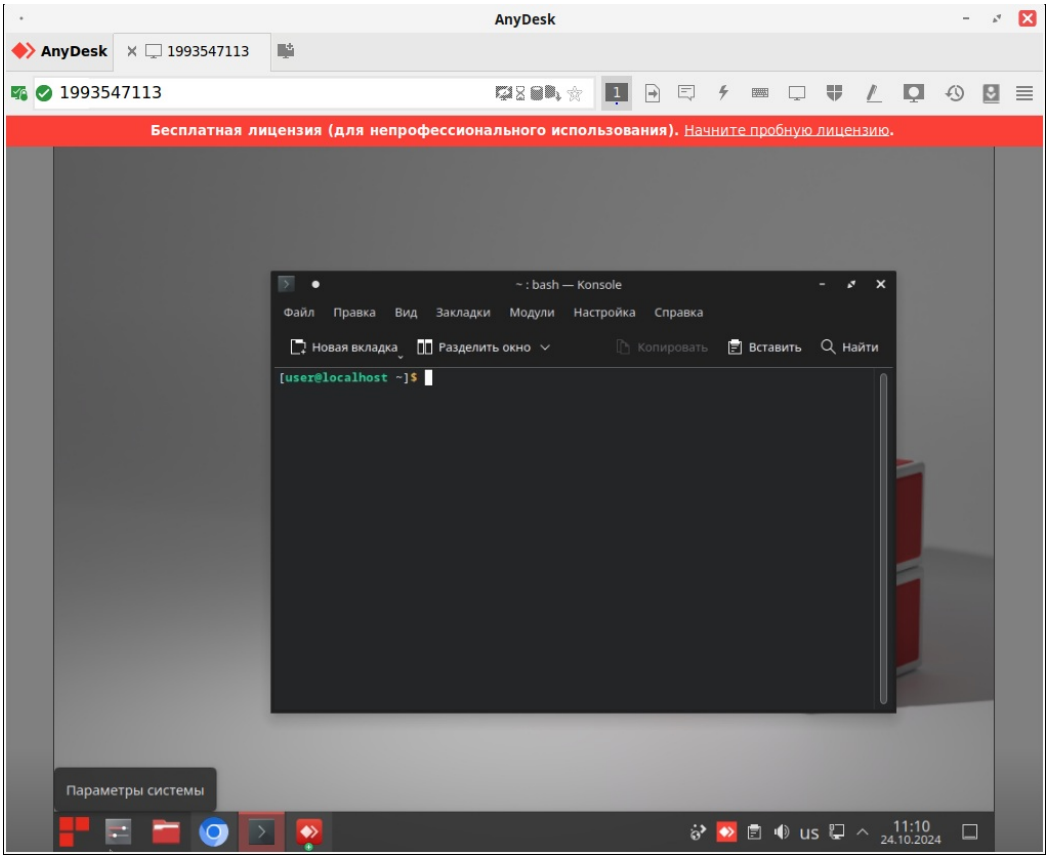
После ввода адреса для подключения нужно будет подтвердить это с компьютера, к которому вы подключаетесь.



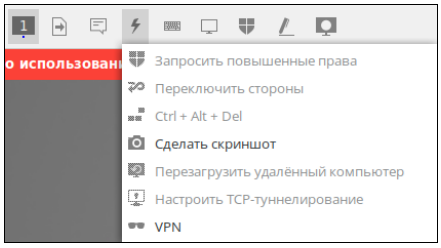
В окне подтверждения можно настроить чем удаленно можно будет управлять.



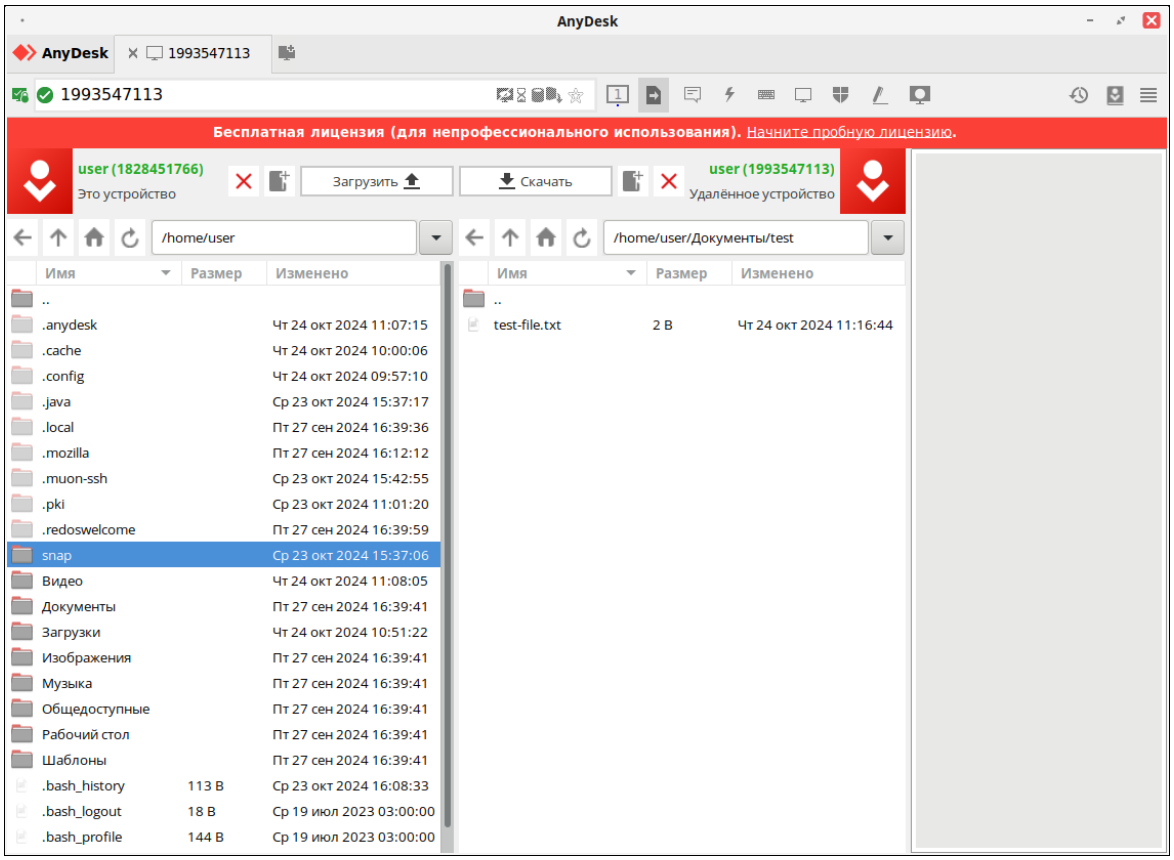
Когда доступ будет получен, сразу же откроется окно с удаленным доступом.



На верхней панели предоставлены дополнительные функции: запись экрана, чат с удаленным компьютером, смена раскладки, перезагрузка компьютера и другое.



Одной из важных функций является встроенный файловый менеджер, с помощью которого можно обмениваться файлами с удаленным компьютером.


AnyDesk
AnyDesk
1993547113
1993547113
Бесплатная лицензия (для непрофессионального использования). Начните пробную лицензию.
user (1828451766)
Это устройство
Загрузить
Скачать
user (1993547113)
Удалённое устройство
/home/user
/home/user/Документы/test
Имя
Размер
Изменено
..
.anydesk Чт 24 окт 2024 11:07:15
.cache Чт 24 окт 2024 10:00:06
.config Чт 24 окт 2024 09:57:10
.java Ср 23 окт 2024 15:37:17
.local Пт 27 сен 2024 16:39:36
.mozilla Пт 27 сен 2024 16:12:12
.muon-ssh Ср 23 окт 2024 15:42:55
.pki Ср 23 окт 2024 11:01:20
.redoswelcome Пт 27 сен 2024 16:39:59
snap Ср 23 окт 2024 15:37:06
Видео Чт 24 окт 2024 11:08:05
Документы Пт 27 сен 2024 16:39:41
Загрузки Чт 24 окт 2024 10:51:22
Изображения Пт 27 сен 2024 16:39:41
Музыка Пт 27 сен 2024 16:39:41
Общедоступные Пт 27 сен 2024 16:39:41
Рабочий стол Пт 27 сен 2024 16:39:41
Шаблоны Пт 27 сен 2024 16:39:41
.bash_history 113 B Ср 23 окт 2024 16:08:33
.bash_logout 18 B Ср 19 июл 2023 03:00:00
.bash_profile 144 B Ср 19 июл 2023 03:00:00
Имя
Размер
Изменено
..
test-file.txt 2 B Чт 24 окт 2024 11:16:44

МойАссистент

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: МойАссистент - 5.1

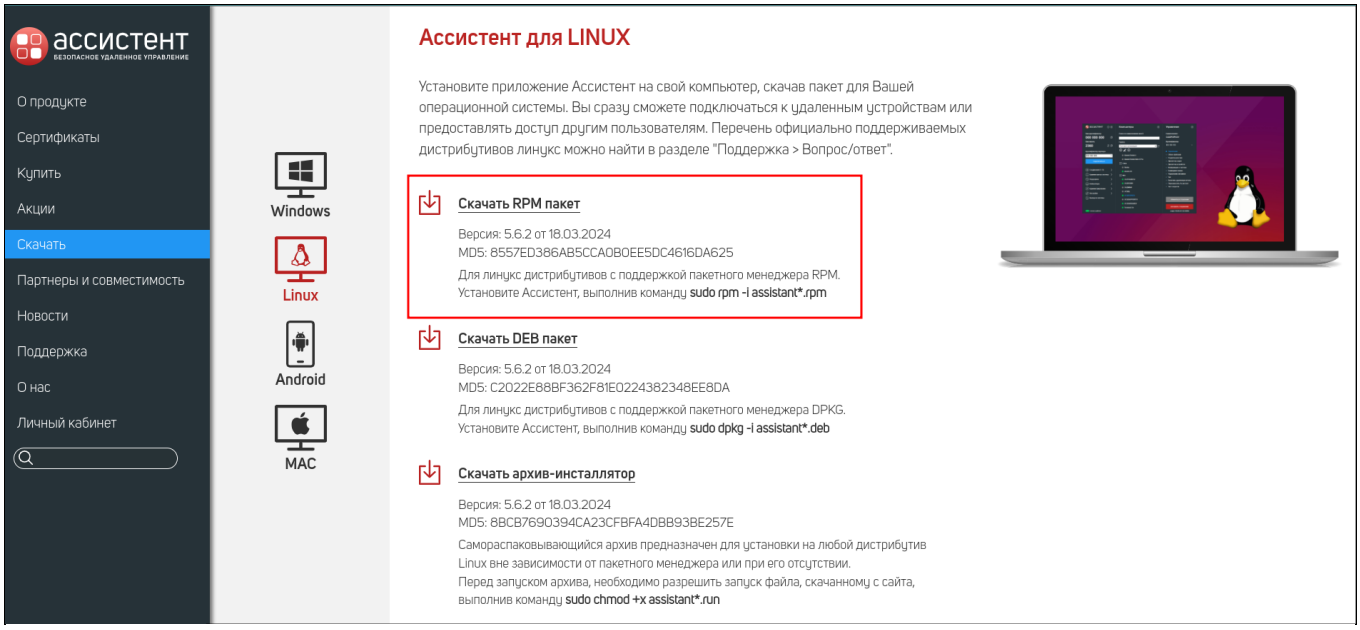
МойАссистент — это удобный и безопасный инструмент, для решения задач удаленного доступа, управления и администрирования.

Вы можете подробнее ознакомиться со средствами удаленного доступа в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Средства удалённого доступа;
- в **Яндекс.Дзен** — Средства удалённого доступа;
- в **VK Видео** — Средства удалённого доступа.

На наших каналах вы также сможете найти много другой полезной информации.

Для того чтобы установить приложение **МойАссистент**, необходимо перейти на сайт https://мойассистент.рф/, в раздел «**Скачать**» - «**Linux**» и выбрать RPM-пакет.



Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

Откройте терминал и перейдите в каталог со скачанным файлом (в примере **/home/user/Загрузки**):

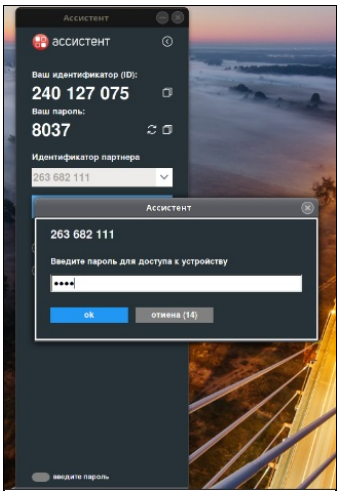
```
cd /home/user/Загрузки/
```

Установите МойАссистент командой:

```
dnf install assistant-5.1-0.x86_64.rpm
```

Для запуска программы в графическом режиме перейдите в «**Главное меню**» - «**Интернет**» - «**Ассистент**».

Для подключения к удалённому ПК, на котором установлен **МойАссистент**, введите «**Идентификатор партнера**», пароль и выполните подключение.


Ассистент
ассистент
Ваш идентификатор (ID):
240 127 075
Ваш пароль:
8037
Идентификатор партнера
263 682 111
Ассистент
263 682 111
Введите пароль для доступа к устройству
ok
отмена (14)
введите пароль

LiteManager

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: LiteManager - 5105

LiteManager Pro/Free — программа удаленного управления компьютерами через Интернет или администрирования в локальной сети.

Программа позволяет легко и быстро управлять рабочим столом компьютера в режиме реального времени, полностью поддерживая Windows, предоставляет надежный удаленный доступ к файловой системе, процессам и сервисам компьютера. **LiteManager** обладает встроенными функциями создания сетевой карты, сбора технической информации, возможностью развертывания и обновления с помощью средств удаленной установки, настройка своего личного ID-роутера (**NOIP**) и многое другое.

Удаленное администрирование теперь возможно и без IP-адреса, с помощью соединения по **ID** вы сможете сами выбирать свой личный уникальный **ID** и подключаться по нему. Клиентский и серверный модули программы способны работать в сетях, подключенных к Интернету через прокси-сервер.

Особенности:

1. Управление клавиатурой и мышью компьютера по сети. В отдельном окне видно удаленный рабочий стол контролируемого компьютера.
2. Управление удалённым компьютером возможно как с другого компьютера, так и с планшета или смартфона.
3. Серверная часть (для управляемого устройства) реализована для работы в среде операционных систем семейства Microsoft Windows. Версия для Linux, Mac OS реализована в тестируемой версии 5.0.
4. Клиентская часть (для управляющего устройства) реализована для Windows, Android, Mac OS, iOS, iPhone, iPad.
5. Широкий спектр режимов работы программы — передача файлов, удаленный диспетчер задач, терминал, *Wake-On-LAN* и многое другое.
6. Несколько режимов удаленной установки.
7. Возможна работа программы и без установки, в т.ч. и с внешнего носителя.
8. Поддержка *Microsoft Remote Desktop Protocol* (RDP).
9. Поддержка мультимониторных систем.
10. Карта сети.
11. Текстовый и аудио-видео чат.
12. Работа через *http-/socks5-прокси*.
13. Каскадное подключение (работа через промежуточный сервер).
14. Управление компьютером через Интернет без IP-адреса (соединение по ID).
15. Возможность запуска личного NoIpServer.
16. Встроенная система запросов (*Helpdesk*).
17. Функция **Quick Support** при необходимости разового подключения к удаленному рабочему столу (распространяется автономным приложением).
18. Трансляция рабочего стола компьютера на мониторы других пользователей, для проведения конференций и обучения.
19. Для учебных заведений, создание и проведение тестов, опросов. Централизованная раздача и сбор файлов тестов.

Установка

Для установки данного приложения, перейдите на сайт производителя по ссылке и скачайте архив для Linux.

> **Примечание.**
>
> Все команды выполняются от локального пользователя.

Разархивируйте скачанный архив командой (в примере /home/user):

```
cd /home/user
```

```
unzip LiteManager_linux.zip
```

Для того чтобы запустить разархивированный **LiteManager**, необходимо дать файлу права. Для этого выполните следующую команду:

```
chmod 0755 LiteManager
```

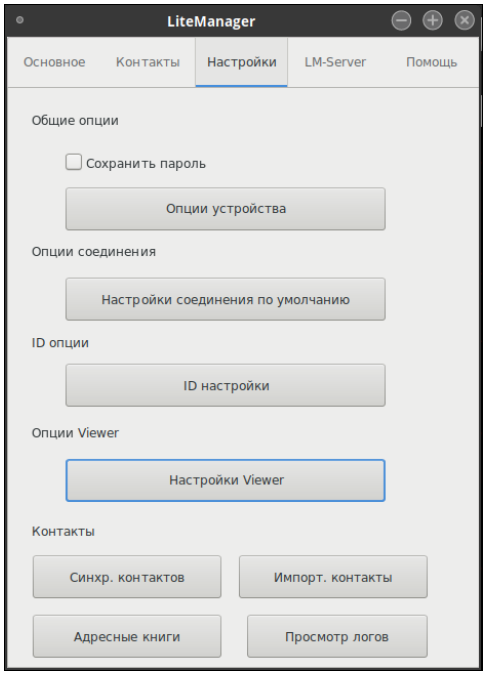
Запустите программу:

```
./LiteManager
```

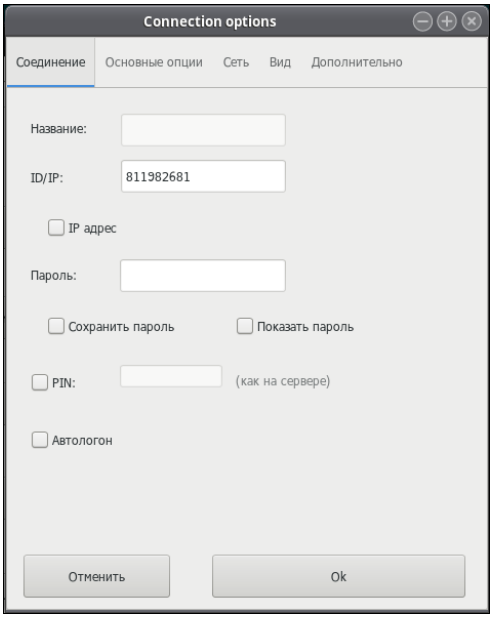
Настройка программы

Чтобы установить русский язык, перейдите в «**Settings**» - «**Viewer settings**» и поставьте галочку на «**Ru**».

Также в настройках клиента («**Настройки Viewer**») на вкладке «**Дополнительно**» вы можете защитить программу паролем, а на вкладке «**Сеть**» настроить прокси-сервер.



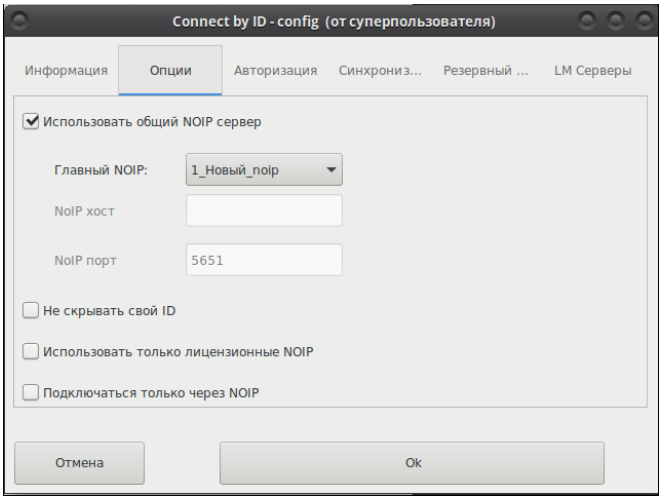
В настройках программы также можно установить «**Соединение по умолчанию**», выбрать основные и дополнительные опции и настроить внешний вид.



Для настройки соединения необходимо ввести **ID/IP** и пароль в соответствующие поля и нажать «**Ok**», после чего при выходе из программы введенные данные сохранятся.

Во вкладке «**Сеть**» можно выбрать порт и настроить **NoIP** и персональный прокси.

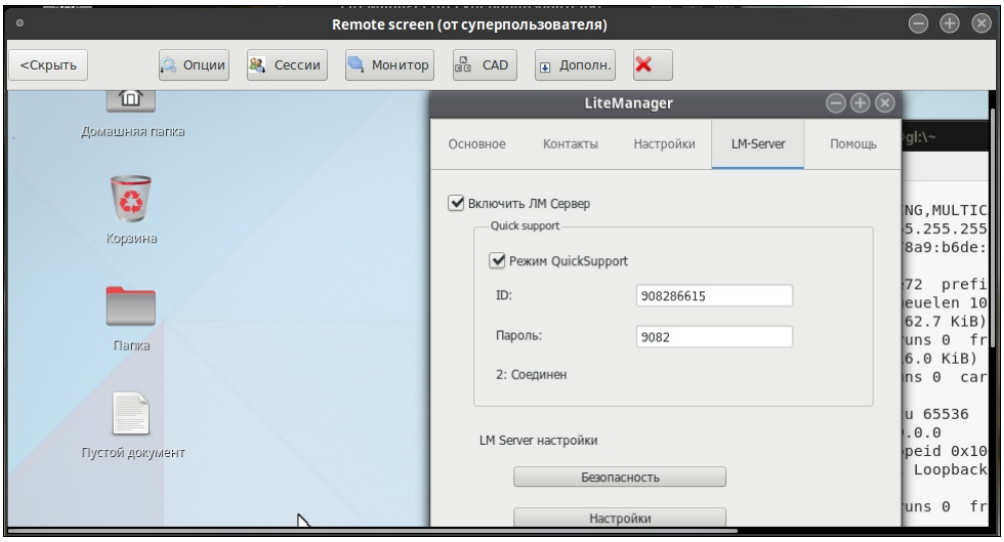
В «**Настройках ID**» можно просмотреть информацию и выбрать подходящий **NoIP**-сервер, настроить личный кабинет с авторизацией, настроить резервный **NoIP**-сервер, выбрать **LM**-сервер.



Работа с LiteManager

Чтобы создать сессию, нужно зайти в «**LM**» - «**Server**» и поставить галочку на «**Включить ЛМ сервер**». После чего сообщить другому пользователю *ID* и *пароль*.

Для подключения к **LM**-серверу во вкладке «**Основное**» впишите **ID/IP** и *пароль*, выберите как хотите подключится и нажмите «**Соединение**».



После подключения вам будут доступны: опции (настройки обозревателя), выбор монитора, вкладка «**Дополнительно**» (возможность передачи комбинаций клавиш **Alt+Shift**, **Shift**, **Ctrl**, **Alt** и **F1-F12**) и кнопка завершения сессии.

RuDesktop

Возможности
Установка
Описание программы
Подключение по постоянному паролю
Подключение к удалённому рабочему столу
Последние сеансы
Избранное
Найдено
Адресная книга
Передача файлов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: rudesktop-2.6.1603

RuDesktop – это программа для удалённого доступа и управления конфигурациями конечных устройств. Она предоставляет широкие возможности для администрирования и контроля над рабочими станциями, ноутбуками и другими устройствами, позволяя оптимизировать рабочие процессы и повысить уровень безопасности. Программа входит в Реестр Российского программного обеспечения.

RuDesktop – это клиент-серверное приложение. **Клиент** – это приложение, которое устанавливается на удалённые (к которым подключаетесь) и локальные компьютеры (административные). **Сервер** обеспечивает соединение клиентов между собой через локальную или глобальную сеть, хранит адресные книги и списки сессий операторов, обеспечивает контроль активности операторов и процессы авторизации и лицензирования.

Возможности

1. **Совместная работа** – обеспечивает подключение к удалённым устройствам по схемам «*один ко многим*» и «*многие к одному*», обмен файлами, общение в текстовом чате для совместного решения задач.

2. **Адресная книга** – предоставляет быстрый доступ к устройствам, назначение удобных псевдонимов и тегов для всех устройств.

3. **Установка, обновление и удаление ПО** на удалённых устройствах и группах устройств – позволяет управлять ПО удалённого компьютера в ручном или автоматическом режиме через запуск скриптов или выполнение задач по политикам **RuDesktop**.

4. **Неограниченное количество управляющих устройств** и **защищённое соединение** – для передачи данных используется шифрованное соединение по протоколу **TLS**.

5. **Инвентаризация оборудования и ПО** – позволяет отслеживать изменения в конфигурации удалённых устройств.

6. **Логирование действий в syslog** – обеспечивает сохранение в журнал действия персонала на локальном сервере и передачу данных в автоматическом режиме во внутренние системы информационной безопасности (SIEM, СКУД и др.).

7. **Передача файлов** – скачивание и загрузка файлов доступны всем пользователям, даже в бесплатной версии.

8. **Интеграция с AD и LDAP** – управление структурой компании, правами доступа и автоматизация администрирования на основе групп AD.

9. **История подключений** – просмотр списка сессий для всех авторизованных устройств в личном кабинете, просмотр списка подключаемых устройств на главном экране приложения (последние сеансы).

Установка

Для установки **RuDesktop** в РЕД ОС выполните следующий алгоритм действий:

1. Скачайте **RuDesktop** на официальном сайте. В разделе Linux выберите дистрибутив РЕД ОС.



2. Перейдите в папку с дистрибутивом (например, /home/user/Загрузки/):

```
cd /home/user/Загрузки/
```

3. Выполните установку (потребуются права **администратора**):

```
sudo dnf install rudesktop-amd64.rpm
```

После установки программа будет доступна из «**Главного меню**» – «**Интернет**» – «**RuDesktop**».

Для запуска программы через терминал введите команду:

```
rudesktop
```

Описание программы

При первом запуске программы создаётся уникальный номер (**ID**) для компьютера. **ID** остаётся неизменным даже после перезапуска или переустановки программы и используется для подключения к вашему рабочему столу. **Пароль** создаётся временный и после перезапуска он изменяется.

В интерфейсе **RuDesktop** есть два основных раздела.

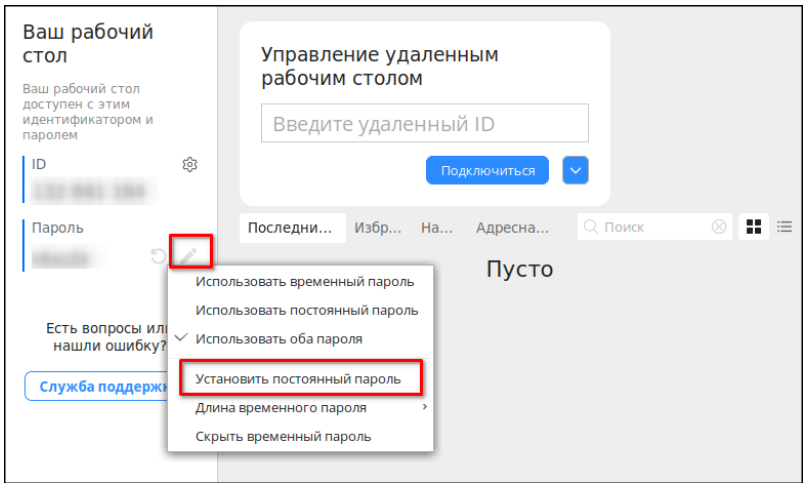
1. **Ваш рабочий стол** – содержит информацию об идентификаторе и пароле, с помощью которых можно подключится к вашему рабочему столу.

2. **Управление удаленным рабочим столом** – в этом разделе вы можете управлять удаленным рабочим столом после установления соединения.

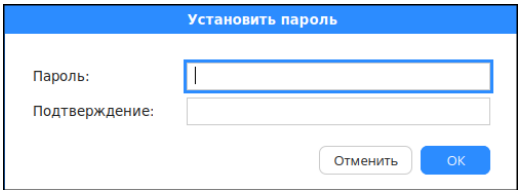
Подключение по постоянному паролю

Для обеспечения удобства администрирования компьютера через **RuDesktop** можно **установить** постоянный пароль на удалённом компьютере и **сохранить** его для подключения на компьютере администратора. Для этого выполните следующий алгоритм действий:

1. Установите постоянный пароль на удалённом компьютере. Для этого нажмите на значок редактирования рядом с паролем и из выпадающего списка выберите «**Установить постоянный пароль**».



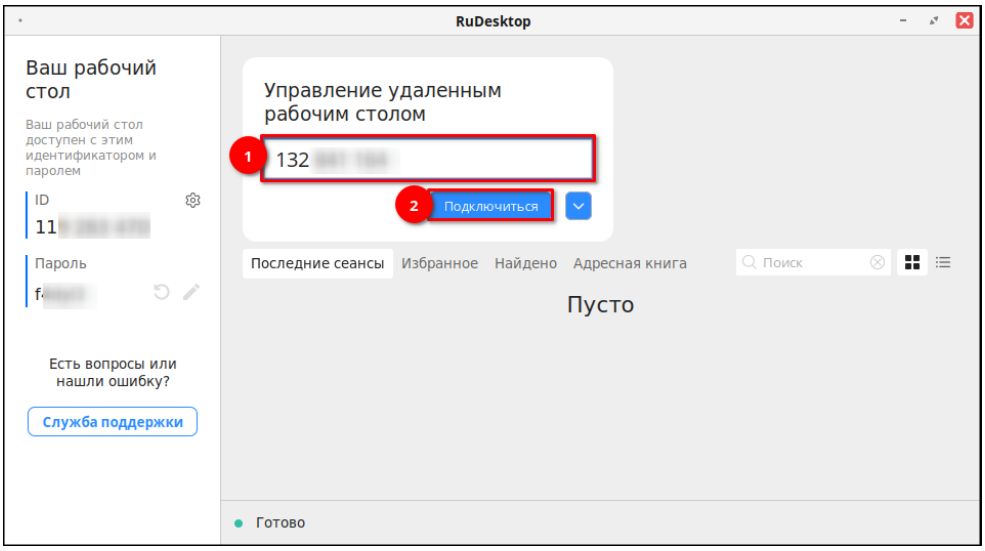
Установите сложный пароль. Нажмите «**OK**».



2. На компьютере администратора выберите адрес удалённого компьютера и введите указанный постоянный пароль для подключения. Это позволит администратору автоматически подключаться к управляемому компьютеру без необходимости каждый раз вводить пароль.

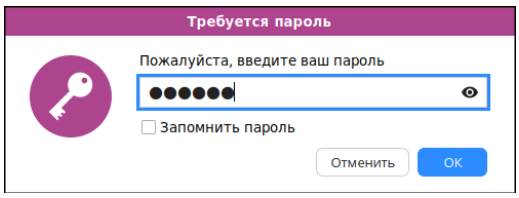
Подключение к удалённому рабочему столу

В разделе Управление удаленным рабочим столом введите **ID** удалённого компьютера (1) и нажмите кнопку «**Подключиться**» (2).

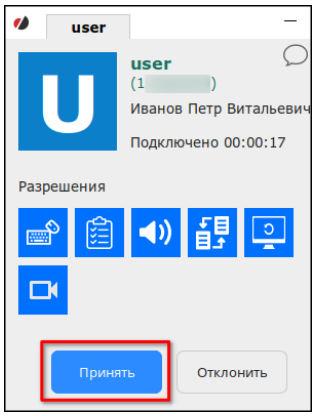


После ввода адреса для подключения вам потребуется подтвердить доступ к удалённому компьютеру, к которому вы пытаетесь подключиться.

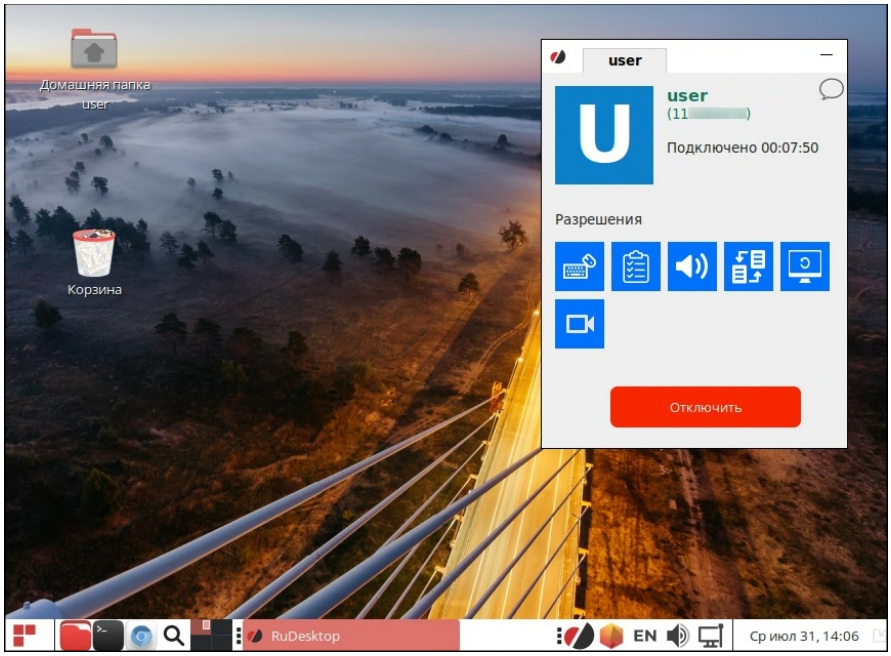
Если у вас имеется пароль для подключения к удалённому рабочему столу, введите его и нажмите «**OK**» для продолжения подключения. Если вы не хотите каждый раз вводить пароль, отметьте опцию «**Запомнить пароль**».



Если пароль неизвестен, ожидайте, пока пользователь подтвердит ваш запрос на подключение к его рабочему столу.



После установления соединения откроется удалённый рабочий стол управляемого компьютера.



Доступные разрешения при подключении:

- разрешить использование клавиатуры и мыши;

 - разрешить использование буфера обмена;

- разрешить передачу звука;

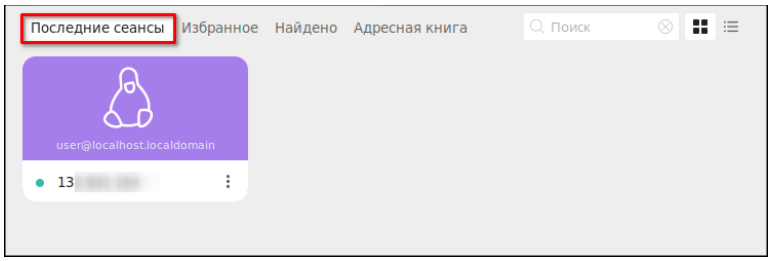
- разрешить копирование и вставку файлов;

 - разрешить удалённый перезапуск;

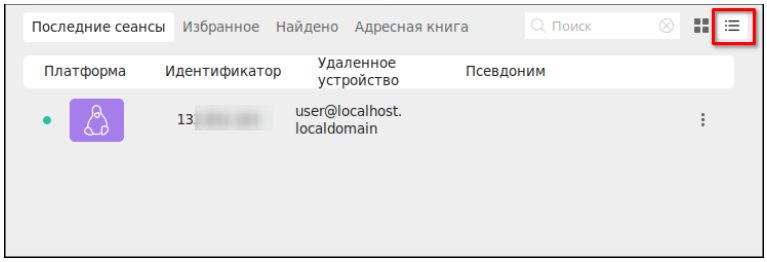
 - разрешить запись сессии.

Последние сеансы

На вкладке «**Последние сеансы**» отображаются недавние сеансы подключения пользователя.



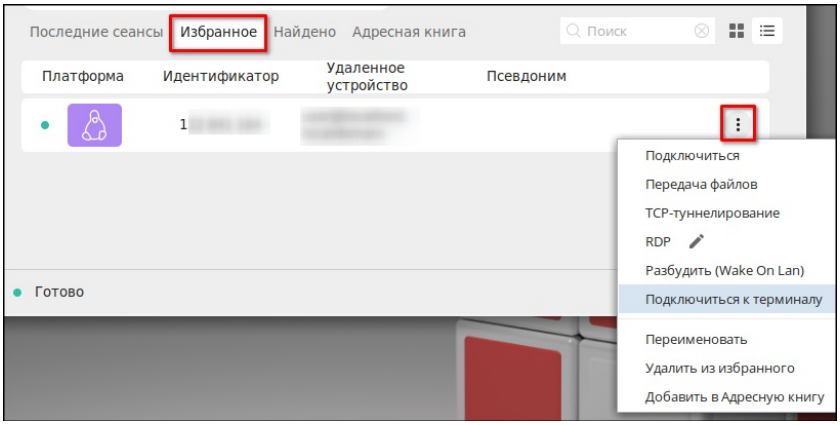
При переключении отображения (▫) последние сеансы подключений будут представлены в виде списка.



Рядом с каждым удаленным устройством доступны опции подключения, передачи файлов, удаления, добавления в адресную книгу. Выберите в выпадающем списке «**Добавить в избранное**» и удалённый рабочий стол будет отображён на вкладке « **Избранное**».

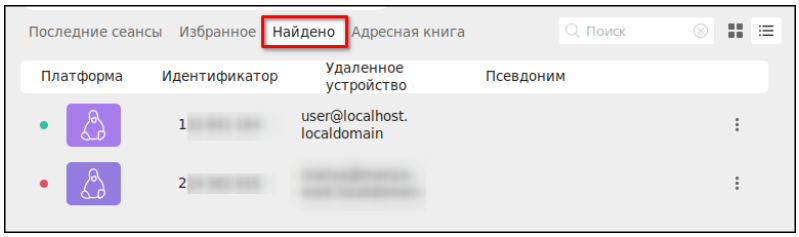
Избранное

На вкладке «**Избранное**» отображаются добавленные идентификаторы удалённых рабочих столов, которые пользователь выбрал для быстрого доступа или удобного отслеживания.



Найдено

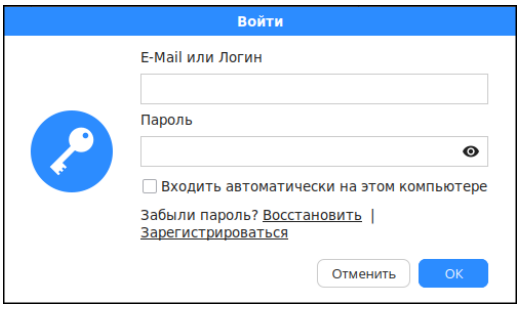
На вкладке «**Найдено**» в **RuDesktop** отображается список результатов поиска, который содержит информацию об удалённых устройствах, найденные в рамках запроса пользователя.



Для поиска нужного устройства воспользуйтесь строкой поиска и начните вводить необходимые значения идентификатора, псевдонима или наименования удалённого устройства. Алгоритм самостоятельно найдёт нужное устройство, опираясь на вводимые значения.

Адресная книга

Для использования адресной книги требуется создать учётную запись и войти в неё. Если у вас уже есть учётная запись **RuDesktop**, введите свой логин и пароль. В случае отсутствия учётной записи нажмите «**Зарегистрироваться**».

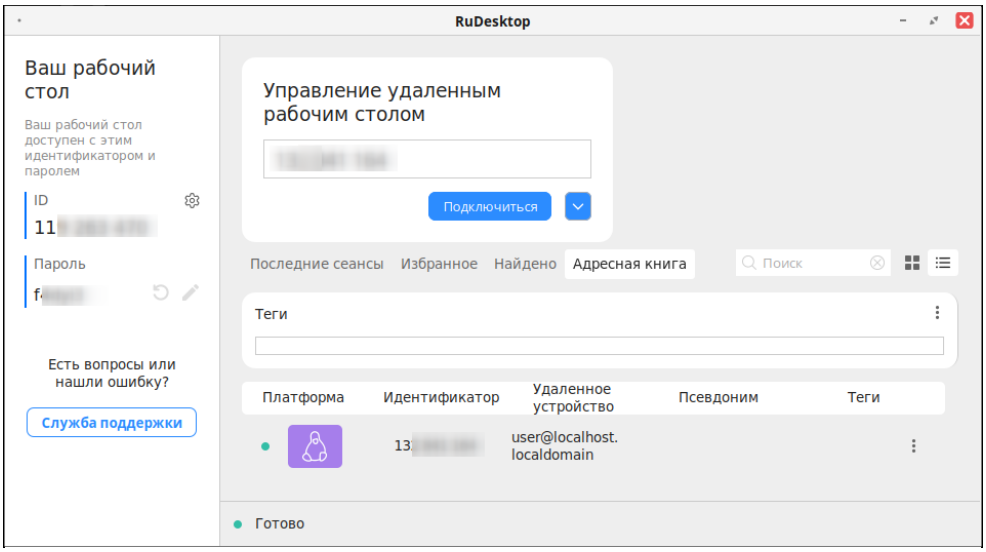


После открытия окна регистрации введите необходимые данные и зарегистрируйтесь.

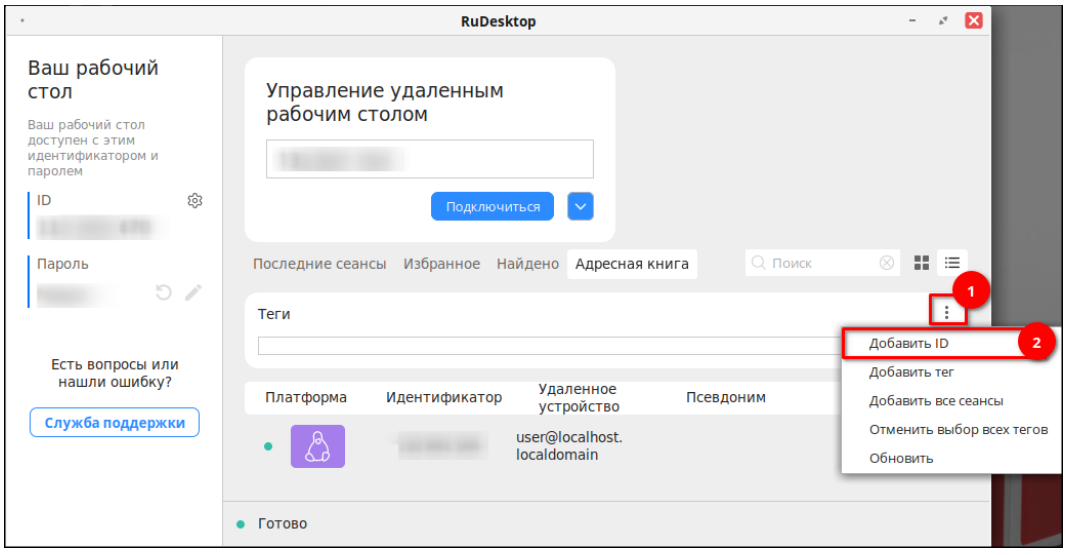
Далее будет отправлена инструкция на e-mail для активации учётной записи, и появится соответствующее сообщение.



Перейдите по ссылке в письме для завершения регистрации. После всех успешно выполненных действий вы сможете войти в систему.



Для добавления адресов удалённых рабочих столов нажмите на значок ⋮ и из раскрывающегося списка выберите «**Добавить ID**». Добавленное устройство будет отображено в адресной книге.



Передача файлов

Для осуществления обмена файлами между двумя удалёнными устройствами с помощью **RuDesktop** можно воспользоваться следующим алгоритмом действий:

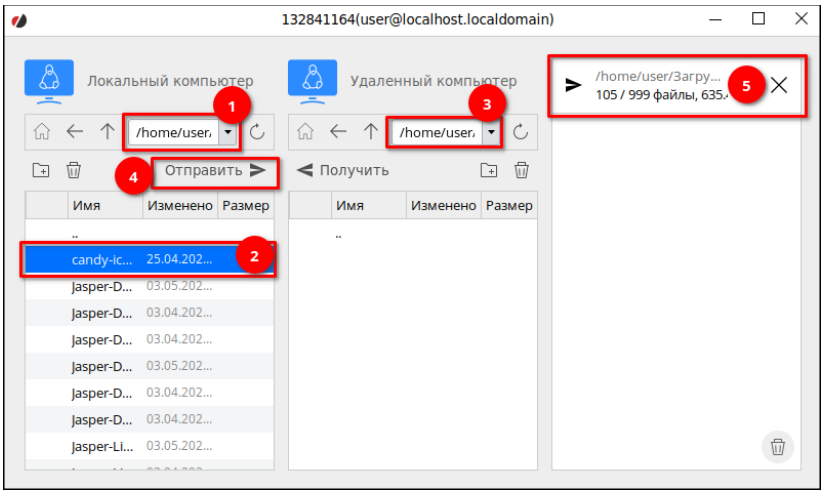
1. Выберите удалённое устройство, с которым вы хотите осуществить обмен файлами.

2. Раскройте список доступных функций для этого устройства.

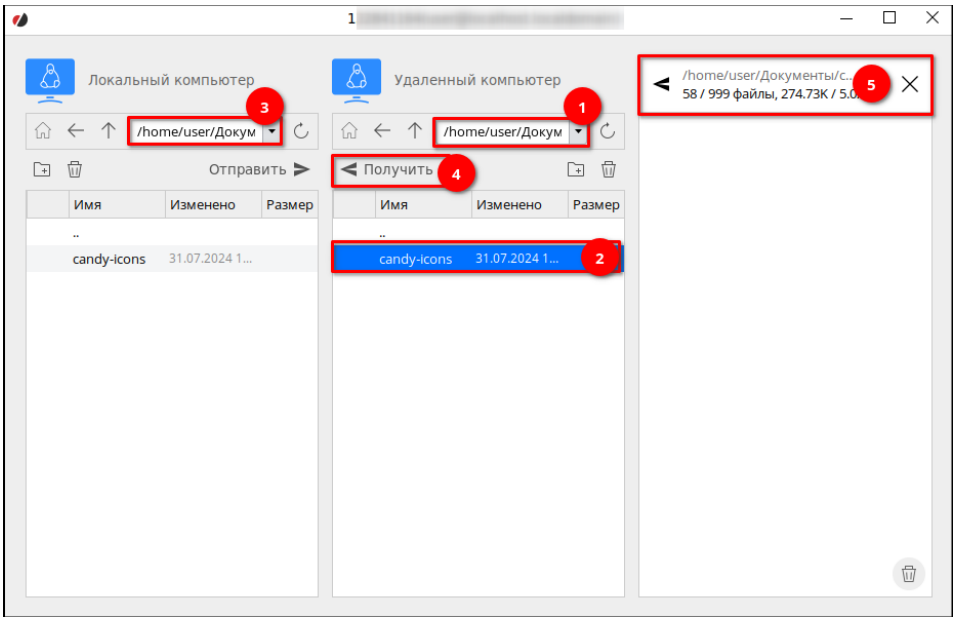
3. Выберите опцию «**Передача файлов**».

4. Подключитесь к удалённому рабочему столу.

5. Для передачи файлов на удаленное устройство в появившемся окне выберите путь на локальном устройстве (1) и выберите файлы, которые нужно передать между устройствами (2). Затем укажите путь назначения на удалённом устройстве (3). Нажмите «**Отправить**» (4). Начнётся процесс передачи файлов (5), дождитесь его завершения.



Для получения файлов с удалённого устройства укажите путь отправления файлов (1) и выберите файлы на удалённом устройстве (2). Затем укажите путь назначения (3) на локальном устройстве для файлов. Нажмите «**Получить**» (4). Начнётся процесс передачи файлов, дождитесь его завершения (5).



Добавление жесткого диска в РЕД ОС

Вы можете подробнее ознакомиться с возможностью добавления жесткого диска в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Добавление жесткого диска в РЕД ОС;
- в **Яндекс.Дзен** — Добавление жесткого диска в РЕД ОС;
- в **VK Видео** — Добавление жесткого диска в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Выключите ПК и подключите к нему жесткий диск.

После загрузки ОС откройте консоль и перейдите в сеанс пользователя **root** с помощью команды:

```
su -
```

Введите пароль пользователя **root**.

Далее с помощью команды `fdisk -l` необходимо посмотреть, какие диски доступны для монтирования.

fdisk — это утилита командной строки для просмотра и управления жесткими дисками и разделами.

```
fdisk -l
```

В списке подключенных дисков должен будет отобразиться, в том числе, и новый диск. Определить этот самый новый диск можно по его размеру.

Следует отметить, что у каждого раздела на жестком диске есть свое название. То есть, **/dev/sda**, **/dev/sdb/** и т. д. (без цифр) — это сами жесткие диски, а вот **/dev/sda1**, **/dev/sda2** — это разделы на жестких дисках.

Рассмотрим пример, когда на подключённом диске **sdb** есть один раздел, который называется **sdb1** и имеет файловую систему **ext4**.

Создайте каталог для монтирования раздела (обычно точка монтирования создается в директориях **/mnt** или **/media**).

```
mkdir -p /mnt/disk1
```

Произведите монтирование:

```
mount /dev/sdb1 /mnt/disk1
```

Если монтирование завершено без ошибок, для автоматического монтирования разделов после перезагрузки сервера внесите изменения в файл **/etc/fstab**. С помощью текстового редактора, например, **nano**, откройте этот файл:

```
nano /etc/fstab
```

Добавьте следующие строки:

```
/dev/sdb1 /mnt/disk1 ext4 defaults 0 0
```

Два параметра в конце строки `"0 0"` (`<dump> <pass>`) определяют, что:

1) Утилита **dump** не будет создавать резервную копию данных в файловой системе. Для дополнительных разделов в этом параметре обычно указывается значение **0**.

2) **fsck** не будет проверять раздел при загрузке ОС. Если же включить проверку **fsck** (установить значение **2** вместо **0**), то при неожиданной перезагрузке ПК процесс перезагрузки может быть довольно продолжительным (из-за проверки **fsck**).

> **Примечание.**
>
> Для однозначной идентификации подключаемых разделов в **/etc/fstab** можно указать идентификатор (UUID).

Командой **blkid** проверьте **UUID** диска, после этого добавьте его в **/etc/fstab**:

```
blkid
```

```
...
```

```
/dev/sdb1: UUID="5baab1ca-c060-49fd-b44a-a19c6c453a2b" TYPE="ext4"
```

Отредактируйте **/etc/fstab**, добавьте строку для монтирования:

```
nano /etc/fstab
```

```
UUID=5baab1ca-c060-49fd-b44a-a19c6c453a2b /mnt/disk1 ext4 defaults 0 0
```

Измените режим доступа к разделам, если нужно. По умолчанию, если каталог создается пользователем **root**, то у каталога будут права этого пользователя:

```
drwxr-xr-x root:root
```

Для смены прав доступа к файлу выполните:

```
chmod -R 777 /mnt/disk1
```

После выполнения всех операций нужно перезагрузить ПК.

Монитирование устройств через systemd

Создание собственных модулей mount
Сетевые и съёмные диски
Примеры монтирования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Файл **fstab** – это текстовый файл, который содержит информацию о различных файловых системах и устройствах хранения информации на компьютере. Это единственный файл, определяющий, как диск и/или раздел будут использоваться и как будут встроены в остальную систему.

Данный файл можно открыть в любом текстовом редакторе, но редактировать его можно только от имени **суперпользователя root**, т.к. файл является важной, неотъемлемой частью системы, без которого система не загрузится.

Вы можете подробнее ознакомиться с возможностью монтирования новых устройств и файловых систем через **systemd**, просмотрев наши обучающие видео:

- на **RuTube** — Настраиваем монтирование systemd вместо файла /etc/fstab;
- в **Яндекс.Дзен** — Настраиваем монтирование systemd вместо файла /etc/fstab;
- в **VK Видео** — Настраиваем монтирование systemd вместо файла /etc/fstab.

На наших каналах вы также сможете найти много другой полезной информации.

Для автоматического монтирования разделов при загрузке операционной системы их указывают в файле **/etc/fstab**, который выглядит следующим образом:

```
[user@localhost ~]$ cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Wed Oct 25 06:21:53 2023
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#                                                  3       4        5 6
/dev/mapper/ro_redos-root /                       ext4    defaults 1 1
UUID=256bd628-c56a-4b53-bc02-601a3f18c4eb /boot                   ext4    defaults        1 2
/dev/mapper/ro_redos-swap none                    swap    defaults 0 0
```

где:

- **1** — имя раздела (уникальный идентификатор);
- **2** — точка монтирования;
- **3** — тип файловой системы;
- **4** — опции монтирования;
- **5** — индикатор необходимости резервной копии;
- **6** — порядок проверки раздела утилитой fsck (0 – отключено).

В файле есть подсказка, что после его заполнения необходимо перезапустить конфигурацию **systemd** (командой `systemctl daemon-reload`). Это означает, что файл на текущий момент является частью системной службы загрузки; **systemd** обрабатывает этот файл, чтобы создать модули для монтирования устройств.

Для отображения списка смонтированных устройств выполните команду:

```
mount
```

В ответе команды выведено довольно много устройств, большинство из них служебные.

С помощью команды `systemctl | grep mount` выведите модули **mount**, используемые в **systemd**.

```
[user@localhost ~]$ systemctl | grep mount
  proc-sys-fs-binfmt_misc.automount                                                  loaded active waiting   Arbitrary Executab
le File Formats File System Automount Point
  -.mount                                                                            loaded active mounted   Root Mount

  boot.mount                                                                         loaded active mounted   /boot

  dev-hugepages.mount                                                                loaded active mounted   Huge Pages File Sy
stem
  dev-mqueue.mount                                                                   loaded active mounted   POSIX Message Queu
e File System
  run-media-user-redos\x2dDVD\x2dx86_64\x2dMUROM\x2d7.3.3.mount                      loaded active mounted   /run/media/user/re
dos-DVD-x86_64-MUROM-7.3.3
  run-user-1000-doc.mount                                                            loaded active mounted   /run/user/1000/doc

  run-user-1000-gvfs.mount                                                           loaded active mounted   /run/user/1000/gvf
s
  run-user-1000.mount                                                                loaded active mounted   /run/user/1000

  run-vmblock\x2dfuse.mount                                                          loaded active mounted   VMware vmblock Fus
e Mount
  sys-fs-fuse-connections.mount                                                      loaded active mounted   FUSE Control File
System
  sys-kernel-config.mount                                                            loaded active mounted   Kernel Configurati
on File System
  sys-kernel-debug.mount                                                             loaded active mounted   Kernel Debug File
System
  sys-kernel-tracing.mount                                                           loaded active mounted   Kernel Trace File
System
```

Среди выведенных модулей присутствуют файловые системы, которые описаны в файле **/etc/fstab**.

Для определения физического места расположения устройства выполните (в примере используется **boot.mount**):

```
systemctl cat boot.mount

# /run/systemd/generator/boot.mount
# Automatically generated by systemd-fstab-generator

[Unit]
Documentation=man:fstab(5) man:systemd-fstab-generator(8)
SourcePath=/etc/fstab
Requires=systemd-fsck@dev-disk-by\x2duuid-256bd628\x2dc56a\x2d4b53\x2dbc02\x2d601a3f18c4eb.service
After=systemd-fsck@dev-disk-by\x2duuid-256bd628\x2dc56a\x2d4b53\x2dbc02\x2d601a3f18c4eb.service
After=blockdev@dev-disk-by\x2duuid-256bd628\x2dc56a\x2d4b53\x2dbc02\x2d601a3f18c4eb.target

[Mount]
Where=/boot
What=/dev/disk/by-uuid/256bd628-c56a-4b53-bc02-601a3f18c4eb
Type=ext4
```

Такие модули находятся во временной папке **/run**, они генерируются во время загрузки. Один из комментариев в файле модуля сообщает о том, что файл сгенерирован автоматически службой **systemd-fstab-generator**.

Создание собственных модулей mount

Модули **mount** можно создавать самостоятельно. Далее будет рассмотрен способ создания нового модуля **mount** вручную.

Собственные модули типа mount следует располагать в каталоге **/etc/systemd/system**. Существуют специальные правила именования таких файлов: они должны содержать путь к точке монтирования, в которой все слэши (кроме начального) заменяются на дефис. Например, если точка монтирования **/home/user/disk1**, то имя файла модуля должно иметь следующий вид – **home-user-disk1.mount**. Если в пути к точке монтирования есть служебные символы, то для генерации имени модуля существует специальная команда:

```
systemd-escape -p "/home/user/*disk-sata"

home-user-\x2adisk\x2dsata
```

В ответе команды видно, что специальные символы заменяются на набор символов **\x2d**.

Для создания нового модуля выполните:

```
nano /etc/systemd/system/home-user-disk1.mount
```

Модуль в своем описании должен содержать обязательную секцию [Mount], в которой указывается устройство и точка монтирования.

Минимальное содержимое модуля выглядит следующим образом:

```
[Unit]
 Description=Новый диск

 [Mount]
 What=/dev/disk/by-uuid/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
 Where=/home/user/disk1

 [Install]
 WantedBy=multi-user.target
```

Секция [Unit] содержит строку с описанием службы точки монтирования.

Секция [Install] задает уровень запуска службы, например **multi-user.target** (для многопользовательского режима без графики) или **graphical.target** (для монтирования устройства при графическом входе в систему).

Секция [Mount] описывает способ монтирования файловой системы.

Здесь параметр **What=** указывает путь к монтируемому устройству. Самый простой пример – **/dev/sda1**, но такой подход крайне не рекомендуется, т.к. при добавлении новых устройств имя может изменяться. Рекомендуется монтировать блочные устройства по **UUID**.

Параметр **Where=** указывает, куда будет производиться монтирование. Если указанной директории не существует, она будет создана.

Параметр **Type=** описывает тип файловой системы.

Параметр **Options=** указывает, какие параметры монтирования следует применить (перечисляются через запятую).

Параметр **DirectoryMode=** определяет режим доступа к файловой системе, используемый при создании этих каталогов. По умолчанию используется значение **0755**.

Параметр **TimeoutSec=** настраивает время ожидания перед завершением выполнения команды монтирования. Если команда не завершится в течение заданного времени, монтирование будет считаться неудачным.

Т.к. монтировать устройства необходимо по **UUID**, уточнить его можно с помощью команды:

```
lsblk -f
```

```
[user@localhost ~]$ lsblk -f
NAME FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINTS
sda
├─sda1
│    ext4   1.0         256bd628-c56a-4b53-bc02-601a3f18c4eb    698,2M    21% /boot
└─sda2
     LVM2_m LVM2        pZDD6y-inX7-Gg1O-e3DM-eLB0-bw8K-Zu91uA
  ├─ro_redos-root
  │  ext4   1.0         0e902942-3c05-4f7a-81c2-af22d16c9b42     26,1G    22% /
  └─ro_redos-swap
     swap   1           6cb04aa0-e9f3-46b3-a424-f8662fa22dbd                [SWAP]
sdb  LVM2_m LVM2        6IEWdc-vSPL-rc4f-bXlI-9K0c-jZZm-QW98Pf
```

После создания и сохранения файла модуля обновите конфигурацию **systemd**:

```
systemctl daemon-reload
```

Далее смонтируйте устройство:

```
systemctl start home-user-disk1.mount
```

После этого можно добавить точку монтирования в автозагрузку, для этого выполните команду:

```
systemctl enable home-user-disk1.mount
```

Сетевые и съёмные диски

Для подключения сетевых и съемных носителей необходимо использовать модуль автомонтирования.

Обратите внимание, что автомонтирование – не то же самое, что автоматический запуск модуля монтирования при загрузке системы.

Файл такого модуля формируется по тем же правилам, но с другим расширением – **.automount**. Данный модуль не содержит параметров монтирования и используется только в связке с mount-модулем, его имя формируется по тем же правилам. Например:

```
[Unit]
 Description=Автомонтирование съемного диска

 [Automount]
 Where=/home/user/disk1
 TimeoutIdleSec=900

 [Install]
 WantedBy=multi-user.target
```

Основная секция такого модуля – [Automount].

Обязательным параметром является **Where=**, который указывает на точку монтирования, а параметр **TimeoutIdleSec** настраивает время ожидания простоя в секундах, после которого файловая система будет отмонтирована.

По завершении создания модуля автомонтирования обновите конфигурацию **systemd** и запустите модуль:

```
systemctl daemon-reload
systemctl start home-user-video.automount
```

После этого можно добавить точку монтирования в автозагрузку, для этого выполните команду:

```
systemctl enable home-user-video.automount
```

Примеры монтирования

Монтирование съемного диска

По аналогии с ранее приведенными действиями сначала будет создан модуль монтирования **home-user-disk01**:

```
[Unit]
 Description=Монтирование съемного диска /home/user/disk01

 [Mount]
 What=/dev/disk/by-uuid/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
 Where=/home/user/disk01
 Type=ntfs
 Options=defaults

 [Install]
 WantedBy=multi-user.target
```

После этого необходимо создать одноименный модуль автомонтирования **home-user-disk01.automount**:

```
[Unit]
 Description=Монтирование съемного диска /home/user/disk01

 [Automount]
 Where=/home/user/disk01
 TimeoutIdleSec=300

 [Install]
 WantedBy=multi-user.target
```

Далее следует обновить конфигурацию systemd и добавить модуль автомонтирования в автозагрузку:

```
systemctl daemon-reload
```

```
systemctl enable --now home-user-disk01.automount
```

Благодаря созданным модулям, указанное устройство будет смонтировано при первом к нему обращении. При неактивности в течение 300 сек (5 мин) устройство будет размонтировано.

Монтирование NFS

Далее будет рассмотрен пример с протоколом сетевого доступа к файловым системам (*NFS*).

Клиентская часть требует установки дополнительного пакета:

```
dnf install nfs-common
```

Для монтирования NFS-ресурса так же необходимо создать два модуля. Первый – модуль монтирования **home-user-foto.mount**:

```
[Unit]
 Description= Монтирование NFS /home/user/foto

 [Mount]
 What=192.168.88.33:/media/nfs
 Where=/home/user/foto
 Type=nfs
 Options=_netdev,auto
 TimeoutSec=10

 [Install]
 WantedBy=multi-user.target
```

Второй – модуль автомонтирования **home-user-foto.automount**:

```
[Unit]
 Description=Монтирование NFS /home/user/foto

 [Automount]
 Where=/home/user/foto
 TimeoutIdleSec=300

 [Install]
 WantedBy=multi-user.target
```

Далее следует обновить конфигурацию systemd и добавить модуль автомонтирования в автозагрузку:

```
systemctl daemon-reload
systemctl enable --now home-user-foto.automount
```

Gnome-disk-utility – утилита для управления дисками

Gnome Disk Utility (**Gnome Disks**) — простая программа для управления дисками с базовым функционалом.

Программа позволяет просматривать информацию о дисках и съемных носителях. Для каждого диска доступна информация о модели, состоянии, серийном номере, информация о разделах, размерах разделов, типах таблиц разделов и другие данные.

Gnome Disk Utility поддерживает форматирование дисков, управление разделами, создание образов и восстановление разделов из образа. Также существует инструмент для оценки производительности диска.

Установка

Для установки программы необходимо перейти в сеанс пользователя **root**:

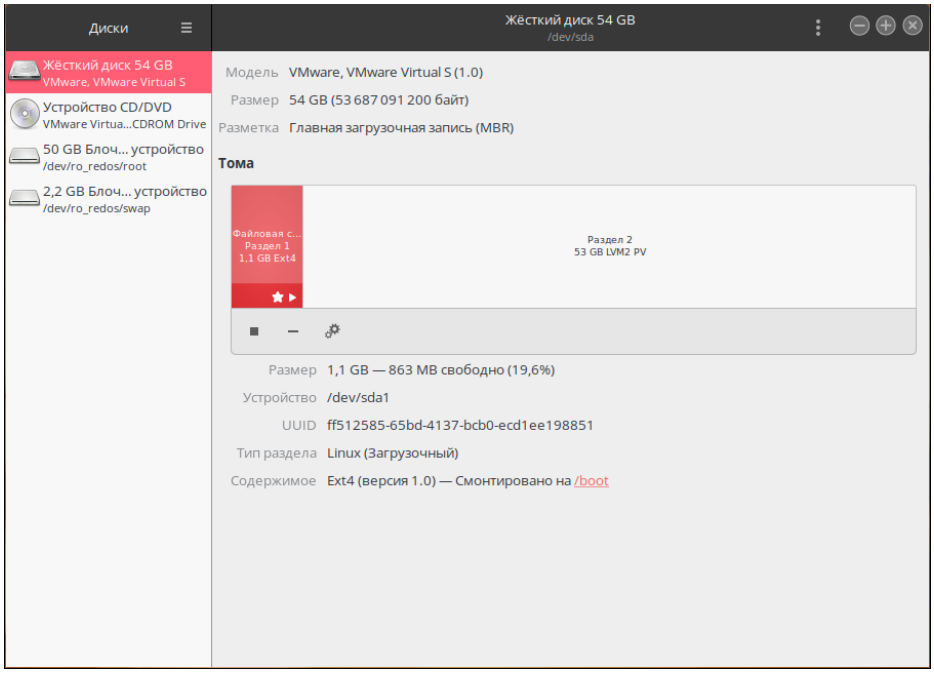
```
su -
```

Затем выполнить команду:

```
dnf install gnome-disk-utility
```

После установки программа доступна из «**Главного меню**» - «**Стандартные**» - «**Диски**» или вызовом через консоль (от **локального** пользователя):

```
gnome-disks
```



В меню программы можно создать или подключить образы дисков, ознакомиться с заданными комбинациями горячих клавиш, просмотреть справку о работе в программе.

В основном окне представлен список используемых дисков, подробная информация о выбранном разделе, а также возможность отмонтирования, удаления и расширенной настройки выбранного раздела.

Gparted – работа с дисковыми разделами

Установка
Интерфейс программы
Создание таблицы разделов
Создание разделов
Изменение размеров разделов
Удаление разделов

Перед началом использования нового жесткого диска, его полный объем необходимо разделить на части. Часть или, по-другому, раздел подразумевает участок диска, предназначенный для комфортного использования и размещения информации. Это помогает структурировать и разграничить отдельно файлы операционной системы от личных данных пользователя.

Если диск не новый, то иногда возникает необходимость в изменении количества или размеров разделов. Для всего этого в РЕД ОС есть различные инструменты, одним из таких инструментов является программа **GParted**.

GParted — это графическая оболочка к утилитам по работе с дисковыми разделами. Название происходит из полного названия – **GNOME Partition Editor**.

Gparted позволяет выполнять все необходимые операции над разделами дисков. Основными операциями являются:

- *Создание* - выделяется из свободного, не занятого другими разделами, места.
- *Удаление* - уничтожаются и раздел и данные на нём.
- *Изменение размера* - информация на разделе сохраняется.
- *Форматирование* - программа поддерживает около 20 типов файловых систем.
- *Монтирование* - стандартная процедура монтирования и размонтирования устройств хранения.
- *Управление флагами* - у разделов есть определённые атрибуты, например, загрузочный.
- *Проверка на ошибки* - проверяются ошибки файловой таблицы раздела.
- *Изменение UUID* - смена Универсального Уникального Идентификатора.
- *Создание таблицы разделов* - основная таблица жёсткого диска, хранит информацию о разделах.

Вы можете подробнее ознакомиться с работой утилиты **Gparted**, просмотрев наши обучающие видео:

- на **RuTube**:
  - Редакторы дисковых разделов в РЕД ОС. GParted;
  - Как отформатировать флешку в РЕД ОС.
- в **Яндекс.Дзен**:
  - Редакторы дисковых разделов в РЕД ОС. GParted;
  - Как отформатировать флешку в РЕД ОС.
- в **VK Видео**:
  - Редакторы дисковых разделов в РЕД ОС. GParted;
  - Как отформатировать флешку в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

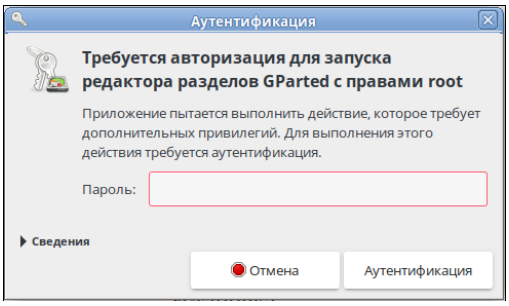
и выполните команду:

```
dnf install gparted
```

После установки программа доступна из «**Главного меню**» - «**Системные**» - «**GParted**».

Для правильной работы утилиту необходимо запускать **с правами суперпользователя**. Если вы запускаете ее из главного меню, то

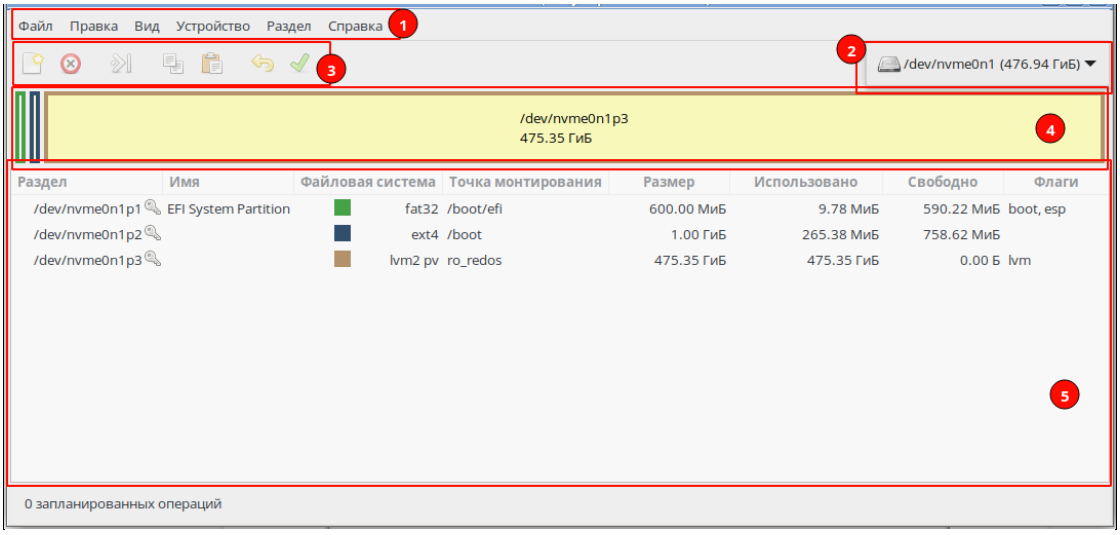
система сама потребует пароль.



Интерфейс программы

После запуска перед вами откроется главное окно программы. Оно состоит из таких областей, как:

1. *Меню* - содержит все команды программы **gparted** для работы с дисковыми устройствами и разделами.
2. *Список устройств* - отображает список доступных устройств.
3. *Панель инструментов* - содержит несколько команд для быстрого доступа.
4. *Сводная диаграмма* - графическая схема выбранного диска, визуально отображает соотношение размеров разделов.
5. *Рабочая область* - отображает все разделы на текущем диске с дополнительной информацией о них. При работе с носителями в нижней части данного поля отображается последовательный список всех операций, которые потом необходимо выполнить.



Программа проста и интуитивно понятна. Для работы необходимо выбрать нужный участок устройства хранения, вызвать контекстное меню и выбрать необходимое действие, в зависимости от возможных действий состав контекстного меню изменяется.

Изначально все действия записываются, а не применяются. Чтобы применить изменения, нужно нажать на зеленую галочку в панели инструментов. Также можно открыть меню «**Правка**» - «**Применить все операции**». Затем потребуется подтвердить всю последовательность действий, поскольку это может вызвать потерю данных.

Обратите внимание, что начинать работу в этой программе лучше с пустым диском, чтобы случайно не потерять данные.

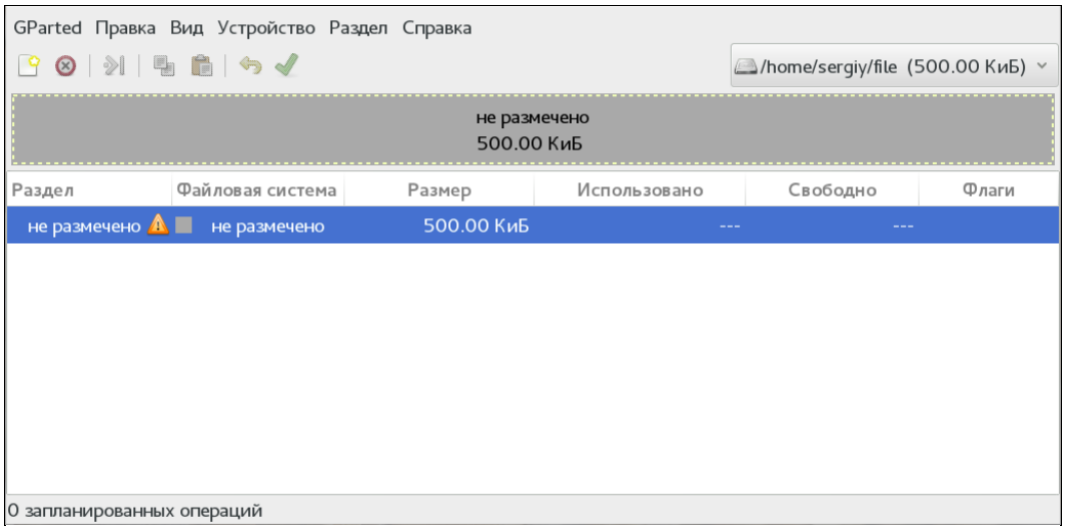
Рассмотрим пример работы с жёстким диском.

Создание таблицы разделов

Для того чтобы хранить информацию на носителе, необходимо его разметить. На одном носителе можно создать несколько независимых частей - разделов. Информация о таком разделении хранится в самом начале носителя и именуется таблицей разделов. Таблицы отличаются разной структурой, надежностью и возможностями. Некоторые не поддерживаются в одной операционной системе, но поддерживаются в другой. Наиболее широко известными типами таблиц разделов являются **msdos** (*MBR*) и **GPT**.

Для создания новой таблицы разделов необходимо открыть меню «**Устройство**» - «**Создать таблицу разделов**».

Вы увидите диалоговое окно, где сможете выбрать нужный вам тип таблицы разделов. По умолчанию выбран параметр **msdos** (*MBR*).



Нажмите «**Применить**», чтобы создать новую таблицу разделов. Приложение запишет новую таблицу разделов на дисковое устройство и обновит информацию о разделах в окне **gparted**.

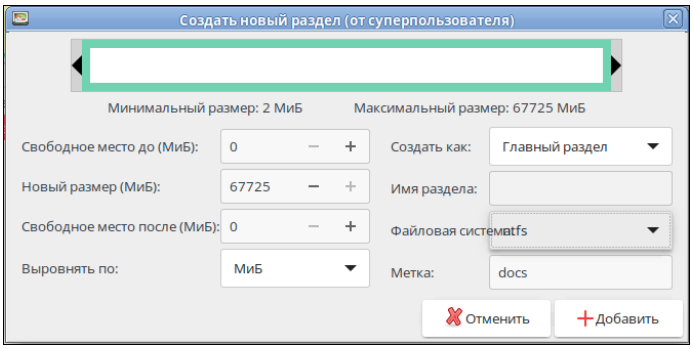
ВАЖНО!

Данная операция удалит все данные со всего дискового устройства!

Создание разделов

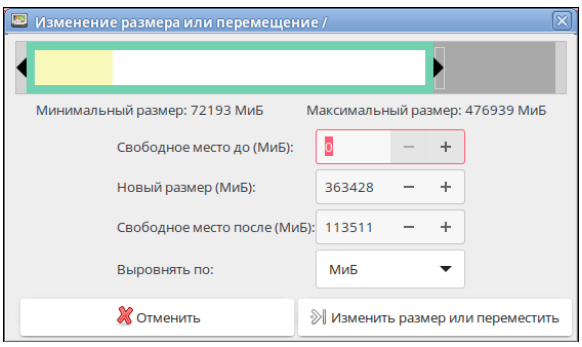
Чтобы создать новый раздел, выберите область «**Не размечено**» и, нажав ПКМ, выберите пункт «**Новый**» из контекстного меню.

После этого необходимо заполнить информацию о будущем разделе. Вы можете тонко настроить расположение раздела от начала или конца свободного пространства и указать размер. А также можно выбрать *файловую систему*, *тип раздела* (первичный/вторичный) и *метку*. Размер и расположение раздела можно также указать, изменяя сам раздел визуально, на линейке в верхней части окна.



Изменение размеров разделов

Для изменения размера необходимо выбрать нужный раздел, открыть контекстное меню, выбрать пункт «**Изменить размер или переместить**». В открывшемся окне новые размеры устанавливаются либо в соответствующих полях, либо мышкой. После установки нужных размеров можно смело применять действия к исполнению. Важно знать, что данные на разделе при изменении его размеров остаются в сохранности.



Удаление разделов

Для удаления необходимо выбрать раздел, вызвать контекстное меню и выбрать пункт «**Удалить**».

ВАЖНО!

Если диск примонтирован, действия с ним будут недоступны.

При этом стоит помнить, что после применения изменений **вся информация** на разделе **будет удалена**.

Blivet-gui – управление разделами и дисками

Интерфейс
Создание раздела
Изменение или удаление раздела

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:**: blivet-gui 2.2.0-3

Blivet-gui является реализацией механизмов управления разделами и дисками. Утилита с графическим интерфейсом создана для удобного управления носителями в РЕД ОС. Интерфейс похож на **gparted**, но **blivet-gui** поддерживает весь набор технологий хранения данных из современных дистрибутивов Linux. Для графического интерфейса **blivet** требуется модуль **Python blivet**. Так же как и **gparted**, **blivet-gui** работает только с правами пользователя **root**.

Программа поддерживает управление дисковыми разделами и хранилищами **LVM2** (включая шифрованные разделы LUKS, логические тома и группы томов). Так же как и в **gparted**, изменения в **blivet-gui** применяются не сразу, а после подтверждения внесённого набора изменений.

Вы можете подробнее ознакомиться с работой утилиты **Blivet-gui**, просмотрев наши обучающие видео:

- на **RuTube** — Управление разделами и дисками с помощью Blivet-gui;
- в **Яндекс.Дзен** — Управление разделами и дисками с помощью Blivet-gui;
- в **VK Видео** — Управление разделами и дисками с помощью Blivet-gui.

На наших каналах вы также сможете найти много другой полезной информации.

Установку программы можно осуществить командой:

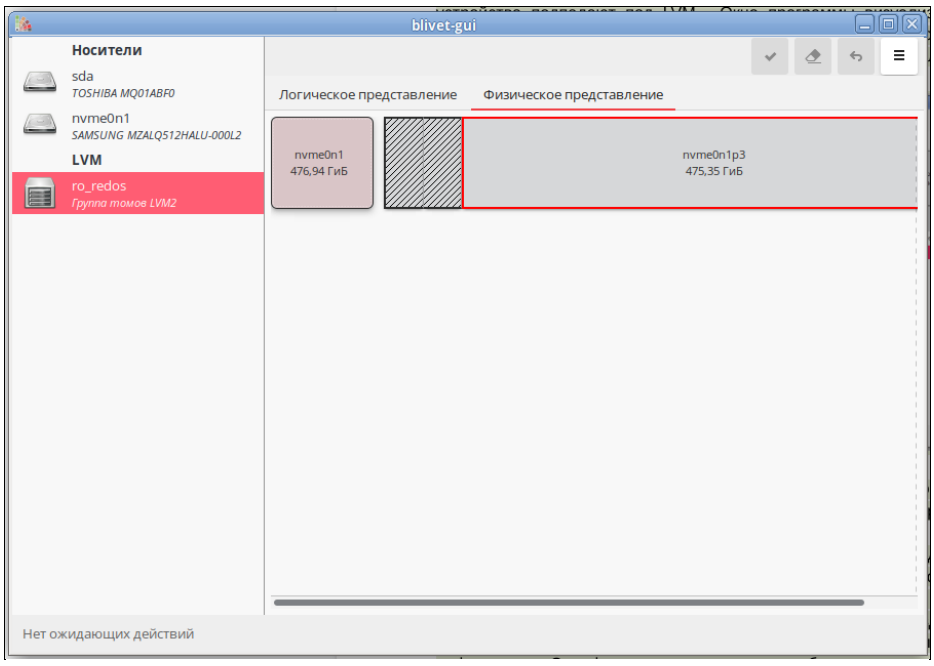
```
dnf install blivet-gui
```

После установки программа доступна в «**Главном меню**» - «**Системные**» - «**blivet-gui**». Интерфейс запускается только с правами пользователя **root**.

Графический интерфейс **blivet** визуально напоминает **gparted**, но без панели меню. Вы можете полностью управлять программой с помощью кнопок в правом верхнем углу окна программы и в соответствующих контекстных меню.

Интерфейс

Слева отображается вертикальный список физических и логических томов в системе. Логические тома находятся под дисками, а блочные устройства подпадают под **LVM**. Окно программы визуализирует объемы в виде горизонтальной полосы. Пользователи **blivet-gui** могут переключать соответствующее представление с помощью вкладок «**Логическое представление**» и «**Физическое представление**».



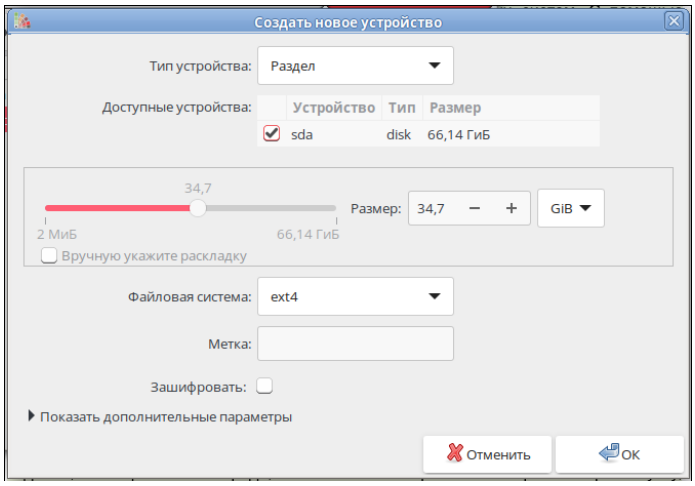
Графический интерфейс **blivet** очень четко показывает физические и логические тома, предоставляя администраторам обзор логических томов, охватывающих несколько физических томов.

В разделе «**Логическое представление**» отображается таблица отдельных томов, включая соответствующую дополнительную информацию.

Все действия для настройки выполняются через контекстные меню. **Blivet-gui** частично поддерживает многие типы файловых систем.

Создание раздела

Для создания раздела необходимо выбрать свободное место на физическом диске, вызвать контекстное меню и выбрать пункт «**Создать**». С помощью графических элементов управления вы можете задать размер логического тома или ввести значение напрямую. Нажатие кнопки «**OK**» создает задачу на создание нового логического диска и подготавливает его к работе.



Изменение или удаление раздела

Для изменения раздела следует выбрать нужный существующий логический раздел, в контекстном меню выбрать пункт «**Изменить**». С помощью команды «**Форматировать**» можно отформатировать раздел. С помощью команды «**Удалить**», соответственно, удалить раздел. Также есть возможность изменить размер всего тома с помощью функции «**Редактирования**» - «**Изменить размер**».

Если впоследствии добавить в систему новые физические тома, то можно, например, сначала интегрировать их с существующим логическим томом, выбрав в контекстном меню пункт «**Изменить**» - «**Изменить родителей**».

Изменения не вступят в силу до тех пор, пока вы их не подтвердите нажатием кнопки с галочкой в правом верхнем углу окна программы.

В отдельном окне отобразятся незавершенные операции, но **blivet** выполняет эти действия только после нажатия кнопки «**OK**».

Baobab – программа для анализа использования разделов диска

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** baobab-3.32.0-1

Baobab — программа для анализа использования ёмкости разделов диска из состава свободной среды рабочего стола **GNOME**. Графически показывает, какие папки занимают больше места на диске.

Baobab позволяет сканировать полностью всю файловую систему, отдельные папки, домашнюю директорию или удаленный каталог (по **FTP**, **SSH**, **HTTPS**). Также непосредственно из программы можно удалять файлы и директории.

Графически использование диска можно отобразить в виде круговой диаграммы или в виде древовидной карты (прямоугольниками).

Вы можете подробнее ознакомиться с работой в **Baobab**, просмотрев наши обучающие видео:

- на **RuTube** — Анализ занятого пространства на дисках;
- в **Яндекс.Дзен** — Анализ занятого пространства на дисках;
- в **VK Видео** — Анализ занятого пространства на дисках.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы перейдите в сеанс пользователя **root**:

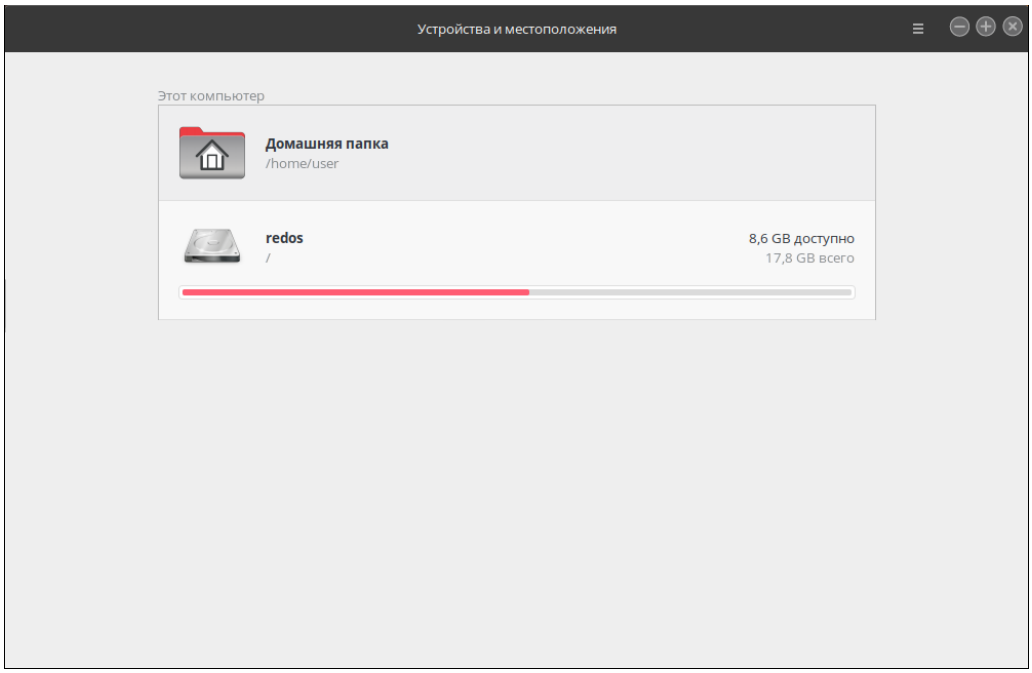
```
su -
```

и выполните команду:

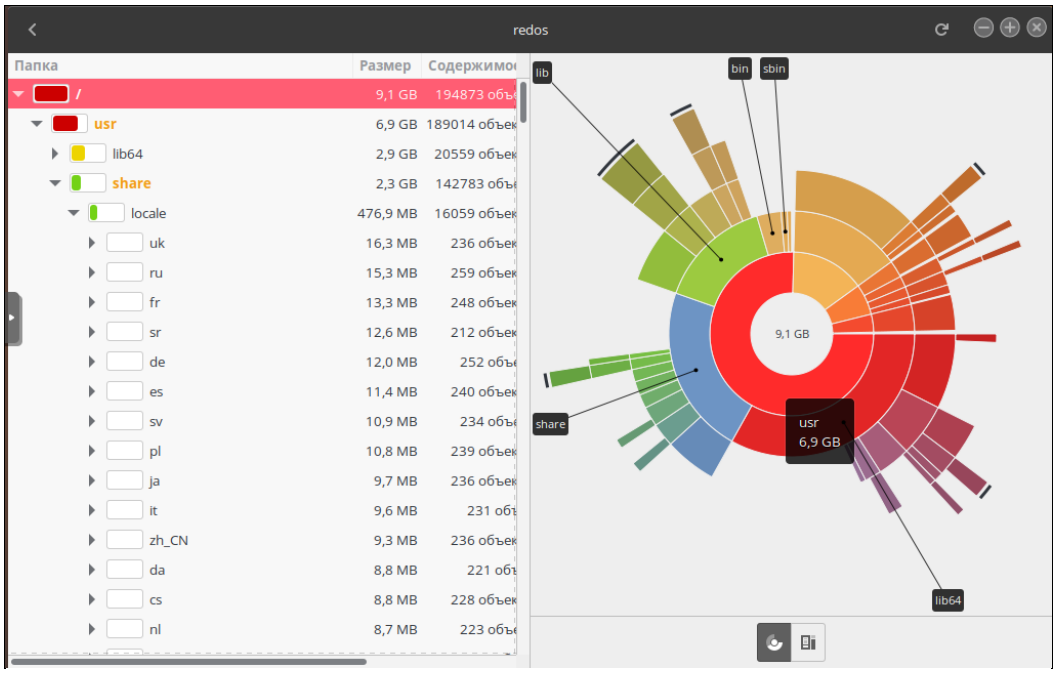
```
dnf install baobab
```

Программа будет доступна из «**Главного меню**» - «**Системные**» - «**Анализатор использования дисков**».

При запуске программы предлагается выбрать диск для проведения анализа.



После этого будет построено дерево каталогов и представлена диаграмма использования дискового пространства. При наведении курсора на какую-либо область диаграммы будет показано, какая доля дискового пространства занята тем или иным каталогом.


redos
Папка
Размер
/ 9,1 GB
usr 6,9 GB
lib64 2,9 GB
share 2,3 GB
locale 476,9 MB
uk 16,3 MB
ru 15,3 MB
fr 13,3 MB
sr 12,6 MB
de 12,0 MB
es 11,4 MB
sv 10,9 MB
pl 10,8 MB
ja 9,7 MB
it 9,6 MB
zh_CN 9,3 MB
da 8,8 MB
cs 8,8 MB
nl 8,7 MB
lib
bin
sbin
9,1 GB
usr
6,9 GB
share
lib64

Менеджер логических томов LVM

Logical Volume Manager (LVM) — это система управления дисковым пространством, абстрагирующаяся от физических устройств. Она позволяет создавать поверх физических разделов (или даже неразбитых винчестеров) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (т.е. как обычные разделы). Основные преимущества **LVM** в том, что, во-первых, одну группу логических томов можно создавать поверх любого количества физических разделов, а во-вторых, размер логических томов можно легко менять прямо во время работы.

Кроме того, **LVM** поддерживает механизм снапшотов, управление разделами «на лету» и зеркалирование, подобное RAID-1.



Из схемы на рисунке видно, что в самом низу рисунка располагаются физические устройства — жесткие диски. Далее начинается зона LVM, а именно – создаются физические тома (**PV**) из разделов жесткого диска, которые потом объединяются в логические группы (**VG**). В качестве примера на схеме представлена единая логическая группа **vgdata** (**/dev/vgdata**), а уже на следующем уровне эта группа разбита на логические тома (**LV**), на которых могут быть созданы файловые системы.

PV (Physical volume) — физический том. Обычно это раздел на диске или весь диск. В том числе, устройства программного и аппаратного RAID (которые уже могут включать в себя несколько физических дисков). Физические тома входят в состав группы томов.

VG (Volume group) — группа томов. Это самый верхний уровень абстрактной модели, используемой системой **LVM**. С одной стороны группа томов состоит из физических томов, с другой – из логических и представляет собой единую административную единицу.

LV (Logical volume) — логический том. Раздел группы томов, эквивалентен разделу диска в не LVM-системе. Представляет собой блочное устройство и, как следствие, может содержать файловую систему.

PE (Physical extent) — физический экстент. Каждый физический том делится на порции данных, называющиеся физическими экстентами. Их размеры те же, что и у логических экстентов.

LE (Logical extent) — логический экстент. Каждый логический том делится на порции данных, называющиеся логическими экстентами. Размер логических экстентов не меняется в пределах группы томов.

Установка РЕД ОС на диски со схемой разбиения **LVM** производится согласно нашей инструкции «Ручная разметка диска».

Механизмы работы LVM

Снапшоты

Снапшот — моментальный снимок, копия файлов и каталогов файловой системы на определённый момент времени. Снимки диска позволят откатить состояние на определенный момент. Это может послужить быстрым вариантом резервного копирования. Однако нужно понимать, что данные хранятся на одном и том же физическом носителе, а значит, данный способ не является полноценным резервным копированием.

Управление разделами «на лету»

LVM увеличивает удобство работы с жестким диском, аппаратные особенности работы скрываются программным обеспечением, поэтому можно изменять размеры дисков, перемещать их «на лету», без остановки приложений или размонтирования файловых систем. Это очень удобно на серверах, когда есть возможность добавить еще один диск или расширить существующие lvm-тома «на лету». LVM работает на уровне ядра, поэтому гарантируется максимальная прозрачность настройки и использования дисков. Программы смогут работать с логическими, виртуальными LVM-разделами, точно так же, как и с обычными.

Зеркалирование

С помощью LVM можно создать зеркальный том — данные, которые мы будем на нем сохранять, будут отправляться на 2 диска. Таким образом, если один из дисков выходит из строя, мы не потеряем свои данные. Зеркалирование томов выполняется из группы, где есть, минимум, 2 диска.

Система управления логическими томами особенно полезна в работе с серверами, поскольку обеспечивает масштабируемость и удобное управление дисковым пространством. Она упрощает планирование дискового пространства и предотвращает проблемы,

возникающие при неожиданно быстром росте занятого места в разделах. LVM не предназначен для обеспечения отказоустойчивости или высокой производительности. Поэтому он часто используется в сочетании с системами RAID.

Примеры использования LVM в РЕД ОС см. в нашей статье «Примеры использования LVM».

Примеры использования LVM

Пример №1 - Разметка дисков с помощью LVM
Пример №2 - Уменьшение размера логического тома
Пример №3 - Увеличение размера логического тома
Пример №4 - Удаление логического тома
Пример №5 - Добавление нового диска к группе томов
Пример №6 - Удаление физического диска из группы томов
Пример №7 - Расширение корневого раздела типа LVM

Вы можете подробнее ознакомиться с информацией по использованию LVM, просмотрев наши обучающие видео:

- на **RuTube** — Работа с LVM в РЕД ОС;
- в **Яндекс.Дзен** — Работа с LVM в РЕД ОС;
- в **VK Видео** — Работа с LVM в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Пример №1 - Разметка дисков с помощью LVM

Предположим, что мы имеем два неразмеченных диска подключенных к компьютеру. Теперь попробуем разметить их с помощью LVM и создать структуру, как на схеме.

Выполним команду:

```
sudo fdisk -l
```

```
[sudo] пароль для user:Диск /dev/sda: 32 GiB, 34359738368 байт, 67108864 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xfa2fa11b
Устр-во Загрузочный начало Конец Секторы Размер Идентификатор Тип
/dev/sda1 * 2048 2099199 2097152 1G 83 Linux
/dev/sda2 2099200 67108863 65009664 31G 8e Linux LVMДиск /dev/sdb: 10 GiB, 10737418240 байт, 20971520 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байтДиск /dev/sdc: 10 GiB, 10737418240 байт, 20971520 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Диск /dev/mapper/ro-root: 28 GiB, 30056382464 байт, 58703872 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Диск /dev/mapper/ro-swap: 3 GiB, 3221225472 байт, 6291456 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
```

Команда показывает диски и их разделы. Среди остальных дисков мы видим 2 диска по 10 Гб. **Диск /dev/sdb: 10 GiB** и **Диск /dev/sdc: 10 GiB.**

Создание физических томов

Сначала необходимо создать физические тома в окружении LVM из /dev/sdb и /dev/sdc. Для этого используем следующую команду:

```
sudo pvcreate /dev/sdb /dev/sdc
```

```
[sudo] пароль для user:
Physical volume "/dev/sdb" successfully created.
Physical volume "/dev/sdc" successfully created.
```

Посмотрим информацию о физических томах с помощью команды **pvs**:

```
sudo pvs
```

```
PV VG Fmt Attr PSize PFree
/dev/sda2 ro lvm2 a-- <31,00g 4,00m
/dev/sdb lvm2 --- 10,00g 10,00g
/dev/sdc lvm2 --- 10,00g 10,00g
```

Основные столбцы, которые интересны:

- **PV** - здесь указываются физические тома;
- **VG** - принадлежность к логической группе;
- **Fmt** - формат тома;
- **PSize** - размер физического том.

/dev/sda2 - это физический том, который был создан при установке РЕД ОС и на нем располагается система, но также видим, что создались два новых физических тома - **/dev/sdb и /dev/sdc** размером 10 Гб и формат их LVM2. Можем также заметить, что пока наши тома не включены ни в какую логическую группу, в отличии от **/dev/sda2** который находится в логической группе ro.

Более подробную информацию о физических томах выводит команда:

```
pvdisplay
```

Создание группы логических томов

Итак, физические тома созданы, приступим к созданию логической группы, для этого выполняем команду:

```
sudo vgcreate vgdata /dev/sdb /dev/sdc
```

```
[sudo] пароль для user:
Volume group "vgdata" successfully created
```

здесь **vgdata** - имя логической группы, **/dev/sdb** и **/dev/sdc** - физические тома.

Таким образом, мы создали логическую группу **vgdata** из двух физических томов.

Давайте посмотрим информацию о созданной логической группе **vgdata**:

```
sudo vgdisplay vgdata
```

```
--- Volume group ---VG Name vgdataSystem ID
Format lvm2
Metadata Areas 2
Metadata Sequence No 1
VG Access read/write
VG Status resizable
MAX LV 0
Cur LV 0
Open LV 0
Max PV 0
Cur PV 2
Act PV 2
VG Size 19,99 GiB
PE Size 4,00 MiB
Total PE 5118
Alloc PE / Size 0 / 0
Free PE / Size 5118 / 19,99 GiB
VG UUID rmdGbk-Sy5Y-bPns-ufg4-vyV2-Zvez-8v1ayB
```

Обратите внимание, что размер vgdata стал суммарно равен двум физическим томам, на это указывает поле VG Size.

Создание логических томов

Следующий уровень абстракции это логические тома, которые создаются на логической группе томов.

Создадим три тома как на схеме 1 - mydocs, films и music

```
sudo lvcreate -L 5G -n mydocs vgdata
```

В данной команде:

-L 5G - указывает на размер логического тома;
-n - задает имя тома;
vgdata - указываем на какой группе создавать логический том.

С помощью команды lvdisplay выведем детальную информацию о логических томах:

```
sudo lvdisplay
```

```
--- Logical volume ---LV Path /dev/ro/swapLV Name swap
VG Name ro
LV UUID O0Y4pj-Xseg-NeCQ-H1yk-nKif-as6R-zR1zKf
LV Write Access read/write
LV Creation host, time localhost, 2020-06-22 10:46:11 +0300
LV Status available
# open 2
LV Size 3,00 GiB
Current LE 768
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 254:1--- Logical volume ---LV Path /dev/ro/rootLV Name root
VG Name ro
LV UUID 9rPYsg-MKbM-DpLK-L1NN-PvcY-RrSm-2aNrV1
LV Write Access read/write
LV Creation host, time localhost, 2020-06-22 10:46:12 +0300
LV Status available
# open 1
LV Size 27,99 GiB
Current LE 7166
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 254:0--- Logical volume ---LV Path /dev/vgdata/mydocsLV Name mydocs
VG Name vgdata
LV UUID A6q4tK-3KEO-UGla-bj3t-0cZB-3Had-1bBdBH
LV Write Access read/write
LV Creation host, time localhost.localdomain, 2020-08-07 14:31:14 +0300
LV Status available
# open 0LV Size 5,00 GiBCurrent LE 1280
Segments 1
Allocation inherit
Read ahead sectors auto
- currently set to 8192
Block device 254:2
```

Видим три логических тома: /dev/ro/swap - том файла подкачки , /dev/ro/root - системный корневой раздел и наш только что созданный том **/dev/vgdata/mydocs**

Создадим второй логический том films:

```
sudo lvcreate -L 10G -n films vgdata
```

Для третьего тома music, используем все оставшееся свободное пространство, для этого в команде укажем параметр **-l 100%FREE**:

```
sudo lvcreate -l 100%FREE -n music vgdata
```

Посмотрим созданные логические тома, а также группу томов в которую они входят:

```
sudo lvs
```

```
LV VG Attr LSize
```

```
root ro -wi-ao---- 27,99g
swap ro -wi-ao---- 3,00gfilms vgdata -wi-a----- 10,00g music vgdata -wi-a----- 4,99g mydocs vgdata -wi-a----- 5,00g
```

Из вывода команды видно, что все три логические тома **films, music и mydoc** входят в группу **vgdata.**
Более подробный вывод показывает команда **lvdisplay.**

Создание файловой системы и монтирование

Следующим шагом будет создание файловой системы на логических томах и в дальнейшем ее монтирование. Приступим к созданию файловой системы ext4 на логических томах.
Для этого выполним команды:

```
sudo mkfs.ext4 /dev/vgdata/mydocs
sudo mkfs.ext4 /dev/vgdata/films
sudo mkfs.ext4 /dev/vgdata/music
```

А теперь смонтируем созданные разделы mydocs, films и music
Но, предварительно создадим для них одноименные каталоги, в качестве точки монтирования.

```
sudo mkdir /media/mydocs /media/films /media/music
```

Теперь выполним команды монтирования:

```
sudo mount /dev/vgdata/mydocs /media/mydocs/
sudo mount /dev/vgdata/films /media/films/
sudo mount /dev/vgdata/music /media/music/
```

Таким образом, мы объединили два физических диска с помощью LVM менеджера в одну логическую группу, затем разделили эту группу на желаемое количество логических томов определенных размеров и создали на них файловую систему.

Пример №2 - Уменьшение размера логического тома

Представим, что нам потребовалось уменьшить раздел films (/dev/vgdata/films), пусть новый размер раздела будет 2 Гб. Посмотрим размеры смонтированных дисков перед уменьшением:

```
sudo df -H
Файловая система Размер Испол Дост Испол%
/dev/mapper/vgdata-mydocs 5,2G 21M 4,9G 1% /media/mydocs
/dev/mapper/vgdata-films 11G 38M 9,9G 1% /media/films
/dev/mapper/vgdata-music 5,2G 21M 4,9G 1% /media/music
```

Перед уменьшением необходимо отмонтировать устройства /dev/vgdata/films:

```
sudo umount /dev/vgdata/films
```

Теперь выполним команду уменьшения размера файловой системы до 2 Гб:

```
sudo resize2fs /dev/vgdata/films 2G
resize2fs 1.42.9 (28-Dec-2013)
Please run 'e2fsck -f /dev/vgdata/films' first.
```

В данной команде параметр 2G указывает на новый желаемый размер, а не на размер на который мы уменьшаем файловую систему. При этом нам предлагается сначала выполнить проверку файловой системы, ок, сделаем это:

```
sudo e2fsck -f /dev/vgdata/films
e2fsck 1.42.9 (28-Dec-2013)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/vgdata/films: 11/655360 files (0.0% non-contiguous), 83137/2621440 blocks
```

Пробуем еще раз запустить уменьшение:

```
sudo resize2fs /dev/vgdata/films 2G
resize2fs 1.42.9 (28-Dec-2013)
Resizing the filesystem on /dev/vgdata/films to 524288 (4k) blocks.
The filesystem on /dev/vgdata/films is now 524288 blocks long.
```

А теперь изменяем размер логического тома:

```
sudo lvreduce -L 2G /dev/vgdata/films
WARNING: Reducing active logical volume to 2,00 GiB.
THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce vgdata/films? [y/n]: y
Size of logical volume vgdata/films changed from 10,00 GiB (2560 extents) to 2,00 GiB (512 extents).
Logical volume vgdata/films successfully resized.
```

Примонтируем раздел и посмотрим размер файловой системы:

```
sudo mount /dev/vgdata/films /media/films/
```

```
sudo df -H
/dev/mapper/vgdata-mydocs 5,2G 21M 4,9G 1% /media/mydocs
/dev/mapper/vgdata-music 5,2G 21M 4,9G 1% /media/music
/dev/mapper/vgdata-films 2,0G 26M 1,9G 2% /media/films
```

Как видим новый размер тома films стал 2Гб.

Пример №3 - Увеличение размера логического тома

Перед увеличением размера тома посмотрим свободное место в логической группе:

```
sudo vgdisplay vgdata
```

```
--- Volume group ---
VG Name vgdata
System ID
Format lvm2
Metadata Areas 2
Metadata Sequence No 11
VG Access read/write
VG Status resizable
MAX LV 0
Cur LV 3
Open LV 3
Max PV 0
Cur PV 2
Act PV 2
VG Size 19,99 GiB
PE Size 4,00 MiB
Total PE 5118
Alloc PE / Size 3070 / 11,99 GiB**Free PE / Size 2048 / 8,00 GiB**VG UUID rmdGbk-Sy5Y-bPns-ufg4-vyV2-Zvez-8v1ayB
```

Видно что в группе свободно 8 Гб, это тот размер который освободился от тома /dev/vgdata/films.

Возьмем их и добавим к /dev/vgdata/music, тем самым увеличив размер тома music на 8 Гб. В отличие от уменьшения, увеличение размера логического тома происходит “на лету” без необходимости размонтирования файловой системы. Выполняем команду:

```
sudo lvextend -L +8G /dev/vgdata/music
Size of logical volume vgdata/music changed from 4,99 GiB (1278 extents) to 8,00 GiB (2048 extents).
Logical volume vgdata/music successfully resized.
```

Теперь необходимо расширить файловую систему на этом логическом томе:

```
sudo resize2fs /dev/vgdata/music
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/vgdata/music is mounted on /media/music; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 2
The filesystem on /dev/vgdata/music is now 3405824 blocks long.
```

Проверяем размер раздела **music**:

```
sudo df -h
```

```
Файловая система Размер Использовано Дост Использовано%
/dev/mapper/vgdata-mydocs 4,8G 20M 4,6G 1% /media/mydocs
/dev/mapper/vgdata-music 13G 25M 13G  1% /media/music
/dev/mapper/vgdata-films 1,9G 25M 1,8G 2% /media/films
```

Пример №4 - Удаление логического тома

Перед удалением логического тома не забудьте сохранить необходимые данные, после этого размонтируйте раздел.

```
sudo umount /dev/vgdata/films
```

Команда удаления:

```
sudo lvremove /dev/vgdata/films
Do you really want to remove active logical volume vgdata/films? [y/n]: y
Logical volume "films" successfully removed
```

В результате на логической группе освободится место.

Пример №5 - Добавление нового диска к группе томов

Для эксперимента мы подключили диск размером 2 Гб к нашей тестовой системе и попробуем включить его в логическую группу LVM - /dev/vgdata.

Выведем текущую информацию о дисках:

```
sudo lvmdiskscan
/dev/ro/root [ 27,99 GiB]
/dev/sda1 [ 1,00 GiB]
/dev/ro/swap [ 3,00 GiB]
/dev/sda2 [ <31,00 GiB] LVM physical volume
/dev/vgdata/mydocs [ 5,00 GiB]
/dev/vgdata/music [ 12,99 GiB]
/dev/sdb [ 10,00 GiB] LVM physical volume
/dev/sdc [ 10,00 GiB] LVM physical volume/dev/sdd [ 2,00 GiB]
```

Новый диск - это **/dev/sdd,** размер его 2 Гб, но тип его не является LVM physical volume, а размер группы vgdata равен 20 Гб.

```
sudo vgs vgdata
VG #PV #LV #SN Attr VSize VFree
vgdata 2 2 0 wz--n- 19,99g 2,00g
```

После добавления размер группы должен стать 22 Гб. Для начала, как и в первой первом примере про разбивку диска с помощью LVM, нам нужно создать из **/dev/sdd** физический том. На данный момент мы видим только существующие физические тома куда не входит /dev/sdd.

```
sudo lvmdiskscan -l
WARNING: only considering LVM devices
/dev/sda2 [ <31,00 GiB] LVM physical volume
/dev/sdb [ 10,00 GiB] LVM physical volume
/dev/sdc [ 10,00 GiB] LVM physical volume
2 LVM physical volume whole disks
1 LVM physical volume
```

Выполняем команду создания физического тома:

```
sudo pvcreate /dev/sdd
Physical volume "/dev/sdd" successfully created.
```

Добавляем физический том в группу vgdata:

```
sudo vgextend vgdata /dev/sdd
Volume group "vgdata" successfully extended
```

Теперь мы видим, что размер группы увеличился на 2 Гб и свободно 4 Гб.

```
sudo vgs vgdata
VG #PV #LV #SN Attr VSize VFree
vgdata 3 2 0 wz--n- <21,99g <4,00g
```

Доступное свободное пространство может быть перераспределено на любой логический раздел, что позволяет увеличить его размер. Данные операции были рассмотрены в предыдущих примерах.

Пример №6 - Удаление физического диска из группы томов

Рассмотрим следующий пример. Представим, что системному администратору потребовалась заменить жесткий диск на другой. При этом данный диск входит в логическую группу LVM. Поэтому первым шагом необходимо убрать из работающей группы томов этот диск, в нашем случае пусть это будет /dev/sdd.

Смотрим текущие состояние /dev/sdd и видим что он входит в группу vgdata и имеет размер 2 Гб.

```
sudo pvs
PV VG Fmt Attr PSize PFree
/dev/sda2 ro lvm2 a-- <31,00g 4,00m
/dev/sdb vgdata lvm2 a-- <10,00g 0
/dev/sdc vgdata lvm2 a-- <10,00g 2,00g
/dev/sdd vgdata lvm2 a-- <2,00g <2,00g
```

Прежде чем его удалить, перенесем данные которые на нем записаны:

```
sudo pvmove /dev/sdd
No data to move for vgdata.
```

Но, поскольку у нас тестовый стенд и данных на дисках нет, то и команда нам сообщает, что данных для переноса нет. Выполняем следующую команду - это удаление из логической группы диск:

```
sudo vgreduce vgdata /dev/sdd
Removed "/dev/sdd" from volume group "vgdata"
```

Удаляем физический диск:

```
sudo pvremove /dev/sdd
Labels on physical volume "/dev/sdd" successfully wiped.
```

Теперь видим, что диск удалился:

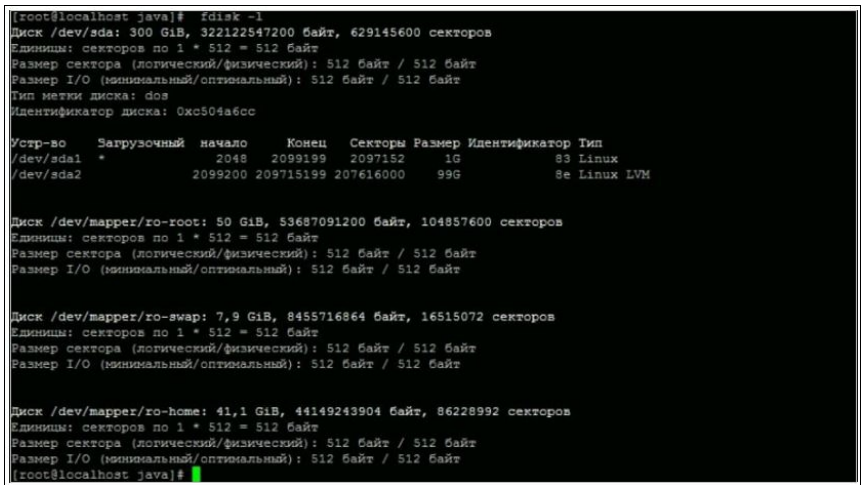
```
sudo pvs
PV VG Fmt Attr PSize PFree
/dev/sda2 ro lvm2 a-- <31,00g 4,00m
/dev/sdb vgdata lvm2 a-- <10,00g 0
/dev/sdc vgdata lvm2 a-- <10,00g 2,00g
```

А значит его можно заменить другим. Как добавить новый диск мы рассмотрели в примере “Пример №5 - Добавление нового диска к группе томов”.

Пример №7 - Расширение корневого раздела типа LVM

Для того чтобы увеличить корневой раздел, используя всё свободное пространство диска **sda**, необходимо выполнить следующие действия: 1. Проверить состояние файловой системы, доступные разделы и свободное место, используя команду:

```
fdisk -l
```

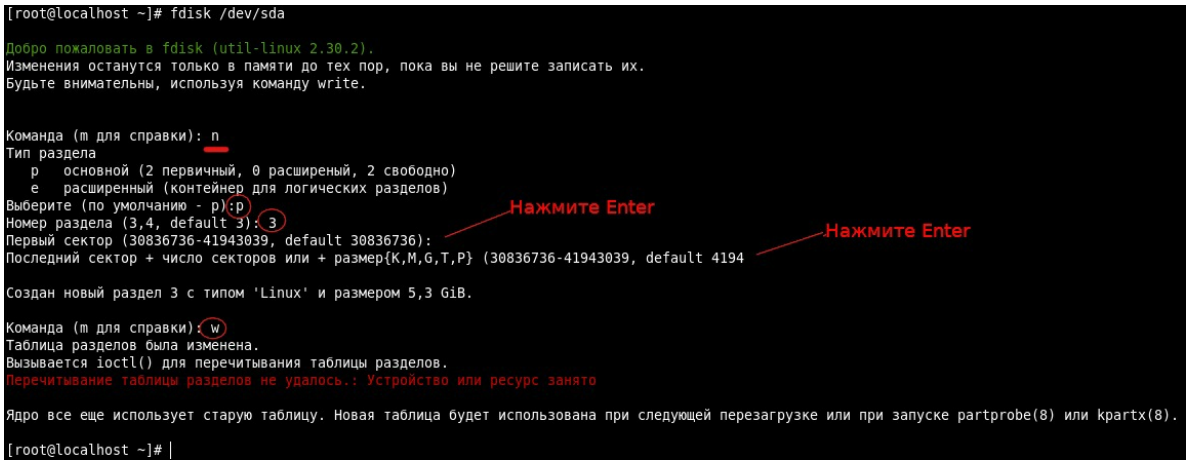


В выводе команды видно, что диск **/dev/sda** имеет размер 300 ГБ, а раздел **/dev/sda2** имеет размер 99 ГБ. На разделе **/dev/sda2** расположены lvm-разделы: • корневой(ro-root) — 50 ГБ; • swap (ro-swap) — 7.9 ГБ; • домашний (ro-home) — 41.1 ГБ.

2. Далее необходимо создать новый раздел, воспользовавшись командой:

```
fdisk /dev/sda
```

Для создания нового раздела требуется ввести нужную команду («**n**») и нажать клавишу «*Enter*». Далее предлагается выбрать тип, который будет установлен для создаваемого раздела, основной («**p**») или расширенный («**e**»). В данном случае следует выбрать основной тип – «**p**». А также необходимо выбрать порядковый номер, который будет присвоен новому разделу, в данном случае – « **3**». Для секторов можно оставить значения по умолчанию, нажав клавишу «*Enter*». Затем остаётся внести изменения в таблицу разделов командой «**w**». После этого терминал сообщает, что изменения в таблицу разделов внесены, а это означает, что новый раздел создан.



Чтобы операционная система узнала о новых границах разделов без перезагрузки, необходимо выполнить команду:

```
partprobe /dev/vda
```

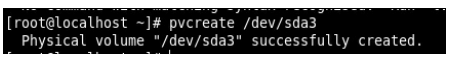
Чтобы убедиться, что внесённые изменения применены, используйте команду:

```
fdisk -l
```

В выводе команды видно, что появился новый раздел **/dev/sda3** размером 200 ГБ.

3. Следующим шагом нужно создать LVM физический том из раздела **sda3**, набрав команду:

```
pvcreate /dev/sda3
```



4. Следует проверить существующую логическую группу, чтобы затем добавить в неё новый физический том. Для этого используются команды:

```
vgs
```

```
[root@localhost ~]# vgs
  VG #PV #LV #SN Attr   VSize   VFree
  ro   1   3   0 wz--n- <13,70g 4,00m
```

```
vgextend ro /dev/sda3
```

```
[root@localhost ~]# vgextend ro /dev/sda3
  Volume group "ro" successfully extended
```

5. Для определения корневого раздела необходимо вывести список существующих логических томов, используя команду:

```
lvdisplay
```

```
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Path                /dev/ro/swap
  LV Name                swap
  VG Name                ro
  LV UUID                XbCnjV-WkUs-SAlh-tbG8-dJmf-s83P-B7s3TH
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:33 +0300
  LV Status              available
  # open                 2
  LV Size                <7,88 GiB
  Current LE             2016
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:1

  --- Logical volume ---
  LV Path                /dev/ro/home
  LV Name                home
  VG Name                ro
  LV UUID                9abMf8-L5u9-RR4j-qdBB-Usxo-BqXK-cUDngx
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:34 +0300
  LV Status              available
  # open                 1
  LV Size                <41,12 GiB
  Current LE             10526
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:2

  --- Logical volume ---
  LV Path                /dev/ro/root
  LV Name                root
  VG Name                ro
  LV UUID                OZx76J-FRay-e5wi-XA5u-f1Cp-r5se-1NIfOM
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:37 +0300
  LV Status              available
  # open                 1
  LV Size                50,00 GiB
  Current LE             12800
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:0
```

В выводе команды видно, что корневой раздел — это /dev/ro/root, его и следует расширить. Для этого используется команда:

```
lvextend -l +100%FREE /dev/ro/root
```

```
[root@localhost ~]# lvextend -l +100%FREE /dev/ro/root
  Size of logical volume ro/root changed from 50,00 GiB (12800 extents) to 250,00 GiB (64000 extents).
  Logical volume ro/root successfully resized.
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Path                /dev/ro/swap
  LV Name                swap
  VG Name                ro
  LV UUID                XbCnjV-WkUs-SA1h-tbG8-dJmf-s83P-B7s3TH
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:33 +0300
  LV Status              available
  # open                 2
  LV Size                <7,88 GiB
  Current LE             2016
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:1

  --- Logical volume ---
  LV Path                /dev/ro/home
  LV Name                home
  VG Name                ro
  LV UUID                9abMf8-L5u9-RR4j-qdBB-Usxo-BqXK-oUDngx
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:34 +0300
  LV Status              available
  # open                 1
  LV Size                <41,12 GiB
  Current LE             10526
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:2

  --- Logical volume ---
  LV Path                /dev/ro/root
  LV Name                root
  VG Name                ro
  LV UUID                OZx76J-FRay-e5wi-XA5u-f1Cp-r5se-1NIfOM
  LV Write Access        read/write
  LV Creation host, time localhost.localdomain, 2020-11-27 16:01:37 +0300
  LV Status              available
  # open                 1
  LV Size                250,00 GiB
  Current LE             64000
  Segments               2
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           254:0

[root@localhost ~]#
```

После расширения раздела, необходимо изменить размер файловой системы.

6. Изменение размера файловой системы

6.1 Перед изменением размера файловой системы необходимо выполнить проверку файловой системы на ошибки, для файловой системы ext4:

```
e2fsck -f /dev/ro/root
```

Если используется файловая система xfs, то команда будет следующая:

```
xfs_growfs /dev/ro/root
```

6.2 Следующая команда автоматически расширяет файловую систему до максимально доступного размера:

```
resize2fs /dev/ro/root
```

```
[root@localhost ~]# resize2fs /dev/ro/root
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/ro/root is mounted on /; on-line resizing required
old_desc_blocks = 7, new_desc_blocks = 32
The filesystem on /dev/ro/root is now 65536000 blocks long.
```

Для просмотра размеров разделов используется команда:

```
df -h
```

```
[root@localhost ~]# resize2fs /dev/ro/root
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/ro/root is mounted on /; on-line resizing required
old_desc_blocks = 7, new_desc_blocks = 32
The filesystem on /dev/ro/root is now 65536000 blocks long.

[root@localhost ~]# 0
-bash: 0: команда не найдена
[root@localhost ~]# dh -h
-bash: dh: команда не найдена
[root@localhost ~]# df -h
Файловая система    Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs              3,9G            0  3,9G            0% /dev
tmpfs                 3,9G          24K  3,9G            1% /dev/shm
tmpfs                 3,9G         9,3M  3,9G            1% /run
tmpfs                 3,9G            0  3,9G            0% /sys/fs/cgroup
/dev/mapper/ro-root   246G         5,7G  230G            3% /
/dev/sda1             976M         126M  784M           14% /boot
/dev/mapper/ro-home    41G         1,6G   37G            4% /home
tmpfs                 797M          24K  797M            1% /run/user/1000
tmpfs                 797M            0  797M            0% /run/user/0
[root@localhost ~]#
```

Как видно из вывода команды, корневой раздел ro-root расширился и имеет размер памяти 246 ГБ.

Утилиты для работы с дисковым пространством

Утилита df — просмотр свободного пространства
Утилита du — просмотр занятого пространства
Утилита find — поиск файлов большого размера

Вы можете подробнее ознакомиться с информацией по поиску файлов в системе и оценке свободного дискового пространства, просмотрев наши обучающие видео:

- на **RuTube**:
  - Утилиты поиска файлов;
  - Анализ занятого пространства на дисках.
- в **Яндекс.Дзен**:
  - Утилиты поиска файлов;
  - Анализ занятого пространства на дисках.
- в **VK Видео**:
  - Утилиты поиска файлов;
  - Анализ занятого пространства на дисках.

На наших каналах вы также сможете найти много другой полезной информации.

Утилита df — просмотр свободного пространства

df — стандартная утилита проверки свободного места, позволяет выводить список подключенных устройств, информацию о занятом месте, а также точку монтирования.

Синтаксис:

```
df <опции> [устройство]
```

Опции:

- **-a**, **--all** — отобразить все файловые системы, в том числе виртуальные, псевдо и недоступные;
- **-B, --block-size=n** — отобразить размеры в блоках по n-байт каждый;
- **-h, --human-readable** — выводить размеры в удобном формате;
- **-H** — выводить все размеры в гигабайтах;
- **-i** — выводить информацию об inode;
- **-k** — выводить размеры в килобайтах;
- **--output** — использовать специальный формат вывода, если не задано, выводит все поля. Доступны такие варианты: 'source', 'fstype', 'itotal', 'iused', 'iavail', 'ipcent', 'size', 'used', 'avail', 'pcent', 'file' и 'target';
- **-P** — использовать формат вывода POSIX;
- **--total** — выводить всю информацию про использованное и доступное место;
- **-t**, **--type** — выводить информацию только про указанные файловые системы;
- **-x** — выводить информацию обо всех, кроме указанных, файловых системах.

Использование:

Для того чтобы просмотреть доступное пространство на всех примонтированных разделах и информацию о них, выполните:

```
df

Файловая система        1K-блоков Использовано Доступно Использовано% Смонтировано в
devtmpfs                   479228         0   479228         0% /dev
tmpfs                      497892         0   497892         0% /dev/shm
tmpfs                      199160      3224   195936         2% /run
/dev/mapper/ro_redos-root  17410832    8998132  7505232        55% /
/dev/sda1                  999320     174776   755732        19% /boot
tmpfs                      99576        76    99500         1% /run/user/42
tmpfs                      99576       132    99444         1% /run/user/1000
```

```
/dev/sr0                4533928     4533928       0         100% /run/media/user/redos-MUROM-8 x86_64
```

Для просмотра свободного пространства какого-либо раздела в наиболее читаемом формате выполните:

```
df -h /root

Файловая система Размер Использовано  Дост Использовано% Смонтировано в
/dev/sda4          16G         12G  3,3G          79% /
```

Утилита du — просмотр занятого пространства

du — утилита, которая позволяет вывести размер всех файлов в определённой папке в байтах или в более удобном формате.

Синтаксис:

```
du <опции> <путь_к_папке>
```

Опции:

- **-a**, **--all** — выводить размер для всех файлов, а не только для директорий, по умолчанию размер выводится только для папок;
- **-B**, **--block-size** — использовать блоки указанного размера, доступны единицы измерения: K, M, G, T, P, E, Z, Y (степень 1024) или KB, MB и т.д. (степень 1000);
- **-c**, **--total** — выводить в конце общий размер всех папок;
- **-d**, **--max-depth** — максимальная глубина вложенности директорий;
- **-h**, **--human-readable** — выводить размеры в степени 1024;
- **--inodes** — выводить информацию об использовании inode;
- **-L**, **--dereference** — следовать по всем символическим ссылкам;
- **-l**, **--count-links** — учитывать размер файла несколько раз для жестких ссылок;
- **-P**, **--no-dereference** — не следовать по символическим ссылкам, это поведение используется по умолчанию;
- **-S**, **--separate-dirs** — не включать размер подпапок в размер папки;
- **--si** — выводить размер файлов и папок в удобном виде, используется степень 1000 вместо 1024;
- **-s**, **--summarize** — выводить только общий размер;
- **-t**, **--threshold** — не учитывать файлы и папки с размером меньше указанного;
- **--time** — отображать время последней модификации для файла или папки, вместо времени модификации можно выводить такие метки, как atime, access, use, ctime;
- **-X**, **--exclude** — исключить файлы из подсчёта;
- **-x**, **--one-file-system** — пропускать примонтированные файловые системы;
- **--version** — вывести версию утилиты.

Использование:

Для просмотра занимаемого пространства теми или иными файлами в какой-либо папке, выполните команду:

```
du /home/user

4    ./Документы/test_dir
328    ./Документы/dark-matter/icons
2336    ./Документы/dark-matter
412    ./Документы/Hoshimati Suisei/Suisei/icons
3584    ./Документы/Hoshimati Suisei/Suisei
5568    ./Документы/Hoshimati Suisei
212    ./Документы/THEMES/Vimix-4k/Vimix/icons
3136    ./Документы/THEMES/Vimix-4k/Vimix
4504    ./Документы/THEMES/Vimix-4k
4508    ./Документы/THEMES
16284    ./Документы

 ...
```

```
8    ./.config/caja-actions
4    ./.config/imsettings
4    ./.config/menus/applications-merged
8    ./.config/menus
62184    ./.config
4    ./.themes
1230796    .
```

Для более читаемого вывода команды можно добавить дополнительные опции:

```
du -sh /home/user

1,2G    /home/user
```

Утилита find — поиск файлов большого размера

Утилита **find** — одна из наиболее важных и часто используемых утилит системы, которая позволяет осуществлять поиск файлов и каталогов на основе специальных условий. Ее можно использовать в различных обстоятельствах, например, для поиска файлов по разрешениям, владельцам, группам, типу, размеру и другим подобным критериям.

Чтобы при помощи **find** найти файлы большого размера необходимо выполнить:

```
find . -xdev -type f -size +<необходимый_размер>
```

Например:

```
find . -xdev -type f -size +100M

./Загрузки/Yandex.rpm
./Загрузки/FreeCAD_0.21.2-Linux-Conda_glibc2.12-aarch64.AppImage
```

Вывести файлы в более удобном формате можно следующим образом:

```
find . -xdev -type f -size +10M -print | xargs ls -lh | sort -k5,5 -h -r | head

-rw-r--r--. 1 user user 21M окт 18 22:28 ./Загрузки/sample-30s.mp4
-rw-------. 1 user user 14M окт 18 22:28 ./Загрузки/Yandex.rpm
-rw-r--r--. 1 user user 12M окт 18 22:28 ./Загрузки/sample-15s.mp4
```

Мониторинг файловой системы с помощью duf

Установка
Синтаксис утилиты
Опции
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: duf-0.8.1-1

Duf (**Disk Usage/Free**) — это терминальная утилита, которая позволяет удобно отображать информацию о дисковом пространстве. Она предоставляет подробные данные о свободном и занятом пространстве на дисках в удобочитаемой и визуально понятной форме по сравнению с классическими утилитами, такими как **df** и **du**.

Основные характеристики:

- цветовое отображение для легкого восприятия;
- настройка в соответствии с тематикой и шириной терминала;
- сортировка результатов в соответствии с потребностями пользователя;
- группировка и фильтрация устройств;
- вывод данных в различных форматах, таких как *JSON*, что позволяет их интегрировать в другие инструменты.

Установка

Для установки утилиты через терминал выполните команду (потребуются права **администратора**):

```
dnf install duf
```

Синтаксис утилиты

Синтаксис утилиты имеет вид:

```
duf [<опции>] [<параметры>]
```

Опции

К основным опциям утилиты относятся:

- **-all** — отобразить все файловые системы, включая псевдоустройства, дублирующиеся и недоступные файловые системы;
- **-avail-threshold** — указать пороговое значение для подсвечивания столбца avail (доступное пространство) в выводе. Указанное значение используется для подсвечивания различных уровней доступного дискового пространства определенным цветом для облегчения визуальной оценки состояния дисков. По умолчанию, если объем доступного дискового пространства менее 10 ГБ, значение будет подсвечено желтым цветом. Если объем доступного дискового пространства менее 1 ГБ, значение будет подсвечено красным цветом;
- **-hide** — используется для скрытия определенных типов устройств в выводе (указываются через запятую).

  Возможные значения для -hide:

  - *local*: локальные устройства;
  - *network*: сетевые устройства;
  - *fuse*: FUSE (Filesystem in Userspace) устройства;
  - *special*: специальные устройства;
  - *loops*: loopback устройства;
  - *binds*: устройства, смонтированные с использованием bind mount.

- **-hide-fs** — исключить из отображаемого списка конкретные типы файловых систем, разделенные запятыми;
- **-hide-mp** — скрыть определенные точки монтирования, разделенные запятыми (поддерживаются шаблоны для указания групп точек монтирования);
- **-inodes** — отобразить информацию об индексных дескрипторах вместо использования блоков. Индексные дескрипторы представляют собой структурные элементы файловой системы, которые содержат информацию о файлах и каталогах;

- **-json** — вывести все устройства в формате JSON, используется для интеграции с другими инструментами и для автоматизированной обработки данных;
- **-only** — показать только определенные устройства, разделенные запятыми: *local*, *network*, *fuse*, *special*, *loops*, *binds*;
- **-only-fs** — показать только определенные файловые системы, разделенные запятыми;
- **-only-mp** — показать только определенные точки монтирования, разделенные запятыми (поддерживаются шаблоны для указания групп точек монтирования);
- **-output** — определить, какие поля будут включены в вывод: *mountpoint*, *size*, *used*, *avail*, *usage*, *inodes*, *inodes_used*, *inodes_avail*, *inodes_usage*, *type*, *filesystem*;
- **-sort** — сортировать вывод по указанным полям: *mountpoint*, *size*, *used*, *avail*, *usage*, *inodes*, *inodes_used*, *inodes_avail*, *inodes_usage*, *type*, *filesystem* (по умолчанию - «*mountpoint*»);
- **-style** — определить стиль вывода: *unicode*, *ascii* (по умолчанию - «*unicode*»);
- **-theme** — установить цветовую тему вывода: *dark*, *light*, *ansi* (по умолчанию - «*dark*»);
- **-usage-threshold** — указать пороговое значение для окрашивания полос использования (желтый, красный) в виде числа с плавающей точкой от 0 до 1 (по умолчанию - «0.5,0.9»);
- **-version** — показать версию утилиты duf;
- **-warnings** — вывести все предупреждения в STDERR;
- **-width** — максимальная ширина вывода.

Примеры использования

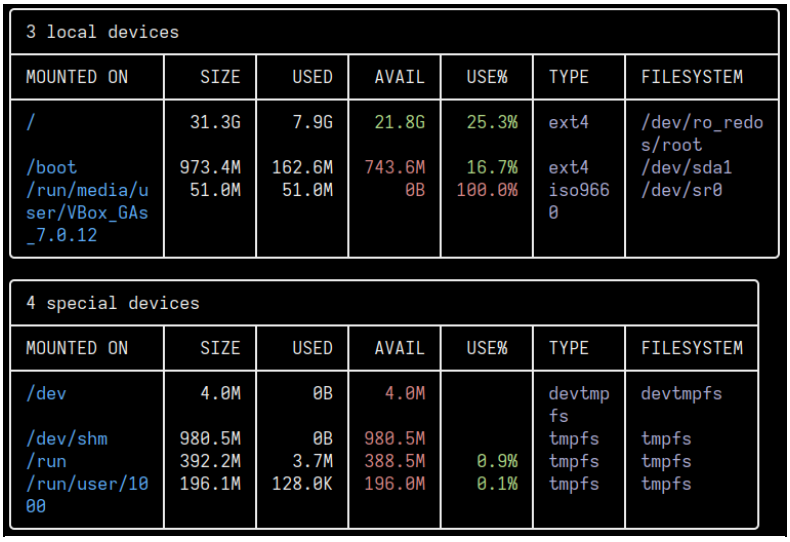
Пример 1. Базовое использование

Для отображения основной информации об использовании дискового пространства выполните команду в терминале:

```
duf
```

Команда **duf** без использования опций выводит основную информацию обо всех файловых системах в удобочитаемом формате с цветовым выделением. По умолчанию отображаются такие колонки, как точка монтирования, размер, использованное пространство, доступное пространство, использование в процентном соотношении, тип и имя файловой системы.

Результат выполнения:



3 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	16.7%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	51.0M	51.0M	0B	100.0%	iso9660	/dev/sr0

4 special devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/dev/shm	980.5M	0B	980.5M		tmpfs	tmpfs
/run	392.2M	3.7M	388.5M	0.9%	tmpfs	tmpfs
/run/user/1000	196.1M	128.0K	196.0M	0.1%	tmpfs	tmpfs

Для каждого типа устройства выводится информация в виде таблицы. Утилита разделяет всю информацию в таблице на колонки, в которых освещена следующая информация:

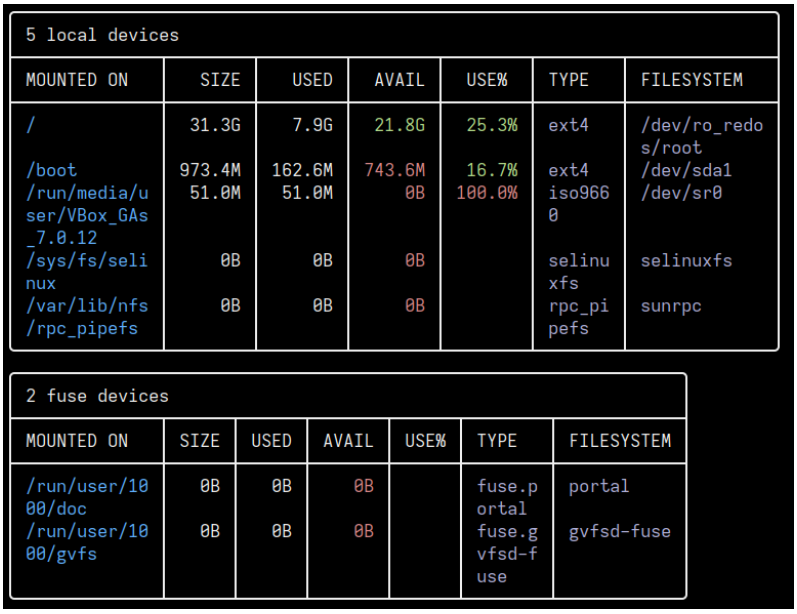
- **MOUNTED ON** — точка монтирования файловой системы, то есть путь в файловой системе, где устройство смонтировано;
- **SIZE** — общий размер файловой системы;
- **USED** — объем занятого пространства на файловой системе;
- **AVAIL** — объем доступного (свободного) пространства на файловой системе;
- **USE%** — процент использованного дискового пространства на файловой системе;
- **TYPE** — тип файловой системы;
- **FILESYSTEM** — имя или путь к устройству или файловой системе.

Пример 2. Показать все файловые системы, включая псевдоустройства и дублирующиеся устройства

Для отображения в выводе всех файловых систем, включая псевдоустройства, дублирующиеся и недоступные файловые системы используется опция **-all**. Она позволяет получить полное представление обо всех файловых системах, включая те, которые обычно скрыты.

```
duf -all
```

Результат выполнения:



5 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	16.7%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	51.0M	51.0M	0B	100.0%	iso9660	/dev/sr0
/sys/fs/selinux	0B	0B	0B		selinuxfs	selinuxfs
/var/lib/nfs/rpc_pipefs	0B	0B	0B		rpc_pipefs	sunrpc

2 fuse devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/run/user/1000/doc	0B	0B	0B		fuse.portal	portal
/run/user/1000/gvfs	0B	0B	0B		fuse.gvfsd-fuse	gvfsd-fuse

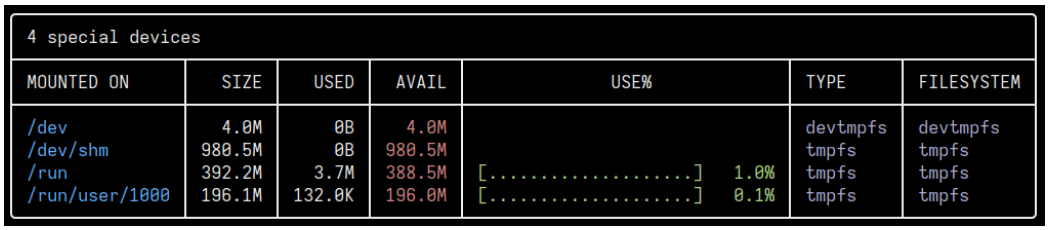
Пример 3. Скрыть определенные устройства

Для исключения из вывода локальных и сетевых устройств используется опция **-hide**.

```
duf -hide local,network
```

Это может быть полезно, если необходимо вывести только определенные типы устройств, исключив ненужные.

Результат выполнения:



4 special devices

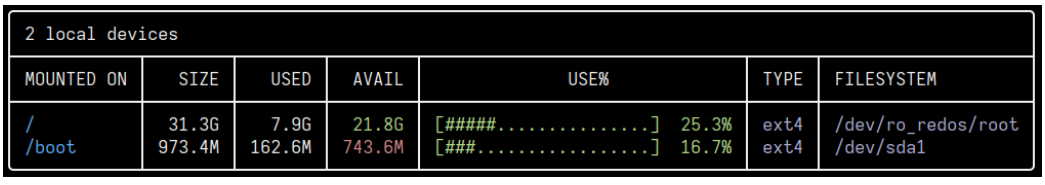
MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/dev/shm	980.5M	0B	980.5M		tmpfs	tmpfs
/run	392.2M	3.7M	388.5M	[..................] 1.0%	tmpfs	tmpfs
/run/user/1000	196.1M	132.0K	196.0M	[..................] 0.1%	tmpfs	tmpfs

Пример 4. Отобразить только определенные файловые системы

Опция **-only** используется для фильтрации по конкретным типам файловых систем. Для отображения только необходимых файловых систем, которые имеют тип *ext4* или *xfs,* введите команду:

```
duf -only-fs ext4,xfs
```

Результат выполнения:



2 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	[#####..............] 25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	[###................] 16.7%	ext4	/dev/sda1

Пример 5. Вывод в формате JSON

Опция **-json** позволит вывести всю информацию о файловых системах в формате *JSON*. Это удобно для последующего анализа или использования в других скриптах и инструментах:

```
duf -json
```

Результат выполнения:

```
{
 "device": "binfmt_misc",
 "device_type": "special",
 "mount_point": "/proc/sys/fs/binfmt_misc",
 "fs_type": "binfmt_misc",
 "type": "binfmt_misc",
 "opts": "rw,nosuid,nodev,noexec,relatime",
 "total": 0,
 "free": 0,
 "used": 0,
 "inodes": 0,
 "inodes_free": 0,
 "inodes_used": 0,
 "blocks": 0,
 "block_size": 4096
}
```

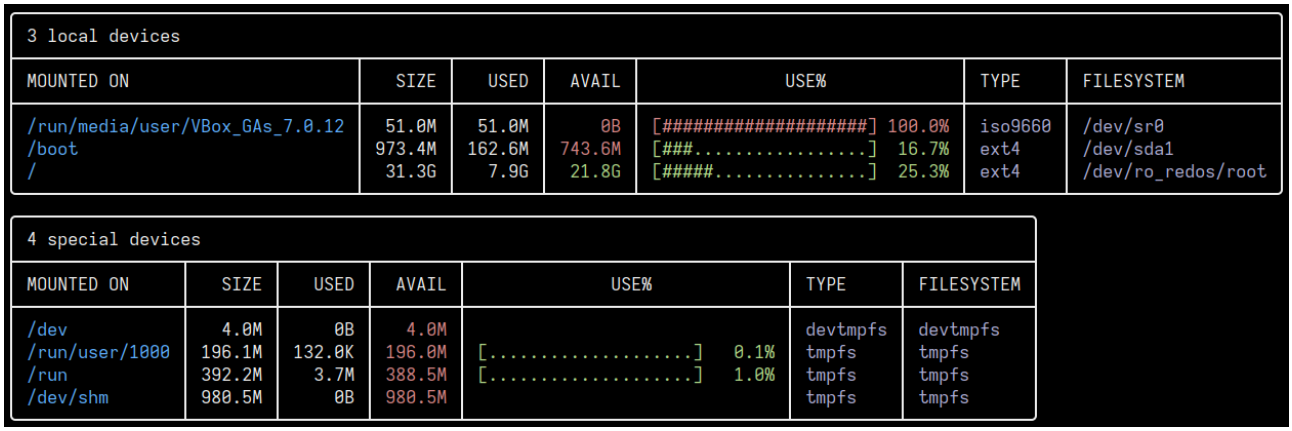

Пример 6. Сортировка по размеру

Для сортировки информации в столбцах таблицы можно воспользоваться опцией **-sort** с указанием столбца. Это позволяет легко увидеть, какие файловые системы имеют наибольший или наименьший размер.

Например, для сортировки выводимой информации по величине общего размера введите в терминале:

```
duf -sort size
```

Результат выполнения:



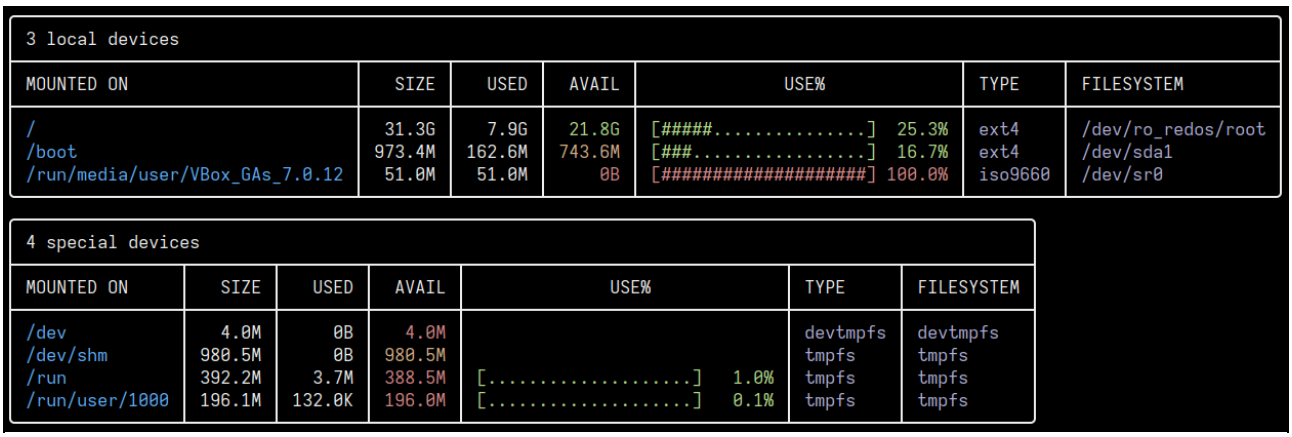
Пример 7. Установка порога для подсвечивания доступного пространства

Опция **-avail-threshold** устанавливает пороговые значения для подсвечивания столбца avail (доступное пространство).

```
duf -avail-threshold 5G,500M
```

В данном примере, если доступное место меньше 5 ГБ, оно будет подсвечено желтым цветом, а если меньше 500 МБ — красным.

Результат выполнения:

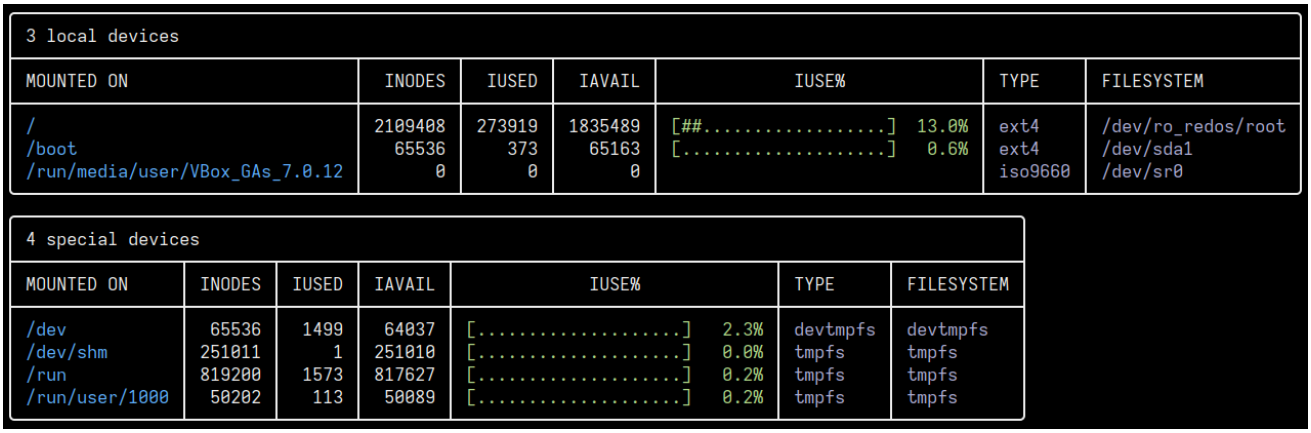


Пример 8. Показать информацию об индексных дескрипторах (inodes)

Для отображения информации об индексных дескрипторах вместо стандартных данных о блоках используется опция **-inodes**. Информация включает количество индексных дескрипторов, использованные и доступные индексные дескрипторы, а также процент использования индексных дескрипторов. Например:

```
duf -inodes
```

Результат выполнения:



3 local devices

MOUNTED ON	INODES	IUSED	IAVAIL	IUSE%	TYPE	FILESYSTEM
/	2109408	273919	1835489	[##.....] 13.0%	ext4	/dev/ro_redos/root
/boot	65536	373	65163	[.....] 0.6%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	0	0	0		iso9660	/dev/sr0

4 special devices

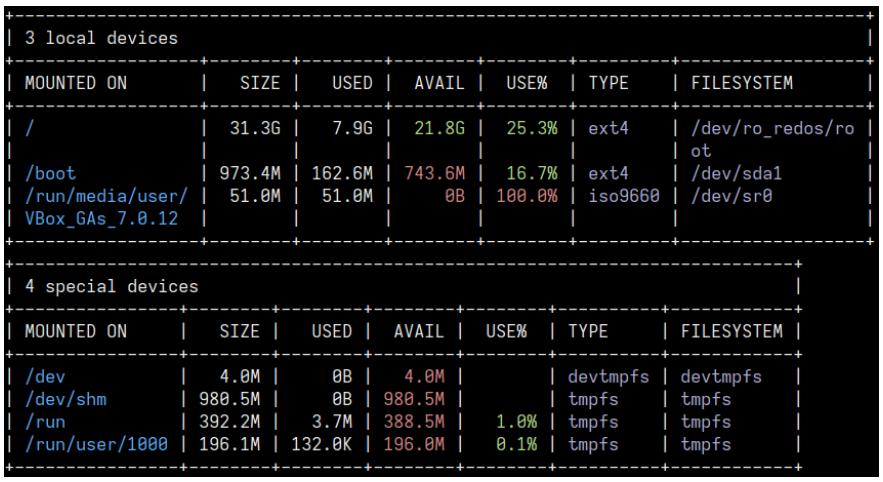
MOUNTED ON	INODES	IUSED	IAVAIL	IUSE%	TYPE	FILESYSTEM
/dev	65536	1499	64037	[.....] 2.3%	devtmpfs	devtmpfs
/dev/shm	251011	1	251010	[.....] 0.0%	tmpfs	tmpfs
/run	819200	1573	817627	[.....] 0.2%	tmpfs	tmpfs
/run/user/1000	50202	113	50089	[.....] 0.2%	tmpfs	tmpfs

Пример 9. Выбор стиля отображения

Опция **-style** с параметром **<ascii>** устанавливает стиль отображения в формате ASCII вместо Unicode. Это может быть полезно для систем, где поддержка Unicode ограничена.

```
duf -style ascii
```

Результат выполнения:



3 local devices

MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/	31.3G	7.9G	21.8G	25.3%	ext4	/dev/ro_redos/root
/boot	973.4M	162.6M	743.6M	16.7%	ext4	/dev/sda1
/run/media/user/VBox_GAs_7.0.12	51.0M	51.0M	0B	100.0%	iso9660	/dev/sr0

4 special devices

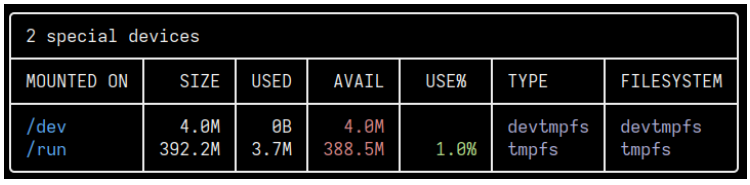
MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/dev/shm	980.5M	0B	980.5M		tmpfs	tmpfs
/run	392.2M	3.7M	388.5M	1.0%	tmpfs	tmpfs
/run/user/1000	196.1M	132.0K	196.0M	0.1%	tmpfs	tmpfs

Пример 10. Показать только определенные точки монтирования

Для фокусировки на конкретных директориях полезна опция **-only-mp.** В примере будут отображены только те файловые системы, которые смонтированы в точках /dev и /run.

```
duf -only-mp /dev,/run
```

Результат выполнения:



2 special devices

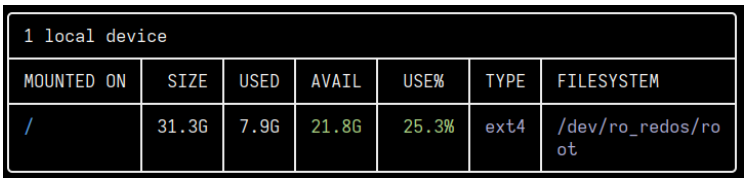
MOUNTED ON	SIZE	USED	AVAIL	USE%	TYPE	FILESYSTEM
/dev	4.0M	0B	4.0M		devtmpfs	devtmpfs
/run	392.2M	3.7M	388.5M	1.0%	tmpfs	tmpfs

Пример 11. Показать информацию о файловой системе

Для отображения информации о конкретном разделе файловой системы или устройстве хранения информации нужно выполнить следующую команду:

```
duf /home
```

Результат выполнения:



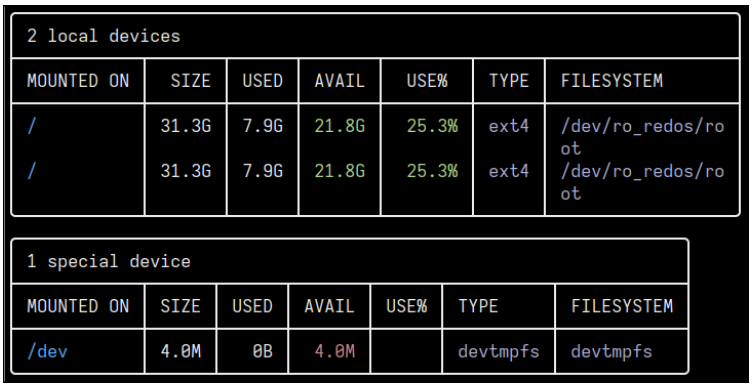
Утилита **duf** анализирует файловую систему, на которой находится директория /home, и выводит информацию о ней.

Пример 12. Показать информацию о файловых системах

В приведенном ниже примере duf выводит информацию о файловых системах, на которых смонтированы директории /dev, /etc/opt и /var/log. Выходные данные имеют три записи, каждая из которых соответствует устройству для одного из входных путей:

```
duf /dev /etc/opt /var/log
```

Результат выполнения:



Пример 13. Вывод информации о точках монтирования

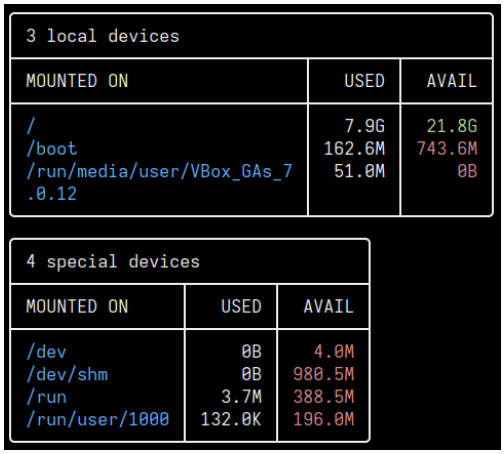
Для вывода определенных столбцов в таблице, можно воспользоваться опцией **-output** с указанием (через запятую) необходимых столбцов.

Например, для вывода столбцов точки монтирования, занятого места и места, которое еще свободно:

```
duf -output mountpoint,used,avail
```

Эта команда выводит информацию только о точках монтирования, объеме использованного и доступного пространства. Это полезно, если нужно кратко оценить текущее использование дискового пространства без дополнительных деталей.

Результат выполнения:



Квоты для директорий в РЕД ОС (ограничение размера каталога)

В данной инструкции будет рассмотрено создание образа файловой системы для хранения нужной информации и последующего его подключения в точку монтирования.

Вы можете подробнее ознакомиться с настройкой квот для каталогов, просмотрев наши обучающие видео:

- на **RuTube** — Создание каталогов с ограничением их размера;
- в **Яндекс.Дзен** — Создание каталогов с ограничением их размера;
- в **VK Видео** — Создание каталогов с ограничением их размера.

На наших каналах вы также сможете найти много другой полезной информации.

Создайте каталог для точки монтирования образа:

```
sudo mkdir -p /data/share/dirquota
```

Создайте образ файловой системы с указанием его объема:

```
sudo dd if=/dev/zero of=/data/quota.img bs=1024 count=100000
```

Отформатируйте файловый образ:

```
sudo mkfs.ext4 /data/quota.img
```

Подключите образ к точке монтирования:

```
sudo mount -o loop /data/quota.img /data/share/dirquota
```

Для автоматического монтирования созданного образа откройте для редактирования файл **fstab**:

```
sudo nano /etc/fstab
```

Добавьте в файл следующую строку:

```
/data/quota.img/ /data/share/dirquota ext4 loop 1 2
```

Для увеличения или уменьшения объема файловой системы можно использовать **resize2fs**:

```
sudo resize2fs -p quota.img 1000M
```

Для проверки целостности выполните:

```
sudo e2fsck -f quota.img
```

Уменьшение размера диска для установки ОС Windows на один диск с РЕД ОС

Изменение размера логического тома
Работа с Gparted
Восстановление загрузчика GRUB

Допустим, имеется один физический диск размером **50 Гб**, на который установлена система РЕД ОС с разбивкой диска по умолчанию. Т.е. все свободное пространство размечено в **LVM**. Необходимо установить на этот диск *ОС Windows* так, чтобы осталась возможность запускать *РЕД ОС*. Для этого следует под *Windows* выделить свободное дисковое пространство.

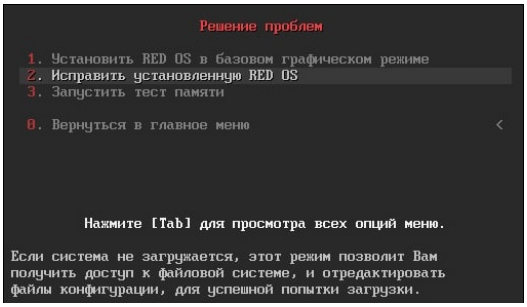
ВАЖНО!

Очень важно, чтобы сначала был уменьшен **размер файловой системы**, затем **тома**. Также важно не уменьшить размер тома больше, чем уменьшен размер файловой системы. В противном случае данные могут быть уничтожены.

Перед выполнением операции **обязательно** необходимо создать **копию** важных **данных**.

Изменение размера логического тома

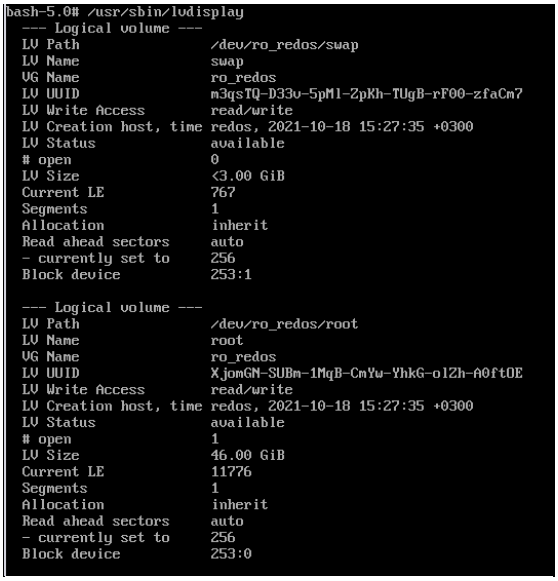
Загрузитесь в режиме восстановления (**Rescue**) с диска установки РЕД ОС. Выберите пункт "**2. Исправить установленную RED OS**".



В этом режиме выберите 3 пункт, для перехода в командную строку. В режиме "**Skip to shell**" дисковые разделы не будет примонтированы, что позволит нам произвести необходимые настройки с логическими томами.



Выполните команду **lvdisplay** для просмотра логических томов.



На рисунке видно, что наибольший размер у **/dev/ro_redos/root**, он имеет размер **46 Гб**, его и следует уменьшать.

Проверьте активность lvm-томов командой **lvscan**:

```
bash-5.0# lvscan
  inactive          '/dev/ro_redos/swap' [<3.00 GiB] inherit
  inactive          '/dev/ro_redos/root' [46.00 GiB] inherit
bash-5.0#
```

Если тома не активны, то активируйте нужный том командой:

```
lvchange -ay /dev/ro_redos/root
```

```
bash-5.0# lvchange -a y /dev/ro_redos/root
bash-5.0# lvscan
  inactive          '/dev/ro_redos/swap' [<3.00 GiB] inherit
  ACTIVE            '/dev/ro_redos/root' [46.00 GiB] inherit
```

Далее следует выполнить проверку LVM-раздела:

```
e2fsck -f /dev/ro_redos/root
```

```
bash-5.0# e2fsck -f /dev/ro_redos/root
e2fsck 1.44.6 (5-Mar-2019)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/ro_redos/root: 196383/3014656 files (0.1% non-contiguous), 1858089/12058624 blocks
```

Уменьшите размер корневого (/) раздела **на файловой системе** до 14 Гб.

14 Гб — это размер, который нужно задать для файловой системы, а не на который уменьшается ФС:

```
resize2fs /dev/ro_redos/root 14G
```

```
bash-5.0# resize2fs /dev/ro_redos/root 14G
resize2fs 1.44.6 (5-Mar-2019)
Resizing the filesystem on /dev/ro_redos/root to 3670016 (4k) blocks.
The filesystem on /dev/ro_redos/root is now 3670016 (4k) blocks long.
```

Уменьшите размер **LVM-тома /dev/ro_redos/root** до размера 14 Гб:

```
lvreduce -L 14G /dev/ro_redos/root
```

```
bash-5.0# lvreduce -L 14G /dev/ro_redos/root
  WARNING: Reducing active logical volume to 14.00 GiB.
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce ro_redos/root? [y/n]: y
  Size of logical volume ro_redos/root changed from 46.00 GiB (11776 extents) to 14.00 GiB (3584 ext
ents).
  Logical volume ro_redos/root successfully resized.
```

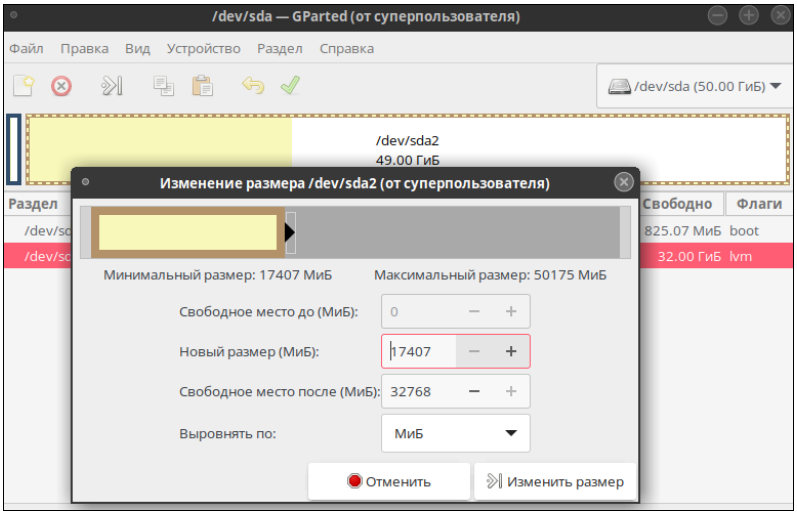
После этого перезагрузите ПК, войдите в систему через графическое окружение.

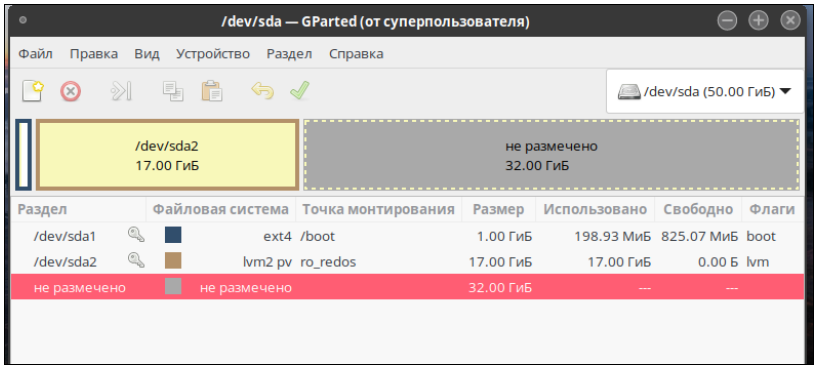
Работа с Gparted

Установите графическую утилиту **Gparted** для последнего шага изменения размера раздела.

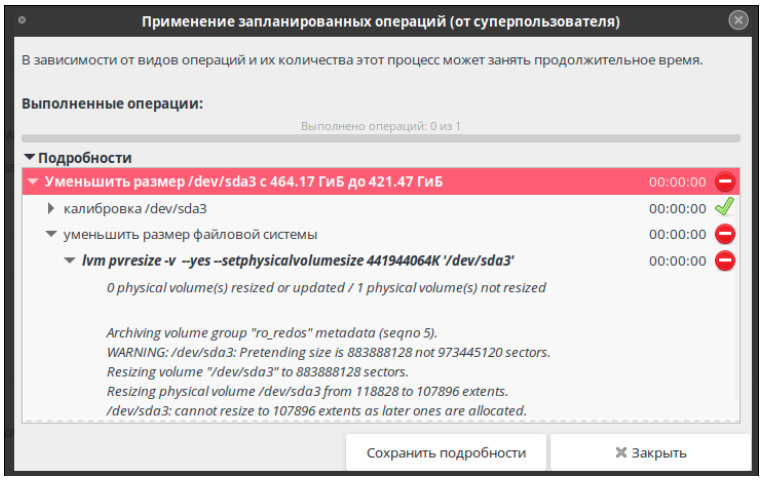
```
dnf install gparted
```

После установки **Gparted** появилась возможность изменить размер раздела, введите необходимые значения.





После уменьшения размера LVM-тома в режиме восстановления с установочного диска РЕД ОС и последующем изменении размера в **Gparted** может возникать ошибка, которая указывает о недостатке свободных экстентов.



Такое происходит из-за того, что свободные экстенты находятся в середине lvm-тома.

Проверить это можно командой:

```
pvs -v --segments /dev/nvme0n1p3
```

где вместо «**/dev/nvme0n1p3**» необходимо указать свой каталог с физическим устройством.

```
[root@localhost admin]# pvs -v --segment /dev/nvme0n1p3
  PV           VG       Fmt  Attr PSize   PFree    Start  SSize LV   Start Type   PE Ranges
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g      0 17920 root     0 linear /dev/nvme0n1p3:0-17919
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g  17920 50816 home     0 linear /dev/nvme0n1p3:17920-68735
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g  68736 50984          0 free
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 119720  1970 swap     0 linear /dev/nvme0n1p3:119720-121689
[root@localhost admin]#
```

Как видно из ответа команды между логическими томами **home** и **swap** есть свободное место. Для успешной разметки в **Gparted** необходимо переместить **swap** в свободное место.

Сначала необходимо убедиться, что раздел **swap** не смонтирован. Для этого нужно выполнить команду:

```
swapoff -a
```

Далее необходимо переместить раздел подкачки. Разделы находятся на одном диске, поэтому следует указать политику распределения **anywhere**. В результате этого логический том перемещается в начало свободного места.

Для этого следует ввести команду:

```
pvmove --alloc anywhere /dev/nvme0n1p3:119720-121689
```

где вместо «**/dev/nvme0n1p3:119720-121689**» указать свои данные логического тома из графы «**PE Rangers**».

```
[root@localhost admin]# pvmove --alloc anywhere /dev/nvme0n1p3:119720-121689
  /dev/nvme0n1p3: Moved: 0,46%
  /dev/nvme0n1p3: Moved: 100,00%
[root@localhost admin]#
```

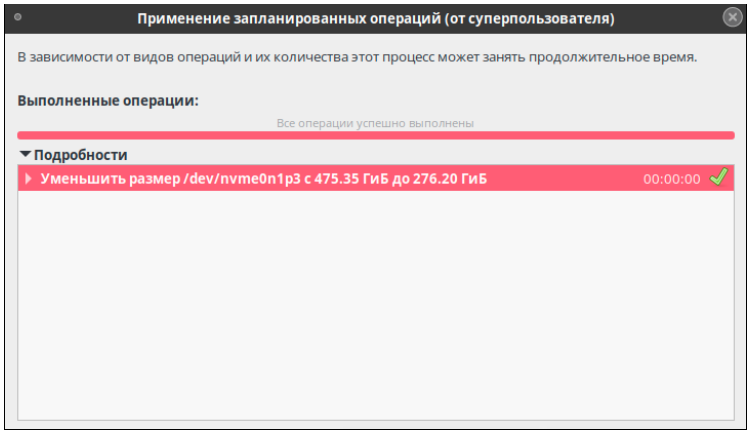
Далее проверяем, что свободные экстенты находятся в конце разделов.

```
pvs -v --segments /dev/nvme0n1p3
```

где вместо «**/dev/nvme0n1p3**» надо указать свой каталог с физическим устройством.

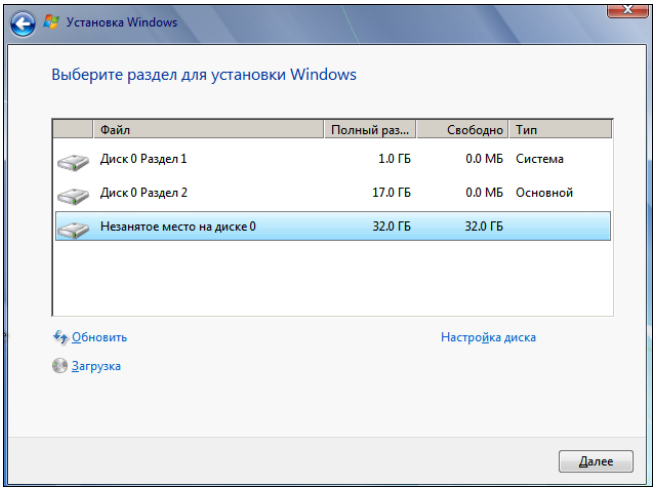
```
[root@localhost admin]# pvs -v --segment /dev/nvme0n1p3
  PV             VG       Fmt  Attr PSize   PFree    Start SSize LV   Start Type   PE Ranges
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g     0 17920 root     0 linear /dev/nvme0n1p3:0-17919
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 17920 50816 home     0 linear /dev/nvme0n1p3:17920-68735
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 68736  1970 swap     0 linear /dev/nvme0n1p3:68736-70705
  /dev/nvme0n1p3 ro_redos lvm2 a--  475,35g <199,16g 70706 50984          0 free
[root@localhost admin]#
```

После этого в **Gparted** появляется возможность изменить размер раздела.



Восстановление загрузчика GRUB

На неразмеченное пространство теперь можно установить операционную систему *Windows*.



После того как *Windows* будет установлена, она заменит загрузчик *GRUB* своим загрузчиком, и в результате пропадет возможность запустить РЕД ОС.

Чтобы исправить данную ситуацию, необходимо по нашей инструкции выполнить восстановление загрузчика **GRUB**.

BleachBit - утилита для выполнения очистки диска

Установка
Настройка BleachBit
Работа с BleachBit
Удаление файлов с многократной перезаписью
Работа с утилитой в терминальном режиме

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** bleachbit-4.4.0-1

BleachBit – это утилита для выполнения очистки диска, выгрузки файлов, которые могут пригодиться, в облако, а также удаления файлов без возможности их восстановления.

К основным возможностям **BleachBit** относятся:

- удаление временных файлов для большинства известных приложений;
- очистка оперативной памяти, виртуальной памяти, раздела подкачки;
- многократная перезапись удалённых файлов для исключения возможности их восстановления;
- удаление неиспользуемых и ошибочных (ссылающихся на несуществующие программы) ярлыков;
- возможность использования консольного интерфейса, позволяющего автоматизировать процесс;
- очистка кеша систем управления пакетами;
- наличие собственного языка разметки **CleanerML**, который можно использовать для написания скриптов очистки накопителя;
- возможность удаления неиспользуемых языков интерфейса;
- удаление cookies, кеша и паролей всех распространённых браузеров и перечня скачанных файлов;
- оптимизация баз данных большого перечня программ, от **aMule** и **Beagle** до **Miro** и **Pidgin**.

Вы можете подробнее ознакомиться с работой утилиты BleachBit, просмотрев наши обучающие видео:

- на **RuTube** — Полное и необратимое удаление данных с дисков;
- в **Яндекс.Дзен** — Полное и необратимое удаление данных с дисков;
- в **VK Видео** — Полное и необратимое удаление данных с дисков.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **bleachbit** необходимо перейти в сеанс пользователя **root**:

```
su -
```

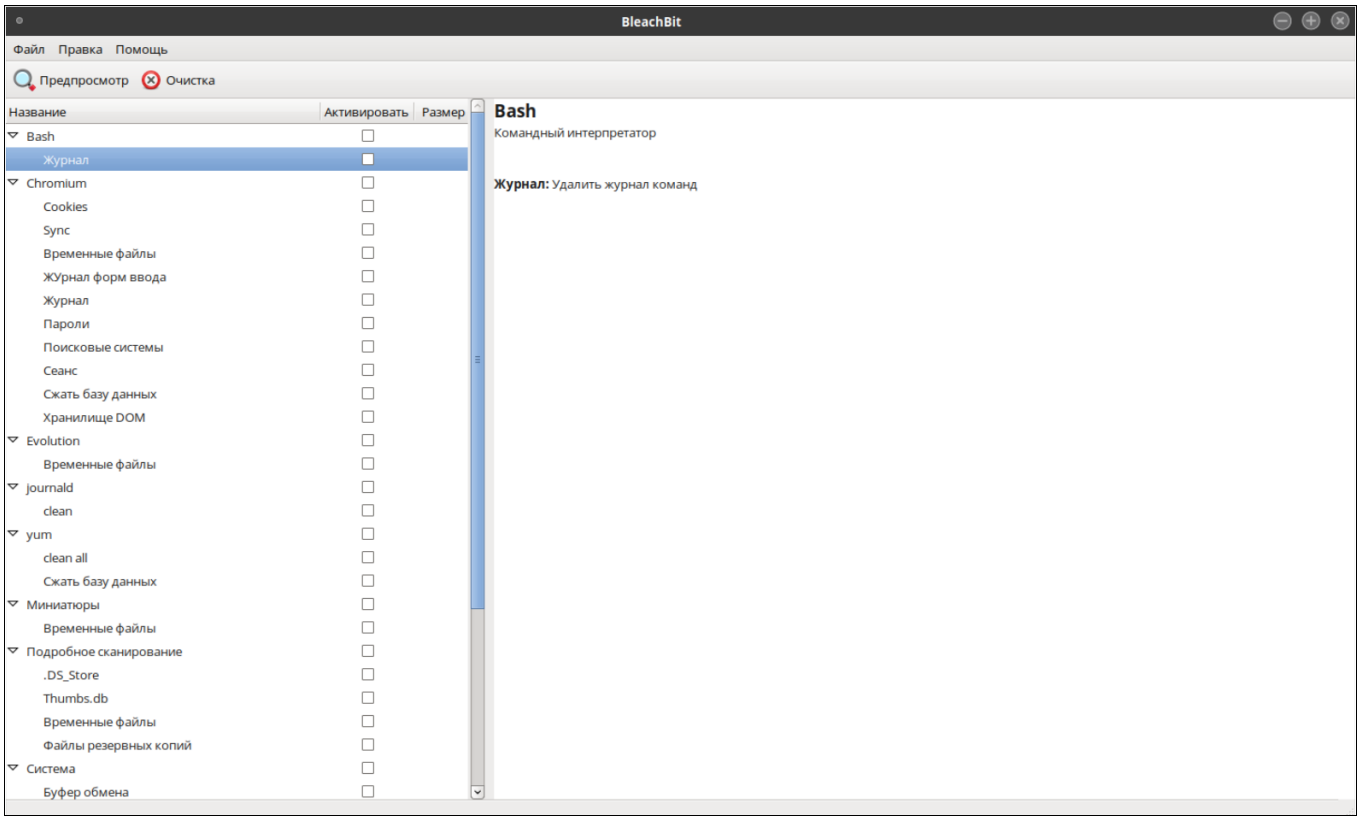
и выполнить следующую команду:

```
dnf install bleachbit
```

Запустить утилиту можно как через «**Главное меню**» - «**Системные**» - «**BleachBit**», так и через терминал командой:

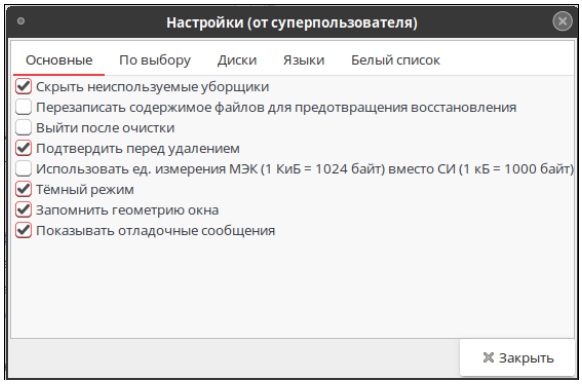
```
bleachbit
```

Структурно интерфейс программы выглядит одинаково для всех версий ОС: слева располагается раздел со списком элементов, которые можно очистить/удалить, справа – раздел, с описанием выполняемых действий.



Настройка BleachBit

При первом запуске программы будет выведено окно с настройками, которое можно открыть через меню «**Правка**» - «**Настройки**».



Окно настроек состоит из пяти вкладок:

Во вкладке «**Общие**» можно настроить:

1. Включение/Отключение автоматической проверки наличия обновлений через Интернет (Рекомендуется отключить);
2. Скрыть/Отобразить неиспользуемые параметры;
3. Перезаписать содержимое файлов для предотвращения восстановления;
4. Запускать или нет программу вместе с компьютером;
5. Выйти после очистки;
6. Подтвердить перед удалением;
7. Использовать единицы измерения МЭК вместо СИ;

Во вкладке «**По выбору**» существует возможность выполнить тонкую настройку каталогов и файлов, которые нужно сканировать на предмет удаления.

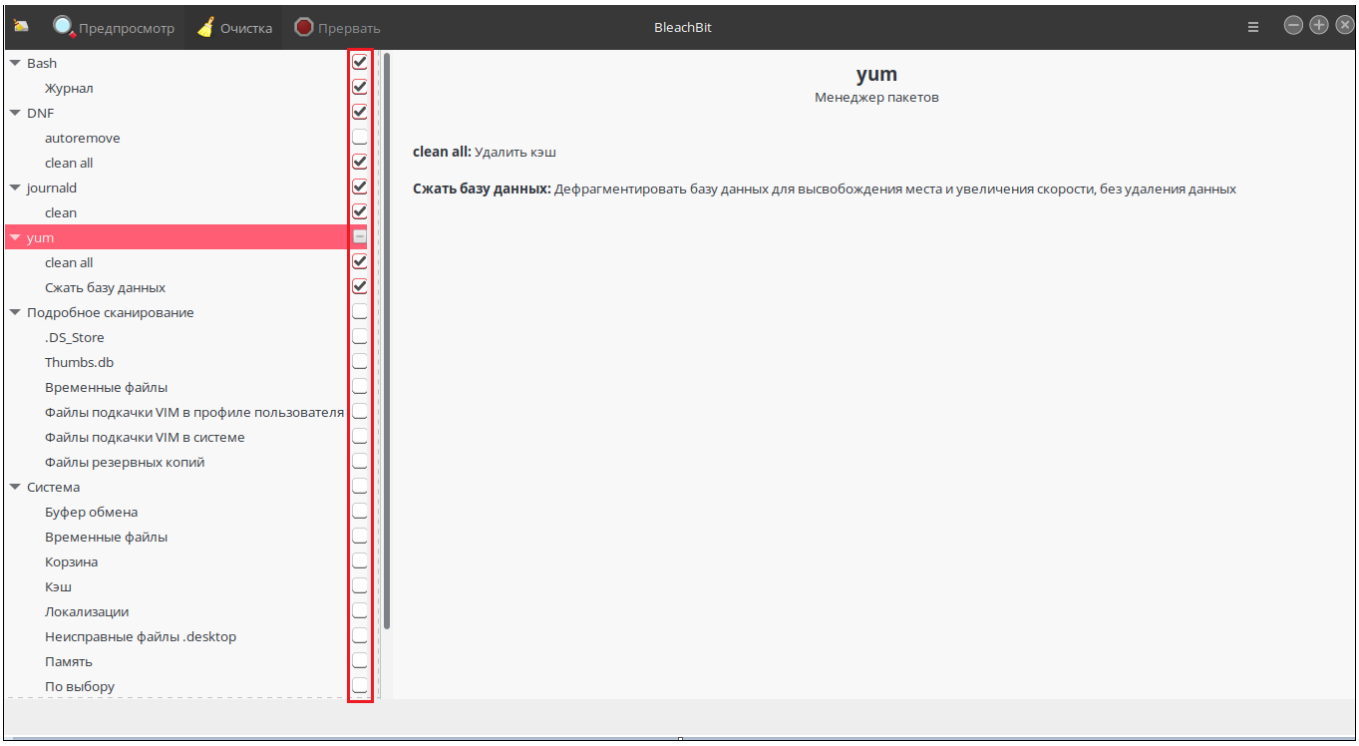
Вкладка «**Диски**» предназначена для настройки режима перезаписи освобождённого дискового пространства, чтобы удалённые файлы и даже их фрагменты нельзя было восстановить.

На вкладке «**Языки**» отображается полный список установленных в системе языков. Можно выбрать те, которые не будут использоваться и которые необходимо удалить.

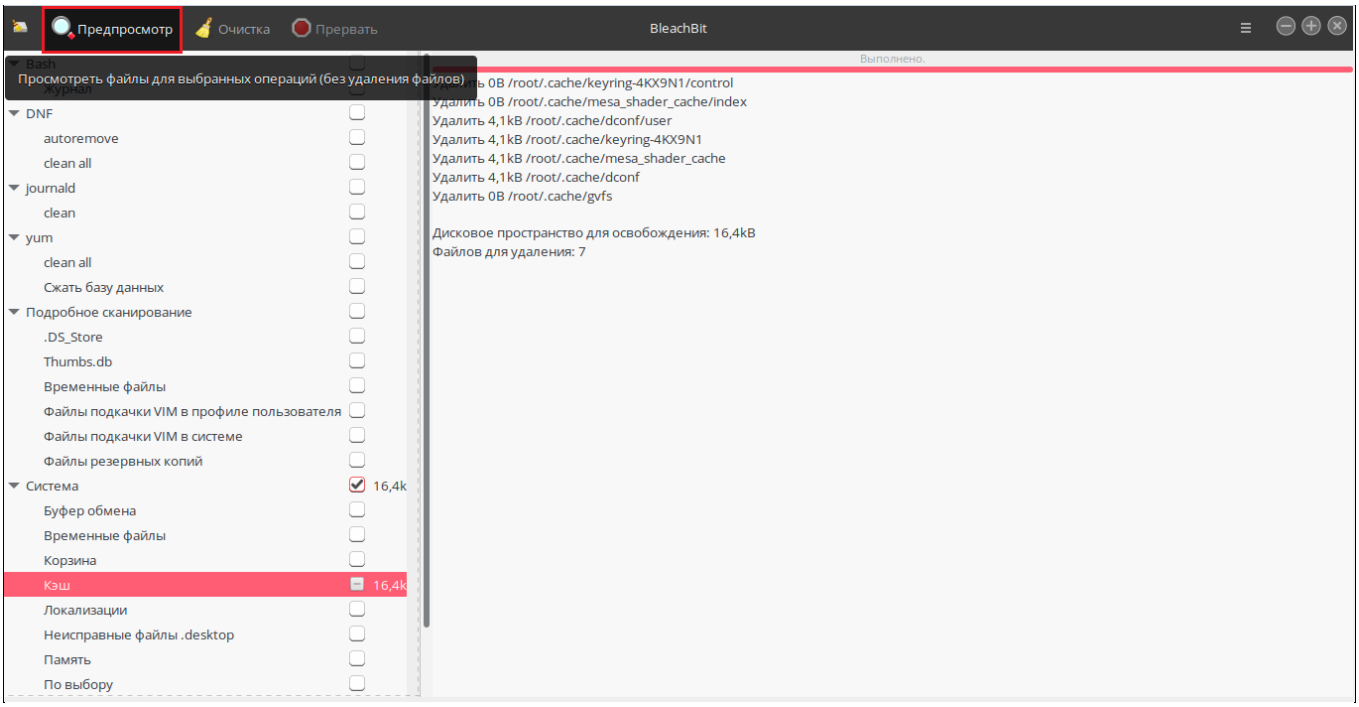
Во вкладке «**Белый список**» указываются каталоги диска, которые утилита будет игнорировать.

Работа с BleachBit

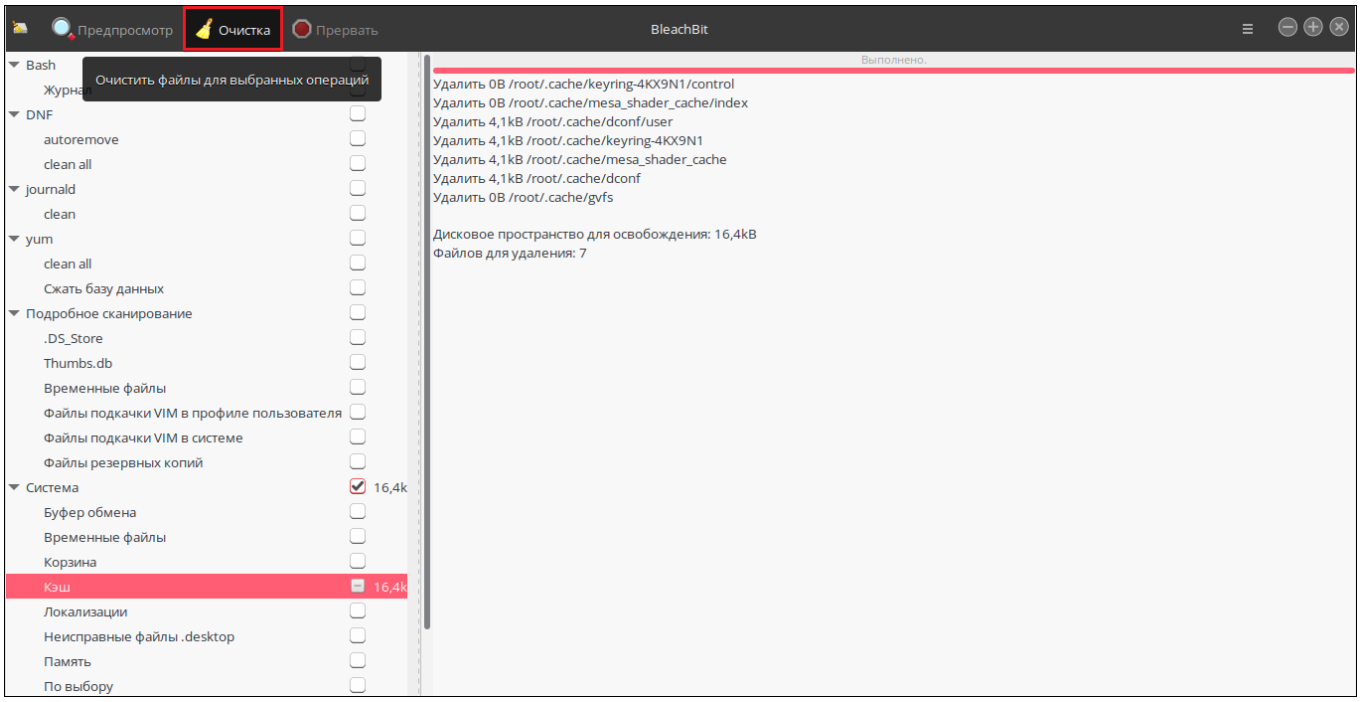
Для освобождения места на диске предназначена левая панель утилиты, где перечислены все категории, скрипты и файлы, обнаруженные во время сканирования диска. Этот перечень зависит не столько от конкретных установленных программ, сколько от вида дистрибутива Linux. Вы можете исключать из списка как целые категории, так и отдельные типы файлов.

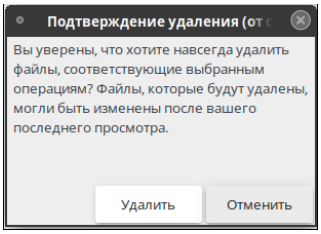


По умолчанию некоторые элементы списка будут помечены флагами, некоторые – нет. Выделите необходимые пункты и нажмите кнопку «**Предпросмотр**» в верхнем меню, чтобы просмотреть все файлы, которые будут очищены, и какой объём дискового пространства будет освобождён.



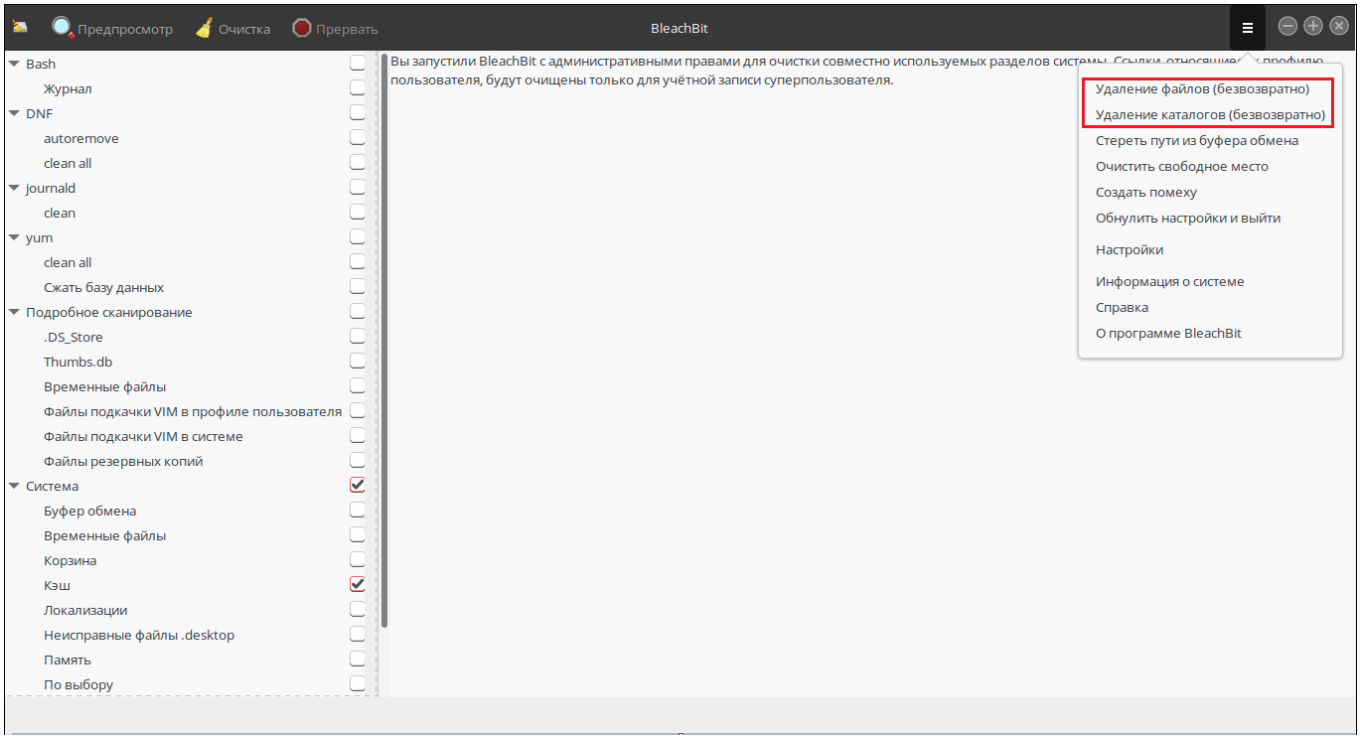
Для запуска работы утилиты требуется нажать на кнопку «**Очистка**» и подтвердить свой выбор.





Удаление файлов с многократной перезаписью

Для удаления файлов в меню **BleachBit** есть соответствующие пункты. При их выборе откроется проводник для выбора файла/каталога для удаления. При использовании такого способа восстановить их уже не получится.



Работа с утилитой в терминальном режиме

В **BleachBit** реализована работа в терминальном режиме и возможностью добавления команды в **crontab**.

Просмотреть доступные ключи можно с помощью команды:

```
bleachbit -h
```

Просмотреть доступные скрипты очистки можно командой:

```
bleachbit -l
```

Аналогом оценки количества освобождаемого места служит команда:

```
bleachbit --preview --preset
```

Ключ **--preset** устанавливает выбранные в графическом интерфейсе наборы опций. Вместо него можно поставить один из сценариев, полученных с помощью ключа **-l**.

Для запуска очистки используется ключ **--clean**:

```
bleachbit --clean --preset
```

Для удаления файлов с многократной перезаписью без возможности восстановления следует использовать ключ **--overwrite**.

DisLocker - инструмент для чтения зашифрованных разделов

Установка
Использование dislocker в режиме FILE
Использование dislocker в режиме FUSE
Проверка работоспособности dislocker

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dislocker-0.7.3-1

DisLocker – инструмент для чтения разделов, зашифрованных в *BitLocker*. Dislocker используется для чтения томов, зашифрованных в системных версиях Windows от Vista до 10, и зашифрованных разделов *BitLocker-To-Go*.

BitLocker-To-Go предназначен для работы со съемными носителями.

BitLocker — технология, которая используется для шифрования разделов диска в операционной системе Windows.

При расшифровке раздела требуется указать каталог, куда будет сохранен **dislocker-file**. Этот файл является виртуальным разделом NTFS, поэтому его можно смонтировать как любой раздел, а затем читать или записывать в него файлы. Запись в виртуальный файл NTFS приведет к изменению содержимого базового раздела BitLocker.

Установка

Для установки *dislocker* перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install dislocker
```

После установки *dislocker* для работы с зашифрованными разделами доступны следующие утилиты:

- **dislocker-bek** – для анализа файла .bek и печати информации о нем;
- **dislocker-metadata** – для печати информации о томе, зашифрованном BitLocker;
- **dislocker-find** – скрипт на Ruby, который находит зашифрованный раздел BitLocker среди подключенных дисков;
- **dislocker-file** – для расшифровки раздела BitLocker в файл, отформатированный как раздел NTFS, который можно смонтировать;
- **dislocker-fuse** – параметр, который используется при вызове команды *dislocker*, он динамически расшифровывает раздел BitLocker с помощью FUSE.

Dislocker поддерживает работу в двух режимах:

- FILE;
- FUSE.

Использование dislocker в режиме FILE

В режиме **FILE** весь раздел *BitLocker* расшифровывается в файл. Этот процесс может занять значительное время, зависящее от размера раздела.

Для *расшифровывания* раздела необходимо выполнить команду вида:

```
dislocker -V /dev/sda3 -u -- /media/<имя_файла>
```

где:

- /dev/sda3 — зашифрованный раздел Bitlocker;
- /media — директория, в которую будет записан файл;

- <имя_файла> — произвольное имя расшифрованного файла.

Далее будет запрошен пароль, с помощью которого был зашифрован раздел. Необходимо его ввести и нажать **Enter**.

Для *монтирования* расшифрованного раздела необходимо создать отдельную директорию:

```
mkdir /media/<директория>
```

И выполнить команду монтирования:

```
mount -o loop /media/<имя_файла> /media/<директория>
```

где:

- /media/<имя_файла> — путь к расшифрованному файлу;
- /media/<директория> — директория монтирования.

Использование dislocker в режиме FUSE

Второй режим предполагает использование **FUSE** — драйвера файловой системы, который позволяет пользователям без особых привилегий создавать их собственные файловые системы. В режиме **FUSE** расшифровывание происходит «на лету». Расшифровывается только тот блок, к которому в данный момент обращается система.

Для использования *dislocker* в режиме **FUSE** необходимо установить дополнительный пакет **fuse-dislocker** командой (с правами пользователя root):

```
dnf install fuse-dislocker
```

Для *расшифровывания* необходимо создать отдельную директорию:

```
mkdir /media/dislocker
```

Для запуска процесса *расшифровывания* раздела используется команда:

```
dislocker -V /dev/sda3 -u -- /media/dislocker
```

где:

- /dev/sda3 — зашифрованный раздел Bitlocker;
- /media/dislocker — директория для расшифровывания раздела. Указывать **имя файла**, как в режиме FILE, **не нужно**!

Далее будет запрошен пароль, с помощью которого был зашифрован раздел. Необходимо его ввести и нажать **Enter**.

Для *монтирования* расшифрованного раздела необходимо создать отдельную директорию:

```
mkdir /media/mount
```

И выполнить команду монтирования:

```
mount -o loop /media/dislocker/dislocker-file /media/mount
```

где:

- /media/dislocker/dislocker-file — файл, который был расшифрован;
- /media/mount — директория монтирования.

Проверка работоспособности dislocker

Проверим работоспособность *dislocker* на примере предоставления доступа к зашифрованным Bitlocker-разделам Windows 7.

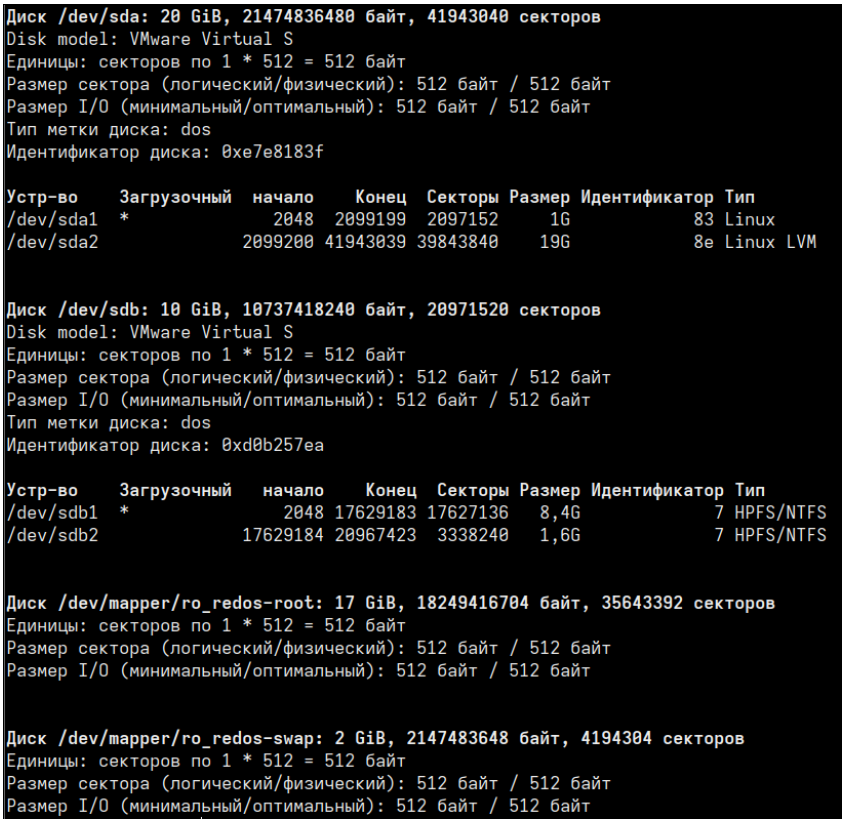
Создайте две директории, прежде чем начать расшифровку.

Первая директория (*/media/bitlocker*) – для вашего «зашифрованного раздела», который представляет собой «файл» виртуального раздела NTFS, созданный программой *dislocker* до того, как вы смонтируете его для доступа.

Вторая директория (*/media/mount*) – для монтирования расшифрованного раздела.

```
mkdir -p /media/bitlocker
mkdir -p /media/mount
```

Находим зашифрованный раздел с помощью `fdisk -l`. Определить его можно, например, по размеру:



```
Диск /dev/sda: 20 GiB, 21474836480 байт, 41943040 секторов
Disk model: VMware Virtual S
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xe7e8183f

Устр-во    Загрузочный  начало    Конец  Секторы Размер Идентификатор Тип
/dev/sda1  *              2048  2099199  2097152     1G            83 Linux
/dev/sda2              2099200 41943039 39843840    19G            8e Linux LVM


Диск /dev/sdb: 10 GiB, 10737418240 байт, 20971520 секторов
Disk model: VMware Virtual S
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0xd0b257ea

Устр-во    Загрузочный   начало    Конец  Секторы Размер Идентификатор Тип
/dev/sdb1  *               2048 17629183 17627136   8,4G             7 HPFS/NTFS
/dev/sdb2             17629184 20967423  3338240   1,6G             7 HPFS/NTFS


Диск /dev/mapper/ro_redos-root: 17 GiB, 18249416704 байт, 35643392 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт


Диск /dev/mapper/ro_redos-swap: 2 GiB, 2147483648 байт, 4194304 секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
```

В данном примере зашифрован раздел **/dev/sdb2**.

После этого запускаем расшифровку раздела на запись и чтение:

```
dislocker -V /dev/sdb2 -u <пароль> -- /media/bitlocker
```

где:

- /dev/sdb2 — имя вашего зашифрованного раздела;
- <пароль> — пароль BitLocker, который был использован для шифрования диска.

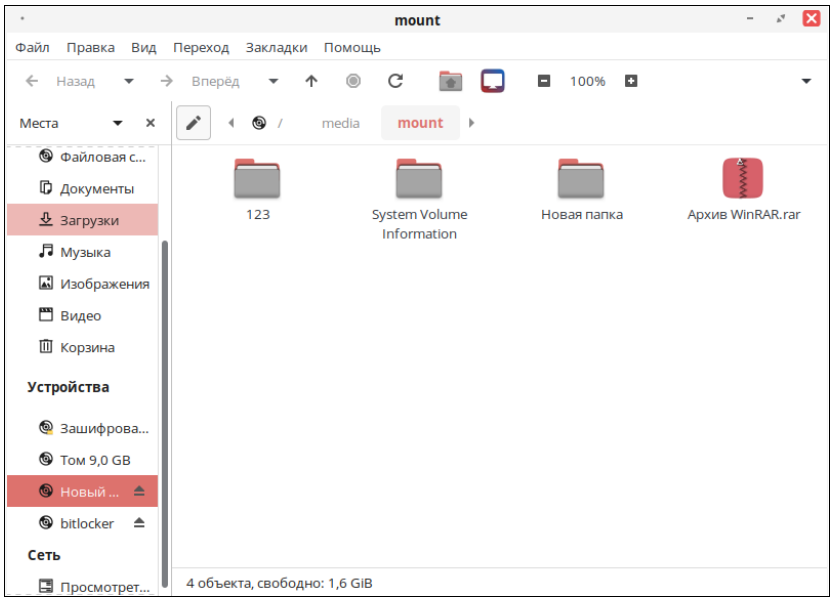
Если том необходимо расшифровать только для чтения, используйте ключ **-r**:

```
dislocker -r -V /dev/sdb2 -u <пароль> -- /media/bitlocker
```

Далее необходимо примонтировать раздел, чтобы можно было получить доступ к файлам. Для этого используется следующая команда:

```
mount -o loop /media/bitlocker/dislocker-file /media/mount
```

Сразу после монтирования будет открыт файловый менеджер с содержимым расшифрованного раздела.



Все изменения будут сохранены после отключения зашифрованного диска.

TRIM

Проверка поддержки TRIM
Включение TRIM с помощью флагов монтирования
Применение TRIM по раписанию cron
Включение TRIM с помощью tune2fs
Настройка TRIM по расписанию с помощью таймера systemd

Когда в операционной системе происходит операция удаления данных с SSD-диска, то физически они не удаляются, а лишь помечаются как «неиспользуемые» в файловой системе. Операция записи новых данных на место «неиспользуемых» предварительно сопровождается уже реальной функцией стирания ранее «удаленных» данных, что приводит к снижению производительности диска.

Чтобы решить эту проблему используется **TRIM** — команда интерфейса ATA, которая сообщает твердотельному диску, какие «неиспользуемые» блоки данных можно физически удалить с твердотельного устройства (**SSD**).

Целью очистки памяти является периодическая оптимизация накопителя, чтобы он работал эффективно и сохранял производительность на протяжении всего срока службы. Часто эта операция может выполняться в фоновом режиме или в ручном.

Примечание.

На твердотельном накопителе с **включенным TRIM**, если вы удалите файл и впоследствии очистите корзину, восстановить удаленные данные уже будет невозможно. В отличие от механических жестких дисков, которые удерживают данные магнитным полем, все, что требуется NAND для полного удаления данных — это команда (**trim**).

Проверка поддержки TRIM

Проверить поддержку **TRIM** можно двумя способами.

Способ №1 — с помощью команды **lsblk**:

```
lsblk -D NAME   DISC-ALN DISC-GRAN DISC-MAX DISC-ZERO
sda        0    512B     2G       0
├─sda1     0    512B     2G       0
├─sda2     0    512B     2G       0
├─sda3     0    512B     2G       0
├─sda4     0    512B     2G       0
└─sda5     0    512B     2G       0
sdb        0      0B     0B       0
```

Если значения столбцов **DISC-GRAN** (отбросить гранулярность) и **DISC-MAX** (отбросить максимальное количество байтов) имеют ненулевые значения, это указывает на поддержку **TRIM**.

Способ №2 — с помощью команды **hdparm**:

```
hdparm -I /dev/sda | grep TRIM

* Data Set Management TRIM supported (limit 8 blocks)
```

Если в выводе присутствует запись TRIM supported, значит диск поддерживает **TRIM**.

Включение операции TRIM в РЕД ОС

Включение TRIM с помощью флагов монтирования

В данном случае операция **TRIM** будет выполняться каждый раз при монтировании раздела диска. Параметр discard в **/etc/fstab** в строке монтирования раздела активирует **TRIM**:

```
/dev/sda1 / ext4 defaults,noatime,discard 0 1
/dev/sda2 /home ext4 defaults,noatime,discard 0 2
```

Примечание.

- не используйте флаг **discard**, если вы периодически выполняете команду **fstrim**;
- если вы используете флаг **discard** для корневого раздела с файловой системой **ext3**, раздел будет смонтирован в режиме только-чтение (**read_only**).

ВАЖНО!

Перед внесением изменений убедитесь, что ваш SSD поддерживает TRIM, иначе вы можете **потерять данные**!

Применение TRIM по расписанию cron

Данный метод не работает для файловых систем VFAT.

Для использования **fstrim** раздел диска должен быть смонтирован и указан точкой монтирования. Для периодического выполнения команды можно задействовать планировщик заданий **cron**, в котором в качестве задания используется команда:

```
fstrim -v /
```

Данная команда будет применена к корневому разделу. Для указания, например, домашнего раздела используйте команду:

```
fstrim -v /home
```

Подробную информацию по работе с планировщиком **cron** см. в нашей статье «Crontab».

После настройки планировщика заданий уберите опцию discard из **/etc/fstab**, если ранее вы ее добавляли.

Приоритетным способом является использование discard. Если с ним возникли проблемы или он не подошел, используйте **fstrim**.

Включение TRIM с помощью tune2fs

В файловой системе **EXT4** флаг discard можно установить с помощью утилиты **tune2fs**. При данном способе флаг discard устанавливается в суперблоке ФС, как опция монтирования по умолчанию.

```
tune2fs -o discard /dev/sdXY
```

где:

- XY — раздел на диске.

Если на диске используется LVM, то команда для корневого раздела может выглядеть примерно следующим образом:

```
tune2fs -o discard /dev/mapper/ro_redos-root
```

Чтобы определить, какой именно раздел применять в команде **tune2fs**, воспользуйтесь командами «**lsblk**», «**df**» или **blkid**, которые выведут на экран имена разделов диска.

Убедиться в активации **trim** можно также с помощью **tune2fs**, при этом команде передается ключ **-l**:

```
tune2fs -l /dev/mapper/vg1-lvroot | grep options

Default mount options:    user_xattr acl discard
```

Использование параметров монтирования по умолчанию вместо редактирования в **/etc/fstab** актуально для внешних дисков, поскольку

для разделов диска признак применения TRIM будет установлен по умолчанию и не придется на каждом компьютере редактировать **/etc/fstab** для добавления опции `discard`.

> **Примечание.**
>
> При использовании данного способа опция `discard` **НЕ будет** показана командой **mount**.

Настройка TRIM по расписанию с помощью таймера systemd

В РЕД ОС присутствует *systemd*-таймер, который предназначен для использования TRIM по расписанию. Активировать таймер можно командой:

```
systemctl enable --now fstrim.timer
```

По умолчанию задание **fstrim** будет выполняться еженедельно, это задание запускает связанную службу **fstrim** по расписанию. Время выполнения **fstrim** по умолчанию настроено на каждый понедельник с точностью запуска в 1 час, т.е. с 00:00 по 01:00.

Для установки собственного времени выполнения задания измените время в таймере **/usr/lib/systemd/system/fstrim.timer**, за это отвечает опция **OnCalendar**.

Пример изменения таймера на каждый понедельник в 12:00.

```
nano /usr/lib/systemd/system/fstrim.timer
```

```
[Unit]
Description=Discard unused blocks once a week
Documentation=man:fstrim
ConditionVirtualization=!container
ConditionPathExists=!/etc/initrd-release

[Timer]
OnCalendar=Mon *-*-* 12:00:00
Persistent=true

[Install]
WantedBy=timers.target
```

Перезапустите таймер для применения внесенных изменений:

```
systemctl daemon-reload
systemctl restart fstrim.timer
```

В статусе таймера в поле **Trigger** будет указано запланированное время выполнения задания:

```
systemctl status fstrim.timer
● fstrim.timer - Discard unused blocks once a week
     Loaded: loaded (/usr/lib/systemd/system/fstrim.timer; enabled; preset: enabled)
     Active: active (waiting) since Fri 2024-10-11 11:35:08 MSK; 10s ago
    Trigger: Mon 2024-10-14 12:09:21 MSK; 3 days left    Triggers: ● fstrim.service
       Docs: man:fstrim
```

Планировщик ввода/вывода

Планировщик ввода-вывода (I/O) — это компонент ядра, который определяет, в каком порядке операции блочного ввода-вывода передаются на устройства хранения (HDD/SSD/NVME). Основной целью планировщика ввода-вывода является оптимизация обработки запросов к диску для повышения производительности и пропускной способности ввода-вывода. Связано это с тем, что когда в системе запущено большое количество процессов, выполняющих запросы ввода-вывода к различным частям хранилища, то эти процессы могут создавать множественные операции ввода-вывода, в результате чего образуется очередь запросов.

В РЕД ОС используются следующие планировщики:

- **mq-deadline** — реализация планировщика deadline с использованием blk-mq. Этот планировщик подходит для большинства случаев, но особенно для тех, в которых операции записи в основном асинхронны. Планировщик mq-deadline сортирует запросы ввода-вывода в очереди на чтение или запись, а затем планирует их выполнение в возрастающем порядке адресации логических блоков (LBA).
- **kyber** — планировщик, основанный на методах активного управления очередями, используемых для сетевой маршрутизации. Реализация основана на "токенах", которые служат механизмом ограничения запросов. Используется две очереди запросов — на запись и на чтение. kyber отдает приоритет запросам на чтение перед запросами на запись. Реализация алгоритма относительно проста и считается эффективной для NVME, SSD или других устройств с низкой задержкой.
- **bfq** (Budget Fair Queuing) — основан на алгоритме от CFQ, но содержит улучшения. В конфигурации по умолчанию он больше нацелен на обеспечение минимальной задержки, а не на достижение максимальной пропускной способности. Этот планировщик обладает относительно высокими расходами на операцию, поэтому он не идеален для устройств с медленными процессорами или устройствами ввода-вывода с высокой пропускной способностью.
- **none** — планировщик ввода-вывода без операций с несколькими очередями. Не переупорядочивает запросы и имеет минимальные расходы. Идеально подходит для быстрых устройств произвольного ввода-вывода, таких как SSD или NVME.

Устаревшими планировщиками ввода-вывода считаются: **noop**, **CFQ**, **Deedline**.

В зависимости от задачи, которую выполняет используемая система, рассмотрены следующие рекомендации по выбору планировщиков.

Вариант использования	Планировщик дисков
Традиционный жесткий диск с интерфейсом SCSI	Рекомендуется **mq-deadline** или **bfq**
Высокопроизводительный SSD или система с привязкой к ЦП с быстрым хранилищем	Рекомендуется **none**, особенно при запуске корпоративных приложений. В качестве альтернативы можно использовать **kyber**
Настольные системы или интерактивные задачи	Рекомендуется **bfq**
Виртуальные гостевые системы	Рекомендуется **mq-deadline**. С адаптером главной шины (HBA), поддерживающим работу с несколькими очередями, рекомендуется использовать **noop**/**none**

РЕД ОС по умолчанию использует планировщик **BFQ**. Для проверки можно вывести содержимое файла **/sys/block/sdX/queue/scheduler**:

```
cat /sys/block/sdX/queue/scheduler
mq-deadline kyber [bfq] none
```

где **X** — буква физического накопителя.

Используемый планировщик выделен квадратными скобками.

Изменение планировщика ввода-вывода

Изменить используемый планировщик без необходимости перезагрузки можно командой:

```
echo none > /sys/block/sdX/queue/scheduler
```

где **X** — буква физического накопителя.

Данная настройка действует только **до** первой **перезагрузки** ОС.

Для постоянной настройки необходимо создать правило **UDEV**.

Создайте файл **/etc/udev/rules.d/60-schedulerset.rules** и запишите в него следующие строки:

- для SSD-дисков:

```
ACTION=="add|change", KERNEL=="sd[a-z]", ATTR{queue/rotational}=="0", ATTR{queue/scheduler}="none"
```

- для NMVE-дисков:

```
ACTION=="add|change", KERNEL=="nvme[0-9]n[0-9]", ATTR{queue/rotational}=="0", ATTR{queue/scheduler}="none"
```

- для HDD-дисков:

```
ACTION=="add|change", KERNEL=="sd[a-z]*", ATTR{queue/rotational}=="1", ATTR{queue/scheduler}="none"
```

Здесь:

- **ATTR{queue/scheduler}** – параметр определяет имя планировщика;
- **ATTR{queue/rotational}=0** – признак планировщика для типов дисков: **SSD** и **NVME**;
- **ATTR{queue/rotational}=1** – признак планировщика для типа дисков: **HDD** (магнитные диски).

Изменения вступят в силу после перезагрузки ОС. Чтобы проверить назначенное правило, выполните команду:

```
cat /sys/block/sdX/queue/scheduler
```

Например:

```
cat /sys/block/sdb/queue/scheduler
[none] mq-deadline kyber bfq
```

Уменьшение числа операций чтения/записи

Опция монтирования barrier=0
Опция монтирования noatime
Перенос /tmp в tmpfs
Отключение swap

Опция монтирования barrier=0

ВАЖНО!

Не рекомендуется отключать барьеры для дисков, которые будут использоваться без источника бесперебойного питания, так как это может привести к повреждению файловой системы и потере данных.

Файловая система **ext4**, которая используется по умолчанию в РЕД ОС, является журналируемой ФС, в такой файловой системе включены барьеры записи.

Включенные барьеры гарантируют, что метаданные файловой системы будут правильно записаны и упорядочены на диске. При этом данная функция сказывается на производительности, особенно для приложений, которые интенсивно используют **fsync** или создают и удаляют большое количество небольших файлов. Для дисков с питанием от батареи отключение барьеров может безопасно повысить скорость операции записи на разделы **ext4**.

Пример отключения барьеров записи через опцию **barrier=0** в строке монтирования **/etc/fstab**:

```
/dev/mapper/ro_redos-root / ext4 defaults,noatime,discard,barrier=0 0 1
```

Опция монтирования noatime

ВАЖНО!

Это может привести к снижению уровня безопасности системы!

Операционная система отслеживает и обновляет информацию о временнЫх отметках доступа к файлам и каталогам, из-за этого происходит незначительное снижение производительности ввода-вывода. Опция **noatime** в строке монтирования (**/etc/fstab**) раздела диска отключит запись о времени последнего доступа к файлу.

Пример монтирования разделов диска с опцией noatime в фале **/etc/fstab**:

```
/dev/mapper/ro_redos-root / ext4 defaults,noatime,discard 0 1
```

Изменения вступят в силу после перезагрузки ПК.

Перенос /tmp в tmpfs

Каталог **/tmp** используется ОС, а также прикладными программами для хранения временных данных. Чтобы сократить число операций записи и чтения на диск в каталог **/tmp**, существует способ размещения **/tmp** в оперативной памяти. Для этой цели применяется временная файловая система под названием **tmpfs**. Чтобы разместить **/tmp** в **tmpfs**, необходимо открыть файл **/etc/fstab** и добавить в него следующую запись:

```
tmpfs /tmp tmpfs defaults,rw,nodev,nofail,noatime,nosuid,size=4G 0 0
```

где **size** – максимально доступный размер оперативной памяти, которая выделяется только по факту заполнения **/tmp**. Обычно значение параметра **size** определяют как половину от всей оперативной памяти. Т.е. для оперативной памяти размером 8G указывается значение 4G.

Изменения вступят в силу после перезагрузки ПК.

Отключение swap

Многие пользователи отключают **swap** при наличии достаточно большого объема ОЗУ (не менее 8 ГБ) или переносят его на отдельный диск с целью продлить срок службы SSD-диска. Ведь, как известно, когда заканчивается оперативная память, операционная система использует пространство подкачки для записи и чтения данных, а это приводит к дополнительным циклам перезаписи, которые изнашивают ячейки памяти SSD.

Здесь стоит заметить, что отключение **swap** может негативно сказаться на работе системы, если свободная оперативная память все-таки закончится. Поскольку при нехватке памяти **OOM Killer** (защитный механизм ядра Linux) принудительно «убивает» наиболее подходящие по приоритету процессы.

Кроме того, если планируется использовать "спящий режим", для его работы требуется наличие **swap**. В то же время сам процесс перехода в спящий режим приводит к большему износу SSD, чем просто загрузка ОС.

Также стоит отметить, что современные SSD-диски имеют намного большие циклы перезаписи данных, чем диски, выпущенные несколько лет назад (в ранние периоды их массового распространения), и эффект от отключения swap может быть совсем незначительным.

Если swap все же будет решено отключить, сделать это можно следующим образом:

1. Откройте файл **/etc/fstab**.

```
sudo nano /etc/fstab
```

2. Найдите строку, которая подключает **swap**, и закомментируйте ее, поставив в начале строки символ **#**.

Пример:

```
#UUID=<ваш-UUID> none      swap   defaults    0 0
```

3. Сохраните внесенные изменения в файле.

Для применения изменений выполните перезагрузку компьютера.

Работа с bluetooth

Установка
Утилита blueman
Настройка автоматического подключения bluetooth-устройств при загрузке
Поддержка bluetooth-кодеков высокого качества в PulseAudio
Настройка интернет-соединения через bluetooth

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: blueberry-1.4.4-3, blueman-1:2.4.3-2, pulseaudio-15.0-1, NetworkManager-bluetooth-1.44.0-1

Bluetooth — это технология беспроводной передачи данных. Она обеспечивает обмен информацией между различными устройствами, соединяя их посредством одной универсальной радиолинии с малым радиусом действия.

Установка

Для работы с **Bluetooth** в РЕД ОС уже предустановлена утилита **blueberry**. Если по какой-либо причине утилита в системе отсутствует, её можно установить вручную.

Для установки необходимо перейти в сеанс пользователя **root**:

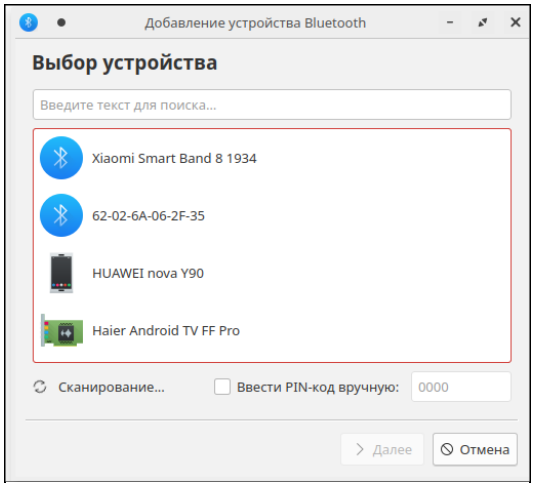
```
su -
```

и выполнить команду:

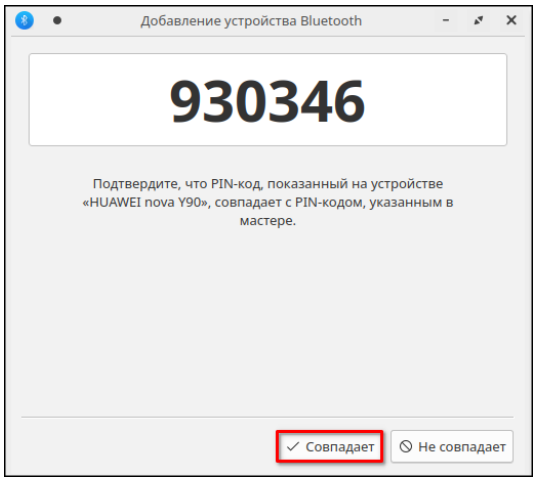
```
dnf install blueberry bluez bluez-cups bluez-hid2hci bluez-mesh bluez-tools
```

Подключение и настройка Bluetooth-устройств доступны из «**Главного меню**» — «**Параметры**» — «**Bluetooth**».

Перед запуском Bluetooth-менеджера необходимо предварительно включить используемый Bluetooth-адаптер (аппаратно). Ниже приведен пример подключения по Bluetooth к смартфону. Убедитесь, что устройства доступны для поиска и включите сопряжение, нажав на устройство.



При сопряжении подтвердите PIN-коды на обоих устройствах.



Утилита blueman

Blueman (*Bluetooth Manager*) — это менеджер Bluetooth, обладающий более удобным интерфейсом по сравнению с Bluetooth-менеджером пакета **blueberry**.

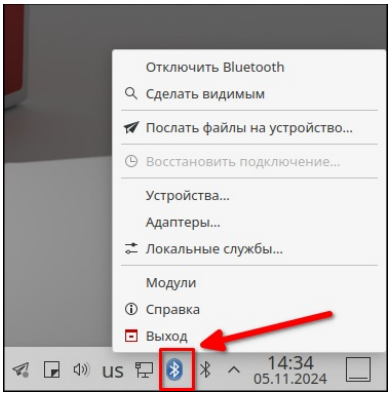
Blueman предоставляет более широкий функционал настройки соединения и управления устройствами.

Для установки **Blueman** выполните команду:

```
dnf install blueman
```

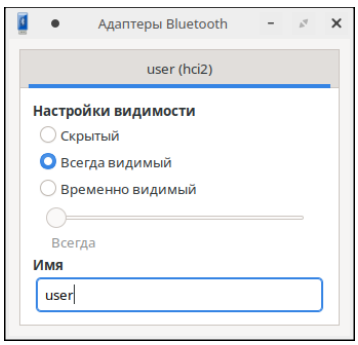
Работа с **Blueman** доступна из «**Главного меню**» — «**Настройки**» — «**Менеджер Bluetooth**» или из «**Главного меню**» — «**Параметры**» — «**Адаптеры Bluetooth**».

Также инструменты утилиты можно открыть через панель задач.

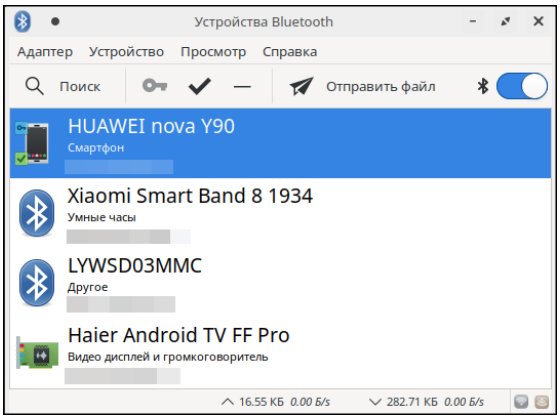


Утилита «**Адаптеры Bluetooth**» позволяет:

- задать имя, под которым будет отображаться устройство;
- задать настройки видимости адаптера для внешних устройств.



В утилите «**Менеджер Bluetooth**» отображается список найденных и подключенных устройств.

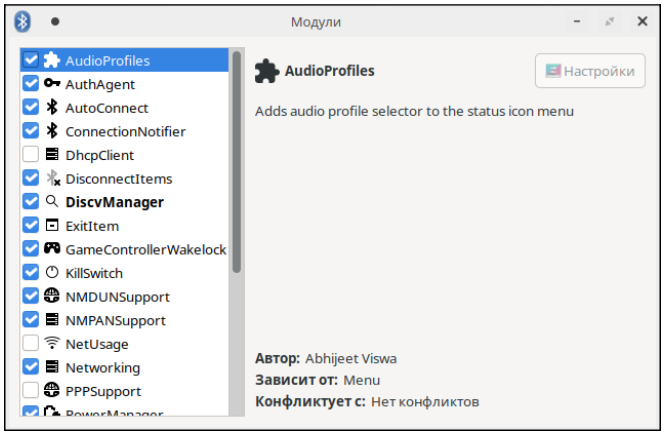


Вкладка «**Адаптер**» содержит компоненты для настройки Bluetooth-адаптера, включающие возможность запуска утилиты «**Адаптеры Bluetooth**» и поиска внешних устройств.

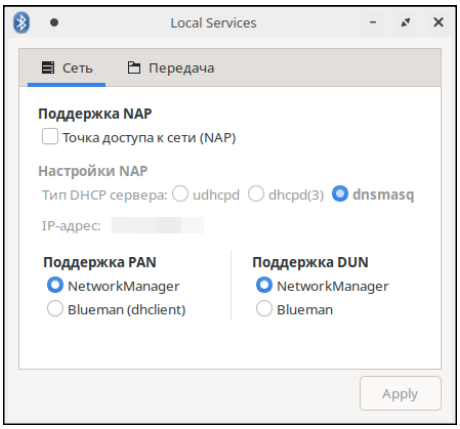
Вкладка «**Устройство**» содержит инструменты для взаимодействия с подключаемым устройством.

Вкладка «**Просмотр**» содержит инструменты для настройки интерфейса утилиты.

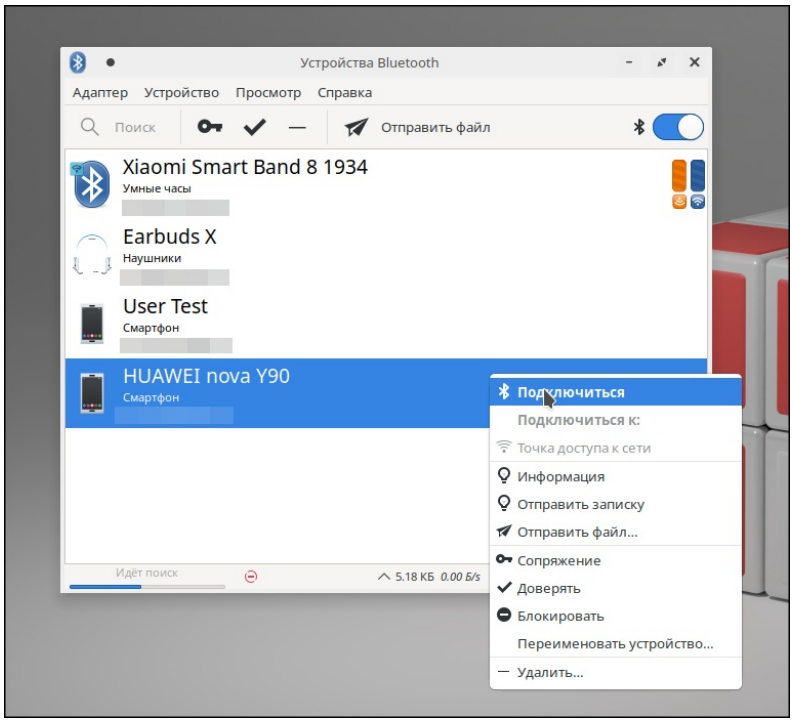
В этой же вкладке пункт «**Модули**» содержит компоненты, которые можно использовать для более функциональной работы **Blueman**, включая показ значков уведомлений, поддержку различных протоколов, отслеживание сетевого трафика и некоторые другие.



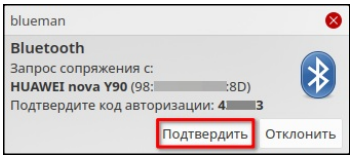
Пункт «**Локальные службы**» содержит инструменты для настройки сетей и передачи данных.



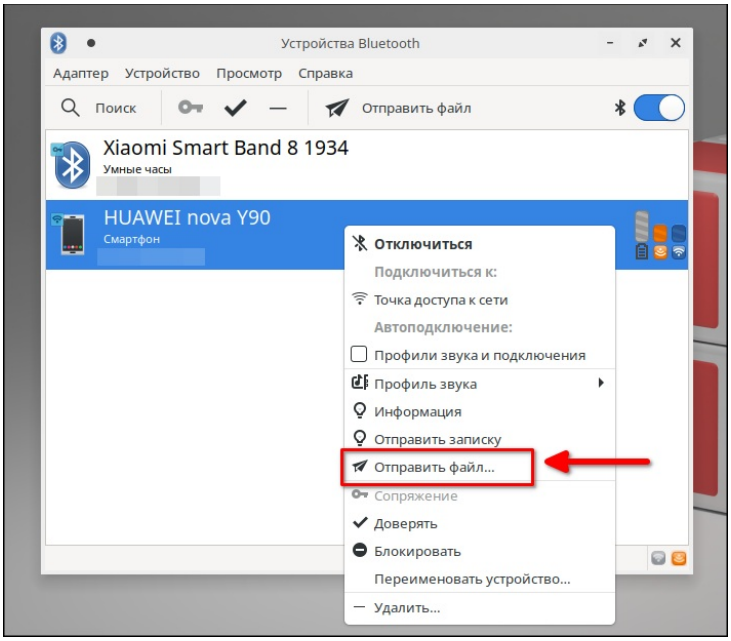
Перед подключением убедитесь, что ваши устройства доступны для поиска. Выберите необходимое устройство и выполните подключение.



При сопряжении подтвердите запрос авторизации.



Для отправки файла на другое устройство выберите необходимое устройство и осуществите передачу данных.



Настройка автоматического подключения bluetooth-устройств при загрузке

Включите автоматический запуск systemd-юнита:

```
systemctl enable bluetooth.service --now
```

Отредактируйте файл конфигурации **/etc/bluetooth/main.conf**:

```
nano /etc/bluetooth/main.conf
```

Активируйте автоматическое подключение доверенных устройств при запуске:

```
[Policy]
 AutoEnable=true
```

Любым способом определите MAC-адрес устройства (отображается как при поиске, так и в списке подключённых), затем войдите в консоль настройки Bluetooth-сервера:

```
bluetoothctl
```

Получите список сопряжённых устройств:

```
devices Paired
```

Если нужное оборудование с MAC-адресом AA:BB:CC:DD:EE:FF уже числится в списке, удалите его:

```
remove AA:BB:CC:DD:EE:FF
```

Запустите процесс поиска новых устройств, убедитесь, что устройство обнаруживается, затем отключите процесс сканирования:

```
scan on
scan off
```

Назначьте устройство доверенным:

```
trust AA:BB:CC:DD:EE:FF
```

Произведите сопряжение и выполните подключение:

```
pair AA:BB:CC:DD:EE:FF
connect AA:BB:CC:DD:EE:FF
```

После этого при следующей загрузке системы или при выходе из режима сна выбранное устройство будет подключено автоматически (при условии, если на компьютере включен bluetooth).

Для выхода из консоли настройки Bluetooth-сервера воспользуйтесь командой:

```
exit
```

Поддержка bluetooth-кодеков высокого качества в PulseAudio

В РЕД ОС по умолчанию установлены пакеты для работы с **PulseAudio**, что позволяет работать с кодеками высокого качества с помощью профиля **A2DP**.

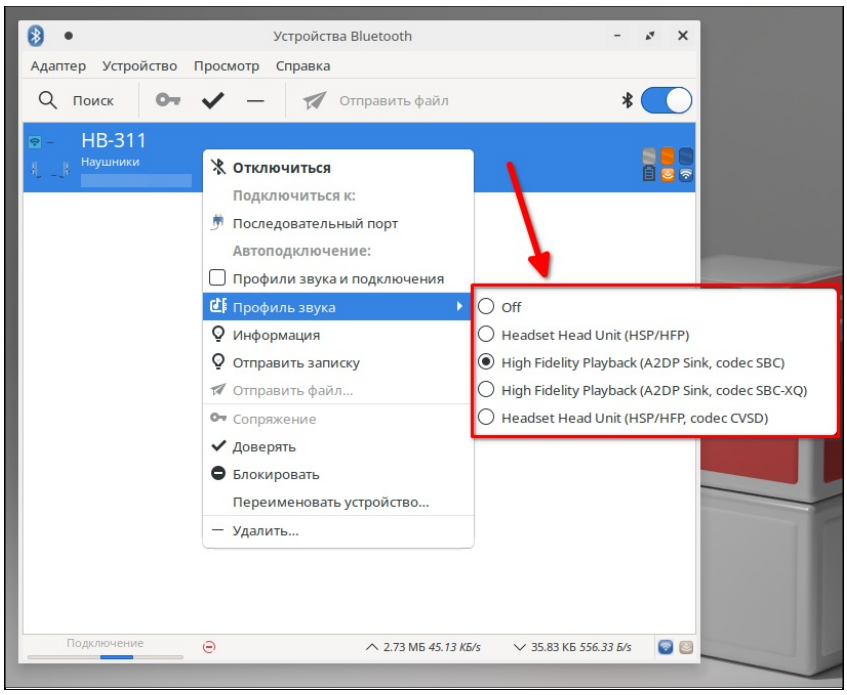
Если по какой-либо причине пакеты в системе отсутствуют, их можно установить вручную командой:

```
dnf install pulseaudio pulseaudio-module-bluetooth alsa-plugins-pulseaudio pulseaudio-libs pulseaudio-libs-glib2 pulseaudio-module-x11 pulseaudio-utils wine-pulseaudio
```

Примечание.

Выбранный кодек должен поддерживаться наушниками аппаратно.

Выбрать кодек можно в окне настройки устройства в менеджере **Blueman**.



Настройка интернет-соединения через bluetooth

Интернет через Bluetooth — это один из вариантов использования мобильного телефона для выхода в Интернет с компьютера.

Этот метод может стать альтернативой, если у компьютера нет Wi-Fi или USB-кабеля для подключения телефона по проводу. В данном случае телефон будет выступать в роли модема.

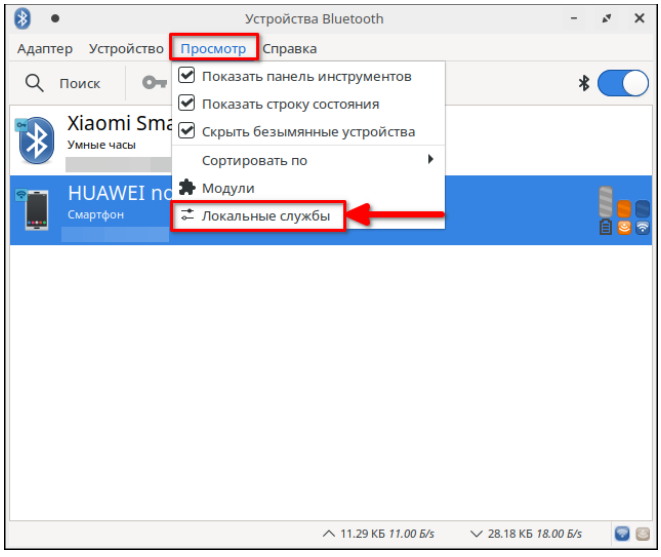
Для реализации данной функции необходим пакет blueman, а также некоторые дополнительные пакеты, которые можно установить командой:

```
dnf install blueman NetworkManager-bluetooth dhcp-client dhcp-server dhcp-devel dnsmasq dnsmasq-utils
```

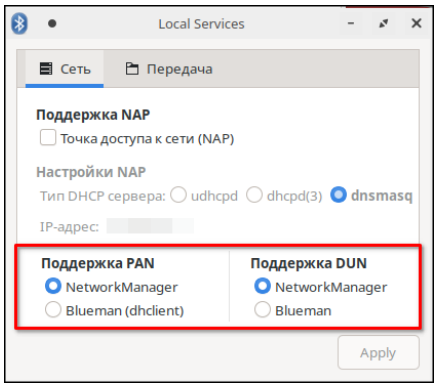
Выполните перезагрузку сетевых подключений:

```
systemctl restart NetworkManager
```

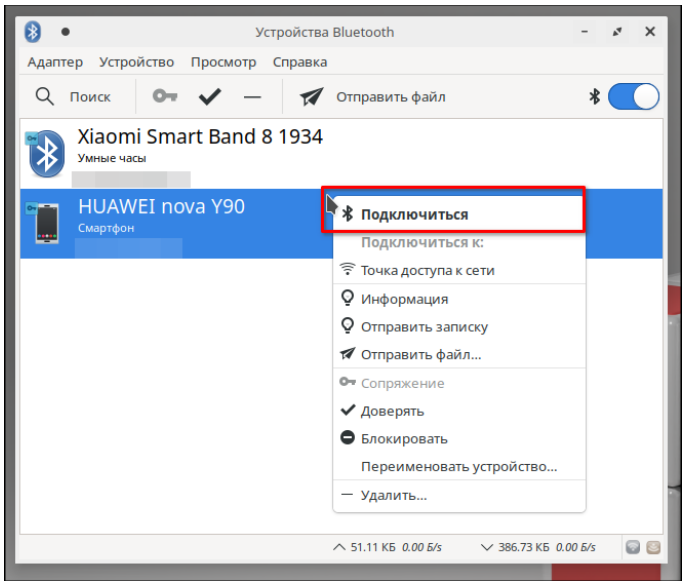
В **Менеджере Bluetooth** выберите пункт меню «**Просмотр**» — «**Локальные службы**».



В открывшемся окне установите значение **NetworkManager** для пунктов «**Поддержка PAN**» и «**Поддержка DUN**».

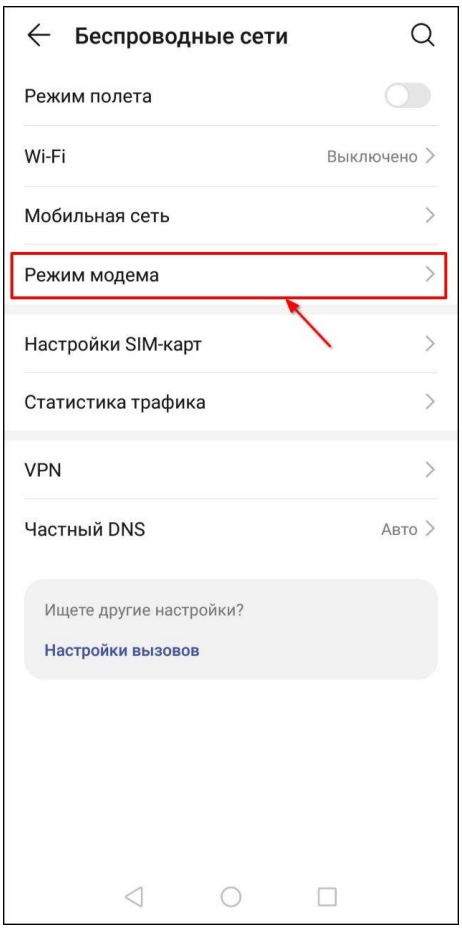


1. Для сопряжения телефона и компьютера выберите необходимое устройство и в контекстном меню нажмите «Подключиться».



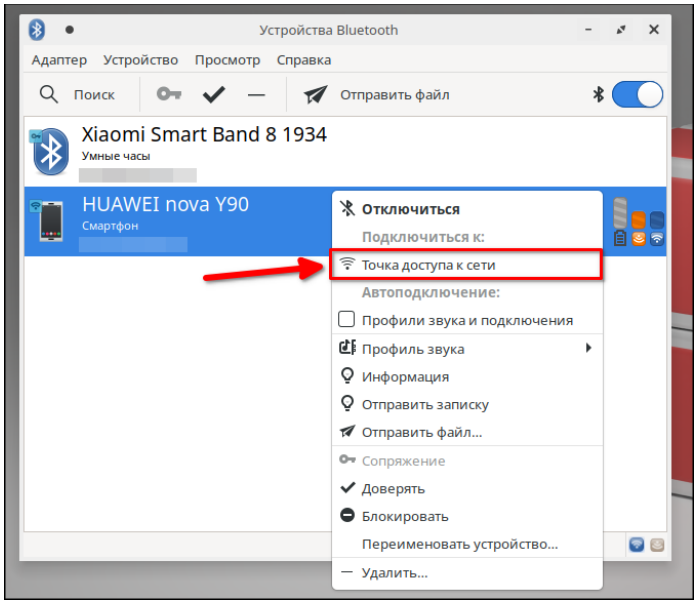
2. Для включения Bluetooth-модема на телефоне необходимо перейти в настройки телефона. Затем выбрать пункт «**Беспроводные сети**», перейти в раздел «**Режим модема**» и активировать Bluetooth-модем.

Стоит обратить внимание, что внешний вид и наименование пунктов меню может отличаться в зависимости от конкретной модели телефона.

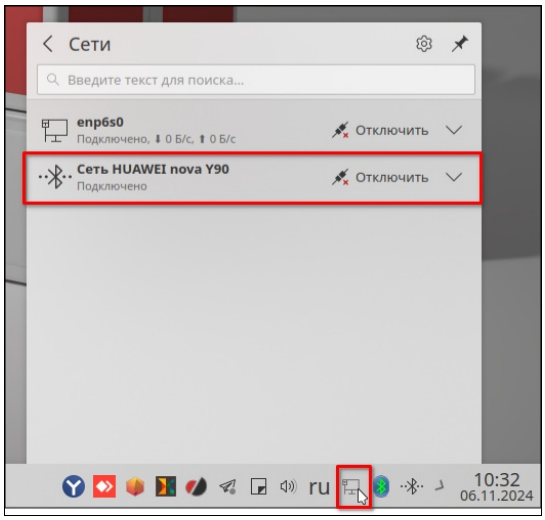




3. Для подключения ПК к Bluetooth-модему телефона выберите сопряжённое устройство и выполните подключение к точке доступа.



В настройках сетевых подключений вашего компьютера после этого должна появиться возможность подключаться к смартфону и управлять установленным соединением.



Однако стоит отметить, что при таком способе Интернет-соединения скорость передачи данных будет невысокой. На стандарте **Bluetooth 5** скорость будет **~1.6 Мбит/с**. Причём оба устройства (и телефон, и компьютер) должны поддерживать этот протокол.

На стандарте **Bluetooth 4** скорость передачи данных будет **не более 1 Мбит/с**.

Отключение CD-ROM

Запрет монтирования CD-ROM

Чтобы отключить **CD-ROM**, вам необходимо создать файл **/etc/modprobe.d/usb-storage.conf** и отредактировать его с помощью текстового редактора.

```
sudo nano /etc/modprobe.d/usb-storage.conf
```

Введите следующие строки в файл:

```
install usb-storage /bin/true
```

Вышеупомянутый файл ***.conf** отражает фальшивую установку **CD-ROM**. Сохраните файл с помощью `Ctrl + O`, затем нажмите `Enter`, и выйдите из редактора с помощью `Ctrl + X`.

Запретите чтение/запись/выполнение всем пользователям, кроме **root**, на каталог, в который монтируются **CD-ROM**.

```
sudo chmod -R 700 /run/media
```

Для вступления изменений в силу перезагрузите компьютер.

Возврат возможности подключения

Для того чтобы вернуть возможность монтирования, выполните следующие команды

```
sudo rm -f /etc/modprobe.d/usb-storage.conf
sudo chmod -R 755 /run/media
```

Перезагрузите компьютер.

Ограничение доступа к USB-накопителям

Примеры выбора устройств по определенным свойствам
Запрет автомонтирования с параметром UDISKS_IGNORE
Создание белого списка с параметром UDISKS_IGNORE
Запрет автомонтирования с параметром authorized
Создание белого списка с параметром authorized

Алгоритм создания белого списка USB-флеш-накопителей состоит из 2 этапов:

Вариант 1:

1. Запрет монтирования всех USB-флеш-накопителей
2. Разрешение монтирования некоторых устройств

Вариант 2:

1. Разрешение монтирования некоторых устройств
2. Запрет монтирования всех иных USB-флеш-накопителей

Вы можете подробнее ознакомиться с информацией по ограничению доступа к USB-накопителям, просмотрев наши обучающие видео:

- на **RuTube** — Ограничение доступа к USB-накопителям;
- в **Яндекс.Дзен** — Ограничение доступа к USB-накопителям;
- в **VK Видео** — Ограничение доступа к USB-накопителям.

На наших каналах вы также сможете найти много другой полезной информации.

Примеры выбора устройств по определенным свойствам

Для создания белого списка USB-флеш-накопителей необходимо знать атрибуты накопителя.

1) Определите ваш флеш-накопитель:

```
 ls -l /dev/sd*

brw-rw---- 1 root disk 8, 0 июн 30 12:59 /dev/sda
brw-rw---- 1 root disk 8, 1 июл 22 12:59 /dev/sda1
brw-rw---- 1 root disk 8, 2 июл 22 12:59 /dev/sda2
brw-rw---- 1 root disk 8, 3 июн 30 12:59 /dev/sda3
brw-rw---- 1 root disk 8, 16 июл 22 13:43/dev/sdb # нужная нам строка
brw-rw---- 1 root disk 8, 17 июн 30 13:43 /dev/sdb1
```

2) Проверьте атрибуты (символы после **sd*** должны вводиться в соответствии с вашим выводом команды `ls -l /dev/sd*`):

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром UDISKS_IGNORE

Для отключения автомонтирования USB-флеш-накопителей необходимо создать правило для **udev**.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
```

Флаг `ENV{UDISKS_IGNORE}` отвечает за игнорирование устройства:

- «0» – false;
- «1» - true.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром UDISKS_IGNORE

Выборка разрешения доступа по трем параметрам:

- серийному номеру устройства;
- модели;
- максимальному потребления тока.

Для их определения выполните поочередно команды:

```
udevadm info -a -p /sys/block/sdb | grep serial
udevadm info -a -p /sys/block/sdb | grep product
udevadm info -a -p /sys/block/sdb | grep bMaxPower
```

в выводе будет отображен серийный номер, модель и значение максимального потребления тока:

```
ATTRS{serial}=="04GS1F3LBIBDWU05"
 ATTRS{model}=="Silicon-Power8G "
 ATTRS{bMaxPower}=="200mA"
```

Запишите эти значения в файл правил в качестве разрешающих.

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ENV{ID_USB_DRIVER}=="usb-storage",ENV{UDISKS_IGNORE}="1"
 ATTRS{serial}=="04GS1F3LBIBDWU05",ENV{UDISKS_IGNORE}="0"
 ATTRS{product}=="DataTraveler 3.0",ENV{UDISKS_IGNORE}="0"
 ATTRS{bMaxPower}=="200mA",ENV{UDISKS_IGNORE}="0"
```

Здесь:

- **1** - заблокировать все usb-накопители;
- **0** - разрешить накопитель по определенным свойствам.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, находится в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Запрет автомонтирования с параметром authorized

Для отключения автомонтирования USB-флеш-накопителей необходимо будет создать правило для **udev** и исполняемый скрипт запрета монтирования USB-флеш-накопителей.

Создайте скрипт:

```
nano /usr/bin/remove_usb.sh
```

```
#!/bin/bash
var=$1
var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
echo 0 > '/sys/bus/usb/devices'$var2'authorized'
```

Измените права на скрипт:

```
chmod +x /usr/bin/remove_usb.sh
```

Параметр **authorized** отвечает за монтирование USB-флеш-накопителя в момент подключения к ПК.

Создайте файл **/etc/udev/rules.d/99-usb.rules**:

```
nano /etc/udev/rules.d/99-usb.rules
```

со следующим содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
```

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

После этого можно проверить и подключить USB-флеш-накопитель. В результате открыть его не удастся.

Создание белого списка с параметром authorized

Выборка по серийному номеру устройства:

```
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
```

Выборка по названию модели. Точное название смотрите в выводе команды:

```
 udevadm info -a -p /sys/block/sdb

ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
```

Для удобства, когда полный список параметров устройства известен, можно производить отбор по конкретному параметру:

```
udevadm info -a -p /sys/block/sdb | grep "ATTRS{serial}"
udevadm info -a -p /sys/block/sdb | grep "ATTRS{product}"
```

Конечный вариант файла **/etc/udev/rules.d/99-usb.rules**:

```
ACTION!="add", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTRS{product}=="DataTraveler 3.0", GOTO="dont_remove_usb"
ATTRS{serial}=="0DM97KDQ", GOTO="dont_remove_usb"
ENV{ID_USB_DRIVER}=="usb-storage", RUN+="/bin/sh -c '/usr/bin/remove_usb.sh $devpath'"
LABEL="dont_remove_usb"
```

Логика данного правила отлична от первого варианта. В первом варианте происходила блокировка сразу всех usb флеш-накопителей, а только потом осуществлялось добавление устройств в белый список. В данном (втором) варианте сначала происходит добавление устройств в белый список, а только потом блокирование устройств (добавление в черный список). Такое действие связано с тем, что параметр **authorized** появляется в момент монтирования и, если его значение установить в **0**, то для дальнейшей работы он становится недоступен. Соответственно, сначала требуется проверить, входит ли флеш-накопитель в белый список, и если входит, то разрешить его монтирование.

Для того чтобы новое правило вступило в силу, необходимо обновить правила **udev**:

```
udevadm control --reload-rules
```

Полный список атрибутов, по которым можно осуществить выборку, отображается в выводе команды:

```
udevadm info -a -p /sys/block/sdb
```

Настройка протоколирования событий подключения USB-накопителей

Создаем правила для **udev**:

```
nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды

```
#log mount/unmount
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo unmount $devnode serial=%E{ID_SERIAL} $(date)>>
/home/user/log.txt"
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

После выполнения данных действий будут фиксироваться все факты подключения/отключения usb-накопителей.

Настройка принадлежности USB-накопителей

В данной статье будет рассмотрен пример разграничения правил для разных пользователей.

Сначала необходимо создать udev-правило, содержащее разрешения на определенные usb-устройства, по выбранным пользователем параметрам.

```
nano /etc/udev/rules.d/80-alloweduserlist1.rules
```

```
ACTION!="add", GOTO="dont_remove_usb"
 ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
 ATTRS{product}=="USB DISK 2.0",GOTO="dont_remove_usb"
 ENV{DRIVER}=="usb-storage",RUN+="/bin/python3 /usr/local/bin/remove_usb.py $devpath"
 LABEL="dont_remove_usb"
 ENV{DRIVER}=="usb-storage", ENV{UDISKS_AUTO}="0"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="add", RUN+="/bin/systemctl start usb-mount-list1@%k.service"
 KERNEL=="sd[a-z][0-9]", SUBSYSTEMS=="usb", ACTION=="remove", RUN+="/bin/systemctl stop usb-mount-list1@%k.service"
```

Затем необходимо создать скрипт для запрета монтирования устройств со следующим содержимым:

```
nano /usr/local/bin/remove_usb.py
```

```
#!/usr/bin/python3
 import os
 import sys
 var = sys.argv[1].strip()
 var2 = os.popen(f"echo {var} | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//'").readlines()[0]
 os.system(f"echo 0 > '/sys/bus/usb/devices{var2.strip()}authorized'")
```

Далее создайте сервис, отвечающий за запуск скрипта, проверяющего список доступных пользователей для данного udev-правила.

```
nano /etc/systemd/system/usb-mount-list1@.service
```

```
[Unit]
 Description=Mount USB Drive on %i

 [Service]
 RemainAfterExit=true
 Type=oneshot
 ExecStart=/usr/bin/python3 /usr/local/bin/usb-mount.py add %i /etc/udev/rules.d/80-alloweduserlist1.rules
 ExecStop=/usr/bin/python3 /usr/local/bin/usb-mount.py remove %i /etc/udev/rules.d/80-alloweduserlist1.rule
```

Следующим этапом формируется список разрешенных пользователей.

Допустимые значения **umask**:

- 0 - rwx - полные права; rw - чтение/запись;
- 2 - r - чтение.

Создайте список разрешенных пользователей (в примере **user1** с правами на чтение) без проверки на группы:

```
mkdir /etc/udevlist
nano /etc/udevlist/userlist1.json
```

```
{"user1": 2}
```

Если необходимо указать несколько пользователей, список указывается в виде `{"user1": 2, "user2": 0, ...}`.

Затем создайте файл соответствия udev-правила со списком разрешенных пользователей:

```
nano /etc/udevlist/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/userlist1.json"}
```

Создайте список разрешенных групп:

```
mkdir /etc/udevlist/group/
nano /etc/udevlist/group/grouplist1.json
```

```
{}
```

Если в правиле необходимо использовать разграничение по группам, список указывается в виде `{"name_group1": 0, "name_group2": 2}`.

После этого создайте файл соответствия udev-правила со списком разрешенных групп:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/group/grouplist1.json"}
```

Создайте файл для других списков, если используются:

```
mkdir /etc/udevlist/otherlists/
nano /etc/udevlist/otherlists/otherlists1.json
```

с содержимым вида:

```
{"others": 7}
```

После этого создайте файл соответствия udev-правила с новым списком:

```
nano /etc/udevlist/group/listudev.json
```

со следующим содержимым:

```
{"/etc/udev/rules.d/80-alloweduserlist1.rules": "/etc/udevlist/otherlists/otherlists1.json"}
```

Затем загрузите скрипт проверки доступа пользователей и монтирования устройств, распакуйте архив и переместите файл скрипта в каталог **/usr/local/bin/**:

```
wget https://redos.red-soft.ru/upload/usb-mount.zip
unzip ./usb-mount.zip -d /usr/local/bin/
```

Для применения настроек перезапустите службы командой:

```
systemctl daemon-reload
```

Настройка учета USB-накопителей

Создаем правила для **udev**:

```
sudo nano /etc/udev/rules.d/99-usb.rules
```

Заносим в файл данные команды (в примере показан учет **USB** на основе серийного номера):

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add",RUN+="/bin/sh /mnt/logs.sh $devnode %E{ID_SERIAL}"
```

Создаем скрипт для ведения лог файла. Если указать путь **/root/log.txt**, то доступ к файлу лога будет только у пользователя **root**.

```
nano /mnt/logs.sh
```

```
path=$1
 serial=$2
 File="/root/log.txt"
 if ! grep -q "$serial" "$File";
 then
 echo $path $serial $(date)>> /root/log.txt
 fi
```

Последний этап – перезапуск правил **udev**:

```
sudo udevadm control --reload-rules
```

Ограничение доступа USB-устройств по defines class code

Существует большое количество устройств, имеющих разный *USB defines class code*. Для того чтобы разрешить подключение определенного класса устройств, потребуется применить следующий алгоритм:

1) Создать правило, в котором прописаны разрешенные устройства, а остальные блокируются:

```
nano /etc/udev/rules.d/99-usb-bInterfaceClass.rules
```

Содержимое правила на примере классов для **token**, **HID**, **audio** и **video** устройств:

```
# Allow all TOKEN devices
 ATTR{bInterfaceClass}=="0b",ACTION=="add",GOTO="usb_rules_end"
 # Allow all c
 ATTR{bInterfaceClass}=="03",ACTION=="add",GOTO="usb_rules_end"
 # Allow all AUDIO devices
 ATTR{bInterfaceClass}=="01",ACTION=="add",GOTO="usb_rules_end"
 # Allow all VIDEO devices
 ATTR{bInterfaceClass}=="0e",ACTION=="add",GOTO="usb_rules_end"
 SUBSYSTEM=="usb",ACTION=="add",RUN+="/bin/sh -c '/usr/bin/reject_usb_bInterfaceClass.sh $devpath'"
 LABEL="usb_rules_end"
```

2) Создать скрипт, изменяющий атрибут **authorized** для определенного устройства:

```
nano /usr/bin/reject_usb_bInterfaceClass.sh
```

Содержимое скрипта:

```
#!/bin/bash
 var=$1
 var2=$(echo $1 | sed 's/.*usb[[:digit:]]//' | sed 's/[a-z].*//'| sed 's/[0-9]-[0-9].//')
 var3=$(echo $var2 | grep '^/[0-9]-[0-9]$')
 var4=$(echo $var2 | grep '^/[0-9]-[0-9].[0-9]$')
 if [ -z "$var3" ] && [ -z "$var4" ]; then
 echo 0 > '/sys/bus/usb/devices'$var2'/authorized'
 fi
```

Сделайте скрипт исполняемым:

```
chmod +x /usr/bin/reject_usb_bInterfaceClass.sh
```

Перезапустите правила **udev**:

```
sudo udevadm control --reload-rules
```

HUB устройства

Есть устройства, которые системой определяются как **HUB**. В момент редактирования правил и перезагрузки **udev** на **HUB**-устройства, которые находятся в системном блоке/кейсе, влияние оказано не будет, так как они не переподключаются. Зато при перезагрузке ОС они заблокируются и в итоге все подключенные к ним устройства ниже по дереву тоже будут заблокированы. Для корректного редактирования устройств подключенных через **HUB** требуется в правилах разрешить:

```
DRIVER=="hub",ACTION=="add",GOTO="end_usb_rules"
```

либо:

```
ATTR{bInterfaceClass}=="09",ACTION=="add",GOTO="usb_rules_end"
```

Перезапустить правила:

```
udevadm control --reload-rules
```

Утилита по созданию правил для монтирования USB-накопителей

Установка
Полная блокировка всех usb
Назначение личной привязки к UDEV-правилу
Протоколирование событий usb-flash накопителей

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** usb_rules-2.1-1

Утилита **usb_rules** основана на работе с правилами **udev** и системными сервисами **systemd**.

Вы можете подробнее ознакомиться с работой утилиты **usb_rules**, просмотрев наши обучающие видео:

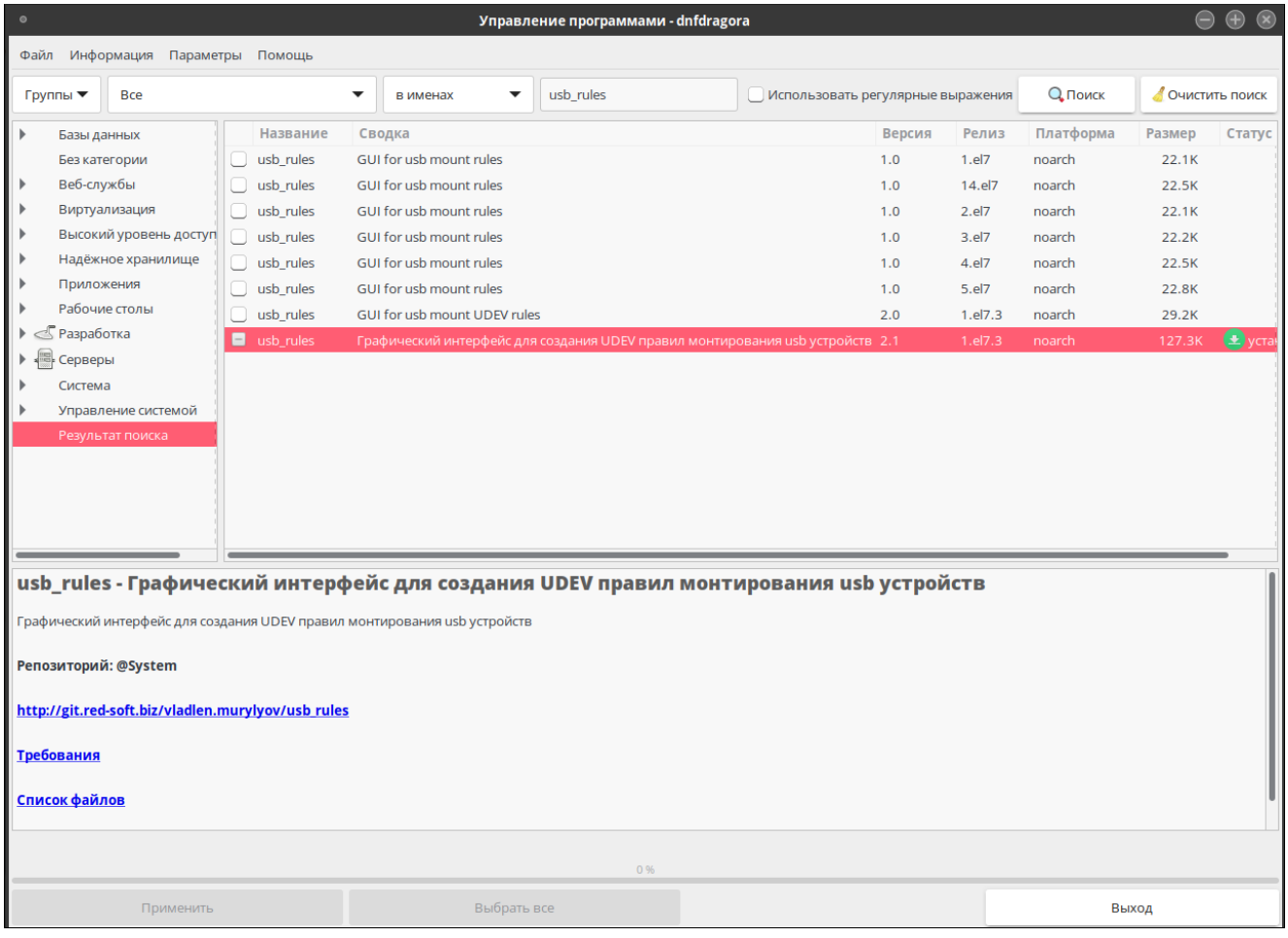
- на **RuTube** — Утилита по созданию правил для монтирования usb-flash накопителей ;
- в **Яндекс.Дзен** — Утилита по созданию правил для монтирования usb-flash накопителей ;
- в **VK Видео** — Утилита по созданию правил для монтирования usb-flash накопителей .

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установка утилиты доступна через пакетный менеджер *dnfdragora* («**Главное меню**» - «**Администрирование**» -«**Управление пакетами dnfdragora**»).

В поисковой строке пакетного менеджера введите название утилиты «**usb_rules**», нажмите «**Enter**» для поиска. Из списка результатов выберите последнюю версию утилиты и нажмите кнопку «**Применить**».



Будет выполнена установка пакета.

Также установка утилиты доступна из терминала. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

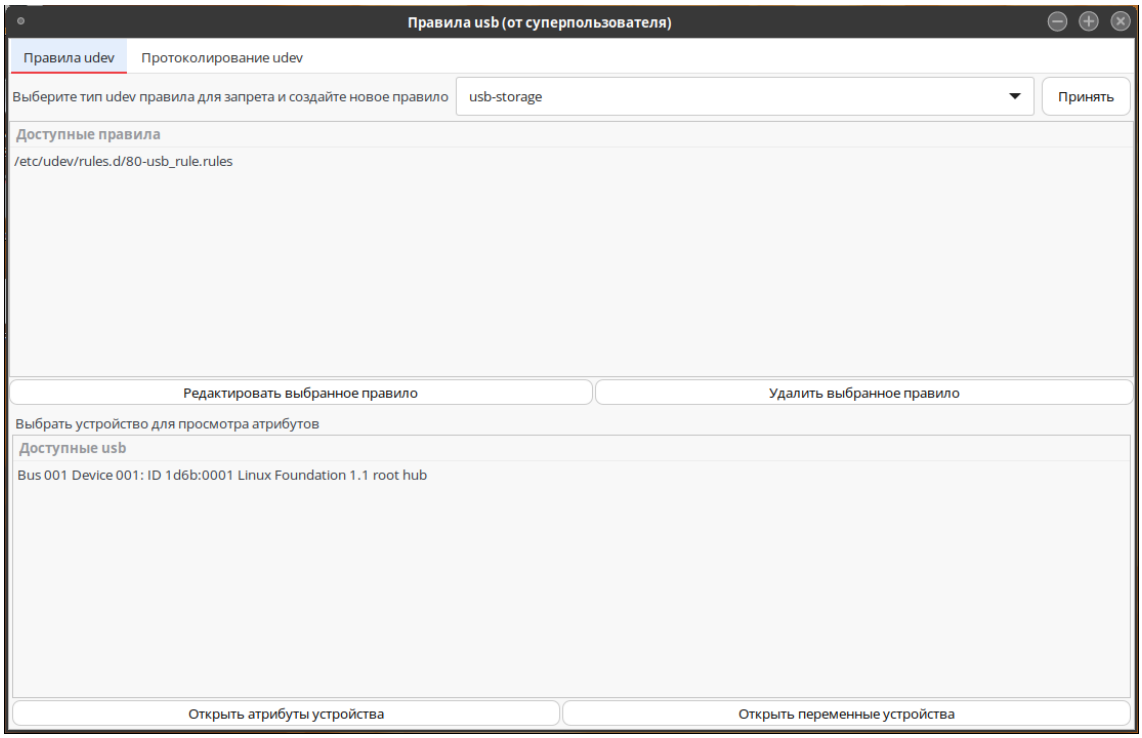
и выполните команду:

```
dnf install usb_rules
```

После установки запуск утилиты доступен с правами пользователя **root** из «**Главного меню**» - «**Параметры**» - «**Настройка ограничения монтирования**» или через терминал с помощью команды:

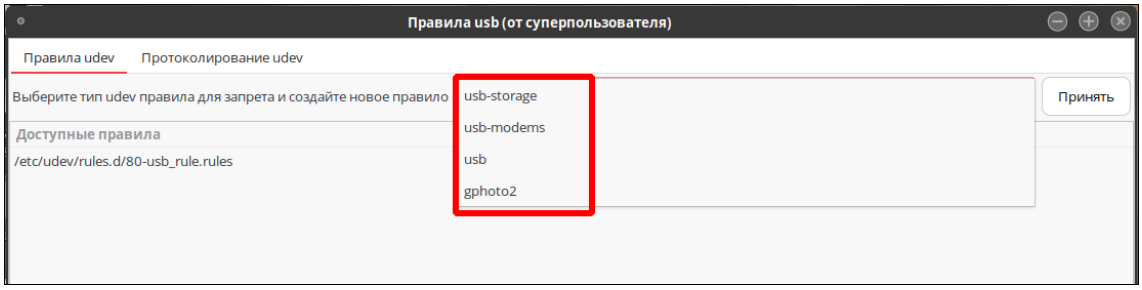
```
usb-rules
```

Стартовое окно утилиты позволяет пользователю ознакомиться с подключенными usb-устройствами и со списком уже созданных правил.



При формировании нового правила пользователю доступны 4 шаблона:

- **usb-storage**;
- **usb-modems**;
- **usb**;
- **gphoto2**.



Каждое из правил отвечает за полную блокировку тех или иных устройств.

Полная блокировка всех usb

Ниже представлено содержимое шаблонов для каждого правила:

```
#type:usb-storage
```

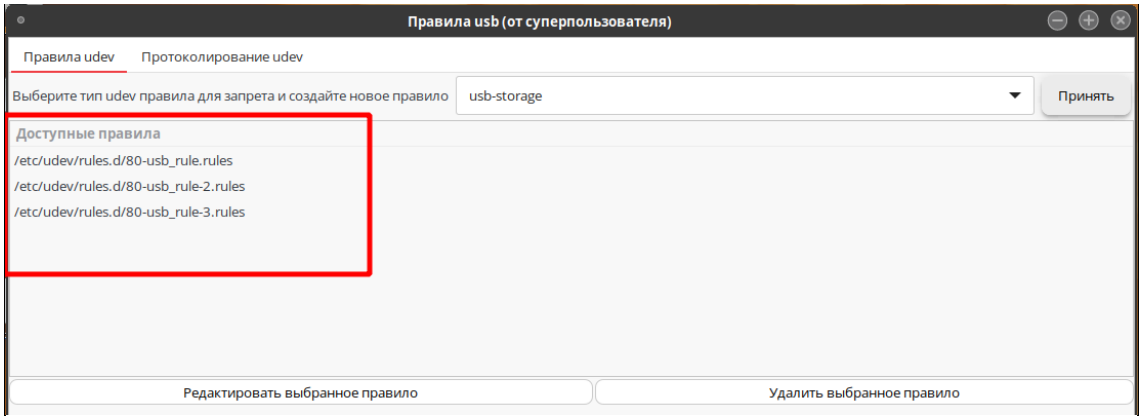
```
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:usb-modems
ACTION!="add", GOTO="dont_remove_usb"
DRIVER!="rndis_host", GOTO="dont_remove_usb"
DRIVER=="rndis_host", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

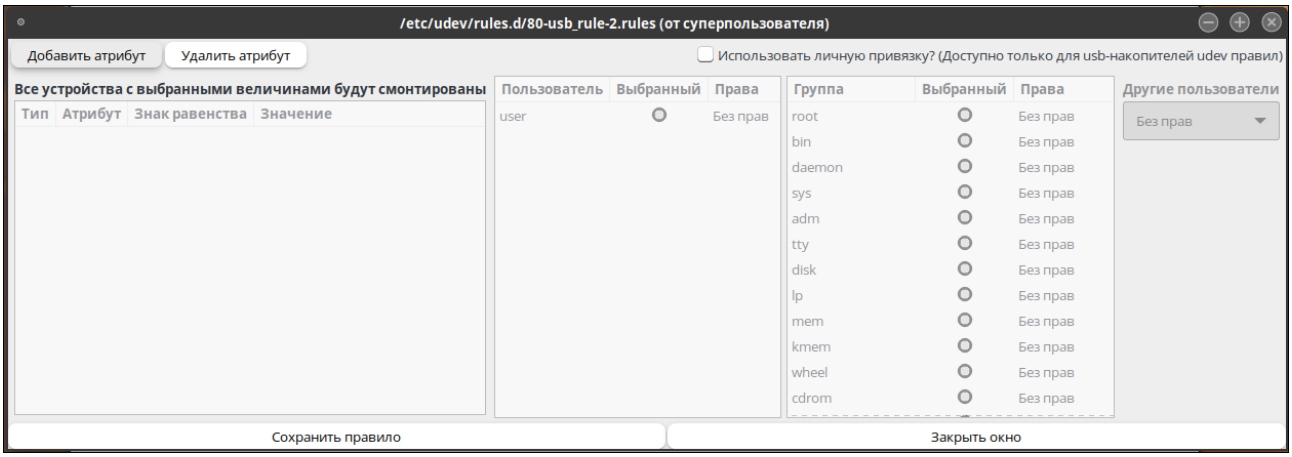
```
#type:usb
ACTION!="add", GOTO="dont_remove_usb"
SUBSYSTEM!="usb", GOTO="dont_remove_usb"
SUBSYSTEM=="usb", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

```
#type:gphoto2
ACTION!="add", GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}!="PTP",GOTO="dont_remove_usb"
ENV{GPHOTO2_DRIVER}=="PTP",ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

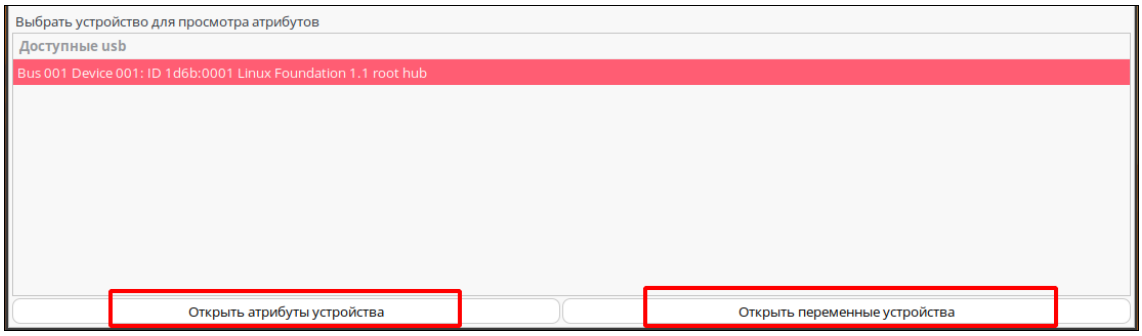
При формировании правила из шаблонного в окне утилиты появляется строка, соответствующая сформированному правилу.



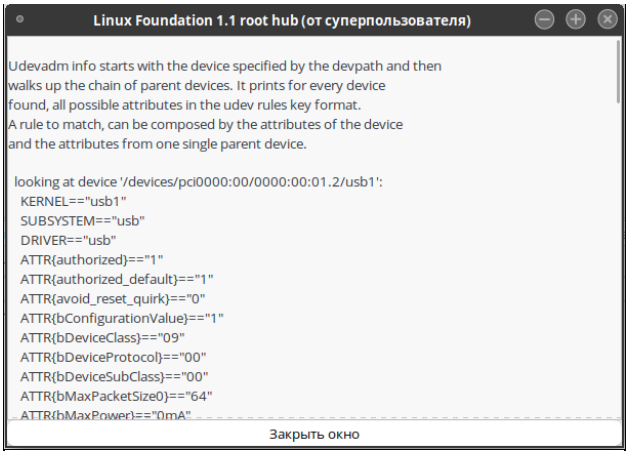
Далее потребуется создать разрешающие монтирование параметры. Для этого необходимо добавить атрибут, который в новом правиле будет отвечать за исключение из блокировки устройств, подходящих под данный параметр. Добавление или удаление таких атрибутов доступно после выбора интересующего правила и нажатия кнопки «**Редактировать правило**».

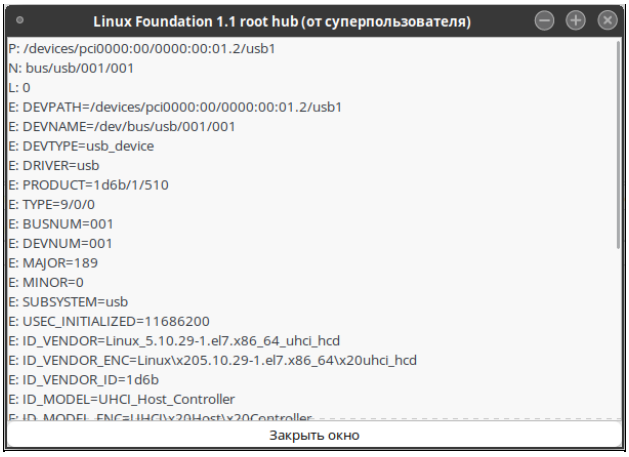


В полях «**Атрибут**» и «**Значение**» необходимо подобрать значения из доступных устройств. Просмотр доступных значений можно осуществить следующим образом:



В результате будут открыты следующие окна:



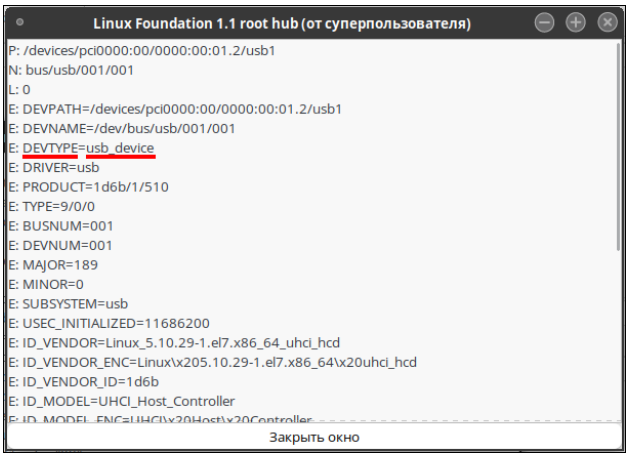


При добавлении пункта **ATTR** следует прописать значение и величины соответствующие:



Значения указываются, соответственно, без фигурных скобок **{}** и без кавычек **""**.

Для указания величин **ENV** следует выбирать величины:

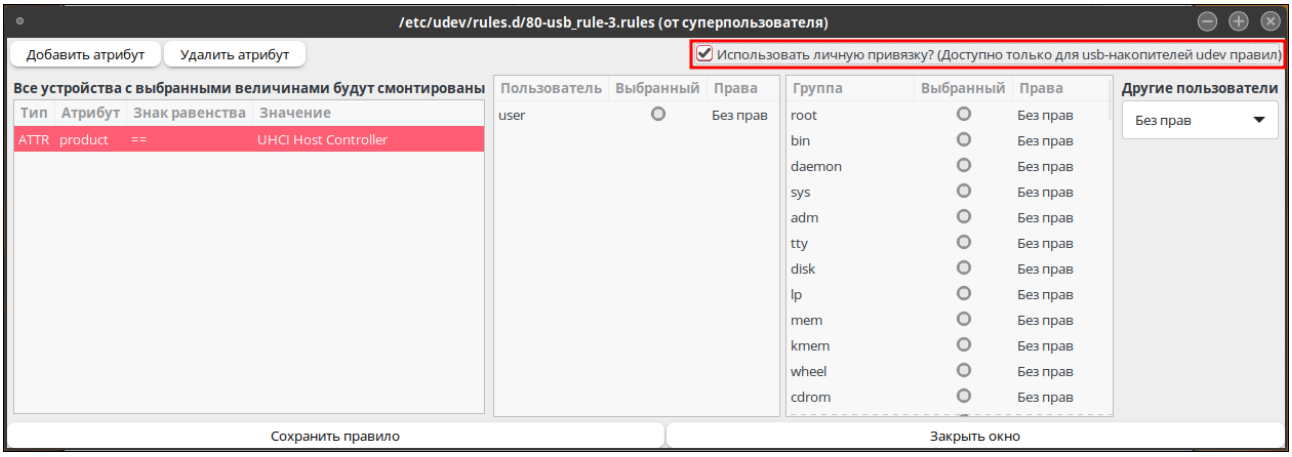


В результате будет сформировано примерно следующее правило **/etc/udev/rules.d/80-usb_rule.rules**:

```
#type:usb-storage
ACTION!="add", GOTO="dont_remove_usb"
ENV{DRIVER}!="usb-storage", GOTO="dont_remove_usb"
ATTR{product}==UHCI Host Controller, GOTO="dont_remove_usb"
ENV{DRIVER}=="usb-storage", ATTR{authorized}="0"
LABEL="dont_remove_usb"
```

Назначение личной привязки к UDEV-правилу

За назначение привязки отвечает поле, которое активируется соответствующим флагом:



По умолчанию все пользователи не имеют прав. Соответственно, потребуется выбрать необходимых пользователей и задать им права «**чтения**», «**чтения и записи**» или «**все права**».

При формировании личной привязки будет создаваться **systemd**-сервис, который будет работать в связке с отведенным под него udev-правилом.

```
nano /etc/systemd/system/usb-mount@.service
```

```
[Unit]
Description=Mount USB Drive on %i

[Service]
RemainAfterExit=true
Type=oneshot
ExecStart=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py add %i /etc/udev/rules.d/80-usb_rule.rules
ExecStop=/usr/bin/python3 /usr/share/usb_rules/usb-mount.py remove %i /etc/udev/rules.d/80-usb_rule.rules
```

Протоколирование событий usb-flash накопителей

Вкладка «**Протоколирование udev**» позволяет протоколировать события, связанные с **usb-flash** накопителями по выбранным пользователем атрибутам. Синтаксис добавления идентичен добавлению **ENV**-атрибутов.

В результате формирования правила для протоколирования будет создан файл **/etc/udev/rules.d/98-usb_logs.rules** со следующим примерным содержимым:

```
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="add", RUN+="/bin/sh -c 'echo connected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
ENV{ID_USB_DRIVER}=="usb-storage",ACTION=="remove", RUN+="/bin/sh -c 'echo disconnected $devnode
USEC_INITIALIZED=%E{USEC_INITIALIZED} $(date)>> /var/log/usblog.txt'"
```

USBIP - утилита для подключения удаленных USB-устройств

Настройка на сервере
Настройка на клиенте
Графическая утилита usbip-gui

USBIP — это утилита, направленная на предоставление в общий доступ USB-устройств через IP-сеть для совместного использования. Чтобы совместно использовать USB-устройства между компьютерами с их полной функциональностью, *USBIP* преобразует «сообщения ввода-вывода USB» в полезные данные **TCP/IP** и передает их между компьютерами. Оригинальные драйверы и приложения для USB-устройств также могут использоваться для удаленных USB-устройств без их модификации. Компьютер может использовать удаленные USB-устройства, как если бы они были напрямую подключены.

Устройства, которые можно подключить через утилиту:

- запоминающие устройства USB: флешки, внешние жесткие диски и картридеры;
- периферийные устройства ввода: USB-клавиатуры, мыши;
- мультимедийные устройства (например, веб-камеры);
- оборудование для печати и сканирования.

Вы можете подробнее ознакомиться с установкой и настройкой утилиты **USBIP**, просмотрев наши обучающие видео:

- на **RuTube** — Подключение удаленных USB устройств. USBIP;
- в **Яндекс.Дзен** — Подключение удаленных USB устройств. USBIP;
- в **VK Видео** — Подключение удаленных USB устройств. USBIP.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка на сервере

Сервер предназначен для публикации **USB-устройств**, которые могут быть удаленно доступны с клиентской стороны. Он выполняет роль хоста, предоставляя подключенные к нему **USB-устройства** (например, флеш-накопители, принтеры, сканеры) для использования через сеть. Это позволяет клиентам взаимодействовать с устройствами так, как если бы они были подключены локально.

Для начала работы необходимо установить утилиту *USBIP* командой (потребуются права **администратора**):

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe usbip-host
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 usbip-host
 vhci-hcd
```

Сохраните изменения и закройте редактор. Чтобы обеспечить автоматический запуск **usbipd** при старте системы, его можно оформить в виде системного юнита:

```
nano /etc/systemd/system/usbipd.service
```

Добавьте в файл следующие строки:

```
[Unit]
 Description=USBIPd
```

```
[Service]
ExecStart=/usr/sbin/usbipd -D
Type=oneshot
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

После создания или изменения системного юнита необходимо перезагрузить настройки менеджера системных служб и включить автоматический запуск службы usbipd, чтобы она запускалась сразу после загрузки системы. Для этого выполните следующие команды:

```
sudo systemctl daemon-reload
sudo systemctl enable usbipd --now
```

Перед тем как открыть доступ к какому-либо usb-устройству, нужно узнать его ID. Сделать это можно командой:

```
usbip list -l
```

Доступ к устройству открывается с помощью команды:

```
sudo usbip bind --busid=1-1
```

где **1-1** - это ID устройства.

Проверить, что устройство успешно привязано и доступно для использования, можно выполнив на сервере команду:

```
usbip list -r localhost
```

Для закрытия доступа к устройству необходимо ввести команду:

```
sudo usbip unbind -b 1-1
```

Настройка на клиенте

Клиент предназначен для подключения **USB-устройств**, опубликованных на сервере. Через клиента устройства, находящиеся на сервере, становятся доступными для локального использования, как если бы они были подключены непосредственно к клиентскому компьютеру.

Для начала работы необходимо установить утилиту *USBIP* командой:

```
sudo dnf install usbip
```

Следующим этапом требуется подключить дополнительные модули:

```
sudo modprobe usbip-core
sudo modprobe vhci-hcd
lsmod | grep usbip
```

Для автоматической загрузки модулей создайте файл конфигурации **/etc/modules-load.d/usbip.conf**:

```
sudo nano /etc/modules-load.d/usbip.conf
```

Добавьте в файл следующие строки:

```
usbip-core
 vhci-hcd
```

Сохраните изменения и закройте редактор.

Проверить доступность USB-устройств, подключенных к серверу, можно выполнив на клиенте команду:

```
sudo usbip list -r <IP-адрес-сервера>
```

Для подключения открытого в общий доступ устройства на сервере к компьютеру-клиенту надо знать его ID и IP-адрес сервера. Для этого необходимо выполнить команду:

```
sudo usbip attach --remote=<IP-адрес-сервера> --busid=1-1
```

где:

- **1-1** — это ID устройства,
- **<IP-адрес-сервера>** — это IP-адрес сервера в формате **xx.xx.xx.xx**.

После подключения USB-устройства оно должно отображаться после выполнения команды:

```
lsusb
```

Для того чтобы отключить устройство из общего доступа, необходимо узнать его порт:

```
sudo usbip port
```

После того, как порт определен, можно отсоединить устройство:

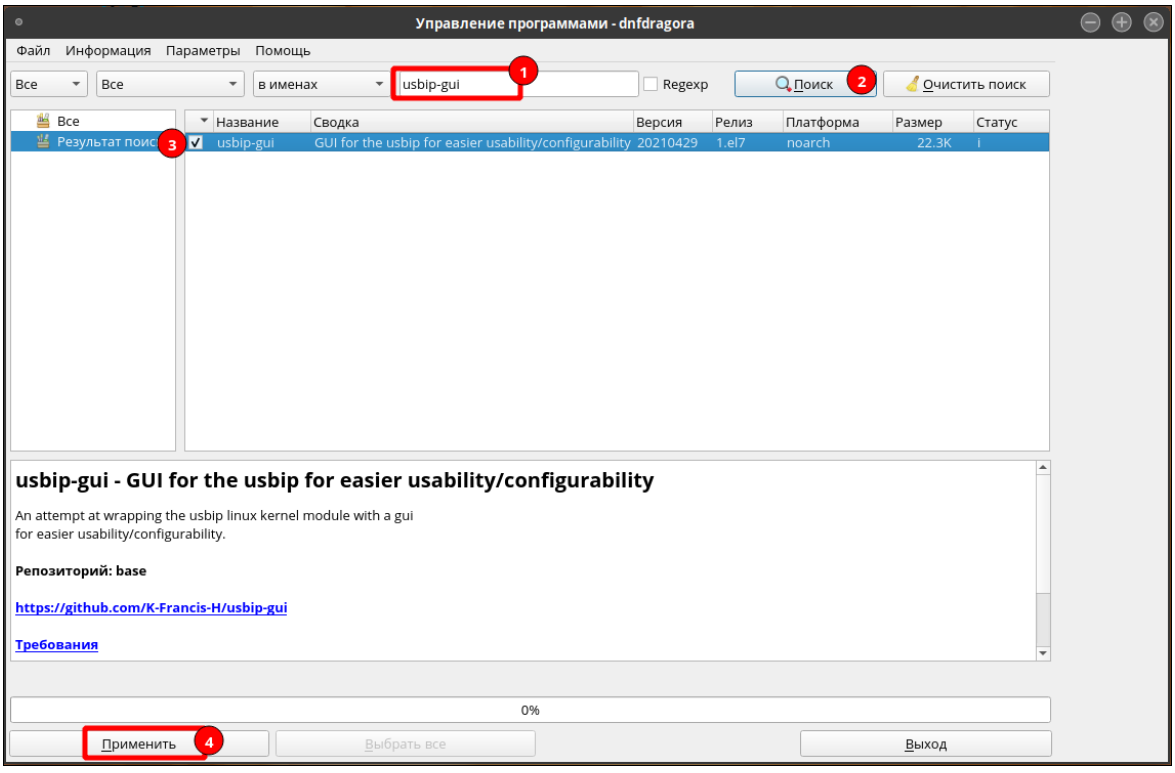
```
sudo usbip detach --port=0
```

Графическая утилита usbip-gui

В РЕД ОС также существует графическая утилита для предоставления в общий доступ USB-устройств через IP-сеть — **usbip-gui**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**usbip-gui**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.

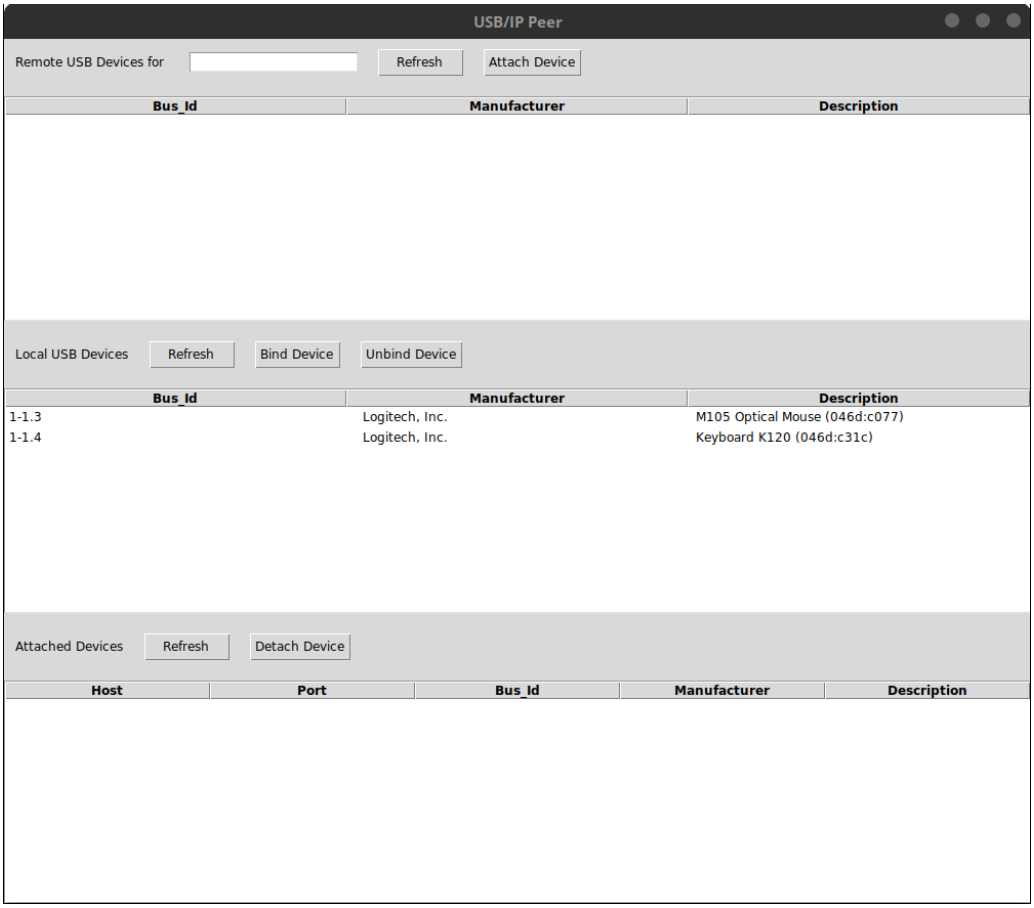


Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

```
sudo dnf install usbip-gui
```

После установки программа будет доступна из «**Главного меню**» — «**Администрирование**» — «**Управление USBIP**». Обратите

внимание, что для работы с программой необходимы права администратора или суперпользователя системы.



Установка драйвера Nvidia в РЕД ОС

Обновление ОС
Информация о видеокарте
Способ 1. Установка проприетарного драйвера Nvidia из репозитория
Способ 2. Установка драйвера Nvidia через run-файл
Переключение используемых видеокарт nVidia и Intel
Переключение видеокарт из терминала
Переключение видеокарт в графическом режиме
Переключение используемых видеокарт nVidia и Intel при использовании менеджера SDDM

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: Nvidia Driver 535

Поддержка видеокарт **Nvidia** в РЕД ОС по умолчанию осуществляется в виде драйвера **nouveau** с открытым исходным кодом. Если драйвер **nouveau** не удовлетворяет достаточным требованиям, например, в нем нет поддержки CUDA ядер, то пользователи могут установить официальный **проприетарный** драйвер **Nvidia.**

Вы можете подробнее ознакомиться с информацией по установке и настройке драйвера Nvidia, просмотрев наши обучающие видео:

- на **RuTube** — Установка видео-драйверов NVIDIA;
- в **Яндекс.Дзен** — Установка видео-драйверов NVIDIA;
- в **VK Видео** — Установка видео-драйверов NVIDIA.

На наших каналах вы также сможете найти много другой полезной информации.

Обновление ОС

ВАЖНО!

Перед установкой драйверов систему необходимо **обновить**!

Перед установкой драйвера NVIDIA убедитесь, что у вас установлены все последние обновления:

```
sudo -E dnf update
```

После установки обновлений необходимо перезагрузить ПК для завершения обновления.

Информация о видеокарте

С помощью утилиты **lshw** можно вывести информацию о видеокарте и об используемом видеодрайвере.

С правами администратора выполните команды:

```
sudo -E dnf install lshw
sudo -E lshw -numeric -C display
```



где **product** — модель видеокарты.

Прежде чем устанавливать драйвер, убедитесь, что он подходит для вашей видеокарты. Для этого выполните следующий алгоритм действий.

1. Перейдите на официальный сайт NVIDIA.

2. Выберите модель вашей видеокарты в разделе поиска драйверов.
3. Узнайте, какая версия драйвера поддерживается для вашей видеокарты.
4. Если ваша видеокарта является устаревшей, учтите, что первый способ может не сработать. В этом случае потребуется скачать драйвер из архива поддерживаемых устройств на сайте NVIDIA.

Способ 1. Установка проприетарного драйвера nVidia из репозитория

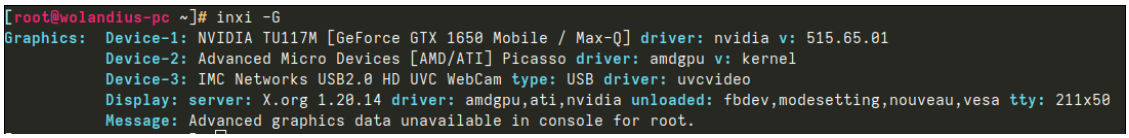
Для установки проприетарного драйвера **nVidia** из репозитория РЕД ОС выполните команду:

```
sudo -E dnf install nvidia-settings nvidia-kmod nvidia-persistenced nvidia-xconfig nvidia-modprobe xorg-x11-drv-nvidia xorg-x11-drv-nvidia-cuda-libs
```

На данном этапе установка завершена. Для применения изменений необходимо перезагрузить ПК.

После перезагрузки запустите в терминале утилиту inxi и убедитесь, что используется драйвер **nVidia**:

```
inxi -G
```



ВАЖНО!

Если ранее в системе уже были установлены проприетарные драйверы, модули ядра или вносились какие-либо другие изменения, то перед этим необходимо обязательно вернуть все настройки к стандартным или выполнять установку драйверов на чистую систему для исключения возможных конфликтов и ошибок.

Способ 2. Установка драйвера nVidia через run-файл

Загрузка драйвера

Загрузите инсталлятор с официального сайта **nVidia** в виде бинарного файла с расширением **RUN**.

Список драйверов доступен по ссылке, здесь представлены как новые драйвера, так и архивные, которые поддерживают старые графические видеокарты.

В описании (вкладка **Supported Products**) к драйверу обратите внимание на наличие вашей модели видеокарты. Если в выбранном драйвере нет вашей модели, то перейдите в описание следующего драйвера. Также для загрузки нужного драйвера можно воспользоваться поиском по параметрам - https://www.nvidia.com/Download/index.aspx?lang=ru.

Отключение драйвера nouveau

Предварительно необходимо отключить используемый по умолчанию драйвер **nouveau**.

Для этого потребуется внести изменения в конфигурацию **grubby** с помощью команды:

```
sudo -E grubby --update-kernel ALL --args="nouveau.modeset=0"
```

Следует заметить, что на ПК, где используется только видеокарта NVIDIA, после перезагрузки будет отсутствовать изображение. Добавьте опцию загрузки в текстовом режиме:

```
sudo -E grubby --update-kernel ALL --args="3"
```

Для обновления конфигурации загрузчика grub2 выполните команду:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Перезагрузите систему.

Проверьте, что драйвер **nouveau** для **nVidia** с открытым исходным кодом больше не используется:

```
lshw -numeric -C display
```

```
[root@wolandius-pc ~]# lshw -numeric -C display
  *-display UNCLAIMED
       description: VGA compatible controller
       product: TU117M [GeForce GTX 1650 Mobile / Max-Q] [10DE:1F91]
       vendor: NVIDIA Corporation [10DE]
       physical id: 0
       bus info: pci@0000:01:00.0
       version: a1
       width: 64 bits
       clock: 33MHz
       capabilities: pm msi pciexpress vga_controller cap_list
       configuration: latency=0
       resources: memory:f6000000-f6ffffff memory:c0000000-cfffffff memory:d0000000-d1ffffff ioport:f000(size=128) memory:f7000000-f707ffff
```

Установка драйвера

Введите логин **root** и пароль. Перейдите в каталог с загруженным драйвером, установите дополнительные пакеты и выполните команду запуска установки:

```
cd /<путь_до_каталога_с_драйвером>sudo dnf install dkms gcc kernel-lt-devel
bash ./NVIDIA-Linux-x86_64-*.run
```

```
[root@wolandius-pc wolandius]# bash ./NVIDIA-Linux-x86_64-515.65.01.run
Verifying archive integrity...
```

В случае возникновения диалогового окна выберите следующее действие:

```
The initramfs will likely need to be rebuilt due to the following condition(s):
* Nouveau is present in the initramfs.

Would you like to rebuild the initramfs?

                    Do not rebuild initramfs                    Rebuild initramfs
```

Would you like to register the kernel module sources with DKMS? This will allow DKMS to automatically build a new module, if you install a different kernel later.

- **Yes**
- No

```
Would you like to register the kernel module sources with DKMS? This will allow DKMS to automatically build
a new module, if you install a different kernel later.

                    Yes                                    No
```

Install NVIDIA's 32-bit compatibility libraries?

- **Yes**
- No

```
Install NVIDIA's 32-bit compatibility libraries?

                    Yes                                    No
```

В случае возникновения диалогового окна выберите следующее действие:

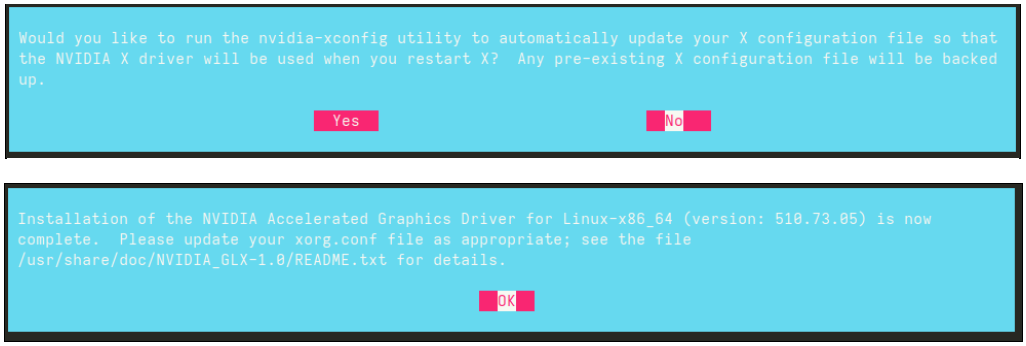
An incomplete installation of libglvnd was found. Do you want to install a full copy of libglvnd? This will overwrite any existing libglvnd libraries.

- Don't install libglvnd files
- **Install and overw.**
- Abort installation

```
An incomplete installation of libglvnd was found. All of the essential
libglvnd libraries are present, but one or more optional components are
missing. Do you want to install a full copy of libglvnd? This will overwrite
any existing libglvnd libraries.

    Don't install   Install and overw          Abort installation.
```

Would you like to run the nvidia-xconfig utility to automatically update your X configuration file so that the NVIDIA X driver will be used when you restart X? Any pre-existing X configuration file will be backed up.

- Yes
- **No**



Далее отключите текстовый режим командой:

```
sudo -E grubby --update-kernel ALL --remove-args="3"
```

Для обновления конфигурации загрузчика grub2 выполните команду:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

На данном этапе установка завершена, перезагрузите ПК. Запустите в терминале утилиту **inxi** и убедитесь, что используется драйвер **Nvidia**:

```
inxi -G
```

```
[root@wolandius-pc ~]# inxi -G
Graphics:  Device-1: NVIDIA TU117M [GeForce GTX 1650 Mobile / Max-Q] driver: nvidia v: 515.65.01
           Device-2: Advanced Micro Devices [AMD/ATI] Picasso driver: amdgpu v: kernel
           Device-3: IMC Networks USB2.0 HD UVC WebCam type: USB driver: uvcvideo
           Display: server: X.org 1.20.14 driver: amdgpu,ati,nvidia unloaded: fbdev,modesetting,nouveau,vesa tty: 211x50
           Message: Advanced graphics data unavailable in console for root.
```

Переключение используемых видеокарт nVidia и Intel

Для систем с двумя видео-адаптерами дополнительно разработан пакет **nvidia-primus**. Данный пакет содержит преднастроенные конфигурации и утилиты для переключения основного видео-контроллера и запуска программ на адаптере **nVidia**, если основным установлен видео-контроллер от **Intel**.

Вы можете подробнее ознакомиться с возможностями переключения основного видео-контроллера, просмотрев наши обучающие видео:

- на **RuTube**:
  - Переключение между видеокартами NVIDIA Intel. Проприетарные драйверы NVIDIA ;
  - Графическая утилита для переключения видеокарт Nvidia и Intel .
- в **Яндекс.Дзен**:
  - Переключение между видеокартами NVIDIA Intel. Проприетарные драйверы NVIDIA ;
  - Графическая утилита для переключения видеокарт Nvidia и Intel .
- в **VK Видео**:
  - Переключение между видеокартами NVIDIA Intel. Проприетарные драйверы NVIDIA ;
  - Графическая утилита для переключения видеокарт Nvidia и Intel .

На наших каналах вы также сможете найти много другой полезной информации.

Для установки пакета выполните команду (потребуются права администратора):

```
sudo dnf install nvidia-primus
```

После установки пакета автоматически запускаются службы **nvidia-hibernate.service**, **nvidia-resume.service**, **nvidia-suspend.service** (поставляются в пакете **xorg-x11-drv-nvidia**), необходимые для корректной работы соответствующих действий (*hibernate*, *resume* и *suspend*).

Перезагрузите систему для применения изменений.

Работа с утилитой возможна как из терминала, так и в графическом режиме.

Переключение видеокарт из терминала

Для переключения основного адаптера *из терминала* используется утилита **prime-select**.

Основные опции утилиты **prime-select**:

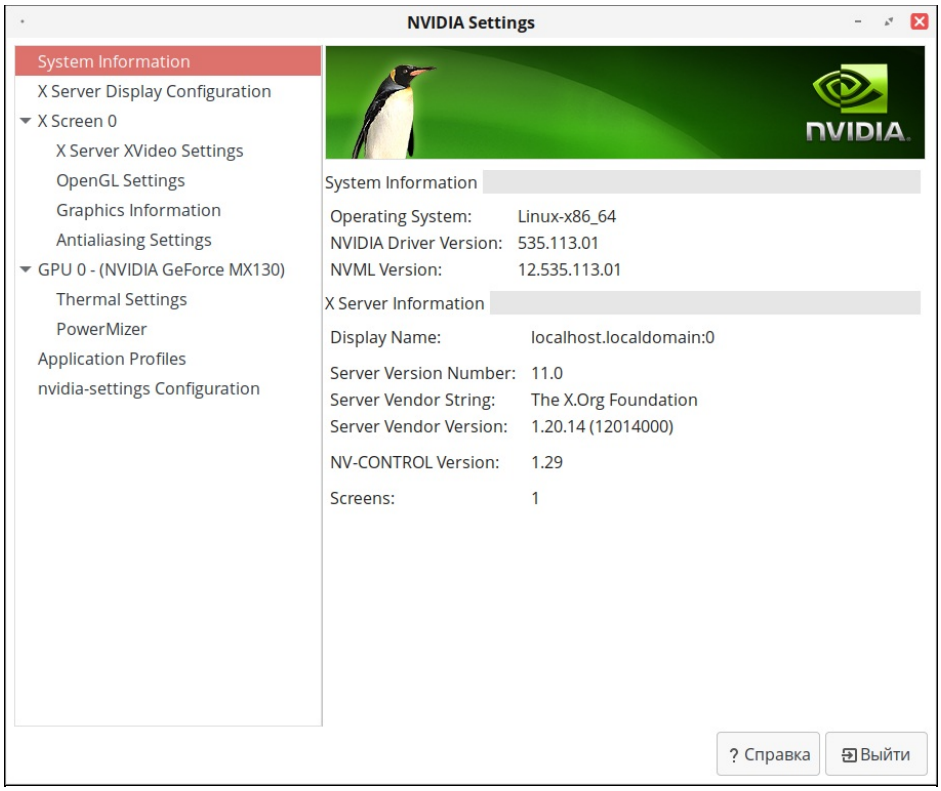
- `intel` — установить основным адаптер *Intel*;
- `nvidia` — установить основным адаптер *nVidia*;
- `status` — показать текущий основной адаптер;
- `-h`, `--help` — вывод справки.

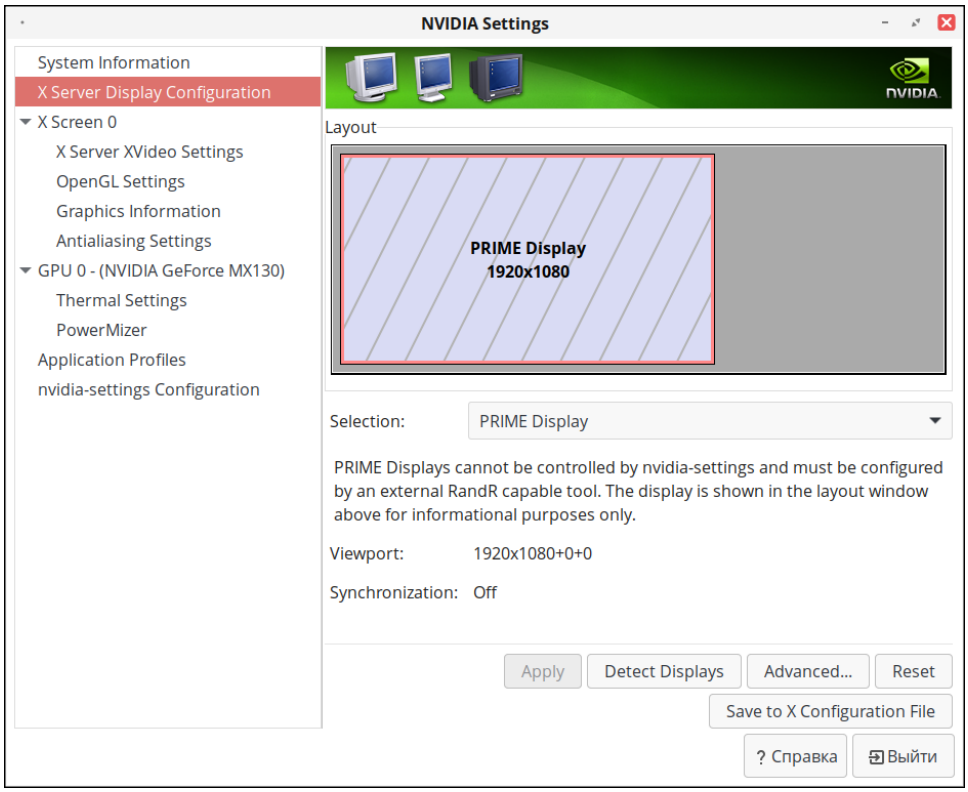
Просмотр текущего используемого видео-адаптера и вывод справки доступны без дополнительных привилегий. Для переключения видео-адаптера потребуются права **администратора** системы, например:

```
sudo prime-select nvidia
```

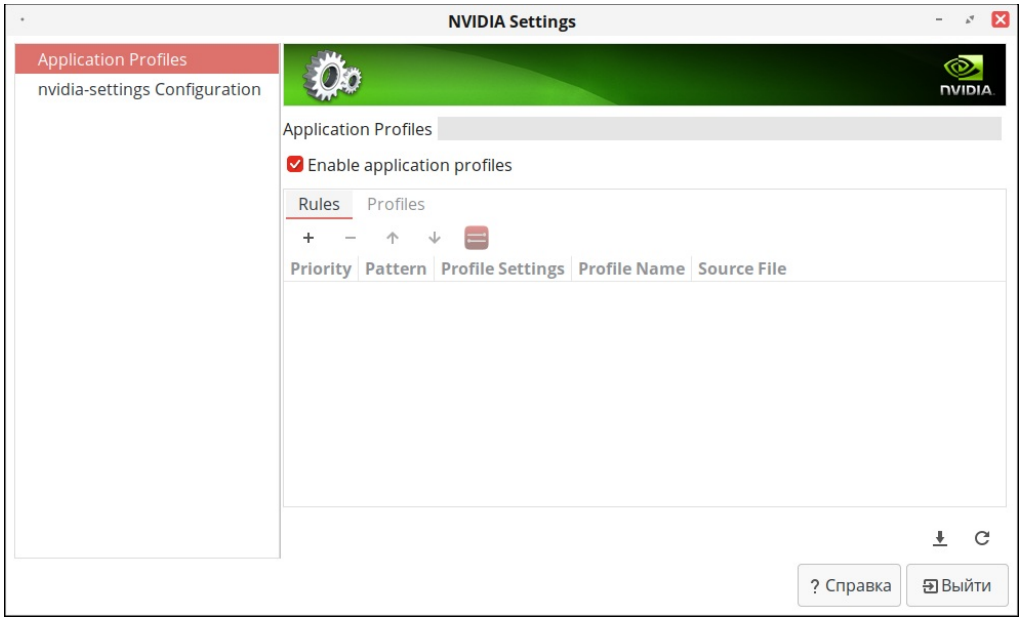
Для применения внесенных изменений потребуется перезагрузка системы.

Также, если основным видео-адаптером установлен **nVidia**, в утилите «**Параметры NVIDIA X Server**» будут доступны разделы по настройке оборудования и просмотр таких параметров, как *яркость*, *гамма*, *атрибуты XVideo*, *температура* и *функции OpenGL*.





В случае если основным видео-адаптером установлен **Intel**, в утилите будут доступны только разделы по настройке профилей приложений.

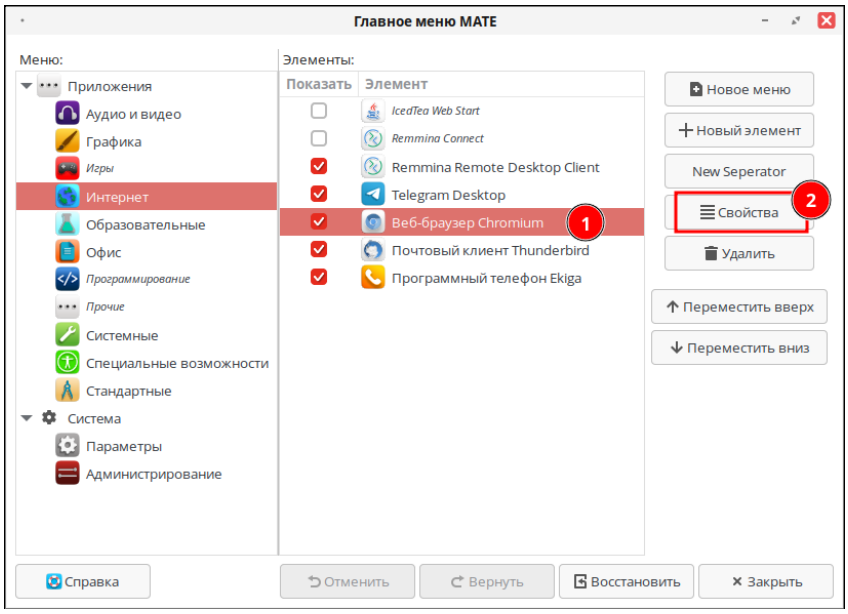


Бывают ситуации, когда в качестве основного видео-адаптера используется **Intel** (например, в ноутбуках для сохранения заряда батареи), но для запуска какой-либо программы необходим контроллер **nVidia**. Для этого можно использовать утилиту **prime-run** (входит в состав пакета **nvidia-primus**), передавая ей имя программы и все ее аргументы (если таковые имеются) в качестве опций. Например:

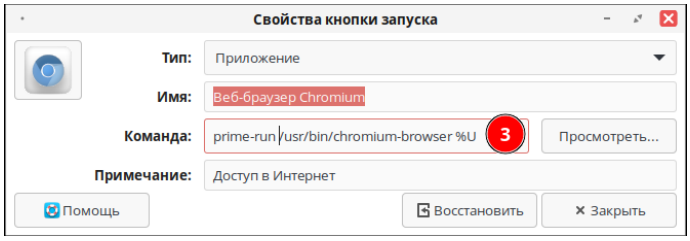
```
prime-run chromium-browser
```

Данный процесс можно упростить, изменив команду запуска непосредственно нужного приложения. Для этого нажмите ПКМ по **Главному меню**, в появившемся контекстном меню выберите «**Редактировать меню**». Будет открыто окно редактирования главного меню.

Далее найдите и выберите нужную программу, нажмите «**Свойства**».



В открывшемся окне «**Свойства кнопки запуска**» в поле **Команда** в начало строки допишите prime run и нажмите «**Закрыть**».



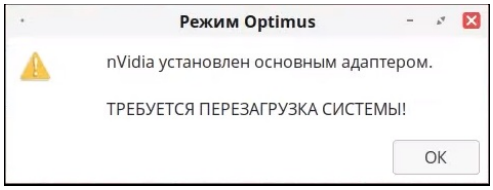
После этого выбранная программа всегда будет запускаться с использованием видео-адаптера **nVidia**.

Переключение видеокарт в графическом режиме

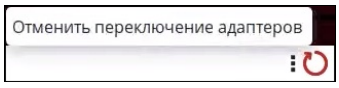
Переключение видео-адаптеров *в графическом режиме* производится с помощью появившейся в системном трее пиктограммы —  .

При нажатии ЛКМ по пиктограмме будет выведена информация об используемом видео-адаптере. Для смены видео-адаптера нажмите ПКМ по пиктограмме и в появившемся меню выберите «**Переключить на адаптер nVidia**».

После этого появится информационное сообщение о том, что видео-адаптер изменен, и требуется перезагрузка системы.



До перезагрузки системы по-прежнему будет использоваться видео-адаптер **Intel**, а смену адаптера можно отменить, нажав ЛКМ по изменившейся пиктограмме и выбрав «**Отменить переключение адаптеров**».



После перезагрузки системы, если смена адаптера не была отменена, будет активирован видеа-адаптер **nVidia**. Пиктограмма в системном трее также изменится —  .

Переключение используемых видеокарт nVidia и Intel при использовании менеджера SDDM

При использовании **SDDM** до перезагрузки системы (при переключении на **nVidia**) необходимо настроить конфигурирование вывода при запуске графической среды.

Запустите терминал и выполните команду:

```
xrandr --listproviders
```

Вывод должен содержать список из двух или более провайдеров (устройств). Наример:

```
xrandr --listproviders

Providers: number : 2
Provider 0: id: 0x221 cap: 0x9, Source Output, Sink Offload crtcs: 3 outputs: 6 associated providers: 0 name:modesetting
Provider 1: id: 0x1f8 cap: 0x0 crtcs: 0 outputs: 0 associated providers: 0 name:NVIDIA-G0
```

В данном примере провайдер с именем `modesetting` представлен адаптером с низкой производительностью, который обеспечивает вывод изображения на дисплей. Провайдер с именем `NVIDIA-G0` представлен более производительным устройством, которое будет выполнять основную нагрузку по формированию изображения для последующего вывода через провайдер `modesetting`. Для этого необходимо, чтобы провайдер `modesetting` обладал функцией **Sink Offload** (в примере подсвечено зеленым).

Откройте файл **/etc/sddm/Xsetup** на редактирование:

```
sudo nano /etc/sddm/Xsetup
```

Добавьте строки вида:

```
xrandr --setprovideroffloadsink <основной_провайдер> <провайдер_вывода>
xrandr --auto
```

Замените следующие блоки на значения из списка провайдеров:

- `<основной_провайдер>` - порядковый номер, id или имя провайдера nVidia (в примере: 1, 0x1f8 или NVIDIA-G0);
- `<провайдер_вывода>` - порядковый номер, id или имя провайдера, обеспечивающего вывод изображения (в примере: 0, 0x221 или modesetting).

Рекомендуется указать имя провайдера или id. Пример:

```
xrandr --setprovideroffloadsink NVIDIA-G0 modesetting
xrandr --auto
```

Примечание.

Если указанные выше действия не были выполнены до перезагрузки и при загрузке ОС изображение не выводится, то переключитесь на использование **Intel**, выполнив следующие шаги:

1. После загрузки ОС (логотип загрузки исчез) нажмите сочетание клавиш *Ctrl+Alt+F3*.

2. Введите имя пользователя и пароль, подтверждая ввод нажатием *Enter*.

3. Выполните команды:

```
sudo prime-select intel
reboot
```

Envycontrol - утилита для переключения режимов графического процессора

Установка
Синтаксис
Опции
Режимы работы
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: python3-envycontrol-3.4.0

Установка

Для установки утилиты через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install python3-envycontrol
```

Дальнейшая работа с утилитой производится с правами администратора.

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
envycontrol [--help] [--version] [-q] [-s режим] [--dm менеджер_режима] [--force-comp] [--coolbits [значение]] [--rtd3 [значение]] [--reset-sddm] [--reset] [--verbose]
```

Опции

Основные опции утилиты:

- **-h, --help** – выводит справку о доступных опциях утилиты;
- **-v, --version** - выводит версию утилиты **envycontrol**;
- **-q, --query** - возвращает текущий режим графики;
- **-s [режим], --switch [режим]** – переключает режим графики: **integrated** (интегрированный), **hybrid** (гибридный), **nvidia**;
- **--dm менеджер_режима** – позволяет вручную указать менеджер отображения для режима **nvidia**: gdm, gdm3, sddm, lightdm;
- **--force-comp** - включает ForceCompositionPipeline в режиме **nvidia**;
- **--coolbits [значение]** - включает Coolbits в режиме **nvidia** (по умолчанию: 28);
- **--rtd3 [значение]** - настраивает управление питанием PCI-Express Runtime D3 (RTD3) в режиме **hybrid**: 0, 1, 2, 3 (по умолчанию: 2);
- **--use-nvidia-current** - использует **nvidia-current** вместо **nvidia** для модулей ядра;
- **--reset-sddm** - восстанавливает исходный файл настройки Xsetup;
- **--reset** - отменяет изменения, внесенные **envycontrol**;
- **--cache-create** - создает кеш, используемый **envycontrol** (работает только в режиме **hybrid)**;
- **--cache-delete** - удаляет созданный кеш **envycontrol**;
- **--cache-query** - показывает созданный кеш **envycontrol**;
- **--verbose** - включает подробный режим вывода информации.

Режимы работы

EnvyControl предоставляет возможность выбора режима работы графики:

1 . **Гибридный режим** - позволяет драйверу автоматически определять, какой графический процессор использовать, обычно предпочитая интегрированную графику и активируя режим NVIDIA только при необходимости. Производительность на внешних экранах может быть снижена.

2 . **Интегрированный режим** - использует только интегрированную графику (Intel или AMD iGPU), отключая работу с видеокартой NVIDIA для снижения энергопотребления. Мониторы, подключенные к NVIDIA dGPU, не будут использоваться.

3 . **Режим NVIDIA** - обеспечивает использование видеокарты от NVIDIA, игнорируя интегрированную графику. Более высокая графическая производительность и более высокое энергопотребление.

Примеры использования

1. Для установки интегрированного графического режима:

```
sudo envycontrol -s integrated
```

2. Для установки гибридного графического режима и включения детального регулирования мощности:

```
sudo envycontrol -s hybrid --rtd3
```

3. Для установки графического режима nvidia и включения ForceCompositionPipeline и Coolbits со значением 24:

```
sudo envycontrol -s nvidia --force-comp --coolbits 24
```

4. Для установки графического режима nvidia и для настройки **lightdm**:

```
sudo envycontrol -s nvidia --dm lightdm
```

5. Для проверки текущего графического режима:

```
envycontrol --query
```

6. Для включения подробного режима вывода информации:

```
sudo envycontrol --verbose
```

7. Для отмены изменений, внесенных **envycontrol**:

```
sudo envycontrol --reset
```

PowerTOP - утилита управления питанием

Обзор
Применение параметров
Формирование отчета

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: powertop-2.9-3

PowerTOP — программа диагностики проблем, связанных с энергопотреблением, предоставляет оценку общего энергопотребления системы, а также индивидуального энергопотребления для каждого процесса, устройства, рабочего ядра, таймера и обработчика прерываний.

Для установки **powertop** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install powertop
```

Работа в программе производится через терминал с правами администратора системы или суперпользователя **root**.

Запуск программы осуществляется командой:

```
powertop
```

Примечание.

Программу следует запускать, когда ноутбук работает от аккумулятора.

Перед использованием программы необходимо откалибровать механизм оценки энергопотребления, выполнив следующую команду:

```
powertop --calibrate
```

Примечание.

Во время калибровки происходит смена яркости экрана и отключение сетевых интерфейсов.

Обзор

Интерфейс утилиты представлен в виде нескольких вкладок:

- *Overview*;
- *Idle stats*;
- *Frequency stats*;
- *Device stats*;
- *Tunables*.

На вкладке **Overview** отображается список компонентов, которые либо чаще всего отправляют сигналы пробуждения на центральный процессор, либо потребляют больше всего энергии.

Вкладка **Idle stats** показывает состояния питания для всех процессоров и ядер.

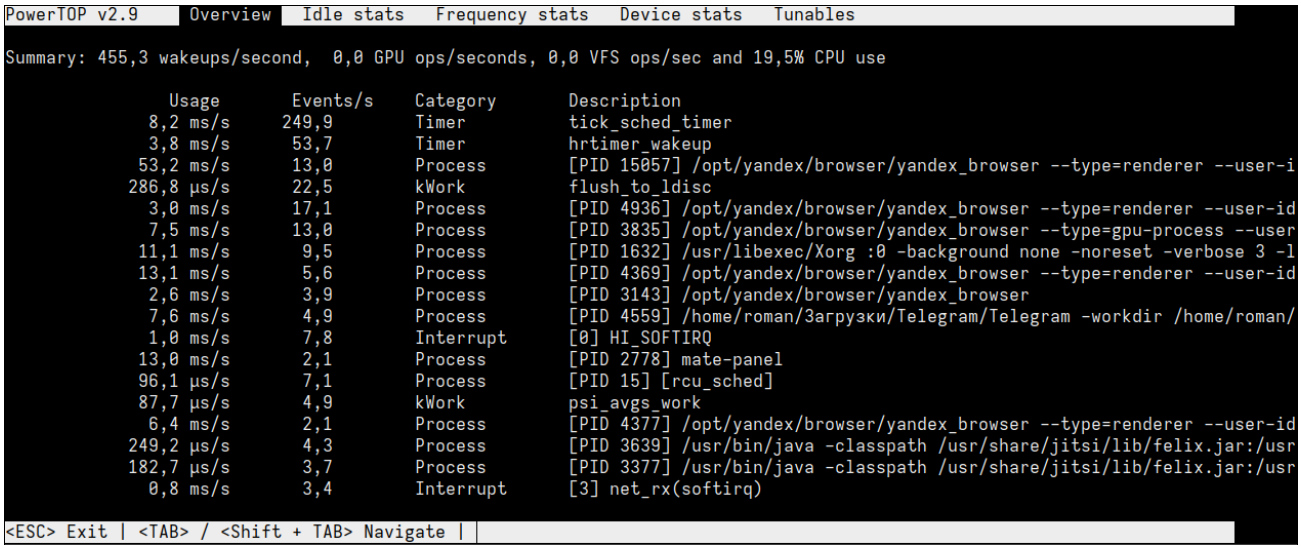
Вкладка **Frequency stats** показывает состояния производительности, включая турборежим (если применимо) для всех процессоров и

ядер.

На вкладке **Device stats** представлена информация, аналогичная вкладке **Overview**, но для устройств.

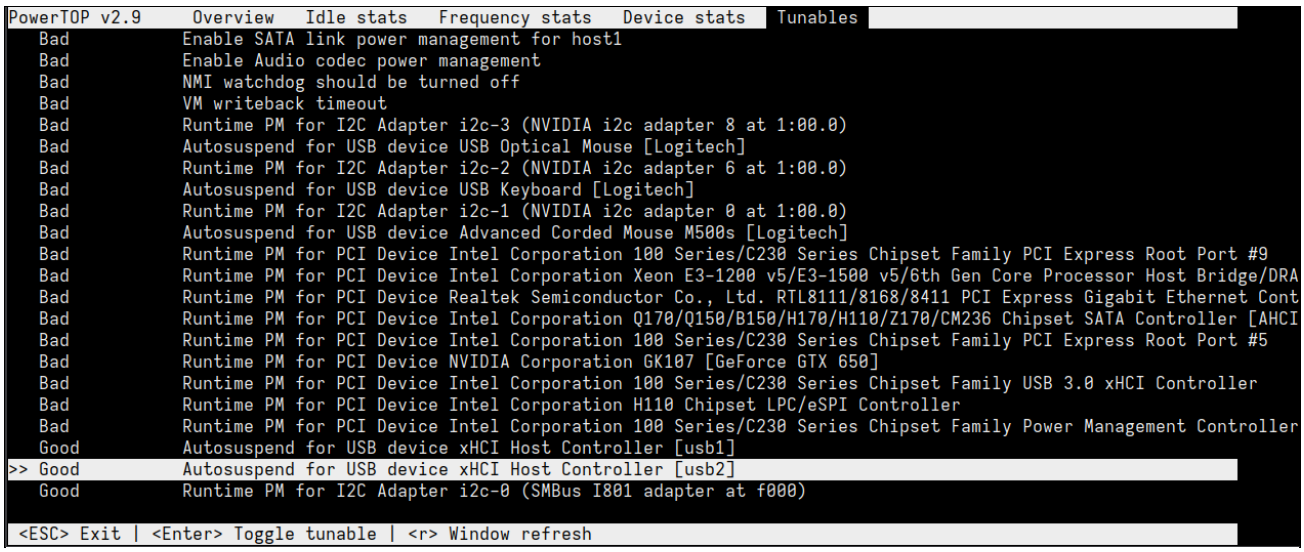
Вкладка **Tunables** содержит предложения **PowerTOP** по оптимизации системы для снижения энергопотребления.

Для переключения между вкладками используйте клавиши **TAB** и **Shift+TAB**, для перемещения по пунктам меню — клавиши **Up** и **Down**, для включения или выключения рекомендуемого параметра — **Enter**.



Применение параметров

Изменение параметров можно производить вручную через вкладку **Tunables**. Устройства, имеющие статус «*Bad*» рекомендуется оптимизировать, нажав клавишу **Enter**. Устройства со статусом «*Good*» работают в оптимальном режиме.



Для применения всех рекомендуемых настроек выполните:

```
powertop --auto-tune
```

Для сохранения установленных параметров необходимо запустить утилиту как службу командой:

```
systemctl start powertop.service
```

Данные настройки действительны до перезагрузки системы. Для автоматического применения рекомендуемых настроек при старте системы необходимо добавить службу **powertop** в автозагрузку. Для этого выполните команду:

```
systemctl enable powertop.service
```

Формирование отчета

Powertop позволяет сформировать отчет в форматах **html** и **csv**.

Для формирования отчета в **html** выполните команду:

```
powertop --html=namereport.html
```

Для формирования отчета в **csv** выполните команду:

```
powertop --csv=namereport.csv
```

TLP и TLPUI — утилиты для управления питанием

Установка TLP, TLP-RDW, TLPUI
Работа в графическом интерфейсе
Запуск TLPUI
Основные возможности утилиты TLPUI
Смена языка интерфейса
Описание интерфейса TLPUI
Работа в терминале
Синтаксис TLP
Команды TLP
Параметры TLP
Примеры использования утилиты
TLP-RDW

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tlp-1.5.0-4, tlp-rdw-1.5.0-4, tlpui-1.5.0-5

TLP и **TLPUI** — это утилиты для управления питанием, которые позволяют значительно улучшить энергопотребление и увеличить время автономной работы устройств.

TLP обеспечивает широкий спектр функций для настройки различных компонентов системы, включая процессор, жесткие диски, беспроводные и сетевые устройства, а также графические и звуковые компоненты. Хотя **TLP** предлагает множество опций для настройки, его использование может быть сложным для обычных пользователей, так как требует работы с командной строкой.

TLPUI предоставляет удобный графический интерфейс для **TLP**, упрощая процесс настройки параметров и избавляя пользователей от необходимости вручную редактировать конфигурационные файлы.

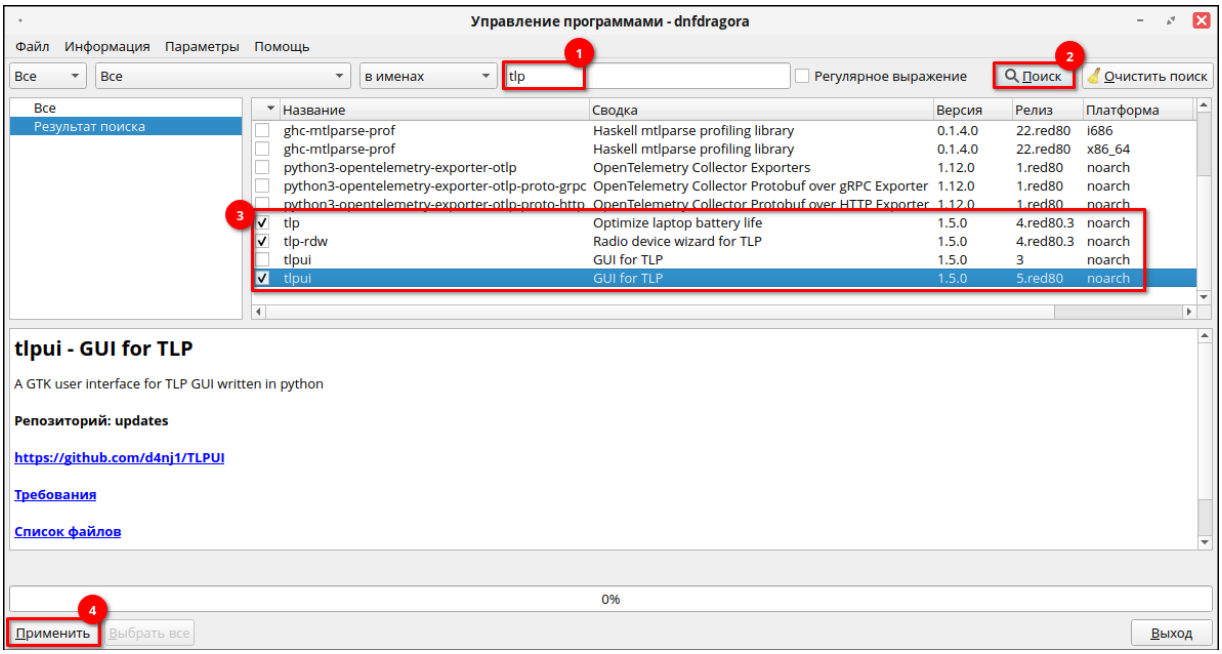
Установка TLP, TLP-RDW, TLPUI

Прежде чем запустить интерфейс **tlpui**, сначала установите необходимые пакеты. Пакеты **tlp** доступны в официальном репозитории РЕД ОС:

- **tlp** – пакет для оптимизации управления энергопотреблением;
- **tlp-rdw** (необязательный) – пакет для управления беспроводными устройствами в **tlp**;
- **tlpui** – графический интерфейс утилиты командной строки **tlp**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимых пакетов по ключевому слову «**tlp**» и отметьте флагом пакеты последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



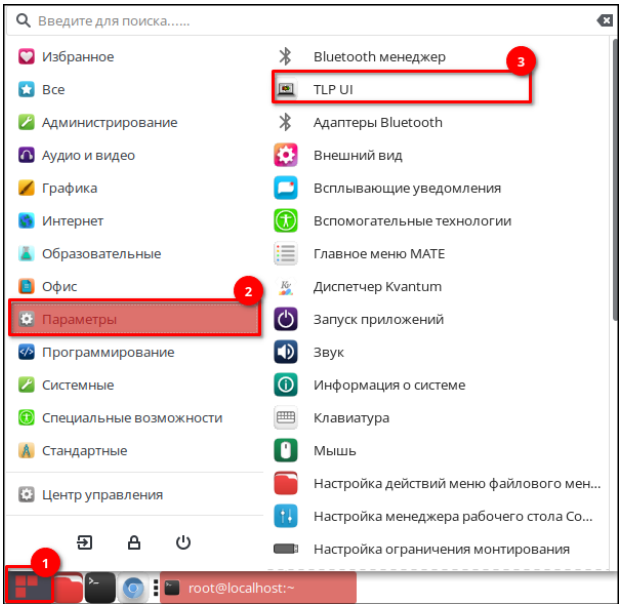
Для установки tlp, tlp-rdw, tlpui через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install tlp tlp-rdw tlpui
```

Работа в графическом интерфейсе

Запуск TLPUI

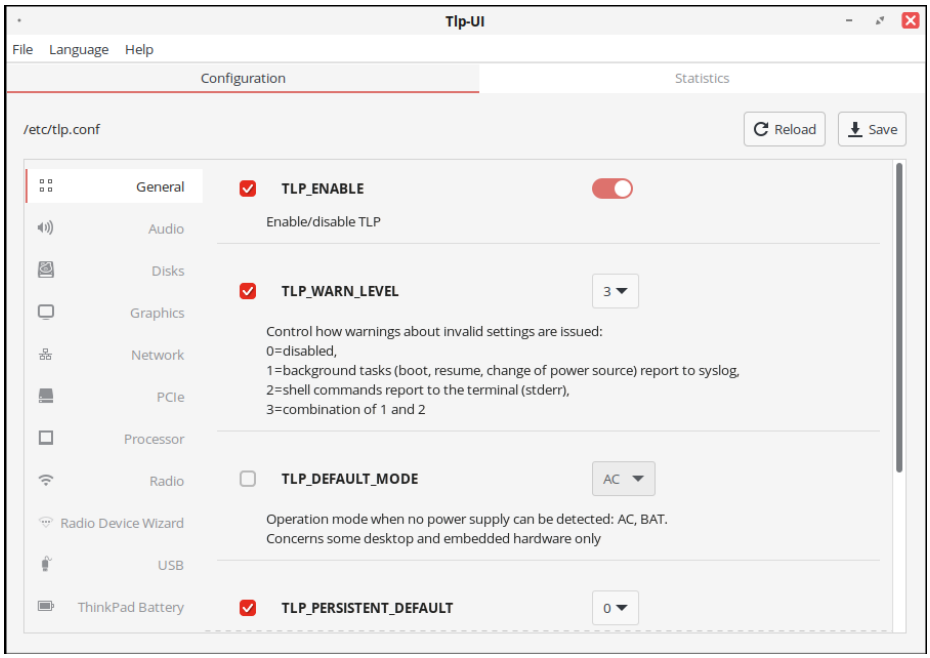
После установки запуск программы доступен из «**Главного меню**» — «**Параметры**» — «**TLP UI**».



Для запуска **tlpui** через терминал введите команду:

```
tlpui
```

Главное окно утилиты выглядит следующим образом:



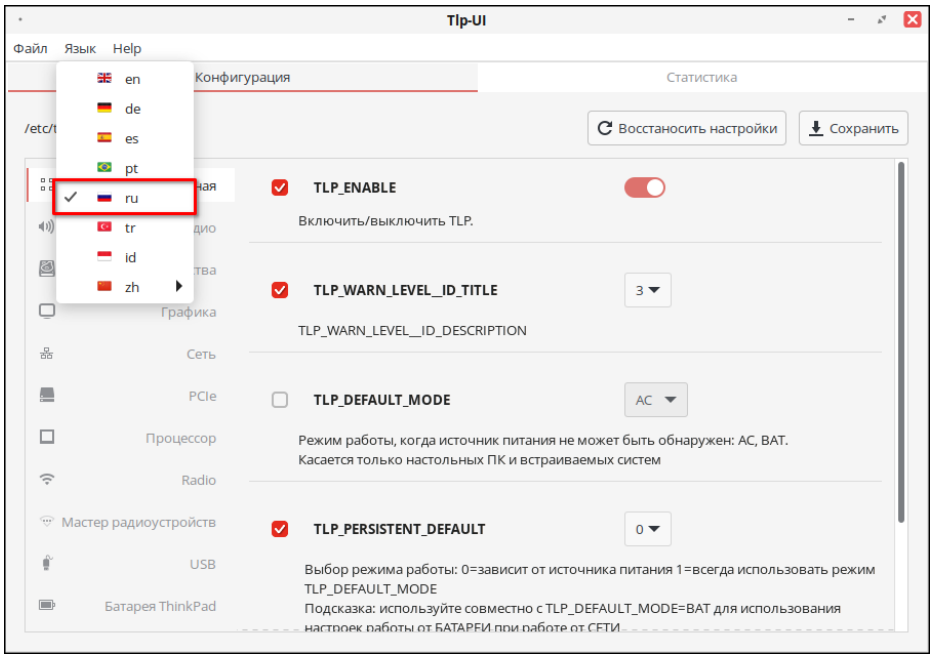
Основные возможности утилиты TLPUI

Основные возможности утилиты **tlpui** включают:

- **графический интерфейс** — обеспечивает удобный доступ к настройкам tlp без необходимости редактирования конфигурационных файлов вручную;
- **настройку параметров процессора** — позволяет регулировать параметры энергосбережения и производительности процессора;
- **управление жесткими дисками** — настройка параметров энергопотребления и производительности для жестких дисков;
- **конфигурацию беспроводных устройств** — позволяет настраивать параметры энергопотребления для Wi-Fi и других беспроводных компонентов;
- **управление сетевыми устройствами** — настройка параметров энергосбережения для сетевых карт и интерфейсов;
- **оптимизацию графических устройств**— позволяет регулировать энергопотребление графических карт;
- **настройку звуковых устройств** — возможность управления параметрами энергопотребления звуковых карт;
- **гибкость конфигурации** — возможность создания и применения различных настроек для различных сценариев использования;
- **мониторинг состояния** — предоставляет информацию о текущем состоянии энергопотребления и параметрах системы.

Смена языка интерфейса

Для смены языка приложения перейдите в меню «**Language**» и в выпадающем списке выберите необходимый язык (в примере выбран русский):



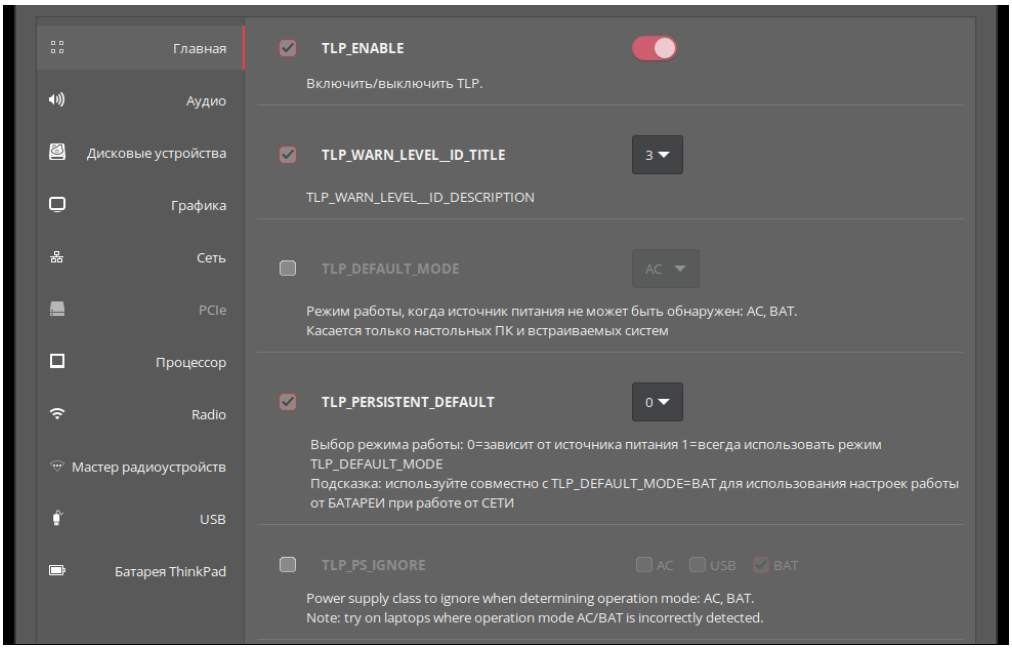
Описание интерфейса TLPUI

Интерфейс **tlpui** состоит из нескольких основных компонентов, которые предоставляют доступ к различным настройкам и параметрам энергосбережения.

Вкладка «Конфигурация»

Главная

На вкладке «**Главная**» интерфейса **tlpui** отображаются основные параметры конфигурации **tlp**, такие как включение/выключение **tlp**, управление предупреждениями, выбор режима работы по умолчанию и игнорирование определённых источников питания.



Параметры:

1. **TLP_ENABLE** — включение/выключение TLP. По умолчанию параметр активен. Для отключения переведите ползунок в положение «выключено». Для применения изменений потребуется перезагрузка.

2. **TLP_WARN_LEVEL_ID_TITLE** — управляет выводом предупреждений о недопустимых настройках.

Возможные значения:

- **0** — отключено;
- **1** — фоновые задачи (загрузка, возобновление работы, смена источника питания) отправляются в системный журнал;
- **2** — команды оболочки сообщают терминалу (stderr);
- **3** — комбинация 1 и 2 (устанавливается по умолчанию).

3. **TLP_DEFAULT_MODE** — определяет режим работы TLP по умолчанию на случай, если источник питания не может быть обнаружен.

Возможные значения:

- **AC** — режим работы от сети;
- **BAT** — режим работы от батареи.

4. **TLP_PERSISTENT_DEFAULT** — выбор режима работы.

Возможные значения:

- **0** — применить настройки в соответствии с фактическим источником питания (по умолчанию);
- **1** — всегда использовать настройки для TLP_DEFAULT_MODE.

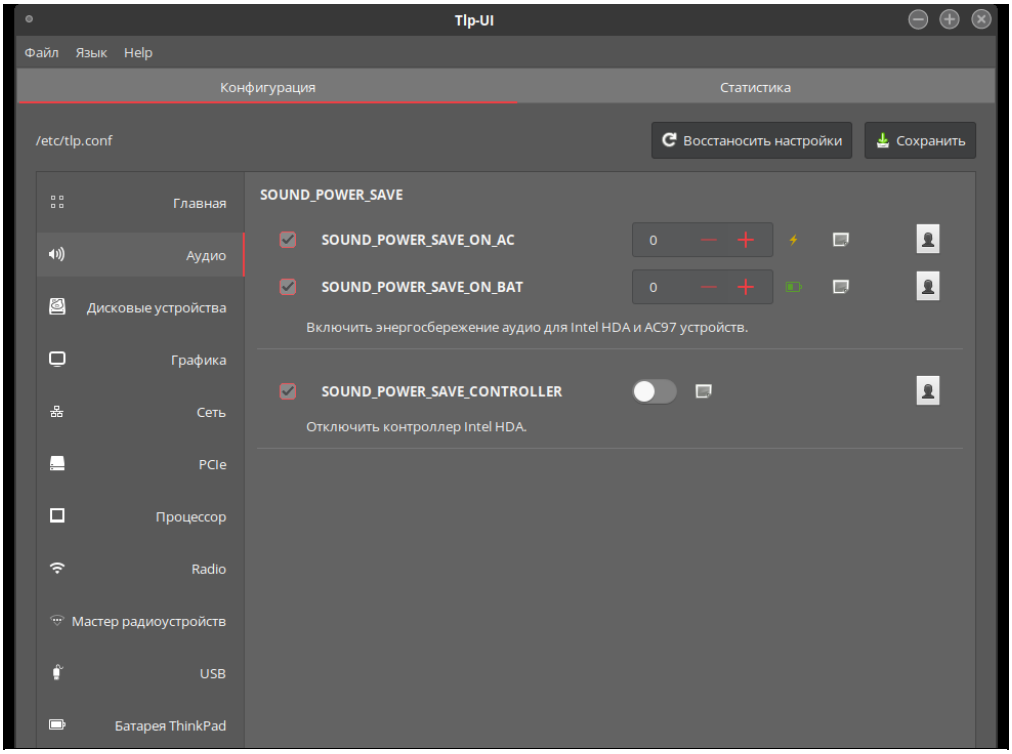
5. **TLP_PS_IGNORE** — класс(ы) источника питания, которые следует игнорировать при определении режима работы.

Возможные значения:

- **AC** — игнорировать сетевой адаптер;
- **BAT** — игнорировать батарею;
- **USB** — игнорировать USB-питание (только для версии 1.4 и выше).

Аудио

Вкладка «**Аудио**» в интерфейсе tlpui позволяет пользователям настроить параметры энергосбережения для звукового оборудования, такие как время ожидания для перехода в режим энергосбережения и выключение звукового контроллера. Эти настройки помогают оптимизировать энергопотребление аудиооборудования на устройстве.



Параметры:

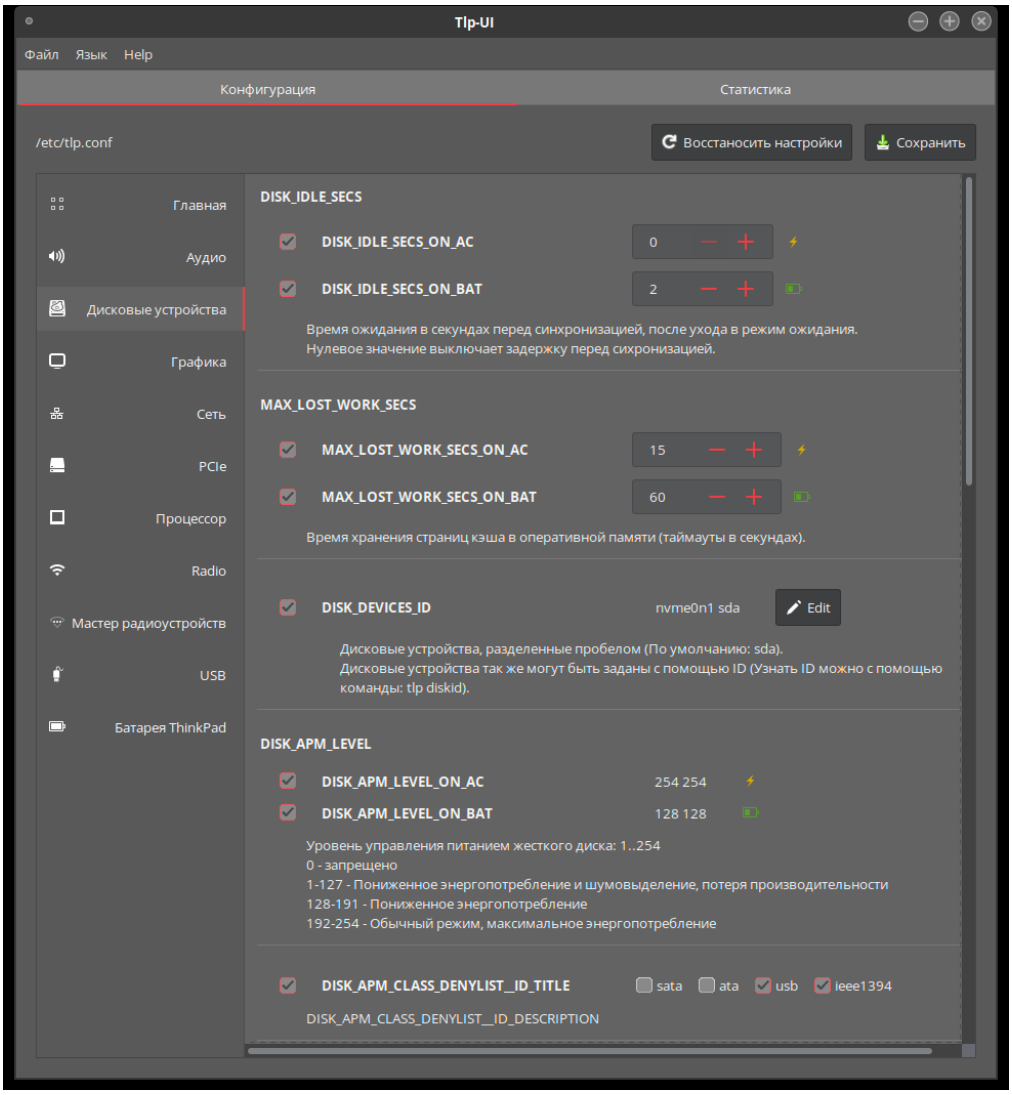
1. **SOUND_POWER_SAVE_ON_AC** — время ожидания (в секундах) для перехода звукового оборудования в режим энергосбережения при работе от сети.

2. **SOUND_POWER_SAVE_ON_BAT** — время ожидания (в секундах) для перехода звукового оборудования в режим энергосбережения при работе от батареи.

3. **SOUND_POWER_SAVE_CONTROLLER** — включить или выключить контроллер вместе со звуковым чипом. Эффективно только когда активировано энергосбережение звука (SOUND_POWER_SAVE_ON_AC/BAT). Поддерживается только HDA.

Дисковые устройства

Вкладка «**Дисковые устройства**» позволяет пользователю настроить параметры энергосбережения для жестких дисков и твердотельных накопителей (SSD). Здесь можно задать различные таймауты, уровни управления питанием и другие параметры для оптимизации энергопотребления дисковых устройств при работе как от сети, так и от батареи.



Параметры:

1. **DISK_IDLE_SECS** — определяет время простоя диска в секундах перед тем, как он будет переведен в режим экономии энергии.

- **DISK_IDLE_SECS_ON_AC** — время ожидания (в секундах) перед синхронизацией после ухода в режим ожидания при работе от сети.
- **DISK_IDLE_SECS_ON_BAT** — время ожидания (в секундах) перед синхронизацией после ухода в режим ожидания при работе от батареи.

Нулевое значение выключает задержку перед синхронизацией.

2 . **MAX_LOST_WORK_SECS** — относится к максимальному времени, в течение которого данные могут быть потеряны в случае внезапного отключения питания или другой неисправности. Этот параметр определяет временной интервал, в течение которого данные могут оставаться в кеше перед записью на диск.

- **MAX_LOST_WORK_SECS_ON_AC** — время хранения страниц кеша в ОЗУ в секундах при работе от сети.
- **MAX_LOST_WORK_SECS_ON_BAT** — время хранения страниц кеша в ОЗУ в секундах при работе от батареи.

3 . **DISK_DEVICES_ID** — определяет идентификаторы устройств жестких дисков, для которых будут применены настройки энергосбережения TLP.

4 . **DISK_APM_LEVEL** — задает уровень управления энергопотреблением для жесткого диска, влияя на баланс между производительностью и энергосбережением.

- **DISK_APM_LEVEL_ON_AC** — уровень управления питанием при работе от сети.
- **DISK_APM_LEVEL_ON_BAT** — уровень управления питанием при работе от батареи.

Возможные значения:

- **1** — максимальное энергосбережение/минимальная производительность (настройка может привести к повышенному износу жесткого диска из-за чрезмерной разгрузки головки чтения-записи);
- **128** — баланс между энергосбережением и износом (стандартная настройка TLP на аккумуляторе);
- **192** — предотвращает чрезмерную разгрузку головок некоторых HDD;
- **254** — минимальное энергосбережение/максимальная производительность (стандартная настройка TLP на переменном токе);

- **255** — отключить APM (не поддерживается некоторыми моделями дисков).

5. **DISK_APM_CLASS_DENYLIST_ID_TITLE** — исключает классы дисков из расширенного управления питанием.

Возможные значения:

- **sata** — для подключения жёстких дисков и SSD;
- **ata** — для подключения дисковых устройств;
- **usb** — для подключения внешних дисков;
- **ieee1394** — для подключения различных устройств, включая внешние диски.

6 . **DISK_SPINDOWN_TIMEOUT** — определяет время простоя в секундах перед тем, как жесткий диск будет переведен в режим остановки вращения для экономии энергии.

- **DISK_SPINDOWN_TIMEOUT_ON_AC** — время ожидания запуска диска при работе от сети;
- **DISK_SPINDOWN_TIMEOUT_ON_BAT** — время ожидания запуска диска при работе от батареи.

Возможные значения:

- **0** — отключить уменьшение оборотов;
- **от 1 до 240** — время ожидания от 5 секунд до 20 минут (шаг в 5 секунд);
- **от 241 до 251** — время ожидания от 30 минут до 5.5 часов (шаг в 30 минут).

7. **DISK_IOSCHED** — устанавливает планировщик ввода-вывода для дисковых устройств.

Возможные значения:

- Планировщики нескольких очередей:
  - **mq-deadline** — многоканальная версия планировщика deadline, обеспечивающая минимальное время отклика для каждой операции ввода-вывода;
  - **none** — отключает планирование, передавая операции ввода-вывода напрямую на устройство без дополнительной очереди;
  - **kyber** — планировщик, оптимизированный для устройств с низкой задержкой, таких как SSD, который учитывает задержку и пропускную способность;
  - **bfq** — предназначен для обеспечения оптимального распределения дискового времени между всеми процессами;
  - **keep** — сохраняет текущий планировщик, не изменяя его.

- Планировщики одной очереди:
  - **deadline** — минимизирует время ожидания операций ввода-вывода, устанавливая жесткие сроки для их выполнения;
  - **cfq** — равномерно распределяет время доступа к диску между процессами;
  - **bfq** — выделяет каждому процессу лимит времени для более эффективного управления и снижения задержки;
  - **noop** — простой планировщик, который полезен для устройств с собственным алгоритмом планирования, например, SSD;
  - **keep** — сохраняет текущий планировщик для систем с одной очередью.

8 . **SATA_LINKPWR** — управляет режимами энергосбережения для SATA-устройств, определяя, как активно будет использоваться энергосбережение на уровне интерфейса SATA.

- **SATA_LINKPWR_ON_AC** — управляет режимом управления питанием для каналов SATA при работе от сети.
- **SATA_LINKPWR_ON_BAT** — устанавливает режим управления питанием для каналов SATA, соединяющих диски и оптические приводы.

Возможные значения:

- **min_power**— максимальное энергосбережение / минимальная производительность;
- **med_power_with_dipm** — лучший баланс между энергосбережением и производительностью (рекомендуется);
- **medium_power** — среднее энергопотребление и производительность;
- **max_performance** — минимальное энергосбережение / максимальная производительность.

9. **SATA_LINKPWR_DENYLIST**_ID_TITLE — позволяет исключить определённые устройства из управления энергопотреблением SATA для предотвращения проблем с совместимостью или производительностью. Диски определяются их хостом, формат — hostX.

10. **AHCI_RUNTIME_PM** — управляет режимами энергосбережения для устройств, подключенных через интерфейс AHCI.

- **AHCI_RUNTIME_PM_ON_AC** — управляет питанием для дисков NVMe, SATA, ATA и USB при работе от сети, предоставляя опцию автоматического выключения бездействующих устройств для экономии энергии.
- **AHCI_RUNTIME_PM_ON_BAT** — контролирует управление питанием для дисков NVMe, SATA, ATA и USB, а также для портов SATA.

Возможные значения:

- **auto** — выключать бездействующие устройства;
- **on** — устройства включены постоянно.

11. **AHCI_RUNTIME_PM_TIMEOUT** — время ожидания в секундах перед приостановкой работы диска или порта. Действует только при активации **AHCI_RUNTIME_PM_ON_AC/BAT**.

12. **BAY_POWEROFF** — позволяет отключать питание для устройств, установленных в сменных отсеках (например, для оптических

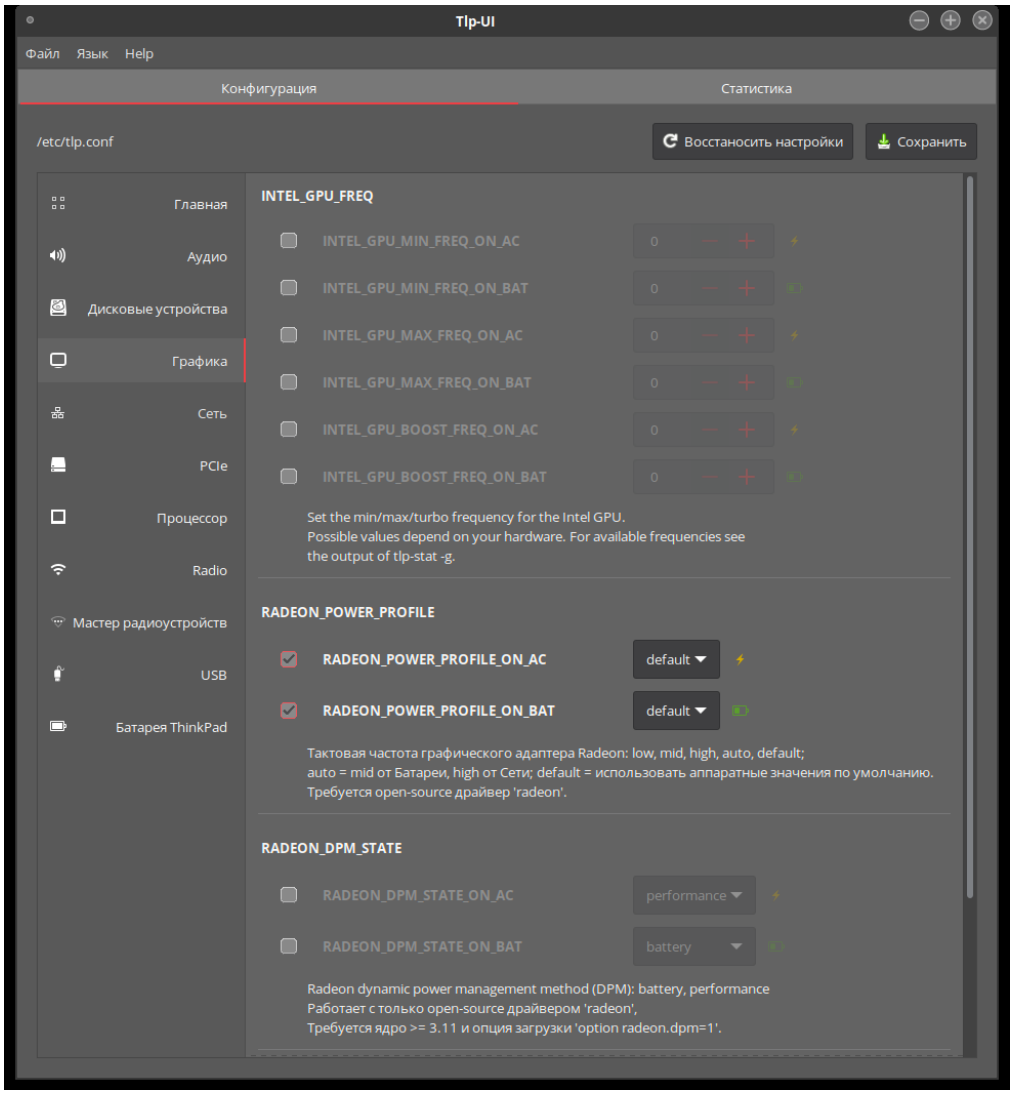
дисководов или дополнительных жестких дисков), когда они не используются, с целью экономии энергии.

- **BAY_POWEROFF_ON_AC** — позволяет управлять выключением оптического привода при работе от сети, что может быть полезным для экономии энергии и увеличения времени автономной работы устройства.
- **BAY_POWEROFF_ON_BAT** — управляет выключением оптического привода при работе от батареи, что помогает экономить заряд батареи и продлевает время автономной работы устройства.

13. **BAY_DEVICE** — отображает устройства оптического привода, для которых могут применяться настройки энергосбережения.

Графика

На вкладке «**Графика**» настраиваются параметры управления энергопотреблением для графических ускорителей, таких как интегрированные графические процессоры Intel и дискретные адаптеры Radeon.



Параметры:

1. **INTEL_GPU_FREQ** — установка минимальной / максимальной / ускоренной частоты для графического процессора Intel. Возможные значения зависят от вашего оборудования.

- **INTEL_GPU_MIN_FREQ_ON_AC** — минимальная частота графического процессора при работе от сети;
- **INTEL_GPU_MIN_FREQ_ON_BAT** — минимальная частота графического процессора при работе от батареи;
- **INTEL_GPU_MAX_FREQ_ON_AC** — максимальная частота графического процессора при работе от сети;
- **INTEL_GPU_MAX_FREQ_ON_BAT** — максимальная частота графического процессора при работе от батареи;
- **INTEL_GPU_BOOST_FREQ_ON_AC** — частота ускорения (Boost) графического процессора при работе от сети;
- **INTEL_GPU_BOOST_FREQ_ON_BAT** — частота ускорения (Boost) графического процессора при работе от батареи.

2. **RADEON_POWER_PROFILE** — управление тактовой частотой графического адаптера Radeon.

- **RADEON_POWER_PROFILE_ON_AC** — устанавливает профиль энергопотребления графического адаптера Radeon при работе от сети;
- **RADEON_POWER_PROFILE_ON_BAT** — устанавливает профиль энергопотребления графического адаптера Radeon при работе от батареи.

Возможные значения:

  - **low** — низкий уровень;

- **mid** — средний уровень;
- **high** — высокий уровень;
- **auto** — использует *средний уровень* при питании от батареи и *высокий уровень* при питании от сети;
- **default** — использует аппаратные настройки по умолчанию.

3. **RADEON_DPM_STATE** — управление Dynamic Power Management (DPM) для графического адаптера Radeon.

- **RADEON_DPM_STATE_ON_AC** — управляет состоянием DPM графического адаптера Radeon при работе от сети.
- **RADEON_DPM_STATE_ON_BAT** — управляет состоянием DPM графического адаптера Radeon при работе от батареи.

Возможные значения:

- **battery** — активируется, когда устройство работает на батарее, в этом режиме система предпринимает шаги для уменьшения энергопотребления;
- **perfomance** — активируется, когда устройство подключено к источнику переменного тока, в этом режиме система может использовать полные ресурсы процессора.

4. **RADEON_DPM_PERF_LEVEL** — установка уровня производительности для Radeon DPM.

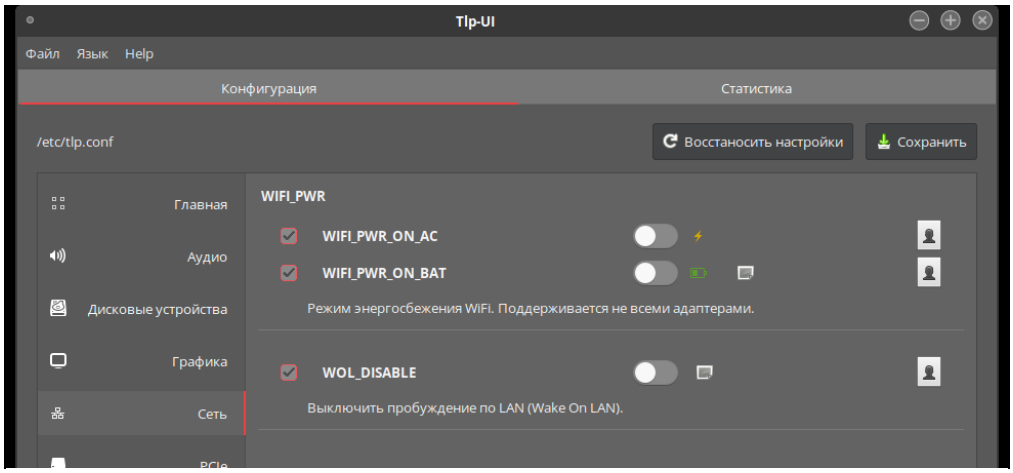
- **RADEON_DPM_PERF_LEVEL_ON_AC** — устанавливает уровень производительности для Radeon DPM при работе от сети;
- **RADEON_DPM_PERF_LEVEL_ON_BAT** — устанавливает уровень производительности для Radeon DPM при работе от батареи.

Возможные значения:

- **auto** — позволяет автоматический контроль уровня производительности графического процессора Radeon;
- **low** — при установке этой настройки графический процессор Radeon будет работать на низком уровне производительности;
- **high** — при выборе этой настройки графический процессор Radeon будет работать на высоком уровне производительности.

Сеть

На вкладке «**Сеть**» предоставлены параметры управления энергопотреблением и функциями, такими как режим энергосбережения Wi-Fi и отключение пробуждения по LAN (Wake-on-LAN), для оптимизации работы сетевых адаптеров.



Параметры:

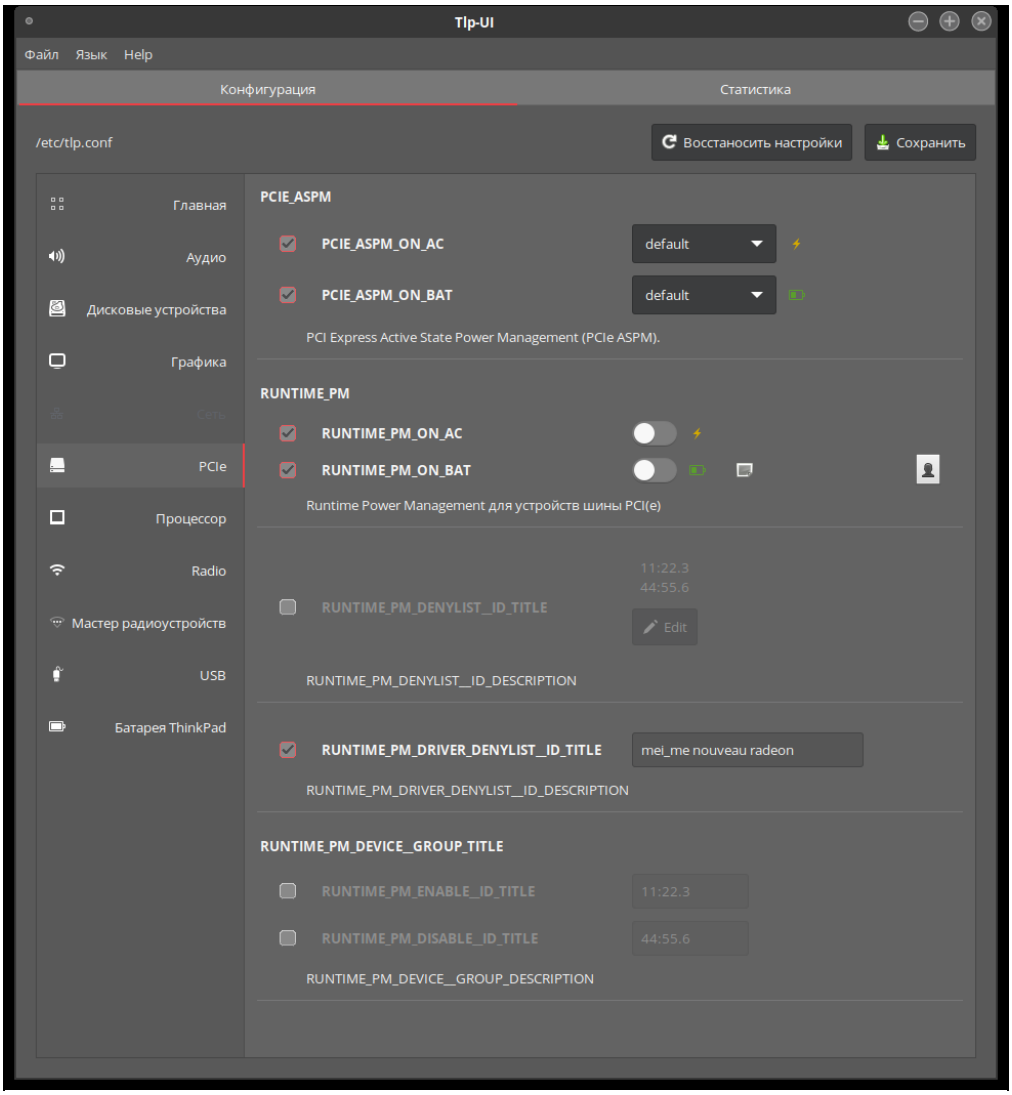
1. **WIFI_PWR** — устанавливает режим энергосбережения Wi-Fi (поддержка адаптера зависит от ядра и драйвера).

- **WIFI_PWR_ON_AC** — определяет уровень мощности Wi-Fi адаптера, когда устройство подключено к источнику питания;
- **WIFI_PWR_ON_BAT** — определяет уровень мощности Wi-Fi адаптера, когда устройство работает от батареи.

2. **WOL_DISABLE** — отключает функцию Wake-on-LAN (WOL), позволяющую удаленно включать компьютер по сети.

PCIe

На вкладке «**PCIe**» настраиваются параметры энергосбережения и управления энергопотреблением для PCIe-устройств, включая режим энергосбережения ASPM, режим управления энергопотреблением во время работы и список исключений для устройств и их драйверов.



Параметры:

1. **PCIE_ASPM** — устанавливает режим энергосбережения (PCIe ASPM).

- **PCIE_ASPM_ON_AC** — устанавливает режим энергосбережения для PCIe ASPM при работе от сети.
- **PCIE_ASPM_ON_BAT** — устанавливает режим энергосбережения для PCIe ASPM при работе от батареи.

Возможные значения:

- **default** — использует настройки по умолчанию, определённые системой или оборудованием;
- **performance** — приоритет производительности;
- **powersave** — снижает потребление энергии;
- **powersupersave** — максимально снижает потребления энергии.

2. **RUNTIME_PM** — управляет энергопотреблением во время работы устройств шины PCI(e).

- **RUNTIME_PM_ON_AC** — активирует управление энергопотреблением в реальном времени при подключении устройства к источнику переменного тока.
- **RUNTIME_PM_ON_BAT** — активирует управление энергопотреблением в реальном времени при работе устройства от батареи.

Возможные значения:

  - **включено** — выключение неактивных устройств;
  - **отключено** — устройства включены постоянно.

3 . **RUNTIME_PM_DENYLIST_ID_TITLE** — представляет список идентификаторов устройств, для которых отключено управление энергопотреблением в реальном времени.

4. **RUNTIME_PM_DRIVER_DENYLIST_ID_TITLE** — представляет список идентификаторов драйверов устройств, для которых отключено управление энергопотреблением в реальном времени.

Возможные значения:

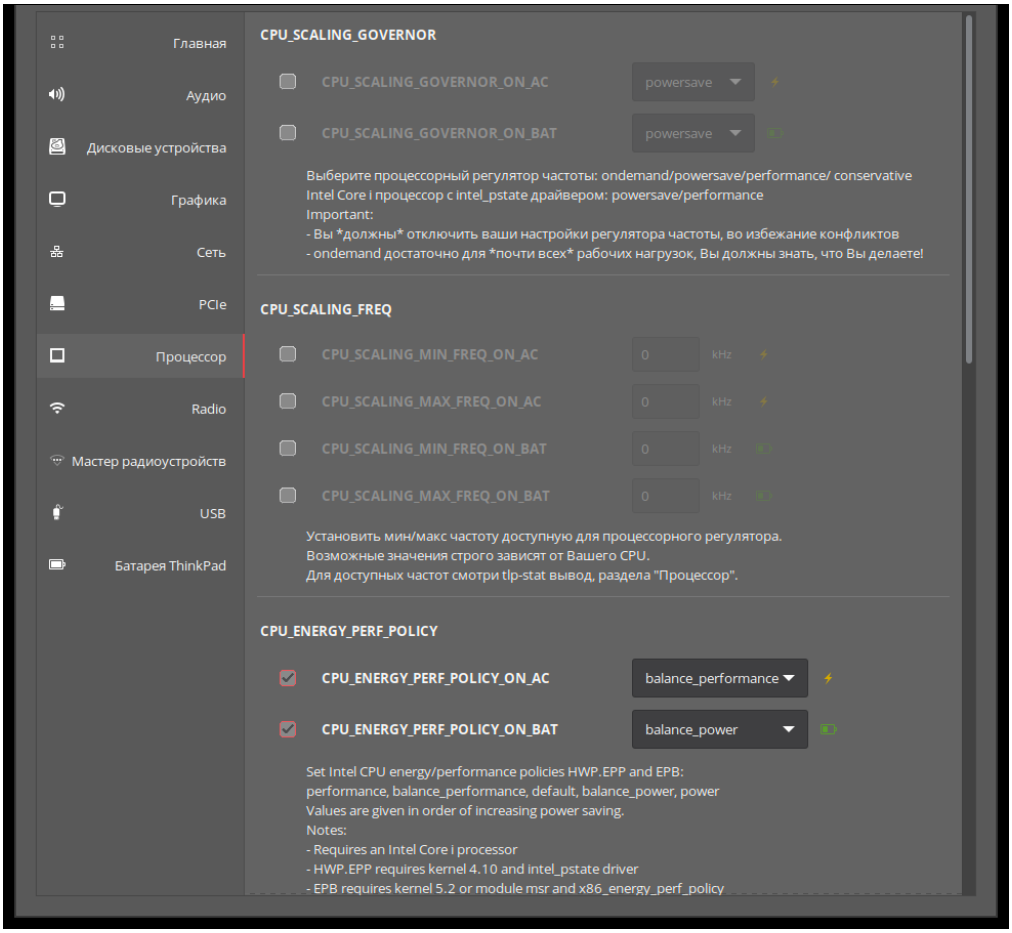
  - **mei_me nouveau radeon** — версия 1.4 и выше;
  - **amdgpu mei_me nouveau nvidia pcieport radeon** — версия 1.3.

5 . **RUNTIME_PM_DEVICE_GROUP_TITLE** — группа устройств, для которых управление энергопотреблением в реальном времени активировано/отключено.

- **RUNTIME_PM_ENABLE_ID_TITLE** — идентификаторы устройств, для которых активировано управление энергопотреблением в реальном времени.
- **RUNTIME_PM_DISABLE_ID_TITLE** — идентификаторы устройств, для которых отключено управление энергопотреблением в реальном времени.

Процессор

На вкладке «**Процессор**» можно настроить параметры управления энергопотреблением для центрального процессора (CPU). Эти параметры могут включать в себя управление частотой процессора, режимом работы ядер, а также другие опции, которые могут повлиять на производительность и энергопотребление процессора.



Параметры:

1. **CPU_SCALING_GOVERNOR** — определяет алгоритм управления частотой процессора в операционной системе.

- **CPU_SCALING_GOVERNOR_ON_AC** — определяет алгоритм управления частотой процессора при подключении устройства к источнику переменного тока.
- **CPU_SCALING_GOVERNOR_ON_BAT** — определяет алгоритм управления частотой процессора при работе устройства от батареи.

Возможные значения:

  - **ondemand** — алгоритм управления частотой процессора, который динамически регулирует частоту процессора в зависимости от нагрузки на систему;
  - **powersave** — алгоритм управления частотой процессора, который старается минимизировать энергопотребление, даже за счет производительности;
  - **performance** — алгоритм управления частотой процессора, который устанавливает максимальную частоту процессора для обеспечения максимальной производительности;
  - **conservative** — алгоритм управления частотой процессора, который старается сохранить высокую производительность, но при этом избегает частых переключений частоты для экономии энергии;
  - **schedutil** — алгоритм управления частотой процессора, который является адаптивным и использует информацию от планировщика задач для регулировки частоты процессора с целью обеспечения баланса между производительностью и энергопотреблением.

2 . **CPU_SCALING_MIN_FREQ** — определяет минимальную частоту процессора, которая может быть установлена в системе при использовании алгоритмов управления частотой процессора.

- **CPU_SCALING_MIN_FREQ_ON_AC** — минимальная частота процессора при подключении устройства к источнику переменного тока.

- **CPU_SCALING_MAX_FREQ_ON_AC** — максимальная частота процессора при подключении устройства к источнику переменного тока.
- **CPU_SCALING_MIN_FREQ_ON_BAT** — минимальная частота процессора при работе устройства от батареи.
- **CPU_SCALING_MAX_FREQ_ON_BAT** — максимальная частота процессора при работе устройства от батареи.

3. **CPU_ENERGY_PERF_POLICY** — управляет энергоэффективностью и производительностью процессора.

- **CPU_ENERGY_PERF_POLICY_ON_AC** — определяет политику энергоэффективности и производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_ENERGY_PERF_POLICY_ON_BAT** — определяет политику энергоэффективности и производительности процессора при работе устройства от батареи.

Возможные значения:

  - **default** — использует стандартные настройки производительности и энергопотребления, предоставляемые операционной системой;
  - **performance** — обеспечивает максимальную производительность процессора, игнорируя энергосберегающие меры;
  - **balance_performance** — обеспечивает баланс между производительностью и энергосбережением, уделяя приоритет производительности;
  - **balance_power** — обеспечивает баланс между производительностью и энергосбережением, уделяя приоритет энергосбережению;
  - **power** — нацелен на минимизацию энергопотребления.

4. **CPU_PERF** — минимальный уровень производительности процессора. ***Возможные значения:*** от 0 до 100%.

- **CPU_MIN_PERF_ON_AC** — минимальный уровень производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_MAX_PERF_ON_AC** — максимальный уровень производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_MIN_PERF_ON_BAT** — минимальный уровень производительности процессора при работе устройства от батареи.
- **CPU_MAX_PERF_ON_BAT** — максимальный уровень производительности процессора при работе устройства от батареи.

5. **CPU_BOOST** — управляет возможностью процессора использовать режимы повышенной производительности.

- **CPU_BOOST_ON_AC** — включает или отключает режимы повышенной производительности процессора при подключении устройства к источнику переменного тока.
- **CPU_BOOST_ON_BAT** — включает или отключает режимы повышенной производительности процессора при работе устройства от батареи.

6. **CPU_HWP_DYN_BOOST_GROUP_TITLE** — устанавливает настройки для динамического ускорения процессора Intel HWP.

- **CPU_HWP_DYN_BOOST_ON_AC** — включает или отключает динамическое ускорение HWP при подключении устройства к источнику переменного тока.
- **CPU_HWP_DYN_BOOST_ON_BAT** — включает или отключает динамическое ускорение HWP при работе устройства от батареи.

7 . **SCHED_POWERSAVE** — управляет настройками энергосбережения планировщика задач, влияя на распределение задач для минимизации энергопотребления.

- **SCHED_POWERSAVE_ON_AC** — активирует или деактивирует режим энергосбережения планировщика задач при подключении устройства к источнику переменного тока.
- **SCHED_POWERSAVE_ON_BAT** — активирует или деактивирует режим энергосбережения планировщика задач при работе устройства от батареи.

8. **NMI_WATCHDOG** — механизм мониторинга и диагностики, который помогает обнаруживать и реагировать на зависания системы и другие критические ошибки.

9.**PLATFORM_PROFILE_GROUP_TITLE** — устанавливает настройки, касающиеся платформенного профиля, который определяет общие параметры производительности и энергосбережения для устройства.

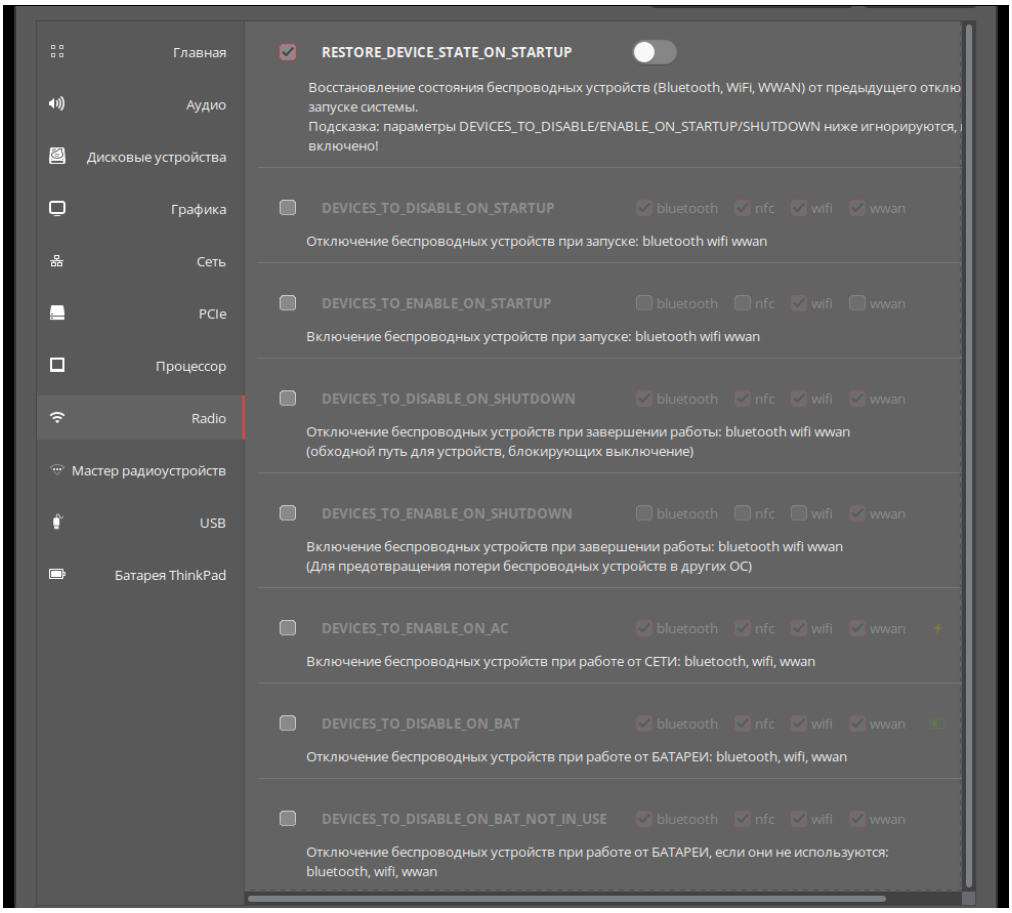
- **PLATFORM_PROFILE_ON_AC** — устанавливает платформенный профиль при подключении устройства к источнику переменного тока.
- **PLATFORM_PROFILE_ON_BAT** — устанавливает платформенный профиль при работе устройства от батареи.

Возможные значения в порядке увеличения энергосбережения:

  - **performance** — обеспечивает максимальную производительность процессора;
  - **balanced** — обеспечивает баланс между производительностью и энергосбережением;
  - **low_power** — обеспечивает максимальное энергосбережение.

Радио

На вкладке «**Радио**» настраиваются параметры энергосбережения для беспроводных устройств, такие как Bluetooth и Wi-Fi. Эти параметры включают управление режимами энергосбережения для беспроводных устройств при работе от сети и от батареи, что помогает оптимизировать энергопотребление и продолжительность работы вашего устройства в различных условиях использования.



Параметры:

1 . **RESTORE_DEVICE_STATE_ON_STARTUP** — восстанавливает состояние беспроводных устройств до настроек, существовавших до выключения или перезагрузки системы.

2 . **DEVICES_TO_DISABLE_ON_STARTUP** — определяет устройства, которые должны быть отключены при запуске системы для экономии энергии или других целей.

3. **DEVICES_TO_ENABLE_ON_STARTUP** — определяет устройства, которые должны быть включены при запуске системы.

4. **DEVICES_TO_DISABLE_ON_SHUTDOWN** — определяет устройства, которые должны быть отключены при выключении системы.

5. **DEVICES_TO_ENABLE_ON_SHUTDOWN** — определяет устройства, которые должны быть включены при выключении системы.

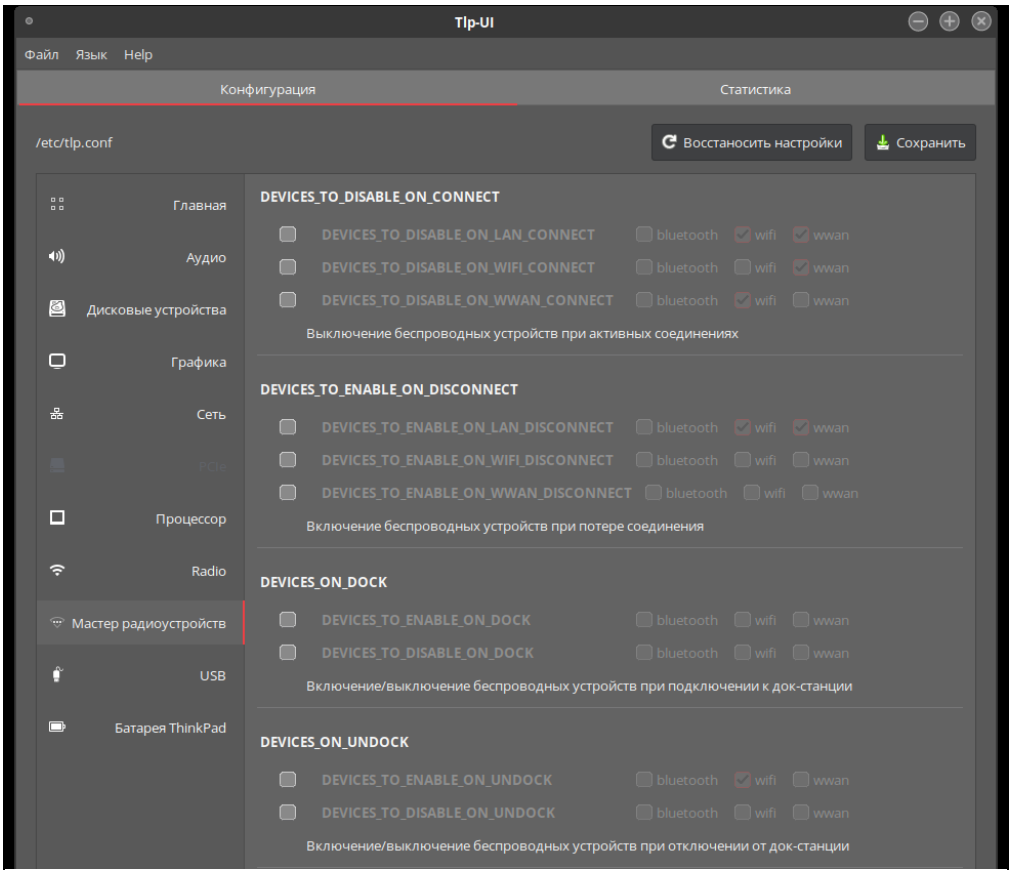
6.**DEVICES_TO_ENABLE_ON_AC** — определяет устройства, которые должны быть включены при подключении устройства к источнику переменного тока (AC).

7. **DEVICES_TO_DISABLE_ON_BAT** — определяет устройства, которые должны быть отключены при работе устройства от батареи.

8. **DEVICES_TO_DISABLE_ON_BAT_NOT_IN_USE** — определяет устройства, которые должны быть отключены при работе устройства от батареи, когда оно не используется.

Мастер радиоустройств

На вкладке «**Мастер радиоустройств**» настраиваются параметры энергосбережения для беспроводных устройств. Эти параметры включают управление режимами энергосбережения для беспроводных устройств при работе от сети и от батареи, что позволяет оптимизировать энергопотребление и продолжительность работы устройства в различных сценариях использования.



Параметры:

1 . **DEVICES_TO_DISABLE_ON_CONNECT** — при установленном соединении LAN, Wi-Fi или WWAN беспроводные устройства отключаются.

- **DEVICES_TO_DISABLE_ON_LAN_CONNECT** — устройства, которые необходимо отключить при подключении к проводной сети.
- **DEVICES_TO_DISABLE_ON_WIFI_CONNECT** — устройства, которые необходимо отключить при подключении к Wi-Fi сети.
- **DEVICES_TO_DISABLE_ON_WWAN_CONNECT** — устройства, которые необходимо отключить при подключении к мобильной сети.

2. **DEVICES_TO_ENABLE_ON_DISCONNECT** — при отключении соединения LAN, Wi-Fi, WWAN беспроводные устройства активируются.

- **DEVICES_TO_ENABLE_ON_LAN_DISCONNECT** — устройства, которые необходимо включить при отключении от проводной сети.
- **DEVICES_TO_ENABLE_ON_WIFI_DISCONNECT** — устройства, которые необходимо включить при отключении от Wi-Fi сети.
- **DEVICES_TO_ENABLE_ON_WWAN_DISCONNECT** — устройства, которые необходимо включить при отключении от мобильной сети.

3. **DEVICES_ON_DOCK** — устройства, которые должны быть активны при подключении к док-станции.

- **DEVICES_TO_ENABLE_ON_DOCK** — устройства, которые необходимо включить при подключении к док-станции.
- **DEVICES_TO_DISABLE_ON_DOCK** — устройства, которые необходимо отключить при подключении к док-станции.

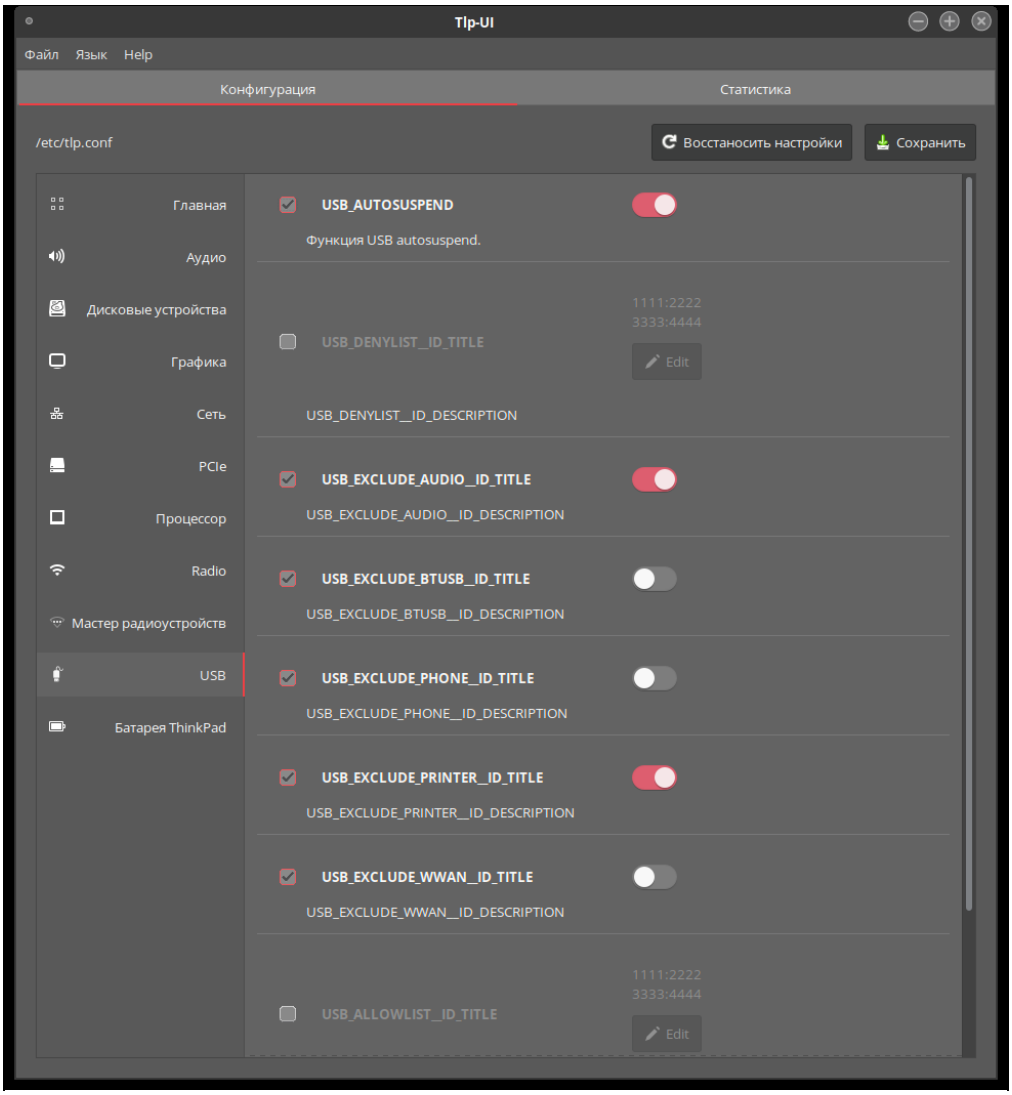
4. **DEVICES_ON_UNDOCK** — устройства, которые должны быть активны при отключении от док-станции.

- **DEVICES_TO_ENABLE_ON_UNDOCK** — устройства, которые необходимо включить при отключении от док-станции.
- **DEVICES_TO_DISABLE_ON_UNDOCK** — устройства, которые необходимо отключить при отключении от док-станции.

Беспроводные устройства: bluetooth, wifi, wwan.

USB

На вкладке «**USB**» настраиваются параметры управления энергопотреблением для портов USB и связанных с ними устройств. Здесь можно установить режимы энергосбережения, такие как отключение USB-портов или управление энергопотреблением подключенных устройств. Это позволяет оптимизировать энергопотребление и продолжительность работы устройства в различных сценариях использования.



Параметры:

1 . **USB_AUTOSUSPEND** — отвечает за автоматическое приостановление работы USB-устройств для экономии энергии. Когда эта функция активирована, USB-устройства переходят в режим низкого энергопотребления после определенного времени бездействия.

2. **USB_DENYLIST** — позволяет указать список USB-устройств, для которых автоматическое приостановление работы будет отключено. Полезно для устройств, испытывающих трудности с выходом из режима автозависания.

3 . **USB_EXCLUDE_AUDIO** — предназначена для исключения аудиоустройств из автоматического приостановления работы. При активировании этой опции USB-аудиоустройства остаются активными и не переходят в режим низкого энергопотребления, обеспечивая постоянную доступность звуковых функций.

4. **USB_EXCLUDE_BTUSB** — исключает Bluetooth-устройства из автоматического приостановления работы, обеспечивая их постоянную активность.

5 . **USB_EXCLUDE_PHONE** — исключает смартфоны из автоматического приостановления работы, обеспечивая их постоянную активность.

6. **USB_EXCLUDE_PRINTER** — исключает принтеры из автоматического приостановления работы, обеспечивая их постоянную активность.

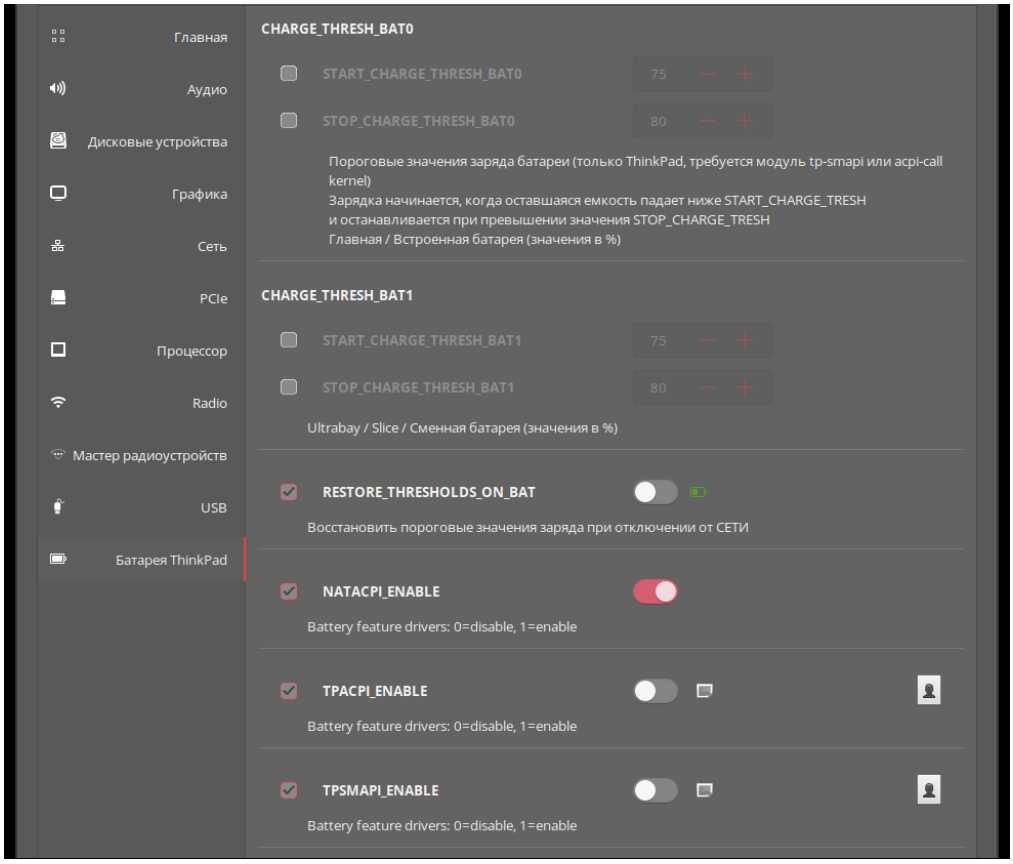
7. **USB_EXCLUDE_WWAN** — исключает WWAN (беспроводные широкополосные сети) устройства из автоматического приостановления работы, обеспечивая их постоянную активность.

8 . **USB_ALLOWLIST** — позволяет указать список USB-устройств, которые будут исключены из автоматического приостановления работы, обеспечивая их постоянную активность.

9 . **USB_AUTOSUSPEND_DISABLE_ON_SHUTDOWN** — отвечает за отключение автоматического приостановления работы для USB-устройств перед выключением системы.

Батарея ThinkPad

Вкладка «**Батарея ThinkPad**» предоставляет возможность управления различными параметрами работы батареи ThinkPad. В этой вкладке можно настроить различные параметры зарядки, разрядки и энергосбережения батареи. Например, пользователь может установить пороги заряда, определить условия начала и прекращения заряда, а также настроить другие параметры, влияющие на производительность и долговечность батареи.



1. **CHARGE_THRESH_BAT0** — задает пороговый уровень заряда для аккумулятора.

- **START_CHARGE_THRESH_BAT0** — определяет пороговый уровень заряда, при достижении которого начинается заряд аккумулятора.
- **STOP_CHARGE_THRESH_BAT0** — определяет пороговый уровень заряда, при достижении которого происходит прекращение заряда аккумулятора.

2. **CHARGE_THRESH_BAT1** — позволяет задать пороговый уровень заряда для сменной батареи в ноутбуках Lenovo ThinkPad, если они поддерживают две батареи.

- **START_CHARGE_THRESH_BAT1** — устанавливает порог заряда, при достижении которого начинается заряд сменной батареи.
- **STOP_CHARGE_THRESH_BAT1** — устанавливает порог заряда, при достижении которого прекращается заряд сменной батареи.

3. **RESTORE_THRESHOLDS_ON_BAT** — восстановление настроенных порогов заряда при отключении от сети.

4. **NATACPI_ENABLE** — включает поддержку ACPI для управления зарядом батареи.

5. **TPACPI_ENABLE** — включает поддержку ACPI для управления различными функциями ThinkPad.

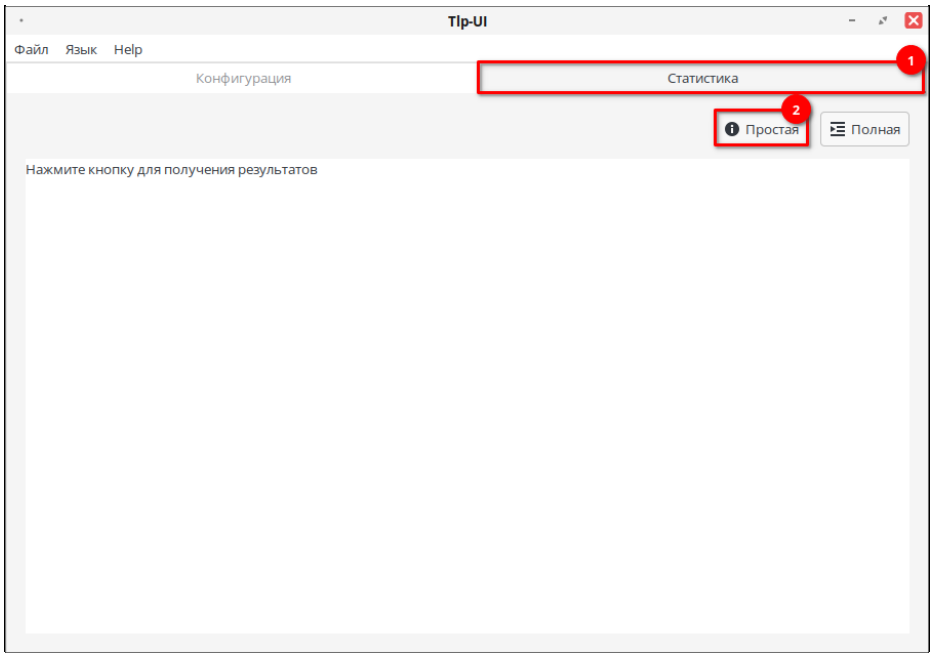
6.**TPSMAPI_ENABLE** — включает поддержку SMAPI для управления различными функциями батареи ThinkPad.

Вкладка «Статистика»

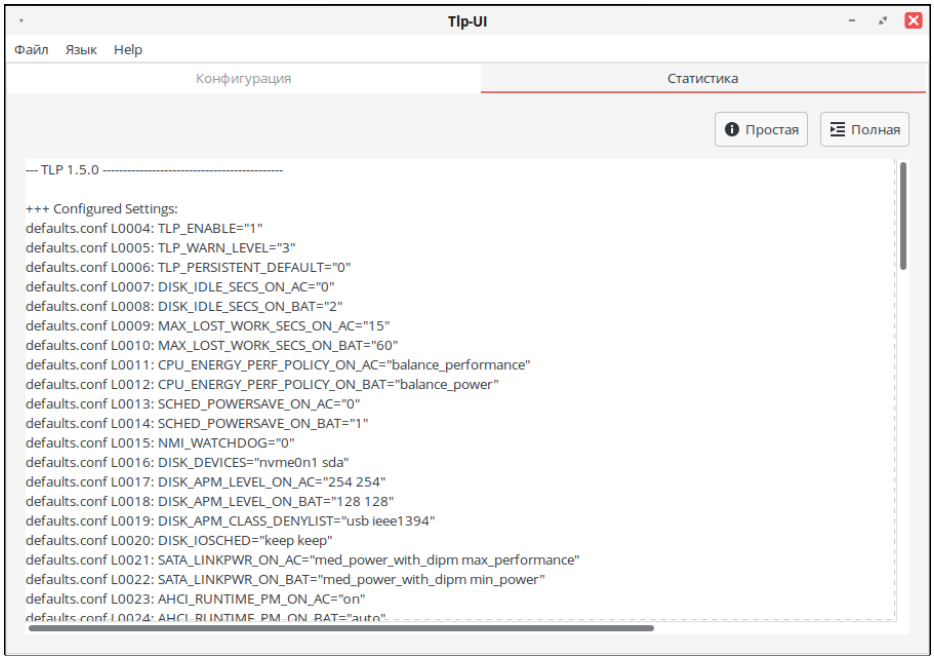
Вкладка "**Статистика**" предоставляет пользователю информацию о статистике использования энергии на компьютере. Здесь отображаются данные о потреблении энергии, времени работы от аккумулятора, времени работы от сети и другие параметры, которые помогают отслеживать и анализировать энергопотребление устройства. Это позволяет пользователям лучше понимать, как и когда их устройство использует энергию, и оптимизировать его работу для экономии энергии и увеличения времени автономной работы.

Просмотр статистики

Для просмотра статистических данных откройте вкладку «**Статистика**» (1) и нажмите кнопку «**Простая**» (2).



После этого будут отражены данные о системе:



Работа в терминале

Синтаксис TLP

Утилита tlp доступна для запуска через терминал при помощи команды следующего вида:

```
tlp [<команды>] [<параметры>] [--параметры_конфигурации=<значение> ... ]
```

Команды TLP

Основные команды утилиты:

- **start** — инициализировать tlp и применить настройки энергосбережения в соответствии с фактическим источником питания, используется для применения измененной конфигурации или выхода из ручного режима.
- **bat, true** — применить профиль настроек батареи и перейти в ручной режим.
- **ac** — применить профиль настроек переменного тока и перейти в ручной режим. Ручной режим означает, что изменения в источнике питания будут игнорироваться до следующей перезагрузки или запуска tlp для возобновления автоматического режима.
- **false** — включить автоматическую приостановку для всех USB—устройств, за исключением тех, которые исключены по

умолчанию или в конфигурации.
- **bayoff** — выключить оптический привод в UltraBay/MediaBay.
- **setcharge** — временно изменить пороговые значения заряда батареи. Если оборудование поддерживает только пороговое значение stop, установить начальное значение равным 0. Настроенные пороговые значения заряда будут восстановлены при следующей загрузке или при повторном использовании tlp setcharge, но без пороговых параметров. **Синтаксис команды имеет вид:** `setcharge [<START_CHARGE_THRESH> <STOP_CHARGE_THRESH>] [BAT0|BAT1|BAT<x>|CMB0]`.
- **fullcharge** — предназначена для зарядки аккумулятора до полной емкости путем временного применения предустановок производителя к пороговым значениям заряда. Настроенные пороговые значения заряда будут восстановлены при следующей загрузке или с помощью tlp setcharge без аргументов threshold (уровень заряда). Команда предназначена для временного увеличения заряда аккумулятора до максимальной емкости, но не изменяет стандартных настроек порогов заряда. **Синтаксис команды имеет вид:** `fullcharge [BAT0|BAT1|BATx|CMB0]`.
- **chargeonce** (только для ThinkPads) — зарядить аккумулятор до порогового значения stop charge один раз. Для этого необходимо временно снять пороговое значение start charge. Настроенное пороговое значение start charge будет восстановлено при следующей загрузке или с помощью tlp setcharge без аргументов. **Синтаксис команды имеет вид:** `chargeonce [BAT0|BAT1]`.
- **discharge** (только для ThinkPads) — принудительно полностью разрядить аккумулятор. **Синтаксис команды имеет вид:** `discharge [BAT0|BAT1]`.
- **recalibrate** (только для ThinkPads) — повторная калибровка аккумулятора: полностью разрядить аккумулятор и зарядить его до 100%. Для этого к пороговым значениям временно применяются настройки производителя. Настроенные пороговые значения будут восстановлены при следующей загрузке или с помощью tlp setcharge. **Синтаксис команды имеет вид:** `recalibrate [BAT0|BAT1]`.
- **diskid** — отобразить идентификаторы дисков для настройки.

Параметры TLP

Основные параметры утилиты:

- **-b, --battery** — проверка состояния заряда и другой информации о батарее;
- **-c, --config** — проверка состояния настроек конфигурации;
- **-d, --disk** — проверка состояния диска;
- **-e, --pcie** — проверка состояния шины PCI Express;
- **-g, --graphics** — проверка состояния графической подсистемы;
- **-p, --processor** — проверка состояния процессора;
- **-r, --rfkill** — проверка состояния переключателей аппаратного блокирования;
- **-s, --system** — проверка состояния системы;
- **-t, --temp** — проверка состояния температуры;
- **-u, --usb** — проверка состояния устройств USB;
- **-w, --warn** — проверка состояния предупреждений;
- **-v, --verbose** — вывод более подробной информации;
- **--cdiff** — проверка состояния различий в конфигурации;
- **--pev** — проверка состояния окружения Power and Environmental Monitoring;
- **-P, --psup** — проверка состояния источника питания;
- **-T, --trace** — проверка состояния трассировки;
- **--udev** — проверка состояния управления устройствами.

Параметры конфигурации:

Добавьте параметры конфигурации, чтобы переопределить конфигурацию системы только для единственного вызова программы. Впоследствии они не сохраняются.

Для ноутбуков с несколькими аккумуляторами выбор осуществляется следующим образом:

- **BAT0** — основной или встроенный аккумулятор;
- **BAT1** — дополнительный или сменный аккумулятор.

Примеры использования утилиты

1. Запустить TLP. После установки tlp запускается автоматически. Если требуется вручную запустить tlp, можно использовать команду:

```
sudo tlp start
```

Также можно использовать эту команду для применения изменений после редактирования конфигурации.

2. Применить режим автоматической приостановки для всех подключенных USB-устройств, кроме тех, которые исключены по умолчанию или в конфигурации:

```
tlp usb
```

3. Выключить оптический привод в MediaBay/Ultrabay:

```
tlp bayoff
```

4. Временно изменить пороговые значения заряда аккумулятора:

```
sudo tlp setcharge [<START_CHARGE_THRESH> <STOP_CHARGE_THRESH>] [BAT0|BAT1|BAT<x>|CMB0]
```

Пример:

```
tlp setcharge 70 90 BAT0
```

В этом примере применяются пороговые значения 70/90% к батарее BAT0. Tlp setcharge изменяет пороговые значения заряда только временно. Чтобы изменения стали постоянными, необходимо активировать или изменить соответствующие настройки в файле конфигурации.

5. Зарядить аккумулятор до полной емкости:

```
tlp fullcharge [BAT0|BAT1|BAT<x>|CMB0|CMB1]
```

Пример:

```
tlp fullcharge BAT1
```

Заряжает аккумулятор BAT1 до полной емкости.

6. Зарядить аккумулятор до порога остановки заряда один раз (только ThinkPad):

```
tlp chargeonce [BAT0|BAT1]
```

Это достигается путем временного поднятия порога стартового заряда. Настроенный порог стартового заряда будет восстановлен при следующей загрузке или с помощью tlp setcharge без аргументов порога.

Пример:

```
tlp chargeonce BAT0
```

7. Для просмотра текущих настроек TLP можно выполнить команду:

```
tlp-stat
```

8. Проверить состояние заряда и другую информацию о батарее:

```
tlp-stat -b
```

9. Проверить состояние системы:

```
tlp-stat -s
```

10. Проверить все параметры TLP:

```
tlp-stat -p
```

TLP-RDW

Синтаксис утилиты **tlp-rdw** имеет следующий вид:

```
tlp-rdw [<команды>]
```

Основные команды утилиты **tlp-rdw:**

- **disable** — отключить управление беспроводными устройствами;
- **enable** — включить управление беспроводными устройствами;
- **<none>** — использование команды без аргументов отображает фактическое состояние.

Пример использования:

Для отключения параметра управления энергопотреблением в режиме реального времени введите команду:

```
tlp-rdw disable
```

Получение технической информации о ПК

inxi
lshw
lshw-gui
hwinfo
hddtemp
hw-probe
Стандартные средства и команды операционной системы РЕД ОС

Для того, чтобы посмотреть технические данные ПК, на котором установлена операционная система РЕД ОС, можно воспользоваться специализированными программами.

Вы можете подробнее ознакомиться с утилитами для получения технической информации о ПК, просмотрев наши обучающие видео:

- на **RuTube** — Информация, мониторинг и тестирование системы;
- в **Яндекс.Дзен** — Информация, мониторинг и тестирование системы;
- в **VK Видео** — Информация, мониторинг и тестирование системы.

На наших каналах вы также сможете найти много другой полезной информации.

inxi

Инструмент для командной строки, который позволяет отображать информацию о системе и об аппаратной части компьютера.

Установка.

```
sudo dnf install inxi
```

Для вывода полной информации, в консоли вводим:

```
inxi -F
```

Ключ -F даёт наиболее полный вывод данных по системе.

Ключ -b выдаёт общую информацию, является упрощённым аналогом предыдущей команды.

Однако, ключи -F и -b не выводят абсолютно всех данных. Да и не всегда они необходимы. Следующие ключи дают информацию по конкретным областям:

```
-h Справка;
-A Показать аудио/звуковую информацию карты;
-C Показать данные о процессоре;
-d Отображает данные накопителей на оптических дисках;
-D Показывает полную информацию о жестком диске;
-f Показать все флаги центрального процессора;
-G Показать информацию о графической карте;
-i Показывает WAN IP-адрес, локальные интерфейсы, наиболее полная;
-I Показать информацию: процессы, время бесперебойной работы, память;
-m Показывает память (RAM). Результаты вывода этого ключа не выдаются при использовании ключей -b или -F;
-o Просмотреть информацию о несмонтированном разделе (включая UUID и маркировки если таковые имеются);
-S Информация о системе: имя хоста, ядро, окружение рабочего стола, дистрибутив.
-u Показать разделы и их UUID.
```

Например для просмотра информации по видеокарте:

```
inxi -G
```

Получим вывод:

```
Graphics:
Device-1: VMware SVGA II Adapter driver: vmwgfx v: 2.15.0.0
Display: x11 server: X.Org 1.19.5 driver: vmware
unloaded: fbdev,modesetting,vesa resolution: 1280×960~60Hz
OpenGL: renderer: llvmpipe (LLVM 5.0 128 bits) v: 2.1 Mesa 17.3.6
```

lshw

Ещё одна консольная утилита для просмотра информации о характеристиках компьютера.

Установка.

```
sudo dnf install lshw
```

Данная утилита требует для запуска права суперпользователя:

```
sudo lshw
```

Используя следующие параметры, можно выбрать формат вывода:

```
-html Вывод аппаратной конфигурации в формате HTML;
-xml Вывод аппаратной конфигурации в формате XML;
-short Отображает только основную информацию;
-c CLASS Показывает только определенный класс оборудования (memory, disk, network, cpu и т.п.).
```

Пример запуска утилиты для получения основной информации о системе:

```
sudo lshw -short
```

Результат работы:

```
H/W path Device Class Description
=====================================================
system VirtualBox
/0 bus VirtualBox
/0/0 memory 128KiB BIOS
/0/1 memory 1983MiB System memory
/0/2 processor Intel® Pentium® CPU G4560 @ 3.50GHz
/0/100 bridge 440FX — 82441FX PMC [Natoma]
/0/100/1 bridge 82371SB PIIX3 ISA [Natoma/Triton II]
/0/100/1.1 scsi0 storage 82371AB/EB/MB PIIX4 IDE
/0/100/1.1/0 /dev/sda disk 12GB VBOX HARDDISK
/0/100/1.1/0/1 /dev/sda1 volume 1GiB EXT4 volume
/0/100/1.1/0/2 /dev/sda2 volume 10GiB Linux LVM Physical Volume partition
/0/100/1.1/1 /dev/cdrom disk DVD reader
/0/100/2 display SVGA II Adapter
/0/100/3 enp0s3 network 82540EM Gigabit Ethernet Controller
/0/100/4 generic VirtualBox Guest Service
/0/100/5 multimedia 82801AA AC’97 Audio Controller
/0/100/6 bus KeyLargo/Intrepid USB
/0/100/6/1 usb1 bus OHCI PCI host controller
/0/100/6/1/1 input USB Tablet
/0/100/7 bridge 82371AB/EB/MB PIIX4 ACPI
```

lshw-gui

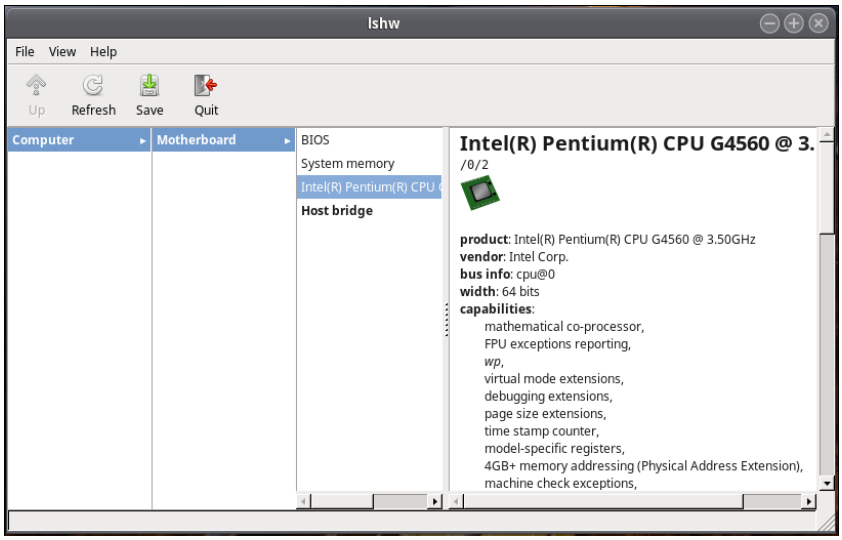
Простой интерфейс для просмотра информации о аппаратном обеспечении компьютера.

Установка.

```
sudo dnf install lshw-gui
```

Запустите через «Меню > Администрирование > Hardware Lister» , или через консоль, набрав команду:

```
sudo lshw-gui
```



В левой части окна отображается оборудование, а в правой части подробная информация о выбранном пункте. lshw-gui позволяет сохранить полученную информацию простым текстом, а также в XML, HTML, JSON форматах.

hwinfo

Консольная утилита для получения информации об аппаратном обеспечении компьютера. Она способна выводить информацию об отдельных категориях аппаратных компонентов, что позволяет получить компактный листинг.

Установка.

```
sudo dnf install hwinfo
```

Для просмотра полной информации о аппаратных компонентах ПК достаточно ввести команду без параметров:

```
hwinfo
```

Однако, полученный вывод не всегда удобен для чтения. Для получения краткого списка компонентов используется параметр short. Он позволяет скрыть подробную информацию о найденных аппаратных компонентах:

```
hwinfo --short
```

Как видно из примера выше, параметры в этой программе записываются через двойной дефис.

Также вы можете выбрать с помощью параметров определённую категорию аппаратных компонентов для просмотра:

```
--cdrom Информация об устройствах для работы с оптическими накопителями;
--cpu Информация о центральном процессоре;
--disk Информация о жестких дисках;
--gfxcard Информация о графическом ускорителе;
--ide Информация об устройствах, подключенных по интерфейсу IDE/SATA;
--memory Информация об оперативной памяти;
--network Информация о сетевых интерфейсах;
--partition Информация о разделах жестких дисков;
--usb Информация об устройствах, подключенных по интерфейсу USB.
```

Если вам нужно получить информацию только об одном устройстве из определённой категории, используйте параметр only. Например, для просмотра информации по разделу жёсткого диска /dev/sda1, команда будет иметь вид:

```
hwinfo --partition --only /dev/sda1
```

Для сохранения журнала работы утилиты в файле достаточно использовать параметр --log с последующим именем файла. В файле сохраняется как журнал работы утилиты, так и выводимая в результате ее работы информация.

```
hwinfo --all --log logfile.txt
```

Файл будет сохранён в корневом каталоге пользователя.

Чтобы сохранить в файл только результат вывода команды howinfo, используется формат:

```
hwinfo --all > logfile.txt
```

Для получения справки по доступным параметрам используется параметр help:

```
hwinfo --help
```

В качестве примера попробуем вывести данные об оперативной памяти:

```
hwinfo --memory
```

Получим:

```
01: None 00.0: 10102 Main Memory
[Created at memory.74]
Unique ID: rdCR.CxwsZFjVASF
Hardware Class: memory
Model: «Main Memory»
Memory Range: 0×00000000-0×7bf57fff (rw)
Memory Size: 1 GB + 896 MB
Config Status: cfg=new, avail=yes, need=no, active=unknown
```

hddtemp

Для успешного прохождения тестов утилиты hddtemp жесткие диски должны поддерживать SMART.
Просмотреть температуру можно командой:

```
hddtemp /dev/sda
```

Вывод команды:

```
/dev/sda: SILICONMOTION SM223AC: 0°C
```

hw-probe

hw-probe - утилита от создателей сайта https://linux-hardware.org/, позволяет одной лаконичной командой собрать в одном файле все основные сведения о системе, аппаратной части и логах, которые могут быть полезными в поисках решения большинства проблем. Результатом работы программы будет ссылка на веб-страницу, по которой можно найти подробную сводку информации о компьютере.

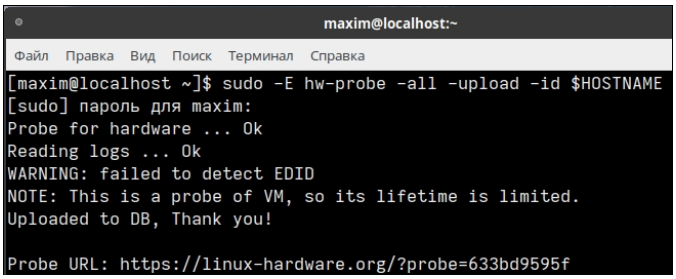
Приватная информация (включая имя пользователя, имя компьютера, IP-адрес, MAC-адрес, серийные номера) **НЕ** собирается в пробе. Инструмент загружает лишь часть *SHA512* хэша от MAC-адреса и серийных номеров для идентификации уникальных компьютеров и компонентов. Данные в базу отправляются по зашифрованному соединению HTTPS.

Устанавливается командой:

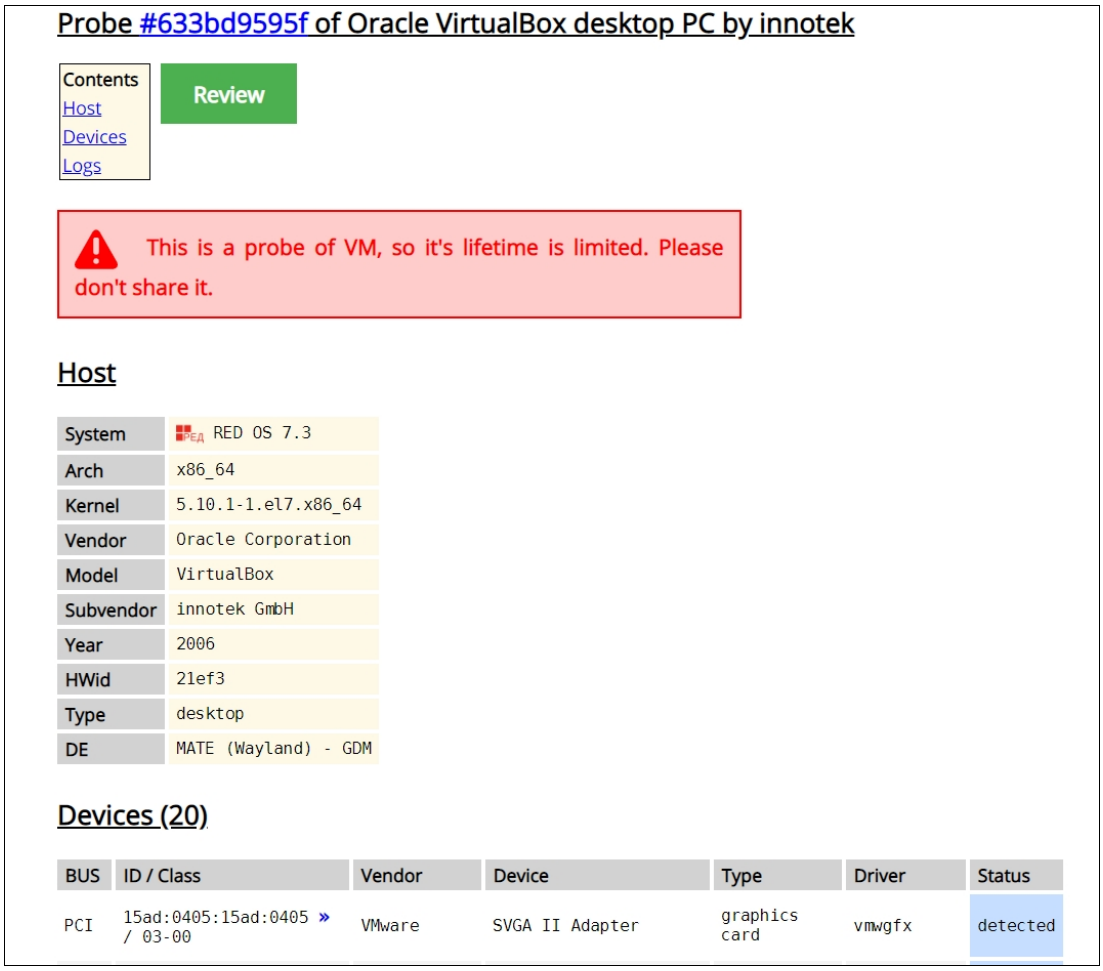
```
sudo dnf install hw-probe
```

Чтобы сгенерировать отчет о системе, нужно выполнить команду:

```
sudo -E hw-probe -all -upload -id $HOSTNAME
```



Терминал предоставляет ссылку, переходя по которой получаем сведения о системе:
https://linux-hardware.org/?probe=633bd9595f



Probe #633bd9595f of Oracle VirtualBox desktop PC by innotek

Contents
Host
Devices
Logs

Review

This is a probe of VM, so it's lifetime is limited. Please don't share it.

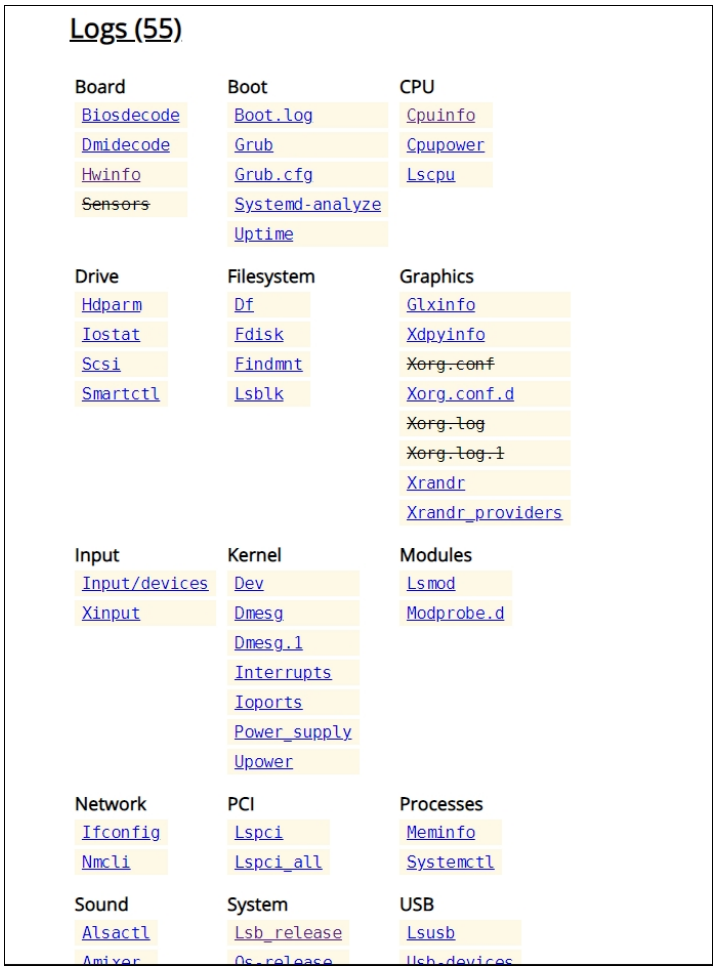
Host

System	RED OS 7.3
Arch	x86_64
Kernel	5.10.1-1.el7.x86_64
Vendor	Oracle Corporation
Model	VirtualBox
Subvendor	innotek GmbH
Year	2006
HWid	21ef3
Type	desktop
DE	MATE (Wayland) - GDM

Devices (20)

BUS	ID / Class	Vendor	Device	Type	Driver	Status
PCI	15ad:0405:15ad:0405 » / 03-00	VMware	SVGA II Adapter	graphics card	vmwgfx	detected

Ниже на этой странице находится необходимый набор логов:



Logs (55)

Board
Biosdecode
Dmidecode
Hwinfo
~~Sensors~~

Boot
Boot.log
Grub
Grub.cfg
Systemd-analyze
Uptime

CPU
Cpuinfo
Cpupower
Lscpu

Drive
Hdparm
Iostat
Scsi
Smartctl

Filesystem
Df
Fdisk
Findmnt
Lsblk

Graphics
Glxinfo
Xdpyinfo
~~Xorg.conf~~
Xorg.conf.d
~~Xorg.log~~
~~Xorg.log.1~~
Xrandr
Xrandr_providers

Input
Input/devices
Xinput

Kernel
Dev
Dmesg
Dmesg.1
Interrupts
Ioports
Power_supply
Upower

Modules
Lsmod
Modprobe.d

Network
Ifconfig
Nmcli

PCI
Lspci
Lspci_all

Processes
Meminfo
Systemctl

Sound
Alsactl
Amixer

System
Lsb_release
Os-release

USB
Lsusb
Usb-devices

При выполнении команды без параметра **-upload**:

```
```

```
sudo -E hw-probe -all
```

информация сохранится локально по пути: **/root/HW_PROBE/LASTEST/hw.info**

Начиная с версии *hw-probe 1.5* можно импортировать отчет в формате html-страницы в указанную директорию:

```
hw-probe -import ./DIR
```

Стандартные средства и команды операционной системы РЕД ОС

Если у вас установлена графическая оболочка Cinnamon, то базовые сведения о системе можно узнать пройдя в «Меню» -> «Параметры» -> «О системе».

Если вам нужна более подробная информация, воспользуйтесь следующими командами из консоли РЕД ОС.

Формат команды	**Описание**
hostnamectl	Имя компьютера и основные данные по ОС.
sudo dmidecode -t 2	Данные по материнской плате (производитель, модель).
lscpu	Информация о процессоре (название модели, семейство, архитектура, его текущая частота, количество ядер, потоков).
cat /proc/meminfo	Просмотр статистики использования памяти в системе читается из файла /proc/meminfo.
free -h	Просмотр основной информации о памяти (общее количество, свободно, используется).
lsb_release -a	Версия, название дистрибутива и дополнительная информация об операционной системе.
blkid	Список подключённых жестких дисков вместе с UUID.
lsblk	Список всех подключённых или созданных в системе блочных устройств.
df -h	Свободное пространство на диске.
df -T	Тип файловой системы.
sudo fdisk -l	Информация о размере диска.
sudo smartctl -a -i /dev/sda	Информация системы SMART жёсткого диска.
mount	Вывод списка смонтированных файловых систем. Каждая строка содержит информацию об имени устройства, директории, в которой оно смонтировано, типе и опциях монтирования в следующей форме: `<имя_устройства> on <директория> type <тип_файловой_системы> (<опции>)` Для отображения только ФС определенного типа используется опция -t.
lspci	Просмотр устройств, подключенных к PCI.
lsusb	Просмотр устройств, подключенных к USB.
uptime	Время работы системы.
ip addr	Информация о сети.
ps aux	Информация о запущенных процессах.

Рассмотрим вывод смонтированных разделов с типом файловой системы ext4:

```
mount -t ext4
```

Результат:

```
/dev/mapper/ro-root on / type ext4 (rw,relatime,seclabel)
/dev/sda1 on /boot type ext4 (rw,relatime,seclabel)
```

hardinfo – подробная информация о системе

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** hardinfo-0.5.2.git20201116-1

HardInfo — утилита просмотра подробной информации о системе и оборудовании. Утилита позволяет производить мониторинг системы в режиме реального времени, а также отображает информацию о запущенных процессах, загруженности процессора и занятости разделов на дисках.

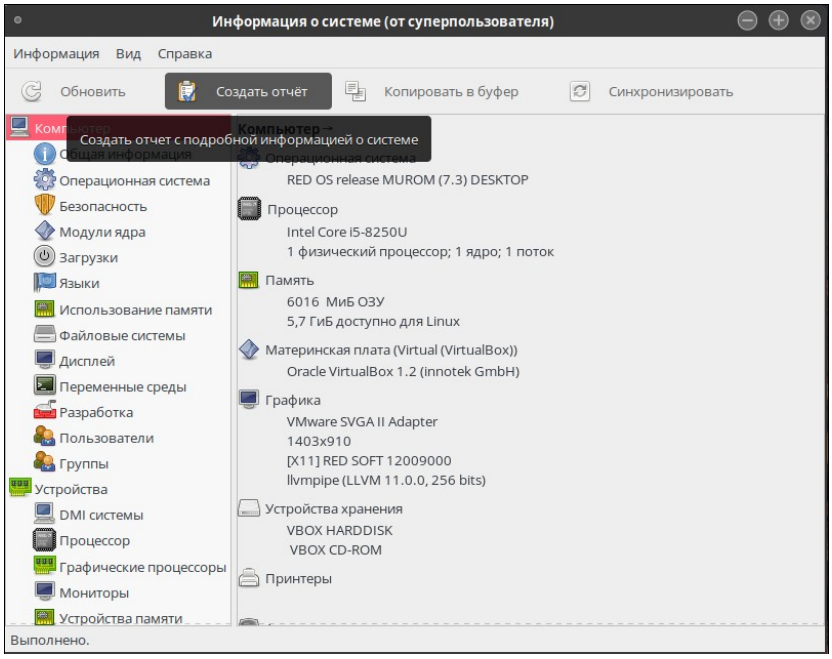
Установка **HardInfo** производится командой:

```
dnf install hardinfo
```

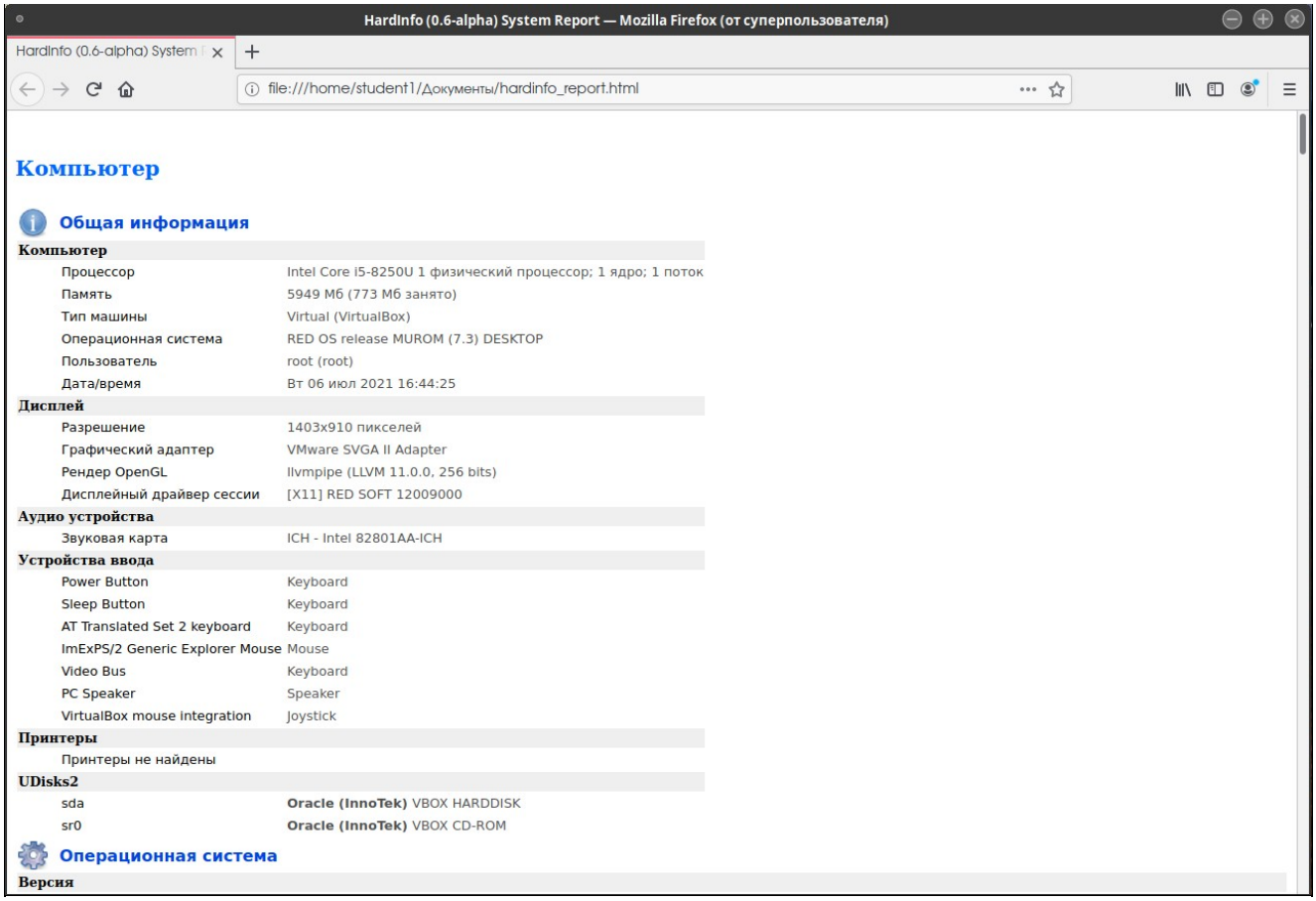
Запуск программы производится через «**Главное меню**» - «**Параметры**» - «**Информация о системе**» или командой:

```
hardinfo
```

Hardinfo позволяет создавать подробный отчёт с информацией о системе.



После создания отчёта его можно просматривать в браузере.



Компьютер

Общая информация

Компьютер	
Процессор	Intel Core i5-8250U 1 физический процессор; 1 ядро; 1 поток
Память	5949 Мб (773 Мб занято)
Тип машины	Virtual (VirtualBox)
Операционная система	RED OS release MUROM (7.3) DESKTOP
Пользователь	root (root)
Дата/время	Вт 06 июл 2021 16:44:25
Дисплей	
Разрешение	1403x910 пикселей
Графический адаптер	VMware SVGA II Adapter
Рендер OpenGL	llvmpipe (LLVM 11.0.0, 256 bits)
Дисплейный драйвер сессии	[X11] RED SOFT 12009000
Аудио устройства	
Звуковая карта	ICH - Intel 82801AA-ICH
Устройства ввода	
Power Button	Keyboard
Sleep Button	Keyboard
AT Translated Set 2 keyboard	Keyboard
ImExPS/2 Generic Explorer Mouse	Mouse
Video Bus	Keyboard
PC Speaker	Speaker
VirtualBox mouse integration	Joystick
Принтеры	
Принтеры не найдены	
UDisks2	
sda	**Oracle (InnoTek)** VBOX HARDDISK
sr0	**Oracle (InnoTek)** VBOX CD-ROM

Операционная система

Версия

hdparm – получение информации о параметрах жестких дисков

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** hdparm-9.62-3

hdparm — это утилита командной строки для Unix-подобных операционных систем. Утилита предназначена для регулировки и просмотра параметров жёстких дисков с интерфейсом *ATA*. Утилита может установить такие параметры, как объём кеш-памяти накопителя, спящий режим, управление питанием, управление акустикой и настройки DMA.

Полезные параметры:

-g	Отображает геометрию устройства (цилиндры, головки, сектора), размер (в секторах) устройства.
-h	Отображает краткую информацию об использовании (помощь).
-H	Считывает температуру некоторых устройств (большинство Hitachi). Также отображает предупреждение, если температура выше нормы.
-i	Отображает идентификационную информацию от драйвера устройства.
-I	Отображает идентификационную информацию прямо от устройства. Более детально.
-t	Отображает скорость чтения с диска, без кэширования данных.
-T	Отображает скорость чтения напрямую из кэша Linux-буфера, без доступа к диску.

Использование команды:

1) Без параметров:

```
sudo hdparm /dev/sda
```

```
/dev/sda:

 Model=VBOX HARDDISK, FwRev=1.0, SerialNo=VB2635c6c9-03c8cc84
 Config={ Fixed }
 RawCHS=16383/16/63, TrkSize=0, SectSize=512, ECCbytes=0
 BuffType=DualPortCache, BuffSize=256kB, MaxMultSect=128, MultSect=128
 CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=209715200
 IORDY=yes, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
 PIO modes:  pio0 pio3 pio4
 DMA modes:  mdma0 mdma1 mdma2
 UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5 udma6
 AdvancedPM=no WriteCache=enabled
```

2) Вывод информации о жестком диске:

```
sudo hdparm -i /dev/sda
```

```
/dev/sda:

 Model=VBOX HARDDISK, FwRev=1.0, SerialNo=VB2635c6c9-03c8cc84
 Config={ Fixed }
 RawCHS=16383/16/63, TrkSize=0, SectSize=512, ECCbytes=0
 BuffType=DualPortCache, BuffSize=256kB, MaxMultSect=128, MultSect=128
 CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=209715200
 IORDY=yes, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
 PIO modes:  pio0 pio3 pio4
 DMA modes:  mdma0 mdma1 mdma2
 UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5 udma6
 AdvancedPM=no WriteCache=enabled
 Drive conforms to: unknown:  ATA/ATAPI-1,2,3,4,5,6

 * signifies the current active mode
```

3) Отображение краткой информации о диске, текущая температура:

```
sudo hdparm -iH /dev/sda
```

```
/dev/sda:
SG_IO: bad/missing sense data, sb[]:  70 00 05 00 00 00 00 0a 04 41 e0 00 21 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 drive temperature (celsius) is:  -18
 drive temperature in range:  yes
 Model=VBOX HARDDISK, FwRev=1.0, SerialNo=VB2635c6c9-03c8cc84
 Config={ Fixed }
 RawCHS=16383/16/63, TrkSize=0, SectSize=512, ECCbytes=0
 BuffType=DualPortCache, BuffSize=256kB, MaxMultSect=128, MultSect=128
 CurCHS=16383/16/63, CurSects=16514064, LBA=yes, LBAsects=209715200
 IORDY=yes, tPIO={min:120,w/IORDY:120}, tDMA={min:120,rec:120}
 PIO modes:  pio0 pio3 pio4
 DMA modes:  mdma0 mdma1 mdma2
 UDMA modes: udma0 udma1 *udma2 udma3 udma4 udma5 udma6
 AdvancedPM=no WriteCache=enabled
 Drive conforms to: unknown:  ATA/ATAPI-1,2,3,4,5,6

 * signifies the current active mode
```

4) Скорость чтения данных с диска:

```
sudo hdparm -tT /dev/sda
```

```
/dev/sda:
 Timing cached reads:   35776 MB in  2.00 seconds = 17932.59 MB/sec
 Timing buffered disk reads: 900 MB in  3.00 seconds = 299.55 MB/sec
```

smartctl и hddtemp – мониторинг состояния жестких дисков

Для успешного прохождения тестов утилит **smartctl** и **hddtemp** жесткие диски должны поддерживать *SMART*.

Проверка, включена ли интеллектуальная функция для диска.

1) Определение дисков в системе:

```
sudo smartctl --scan
```

Отобразится список дисков в вашем компьютере:

```
/dev/sda -d scsi # /dev/sda, SCSI device
```

2) Информация о диске:

```
sudo smartctl -i /dev/sda
```

Пример:

```
=== START OF INFORMATION SECTION ===
Model Family:     Toshiba 2.5" HDD MK..65GSX
Device Model:     TOSHIBA MK3265GSXN
Serial Number:    3192P99AT
LU WWN Device Id: 5 000039 322201685
Firmware Version: GH101M
User Capacity:    320 072 933 376 bytes [320 GB]
Sector Size:      512 bytes logical/physical
Rotation Rate:    5400 rpm
Form Factor:      2.5 inches
Device is:        In smartctl database [for details use: -P show]
ATA Version is:   ATA8-ACS (minor revision not indicated)
SATA Version is:  SATA 2.6, 3.0 Gb/s (current: 3.0 Gb/s)
Local Time is:    Mon Mar  5 00:02:01 2018 MSK
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

3) Подробная информация о состоянии:

```
sudo smartctl -A /dev/sda
```

Пример:

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000b   100   100   050    Pre-fail  Always       -       0
  2 Throughput_Performance  0x0005   100   100   050    Pre-fail  Offline      -       0
  3 Spin_Up_Time            0x0027   100   100   001    Pre-fail  Always       -       1141
  4 Start_Stop_Count        0x0032   100   100   000    Old_age   Always       -       7407
  5 Reallocated_Sector_Ct   0x0033   100   100   050    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000b   100   100   050    Pre-fail  Always       -       0
  8 Seek_Time_Performance   0x0005   100   100   050    Pre-fail  Offline      -       0
  9 Power_On_Hours          0x0032   058   058   000    Old_age   Always       -       17038
 10 Spin_Retry_Count        0x0033   245   100   030    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -       7224
191 G-Sense_Error_Rate      0x0032   100   100   000    Old_age   Always       -       176
192 Power-Off_Retract_Count 0x0032   098   098   000    Old_age   Always       -       1279
193 Load_Cycle_Count        0x0032   047   047   000    Old_age   Always       -       531423
194 Temperature_Celsius     0x0022   100   100   000    Old_age   Always       -       39 (Min/Max 10/53)
196 Reallocated_Event_Count 0x0032   100   100   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0032   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0030   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x0032   200   200   000    Old_age   Always       -       1
220 Disk_Shift              0x0002   100   100   000    Old_age   Always       -       89
222 Loaded_Hours            0x0032   070   070   000    Old_age   Always       -       12360
223 Load_Retry_Count        0x0032   100   100   000    Old_age   Always       -       0
224 Load_Friction           0x0022   100   100   000    Old_age   Always       -       0
```

```
226 Load-in_Time          0x0026   100   100   000    Old_age   Always       -       309
240 Head_Flying_Hours     0x0001   100   100   001    Pre-fail  Offline      -       0
```

Ключевое значение имеет содержимое 3-х столбцов:

- **VALUE** - текущее значение параметра;
- **WORST** - наихудшее значение, которого когда-либо достигало значение *Value*;
- **THRESH** - значение, которое должен достигнуть *Value* этого же атрибута, чтобы состояние атрибута было признано критическим.

Критичным является поле **WHEN_FAILED**, если оно имеет значение **FAIL**, то высока вероятность выхода жесткого диска из строя в ближайшее время.

4) Проверка жесткого диска на наличие критических ошибок:

```
sudo smartctl -H /dev/sda
```

Пример:

```
=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED
```

Если результат не **PASSED**, то диск следует заменить.

5) Расширенные встроенные тесты:

```
sudo smartctl --test=long /dev/sda
```

Пример:

```
=== START OF OFFLINE IMMEDIATE AND SELF-TEST SECTION ===
Sending command: "Execute SMART Extended self-test routine immediately in off-line mode".
Drive command "Execute SMART Extended self-test routine immediately in off-line mode" successful.
Testing has begun.
Please wait 98 minutes for test to complete.
Test will complete after Mon Mar  5 01:46:10 2018
```

Для прерывания теста используйте:

```
sudo smartctl -X
```

Для просмотра результатов выполнения тестов используется команда вывода внутреннего журнала после завершения теста:

```
sudo smartctl -l selftest /dev/sda
```

Для просмотра температуры используется утилита **hddtemp**. Просмотреть температуру можно командой:

```
hddtemp /dev/sda
```

Вывод команды:

```
/dev/sda: SILICONMOTION SM223AC: 0°C
```

sysbench - утилита тестирования производительности

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** sysbench 1.0.17-2

sysbench — многоцелевая утилита для тестирования производительности с открытым исходным кодом, она позволяет оценить параметры производительности процессора, памяти и файловой системы.

Установка **sysbench** производится командой:

```
dnf install sysbench
```

Синтаксис использования утилиты:

```
sysbench <основные_опции> --test=<имя_теста> <опции> <команда>
```

Основные опции:

- **--num-threads=N** — число потоков [1];
- **--max-requests=N** — ограничение общего кол-ва запросов [10000].

Используемые команды:

- **prepare** — подготовка теста (создание таблиц, вставка данных и т.п.);
- **run** — выполнение теста;
- **cleanup** — очистка данных (после этапа подготовки);
- **help** — вывод дополнительных параметров теста.

Тестирование производительности процессоров (--test=cpu):

```
sysbench --test=cpu run

Running the test with following options:
Number of threads: 1
Initializing random number generator fr om current time


Prime numbers lim it: 10000

Initializing worker threads...

Threads started!

CPU speed:
  events per second:  1085.35

General statistics:
  total time:                          10.0007s
  total number of events:              10856

Latency (ms):
    min:                                    0.85
    avg:                                    0.92
    max:                                    5.18
    95th percentile:                        0.97
    sum:                                 9991.47

Threads fairness:
  events (avg/stddev):           10856.0000/0.00
  execution time (avg/stddev):   9.9915/0.00
```

Тестирование производительности последовательных операций чтения/записи в оперативную память (--test=memory)

```
sysbench --test=memory run

Running memory speed test with the following options:
  block size: 1KiB
  total size: 102400MiB
  operation: write
  scope: global

Initializing worker threads...

Threads started!

Total operations: 52150080 (5212932.28 per second)

50927.81 MiB transferred (5090.75 MiB/sec)


General statistics:
  total time:                          10.0001s
  total number of events:              52150080

Latency (ms):
    min:                                    0.00
    avg:                                    0.00
    max:                                    2.39
    95th percentile:                        0.00
    sum:                                 4543.73

Threads fairness:
  events (avg/stddev):           52150080.0000/0.00
  execution time (avg/stddev):   4.5437/0.00
```

Тестирование разнообразной нагрузки на файловую подсистему (--test=fileio)

```
sysbench --test=fileio --file-test- mode=seqwr run
Running the test with following options:
Number of threads: 1
Initializing random number generator from current time


Extra file open flags: (none)
128 files, 16MiB each
2GiB total file size
Block size 16KiB
Periodic FSYNC enabled, calling fsync() each 100 requests.
Calling fsync() at the end of test, Enabled.
Using synchronous I/O mode
Doing sequential write (creation) test
Initializing worker threads...

Threads started!


File operations:
  reads/s:                      0.00
  writes/s:                     22474.07
  fsyncs/s:                     28776.01

Throughput:
  read, MiB/s:                  0.00
  written, MiB/s:               351.16

General statistics:
  total time:                          10.0012s
  total number of events:              512508

Latency (ms):
    min:                                    0.00
    avg:                                    0.02
    max:                                   11.48
    95th percentile:                        0.08
```

```
    sum:                                  9805.95

Threads fairness:
    events (avg/stddev):          512508.0000/0.00
    execution time (avg/stddev):  9.8060/0.00
```

glxgear и glxinfo – тестирование производительности графического ускорителя

3D-ускорение
Проверка производительности

glxgears - это популярный OpenGL-тест, который входит в пакет утилит **mesa-utils**.

3D-ускорение

Чтобы определить, работает ли 3D-ускорение, используйте утилиту **glxinfo**. Выполните команду:

```
glxinfo  | grep rendering
```

Вывод должен быть примерно следующим:

```
direct rendering: Yes
```

Проверка производительности

Чтобы узнать, сколько кадров в секунду (fps) выдает ваша видеокарта, запустите следующую команду:

```
glxgears -info
```

Примечание! Этот тест (с шестернёй) не очень эффективный, многие драйвера могут хорошо работать, но при этом показывать мало FPS в этом тесте.

Чтобы запустить **glxgears** с отключенной вертикальной синхронизацией, запустите следующую команду:

```
vblank_mode=0 glxgears
```

sensors - утилита для мониторинга датчиков температуры

Данная утилита - свободное ПО, состоящее из драйверов и утилит, позволяющее отслеживать температуру, напряжение, скорость вращения вентиляторов в вашей системе. Следует помнить, что набор датчиков индивидуален для каждой системы, поэтому некоторые возможности могут быть недоступны.

Используйте **sensors-detect** для обнаружения и формирования списка модулей ядра.

По окончании определения датчиков будут доступны снимаемые ими значения.

Пример:

```
sensors-detect
```

```
This program will help you determine which kernel modules you need
to load to use lm_sensors most effectively. It is generally safe
and recommended to accept the default answers to all questions,
unless you know what you're doing.

Some south bridges, CPUs or memory controllers contain embedded sensors.
Do you want to scan for them? This is totally safe. (YES/no):
Module cpuid loaded successfully.
Silicon Integrated Systems SIS5595...                       No
VIA VT82C686 Integrated Sensors...                          No
VIA VT8231 Integrated Sensors...                            No
AMD K8 thermal sensors...                                   No
AMD Family 10h thermal sensors...                           No
...
Now follows a summary of the probes I have just done.
Just press ENTER to continue:
Driver `coretemp':
* Chip `Intel digital thermal sensor' (confidence: 9)
Driver `lm90':
* Bus `SMBus nForce2 adapter at 4d00'
  Busdriver `i2c_nforce2', I2C address 0x4c
  Chip `Winbond W83L771AWG/ASG' (confidence: 6)
Do you want to overwrite /etc/conf.d/lm_sensors? (YES/no):
ln -s '/usr/lib/systemd/system/lm_sensors.service' '/etc/systemd/system/multi-user.target.wants/lm_sensors.service'
Unloading i2c-dev... OK
Unloading cpuid... OK
```

Просмотр датчиков

Пример запуска *sensors*:

```
sensors
```

```
coretemp-isa-0000
Adapter: ISA adapter
Core 0:       +58.0°C  (high = +84.0°C, crit = +100.0°C)
Core 1:       +59.0°C  (high = +84.0°C, crit = +100.0°C)
Core 2:       +59.0°C  (high = +84.0°C, crit = +100.0°C)
Core 3:       +60.0°C  (high = +84.0°C, crit = +100.0°C)

nouveau-pci-0100
Adapter: PCI adapter
temp1:        +57.0°C  (high = +95.0°C, hyst =  +3.0°C)
                       (crit = +105.0°C, hyst =  +5.0°C)
                       (emerg = +135.0°C, hyst =  +5.0°C)
```

screentest – утилита тестирования мониторов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** screentest-2.0-2

screentest — небольшая утилита тестирования мониторов. Отображаемые тестовые экранные шаблоны помогут быстро оценить качество монитора и с лёгкостью выявить дефекты. Имеющиеся тесты являются гораздо более показательными в оценке недостатков мониторов, чем обычные фотографии (картинки).

Вы можете подробнее ознакомиться с работой утилиты **screentest**, просмотрев наши обучающие видео:

- на **RuTube** — screentest - утилита тестирования мониторов;
- в **Яндекс.Дзен** — screentest - утилита тестирования мониторов;
- в **VK Видео** — screentest - утилита тестирования мониторов.

На наших каналах вы также сможете найти много другой полезной информации.

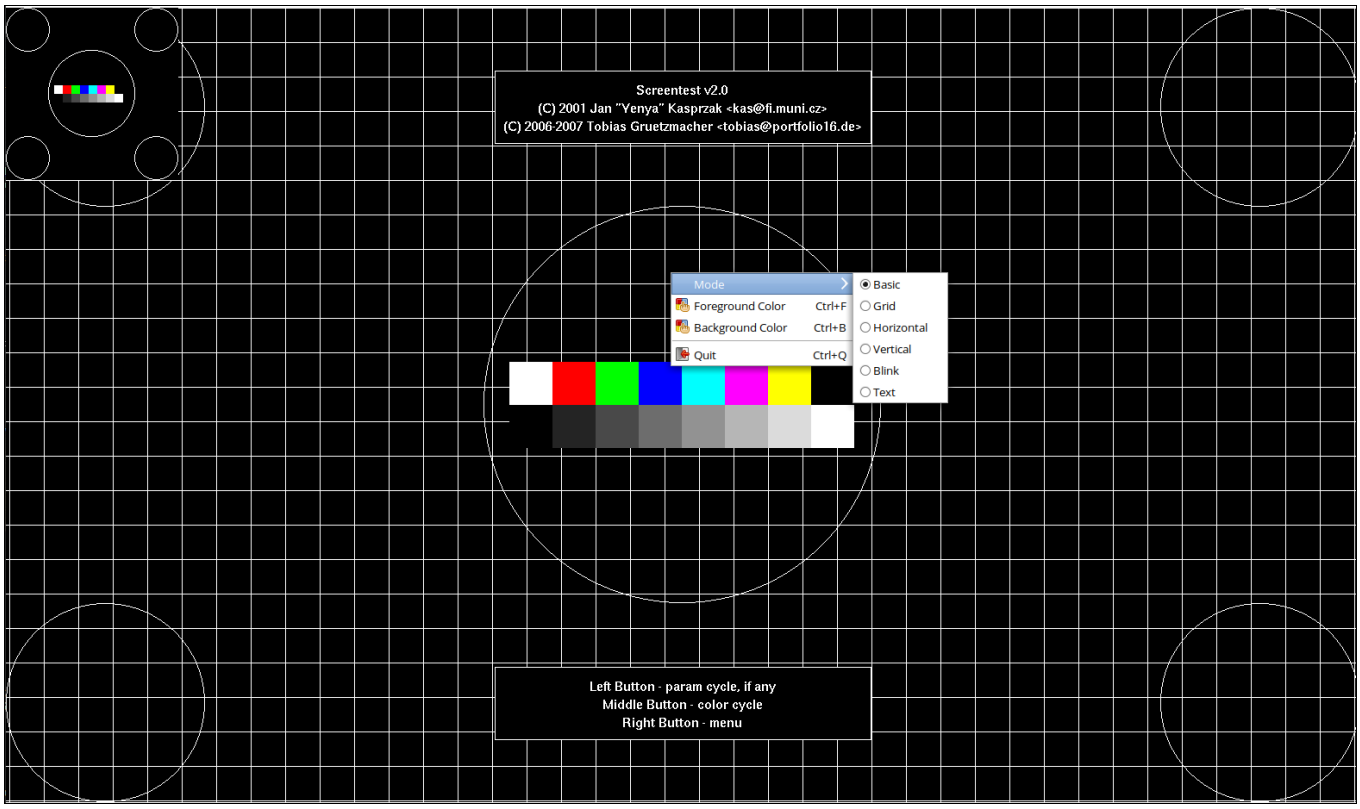
Установка **screentest** производится командой:

```
dnf install screentest
```

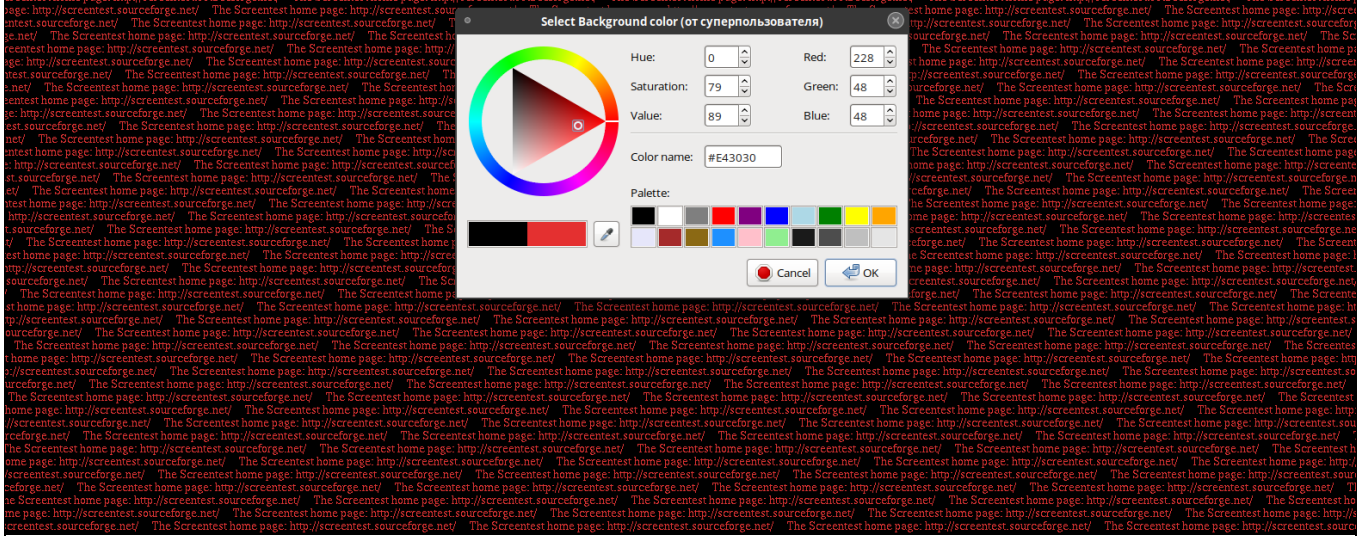
Для старта теста запустим утилиту в терминале:

```
screentest
```

Тест и его настройки выглядят следующим образом:



Screentest имеет множество различных настроек, что позволяет быстро и качественно выявить любые дефекты монитора.


Select Background color (от суперпользователя)
Hue:
0
Saturation:
79
Value:
89
Red:
228
Green:
48
Blue:
48
Color name:
#E43030
Palette:
Cancel
OK

glmark2 – тестирование графических процессоров

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** glmark2-2017.07-2.20180717git0003eff

glmark2 — утилита для тестирования видеокарт (графических процессоров).

glmark2 без дополнительных опций запускает полную серию тестов, визуально выглядящих как различного вида двух- и трёхмерная анимация, в терминале одновременно будут выводится измеренные значения **FPS** (количество сменяемых кадров за единицу времени).

Установка **Glmark2** производится командой:

```
dnf install glmark2
```

Тест производительности видеокарты будет выглядеть следующим образом:

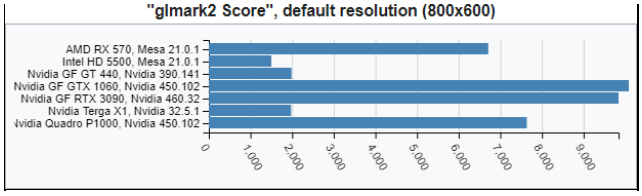




Результаты тестов выводятся в формате набранных баллов.

```
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[function] fragment-complexity=medium:fragment-steps=5: FPS: 147 FrameTime: 6.80
3 ms
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[loop] fragment-loop=false:fragment-steps=5:vertex-steps=5: FPS: 185 FrameTime:
5.405 ms
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[loop] fragment-steps=5:fragment-uniform=false:vertex-steps=5: FPS: 186 FrameTim
e: 5.376 ms
** GLX does not support GLX_EXT_swap_control or GLX_MESA_swap_control!
** Failed to set swap interval. Results may be bounded above by refresh rate.
[loop] fragment-steps=5:fragment-uniform=true:vertex-steps=5: FPS: 163 FrameTime
: 6.135 ms
=======================================================
                                  glmark2 Score: 164
=======================================================
```

Для сравнения ниже приведены результаты тестирования наиболее распространённых видеокарт.



Также следует понимать, что **glmark2** по умолчанию запускает тест в маленьком окне **800x600**, для того чтобы открыть тест с желаемым разрешением, достаточно прописать «**glmark2 -s 1920x1080**» (в этом случае тест будет производится с разрешением **1920x1080**).

Однако следует понимать, что результаты теста при изменении разрешения могут существенно отличаться.

stress-ng – утилита нагрузочного тестирования аппаратного обеспечения

stress-ng — специализированная консольная утилита для проведения нагрузочного стресс-тестирования аппаратного обеспечения различными способами.

Вы можете подробнее ознакомиться с примером использования утилиты для проведения тестирования аппаратного обеспечения ПК, просмотрев наши обучающие видео:

- на **RuTube** — Информация, мониторинг и тестирование системы;
- в **Яндекс.Дзен** — Информация, мониторинг и тестирование системы;
- в **VK Видео** — Информация, мониторинг и тестирование системы.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты необходимо выполнить команду (с правами **администратора** системы):

```
dnf in stress-ng
```

Тестирование процессора

Для подавляющего большинства ситуаций классическим примером стресс-теста можно использовать тест, выполняемый следующей командой:

```
stress-ng --cpu 16 --cpu-method matrixprod --metrics --timeout 60
```

В данном тесте задействованы 16 потоков для тестирования 16-поточного процессора. Естественно, количество потоков следует задавать в соответствии со спецификацией используемого процессора.

Тестирование дисковой подсистемы

Для проведения стресс-тестирования накопителей, таких как жёсткие диски, можно для начала провести низкоуровневый тест ввода/вывода, данный тест требует **root**-прав:

```
stress-ng --sequential 0 --class io --timeout 60s --metrics-brief
```

Тестирование памяти

Чтобы провести стресс-тест памяти, используйте команду:

```
stress-ng --sequential 0 --class memory --timeout 60s --metrics-brief
```

Комплексное тестирование

Если необходимо провести комплексное стресс-тестирование, можно задействовать работу нескольких основных подсистем вместе одной командой:

```
stress-ng --cpu 4 --io 4 --vm 1 --vm-bytes 1G --timeout 60s --metrics-brief
```

Проверка состояния жесткого диска

Smartmontools
Gsmartcontrol
Gnome disk utility
BadBlocks

Smartmontools

Smartmontools — утилита, предназначенная для проверки состояния жесткого диска. Чтобы посмотреть количество установленных жестких дисков наберите команду:

```
$ sudo smartctl --scan
```

На запрос пароля привилегированного пользователя, введите пароль локального пользователя с правами администратора.

Чтобы посмотреть информацию о жестком диске, а также узнать, поддерживает ли он технологию анализа SMART и включена ли она, наберите команду:

```
smartctl -i /dev/sda

smartctl 6.6 2018-08-10 r4748 [x86_64-linux-4.19.56-2.el7.x86_64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org
=== START OF INFORMATION SECTION ===
Model Family: Seagate Barracuda 3.5
Device Model: ST1000DM010-2EP102
Serial Number: ZN179JYJ
LU WWN Device Id: 5 000c50 0b6491aa4
Firmware Version: CC43
User Capacity: 1 000 204 886 016 bytes [1,00 TB]
Sector Sizes: 512 bytes logical, 4096 bytes physical
Rotation Rate: 7200 rpm
Form Factor: 3.5 inches
Device is: In smartctl database [for details use: -P show]
ATA Version is: ATA8-ACS T13/1699-D revision 4
SATA Version is: SATA 3.0, 6.0 Gb/s (current: 3.0 Gb/s)
Local Time is: Thu Aug 22 14:01:23 2019 MSK
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

В данном выводе указана информация о вашем жестком диске.

SMART support is: Available - device has SMART capability — жесткий диск поддерживает технологию анализа SMART. Если технология не поддерживается, вместо слова **Available** будет **Unavailable**.

SMART support is: Enabled — технология анализа SMART включена. Если она выключена у вас, то для включения введите:

```
smartctl -s on /dev/sda
```

Для выключения:

```
smartctl -s off /dev/sda
```

Для вывода атрибутов SMART введите:

```
smartctl -A /dev/sda
```

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 10
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000f   080   072   006    Pre-fail  Always       -       110427890
  3 Spin_Up_Time            0x0003   097   097   000    Pre-fail  Always       -       0
  4 Start_Stop_Count        0x0032   100   100   020    Old_age   Always       -       25
  5 Reallocated_Sector_Ct   0x0033   100   100   010    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000f   100   253   045    Pre-fail  Always       -       716102
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       42
 10 Spin_Retry_Count        0x0013   100   100   097    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   020    Old_age   Always       -       25
183 Runtime_Bad_Block       0x0032   100   100   000    Old_age   Always       -       0
184 End-to-End_Error        0x0032   100   100   099    Old_age   Always       -       0
187 Reported_Uncorrect      0x0032   100   100   000    Old_age   Always       -       0
188 Command_Timeout         0x0032   100   100   000    Old_age   Always       -       0 0 0
189 High_Fly_Writes         0x003a   100   100   000    Old_age   Always       -       0
190 Airflow_Temperature_Cel 0x0022   070   059   040    Old_age   Always       -       30 (Min/Max 24/30)
193 Load_Cycle_Count        0x0032   100   100   000    Old_age   Always       -       25
194 Temperature_Celsius     0x0022   030   021   000    Old_age   Always       -       30 (0 21 0 0 0)
195 Hardware_ECC_Recovered  0x001a   003   003   000    Old_age   Always       -       110427890
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   200   200   000    Old_age   Always       -       0
240 Head_Flying_Hours       0x0000   100   253   000    Old_age   Offline      -       42h+36m+02.609s
241 Total_LBAs_Written      0x0000   100   253   000    Old_age   Offline      -       85113048
242 Total_LBAs_Read         0x0000   100   253   000    Old_age   Offline      -       25314842
```

В данном выводе стоит смотреть на значения в колонке **RAW_VALUE**.

Наиболее важные атрибуты отмечены как **pre_fail** в колонке **TYPE**.
1 Raw_Read_Error_Rate — количество ошибок чтения. На дисках Seagate и Samsung большие значения - норма.

2 Spin_Up_Time — время раскрутки диска из состояния покоя до рабочей скорости. Растет при износе диска.

5 Rellocated Sector Count — количество переназначенных секторов. Если диск обнаружил ошибку чтения/записи он перенесет сектор в резерв. Чем меньше значение, тем лучше.

7 Seek Error Rate — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики или поверхности жёсткого диска.

196 Rellocation Event Count - число операций переназначения. **Raw Value** хранит общее число попыток переноса информации с переназначенных секторов в резервную область как успешных так и провальных.
Более подробную информацию можно найти на странице википедии.

Для того, чтобы провести тест самодиагностики, наберите команду:

```
smartctl -t <тип_теста> /dev/sda
```

Тип теста может быть:

- **long** — расширенный;
- **short** — короткий;
- **conveyance** — тест на выявления ошибок при записи/чтении.

Тесты выполняются в фоновом режиме. Чтобы просмотреть результат, наберите:

```
smartctl -l selftest /dev/sda

=== START OF READ SMART DATA SECTION ===
SMART Self-test log structure revision number 1
Num Test_Description Status Remaining LifeTime(hours) LBA_of_first_error
# 1 Conveyance offline Self-test routine in progress 60% 43 -
# 2 Short offline Completed without error 00% 42 -
# 3 Short offline Aborted by host 90% 42 -
# 4 Short captive Completed without error 00% 41 -
# 5 Short offline Completed without error 00% 41 -
```

Completed without error означает, что тест завершился без ошибок.

Для просмотра полной информации, включающей в себя показатели атрибутов SMART, информацию о жестком диске и результаты диагностических тестов, наберите:

```
$ sudo smartctl -a /dev/sda
```

Gsmartcontrol

Gsmartcontrol — это графическая утилита к **smartctl**, позволяющая оценивать состояние и работоспособность жёсткого диска или

твердотельного накопителя по показаниям S.M.A.R.T.

Основными возможностями программы являются:

- вывод информации об ошибках работы дисков;
- отображение информации о дисках, атрибутов, статистики;
- включение/выключение автоматического сбора данных о состоянии дисков;
- выполнение тестов «SMART self-tests»;
- включение/выключение SMART;
- создание отчетов по проведенным тестам.

Вы можете подробнее ознакомиться с информацией о проверке состояния жесткого диска, просмотрев наши обучающие видео:

- на **RuTube** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **Яндекс.Дзен** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **VK Видео** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install gsmartcontrol
```

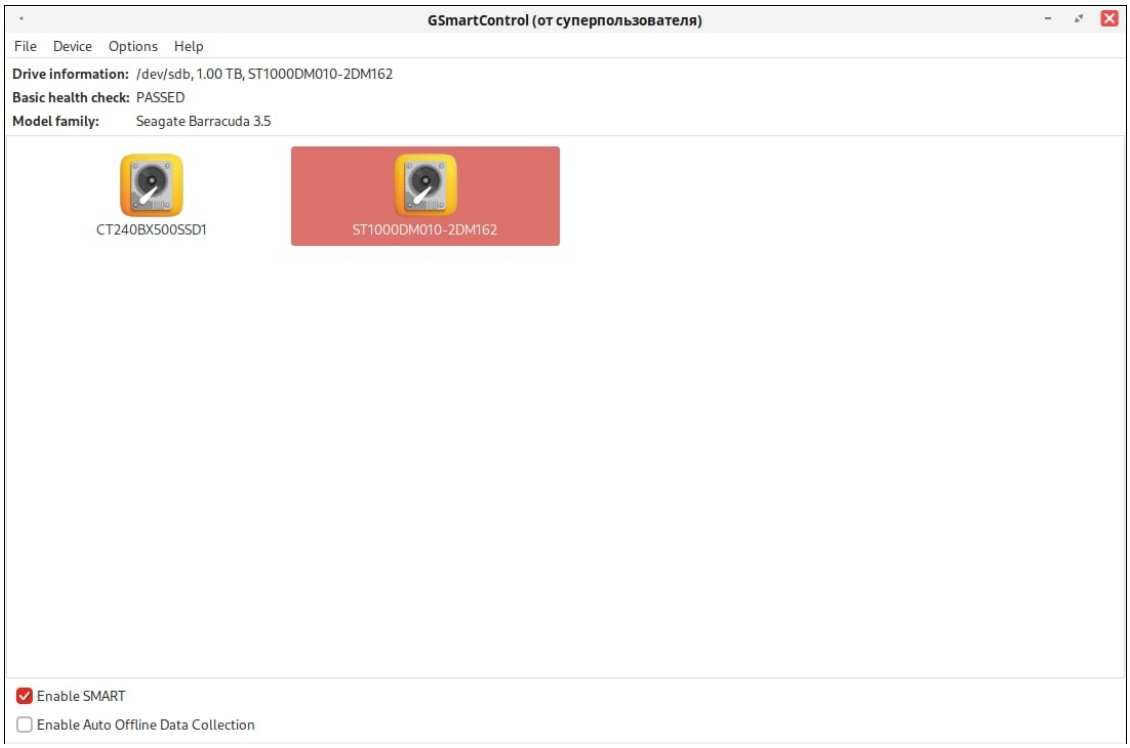
После установки программа будет доступна из «**Главного меню**» - «**Системные**» - «**Контроль S.M.A.R.T.**» или при помощи команды в терминале:

```
gsmartcontrol
```

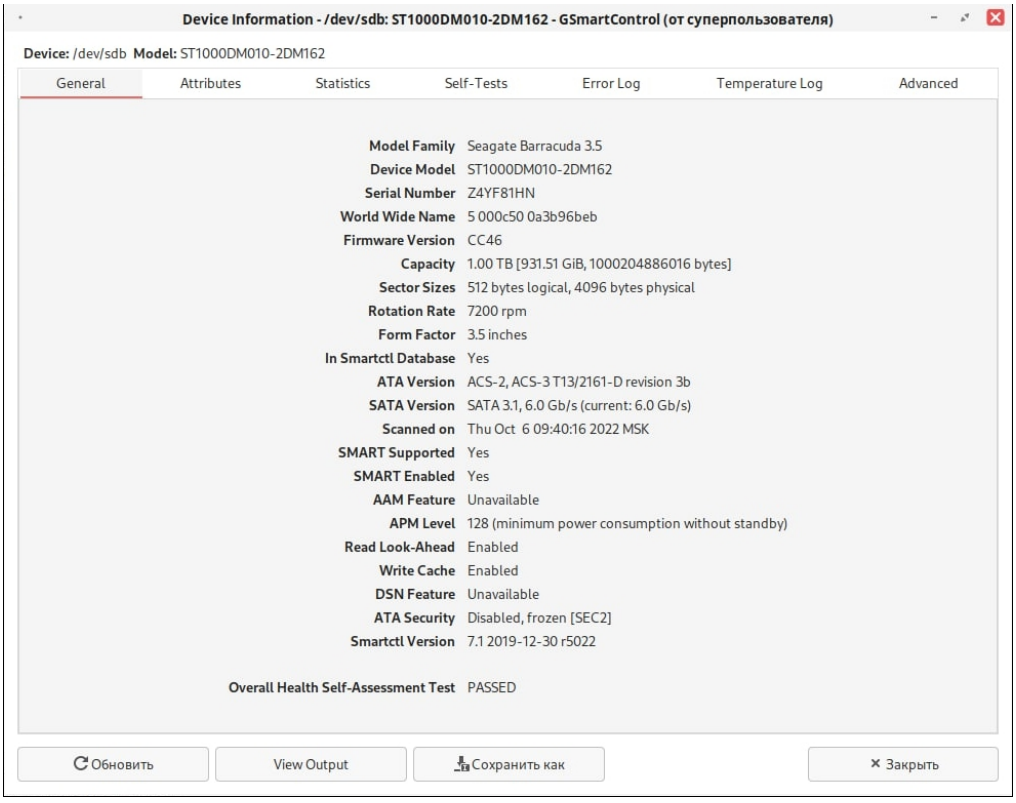
Обратите внимание, что для работы с утилитой необходимы права администратора или суперпользователя (**root**) системы.

Работа с утилитой

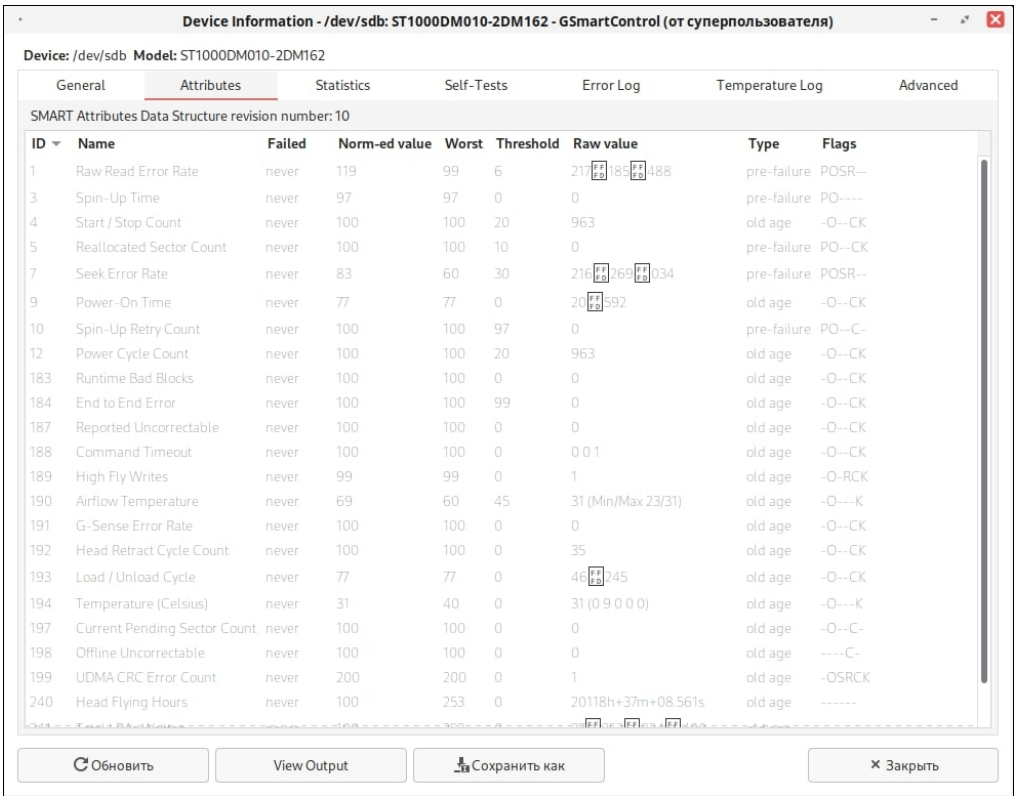
При запуске программа выглядит следующим образом:



Здесь отображены все диски, доступные для сканирования. При нажатии ПКМ на нужный диск выберите «**View details**», на вкладке «**General**» будет выведена вся информация о диске.



На вкладке «**Attributes**» указаны атрибуты проверки, нормальное, плохое и пороговое значение для каждого атрибута для удобного ориентирования по выявленным значениям в ходе проверок диска.



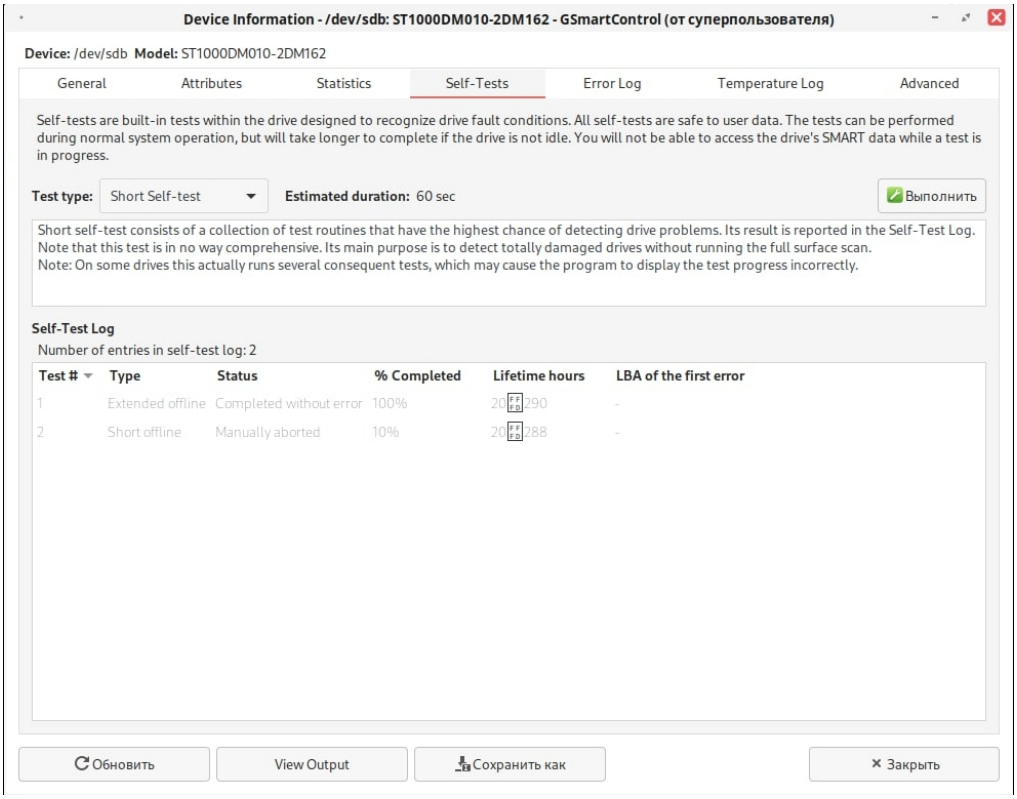
Часто используемые атрибуты:

- **Raw Read Error Rate** — частота ошибок при чтении данных с диска, происхождение которых обусловлено аппаратной частью диска, если значение большое, значит ошибки встречаются редко;
- **Spin-Up Time** — время раскрутки пакета дисков из состояния покоя до рабочей скорости, значение возрастает при износе диска;
- **Start/Stop Count** — полное число циклов запуск-остановка шпинделя. У дисков некоторых производителей (например, Seagate) — счётчик включения режима энергосбережения. В поле raw value хранится общее количество запусков/остановок диска;
- **Reallocated Sectors Count** — число операций переназначения секторов. Когда диск обнаруживает ошибку чтения/записи, он помечает сектор «переназначенным» и переносит данные в специально отведённую резервную область. Чем больше значение, тем хуже состояние поверхности дисков. Поле raw value содержит общее количество переназначенных секторов;
- **Seek Error Rat**e — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики и/или поверхности жёсткого диска;
- **Power-On Time** — число часов (минут, секунд — в зависимости от производителя), проведённых во включенном состоянии;
- **Spin-Up Retry Count** — число повторных попыток раскрутки дисков до рабочей скорости в случае, если первая попытка была неудачной. Если значение атрибута увеличивается, то велика вероятность неполадок с механической частью;
- **Power Cycle Count** — количество полных циклов включения-выключения диска;
- **End-to-End error** — данный атрибут - часть технологии HP SMART IV - означает, что после передачи данных через кэш-память чётность данных между хостом и жестким диском не совпадает;
- **Reported Uncorrectable** — ошибки, которые не могли быть восстановлены, используя методы устранения ошибки аппаратными средствами;
- **Command Timeout** — количество прерванных операций в связи с HDD тайм-аут. Обычно это значение атрибута должно быть равно нулю, и, если значение гораздо выше нуля, то, скорее всего, там будут какие-то серьезные проблемы с питанием или окисленные кабели для передачи данных;
- **Airflow Temperature** — температура воздуха внутри корпуса жёсткого диска;
- **G-sense Error Rate** — количество ошибок, возникающих в результате ударных нагрузок. Атрибут хранит показания встроенного акселерометра, который фиксирует все удары, толчки, падения и даже неаккуратную установку диска в корпус компьютера;
- **Load/Unload Cycle** — количество циклов перемещения блока магнитных головок в парковочную зону / в рабочее положение;
- **Temperature** — температура жёсткого диска;
- **Current Pending Sector Count** — число секторов, являющихся кандидатами на замену. Они пока не определены как плохие, но считывание с них отличается от чтения стабильного сектора, это так называемые подозрительные или нестабильные сектора;
- **Head flying hours** — время позиционирования головок.

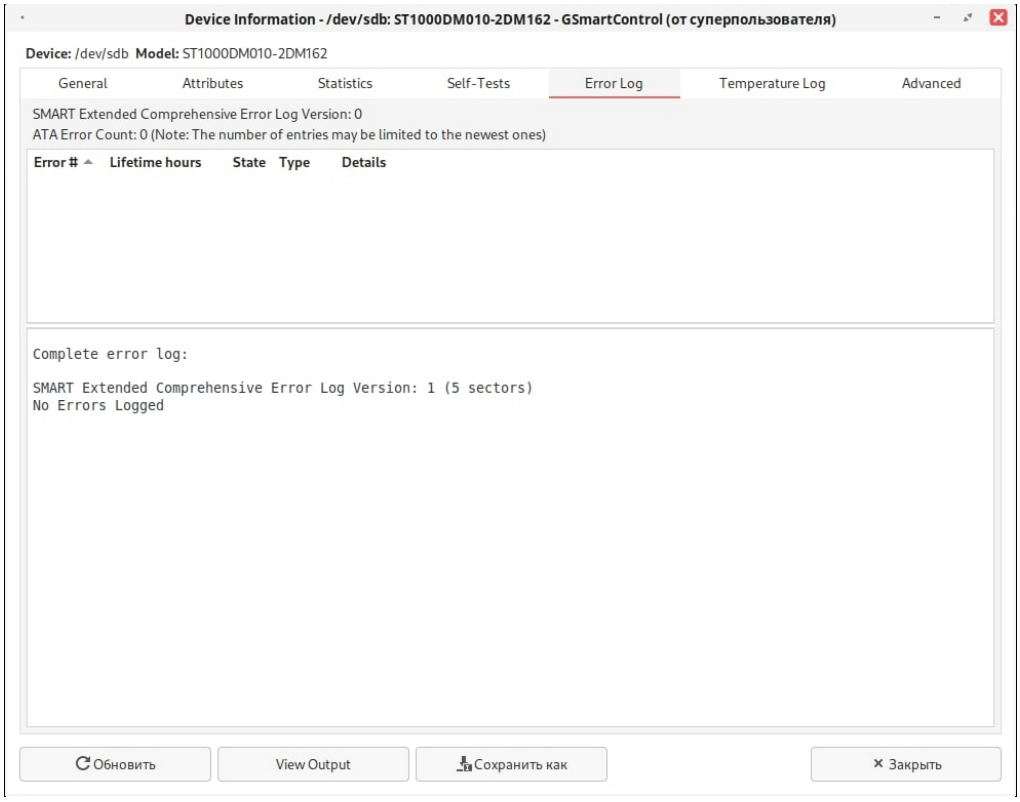
На вкладке «**Statistics**» выводится статистика использования диска.

На вкладке «**Self-Tests**» можно выполнять проверки жесткого диска. Доступно три варианта проверки:

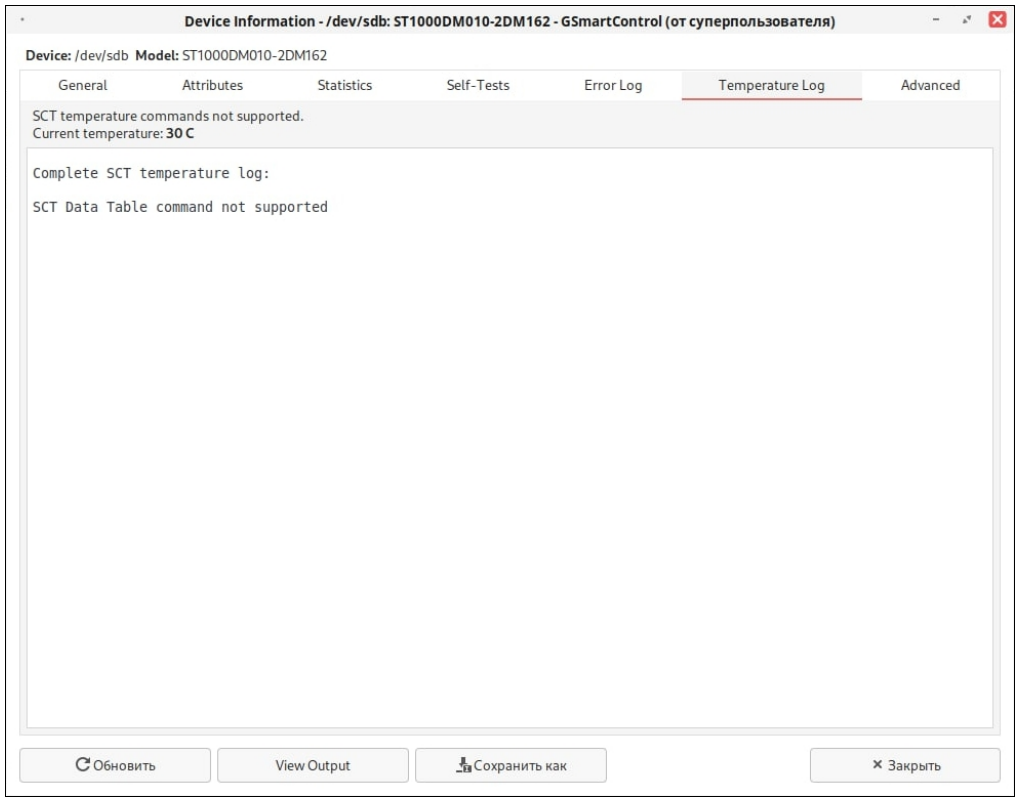
- **Быстрый тест** — продолжительностью 1 мин.
- **Расширенный тест** — продолжительностью более 1 часа, полный тест с процедурами проверки и пр.
- **Тест передачи** — продолжительностью 2 мин., тест подходит для обнаружения физических сбоев.



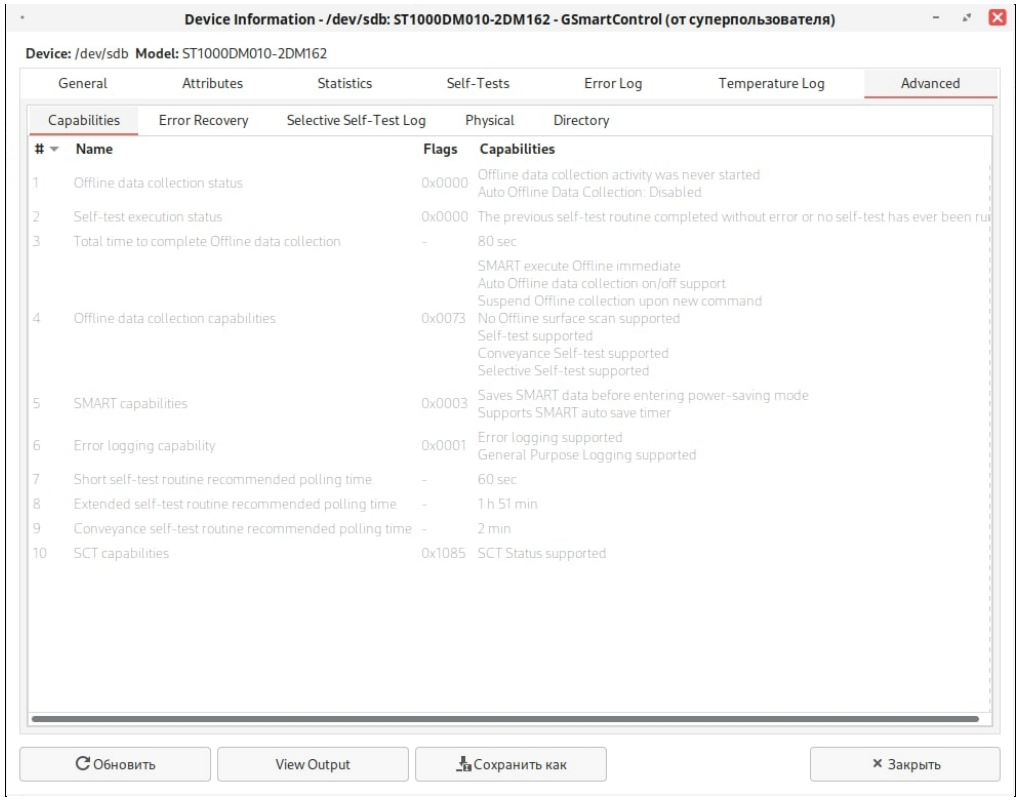
На вкладке «**Error Log**» ведется журнал ошибок с указанием деталей и подробным описанием при выборе любой из выявленных ошибок.



На вкладке «**Temperature Log**» ведется учет температурного режима используемого диска (если поддерживается).



На вкладке «**Advanced**» отображаются дополнительные параметры.



Все представленные утилитой результаты проверок можно сохранить в текстовом формате, например, для передачи информации о состоянии диска в сервисные центры или техническую поддержу.

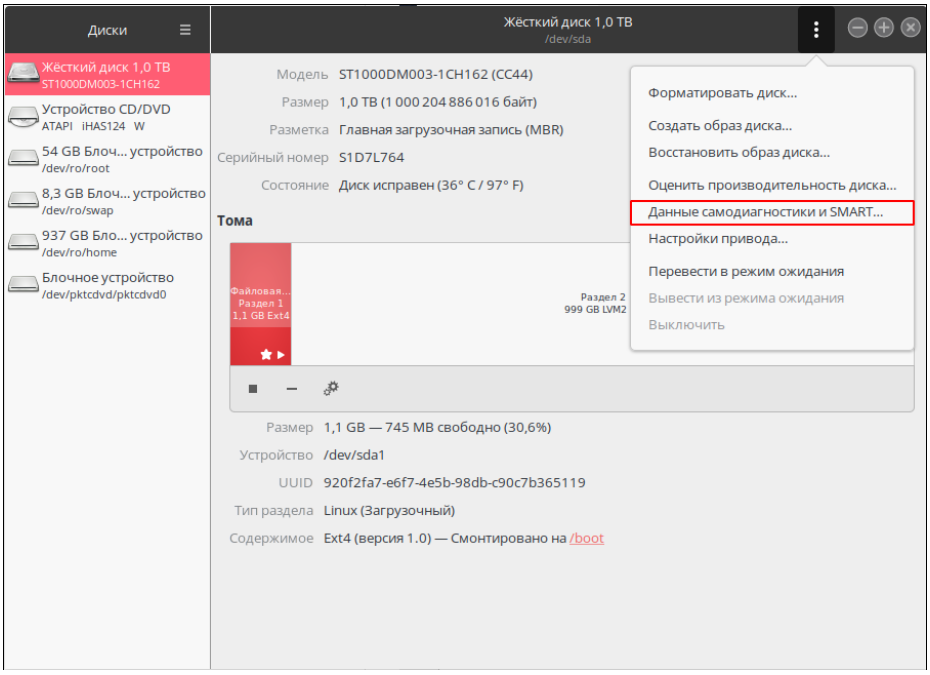
Gnome disk utility

Gnome disk utility — утилита с графической оболочкой для просмотра информации атрибутов SMART и тестирования диска. Для установки воспользуйтесь утилитой **yum** или **dnf** в зависимости от используемой версии РЕД ОС.

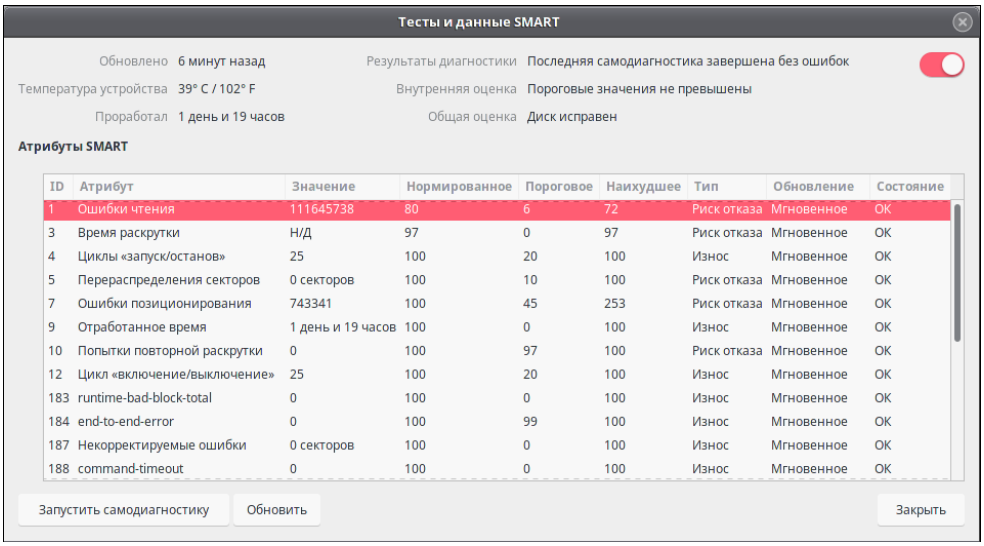
```
dnf install gnome-disk-utility
```

После установки утилита находится в **«Меню» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой Cinnamon и в **«Приложения» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой MATE.

После запуска приложения, выберите жесткий диск на панели справа, и нажмите на значок дополнительного меню, там выберите данные самодиагностики SMART.



В открывшемся окне вы можете просмотреть значения атрибутов SMART, температуры жесткого диска, результат последнего теста самодиагностики и запустить новый тест. Доступные тесты аналогичные таковым из утилиты **smartmontools**.



BadBlocks

Утилита **badblocks** используется для поиска сбойных блоков на устройстве (в разделе диска, например, */dev/sda1*).

Синтаксис утилиты:

```
badblocks [-<параметры>] <устройство> [<конечный_блок>] [<начальный_блок>]
```

Параметры [**<конечный_блок>**], [**<начальный_блок>**] являются необязательными и указывают диапазон проверяемых блоков. Если они не указаны, тогда (по умолчанию) проверке подлежат все блоки, начиная с самого первого блока и заканчивая самым последним блоком, которые используются на устройстве.

Основные параметры:

- **-b** - размер блока (в байтах);

- **-c** - порция блоков (по умолчанию 64 блока);
- **-f** - принудительный запуск теста с помощью чтения/записи;
- **-i** - входной файл (читает список уже существующих сбойных блоков);
- **-o** - исходящий файл (сохраняет список сбойных блоков в указанный файл);
- **-p** - число раз поиска (по умолчанию только одна проверка);
- **-n** - принудительное использование режима чтения-записи (только в размонтированной системе);
- **-s** - отображение хода процесса проверки;
- **-v** - подробные сообщения о проверке;
- **-w** - использование режима реальной записи (приводит к уничтожению информации на диске).

Пример использования утилиты

1. Выберите раздел жесткого диска для проверки. Для просмотра всех подключенных устройств и проверки расположения диска можно воспользоваться командой:

```
fdisk -l <имя_раздела>

  или

lsblk
```

2. Запустите проверки с помощью утилиты:

```
badblocks -v /dev/sda1Checking blocks 0 to 1048575
Checking for bad blocks (read-only test): done

Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Из вывода консоли видно, что проверка происходит только для чтения. При попытке использовать параметр **-n** (проверка чтения/записи) возникает следующее предупреждение:

```
/dev/ro_redos/root is mounted; it's not safe to run badblocks!
```

Поэтому для проверки дисков на чтение/запись рекомендуется использовать **live-сессию**.

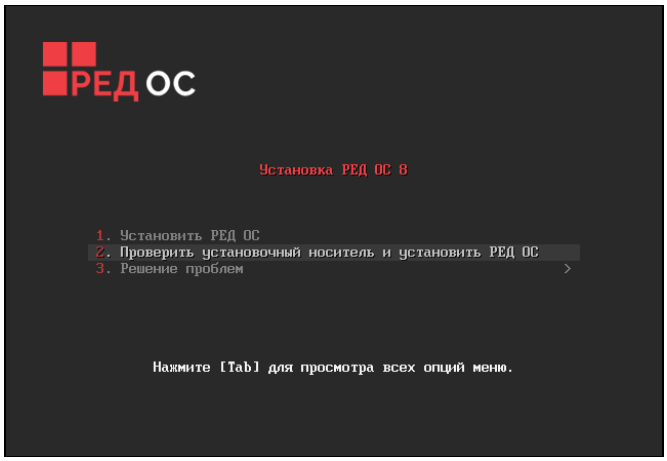
```
badblocks -v /dev/sda1

Checking for bad blocks in non-destructive read-write mode
From block 0 to 1048575
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

```
badblocks -v /dev/ro_redos/root

Checking for bad blocks in non-destructive read-write mode
From block 0 to 17821695
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

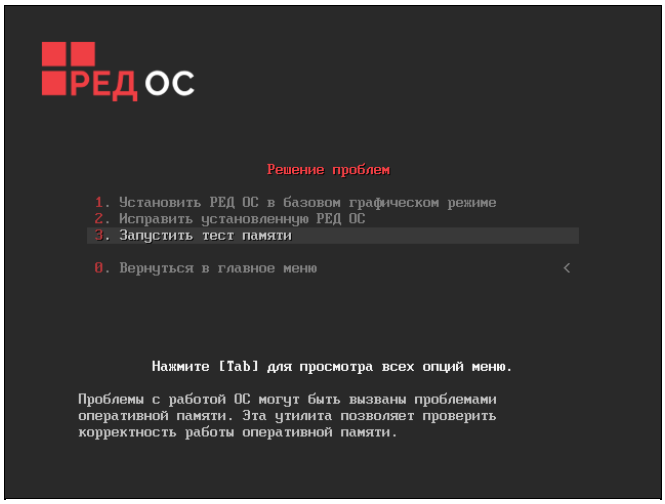
Тестирование оперативной памяти

Чтобы протестировать оперативную память на ошибки нужно запустить ОС с загрузочной флешки или диска.

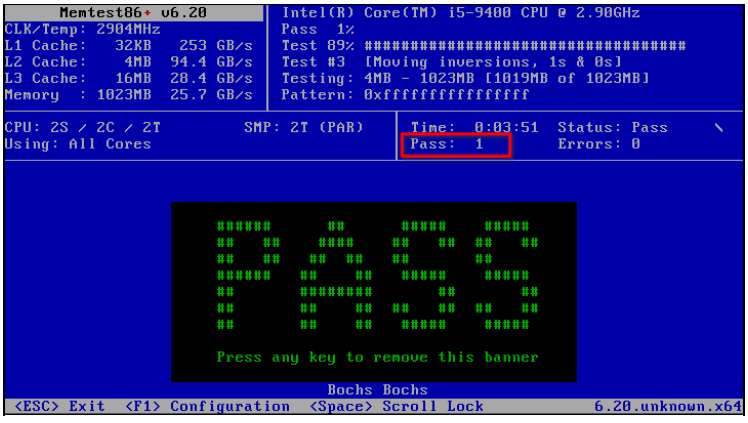
В открывшемся меню необходимо выбрать третий пункт «**Решение проблем**».



Затем выбрать третий пункт «**Запустить тест памяти**».



Запустится тест памяти. Данный процесс будет выполняться бесконечно, пока вы не остановите его. Вам нужно дождаться окончания хотя бы одного цикла проверки (значение **Pass** должно быть **>= 1**). В случае обнаружения ошибки она отобразится в списке.



minicom - программа настройки параметров COM-портов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: minicom-2.7.1-17

Minicom — консольная программа для установки сеансов связи с устройствами через последовательный порт (**COM**).

Для подключения к com-порту программу можно запускать с заданными аргументами или использовать псевдографический оконный интерфейс для изменения и сохранения собственных настроек подключения.

Сначала необходимо узнать рабочий COM-порт с помощью команды:

```
dmesg | grep "ttyS"
```

Вывод команды будет выглядеть примерно так:

```
[ 0.430791] 00:05: ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200) is a 16550A
```

где «**ttyS0**» - имя рабочего порта, который необходимо настроить.

Для установки **minicom** перейдите в сеанс пользователя **root**:

```
su-
```

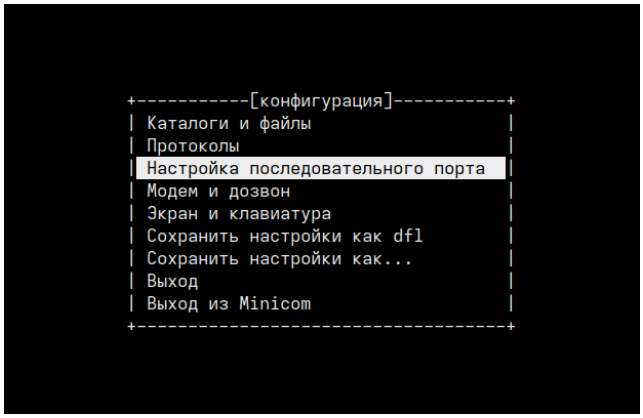
и выполните команду:

```
dnf install minicom
```

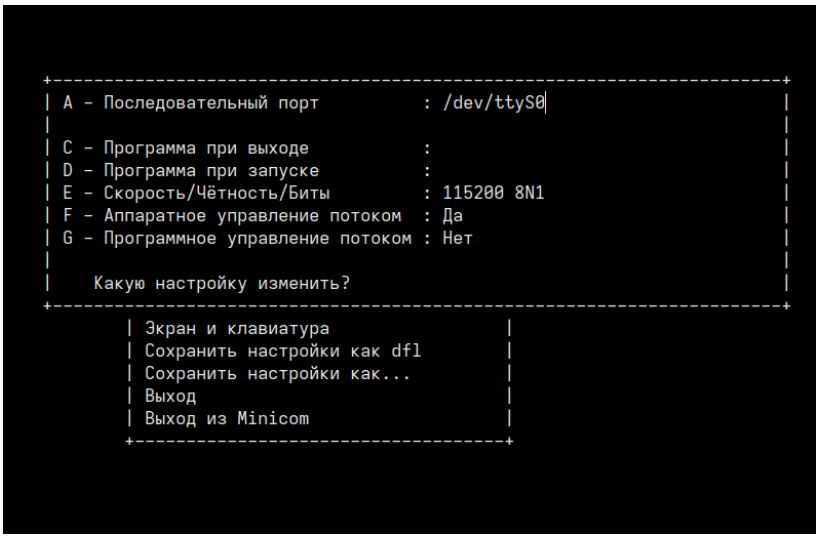
После установки запустите программу **minicom** (запуск лучше осуществлять с правами администратора, т.к. программе могут понадобиться повышенные права для доступа к порту или для сохранения настроек) с помощью команды:

```
minicom -s
```

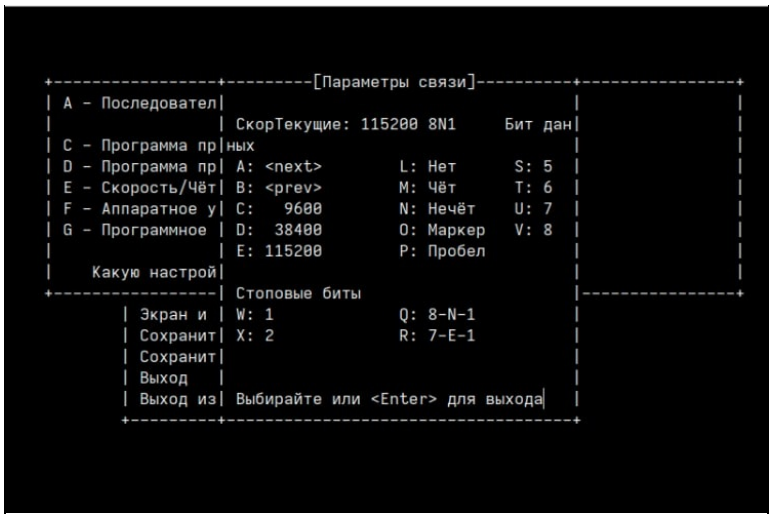
В открывшемся окне выберите пункт «**Настройка последовательного порта**».



Затем укажите необходимый COM-порт, изменяя в графе «**A - Последовательный порт**» адрес файла (в данном случае **dev/ttyS0**). Для редактирования нажмите клавишу «**A**» в строке «**Какую настройку изменить?**», курсор автоматически переведет вас в графу «**Последовательный порт**». Нажмите «**Enter**», чтобы применить изменения и вернуться в выбор настроек.



Далее в графе «**E - Скорость/Чётность/Биты**» можно настроить необходимые вам параметры. Для редактирования нажмите клавишу «**E**» в строке «**Какую настройку изменить?**», курсор автоматически переведет вас в графу «**Скорость/Четность/Биты**». Нажмите «**Enter**», чтобы применить изменения и вернуться в выбор настроек.



Для применения всех внесенных изменений и возврата в начальное меню «**Конфигурация**» еще раз нажмите «**Enter**».

Для сохранения установленных настроек выберите в меню «**Сохранить настройки как dfl**» или «**Сохранить настройки как...**» (если необходимо сохранить иначе).

Если выбрать пункт «**Сохранить настройки как...**» и указать имя файла настроек, например «**com1**», то это не изменит настройки по умолчанию (**dfl**), и в дальнейшем можно будет запускать программу с конкретными параметрами, указав имя файла с сохраненными настройками, например:

```
minicom com1
```

IMSProg - I2C/MicroWire/SPI программатор для CH341a

Установка
Сборка из исходного кода
Подключение микросхем
Выбор типа микросхемы
Основные операции программатора
Редактор базы микросхем
Список поддерживаемых микросхем

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: imsprog-1.4.4-1

IMSProg — программа, предназначенная для работы с программаторами **CH341a** и поддерживающая запись, чтение, стирание и проверку **I2C**, **SPI**, **DataFlash** и **MicroWire EEPROM/Flash** микросхем (серий *24xxx*, *25xxx*, *45xxx*, *93xxx*, *95xxx*). Программа имеет графический интерфейс и использует виджет **QHexEdit2** и доработанный набор библиотек программатора **SNANDer** для отображения шестнадцатеричного дампа прошивки микросхемы.

Для установки параметров микросхем **SPI** доступна кнопка «Поиск» для чтения параметров микросхемы (чтение информации JEDEC), а также поддерживается установка параметров микросхемы вручную. Для **I2C** и **MicroWire EEPROM** возможен только ручной выбор параметров.

Формат базы данных микросхем основан на формате программаторов EZP2019, EZP2020, EZP2023, Minpro I, XP866+. Редактирование БД микросхем производится с помощью отдельного компонента программы EZP Chip data Editor.

Установка

Для установки **IMSProg** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install imsprog
```

Дальнейшая работа с программой выполняется с правами непривилегированного пользователя.

После установки программа доступна из «**Главного меню**» — «**Программирование**» — «**IMSProg**».

Сборка из исходного кода

Также доступна самостоятельная сборка компонентов программы из исходного кода. Для этого необходимо установить дополнительные пакеты, выполнив последовательно ряд команд (для установки дополнительных компонентов необходимы права **администратора** или суперпользователя **root**):

```
dnf install cmake
dnf install libusb libusb1 libusb1-devel
dnf install qt5-qtbase-devel
dnf install pkgconf-pkg-config
dnf install qt5-linguist
```

Выйдите из сеанса администратора или суперпользователя **root**:

```
exit
```

Далее скачайте репозиторий программы с сайта **GitHub**, перейдите в каталог со скачанным архивом и распакуйте его (в примере **/home/user/Загрузки**), затем перейдите в каталог с распакованным архивом:

```
cd /home/user/Загрузки/
unzip IMSProg-main
```

```
cd IMSProg-main/
```

Для сборки программатора выполните последовательно ряд следующих команд:

```
cd IMSProg_programmer
mkdir build
cd build
cmake ..
make -j4
sudo make install
```

Вернитесь в исходный каталог с распакованным архивом:

```
cd /home/user/Загрузки/IMSProg-main/
```

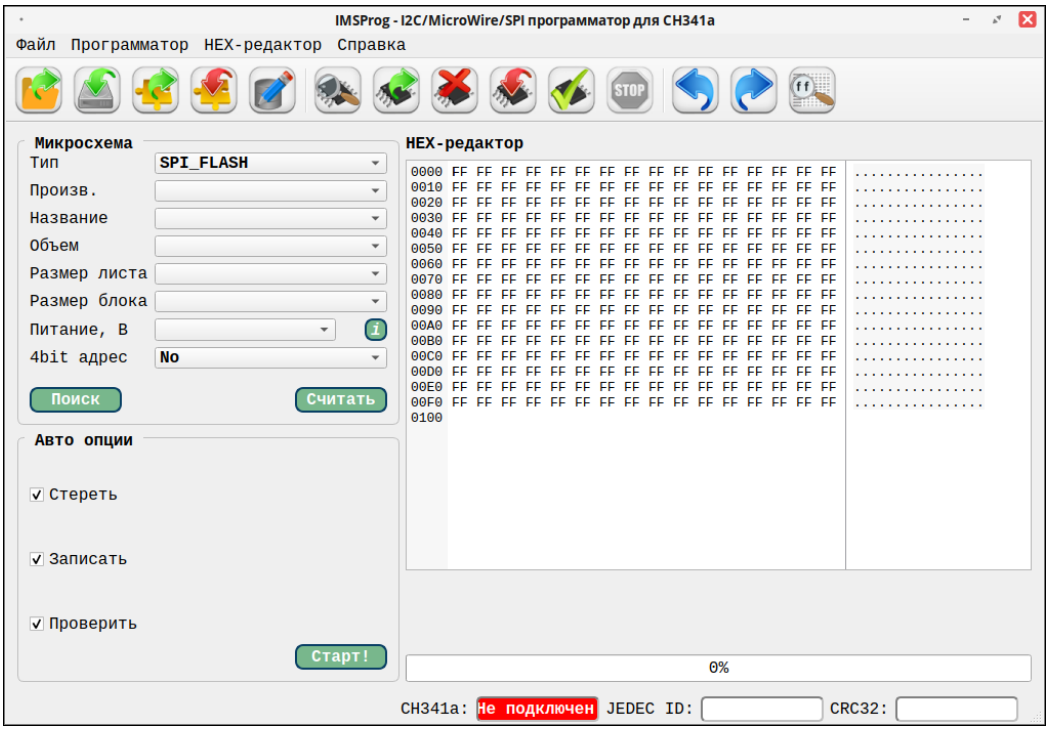
Для сборки редактора базы микросхем выполните последовательно ряд следующих команд:

```
cd IMSProg_editor
mkdir build
cd build
cmake ..
make -j4
sudo make install
```

Запуск программ будет доступен из «**Главного меню**» — «**Программирование**».

Программатор имеет название **IMSProg**, редактор параметров имеет название **IMSProg-редактор**.

Окно программатора выглядит следующим образом:



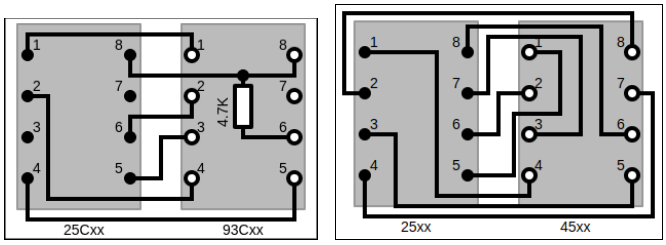
Подключение микросхем

Вставьте микросхему в соответствующий разъем программатора **CH341a**.

Микросхемы серий *24xxx* и *25xxx* должны быть вставлены непосредственно, в соответствии с маркировкой на печатной плате программатора **CH341a**. Микросхемы серии *M95xxx* устанавливаются как *25xxx*.

Микросхемы серии *93xxx* необходимо вставить в адаптер *93xxx*, а адаптер — в гнездо программатора с маркировкой *25xxx*.

Микросхемы *DataFlash* серии *AT45DBxxx* должны быть установлены в переходник **SOP-8 DIP-8**, который, в свою очередь, должен быть вставлен в адаптер *45xxx*. Адаптер *45xxx* устанавливается в гнездо программатора с маркировкой *25xxx*.



Если напряжение питания микросхемы составляет 1.8V, ее необходимо вставить в адаптер 1.8V, а адаптер — в нужное гнездо программатора.



Подключите программатор **CH341a** к USB-разъему компьютера и запустите программу IMSProg.

Подключать и отключать устройство (программатор **CH341a**) к порту USB можно в любое время, когда основные операции (чтение, проверка и программирование) не выполняются.

Выбор типа микросхемы

Выберите тип используемой микросхемы из выпадающего меню **Тип**. Доступны следующие типы микросхем:

- **SPI_FLASH** – при использовании микросхем SPI NOR FLASH серии *25xxx*;
- **24_EEPROM** – при использовании i2c EEPROM серии *24xxx*;
- **93_EEPROM** – при использовании MicroWire EEPROM серии *93xxx*;
- **25_EEROM** – при использовании SPI EEPROM;
- **95_EEPROM** – при использовании микросхем ST *M95xxx*.

При использовании микросхем SPI NOR FLASH серии *25xxx* и микросхем DataFlash серии *45xxx* будет доступна кнопка «Поиск» (), при нажатии на которую считывается информация JEDEC о микросхеме и загружаются все параметры этой микросхемы из базы данных. Любой параметр (объем микросхемы, размер страницы, размер блока, напряжение питания (VCC) или поддержка 4-битного адреса) может быть изменен вручную.

Вручную достаточно ввести данные выпадающего меню «Произв.» и «Название» – все остальные параметры будут автоматически загружены из базы данных микросхем.

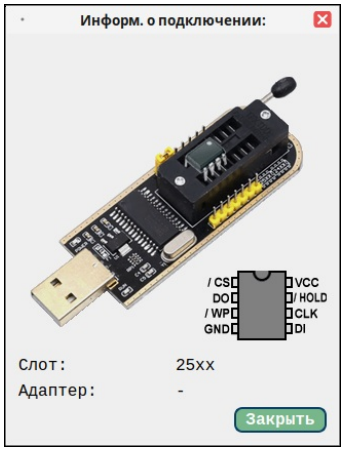
При использовании микросхем серий *24xxx, 25xxx* (не NOR FLASH), *95xxx* или *93xxx* необходимо вручную ввести данные всплывающего меню «Произв.» и «Название», поскольку для этих типов микросхем автоопределение не поддерживается. Все остальные параметры будут автоматически загружены из базы данных микросхем.

Основные операции программатора

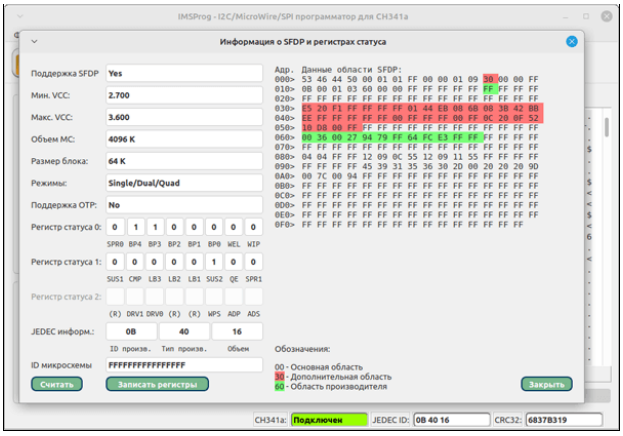
- Кнопка «Считать» () или сочетание клавиш *Ctrl+R* – вызывает функцию чтения данных из микросхемы в буфер компьютера;
- Кнопка  или сочетание клавиш *Ctrl+W* – вызывает функцию записи данных из буфера компьютера в микросхему;
- Кнопка  или сочетание клавиш *Ctrl+E* – приводит к стиранию всех данных микросхемы;
- Кнопка  или сочетание клавиш *Ctrl+T* – вызывает процесс побайтового сравнения данных в микросхеме и в буфере компьютера;
- Индикатор выполнения показывает ход выполнения операций чтения, стирания и проверки;
- Кнопка «**Старт!**» используется для последовательного выполнения операций стирания, записи и верификации. Если одна из этих

операций не нужна, можно снять флажок с чекбокса конкретной операции;

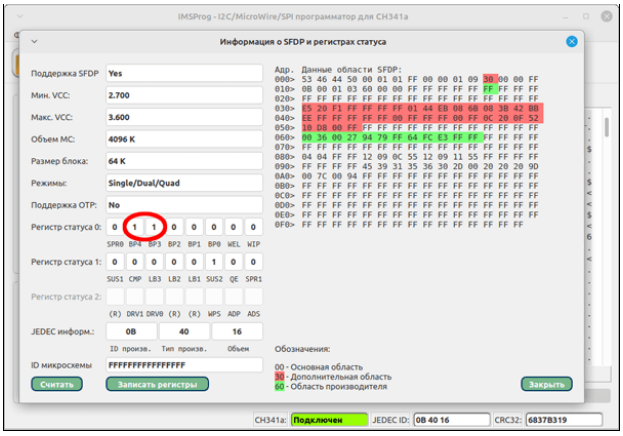
- Кнопка  или сочетание клавиш *Ctrl+I* – позволяет аварийно прервать операции чтения, записи, стирания или сравнения данных микросхемы;
- Кнопка «**i**» – выводит на экран информацию об используемом слоте и адаптере, необходимыми для работы с выбранной микросхемой.



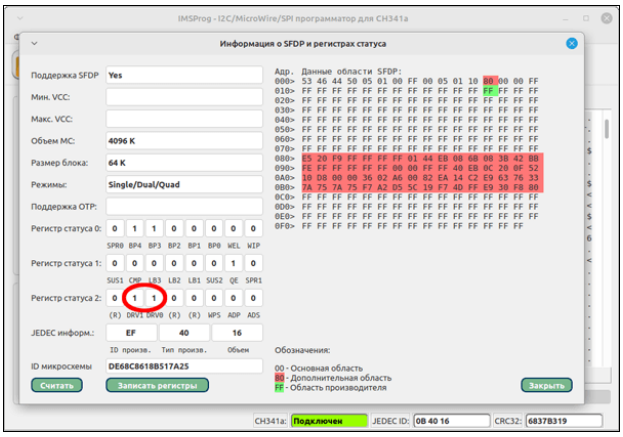
- Пункт меню «Программатор» – «Информ. о МС» или сочетание клавиш *Ctrl+P* служит для отображения и изменения регистров состояния, уникального серийного номера и области **e Serial Flash Discoverable Parameter (SFDP) SPI NOR Flash** микросхем. Эта информация может пригодиться при использовании микросхем, которых нет в базе, и для анализа проблем при ошибках записи.



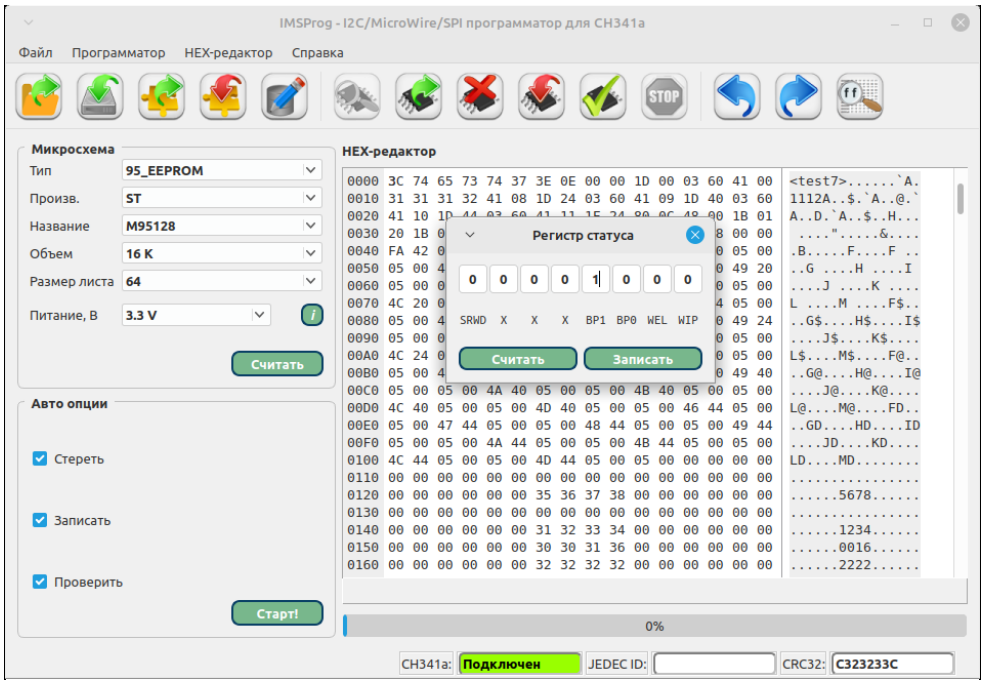
Если микросхема **SPI NOR FLASH** определяется нормально, но не читается (выдает сообщение вида «*Ошибка чтения сектора 0*»), возможно микросхема заблокирована. В этом случае в окне «Информ. о МС» измените биты **BP4** и **BP3** на нулевые и нажмите кнопку «Записать регистры». Затем повторите операцию чтения микросхемы.



Если микросхема **SPI NOR FLASH** считывается ненадежно (каждый раз с разной контрольной суммой) и в ней доступен «Регистр статуса 2», то можно изменить биты **DRV0** и **DRV1** на нулевые и нажать кнопку «Записать регистры». Это увеличит мощность выходного каскада выхода **DO** микросхемы. После этого повторить операцию чтения микросхемы.



Для микросхем серий *25xxx*, *95xxx*, у которых в есть только один регистр статуса, форма «Информ. о МС» выглядит следующим образом:



Операции с файлами

Кнопка  или сочетание клавиш *Ctrl+S* – используется для записи содержимого буфера компьютера в файл.

Кнопка  или сочетание клавиш *Ctrl+O* – используется для загрузки файла в буфер компьютера.

Кнопка  или сочетание клавиш *Ctrl+Shift-S* – используется для сохранения части компьютерного буфера в файл (необходимо ввести начальный адрес и длину части или конечный адрес). Эта операция может быть использована при разбиении двоичного образа данных на части.

Кнопка  или сочетание клавиш *Ctrl+Shift-O* – используется для загрузки небольшого файла по определенному адресу в буфере. При этом фрагмент данных в буфере будет заменен новыми данными из файла.

Кнопка  или сочетание клавиш *Ctrl+Q* – служит для вызова модуля редактора базы данных микросхем.

Операции с буфером (шестнадцатеричным редактором)

Шестнадцатеричный редактор микросхем (правая часть экрана) используется для отображения и изменения данных буфера.

Он содержит следующие элементы управления:

- Кнопка  или сочетание клавиш *Ctrl+Z* – отмена последней операции,

- Кнопка  или сочетание клавиш *Ctrl+Shift+Z* – повтор операции и
- Кнопка  или сочетание клавиш *Ctrl+F* – функция поиска/замены кода или строки.

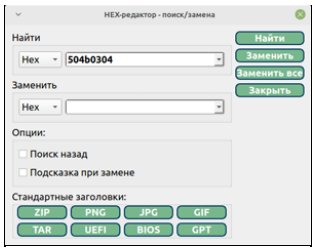
Сочетание клавиш *Ctrl+A* производит пересчет контрольной суммы буфера по алгоритму **CRC32**.

Сочетание клавиш *Ctrl+G* производит переход к просмотру кода по введенному шестнадцатеричному адресу.

Операции поиска и замены

Поиск и замену можно производить как шестнадцатиричного кода (опция **Hex** в выпадающем меню), так и текстовую информацию (**UTF-8** в выпадающем меню). Возможен поиск как вперед, так и назад.

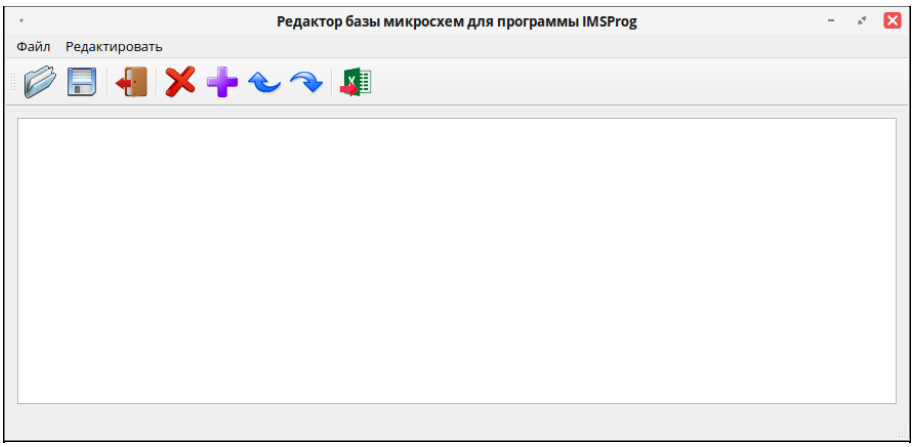
Для удобства поиска внизу формы есть панель «Стандартные заголовки». С помощью клавиш на этой панели поле поиска автоматически заполняется стандартными заголовками архивов, изображений или системных разделов.



Редактор базы микросхем

Редактор базы микросхем **IMSProg_editor** – это самостоятельная программа, которая может быть запущена как из «Главного меню» – «Программирование», так и из программатора IMSProg нажатием на кнопку  . Окно редактора параметров микросхем выглядит следующим образом:

Окно редактора параметров микросхем выглядит следующим образом:



Все операции в редакторе становятся доступными только после загрузки файла базы микросхем с расширением **.Dat**.

Далее будут рассмотрены основные действия для работы с программой.

Пункт меню «Файл»

Кнопка «Открыть» () или сочетание клавиш *Ctrl+O* – позволяет загрузить файл данных.

Кнопка «Сохранить» () или сочетание клавиш *Ctrl+S* – сохраняет таблицу параметров микросхем в файл базы данных.

Кнопка «Выход» () или сочетание клавиш *Ctrl+X* – выход из редактора.

Кнопка «Экспорт в CSV формат» () – позволяет выгрузить данные о микросхемах в формате CSV для дальнейшей обработки программой электронных таблиц – Libre Office Calc, Open Office Calc, Google Tables и т. д.

Кнопка «Импорт из CSV файла» () – загружает таблицу в формате CSV и добавляет данные из нее к существующим данным в

таблице.

Пункт меню «Редактировать»

Кнопка «Удалить строки» () или клавиша *Del* – удаляет одну или несколько строк.

Кнопка «Добавить строку» () или клавиша *Ins* – добавляет строку ниже выделенной и копирует все данные из выделенной строки в новую.

Кнопка «Переместить вверх» () или сочетание клавиш *Ctrl+Вверх* – перемещает выделенную строку вверх.

Кнопка «Переместить вниз» () или сочетание клавиш *Ctrl+Вниз* – перемещает выделенную строку вниз.

Кнопка «Импорт выделенных строк в CSV формат» () – сохраняет выделенные строки в файл формата CSV.

Наиболее свежую версию файла базы данных микросхем можно скачать с этой страницы как в формате **.Dat**, так и в формате **.csv**.

Список поддерживаемых микросхем

Тип микросхемы	Серия микросхем	
i2C EEPROM	24C01, 24C02, 24C04, 24C08, 24C16, 24C32, 24C64, 24C128, 24C256, 24C512, 24C1024	
MicroWire EEPROM	93C46, 93C56, 93C66, 93C76, 93C86	
Serial SPI Bus EEPROM	ST	M95010, M95020, M95040, M95080, M95160, M95320, M95640, M95128, M95256, M95512, M95M01, M95M02
	ATMEL	AT25010, AT25020, AT25040, AT25080, AT25160, AT25320, AT25640, AT25128, AT25256, AT25F512, AT25F1024, AT25F2048, AT25F4096
	MICROCHIP	25AA010, 25AA020, 25AA040, 25AA080, 25AA160, 25AA320, 25AA640, 25AA128, 25AA256, 25AAF512, 25AAF1024, 25LC010, 25LC020, 25LC040, 25LC080, 25LC160, 25LC320, 25LC640, 25LC128, 25LC256, 25LC512, 25LC1024
	ONSEMI	CAT25C01, CAT25C02, CAT25C04, CAT25C08, CAT25C16, CAT25C32, CAT25C64, CAT25C128, CAT25C256, CAT25C512
DataFlash 45xx	ATMEL	AT45DB011, AT45DB021, AT45DB041, AT45DB081, AT45DB161, AT45DB321
	ADESTO	AT45DB011, AT45DB021, AT45DB041, AT45DB081, AT45DB161, AT45DB321, AT45DB641
SPI NOR Flash	SPANSION	FL016AIF, S25FL016P, S25FL032P, FL064AIF, S25FL064P, S25FL256S, S25FL128P, S25FL129P, S25FL116K, S25FL132K, S25FL164K
	XTX	XT25F02E, XT25F04D, XT25F08B, XT25F16B, XT25F32F, XT25F64F, XT25F128F, XT25W02E, XT25W04D, XT25Q08D(1.8V), XT25Q16D(1.8V), XT25Q64D(1.8V), XT25F128D(1.8V)
	EON	EN25B10T, EN25B20T, EN25B40T, EN25B80T EN25B16T, EN25B32T, EN25B64T, EN25F64, EN25Q40A, EN25Q80B, EN25Q16, EN25Q32C, EN25Q64, EN25Q128, EN25F10A, EN25F20A, EN25F40, EN25F80, EN25F16, EN25F32, EN25S10A(1.8V), EN25S20A(1.8V), EN25S40A(1.8V), EN25S80B(1.8V), EN25S16B(1.8V), EN25S64A(1.8V), EN25QE32A, EN25E10A, EN25E40A, EN25SE16A(1.8V), EN25SE32A(1.8V), EN25T80, EN25QA32B, EN25QA64A, EN25QA128A, EN25QW16A, EN25QW32A, EN25QH16, EN25QH32B, EN25QH64A, EN25QH128A, EN25Q256, EN25QX64A, EN25QX128A, EN25QX256A, EN25QY256A, EN25SX64A(1.8V), EN25SX128A(1.8V)
	ATMEL	AT26DF161, AT25DF321
	MICRON	M25P10, M25P20, M25P40, M25P80, M25P016, M25P32, M25P64, M25P128, N25Q032A, N25Q064A, MT25QL64AB, N25Q128A, MT25QL128AB, N25Q256A, MT25QL256AB, MT25QL512AB, N25Q032A(1.8V), N25Q064A(1.8V), MT25QU64AB(1.8V), N25Q128A(1.8V), MT25QU128AB(1.8V), MT25QU256AB(1.8V), MT25QU512AB(1.8V)
	XMC	XM25QH10B, XM25QH20B, XM25QH40B, XM25QH80B, XM25QH16C, XM25QH32B, XM25QH64C, XM25QH128C, XM25QH256C, XM25QH512C, XM25LU64C(1.8V), XM25LU128C(1.8V), XM25QU256C(1.8V), XM25QU512C(1.8V), XM25QW16C, XM25QW32C, XM25QW64C, XM25QW128C, XM25QW256C, XM25QW512C, XM25QU41B(1.8V), XM25QU80B(1.8V), XM25QU16C(1.8V), XM25LU32C(1.8V), XM25QH32A, XM25QH64A, XM25QH128A
	AMIC	A25L10PU, A25L20PU, A25L40PU, A25L80PU, A25L16PU, A25L10PT, A25L20PT, A25L40PT, A25L80PT, A25L16PT, A25L010, A25L020, A25L040, A25L040, A25L080, A25L016, A25L032, A25LQ080, A25LQ16, A25LQ32, A25LQ64
	EXCELSEMI	ES25P10, ES25P20, ES25P40, ES25P80, ES25P16, ES25P32, ES25M40A, ES25M80A, ES25M16A
	DOUQI	DQ25Q64AS
	Zbit	ZB25LD10A(1.8V), ZB25LD20A(1.8V), ZB25LD40B(1.8V), ZB25LD80(1.8V), ZB25D10A, ZB25D20A, ZB25D40B, ZB25D80B, ZB25VQ16, ZB25VQ32, ZB25VQ64, ZB25VQ128, ZB25LQ16(1.8V), ZB25LQ32(1.8V), ZB25LQ64(1.8V), ZB25LQ128(1.8V), ZB25VQ20A, ZB25VQ40A, ZB25VQ80A, ZB25VQ16A
	ONSemi	LE25U20AMB, LE25U40CMC
	Boya	BY25Q05AW, BY25Q10AW, BY25Q20BL(1.8V), BY25Q40BL(1.8V), BY25Q80AW(1.8V), BY25Q16BL(1.8V), BY25D05AS, BY25D10AS, BY25D20AS, BY25D40AS, BY25Q80BS, BY25Q16BS, BY25Q32BS, BY25Q64AS, BY25Q128AS, BY25Q256ES, BY25Q10AL(1.8V), BY25Q20AL(1.8V), BY25Q40AL(1.8V), BY25Q32AL(1.8V), BY25Q64AL(1.8V), BY25Q128EL(1.8V)

PFLASH	Pm25LQ512B, Pm25LQ010B, Pm25LQ020B, PM25LQ016, PM25LQ032, PM25LQ064, PM25LQ128, Pm25LQ040B
Puya	P25Q06H, P25Q40H, P25Q11H, P25Q21H, P25Q10H, P25Q20H, P25Q40H, P25Q80H, P25Q16H, P25Q32H, P25Q64H, P25Q128H
ESMT	F25L004A, F25L008A, F25L016, F25L032, F25L064, F25L16QA, F25L32QA, F25L64QA
ISSI	IS25LQ010, IS25LQ020, IS25LP080D, IS25LP016D, IS25LP032D, IS25LP064D, IS25LP128F, IS25LP256D, IS25LP512D, IS25WP040D(1.8V), IS25WP080D(1.8V), IS25WP016D(1.8V), IS25WP032D(1.8V), IS25WP064D(1.8V), IS25WP128F(1.8V), IS25WP256D(1.8V), IS25WP512D(1.8V)
Fudan	FM25W04, FM25W16, FM25W32, FM25W64, FM25W128, FM25Q04, FM25Q08, FM25Q16, FS25Q32, FS25Q64, FS25Q128
Zetta	ZD25Q64B, ZD25LQ128(1.8V), ZD25LQ64(1.8V), ZD25WD20B, ZD25WD40B, ZD25Q80C, ZD25Q16B, ZD25Q32C
PCT	PCT25VF016B, PCT25VF032B, PCT25VF064C, PCT25VF020B, PCT25VF040B, PCT25VF080B, PCT26VF016, PCT26VF032, PCT25VF010A
MXIC	MX25L8005M, MX25L1605D, MX25L3205D, MX25L6405D, MX25L12805D, MX25L25635E, MX25L51245G, MX25U5121E(1.8V), MX25U1001E(1.8V), MX25U2035F(1.8V), MX25U4035F(1.8V), MX25U80356(1.8V), MX25U1632F(1.8V), MX25U3232F(1.8V), MX25U6432F(1.8V), MX25U12832F(1.8V), MX25U25643G(1.8V), MX25U51245G(1.8V), MX25R2035F, MX25R4035F, MX25R8035F, MX25R1635F, MX25R3235F, MX25R6435F
GigaDevice	GD25F40, GD25F80, GD25D40, GD25D80, GD25D05C, GD25D10C, GD25Q20C, GD25Q40C, GD25Q80C, GD25Q16C, GD25Q32, GD25Q64CSIG, GD25Q128CSIG, GD25Q256CSIG, GD25LD05C(1.8V), GD25LD10C(1.8V), GD25LD20C(1.8V), GD25LD40C(1.8V), GD25LQ80C(1.8V), GD25LQ16C(1.8V), GD25LQ32E(1.8V), GD25LQ64E(1.8V), GD25LQ128(1.8V), GD25LQ256D(1.8V), GD25WD05C, GD25WD10C, GD25WD20E, GD25WD40E, GD25WD80C, GD25WQ20E, GD25WQ40E, GD25WQ80E, GD25WQ16E, GD25WQ32E, GD25WQ64E, GD25WQ128E, GD25WB256E, GD25LB512ME(1.8V), YC25Q128
PARAGON	PN25F08, PN25F16, PN25F32, PN25F64, PN25F128
WINBOND	W25P80, W25P16, W25P32, W25X05, W25X10, W25X20, W25X40, W25X80, W25X16, W25X32VS, W25X64, W25Q20CL, W25Q40BV, W25Q80BL, W25Q16DV, W25Q32BV, W25Q64BV, W25Q128BV, W25Q256FV, W25Q20BW(1.8V), W25Q80, W25Q10EW(1.8V), W25Q20EW(1.8V), W25Q40EW(1.8V), W25Q80EW(1.8V), W25Q16JW(1.8V), W25Q32FW(1.8V), W25Q64DW(1.8V), W25Q128FW(1.8V), W25Q256JW(1.8V), W25M512JW(1.8V), W25Q512JV, W25M512JV, W25Q32JW(1.8V)
Fidelix	FM25Q04A, FM25Q08A, FM25Q16A, FM25Q32A, FM25Q64A, FM25Q128A, FM25M04A(1.8V), FM25M08A(1.8V) FM25M16A(1.8V), FM25M32B(1.8V), FM25M64A(1.8V)

Подключение принтеров HP

Установка принтеров HP с помощью HPLIP

HPLIP (**HP** **L**inux **I**maging and **P**rinting) предоставляет драйвера для принтеров HP. Также он включает в себя **поддержку сканера** и факса. **HPLIP** рекомендуется для большинства принтеров **HP inkjet** и **laserjet**. Список поддерживаемого оборудования представлен по ссылке.

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

1. Для установки **hplip** перейдите в сеанс пользователя **root**:

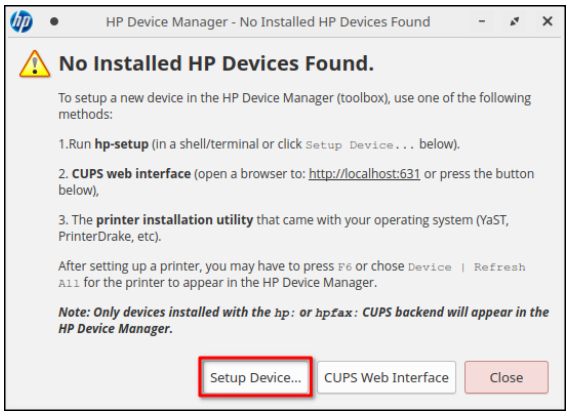
```
su -
```

и выполните команду:

```
dnf install hplip-gui python3-distro
```

2. После установки программа будет доступна из «**Главного меню**» – «**Администрирование**» – «**HP Device Manager**» (или «**Управление устройствами HP**»).

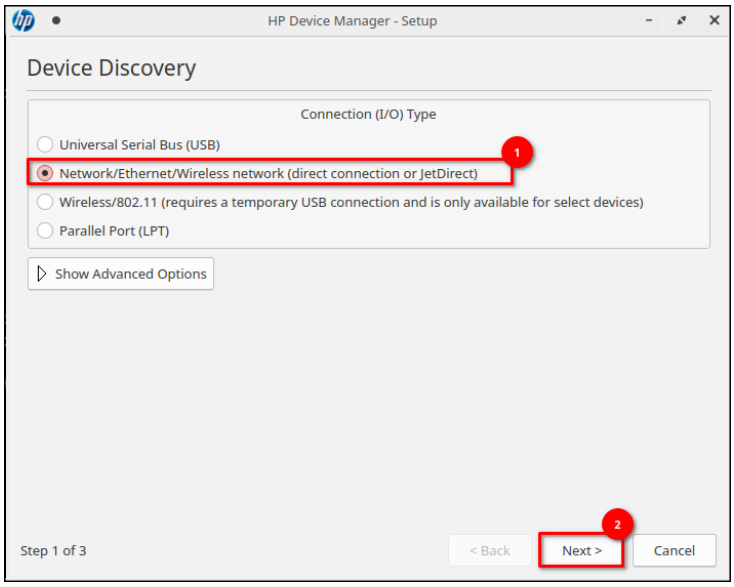
3. Далее выберите **Setup Device...**



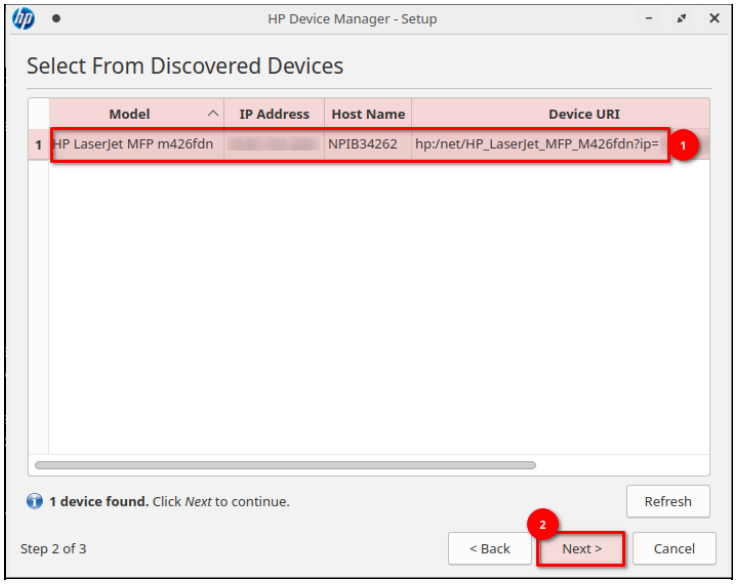
4. Выберите способ подключения принтера.

Если это *USB-принтер*, нажмите **Далее**.

Если *сетевой* – выберите второй пункт (**Network/Ethernet/Wireless network**).



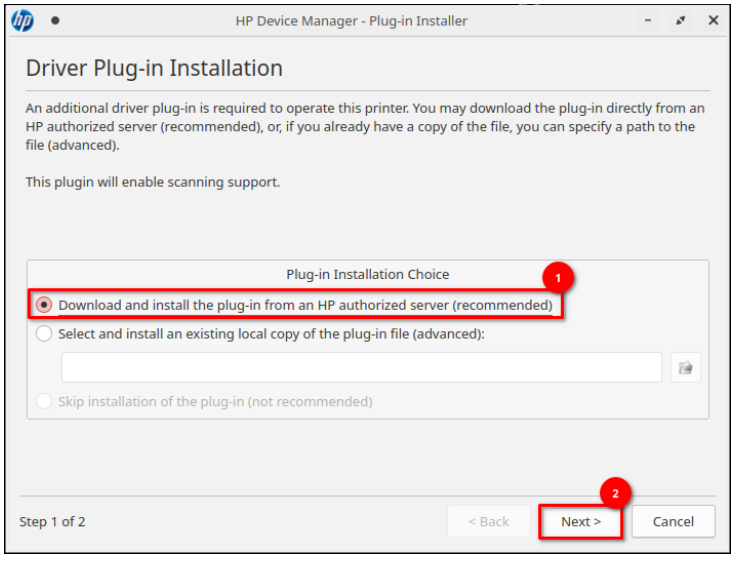
5. В случае с *сетевым* принтером выберите необходимый из списка найденных.



6. Установите плагин.

Запустите команду установки плагина:

```
/usr/bin/hp-plugin
```



В случае возникновения ошибки загрузки плагина, его можно скачать самостоятельно и применить, выбрав второй пункт.

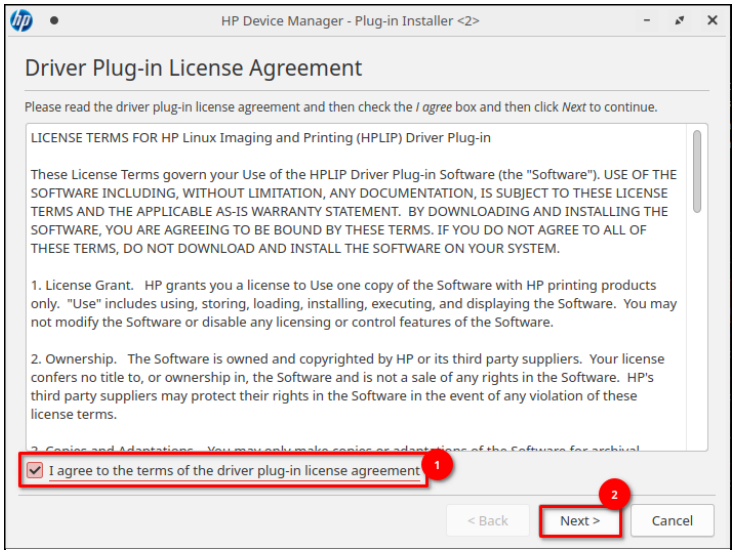
Скачать плагин можно по этой или этой ссылке.

Его версия должна совпадать с версией **hplip**, которая показана в **HP Device Manager** в меню **Help - About**. При обновлении **hplip** необходимо установить соответствующую версию плагина командой:.

```
hp-plugin
```

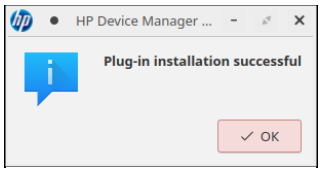
Затем выберите файл плагина в окне установки плагина **hp**.

7. Примите лицензионное соглашение.

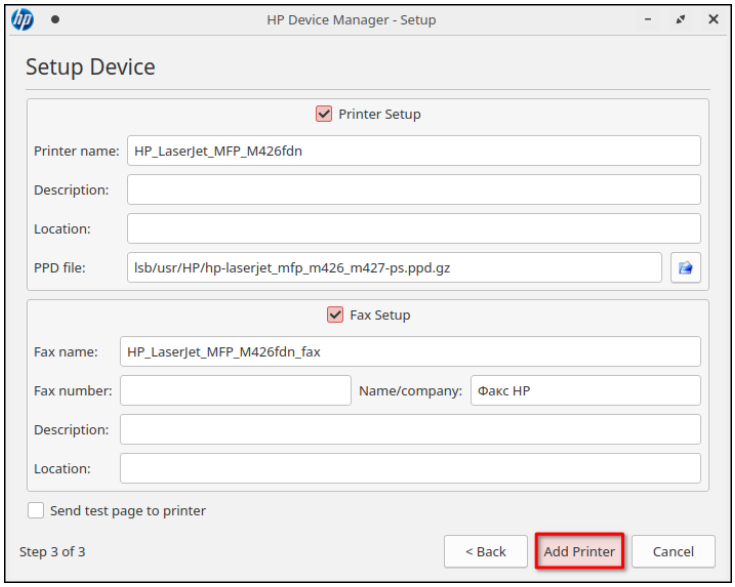


8. Введите пароль пользователя **root** во всплывающем окне.

9. Если после этого появилось окно, как на картинке ниже, то плагин **hplip** установлен успешно. Нажмите «**OK**».

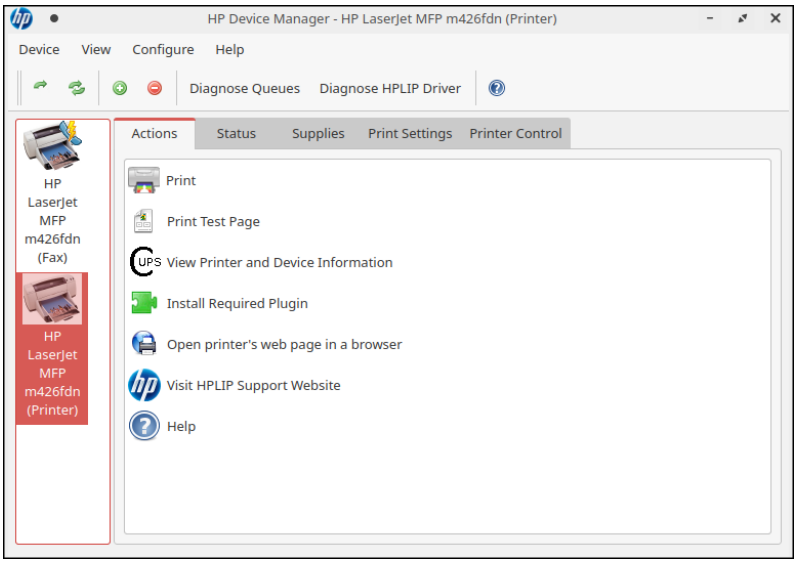


10. Нажмите «**Add Printer**».



11. Далее во всплывающем окне введите пользователя **root** и его **пароль**.

12. Принтер установлен и его видно в окне **HP Device Manager**.



13. Установите плагины для принтера **HP** в приложении **HP Device Manager**, выбрав на вкладке **Action** пункт "**Install required Plugin**" или запустив от **локального** пользователя команду hp-plugin.

ВАЖНО!

Есть список принтеров / МФУ, с которыми могут быть проблемы после установки:

HP LaserJet P2035
HP LaserJet Pro P1606dn
HP LaserJet Pro P1566
HP LaserJet Pro P1102
HP LaserJet Pro M12a
HP LaserJet Pro M12w
HP LaserJet Pro P1102w
HP LaserJet Pro CP1025nw
HP LaserJet 1022
HP LaserJet 1022n
HP LaserJet 1022nw
HP LaserJet 1020
HP LaserJet 1018
HP LaserJet 1005
HP LaserJet 1000
HP LaserJet P1005
HP LaserJet P1006
HP LaserJet P1007
HP LaserJet P1008
HP LaserJet P1505/P1505n
HP LaserJet P2014/P2014n
HP LaserJet M1005 MFP
HP LaserJet M1120 MFP
HP LaserJet Pro M1132s MFP
HP LaserJet Pro M1212nf MFP

Решаются такие проблемы следующим образом:

1) Войдите в систему как **root** (можно сделать и в консольном окне MATE/Cinnamon).

2) Удалите пакет system-config-printer-udev:

```
dnf remove system-config-printer-udev
```

3) В папке **/etc/udev/rules.d** создайте файл, например, «**60-hp_brainless.rules**», где пропишите следующее правило для менеджера устройств **udev**. Данное правило будет запускать команду загрузки **firmware** по наступлении события «**Включение принтера**»:

```
ACTION!="add", GOTO="skip_hp"
SUBSYSTEM!="usb", GOTO="skip_hp"
ATTRS{idVendor}=="03f0", ATTRS{idProduct}=="2b17", ATTRS{dev}=="*", RUN+="hp-firmware  -n --
device=hp:/usb/HP_LaserJet_1020?serial=FN1DNNJ"
LABEL="skip_hp"
```

Здесь **idVendor** и **idProduct** указаны для **HP LaserJet 1020**, если у вас другая модель, то эти значения можно узнать в выводе команды `lsusb`.

Значение параметра **--device** так же приведено в качестве примера. Для вашего принтера, подключенного к ПК, вы сможете получить его из вывода команды `lpinfo -v`.

В позиции аргументов утилиты `hp-firmware` укажите значения для Вашего принтера и укажите обязательно неинтерактивный режим (подробнее об этой команде и её опциях см. здесь).

4) Обязательно перезапустите менеджер **udev** следующими командами:

```
udevadm control --reload-rules
udevadm trigger
```

Подключение принтеров Canon

Автоматическая установка драйвера
Ручная установка драйвера
Регистрация принтера в спулере печати
Мониторинг состояния принтера

Для принтеров: LBP112, LBP113w, LBP151dw, LBP6030, LBP6030B, LBP6030w, LBP6230dw, LBP7100Cn, LBP7110Cw используйте драйвер UFRII LT, который доступен по ссылке.

Для серий Canon i-SENSYS, imagePRESS, imageRUNNER, iR драйвер доступен по ссылке.

Для принтера модели Canon imageRUNNER 1133A драйвер доступен по ссылке. При установке выберите модель Canon-MFP5800 Series UFRII LT.

Для установки драйвера скачайте, распакуйте его и перейдите в распакованный каталог.

В терминале запустите скрипт установки install.sh и следуйте инструкциям инсталлятора.

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Автоматическая установка драйвера

Для автоматической установки принтера Canon воспользуйтесь драйвером по ссылке. Архив **canon.zip** содержит интерактивный скрипт установки принтера.

Скачайте архив с драйвером и распакуйте его командой:

```
unzip canon.zip
```

Перейдите в распакованный каталог и от пользователя **root** выполните запуск скрипта автоматической настройки:

```
./canon-install.sh
```

Ручная установка драйвера

Ниже рассмотрен вариант ручной установки драйвера **версии 2.71** для принтеров Canon **серии LBP**. Поддерживаемые модели представлены в таблице. Драйвер доступен по ссылке. Архив **canon.zip** содержит интерактивный скрипт установки принтера, запустите его от пользователя **root**.

Поддерживаемые модели принтеров:

Принтер	Название файла PPD
LBP1120	CNCUPSLBP1120CAPTK.ppd
LBP1210	CNCUPSLBP1210CAPTK.ppd
LBP2900	CNCUPSLBP2900CAPTK.ppd
LBP3000	CNCUPSLBP3000CAPTK.ppd
LBP3050	CNCUPSLBP3050CAPTK.ppd
LBP3018	CNCUPSLBP3050CAPTK.ppd
LBP3010	CNCUPSLBP3050CAPTK.ppd
LBP3150	CNCUPSLBP3150CAPTK.ppd
LBP3108	CNCUPSLBP3150CAPTK.ppd
LBP3100	CNCUPSLBP3150CAPTK.ppd

LBP3200	CNCUPSLBP3200CAPTK.ppd
LBP3210	CNCUPSLBP3210CAPTK.ppd
LBP3250	CNCUPSLBP3250CAPTK.ppd
LBP3300	CNCUPSLBP3300CAPTK.ppd
LBP3310	CNCUPSLBP3310CAPTK.ppd
LBP3500	CNCUPSLBP3500CAPTK.ppd
LBP5000	CNCUPSLBP5000CAPTK.ppd
LBP5050	CNCUPSLBP5050CAPTK.ppd
LBP5100	CNCUPSLBP5100CAPTK.ppd
LBP5300	CNCUPSLBP5300CAPTK.ppd
LBP6018	CNCUPSLBP6018CAPTK.ppd
LBP6000	CNCUPSLBP6018CAPTK.ppd
LBP6020	CNCUPSLBP6020CAPTK.ppd
LBP6200d	CNCUPSLBP6200CAPTK.ppd
LBP6300dn	CNCUPSLBP6300CAPTK.ppd
LBP7200C	CNCUPSLBP7200CCAPTK.ppd
LBP9100Cdn	CNCUPSLBP9100CCAPTK.ppd

Выполните удаление system-config-printer-udev, поскольку в некоторых случаях автоматически добавленный принтер работает некорректно:

```
dnf remove system-config-printer-udev
```

Перейдите в каталог с загруженным архивом и выполните распаковку:

```
unzip canon.zip
```

Перейдите в каталог **canon** и выполните установку пакетов командой:

```
dnf localinstall cnd*
```

Регистрация принтера в спулере печати

Данные для команды возьмите из приведенной выше таблицы.

Команда для установки принтера **LBP2900**:

```
sudo lpadmin -p LBP2900 -m CNCUPSLBP2900CAPTK.ppd -v ccp://localhost:59687 -E
```

Для регистрации в системе определите адрес принтера:

```
sudo dmesg | grep printer
```

Вывод команды:

```
5.876692] usblp 1-10:1.0: usblp0: USB Bidirectional printer dev 7 if 0 alt 0 proto 2 vid 0x04A9 pid 0x2676
```

Обратите внимание на значение (в данном случае **0**) после **usblp** в строке вывода.

```
sudo /usr/sbin/ccpdadmin -p LBP2900 -o /dev/usb/lp0
```

LBP2900 — название принтера, указанное в таблице, представленной ранее. Пожалуйста, укажите название вашего принтера.

При этом в файле **/etc/ccpd.conf** появится запись:

```
<Printer LBP2900>
```

```
DevicePath /dev/usb/lp0
</Printer>
```

Для настройки нового сервиса ccpd создайте файл **/etc/systemd/system/ccpd.service** со следующим содержимым:

```
[Unit]
Description=CCPD Printing Daemon
After=cups.service
[Service]
Type=forking
ExecStart=/usr/sbin/ccpd
TimeoutSec=5
[Install]
WantedBy=multi-user.target
```

Удалите старый сервис:

```
rm -f /etc/rc.d/init.d/ccpd
```

Перезагрузите **systemd** с поиском новых юнитов и перезапустите сервисы **ccpd** и **cups**:

```
systemctl daemon-reload
systemctl restart ccpd cups
```

Добавьте в автозагрузку **ccpd**:

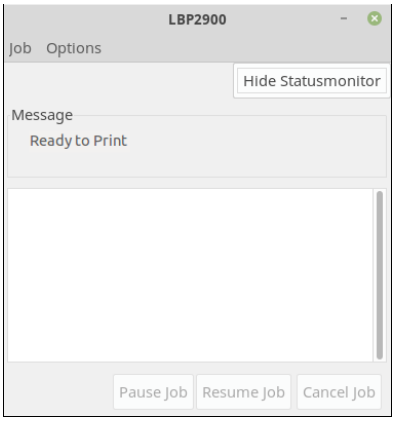
```
systemctl enable ccpd
```

Мониторинг состояния принтера

Просмотреть статус принтера можно с помощью команды:

```
captstatusui -P LBP2900
```

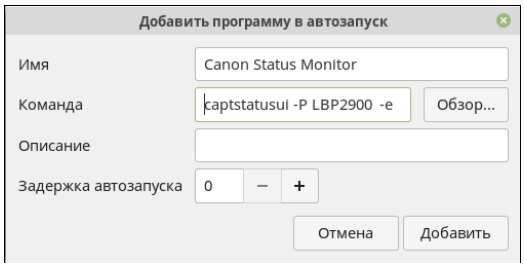
После появления окна с надписью "Ready to Print" принтер будет готов к работе.



Для появления монитора состояния только при возникновении проблемы добавьте в автозагрузку команду:

```
captstatusui -P LBP2900 -e
```

Для добавления в автозагрузку в **MATE** перейдите в «**Главное меню**» — «**Параметры**» — «**Запуск приложений**», нажмите на кнопку «**Custom Add**» и в поле **"Команда"** впишите captstatusui -P LBP2900 -e.



Опция **-e** указывает, что окно статуса не будет показываться до тех пор, пока не случится ошибка.

Также можно создать пользовательскую кнопку на рабочем столе, в команде запуска кнопки пропишите `captstatusui -P LBP2900`, данная настройка позволит пользователю управлять задачами печати: **"Resume job"**, **"Cancel Job"**. Например, после замены бумаги в лотке принтера, нажмите кнопку **"Resume job"** для возобновления печати.

Установка драйверов Pantum

Драйверы **Pantum** необходимы для начала работы на принтерах фирмы *Pantum*.

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки пакетов сначала необходимо установить пакет redos-3rdparty-pantum. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install redos-3rdparty-pantum
```

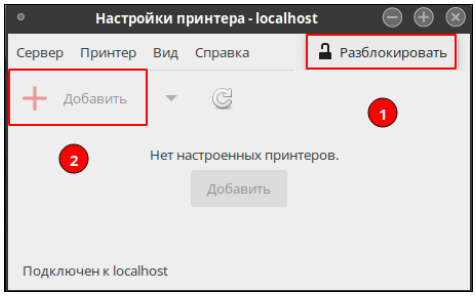
В результате будет подключен новый репозиторий **3rdparty-pantum**.

Далее необходимо установить пакеты с драйверами:

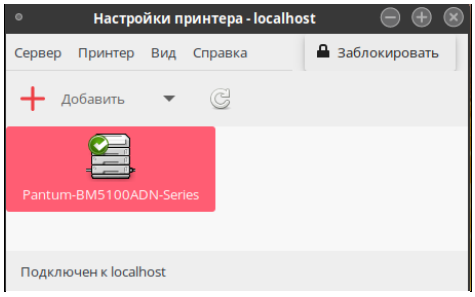
```
dnf install pantum-drivers-cups pantum-drivers-sane --refresh
```

После успешной установки драйверов необходимо подключить принтер. Сделать это можно через «**Главное меню**» - «**Администрирование**» - «**Настройки принтера**».

Для работы с программой необходимо нажать **Разблокировать**, потребуется ввести пароль администратора или суперпользователя (**root**) системы. После аутентификации добавьте новое устройство, нажав кнопку **Добавить**.

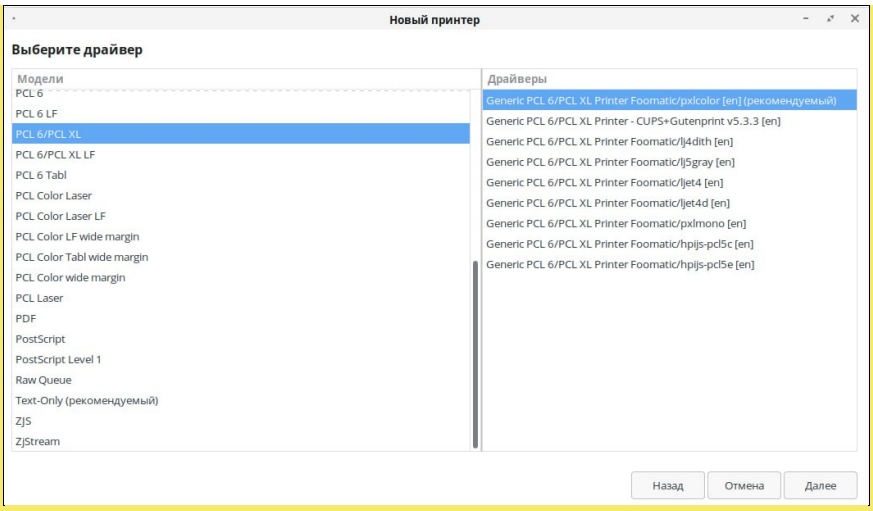


Если все настроено верно, принтер будет добавлен и готов к работе.



Примечание.

Если принтер не работает с родными драйверами, стоит попробовать использовать **Generic**. Для этого нажмите кнопку «**Добавить**», выберите устройство и нажмите «**Далее**», будет открыто окно для выбора необходимого драйвера. Выберите **Generic** и определите необходимую модель. После этого укажите описание принтера и нажмите кнопку «**Применить**».


Новый принтер
Выберите драйвер
Модели
PCL 6
PCL 6 LF
PCL 6/PCL XL
PCL 6/PCL XL LF
PCL 6 Tabl
PCL Color Laser
PCL Color Laser LF
PCL Color LF wide margin
PCL Color Tabl wide margin
PCL Color wide margin
PCL Laser
PDF
PostScript
PostScript Level 1
Raw Queue
Text-Only (рекомендуемый)
ZJS
ZjStream
Драйверы
Generic PCL 6/PCL XL Printer Foomatic/pxlcolor [en] (рекомендуемый)
Generic PCL 6/PCL XL Printer - CUPS+Gutenprint v5.3.3 [en]
Generic PCL 6/PCL XL Printer Foomatic/lj4dith [en]
Generic PCL 6/PCL XL Printer Foomatic/lj5gray [en]
Generic PCL 6/PCL XL Printer Foomatic/ljet4 [en]
Generic PCL 6/PCL XL Printer Foomatic/ljet4d [en]
Generic PCL 6/PCL XL Printer Foomatic/pxlmono [en]
Generic PCL 6/PCL XL Printer Foomatic/hpijs-pcl5c [en]
Generic PCL 6/PCL XL Printer Foomatic/hpijs-pcl5e [en]
Назад
Отмена
Далее

Настройка cups

Настройка возможности сбора аудита с серверов печати
Настройка централизованного назначения группам пользователей устройств печати
Копирование печатаемых файлов
Журналирование печати

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка возможности сбора аудита с серверов печати

По умолчанию логи работы Cups отправляются в syslog. Для того, что бы логи Cups стали доступны в панели администрирования Cups (по умолчанию панель администрирования Cups находится по адресу http://localhost:631/), требуется изменить файл:

```
nano /etc/cups/cups-files.conf
```

Приводим строки к виду:

```
ErrorLog /var/log/cups/error_log
PageLog /var/log/cups/page_log
AccessLog /var/log/cups/access_log
```

Добавьте в файл **/etc/cups/cupsd.conf** параметр **PageLogFormat**:

```
nano /etc/cups/cupsd.conf
```

```
PageLogFormat %p %u %j %T %P %C %{job-billing} %{job-originating-host-name} %{job-name} %{media} %{sides}
```

И измените значение **LogLevel**:

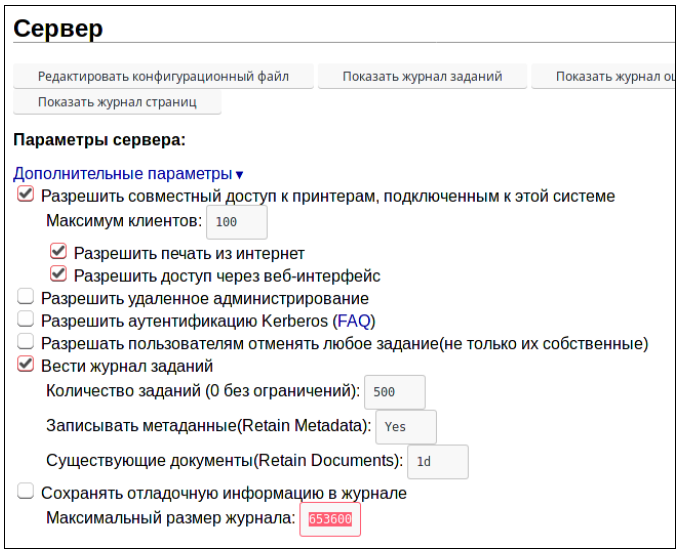
```
LogLevel info
```

Описание возможных уровней ведения лога:

- **debug2** - записывать все;
- **debug** - записывать почти все;
- **info** - записывать все запросы и изменения состояния;
- **warn** - запись ошибок и предупреждений;
- **error** - запись только ошибок;
- **none** - ничего не записывать.

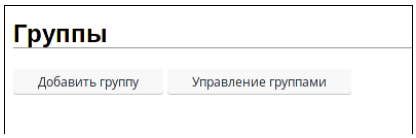
В параметре (**MaxLogSize**), отвечающем за максимальный размер файла, измените значение с "**0**" на нужное.

Пример настроек через веб-интерфейс http://localhost:631/ :



Настройка централизованного назначения группам пользователей устройств печати

Создайте группу:

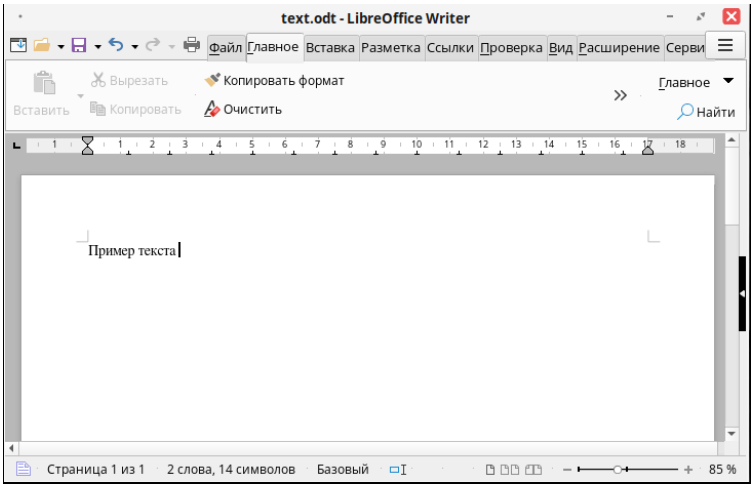


После создания группы нажмите "**Управление группами**", в выпадающем списке "**Администрирование**" выберите список разрешенных пользователей.

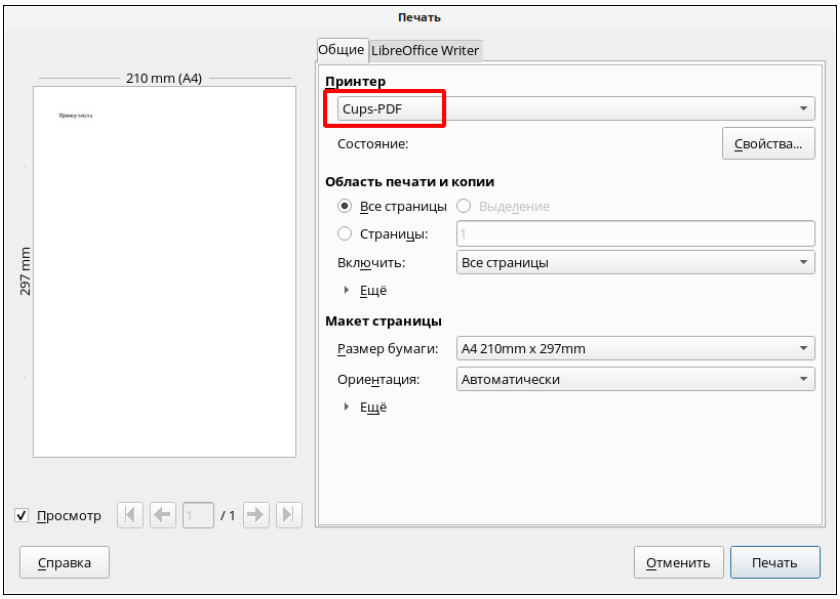
Впишите нужных пользователей, которым требуется разрешить доступ к группе устройств.

Копирование печатаемых файлов

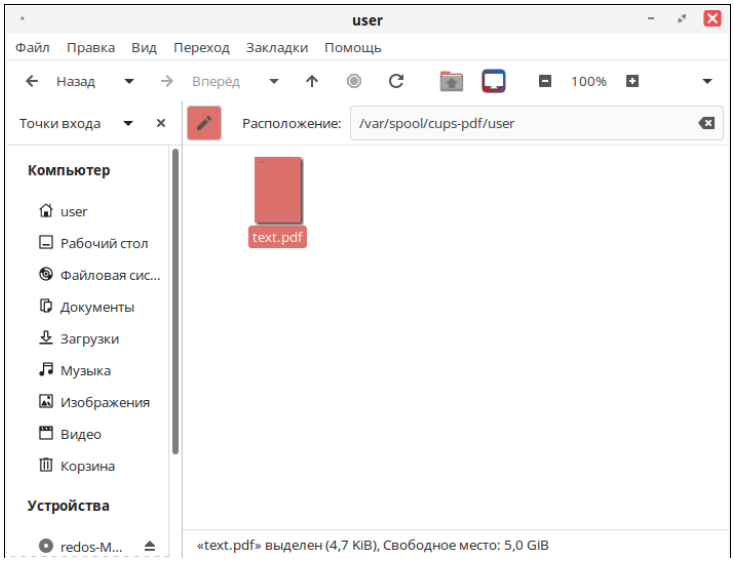
В РЕД ОС поддерживается функция теневого копирования файлов при использовании системы печати **CUPS**.



В примере будет использоваться виртуальный принтер **Cups-PDF** для наглядной демонстрации печати, а также расположения печатаемого файла и его копии.



По умолчанию распечатанный с помощью виртуального принтера файл отправляется в каталог **/var/spool/cups-pdf/<имя_пользователя>/**.



Распечатанный на обычном принтере файл будет располагаться в каталоге **/var/spool/<имя_принтера>/<имя_пользователя>/**.

Также, при использовании принтера, сервис **CUPS** автоматически создает рабочие файлы в каталоге **/var/spool/cups/**. Для доступа к данному каталогу требуются права суперпользователя. Проверку прав доступа можно осуществить командой:

```
ls -l /var/spool/ | grep "cups"

drwx--x---. 3 root lp 4096 апр 12 13:09 cups
drwxr-xr-x. 4 root root 4096 апр 12 13:09 cups-pdf
```

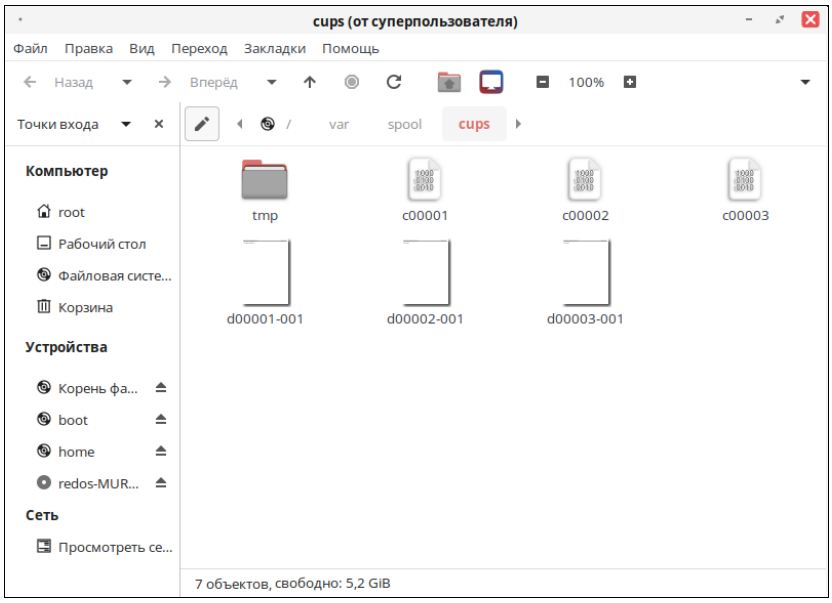
В каталоге хранятся файлы двух типов:

- **управляющие файлы**, начинающиеся на «**c**» («c00001», «c99999», «c100000» и т. д.);
- **файлы данных**, начинающиеся на «**d**» («d00001-001», «d99999-001», «d100000-001» и т. д.).

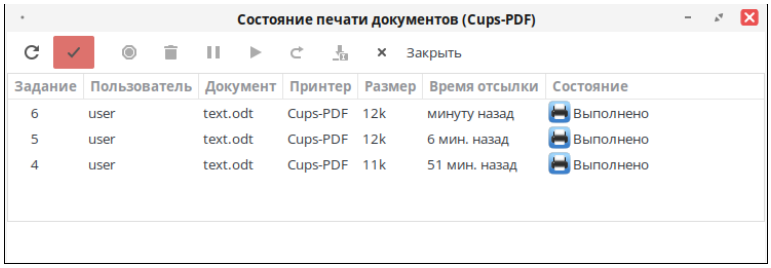
В именах файлов указывается **ID задания** из очереди печати, в данном случае задание имеет порядковый номер 1 — [d **00001**-001], и **ID принтера**, с которого производилась печать файла, в данном случае ID принтера — 1 [d00001- **001**].

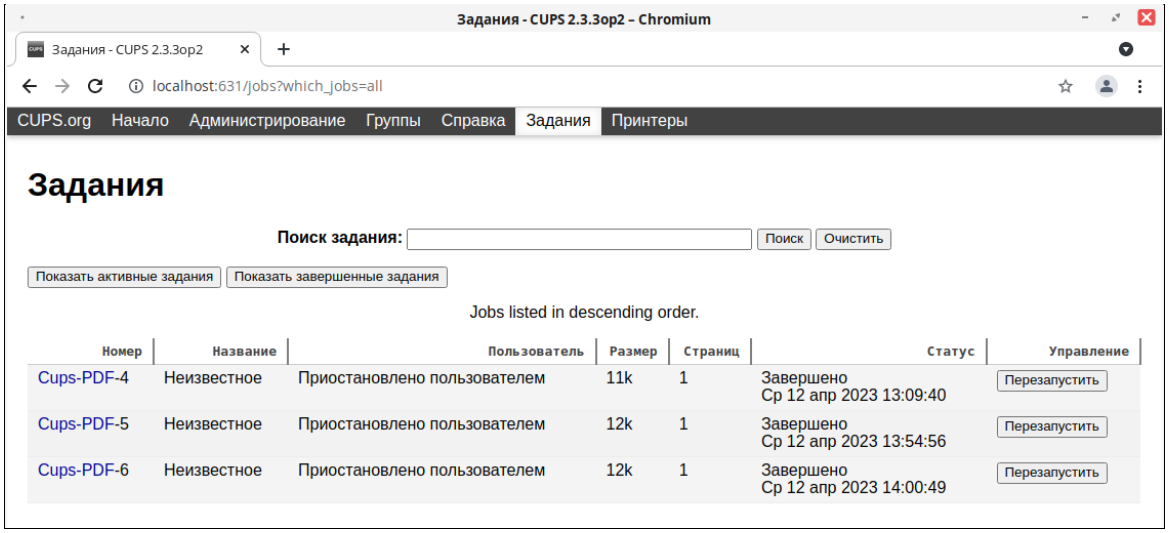
Управляющие файлы представляют собой сообщения, передаваемые принтеру с командами для печати, а файлы данных — это исходные файлы печати, отправленные на печать.

Файлы управления обычно очищаются после отправки 500-го задания, а файлы данных удаляются сразу после успешной печати задания.



Узнать ID заданий или процессов можно как локально в настройках CUPS системы, так и с помощью веб-формы.





Журналирование печати

В системе предусмотрено автоматическое журналирование печатаемых файлов. Активные и завершенные задания можно посмотреть в веб-интерфейсе во вкладке «**Задания**» (см. рисунок выше) или с помощью консольных команд:

- для завершенных заданий:

```
lpstat -W completed
```

- для незавершенных заданий:

```
lpstat -W not-completed
```

В выводе отображаются данные вида:

```
<принтер>-<ID_документа>-<пользователь>-<размер>-<дата>:<время>
```

Например:

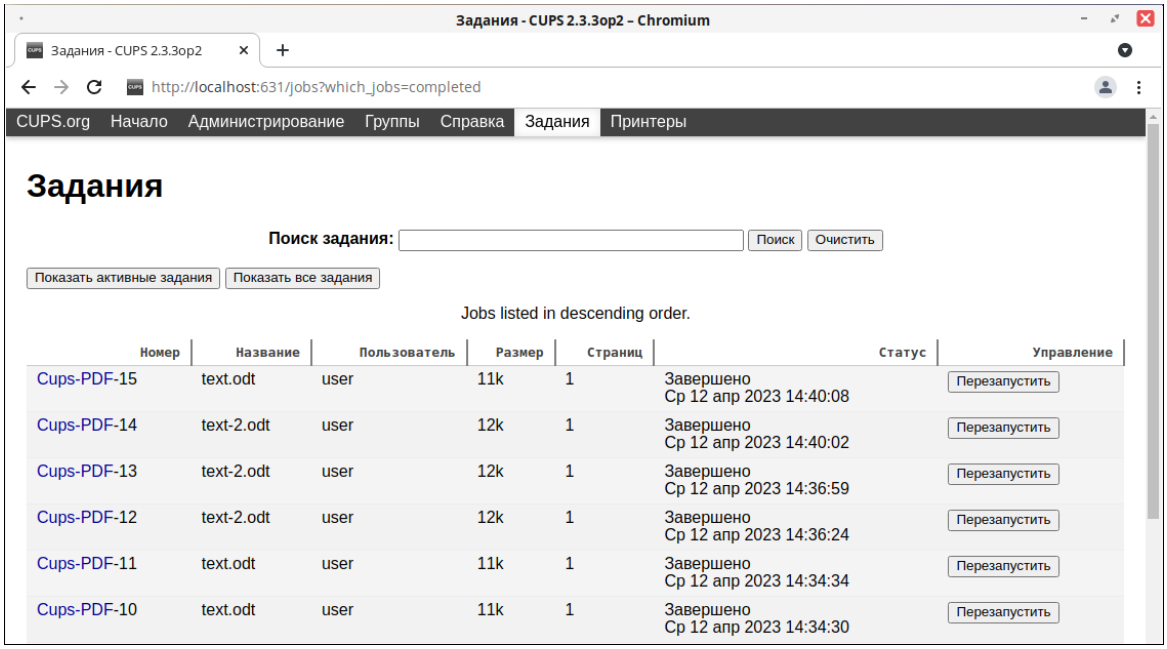
```
lpstat -W completed

Cups-PDF-7          user        12288   Ср 12 апр 2023 14:27:26
Cups-PDF-6          user        12288   Ср 12 апр 2023 14:00:49
Cups-PDF-5          user        12288   Ср 12 апр 2023 13:54:56
Cups-PDF-4          user        11264   Ср 12 апр 2023 13:09:40
```

Для приведения веб-интерфейса в более упорядоченный вид и демонстрации названия документа необходимо внести изменения в настройки **CUPS** — в файл конфигурации **/etc/cups/cupsd.conf**, например, изменив значения параметров JobPrivateAccess и JobPrivateValues в секции **<Policy default>** на указанные:

```
# Set the default printer/job policies...
<Policy default>
JobPrivateAccess all
JobPrivateValues none
```

Для принятия изменений необходимо перезагрузить систему.

После перезагрузки список заданий будет отображаться следующим образом:



Подключение сетевого принтера по IPP

Подключение сетевого принтера в конфигурации РЕД ОС - РЕД ОС
Отключение автоматического отображения сетевых принтеров

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

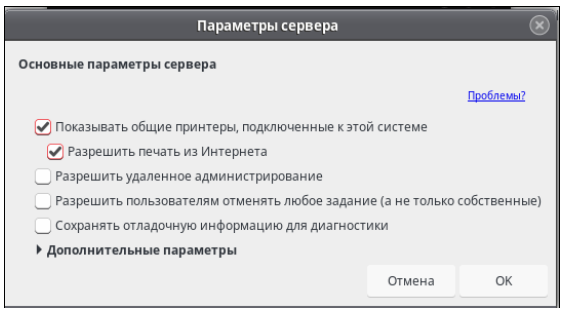
Подключение сетевого принтера в конфигурации РЕД ОС - РЕД ОС

1) Настройка ПК, к которому подключен принтер по **USB**.

Откройте управление принтерами: Меню - "Администрирование" - "Настройки принтера".

Принтер уже должен быть добавлен в качестве локального.

Далее требуется зайти в "Сервер" - "Параметры" и выставить флаги:



Далее требуется отредактировать конфигурационный файл. Откройте файл:

```
sudo nano /etc/cups/cupsd.conf
```

приведите строку к виду:

```
BrowseLocalProtocols dnssd cups
```

Перезапустите службу:

```
sudo systemctl restart cups
```

2) Настройка ПК, на котором будет совершаться подключение сетевого принтера:

Сначала проверьте доступ к **631** порту ПК, к которому будет подключение:

```
nmap -Pn -p 631 ip_adress
```

если утилита отсутствует, то выполните установку:

```
sudo dnf install nmap
```

ключевая фраза, которая интересует из вывода команды:

```
631/tcp open ipp
```

Далее требуется установить утилиту (если отсутствует):

```
sudo dnf install cups-ipptool
```

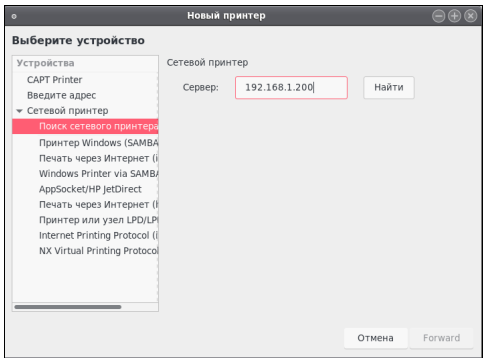
Перезапустите службу:

```
systemctl restart cups
```

Далее добавление принтера на клиентском компьютере.

Откройте: Меню - "Администрирование" - "Настройки принтера"

Нажмите "Добавить". "Network Printer" - "Find Network Printer" и введите IP-адрес ПК, к которому подключен принтер через usb.



Нажмите кнопку "Найти". После добавления принтера выполните печать тестовой страницы.

Отключение автоматического отображения сетевых принтеров

Чтобы отключить автоматическое добавление или отображение всех доступных сетевых принтеров необходимо отключить сервис avahi-daemon. Для этого выполните команды:

```
sudo systemctl disable avahi-daemon
sudo systemctl stop avahi-daemon
```

Подключение к РЕД ОС принтера, открытого в общий доступ на ОС Windows

Подключение через SAMBA. В локальной сети
Подключение через SAMBA. В доменной сети
Подключение с помощью LPD

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Подключение через SAMBA

В локальной сети

ВАЖНО!

Данная настройка касается только одноранговой локальной сети без доменной структуры. Для сетей в домене есть инструкция ниже. Перед настройкой, вы должны убедиться, что на компьютере Windows с подключенным принтером установлен драйвер, возможна печать, правильно настроен общий доступ к принтеру.

Для настройки подключения принтера используйте имя компьютера на котором он установлен, а не его ip-адрес см. статью.

1. Получите доступ к сетевым ресурсам Windows.

1.1 Откройте файл конфигурации **samba**:

```
nano /etc/samba/smb.conf
```

Следующие параметры должны быть в этом конфигурационном файле:

```
printing = cups
printcap name = cups
load printers = yes
cups options = raw
```

1.2 Создайте в РЕД ОС пользователя с таким же именем, как и на **windows**. Для этого выполните команду:

```
useradd -d /dev/null -s /sbin/nologin user
```

Таким образом будет создан пользователь **user**. Поскольку **Samba** использует пользователей которые уже есть в системе, то надо внести его в базу данных **SMB** и назначить пароль для доступа к общим ресурсам **windows**. Пароль такой же, как и на **windows**.

1.3 Создание пользователя samba и активируйте его:

```
smbpasswd -a user
smbpasswd -e user
```

Для проверки выведем список пользователей **samba**:

```
pdbedit -L -v
```

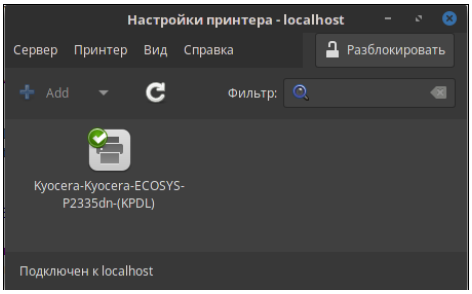
1.3 Проверяем доступ и смотрим имя принтера:

```
smbclient -L win_computer --user=user
Enter WORKGROUP\user's password:
Sharename Type Comment
--------- ---- -------
123 Disk
```

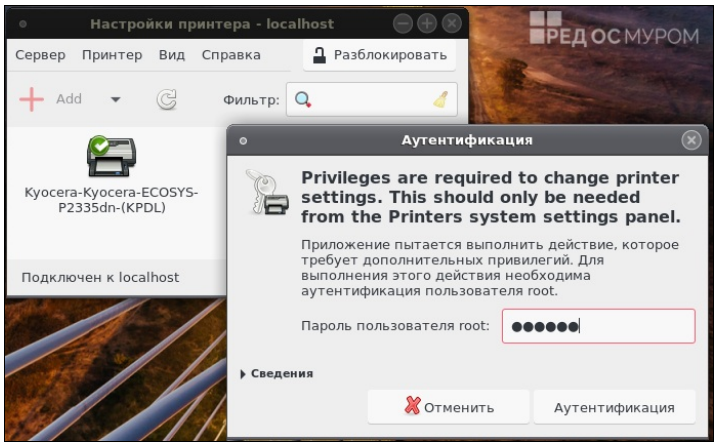
```
ADMIN$ Disk Удаленный Admin
C$ Disk Стандартный общий ресурс
IPC$ IPC Удаленный IPC
P2335 Printer P2335dn
print$ Disk Драйверы принтеров
```

Здесь имя принтера **P2335**. Когда публикуете принтер на **Windows** в общий сетевой доступ, то назначьте имя принтеру без пробелов!

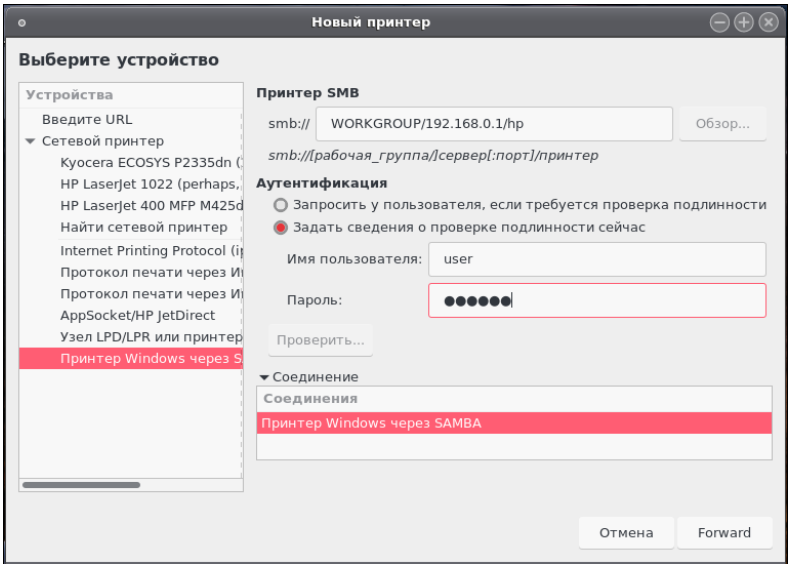
2. Откройте в меню вкладку «**Система**» - «**Администрирование**» - «**Настройки принтера**».



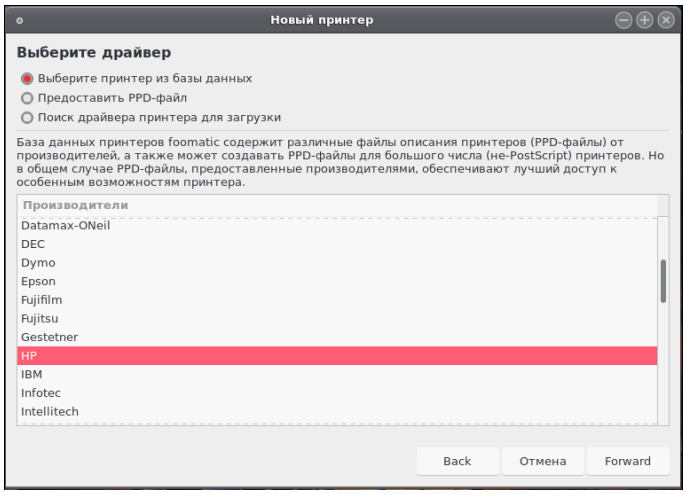
2.1 Нажмите кнопку «**Разблокировать**». Введите пароль текущего пользователя или пароль **root**, в зависимости от настроенных политик пользователей.

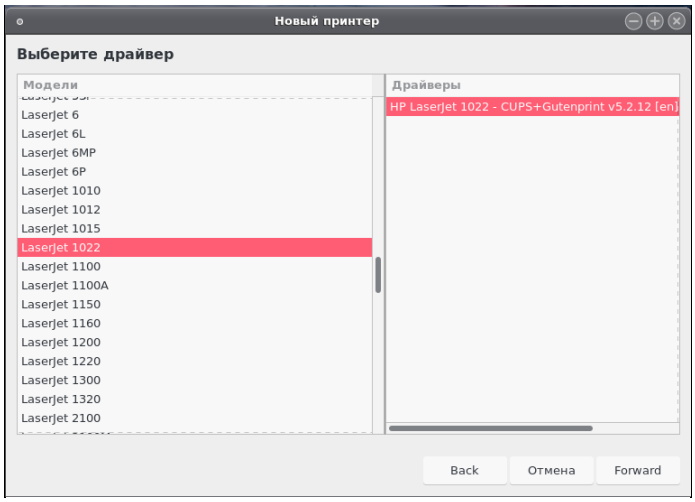


2.2 Нажмите кнопку «**Add**». В открывшемся окне выберите «**Принтер Windows через SAMBA**». Впишите рабочую группу, адрес принтера и сведения о проверки пользователя, если необходимо. Нажмите «**Forward**».

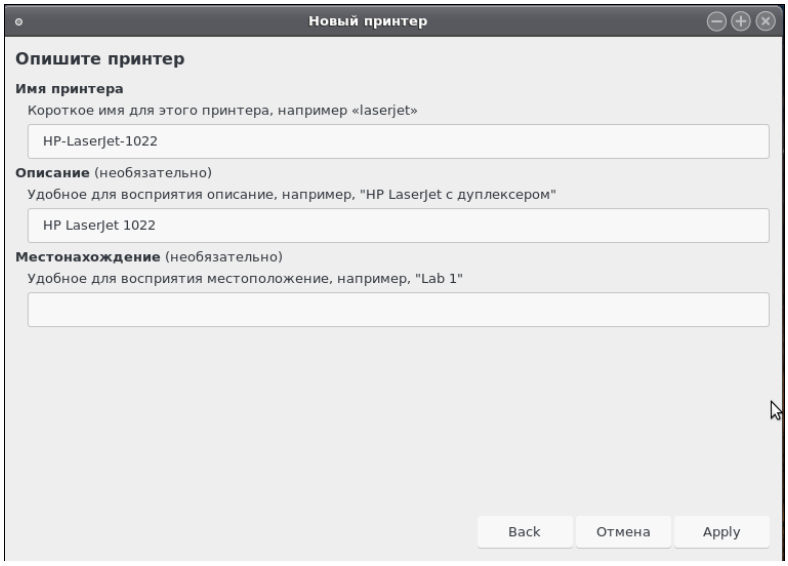


2.3 Выберите драйвер принтера из списка или предоставьте **PPD**.





2.4 Введите дополнительную информацию о принтере и/или нажмите «**Apply**».



2.5 Введите пароль текущего пользователя или пароль **root**, в зависимости от настроенных политик пользователей.

Все, принтер добавлен.

Некоторые принтеры могут работать с универсальным драйвером **Generic - PCL Laser**.

В доменной сети

1.1 Откройте файл конфигурации **samba**:

```
nano /etc/samba/smb.conf
```

Помимо других атрибутов, следующие параметры должны быть в этом конфигурационном файле:

```
printing = cups
printcap name = cups
load printers = yes
cups options = raw
```

1.2 Проверяем доступ и смотрим имя принтера:

```
smbclient -L 10.81.81.150 --user=domainuser
Enter DOMAIN\user's password:
Sharename Type Comment
--------- ---- -------
123 Disk
ADMIN$ Disk Удаленный Admin
C$ Disk Стандартный общий ресурс
IPC$ IPC Удаленный IPC
P2335 Printer P2335dn
print$ Disk Драйверы принтеров
```

Здесь имя принтера **P2335**.

Когда публикуете принтер на **Windows** в общий сетевой доступ, то назначьте имя принтеру без пробелов!

1.3 Далее выполните операции пункта 2.2, только вместо имени группы **WORKGROUP** должно быть указано имя домена.

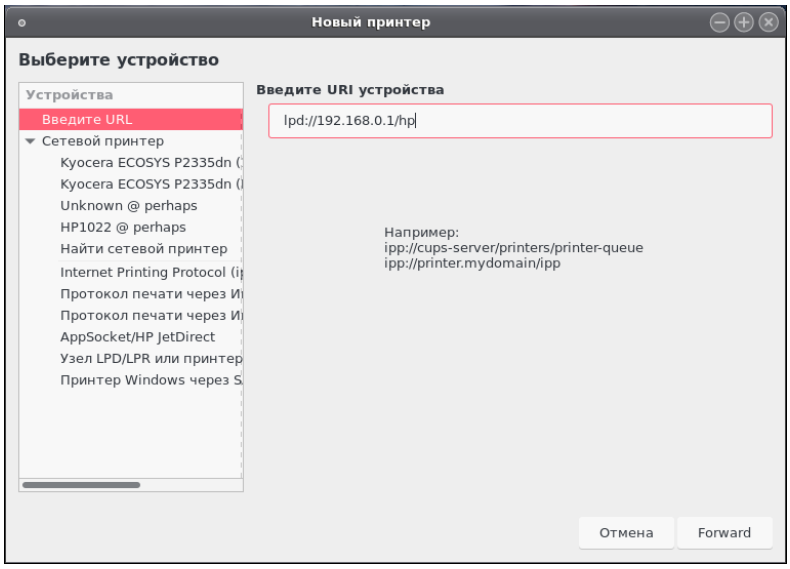
Подключение с помощью LPD

ВАЖНО!

Убедитесь, что следующие компоненты Windows добавлены в систему: служба печати LPD, клиент интернет-печати, монитор LPR-портов, факсы и сканирование Windows. Добавить их можно в панели управления в «**Включение или отключение компонентов Windows**». Убедитесь, что служба LPD запущена.

Для подключения по протоколу LPD впишите URI устройства, например:

lpd://192.168.0.1/hp



Дальнейшая настройка аналогична пунктам 2.2-2.4.

Подключение принтера к РЕД ОС и Windows открытого в общий доступ на РЕД ОС

Предварительная подготовка
Подключение через Samba
Подключение принтера в домене
Подключение принтера через протокол LPD

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка

> **Примечание.**
>
> Данный пункт актуален **только для систем, использующих брандмауэр firewalld**.

Перед началом настройки рекомендуется проверить статус брандмауэра **firewalld** с помощью команды:

```
firewall-cmd --state
```

Если в ответе команды отображается running, в конфигурацию брандмауэра **firewalld** необходимо добавить разрешающее правило для работы службы **samba**. Для этого выполните следующие команды (потребуются права **администратора**):

```
sudo firewall-cmd --add-service=samba --permanent
sudo firewall-cmd --reload
```

Подробную информацию о работе брандмауэра **firewalld** см. в нашей статье «Настройка брандмауэра Firewall».

Если в системе брандмауэр **firewalld** не используется или при проверке статуса выводится сообщение not running, перейдите к следующему пункту.

Подключение через Samba

Подключение принтера к ПК с Windows в рабочей группе

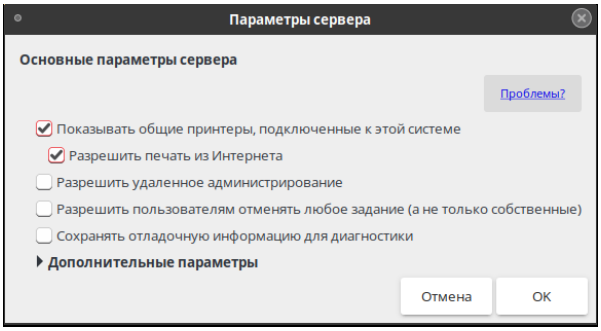
Первым шагом нужно внести машину с принтером в рабочую группу **WORKGROUP** (за имя группы отвечает параметр «*workgroup*», для примера взята рабочая группа *WORKGROUP*), для этого откройте конфигурационный файл samba и приведите секцию **[global]** к виду:

```
nano /etc/samba/smb.conf

[global]
   workgroup = WORKGROUP
   security = user
   map to guest = bad user
   passdb backend = tdbsam

   printing = cups
   printcap name = cups
   load printers = yes
   cups options = raw
```

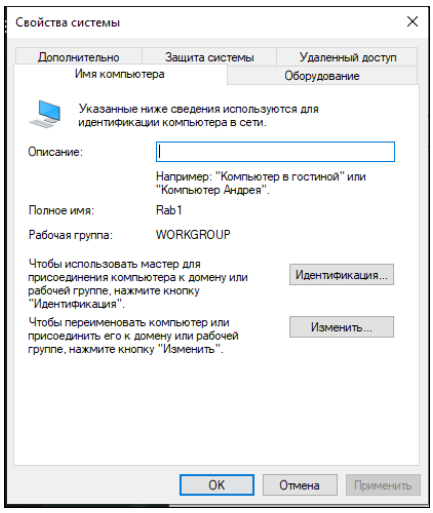
Запустите **Samba** и добавьте ее в автозагрузку:

```
systemctl start smb
systemctl enable smb
```

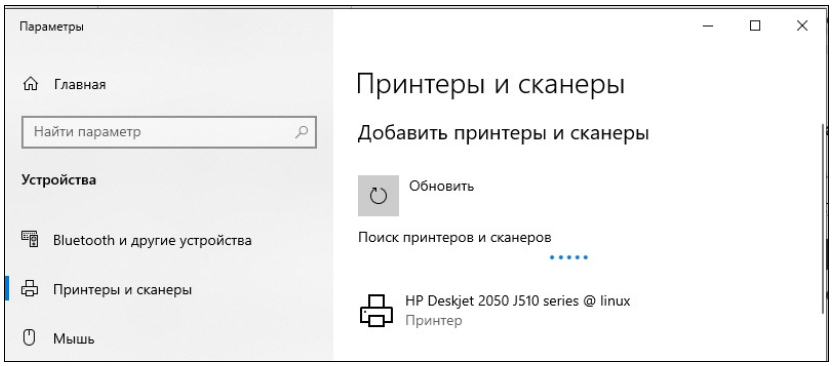
После этого перейдите в **Системное меню – «Администрирование» – «Настройки принтера» – «Сервер» – «Параметры»** и поставьте галочку на следующих пунктах:



Windows должен находиться в той же рабочей группе, что и РЕД ОС. Убедитесь в том, что компьютер на *Windows* находится в той же рабочей группе, перейдя в свойства системы (для *Windows 10*: **«Свойства системы» – «Дополнительные параметры системы» – «Имя компьютера»)**.

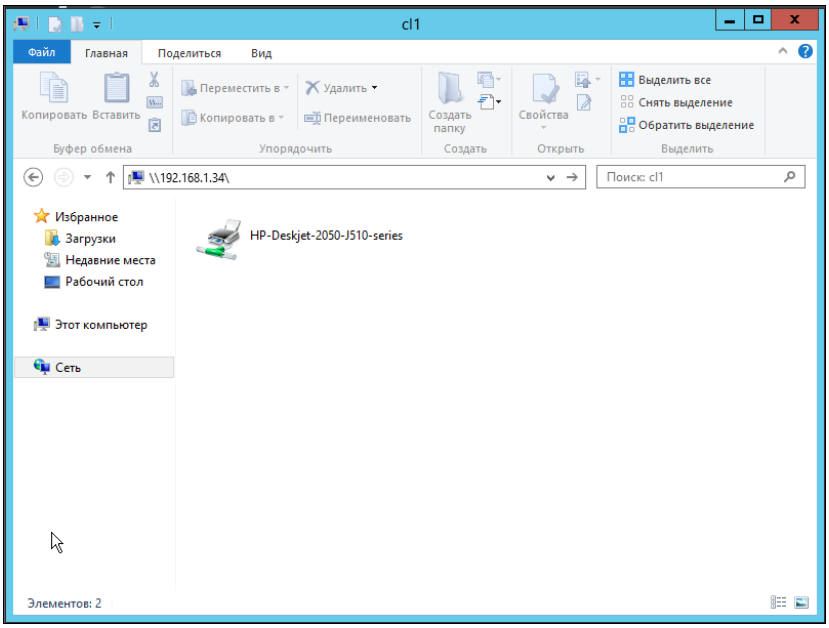


Теперь вы можете добавить принтер в Windows, выберите **«Принтеры и сканеры» – «Добавить принтер или сканер»**.



Принтер будет доступен в проводнике по адресу:

\\<IP_адрес_сервера>



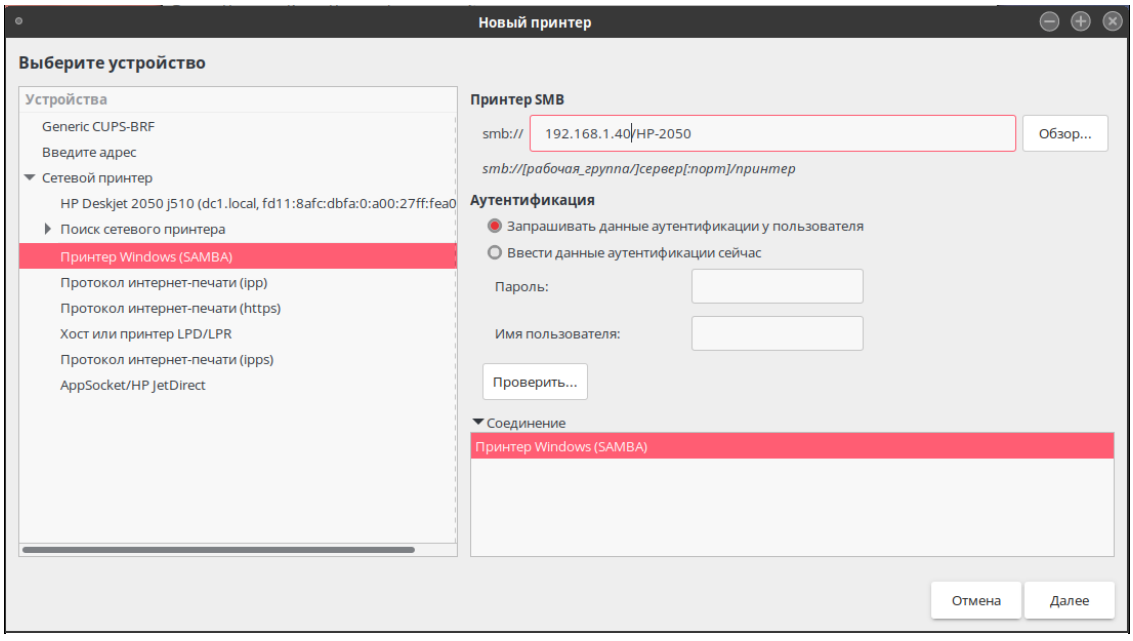
Подключение принтера к ПК с РЕД ОС в рабочей группе

Первым шагом нужно внести машину с принтером в рабочую группу **WORKGROUP** (за имя группы отвечает параметр «*workgroup*», для примера взята рабочая группа *WORKGROUP*), для этого откройте конфигурационный файл **samba** и приведите секцию **[global]** к виду:

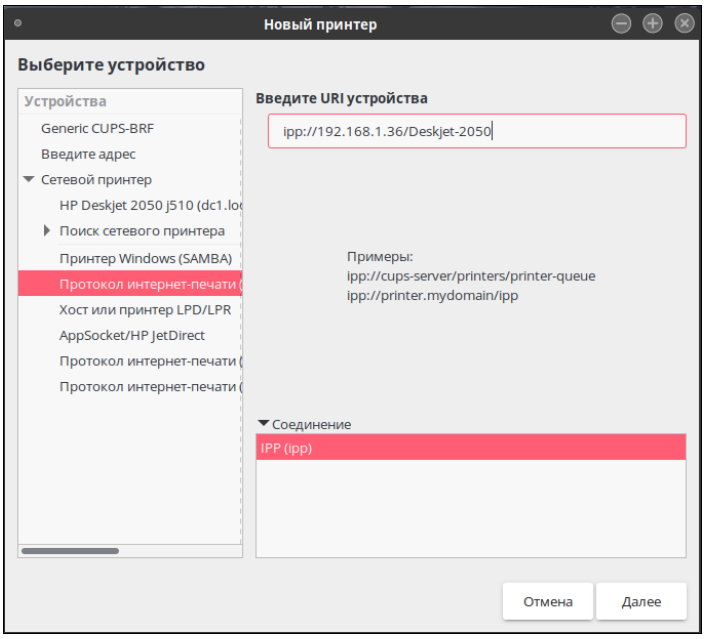
```
nano /etc/samba/smb.conf

[global]
  workgroup = WORKGROUP
  security = user
  map to guest = bad user
  passdb backend = tdbsam

  printing = cups
  printcap name = cups
  load printers = yes
  cups options = raw
```

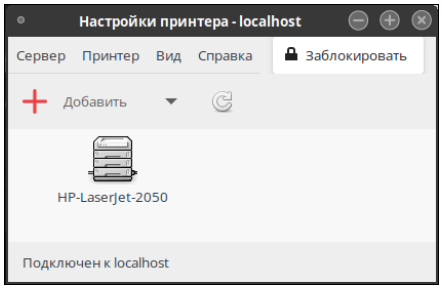
Перейдите в **Системное меню – «Администрирование» – «Настройка принтера» – «Разблокировать» – «Добавить»**. Открытый в общий сетевой доступ на основной машине принтер должен появиться в «**Сетевой принтер**» первым.

Вы можете добавить принтер **Samba** через IP-адрес:



Также вы можете добавить принтер через **«Сетевой принтер» - «Протокол интернет-печати IPP»**.



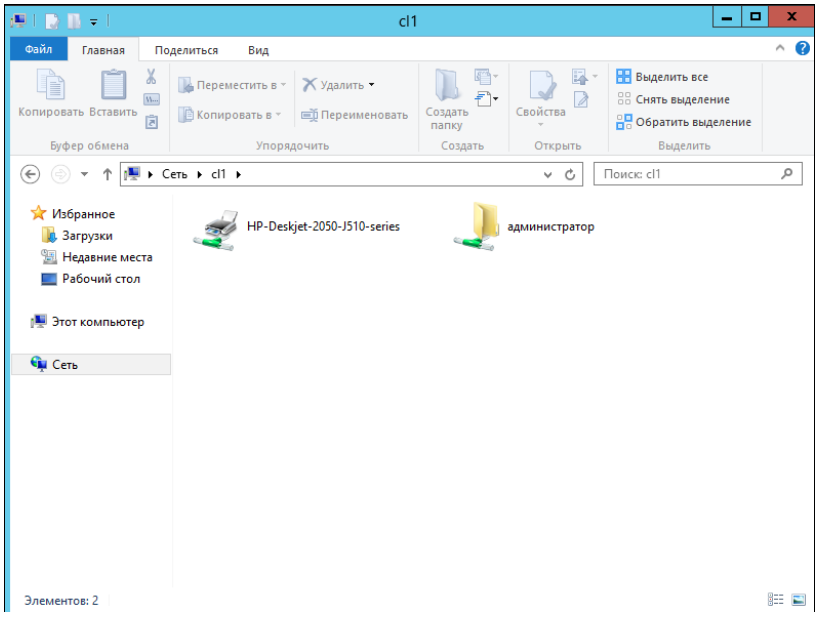


Подключение принтера в домене

Подключение принтера в домене РЕД ОС на пользователя домена с ОС Windows

Открытый в общий сетевой доступ принтер на РЕД ОС будет отображаться в проводнике по адресу:

\\<доменное_имя_(или_адрес)>



Подключение принтера в домене РЕД ОС на пользователя домена с ОС РЕД ОС

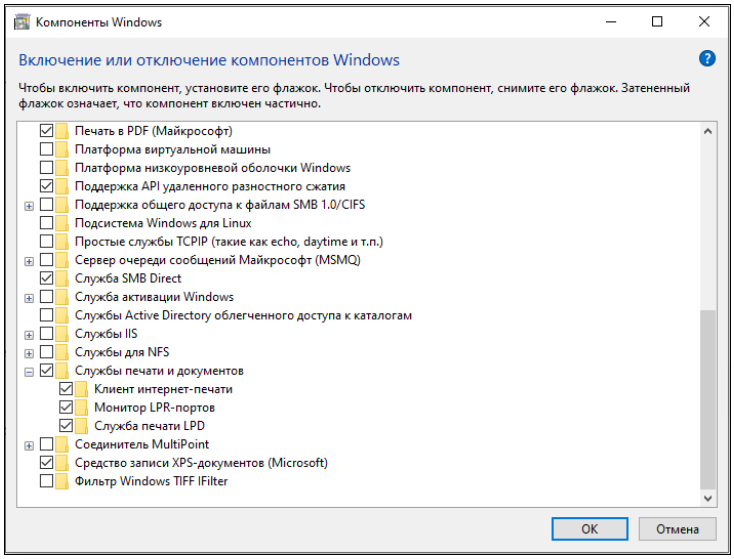
Открытый сетевой принтер на РЕД ОС будет отображаться в **Главное меню – «Администрирование» – «Настройка принтера» – «Разблокировать» – «Добавить» – «Сетевой принтер»**.

Принтер будет иметь имя сервера или клиента в конце.

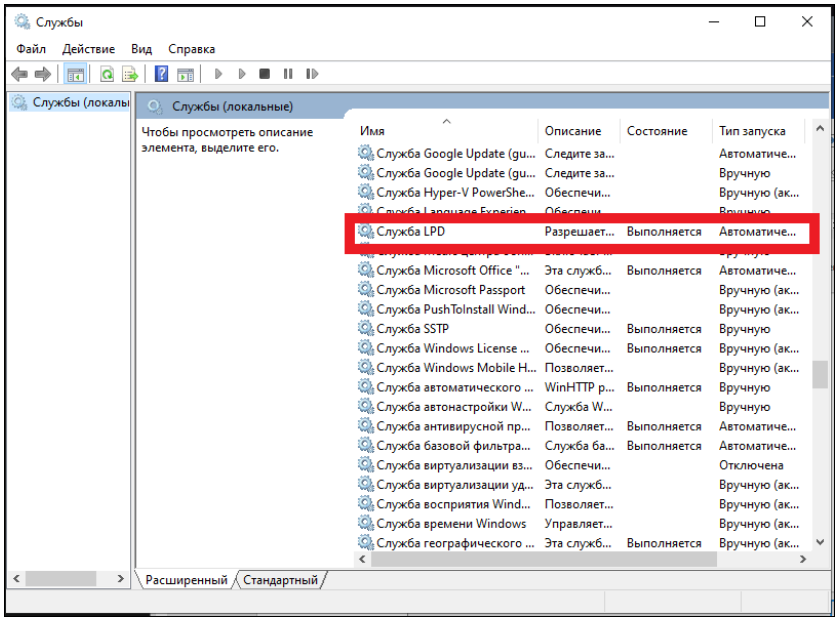
Подключение принтера через протокол LPD

LPD — сетевой протокол прикладного уровня для передачи документов на печать, предоставляющий базовые возможности печати.

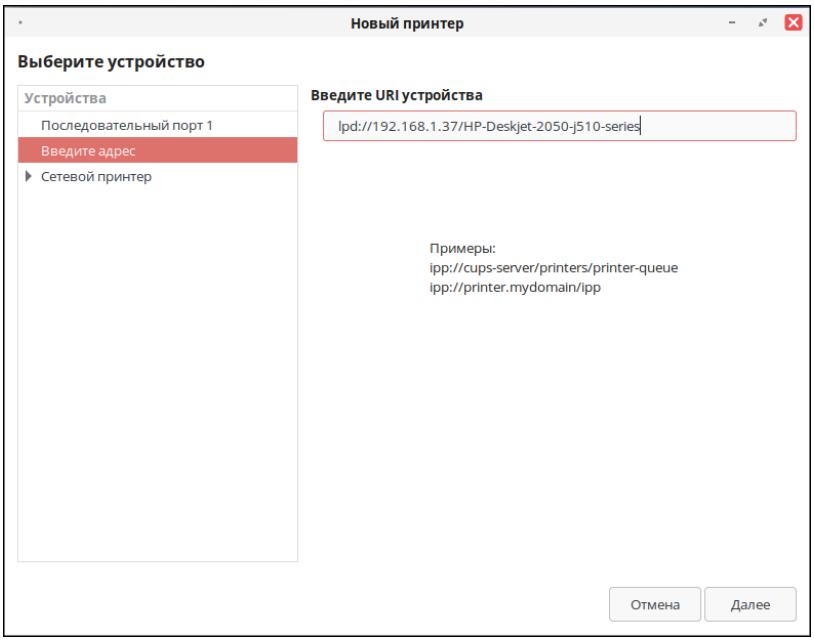
Для подключения принтера через протокол LPD на *Windows* (в данном примере используется *Windows 10*) подключите два компонента в «**Включение или отключение компонентов Windows**»: «**Служба печати LPD**» и «**Монитор LPR-портов**».

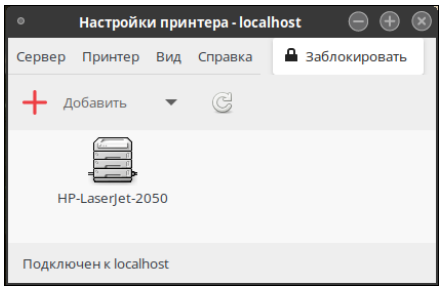


Далее в «**Службы**» должна появиться служба **LPD**.



В РЕД ОС в свойствах принтера необходимо выбрать «**Введите адрес**», в котором следует указать путь к принтеру в формате:


Новый принтер
Выберите устройство
Устройства
Последовательный порт 1
Введите адрес
Сетевой принтер
Введите URI устройства
lpd://192.168.1.37/HP-Deskjet-2050-j510-series
Примеры:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp
Отмена
Далее


Настройки принтера - localhost
Сервер
Принтер
Вид
Справка
Заблокировать
Добавить
HP-LaserJet-2050
Подключен к localhost

Установка драйверов foo2zjs

foo2zjs — это открытый драйвер для принтеров, которые используют протокол печати Zenographics ZjStream, таких как Minolta magicolor 2200/2300/2430 DL, Minolta Color PageWorks/Pro L и HP LaserJet 1000/1005/1018/1020/1022.

```
sudo dnf install foo2zjs
```

Данные драйверы поддерживают определенный ряд устройств, список приведен ниже:

Модель принтера	Тип печати
Konica Minolta magicolor 2430 DL	B/W and color
Minolta/QMS 2300 DL	B/W and color
Minolta/QMS 2200 DL	B/W and color
HP LaserJet P2035	B/W
HP LaserJet M1319 MFP	B/W
HP LaserJet Pro P1606dn	B/W
HP LaserJet Pro P1566	B/W
HP LaserJet Pro P1102	B/W
HP LaserJet Pro CP1025nw	B/W and color
HP LaserJet 1022	B/W
HP LaserJet 1020	B/W
HP LaserJet 1018	B/W
HP LaserJet 1005	B/W
HP LaserJet 1000	B/W
HP Color LaserJet CP1215	B/W and color
HP Color LaserJet 1600	B/W and color
HP Color LaserJet 2600n	B/W and color
Konica Minolta magicolor 2530 DL	B/W and color
Konica Minolta magicolor 2490 MF	B/W and color
Xerox Phaser 6115MFP	B/W and color
Konica Minolta magicolor 2480 MF	B/W and color
Konica Minolta magicolor 1690MF	B/W and color
Konica Minolta magicolor 1680MF	B/W and color
Konica Minolta magicolor 1600W	B/W and color
Samsung CLP-300	B/W and color
Samsung CLP-315	B/W and color
Samsung CLP-325	B/W and color
Samsung CLP-365	B/W and color
Samsung CLP-600	B/W and color
Samsung CLP-610	B/W and color
Samsung CLP-2160	B/W and color
Samsung CLP-3160	B/W and color
Samsung CLP-3175	B/W and color
Xerox Phaser 6110	B/W and color
Xerox Phaser 6110MFP	B/W and color
HP LaserJet M1005 MFP	
HP LaserJet M1120 MFP	
HP LaserJet P1005	
HP LaserJet P1006	

HP LaserJet P1007	
HP LaserJet P1008	
HP LaserJet P1505/P1505n	
HP LaserJet P2014/P2014n	
HP LaserJet Pro M1212nf MFP	
Oki C301dn	
Oki C310dn	
Oki C511dn	
Oki C810dn	
Oki C3100n/C3200n	
Oki C3300n/C3400n	
Oki C3530n MFP	
Oki C5100n/C5150n/C5200n	
Oki C5500n/C5600n/C5800n	
Dell 1355 Multifunction Color Printer	
Dell C1765 Multifunction Color Printer	
Epson AcuLaser CX17NF	
Epson AcuLaser M1400	
Fuji Xerox DocuPrint CM205 Multifunction Color Printer	
Fuji Xerox DocuPrint CM215 Multifunction Color Printer	
Fuji Xerox DocuPrint M215	
Fuji Xerox DocuPrint P205	
Xerox WorkCentre 3045 Multifunction Monochrome Printer	
Xerox WorkCentre 6015 Multifunction Color Printer	

Установка принтеров Samsung

Вы можете подробнее ознакомиться с примерами установки и подключения принтеров и драйверов для них, просмотрев наши обучающие видео:

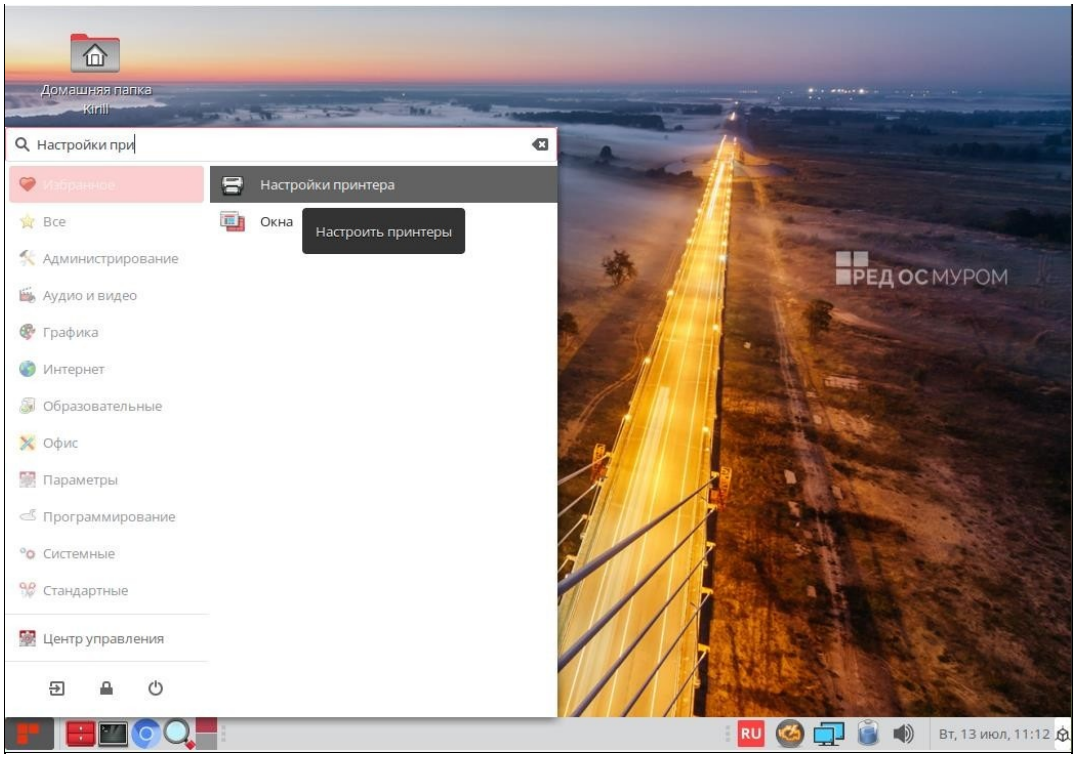
- на **RuTube** — Подключение и установка драйверов принтеров в РЕД ОС;
- в **Яндекс.Дзен** — Подключение и установка драйверов принтеров в РЕД ОС.
- в **VK Видео** — Подключение и установка драйверов принтеров в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

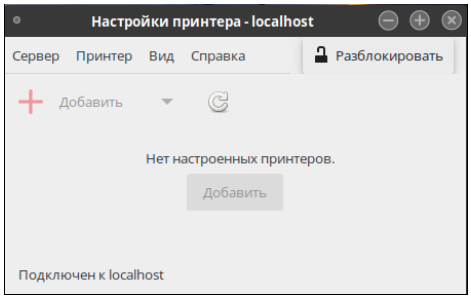
Перед настройкой принтера необходимо с правами администратора установить **OpenPrintingPPDs-ghostscript** и **OpenPrintingPPDs-postscript** актуальной версии командами:

```
dnf install OpenPrintingPPDs-ghostscript
dnf install OpenPrintingPPDs-postscript
```

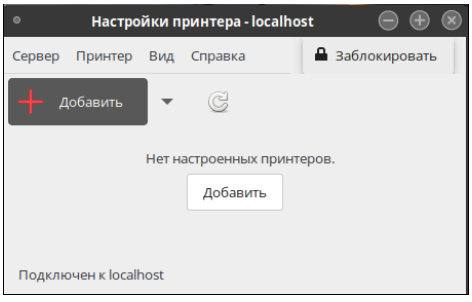
Затем запустите «**Настройки принтера**».



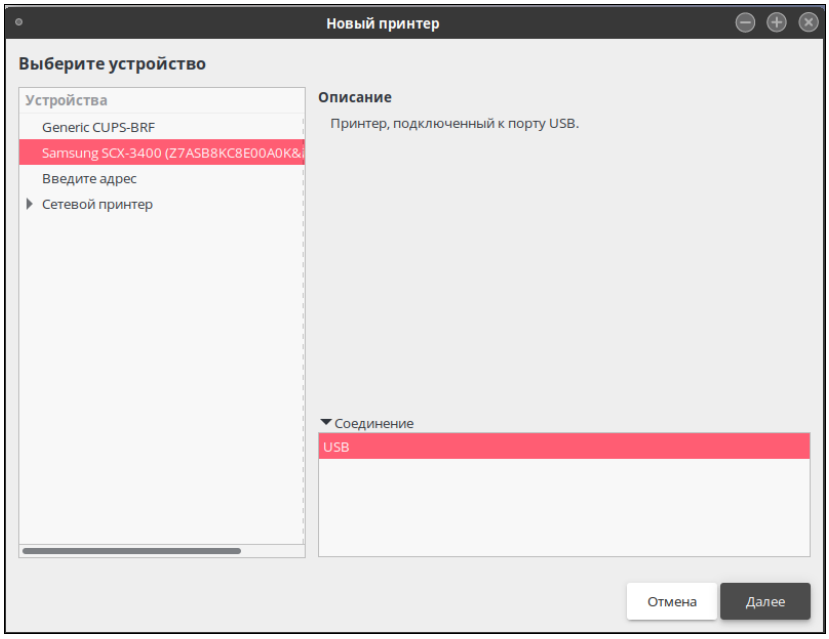
Изначально функция добавления принтеров недоступна.



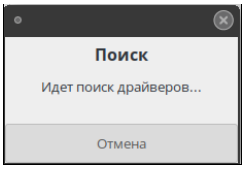
Для того чтобы разблокировать функцию добавления принтеров, нажмите «**Разблокировать**» и введите пароль администратора, далее нажмите «**Добавить**».

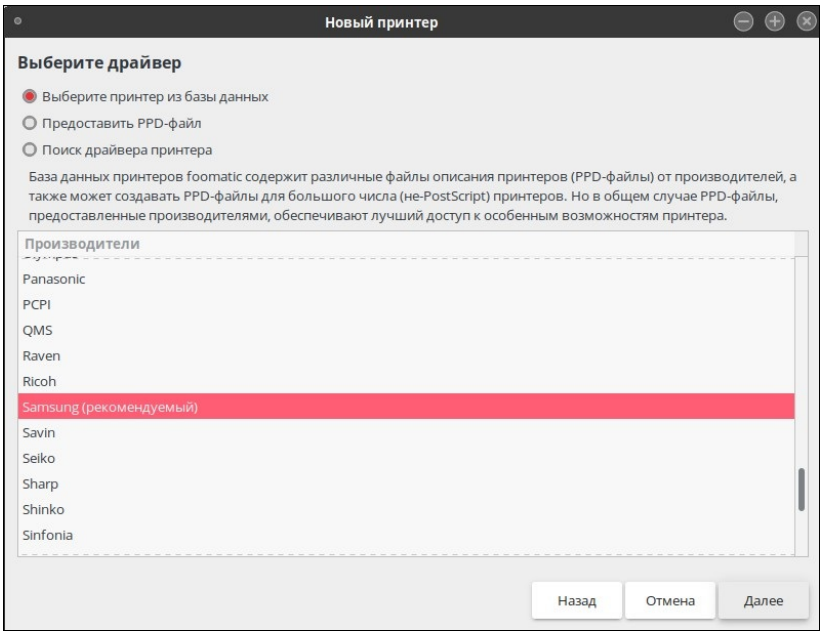


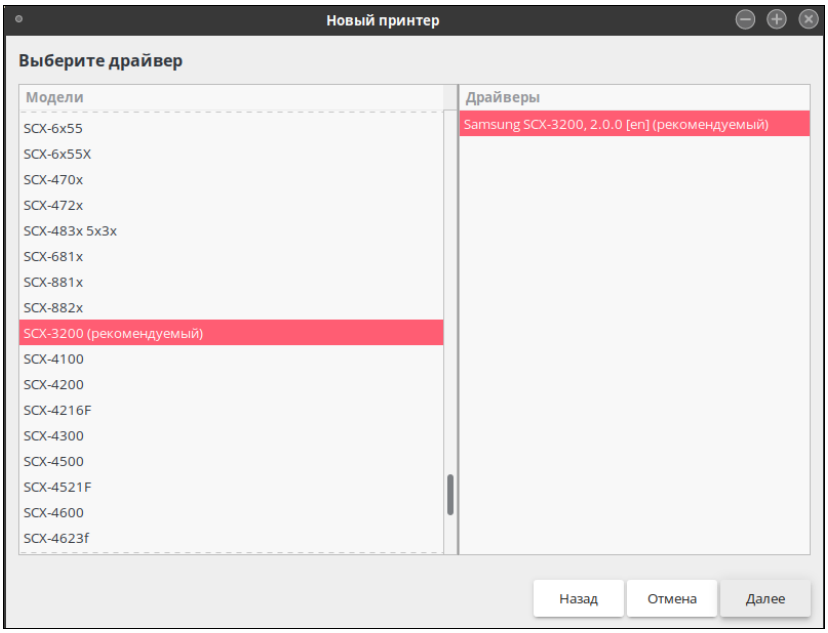
В данном примере принтер **Samsung SCX-3400** подключен по USB, выберите нужный принтер и нажмите « **Далее**».



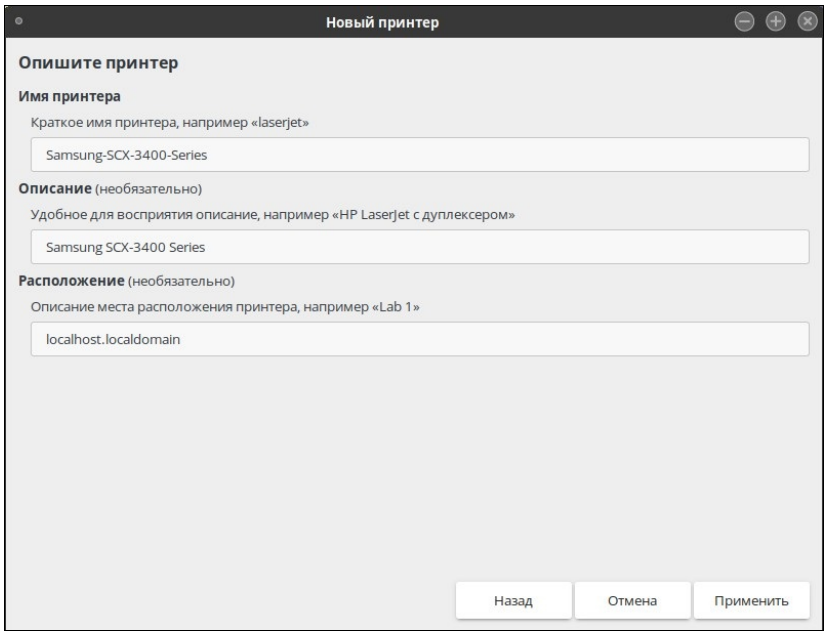
После поиска драйверов приложение корректно предлагает необходимый драйвер.



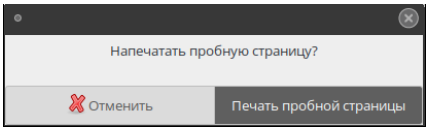




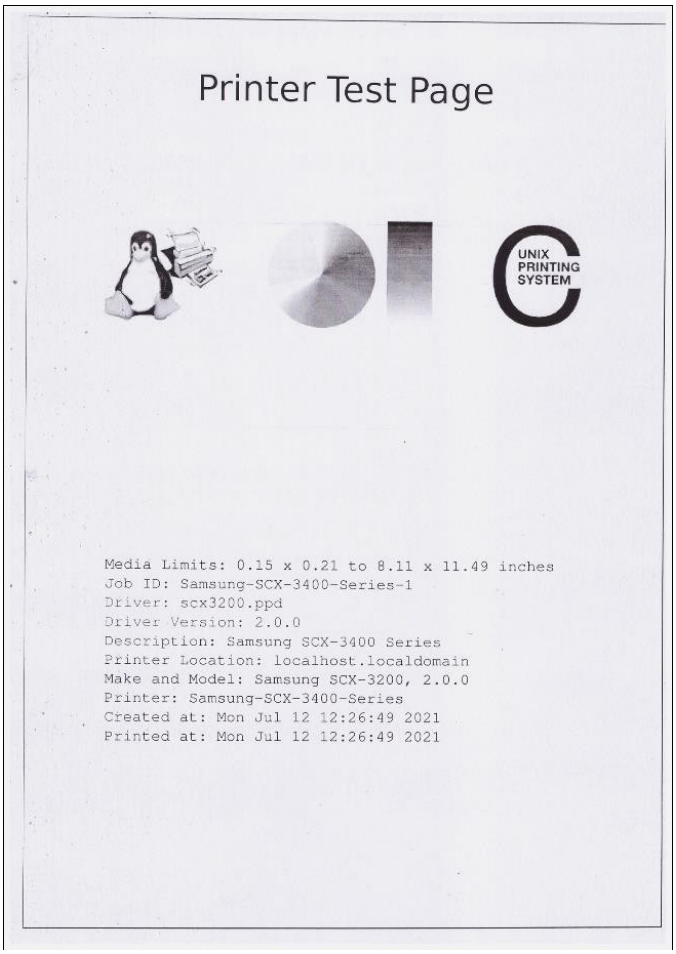
На данном этапе можно дать описание принтеру для удобства дальнейшего использования.



Для проверки работоспособности можно напечатать пробную страницу.



Внешний вид пробной страницы.



Список принтеров

Список принтеров Samsung, драйвера для которых устанавливаются описанным выше способом.

1. Samsung C48X	33. Samsung CLP-770
2. Samsung C140X	34. Samsung CLP-775
3. Samsung C145X	35. Samsung CLX-92X1 93X1
4. Samsung C268X	36. Samsung CLX-216X
5. Samsung C460	37. Samsung CLX-981X
6. Samsung C470	38. Samsung CLX-982X
7. Samsung C1810	39. Samsung CLX-2170
8. Samsung C1860	40. Samsung CLX-3160
9. Samsung C2620	41. Samsung CLX-3300
10. Samsung C2670	42. Samsung CLX-4190
11. Samsung C4820	43. Samsung CLX-6200
12. Samsung CLP-200	44. Samsung CLX-6220
13. Samsung CLP-300	45. Samsung CLX-6240
14. Samsung CLP-310	46. Samsung CLX-6250
15. Samsung CLP-310N	47. Samsung CLX-6260
16. Samsung CLP-315	48. Samsung CLX-8380
17. Samsung CLP-350	49. Samsung CLX-8385
18. Samsung CLP-410	50. Samsung CLX-8385X
19. Samsung CLP-500	51. Samsung CLX-8540
20. Samsung CLP-510	52. Samsung CLX-8640 8650
21. Samsung CLP-550	53. Samsung CLX-9250 9350

22. Samsung CLP-550N	54. Samsung CLX-9252 9352
23. Samsung CLP-600	55. Samsung K-401 – K7600
24. Samsung CLP-610	56. Samsung M262X 282X
25. Samsung CLP-620	57. Samsung M267X 287X
26. Samsung CLP-650	58. Samsung M283X – M458X
27. Samsung CLP-650N	59. Samsung ML1000 – ML8950
28. Samsung CLP-660	60. Samsung SCX-470X – SCX-8240
29. Samsung CLP-660N	61. Samsung SF-565P
30. Samsung CLP-660ND	62. Samsung SI-630A
31. Samsung CLP-670	63. Samsung X401 – X7600
32. Samsung CLP-680	

Настройка сканеров

Проверка поддержки сканера в Linux на уровне драйверов
Проверка распознавания системой сканера, как устройства
Разрешение сканеру обращаться к ядру системы

Вы можете подробнее ознакомиться с примерами установки и подключения сканеров, просмотрев наши обучающие видео:

- на **RuTube** — Работа со сканерами в РЕД ОС;
- в **Яндекс.Дзен** — Работа со сканерами в РЕД ОС.
- в **VK Видео** — Работа со сканерами в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Проверка поддержки сканера в Linux на уровне драйверов

Прежде всего стоит проверить, поддерживается ли подключенный или планируемый к покупке сканер на уровне драйверов. Данную информацию можно получить на сайте проекта SANE. В частности, на странице раздела со стабильной поддержкой (http://www.sane-project.org/sane-mfgs), где рекомендуется выполнять поиск по производителю (заголовок «**Scanners**», список «**Manufacturers**»).

Данные о сканерах представлены в таблицах, где стоит обратить особое внимание на столбец «**Статус**», в котором могут быть указаны следующие параметры:

- **Complete** — полная поддержка;
- **Good** — поддерживается большинство функций;
- **Basic** — поддерживается только базовый функционал;
- **Unsupported** — не поддерживается;
- **Untested** — не тестировался, вероятнее всего работать не будет, но можно проверить самостоятельно или выполнить поиск драйверов в нестабильной ветке SANE.

Если «**Статус**» имеет последние два значения, то сканер не заработает.

Если указанной модели сканера нет в списке, необходимо выполнить проверку на сайте производителя. Если вендор предоставляет драйвера для сканера, тогда необходимо их скачать и установить (обычно в архиве с драйвером предоставляется скрипт, который автоматически устанавливает драйвер).

Если сканер поддерживается, но в данный момент не сканирует, можно применить следующие рекомендации.

Ряд устройств поддерживается драйверами **sane-airscan**, список поддерживаемых устройств доступен по ссылке — https://github.com/alexpevzner/sane-airscan.

Ряд устройств **HP** поддерживаются **libsane-hpaio** из пакета **hplip**, список устройств доступен по ссылке — https://developers.hp.com/hp-linux-imaging-and-printing/supported_devices/index.

Проверка распознавания системой сканера, как устройства

Сначала рекомендуется проверить, определяется ли сканер физически. Большинство сканеров подключается по **USB**, поэтому необходимо открыть терминал и ввести команду, показывающую все подключенные USB-устройства:

```
lsusb

 или

sane-find-scanner
```

Если в списке нет нужного сканера, то, скорее всего, проблема аппаратная. Стоит проверить, подключён ли сканер по **USB**, не переломился ли кабель и исправен ли сам сканер. Также могут быть проблемы с распознаванием сканера в **BIOS** или **UEFI** компьютера. Часто помогает отключение **XHCI** в **UEFI**.

Если же в выводе терминала есть строка вида (наименование сканера и ID могут отличаться):

```
Bus 003 Device 005: ID 04a9:2220 Canon, Inc. CanoScan LIDE 25
```

значит система видит сканер как USB-устройство и можно продолжить настройку.

Теперь нужно ввести в терминале:

```
scanimage -L
```

Если система не может выполнить команду, то, вероятно, не установлен пакет **sane-backends**. Для установки пакета выполните:

```
dnf install sane-backends
```

Затем повторите ввод:

```
scanimage -L
```

Положительным ответом будет считаться строка, аналогичная данной:

```
device `plustek:libusb:003:008' is a Canon CanoScan LiDE25 flatbed scanner
```

Если терминал выдаёт отрицательный ответ (примерно следующего вида):

```
No scanners were identified. If you were expecting something different,
check that the scanner is plugged in, turned on and detected by the
sane-find-scanner tool (if appropriate). Please read the documentation
which came with this software (README, FAQ, manpages)
```

это может означать:

- аппаратную проблему;
- отсутствие прав на работу со сканером у активной в данный момент учётной записи пользователя;
- сканеру запрещено обращаться к ядру (где обычно находятся драйвера).

Про решение аппаратных проблем было сказано выше.

Перейдем к настройке прав учётной записи пользователя.

Введённая в терминал команда:

```
whoami
```

покажет логин активного в данный момент пользователя.

Далее нужно определить, в каких группах состоит этот пользователь:

```
groups <имя_пользователя>
```

где <имя_пользователя> — логин, полученный по команде whoami.

Если в этом списке не указана группа **lp**, необходимо добавить пользователя в группу:

```
sudo usermod -G lp -a user1
```

где user1 — логин добавляемого пользователя.

Для тестирования сканера выполните команду:

```
scanimage -T
```

Разрешение сканеру обращаться к ядру системы

Если ответ терминала по-прежнему отрицательный, то, возможно, сканеру запрещено обращаться к ядру. Разрешение можно предоставить, отредактировав конфигурационный файл **40-libsane.rules**, или если такого файла нет, **60-libsane.rules** в текстовом редакторе, запущенном с правами суперпользователя:

```
sudo nano /lib/udev/rules.d/40-libsane.rules
```

В открывшемся тексте должна отображаться строка с параметрами сканера со схожим названием. Нужно скопировать строку с этими данными и вставить её копию сразу под найденной, заменив в копии название сканера и номера idVendor и idProduct на полученные ранее по команде lsusb. Например:

В качестве примера будет также рассмотрен сканер **CanoScan LIDE 25**. При подключении другого сканера название и значения параметров idVendor и idProduct будут другими, также может отличаться номер USB-порта.

Строка с похожим сканером в файле **40-libsane.rules**:

```
# Canon CanoScan LiDE 60
ATTRS{idVendor}=="04a9", ATTRS{idProduct}=="221c", ENV{libsane_matched}="yes"
```

Данные от утилиты **lsusb**:

```
Bus 003 Device 005: ID 04a9:2220 Canon, Inc. CanoScan LIDE 25
```

В файле **40-libsane.rules** в копии строки, в заголовке меняется номер модели сканера с *60* на **25**, а двойной **ID 04a9:2220**, полученный от lsusb нужно разделить на idVendor — **04a9** и idProduct — **2220**. В результате, основная и новая строки будут выглядеть так:

```
# Canon CanoScan LiDE 60
ATTRS{idVendor}=="04a9", ATTRS{idProduct}=="221c", ENV{libsane_matched}="yes"
# Canon CanoScan LiDE 25
ATTRS{idVendor}=="04a9", ATTRS{idProduct}=="2220", ENV{libsane_matched}="yes"
```

Сохраните файл и закройте его.

Теперь снова выполните в терминале команду:

```
scanimage -L
```

Ответ должен быть положительным:

```
device `plustek:libusb:003:008' is a Canon CanoScan LiDE25 flatbed scanner
```

Если сканер по-прежнему не найден, рассмотрим, как SANE работает со сканером.

У SANE есть конфигурационный файл, который обеспечивает доступ к драйверам. Находится он в каталоге **/etc/sane.d/dll.conf**. Выглядит он как список из других конфигурационных файлов, которые находятся в той же папке, что и **dll.conf**. Когда мы запускаем команду scanimage -L, а она, в свою очередь, обращается к конфигурационному файлу **dll.conf**, который обращается к конфигурационным файлам, отвечающим непосредственно за определенные модели сканера. Сами конфигурационные файлы ведут драйверам, которые находятся в **/usr/lib64/sane/**.

Решением проблемы может быть следующее:

В конфигурационном файле **/etc/sane.d/dll.conf** должен быть указан файл конфигурации (причем он не должен быть закомментирован символом «#»), в котором должен быть указан Vendor ID и Product ID.

Например:

Bus 003 Device 005: ID **04a9:2220** Canon, Inc. CanoScan LIDE 25

Bus 003 Device 005: ID **«Vendor ID»:«Product ID»** Canon, Inc. CanoScan LIDE 25

Запись в конфигурационном файле с указанием поддерживаемых сканеров должна выглядеть следующем образом:

```
#Samsung X7600 Series
 usb 0x04e8 0x3326
```

Решение проблемы, если сканер виден под root, но не виден под пользователем:

lsusb

```
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 002: ID 03f0:622a Hewlett-Packard
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

Здесь строка Bus 003 Device 002: ID 03f0:622a Hewlett-Packard — это наше МФУ. Заходим в **/dev/bus/usb/**, проверяем через ls -al и находим **003** (по аналогии из вывода lsusb - это **Bus 003**), заходим в **003** и для устройства **002** (Device 002) устанавливаем права **666**.

```
cd /dev/bus/usb/003
```

```
chmod 666 002
```

Тогда сканер будет виден под пользователем.

Смена менеджера входа в систему (lightdm и sddm)

Менеджер входа в систему lightdm
Установка и активация
Автоматический вход пользователя
Менеджер входа в систему sddm
Установка и активация
Темы оформления sddm

Менеджер входа в систему — графическая оболочка, при помощи которой пользователь осуществляет вход в систему.

В РЕД ОС 8 в графических оболочках MATE и GNOME по умолчанию установлен **gdm**, в KDE Plasma — **sddm**. Чтобы определить, какой менеджер входа в систему используется можно посмотреть статус display-manager.service. Для этого выполните команду:

```
systemctl status display-manager.service
```

Вы можете подробнее ознакомиться с возможностью смены менеджера входа в систему, просмотрев наши обучающие видео:

- на **RuTube** — Смена менеджера входа в систему (lightdm и sddm) ;
- в **Яндекс.Дзен** — Смена менеджера входа в систему (lightdm и sddm) ;
- в **VK Видео** — Смена менеджера входа в систему (lightdm и sddm) .

На наших каналах вы также сможете найти много другой полезной информации.

Менеджер входа в систему lightdm

Установка и активация

Для смены менеджера необходимо установить пакеты **lightdm** и **system-config-language**.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

И выполните команду:

```
dnf install lightdm system-config-language
```

Отключите менеджер входа в систему по умолчанию:

```
systemctl disable gdm
```

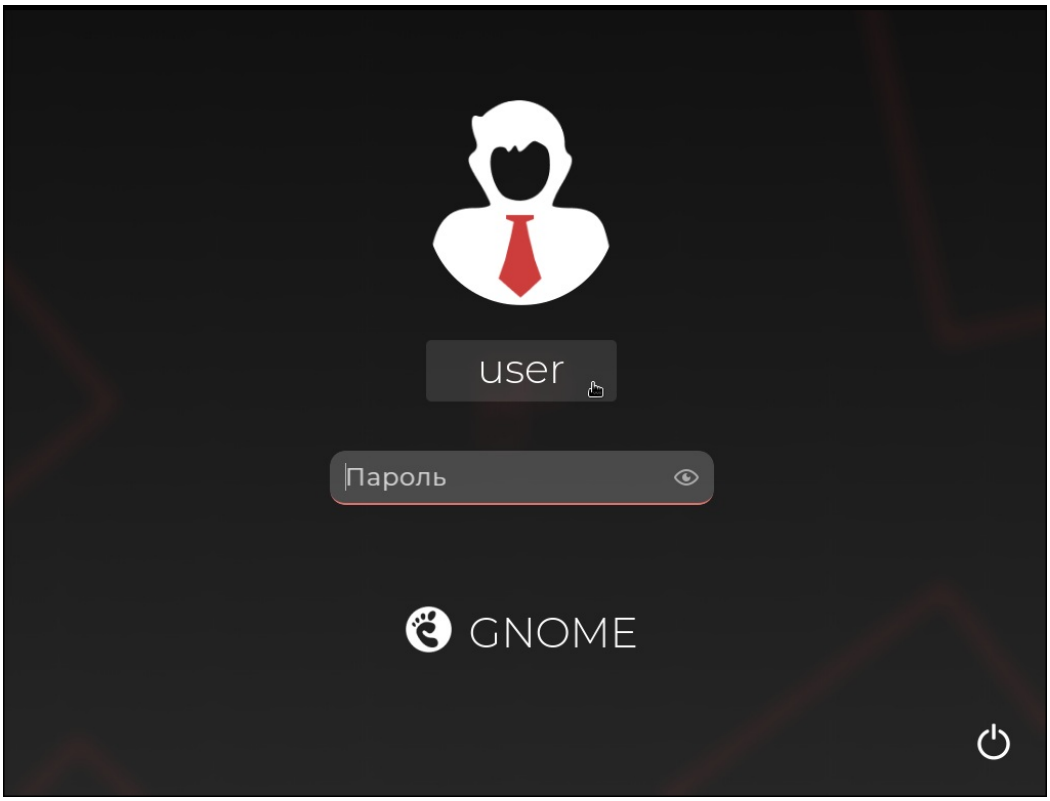
Затем включите новый менеджер:

```
systemctl enable lightdm
```

Перезагрузите систему:

```
reboot
```

При запуске менеджер входа изменится и будет выглядеть следующим образом:



Автоматический вход пользователя

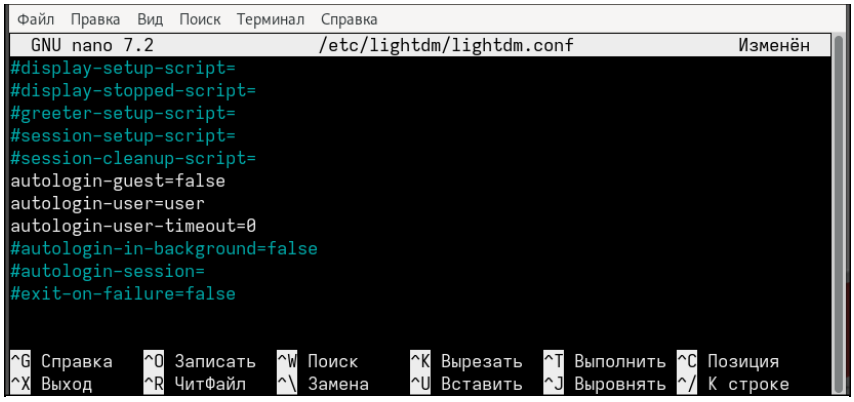
Для включения автоматического входа в **LightDM** в терминале откройте конфигурационный файл:

```
nano /etc/lightdm/lightdm.conf
```

и раскомментируйте строки:

```
#autologin-guest=false
 #autologin-user=user
 #autologin-user-timeout=0
```

Должно выглядеть следующим образом:



где

- **autologin-guest** — указывает, что вход будет по умолчанию происходить под гостем;
- **autologin-user** — указывает, под каким пользователем будет осуществляться вход;
- **autologin-user-timeout** — количество секунд ожидания загрузки пользователя по умолчанию.

Менеджер входа в систему sddm

Примечание.

Обратите внимание, что стандартная тема дисплейного менеджера работает **только** с **локальными** пользователями. Для работы с доменными пользователями см. «Темы оформления sddm».

Установка и активация

Для смены менеджера необходимо установить пакеты **sddm** и **sddm-themes**. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install sddm sddm-themes
```

Отключите менеджер входа в систему по умолчанию:

```
systemctl disable gdm
```

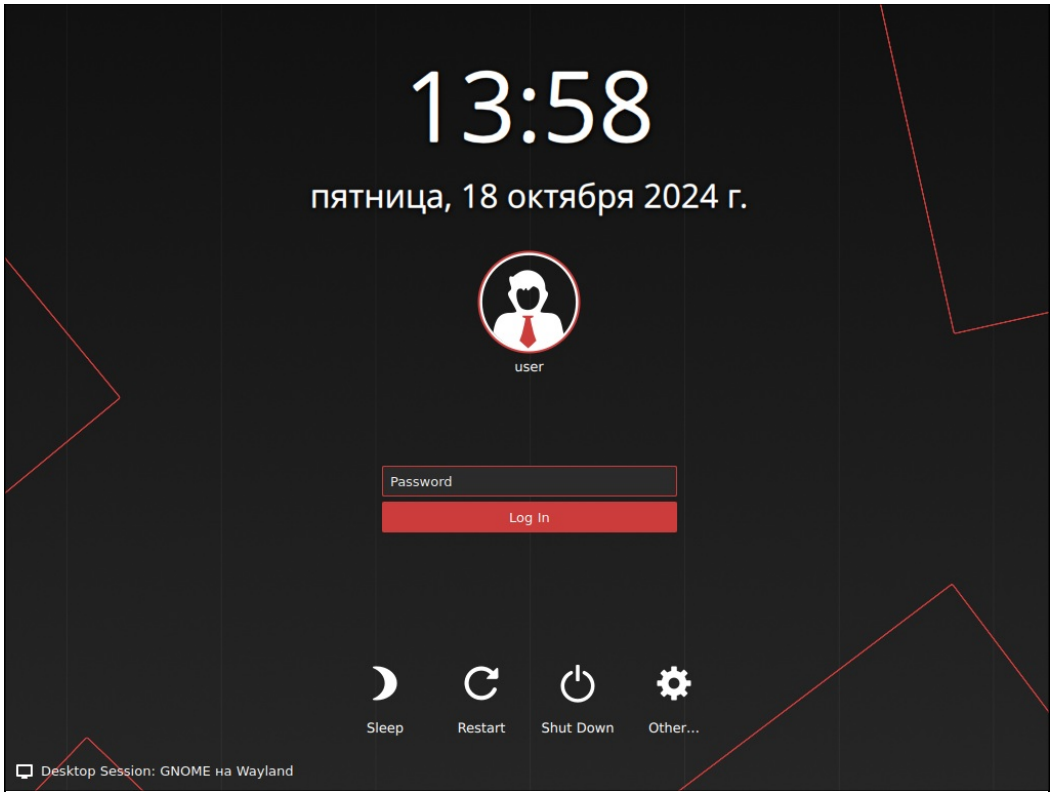
Затем включите новый менеджер:

```
systemctl enable sddm
```

Перезагрузите систему:

```
reboot
```

При запуске менеджер входа изменится и будет выглядеть следующим образом:



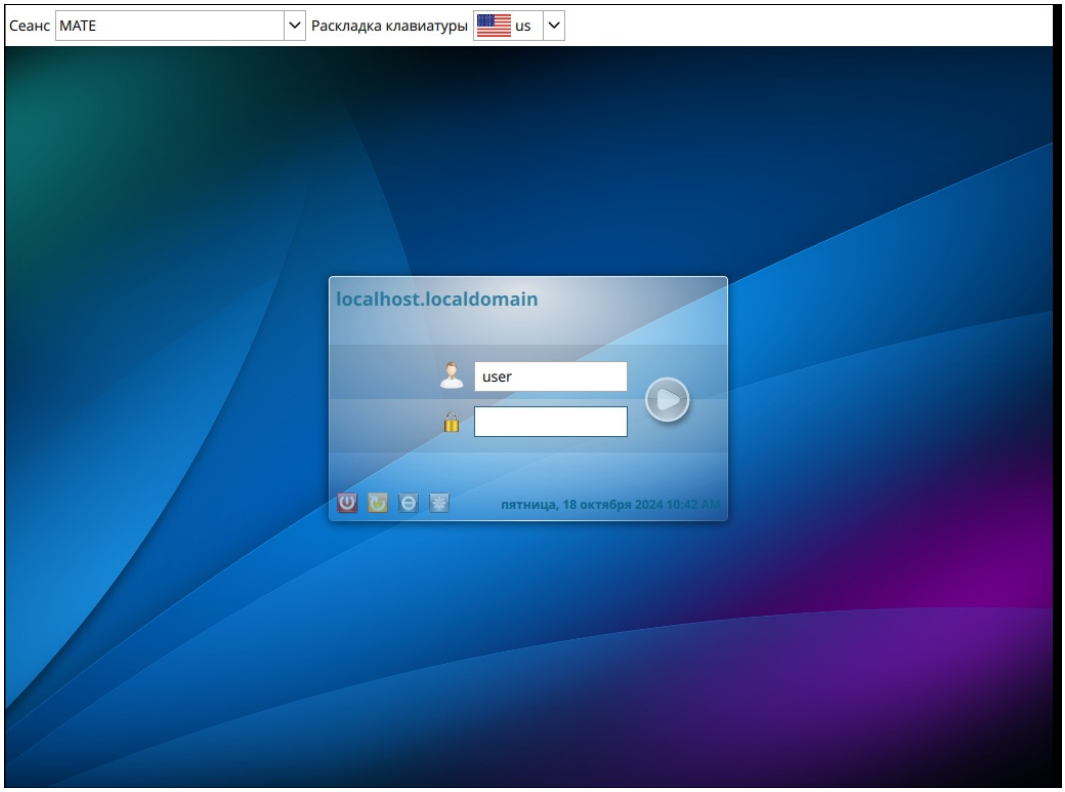
Примечание.

При использовании гибридной графики **nVidia** в связке с менеджером входа в систему **SDDM** переключение между видеокартами необходимо производить согласно нашей инструкции «Переключение используемых видеокарт nVidia и Intel при использовании менеджера SDDM».

Темы оформления sddm

В установленном из репозитория пакете **sddm-themes** существует 3 темы: «***elarun***», «***maldives***» и «***maya***».

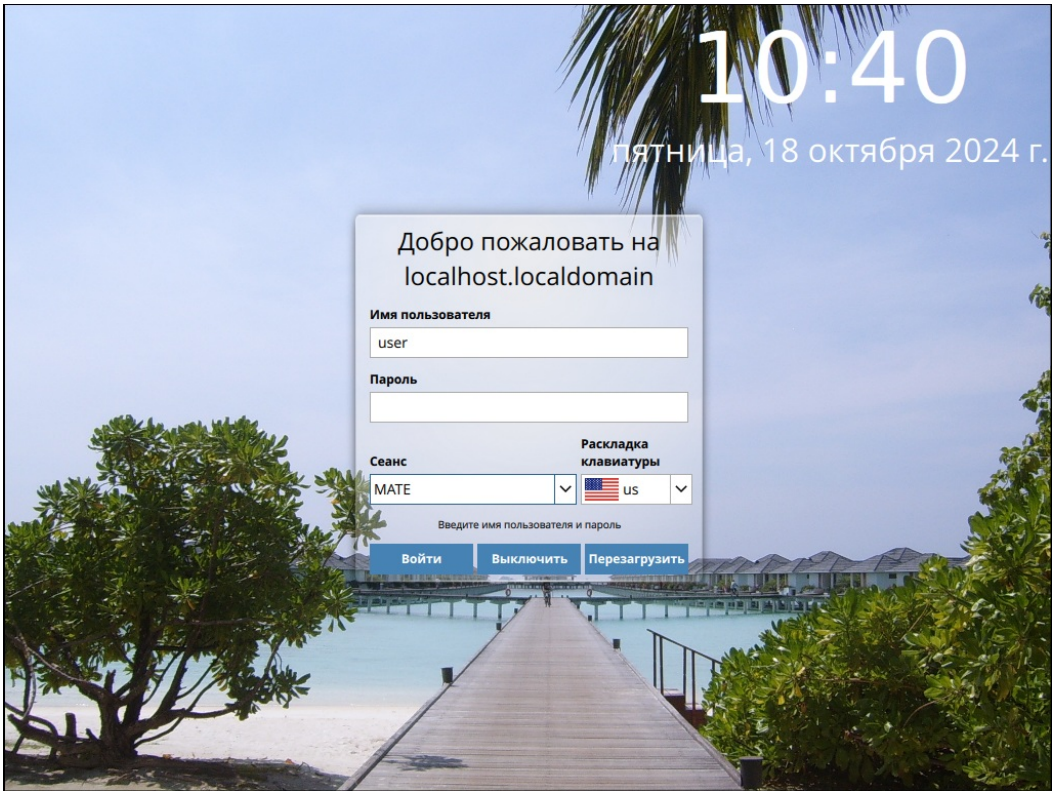
Тема **elarun** выглядит следующим образом:



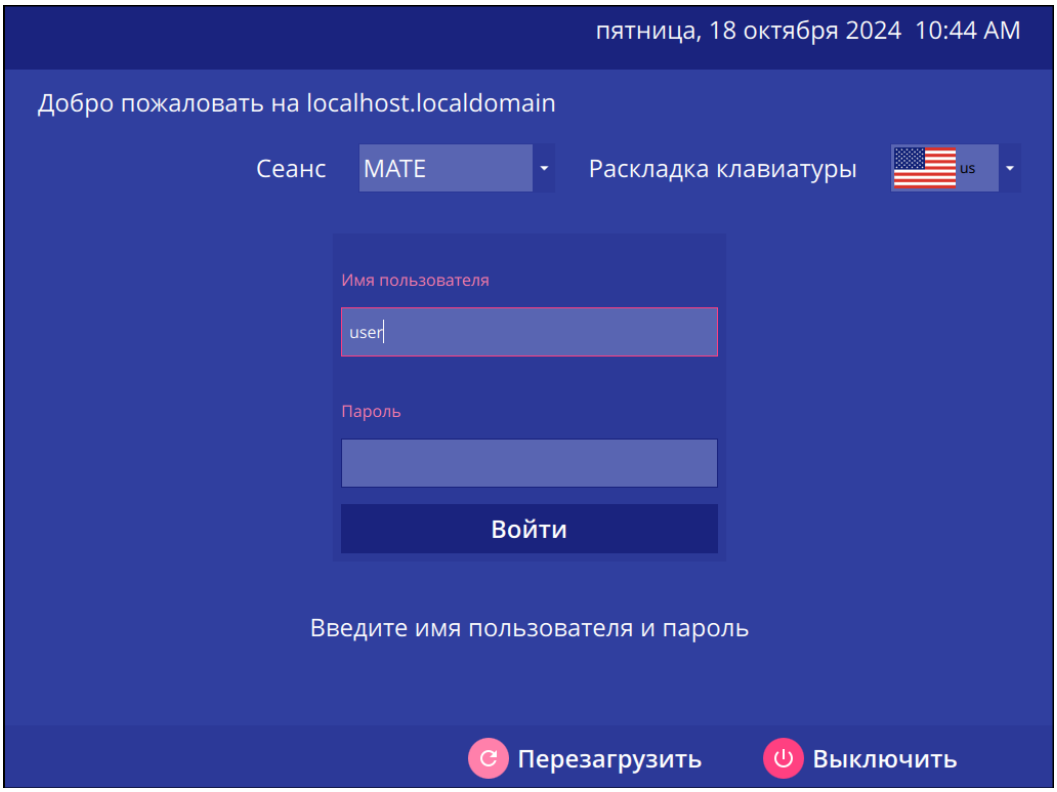
Обратите внимание! При входе в систему **под учетной записью доменного пользователя** с использованием темы **maldives**, в сеансе работы ограничиваются следующие возможности:

- доступ к звуковым устройствам;
- подключение USB-устройств, таких как флешки и веб-камеры.

Тема **maldives** выглядит следующим образом:



Тема **maya** выглядит следующим образом:



Для изменения темы необходимо в файле **/etc/sddm.conf** в графе [**Theme**] раскомментировать строку «**Current=**» и добавить предпочитаемую тему оформления вместо базовой.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и откройте файл в редакторе **nano**:

```
nano /etc/sddm.conf
```

```
[Theme]
# Current theme name
Current=elarun

# Cursor theme used in the greeter
#CursorTheme=

# Number of users to use as threshold
# above which avatars are disabled
# unless explicitly enabled with EnableAvatars
#DisableAvatarsThreshold=7

# Enable display of custom user avatars
#EnableAvatars=true
```

Также можно устанавливать и сторонние темы оформления для **sddm**.

Для корректной установки необходимо добавить скачанную тему в **/usr/share/sddm/themes/**, а после этого в файле **/etc/sddm.conf** изменить строку «**Current=**» на нужную.

Отключение информационного сообщения при входе в сеанс пользователя

ВАЖНО!

Отключение информационного сообщения при входе в сеанс пользователя нарушает условия сертификации ФСТЭК. Отключение данного информационного сообщения допускается **только в стандартной редакции ОС**.

Узнать редакцию установленной РЕД ОС можно командой `lsb_release -a | grep Edition:`

lsb_release -a | grep Edition:

```
Edition:    Standard
```

Для того, чтобы отключить информационное сообщение при входе в сеанс пользователя, нужно закомментировать последнюю строку (`/usr/bin/zenity --warning --text "$TEXTMSG" --no-wrap`) в файле **/etc/gdm/PreSession/Default**.

```
nano /etc/gdm/PreSession/Default
```

```
...
#/usr/bin/zenity --warning --text "$TEXTMSG" --no-wrap
```

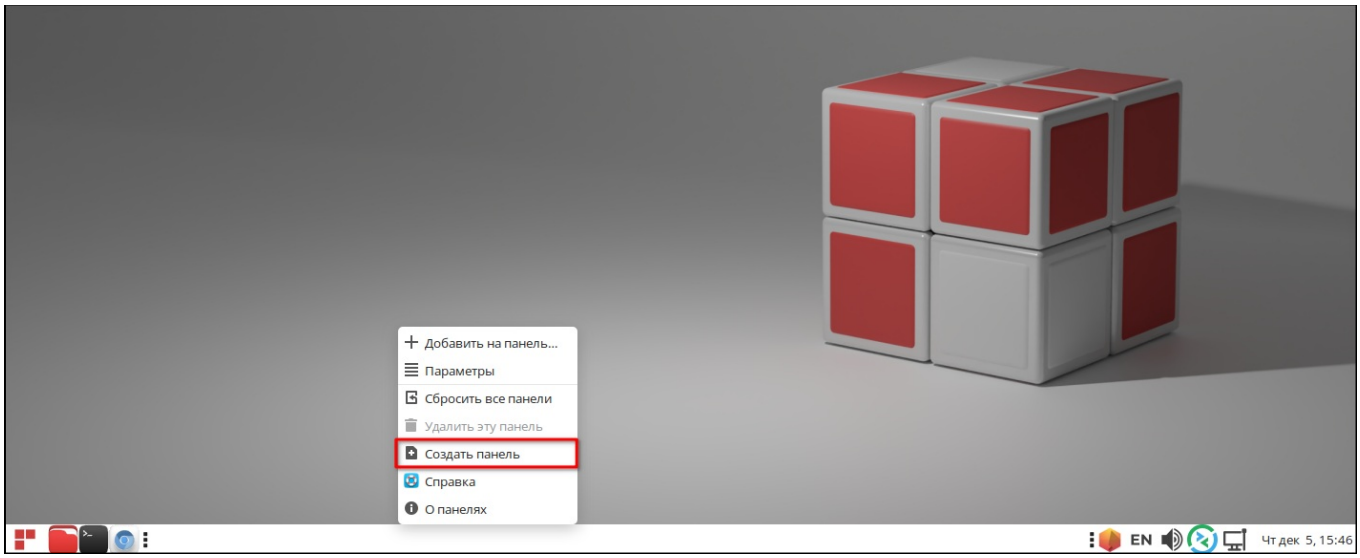
Добавление системной панели на второй монитор

Mate
KDE Plasma

Для удобства работы на втором мониторе зачастую требуется доступ к системной панели.

Mate

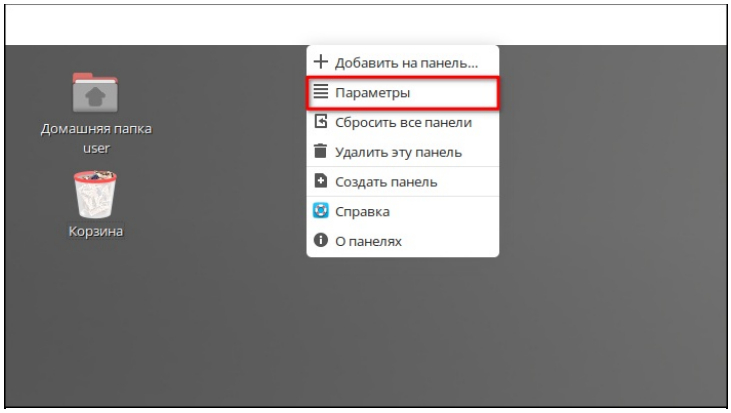
Для того чтобы добавить панель на второй монитор, необходимо нажать правой кнопкой мыши по панели на основном мониторе и выбрать в появившемся меню пункт «**Создать панель**».



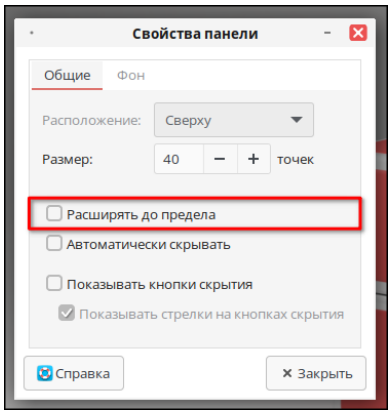
После выбора появится пустая панель в верхней части монитора.



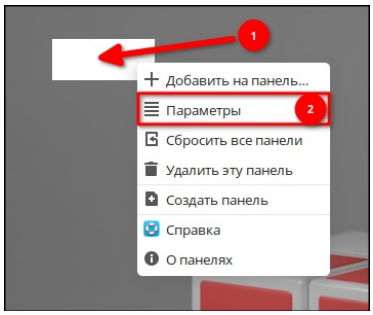
Нажимаем правой кнопкой мыши по новой панели и выбираем «**Параметры**».



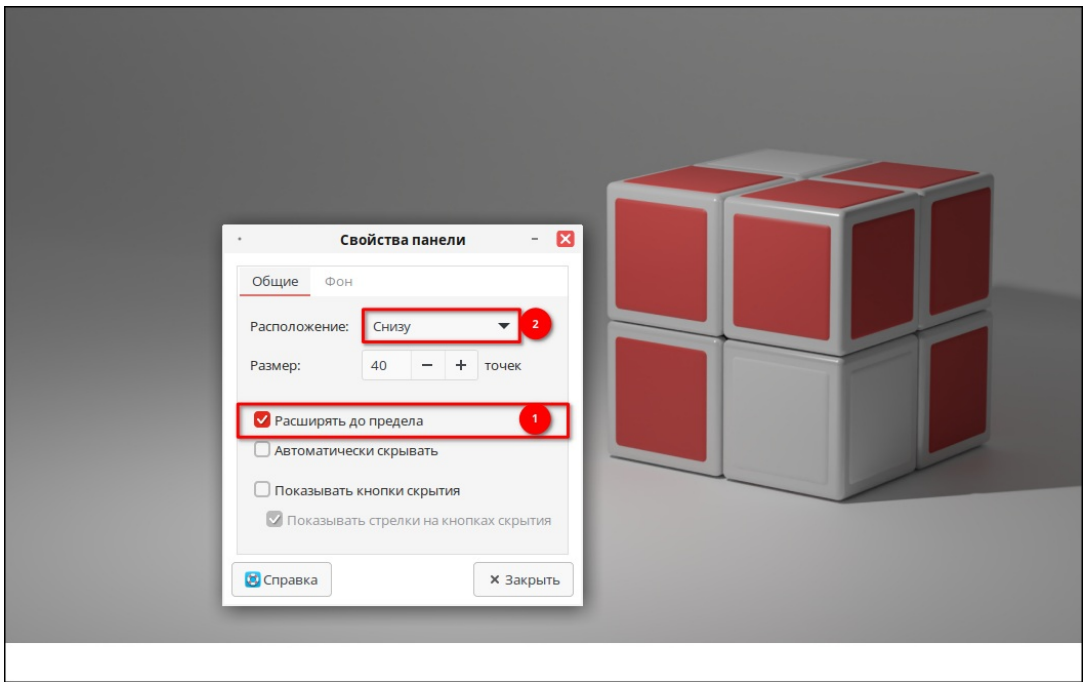
Снимаем галочку «**Расширять до предела**», панель изменит свои размеры.



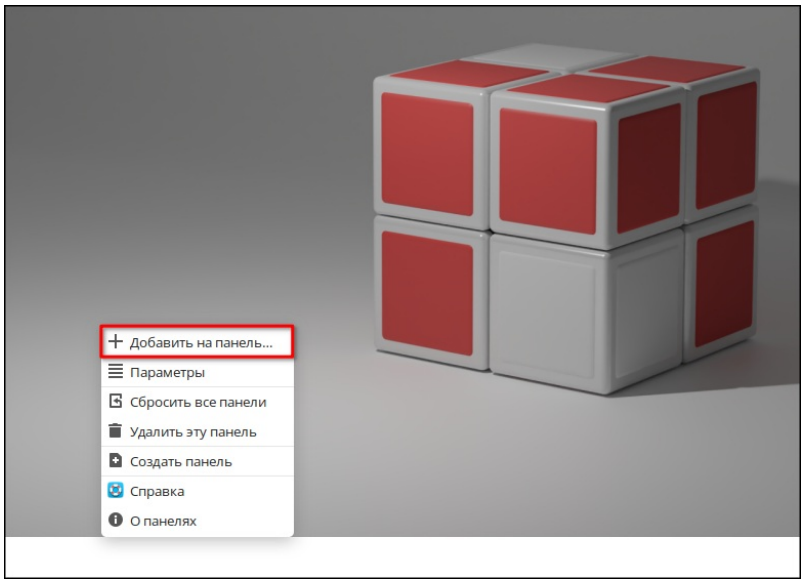
Далее при помощи мыши перетаскиваем панель на второй монитор, нажимаем на нее правой кнопкой (1) и выбираем «**Параметры**» (2).



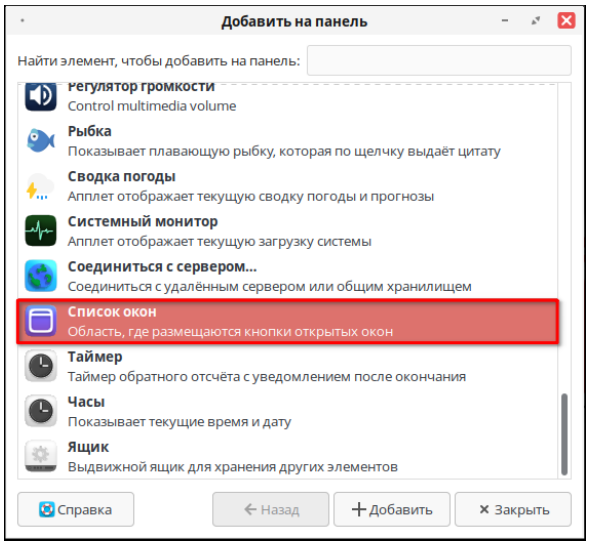
Устанавливаем галочку «**Расширять до предела**», выбираем расположение нашей панели.



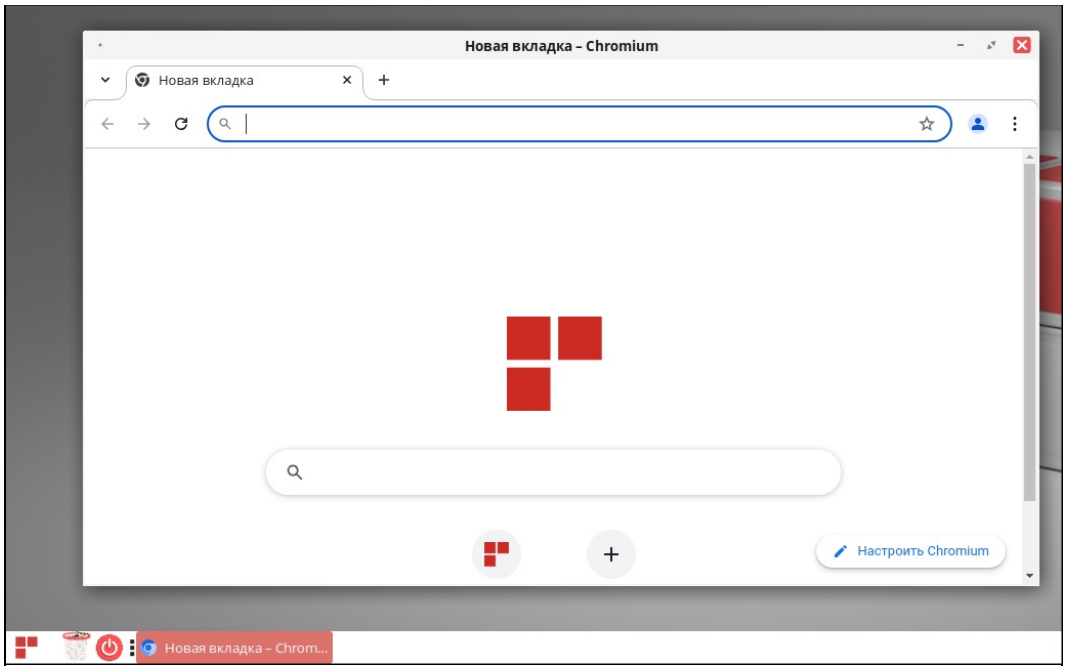
Чтобы добавить «**Список окон**» на новой панели, необходимо нажать на нее правой кнопкой мыши и выбрать «**Добавить на панель...**».



Из представленного списка выбираем «**Список окон**» и нажимаем «**Добавить**».



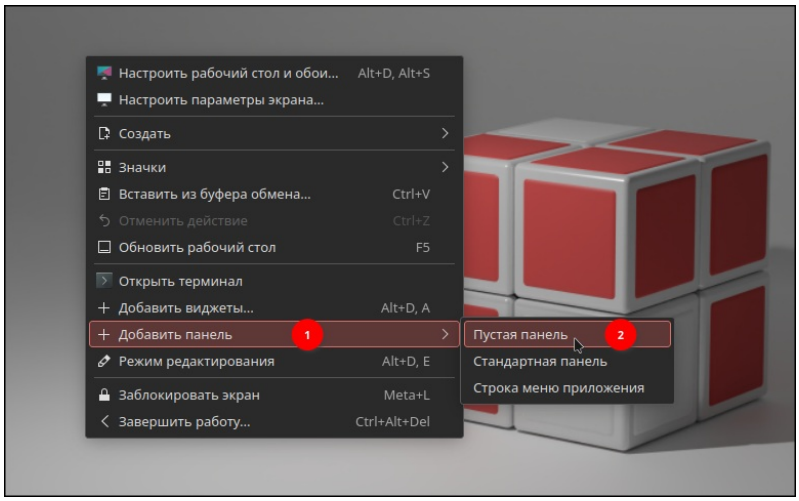
В результате на втором мониторе открытые окна приложений будут отображаться на системной панели.



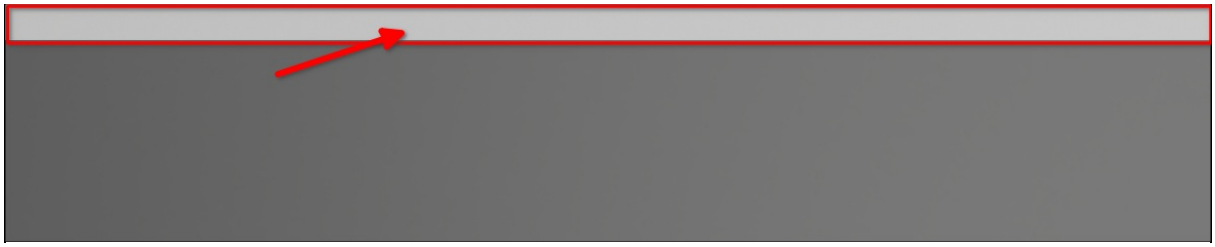
KDE Plasma

В **KDE Plasma** для того чтобы добавить панель на второй монитор, необходимо нажать правой кнопкой мыши по рабочему столу на

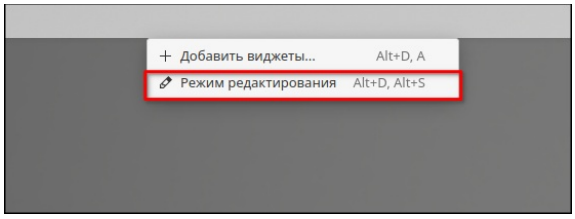
основном мониторе и выбрать в появившемся меню пункт «**Добавить панель**» - «**Пустая панель**».



После выбора появится пустая панель в верхней части монитора.



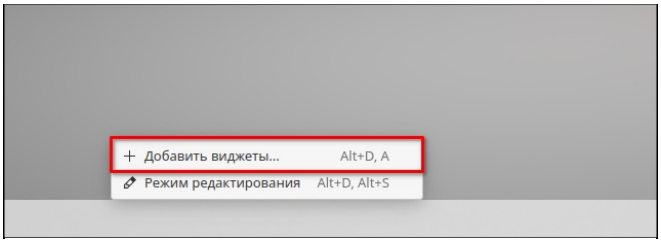
Нажимаем правой кнопкой мыши по новой панели и выбираем «**Режим редактирования**».



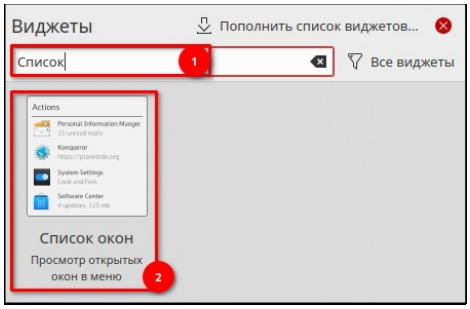
Переместите панель на второй монитор. Для этого нажмите на панель и, удерживая ее, перетащите её в нижнюю область экрана второго монитора.



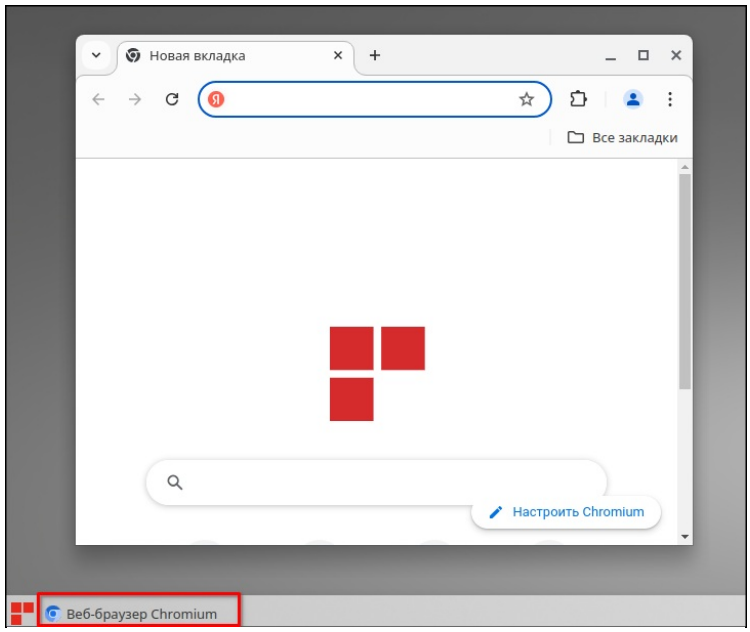
Для добавления виджета «**Список окон**» на новую панель необходимо нажать на нее правой кнопкой мыши и выбрать «**Добавить виджеты...**».



В строке поиска вводим название виджета и из представленного списка выбираем «**Список окон**».



В результате на втором мониторе открытые окна приложений будут отображаться на системной панели.


Новая вкладка
Все закладки
Настроить Chromium
Веб-браузер Chromium

Управление с помощью dconf

Возможности dconf
Управление ключами dconf
GSettings
Установка настроек рабочего стола по умолчанию
Блокировка настроек рабочего стола
Настройка общих для всех пользователей горячих клавиш
Dconf-editor

Возможности dconf

Dconf – низкоуровневая система конфигурации. При помощи **dconf** в **GNOME** и **Unity** хранятся настройки большинства программ.

Dconf это простая система конфигурации основанная на ключах. Ключи находятся в неструктурированной базе данных (ключи, логически связанные между собой объединены в категории). База данных хранится в бинарном файле, который располагается в **~/.config/dconf**.

Управление ключами dconf

В большинстве случаев пользователю не нужно вручную редактировать настройки хранящиеся в **dconf**. Но иногда графическое представление тому или иному параметру отсутствует и единственным способом изменить его значение является редактирование ключа напрямую. Это можно осуществить несколькими способами.

GSettings

GSettings - это консольная утилита, при помощи которой можно управлять ключами **dconf**.

Синтаксис использования **GSettings**:

```
gsettings [--schemadir <КАТАЛОГ_СХЕМ>] <КОМАНДА> [<АРГУМЕНТЫ>]
```

Команды:

Команда	**Описание**
help	Показать справку
list-schemas	Список установленных схем
list-relocatable-schemas	Список перемещаемых схем
list-keys	Список ключей схемы
list-children	Список потомков схемы
list-recursively	Список ключей и значений, рекурсивно
range	Запросить диапазон значений ключа
describe	Запросить описание ключа
get	Получить значение ключа
set	Изменить значение ключа
reset	Сбросить значение ключа
reset-recursively	Сбросить все значения в заданной схеме
writable	Проверить ключ на запись
monitor	Следить за изменениями

Для того чтобы получить более подробную справку по интересующей команде, выполните:

```
gsettings help <КОМАНДА>
```

Поиск соответствий схемы настройкам рабочего стола.

Здесь необходимо выяснить пути и названия элементов схемы, отвечающих за конкретные настройки рабочего стола. Например, что именно определяет фон или цвет рабочего стола.

Для начала открываем консоль и набираем от имени обычного пользователя:

```
gsettings list-schemas | grep background

org.mate.background
org.mate.SettingsDaemon.plugins.background
org.gnome.desktop.background
```

Тем самым мы получим список схем, в которых может содержаться интересующая нас информация. Теперь выясняем, что именно из перечисленного отвечает за интересующие нас настройки рабочего стола:

```
gsettings monitor org.mate.background
```

Откройте параметры рабочего стола и попробуйте изменить фон, цвет, или иной пункт. В терминале появится информация вида схема/ключ/значение.

```
gsettings list-recursively org.mate.background

org.mate.background picture-opacity 100
org.mate.background secondary-color '#3C8F25'
org.mate.background show-desktop-icons true
org.mate.background background-fade true
org.mate.background primary-color '#5891BC'
org.mate.background picture-filename '/usr/share/design/current/backgrounds/default.png'
org.mate.background color-shading-type 'vertical-gradient'
org.mate.background picture-options 'zoom'
org.mate.background draw-background true
```

Установка настроек рабочего стола по умолчанию

Здесь административно установить настройки рабочего стола, которые будут применяться у всех вновь создаваемых пользователей. Например, так можно определить конкретный фон или цвет рабочего стола. Эти изменения не затронут ранее созданных пользователей, которые уже используют графическую среду. Кроме того, пользователи смогут изменить установленные администратором настройки, если захотят. Чтобы заблокировать им такую возможность, читайте следующий раздел.

Все действия выполняются с правами пользователя **root**:

```
su -
```

Создаём файл (если уже существует, то оставьте без изменений):

```
nano /etc/dconf/profile/user
```

```
user-db:user
system-db:local
```

Создаём директорию:

```
mkdir -p /etc/dconf/db/local.d
```

Создаём файл:

```
nano /etc/dconf/db/local.d/00_background
```

Сохраняем в него только те ключи и значения, полученные на шаге 1, которые нас интересуют. В квадратных скобках указываем название схемы.

```
[org/mate/desktop/background]
secondary-color='#858 5d4d45b5b'
background-fade=true
primary-color='#babadada5555'
picture-filename='/usr/share/backgrounds/mate/desktop/MATE-Stripes-Dark.png'
color-shading-type='vertical-gradient'
picture-options='zoom'
```

```
draw-background=true
```

Блокировка настроек рабочего стола

Пока были определены значения, которые в дальнейшем будут использоваться по умолчанию. Пользователь всё ещё имеет возможность их поменять. Чтобы пользователь не мог внести изменения в настройки рабочего стола никакими средствами, создадим ещё один файл:

```
nano /etc/dconf/db/local.d/locks/00_background
```

```
/org/mate/desktop/background/secondary-color
/org/mate/desktop/background/background-fade
/org/mate/desktop/background/primary-color
/org/mate/desktop/background/picture-filename
/org/mate/desktop/background/color-shading-type
/org/mate/desktop/background/picture-options
/org/mate/desktop/background/draw-background
```

и выполним команду:

```
dconf update
```

Здесь стоит обратить внимание, что схема указана другая - не **/org/mate/background**, а **/org/mate/desktop/background**. В случае с **MATE** это связано с особенностью обработки схем **dconf** и **gsettings**. Посмотреть текущие схемы можно в директории **/usr/share/glib-2.0/schemas**.

Новые настройки вступают в силу немедленно.

Пример настройки dconf - настройка общих для всех пользователей горячих клавиш

Для понимания, какие параметры **dconf** требуется изменить, выполните в терминале команду для «прослушивания» изменений в системе:

```
dconf watch /
```

Параллельно с запущенным **dconf** зайдите в графическую утилиту «**Сочетание клавиш клавиатуры**» («**Главное меню**» — «**Параметры**») и настройте нужные вам сочетания клавиш.

В терминале вы увидите применяемые изменения, например:

```
dconf watch /
/org/mate/marco/global-keybindings/run-command-window-screenshot
 '<Alt>F3'
```

Далее создайте файл (если уже существует, то оставьте без изменений):

```
nano /etc/dconf/profile/user
```

с содержимым:

```
user-db:user
system-db:local
```

Создайте файл, который будет отвечать за настройки по умолчанию:

```
nano /etc/dconf/db/local.d/00_session
```

```
[org/mate/marco/global-keybindings]
run-command-window-screenshot='<Alt>F3'
```

И в конце обновите **dconf** командой:

```
dconf update
```

После этого для новых пользователей будут вступать в силу параметры нового **dconf** по умолчанию.

Dconf-editor

Dconf-editor – является наиболее часто используемым графическим приложением для редактирования ключей **dconf**. В приложении все ключи представлены в виде дерева, можно искать ключи по их названию, жирным текстом выделяются ключи, значение которых было изменено.

По умолчанию **dconf-editor** не установлен на РЕД ОС. Чтобы установить его нужно использовать специальную команду в консоли:

```
sudo dnf install dconf-editor
```

Для запуска используется консольная команда:

```
dconf-editor
```

С помощью **dconf-editor** можно получить быстрый доступ к множеству "скрытых" настроек, как системных, так и внешнего вида, позволяя быстро сделать в системе комфортное и удобное для себя рабочее окружение.

Настройка режимов работы мониторов с помощью XRandR

Добавление нового разрешения экрана
Работа с несколькими мониторами
Настройка положения монитора
Настройка виртуального разрешения
Поворот изображения
Отключение монитора

Добавление нового разрешения экрана

Бывают ситуации, когда после установки ОС при подключении монитора нет нужного разрешения для используемого монитора. Для решения подобных проблем можно воспользоваться программой XRandR.

XRandR – это официальная программа настройки оконной системы. С ее помощью можно изменить параметры вывода изображения на экране, такие как размер, ориентация или отражение выходных данных. Также можно установить размер самого экрана. Для того, чтобы задать требуемый размер экрана в РЕД ОС, необходимо выполнить несколько шагов:

1. Создать файл конфигурации:

```
nano /etc/X11/xorg.conf
```

Откроется пустой файл, в который необходимо скопировать следующую настройку:

```
Section "Device"
 Identifier "Configured Video Device"
 EndSection

 Section "Monitor"
 Identifier "Configured Monitor"
 EndSection

 Section "Screen"
 Identifier "Default Screen"
 Monitor "Configured Monitor"
 Device "Configured Video Device"
 EndSection
```

2. Сохранить документ, нажав сочетание клавиш *«CTRL+O»*, и выполнить команду:

```
gtf 1920 1600 60 >> /etc/X11/xorg.conf
```

После выполнения команды в ранее сохраненный файл конфигурации будут добавлены новые строки:

```
# 1920x1600 @ 60.00 Hz (GTF) hsync: 99.36 kHz; pclk: 260.72 MHz
 Modeline "1920x1600_60.00" 260.72  1920 2064 2272 2624  1600 1601 1604 1656  -HSync +Vsync
```

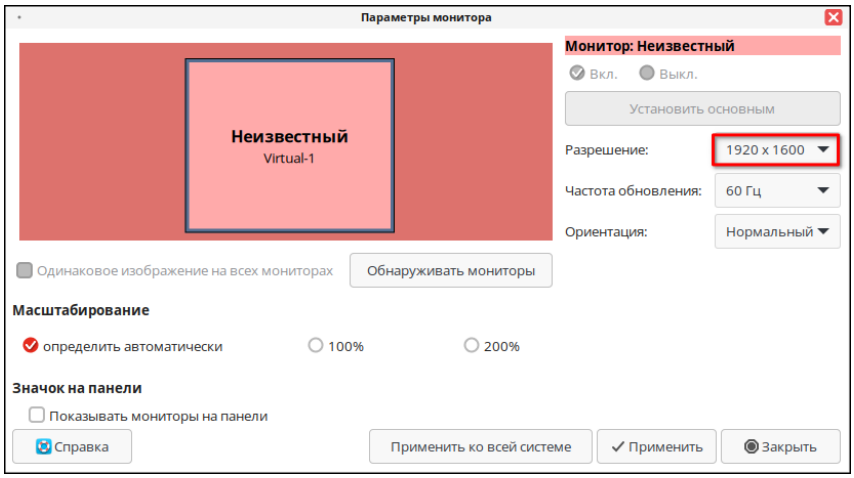
Последнюю строку необходимо переместить в блок **Section «Monitor»**. Должен получиться примерно такой код:

```
Section "Monitor"
 Identifier "Configured Monitor"
 Modeline "1920x1600_60.00" 260.72  1920 2064 2272 2624  1600 1601 1604 1656  -HSync +Vsync
 EndSection
```

3. Перезагрузить компьютер.

4. Перейти в *«Параметры системы»* - *«Экран»*. В графе *«Разрешение экрана»* должно появиться указанное разрешение 1920x1080.

Результат настройки конфигурации.



Работа с несколькими мониторами

Для отображения списка интерфейсов, по которым могут быть подключены мониторы, а также доступных режимов работы монитора (разрешение и частота обновления в герцах) выполните команду:

```
xrandr

Screen 0: minimum 320 x 200, current 1920 x 1600, maximum 8192 x 8192
VGA-1 connected primary 1920x1600+0+0 0mm x 0mm
   1920x1600     60.00*
   1920x1080     60.00
   1680x1050     59.95
   1280x1024     75.02    60.02
   1440x900      59.89
   1280x960      60.00
   1280x854      59.95
   1280x720      60.00
   1024x768      75.03    70.07    60.00
   832x624       74.55
   800x600       72.19    75.00    60.32    56.25
   640x480       75.00    72.81    66.67    59.94
   720x400       70.08
DP-1 disconnected
HDMI-1 disconnected
```

Вывод команды сообщает, что в данный момент монитор подключен к видеокарте по порту **VGA-1**, порты **DP-1** и **HDMI-1** отключены.

В случае, если РЕД ОС используется на ноутбуке, моноблоке или другом устройстве, имеющем встроенный дисплей, интерфейс может иметь название **LVDS** или **DSI**.

При подключении второго монитора система определит первый подключенный монитор как основной. Для изменения основного монитора необходимо выполнить команду вида:

```
xrandr --output <интерфейс> --primary
```

Например:

```
xrandr --output HDMI-1 --primary
```

Данная команда установит монитор, подключенный по **HDMI-1**, в качестве основного.

Настройка положения монитора

Также можно настроить положение мониторов относительно друг друга. Например, мониторы подключены к портам **VGA-1** и **HDMI-1**. Необходимо монитор **HDMI-1** расположить справа относительно монитора **VGA-1**. Для этого следует выполнить команду:

```
xrandr --output "HDMI-1" --right-of "VGA-1"
```

Аналогично можно использовать параметр **--left-of**.

Настройка виртуального разрешения

В случае, если необходимо сделать виртуальный экран большего разрешения, чем физический, используется команда:

```
xrandr --output <интерфейс> --mode 1920x1080 --fb 2560x1440 --panning 2560x1440
```

После использования данной команды размер виртуального разрешения будет установлен 2560x1440 пискелей при размере 1920x1080 пислелей физического.

ВАЖНО!

Данный режим **НЕ** работает как DSR от Nvidia или Виртуальное сверхвысокое разрешение от AMD, и изображение не будет подстраиваться под реальное разрешение экрана, объекты вне границ экрана отображаться не будут.

Поворот изображения

Для поворота изображения на экране для нужного интерфейса используется параметр **--rotate**, где значения **left** и **right** поворачивают изображение в указанную сторону. Также можно использовать параметр **inverted** для поворота экрана на 180°.

Отключение монитора

Отключить ненужный в данный момент дисплей можно с помощью опции **--off**, например:

```
xrandr --output HDMI-1 --off
```

Дисплей, подключенный через порт **HDMI-1**, будет отключен.

RedShift - утилита изменения цветового профиля экрана

Основные настройки программы
Сохранение настроек
Автозагрузка

RedShift — свободное программное обеспечение, которое изменяет цветовой профиль экрана в зависимости от времени суток и местоположения, снижая утомляемость глаз при продолжительной работе у монитора.

Для того чтобы начать работать с программой, необходимо установить пакет из репозитория командой (потребуются права **администратора**):

```
sudo dnf install redshift redshift-gtk
```

Вы можете подробнее ознакомиться с работой утилиты **RedShift**, просмотрев наши обучающие видео:

- на **RuTube** — RedShift - утилита изменения цветового профиля экрана;
- в **Яндекс.Дзен** — RedShift - утилита изменения цветового профиля экрана;
- в **VK Видео** — RedShift - утилита изменения цветового профиля экрана.

На наших каналах вы также сможете найти много другой полезной информации.

Основные настройки программы

1. Настройки температуры.

RedShift равномерно переводит цветовую температуру дисплея компьютера между дневной и ночной температурами, чтобы глаза пользователя могли медленно адаптироваться.

Ночью цветовая температура низкая и обычно составляет **3000–4000 K**, что предпочтительно соответствует температуре освещения в комнате.

Типичная цветовая температура в дневное время составляет **5500–6500 K**. Чтобы задать температуру в формате ***День*:*Ночь*** используется команда:

```
redshift -t 6500:3500
```

где **6500** - температура по умолчанию.

Установка значения **более 6500** приводит температуру к более холодному синему цвету, а установка значения **менее 6500** приводит температуру к более теплому красному цвету.

2. Настройки яркости.

Регулировка уровня яркости подсветки монитора осуществляется изменением уровня освещенности экрана от светлого до тёмного. Низкая освещённость преимущественно используется в вечернее и ночное время. Высокая интенсивность свечения полезна для работы днём. Благодаря регулировке яркости монитора можно снять лишнее напряжение с глаз.

Чтобы задать яркость, используется команда:

```
redshift -b 0.5
```

Значение яркости можно установить в диапазоне **от 0.1 до 1.0**.

3. Настройка гаммы.

Гамма показывает соотношение между уровнями трех основных цветов цветового пространства RGB и силу излучаемого монитором светового потока.

Чтобы задать значение гаммы, используется команда:

```
redshift -g 0.5
```

Значение гаммы можно установить в диапазоне **от 0.1 до 1.0**.

Сохранение настроек

Для того чтобы настройки работали постоянно, необходимо создать файл настроек в **/home/user**, где ***user*** — имя пользователя.

```
nano /home/user/.config/redshift.conf
```

Записываем в файл конфигурации параметры в следующем виде:

```
[redshift]temp-day=6500
temp-night=3500

transition=1

brightness-day=0.8
brightness-night=0.6

gamma=0.8
```

где:

- ***temp-day*** — температура цвета днем;
- ***temp-night*** — температура цвета ночью;
- ***transition*** — определяет плавный переход между температурой (при значении 0 сразу устанавливает значение температуры, при значении 1 осуществляется плавный переход);
- ***brightness-day*** — яркость днем;
- ***brightness-night*** — яркость ночью;
- ***gamma*** — установка гаммы для всех цветов.

Сохраняем и закрываем файл.

Далее запускаем программу ***RedShift*** через терминал командой:

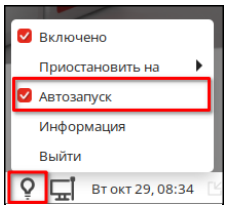
```
redshift-gtk
```

или через «**Главное меню**» — «**Стандартные**» — «**Redshift**».

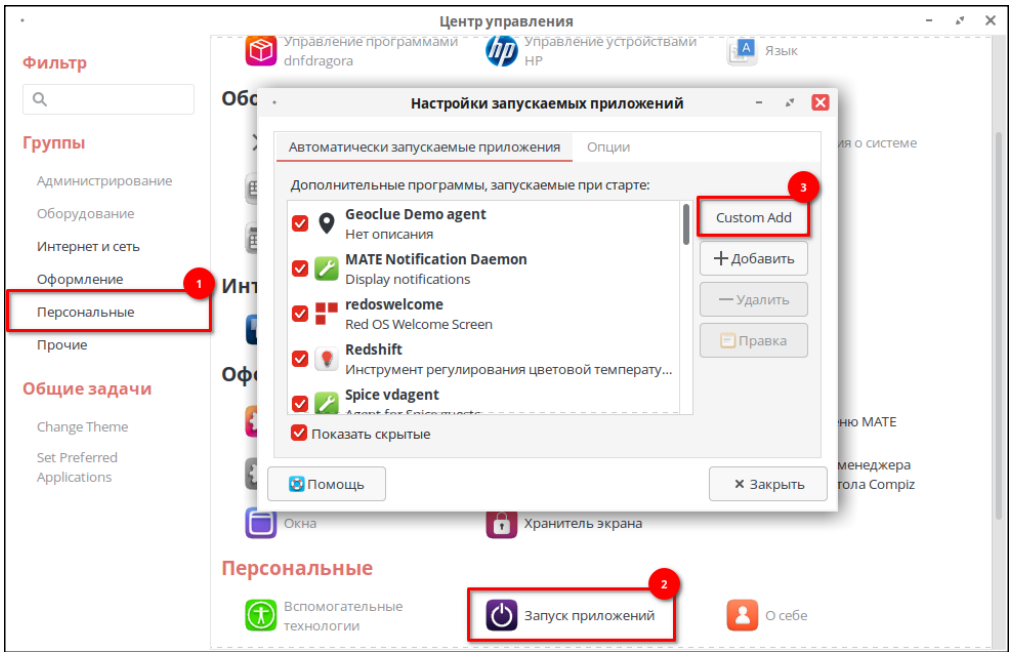
На панели задач должен появиться значок ***RedShift***, при этом применятся все настройки, выставленные в файле конфигурации.

Автозагрузка

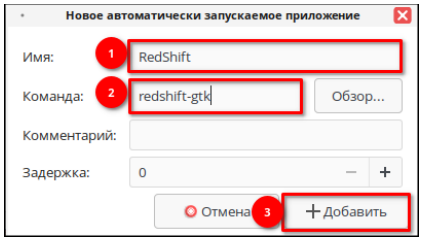
Для добавления ***RedShift*** в автозагрузку можно воспользоваться функцией «**Автозапуск**» в меню ***RedShift***.



Также можно воспользоваться средствами операционной системы. В **MATE** для этого заходим через «**Главное меню**» — «**Центр управления**». Открываем раздел «**Персональные**» (1) — «**Запуск приложений**» (2). Далее нажимаем кнопку «**Custom Add**» (3).



В поле «**Имя**» вписываем **RedShift** (1), в поле «**Команда**» — **redshift-gtk** (2) и нажимаем «**Добавить**» (3).



После перезагрузки ***RedShift*** запустится автоматически.

Панель быстрого запуска Plank

Установка и запуск
Настройка plank
Описание настроек Plank
Добавление и удаление значков
Установка тем в Plank

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** plank-0.11.89

Plank — панель, которую можно использовать для запуска, переключения между запущенными приложениями, выводить различную информацию, такую как системные уведомления, пользовательские сообщения и т. п. Преимущество дока над обычной панелью заключается в гибкости настройки — с легкостью можно изменить размер, место расположения, эффекты, заставить ее появляться и исчезать в нужный момент.

Вы можете подробнее ознакомиться с настройкой панели Plank, просмотрев наши обучающие видео:

- на **RuTube** — Новые темы для РЕД ОС. Установка панели быстрого запуска Plank;
- в **Яндекс.Дзен** — Новые темы для РЕД ОС. Установка панели быстрого запуска Plank.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и запуск

Устанавливается панель командой:

```
dnf install plank plank-docklets
```

Для запуска выполните команду:

```
plank
```

Также можно запустить *plank* с помощью меню: *«**Меню**»* — *«**Стандартные**»* — «***Plank***».

Добавление *plank* в автозапуск осуществляется командой:

```
ln -s /usr/share/applications/plank.desktop /etc/xdg/autostart/
```

Настройка plank

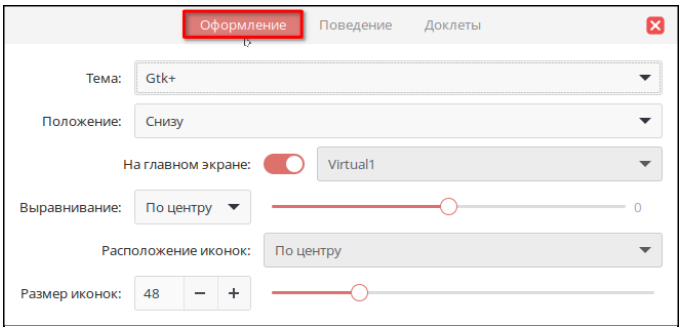
Чтобы вызвать панель настроек, необходимо ввести в консоли:

```
plank --preferences
```

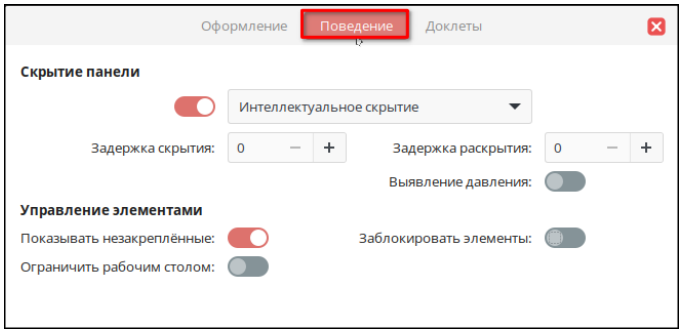
Также панель настроек можно запустить, нажав на панели *plank* *«**CTRL + ПКМ**»* — «**Параметры**».

Описание настроек Plank

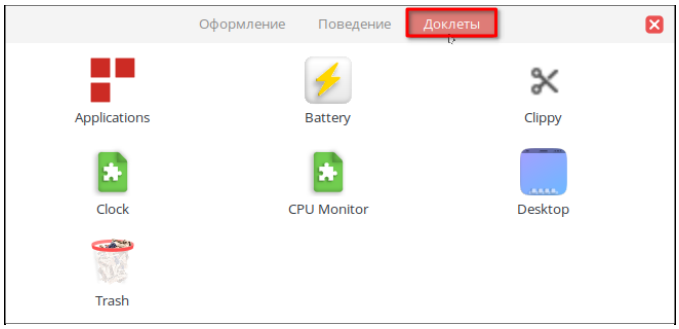
На вкладке «***Оформление***» можно изменить тему, положение *plank*, выбрать монитор для отображения панели, выбрать выравнивание, расположение и размер иконок.



На вкладке «***Поведение***» можно выбрать необходимый режим появления/скрытия *plank* либо отключить скрытие панели.

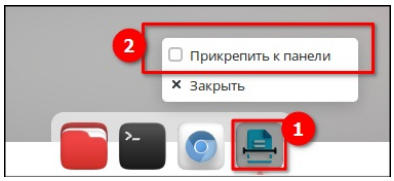


Доклеты на панель добавляются двойным кликом **ЛКМ**.



Добавление и удаление значков

Для того чтобы добавить новый значок на панель, необходимо запустить программу, и ярлык автоматически отобразится в *Plank*. Затем необходимо щёлкнуть **ПКМ** по нужному значку (1) и выбрать опцию «***Прикрепить к панели***» (2).



Для удаления значка нужно убрать галочку с опции «***Прикрепить к панели***» либо левой кнопкой мыши вытянуть его из панели.

Установка тем в Plank

Для начала нужно убедиться, что каталог для сохранения тем существует, перейдя по следующему пути:

```
cd ~/.local/share/plank/themes
```

Если данного каталога не существует, нужно его создать:

```
mkdir -p ~/.local/share/plank/themes
```

Чтобы извлечь скачанные темы в формате ***.zip**, выполните:

```
cd ~/Загрузки
unzip ShadesOfGray.zip
```

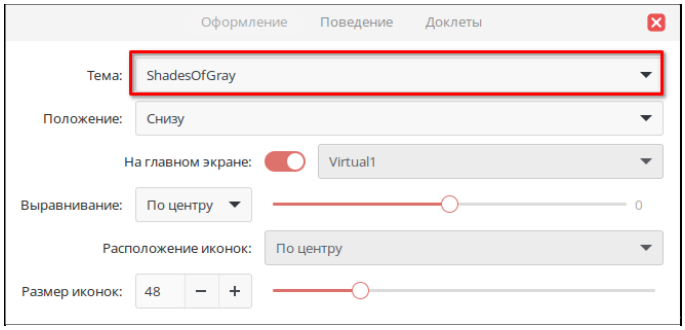
Для архивов тем формата ***.tar**, выполните:

```
cd ~/Загрузки
tar -zxvf ShadesOfGray.tar.gz
```

Перемещение файлов темы (убедитесь, что вы перемещаете фактическую папку темы, а не папку, содержащую папку темы) осуществляется командой:

```
mv ShadesOfGray ~/.local/share/plank/themes
```

После перемещения файлов во вкладке «***Тема***» появится соответствующая тема.



Shotwell - утилита для автоматической смены обоев рабочего стола (слайд-шоу)

Для установки слайд-шоу в качестве обоев рабочего стола используется приложение **Shotwell**.

Вы можете подробнее ознакомиться с настройкой приложения **Shotwell**, просмотрев наши обучающие видео:

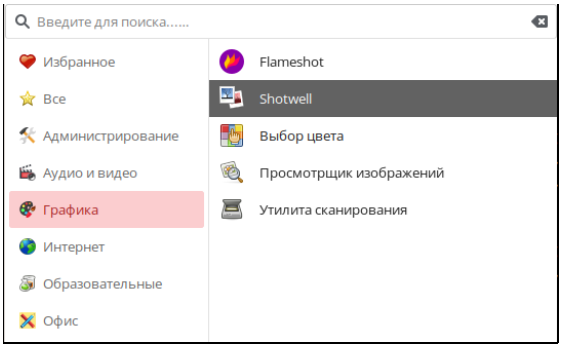
- на **RuTube** — Автоматическая смена обоев рабочего стола. Shotwell;
- в **Яндекс.Дзен** — Автоматическая смена обоев рабочего стола. Shotwell;
- в **VK Видео** — Автоматическая смена обоев рабочего стола. Shotwell.

На наших каналах вы также сможете найти много другой полезной информации.

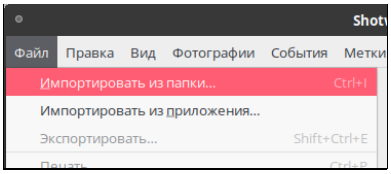
Установить его можно следующей командой:

```
dnf install shotwell
```

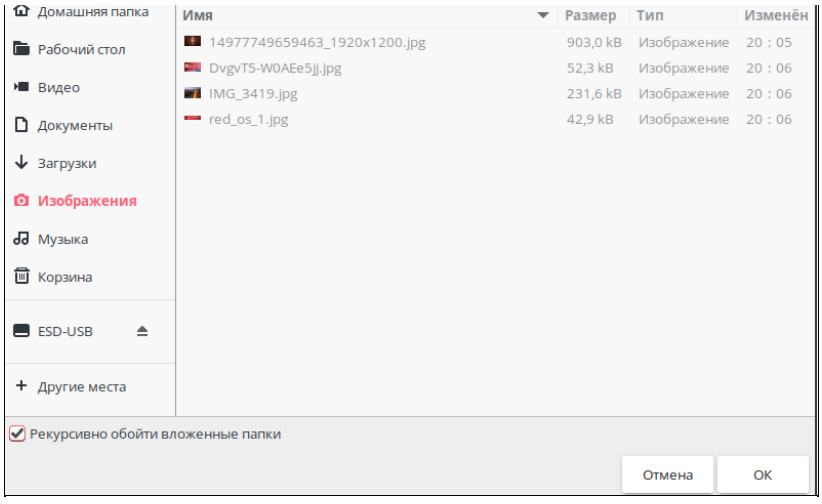
Программа будет доступна из «*Меню*»— «*Графика*» — «*Shotwell*».



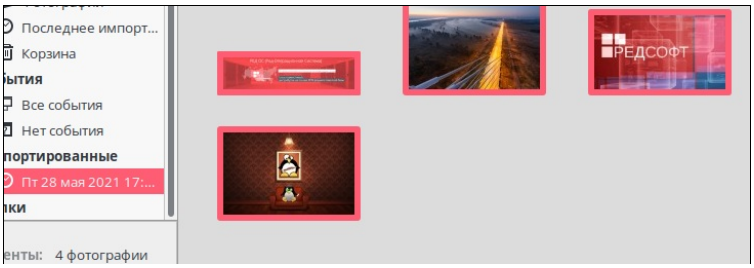
Для того чтобы создать слайд-шоу из собственных снимков/обоев на рабочем столе РЕД ОС, у вас в локальной папке уже должны быть сохранены какие-то снимки или обои из сети, которые отобразятся в Shotwell. Для того чтобы они отобразились, их нужно импортировать. Для этого необходимо выбрать *«Файл»→»Импортировать из папки...»*.



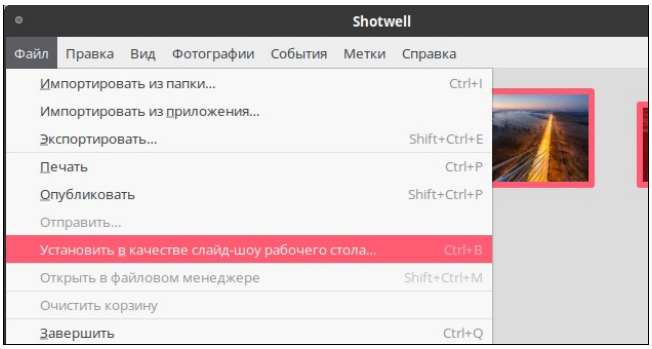
Выбираем каталог с изображениями и нажимаем **«OK»**.



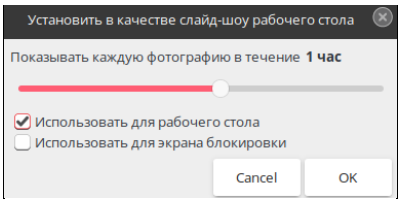
После того как изображения были импортированы в программу, можно приступать к созданию слайд-шоу. Для этого выбираем изображения, которые хотим видеть в слайд-шоу.



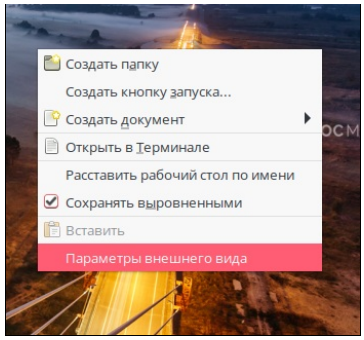
Затем нажимаем на *«Файл»→»Установить в качестве слайд-шоу рабочего стола»*.



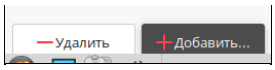
Откроется окно настройки времени и места использования данного слайд-шоу. Настраиваем под себя и нажимаем **«OK»**.



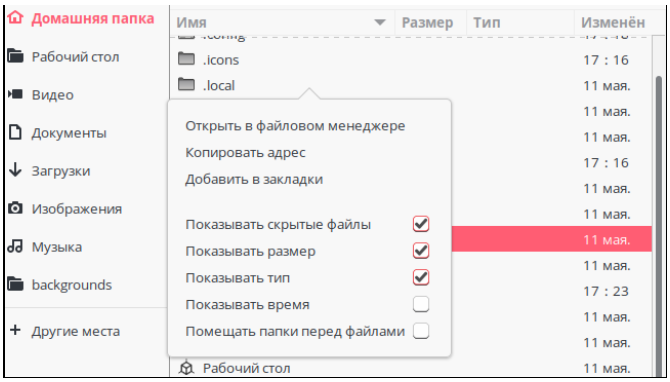
После этого нажимаем правой кнопкой мыши на рабочем столе и открываем параметры внешнего вида.



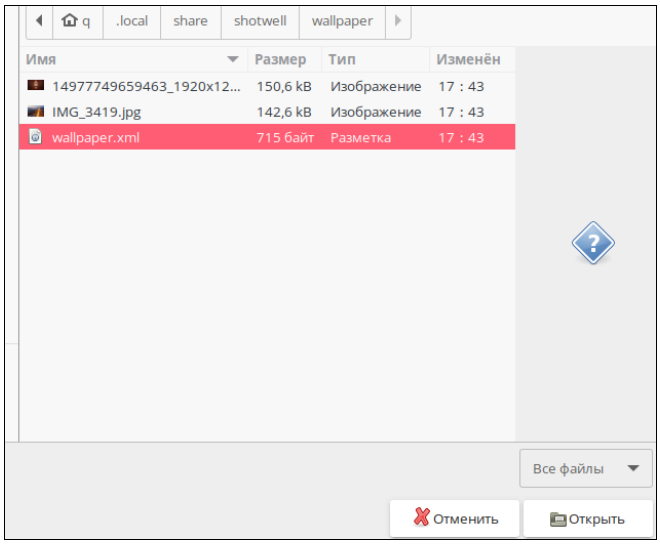
В открывшемся окне нажимаем **«Добавить»**.



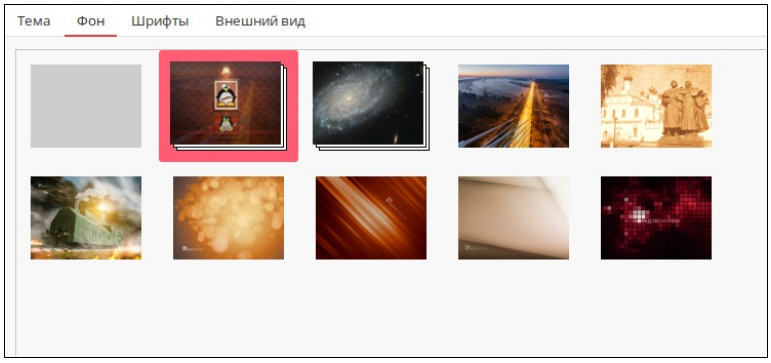
В каталоге **«Домашняя папка»** нажимаем ПКМ и включаем показ скрытых файлов.



Открываем каталог **.local/share/shotwell/wallpaper**, в нем будет находиться **wallpaper.xml** - это созданное слайд-шоу. Для того чтобы его увидеть, нужно включить отображение всех файлов и после этого выбрать **wallpaper.xml**.



Далее в окне появится созданное слайд-шоу для рабочего стола, выбираем его.



Готово! Автоматическая смена обоев настроена.

В дальнейшем будет достаточно просто изменить слайд-шоу в Shotwell.

Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев

Установка zenity
Синтаксис и опции
Примеры использования
Диалоговое окно для вывода предупреждения
Диалоговое окно с запросом
Диалоговое окно с календарем
Диалоговое окно с полем ввода
Добавление zenity в bash-сценарии
Пример 1 Диалоговое окно с сообщением
Пример 2 Диалоговое окно формы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zenity-3.99.90

Zenity — кроссплатформенная утилита, позволяющая создавать различные типы диалоговых окон GTK+ в командной строке и сценариях командной оболочки. Утилита упрощает взаимодействие между пользователем и командной оболочкой.

Вы можете подробнее ознакомиться с возможностями графического окружения **MATE**, просмотрев наши обучающие видео:

- на **RuTube** — Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- в **Яндекс.Дзен** — Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- в **VK Видео** — Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев .

На наших каналах вы также сможете найти много другой полезной информации.

Установка zenity

По умолчанию в РЕД ОС утилита **zenity** уже установлена (расположена в каталоге /usr/bin/zenity). Проверьте, установлена ли утилита **zenity** в вашей системе и доступна ли она для использования, выполнив следующую команду:

```
which zenity
```

Если по какой-либо причине утилита zenity не установлена, для ее установки выполните команду (потребуются права **администратора**):

```
sudo dnf install zenity
```

Синтаксис и опции

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
zenity [опции]
```

Основные опции:

- **-h, --help** — вывести справку по работе с утилитой;
- **--version** — вывести версию утилиты;
- **--about** — просмотреть информацию о программе;
- **--help-general** — показать общие параметры.

Виды диалоговых окон:

- **--calendar** — диалоговое окно выбора даты;
- **--entry** — диалоговое окно с полем ввода текста;
- **--error** — диалоговое окно для вывода ошибки;
- **--info** — диалоговое окно для вывода информации;
- **--file-selection** — диалоговое окно выбора файлов;

- **--list** — диалоговое окно со списком;
- **--notification** — диалоговое окно уведомления;
- **--progress** — диалоговое окно выполнения процесса;
- **--question** — диалоговое окно запроса;
- **--warning** — диалоговое окно предупреждения;
- **--scale** — диалоговое окно шкалы;
- **--text-info** — диалоговое окно с текстовой информацией;
- **--color-selection** — диалоговое окно выбора цвета;
- **--password** — диалоговое окно пароля;
- **--forms** — диалоговое окно формы.

Параметры общего назначения:

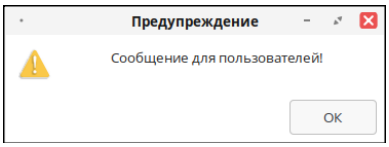
- **--title="ЗАГОЛОВОК"** — установить заголовок диалога;
- **--width=<ШИРИНА>** — установить ширину;
- **--height=<ВЫСОТА>** — установить высоту;
- **--timeout=<ЗАДЕРЖКА>** — установить задержку диалога в секундах;
- **--ok-label="ТЕКСТ"** — установить метку для кнопки «OK»;
- **--cancel-label="ТЕКСТ"** — установить метку для кнопки «Отменить»;
- **--extra-button="ТЕКСТ"** — добавить дополнительную кнопку;
- **--modal** — установить модальное свойство.

Примеры использования

Диалоговое окно для вывода предупреждения

Для вывода диалогового окна с предупреждением введите в терминал команду:

```
zenity --warning --text="Сообщение для пользователей" --width=300
```



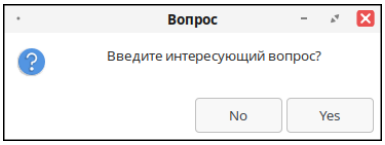
Параметры диалога предупреждения:

- **--warning** — показать диалог с предупреждением;
- **--text="ТЕКСТ"** — установить текст диалога;
- **--icon="ИМЯ_ЗНАЧКА"** — установить имя значка;
- **--no-wrap** — запретить перенос текста;
- **--no-markup** — не включать разметку Pango;
- **--ellipsize** — включить усечение текста в диалогах для уменьшения размера окна с длинным текстом.

Диалоговое окно с запросом

Для вывода диалогового окна с вопросом введите в терминал следующую команду:

```
zenity --question --text="Введите интересующий вопрос?" --width=300
```



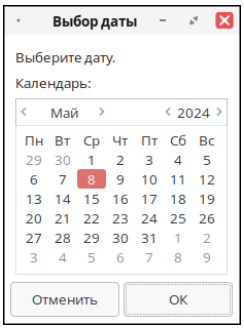
Параметры, используемые для запроса:

- **--question** — показать диалог с запросом;
- **--text="ТЕКСТ"** — установить текст диалога;
- **--icon="ИМЯ_ЗНАЧКА"** — установить имя значка;
- **--no-wrap** — запретить перенос текста;
- **--no-markup** — не включать разметку Pango;
- **--default-cancel** — фокус по умолчанию находится на кнопке «Отменить»;
- **--ellipsize** — включить усечение текста в диалогах для уменьшения размера окна с длинным текстом;
- **--switch** — скрыть кнопки «OK» и «Отменить».

Диалоговое окно с календарем

Для вывода диалогового окна с календарем для выбора желаемой даты введите следующую команду:

```
zenity --calendar
```



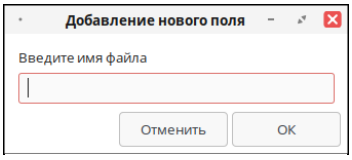
Параметры, используемые для вывода диалогового окна, в котором будет отображен календарь:

- **--calendar** — показать диалог выбора даты;
- **--text="ТЕКСТ"** — установить текст, отображаемый над календарем;
- **--day=<ДЕНЬ>** — установить день в календаре (число от 1 до 31);
- **--month=<МЕСЯЦ>** — установить месяц в календаре (число от 1 до 12);
- **--year =<ГОД>** — установить год в календаре;
- **--date-format=<ШАБЛОН>** — установить формат возвращаемой даты.

Диалоговое окно с полем ввода

Для запроса данных для ввода от пользователя выполните:

```
zenity --entry --text="Введите имя файла"
```



Параметры ввода текста:

- **--entry** — показать диалог с полем ввода;
- **--text="ТЕКСТ"** — установить текст диалога;
- **--entry-text="ТЕКСТ"** — установить текст для поля ввода;
- **--hide-text** — скрывать текст в поле ввода.

Добавление zenity в bash-сценарии

Пример 1 Диалоговое окно с сообщением

Для создания диалогового окна с сообщением при первом входе пользователя в систему выполните следующий алгоритм действий.

В РЕД ОС 7.3:

Для отображения диалогового окна при первом входе в систему добавьте сценарий в файл **/etc/gdm/PreSession/Default**. Выполните следующий алгоритм действий.

1. Откройте файл **/etc/gdm/PreSession/Default**, выполнив команду в терминале (потребуются права **администратора**):

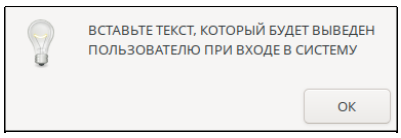
```
nano /etc/gdm/PreSession/Default
```

2. Добавьте в файл следующие строки и сохраните файл:

```
export LANG=ru_RU.UTF-8
 /usr/bin/zenity --info --text="ВСТАВЬТЕ ТЕКСТ, КОТОРЫЙ БУДЕТ ВЫВЕДЕН ПОЛЬЗОВАТЕЛЮ ПРИ ВХОДЕ В СИСТЕМУ" --width=300 --
height=150
```

где:

- **export LANG=ru_RU.UTF-8** — параметр, необходимый для работы с русским языком (является обязательным, иначе авторизация не будет проходить успешно);
- **--info** — диалог для вывода информации;
- **--text="ТЕКСТ"** — текст для отображения;
- **--width=<Значение>** — ширина диалогового окна;
- **--height=<Значение>** — высота диалогового окна.



В РЕД ОС 8.0:

1. Создайте файл в каталоге **/home/user1/** (замените user1 на актуальное имя пользователя):

```
nano /home/user1/zenitywel.sh
```

2. Добавьте в него следующие строки:

```
#!/bin/bash
 export LANG=ru_RU.UTF-8
 /usr/bin/zenity --info --text="Добро пожаловать" --width=300 --height=150
```

3. Выдайте права на исполнение файла:

```
chmod +x /home/user1/zenitywel.sh
```

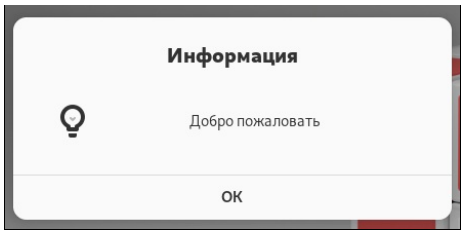
4. Создайте файл в каталоге **/etc/xdg/autostart/** для автозапуска уведомления во время авторизации пользователя:

```
nano /etc/xdg/autostart/WelcomeZenity.desktop
```

5. Добавьте в него следующие строки:

```
[Desktop Entry]
 Type=Application
 Name=Welcome Message
 Comment=Shows a welcome message
 Exec=/home/user1/zenitywel.sh
 Terminal=false
 X-MATE-Autostart-enabled=true #если используется графическая оболочка MATE
 X-GNOME-Autostart-enabled=true #если используется графическая оболочка GNOME
 X-KDE-Autostart-enabled=true #если используется графическая оболочка KDE
```

6. Перезапустите ПК. После авторизации пользователя отобразится диалоговое окно.



Пример 2 Диалоговое окно формы

Для создания **bash-скрипта** выполните следующий алгоритм действий:

1. Для создания файла скрипта введите команду:

```
nano newscript.sh
```

2. Впишите в файл следующие строки и сохраните файл:

```
#!/bin/bash

zenity --forms --title="Добавление сведений" \
	--text="Введите информацию ниже:" \
	--separator="," \
	--add-entry="Имя" \
	--add-entry="Фамилия" \
	--add-combo=Пол \
	--combo-values="мужской|женский"\
	--add-entry="СНИЛС" \
	--add-calendar="Дата рождения"

case $? in
0)
	echo "Информация добавлена.";;
1)
	echo "Информация не добавлена.";;
-1)
	echo "Произошла ошибка.";;
esac
```

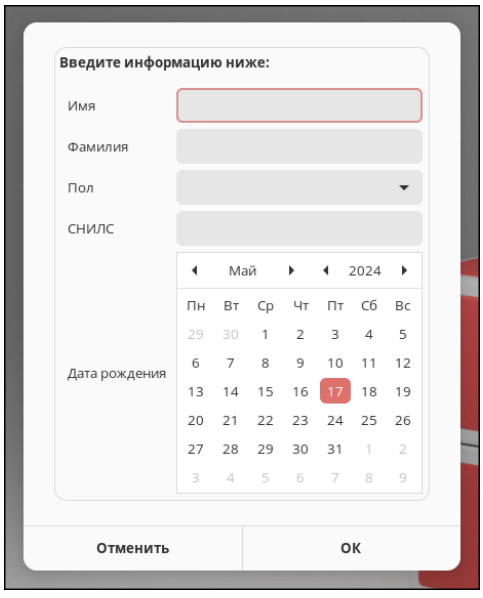
3. Для предоставления прав на выполнение файла выполните команду:

```
chmod +x newscript.sh
```

4. Для запуска скрипта выполните команду:

```
./newscript.sh
```

Результат выполнения скрипта:



С дополнительной информацией по созданию интерактивных меню можно ознакомиться в наших статьях:

- Dialog — утилита для создания диалоговых окон в консольных приложениях ;
- Yad — утилита для создания диалоговых окон с использованием терминала или сценариев .

Yad — утилита для создания диалоговых окон с использованием терминала или сценариев

Установка yad
Синтаксис и опции
Примеры использования
Диалоговое окно формы ввода
Диалоговое окно выбора цвета
Диалоговое окно с календарем
Ссылка в диалоговом окне
Список в диалоговом окне
Диалоговое окно для ввода текста
Добавление yad в bash-сценарии
Пример 1. Диалоговое окно записной книжки
Пример 2. Диалоговое окно с сообщением

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: yad-13.0

Yad (**Yet Another Dialog**) — программа для построения графических диалоговых окон (**GTK3**) из сценариев оболочки или командной строки, что позволяет предоставлять и запрашивать информацию у пользователя.

С ее помощью можно создавать диалоговые окна с различными элементами управления, включая кнопки, флажки, текстовые поля и т.д.

Yad может использоваться для создания пользовательских интерфейсов для скриптов командной строки и других приложений.

Установка yad

По умолчанию в РЕД ОС утилита **yad** уже установлена (расположена в каталоге **/usr/bin/yad**). Проверьте, установлена ли утилита **yad** в вашей системе и доступна ли она для использования, выполнив следующую команду:

```
which yad
```

Если по какой-либо причине утилита **yad** не установлена, для ее установки выполните следующую команду (потребуются права **администратора**):

```
sudo dnf install yad
```

Синтаксис и опции

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
yad [опции]
```

Основные опции:

- **-h**, **--help** — вывести справку по работе с утилитой;
- **--version** — вывести версию утилиты;
- **--about** — просмотреть информацию о программе;
- **--help-general** — показать общие параметры.

Опции утилиты, отвечающие за вид диалогового окна:

- **--app** — диалоговое окно выбора приложения;
- **--calendar** — диалоговое окно выбора даты;
- **--color** — диалоговое окно выбора цвета;
- **--dnd** — диалоговое окно для перетаскивания объектов;
- **--entry** — диалоговое окно с полем ввода текста;
- **--icons** — диалоговое окно со значками ярлыков;
- **--file** — диалоговое окно выбора файлов;

- **--font** — диалоговое окно выбора шрифта;
- **--form** — диалоговое окно формы;
- **--html** — диалоговое окно HTML;
- **--list** — диалоговое окно со списком;
- **--multi-progress** — диалоговое окно с несколькими индикаторами выполнения;
- **--notebook** — диалоговое окно блокнота;
- **--notification** —диалоговое окно уведомления;
- **--print** — диалоговое окно печати;
- **--progress** — диалоговое окно выполнения процесса;
- **--text-info** — диалоговое окно с текстовой информацией;
- **--scale** — диалоговое окно шкалы.

Опции общего назначения:

- **--title="ЗАГОЛОВОК"** —установить заголовок диалога;
- **--window-icon=<ICON>** — установить значок окна;
- **--width=<ШИРИНА>** — установить ширину;
- **--height=<ВЫСОТА>** — установить высоту;
- **--timeout=<ЗАДЕРЖКА>** — установить задержку диалога в секундах;
- **--ok-label="ТЕКСТ"**— установить метку для кнопки «**ОК**»;
- **--cancel-label="ТЕКСТ"** — установить метку для кнопки «**Отменить**»;
- **--extra-button="ТЕКСТ"** — добавить дополнительную кнопку;
- **--modal** — установить модальное свойство;
- **--posx=<ЧИСЛО>** — установить горизонтальное положение диалогового окна;
- **--posy=<ЧИСЛО>** — установить вертикальное положение диалогового окна;
- **--geometry=<ШИРИНА>x<ВЫСОТА>+<X>+<Y>** — установить размеры диалогового окна;
- **--timeout-indicator=<ПОЗИЦИЯ>** — показывать индикатор задержки в позиции (*top*, *bottom*, *left* или *right*);
- **--no-buttons** — не показывать кнопки;
- **--no-focus** — не фокусировать диалоговое окно;
- **--fullscreen** — запустить диалог в полноэкранном режиме;
- **--text="ТЕКСТ"** — текст сообщения;
- **--text-width=<ЧИСЛО>** — установить максимальную ширину текста диалога в символах;
- **--text-align=<ТИП>** — задать тип выравнивания текста диалога (*left*, *right*, *center* или *fill*);
- **--icon-theme=<ТЕМА>** — использовать указанную тему значков GTK вместо стандартной;
- **--sticky** — сделать окно видимым на всех рабочих столах;
- **--fixed** — сделать окно фиксированной ширины и высоты;
- **--center** — разместить окно в центре экрана;
- **--mouse** — разместить окно под позицию мыши;
- **--on-top** — разместить окно поверх других окон;
- **--undecorated** — удалить заголовок и рамки окна;
- **--enable-spell** — включить проверку орфографии.

Пользовательские параметры диалогового окна:

- **--pname="ТЕКСТ"** — установить имя программы;
- **--image=<ИЗОБРАЖЕНИЕ>** — установить имя значка программы;
- **--pversion="ТЕКСТ"** — установить строку версии программы;
- **--copyright="ТЕКСТ"** — установить строку авторского права программы;
- **--comments="ТЕКСТ"** — подробное описание программы;
- **--license="ТЕКСТ"** — установить лицензию программы, где значением может быть одна из предопределенных лицензий (GPL2, GPL3, LGPL2, LGPL3, BSD, MIT или ARTISTIC), имя файла с текстом лицензии или произвольная строка;
- **--authors="ТЕКСТ"** — установить список авторов программы через запятую;
- **--website=<URI>** — установить ссылку на сайт программы;
- **--website-label=<МЕТКА>** — установить метку для ссылки на сайт программы.

Опции выбора приложения:

- **--enable-fallback**— показать резервные приложения;
- **--enable-other** — показать другие приложения;
- **--enable-all**— показать все доступные приложения;
- **--extened** — показать расширенную информацию о выбранном приложении, где полями вывода являются имя, отображаемое имя, описание, значок и исполняемый файл.

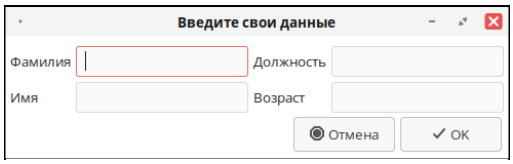
Примеры использования

В зависимости от ситуации, требующей незамедлительного вмешательства пользователя или запуска окна в определенное время, можно использовать соответствующие команды в скрипте или непосредственно из командной строки. В диалоговой форме можно получать данные от пользователя, а затем передавать их в скрипт.

Диалоговое окно формы ввода

Для вывода диалогового окна для получения данных от пользователя введите команду:

```
yad --form --title="Введите свои данные" --columns=2 --field="Фамилия" --field="Имя" --field="Должность" --field="Возраст"
```

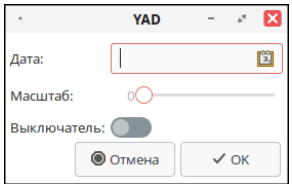


Параметры диалога формы ввода:

- **--form** — отобразить диалог формы с полями ввода;
- **--field=<МЕТКА>[:ТИП]** — добавить поле к форме (список типов указан на странице руководства **yad**);
- **--align=<ТИП>** — задать выравнивание меток полей (*left*, *center* или *right*);
- **--columns=<ЧИСЛО>** — задать количество колонок в форме;
- **--homogeneous** — сделать высоту и ширину полей формы одинакового размера;
- **--output-by-row** — упорядочить вывод по строкам;
- **--focus-field=<ЧИСЛО>** — задать поле, получающее фокус;
- **--changed-action=<КОМАНДА>** — задать действие при изменении поля.

Для создания формы с указанными полями, введите следующую команду в терминале:

```
yad --form --field="Дата::DT" --field="Масштаб::SCL" --field="Выключатель::SW"
```



Типы полей формы:

--field=МЕТКА[:ТИП] — тип может быть *H*, *RO*, *NUM*, *CHK*, *CB*, *CBE*, *CE*, *FL*, *SFL*, *DIR*, *CDIR*, *FN*, *MFL*, *MDIR*, *DT*, *SCL*, *SW*, *APP*, *ICON*, *CLR*, *BTN*, *FBTN*, *LINK*, *LBL* или *TXT*.

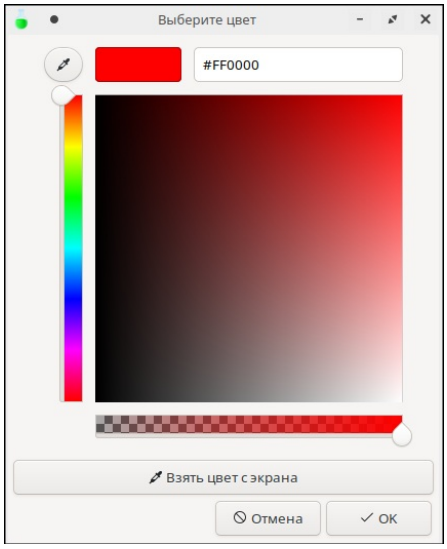
- **H** — тип скрытого поля, все символы отображаются как невидимые символы;
- **RO** — поле только для чтения;
- **NUM** — числовое поле ЗНАЧЕНИЕ[!ДИАПАЗОН[!ШАГ![PREC]]] задает формат начального значения, диапазона, шага, **PREC** — это точность десятичных дробей;
- **CHK** — поле-флажок, где начальное значение представляет собой логическую константу, нечувствительную к регистру (*ИСТИНА* или *ЛОЖЬ*);
- **CB** — поле со списком, где начальное значение представляет собой список ЗНАЧ1!ЗНАЧ2!...;
- **CBE** — редактируемое поле со списком;
- **CE** — запись с завершением;
- **FL** — кнопка выбора файла;
- **SFL** — поле для создания файла;
- **DIR** — кнопка выбора директории;
- **CDIR** — поле для создания папки;
- **FN** — кнопка выбора шрифта;
- **MFL** — выбрать несколько файлов;
- **MDIR** — выбор нескольких папок;
- **DT** — поле выбора даты;
- **SCL** — поле масштаба, принимающее значения в диапазоне **0..100**;
- **S W** — поле выключателя, где начальное значение представляет собой логическую константу, нечувствительную к регистру (*ИСТИНА* или *ЛОЖЬ*);
- **APP** — кнопка выбора приложения, где входное значение для этого поля имеет тип **mime**, выходное значение — исполняемый файл для выбранного приложения;
- **ICON** — поле значка имеет две иконки: слева отображается текущий значок, а справа можно щелкнуть и вызвать yad-con-браузер для выбора значка;
- **CLR** — кнопка выбора цвета;
- **BTN** — поле кнопки (метка может быть в виде текста в формате LABEL[!ICON[!TOOLTIP]], где «**!**» является разделителем элементов, **LABEL** — это текст надписи на кнопке или идентификатор, **ICON** — значок кнопки (идентификатор или имя файла), **TOOLTIP** — это необязательный текст для всплывающей строки справки);
- **FBTN** — поле кнопки с полным рельефом;
- **LINK** — поле кнопки ссылки;
- **LBL** — текстовая метка (если имя поля пустое, будет показана горизонтальная разделительная линия);
- **TXT** — многострочный ввод текста, занимающий всю ширину формы.

При использовании наименования поля без типа будет выведена простая текстовая запись.

Диалоговое окно выбора цвета

Для вывода диалогового окна выбора цвета введите в терминал следующую команду:

```
yad --title="Выберите цвет" --color --init-color=RED --picker
```



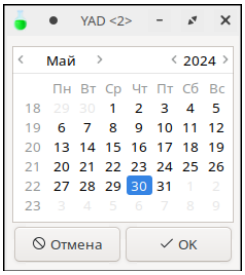
Параметры диалога выбора цвета:

- **--color** — отобразить диалог для выбора цвета;
- **--init-color=<ЦВЕТ>** — задать начальное значение цвета;
- **--gtk-palette** — показать системную палитру;
- **--palette="ИМЯ_ФАЙЛА"** — указать путь к файлу палитры;
- **--expand-palette** — раскрыть пользовательскую палитру;
- **--picker** — показать кнопку выбора цвета;
- **--mode=<РЕЖИМ>** — установить режим вывода на экран, где значения — *hex* (по умолчанию) или *rgb*;
- **--alpha** — добавить прозрачность к значению цвета.

Диалоговое окно с календарем

Для вывода диалогового окна с календарем введите следующую команду:

```
yad --calendar --day=30 --show-weeks
```



Параметры, используемые для вывода диалогового окна, в котором будет отображен календарь:

- **--calendar** — показать диалог выбора даты;
- **--day=<ДЕНЬ>** — установить день в календаре (число от 1 до 31);
- **--month=<МЕСЯЦ>** — установить месяц в календаре (число от 1 до 12);
- **--year =<ГОД>** — установить год в календаре;
- **--details="ИМЯ_ФАЙЛА"** — задать имя файла с описанием дат;
- **--show-weeks** — показать нумерацию недель слева.

Ссылка в диалоговом окне

1. Выберите директорию и создайте файл, например:

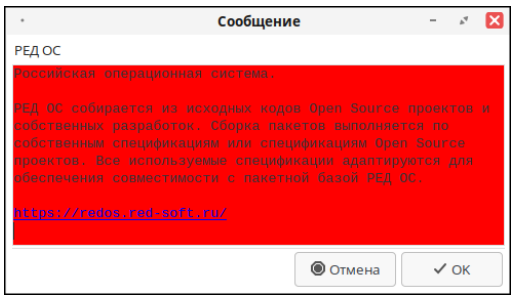
```
nano /home/user/text.txt
```

2. Запишите в него требуемую информацию:

«Российская операционная система.
РЕД ОС собирается из исходных кодов Open Source проектов и собственных разработок. Сборка пакетов выполняется по собственным спецификациям или спецификациям Open Source проектов. Все используемые спецификации адаптируются для обеспечения совместимости с пакетной базой РЕД ОС.
https://redos.red-soft.ru/.

3. Сохраните файл и выполните следующую команду в терминале:

```
yad --text-info --back=red </home/user/text.txt --show-uri --text="РЕД ОС" --title="Сообщение" --wrap --editable --tail --show-cursor
```



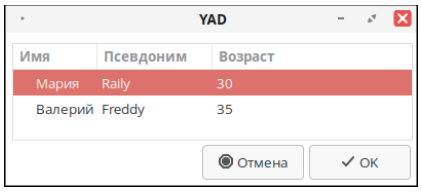
Параметры:

- **--text-info** — создает окно для отображения текстовой информации;
- **--back=ЦВЕТ** — использует указанный цвет для фона;
- **--wrap** — включить перенос текста;
- **--editable** — разрешить изменения в тексте;
- **--tail** — автопрокрутка до конца текста;
- **--show-cursor** — показывать курсор в режиме только для чтения;
- **--text="ТЕКСТ"** — текст сообщения;
- **--show-uri** — сделать URI кликабельным.

Список в диалоговом окне

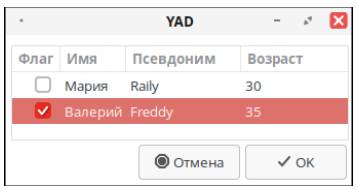
Диалоговое окно для списка можно получить, введя команду:

```
yad --list --column="Имя" --column="Псевдоним" --column=Возраст Мария Raily 30 Валерий Freddy 35 --height=150 --width=400
```

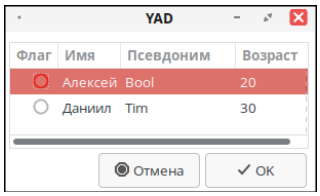


Для добавления в список элементов **--checklist** или **--radiolist** можно воспользоваться следующими примерами:

```
yad --list --checklist --width=300 --height=130 --column="Флаг" --column="Имя" --column= "Псевдоним" --column="Возраст" false Мария Raily 30 false  Валерий Freddy 35
```

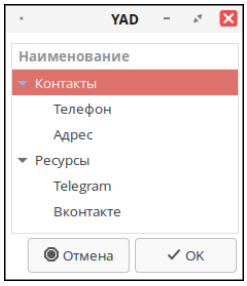



```
yad --list --radiolist --width=302 --height=123 --column="Флаг" --column="Имя" --column="Псевдоним"  --column="Возраст"   false Алексей Bool 20 false Даниил Tim 30
```



Отобразить список в режиме дерева можно следующим образом:

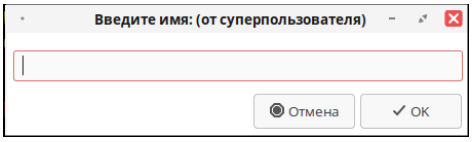
```
yad --list --tree --column "Наименование" f  "Контакты" 1:f  "Телефон" 2:f "Адрес" v  "Ресурсы" 3:v "Telegram"  4:v "Вконтакте"
```



Диалоговое окно для ввода текста

Диалоговое окно для ввода текста с заголовком «***Введите имя:***» шириной 450 и высотой 100 можно получить, выполнив команду:

```
yad --entry --title="Введите имя:" --height=100 --width=450
```



Добавление yad в bash-сценарии

Пример 1. Диалоговое окно записной книжки

Блокнот представляет собой сложный диалог, который поглощает другие диалоги на своих вкладках. Диалоги идентифицируются уникальным ключом (целым числом) и должны запускаться в специальном режиме плагина (опция *--plug*). В следующем примере запускается диалоговое окно записной книжки с двумя вкладками: первая содержит простой текст, а вторая — диалоговое окно ввода.

1. Выберите нужную директорию и создайте файл в формате **sh**:

```
nano /home/user/Документы/script.sh
```

2. Впишите в файл следующие строки и сохраните:

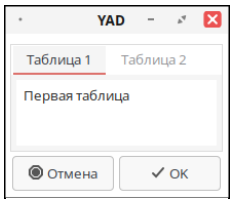
```
#! /bin/sh
 yad --plug=123 --tabnum=1 --text="Первая таблица" &> res1 &
 yad --plug=123 --tabnum=2 --text="Вторая таблица" --entry &> res2 &
 yad --notebook --key=123 --tab="Таблица 1" --tab="Таблица 2"
```

3. Для выполнения *bash-скрипта* назначьте пользователю права на выполнение с помощью следующей команды:

```
chmod u+x script.sh
```

4. Запустите скрипт с помощью команды:

```
sh script.sh
```



Пример 2. Диалоговое окно с сообщением

Для создания диалогового окна с сообщением при первом входе пользователя в систему выполните следующий алгоритм действий.

В РЕД ОС 7.3:

1. Откройте файл **/etc/gdm/PreSession/Default**, введя команду в терминале (потребуются права **администратора**):

```
nano /etc/gdm/PreSession/Default
```

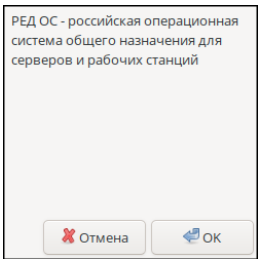
2. Впишите в файл следующие строки и сохраните:

```
export LANG=ru_RU.UTF-8 /usr/bin/yad --center --geometry=250x250 --text="РЕД ОС — российская операционная система общего назначения для серверов и рабочих станций"
```

где**:**

- **export LANG=ru_RU.UTF-8** — параметр, необходимый для работы с русским языком (является обязательным, иначе авторизация не будет проходить успешно);
- **--geometry= 250x250** — задать размеры окна;
- **--center** — выровнять диалоговое окно по центру;
- **--text="ТЕКСТ"** — текст сообщения.

3. Перезагрузите ПК. После авторизации пользователя появится окно с уведомлением.



В РЕД ОС 8.0:

1. Создайте скрипт **/home/user1/yadwel.sh** (замените user1 на актуальное имя пользователя):

```
nano /home/user1/yadwel.sh
```

2. Добавьте в него следующие строки:

```
#!/bin/bash
 export LANG=ru_RU.UTF-8
 /usr/bin/yad --center --geometry=250x250 --text="РЕД ОС — российская операционная система общего назначения для серверов и рабочих станций"
```

3. Выдайте права на исполнение файла:

```
chmod +x /home/user1/yadwel.sh
```

4. Создайте файл в каталоге **/etc/xdg/autostart/** для автозапуска уведомления во время авторизации пользователя:

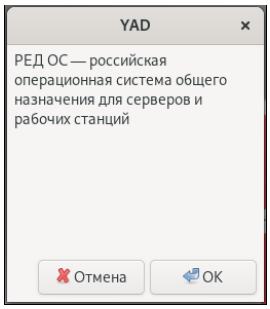
```
nano /etc/xdg/autostart/WelcomeYad.desktop
```

5. Добавьте в него следующие строки:

```
[Desktop Entry]
```

```
Type=Application
Name=Welcome Message
Comment=Shows a welcome message
Exec=/home/user1/yadwel.sh
Terminal=false
X-MATE-Autostart-enabled=true ##если используется графическая оболочка MATE
X-GNOME-Autostart-enabled=true #если используется графическая оболочка GNOME
X-KDE-Autostart-enabled=true #если используется графическая оболочка KDE
```

6. Перезагрузите ПК. После авторизации пользователя появится окно с уведомлением.



В наших статьях можно подробнее ознакомиться с использованием утилит создания интерактивных меню в РЕД ОС:

- Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- Dialog — утилита для создания диалоговых окон в консольных приложениях .

Dialog – утилита для создания диалоговых окон в консольных приложениях

Установка
Синтаксис и опции
Примеры использования
Диалоговое окно сообщения с кнопкой «OK»
Сообщение с кнопками «Да» и «Нет»
Диалоговое окно с календарем
Диалоговое окно с контрольным списком
Диалоговое окно формы
Добавление dialog в bash-сценарии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dialog 1.3-20210621

Dialog — это утилита для построения консольных интерфейсов. Диалоговые окна можно легко включить в сценарии оболочки для взаимодействия с пользователями. **Dialog** позволяет создавать интерфейсы на любом консольном языке.

Установка

Пакет диалогов по умолчанию не установлен в РЕД ОС. Установить **dialog** можно, выполнив следующую команду в терминале (потребуются права **администратора**):

```
sudo dnf install dialog
```

Команда устанавливает пакет диалогов и необходимые библиотеки для системы.

Синтаксис и опции

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
dialog [опции]
```

Основные опции:

- **-h, --help** — вывести справку по работе с утилитой;
- **--version** — вывести версию утилиты;
- **--about** — просмотреть информацию о программе;
- **--help-general** — показать общие параметры.

Опции общего назначения:

- **--title="Заголовок"** — задает заголовок диалога;
- **--backtitle="Заголовок"** — задает строку заголовка, которая будет отображаться на фоне в верхней части экрана;
- **--ascii-lines** — рисует знаки «**---**», «**|**», «**++++**» вместо обычных линий рамок;
- **--scrollbar** — добавляет полосы прокрутки;
- **--defaultno** — добавляет кнопку «**Нет**» по умолчанию;
- **--clear** — очищает экран перед отображением диалога.

Опции утилиты, отвечающие за вид диалогового окна:

- **--buildlist** — диалоговое окно списка сборки, отображающее списки с невыбранными и выбранными элементами. Синтаксис диалогового окна имеет вид: `--buildlist <text> <height> <width> <list-height> <tag1> <item1> <status1>...`;
- **--calendar** — диалоговое окно календаря, отображающее день, месяц или год. Синтаксис диалогового окна имеет вид: `--calendar <text> <height> <width> <day> <month> <year>`;
- **--checklist** — диалоговое окно контрольного списка. Синтаксис диалогового окна имеет вид: `--checklist <text> <height> <width> <list height> <tag1> <item1> <status1>...`;
- **--dselect** — диалоговое окно выбора каталога. Синтаксис диалогового окна имеет вид: `--dselect <directory> <height> <width>`;
- **--editbox** — диалоговое окно редактирования. Синтаксис диалогового окна имеет вид: `--editbox <file> <height> <width>`;
- **--form** — диалоговое окно формы. Синтаксис диалогового окна имеет вид: `--form <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1>...`;
- **--fselect** — диалоговое окно выбора файла. Синтаксис диалогового окна имеет вид: `--fselect <filepath> <height> <width>`;
- **--gauge** — диалоговое окно индикатора. Синтаксис диалогового окна имеет вид: `--gauge <text> <height> <width> [<percent>]`;
- **--infobox** — информационное окно. Синтаксис диалогового окна имеет вид: `--infobox <text> <height> <width>`;
- **--inputbox** — диалоговое поле ввода данных от пользователя. Синтаксис диалогового окна имеет вид: `--inputbox <text> <height> <width> [<init>]`;
- **--inputmenu** — диалоговое окно меню ввода. Синтаксис диалогового окна имеет вид: `--inputmenu <text> <height> <width> <menu height> <tag1> <item1>...`;
- **--menu** — диалоговое окно меню. Синтаксис диалогового окна имеет вид: `--menu <text> <height> <width> <menu height> <tag1> <item1>...`;
- **--mixedform** — диалоговое окно смешанной формы, состоящее из меток и полей. Синтаксис диалогового окна имеет вид: `--mixedform <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1> <itype>...`;
- **--mixedgauge** — диалоговое окно смешанного счетчика. Синтаксис диалогового окна имеет вид: `--mixedgauge <text> <height> <width> <percent> <tag1> <item1>...`;
- **--msgbox** — диалоговое окно сообщения. Синтаксис диалогового окна имеет вид: `--msgbox <text> <height> <width>`;
- **--passwordbox** — диалоговое поле пароля. Синтаксис диалогового окна имеет вид: `--passwordbox <text> <height> <width> [<init>]`;
- **--passwordform** — диалоговое окно формы с вводом пароля. Синтаксис диалогового окна имеет вид: `--passwordform <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1>...`;
- **--pause** — диалоговое окно паузы. Синтаксис диалогового окна имеет вид: `--pause <text> <height> <width> <seconds>`;
- **--prgbox** — диалоговое окно для отображения вывода команды. Синтаксис диалогового окна имеет вид: `--prgbox <text> <command> <height> <width>`;
- **--programbox** — диалоговое окно программного блока. Синтаксис диалогового окна имеет вид: `--programbox <text> <height> <width>`;
- **--progressbox** — диалоговое окно прогресса. Синтаксис диалогового окна имеет вид: `--progressbox <text> <height> <width>`;
- **--radiolist** — диалоговое окно радиосписка. Синтаксис диалогового окна имеет вид: `--radiolist <text> <height> <width> <list height> <tag1> <item1> <status1>...`;
- **--rangebox** — диалоговое окно с выбором диапазона значений. Синтаксис диалогового окна имеет вид: `--rangebox <text> <height> <width> <min-value> <max-value> <default-value>`;
- **--tailbox** — диалоговое окно отображения текста из файла. Синтаксис диалогового окна имеет вид: `--tailbox <file> <height> <width>`;
- **--tailboxbg** — диалоговое окно отображения текста из файла в качестве фоновой задачи. Синтаксис диалогового окна имеет вид: `--tailboxbg <file> <height> <width>`;
- **--textbox** — диалоговое окно с текстовым полем. Синтаксис диалогового окна имеет вид: `--textbox <file> <height> <width>`;
- **--timebox** — диалоговое окно, позволяющее выбрать время. Синтаксис диалогового окна имеет вид: `--timebox <text> <height> <width> <hour> <minute> <second>`;
- **--treeview** — диалоговое окно отображения данных в виде дерева. Синтаксис диалогового окна имеет вид: `--treeview <text> <height> <width> <list-height> <tag1> <item1> <status1> <depth1>...`;
- **--yesno** — диалоговое окно «Да»/«Нет». Синтаксис диалогового окна имеет вид: `--yesno <text> <height> <width>`.

Параметры диалоговых окон:

- **--text** — задает заголовок или содержимое поля;

- **--height** — задает высоту диалогового окна;
- **--width** — задает ширину диалогового окна;
- **--list-height** — высота списка.

Примеры использования

Диалоговое окно сообщения с кнопкой «OK»

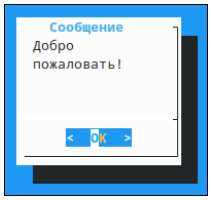
Окно сообщения отображает сообщение и требует от пользователя нажать кнопку «**OK**».

Формат сообщения следующий: `--msgbox <text> <height> <width>`

Для вывода на экран сообщения "**Hello world!**", необходимо воспользоваться следующей командой в консоли:

```
dialog --title "Сообщение" --msgbox "Добро пожаловать!" 8 20
```

Результат выполнения этой команды выглядит следующим образом:



Сообщение с кнопками «Да» и «Нет»

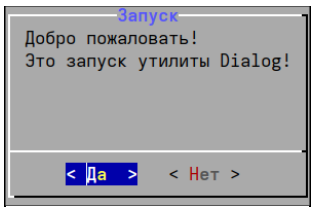
Параметр **--yesno** — предоставляет простое сообщение с кнопками « **Да**» и «**Нет**».

Формат сообщения следующий: `--yesno <text> <height> <width>`

Например, для вывода сообщения введите в терминал команду:

```
dialog --title "Запуск" --yesno "Добро пожаловать! \nЭто запуск утилиты Dialog!" 9 30
```

После запуска будет выведено следующее диалоговое окно:



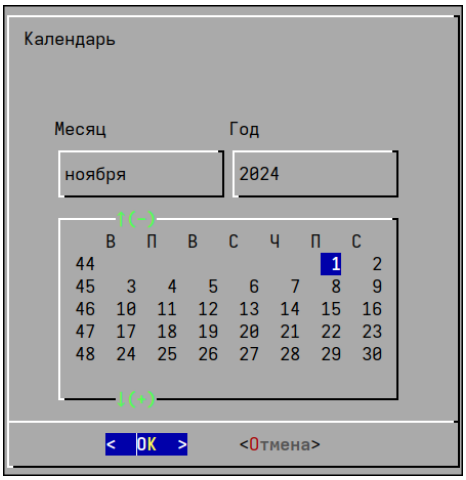
Программа будет ждать пользовательского выбора. Нажмите кнопку «**Да**», «**Нет**» или клавишу «**Esc**».

Диалоговое окно с календарем

Календарь — предоставляет календарь для отображения выбранной даты.

Формат календаря: `--calendar <text> <height> <width> <day> <month> <year>`

```
dialog --calendar "Календарь" 5 45 01 11 2024
```

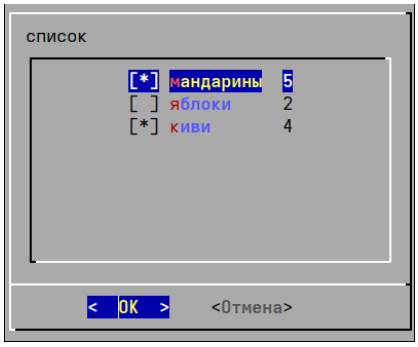


Диалоговое окно с контрольным списком

Контрольный список — отображает несколько записей, каждую из которых можно включить или отключить.

Формат списка: `--checklist <text> <height> <width> <list height> <tag1> <item1> <status1>...`

```
dialog --checklist "список" 15 40 12 "мандарины" 5 "on" "яблоки" 2 "off" "киви" 4 "on"
```

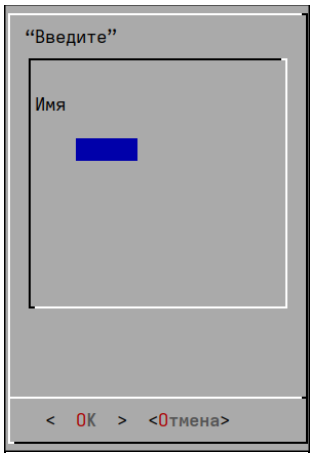


Диалоговое окно формы

Форма позволяет создать форму с метками и текстовыми полями для заполнения.

Формат формы следующий: `--form <text> <height> <width> <form height> <label1> <l_y1> <l_x1> <item1> <i_y1> <i_x1> <flen1> <ilen1>...`

```
dialog --form "Введите" 20 30 20 "Имя" 2 1 "" 4 5 6 7
```



Добавление dialog в bash-сценарии

Для создания bash-скрипта выполните следующий алгоритм действий:

1. Для создания пустого файла скрипта введите команду:

```
touch newscript.sh
```

2. Для открытия файла используйте любой текстовый редактор, например:

```
nano newscript.sh
```

3. Впишите в файл следующие строки и сохраните файл:

```
#! /bin/sh

DIALOG=${DIALOG=dialog}
$DIALOG --backtitle "Окно для выбора устройств" \
--title "Выбор устройств" --clear \
--radiolist "Список устройств" 20 61 5 \
"Aqara LED Light Bulb" "Умная лампа" ON \
"Yeelight Lightstrip Pro" "Умная светодиодная лента" off \
"Yeelight Ceiling Light" "Умный потолочный светильник" off \
"Aqara Gas Sensor" "Датчик газа" off \
"Aqara TVOC Air Quality Monitor" "Монитор качества воздуха" off
```

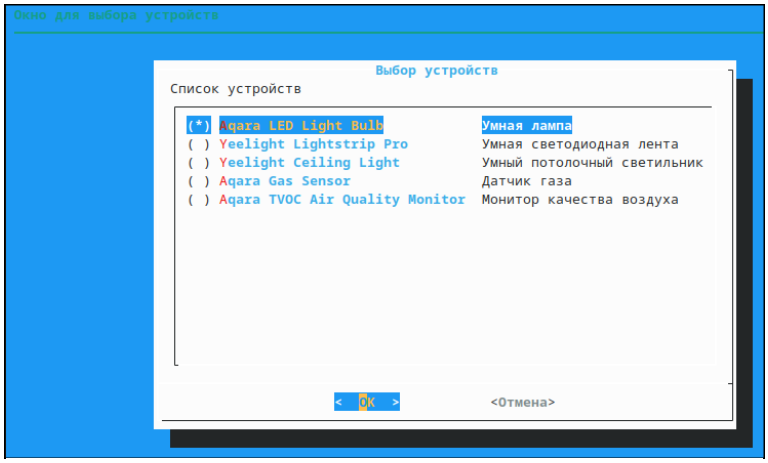
4. Для предоставления прав на выполнение файла выполните команду:

```
chmod +x newscript.sh
```

5. Для запуска скрипта выполните команду:

```
./newscript.sh
```

Результат выполнения скрипта:



В наших статьях можно подробнее ознакомиться с использованием утилит создания интерактивных меню в РЕД ОС:

- Zenity — утилита для создания диалоговых окон из командной строки или с помощью сценариев ;
- Yad — утилита для создания диалоговых окон с использованием терминала или сценариев .

Полноэкранный редактор VI и улучшенный редактор VIM

Режимы работы редактора
Ввод текста
Команды
Перемещение курсора
Редактирование
Командная строка
Блоки, буферы, окна редактирования. Повторители
Открыть/создать файл
Дополнительные опции
Улучшенный редактор VIM

Редактор **vi** - универсальный полноэкранный текстовый редактор в среде UNIX. Универсальность означает, что, во-первых, этот редактор есть во всех UNIX-подобных ОС и, во-вторых, этот редактор работает с практически любым видом терминала (**ANSI**, **VT100**, **VT220**, **VT320**, **DEC** и т. д.). Эта универсальность выражается непривычным (для пользователей **DOS**) пользовательским интерфейсом: для управления редактором используются лишь «обычные» кнопки клавиатуры (алфавитно-цифровые символы и знаки препинания).

Имеющиеся на многих типах терминалов функциональные клавиши практически не используются. Если клавиатура терминала имеет стрелочные клавиши, то они используются, но в ограниченном контексте.

Вы можете подробнее ознакомиться с информацией по работе с редактором **vim**, просмотрев наши обучающие видео:

- на **RuTube** — Текстовый редактор vim;
- в **Яндекс.Дзен** — Текстовый редактор vim;
- в **VK Видео** — Текстовый редактор vim.

На наших каналах вы также сможете найти много другой полезной информации.

Режимы работы редактора

Ввод текста

В этом режиме все, что набирается на клавиатуре, отображается на экране терминала и запоминается в буфере редактора.

В данном режиме нет возможности осуществлять операции редактирования текста, за исключением стирания последнего набранного символа (с помощью комбинации клавиш «Ctrl+H»).

Командный режим

В этом режиме символы клавиатуры выполняют специальные функции (перемещение курсора, стирание частей текста, и т. д.), то есть функции редактирования.

В данном режиме набираемые команды **не отображаются на экране**.

Режим командной строки

Режим командной строки позволяет производить более глобальные операции с текстом: записывать отредактированный текст в файл, считывать новый файл, выходить из vi, производить настройку редактора, поиск по шаблону, а также осуществлять некоторые функции редактирования.
Команды отображаются в нижней части экрана (в командной строке редактора).

Ввод текста

«Return» - создает пустую строку и переводит курсор в ее начало;

«Ctrl+H» - уничтожает последний введенный символ (это действие не отображается на экране до выхода в командный режим);

«Ctrl+[» или клавиша «Esc» - переводят редактор в командный режим.

В режиме ввода текста стрелочная клавиатура **не работает**.

Команды

i - переход в режим набора методом вставки перед текущим символом;
a - переход в режим набора методом вставки за текущим символом;
R - переход в режим набора текста методом набивки.

Перемещение курсора

h, j, k, l - на один символ (одну строку), как показано стрелками;
^ или **0** - в начало текущей строки;
$ - в конец текущей строки;
w - на слово вправо;
b - на слово влево;
} - на параграф вперед (параграф - это блок текста, отделенный пустой строкой);
{ - на параграф назад;
[[- в начало текста;
]] - в конец текста.
Кнопки стрелочной клавиатуры также позволяют перемещаться по тексту.

Редактирование

Предположим, в нашем файле записан текст, который необходимо отредактировать. Для этого необходимо перейти в режим ввода. Самый простой способ - из командного режима нажатие клавиши "**i**". После чего можно приступать к вводу текста. <ESC> вернет нас к командному режиму.

Другие важные команды:

Команда	Описание команды
R,i	переход в режим ввода - замена текста под курсором
I	переход в режим ввода с начала текущей строки
o	переход в режим ввода с новой строки под курсором
O	переход в режим ввода с новой строки над курсором
a	переход в режим ввода после курсора
x	стирание символа под курсором
X	стирание символа перед курсором
dd	стирание текущей строки
d<число>d	стирание числа строк, начиная с текущей
yy	копирование текущей строки в неименованный буфер
y<число>y	копирование числа строк начиная с текущей в неименованный буфер
p	вставка строки из неименованного буфера под курсор
P	вставка строки из неименованного буфера над курсором
J	слияние текущей строки со следующей
u	отмена последней команды
.	повтор последней команды
:	переход в режим командной строки

Командная строка

:q или **:q!** - выход из редактора без сохранения изменений;

:x - выход из редактора с записью, если файл был модифицирован;

:w или **w <имя_файла>** или **w! <имя_файла>** - запись файла и возвращение в командный режим;

:e <имя_файла> или **:e! <имя_файла>** - загрузка указанного файла;

:r <имя_файла> - добавить содержимое указанного файла к редактируемому сразу за текущей строкой;

:set nu - включить нумерацию строк;

:set nonu - отключить нумерацию строк;

:!command - выполнить команду UNIX, не покидая редактора;

:/word - выполнить поиск слова word в тексте;

:/ - повторить поиск слова word далее по тексту.

Блоки, буферы, окна редактирования. Повторители

Повторители

Командам и движениям курсора можно давать повторители (числа), например:
2w - передвинуть курсор на два слова вперед;
10l - передвинуть курсор на десять символов вправо;
d10l - стереть десять символов справа от курсора;
2d10l - стереть двадцать символов справа от курсора;
5J - слить пять последующих строк в одну;
4. - повторить последнюю введенную команду четыре раза.

Буферы vi

Редактор имеет три типа буферов: буфер стирания (**0-9**), неименованный буфер и именованные буферы (**a-z**).

В буферы стирания автоматически заносятся стираемые элементы. В **буфере 0** хранится последний стертый элемент, в **буфере 1** - предпоследний и т. д.

Занести в буфер:

yy - занести текущую строку в неименованный буфер;

y<движение_курсора> - занести указанный движением курсора блок текста в неименованный буфер;

"ayy - занести текущую строку в именованный буфер «a»;

"Ayy - добавить текущую строку к содержимому именованного буфера «a»;

"by10j - занести последующие 10 строк в именованный буфер «b».

Вставить из буфера:

p - вставить в текущую позицию содержимое неименованного буфера;

"ap - вставить в текущую позицию содержимое именованного буфера «a»;

"1p - вставить в текущую позицию содержимое буфера стирания «1».

Многооконное редактирование

Редактировать сразу несколько файлов можно либо пользуясь командной редактора :e <имя_файла>, либо указав все необходимые файлы в командной строке при вызове редактора (например: `vi <файл_1> <файл_2> <файл_3>`). В последнем случае вы двигаетесь по списку файлов с помощью команд:
:n - переходим к следующему файлу в списке;
:rew - возвращаемся к редактированию первого файла в списке.
Именованные буферы сохраняют свое содержимое при переходе к редактированию другого файла.

Открыть/создать файл

`vi test1.txt` - открыть один файл.

`vi test1.txt test2.txt` - открыть файл test1.txt, после выхода из него открыть файл test2.txt.

Файл открывается в командном режиме с помощью команды vi. Здесь мы можем просмотреть файл, переместиться по его содержимому, стереть текст, но внести изменения или ввести текст в этом режиме нельзя.

Создание файла происходит при помощи той же команды. Создание файла происходит в момент сохранения.

Для открытия или создания нового файла в командном режиме необходимо выполнить команду:

```
:e <имя_файла>
```

Перед этим нужно сохранить предыдущий файл:

:w - сохраняет файл с существующим именем;
:sav <имя_файла> - «Сохранить как».

Дополнительные опции

Дополнительные возможности редактора:

Команда	Описание команды
G	перейти в конец файла
<number>G	перейти на конкретную строку <number>
:<number>	перейти на <number> строк вперед
:set nu[mber]	отобразить слева нумерацию строк (^ nonu[mber] - спрятать нумерацию)
:set wrap	переносить длинные строки (:set nowrap - не переносить)
:syntax on/off	включить/выключить подсветку синтаксиса
:colorscheme <name>	задать цветовую тему (где <name> - имя темы, TAB работает как авто-дополнение)
/мама	поиск текста "мама" в файле
n	повторить поиск
:h или :help	список возможной помощи (:viusage, :exusage)
:set fileformat=dos :set fileformat=unix	привести концы строк в файле к виду dos или unix, соответственно
:set ts=4	задать размер табуляции в 4 пробела

Улучшенный редактор VIM

Vim расшифровывается как **Vi Improved**, улучшенный vi. В сравнении с классическим vi **Vim** отличается следующими улучшениями:

- Работа со многими файлами одновременно. Разбиение окон редактирования может производиться многократно как по горизонтали, так и по вертикали.
- Поддержка Unicode.
- Поддержка визуального режима, который позволяет, например, выполнять операции над блоками текста.
- Неограниченная глубина отмены (undo) и возврата (redo) действий.
- Режим сравнения двух файлов, перенос отдельных изменений из одного файла в другой.
- Широкая файловая поддержка (файл со справкой и более 200 файлов с описанием синтаксиса).
- Подсветка синтаксиса, автоматическое определение величины отступа для каждой строки в зависимости от языка программирования (изначально поддерживает более 200 языков программирования и форматов конфигурационных файлов).
- Интеграция с операционной системой, дающая возможности, близкие к интегрированным средам разработки, такие как поиск ошибки по сообщению компилятора, автодополнение идентификаторов и др.
- Поддержка языка сценариев; возможность написания модулей расширения — плагинов.
- Автоматическое продолжение команд, слов, строк целиком и имён файлов.
- Автоматический вызов внешних команд (например, автоматическая распаковка файла перед редактированием).
- Распознавание и преобразование файлов различных форматов.
- Удобный механизм истории команд, поисковых слов и т. д.
- Запись и исполнение макросов.
- Возможность сохранения настроек и сеанса.
- Возможна интеграция с языками программирования Perl, Tcl, Python и Ruby.
- Поддержка языков с письмом справа налево (арабских и других).
- Сворачивание (folding) текста для лучшего обзора.
- Возможно использование графического интерфейса в специальных версиях (GTK, Motif, ...).
- Хорошо конфигурируется и настраивается под нужды пользователя.
- Для программистов: поддержка цикла разработки «редактирование — компиляция — исправление» программ. Автоматическое выполнение сборки/компиляции, обнаружение и распознавание ошибок, переход к строкам ошибок в тексте программы.

Режимы работы

В **ViM** существуют *3 режима* работы:

Основной - предназначен для просмотра файла, ввода команд и перехода из него в другие режимы. Из любого режима в командный можно попасть по нажатии «**ESC**». При нажатии клавиши «**:**» становится доступна командная строка ViM, в которой можно вводить команды. Основные команды - команда выхода **quit** (ViM понимает сокращения, поэтому можно давать команду одной буквой «**q**»), команда сохранения **write** (или «**w**»), параметром которой может быть имя файла и вызов справки по, очевидно, **help** (или «**h**»). На остальные клавиши (и их последовательности) можно присвоить любое действие, либо использовать значения по умолчанию.

Визуальный – предназначен, в первую очередь, для выделения блоков текста. Для запоминания предлагаются 3 варианта перехода в этот режим – клавишей «**v**» для посимвольного выбора, «**Shift+v**» для построчного и «**Ctrl+v**» для блочного. В нормальном режиме (при переходе по «**v**») можно оперировать следующими сущностями: слово («**w**»), предложение («**s**»), параграф («**p**») и блок («**b**»). Выделение при этом начинать с позиции курсора («**a**»), или же с начала блока («**i**»). Например, выделение текущего блока (участка,

ограниченного парными элементами) можно произвести следующим образом «**Esc+vib**». Копирование в буфер выделенного текста осуществляется по «**y**», вырезание по «**d**», а вставка соответственно «**p**».

Режим редактирования - переход в режим редактирования осуществляется нажатием клавиши «**Ins**».

Основные возможности

Все возможности и команды редактора **ViM** перечислить весьма затруднительно (HTML-документация по нему занимает около пяти мегабайт), но на группе наиболее полезных остановиться необходимо. Перечисленные ниже команды вводятся в основном режиме (если нет специального уточнения). Все они имеют командностроочные аналоги и могут быть легко переопределены пользователями.

Переходы

Для перехода на строку с номером *n* воспользуйтесь командой *G*. Так, для перехода к началу текста наберите **0G**, для сотой строки **100G**, а для конца документа - **$G**. Для перехода на **n** символов в нужную вам сторону можете использовать клавиши со стрелками. То есть для перехода на 1000 символов вниз наберите 1000 и нажмите стрелку вниз.

Для перемещения по тексту используйте следующие команды: «**(**», «**)**» для перемещения по предложениям, «**{**», «**}**» для параграфов, «**[[**», «**]]**» для функций, «**%**» - переход к парной скобке, «**' '**» - к предыдущему положению, а «CTRL+O», «CTRL+I» - соответственно назад и вперед по истории переходов.

Метки

Используются для отметки позиции ^<метка>, где <меткой> является любая буква для быстрого к ней перехода. Метки нижнего регистра действительны в пределах данного файла, метки верхнего регистра действуют во всех открытых файлах. Список всех меток можно получить командой **marks**. Для того чтобы установить метку на текущей строке используйте клавиши **M X**. Для того чтобы перейти на метку **X** введите команду: **' X**.

Регистры

В редакторе доступно множество именованных регистров (хранилищ данных, буферов). Регистр отмечается «**' 'буква**». К нему применимы все стандартные действия - копирование в него (**"меткау**), вырезание (**"метка^**), и вставка из него (**''меткар**), можете вместо **p** использовать **[p,]p** для вставки соответственно перед, или после курсора). В режиме редактирования вставка из регистра осуществляется по «Ctrl+R метка». Для добавления данных в регистр используйте заглавную метку.

Также вы можете писать в регистр, воспользовавшись командой «**^метка**» и завершая запись по «**q**». Таким образом, вы сохраняете макрос, выполнить который можно по «**@метка**».

Регистры с метками «*****» и «**+**» совпадают с X-Window clipboards, «**%**» - соответствует редактируемому файлу. Для просмотра содержимого всех регистров воспользуйтесь командой **:registers**, либо **:reg <метка_1><метка_2>...** для просмотра некоторых.

Фолды

Предназначены для сокрытия не нужных в данный момент данных, чтобы те не отвлекали внимания. Например, кода подпрограммы, с которой вы в данный момент не работаете. По умолчанию фолды активированы в режиме их ручной расстановки. Если вы хотите их автоактивации по отношению к табуляции, то добавьте в конфигурационный файл строку:

```
set foldmethod=indent
```

Все команды для работы с фолдами начинаются с **z**. Открытие фолда производится, например, по **zo** (или стрелке вправо) на нем, закрытие кода в фолд - по **zc**.

Сессии

При ведении группы проектов нередко желательно сохранить текущее состояние и настройки редактора, чтобы в дальнейшем продолжить работу с того же места. Для этого и предназначены сессии, что создаются командой **:mksession /path/to/Session.vim**, а читаются простой командой **:so /path/to/Session.vim**. Гораздо чаще, впрочем, возникает нужда в сохранении не всей сессии, но только текущего контекста (во что входит, например, положение курсора в коде, текущая расстановка фолдов и многое другое, о чем читайте в документации). Это действие выполняет команда **:mkview**, чтение - **:loadview**. Очень удобно сделать сохранение и чтение контекста автоматическим при начале и окончании редактирования файла. В **ViM** команда **au** используется для создания автоматических команд. Это может быть реализовано следующим кодом (применяется для всех файлов, имеющих точку в имени). Нажмите клавишу «**:**» и введите следующие команды по одной (нажимая Enter после каждой):

```
au BufWinLeave *.* mkview
```

```
au BufWinEnter *.* silent loadview
```

Поиск и замена

Поиск осуществляется командами «/» для поиска (по регулярному выражению) вперед, а «**?**» в обратном направлении. Для продолжения поиска используйте «**n**», а для прошлого варианта «**N**». Для поиска слова под курсором используются соответственно «**#**» и «*****».

Для поиска с заменой используйте **^s^TO/m что/gic**, где «**%**» означает работу со всем текстом (а не с текущей строкой), «g» - глобальная замена (а не первое совпадение), «i» - игнорирование регистра, а «c» - подтверждение каждого действия.

Автодополнение

Производится по содержимому данного файла, а также указанных в переменной **dictionary** по нажатию клавиш ' '.

Отмена

«**u**» для отмены и ' ' смена регистра.

«**~**» для выделенного участка (или буквы под курсором). «**U**» - принудительно установить верхний регистр, а «**u**» - нижний регистр.

Повторить

«**.**»

Конфигурация

Основным конфигурационным файлом является **~/.vimrc**. Активация русского шрифта в GUI-режиме плюс выбор темы для обоих режимов осуществляется, например, следующим кодом:

```
if has("gui_running")
colorscheme candy
set guifont=-cronyx-courier-medium-r-normal-*-*-120-*-*-m-*-koi8-r endif
if !has("gui_running") colorscheme elflord endif
```

Перечень наиболее используемых «горячих» клавиш:

Выход по **F10**:

```
nmap <F10> :q<CR>
imap <F10> <ESC>:q<CR>
```

Сохранение по **F2**:

```
nmap <F2> :w<CR>
imap <F2> <ESC>:w<CR>i<Right>
```

Компиляция по **F9**:

```
nmap <F9> :make<CR>
imap <F9> <ESC>:make<CR>
```

Текстовые редакторы в РЕД ОС

GNU Emacs
nano
pluma

GNU Emacs

Emacs — один из широко распространённых консольных текстовых редакторов.

Для использования **Emacs** понадобится изучить набор команд и горячих клавиш, а также настроить редактор под себя. **Emacs** имеет встроенный язык программирования, который может использоваться для настройки, расширения и изменения поведения редактора. Функции написаны на языке **Elisp**. Синтаксис **Lisp** довольно сложен для новичков, но новичкам и не обязательно писать свои расширения, по умолчанию в редакторе есть почти всё необходимое.

Для установки редактора перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install emacs
```

Вместе с консольной версией установится и графическая оболочка, поэтому для запуска именно консольной версии необходимо использовать параметр **–nw**.

```
emacs -nw
```

Чтобы открыть руководство в **Emacs**, нажмите клавиши `CTRL+H`, а затем `R`. Закрыть **Emacs** можно с помощью сочетания клавиш `CTRL+X`, а затем `CTRL+C`.

Для новичков **Emacs** имеет большой недостаток - он не русифицирован и имеет только английскую версию интерфейса.

Emacs является редактором с большим количеством дополнительных возможностей. Его можно использовать как:

- текстовый редактор;
- программу для чтения почты и новостей **Usenet**;
- интегрированную среду разработки (**IDE**);
- операционную систему;
- написать свой скрипт и использовать для любых функций.

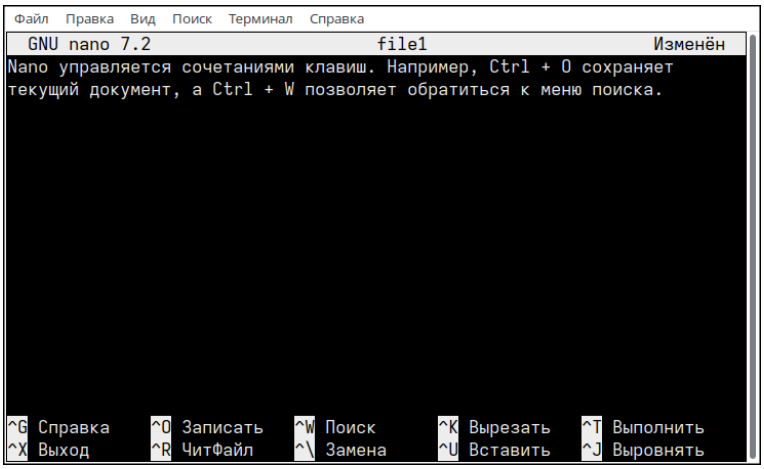
nano

nano - очень простой текстовый редактор с интерфейсом **curses**, с ним разберётся любой новичок. Редактор предустановлен в РЕД ОС по умолчанию.

Запускается редактор командой (можно использовать для запуска различные опции):

```
nano <опции>
```

Чтобы открыть какой-либо файл, достаточно передать его в параметрах команде **nano**. Если указанного файла не существует, будет создан новый.



Главное окно программы выглядит интуитивно понятно - в верхней строке находится версия редактора и имя файла, а также уведомление был ли файл изменен. Затем идет текстовое поле, а внизу - имя файла и основные сочетания клавиш, которые вы можете использовать для работы с программой. Например, для выхода из редактора используется сочетание CTRL+X.

pluma

Pluma (**pluma**) - это небольшой и легкий текстовый редактор, разработанный специально для рабочего стола **MATE**. **Pluma** использует интерфейс со вкладками, который позволяет редактировать более одного документа одновременно.

Pluma поддерживает большинство стандартных функций редактирования. За счёт подключаемых плагинов можно увеличивать возможности программы. Новые функции постоянно находятся в стадии разработки, в настоящее время в **Pluma** есть:

- подсветка синтаксиса;
- проверка орфографии;
- браузер файлов;
- сортировка;
- вставка даты / времени;
- поиск и замена;
- поддержка печати и предварительного просмотра и др.

Он имеет большинство стандартных функций текстового редактора и полностью поддерживает международный текст в Юникоде. Расширенные функции включают подсветку синтаксиса и применение автоматического отступа исходного кода, печать и редактирование нескольких документов в одном окне. **Pluma** расширяется с помощью системы плагинов, которая в настоящее время включает поддержку проверки орфографии, сравнения файлов, просмотра списков изменений **VCS** и настройки уровней отступов.

Запускается редактор командой:

```
pluma <параметры>
```

WPS Office

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** WPS-Office - 11.1.0.11664

WPS Office — офисный пакет, созданный китайским разработчиком программного обеспечения **Kingsoft**, как альтернатива **Microsoft Office**.

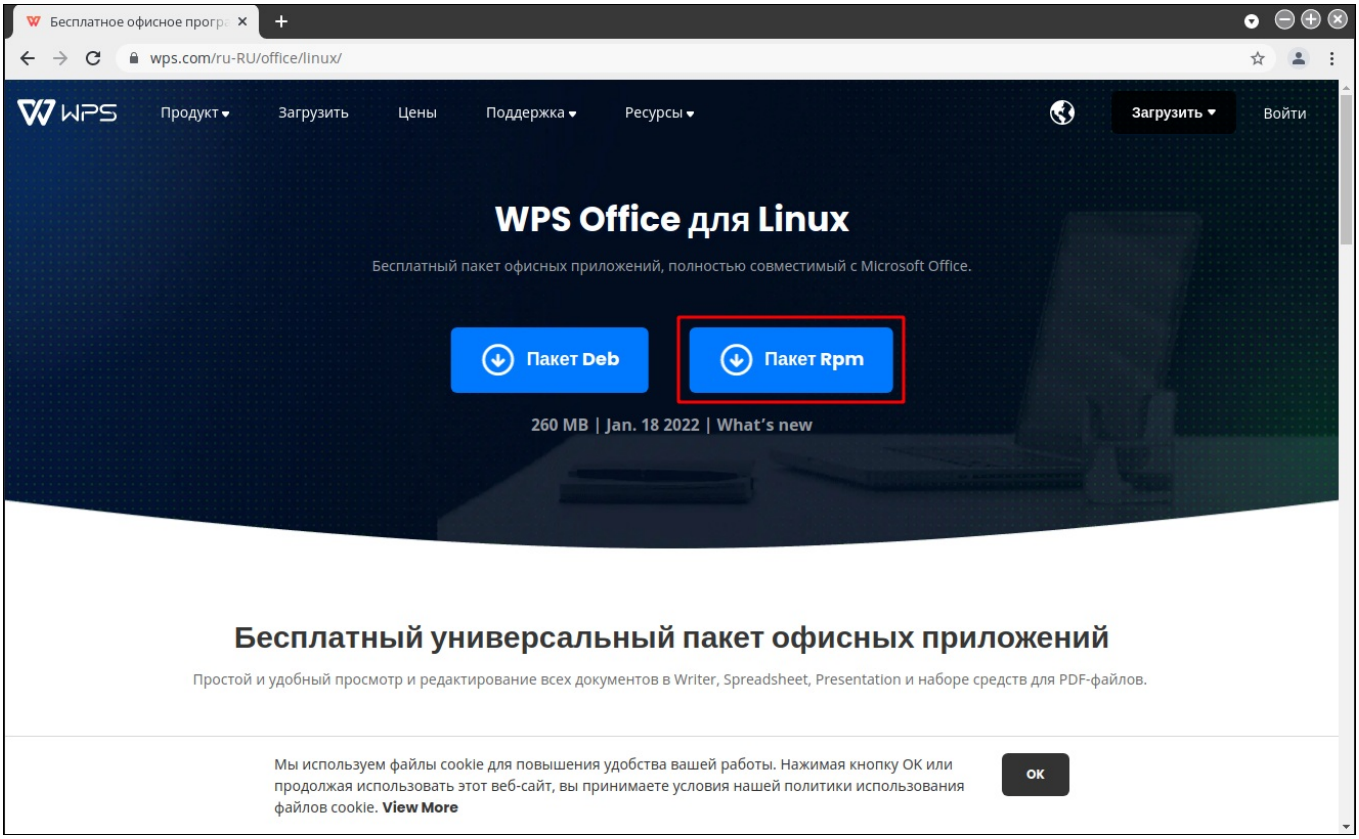
Пакет состоит из текстового процессора **WPS Writer**, программы создания презентаций **WPS Presentation** и табличного процессора **WPS Spreadsheets**.

Основные характеристики:

- Поддержка форматов **DOCX**, **XLSX**;
- Встроенная панель **Google Search**;
- Переключение по вкладкам;
- Экспорт в PDF-файл (также существуют дополнительные инструменты распознавания текстов из изображений и PDF);
- Шифрование перед сохранением;
- Подготовка на печать несколько новых документов;
- Поддержка **OLE Automation** (технология связывания и внедрения объектов в другие документы и объекты).

Установка

Для установки **WPS Office** необходимо скачать rpm-пакет с официального сайта разработчика.



После загрузки файла в консоли выполните следующие действия:

1. Перейдите в сеанс пользователя **root**:

```
su -
```

2. Перейдите в папку с дистрибутивом (в качестве примера /home/user/Загрузки/:

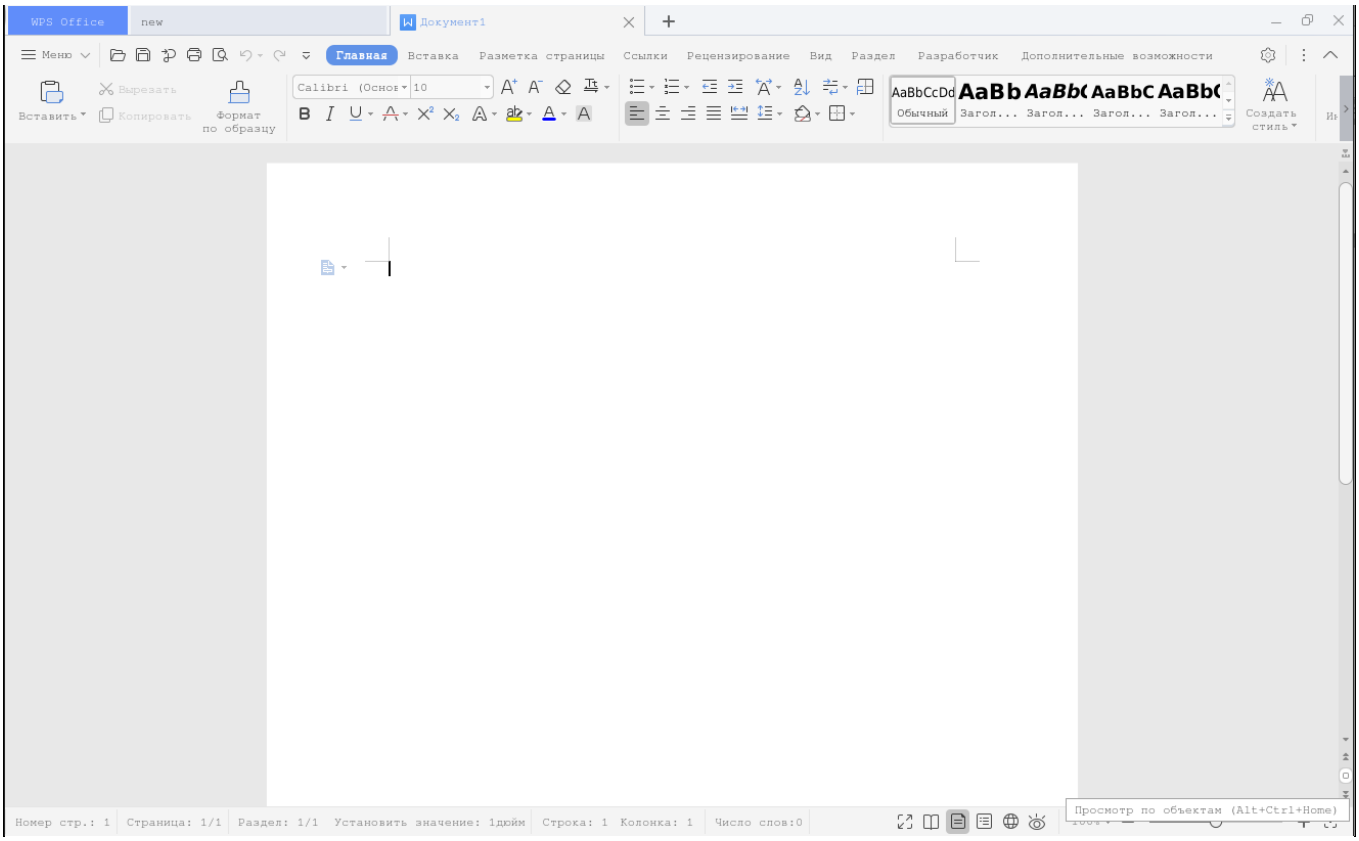
```
cd /home/user/Загрузки/
```

3. Установите **WPS Office**:

```
dnf install wps-office-11.1.0.10920.XA-1.x86_64.rpm
```

После установки компоненты **WPS Office** будут доступны в «**Главном меню**» - «**Офис**» или выполните команду от локального пользователя:

```
wps
```



OnlyOffice

Установка rpm-пакета с официального сайта
Добавление репозитория OnlyOffice

Окружение:

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** OnlyOffice - 7.2.1

OnlyOffice - это бесплатный офисный пакет для работы с текстовыми документами, электронными таблицами и презентациями без подключения к интернету.

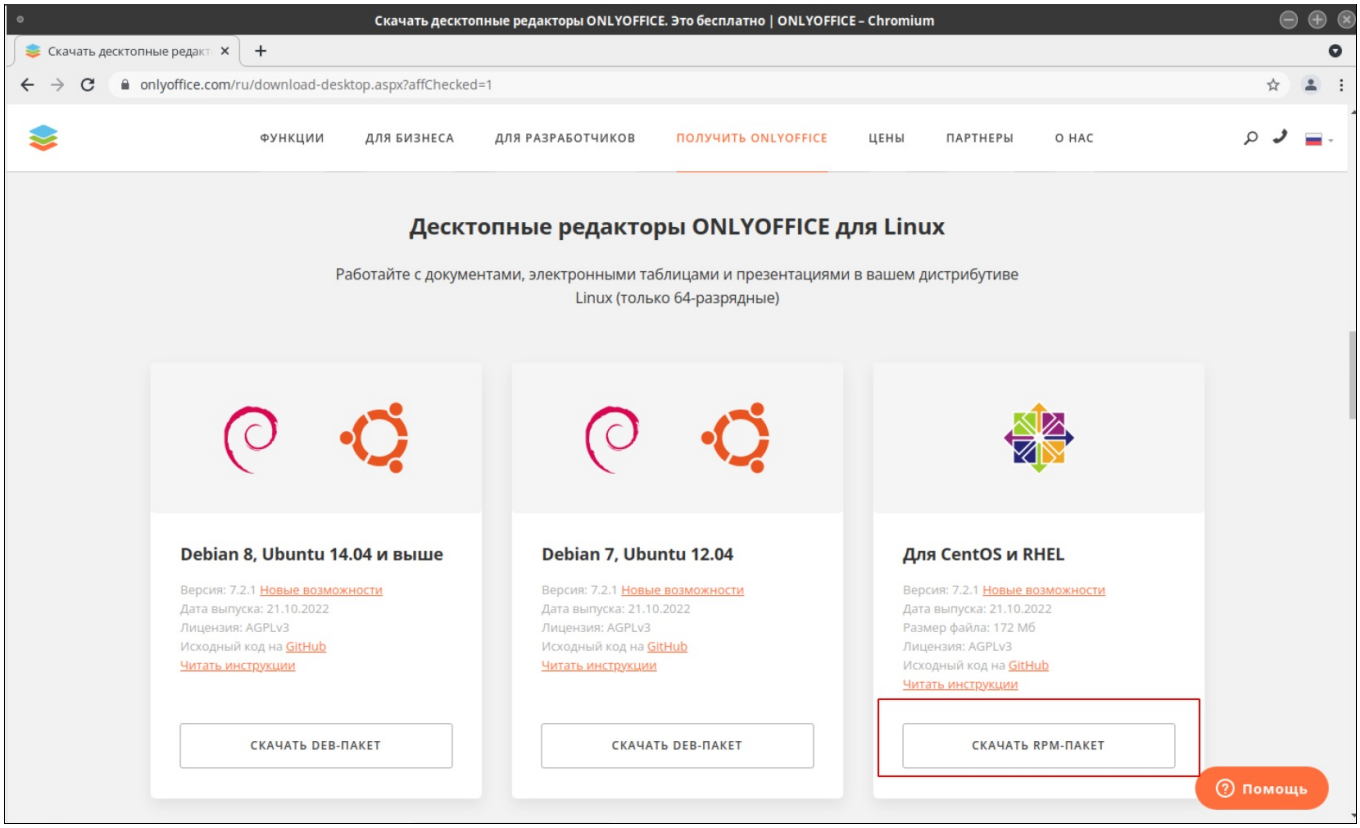
Приложение подключается к облачным и серверным версиям **OnlyOffice**, позволяя тем самым совместно редактировать документы в режиме реального времени.

Редакторы **OnlyOffice** полностью совместимы с **MS Office** и **OpenDocument** и поддерживают популярные форматы:

- DOC, DOCX, ODT, RTF, TXT;
- PDF;
- HTML;
- EPUB;
- XPS;
- DjVu;
- XLS, XLSX, ODS, CSV;
- PPT, PPTX, ODP.

Установка rpm-пакета с официального сайта

Для установки **OnlyOffice** необходимо скачать **rpm-пакет** с официального сайта разработчика.



После загрузки файла в консоли выполните следующие действия:

1. Перейдите в сеанс пользователя **root**:

```
su -
```

2. Перейдите в папку «**Загрузки**»:

```
cd /home/user/Загрузки/
```

3. Установите **OnlyOffice**:

```
dnf install onlyoffice-desktopeditors.x86_64.rpm
```

После установки программа будет доступна в «**Главном меню**» - «**Офис**» - «**ONLYOFFICE Desktop Editors**».

Добавление репозитория OnlyOffice

Для удобства работы и легкости обновления в будущем репозиторий **OnlyOffice** можно добавить непосредственно в ОС. Для этого необходимо:

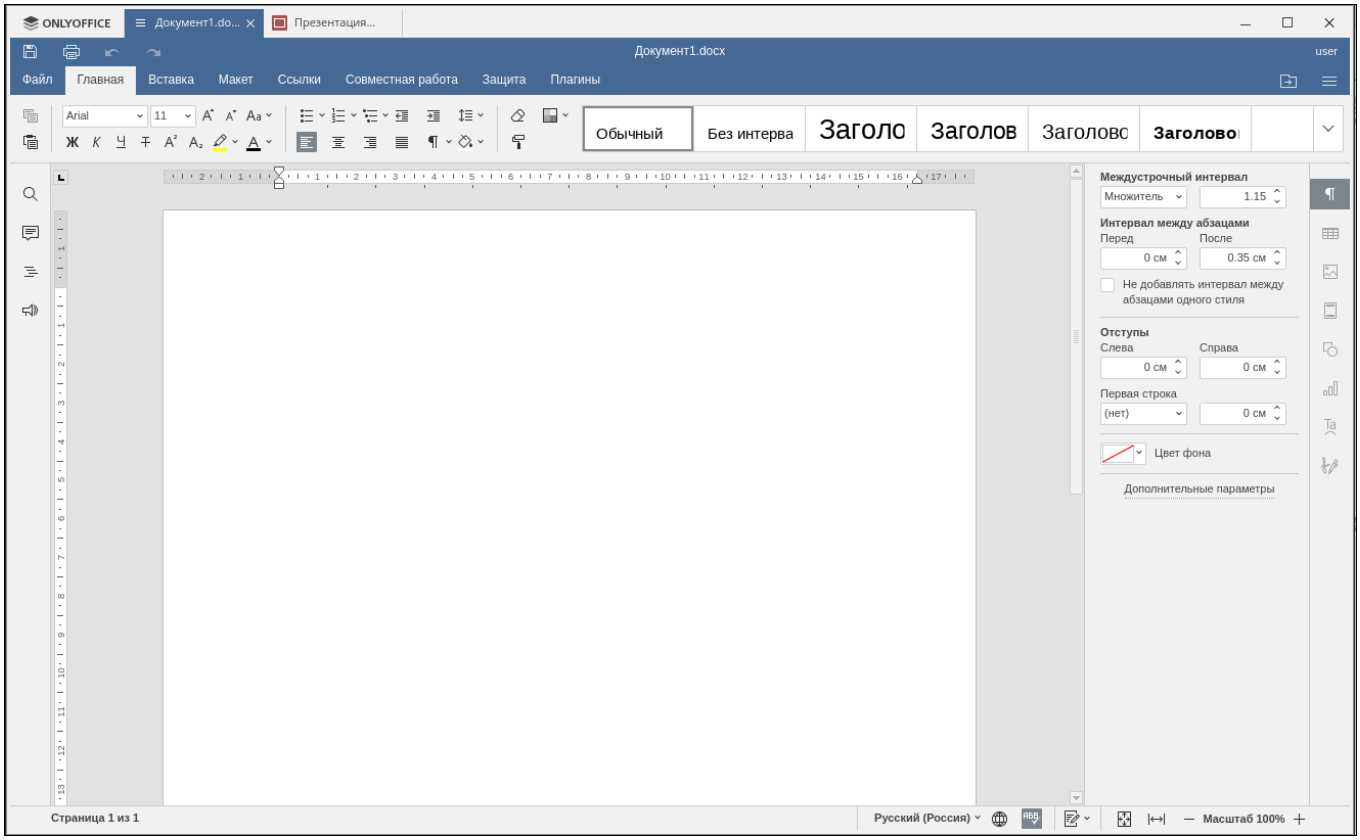
1. Добавить репозиторий командой **от пользователя root:**

```
dnf install https://download.onlyoffice.com/repo/centos/main/noarch/onlyoffice-repo.noarch.rpm
```

2. Провести стандартную установку пакета **от пользователя root:**

```
dnf install onlyoffice-desktopeditors
```

Для запуска перейдите в «**Главное меню**» - «**Офис**» - «**ONLYOFFICE Desktop Editors**»



МойОфис

Установка
Настройка панели Образование

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: МойОфис 2022.01-1.28.0.4

«**МойОфис Образование**» – это комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями.

«**МойОфис Текст**» обеспечивает удобное и быстрое создание документов с использованием шаблонов, стилей и средств форматирования текста. Функции совместного редактирования обеспечивают эффективную совместную работу сотрудников.

«**МойОфис Таблица**» – это приложение для быстрой и удобной работы с электронными таблицами и анализа данных. Продукт поддерживает расширенный набор формул и средств для обработки данных. Совместное редактирование на любой из поддерживаемых платформ обеспечивает быстрый анализ и подготовку документов группой сотрудников даже вне офиса.,

«**МойОфис Презентация**» – приложение с полным набором инструментов для просмотра графических презентаций.

Установка

Для установки «**МойОфис**» необходимо скачать пакет в формате **.rpm** с официального сайта разработчика.

После загрузки файла в консоли перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install /home/user/Загрузки/myoffice-standard-home-edition-2022.01-1.28.0.4.x86_64.rpm
```

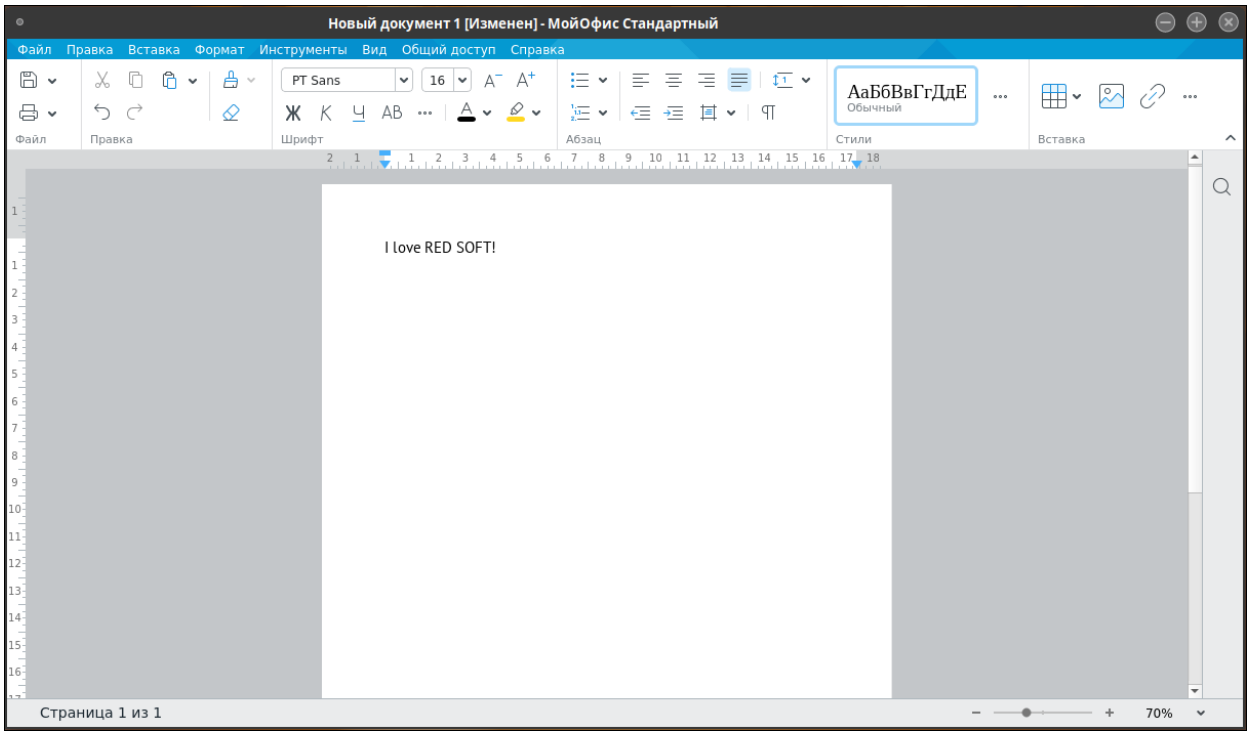
После установки редакторы будут доступны в «**Главном меню**» - «**Офис**» - «**МойОфис**».

При первом запуске потребуется принять лицензионное соглашение.



Нажмите «**Принять**».

После этого «**МойОфис**» готов к работе.



Настройка панели Образование

Для изменения данных на панели *Образование* перейдите в сеанс пользователя **root**:

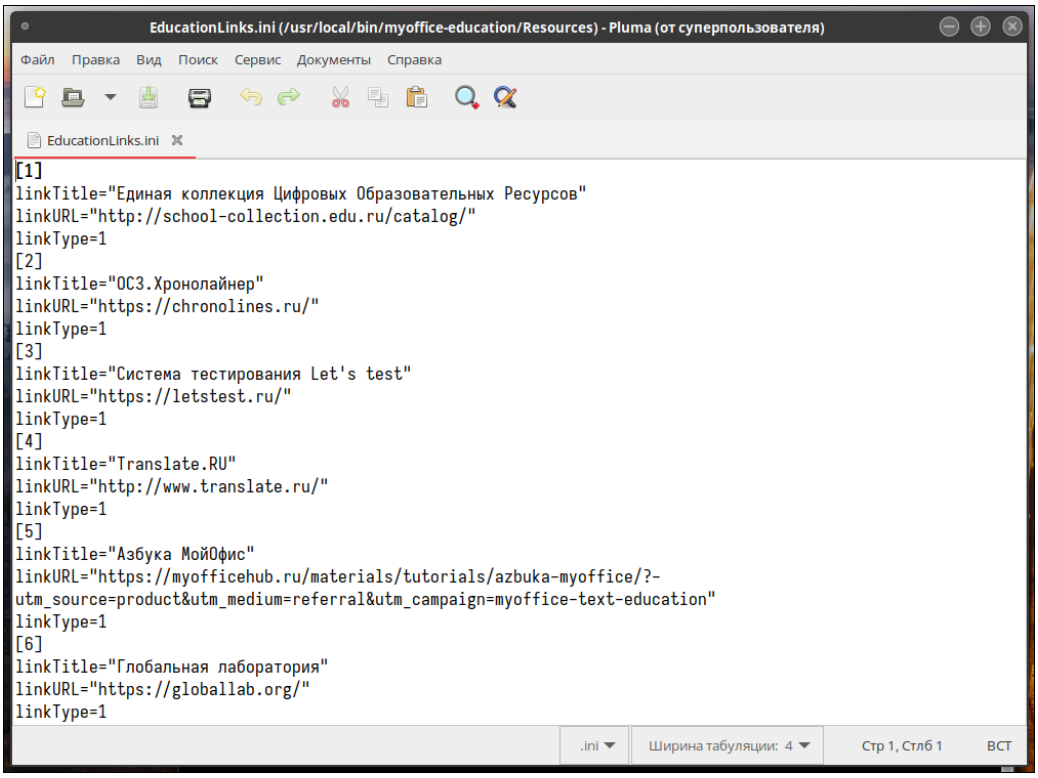
```
su -
```

и внесите изменения в следующий файл:

```
nano /usr/local/bin/myoffice-education/Resources/EducationLinks.ini
```

Изменения вносятся в список ресурсов, где:

- **[номер секции]** – порядок следования ссылки в панели *Образование*;
- **linkTitle** – заголовок ссылки (то, что отображается на панели *Образование*);
- **linkURL** – ссылка на ресурс;
- **linkType** – тип иконки, расположенный слева от ссылки:
  - 0 – дневник;
  - 1 – указатель ссылки.



Пример:

```
[7]
linkTitle="Библиотека"
linkURL="https://uchebnik.mos.ru/"
linkType=0

[8]
linkTitle="Электронный дневник"
linkURL="https://schools.school.mosreg.ru"
linkType=0
```

Сохраните изменения, нажав **Ctrl+O**, затем **Enter** и **Ctrl+X**.

Перезапустите редактор текста или таблицы – панель *Образование* будет обновлена.

Р7-Офис

Установка Р7-Офис. Редакторы документов
Технические требования
Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora
Активация лицензии

Установка Р7-Офис. Органайзер
Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora

Установка Р7-Графика
Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora
Активация лицензии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: r7-release-1.0-1, r7-office-2024.4.1-630, r7organizer-3.1.2-1, R7Grafika-1.8.221111227-1

Установка Р7-Офис. Редакторы документов

Р7-Офис – это российский офисный пакет включающий в себя профессиональные редакторы документов, таблиц и презентаций.

Десктопные редакторы **Р7-Офис** позволяют работать с документами во всех популярных форматах самостоятельно или совместно с другими людьми с помощью широких функций совместной работы.

Текстовый редактор **Р7-Офис** поддерживает открытие и сохранение документов в таких популярных форматах, как **ODT**, **DOCX**, **PDF** и многих других. Обладает широкими возможностями по форматированию и вставке текста, таблиц, картинок и колонтитулов.

Табличный редактор **Р7-Офис** поддерживает открытие и сохранение табличных документов в таких популярных форматах, как **XLS**, **XLSX**, **ODS** и других. Обладает широкими возможностями по созданию, редактированию таблиц, вставке данных, созданию формул и построению графиков. В редакторе имеется большое количество встроенных функций и формул: финансовые, математические, поисковые и прочие для реализации разных целей и задач.

Редактор презентаций **Р7-Офис** – это профессиональный инструмент для создания презентаций. С его помощью можно создавать яркие демонстрационные материалы в таких популярных форматах, как **PPTX**, **PPT**, **ODP** и других. Удобная настройка показа слайдов и коллекция готовых переходов позволяет создавать современные интерактивные презентации.

Офисный пакет **Р7-Офис** для РЕД ОС размещается в отдельном подключаемом (с помощью пакета **r7-release**) репозитории. **Р7-Офис** в данном репозитории был собран специально для работы в РЕД ОС и использует необходимые зависимости из репозитория РЕД ОС.

Вы можете подробнее ознакомиться с работой офисных пакетов **Р7-Офис** и **Р7-Органайзер**, просмотрев наши обучающие видео:

- на **RuTube** — Р7-Офис и РЕД ОС;
- в **Яндекс.Дзен** — Р7-Офис и РЕД ОС;
- в **VK Видео** — Р7-Офис и РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

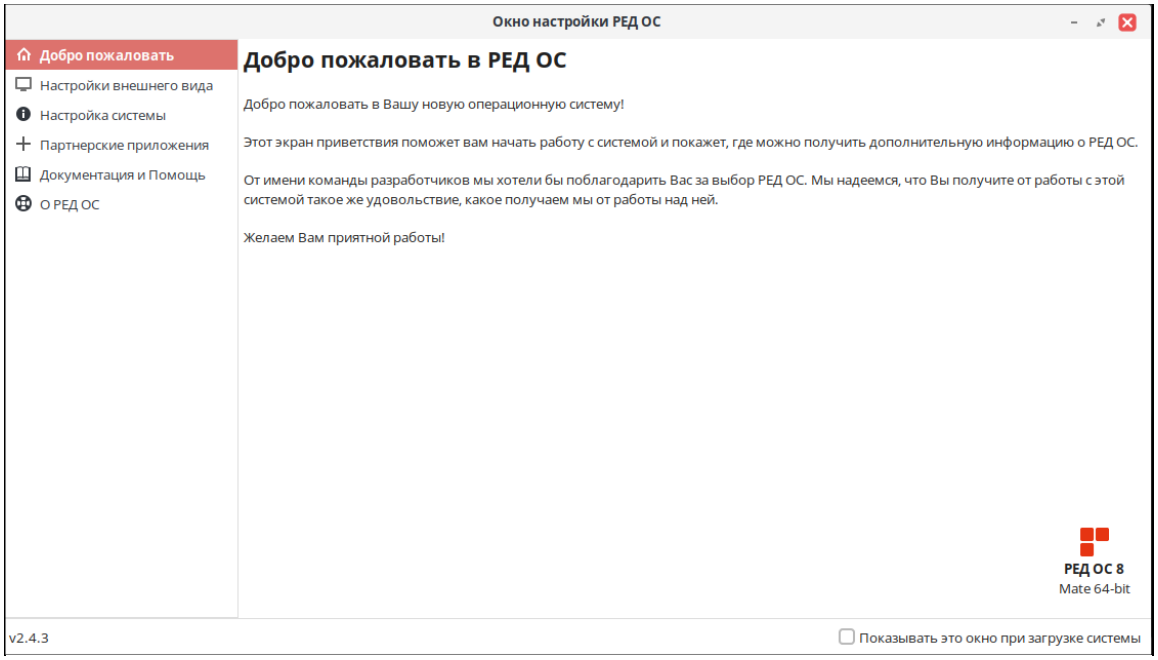
Технические требования

Для корректной работы программного обеспечения используемое оборудование должно выполнять следующие технические требования:

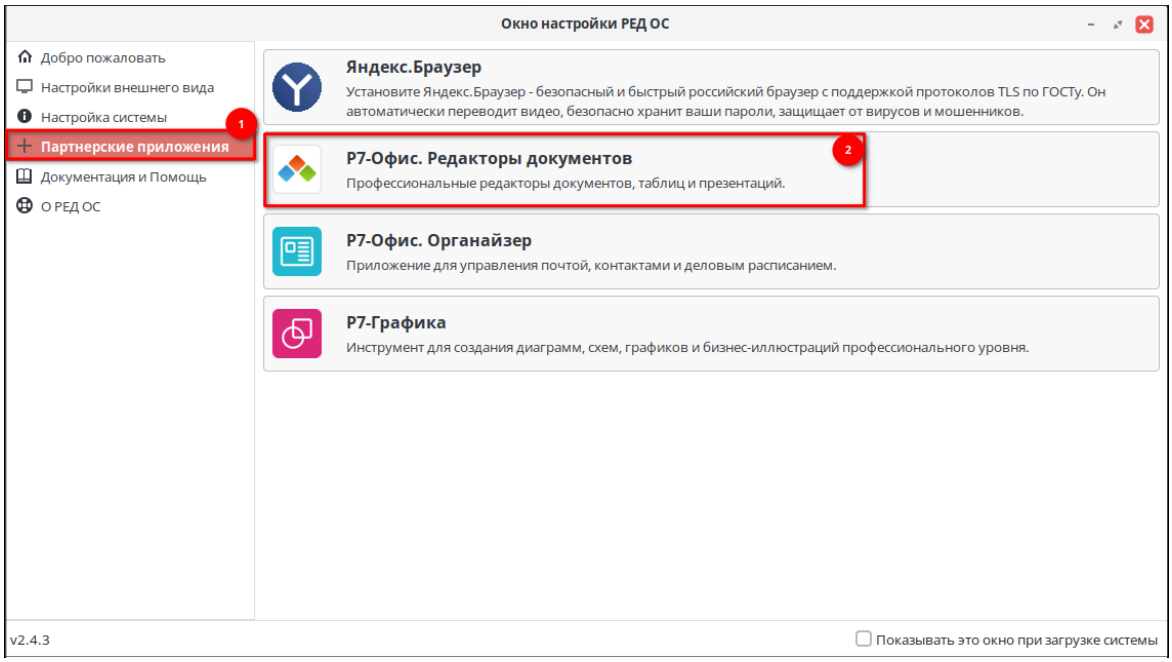
- двухъядерный процессор **2 ГГц и выше**;
- оперативная память **не менее 2 Гб**;
- свободное дисковое пространство **не менее 2 Гб**.

Установка через «Окно настройки РЕД ОС»

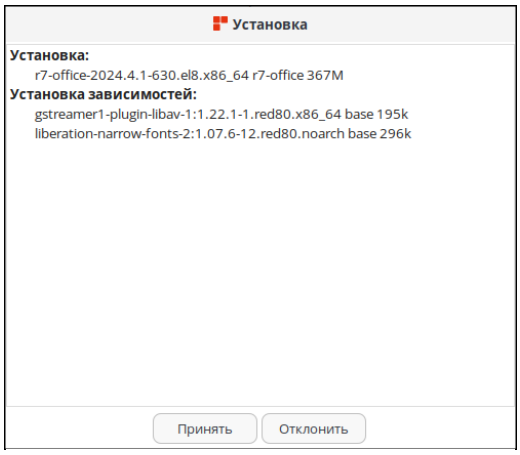
Откройте утилиту «Окно настройки РЕД ОС».



Перейдите на вкладку «**Партнерские приложения**», затем выберите из списка «**Р7-Офис. Редакторы документов**».



Далее в появившемся окне «**Установка**» ознакомьтесь со списком устанавливаемых пакетов и зависимостей и нажмите «**Принять**». Начнётся установка офисных пакетов **Р7-Офис**.



После установки редакторы будут доступны из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Профессиональный (десктопная версия)**».

Установка через терминал

Перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду подключения репозитория и установки офисного пакета:

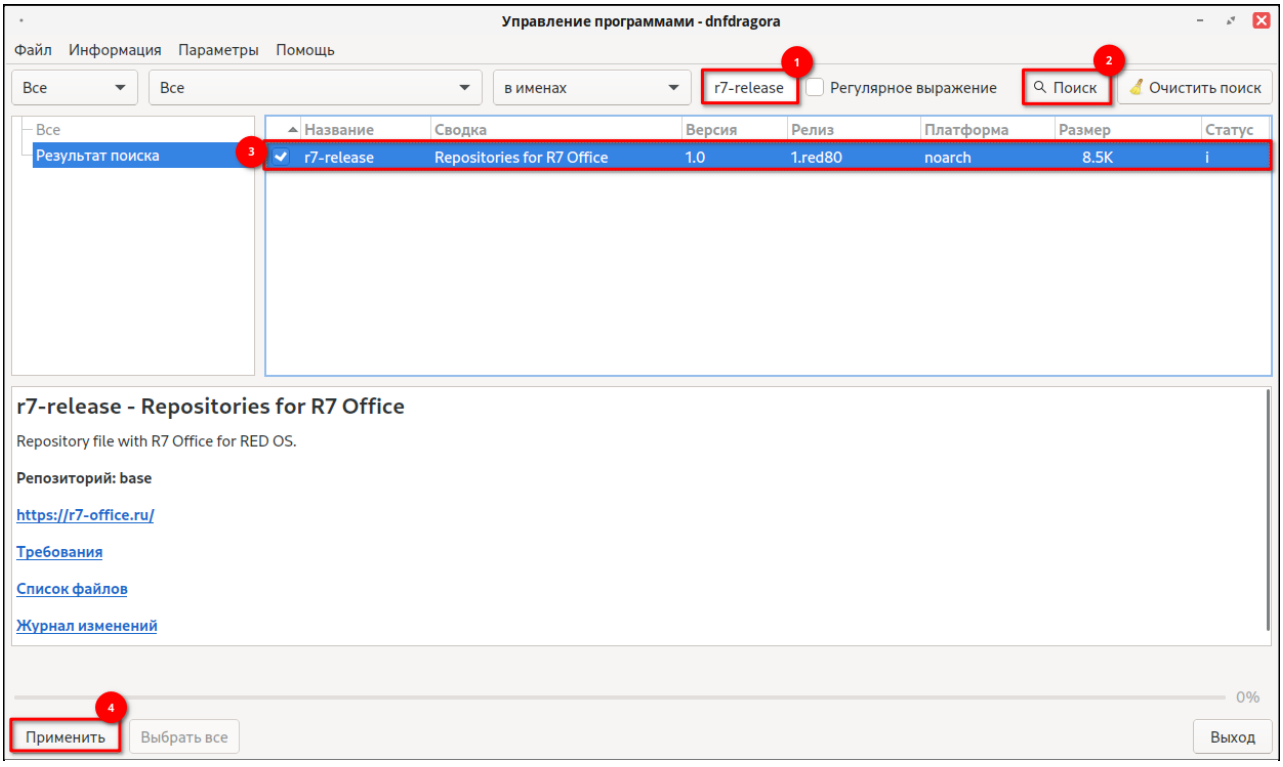
```
dnf install r7-release && dnf install r7-office
```

После установки редакторы будут доступны из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Профессиональный (десктопная версия)**».

Установка через dnfdragora

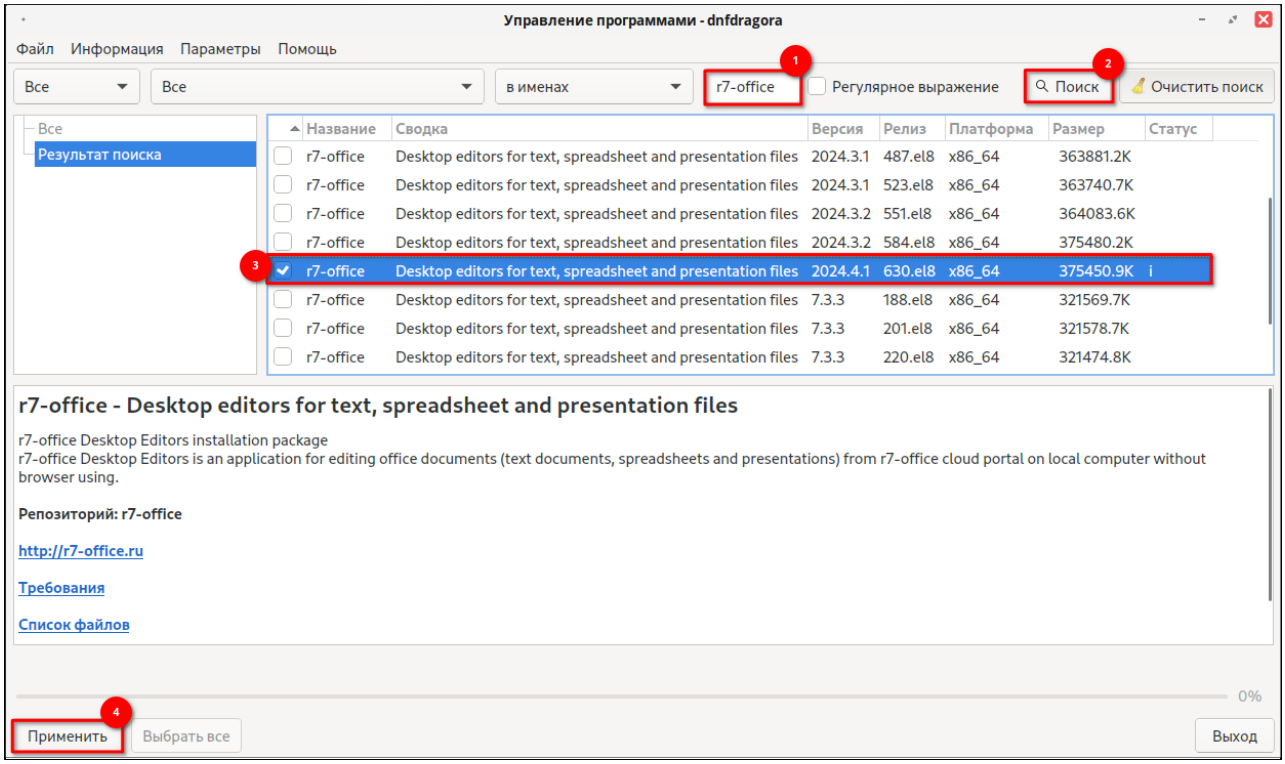
Для установки **Р7-Офис** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» – «**Администрирование**» – «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**r7-release**».

В результате поиска будет предложен к установке подключаемый репозиторий **r7-release**. Отметьте флагом репозиторий последней версии, нажмите кнопку «**Применить**» и дождитесь окончания установки.



После установки репозитория в строке поиска необходимо ввести название пакета «**r7-office**». Затем отметьте флагом пакет

последней версии и нажмите кнопку «**Применить**» для его установки.



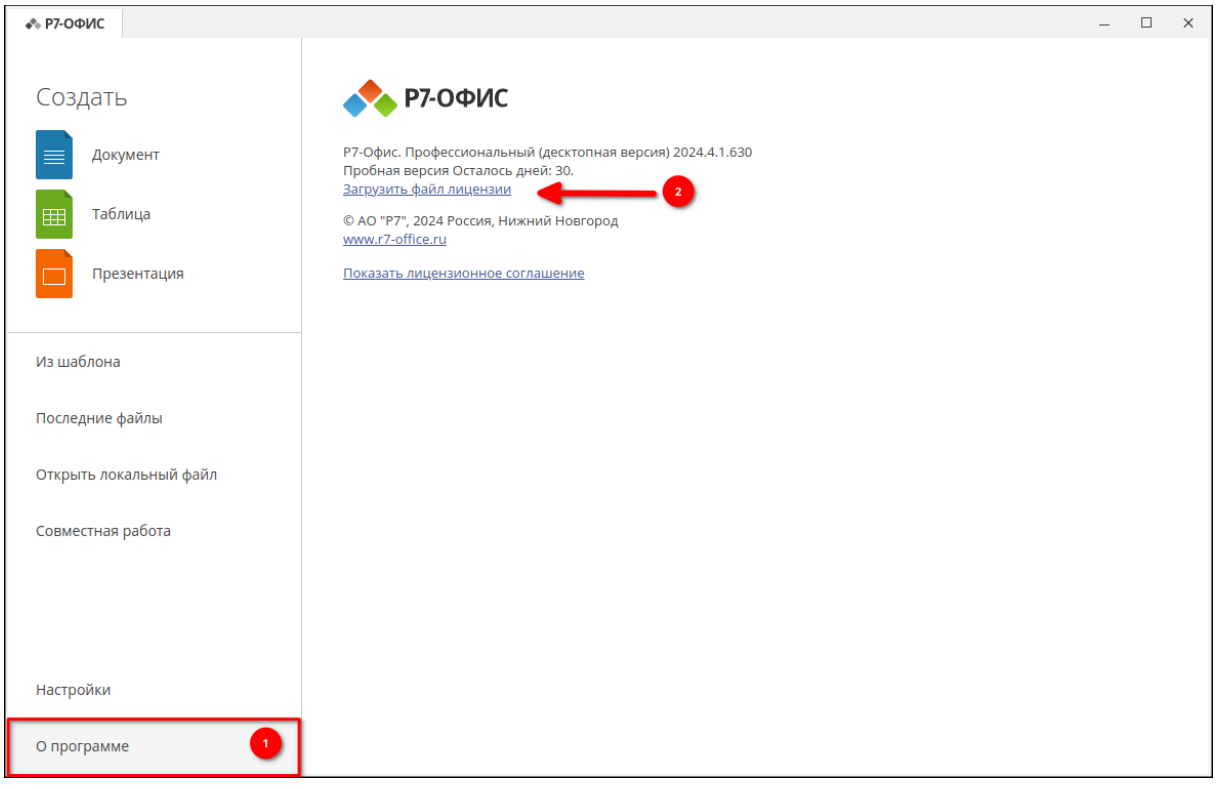
После установки редакторы будут доступны из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Профессиональный (десктопная версия)**».

Активация лицензии

Офисный пакет **Р7-Офис** предоставляет 30-дневный бесплатный пробный период на рассмотрение и изучение функций редакторов.

По истечении бесплатного пробного периода необходимо запросить у официального разработчика соответствующую лицензию.

Для этого в основном меню программы перейдите во вкладку «**О программе**» – «**Загрузить файл лицензии**» и укажите путь к загруженному файлу лицензии в формате ***.lickey**.



Установка Р7-Офис. Органайзер

Р7-Офис. Органайзер – это приложение для управления почтой, контактами и деловым расписанием. Включает в себя почтовый клиент с интуитивно понятным интерфейсом, надежной защитой от спама и удобным редактором писем с автоматической проверкой орфографии.

Фильтры, тэги и папки для сортировки писем позволяют организовать входящую почту. Также возможно подключить несколько аккаунтов.

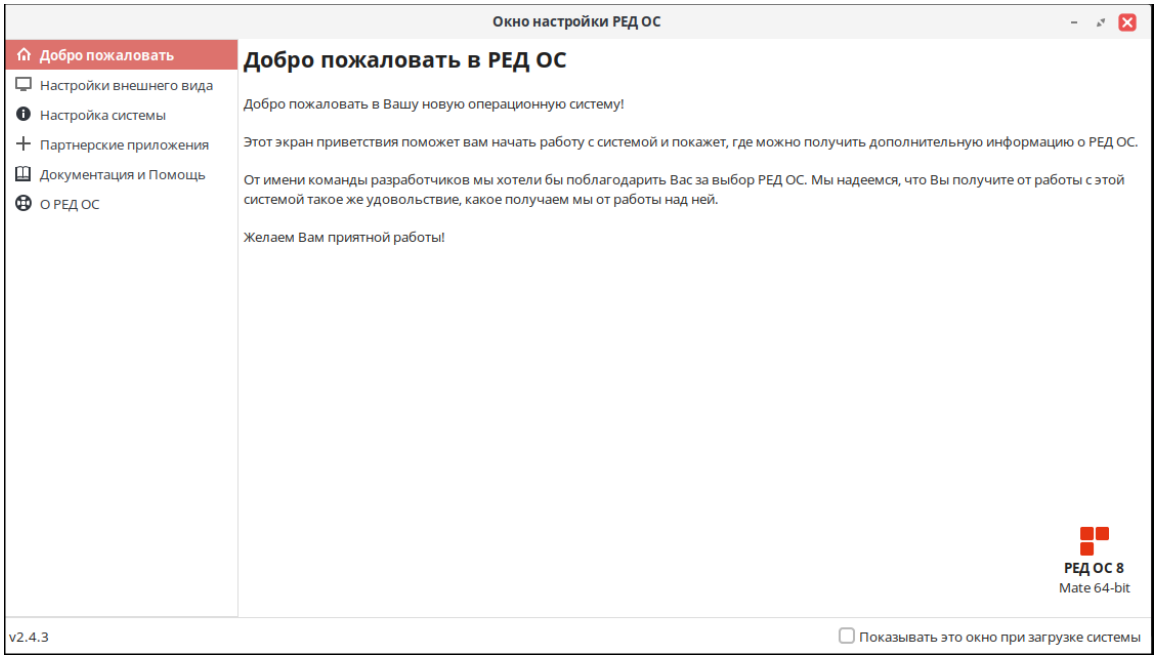
Личные и рабочие контакты хранятся в адресной книге и синхронизированы с почтой и календарем. В адресной книге доступно создание списков рассылки и ведение подробных карточек контактов.

Календарь с расписанием и списком дел – на день, неделю или месяц, напомнит о событиях и задачах.

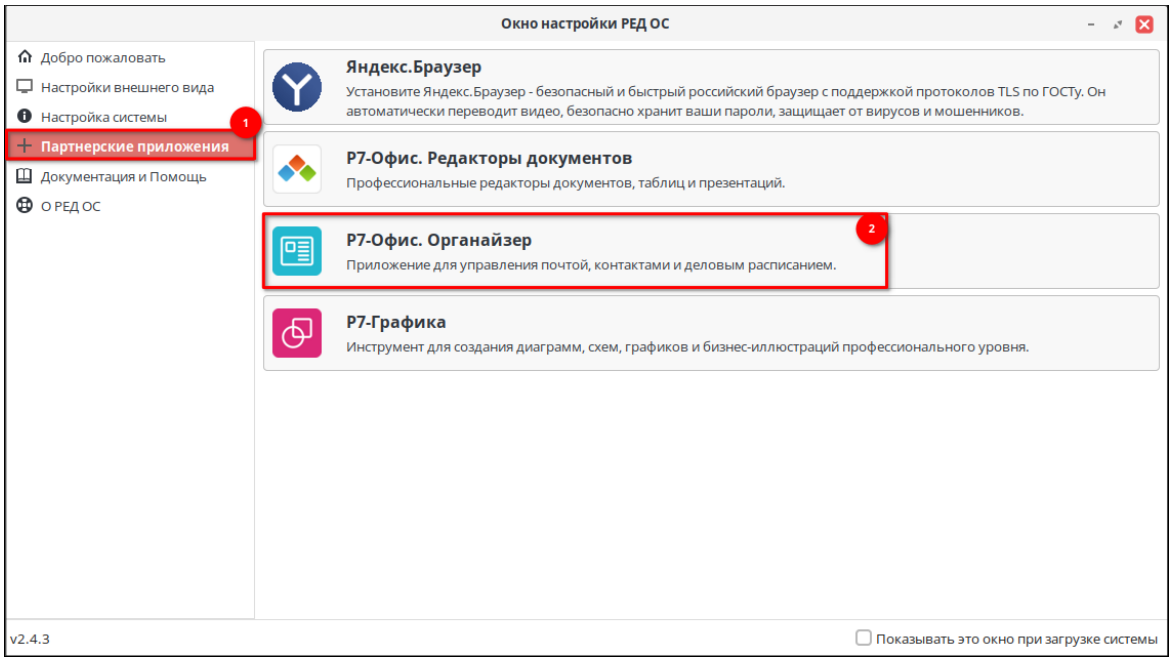
Доступна возможность создания нескольких календарей под разные группы событий и предоставления доступа коллегам. Общие календари позволяют выбрать удобное время для собрания и сделать рассылку приглашений.

Установка через «Окно настройки РЕД ОС»

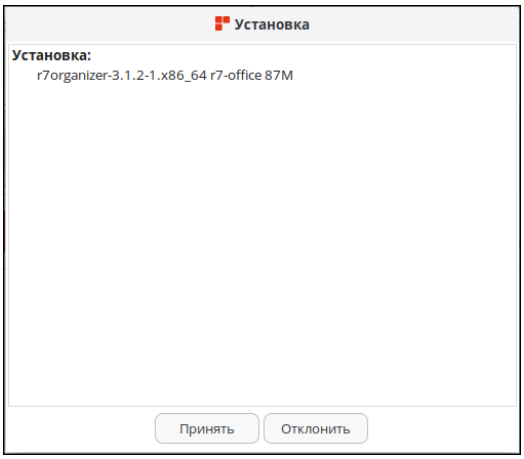
Откройте утилиту «Окно настройки РЕД ОС».



Перейдите на вкладку «**Партнерские приложения**», затем выберите из списка «**Р7-Офис. Органайзер**».



Далее в появившемся окне «**Установка**» ознакомьтесь со списком устанавливаемых пакетов и нажмите «**Принять**». Начнётся установка пакета **Р7-Офис. Органайзер**.



После установки органайзер будет доступен из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Органайзер**».

Установка через терминал

Перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду подключения репозитория и установки органайзера:

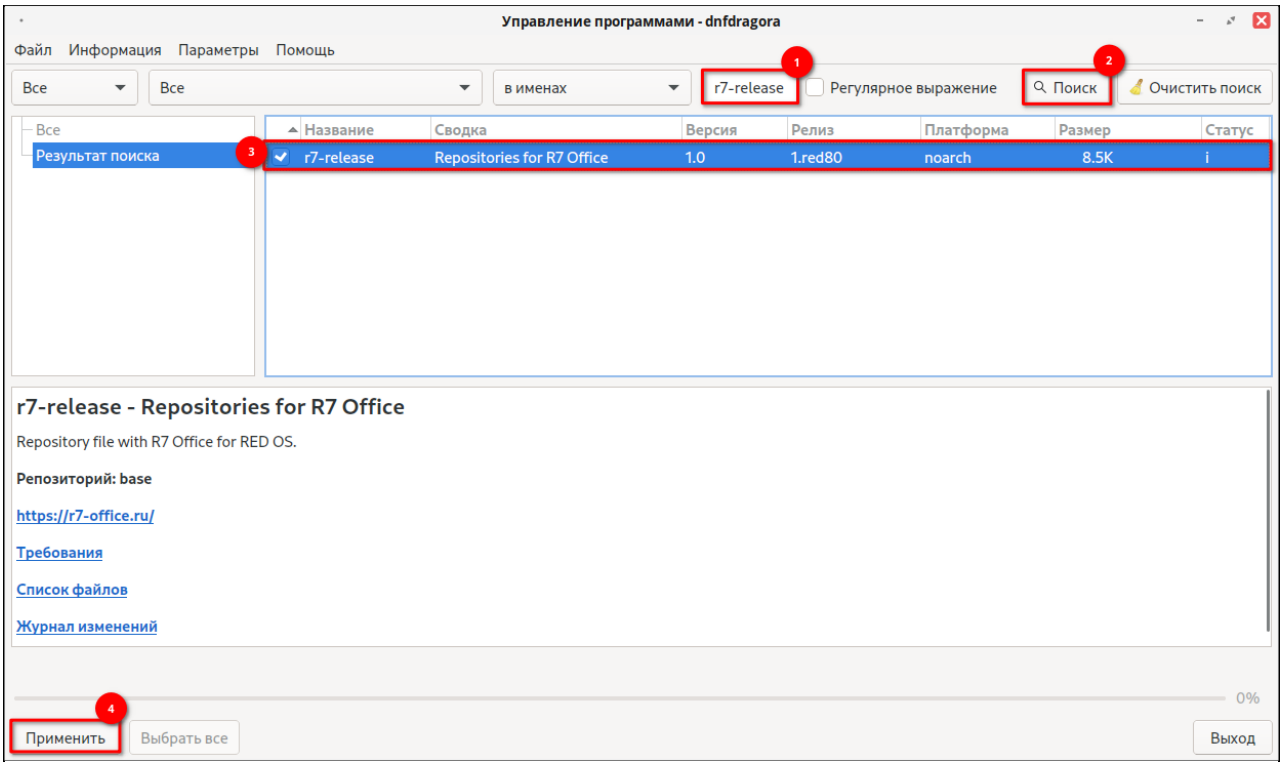
```
dnf install r7-release && dnf install r7organizer
```

После установки органайзер будет доступен из «**Главного меню**» – «**Офис**» – «**Р7-Офис. Органайзер**».

Установка через dnfdragora

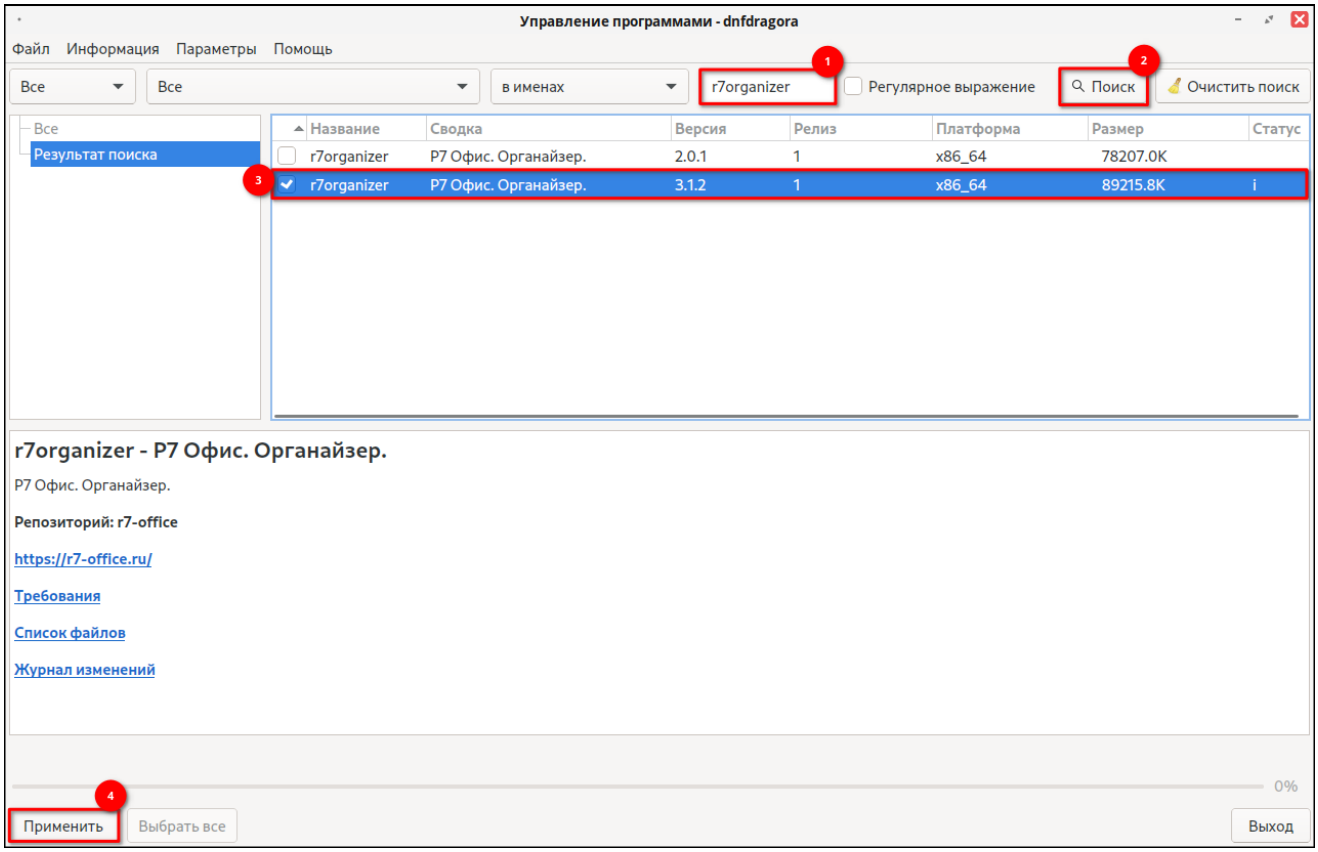
Для установки **Р7-Офис. Органайзер** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» – «**Администрирование**» – «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**r7-release**».

В результате поиска будет предложен к установке подключаемый репозиторий **r7-release**. Отметьте флагом репозиторий последней версии, нажмите кнопку «**Применить**» и дождитесь окончания установки.



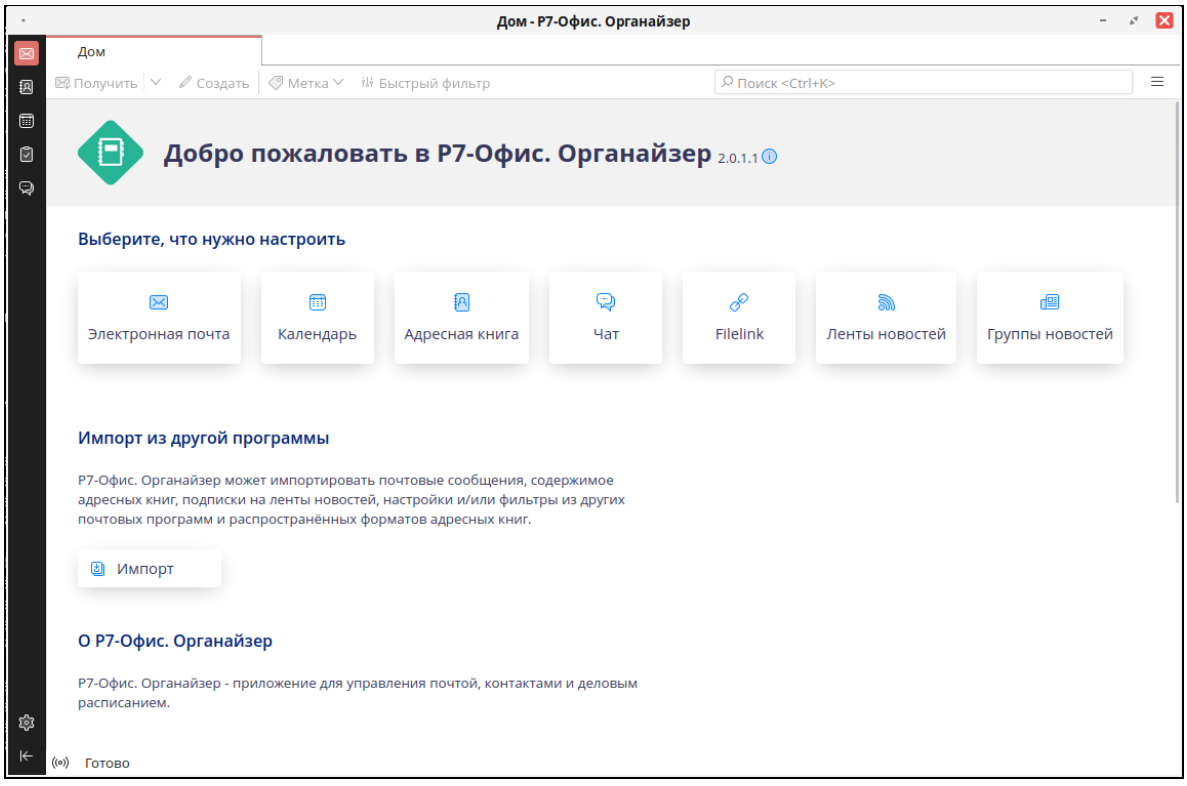
После установки репозитория в строке поиска необходимо ввести название пакета непосредственно самого

органайзера «**r7organizer**». Затем отметьте флагом пакет последней версии и нажмите кнопку « **Применить**» для его установки.



После установки органайзер будет доступен из «**Главного меню**» – «**Офис**» – «**P7. Органайзер**».

Окно **Органайзера** выглядит следующим образом:



Установка P7-Графика

P7-Графика – это инструмент для создания диаграмм, схем, графиков и бизнес-иллюстраций профессионального уровня.

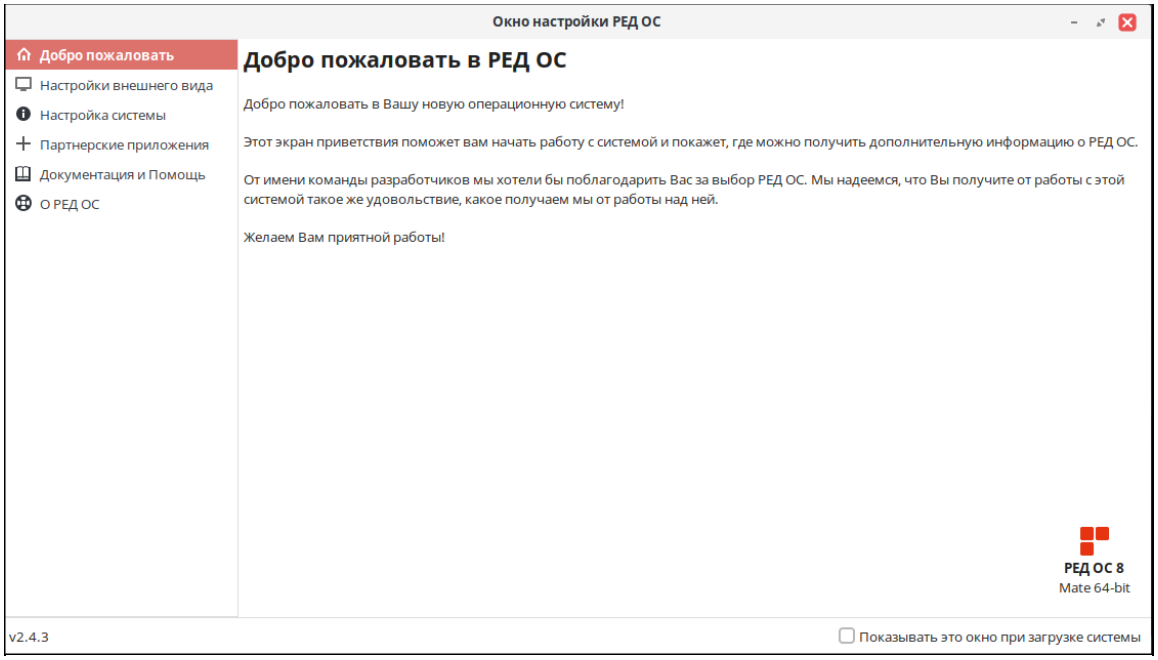
P7-Графика поддерживает открытие, редактирование и сохранение файлов **Visio** в формате ***.vsdx**. Имеет обширную библиотеку шаблонов тематических элементов, а также позволяет импортировать и экспортировать эти библиотеки для обмена данных с другими людьми.

Р7-Графика позволяет экспортировать диаграммы в различные форматы файлов, такие как **PNG**, **JPEG**, **PDF**, **SVG** и другие. Также доступен импорт существующих диаграмм из других приложений и последующее их редактирование в **Р7-Графика**.

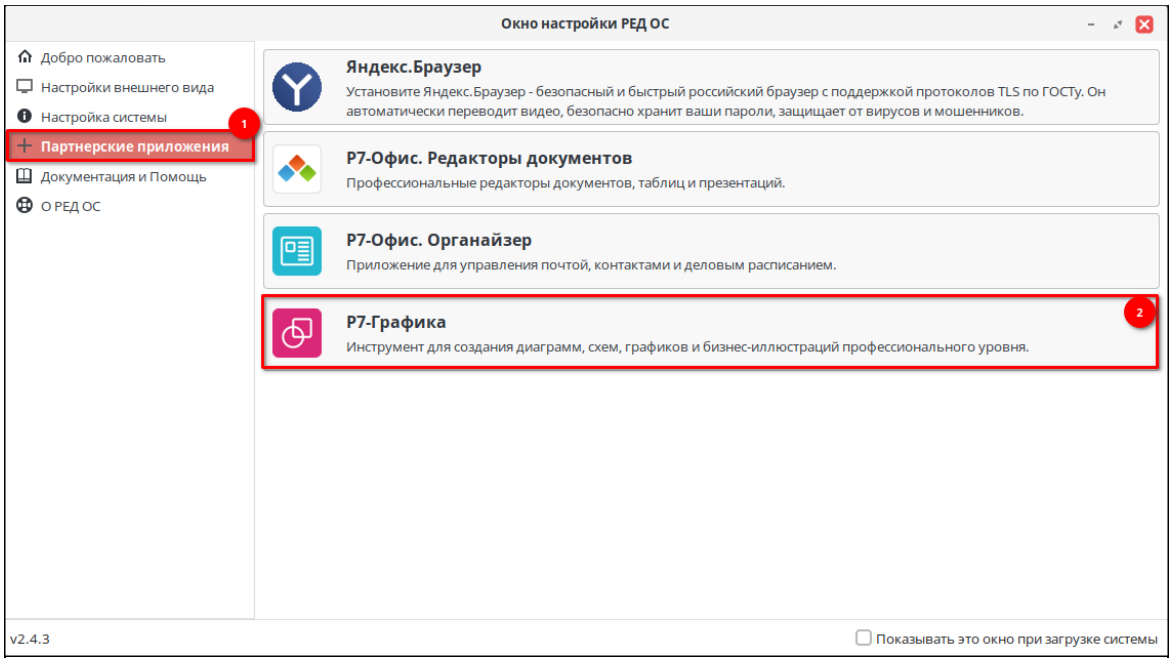
Р7-Графика имеет интуитивный интерфейс, здесь можно быстро добавлять и настраивать элементы, соединять их линиями и создавать профессиональные диаграммы.

Установка через «Окно настройки РЕД ОС»

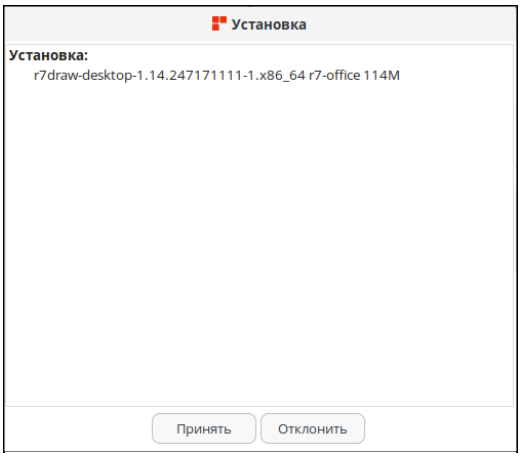
Откройте утилиту «Окно настройки РЕД ОС».



Перейдите на вкладку «**Партнерские приложения**», затем выберите из списка «**Р7-Графика**».



Далее в появившемся окне «**Установка**» ознакомьтесь со списком устанавливаемых пакетов и нажмите «**Принять**». Начнётся установка пакета **Р7-Графика**.



После установки редактор диаграмм будет доступен из «**Главного меню**» – «**Графика**» – «**Р7-Графика**».

Установка через терминал

Перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду подключения репозитория и установки **Р7-Графики**:

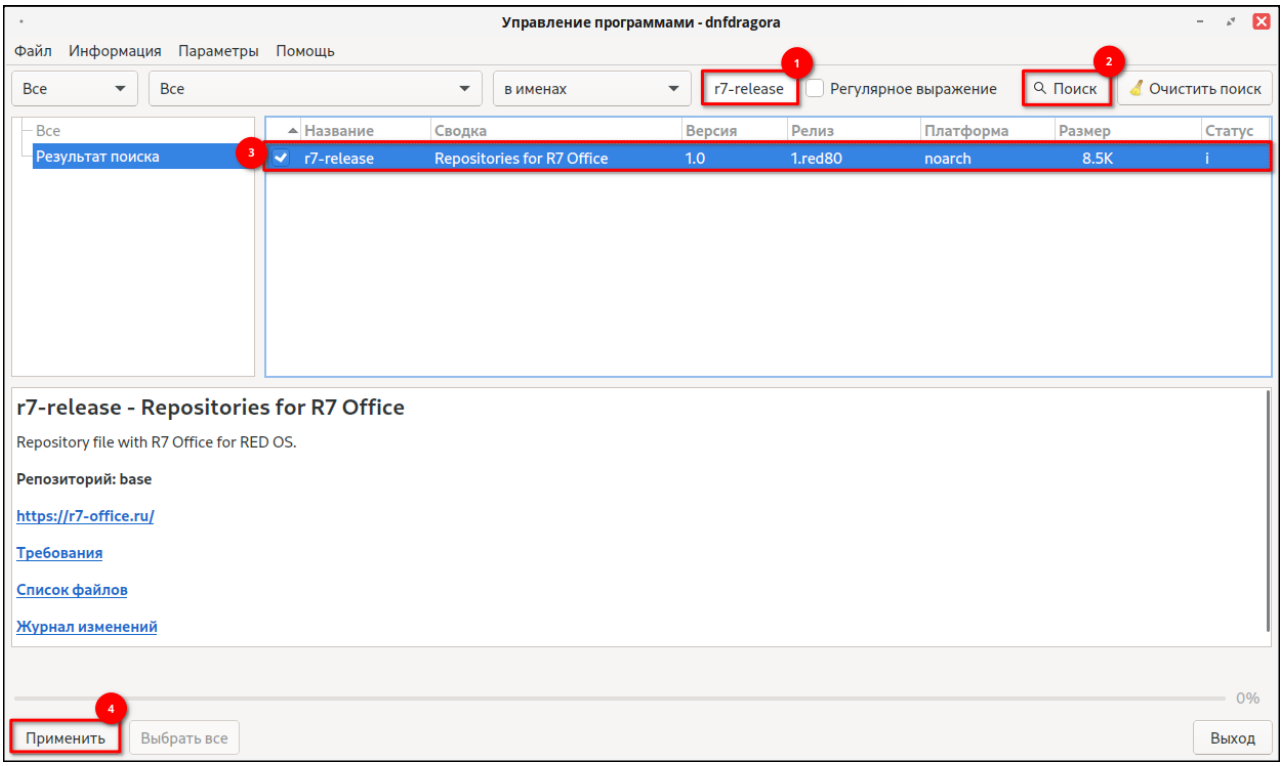
```
dnf install r7-release && dnf install R7Grafika
```

После установки редактор диаграмм будет доступен из «**Главного меню**» – «**Графика**» – «**Р7-Графика**».

Установка через dnfdragora

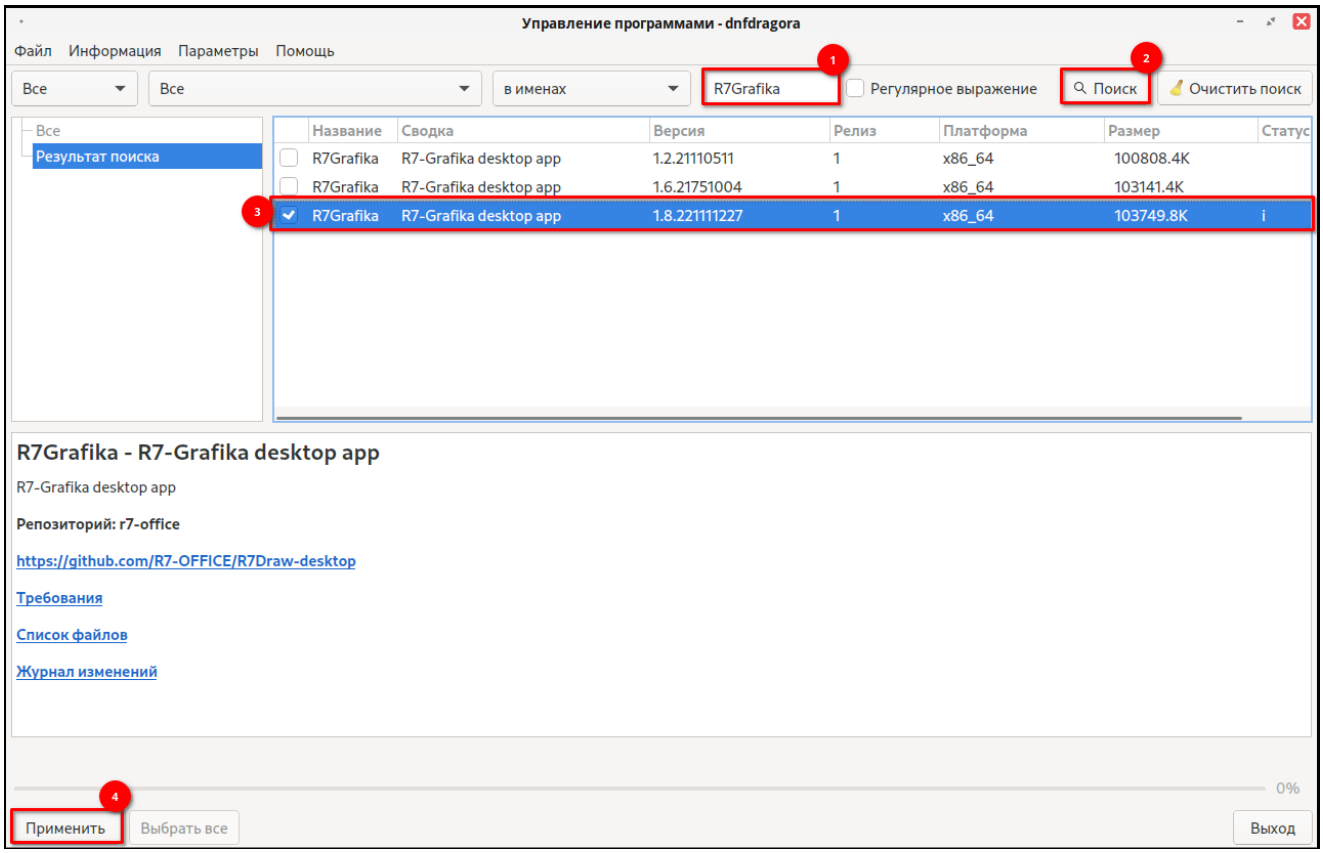
Для установки **Р7-Графики** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» – «**Администрирование**» – «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**r7-release**».

В результате поиска будет предложен к установке подключаемый репозиторий **r7-release**. Отметьте флагом репозиторий последней версии, нажмите кнопку «**Применить**» и дождитесь окончания установки.



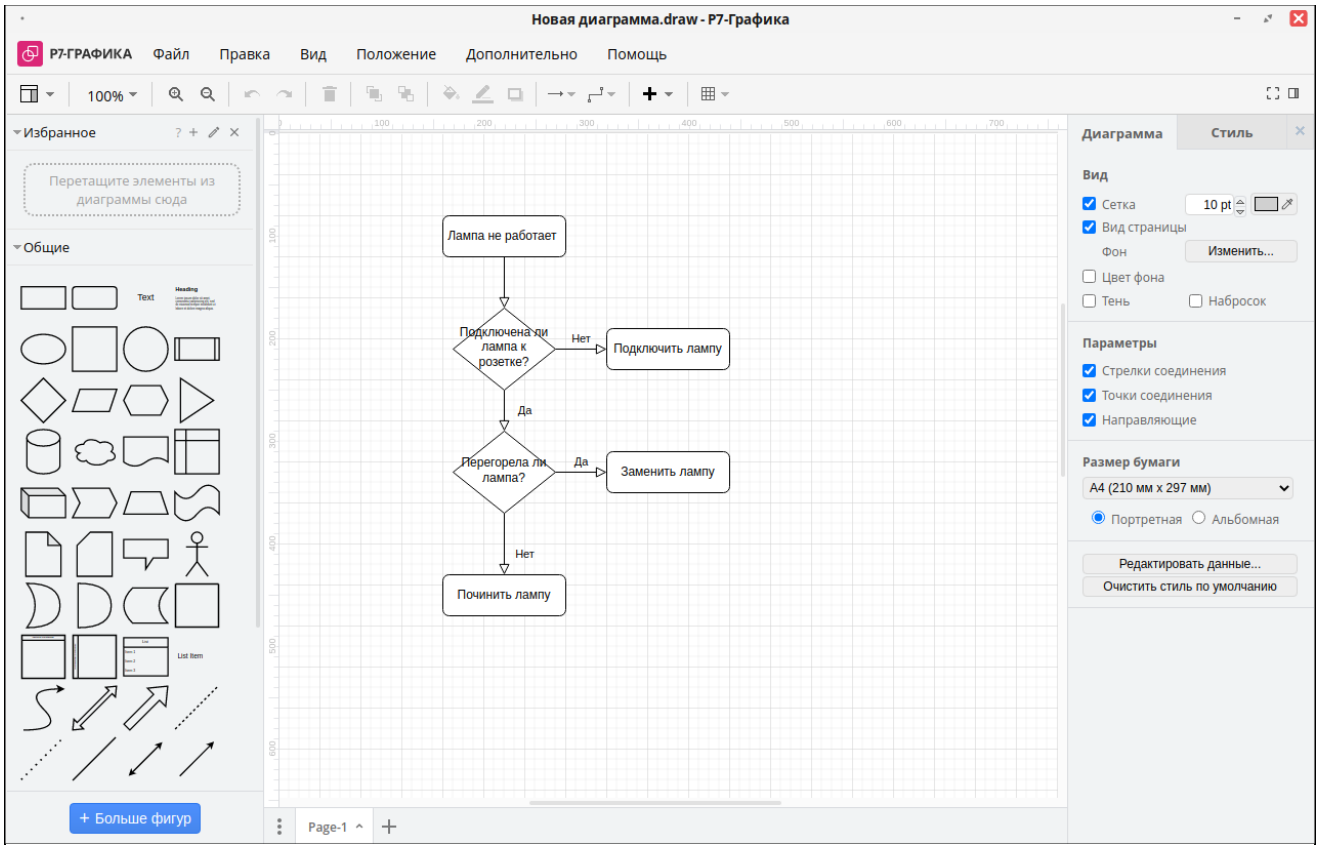
После установки репозитория в строке поиска необходимо ввести название пакета непосредственно самого редактора

диаграмм «**R7Grafika**». Затем отметьте флагом пакет последней версии и нажмите кнопку « **Применить**» для его установки.



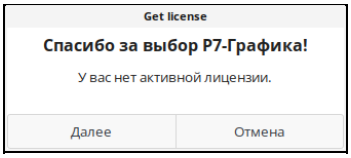
После установки редактор диаграмм будет доступен из «**Главного меню**» – «**Графика**» – «**Р7-Графика**».

Окно редактора диаграмм **Р7-Графика** выглядит следующим образом:

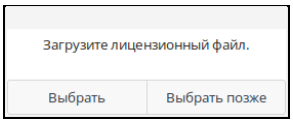


Активация лицензии

При первом запуске **Р7-Графики** будет выведено информационное сообщение об отсутствии активной лицензии. Лицензию необходимо запросить у официального разработчика. Нажмите **Далее**.



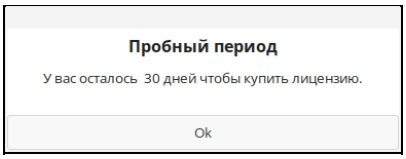
Для привязки имеющейся лицензии в следующем окне нажмите **Выбрать**.

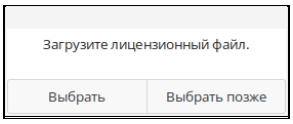


По нажатии **Выбрать позже** окно будет закрыто, и будет запущен непосредственно сам редактор диаграмм **Р7-Графика**.

Р7-Графика предоставляет 30-дневный бесплатный пробный период на рассмотрение и изучение функций редактора. По истечении бесплатного пробного периода необходимо загрузить соответствующую лицензию.

Возможность загрузки лицензии будет доступна при каждом последующем запуске **Р7-Графики** – будет появляться информационное окно с оставшимся количеством дней бесплатного периода, а затем окно для выбора лицензии.





Texmacs — программа для редактирования документов

Установка
Описание программы
Возможности программы

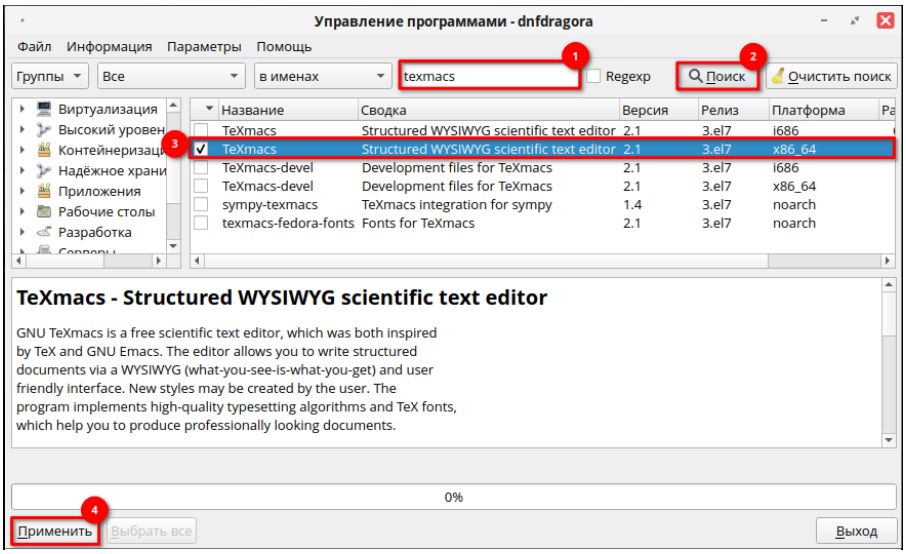
Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: TeXmacs-2.1

Texmacs — текстовый редактор с открытым исходным кодом, который предназначен для создания и редактирования технических документов с различными типами содержимого: текстом, математикой, графикой, интерактивным контентом, слайдами и т.д. Он поддерживает множество форматов, включая LaTeX, HTML, PDF и другие.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал. Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**texmacs**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install texmacs
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

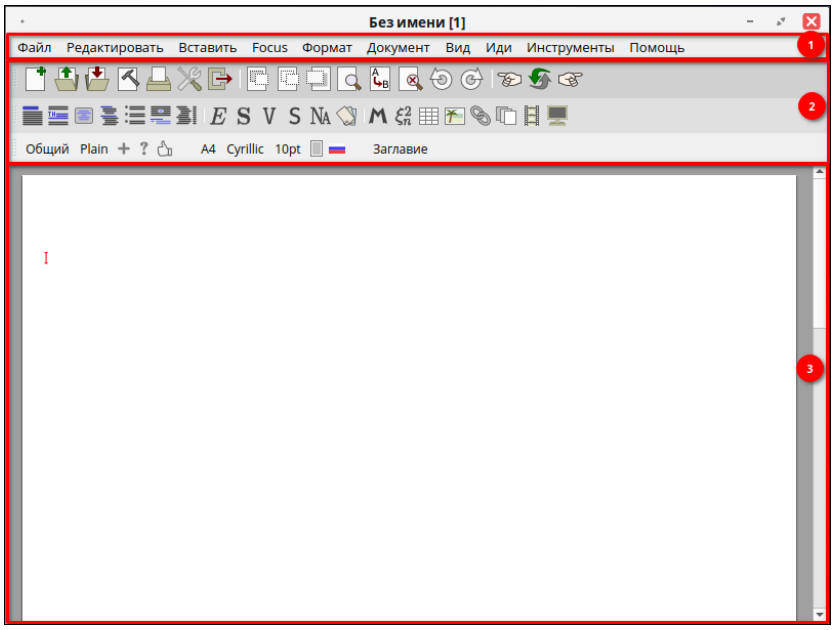
Для запуска программы через терминал введите команду:

```
texmacs
```

После установки программа будет доступна из «**Главного меню**» — «**Образование**» — «**GNU TeXmacs**».

Описание программы

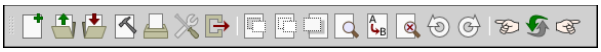
Интерфейс программы стандартный и состоит из нескольких типовых частей.



1 . **Основное меню программы** — здесь доступны основные возможности программы, такие как создание и редактирование документов, настройка параметров программы, панелей инструментов и другие.

2 . **Панели инструментов** предоставляют быстрый доступ к основным функциям программы. По умолчанию отображается *Главная панель инструментов*, *Панель инструментов режимов* и *Панель инструментов фокусировки*. Панели можно скрывать и отображать через основное меню.

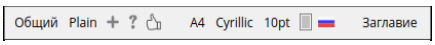
Главная панель инструментов предоставляет доступ к основным функциям программы, таким как создание, открытие, сохранение документов, а также другие часто используемые команды.



Панель инструментов режимов позволяет переключаться между различными режимами работы программы. Здесь можно выбрать, например, режим редактирования, просмотра или презентации.



Панель инструментов фокусировки содержит инструменты для управления вниманием пользователя, такие как инструменты увеличения или уменьшения масштаба, навигации по документу, а также инструменты для выделения и поиска.



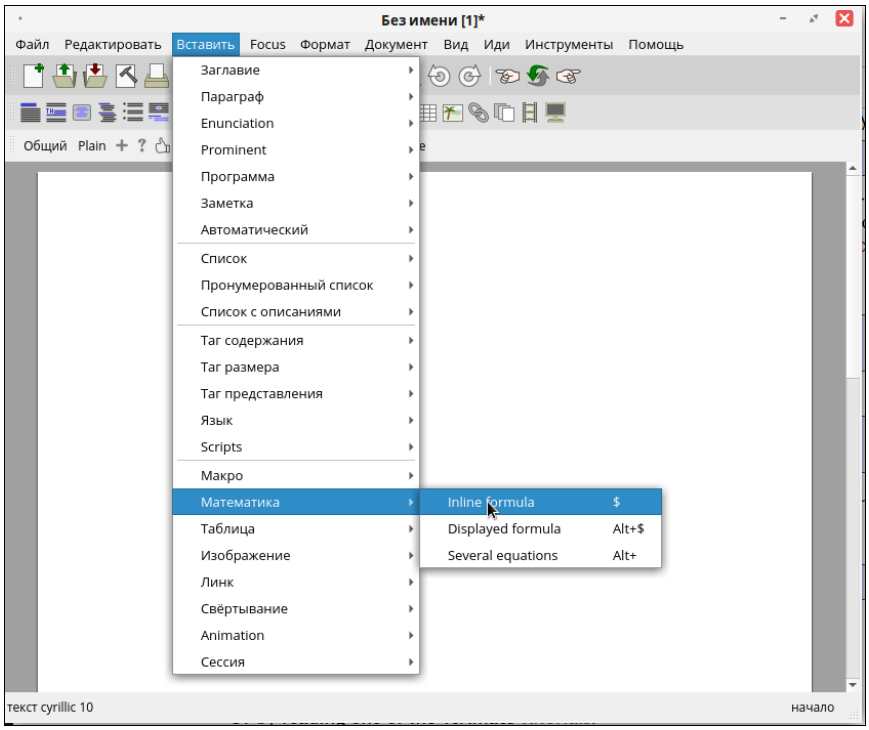
3. **Основное рабочее поле**. В данном поле происходит процесс создания, редактирования и форматирования документов.

Возможности программы

Основные возможности **Texmacs**:

1. Создание в документах формул, таблиц, изображений и других элементов.

Для вставки формулы в документ перейдите в меню «**Вставить**» — «**Математика**» (или щёлкните ЛКМ по значку  на панели инструментов), а затем выберите «**Inline formula**».

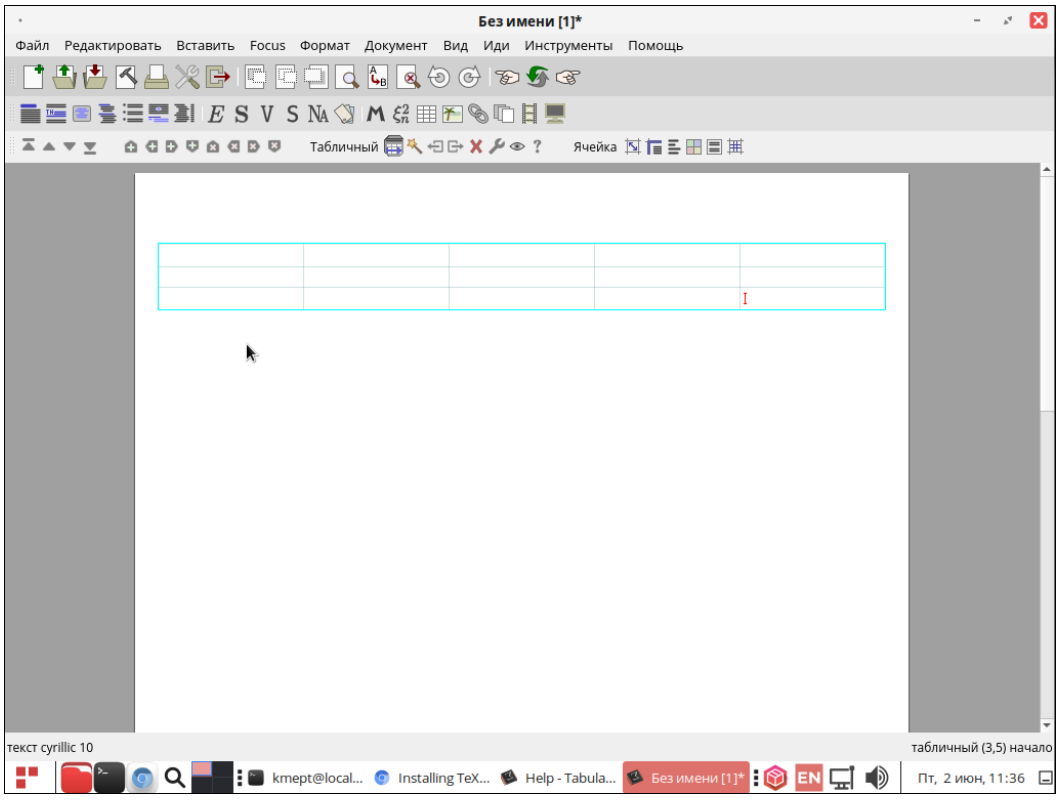


Для добавления математических формул на *Панели инструментов режимов* появляются дополнительные математические элементы. Введите нужное математическое выражение.

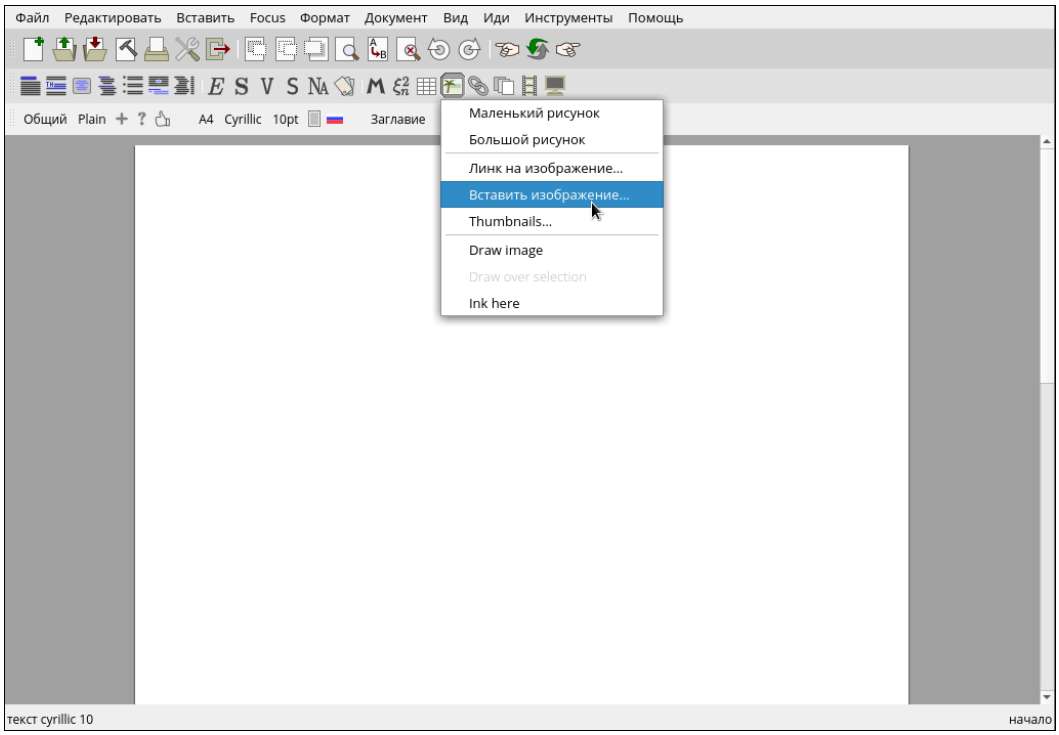


Для создания таблицы перейдите в пункт меню «**Вставить**» — «**Таблица**» (или щёлкните ЛКМ по значку  на панели инструментов), а затем выберите тип таблицы.

Появится *Панель для создания и редактирования таблиц*. При запуске новой таблицы её размер минимален, а ячейки пусты.

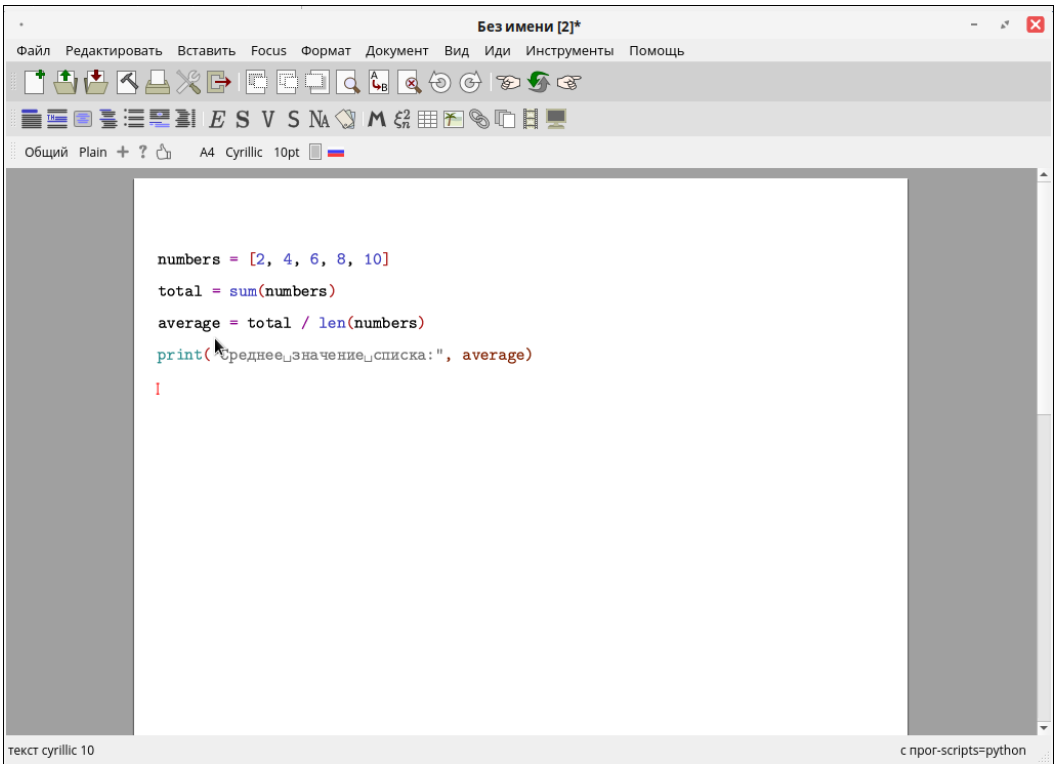


Для вставки изображения перейдите в пункт меню «**Вставить**» — «**Изображение**» — (или щёлкните ЛКМ по значку  на панели инструментов) и выберите «**Вставить изображение...**».



2. Поддержка многих языков программирования, включая Java, Python и C++.

Для создания кода на языке программирования Python перейдите в пункт меню «**Вставить**» — «**Программа**» — «**Inline code**» — «**Python**».



3. Интеграция с другими программами, например, Octave для выполнения математических вычислений.

Для установки программы **octave** через терминал выполните команду (потребуются права **администратора**):

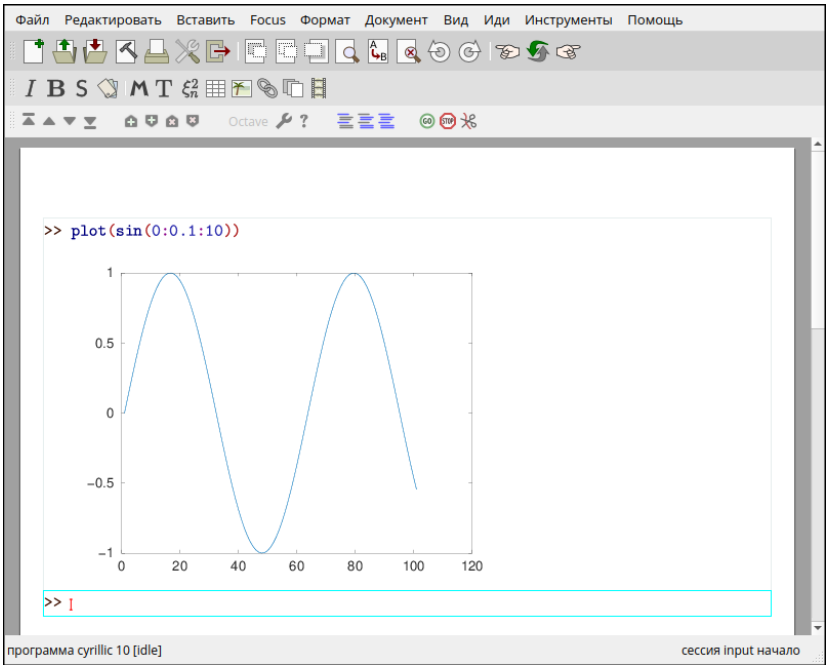
```
sudo dnf install octave
```

Для открытия **octave** перейдите в пункт меню «**Вставить**» — «**Сессия**» — «**Octave**». В открывшемся окне можно вводить команды и получать результаты в документе **TeXmacs**.

Например, введите следующую команду и нажмите **Enter**, чтобы построить график функции синуса:

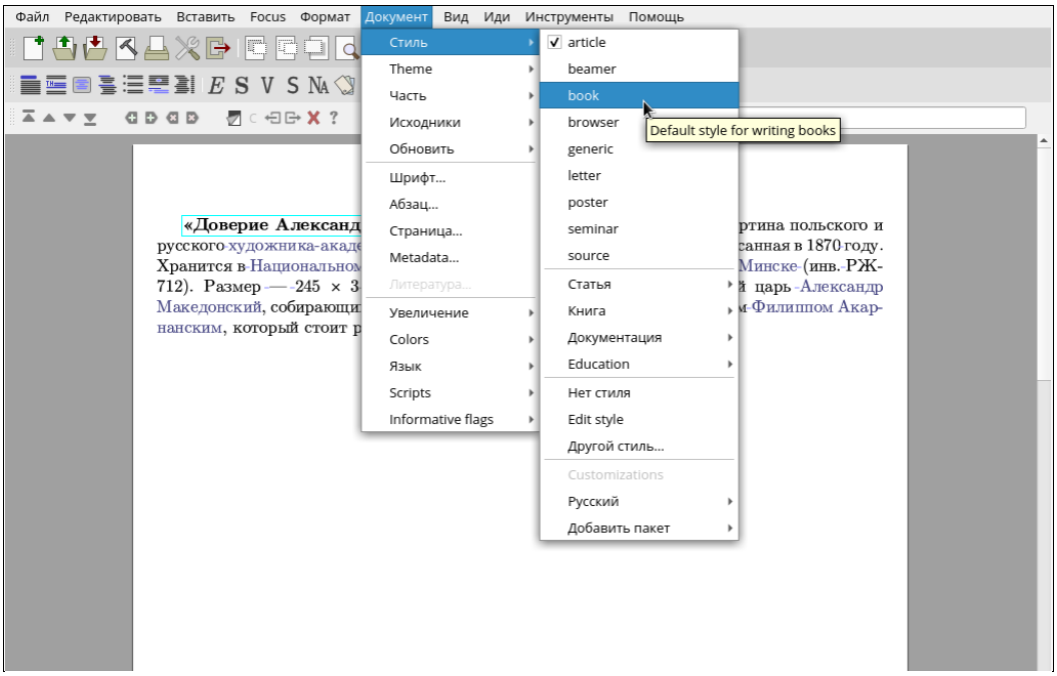
```
plot(sin(0:0.1:10))
```

Пример работы с **octave** внутри **texmacs**:



4. Автоматическое форматирование документов в соответствии с выбранным стилем.

Для форматирования документа перейдите в «**Документ**» — «**Стиль**» и выберите необходимый стиль.



5. Визуализатор графов.

Для создания графа предварительно необходимо установить пакет **texlive-standalone**, который предназначен для создания отдельных графиков и других элементов, которые можно вставлять в документ.

Для этого в терминале выполните команду (потребуются права **администратора**):

```
sudo dnf install texlive-standalone
```

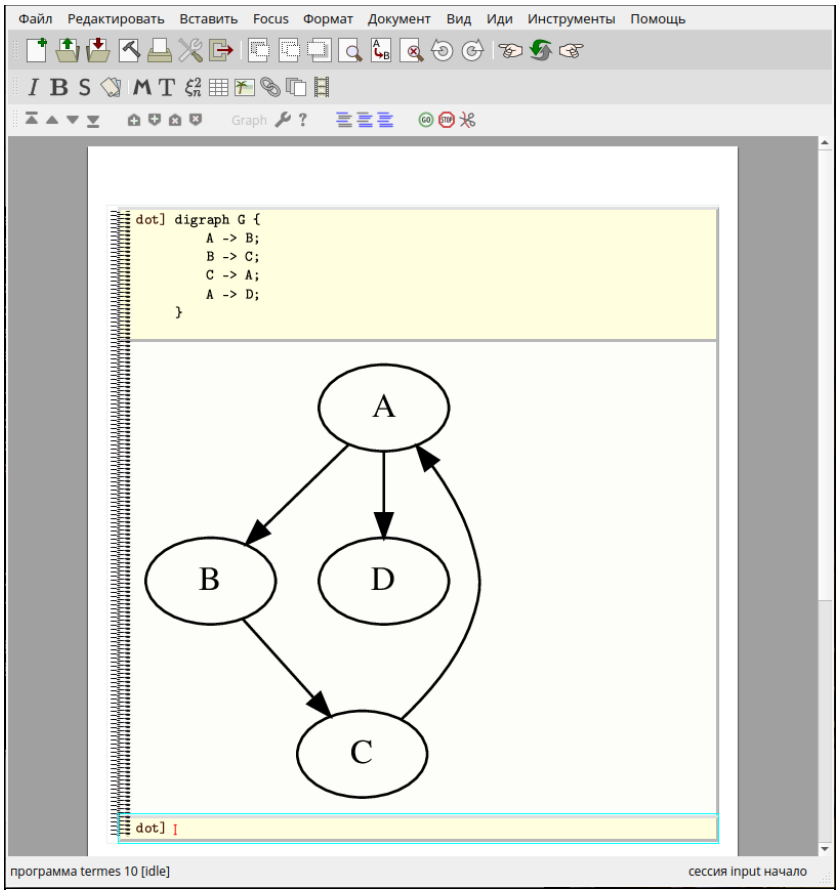
Для создания графа перейдите в меню «**Вставить**» — «**Сессия**» — «**Graph**».

Введите команду и нажмите Enter:

```
digraph G {
 A -> B;
 B -> C;
 C -> A;
 A -> D;
```

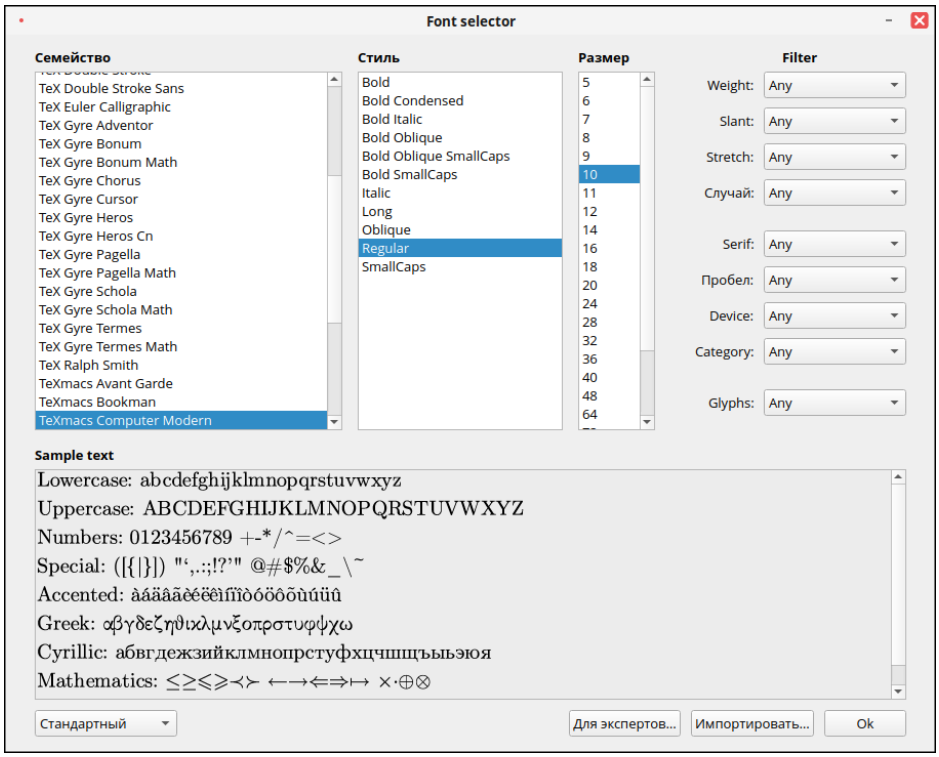
```
}
```

Этот код создаст простой ориентированный граф с вершинами A, B, C, D и рёбрами между ними. Можно изменять и дополнять этот код для создания более сложных графов.



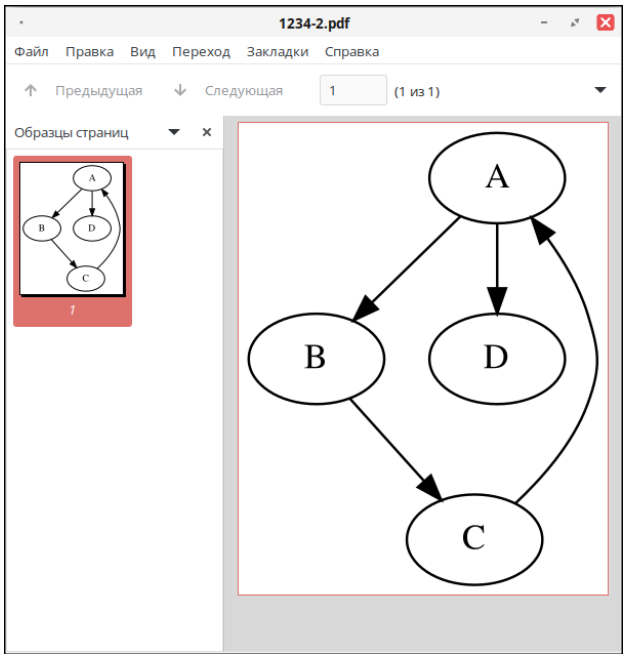
6. Поддержка встроенных шрифтов и возможность добавления новых шрифтов.

Для открытия Меню шрифтов выберите пункт меню «**Формат**» — «**Шрифт...**».



7. Возможность экспорта документов в различные форматы, включая PDF, HTML и LaTeX.

Для экспорта документа в формате PDF перейдите в меню «**Файл**» — «**Экспортировать**» — «**Pdf..**». Укажите имя файла и место для сохранения, затем нажмите «**Сохранить**».


1234-2.pdf
Файл Правка Вид Переход Закладки Справка
Предыдущая Следующая 1 (1 из 1)
Образцы страниц
A
B
D
C
1

Файловый менеджер Double Commander

Установка
Описание программы
Избранные каталоги
Файлы
Поиск
Вкладки
Настройка параметров

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** doublecmd-gtk-1.0.3-3, doublecmd-qt-1.0.3-3

Double Commander - двухпанельный кроссплатформенный файловый менеджер с открытым исходным кодом. Аналогичен по функциональности **Total Commander** и совместим с его плагинами.

Double Commander работает под *ОС Windows*, *macOS*, *FreeBSD*, а также *GNU/Linux* с графическими интерфейсами **GTK** и **Qt**, выбор между которыми нужно производить в зависимости от используемой графической оболочки.

GTK используется в таких DE, как *Cinnamon*, *GNOME*, *LXDE*, *MATE* или *Xfce*.

Qt используется в таких DE, как *KDE* или *LXQt*. Однако данные требования не обязательны, т.к. в РЕД ОС оба интерфейса успешно работают на каждой из DE.

Установка

В РЕД ОС *Double Commander* установлен по умолчанию и доступен из «**Главного меню**» - «**Стандартные**» - «**Double Commander**».

Если по какой-либо причине *Double Commander* отсутствует в системе, программу можно установить из репозитория. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

Для использования программы **с интерфейсом GTK** выполните команду:

```
dnf install doublecmd-gtk
```

Для использования программы **с интерфейсом Qt5** выполните команду:

```
dnf install doublecmd-qt
```

Дальнейшая работа в программе производится с **правами локального пользователя**.

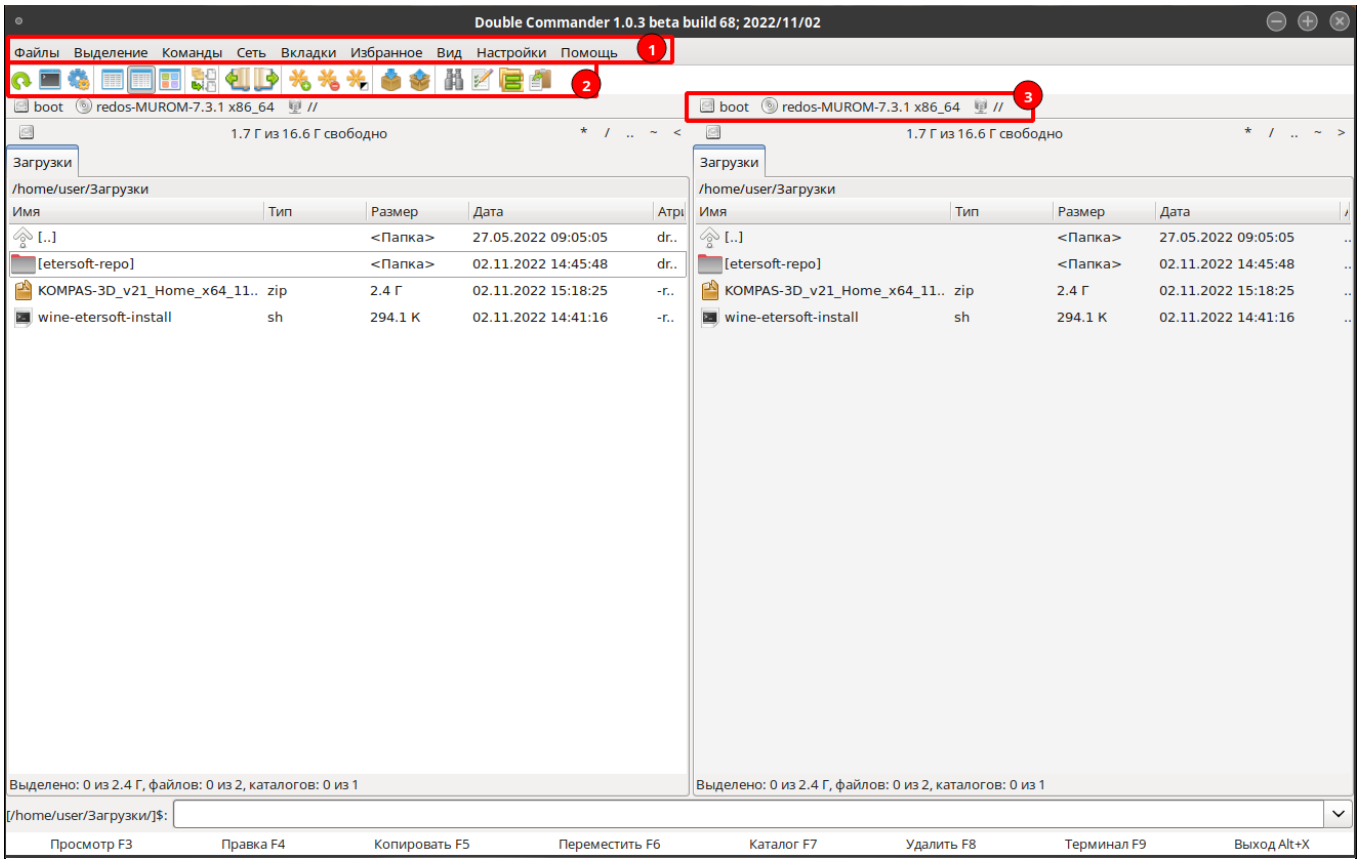
Описание программы

Основные характеристики *Double Commander*:

- встроенный редактор с подсветкой синтаксиса (**F4**);
- встроенный просмотрщик файлов (**F3**) для просмотра файлов любых размеров в шестнадцатеричном, двоичном или текстовом формате;
- работа с архивами так же, как с подкаталогами. Доступно копирование файлов в архив и из него. Поддерживаются следующие типы архивов: *ZIP*, *TAR*, *GZ*, *BZ2*, *XZ*, *LZMA*, *7Z*, а также *RPM*, *CPIO*, *DEB*, *RAR*, *ZIPX*;
- поддержка Unicode;
- поддержка консольных архиваторов, аналогично плагину **MultiArc** для *Total Commander*, со схожим форматом файла настроек;
- поддержка вкладок файловых панелей;
- настраиваемые колонки;
- инструмент синхронизации каталогов;

- инструмент группового переименования;
- протоколирование файловых операций;
- настраиваемая панель инструментов с кнопками для запуска внешних программ или внутренних команд меню;
- поддержка *WCX*, *WDX*, *WFX* и *WLX* плагинов от *Total Commander*.

Окно программы выглядит следующим образом:



Главное меню (1) включает в себя следующие пункты:

- Файлы;
- Выделение;
- Команды;
- Сеть;
- Вкладки;
- Избранное;
- Вид;
- Настройки;
- Помощь.

Панель инструментов (2) с функциональными кнопками для быстрой и удобной работы с содержимым и настройками самой программы.

Кнопки **быстрого перехода** к разделам (3).

Функциональные кнопки на *Панели инструментов* представлены следующими действиями:

- «**Обновить**»  ;
- «**Запуск терминала**»  ;
- «**Параметры**»  ;
- «**Поиск**»  .

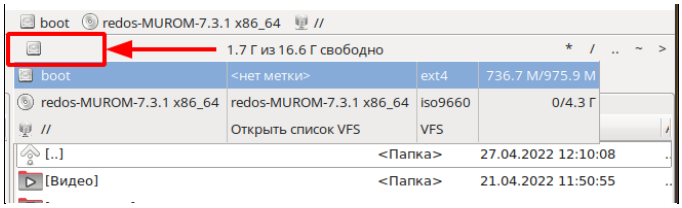
В неё также входят группы кнопок **способа отображения файлов** в панелях  , **выделения** и **снятия выделения** файлов  , кнопки «**Упаковать**» / «**Распаковать**»  и некоторые другие.

Добавлять и удалять необходимые функциональные кнопки можно через пункт меню «**Настройки**» - «**Параметры**» - «**Панель инструментов**».

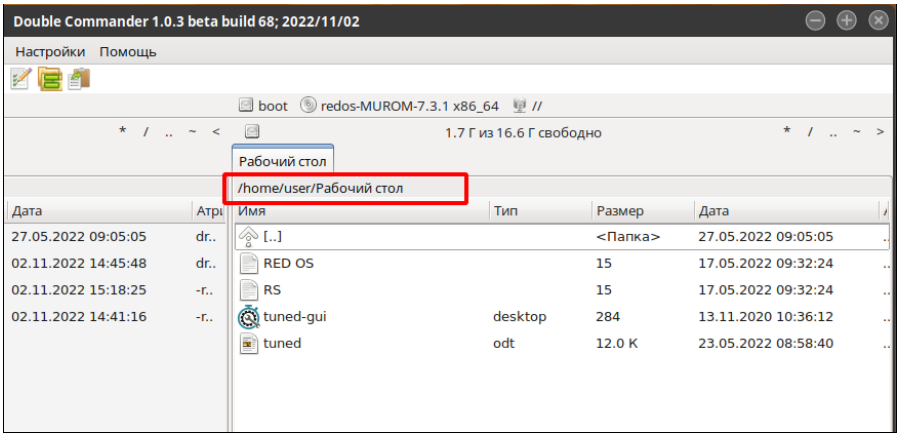
Над файловыми панелями доступны следующие действия с каталогами:

- список разделов (представлен на рисунке ниже);
- переход в корень файловой системы («/»);
- переход в домашний каталог («~»);
- управление избранными каталогами («*»);
- переход на уровень выше («..»);
- дублирование панелей («>» и «<»).

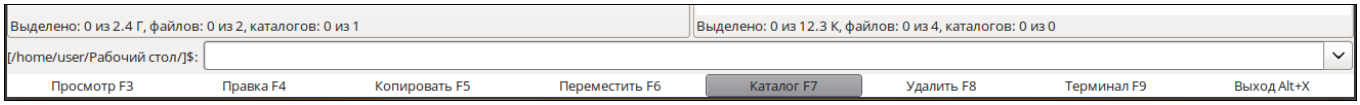
Кнопка списка разделов по функции аналогична кнопкам быстрого перехода (**3**).



Ниже располагается строка-заголовок с полным адресом текущего каталога. Данная строка также выполняет роль быстрых ссылок: с её помощью можно простым кликом перейти в любой из родительских каталогов.



Внизу окна *Double Commander* расположена «**Командная строка**», используемая для ввода команд вручную, а также панель функциональных клавиш «**F3**» - «**F9**» и «**Выход Alt+X**».



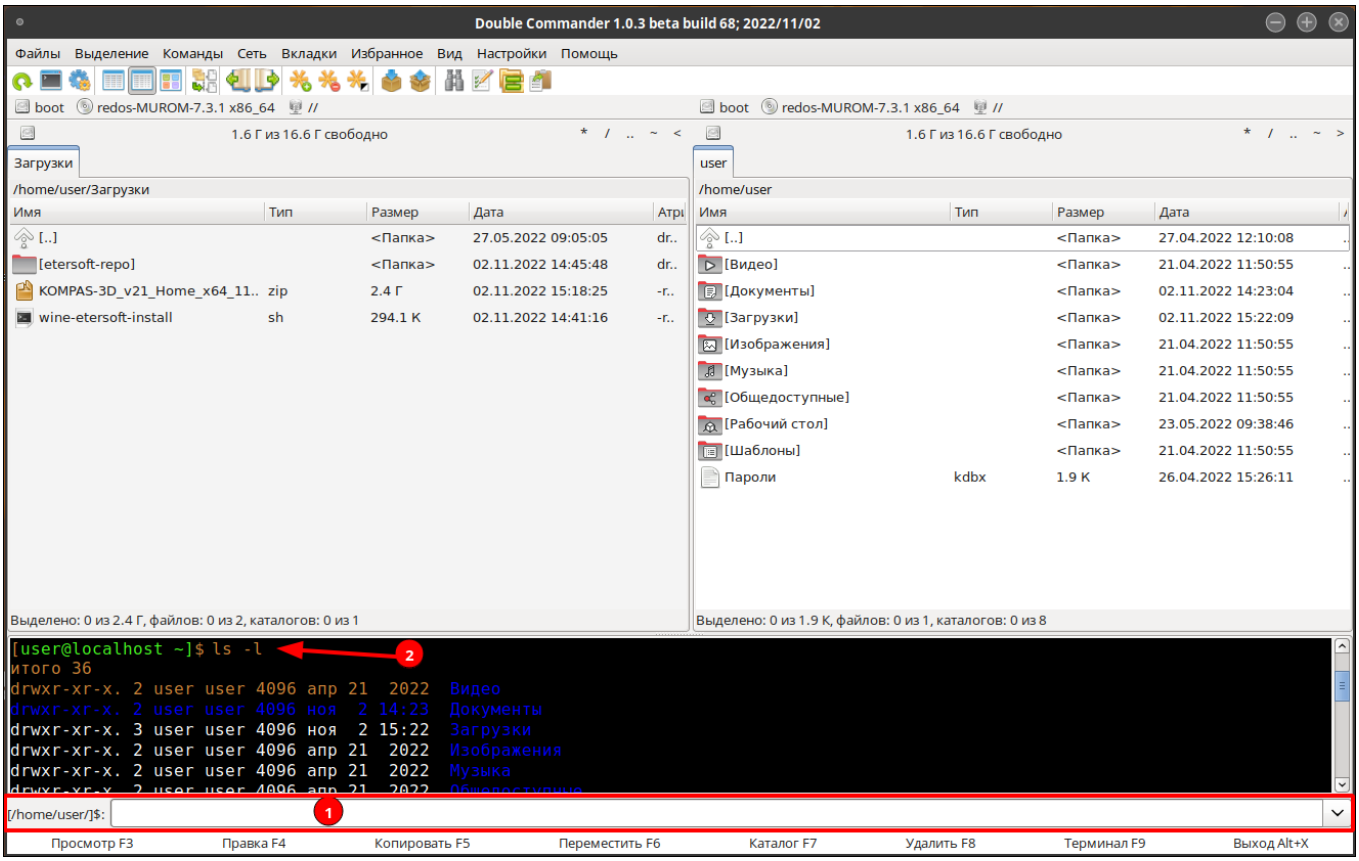
Для отображения результатов выполнения набранных команд из «**Командной строки**», а также действий в файловых панелях, во встроенном окне терминала *Double Commander* необходимо выставить флаг в чекбоксе «**Окно терминала**» в пункте меню «**Настройки**» - «**Параметры**» - «**Вид окна**».

По умолчанию используется **xterm**, но в системе он не установлен по умолчанию. Для установки выполните команду в терминале (с правами пользователя **root**):

```
dnf install xterm
```

Изменить терминал, используемый по умолчанию, можно в пункте меню «**Настройки**» - «**Параметры**» - «**Инструменты**» - «**Терминал**» в полях «**Команда**». Например, на **mate-terminal**, используемый в окружении *Mate*, или **gnome-terminal**, используемый в *Cinnamon*.

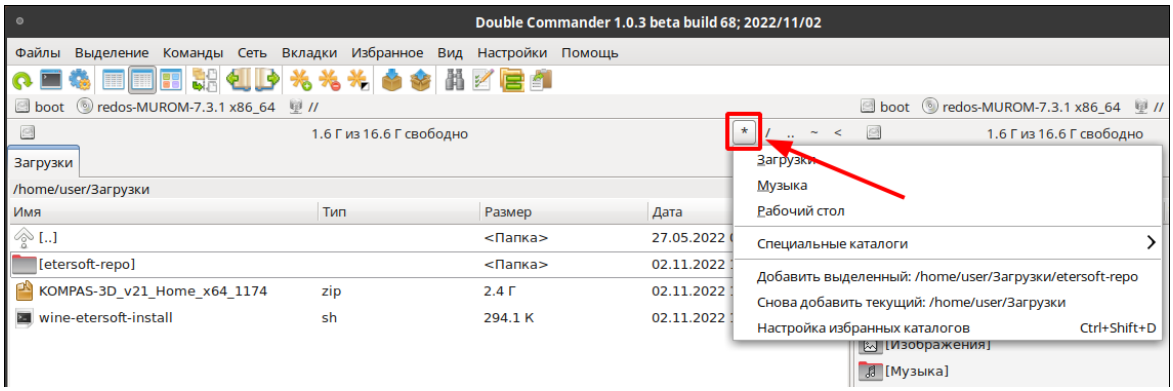
Для передачи команды в терминал выполните ее в текстовом поле (**1**), результат выполнения набранной команды будет отображен в поле терминала (**2**). Команды выполняются в активной файловой панели.



Избранные каталоги

Избранные каталоги («*» или «**Ctrl+D**») - это список каталогов и инструменты его изменения для формирования требуемого перечня быстрого доступа. Данный функционал также доступен из пункта меню «**Команды**» - «**Избранные каталоги**».

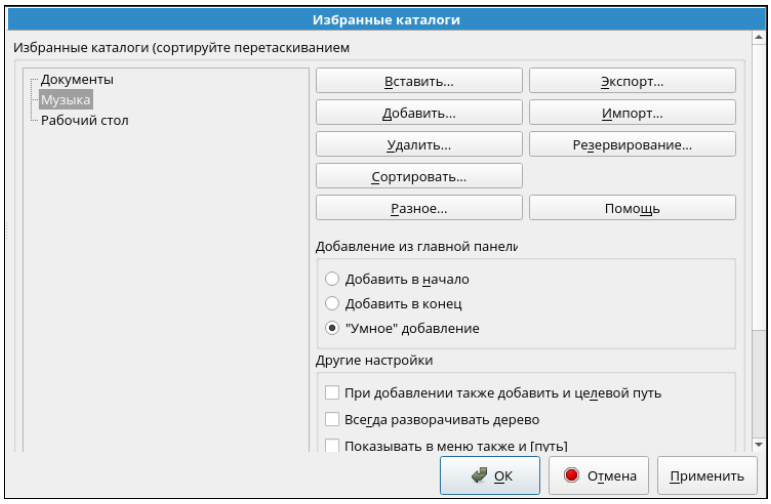
При активации нажатием на кнопку (*) или вызовом сочетания клавиш (**Ctrl+D**) появляется контекстное меню.



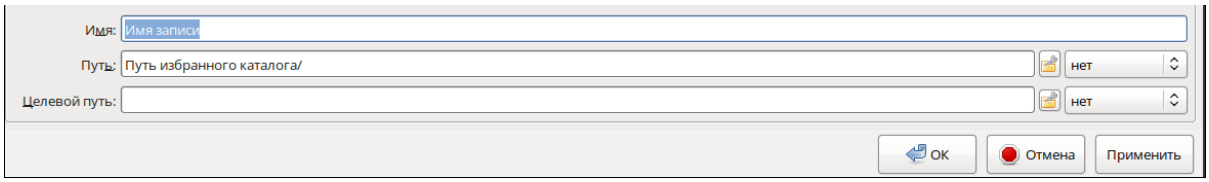
В списке будут отображены добавленные каталоги, ниже представлены пункты добавления текущего или выделенного каталога в перечень. Для того чтобы добавить нужный каталог в избранные, необходимо выделить его курсором мыши и выбрать функцию «**Избранные каталоги**» одним из перечисленных выше способов.

Редактирование разделов доступно через это же контекстное меню в пункте «**Настройка избранных каталогов**». Там можно добавить, удалить, экспортировать, импортировать, создать резервную копию и восстановить из резервной копии нужные каталоги.

Окно настройки избранных каталогов представлено на рисунке ниже.



Добавить избранный каталог можно вручную, указав имя и путь в полях нижней панели текущего окна.



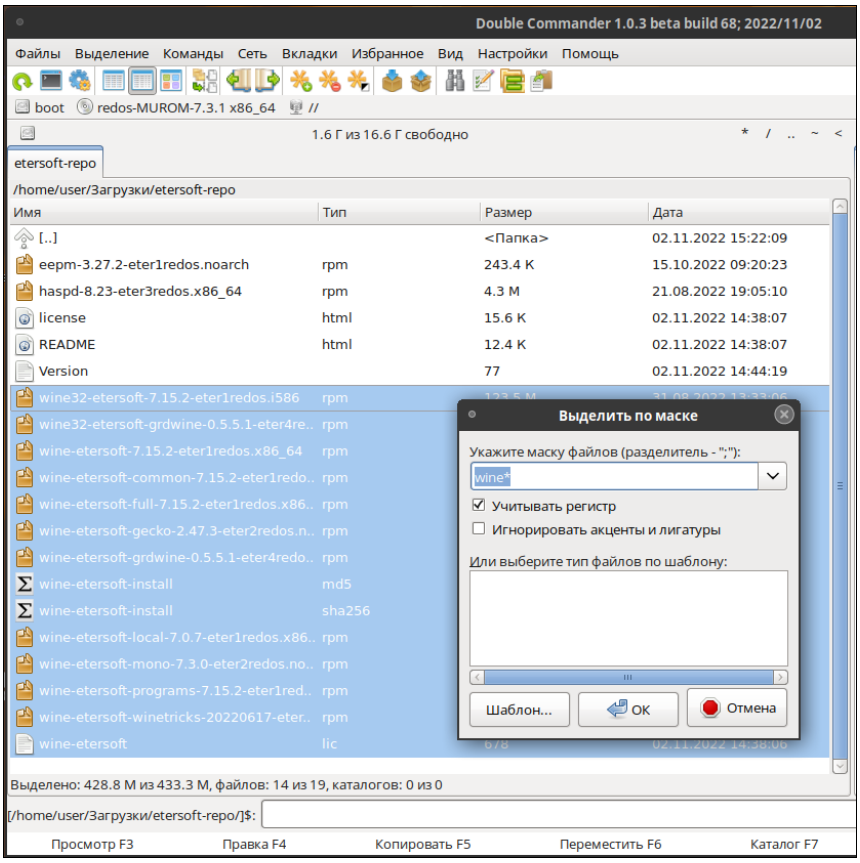
Файлы

Пункт меню «**Файлы**» *Double Commander* позволяет:

- создавать символьные или жесткие ссылки на файлы;
- изменять атрибуты файлов;
- создавать каталоги;
- распаковывать / упаковывать файлы и каталоги;
- разрезать файлы или объединять их;
- подсчитывать и проверять контрольные суммы;
- сравнивать файлы по содержимому;
- применять групповое переименование.

Инструмент группового переименования позволяет присвоить нескольким файлам разные наименования с одной маской (например: picture 1 , picture 2, picture 3 и т.д.).

В пункте меню «**Выделение**» можно быстро выделить файлы или папки, сгруппировав файлы по расширению или выделив группу.



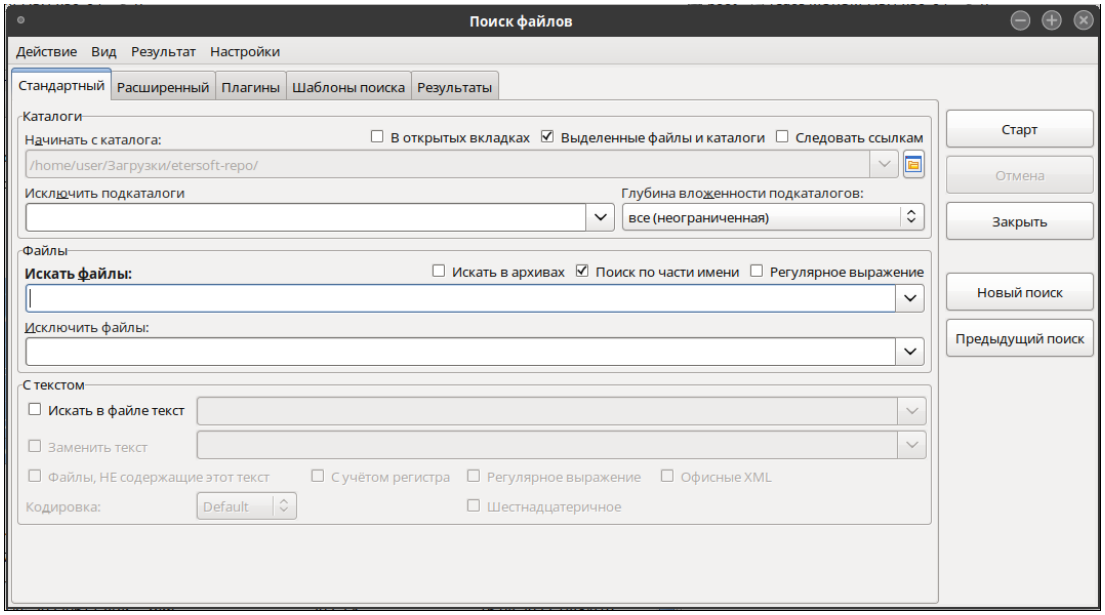
Пункт «**Сохранить выделение**» - сохраняет выделенный список в буфер обмена.

Пункт «**Восстановить выделение**» - восстанавливает ранее сохраненный выделенный список из буфера обмена.

Double Commander даёт возможность сохранить наименования выделенных файлов в текстовый документ, с возможностью сохранения как полных имен с абсолютным путём к файлам, так и сокращенных.

Поиск

Широкие возможности поиска в *Double Commander* представлены в виде отдельно открывающегося окна с вкладками. Поиск доступен из пункта меню «**Команды**» - «**Поиск...**».



Параметры места поиска:

- «**В открытых вкладках**» - поиск будет осуществляться в открытых вкладках;
- «**Выбранные файлы и каталоги**» - поиск ведётся только среди выделенных файлов или каталогов активной панели;
- «**Следовать ссылкам**» - если будет найдена символьная ссылка на каталог, то целевой каталог будет прочитан и использован,

иначе эта символьная ссылка будет считаться обычным файлом.

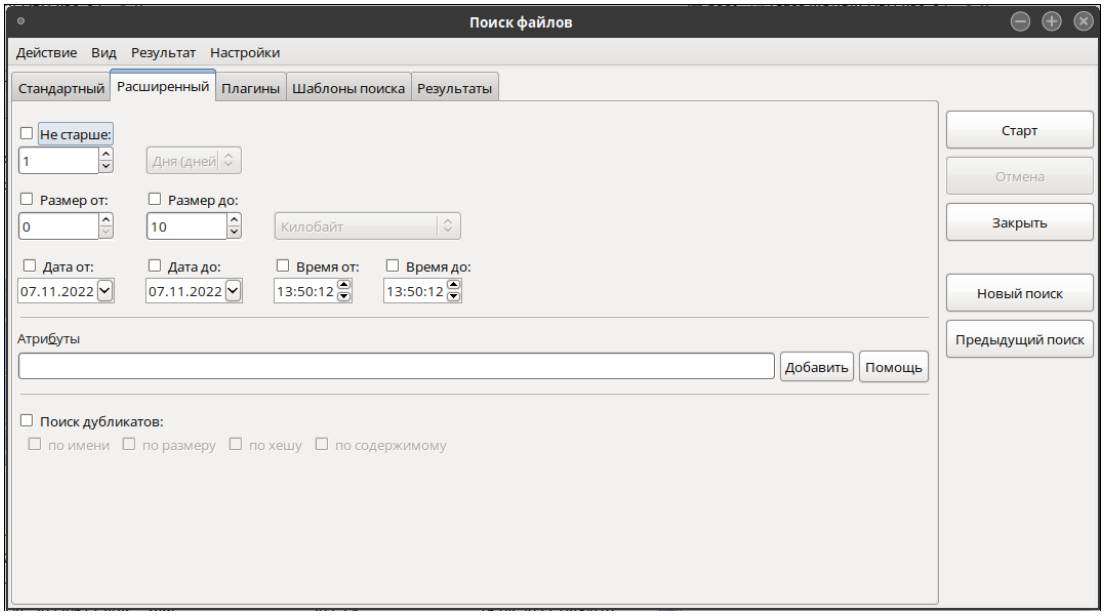
По умолчанию в строке «**Начинать с каталога**» используется текущий каталог активной панели. Также вы можете исключить подкаталоги и указать глубину вложенности.

В строке «**Искать файлы**» задаётся маска, по которой будет произведён поиск.

Дополнительные параметры этого поиска: «**Искать в архивах**», «**Поиск по части имени**», «**Регулярное выражение**», строка «**Исключить файлы**».

Если отметить «**Искать в файле текст**», то во время поиска будет происходить просмотр содержимого файлов, а в результат попадут только файлы, содержащие запрашиваемый текст.

Вкладка «**Расширенный**» позволяет указать дополнительные условия поиска файла: дату, время и возраст файла (по дате модификации), минимальный и максимальный размер файла, а также атрибуты.



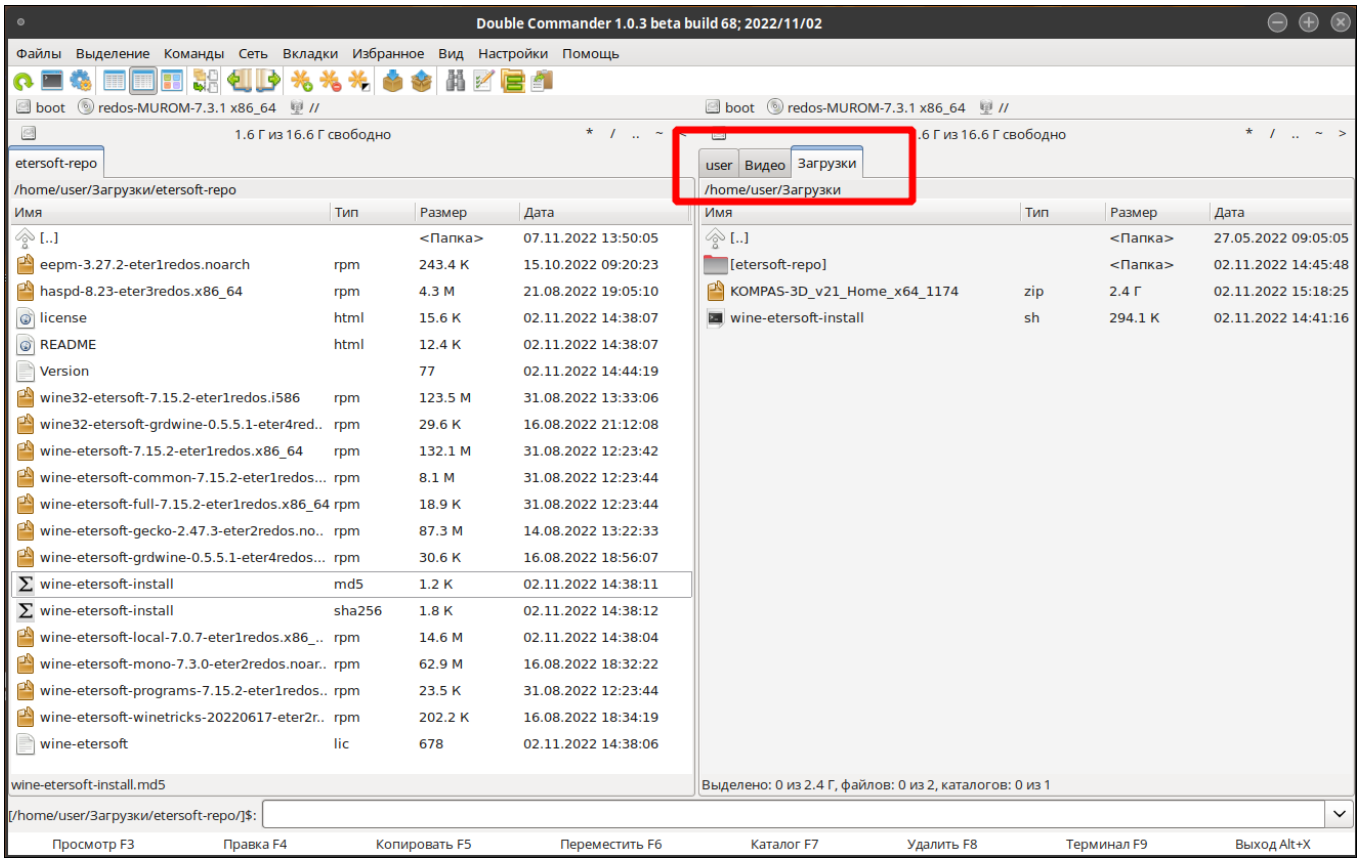
Вкладка «**Плагины**» задаёт поиск с помощью информационных (контентных, *WDX*) или поисковых (*DSX*) плагинов.

Вкладка «**Шаблоны поиска**» сохраняет параметры поиска для повторного использования.

Вкладки

Меню «**Вкладки**» предназначено для создания дополнительных вкладок в панелях и управления ими: создать вкладки, загрузить из файла, переименовать. Во вложенном разделе «**Опции вкладки**» изменяются состояния вкладок.

Вкладку можно создать с помощью сочетания клавиш «**Ctrl+T**» или через пункт меню «**Вкладки**».



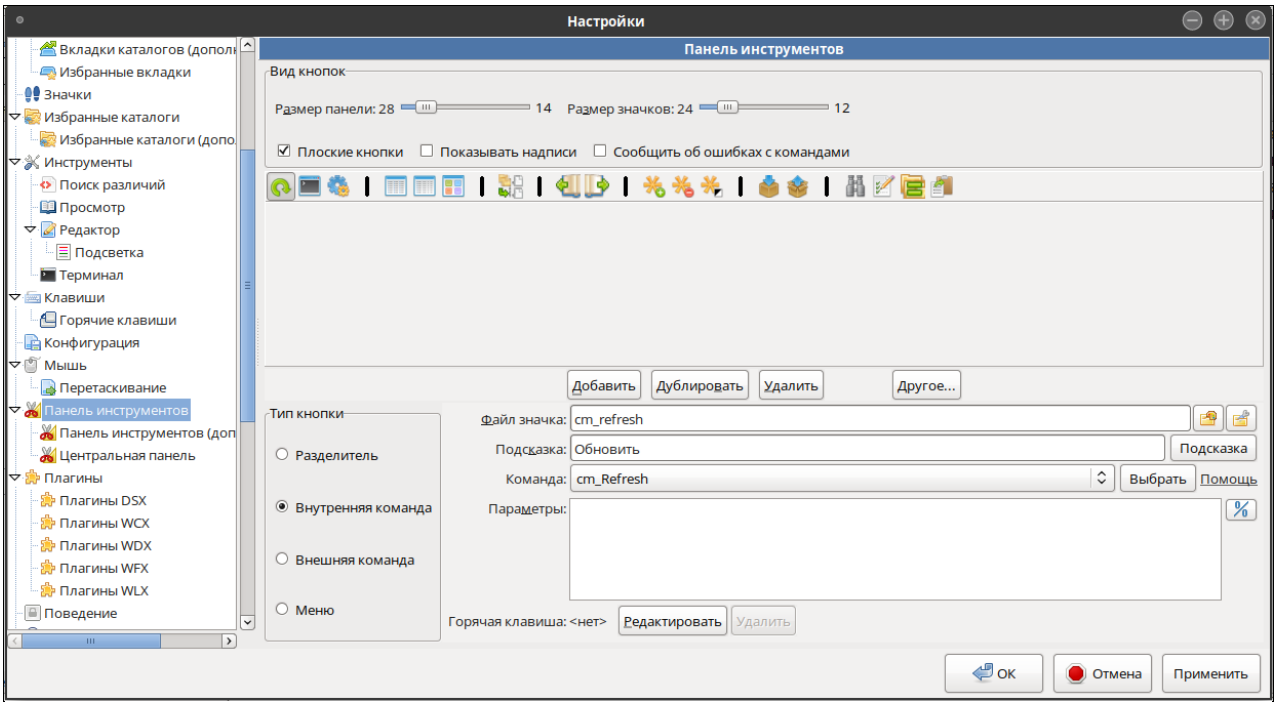
Подменю «**Опции вкладки**» позволяет назначить вкладку обычной или заблокированной, причём у заблокированной может быть несколько статусов:

- «**Заблокировать вкладку**» - блокирует смену каталога вкладки и предлагает при этом открыть этот же каталог в новой вкладке;
- «**Заблокировать с возможностью смены каталога**» - в этом случае можно сменить каталог, однако, если переключиться на другую вкладку, а потом обратно, в ней будет открыт каталог, с которым она была заблокирована;
- «**Заблокировать и открывать каталоги в новых вкладках**» - при попытке войти в любой другой каталог в панели, он откроется в новой вкладке.

Заблокированные вкладки помечаются значком «*».

Настройка параметров

Диалоговое окно, доступное через пункт меню «**Настройки**» - «**Параметры**», позволяет устанавливать и выбирать нужные пользователю параметры программы, такие как «**Вид окна**», «**Панель инструментов**», «**Шрифты**» и пр.


Настройки
Вкладки каталогов (дополн
Избранные вкладки
Значки
Избранные каталоги
Избранные каталоги (допо
Инструменты
Поиск различий
Просмотр
Редактор
Подсветка
Терминал
Клавиши
Горячие клавиши
Конфигурация
Мышь
Перетаскивание
Панель инструментов
Панель инструментов (доп
Центральная панель
Плагины
Плагины DSX
Плагины WCX
Плагины WDX
Плагины WFX
Плагины WLX
Поведение
Панель инструментов
Вид кнопок
Размер панели: 28
14
Размер значков: 24
12
Плоские кнопки
Показывать надписи
Сообщить об ошибках с командами
Добавить
Дублировать
Удалить
Другое...
Тип кнопки
Разделитель
Внутренняя команда
Внешняя команда
Меню
Файл значка:
cm_refresh
Подсказка:
Обновить
Подсказка
Команда:
cm_Refresh
Выбрать
Помощь
Параметры:
Горячая клавиша: <нет>
Редактировать
Удалить
OK
Отмена
Применить

Файловый менеджер Midnight Commander

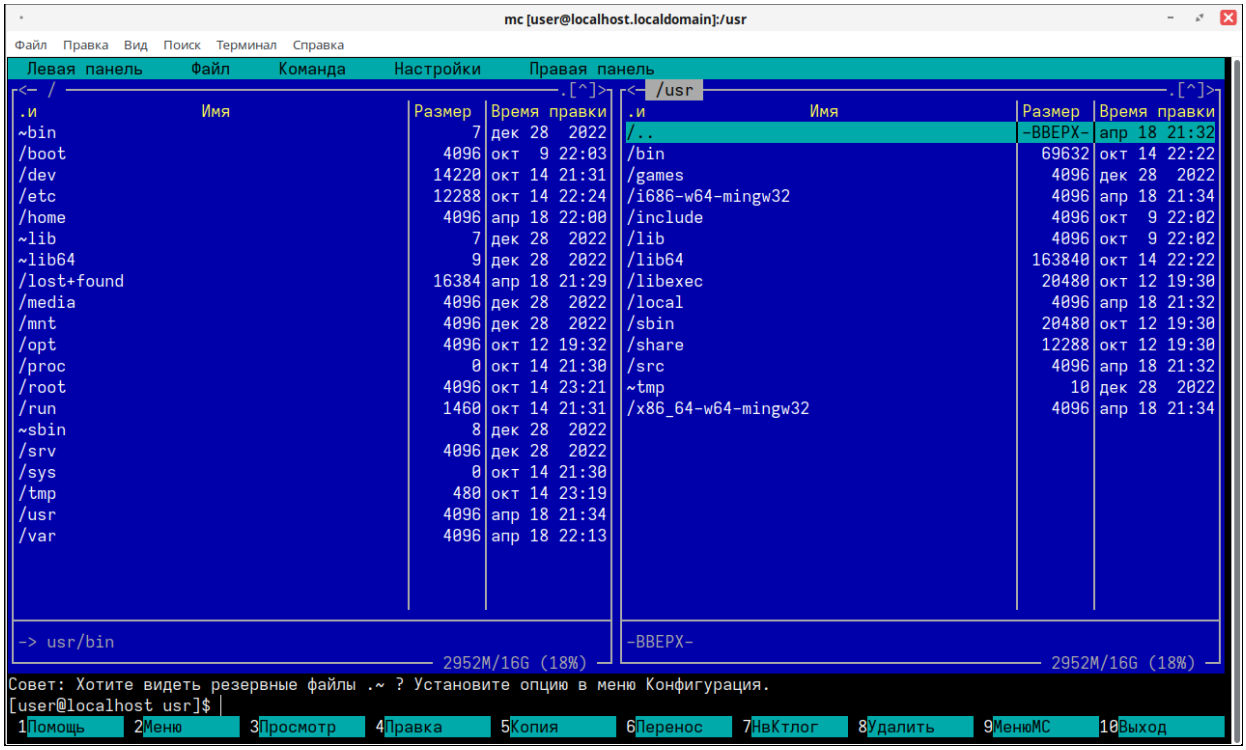
Midnight Commander (mc, MC) – текстовая полнофункциональная программа, которая позволяет пользователю копировать, перемещать и удалять файлы и директории, производить поиск файлов и запускать на выполнение команды оболочки. Также в него встроен редактор и программа для просмотра файлов.

Вы можете подробнее ознакомиться с работой файлового менеджера **MC**, просмотрев наши обучающие видео:

- на **RuTube** — Файловые менеджеры в РЕД ОС;
- в **Яндекс.Дзен** — Файловые менеджеры в РЕД ОС;
- в **VK Видео** — Файловые менеджеры в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Экран **MC** делится на несколько частей. Самая верхняя строка - строка основного меню программы. Она может быть не видна, но при нажатии клавиши *F9* или при щелчке мыши эта строка отображается в верхней части экрана. В центральной части расположены левая и правая панели. Внизу находится строка подсказки и полезных советов. Вторая строка снизу является командной, а в самой нижней части отображается строка с назначением функциональных клавиш.



Файловый менеджер Midnight Commander

MC позволяет одновременно наблюдать содержимое двух каталогов. Одна из панелей является текущей (в этой панели находится выделитель). Практически все команды оперируют над текущей панелью. Хотя некоторые файловые операции, такие как «**Переименовать**» или «**Копировать**», по умолчанию используют каталог неактивной панели в качестве каталога назначения (при выполнении подобных команд всегда появляется запрос на подтверждение).

Поддержка мыши

MC поддерживает управление мышью. При щелчке левой кнопкой мыши на файле, этот файл становится текущим. При щелчке правой кнопкой, файл помечается (или пометка снимается, в зависимости от предыдущего состояния).

При двойном щелчке на файле, будет произведена попытка его запуска, если это запускаемый файл. Если расширение файла связано с какой-либо программой, то эта программа будет запущена.

Также можно выполнять команды, связанные с метками функциональных клавиш, щелкнув мышью на них.

При щелчке мышью на верхней границе панели, список файлов прокрутится на одну страницу назад. Соответственно, щелчок на нижней границе приведёт к прокрутке на страницу вперёд. Этот метод также работает с просмотром помощи и деревом каталогов.

По умолчанию значение параметра автоповтора для клавиш мыши равно 400 миллисекундам. Это значение может быть изменено путём редактирования в файле **.mc.ini** параметра **mouse_repeat_rate**.

Если **MC** сконфигурирован с поддержкой мыши, то вы можете вырезать и склеивать фрагменты текста, используя клавишу *Shift*.

Меню

Строка меню появляется при нажатии *F9* или при щелчке мышью в верхней строке экрана. Строка меню состоит из пяти подменю: «Левая панель», «Файл», «Команда», «Настройки» и «Правая панель».

Меню *Левая панель* и *Правая панель* позволяют оперировать панелями.

В меню *Файл* предлагается список команд, которые могут быть применены к текущему файлу или к любым помеченным файлам.

В меню *Команда* содержатся более общие команды, которые никак не связаны с текущим файлом или помеченной группой файлов.

Меню *Настройки* позволяет устанавливать различные настройки для работы в MC.

Горячие комбинации клавиш Midnight Commander

В данном разделе речь пойдет о горячих клавишах для файлового менеджера Midnight Commander, знание которых позволяет повысить удобство и скорость работы.

Работа с файлами

Сочетание	Действие
F3	Просмотреть файл
F4	Редактировать файл
Shift+F4	Создать новый файл
+	Вызвать окно для выделения группы
\	Снять отметку с группы

Работа с командной строкой

Сочетание	Действие
Alt+Enter	Вставить файл или каталог, на котором установлен курсор, в командную строку
Alt+p	Вернуть предыдущую выполненную команду в командную строку
Ctrl + x,t	Вставка всех выделенных объектов в командную строку
Ctrl + x, Ctrl + p	Вставить в командную строку полный путь, установленный на неактивной панели
Alt+t	Смена режима отображения панели
Alt+.	Скрыть или показать скрытые файлы и каталоги, которые начинаются на точку
Alt+a	Вставить в командную строку полный путь, установленный на активной панели
Alt+c	Смена текущего каталога
Alt+h	Просмотр последних выполненных команд
Alt+i	Смена каталога на неактивной панели на каталог, в котором находится пользователь
Alt+o	Неактивная панель переходит в каталог, на который указывает активная панель
Ctrl+x, q	Просмотр содержимого файла на второй панели
Ctrl+x,i	Просмотр информации о текущем объекте на второй панели
Ctrl+o	Скрыть или показать панели
Ctrl+r	Перечитать содержимое каталога
Ctrl+Space	Показать размер текущего каталога

Работа с поиском

Сочетание	Действие
Alt+Shift+?	Расширенный поиск
Ctrl+s	Поиск файла или каталога

Работа с правками

Сочетание	Действие
Ctrl+x,o	Просмотр или изменения владельца, группы
Ctrl+x,c	Просмотр или изменение прав доступа

Работа со ссылками

Сочетание	Действие
Ctrl+x,l	Создать жесткую ссылку
Ctrl+x,s	Создать символьную ссылку symlink
Ctrl+x,Ctrl+s	Редактировать символическую ссылку

Горячие комбинации клавиш для редактора Midnight Commander (MCEdit)

Отдельно рассмотрим горячие комбинации клавиш для работы в текстовом редакторе.

MCEdit - редактор текстовых и двоичных файлов с заменой регулярных выражений, подсветкой синтаксиса, макросами и конвейером оболочки.

При запуске Midnight Commander под этим именем требуется запустить внутренний редактор и открыть файл, указанный в командной строке.

Внутренний редактор файлов - это полнофункциональный полноэкранный редактор. Он может редактировать файлы размером до 64 мегабайт. Можно редактировать двоичные файлы. В настоящее время он поддерживает следующие функции: копирование блоков, перемещение, удаление, вырезание, вставка; клавиша для отмены нажатия клавиши; выпадающие меню; вставка файла; макрокоманды; поиск и замена регулярных выражений (наш собственный поиск и замена scanf-printf); выделение текста стрелкой *Shift* (если поддерживается терминалом); переключатель вставки-перезаписи; перенос слова; настраиваемый размер вкладки; подсветка синтаксиса для различных типов файлов; и возможность передавать текстовые блоки по конвейеру через команды оболочки, такие как **indent** и **ispell**.

Изменение вида редактора

Сочетание	Действие
Alt+n	Показать или скрыть нумерацию строк
Ctrl+s	Включить или выключить подсветку синтаксиса
Alt+Shift+-	Включить или отключить отображения табуляций и пробелов
Alt+Shift++	Включить или отключить автовыравнивание возвратом каретки

Работа с текстом

Сочетание	Действие
F3	Начать выделение текста, повторное нажатие *F3* закончит выделение
Shift+F3	Начать выделение блока текста, повторное нажатие *F3* закончит выделение
F5	Скопировать выделенный текст
F6	Переместить выделенный текст

F8	Удалить выделенный текст
Ctrl+k	Удалить часть строки до конца строки
Ctrl+y	Удалить строку
Ctrl+x	Перейти в конец слова
Ctrl+z	Перейти на начало предыдущего слова
Alt+l	Переход на строку по номеру строки
Alt+u	Выполнить команду и вставить вывод результата команды в позицию под курсором
Alt+t	Сортировка строк выделенного текста
Tab	Сдвинуть вправо выделенный текст
Ctrl+u	Отменить действия

Работа с файлами

Сочетание	Действие
Ctrl+n	Создать новый файл
Ctrl+f	Копировать выделенный текст в файл
Shift+F5	Вставка текста из файла

Fdupes – программа проверки наличия дубликатов файлов

Fdupes – это программа для сканирования каталогов на наличие дубликатов файлов. Она может сканировать заданный каталог, выводя список найденных дубликатов, автоматически их удаляя или требуя подтверждения удаления.

Вы можете подробнее ознакомиться с работой программы **fdupes**, просмотрев наши обучающие видео:

- на **RuTube** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **Яндекс.Дзен** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **VK Видео** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов.

На наших каналах вы также сможете найти много другой полезной информации.

Устанавливается командой:

```
dnf install fdupes
```

Для поиска *дубликатов файла* выполните следующую команду:

```
fdupes /media/files

/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
```

Для поиска *повторяющихся файлов* с учетом вложенных каталогов используется параметр **-r**:

```
fdupes -r /media/

/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
```

Для просмотра *размеров дубликатов*, найденных в папке, используется параметр **-S**:

```
fdupes -S /media/files

10 bytes each:
/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
```

Для поиска *дубликатов файлов в нескольких директориях* задаются нужные каталоги по очереди:

```
fdupes -r /dev /media

/media/files/file3.txt
/media/files/file2.txt
/media/files/file1.txt
/media/files/file4.txt
/media/files/file5.txt
/dev/mapper/document
/dev/mapper/document2
```

Для *удаления дубликатов* файлов используется параметр **-d**:

```
fdupes -d /dev/mapper/ /media/files/

Set 1 of 2:
   1 [-] /media/files/file3.txt
   2 [-] /media/files/file2.txt
   3 [+] /media/files/file1.txt
   4 [-] /media/files/file4.txt
```

```
   5 [-] /media/files/file5.txt

Set 2 of 2:
   1 [+] /dev/mapper/document
   2 [-] /dev/mapper/document2

( Preserve files [1 - 2, all, help] ):1
```

В появившемся списке необходимо отметить файлы, которые удалять не нужно, и нажать «**DELETE**», программа удалит не помеченные файлы.

FSlint – графическая утилита поиска дубликатов файлов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** fslint-2.47-1

FSlint — программа для очистки файловой системы от «мусорных» файлов. **FSlint** можно применять для поиска и удаления одинаковых файлов (дубликатов файлов), битых символических ссылок, пустых директорий, файлов с некорректными именами, временных файлов и прочего.

Вы можете подробнее ознакомиться с работой в программе **FSlint**, просмотрев наши обучающие видео:

- на **RuTube** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **Яндекс.Дзен** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов;
- в **VK Видео** — Повторяющиеся файлы в РЕД ОС - как избавиться от дубликатов.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

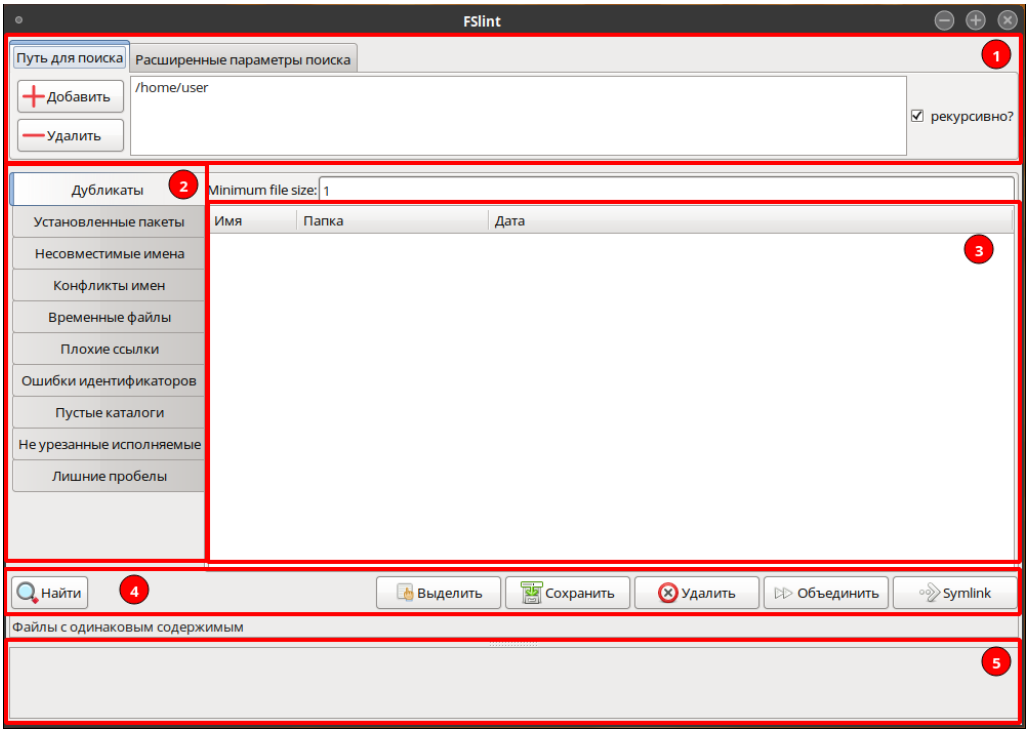
и выполните команду:

```
dnf install fslint
```

После установки программа будет доступна из «**Главного меню**» - «**Системные**» - «**FSlint**» или через консоль:

```
fslint-gui
```

Окно программы выглядит следующим образом:



1. Добавление директорий, в которых необходимо осуществить поиск файлов. Доступна вкладка с расширенными параметрами поиска, где можно исключить некоторые пути и установить дополнительные параметры.

2. Выбор критерия поиска.

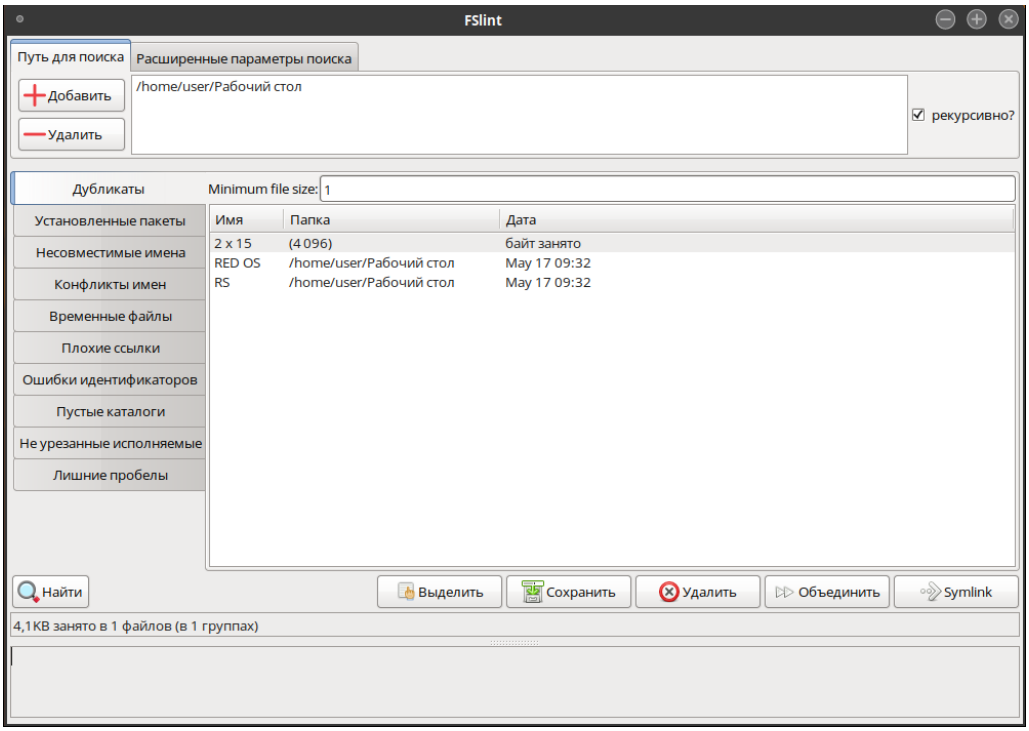
3. Поле для вывода результата поиска.

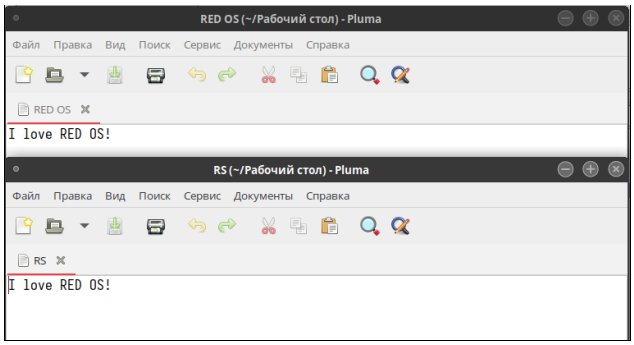
4. Доступные для выполнения команды над файлами.

5. Информационное поле.

Для осуществления поиска дубликатов файлов необходимо указать директории, по которым будет осуществляться поиск, нажав кнопку «**Добавить**». Затем в критериях поиска выбрать «**Дубликаты**» и нажать кнопку «**Найти**».

Результат поиска будет выглядеть примерно следующим образом:





Утилиты для архивирования, восстановления и копирования файлов в терминале

dd
tar
zip
unrar
rsync
p7zip

Вы можете подробнее ознакомиться с работой утилит для архивирования, копирования и восстановления файлов, просмотрев наши обучающие видео:

- на **RuTube**:
  - Консольные утилиты для работы с архивами.
- в **Яндекс.Дзен**:
  - Копирование и клонирование дисков;
  - Консольные утилиты для работы с архивами.
- в **VK Видео**:
  - Консольные утилиты для работы с архивами.

На наших каналах вы также сможете найти много другой полезной информации.

dd

Команда для копирования системного раздела диска в файл с условным названием /media/device/sda.bin:

```
dd if=/dev/sda1 of=/media/device/sda1.bin bs=4096
```

С учетом возможности перенаправления стандартного ввода/вывода команда dd позволяет применять для копирования алгоритмы сжатия или защитного преобразования:

```
dd if=/dev/sda1 bs=4096 | gzip > /media/device/sda1.bin.gz2
```

Команда для восстановления системного раздела диска (для этого потребуется загрузиться с отдельного диска, и примонтировать носитель, на котором был размещен файл с образом):

```
dd if=/media/mountpoint/sda1.bin of=/dev/sda1 bs=4096
```

tar

tar упаковка:

```
tar -cf jpg.tar *.jpg
```

или указав каталог:

```
tar -cf jpg.tar ~/files
```

распаковка:

```
tar -xvf archive.tar
```

в папку:

```
tar -xvf archive.tar -C /path
```

gzip сжатие:

```
tar -cvzf files.tar.gz ~/files
```

распаковка:

```
tar -xzvf archive.tar.gz
```

bzip2 сжатие:

```
tar -cvjf files.tar.bz2 ~/files
```

распаковка:

```
tar -xjvf /path/to/archive.tar.bz2
```

в папку:

```
tar -xjvf archive.tar.bz2 -C /path/to/folder
```

Создание архива на удаленной машине

```
tar -cvpz ./ | ssh root@10.81.1.190 "( cat >  /home/user/ssh_backup.tar )"\
```

Синхронизация папок

zip

zip сжатие:

```
zip file_archive.zip -r /var/log/
zip file_archive.zip file1.txt file2.log
```

Распаковка:

```
unzip file_archive.zip
unzip file_archive.zip -d /tmp
```

unrar

Для работы с архивами rar установите пакет:

```
sudo dnf install unrar
```

Распаковка:

```
unrar x archive.rar
unrar x archive.rar ./folder
```

rsync

Rsync - это программное обеспечение с открытым исходным кодом, которое можно использовать для синхронизации файлов и папок с локального компьютера на удаленный и наоборот. Примечательная особенность Rsync - возможность передавать зашифрованные файлы с помощью SSH и SSL. Кроме того, здесь передача файлов выполняется в один поток, в отличие от других подобных программ, создающий отдельный поток для передачи каждого файла. Это увеличивает скорость и убирает дополнительные задержки, которые становятся проблемой при передаче большого количества маленьких файлов.
Основные параметры rsync:
`-v` - Выводить подробную информацию о процессе копирования;
`-q` - Минимум информации;
`-c` - Проверка контрольных сумм для файлов;
`-a` - Режим архивирования, когда сохраняются все атрибуты оригинальных файлов;
`-R` - Относительные пути;
`-b` - Создание резервной копии;
`-u` - Не перезаписывать более новые файлы;
`-l` - Копировать символьные ссылки;
`-L` - Копировать содержимое ссылок;
`-H` - Копировать жесткие ссылки;
`-p` - Сохранять права для файлов;
`-g` - Сохранять группу;
`-t` - Сохранять время модификации;
`-x` - Работать только в этой файловой системе;
`-e` - Использовать другой транспорт, например, ssh;

-z - Сжимать файлы перед передачей;
--delete - Удалять файлы которых нет в источнике;
--exclude - Исключить файлы по шаблону;
--recursive - Перебирать директории рекурсивно;
--no-recursive - Отключить рекурсию;
--progress - Выводить прогресс передачи файла;
--stat - Показать статистику передачи;
--version - Версия утилиты.
Rsync позволяет синхронизировать файлы и папки в пределах одной машины. Давайте сначала рассмотрим использование rsync для синхронизации файла на локальном компьютере:

```
rsync -zvh file /tmp/backups/
```

Синхронизация папок rsync выполняется так же, как и файлов:

```
rsync -zvh /var/account/* /tmp/backups/
```

Если вы хотите, чтобы все атрибуты файлов, такие, как дата изменения и создания сохранялись, необходимо использовать опцию -a:

```
rsync -azvh /var/account/* /tmp/backups/
```

Синхронизация файлов производится следующим образом. Скопируем локальную папку files, на удаленный сервер:

```
rsync -avz /home/files root@10.81.1.190:/home/user
```

По умолчанию rsync попытается использовать транспорт ssh. Если вы хотите использовать ранее созданный сервер rsync, нужно указать это явно:

```
rsync -avz /home/files rsync://10.81.1.190:/share
```

Точно также можно синхронизировать файлы с rsync из удаленного сервера:

```
rsync -avz root@10.81.1.190:/home/ /home/files/
```

p7zip

7-Zip — свободный файловый архиватор с высокой степенью сжатия данных благодаря формату 7z с компрессией LZMA. Кроме формата 7z поддерживает также ZIP, GZIP, BZIP2 и TAR. Может распаковать множество других форматов, например CAB, CHM, DEB, ISO, LZMA, MSI, RAR и другие. Формат 7z достаточно популярен среди архивов, поэтому имеет смысл иметь поддержку 7z в системе, а также создавать свои архивы в виде 7z формата, ибо сжатие с помощью 7z на 30-50% лучше, чем сжатие с помощью ZIP.
Основные параметры:
a – Создание архива, добавить файлы в архив
b - Бенчмарк
d - Удалить файлы из архива
e - Извлечь файлы из архива (без использования имён директорий)
l - Список содержимого архива
t - Тестировать архив на целостность
u - Обновить файлы в архиве
x - Извлечь файлы с полными путями

Для упаковки в архив archive.7z файлов file, file1, file2 в директории /home/user/files, выполните команду:

```
7z a archive.7z file file1 file2
```

Для упаковки в архив archive.7z всего содержимого директории /home/user/files, выполните команду(в текущем каталоге):

```
7z a archive.7z
```

Файл archive.7z будет создаваться в текущей директории. Можно использовать абсолютный/относительный путь, например:

```
7z a /home/user/archive.7z
```

Опция -t определяет формат архива на выходе. Например -t7z устанавливает 7z формат (он же используется по умолчанию). Также можно определить иной формат архива: zip, gzip, bzip2 или tar. Распаковка архива в текущую директорию:

```
7z x archive.7z
```

Чтобы распаковать архив в определенную директорию используется опция -o, за которой без пробела указывается путь до директории:

```
7z x archive.7z -o./files
```

Для просмотра содержимого архива используется команда:

```
7z l archive.7z
```

Чтобы проверить целостность архива (проверить, что архив «не битый») используется команда:

```
7z t archive.7z
```

Сохранение в файл вывода консоли

Перенаправление стандартного вывода
Перенаправление вывода ошибок
Перенаправление стандартного вывода и стандартного вывода ошибок в один файл
Перенаправление стандартного ввода
Конвейеры

Многие программы выводят в консоль какую-либо информацию. Этот вывод часто делится на два типа:

1. Результаты работы программы, т.е. данные, для получения которых и создавалась эта программа;
2. Сообщения о состоянии или об ошибках.

Например, если посмотреть на вывод программы `ls`, можно увидеть, что она выводит на экран результаты своей работы и иногда сообщения об ошибках. Согласно основной идее Unix, что «всё — есть файл», программы, в действительности, выводят свои результаты в специальный файл, который называется **стандартным выводом** или **стандартным потоком вывода** (часто обозначается как **stdout**), а сообщения о состоянии — в специальный файл **стандартный вывод ошибок** или **поток ошибок** (**stderr**). По умолчанию оба эти потока связаны с экраном и не сохраняются на диске.

Кроме того, многие программы принимают ввод из специального файла с названием **стандартный ввод** или **стандартный поток ввода** (**stdin**), который по умолчанию связан с клавиатурой.

Механизм перенаправления ввода/вывода позволяет изменять направление вывода и ввода. Обычно **вывод** осуществляется на экран, а **ввод** — с клавиатуры, но механизм перенаправления ввода/вывода позволяет изменить этот порядок.

Вы можете подробнее ознакомиться с перенаправлением вывода консоли в файл, просмотрев наши обучающие видео:

- на **RuTube** — Перенаправление в bash;
- в **Яндекс.Дзен** — Перенаправление в bash;
- в **VK Видео** — Перенаправление в bash.

На наших каналах вы также сможете найти много другой полезной информации.

Перенаправление стандартного вывода

Механизм перенаправления ввода/вывода позволяет явно указать, куда должен осуществляться стандартный вывод. Чтобы перенаправить стандартный вывод в файл вместо экрана, нужно добавить в команду оператор перенаправления «**>**» и имя файла. Например, можно сообщить командной оболочке, что она должна направить вывод команды `ls` в файл вместо экрана:

```
ls /usr/bin > listing.txt
```

Просмотрев содержимое файла (например, командной `cat listing.txt`), можно увидеть ту же информацию, как если бы вывод осуществлялся непосредственно в консоль.

Теперь попробуйте выполнить предыдущую команду, но для другого каталога, например:

```
ls /etc > listing.txt
```

Затем просмотрите содержимое файла. Вы увидите, что старая информация в нём была перезаписана. Это объясняется тем, что при перенаправлении вывода с помощью оператора «**>**» файл назначения всегда перезаписывается с самого начала.

Примечание.

Если понадобится очистить какой-нибудь файл (или создать новый, пустой файл), это можно сделать с помощью команды:

```
> listing.txt
```

Простой оператор перенаправления, без предшествующей ему команды, очистит существующий файл или создаст новый, пустой файл.

Для добавления вывода в конец существующего файла без перезаписи необходимо использовать оператор перенаправления «**>>**»:

```
ls /etc >> listing.txt
```

Оператор «**>>**» просто добавит результаты в конец файла. Если файл не существует, он будет создан, как при использовании оператора «**>**».

Перенаправление вывода ошибок

При попытке перенаправить вывод с указанием имени несуществующего каталога командой:

```
ls /folder > listing.txt
```

На экран будет выведено следующее сообщение:

```
ls: невозможно получить доступ к '/folder': Нет такого файла или каталога
```

Однако сообщение об ошибке выведено в терминал, а не в файл. Дело в том, что обычно программы не выводят сообщения об ошибках в стандартный вывод — они выводят сообщения об ошибках в поток ошибок.

Поскольку перенаправлен только стандартный вывод, а стандартный вывод ошибок — нет, сообщение об ошибке появилось на экране терминала.

Перенаправление стандартного вывода ошибок осуществляется не так просто, как стандартного вывода. Чтобы перенаправить поток ошибок, нужно указать его *дескриптор файла*.

Первые три потока (иными словами — стандартных файла) были уже упомянуты как стандартный ввод, вывод и вывод ошибок. К ним можно обратиться по их уникальным цифровым идентификаторам, которые и называются **файловыми дескрипторами**:

Стандартный файловый поток	Дескриптор
Ввода	0
Вывода	1
Ошибок	2

Командная оболочка ссылается на стандартные потоки как на файлы по их дескрипторам (иногда говорят, «номерам потока»). Так как стандартному потоку ошибок соответствует файловый дескриптор **2**, можно перенаправить его, например, таким образом:

```
ls /folder 2> listerrors.txt
```

Примечание.

Номер файлового дескриптора помещается непосредственно перед оператором перенаправления, без пробела!

Теперь на экран не выводится сообщение об ошибке.

Перенаправление стандартного вывода и стандартного вывода ошибок в один файл

Для перенаправления всего вывода в один файл необходимо поток ошибок направить в поток вывода, а его, в свою очередь, перенаправить в файл. Например:

```
ls /etc > listing.txt 2>&1
```

Примечание.

Обратите внимание, что порядок перенаправления играет важную роль! Перенаправление стандартного вывода ошибок всегда должно производиться **после** перенаправления стандартного вывода, иначе команда сработает не так, как ожидается.

Если порядок перенаправления изменить, как показано ниже, стандартный вывод ошибок будет перенаправлен на экран:

```
ls /etc 2>&1 > listing.txt
```

Версия **bash**, имеющаяся в РЕД ОС, поддерживает и другой, более короткий способ написания данного перенаправления:

```
ls /etc &> listing.txt
```

В примере используется единственный оператор **&>**, перенаправляющий стандартный вывод и стандартный вывод ошибок в файл **listing.txt**. Аналогично можно перенаправить стандартный вывод и стандартный вывод ошибок с добавлением в конец одного и того же файла:

```
ls /etc &>> listing.txt
```

Примечание.

Между символами в операторе перенаправления не должно быть пробелов!

Иногда случаются ситуации, когда вывод программы совсем не нужен, его желательно не просто перенаправить в файл, а перенаправить в никуда. Для этого достаточно указать в качестве целевого файла для перенаправления вывода специальный файл `/dev/null`. Этот файл представляет системное устройство, называемое *битоприёмником* (**bit bucket**), которое принимает любой ввод и ничего с ним не делает. Например:

```
ls /etc > /dev/null
ls /etc 2> /dev/null
ls /etc &> /dev/null
```

Перенаправление стандартного ввода

Выше использовалась команда `cat listing.txt` для вывода содержимого файла на экран терминала. Утилита (**cat**) может принимать данные как прямым чтением из файла (как в примере), так и считыванием из потока ввода (напрямую с клавиатуры или из перенаправленного потока), а получив данные, утилита cat выводит их в стандартный поток вывода (обычно — это экран).

В качестве примера содержимое файла с листингом будет направлено в поток ввода, для этого выполните следующую команду:

```
cat < listing.txt
```

На экране будет показано всё то же содержимое листинга.

Таким способом можно подать на вход программе, читающей данные из потока ввода, информацию из файла.

Конвейеры

Умение команд читать данные со стандартного ввода и выводить результаты в стандартный вывод используется механизмом командной оболочки, который называется **конвейером**. С помощью оператора конвейера «|» (вертикальная черта) стандартный вывод одной команды можно связать со стандартным вводом другой:

```
<команда_1> | <команда_2>
```

Для демонстрации этого механизма понадобится несколько команд. Например, необходимо получить листинг всего содержимого папки **/etc**, включая все подкаталоги, и вывести на экран только имена с расширением **.conf**. Для выбора строк по заданному шаблону применяется утилита grep, которая, как и **cat**, может принимать данные как из файла, так и из потока ввода. Перенаправьте вывод команды `ls -R` на ввод команде `grep "\.conf"`:

```
ls -R /etc | grep "\.conf"
```

Если данный вывод необходимо сохранить в файл для дальнейшей работы, то операторы перенаправления и конвейеры можно сочетать в одной комбинированной команде. Например:

```
ls -R /etc | grep "\.conf" > list_of_conf.txt
```

Важно отметить, что можно сочетать несколько конвейеров в одной составной команде. Такие команды часто называют **фильтрами**.

Recoll – поиск документов по содержимому

Recoll - приложение, позволяющее производить поиск документов по их содержимому.
Поддерживаемые форматы:

```
Text, HTML, email, OpenDocument, Microsoft Office и Office Open XML, AbiWord, KWord, Gaim, Lyx, Scribus, PDF, WordPerfect, PostScript, RTF, TeX, DVI, DjVu, MP3 и другие аудиоформаты, JPEG и другие форматы изображения.
```

Вы можете подробнее ознакомиться с информацией по поиску файлов в системе, просмотрев наши обучающие видео:

- на **RuTube** — Утилиты поиска файлов;
- в **Яндекс.Дзен** — Утилиты поиска файлов;
- в **VK Видео** — Утилиты поиска файлов.

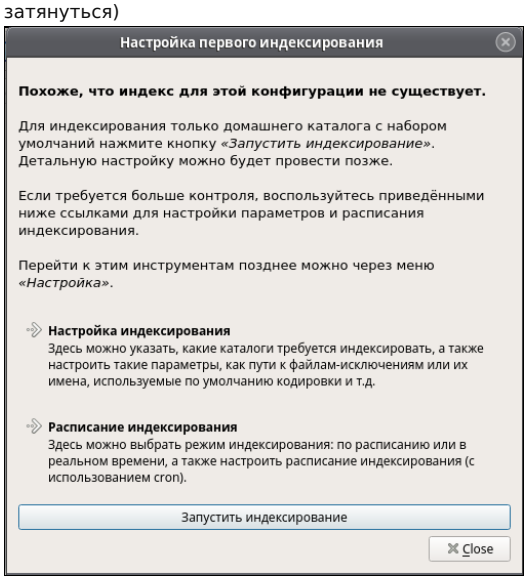
На наших каналах вы также сможете найти много другой полезной информации.

Установка:

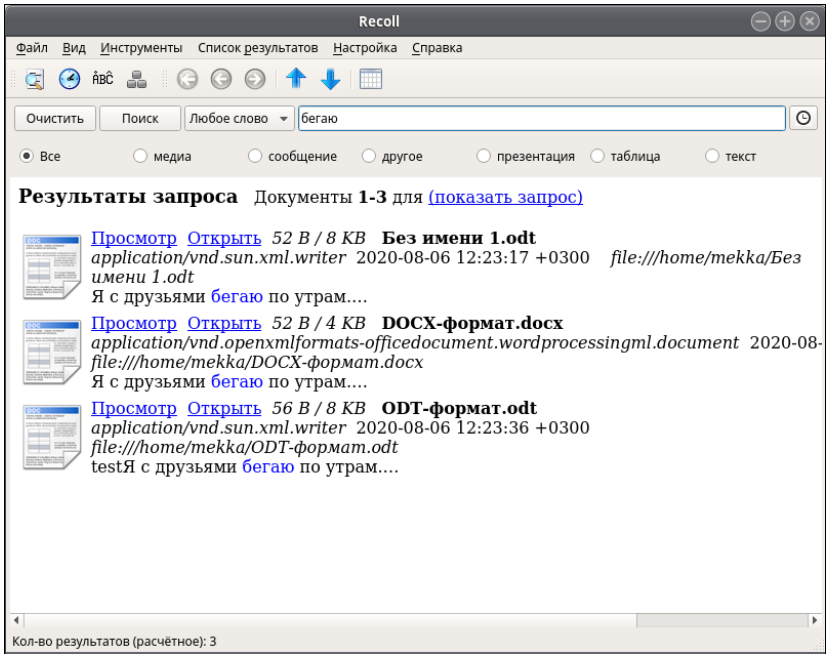
```
dnf install recoll
```

Далее запускаем из Меню -> Стандартные -> Recoll

Первый запуск сопровождается индексацией по файлам во всей системе. Запускаем её (если файлов на диске много, процесс может затянуться)



Далее достаточно в поиск ввести слово и соответствующий фильтр, чтобы Recoll знал, как и что ему искать:



ВАЖНО

Самое важное в процессе поиска, это обновлять индексы. Так как приложение ориентируется только на те файлы, которые он проиндексировал. Файлы, созданные и отредактированные после индексации программа уже не учитывает. Чтобы запустить процесс индексации необходимо перейти в раздел Файл -> Обновить индекс.

Ripgrep — рекурсивный поиск в текущем каталоге шаблона регулярного выражения

Установка
Синтаксис
Опции
Позиционные аргументы
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: ripgrep-13.0.0

Ripgrep (или rg) — это инструмент командной строки для рекурсивного поиска в текущем каталоге шаблона регулярного выражения. **Ripgrep** предназначен для замены стандартной команды **grep** с улучшенной производительностью и удобством использования. **Ripgrep** обладает высокой скоростью работы благодаря использованию многопоточности и оптимизированным алгоритмам.

По умолчанию **ripgrep** будет учитывать .gitignore и автоматически пропускать скрытые файлы/каталоги и двоичные файлы. Стандартный набор регулярных выражений ripgrep гарантирует линейное время поиска. Поэтому такие функции, как обратные ссылки и произвольные проверки, не поддерживаются. Флаг **--pcre2** можно использовать для включения обратных ссылок и проверок.

Ripgrep поддерживает файлы конфигурации. Установите **RIPGREP_CONFIG_PATH** в файл конфигурации. Файл может содержать один аргумент оболочки на строку. Строки, начинающиеся с #, игнорируются.

Установка

Для установки **ripgrep** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install ripgrep
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
rg [<ОПЦИИ>] ШАБЛОН [ПУТЬ ...]
```

Для просмотра опций ripgrep используйте команду:

```
rg --help
```

Опции

Основные опции утилиты ripgrep:

- **-A, --after-context** — показывать количество строк после каждого совпадения (переопределяет флаг **--context** и **--passthru flags**);
- **--auto-hybrid-regex** — динамически выбирать между поддерживаемыми регулярными выражениями в зависимости от функций, используемых в шаблоне;
- **-B, --before-context** — показывать количество строк перед каждым совпадением;
- **--binary** — выполнять поиск в двоичных файлах (по умолчанию ripgrep пытается автоматически пропускать двоичные файлы, чтобы повысить релевантность результатов и ускорить поиск);
- **--block-buffered** — использовать буферизацию блоков;
- **-b, --byte-offset** — выводить смещение на основе 0 байт во входном файле перед каждой строкой вывода, если указано **-o** (**--only-matching**), выводить смещение самой соответствующей части;

- **-s, --case-sensitive** — выполнять поиск с учётом регистра;
- **--color** — определять использование цветов;
- **--colors** — определять настройки цвета для использования в выходных данных;
- **--column** — определять номер столбца, начиная с 1;
- **-C, --context** — показывать количество строк после каждого совпадения;
- **--context-separator** — разделять несмежные строки контекста в выходных данных;
- **-c, --count** — показывать количество строк, соответствующих заданным шаблонам для каждого искомого файла;
- **--count-matches** — показывать количество отдельных совпадений с заданными шаблонами для каждого искомого файла;
- **--crlf** — обрабатывать CRLF (\r \ n) как символ завершения строки, а не просто \n;
- **--debug** — показывать сообщения отладки;
- **--dfa-size-limit** — верхний предел размера регулярного выражения DFA;
- **-E, --encoding** — использовать кодировку текста для всех искомых файлов;
- **-f, --file** — искать по одному шаблону из файла на строку;
- **--files** — распечатать каждый файл, в котором будет выполняться поиск;
- **-l, --files-with-matches** — распечатать только те пути, которые имеют хотя бы одно совпадение;
- **--files-without-match** — распечатать только те пути, которые содержат нулевые совпадения;
- **-F, --fixed-strings** — определять рисунок как литеральную строку, а не регулярное выражение;
- **-L, --follow** — переходить по символическим ссылкам во время проверки каталогов;
- **-g, --glob** — включать или исключать файлы и каталоги для поиска;
- **--glob-case-insensitive** — обрабатывать шаблоны, заданные с помощью флага -g / --glob, без учёта регистра;
- **--heading** — выводить путь к файлу;
- **--hidden** — выполнять поиск скрытых файлов и каталогов;
- **--iglob** — включать файлы и каталоги в поиск с учётом регистра;
- **-i, --ignore-case** — игнорировать регистры символов при поиске;
- **--ignore-file** — указывать файл (файлы), содержащие шаблоны, которые будут использоваться для игнорирования файлов во время поиска;
- **--ignore-file-case-insensitive** — то же, что и **--ignore-file**, но шаблоны в этом файле будут применяться без учёта регистра;
- **--include-zero** — включать в вывод результат поиска, даже если найденная строка отсутствует (например, для пустых файлов);
- **-v, --invert-match** — выводить только те строки, которые не соответствуют заданному шаблону (инверсия совпадений);
- **--json** — выводить результаты поиска в формате JSON;
- **-n, --line-number** — добавлять к каждому найденному совпадению номер строки, в которой было найдено это совпадение;
- **-x, --line-regexp** — искать совпадения только среди целых строк, игнорируя различные подстроки;
- **-M, --max-columns** — устанавливать максимальное количество отображаемых столбцов (символов) для всех строк в выводе;
- **--max-columns-preview** — аналогично **-M**, используется для предварительного просмотра, ограничивая количество видимых столбцов;
- **-m, --max-count** — ограничивать общее количество совпадений, которые будут выводиться в результате поиска;
- **--max-depth** — задать максимальную глубину обхода каталогов, т.е. сколько уровней директорий будет обходить утилита;
- **--max-filesize** — ограничивать размер обрабатываемых файлов (при превышении указанного размера файл будет игнорироваться);
- **--mmap** — использовать память для отображения файлов;
- **-U, --multiline** — включать режим поиска по многострочным совпадениям, используется для текста, который может находиться на нескольких строках;
- **--multiline-dotall** — включать режим поиска по многострочным совпадениям с учётом всех символов;
- **--no-config** — отключать использование конфигурационных файлов ripgrep;
- **-I, --no-filename** — подавлять вывод имён файлов при выводе результатов поиска, если нужно получить только совпадения без указания, в каких файлах они были найдены;

- **--no-heading** — отключать вывод заголовков (имён файлов) перед результатами поиска;
- **--no-ignore** — выполнять поиск по всем файлам и директориям, независимо от правил игнорирования;
- **-N, --no-line-number** — отключать вывод номеров строк при совпадении;
- **--no-messages** — подавлять вывод информационных сообщений, таких как предупреждения об отсутствии файлов или о том, что некоторые файлы были проигнорированы;
- **--no-mmap** — отключать использование отображения файлов в память при поиске;
- **--no-pcre2-unicode** — отключать поддержку юникодных символов в регулярных выражениях с использованием библиотеки PCRE2;
- **--no-require-git** — позволять использовать ripgrep без необходимости находиться в каталоге Git или проекте, управляемом системой контроля версий;
- **--no-unicode** — отключать поддержку символов Unicode в выводе, что может быть полезно для консольных эмуляторов, которые не поддерживают или неправильно отображают UTF-8;
- **-0, --null** — использовать нулевой байт в качестве разделителя между именами файлов в выводе;
- **--null-data** — аналогично -0, но используется во время обработки входных данных;
- **--one-file-system** — ограничивать поиск только текущей файловой системой, что предотвращает переход через смонтированные файловые системы, такие как сетевые или внешние диски;
- **-o, --only-matching** — выводить только совпадающую часть строки, а не всю строку;
- **--passthru** — позволять вывести строки, которые были найдены, но не соответствуют заданному шаблону;
- **--path-separator** — задать символ-разделитель для путей в выводе;
- **-P, --pcre2** — включать поддержку регулярных выражений PCRE2, что позволяет использовать более сложные регулярные выражения при выполнении поиска;
- **-p, --pretty** — выводить результаты в красивом формате (псевдоним для --color=always --heading --line-number);
- **-q, --quiet** — отключить вывод результатов и сообщений об ошибках, прекратить поиск, если в файле найдено соответствие;
- **--regex-size-limit** — установить лимит на размер регулярного выражения;
- **-e, --regexp** — указать регулярное выражение для поиска;
- **-r, --replace** — заменить найденные совпадения на указанный текст;
- **-z, --search-zip** — искать в ZIP-архивах и других сжимаемых файлах;
- **-S, --smart-case** — поиск выполняется без учёта регистра;
- **--sort** — сортировать выводимые результаты по определённому критерию;
- **--sortr** — сортировать результаты поиска;
- **--stats** — вывести статистику о результатах поиска, включая количество найденных совпадений и время выполнения;
- **-a, --text** — обрабатывать двоичные файлы как текст;
- **-j, --threads** — указывать число потоков, которое будет использовано для параллельной обработки;
- **--trim** — обрезать лишние пробелы в начале и конце строк результатов, улучшая читаемость;
- **-t, --type** — задать тип файлов для поиска, что позволяет ограничить поиск определённым форматом файлов (например, только .txt или .md);
- **--type-add** — добавить новый тип файлов, который можно использовать в команде поиска;
- **--type-clear** — очистить ранее определённые типы файлов, вернуть настройки по умолчанию;
- **--type-list** — выводить список доступных типов файлов, помогает выбрать, какие типы следует использовать в поиске;
- **-T, --type-not** — исключить указанные типы файлов из процесса поиска;
- **-u, --unrestricted** — отключить все ограничения, которые могут применяться к поиску, включая ограничения на типы файлов и размеры;
- **-V, --version** — вывести версию утилиты ripgrep;
- **--vimgrep** — вывести результаты поиска в формате, совместимом с vim, что позволяет удобнее обрабатывать результаты в текстовом редакторе Vim;
- **-H, --with-filename** — вывести имя файла перед совпадениями, даже если в поиске участвует только один файл;
- **-w, --word-regexp** — искать только по целым словам, игнорируя частичные совпадения.

Позиционные аргументы

Шаблон

Шаблон — регулярное выражение, используемое для поиска. Для сопоставления шаблона, начинающегося с тире, используйте опцию **-e /--regexp**.

Путь

Путь — файл или каталог для поиска. Поиск в каталогах выполняется рекурсивно. Пути, указанные явно в командной строке, переопределяют **glob** и игнорируют правила.

Примеры использования

Рассмотрим примеры для нескольких основных опций утилиты **ripgrep**:

1. Опция **-i, --ignore-case**:

```
rg -i "so" ./3d.txt
```

Например, если файл ./3d.txt содержит следующие данные:

```
Sun of the sleepless! Melancholy star!
Whose tearful beam glows tremulously far,
That show'st the darkness thou canst not dispel,
How like art thou to Joy remembered well!

So gleams the past, the light of other days,
Which shines, but warms not with its powerless rays;
A night-beam Sorrow watcheth to behold,
Distinct, but distant – clear, but oh, how cold!

George Gordon Byron
```

Результат поиска (без учета регистра) строк, в которых встречается "**so**" в файле ./3d.txt:

```
6:So gleams the past, the light of other days,
8:A night-beam Sorrow watcheth to behold,
```

2. Опция **-w, --word-regexp**:

```
rg -w "So" ./3d.txt
```

Результат поиска (с учетом регистра) только полных слов "**So**" в файле ./3d.txt:

```
6:So gleams the past, the light of other days,
```

3. Опция **-n, --line-number**:

```
rg -n "to" ./3d.txt
```

Пример выводит номера строк, в которых найдено совпадение с текстом "**to**" в файле ./3d.txt.

```
4:How like art thou to joy remember'd well!
8:A night-beam Sorrow watcheth to behold,
```

4. Опция **-l, --files-with-matches**:

```
rg -l "a" /home/user/Документы
```

Пример выводит список файлов в каталоге /home/user/Документы, в которых найдены строки, содержащие "**a**".

```
/home/user/Документы/sample1.json  /home/user/Документы/3d.txt
```

5. Опция **-c, --count**:

```
rg -c "s" ./3d.txt
```

Пример выводит только количество строк, содержащих совпадения с "**s**" в файле ./3d.txt.

```
6
```

6. Опция **-A, --after-context <параметр>**:

```
rg -A 3 "the" ./3d.txt
```

Пример выводит 3 строки после каждого совпадения с "**the**" в файле ./3d.txt:

```
1:Sun of the sleepless! Melancholy star!
2-Whose tearful beam glows tremulously far,
3:That show’st the darkness thou canst not dispel,
4-How like art thou to Joy remembered well!
5-
6:So gleams the past, the light of other days,
7-Which shines, but warms not with its powerless rays;
8-A night-beam Sorrow watcheth to behold,
9-Distinct, but distant – clear, but oh, how cold!
```

7. Опция **-v, --invert-match**:

```
rg -v "to" ./3d.txt
```

Пример выводит строки из файла ./3d.txt, которые не содержат совпадения с "**to**".

```
1:Sun of the sleepless! Melancholy star!
2:Whose tearful beam glows tremulously far,
3:That show’st the darkness thou canst not dispel
5:
6:So gleams the past, the light of other days,
7:Which shines, but warms not with its powerless rays;
9:Distinct, but distant – clear, but oh, how cold!
10:
11:George Gordon Byron
```

8. Опция **-C, --context <параметр>**:

```
rg -C 2 "warms" ./3d.txt
```

Пример выводит 2 строки ДО и 2 строки ПОСЛЕ каждого совпадения с "**warms**" в файле ./3d.txt:

```
5-
6-So gleams the past, the light of other days,
7:Which shines, but warms not with its powerless rays;
8-A night-beam Sorrow watcheth to behold,
9-Distinct, but distant – clear, but oh, how cold!
```

9. Опция **-F, --fixed-strings**:

```
rg -F "like art" ./3d.txt
```

Пример выполнит поиск точного текста "**like art**" в файле ./3d.txt, не интерпретируя его как регулярное выражение:

```
4:How like art thou to Joy remembered well!
```

10. Опция **-s, --case-sensitive**:

```
rg -s "am" ./3d.txt
```

Пример выполнит поиск строки "**am**" в файле ./3d.txt, учитывая регистр символов (по умолчанию):

```
2:Whose tearful beam glows tremulously far,
6:So gleams the past, the light of other days,
8:A night-beam Sorrow watcheth to behold,
```

11. Опция **-L, --follow**:

```
rg -L "no" /home/user/Документы
```

Пример выполнит поиск в файлах в указанном каталоге /home/user/Документы, следуя символическим ссылкам:

```
/home/user/Документы/sample1.json  4:That show’st the darkness thou canst not dispel,
8:Which shines, but warms not with its powerless rays;

/home/user/Документы/3d.txt
3:That show’st the darkness thou canst not dispel,
7:Which shines, but warms not with its powerless rays;
```

12. Опция **-u, --unrestricted**:

```
rg -u "of" ./3d.txt
```

Пример отключит "умный" поиск и все ограничения, которые могут применяться к поиску, и выполнит точное сопоставление с "**of**" в файле ./3d.txt.

```
1:Sun of the sleepless! Melancholy star!
6:So gleams the past, the light of other days,
```

13. Опция **-V, --version**:

```
rg --version
```

Команда выводит номер версии **ripgrep**.

```
ripgrep 13.0.0
```

14. Опция **--type-list**:

```
rg --type-list
```

Пример выводит список всех известных типов файлов, которые **ripgrep** может обрабатывать.

```
agda: *.agda, *.lagda
aidl: *.aidl
amake: *.bp, *.mk
asciidoc: *.adoc, *.asc, *.asciidoc
asm: *.S, *.asm, *.s
asp: *.ascx, *.ascx.cs, *.ascx.vb, *.aspx, *.aspx.cs, *.aspx.vb
ats: *.ats, *.dats, *.hats, *.sats
avro: *.avdl, *.avpr, *.avsc
awk: *.awk
bazel: *.BUILD, *.bazel, *.bazelrc, *.bzl, BUILD, WORKSPACE
bitbake: *.bb, *.bbappend, *.bbclass, *.conf, *.inc
brotli: *.br
buildstream: *.bst
bzip2: *.bz2, *.tbz2
c: *.[chH], *.[chH].in, *.cats
cabal: *.cabal
cbor: *.cbor
[...]
vimscript: *.vim
webidl: *.idl, *.webidl, *.widl
wiki: *.mediawiki, *.wiki
xml: *.dtd, *.rng, *.sch, *.xhtml, *.xjb, *.xml, *.xml.dist, *.xsd, *.xsl, *.xslt
xz: *.txz, *.xz
yacc: *.y
yaml: *.yaml, *.yml
yang: *.yang
z: *.Z
zig: *.zig
zsh: *.zsh, .zlogin, .zlogout, .zprofile, .zshenv, .zshrc, zlogin, zlogout, zprofile, zshenv,
zshrc
zstd: *.zst, *.zstd
```

15. Опция **--sort <параметр>**:

```
rg --sort accessed "ss" /home/user/Документы
```

Пример позволяет сортировать файлы по заданному критерию ("**path**", "**modified**", "**accessed**", "**created**", "**none**"):

```
/home/user/Документы/3d.txt
1:Sun of the sleepless! Melancholy star!
3:That show’st the darkness thou canst not dispel, 7:Which shines, but warms not with its powerless rays;
 /home/user/Документы/sample1.json  2:Sun of the sleepless! Melancholy star!
4:That show’st the darkness thou canst not dispel,
8:Which shines, but warms not with its powerless rays;
```

16. Опция **-m, --max-count <параметр>**:

```
rg -m 10 "beam" /home/user/Документы
```

Пример останавливает поиск в каждом файле указанного каталога после заданного числа совпадений:

```
2:Whose tearful beam glows tremulously far,
8:A night-beam Sorrow watcheth to behold,
```

17. Опция **--color <параметр>**:

```
rg --color always "to" ./3d.txt
```

Пример использует цветовое выделение для совпадающих строк ("**always**", "**ansi**", "**auto**","**never**").

```
4:How like art thou to Joy remembered well!
8:A night-beam Sorrow watcheth to behold,
```

Эти примеры показывают разнообразие опций для работы с текстовыми данными и их возможности для поиска с помощью **ripgrep**.

Просмотр и управление файлами и каталогами с помощью утилиты tree

Установка
Синтаксис и опции
Примеры использования
Сравнение работы с командой ls

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tree-1.8.0-1

Tree — консольная утилита для просмотра и управления файлами и директориями. Она предоставляет простой, но мощный интерфейс для навигации по файловой системе и выполнения различных операций с файлами, таких как создание, удаление, копирование, перемещение и изменение атрибутов.

Основные функции программы **tree**:

1 . *Просмотр содержимого директорий и файлов*. **Tree** позволяет быстро просматривать содержимое директории, включая имена файлов и папок, их размеры и даты изменения.

2. *Перемещение, копирование и удаление файлов и директорий*. **Tree** предоставляет возможность перемещать, копировать и удалять файлы и директории в текущей директории или в какой-либо другой.

3. *Изменение атрибутов файлов и директорий*. С помощью **Tree** можно изменять атрибуты файлов, такие как разрешения, владелец, группа и время доступа.

4 . *Поиск файлов и директорий по имени*. **Tree** поддерживает поиск файлов и директорий в текущей директории и во всех поддиректориях по заданному имени.

5 . *Сортировка файлов и директорий по различным критериям*. **Tree** позволяет сортировать файлы и директории по имени, размеру, дате изменения, времени последнего доступа и другим параметрам.

6 . *Поддержка многопанельного интерфейса*. **Tree** может быть запущена в многопанельном режиме, что позволяет просматривать несколько директорий одновременно.

7. *Использование горячих клавиш*. **Tree** имеет набор горячих клавиш для быстрого доступа к наиболее часто используемым функциям.

8. П*оддержка архивов*. **Tree** поддерживает работу с архивами **ZIP** и **TAR**, позволяя просматривать их содержимое и извлекать файлы.

9. *Интеграция с другими программами*. **Tree** может интегрироваться с другими программами, такими как **Midnight Commander** или **Nautilus**, для удобной работы с файлами и директориями.

10. *Поддержка Unicode*. **Tree** поддерживает отображение файлов и директорий на разных языках, включая русский.

Утилита **Tree** полезна для быстрой и удобной навигации по файловой системе РЕД ОС.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните следующую команду:

```
dnf install tree
```

Синтаксис и опции

Синтаксис программы выглядит следующим образом:

```
tree [опции]
```

Опции утилиты, отвечающие за вывод дерева папок и файлов:

- **-a** — вывод всех без исключения файлов;
- **-d** — вывод только списка директорий;
- **-l** — переход по символическим ссылкам, которые ведут к папкам;
- **-f** — вывод содержимого папок с префиксами пути;
- **-x** — учитывает только текущую файловую систему;
- **-L** — уровень вложенности для отображения в выводе;
- **-R** — рекурсивный переход по каталогам всех уровней;
- **-P** — отображение файлов, название которых соответствует шаблону;
- **-I** — исключение из вывода файлов, название которых соответствует шаблону;
- **-o** — печать вывода в файл с заданным именем;
- **--noreport** — запрет вывода отчета по количеству папок и файлов в конце дерева;
- **--charset** — кодировка для отображения графических и html-файлов;
- **--filelimit** — папки, которые содержат больше файлов, чем указано, показаны не будут.

Опции утилиты, использующиеся для управления отображением названий документов:

- **-q** — замена непечатаемых символов в названиях файлов знаком «**?**»;
- **-N** — вывод непечатаемых символов в названиях файлов как есть;
- **-Q** — заключить названия файлов в двойные кавычки;
- **-p** — для каждого из файлов указать его название и список разрешенных действий;
- **-u** — вывод имени или идентификатора учетной записи, под которой был создан файл;
- **-g** — вывод имени или идентификатора группы пользователей, которая имеет права на доступ к файлу;
- **-s** — вывод рядом с названием файла его размера в байтах;
- **-h** — вывод размера файла в удобном формате с добавлением к числу буквенного сокращения (K, M, G, T);
- **-D** — печать даты последнего изменения файла (либо последнего изменения статуса в комбинации с опцией **-c**);
- **-F** — добавление символа «**/**» для папок, «**=**» — для файлов сокета, «*****» — для исполняемых файлов, «**>**» — для door-файлов, «**|**» — для специальных файлов FIFO;
- **--inodes** — вывод номера индексных дескрипторов для файлов и папок;
- **--device** — указать номер устройства, которому принадлежит файл или папка.

Опции утилиты, использующиеся для сортировки результатов:

- **-v** — упорядочить вывод по уровням вложенности;
- **-t** — сортировка вывода по дате последнего изменения файлов и папок;
- **-c** — сортировка вывода по дате последнего изменения статуса;
- **-U** — вывод результатов в том порядке, в котором папки расположены на диске;
- **-r** — сортировка вывода в обратном порядке;
- **--dirsfirst** — сначала вывод папок, потом — файлов.

Опции отображения дерева:

- **-i** — убрать линии («ветки» дерева), файлы и папки отображаются в виде списка;
- **-n** — сделать дерево одноцветным;
- **-C** — вернуть дереву разноцветное отображение после использования опции **-n**.

Примеры использования

1. Вывод дерева файлов и каталогов с указанием их размера:

```
tree -h

.
```

```
├── [   60]  test.log
├── [ 4.0K]  Видео
├── [ 4.0K]  Документы
├── [ 4.0K]  Загрузки
│   └── [ 3.8K]  create_minimal_image_moby.sh
├── [ 4.0K]  Изображения
│   └── [ 339K]  2023-07-11_09-46.png
├── [ 4.0K]  Музыка
├── [ 4.0K]  Общедоступные
├── [ 4.0K]  Рабочий стол
└── [ 4.0K]  Шаблоны
    ├── [  182]  test.sh
    └── [  172]  text.sh

8 directories, 5 files
```

2. Сортировка вывода в обратном порядке:

```
tree -r

.
├── Шаблоны
│   ├── text.sh
│   └── test.sh
├── Рабочий стол
├── Общедоступные
├── Музыка
├── Изображения
│   └── 2023-07-11_09-46.png
├── Загрузки
│   └── create_minimal_image_moby.sh
├── Документы
├── Видео
└── test.log

8 directories, 5 files
```

3. Вывод даты последнего изменения файлов:

```
tree -h -D

.
├── [   60 Jul 10 11:34]  test.log
├── [ 4.0K Jul  6 16:42]  Видео
├── [ 4.0K Jul  6 16:42]  Документы
├── [ 4.0K Jul 11 09:46]  Загрузки
│   └── [ 3.8K Jul  7 15:57]  create_minimal_image_moby.sh
├── [ 4.0K Jul 11 09:46]  Изображения
│   └── [ 339K Jul 11 09:46]  2023-07-11_09-46.png
├── [ 4.0K Jul  6 16:42]  Музыка
├── [ 4.0K Jul  6 16:42]  Общедоступные
├── [ 4.0K Jul  6 16:42]  Рабочий стол
└── [ 4.0K Jul 11 09:46]  Шаблоны
    ├── [  182 Jul 10 11:34]  test.sh
    └── [  172 Jul 10 11:27]  text.sh

8 directories, 5 files
```

4. Также функционал утилиты **tree** позволяет искать файлы с помощью установленной маски, например, для поиска файлов с расширекнием **.png** выполните:

```
tree -P '*.png' --prune

.
└── Изображения
    └── 2023-07-11_09-46.png

1 directory, 1 file
```

5. Существует возможность перенаправления результата выполнения команды в файл:

```
tree -P '*.png' --prune -o output_tree.txt
cat output_tree.txt

.
└── Изображения
    └── 2023-07-11_09-46.png

1 directory, 1 file
```

Сравнение работы с командой ls

В стандартный набор программ РЕД ОС входит утилита **ls**, которая отображает каталоги и их содержимое.

Простая команда **ls** без опций передает на вывод список файлов и папок внутри текущей директории:

```
ls

 output_tree.txt  Видео      Загрузки    Музыка       'Рабочий стол'
 test.log         Документы  Изображения  Общедоступные  Шаблоны
```

С помощью команды **ls** можно просмотреть расширенную информацию о папках и файлах, используя опцию **-g**:

```
ls -g

итого 40
-rw-rw-r--. 1 user  133 июл 11 09:54  output_tree.txt
-rw-rw-r--. 1 user   60 июл 10 11:34  test.log
drwxr-xr-x. 2 user 4096 июл  6 16:42  Видео
drwxr-xr-x. 2 user 4096 июл  6 16:42  Документы
drwxr-xr-x. 2 user 4096 июл 11 09:46  Загрузки
drwxr-xr-x. 2 user 4096 июл 11 09:46  Изображения
drwxr-xr-x. 2 user 4096 июл  6 16:42  Музыка
drwxr-xr-x. 2 user 4096 июл  6 16:42  Общедоступные
drwxr-xr-x. 2 user 4096 июл  6 16:42 'Рабочий стол'
drwxr-xr-x. 2 user 4096 июл 11 09:46  Шаблоны
```

Для обратной сортировки вывода команды используется опция **-r**:

```
ls -g -r

итого 40
drwxr-xr-x. 2 user 4096 июл 11 09:46  Шаблоны
drwxr-xr-x. 2 user 4096 июл  6 16:42 'Рабочий стол'
drwxr-xr-x. 2 user 4096 июл  6 16:42  Общедоступные
drwxr-xr-x. 2 user 4096 июл  6 16:42  Музыка
drwxr-xr-x. 2 user 4096 июл 11 09:46  Изображения
drwxr-xr-x. 2 user 4096 июл 11 09:46  Загрузки
drwxr-xr-x. 2 user 4096 июл  6 16:42  Документы
drwxr-xr-x. 2 user 4096 июл  6 16:42  Видео
-rw-rw-r--. 1 user   60 июл 10 11:34  test.log
-rw-rw-r--. 1 user  133 июл 11 09:54  output_tree.txt
```

Для вывода подробной информации о файлах и каталогах используется опция **-l**:

```
ls -l

итого 40
-rw-rw-r--. 1 user user  133 июл 11 09:54  output_tree.txt
-rw-rw-r--. 1 user user   60 июл 10 11:34  test.log
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Видео
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Документы
drwxr-xr-x. 2 user user 4096 июл 11 09:46  Загрузки
drwxr-xr-x. 2 user user 4096 июл 11 09:46  Изображения
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Музыка
drwxr-xr-x. 2 user user 4096 июл  6 16:42  Общедоступные
drwxr-xr-x. 2 user user 4096 июл  6 16:42 'Рабочий стол'
drwxr-xr-x. 2 user user 4096 июл 11 09:46  Шаблоны
```

Для рекурсивного вывода содержимого каталогов используется опция **-R**:

```
ls -R

.:
 output_tree.txt   Видео      Загрузки     Музыка        'Рабочий стол'
 test.log          Документы  Изображения  Общедоступные  Шаблоны

./Видео:

./Документы:

./Загрузки:create_minimal_image_moby.sh

./Изображения:2023-07-11_09-46.png

./Музыка:

./Общедоступные:

'./Рабочий стол':

./Шаблоны:test.sh  text.sh
```

Одним из главных преимуществ использования утилиты **tree** является ее способность отображать иерархическую структуру каталогов, что помогает быстро найти нужный файл или каталог. Кроме того, tree позволяет быстро создавать новые каталоги и файлы, а также копировать, перемещать и удалять файлы.

В отличие от команды **ls**, которая выводит список файлов и каталогов в текущей директории, **tree** позволяет просматривать содержимое всех подкаталогов и файлов в заданной директории.

tre-command - утилита для отображения структуры директорий

Установка
Синтаксис и опции
Примеры использования
Удаление

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: tre-command-0.4.0-1

Tre-command — консольная утилита для просмотра и управления файлами и директориями (современная альтернатива программе *tree*). По возможности использует git ls-файлы в качестве источника файла. Tre также может создавать псевдонимы оболочки, которые при запуске открывают связанный с ним файл в редакторе по умолчанию.

Основные функции:

- отображает структуру каталогов в виде древовидной диаграммы, как в классической версии tree;
- создает псевдонимы оболочки для каждого листинга, который открывает файлы;
- выводит структуру в цветах с учетом настроек.

Утилита *tre* полезна для быстрой и удобной навигации по файловой системе РЕД ОС.

Установка

Для установки утилиты через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install tre-command
```

Синтаксис и опции

Синтаксис программы выглядит следующим образом:

```
tre-command [<опции>] [<путь_к_директории>]
```

Опции утилиты:

- **-a, --all** — вывод всех файлов и каталогов;
- **-c, --color <ПАРАМЕТР>** — цвет выходных данных (automatic, always или never; автоматически означает, что tre будет включать цвета, в противном случае цвета будут отключены);
- **-d, --directories** — вывод только списка каталогов;
- **-e, --editor <КОМАНДА>** — создание псевдонима для отображаемого результата в файле /tmp/tre_aliases_$USE;
- **-E, --exclude <ШАБЛОН>** — исключение путей, соответствующих шаблону регулярного выражения;
- **-h, --help** — вывод справки;
- **-j, --json** — вывод JSON вместо древовидной диаграммы;
- **-l, --limit <ЛИМИТ>** — ограничение глубины вывода дерева файлов;
- **-p, --portable** — создание абсолютных путей для псевдонимов редактора, по умолчанию в псевдонимах используются относительные пути для повышения производительности;
- **-s, --simple** — обычный вывод файлов и каталогов;
- **-V, --version** — вывод версии программы.

Примеры использования

1. Для отображения только каталогов в виде дерева перейдите в нужную директорию и введите команду:

```
tre-command --directories
```

Результат выполнения команды:

```
[user@localhost Загрузки]$ cd candy-icons
[user@localhost candy-icons]$ ls
apps  devices  index.theme  LICENSE  mimetypes  places  preferences  preview  README.md  status
[user@localhost candy-icons]$ tre-command --directories
.
├── status
│   └── scalable
├── devices
│   └── scalable
├── preview
├── places
│   ├── 16
│   └── 48
├── mimetypes
│   └── scalable
├── preferences
│   └── scalable
└── apps
    └── scalable
[user@localhost candy-icons]$
```

2. Для отображения JSON, содержащего файлы в древовидной иерархии, вместо обычной древовидной диаграммы введите команду:

```
tre-command --json
```

```
[user@localhost preview]$ tre-command --json
{
  "type": "directory",
  "name": ".",
  "path": ".",
  "contents": [
    {
      "type": "file",
      "name": "folders.png",
      "path": "./folders.png"
    },
    {
      "type": "file",
      "name": "cli.png",
      "path": "./cli.png"
    },
    {
      "type": "file",
      "name": "candy.png",
      "path": "./candy.png"
    },
    {
      "type": "file",
      "name": "icons.png",
      "path": "./icons.png"
    }
  ]
}
```

3. Команда «tre-command -E "/*.svg"» использует опцию **--exclude** для исключения всех файлов или каталогов, пути которых соответствуют шаблону регулярного выражения "/*.svg".

```
tre-command -E "/*.svg"
```

```
[user@localhost Документы]$ tre-command
.
├── file1.svg
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
├── каталог1
└── file2.svg
[user@localhost Документы]$ tre-command -E "/*.svg"
.
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
└── каталог1
```

4. Для ограничения глубины вывода дерева введите команду с опцией **-l** и задайте лимит уровня вложенности:

```
tre-command -l 3
```

```
[user@localhost Документы]$ tre-command -l 1
.
├── каталог
└── каталог1
[user@localhost Документы]$ tre-command -l 2
.
├── каталог
│   ├── каталог1
│   └── каталог2
└── каталог1
[user@localhost Документы]$ tre-command -l 3
.
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
└── каталог1
```

5. Для отключения цветового оформления вывода файлов и каталогов введите команду:

```
tre-command -c never
```

```
[user@localhost Документы]$ tre-command -c never
.
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
└── каталог1
[user@localhost Документы]$
```

6. Для создания псевдонима отображаемого результата в файле /tmp/tre_aliases_$USE выполните команду:

```
tre-command --editor ['Copy_pass']
```

```
[user@localhost Документы]$ tre-command --editor ['Copy_pass']
[0] .
├── [1] каталог
│   ├── [2] каталог1
│   │   ├── [3] file1
│   │   └── [4] file2
│   └── [5] каталог2
└── [6] каталог1
```

В файл /tmp/tre_aliases_$USE будет записан следующий результат:

```
 GNU nano 7.2                                          tre_aliases_user
alias e0="eval '[Copy_pass] \".\"'"
alias e1="eval '[Copy_pass] \"./каталог\"'"
alias e2="eval '[Copy_pass] \"./каталог/каталог1\"'"
alias e3="eval '[Copy_pass] \"./каталог/каталог1/file1\"'"
alias e4="eval '[Copy_pass] \"./каталог/каталог1/file2\"'"
alias e5="eval '[Copy_pass] \"./каталог/каталог2\"'"
alias e6="eval '[Copy_pass] \"./каталог1\"'"
```

7. Для исключения определенных файлов или директорий при использовании команды *tre-command* можно использовать опцию **--exclude**. Например, если нужно исключить файлы или директории с именем "**каталог2**", можно использовать следующую команду:

```
tre-command --exclude "каталог2"
```

Результат:

```
[user@localhost Документы]$ tre-command --exclude "каталог2"
.
├── каталог
│   └── каталог1
│       ├── file1
│       └── file2
└── каталог1
```

8. Можно также указать несколько исключений, разделяя их запятыми или используя опцию **--exclude** несколько раз, если нужно исключить более одного элемента. Например:

```
tre-command --exclude "каталог2" --exclude "каталог1"
```

```
[user@localhost Документы]$ tre-command --exclude "каталог2" --exclude "каталог1"
.
└── каталог
```

9. Также можно использовать несколько опций. Например, для вывода древовидной диаграммы всех файлов и каталогов в текущей директории с использованием цветов введите команду:

```
tre-command -a -c always
```

```
[user@localhost Документы]$ tre-command -a -c always
.
├── file1.svg
├── каталог
│   ├── каталог1
│   │   ├── file1
│   │   └── file2
│   └── каталог2
├── каталог1
└── file2.svg
```

10. Вывести только список каталогов без использования цветового оформления:

```
tre-command -d -c never
```

```
[user@localhost Документы]$ tre-command -d -c never
.
├── каталог
│   ├── каталог1
│   └── каталог2
└── каталог1
```

11. Исключить все файлы и каталоги, пути которых содержат слово "**/каталог**" и вывести JSON вместо древовидной диаграммы:

```
tre-command -E "/каталог" -j
```

```
[user@localhost Документы]$ tre-command -E "/каталог" -j
{
  "type": "directory",
  "name": ".",
  "path": ".",
  "contents": [
    {
      "type": "file",
      "name": "file1.svg",
      "path": "./file1.svg"
    },
    {
      "type": "file",
      "name": "file2.svg",
      "path": "./file2.svg"
    }
  ]
}
```

12. Создать псевдоним для отображаемого результата в файле /tmp/tre_aliases и использовать абсолютные пути для псевдонимов редактора:

```
tre-command -e "emacs" -p
```

```
[user@localhost Документы]$ tre-command -e "emacs" -p
[0] .
├── [1] file1.svg
├── [2] каталог
│   ├── [3] каталог1
│   │   ├── [4] file1
│   │   └── [5] file2
│   └── [6] каталог2
├── [7] каталог1
└── [8] file2.svg
```

Удаление

Для удаления утилиты *tre-command* можно использовать следующую команду:

```
dnf remove tre-command
```

zoxide - легкая навигация по каталогам

Установка утилиты
Запуск и настройка утилиты
Возможности утилиты
Основные опции утилиты
Основные команды утилиты

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zoxide-0.9.4-1

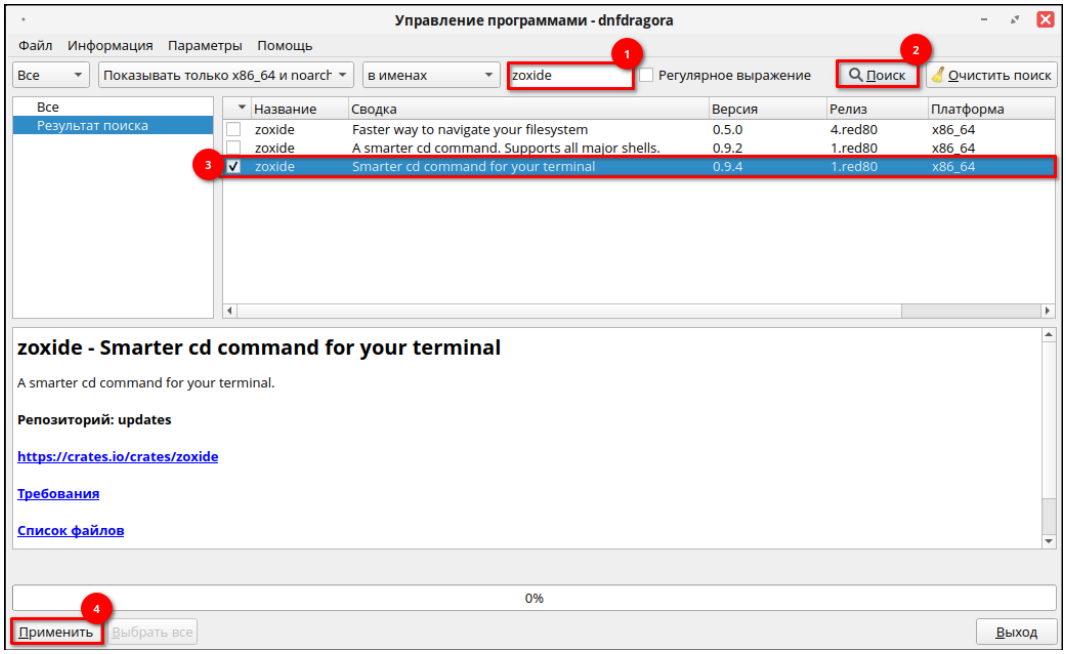
Zoxide — это удобная утилита командной строки, предоставляющая легкую навигацию по каталогам. Она является альтернативой команде **cd**, но с дополнительными возможностями и улучшениями.

Zoxide помогает быстро перемещаться между каталогами с помощью интеллектуального алгоритма запоминания путей. Утилита отслеживает каталоги, которые пользователь использует чаще всего, и применяет алгоритм ранжирования для перехода к лучшему совпадению. Алгоритм ранжирования подразумевает создание рейтинга для каталогов путем отслеживания посещений. При каждом новом посещении каталога его рейтинг будет увеличен на 1. Чем выше рейтинг, тем больше вероятность использования данного каталога как наилучшего совпадения.

Установка утилиты

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**zoxide**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install zoxide
```

Запуск и настройка утилиты

Для использования утилиты **zoxide** введите команду, которая применяется для настройки автоматической интеграции программы с оболочкой командной строки:

```
zoxide init bash
```

При успешной интеграции в ответе команды будет выведено сообщение с рекомендациями по инициализации **zoxide** вида:

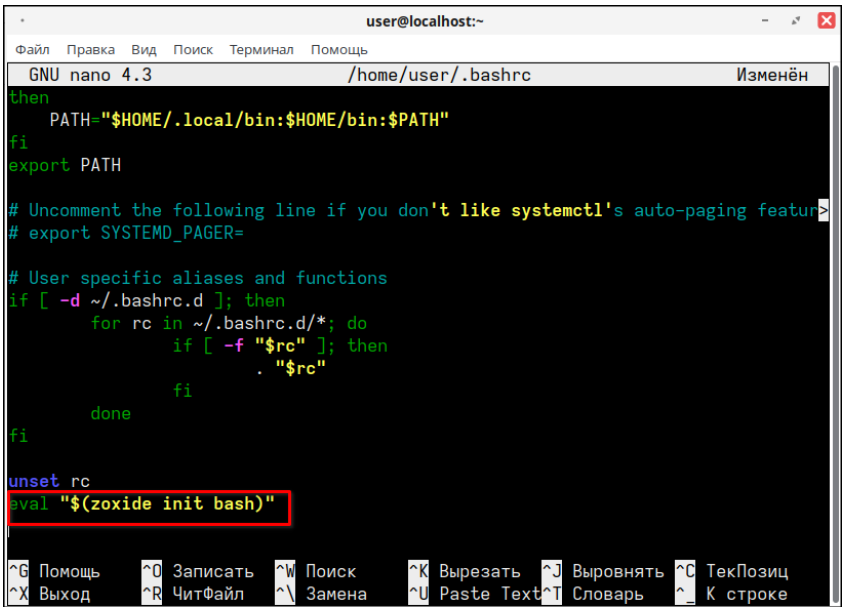
```
# To initialize zoxide, add this to your configuration (usually ~/.bashrc):
#
# eval \"$(zoxide init bash)\""
```

Для автоматической активации **zoxide** при запуске нового терминала в конец файла **~/.bashrc** определенного пользователя добавьте указанную выше строку:

```
eval "$(zoxide init bash)"
```

Файл **~/.bashrc** является скриптом настроек, который выполняется каждый раз, когда пользователь запускает новый терминал или интерактивную сессию **Bash**. В этом файле можно определить переменные среды, настроить псевдонимы команд, добавить функции и выполнить другие настройки, которые должны быть применены при запуске оболочки. Открыть файл можно с помощью команды:

```
nano ~/.bashrc
```



Для применения внесенных изменений перезагрузите файл настроек с помощью команды:

```
source ~/.bashrc
```

Изменения в файле **~/.bashrc** будут применены немедленно, и станет доступно использование новых переменных, псевдонимов и других настроек.

Возможности утилиты

Zoxide предлагает ряд полезных возможностей для удобной навигации по каталогам. Для быстрого перехода в часто посещаемый каталог, вместо полного указания пути к каталогу, можно использовать команду **z** в сочетании с частью имени каталога.

Рассмотрим пример создания символьной ссылки на каталог «**/home/user/**», для быстрого перехода к нему с помощью команды **z**.

1. Откройте терминал.
2. Перейдите в нужный каталог (в примере «**/home/user/**»):

   ```
   cd /home/user/
   ```

3. Создайте символьную ссылку с именем doc на каталог «**/home/user/**»:

   ```
   ln -s /home/user/ doc
   ```

4. Теперь для перехода в каталог «**/home/user/**» можно использовать команду:

```
z doc
```

Утилита **zoxide** считает символьную ссылку и перейдет в каталог «**/home/user/**».

> **Примечание.**
>
> Прежде чем использовать псевдонимы и команды, связанные с утилитой **zoxide**, выполните настройку утилиты, как показано в предыдущем пункте Запуск и настройка утилиты.

Zoxide запоминает посещенные пользователем каталоги и предлагает наиболее вероятные варианты для перехода, что позволяет быстро перемещаться между часто используемыми каталогами.

Zoxide автоматически обновляет историю переходов между сеансами, что позволяет сохранять состояние навигации между различными запусками терминала. Данная возможность позволяет не производить заново настройку утилиты.

Основные опции утилиты

Утилита имеет всего две опции:

-h, --help — выводит справку по использованию zoxide, включая доступные команды, опции и переменные среды;

-V, --version — выводит версию Zoxide.

Основные команды утилиты

Zoxide add — добавляет новый каталог в базу данных **zoxide** или увеличивает его рейтинг, если каталог уже существует в базе данных. Для добавления каталога в базу данных используйте команду вида:

```
zoxide add <имя_каталога>
```

Например:

```
zoxide add Документы
```

После выполнения вышеприведенной команды каталог «**/Документы**» будет добавлен в базу данных **zoxide** с начальным рейтингом 1. Если каталог уже существует в базе данных, его рейтинг будет увеличен на 1.

Zoxide query — позволяет найти каталог в базе данных.

Чтобы убедиться, что каталог был добавлен в базу данных, выполните команду **zoxide query <имя каталога>**:

```
zoxide query Документы
```

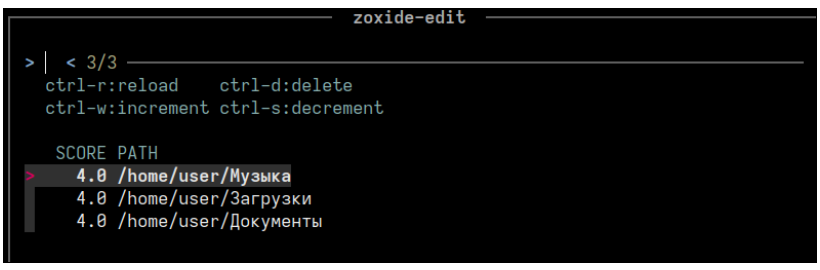
В терминале отобразится искомый каталог, добавленный в базу данных.

Также можно увидеть вывод, содержащий информацию о каталоге «**Документы**» и его ранге, если выполнить команду вместе с ключом **-s, -- score**:

```
zoxide query -s Документы
```

Zoxide edit — позволяет редактировать базу данных **zoxide** вручную. После выполнения команды откроется текстовый редактор, в котором можно изменить имя или теги каталога «**/Документы**». Доступно добавление, удаление и изменение записей в БД:

```
zoxide edit
```



Если текстовый редактор не открывается и появляется сообщение вида: «**zoxide: could not find fzf, is it installed?**», необходимо установить утилиту **fzf**.

Для установки утилиты выполните команду (потребуются права **администратора**):

```
sudo dnf install fzf
```

Zoxide import — импортирует записи из других приложений или инструментов для управления историей каталогов. Может быть полезно, если у вас уже есть существующая история каталогов, которую необходимо использовать с **zoxide**.

Предположим, существует файл с именем «**file.txt**», содержащий список каталогов, которые требуется импортировать в историю каталогов **zoxide**.

Выполните команду *zoxide import*, указав путь к файлу «**file.txt**», чтобы импортировать каталоги из файла в историю:

```
zoxide import /путь/к/файлу/file.txt
```

Zoxide init — создает конфигурацию оболочки для **zoxide**.

```
zoxide init <значение>
```

Допустимые значения: *bash*, *elvish*, *fish*, *nushell*, *posix*, *powershell*, *xonsh*, *zsh*.

- **Для bash:**

Откройте файл конфигурации (обычно **~/.bashrc**):

```
vim ~/.bashrc
```

Добавьте строку в конец файла:

```
eval "$(zoxide init bash)"
```

- **Для elvish:**

Откройте файл конфигурации (обычно **~/.elvish/rc.elv**):

```
vim ~/.elvish/rc.elv
```

Добавьте строку в конец файла:

```
"eval $(zoxide init elvish | slurp)"
```

- **Для fish:**

Откройте файл конфигурации (обычно **~/.config/fish/config.fish**):

```
vim ~/.config/fish/config.fish
```

Добавьте строку в конец файла:

```
zoxide init fish | source
```

- **Для nushell**:

Найдите файл конфигурации, выполнив команду в Nushell:

```
config path
```

Добавьте к нему строку ниже.

```
startup = ["zoxide init nushell --hook prompt | save ~/.zoxide.nu", "source ~/.zoxide.nu"]
```

- **Для posix**:

Добавьте строку в конец файла:

```
eval "$(zoxide init posix --hook prompt)"
```

- **Для powershell**:

Добавьте в конец файла конфигурации (найдите его, запустив echo $profile в PowerShell):

```
Invoke-Expression (& { (zoxide init powershell | Out-String) })
```

- **Для xonsh**:

Откройте файл ниже для редактирования (обычно ~/.xonshrc):

```
vim ~/.xonshrc
```

Добавьте строку в конец файла:

```
execx($(zoxide init xonsh), 'exec', __xonsh__.ctx, filename='zoxide')
```

- **Для zsh:**

Откройте файл для редактирования (обычно ~/.zshrc):

```
$ vim ~/.zshrc
```

Добавьте к нему строку ниже.

```
eval "$(zoxide init zsh)"
```

Zoxide remove — удаляет каталог из базы данных zoxide:

```
zoxide remove Документы
```

После удаления каталога из базы данных выполните команду «**zoxide query Документы».** Если каталог был удален, появится сообщение вида: «**no match found**».

Atril - универсальный просмотрщик документов

Установка
Основные функции программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: atril-1:1.26.0-11

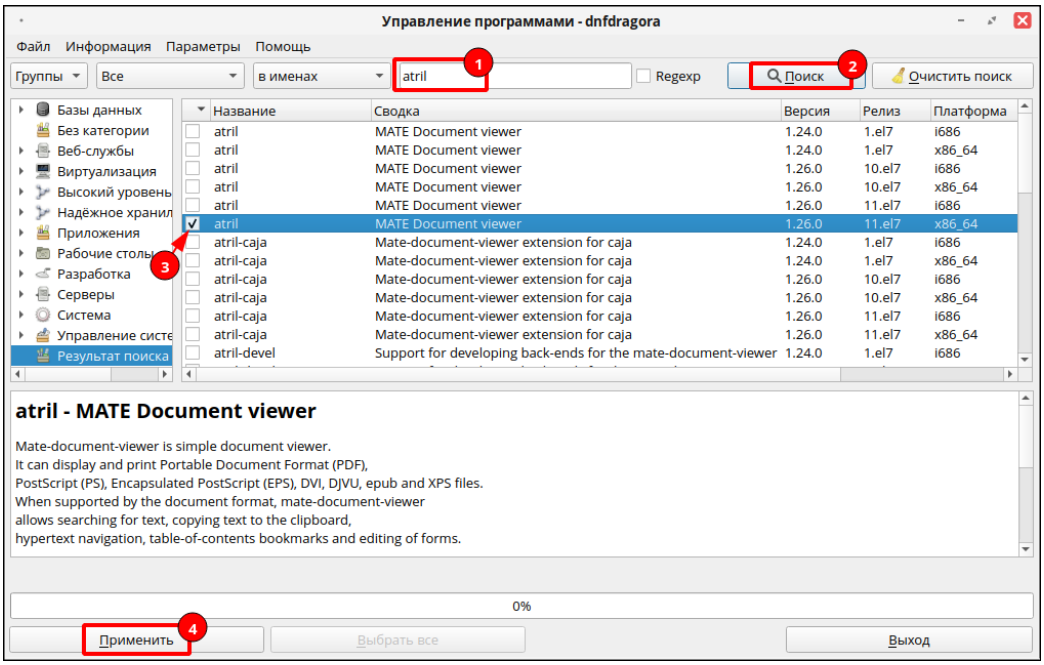
Atril — универсальное графическое приложение для просмотра электронных документов различных форматов, таких как: **PDF**, **Postscript** (PS), **TIFF**, **DVI**, **DjVu**, **CBR**, **XPS** и пр. Для форматов **PDF** и **DVI** поддерживается поиск текста, копирование фрагментов текста в буфер обмена, гипертекстовая навигация.

Atril имеет простой пользовательский интерфейс и интегрирован в рабочую среду MATE, но также может использоваться и в других графических окружениях.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**atril**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install atril
```

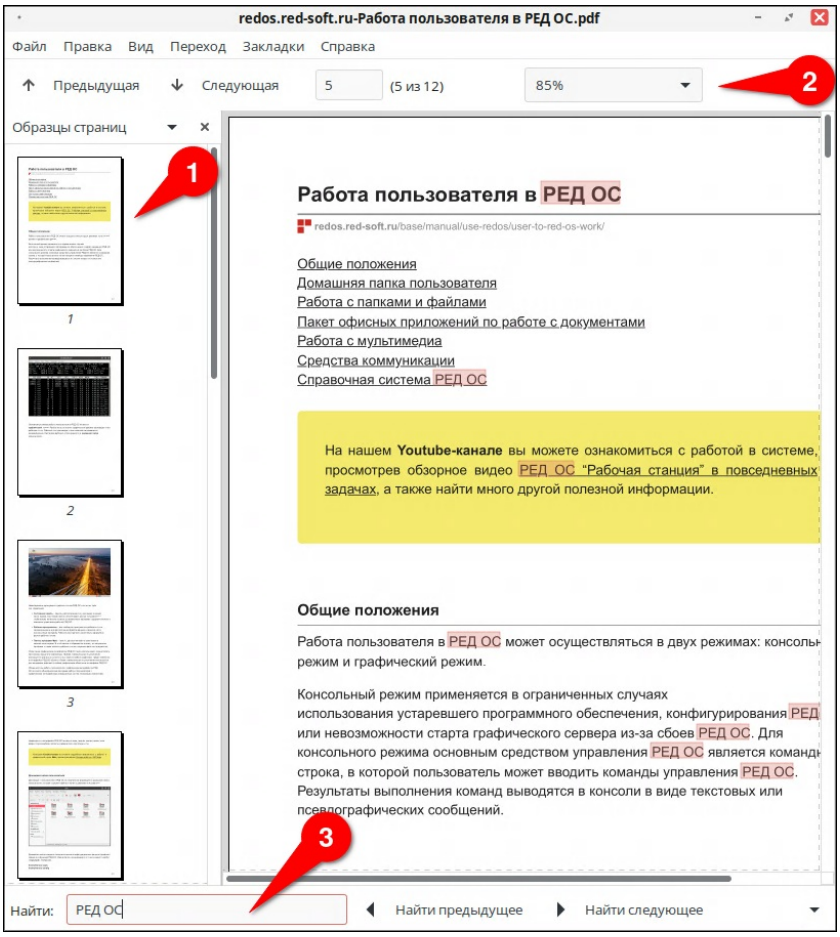
Дальнейшая работа в программе выполняется от **локального** пользователя.

После установки программа будет доступна из «**Главного меню**» - «**Офис**» - «**Просмотрщик документов**».

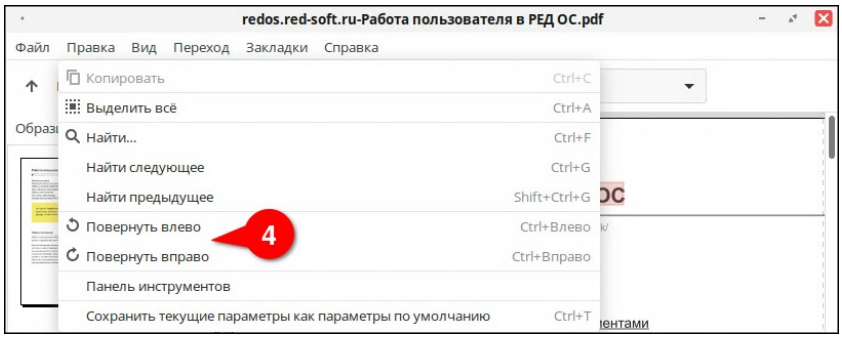
Основные функции программы

Atril может отображать миниатюры страниц, облегчающие навигацию при просмотре документов большого объёма (**1**).

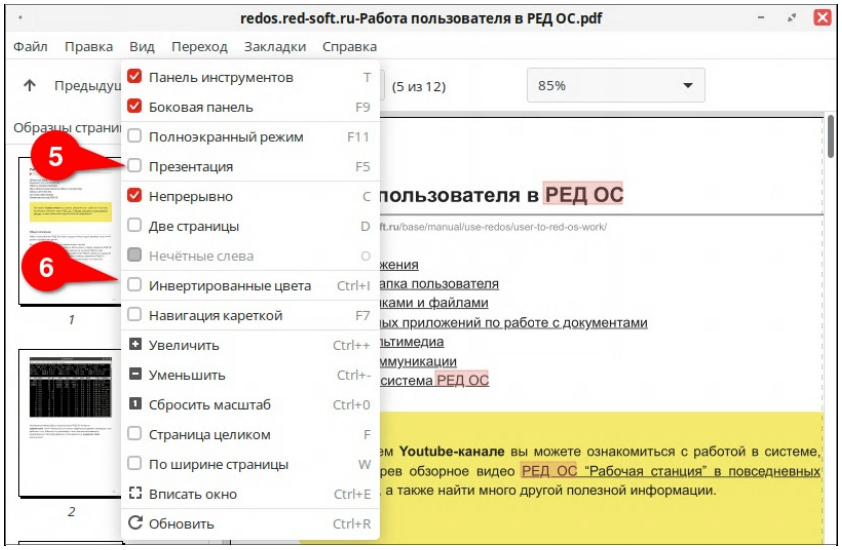
Поддерживается масштабирование (**2**) и поворот страницы (**4**), одно-страничный и двух-страничный просмотр.



Функция поиска по тексту документа (**3**) вызывается сочетанием клавиш *Ctrl+F*. Программа показывает количество найденных результатов, подсвечивая их на странице.



Имеется возможность просмотра документа в режиме презентации (**5**), а также поддерживается функция инвертирования цвета (**6**).



Okular - универсальный просмотрщик документов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: okular-20.08.1-1

Okular – это программа с открытым исходным кодом для просмотра различных типов документов с широким набором функций. Позволяет подключать дополнительные модули, за счёт чего расширять список поддерживаемых форматов файлов.

Основные возможности **okular**:

- Просмотр документов – поддерживает широкий спектр форматов документов, включая **PDF**, **PostScript**, **DjVu**, **EPub** и другие, что позволяет просматривать различные типы документов без необходимости установки различных специализированных программ.
- Навигация и масштабирование – предоставляет различные инструменты для удобной навигации по документам, включая возможность быстрого перехода к определенной странице или разделу. Также имеется функция масштабирования, позволяющая увеличивать или уменьшать изображение для более удобного чтения.
- Закладки и аннотации – пользователи могут добавлять закладки к интересующим страницам и создавать аннотации, чтобы отмечать важные места или добавлять комментарии в документы. Это полезные функции для обозначения ключевых моментов или для совместной работы над документами.
- Настройки и расширения – предоставляет множество настроек для более тонкой настройки программы.

Для установки **okular** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install okular
```

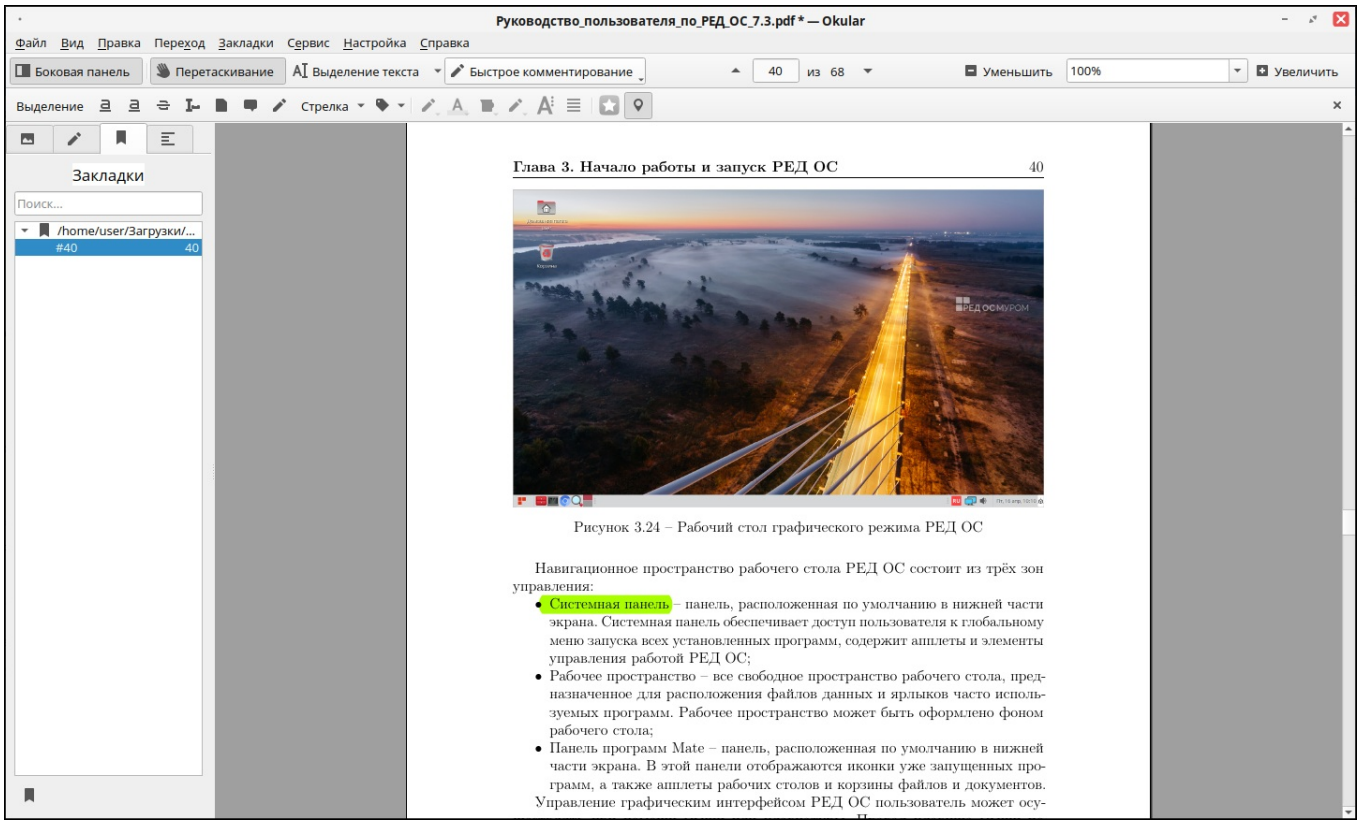
Дальнейшая работа в программе производится с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

После установки запуск программы доступен из «**Главного меню**» — «**Офис**» — «**Okular**» или через терминал (с правами **непривилегированного** пользователя) командой:

```
okular
```

Главное окно программы выглядит следующим образом:



В верхней части окна расположено **основное меню**, где доступны все действия для работы и настройки программы.

Ниже расположена **панель инструментов**, с помощью которой можно показать/скрыть боковую панель, выбрать действие по нажатии ЛКМ – перетаскивать (прокручивать) файл или выделить текст, также здесь доступно быстрое комментирование, переход к нужной странице файла и настройка масштаба страницы.

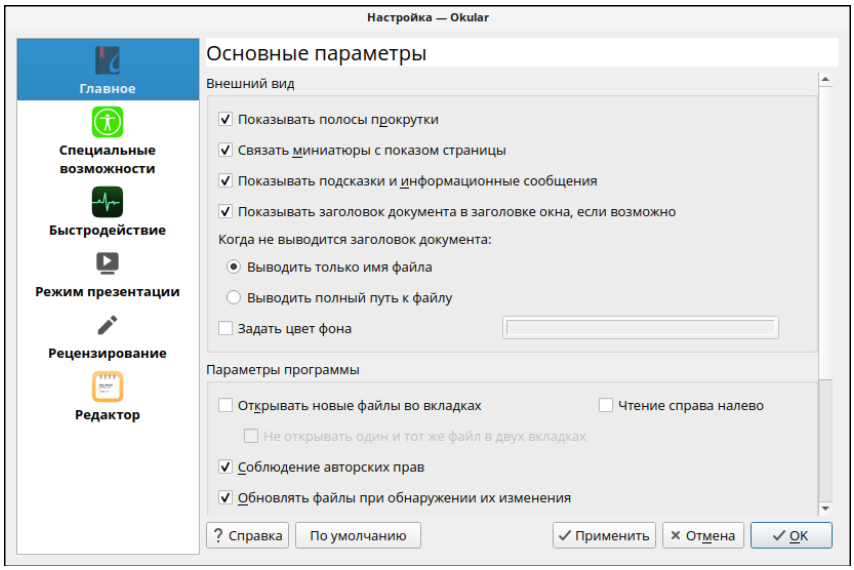
На **панели инструментов** расположены дополнительные инструменты для внесения правок в файл – подчеркивание текста прямой и волнообразной линией, зачеркивание текста, добавление встроенных и висящих заметок, добавление произвольных линий, стрелок и штампов, а также настройка цвета, заливки, текста добавляемых комментариев и линий.

Слева расположена боковая панель, на которой есть несколько вкладок:

- *миниатюры* – отображаются миниатюры открытого файла;
- *рецензирование* – отображаются внесенные в файл корректировки и комментарии, а также имя пользователя, который их внес;
- *закладки* – отображаются добавленные закладки;
- *содержание* – вкладка становится доступна, если в открытом файле существуют заголовки.

Через пункт меню «**Настройка**» можно настроить язык программы, комбинации клавиш для удобства работы, отображаемые панели инструментов и их содержимое, а также дополнительные модули.

Для настройки непосредственно программы **Okular** выберите «**Настройка**» – «**Настроить Okular**». Будет открыто окно редактирования основных параметров программы, специальных возможностей, быстродействия, режима презентации, режима рецензирования и редактора.


Настройка — Okular
Главное
Специальные возможности
Быстродействие
Режим презентации
Рецензирование
Редактор
Основные параметры
Внешний вид
Показывать полосы прокрутки
Связать миниатюры с показом страницы
Показывать подсказки и информационные сообщения
Показывать заголовок документа в заголовке окна, если возможно
Когда не выводится заголовок документа:
Выводить только имя файла
Выводить полный путь к файлу
Задать цвет фона
Параметры программы
Открывать новые файлы во вкладках
Чтение справа налево
Не открывать один и тот же файл в двух вкладках
Соблюдение авторских прав
Обновлять файлы при обнаружении их изменения
Справка
По умолчанию
Применить
Отмена
OK

Создание скриншотов с помощью Flameshot

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** flameshot-12.1.0-2

FlameShot — мультиплатформенный инструмент для создания скриншотов. Эта небольшая программа предлагает дополнительные возможности для быстрого редактирования скриншотов. Скриншоты можно создавать и стандартными средствами системы. Для этого достаточно нажать клавишу Print Screen, после чего скриншот будет сохранен в папке с изображениями.

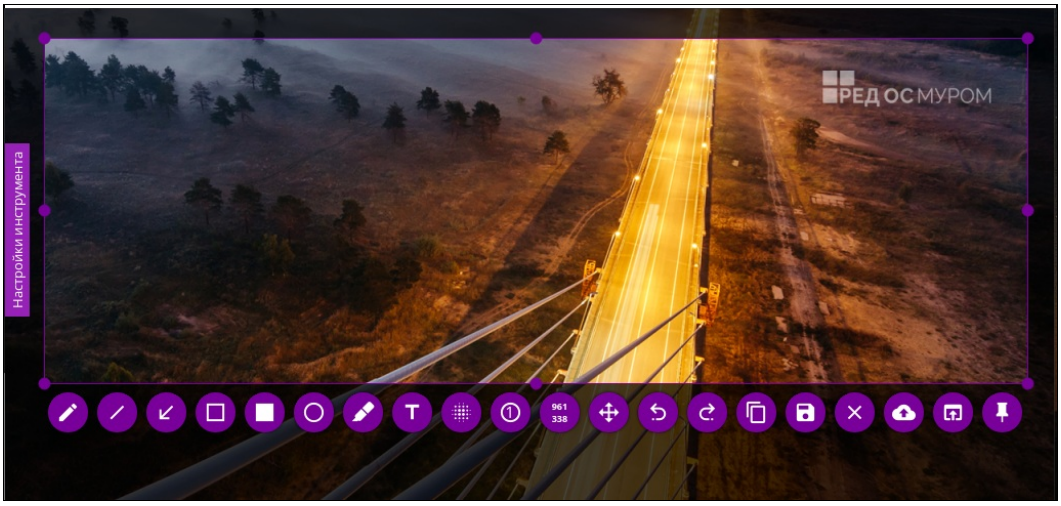
Однако главное преимущество **FlameShot** — возможность захвата выделенной области экрана и добавление к ней различных выделений и указателей. Это может быть особенно полезным для создания онлайн-инструкций.

Данная программа по умолчанию установлена в РЕД ОС.

Примечание.

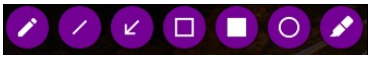
Обратите внимание, что **FlameShot** не предусмотрен для использования в графических окружениях **GNOME** и **KDE Plasma**. Корректная работа программы гарантируется только при использовании графического окружения **MATE**.

Для запуска **Flameshot**, откройте системное *"Меню"* — *"Графика"* — *"Flameshot"*. После запуска программы, чтобы сделать скриншот, нажмите на значок **Flameshot** в системном трее. Выделите нужную часть экрана и можете приступать к редактированию.



Возможности программы

Для удобной работы со снимками экрана FlameShot имеет ряд полезных функций:

 — Инструменты для изменения рисунка: карандаш, маркер, фигуры, прямоугольное выделение.

 — Вставка текста.

 — Размытие изображения.

 — Метки с увеличивающимся цифровым счетчиком.

 — Показывает размер выделения.

 — Модуль перемещения изображения по экрану.

 — Повторить/отменить последнее изменение.

 — Скопировать изображение в буфер обмена.

 — Сохранить снимок.

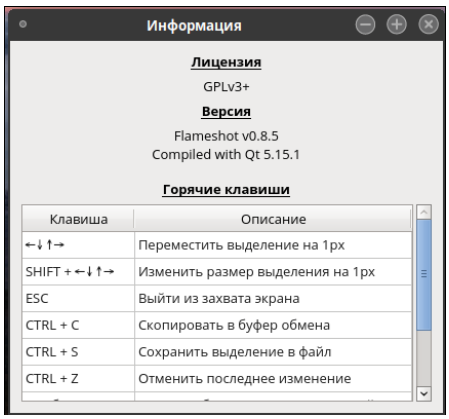
— Покинуть захват экрана.

— Загрузить изображение в Imgur (Imgur - программное обеспечение для загрузки, обмена и хранения фотографий и картинок).

— Выбор приложения для открытия снимка.

— Прикрепить изображение к рабочему столу.

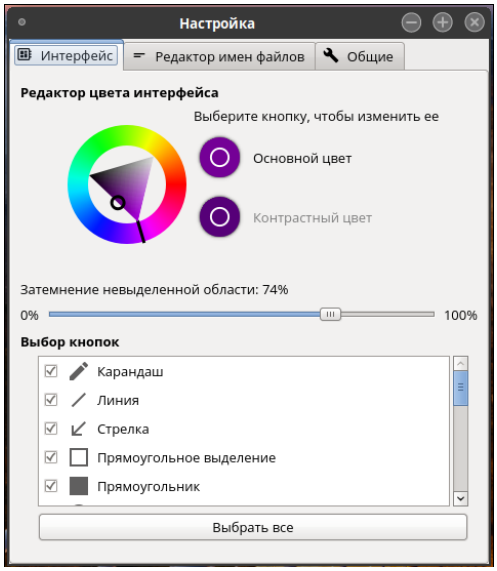
Для просмотра списка горячих клавиш щёлкните ПКМ по значку и выберите в контекстном меню пункт **«Информация»**.



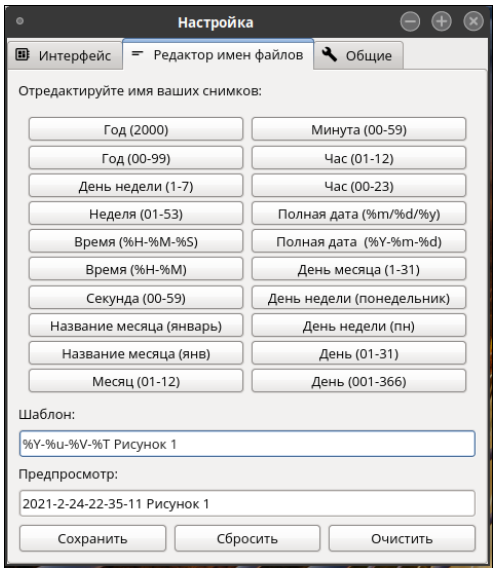
Пользовательские настройки Flameshot

Для изменения настроек щёлкните ПКМ по значку и выберите в контекстном меню пункт **«Настройка»**. На вкладке **«Интерфейс»** доступны настройки:

- Изменение цвета интерфейса;
- Настройка отображения кнопок.



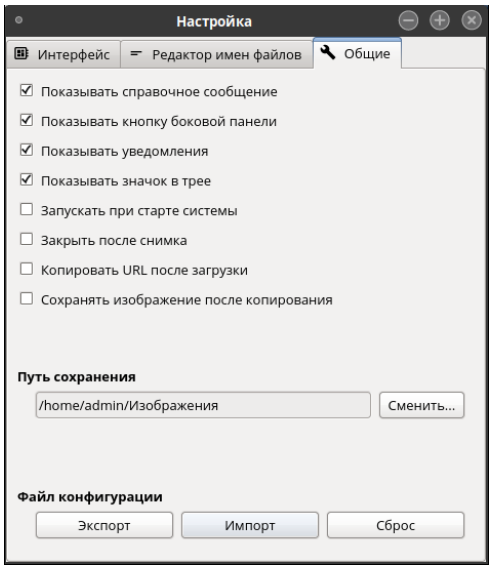
На вкладке **«Редактор имен файлов»** вы можете составить шаблон имени создаваемых файлов.



На вкладке **«Общие»** доступны настройки:

- Включение/отключение простейших функций;
- Путь сохранения файла;
- Экспорт/импорт файла конфигурации.

На вкладке **«Общие»** вы можете настроить простейшие функции, путь сохранения файлов, а также загрузить готовый конфигурационный файл.



Создание скриншотов с помощью kSnip

Установка
Основные возможности
Работа в ksnip через терминал
Расширенная настройка

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ksnip-1.10.1-1

Ksnip — это кроссплатформенная программа для создания скриншотов. Она включает в себя такие функции редактирования скриншотов, как добавление аннотаций и графических элементов, а также размытие областей.

Вы можете подробнее ознакомиться с работой в **kSnip**, просмотрев наши обучающие видео:

- на **RuTube** — Делаем скриншоты в РЕД ОС. Ksnip;
- в **Яндекс.Дзен** — Делаем скриншоты в РЕД ОС. Ksnip;
- в **VK Видео** — Делаем скриншоты в РЕД ОС. Ksnip.

На наших каналах вы также сможете найти много другой полезной информации.

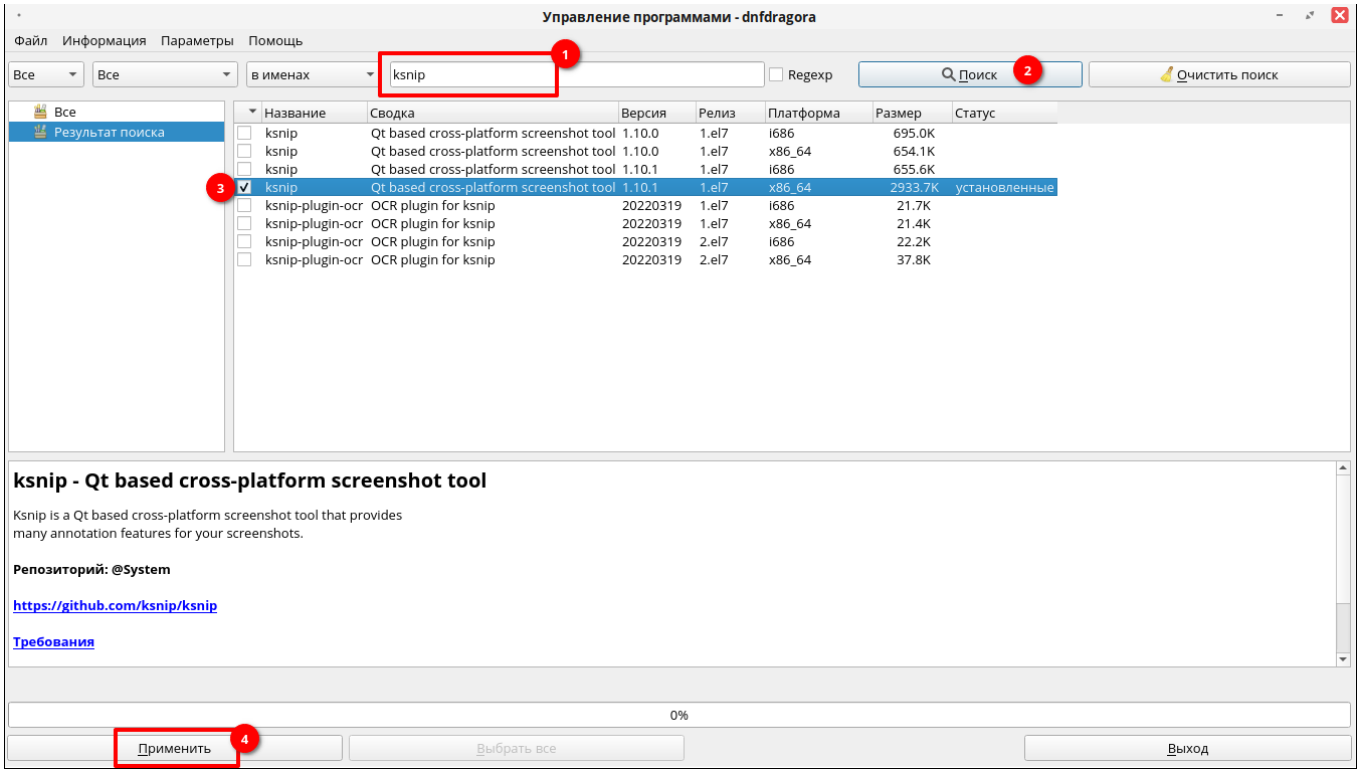
Примечание.

Обратите внимание, что **ksnip** не предусмотрена для использования в графическом окружении **GNOME**.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**ksnip**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки через терминал необходимо перейти в сеанс пользователя **root**:

```
su -
```

и выполнить команду:

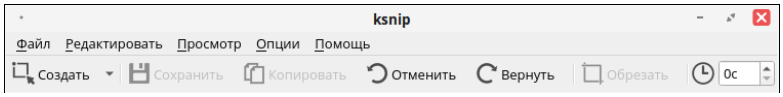
```
dnf install ksnip
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки запустить программу можно через «**Меню**» - «**Стандартные**» - «**Снимки экрана kSnip**».

Основные возможности

При открытии программы появляется компактная панель.



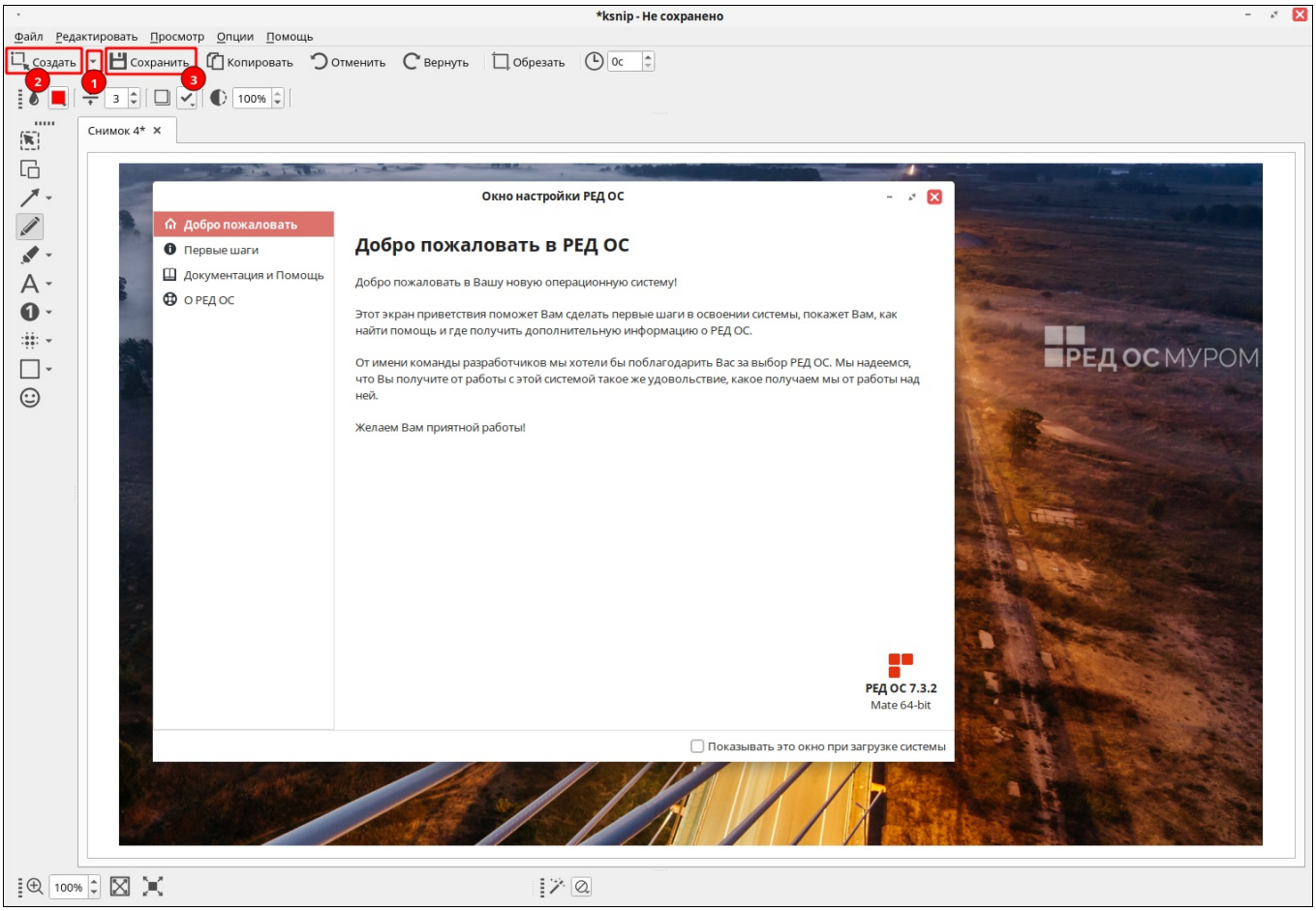
Основные функции программы **ksnip**:

- создание скриншотов различных областей экрана;
- создание скриншотов активного окна;
- создание скриншотов экрана целиком;
- создание скриншотов всех экранов;
- установка времени задержки перед созданием скриншота;
- добавление графических элементов: надписей, стрелок, счётчиков и др.;
- автоматическая загрузка скриншотов на сервис imgur.com, включая анонимный режим;
- поддержка командной строки;
- автоматическое сохранение скриншотов в заданную директорию;
- автоматическое копирование скриншотов в буфер обмена;
- печать скриншотов и экспорт в PDF/PS.

Ksnip позволяет создавать скриншоты различных областей экрана:

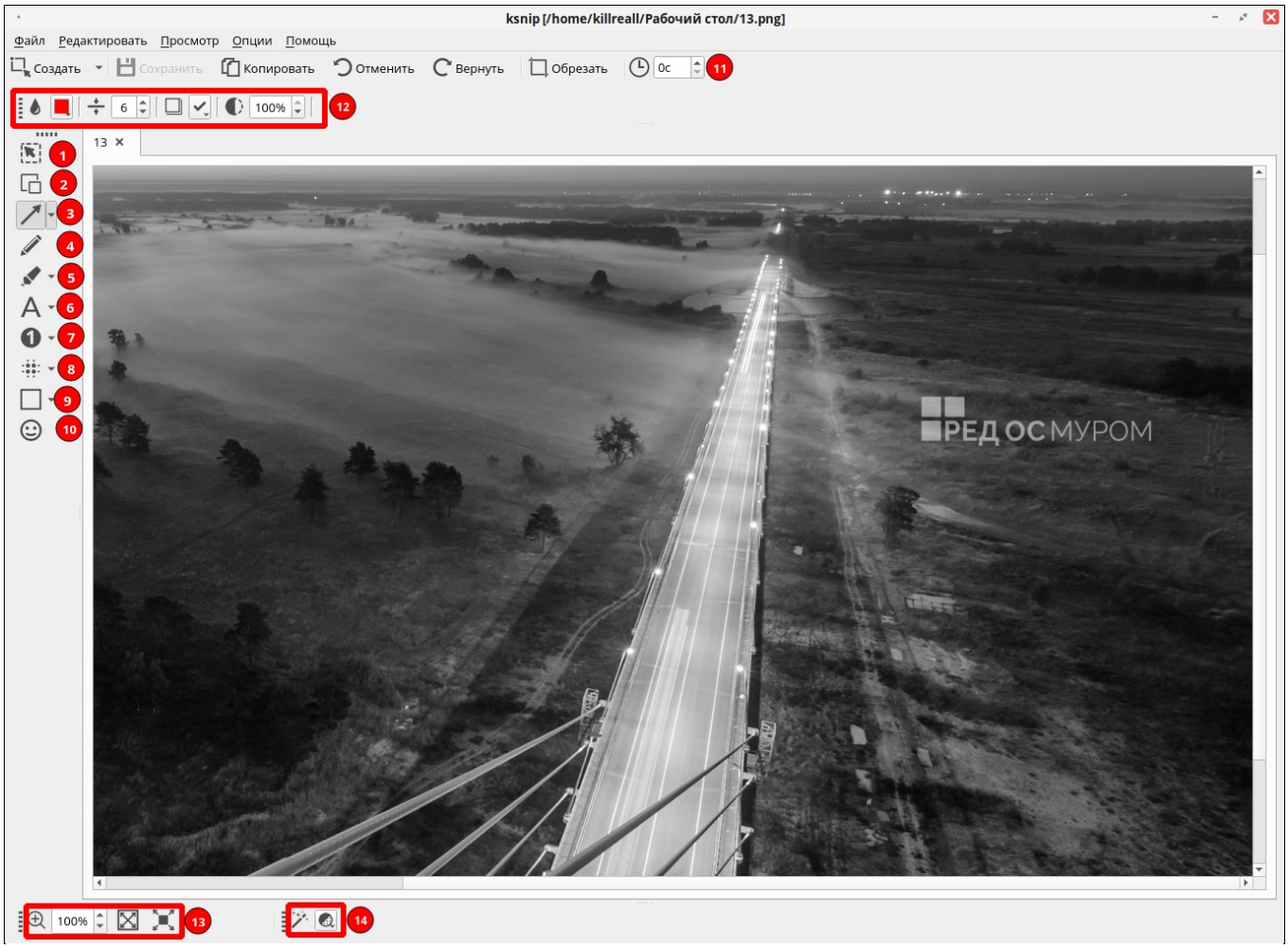
- **Произвольная прямоугольная область.** Скриншот прямоугольной области, размер которой определяет сам пользователь.
- **Текущий экран.** Скриншот всего рабочего стола.
- **Полноэкранный режим.** Скриншот всех мониторов.
- **Активное окно.** Скриншот отдельного окна.

В **ksnip** есть возможность выбирать тип создаваемого скриншота (1). Для создания скриншота нажмите кнопку «**Создать**» (2). При необходимости сохраните полученный скриншот (3).



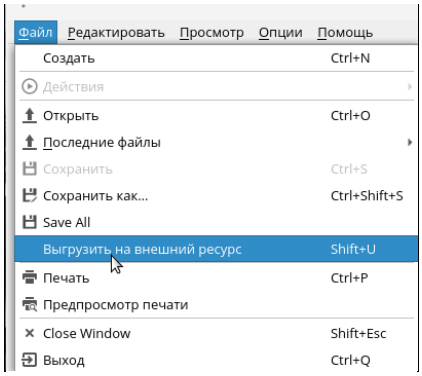
Ksnip обладает целым рядом инструментов для добавления аннотаций и графических элементов:

- Инструмент «**Выбор**» (1) позволяет выделять созданные графические элементы на скриншоте;
- Инструмент «**Дублирование**» (2) позволяет скопировать выделенную область на скриншоте и использовать её в качестве отдельного элемента;
- Добавление стрелок и линий (3);
- Произвольное рисование карандашом (4), линия имеет эффект сглаживания, степень сглаживания можно задать в настройках;
- Элемент «**Маркер**» (5);
- Добавление надписей (6);
- Добавление нумерованных счётчиков (7);
- Размытие областей на скриншоте (8);
- Добавление прямоугольников и окружностей (9);
- Добавление стикеров (10);
- Таймер для установки задержки времени перед созданием скриншота (11);
- Панель настройки выбранного инструмента (12);
- Масштабирование (13);
- Графические эффекты (14).

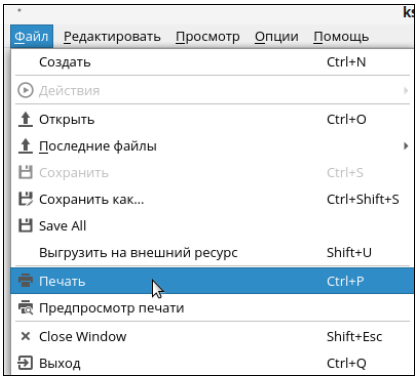


Скриншот может быть автоматически скопирован в буфер обмена и/или сохранен в заданную директорию. Также можно установить задержку создания скриншота по времени.

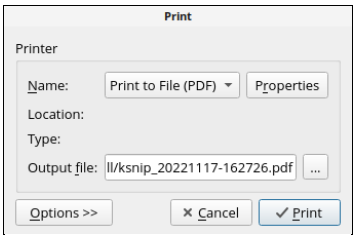
Для выгрузки на внешний ресурс есть соответствующий пункт в меню «**Файл**».



Скриншот также можно отправить на печать.

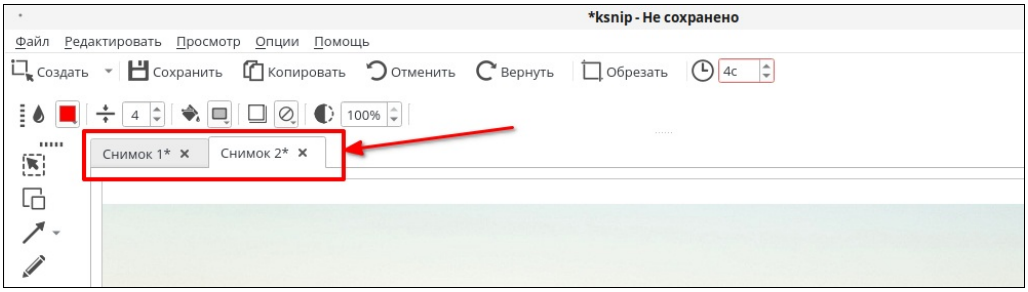


Через функцию печати можно осуществить экспорт скриншота **в формат PDF**.



Дополнительные особенности:

- Если при открытом скриншоте создать новый, то появится новая вкладка в основном рабочем поле. После этого можно перемещаться между несколькими скриншотами.



- Программа сохраняет изображения до тех пор, пока не будет закрыта в системном трее.

Работа в ksnip через терминал

Программа **ksnip** поддерживает режим работы в терминале. Ниже приведены основные команды для работы.

Запуск выполняется командой:

```
ksnip
```

Вывод справочной информации:

```
ksnip --help
```

Вывод текущей версии приложения:

```
ksnip -v
```

Запуск выбора области скриншота:

```
ksnip -r
```

Создание скриншота в полноэкранном режиме, включая все мониторы:

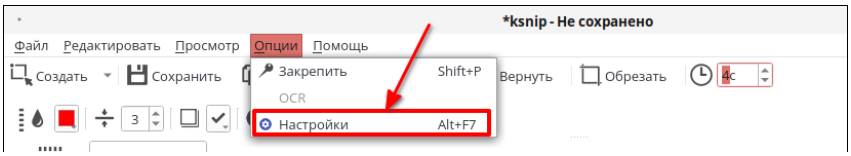
```
ksnip -f
```

Сохранение скриншота в каталоге по умолчанию без открытия в редакторе:

```
ksnip -s
```

Расширенная настройка

В **ksnip** можно произвести более детальную настройку программы.



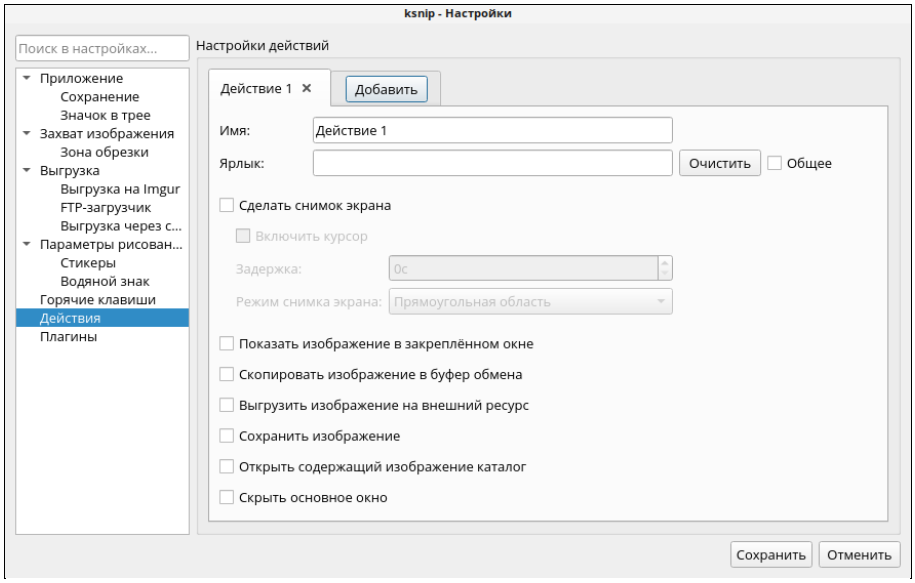
Например, можно настроить использование горячих клавиш для более удобной и практичной работы.

По умолчанию конфигурация горячих клавиш представлена следующим образом:

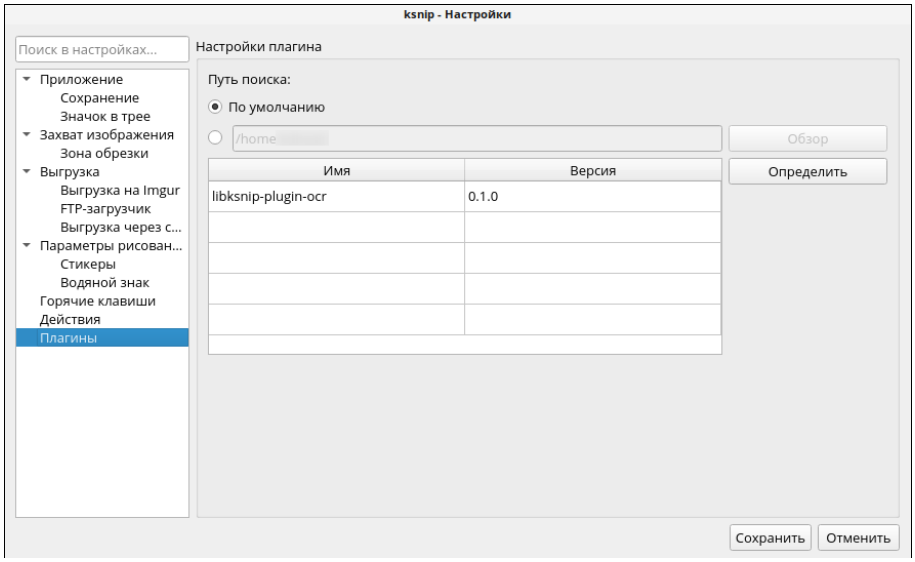
- снимок выделенной области: **Alt+Shift+R**.
- снимок последней области: **Alt+Shift+L**.
- снимок всего экрана: **Alt+Shift+F**.
- снимок текущего экрана: **Alt+Shift+C**.
- снимок активного окна: **Alt+Shift+A**.

Можно настраивать **Действия**.

Действие – это своеобразный шаблон с предустановленными пользовательскими настройками. Оно позволяет оптимизировать и упростить создание скриншотов.



Таже в **ksnip** поддерживается функция добавления плагинов.



Создание скриншотов с помощью mate-screenshot

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: mate-screenshot-1.28.0

Вы можете подробнее ознакомиться с созданием скриншотов и возможностью записи видео с экрана, просмотрев наши обучающие видео:

- на **RuTube** — Запись видео с экрана;
- в **Яндекс.Дзен** — Запись видео с экрана.

На наших каналах вы также сможете найти много другой полезной информации.

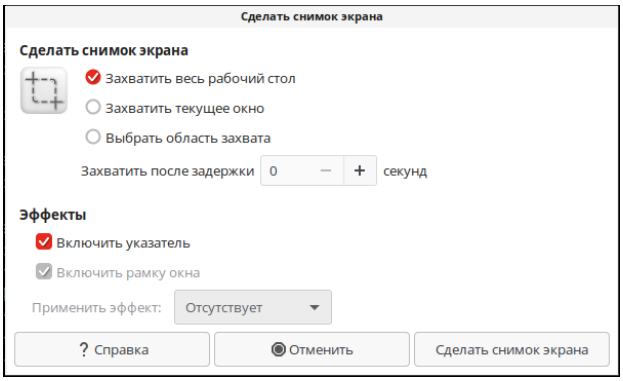
Для установки программы выполните команду:

```
dnf install mate-screenshot
```

Все снимки экрана сохраняются в папку **/home/<пользователь>/Изображения**.

Видео-файлы сохраняются в каталог **/home/<пользователь>/**.

Графический интерфейс программы доступен из «**Главного меню**» - «**Стандартные**» - «**Сделать снимок экрана**».



Горячие клавиши РЕД ОС для создания скриншотов:

Скриншот рабочего стола	PrintScreen
Скриншот отдельного окна	Alt + PrintScreen
Скриншот отдельной области	Shift + PrintScreen
Скриншот отдельной области (будет скопирован в буфер обмена)	Shift + Control + PrintScreen
Скриншот рабочего стола (будет скопирован в буфер обмена)	Control + PrintScreen
Скриншот отдельного окна (будет скопирован в буфер обмена)	Control + Alt + PrintScreen
Запись видео (окончить запись можно тем же сочетанием клавиш)	Shift + Control + Alt + R

Для смены горячих клавиш необходимо перейти в «**Главное меню**» - «**Параметры**» - «**Смена клавиш клавиатуры**».

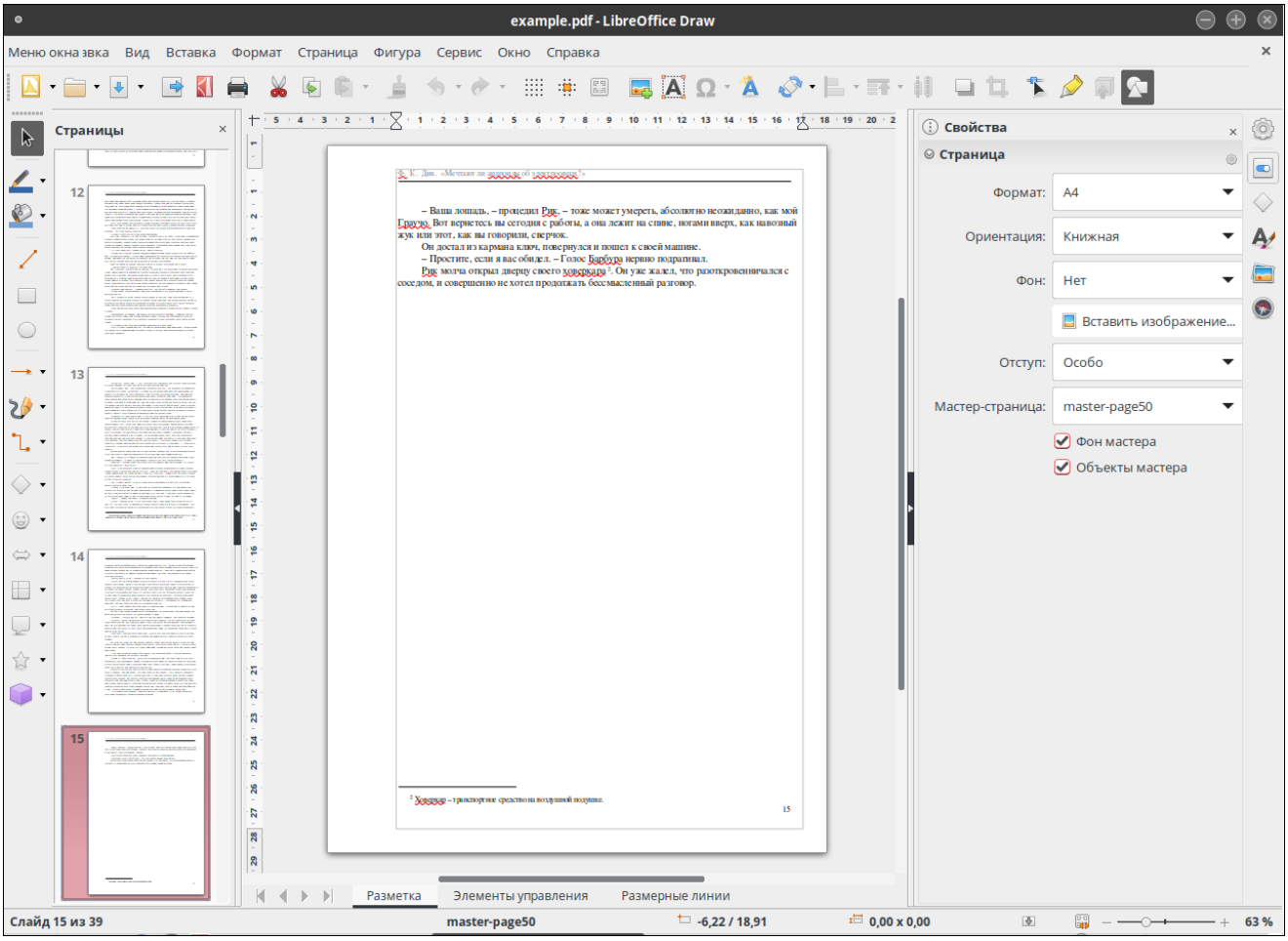
LibreOffice Draw – программа редактирования PDF-файлов

Если вам нужно внести в файл PDF больше изменений, чем просто базовое редактирование страниц, то можно воспользоваться программой **Draw** из пакета офисных приложений **LibreOffice**, который уже предустановлен в РЕД ОС.

Для запуска LibreOffice Draw в **MATE** и **KDE Plasma** необходимо перейти в ***«Главное меню»*** – ***«Офис»*** – ***«LibreOffice Draw»***.

Для запуска LibreOffice Draw в **GNOME** необходимо перейти в меню «**Показать приложения**», ввести в поисковой строке «***LibreOffice Draw***» и выбрать приложение.

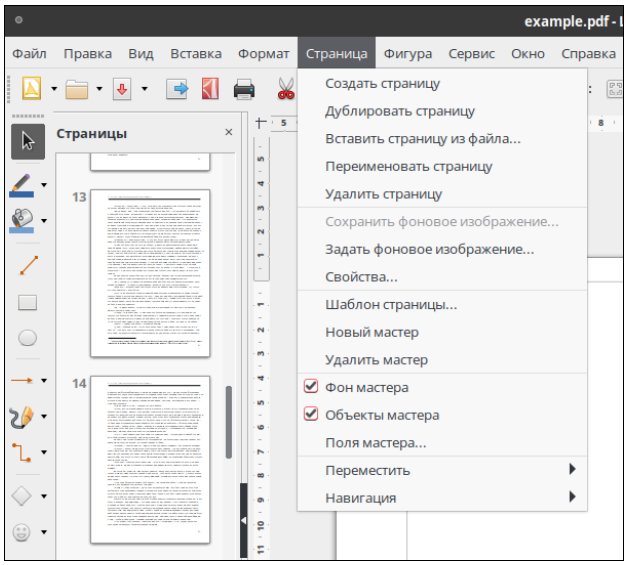
Draw работает аналогично текстовому редактору: вы можете изменять, добавлять и удалять текст в PDF. Для начала работы откройте нужный вам pdf-файл либо создайте новый. После открытия программа будет выглядеть следующим образом:



В левой части экрана доступна панель рисования и панель для просмотра страниц. В правой части экрана находится панель «**Свойства**». В этой панели отображены настройки для страниц документа.

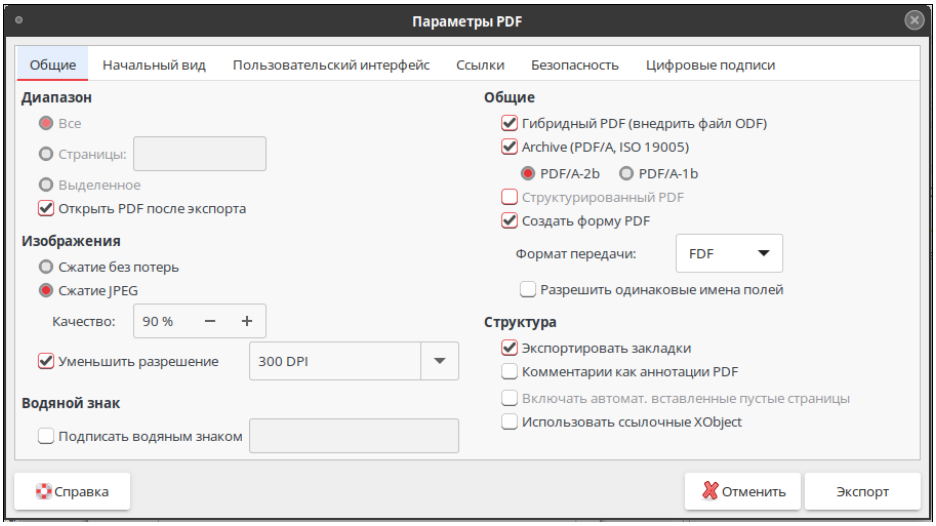
При редактировании текста вы можете изменить его стиль. Для этого существует панель свойств, находящаяся в левой части экрана.

Draw также позволяет добавлять новые страницы или удалять старые. Чтобы добавить/удалить страницу, перейдите в раздел «**Страница**» в верхней панели программы.

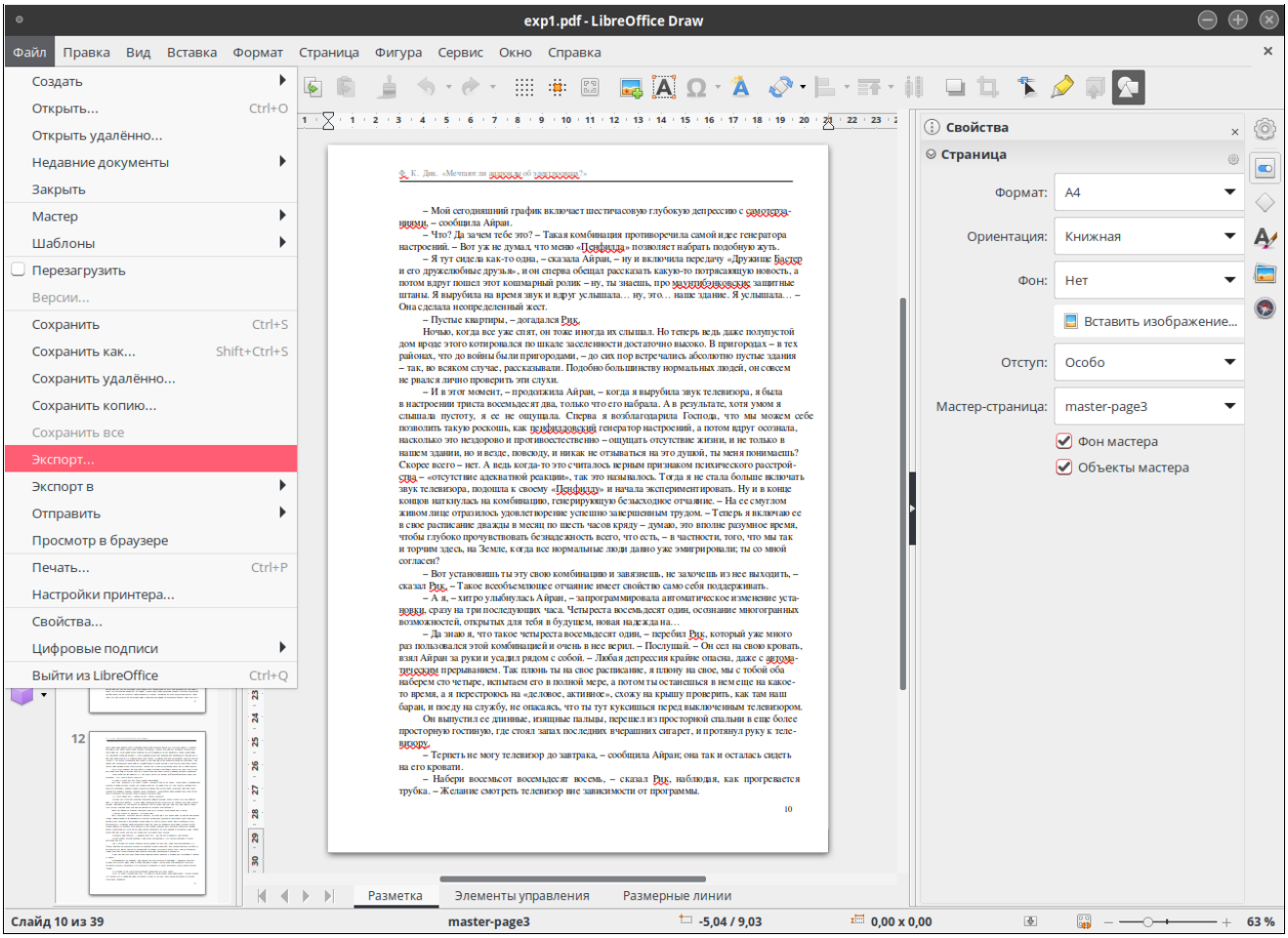


После завершения редактирования, чтобы сохранить файл в pdf, перейдите в раздел «**Файл**» – «**Экспорт в ...**» – «**Экспорт в PDF**». После этого откроется окно с параметрами сохранения. В нем вы можете настроить:

- Диапазон сохраняемых страниц;
- Сжатия и уменьшения разрешения;
- Подпись водяными знаками;
- Структуру файла;
- Ссылки;
- Шифрования;
- Цифровую подпись.



Также **LibreOffice Draw** можно использовать для конвертации PDF в некоторые другие форматы. Для этого откройте ваш документ, перейдите в раздел «**Файл**» в верхней панели программы и выберите пункт « **Экспорт**».



После этого выберите нужный вам формат. Доступные форматы для конвертации: **HTML, XHTML, SWF, BMP, EMP, EPS, GIF, JPEG, PNG, SVG, TIFF, WMF**. После того как вы выбрали, в какой формат конвертировать ваш документ, появится окно для настройки параметров сохранения.

PDFArranger - программа для обработки PDF-файлов

Возможности программы
Установка
Описание программы
Объединение PDF-файлов
Вращение страниц
Перестановка страниц
Удаление и добавление страниц
Обрезка белых границ
Установка метаданных

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pdfarranger-1.8.2-4

PDFArranger — простая и удобная программа, предназначенная для работы с PDF-файлами. Она позволяет пользователю добавлять, удалять, объединять, разделять, вращать и переставлять страницы PDF-документов.

PDFArranger поддерживает большинство основных операций с PDF-файлами, позволяя быстро и эффективно обрабатывать их для различных целей. Программа **PDFArranger** является удобным инструментом для работы с PDF-документами, обеспечивая основные функции по их обработке и редактированию.

Примечание.

В РЕД ОС 8 программа **PDFArranger** является аналогом утилит *PDFedit* и *PDF-Shuffler* в РЕД ОС 7.3.

Возможности программы

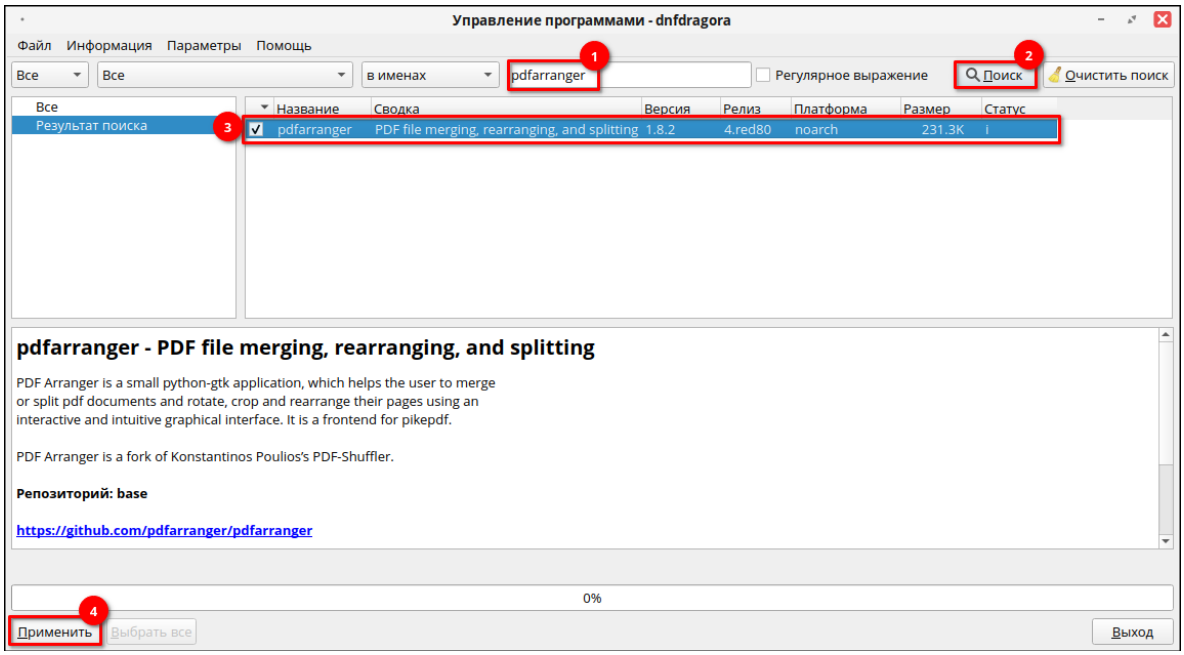
Основные возможности программы **PDFArranger** включают:

- объединение PDF-файлов — пользователь может объединять несколько PDF-документов в один файл;
- разделение PDF-файлов — есть возможность разделить один PDF-документ на несколько отдельных файлов по выбранным страницам или диапазонам страниц;
- вращение страниц — пользователь может поворачивать страницы PDF-документов на 90°, 180° или 270° для коррекции ориентации содержимого;
- перестановка страниц — предоставляется возможность менять порядок страниц в PDF-документе для удобства чтения или презентации;
- удаление и добавление страниц — можно удалять ненужные страницы из PDF-файла или добавлять новые страницы из других источников;
- установка метаданных — есть возможность устанавливать метаданные для PDF-файлов, такие как название, автор, ключевые слова и дата создания.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**pdfarranger**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
dnf install pdfarranger
```

Т.к. в РЕД ОС 8 программа PDFArranger является аналогом утилиты PDF-Shuffler в РЕД ОС 7.3 для установки также можно использовать следующий алиас:

```
dnf install pdfshuffler
```

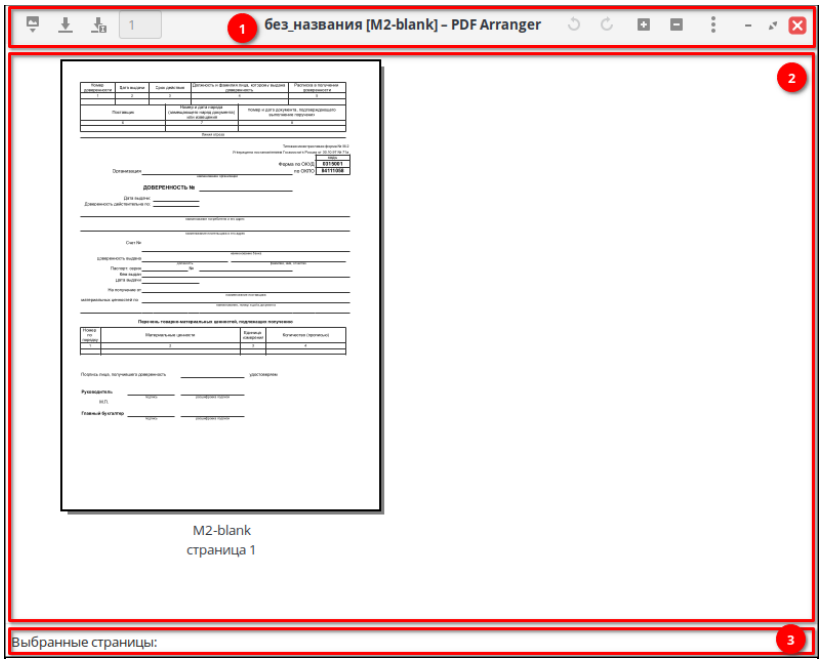
После установки программа доступна в «**Главном меню**» — «**Офис**» — «**PDFArranger**».

Также программу можно запустить через терминал, для этого введите команду:

```
pdfarranger
```

Описание программы

Главное окно программы выглядит следующим образом:



Окно состоит из следующих элементов:

1. **Панель инструментов** — основные действия для работы с программой.

2. **Рабочая область** — отображаются файлы.

3. **Область выбранных страниц** — отображается информация о выбранных страницах.

Вверху находится панель инструментов, на которой отражены основные действия для работы с программой.

На панели инструментов доступны следующие основные действия:

 — открыть файл и добавить его к текущему документу;

 — сохранить;

 — сохранить как;

 — повернуть влево;

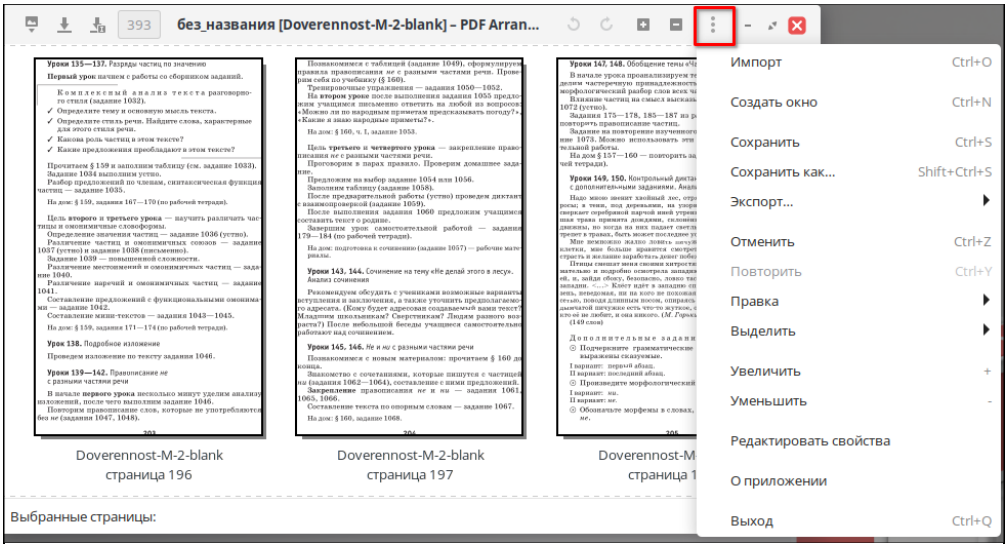
 — повернуть вправо;

 — увеличить;

 — уменьшить;

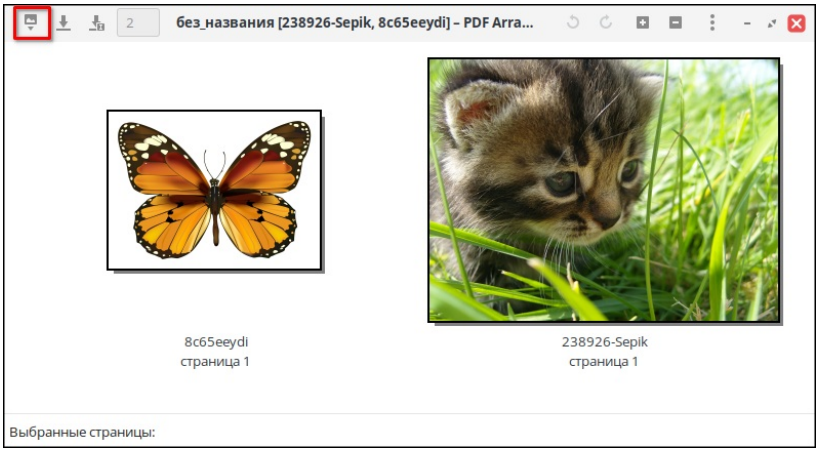
 — основное меню.

В основном меню представлены инструменты для импорта, редактирования и управления PDF-документами. Пользователи могут создавать новые окна, сохранять изменения, экспортировать страницы, отменять и повторять действия, а также выполнять различные операции редактирования, такие как поворот, обрезка, удаление и дублирование страниц.

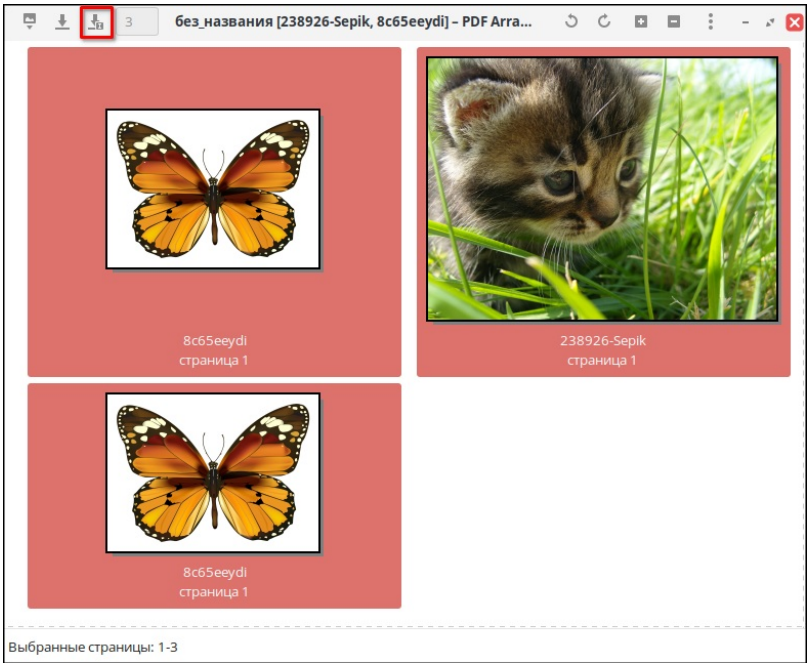


Объединение PDF-файлов

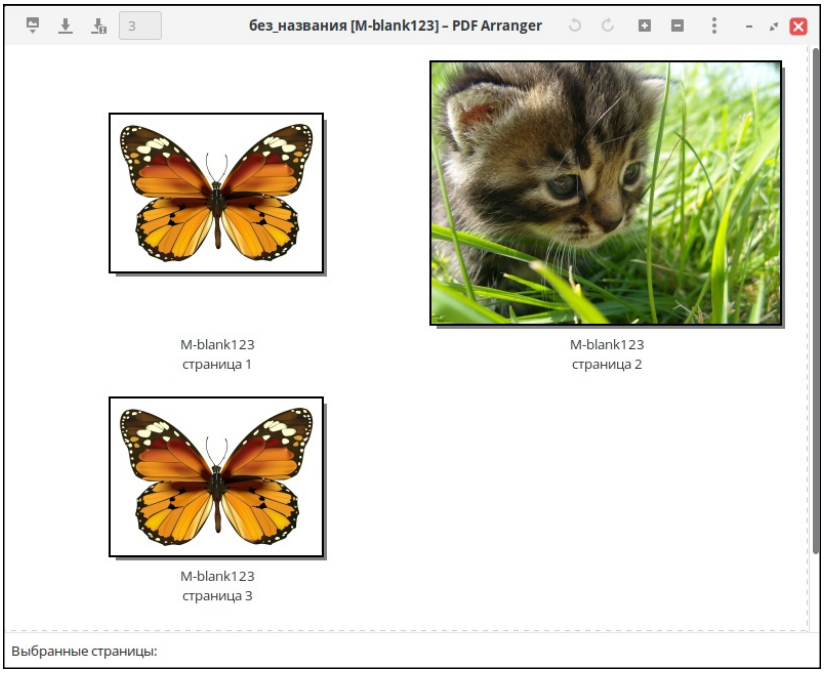
Можно объединить PDF-документы и другие файлы (например, изображения) в один PDF-файл. Для объединения нескольких файлов загрузите их поочередно в программу с помощью инструмента «**Открыть файл и добавить его к текущему документу**».



После редактирования выделите страницы и сохраните получившийся файл, нажав «**Сохранить как...**».

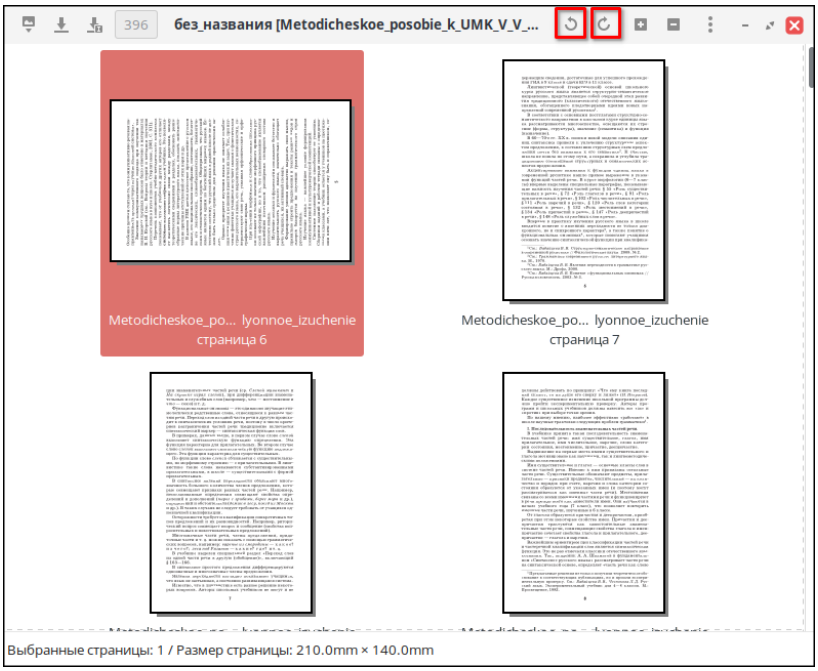


После выполненных действий откройте объединенный PDF-файл.



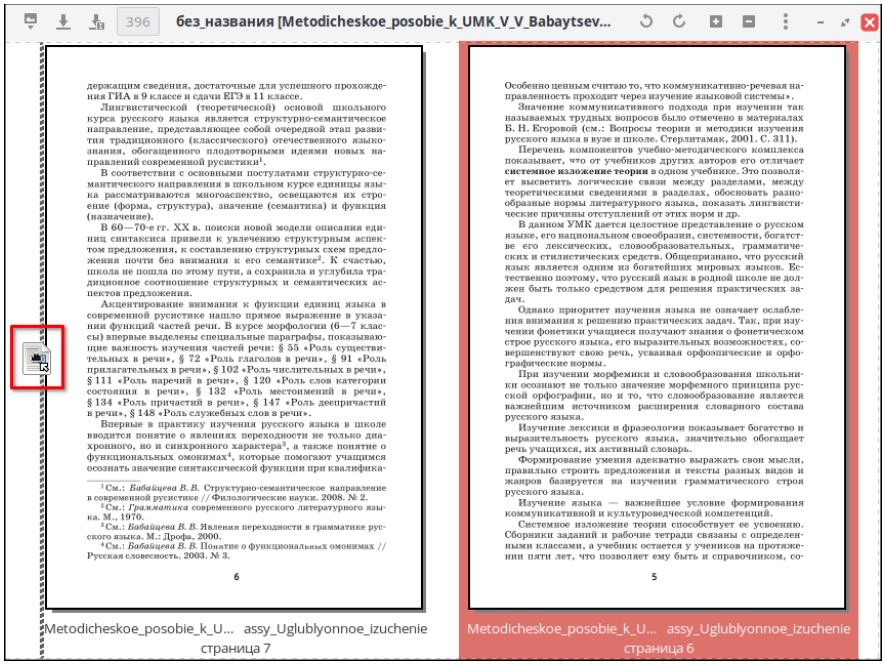
Вращение страниц

С помощью инструментов «**Повернуть влево**» и «**Повернуть вправо**» программа позволяет поворачивать страницы файла PDF под разными углами на 90°, 180° или 270° для коррекции ориентации содержимого.



Перестановка страниц

Для изменения порядка страниц в PDF-файле перетащите страницы в нужные позиции. После перестановки сохраните обновленный файл.

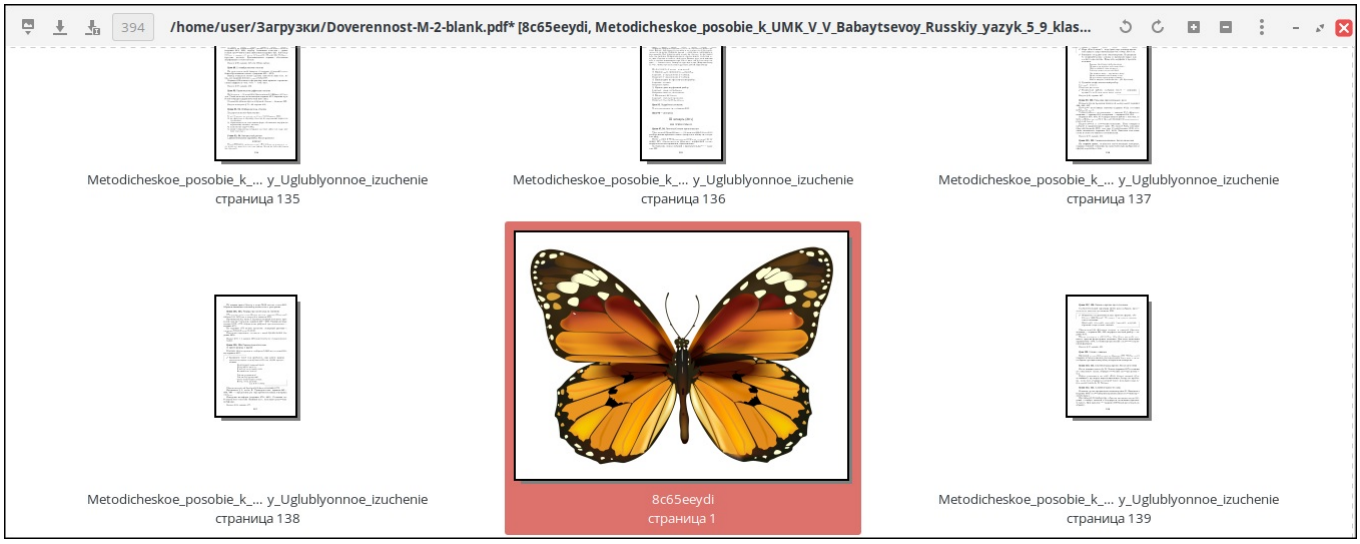


Удаление и добавление страниц

Для удаления страниц откройте PDF-документ и выберите страницы, которые хотите удалить, удалите их и сохраните изменения.

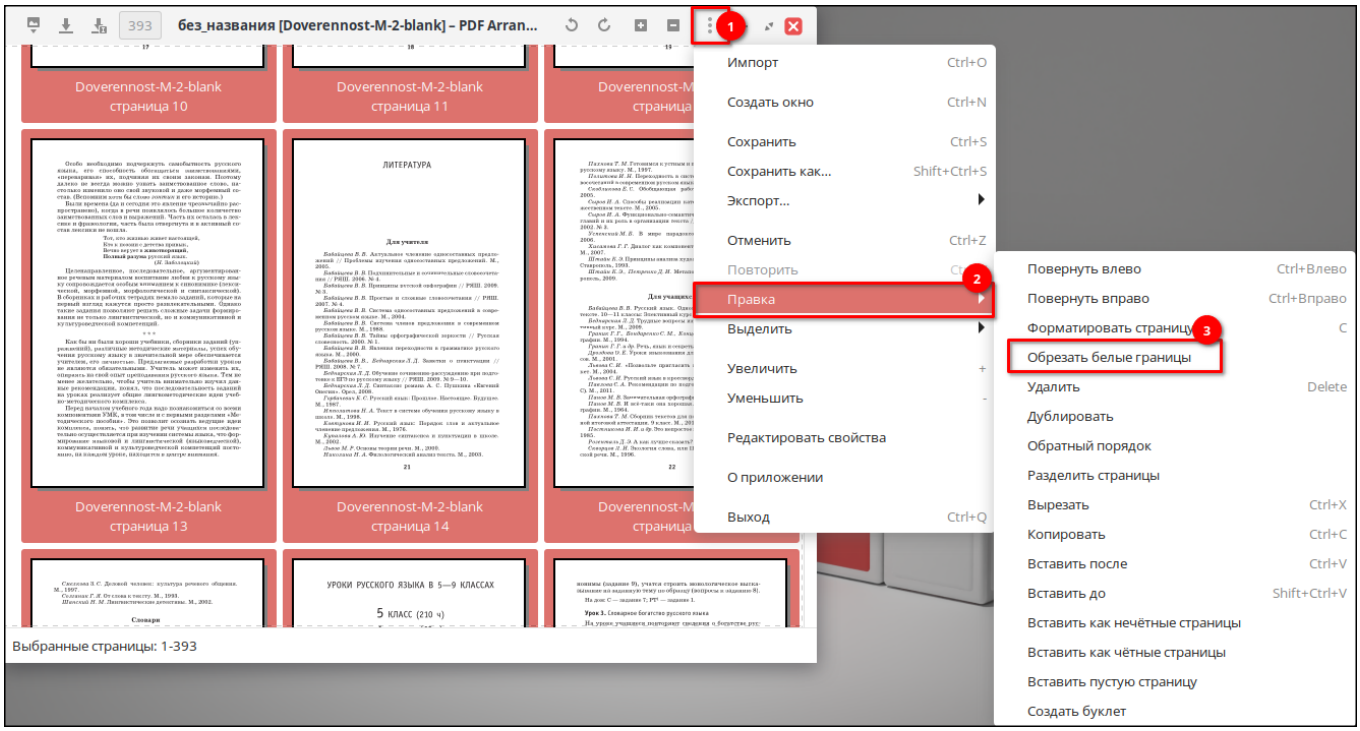


Для добавления страниц выберите «**Открыть файл и добавить его к текущему документу**». Файл будет добавлен в конец открытого документа. С помощью мыши перетащите добавленные страницы на нужные позиции и сохраните изменения.

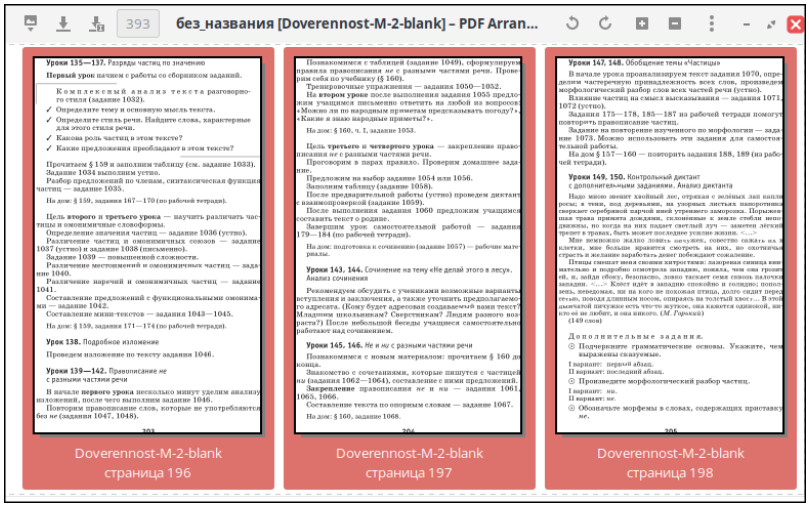


Обрезка белых границ

Для обрезки белых границ выберите страницы для редактирования, перейдите в «**Основное меню**» — «**Правка**» — «**Обрезать белые границы**».

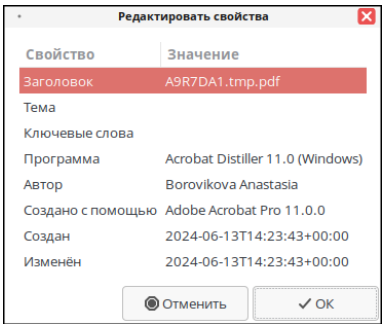


Также можно щелкнуть ПКМ по выделенным страницам и выбрать в контекстном меню «**Обрезать белые границы**». Границы выбранных страниц будут обрезаны. Сохраните изменения.



Установка метаданных

Для установки метаданных для PDF-файла откройте документ и перейдите в «**Основное меню**» — «**Редактировать свойства**». Введите необходимую информацию (заголовок, тему, ключевые слова, программу, автора, дату создания и дату изменения) и нажмите «**ОК**».



poppler – утилита конвертации PDF в различные форматы

Утилиты из poppler-utils
Установка poppler-utils
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: poppler-utils-22.08.0

Для конвертации PDF-документов в различные форматы можно воспользоваться пакетом **poppler-utils**, который предоставляет инструменты на основе библиотеки Poppler для работы с PDF-файлами. Этот пакет включает несколько утилит, которые позволяют преобразовывать PDF-документы в разные форматы, а также получать информацию о них.

Утилиты из poppler-utils

Вот основные утилиты, доступные в poppler-utils, которые могут быть полезны для конвертации PDF:

1. **pdftocairo** — позволяет конвертировать PDF в форматы PNG, JPEG, PDF, PS, EPS и SVG с использованием библиотеки Cairo.
2. **pdftohtml** — преобразует PDF в формат HTML.
3. **pdftoppm** — конвертирует PDF в изображения в формате PPM, PNG и JPEG.
4. **pdftops** — преобразует PDF в формат PostScript (PS).

Установка poppler-utils

В РЕД ОС утилита **poppler-utils** установлена по умолчанию. Если по какой-то причине она отсутствует, вы можете установить её с помощью следующей команды (потребуются права администратора):

```
sudo dnf install poppler-utils
```

Примеры использования

После установки утилит можно использовать их для конвертации PDF-документов. Вот несколько примеров:

Преобразование PDF в PS

Чтобы преобразовать PDF-документ в формат PostScript, используйте следующую команду:

```
pdftocairo -ps example.pdf example.ps
```

Преобразование PDF в PNG

Для конвертации PDF в формат PNG можно использовать:

```
pdftocairo -png example.pdf example.png
```

Преобразование PDF в HTML

Для преобразования PDF в HTML, выполните:

```
pdftohtml example.pdf example.html
```

Преобразование PDF в JPEG

Для конвертации PDF в формат JPEG:

```
pdftocairo -jpeg -f 2 -l 4 example.pdf  example.jpg
```

Преобразование PDF в PPM

Для преобразования PDF в PPM:

```
pdftoppm example.pdf example
```

Adobe Acrobat Reader

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** snapd-2.65.1, acrordrdc 2021.007.20091

Adobe Acrobat Reader — это инструмент для просмотра, редактирования и конвертации PDF-файлов в удобный формат и дальнейшей работы с ними. Он дает возможность добавлять свои заметки, сканировать бумажные файлы и отправлять их на печать.

Установить **Adobe Acrobat Reader** можно с помощью **snap**. Для этого необходимо установить пакет **snap**. Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install snapd
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

После установки необходимо активировать сокет **snap** и добавить его в автозагрузку командой:

```
systemctl enable --now snapd.socket
```

Чтобы включить поддержку классической привязки и создать символическую ссылку между **/var/lib/snapd/snap** и **/snap**, выполните следующую команду:

```
ln -s /var/lib/snapd/snap /snap
```

После этого перезагрузите систему, чтобы убедиться, что пути **snap** были обновлены правильно.

Подробную информацию о работе с утилитой **snap** см. в нашей инструкции «Snap - изолированная среда для запуска приложений».

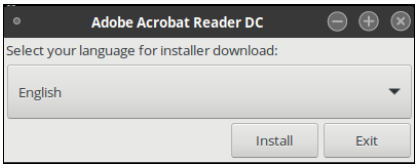
Затем с помощью **snap** установите пакет **acrordrdc**:

```
snap install acrordrdc
```

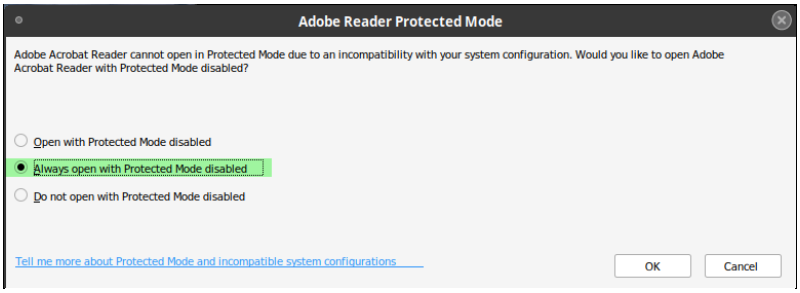
После этого можно запустить установку **Acrobat Reader**:

```
snap run acrordrdc
```

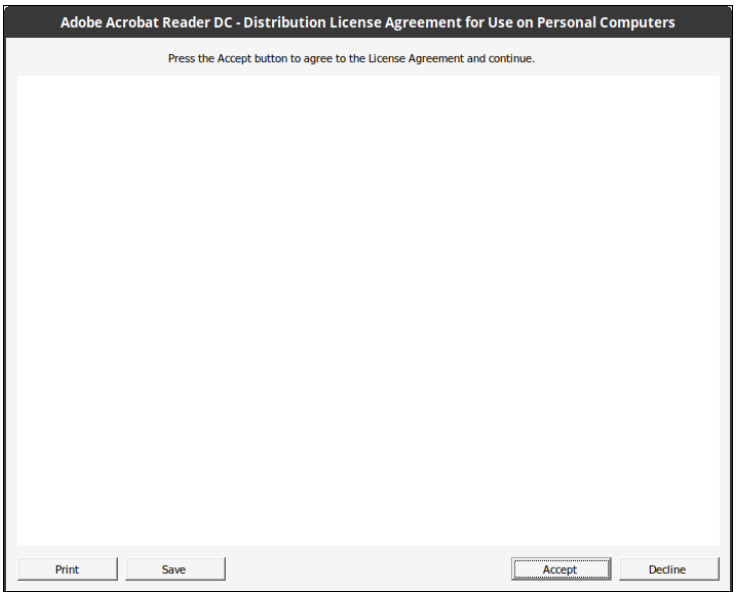
Выберите предпочитаемый язык и нажмите «**Install**»:



Выберите пункт запуска программы с отключенным защищенным режимом:



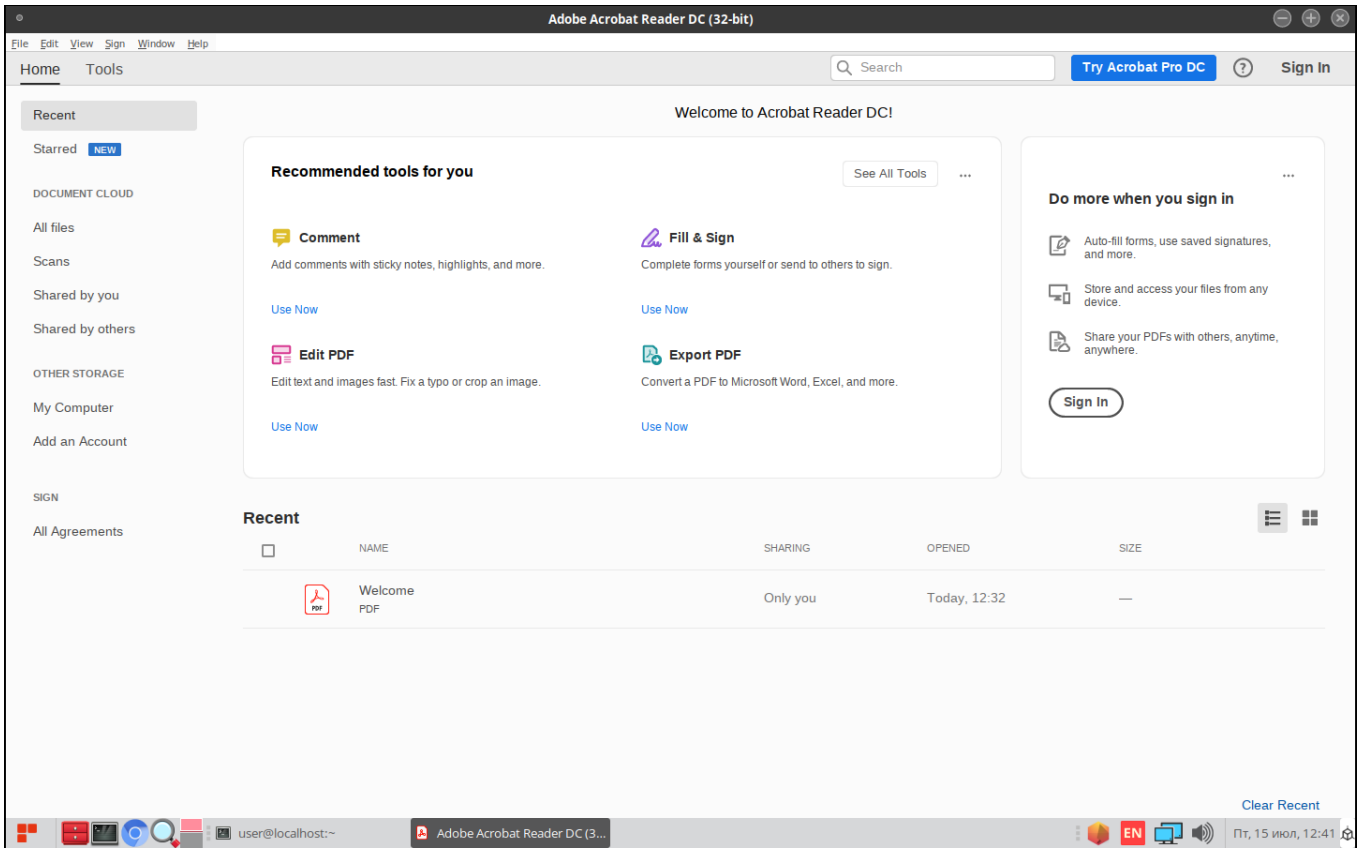
Примите лицензионное соглашение:



Далее будет запущен **Adobe Acrobat Reader**.

При дальнейшей работе запуск программы доступен из «**Главного меню**» - «**Офис**» - «**Adobe Acrobat Reader DC**» или командой в терминале (с правами локального пользователя):

```
acrordrdc
```



Распознавание текста с помощью YAGF

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** yagf-0.9.5-17

YAGF — графический интерфейс для консольных программ распознавания текстов: ***CuneiForm*** и ***Tesseract***. **YAGF** позволяет управлять сканированием изображений, их предварительной обработкой и распознаванием. Программа поддерживает все основные растровые графические форматы (**JPEG, PNG, BMP, TIFF, GIF, PNM, PPM, PBM** и другие).

Вы можете подробнее ознакомиться с работой в программах для распознавания текста, просмотрев наши обучающие видео:

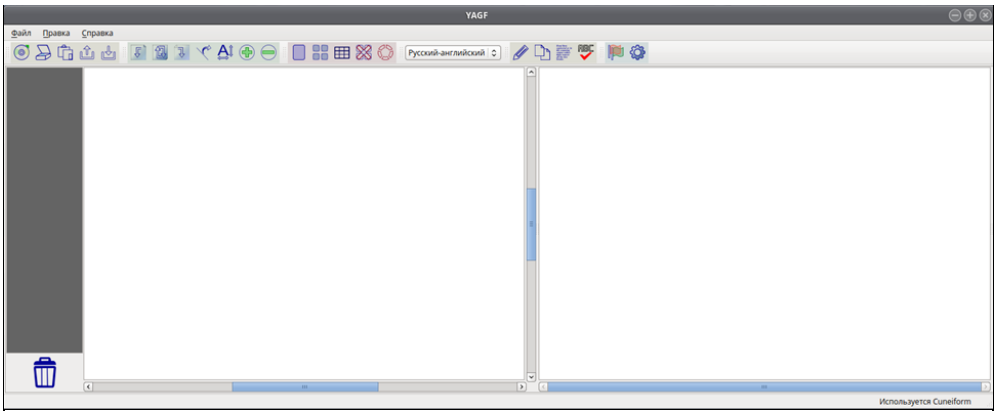
- на **RuTube** — Распознавание текста;
- в **Яндекс.Дзен** — Распознавание текста;
- в **VK Видео** — Распознавание текста.

На наших каналах вы также сможете найти много другой полезной информации.

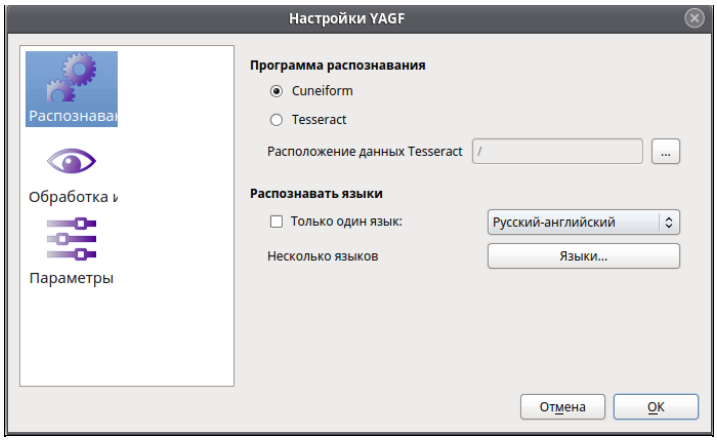
Для установки оболочки **YAGF** и дополнительных языковых пакетов словарей выполните команду с правами пользователя **root**:

```
dnf install yagf aspell-ru aspell-en
```

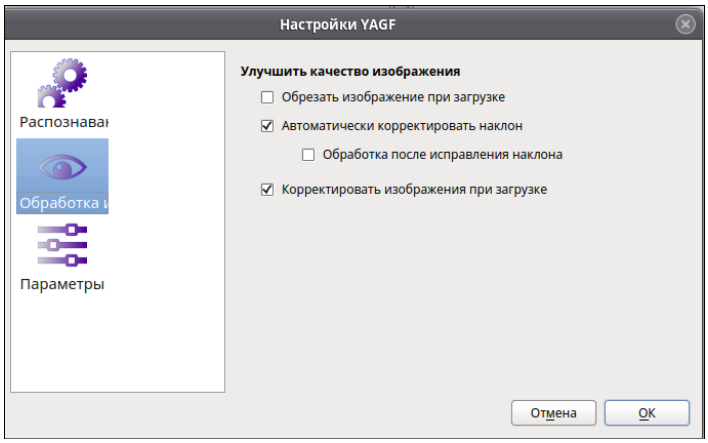
После установки программа будет доступна из «**Главного меню**» — «**Офис**» — «**YAGF**».



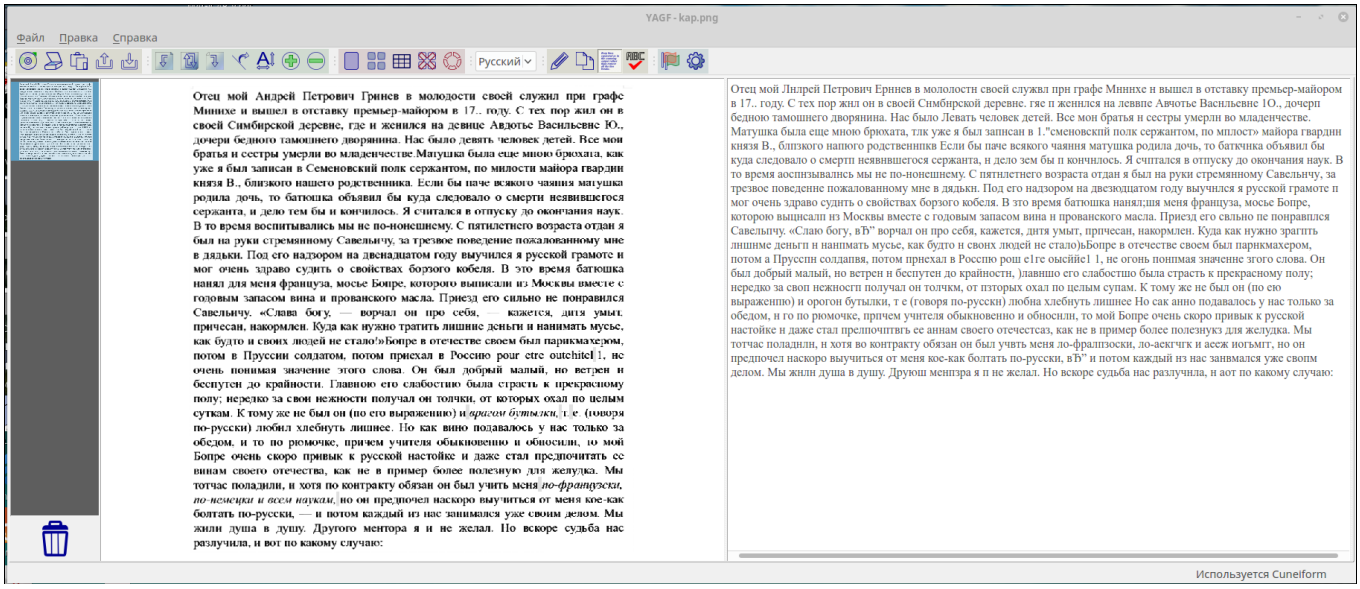
В настройках программы выберите язык распознаваемого текста.



На вкладке «**Обработка изображений**» снимите галочку с пункта «**Обрезать изображение при загрузке**», чтобы не возникало проблем с отображением загруженного в программу документа.



Программа позволяет открыть для распознавания файлы, сохраненные на жестком диске, или сканировать новое изображение. Для того чтобы загрузить изображение, перейдите в меню **Файл > Открыть** и в диалоговом окне выберите один или несколько файлов. Кроме этого имеется возможность перетаскивать графические файлы мышью на темную полосу в левой части главного окна программы.



В **YAGF** можно получать изображения со сканера с помощью программы *XSane*. Если *XSane* не установлена, то установите эту программу командой от пользователя **root**:

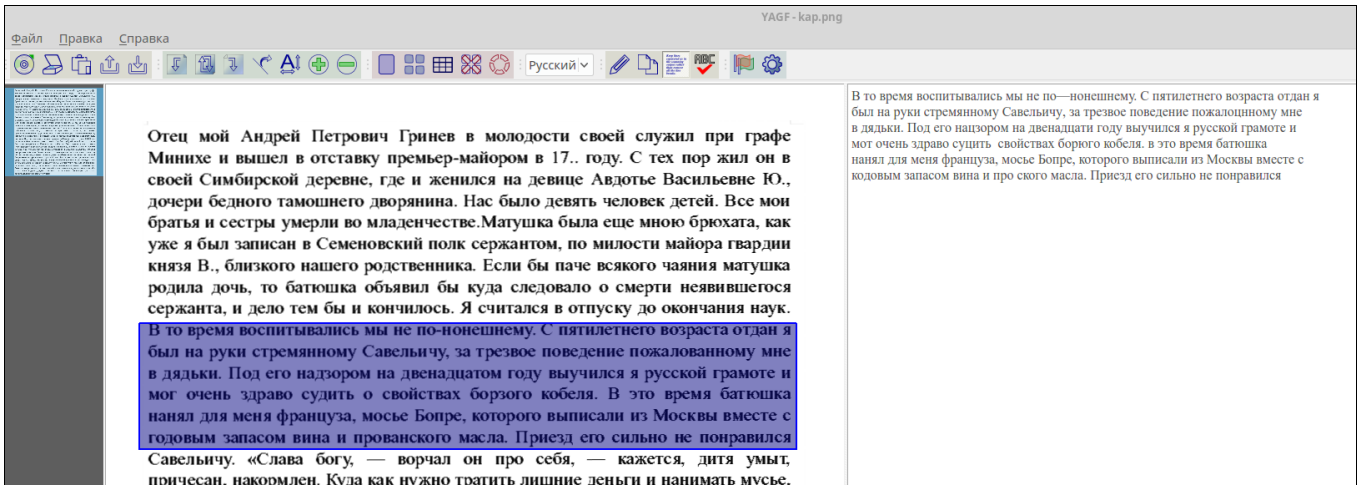
```
dnf install xsane
```

Чтобы получить изображение перейдите в меню **Файл > Сканировать**. Будет запущена программа *XSane*. При необходимости настройте параметры сканирования в *XSane* и нажмите кнопку «**Сканировать**». После завершения сканирования в окне просмотра изображений *YAGF* появится сканированное изображение.

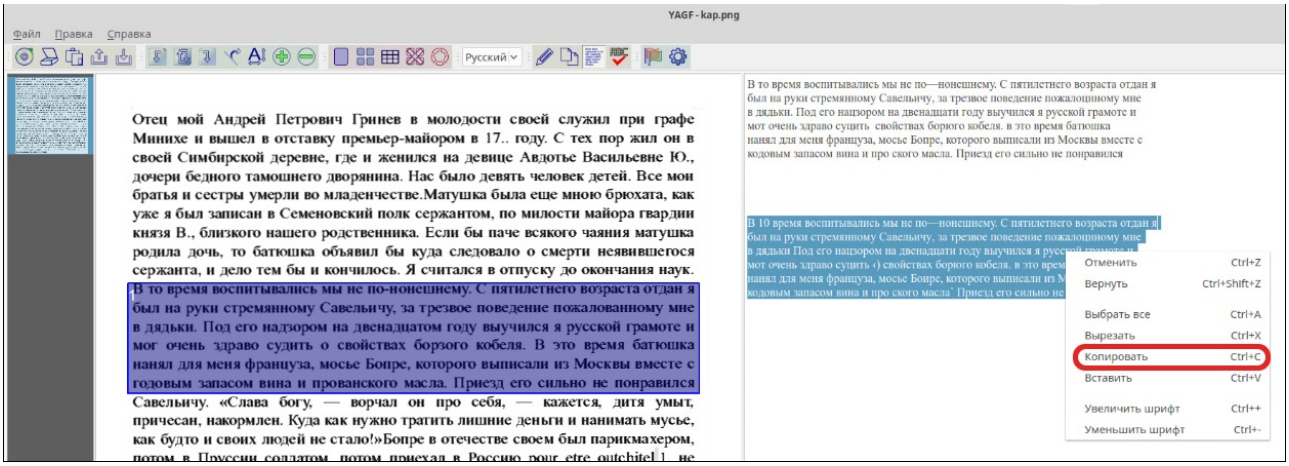
YAGF предоставляет простые операции подготовки сканированного изображения, такие как выделение блока текста для распознавания и поворот. Если изображение ориентировано неправильно, его можно повернуть на 90 градусов по часовой или против часовой стрелки, а также на 180 градусов. Делается это с помощью кнопок на панели быстрого доступа в окне просмотра изображений.

Если необходимо распознать не весь текст на изображении, а отдельную его часть, то для этого выделите мышью один или несколько фрагментов в окне просмотра изображений.

Для распознавания текста на изображении, перейдите в меню **Файл > Распознать** или воспользуйтесь комбинацией клавиш **Ctrl+R**.



Для сохранения текста в меню **Файл** и выберете пункт «**Сохранить весь текст**» или «**Сохранить текст на текущей странице**». Также можно скопировать текст в буфер обмена с помощью правой кнопки мыши.



Примечание.

Для распознавания текста на английском языке с помощью **Tesseract** в программе **YAGF** необходимо указать стандартный путь расположения файлов - *«Настройки»* - *«Распознавание»* - *«Расположение данных Tesseract»* - **/usr/share/tesseract/tessdata/**.

После сохранения пути выберите язык в настройках.

Распознавание текста с помощью gImageReader

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: gimagereader-gtk-3.3.1

gimagereader - программа, предназначенная для распознавания текста (**GUI Tesseract**).

gimagereader поддерживает автоматическое определение макета страницы, при этом пользователь может вручную определить и настроить регионы распознавания. Приложение позволяет импортировать изображения с диска, сканирующих устройств, буфера обмена и скриншотов.

gimagereaderтакже поддерживает многостраничные документы **PDF**.

Особенности **gimagereader**:

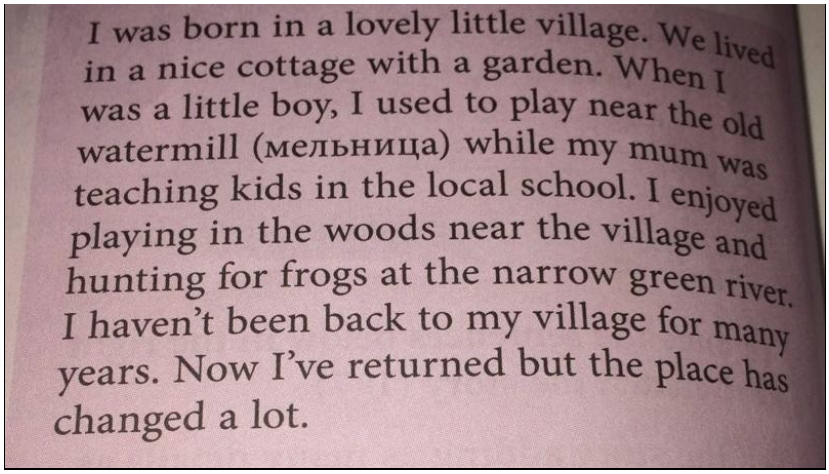
- поддержка следующих форматов изображений: **jpeg**, **png**, **tiff**, **gif**, **pnm**, **pcx**, **bmp**;
- поддержка формата электронных документов PDF. Возможность выбрать отдельные страницы и диапазон страниц для распознавания;
- автоматическое обнаружение расположения страницы;
- выделение области с текстом для распознавания;
- получение изображения напрямую со сканера. Настройка разрешения, сохранение в формат **png**;
- проверка орфографии.

Установка программы в РЕД ОС производится командой:

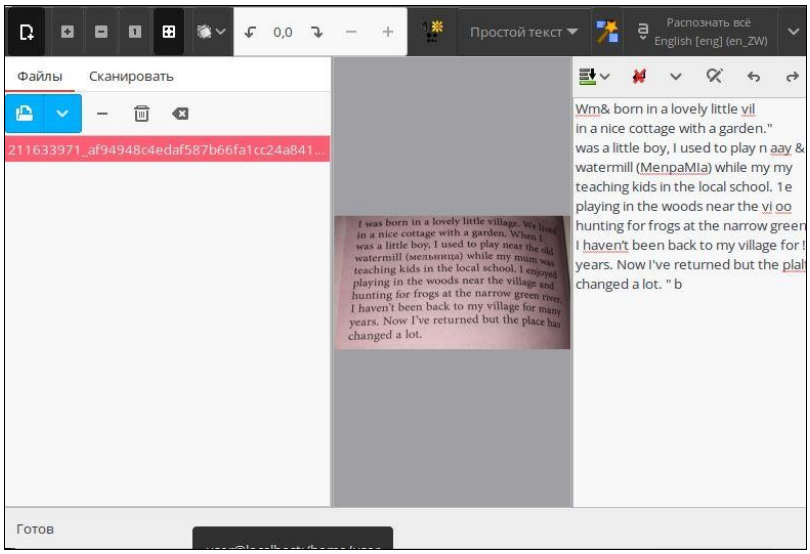
```
dnf install gimagereader-gtk tesseract-langpack-rus
```

После установки команда будет доступна в «**Главном меню**» - «**Графика**» - «**gImageReader**».

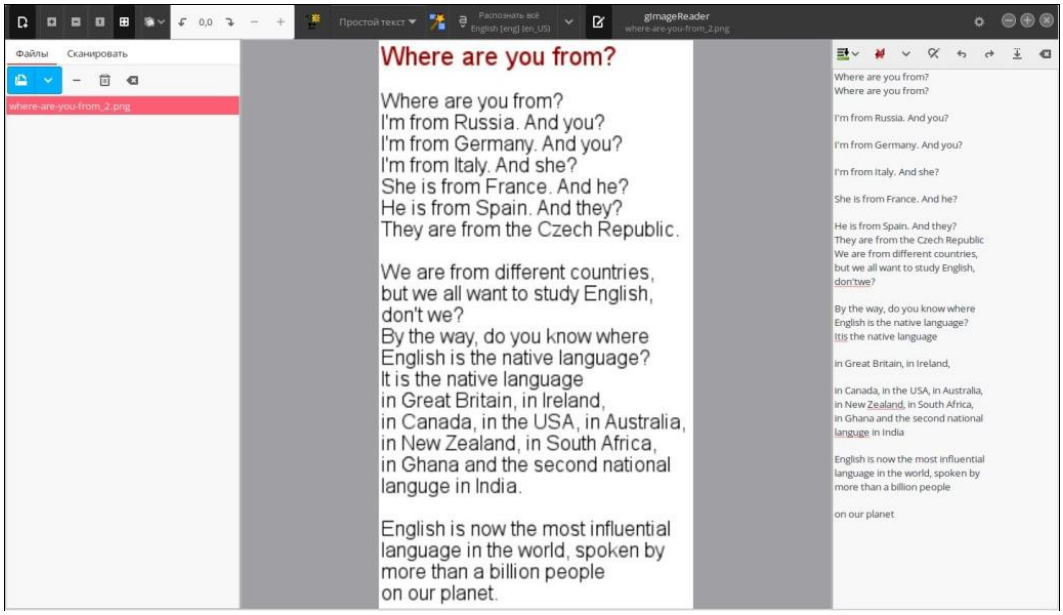
Для проверки загрузите в программу картинку с любым текстом.



Выберите язык и нажмите на кнопку «**Распознать все**» (так программа распознает весь текст на картинке).

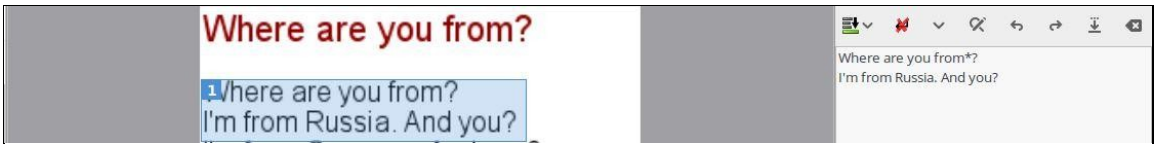


Как видно из примера, не весь текст распознан правильно, скорее всего это связано с плохим изображением (неровные линии текста, разное освещение), поэтому возьмем другой текст и проверим работоспособность программы на нем.



С другого изображения весь текст распознан корректно.

Для распознавания определенного отрывка текста необходимо выделить нужную область, после чего нажать на кнопку «**Распознать выделенное**».



Текст успешно распознан.

Простые графические редакторы

GIMP
Pinta

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** pinta-1.7-1, gimp-2.10.30-1

GIMP

GNU Image Manipulation Program (**GIMP**) — свободно распространяемый растровый графический редактор, программа для создания и обработки растровой графики и частичной поддержкой работы с векторной графикой.

Вы можете подробнее ознакомиться с работой в GIMP, просмотрев наши обучающие видео:

- на **RuTube** — Растровый графический редактор GIMP;
- в **Яндекс.Дзен** — Растровый графический редактор GIMP;
- в **VK Видео** — Растровый графический редактор GIMP.

На наших каналах вы также сможете найти много другой полезной информации.

Работа с фотографиями

В **GIMP** присутствует набор инструментов цветокоррекции:

- кривые;
- уровни;
- микшер каналов;
- постеризация;
- тон-насыщенность;
- баланс цветов;
- яркость-контраст;
- обесцвечивание.

При помощи фильтров, инструментов, масок и слоёв с разными типами наложения можно:

- выравнивать заваленный горизонт;
- убирать искажения, вносимые оптикой;
- корректировать перспективу;
- выполнять клонирование объектов с учётом перспективы;
- кадрировать фотографии;
- удалять дефекты вроде пыли на матрице (штамп, лечебная кисть);
- имитировать использование различных цветофильтров;
- «вытаскивать» потерянную детализацию в тенях.

Рисование

Для удобства рисования реализованы следующие возможности:

- несколько рисующих инструментов;
- свободно масштабируемые кисти;
- поддержка кистевой динамики;
- поддержка графических планшетов.

Экранные фильтры

Дополнительные возможности по коррекции изображений на протяжении всей работы реализованы в виде экранных фильтров.

К ним относятся:

- имитация разных типов дальтонизма (протанопия, дейтеранопия, тританопия);
- гамма-коррекция;
- коррекция контраста;
- управление цветом.

Настраиваемый интерфейс

Благодаря следующим функциям можно осуществлять удобную настройку интерфейса:

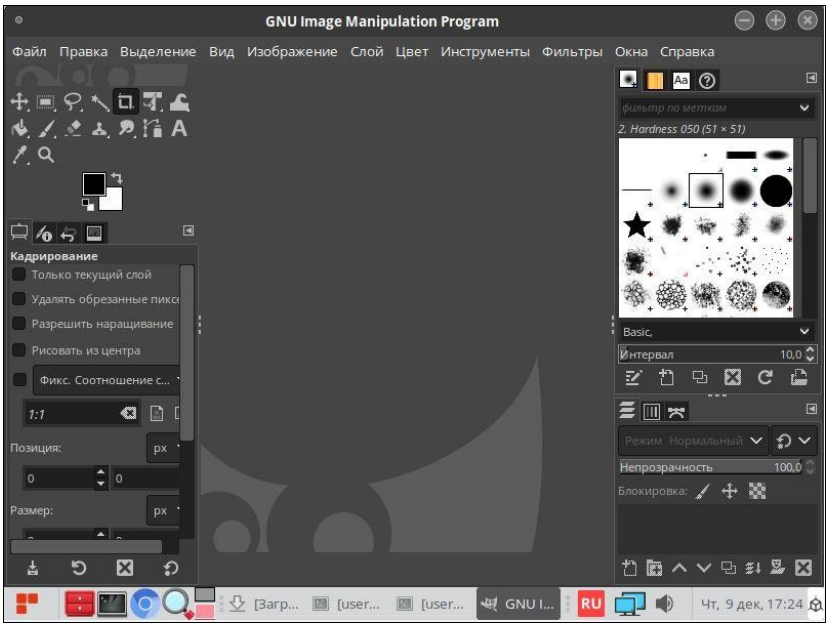
- плавающие диалоги легко группируются и перегруппируются;
- возможна полная перенастройка клавиатурных комбинаций, действий мыши, а также устройств ввода, таких как **Griffin PowerMate**;
- любое меню можно превратить в свободно перемещаемое окно.

Установка

Установка редактора осуществляется следующей командой (с правами пользователя **root**):

```
dnf install gimp
```

После установки программа доступна в «**Главном меню**» - «**Графика**» - «**GNU Image Manipulation Program**».



Pinta

Pinta — легковесный кроссплатформенный растровый графический редактор.

Pinta является редактором с большим количеством функций, характерных для программного обеспечения такого класса, включая инструменты для рисования, фильтры и эффекты, инструменты для управления параметрами цвета (контрастность, яркость, преобразование в чёрно-белое изображение и т. п.).

Основные особенности программы:

- простое меню инструментов и возможностей;
- безлимитная история действий (с возможностью отмены любого);
- многоязычный интерфейс (55 языков);
- гибкая компоновка панели инструментов, в том числе с плавающими окнами и стыковкой по краю изображения.

Базовые инструменты включают:

- кисть и карандаш;
- заливка цветом и градиент;
- ластик;
- инструменты выделения (прямоугольное, эллиптическое, лассо, волшебная палочка, пипетка);
- инструменты для перемещения и копирования;
- текст;
- линейка и кривые;
- инструменты для рисования геометрических фигур;
- лупа для масштабирования.

Стандартная палитра цветов предоставляет доступ сразу к 48 цветам, с возможностью выбора любого другого. При этом из меню программы также доступны:

- кадрирование;
- изменение размера изображения и холста;
- отражение;
- поворот.

В отличие от некоторых простых графических редакторов (таких, например, как **MS Paint** или **XPaint**), Pinta также имеет поддержку слоев изображения. Важной особенностью является возможность использования прозрачности (прозрачного цвета) и альфа-каналов.

Среди фильтров и эффектов, доступных в **Pinta** по умолчанию, можно отметить:

- расфокусировку;
- размытие (в том числе по Гауссу);
- пикселизацию;
- эффекты карандашного наброска или наброска чернилами;
- удаление эффекта красных глаз на фотографиях и пр.

Редактор **Pinta** позволяет открывать и сохранять изображения в следующих форматах:

- ORA;
- BMP;
- PNG;
- JPEG (JPG);
- TGA;
- TIFF;
- ICO.

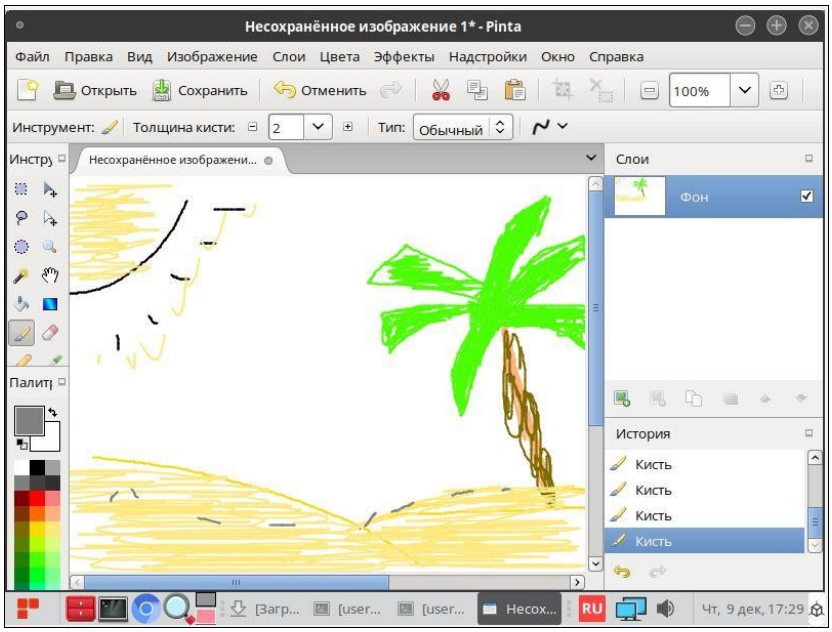
Изображения в формате GIF **Pinta** может только открывать (импортировать), при этом для анимированных GIF открывается только первый кадр. Сохранение в GIF не поддерживается.

Установка

Установка редактора осуществляется следующей командой (с правами пользователя **root**):

```
dnf install pinta
```

После установки программа доступна в «**Главном меню**» - «**Графика**» - «**Pinta**».


Несохранённое изображение 1* - Pinta
Файл Правка Вид Изображение Слои Цвета Эффекты Надстройки Окно Справка
Открыть Сохранить Отменить
100%
Инструмент: Толщина кисти: 2 Тип: Обычный
Несохранённое изображени...
Слои
Фон
История
Кисть
Кисть
Кисть
Кисть
Несох...
RU
Чт, 9 дек, 17:29

Графический редактор Krita

Установка
Работа в программе
Инструмент Кисть
Работа со слоями
Применение фильтров
Анимация и векторная графика
Сохранение результатов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: krita-4.4.1-4

Krita – бесплатный растровый графический редактор с открытым исходным кодом, предоставляющий широкий спектр инструментов для рисования и создания графики.

Krita поддерживает редактирование слоев и масок (по аналогии с *Adobe Photoshop*), работу в различных цветовых пространствах и с различными цветовыми моделями — **RGB**, **CMYK**, **LAB**, в режиме от 8 до 32 бит с плавающей точкой на канал. Кроме того, реализованы популярные фильтры, корректирующие слои, маски и динамические фильтры, а также серия инструментов для ретуши.

Основным приоритетом разработчики ставят реализацию возможностей для художников и иллюстраторов:

- полноценные инструменты для работы с покадровой анимацией, включая экспорт анимации с использованием **FFmpeg**;
- широкий выбор кистей (в том числе смешивающие, фильтрующие, эффектные, спрей, кисти для заполнения объёмов);
- большое количество режимов наложения;
- управление динамикой кистей с помощью графического планшета;
- имитация бумаги и пастели;
- поворот и зеркалирование холста;
- псевдо-бесконечный холст.

Krita также предоставляет широкий выбор инструментов для рисования, растровой графики, ретуширования и рисования с использованием планшетного стилуса. Благодаря своей открытой архитектуре, **Krita** позволяет расширять свои возможности с помощью плагинов и скриптов, что делает программу настраиваемой и гибкой.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

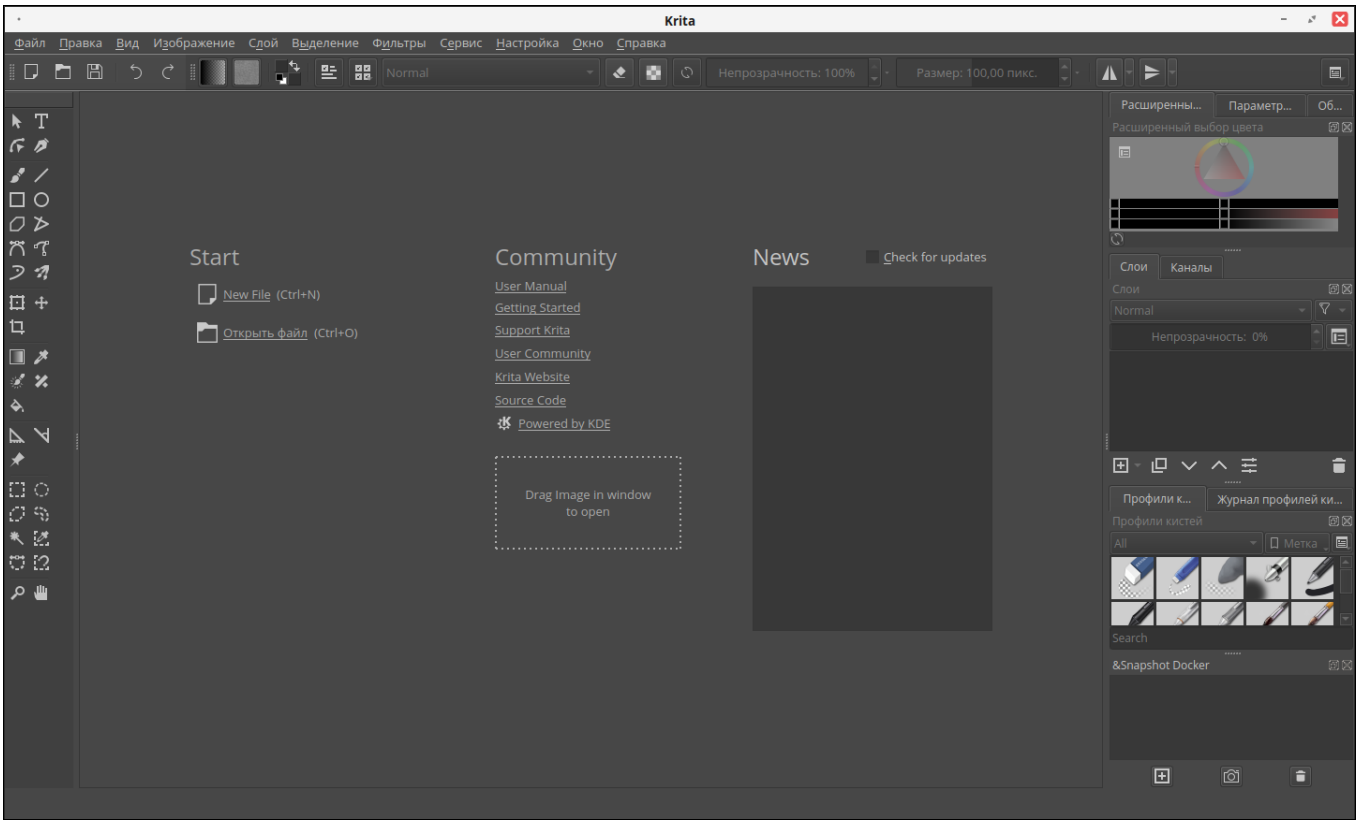
```
dnf install krita
```

Дальнейшая работа с программой производится с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

После установки программа доступна из «**Главного меню**» – «**Графика**» – «**Krita**».

Главное окно программы выглядит следующим образом:



В верхней части окна находится **основное меню** программы, где доступны все инструменты и действия по работе с **Krita**.

Под основным меню расположена **верхняя панель инструментов**, на которой можно настроить палитру, градиенты, текстуры, а также некоторые параметры кистей;

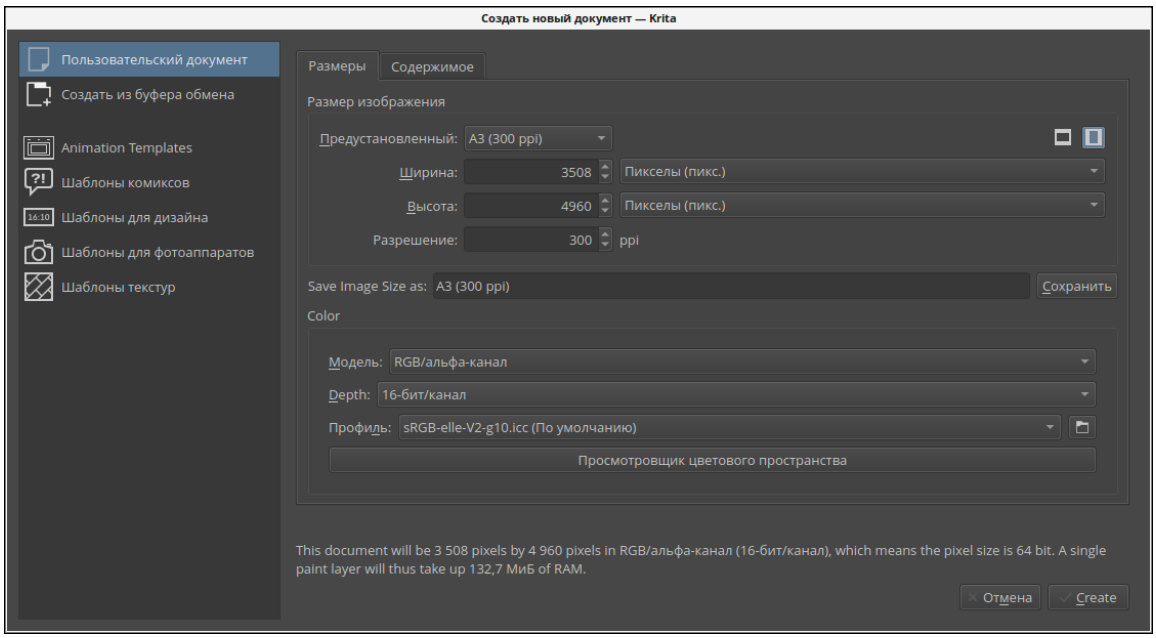
Слева расположена **панель инструментов** – здесь доступны основные инструменты, необходимые для работы.

Справа расположены компоненты для работы со слоями, цветом и профилями кистей.

В центре окна расположена **рабочая область**, где будет производиться работа непосредственно с изображением.

Работа в программе

Перед началом работы необходимо создать новый холст – задать размеры и заполнение. Для создания нового холста в основном меню выберите «**Файл**» – «**New**».



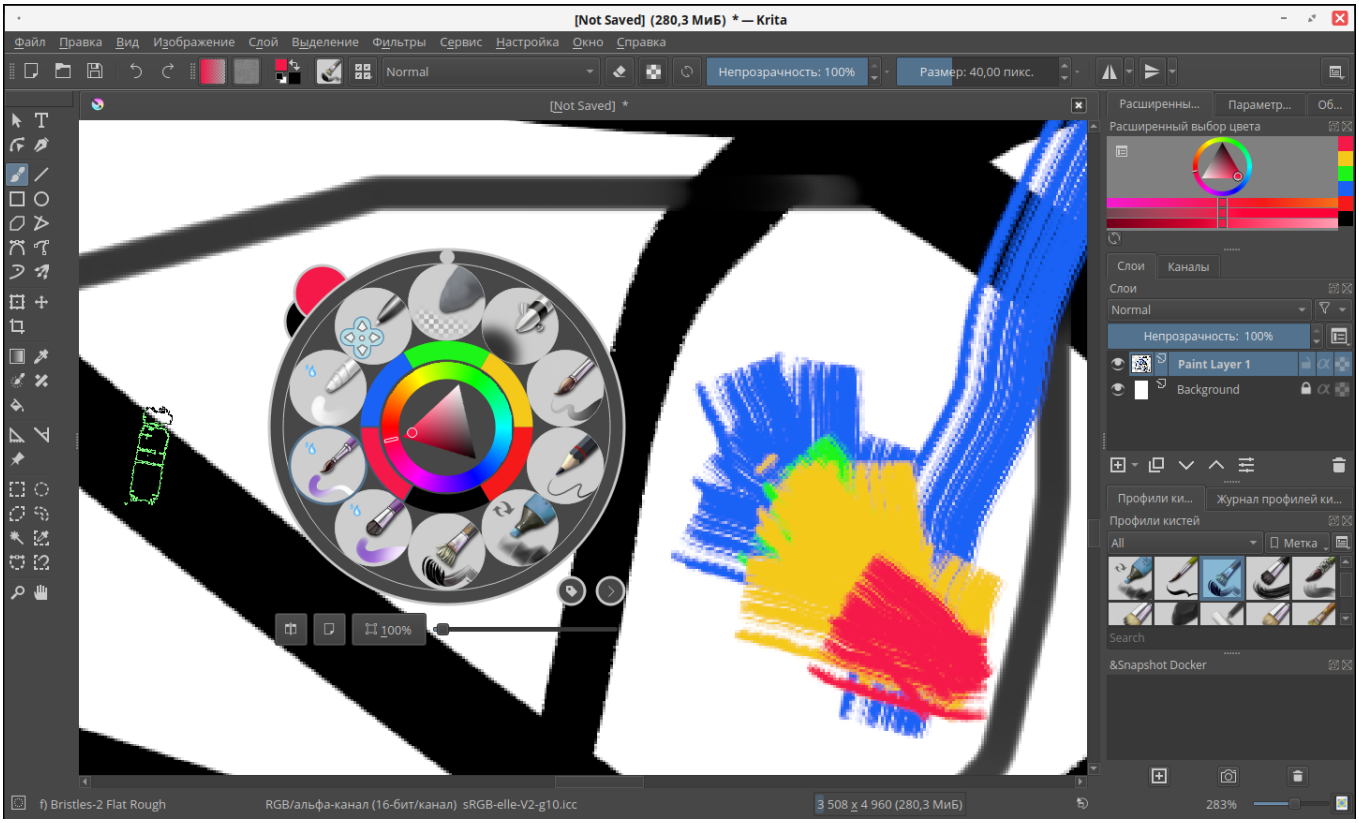
В открывшемся окне параметры холста можно задать вручную либо выбрать преднастроенный шаблон.

Инструмент Кисть

Основным инструментом в **Krita** являются кисти – здесь доступно большое количество кистей различного назначения, таких как кисти для акварели, масляные кисти, карандаши, графитные кисти и пр.

Каждая кисть имеет собственные настраиваемые параметры – прозрачность, размер, форма, текстура и насыщенность краски. Данные параметры можно легко изменять для достижения необходимого эффекта в верхней панели инструментов.

Наиболее часто используемые кисти доступны по нажатии ПКМ на холсте, здесь также доступно изменение параметров выбранной кисти.



Krita предоставляет возможность создания собственных наборов кистей и импорта их в программу, что позволяет пользователям применять в работе собственный стиль и реализовывать индивидуальные творческие потребности.

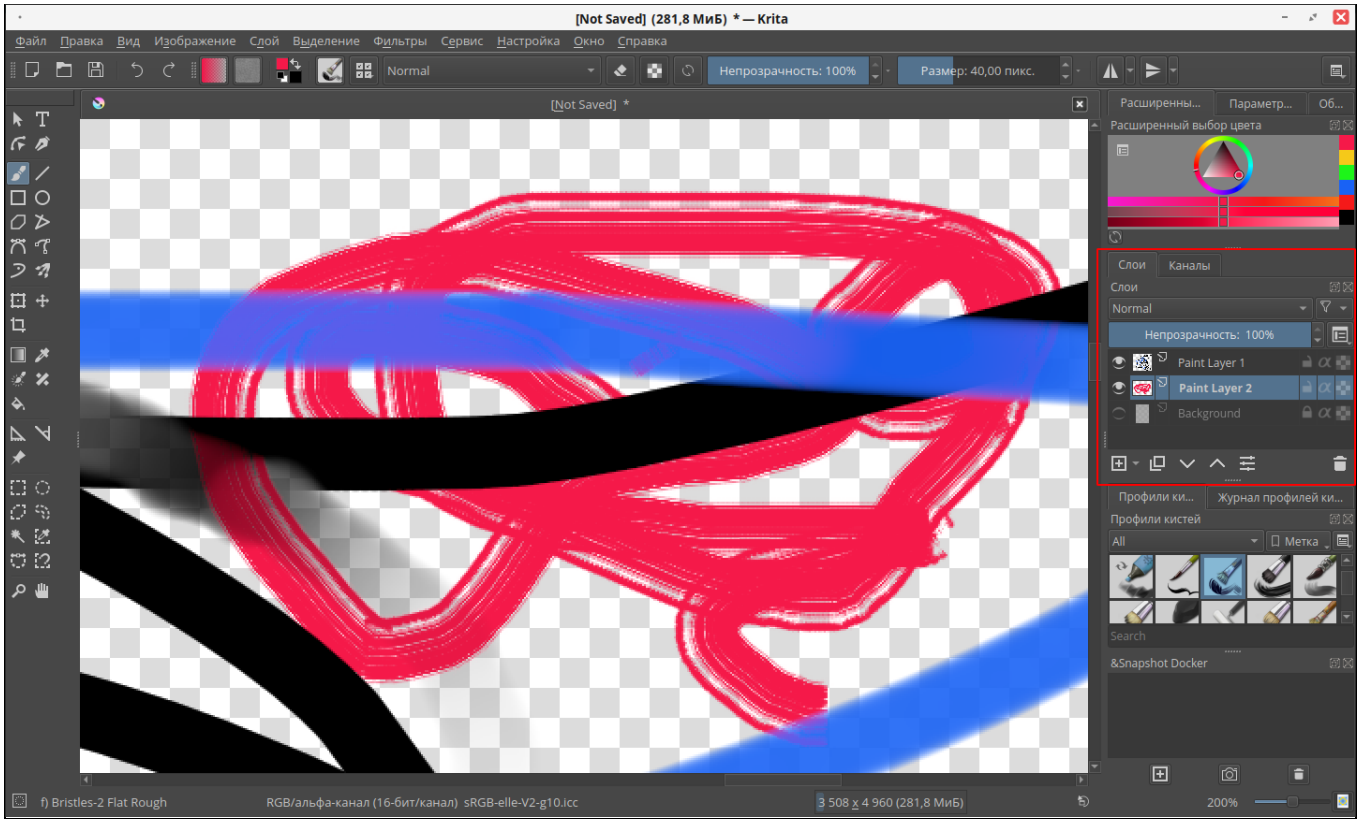
При работе с кистями в Krita также доступны различные инструменты, такие как режимы смешивания, оптическая настройка и настройка параметров нажатия на стилус.

Krita поддерживает работу с таблетками и стилусами, что позволяет имитировать рисование на бумаге или холсте.

Работа со слоями

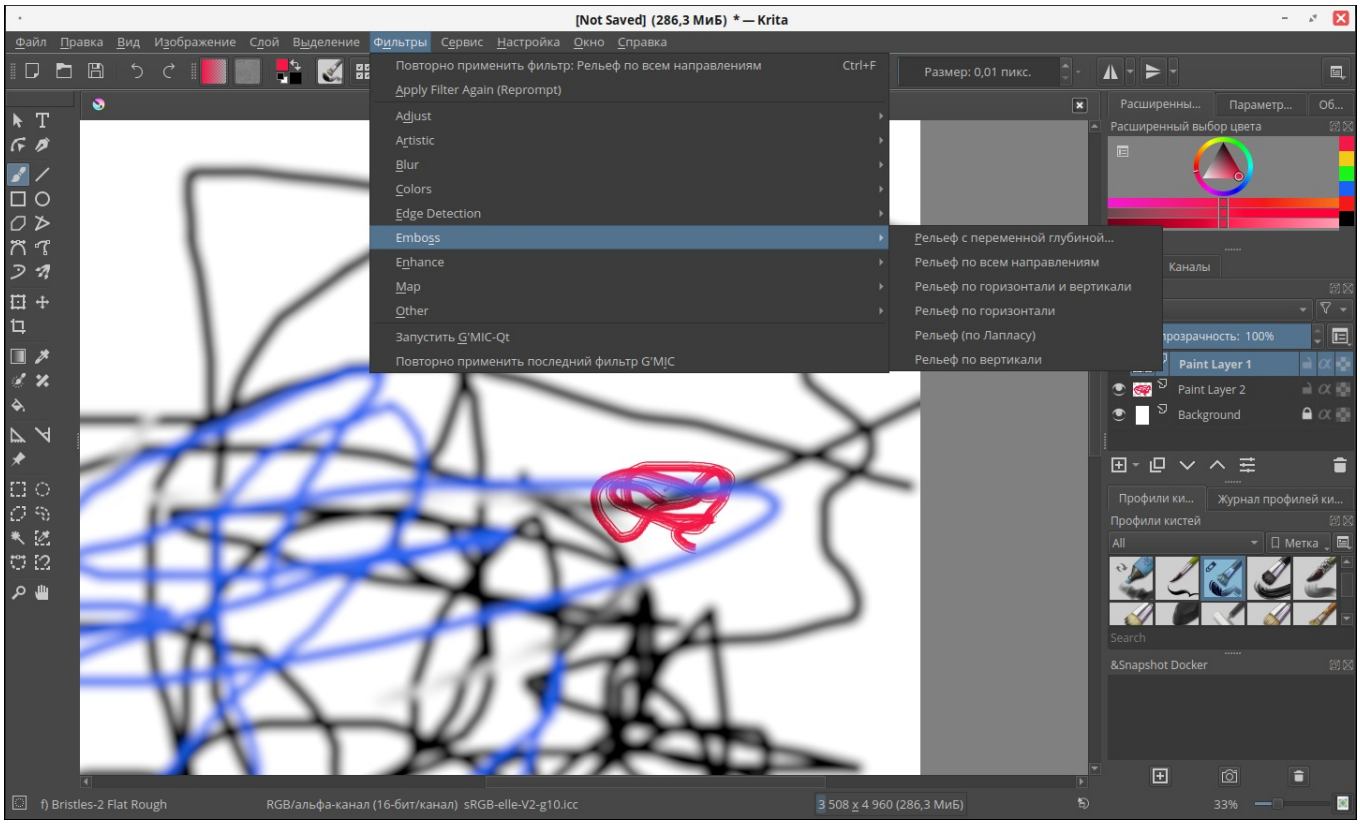
С помощью слоев можно группировать объекты на изображении и выполнять над ними различные действия независимо друг от друга, а также просматривать, как изображение будет выглядеть без этих объектов или модифицировать их в любое время.

Управление доступными слоями производится с помощью компонентов в правой части окна. При выборе определенного слоя он становится активным, и все действия выполняются только на нем.



Применение фильтров

В **Krita** созданное изображение можно улучшить с помощью доступных фильтров изображений, для этого выберите в основном меню программы пункт «**Фильтры**» и примените необходимый фильтр.



Анимация и векторная графика

Krita также предоставляет широкий спектр возможностей для работы с анимацией и векторной графикой.

Основные возможности работы с анимацией:

- создание и редактирование анимированных изображений;
- использование временных слоев для создания плавных переходов между кадрами;
- управление временными интервалами и скоростью анимации;
- импорт и экспорт различных форматов анимаций, включая **GIF**, **AVI**, **MP4**.

Основные возможности работы с векторной графикой:

- создание и редактирование векторных объектов;
- применение различных эффектов и фильтров к векторным элементам;
- использование кривых Безье и редактирование точек управления для создания сложных форм;
- экспорт векторных изображений в форматы **SVG** и **PDF**.

Сохранение результатов

Для сохранения готового изображения или анимации в основном меню программы выберите «**Файл**» – «**Сохранить**». По умолчанию программа сохраняет результат работы в формате ***.kra**.

Программы для сканирования в РЕД ОС

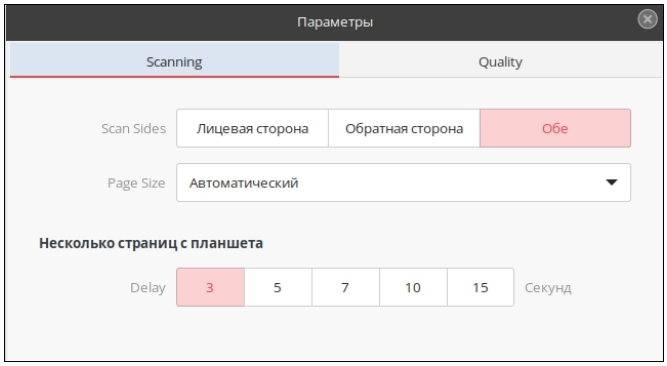
Simple Scan
XSane
GIMP-XSane

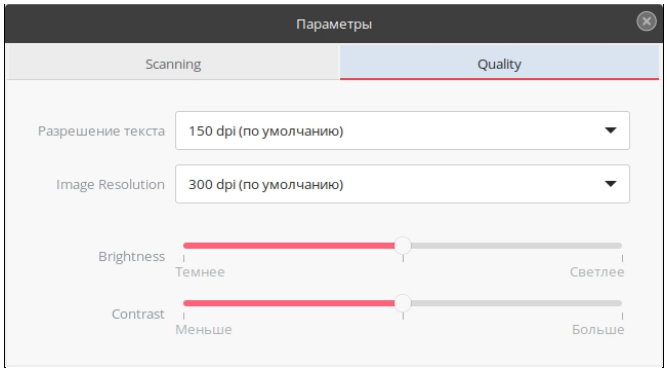
Simple Scan

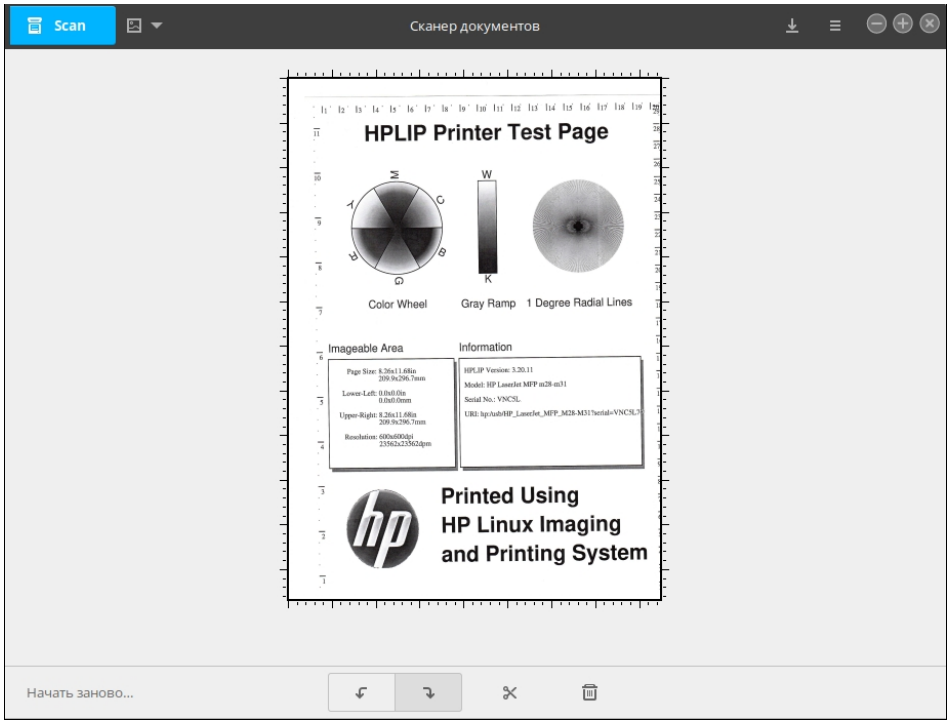
Simple Scan (англ. *simple scan* — простое сканирование) — программа для работы со сканерами; является графическим интерфейсом для прикладной программы **SANE**, которая, в свою очередь, предоставляет стандартизированный доступ к устройствам сканирования растровых изображений.

Simple Scan включает в себя базовый набор функций и настроек для сканирования, такие как установка размера страницы, выбор сканируемой стороны документа, задержка загрузки (в секундах для нескольких страниц), качество отсканированного документа, яркость и контрастность.

Изменение любого из этих параметров доступно в меню настроек окна программы.







Для сканирования документа необходимо нажать в верхнем левом углу кнопку «**Scan**». После успешного сканирования вы можете сохранить изображение в форматах:

- .PDF (многостраничный);
- .JPEG (сжатый);
- .PNG (без потерь качества);
- .WebP (сжатый).

Дополнительно **Simple Scan** позволяет сразу отправлять результат сканирования по почте, распечатать изображения, настроить организацию страниц, настроить параметры сканирования под себя.

Также есть возможность отредактировать полученное изображение с помощью простейшего меню взаимодействия, состоящего из поворотов изображения и его обрезки, или отсканировать документ заново.

XSane

XSane — компьютерная программа для работы с устройствами сканирования изображений. Является графическим интерфейсом для программы *SANE*. Связка пакетов *SANE* и *XSane* поможет сканировать изображение или негатив пленки на вашем сканере. Поддерживается пакетное сканирование в «полуавтоматическом» режиме (минимальное нажатие кнопок).

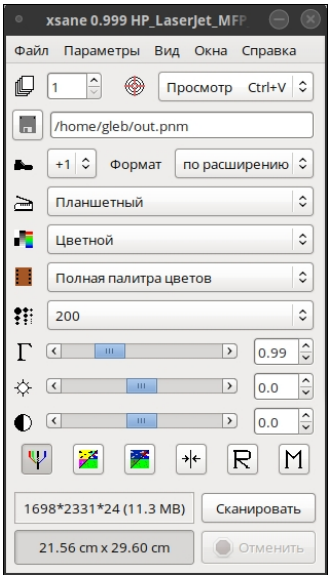
Основные функции программы:

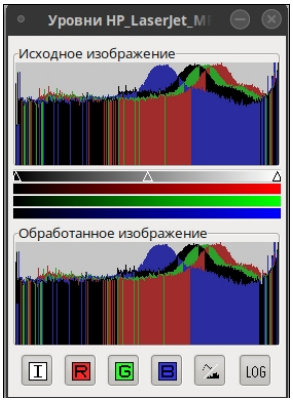
1. Предварительное сканирование (просмотр).
2. Автоматическая корректировка цветов.
3. Ручное и автоматическое выделение необходимой области для сканирования.
4. Раздельная настройка разрешения сканирования по ширине и длине изображения.
5. Печать на принтере отсканированных изображений.
6. Отправка изображения на печать. По умолчанию это производится командой **lpr** протокола *Line Printer Daemon* (**LPD**).
7. Отправка изображения программе оптического распознавания текста (при её наличии в операционной системе).
8. Создание многостраничных документов (пакетное сканирование).
9. Многооконный интерфейс.

Команда для установки *XSane*:

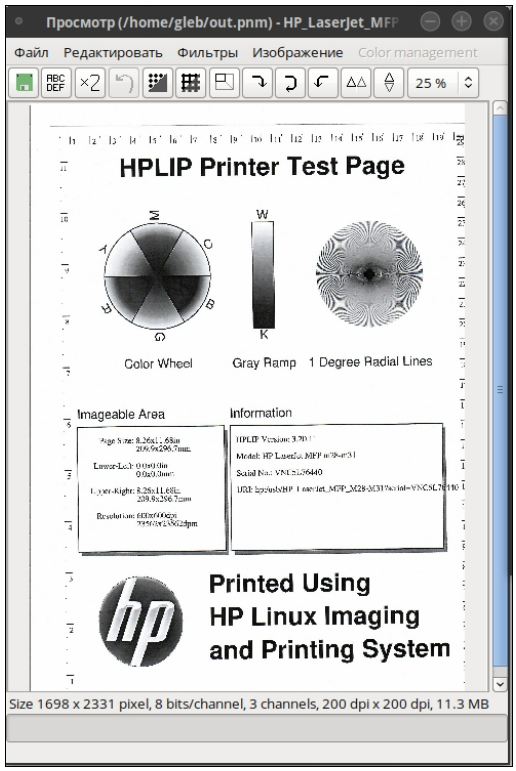
```
# dnf install xsane
```

После установки программа доступна в *Главном меню — Графика*. После запуска программы и выбора необходимого оборудования появляются окна настройки сканирования и контрастности.





После настройки всех доступных параметров и нажатия кнопки «**Сканировать**» будут доступны функции редактирования изображения, а именно: поворот изображения, размытие, масштабирование, отражение по горизонтали и вертикали, обрезка.



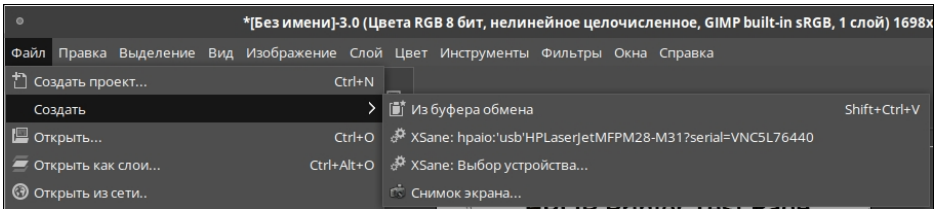
GIMP-XSane

GNU Image Manipulation Program (GIMP) — свободно распространяемый растровый графический редактор, программа для создания и обработки растровой графики с частичной поддержкой работы с векторной графикой.

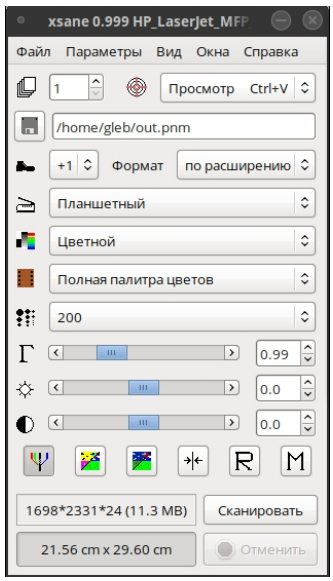
Также *XSane* может работать совместно с *GIMP*, как плагин для последнего. Для установки плагина выполните команду:

```
# dnf install xsane-gimp
```

Чтобы начать сканирование, в меню нажмите «**Файл**» - «**Создать**» - «**XSane: выбор устройства...**».

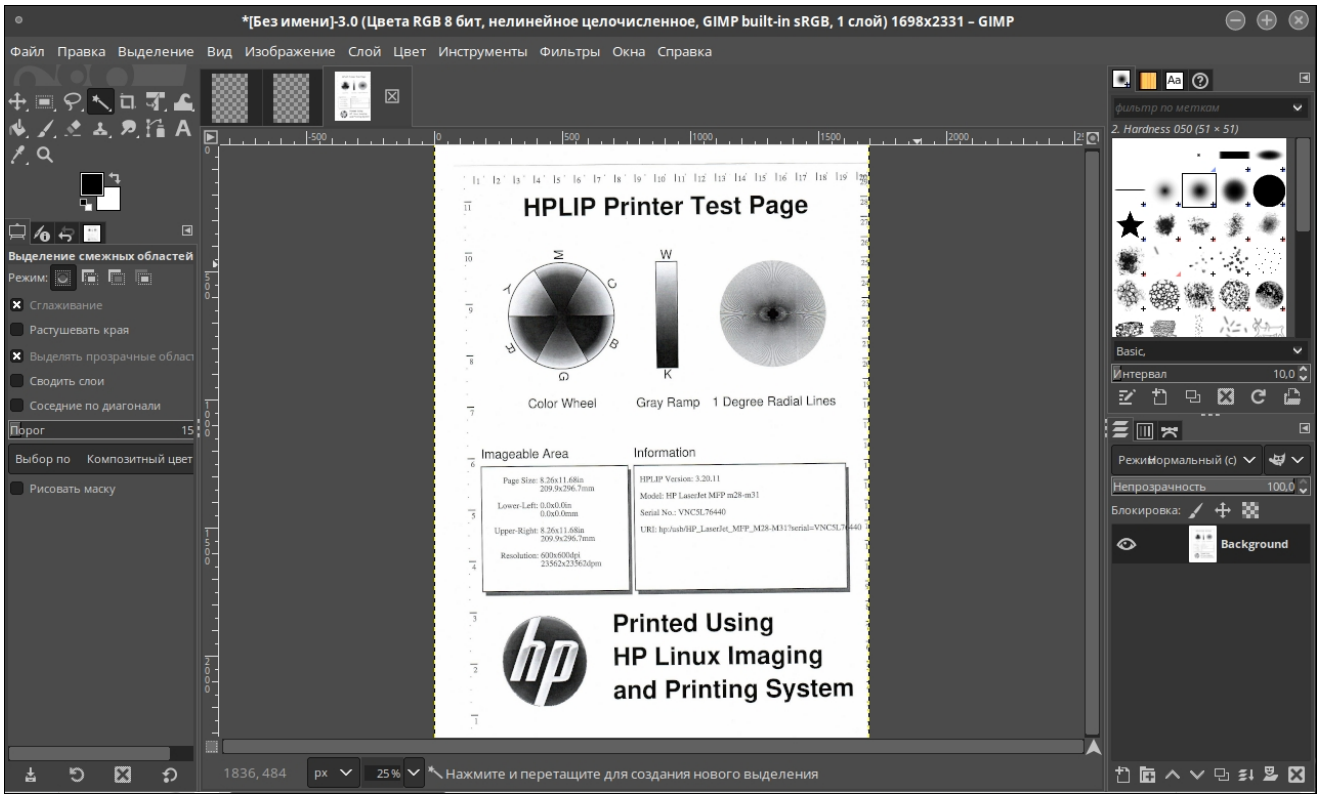


Появится окно настройки параметров сканирования изображения *XSane*.



После индивидуальной настройки всех требуемых параметров нажмите кнопку «**Сканировать**», по завершении сканирования

полученное изображение при необходимости можно отредактировать.



gscan2pdf - программа для сканирования и обработки документов

Возможности программы
Установка gscan2pdf
Параметры сканирования документа
Работа с отсканированными объектами
Распознавание текстов на сканах
Общие параметры настроек gscan2pdf

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** gscan2pdf-2.8.0-1

Gscan2pdf – программа для создания файлов в формате **PDF** или **DjVu** из отсканированных документов, которая позволяет выполнять простые операции, такие как обрезка, поворот и удаление страниц. *Gscan2pdf* может сканировать несколько страниц одновременно.

Возможности программы

Основные возможности программы:

- Сканирование и сохранение документов в форматы: **pdf, gif, jpeg, png, pnm, ps, tiff, hOCR**;
- Сохранение отдельно выделенных страниц;
- Импорт файлов следующих форматов: **jpg, png, pnm, ppm, pbm, gif, tif, tiff, pdf, djvu, ps, gs2p**
- Инструменты для минимальной обработки изображений при сканировании: повороты, установка порога, очистка документа, негатив и кадрирование;
- Встроенная функция распознавания отсканированного документа (OCR - англ. optical character recognition). Для использования **OCR** необходимо настроить **tesseract** или **Cuneiform**.

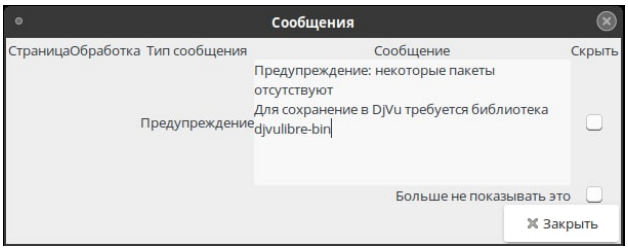
Установка gscan2pdf

Установка *gscan2pdf* в РЕД ОС 7.3 выполняется командой:

```
dnf install gscan2pdf
```

После установки программа доступна из «**Главного меню**» - «**Графика**» - «**gscan2pdf**».

При первом запуске возможно появление предупреждающего сообщения вида:



Для решения данной проблемы необходимо установить дополнительную библиотеку командой:

```
dnf install djvulibre
```

Параметры сканирования документа

Для начала работы нажмите на значок сканирования в главном окне программы или сочетание клавиш «**CTRL+G**». При этом откроется диалоговое окно предварительной установки параметров сканирования, а также выбор модели сканера.

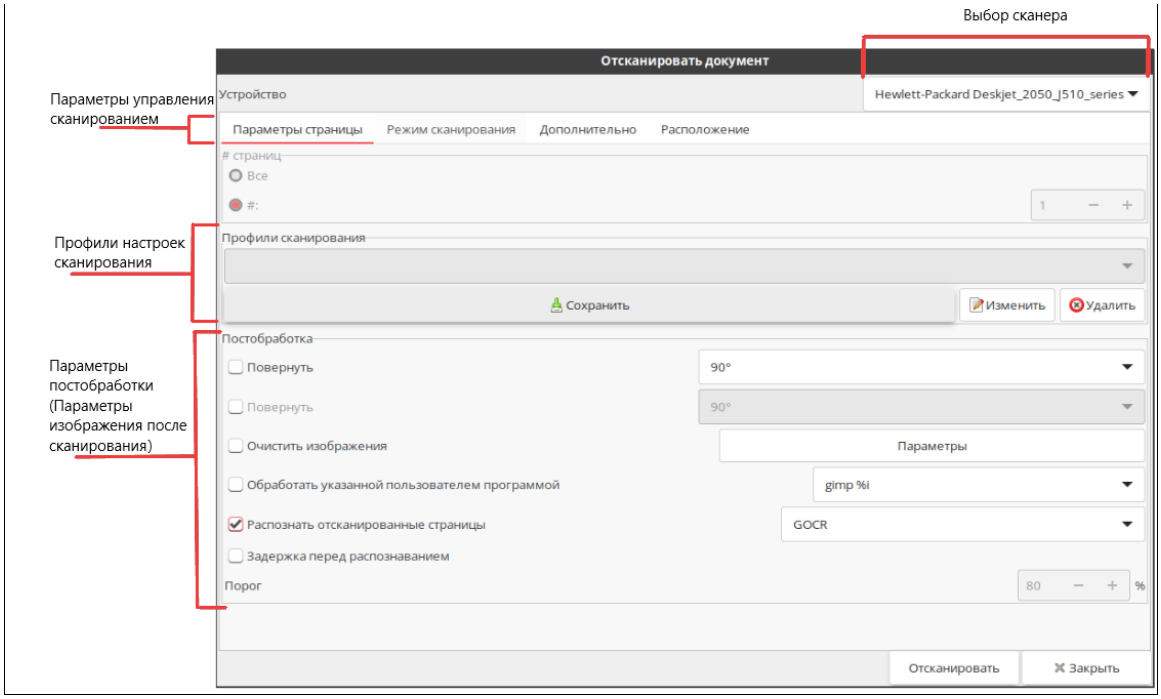


Рисунок 1 – Параметры сканирования

Вкладка «Параметры страницы»

На данной вкладке пользователь может настроить:

- выбор количества страниц;
- выбор профиля сохраненных настроек для сканирования;
- параметры постобработки:
  - поворот изображения;
  - очистка изображения;
  - обработка изображения отдельными программами;
  - включение/выключение автоматической функции распознавания страниц.

Вкладка «Режим сканирования»

В режиме сканирования доступен выбор цвета сканируемого объекта – черно-белый, цветной, штриховой. Также имеется возможность изменить разрешение сканирования, которое определяет качество сканируемого объекта в пкс/дюйм. (от 75 до 1200 пкс/дюйм).

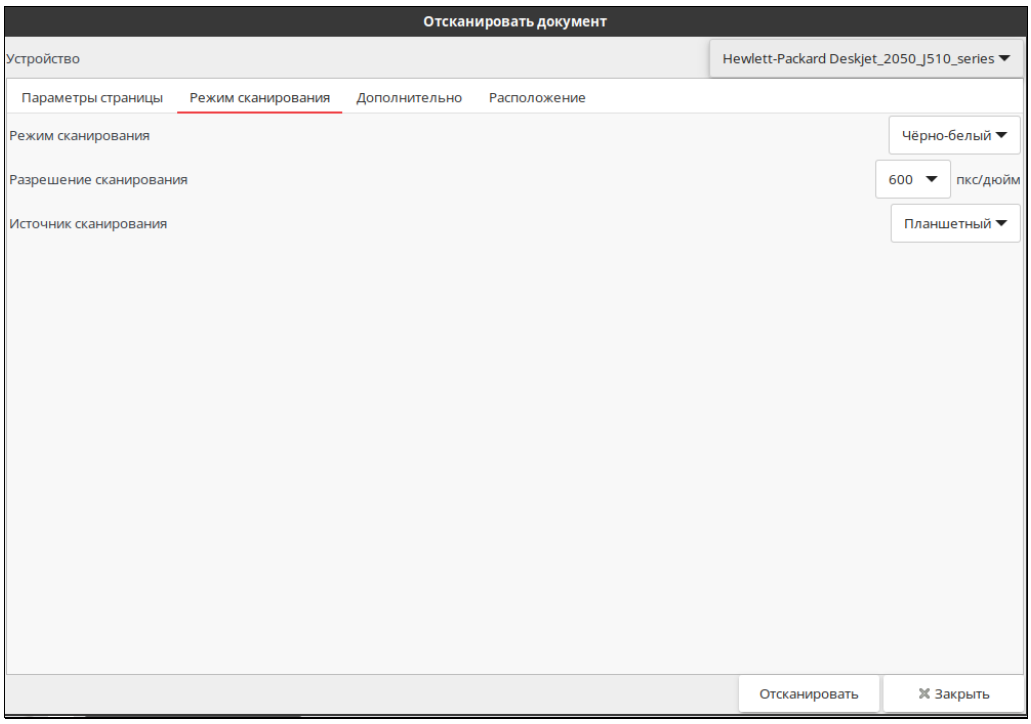


Рисунок 2 – Режим сканирования

Вкладка «Дополнительно»

На вкладке «**Дополнительно**» настраивается яркость, контрастность и метод сжатия изображения.

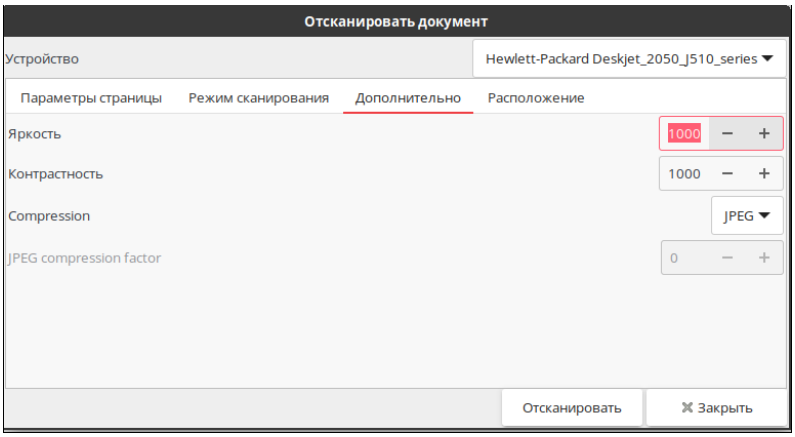


Рисунок 3 – Дополнительные параметры

Вкладка «Расположение»

На вкладке «**Расположение**» выбирается формат бумаги.

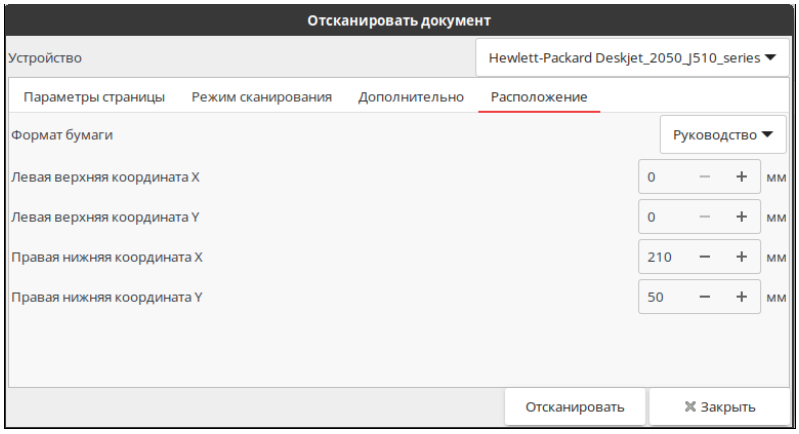


Рисунок 4 – Параметры расположения

Работа с отсканированными объектами

Отсканированное изображение при необходимости можно отредактировать. Из элементов редактирования здесь имеется: поворот изображения, масштабирование, порог (отвечает за насыщенность изображения), яркость/контраст, негатив, не резкая маска, кадрирование.

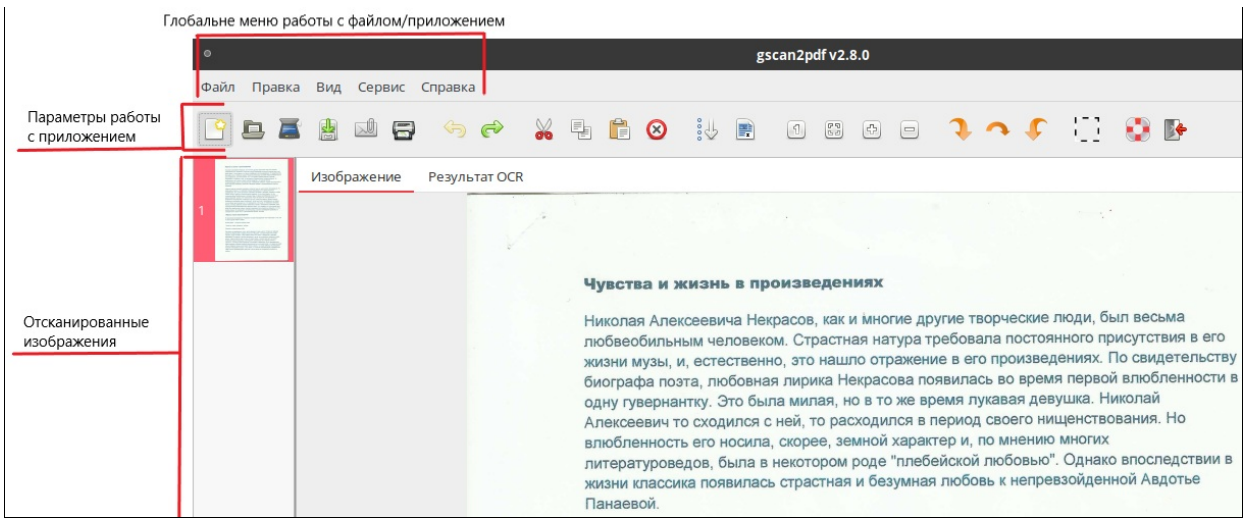


Рисунок 5 – Окно работы с отсканированными изображениями

При сохранении отсканированного документа открывается диалоговое окно с настройками, в котором можно настроить следующие параметры для сохраняемого документа:

- изменение диапазона страниц;
- выбор формата, в котором сохраняется изображение;
- установка даты и времени;
- описание и указание автора;
- снижение разрешения;
- сжатие изображения;
- выбор шрифта для не-ASCII текста;
- перехват после сохранения - это указанные пользователем дополнительные команды (программы) обработки изображений.

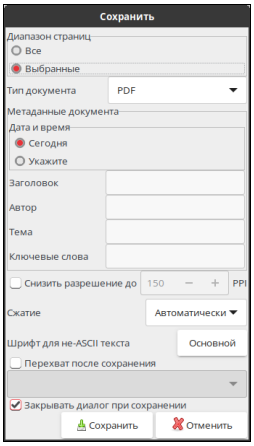


Рисунок 6 – Сохранение изображения

Распознавание текстов на сканах

Сперва необходимо установить доступные движки для распознавания текстов. Команда для установки **cuneiform**:

```
dnf install cuneiform
```

Стандартная установка у **tesseract** в отличие от с**uneiform** не содержит языковой пакет для русского языка, поэтому его нужно установить дополнительно. Для установки **tesseract** используется следующая команда:

```
dnf install tesseract tesseract-langpack-rus
```

После этого можно приступать непосредственно к распознаванию текста, для этого необходимо:

1. Импортировать или отсканировать необходимые файлы.
2. После завершения загрузки файлов перейти в «**Сервис**» - «**Распознать текст**».

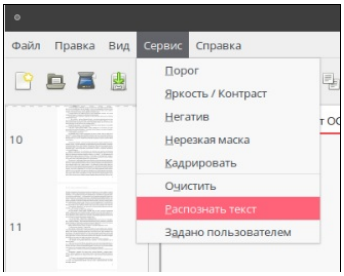


Рисунок 7 – Расположение вкладки распознавания текста

3. Откроется окно OCR, в котором доступны следующие настройки:
    - Диапазон страниц;
    - Движок OCR;
    - Языки распознавания;
    - Задержка перед распознаванием;
    - Порог.

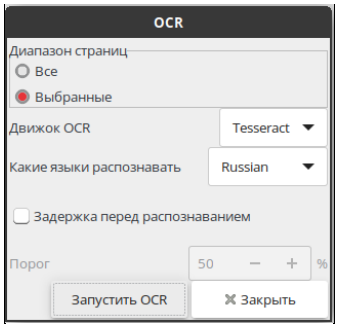


Рисунок 8 - Окно настроек OCR

4. После указания настроек можно запускать распознавание. Если документ имеет большое количество страниц, процесс может занять некоторое время.
5. После завершения процесса для каждой страницы появится ее распознанная копия в окне «**Результат OCR**». При необходимости можно редактировать результаты распознавания, для этого следует воспользоваться нижней панелью. После завершения можно сохранить результат в нужном формате.

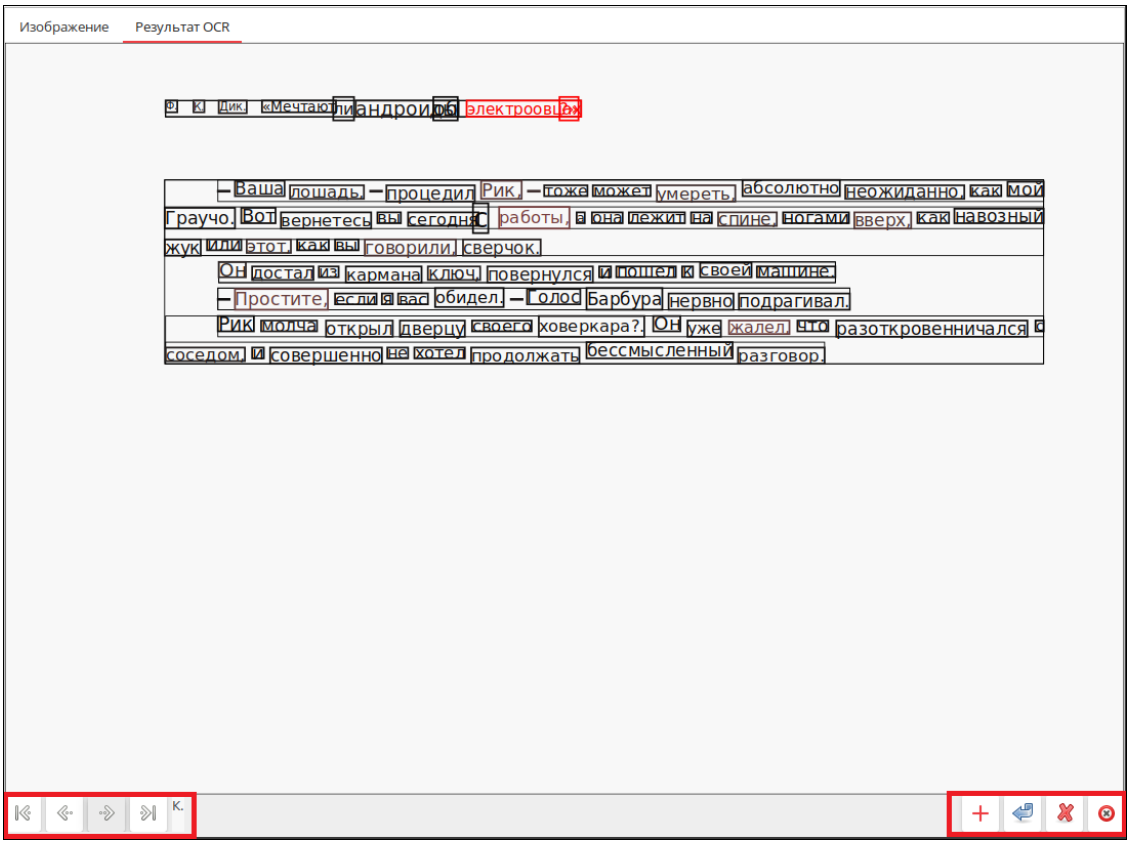


Рисунок 9 - Расположение кнопок панели редактирования

Общие параметры настроек gscan2pdf

В меню «**Правка**» – «**Параметры**» можно настроить общие параметры сканирования, например:

- выбор графического интерфейса - назначается интерфейс для доступа к сканеру;
- черный список устройств;
- возможность пакетного сканирования с планшетного сканера («**Пакетное сканирование**» — способ одновременной оцифровки нескольких оригиналов, установленных или закрепленных в сканере).

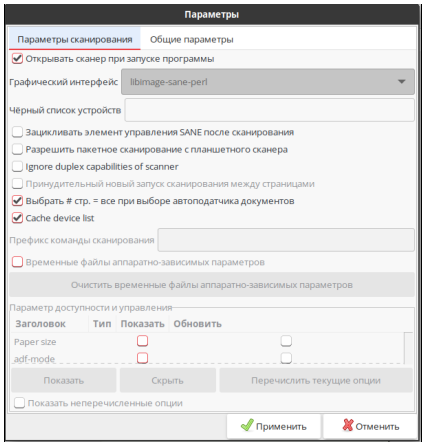


Рисунок 10 – Параметры сканирования

На вкладке «**Общие параметры**» доступны следующие настройки:

- изменение формата именования файлов по умолчанию;
- возможность указать временный каталог;
- включить/выключить просмотр файла после сохранения и др.

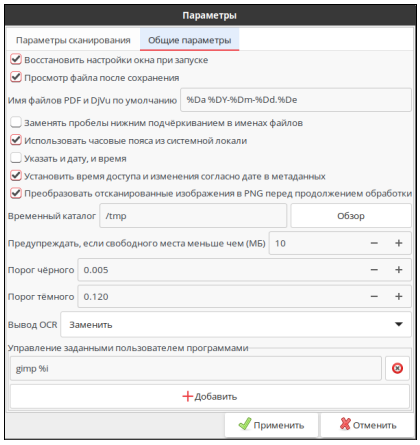


Рисунок 11 – Общие параметры

NAPS2 – программа для сканирования документов и изображений

Возможности
Установка
Запуск
О программе
Пакетное сканирование
Настройка
Сканирование
Распознавание текста с помощью OCR
Импорт
Поворот, обрезка, изменение изображений
Редактирование PDF-файла
Удаление документа

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: naps2-7.1.2

NAPS2 (Not Another PDF Scanner 2) — это программа, которая позволяет сканировать документы и изображения, сохраняя их в форматы PDF, JPEG, PNG или TIFF.

NAPS2 поддерживает различные типы сканеров и обладает интуитивно понятным интерфейсом.

Возможности

К основным возможностям программы NAPS2 можно отнести:

1. Сканирование документов — позволяет подключить сканер и сканировать документы с различными настройками.

2. Обработка изображений — после сканирования NAPS2 предоставляет инструменты для обработки изображений.

3. Сохранение в различных форматах — позволяет сохранять отсканированные документы в формате PDF или в виде отдельных изображений (например, JPEG или PNG).

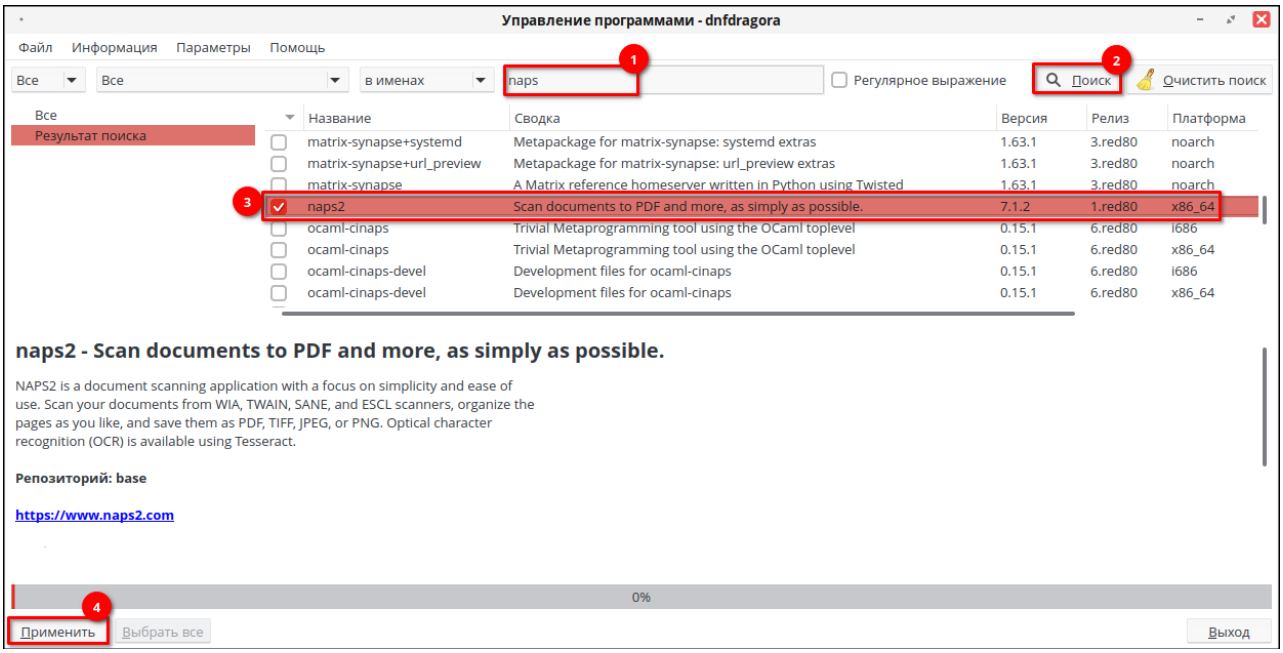
4. Функциональность — программа предлагает различные настройки для сканирования и сохранения, включая выбор профиля сканирования, настройку качества изображения, выбор расположения сохраняемых файлов и другие.

5. Пакетная обработка — поддерживает пакетную обработку, что означает возможность сканирования и обработки нескольких документов одновременно.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**naps**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



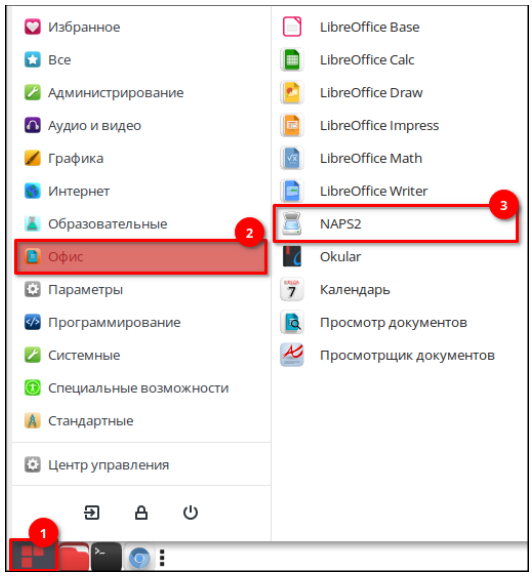
Для установки NAPS2 через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install naps2
```

Запуск

Запустить программу можно либо через меню приложений, либо через терминал.

Для запуска программы сканирования документов через меню приложений перейдите в «**Главное меню**» — «**Офис**» — «**NAPS2**».

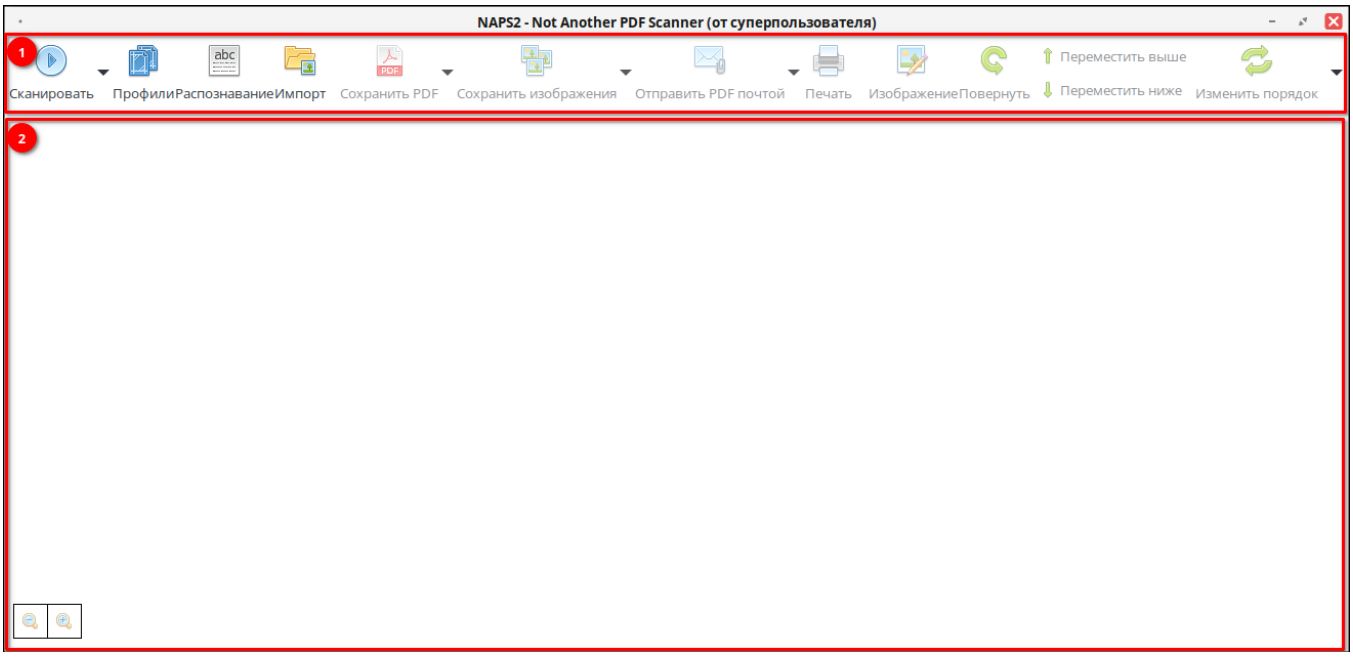


Для запуска NAPS2 через терминал выполните команду:

```
naps2
```

О программе

Главное окно программы выглядит следующим образом:



В верхней части окна расположена панель инструментов (1), где доступны основные инструменты для работы со сканируемым файлом. Основную часть окна занимает рабочая область (2), на которой располагаются открытые документы.

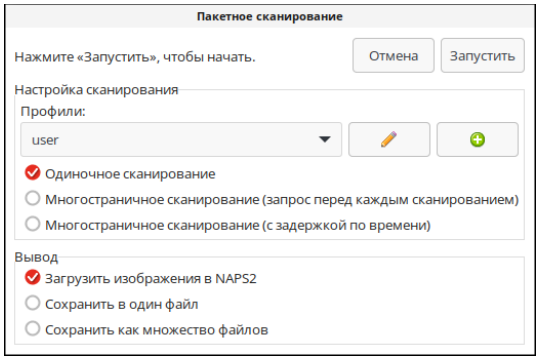
Инструменты:

- Сканировать (Пользователь, Профиль, Пакетное сканирование);
- Профили;
- Распознавание;
- Импорт;
- Сохранить PDF (Все, Выбранные, Настройки PDF);
- Сохранить изображения (Все, Выбранные, Настройки изображения);
- Отправить PDF почтой (Все, Выбранные, Параметры эл.почты, Настройки PDF);
- Печать;
- Изображение;
- Повернуть;
- Переместить выше;
- Переместить ниже;
- Изменить порядок;
- Удалить;
- Очистить;
- Язык;
- О программе.

С помощью инструментов можно перетаскивать страницы в любом удобном пользователю порядке, чередовать страницы для двустороннего сканирования вручную, поворачивать страницы вручную или автоматически под нужным углом, редактировать изображения для обрезки или изменения яркости и контрастности.

Пакетное сканирование

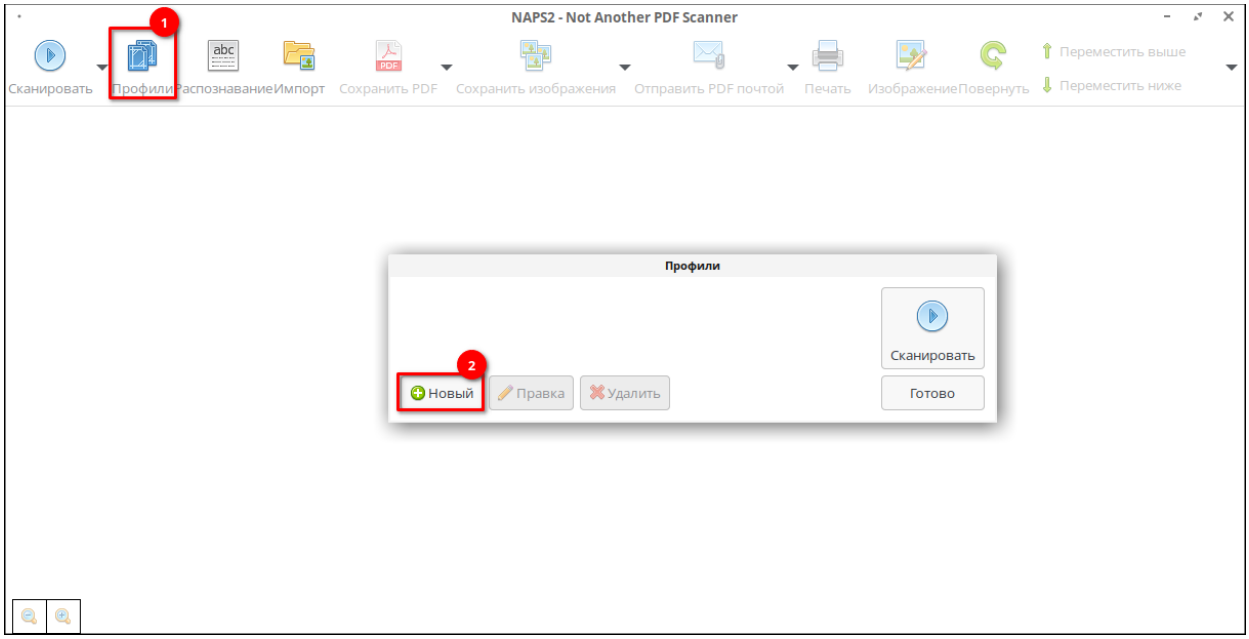
Для использования расширенных функций пакетного сканирования с целью автоматизации задач сканирования перейдите в инструмент «**Сканировать**» — «**Пакетное сканирование**». Можно объединять несколько отсканированных документов вместе, автоматически нумеровать файлы и ставить временные метки.



Настройка

Перед настройкой программы NAPS2 подключите к компьютеру сканер и установите его драйверы.

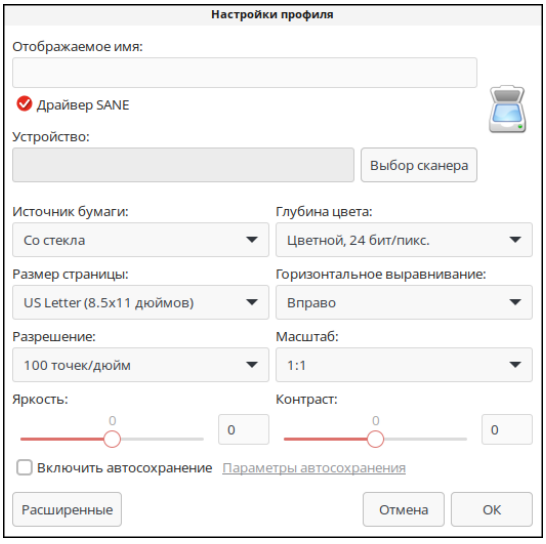
Для настройки нового профиля в главном меню выберите пункт «**Профиль**» (1), а затем в появившемся окне нажмите «**Новый**» (2).



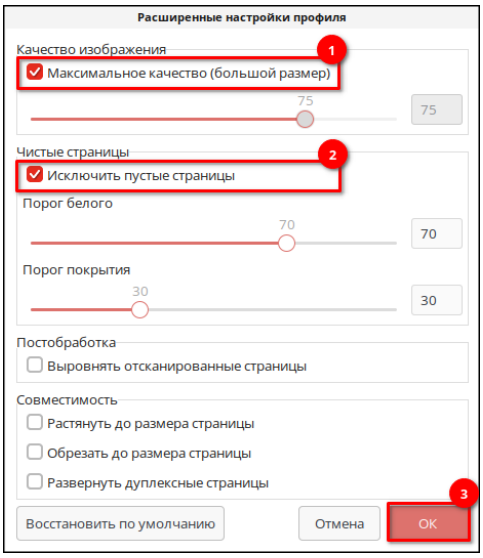
В окне «**Настройка профиля**» введите имя профиля и выберите драйвер. Для подключения к USB-сканерам и сетевым сканерам используйте драйверы SANE и ESCL. Выберите сканер из установленных на компьютере и определите настройки сканера.

Выберите источник бумаги, определите глубину цвета, размер страницы, горизонтальное выравнивание, разрешение и масштаб страницы. Также можно задать параметры автосохранения, установив флаг для соответствующего параметра.

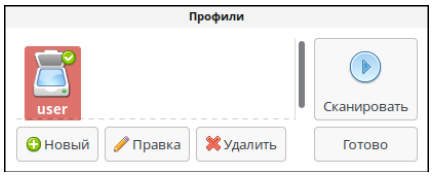
Дополнительно можно задать расширенные настройки профиля.



В окне «Расширенные настройки профиля» в пункте «**Качество изображения**» установите флаг «**Максимальное качество (большой размер)**» (1) и «**Исключить пустые страницы**» (2), закройте окно, нажав кнопку «**OK**» (3).

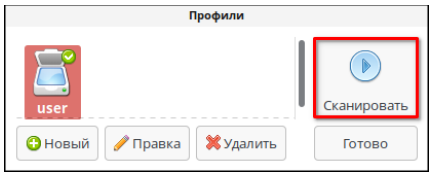


После нажатия кнопки «**OK**» в окне «**Профили**» появится созданный профиль.

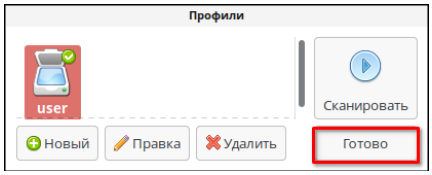


Сканирование

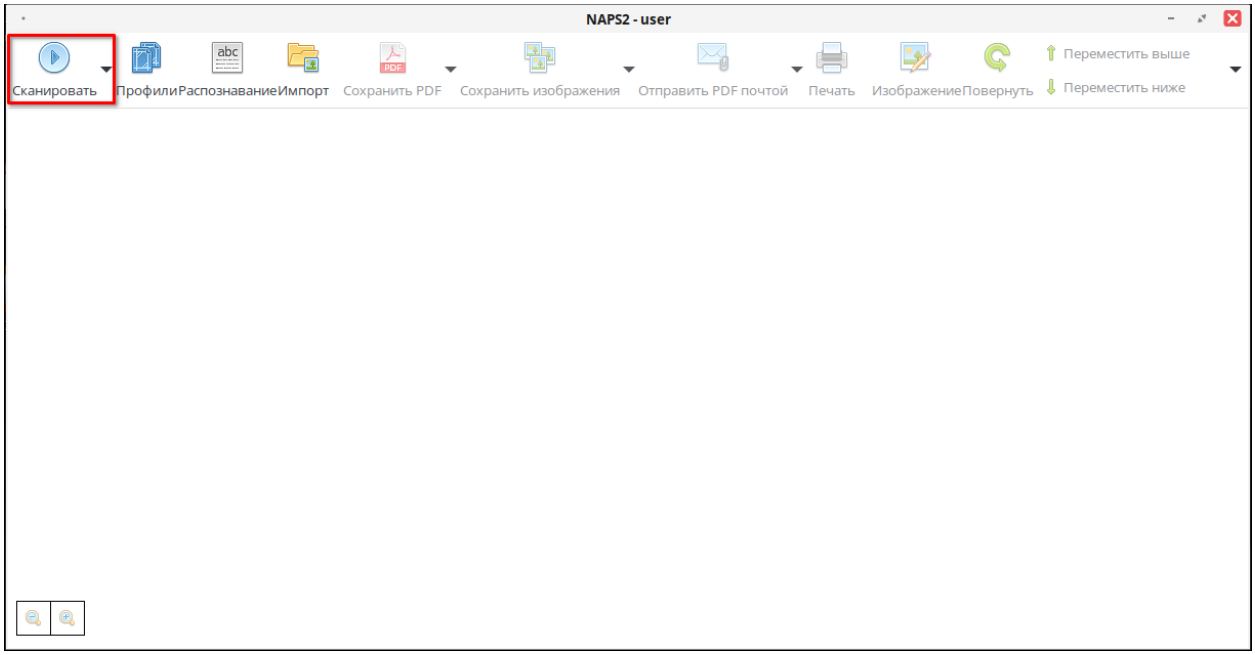
Для сканирования поместите в сканер документ, в окне «**Профили**» выберите нужный профиль и нажмите кнопку «**Сканировать**».



Для закрытия окна нажмите кнопку «**Готово**»:

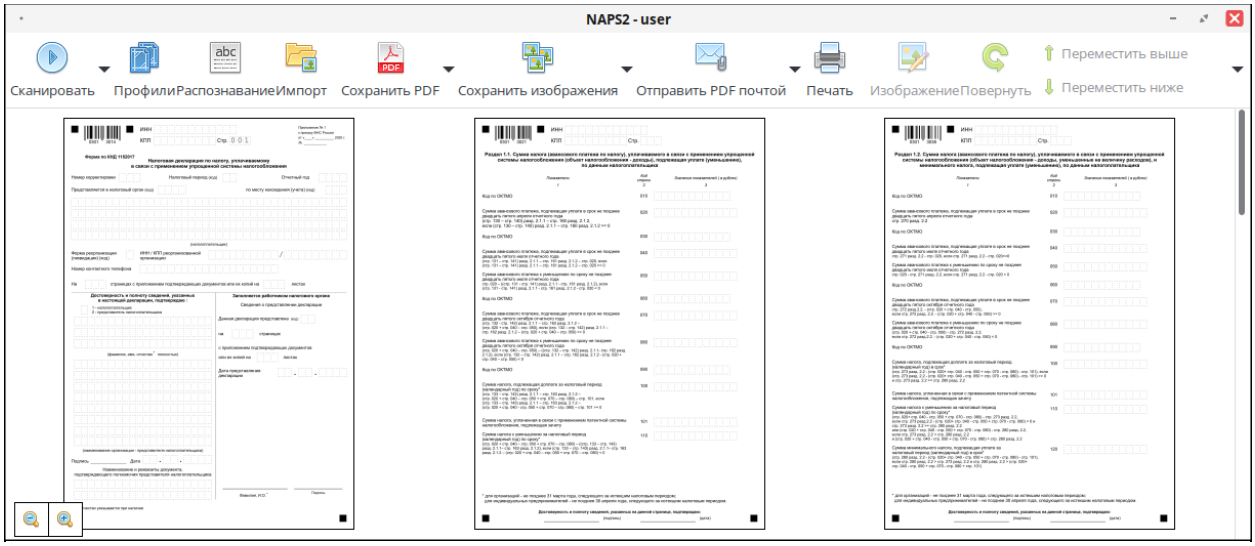


Также можно нажать на кнопку «**Сканировать**» на панели инструментов.

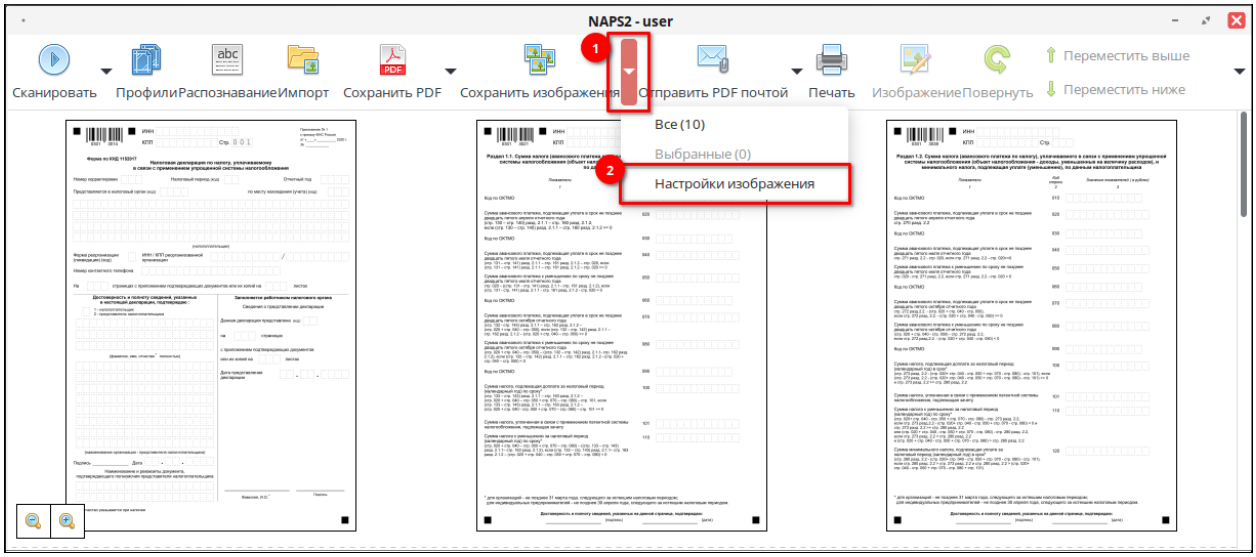


После открытия окна настроек произведите нужные настройки и нажмите «**Сканировать**».

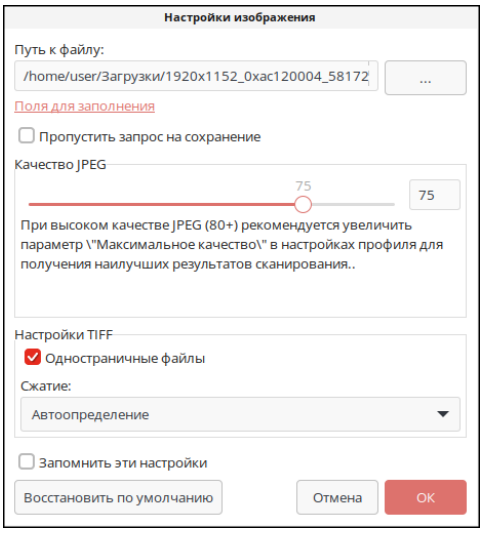
После выполненных действий в главном окне программы отобразится отсканированный документ.



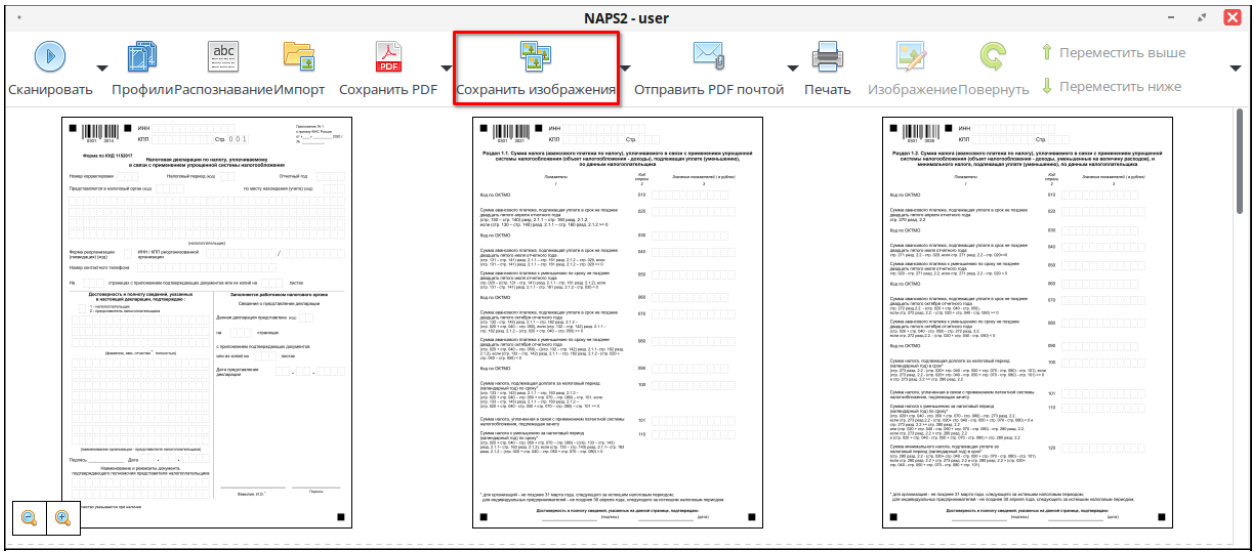
Для определения настроек сохранения нажмите на стрелку рядом с инструментом «**Сохранить изображение**» и выберите в выпадающем меню пункт «**Настройки изображения**».



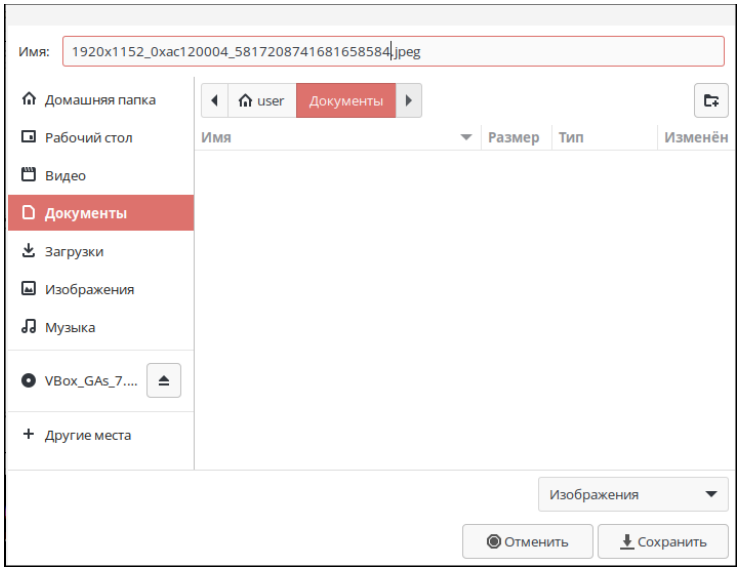
Установите необходимые настройки и нажмите кнопку «**OK**».



Для сохранения изображения нажмите «**Сохранить изображение**».



Выберите имя файла и каталог для сохранения и нажмите «**Сохранить**».

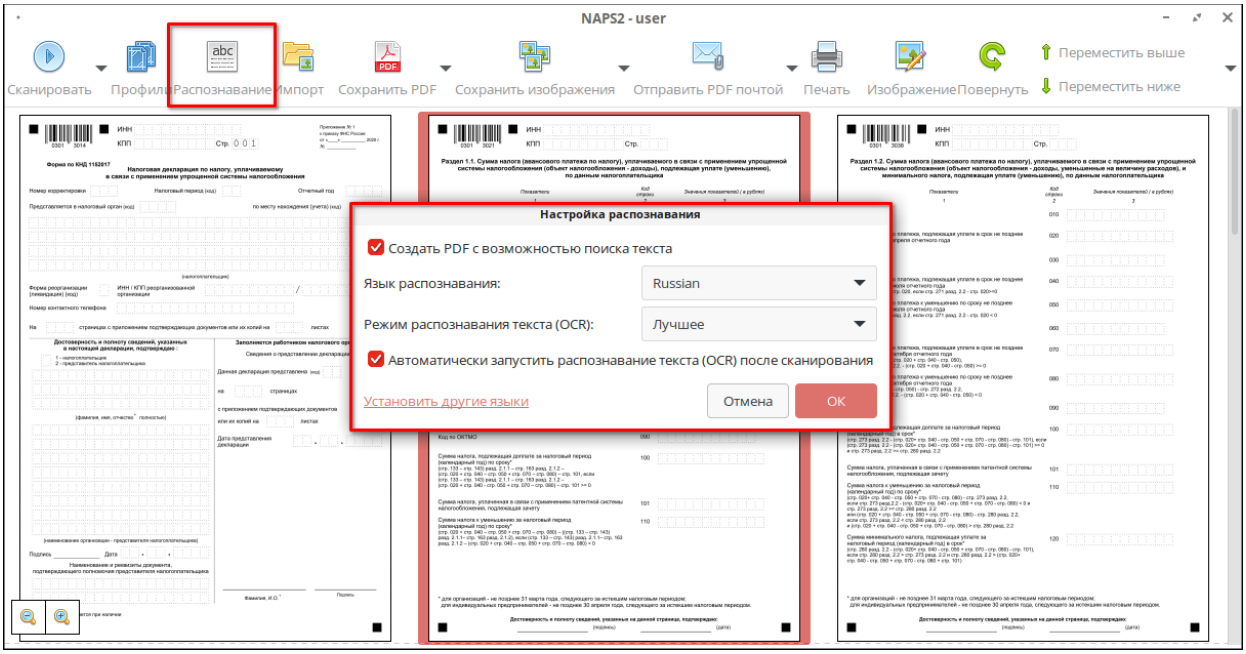


Отсканированный документ будет успешно сохранен.

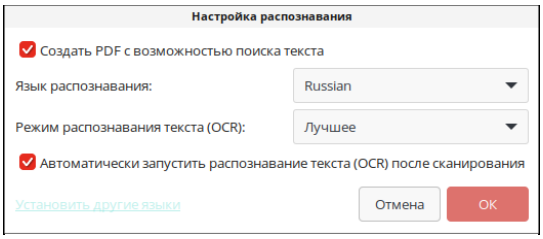
В NAPS2 также доступна возможность отправки отсканированных документов по почте или отправки на печать.

Распознавание текста с помощью OCR

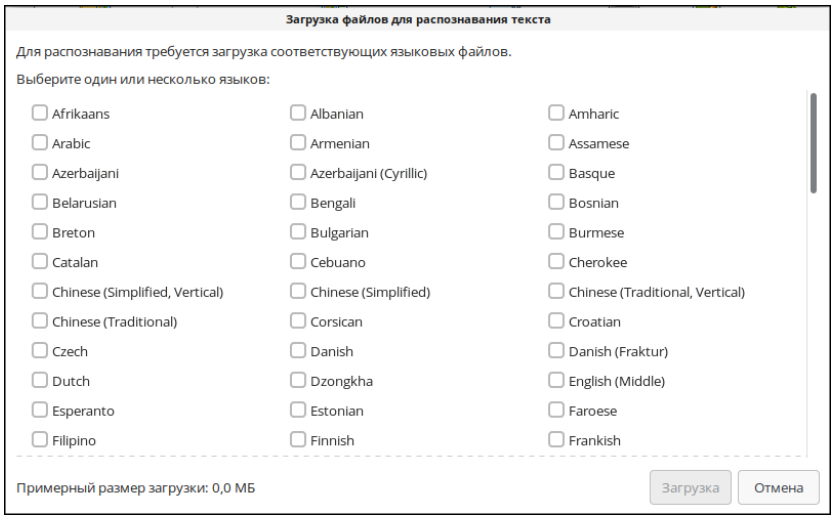
Для выполнения поиска по тексту, включенному в PDF-файлы, с помощью оптического распознавания символов (OCR) на любом из более чем 100 языков выберите инструмент «**Распознавание**».



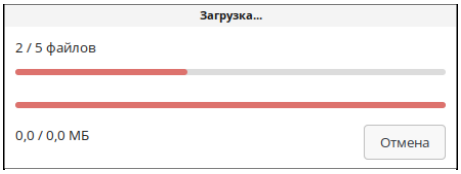
В появившемся диалоговом окне «**Настройка распознавания**» выберите язык и режим распознавания текста, поставьте флаги напротив «**Создать PDF с возможностью поиска текста**» и «**Автоматически запустить распознавание текста (OCR) после сканирования**».



При нажатии на функцию «**Установить другие языки**» можно загрузить дополнительные языковые пакеты.



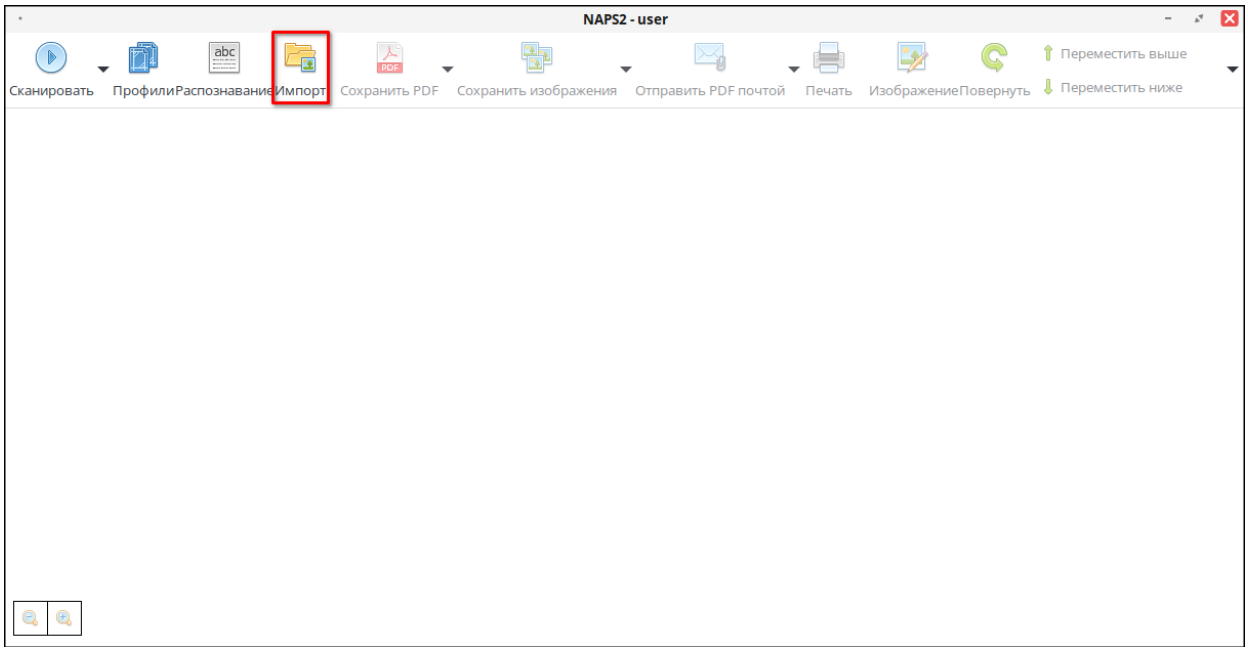
Для загрузки файлов для распознавания текста отметьте флагом нужные языки и нажмите «**Загрузка**». Дождитесь окончания загрузки.



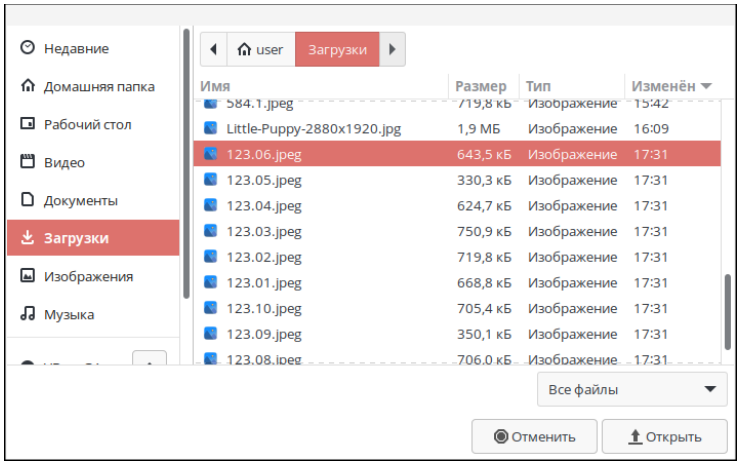
Импорт

NAPS2 может объединять несколько документов в один. Для этого необходимо нажать «**Импорт**» и выбрать нужные документы. Далее выбрать «**Сохранить PDF**» и выбрать пункт «**Все**». Программа сохранит все открытые документы в один. Таким же образом можно

сохранить все страницы документов в форматы *JPEG*, *GIF*, *PNG*.

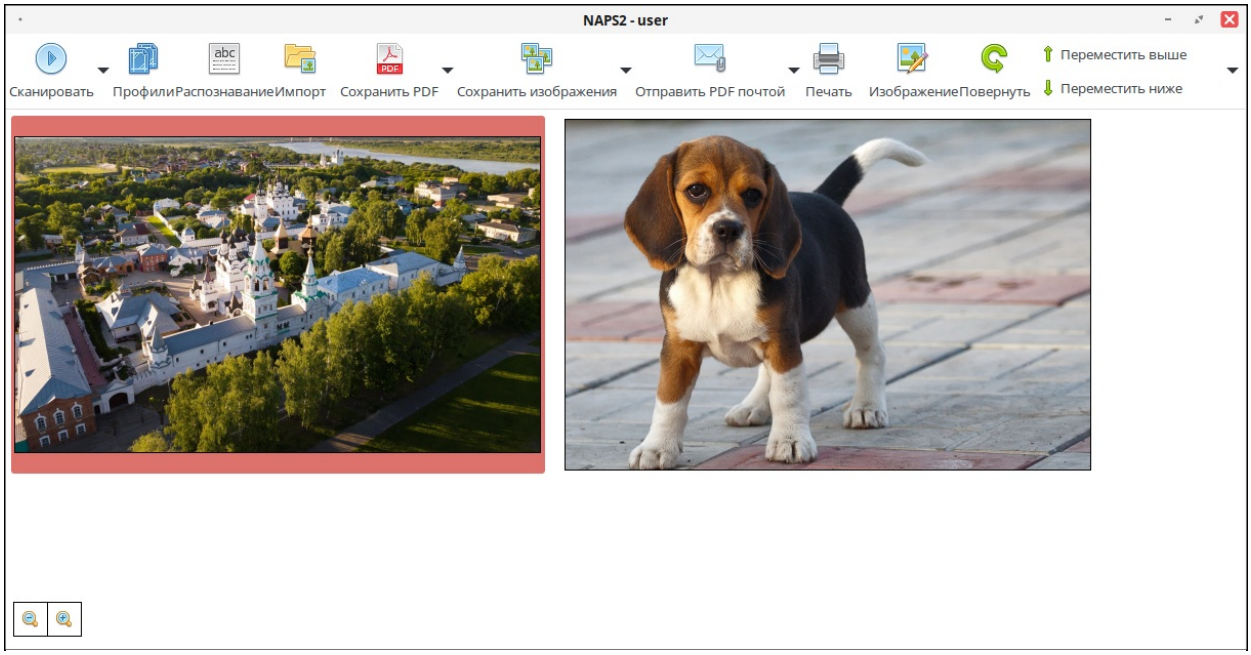


В диалоговом окне выбора файла выберите необходимые документы для импорта на рабочую область и нажмите «**Открыть**».

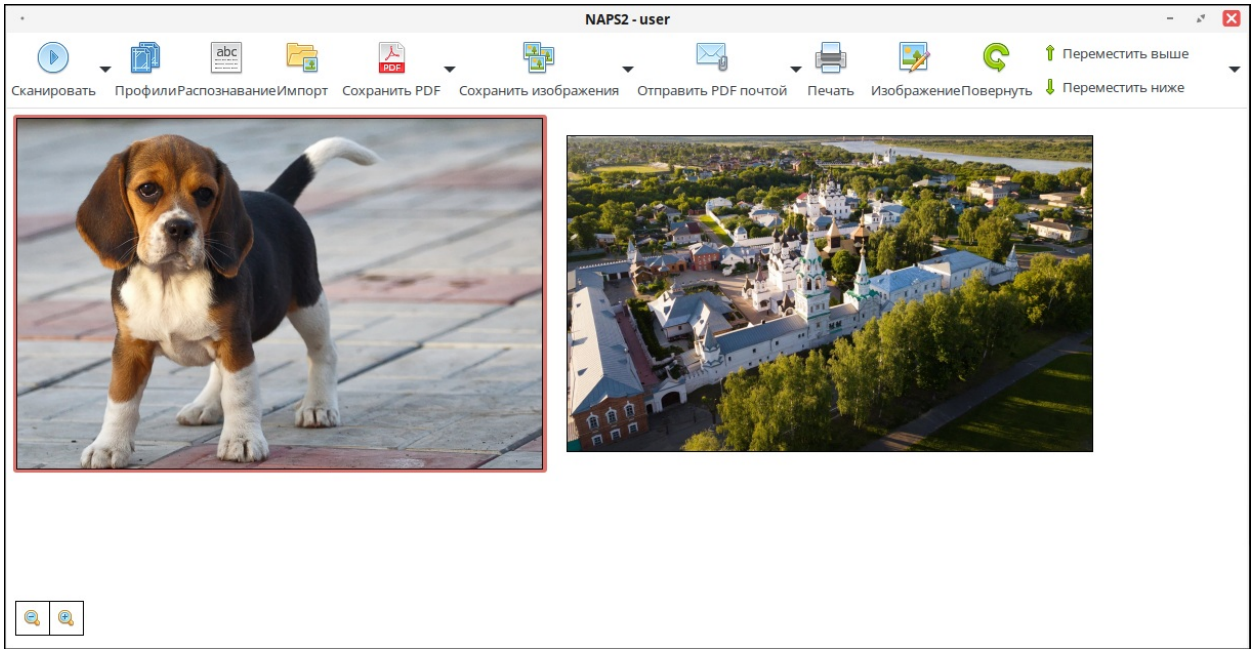


Поворот, обрезка, изменение изображений

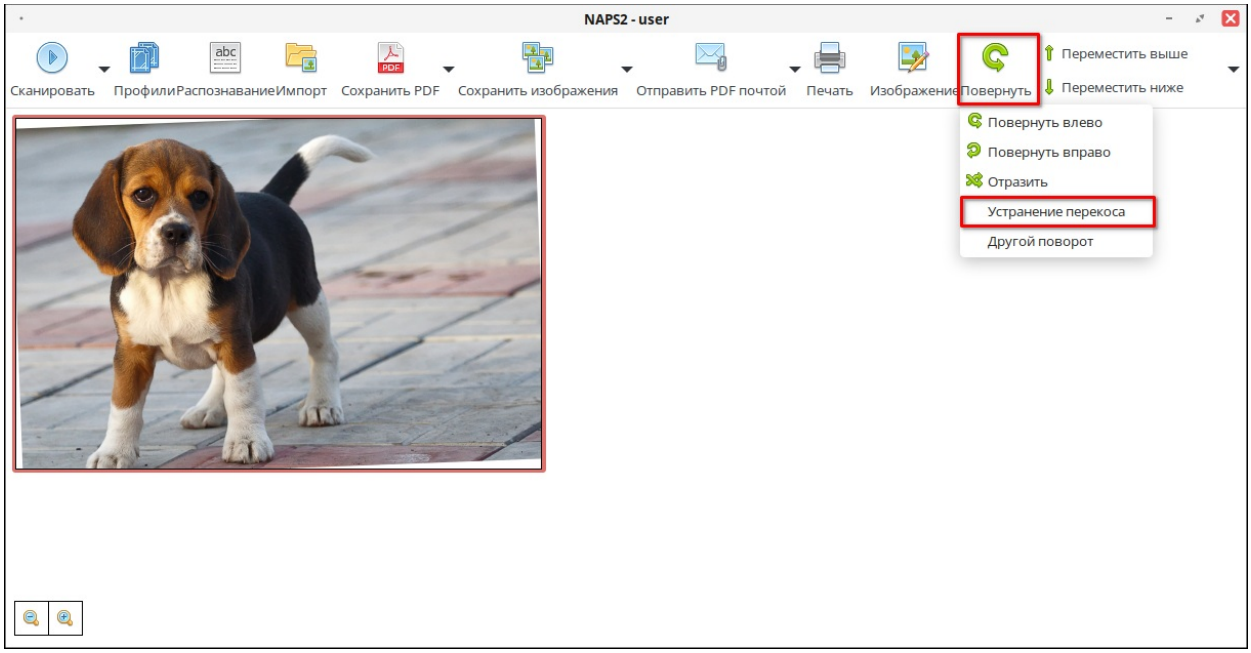
Страницы документов и изображения можно перетаскивать в любом удобном порядке.



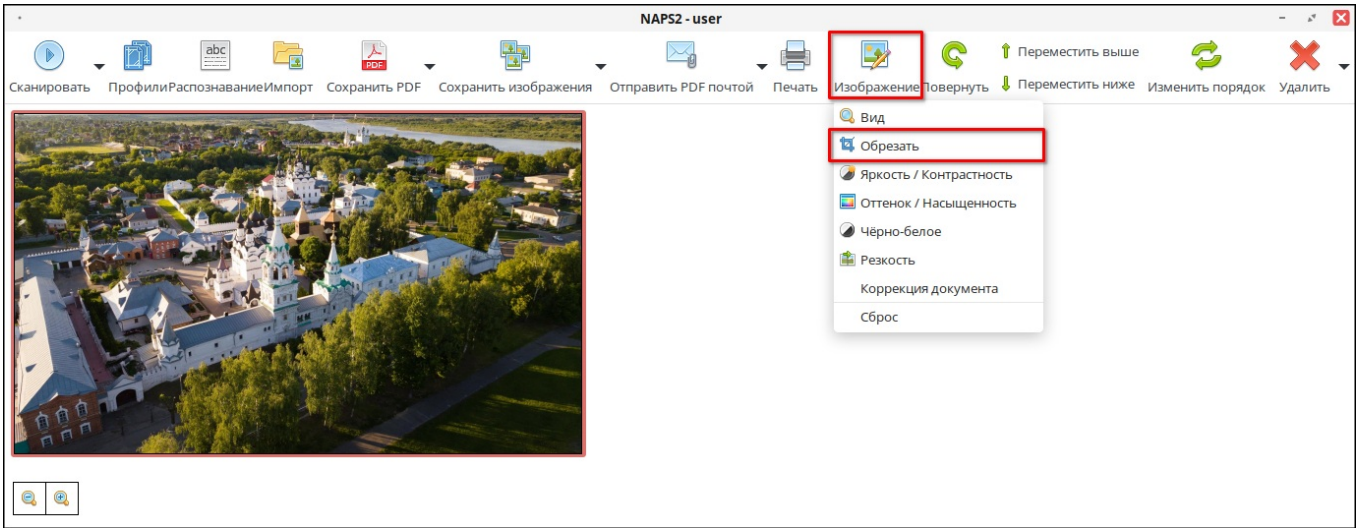
Для этого щелкните по изображению ЛКМ и, удерживая ее, перенесите изображение в нужное место.



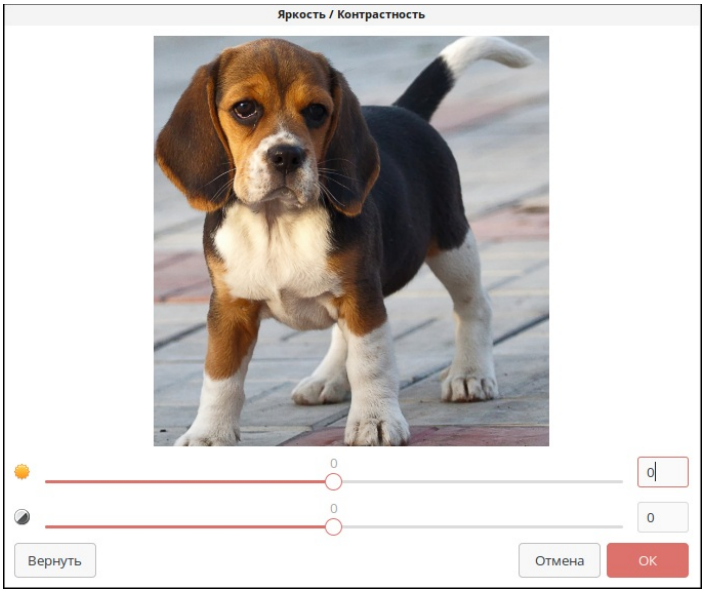
В программе предусмотрены функции поворота изображения вручную или автоматически под прямым углом. Для устранения перекоса на изображении выберите инструмент «**Повернуть**» — «**Устранение перекоса**».



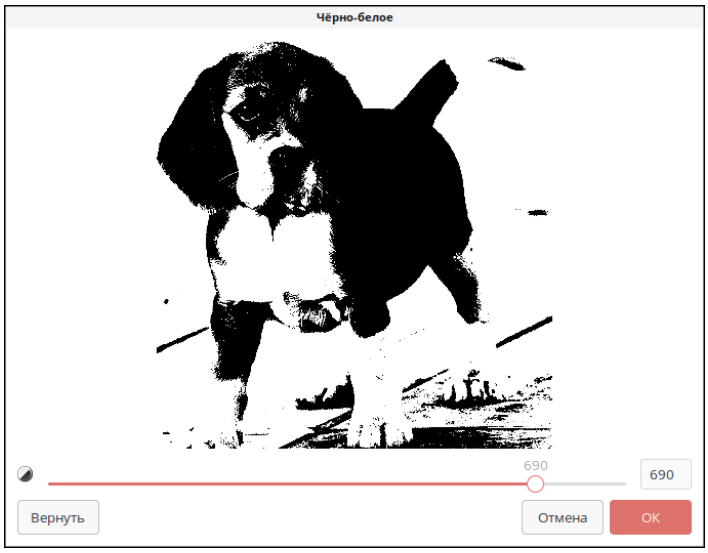
Используйте инструменты редактирования изображений для обрезки. Нажмите «**Изображение**» — «**Обрезать**» и выделите нужную область. После этого нажмите «**OK**».



Для применения функции изменения яркости и контрастности выберите «**Изображение**» — «**Яркость/контрастность**». Далее установите нужные настройки.



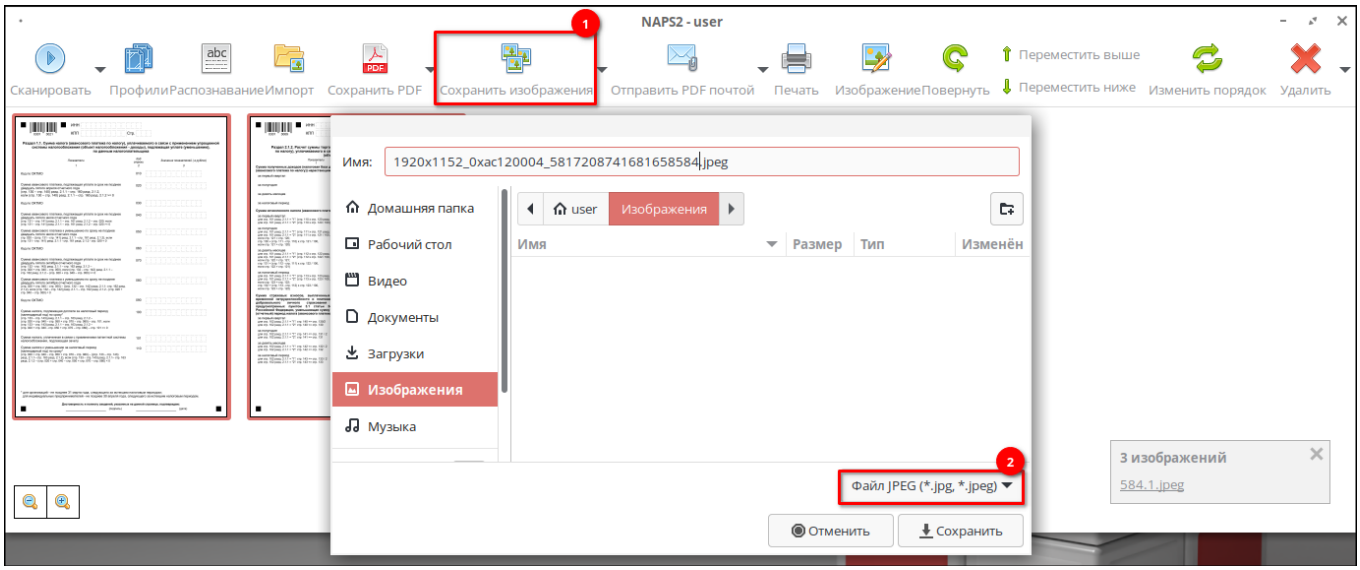
Для перевода изображения в черно-белый формат выберите «**Изображение**» — «**Чёрно-белое**».



Редактирование PDF-файла

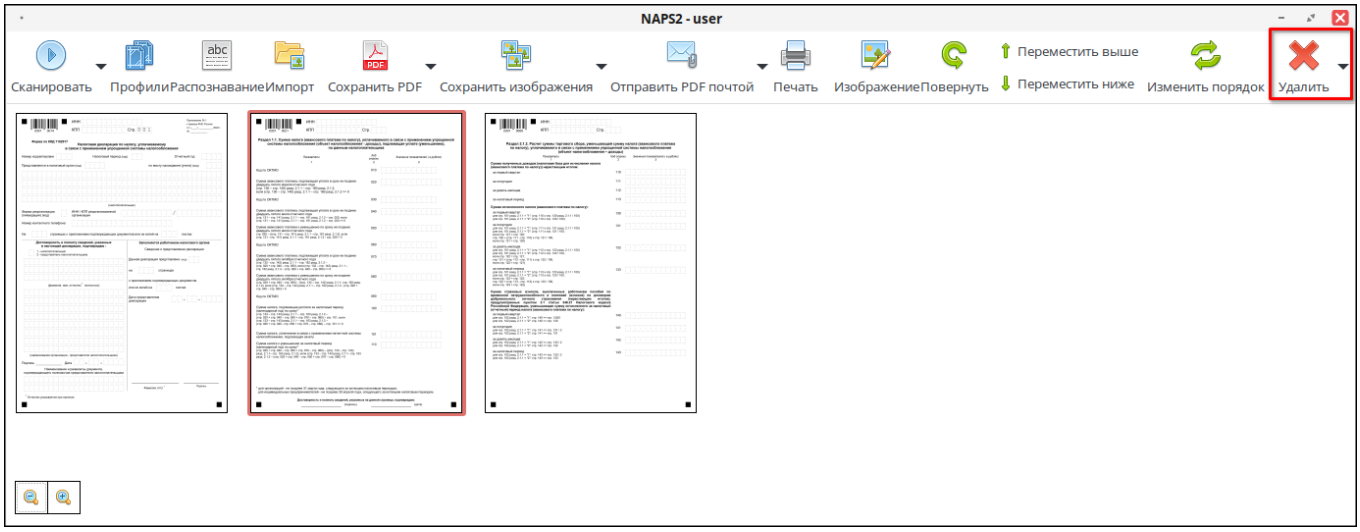
Для редактирования PDF-файла экспортируйте нужный документ в программу NAPS2. Документ будет разложен по страницам, можно удалить ненужные или добавить новые страницы, а также объединить их с другим документом. После выполненных преобразований сохраните подготовленный файл на компьютере как новый документ в формате PDF.

Для изменения формата документа, загруженного в формате PDF, нажмите «**Сохранить изображение**» и выберите нужный формат.

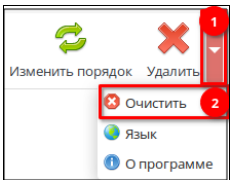


Удаление документа

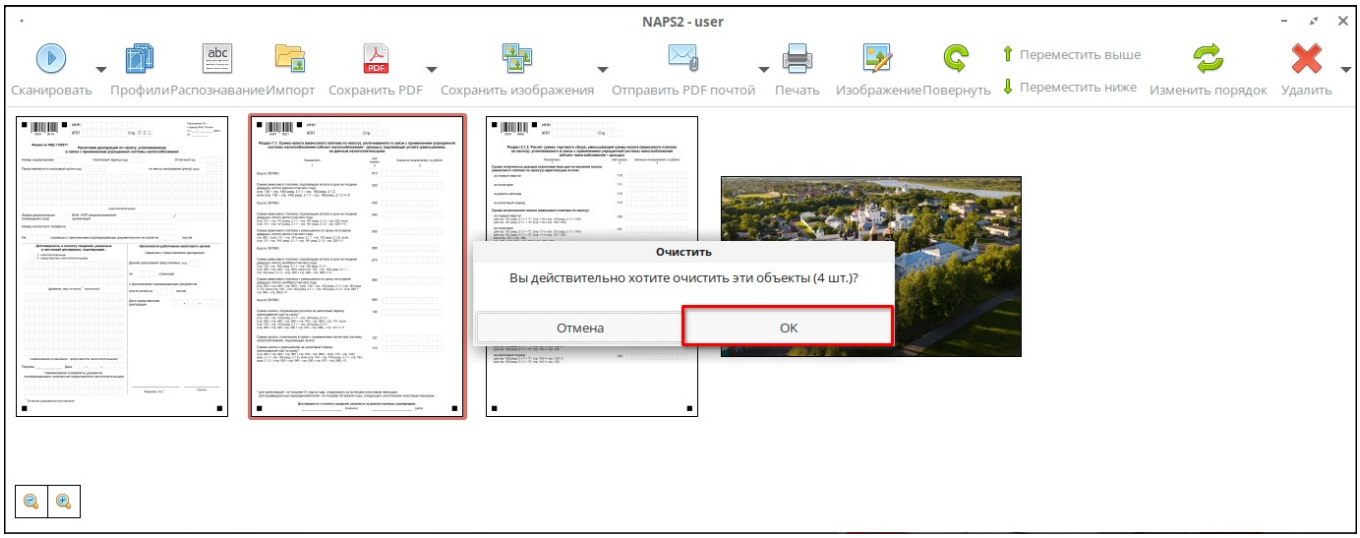
Для удаления страницы документа из рабочей области программы выделите нужную страницу и нажмите на инструмент «**Удалить**».



Для удаления всех документов из рабочей области нажмите на выпадающий список инструмента «**Удалить**» — «**Очистить**».



Появится предупреждающее сообщение об удалении объектов. Для очистки рабочей области нажмите «**OK**».


NAPS2 - user
Сканировать
Профили
Распознавание
Импорт
Сохранить PDF
Сохранить изображения
Отправить PDF почтой
Печать
Изображение
Повернуть
Переместить выше
Переместить ниже
Изменить порядок
Удалить
Очистить
Вы действительно хотите очистить эти объекты (4 шт.)?
Отмена
OK

Каталогизаторы фотоальбомов

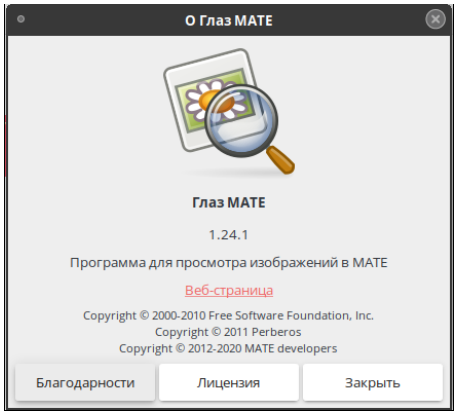
Pix
gThumb

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** eom-1:1.24.1-2, pix-2.6.2-1, gthumb-3.10.1-1

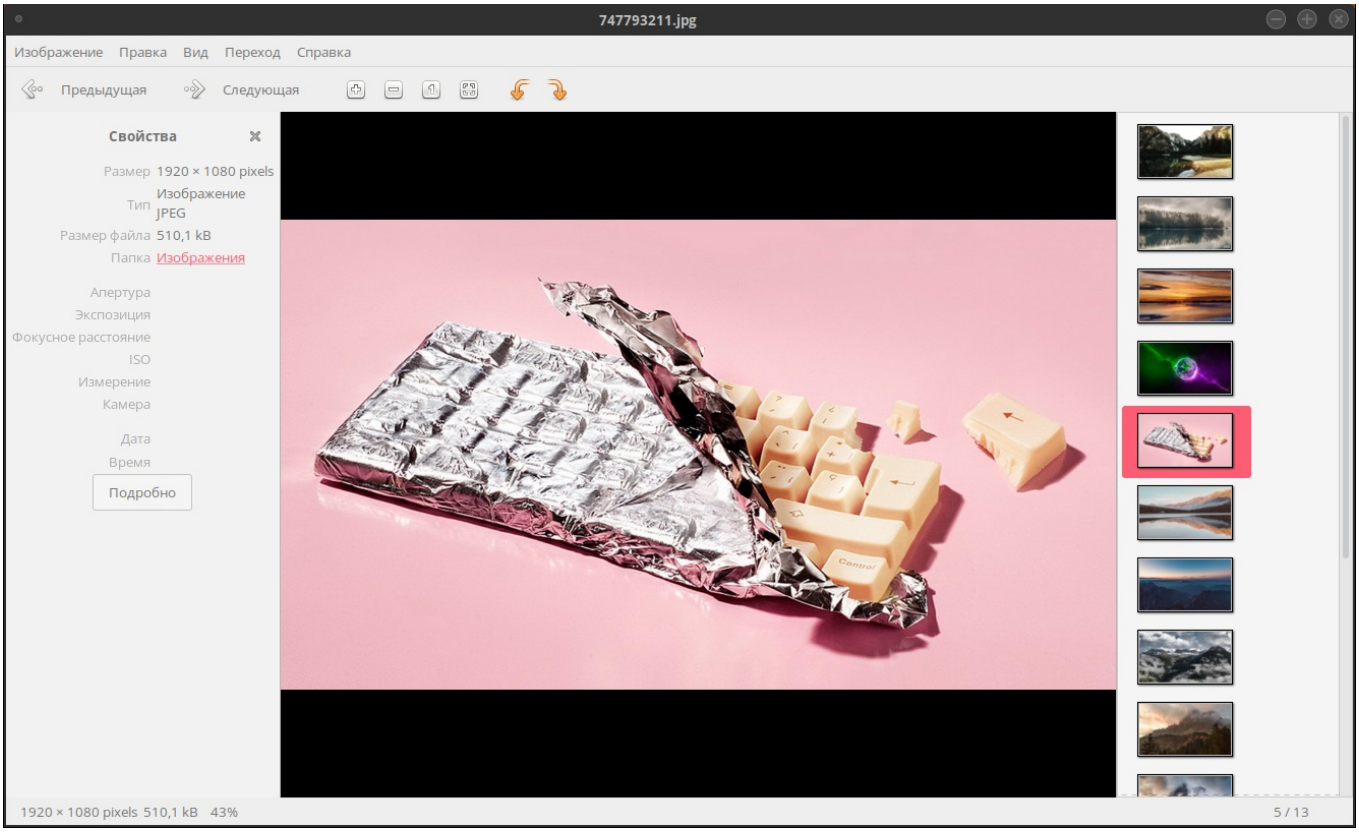
Многие пользователи хранят и просматривают различные изображения, поэтому неотъемлемой частью любой ОС является программа просмотра изображений.

В РЕД ОС по умолчанию установлена программа **Глаз MATE**.



Функционала этой программы достаточно, чтобы просматривать изображения. **Глаз MATE** поддерживает несколько элементарных функций:

- переключение между изображениями в каталоге;
- масштабирование размера изображения под настройки экрана пользователя;
- установка картинки в качестве фонового изображения рабочего стола;
- поворот и отражение изображений и др.



В репозитории РЕД ОС имеются две программы с большим функционалом для просмотра изображений:

- **Pix**;
- **gThumb**.

Программы предназначены для просмотра, редактирования и упорядочивания коллекции графических и видео-файлов, имеют простейшие функции редактирования графики (различные коррекции, в том числе автоматические).

Основные возможности программ:

- просмотр изображений;
- автоматическое обновление содержимого директорий при просмотре;
- копирование, перемещение, удаление изображений или директорий;
- поддержка просмотра основных форматов: BMP, JPEG, GIF, PNG, TIFF, TGA, ICO, XPM;
- просмотр данных EXIF;
- фильтрация изображений;
- сортировка;
- редактирование;
- экспорт в различные форматы;
- просмотр слайд-шоу;
- автоматический поворот изображений на основе метаданных;
- создание фотоальбомов;
- импорт изображений с внешних устройств;
- поиск дубликатов;
- встроенная функция для массового переименования файлов с использованием шаблонов;
- поддержка плагинов и др.

Вы можете подробнее ознакомиться с возможностями **Pix** и **gThumb**, просмотрев наши обучающие видео:

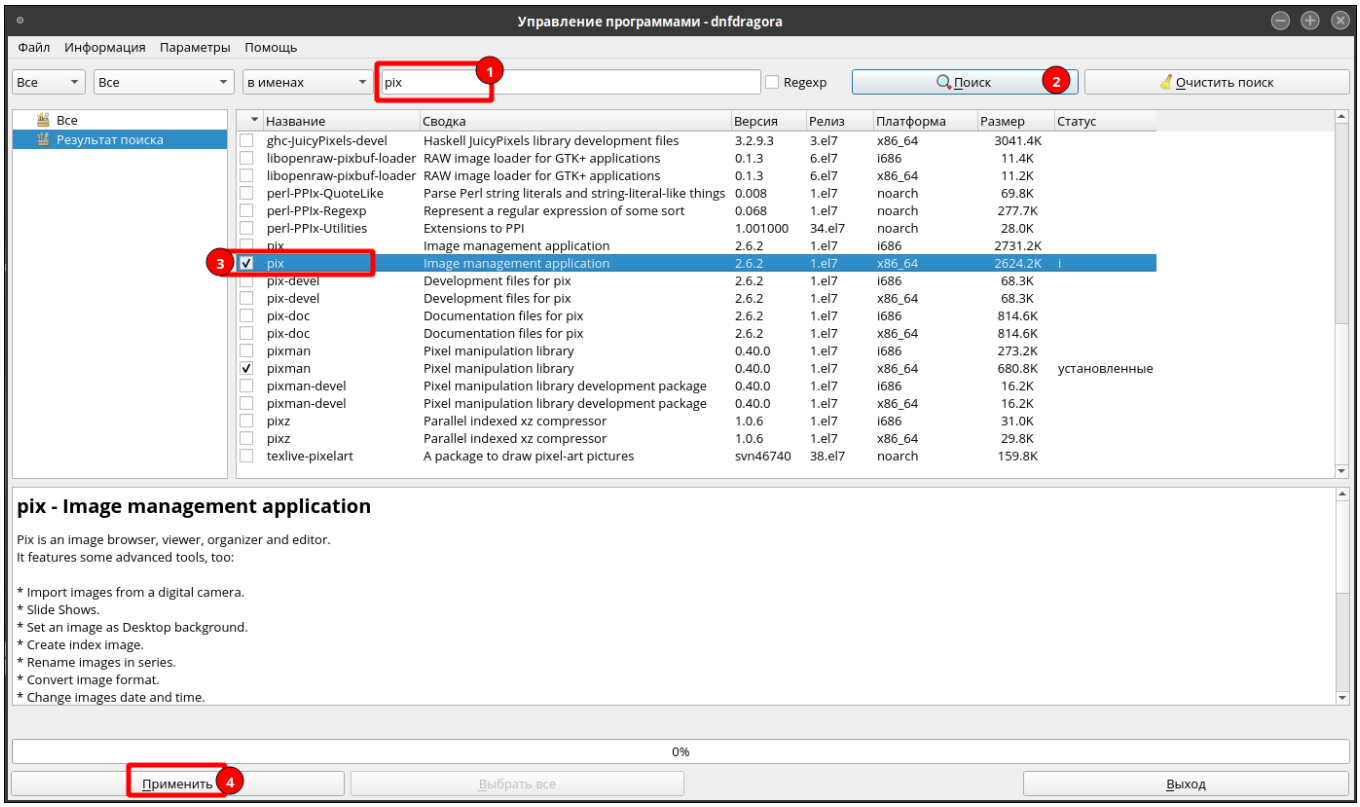
- на **RuTube** — Каталогизаторы фотоальбомов в РЕД ОС;
- в **Яндекс.Дзен** — Каталогизаторы фотоальбомов в РЕД ОС;
- в **VK Видео** — Каталогизаторы фотоальбомов в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Pix

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**pix**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install pix
```

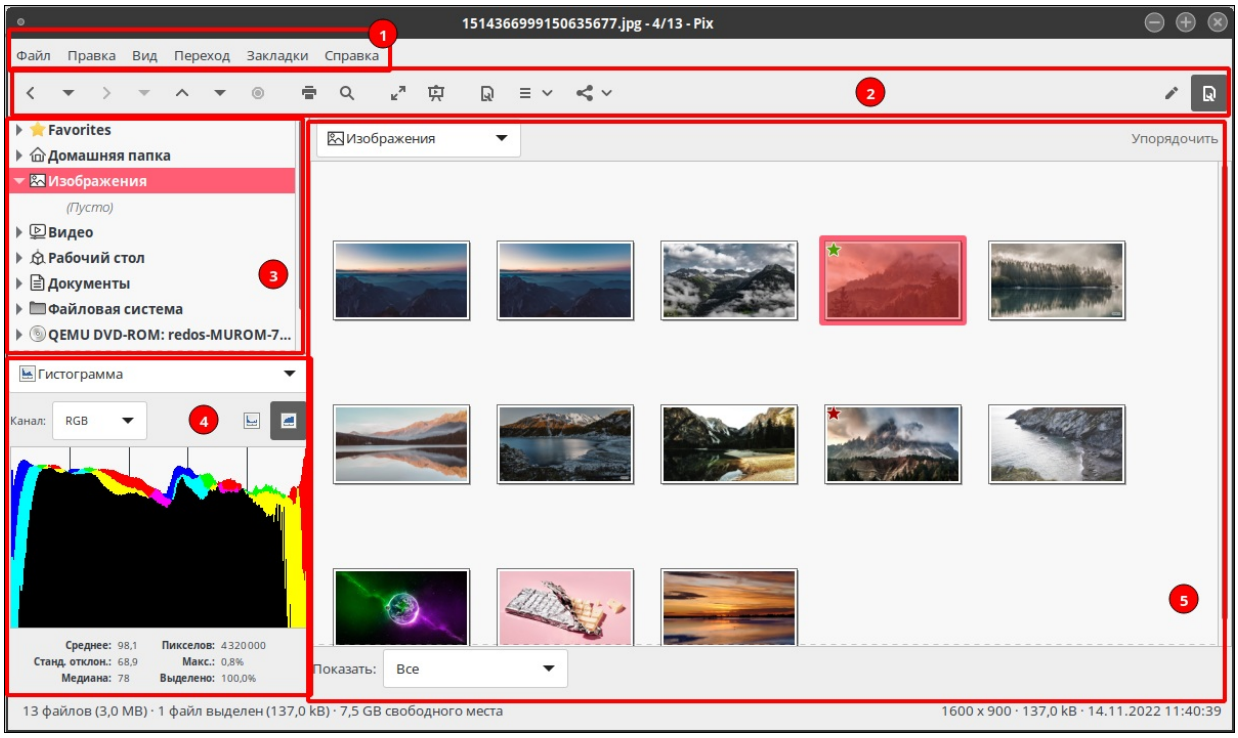
Дальнейшая работа в программе выполняется от ***локального пользователя***.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**Каталогизатор изображений Pix**».

Описание программы

Pix имеет классический интерфейс, в верхней части окна программы находится стандартное основное меню (**1**).

Ниже основного меню находится панель инструментов (**2**). Вид панели инструментов немного отличается в разных режимах программы (режим просмотра и режим навигации). При наведении на иконку появляется всплывающая подсказка о назначении инструмента.

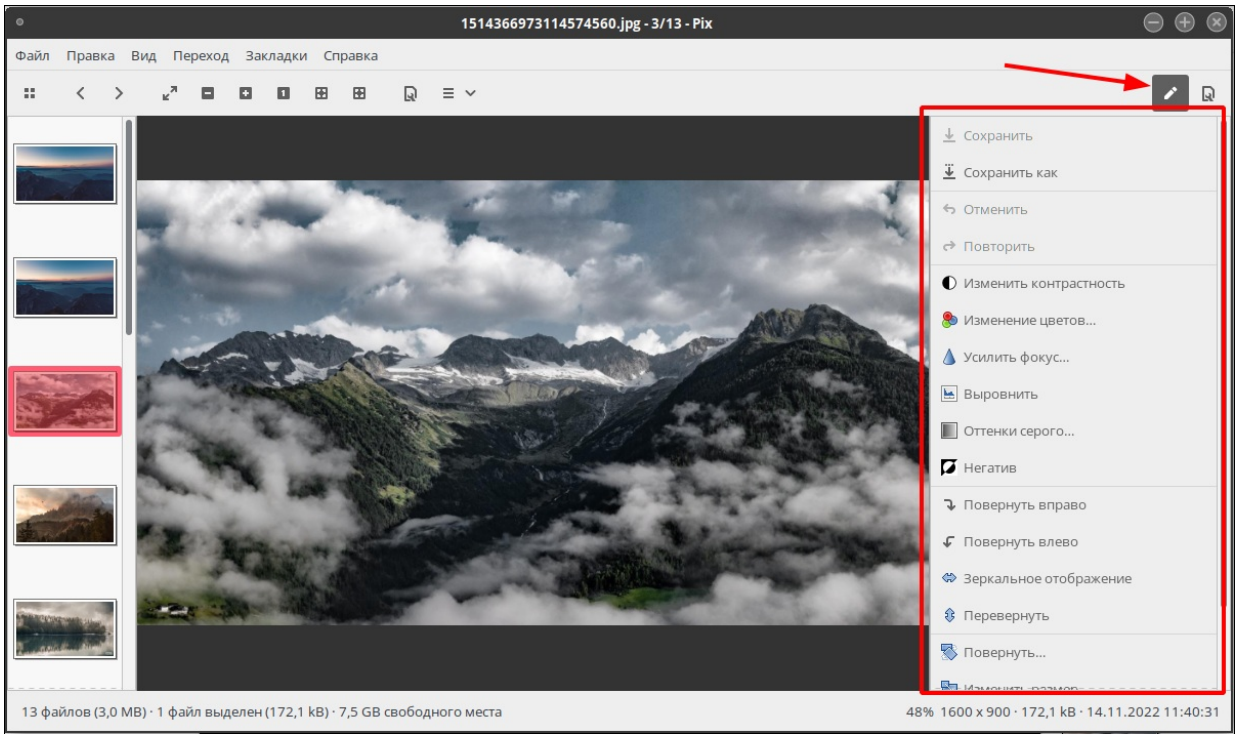


Программа имеет большой функционал, который позволяет осуществлять навигацию по дереву каталогов (**3**) и просматривать файлы изображений.

В поле свойств изображения (**4**) можно просмотреть основную информацию о выбранном изображении или вывести его гистограмму на линейной или логарифмической шкале.

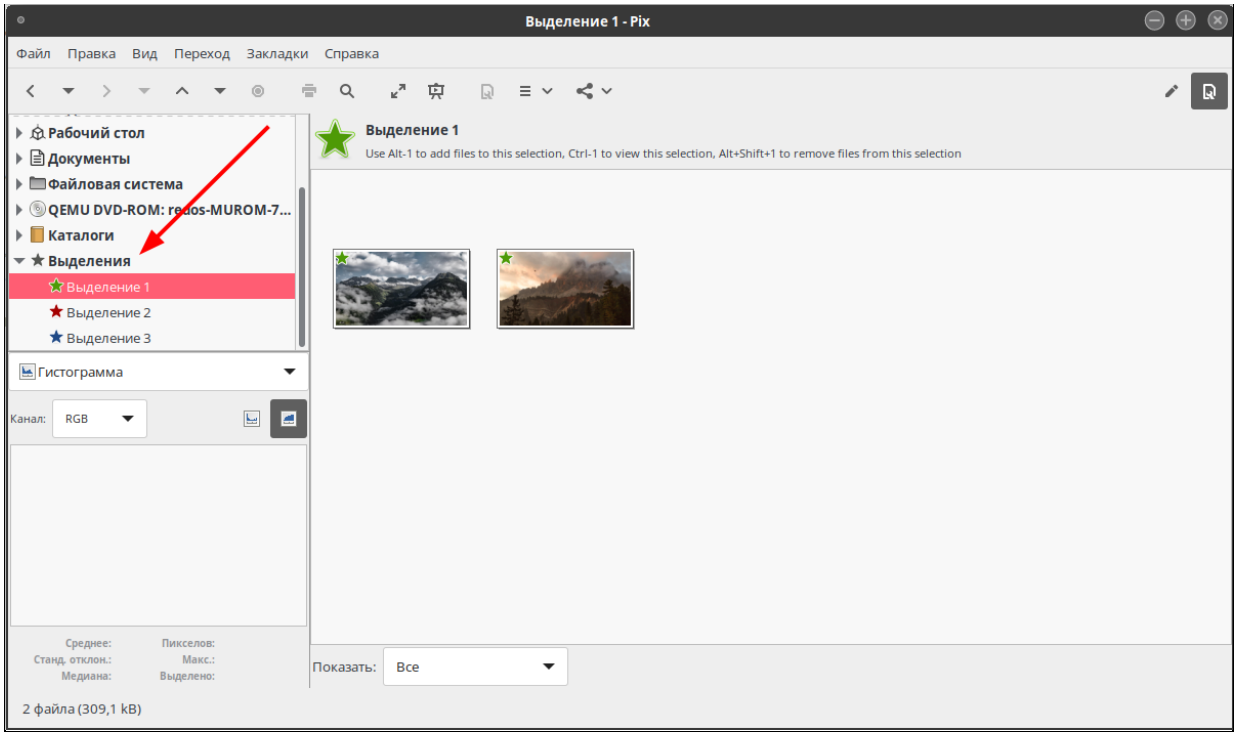
В поле просмотра изображений (**5**) отображается список доступных файлов в выбранном каталоге дерева.

Функции редактирования изображений доступны через иконку с карандашом на панели инструментов.



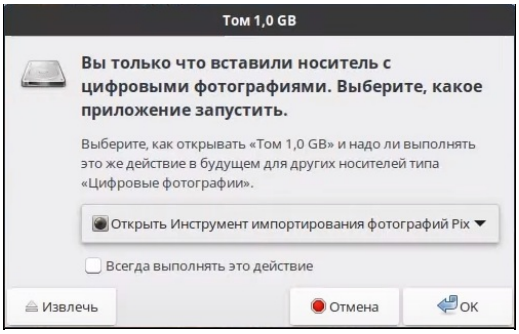
Здесь можно найти много полезных инструментов для простой коррекции фотографии, а именно — яркость и контрастность, поворот влево или вправо, а также зеркальное отображение, произвольный поворот, изменение размера и устранение эффекта красных глаз. После любых изменений программа предлагает сохранить изменения в файле.

Pix обладает базовыми функциями для организации изображений. Нажав правой кнопкой мыши по изображению либо выделив сразу несколько изображений, можно добавить их в одно из трех Выделений — это полезно при отсмотре каталога. Затем в дереве каталогов можно открыть выделения и просмотреть все отмеченные фото.

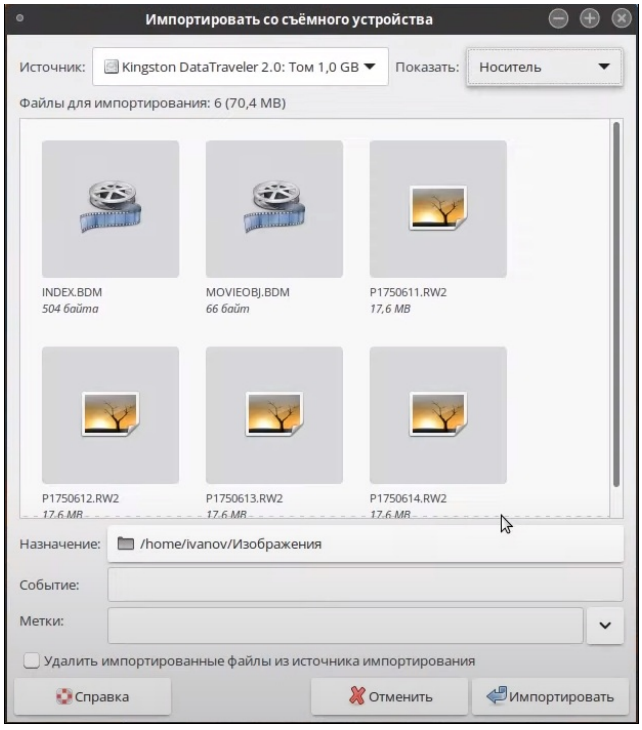


Также есть возможность присвоить метки и добавлять комментарии. Нажав правой клавишей мыши по нужному изображению, можно установить его в качестве фона рабочего стола.

Полезен также инструмент, позволяющий импортировать фотографии прямо из камеры или съемного носителя. Для этого необходимо подсоединить устройство, откроется окно, в котором будет предложено открыть **Инструмент импортирования фотографий Pix**. При этом не обязательно, чтобы *Pix* был открыт заранее.

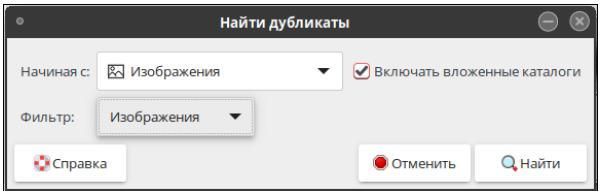


Нажмите «**OK**», откроется меню импорта, в котором можно выбрать необходимые файлы и указать папку назначения.

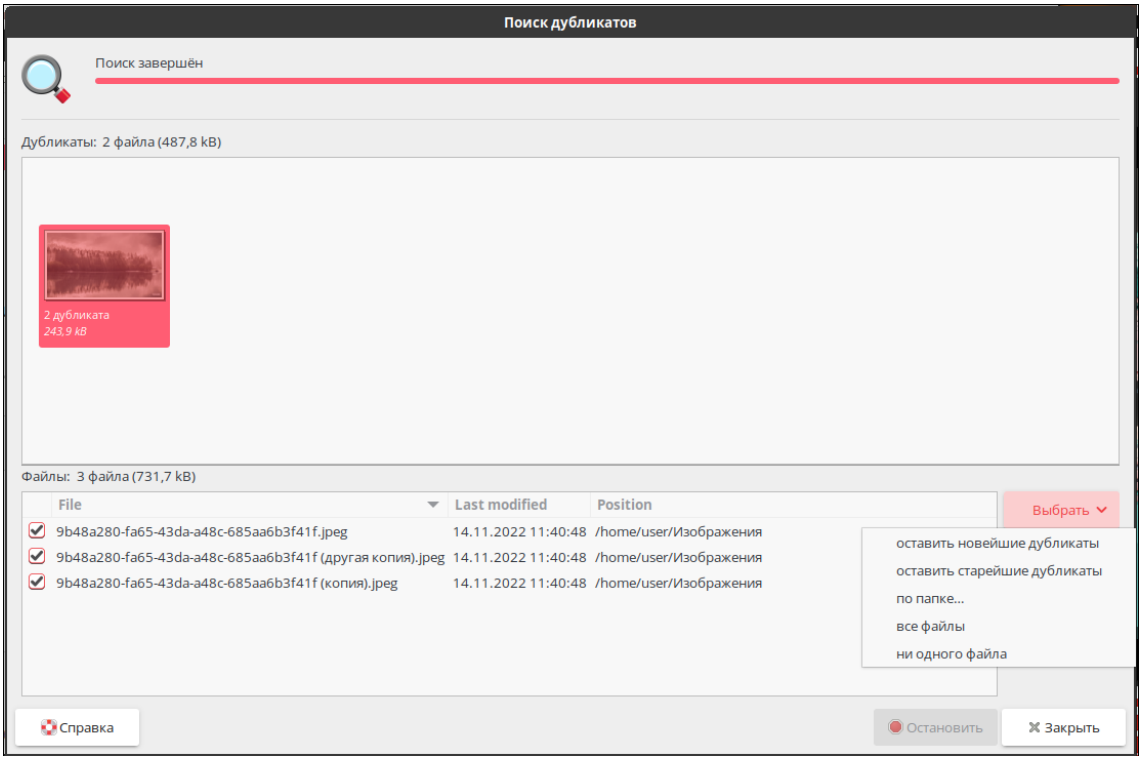


Бывают ситуации, когда при копировании или перемещении фотографий появляются одинаковые фото (дубли), которые занимают полезное место на диске. *Pix* может помочь в решении данной проблемы.

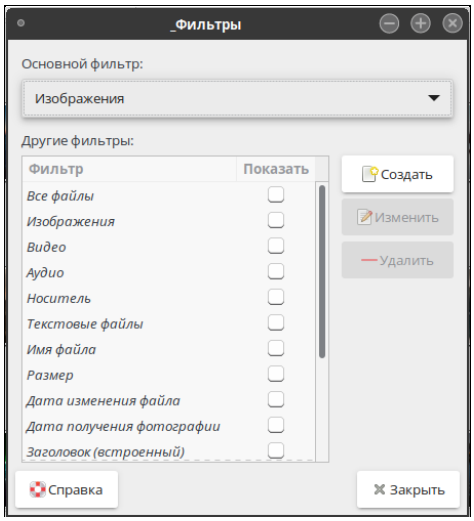
В основном меню откройте раздел «**Правка**» - «**Найти дубликаты...**», выберите нужный каталог и нажмите «**Найти**». Начнется поиск дубликатов.

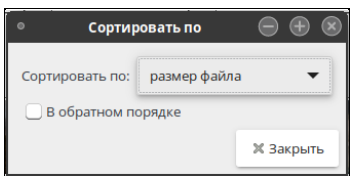


Нажав на любую фотографию, можно узнать, где находится копия. Также доступен выбор необходимых действий, которые нужно сделать с дубликатами, после чего можно удалять копии.



Также могут оказаться полезны функции фильтров и сортировки. Для настройки перейдите в пункт меню «**Вид**» - «**Сортировать по...**» или «**Вид**» - «**Фильтр...**» и установите необходимые значения.



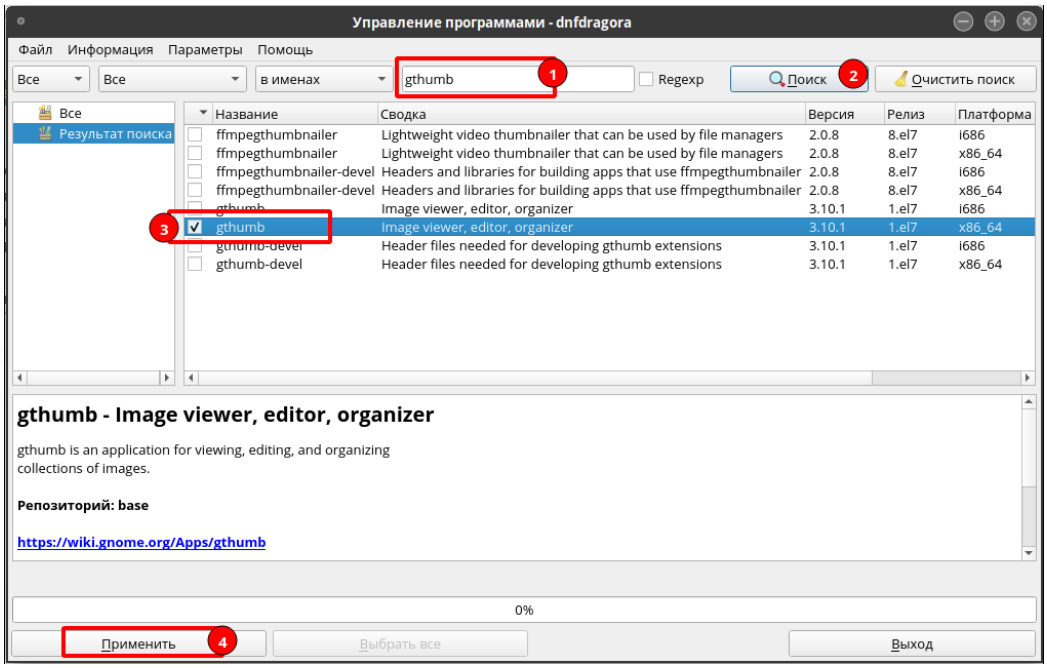


gThumb

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**»

— «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**gthumb**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

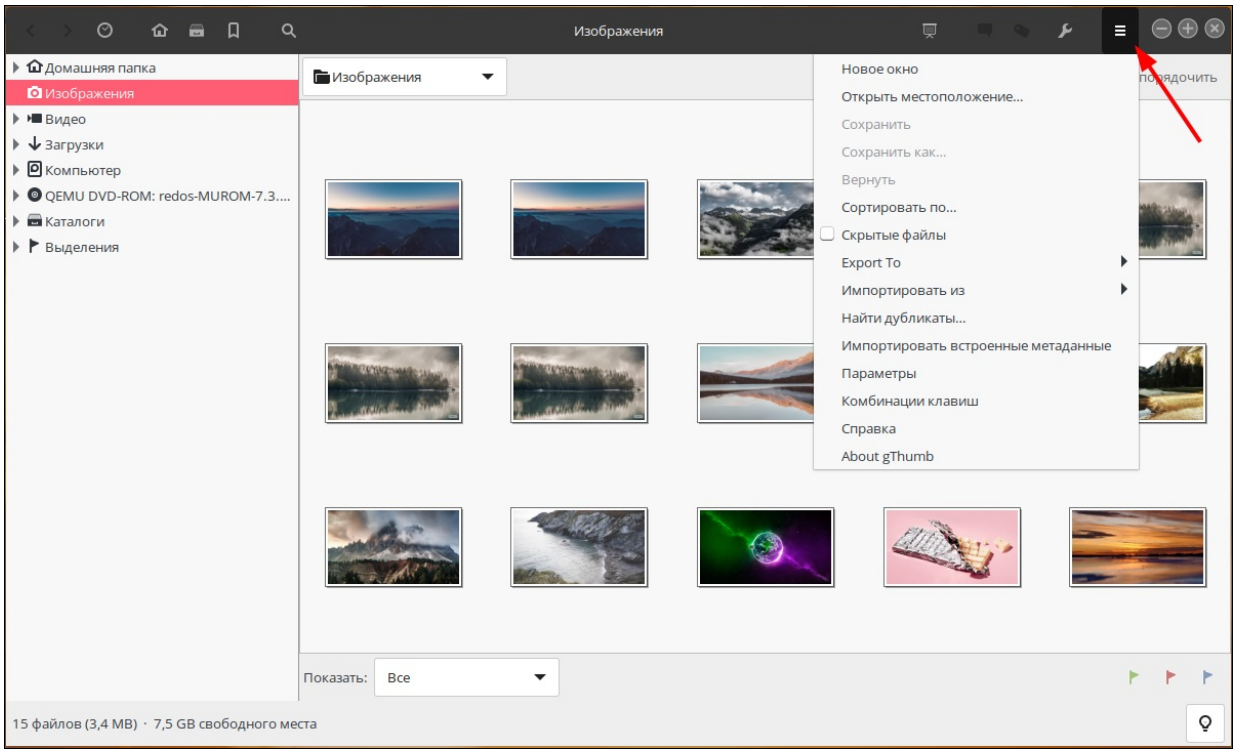
```
dnf install gthumb
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**Каталогизатор изображений gThumb**».

Описание программы

Функционал программы *gThumb* похож на *Pix*, основные отличия заключаются в более современном интерфейсе. Стандартного меню нет, оно доступно через кнопку в правой части заголовка окна.

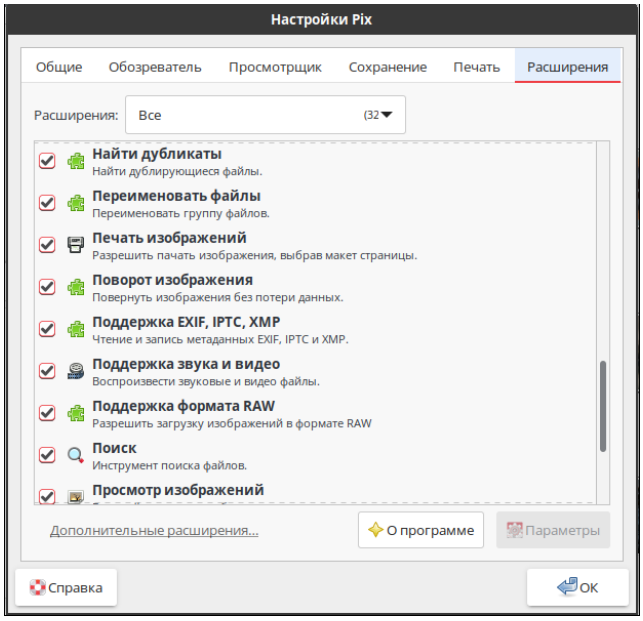


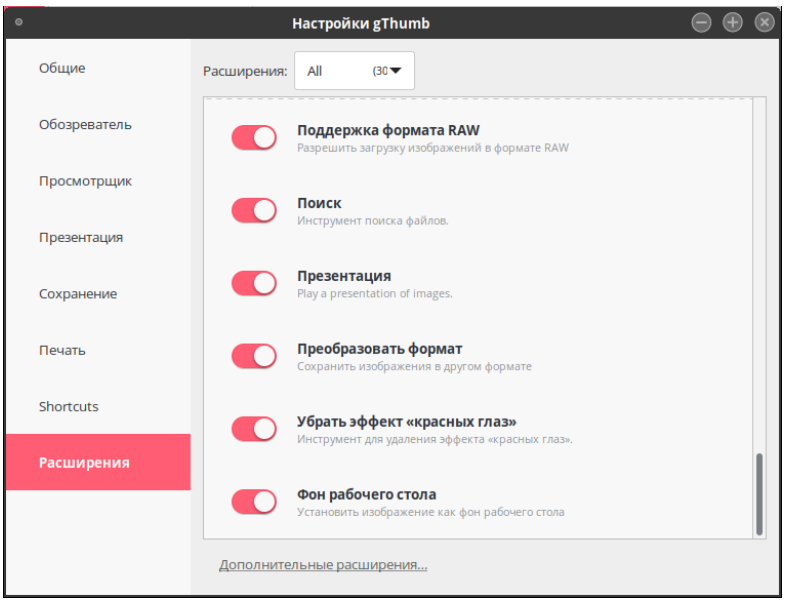
gThumb имеет большой функционал, позволяющий не только просматривать файлы изображений и осуществлять навигацию по дереву каталогов, но и редактировать файлы. Большим преимуществом перед *Pix* является открытие RAW-файлов — для фотографов это очень полезная функция.

Еще одной полезной функцией может оказаться массовое переименование файлов. Для этого выделите все нужные фотографии и нажмите по ним ПКМ, в контекстном меню выберите «**Переименовать**». Откроется окно, в котором можно задать шаблон, указать начало нумерации, сортировку и увидеть список файлов с новыми наименованиями в таблице предварительного просмотра.

Также доступны перечисленные ранее функции из *Pix*, такие как поиск дубликатов, редактирование изображений, инструменты для организации изображений в каталогах, импорт с фотокамеры или съемного носителя и т. д.

Функционал данных программ может быть легко дополнен за счёт использования различных расширений. Расширения можно подключать в настройках программ.





Darktable — программа каталогизации и обработки цифровых фотографий в формате RAW

Установка

Описание программы

Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: darktable-3.6.1

Darktable — это программа для каталогизации и обработки цифровых фотографий в формате **RAW**. Она предоставляет пользователям различные инструменты для редактирования изображений и управления фотоколлекцией.

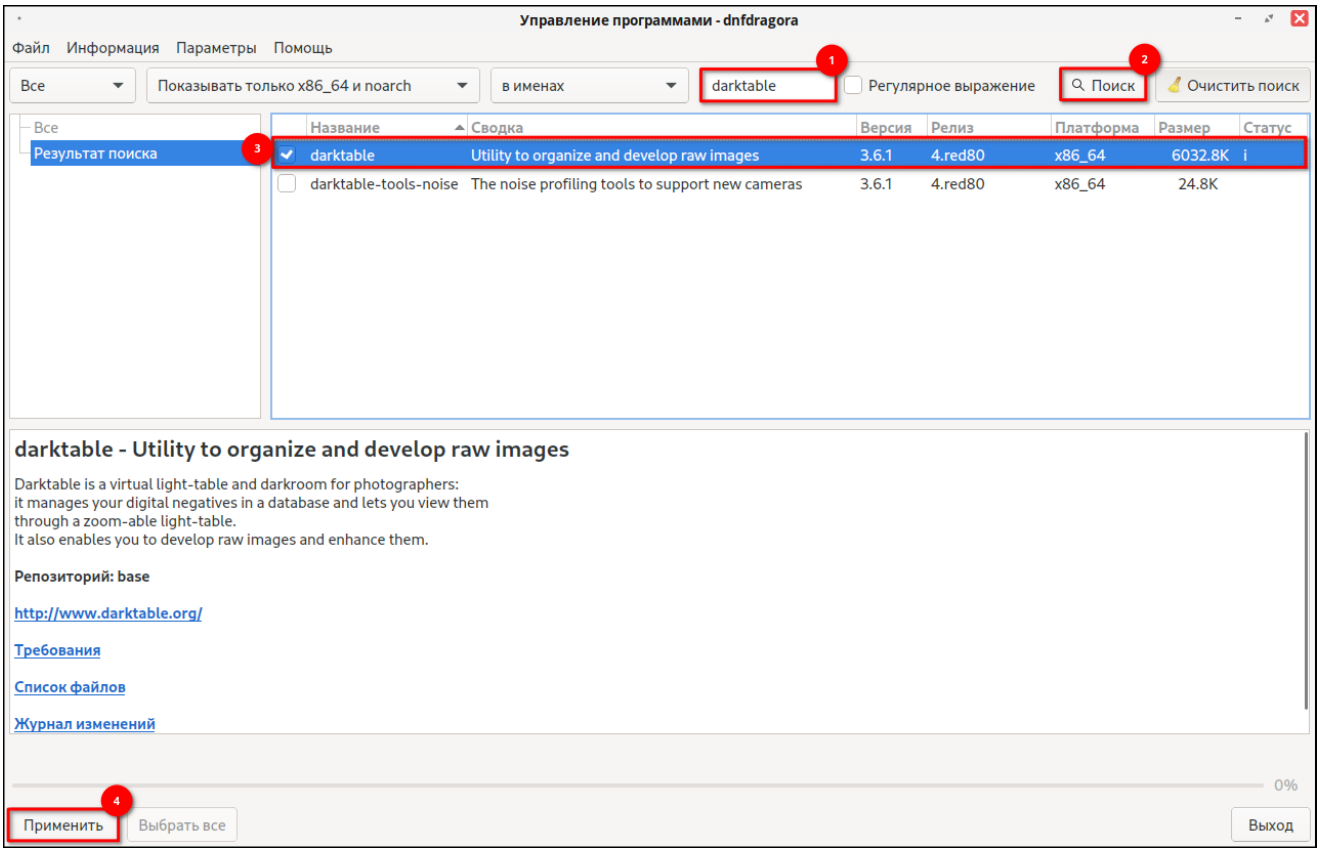
Основные возможности **Darktable**:

- поддерживает широкий спектр форматов RAW от различных камер;
- работает с форматами JPEG, TIFF, PNG, OpenEXR и другими;
- все изменения сохраняет отдельно от оригинального файла, позволяя вернуться к исходному изображению;
- обрабатывает изображения с глубиной цвета 32 бита на канал в цветовом пространстве CIE LAB;
- поддерживает использование масок и слоев для точного редактирования отдельных участков изображения;
- позволяет ускорить обработку изображений благодаря поддержке OpenCL;
- полностью поддерживает работу с цветовыми профилями и пространства, такими как sRGB, Adobe RGB, XYZ и линейный RGB;
- более 60 модулей для разных задач: трансформация, цветокоррекция, улучшение качества и художественные эффекты;
- поддерживает параметрические и нарисованные маски, а также работу с графическими планшетами;
- компенсирует дисторсию и хроматические аберрации объектива;
- каталогизирует изображения, добавляет метки и позволяет искать фотографии по разным параметрам;
- поддерживает прямую съемку через подключенный фотоаппарат;
- экспортирует изображения в разные форматы, включая JPEG, PNG, TIFF, WebP, PPM, TIFF, PFM, OpenEXR;
- может экспортировать изображения на онлайн-сервисы;
- поддерживает цветовые профили ICC и OpenCL для аппаратного ускорения.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**darktable**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните следующую команду (потребуются права **администратора**):

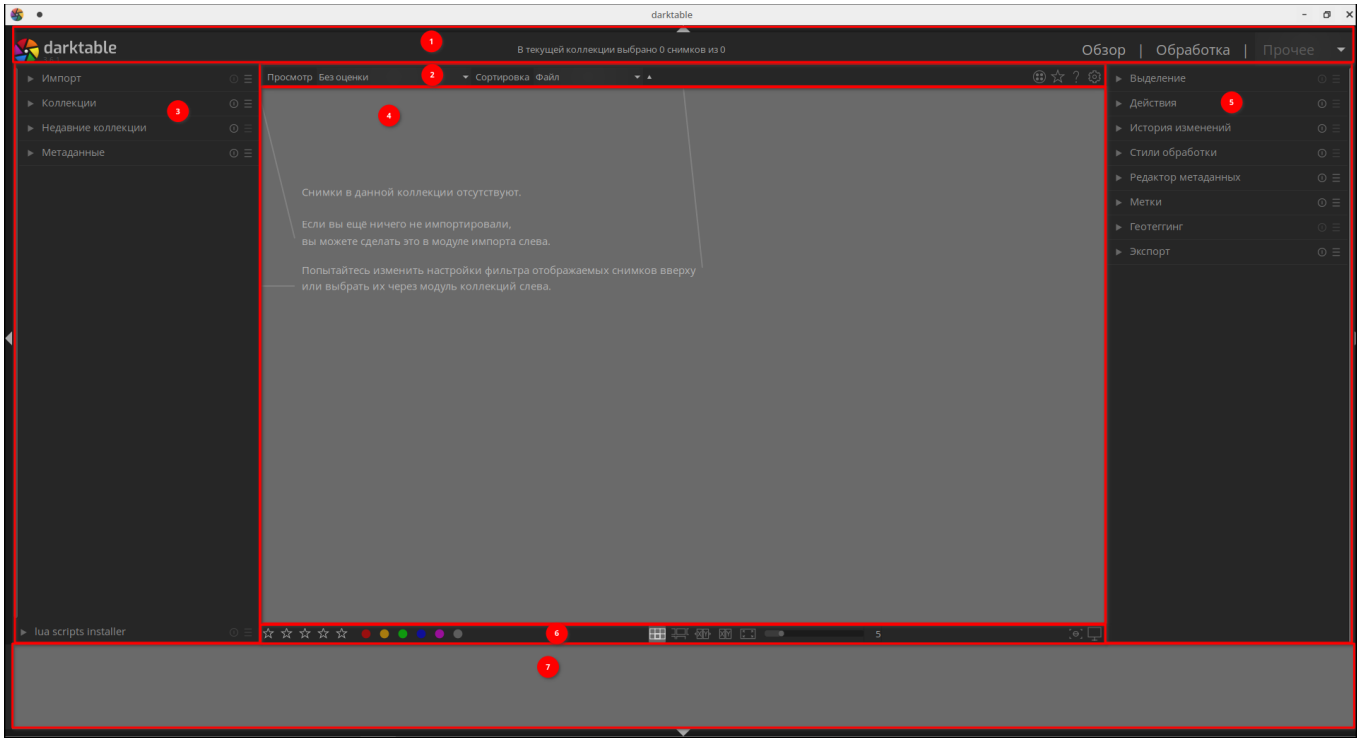
```
sudo dnf install darktable
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

После установки программа будет доступна из «**Главного меню**» — «**Графика**» — «**Darktable**».

Описание программы

Главное окно программы **Darktable** выглядит следующим образом.



Интерфейс программы разделен на несколько ключевых частей:

1. **Панель режимов** позволяет переключаться между режимами работы. В зависимости от режима работы содержание всех панелей будет меняться.

2. **Верхняя панель** предоставляет быстрый доступ к основным настройкам и функциям программы, включая глобальные параметры и режимы работы.

3. **Левая панель** предназначена для предоставления дополнительной информации, а также для навигации по различным элементам интерфейса.

4 . **Центральная часть** отображается основная рабочая область, где могут быть представлены такие элементы, как текущее изображение, группа изображений, карта и другие объекты, с которыми ведется работа.

5 . **Правая панель** содержит набор инструментов для редактирования и обработки изображений, позволяя пользователям вносить необходимые изменения.

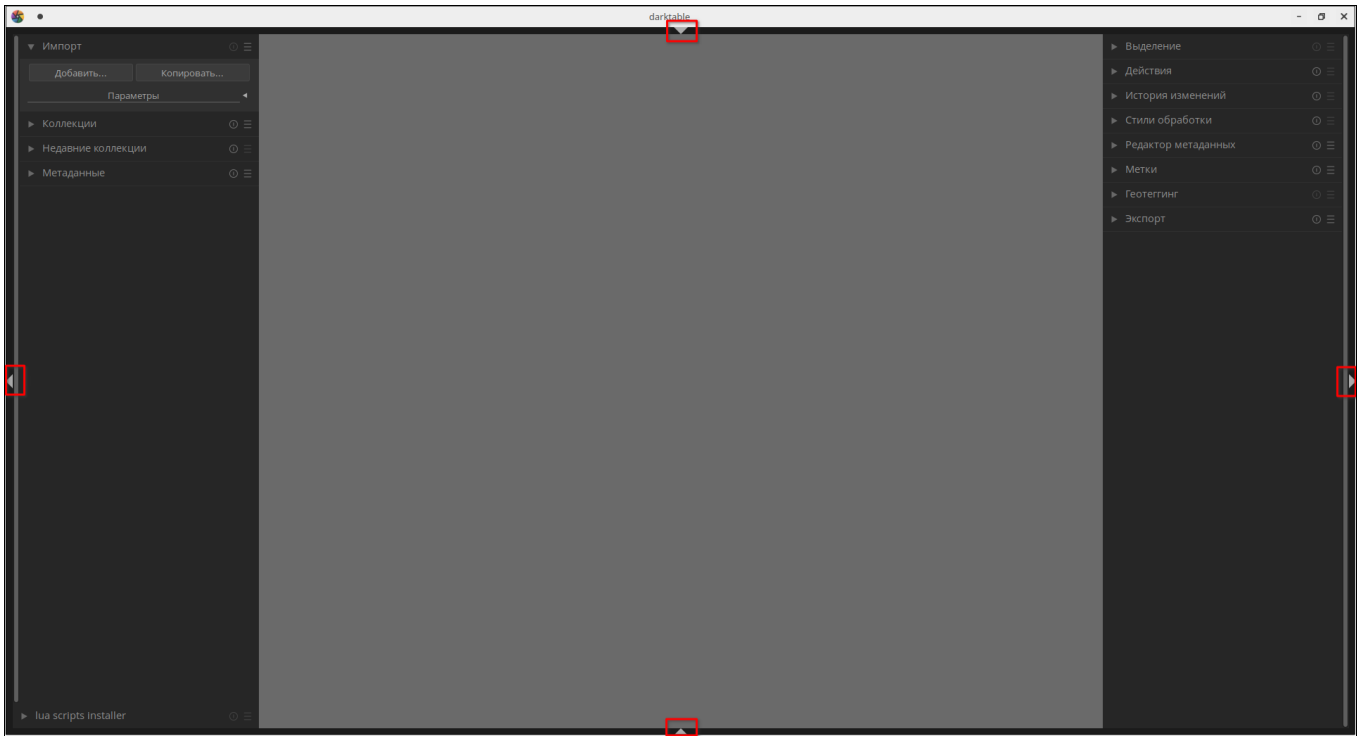
6. **Нижняя панель** предоставляет дополнительные настройки и функции, которые могут понадобиться для более детальной работы с изображениями или проектами.

7 . **Лента фотографий** располагается в нижней части окна программы, отображает такие же изображения, что расположены в центральной части программы, позволяет взаимодействовать с изображениями вне режимов Обзор и Слайдшоу. Для включения/выключения используется сочетание клавиш **Ctrl+F**. Можно перемещаться по ленте фотографий, прокручивая ее колесиком мыши.

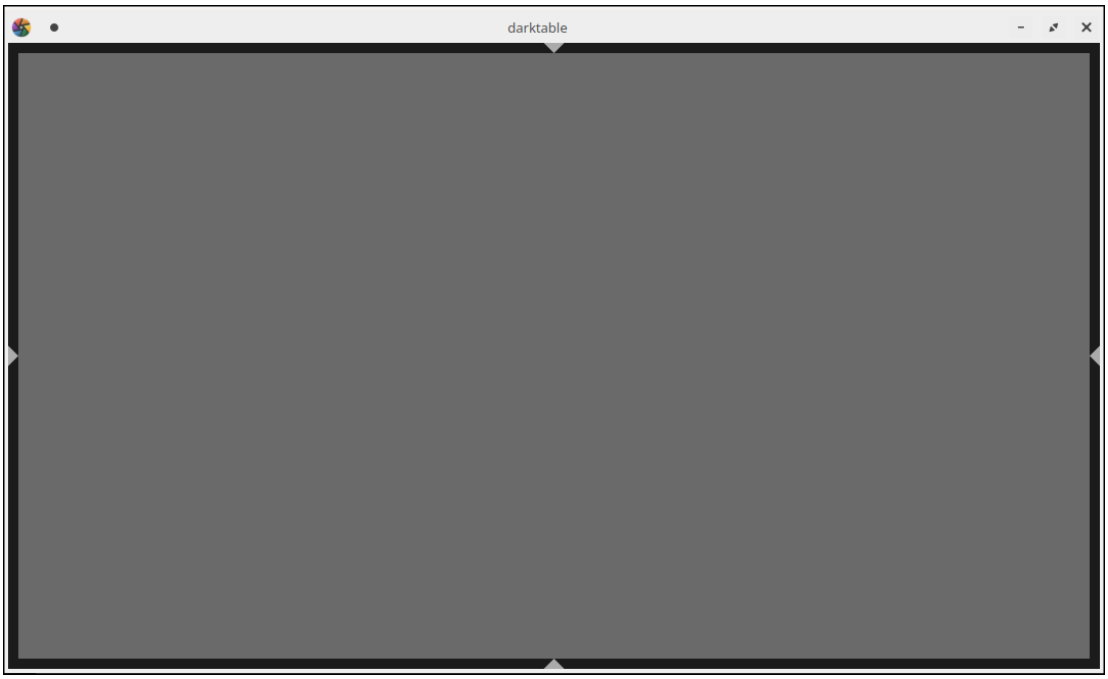
Расширение пространства рабочей области

Для расширения пространства рабочей области доступно несколько вариантов.

1. Каждая панель может быть скрыта или возвращена нажатием на кнопку в виде треугольника  , расположенную рядом с панелью.



2. При нажатии клавиши **TAB** все панели сворачиваются, а центральная область занимает все освободившееся пространство. Повторное нажатие **TAB** возвращает к предыдущему виду.



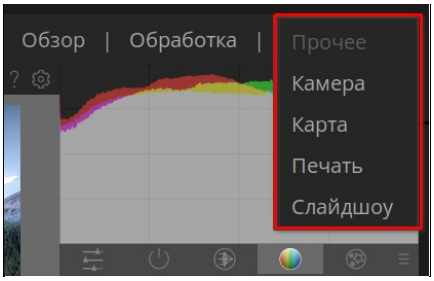
3. Для перехода/возврата просмотра окна программы на полный экран необходимо нажать клавишу **F11**.

Режим работы

В **Darktable** реализовано шесть режимов работы.

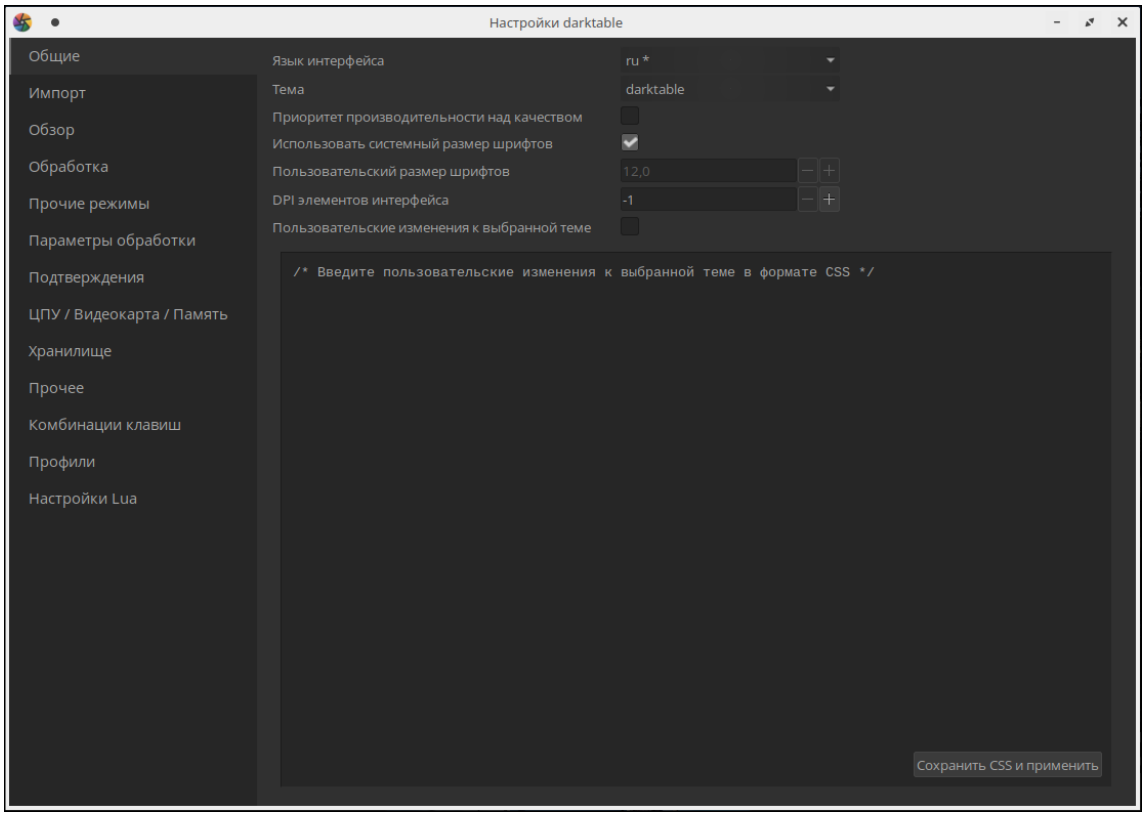
Переключаться между ними можно, щелкая курсором мыши по названию режима в панели, расположенной справа сверху окна программы, активный режим подсвечивается, или с помощью горячих клавиш:

- **L** (**lightable**) — в режиме Обзор осуществляется управление снимками и фотоархивом, осуществляется оценка изображений, добавляются ключевые слова (теги), присваиваются цветовые метки и экспортируются изображения;
- **D** (**darkroom**) — в режиме Обработка происходит редактирование снимка с использованием доступных модулей;
- **T** (**camera tethering**) — режим Камера предназначен для съёмки камерой, подключенной к компьютеру, обеспечивает захват изображений для передачи и просмотра на компьютере;
- **M** (**map**) — в режиме Карта отображаются снимки с географическими координатами (геотеги) и предоставляется возможность вручную привязать изображение к карте;
- **P** (**print**) — режим Печать предназначен для отправки изображений на печать;
- **S** (**slideshow**) — в режиме Слайдшоу осуществляется показ изображений в виде слайд-шоу, процесс конвертации снимков производится на лету.



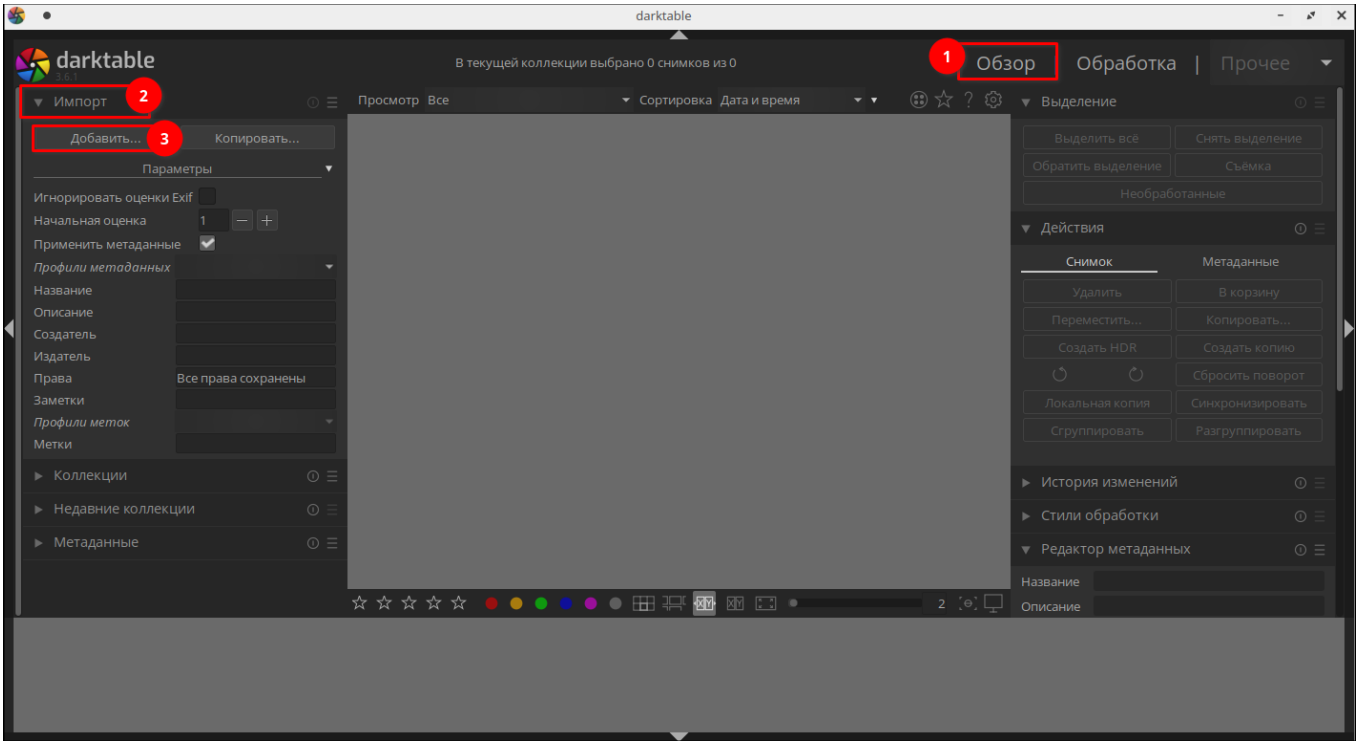
Общие настройки

При нажатии кнопки  на верхней панели окна программы откроется доступ к различным настройкам, позволяющим настроить поведение программы **Darktable**.



Импорт изображений

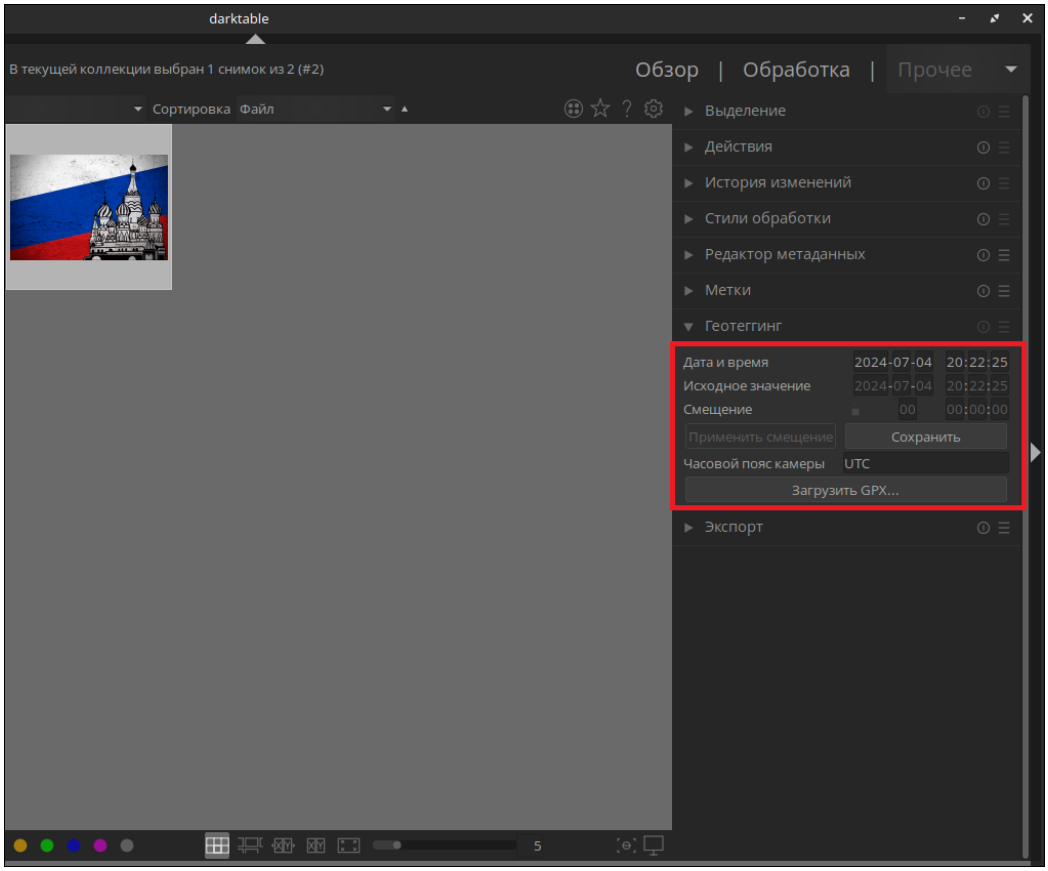
После запуска программы первый раз ее центральная часть не содержит данных. Для добавления данных в программу необходимо импортировать изображение. Можно импортировать либо одно изображение, либо папку.



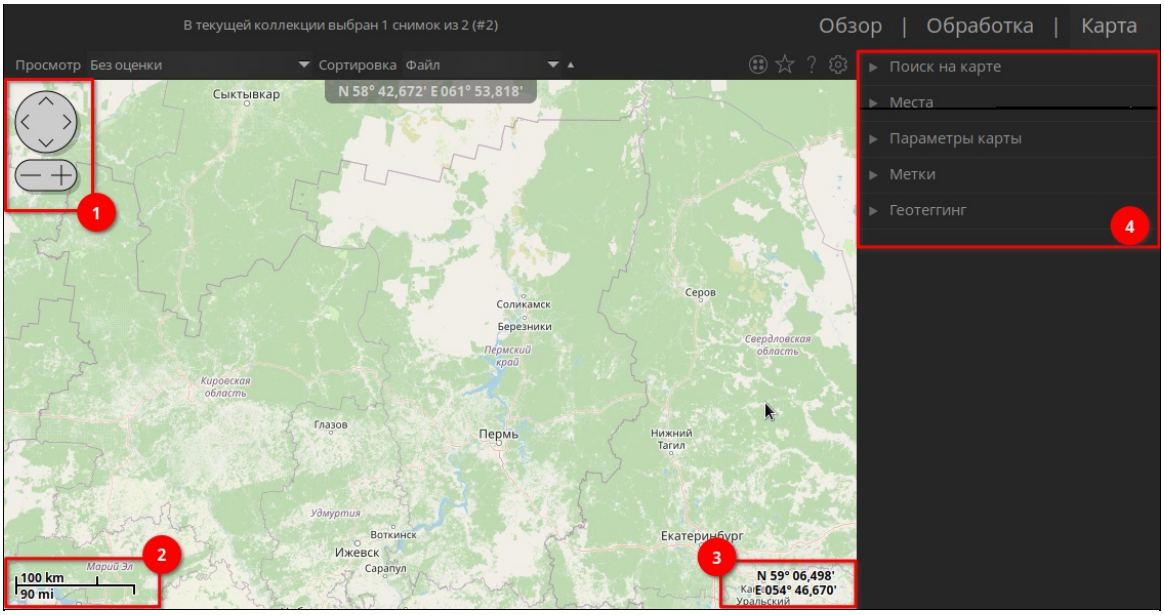
Добавление геотегов к фотографиям

Для точного определения местоположения сделанных фотографий рекомендуется использовать функцию **геотеггинга**. Эта возможность позволяет добавлять к изображениям данные о географических координатах, что полезно при обработке большого количества снимков, сделанных в разных местах.

Если изображение имеет отметку времени по **UTC** (**Coordinated Universal Time** — всемирное координированное время), можно применить GPX-трек без дополнительных настроек. Для применения геотегов нужно перейти в режим Обзор в раздел «**Геотеггинг**» и добавить GPX-трек к снимку.



Кроме этого, можно вручную определить географические координаты изображения в режиме Карта. Режим Карта отображает карту мира с открытыми изображениями, привязанными к их географическому положению. Данные карты берутся из открытых источников в Интернете. Навигацию можно осуществлять по карте. Удерживая ЛКМ, можно перемещаться по карте, а колесиком прокрутки регулировать её масштаб.

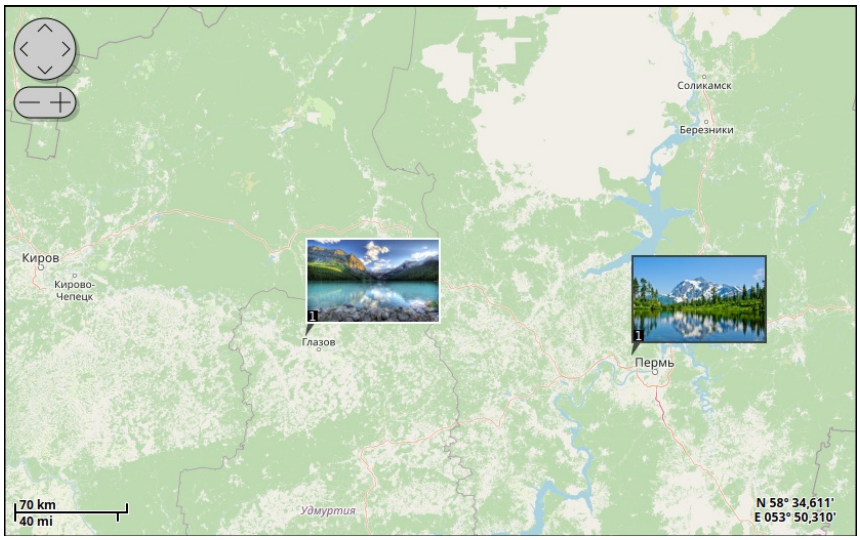


На карте представлены элементы управления и информационная панель для ориентации. Навигационные инструменты расположены в верхнем левом углу карты и служат альтернативой управлению с помощью мыши (1).

Шкала расстояний находится внизу слева (2).

В правом нижнем углу отображаются географические координаты центральной точки карты (3).

Рядом с картой находятся дополнительные панели, предоставляющие расширенные настройки и управление картой (4). Изображения, для которых определены географические координаты, отмечаются на карте небольшими значками.

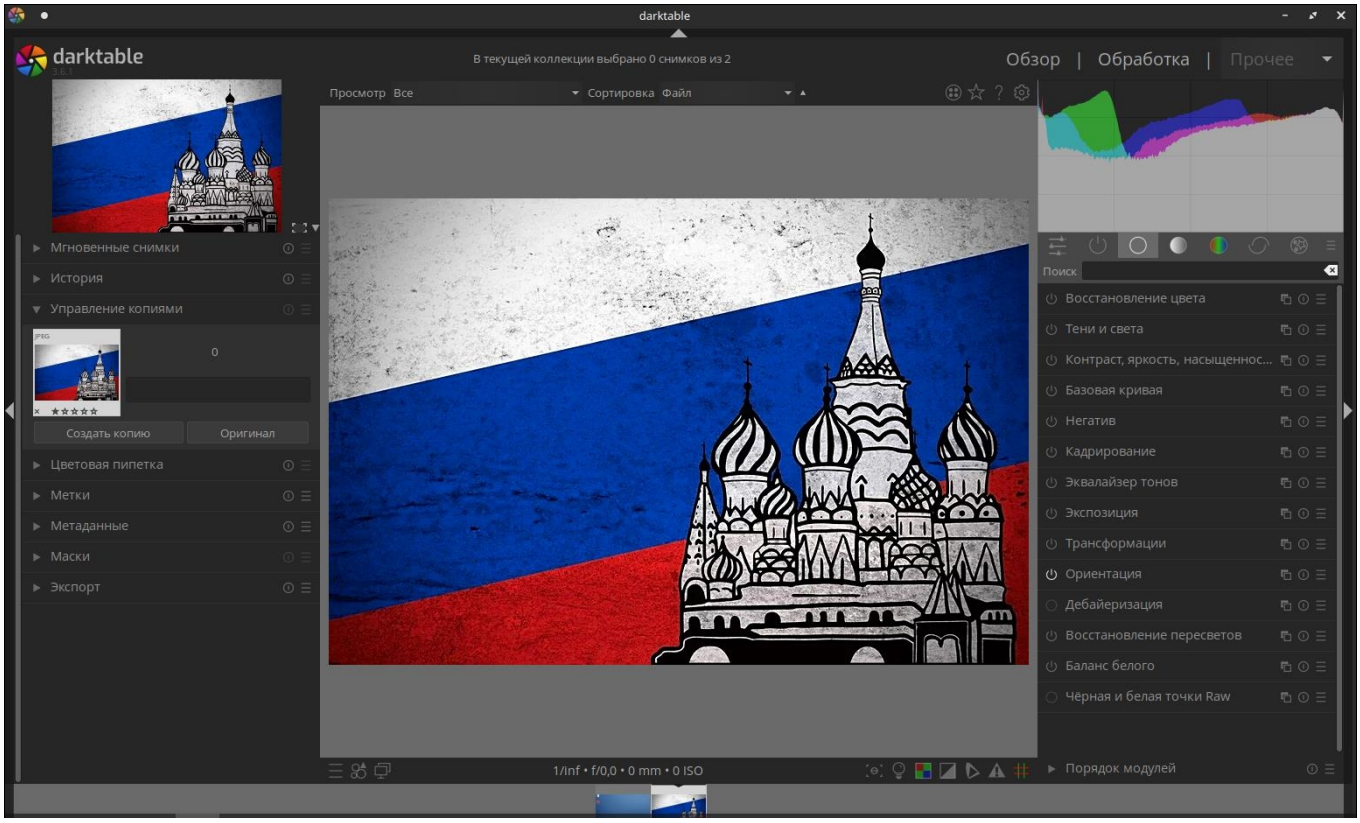


Для назначения географических координат изображению откройте ленту фотографий на нижней панели. Чтобы задать изображению местоположение, просто перетащите соответствующую фотографию с ленты фотографий на нужную точку на карте. **Darktable** автоматически сохранит новые координаты (широту и долготу) в метаданные изображения. Эти данные будут включены в экспортированное изображение.

Чтобы убрать географическую привязку у изображения, достаточно перетащить его обратно на ленту фотографий.

Обработка/редактирование снимков

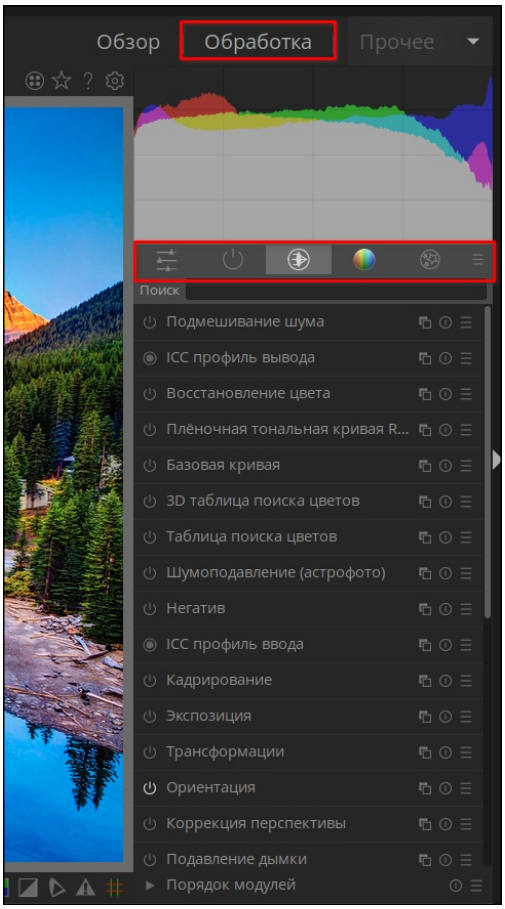
Обработка — режим, предназначенный для редактирования изображений. Здесь можно внести необходимые корректировки.



На панели справа можно выбрать настройки коррекции для улучшения изображений: повышение резкости размытых снимков, коррекцию баланса белого цвета и обрезку элементов, которые могли случайно попасть в кадр.

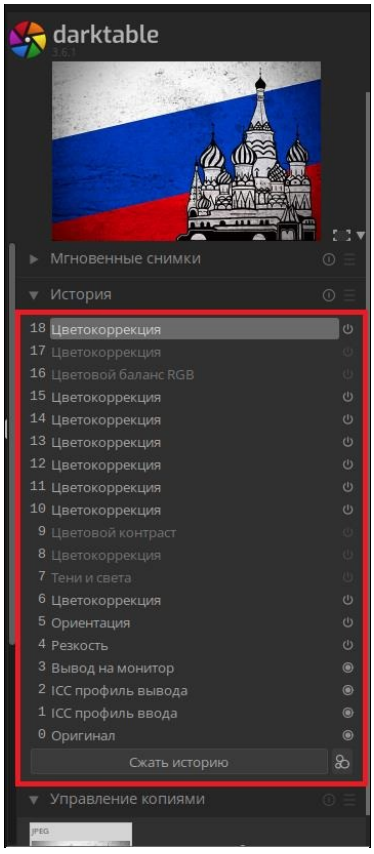
С помощью регулировок контрастности объект можно сделать ярче. Бегунки панели позволят экспериментировать с цветами, настраивать освещение. Здесь доступны такие эффекты, как размытие движения и виньетирование.

Darktable группирует все эти задачи в модули. Некоторые из них видны при настройках по умолчанию и организованы в разделы: «**Базовые модули**», «**Тон**», «**Цветокоррекция**», «**Коррекция**» и «**Эффекты**».



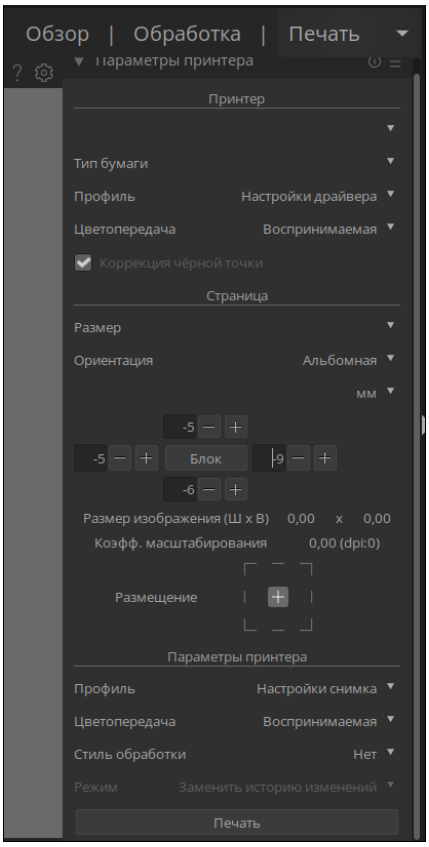
Отслеживание изменений

В левой части окна можно увидеть список изменений, внесенных в текущее изображение. В разделе «**История**» **Darktable** уже автоматически применил к фотографии несколько стандартных настроек. Но можно и отменить их, вернувшись к оригиналу. Также во время работы есть возможность создавать собственные промежуточные копии картинки, снапшоты.



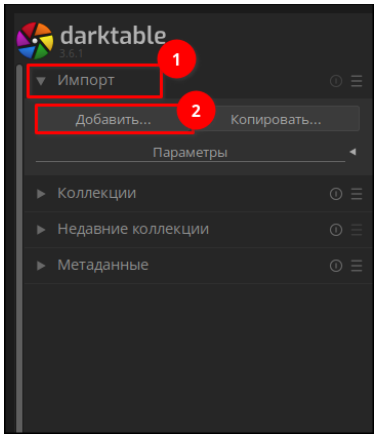
Использование функций печати

Эта функция дает возможность печатать изображение. Выберите принтер, установите размер бумаги, настройте цветовой профиль и прочие параметры. **Darktable** обеспечивает предварительный просмотр картинки, что позволяет увидеть ее расположение на листе бумаги.

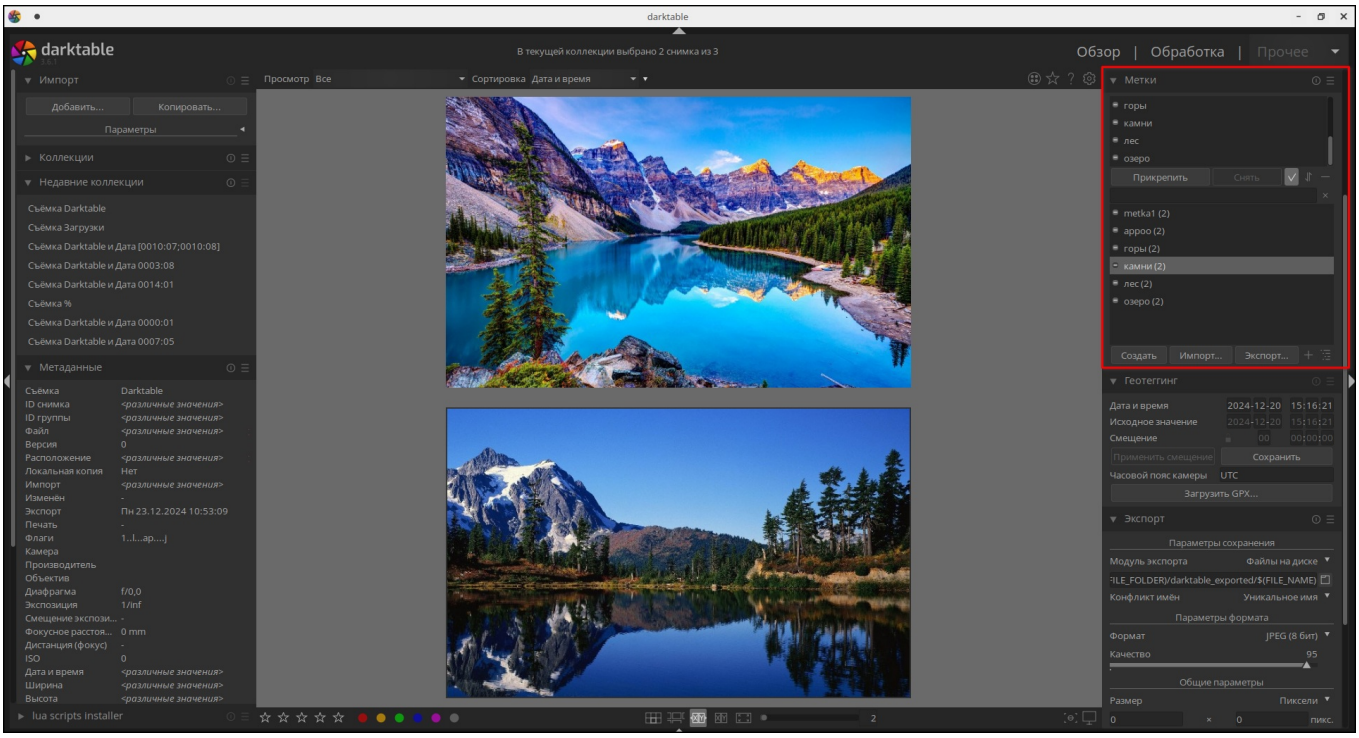


Пример работы

1. **Импорт**. Для импорта фотографии перейдите в режим Обзор — «**Импорт**» (1). Нажмите кнопку «**Добавить**» (2). Откроется меню импорта, в котором можно выбрать необходимые файлы и указать папку назначения.



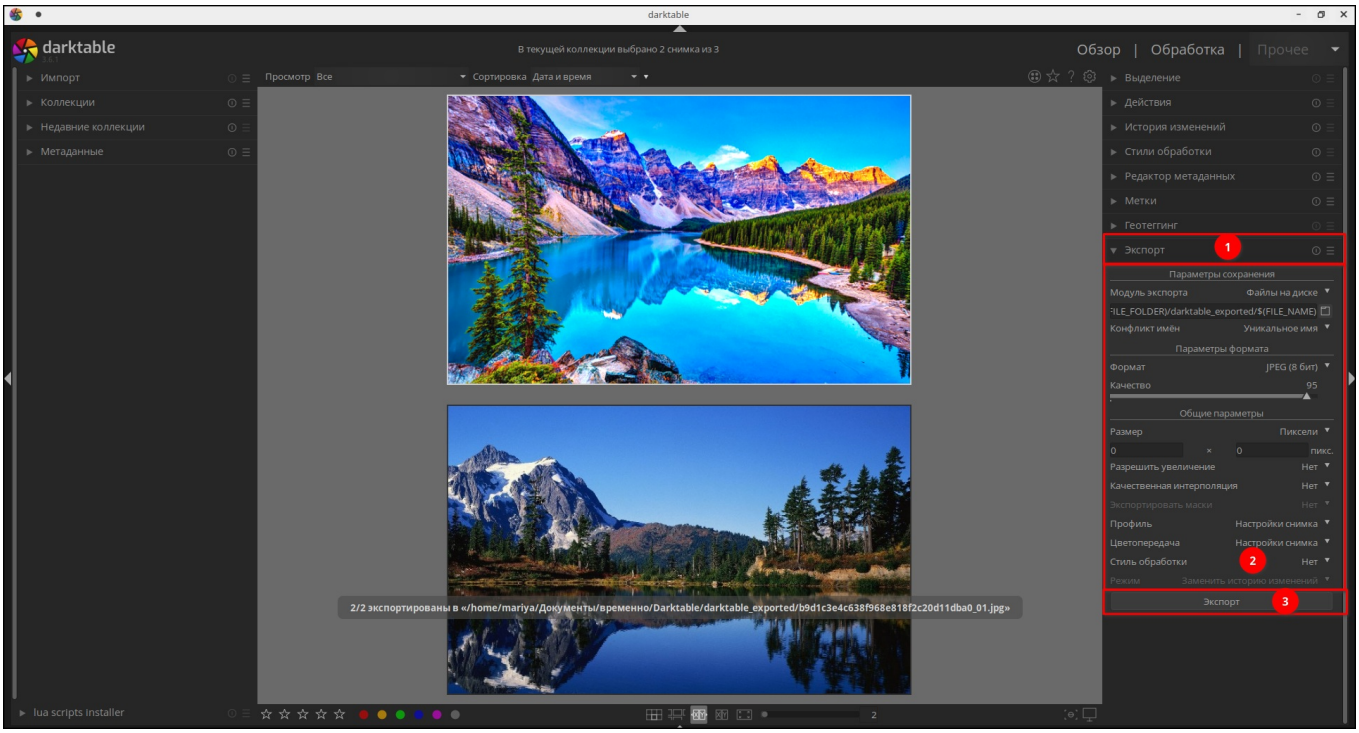
2. **Категоризация и отбор**. Просмотрите изображения, отметьте удачные/неудачные кадры, поставьте метки, рейтинги, ключевые слова. По рейтингам, меткам, ключевым словам в дальнейшем можно отбирать, искать и сортировать изображения. Данный шаг не является обязательным, но чем больше изображений импортировано, тем сложнее в них ориентироваться.



3. **Обработка**. Перейдите в режим Обработка. На этом шаге происходит конвертирование и редактирование изображения.



4 . **Экспорт**. Все изменения в **Darktable** сохраняются в базе данных приложения, а оригинальный файл изображения остаётся нетронутым. Необходимо выполнить экспорт таким образом, чтобы потом можно было загрузить файл в Интернет или открыть в другой графической программе. Экспорт изображений осуществляется в режиме Обзор, в разделе «**Экспорт**», расположенном на правой панели. Для осуществления экспорта необходимо выбрать параметры.



5 . **Печать**. Для отправки изображения на принтер перейдите в режим Печать, настройте параметры макета печати и выберите принтер.



GUVCView — программа для работы с веб-камерами

Установка

Описание программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** guvcview-2.0.6-1

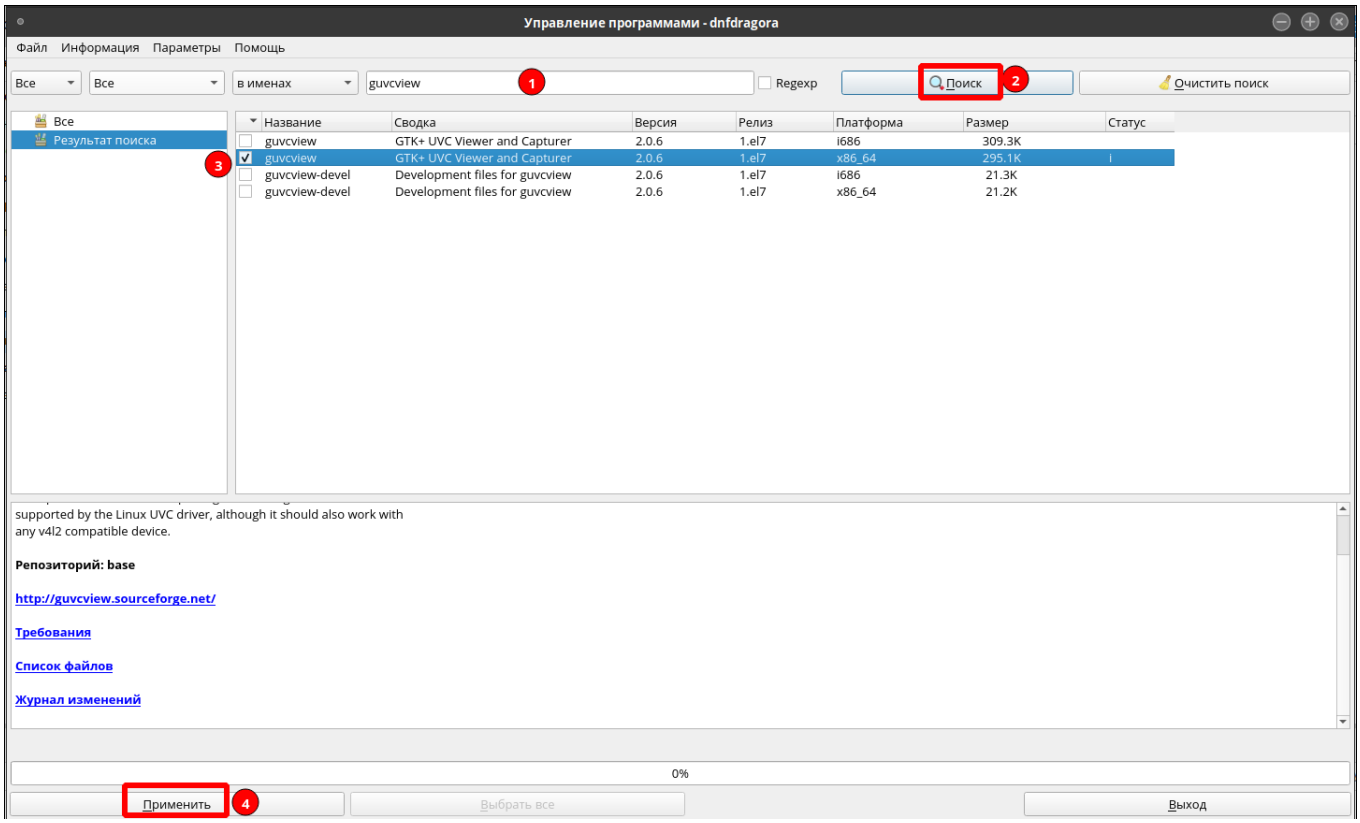
Guvcview (GTK + UVC Viewer) — программа для работы с веб-камерами, использующими протокол передачи видео UVC, выполняющая функции фотографирования и видеосъемки.

С помощью *guvcview* можно захватывать видео или изображения вместе со звуком.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**guvcview**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

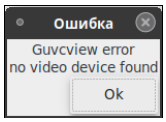
```
dnf install guvcview
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

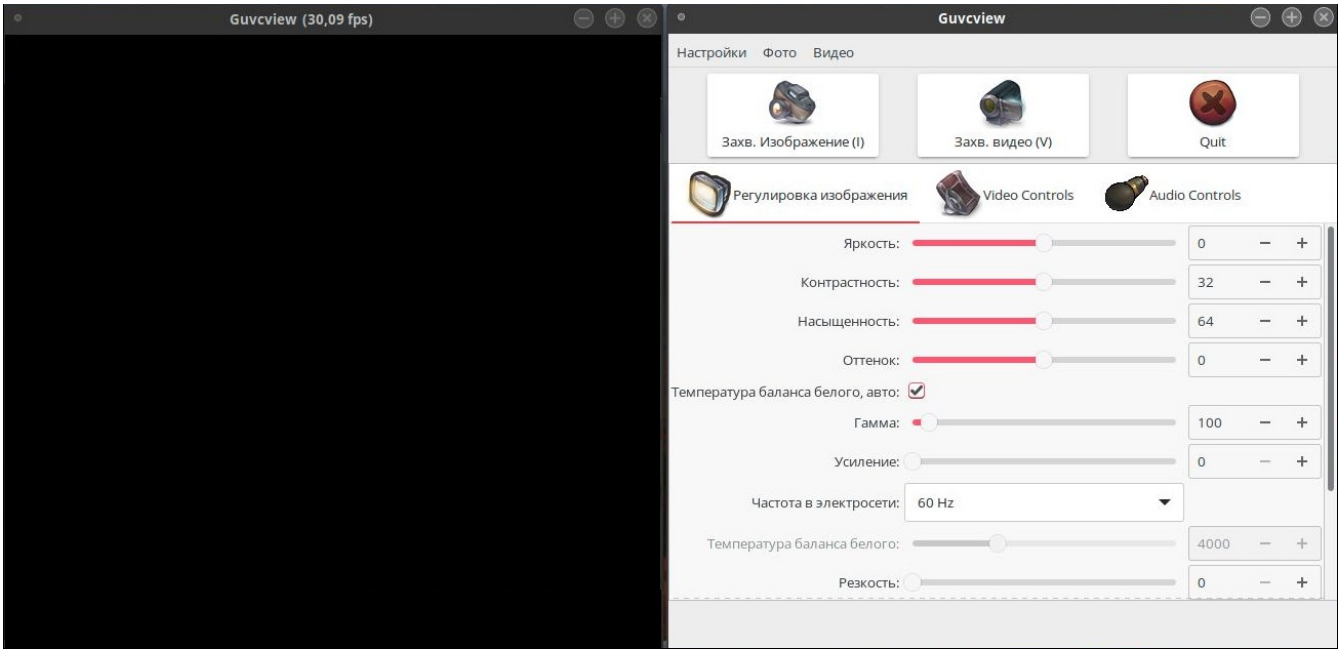
После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**Работа с веб-камерой**».

Описание программы

Если к машине не подключена ни одна веб-камера, будет выведено соответствующее сообщение, а программа не запустится.

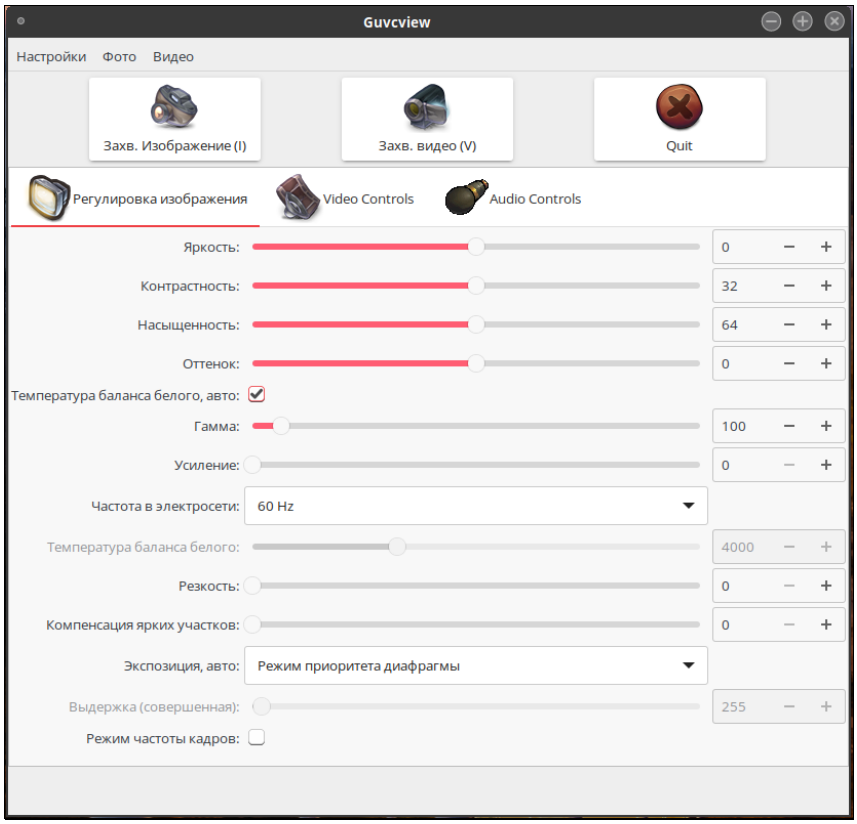


При успешном запуске программы с подключенным устройством появятся две формы. Первая форма содержит изображение с камеры, а на второй находятся настройки и элементы управления.



В настройках изображения (вкладка «**Регулировка изображения**») можно регулировать:

- яркость;
- контрастность;
- насыщенность;
- оттенок;
- гамму;
- усиление;
- частоту электросети;
- температуру баланса белого;
- резкость;
- компенсацию ярких участков;
- экспозицию;
- выдержку (если поддерживается).

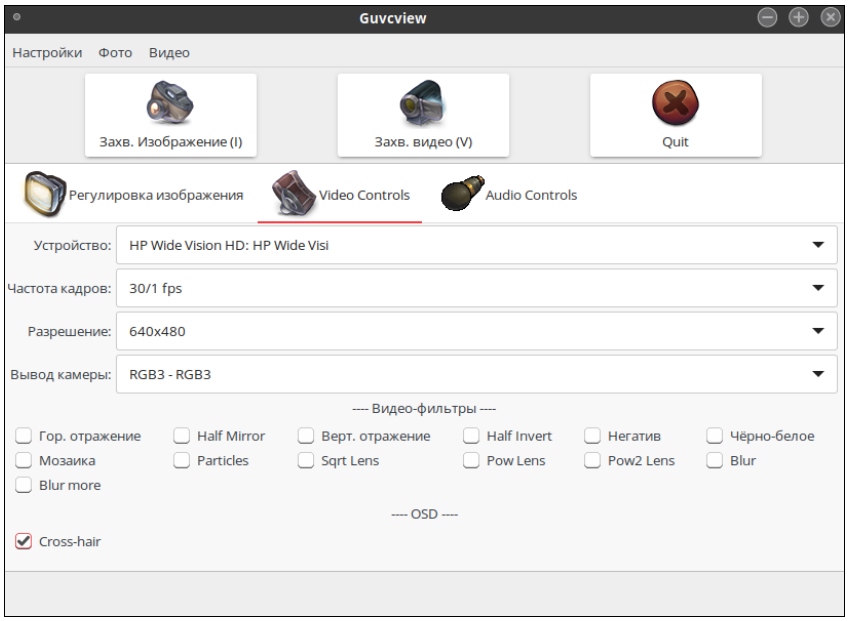


В настройках видео (вкладка «**Video Controls**») можно выбрать и установить:

- устройство;
- частоту кадров;
- разрешение;
- вывод камеры.

Также в программе к съемке можно применять видео-фильтры:

- горизонтальное отражение;
- Half Mirror;
- вертикальное отражение;
- Half Invert;
- негатив;
- черно-белое;
- мозаика;
- Particles;
- Sqrt Lens;
- Pow Lens;
- Pow2 Lens;
- Blur;
- Blur more.

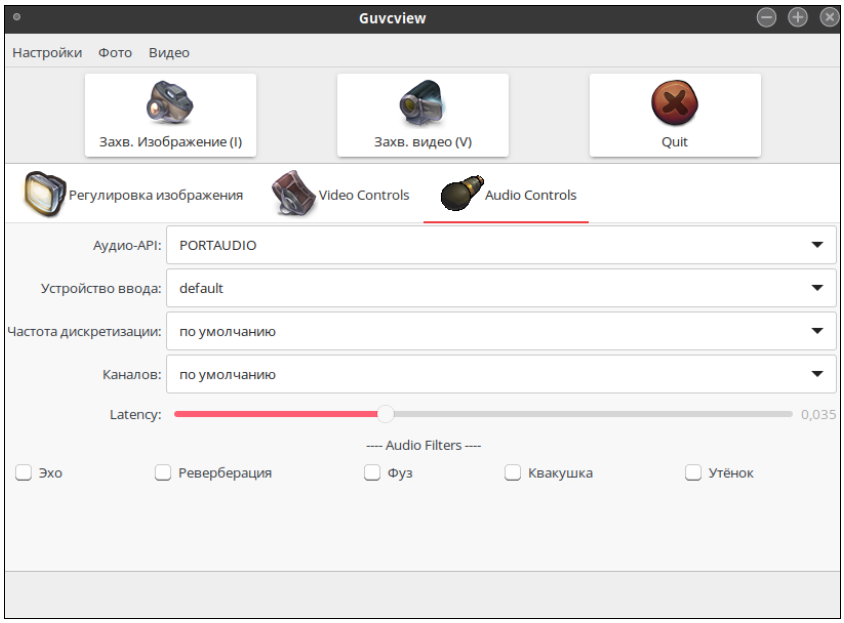


В настройках микрофона (вкладка «**Audio Controls**») можно изменить:

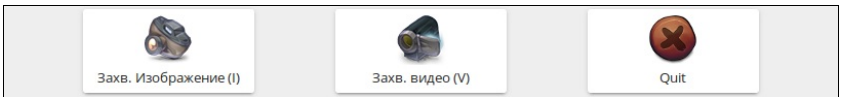
- аудио-API (PORTAUDIO,PULSEAUDIO);
- устройство;
- частоту дискретизации;
- количество каналов;
- задержку (latency).

Также к звуку можно применить аудио-фильтры:

- эхо;
- реверберация;
- фуз;
- квакушка;
- утенок.



В верхней части интерфейса располагаются три кнопки управления: «**Захват изображения**», «**Захват видео**» и «**Выход**». Произвести запуск фотосъемки и видеосъемки можно клавишами «**I**» и «**V**».



В *guvcview* можно сохранить профиль и загрузить уже готовый. Для этого перейдите в пункт меню « **Настройки**» — «**Сохранить профиль**» / «**Загрузить профиль**».

В пункте меню «**Фото**» — «**Файл**» можно выбрать путь и формат (*raw*, *jpeg*, *png*, *bmp*) сохранения фото.

В пункте меню «**Видео**» — «**Файл**» можно выбрать путь и формат (*mkv*, *webm*, *avi*) сохранения видео-файлов.

В «**Видео**» также можно выбрать видео/аудио кодеки и изменить их свойства.

Поддерживаемые видео-кодеки:

- *Raw camera input*;
- *MJPG*;
- *MPEG*;
- *FLV1*;
- *WMV1*;
- *MPG2*;
- *MS MP4 V3*;
- *MPEG4-ASP*;
- *MPEG4-AVC* (H264);
- *HEVC* (H265);
- *VP8*;
- *VP9*;
- *Theora*.

Поддерживаемые аудио-кодеки:

- *PCM*;
- *MP2*;
- *MP3*;
- *AC-3*;
- *AAC*;
- *Vorbis*.

Synfig Studio — создание векторной анимации

Установка
Описание программы
Первоначальная настройка
Работа в программе
Функция связывания
Движение
Шкала времени
Ключевые кадры
Просмотр анимации
Рендеринг

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** synfigstudio-1.4.0-1

Synfig Studio — это свободное программное обеспечение для создания векторной 2D анимации.

Анимация — это быстрый показ последовательности изображений, создающий иллюзию движения. Традиционно 2D анимация создавалась путём рисования каждого изображения отдельно. Такие изображения называются «кадры» (также используется термин «фреймы»), а сам этот метод называется «покадровая анимация». Но создание иллюзии "живого" движения требует большого количества кадров (обычно 24 кадра в секунду), поэтому метод покадровой анимации очень медленный и требует много времени и ресурсов.

Synfig Studio использует две технологии создания кадров:

- *Morphing animation* — морфинг;
- *Cutout animation* — перекладная анимация.

Морфинг создаёт плавный переход между двумя изображениями, это достигается путём преобразования одной формы в другую, часто с использованием специальных точек-фиксаторов. Для векторных изображений *Synfig Studio* делает эти переходы автоматически, анимация создаётся просто подстановкой изображения в ключевых позициях, находящихся на сравнительно больших промежутках времени. Художник создаёт столько кадров, сколько необходимо, чтобы получить основу движения анимационной сцены, о создании промежуточных кадров позаботится *Synfig*.

Перекладная анимация заключается в разделении объекта на составные части и простого их изменения (например, перемещения, вращения и изменения размера) в разных позициях времени анимации. *Synfig Studio* использует эти позиции и создаёт плавные переходы между каждой из них. Перекладная анимация может быть создана с использованием как растровых, так и векторных изображений.

В обоих случаях задачей *Synfig Studio* является заполнить пробелы между так называемыми "ключевыми кадрами", чтобы получилась плавная анимация. Этот процесс называется "фазовка" или "твининг" (*tweening*), хотя фазовка — не единственное достоинство *Synfig Studio*.

Вы можете подробнее ознакомиться с работой в Synfig Studio, просмотрев наши обучающие видео:

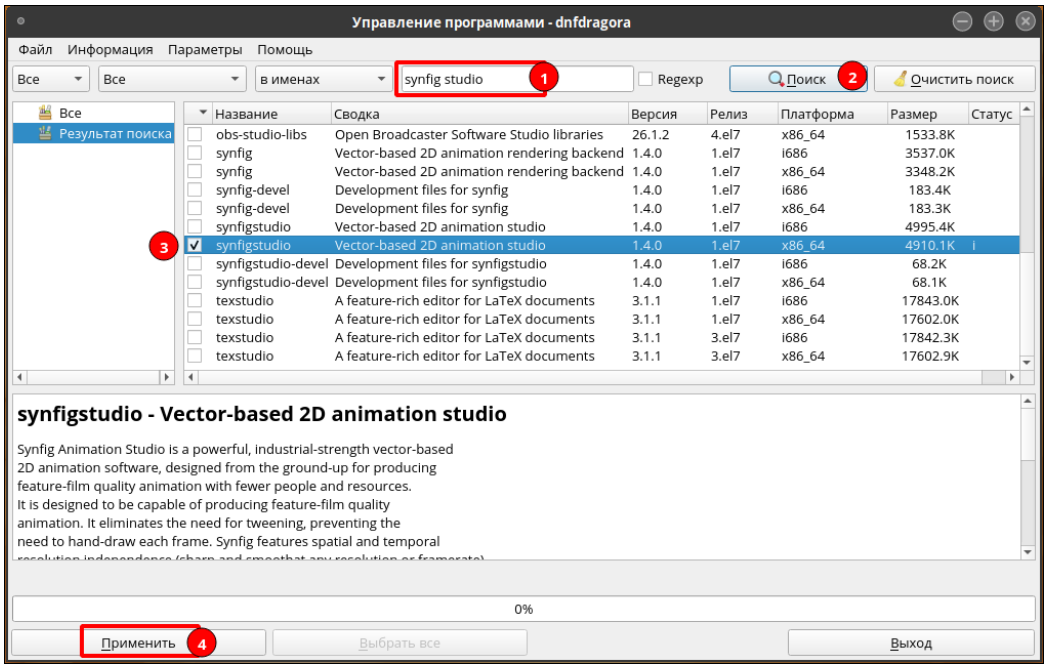
- на **RuTube** — Создание анимации с помощью Synfig Studio;
- в **Яндекс.Дзен** — Создание анимации с помощью Synfig Studio;
- в **VK Видео** — Создание анимации с помощью Synfig Studio.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**synfig studio**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

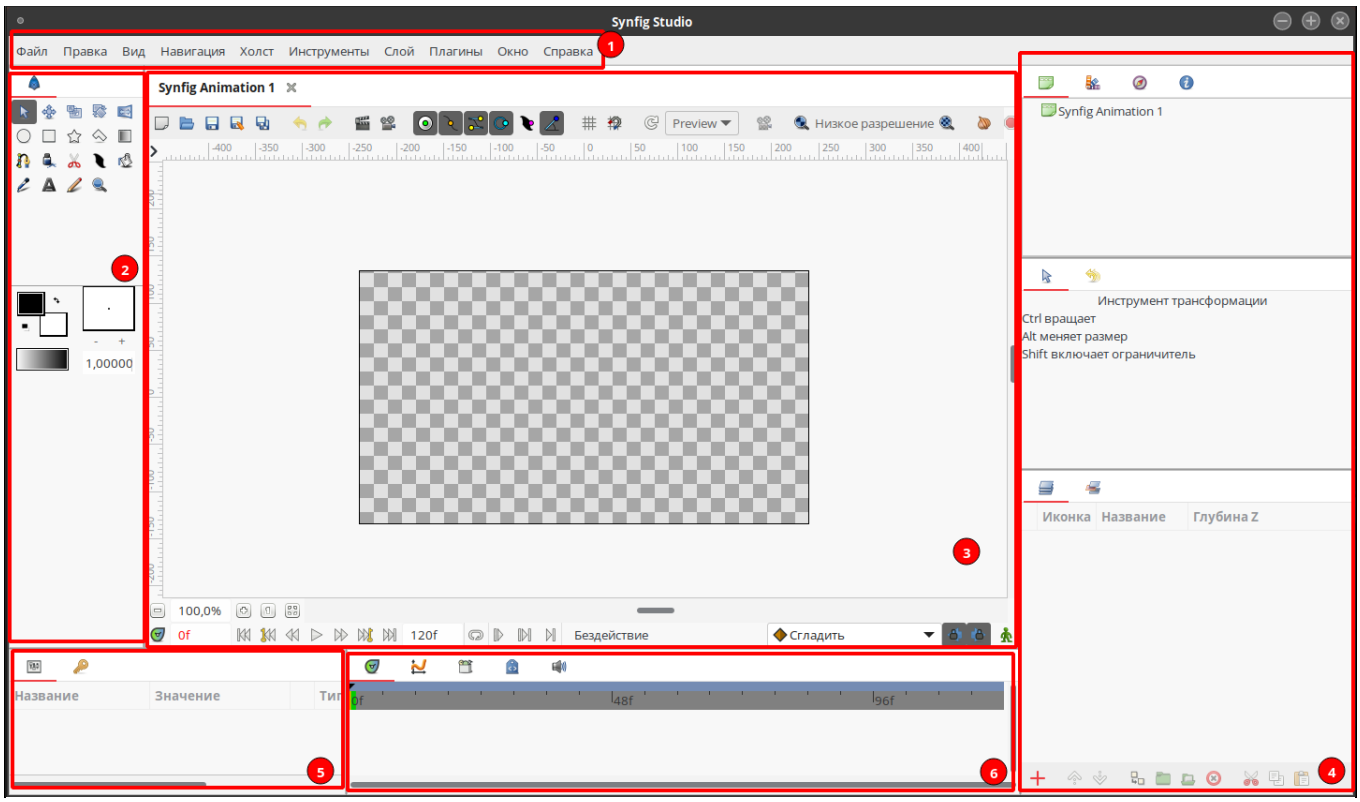
```
dnf install synfigstudio
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Графика**» - «**Редактор 2D анимации Synfig Studio**».

Описание программы

Окно программы выглядит следующим образом:



1. *Основное меню программы* — здесь доступны настройки программы и действия для работы над проектом.

2. *Панель инструментов* — основные действия над проектом: открытие файлы, выбор инструменты, изменение цвета и т.д.

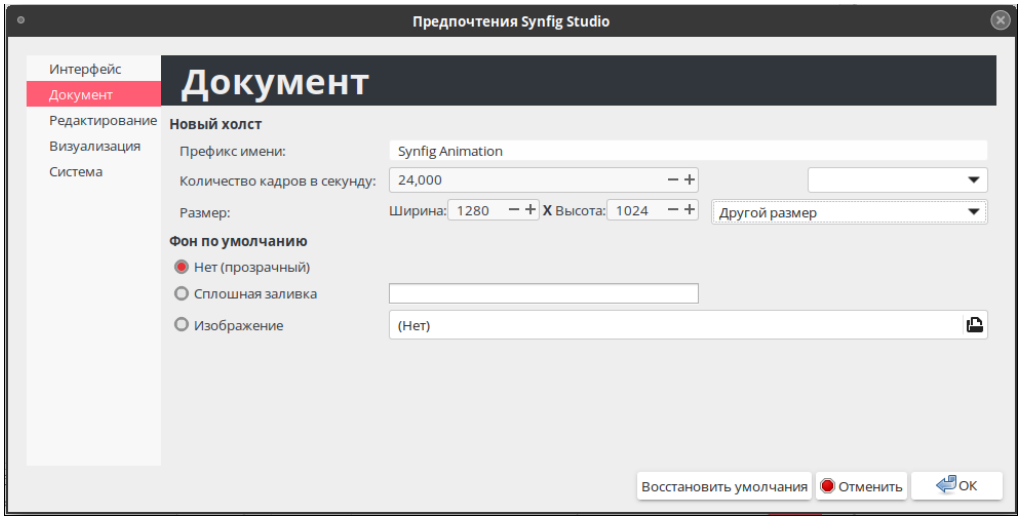
3. *Холст* — рабочая область программы, где создается анимация.

4. Панели *Навигатор*, *Параметры инструментов* и *Слои* — используются для создания эффектов будущей анимации.

5. *Панель параметров и отслеживания времени* — здесь можно найти подробные параметры и настройки для активного элемента, такие как цвет, ширина, непрозрачность, местоположение и т.д. Справа находится панель *Отслеживания времени*, которая позволяет создавать и изменять ключевые точки.

Первоначальная настройка

Для первоначальной настройки документа установите необходимый размер холста. Для этого перейдите в пункт меню **Правка** — **Настройки**, далее выберите раздел **Документ**.



В качестве примера размер холста будет установлен **1280x1024** пикс. Нажмите **OK** для применения изменений.

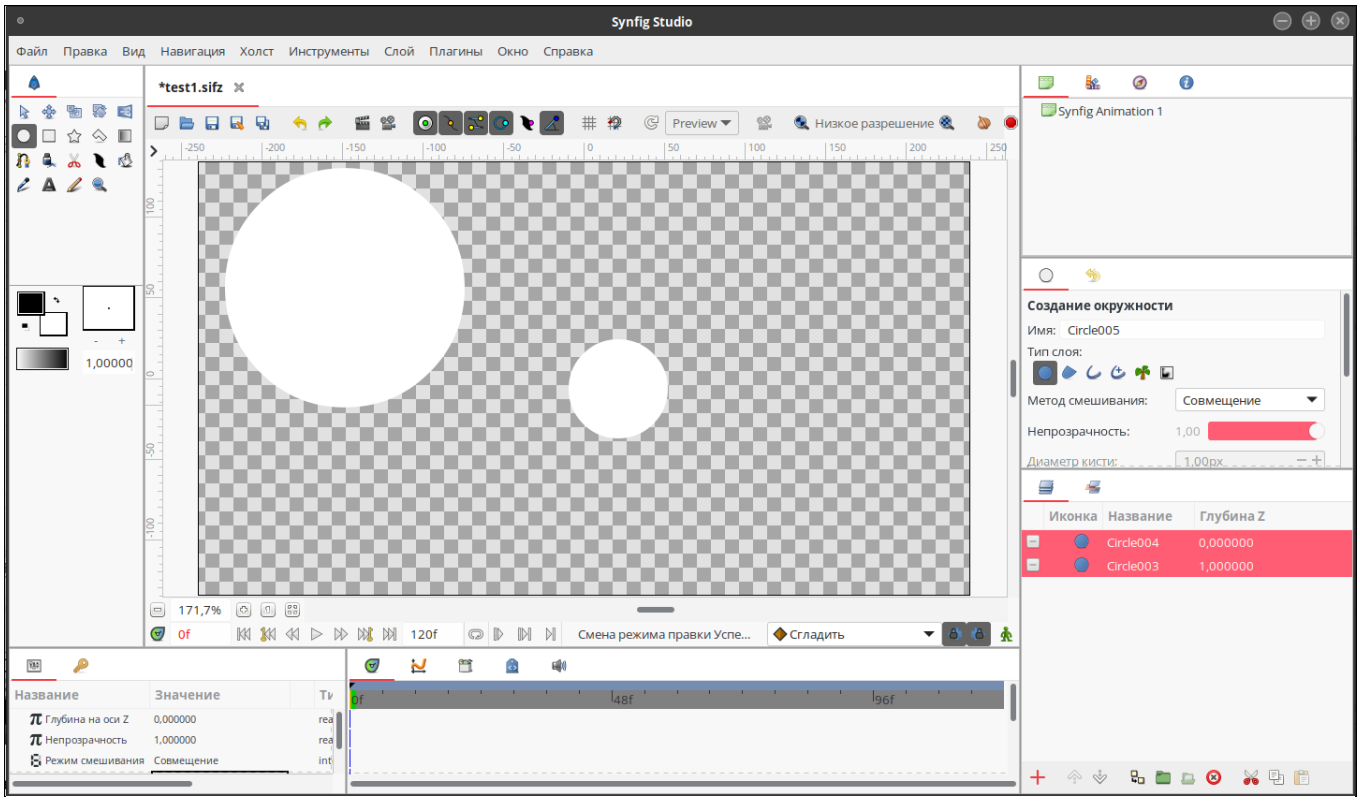
Для масштабирования холста нажмите и удерживайте клавишу **Ctrl** и вращайте колесо мыши. Масштабирование также доступно из пункта меню **Вид** — **Увеличить** / **Уменьшить** или использованием функции **Наилучшее заполнение**.

Для сохранения внесенных в проект изменений выберите пункт меню **Файл** — **Сохранить**. В окне сохранения необходимо ввести имя файла, затем нажать кнопку «**Сохранить**».

Работа в программе

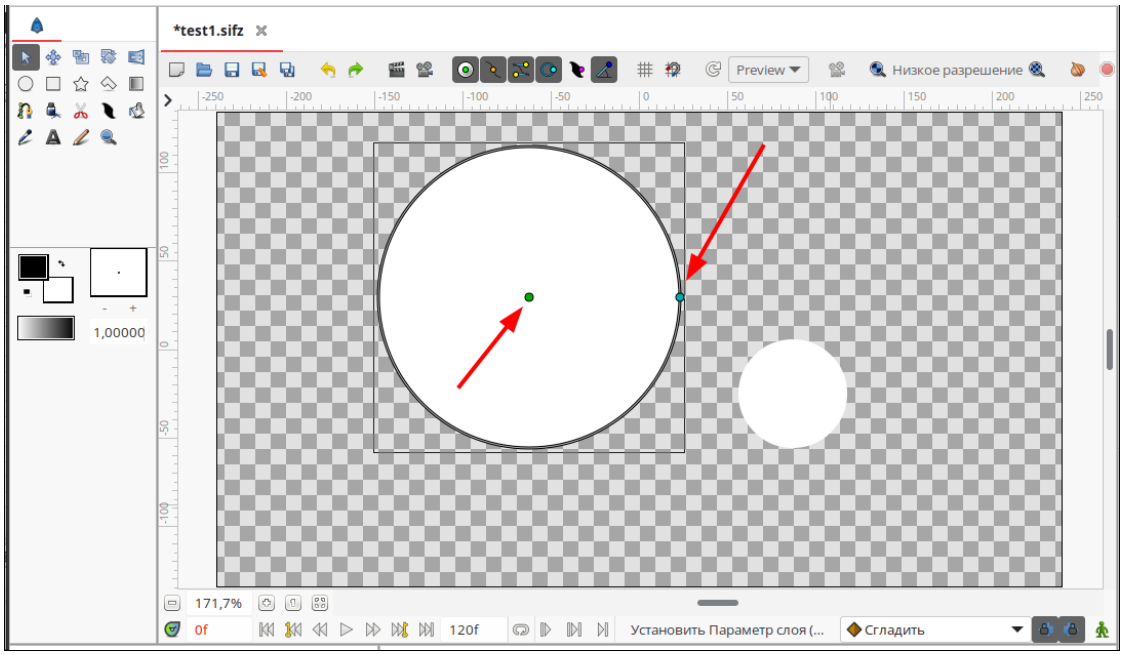
В *Synfig Studio* изначально включен «режим рисования», в котором создаются и изменяются изображения. Однако эти изменения не будут преобразованы в анимацию. В данном режиме объекты подготавливаются.

Для примера будут нарисованы два круга, для этого на *Панели инструментов* (**2**) выберите инструмент **Окружности**.



Для изменения размера фигуры или перемещения ее на холсте выберите **Инструмент трансформации** на *Панели инструментов*, щелкните по объекту и двигайте управляющие точки. Точка в центре фигуры — для перемещения, точка на границе фигуры — для изменения размера.

Если необходимо выделить несколько объектов, щелкайте по ним мышью, удерживая клавишу **Ctrl**.



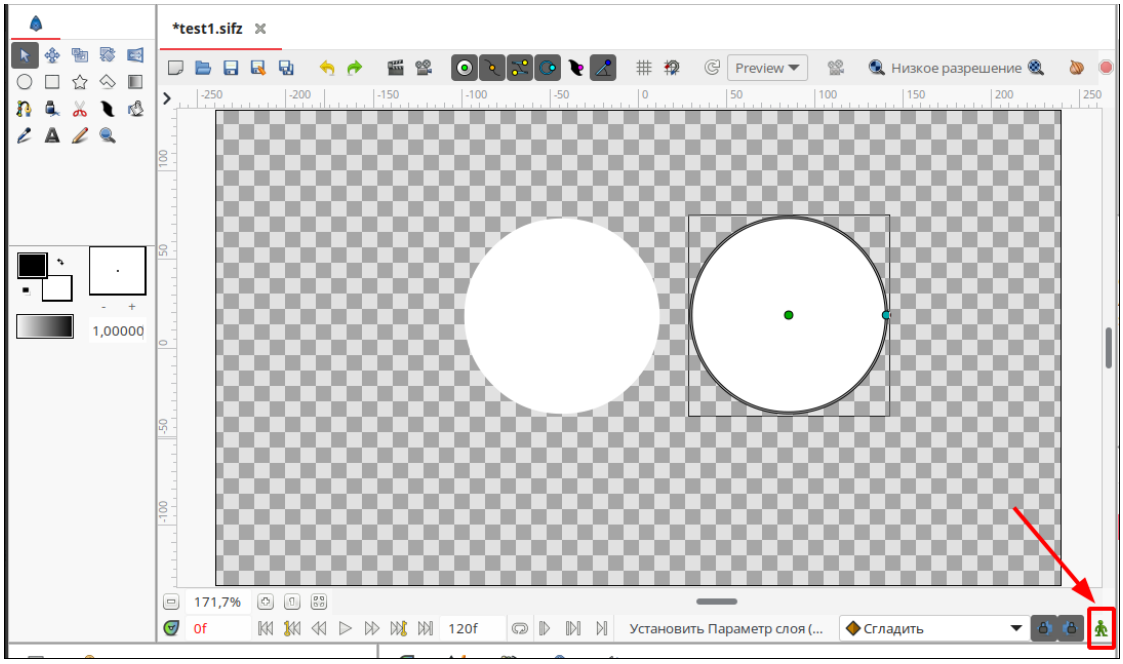
Функция связывания

Когда необходимо, чтобы у нескольких объектов был одинаковый размер, можно применить **функцию связывания**. Для этого выберите нужные объекты, выделите их точки радиуса (на границе фигуры), затем нажмите по любой из выделенных точек ПКМ и в контекстном меню выберите пункт «**Связь**». После этого точки радиуса фигур будут зависеть друг от друга — при изменении радиуса одной окружности автоматически будет изменяться радиус и у другой.

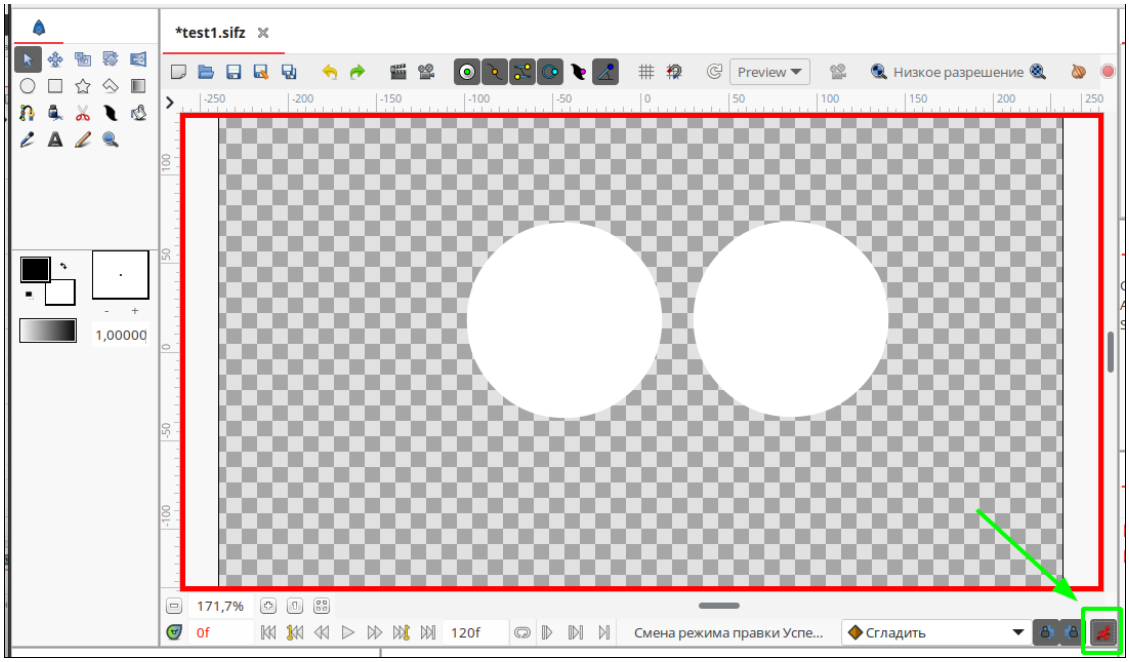
Связывание является фундаментальной концепцией *Synfig*. Вы можете создавать связи не только между управляющими точками, но и между параметрами.

Движение

Для того чтобы любые изменения объектов были обработаны как анимация, необходимо переключиться в соответствующий режим. Для этого в программе *Synfig Studio* предназначена зеленая кнопка «**Включить режим редактирования анимации**».



После нажатия на кнопку вокруг холста появляется красная рамка, а на кнопке переключения будет изображен красный человек. Для выхода из режима анимации достаточно еще раз нажать на эту же кнопку.



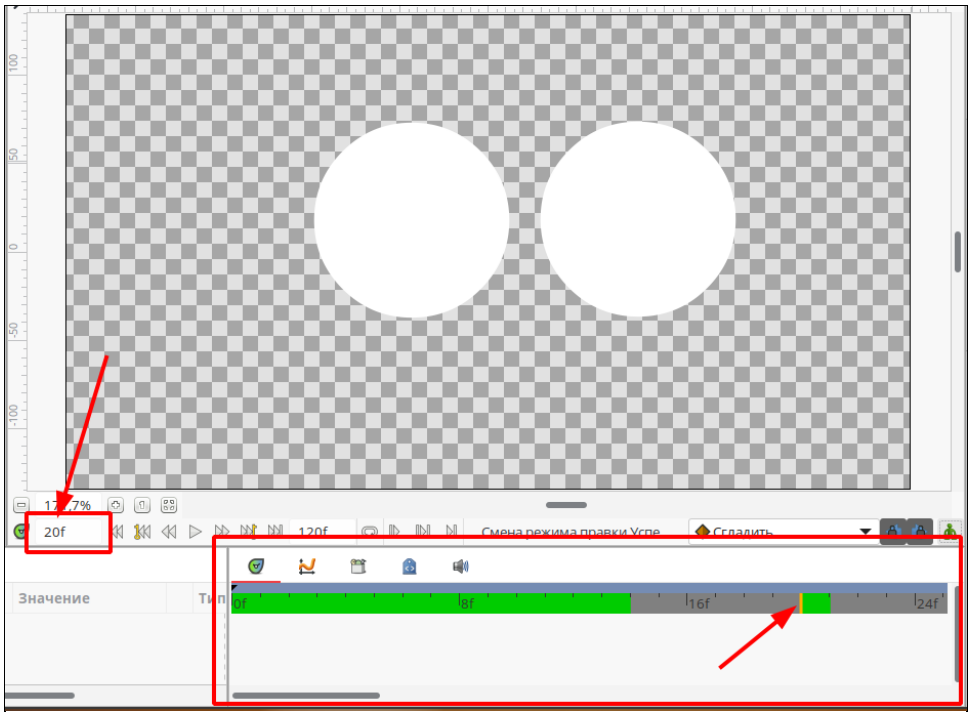
Шкала времени

Эффект анимации является результатом быстрой смены похожих изображений. Любые изменения протекают во времени, поэтому в *Synfig* предусмотрена панель «шкала времени». Похожая панель есть в большинстве программ для анимации, однако называться она может по-разному. Шкалу времени можно сравнить с кинолентой или фотопленкой, где в каждом кадре может быть запечатлено какое-нибудь изображение.

На шкале присутствуют деления, более крупные из которых помечены как **0f**, **24f**, **48f** и т.д.

F – это сокращение от *frame* (кадр), а **s** – от *second* (секунда).

В каждой секунде 24 кадра (задано «по-умолчанию», но вы можете изменить этот параметр в *Настройках*). Если щелкнуть в любом месте шкалы, то вы увидите линию, указывающую текущий кадр, также он будет указан в нижнем левом углу рабочей области.

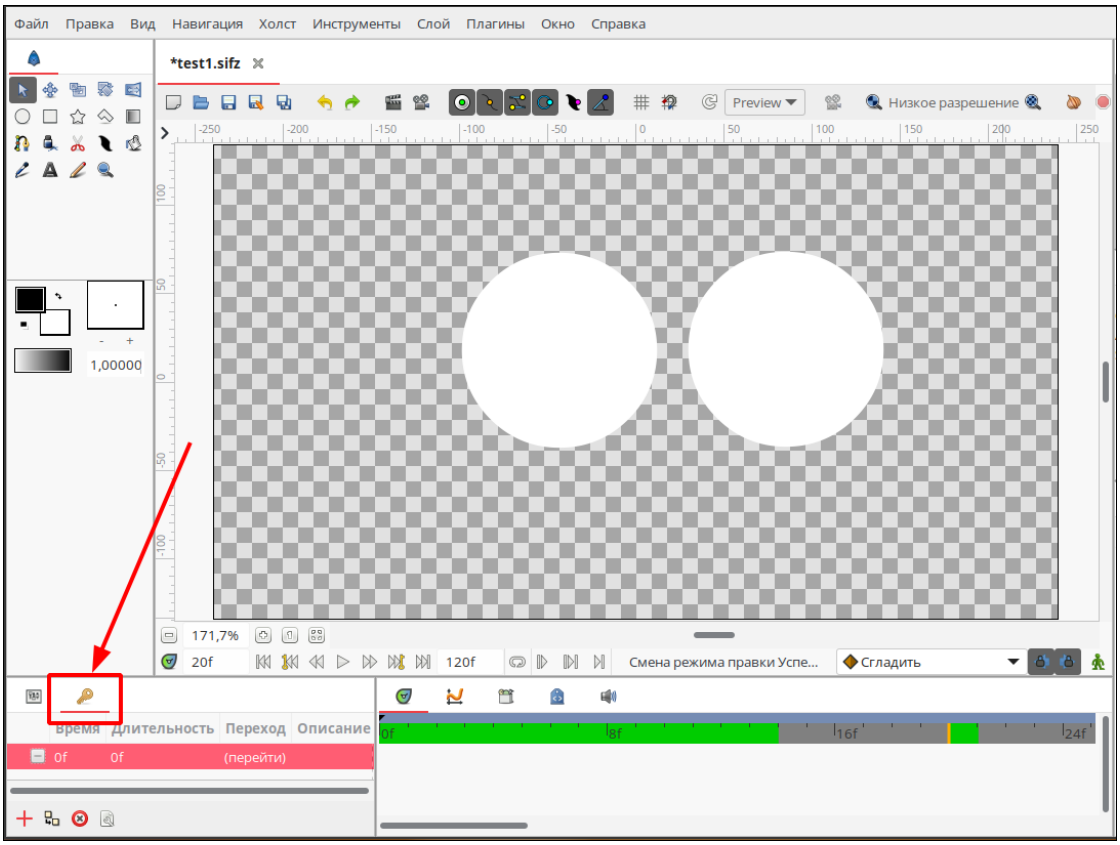


Ключевые кадры

Ключевой кадр — это изображение, на котором фиксируется положение объектов в определенный момент времени, поэтому необязательно прорисовывать каждый кадр. Достаточно указать программе начальное и конечное «состояние» объекта, все остальное программа попытается вычислить сама.

Начальное и конечное положение фиксируется в ключевых кадрах. Однако, в большинстве случаев, таких кадров бывает намного больше двух, т. к. при достаточно сложном изменении объекта программа не может корректно вычислить траекторию и характер изменения.

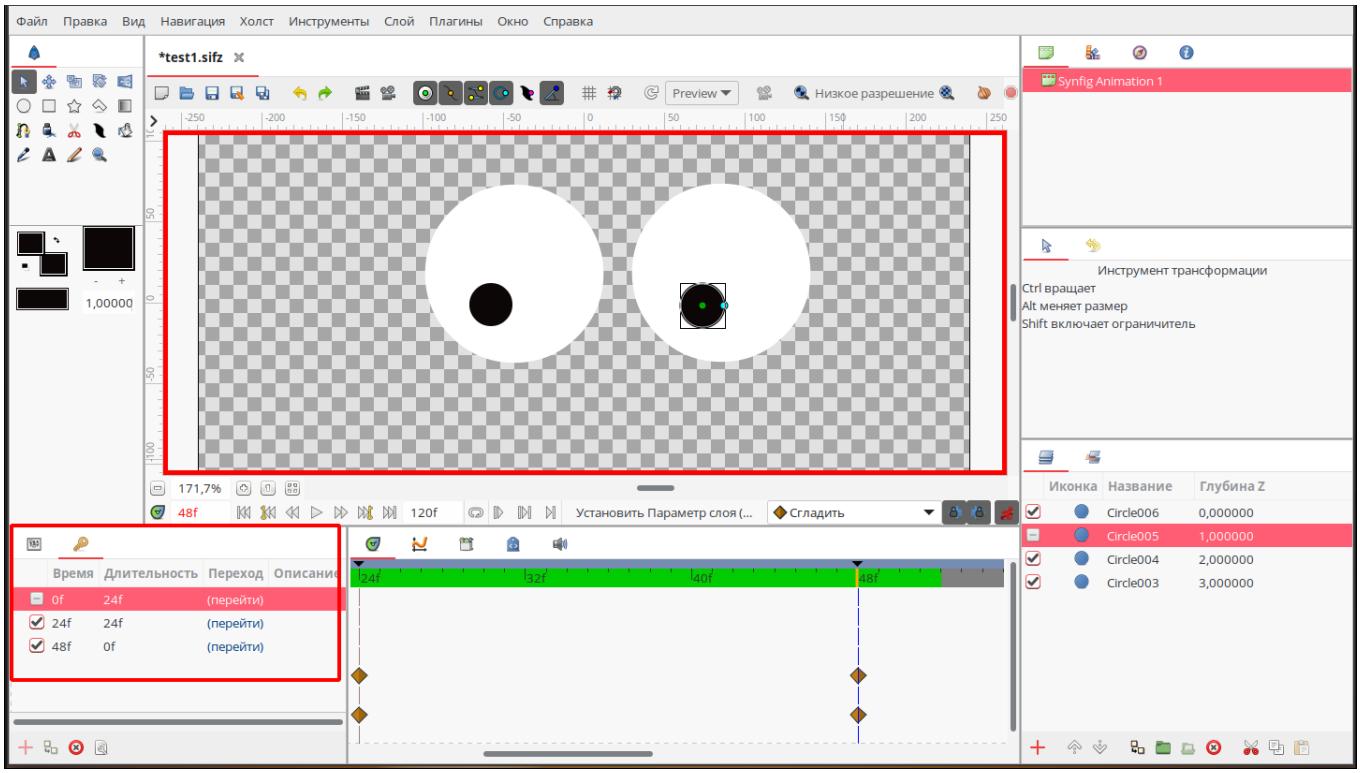
Для работы с ключевыми кадрами перейдите на *Панель параметров* (**5**) и откройте на вкладку с изображением ключа.



Здесь с помощью кнопки со знаком «+» можно добавлять ключевые кадры. В этих кадрах будет зафиксировано изменение фигуры, а в остальных — оно будет вычислено.

Перейдите на ползунке времени в позицию «**24f**» и измените положение фигуры. Добавьте ещё один ключевой кадр, щёлкнув на кнопку со знаком «**+**».

Повторите операцию для значения «**48f**» на шкале времени, измените положение и, для примера, размер. Должно получиться три ключевых кадра.

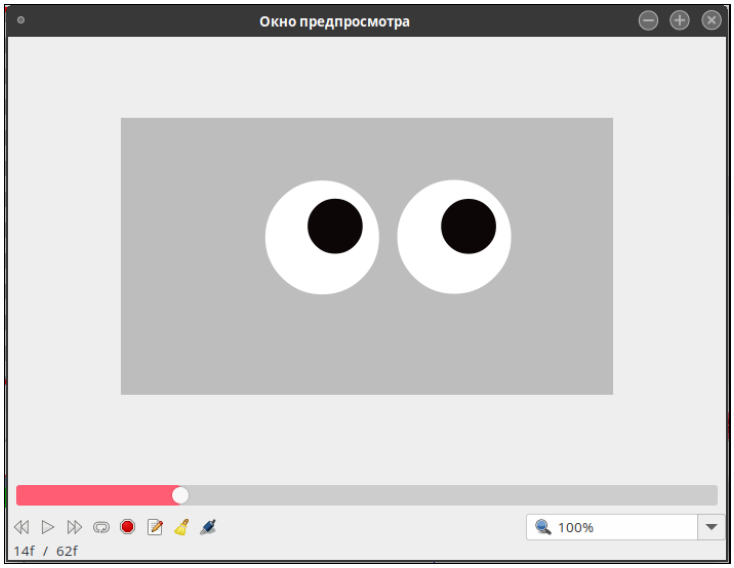


Благодаря позициям круга на различных ключевых кадрах, *Synfig* может понять, какое движение вы хотите получить (передвинуть круг, в частности), и дорисовать промежуточные изображения между этими состояниями. Каждое изображение будет составлять кадр вашей анимации, и, в конечном итоге, круг будет двигаться.

Просмотр анимации

Просмотреть созданную анимацию можно несколькими способами:

- зажав левую кнопку мыши и передвигая ею по шкале времени;
- нажав кнопку «**Воспроизвести**» в рабочей области ();
- воспользовавшись функцией предварительного просмотра (**Файл** — **Предварительный просмотр**).



Рендеринг

Для того чтобы сохранить файл, достаточно выполнить стандартную операцию сохранения. При этом будет сохранен файл в формате программы *Synfig*; другими словами, будут сохранены данные, описывающие определенным способом объекты и их изменения.

Чтобы получить изображение, необходима специальная программа (ее включают многие графические процессоры, в том числе и *Synfig Studio*), осуществляющая преобразование, в данном случае, векторного изображения в растровое. Процесс получения изображения называется **рендерингом** (от англ. *rendering*). Можно сказать, что во время этого процесса происходит визуализация изображения.

Однако требуется сохранить не простой рисунок, а анимацию (множество изображений). Она может храниться во многих форматах (видеоформатах и формате flash-анимации), в том числе и одном графическом — **GIF**. В нем и будет сохранена созданная анимация.

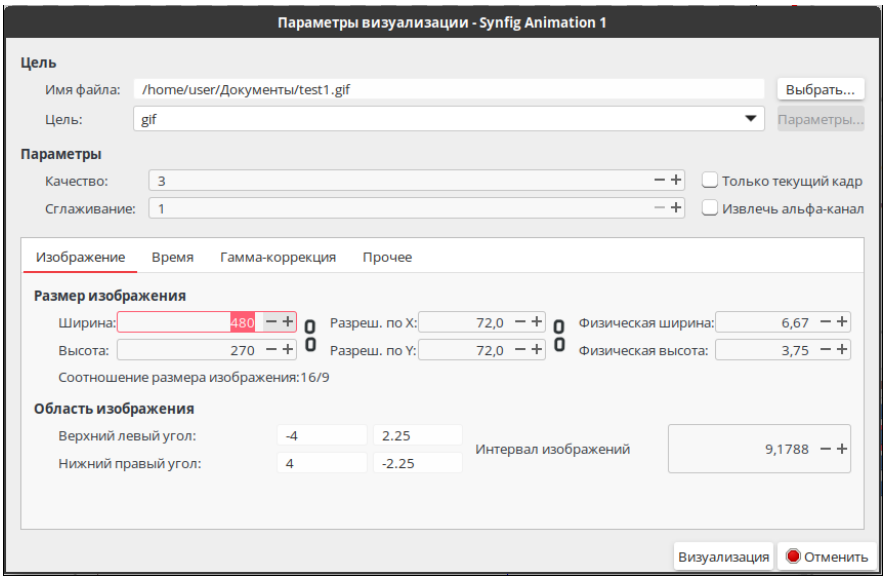
Для того чтобы вызвать окно рендеринга в *Synfig Studio*, необходимо выбрать пункт меню **Файл** — **Визуализация**. Откроется соответствующее диалоговое окно.

Поле **Имя файла** указывается место сохранения и имя файла (с расширением); кнопка «**Выбрать...**» вызывает диалоговое окно выбора папки.

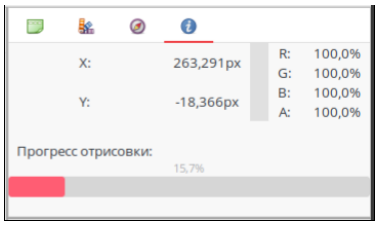
Выпадающий список «**Цель**» позволяет выбрать формат публикации. Выберите «**gif**».

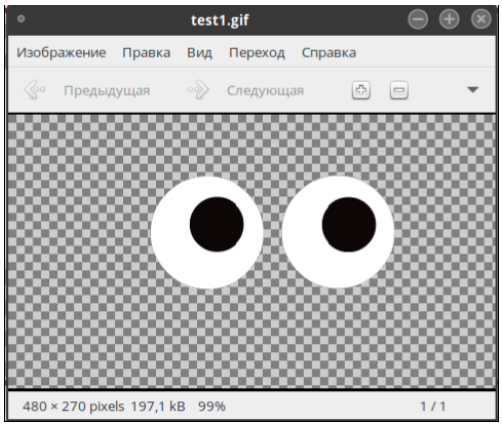
Вкладка «**Изображение**» управляет размерами и некоторыми другими параметрами изображения.

На вкладке «**Время**» можно настроить количество кадров в секунду, начало и окончание анимации.



Нажмите кнопку «**Визуализация**» для запуска процесса рендеринга, который может длиться от нескольких секунд до достаточно продолжительного времени (в зависимости от сложности анимации и мощности компьютера). Прогресс рендеринга можно увидеть во вкладке «**Инфо**» *Панели навигации*.





Imagination - программа для создания слайд-шоу

Установка
Описание программы
Работа в программе

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** imagination-3.6-3

Imagination - программа, позволяющая создавать слайд-шоу из изображений. *Imagination* имеет большое количество встроенных переходов, возможность добавления аудио в качестве музыкального сопровождения и создания подписей к изображениям.

Вы можете подробнее ознакомиться с созданием слайд-шоу в **Imagination**, просмотрев наши обучающие видео:

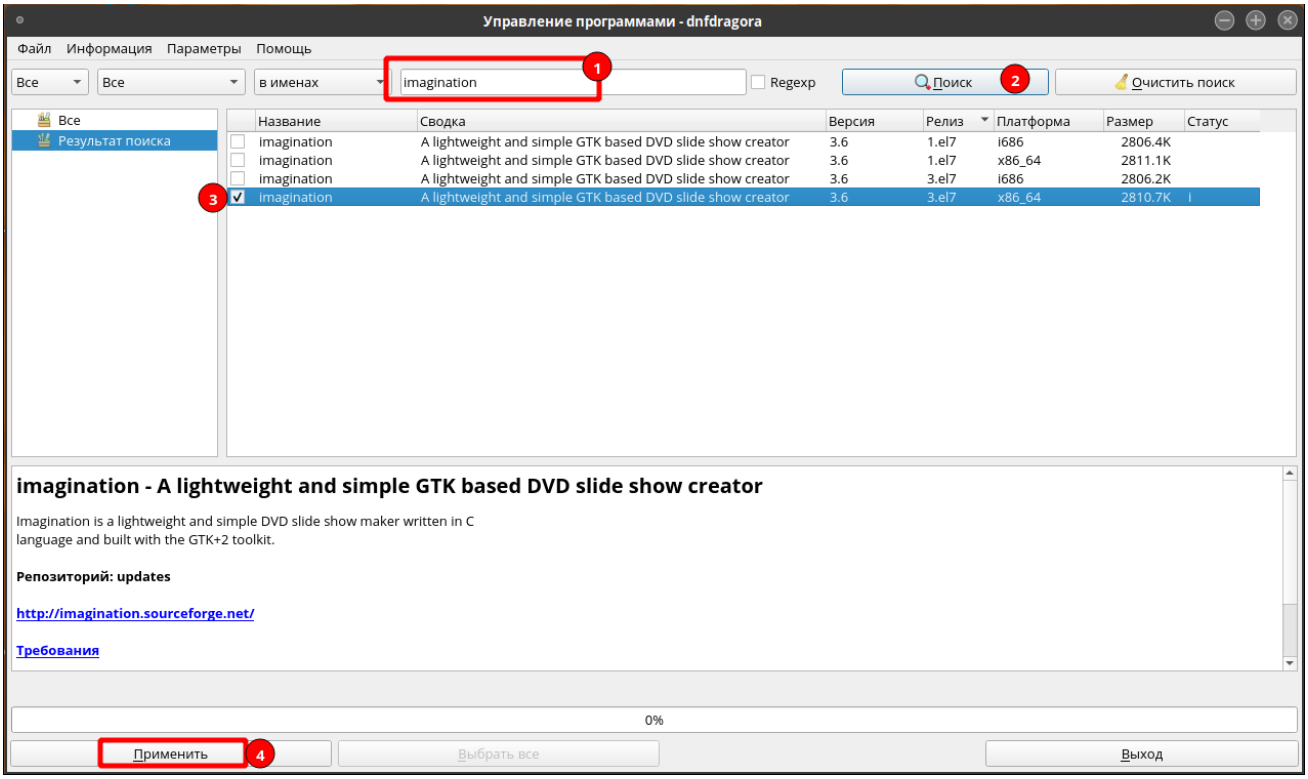
- на **RuTube** — Как сделать слайд шоу в РЕД ОС. Imagination;
- в **Яндекс.Дзен** — Как сделать слайд шоу в РЕД ОС. Imagination;
- в **VK Видео** — Как сделать слайд шоу в РЕД ОС. Imagination.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**imagination**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

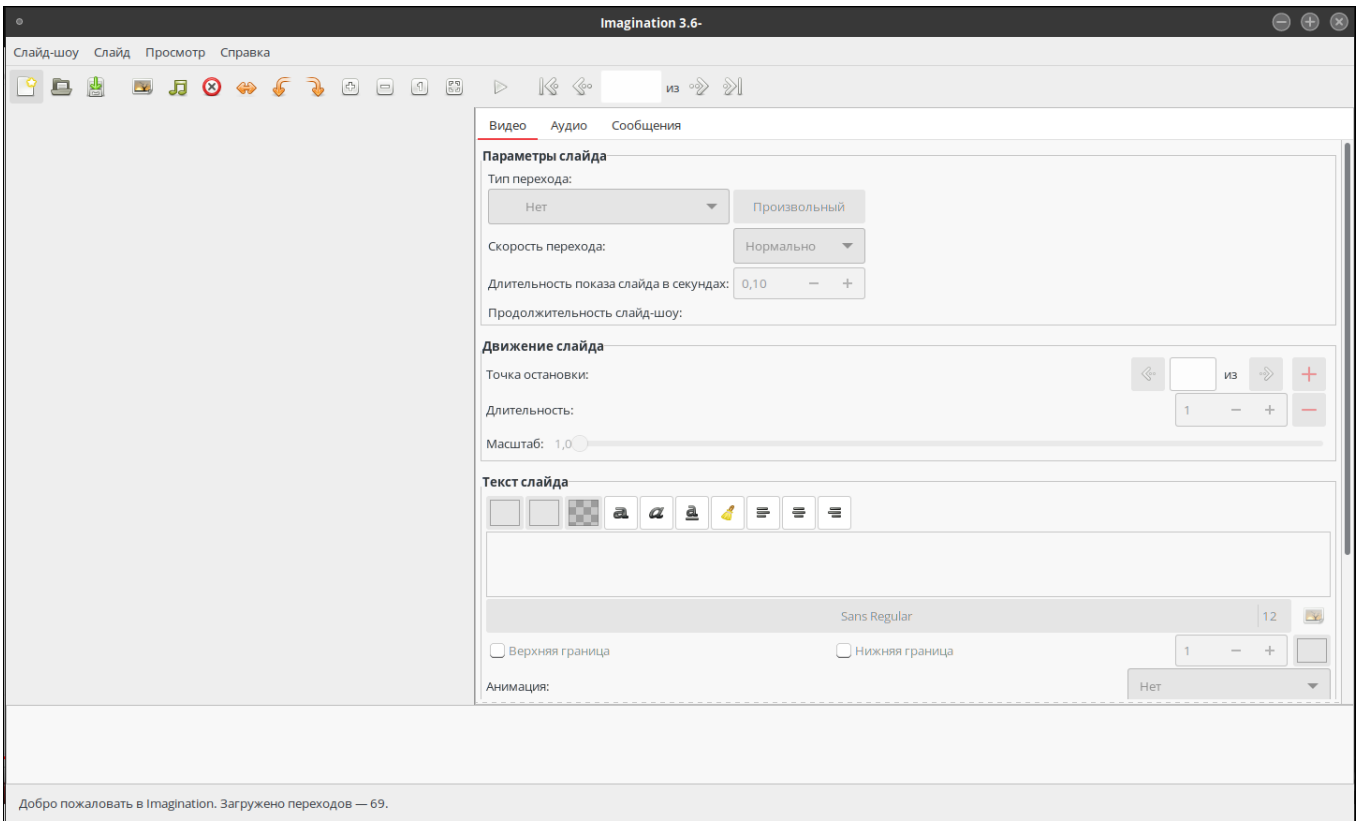
и выполните команду:

```
dnf install imagination
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

Описание программы

После установки программа будет доступна из «**Главного меню**» - «**Аудио и видео**» - «**Создание слайд-шоу**».



Вверху находится *основное меню* программы, в котором перечислены основные действия для слайд-шоу, действия для слайдов, а также параметры просмотра.

По умолчанию частота кадров предварительного просмотра составляет *15 кадров в секунду*, что дает эффект притормаживающей картинки, особенно это заметно при наложении эффектов переходов. Для большей плавности во время предварительного просмотра рекомендуется устанавливать максимальные значения количества кадров.

Ниже основного меню располагается *панель инструментов*, на которой доступны действия для создания и работы со слайд-шоу.



Кнопки панели инструментов:

1. Создание нового проекта слайд-шоу.

2. Открытие существующего проекта.

3. Сохранение проекта слайд-шоу.

4. Импорт изображений и музыкальных файлов (если они требуются для фона).

5. Удаление выбранного слайда.

6. Поворот по горизонтали.

7. Повороты влево/вправо на 90 градусов.

8. Размер слайдов в области предварительного просмотра.

9. Кнопки для навигации.

10. Кнопка воспроизведения/паузы.

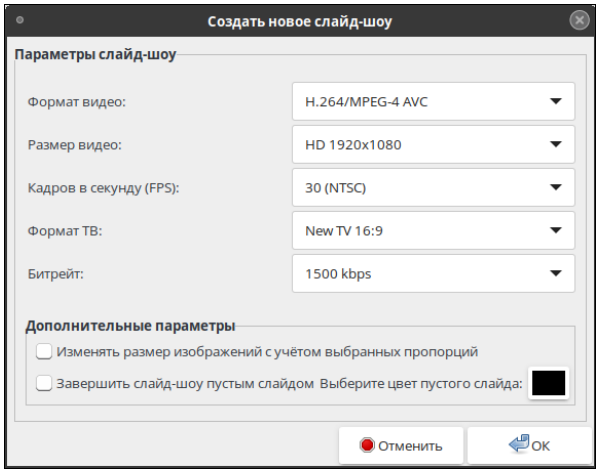
11. Кнопки перемещения по слайдам.

Ниже находится окно предварительного просмотра, его размер можно расширить.

Справа расположены настройки для видео, где есть возможность добавления переходов, движения, а также текста на слайды. В этом же окне есть вкладка для настройки добавляемых аудио-файлов.

Работа в программе

Для создания слайд-шоу выберите пункт меню «**Слайд-шоу**» - «**Новый**» либо нажмите на кнопку «**Создать новое слайд-шоу**» на панели инструментов. При этом будет выведено окно с настройками будущего слайд-шоу, в котором необходимо задать настройки формата видео, размера изображения, количества кадров в секунду и дополнительных параметров.

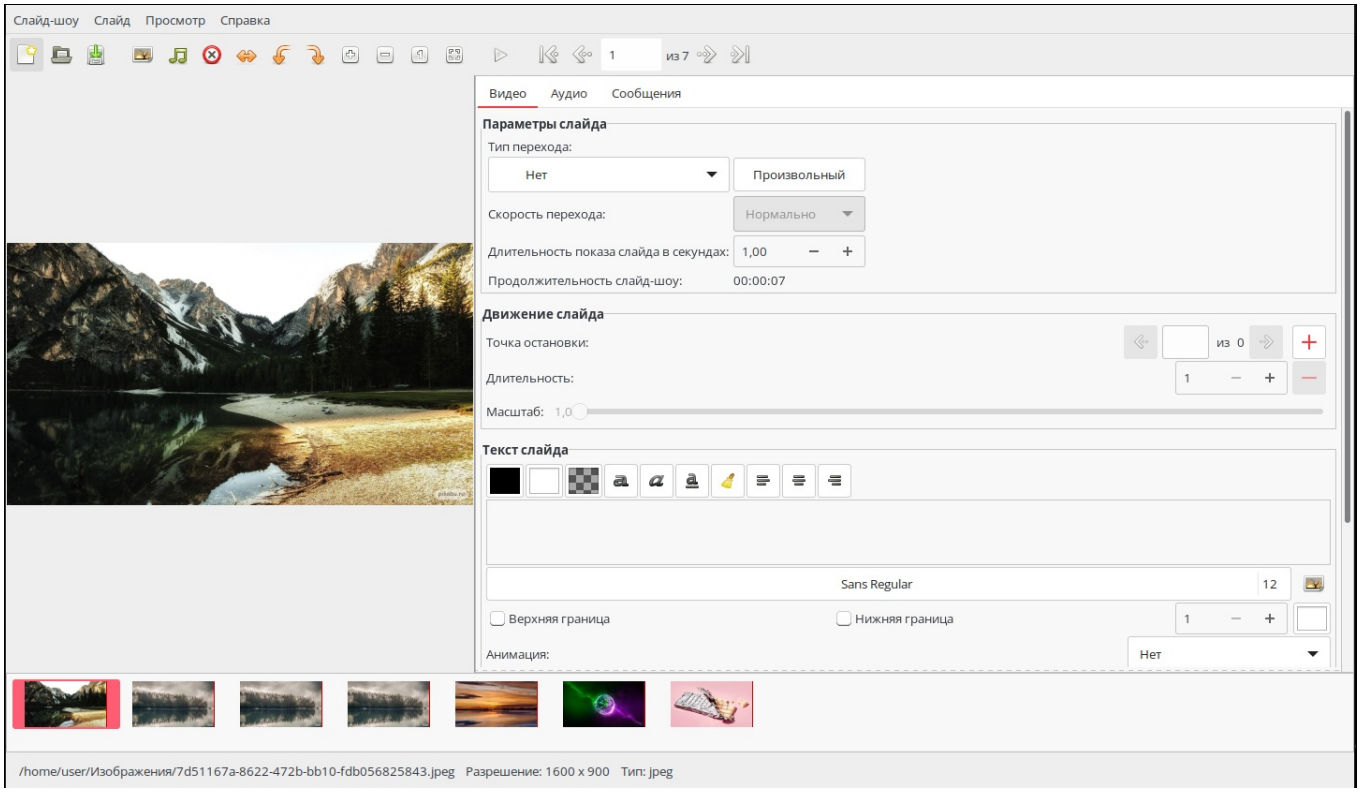


Для примера будут установлены обычные настройки. Также будет снят флаг с опции «**Изменять размер изображений с учетом выбранных пропорций**», чтобы оригинальные фото не были искажены.

Во втором пункте дополнительных настроек можно выбрать цвет для завершения слайд-шоу. Для сохранения настроек нажмите «**OK**».

После определения настроек необходимо импортировать изображения, для этого выберите в пункте меню «**Слайд-шоу**» - «**Импорт изображений**» или нажмите на кнопку «**Импорт изображений**» на панели инструментов.

Теперь слайды отображаются в нижней навигационной панели и по ним можно перемещаться.



Для добавления произвольных переходов выберите необходимый слайд, в параметрах слайда нажмите кнопку «**Произвольный**», программа случайным образом добавит произвольный переход. Также можно изменить скорость перехода и длительность показа выбранного слайда, при этом будет отображаться общая продолжительность слайд-шоу.

Для добавления текста на слайд предусмотрено много тонких настроек, в том числе и анимация появления. Внизу есть ползунки для точного позиционирования.

Для добавления фоновой музыки нажмите кнопку «**Импорт музыкального файла**» на панели инструментов, выберите аудио-файл и нажмите «**Открыть**». Все изменения производятся во вкладке «**Аудио**» окна настройки параметров слайда. Если добавлено несколько песен, то можно изменить их порядок с помощью клавиш  . В этом разделе также доступна регулировка длительности затухания - по умолчанию 5 секунд.

Незавершенный проект можно сохранить отдельным файлом для дальнейшего редактирования. Для этого в основном меню выберите «**Слайд-шоу**» - «**Сохранить как**», будет сохранен файл вашего проекта. Таким же образом вы сможете передать свой проект, чтобы его можно было доработать или изменить.

Когда проект полностью завершен, перейдите в пункт меню «**Слайд-шоу**» - «**Экспорт**», задайте имя файла и укажите место для его сохранения.

KolourPaint — растровый графический редактор

Установка
Описание программы
Скриншоты
Эффекты изображения
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kolourpaint-23.08.5

KolourPaint — редактор растровой графики. **KolourPaint** подходит для использования в таких задачах, как:

- составление диаграмм и рисование,
- обработка изображений,
- создание и редактирование снимков экрана,
- редактирование иконок.

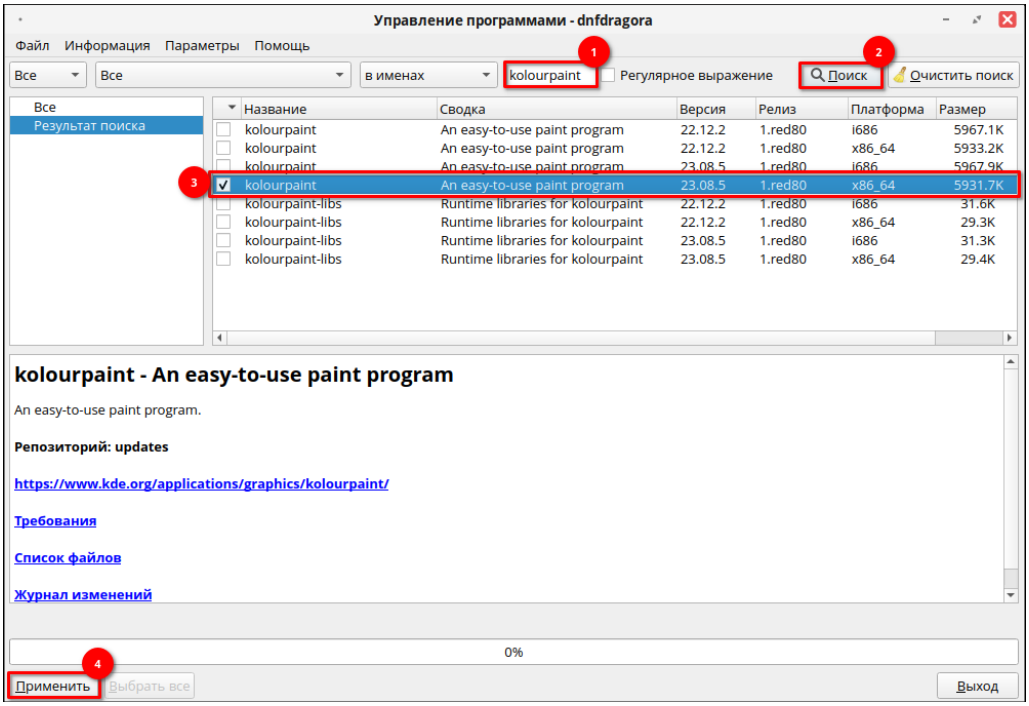
Редактор предоставляет широкий набор инструментов для рисования, включая кисти, карандаш, ластик, заливку, выделение и т. д. **KolourPaint** предлагает несколько шрифтов и параметров настройки, чтобы сделать текст более выразительным и соответствующим стилю рисунка.

KolourPaint также поддерживает работу с разными форматами файлов, включая PNG, JPEG, BMP, GIF и другие. Это позволяет пользователям импортировать и экспортировать свои рисунки в различных форматах, что облегчает их использование в других программах или публикацию в Интернете.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kolourpaint**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install kolourpaint
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Для просмотра

сведений о версии введите команду:

```
kolourpaint --version
```

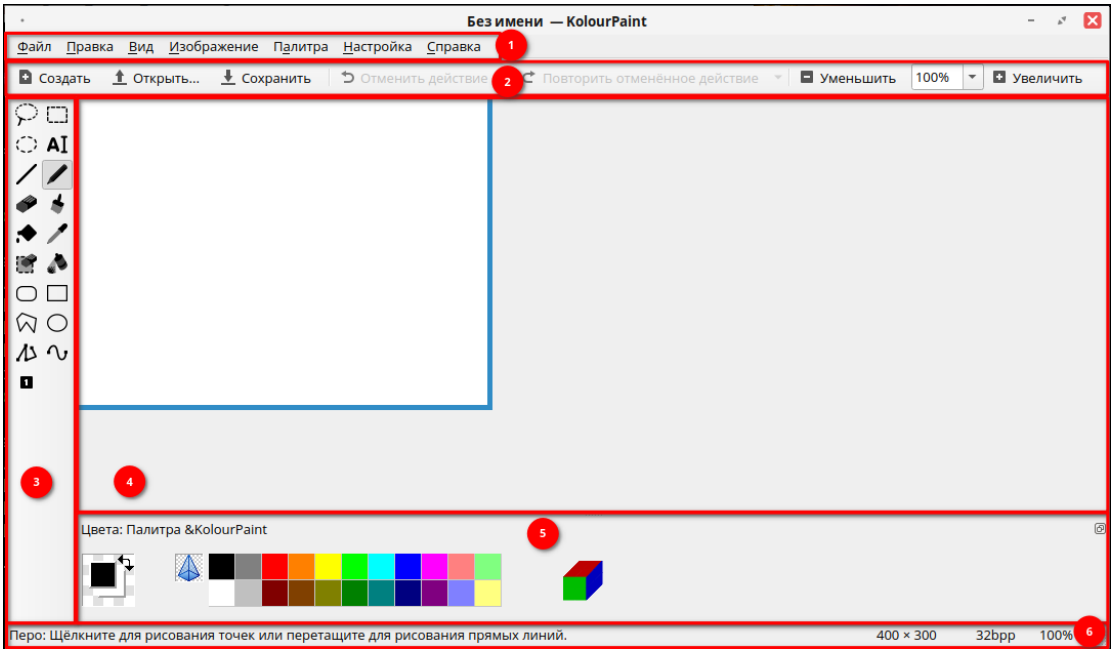
Для запуска программы через терминал введите команду:

```
kolourpaint
```

После установки программа будет доступна из «**Главного меню**» — «**Графика**» — «**KolourPaint**».

Описание программы

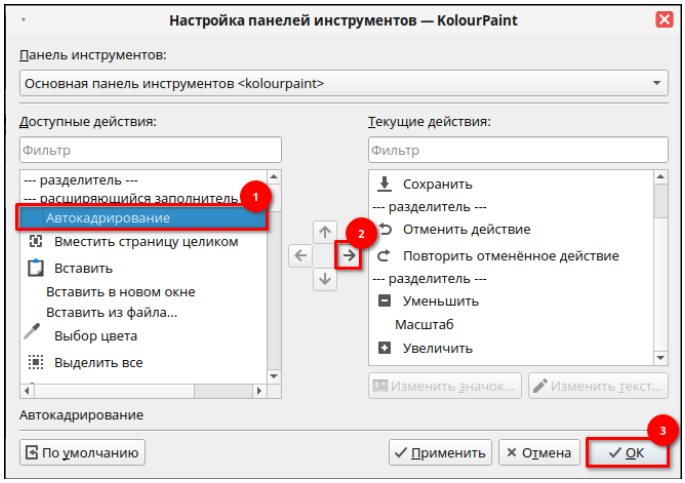
Интерфейс программы стандартный и состоит из нескольких типовых частей.



1 . **Основное меню программы** позволяет выполнять различные действия с изображениями, настраивать программу и панели инструментов.

2. **Основная панель инструментов** позволяет получить быстрый доступ к основным возможностям программы.

Для настройки панели инструментов перейдите в меню «**Настройка**» — «**Панели инструментов...**». В списке «**Доступные действия**» выберите инструмент, перетащите его в список «**Текущие действия**» с помощью стрелки  и нажмите «**OK**».



3 . **Боковая панель инструментов** — позволяет получить доступ к основным функциям рисования и редактирования изображений. Для быстрого выбора инструмента нажмите комбинацию клавиш, связанную с ним.

 **Свободное выделение (M)** — свободное выделение определённой области изображения.

 **Прямоугольное выделение (S)** — прямоугольное выделение определённой области изображения.

 **Эллиптическое выделение (I)** — эллиптическое выделение определённой области изображения.

 **Текст (T)** — добавление текста на изображение.

 **Линия (L)** — рисование прямых линий.

 **Перо (P)** — рисование свободных линий с перьевым наконечником.

 **Ластик (A)** — очистка части изображения.

 **Кисть (B)** — ЛКМ выполняет рисование основным цветом, ПКМ — позволяет рисовать цветом фона.

 **Заливка (F)** — заполнение выделенной области или закрытой формы выбранным цветом.

 **Выбор цвета (C)** — выбор цвета из изображения для использования с другими инструментами.

 **Очистка цвета (O)** — удаление определённого цвета из изображения.

 **Распылитель (Y)** — распыление краски с созданием текстурированного эффекта.

 **Округлённый прямоугольник (U)** — рисование прямоугольника с закруглёнными углами.

 **Прямоугольник (R)** — рисование прямоугольника.

 **Многоугольник (G)** — рисование многоугольника.

 **Эллипс (E)** — рисование эллипса.

 **Соединённые линии (N)** — рисование соединённых линий.

 **Кривая (V)** — рисование кривых Безье.

 **Масштаб (Z)** — приближение и отдаление изображения для более детальной работы.

Общие параметры инструментов:

Для выбора размера ластика нажмите на один из квадратов. Можно выбрать один из квадратов с длиной стороны 2, 3, 5, 9, 17 и 29 пикселей.



Параметр выбора ширины линии доступен для инструментов: кривая, эллипс, линия, многоугольник, прямоугольник и скруглённый прямоугольник. Для выбора ширины линии щёлкните по одной из линий. Доступна ширина линии в 1, 2, 3, 5 и 8 пикселей.



Настройка стиля заливки доступна для инструментов: эллипс, многоугольник, прямоугольник и прямоугольник со скруглением. Для выбора стиля заливки щелкните по одному из прямоугольников. К выбору доступны варианты: без заливки, заливка цветом фона или заливка цветом переднего плана.



4. **Рабочая область** — область для редактирования изображений.

5 . **Цветовая палитра** — панель для настройки цвета и прозрачности изображения. Цветовая палитра разделена на три секции:

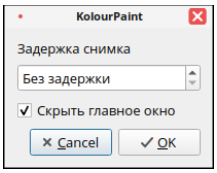
цветовая табличка, палитра и инструмент для настройки степени схожести цветов. Цветовая табличка показывает текущий основной цвет и цвет фона. При рисовании с использованием ЛКМ используется основной цвет, при использовании ПКМ — цвет фона. Чтобы поменять местами основной и фоновый цвета можно щёлкнуть по двунаправленной стрелке. Пирамида представляет прозрачный цвет.

6 . **Строка состояния** — это панель, расположенная внизу рабочей области, на которой отображаются подсказки по работе с инструментами. При выделении определённой области в строке состояния отобразятся размеры выделения.

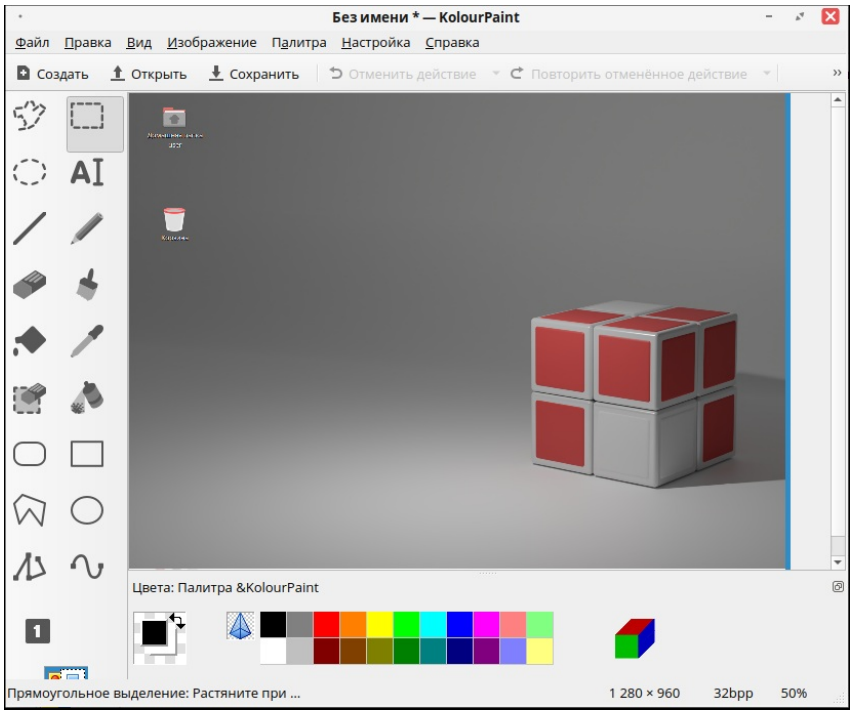
Скриншоты

Для сохранения понравившегося изображения, кадра из видеоролика, компьютерной игры или презентации можно использовать функцию создания скриншота. Для получения снимка экрана перейдите в меню «**Файл**» — «**Сделать снимок экрана**».

С помощью диалогового окна можно изменить задержку снимка экрана в секундах и скрыть главное окно во время создания снимка экрана. После выбора параметров нажмите «**OK**».



Сделанный снимок экрана будет помещён непосредственно в рабочую область **KolourPaint**.

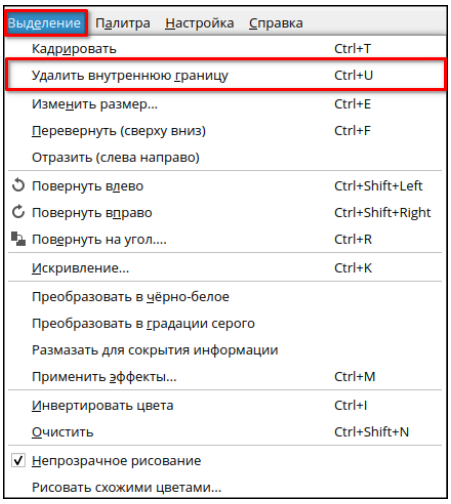


Эффекты изображения

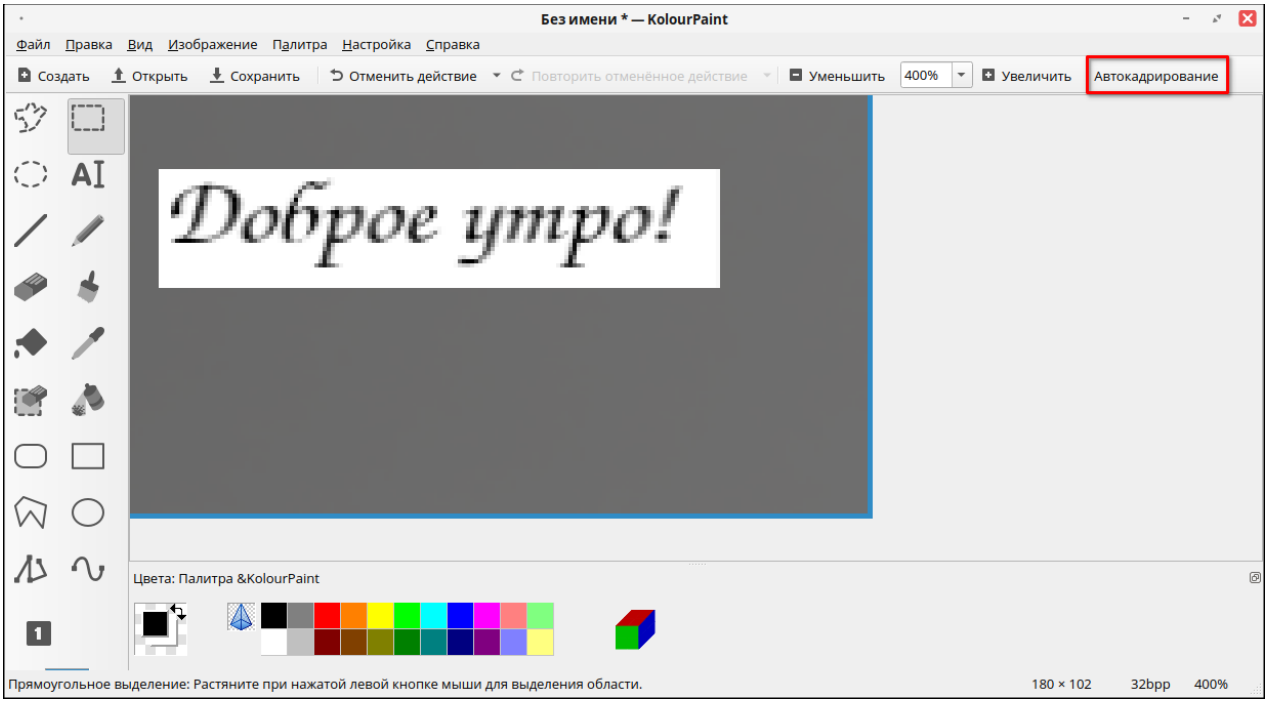
Эффекты в **KolourPaint** позволяют изменять внешний вид изображения различными способами.

Удаление внутренней границы / Автокадрирование

Инструмент **Удаление внутренней границы** предназначен для удаления тонкой границы вокруг выделенной области или фигуры. Для его использования перейдите в меню «**Выделение**» — «**Удалить внутреннюю границу**».

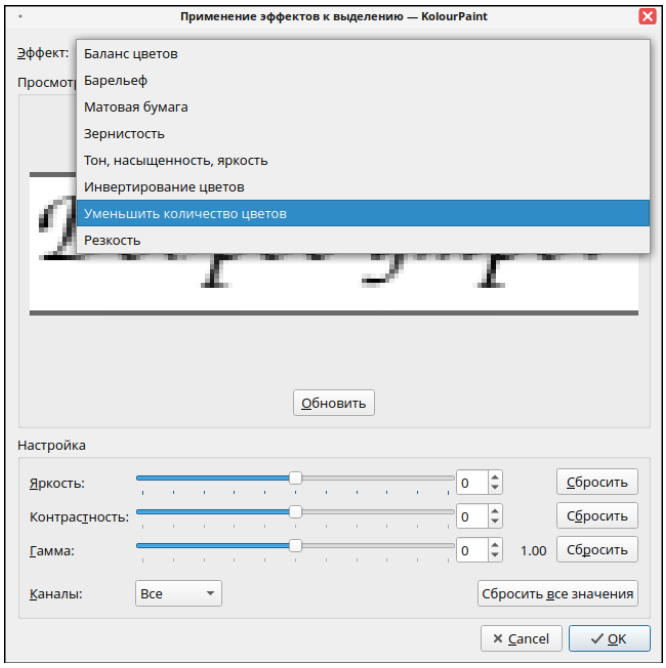


Автокадрирование удаляет прозрачные области вокруг изображения, обрезая его до минимальных размеров.



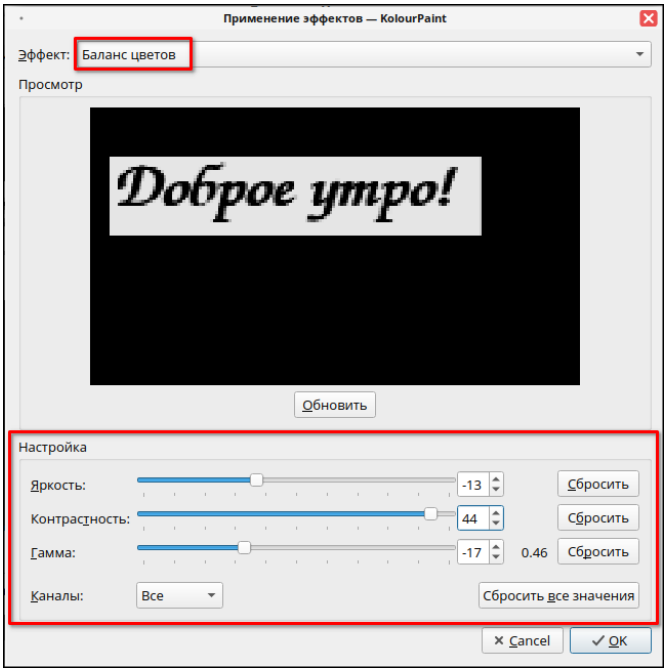
Дополнительные эффекты

Дополнительные эффекты можно выбрать в меню «**Выделение**» — «**Применить эффекты...**». Диалоговое окно содержит следующие инструменты:



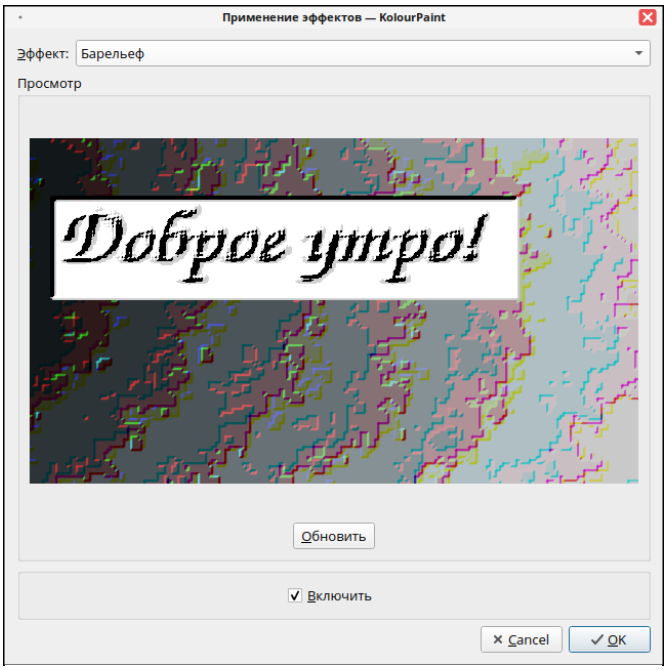
Баланс

Баланс корректирует уровни яркости и контрастности изображения, чтобы сделать его более равномерным. Инструмент позволяет изменить яркость, контраст и гамму всего изображения или выделенной области. Для изменения настроек баланса цветов используйте поля ввода числа и кнопки «**Сбросить**».



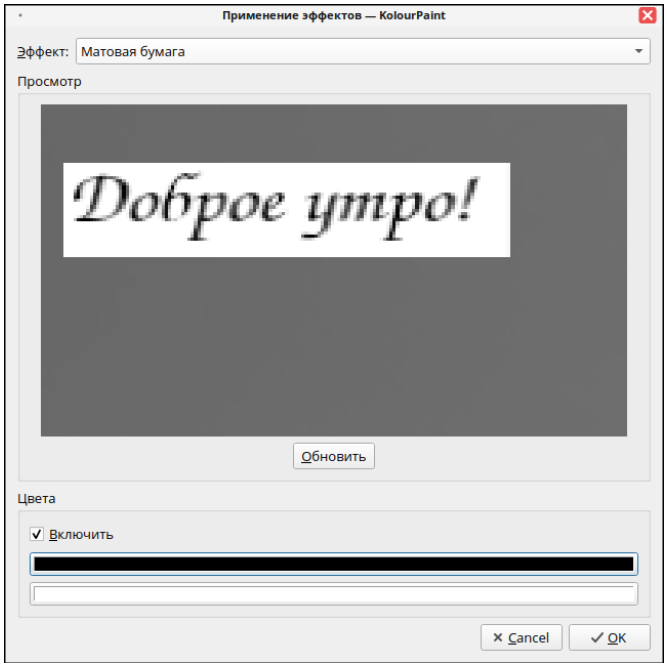
Барельеф

Барельеф создаёт эффект объёма на изображении, эффект гравюры. Для применения эффекта установите флаг рядом с параметром «**Включить**».



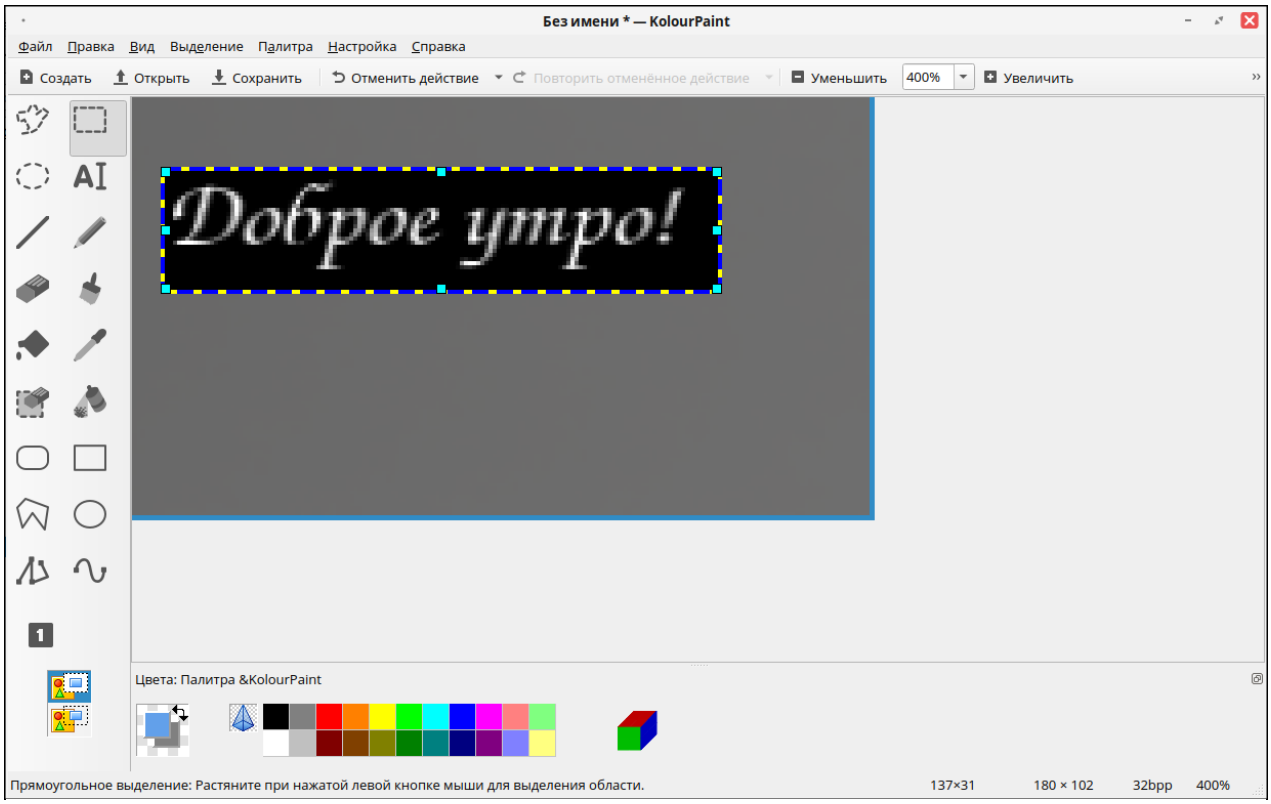
Матовая бумага

Матовая бумага создаёт эффект, как будто объект вдавлен в поверхность. Такие текстуры могут использоваться для фонов, создания объёмных объектов или для достижения определённого художественного стиля. Области, закрашенные выбранным цветом, будут перерисованы с заменой цвета на его градации. После выбранных параметров нажмите «OK».



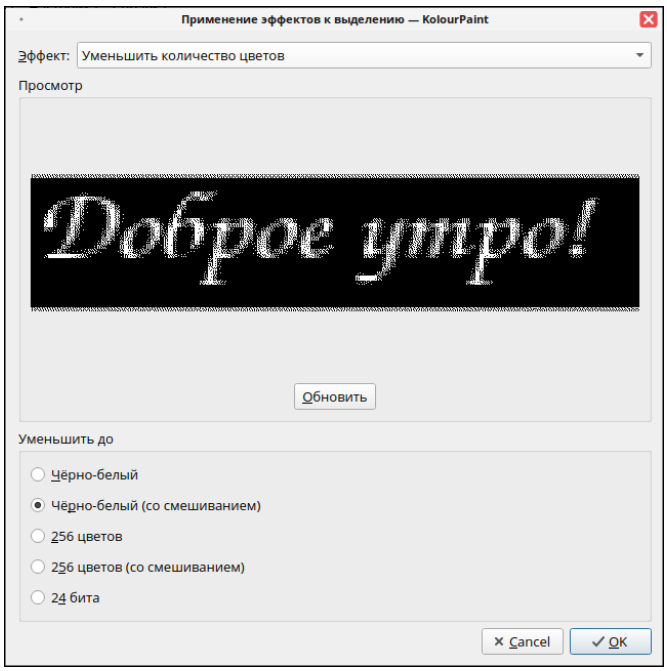
Инвертировать цвета

Инструмент инвертирует все цвета на изображении, делая их противоположными (например, чёрный становится белым, а белый становится чёрным).



Уменьшить количество цветов

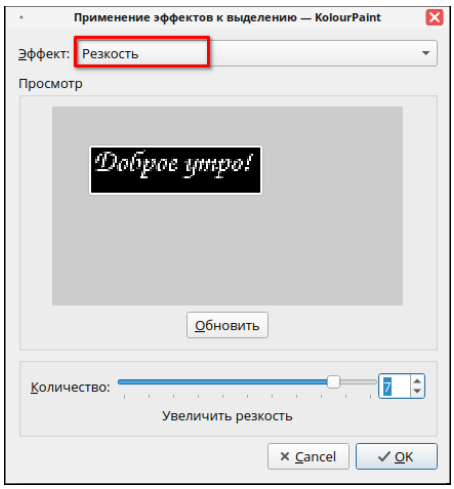
Уменьшает количество цветов во всем изображении или в выделенной области, со смешиванием или без него, что может придать ему эффект стилизации или сделать его более простым. Параметр доступен через меню «**Выделение**» — «**Применить эффекты...**».



Резкость

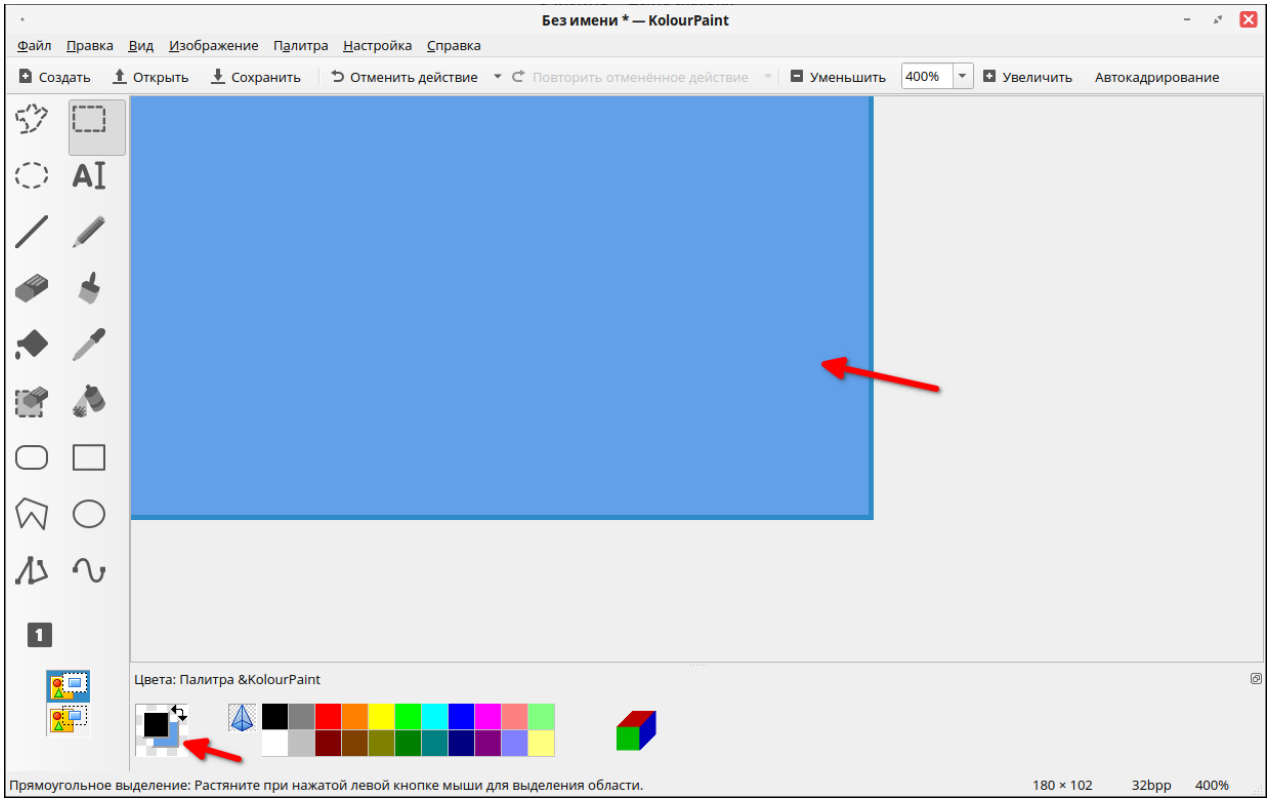
Параметр доступен через меню «**Выделение**» — «**Применить эффекты...**».

Увеличивает или уменьшает резкость изображения, делая его более чётким или размытым.



Очистить

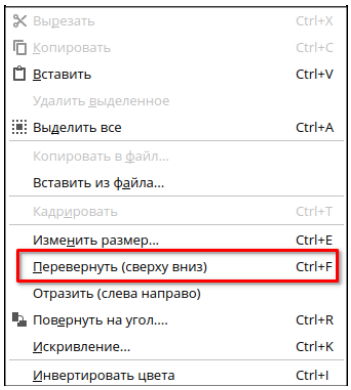
Заполняет всю область изображения цветом фона. Инструмент доступен в меню «**Изображение**» — «**Очистить**».



Для очистки всего изображения дважды щёлкните по инструменту  .

Перевернуть (сверху вниз)

Для переворота изображения сверху вниз щёлкните по нему ПКМ и в контекстном меню выберите «**Перевернуть (сверху вниз)**».



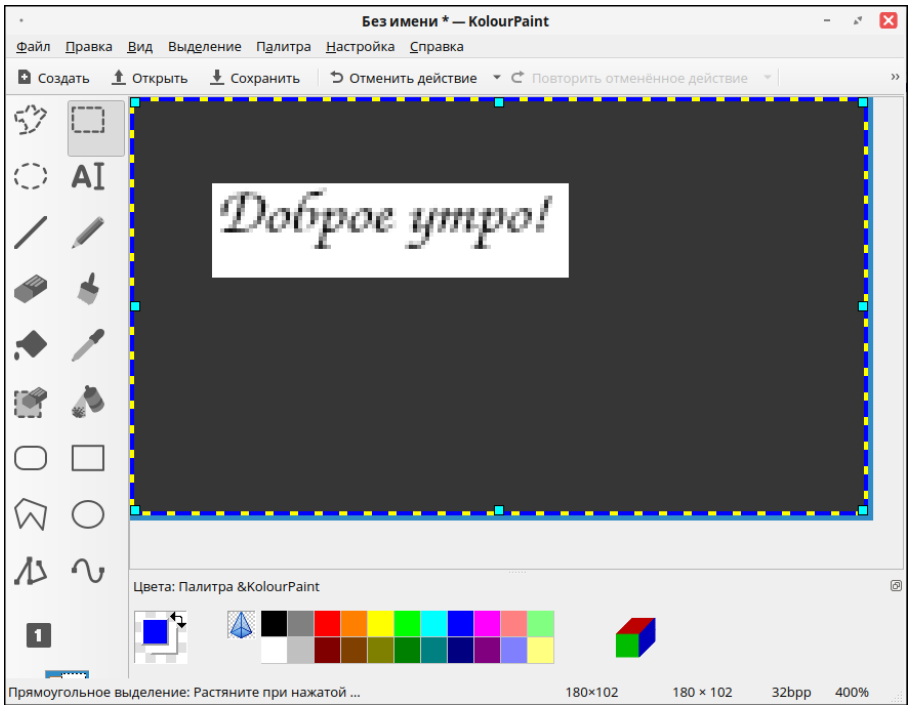
Данный эффект переворачивает всё изображение или выделенную область относительно горизонтальной оси.



Преобразовать в оттенки серого

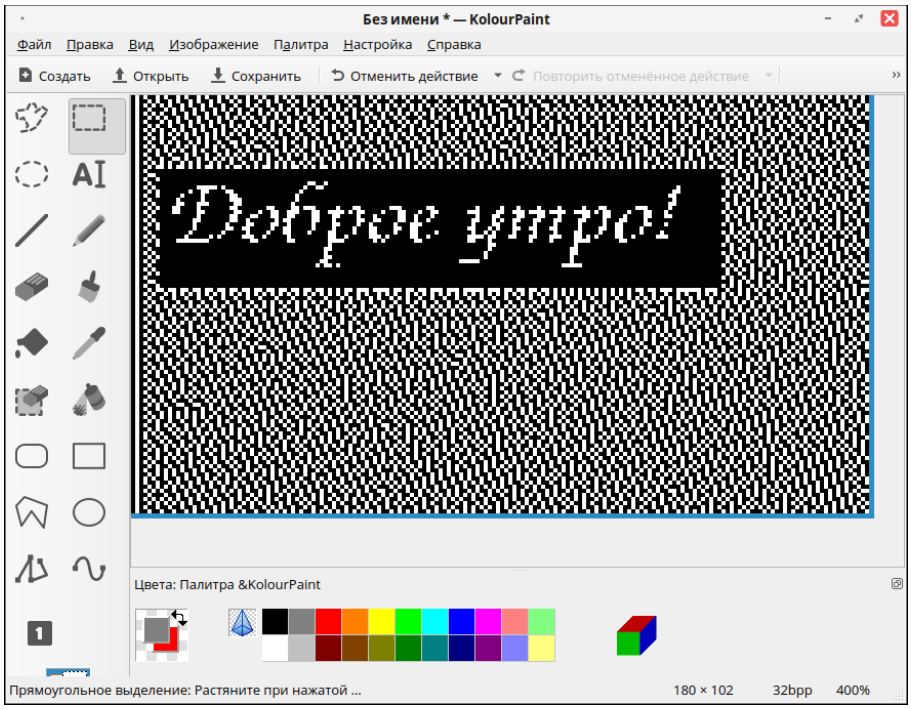
Преобразует изображение или выделенную область в оттенки серого, удаляя все цвета.

Параметр доступен через меню «**Выделение**» — «**Преобразовать в градации серого**».



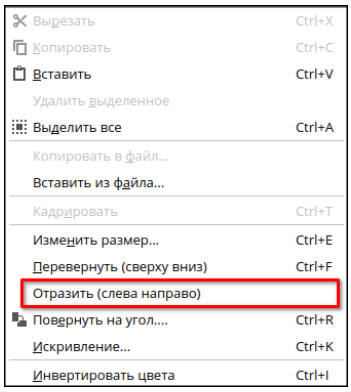
Сделать чёрно-белым (со смешиванием)

Преобразует изображение или выделенную область в черно-белое, но сохраняет некоторые детали, смешивая чёрный и белый цвета. Параметр доступен через меню «**Выделение**» — «**Преобразовать в черно-белое**».



Отразить (слева направо)

Отражает изображение горизонтально, меняя его сторону. Для отражения изображения щёлкните по нему ПКМ и в контекстном меню выберите «**Отразить (слева направо)**».

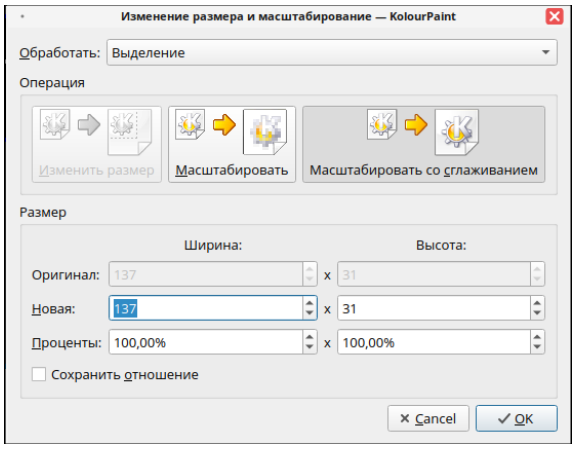


Изменить размер / Масштабировать

Параметр доступен через меню «**Выделение**» — «**Изменить размер...**». Изменяет размер изображения, делая его больше или меньше. Размеры изображения могут быть увеличены, но при этом не вносятся никаких фактических изменений.

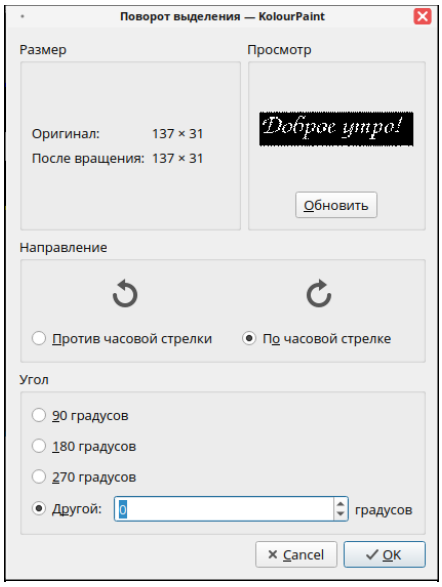
При использовании команды «**Масштабировать со сглаживанием**» происходит смешивание соседних цветов.

Можно установить новый размер в пикселях или в процентах от исходного значения. Включив опцию «**Сохранить отношение**», ширина и высота будут изменяться в одинаковых пропорциях. Обычное масштабирование возможно только для выделенных областей, текстовые области можно изменять только по размеру.



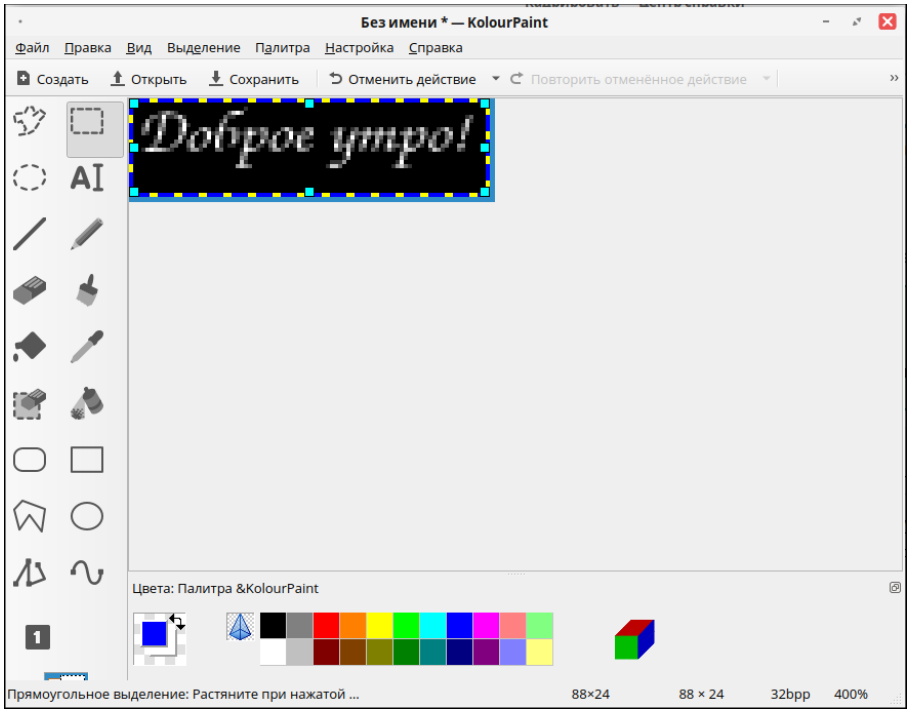
Поворот выделения

Поворачивает выделенную область на определённый угол в указанном направлении.



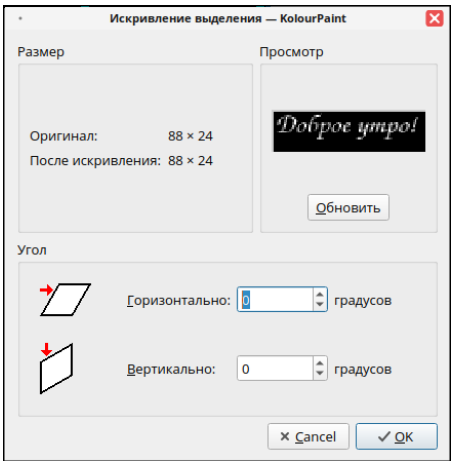
Кадрировать

Обрезает края выделенной области изображения для получения нужного размера или соотношения сторон. Задайте выделенную область и перейдите в меню «**Выделение**» — «**Кадрировать**».



Искривление

Параметр доступен через меню «**Выделение**» — «**Искривление...**». Искажает все изображение или выделенную область, деформируя его в определённых направлениях по горизонтали и/или вертикали.



Пример работы

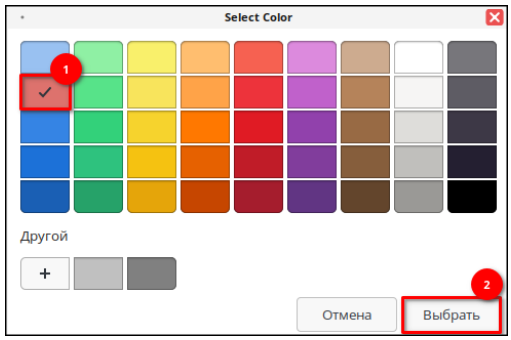
Для создание простого рисунка выполните следующий алгоритм действий:

1. Выберите  на панели инструментов.

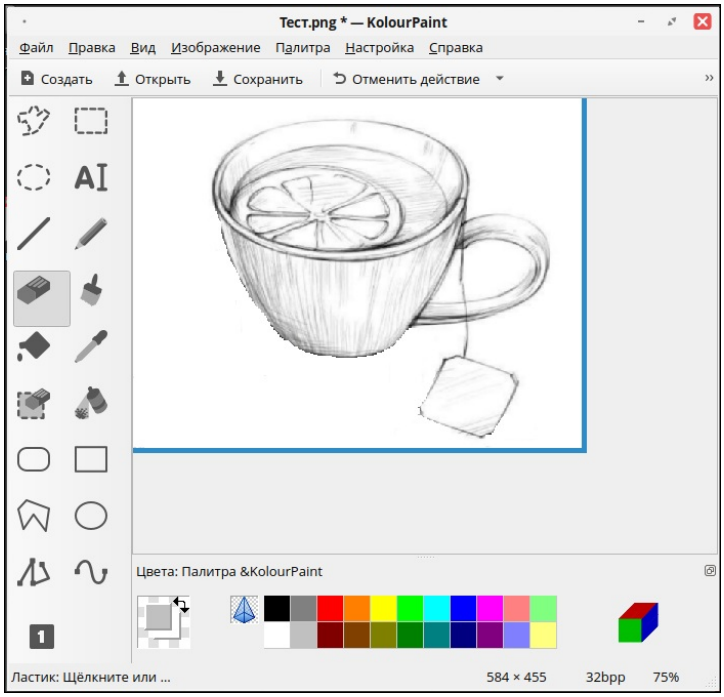
2. На палитре цветов выберите нужный основной цвет и цвет фона. Левый квадрат представляет **основной цвет** (цвет переднего плана), а правый квадрат представляет **цвет фона** (цвет заднего плана).



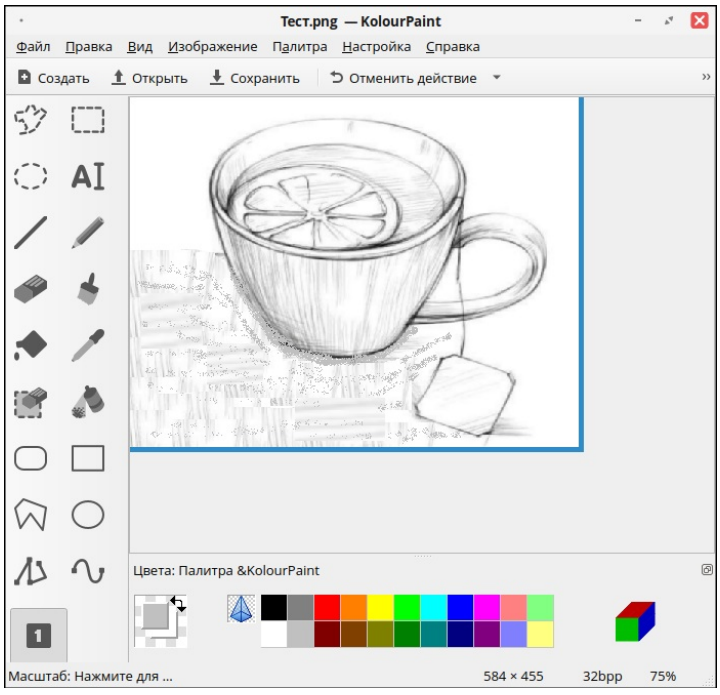
Для выбора **основного цвета** выберите его на палитре. Для выбора **цвета фона** кликните дважды на правый квадрат. После клика на правый квадрат откроется диалоговое окно «**Выбор цвета**». В этом окне можно выбрать цвет фона.



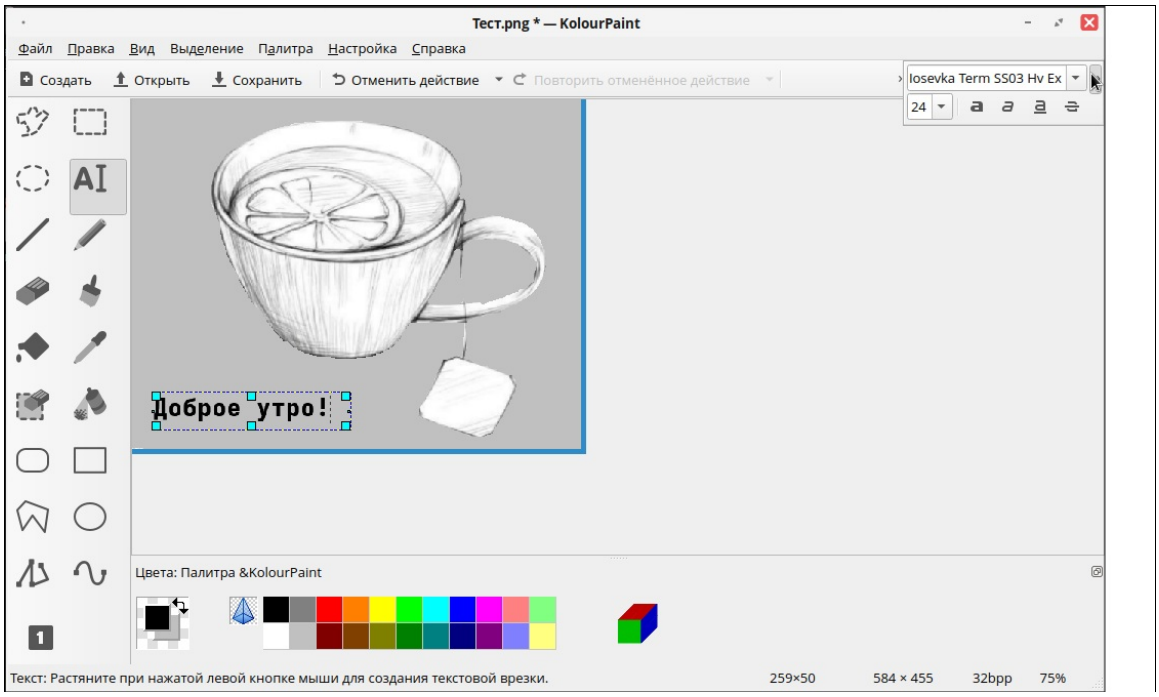
3. В рабочей области нарисуйте линию или фигуру, используя выбранную кисть и цвет.



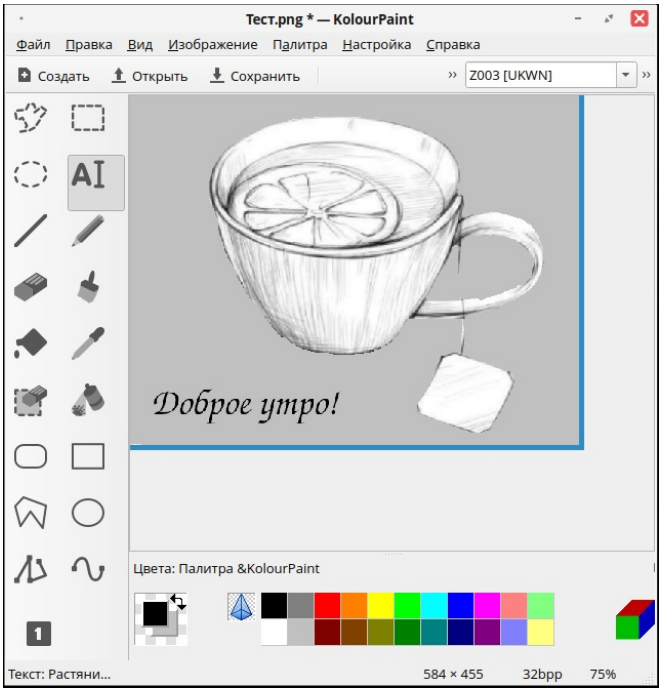
4. Выберите на панели инструментов. На палитре цветов выберите цвет, которым хотите заполнить область. В рабочей области кликните на область, которую хотите заполнить выбранным цветом. Закрашиваемая область должна иметь сплошной контур, иначе краска заполнит остальные части рисунка. Для отмены неправильного закрашивания нажмите **CTRL+Z**, исправьте контур и закрасьте снова нужную область.



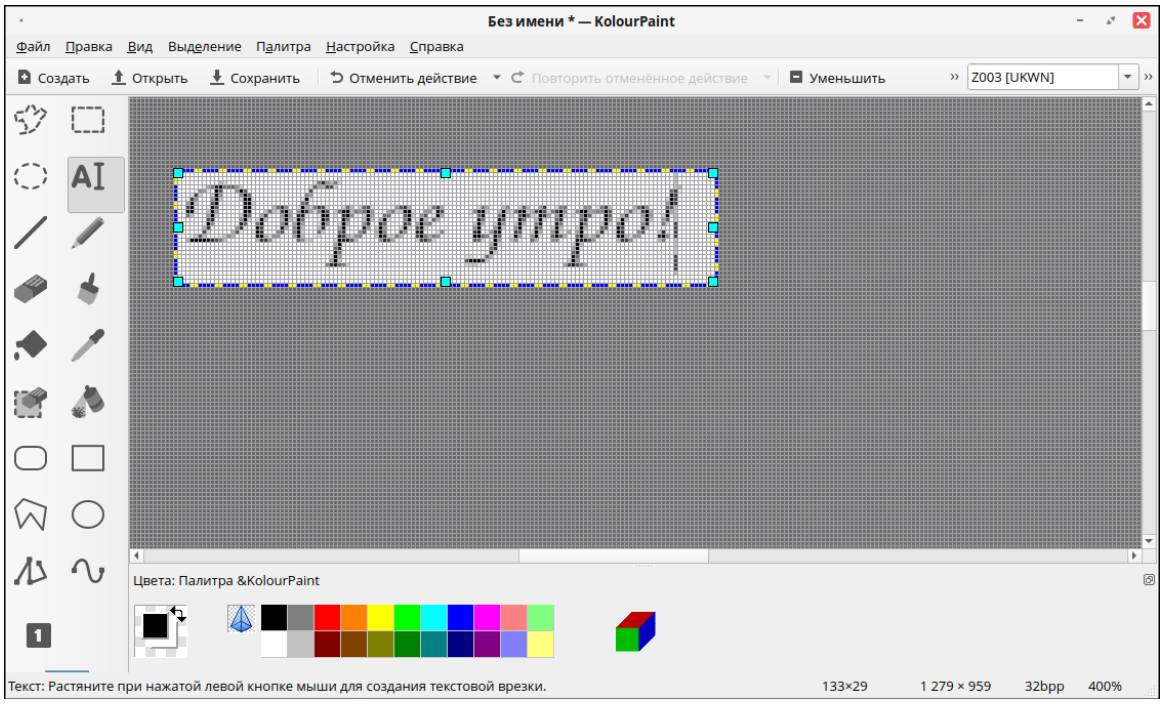
5. Для добавления текста к изображению на панели инструментов выберите инструмент AI. В рабочей области кликните в выбранном месте для размещения текста, протяните рамку, внутри которой будет расположен текст, и введите его.



Выберите шрифт и размер текста.



Для точного редактирования каждого пиксела при масштабе в 400% или большем (кратным 100%) можно использовать режим «**Показать сетку**», расположенном в меню «**Вид**».


Без имени * — KolourPaint
Файл Правка Вид Выделение Палитра Настройка Справка
Создать Открыть Сохранить Отменить действие Повторить отменённое действие Уменьшить
Z003 [UKWN]
Доброе утро!
Цвета: Палитра &KolourPaint
Текст: Растяните при нажатой левой кнопке мыши для создания текстовой врезки.
133×29
1 279 × 959
32bpp
400%

IrfanView — программа для работы с графическими файлами

Установка IrfanView
Запуск установщика с использованием терминала
Запуск установщика с использованием графического интерфейса
Обзор установки IrfanView
Установка плагинов для IrfanView
Запуск установщика плагинов с использованием терминала
Запуск установщика плагинов с использованием графического интерфейса
О программе
Печать документов через IrfanView

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: iview4.67

IrfanView — небольшая по размеру программа для просмотра/воспроизведения графических, видео- и аудиофайлов, поддерживает большое количество форматов, в том числе **BMP**, **HDR**, **JPEG**, **PNG**, **EXE**, **DLL**, **MPEG** и **PSD**. Отлично подходит для печати документов формата **TIF**.

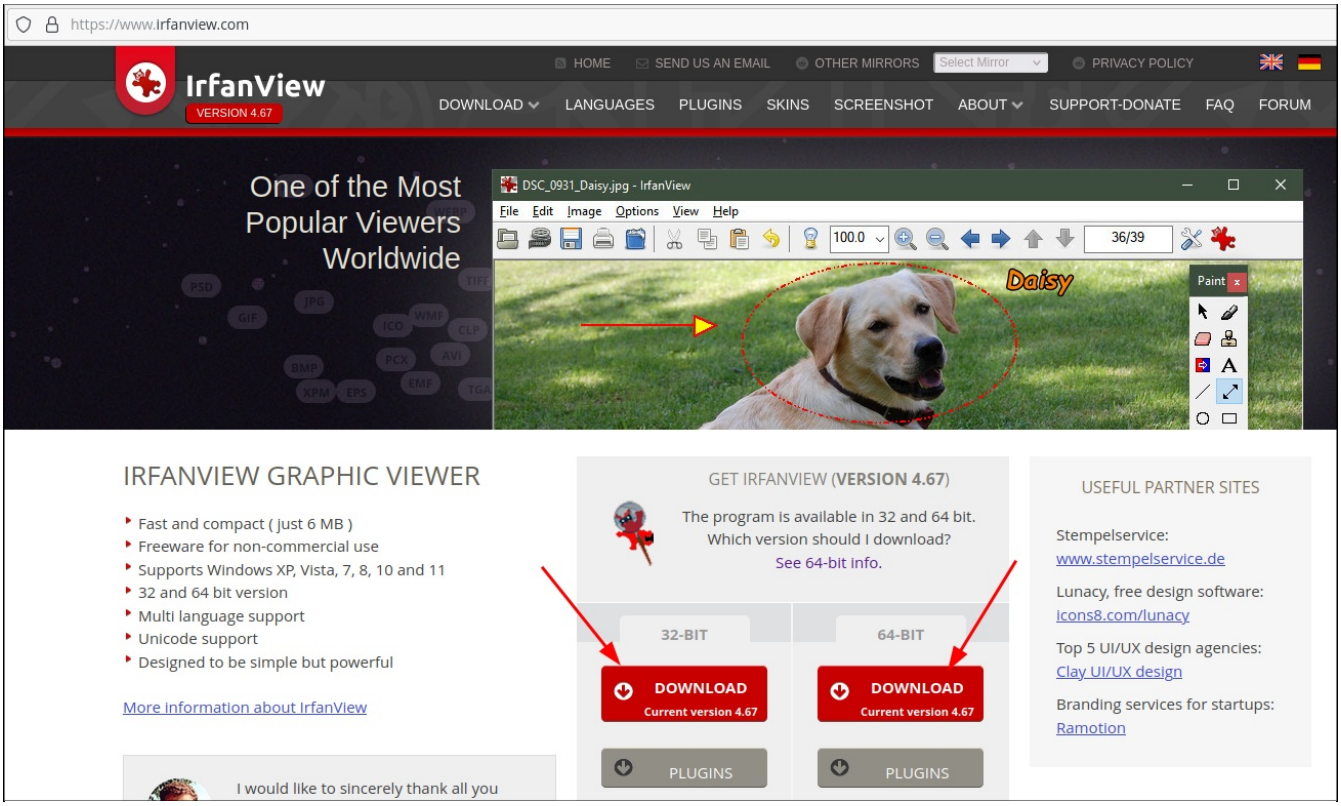
Примечание.

Для следующих этапов установки **IrfanView** потребуется **Wine**. С установкой и настройкой **Wine** можно ознакомиться в наших инструкциях «Работа с Wine».

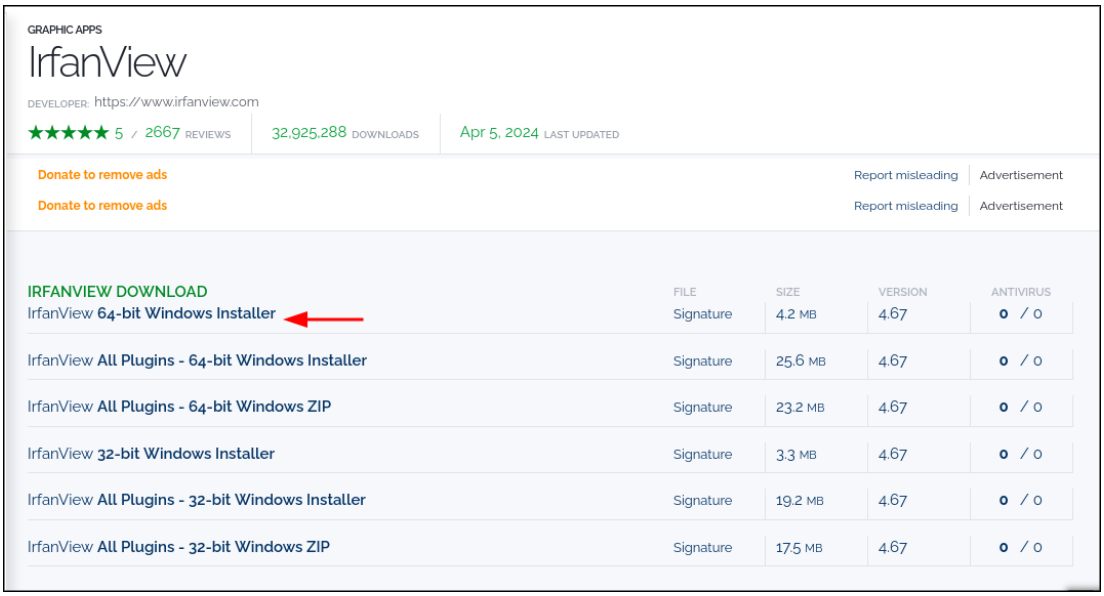
Установка IrfanView

Для загрузки установщика программы перейдите на официальный сайт **IrfanView** в раздел «**Download**» - «**Irfanview**» (предлагаются 32-битные и 64-битные версии программы **IrfanView**).

Откроется страница с установочными архивами и плагинами.



Скачайте установщик **IrfanView**.



После этого установите программу через **Wine**, используя терминал или графический интерфейс.

Запуск установщика с использованием терминала

Перейдите в каталог со скачанным файлом (в примере **/home/user/Загрузки/**):

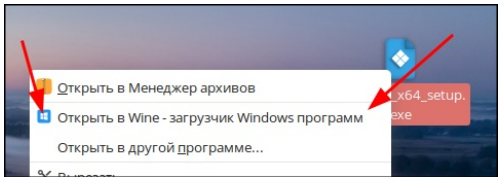
```
cd /home/user/Загрузки/
```

Выполните команду установки:

```
wine ./<название_файла>
```

Запуск установщика с использованием графического интерфейса

Вызовите контекстное меню, нажав ПКМ по файлу установщика, и выберите пункт «*Открыть в Wine — загрузчик Windows программ*».

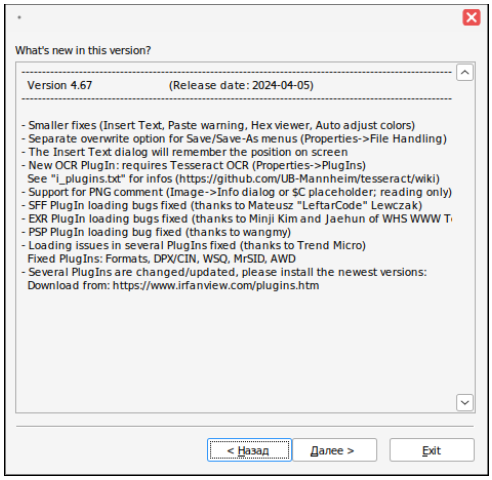


Обзор установки IrfanView

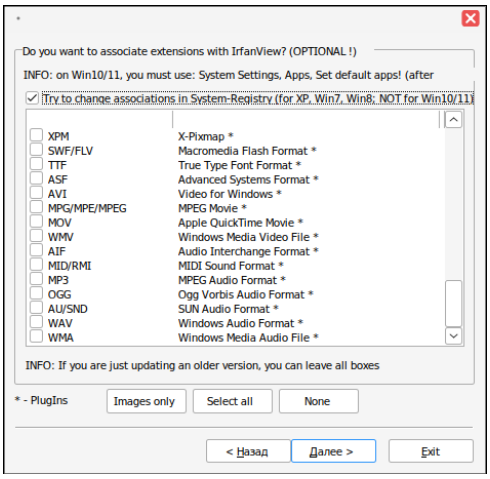
Запустите инсталлятор «**IrfanView -bit setup**». Определите необходимость создания ярлыков приложения. Для выбора каталога установки, отличного от каталога по умолчанию, нажмите «**Browse**» и определите свой каталог установки. Для продолжения нажмите «**Далее**».



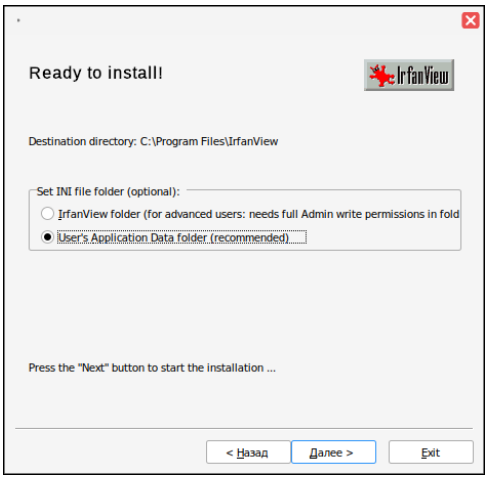
Ознакомьтесь с новыми возможностями данной версии и нажмите «**Далее**».



Выберите расширения файлов, которые по умолчанию будут открываться в **IrfanView** (по желанию).



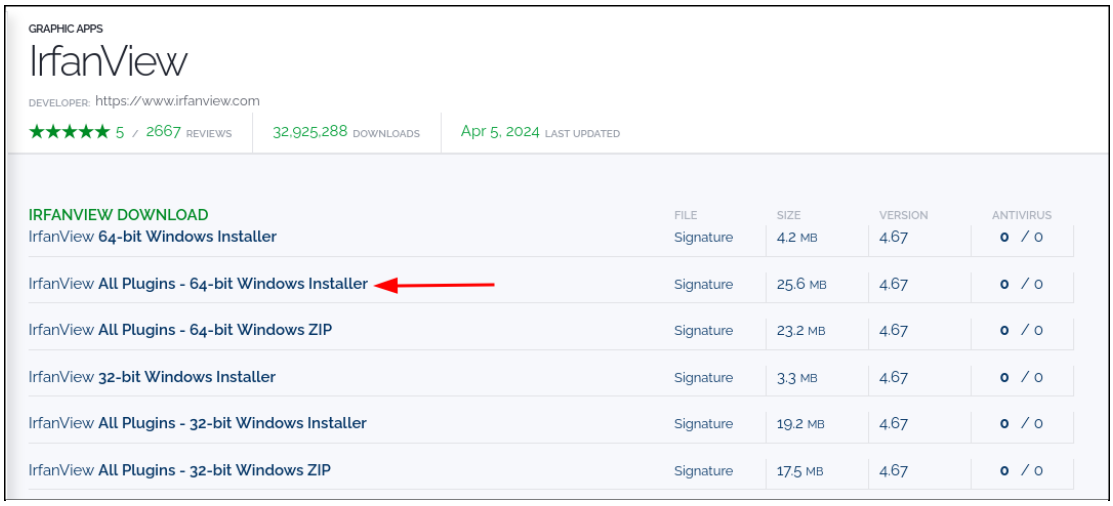
В следующем окне оставьте рекомендуемые настройки по умолчанию и нажмите «**Далее**».



При успешном завершении установки появится соответствующее сообщение. После установки программа будет доступна из «**Главного меню**» - «**Wine**» - «**IrfanView**».

Установка плагинов для IrfanView

Для расширения функционала программы можно установить дополнительные плагины. Они находятся на официальном сайте **IrfanView** в разделе «**Download**» - «**Irfanview**».



Запуск установки производится точно таким же способом, как и установка самой программы - через **терминал** либо **графическим способом** с открытием через **Wine**.

Запуск установщика плагинов с использованием терминала

Перейдите в каталог со скаченным файлом (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
```

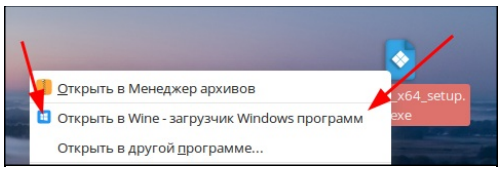
Выполните команду установки:

```
wine ./<название_файла>
```

При установке должен быть указан путь к каталогу, в который была установлена сама программа **IrfanView**.

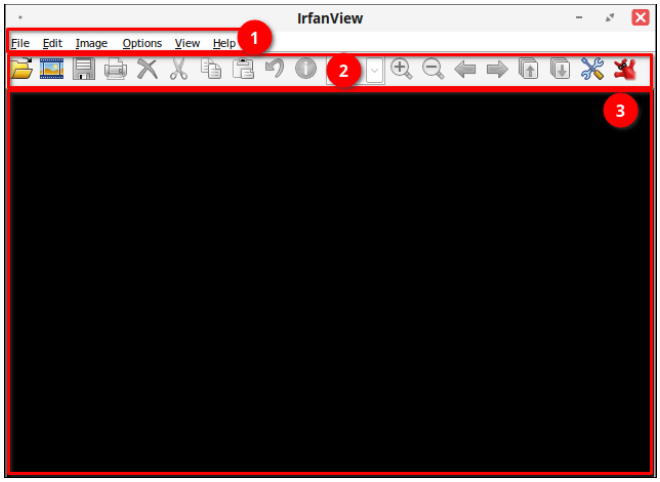
Запуск установщика плагинов с использованием графического интерфейса

Вызовите контекстное меню, нажав ПКМ по файлу установщика, и выберите пункт «*Открыть в Wine – загрузчик Windows программ*».



О программе

Главное окно программы выглядит следующим образом:



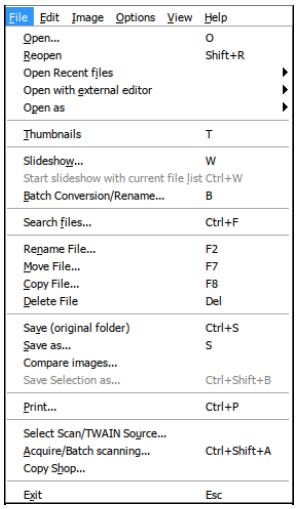
В верхней части окна расположено **основное меню** (1), где доступны все действия для работы и настройки программы.

Ниже расположена панель инструментов (2), с помощью которой доступны инструменты для работы с файлом.

Основную часть окна занимает рабочая область (3), на которой располагаются открытые файлы.

В основном меню представлены основные возможности программы.

Меню «**File**» («**Файл**») отвечает за работу с файлом, например, открытие, сохранение, удаление, печать, переименование и прочее.



Пункт «**Print**» отвечает за печать открытого файла с настройками масштабирования, выбор количества листов для печати и другие параметры. Также программа позволяет отсканировать файл и напечатать его.

С помощью «**Slideshow**» можно настроить слайд-шоу.

1. Инструмент «**Настройки слайдов**» отвечает за периодичность переключения изображений. Активация переключения происходит по щелчку ЛКМ или автоматически. Кнопка «**Play slideshow**» определяет начало показа слайд-шоу, а «**Cancel**» - выход из меню настроек.

2. В разделе «**Опции слайд-шоу**» можно скрыть курсор мыши, включить повторное воспроизведение аудиофайла, определить, с какого файла начинать показ, настроить отображение текста.

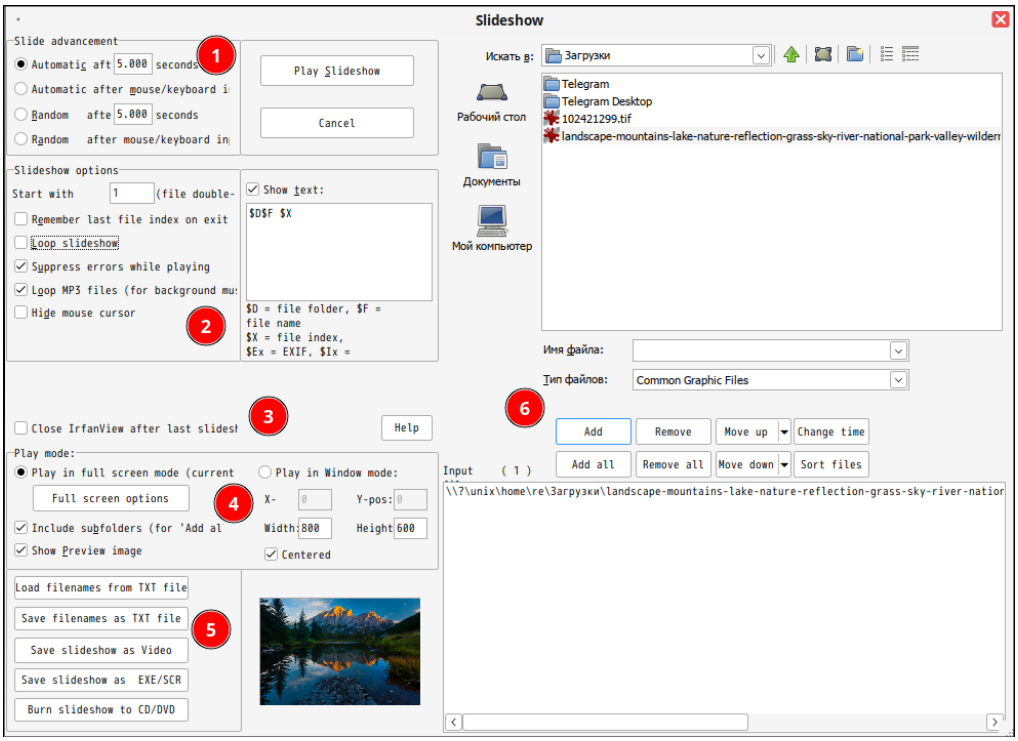
3. В чекбоксе «**Close IrfanView after last slidest**» доступна возможность настройки выхода из режима слайд-шоу после показа последнего файла.

4. В разделе «**Режим воспроизведения**» можно изменить настройки режима показа слайд-шоу - *полноэкранный режим* или *режим*

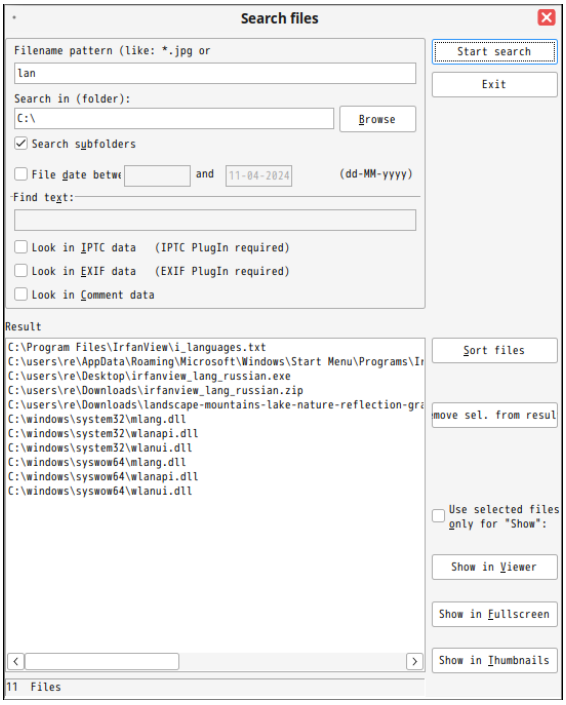
окна, а так же масштаб оконного режима.

5. Слайд-шоу можно сохранить в видеофайл в форматах **EXE/SCR** или записать на CD/DVD/BD-диски.

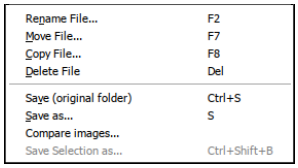
6. В правой части окна доступен поиск файлов, которые будут использоваться в слайд-шоу. Можно добавить все сразу при помощи кнопки «**Add all**» или выбрать вручную с помощью «**Add**». Также файлы можно убирать вручную и автоматически, если они не нужны в показе.



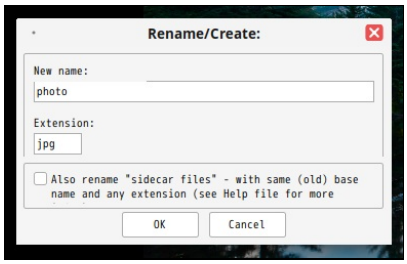
В пункте«**Search Files**» можно найти необходимый файл по названию или по его расширению.



Далее приведены пункты, которые отвечают за ряд дополнительных функций в этом редакторе.



1. **Rename File** — переименование файла и изменение расширения.



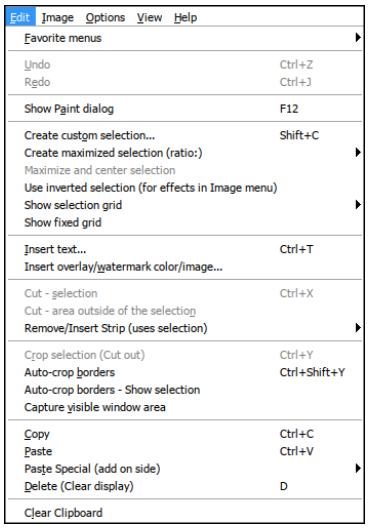
2. **Move** — перемещение файла.

3. **Copy** — копирование файла.

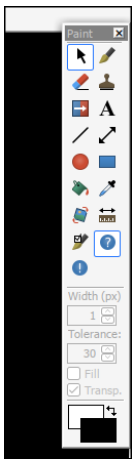
4. **Delete** — удаление файла.

5. «**Save**» и «**Save as...**» — сохранение файла. «**Save**» отвечает за сохранение текущего файла в текущей папке, из которой он был открыт. «**Save as...**» позволяет выбрать каталог для сохранения.

Меню «**Edit**» («**Правка**») отвечает за редактирование изображений.

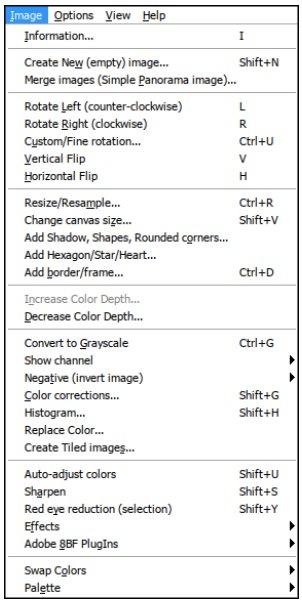


Show Paint dailog открывает диалоговое окно с различными инструментами для рисования.



Также в этом пункте настраивается выделение, кадрирование фотографий, копирование и вставка отдельных элементов, добавление на фотографию текста или водяного знака, очистка рабочей области.

В меню «**Image**» («**Изображение**») производится настройка рабочей области, изменение размера холста и изображения, поворот влево и вправо на 90 градусов, поворот вертикально и горизонтально, добавление рамок и виньеток на изображение.

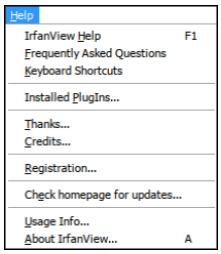


Также можно настроить цвета автокоррекцией или вручную, заменить цвет, повысить резкость, убрать красные глаза на фотографии, добавить эффекты и фильтры, инвертировать цвета на фотографии.

В меню «**Options**» («**Опции**») можно, по желанию, изменить язык самой программы, отправить файл по почте, сделать снимок экрана, изменить дату и время съемки фотографии.

В меню «**View**» («**Вид**») производятся настройки отображения, строк состояния, панелей инструментов, меню, а также настройка полноэкранного или оконного режима, приближения и отдаления фотографий.

В меню «**Help**» («**Справка**») можно посмотреть различные клавиатурные команды, ответы на вопросы, проверить наличие обновлений, просмотреть, установленные плагины и версию программы.



Панель инструментов обеспечивает быстрый доступ к основным возможностям программы.



1. Открыть файл.

2. Запустить слайд-шоу.

3. Сохранить файл.

4. Печать.

5. Удалить файл.

6. Вырезать выделенное.

7. Скопировать выделенное.

8. Вставить выделенное.

9. Отменить последнее действие.

10. Просмотреть сведения о файле.

11. Задать масштаб изображения.

12. Приблизить изображение.

13. Отдалить изображение.

14. Предыдущий файл в списке.

15. Следующий файл в списке.

16. Предыдущая страница.

17. Следующая страница.

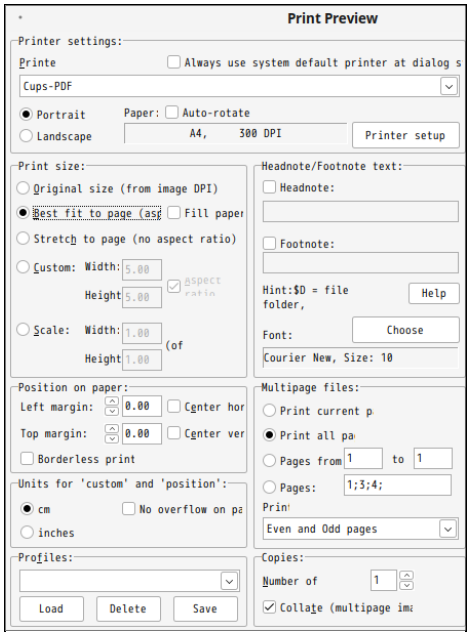
18. Настройка программы.

19. О программе.

Печать документов через IrfanView

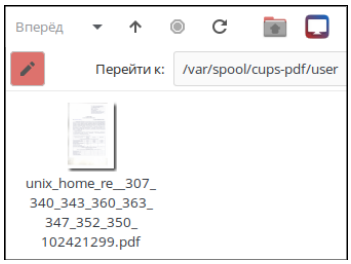
IrfanView можно использовать для печати файлов. Для этого необходимо открыть нужный файл и нажать **Print**.

Далее в выпадающем меню выбрать необходимые настройки для печати, например, распечатать текущий лист или весь файл, выбрать необходимый масштаб на странице и прочее. Принтер можно выбрать по умолчанию или установить его вручную.



В примере используется виртуальный принтер **CUPS-PDF** для демонстрации печати.

По умолчанию файлы, распечатанные виртуальным принтером, находятся в каталоге **/var/spool/cups-pdf/<имя_пользователя>**.



Scribus — программа для вёрстки страниц

Основные возможности программы
Установка
Запуск
Описание программы
Пример работы
Создание листовки
Экспорт файла

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: scribus-1.5.6.1 scribus-1.5.8-7

Scribus — это программа для профессионального дизайна и вёрстки страниц. Она предлагает поддержку большинства текстовых и графических форматов, включая **SVG**, шрифты **TrueType** и **OpenType**, **CMYK**, высокоуровневый экспорт в **PDF**. С помощью **Scribus** можно создавать различные типы визитных карточек, брошюр, информационных бюллетеней, журналов, каталогов и других документов. Программа обладает широкими возможностями по настройке дизайна страницы и форматированию текста.

Основные возможности программы

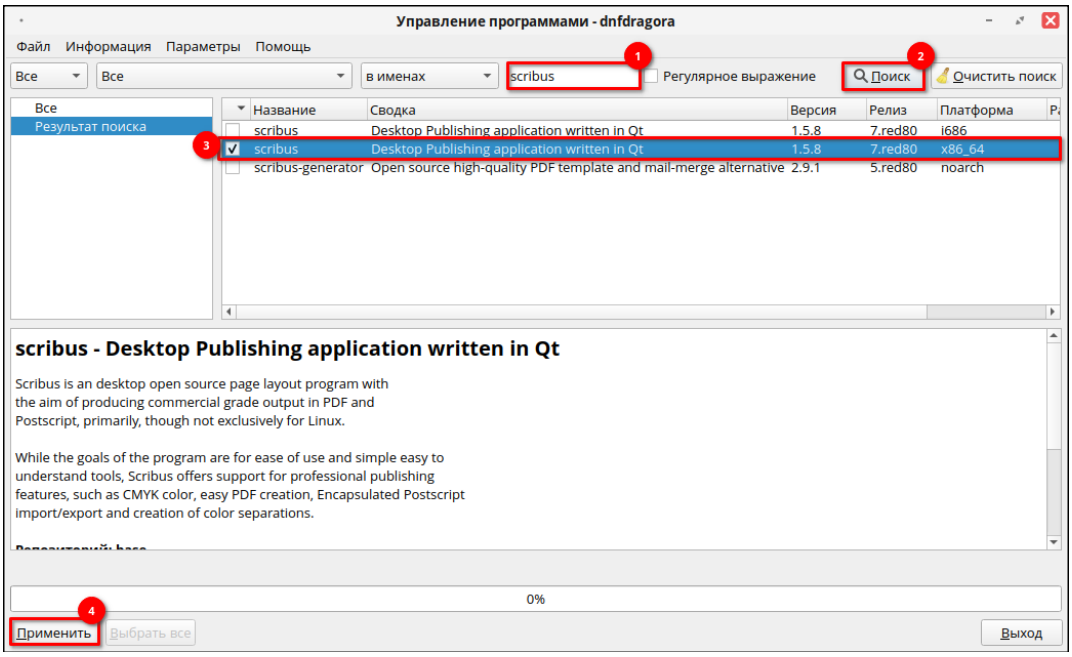
Основными возможностями **Scribus** являются:

- настройка полей и направляющих;
- предустановленные профили для различных типов печатных изданий;
- поддержка разнообразных размеров и форматов бумаги;
- векторные инструменты, включая **кривые Безье** и примитивы;
- вставка и базовая обработка изображений;
- импорт и экспорт векторной графики в формате **SVG**;
- полная поддержка **Unicode**, включая специальные символы и различные направления текста;
- возможность создания текстовых блоков различной формы и их трансформация;
- обтекание текстом других объектов и линковка текстовых блоков;
- настройка шрифтов, кернинга, интерлиньяжа и других параметров текста;
- создание и применение предустановленных стилей текста;
- поддержка множества графических форматов и совместимость с **PDF 1.4**;
- возможность создания интерактивных **PDF**, включая формы и **JavaScript**-сценарии;
- поддержка цветовых профилей **CMYK** и **RGB**;
- интуитивно понятный интерфейс с возможностью настройки горячих клавиш;
- функция черновика для удобства работы с элементами документа.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**scribus**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install scribus
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

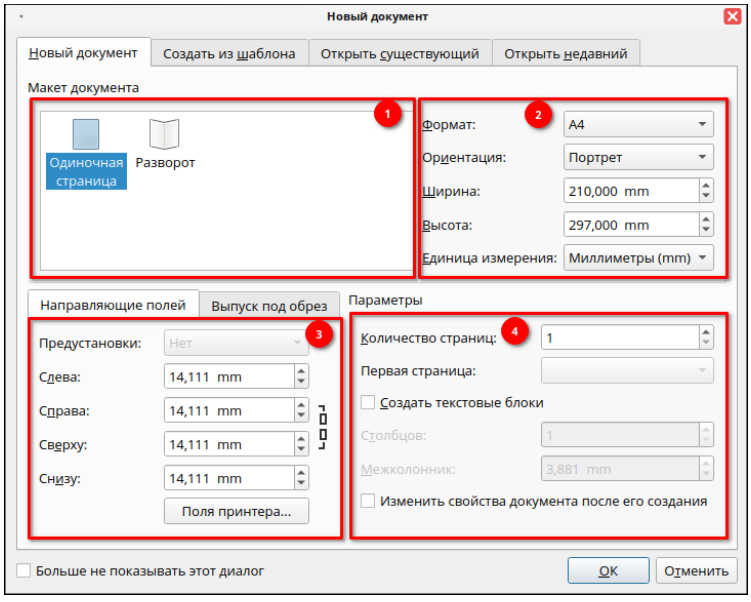
Запуск

Запустить программу можно либо в графическом режиме, либо через терминал. После установки программа будет доступна из «**Главного меню**» — «**Графика**» — «**Издательская система Scribus**» или «**Scribus**». Запустить программу через терминал можно, введя команду:

```
scribus
```

Описание программы

При запуске **Scribus** появляется окно настроек нового документа.



Окно **Новый документ** состоит из следующих областей:

1. В области **Макет документа** производится выбор типа документа.

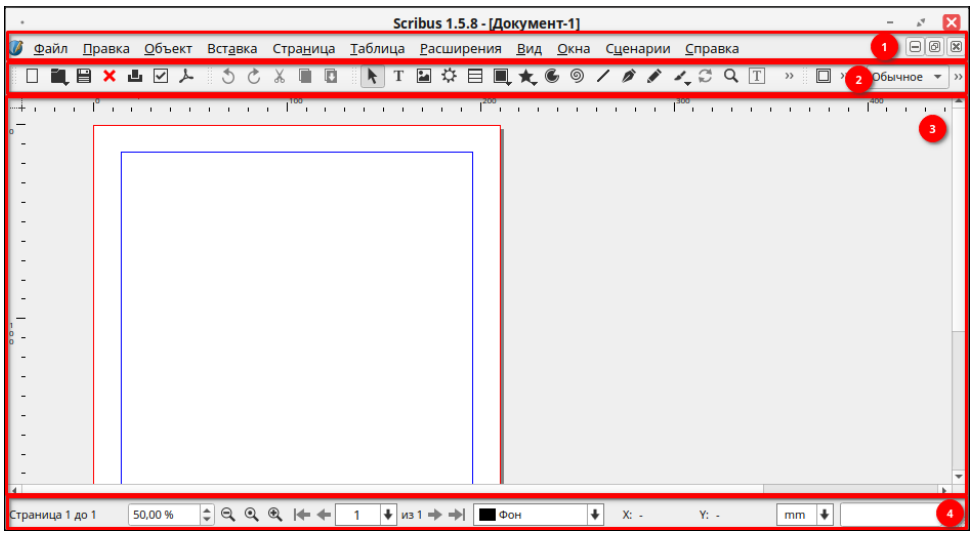
2. В области **Формат страницы** производится выбор размера документа (обычно формат A4), ориентации (по умолчанию Портрет).

После выбора определённого формата в полях «*Ширина*» и «*Высота*» будут автоматически установлены соответствующие размеры, которые можно изменить.

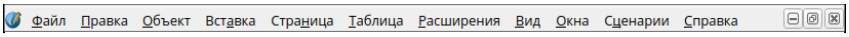
3. В области **Направляющие полей** можно установить отступы для документа, выбрав предпочтительные единицы измерения.

4. В области **Параметры** доступна настройка страниц нового документа и создание необходимого количества текстовых блоков.

Интерфейс программы стандартный и состоит из нескольких типовых частей.



1. **Основное меню** — позволяет выполнять различные действия с создаваемым документом, а также настраивать программу.



В основном меню доступны такие действия, как:

- операции с файлами;
- команды общего редактирования документа;
- команды работы с графическими объектами;
- вставка текстовых блоков, изображений, фигур, символов, линий;
- работа с макетом публикации;
- просмотр публикации и вывод служебных элементов;
- применение сценариев;
- управление окнами документов;
- описание программы и помощь по её использованию.

2. **Панель инструментов** — стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы. Эти панели можно скрывать и отображать через основное меню. По умолчанию отображаются следующие панели инструментов:

- *Панель Файл* — собраны функции для работы с файлами, такие как создание, открытие, сохранение и печать документов.



- *Панель Правка* содержит инструменты для редактирования текста и объектов в документе, включая копирование, вставку элементов, отмену действий.



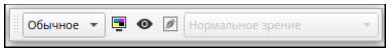
- *Панель Инструменты* предлагает различные функции для настройки документа, например, выбор объекта, добавление изображения, добавление таблицы, добавление фигуры, многоугольника, кривой Безье, блоков или линий, изменение масштаба.



- *Панель PDF-инструменты* включает опции для работы с PDF-файлами, содержит инструменты создания форм, вставки текстовой и ссылочной аннотации.



- *Панель Инструменты просмотра* позволяет переключаться между режимами просмотра и выбрать качество показа изображений в документе.



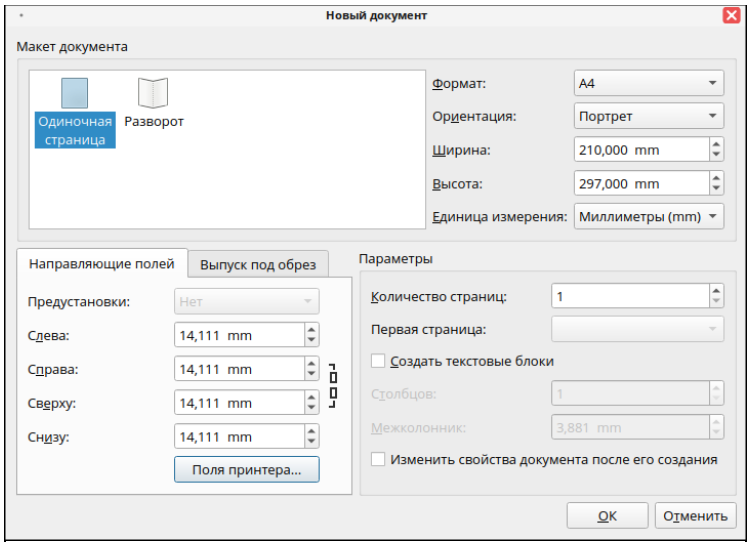
3. **Основное рабочее поле**. В данном поле происходит весь процесс вёрстки документа.

4 . **Панель состояния**. Здесь отображаются опции и действия, которые относятся к выбранному в данный момент инструменту. Инструменты можно выбирать через панель инструментов.

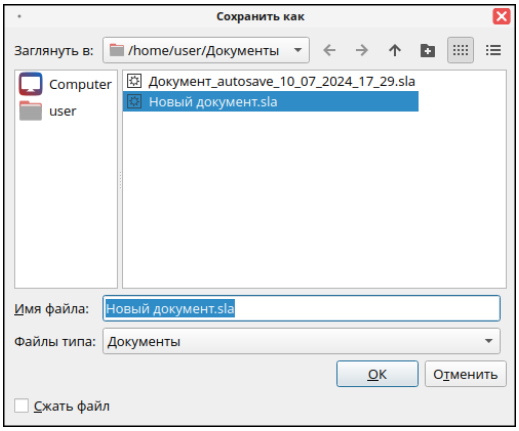
Пример работы

Создание листовки

1. Для создания нового документа в формате A4 с односторонним оформлением страницы перейдите в меню «**Файл**» — «**Создать...**» или кликните по значку на панели инструментов ( ). После выбора параметров нажмите «**OK**».

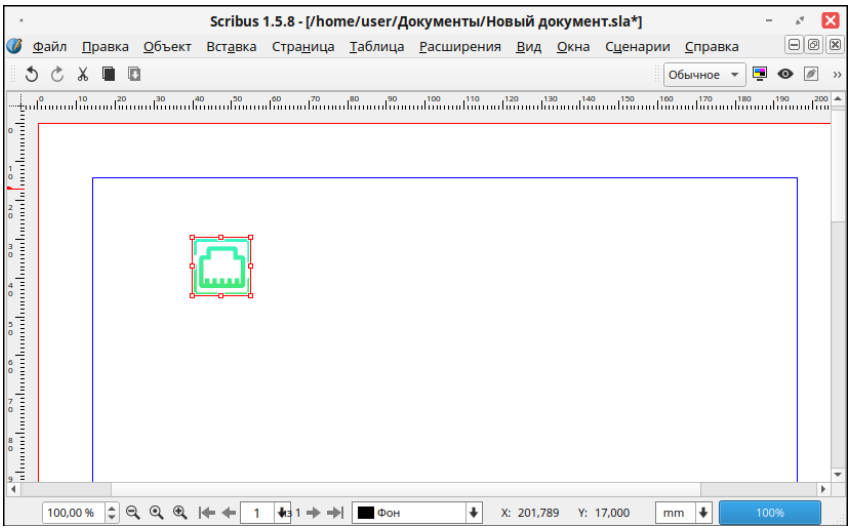


2. Для сохранения документа перейдите в меню «**Файл**» — «**Сохранить как...**». В открывшемся окне выберите папку для сохранения документа. В поле «**Имя файла**» введите желаемое название документа. Выберите формат файла. После выбора параметров нажмите «**OK**».

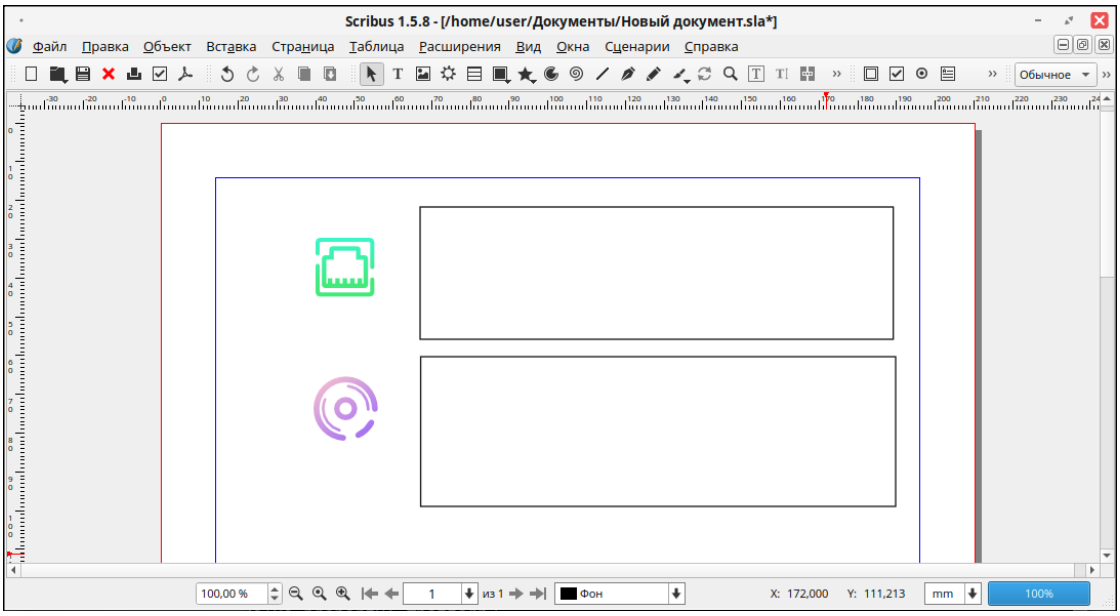


3. Скачайте из интернета или сохраните в предварительно созданную папку необходимые изображения для вёрстки.

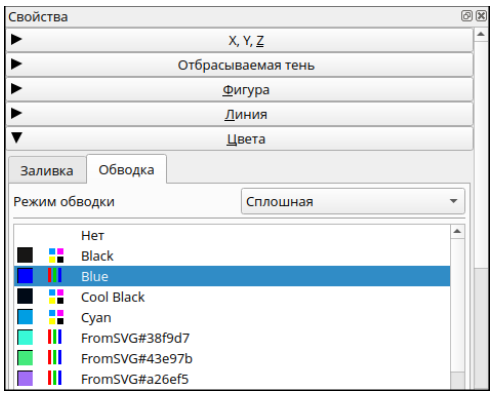
4. Импортируйте векторную графику в документ с помощью меню «**Файл**» — «**Импортировать**» — «**Вставить векторный графический файл...**».



5. Теперь создайте блоки, в которых будут располагаться текст и изображение, с помощью меню «**Вставка**» — «**Фигура**» — «**Типовые фигуры**» — . Расположите курсор мыши на листе в точке, где будет начинаться блок. Затем нажмите ЛКМ и, удерживая, проведите курсором до желаемого конечного положения блока. После достижения конечной точки блока отпустите ЛКМ для завершения размещения. Второй блок создайте аналогичным образом.

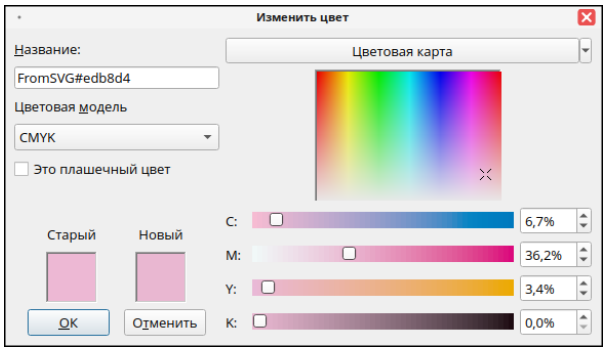


6. Для изменения цвета заливки и контура объекта щёлкните ПКМ по объекту и выберите из контекстного меню пункт «**Свойства**» — «**Цвета**».



Если логотип содержал, например, прямое указание цвета или точное предписание цвета CMYK, откройте меню «**Правка**» — «**Цвета и заливки...**».

После двойного щелчка по цвету откроется окно «**Изменить цвет**», в котором можно изменить цветовую модель (CMYK, RGB, веб-палитра RGB, Lab, HLC) и название цвета.

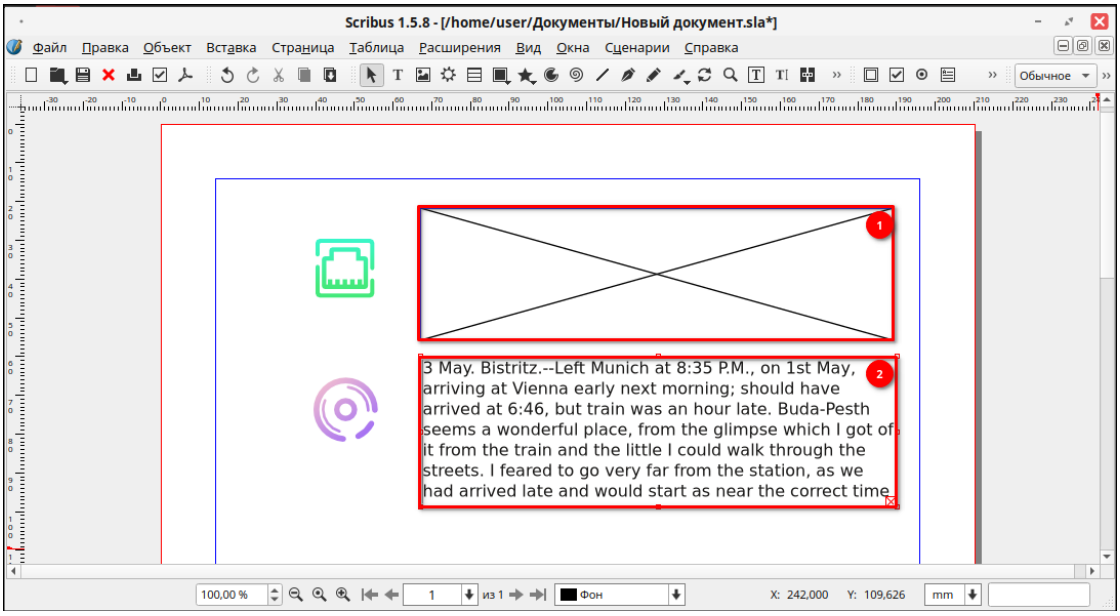


7. Для преобразования блоков и вставки текста выполните следующие действия.

Для преобразования блока в блок изображения щёлкните ПКМ по рамке и выберите «**Преобразовать в**» — «**Блок изображения**» (1).

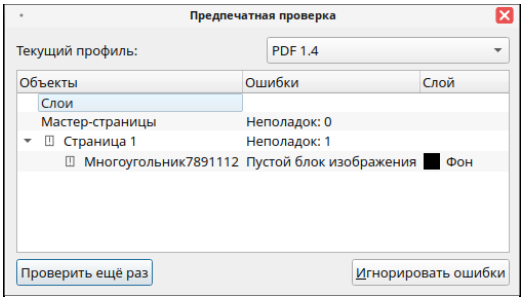
Для преобразования блока в текстовый блок щёлкните ПКМ по рамке и выберите «**Преобразовать в**» — «**Текстовый блок**».

Для вставки текста щёлкните ПКМ по рамке и выберите «**Содержимое**» — «**Вставить текст...**». Выберите файл с текстом и нажмите «**OK**». В блоке отобразится текст из файла (2).

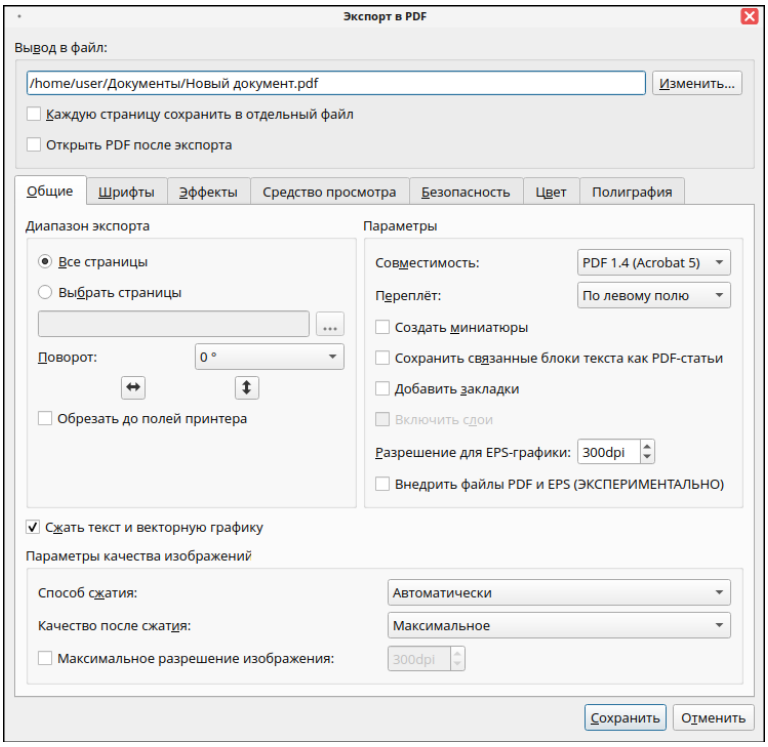


Экспорт файла

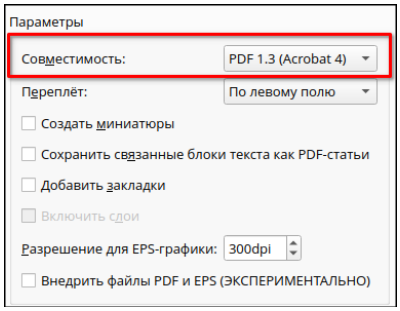
1. Для экспорта файла нажмите кнопку «**Сохранить как PDF**» (). Если PDF содержит какие-либо ошибки, появляется окно *Предпечатной проверки*. Исправьте ошибки или нажмите «**Игнорировать ошибки**».



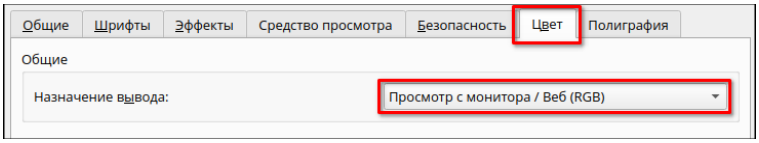
2. В появившемся окне «**Экспорт в PDF**» задайте параметры.



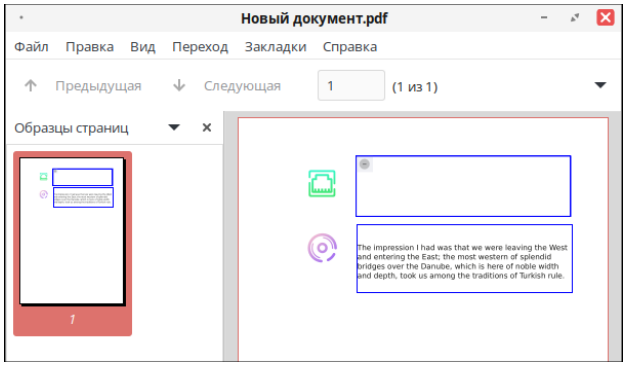
На вкладке «**Общие**» в параметрах совместимости выберите *PDF 1.3 (Acrobat 4)*.



На вкладке «**Цвет**» установите «**Просмотр с монитора / Веб (RGB)**».



После выбора параметров нажмите «**Сохранить**». После выполненных действий документ будет доступен для просмотра.



Редактор шрифтов FontForge

Установка
Обзор программы
Освоение инструментов
Понимание кривых Безье
Инструменты точек
Глифы
Инструменты рисования
Инструменты преобразования
Инструменты Прямоугольник, Эллипс, Многоугольник, Звезда
Действия кнопок мыши
Слои

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: fontforge-20190801-8

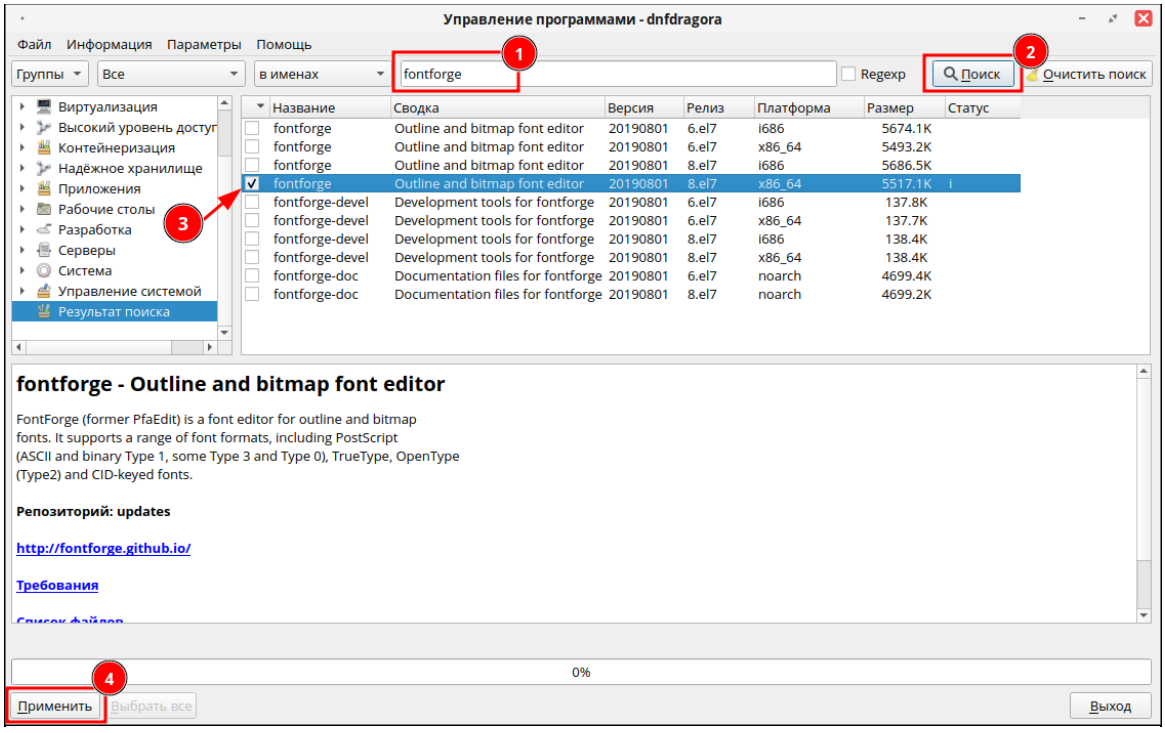
FontForge – многофункциональный редактор шрифтов с открытым исходным кодом, предоставляющий возможность создания, редактирования, конвертации и работы с различными форматами шрифтов, включая *TrueType* (TTF), *OpenType* (OTF), *PostScript* (PS), *SVG*, *UFO* и другие. Редактор также предлагает широкий спектр инструментов для творческого процесса в области шрифтов и типографики.

Среди работ автора программы также есть известные шрифты *Caslon Roman*, *Unicode font*, семейство шрифтов *Monospace* и т. д.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки редактора через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**fontforge**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fontforge
```

Дальнейшая работа в программе выполняется с правами непривилегированного пользователя, **выйдите** из сеанса пользователя **root**:

```
exit
```

После установки запуск редактора доступен из «**Главного меню**» - «**Графика**» - «**FontForge**» или через терминал с помощью команды:

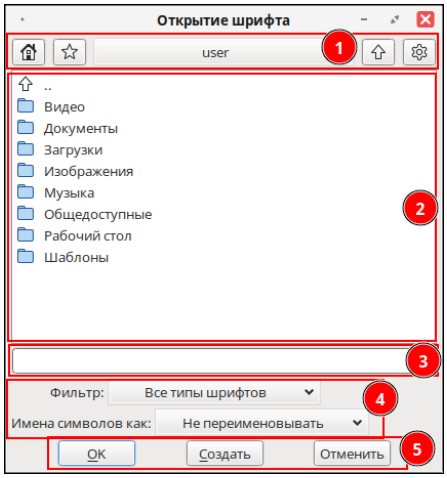
```
fontforge
```

Обзор программы

После запуска приветственное окно редактора выглядит следующим образом:



Вместе с приветственным окном активируется форма «**Открытие шрифта**», которая может быть использована для открытия уже существующего проекта или создания нового.



В форме «**Открытие шрифта**» доступны следующие инструменты:

1. Навигация по каталогам – здесь доступны:

- перемещение в домашний каталог пользователя;
- добавление каталога в закладки;
- перемещение по дереву каталогов на уровень выше;
- режим отображения файлов и каталогов.

2. Список файлов и подкаталогов, содержащихся в текущем каталоге.

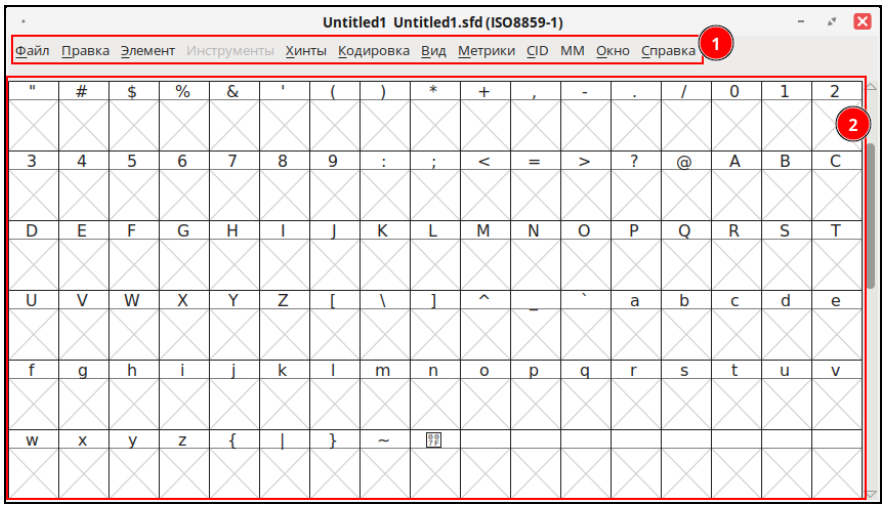
3. Текстовое поле, в котором отображается путь к файлу.

4. Параметры фильтрации найденных файлов по типам файлов и именам символов.

5. Кнопки действий:

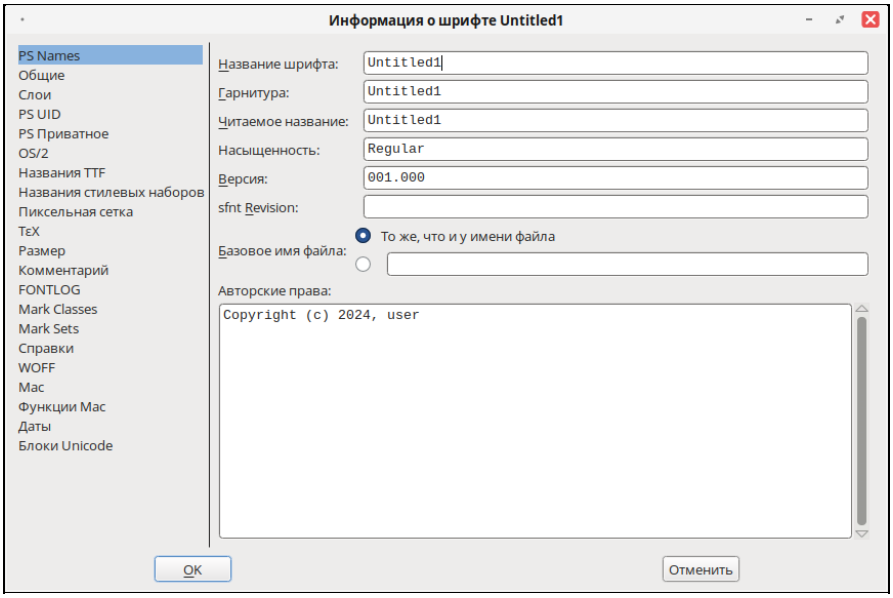
- **OK** – для открытия существующего проекта;
- **Создать** – для создания нового проекта;
- **Отменить** – для завершения работы.

После открытия проекта подгружается окно **Font View**, в котором показана таблица всех глифов в шрифте. Т.к. в рассматриваемом примере проект новый, все ячейки пусты.



В окне просмотра шрифта доступно основное меню (**1**), в котором расположены все необходимые для работы действия, и поле для просмотра глифов в шрифте (**2**).

Выберите пункт меню «**Элемент**» – «**Информация о шрифте**», чтобы заполнить информацию о создаваемом шрифте. В разделе **PS Names** заполните поля собственными данными о шрифте.



Освоение инструментов

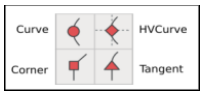
В процессе создания шрифта в **FontForge** используются различные инструменты и утилиты, включая инструменты рисования. Они отличаются от тех, с которыми знакомы пользователи, работающие с векторной графикой. Прежде чем рассматривать сами инструменты рисования в **FontForge**, сначала необходимо изучить работу с кривыми Безье.

Понимание кривых Безье

Концепция "кривых Безье" относится к математическому подходу, применяемому для создания плавных кривых в цифровой форме. Обычно используются кубические и квадратичные кривые, но в дизайне также используются альтернативные кривые *Spiro*, поддерживаемые **FontForge**.

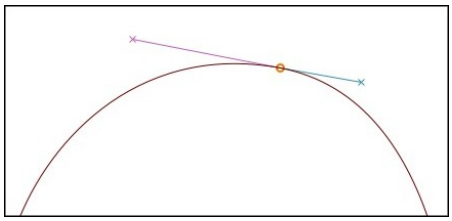
Инструменты точек

Панель инструментов для точек кривых, угловых и касательных выглядит следующим образом:



Точки кривой (круглой формы)

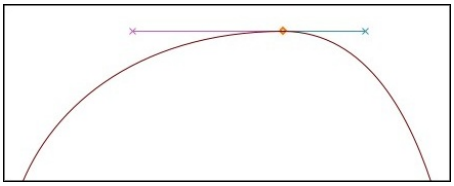
У каждой точки кривой присутствуют две ручки, их расположение связано между собой таким образом, что линия, соединяющая их, всегда остаётся прямой, обеспечивая создание плавной кривой с обеих сторон.



Точка кривой позволяет добавить новую точку на контуре.

Точки H / V кривой (точки в форме ромба)

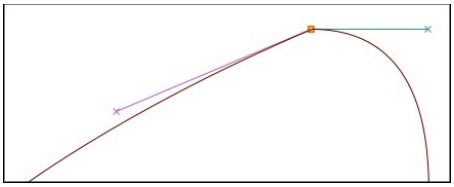
Точки H/V кривой (горизонтальные/вертикальные) представляют собой специальный тип точек кривой, которые привязаны к горизонтальной или вертикальной оси, что является важным условием для корректного формирования кривых Безье.



Инструмент *Точки H/V кривой* позволяет добавить новую точку на контуре.

Угловые точки (точки квадратной формы)

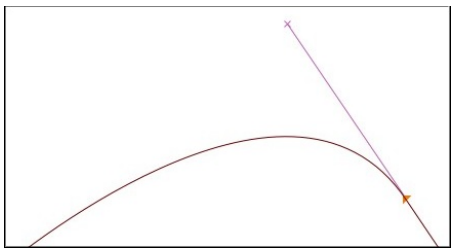
Каждая точка может содержать 0, 1 или 2 маркера Безье, причем каждая ручка может быть установлена независимо от других, что позволяет создавать разрывы в контуре. Без маркеров точки будут иметь прямые линии.



Угловая точка создает резкий изгиб контура.

Точки касательной (точки треугольной формы)

Каждая точка может содержать 0, 1 или 2 маркера Безье, причем каждая ручка может быть установлена независимо от других, что позволяет создавать разрывы в контуре. Без маркеров точки будут иметь прямые линии.



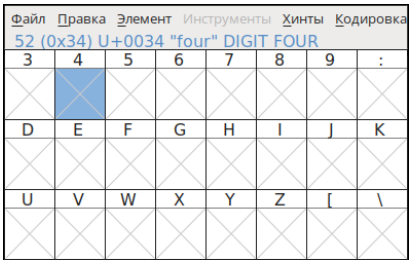
Точка касания позволяет перейти от прямого сегмента к изогнутому вдоль контура.

Глифы

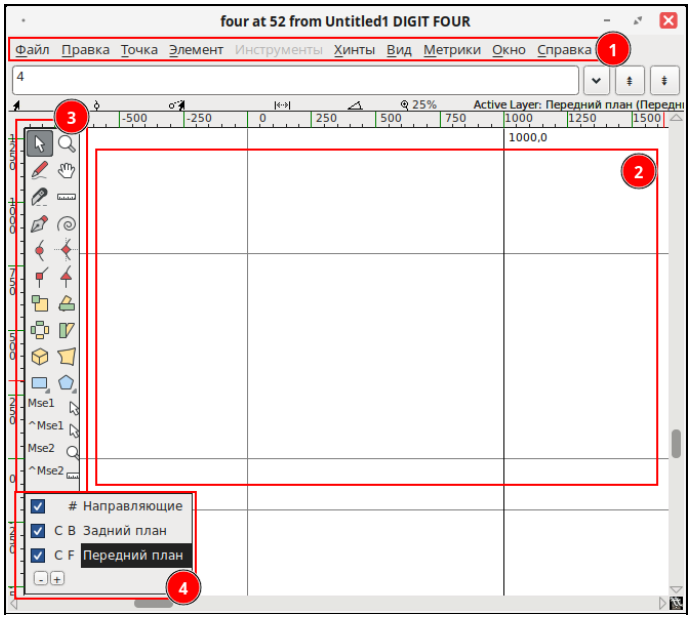
Для редактирования глифа необходимо дважды кликнуть по полю, при этом будет открыто окно **Character View**. Здесь можно рисовать и редактировать глифы двумя способами:

- один за другим при помощи интерфейса со вкладками;

- параллельно с подготовленным текстовым файлом слов.



Окно **Character View** выглядит следующим образом:



В верхней части окна находится основное меню (**1**), где доступны все действия по работе с **FontForge**.

Окно для рисования (**2**) предназначено для создания символов в определённом стиле.

Панель инструментов (**3**) предоставляет основные действия для работы со шрифтом.

Панель инструментов для слоев (**4**) предоставляет возможность отображения/скрытия при работе определенного слоя.

Инструменты рисования

Инструмент «**Указатель**» ( ) позволяет выделять и перемещать точки контура или сами контуры символа. Выделение производится щелчком по нужным точкам/контурам или выделением при нажатой ЛКМ области, содержащей нужные точки. Также щелчком можно выделить правую границу символа. Добавление или исключение точек производится при нажатой клавише *Shift*.

Инструмент «**Лупа**» ( ) позволяет изменять масштаб в окне символа. Увеличение производится щелчком в окне символа (или с использованием горячей клавиши *Z*), уменьшение — щелчком при нажатой клавише-модификаторе *Alt* (или с использованием горячей клавиши *X*).

Инструмент «**Свободное рисование**» ( ) позволяет создавать неровные контуры. Для рисования зажмите ЛКМ в области рисования, затем проведите необходимые линии. После этого вернитесь к инструменту «**Указатель**», чтобы выделить точки на нарисованном контуре. При выборе точки контура она подсвечивается желтым цветом. Можно также выбрать и переместить контрольные точки, чтобы изменить форму кривой.

Инструмент «**Перо**» ( ) позволяет добавить точку на кривой и переместить ее контрольные точки.

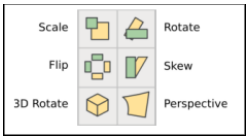
Инструмент «**Спиро**» ( ) активирует режим рисования spi-кривых, который позволяет создавать кривые, изменяющие форму при перемещении узлов.

Инструмент «**Нож**» ( ) позволяет разрезать контур между точками. На образующихся концах контура создаются две новые точки кривых, между которыми нет соединения. Чтобы разрезать контур, надо провести курсор в точке разреза, удерживая нажатой ЛКМ. Может оказаться полезным, если для дальнейшей работы требуется только часть нарисованной фигуры.

Инструмент «**Линейка**» ( ) позволяет измерять расстояние, угол и смещение по осям *X* и *Y* от точки, где была отпущена ЛКМ до текущего положения курсора. При использовании отображается "всплывающая подсказка" рядом с курсором, предоставляющая более подробные сведения об измерениях и координатах.

Инструменты преобразования

Панель инструментов преобразования выглядит следующим образом:



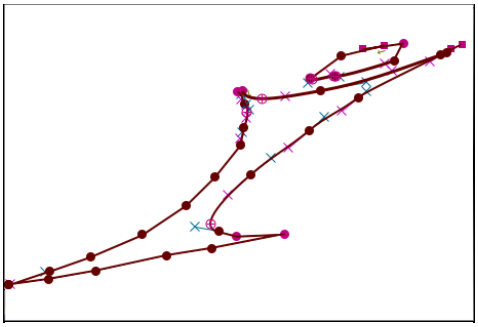
При двойном клике по любому инструменту трансформации можно ввести числовые значения. Инструмент «**Масштабирование**» (*Scale*) позволяет изменять масштаб объекта вручную с возможностью сохранения пропорций при удержании клавиши *Shift*.

Инструмент «**Поворот**» (*Rotate*) используется для произвольного вращения объекта вокруг начальной точки нажатия мыши.

Инструмент «**Поворот в 3D**» (*3D rotate*) позволяет вращать объект в 3D и отображать результат на плоскости *XY*.

Инструмент «**Отразить**» (*Flip*) отражает выделение по горизонтали или вертикали с использованием точки начального нажатия мыши в качестве центра преобразования.

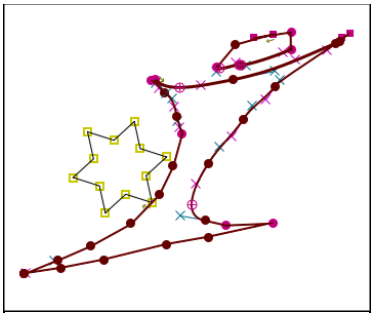
Инструмент «**Наклонить**» (*Skew*) позволяет наклонить фигуру.



Инструменты Прямоугольник, Эллипс, Многоугольник, Звезда

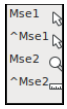
Инструменты позволяют быстро рисовать примитивные геометрические фигуры, без необходимости построения их из отдельных отрезков линий. Чтобы переключиться на альтернативный инструмент, щелкните по зоне шеврона в этих инструментах, а для открытия параметров формы выполните двойной щелчок.

Для прямоугольника можно настроить углы и ограничивающую рамку, для эллипса – ограничивающий прямоугольник или центрирование, для многоугольника можно задать количество вершин, а для звезды – количество точек и их глубину в процентах.



Действия кнопок мыши

Панель инструментов для действий кнопок мыши выглядит следующим образом:



На панели инструментов можно просмотреть текущий инструмент и доступные операции для кнопок мыши:

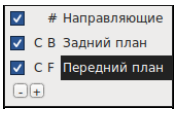
- ЛКМ (*Mse1*);
- *Ctrl* + ЛКМ (*^Mse1*);

- Кнопка колесика мыши (*Mse2*);
- *Ctrl* + Кнопка колесика мыши (*^Mse2*).

Так можно использовать несколько различных инструментов, не прибегая к многократному поиску на панели инструментов.

Слои

Панель инструментов для слоев выглядит следующим образом:



Холст в **FontForge** имеет три слоя: направляющий, задний план и передний план. Направляющие слои предназначены для вставки направляющих, для рисования используются передний и задний план. Для создания окончательного шрифта будет использован только верхний слой переднего плана.

Активный флаг показывает видимость каждого слоя. Флаг можно снять, чтобы сделать слой невидимым. Символы *C* (или *Q*) показывают, какие кривые используются – кубические или квадратные, символы *#*, *B* или *F* указывают тип каждого слоя. Дополнительные слои можно создавать или удалять с помощью кнопок «**+**» или «**−**» на панели. Типом слоя и кривой также можно управлять щелчком правой кнопки мыши (при наличии дополнительных слоев).

Аудиоплеер Audacious

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** audacious-4.2-3

Audacious — аудиоплеер с открытым исходным кодом. Позволяет перетаскивать папки и отдельные аудио-файлы в окно плеера, искать исполнителей и альбомы во всей музыкальной библиотеке или создавать и редактировать собственные списки воспроизведения, а также слушать компакт-диски или трансляции музыки из Интернета.

В **audacious** есть возможность настраивать звук с помощью графического эквалайзера или изменять динамический диапазон с помощью звуковых эффектов. С помощью подключаемых модулей **audacious** способен извлекать тексты аудио-файлов, отображать уровень громкости, а с помощью «скинов» позволяет изменять внешний интерфейс, например, на **Winamp Classic**.

Для установки **audacious** перейдите в сеанс пользователя **root**:

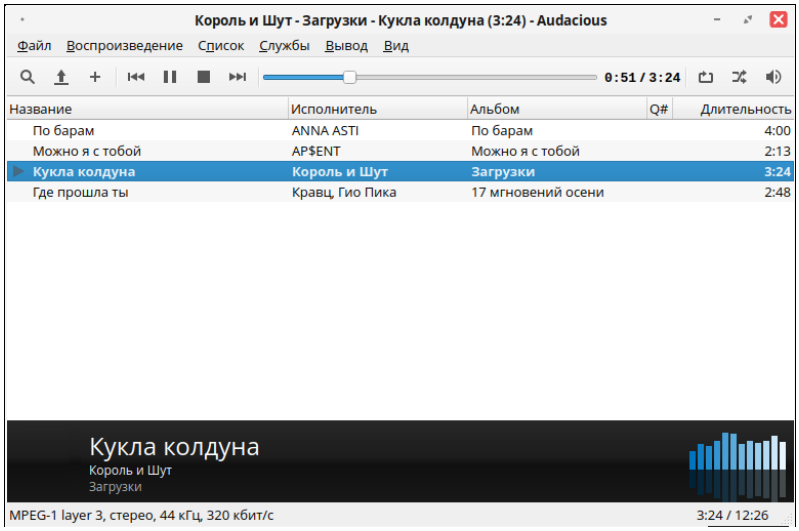
```
su -
```

и выполните команду:

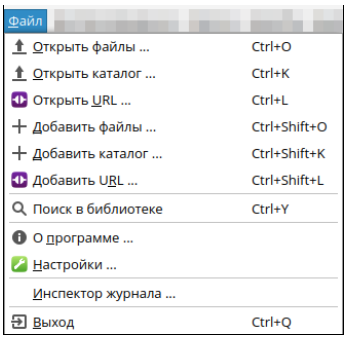
```
dnf install audacious
```

Далее работа в программе выполняется с правами локального пользователя.

После установки аудио-проигрыватель будет доступен из «**Главного меню**» - «**Аудио и видео**» - «**Audacious**».

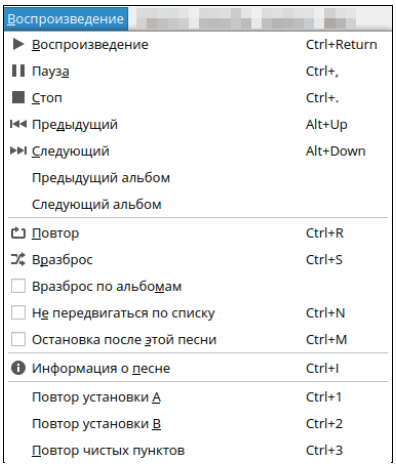


Из пункта меню «**Файл**» доступны базовые функции для добавления отдельных аудиозаписей и каталогов, а также URL списков трансляции медиа-потока из Интернета.



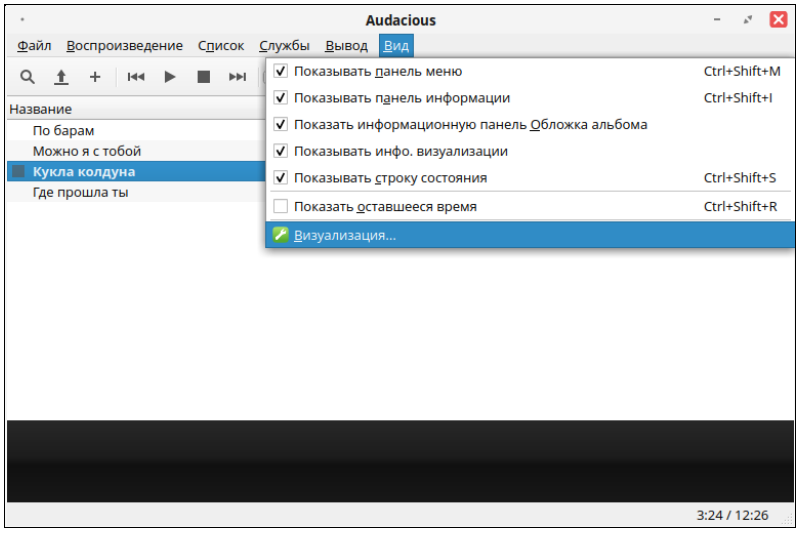
Функции пункта меню «**Воспроизведение**» интуитивно простые, элементы управления («**Воспроизведение**», «**Пауза**», «**Стоп**» и др.) представлены на верхней панели проигрывателя, также есть возможность включить повтор конкретного трека или перемешать все треки в списке аудиозаписей.

Из пункта меню «**Список**» можно создавать и управлять своими списками аудио. Здесь доступны функции сортировки, поиска определенного трека из списка, удаление дубликатов, а также экспорт и импорт списка.

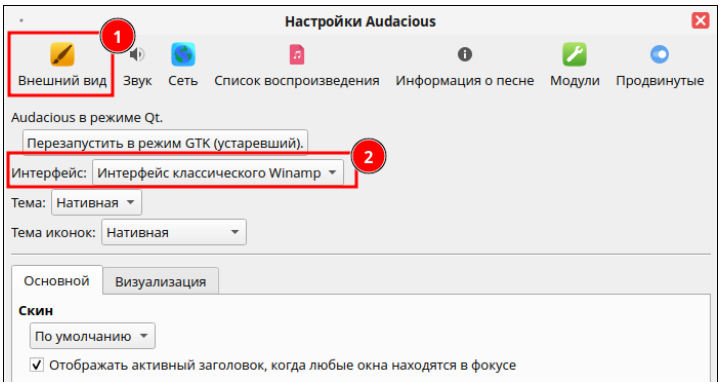


Также в Audacious есть возможность изменить вид приложения под классический интерфейс проигрывателя **Winamp**, для этого необходимо:

- Открыть пункт меню «**Вид**»;
- Выбрать пункт «**Визуализация**»;



- Далее открыть вкладку «**Внешний вид**»;
- И параметре «**Интерфейс**» выбрать «**Интерфейс классического Winamp**».



В результате изменится внешний вид приложения **Audacious**.


AUDACIOUS
0:07
??? ?@??:? ?? (2:48) --- ?@???. (
320 KBIT/S, 44 KHZ, STEREO
RAND
REP
PLAYLIST
ANNA ASTI - По барам - По барам 4:00
AP$ENT - Можно я с тобой - Можно я 2:13
Король и Шут - Загрузки - Кукла кол 3:24
Кравц, Гио Пика - 17 мгновений осе 2:48
2:48/12:20
0:07

AlsaMixer - настройка звуковых карт

Навигация в программе
Настройка звука с помощью AlsaMixer
Настройка микрофона с помощью AlsaMixer
Решение возникающих проблем

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: alsa-utils-1.2.12-1

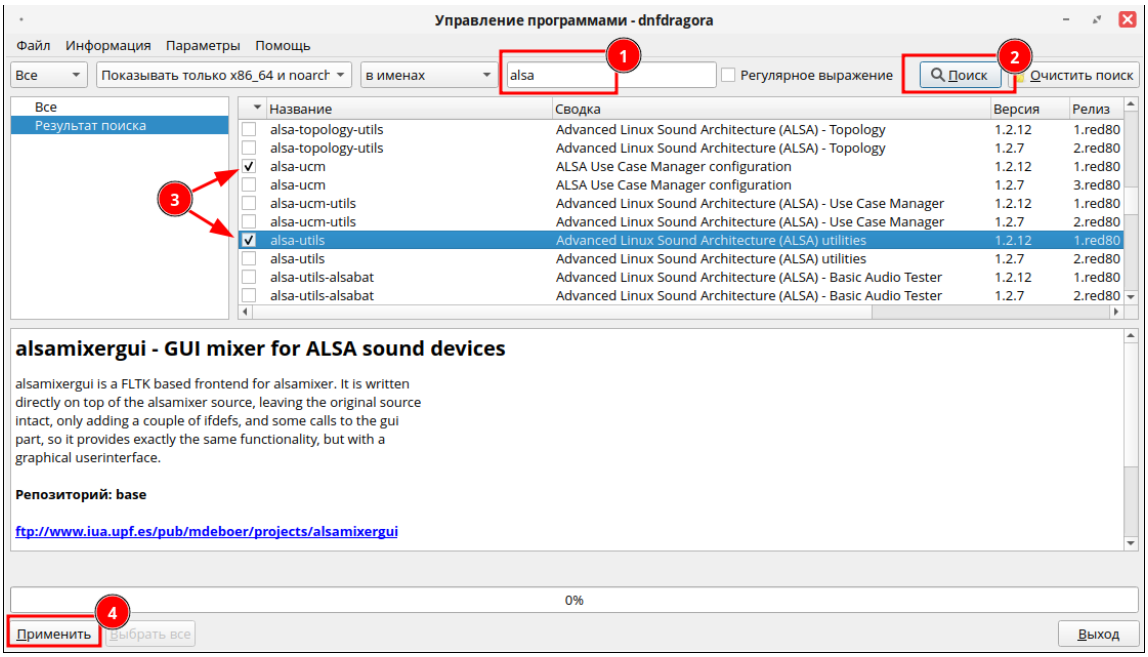
AlsaMixer — это псевдографическое приложение для просмотра и управления свойствами звуковых карт, установленных на компьютере.

В РЕД ОС **AlsaMixer** установлен по умолчанию и запускается с помощью команды с правами локального пользователя:

```
alsamixer
```

Однако, если на вашем компьютере приложение по каким-либо причинам отсутствует, установить его можно двумя способами — через графический менеджер пакетов или через терминал.

Для установки приложения через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимых пакетов по ключевому слову «**alsa**» и отметьте флагом пакеты **alsa-utils**, **alsa-ucm** и **alsa-plugins-pulseaudio** последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Подтвердите транзакцию, нажав кнопку «**Хорошо**». Установка займет некоторое время, после успешной установки окно с транзакцией исчезнет. Сам пакет будет отмечен как установленный.

Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install alsa-utils alsa-ucm alsa-plugins-pulseaudio
```

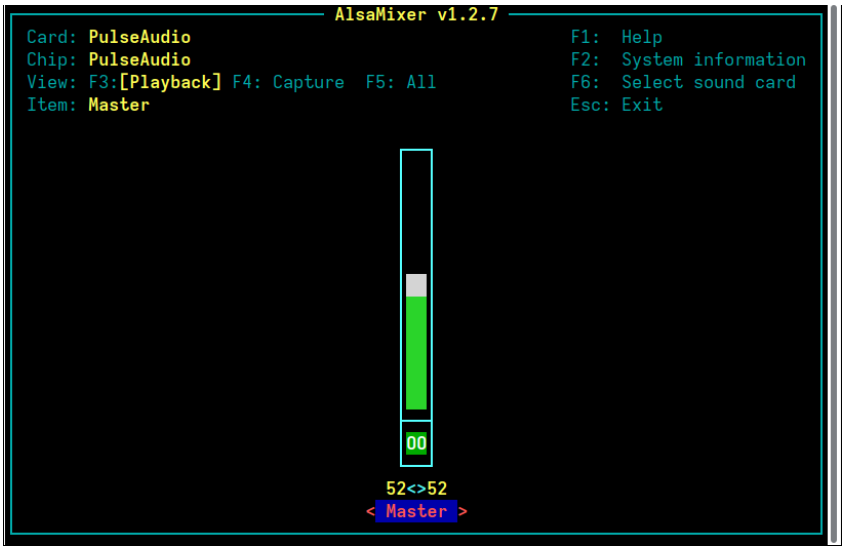
Дальнейшая работа в программе выполняется **от локального пользователя**.

Навигация в программе

После ввода команды запуска появится интерфейс программы с ползунком «**Master**», который управляет громкостью звуковых устройств по умолчанию. Можно управлять общим уровнем звука с помощью клавиш со стрелками вверх и вниз.

Также допускается управление отдельными звуковыми каналами:

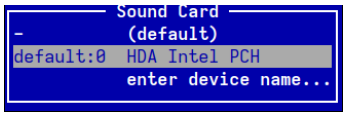
- **Q**, **Z** — для управления левым каналом;
- **E**, **C** — для управления правым каналом.



Слева вверху пользователю предоставляется информация о следующих параметрах устройства:

- **Card** — текущее звуковое устройство;
- **Chip** — драйвер звукового устройства;
- **View** — выбранный режим работы;
- **Item** — строка состояния выбранного параметра (чаще всего, показывает значения усиления в децибелах).

При нажатии клавиши **F6** появляется список звуковых устройств компьютера, в котором можно выбрать именно то устройство, которое нуждается в дополнительной настройке.

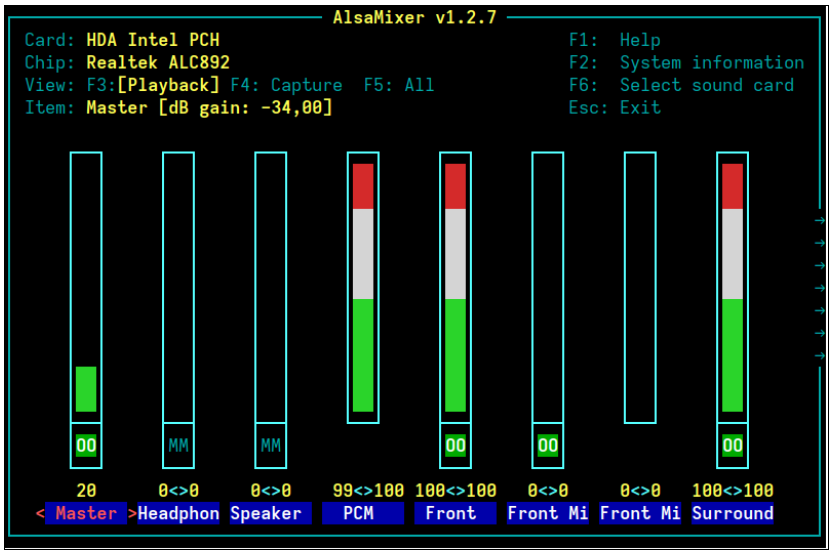


Также звуковую карту можно выбрать с помощью команды в консоли при запуске **AlsaMixer**:

```
alsamixer -c<N>
```

где **N** — целое число, обозначающее ID звукового устройства (по умолчанию имеет значение 0).

После выбора звуковой карты из списка количество настраиваемых параметров на экране заметно увеличится.



Переключаться между ползунками можно с помощью клавиш со стрелками вправо и влево. Для отключения параметра ползунка, нажмите клавишу **M**, тогда в нижней части ползунка надпись «**OO**» сменится на «**MM**», что и будет означать отключение ползунка (некоторые ползунки отключены по умолчанию).

По умолчанию программа запускается в режиме настройки воспроизведения. Если необходимо настроить микрофон или другие устройства ввода звука, следует переключится в режим настройки соответствующих устройств с помощью клавиши **F4**. Также с помощью клавиши **F5** можно перейти в общий режим, в котором объединены ползунки для настройки воспроизведения и ввода звука. Вернуться в режим настройки только устройств воспроизведения можно нажатием клавиши **F3**. Переключение между режимами также доступно с помощью клавиши **Tab**.

Настройка звука с помощью AlsaMixer

В зависимости от устройства количество настраиваемых свойств может меняться. Среди общих параметров всех устройств можно выделить следующие:

- **Master** — отвечает за весь вывод звука вне зависимости от устройства, за исключением параметра **Master Mono**. Обычно не должен быть отключён;
- **Headphone** — отвечает за вывод звука устройств, подключённых к передней панели компьютера;
- **Headphone Jack Sense** — если этот параметр включён, то все звуковые выходы отключаются при подключении устройства к передней панели компьютера;
- **PCM** — отвечает за воспроизведение всех звуковых и видео файлов. Отключить его нельзя, но важно следить, чтобы усиление этого параметра не превышало **0 dB**;
- **External Amplifier** — отвечает за воспроизведение звука источников с дополнительным питанием (например, колонки).

Настройка микрофона с помощью AlsaMixer

Ключевые параметры настройки захвата аудио меняются в зависимости от установленного устройства. Чаще всего при настройке микрофона необходимо настраивать следующие параметры:

- **Capture** — параметр, отвечающий за чувствительность микрофона;
- **Mic Boost** — позволяет дополнительно увеличивать чувствительность микрофона;
- **Input Source** — определяет, с какого входа будет захватываться звук (с передней панели или напрямую, с материнской платы).

Решение возникающих проблем

Alsamixer не определяет звуковую карту

Необходимо обновить пакеты **alsa**. Для этого выполните команду:

```
dnf update alsa-utils
```

Нет звука

Убедитесь, что ползунки «**Master**» и «**PCM**» не отключены.

Также в некоторых случаях помогает установка дополнительного пакета **alsa-sof-force**. Установить его можно командой в терминале:

```
dnf install alsa-sof-force
```

Искажение звука

Убедитесь, что усиление параметра «**PCM**» не превышает **0**.

Ошибка при запуске AlsaMixer

Убедитесь, что запуск программы **AlsaMixer** производится от имени локального пользователя, а **не** от пользователя **root**.

Если же вы сталкиваетесь с ошибкой вида:

```
alsamixer: сбой функции snd_ctl_open по умолчанию: такого устройства нет
```

необходимо вручную выбрать устройство, которое будете настраивать программой **AlsaMixer**, с помощью команды:

```
alsamixer -c**N**
```

где **N** — целое число, обозначающее ID звукового устройства (по умолчанию имеет значение 0).

Если вы подключили к компьютеру альтернативную или внешнюю звуковую карту, можно открыть её настройки, обращаясь к устройству по имени. Например:

```
alsamixer -c usb
```

hdajackretask - управление портами звуковых устройств

hdajackretask — графическая утилита, предназначенная для управления портами звуковых устройств на звуковых картах *HDA Intel*. **hdajackretask** входит в набор **alsa-tools**.

Для установки **alsa-tools** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

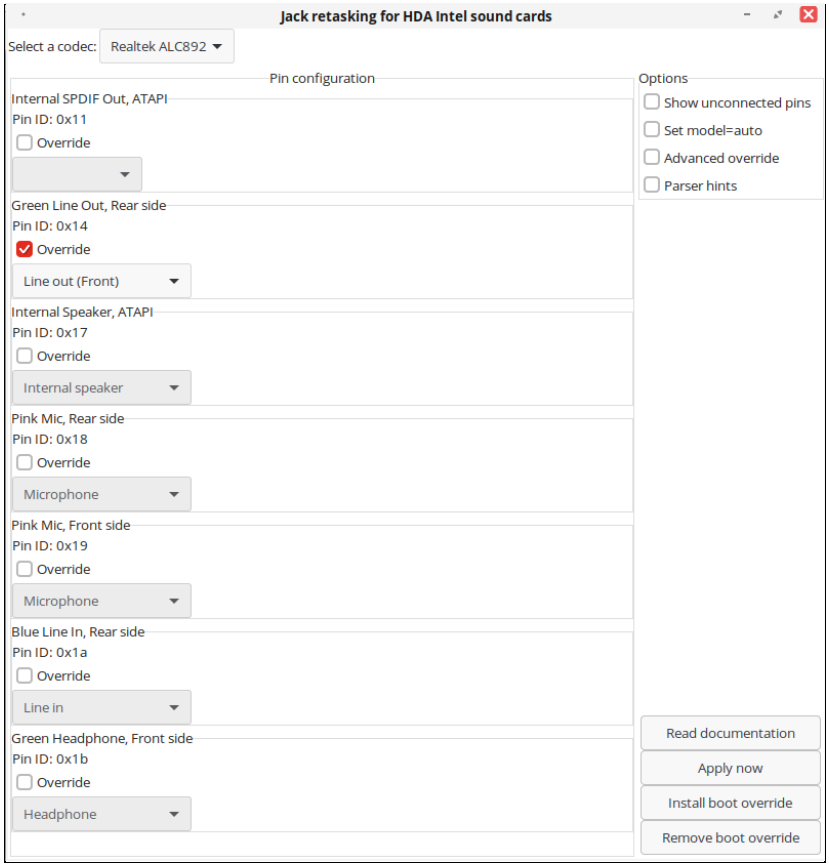
```
dnf install alsa-tools
```

Дальнейшая работа в программе выполняется с правами **локального пользователя**.

После установки **hdajackretask** доступен из «**Главного меню**» — «**Аудио и Видео**» — «**HDAJackRetask**» или из терминала командой:

```
hdajackretask
```

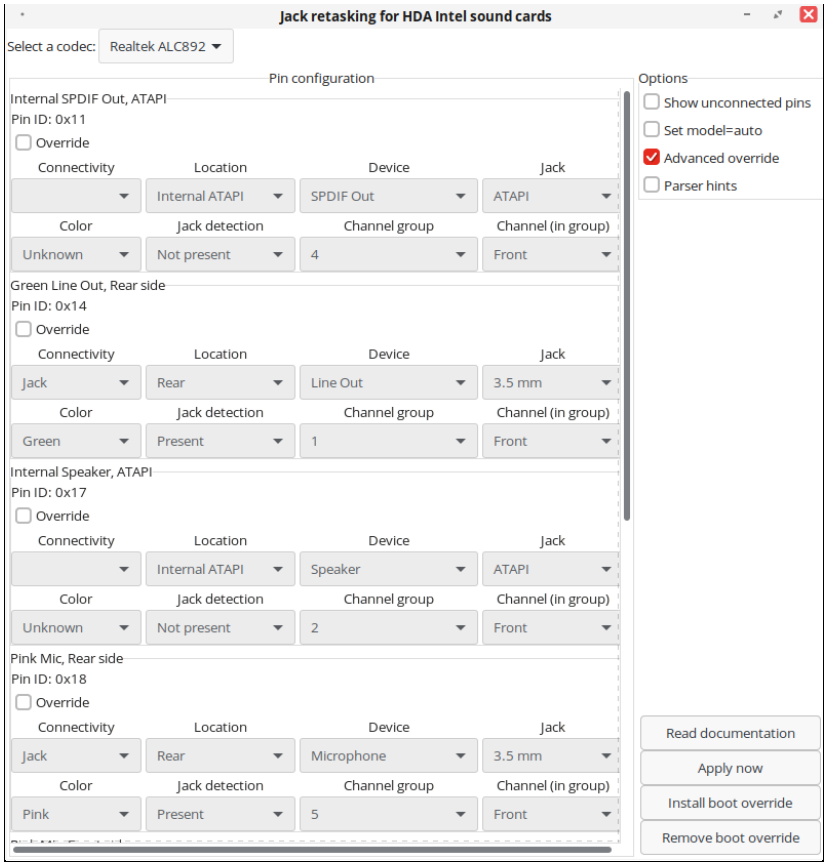
Окно программы выглядит следующим образом:



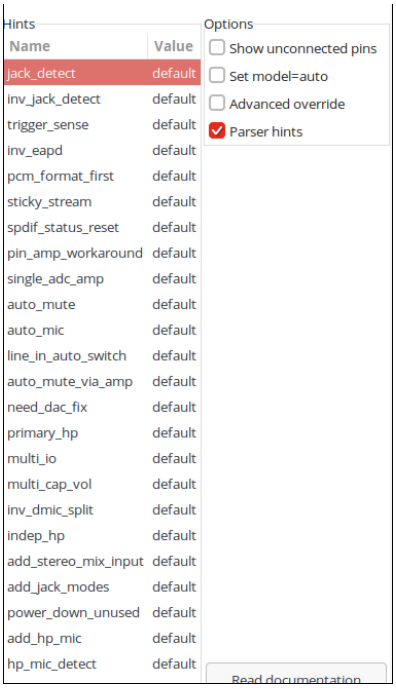
На верхней панели окна программы есть возможность выбрать используемый кодек звуковой карты. Как правило, к звуковым устройствам компьютера относится только первый кодек в выпадающем списке, а остальные кодеки относятся к HDMI.

В разделе «**Options**» находятся дополнительные настройки, влияющие как на работу звукового оборудования, так и на количество параметров, редактируемых в разделе «**Pin configuration**». Рассмотрим их подробнее:

1. **Show unconnected pins** — BIOS компьютера иногда может давать сбой и не показывать по умолчанию все существующие порты. В таком случае можно попробовать установить флаг для этой настройки, тогда в разделе «**Pin configuration**» появятся новые порты, которые физически могут отсутствовать в вашей системе, но существует большая вероятность появления необходимого для работы порта.
2. **Set model = auto** — некоторые кодеки, особенно старые, игнорируют переопределения, созданные пользователем в программе. Во многих подобных случаях помогает установка флага для этого параметра. Однако существует вероятность, что звуковая карта не примет новые параметры в том случае, если она является устаревшей или установленное в системе ядро имеет версию 3.8 или ниже.
3. **Advanced override** — расширенный режим, который открывает доступ к дополнительным параметрам каждого порта. Не рекомендуется для неопытных пользователей. Прежде чем изменять расширенные параметры портов, необходимо ознакомиться со спецификацией *Intel High-Definition Audio*.



4. **Parser hints** — позволяет пользователю отправлять специальные «подсказки» для драйвера, которые помогают избежать конфликтов или несовпадений между конфигурациями BIOS и драйверами звуковой карты. Для неопытных пользователей, которые не ознакомлены с документацией к драйверу, рекомендуется оставлять значения всех параметров «**default**».



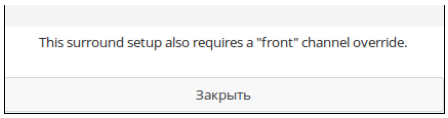
Все настройки портов находятся в графе «**Pin configuration**», которая представляет собой список всех портов, которые смог обнаружить BIOS компьютера. Каждый порт в стандартном виде имеет всего один параметр — тип устройства, которое будет с ним работать. Обычно предлагаемые устройства можно разделить на следующие группы:

- **Line Out** — активные устройства для вывода звука. Например, колонки, которым нужен дополнительный источник питания. Как правило, на такие устройства звук выводится с большим усилением;
- **Line In** — устройства для ввода звука;
- **Internal speaker / mic** — встроенный динамик/микрофон на материнской плате ПК;
- **Headphones** — устройства для вывода звука, которые не требуют дополнительного источника питания. На такие устройства

звук выводится с меньшим усилением, чем на устройствах типа **Line Out**.

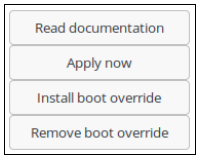
Для того чтобы иметь возможность редактировать параметры, следует пометить порт как переопределяемый (установить на нём флаг **Override**).

Важно учитывать, что если попытаться переопределить устройство **Line Out (Back)**, то обязательно нужно переопределить или пометить как переопределяемое устройство **Line Out (Front)**. Если попытаться переопределить устройство **Line Out (Center/LFE)**, то необходимо переопределить или пометить как переопределяемые устройства **Line Out (Back)** и **Line Out (Front)**. При игнорировании этих условий, если пользователь попытается принять изменения, программа выдаст ошибку следующего вида:



В правом нижнем углу окна программы находятся четыре кнопки, которые отвечают за следующие функции:

- **Read documentation** — вызывает окно с краткой инструкцией по работе в программе;
- **Apply now** — применяет изменения, внесённые пользователем. После перезагрузки компьютера изменения не сохраняются;
- **Install boot override** — сохраняет изменения в загрузочном секторе компьютера, чтобы они сохранялись даже после перезагрузки;
- **Remove boot override** — удаляет информацию об изменениях в загрузочном секторе компьютера. При следующем включении компьютера все параметры загружаются со значениями по умолчанию.



Настройка звука с помощью PulseAudio

Настройка звука с помощью графического интерфейса
Настройка звука с помощью pavucontrol
Настройка звука с помощью PulseAudio через терминал

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: pipewire-1.0.3-3, pavucontrol-5.0-3

PulseAudio — кроссплатформенный звуковой сервер, созданный в качестве улучшенной замены таких серверов, как ESD, ARts.

PulseAudio принимает звук от одного или нескольких источников (процессов или устройств) и направляет одному или нескольким приёмникам (звуковым платам, серверам PulseAudio или процессам). Одной из основных целей проекта является предоставление возможности перенаправления любых звуковых потоков, включая и потоки от процессов, требующих прямого доступа к аудиоустройствам. Это достигается с помощью специальных псевдоустройств, работающих непосредственно с другими звуковыми системами, такими как aRts или ESD.

В РЕД ОС пользователь может настроить систему ALSA так, чтобы она использовала виртуальное устройство, созданное сервером **PulseAudio**. Тогда программы, работающие со звуком через драйвер ALSA, будут на самом деле работать с **PulseAudio**, который взаимодействует с помощью ALSA уже с реальным устройством.

Основные возможности:

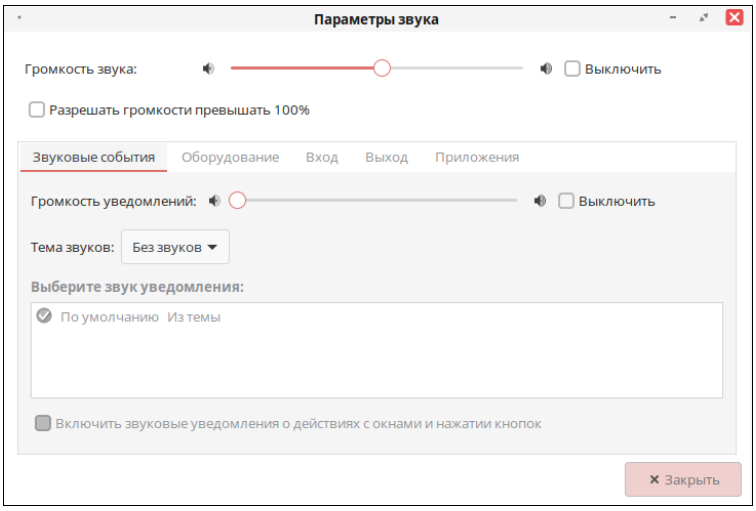
- раздельная установка уровней громкости для разных программ;
- смешивание потоков от разных звуковых плат;
- расширяемая модульная система с поддержкой динамически загружаемых библиотек;
- совместимость со многими популярными аудиоприложениями;
- работа с несколькими источниками и приёмниками звука;
- приемлемая для повседневного непрофессионального использования задержка и возможность ею управлять;
- использование технологии zero-copy, сберегающей машинное время;
- интерфейс командной строки с возможностью использования сценариев;
- демон, перенастраиваемый с помощью командной строки;
- встроенное преобразование аудиоформатов;
- синхронизация потоков воспроизведения;
- смешиваемые потоки могут иметь разные частотные характеристики;
- эффективный микшер, даже для звуковых плат без микшера, предотвращающий «монополизацию» звукового устройства отдельной программой.

Настройка звука с помощью графического интерфейса

Работа с утилитой

Утилита настройки звука доступна из «**Главного меню**» — «**Параметры**» — «**Звук**». Также открыть утилиту можно, нажав ПКМ на иконку регулировки громкости и выбрав пункт «**Параметры звука**».

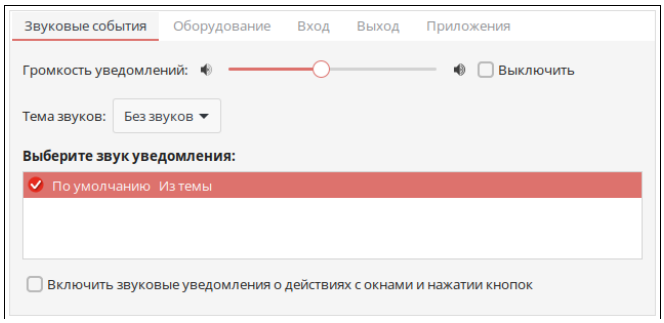
Окно программы выглядит следующим образом:



В верхней части окна находится регулировка громкости звука, флаг полного выключения звука и флаг увеличения максимального порога громкости до 150%.

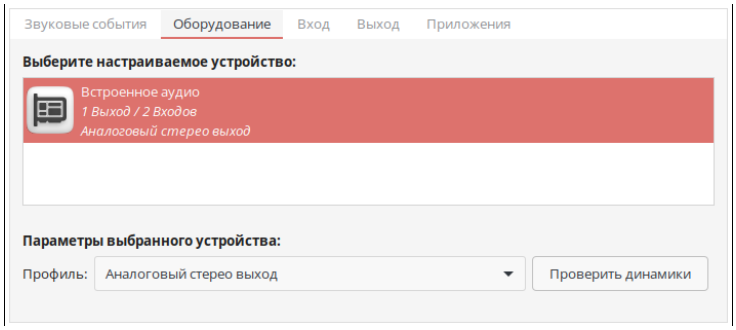
Вкладка «Звуковые события»

На вкладке «**Звуковые события**» можно выбрать тему звуковых событий, а также их громкость.



Вкладка «Оборудование»

В графе «**Выберите настраиваемое устройство**» можно выбрать звуковую карту для настройки.



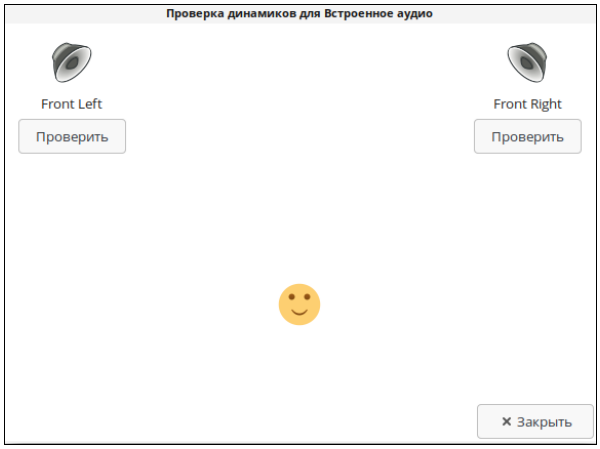
Главным параметром для настройки выбранной звуковой карты является выпадающий список «**Профиль**», в котором доступен выбор режима работы звукового устройства. Утилита предлагает на выбор следующие виды звуковых профилей:

- *Аналоговый стерео дуплекс* — работает с устройствами ввода и вывода звука одновременно;
- *Аналоговый стерео выход* — работает только с устройствами вывода звука;
- *Аналоговый стерео вход* — работает только с устройствами ввода звука;
- *Цифровой стерео выход* — позволяет получать более высокое качество звука, но не все устройства способны поддерживать этот режим;
- *Цифровой стерео выход + Аналоговый стерео вход* — позволяет использовать аналоговые устройства ввода звука одновременно с цифровыми устройствами вывода звука;
- *Выключено* — отключает звуковое устройство.

Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.

При нажатии на кнопку «**Проверить динамики**» появляется окно, позволяющее воспроизводить тестовые звуковые дорожки в различных каналах, количество которых зависит от звукового устройства.

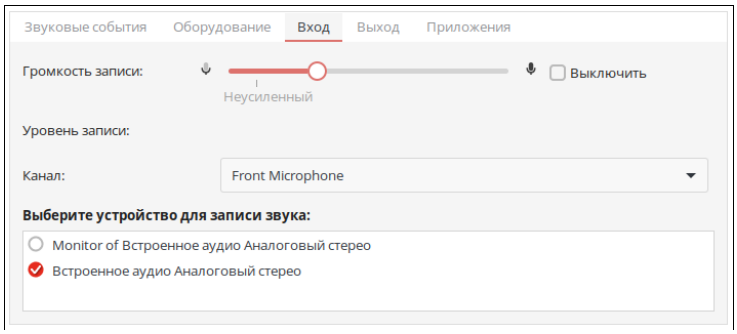


При нажатии кнопки «**Проверить**» рядом с иконкой по выбранному каналу будет воспроизведена звуковая дорожка. Например, при использовании наушников и нажатии кнопки «**Проверить**» возле иконки «**Front Left**» воспроизводимую звуковую дорожку будет слышно только в левом наушнике.

Вкладка «Вход»

Параметр «**Громкость записи**» позволяет пользователю настраивать чувствительность микрофона под свои нужды.

В момент настройки можно наблюдать за уровнем чувствительности микрофона по шкале «**Уровень записи**».



Выпадающий список «**Канал**» предлагает на выбор следующие каналы для работы устройств ввода звука:

- *Front Microphone* — канал микрофона с порта на передней панели компьютера;
- *Rear Microphone* — канал микрофона с порта на материнской плате;
- *Line In* — канал для устройств ввода звука с дополнительного порта на материнской плате. Отличительной особенностью от обычного канала для микрофона является более низкая чувствительность. Данный канал предназначен для электронных устройств, которые имеют возможность ввода звука в компьютер. Например, микшеры, синтезаторы, дрампады и др.

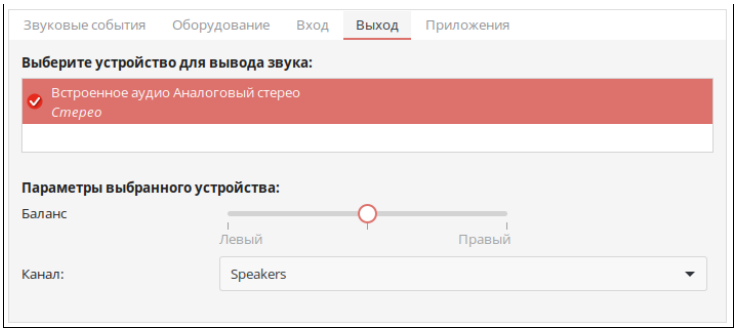
Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.

Последним пунктом настроек на этой вкладке является выбор устройства для записи звука. От выбранного устройства также зависит количество настроек на вкладке.

Вкладка «Выход»

В отличие от вкладки «**Вход**» список устройств для вывода звука предоставляется сразу. От выбранного устройства зависит набор настраиваемых параметров.



Настройка баланса позволяет отрегулировать громкость звучания в каналах относительно друг друга. Доступен следующий выбор каналов:

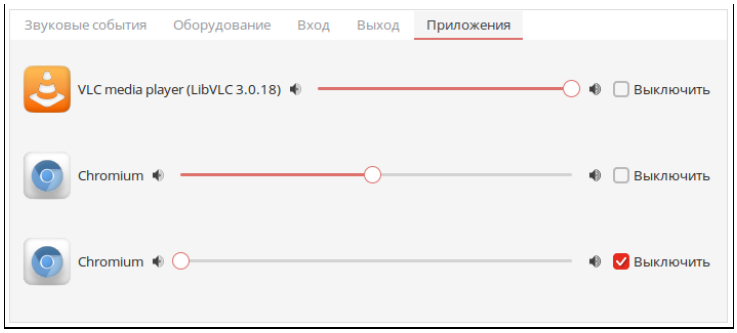
- *Speakers* — канал устройств вывода звука с порта на передней панели компьютера;
- *Headphones* — канал устройств вывода звука с порта на материнской плате;
- *Line Out* — канал устройств вывода звука с дополнительного порта на материнской плате без усиления. Чаще всего используется для подключения усилителей или активных колонок. На обычных устройствах звук будет очень тихим.

Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.

Вкладка «Приложения»

Данная вкладка позволяет установить громкость звучания для определённого приложения или отключить звук в нём совсем.



Настройка звука с помощью pavucontrol

Pavucontrol — это регулятор громкости для **PulseAudio** с расширенными возможностями.

Для его установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install pavucontrol
```

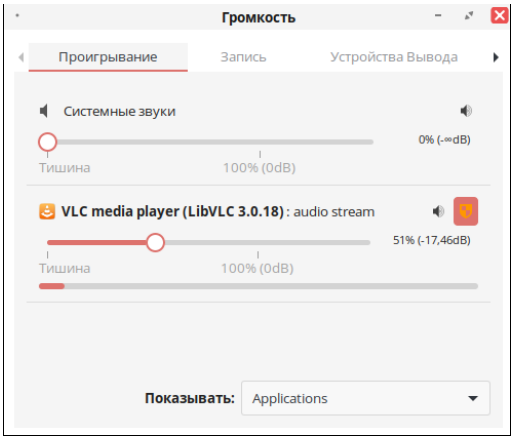
После установки запуск утилиты **pavucontrol** доступен из «**Главного меню**» — «**Аудио и Видео**» — «**Регулятор громкости PulseAudio**» или через терминал командой:

```
pavucontrol
```

Программа представляет из себя окно с пятью вкладками: «**Проигрывание**», «**Запись**», «**Устройства вывода**», «**Устройства ввода**» и «**Конфигурация**».

Вкладка «Проигрывание»

Данная вкладка позволяет регулировать уровень громкости запущенных приложений и системных звуков независимо друг от друга.



Для системных звуков доступен только ползунок регулировки громкости. Для приложений дополнительно добавляются настройки амплитуды сигнала. При нажатии на иконку динамика () звук выбранного канала будет заглушен. Нажатие на иконку щита () позволяет регулировать звуковые каналы устройства по отдельности.

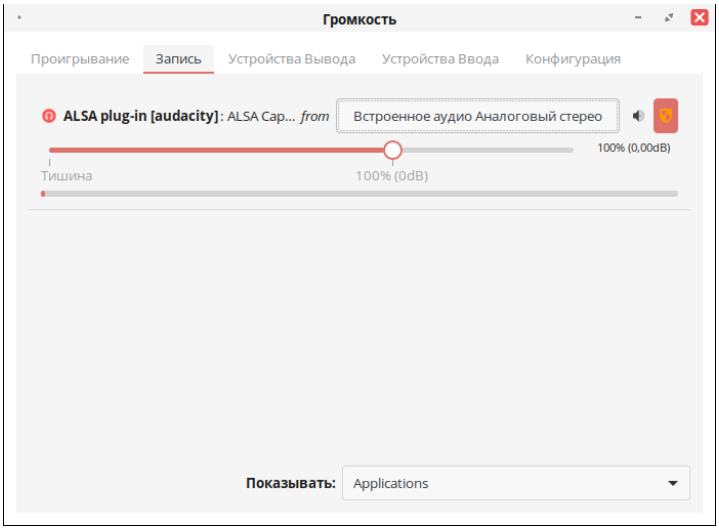


В нижней части окна есть выпадающий список, сортирующий выводимые на экран приложения. Список состоит из трёх пунктов:

- *Applications* — показывает потоки приложений в системе;
- Virtual Streams — показывает потоки виртуальных приложений;
- *All Streams* — показывает все звуковые потоки в системе.

Вкладка «Запись»

На этой вкладке можно настроить уровни чувствительности микрофона для каждого приложения в отдельности. Интерфейс по внешнему виду схож с интерфейсом во вкладке «**Проигрывание**». Каждое приложение с запущенной записью имеет свой ползунок для настройки чувствительности записи и показатель амплитуды сигнала.



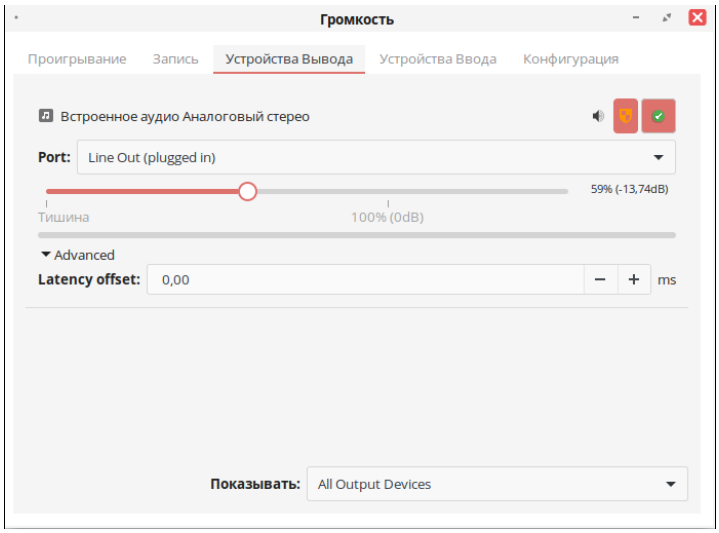
Нажатие на иконку динамика () останавливает запись звука в приложении. При нажатии на иконку щита () появляется возможность редактирования записи в разные каналы независимо друг от друга.

Выпадающий список «**Показывать**» предлагает те же параметры, что и на вкладке «**Проигрывание**».

Вкладка «Устройства вывода»

Вкладка «**Устройства вывода**» отвечает за настройку подключенных устройств для вывода звука. Для каждого подключенного устройства основным параметром для настройки является параметр **Port**. **Port** — позволяет выбрать, с какого порта будет работать

подключенное устройство. Например, **Line Out** отвечает за использование портов на материнской плате, а **Handphones** — портов на передней панели компьютера.



Звуковое устройство имеет ползунок для регулировки громкости, показатель амплитуды сигнала, иконку динамика ( ), чтобы заглушить звук, иконку щита ( ) для регулировки каналов устройства по отдельности. Также доступна кнопка «**Set As Fallback**» ( ), которая указывает на устройство, выбранное системой как устройство по умолчанию.

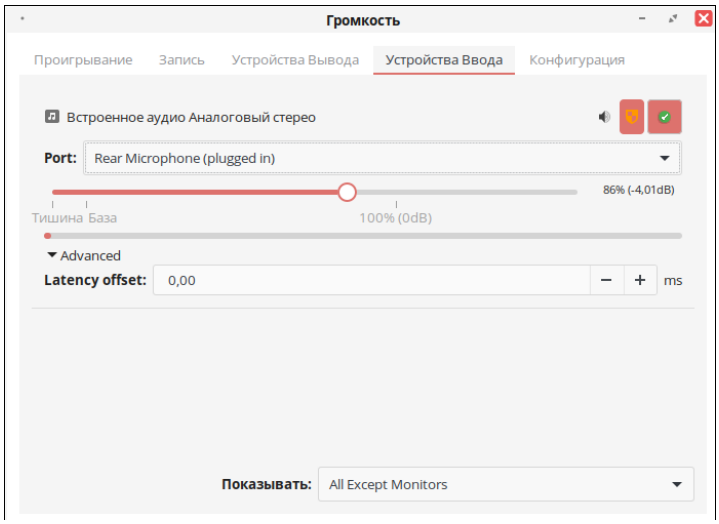
Параметр **Latency offset** отвечает за задержку воспроизведения звука. Он особенно полезен для тонкой настройки синхронизации между устройствами воспроизведения и устройствами ввода. Например, с помощью данной настройки можно избавиться от эффектов эха при разговорах по видеосвязи.

Выпадающий список «**Показывать**» имеет следующие варианты:

- *Hardware Output Devices* — показывает только физические устройства вывода;
- *Virtual Output Devices* — показывает только виртуальные устройства вывода;
- *All Output Devices* — показывает все устройства вывода.

Вкладка «Устройства ввода»

Вкладка для настройки устройств ввода схожа с содержимым вкладки «**Устройства вывода**» за исключением выпадающего списка «**Показывать**».



Выпадающий список «**Показывать**» имеет следующие параметры для сортировки звуковых устройств ввода:

- *Hardware Input Devices* — показывает только физические устройства ввода звука;
- *Virtual Input Devices* — показывает только виртуальные устройства ввода звука;
- *Monitors* — показывает только мониторы, подключённые через HDMI или DVI, т.к. они также являются звуковыми устройствами;
- *All Except Monitors* — показывает все устройства ввода звука, кроме мониторов;
- *All Input Devices* — показывает все устройства ввода звука.

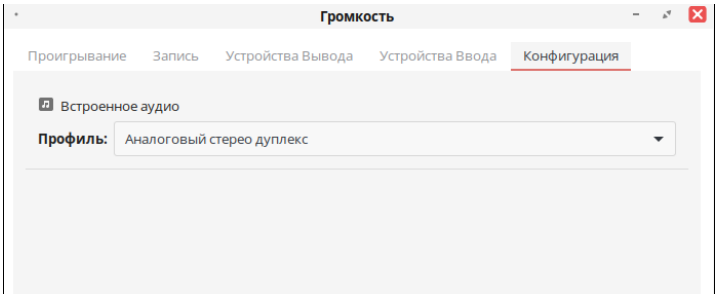
Вкладка «Конфигурация»

Вкладка «**Конфигурация**» содержит в себе только один параметр — **Профиль**. Выбор этого параметра работает аналогично такому же параметру в графическом интерфейсе **PulseAudio**:

- *Аналоговый стерео дуплекс* — работает с устройствами ввода и вывода звука одновременно;
- *Аналоговый стерео выход* — работает только с устройствами вывода звука;
- *Аналоговый стерео вход* — работает только с устройствами ввода звука;
- *Цифровой стерео выход* — позволяет получать более высокое качество звука, но не все устройства способны поддерживать этот режим;
- *Цифровой стерео выход + Аналоговый стерео вход* — позволяет использовать аналоговые устройства ввода звука одновременно с цифровыми устройствами вывода звука;
- *Выключено* — отключает звуковое устройство.

Примечание.

Список профилей может отличаться в зависимости от подключенных звуковых устройств.



Настройка звука с помощью PulseAudio через терминал

Настраивать звуковые устройства с помощью **PulseAudio** через терминал можно с помощью утилиты **pactl**. Чтобы вывести на экран список всех звуковых устройств с полной информацией, необходимо выполнить команду:

```
pactl list
```

Список всех звуковых устройств может быть очень длинным, поэтому программе стоит уточнять, о каких конкретно устройствах вы хотите вывести информацию на экран. Для этого нужно указать тип устройства.

Для получения информации по устройствам ввода звука, используйте команду:

```
pactl list sources
```

Для получения информации по устройствам вывода звука, используйте команду:

```
pactl list sinks
```

```
[user@localhost ~]$ pactl list sinks
Аудиоприёмник №1
        Состояние: SUSPENDED
        Имя: alsa_output.pci-0000_00_1b.0.analog-stereo
        Описание: Встроенное аудио Аналоговый стерео
        Драйвер: module-alsa-card.c
        Спецификация отсчётов: s16le 2-канальный 4410
        Схема каналов: front-left,front-right
        Модуль-владелец: 20
        Звук выключен: нет
        Громкость: front-left: 38673 /  59% / -13,74 dB,   front-right: 38673 /
 59% / -13,74 dB
                баланс 0,00
        Базовая громкость: 65536 / 100% / 0,00 dB
        Мониторный источник: alsa_output.pci-0000_00_1b.0.analog-stereo.monitor
        Задержка: 0 мкс, настроено на 0 мкс
        Флаги: HARDWARE HW_MUTE_CTRL HW_VOLUME_CTRL DECIBEL_VOLUME LATENCY
        Свойства:
                alsa.resolution_bits = "16"
                device.api = "alsa"
                device.class = "sound"
                alsa.class = "generic"
                alsa.subclass = "generic-mix"
```

Важным параметром устройства, который следует запомнить, является «Имя». Имя устройства очень часто используется для настройки с помощью других команд.

Смена профиля работы звуковых устройств

Список доступных профилей можно посмотреть в информации к звуковой карте, для этого в терминале необходимо выполнить следующую команду:

```
pactl list cards
```

В строке «**Профиль**» отображаются доступные имена профиля и их краткие описания. Звуковые профили позволяют переключать количество активных выходов и входов на звуковой карте. Самым необходимым параметром профиля является его имя, оно указано в начале каждой строки.

```
    Профили:
            input:analog-stereo: Аналоговый стерео вход (аудиоприёмников: 0, источников: 1, приоритет: 32833, доступен: да)
            output:analog-stereo: Аналоговый стерео выход (аудиоприёмников: 1, источников: 0, приоритет: 39268, доступен: да)
            output:analog-stereo+input:analog-stereo: Аналоговый стерео дуплекс (аудиоприёмников: 1, источников: 1, приоритет: 39333, доступен: да)
            output:analog-surround-40: Аналоговый объёмный 4.0 выход (аудиоприёмников: 1, источников: 0, приоритет: 33968, доступен: да)
            output:analog-surround-40+input:analog-stereo: Аналоговый объёмный 4.0 выход + Аналоговый стерео вход (аудиоприёмников: 1, источников: 1, приоритет: 34033, доступен: да)
            output:iec958-stereo: Цифровой стерео (IEC958) выход (аудиоприёмников: 1, источников: 0, приоритет: 38268, доступен: да)
            output:iec958-stereo+input:analog-stereo: Цифровой стерео (IEC958) выход + Аналоговый стерео вход (аудиоприёмников: 1, источников: 1, приоритет: 38333, доступен: да)
            off: Выключено (аудиоприёмников: 0, источников: 0, приоритет: 0, доступен: да)
```

Для смены звукового профиля используется команда вида:

```
pactl set-card-profile <имя_карты> <имя_профиля>
```

Управление громкостью звуков

Громкость в **PulseAudio** регулируется командой вида:

```
pactl set-sink-volume <имя_устройства_вывода> <уровень_громкости>
```

Стоит отметить, что уровень громкости вводится от **0** до **65535** (от 0% до 100%). Если попытаться выставить громкость больше, чем на 65535, то звук будет выводится с усилением (и будет указываться больше, чем 100%). Слишком большое усиление может искажать звук.

Приостановка звука

Источник звука можно заглушить командой вида:

```
pactl suspend-sink <имя_источника> true
```

Вернуть звук из источника можно, поменяв значение последнего параметра с **true** на **false**:

```
pactl suspend-sink <имя_источника> false
```

Также последний параметр можно задавать целыми числами, где **1** — это *true*, а **0** — *false*.

Похожими действиями можно и приостановить запись из устройства ввода:

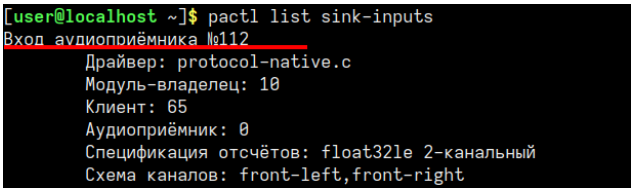
```
pactl suspend-source <имя_устройства_ввода> true
pactl suspend-source <имя_устройства_ввода> false
```

Громкость звука в приложениях

Чтобы изменять громкость звука для конкретного запущенного приложения, нужно сначала узнать для этого приложения номер входа аудиоприёмника (для приложений с проигрыванием звуков) или выход источника (для приложений с записью звука).

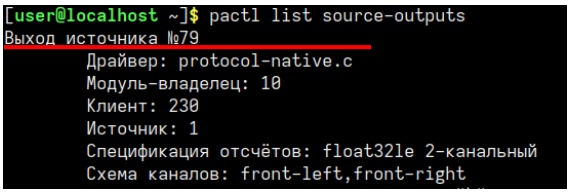
Чтобы узнать номера аудиоприёмников, в терминале необходимо выполнить команду:

```
pactl list sink-inputs
```

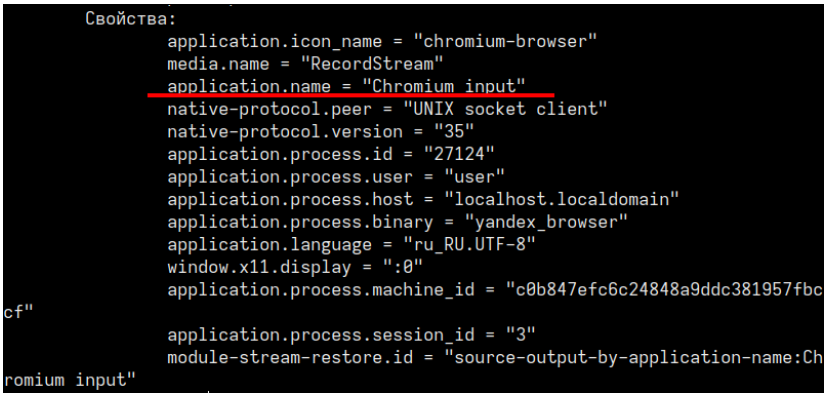


Для определения номера выхода источника команда будет выглядеть следующим образом:

```
pactl list source-outputs
```



У каждого входа аудиоприёмника и выхода источника есть свои свойства. Для определения номера конкретного приложения, следует обратить внимание на свойство «**application.name**», в котором указано название приложения:



Для регулировки звука следует использовать следующие команды:

```
pactl set-sink-input-volume <номер_входа_аудиоприёмника> <громкость_звука>
pactl set-source-output-volume <номер_выхода_источника> <громкость_звука>
```

Перемещение звукового потока

При необходимости перенести звук программы на другой источник звука (например, перенести звук с USB-колонок на наушники) можно воспользоваться следующей командой:

```
pactl move-sink-input <номер_входа_аудиоприёмника> <имя_источника>
```

Обратите внимание, что **pactl** не позволяет переносить звуки со всех приложений одновременно.

Audacity - редактор звуковых файлов

Установка
Описание программы
Запись звука
Сохранение результата
Звуковая дорожка
Обрезка треков
Объединение звука
Затухание и нарастание звука
Фильтрация шума

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** audacity-3.1.3-3

Audacity – мультиплатформенный редактор звуковых файлов, распространяемый на бесплатной основе.

Вы можете подробнее ознакомиться с работой редактора **audacity**, просмотрев наши обучающие видео:

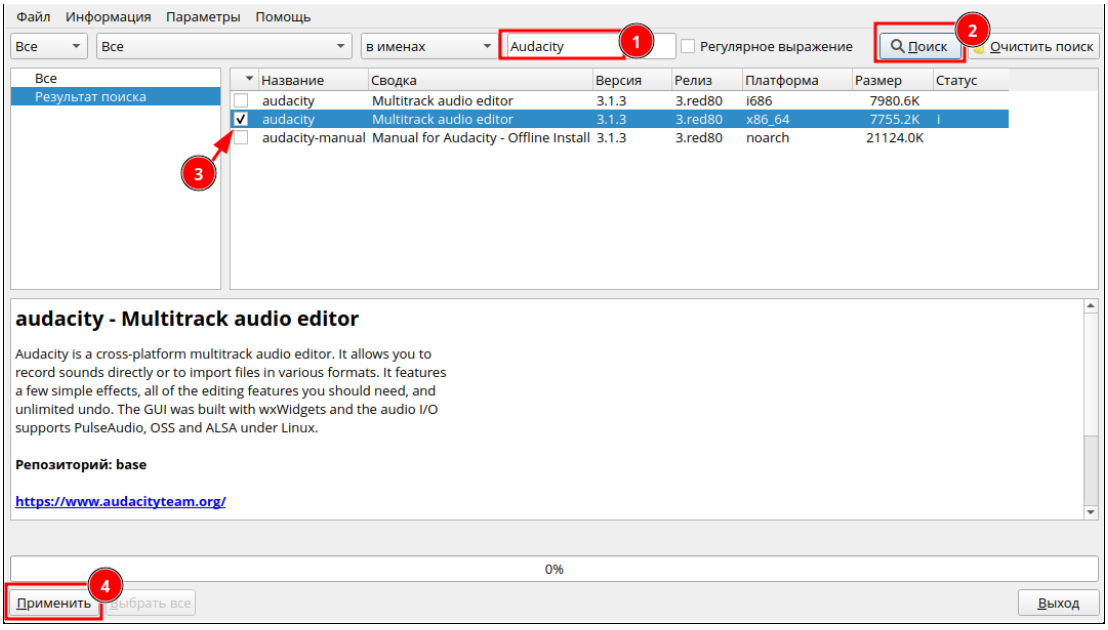
- на **RuTube** — Запись и обработка звука;
- в **Яндекс.Дзен** — Запись и обработка звука;
- в **VK Видео** — Запись и обработка звука.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**audacity**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install audacity
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Аудио и видео**» - «**Audacity**».

Описание программы

Звуковой редактор имеет простой и понятный интерфейс. В верхней части окна находятся кнопки управления записью, различные инструменты для работы и настройки устройств ввода. Все кнопки имеют поясняющие надписи, которые появляются при наведении курсора.

Рассмотрим их более подробно:

1. Вверху программы находится **основное меню** с доступными настройками как аудиодорожек, так и самой программы.



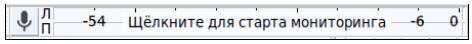
2. Крупными значками представлена **панель воспроизведения** с кнопками записи, начала воспроизведения, паузы и остановки, перехода в начало и конец трека.

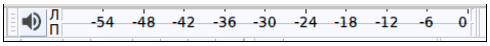


3. Следующая группа - **Инструменты** – выделение, масштабирование, отрисовка, сдвиг во времени и др.



4. **Индикация уровней звука** – сверху отражается уровень звука на входе (микрофон), снизу – на выходе (динамик).





5. **Панель отображения скорости воспроизведения**.



6. **Микшер** для управления параметрами звуковой карты. Правый устанавливает уровень сигнала на выходе (звуковая карта), а левый – на входе (микрофон).



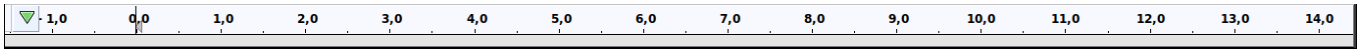
7. **Панель выбора устройств** - позволяет выбрать устройства, с которых будет вестись запись.



8. Раздел **Правка** – с помощью этой панели можно вырезать, копировать, заполнять тишиной выделенную зону, синхронизировать дорожки, масштабировать и др.



9. **Шкала времени** аудиодорожки.



Запись звука

Чаще всего **Audacity** используется для записи звука.

Перед записью необходимо выбрать устройство на **Панели выбора устройств**, с помощью которого будет записан аудиофрагмент, а затем запустить его мониторинг.

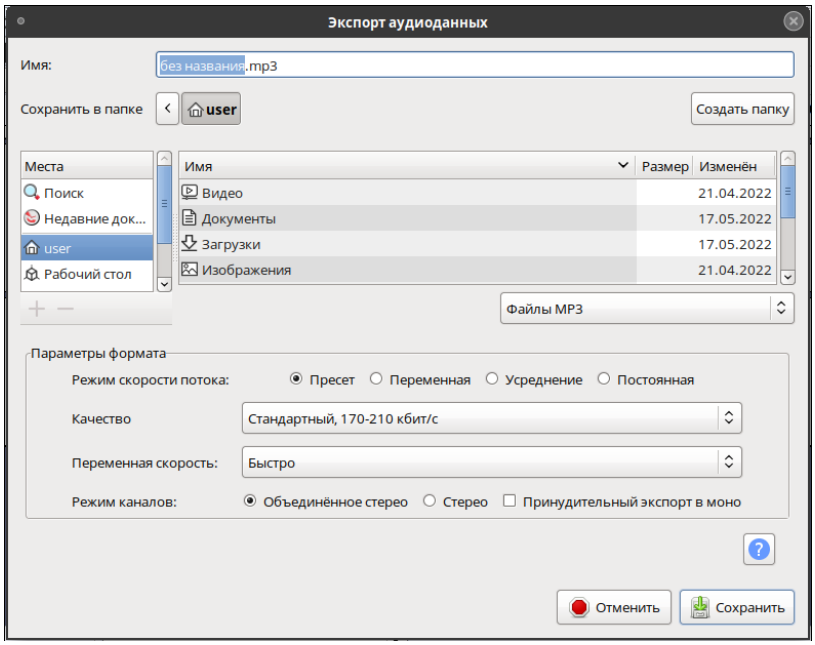
В выпадающем списке **Каналы записи** с **Панели выбора устройств** установите моно- или стереозапись.

Для начала записи нажмите на кнопку «**Запись**». После того как процесс окончен – нажмите «**Стоп**». Также запись можно приостановить, нажав на кнопку «**Пауза**», чтобы вскоре продолжить.

Прослушать записанный отрывок можно, нажав на кнопку «**Воспроизвести**».

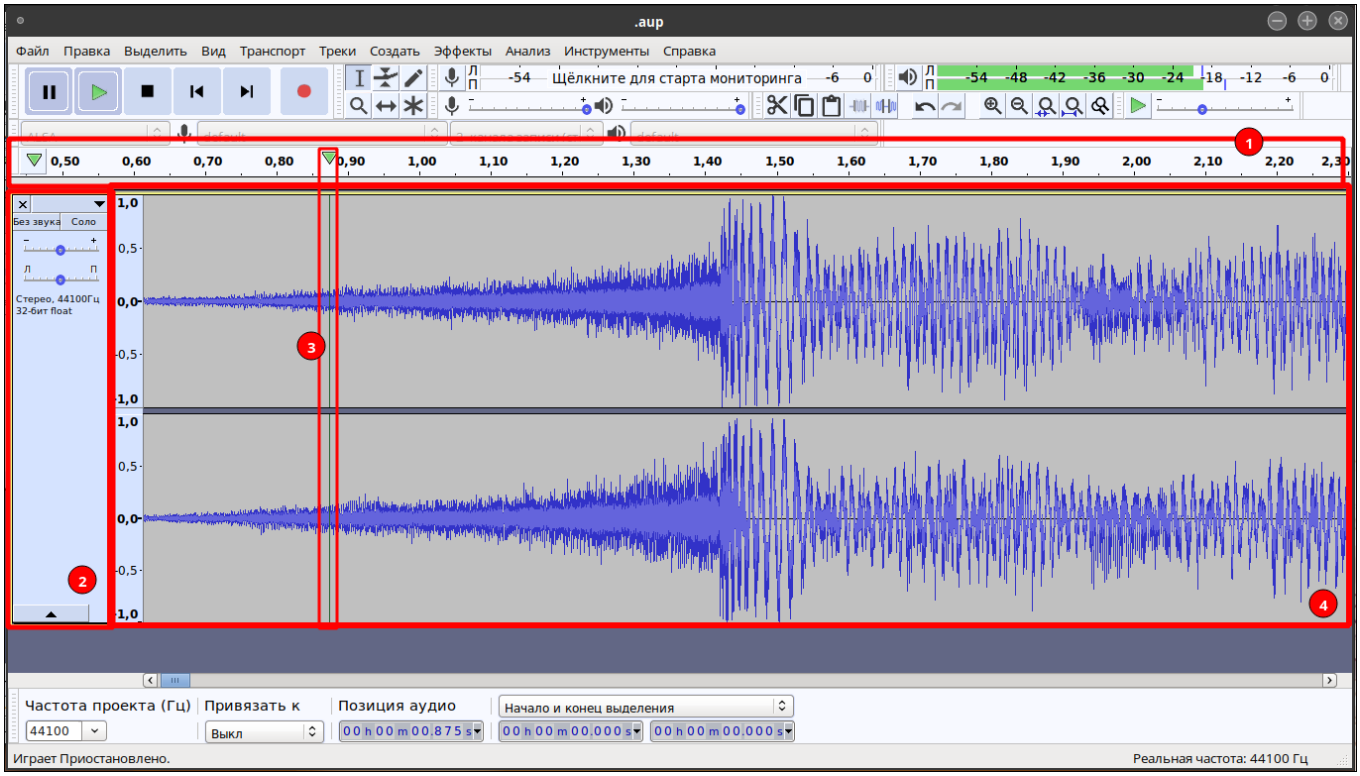
Сохранение результата

Для сохранения файла необходимо перейти в пункт меню «**Файл**» – «**Экспорт**», затем в открывшемся окне выбрать формат файла, качество, указать название и нажать кнопку «**Сохранить**».



Звуковая дорожка

Звуковая дорожка – это способ визуализации цифровой аудиозаписи. Она состоит из следующих компонентов:



1. **Шкала времени** – отображается вверху и показывает длительность трека.

2. **Свойства аудио** - здесь вы можете менять различные свойства аудиодорожки, отключается звучание текущей дорожки, изменяется вид её визуализации (волновая форма, спектр), цвета для окрашивания различных элементов трека. Также с помощью крестика вы можете удалять композиции.

3. **Скруббер** – линия, которая отмечает текущую позицию, из которой начнётся проигрывание файла.

4. **Аудиодорожка** - визуализирует изменение сигнала на протяжении записи.

Любые дополнительные аудиодорожки будут расположены ниже.

Обрезка треков

Audacity позволяет вырезать фрагменты аудиофайлов. Для удобства можно изменить масштаб с помощью инструмента увеличить или уменьшить ().

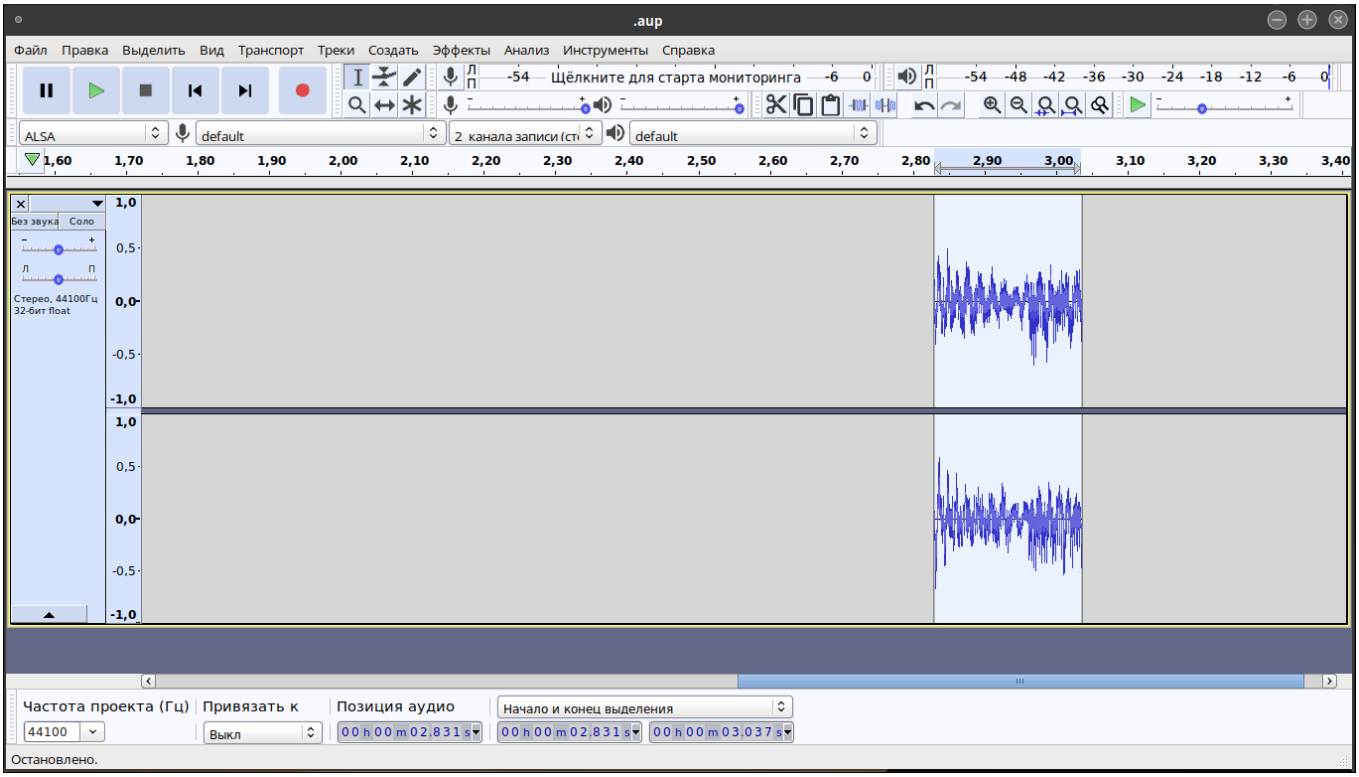
Прежде чем обрезать трек, нужно мышкой выделить необходимую часть и нажать кнопку «**Вырезать**». В таком случае вырезанная часть будет изъята из редактируемой аудиодорожки.

Однако если должен использоваться именно выделенный фрагмент, тогда для сохранения выделенного фрагмента аудиофайла необходимо выполнить следующие действия:

1. Переключитесь на инструмент «**Выделение**» и отметьте необходимую часть записи.

2. Откройте пункт меню «**Правка**» - «**Специальное удаление**» - «**Обрезать аудио**».

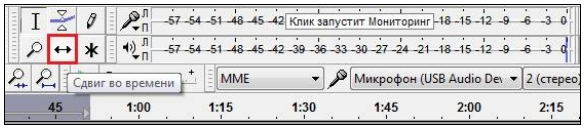
После этого останется доступен только выделенный фрагмент аудиофайла.

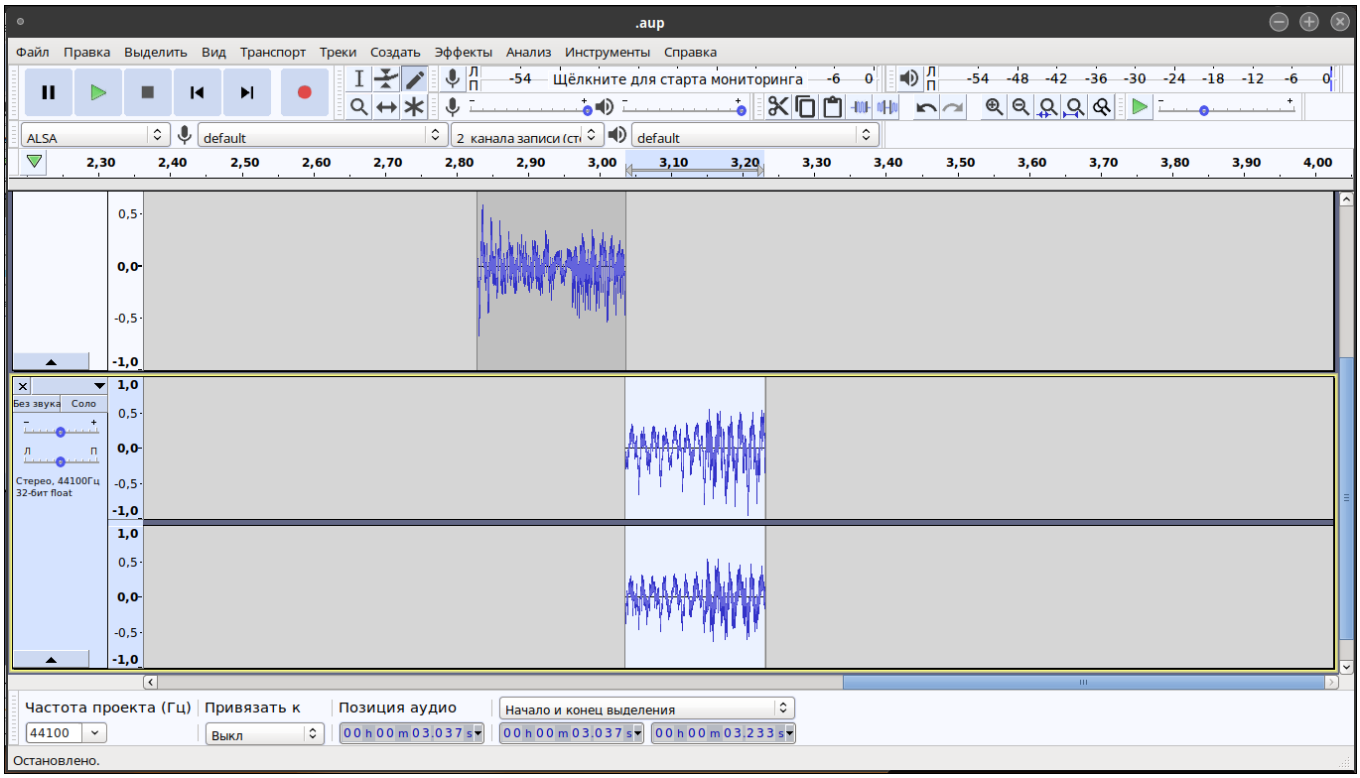


Объединение звука

Для соединения нескольких фрагментов аудио в один импортируйте («**Файл**» - «**Импорт**») все необходимые файлы и поместите их на разные дорожки.

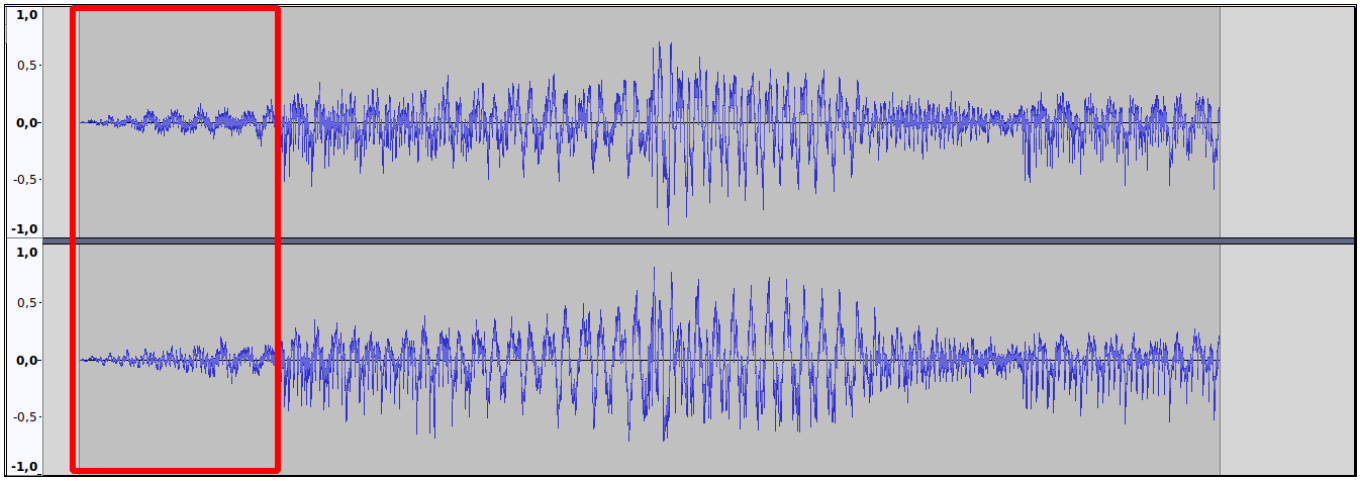
Затем, используя инструмент «**Сдвиг во времени**», необходимо переместить их визуально в нужном порядке.



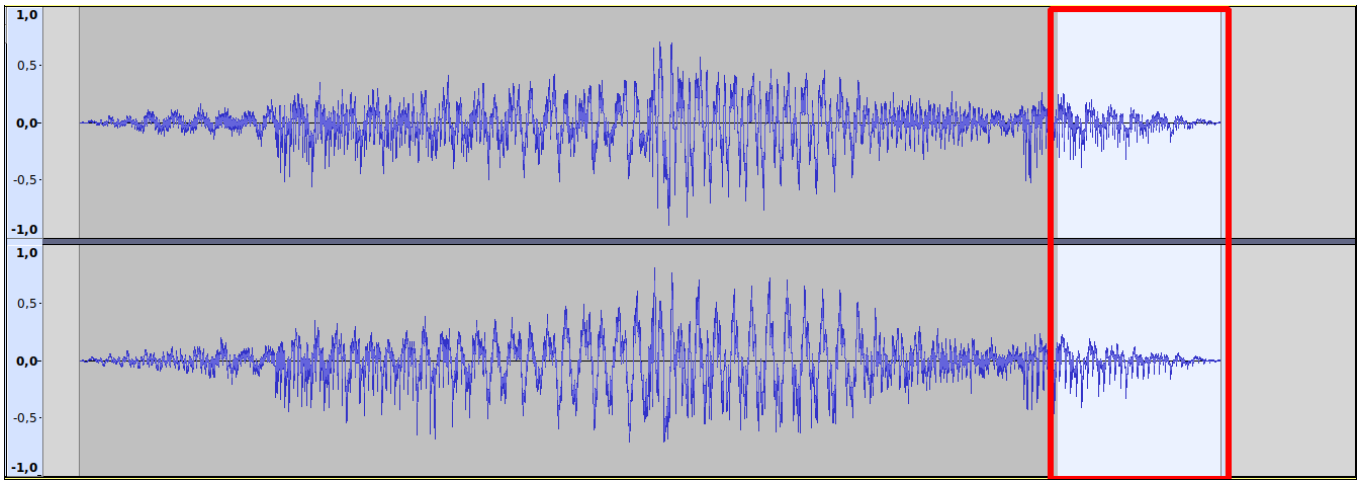


Затухание и нарастание звука

Рассмотрим создание нарастания в начале записи. Для этого выделите начальный фрагмент нужной длительности и перейдите в «**Эффекты**» – «**Фейд-вход**».



Также можно создать затухание — выделите фрагмент необходимой длины, затем перейдите в «**Эффекты**» и выберите «**Фейд-выход**».

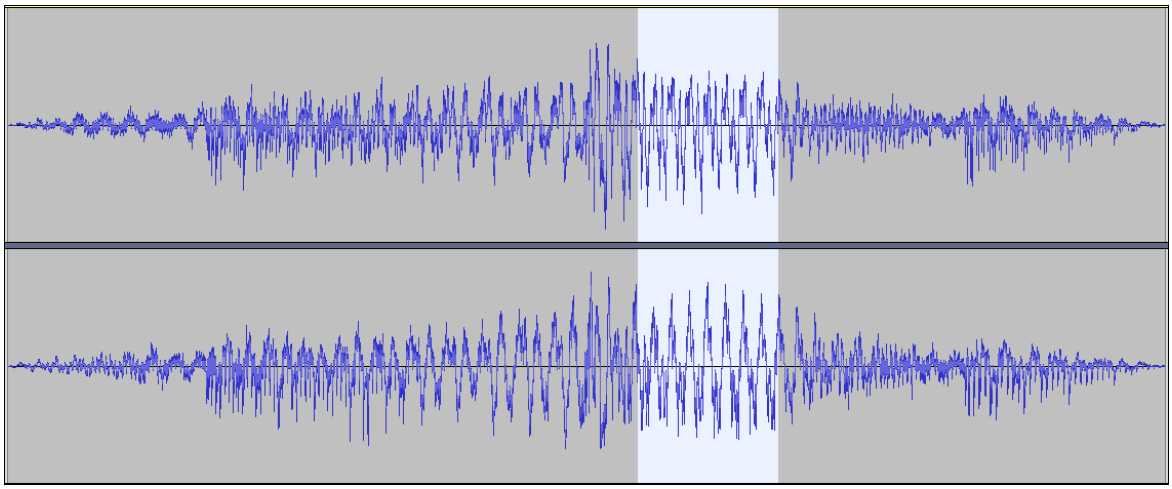


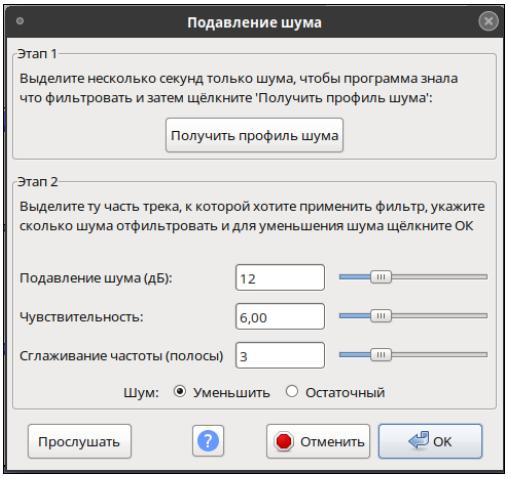
Фильтрация шума

Одним из самых полезных инструментов является фильтр шума. Бывает так, что при записи вы забыли отключить все посторонние предметы, которые издают шум, например, кулер компьютера. В таком случае на помощь приходят инструменты для очистки шума.

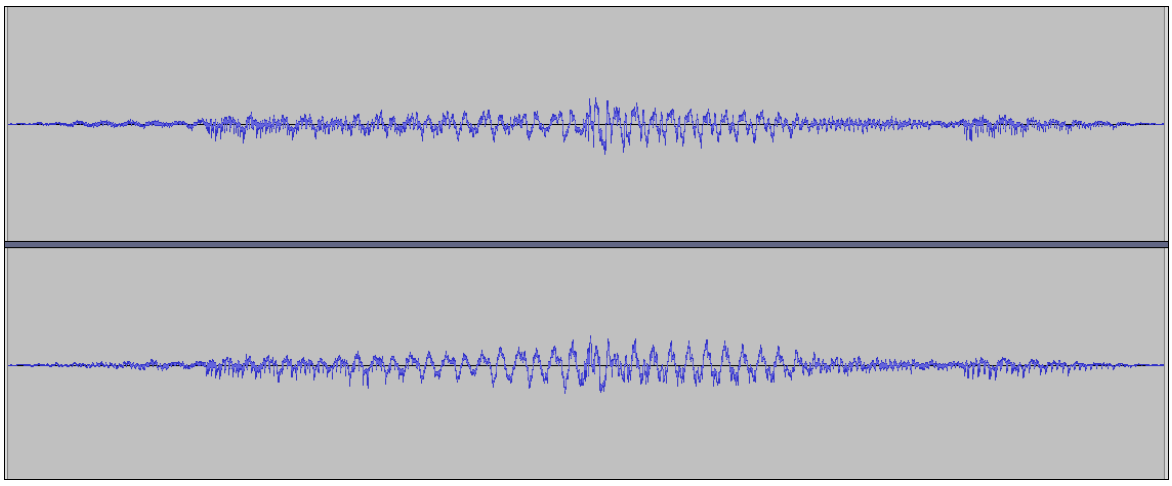
Удаление шумов, писка и других звуков совершается инструментами «**Подавление шума**» и «**Удаление щелчков**», расположенных на вкладке меню «**Эффекты**».

Сначала нужно «научить» функцию распознавать, где шум есть, а где его нет. Для этого выделите фрагмент аудио, где есть только шум, затем перейдите в пункт меню «**Эффекты**» и выберите пункт «**Подавление шума**». Будет открыто окно, в котором необходимо нажать на кнопку «**Получить профиль шума**», а также можно настроить чувствительность и другие параметры.





После этого выделите всю дорожку и еще раз откройте окно «**Подавление шума**», нажмите «**OK**», чтобы запустить процедуру удаления шума.



Посторонние шумы будут удалены со звуковой дорожки.

DeaDBeef - мультимедийный проигрыватель

Установка DeadBeef
Описание аудиопроигрователя DeadBeef
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: deadbeef-1.9.6-1

DeadBeef — это легковесный аудиоплеер, написанный на языках программирования *C* и *C++*.

Основные возможности **DeadBeef** включают:

- поддержку воспроизведения форматов MP3, OGG, FLAC/OGA, APE, WAV Pack, WV/ISO.WV, AAC/M4A, ALAS, MPC/MPP/MP+, TTA, WMA, SHN, SID, NSF, MOD, S3M, VTX, VGM/VGZ, PSF, MIDI, AUDIO CDF, а также других форматов, поддерживаемых через ffmpeg / libav;
- использование небольшого объема памяти и ресурсов процессора;
- поддержку расширения функционала с помощью плагинов;
- поддержку плейлистов CUE, M3U и PLS;
- поддержку воспроизведения интернет радио, а также обычных MP3 файлов по HTTP и HTTPS;
- глобальные горячие клавиши;
- поддержку чтения и записи ID3v1, ID3v2, APEv2, vorbiscomment;
- высокое качество передискретизации с помощью libsamplerate;
- воспроизведение с помощью Alsa, OSS и PulseAudio;
- встроенный скробблер last.fm/libre.fm;
- поддержку нескольких списков воспроизведения;
- 18-полосный эквалайзер;
- воспроизведение файлов прямо из архива;
- многоканальное воспроизведение аудиофайлов.

Установка DeadBeef

Для установки **DeadBeef** перейдите в сеанс пользователя **root**:

```
su -
```

Выполните команду:

```
dnf install deadbeef
```

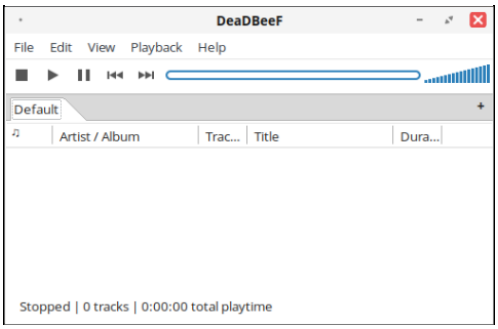
Завершите сеанс пользователя **root**:

```
exit
```

После установки запуск аудиопроигрывателя будет доступен из «**Главного меню**» — «**Аудио и видео**» — «**DeaDBeeF**» или через терминал (с правами непривилегированного пользователя):

```
deadbeef
```

Окно программы выглядит следующим образом:



Описание аудиопроигрователя DeadBeef

Аудиопроигрыватель имеет простой и понятный интерфейс. Рассмотрим подробнее элементы проигрывателя.

1. Вверху программы находится **основное меню**, состоящее из пяти основных пунктов**:** «**File**», «**Edit**», «**View**», «**Playback**», «**Help**».

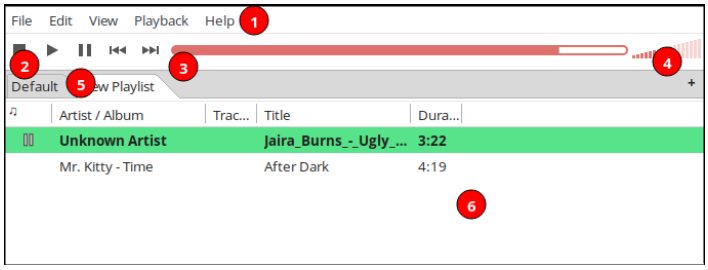
2. **Панель воспроизведения** с кнопками начала воспроизведения, паузы, остановки, перемотки трека.

3. Элемент **SeekBar** представляет собой слайдер, с помощью которого можно перемещаться по аудиозаписи.

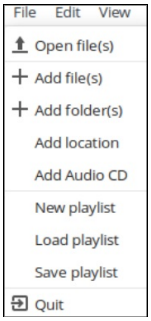
4. **Панель индикации** громкости звука показывает изменение уровня громкости.

5 . **Панель плейлистов** отображает список всех плейлистов, переключение между ними осуществляется однократным нажатием левой кнопки мыши.

6. Через **панель аудиозаписей** можно поменять порядок аудиозаписей или добавить новую композицию.

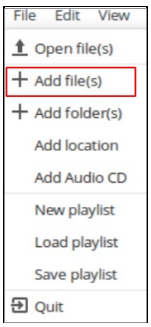


Из пункта меню «**File**» доступны базовые функции для добавления отдельных аудиозаписей и каталогов, а также URL списков трансляций медиапотока из интернета через пункт подменю «**Add location**».

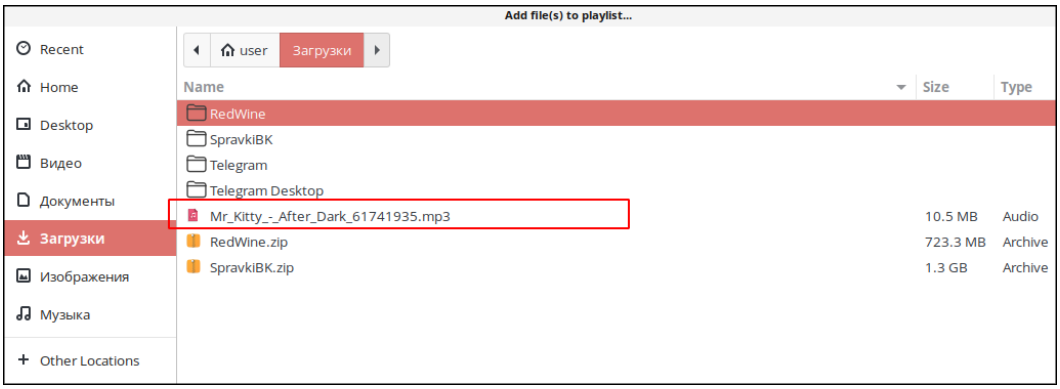


Функции «**Open file(s)**», «**Add file(s)**» и «**Add folder(s)**» отвечают за открытие файла, добавление аудиозаписи и папки с аудиозаписями.

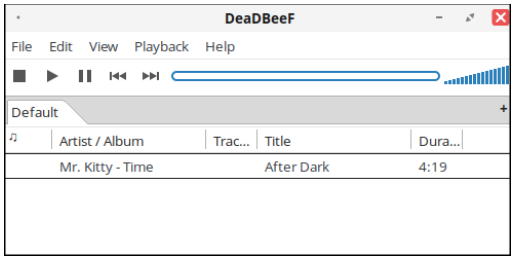
Для добавления аудиозаписи перейдите в меню «**File**» — подменю «**Add file(s)**».



Выберите файл, предварительно скачанный из интернета.



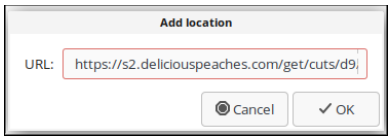
После этих действий аудиозапись должна появиться в вашем плейлисте.



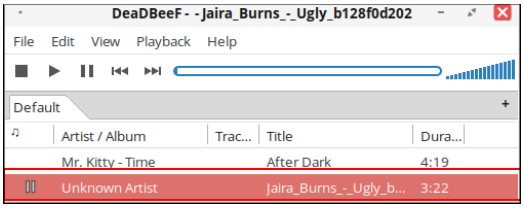
Функции «**Open file(s)**» и «**Add floder(s)**» работают по аналогии.

Функция «**Add location**» отвечает за добавление музыки по URL.

Для добавления музыки нужно скопировать прямую ссылку на выбранный трек и вставить ссылку в терминал, который появится после выбора функции «**Add location**».



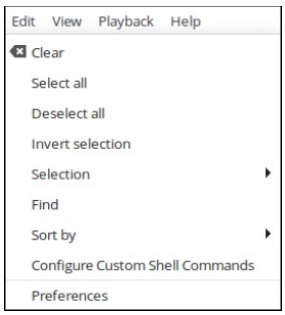
После выполненных действий аудиозапись отобразится в плейлисте проигрывателя.



Функция «**Add Audio CD**» добавляет в плейлист аудио из CD-проигрывателя.

Инструменты «**New playlist**», «**Load playlist**», «**Save playlist**» отвечают за манипуляции с плейлистами (создание нового, загрузку и сохранение плейлиста).

Функции меню «**Edit**» включают выделение, отмену выделения, удаление, обрезку аудиозаписей, сортировку по разным критериям.



Функции «**Select all**», «**Deselect all**» и «**Invert selection**» позволяют выделить все аудиозаписи, находящиеся в плейлисте, снять выделение со всех аудиозаписей, сделать выделенными те области, которые были ранее не выделенными.

Подменю «**Selection**» имеет 2 функции: «**Remove**» (позволяет удалить аудиозаписи из плейлиста) и «**Crop**» (позволяет вырезать их).

С помощью функции «**Find**» доступен быстрый поиск аудиозаписи по ее названию.

Функция «**Sort by**» отвечает за сортировку по различным критериям, например: «**Date**» — по дате, «**Artist**» — по авторам, «**Random**» — сортирует музыку рандомно (в случайном порядке).

С помощью функции «**Configure Custom Shell Commands**» можно создавать дополнительные команды (например, для записи радио или поиск данных об исполнителе и произведении).

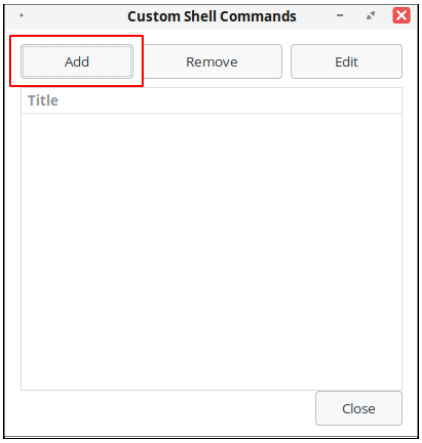
Пример работы

Создание команды для поиска данных об исполнителе.

1. Перейдите в меню «**Edit**» — подменю «**Configure Custom Shell Commands**».



2. Далее в появившемся окне нажмите кнопку «**Add**».



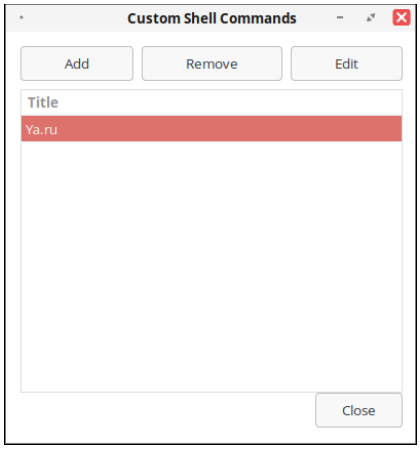
3. Добавьте информацию о поисковой системе, через которую будет происходить поиск данных (система может быть любая, рассмотрим на примере системы **Yandex**).

4. Укажите ссылку на поиск **ya.ru**: http://ya.ru/yandsearch.

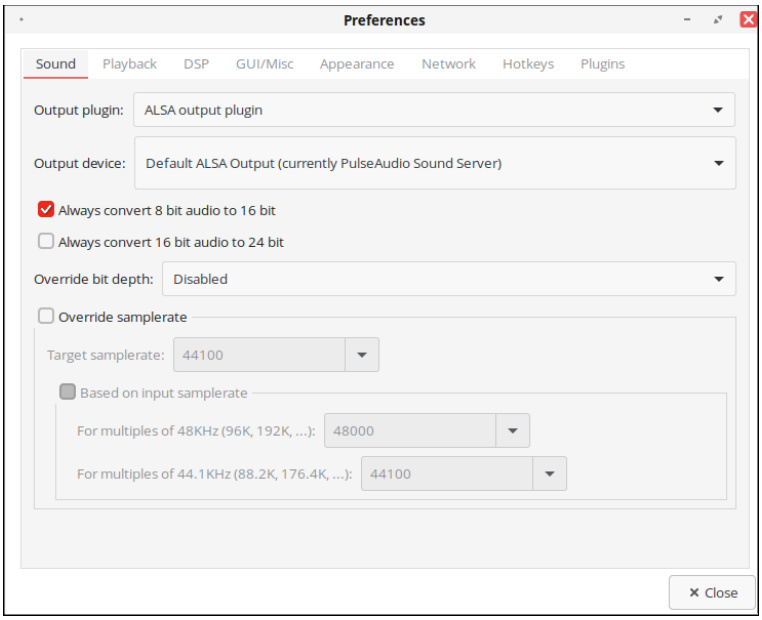
5. Отметьте флагами пункты «**Single Tracks**», «**Local**», «**Remote**».



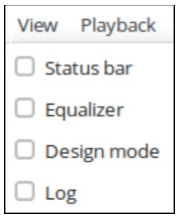
6. Далее команда появится в окне «**Configure Custom Shell Commands**».



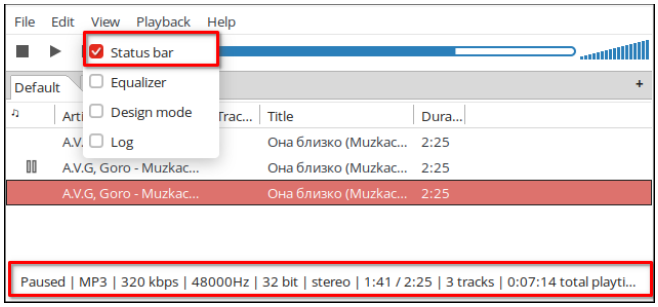
В меню «**Edit**» рассмотрим последний пункт «**Pereferenses**». Он содержит общие настройки приложения: от звучания музыки до кастомизации приложения.



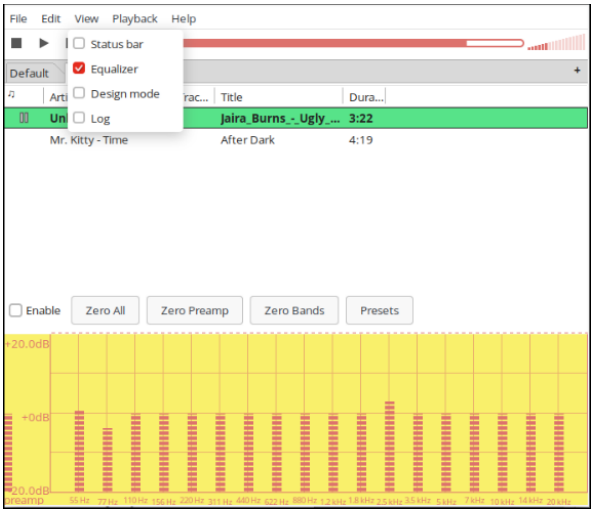
В меню «**View**» находятся параметры внешнего вида интерфейса приложения.



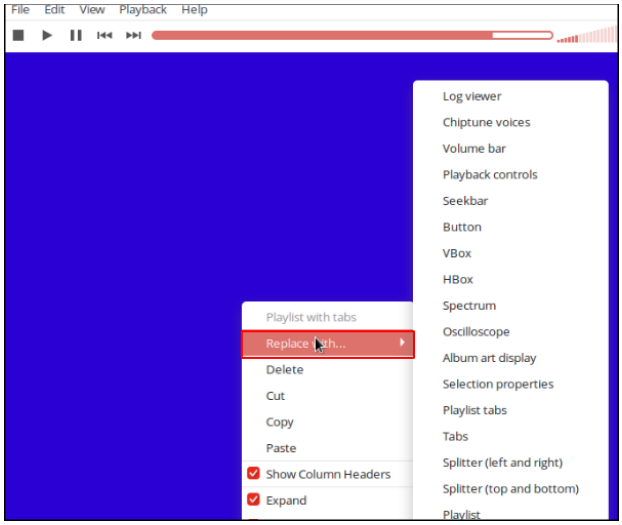
Функция «**Status bar**» добавляет информацию об статусе приложения.



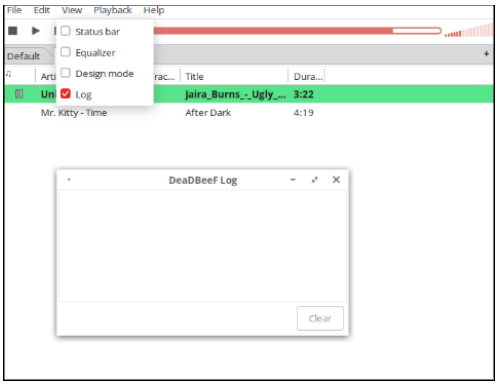
Функция «**Equaliser**» позволяет настраивать звучание музыки.



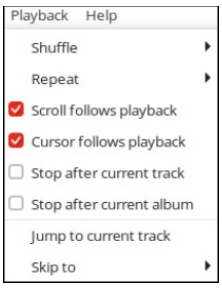
Функция «**Design mood**» добавляет на ПКМ возможность настройки внешнего вида приложения.



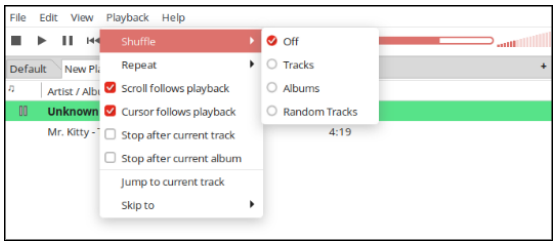
Функция «**Log**» отображает окно логов.



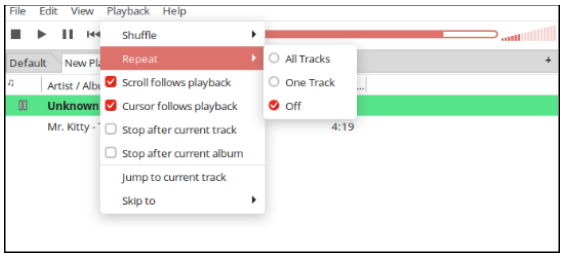
В меню «**Playback**» доступны параметры воспроизведения, повтора аудиозаписей, остановки после конкретной записи или ее пропуска.



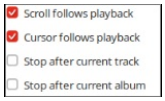
Функция «**Shuffle**» перемешивает воспроизведение аудиозаписей по трекам и альбомам.



Функция «**Repeat**» включает возможность повтора одной определенной аудиозаписи или всех записей, находящихся в плейлисте.

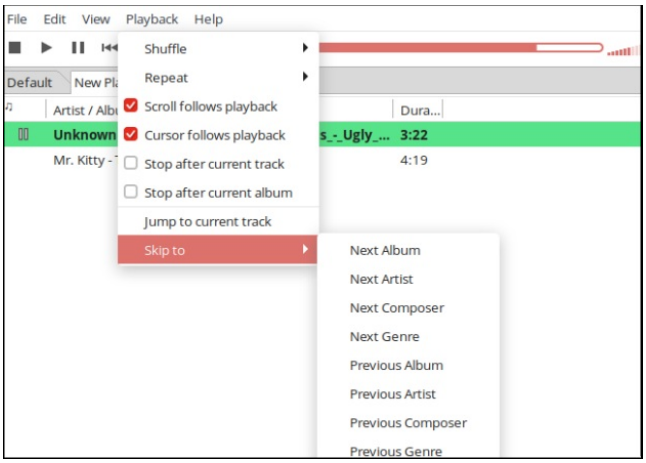


Установите флаги рядом с пунктами «**Scroll follows playback**», «**Cursor follows playback**», «**Stop after current track**», «**Stop after current album**» для отслеживания воспроизведения и остановки после определенных аудиозаписи или альбома.



Функция «**Jump to current track**» позволяет перейти к текущем треку.

С помощью «**Skip to**» имеется возможность пропуска треков по заданным параметрам.



Rhythmbox — музыкальный проигрыватель

Установка
Описание музыкального проигрывателя
Панель инструментов проигрывателя
Боковая панель
Источники воспроизведения
Настройки
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: rhythmbox-3.4.4

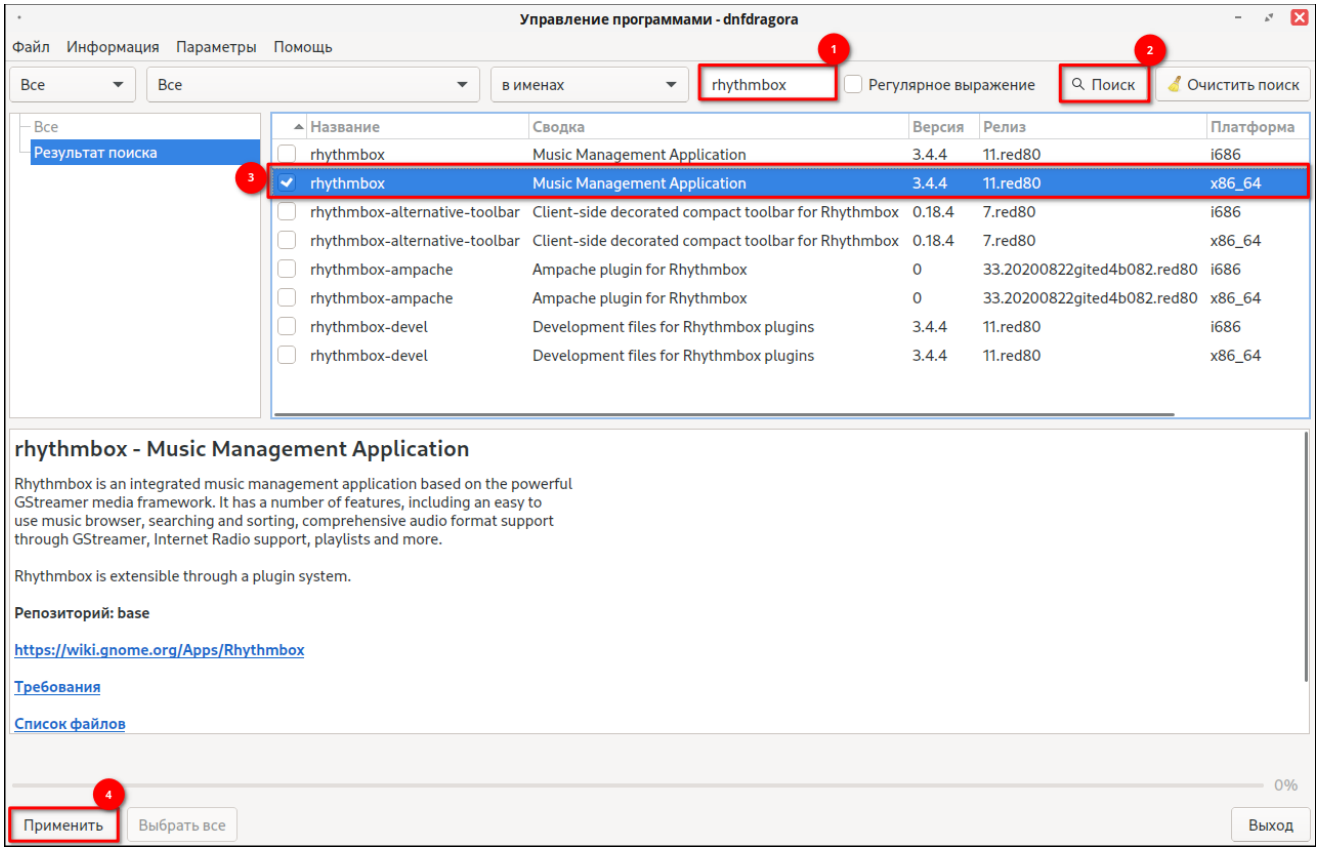
Rhythmbox — это музыкальный проигрыватель, который предлагает широкий спектр функций для управления музыкальной коллекцией. Он позволяет:

- импортировать музыку из различных источников;
- создавать и управлять списками воспроизведения;
- настроить **Rhythmbox** в качестве цифрового аудиосервера;
- подключаться к различным музыкальным сервисам, таким как Last.fm, Libre.fm и Magnatune, для получения рекомендаций;
- поддерживать различные форматы, включая MP3, OGG, FLAC;
- слушать интернет-радио;
- управлять музыкальной коллекцией с помощью простого и интуитивного интерфейса.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**rhythmbox**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install rhythmbox
```

После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**Rhythmbox**».

Описание музыкального проигрывателя

Окно музыкального проигрывателя выглядит следующим образом:



1 . **Панель инструментов** — предоставляет доступ к функциям проигрывателя и информации о текущем треке. Включает в себя ползунок времени, который отображает позицию воспроизведения трека; позволяет перейти к другой части трека. Также включает в себя ползунок громкости и кнопку для доступа к меню приложения.

2. **Боковая панель** — отображает список доступных источников. Может также отображать очередь воспроизведения.

3 . **Браузер** — позволяет просматривать и фильтровать треки в фонотеке по жанру, исполнителю или названию альбома. Также в браузер встроена функция поиска, с помощью которой можно просматривать только те треки, которые соответствуют нужным критериям.

4. **Список треков** — перечисляет треки из выбранного источника.

Панель инструментов проигрывателя

Область панели инструментов отображает подробности о воспроизводимой в данный момент дорожке.

 **Предыдущий** — переходит к предыдущему треку в плейлисте;

 **Воспроизвести** — начинает воспроизведение текущего трека;

 **Пауза** — приостанавливает воспроизведение текущего трека;

 **Следующий** — переходит к следующему треку в плейлисте;

Повторять — повторяет воспроизведение дорожек с начала списка после окончания последней дорожки;

 **В случайном порядке** — воспроизводит дорожки в случайном порядке.

При воспроизведении или выборе дорожки отображается её название, а под ним — имя исполнителя и название альбома.

Также отображается индикатор, показывающий ход воспроизведения трека, и ползунок времени.



Для регулирования громкости используйте колёсико мыши, прокручивая её вверх или вниз, пока указатель мыши находится над

кнопкой регулировки громкости  .

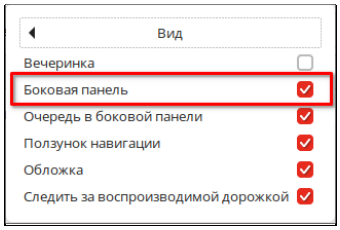
 **Основное меню** — открывает меню приложения, которое предоставляет доступ к различным опциям, таким как инструменты, параметры, справка.

Боковая панель

На боковой панели **Rhythmbox** можно получить доступ к следующим источникам:

- Музыка,
- Радио,
- Аудиодиски,
- Плейлисты,
- Подкасты,
- Сайты для обмена музыкой,
- Очереди воспроизведения.

Можно включить/выключить боковую панель, нажав кнопку  и включив/отключив флаг для параметра «**Вид**» — «**Боковая панель**».

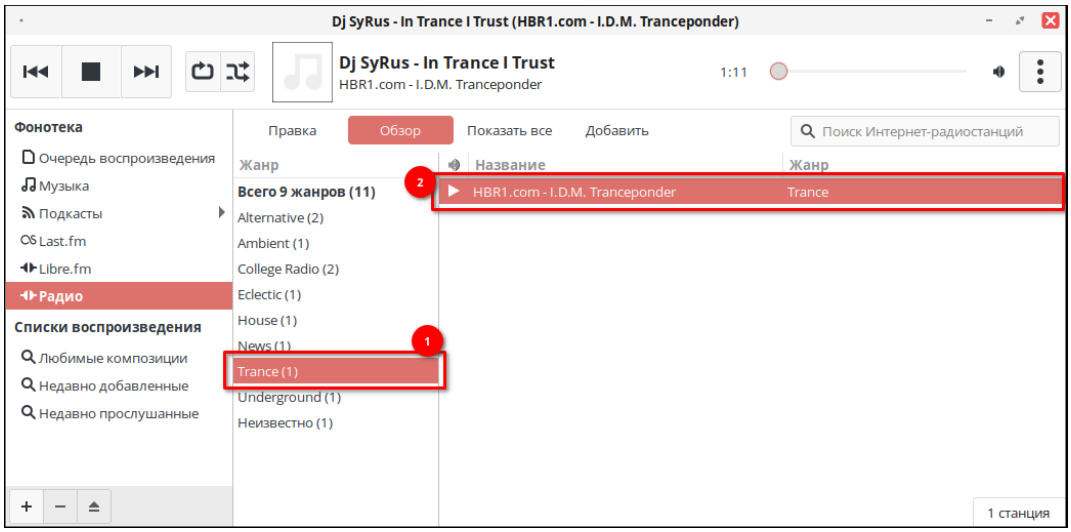


Источники воспроизведения

Источник «Радио»

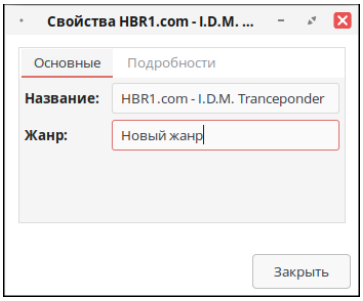
Для прослушивания потокового аудио из Интернета можно использовать источник «**Радио**».

Список радиостанций появится в различных категориях. Выберите жанр и радиостанцию, которую хотите слушать, дважды кликнув по ней.



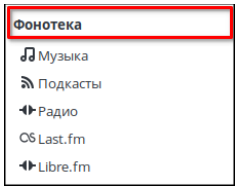
Для добавления новой радиостанции нажмите «**Добавить**» и введите URL-адрес радиостанции.

Для изменения жанра радиостанции щелкните на радиостанцию ПКМ и выберите «**Свойства**». В свойствах измените жанр на новый.



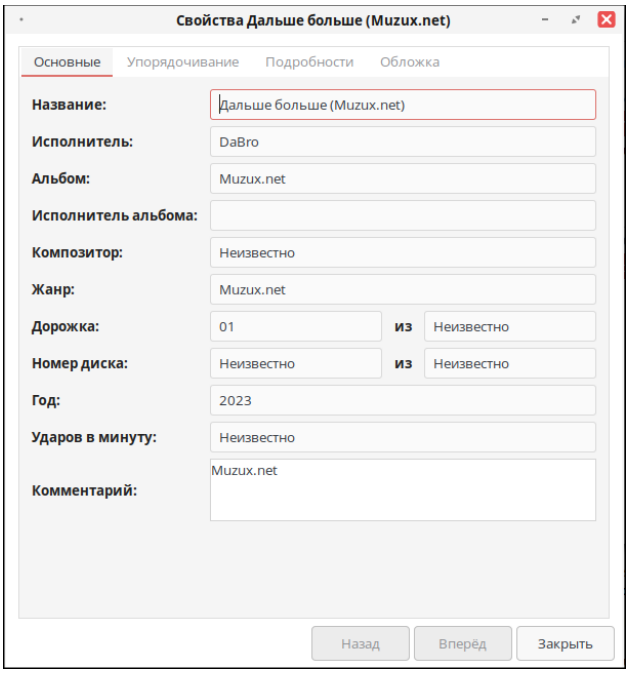
Источник «Фонотека»

Фонотека — основной источник, который содержит музыкальные файлы, импортированные в **Rhythmbox**.



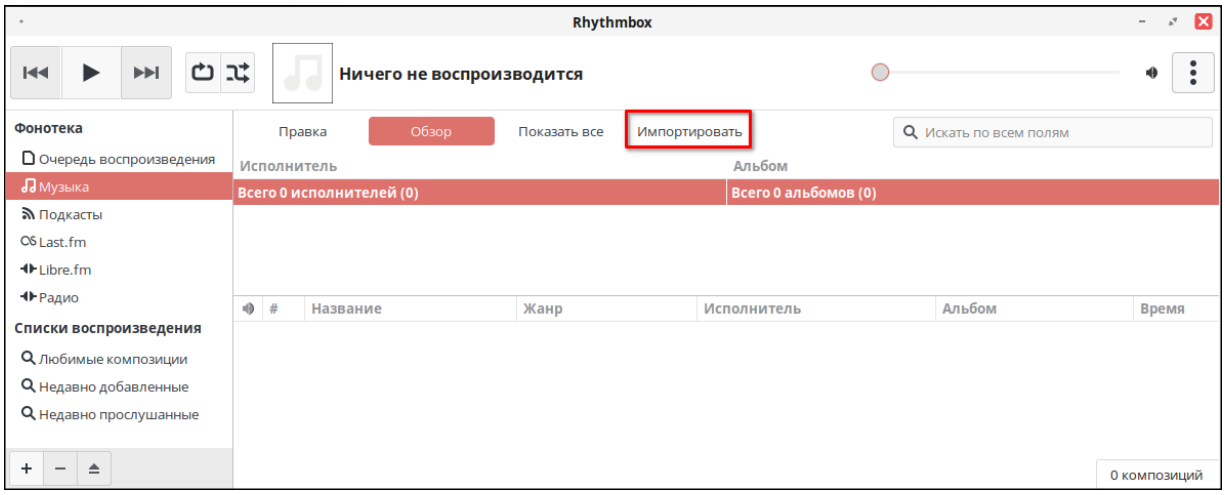
Библиотека может содержать не только музыкальные файлы, которые физически находятся на компьютере пользователя, но и музыкальные файлы, доступные через сетевые службы.

Файлы отображаются в списке треков вместе с информацией, сохранённой в тегах. Теги можно изменить, щёлкнув по файлу ПКМ, затем выбрав пункт «**Свойства**» и изменив информацию в появившемся окне.

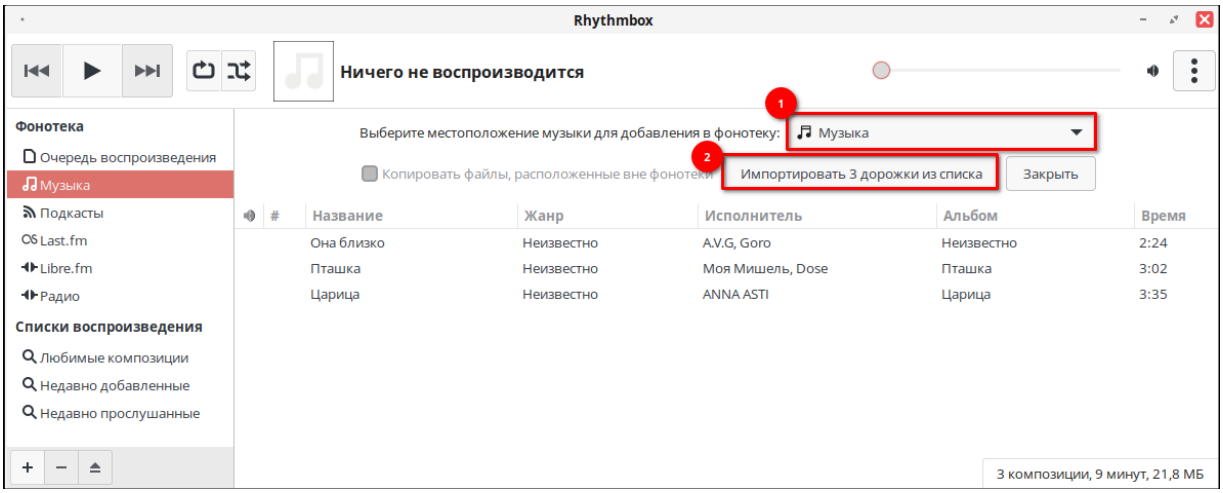


Для добавления дорожек можно воспользоваться следующими способами.

1. Для импорта нескольких музыкальных файлов в фонотеку нажмите «**Импортировать**» в браузере.



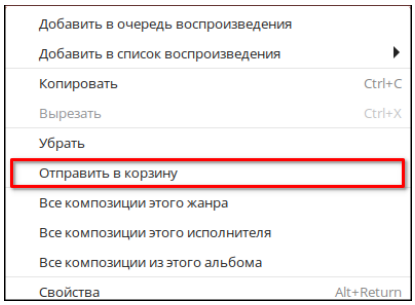
Выберите местоположение музыки, выберите папку в окне выбора файлов и нажмите кнопку «**Открыть**». Далее нажмите «**Импортировать дорожки из списка**», будут импортированы все музыкальные файлы, находящиеся в папке.



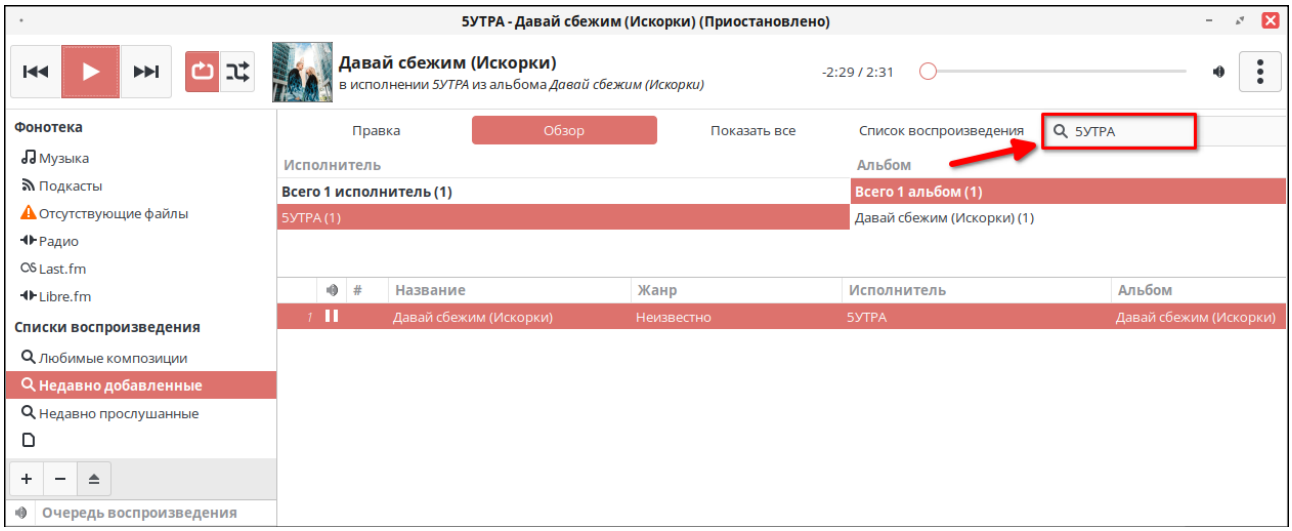
2. Переместите файлы путём перетаскивания из файлового менеджера в окно **Rhythmbox**.

Для удаления дорожки из фонотеки нажмите ПКМ на дорожку и выберите «**Убрать**».

Для удаления дорожки из фонотеки и с диска нажмите ПКМ на дорожку и выберите «**Отправить в корзину**». Дорожка будет удалена, а файл будет перемещён в корзину файлового менеджера.

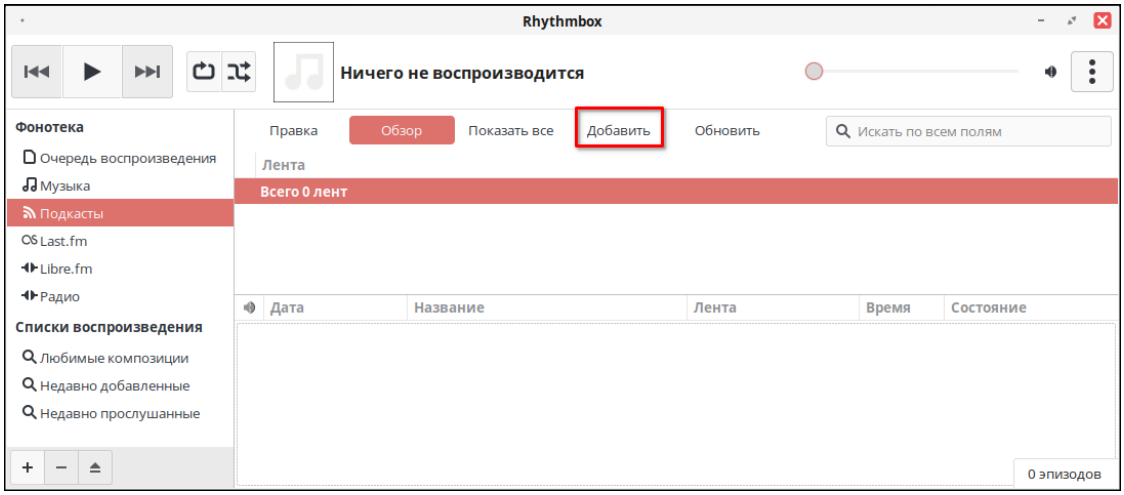


Для поиска дорожек по ключевому слову используйте поле поиска. Введите текст в поле поиска, и по мере ввода будут отображаться только дорожки, соответствующие введенному тексту.

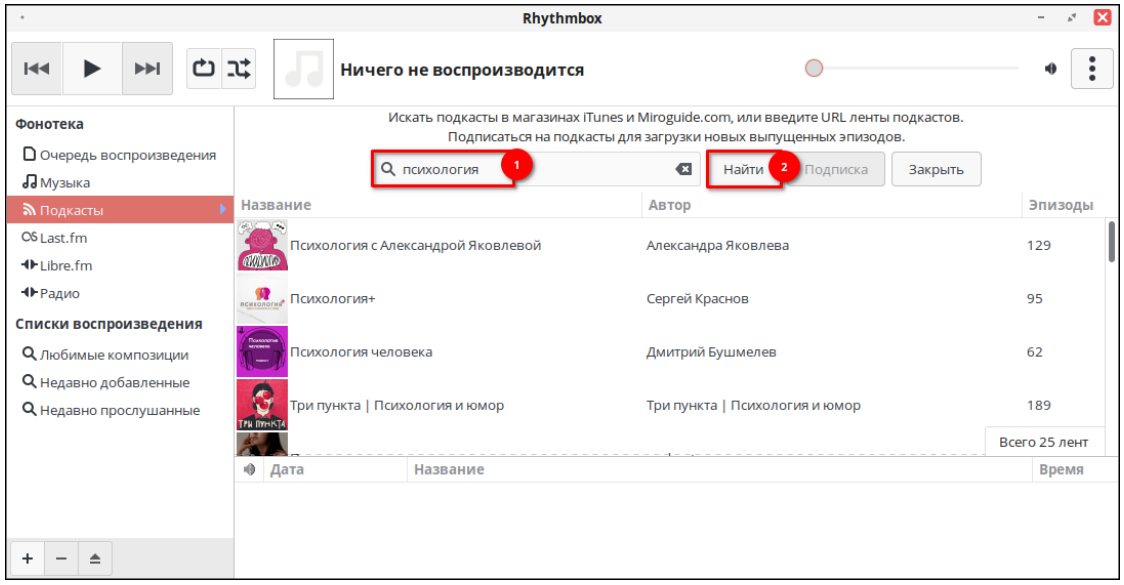


Источник «Подкасты»

В источнике «**Подкасты**» можно подписаться на каналы подкастов и при появлении новых эпизодов получать уведомления о них. Для добавления подкаста выберите «**Добавить**» в верхней части окна подкастов.



В появившемся окне в строке поиска введите ключевое слово (1) или URL-адрес подкаста и нажмите «**Найти**» (2). **Rhythmbox** получит список подкастов и эпизодов.



Выберите подкасты, на которые хотите подписаться, и нажмите «**Подписка**». Для отображения списка подкастов и доступных выпусков нажмите «**Закрыть**».

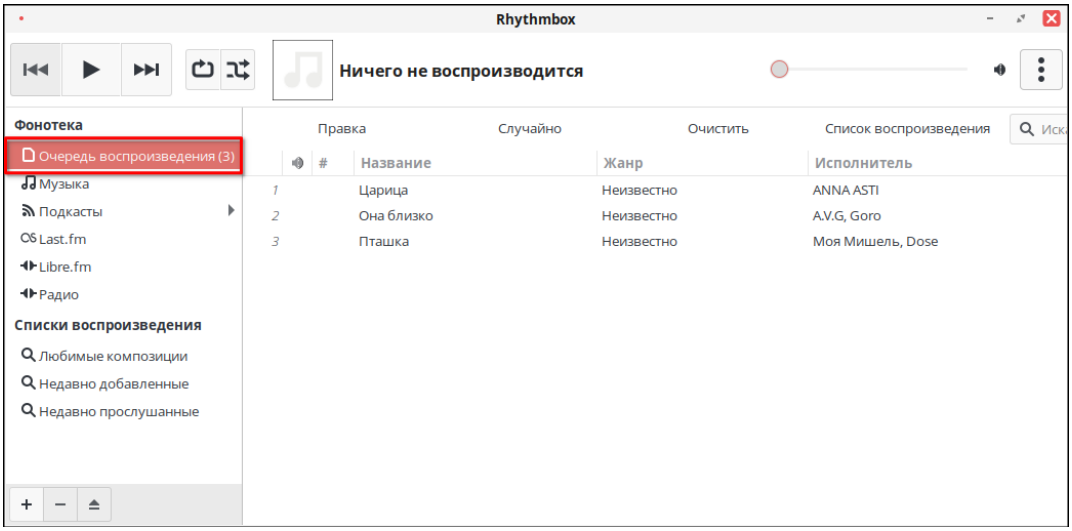
Для удаления подкаста щёлкните ПКМ на названии канала подкастов и выберите «**Удалить ленту подкастов**», затем выберите

«**Удалить только ленту**» или выберите «**Удалить ленту и файлы**».

Для обновления подкастов щёлкните ПКМ на источнике «**Подкасты**» и выберите «**Обновить ленту подкастов**» или «**Обновить все ленты**».

Источник «Очередь воспроизведения»

Очередь воспроизведения — это источник, предназначенный для временного хранения треков. При добавлении трека в очередь воспроизведения музыкальный проигрыватель **Rhythmbox** автоматически переключается на этот источник после воспроизведения трека.



После воспроизведения трека он будет автоматически удалён из источника очереди воспроизведения. Как только очередь воспроизведения опустеет, музыкальный проигрыватель **Rhythmbox** перейдёт к источнику, который был воспроизведён ранее.

Источник «Звуковой компакт-диск»

Музыкальный проигрыватель **Rhythmbox** может воспроизводить и записывать аудиодиски.

Когда аудиодиск будет вставлен, он появится на боковой панели, а треки можно будет просмотреть в главном окне **Rhythmbox**.

Для управления воспроизведением, приостановкой и перемоткой используйте тот же порядок действий, что и в фонотеке.

Для записи на диск треков вставьте чистый компакт-диск, нажмите кнопку «**Создать**», начнётся процесс записи.

Источник «Портативные звуковые проигрыватели»

Rhythmbox может определять, когда портативный аудиоплеер подключен к компьютеру, и считывать сохранённые на нем треки.

При подключении портативного аудиоплеера к компьютеру **Rhythmbox** может автоматически обнаружить его и отобразить значок плеера на боковой панели. Этот источник работает так же, как и источник из библиотеки, пользователи могут воспроизводить музыку с плеера, как если бы она была сохранена на их компьютере.

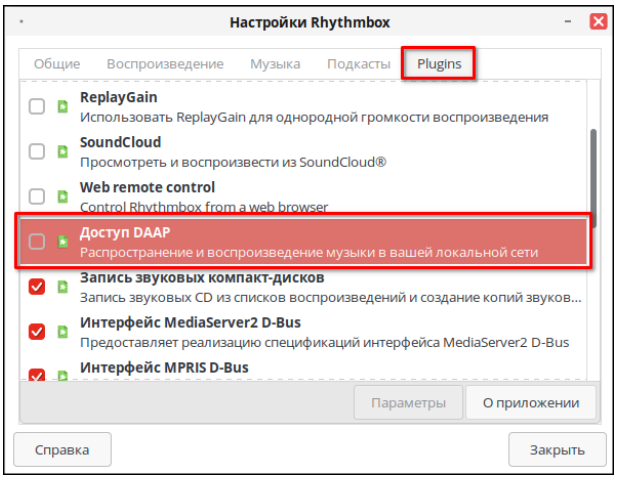
Rhythmbox совместим с большинством портативных аудиоплееров, включая Apple iPod, MTP-плееры и проигрыватели с накопителем данных.

Источник «Общий ресурс DAAP»

DAAP (Digital Audio Access Protocol) — это сетевой протокол для обмена цифровой музыкой между устройствами и приложениями. **Rhythmbox** поддерживает протокол DAAP, что позволяет пользователям обмениваться музыкой не только между собой, но и с пользователями других приложений, совместимых с DAAP, таких как iTunes.

После запуска **Rhythmbox** автоматически ищет общие ресурсы DAAP в локальной сети и отображает их в боковой панели. При включении общего доступа **Rhythmbox** публикует свою медиатеку и списки воспроизведения, что позволяет другим пользователям слушать музыку пользователя, а пользователю — слушать музыку, хранящуюся на компьютерах других пользователей.

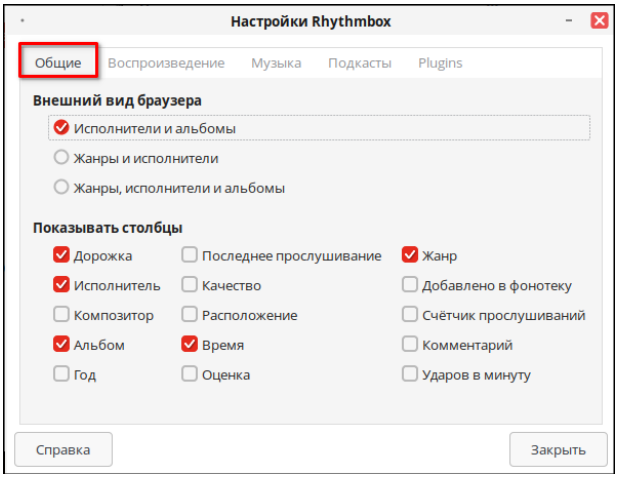
Для отключения функции обмена музыкой по протоколу DAAP в **Rhythmbox** перейдите в меню  — «**Параметры**». На вкладке «**Plugins**» снимите флаг «**Доступ DAAP**».



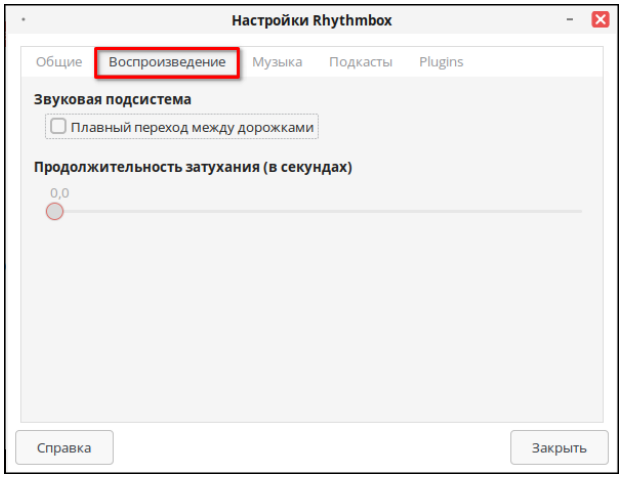
Настройки

Для настройки **Rhythmbox** перейдите в меню — «**Параметры**».

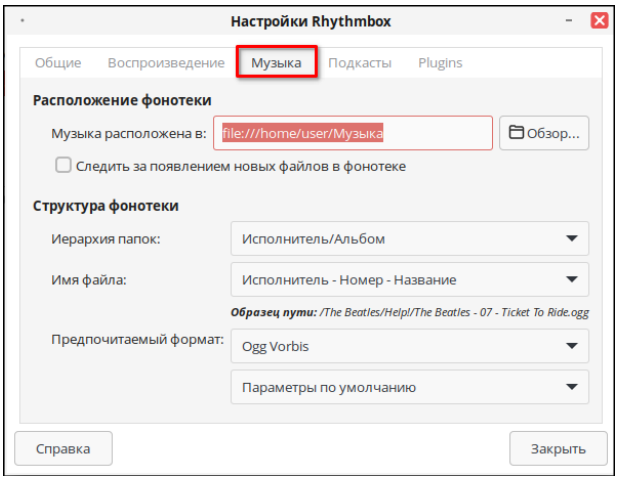
На вкладке «**Общие**» выберите столбцы для отображения в **Rhythmbox**.



На вкладке «**Воспроизведение**» задайте переходы между дорожками и установите продолжительность затухания.



На вкладке «**Музыка**» выберите расположение и структуру фонотеки. Задайте папку, за наличием новых композиций в которой будет следить **Rhythmbox**. Для отключения функции отслеживания новых файлов уберите флаг «**Следить за появлением новых файлов в фонотеке**».



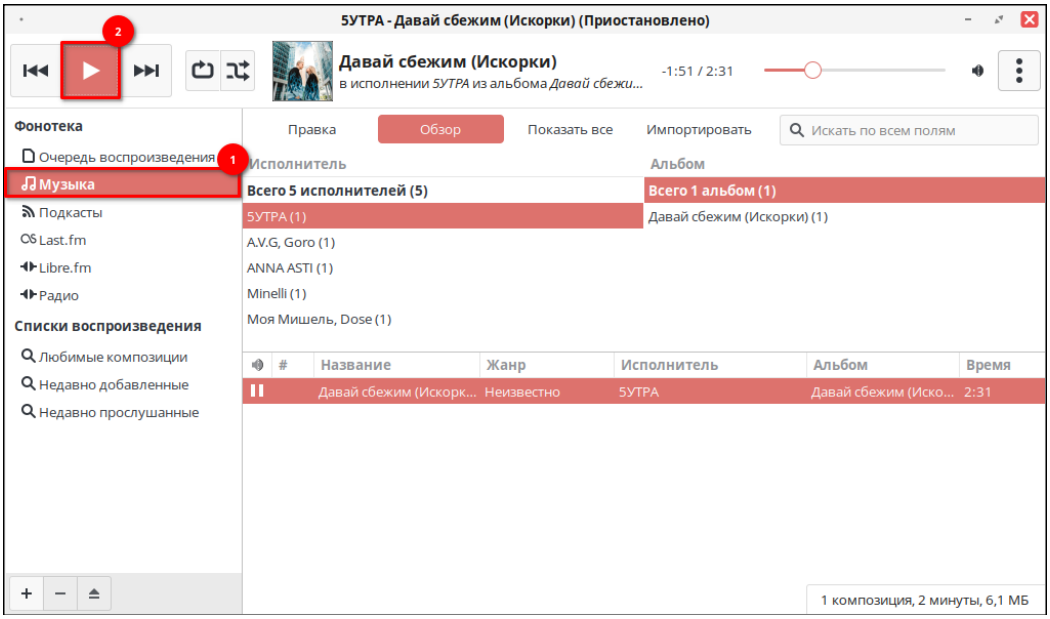
На вкладке «**Подкасты**» настройте параметры загрузки подкастов и частоту проверки новых эпизодов.

Для добавления на боковую панель дополнительных источников на вкладке «**Plugins**» отметьте флагом нужные плагины.

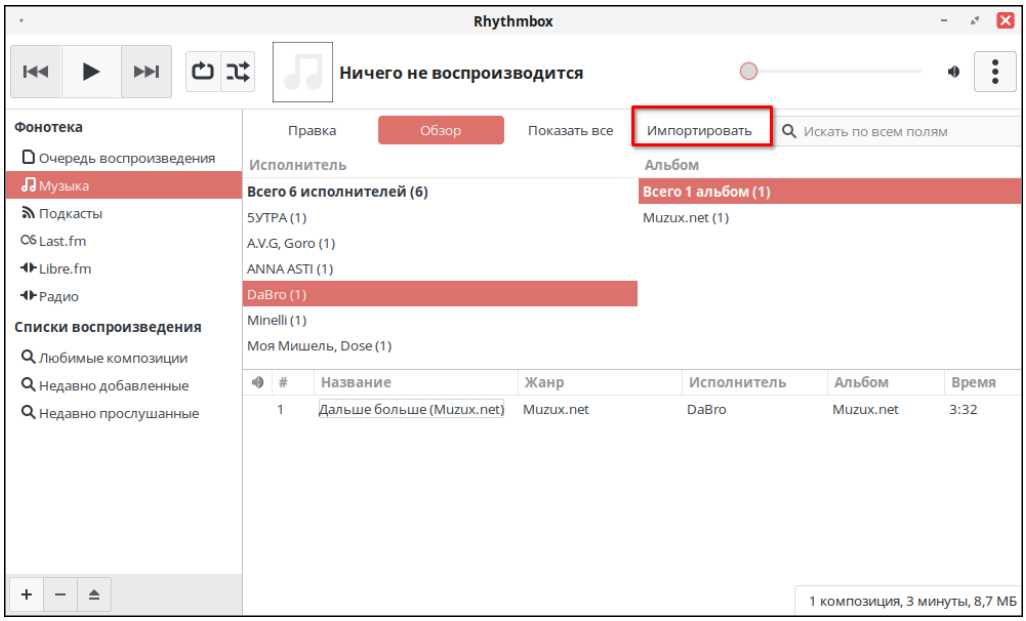
На боковой панели появятся дополнительные источники:

Пример работы

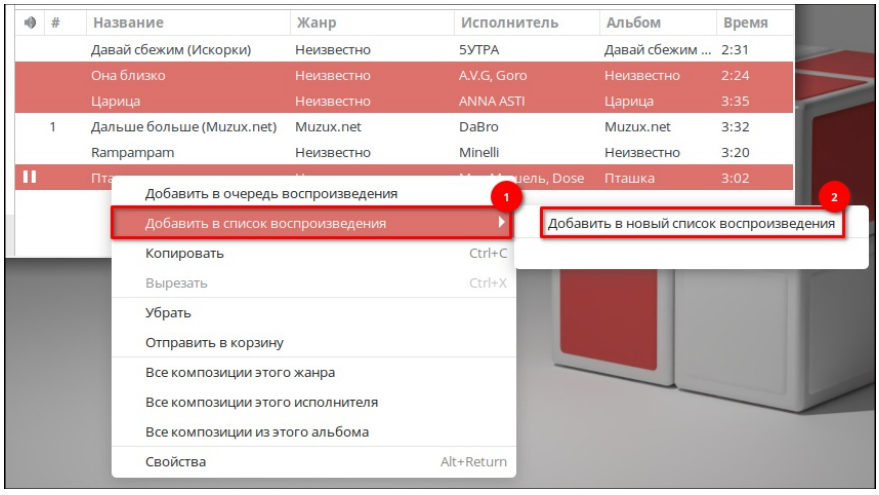
1. Для воспроизведения музыки с помощью **Rhythmbox** необходимо выбрать источник музыки на боковой панели и нажать «**Воспроизвести**» (или двойным нажатием щелкните по треку ЛКМ).



2. Для добавления музыки в фонотеку выберите «**Импортировать**» или перетащите файлы в окно **Rhythmbox**. После импорта файлов они появятся в соответствующих панелях.

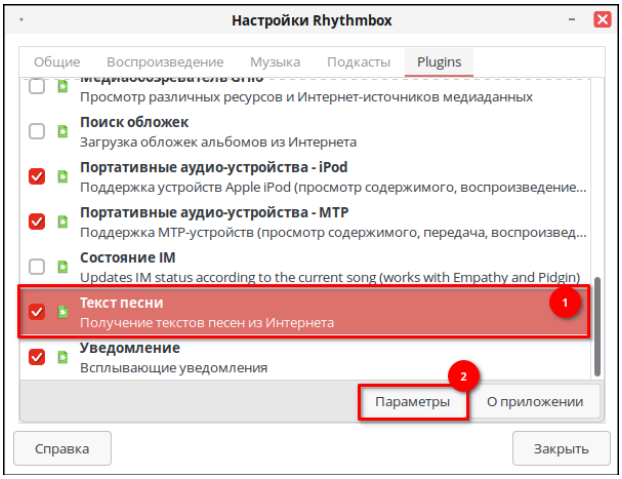


3. Для создания плейлиста выберите несколько треков и нажмите ПКМ на одном из них, а затем выберите «**Добавить в список воспроизведения**» — «**Добавить в новый список воспроизведения**».



4. Во время воспроизведения музыки можно использовать элементы управления воспроизведением в верхней части окна **Rhythmbox**.

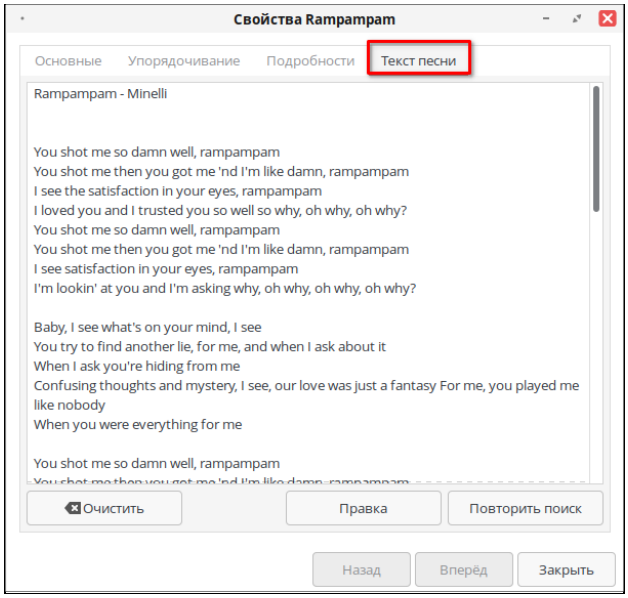
5. **Rhythmbox** предлагает плагины, которые можно активировать, чтобы получить дополнительную функциональность. Перейдите в основное меню — «**Параметры**». На вкладке «**Plugins**» активируйте необходимые плагины, например, «**Текст песни**» (1). Затем нажмите «**Параметры**» (2).



Выберите поисковые машины и папку с текстами песен.

Для просмотра текста песни нажмите на трек ПКМ и выберите «**Свойства**». Перейдите на вкладку «**Текст песни**». Если текст песни доступен, он будет отображаться в окне. Если текст песни не доступен, медиапроигрыватель начнет поиск интернете, в этом случае может потребоваться некоторое время, чтобы текст песни был загружен и отображен. Если текст песни не найден, в окне будет

выведено соответствующее сообщение.



Видеоредактор Kdenlive

Установка
Описание программы
Работа в программе

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** kdenlive-21.04.2-1

Kdenlive — это нелинейный видеоредактор, который позволяет добавлять эффекты и переходы, собирать видео в выбранный формат, при этом занимает мало места на диске и обладает обширным функционалом.

Вы можете подробнее ознакомиться с работой в **Kdenlive**, просмотрев наши обучающие видео:

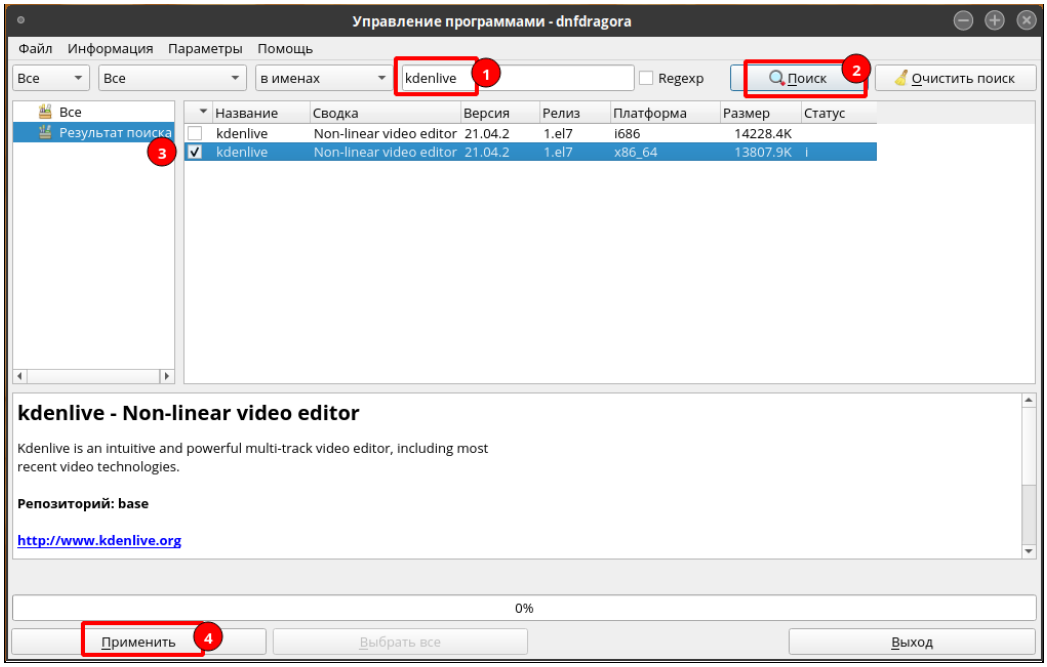
- на **RuTube** — Видеоредакторы. Установка и обзор Kdenlive;
- в **Яндекс.Дзен** — Видеоредакторы. Установка и обзор Kdenlive;
- в **VK Видео** — Видеоредакторы. Установка и обзор Kdenlive.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kdenlive**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

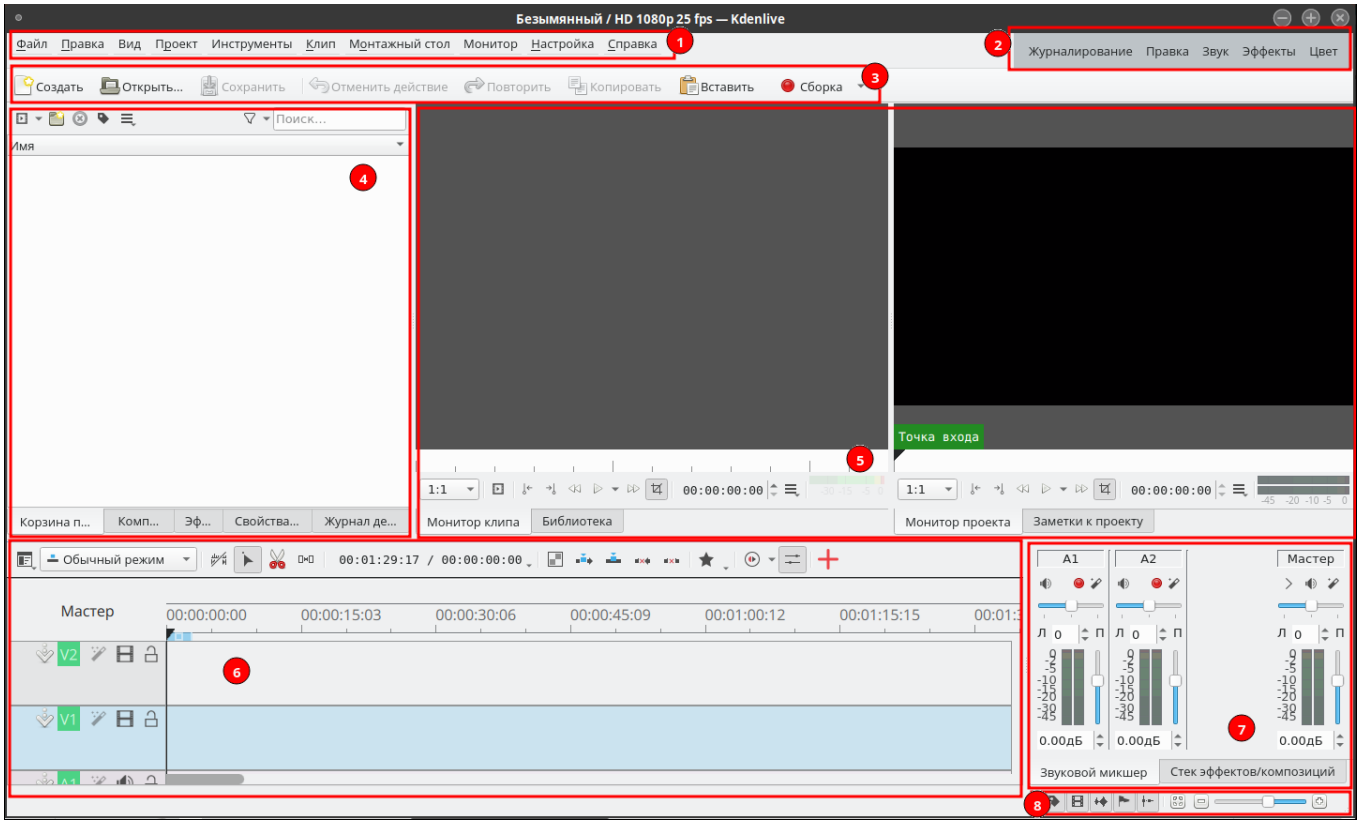
```
dnf install kdenlive
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Аудио и видео**» - «**Видеоредактор Kdenlive**».

Описание программы

Главное окно программы выглядит следующим образом:



Для комфортной работы необходимо отключить опцию «**Форсировать тему значков Breeze**» в пункте меню «**Настройки**», для применения изменений перезапустите программу.

1. *Основное меню* — основные настройки программы и действия для работы с файлами.

2. *Макеты* — шаблоны для выполнения различного рода задач: журналирование, правка, звук, эффекты, цвет.

3. Панель инструментов — основные действия для работы с проектом, таких как создание нового и открытие существующего проекта, сохранение проекта, отмена или повтор действия, копирование и вставка, а также сборка готового проекта.

4. *Корзина проекта* - все рабочие файлы проекта, доступно создание папок для упорядочивания открытых файлов, метки и быстрый поиск, если файлов большое количество.

Во вкладке **Композиции** и **Эффекты** доступны основные переходы и эффекты.

В **Свойствах клипа** отражается вся информация о выбранном видео.

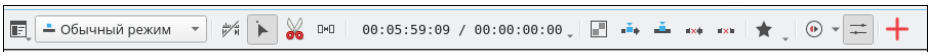
В **Журнале действий** отображается каждый выполненный шаг и можно отменить ошибочное действие.

5. *Монитор клипа* и *монитор проекта*. *Монитор клипа* позволяет посмотреть исходный материал в корзине проекта. *Монитор проекта* отражает видео с монтажного стола (timeline).

В каждом мониторе при наведении курсора мыши открываются свои функции, в том числе просмотр на весь экран.

В левом нижнем углу каждого монитора есть настройка с разрешением отображения, по умолчанию стоит **1:1**, но, при желании, можно изменить это значение.

6. *Монтажный стол* (Timeline). По умолчанию при открытии доступны 2 аудио- и 2 видеодорожки.



Первой располагается кнопка настроек композитинга дорожек, а также положения звуковых дорожек (по умолчанию звуковые дорожки находятся под видео).

Далее представлен список доступных режимов, по умолчанию установлен **Обычный режим**.

Затем располагаются инструменты для работы с дорожками: выбор, ножницы, вставка пробелов, соединение клипов и т. д.

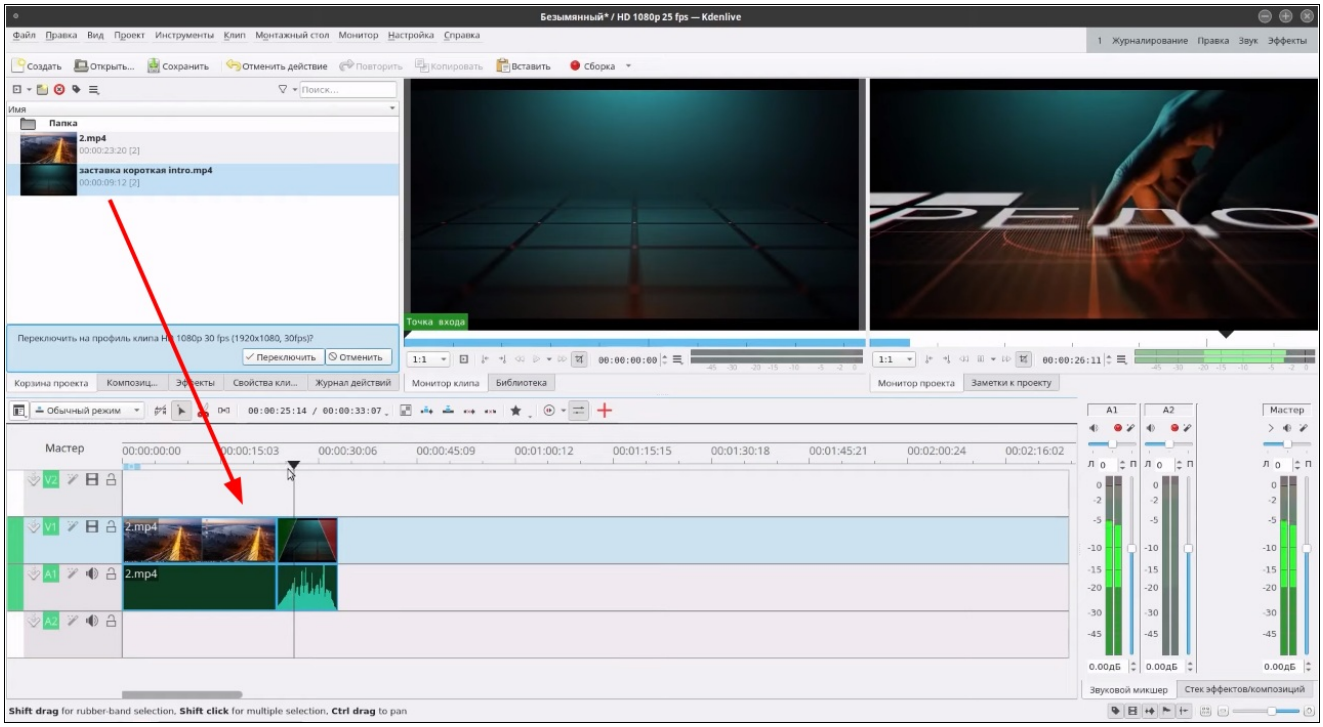
7. *Звуковые микшеры* - для первой и второй дорожек, а также один общий (мастер).

8. *Настройки для меток*, отображения миниатюр видео на монтажном столе, комментарии к маркерам, а также уровень масштабирования.

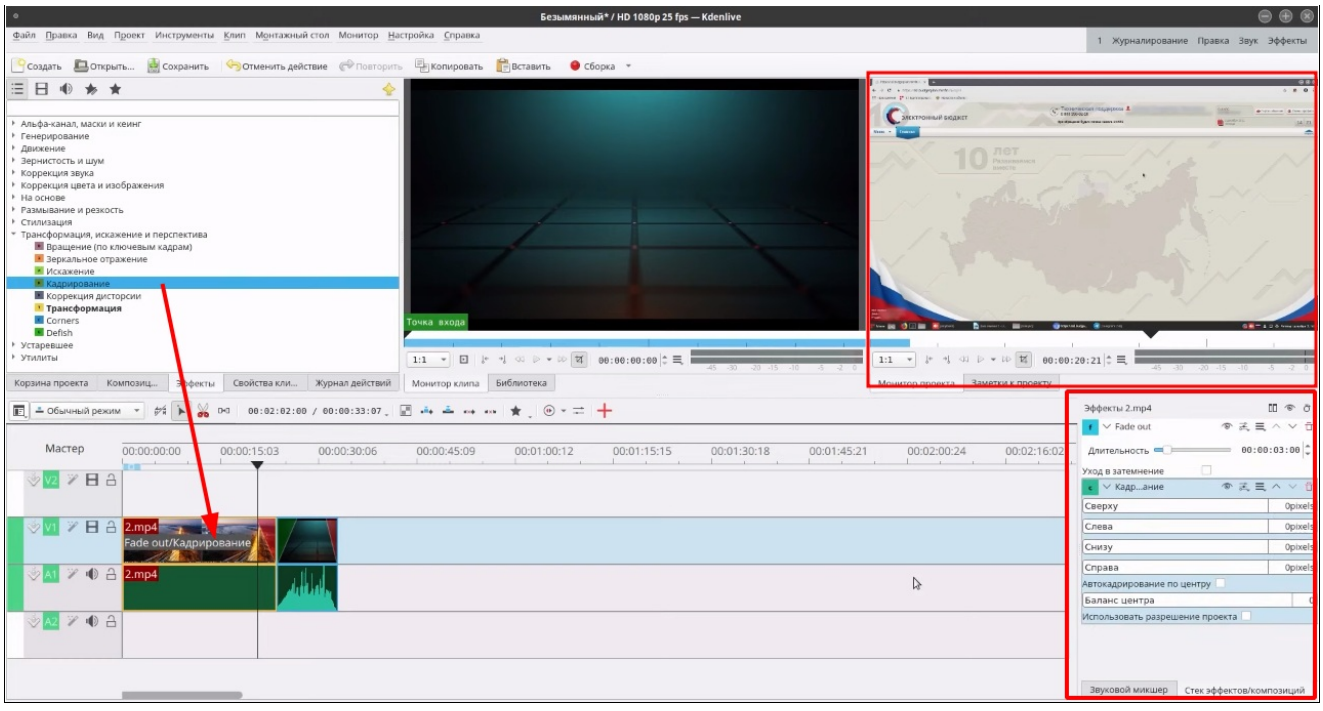
Вы можете установить удобные для себя настройки каждой области, а затем сохранить получившийся макет через пункт меню «**Вид**» - «**Сохранить макет**».

Работа с программой

Для создания нового клипа переместите из **Корзины проекта** нужные видео на **Монтажный стол**.



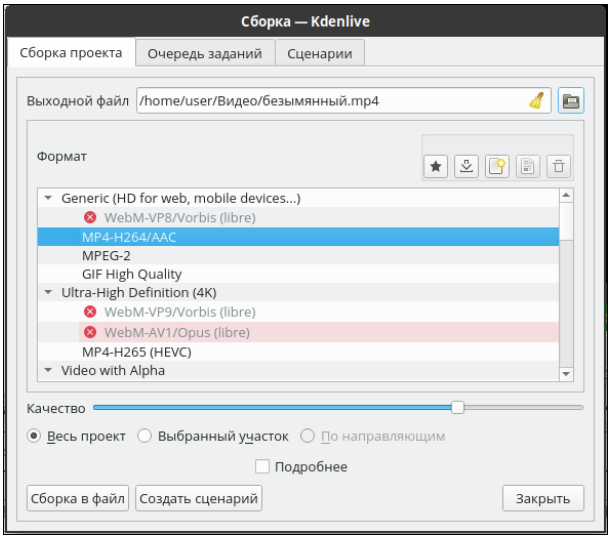
При наведении курсора на начало или конец клипа появляются точки бирюзового и красного цвета, при нажатии на которые применяется стандартный переход (fade in и fade out) соответственно. Их можно сделать короче или длиннее, перемещая точки на временной шкале. Также все примененные эффекты отображаются на миниатюре видео и в разделе **Стек эффектов**, раскрыв который вам будут доступны настройки. Дополнительно в *Стеке* можно удалить ненужный эффект либо посмотреть, как выглядело видео без примененного эффекта.



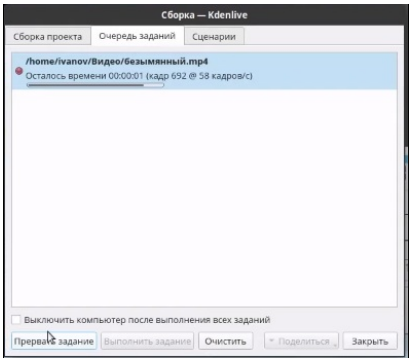
Если необходимо изменить длину отрезка видео, то при активном **Инструменте выбора** можно растянуть края видео и добиться желаемого результата. **Инструмент обрезки** делает это при наведении курсора и нажатии левой кнопки мыши, оставляя отрезанную

часть.

При завершении работы над проектом необходимо его собрать в итоговое видео. Для этого нажмите «**Сборка**» на панели инструментов. Далее потребуется выбрать путь и название для выходного файла, а также формат сохраняемого проекта.



Здесь также есть возможность сборки *всего проекта* либо *выбранного участка*. После определения всех настроек нажмите кнопку «**Сборка в файл**», будет открыта вкладка **Очередь заданий** с прогрессом готовности проекта. Здесь можно установить флаг «**Выключить компьютер после выполнения всех заданий**», если проект большой и сборка выполняется длительное время.



Видеоредактор Shotcut

Возможности Shotcut
Установка
Описание интерфейса
Создание проекта
Импорт медиафайлов
Добавление файлов на временную шкалу
Редактирование видео
Добавление аудио
Экспорт проекта

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: shotcut-24.02.29

Shotcut — это бесплатная программная платформа для редактирования видео- и аудиоформатов, которая предоставляет пользователю широкие возможности для создания собственного контента.

Возможности Shotcut

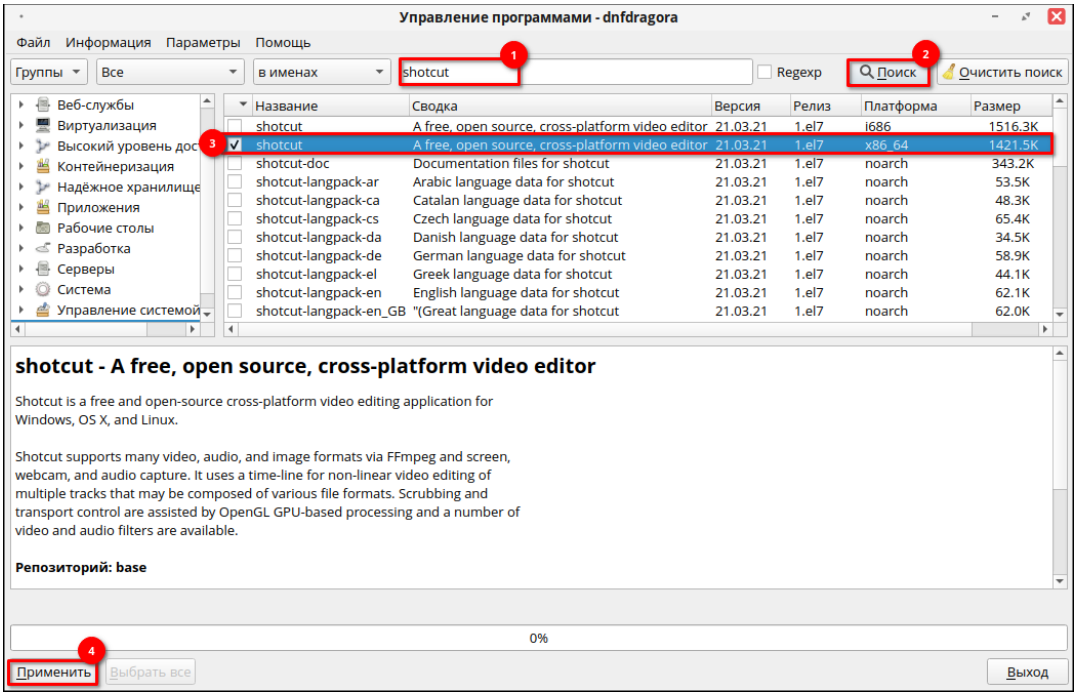
Основными возможностями программы Shotcut являются:

- простой и удобный интерфейс;
- поддержка видео- и аудиоформатов, включая HD и 4K;
- импорт различных типов файлов в проекты;
- добавление эффектов и фильтров к видео (стабилизация изображения, цветокоррекция, наложение текста и др.);
- монтаж звука;
- наложение звука на видео;
- регулировка уровня звука;
- экспорт видео в различные форматы и разрешения;
- большое количество бесплатных образцов (эффекты, фильтры, шрифты и др.).

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**shotcut**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install shotcut
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Для запуска программы через терминал введите команду:

```
shotcut
```

После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**Видеоредактор Shotcut**» (РЕД ОС 7.3) или «**Shotcut**» (РЕД ОС 8.0).

Описание интерфейса

Интерфейс Shotcut в РЕД ОС 7.3 не русифицирован по умолчанию. Для смены языка программы перейдите в меню «**Settings**» — «**Language**» — **Russian**. После выполнения настройки интерфейс станет частично русифицированным.

Интерфейс программы в РЕД ОС 8.0 русифицирован, что делает его использование более удобным.

Окно программы можно визуально разделить на шесть основных зон:

1. **Основное меню** состоит из шести пунктов.

- **Файл** — позволяет открыть/закрыть, создать или экспортировать видеоролик.
- **Правка** — используется для отмены и повтора действий, а также для вырезания, копирования и вставки.
- **Вид** — настройка видимых панелей, размера окна и прочих параметров отображения.
- **Проигрыватель** — используется для настройки времени перехода вперёд/назад, обрезки клипа, а также для переключения между источником и проектом.
- **Настройки** — настройка параметров программы.
- **Справка** — содержит различную информацию, включая ссылки на полезные статьи, форумы, уроки, раздел вопросов и ответов.

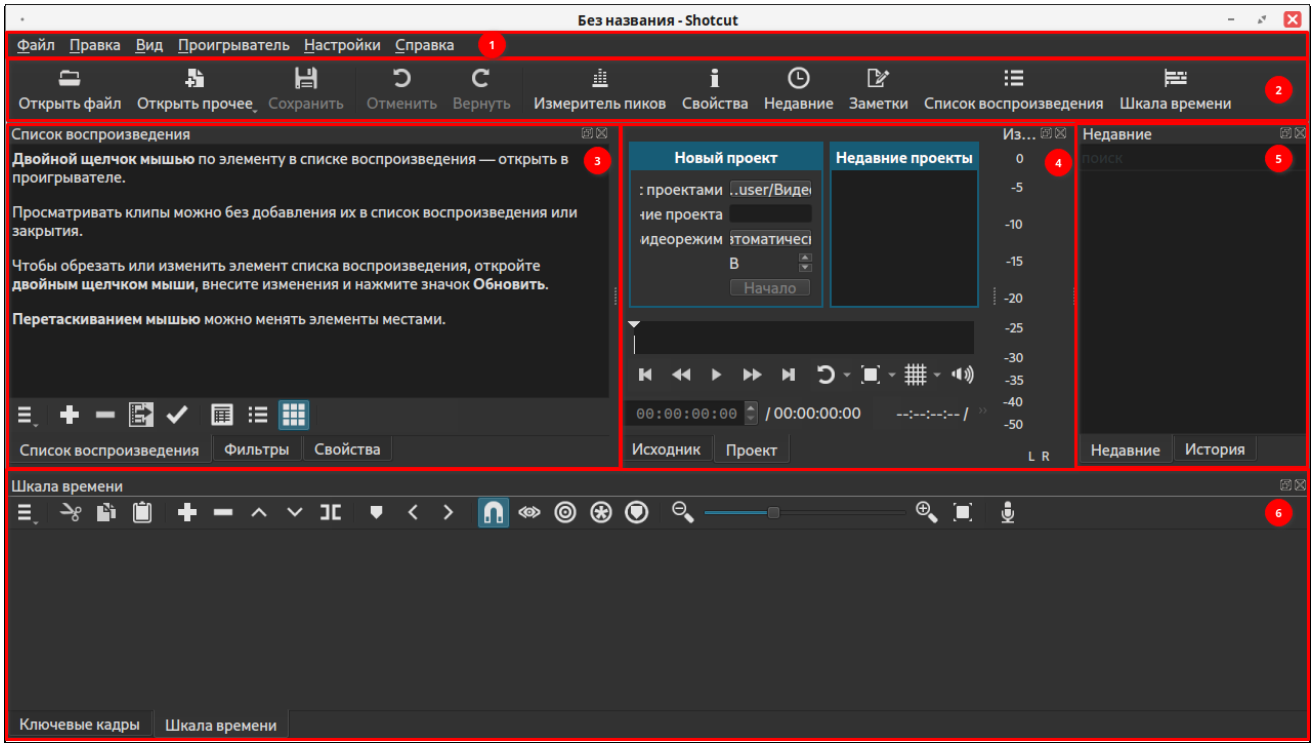
2. **Панель инструментов** — предоставляет быстрый доступ к основным опциям программы. По умолчанию видны не все доступные опции, чтобы увидеть полный список, нажмите на стрелку справа.

3. **Свойства** — отображает все данные о ролике, с которым ведётся работа в текущий момент. Здесь также расположен список использованных фильтров и список воспроизведения.

4. **Проигрыватель** — область для просмотра видеоролика.

5. **Дополнительная информация** — по умолчанию в этой зоне отображается список файлов, с которыми пользователь недавно работал. Также здесь откроется перечень заданий либо история.

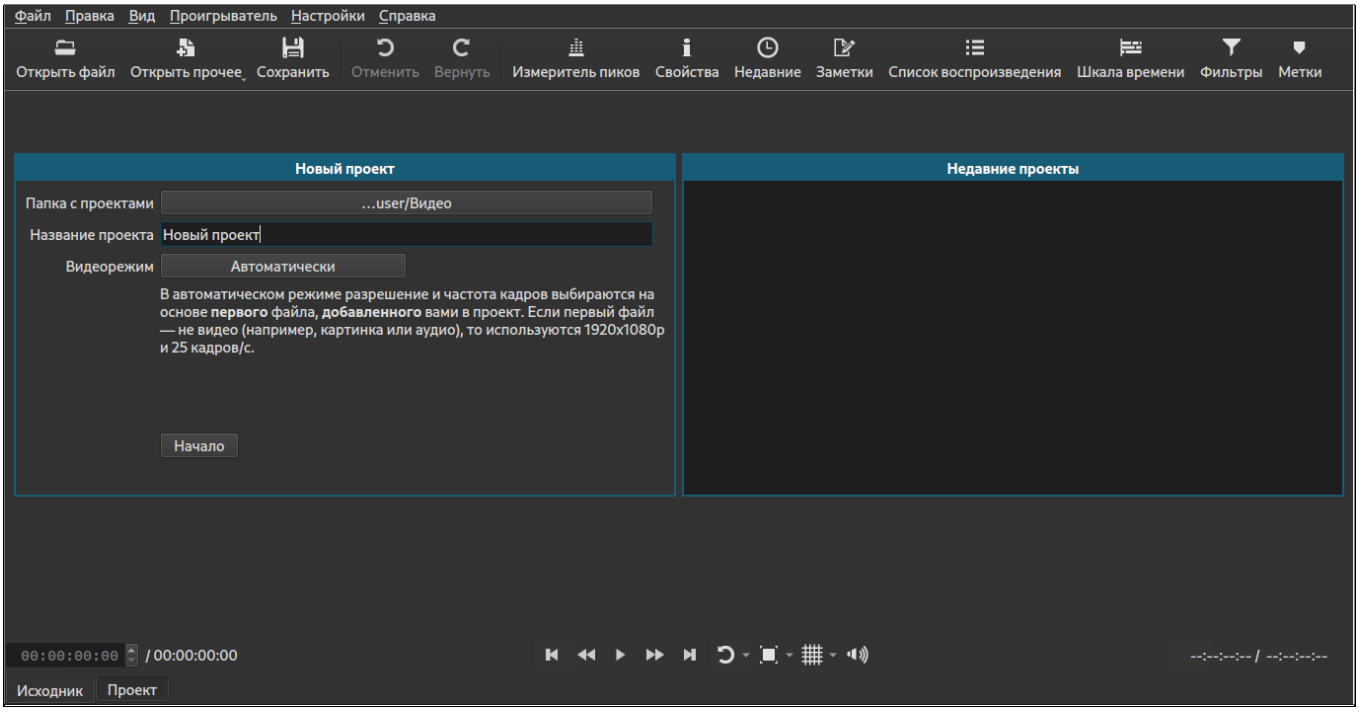
6 . **Область монтажа** — по умолчанию в этой области расположены шкала времени и ключевые кадры видеоролика, внизу окна находится переключатель вкладок.



Создание проекта

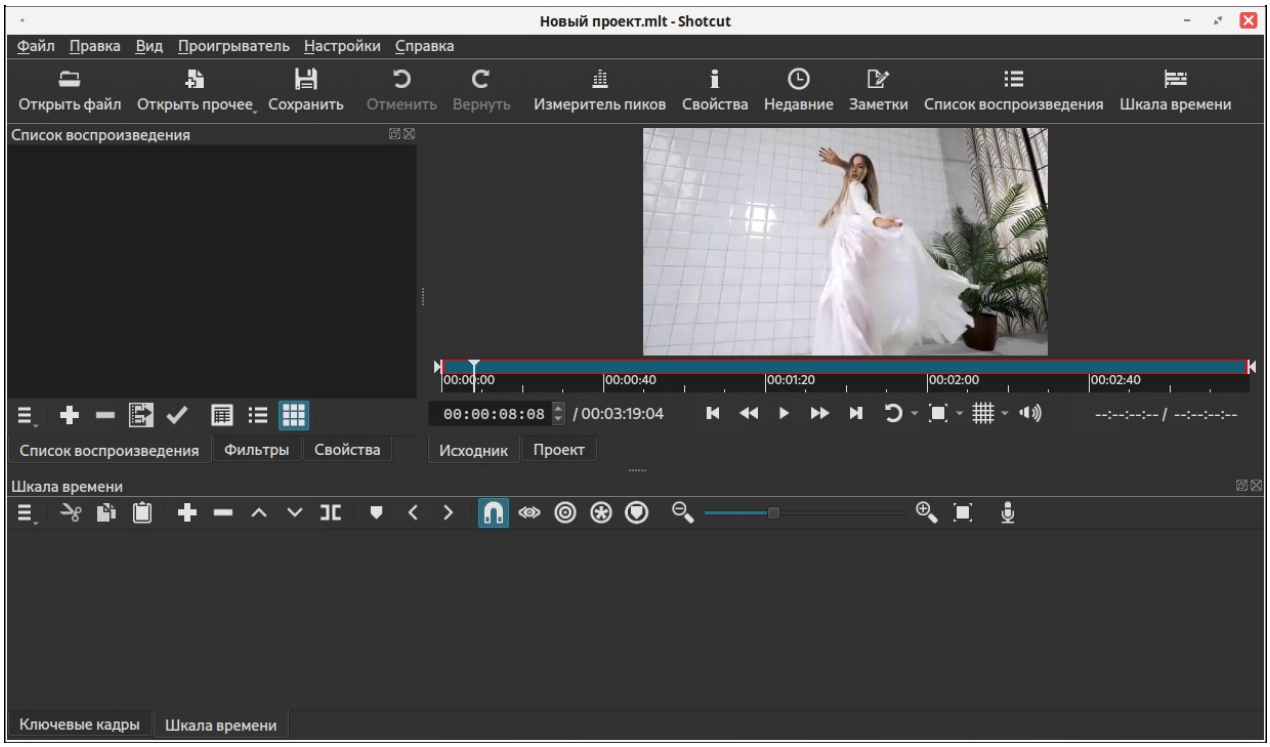
Окно создания нового проекта автоматически открывается сразу же после запуска программы.

Для создания нового проекта выберите в основном меню пункт «**Файл**» — «**Новый**» или нажмите комбинацию клавиш Ctrl+N. В открывшемся окне выберите папку для сохранения проекта, укажите название проекта, при необходимости выберите видеорежим.



Импорт медиафайлов

Для импорта медиафайла в проигрыватель перейдите в меню «**Файл**» — «**Открыть файл...**». Выберите видеоролик и нажмите «**Открыть**». Видеоролик появится в проигрывателе. При добавлении нескольких файлов они отображаются в списке воспроизведения.



Добавление файлов на временную шкалу

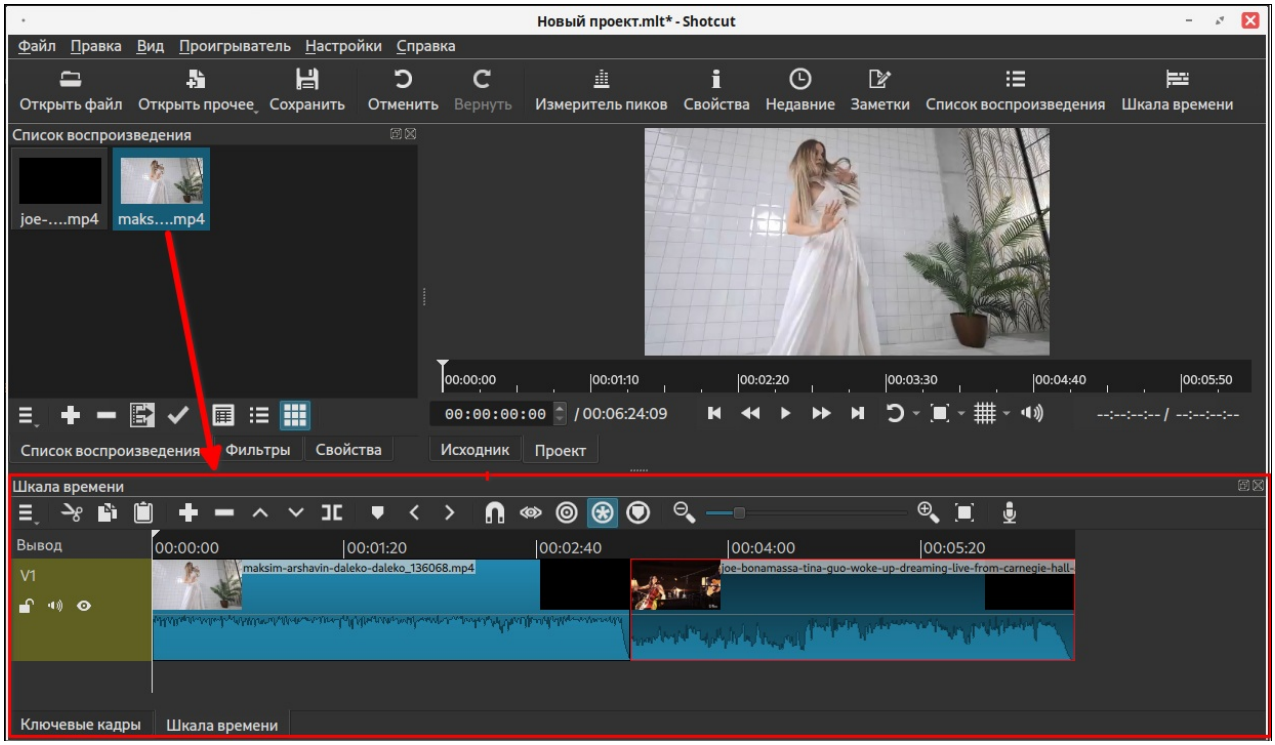
Добавление файлов на временную шкалу позволяет организовать и упорядочить медиафайлы в проекте.

Первый способ:

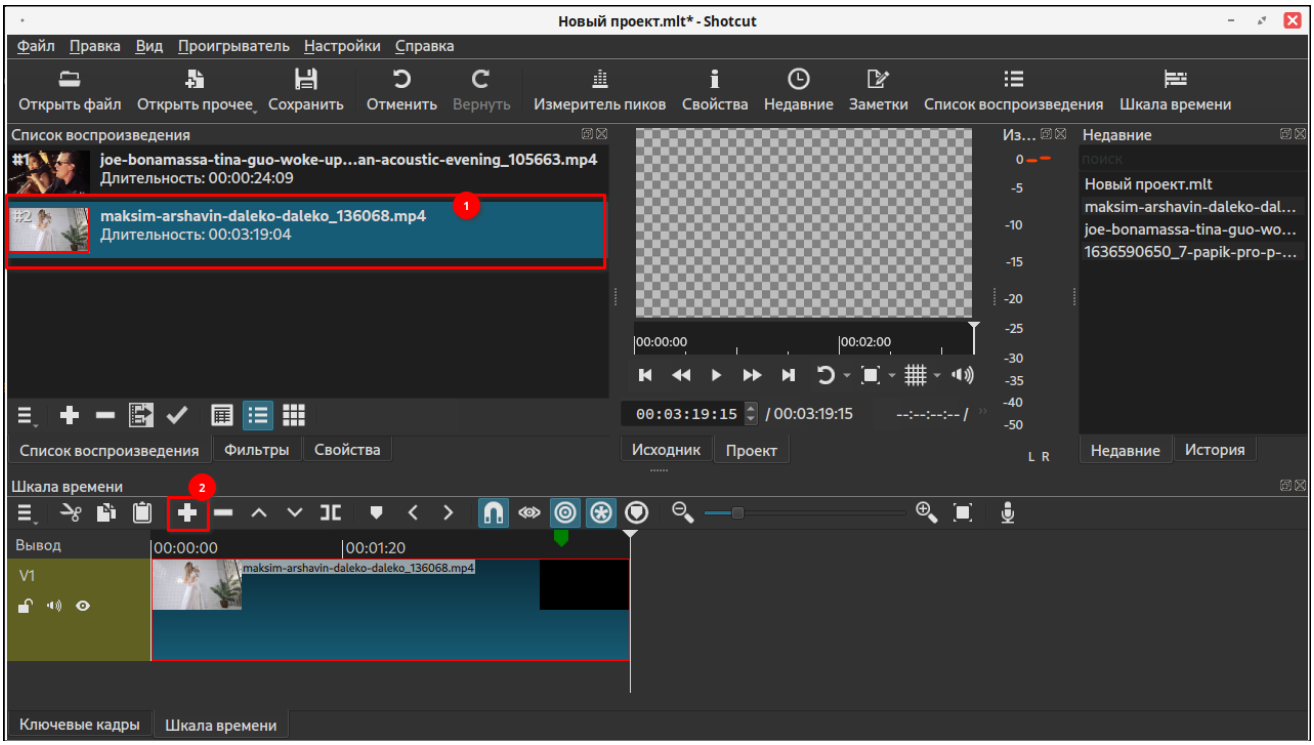
1. Импортируйте необходимые файлы в проект.

2. Перетащите файлы из списка воспроизведения на временную шкалу.

3. Разместите файлы в нужном порядке.

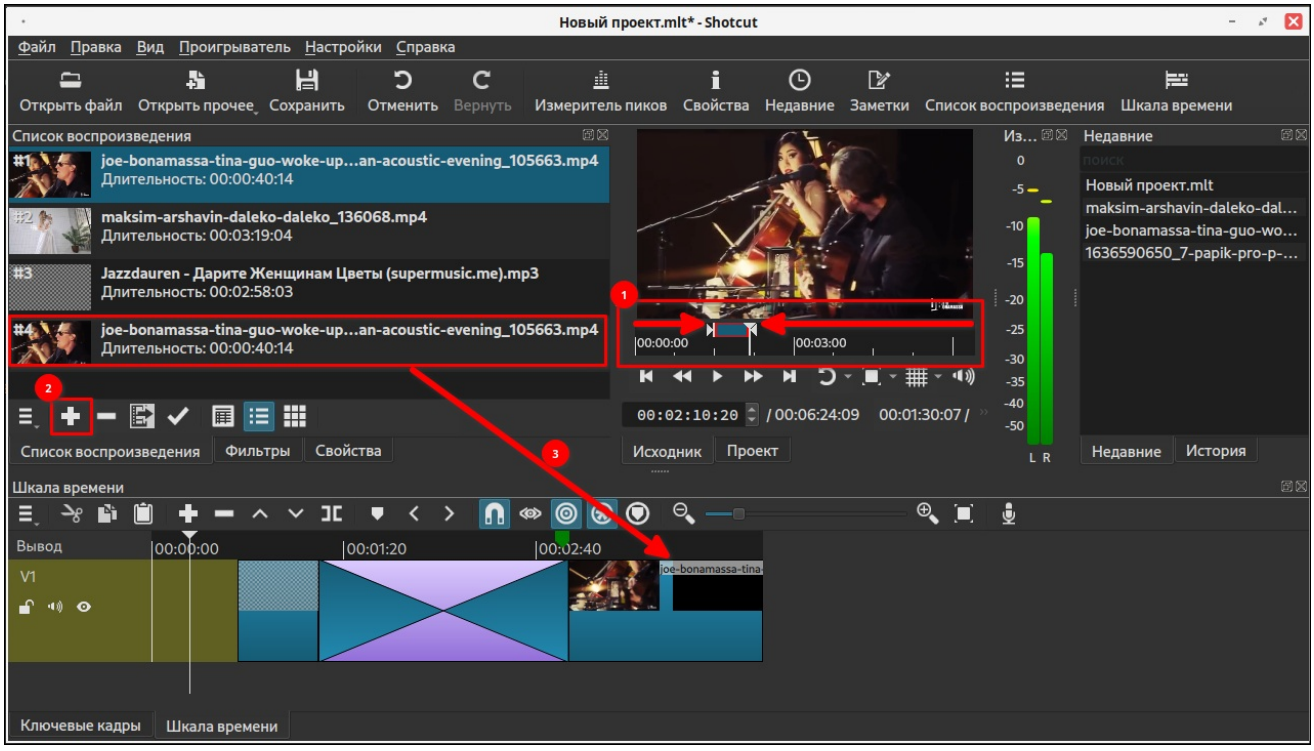


Второй способ. Для добавления файлов на временную шкалу дважды щелкните по нужному видео в списке воспроизведения (1) и на панели инструментов временной шкалы нажмите кнопку «**Добавить**» (2).



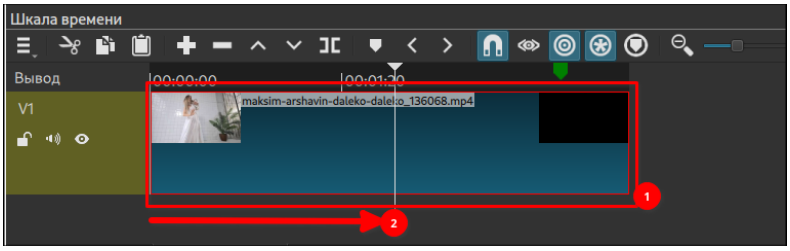
Редактирование видео

Для использования части видео в проигрывателе сдвиньте временные метки (1), нажмите «**Добавить источник в список воспроизведения**» (2) и перетащите сцену на временную шкалу (3).

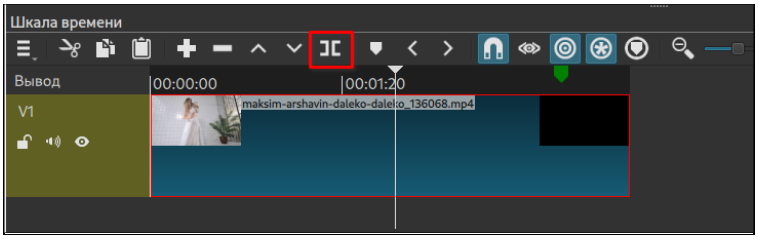


Для обрезки видео выполните следующие действия.

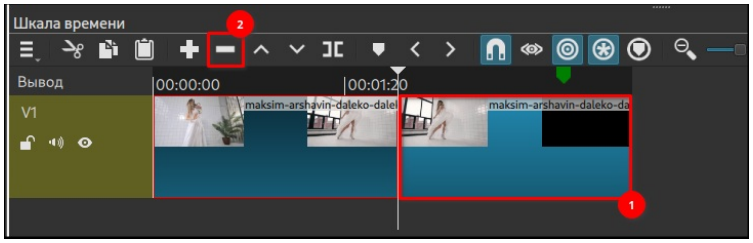
1. Выделите кадр и переместите указатель воспроизведения к точке, где клип нужно разделить.



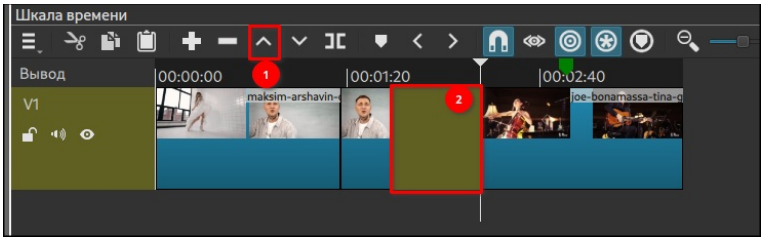
2. Выберите инструмент «**Разделение по точкам воспроизведения**».



В результате появятся два фрагмента видео. Для удаления лишнего фрагмента выберите его (1) и нажмите кнопку «**Удалить**» (2). Лишний фрагмент будет удалён. Следующий клип сдвинется на место вырезанного фрагмента.



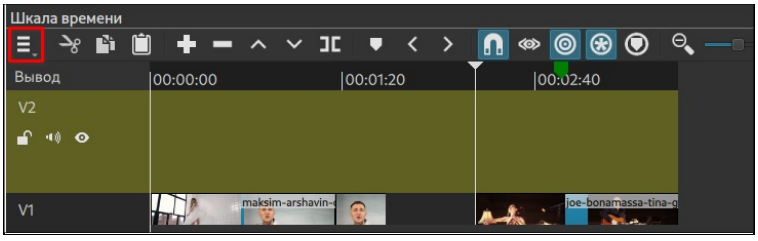
Если необходимо оставить пустое пространство вместо вырезанного фрагмента, выберите фрагмент и нажмите «**Поднять**» (1). На месте вырезанного фрагмента останется незаполненное пространство (2).



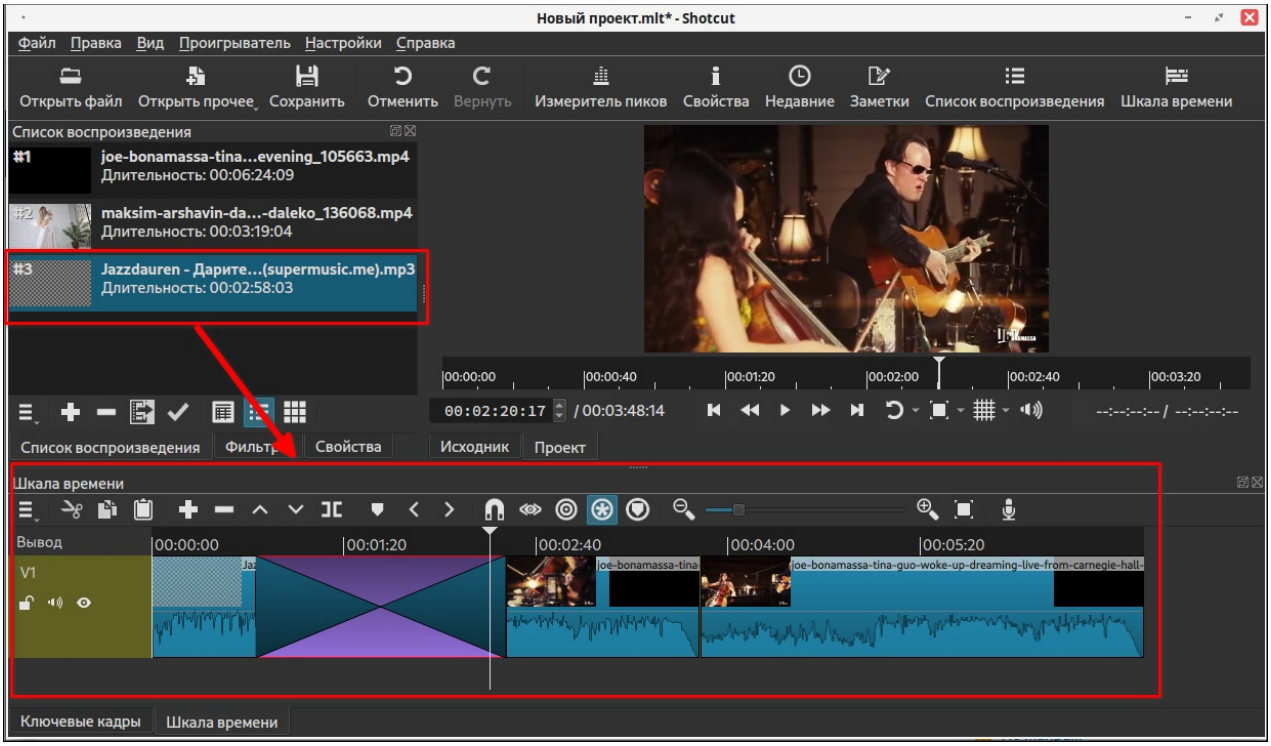
Добавление аудио

Shotcut позволяет использовать аудиофайлы с компьютера для озвучки. Пользователи могут полностью заменить звук или изменить его частично.

Для добавления аудиодорожки перейдите в меню временной шкалы и из выпадающего списка выберите «**Действия с дорожкой**» — «**Вставить дорожку**». На временной шкале отобразится аудиодорожка.



Для добавления аудио в проект перетащите аудиофайлы из списка воспроизведения на аудиодорожку на временной шкале. Настройте громкость и добавьте эффекты.

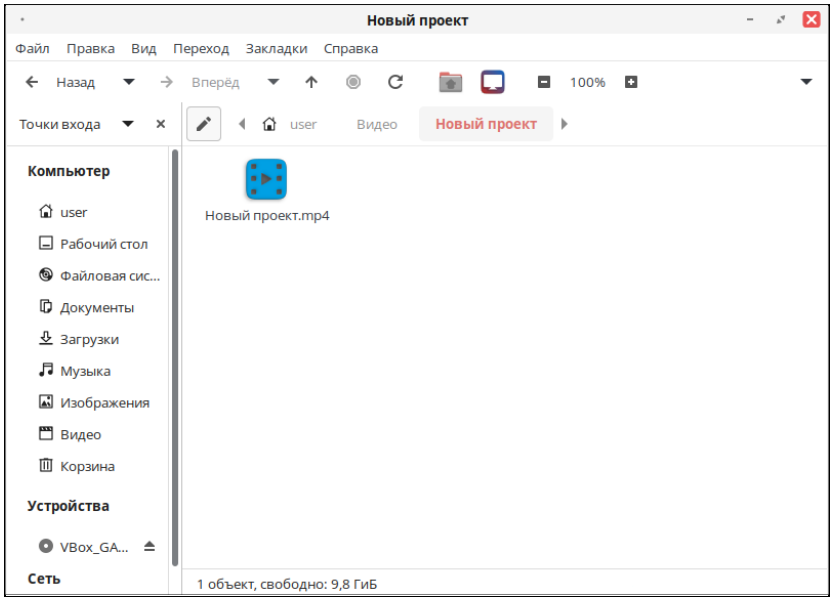


Экспорт проекта

После завершения обработки материала можно сохранить проект. Для этого перейдите в меню «**Файл**» — «**Экспорт**» — «**Видео...**».

Введите название проекта, выберите каталог и нажмите «**Сохранить**».

Проект будет экспортирован в выбранный видеоформат.



Видеоредактор OBS Studio

Установка
Описание программы
Первоначальная настройка
Настройки звука/микрофона, видео
Запись аудио
Запись экрана и звука
Перепаковка записей

Окружение

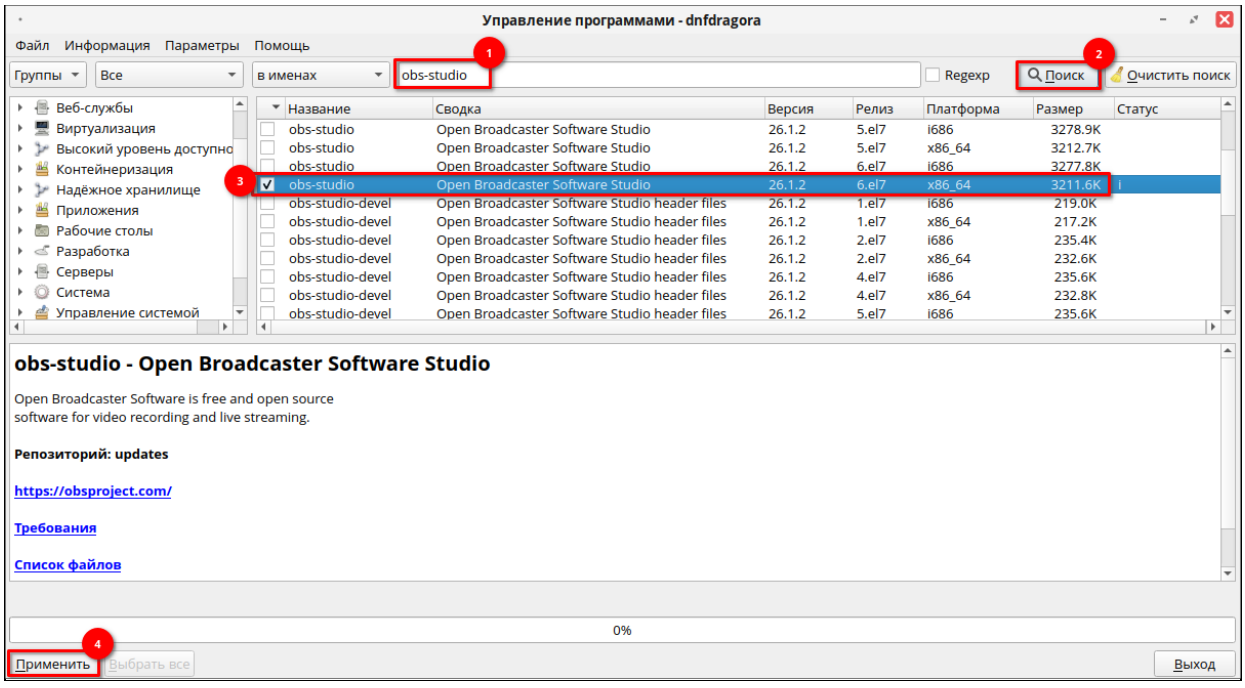
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: obs-30.1.0

OBS Studio (Open Broadcaster Software Studio) — это программа для потокового вещания (стримов) и записи видео. Приложение поддерживает работу с несколькими источниками одновременно, позволяет комбинировать различные видео/аудиопотоки, создавая непрерывную трансляцию, что подходит для трансляций игр, проведения семинаров, онлайн-фестивалей.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**obs-studio**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install obs-studio
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

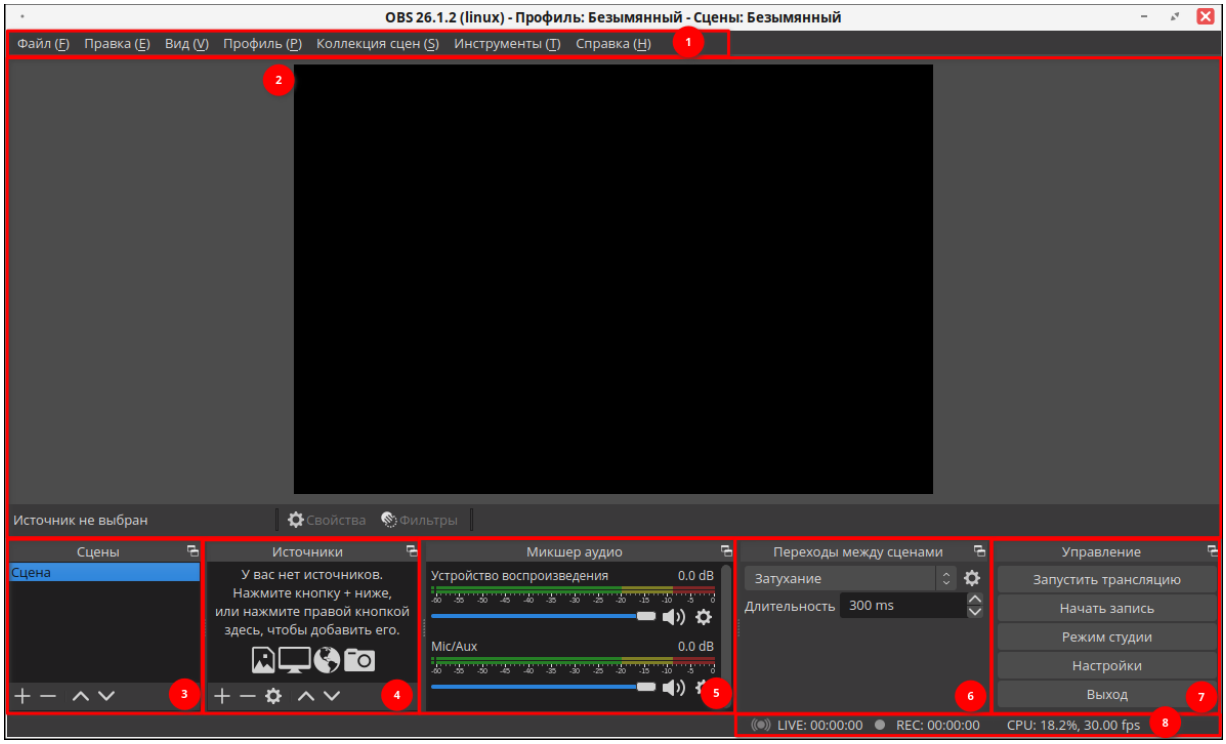
Для запуска программы через терминал введите команду:

```
obs studio
```

После установки программа будет доступна из «**Главного меню**» — «**Аудио и видео**» — «**OBS Studio**».

Описание программы

Главное окно программы состоит из нескольких типовых частей.



1. **Основное меню программы** позволяет выполнять различные действия с создаваемым файлом, а также настраивать программу и панель инструментов.

2. **Рабочая область** отображает видео- и аудиоконтент.

3. **Сцены** — список всех сцен, которые созданы в **OBS Studio**.

4. **Источники** — список всех источников (например, видеокамеры, микрофоны, экраны).

5. **Микшер аудио** позволяет регулировать уровни аудиосигналов и настраивать аудиоэффекты.

6 . **Переходы между сценами** позволяют настроить переходы между сценами, чтобы сделать видео более плавным и профессиональным.

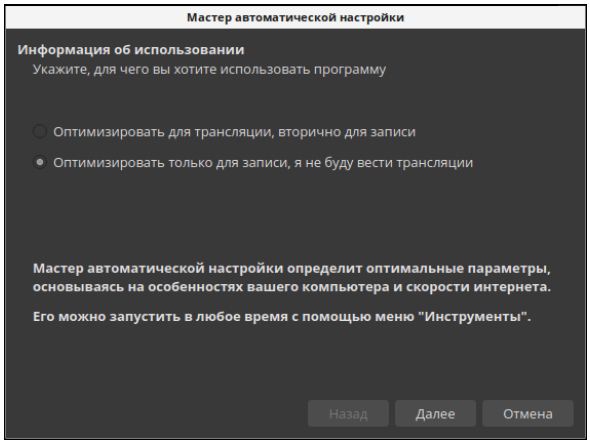
7 . **Панель управления трансляцией** позволяет настроить параметры трансляции, такие как выбор сервера, настройка качества видео и аудио, и т. д.

8. **Строка состояния трансляции** отображает информацию о текущем состоянии трансляции, например, статус соединения, качество видео и аудио, и т. д.

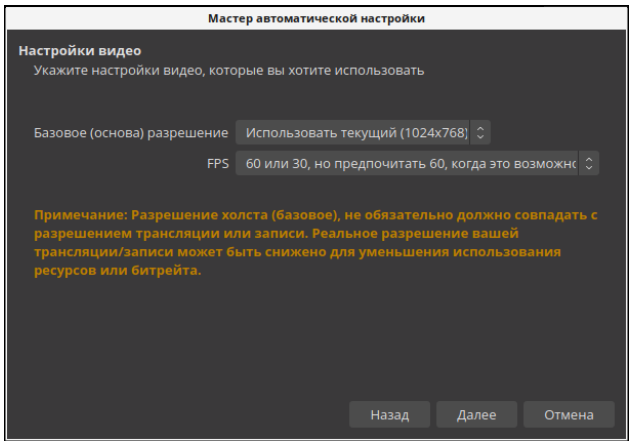
Первоначальная настройка

Для первоначальной настройки необходимо выполнить следующий алгоритм действий:

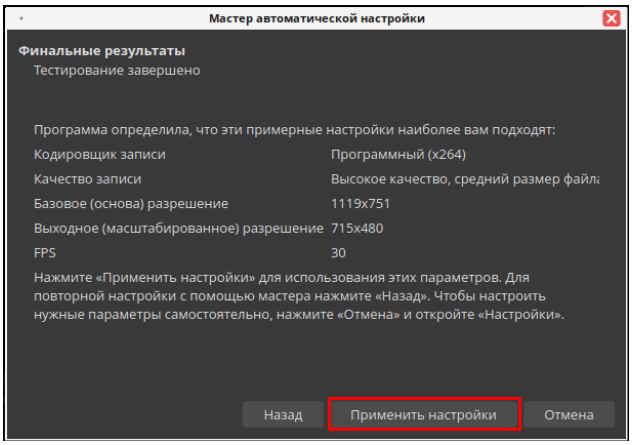
1. При первой загрузке **OBS Studio** запустится мастер автоматической настройки.



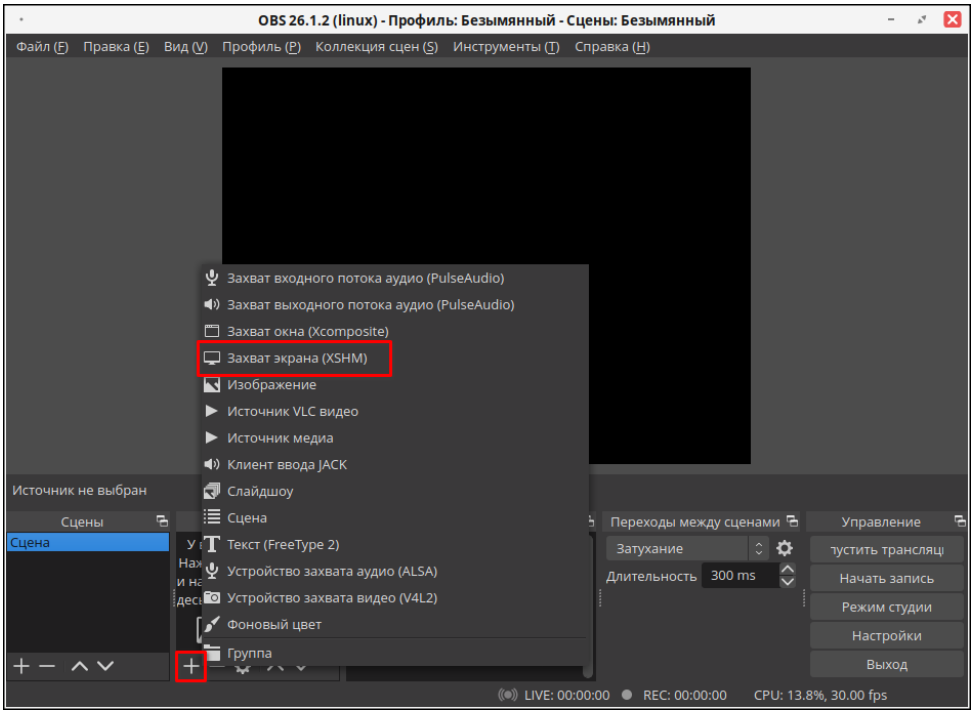
Следуйте инструкциям, чтобы получить подходящие начальные настройки видео.



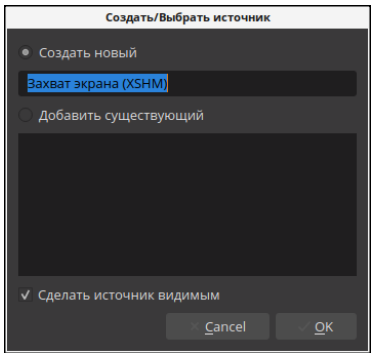
По окончании настроек нажмите «**Применить настройки**» для использования выбранных параметров.



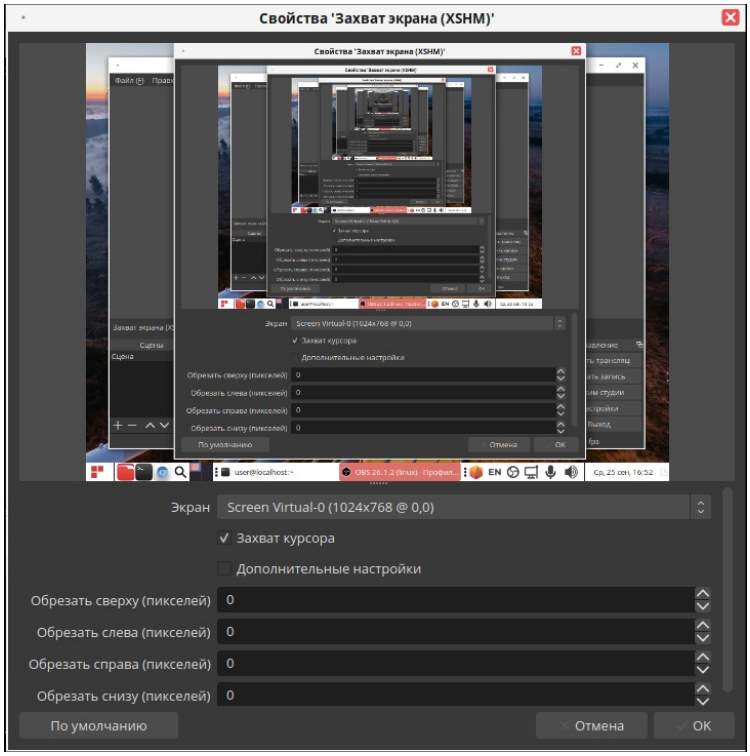
2. Добавьте источники к сценам. Для добавления нового источника нажмите на значок  на панели «**Источники**», расположенной в нижней части главного экрана. Выберите источник, например, «**Захват экрана (XSHM)**».



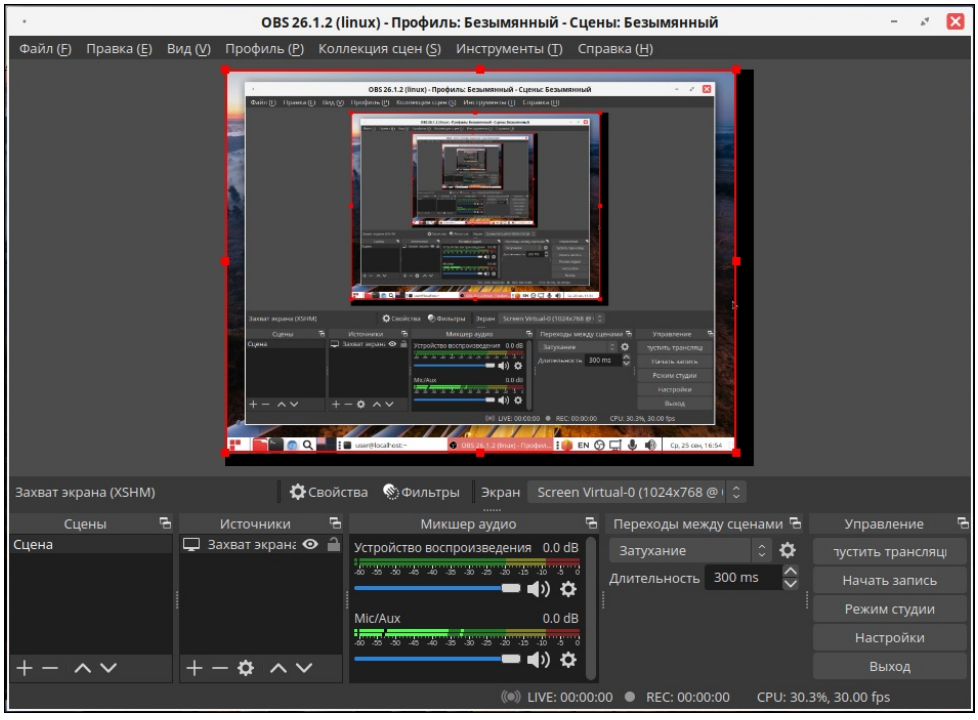
Напишите наименование источника и нажмите «**OK**».



В открывшемся окне выберите экран и нажмите «**OK**».



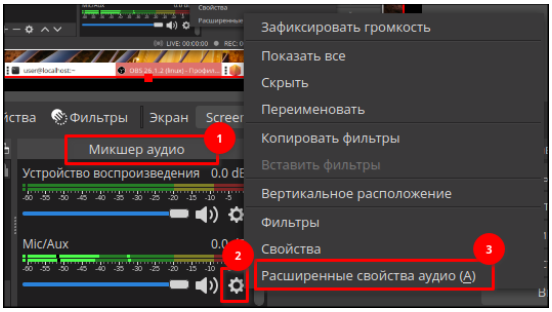
Выбранный экран отобразится в рабочей области.



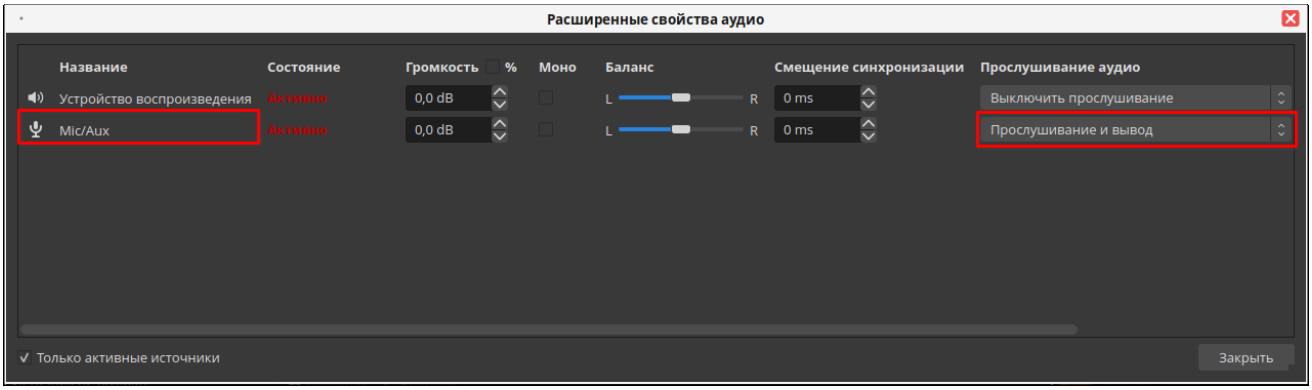
Для изменения размера источника кликните на его название и в рабочей области появится красная граница вокруг него. Для изменения размера потяните мышкой за одну из сторон источника.

3. Настройте аудио. В панели «**Микшер аудио**» (1) выберите рядом с источником медиа «**Свойства**» (2) — «**Расширенные настройки**

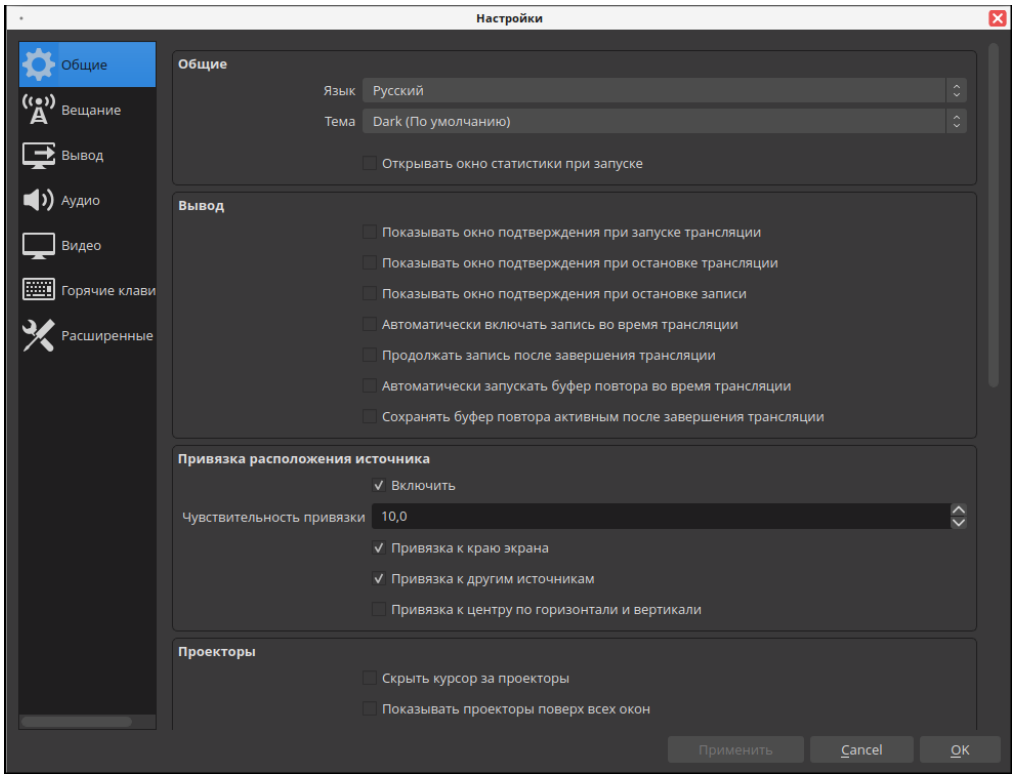
аудио»(3).



В окне настроек аудио выберите желаемый источник аудио и в параметре «**Прослушивание аудио**» выберите «**Прослушивание и вывод**».



4. Откройте панель с общими настройками в меню «**Файл**» — «**Настройки**». После открытия окна с общими настройками можно выбрать необходимые параметры.



В разделе Общие можно выбрать тёмную или светлую тему оформления, выбрать привязку расположения источника, показывать подтверждение для запуска/остановки потоков, включить/отключить автоматическую запись при потоковой передаче.

В разделе Вещание можно выбрать одну из включенных служб, установить пользовательский сервер потоковой передачи, выбрать сервер, ввести свой ключ потока.

В разделе Вывод можно настроить расширенный режим вывода для настройки потока и записи.

В разделе Аудио можно изменить частоту дискретизации, выбрать до двух настольных аудиоустройств, до трех микрофонов, вспомогательных устройств, включить дополнительные функции для каждого устройства.

В разделе Видео можно задать разрешение. **Базовое разрешение** — должно соответствовать разрешению дисплея используемого

монитора. **Выходное разрешение** — должно соответствовать выходному разрешению потока/записи. **Общее значение** FPS должно соответствовать желаемому выходному FPS.

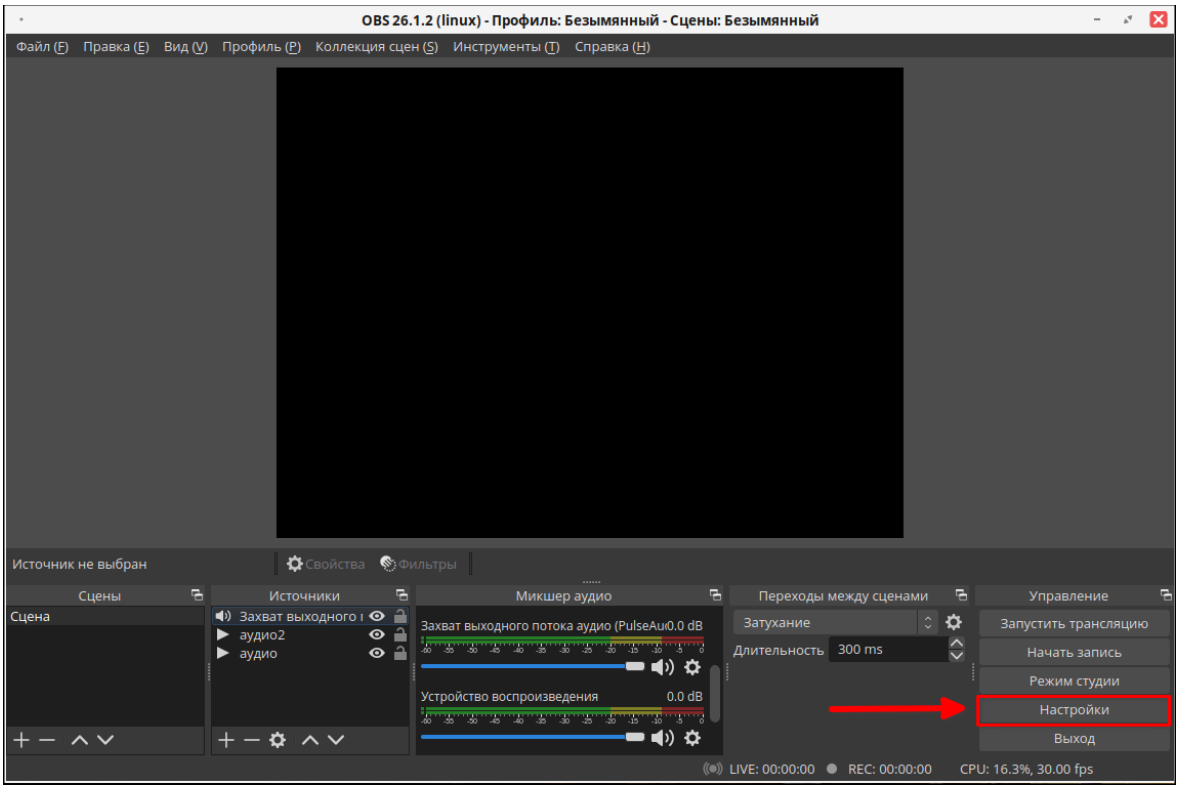
В разделе Горячие клавиши можно настроить быстрый доступ к тем или иным действиям.

В разделе Расширенные настройки можно активировать задержку потока, настроить автоматическое повторное подключение.

Настройки звука/микрофона, видео

Чтобы настроить **OBS Studio** для записи видео, выполните следующий алгоритм действий:

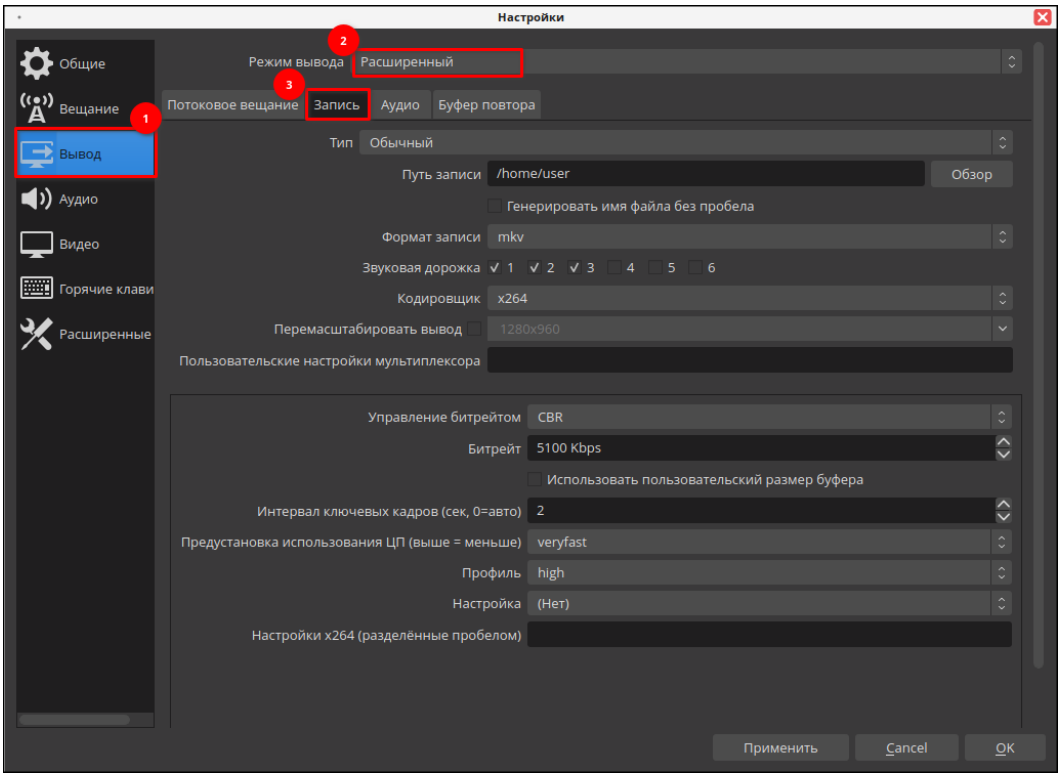
1. На панели управления трансляцией откройте «**Настройки**».



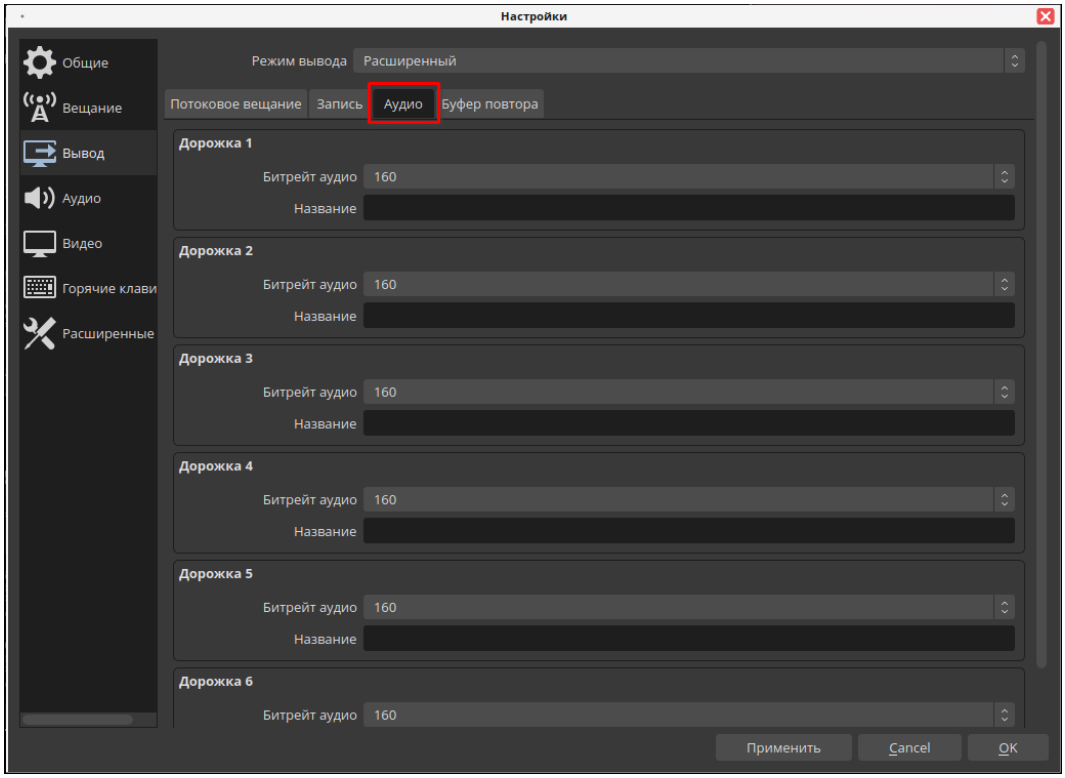
2. Перейдите в раздел Вывод. Установите режим вывода на «**Расширенный**».

На вкладке «**Запись**» установите следующие параметры:

- Тип записи: обычный;
- Путь записи: укажите удобный путь для записи;
- Формат записи: MKV;
- Звуковая дорожка: установите звуковые дорожки: 1, 2, 3 (например, дорожка 2 - микрофон, дорожка 3 - все системные звуки);
- Кодировщик: выберите кодировщик;
- Битрейт: 5100 Kbps;
- Интервал ключевых кадров: 2 сек.;
- Предустановка использования ЦП: veryfast;
- Профиль: high.



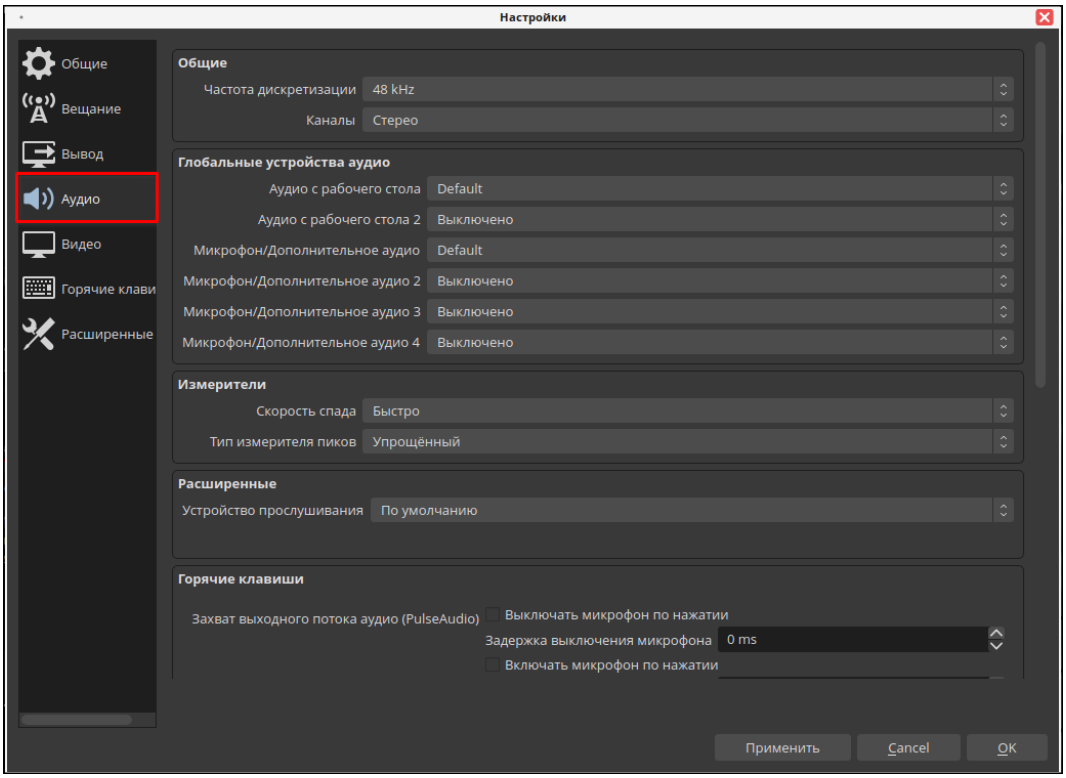
На вкладке «**Аудио**» установите битрейт аудио на дорожках — 160.



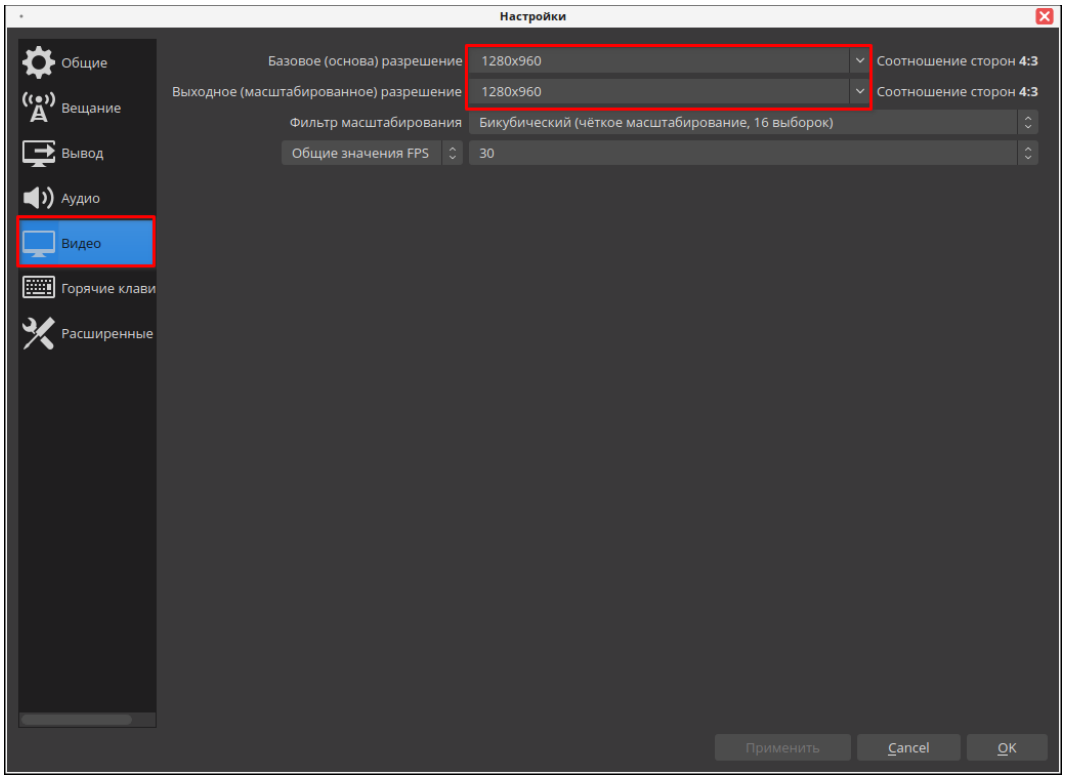
3. Перейдите в раздел Аудио.

Установите следующие параметры:

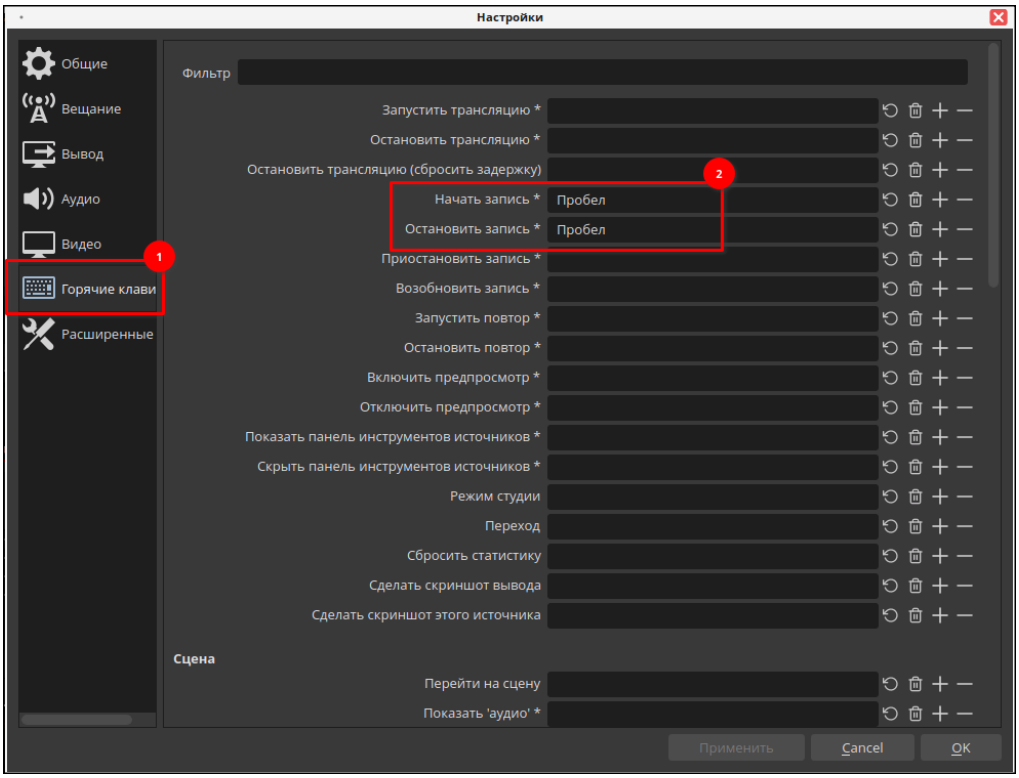
- Частота дискретизации: 48;
- Каналы: Стерео;
- Аудио с рабочего стола: Default;
- Звук рабочего стола: отключено;
- Микрофон: Default.



4. В разделе Видео установите разрешение экрана используемого монитора. Например, 1280*960.

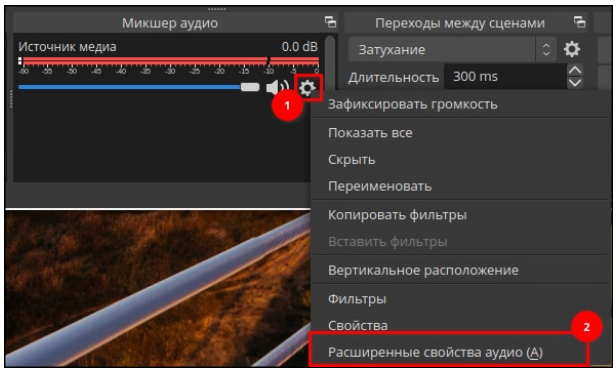


5. В разделе Горячие клавиши установите значение «**Пробел**» для пунктов «**Начать запись**» и «**Остановить запись**».



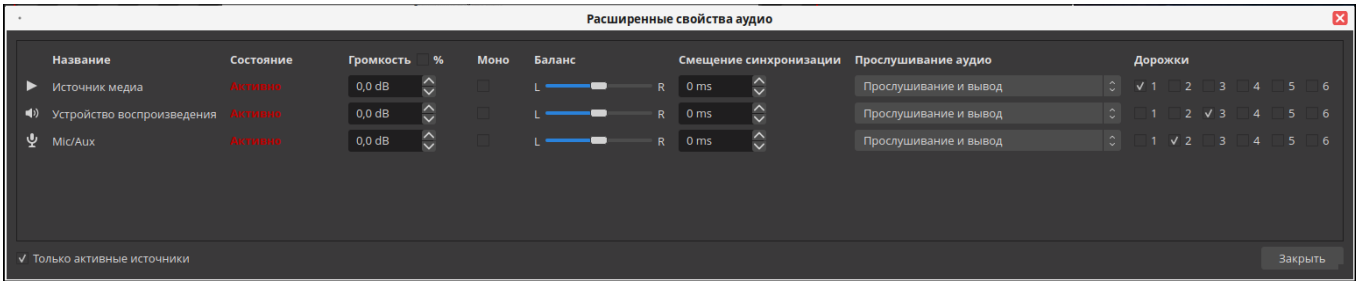
Нажмите «**Применить**» и «**OK**».

6. Перейдите в Микшер аудио, щёлкните на значок  и выберите «**Расширенные свойства аудио**».



В левой части окна отобразятся названия источников звука, а в правой — звуковые дорожки.

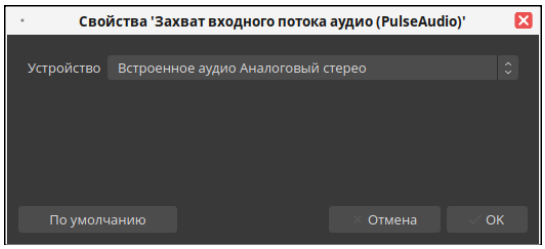
Установите напротив каждого источника флаг рядом с определенной дорожкой.



Запись аудио

Для записи аудио выполните следующий алгоритм действий:

1. Нажмите на кнопку  и выберите источник звука «**Захват входного потока аудио**». Выберите устройство.



2. Нажмите «**Начать запись**» (или воспользуйтесь горячей клавишей), чтобы начать запись видео с экрана. Красная точка на значке REC в нижней части экрана указывает на то, что запись началась.

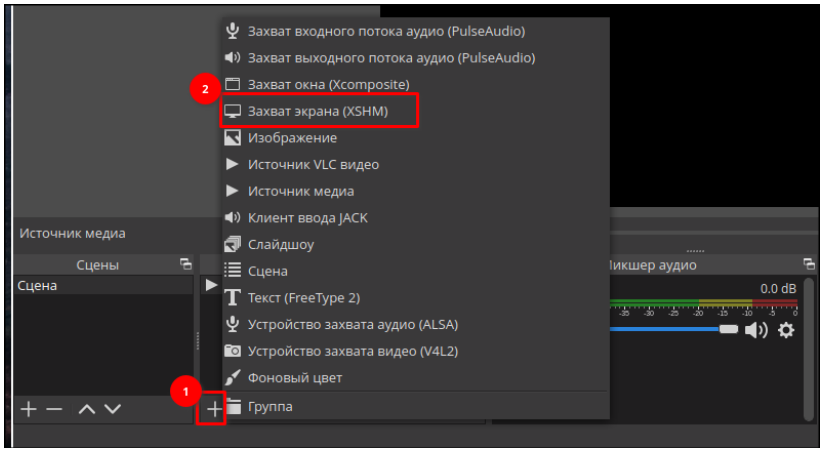
3. Чтобы остановить запись, нажмите на кнопку «**Остановить запись**» (или используйте горячую клавишу).

4. Для просмотра записей перейдите в меню «**Файл**» — «**Показать записи**».

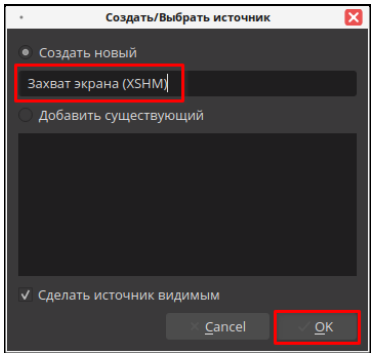
Запись экрана и звука

Для записи видео экрана и звука используется функция захвата экрана.

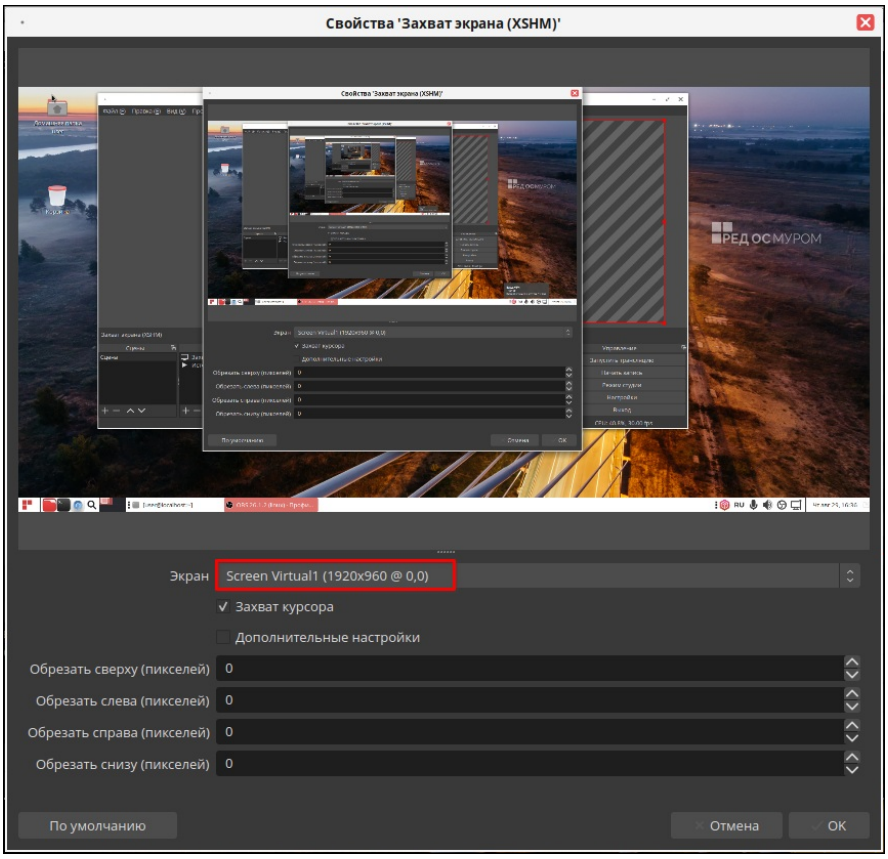
1.Нажмите на кнопку  и выберите «**Захват экрана**» из списка источников.



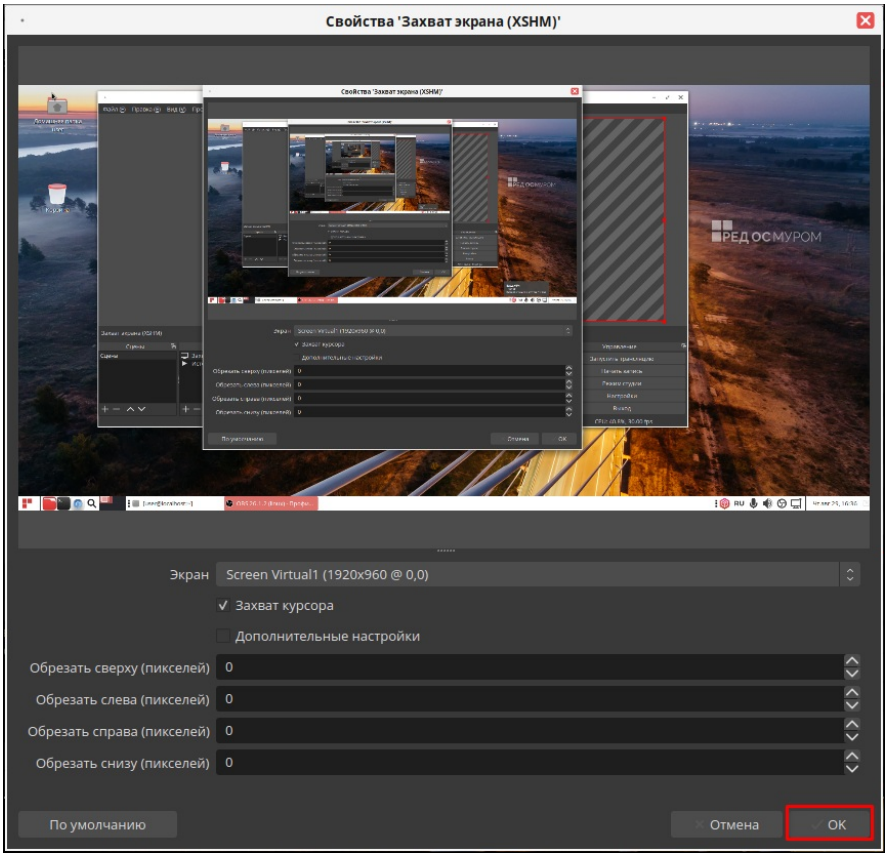
2. Введите название для источника захвата экрана и нажмите «**OK**».



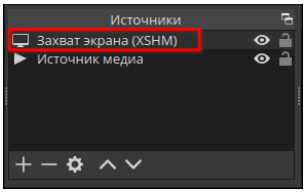
3. В открывшемся окне выберите экран, который необходимо записать. Если несколько экранов, убедитесь, что вы выбрали правильный. Запомните разрешение экрана, так как оно понадобится при редактировании видео.



4. Нажмите «**OK**» для сохранения настроек захвата экрана.

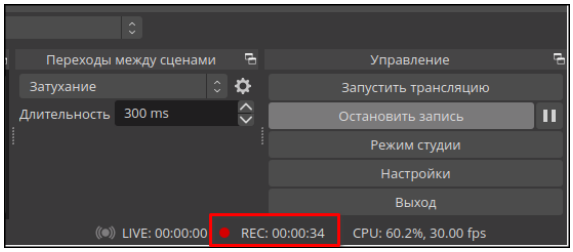


5. В списке источников будет отображен новый источник «**Захват экрана**».



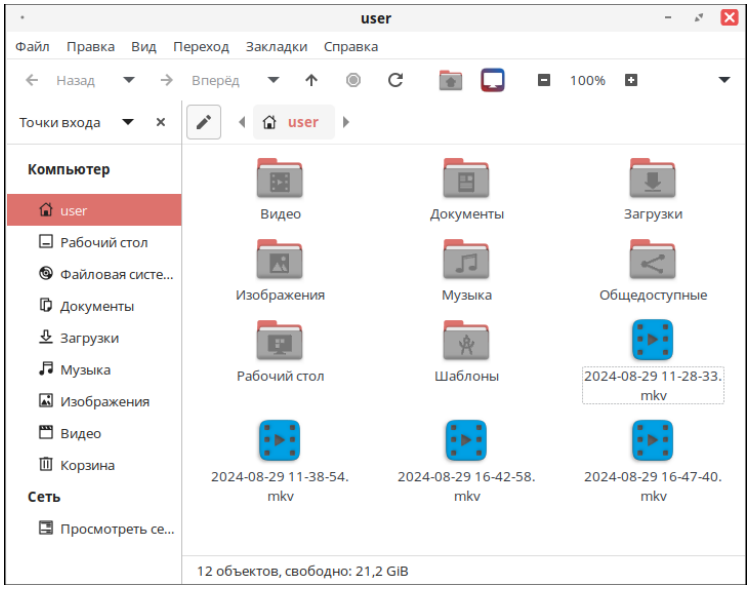
6. Нажмите «**Начать запись**» (или воспользуйтесь горячей клавишей), чтобы начать запись видео с экрана. Красная точка на значке

REC в нижней части экрана указывает на то, что запись началась.



7. Чтобы остановить запись, нажмите на кнопку «**Остановить запись**» или используйте горячую клавишу.

8. Для просмотра записей перейдите в меню «**Файл**» — «**Показать записи**». После этого можно начинать редактирование или просмотр записей.



Если необходимо записывать только звук, а не показывать какие-либо изображения, можно:

- поместить источник захвата экрана позади всех других источников;
- отредактировать преобразование источника захвата экрана, чтобы установить размер с нулевой шириной на нулевую высоту.

Перепаковка записей

Перепаковка записей — позволяет конвертировать любой формат видео в mp4-формат. Для конвертирования записей в другом формате перейдите в меню «**Файл**» — «**Перепаковать записи**». В открывшемся окне загрузите файл, нажав на значок  и выбрав запись (или несколько записей). Затем нажмите «**Перепаковка**».

SimpleScreenRecorder — программа записи экрана

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: simplescreenrecorder-0.4.4

Вы можете подробнее ознакомиться с созданием скриншотов и возможностью записи видео с экрана, просмотрев наши обучающие видео:

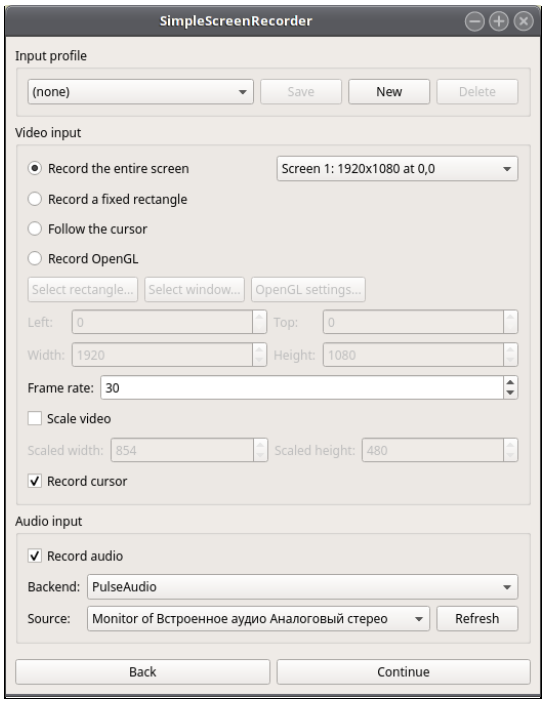
- на **RuTube** — Запись видео с экрана;
- в **Яндекс.Дзен** — Запись видео с экрана.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы выполните команду (потребуются права **администратора**):

```
sudo dnf install simplescreenrecorder
```

Запуск программы доступен из «**Главного меню**» - «**Аудио и Видео**» - «**SimpleScreenRecorder**».



Раздел Video input содержит параметры:

1) **Record the entire screen** — в случае если мониторов несколько, можно указать, какой именно записывать и захватывать с него видео.

2) **Record a fixed rectangle** — в случае, когда снимать видео необходимо с определенного участка экрана, с помощью инструмента Select rectangle можно выделить область при помощи мыши. Select window — инструмент, при помощи которого можно выбрать любое окно, с которого необходимо захватывать видео.

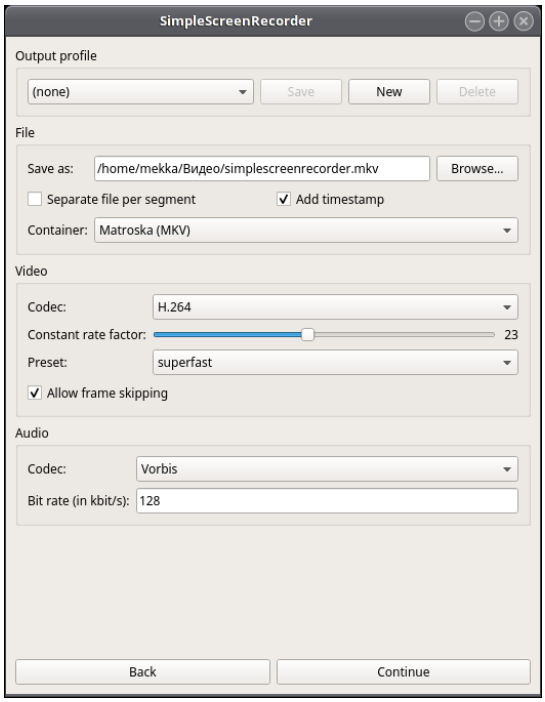
3) **Follow the cursor** — в таком режиме можно захватывать видео только в пределах движения курсора. Этот самый предел необходимо указывать в параметре Width и Height.

4) **Record OpenGL** — запись видео с программ, поддерживающих OpenGL (в основном касается игр).

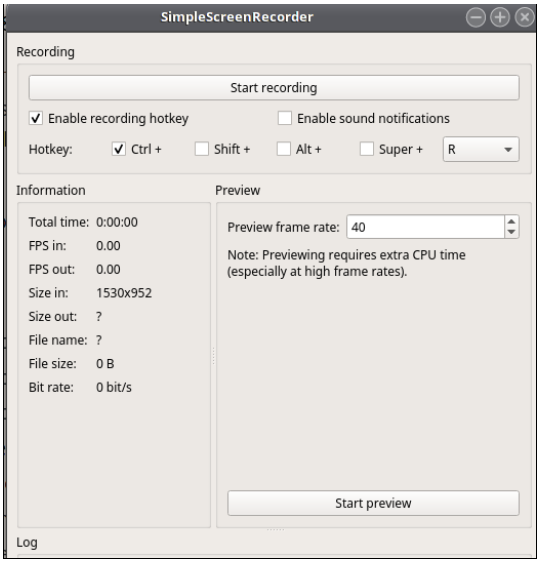
Frame Rate — частота кадров записи (чем больше, тем плавнее итоговая картинка, но размер больше). Учтите, что человек воспринимает нормально 24 кадра или более, меньше кадров для человека будет казаться изображением дёрганным.

Audio Input — если видео запись звука не нужна, можно выключить, сняв галку с атрибута « **Record Audio**».

Все настройки можно сохранить в профиль для будущих записей в Разделе Input Profile.



Для создаваемого профиля можно задать различные настройки, в том числе, путь для сохранения файла.



Начать запись можно с помощью кнопки «**Start Recording**». Закончить с помощью той же кнопки (на кнопке будет надпись «**Pause Recording**»).

Start Preview — необходима для проверки записи без фактической записи в файл в реальном времени. Для создаваемого профиля можно задать различные настройки, в том числе, путь для сохранения файла.

Видеоредактор VLC

Установка
Описание программы
Запись видео с экрана
Запись аудио- и видеофайла
Настройки
Сброс настроек
Просмотр списка воспроизведения
Преобразование и сохранение медиафайла
Настройка потокового вещания VLC

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: vlc-3.0.21

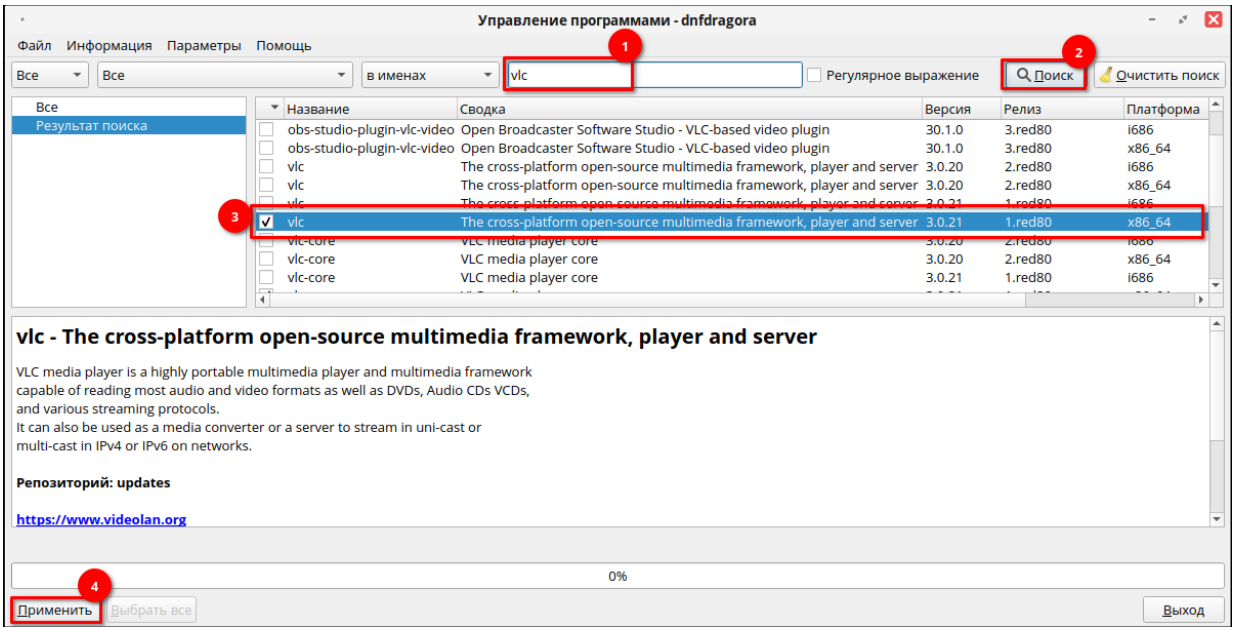
VLC Media Player — кроссплатформенный медиапроигрыватель, разрабатываемый проектом VideoLAN. Плеер **VLC** можно использовать в качестве сервера для трансляции потока аудио/видео по сети. Для воспроизведения файлов мультимедиа не требуется установка дополнительных кодеков.

VLC может воспроизводить DVD и потоковое незашифрованное видео (IPTV) и интернет-радио. Также программа может записывать потоковое аудио/видео на компьютер. **VLC Media Player** поддерживает следующие форматы: **MKV**, **MP4**, **AVI**, **MOV**, **OGG**, **FLAC**, **CD**, **ASF**, **TS**, **M2TS**, **Webm** и **AAC**.

Установка

По умолчанию программа уже предустановлена в РЕД ОС. Если программа у вас не установлена, установить её можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**vlc**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install vlc
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

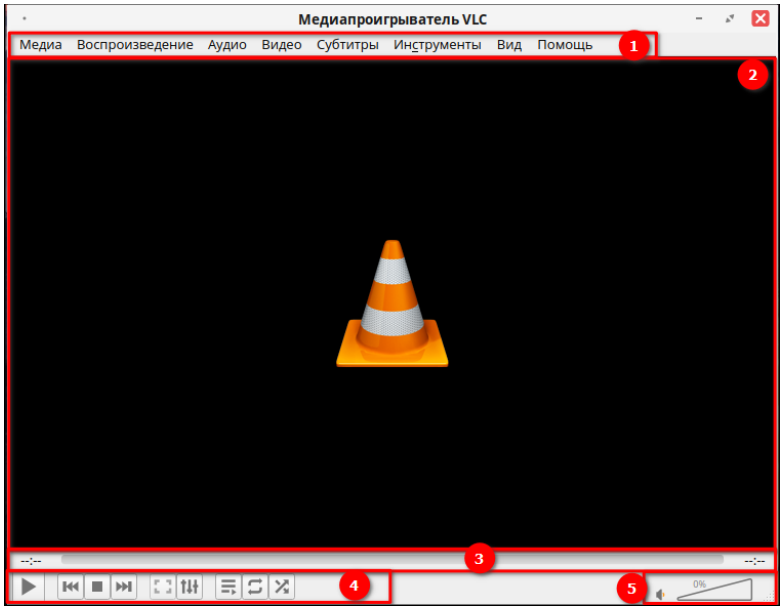
Для запуска программы через терминал введите команду:

```
vlc
```

Для запуска программы через графический интерфейс перейдите в «**Главное меню**» — «**Аудио и Видео**» («**Мультимедиа**») — «**Медиаплеер VLC**».

Описание программы

Главное окно программы выглядит следующим образом:



1. **Основное меню** позволяет выполнять различные действия с создаваемым видео, а также настраивать программу и плейлист.

2. **Рабочая область** предназначена для размещения элементов.

3. **Слайдер дорожки** находится поверх кнопок управления. Он показывает ход воспроизведения медиафайла. Вы можете перетащить ползунок дорожки влево для перемотки назад или вправо для перемотки вперёд воспроизводимой дорожки.

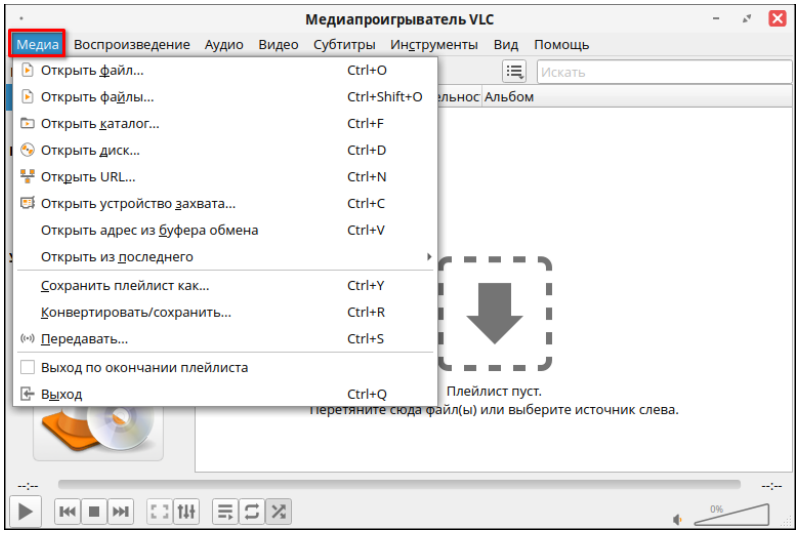


4. **Панель инструментов** — основные действия для работы с плейлистом, такие как воспроизведение, открытие файла, предыдущая или следующая позиция плейлиста, режим повтора, случайный порядок.

5. **Регулятор громкости** расположен в правом нижнем углу окна. Значок динамика увеличивает, уменьшает громкость или отключает звук. Ползунок показывает текущую громкость воспроизведения. Нажатие на него изменяет громкость. Громкость воспроизведения также отображается в процентах поверх ползунка.

Меню «Медиа»

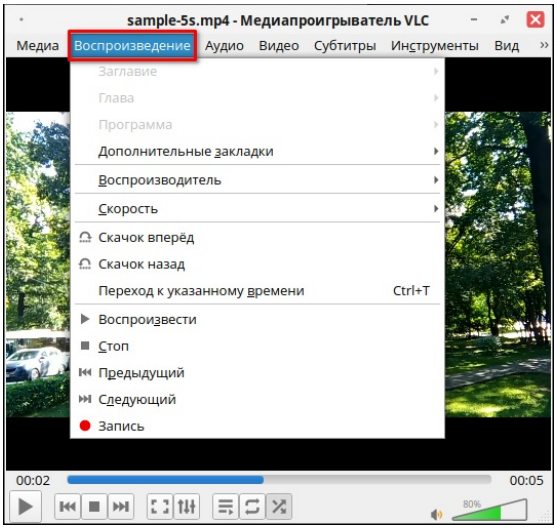
Из пункта меню «**Медиа**» доступны базовые функции для добавления и сохранения видео- и аудиозаписей.



Для воспроизведения медиафайла перейдите в меню «**Медиа**» — «**Открыть файл**». Выберите файл.

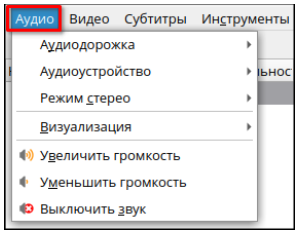
Меню «Воспроизведение»

В пункте меню «**Воспроизведение**» размещены основные действия для работы с плейлистом.



Меню «Аудио»

Для настройки параметров звука перейдите в меню «**Аудио**» и выберите все необходимые настройки.



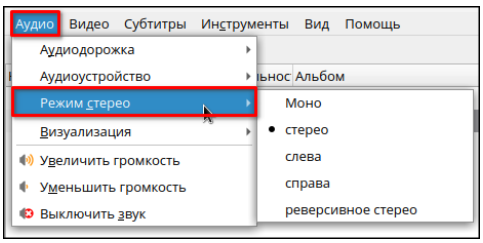
Раздел «**Аудиодорожка**» позволяет включать и отключать аудиодорожки.

Для включения аудиодорожки выберите в меню «**Аудио**» — «**Аудиодорожка**» — «**Дорожка 1**».

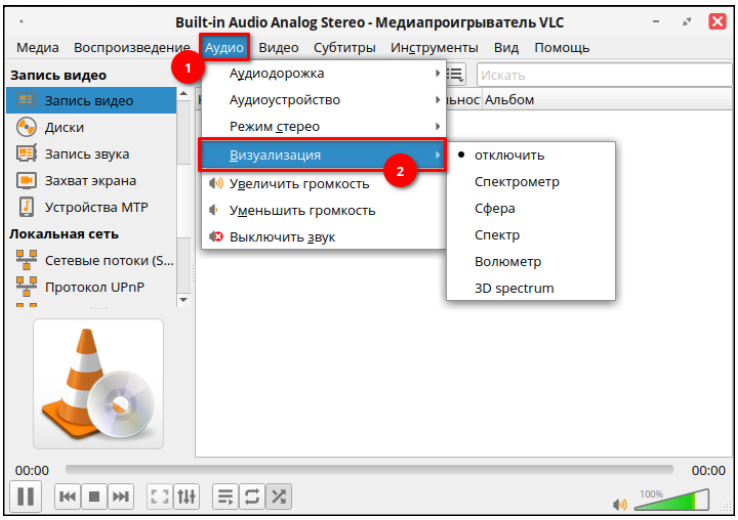
Для отключения аудиодорожки перейдите в «**Аудио**» — «**Аудиодорожка**» — «**Отключить**».

Опция «**Режим стерео**» позволяет прослушивать аудиофайлы в различных режимах:

- ***моно*** (монофонический звук) использует один канал для воспроизведения звука;
- ***стерео*** относится к звуку, который использует два канала для воспроизведения звука или стереофонического звучания;
- при выборе опции ***слева*** музыка будет воспроизводиться только в левом динамике;
- при выборе опции ***справа*** музыка будет воспроизводиться только из динамика справа;
- ***реверсивное стерео*** предназначено для воспроизведения звука одновременно с видео.

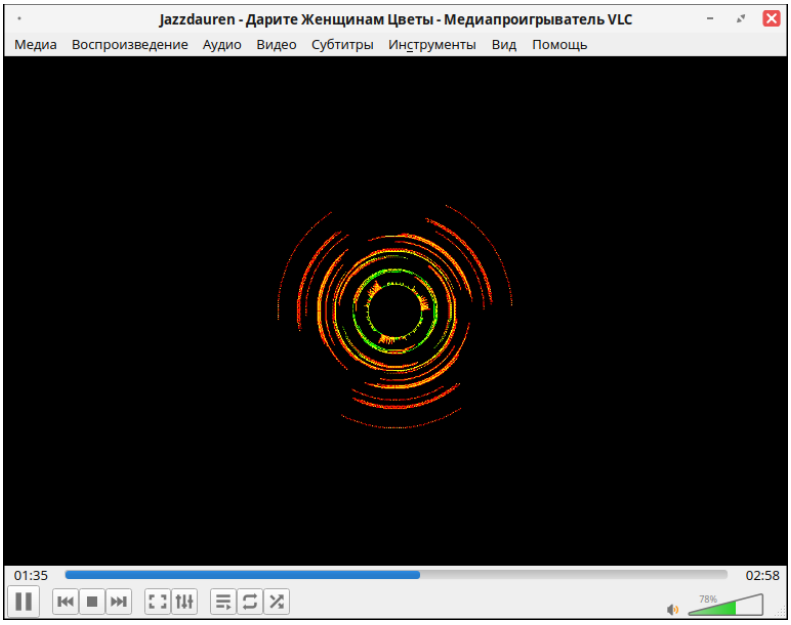


Для просмотра доступных визуальных эффектов перейдите в меню «**Аудио**» — «**Визуализация**».



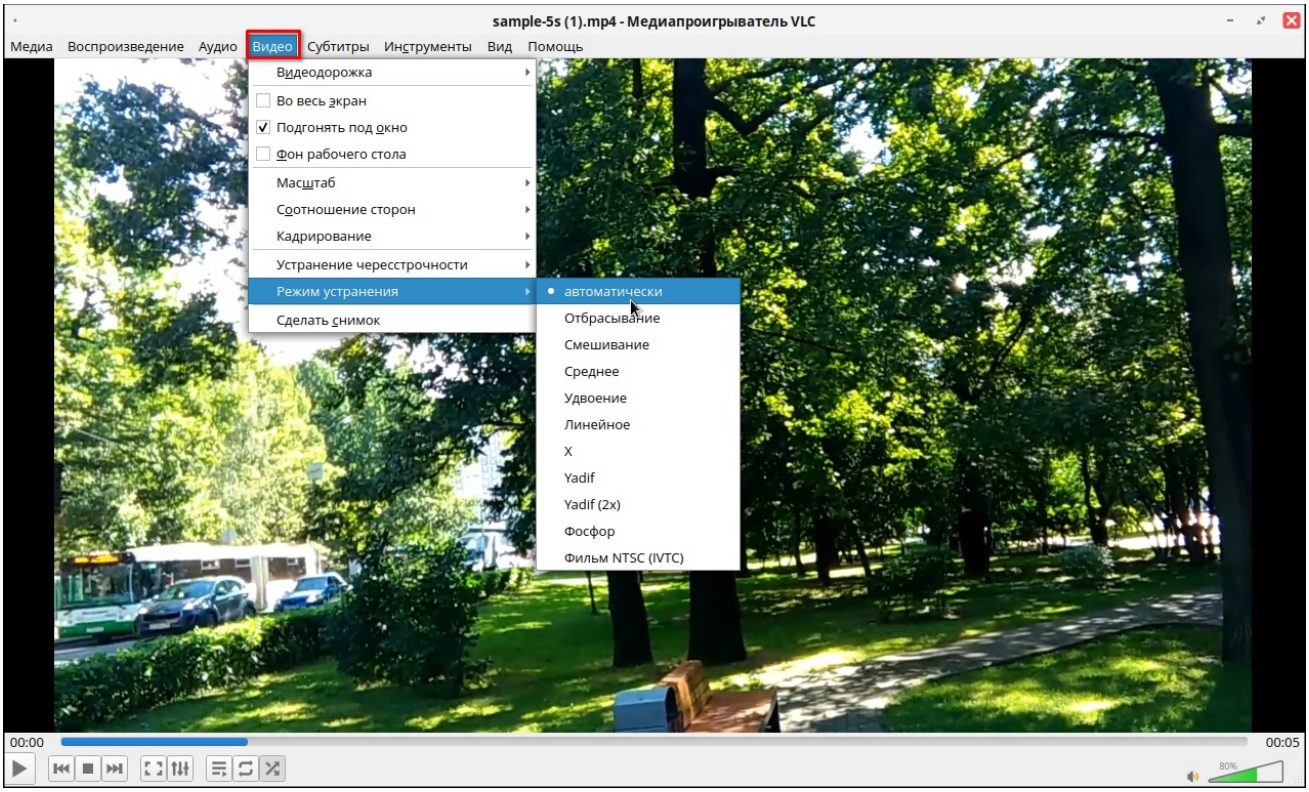
С помощью визуализации можно добавить спектрометр, сферу, волюметр, геометрические формы, которые будут генерировать изображения на основе музыкального произведения.

Спектрометр отображает звуковые частоты аудио в виде графического спектра:



Меню «Видео»

В меню «**Видео**» содержатся настройки, которые позволяют пользователю управлять отображением и воспроизведением видео.



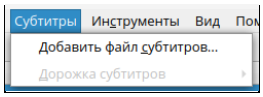
Меню «Субтитры»

Старые форматы файлов (например, ***.avi**) не могут обрабатывать субтитры напрямую. Файл субтитров содержит текст субтитров и временные метки.

Для добавления файла субтитров перейдите в меню «**Субтитры**» — «**Добавить файл субтитров...**».

Субтитры можно скачать с официального сайта.

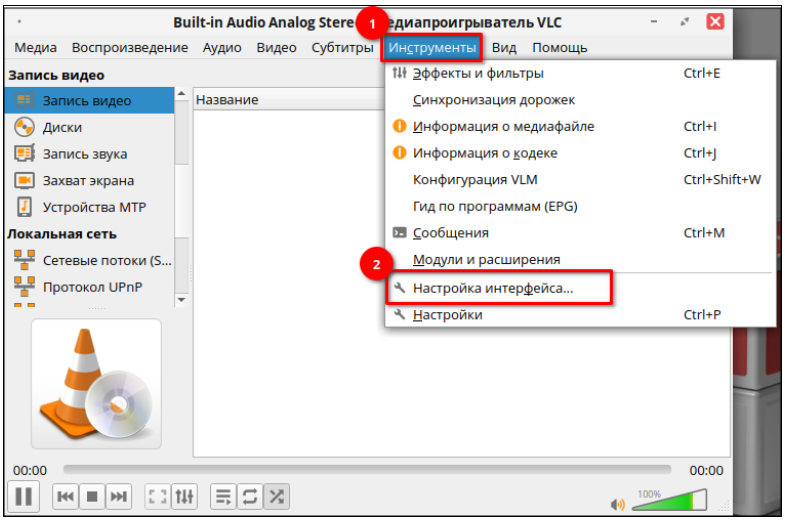
Примечание. Для автоматической загрузки субтитров убедитесь, что файл субтитров находится в той же папке, что и видеофайл, имеет такое же имя (за исключением расширения), как видеофайл, и использует поддерживаемый формат (например, ***.cdg**, ***.idx**, ***.srt**, ***.sub**, ***.ass**, ***.ssa** и другие). Например, если ваш видеофайл называется **film.mp4**, то файл субтитров должен называться **film.srt**.



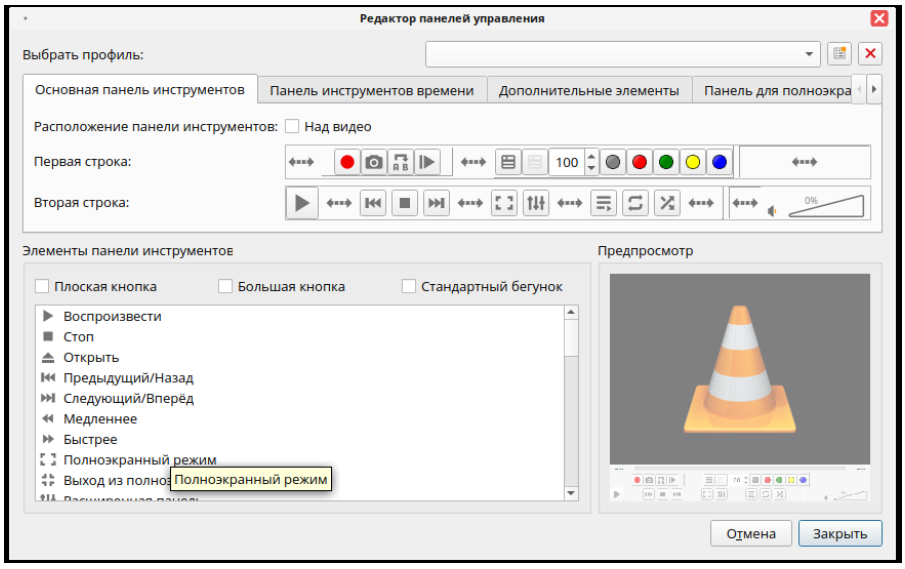
После добавления субтитров вы сможете включить их в меню: «**Субтитры**» — «**Дорожка субтитров**». Будут перечислены все треки с субтитрами. Для отключения опции выберите «**Субтитры**» — «**Дорожка субтитров**» — «**Отключить**».

Меню «Инструменты»

Изменить настройки элементов интерфейса можно в меню «**Инструменты**» (1) — «**Настройка интерфейса...**» (2).



В открывшемся окне можно производить настройку интерфейса плеера.



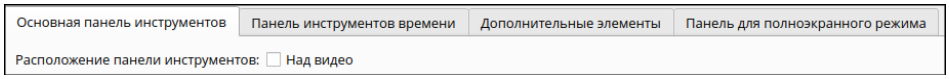
Рядом со строкой выбора профиля находятся две кнопки.



 — позволяет создать собственный профиль.

 — удаляет профиль.

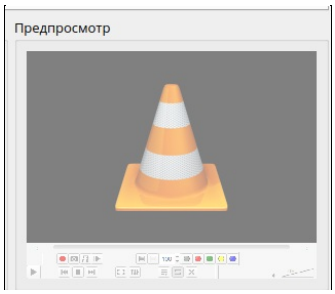
В области ниже можно выбрать тот участок интерфейса, в котором нужно изменить расположение кнопок и ползунков. Переключаться между такими участками позволяют четыре вкладки.



Кнопки и ползунки можно перемещать, зажав нужный элемент ЛКМ, после чего перенести его в нужное место или удалить. Для удаления элемента необходимо просто перетащить его за рабочую область.



Просмотреть результат изменений можно в окне предпросмотра.

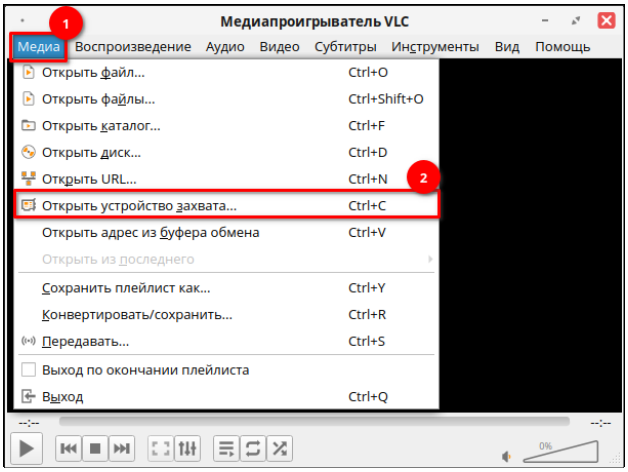


По окончании всех изменений нужно будет просто нажать кнопку «**Закрыть**». Это позволит сохранить все настройки и просмотреть результат в самом плеере. На этом процесс настройки интерфейса завершён.

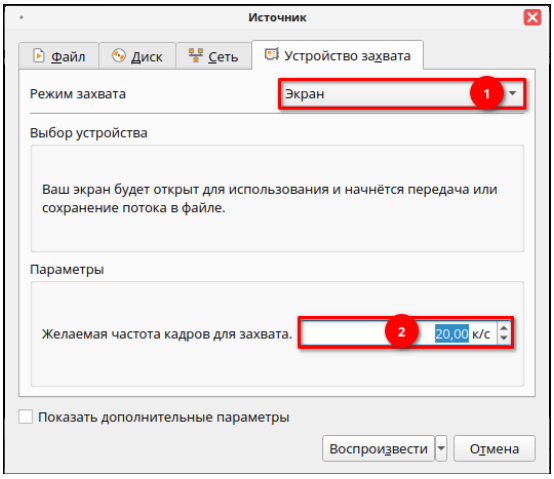
Запись видео с экрана

Для записи видео экрана вашего компьютера необходимо выполнить следующие действия:

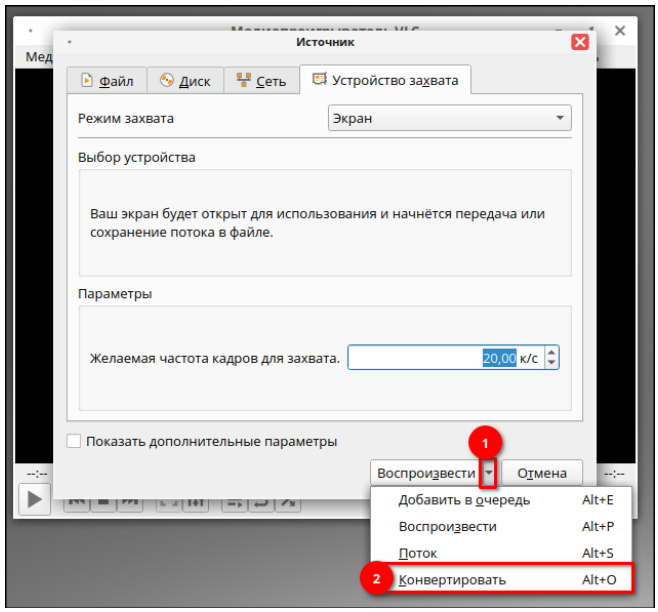
1. Открыть меню «**Медиа**» и выбрать пункт «**Открыть устройство захвата...**».



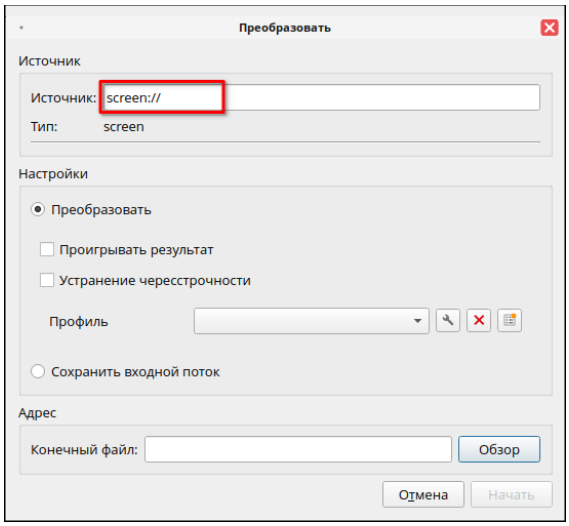
2. В режиме захвата выбрать «**Экран**», в параметрах указать желаемую частоту кадров. Рекомендуется указать значение **20 к/с**, в зависимости от желаемой плавности видео и свободной памяти (чем выше количество кадров в секунду, тем более качественное видео и больший размер выходного файла).



3. Раскрыть выпадающий список, нажав на стрелку рядом с кнопкой «**Воспроизвести**» и выбрать «**Конвертировать**» для продолжения процесса.

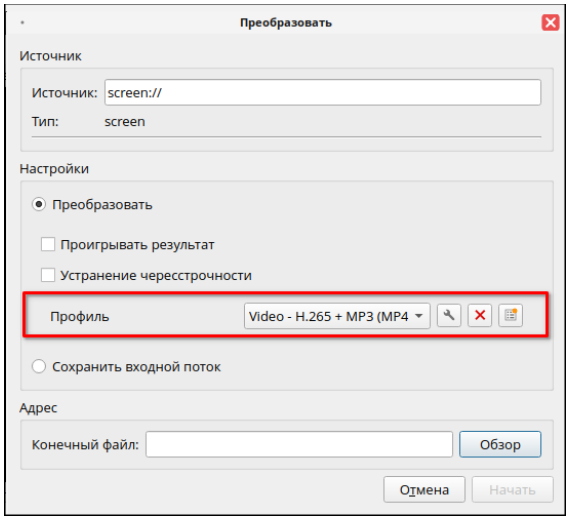


4. После нажатия кнопки «**Конвертировать**» должно появится окно «**Преобразовать**». Необходимо убедиться, что источником видео является экран компьютера (в строке «**Источник**» должно отображаться **screen://)**.

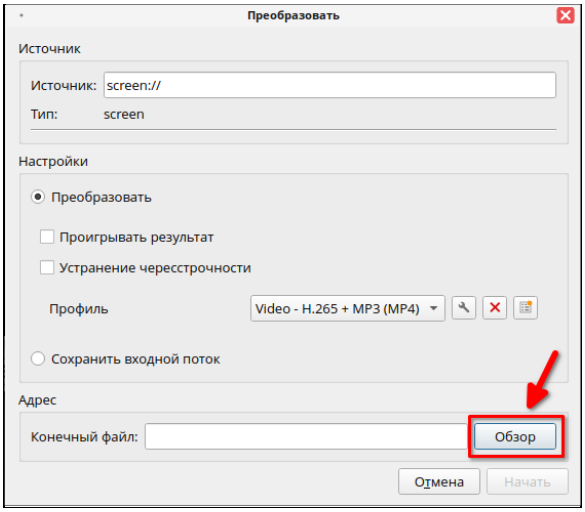


5. В Профиле настроить параметры видео, выбрать подходящий кодек. Например, **Video - H.264 + MP3 (MP4)**.

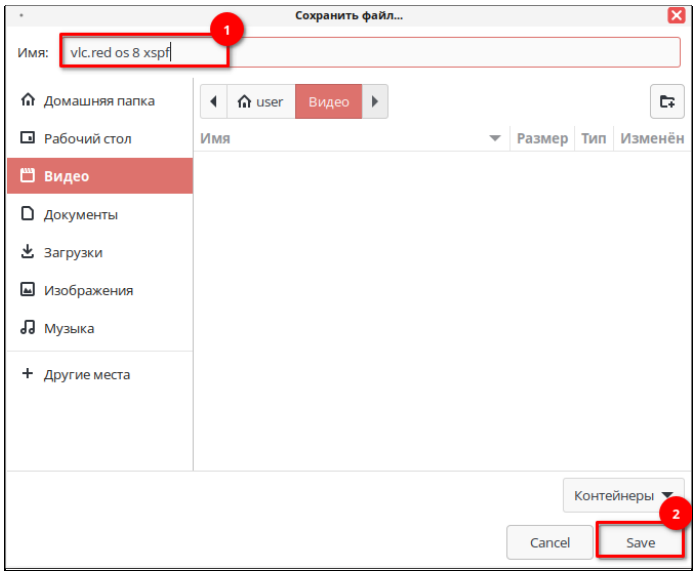
Кодеки – это специальные программы для кодирования и сжатия видео- и аудиодорожки.



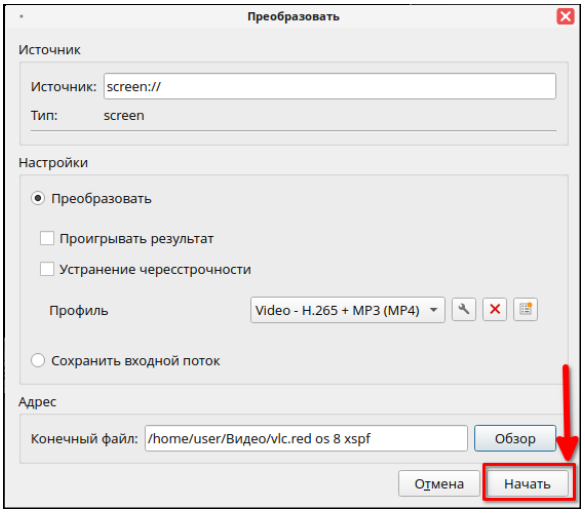
6. Для сохранения видеофайла нажать кнопку «**Обзор**».



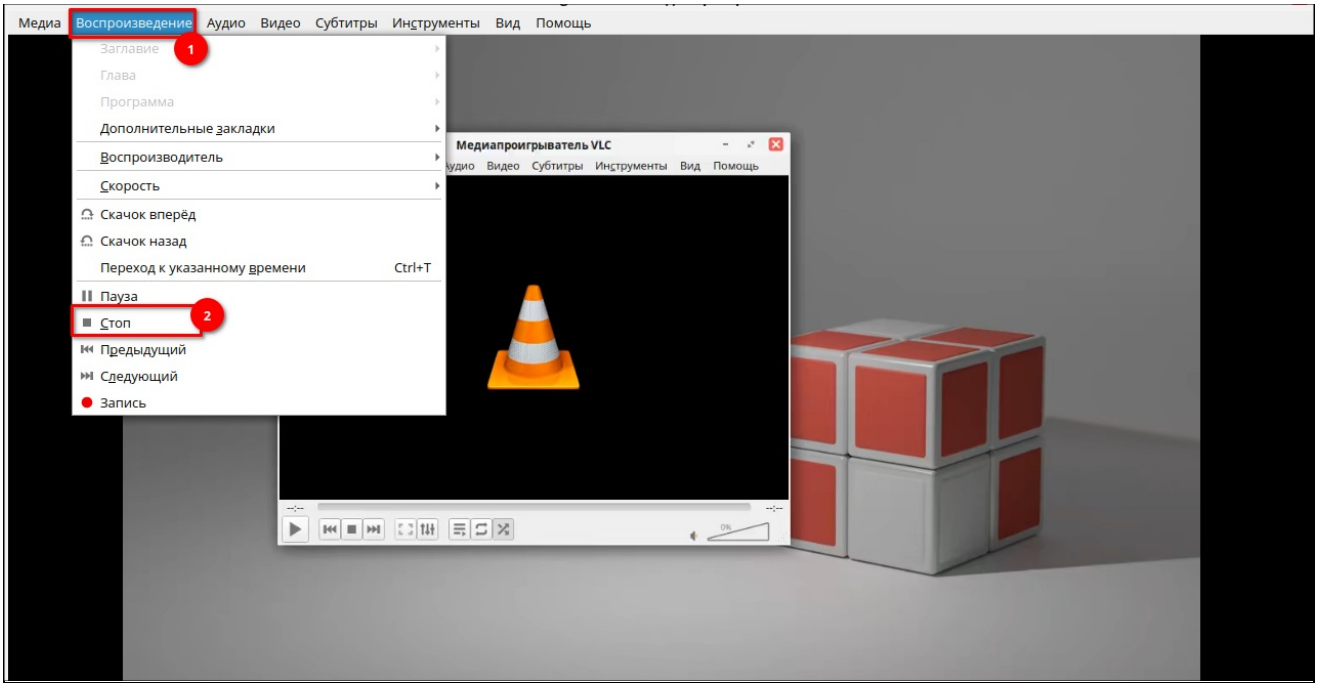
В открывшемся окне выбрать путь, ввести имя для сохранения файла и нажать «**Save**».



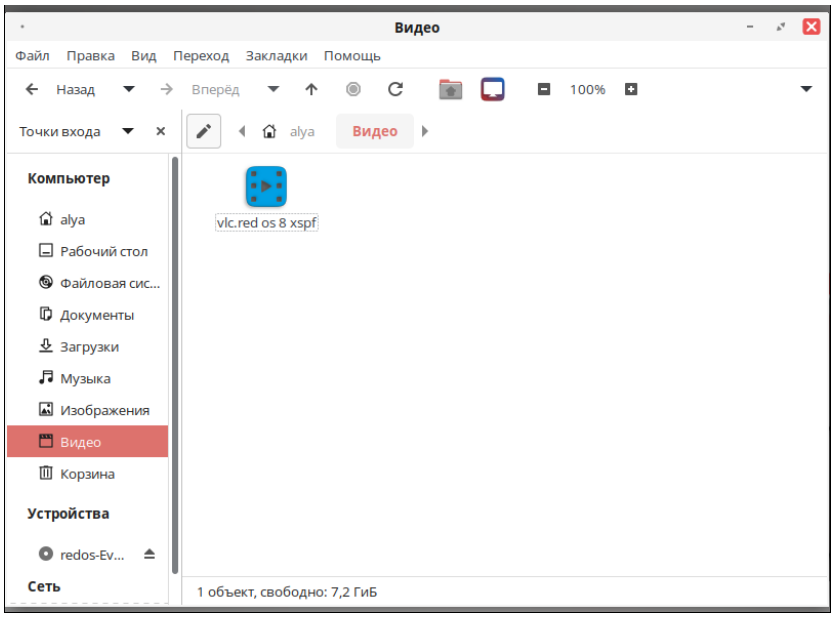
7. Для начала записи нажать кнопку «**Начать**». Начнётся запись видео всего рабочего стола. Запись можно поставить на паузу, а затем восстановить.



8. Для остановки записи перейти в меню «**Воспроизведение**» (1) — «**Стоп**» (2).

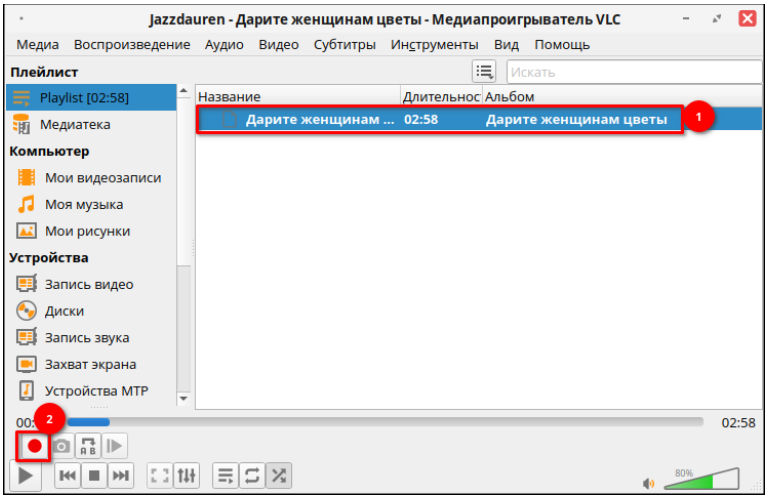


9. После окончания записи видео необходимо проверить его сохранение в диспетчере файлов, щёлкнуть по нему для просмотра результата записи.



Запись аудио- и видеофайла

Для записи аудио- и видеофайла на панели инструментов отобразите кнопку  . Для этого выберите в меню «**Вид**» — «**Доп. элементы управления**». Откройте аудио- или видеофайл (1) и нажмите на кнопку записи (2).



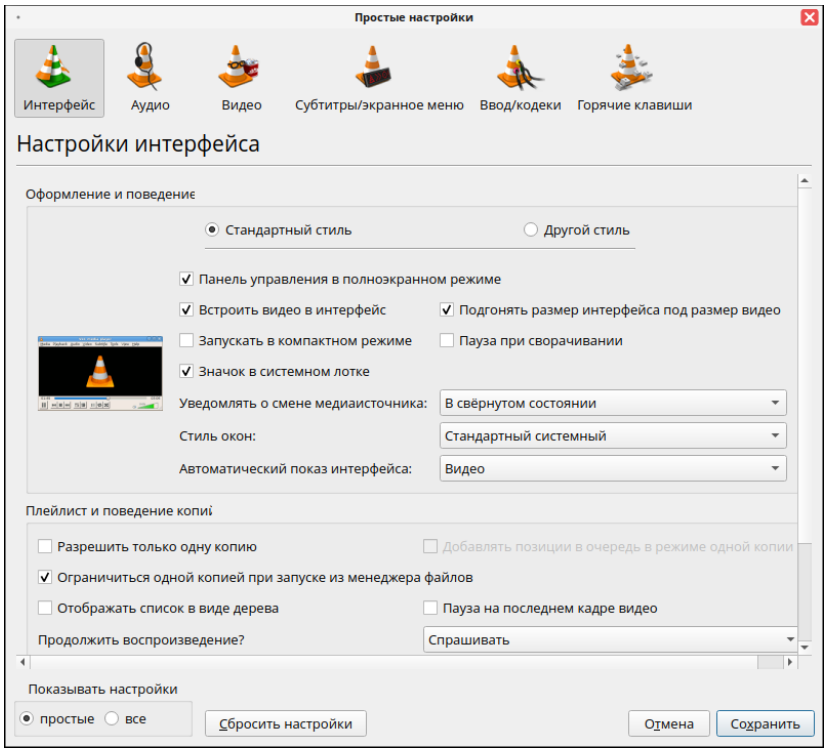
После записи медиафайла снова нажмите на красную кнопку.

Запись будет сохранена в отдельном файле в разделе «**Компьютер**» — «**Моя музыка**» или «**Мои видеозаписи**».

Для обрезки видео используйте кнопку  .

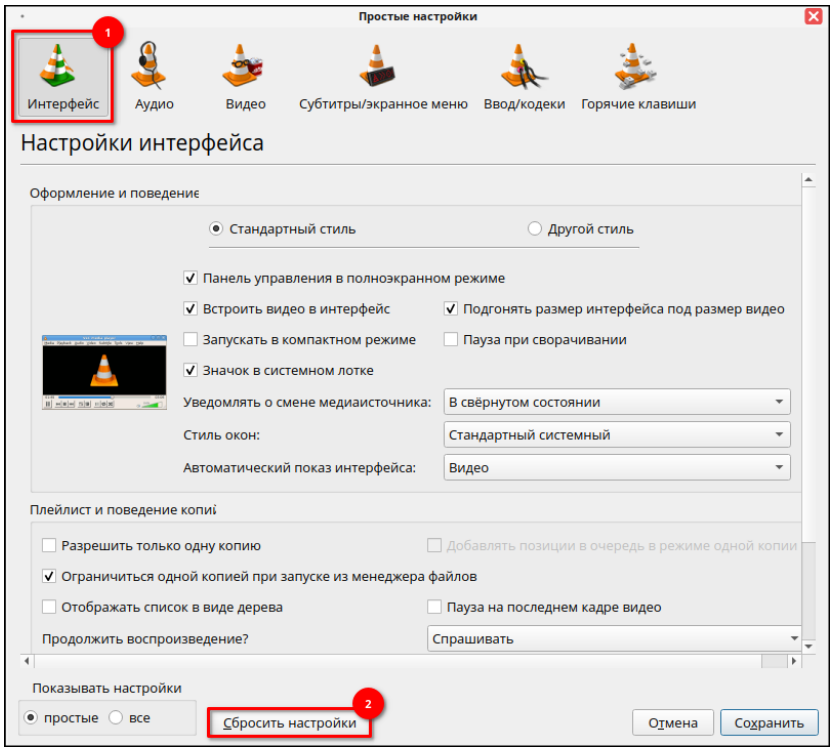
Настройки

Для доступа к панели настроек перейдите в меню «**Инструменты**» — «**Настройки**». Панель настроек позволяет изменять основные параметры VLC.



Сброс настроек

Для сброса настроек перейдите в меню «**Инструменты**» — «**Настройки**». Выберите вкладку с необходимыми настройками (1) и нажмите кнопку «**Сбросить настройки**» (2).



Просмотр списка воспроизведения

Для просмотра списка воспроизведения перейдите в меню «**Вид**» — «**Плейлист**».

1. **Плейлист** — текущий плейлист позволяет просматривать и управлять текущим списком воспроизведения мультимедийных файлов. Медиатека содержит все доступные аудио- и видеофайлы.

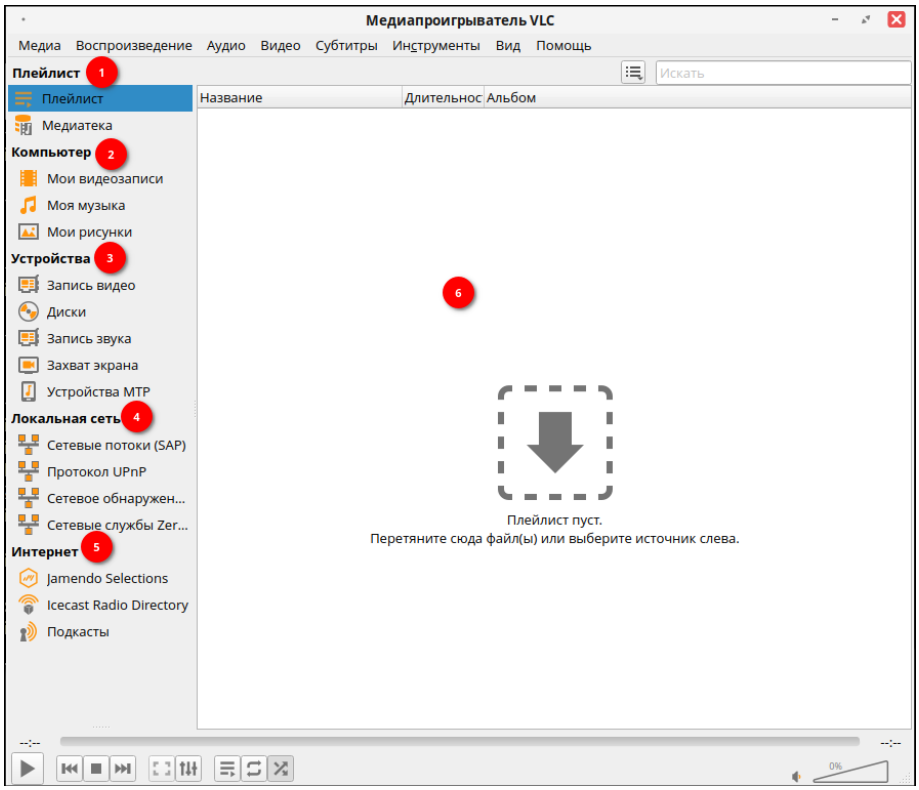
2. В разделе **Компьютер** отображаются стандартные каталоги и папки на компьютере, где обычно хранятся видео-, аудио- и снимки экрана.

3. **Устройства** — доступ к оптическим устройствам.

4. **Локальная сеть** — источники локальной сети, где можно обращаться к медийным файлам, которые доступны в локальной сети, используя различные сетевые протоколы, такие как SAP (Session Announcement Protocol), UPnP (Universal Plug and Play).

5. **Интернет** — раздел предлагает доступ к различным интернет-источникам, таким как подкасты, онлайн радиостанции и другие потоковые сервисы для онлайн прослушивания или просмотра.

6. **Список медиафайлов** — отображаются все доступные на устройстве медиафайлы.



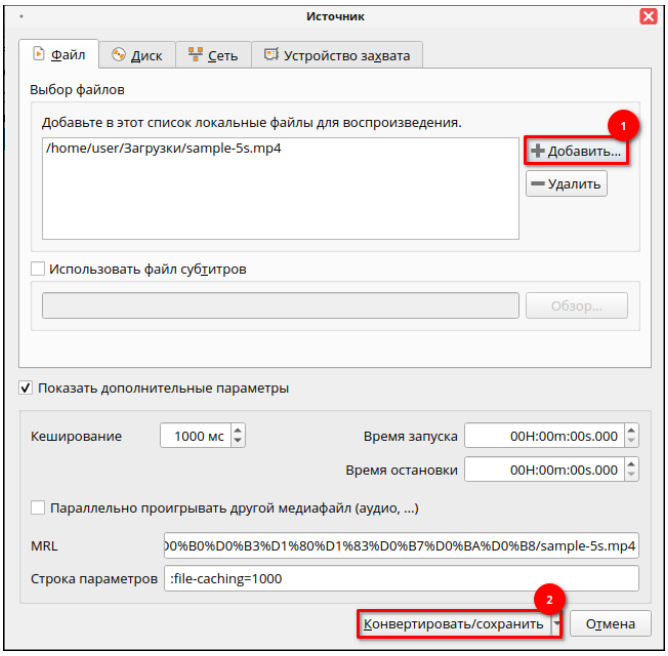
Преобразование и сохранение медиафайла

Для преобразования медиафайла из одного формата в другой выполните следующие шаги:

1. Перед конвертацией убедитесь, что выбранный формат поддерживается VLC. Перейдите в меню «**Медиа**» и выберите пункт «**Конвертировать/сохранить**». Появится диалоговое окно «**Источник**».

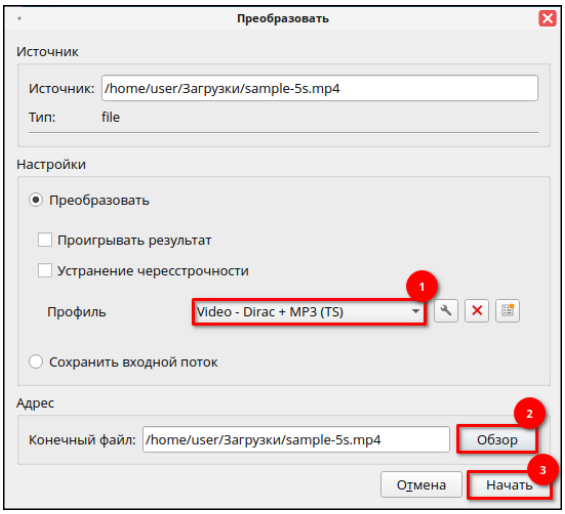
2. Для добавления файла нажмите «**Добавить...**» (1) и выберите файлы для конвертирования.

3. После добавления файла в список, нажмите на кнопку «**Конвертировать/сохранить**» (2). Перед началом конвертации вы можете настроить параметры выходного файла, такие как формат, качество и расположение сохранения.



4. Для конвертации медиафайла в появившемся диалоговом окне «**Преобразовать**» выберите **Профиль** для преобразования медиафайла (1).

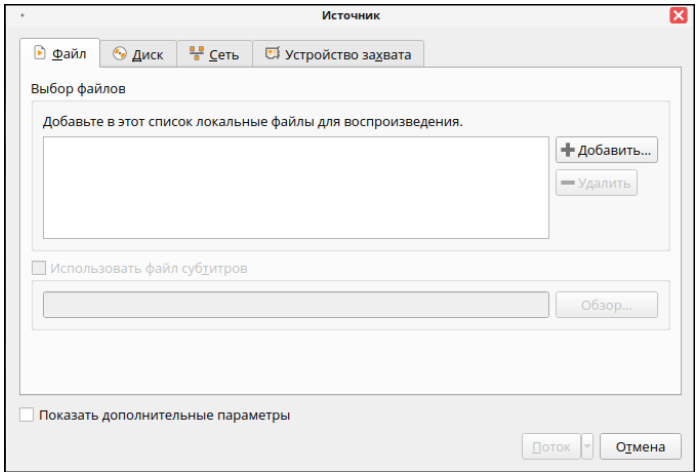
Для сохранения медиафайла нажмите «**Обзор**» (2), выберите имя и адрес конечного файла. Для запуска процесса конвертации и сохранения видео нажмите «**Начать**» (3). Дождитесь окончания конвертации и сохранения медиафайла.



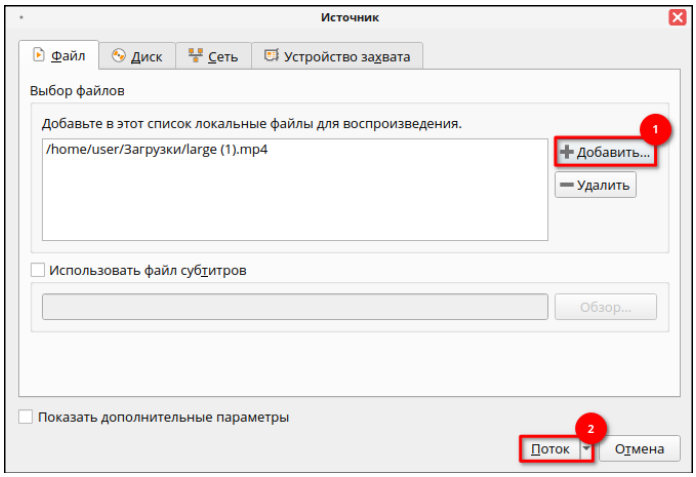
Настройка потокового вещания VLC

Для настройки видеовещания в рамках локальной сети выполните следующий алгоритм действий:

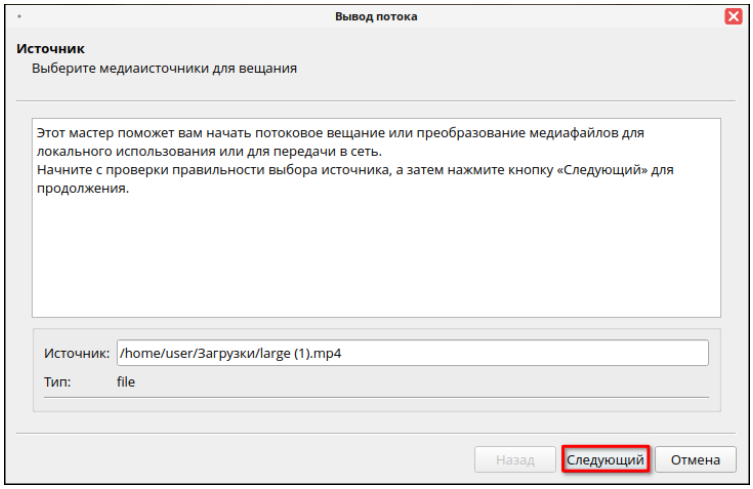
1. Перейдите в меню «**Медиа**» — «**Передавать...**». Откроется диалоговое окно «**Источник**».



2. Нажмите кнопку «**Добавить**» (1), выберите файл для воспроизведения и нажмите « **Поток**» (2).

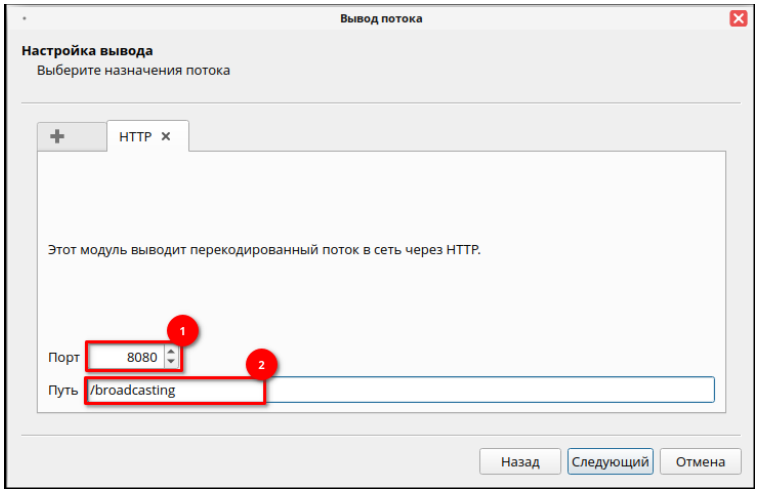


3. В окне «**Вывод потока**» проверьте выбор медиаисточника и нажмите кнопку «**Следующий**» для продолжения.

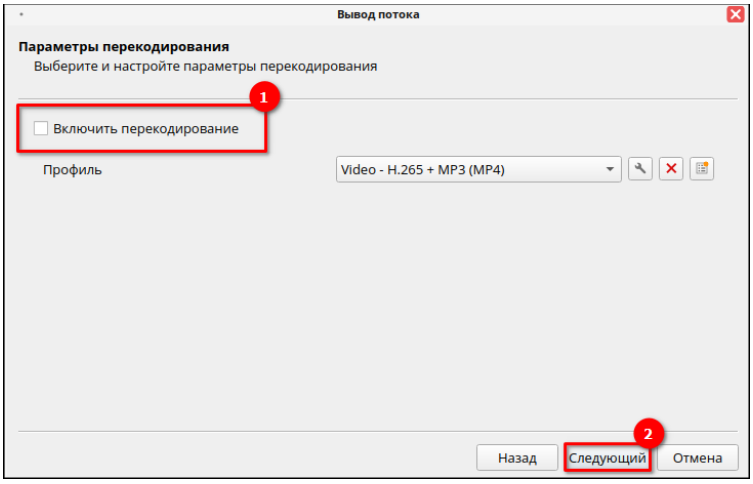


4. Выберите протокол для вещания из выпадающего списка. Отметьте HTTP и нажмите «**Добавить**».

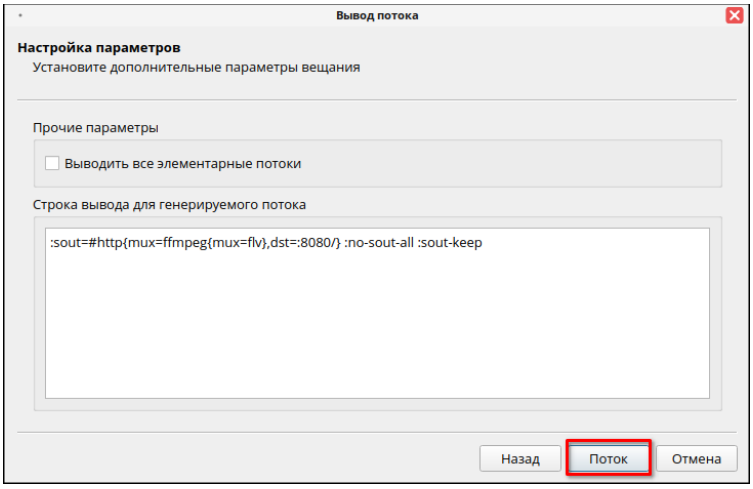
5. Укажите порт (например, **8080**) и произвольное слово в поле «**Путь**» (например, "**/broadcasting**").



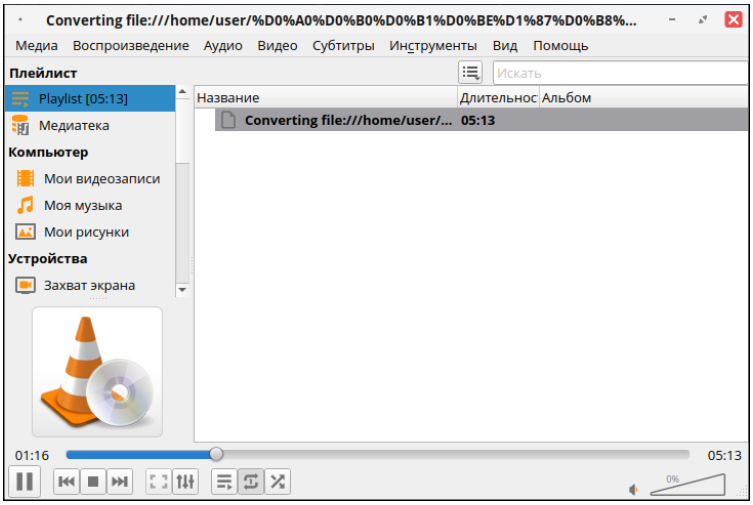
6. Выберите и настройте параметры перекодирования (1) и нажмите «**Следующий**» (2).



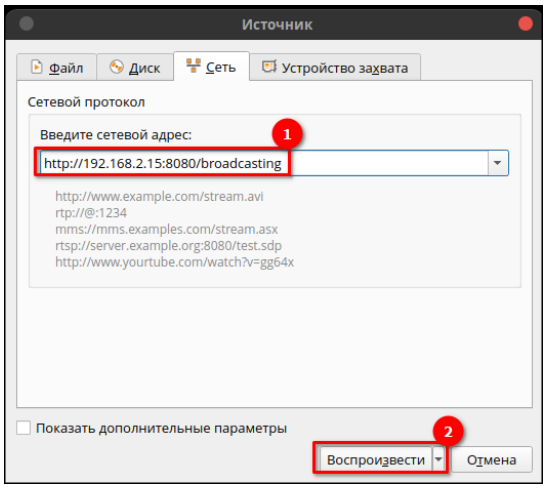
7. Подтвердите настройки, нажав «**Поток**».



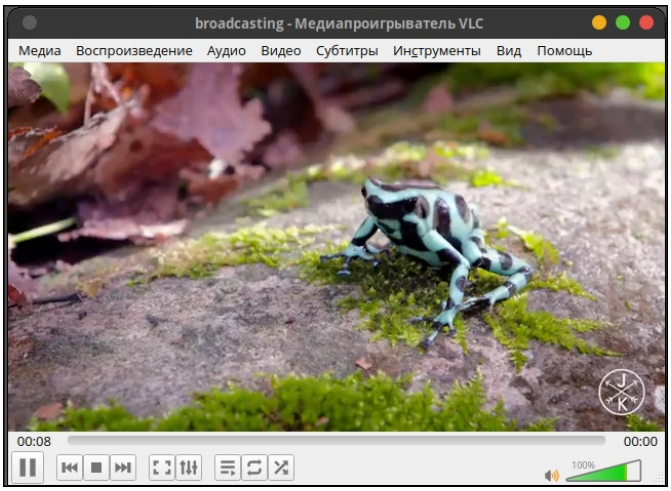
Трансляция отобразится в плеере.



8. Проверьте правильность настройки трансляции. Откройте другой плеер VLC. Перейдите в меню «**Медиа**» — «**Открыть URL**». В появившемся окне введите локальный IP-адрес. Добавьте порт и путь, указанные при потоковой настройке. Например, «**http://192.168.2.15:8080/broadcasting**». Замените адрес 192.168.2.15 на свой локальный (сетевой) IP-адрес. Нажмите кнопку «**Воспроизвести**».



В другом плеере отобразится видеовещание **broadcasting**.


broadcasting - Медиапроигрыватель VLC
Медиа Воспроизведение Аудио Видео Субтитры Инструменты Вид Помощь
00:08
00:00
100%

DaVinci Resolve - редактирование видео

Установка
Первоначальная настройка

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** DaVinci_Resolve_18.0.4

DaVinci Resolve — приложение для цветокоррекции и нелинейного редактирования видео, также является единственным в мире решением для монтажа и цветокоррекции, наложения визуальных эффектов, создания графики и постобработки звука в единой программной среде.

DaVinci Resolve используется для монтажа фильмов, сериалов, рекламных роликов, телепрограмм и видеоклипов.

Примечание.

Программа работает только с проприетарными видеодрайверами **Nvidia** и **AMD**. По большей части *DaVinci Resolve* оптимизирована под *Nvidia*, поэтому убедитесь что у вас установлена последняя версия видеодрайвера.

Подробную информацию об установке видеодрайвера см. в нашей статье «Установка драйвера Nvidia в РЕД ОС».

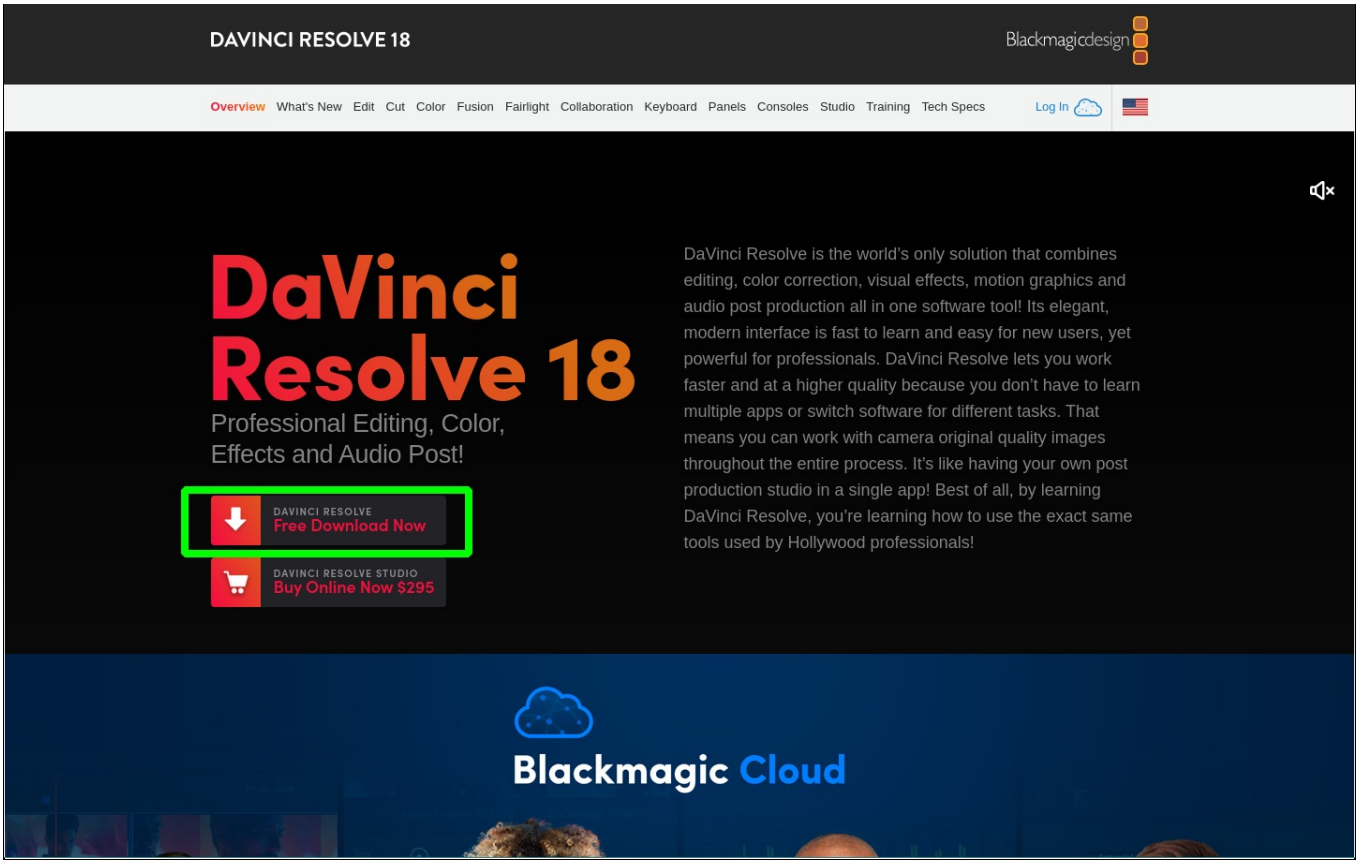
Вы можете подробнее ознакомиться с установкой и работой программы **DaVinci Resolve**, просмотрев наши обучающие видео:

- на **RuTube** — Установка DaVinci Resolve в РЕД ОС;
- в **Яндекс.Дзен** — Установка DaVinci Resolve в РЕД ОС;
- в **VK Видео** — Установка DaVinci Resolve в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Перейдите на официальный сайт DaVinci Resolve и нажмите **Загрузить сейчас**.



Потребуется ввести контактные данные, а затем можно будет загрузить дистрибутив. В данном случае будет загружена бесплатная редакция.

После загрузки нужно распаковать скачанный архив. Для этого перейдите в папку с архивом (в примере **/home/user/Загрузки/**):

```
cd /home/user/Загрузки/
```

И выполните команду распаковки:

```
unzip ./DaVinci_Resolve_18.0.4_Linux.zip
```

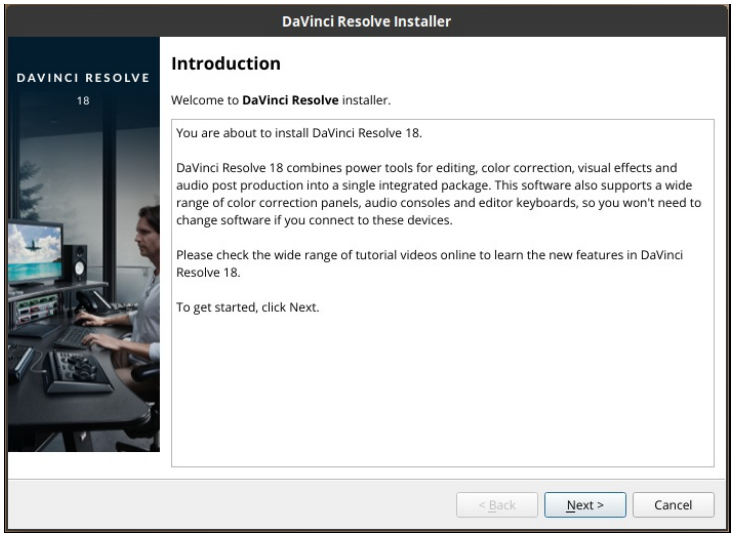
Назначьте файлу установки права на исполнение:

```
chmod +x ./DaVinci_Resolve_18.0.4_Linux.run
```

Для установки программы выполните:

```
./DaVinci_Resolve_18.0.4_Linux.run -i
```

Запуск установки также можно осуществить графически, дважды кликнув по файлу **DaVinci_Resolve_18.0.4_Linux.run**. Появится окно установщика.



Нажмите **Next**, ознакомьтесь с описанием программы, примите лицензионное соглашение и начните установку. Потребуется ввести пароль администратора или суперпользователя (**root**) системы.

Первоначальная настройка

После завершения процедуры установки перед непосредственным запуском программы потребуется произвести первоначальную настройку.

Программа устанавливается в каталог **/opt/resolve/bin/**. Перейдите в данный каталог и попробуйте запустить программу через терминал, чтобы убедиться в отсутствии каких-либо ошибок.

```
cd /opt/resolve/bin/
./resolve
```

Возможно появление сообщения вида:

```
./resolve: error while loading shared libraries: libgpudetect.so: cannot open shared object file: No such file or directory
```

Для решения данной проблемы необходимо создать символьную ссылку:

```
ln -s /lib64/libcrypt.so.2.0.0 libgpudetect.so
```

А также потребуется установить дополнительный пакет, выполнив команду:

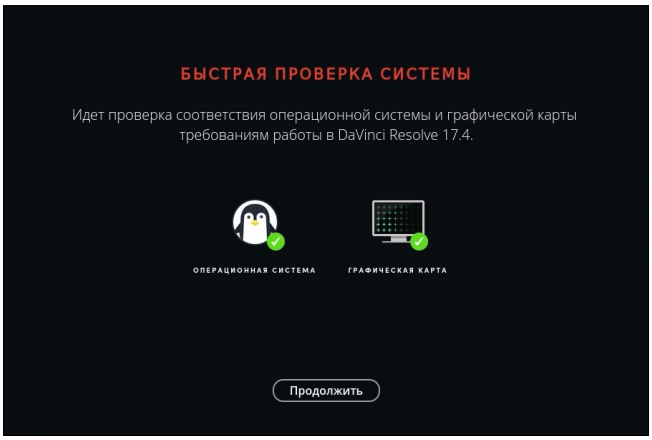
```
dnf install libxcrypt-compat
```

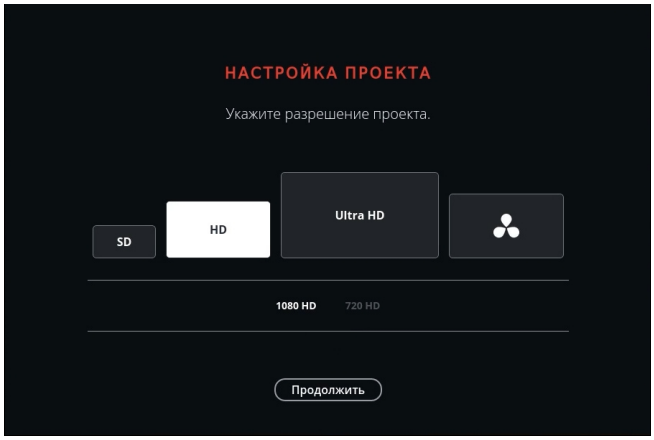
На этом подготовка системы окончена, и теперь можно запускать программу из «**Главного меню**» — «**DaVinci Resolve**» — «**DaVinci Resolve**».

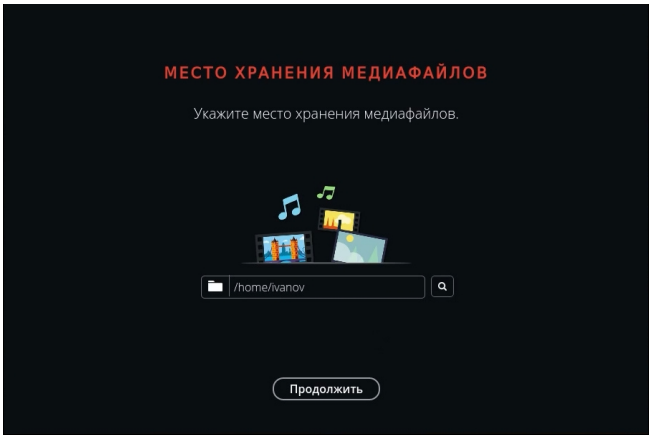
Приветственное окно программы выглядит следующим образом:

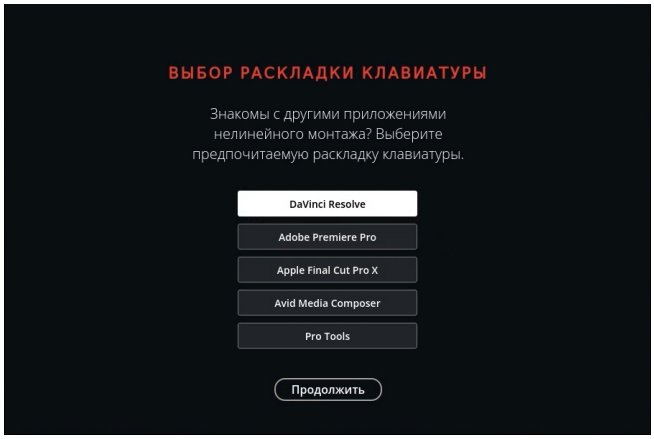


На начальном этапе можно установить русский язык и кратко ознакомиться с нововведениями. При нажатии на кнопку «**Продолжить**» можно пройти процедуру проверки и настройки, в том числе изменить место сохранения медиафайлов и настроить раскладку клавиатуры.

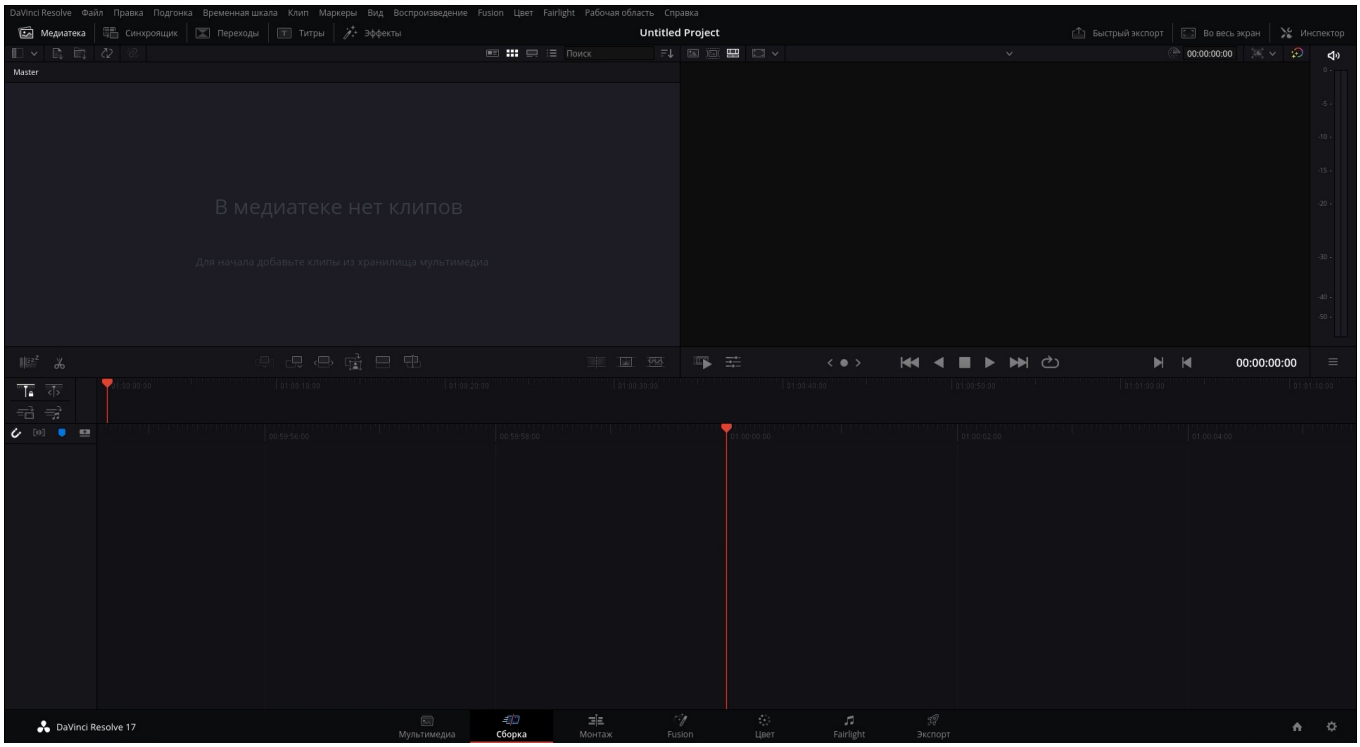








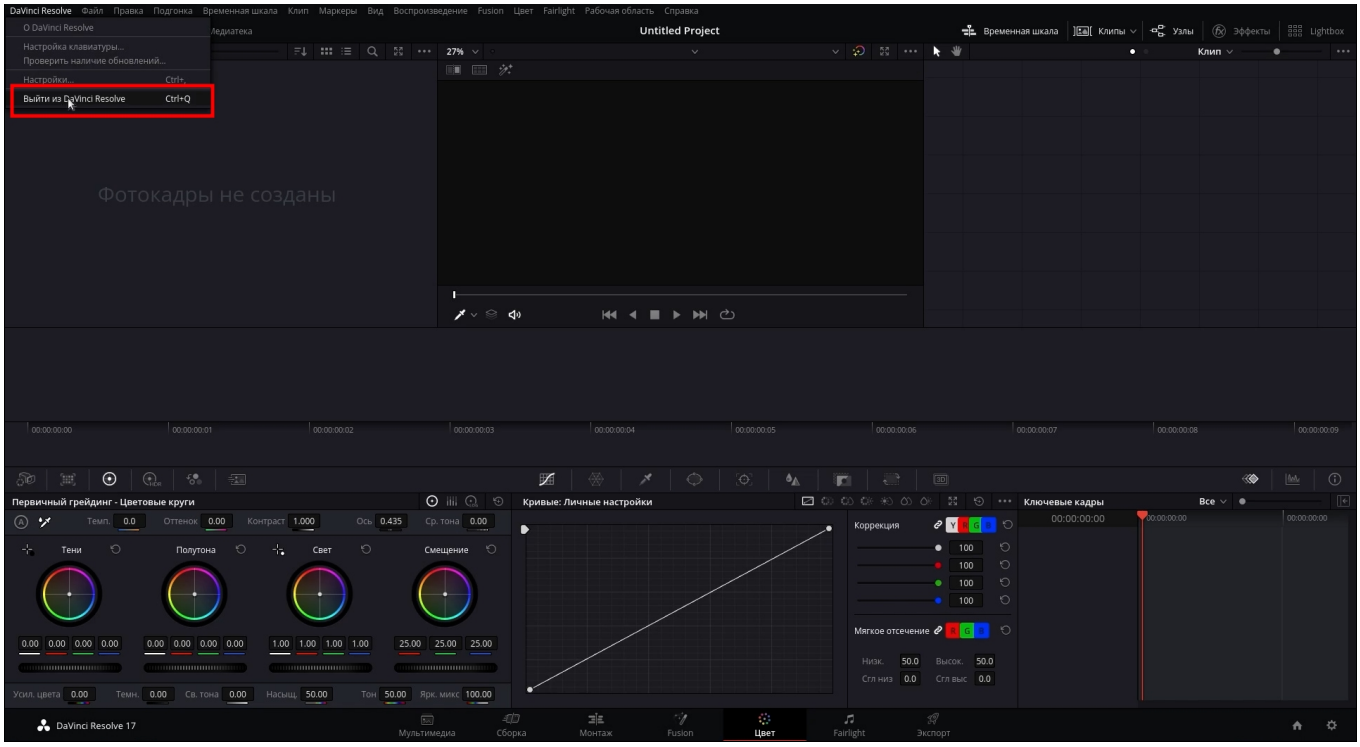
По завершении откроется главное окно видеоредактора **DaVinci Resolve**.



Интерфейс программы состоит из нескольких частей, переход между которыми можно осуществлять кнопками в нижней части экрана.



У приложения отсутствует рамка окна, поэтому для выхода необходимо выбрать пункт меню «**DaVinci Resolve**» - «**Выход из приложения**».



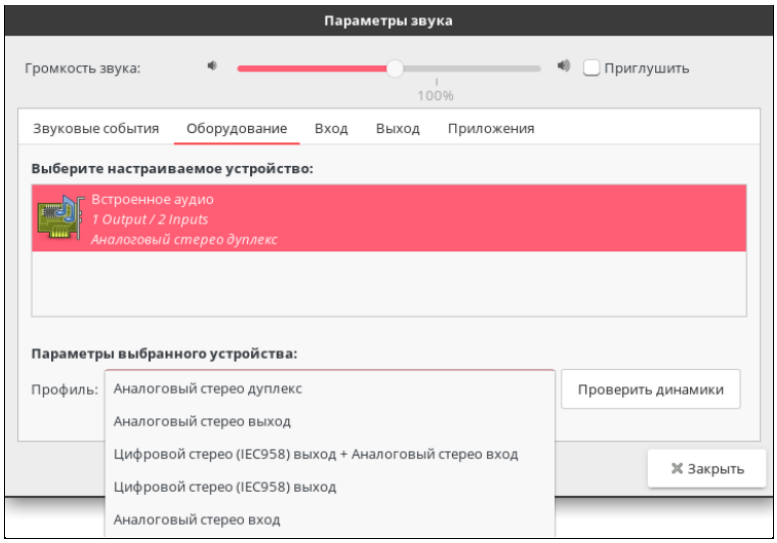
Решение проблем со звуком

Выбор оборудования
Отсутствует оборудование в списке доступных
Выбор оборудования через alsamixer
Проверка поддержки устройства ядром
Отсутствует звук у доменного пользователя

При возникновении проблем, связанных со звуком, существует несколько вариантов их решения.

Выбор оборудования

Бывают ситуации, когда необходимо вручную выбрать, какое именно устройство должно использоваться в ОС для ввода и вывода аудио-информации. Для этого выберите устройство в списке оборудования и установите для него необходимые параметры.

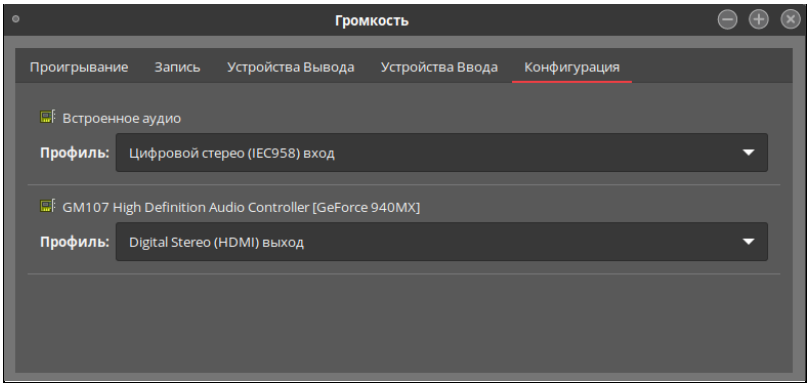


Отсутствует оборудование в списке доступных

Для решения данной проблемы на некоторых моделях ПК может подойти установка дополнительного пакета (потребуются права администратора):

```
dnf install alsa-sof-force
```

После установки необходимо перезагрузить ПК и проверить наличие аудиовыходов в параметрах звука.



Также не стоит забывать о системных обновлениях, соответственно, необходимо проверить работу оборудования на актуальных пакетах ОС. Для этого выполните следующие команды (потребуются права администратора):

```
dnf makecache
dnf update
dracut -f -v --regenerate-all
```

Затем для корректной загрузки необходимо обновить конфигурацию **GRUB**:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

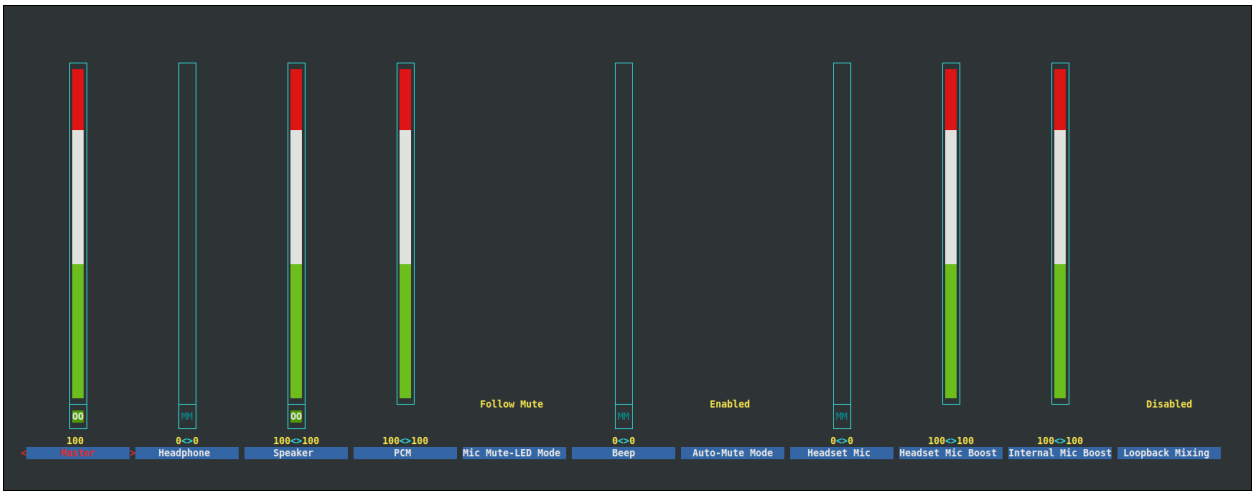
```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Для применения настроек потребуется перезагрузить ПК:

```
reboot
```

Выбор оборудования через alsamixer

В решении проблем со звуком также может помочь вариант с выбором звуковой карты из консоли через утилиту **alsamixer**.



С помощью клавиши **F6** можно выбрать необходимую звуковую карту.

Проверка поддержки устройства ядром

С выходом нового оборудования при возникновении проблем стоит обратить внимание на поддержку такого оборудования ядром. Проверить поддержку можно по нашей инструкции «Поддержка звука».

Отсутствует звук у доменного пользователя

Если звук отсутствует у доменного пользователя, в первую очередь необходимо проверить наличие файла **/var/lib/AccountsService/users/<доменный_пользователь>**. Если файл отсутствует, его необходимо создать по примеру файла локального пользователя.

Также попробуйте добавить пользователя в группу *audio*:

```
usermod -aG audio <доменный_пользователь>@<домен>
```

Если предложенные рекомендации не помогли с решением проблемы, необходимо собрать диагностическую информацию с помощью утилиты loginfo для дальнейшего ее изучения.

Почтовый клиент Evolution

Установка Evolution
Основные функции

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: evolution-3.50.2

Evolution – свободно распространяемая программа для работы с электронной почтой, управления адресной книгой и функцией планировщика задач. Входит в состав среды рабочего стола **GNOME** в качестве поставляемой по умолчанию почтовой программы.

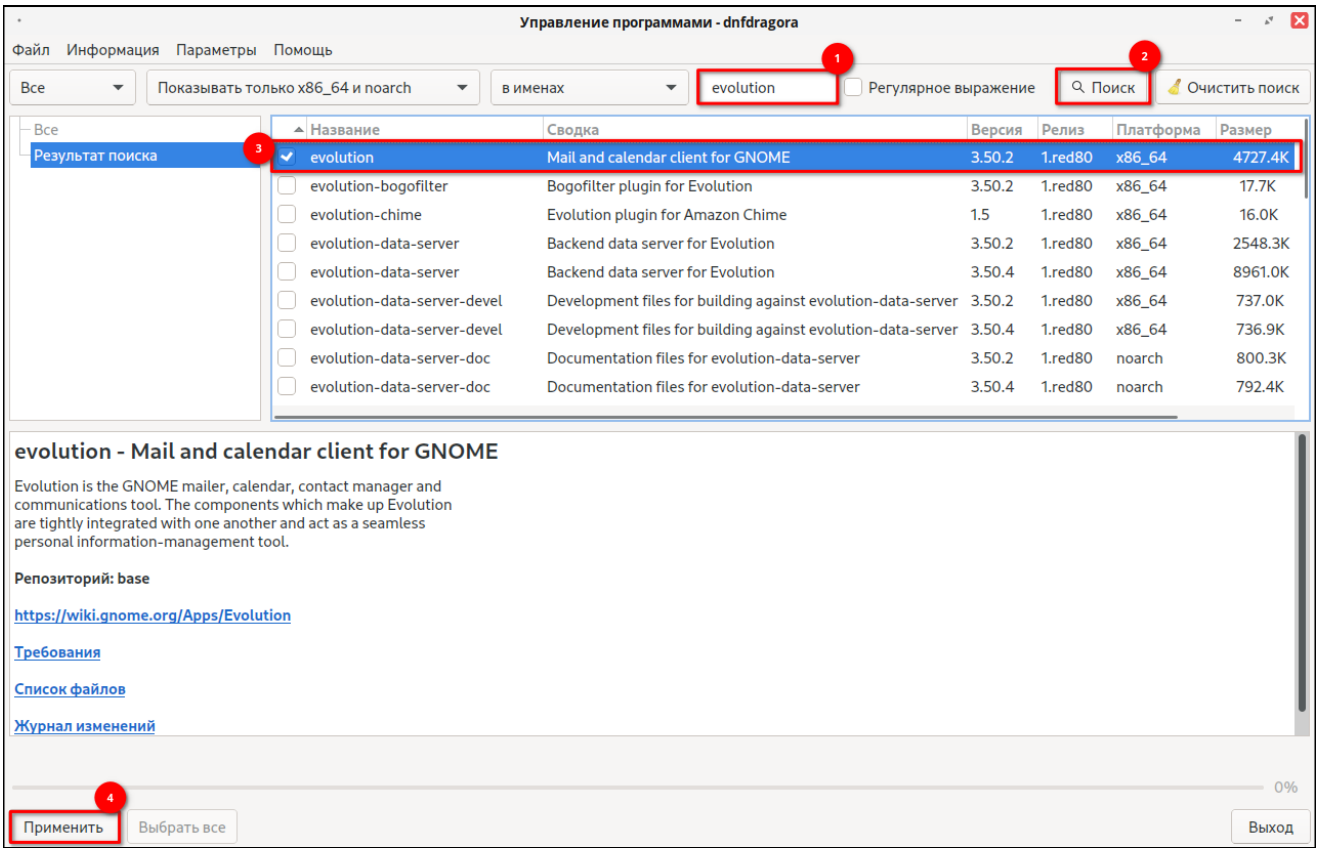
Evolution поддерживает следующие функции и протоколы:

- получение электронной почты по протоколам **POP3** и **IMAP** и её отправка по **SMTP**;
- поддержка расширений протокола **IMAP4** для быстрого обновления содержимого папок **Quick Resync** и уведомлений со стороны сервера **IMAP IDLE**;
- поддержка локальной почты на **UNIX**-системах;
- поддержка защищённых протоколов связи **SSL**, **TLS** и **STARTTLS**;
- шифрование переписки при помощи **GPG** и **S/MIME**;
- использование библиотеки **NSS** для управления сертификатами, что позволяет использовать общее хранилище между совместимыми программами, например, **Mozilla Firefox**, **Mozilla Thunderbird**, **LibreOffice** и пр;
- поиск по почтовым папкам и сортировка почты по критериям;
- автоматическая фильтрация спама с использованием **SpamAssassin** и **Bogofilter**;
- возможность работы с серверами **Microsoft Exchange Server**, **Novell GroupWise** и **Kolab**;
- календарь с поддержкой формата файлов **iCalendar** и протоколов **WebDAV**, **CalDAV** и возможностью подключения к **Google Calendar**;
- адресная книга с поддержкой локальных контактов, протоколов **CardDAV**, **LDAP** и контактов **Google**;
- интеграция адресной книги с **LibreOffice**;
- поддержка аватаров пользователей из адресной книги, из заголовков **X-Face**, **Face** и автоматический поиск их по хешу адреса электронной почты на сервисе **Gravatar**;
- поддержка расширений для чтения лент новостей **RSS**, синхронизации с мобильными устройствами и **VoIP** приложением **Ekiga**;
- импорт почты из архивов **Microsoft Outlook** (файлы с расширениями **.dbx**, **.pst**) и **Berkley Mailbox**.

Установка Evolution

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Evolution** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**evolution**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

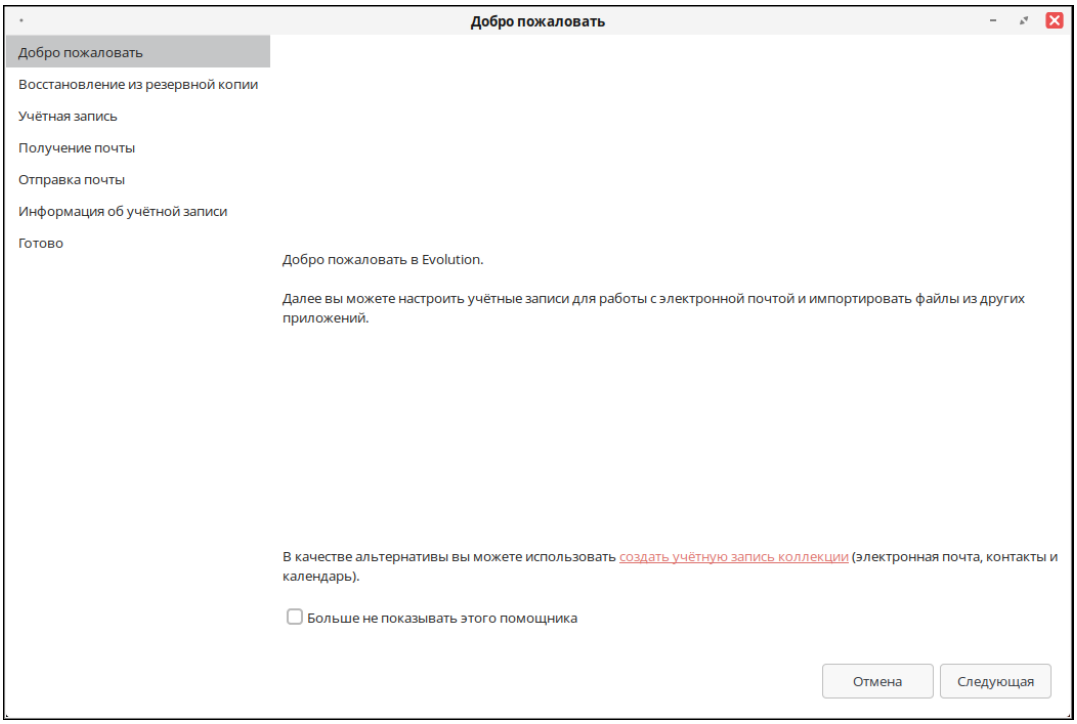
```
dnf install evolution
```

После установки **Evolution** будет доступен из «**Главного меню**» – «**Офис**» – «**Evolution**».

При первом запуске почтового клиента будет выведено окно с настройкой основных функций для работы программы. Здесь вы можете создать новую учетную запись или импортировать файлы из уже существующей, задать параметры почтового сервера, настроить параметры получения и отправки почты.

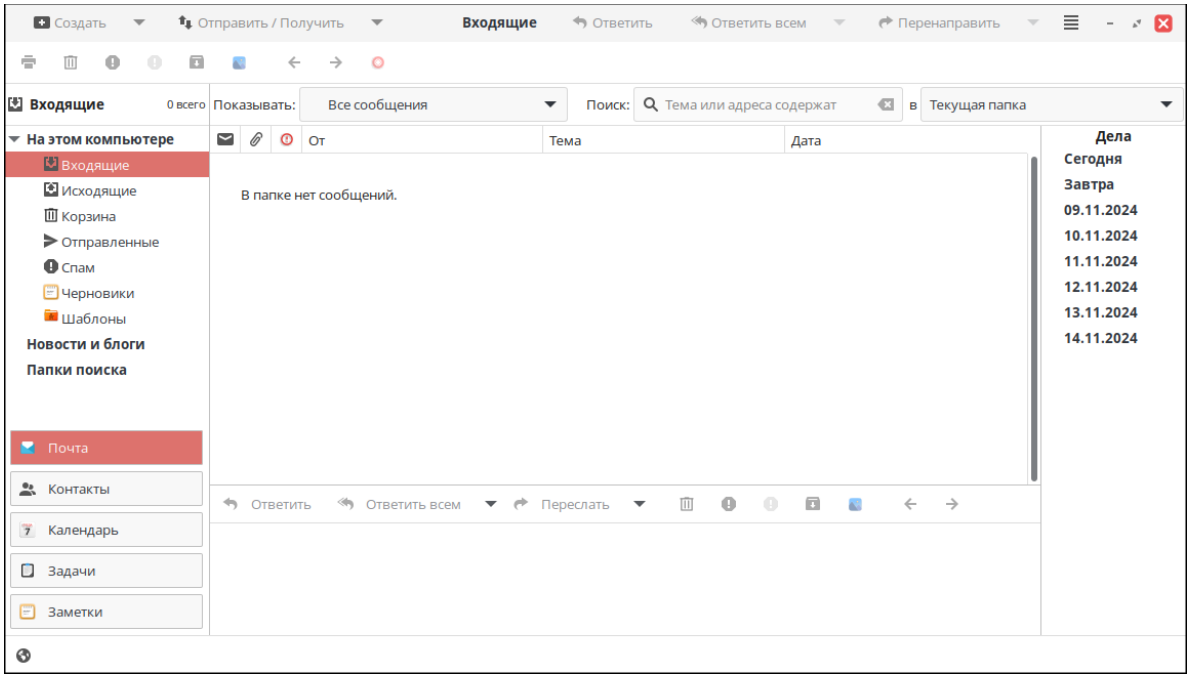
На шаге «**Информация об учетной записи**» необходимо проверить правильность введенных данных и указанных параметров почтового сервера. Если все настроено верно, перейдите к шагу «**Готово**» и начните пользоваться почтовым клиентом.

В противном случае нажмите «**Назад**» и внесите необходимые изменения в настройки клиента.

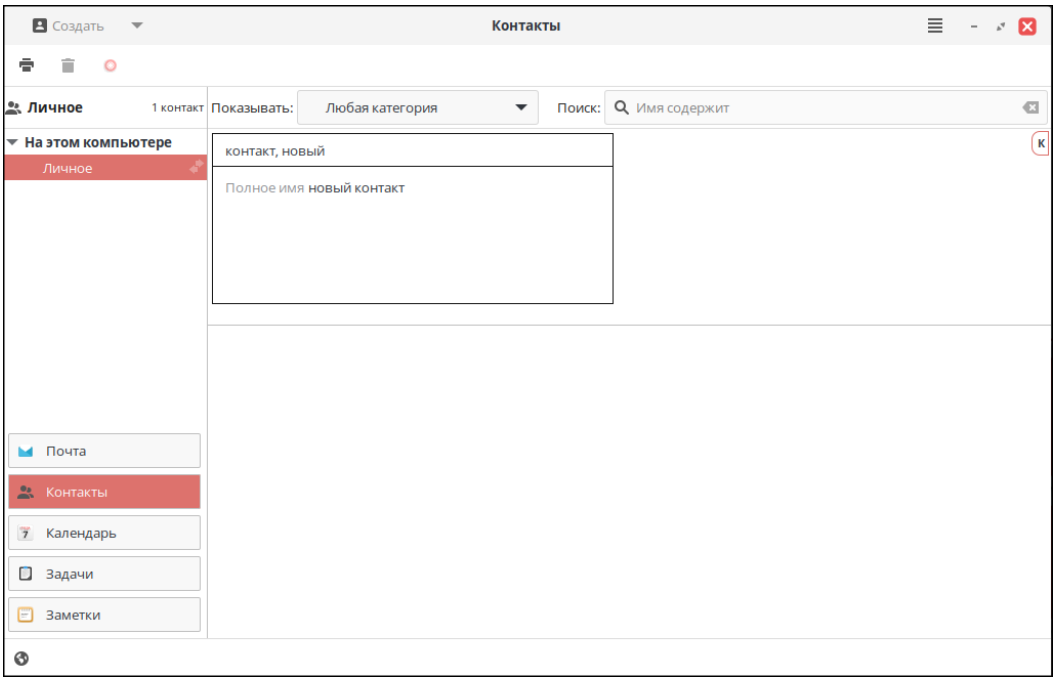


Основные функции

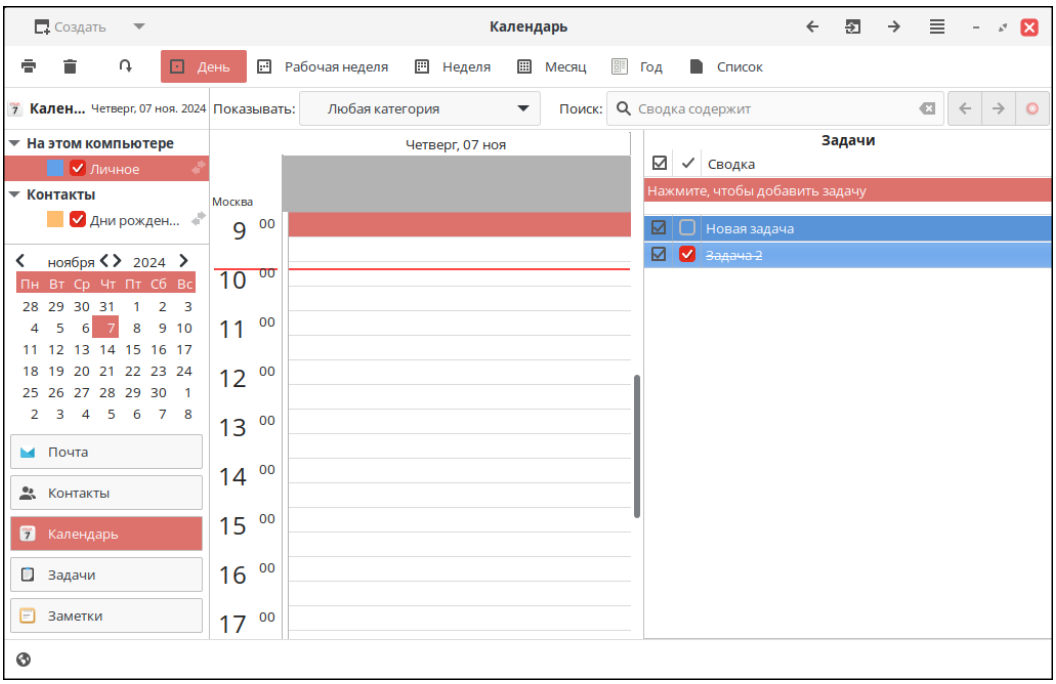
В **Evolution** реализованы стандартные функции почтового клиента – работа непосредственно с электронный почтой.



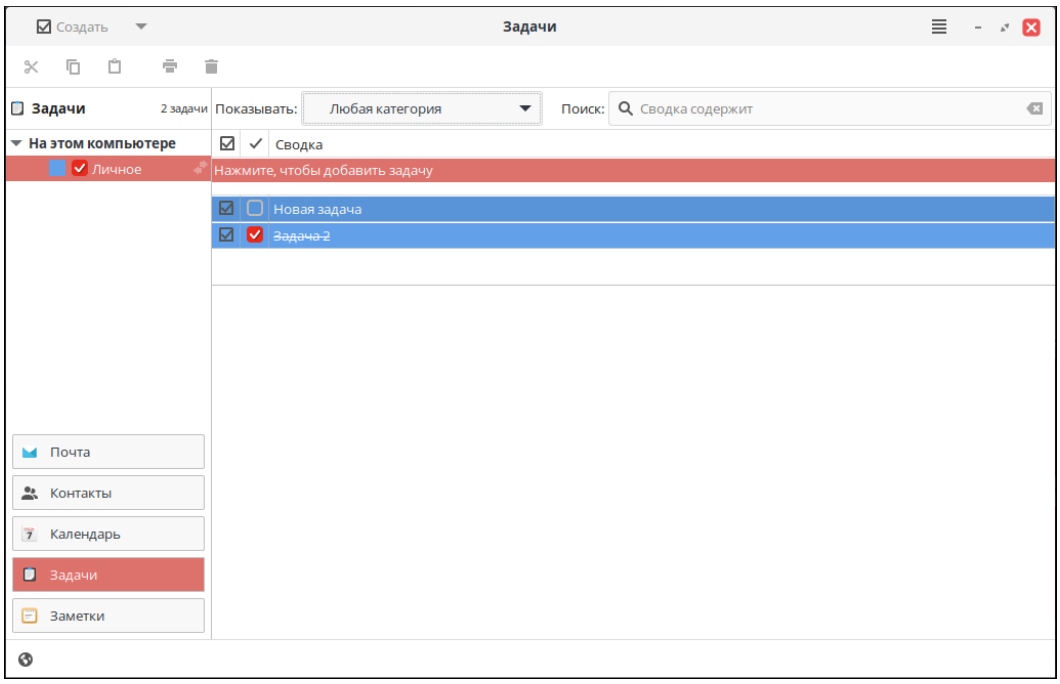
Отдельная вкладка для работы с контактами – добавьте новые контакты.



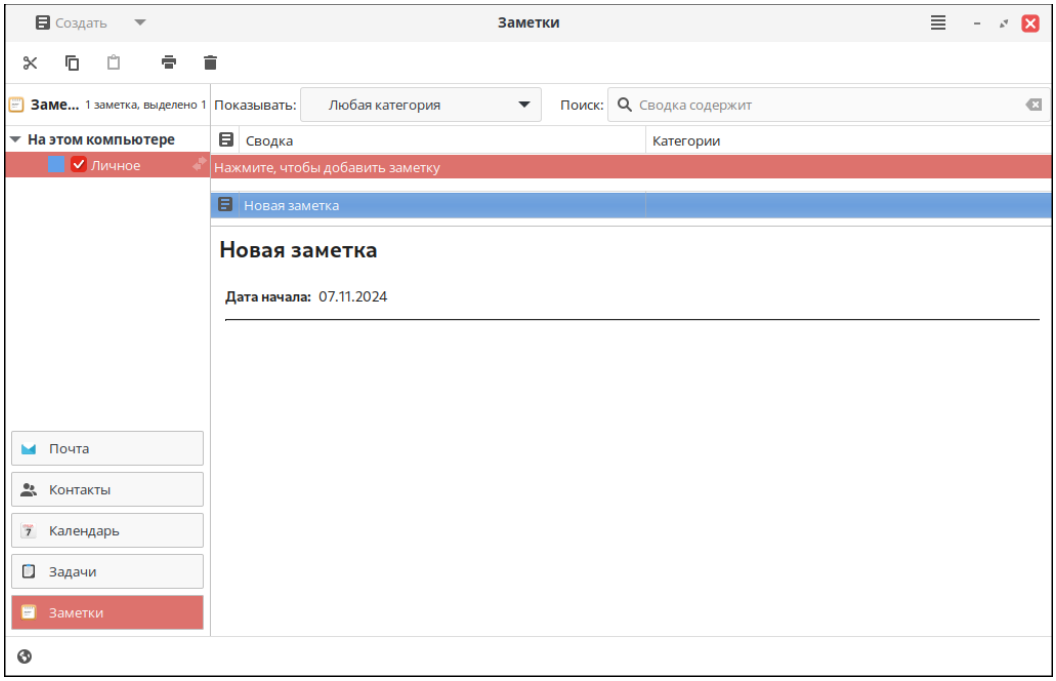
Календарь, в котором можно добавлять мероприятия на определенный день, настраивать оповещение о предстоящем мероприятии или событии.



Вкладка «**Задачи**» – возможность создавать задачи, устанавливать сроки их выполнения, приоритет и текущее состояние.



Также доступно ведение заметок.



Почтовый клиент Thunderbird

Установка

Основные возможности программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: thunderbird-102.15.0-1

Mozilla Thunderbird — это бесплатное приложение для работы с электронной почтой, разработанное командой *Mozilla Foundation*. Это один из самых популярных почтовых клиентов, который предоставляет широкие возможности для организации и управления электронной почтой.

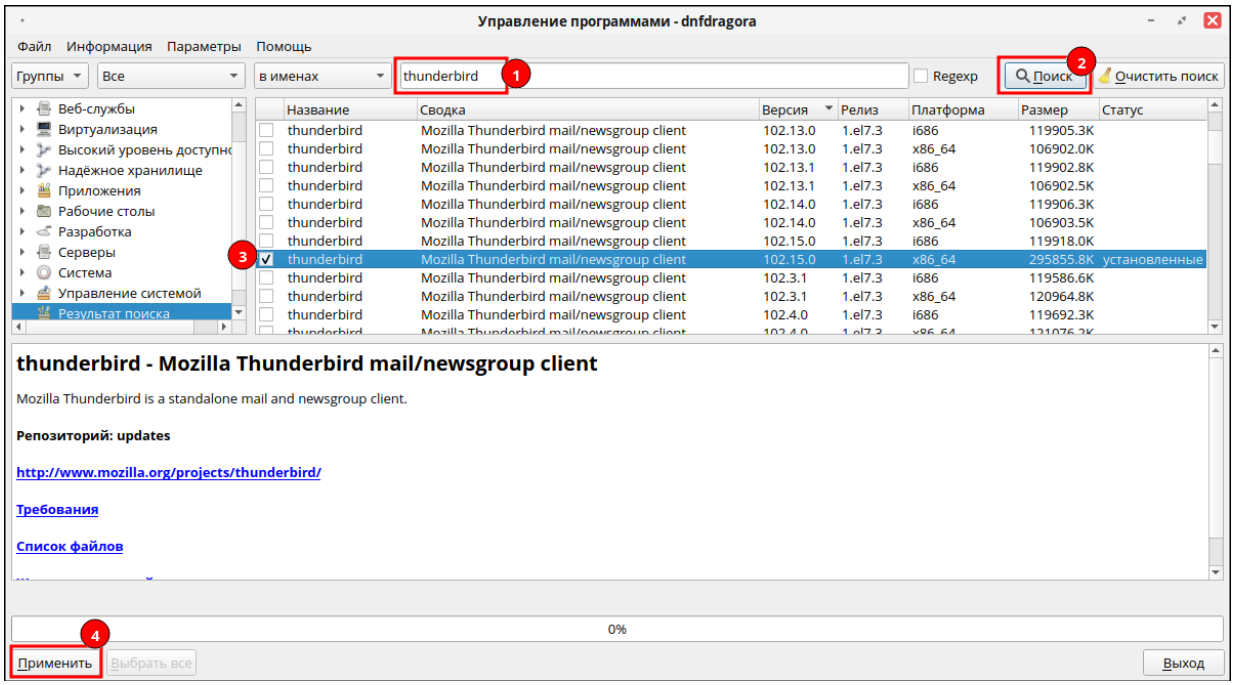
Thunderbird позволяет гибко настраивать учетную запись электронной почты, устанавливать и настраивать различные фильтры и правила, создавать папки для организации писем, устанавливать шаблоны и многое другое. Все письма и контакты хранятся локально на компьютере, обеспечивая безопасность и конфиденциальность данных.

Поддерживаются популярные почтовые протоколы, включая **POP3**, **IMAP** и **SMTP**. Есть возможность подключать почтовые ящики от разных провайдеров с автоматическим обнаружением настроек и управлять ими из одного интерфейса.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Thunderbird** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**thunderbird**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

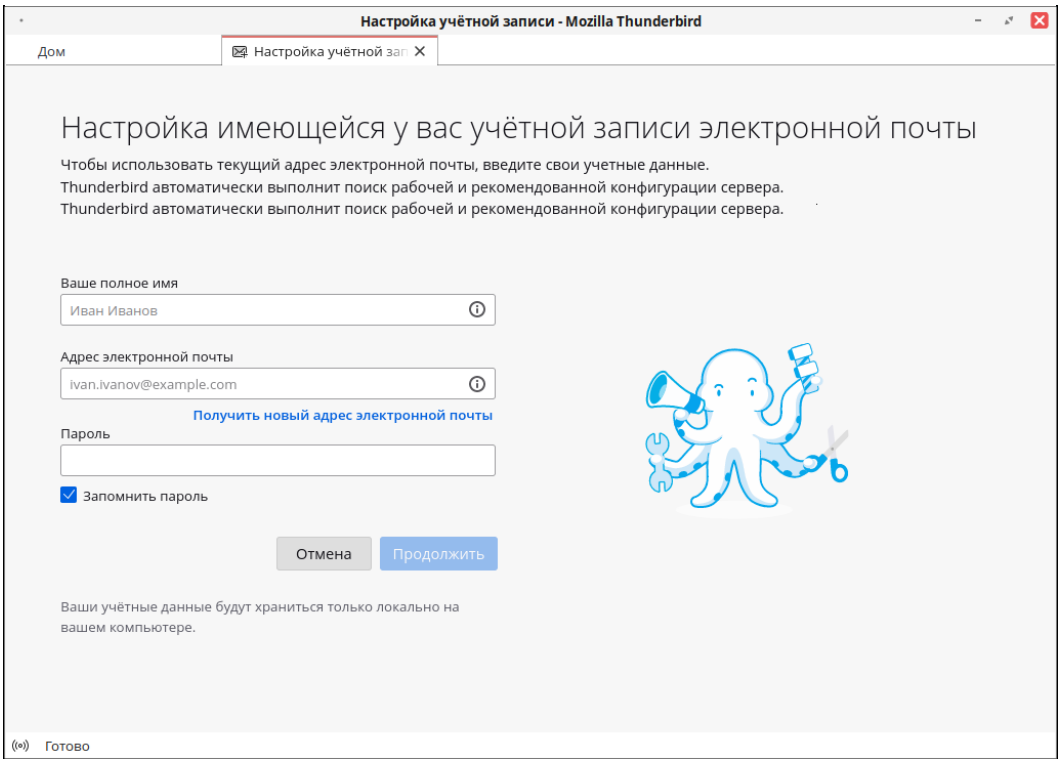
```
su -
```

и выполните команду:

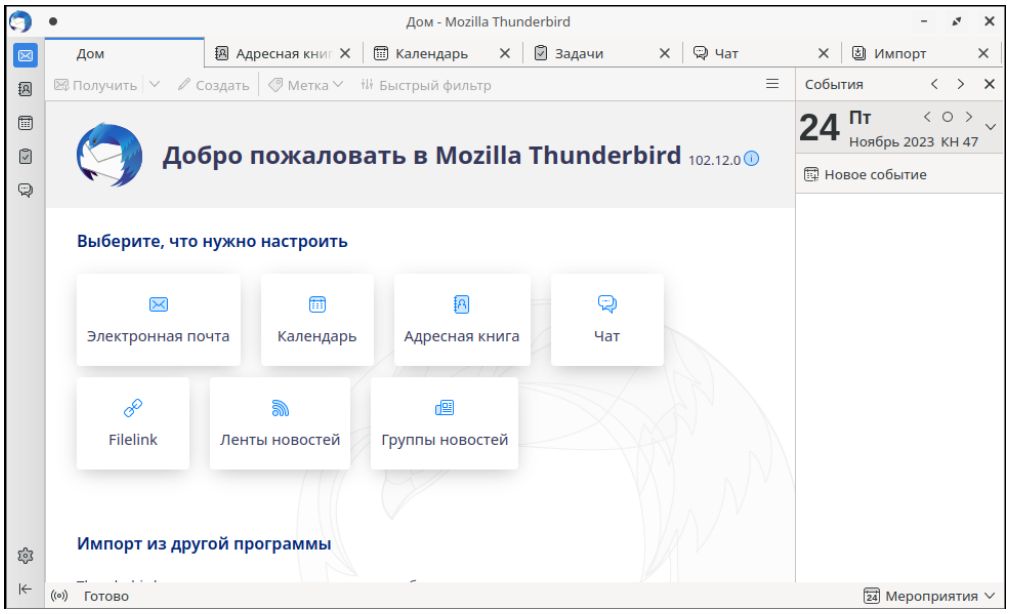
```
dnf install thunderbird
```

После установки **Thunderbird** будет доступен из «**Главного меню**» — «**Интернет**» — «**Почтовый клиент Thunderbird**».

При первом запуске почтового клиента будет предложено ввести данные существующей учетной записи для автоматического определения настроек сервера.

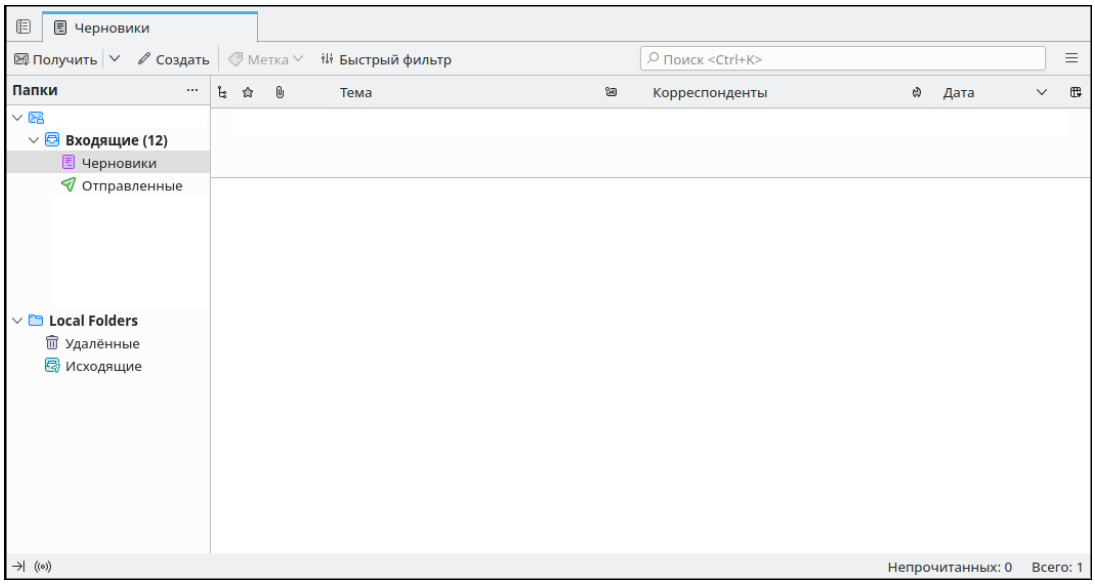


После входа в учетную запись будет открыта домашняя страница почтового клиента, где можно выбрать, что нужно настроить.



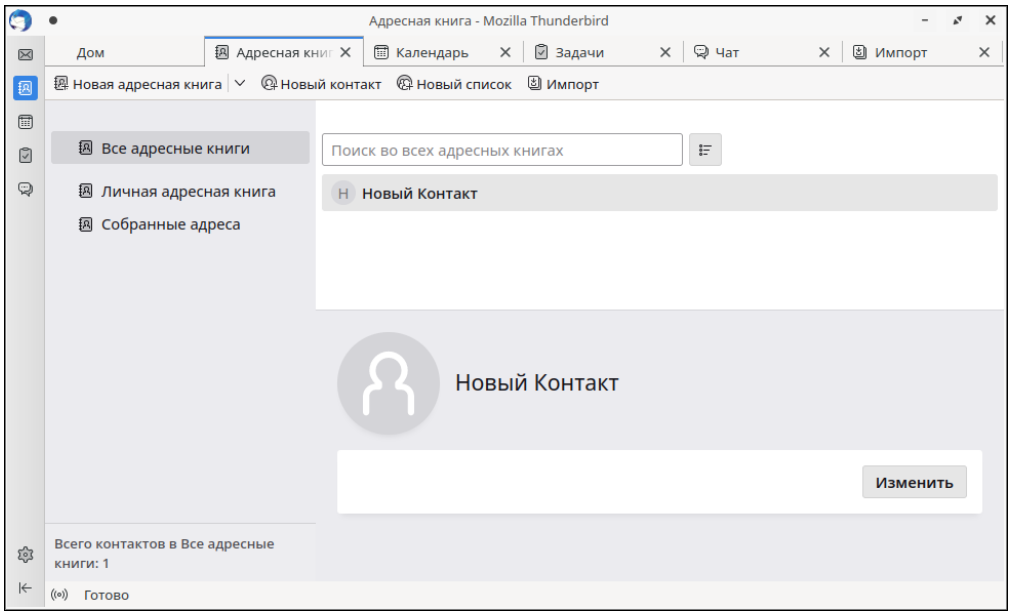
Основные возможности программы

Thunderbird имеет стандартный набор функций почтового клиента, основная из которых — работа с электронной почтой. Thunderbird умеет сохранять письма и вложения локально на компьютере, что обеспечивает доступ к ним даже без интернета. Кроме того, встроенный поиск позволяет быстро находить нужные сообщения.

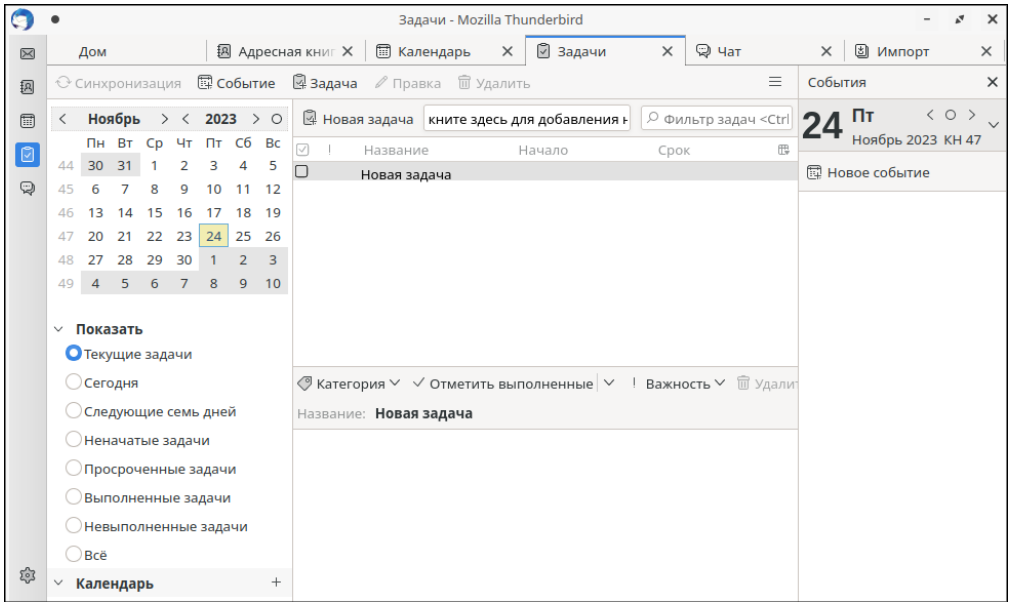


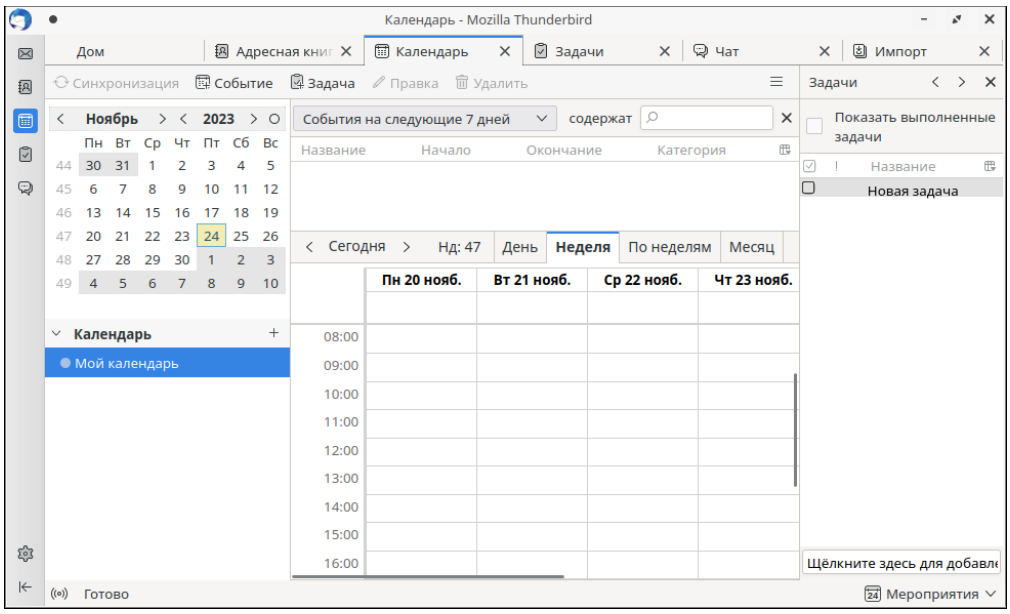
Thunderbird включает встроенные инструменты для борьбы со спамом и обнаружения вредоносных программ. Он также поддерживает шифрование и аутентификацию, чтобы обеспечить безопасность электронных писем.

Также доступна возможность работы с адресной книгой.

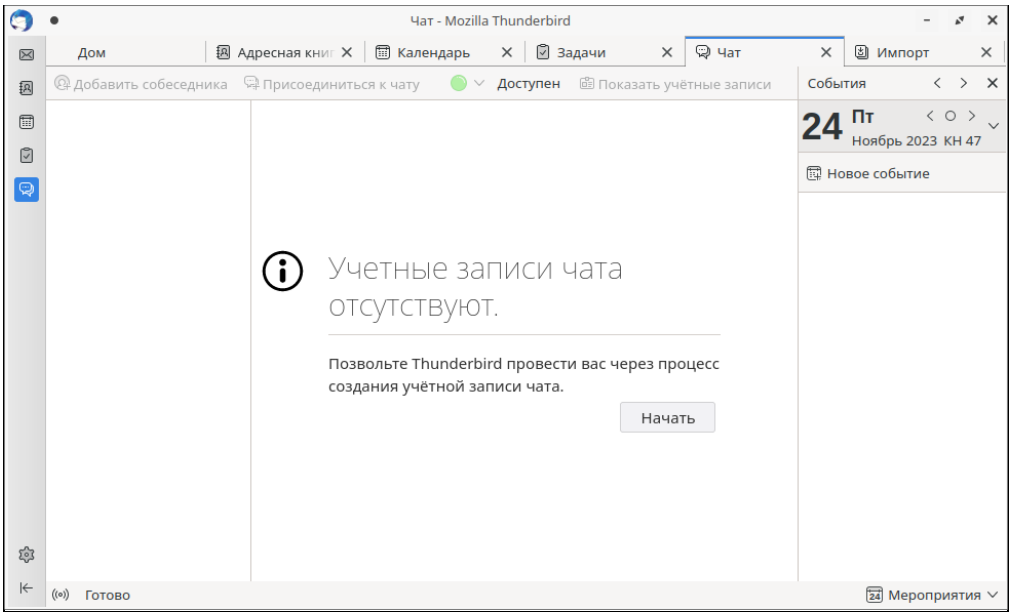


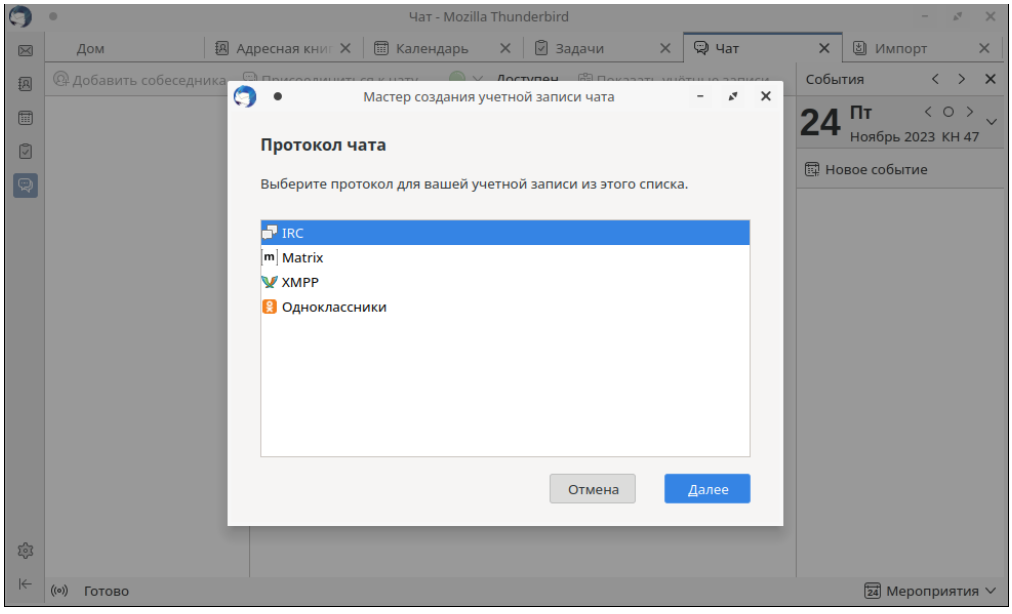
Присутствуют функции календаря, совмещенного с задачами, что позволяет управлять своим временем и не пропускать важные события.





Имеется возможность подключения учетной записи для чата, для выбора доступны такие протоколы, как **IRC**, **Matrix**, **XMPP**, **Одноклассники**.

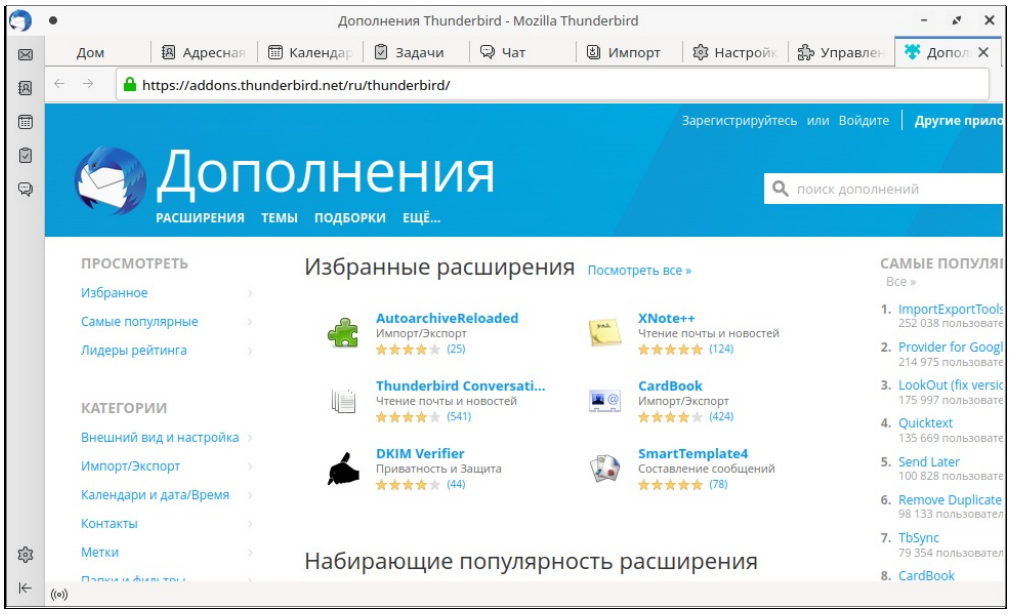




Thunderbird поддерживает подписку на новостные рассылки и чтение **RSS**-каналов, позволяя получать свежие новости и информацию из интересующих источников.

Главным достоинством **Thunderbird** можно назвать возможность установки различных дополнений, тем оформления, расширений. Это

позволяет гибко настраивать внешний вид почтового клиента под свой вкус, а также расширять функционал и возможности программы.



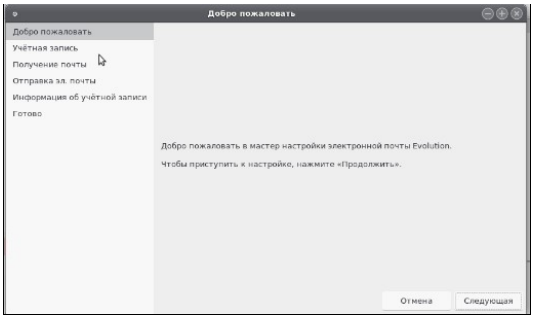
Настройка в Evolution подключения к MS Exchange

У вас должен быть установлен плагин для работы **EWS**. Установить его можно командой:

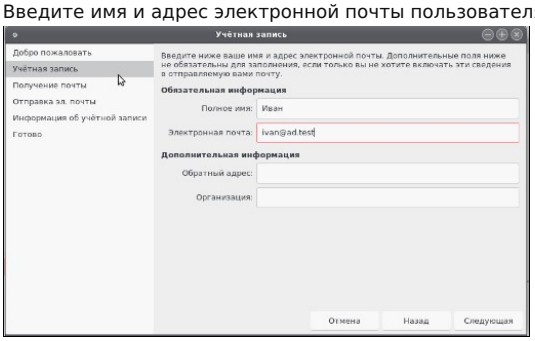
```
dnf install evolution-ews
```

Перейдите в меню «Файл > Создать > Учетная запись почты».

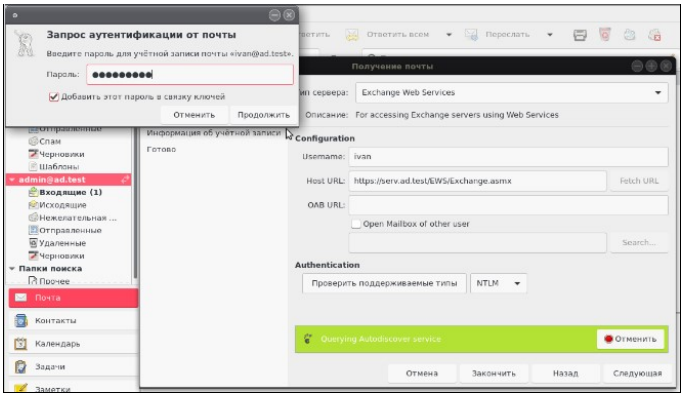
Откроется окно. Нажмите кнопку «Следующая».



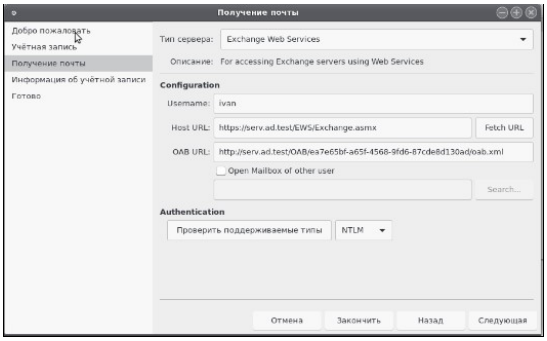
Введите имя и адрес электронной почты пользователя и нажмите кнопку «Следующая».



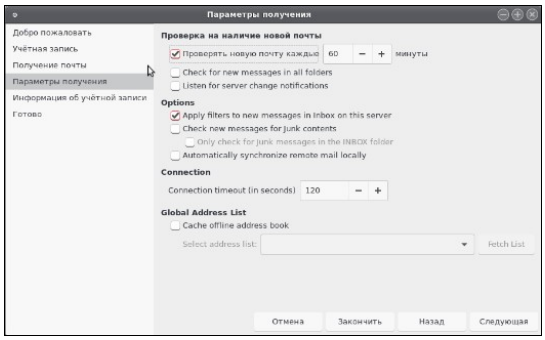
Выберете тип сервера Exchange Web Services. Введите правильный адрес к EWS и нажмите кнопку «Fetch URL».
Если все сделано правильно, откроется окно ввода пароля пользователя. Введите пароль и нажмите кнопку «Продолжить».



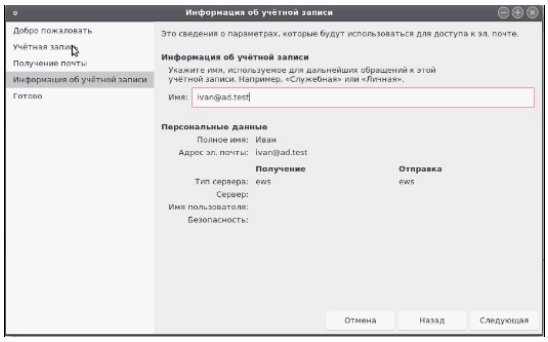
Если пароль введен верно, сервер вернет OAB URL, он отобразится в соответствующем окне. Нажмите кнопку «Следующая».



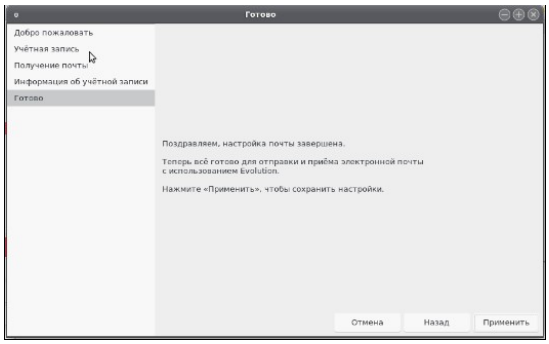
В следующем окне настройте параметры получения или оставьте их по умолчанию. Нажмите кнопку «Следующая».



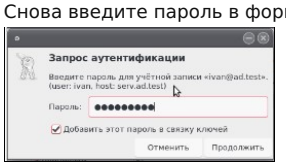
Укажите имя учетной записи для обращений или оставьте значение по умолчанию. Нажмите кнопку «Следующая».



Нажмите кнопку «Применить».



Снова введите пароль в форме ввода пароля.



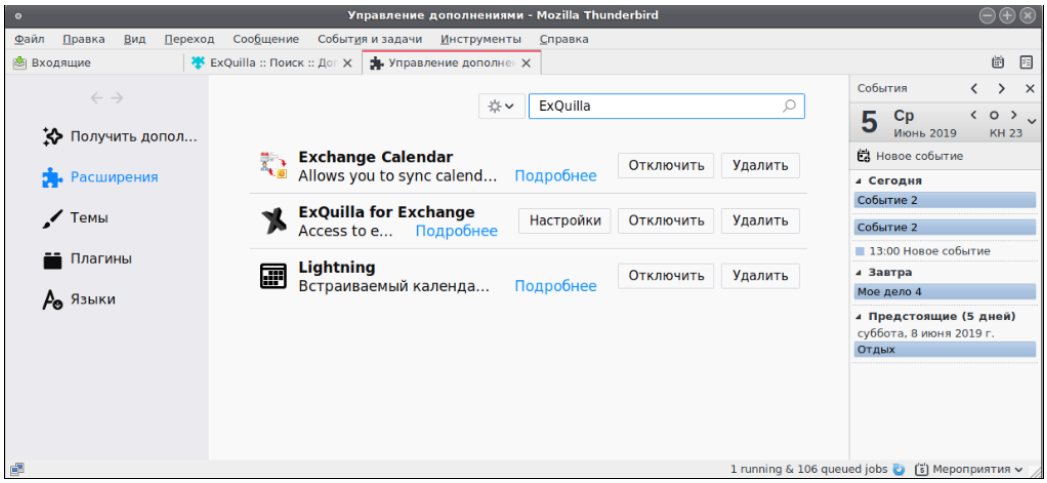
На этом почта подключена. Также автоматически подключен календарь, задачи, заметки. Есть возможность просмотра адресных книг.

Настройка календаря Exchange в Thunderbird

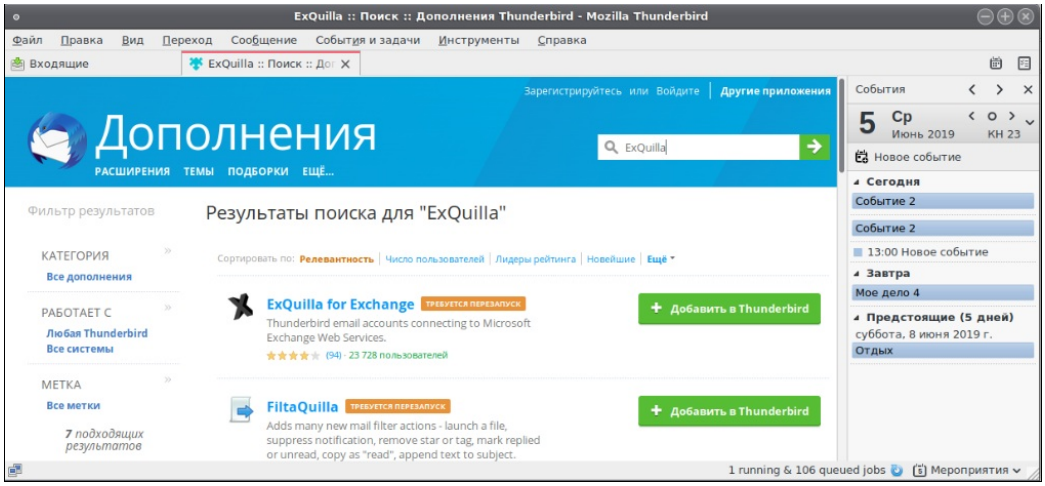
Настройка почты

Для подключения почты Exchange к Thunderbird скачайте и установите плагин ExQuilla for Exchange.

Для этого в меню нажмите Инструменты > Дополнения. В открывшемся окне выберите Расширения и в верхнем правом углу в строку поиска введите "ExQuilla".



В списке найденного нажмите кнопку "Добавить в Thunderbird" напротив плагина ExQuilla for Exchange. После установки перезагрузите почтовый клиент.

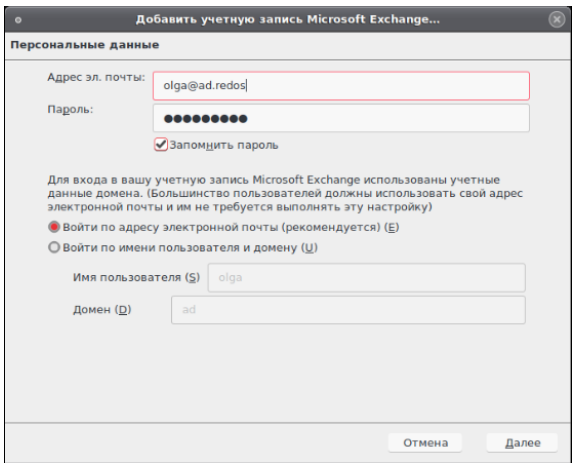


ВАЖНО

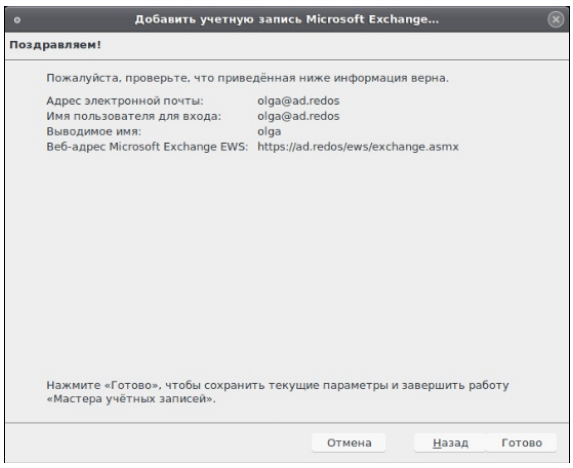
У вас должен быть установлен плагин Lighting

Далее подключите календарь. Выберите меню "Файл" > "Создать" > "Добавить учетную запись Microsoft Exchange".

В открывшемся окне введите адрес эл. почты, пароль и нажмите кнопку "Далее"

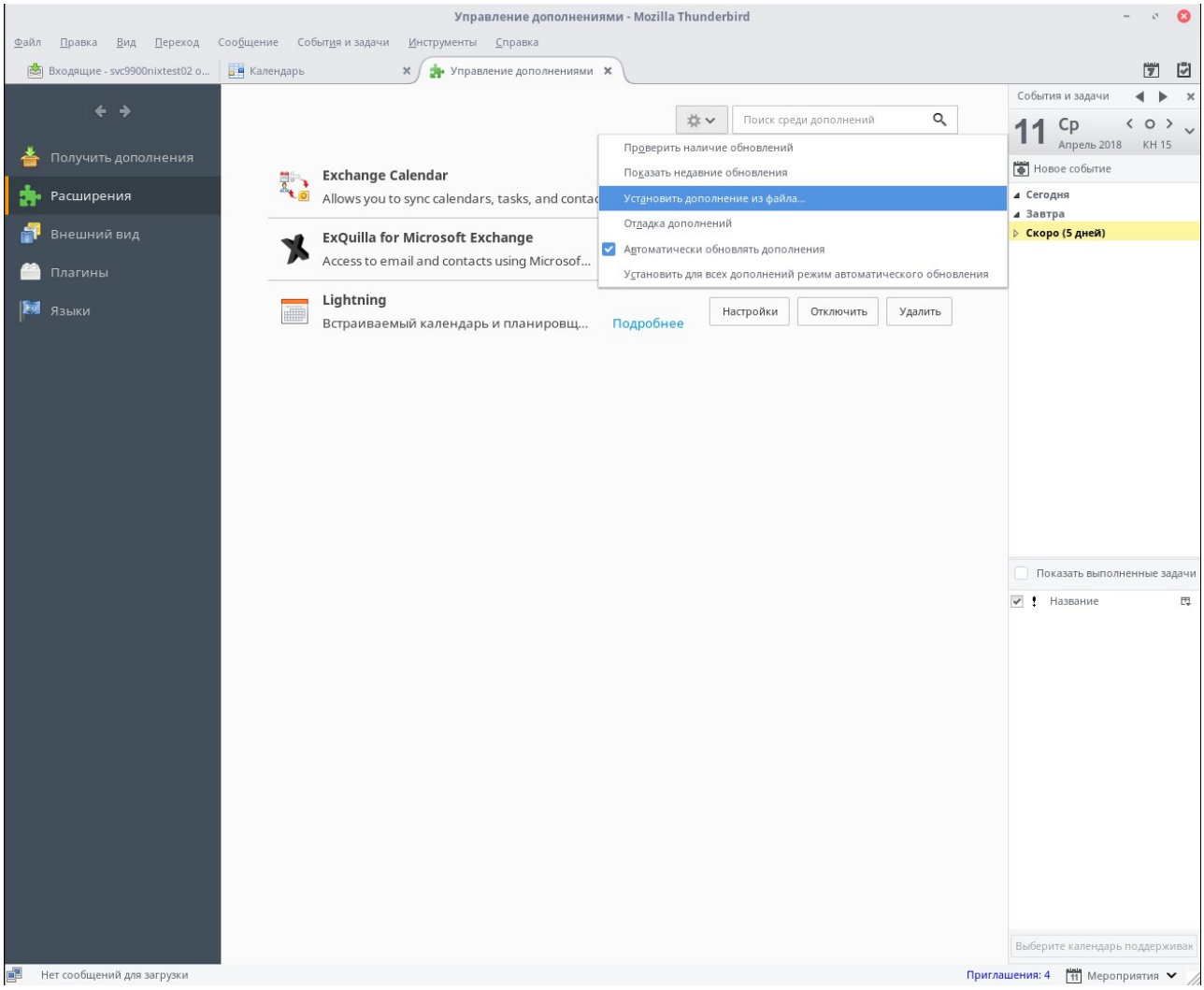


Должен автоматически определится адрес почтового сервера и появиться окно с успешным подключением. Остается только нажать кнопку "Готово".



Настройка календаря

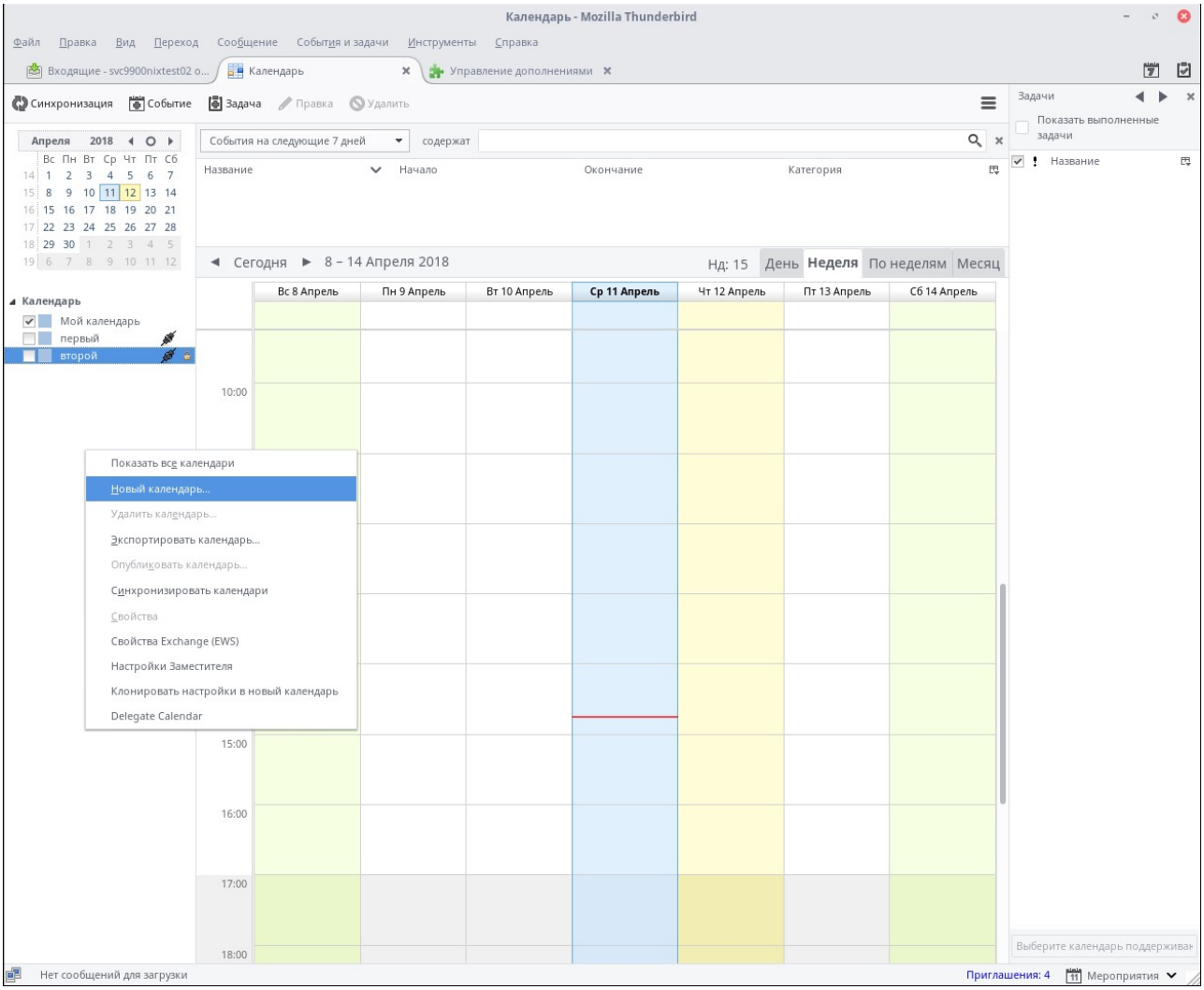
1. Скачайте дополнение ExchangeCalendar по ссылке:
https://github.com/ExchangeCalendar/exchangecalendar/releases
Откройте Thunderbird перейдите в меню и выберите пункт “Дополнения”.
Перейдите на вкладку “Расширения” и нажмите на шестеренку, затем выберите пункт “Установить дополнение из файла”.



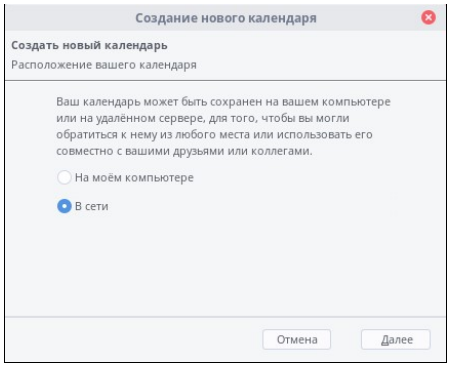
Выберите скачанный файл дополнения и нажмите “Ок”. Затем установите его и перезагрузите почтовый клиент.

2. Добавьте календарь.

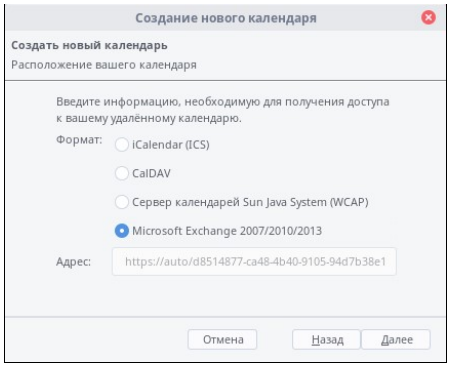
Откройте Thunderbird перейдите на вкладку “Календарь”.
В списке календарей нажмите на правую кнопку мыши и выберете “Новый календарь”.



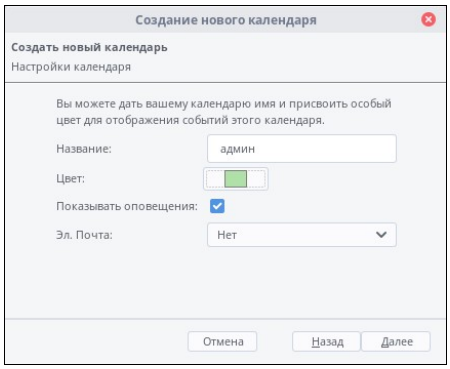
В открывшемся окне выберете “В сети” и нажмите кнопку “Далее”.



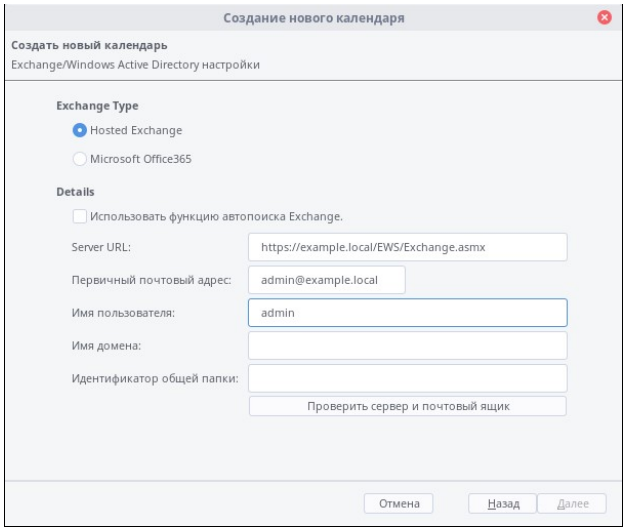
Выберите пункт “Microsoft Exchange 2007/2010/2013” и нажмите кнопку “Далее”.



Введите название календаря, выберите цвет, при выборе электронной почты укажите её или выберите “Нет” и нажмите кнопку “Далее”.



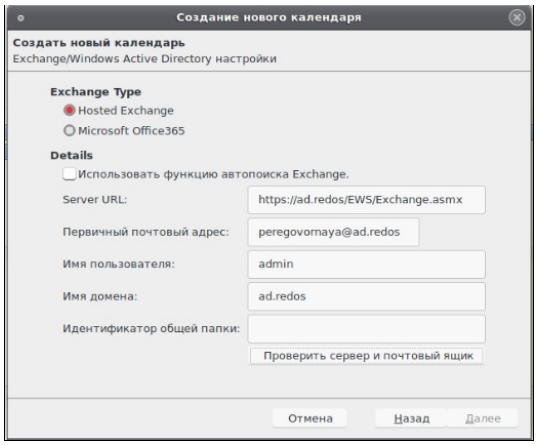
Выберите “Hosted Exchange”, введите Server URL. Обычно, адрес следующий https://<имя почтового сервера>/EWS/Exchange.asmx. Введите первичный почтовый адрес и имя пользователя, затем нажмите кнопку “Проверить сервер и аккаунт”.



В открывшемся окне введите пароль от аккаунта. Окно может появляться несколько раз.
Теперь нажмите кнопку “Далее” и “Готово”.
Календарь подключен.

Подключение общего календаря помещений или оборудования

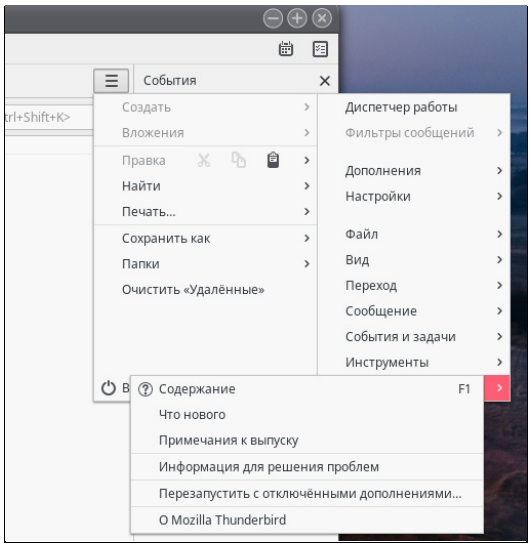
Для подключения любого общего календаря нужно при его подключении вписать в поле "Первичный почтовый адрес" адрес этого календаря. Пример на скриншоте ниже.

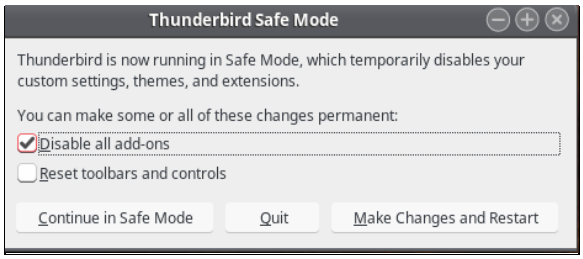


Thunderbird запуск Google-почты

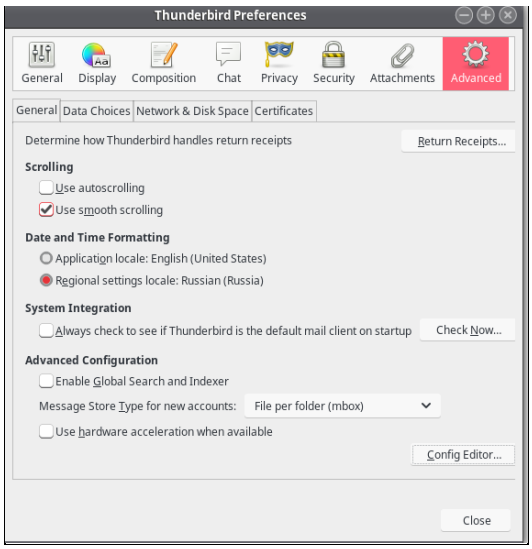
Настройка добавления Google аккаунта в ThunderBird при возникновении проблемы при авторизации с использованием OAuth2:

Включите Безопасный Режим Thunderbird для этого зайдите в Справку-> Перезапустить с отключенными дополнениями -> Disable all add-ons -> Continue in safe mode



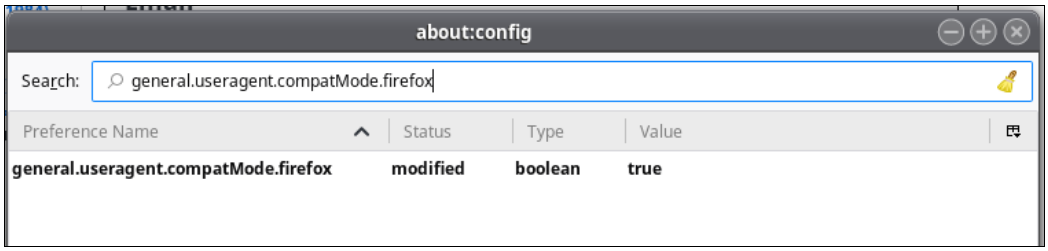


После запуска в безопасном режиме откройте Thunderbird Preferences -> Advanced -> General -> Config Editor -> согласитесь с уведомлением, откроется список доступных конфигураций



Воспользуйтесь поиском **general.useragent.compatMode.firefox** и измените значение на true.

Если параметр отсутствует, добавьте его с меткой boolean, значение true.



Выйдите из безопасного режима и попробуйте ввести данные Google аккаунта.

Firefox

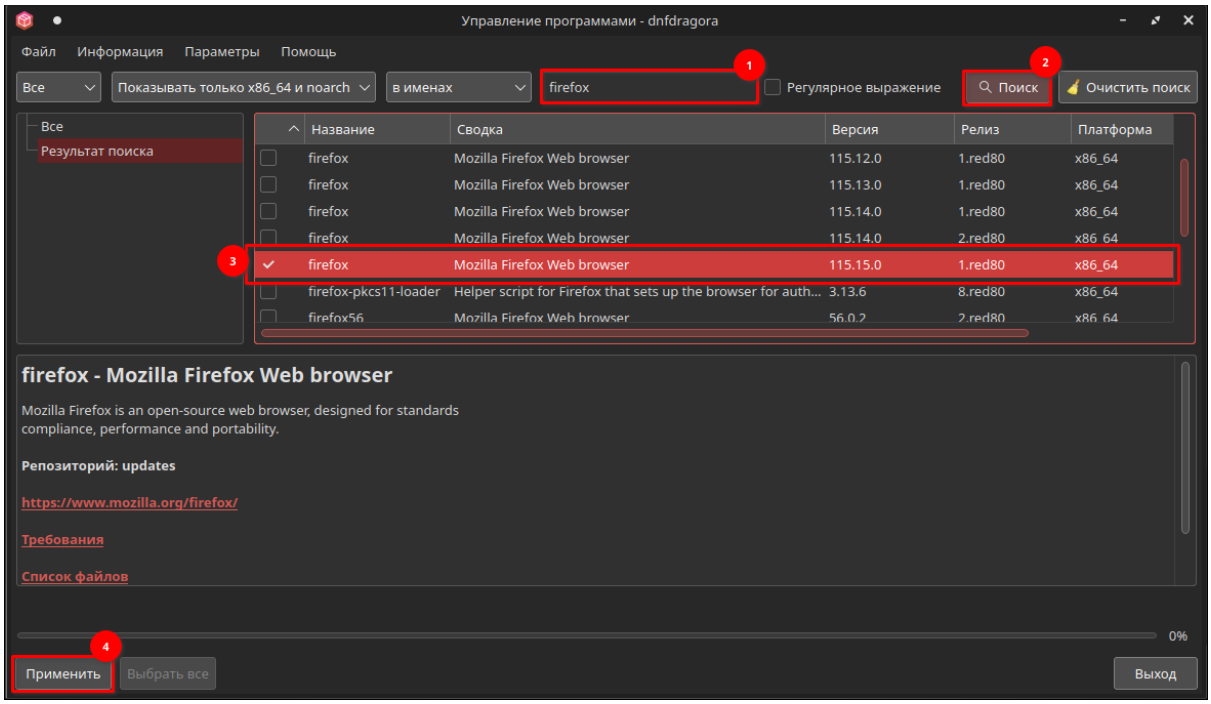
Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: firefox-115.15.0-1

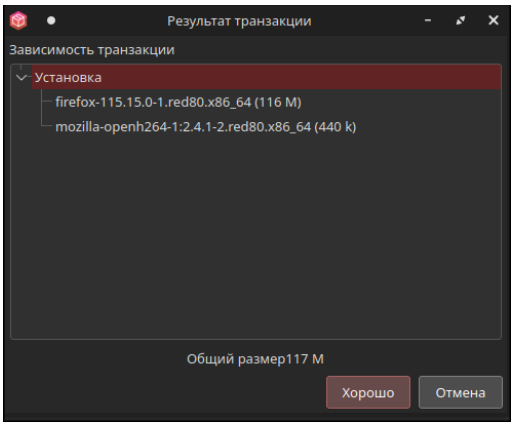
Firefox — свободный интернет-браузер, созданный компанией **Mozilla Corporation** на основе движка **Quantum**.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**firefox**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Согласитесь с установкой зависимых пакетов, нажав кнопку «**Хорошо**».



Установка займет некоторое время, после успешной установки окно с транзакцией исчезнет. Сам пакет будет отмечен как установленный.

Для установки браузера через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install firefox
```

Работа в программе выполняется от локального пользователя.

После установки браузер будет доступен из «**Главного меню**» — «**Интернет**» — «**Firefox**».

Яндекс.Браузер

Установка через «Окно настройки РЕД ОС»
Установка через терминал
Установка через dnfdragora
Решение проблем

Окружение

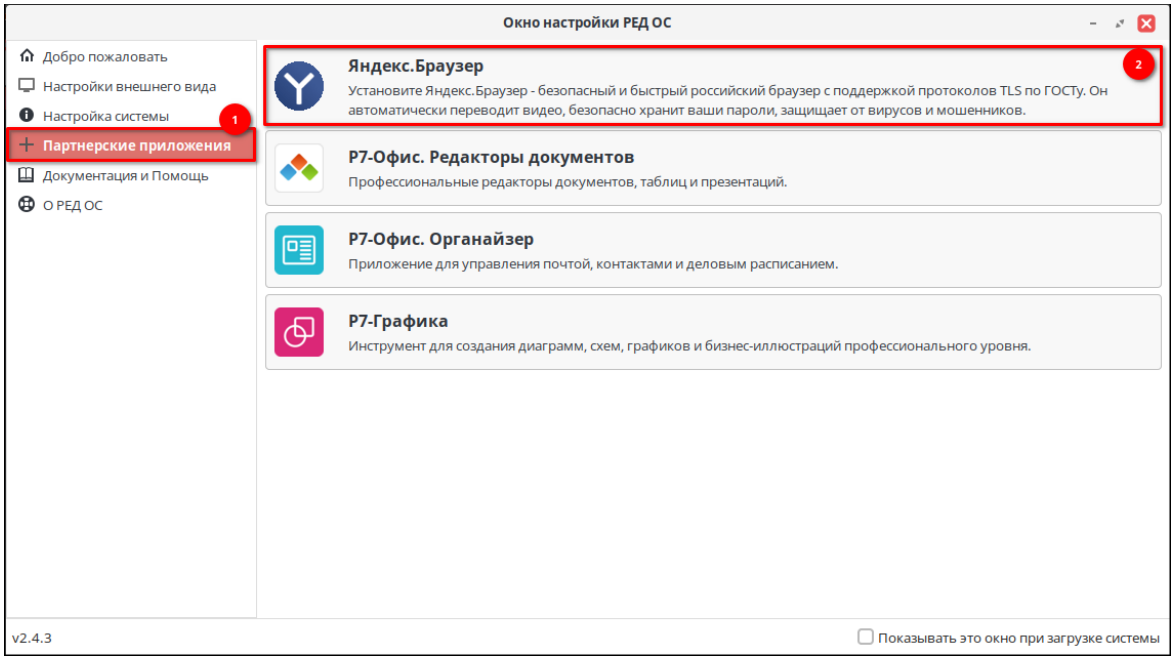
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** yandex-browser-release-2.0-2, yandex-browser-stable-24.7.1.1202-1

Яндекс.Браузер для РЕД ОС размещается в отдельном подключаемом (с помощью пакета **yandex-browser-release**) репозитории. **Яндекс.Браузер** в данном репозитории был собран специально для работы в РЕД ОС и использует зависимости и кодеки из репозитория РЕД ОС. Репозиторий подключен **во всех** поддерживаемых версиях и редакциях РЕД ОС.

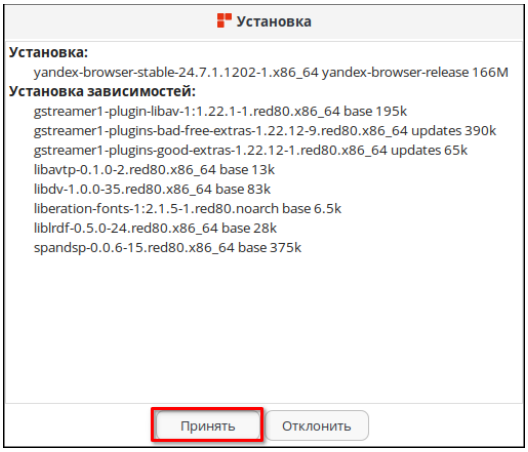
Установка через «Окно настройки РЕД ОС»

Откройте утилиту «Окно настройки РЕД ОС».

Перейдите на вкладку «**Партнерские приложения**», затем выберите из списка **Яндекс.Браузер**.



Далее в появившемся окне «**Установка**» со списком устанавливаемых пакетов и зависимостей нажмите кнопку « **Принять**». Начнётся установка **Яндекс.Браузера**.



После установки **Яндекс.Браузер** будет доступен из «**Главного меню**» - «**Интернет**» - «**Yandex Browser**».

Установка через терминал

Для установки браузера через терминал выполните команду (потребуются права **администратора**):

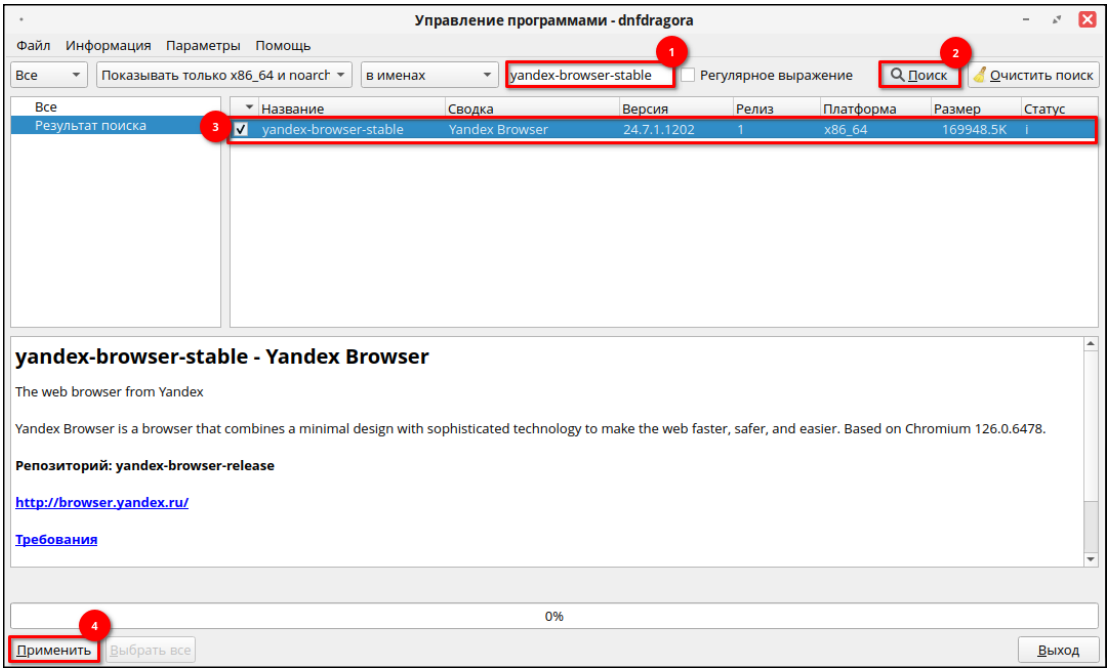
```
sudo dnf install yandex-browser-stable
```

После установки **Яндекс.Браузер** будет доступен из «**Главного меню**» - «**Интернет**» - «**Yandex Browser**».

Установка через dnfdragora

Для установки **Яндекс.Браузера** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**yandex-browser-stable**».

В результатах поиска появится пакет **yandex-browser-stable**. Отметьте флагом пакет и нажмите кнопку «**Применить**» для его установки.



После установки браузер будет доступен из «**Главного меню**» - «**Интернет**» - «**Yandex Browser**».

Решение проблем

В некоторых случаях при попытке установить **Яндекс.Браузер** через терминал или менеджер пакетов dnfdragora пакет **yandex-browser-stable** может быть не найден. Такая ситуация может произойти, если в используемой системе по каким-либо причинам не подключен репозиторий браузера **yandex-browser-release**.

Для решения данной проблемы в терминале рекомендуется выполнить команду подключения репозитория и установки браузера (потребуются права **администратора**):

```
dnf install yandex-browser-release && dnf install yandex-browser-stable
```

Сквозная аутентификация в браузерах

Chromium
Яндекс
Mozilla Firefox
SSO для нескольких доменов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Технология единого входа (англ. **Single Sign-On**) - это механизм, позволяющий пользователю пройти аутентификацию (вход со своими учетными данными) единовременно и получить доступ к различным программным продуктам, используя один идентификатор.

Предварительно необходимо ввести в домен компьютер по инструкции и убедиться, что доменный пользователь получает билет **Kerberos**.

Chromium

Создайте папку, выполнив в консоли команду от пользователя **root**:

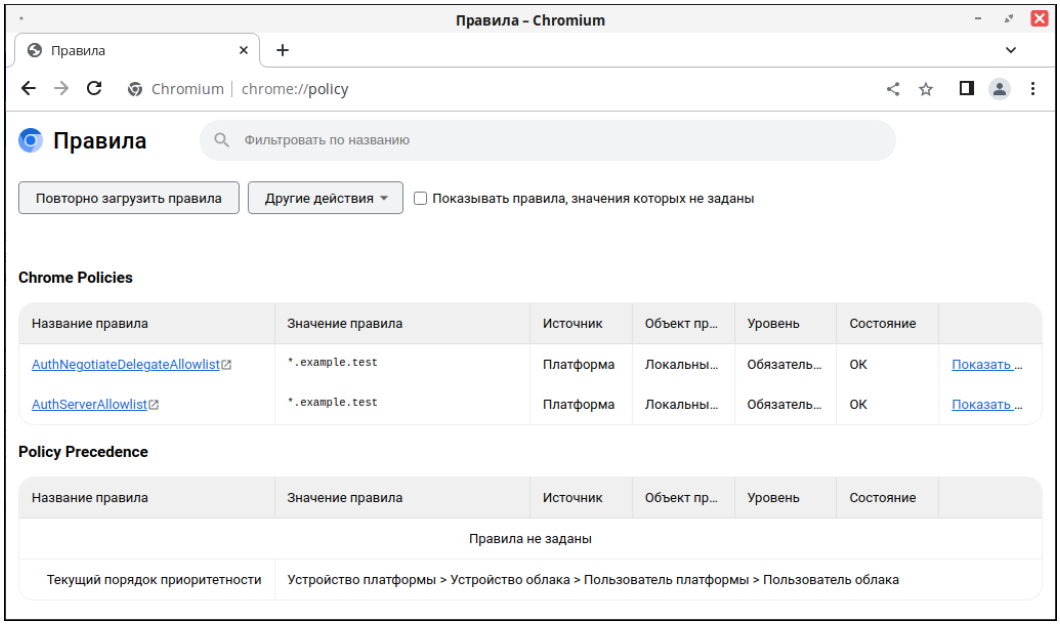
```
mkdir -p /etc/chromium/policies/managed/
```

В ней создайте файл **mydomain.json** следующего содержания:

```
{
 "AuthServerAllowlist": "*.example.test",
 "AuthNegotiateDelegateAllowlist": "*.example.test"
 }
```

где ***.example.test** - имя вашей kerberos-области (**realm**).

После сохранения файла созданные политики будут отображаться в браузере по адресу chrome://policy.



Яндекс

Создайте папку, выполнив в консоли команду от пользователя **root**:

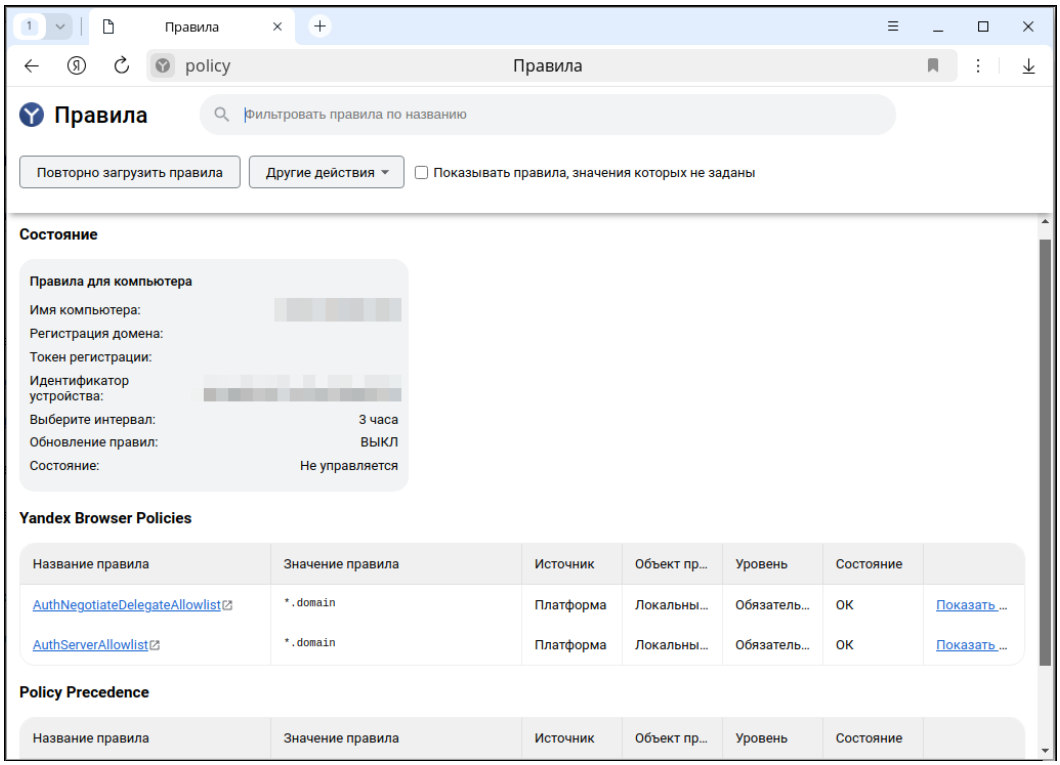
```
mkdir -p /etc/opt/yandex/browser/policies/managed/
```

В папке **managed** создайте файл **mydomain.json** и добавьте в него код:

```
{
 "AuthServerAllowlist": "*.domain",
 "AuthNegotiateDelegateAllowlist": "*.domain"
 }
```

где ***.domain** — имя Kerberos-области (**realm**).

После сохранения файла созданные политики будут отображаться в браузере по адресу browser://policy/.



Mozilla Firefox

В адресной строке введите **about:config**, затем необходимо согласиться с тем, что вы понимаете риски.

В строке поиска найдите параметры:

```
network.negotiate-auth.trusted-uris,
network.automatic-ntlm-auth.trusted-uris,
network.negotiate-auth.delegation-uris
```

и укажите в этих параметрах имя вашей kerberos-области (**realm**):

```
.example.test
```

Теперь вы можете успешно войти на сайт, поддерживающий SSO, под доменным пользователем.

SSO для нескольких доменов

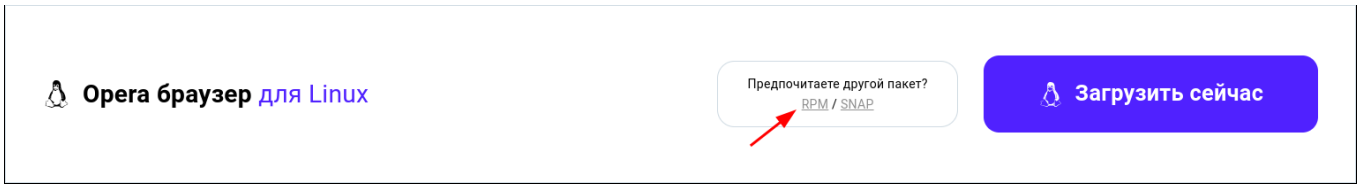
Для включения технологии единого входа *для нескольких доменов* синтаксис файла **.json** должен быть иметь следующий вид:

```
{
"AuthNegotiateDelegateAllowlist": "domain1.example.com,domain2.example.com"
"AuthServerAllowlist": "URL1,URL2"
}
```

Opera

Для установки браузера **Opera** перейдите на официальный сайт разработчика.

Перейдите к разделу «**Загрузить все браузеры Opera**» и раскройте список доступных пакетов для нужного браузера. Рядом с «**Opera браузер для Linux**» нажмите на **RPM**. Начнется загрузка RPM-пакета браузера.



После загрузки перейдите в каталог, куда был скачан пакет (в примере **/home/user/Загрузки/**), кликните ПКМ по файлу и в появившемся контекстном меню выберите «**Открыть в Средство установки пакетов dnfdragora**». Введите пароль *администратора* системы для начала установки пакета.

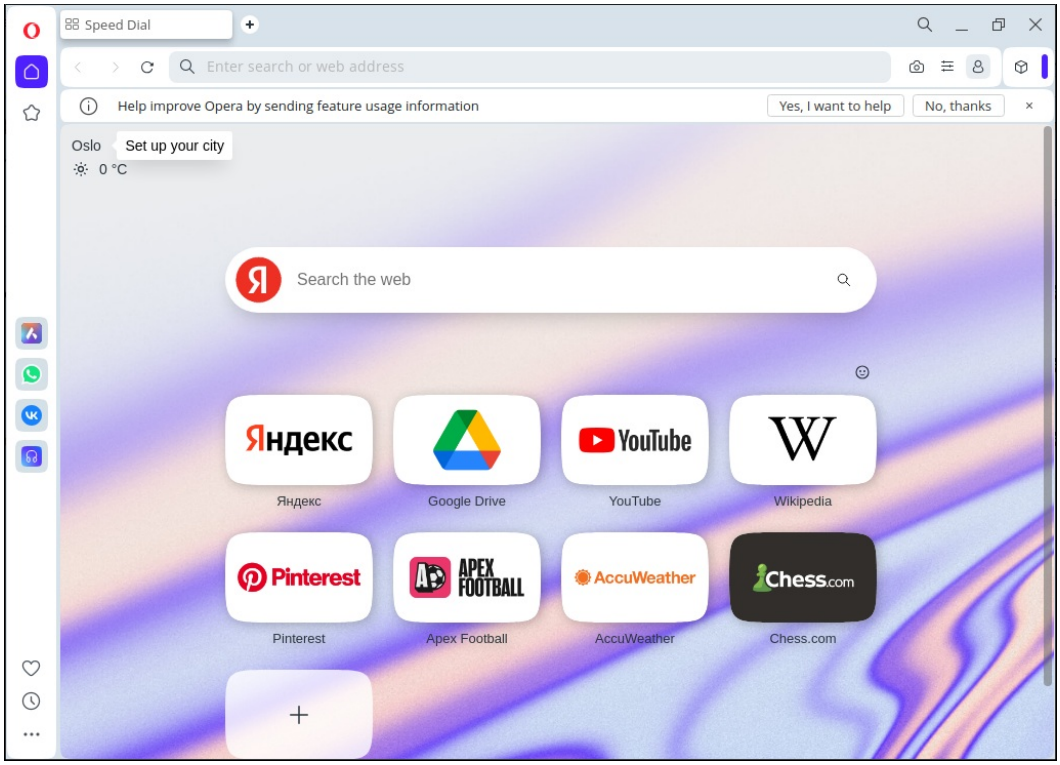
Установку также можно выполнить через терминал (потребуются права *администратора* системы). Перейдите в каталог со скачанным пакетом:

```
cd /home/user/Загрузки/
```

выполните установку:

```
sudo dnf install ./opera-stable_109.0.5097.35_amd64.rpm
```

После установки браузер будет доступен из «**Главного меню**» - «**Интернет**» - «**Opera**».



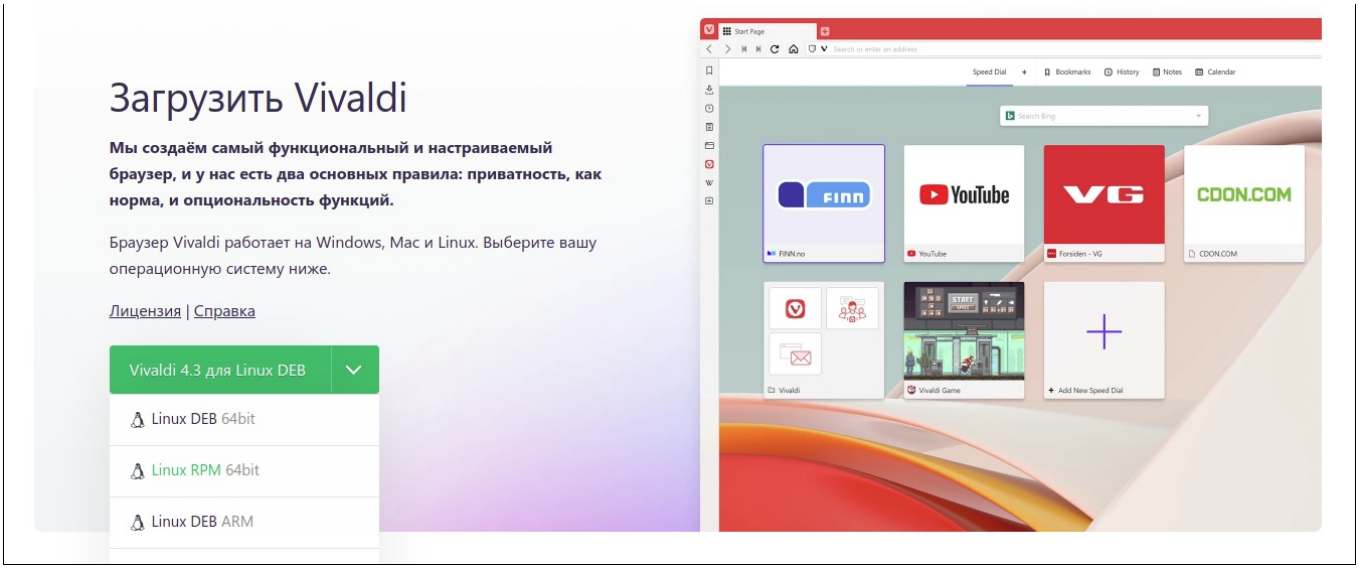
Vivaldi

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Vivaldi - 5.4.2753

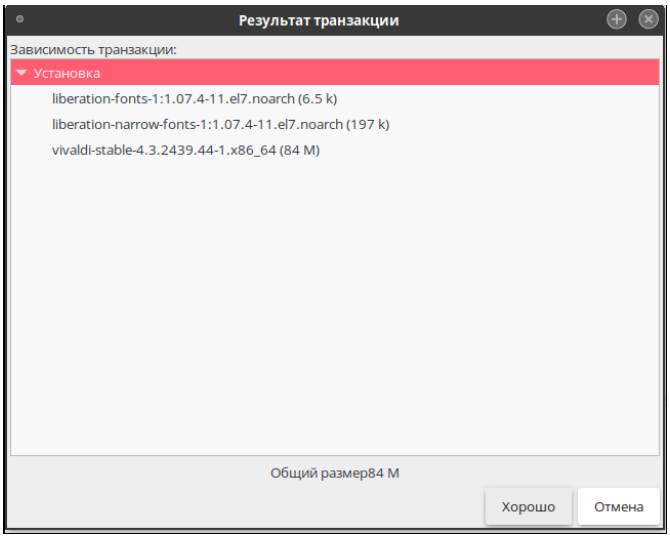
Vivaldi — интернет-браузер, созданный компанией **Vivaldi Technologies** на основе движка **Blink**. Первая тестовая версия стала доступна 27 января 2015 года.

Для загрузки данного браузера необходимо перейти на сайт разработчика и скачать файл «**Linux RPM 64bit**».



После завершения загрузки необходимо перейти в папку, куда был загружен RPM-пакет, и запустить установку двойным нажатием на него.

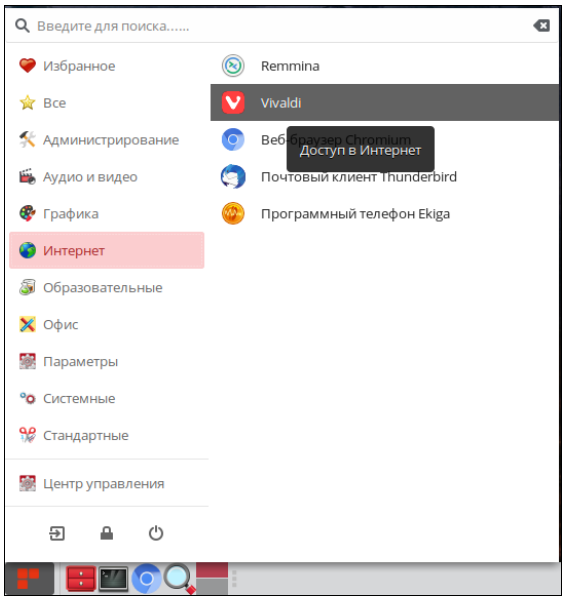
В результате откроется диалоговое окно:



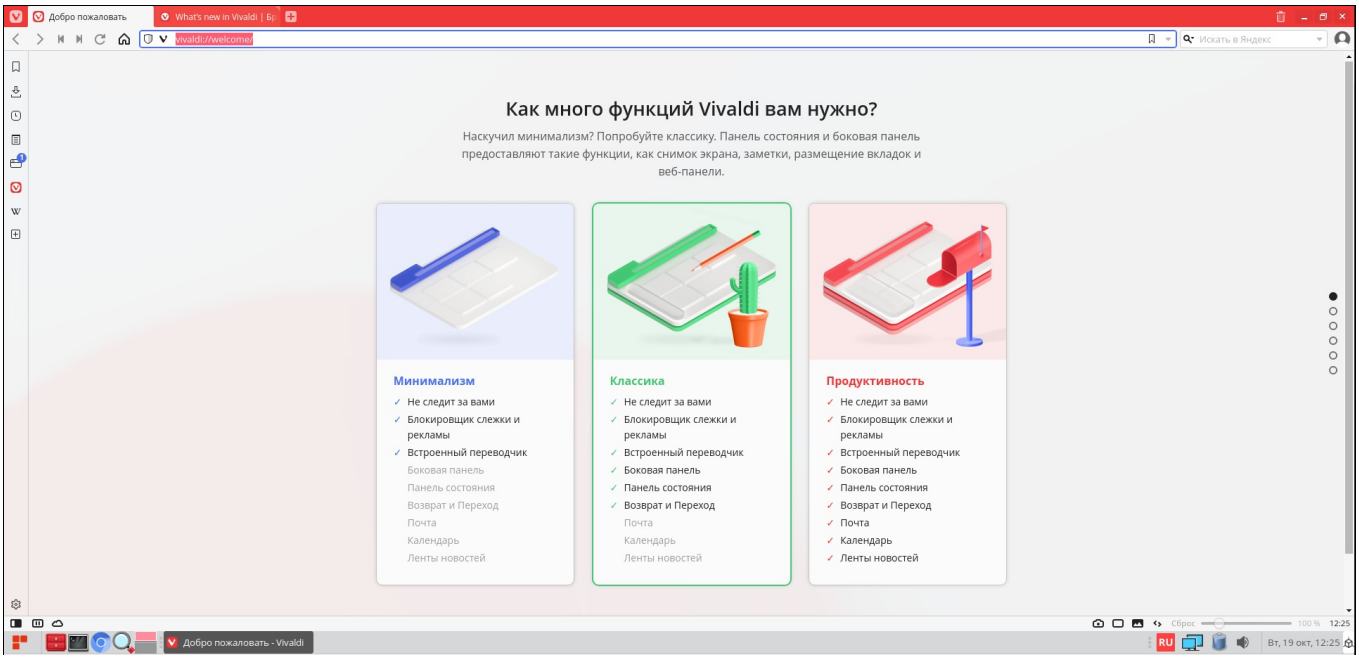
Для установки браузера из консоли потребуется открыть терминал в той директории, куда был скачан RPM-пакет, и выполнить команду:

```
sudo -E dnf install ./vivaldi-stable-5.4.2753.51-1.x86_64.rpm
```

По завершении установки браузер станет доступен из «**Меню**» - «**Интернет**».



При первом запуске **Vivaldi** предоставит возможность выбора режима функциональности для дальнейшей работы, после этого можно будет приступить непосредственно к работе с браузером.



Сбор и просмотр диагностической информации браузеров

Сбор информации в браузерах на основе Chrome
Просмотр лога NetExport с помощью Net Log Viewer

Окружение

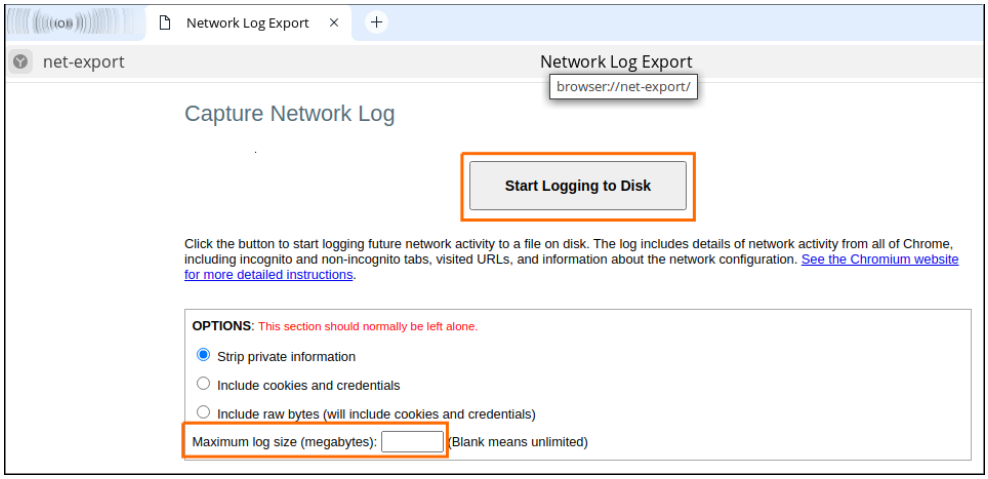
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Сбор информации в браузерах на основе Chrome

При возникновении проблем подключения, отображения информации, производительности может потребоваться анализ логов, полученных посредством встроенного в браузер инструмента **NetLog**. **NetLog** позволяет собирать следующие данные:

- попытки **TCP**-соединений к **IP**-адресам;
- эффективные (применённые) настройки прокси;
- изменение настроек прокси в процессе сбора логов;
- события изменения сети;
- задержки при постановке в очередь **DNS**-запросов;
- результаты предварительных **DNS**-запросов;
- попадания в кеш при разрешении **DNS**-запросов;
- информация о чтениях/записях в кеш браузера;
- прочие ошибки.

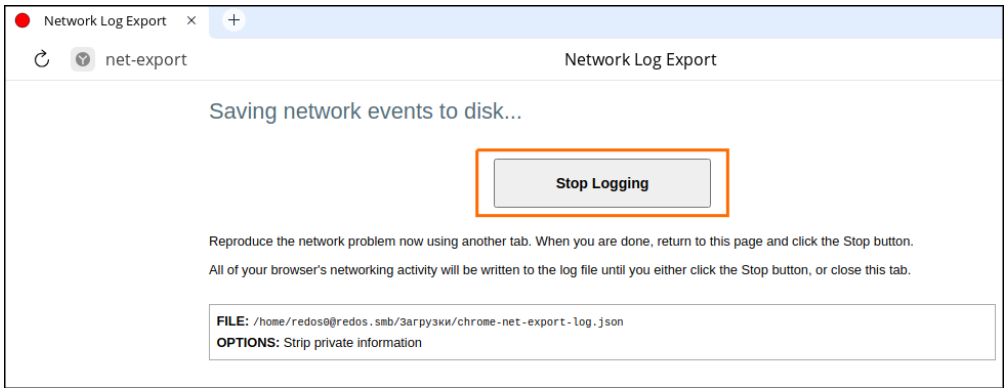
Для запуска сбора логов необходимо открыть браузер, ввести в адресной строке chrome://net-export (для браузера *Яндекс* — browser://net-export) и нажать **Enter**. Откроется страница настройки и запуска сбора информации.



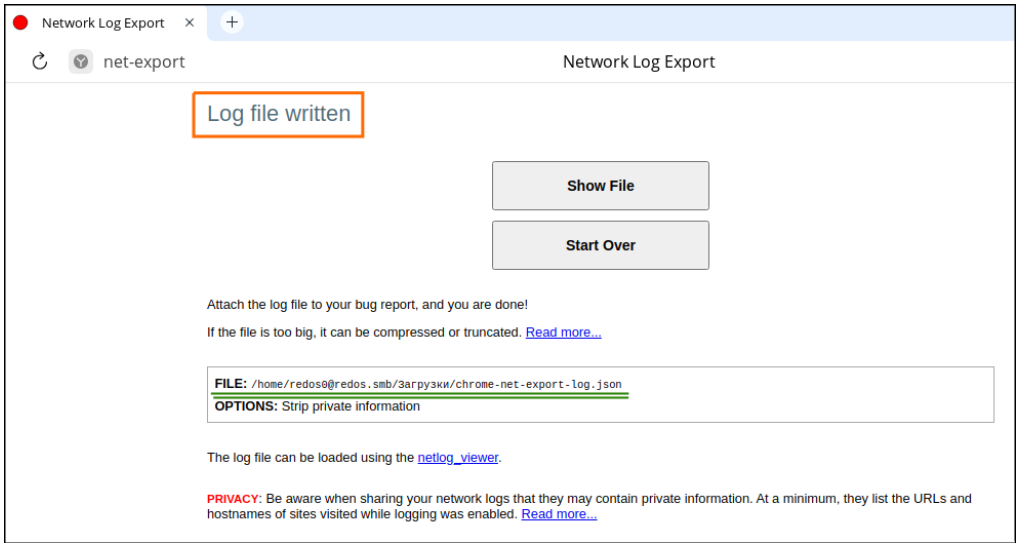
По умолчанию сбор информации не включает приватные данные (*cookies* и данные аутентификации) и не ограничен по размеру. Для ограничения размера файла лога можно указать значение (в мегабайтах) в поле **Maximum log size**. Для начала записи следует нажать кнопку «**Start Logging to Disk**». Появится диалог сохранения файла лога, в котором будет необходимо выбрать его местоположение и имя.

Следующим шагом, не закрывая текущей вкладки «**Network Log Export**», следует воспроизвести действия, при которых проявляется исследуемая проблема.

Затем осуществить переход на вкладку «**Network Log Export**» и нажать кнопку «**Stop Logging**».



Страница обновится и на ней появится надпись «**Log file written**», что свидетельствует об успешной записи файла лога.



Полный путь к сформированному файлу будет отображён в информационном поле **FILE** ниже кнопок **Show File** и **Start Over**.

Просмотр лога NetExport с помощью Net Log Viewer

Инструмент **Net Log Viewer** позволяет просмотреть сохраненный ранее лог в формате удобном для анализа.

1. Установка пакета **git** (потребуются права администратора):

```
sudo dnf install git
```

2. В результате выполнения следующей команды в текущем каталоге будет создан подкаталог catapult, куда будет загружен необходимый набор утилит:

```
git clone https://chromium.googlesource.com/catapult
```

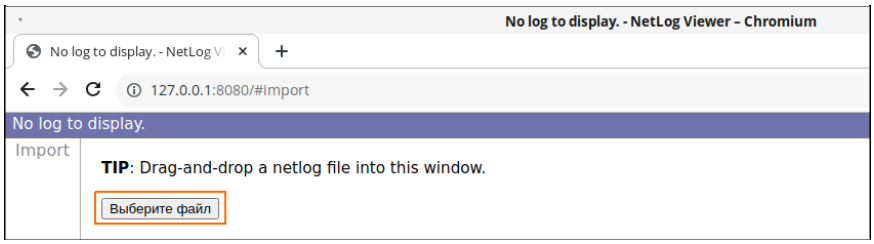
> **Примечание.**
>
> Для размещения набора утилит **Catapult** потребуется около **1 Гб** свободного дискового пространства.

3. Запуск инструмента **Net Log Viewer** производится командой:

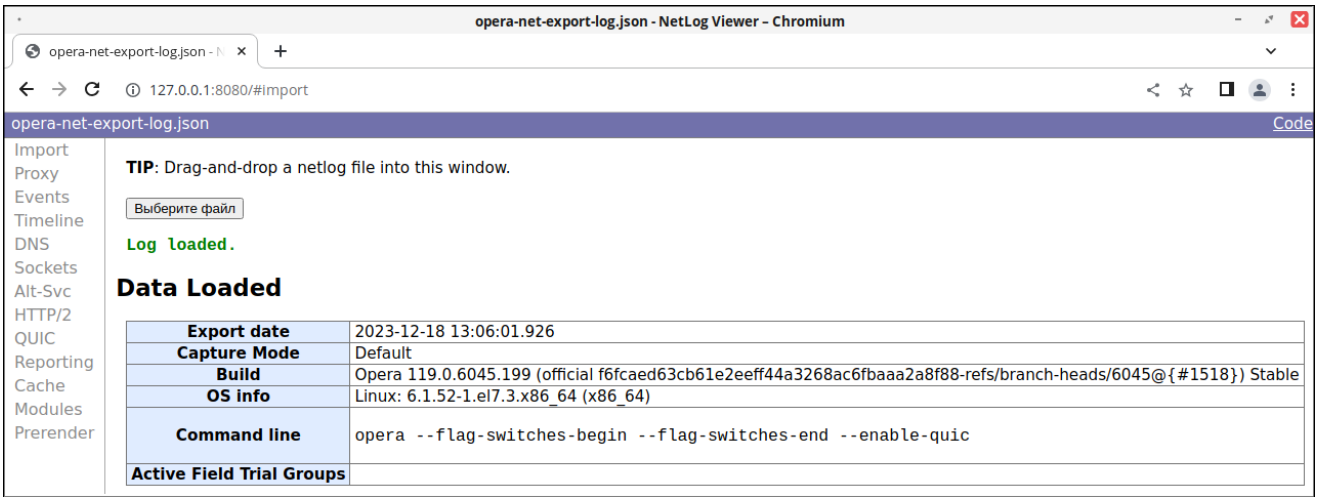
```
./catapult/netlog_viewer/bin/serve_static
```

4. При выполнении команды из п. 3 будет запущен HTTP-сервер, прослушивающий TCP-порт **8080**, к которому следует подключиться для загрузки и обработки лога. **URL** для ввода в адресную строку браузера: http://127.0.0.1:8080 или http://localhost:8080.

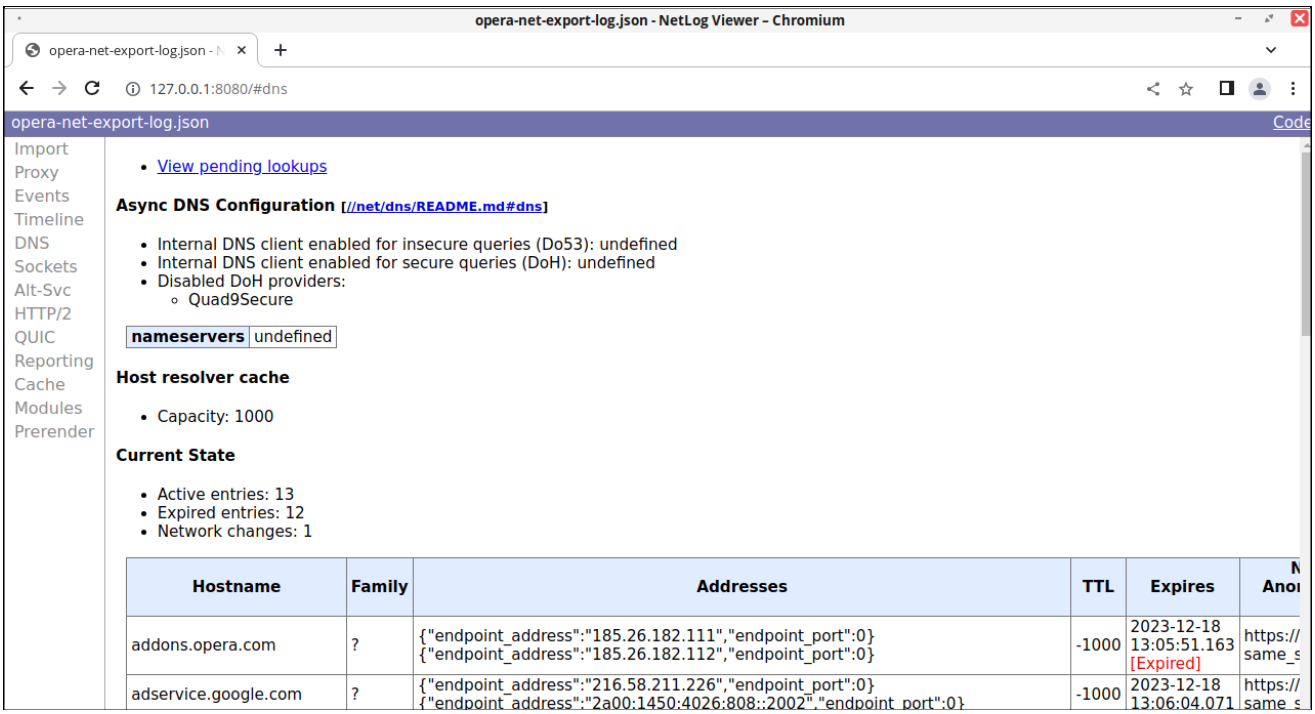
При переходе на указанный выше адрес отобразится страница импорта файла, созданного инструментом **NetLog**. Для выбора файла лога предназначена кнопка «**Выберите файл**».



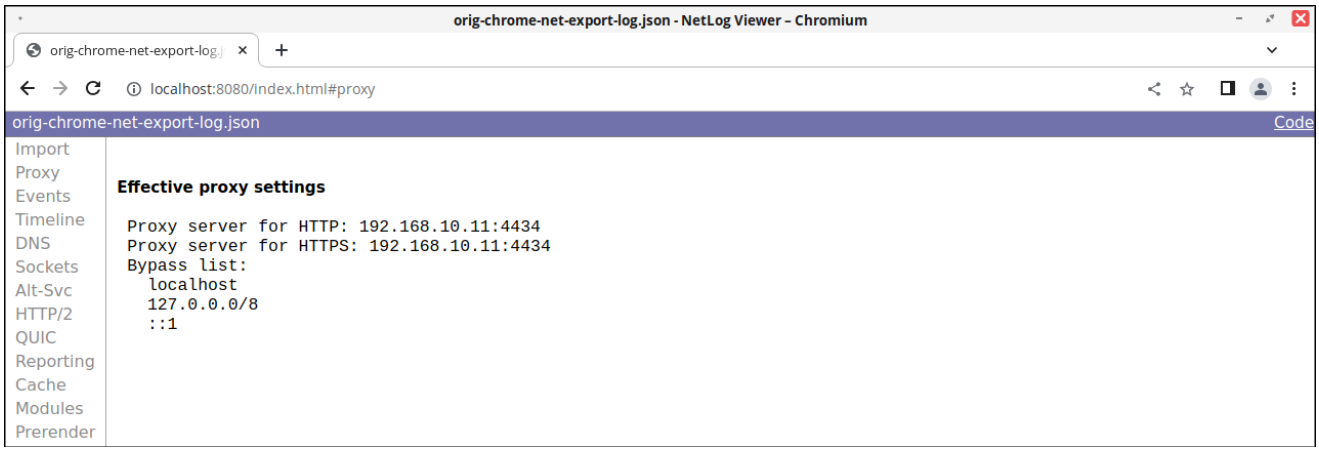
5. После успешной загрузки будет отображена общая информация об условиях сбора лога и запуска браузера. Поле **Command line** может быть полезно для определения параметров, переданных при запуске исполняемого файла, часть которых могла быть скрыта в командной строке посредством применения alias или промежуточного сценария запуска. В правой части страницы будет выведен список, который используется для перехода к различным типам данных.



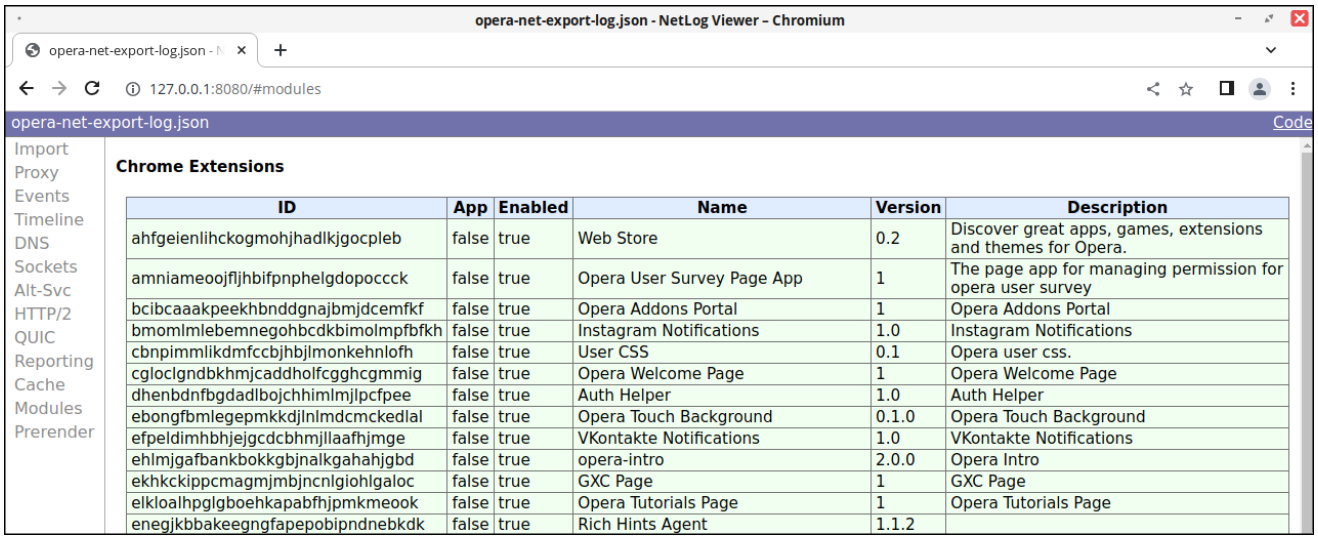
На странице **DNS** отображаются данные конфигурации **DNS**, состояние записей в кеше браузера.



На странице **Proxy** доступна информация об эффективных (действовавших на момент сбора лога) адресах прокси-серверов и адресах исключений. Значения данных параметров могли быть переданы браузеру различными способами (через параметры командной строки, переменные окружения, настройки в графическом режиме, WPAD), поэтому при анализе проблем доступности важно знать эффективные (действующие) значения.



На странице **Modules** в таблице представлена общая информация о загруженных расширениях браузера.



ID	App	Enabled	Name	Version	Description
ahfgeienlihckogmohjhadlkjgocpleb	false	true	Web Store	0.2	Discover great apps, games, extensions and themes for Opera.
amniameoojfljhbifpnphelgdopoccck	false	true	Opera User Survey Page App	1	The page app for managing permission for opera user survey
bcibcaaakpeekhbnddgnajbmjdcemfkf	false	true	Opera Addons Portal	1	Opera Addons Portal
bmomlmlebemnegohbcdkbimolmpfbfkh	false	true	Instagram Notifications	1.0	Instagram Notifications
cbnpimmlikdmfccbjhbjlmonkehnlofh	false	true	User CSS	0.1	Opera user css.
cgloclgndbkhmjcaddholfcgghcgmmig	false	true	Opera Welcome Page	1	Opera Welcome Page
dhenbdnfbgdadlbojchhimlmjlpcfpee	false	true	Auth Helper	1.0	Auth Helper
ebongfbmlegepmkkdjlnlmdcmckedlal	false	true	Opera Touch Background	0.1.0	Opera Touch Background
efpeldimhbhjejgcdcbhmjllaafhjmge	false	true	VKontakte Notifications	1.0	VKontakte Notifications
ehlmjgafbankbokkgbjnalkgahahjgbd	false	true	opera-intro	2.0.0	Opera Intro
ekhkckippcmagmjmbjncnlgiohlgaloc	false	true	GXC Page	1	GXC Page
elkloalhpglgboehkapabfhjpmkmeook	false	true	Opera Tutorials Page	1	Opera Tutorials Page
enegjkbbakeegngfapepobipndnebkdk	false	true	Rich Hints Agent	1.1.2	

Настройка Openfire

Openfire — кроссплатформенный XMPP-сервер, написанный на **Java** и использующий двойное лицензирование под *Apache License 2.0* и коммерческой лицензией.

Большая часть задач администрирования сервера решается через веб-интерфейс под управлением **Jetty** (контейнер сервлетов *javax.servlet*, реализующий спецификацию *Servlets 3.1* и предоставляющий функциональность *J2EE*, http-сервера и http-клиента), доступный на портах **9090** (HTTP) и **9091** (HTTPS) по умолчанию; администраторам доступно редактирование настроек сервера, добавление и удаление пользователей, комнат конференций и так далее.

Установка сервера *Openfire* выполняется командой:

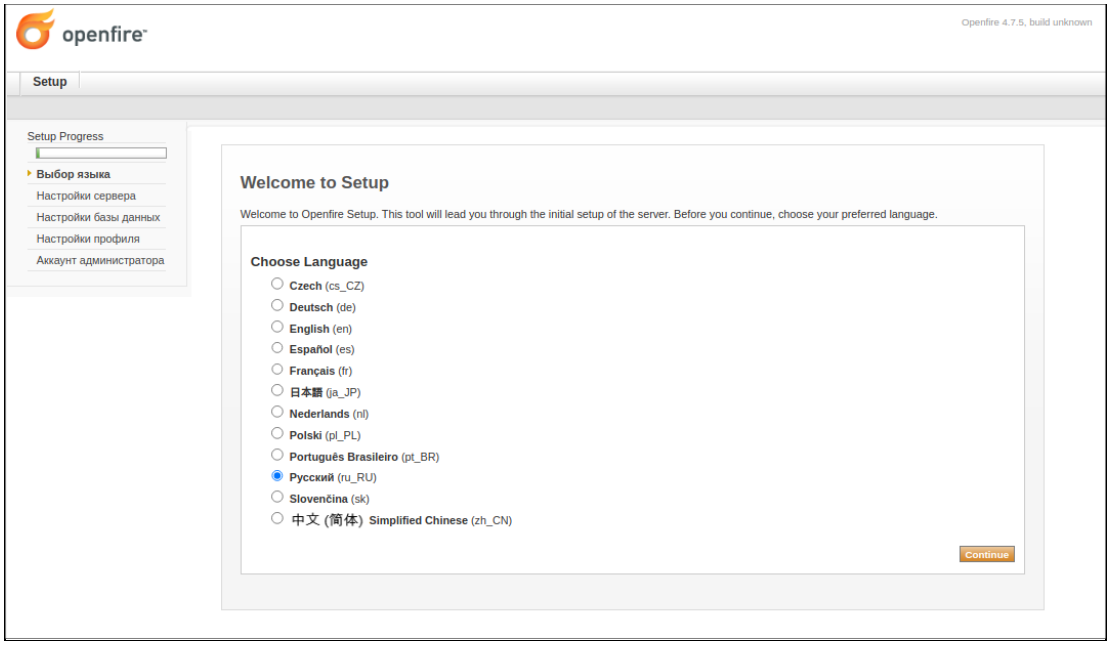
```
dnf install openfire
```

Добавить в автозагрузку и запустить сервер:

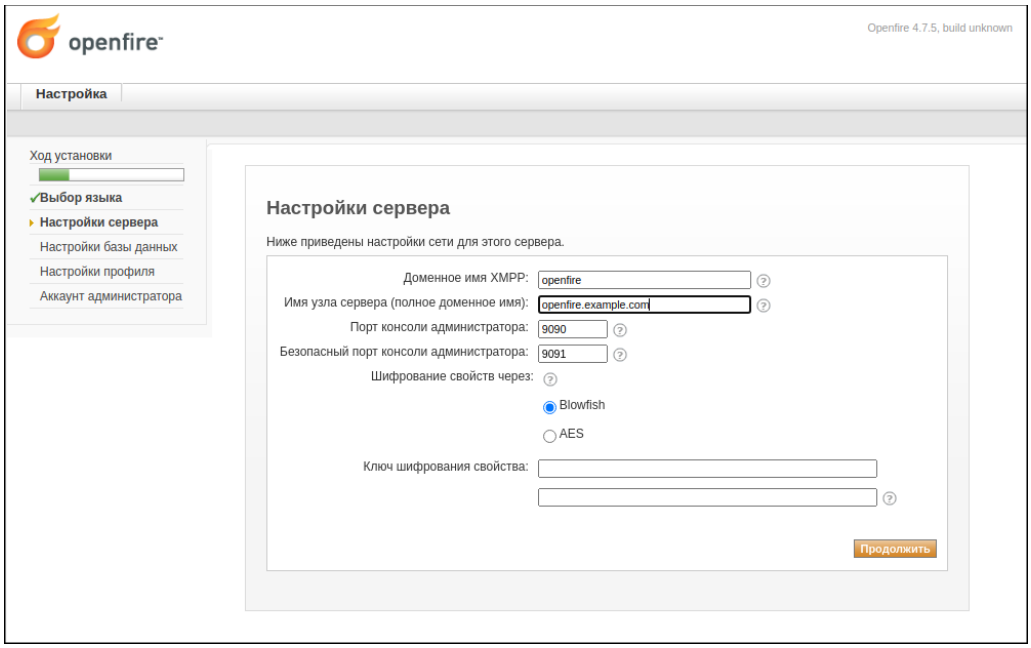
```
systemctl enable openfire --now
```

Для дальнейшей настройки *Openfire*-сервера откройте браузер и перейдите по адресу **http://<IP-адрес сервера>:9090.**

Выберите русский язык и нажмите «**Continue**»:



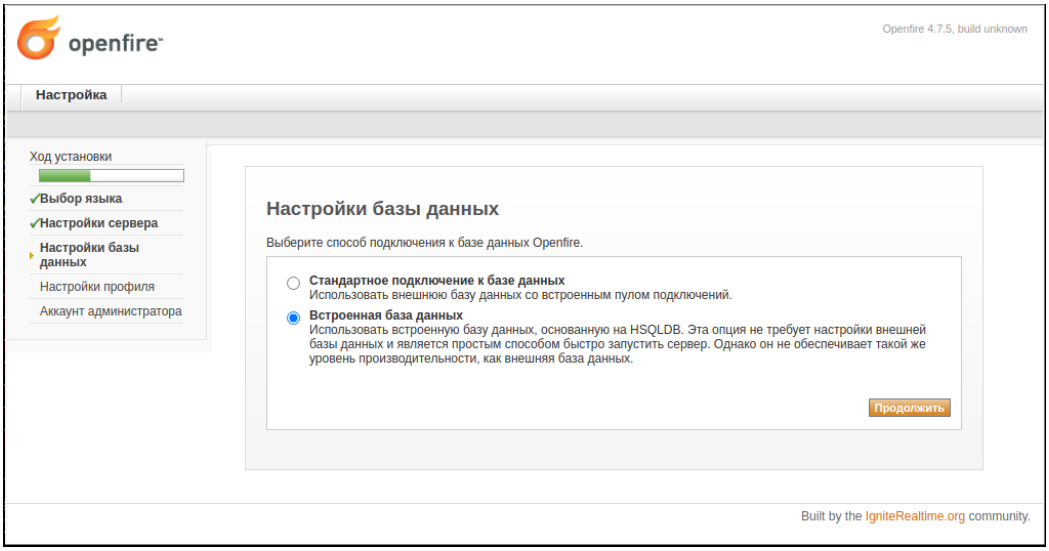
После выбора языка в параметрах сервера нужно заполнить графы «*Доменное имя XMPP*» и «*Имя узла сервера (полное доменное имя)*». В графе «**Доменное имя XMPP**» нужно вписать имя сервера, а в «**Имя узла сервера**» - полное имя домена.



На следующем шаге необходимо выбрать тип базы данных, которую будет использовать *openfire*.

«***Стандартное подключение к базе данных***» использует внешнюю базу данных, например, MySQL, MariaDB и др.

«***Встроенная база данных***» использует встроенную базу данных, которую не нужно настраивать, но предлагающую меньший уровень исполнения, чем внешняя. В нашем примере будем использовать тип «***Встроенная база данных***».

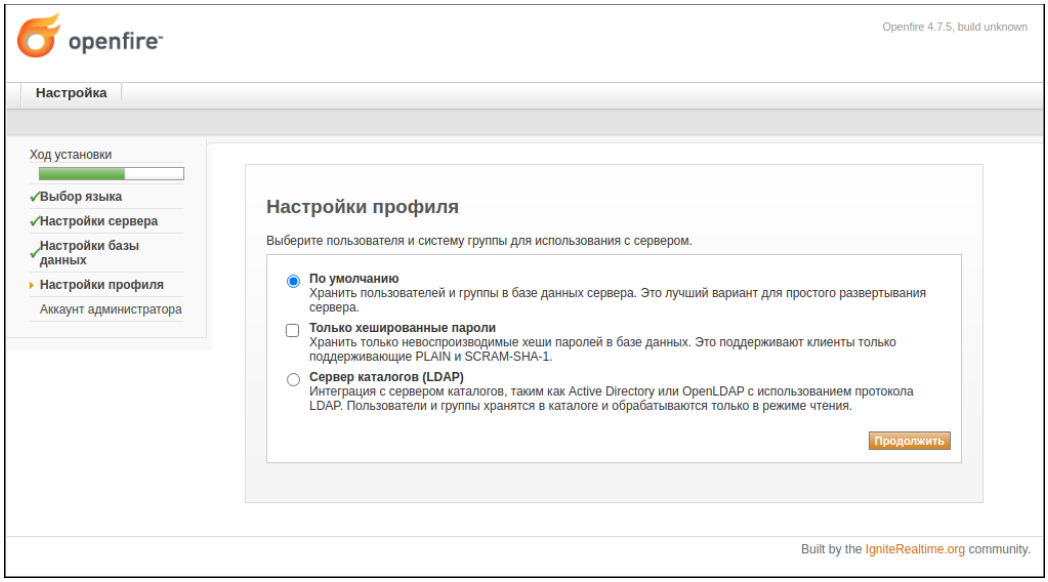


Переходим к настройкам профиля. В настройке профиля выбираем «***По умолчанию***».

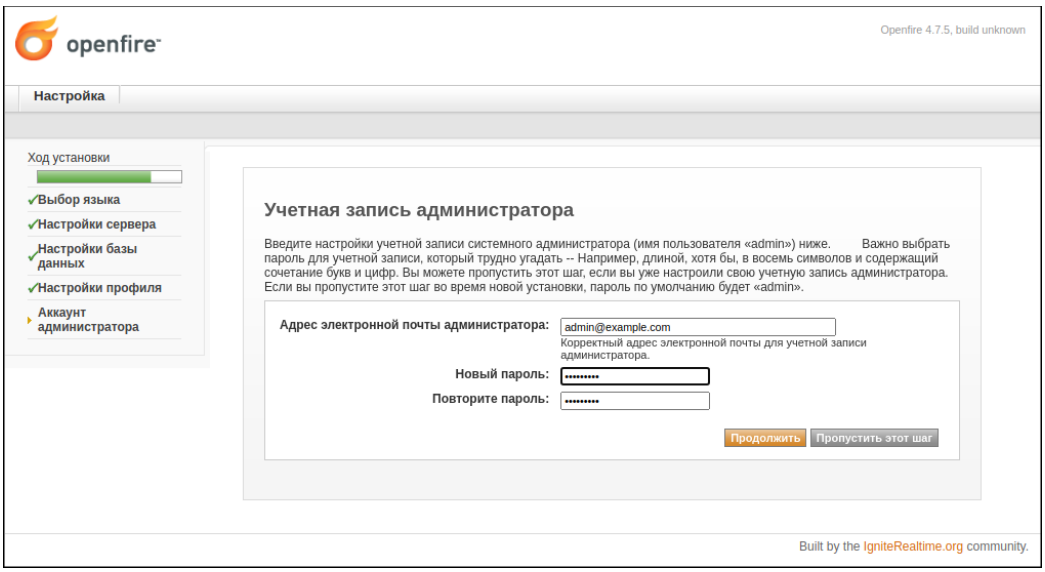
По умолчанию – уже настроенный профиль для простого развертывания сервера.

Только хешированные пароли – используется для хранения в базе данных только необратимых хеш-паролей.

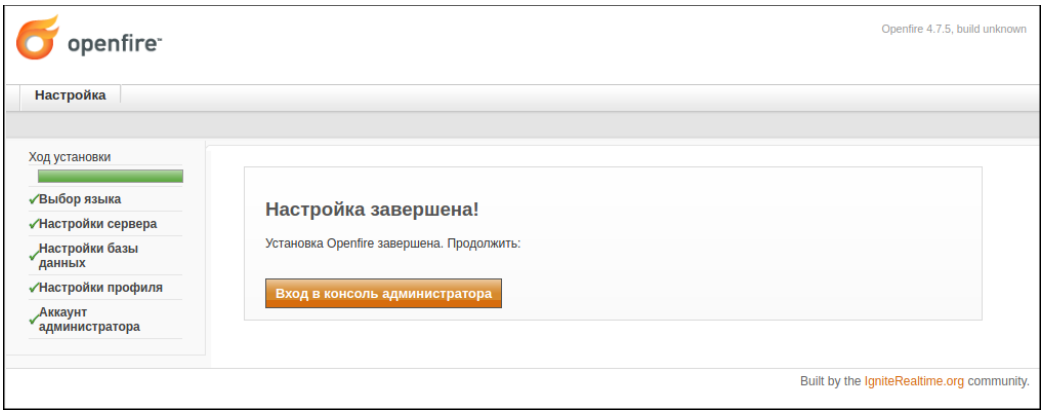
Сервер каталогов (LDAP) – использование сервера каталогов (Active Directory или OpenLDAP) с использованием протокола **LDAP**. Пользователи и группы хранятся в каталоге и обрабатываются только в режиме чтения.



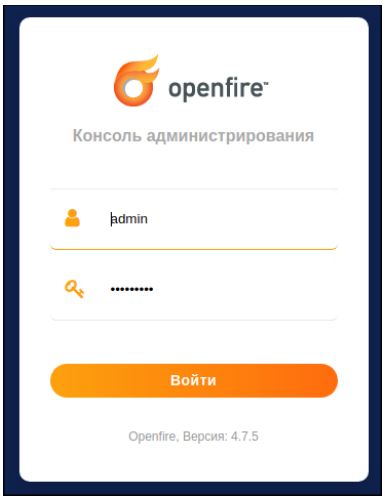
В настройках администратора необходимо ввести свой пароль и почту.



Затем необходимо войти в консоль администратора.

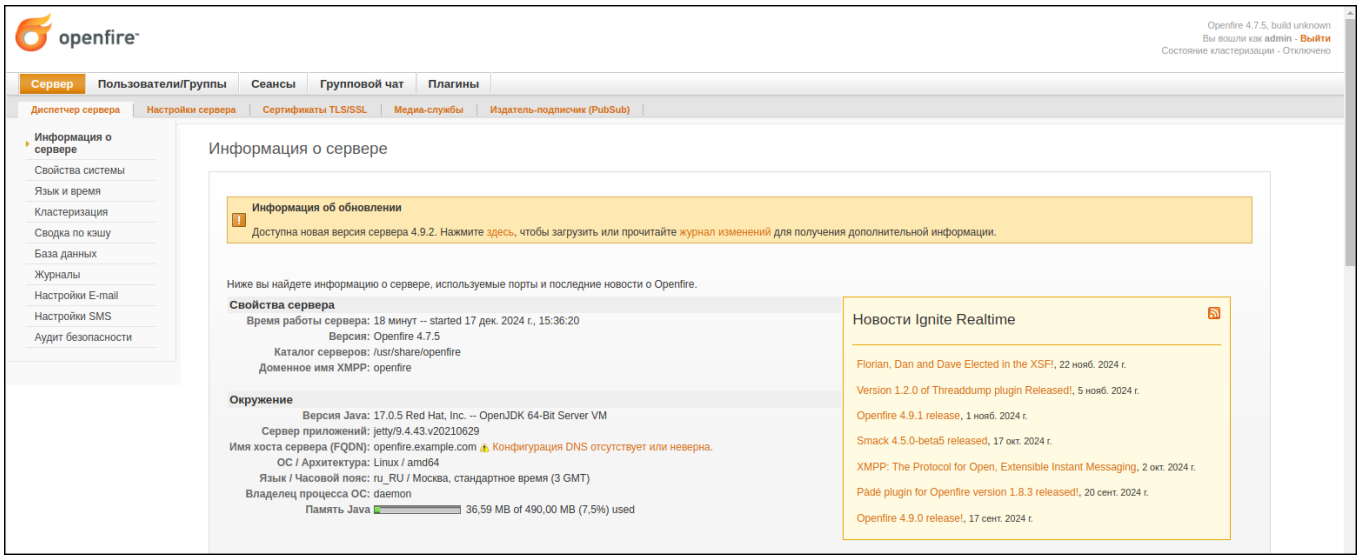


Имя пользователя по умолчанию **admin**.

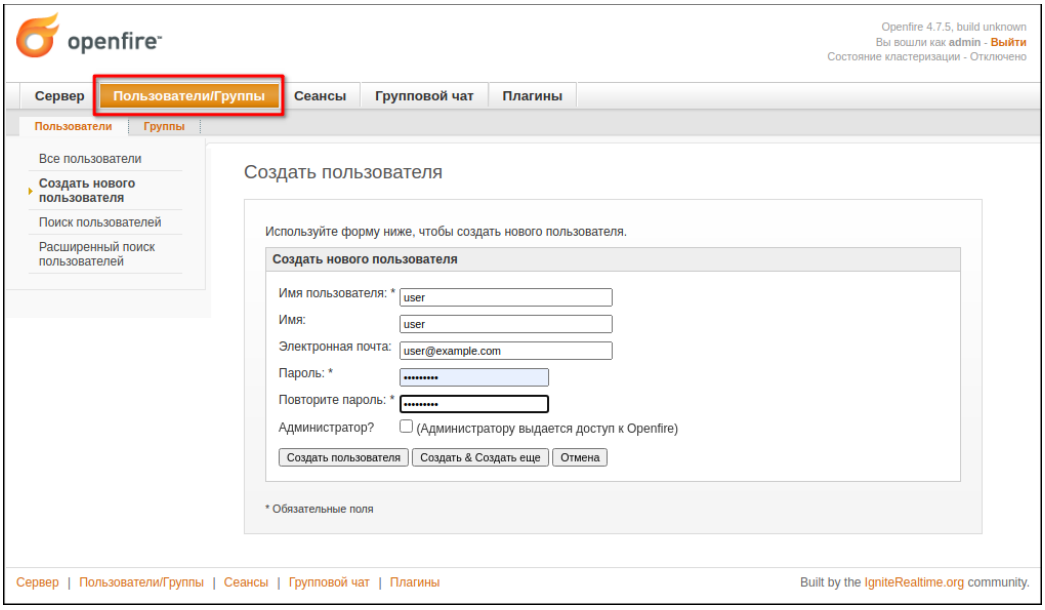


В консоли администратора доступны следующие настройки:

- *Создание кластеризации* – если у вас не встроенная база данных, вы можете с помощью кластеризации соединить несколько Openfire-серверов для более удобной работы. В подвкладке «Настройка сервера» также есть настройка «Сервер-сервер», позволяющая настроить соединение с удаленным сервером.
- *Сообщения оффлайн* – настройка хранения сообщений в автономном режиме, чтобы отправляемые сообщения занимали меньше места на сервере.
- *Хранение закрытых данных* – дает возможность пользователю скрывать свои настройки.
- Во вкладке «*Пользователи/группы*» вы можете создавать пользователей и распределять их по созданным группам (см. создание пользователя ниже).
- Во вкладке «*Сеансы*» вы можете посмотреть сеансы клиента/сервера и компоненты сеансов, а так же настроить их в «*Инструментах*».
- Во вкладке «*Групповой чат*» вы можете создать комнату и общаться с пользователями, а так же настроить сервис.
- Во вкладке «*Плагины*» вы можете установить удобные плагины для работы с Openfire-сервером.



Последний шаг – создание пользователей. Заходим в раздел «***Пользователи/группы***» – «***Создать нового пользователя***». Вводим имя пользователя, пароль, подтверждение пароля и нажимаем «***Создать пользователя***».



Настройка SSO openfire

Настройка сервера jabber/xmpp с базой данных единого входа SSO на FreeIPA.

Требования

- Нужен рабочий домен ipa.

В примере домен IPA - IPA.EXAMPLE.COM. Сервер, содержащий каталог kercos kdc, ldap и DNS-сервер, - ipa.example.com.

- сервер, подключенный к домену IPA, где мы установим программное обеспечение jabber/xmpp.

В данном случае сервер openfire.example.com.

Установка

Установите его от пользователя root:

```
[root@openfire ~] dnf install openfire
```

Конфигурирование

Переведите selinux в режим disabled.

На время настройки сервиса переведите selinux в режим disabled. Для этого измените содержимое конфигурационного файла:

```
nano /etc/selinux/config
```

Заменив текст SELINUX=enforcing на SELINUX=disabled

Более подробно см.ссылку
Не забудьте включить selinux после завершения настройки.

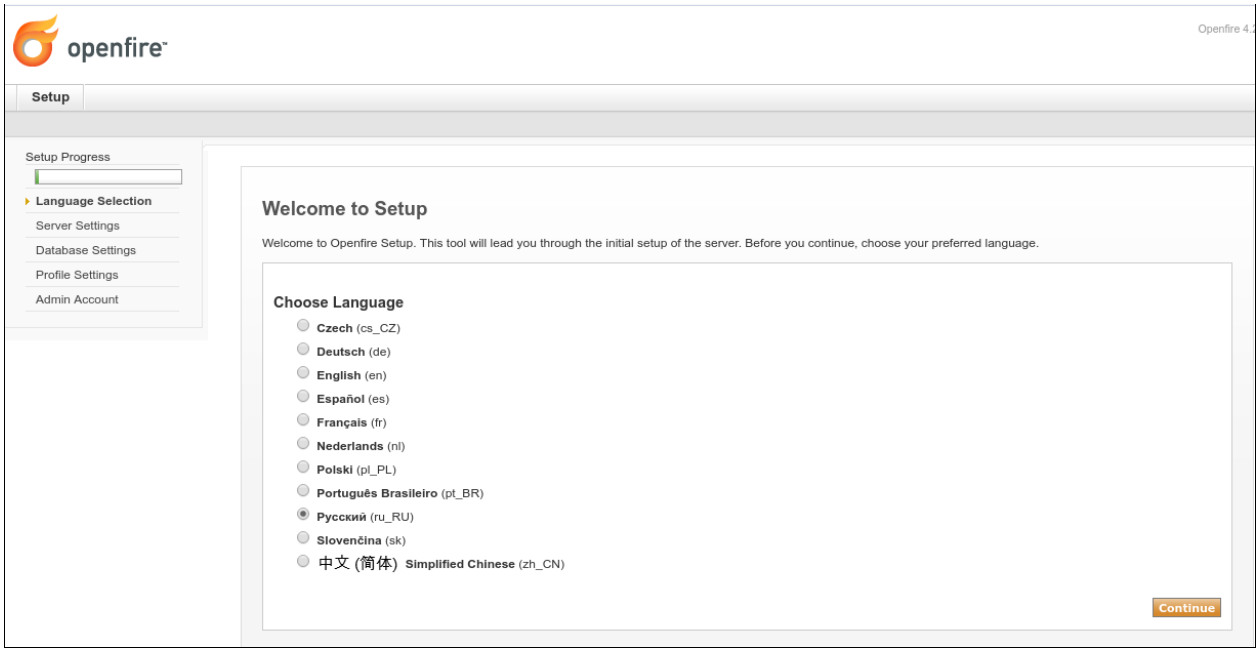
Openfire имеет приятный веб-интерфейс для настройки чат-сервера. Чтобы получить доступ к нему, нам нужно сначала запустить демон openfire:

Запуск демона

```
[root@openfire ~] systemctl start openfire
[root@openfire ~] # systemctl enable openfire
```

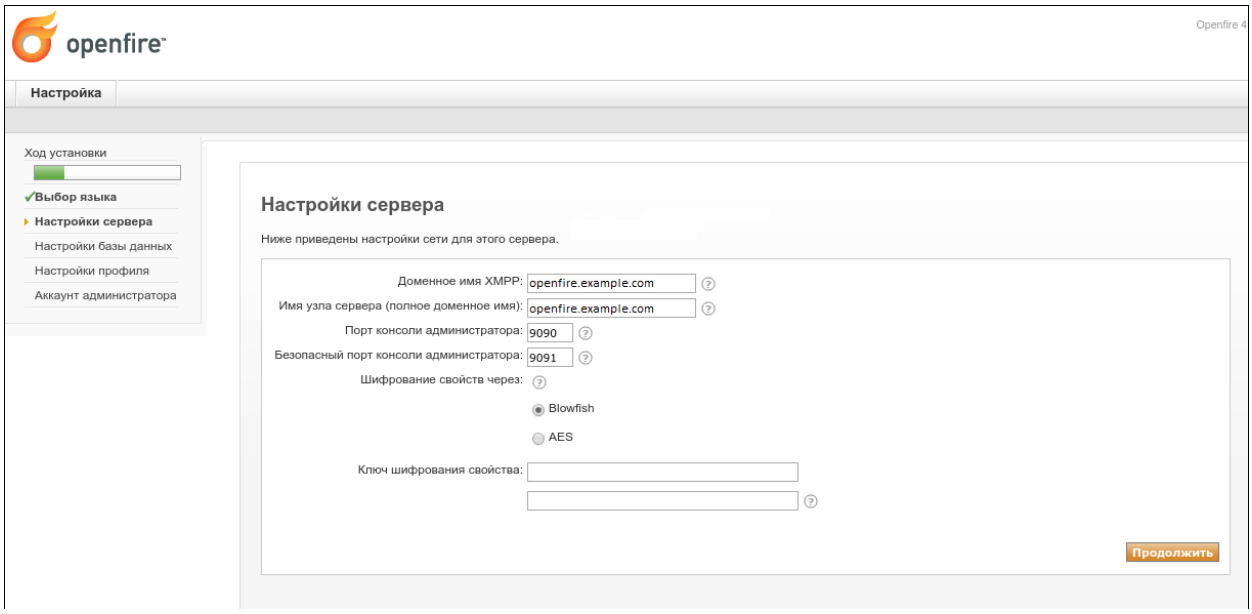
Настройка из веб-интерфейса

Веб-интерфейс доступен по адресу localhost:9090

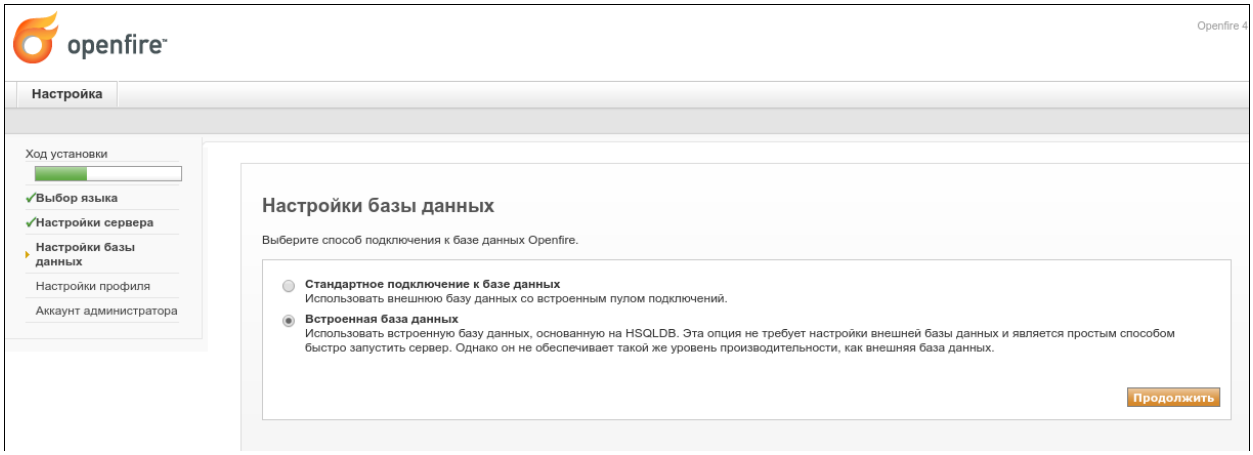


Выберите русский язык и нажмите кнопку «Continue»;

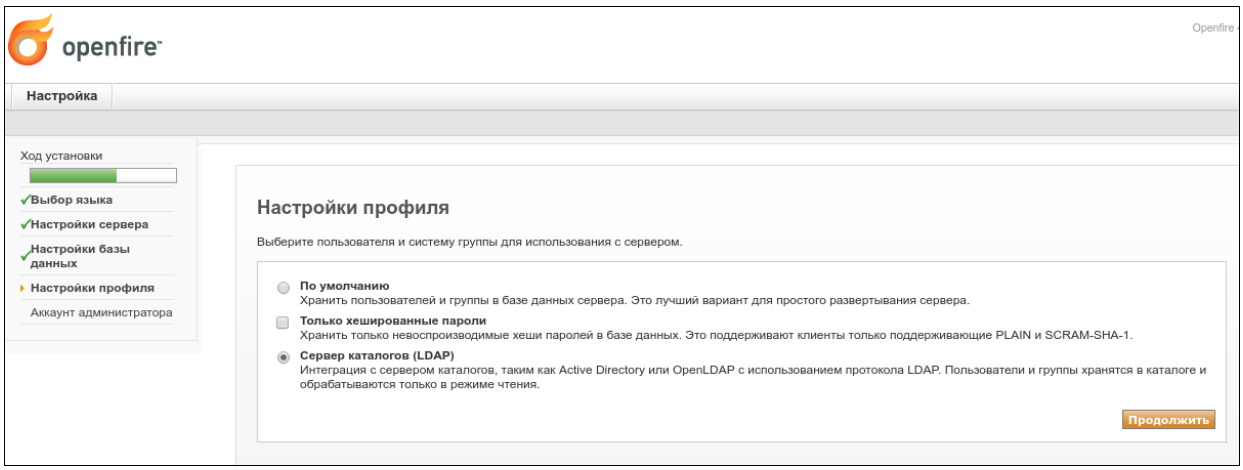
В поле «Доменное имя XMPP» введите fqdn чат-сервера: openfire.example.com. Другие настройки можно оставить без изменений, затем нажмите «Продолжить»;



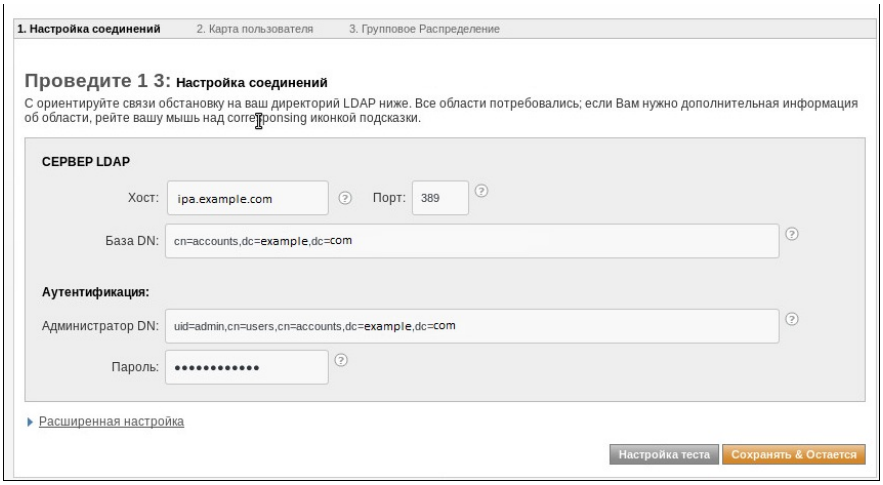
Подключите стороннюю базу данных или используйте встроенную базу данных. Нажмите «Продолжить»;



Выберите «Сервер каталогов (LDAP)» и нажмите «Продолжить»;



Далее заполните fqdn ldap-сервера, в нашем случае:.ipa.example.com. Оставьте стандартный порт ldap (389) и в качестве базы ldap выберите cn= accounts,dc =example,dc = com. Введите администратора DN, в данном случае uid=admin,cn=users,cn=accounts,dc=example,dc=com как на скриншоте.



Оставьте поля аутентификации пустыми (если вы не изменили стандартную установку ipa, ipa разрешает анонимные привязки ldap, если вы отключили это, тогда вам нужно будет ввести имя пользователя / пароль для привязки к серверу ldap) и нажать «Тест», вы должны увидеть сообщение об успешном завершении.

Следующий экран (Настройки профиля: User Mapping) можете ничего не изменять. Просто убедитесь, что в поле «имя пользователя» стоит значение «uid» и нажмите «Продолжить». Вы также можете нажать «Настройки теста», и вы должны увидеть некоторую информацию о своих пользователях ipa, поскольку openfire сопоставляет их с собственной базой данных.

Следующий экран - Настройки профиля: Групповое сопоставление. Откройте «дополнительные настройки» и заполните там "(cn = ipausers)". Этот фильтр получит все члены группы ldap «ipausers» (которая является стандартной группой для каждого пользователя). Его можно использовать, чтобы автоматически добавлять эту группу в адресную книгу каждому клиенту.

Можно использовать фильтр ldap для получения нескольких групп. Если у нас есть 2 группы, ipausers и yurist, мы можем использовать этот фильтр для создания двух групп openfire:

```
(|(cn=ipausers)(cn=yurist))
```

Вы можете отредактировать ldap-фильтр после настройки на веб-интерфейсе (вкладка свойств сервера).

Последним шагом в настройке является учетная запись администратора, введите «admin», и подтвердите. После этого вы можете войти в консоль администратора openfire. Введите имя пользователя и пароль администратора.

Если теперь вы нажмете «Пользователи/Группы», вы увидите своих пользователей ipa на сервере openfire.

Конфигурация SSO

dns autodiscovery

Клиенты xmpp/jabber могут использовать записи dns srv для поиска серверов. Это очень полезно. Мы добавим следующую запись srv в нашу dns зону ipa.example.com:

```
_xmpp-client._tcp 0 100 5222 openfire
```

где _xmpp-client._tcp - это запись, 0 - приоритет, 100 - вес, 5222 - это порт tcp, а openfire – сервер. У вас должна существовать A запись сервера openfire.

Проверьте запись:

```
$ host -t srv _xmpp-client._tcp.example.com
_xmpp-client._tcp.example.com имеет запись SRV 0 100 5222 openfire.example.com.
```

Теперь мы можем подключиться к pidgin только с доменом example.com вместо openfire.example.com, автообнаружение dns автоматически обнаружит сервер.

Создать основную цель службы xmpp

Нам нужно создать основную службу обслуживания kerberos и подключить ее к чат-серверу openfire.example.com. Используйте веб-интерфейс ipa или консоль (у вас должен быть действительный билет администратора kerberos):

```
kinit admin
ipa service-add xmpp/openfire.example.com
```

Проверьте созданную службу:

```
admin@openfire ~] $ipa service-find openfire.example.com
------------------
2 services matched
------------------
  Principal: postgres/openfire.example.com@EXAMPLE.COM
  Keytab: True
  Managed by: openfire.example.com
  Principal: xmpp/ openfire.example.com@ EXAMPLE.COM
  Keytab: True
  Managed by: openfire.example.com
----------------------------
Number of entries returned 2
```

Как вы видите, у этого хоста есть два принципиала: обслуживания и xmpp.

Получите keytab для принципиала службы xmpp

Выполните на сервере openfire команду

```
ipa-getkeytab -s ipa.example.com -p xmpp/openfire.example.com -k openfire.keytab -e des3-hmac-sha1
```

Здесь мы выгружаем keytab для xmpp/openfire.example.com в файл openfire.keytab с правильным шифрованием.

```
[admin@openfire ~] $klist -k -t openfire.keytab
Имя ключевого слова: WRFILE: openfire.keytab
Главный администратор KVNO
---- ----------------- ---------------------------- --------------------------
   3 06/15/12 18:29:53 xmpp/openfire.example.com@EXAMPLE.COM
```

Поместите openfire.keytab в /usr/share/openfire/conf/, сделайте его читаемым только для пользователя - daemon (openfire работает как пользовательский демон).

```
[admin@openfire ~] $ cp /root/openfire.keytab /usr/share/openfire/conf/
[admin@openfire ~] $ chown daemon:daemon /usr/share/openfire/conf/openfire.keytab
```

Проверьте keytab:

```
# kinit -k -t openfire.keytab xmpp/openfire.example.com
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: xmpp/openfire.example.com@EXAMPLE.COM

Valid starting     Expires            Service principal
06/16/12 23:28:35  06/17/12 23:28:35  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

gss.conf

создайте файл gss.conf в /opt/openfire/conf с похожим контентом:

```
com.sun.security.jgss.accept {
   com.sun.security.auth.module.Krb5LoginModule
   required
   storeKey=true
   keyTab="/usr/share/openfire/conf/openfire.keytab"
   doNotPrompt=true
   useKeyTab=true
   realm="EXAMPLE.COM"
   principal="xmpp/openfire.example.com@EXAMPLE.COM"
   debug=true
   isInitiator=false;
};
```

openfire.xml

последний шаг - отредактировать /usr/share/openfire/conf/openfire.xml и добавить блок gssapi/sasl. Добавьте его в конец файла перед тегами <setup>true</setup></jive>

```
  <sasl>
     <mechs>GSSAPI</mechs>
```

```
    <realm>EXAMPLE.COM</realm>
    <gssapi>
      <debug>true</debug>
      <config>/usr/share/openfire/conf/gss.conf</config>
      <useSubjectCredsOnly>false</useSubjectCredsOnly>
    </gssapi>
  </sasl>
```

Перезапустите демон openfire

```
# systemctl restart openfire
```

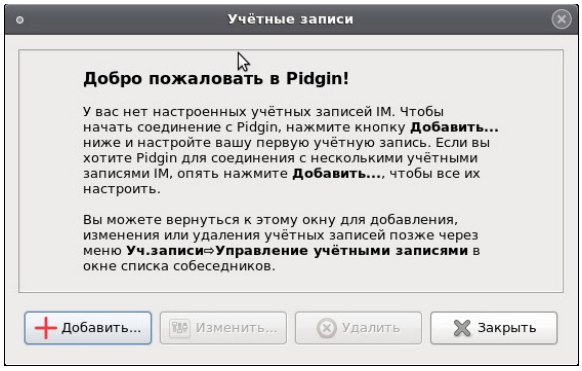
Стоит отметить, что в файле openfire.xml, по-видимому, не хватает информации, которую мы только что добавили после перезагрузки демона. Информация была добавлена в базу данных, но она исчезла из XML-файла. На веб-интерфейсе сервера openfire на вкладке настроек сервера будут установлены настройки.

Логин с SSO

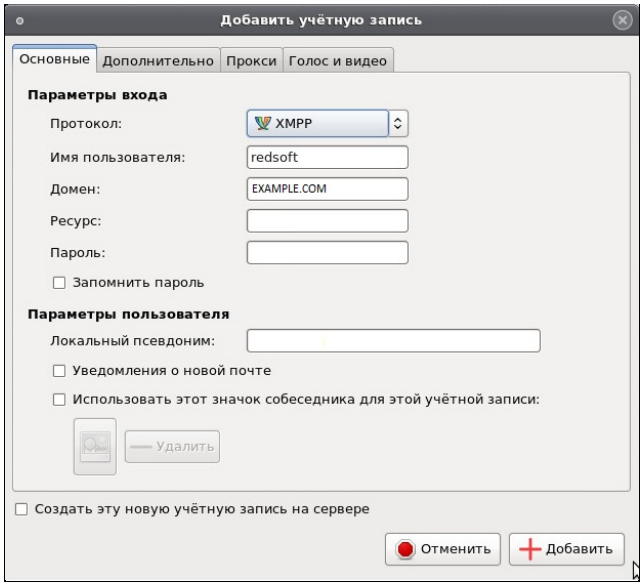
На рабочей станции введенной в домен установите пакет krb5-workstation и pidgin:

```
# dnf –y install krb5-workstation pidgin
```

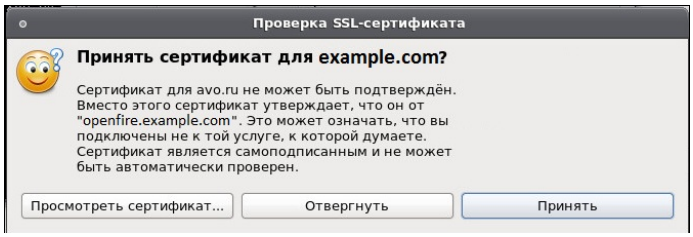
Запустите pidgin (приложения -> интернет ->Клиент обмена мгновенными сообщениями Pidgin);



Добавьте учетную запись xmpp: в закладке «Имя пользователя» введите имя пользователя с именем пользователя ipa, которое вы хотите протестировать, в поле домена заполните имя домена (EXAMPLE.COM); на вкладке «Дополнительно» должен быть заполнен только «порт подключения» (5222), а «Безопасность подключения» должна «требовать шифрования». Вот и все, нажмите «Сохранить», и вам будет предложено принять сертификат с сервера.



Примите SSL-сертификат

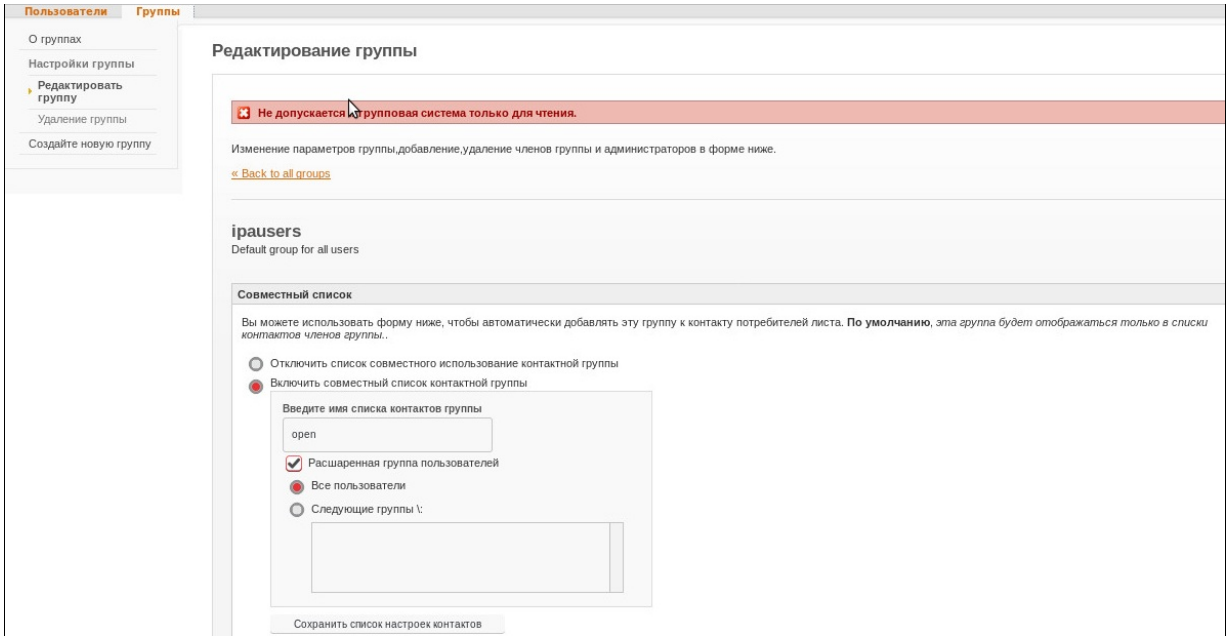


Проверьте получение дополнительного билета kerberos с сервере xmpp:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_500
Default principal: ipauser1@IPA.ASENJO.NX

Valid starting     Expires            Service principal
06/16/12 23:29:03  06/17/12 23:29:00  krbtgt/EXAMPLE.COM@EXAMPLE.COM
    renew until 06/23/12 23:29:00
06/16/12 23:29:09  06/17/12 23:29:00  xmpp/openfire.example.com@EXAMPLE.COM
    renew until 06/23/12 23:29:00
```

Для того, что бы у клиентов появился список пользователей, настройте это на openfire сервере.

Перейдите на вкладку Пользователи и группы, Группы. Нажмите на группу ipausers. Включите совместный список контактной группы и введите её название. Выберите «Разрешенная группа пользователей» и «Все пользователи».



Нажмите на кнопку «Сохранить список настроек контактов».

Pidgin

Pidgin - это чат-программа, которая позволяет вам входить в учетные записи в нескольких чат-сетях одновременно. Это означает, что вы можете одновременно общаться с друзьями на XMPP и сидеть в IRC-канале. *Pidgin* работает на *Windows, Linux* и других UNIX-подобных операционных системах.

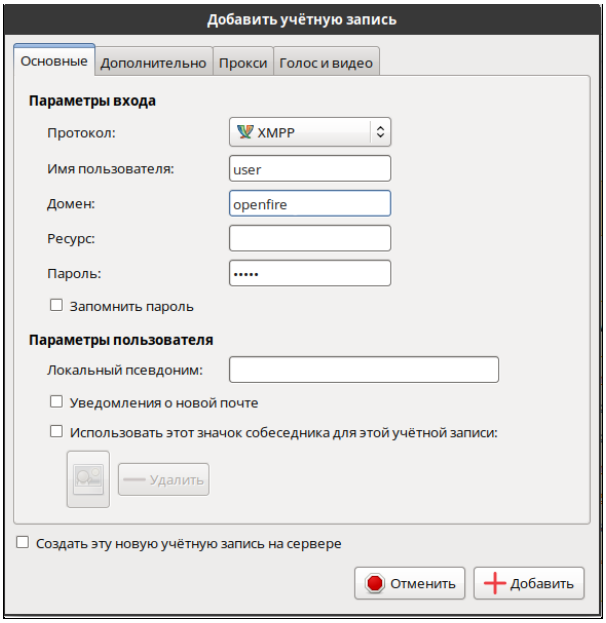
Pidgin поддерживает множество функций этих чат-сетей, такие как передача файлов, удаленные сообщения, значки друзей, пользовательские смайлики и уведомления о вводе текста. Многочисленные плагины также расширяют функциональность Pidgin сверх стандартных функций.

Для установки выполните команду:

```
dnf install pidgin
```

Запуск *pidgin* осуществляется через *«Меню» - «Интернет» - «Клиент обмена мгновенными сообщениями Pidgin»*.

В открывшемся окне нажмите на кнопку «*Добавить*». Далее выберите протокол «*XMPP*» и в полях «*Имя пользователя*» и «*Пароль*» впишите данные одного из созданных на сервере пользователей. В поле «*Домен*» введите имя сервера, тип протокола выберите XMPP.



После создания учетной записи вам необходимо будет принять условия пользовательского соглашения, нажав кнопку «*Принять*». После этого вам будут доступны функции общения. Для создания чата, отправки сообщения и другого функционала нажмите «*Собеседники*».

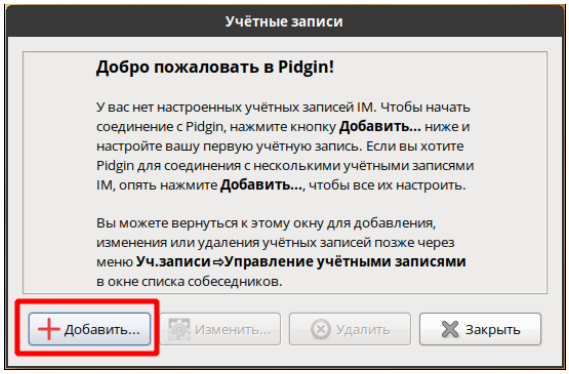
Расширение Pidgin для работы Skype for Business

Skype for business - коммуникационная программа-клиент, позволяющая пользователям общаться друг с другом в реальном времени, используя различные виды коммуникаций: мгновенные сообщения, видео- и голосовую связь, общий доступ к рабочему столу, конференции, передачу файлов. У программы также имеется собственная серверная часть. Тем самым программа является клиентом объединённых коммуникаций и позволяет пользователям общаться и обмениваться информацией.

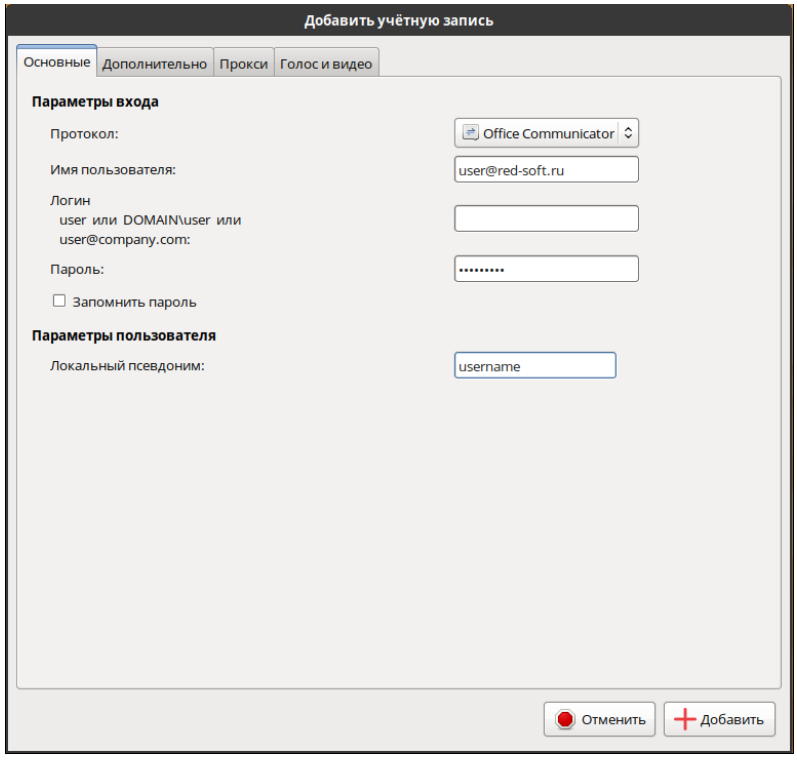
Пакет расширения можно установить следующей командой:

```
dnf install pidgin-sipe purple-sipe
```

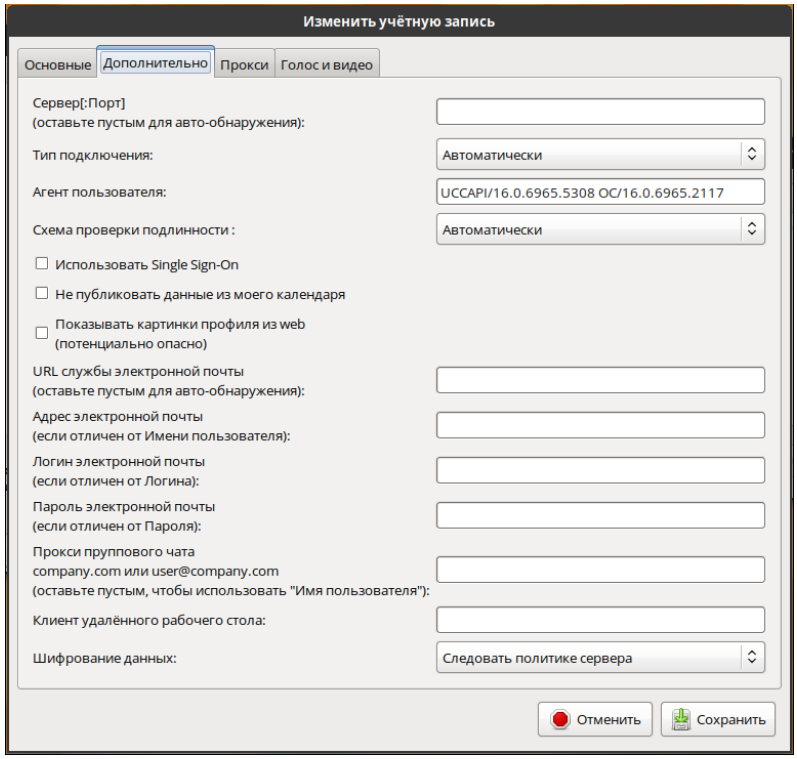
Далее необходимо создать аккаунт при запуске **Pidgin**, для этого нажмите «**Добавить...**».



В открывшемся окне выберите протокол – **Office communicator.**



Далее на вкладке **Дополнительно** пропишите данные вашего **Агента пользователя**, например:



После этого нажмите «**Сохранить**» и проверьте подключение к серверу.

PSI

PSI - это бесплатное приложение для обмена мгновенными сообщениями, предназначенное для сети XMPP. Быстрый и легкий *Psi* полностью открыт и совместим с *Windows, Linux* и *macOS*.

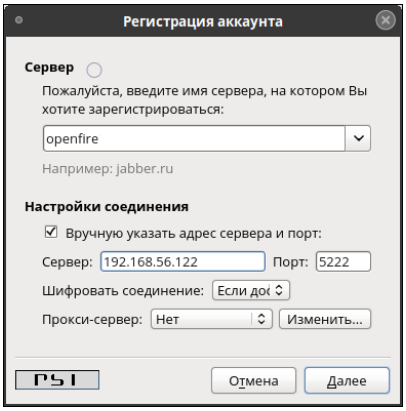
PSI очень удобен, благодаря полной поддержке *Unicode* и локализации, простой передаче файлов, настраиваемым наборам иконок и многим другим полезным функциям.

Для установки выполните команду:

```
dnf install psi
```

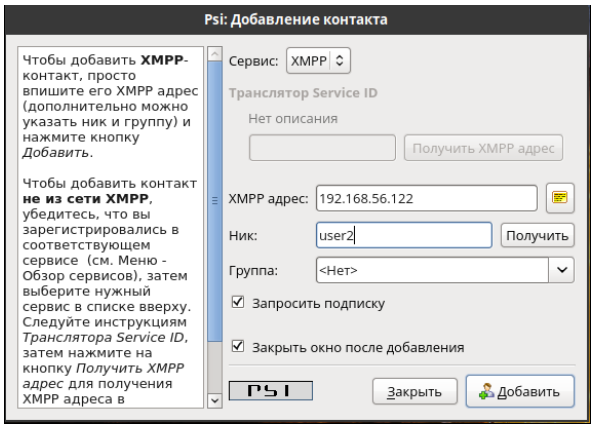
Запуск *psi* осуществляется через *«Меню» - «Интернет» - «Psi»*.

После запуска вам будет предложено создать нового пользователя — для этого введите имя пользователя и нажмите «*Добавить*». После чего откроется окно регистрации аккаунта. В поле «*Сервер*» введите имя сервера, установите галочку в поле «*Вручную указать адрес сервера и порт*», впишите ip-адрес сервера и нажмите «*Далее*».



После этого нажмите кнопку «*Доверять*» и впишите имя нового пользователя, не созданного на сервере, и пароль. Внизу нажмите на кнопку выбора статуса и установите параметр «*Доступен*», после чего учетная запись подключится к серверу.

Для добавления контактов в окне *Psi* в левом нижнем углу нажмите на значок **PSI** и выберите «*Добавить контакт*». В поле «*XMPP-адрес*» вводим ip-адрес сервера, а в графе «*Ник*» – никнейм нужного человека.



В окне *Psi* появится контакт.

Jitsi

Jitsi - это система интернет-телефонии и мгновенного обмена сообщениями, поддерживающая XMPP. Написана на *Java*.

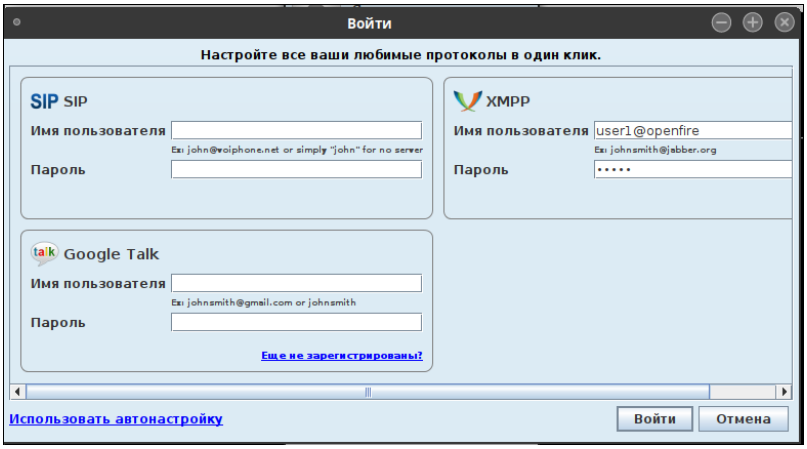
Программа также позволяет совершать видео-звонки и обеспечивает передачу файлов.

Для установки выполните команду:

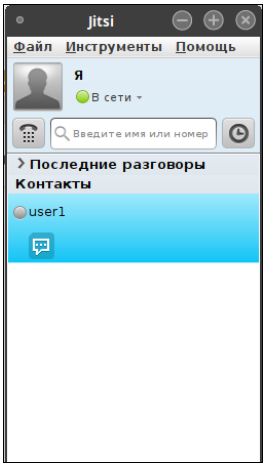
```
dnf install jitsi
```

Запуск *Jitsi* осуществляется через *«Меню» - «Интернет» - «Jitsi»*.

После запуска откроется окно с выбором протокола. В протоколе XMPP заполните поля «*Имя пользователя*» и «*Пароль*» и нажмите «*Войти*».



После этого откроется окно программы и список пользователей, зарегистрированных на одном сервере.



Linphone

Установка
Первый запуск и создание аккаунта
Дополнительные настройки linphone

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: linphone-2:4.3.2-1

Linphone – кроссплатформенный программный клиент IP-телефонии в стандарте **SIP** с открытым исходным кодом. Программа **linphone** предназначена для организации аудио и видео-вызовов, а также обмена текстовыми сообщениями.

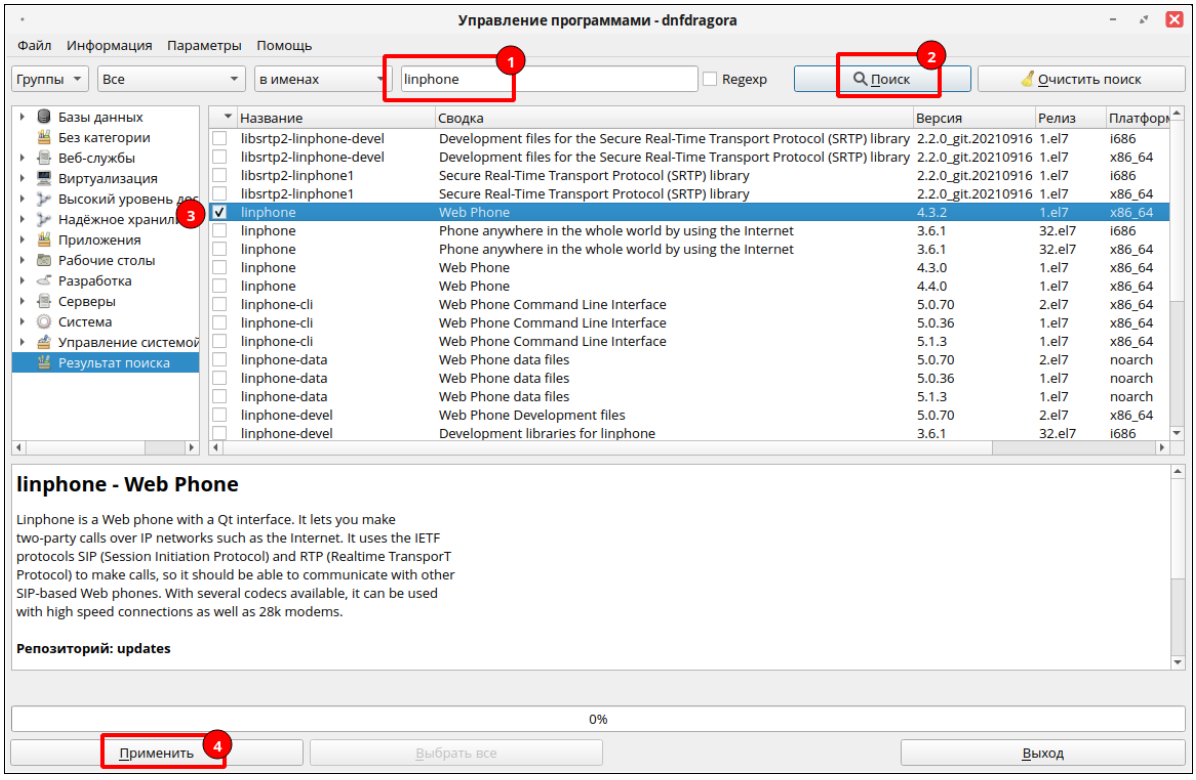
Возможности **Linphone**:

- аудио- и видеозвонки в фомате HD;
- аудиоконференции;
- переадресация вызовов;
- запись разговоров;
- адресная книга;
- поддержка IP-адресов;
- обмен смс-сообщениями;
- история вызовов;
- шифрование связи.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**linphone**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

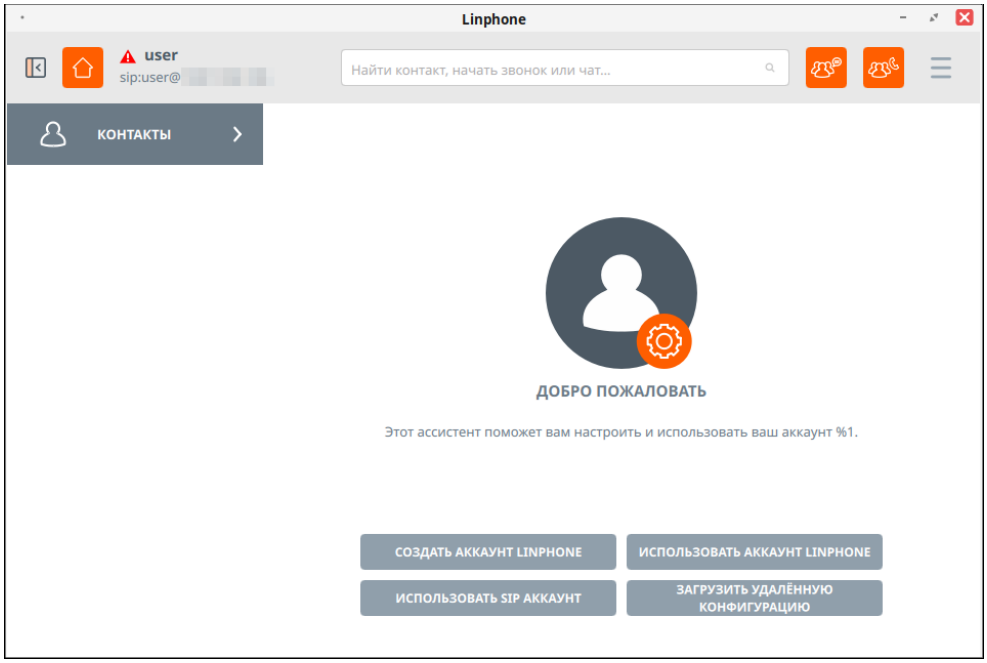
```
dnf install linphone
```

Дальнейшая работа в программе выполняется от локального пользователя.

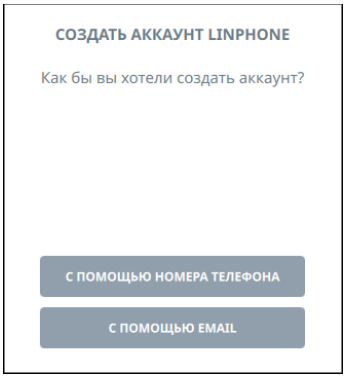
После установки программа будет доступна из «**Главного меню**» - «**Интернет**» - «**Linphone**».

Первый запуск и создание аккаунта

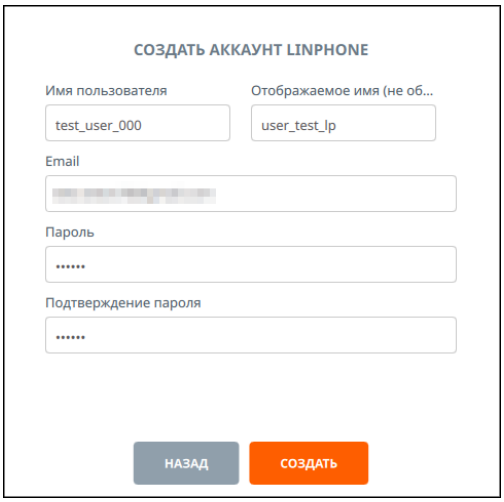
При первом запуске программы будет предложено выбрать способ авторизации.



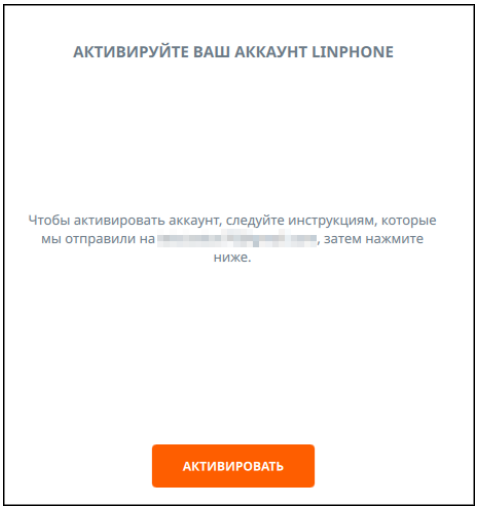
В примере рассмотрен вариант создания нового аккаунта. Нажмите кнопку «**Создать аккаунт Linphone**» и выберите предпочитаемый вариант регистрации – по *номеру телефона* или по *email* (в примере рассмотрен вариант регистрации по **email**).

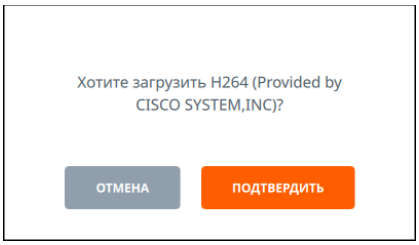


Далее будет открыта форма регистрации, в которой необходимо указать имя пользователя, никнейм (отображаемое имя), адрес электронной почты, а также задать пароль учетной записи. Нажмите «**Создать**».

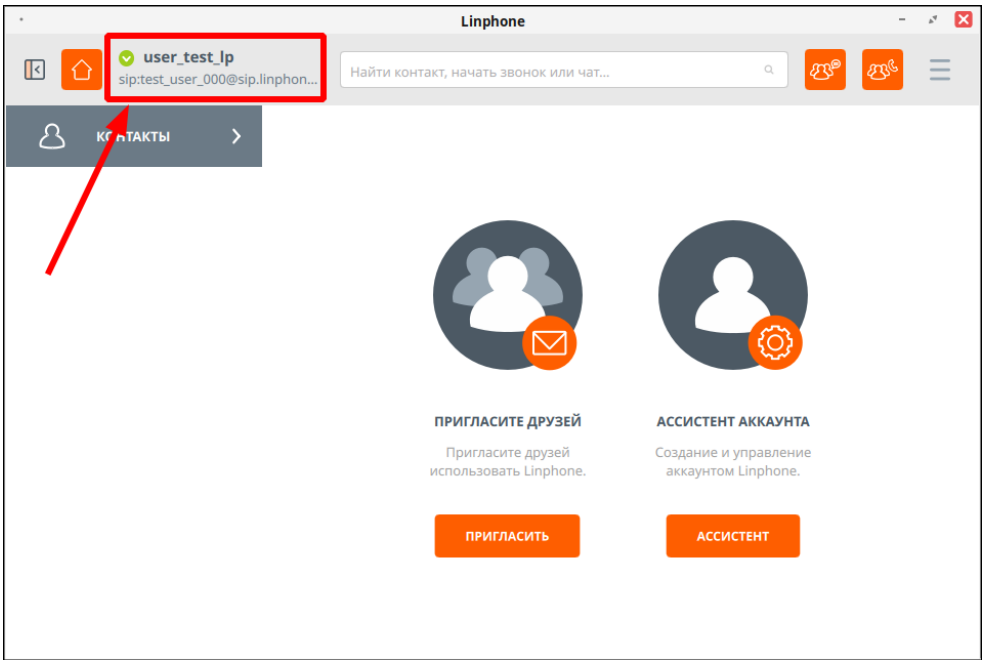


Затем необходимо активировать созданный аккаунт. Перейдите в сообщения электронной почты и следуйте подсказкам. После этого в окне **linphone** нажмите «**Активировать**», будет предложено загрузить дополнительный пакет, подтвердите загрузку.

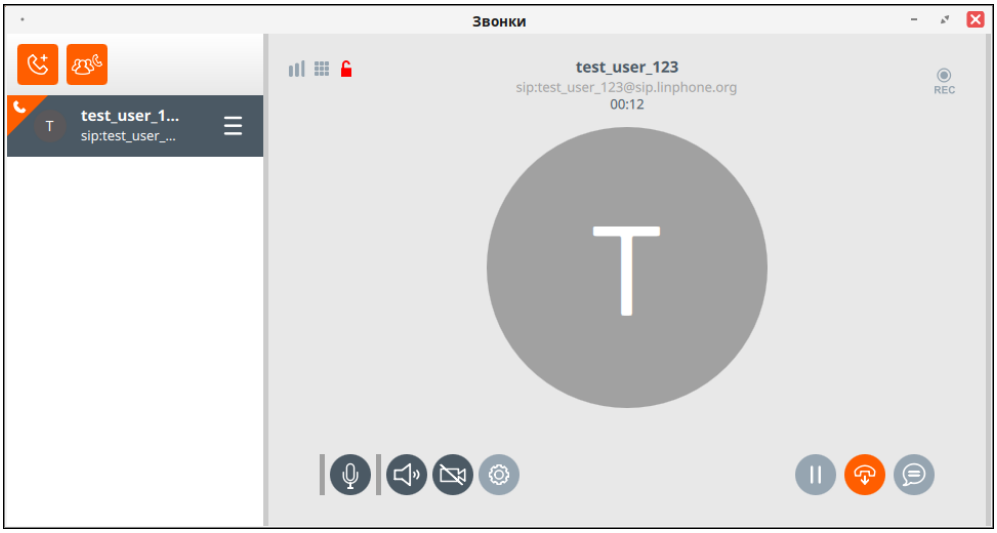




После активации аккаунта статус учетной записи будет изменен на «**Доступен**».

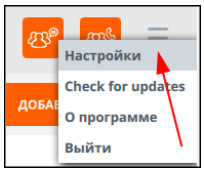


Для проверки работоспособности можно найти контакт по имени или номеру телефона и позвонить ему по аудио- или видеосвязи.

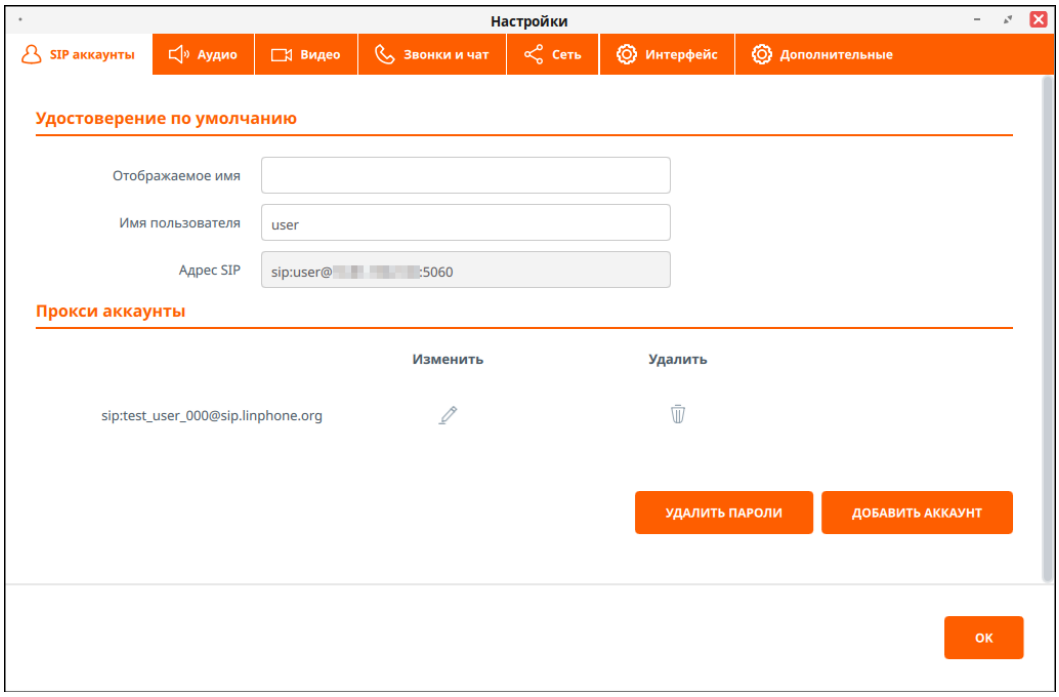


Дополнительные настройки linphone

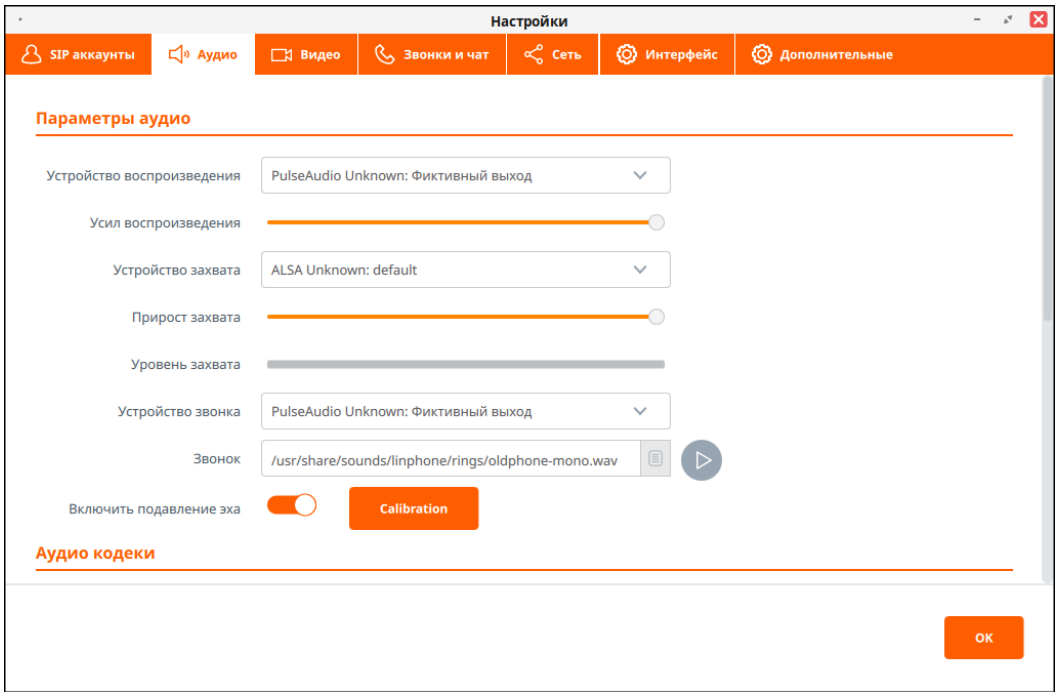
Для тонкой настройки каких-либо параметров выберите пункт меню **Настройки**.



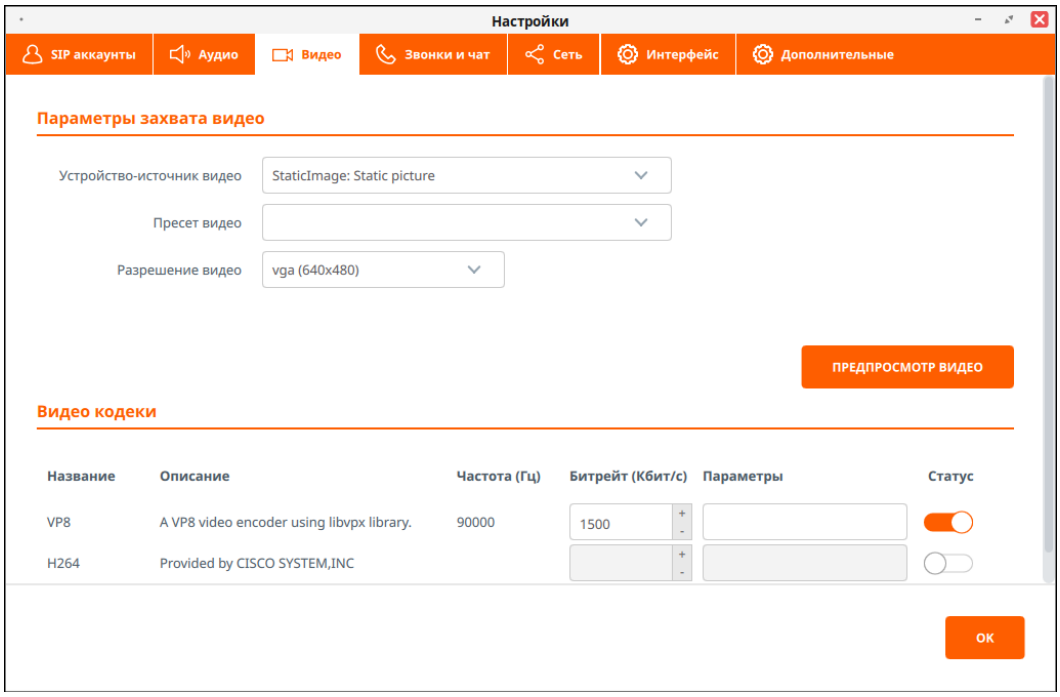
На вкладке «**SIP аккаунты**» можно изменять никнейм и имя пользователя, а также просматривать список аккаунтов.



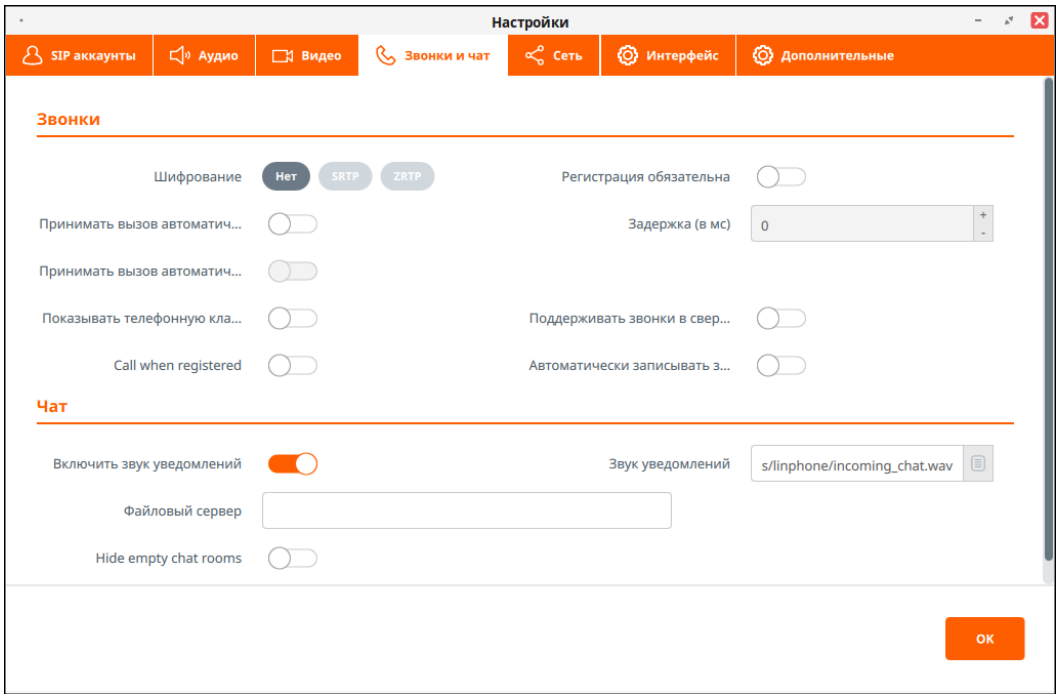
На вкладке «**Аудио**» настраиваются параметры аудио, такие как устройства воспроизведения, усиление воспроизведения, устройства захвата, уровень захвата, подавление эха, а также параметры аудиокодеков.



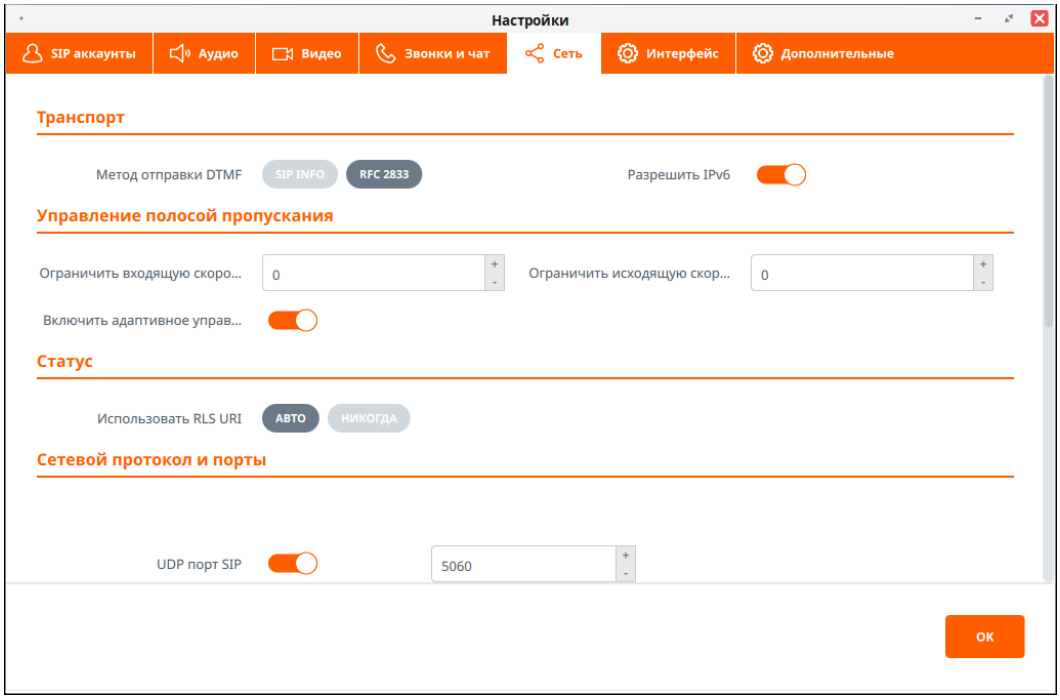
На вкладке «**Видео**» задаются параметры захвата видео и видеокодеки.



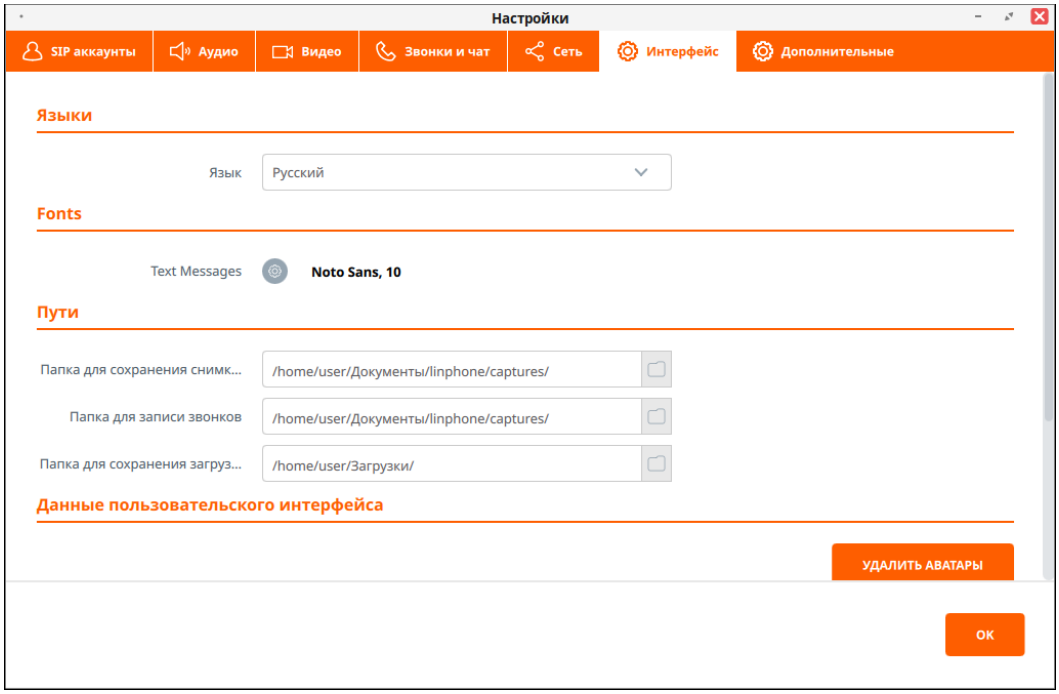
На вкладке «**Звонки и чат**» настраиваются уведомления, звуки уведомлений, шифрование звонков, прием вызовов, а также автоматическая запись звонков.



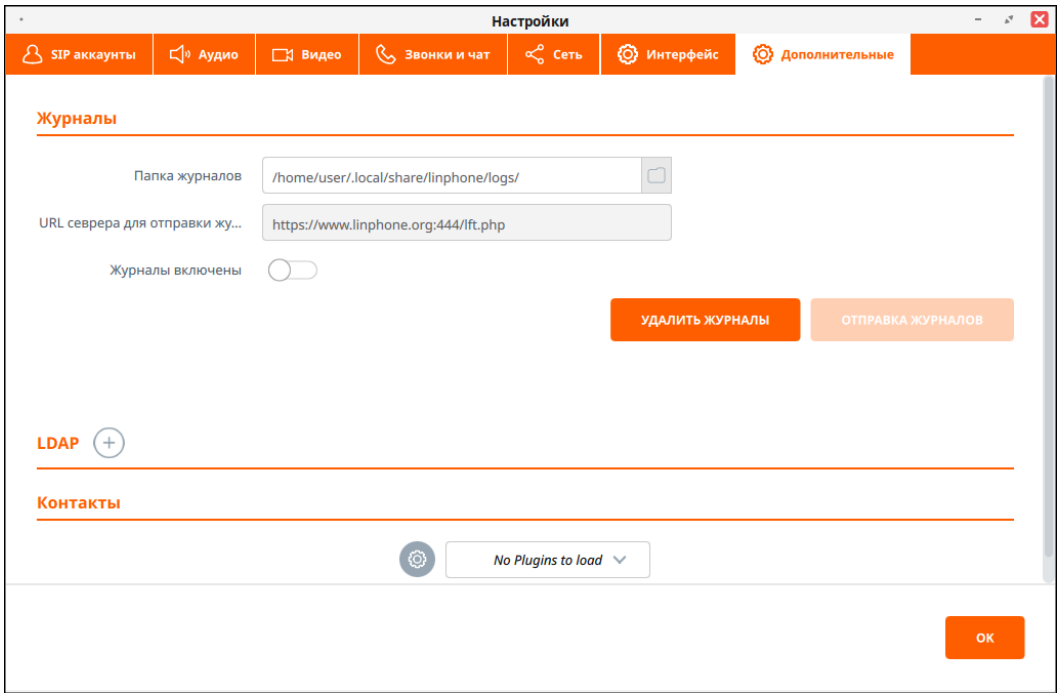
На вкладке «**Сеть**» доступна настройка используемого протокола сети, ограничение входящей и исходящей пропускной способности, безопасность сети и пр.



На вкладке «**Интерфейс**» устанавливается язык интерфейса, шрифт текстовых сообщений, каталоги хранения снимков, записей звонков и прочих загрузок.



На вкладке «**Дополнительные**» доступны настройки журналов, LDAP и контактов.


Настройки
SIP аккаунты
Аудио
Видео
Звонки и чат
Сеть
Интерфейс
Дополнительные
Журналы
Папка журналов
/home/user/.local/share/linphone/logs/
URL севрера для отправки жу...
https://www.linphone.org:444/lft.php
Журналы включены
УДАЛИТЬ ЖУРНАЛЫ
ОТПРАВКА ЖУРНАЛОВ
LDAP
Контакты
No Plugins to load
OK

Telegram

Установка Telegram
Запуск программы
Запуск программы в MATE
Запуск программы в KDE
Запуск программы в GNOME
Запуск через терминал
Авторизация в мессенджере
Настройка программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: telegram 4.14.12

Установка Telegram

Установить программу можно через терминал, либо через графический менеджер пакетов.
Для установки Telegram через терминал перейдите в сеанс пользователя root:

```
su -
```

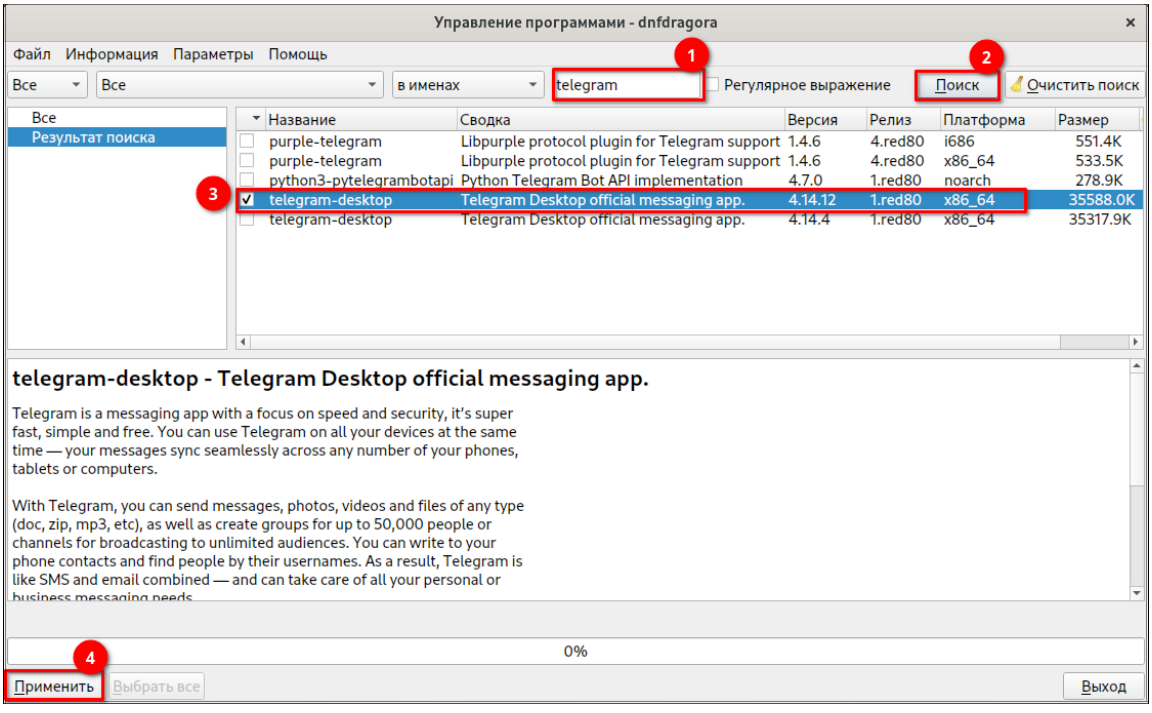
Выполните команду для установки:

```
dnf install telegram-desktop
```

Завершите сеанс пользователя root:

```
exit
```

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», в строку поиска введите ключевое слово «**telegram**» (1), выполните поиск (2) и отметьте флагом пакет последней версии (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.

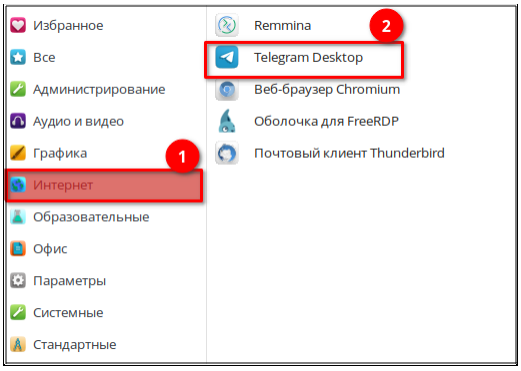


После установки запуск программы доступен из меню или через терминал.

Запуск программы

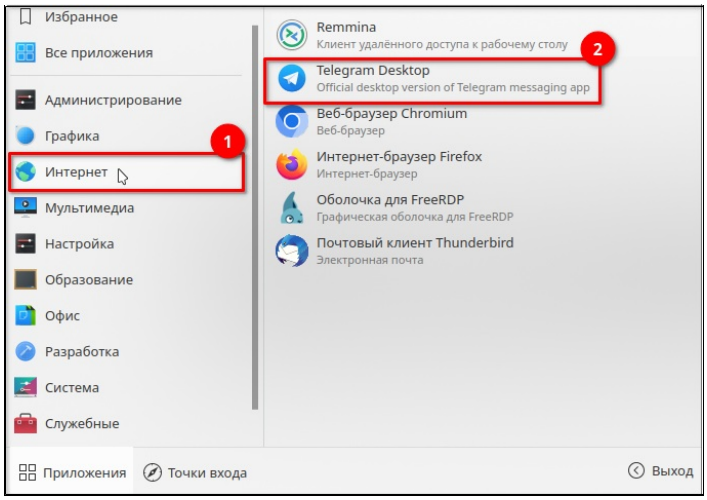
Запуск программы в MATE

Если вы используете графическую оболочку **MATE** запуск мессенджера доступен из «**Главного меню**» - «**Интернет**» (1) - «**Telegram Desktop**» (2).



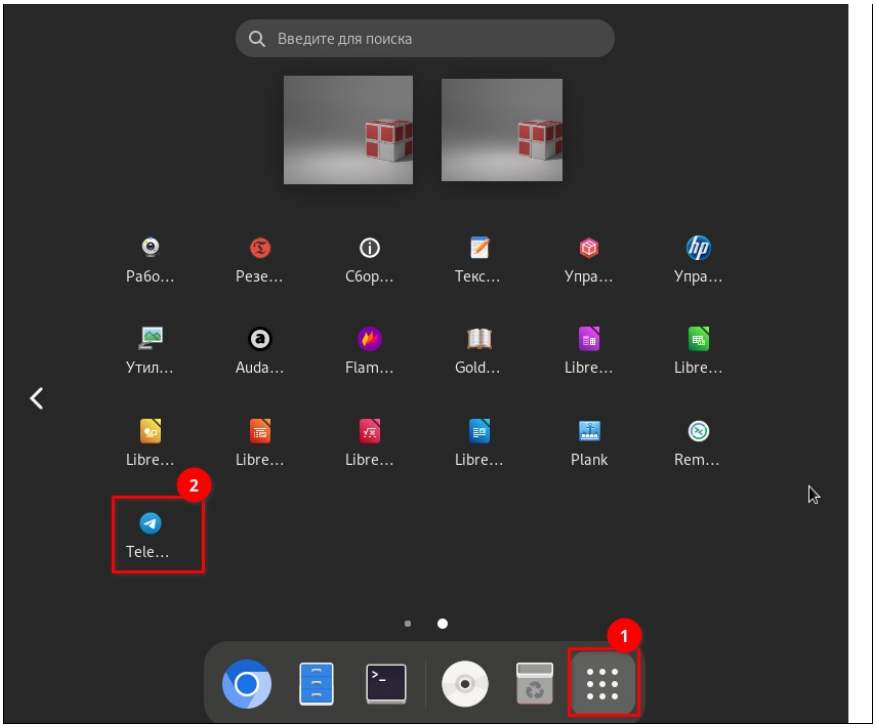
Запуск программы в KDE

Если вы используете графическую оболочку **KDE Plasma** запуск мессенджера доступен из «**Главного меню**» - «**Интернет**» (1) - «**Telegram Desktop**» (2).



Запуск программы в GNOME

Если вы используете графическую оболочку **GNOME** запуск мессенджера доступен из меню «**Показать приложения**» (1) - «**Telegram Desktop**» (2).



Запуск через терминал

Для запуска программы через терминал выполните:

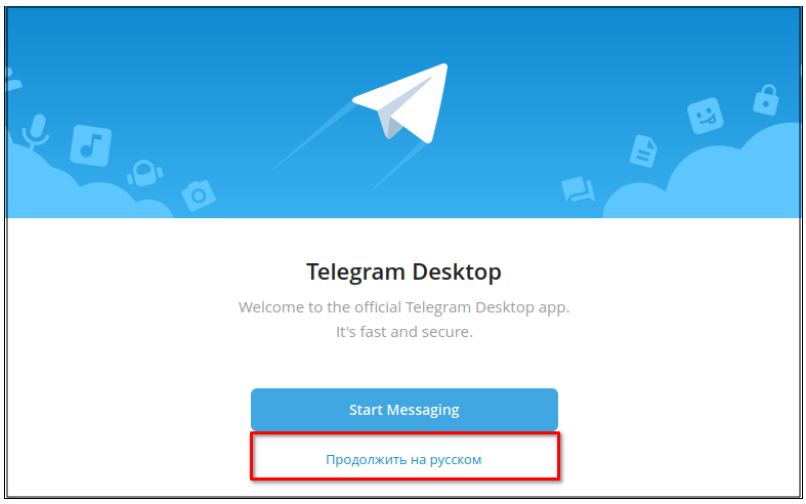
```
telegram-desktop
```

Авторизация в мессенджере

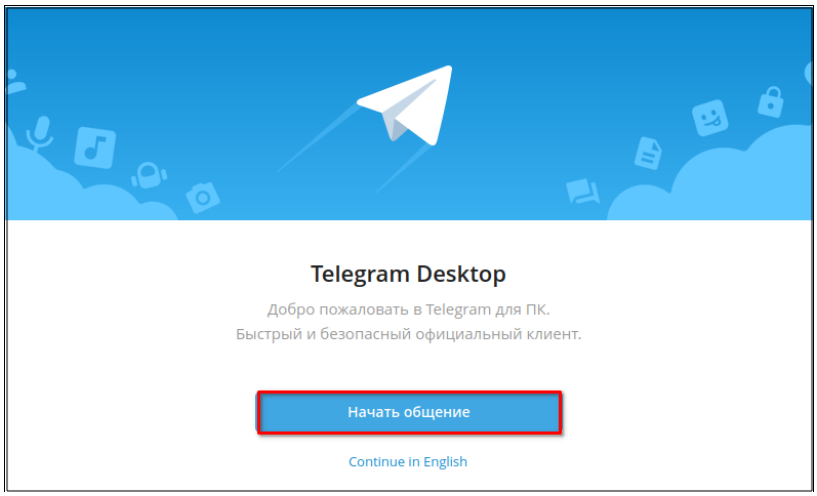
После запуска **Telegram** будет открыто диалоговое окно мессенджера.

По умолчанию в интерфейсе используется английский язык. Для перехода в интерфейс на английском языке нажмите «**Start Messaging**».

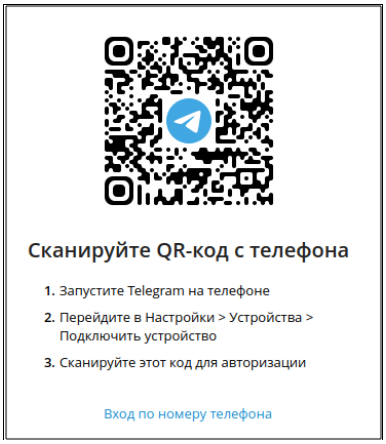
Для смены языка интерфейса на русский нажмите кнопку «**Продолжить на русском**».



Нажмите кнопку «**Начать общение**» для продолжения входа.



Вход в учетную запись может быть произведен через сканирование QR-кода или по номеру телефона.

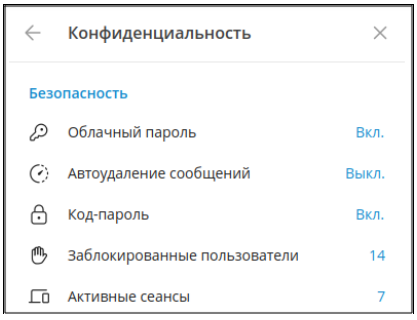


Настройка программы

Для защиты от мошенников рекомендуется установить сложный облачный пароль. Для этого перейдите в «**Настройки**» - «**Конфиденциальность**» - «**Облачный пароль**». Установите пароль.

Для предотвращения несанкционированного доступа к мессенджеру рекомендуется установить код-пароль. Для этого перейдите в «**Настройки**» - «**Конфиденциальность**» - «**Код-пароль**». Установите пароль. Дополнительно можно задать автоматическую блокировку мессенджера при неактивности определенное количество времени (1 минуту, 5 минут, 1 час, 5 часов или самостоятельно заданный промежуток времени). При необходимости код-пароль можно изменить или отключить.

В параметрах конфиденциальности доступна настройка видимости номера телефона, времени входа, фотографии профиля и прочие данные.



Gajim

Установка и запуск
Добавление учётной записи
О программе
Установка модулей
Добавление контакта в Gajim

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: gajim-1.7.3

Gajim представляет собой бесплатный мессенджер с открытым исходным кодом, совместимый с различными операционными системами и реализующий поддержку протокола Jabber. Разработанный на Python и использующий графический интерфейс GTK+, **Gajim** обладает широким спектром функций.

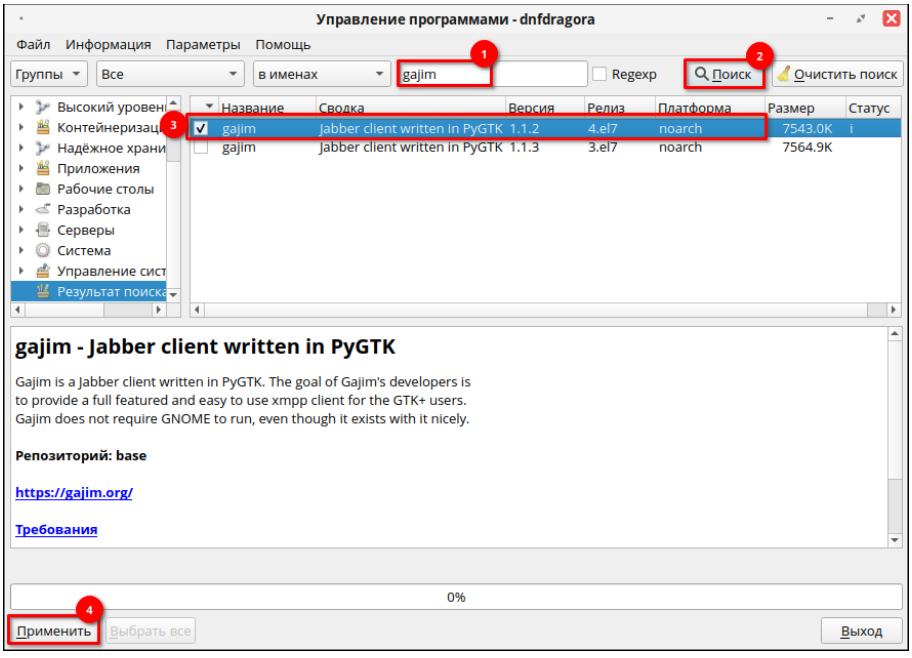
Основные возможности **Gajim**:

- поддержка многих языков, включая русский;
- смайлики, аватары, сообщения о статусе, поддержка расширенных статусов;
- вкладки в окне беседы, возможность объединить окно списка контактов (ростера) с окном беседы;
- поддержка метаконтактов;
- поддержка конференций (с протоколом MUC), приглашений, преобразования чата в конференцию, сокрытие конференций в ростере;
- закладки для комнат;
- поддержка транспортов;
- передача файлов;
- командная строка;
- шифрование паролей;
- генератор RST;
- OpenPGP-шифрование;
- URL-граббер, проверка орфографии, поддержка разметки текста reStructuredText.

Установка и запуск

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**gajim**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install gajim
```

Для запуска программы через терминал введите команду:

```
gajim
```

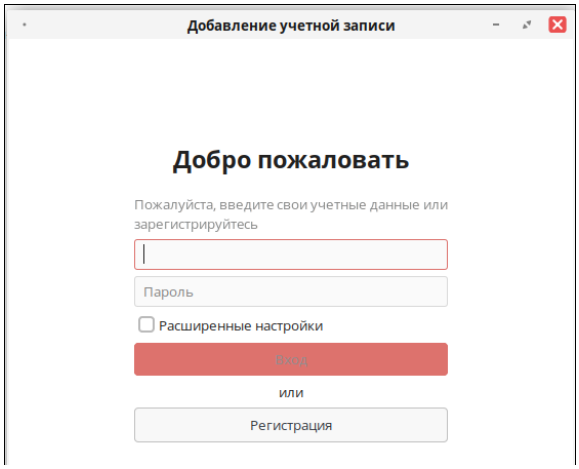
После установки программа будет доступна из «**Главного меню**» — «**Интернет**» — «**Gajim**».

Когда программа запущена, в системном трее отображается значок  .

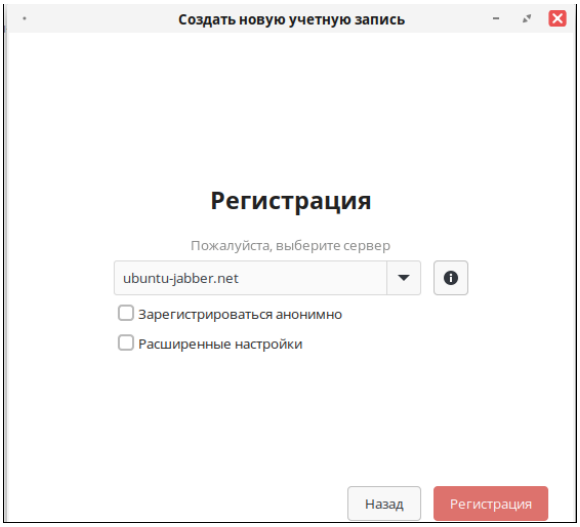
Добавление учётной записи

При первом запуске **Gajim** будет выведено диалоговое окно добавления учётной записи, предлагающее ввести свои учётные данные или зарегистрироваться.

Если учётной записи нет или необходимо создать новую нажмите кнопку «**Регистрация**».



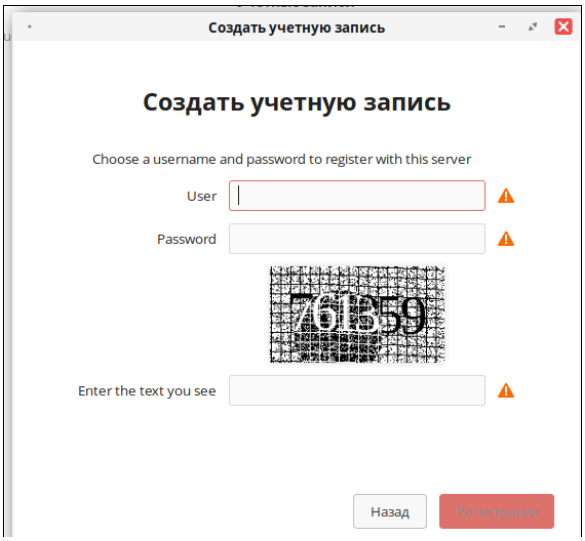
Выберите сервер, параметры и нажмите кнопку «**Регистрация**».



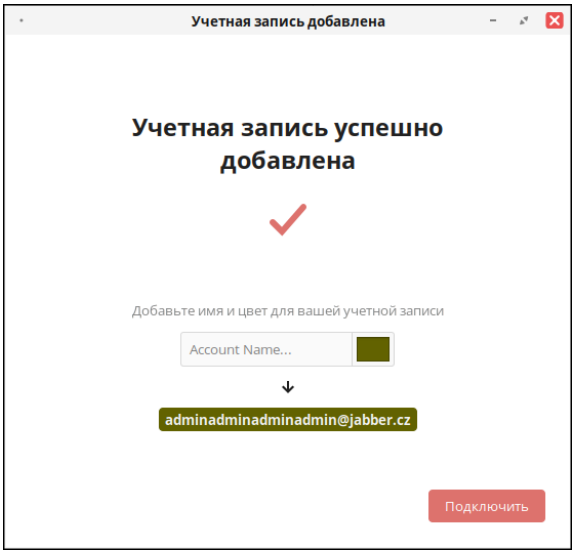
После выбора сервера в **Gajim** и нажатия кнопки «**Регистрация**», начинается процесс подключения к серверу.

После инициализации процесса подключения **Gajim** выполнит проверку доступности сервера. В течение нескольких секунд по завершении проверки, будет отображено диалоговое окно, в котором пользователю будет предложено ввести свои учётные данные для аутентификации в системе.

Для регистрации нового пользователя необходимо ввести логин, пароль и выполнить проверку капчи. Рекомендуется придерживаться использования английских букв, цифр, символов подчёркивания, тире и точки при создании логина. После заполнения данных следует нажать кнопку «**Регистрация**». В случае, если выбранное имя пользователя уже зарегистрировано на сервере, система выведет сообщение об ошибке. Тогда потребуется вернуться к предыдущему шагу и выбрать альтернативное имя пользователя.



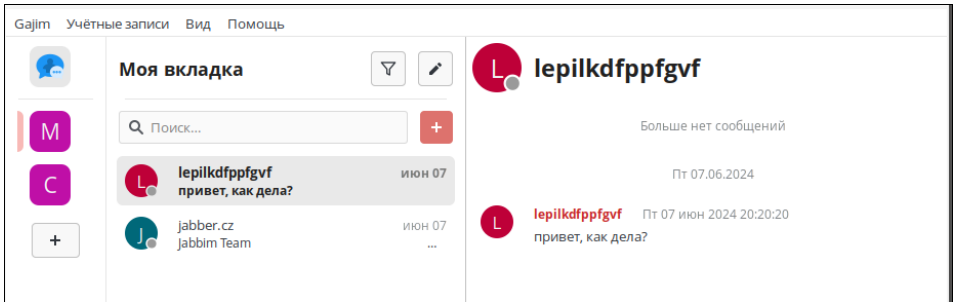
По завершении процесса регистрации на экране появится уведомление, подтверждающее успешное создание учётной записи.



После завершения процесса регистрации пользователь может сообщить свой JID другим лицам для добавления в список контактов. Программа **Gajim** автоматически начнёт процедуру подключения к сети. Перед инициализацией подключения **Gajim** запросит пароль от учётной записи для подтверждения идентичности пользователя. В случае успешного ввода пароля и подключения к сети, в главном окне программы отобразится приветственное сообщение.

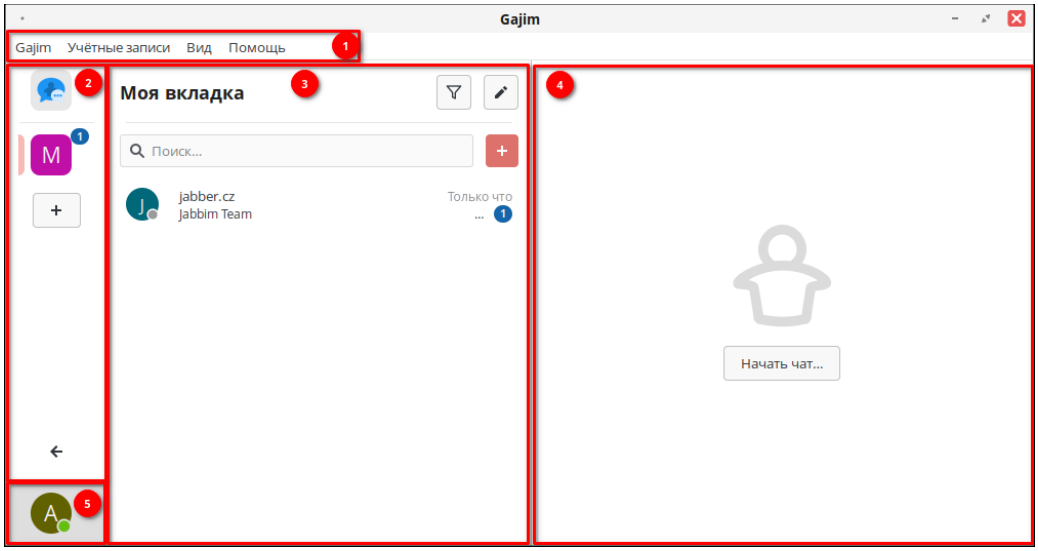


Если процедура регистрации и подключения к сети была выполнена корректно, окно чата Gajim будет выглядеть следующим образом:



О программе

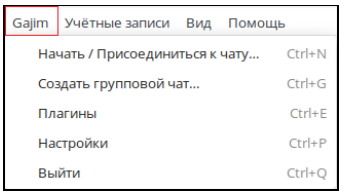
Главное окно программы **Gajim** содержит следующие элементы:



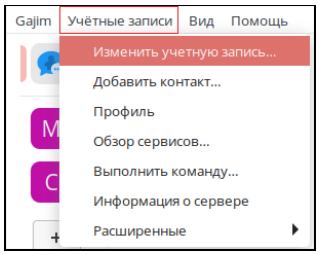
1. **Основное меню** — представляет собой выпадающий список, где доступны все действия для работы и настройки программы.
2. **Область настроек** — осуществляет навигацию по вкладкам и добавляет вкладки.
3. **Список контактов** (**ростер**) — позволяет просматривать и управлять контактами, создавать группы контактов и просматривать их статус.
4. **Поле чата** — отображает текущие чаты.
5. **Поле статуса** — отображает учётную запись и текущее состояние подключения.

В основном меню представлен доступ к основным функциям программы.

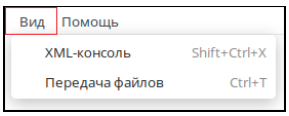
Меню «**Gajim**» отвечает за настройку различных параметров мессенджера и позволяет подключать плагины.



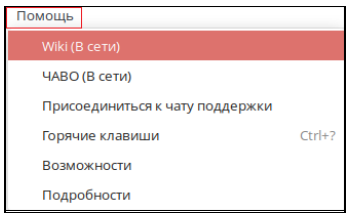
Меню **«Учётные записи»** в Gajim отвечает за настройку учётных записей и параметров соединения с серверами XMPP. Здесь можно добавлять, удалять и редактировать учётные записи, а также настраивать параметры подключения, добавлять контакты и менять настройки профиля.



Меню **«Вид»** в Gajim отвечает за XML-консоль и передачу файлов.



Меню «**Помощь**» в Gajim отвечает за доступ к справочной информации и документации по программе. В этом меню можно найти информацию о различных функциях и настройках Gajim, а также ссылки на официальные ресурсы и форумы для получения дополнительной помощи и поддержки.

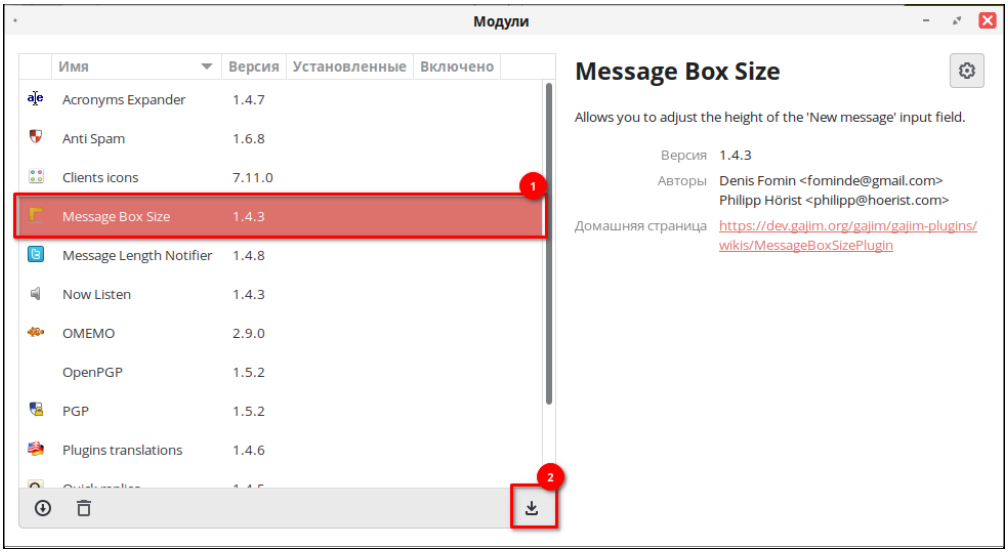


Установка модулей

Для расширения функционала программы можно установить модули. Для установки дополнительных модулей перейдите в меню «**Gajim**» — «**Плагины**».

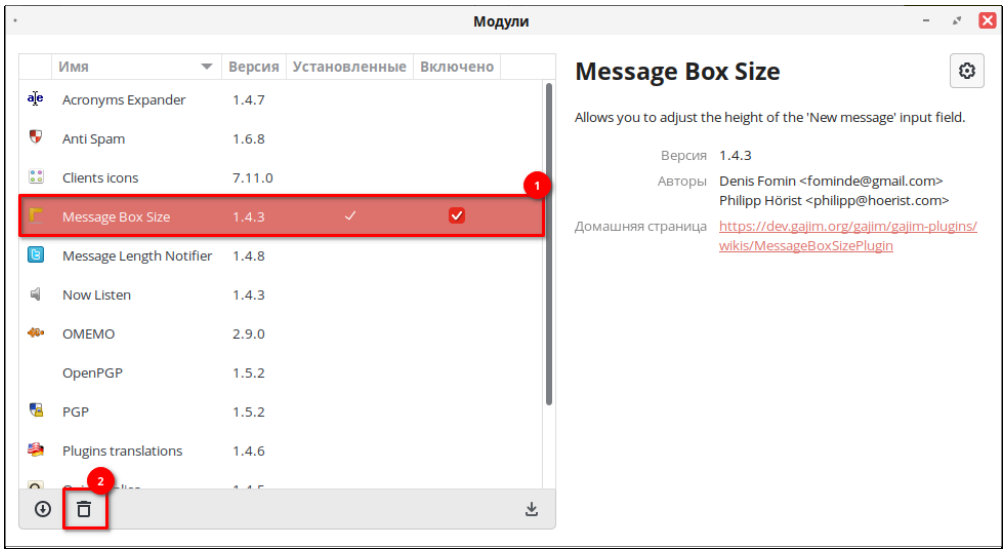
Для установки новых модулей выполните следующие шаги:

1. Выберите из списка модуль, который хотите установить.
2. Нажмите на кнопку загрузки модуля.



Для удаления модуля выполните следующий алгоритм действий:

1. Выберите из списка модуль, который хотите удалить.
2. Нажмите на кнопку «**Удалить плагин**».



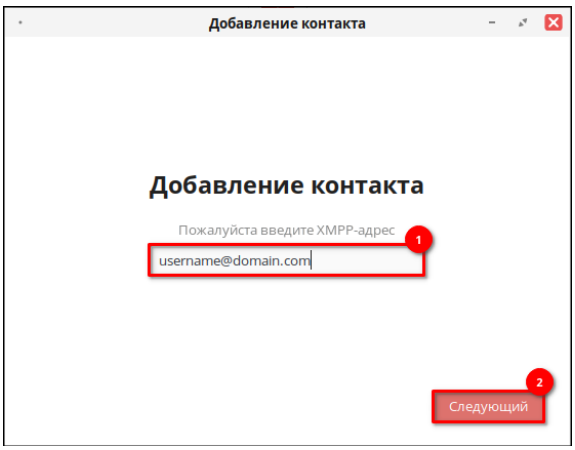
Модули в **Gajim** добавляют дополнительные функциональные возможности. Далее приведён список наиболее популярных из доступных плагинов:

1. **Acronyms Expander** — автоматически расшифровывает аббревиатуры и акронимы в сообщениях.
2. **Anti Spam** — предназначен для борьбы со спамом, позволяет блокировать сообщения от неизвестных контактов или содержащие определённые слова или фразы.
3. **Clients icons** — отображает значки клиентов в реестре и групповых чатах.
4. **Message Box Size** — позволяет настраивать размер окна ввода сообщений, делая его больше или меньше в зависимости от ваших предпочтений.

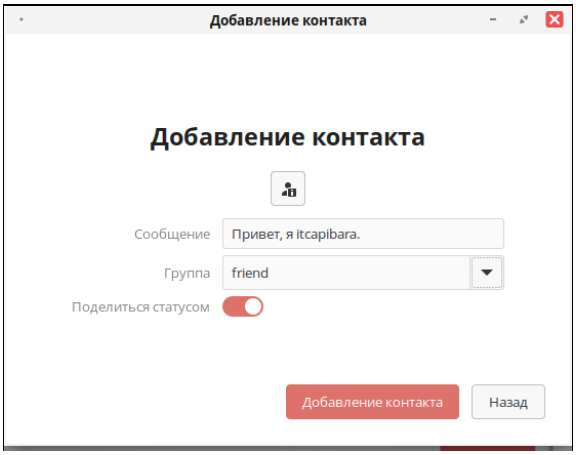
5. **Now Listen** — может отображать информацию о музыке, которую вы слушаете, в вашем статусе, позволяя вашим контактам видеть, что играет у вас в данный момент.
6. **Quick replies** — предоставляет возможность быстро отвечать на сообщения, используя заранее настроенные короткие ответы.
7. **Regex Filter** — использует регулярные выражения для фильтрации входящих сообщений, позволяя блокировать или пропускать сообщения на основе сложных правил, заданных пользователем.
8. **Triggers** — позволяет настроить автоматические действия (триггеры) в ответ на различные события в **Gajim**.

Добавление контакта в Gajim

Для добавления собеседников в **Gajim** перейдите в меню «**Учётные записи**» — «**Добавить контакт...**». Появится окно, в котором нужно ввести XMPP-адрес (JID), обычно состоит из имени пользователя и домена, разделённых символом «**@**». После заполнения JID нажмите «**Следующий**».



Напишите текст сообщения для собеседника и определите группу для контакта. После заполнения данных нажмите «**Добавление контакта**».



В контактном списке появится добавленный контакт (). Собеседнику придёт запрос на подписку. Когда он примет его, значок контакта сменится ().

Skype

Предварительная подготовка
Установка skype

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: skype-8.105.0.208

Предварительная подготовка

В качестве предварительной подготовки необходимо установить пакет **snap**, который является отдельной изолированной "программной средой" для работы того или иного приложения. Подробную информацию о **snap** и его установке в РЕД ОС см. в нашей статье «Snap - изолированная среда для запуска приложений».

Установка skype

После успешной установки **snap** можно перейти к непосредственной установке **skype**.

Для этого в терминале необходимо выполнить команду:

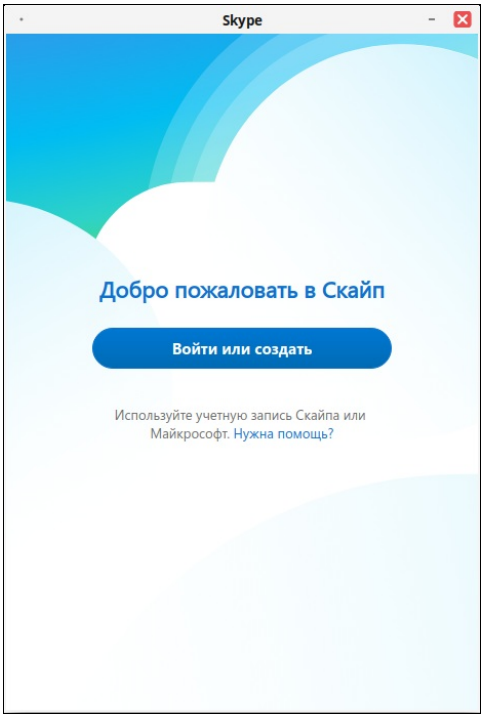
```
sudo snap install skype
```

Будет выполнена загрузка необходимых пакетов и установка **skype**.

Запуск программы доступен из «**Меню**» - «**Интернет**» - «**Skype**» или через терминал с помощью команды:

```
snap run skype
```

Для использования **Skype** необходимо войти под учетной записью *Skype* или *Microsoft* или зарегистрироваться.



Zoom

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zoom-6.2.3.2056-1

Сначала необходимо скачать **Zoom** с официального сайта, перейдя по ссылке.

Выберите тип Linux - **RedHat**, архитектура ОС - **64**-разрядная, версия - **8.0+**.

Для установки программы перейдите в сеанс **пользователя root**:

```
su -
```

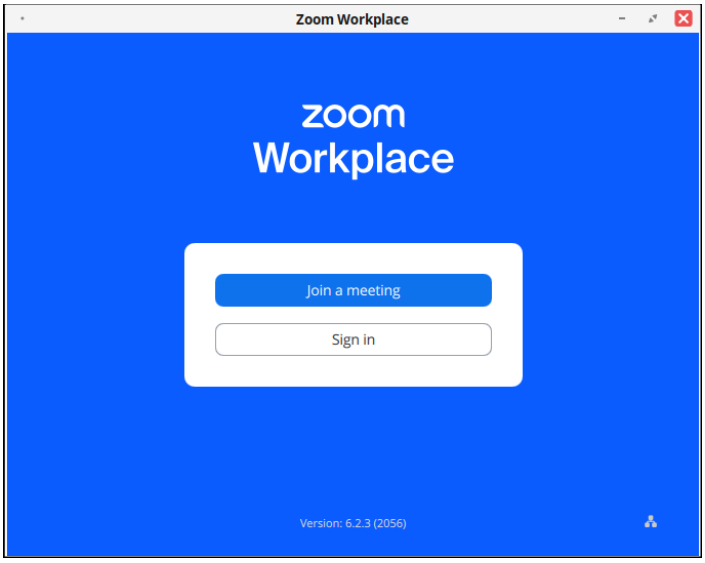
Перейдите в папку с загруженным файлом (в примере /home/user/Загрузки).

```
cd /home/user/Загрузки/
```

и выполните команду:

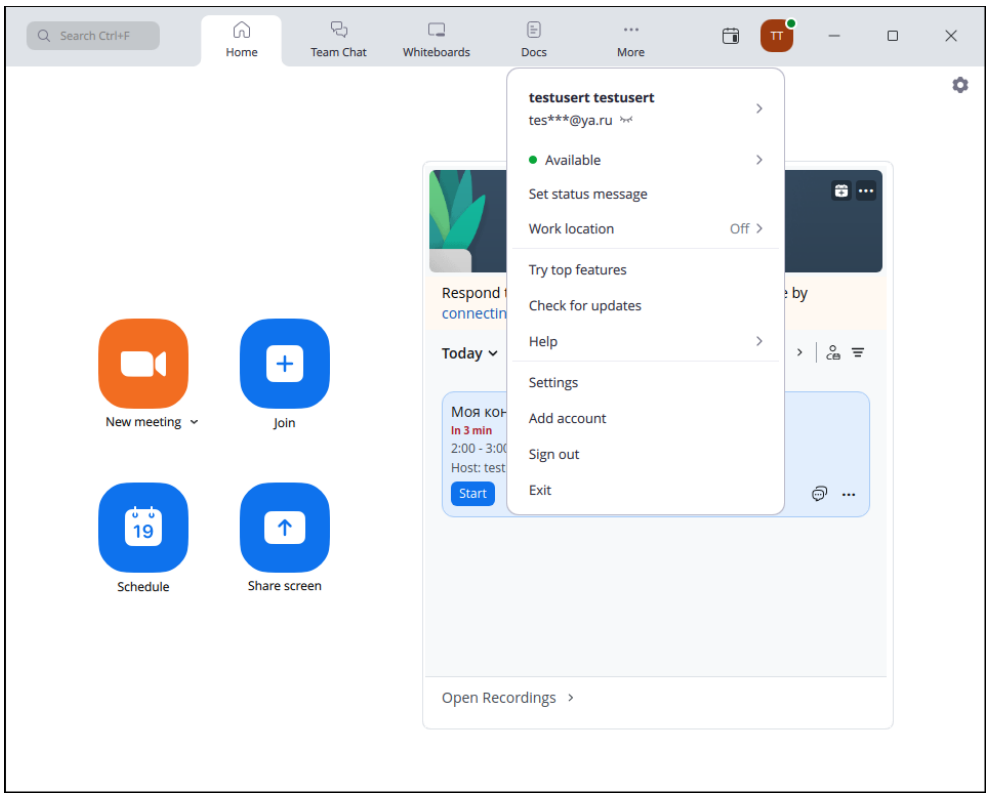
```
dnf install zoom_x86_64.rpm
```

После установки запуск программы доступен из «**Главного меню**» - «**Интернет**» - «**Zoom Workplace**».



После запуска программы будет предложено **Войти** или **Присоединиться к конференции**.

После ввода ваших данных приложение будет готово к использованию.



Для удаления программы **Zoom** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf remove zoom
```

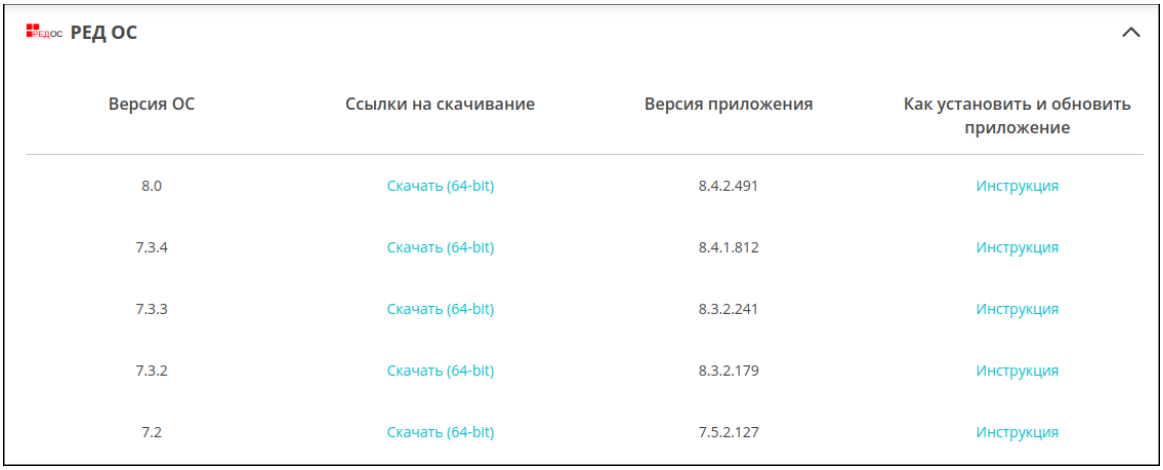
TrueConf

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: trueconf-8.4.2.491

TrueConf — российский аналог *Zoom*. Скачайте программу с официального сайта по ссылке.

Выберите используемую версию РЕД ОС и скачайте пакет.



РЕД ОС

Версия ОС	Ссылки на скачивание	Версия приложения	Как установить и обновить приложение
8.0	Скачать (64-bit)	8.4.2.491	Инструкция
7.3.4	Скачать (64-bit)	8.4.1.812	Инструкция
7.3.3	Скачать (64-bit)	8.3.2.241	Инструкция
7.3.2	Скачать (64-bit)	8.3.2.179	Инструкция
7.2	Скачать (64-bit)	7.5.2.127	Инструкция

Перейдите в сеанс пользователя **root**:

```
su -
```

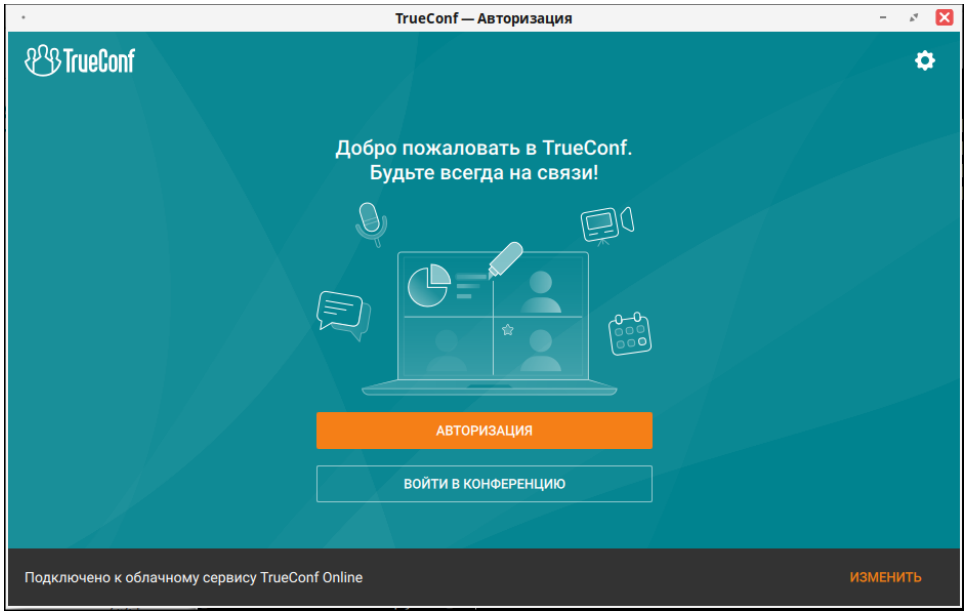
Перейдите в папку с загруженным файлом (в примере /home/user/Загрузки).

```
cd /home/user/Загрузки/
```

Выполните команду установки:

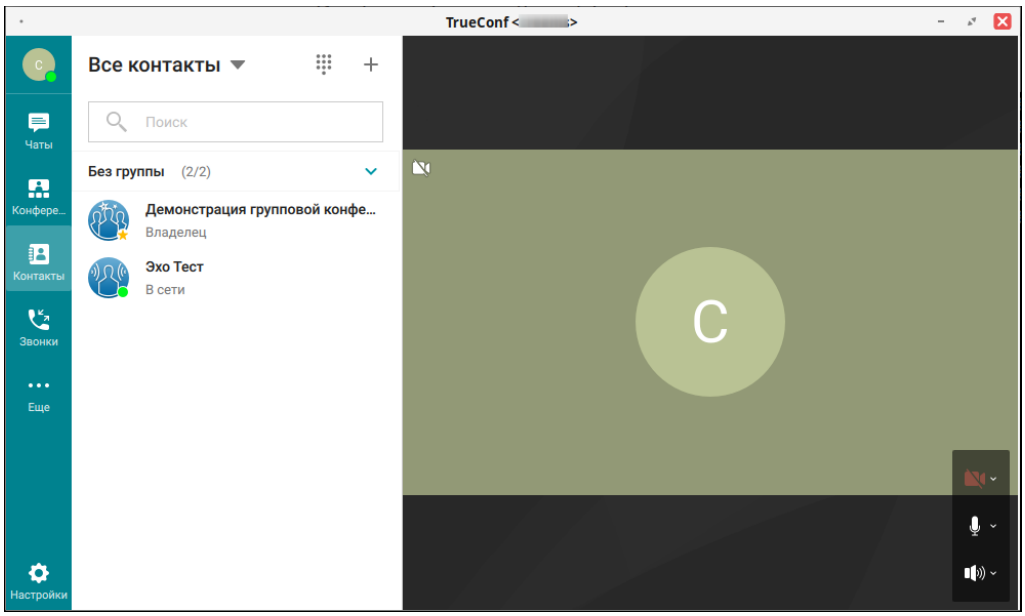
```
dnf install trueconf_client_redos80_x86_64.rpm
```

После установки запуск программы доступен из «**Главного меню**» — «**Интернет**» — «**TrueConf**».



После запуска программы будет предложено **Войти** или **Создать новый аккаунт**.

После ввода ваших данных приложение будет готово к использованию.



Для удаления программы **TrueConf** перейдите в сеанс пользователя **root:**

```
su -
```

и выполните команду:

```
dnf remove trueconf
```

Установка WINE

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки необходимо открыть терминал, войти под суперпользователем **root** и начать установку:

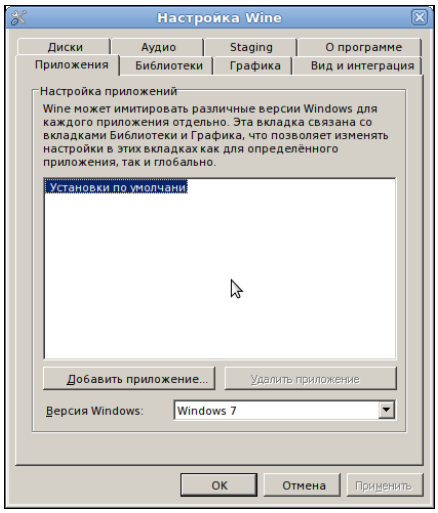
```
# dnf install wine
```

После установки запустите команду от имени обычного пользователя, чтобы увидеть конфигурацию *Wine*:

```
winecfg
```

Примечание.

При первом запуске команды **winecfg** создается префикс **.wine** 64-х разрядный по умолчанию.



Работа с программами в WINE

Установка программ в Wine
Запуск программы
Удаление программ в Wine

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка программ в Wine

Для легковесных программ достаточно команды:

```
wine filename.exe
```

Но чаще всего перед установкой программы в *wine* требуется настройка префикса.

Если при установке префикс не указывается, программа ставится в префикс по умолчанию.

Если установщик программы запускается файлом с расширением **.msi**, используем команду:

```
wine msiexec /i filename.msi
```

Установка в префикс не по умолчанию, например **.wine_prefix**, осуществляется следующим образом:

```
WINEPREFIX="/home/$USER/.wine_prefix" wine "/home/$USER/Downloads/filename.exe"
```

Запуск программы

Чтобы запустить программу, необходимо указать полный путь к исполняемой программе или имени программы, как показано в примере ниже:

```
wine /<путь_к_файлу>/program.exe
```

Первый запуск программы может длиться достаточно долгое время.

Запуск **bat**-файлов осуществляется командой:

```
wine start filename.bat
```

Удаление программ в Wine

Для удаления программ необходимо использовать команду:

```
wine uninstaller
```

или удаление из префикса:

```
WINEPREFIX="/home/$USER/.wine" wine uninstaller
```

После этого откроется окно «**Установка/удаление программ**», где следует выбрать нужную программу и нажать кнопку «**Удалить**».

При помощи **wine uninstaller** можно устанавливать программы, нажав на кнопку «**Установить**» и выбрав необходимую для установки программу.

Удаление программы без использования **GUI** осуществляется следующим образом:

```
wine uninstaller --remove <название_программы>
```

или из префикса:

```
WINEPREFIX="/home/$USER/.wine_prefix" wine uninstaller --remove <название_программы>
```

Также есть возможность удалить программу, используя ее собственную программу удаления:

```
wine /<путь_к_папке_с_программой>/uninstall.exe
```

Префиксы WINE

Настройка префикса
winefile - файловый менеджер Wine
Работа с реестром

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для разных программ могут потребоваться разные дополнительные компоненты, разные настройки *Wine* и т. п. Для этого существуют префиксы *Wine*. Используя для каждой программы свой префикс, вы можете обеспечить им индивидуальное окружение.

Для примера создадим и сконфигурируем 64-х разрядный префикс с именем **.wine_prefix** в домашнем каталоге пользователя:

```
WINEARCH=win64 WINEPREFIX="/home/$USER/.wine_prefix" winecfg
```

где **WINEARCH=win64** — указывает, что префикс создается под архитектуру **amd64**, что позволит запускать в нем 64-разрядные программы, а также 32-разрядные. Для создания 32-разрядного префикса необходимо заменить 64 на 32.

WINEPREFIX="/home/$USER/.wine_prefix" — указывает путь расположения создаваемого префикса.

> **Примечание.**
>
> Кавычки используются в случаях, если в имени папок содержится пробел, например **"/home/user/Рабочий стол"**.

winecfg — запускает программу конфигурирования префикса.

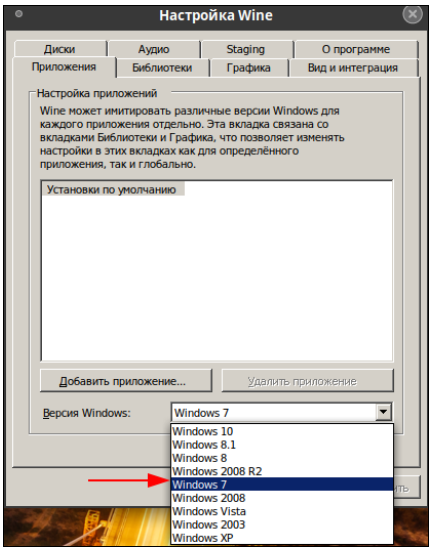
Для запуска программ с префиксом каждый раз указывать архитектуру не требуется, поэтому после создания параметр **WINEARCH=win64** прописывать не нужно.

Пример запуска программы *internet explorer* с префиксом:

```
WINEPREFIX=/home/$USER/.wine_prefix wine /home/$USER/.wine/drive_c/Program\ Files/Internet\ Explorer/iexplore.exe
```

Настройка префикса

Версия *Windows* позволяет выбирать режим запуска с необходимой версией Windows (Windows 7 - по умолчанию).



Вкладка «**Диски**» позволяет управлять виртуальными и физическими разделами. В стандартной конфигурации подключено 2 раздела: **C** и **Z**.

C — является системным каталогом префикса;

Z — ведет в корень файловой системы Linux, в некоторых случаях такое поведение нежелательно, поэтому данный диск рекомендуется удалить, тем самым изолировав префикс от основной системы.

> **Примечание.**
>
> Вредоносные программы для Windows потенциально способны нанести вред Linux-системе.

Вкладка «**Вид и интеграция**» дает возможность выбора ассоциаций каталогов Windows-пользователя с домашними каталогами Linux-пользователя. Данная возможность располагается в блоке «**Папки**» в нижней половине окна.

В префиксе стандартные каталоги Windows-пользователя располагаются по пути **/home/user/.wine_prefix/drive_c/users/$USER/**.

Ссылки в данном случае указывают на домашние каталоги Linux-пользователя, который создал префикс.

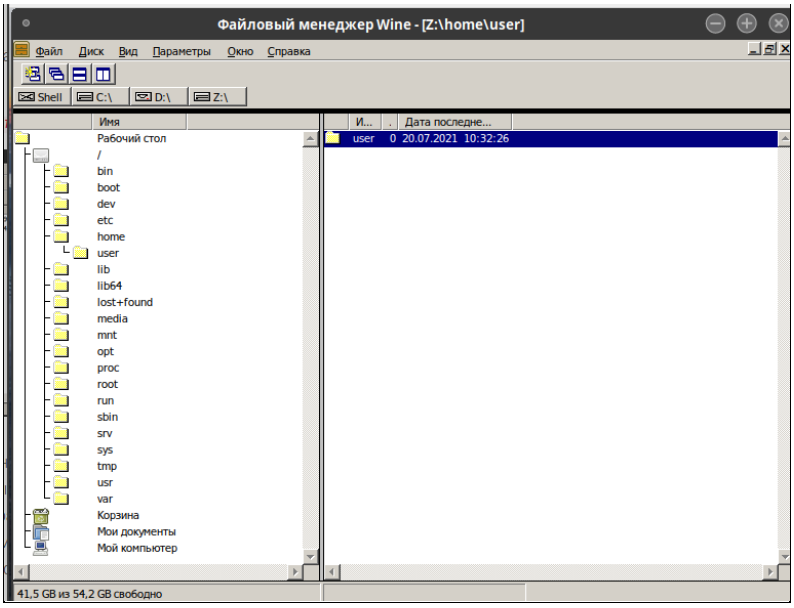
Остальные вкладки подробно описаны и интуитивно понятны.

winefile - файловый менеджер Wine

Winefile является аналогом проводника *Windows*.

Запуск **winefile** осуществляется командой:

```
WINEPREFIX="/home/$USER/.wine_prefix" wine winefile
```



Работа с реестром

Для открытия реестра используется инструмент **regedit**:

```
wine regedit
```

Чтобы перемещаться по реестру, кликните на ключах в левой части панели, чтобы перейти на следующий уровень глубины.

Чтобы удалить ключ, кликните на нем и в меню **Edit** выберите «**Delete**».

Чтобы добавить ключ или значение, определите место, где вы хотите поместить его, и выберите «**New**» из меню «**Edit**».

Чтобы изменить существующий ключ, выделите его в правой панели и выберите «**Modify**» из меню «**Edit**». Другой способ проделать то же самое, это щелчок правой кнопкой мыши на ключе или значении.

Файлы реестра располагаются в папке префикса, например:

```
/home/$USER/.wine_prefix/
```

- **system.reg** — содержит ветвь HKEY_LOCAL_MACHINE;
- **user.reg** — HKEY_CURRENT_USER;
- **userdef.reg** — HKEY_HKEY_USERS\.Default (содержит настройки Windows пользователя по умолчанию).

Установка winetricks

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Winetricks - вспомогательный скрипт для загрузки и установки различных распространяемых библиотек, необходимых для запуска некоторых программ в *Wine*, а также настройки окружения.

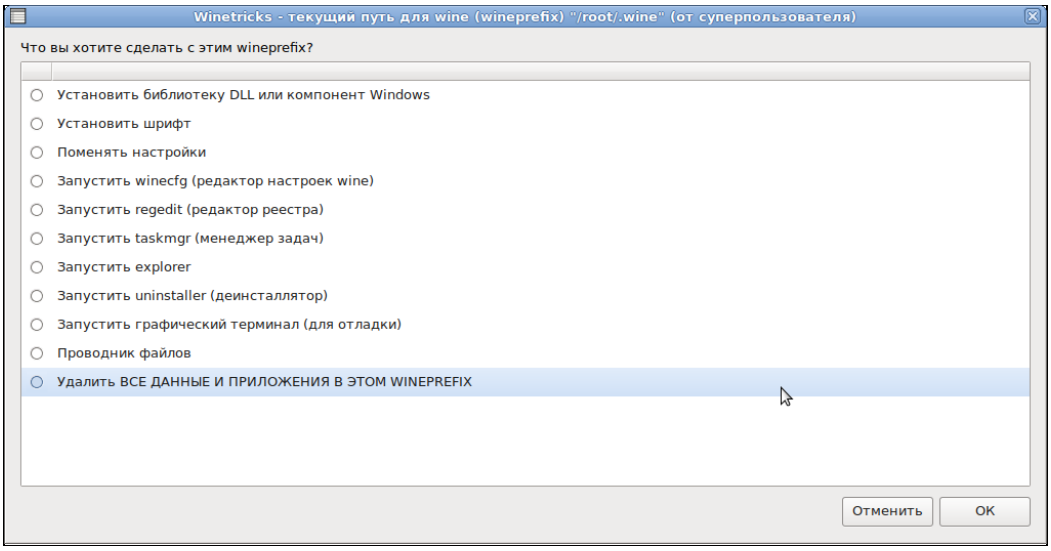
Для установки winetricks требуются права администратора:

```
# dnf install winetricks
```

Чтобы открыть диалоговое окно программы для работы в графическом режиме, необходимо вызвать команду:

```
winetricks
```

При выборе пункта меню, установленного по умолчанию, открывается следующее окно, которое содержит список доступных над wine-префиксом операций, где можно доустановить библиотеки, шрифты, вызвать редактор реестра или окошко настроек wine (**winecfg**).



Есть возможность установить пакеты напрямую через терминал:

```
winetricks <название_пакета>
```

Чтобы отобразить все установленные пакеты введите команду:

```
winetricks dlls list
```

Дополнительные возможности WINE

Пакет Dotnet
Пакет Mono
Установка Gecko
Виртуальный рабочий стол в Wine
Углубление в функционал Wine

Wine — свободное программное обеспечение, позволяющее пользователям ОС на базе ядра Linux исполнять 32- и 64- битные приложения созданные исключительно для *Microsoft Windows*. Название **W.I.N.E.** расшифровывается как «*Wine Is Not an Emulator*» — «W.I.N.E. — это не эмулятор». Имеется в виду, что *Wine* не является эмулятором компьютера или виртуальной машиной, как, например, qemu, VirtualBox и другие подобные им. *Wine* — это свободная реализация *Windows API*.

Вы можете подробнее ознакомиться с возможностями WINE в РЕД ОС, просмотрев наши обучающие видео:

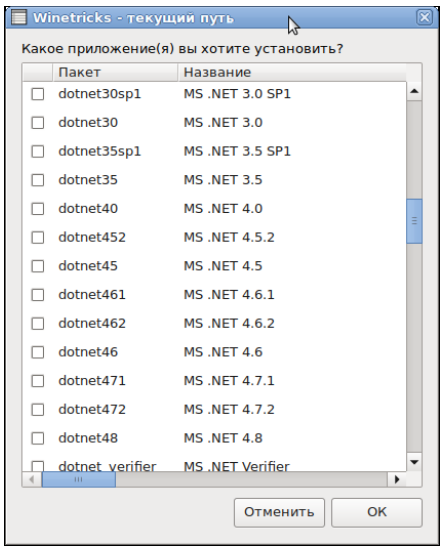
- на **RuTube** — Работа с WINE в РЕД ОС;
- в **Яндекс.Дзен** — Работа с WINE в РЕД ОС;
- в **VK Видео** — Работа с WINE в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

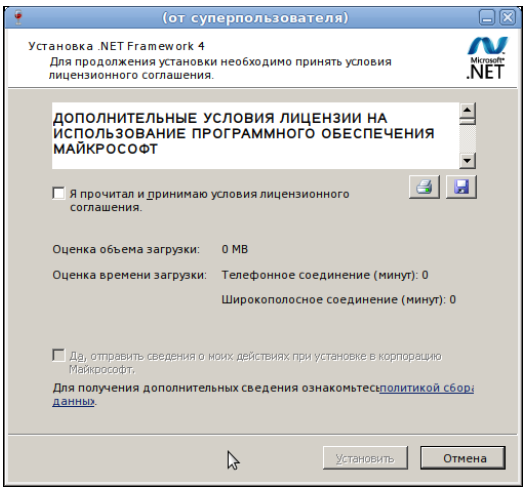
Пакет Dotnet

Для установки пакета в графическом режиме необходимо запустить **winetricks**.

При открытии окна выбрать пункт меню, установленный по умолчанию, затем необходимо выбрать пункт «**Установить библиотеку DLL или компонент Windows**». В списке приложений следует выбрать пакет для установки в зависимости от того, какая версия необходима, и нажать «**OK**».



Затем откроется окно установки программы, где необходимо изучить и принять условия лицензионного соглашения и следовать инструкциям по установке.



Для полуавтоматической установки (название и описание компонентов выводятся по ключу **-help**):

```
winetricks "components names"
```

Пример установки *.NET* Framework 4.5:

```
winetricks -q dotnet45
```

Пакет Mono

Mono — программная платформа, позволяющая разработчикам достаточно просто создавать развитые кроссплатформенные приложения.

В базовом варианте **Mono** состоит из нескольких компонентов:

- Компилятор языка C#;
- Среда исполнения **Mono** — состоит из среды исполнения (*CLI*) непосредственно, компилятора среды исполнения (*Just-In-Time, JIT*), генератора машинного кода (*Ahead-Of-Time, AOT*), загрузчика сборок, сборщика мусора, подсистемы управления многопоточностью и компонентов поддержки взаимодействия между сборками и *COM* (или аналогами в Linux, например *XCOM*);
- Базовая библиотека классов — набор стандартных классов, совместимых с классами *Microsoft .NET Framework;*
- Библиотека классов **Mono** — набор классов, поддерживающих дополнительные функции для разработки Linux-приложений. Например, классы для поддержки *Zip*, *OpenGL*, *Cairo*, *Gtk+*.

Данный пакет ставится автоматически при установке Wine из репозитория версии 4.4.

Установка Gecko

Gecko – это свободный движок вывода веб-страниц для браузера при работе в интернете **wine**. Если **wine** не работает с интернетом и вы не запускаете **windows.exe** браузер, то вам **Gecko** не нужен.

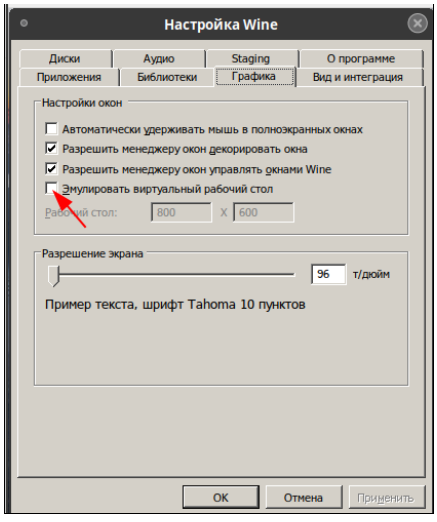
Обычно при запуске приложения для работы с веб-страницами *Wine* автоматически ищет *Gecko* сперва в **/usr/share/wine/gecko**. Если *Wine* не находит архив с *Gecko* там, то он автоматически загружает его из интернета, но некоторые приложения не любят ждать, пока загрузиться *Gecko* и зависают или вылетают.

Данный пакет ставится автоматически при установке Wine из репозитория версии 4.4.

Виртуальный рабочий стол в Wine

Имитация рабочего стола *Windows* в **wine** необходима для решения проблем, связанных с разрешением экрана, а также при сворачивании программ в **wine**.

Рабочий стол можно включить через **winecfg**.



Запущенная программа размещается в рамках виртуального рабочего стола.

Также есть возможность запустить рабочий стол, не используя интерфейс:

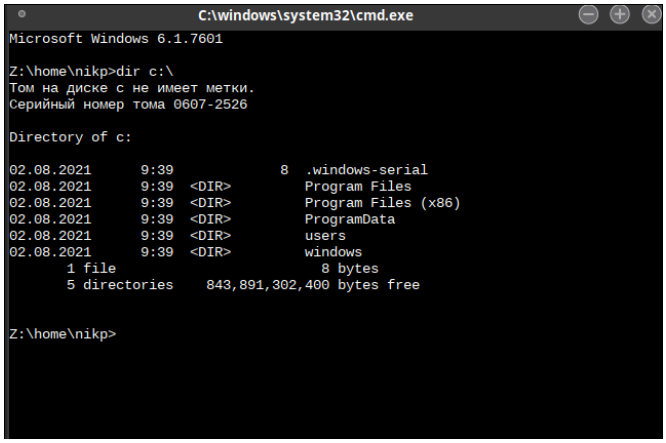
```
wine explorer /desktop="desk",800x600 regedit
```

- **explorer** — проводник *Windows*;
- **/desktop="desk",800x600 regedit** — создать рабочий стол с именем *desk* и разрешением *800x600*, затем запустить программу *regedit* (редактор реестра).

Углубление в функционал Wine

Wineconsole — позволяет запускать консоль *windows*, в основном используется для отладки.

```
wineconsole cmd
```



Wineserver — служба, исполняющая роль ядра Windows. Для каждого префикса запускается своя служба, что позволяет выполнять одновременно несколько программ из разных префиксов.

В случаях, когда программа зависла, поможет перезапуск **wineserver** (жесткая перезагрузка):

```
wineserver -k
```

или с префиксом:

```
WINEPREFIX="/home/$USER/.wine_prefix" wineserver -k
```

- **wineserver -d[n]:** — выводит отладочную информацию, имеет 3 уровня:
  - **0** — не выводит информацию;
  - **1** — выводит основную информацию;
  - **2** — выводит полную информацию.
- **wineserver -f:** — выводит сервер на передний план для упрощения отладки;
- **wineserver -p[n]:** — определяет время до остановки сервера, когда все клиентские процессы завершились, что позволяет быстрее запускать приложения, по умолчанию 3 секунды, если значение n не указано, сервер будет работать вечно;
- **wineserver -w:** — ожидает завершения предыдущей сессии ядра для корректного старта новой сессии.

Wineboot - выполняет инициализацию, запуск и перезагрузку префикса. Также выполняет симуляцию перезапуска и завершения работы программ (мягкая перезагрузка).

```
wineboot -r
```

Создание префикса через **wineboot**:

```
WINEPREFIX="/home/$USER/.wine_prefix" wineboot -i
```

- **-i** — инициализировать префикс.

Установка и запуск игр

Запуск с помощью AppImage
Установка игр из пакета
Установка игр через STEAM
Установка игр через платформу WINE
Установка игр через платформу Port Wine

Вы можете подробнее ознакомиться с возможностью установки игр на РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube**:
  - Как устанавливать игры в РЕД ОС;
  - Установка игр в РЕД ОС с помощью PortProton .
- в **Яндекс.Дзен**:
  - Как устанавливать игры в РЕД ОС;
  - Установка игр в РЕД ОС с помощью PortProton .
- в **VK Видео**:
  - Как устанавливать игры в РЕД ОС;
  - Установка игр в РЕД ОС с помощью PortProton .

На наших каналах вы также сможете найти много другой полезной информации.

Запуск с помощью AppImage

Большинство современных игр и программ требуют для своей работы дополнительные компоненты (библиотеки, утилиты и так далее). Это значит, что для того, чтобы запустить такую игру в РЕД ОС, нужно сначала дополнительно установить эти компоненты.

Для запуска игр и программ без привязки к дополнительным компонентам был разработан формат **AppImage**.

Ключевая идея AppImage заключается в том, что *одна программа – это один файл*. Программы в формате AppImage состоят всего из одного файла с расширением AppImage, например, *gimp.AppImage*.

Работать с программами в формате AppImage очень просто. Вы просто скачиваете программу, делаете файл программы исполняемым и запускаете. Ничего не нужно устанавливать, программа просто работает.

Поэтому сначала рассмотрим самый простой способ запуска игр – без установки. В этом случае пакет сразу готов к запуску. Для этого необходимо:

1. Скачать пакет с сайта с интересующим вас приложением или игрой через браузер по ссылке, например:

https://blub-game.com/download.html

или в терминале выполнить следующую команду:

```
$ wget https://blub-game.com/d/linux64/blubVolley.AppImage
```

2. Необходимо предоставить права на исполнение для полученного файла:

```
$ chmod +x blubVolley.AppImage
```

3. Последним шагом осталось запустить игру, выполнив команду:

```
$ ./blubVolley.AppImage
```

Приложение запускается в отдельном окне – так, как если бы оно было установлено у вас в системе.

Установка игр из пакета

Далее рассмотрим способ установки игры из готовых пакетов. Пакеты могут быть получены у стороннего разработчика или входить в используемый репозиторий. Для установки игры необходимо:

1. Скачать пакет(ы) через браузер по ссылке, например:

https://centos.pkgs.org/7/epel-x86_64/aisleriot-3.22.2-1.el7.x86_64.rpm.html

или в терминале выполнить следующую команду:

```
$ wget https://rpmfind.net/linux/epel/7/x86_64/Packages/a/aisleriot-3.22.2-1.el7.x86_64.rpm
```

2. От root-пользователя запустить локальную установку пакета с зависимостями, выполнив команду:

```
# dnf localinstall aisleriot-3.22.2-1.el7.x86_64.rpm
```

После установки пакета и зависимостей терминал выведет приблизительно следующее сообщение:

```
Установлено:
 aisleriot.x86_64 1:3.22.2-1.el7
Установлены зависимости:
 gc.x86_64 0:7.2d-7.el7 guile.x86_64 5:2.0.13-1.el7
Выполнено!
```

3. Запуск игры производится через *«Главное меню»* – *«Игры»*.



Рис. 1 - Запуск игры из пакета

Установка игр через STEAM

Для того чтобы установить и запустить игру через онлайн-сервис цифрового распространения компьютерных игр и программ Steam, необходимо с правами root-пользователя установить клиент **Steam**, выполнив команду:

```
# dnf install steam
```

В *«Главном меню»* - *«Интернет»* отобразится установленное приложение Steam, при нажатии на которое появится значок запуска на рабочем столе. После первого запуска Steam необходимо дождаться скачивания всех обновлений, а затем выполнить его настройку.

Сначала пользователю необходимо создать аккаунт Steam, если его еще не существует. Если аккаунт Steam уже есть, можно выполнить вход.

Далее для более удобной работы можно изменить языковые настройки в меню *«Steam»* - *«Settings»* - *«Interface»*. После смены языка потребуется перезапуск Steam.

Затем в меню *«Steam»* - *«Настройки»* необходимо выбрать пункт *«Совместимость»* и активировать функцию на *«Включить Steam Play для всех других продуктов»* (Рис. 2). Это нужно для того, чтобы Steam Play включался во всех играх библиотеки пользователя. Также требуется выбрать версию **Proton**, который будет способствовать запуску игр.

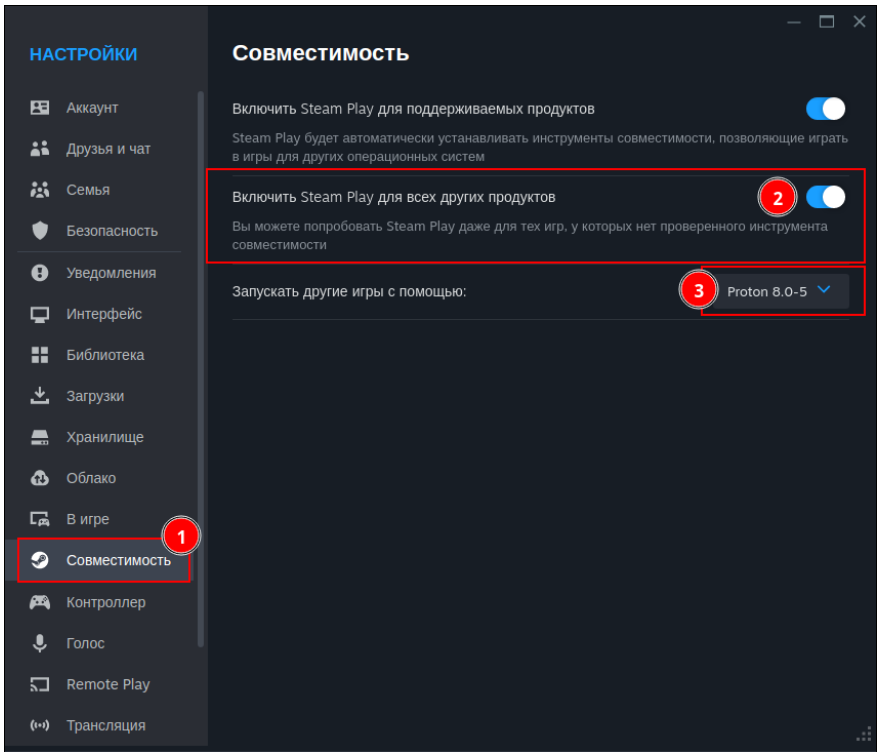


Рис. 2 – Установка флажка включения Steam Play

Существует сайт www.protondb.com, где перечислены все игры, поддерживаемые *Proton*, и указаны статусы к каждой игре. Перейдя в раздел с игрой, можно узнать более подробную информацию о возможности запуска игры, а также о дополнительных настройках, если при запуске возникают трудности.

После настройки Steam можно перейти в библиотеку пользователя или в магазин и скачать нужную игру. В данном случае с сайта *protondb.com* выбрана бесплатная нативная игра **«Toy Robot»**.

После скачивания игры необходимо перейти в библиотеку игр пользователя и нажать правой кнопкой мыши на игре из списка. В контекстном меню выбрать пункт *«Свойства...»*. Во вкладке *«Совместимость»* установить флажок на использование инструментов совместимости и выбрать необходимую версию Proton для запуска игры (Рис. 3).

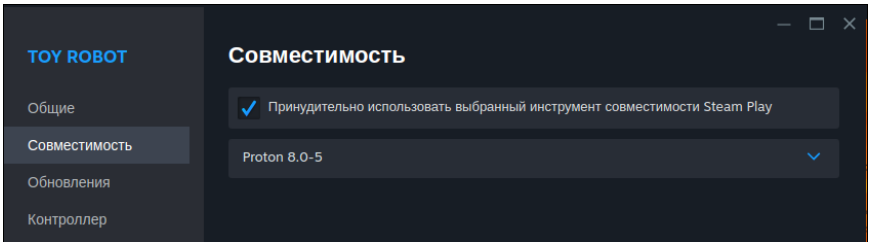


Рис. 3 – Установка флажка на использование Proton

На этом процедура настройки завершена. Можно запускать игру.

Установка игр через платформу WINE

WINE – это свободное программное обеспечение, позволяющее пользователям UNIX-подобных ОС исполнять 16-, 32- и 64-х битные приложения, том числе игры, созданные исключительно для *Microsoft Windows*, без наличия при этом установленной Microsoft Windows.

Название **W.I.N.E.** – рекурсивный акроним и расшифровывается как *«Wine Is Not an Emulator»* - «W.I.N.E. – это не эмулятор». Имеется в виду, что Wine не является эмулятором компьютера или виртуальной машиной, как Virtual Box и другие, Wine – это альтернативная, свободная реализация *Windows API*.

Для того чтобы установить Wine, необходимо в терминале с правами root-пользователя выполнить команду:

```
# dnf install wine
```

После установки в *«Главном меню»* появится раздел *«Wine»*, который включает в себя несколько программ:

1. ***Notepad*** – простой блокнот.

2. ***Regedit*** – инструмент для открытия реестра, также можно открыть в консоли, выполнив команду:

```
$ wine regedit
```

3. ***Wine Boot*** – инструмент, с помощью которого можно симулировать перезагрузку.

4. ***Wine Configuration*** – маленькая, но мощная утилита, которая позволяет настраивать Wine в соответствии с нуждами пользователя. *Winecfg* можно запустить под правами обычного пользователя через терминал, набрав команду:

```
$ winecfg
```

В *Winecfg* есть несколько вкладок, отвечающих за настройки Wine.

Вкладка *«Приложения»* позволяет создавать конфигурации, выбираемые при запуске в Wine определенных приложений, а также выбирать версию Windows для обеспечения совместимости.

Вкладка *«Библиотеки»* позволяет контролировать работу Wine с библиотеками Windows. Это особенно важно, т.к. некоторые приложения не совместимы с определенными версиями библиотек или требуют определенных нестандартных библиотек.

Вкладка *«Графика»* позволяет устранять проблемы с разрешением экрана или менеджером окон.

Вкладка *«Вид и интеграция»* позволяет менять внешний вид приложений, запущенных в Wine, если в этом есть необходимость.

Вкладка *«О программе»* содержит сведения о текущей версии Wine.

Вкладка *«Staging»* представляет собой набор чекбоксов, которые позволяют включать или отключать различные возможности, предоставляемые патчами.

Вкладка *«Аудио»* позволяет настраивать ввод и вывод звука. Вкладка *«Диски»* позволяет осуществлять доступ к подключенным устройствам.

5. ***Wine File*** – файловый менеджер.

После установки Wine в домашней папке пользователя будет создан профиль **.wine** (изначально он скрыт, чтобы отобразить профиль необходимо ПКМ нажать в пустом месте папки и выбрать пункт «Скрытые файлы»). Профиль создается конфигуратором Wine. Можно создавать несколько профилей, т.к. для разных программ могут требоваться разные дополнительные компоненты и разные настройки Wine. Для этого существуют ***префиксы*** Wine, благодаря которым можно избежать конфликтов и создать свое окружение для подобного рода программ.

Для создания нового профиля в *Wine Configuration* нужно указать путь к папке профиля через переменную окружения или в терминале выполнить следующую команду:

```
WINEPREFIX=~/.wine_for_games winecfg
```

Если папки не было изначально, она будет автоматически создана. Разные профили между собой не связаны, они существуют как несколько Windows на одном компьютере.

Чтобы установить заранее скачанную игру для Windows через Wine, необходимо в терминале выполнить команду:

```
$ wine [/путь_к _файлу/program.exe]
```

В нашем примере команда будет выглядеть следующим образом:

```
$ wine /home/user/Stalker/setup.exe
```

После выполнения команды запускается установщик пакета (Рис. 4), где предлагается выбрать папку установки, создание ярлыка, а также язык и установку дополнительного ПО.

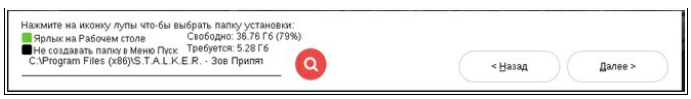


Рис. 4 – Подготовка к установке игры

После выбора всех нужных пунктов необходимо нажать кнопку *«Установить»*, начнется процесс установки игры. После установки игры следует нажать кнопку *«Завершить»*. Игра установлена и готова к запуску.

Установка игр через платформу Port Wine

Port Wine – это модифицированная версия *Wine*, которая позволяет запускать более сложные и энергоемкие игры в Linux, которые не поддерживает обычный *Wine*.

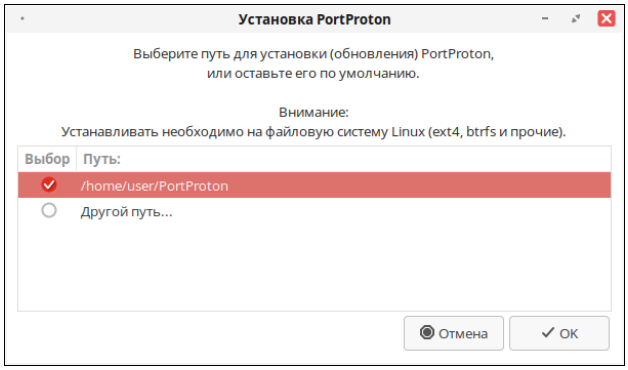
Для корректной работы **PortWine** необходимо сначала установить дополнительные пакеты:

```
dnf install curl icoutils libcurl wget zenity bubblewrap zstd cabextract tar goverlay openssl steam
```

После этого необходимо скачать установочный файл **PortWine** и запустить его установку:

```
wget -c "https://github.com/Castro-Fidel/PortProton_ALT/raw/main/portproton" && sh portproton
```

Появится окно настройки параметров перед установкой - необходимо будет выбрать путь установки **PortProton**.



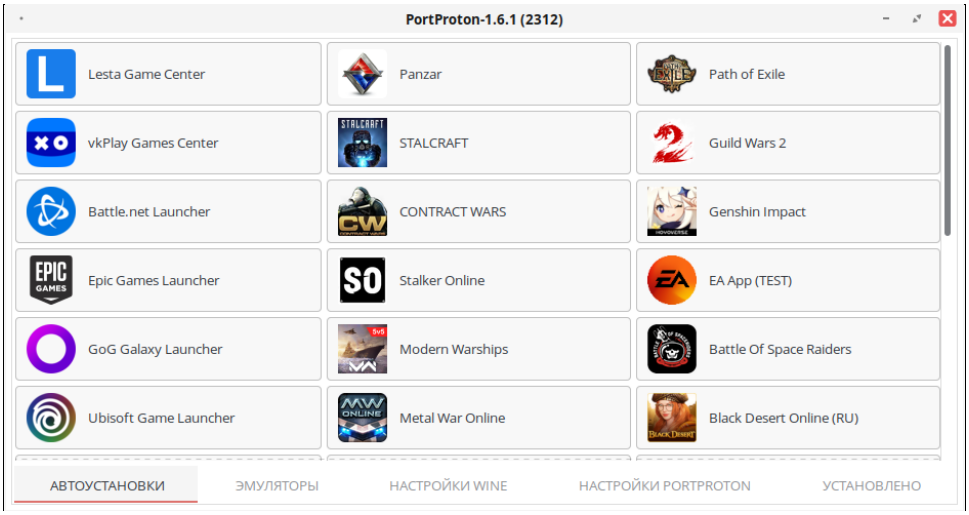
Начнется процесс установки.

После завершения установки программа будет доступна из «**Главного меню**» - «**Игры**» - «**PortProton**».

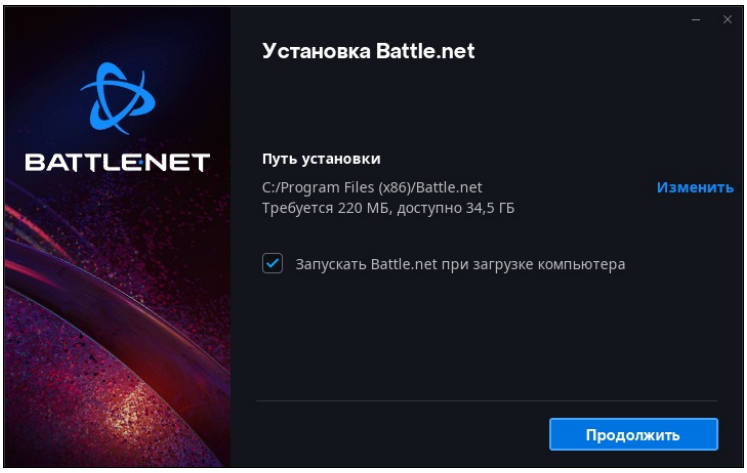
При первом запуске произойдет автоматическая загрузка необходимых библиотек и инициализация приложения.



После завершения первого запуска будет открыто окно с выбором необходимого лаунчера:



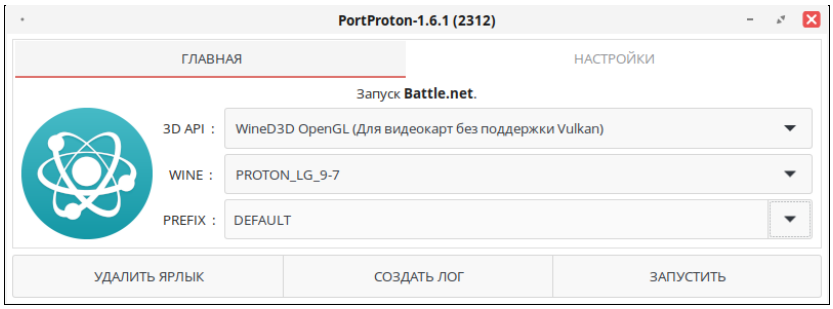
Выберите **Battle.net Launcher**. При первом запуске лаунчера также произойдет обновление конфигураций. Далее появится окно установщика **Battle.net**.



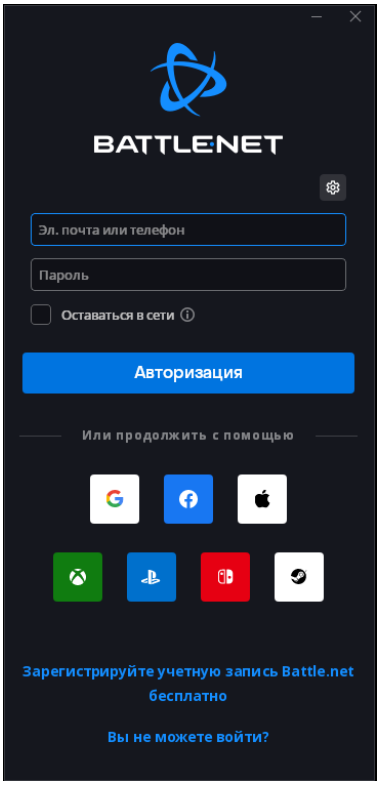
Для запуска установки нажмите «**Продолжить**».

После завершения установки будет выведено информационное окно, в котором необходимо указать, добавлять ли значок **Battle.net** в «**Главное меню**» - «**Игры**».

Запустите программу и установите необходимые настройки для запуска. Выбор зависит от возможностей используемой видеокарты.



После запуска **BattleNet** откроется окно авторизации пользователя.

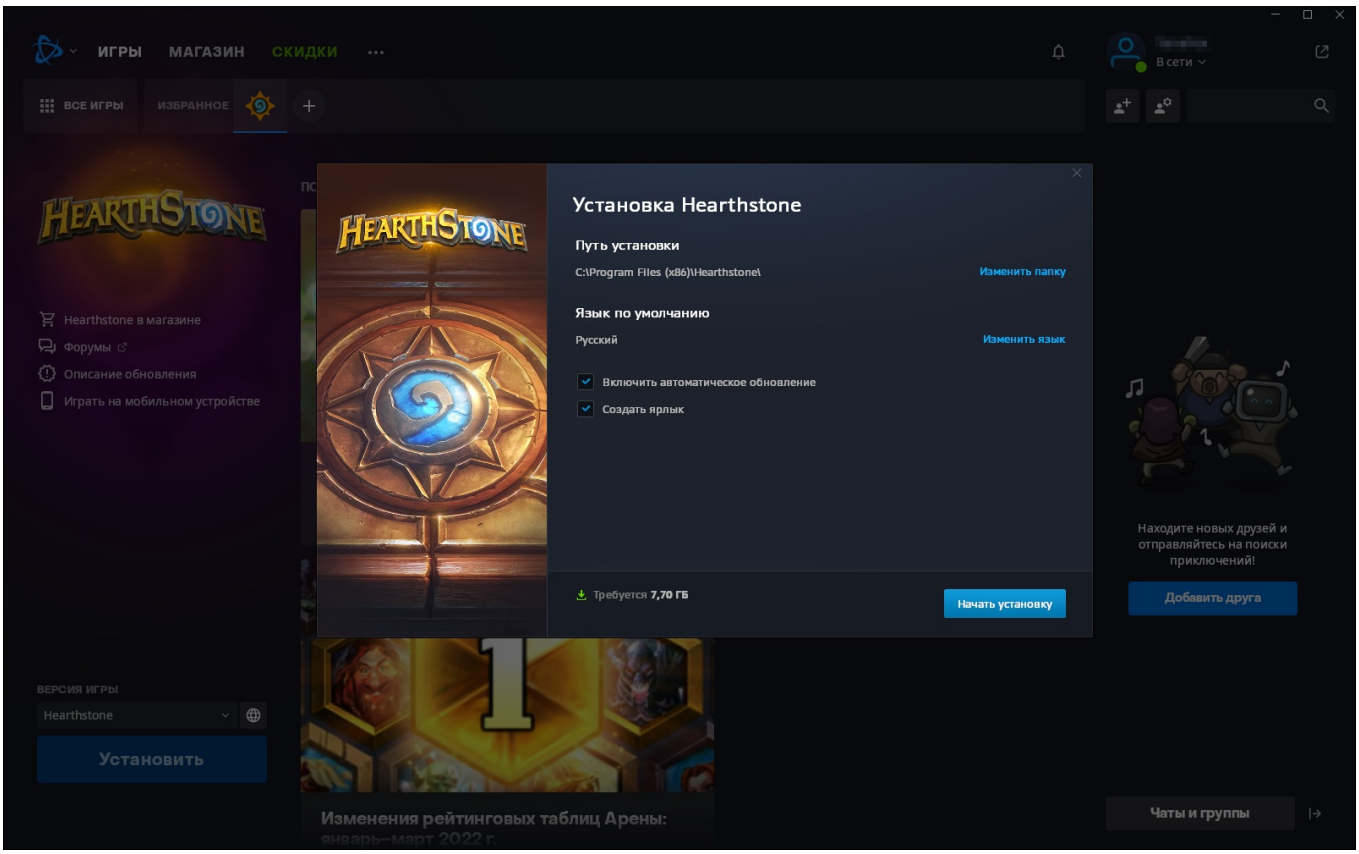


Если аккаунт в системе уже есть, просто выполняется вход, если же его нет, необходимо зарегистрироваться.

При регистрации необходимо указать дату рождения, имя и фамилию, номер телефона (необязательное поле) и адрес электронной почты. Далее потребуется указать имя пользователя в системе или оставить случайно сгенерированное имя и установить пароль для входа в систему. После этого регистрация завершится и будет выполнен вход в учетную запись.

Из списка игр следует выбрать интересующую (в данном случае **Hearthstone**) и нажать на кнопку *«**Установить**»*.

После этого откроется окно менеджера установки, где потребуется выбрать путь к игре, включение или отключение автоматических обновлений и создание ярлыка на рабочем столе. После настройки необходимо нажать кнопку «**Начать установку**» для скачивания и установки игры.



После завершения установки игра будет доступна для использования.



CherryTree – программа систематизации и ведения заметок

Базовые функции cherrytree
Вкладки cherrytree
Параметры cherrytree

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** cherrytree-0.38.11-1

Cherrytree - это удобное приложение для записи коротких заметок, позволяющее иерархически структурировать всю нужную информацию в наглядном виде. Утилита может выступать в качестве текстового редактора, позволяя вставлять в текст таблицы, изображения, ссылки и другие элементы.

Установка производится командой:

```
dnf install cherrytree
```

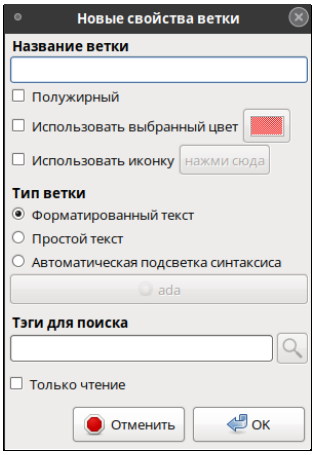
Вы можете подробнее ознакомиться с настройкой и работой утилиты **cherrytree**, просмотрев наши обучающие видео:

- на **RuTube** — CherryTree - программа систематизации и ведения заметок;
- в **Яндекс.Дзен** — CherryTree - программа систематизации и ведения заметок;
- в **VK Видео** — CherryTree - программа систематизации и ведения заметок.

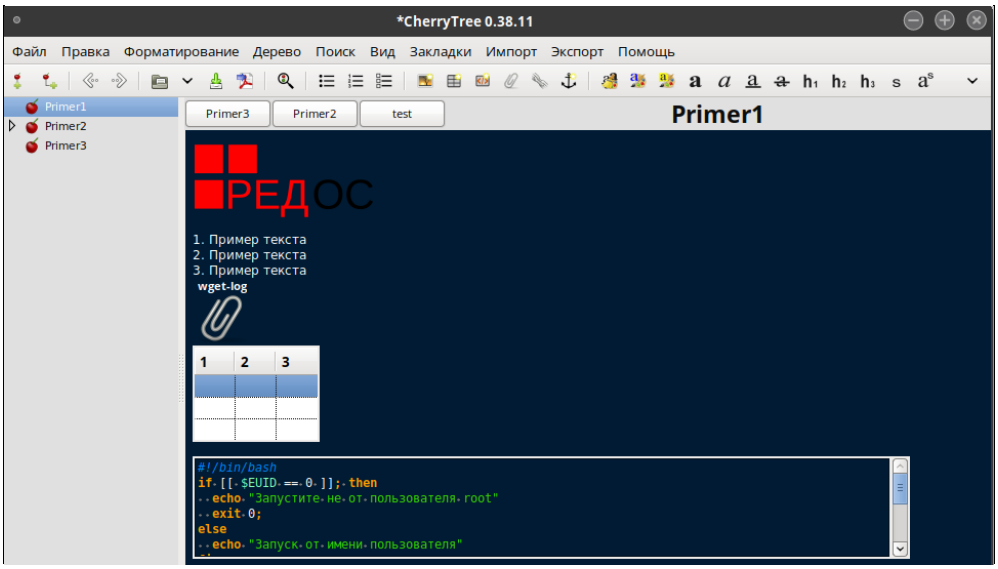
На наших каналах вы также сможете найти много другой полезной информации.

Базовые функции cherrytree

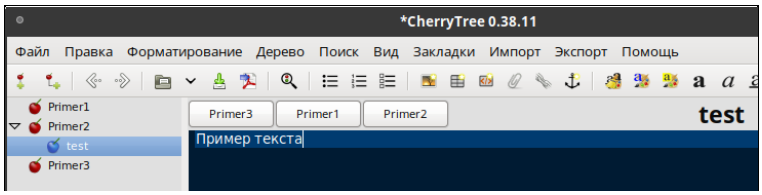
Программа представляет собой иерархическую структуру для хранения информации. Для добавления нового дерева необходимо нажать на иконку «**Добавить ветку с тем же родителем**», либо в верхнем меню выбрать пункт «**Дерево**», в котором будут находиться расширенные настройки ветвей. Необходимо задать название и выбрать тип ветки:



Созданную ветку можно использовать как текстовый редактор, в котором можно добавить изображение, таблицу, ссылку на файл или веб-сайт, так же можно вставить блок кода разных языков программирования. Для применения вышеперечисленных функций используйте верхнюю панель инструментов:

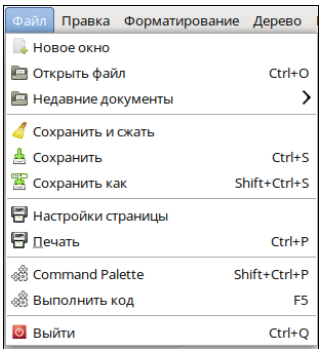


Для каждой ветки можно добавить дочернюю ветвь, для её добавления нажмите правой кнопкой мыши по необходимой ветке и выберите «**Добавить дочернюю ветвь**». В ней также можно хранить информацию, при нажатии на стрелочку возле основной ветви будет открываться дочерняя ветвь:

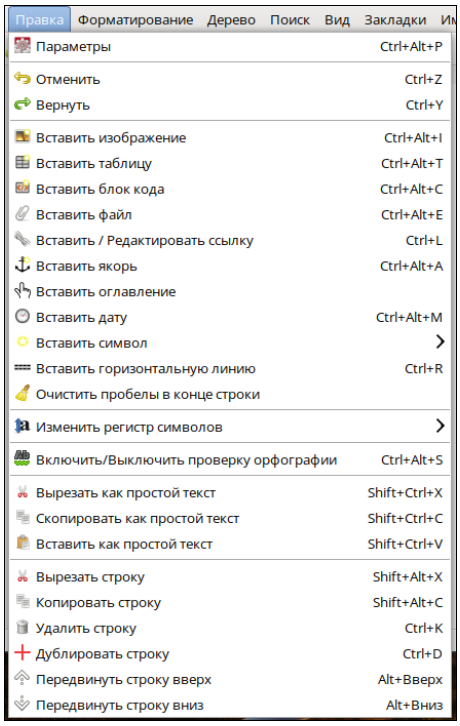


Вкладки cherrytree

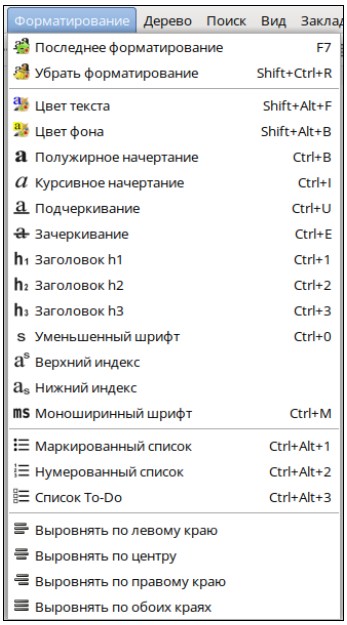
Вкладка «**Файл**» - позволяет сохранить текущий файл или открыть новый, настроить печать и выполнить код.



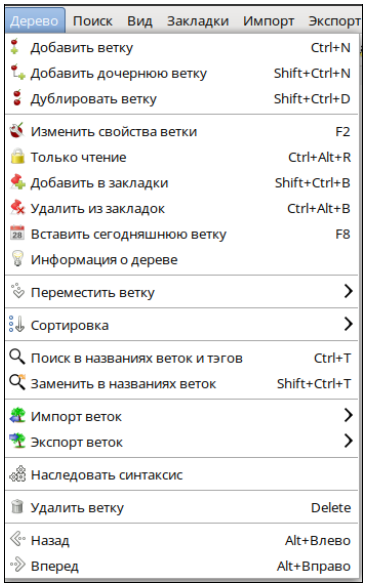
Вкладка «**Правка**» - позволяет перейти в параметры, отменить или вернуть действие, применить базовые функции и т.д.



Вкладка «**Форматирование**» - позволяет изменить настройки текста: цвет, фон, выравнивание, нумерация и т.д.



Вкладка «Дерево» - позволяет добавить или дублировать ветки, изменить свойства, отсортировать, импортировать или экспортировать ветки и т.д.



Вкладка «**Поиск**» - позволяет осуществлять поиск по определённым, либо по всем веткам.

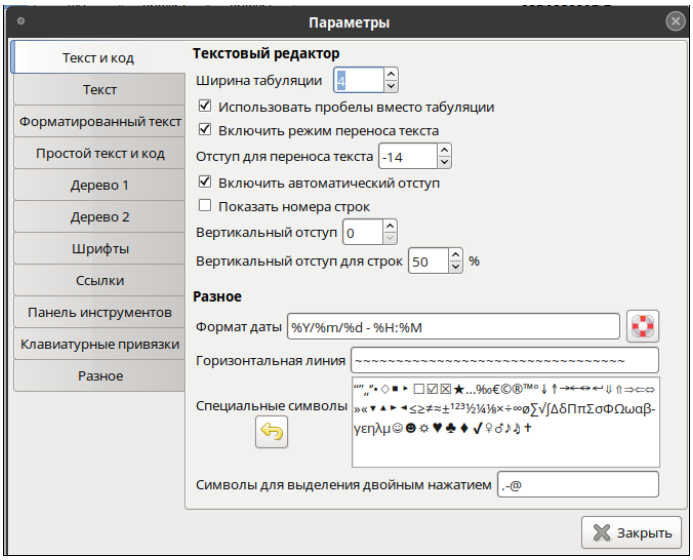
Вкладка «**Вид**» - позволяет настроить видимые части интерфейса программы.

Вкладка «**Закладки**» - позволяет переходить на ранее сохранённые ветви.

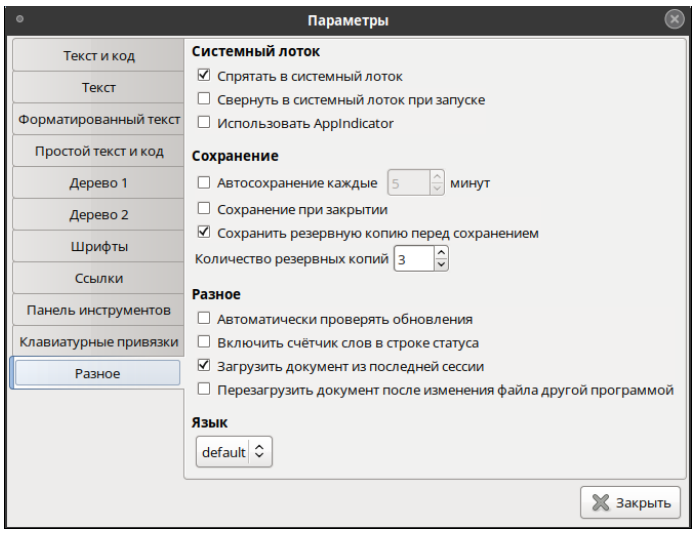
Вкладки «**Импорт/Экспорт**» - позволяют импортировать или экспортировать файл в разные форматы (PDF, HTML, текстовый файл, документ CherryTree).

Параметры cherrytree

В параметрах утилиты можно настроить формат текста, интерфейс деревьев, изменить кнопки на панели управления, добавить горячие клавиши и т.д.



Программу можно добавить в системный трей. Для добавления зайдите в раздел «**Разное**» и поставьте галочки «**Спрятать в системный лоток**» или «**Свернуть в системный лоток при запуске**».


Параметры
Текст и код
Текст
Форматированный текст
Простой текст и код
Дерево 1
Дерево 2
Шрифты
Ссылки
Панель инструментов
Клавиатурные привязки
Разное
Системный лоток
Спрятать в системный лоток
Свернуть в системный лоток при запуске
Использовать AppIndicator
Сохранение
Автосохранение каждые
5
минут
Сохранение при закрытии
Сохранить резервную копию перед сохранением
Количество резервных копий
3
Разное
Автоматически проверять обновления
Включить счётчик слов в строке статуса
Загрузить документ из последней сессии
Перезагрузить документ после изменения файла другой программой
Язык
default
Закрыть

ClipIt – менеджер буфера обмена

Clipit — удобный менеджер буфера обмена. Легковесное и простое в использовании приложение, которое позволяет сохранить историю работы с буфером обмена для дальнейшего использования ранее помещенного в него текста.

Вы можете подробнее ознакомиться с работой в **ClipIt**, просмотрев наши обучающие видео:

- на **RuTube** — ClipIt - менеджер буфера обмена;
- в **Яндекс.Дзен** — ClipIt - менеджер буфера обмена;
- в **VK Видео** — ClipIt - менеджер буфера обмена.

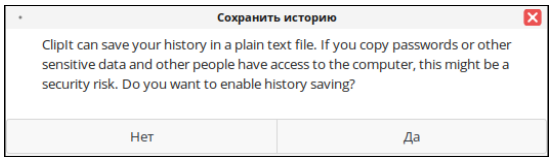
На наших каналах вы также сможете найти много другой полезной информации.

Устанавливается следующей командой:

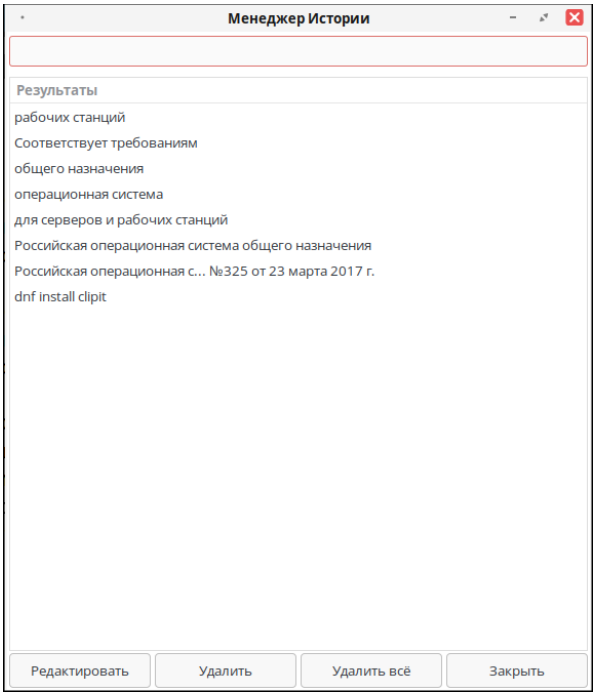
```
dnf install clipit
```

Для запуска необходимо перейти в *«**Меню**» - «**Стандартные**» - «**Clipit**»*.

При первом запуске программа предложит вам включить сохранение истории.



Программа при запуске добавляет свой значок в панель задач. При клике на значок открывается выпадающее меню со списком последних копирований в буфер обмена (история копирований). Если кликнуть по какому-либо элементу в истории, то соответствующий текст автоматически попадет в буфер обмена.

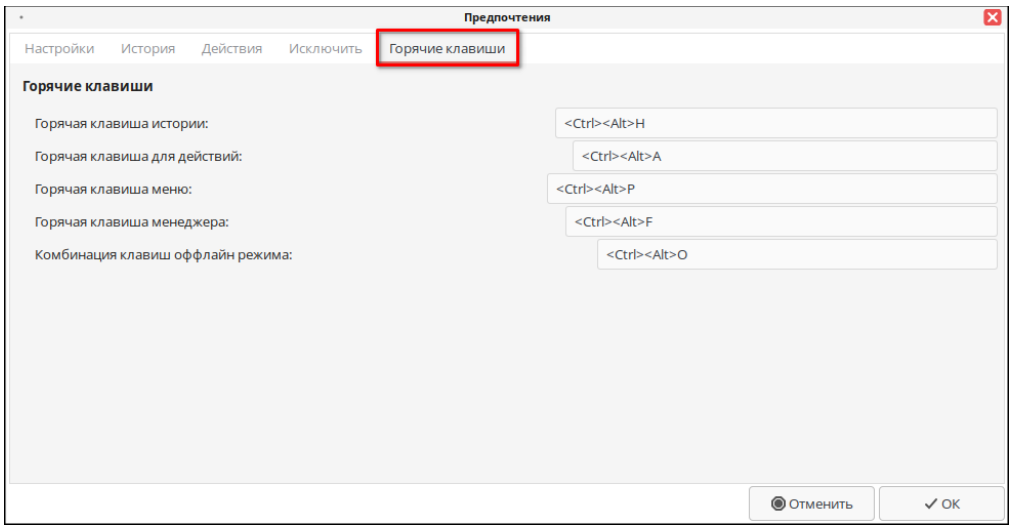


Если стартовые настройки программы вам не подходят, то при помощи пункта меню «***Параметры***» можно произвести более тонкую донастройку.

В настройках программы *Clipit* можно:

- указать количество элементов, которые необходимо хранить в истории (значение от 5 до 1000);
- задать количество элементов, которые будут отображаться в выпадающем меню (значение от 5 до 100);
- выполнить настройки внешнего вида меню;
- добавить фильтры, чтобы текст, удовлетворяющий фильтру, не попадал в историю (в качестве фильтра необходимо задать регулярное выражение).

Clipit поддерживает использование горячих клавиш. Например, чтобы открыть выпадающее меню с историей, нужно нажать «**Ctrl+Alt+H**». Меню при этом отображается сразу рядом с курсором мыши, и вы можете тут же выбрать любой элемент. Переназначить горячие клавиши можно в настройках программы во вкладке «*Горячие клавиши*».

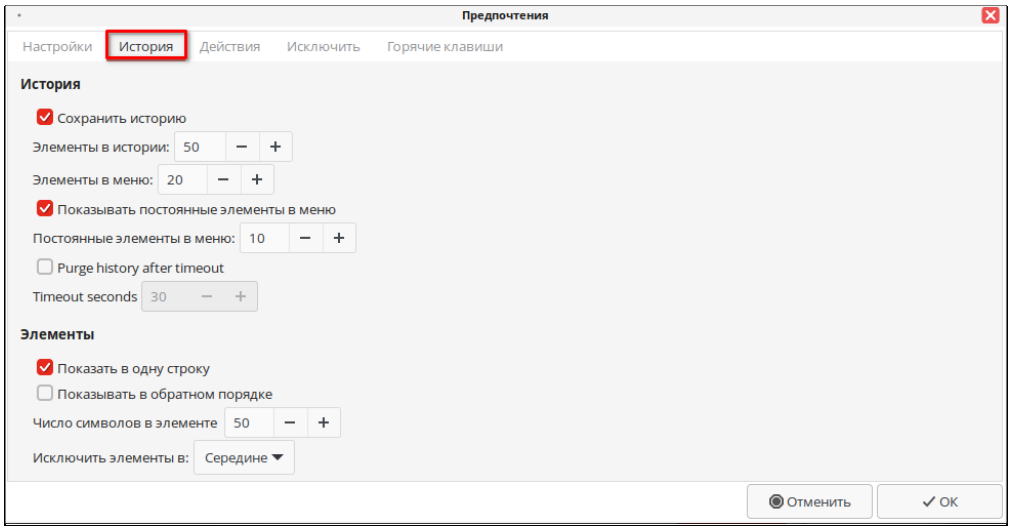


Установка количества элементов, которые должны храниться в истории и которые будут отображаться в выпадающем меню, осуществляется на вкладке «*История*».

Если указанное количество элементов в меню меньше указанного количества элементов в истории, то при превышении указанного в настройках предела элементов в меню более старые элементы автоматически скрываются.

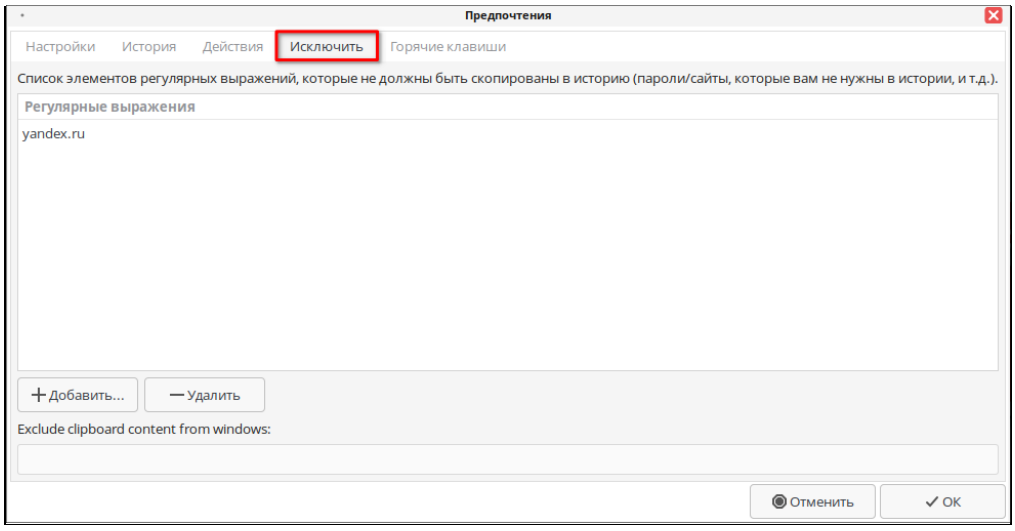
Если в процессе работы вам необходимо будет вернуться к скрытым элементам, необходимо будет выбрать пункт «*Управление историей*» в меню программы, затем найти нужный элемент и дважды кликнуть по нему левой кнопкой мыши.

Однако если превышен указанный предел элементов в истории, то самые старые элементы удаляются.



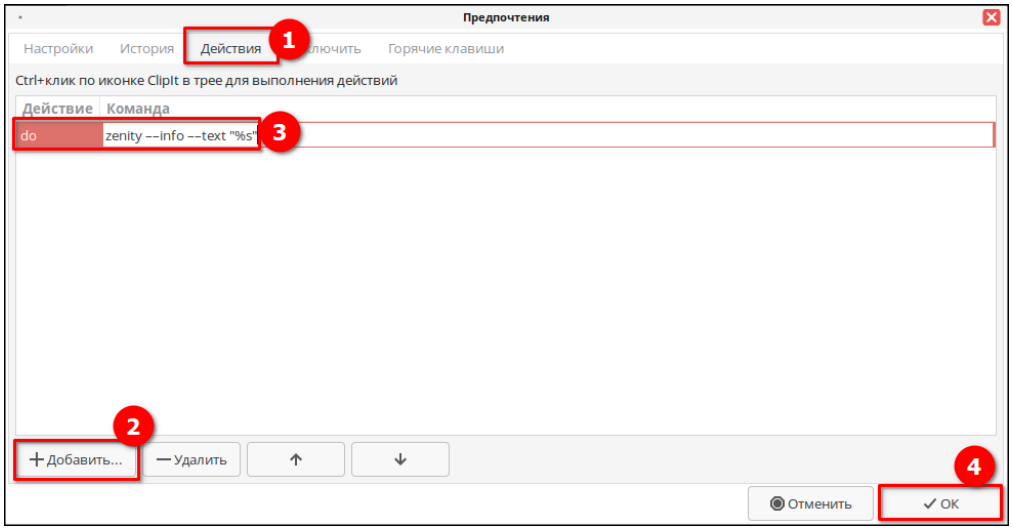
Clipit также поддерживает исключение списка элементов регулярных выражений, которые не должны быть скопированы, например, пароли или важная информация, которые не нужны в истории.

Например, при добавлении в регулярные выражения сайта **yandex.ru** данная ссылка не будет скопирована в историю.

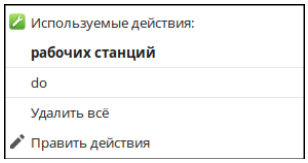


Программа также дает возможность создавать действия во вкладке настроек «*Действия*».

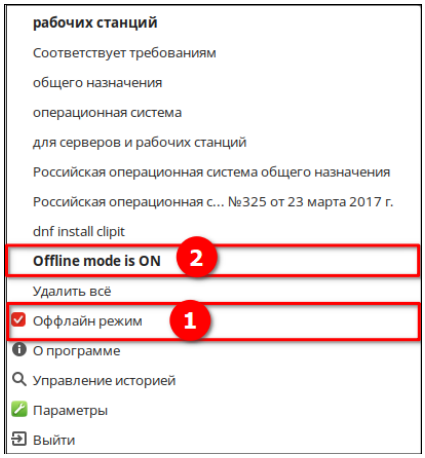
Действия — это какие-либо команды, которые вы можете выполнять над элементами в списке истории. Например, определим действие **do** и команду **zenity --info --text "%s"**.



При выполнении действия (сочетание клавиш «**Ctrl+Alt+A**») будет получено всплывающее окно с текстом из буфера обмена.



В меню программы присутствует галочка «*Оффлайн режим*» (1), при её включении скопированный текст не будет попадать в менеджер истории, а в меню появится информационное сообщение «**Offline mode is ON**» (2).



Торренты

Принцип работы
qbittorrent
transmission

В настоящее время компьютерные файлы уже не такие легковесные, как раньше, и даже короткие HD-видео могут иметь размер более гигабайта. Проблема в том, что чем файл больше, тем труднее им поделиться.

Если большое число пользователей одновременно будут пытаться получить доступ к большому файлу, то работа даже мощного сайта может быть очень медленной. В итоге даже может произойти сбой загрузки. Для решения данной проблемы были созданы торренты.

Торренты – это способ распространения данных. Торренты передают данные по протоколу **BitTorrent**. Скачивая файл через **BitTorrent**, загрузка идет тем быстрее, чем большее количество людей участвует в ней. Это работает с любыми типами файлов.

Вы можете подробнее ознакомиться с торрентами, просмотрев наши обучающие видео:

- на **RuTube** — Торренты и как с ними жить;
- в **Яндекс.Дзен** — Торренты и как с ними жить;
- в **VK Видео** — Торренты и как с ними жить.

На наших каналах вы также сможете найти много другой полезной информации.

Принцип работы

Большой файл условно разбивается на маленькие блоки. Программе, работающей по протоколу **BitTorrent**, для начала процесса скачивания большого файла необходима служебная информация обо всех этих блоках. Эта информация хранится в файле, который называется торрент. **Торрент** - это служебный файл, содержащий всю информацию о нужном файле, и о его частях, которые нужны для завершения загрузки.

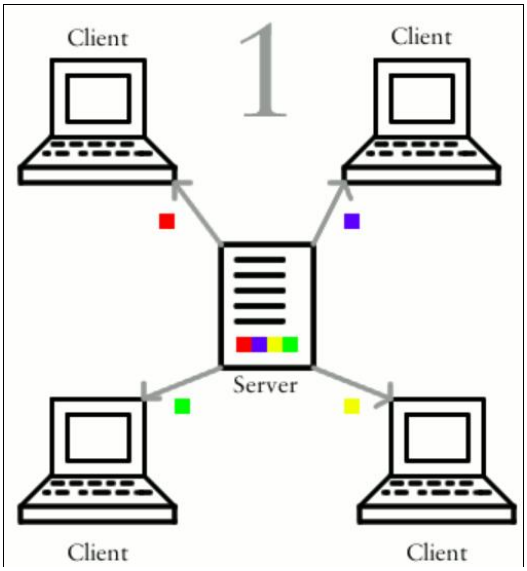
BitTorrent решил проблему медленного скачивания файлов с одного сервера, делая каждого участника процесса - источником. Таким образом, пользователи получают части файла и отдают их друг другу. Те, кто скачивает, или скачали и хранят файл, становятся сетью из нескольких источников. Все обеспечивают частями файлов друг друга. Это делает загрузку быстрой и надежной.

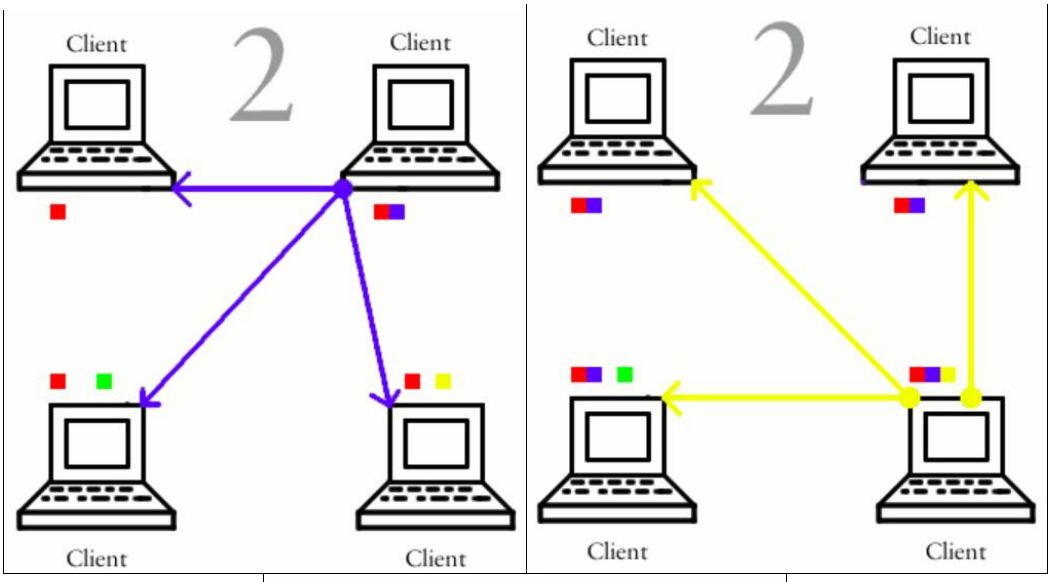
Для обеспечения такого взаимодействия в сети существует выделенный сервер - **ТРЕКЕР**, он регистрирует всех качающих и раздающих, и присваивает им статусы:

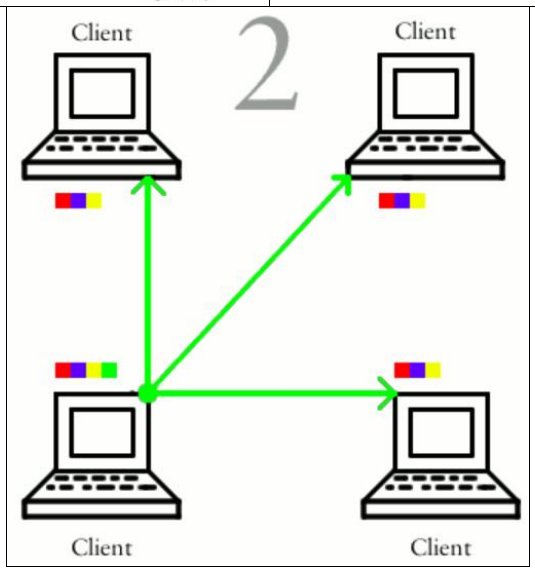
- **ПИР**, если идет загрузка.
- **СИД**, если загрузка закончена и происходит процесс раздачи.
- **ЛИЧ**, если файл загружен не полностью, но загрузка приостановлена.

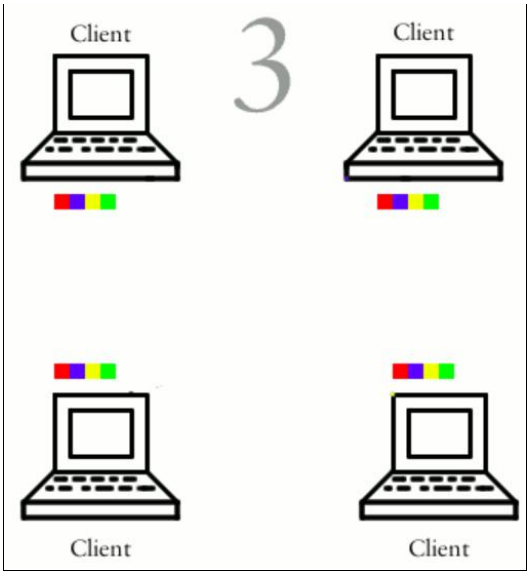
Процесс получения файла с помощью **BitTorrent** условно можно разделить на три этапа:

1. Регистрация пользователя в трекере с помощью торрент-файла и получение первых сегментов файла с сервера.
2. Получение остальных частей файлов от ПИРов, ЛИЧей и СИДов.
3. Перевод статуса пользователя в СИД или ЛИЧ, ожидание новой раздачи.

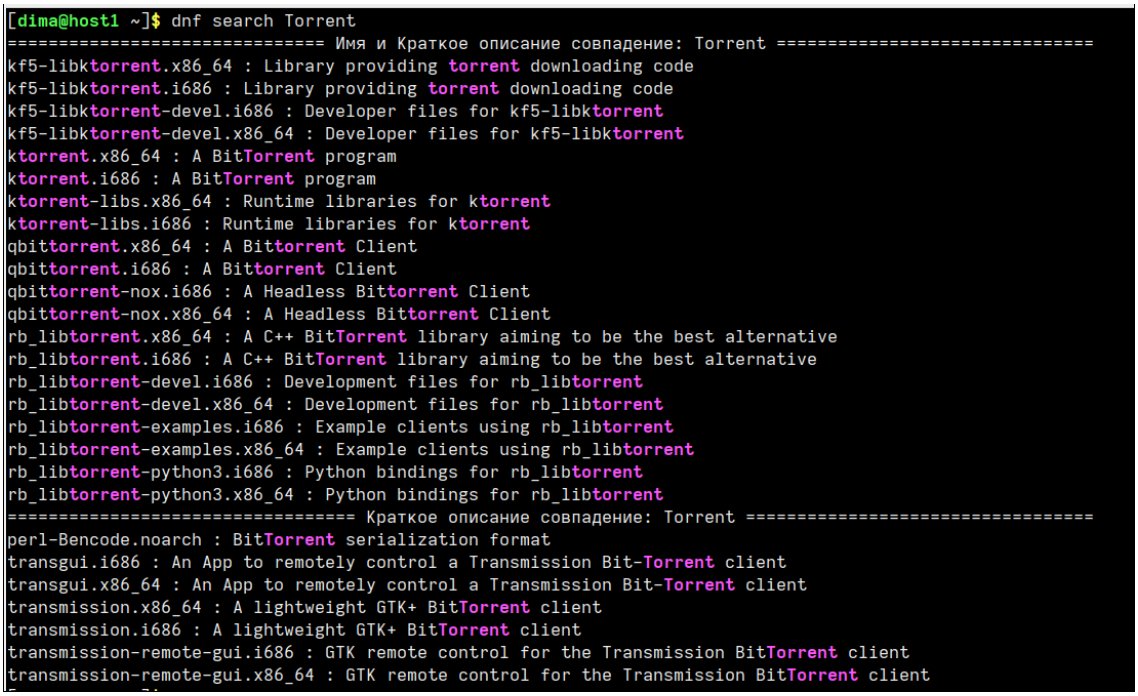








В репозиториях РЕД ОС имеется ряд приложений, реализующих поддержку протокола **BitTorrent**, для загрузки файлов. Менеджер пакетов нам подскажет, что это за программы, если мы осуществим поиск по строке «**Torrent**»:



Из полученного списка видно, что в поиске отобразились несколько **BitTorrent**-клиентов и несколько различных библиотек. Рассмотрим две программы из списка - **qbittorrent** и **transmission**.

qbittorrent

Интерфейс **qbittorrent** предельно прост и минималистичен, что и требуется для программы подобного рода. Программа практически не требует первоначальной настройки параметров, только указания папки для сохранения файлов.

Интерфейс состоит из нескольких частей:

1. **Панель меню**, в котором доступны «*Файл*», «*Правка*», «*Вид*», «*Инструменты*», «*Справка*». Состав меню минимален и, в тоже время, достаточен для работы программы.
2. **Панель инструментов** содержит основные кнопки, может быть скрыта с помощью опции меню «*Вид*».
3. **Панель закладок**. Это функциональные закладки, которые позволяют переключаться между разными функциями программы, такими как «*Управление торрентами*», «*Поиск торрентов*», «*Менеджер RSS подписок*», «*Журнал активности*». По умолчанию доступны только две первые закладки, остальные скрыты через меню «*Вид*».
4. **Панель статуса**. Может быть скрыта через меню «*Вид*». Отображает сведения о соединении, имеет несколько полей, которые позволяют переходить к настройкам программы или переключать режим её работы.

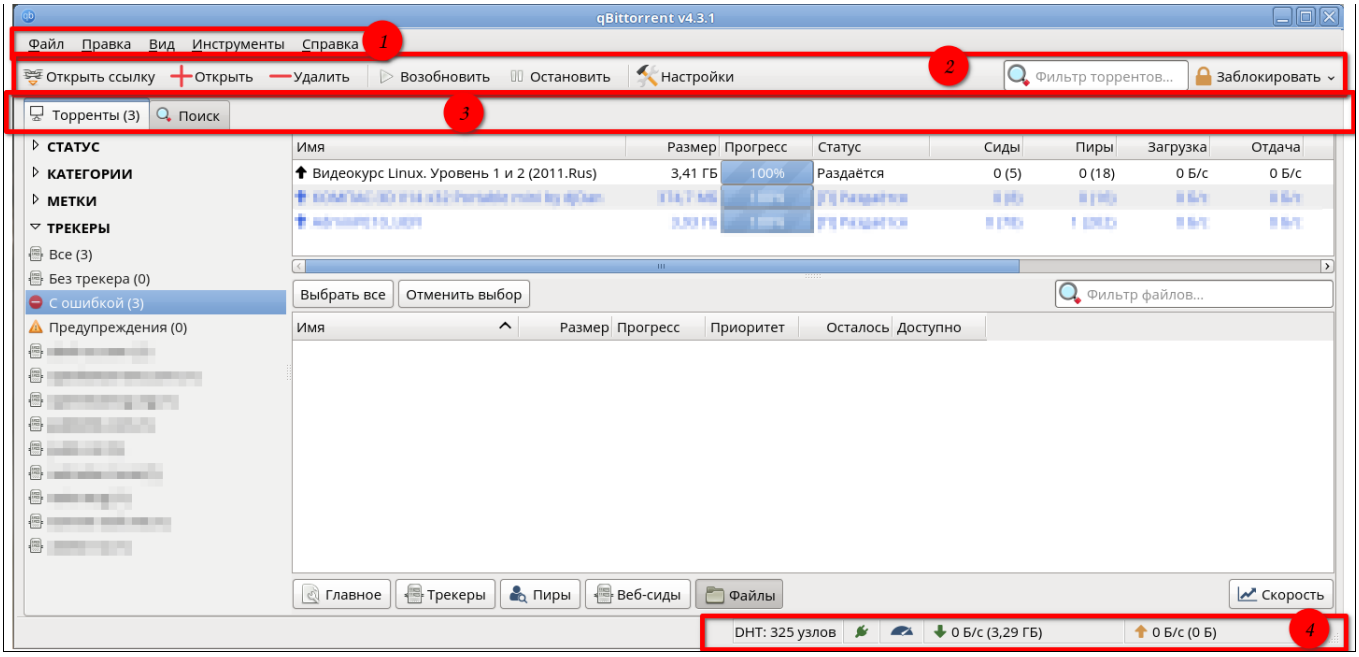
Для установки **qbittorrent** перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

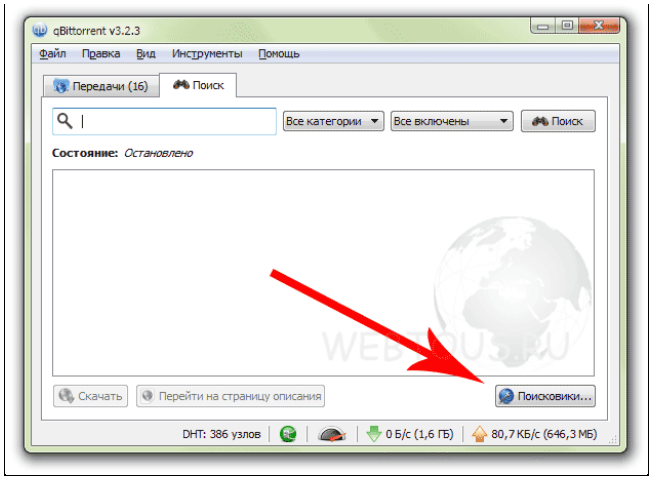
```
dnf install qbittorrent
```

После установки программа будет доступна из «**Главного меню**» - «**Интернет**» - «**qBittorrent**».

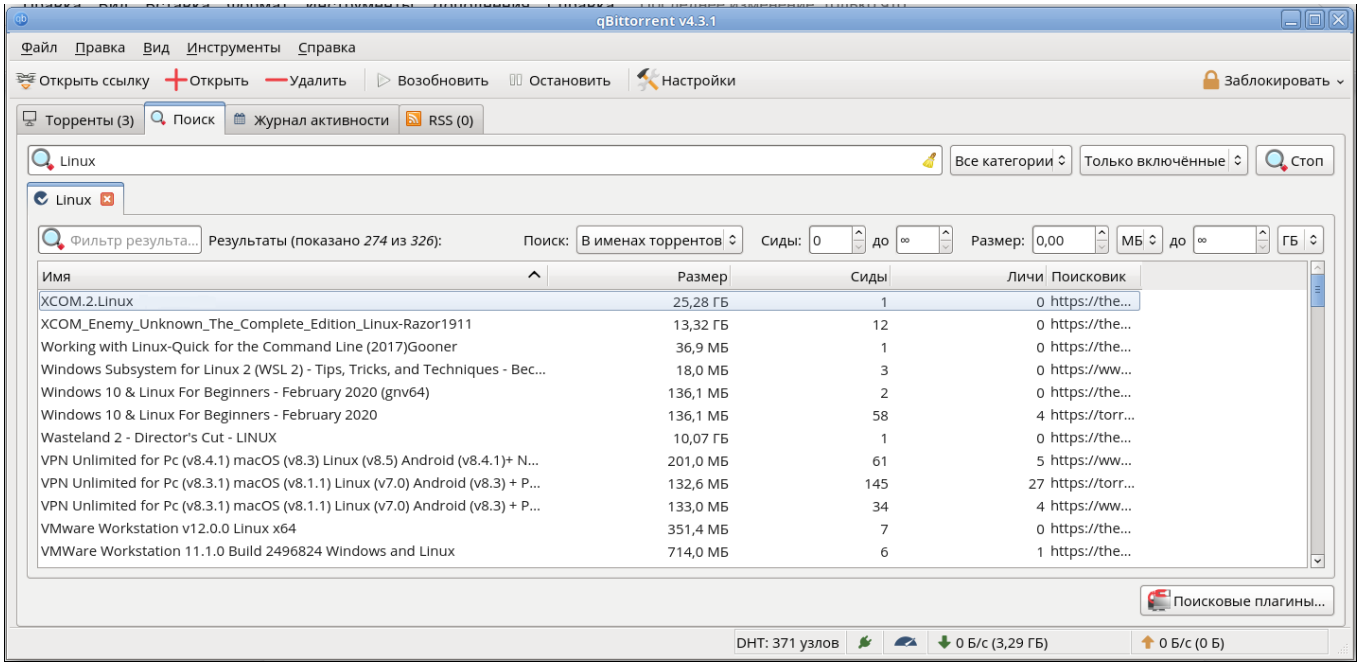


Закладка «Поиск»

При помощи закладки «*Поиск*» можно искать торренты, для этого нужно добавить необходимые ссылки. По умолчанию список пуст, поэтому можно просто нажать кнопку «*Поисковые плагины*» и проверить обновления. Вы получите небольшой список сайтов, по которым уже можно искать торренты. Можно добавлять свои ссылки на источники. Ссылки в списке можно отключать без удаления.



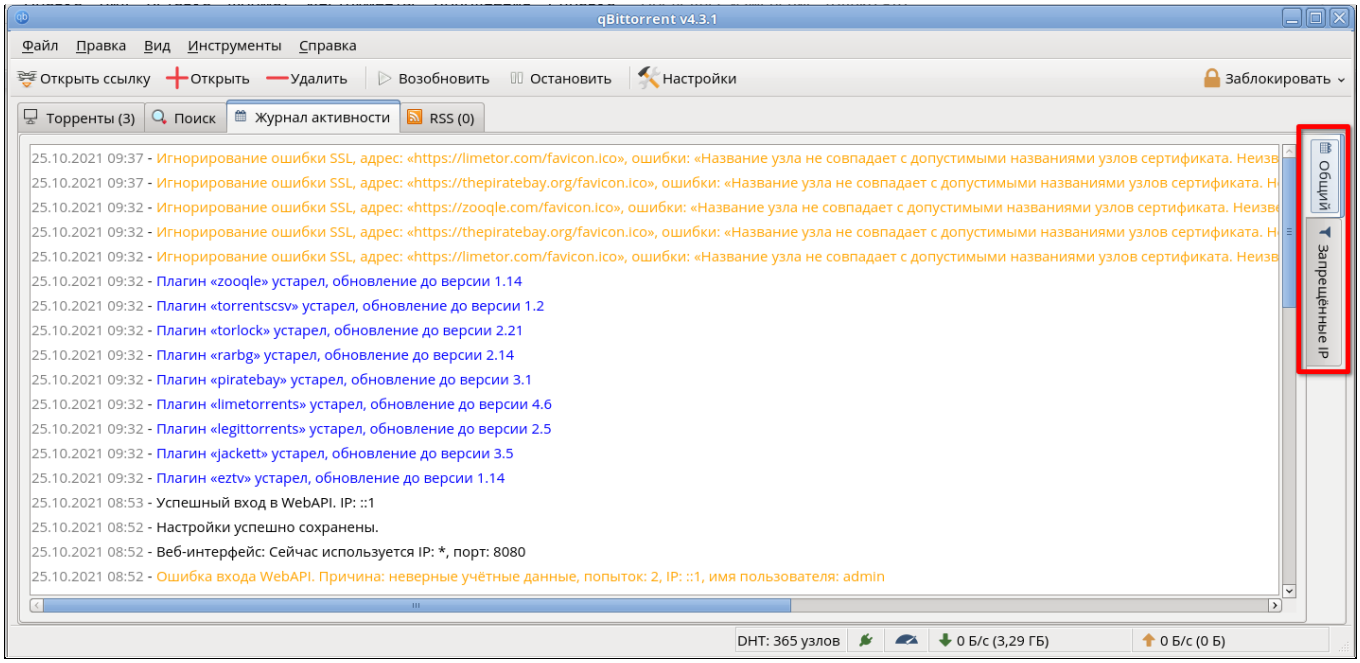
После добавления источников в строке поиска можно вводить нужные фразы и осуществлять поиск торрентов.



Для каждого найденного торрента доступна ссылка на страницу описания и кнопка «**Загрузить**».

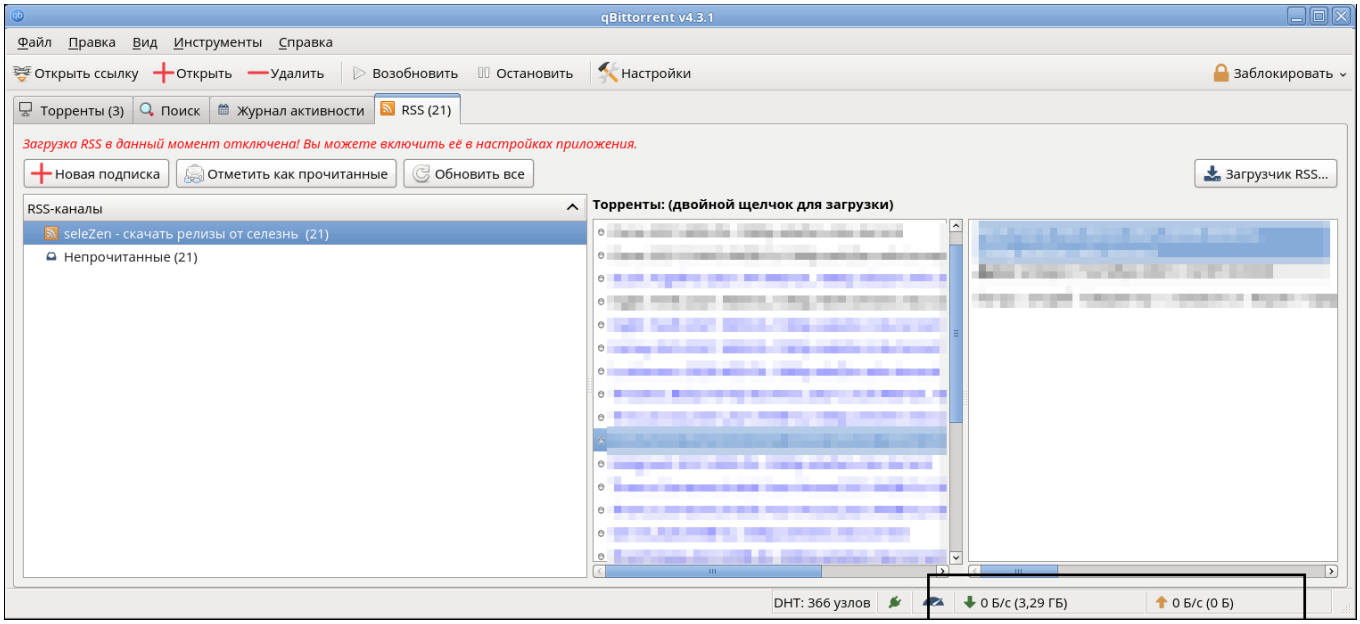
Закладка «Журнал активности»

На данной вкладке отображается список служебных сообщений о состоянии программы. Отображается два журнала – «*Общий*» и «*Запрещенные IP*».



Закладка «RSS»

RSS (Rich Site Summary, полная сводка сайта) – это автоматически генерируемая сводка в формате **rss** или **xml**, в которой отображаются недавно опубликованные статьи и новости. **RSS** - это отличный способ структурирования и фильтрации данных.

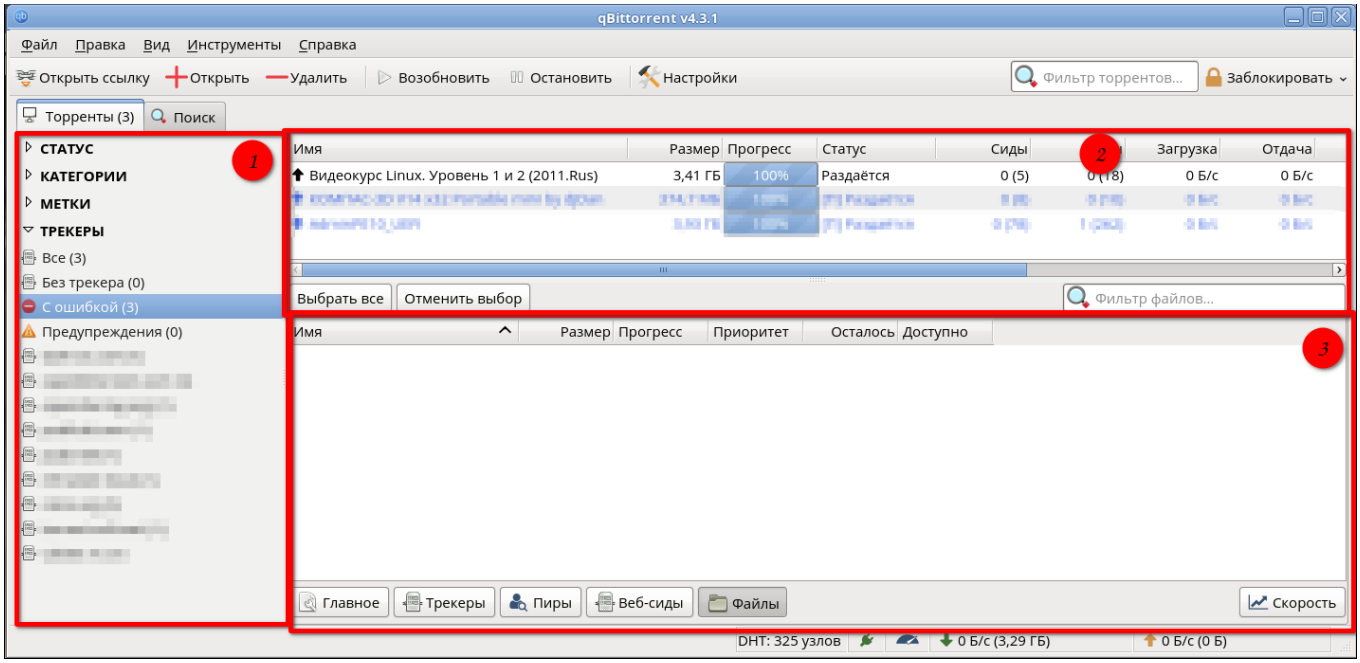


Для настройки подписок будет необходимо поискать ссылки на **RSS** в интернете. После этого добавьте найденную ссылку, нажмите «*Обновить*» и из полученного списка можно добавить в загрузку любой торрент.

Закладка «Торренты»

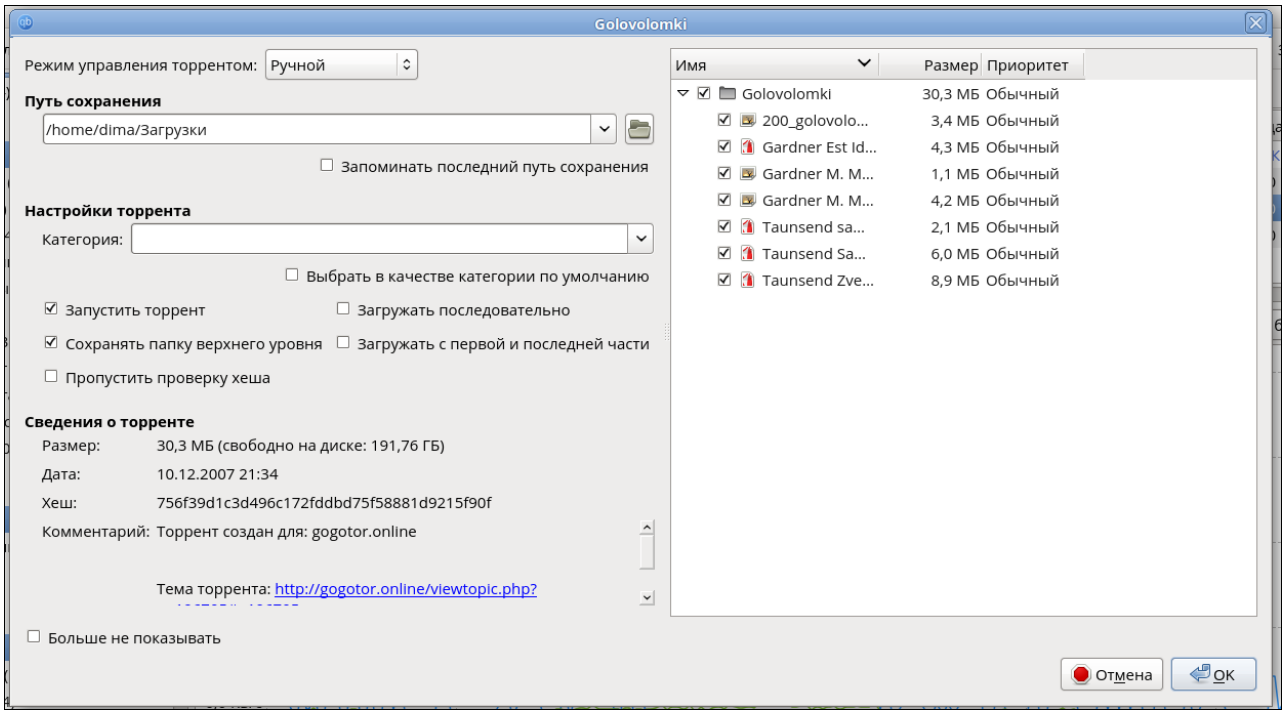
Перейдем к рассмотрению основной закладки программы. Она разделена на 3 части:

1. **Список фильтров** имеющихся торрентов. Если вы активно пользуетесь торрентами, то ваш список может быть довольно большим. Выбрав для отображения категорию, например, по статусу «*Загружаются*», можно увидеть во втором блоке список загружаемых торрентов.
2. **Таблица добавленных в программу торрентов** с некоторыми параметрами, например, процесс загрузки. В каждой строчке отображается отдельный торрент. Выделять группу можно стандартно с помощью зажатой клавиши «*Shift*». Для одиночного или группового выделения доступно контекстное меню с дополнительными функциями.
3. **Блок отображения свойств торрентов**. В нижней части третьего блока имеются кнопки, которые как отображают содержимое, за которое они отвечают, так и скрывают это содержимое, позволяя увеличить область отображения второго блока. Всего кнопок 6 - «*Главное*», «*Трекеры*», «*Пиры*», «*Веб-сиды*», «*Файлы*» и «*Скорость*».



Добавление торрента в загрузку

После получения торрент-файла откройте его с помощью программы qbittorrent, появится окно добавления торрента. Укажите путь сохранения и выберите загружаемый торрент. Остальное можно оставить без изменения. Нажмите «*ОК*», файл добавится в список торрентов программы и начнется процесс загрузки.



transmission

Transmission — самый простой торрент-клиент. Любое действие можно сделать несколькими щелчками мышью. Клиент имеет простую и интуитивно понятную оболочку. **Transmission** использует минимум системных ресурсов компьютера.

В программе очень мало настроек, но они все нужны, чтобы оптимизировать приложение. По сравнению с qbittorrent, тут нет **RSS**, поиска торрентов и других сложных функций, но программа всё равно обладает всем необходимым функционалом. Добавлять в неё торрент-файлы, управлять процессом загрузки и скоростью так же просто. Осталось только попробовать и выбрать понравившуюся программу.

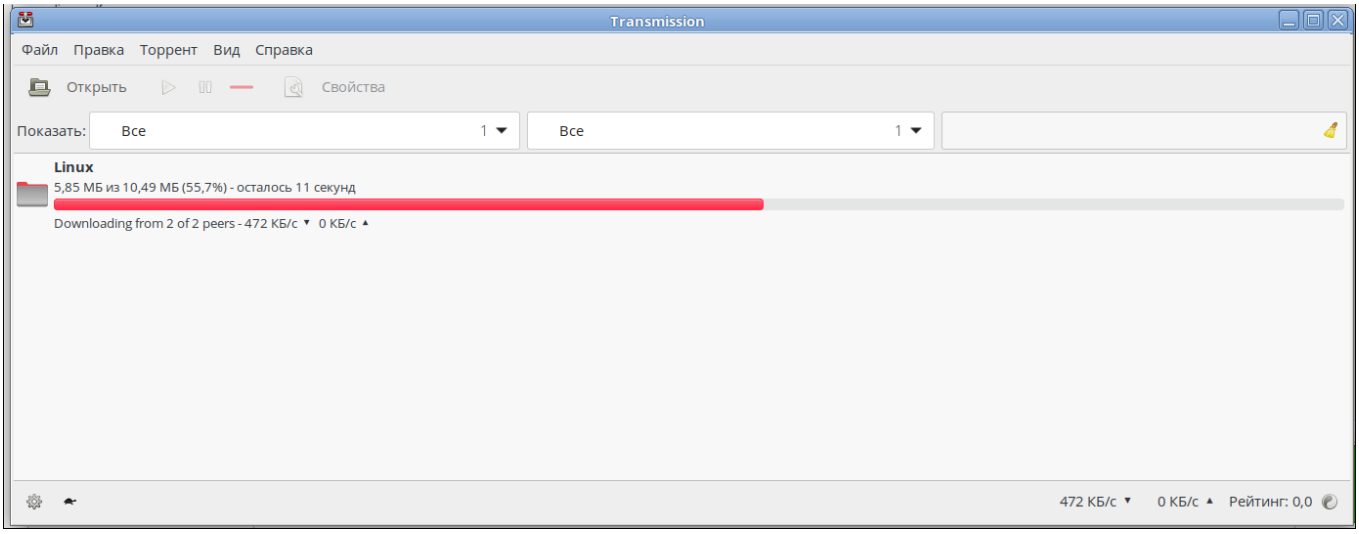
Для установки **transmission** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install transmission
```

После установки программа будет доступна из «**Главного меню**» - «**Интернет**» - «**Transmission**».



Важно отметить, что в данной статье рассмотрены не все функции и возможности торрент-клиентов, а только самые необходимые. Здесь не рассмотрены процесс удалённого доступа к программам, возможность организации трекера и многое другое. Однако, рассмотренных возможностей вполне достаточно, чтобы определиться с выбором программы для работы и перейти к её

использованию и изучению.

Автоматическое обнаружение сторонних ОС с помощью os-prober

Возможности
Вывод информации о других операционных системах
Отображение дополнительных операционных систем при загрузке

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: os-prober-1.77-9

Утилита **os-prober** автоматически обнаруживает другие установленные операционные системы на компьютере и предоставляет результаты в удобном формате, что упрощает идентификацию доступных загрузочных вариантов.

Возможности

Основные возможности утилиты **os-prober**:

- **os-prober** позволяет обнаружить различные операционные системы, установленные на вашем компьютере;
- утилита работает совместно с загрузчиком **grub2** для автоматического обнаружения операционных систем, отличных от Linux;
- **os-prober** поддерживает различные файловые системы.

Вывод информации о других операционных системах

При выполнении в терминале команды os-prober:

```
sudo os-prober
```

Утилита просканирует все доступные диски в системе на наличие других операционных систем и выведет информацию о их наличии на компьютере.

Для каждой обнаруженной ОС будет выведена строка в формате:

```
<раздел>:<описательное_имя>:<короткое_имя>:<тип_загрузчика>
```

Пример вывода:

```
/dev/sda1:Windows 10:Windows:chain
```

Если на диске существует только одна ОС, вывод утилиты будет пустым.

Отображение дополнительных операционных систем при загрузке

Для отключения обнаружения сторонних операционных систем при включении ПК необходимо добавить соответствующий параметр в конфигурационный файл **/etc/default/grub**.

Откройте файл конфигурации **/etc/default/grub** в текстовом редакторе:

```
sudo nano /etc/default/grub
```

Добавьте в конец файла параметр:

```
GRUB_DISABLE_OS_PROBER=true
```

Сохраните файл. Пример файла конфигурации **/etc/default/grub**:



Для применения внесённых настроек в файле **/etc/default/grub** выполните обновление конфигурации **grub2** командой:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Для вступления в силу изменений выполните команду перезагрузки:

```
reboot
```

Оптимизация команд с помощью hyperfine

Установка
Синтаксис
Опции
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: hyperfine-1.17.0-1

Hyperfine — это инструмент командной строки, предназначенный для измерения и сравнения производительности различных команд, алгоритмов или сценариев. Он работает путём многократного запуска команды или сценария и измерения времени, необходимого для её выполнения. Затем он вычисляет среднее время выполнения, медиану и стандартное отклонение, чтобы дать пользователю представление о производительности команды.

Hyperfine учитывает различные факторы, которые могут повлиять на производительность — кеширование, нагрузка на систему и другие процессы, работающие в фоновом режиме. Это позволяет получить более точные результаты и принимать обоснованные решения о том, как оптимизировать свои команды и сценарии.

Установка

Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install hyperfine
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
hyperfine [опции] <команда>
```

Опции

Основные опции утилиты:

- **-w, --warmup <число>** — выполняет число прогревающих запусков перед фактическим тестированием производительности;
- **-m, --min-runs <число>** — выполняет не менее указанного количества запусков для каждой команды (по умолчанию: 10);
- **-M, --max-runs <число>** — выполняет не более указанного количества запусков для каждой команды (по умолчанию ограничения нет);
- **-r, --runs <число>** — выполняет ровно указанное количество запусков для каждой команды (если эта опция не указана, **hyperfine** автоматически определяет количество запусков);
- **-s, --setup <команда>** — выполняет команду перед каждым набором запусков;
- **-p, --prepare <команда>** — выполняет команду перед каждым запуском;
- **-c, --cleanup <команда>** — выполняет команду после завершения всех тестовых запусков для каждой команды;
- **-P, --parameter-scan <значение> <MIN> <MAX>** — выполняет тесты для каждого значения в указанном диапазоне;
- **-D, --parameter-step-size <шаг>** — определяет шаг перебора значений в диапазоне;
- **-L, --parameter-list <значение> <список_значений>** — выполняет тесты для каждого значения из списка;
- **-S, --shell <оболочка>** — устанавливает оболочку, используемую для выполнения команд;
- **-N** — алиас для ***--shell=none*** (оболочка не будет использоваться);
- **-i, --ignore-failure** — игнорирует ненулевые коды возврата тестируемых программ;

- **--style <тип>** — устанавливает стиль вывода:
    - **auto** — автоматически определяет стиль вывода (по умолчанию),
    - **basic** — отключает цветовую схему вывода и интерактивные элементы,
    - **full** — включает все эффекты,
    - **nocolor** — вывод без цвета,
    - **color** — вывод в цвете,
    - **none** — отключает все выходные данные;
- **--sort <метод>** — указывает порядок сортировки сводки сравнения производительности и экспортированных таблиц для форматов разметки (Markdown, AsciiDoc, org-mode):
    - **auto** — автоматически определяет порядок сортировки (по умолчанию),
    - **command** — сортирует результаты по имени команды,
    - **mean-time** — сортирует результаты по среднему времени выполнения команды;
- **-u, --time-unit <единица>** — устанавливает единицу времени (по умолчанию: секунда, возможные значения: миллисекунда, секунда);
- **--export-asciidoc <файл>** — экспортирует сводную статистику синхронизации в виде таблицы AsciiDoc в указанный файл;
- **--export-csv <файл>** — экспортирует сводную статистику синхронизации в формате **CSV** в указанный файл;
- **--export-json <файл>** — экспортирует сводную статистику синхронизации и тайминги отдельных запусков в формате JSON в данный файл;
- **--export-markdown <файл>** — экспортирует сводную статистику времени в виде таблицы Markdown в данный файл;
- **--export-orgmode <файл>** — экспортирует сводную статистику времени как таблицу Emacs в указанный файл;
- **--show-output** — выводит стандартный вывод (stdout) и вывод ошибок (stderr);
- **--output <путь>** — перенаправляет выходные данные:
    - **null** — данные не будут сохранятся или отображаться (по умолчанию);
    - **pipe** — данные будут переданы через канал перед тем, как будут удалены из вывода,
    - **inherit** — данные будут отображены в терминале,
    - **путь к файлу** — вывод будет записан в указанный файл;
- **--input <путь>** — считывает входные данные из заданного файла (null или путь к файлу);
- **-n, --command-name <имя>** — устанавливает команде имя;
- **-h, --help** — выводит справку;
- **-V, --version** — выводит версию программы.

Примеры использования

1. Измерение времени выполнения команды 'ls -l':

```
hyperfine 'ls -l'
```

Результат:

```
Benchmark 1: ls -l
  Time (mean ± σ):      0.7 ms ±  0.6 ms    [User: 0.8 ms, System: 0.7 ms]
  Range (min … max):    0.3 ms …  9.0 ms    267 runs
```

где:

- **Benchmark** — используется для измерения времени выполнения команд или программ;
- **Time** — среднее время выполнения команды, включая стандартное отклонение (σ). Среднее время выполнения команды 'ls -l' составляет 0.7 мс со стандартным отклонением 0.6 мс;
- **Range** — диапазон времени выполнения команды от минимального до максимального значения. Минимальное время выполнения команды составляет 0.3 мс, а максимальное — 9.0 мс.

2. Сравнение времени выполнения нескольких команд ('ls -l' и 'ls -a'):

```
hyperfine 'ls -l' 'ls -a'
```

Результат:

```
Benchmark 1: ls -l
  Time (mean ± σ):      1.5 ms ±  0.5 ms    [User: 0.7 ms, System: 1.1 ms]
  Range (min … max):    1.1 ms …  4.7 ms    928 runs  Benchmark 2: ls -a
  Time (mean ± σ):      0.8 ms ±  0.6 ms    [User: 0.5 ms, System: 0.7 ms]
  Range (min … max):    0.4 ms …  5.7 ms    700 runs  Summary  ls -a ran
    1.87 ± 1.42 times faster than ls -l
```

где:

- **Summary** — сводный итог сравнительной производительности команд (**ls -a** выполнялась в среднем в 1.87 раз быстрее, чем команда **ls -l** со стандартным отклонением 1.42 мс).

3. Выполнение 5 предварительных запусков перед основными измерениями:

```
hyperfine -w 5 'ls -a'
```

Результат:

```
Benchmark 1: ls -a
  Time (mean ± σ):      0.1 ms ±  0.4 ms    [User: 0.5 ms, System: 0.3 ms]
  Range (min … max):    0.0 ms …  4.5 ms    1230 runs
```

4. Ограничение количества запусков команды:

```
hyperfine -M 50 'ls -a'
```

Результат:

```
Benchmark 1: ls -a
  Time (mean ± σ):      0.8 ms ±  0.2 ms    [User: 0.5 ms, System: 0.8 ms]
  Range (min … max):    0.6 ms …  1.3 ms    50 runs
```

5. Экспорт статистики в формате CSV в файл:

```
hyperfine --export-csv sample4.csv 'ls'
```

Результат:

```
Benchmark 1: ls
  Time (mean ± σ):      0.3 ms ±  1.1 ms    [User: 0.5 ms, System: 0.4 ms]
  Range (min … max):    0.0 ms … 13.7 ms    191 runs
```

6. Экспорт статистики и результатов запусков в формате JSON:

```
hyperfine --export-json sample1.json 'ls'
```

Результат:

```
Benchmark 1: ls
  Time (mean ± σ):      0.1 ms ±  0.3 ms    [User: 0.5 ms, System: 0.3 ms]
  Range (min … max):    0.0 ms …  4.2 ms    860 runs
```

7. Направление вывода результатов в файл:

```
hyperfine --output ./3d.txt 'ls -v' -N
```

Результат:

```
Benchmark 1: ls -v
```

```
  Time (mean ± σ):      1.1 ms ±  0.4 ms    [User: 0.3 ms, System: 0.6 ms]
  Range (min … max):    0.9 ms …  5.0 ms    2737 runs
```

Улучшение визуализации различий в коде с утилитой diff-so-fancy

Возможности
Установка
Синтаксис
Опции
Рекомендуемые стандартные цвета
Настройка дополнительных цветов
Сравнение файлов с помощью diff-so-fancy
Настройка внешнего вида diff-so-fancy

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: diff-so-fancy-1.4.4

Утилита **diff-so-fancy** предназначена для улучшения визуального представления вывода команды git diff. Она форматирует вывод, делая его более читаемым и удобным для анализа. Благодаря улучшенному форматированию и цветовой подсветке, разработчики могут легко понять, какие изменения были внесены.

Возможности

Основные возможности **diff-so-fancy**:

1. **Улучшенное форматирование** — выделение изменённых строк и слов внутри строк для лучшей наглядности.
2. **Удаление избыточной информации** — сокрытие ненужных символов и заголовков, что делает вывод более компактным и чистым.
3. **Цветовое выделение** — использование различных цветов для выделения добавленных и удалённых строк.

Установка

Для установки **diff-so-fancy** выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install diff-so-fancy
```

Синтаксис

Утилита **diff-so-fancy** доступна для запуска через терминал при помощи команды следующего вида:

```
diff-so-fancy [--version] [--help] [<опции>] [<аргументы>]
```

Опции

Основные опции утилиты:

- **--width <ширина>** — устанавливает ширину вывода в символах. Например, --width 120 задает ширину 120 символов;
- **--theme <тема>** — применяет заданную тему оформления для вывода;
- **--no-inline** — отключает отображение изменений в строке;
- **--color <цвет>** — настраивает цветовую схему для различных элементов вывода;
- **--ignore-space-change** — игнорирует изменения пробелов при сравнении;
- **--no-abbrev** — отключает укороченное отображение идентификаторов коммитов.

Рекомендуемые стандартные цвета

Для просмотра рекомендованных цветов выполните команду:

```
diff-so-fancy --colors
```

Для настройки цветов включите цветовое отображение:

```
git config --global color.ui true
```

Для настройки цвета обычного текста (ДО изменений) выполните:

```
git config --global color.diff-highlight.oldNormal "red bold"
```

Для настройки цвета выделенного текста (ДО изменений) выполните:

```
git config --global color.diff-highlight.oldHighlight "red bold 52"
```

Для настройки цвета обычного текста (ПОСЛЕ изменений) выполните:

```
git config --global color.diff-highlight.newNormal "green bold"
```

Для настройки цвета выделенного текста (ПОСЛЕ изменений) выполните:

```
git config --global color.diff-highlight.newHighlight "green bold 22"
```

Настройка дополнительных цветов

Для более удобного восприятия изменений в файлах можно настроить дополнительные цвета для различных элементов diff.

Для настройки дополнительных цветов для метаданных выполните:

```
git config --global color.diff.meta "yellow"
```

Git поддерживает стандартные цветовые названия, такие как red, green, blue, yellow, magenta, cyan, white, black и т. д.

Для настройки цветов заголовков фрагментов выполните:

```
git config --global color.diff.frag "magenta bold"
```

Для настройки цветов коммитов выполните:

```
git config --global color.diff.commit "yellow bold"
```

Для настройки цветов строк, которые были удалены или изменены в старой версии файла, выполните:

```
git config --global color.diff.old "red bold"
```

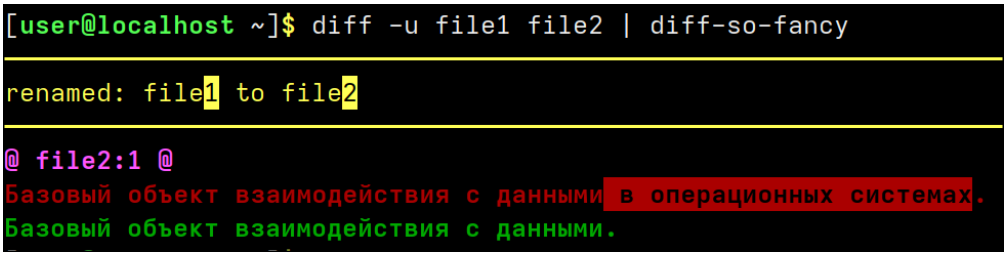
Для настройки цветов пробелов выполните:

```
git config --global color.diff.whitespace "red reverse"
```

Сравнение файлов с помощью diff-so-fancy

Для сравнения содержимого двух файлов с помощью утилиты **diff-so-fancy** введите следующую команду:

```
diff -u file1 file2 | diff-so-fancy
```



Эта команда улучшает восприятие результатов сравнения, делая их более удобными для анализа.

Настройка внешнего вида diff-so-fancy

Утилита **diff-so-fancy** предоставляет гибкие возможности для настройки отображения изменений, позволяя адаптировать вывод под предпочтения пользователя.

Для настройки вывода через аргументы командной строки, используйте следующую команду:

```
git diff --color | diff-so-fancy --width 120 --theme solarized-dark
```

где:

- **--width 120** — устанавливает ширину вывода в 120 символов;
- **--theme solarized-dark** — применяет тему оформления solarized-dark.

Ведение финансового учета с помощью kmymoney

Возможности
Установка
Настройка
Описание
Счета
Создание графиков
Статьи бюджета
Метки
Контрагенты
Книга учёта
Инвестиции
Отчёты
Бюджеты
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kmymoney-5.1.3

KMyMoney — это бесплатная программа для ведения домашней бухгалтерии, которая предлагает широкий спектр функций, сравнимых с коммерческими программами управления личными финансами.

KMyMoney не предназначена для удовлетворения потребностей среднего и крупного бизнеса, но может быть подходящим решением для малого бизнеса. Она может быть адаптирована под требования данной категории пользователей с помощью дополнительных модулей.

Возможности

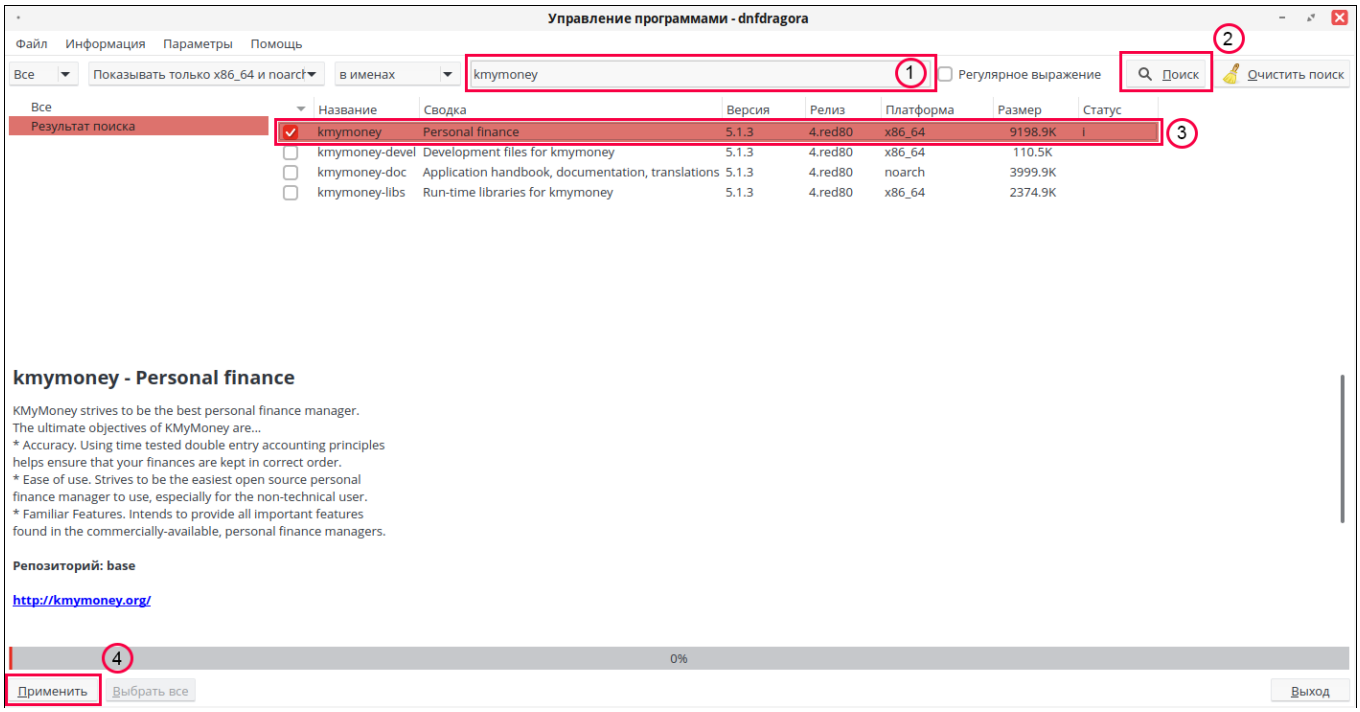
Основные возможности **KMyMoney**:

- поддерживает несколько валют, что позволяет вести учёт в разных валютах одновременно;
- позволяет создавать и управлять несколькими счетами, что удобно для учёта доходов и расходов по разным категориям;
- позволяет создавать бюджеты и отслеживать их выполнение;
- предоставляет инструменты для анализа финансовых показателей;
- поддерживает импорт и экспорт данных в различных форматах, что упрощает обмен данными с другими программами;
- синхронизирует данные с облачными сервисами, такими как Dropbox или Google Drive;
- обеспечивает защиту данных с помощью шифрования и паролей;
- отправляет пользователям напоминания о предстоящих платежах и событиях, связанных с финансами;
- предоставляет пользователям различные графики и диаграммы, которые помогают визуализировать финансовые данные и лучше понимать их.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kmymoney**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install kmymoney
```

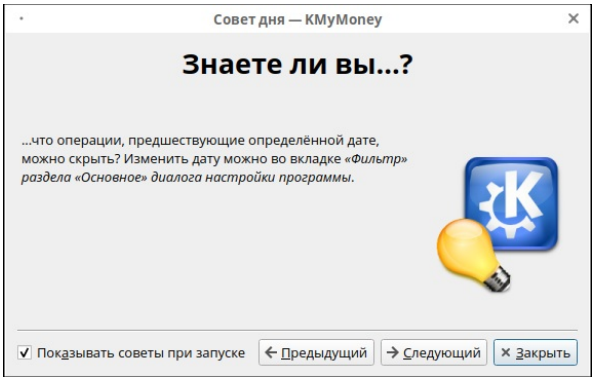
Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Для запуска программы через терминал введите команду:

```
kmymoney
```

После установки программа будет доступна из «**Главного меню**» — «**Офис**» — «**KmyMoney**».

Настройка

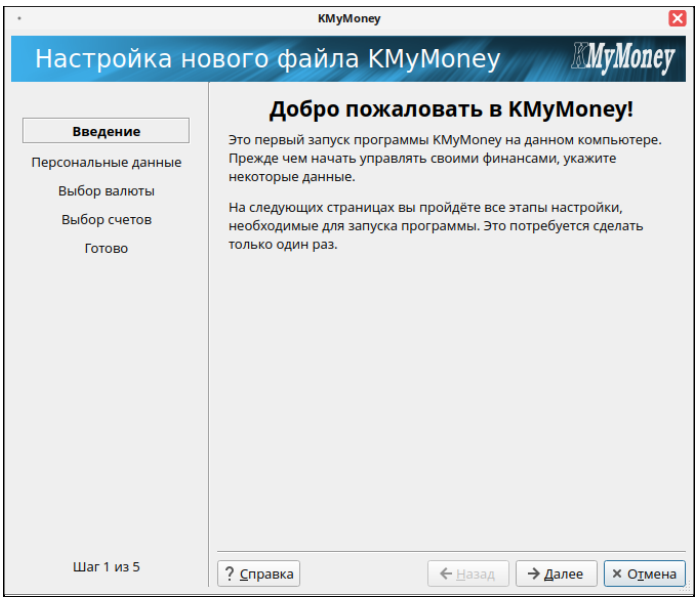
По завершении загрузки **KMyMoney** будут показаны два окна. Первое окно «**Совет дня**» содержит полезные советы по работе с приложением.



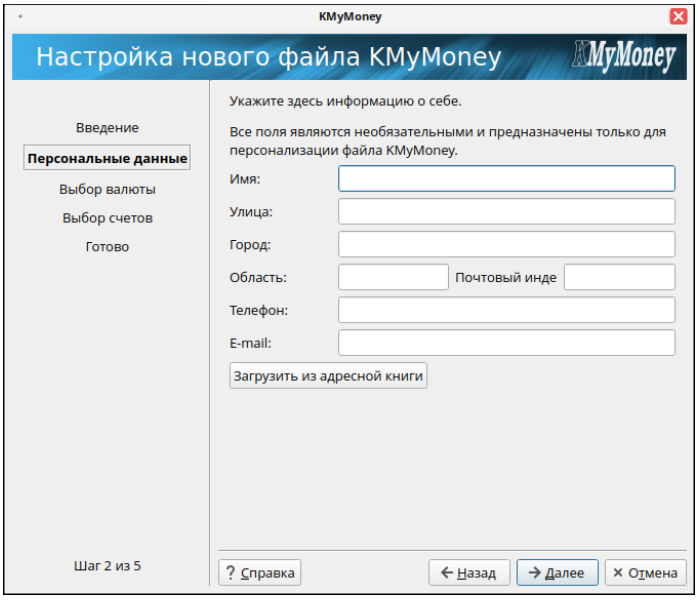
Рекомендуется ознакомиться с содержанием советов. По умолчанию окно будет показано вновь при следующем запуске **KMyMoney**. Для его отключения снимите соответствующий флаг «**Показывать советы при запуске**».

Для включения окна с советами выберите в меню «**Справка**» — «**Показывать совет дня**». Чтобы закрыть диалог «**Совет дня**», нажмите кнопку «**Закрыть**».

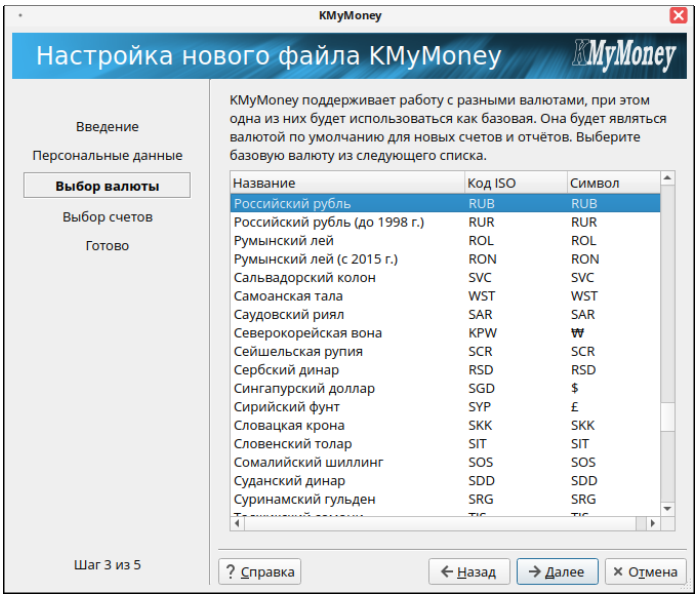
При первом запуске **KMyMoney** необходимо провести первоначальную настройку в соответствии с целями, для которых используется приложение. Так как все поля являются необязательными, можно оставить их пустыми и продолжить использовать **KmyMoney.**



Укажите имя и адрес и нажмите кнопку «**Далее**».

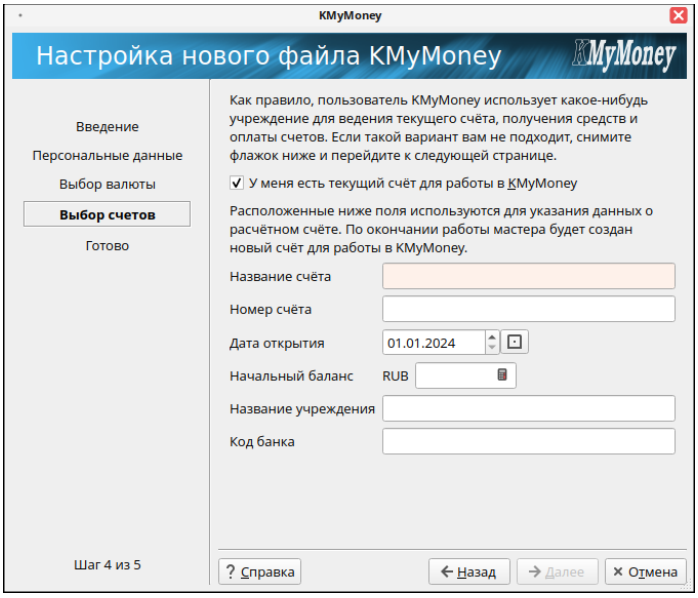


В **KMyMoney** можно работать с несколькими валютами, но одна будет использоваться как базовая. Задайте базовую валюту и нажмите кнопку «**Далее**». В приведённом примере в качестве базовой валюты выбран Российский рубль.



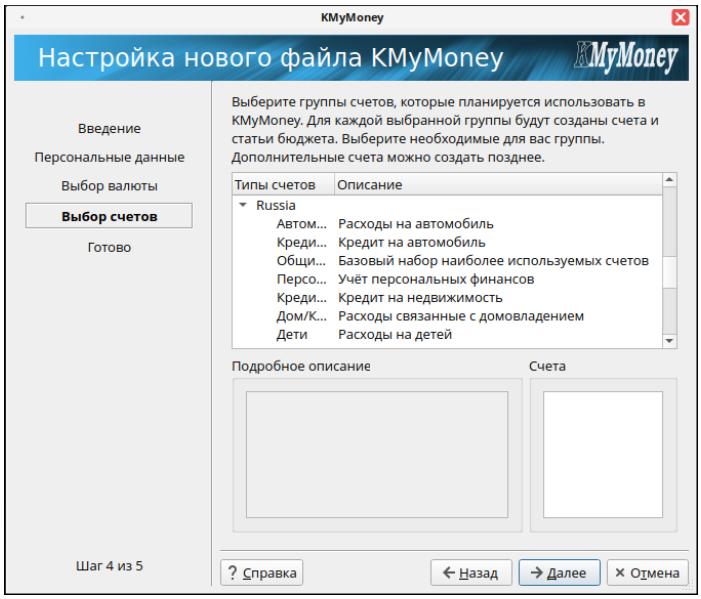
Укажите название и номер счёта. Введите дату открытия счёта и его начальный баланс. Для управления финансовыми данными, начиная с 1 января 2024 года, укажите баланс счёта на эту дату. Нужное значение можно узнать из банковской выписки. Далее укажите название и код учреждения (для работы с онлайн-банком).

Если создавать начальный счёт не требуется, снимите соответствующий флаг. По завершении ввода данных перейдите к следующему шагу, нажав кнопку «**Далее**».

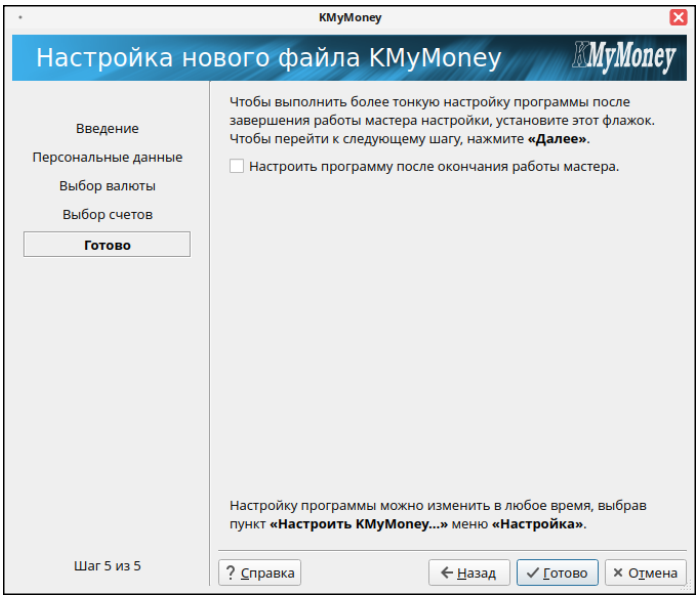


Выберите страну и шаблон. Каждый шаблон имеет свой набор статей бюджета для организации финансовых данных. Чтобы выбрать несколько шаблонов, зажмите **Ctrl**, затем щёлкните по нужным шаблонам. Программа отобразит иерархию счетов в области предварительного просмотра.

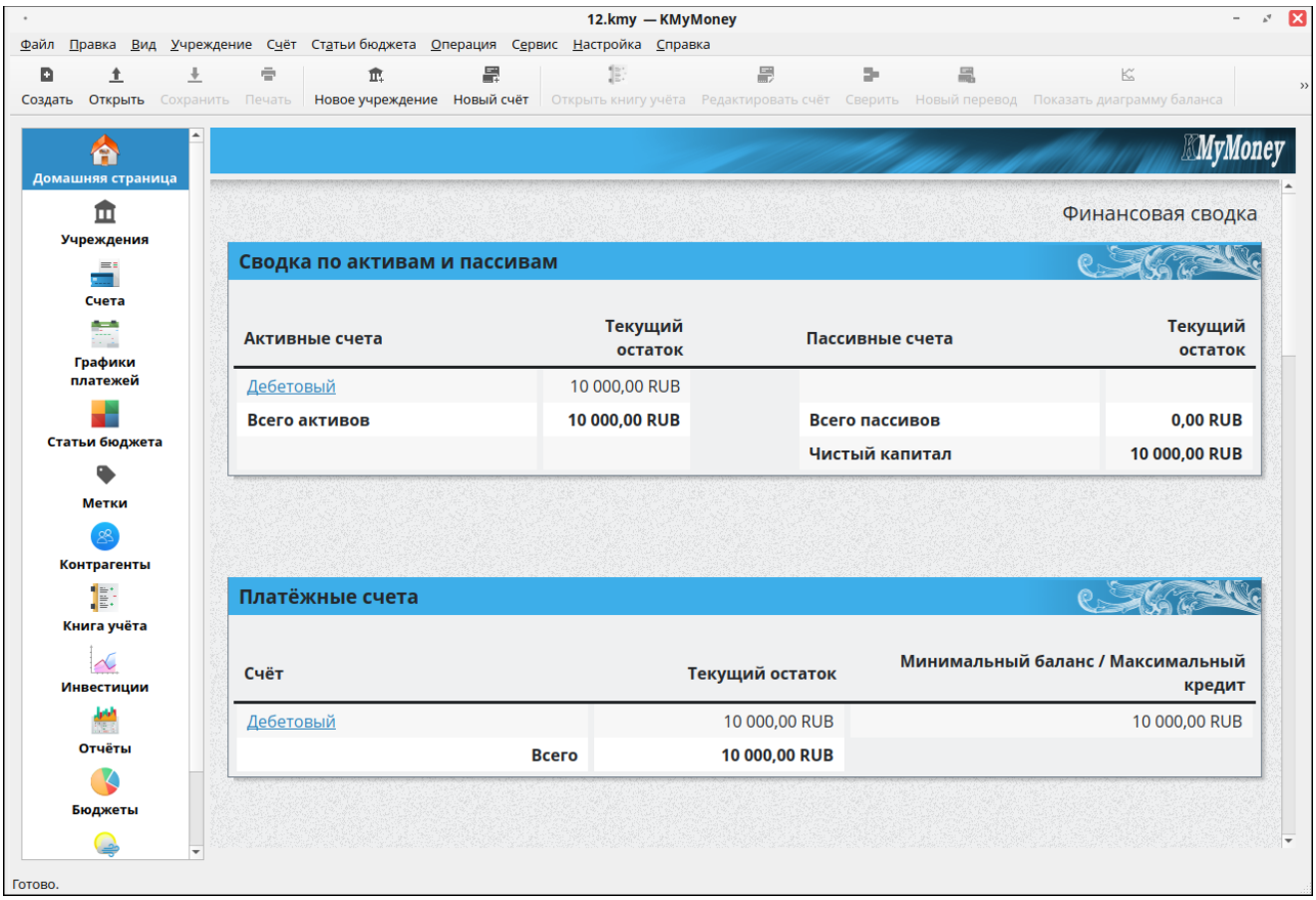
Если вам не удаётся найти подходящий шаблон, вы можете пропустить этот шаг и настроить статьи бюджета вручную позже. Затем вы сможете настроить пользовательские предпочтения. Если вы установили соответствующий флаг, после окончания работы мастера будет показан диалог настройки параметров приложения. Введите все необходимые данные и нажмите кнопку «**Далее**» для продолжения.



На последней странице мастера можно выбрать расширенную настройку программы. После первоначальной настройки приложение готово к работе. Нажмите кнопку «**Готово**».

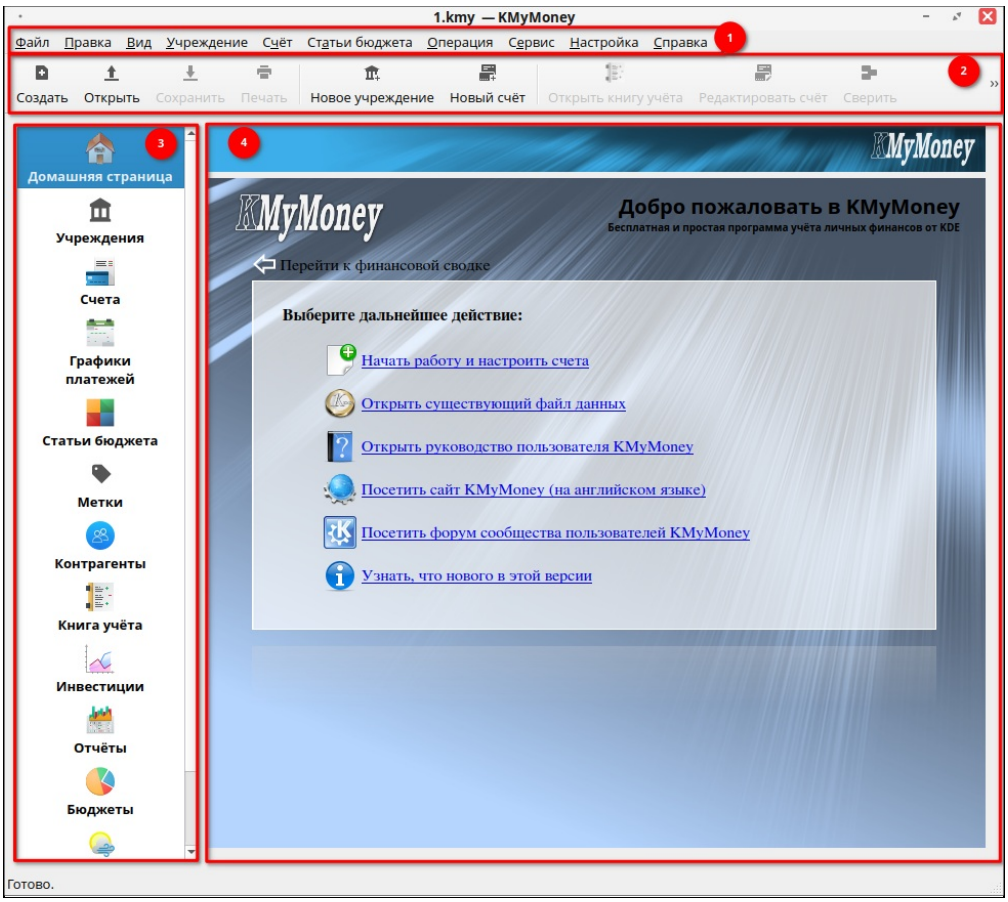


KMyMoney создаст и откроет файл.



Описание программы

Главное окно программы выглядит следующим образом:



1. **Основное меню** программы — здесь собраны основные возможности программы.

2. **Панель инструментов** — настраиваемая панель для быстрого доступа к наиболее востребованным функциям программы. Для её настройки перейдите в пункт меню «**Настройки**» — «**Панели инструментов...**».

3. **Меню выбора представления**. В этом меню отображаются различные варианты просмотра финансовых данных. Можно выбрать из доступных представлений, которые зависят от установленного программного обеспечения. Модули, подключенные к программе, могут добавить новые варианты. Щёлкните по значку, чтобы открыть соответствующее представление в области просмотра. Каждое представление обеспечивает детализированный обзор финансового положения, предоставляя доступ к просмотру и редактированию соответствующих данных.

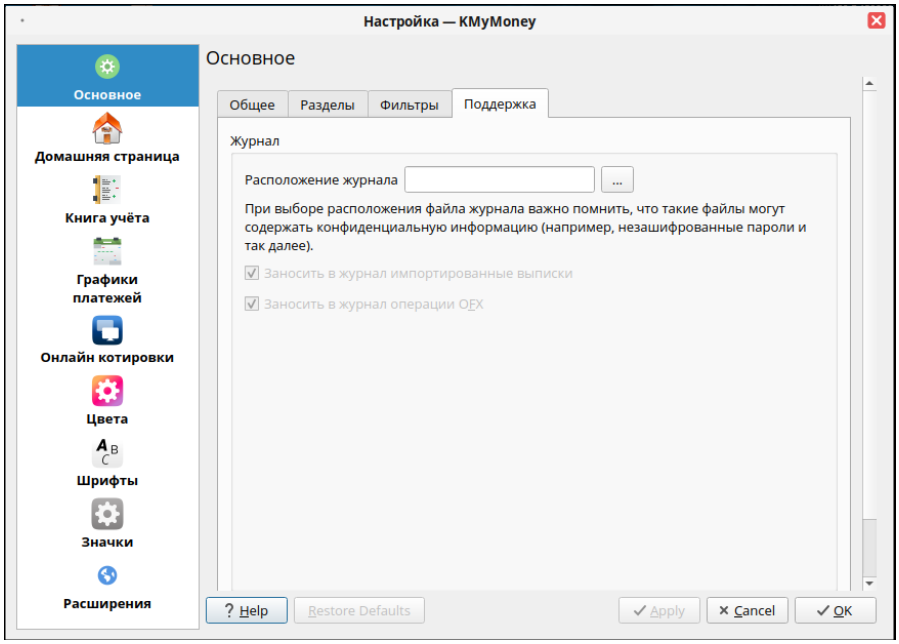
Меню выбора представления содержит следующие значки:

- **Домашняя страница**: отображение сводных данных о вашем финансовом положении.
- **Учреждения**: иерархическое представление всех учреждений и счетов, связанных с ними.
- **Счета**: иерархическое представление всех счетов, позволяющее просматривать и управлять вашими финансами.
- **Графики платежей**: отображение повторяющихся выплат и поступлений, помогающее планировать ваш бюджет.
- **Статьи бюджета**: специальные счета, которые группируют связанные операции.
- **Метки**: дополнительные счета, которые могут быть использованы в сочетании со статьями бюджета для группировки связанных операций.
- **Контрагенты**: список всех контрагентов, с которыми вы работаете, включая лица и учреждения, которым вы платите или от которых получаете деньги.
- **Книга учёта**: подробный журнал операций по счетам.
- **Инвестиции**: обзор портфеля ценных бумаг.
- **Отчёты**: набор полезных отчётов,который позволяет просматривать ваше финансовое состояние с различных сторон.
- **Бюджеты**: ваши бюджеты.

- **Прогноз**: представление, которое позволяет просматривать прогноз для счетов и статей.
- **Исходящие**: представление, используемое модулем сетевой работы с банками для отображения сообщений о выполненных операциях.

4. **Область просмотра**. Данная область предназначена для работы с текущей вкладкой рабочей панели.

Для расширенной настройки **KMyMoney** выберите пункт «**Настройка**» — «**Настроить KMyMoney...**». Будет открыто окно настройки, в котором можно персонализировать программу:



Счета

Счета используются для создания операций. Операции могут быть связаны с одним или несколькими счетами.

Счета-Активы — это счета, на которых хранятся деньги и имущество, которое требуется отслеживать. Типы активов:

- Текущий счёт,
- Сберегательный счёт,
- Наличные,
- Ссудный счёт,
- Инвестиции,
- Актив (имущество, коллекции и т.д.).

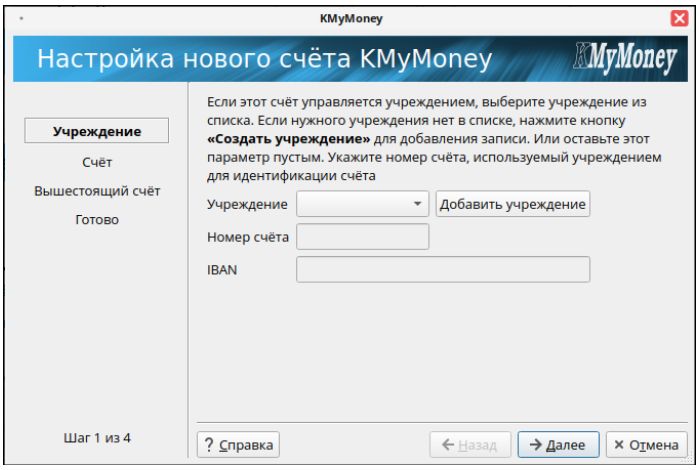
Счета-Пассивы — это счета, которые представляют долги и заёмные средства, которые требуется отслеживать. Типы пассивов:

- Кредитная карта,
- Ссудный счёт,
- Пассив (любое обязательство пользователя, отличное от кредита).

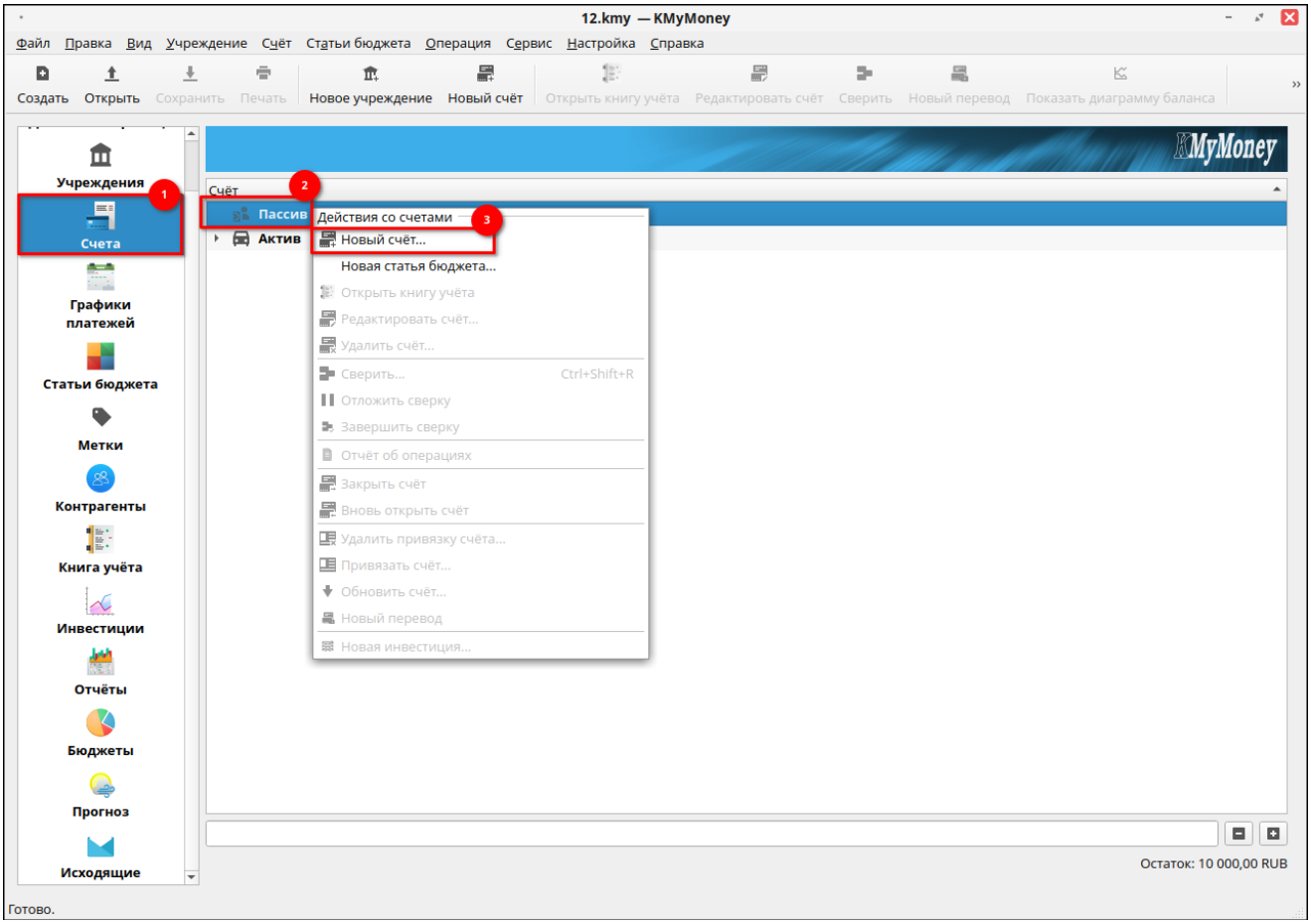
В представлении «**Счета**» можно внести информацию о наличных деньгах и пластиковых картах.

Существует несколько способов создания счёта. При любом способе вызывается **Мастер создания нового счета**. Мастер позволяет поэтапно указать сведения о счёте. Создайте счёт с помощью одного из нижеприведенных способов.

1. Для создания счёта с помощью меню выберите пункт меню «**Счёт**» **—** «**Новый счёт...**».



2. Для создания счёта с помощью представления счетов откройте представление «**Счета**» (1). Щёлкните ПКМ по значку дерева «**Пассивы**» (2) или «**Активы**» в рабочей области и выберите в контекстном меню пункт « **Новый счёт...**» (3).



3. Для создания счёта с помощью панели инструментов нажмите на значок «**Новый счёт**».

Для отслеживания счёта с помощью **KMyMoney** выберите счёт в меню « **Файл**» — «**Создать**».

Если ранее использовалась другая программа для управления личными финансами, её данные можно импортировать в **KMyMoney**.

Сводная информация по счетам будет показана на домашней странице.

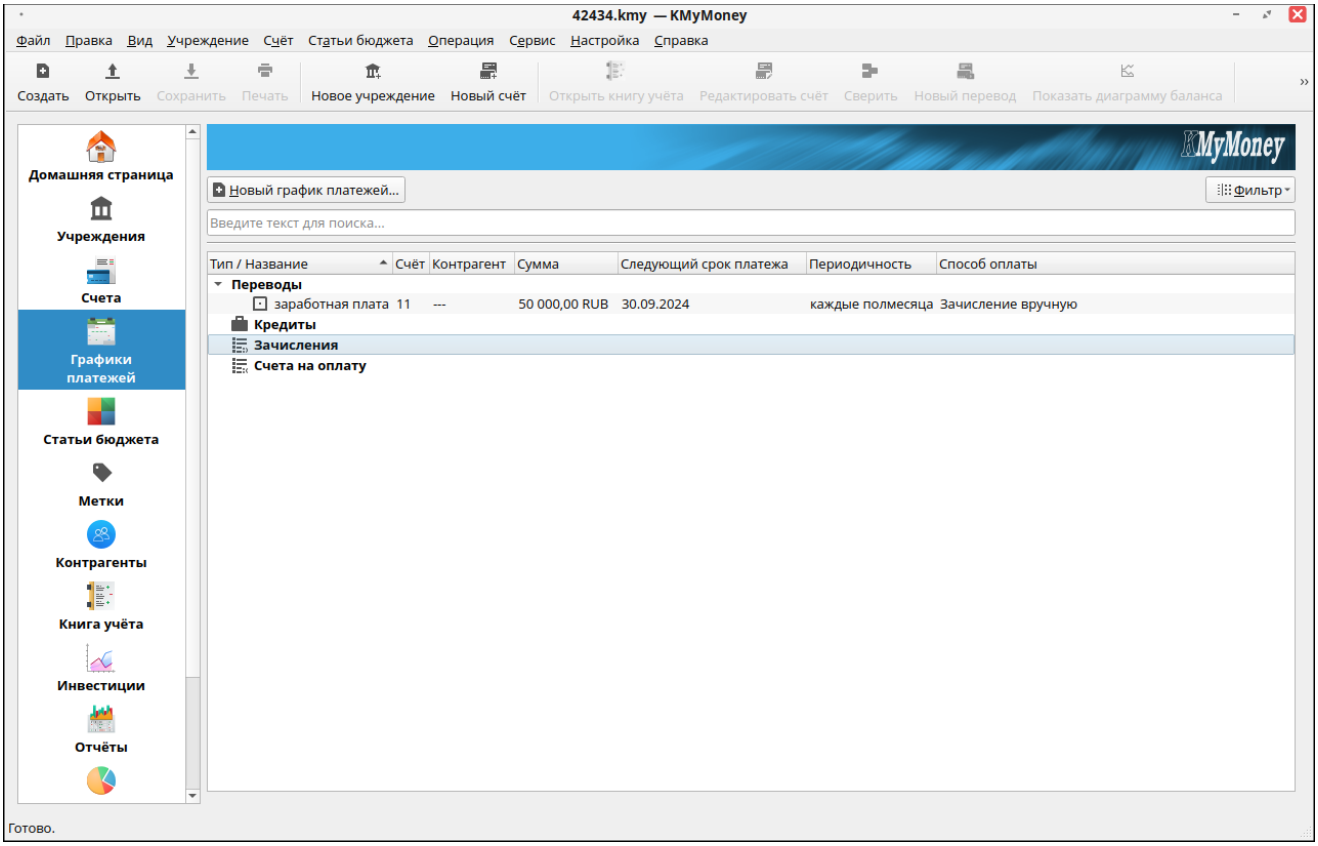
Операции можно создавать вручную в «**Книге учёта**» или автоматически, выполнив настройку параметров в представлении «**Графики**».

Создание графиков

С помощью графиков можно отражать поступление или расходование денежных средств, которое происходит на регулярной основе: платежи по заработной плате, налогам и сборам, страховке, кредитным картам, кредитам, ипотеке, аренде и коммунальным платежам. Планирование регулярных выплат позволяет получать напоминания.

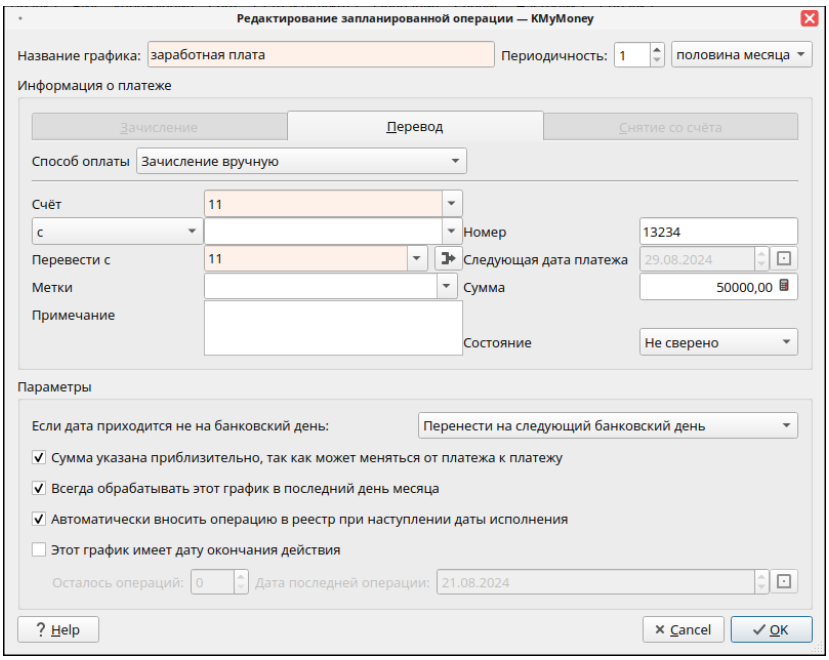
Типы графиков:

- **Переводы** — предназначен для средств, которые снимаются с одного счёта и поступают на другой;
- **Кредиты** — предназначен для работы с кредитным счётом;
- **Зачисления** — предназначен для средств, поступающих на счёт;
- **Счета на оплату** — предназначен для средств, выплачиваемых со счета.



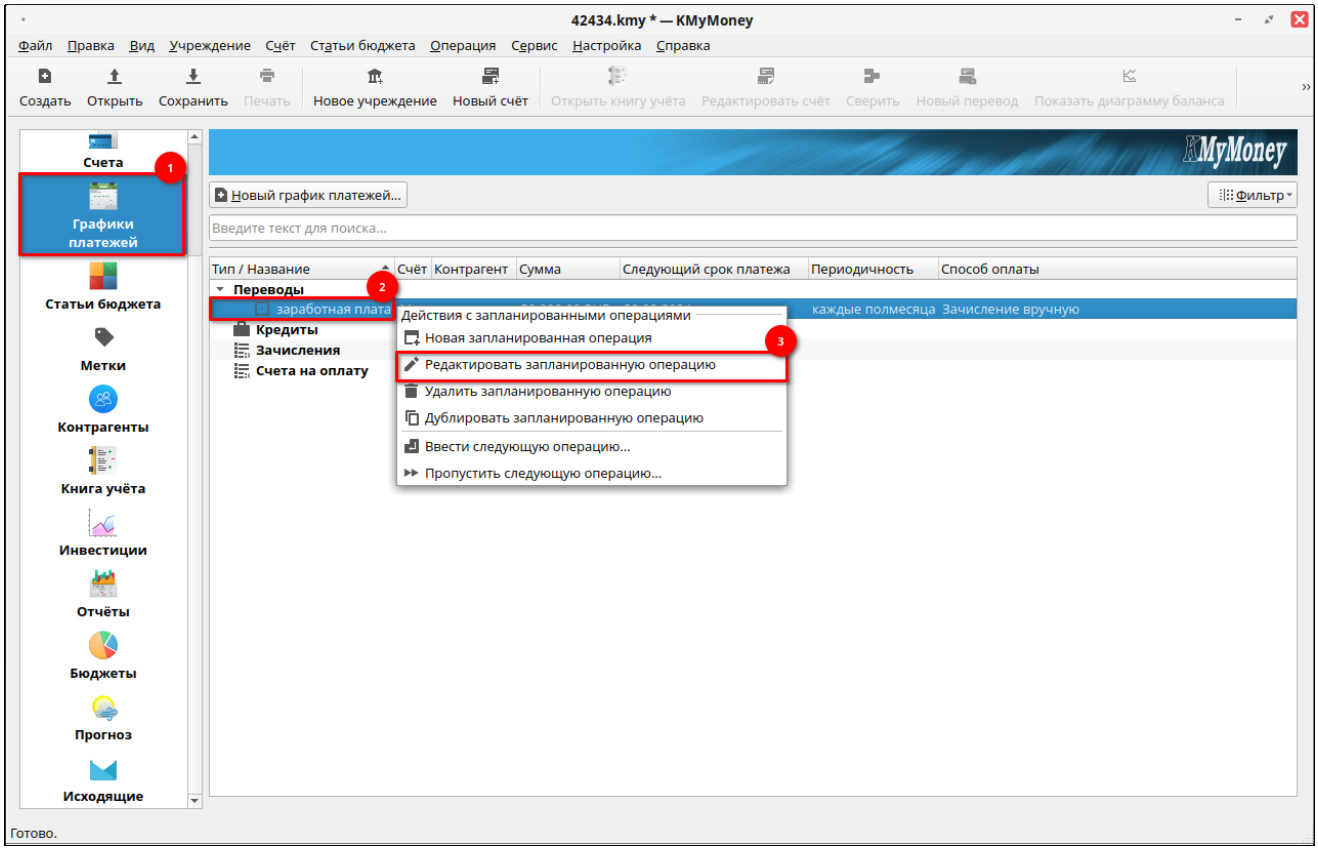
Для настройки графика платежей щёлкните по значку «**Графики**» в меню выбора представления. Необходимо указать следующие данные:

- Название графика,
- Периодичность,
- Способ оплаты,
- Следующая дата платежа,
- Сумма,
- Параметры операций,
- Параметры расписания.



По завершении настройки нажмите кнопку «**OK**».

Для редактирования графика выберите его в списке, щёлкните по нему ПКМ и выберите в контекстном меню пункт « **Редактировать запланированную операцию**».



Появится диалоговое окно, в котором можно указать необходимые данные.

Для удаления графика выберите график, щёлкните по нему ПКМ и выберите в контекстном меню пункт « **Удалить запланированную операцию**».

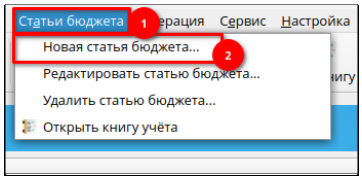
Для дублирования графика щёлкните по нему ПКМ и из контекстного меню выберите опцию « **Дублировать запланированную операцию**».

Статьи бюджета

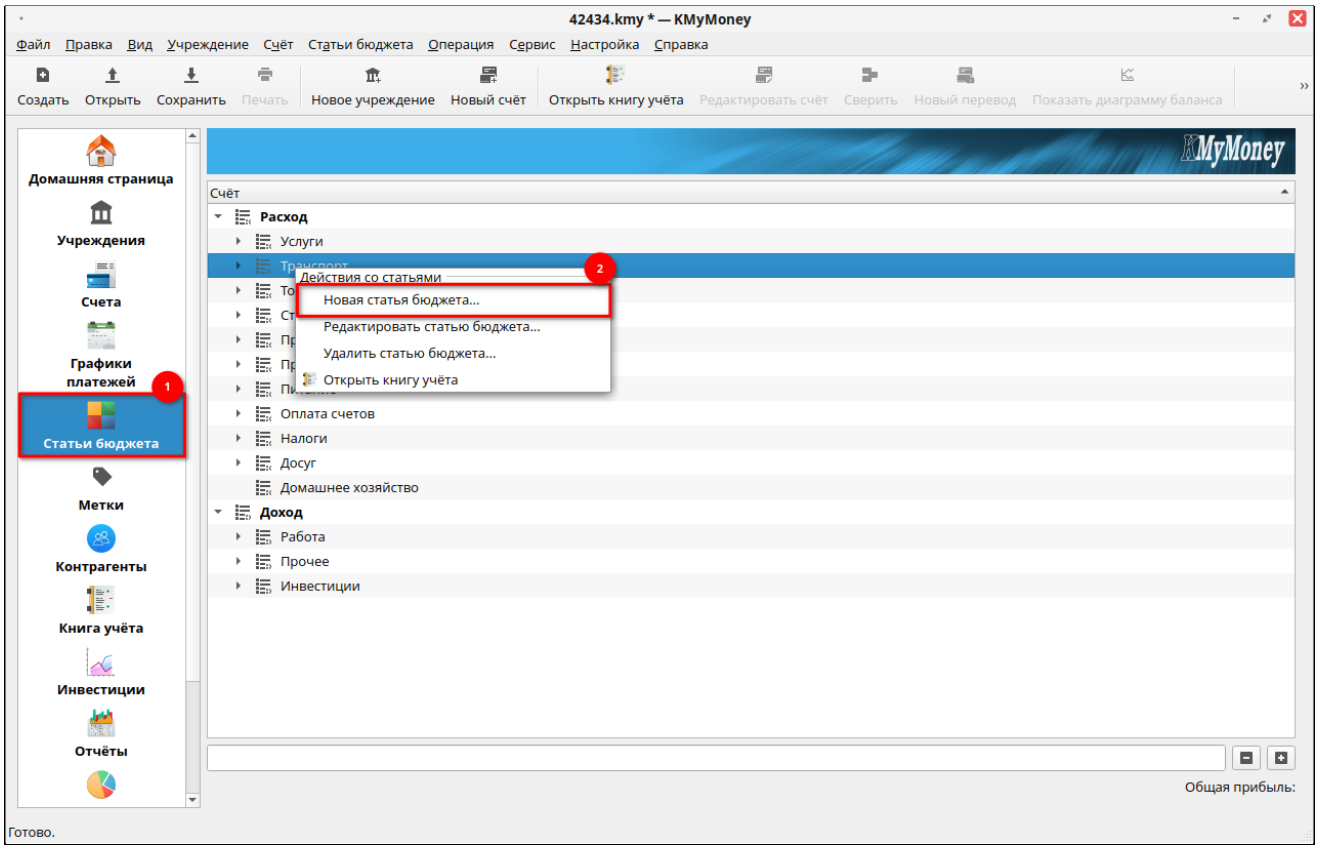
В представлении «**Статьи бюджета**» создаются статьи расходов и доходов. Для каждой из статей бюджета отображается общая сумма по операциям.

Для создания статьи выберете один из следующих способов.

1. Выберите пункт меню «**Статьи бюджета**» (1) — «**Новая статья бюджета...**» (2).



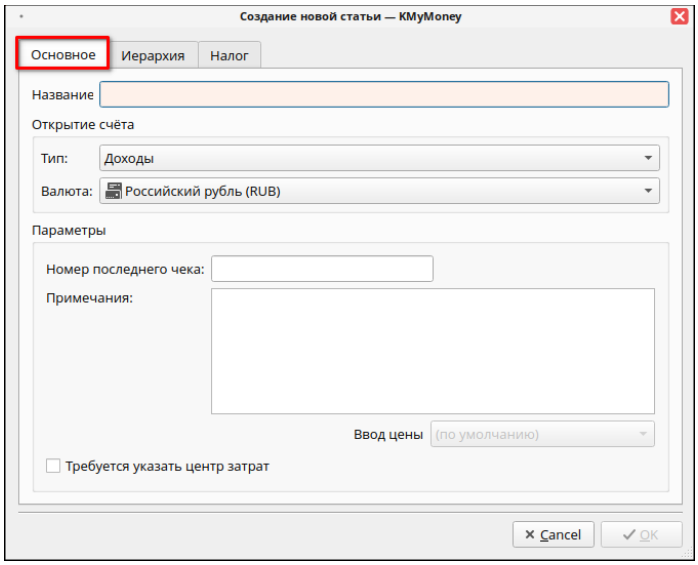
2. Выберите родительский элемент в дереве представления «**Статьи бюджета**» (1), щёлкните по нему ПКМ и выберите в контекстном меню пункт «**Новая статья бюджета...**» (2).



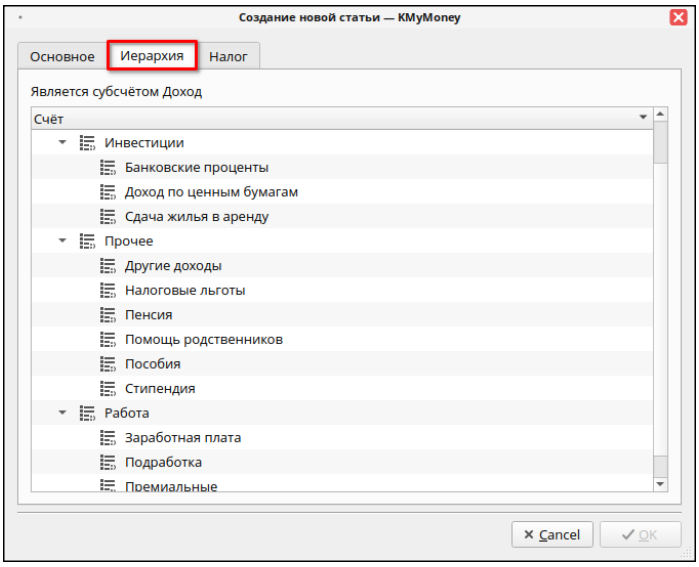
3. Укажите название новой статьи при добавлении или редактировании операции в книге учёта.

При любом способе будет открыто диалоговое окно «**Создание новой статьи**», которое содержит три вкладки: «**Основное**», «**Иерархия**», «**Налог**». На каждой из них можно изменить определённые параметры статьи.

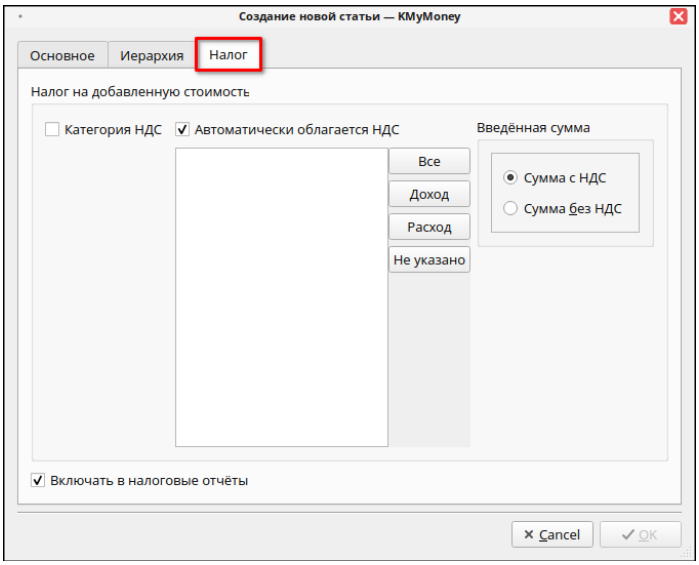
Вкладка «**Основное**» содержит редактируемые поля, в которых можно указать название, тип и валюту, а также поля « **Номер последнего чека**», «**Примечания**» и флаг «**Требуется указать центр затрат**».



На вкладке «**Иерархия**» для статьи можно выбрать подходящий вышестоящий счёт.



На вкладке «**Налог**» можно указать или изменить параметры НДС, а также установить флаг для включения статьи в налоговые отчёты. Статью расходов или доходов можно преобразовать в статью НДС и указать процентную ставку.



Для настройки статьи бюджета щёлкните по значку в меню выбора представления. Представление «**Статьи бюджета**» содержит сводные данные по всем существующим в текущей базе данных статьям бюджета. Статьи подразделены на доходы и расходы и расположены в алфавитном порядке. Для каждой из статей показано соответствующее значение баланса.

Для редактирования статьи щёлкните по её названию ПКМ и выберите в контекстном меню пункт « **Редактировать статью бюджета...**».

Для удаления статьи выберите её в дереве статей, щёлкните по ней ПКМ, в открывшемся контекстном меню нажмите « **Удалить**». Если со статьёй не связаны операции, графики платежей или бюджеты, она не установлена в качестве статьи по умолчанию для новых операций, она будет удалена.

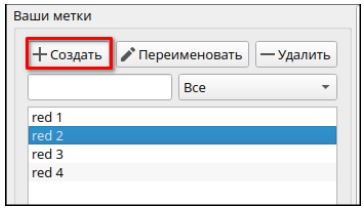
При удалении статей, имеющих связи, будет предложено определить другую статью для привязки связанных элементов или выбрать, следует ли удалять подкатегории.

Метки

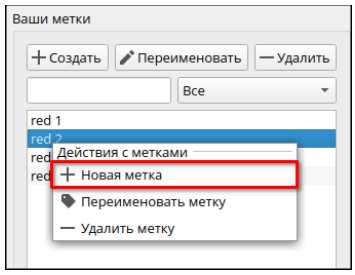
Представление «**Метки**» представляет собой счёта без управления, которые не имеют стоимости, использовать их необязательно.

Добавить новую метку можно тремя способами.

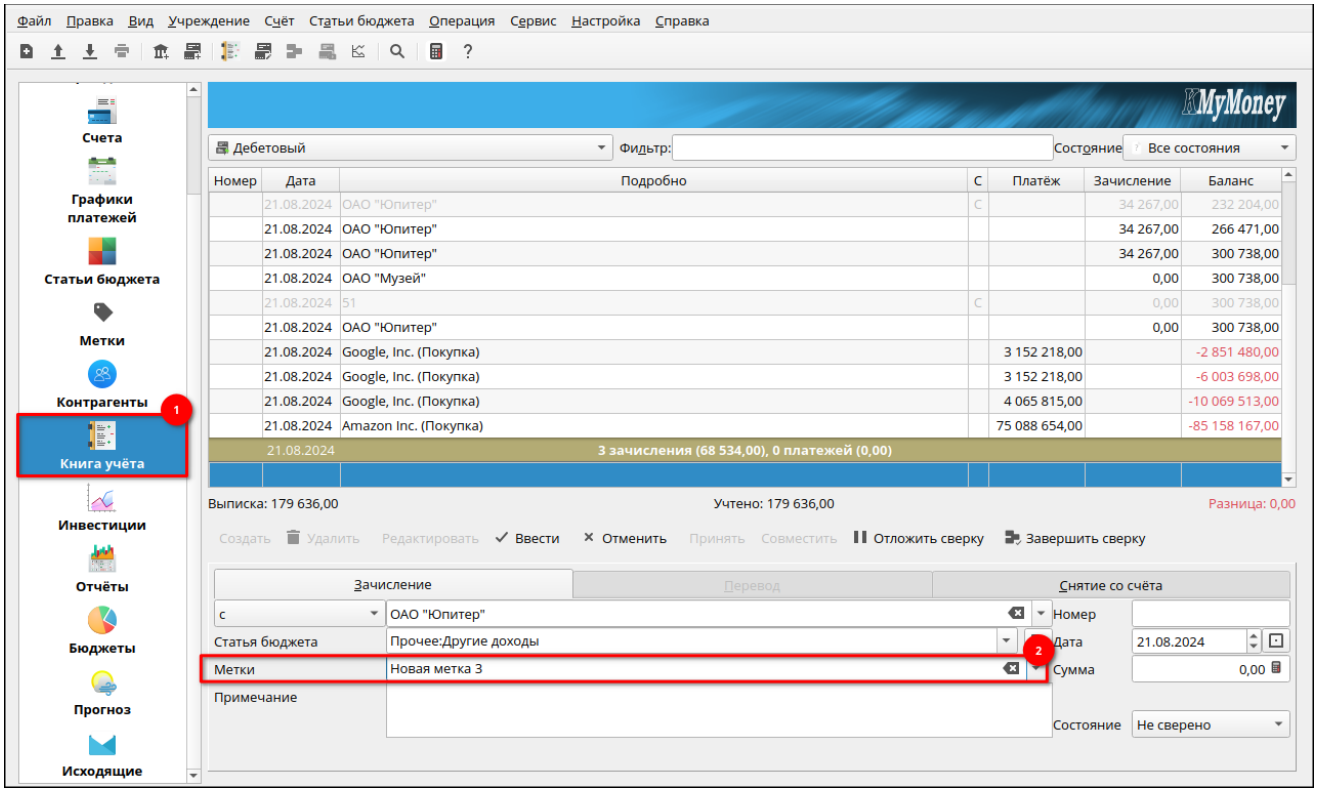
1. Щёлкните по кнопке «**Создать**», расположенной над списком меток.



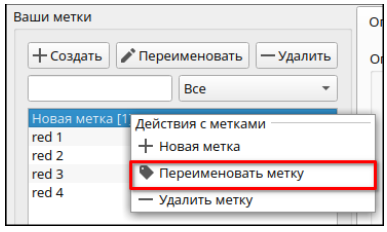
2. Щёлкните ПКМ по любой метке и выберите в контекстном меню пункт «**Новая метка**».



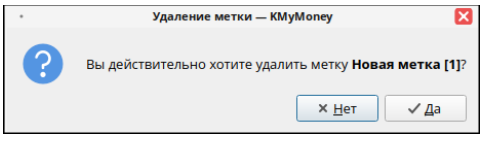
3. Введите название в поле «**Метки**» непосредственно на странице книги учёта или в окне разбивки операции.



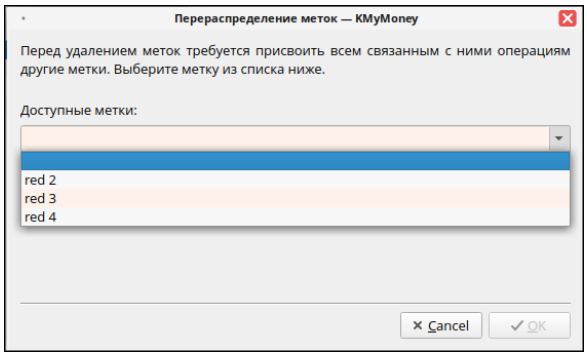
Для переименования метки щёлкните по её названию ПКМ и выберите в контекстном меню пункт « **Переименовать метку**».



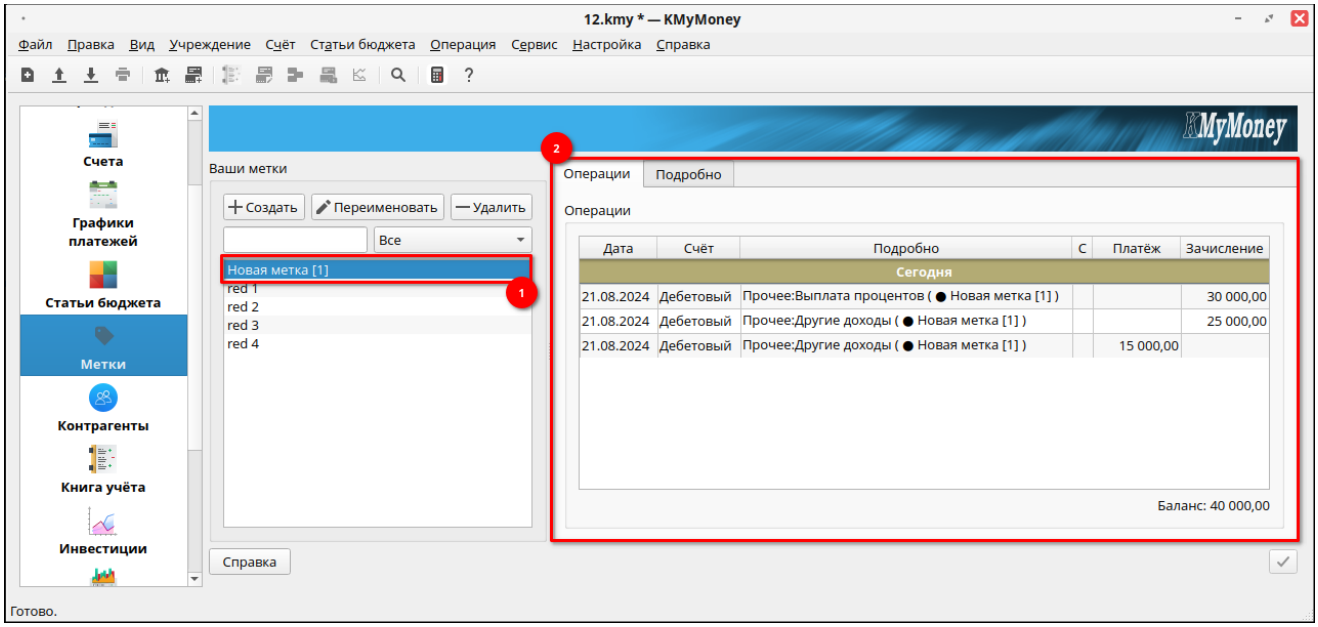
Для удаления метки щёлкните по её названию ПКМ и выберите в контекстном меню пункт «**Удалить метку**».



Если метка используется для каких-либо операций, появится диалоговое окно, которое позволяет назначить для них другую метку.

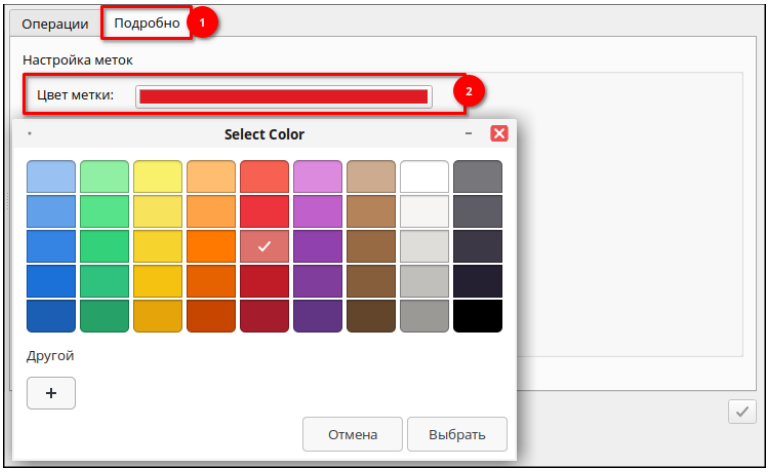


Для просмотра или редактирования операций, связанных с конкретной меткой выберите метку в списке и затем выберите соответствующую вкладку в правой части диалогового окна.



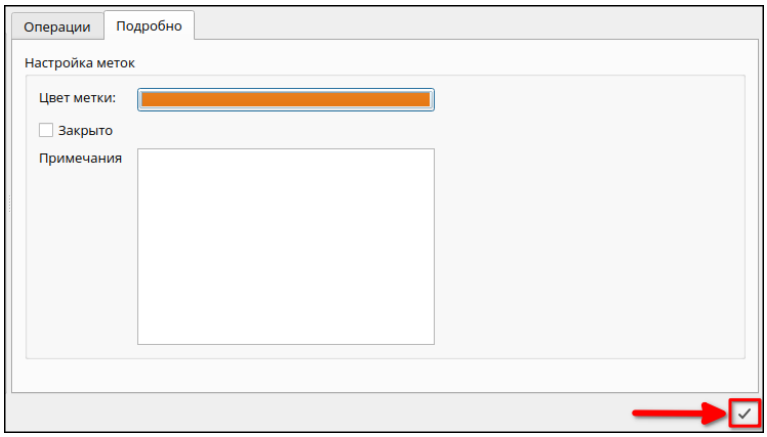
Для просмотра списка операций, для которых назначена выбранная метка, перейдите на вкладку «**Операции**». По двойному щелчку по записи операции она будет показана в книге учёта для счета, на котором к операции была добавлена метка.

Для просмотра и редактирования сведений, связанных с конкретной меткой, перейдите на вкладку «**Подробно**». Для вызова диалогового окна выбора цвета щёлкните по цветовой полосе.



Установка флага «**Закрыто**» сделает невозможным использование метки для новых операций.

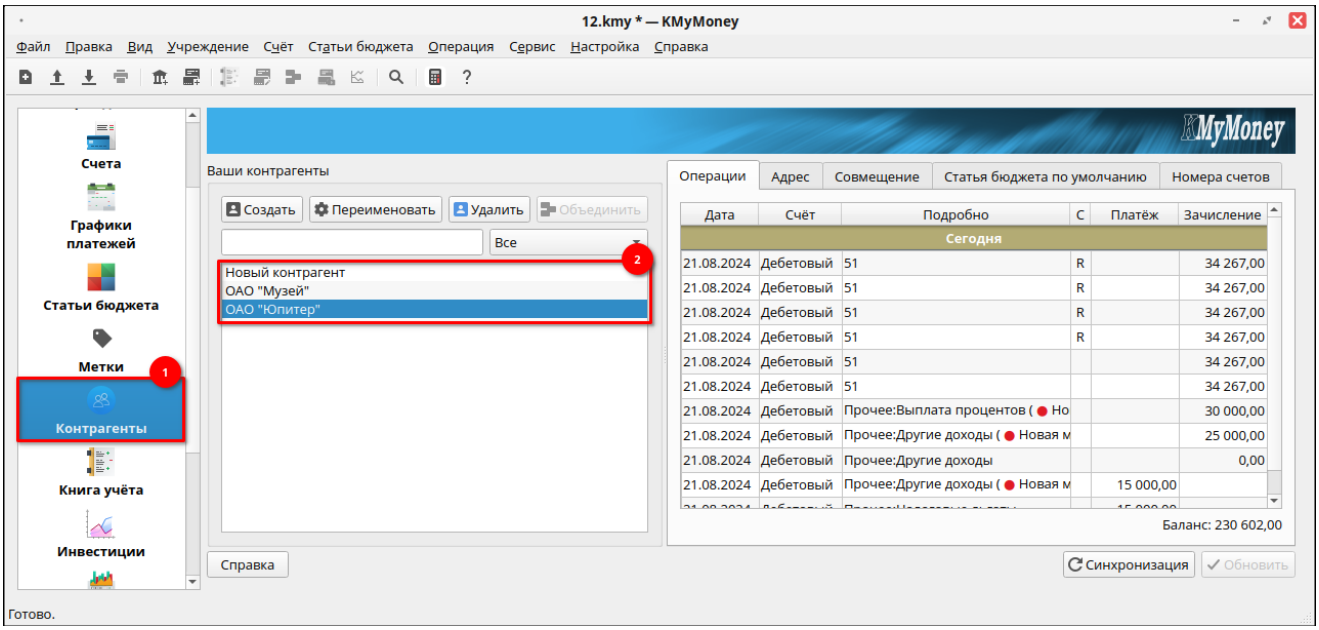
По завершении настройки нажмите кнопку «**Принять**», которая расположена в правой нижней части окна.



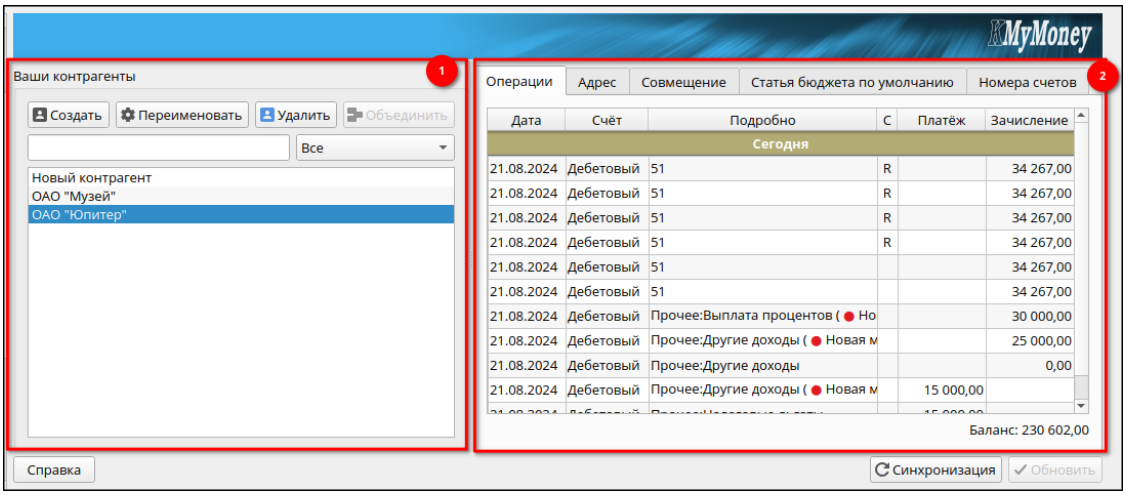
Контрагенты

Представление «**Контрагенты**» (1) содержит подробные сведения обо всех получателях и плательщиках, участвующих в операциях.

Сведения о контрагентах сохраняются на основе существующих операций, можно выбрать получателя из списка (2).



Представление «**Контрагенты**» содержит основные две области: «**Ваши контрагенты**» (1) и **область сведений** (2).



В области «**Ваши контрагенты**» можно создавать, переименовывать, удалять и объединять записи контрагентов. Контрагенты в списке упорядочены по алфавиту.

В **области сведений** доступны вкладки: операции, адрес, совмещение, статья бюджета по умолчанию и номера счетов для выбранного контрагента.

Для просмотра всех операций, связанных с контрагентом, выберите его в списке и перейдите в область сведений на вкладку

«**Операции**». Для открытия операции в «**Книге учёта**» дважды щёлкните по интересующей операции.

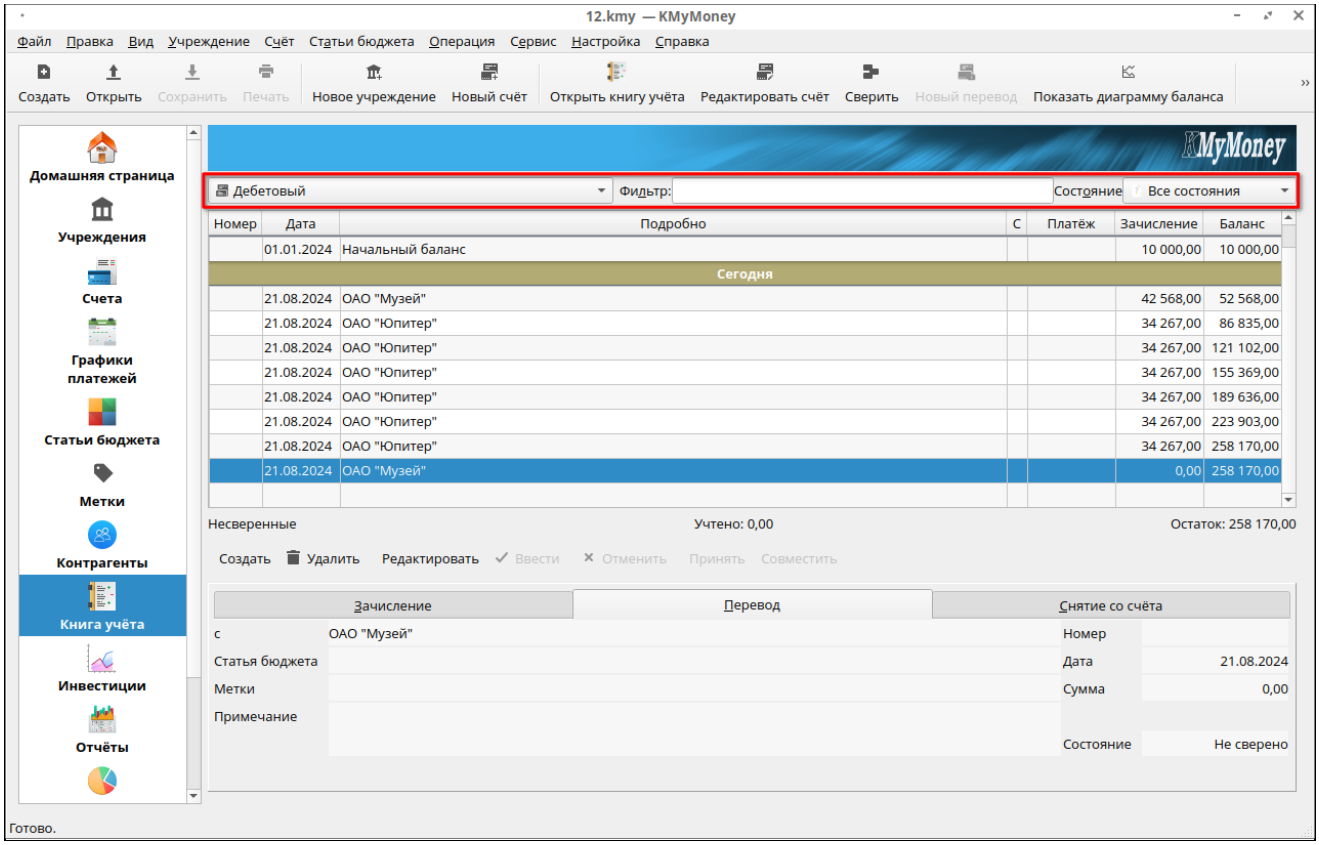
Книга учёта

Представление «**Книга учёта**» позволяет вносить, отслеживать, удалять и редактировать операции по заданным счетам.

Представление содержит три части:

- Область фильтра,
- Список операций,
- Форма ввода операций.

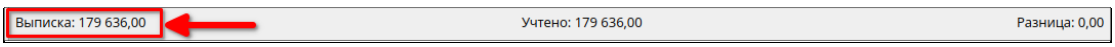
В области фильтра можно выбрать любой счёт. Параметры формы ввода операций зависят от типа счета.



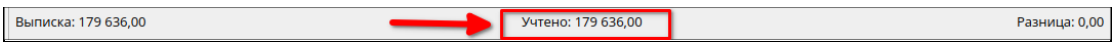
Внесённая операция будет показана в списке операций. Здесь можно изменить свойства операции или создать новую операцию. По умолчанию операции упорядочены по дате. Для изменения порядка сортировки операций щёлкните по заголовку списка операций ПКМ.

Под списком операций расположены три значения:

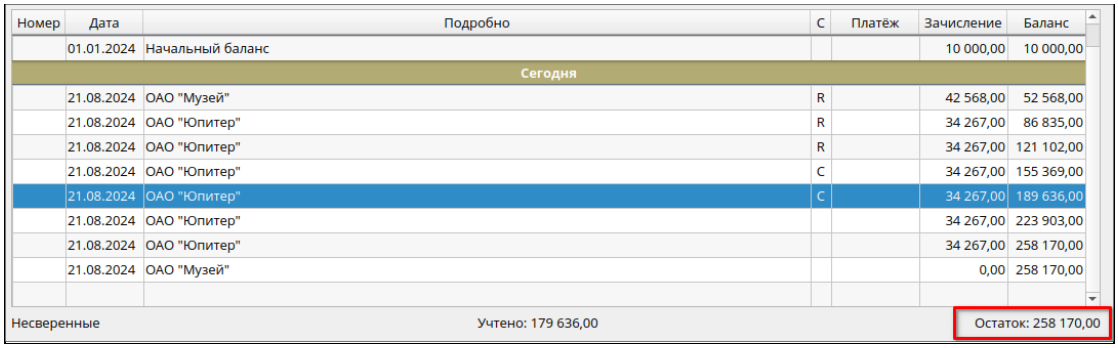
- **Последняя сверка**. Дата последней сверки счёта. Для выполнения сверки счета откройте его в книге учёта и, щёлкнув по значку, выберите пункт меню «**Счёт**» **—** «**Сверить...**».



- **Учтено**. Общая сумма по всем учтённым и сверенным операциям по счёту. Более подробные сведения об учёте и сверке операций доступны в этом разделе.



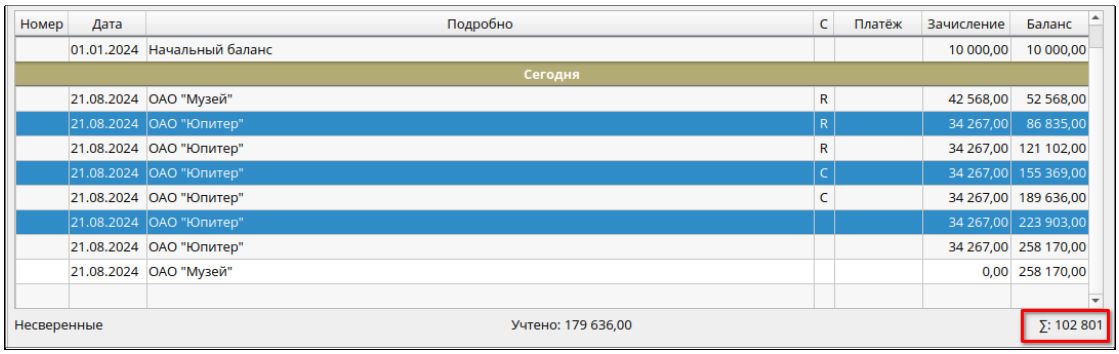
- **Остаток** представляет собой сумму всех операций по счёту. Остаток будет показан только при выборе одной операции.



Номер	Дата	Подробно	С	Платёж	Зачисление	Баланс
	01.01.2024	Начальный баланс			10 000,00	10 000,00
		Сегодня				
	21.08.2024	ОАО "Музей"	R		42 568,00	52 568,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	86 835,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	121 102,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	155 369,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	189 636,00
	21.08.2024	ОАО "Юпитер"			34 267,00	223 903,00
	21.08.2024	ОАО "Юпитер"			34 267,00	258 170,00
	21.08.2024	ОАО "Музей"			0,00	258 170,00

Несверенные | Учтено: 179 636,00 | Остаток: 258 170,00

При выборе нескольких операций будет показана их сумма.



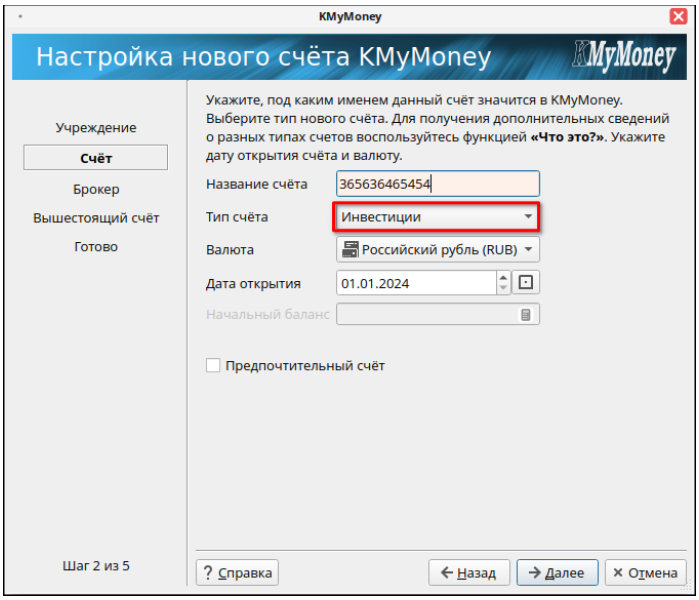
Номер	Дата	Подробно	С	Платёж	Зачисление	Баланс
	01.01.2024	Начальный баланс			10 000,00	10 000,00
		Сегодня				
	21.08.2024	ОАО "Музей"	R		42 568,00	52 568,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	86 835,00
	21.08.2024	ОАО "Юпитер"	R		34 267,00	121 102,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	155 369,00
	21.08.2024	ОАО "Юпитер"	C		34 267,00	189 636,00
	21.08.2024	ОАО "Юпитер"			34 267,00	223 903,00
	21.08.2024	ОАО "Юпитер"			34 267,00	258 170,00
	21.08.2024	ОАО "Музей"			0,00	258 170,00

Несверенные | Учтено: 179 636,00 | ∑: 102 801

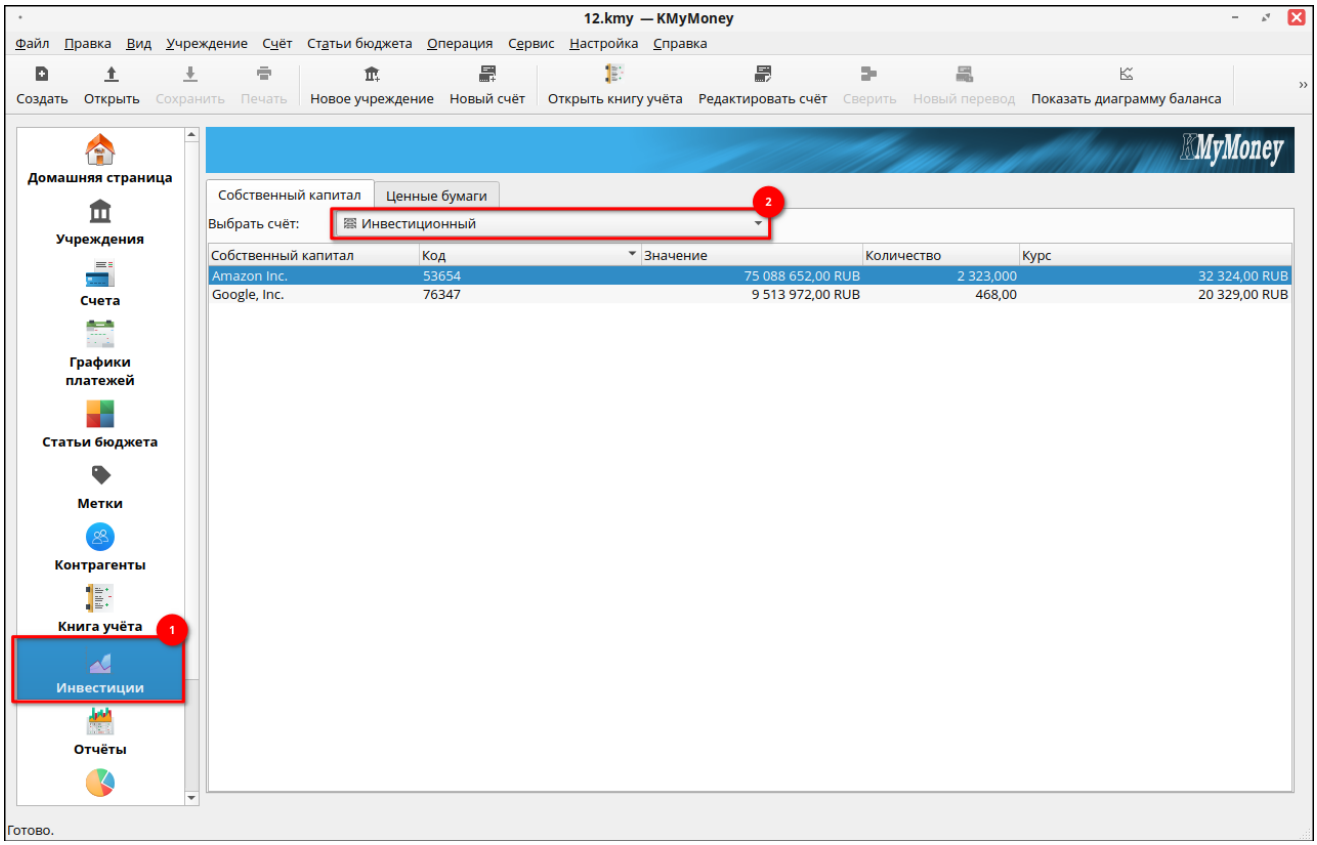
Инвестиции

Инвестиционные счета KMyMoney предназначены только для ценных бумаг. У каждой ценной бумаги имеется базовая валюта, в которой она продаётся или покупается. Если при инвестиционной операции присутствуют денежные средства, она должна быть связана с **брокерским счётом**, на котором хранятся деньги.

Для создания инвестиционного счёта для хранения информации о ценных бумагах выберите пункт меню «**Счёт**» — «**Новый счёт...**». При создании счёта укажите в поле тип счёта «**Инвестиции**».

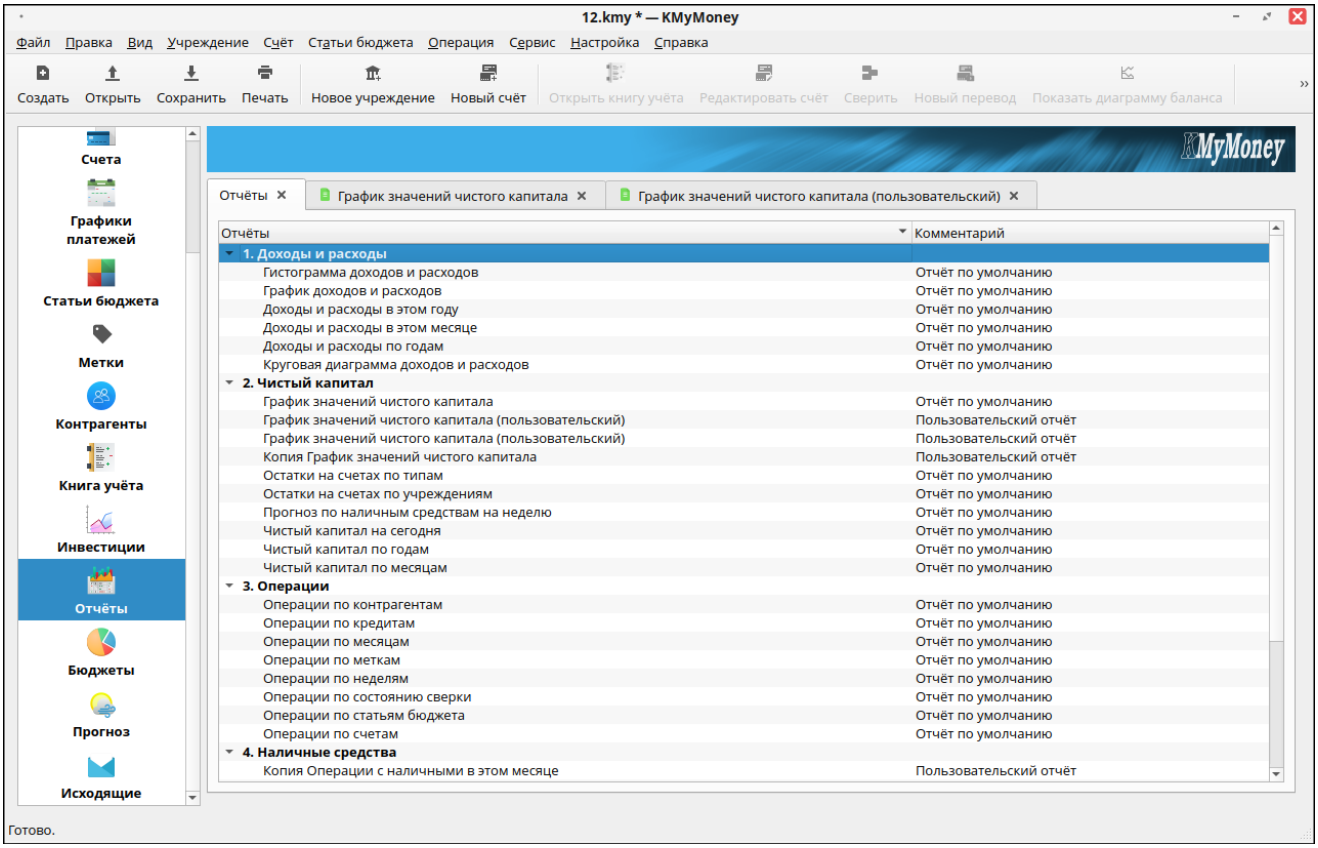


Для работы с новым инвестиционным счётом перейдите к просмотру представления «**Инвестиции**» (1) и выберите созданный счёт в раскрывающемся списке «**Выбрать счёт**» (2).

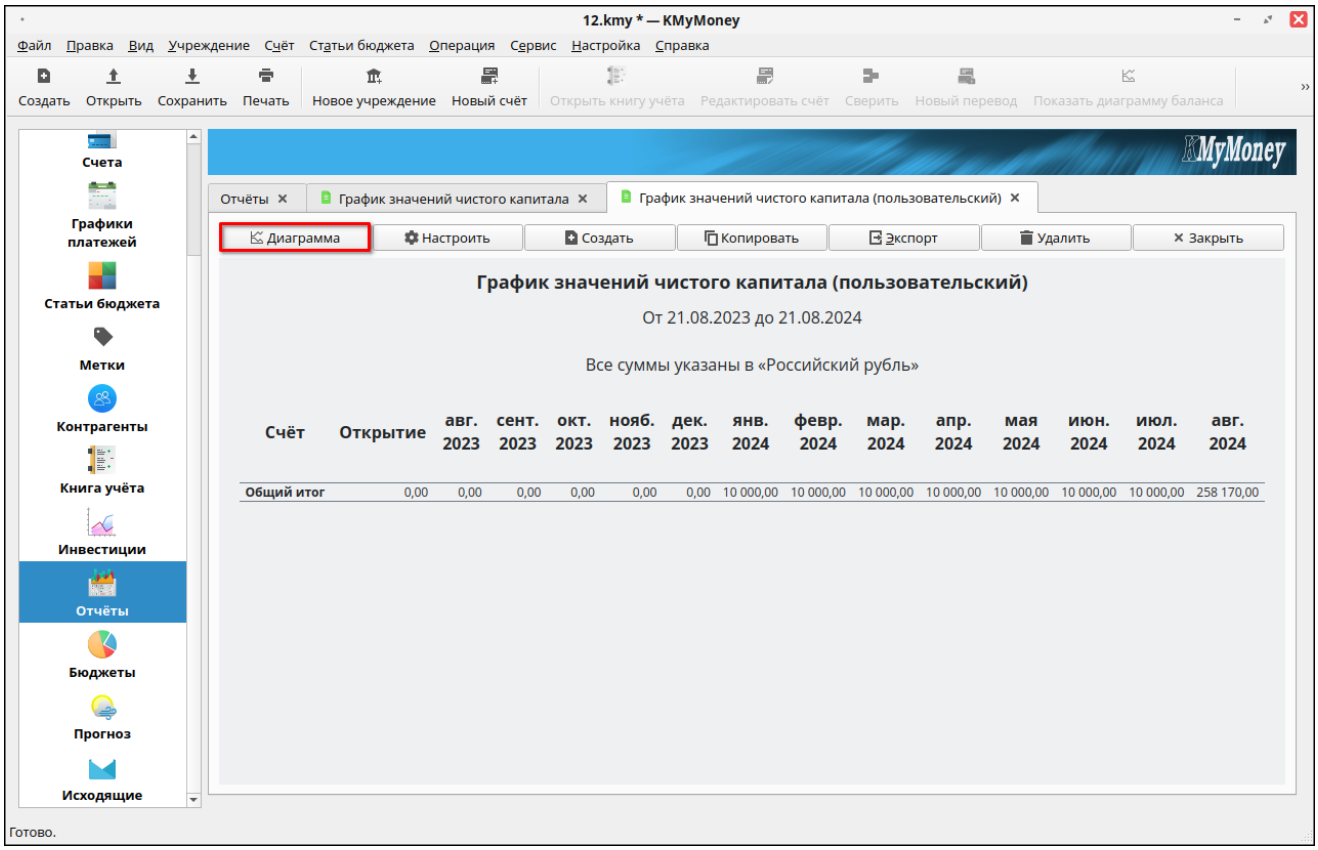


Отчёты

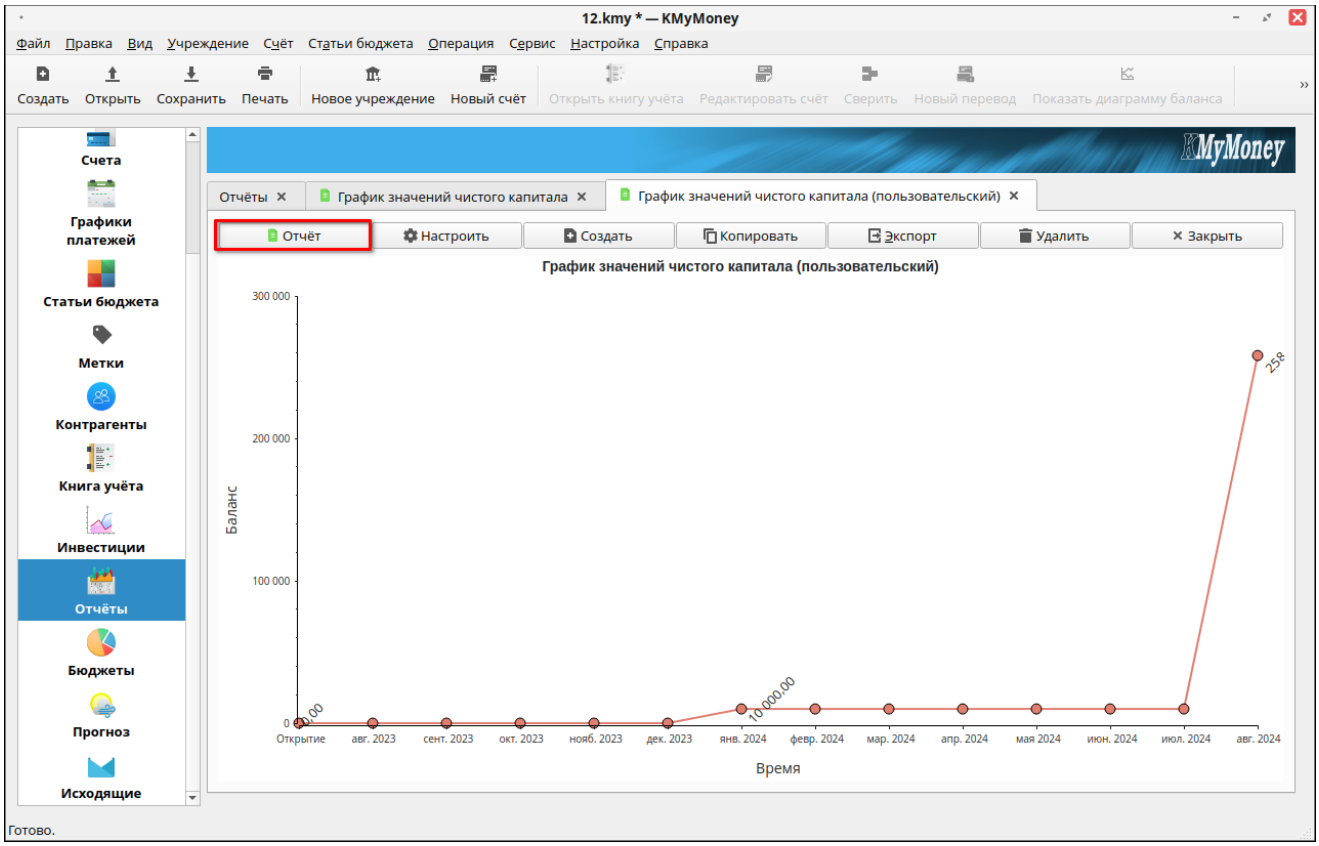
Итоги отчётного периода можно посмотреть в представлении «**Отчёты**» в текстовом или в графическом виде. **KmyMoney** позволяет выводить множество отчётов. Имеется набор стандартных отчётов. Ссылку на любой отчёт можно разместить на домашней странице.



Переключиться на графическое представление отчёта можно с помощью кнопки «**Диаграмма**».

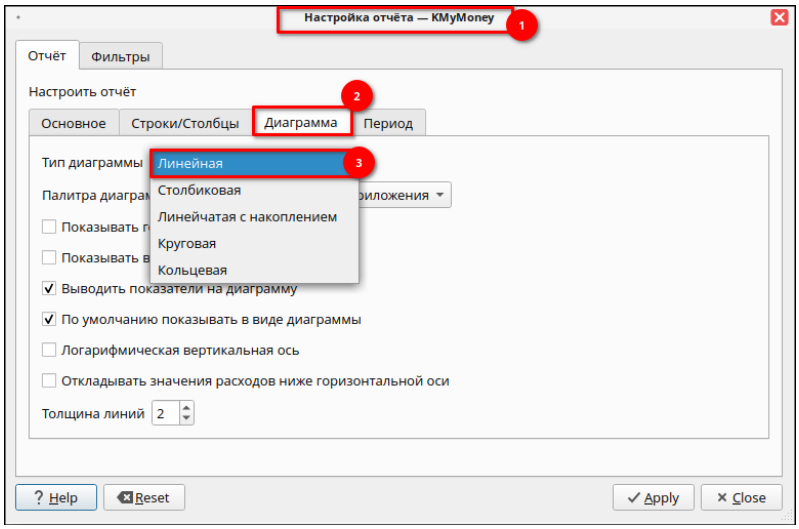


Переключиться на текстовое представление отчёта можно с помощью кнопки «**Отчёт**».

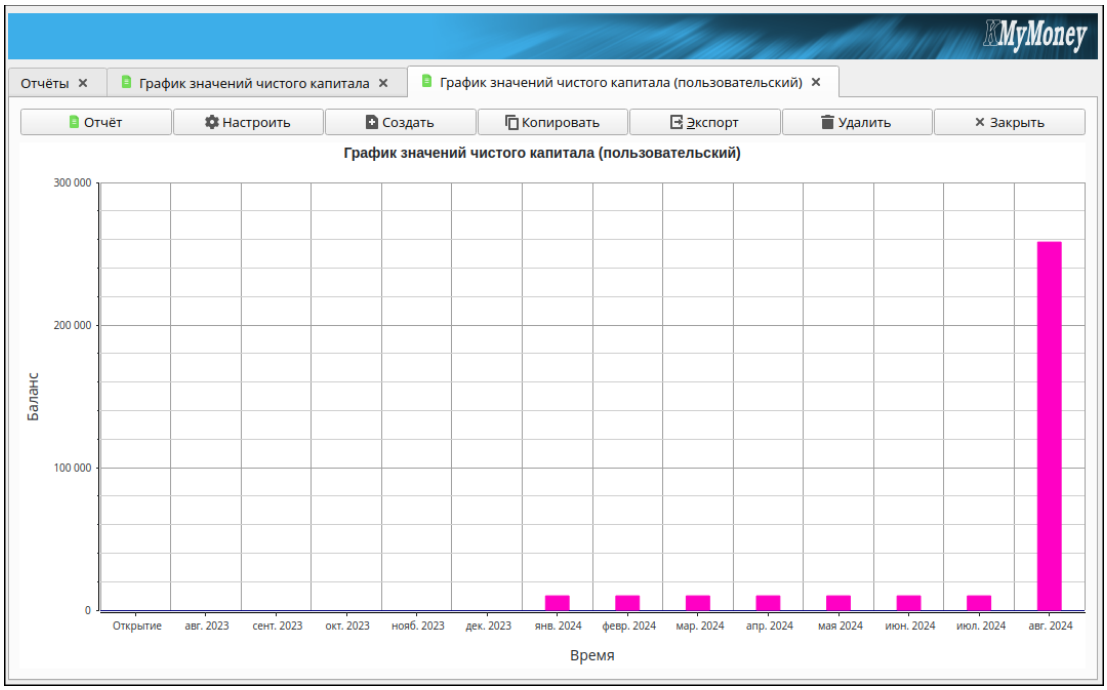


Внешний вид отчётов можно редактировать с помощью диалогового окна настройки отчёта.

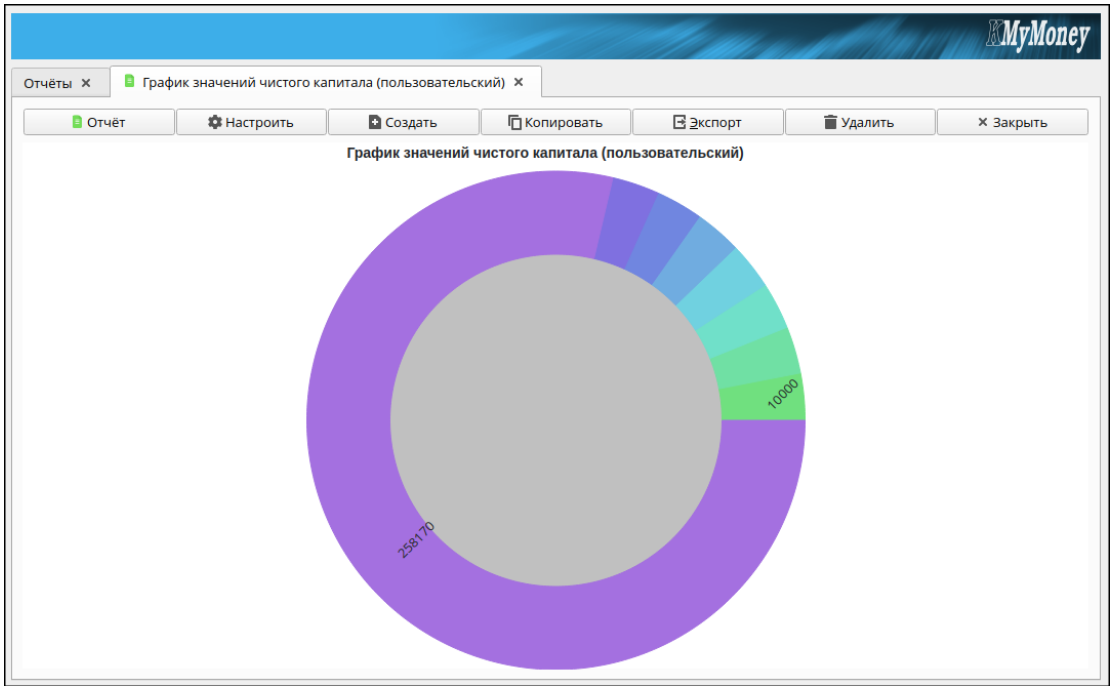
В настройках отчёта (1) на вкладке «**Диаграмма**» (2) можно задать тип диаграммы (3):



Столбиковая диаграмма аналогична линейной, но в ней для каждого временного среза будет показан столбец, соответствующий значениям.



Кольцевая диаграмма похожа на круговую, но в ней будет показано по одному кольцу для каждого временного среза в отчёте.



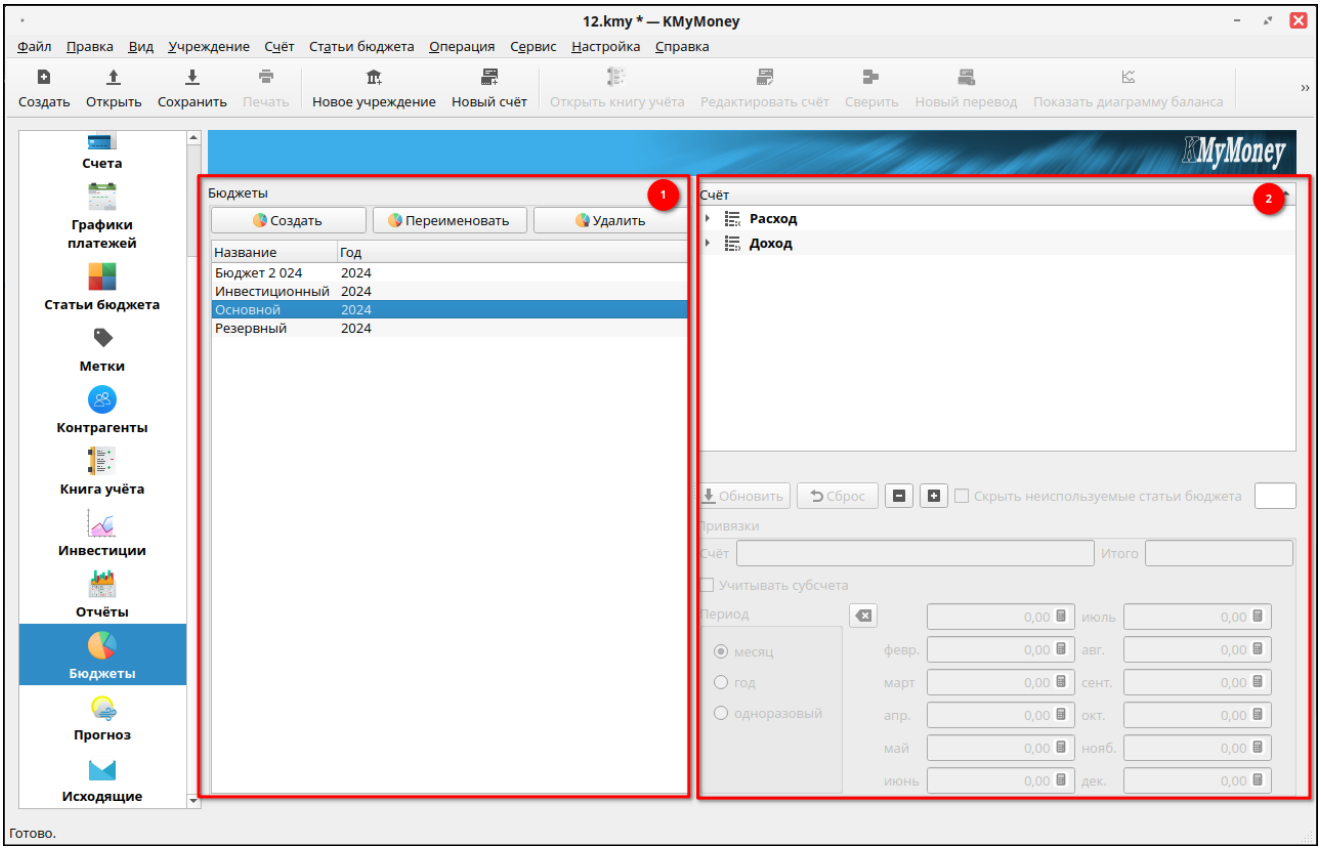
Бюджеты

Бюджет — это упорядоченный по статьям список ожидаемых доходов и расходов за определённый период. Для одного года можно создать несколько бюджетов.

В представлении «**Бюджеты**» есть две основных части:

1. Слева доступны список бюджетов пользователя и кнопки для создания, переименования и удаления бюджетов.

2. Справа отображается: список счетов и дополнительные параметры настройки бюджета.

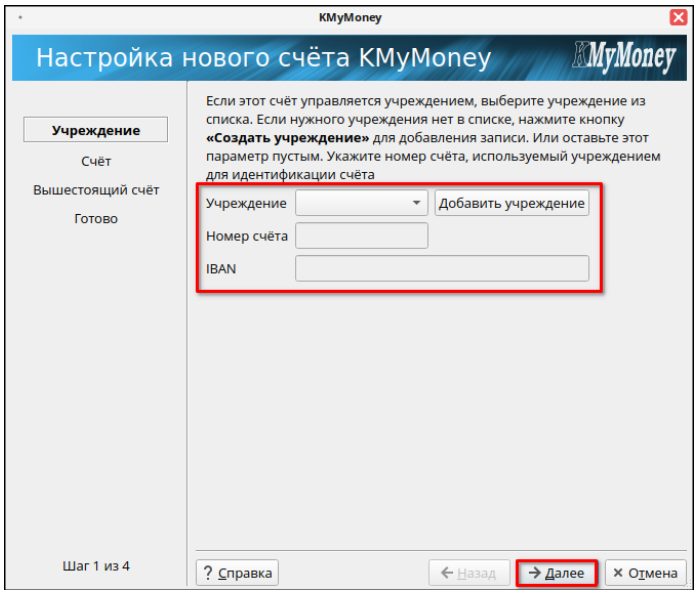


Пример работы

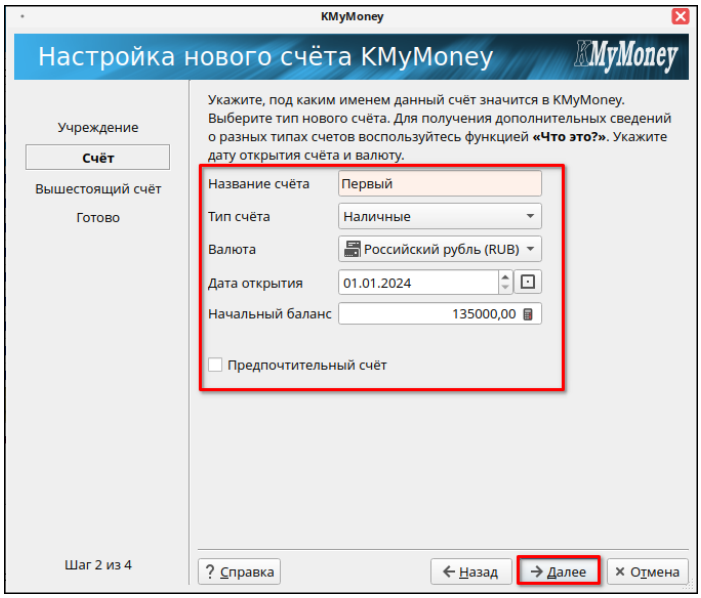
Рассмотрим пример ведения бюджета в личных целях.

1. Первоначально создайте счёт для учёта наличных денег. Для этого перейдите в меню «**Счёт**» — «**Новый счёт**».

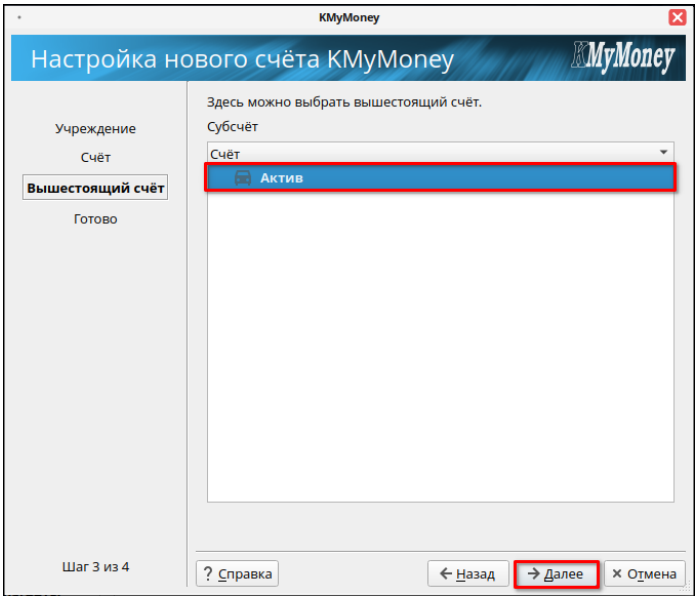
В мастере создания счета на первом шаге предлагается указать учреждение, в котором находятся деньги. Вы можете пропустить этот шаг и нажать «**Далее**».



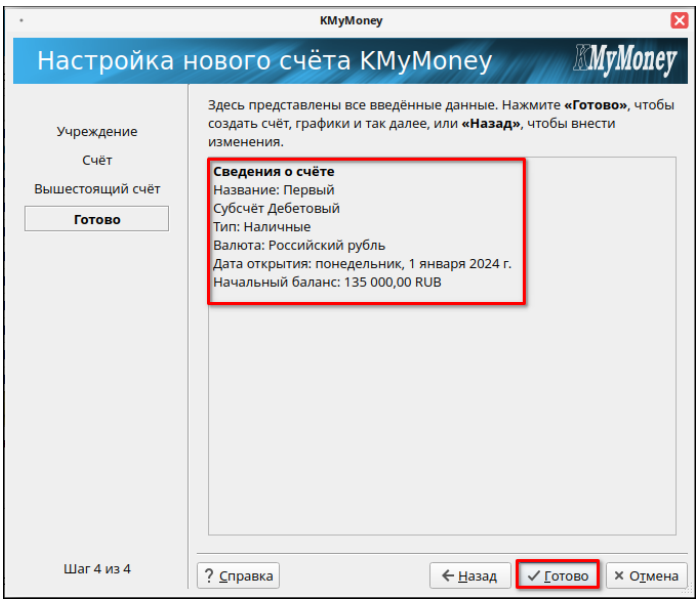
2. Введите название счёта, из списка выберите тип счёта «**Наличные**», укажите валюту и начальный остаток на счёте. Если вы хотите, чтобы этот счёт использовался по умолчанию, установите флажок рядом с опцией «**Предпочтительный счёт**».



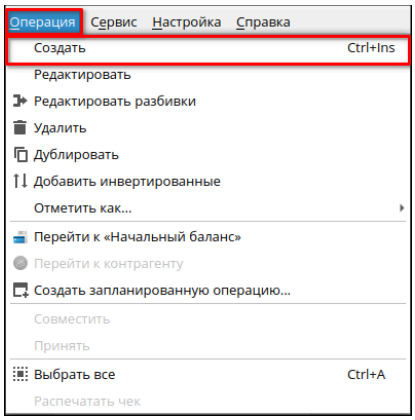
3. На следующем шаге выберите родительский счёт, укажите «**Актив**» и нажмите «**Далее**».



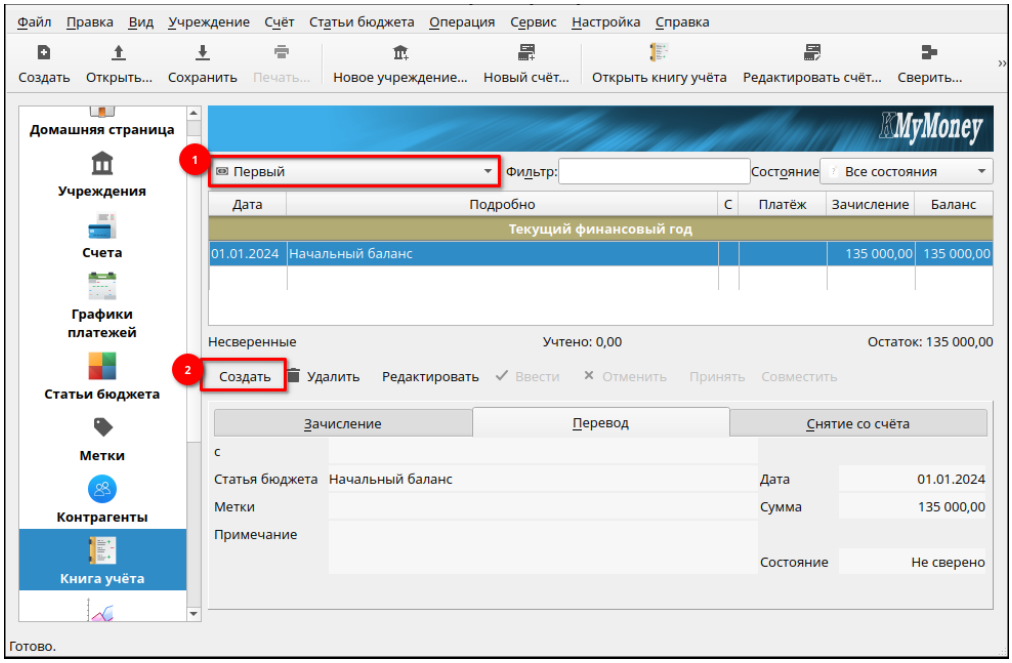
4. Просмотрите сводную информацию о созданном счёте и нажмите «**Готово**».



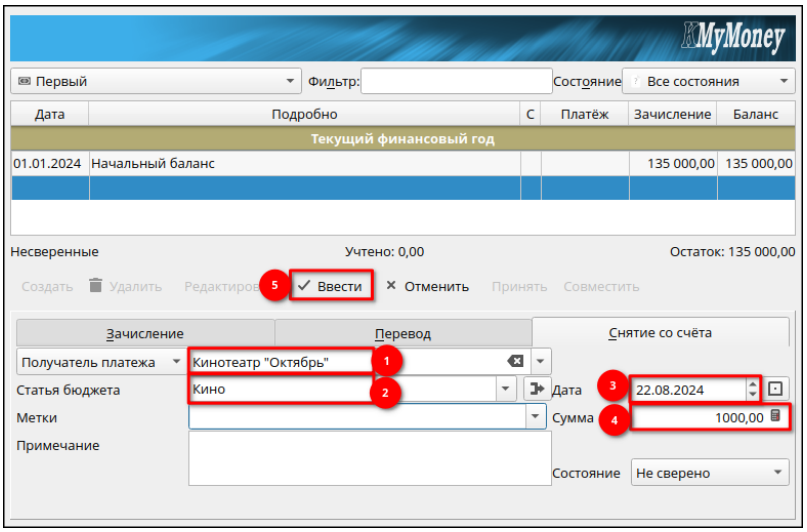
5. Для учёта расходов выберите в меню «**Операция**» — «**Создать**».



6. Выберите из списка счёт (1), с которого вы производите платёж. Это тот счёт, с которого будут списаны денежные средства. Нажмите кнопку «**Создать**» (2).

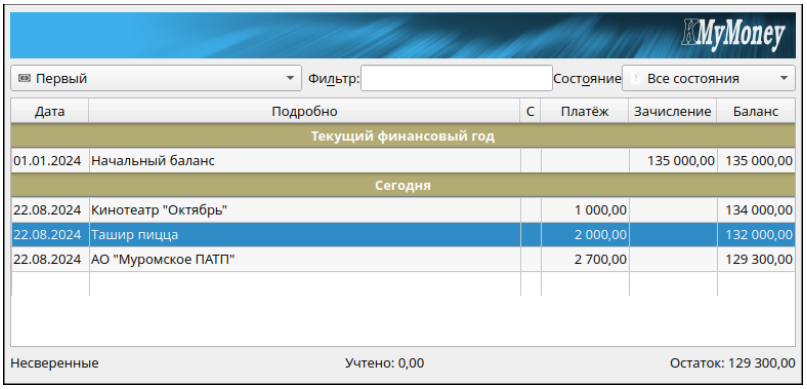


7. Перейдите на вкладку «**Снятие со счета**». Введите данные о получателе платежа (1) и согласитесь на добавление получателя. Укажите статью бюджета (2), дату (3) и сумму платежа (4). При желании добавьте примечание. Нажмите «**Сохранить**» или клавишу **Enter**. Повторите этот процесс для всех ваших платежей.

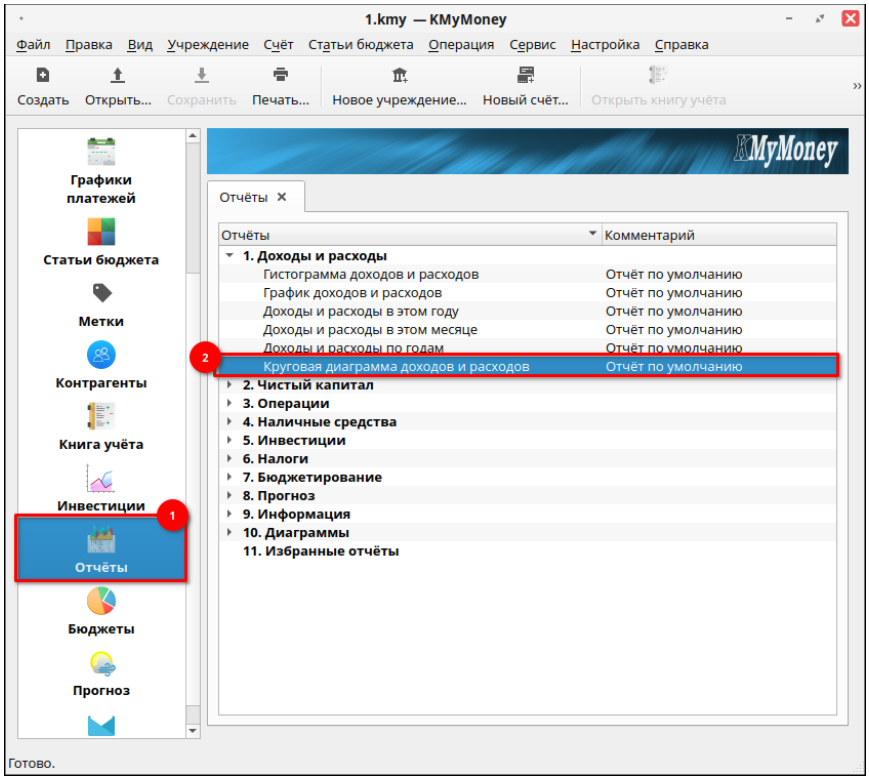


8. Доходы учитываются на вкладке «**Зачисления**». Если вы переводите деньги со счёта в кошелёк, используйте вкладку « **Перевод**».

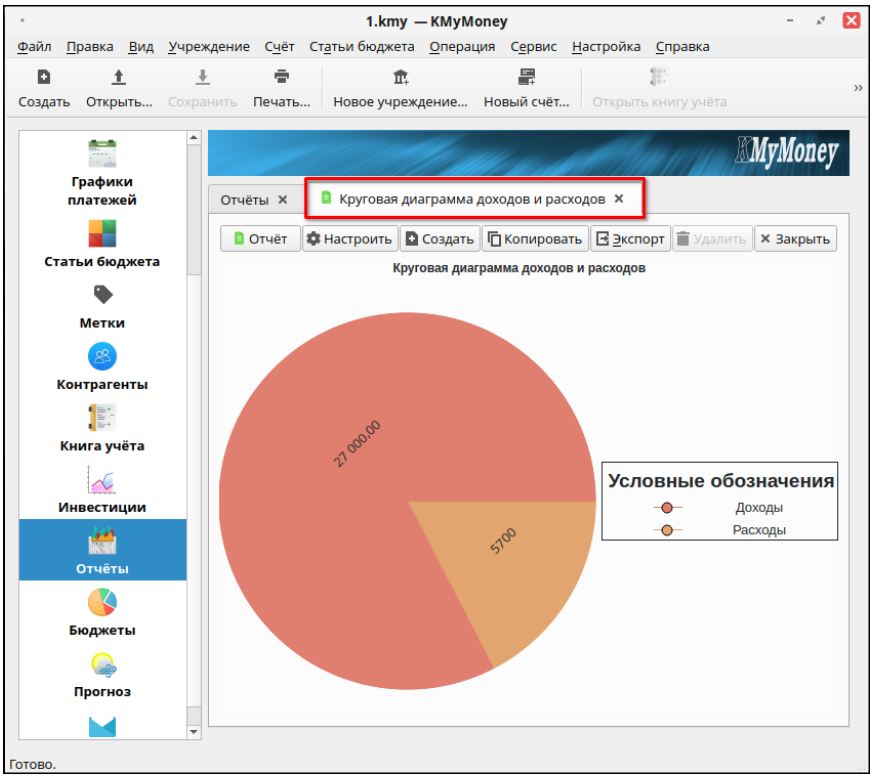
9. В окне операций отображаются все проведённые операции со счётом: зачисления, списания, остатки после каждой операции и текущий остаток, а также получатели и отправители платежей.



10. Для отслеживания движения денежных средств нажмите на значок «**Отчёты**» (1). В открывшемся списке выберите нужный вид отчёта (2).



Программа отобразит выбранную диаграмму. В примере круговая диаграмма доходов и расходов.


1.kmy — KMyMoney
Файл Правка Вид Учреждение Счёт Статьи бюджета Операция Сервис Настройка Справка
Создать Открыть... Сохранить Печать... Новое учреждение... Новый счёт... Открыть книгу учёта
Графики платежей
Статьи бюджета
Метки
Контрагенты
Книга учёта
Инвестиции
Отчёты
Бюджеты
Прогноз
KMyMoney
Отчёты
Круговая диаграмма доходов и расходов
Отчёт Настроить Создать Копировать Экспорт Удалить Закрыть
Круговая диаграмма доходов и расходов
27 000.00
5700
Условные обозначения
Доходы
Расходы
Готово.

Livemedia-creator – создание образа системы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** lorax-38.6-2

Livemedia-creator автоматизирует процесс создания образа системы. **Livemedia-creator** входит в состав пакета **lorax**. Процесс создания установочного образа в *livemedia-creator* включает два этапа: сначала создается временный образ дистрибутива в соответствии с настройками в файле **kickstart**, затем *livemedia-creator* создает загрузочный образ.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install lorax
```

Также необходимо установить дополнительные пакеты:

```
dnf install virt-install libvirt qemu-kvm
```

Livemedia-creator использует **virt-install** для создания временной виртуальной машины, где будет запущен процесс создания образа. Для создания образа потребуется файл *kickstart* и загрузочный ISO-образ.

Информацию по созданию **kickstart-файла** см. в нашей статье «Автоматизация развертывания (kickstart)».

Пример использования:

```
livemedia-creator --make-iso --iso=/home/user/redos-8-20240218.1-Everything-x86_64-DVD1.iso --ks=/root/test-ks.cfg --tmp=/home/user/lmc --iso-only --project=REDOS --releasever=8.0
```

Опции:

- **--iso** - путь к установочному образу;
- **--ks** - путь к файлу *kickstart*;
- **--tmp** - указывает директорию, в которую будет сохранен образ. По умолчанию используется **/var/tmp**;
- **--iso-only** - после завершения создания образа будет сохранен только загрузочный образ (ISO-файл);
- **--project** - имя операционной системы, которое будет отображаться в загрузчике;
- **--releasever** - версия операционной системы в загрузчике.

Более подробную информацию о других опциях можно узнать из официальной документации по ссылке: https://weldr.io/lorax/livemedia-creator.html.

После выполнения команды будет запущена временная виртуальная машина, где начнется процесс создания образа. К машине можно подключиться через **VNC**, чтобы понаблюдать за процессом установки. По умолчанию адрес VNC **127.0.0.1:0**.

После завершения установки образ будет сохранен в указанной директории в виде файла с названием **boot.iso** (по умолчанию). Также путь к этому файлу и к файлам логов будут указаны в выводе команды *livemedia-creator*. Название итогового образа можно задать при его создании с помощью опции **--iso-name**. Полученный загрузочный образ системы можно примонтировать в систему, чтобы убедиться, что файловая система была создана правильно. Далее образ можно записать на носитель и загрузиться с него в качестве Live-системы.

Пример kickstart-файла для создания загрузочного образа с конфигурацией минимального сервера:

```
# Generated by Anaconda 33.25.4
# Generated by pykickstart v3.30
#version=F33
%packages --multilib
@^server-minimal
dracut-live
syslinux
```

```
memtest86+
grub2-efi
redos-logos

%end

# Keyboard layouts
keyboard --xlayouts='us','ru' --switch='grp:alt_shift_toggle'
# System language
lang ru_RU.UTF-8

# Network information
network --bootproto=dhcp --device=ens18 --ipv6=auto --no-activate
network --hostname=localhost.localdomain

# Use CDROM installation media
cdrom

# Run the Setup Agent on first boot
#firstboot --enable
firstboot --disable
eula --agreed
shutdown

# Generated using Blivet version 3.3.0
ignoredisk --only-use=sda
part swap --asprimary --size=1024
part / --fstype ext4 --size=6000

# Partition clearing information
clearpart --none --initlabel

# System timezone
timezone Europe/Moscow --utc
timesource --ntp-disable

# Root password

rootpw --iscrypted
$6$5pjWyUOcrx5BkA2/$x.ZzjsgX4NUcUjSgGG.8EWiLfAIxfNy.m8xRKRMLUraz1MGJ99xohKFEs3S9PDoHSecJvuBbxLdbsvF3an52s.v

user --groups=wheel --name=user --
password=$6$Jsrft0ayMeAAOTaN$1gm9H9qwqBKYuBM7U3AkvJLzR78tDHqZWc55P0zWgJFxfSDKAEqBmSz5fdeqscN04sc6zw3tqlJiAEZBhxv1a/ --
iscrypted --gecos="user"


%anaconda
pwpolicy root --minlen=6 --minquality=1 --notstrict --nochanges --notempty
pwpolicy user --minlen=6 --minquality=1 --notstrict --nochanges --emptyok
pwpolicy luks --minlen=6 --minquality=1 --notstrict --nochanges --notempty
%end
```

ISO Master – утилита для редактирования ISO-образов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: isomaster-1.3.15-1

ISO Master – программа для редактирования ISO-образов оптических дисков. **ISO Master** не создаёт ISO-образы с компакт-дисков и не записывает их на диски, а только позволяет создавать их из произвольных каталогов и файлов или извлекать и изменять содержимое уже существующих образов. При необходимости к образу можно присоединить скрытые файлы или каталоги. **ISO Master** поддерживает различные файловые системы (960, Joliet, Rock Ridge и др.).

Ключевые особенности **ISO Master**:

- извлечение, удаление, добавление файлов и каталогов;
- поддержка ISO-образов, а также большинства NRG-образов и некоторых однотрековых MDF-образов;
- возможность переименования файлов и каталогов;
- выбор типа имён файлов Rock Ridge и/или Joliet;
- возможность выбора имени диска и издателя;
- просмотр и редактирование файлов внешними редакторами;
- просмотр и изменение правовых атрибутов файлов и каталогов;
- возможность работы с загрузочной записью – извлечение, удаление, установка из файла;
- поддержка файловых систем ISO 9660, Joliet, Rock Ridge, El Torito.

ISO Master простой в использовании графический редактор образов. Он может открывать файлы ISO, NRG и некоторые файлы MDF, но сохранение возможно только в формате ISO.

Меню **ISO Master** переведено на русский язык, поэтому выполнять задачи с помощью утилиты смогут даже начинающие пользователи. Из минусов программы выделяют отсутствие интегрированного рекордера, готовые образы можно записать на оптический диск только посредством дополнительных инструментов.

Установка

Утилита **ISO Master** находится в репозитории РЕД ОС, для установки перейдите в сеанс пользователя **root**:

```
su -
```

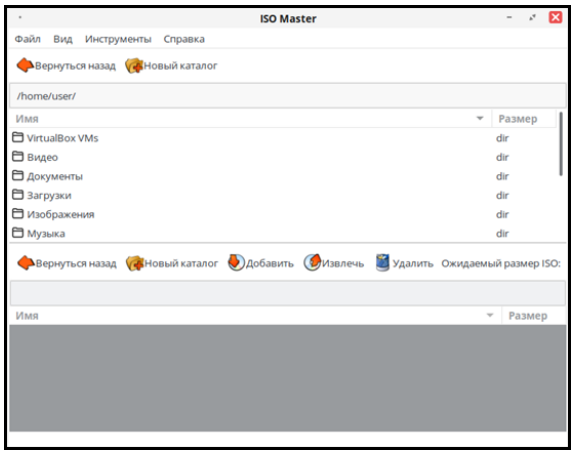
и выполните команду:

```
dnf install isomaster
```

После установки запуск программы доступен из «Главного меню» — «Аудио и видео» — «ISO Master» или через терминал (с правами локального пользователя) командой:

```
isomaster
```

Интерфейс утилиты **ISO Master** выглядит следующим образом:



Окно **ISO Master** разделено на две части:

- верхняя область окна отображает файлы и каталоги на используемой системе;
- нижняя область окна отображает файлы и каталоги в образе диска.

Для открытия существующего образа (ISO) нажмите «Файл» - «Открыть».

Для создания нового образа нажмите «Файл» - «Новый».

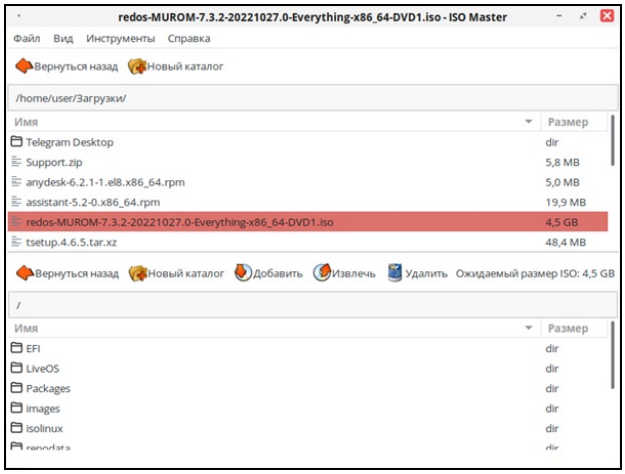
Для добавления одного или нескольких файлов или каталогов в образ выберите их в верхней области окна и нажмите «Добавить в образ» на панели инструментов в центре окна.

Для извлечения одного или нескольких файлов из образа выберите их в нижней области окна и нажмите «Извлечь из образа» на панели инструментов в центре окна.

Доступно удаление файлов и каталогов из образа, а также создание каталогов как в образе, так и на используемой системе. Дополнительные опции появляются при нажатии ПКМ по выбранному элементу в нижней части окна.

После внесения изменений в новый образ для сохранения результатов нажмите «Образ» - «Сохранить как». Обратите внимание, что исходный образ перезаписать нельзя.

При выборе какого-либо образа содержимое отображается в нижней части окна.



Отдельно стоит отметить, что **ISO Master** предоставляет пользователю возможность создавать или удалять загрузочную запись, а также создавать автозагрузочный файл, работающий без эмуляции. То есть создать загрузочный диск или флешку можно без каких-либо дополнительных инструментов.

genisoimage - утилита создания ISO-образов файловой системы

Установка
Синтаксис
Работа с утилитой
Создание ISO-образа отдельного каталога
Создание образа работающей системы
Создание копии локального репозитория

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: genisoimage-1.1.11-42

Genisoimage — это инструмент командной строки для создания образов файловой системы. Обычно используется для создания загрузочных компакт-дисков, дисков резервного копирования или для распространения больших объемов данных в одном файле. Полученный ISO-образ можно записать на носитель с помощью программного обеспечения для записи или смонтировать как виртуальный привод.

С помощью **genisoimage** можно создать:

- ISO-образ отдельного каталога;
- ISO-образ работающей системы;
- ISO-образ копии локального репозитория.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install genisoimage
```

Дальнейшая работа с утилитой производится с правами **администратора** или суперпользователя **root**.

Синтаксис

Синтаксис утилиты имеет вид:

```
genisoimage [<опции>] [-o <имя_образа>] <путь_к_источнику> [<путь_к_источнику_2> ...]
```

где:

- `<опции>` – необходимые опции;
- `<имя_образа>` – имя создаваемого образа, допускается указывать полный путь к создаваемому образу;
- `<путь_к_источнику>` – путь к источнику, из которого будет создан образ; может быть указано несколько источников с использованием опции `-graft-points`.

Пример использования опции `-graft-points`:

```
genisoimage -V test_iso -r -o test_iso.iso -graft-points /downloads=/home/user/Загрузки/ /docs=/home/user/Документы/
/images=/home/user/Изображения/
```

Необходимые источники указываются в формате `<цель>=<источник>` через пробел.

Работа с утилитой

Создание ISO-образа отдельного каталога

Рассмотрим пример создания копии раздела **/home**.

Для этого необходимо выполнить команду:

```
genisonimage -V home_iso -r -o /home.iso /home
```

где:

- `-V home_iso` – задать метку образа, которая будет видна при его монтировании;
- `-r` – сгенерировать записи SUSP и RR, необходимые для создания файловой системы **ISO9660**;
- `-o /home.iso` – имя созданного файла образа;
- `/home` – источник, из которого создается образ.

Создание образа работающей системы

Для создания образа работающей системы необходимо:

- создать временный каталог, в котором будет создаваться ISO-образ:

```
mkdir /tmp/iso
```

- примонтировать корневой раздел **/** в каталог **/mnt**.

В случае использования **LVM** выполнить команду:

```
mount /dev/ro_redos/root /mnt
```

- скопировать содержимое раздела **/** в каталог **/tmp/iso**:

```
cp -a /mnt/* /tmp/iso
```

- размонтировать **/mnt**:

```
umount /mnt
```

- после этого создать ISO-образ:

```
genisoimage -r -o /redos.iso /tmp/iso
```

где:

- `/redos.iso` – место расположения и название созданного образа;
- `/tmp/iso` – ранее созданный каталог; источник, из которого создается ISO-образ.

Примечание.

Процесс может занять некоторое время в зависимости от размера корневой файловой системы.

Создание копии локального репозитория

Утилита **genisonimage** позволяет создавать копии локального репозитория.

Для этого необходимо предварительно создать локальный репозиторий по нашей инструкции «Создание локального репозитория».

Далее для каждого репозитория необходимо создать отдельный образ:

```
genisonimage -V redos-7.3base -r -o /tmp/iso/redos-7.3base.iso /var/www/html/repo/red-os-7.3/base7.3
genisonimage -V redos-7.3update -r -o /tmp/iso/redos-7.3update.iso /var/www/html/repo/red-os-7.3/base7.3
genisonimage -V redos-7.3update -r -o /tmp/iso/redos-7.3kernels.iso /var/www/html/repo/red-os-7.3/kernels7.3
```

где:

- `-V redos-7.3base` – метка образа, которая видна при его монтировании;
- `-r` – сгенерировать записи SUSP и RR, необходимые для создания файловой системы ISO9660;
- `-o /tmp/iso/redos-7.3base.iso` – путь до создаваемого образа;
- `/var/www/html/repo/red-os-7.3/base7.3` – источник, из которого создается образ.

Примечание.

Процесс может занять некоторое время в зависимости от размера локального репозитория.

Dracut - ПО для создания загрузочного образа (initramfs)

Основные опции
Создание образа initramfs
Информация об образе

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dracut-056-9

Dracut — набор инструментов, обеспечивающих расширенные функции для автоматизации процесса загрузки Linux. Инструмент под названием *dracut* используется для создания загрузочного образа Linux (**initramfs**) путем копирования инструментов и файлов из установленной системы и объединения их со средой *dracut*, которая обычно находится в каталоге **/usr/lib/dracut/modules.d**.

В отличие от существующих загрузочных образов Linux, платформа *Dracut* пытается ввести как можно меньше жестко запрограммированной логики в **initramfs**. По сути, **initramfs** имеет одну цель: найти и смонтировать настоящую корневую файловую систему, чтобы процесс загрузки мог перейти к ней. Эта функция зависит от доступности устройства. Поэтому вместо жестко запрограммированных сценариев для определения доступности и пригодности устройства **initramfs** *dracut* зависит от диспетчера устройств Linux (**udev**) для создания символических ссылок на узлы устройств. Когда появляется узел устройства корневой файловой системы, *Dracut* монтирует его как новую корневую файловую систему, что помогает сократить время, необходимое для **initramfs**.

Основные опции

К основным опциям *dracut* относятся:

- `--kver <версия_ядра>` - позволяет создать образ с указанной версией ядра (по умолчанию образ сохраняется в каталог **/boot**);
- `-f, --force` - перезаписать существующий файл **initramfs**;
- `-a, --add <список_модулей_dracut>` - добавить список модулей *dracut* (через пробел) к набору модулей по умолчанию;
- `-o, --omit <список_модулей_dracut>` - отключить указанный список модулей *dracut* (через пробел);
- `-m, --modules <список_модулей_dracut>` - список модулей *dracut* (через пробел) для вызова при сборке **initramfs**. Этот параметр позволяет *dracut* включать только указанные модули;
- `--add-drivers <список_модулей_ядра>` - список модулей ядра (через пробел) для добавления в **initramfs**. Модули ядра должны быть указаны без суффикса «**.ko**»;
- `--filesystems <список_модулей_ФС>` - список модулей файловой системы ядра (через пробел) для включения в **initramfs** только общего назначения. Модули должны быть указаны без суффикса «**.ko**»;
- `-H, --hostonly` - создать образ только с теми параметрами, которые необходимы для загрузки конкретной машины.

Создание образа initramfs

Для создания образа **initramfs** используется команда:

```
dracut
```

Данная команда создаст образ **initramfs** общего назначения со всеми возможными функциями, полученными в результате комбинации установленных модулей *dracut* и системных инструментов. Образ **/boot/initramfs-<версия_ядра>.img** будет содержать модули используемого в данный момент системой ядра.

Если такой **initramfs**-образ уже существует, будет выведена ошибка с предложением использования опции **--force** для перезаписи уже существующего образа.

```
dracut

dracut: Will not override existing initramfs (/boot/initramfs-5.15.125-1.el7.3.x86_64.img) without --force
```

Также можно указать собственное имя для создаваемого образа, передав его команде в качестве аргумента:

```
dracut new-images-03-10-2023.img
```

Файлы образов по умолчанию хранятся в каталоге **/boot**. Однако обратите внимание, что при указании собственного имени образа (как приведено в примере выше) он будет сохранен в той директории, из которой выполнялась команда. Для сохранения образа в необходимом каталоге потребуется указать полный путь к создаваемому образу, например:

```
dracut /boot/new-images-03-10-2023.img
```

Для просмотра содержимого каталога **/boot** и списка имеющихся образов выполните следующую команду:

```
ll /boot
```

```
[root@localhost user]# ll /boot
итого 322044
-rw-r--r--. 1 root root    243138 авг 17 10:15 config-5.15.125-1.el7.3.x86_64
-rw-r--r--. 1 root root    242516 окт  6  2022 config-5.15.72-1.el7.3.x86_64
-rw-r--r--. 1 root root    243099 янв 16  2023 config-5.15.87-1.el7.3.x86_64
drwxr-xr-x. 3 root root      4096 июл  6 14:27 efi
drwxr-xr-x. 2 root root      4096 июл  6 14:31 grub
drwx------. 6 root root      4096 окт  4 14:16 grub2
-rw-------. 1 root root 109608962 сен 18 15:18 initramfs-0-rescue-d10c8030d88c4fb5b67dc7aab5e80a0b.img
-rw-------. 1 root root  33126818 сен 18 15:16 initramfs-5.15.125-1.el7.3.x86_64.img
-rw-------. 1 root root  35105011 июл  6 16:56 initramfs-5.15.72-1.el7.3.x86_64.img
-rw-------. 1 root root  32775360 сен 18 15:15 initramfs-5.15.87-1.el7.3.x86_64.img
drwxr-xr-x. 3 root root      4096 июл  6 14:41 loader
drwx------. 2 root root     16384 июл  6 14:23 lost+found
-rw-------. 1 root root  33667660 окт  4 15:27 new-images-03-10-2023.img
-rw-r--r--. 1 root root    280149 авг 17 10:18 symvers-5.15.125-1.el7.3.x86_64.gz
-rw-r--r--. 1 root root    279524 окт  6  2022 symvers-5.15.72-1.el7.3.x86_64.gz
-rw-r--r--. 1 root root    279819 янв 16  2023 symvers-5.15.87-1.el7.3.x86_64.gz
-rw-------. 1 root root   5949734 авг 17 10:15 System.map-5.15.125-1.el7.3.x86_64
-rw-------. 1 root root   5892910 окт  6  2022 System.map-5.15.72-1.el7.3.x86_64
-rw-------. 1 root root   5919259 янв 16  2023 System.map-5.15.87-1.el7.3.x86_64
-rwxr-xr-x. 1 root root  17647264 сен 18 15:16 vmlinuz-0-rescue-d10c8030d88c4fb5b67dc7aab5e80a0b
-rwxr-xr-x. 1 root root  17647264 авг 17 10:15 vmlinuz-5.15.125-1.el7.3.x86_64
-rwxr-xr-x. 1 root root  15288800 окт  6  2022 vmlinuz-5.15.72-1.el7.3.x86_64
-rwxr-xr-x. 1 root root  15502336 янв 16  2023 vmlinuz-5.15.87-1.el7.3.x86_64
```

Информация об образе

Для просмотра информации об используемом образе можно воспользоваться командой:

```
lsinitrd | less
```

В выводе отображается имя образа, его размер, версия *dracut* и список включенных в образ модулей *dracut*:

```
Image: /boot/initramfs-5.15.125-1.el7.3.x86_64.img: 33M
================================================================================
Version: dracut-056-9.el7

Arguments:  --force

dracut modules:
bash
systemd
systemd-initrd
systemd-sysusers
nss-softokn
dbus-broker
rngd
dbus
i18n
network-manager
network
ifcfg
drm
plymouth
dm
kernel-modules
kernel-modules-extra
kernel-network-modules
...
```

Некоторые модули в dracut по умолчанию отключены, но их можно добавить, используя файл конфигурации /etc/dracut.conf или команду вида:

```
dracut --add module <название_модуля>
```

Используя команду `dracut --list modules`, можно вывести список всех модулей *dracut*, доступных в системе:

```
dracut --list modules

bash
systemd
systemd-network-management
warpclock
fips
systemd-ac-power
systemd-ask-password
systemd-coredump
systemd-hostnamed
systemd-initrd
systemd-integritysetup
systemd-journald
systemd-ldconfig
systemd-modules-load
systemd-networkd
systemd-repart
systemd-resolved
systemd-rfkill
systemd-sysctl
...
```

Все модули *dracut* расположены в каталоге **/usr/lib/dracut/modules.d**. В этом каталоге все модули представлены в виде подкаталогов и содержат ряд скриптов. Каждый модуль обеспечивает определенную функциональность.

После секции модулей выведен список содержимого сжатого образа:

```
========================================================================
drwxr-xr-x  12 root     root          0 Sep  6 17:12 .
crw-r--r--   1 root     root      5,   1 Sep  6 17:12 dev/console
crw-r--r--   1 root     root      1,  11 Sep  6 17:12 dev/kmsg
crw-r--r--   1 root     root      1,   3 Sep  6 17:12 dev/null
crw-r--r--   1 root     root      1,   8 Sep  6 17:12 dev/random
crw-r--r--   1 root     root      1,   9 Sep  6 17:12 dev/urandom
lrwxrwxrwx   1 root     root          7 Sep  6 17:12 bin -> usr/bin
drwxr-xr-x   2 root     root          0 Sep  6 17:12 dev
drwxr-xr-x  15 root     root          0 Sep  6 17:12 etc
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/authselect
-rw-r--r--   1 root     root       2428 Jul 31 10:58 etc/authselect/nsswitch.conf
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/cmdline.d
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/conf.d
-rw-r--r--   1 root     root        124 Sep  6 17:12 etc/conf.d/systemd.conf
drwxr-xr-x   7 root     root          0 Sep  6 17:12 etc/dbus-1
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/dbus-1/interfaces
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/dbus-1/services
-rw-r--r--   1 root     root        838 Oct 10  2022 etc/dbus-1/session.conf
drwxr-xr-x   2 root     root          0 Sep  6 17:12 etc/dbus-1/session.d
-rw-r--r--   1 root     root        833 Oct 10  2022 etc/dbus-1/system.conf
...
```

Функционал программы также предоставляет возможность ручного добавления драйверов, отключения ненужных модулей, добавление дополнительной информации для ускорения загрузки. Дополнительно реализована возможность поиска корневого раздела на сетевом диске.

Подробную информацию о работе с *dracut* можно получить, выполнив команду:

```
man dracut
```

О репозиториях

Репозито́рий РЕД ОС представляет собой хранилище (место), где хранятся и поддерживаются пакеты программ в формате **.rpm**.

Кроме официального репозитория существует множество сторонних, но их подключение настоятельно не рекомендовано. Это может приводить к коллизиям пакетов и проблеме несовместимости версий.

Поскольку репозитории Linux расположены в интернете, существует вероятность подмены репозитория злоумышленником на свой, содержащий модифицированные пакеты. Наш репозиторий имеет защиту от подмены. Защита реализована при помощи сверки цифровых подписей.

На клиенте подключенный репозиторий представляет из себя файл с расширением **.repo**, содержащий информацию о репозитории. Находится он по пути **/etc/yum.repos.d/**.

Для управления пакетами в РЕД ОС используется пакетный менеджер **DNF**, графический пакетный менеджер **dnfdragora** и утилиты для обслуживания **dnf-utils**.

Все действия по разворачиванию репозитория происходят на серверной части.

Создание локального репозитория

Подготовка сервера
Создание локального зеркала репозитория РЕД ОС 8
Настройка на клиентском ПК

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: httpd-2.4.62-2, createrepo_c-0.20.1-1, dnf-utils-4.4.2-1

Вы можете подробнее ознакомиться с созданием локальных репозиториев, просмотрев наши обучающие видео:

- на **RuTube** — Создание локального репозитория РЕД ОС;
- в **Яндекс.Дзен** — Создание локального репозитория РЕД ОС;
- в **VK Видео** — Создание локального репозитория РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

В рамках данной статьи все действия должны выполняться с правами **администратора** системы или **суперпользователя root**.

Перейдите в сеанс пользователя **root** (если данная учётная запись включена):

```
su -
```

или выполните от имени администратора (пользователя в группе *wheel*) команду:

```
sudo su -
```

Подготовка сервера

Установите пакеты, необходимые для организации зеркала репозитория, доступного по протоколу **HTTP**:

```
dnf install httpd createrepo_c dnf-utils
```

Запустите и добавьте в автозагрузку службу **httpd**:

```
systemctl enable httpd --now
```

ВАЖНО!

Для создания локальных репозиториев **Base** и **Updates** необходимо предварительно убедиться, что у вас есть необходимый объем требуемого свободного дискового пространства.

Для получения информации о необходимом объеме для какого-либо определенного репозитория выполните команду:

```
dnf repoinfo <название_репозитория> | grep -iE 'размер.*репозитория'
```

Чтобы узнать более точный размер **всех подключенных** репозиториев, можно воспользоваться командой:

```
dnf repoinfo | grep -iE 'размер.*репозитория' | awk -F ':' '{size = $2; sub(/M$/, "", size); if (index($2, "M") > 0) total += size / 1024; else total += size} END {printf "Общий размер \033[41mвсех подключенных\033[0m репозиториев: %.2f G\n", total}'
```

Для размещения репозиториев можно использовать каталог, отличный от **/var/www/html/**, создав для него символическую ссылку и установив правильный контекст SELinux (для файловых систем с поддержкой *Extended File Attributes* - **ext2**, **ext3**, **ext4**, **jfs**, **xfs**, **btrfs**):

```
ln -s /mnt/repodisk/ /var/www/html/repos
semanage fcontext -a -t httpd_sys_content_t "/mnt/repodisk(/.*)?"
```

Здесь в качестве примера используется каталог **/mnt/repodisk/**.

Обратите внимание, что для пользователя или группы **apache** файлы и каталоги в директории репозитория должны быть доступны для чтения. Управление правами доступа подробно описано в статье «Настройка прав доступа к файлам и каталогам».

Создание локального зеркала репозитория РЕД ОС 8

Создайте конфигурационный файл описания репозитория-источника в каталоге **/etc/yum.repos.d/**:

```
nano /etc/yum.repos.d/redos8_base_src.repo
```

Вставьте следующее содержимое (пример для репозитория **Base**):

```
[redos8_base_src]
 name=RedOS 8 - Base (Mirror source)
 baseurl=https://repo1.red-soft.ru/redos/8.0/$basearch/os,https://mirror.yandex.ru/redos/8.0/$basearch/os,http://repo.red-
soft.ru/redos/8.0/$basearch/os
 gpgcheck=1
 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
 enabled=0
```

Значение `redos8_base_src` — это ID (идентификатор) репозитория-источника, который будет применён далее в команде `reposync`. Задать другое значение ID можно с соблюдением уникальности, применением только латиницы (**a-z**), цифр (**0-9**) и спец. символов (**-** , **_** , **.** , **:**).

Создайте каталог для размещения содержимого локальных репозиториев:

```
mkdir -p /var/www/html/repos/redos8/
cd /var/www/html/repos/redos8/
```

Запустите процедуру создания зеркала репозитория-источника. Начнется загрузка пакетов репозитория. Обратите внимание, что на машине должен быть **доступ к сети Интернет**.

```
reposync --repoid=redos8_base_src --download-metadata --downloadcomps
```

При использовании дополнительного параметра `--newest-only` будут загружены только самые новые версии каждого пакета.

Для формирования/обновления метаданных локального репозитория необходимо выполнить команду:

```
createrepo -v /var/www/html/repos/redos8/redos8_base_src/ -g comps.xml
```

Параметр `-g comps.xml` требуется **только** при создании зеркала репозитория **RedOS - Base**.

ВАЖНО!

По аналогии создайте зеркало репозитория с обновлениями системы — **RedOS - Updates**.

Конфигурация репозитория **RedOS - Updates** находится в файле **/etc/yum.repos.d/RedOS-Updates.repo**.

Настройка на клиентском ПК

Для подключения локального репозитория на клиенте создайте запись для репозитория в каталоге **/etc/yum.repos.d/**, например:

```
nano /etc/yum.repos.d/RedOS8-Base-local.repo
```

Заполните файл следующим содержимым:

```
[RedOS8-Base-local]
 name=Local RED OS 8 Base repo
 baseurl=http://192.168.101.10/repos/redos8/redos8_base_src/
 # baseurl=http://repo.your.domain/repos/redos8/redos8_base_src/
 gpgcheck=1
 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
 enabled=1
```

Значение параметра `baseurl` задайте в зависимости от протокола, имени или IP-адреса сервера и пути к репозиторию.

ВАЖНО!

Настройка обращения к локальным репозиториям **Base** и **Updates** может быть осуществлена двумя способами:

- созданием собственных файлов репозиториев;
- редактированием файлов репозиториев, используемых по умолчанию.

При создании собственных файлов локальных репозиториев **не рекомендуется** удалять имеющиеся файлы репозиториев по умолчанию (**RedOS-Base.repo**, **RedOS-Updates.repo**) – их необходимо отключить, изменив значение параметра `enabled=1` на `enabled=0`! Иначе при обновлении системы данные файлы вновь появятся в каталоге **/etc/yum.repos.d/**.

В случае если были изменены и настроены файлы репозиториев по умолчанию (**RedOS-Base.repo**, **RedOS-Updates.repo**), после обновления системы в каталоге **/etc/yum.repos.d/** будут сохранены новые файлы расширением **.rpmnew** – они являются резервной копией стандартных конфигурационных файлов и не повлияют на текущую настройку локальных репозиториев, удалять их **не рекомендуется**.

Обновите информацию о репозиториях, для этого выполните следующие команды:

```
dnf makecache
```

Если настройка выполнена верно, команда будет завершена без ошибок.

Создание локального репозитория с использованием HTTPS

Предварительная настройка
Настройка SSL (HTTPS) для локального репозитория
Выпуск ключа и сертификата для веб-сервера
Настройка httpd для работы с SSL
Настройка на клиентском ПК

Окружение

- **Версия РЕД ОС**:
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: openssl-1:3.1.5-5, mod_ssl-2.4.58-1

В рамках данной статьи все действия должны выполняться с правами **администратора** системы или **суперпользователя root**.

Перейдите в сеанс пользователя **root** (если данная учётная запись включена):

```
su -
```

или выполните от имени администратора (пользователя в группе *wheel*) команду:

```
sudo su -
```

Предварительная настройка

В рамках предварительной настройки сервера создайте локальный репозиторий согласно нашей инструкции «Создание локального репозитория».

Настройка SSL (HTTPS) для локального репозитория

Использование **SSL** позволит обеспечить шифрование и целостность передаваемых данных, а также доверие к ресурсу, на котором расположены репозитории.

Выпуск ключа и сертификата для веб-сервера

Для настройки **SSL** необходимо получить SSL-сертификат от удостоверяющего центра (CA), запрос в который можно составить с помощью **openssl**:

1. Подготовьте файл конфигурации **openssl** для генерации запроса на сертификат веб-сервера:

```
nano /etc/httpd/openssl_repo.cnf
```

Содержимое файла:

```
[req]
 default_bits = 2048
 utf8 = yes
 distinguished_name = req_distinguished_name
 req_extensions = req_ext

 [req_distinguished_name]
 countryName = Country Name (2 letter code)
 countryName_default = RU
 commonName = Common Name (FQDN)
 commonName_max = 64
 commonName_default = repo.your.domain
 organizationName = Organization Name
```

```
organizationName_default = RedSoft

[req_ext]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
basicConstraints = CA:FALSE
subjectAltName = @alt_names

[alt_names]
DNS.1 = repo.your.domain
```

Значение repo.your.domain необходимо заменить на полное имя вашего хоста (сайта), которое будет использоваться при доступе к данному веб-серверу с репозиториями.

Примечание.

DNS-имя веб-сервера должно корректно разрешаться на клиентах. Это достигается либо созданием соответствующей записи на DNS-сервере, либо добавлением IP-адреса и имени веб-сервера в файл **/etc/hosts** на каждом клиенте.

2. Выполните генерацию закрытого ключа веб-сервера:

```
openssl genpkey -algorithm RSA -out /etc/pki/tls/private/web_repo.key
```

3. Выполните формирование запроса на сертификат:

```
openssl req -new -key /etc/pki/tls/private/web_repo.key -config /etc/httpd/openssl_repo.cnf -reqexts req_ext -out /root/web_repo.csr
```

4. Используйте сформированный файл запроса **/root/web_repo.csr** для выпуска сертификата веб-сервера в центре сертификации.

5. Полученный из центра сертификации файл сертификата разметите в системе:

```
cp /<путь_к_сертификату>/<имя_серитификата>.cer /etc/pki/tls/certs/web_repo.cer
```

Вариант с созданием и использованием собственного центра сертификации на базе **openssl** рассмотрен в разделе «**Генерация сертификата**» статьи «Настройка SSL для веб-серверов».

В качестве ***временной альтернативы*** можно выпустить *самоподписанный* сертификат (без использования ЦС) сроком на 30 дней для веб-сервера с помощью команды:

```
openssl req -x509 -nodes -newkey rsa:2048 -days 30 -keyout /etc/pki/tls/private/web_repo.key -out /etc/pki/tls/certs/web_repo.cer
```

где:

- -x509 — определяет необходимость создания самоподписанного сертификата, а не запроса на подпись;
- -nodes — пропустить опцию защиты сертификата с помощью пароля;
- -newkey rsa:2048 — указывает необходимость генерации нового сертификата и нового ключа RSA длиной 2048 бит;
- -days 30 — определяет срок действия сертификата (в днях);
- -keyout — каталог хранения и имя закрытого ключа;
- -out — каталог хранения и имя создаваемого сертификата.

Потребуется указать некоторые данные для запроса сертификата - страну, область, город или другой населенный пункт, наименование организации, наименование подразделения организации и сервер. Важным параметром здесь является Common Name (CN), где необходимо указать доменное имя сервера или его IP-адрес.

```
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/var/lib/dnf/server2.key'
-----
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:msk
Locality Name (eg, city) [Default City]:msk
Organization Name (eg, company) [Default Company Ltd]:rs
Organizational Unit Name (eg, section) []:rs
Common Name (eg, your name or your server's hostname) []:repo.your.domain
Email Address []:admin@rs.ru
```

В результате будут сформированы необходимые файлы — закрытый ключ и **самоподписанный** сертификат.

Настройка httpd для работы с SSL

Установите дополнительный модуль веб-сервера:

```
dnf install mod_ssl
```

Откройте файл конфигурации **SSL** службы **httpd**:

```
nano /etc/httpd/conf.d/ssl.conf
```

В секции определения настроек виртуального хоста **SSL** заполните выделенные параметры (раскомментируйте при необходимости):

```
<VirtualHost _default_:443>

ServerName repo.your.domain
SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/web_repo.cer
SSLCertificateKeyFile /etc/pki/tls/private/web_repo.key

</VirtualHost>
```

Для корректной работы значение параметра `ServerName` должно совпадать со значением полей `Common Name` и `Subject Alternative Name` сертификата веб-сервера.

Перезапустите **httpd** и проверьте его статус:

```
systemctl restart httpd
systemctl status httpd
```

Настройка на клиентском ПК

Для подключения локального репозитория на клиенте создайте запись для репозитория в каталоге **/etc/yum.repos.d/**, например:

```
nano /etc/yum.repos.d/RedOS8-Base-local.repo
```

Заполните файл следующим содержимым:

```
[RedOS8-Base-local]
name=Local RED OS 8 Base repo
baseurl=https://repo.your.domain/repos/redos8/redos8_base_src/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-RED-SOFT
enabled=1
```

Значение параметра `baseurl` задайте в зависимости от протокола, имени или IP-адреса сервера и пути к репозиторию.

Доступ к веб-серверу необходимо обеспечить по его DNS-имени.

С сервера, на котором настроен локальный репозиторий, необходимо скопировать сертификаты корневого и промежуточных центров сертификации (CA) в хранилище доверенных корневых сертификатов клиента. Скопировать необходимые файлы сертификатов на клиентскую машину можно, например, посредством команды scp.

На клиенте скопируйте полученный файл в хранилище сертификатов и обновите список доверенных сертификатов CA:

```
cp /<путь_к_сертификату>/CA.cer /etc/pki/ca-trust/source/anchors/
update-ca-trust extract
```

Примечание.

Если используется **временный самоподписанный** сертификат веб-сервера, то в конфигурационный файл репозитория **/etc/yum.repos.d/RedOS8-Base-local.repo** потребуется добавить строку `sslverify=0`.

По умолчанию параметр `sslverify=1`, однако в случае если сертификат не был добавлен в доверенные корневые сертификаты клиента, необходимо использовать значение `0` (раскомментировать строку `#sslverify=1`) для пропуска его проверки.

ВАЖНО!

Настройка обращения к локальным репозиториям **Base** и **Updates** может быть осуществлена двумя способами:

- созданием собственных файлов репозиториев;
- редактированием файлов репозиториев, используемых по умолчанию.

При создании собственных файлов локальных репозиториев **не рекомендуется** удалять имеющиеся файлы репозиториев по умолчанию (**RedOS-Base.repo**, **RedOS-Updates.repo**) – их необходимо отключить, изменив значение параметра `enabled=1` на `enabled=0`! Иначе при обновлении системы данные файлы вновь появятся в каталоге **/etc/yum.repos.d/**.

В случае если были изменены и настроены файлы репозиториев по умолчанию (**RedOS-Base.repo**, **RedOS-Updates.repo**), после обновления системы в каталоге **/etc/yum.repos.d/** будут сохранены новые файлы расширением **.rpmnew** – они являются резервной копией стандартных конфигурационных файлов и не повлияют на текущую настройку локальных репозиториев, удалять их **не рекомендуется**.

Обновите информацию о репозиториях, для этого выполните следующие команды:

```
dnf makecache
```

Если настройка выполнена верно, команда будет завершена без ошибок.

Настройка синхронизации локального репозитория

Вы можете подробнее ознакомиться с возможностью обновления репозиториев в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Обновления и изменения в принципах работы с репозиториями РЕД ОС;
- в **Яндекс.Дзен** — Обновления и изменения в принципах работы с репозиториями РЕД ОС;
- в **VK Видео** — Обновления и изменения в принципах работы с репозиториями РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

1) Перейдите в сеанс пользователя **root**:

```
su -
```

Далее команды будут выполняться с правами пользователя **root**, если не указано иное.

2) Обновите данные о пакетах в основном репозитории.

```
dnf clean all
dnf repolist
```

3) Синхронизируйте пакеты основного репозитория с локальным.

Пример синхронизации:

```
reposync -p /var/www/html/repo/red-os-8/base8/ --repo base8 --downloadcomps --download-metadata --norepopath
```

Если нужно синхронизировать только новые пакеты и удалить пакеты из локального репозитория, которых уже нет в основном, то воспользуйтесь командой:

```
reposync -p /var/www/html/repo/red-os-8/base8/ --repo base8 --downloadcomps --download-metadata --norepopath --newest-only --delete
```

4) Обновите метаданные репозитория.

```
createrepo --update /var/www/html/repo/red-os-8/base8/ -g comps.xml
```

Также для обновления репозитория можно воспользоваться скриптом по созданию локального репозитория.

Пример содержимого скрипта:

```
#!/bin/bash
 DESTDIR=/var/www/html/repo/red-os-8
 REPOIDS="base8 updates8 kernels8"
 dnf makecache
 for REPOID in $REPOIDS; do
   if [[ -f "$DESTDIR/$REPOID/.repodata" ]];
    then
      rm -rf $DESTDIR/$REPOID/.repodata
   fi
   reposync --repo $REPOID --newest-only --downloadcomps -p $DESTDIR
   if [[ -f "$DESTDIR/$REPOID/comps.xml" ]];
    then
      createrepo --update $DESTDIR/$REPOID -g comps.xml
    else
      createrepo --update $DESTDIR/$REPOID
   fi
 done
```

В переменной **DESTDIR** укажите свой путь до местонахождения вашего репозитория.

В строковой переменной **REPOIDS** указываются идентификаторы ваших репозиториев, а в цикле скрипта обрабатывается каждый из них.

Следующим шагом добавьте этот скрипт в планировщик задач **crontab**.

Модули ядра

Общая информация
Загрузка/выгрузка модулей ядра
Автозагрузка модулей
Черный список

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ядра**: 6.6.51-1

Модули ядра – это фрагменты кода, которые могут быть загружены и выгружены в ядро по требованию. Они расширяют функциональность ядра без необходимости перезагрузки системы. Модуль может быть настроен, как встроенный в ядро или как загружаемый во время работы операционной системы.

Примеры модулей ядра – это *драйверы* различных устройств.

Общая информация

Все модули хранятся в папке **/lib/modules/**. Т.к. модули рассчитаны только на определенную версию ядра, для каждой установленной версии создается свой подкаталог.

Чтобы просмотреть список установленных версий ядра, выполните следующую команду:

```
ls /lib/modules/
```

Если у вас только одна версия ядра, терминал выведет примерно следующее:

```
6.6.51-1.red80.x86_64
```

Если версий ядра несколько, все они будут указаны.

Может возникнуть необходимость просмотреть все установленные модули для текущего ядра в системе, для этого следует выполнить команду:

```
find /lib/modules/$(uname -r) -name *.ko

/lib/modules/6.6.51-1.red80.x86_64/kernel/fs/sysv/sysv.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/fs/ufs/ufs.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/fs/hfs/hfs.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/fs/nfs_common/nfs_acl.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/fs/nfs_common/grace.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/fs/coda/coda.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/crc8.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/ts_bm.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/asn1_encoder.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/crc4.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/ts_fsm.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/reed_solomon/reed_solomon.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/math/cordic.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/crc7.ko
/lib/modules/6.6.51-1.red80.x86_64/kernel/lib/lru_cache.ko
```

Иногда возникает необходимость уточнить, установлен ли какой-либо конкретный модуль ядра, для этого можно отфильтровать вывод поиска с помощью **grep**. Рассмотрим команду на примере модуля **ip_tables**:

```
find /lib/modules -name *.ko | grep ip_tables

/lib/modules/6.6.51-1.red80.x86_64/kernel/net/ipv4/netfilter/ip_tables.ko
```

Для просмотра драйверов и модулей, загруженных в данный момент в системе, используется команда:

```
lsmod
```

```
Module                  Size  Used by
uinput                 20480  1
snd_seq_dummy          12288  0
snd_hrtimer            12288  1
qrtr                   49152  2
rfkill                 28672  3
sunrpc                839680  1
snd_hda_codec_generic  110592  1
ledtrig_audio          12288  1 snd_hda_codec_generic
snd_hda_intel          61440  2
intel_rapl_msr         20480  0
snd_intel_dspcfg       36864  1 snd_hda_intel
joydev                 24576  0
intel_rapl_common      36864  1 intel_rapl_msr
```

Вывод представляет собой таблицу, в которой три столбца:

- *Module* — название модуля;
- *Size* — размер модуля (в байтах);
- *Used by* — количество экземпляров модуля, используемое в настоящее время. Нулевое значение говорит о том, что модуль не используется. Разделенный запятыми список после количества показывает, какие зависимости есть у модуля.

Если список загруженных в данный момент модулей большой, а интересует узнать, загружен ли какой-либо конкретный модуль, следует отфильтровать вывод командой **grep**:

```
lsmod | grep fuse
```

Если модуль загружен, *lsmod* его выведет. В противном случае — ответа на команду не будет.

В нашем случае модуль загружен и команда его показывает следующим образом:

```
fuse                  208896  5
```

Для отображения подробной информации о модуле используется команда:

```
modinfo <имя_модуля>
```

.

Выполним ее на примере модуля *fuse*:

```
modinfo fuse

filename:       /lib/modules/6.6.51-1.red80.x86_64/kernel/fs/fuse/fuse.ko
alias:          devname:fuse
alias:          char-major-10-229
alias:          fs-fuseblk
alias:          fs-fuse
license:        GPL
description:    Filesystem in Userspace
author:         Miklos Szeredi alias:          fs-fusectl
depends:
retpoline:      Y
intree:         Y
name:           fuse
vermagic:       6.6.51-1.red80.x86_64 SMP preempt mod_unload
sig_id:         PKCS#7
signer:         Build time autogenerated kernel key
sig_key:        7D:17:9F:94:5B:21:CB:37:D6:2C:F8:DA:24:AE:5E:6C:BF:6C:51:C4
sig_hashalgo:   sha512
signature:      CC:1D:9B:D8:90:10:9A:1F:75:2B:B5:D7:A1:76:EC:C4:EE:9B:82:21:
  D2:F6:60:E4:74:CA:54:40:D6:60:A5:61:AE:8C:F5:95:74:2C:B3:21:
  1D:B6:1B:64:B3:05:37:8B:3E:00:05:2F:24:03:92:E4:1B:79:03:BE:
  B9:A8:B1:E6:1C:16:67:C6:82:52:0D:D0:19:5D:C6:83:C9:B7:56:D9:
  55:35:78:25:33:89:47:0A:29:8B:C8:2B:4E:03:F2:5C:D0:C0:CF:A8:
  B0:33:54:66:3E:36:49:F4:77:89:03:2C:6F:E5:9F:42:B4:C6:30:4C:
  44:AD:04:DC:FE:92:E9:CE:1A:7F:FC:48:9E:4B:70:AB:F4:82:E4:D8:
  67:DD:B2:11:64:73:73:3A:85:B5:EA:4C:28:99:34:62:D4:A7:5C:62:
  EE:2C:57:FF:3E:1A:15:C8:13:39:7F:43:6C:C9:66:61:35:CA:99:66:
  2D:47:FF:B8:2E:75:59:E1:9E:33:A8:D3:01:F1:31:6B:E6:68:CC:1B:
```

```
  64:A3:A9:96:68:D5:F8:7E:9A:64:56:10:F1:2A:68:B3:4E:5B:7A:27:
  70:9C:81:F0:CD:E7:44:52:D8:26:0B:02:D3:8F:A2:8C:5F:BD:5C:4B:
  63:23:57:C2:0E:D5:E1:99:F2:BB:2D:4D:A5:A7:56:2E:6F:7D:84:11:
  30:BB:0E:03:26:FE:BC:A8:49:FF:7A:F4:0E:8D:AD:EC:CA:4B:CC:FE:
  07:70:F4:7E:60:5D:2C:4C:E7:D1:DA:28:E9:B0:1E:DD:13:4E:06:2D:
  66:F5:0F:63:98:D7:63:E4:DD:DC:74:2A:C7:C0:FC:8F:D4:3F:9F:20:
  2B:D3:E5:DF:B7:A3:8A:6F:8B:A8:55:BC:FB:3C:39:A7:97:44:7D:53:
  46:9B:B9:33:DF:BD:78:2A:BC:D0:2A:92:DB:A8:17:3F:E3:A5:25:C9:
  B7:0C:B2:80:F3:55:C1:2E:72:74:01:21:0A:AB:10:75:29:DF:5C:6F:
  28:24:91:04:FF:29:A3:7C:64:6A:7D:6A:4F:F0:76:56:F9:42:FD:E5:
  BF:90:10:87:D5:DE:FD:48:85:A6:04:D4:A4:F0:7A:F5:42:6F:C2:EB:
  74:85:BC:34:08:41:9C:51:05:7C:39:C9:DA:CE:67:77:69:3C:AD:B4:
  6D:4E:40:03:DC:26:CE:F4:5D:8F:E8:BA:FB:D9:8B:BA:E9:58:F5:C3:
  FE:4F:9F:3D:EA:92:D1:DB:E7:13:16:36:B5:CB:3B:CD:B1:50:EE:DD:
  4B:72:76:76:AB:EB:7F:BB:E1:6C:2E:31:C5:E9:6D:14:F9:06:03:38:
  B3:50:37:82:A6:64:7F:BF:43:25:78:16
parm:           max_user_bgreq:Global limit for the maximum number of backgrounded requests an unprivileged user can set (uint)
parm:           max_user_congthresh:Global limit for the maximum congestion threshold an unprivileged user can set (uint)
parm:           allow_sys_admin_access:Allow users with CAP_SYS_ADMIN in initial userns to bypass allow_other access check (bool)
```

Есть возможность просмотреть список опций, установленных для загруженного модуля. Просмотр осуществляется командой **systool** (входит в пакет **sysfsutils**):

```
systool [<опция> [имя_модуля]]

  -a   Show attributes
  -b <bus_name> Show a specific bus
  -c <class_name> Show a specific class
  -d   Show only devices
  -h   Show usage
  -m <module_name> Show a specific module
  -p   Show path to device/driver
  -v   Show all attributes with values
  -A <attribute_name> Show attribute value
  -D   Show only drivers
  -P   Show device's parent
```

Команда **systool** без переданных параметров выводит список всех модулей, разделенный на секции: *bus, class, devices, modules*. Это сделано для того, чтобы можно было корректно передавать команде опции и получать правильный вывод.

Чтобы отобразить конфигурацию определенного модуля, например **ip_tables**, выполним команду:

```
modprobe -c | grep fuse

alias char_major_10_229 fuse
alias devname:fuse fuse
alias fs_fuse fuse
alias fs_fuseblk fuse
alias fs_fusectl fuse
alias symbol:efuse_one_byte_read rtlwifi
alias symbol:efuse_power_switch rtlwifi
alias symbol:efuse_read_1byte rtlwifi
alias symbol:efuse_shadow_read rtlwifi
alias symbol:fuse_abort_conn fuse
alias symbol:fuse_conn_destroy fuse
alias symbol:fuse_conn_get fuse
alias symbol:fuse_conn_init fuse
alias symbol:fuse_conn_put fuse
alias symbol:fuse_dax_cancel_work fuse
alias symbol:fuse_dequeue_forget fuse
```

Получить список зависимостей модуля (или псевдонима), включая сам модуль, с созданием (возможно пустого) набора имён файлов модулей, по одному в строке, каждое из которых начинается с «*insmod*», можно с помощью команды:

```
modprobe --show-depends fuse

insmod /lib/modules/6.6.51-1.red80.x86_64/kernel/fs/fuse/fuse.ko
```

Загрузка/выгрузка модулей ядра

Загрузка модулей ядра осуществляется командами **modprobe** и **insmod**. Принцип их действия один и тот же, но отличаются передаваемые параметры. Команде **modprobe** передается только название модуля **modprobe <имя_модуля>**.

Например:

```
modprobe fuse
```

Для команды **insmod** необходимо передать адрес файла модуля (его можно узнать командой *modinfo*):

```
modinfo fuse | grep filename

filename:       /lib/modules/6.6.51-1.red80.x86_64/kernel/fs/fuse/fuse.ko
 insmod /lib/modules/6.6.51-1.red80.x86_64/kernel/fs/fuse/fuse.ko
```

Для выгрузки (выключения) модуля из ядра также можно использовать одну из двух команд - **modprobe** или **rmmode**. Команде **modprobe** обязательно требуется передать опцию **–r**:

```
modprobe -r fuse
```

Если после выполнения команды выгрузки возникает ошибка типа:

```
modprobe: FATAL: Module fuse is in use.
```

это значит, что в данный момент модуль выгружен быть не может, т.к. он используется. Бывает, что в ошибке явно указывается, какими модулями используется необходимый к выгрузке, и тогда сперва требуется выгрузить их.

Автозагрузка модулей

Для того чтобы каждый раз не производить ручную загрузку тех или иных модулей, работать с которыми требуется регулярно, в РЕД ОС существует отдельный каталог, в котором можно настроить автоматическую загрузку модулей при старте системы - **/etc/modules-load.d/**. В каталоге хранятся конфигурационные файлы ***.conf**, содержащие наименования необходимых модулей.

Кроме указанной выше директории также считываются файлы конфигурации из **/run/modules-load.d/*.conf** и **/usr/lib/modules-load.d/*.conf**. Если директории пустые, то можно создать файл и поместить нужные модули для автозагрузки. Каждый файл конфигурации имеет имя вида ***/modules-load.d/<program>.conf** .

Файлы конфигурации содержат список имён модулей ядра для загрузки, разделённых символами новой строки. Пустые строки и строки, чей первый не пробельный символ - **#** (решётка) или **;** (точка с запятой) игнорируются.

Например, можно создать файл **autorun.conf** в каталоге **/etc/modules-load.d/**:

```
nano /etc/modules-load.d/autorun.conf
```

В данный файл построчно добавляются все необходимые модули, например:

```
video
e1000
serio_raw
```

При следующей загрузке системы указанные в файле модули будут автоматически загружены.

Черный список

Чёрный список в контексте модулей ядра – это механизм, предотвращающий загрузку того или иного модуля. Это может быть полезно, если связанное оборудование не требуется или загрузка этого модуля вызывает проблемы. Например, могут быть два модуля ядра, которые пытаются управлять одним и тем же компонентом оборудования, и загрузка их вместе приведёт к конфликту.

Для запрета загрузки определенного модуля ядра создайте конфигурационный файл **block_modules.conf** в каталоге **/etc/modprobe.d/** и добавьте в нем строку для каждого модуля, который вы хотите добавить в чёрный список, используя ключевое слово «**blacklist**».

Например, если вы хотите запретить загрузку модуля **pcspkr**, создайте файл **/etc/modprobe.d/block_modules.conf** и добавьте в него строку:

```
blacklist pcspkr /bin/true
```

* где */bin/true* устанавливает запрет на загрузку модулей, зависящих от занесенного в черный список.

Некоторые модули загружаются как часть **initramfs**. То есть можно выделить модули, которые загружаются:

- из файлов **.ko**;
- как часть initramfs (initial ramdisk).

Для запрета загрузки модулей первого типа (загружаемых из файлов **.ko**) достаточно внести запись об этом модуле в файл **/etc/modprobe.d/*.conf** с директивой **blacklist**.

Для запрета загрузки модулей второго типа, кроме создания конфигурационного файла, необходимо также пересоздать **initramfs**. Пересоздание *initramfs* осуществляется следующей командой:

```
dracut --force /boot/initramfs-6.6.51-1.red80.x86_64.img 6.6.51-1.red80.x86_64 -v
```

* где **6.6.51-1.red80.x86_64** - это текущая версия ядра.

Настройка zswap

Включение и выключение Zswap
Изменение параметров

Zswap – это функция ядра, предоставляющая сжатый кэш в оперативной памяти для страниц подкачки. Страницы, которые ранее выгружались на жесткий диск, вместо этого сжимаются и сохраняются в пуле ОЗУ. Как только этот пул памяти заполнен или доступная оперативная память исчерпана, давно не использовавшиеся страницы разжимаются и выгружаются в подкачку, а сжатая её версия удаляется из пула. После того как страница была перемещена в режим подкачки, сжатая версия в пуле памяти может быть освобождена и использована снова.

Для дальнейшей настройки **zswap** перейдите в сеанс пользователя **root**:

```
su -
```

Далее все команды выполняются с правами пользователя **root**, если не указано иное.

Сначала необходимо определить, включен ли **Zswap** и какие у него настройки, выполнив команду в терминале:

```
grep -R . /sys/module/zswap/parameters

/sys/module/zswap/parameters/same_filled_pages_enabled:Y     # (функция идентификации страниц с одинаковыми значениями)
/sys/module/zswap/parameters/enabled:N     # (zswap выключен)
/sys/module/zswap/parameters/max_pool_percent:20     # (максимальный размер пула в оперативной памяти)
/sys/module/zswap/parameters/compressor:lzo     # (алгоритм сжатия данных)
/sys/module/zswap/parameters/zpool:zbud     # (zpool алгоритм управления памятью)
/sys/module/zswap/parameters/accept_threshold_percent:90     # (пороговое значение, при котором zswap снова начнет принимать страницы после того, как заполнится)
```

Дополнительную проверку наличия Zswap в ядре можно осуществить командой:

```
cat /boot/config-`uname -r` | grep -i zswap

CONFIG_ZSWAP=y     # (буква «y» означает, что поддержка есть)
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_DEFLATE is not set
CONFIG_ZSWAP_COMPRESSOR_DEFAULT_LZO=y
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_842 is not set
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_LZ4 is not set
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_LZ4HC is not set
# CONFIG_ZSWAP_COMPRESSOR_DEFAULT_ZSTD is not set
CONFIG_ZSWAP_COMPRESSOR_DEFAULT="lzo"
CONFIG_ZSWAP_ZPOOL_DEFAULT_ZBUD=y
# CONFIG_ZSWAP_ZPOOL_DEFAULT_Z3FOLD is not set
# CONFIG_ZSWAP_ZPOOL_DEFAULT_ZSMALLOC is not set
CONFIG_ZSWAP_ZPOOL_DEFAULT="zbud"
# CONFIG_ZSWAP_DEFAULT_ON is not set
```

Просмотреть сообщение, отображающееся при загрузке системы, можно командой:

```
dmesg | grep zswap

[ 0.781818] zswap: loaded using pool lzo/zbud
```

Включение и выключение Zswap

Для разового включения модуля **Zswap** выполните команду:

```
echo 1 > /sys/module/zswap/parameters/enabled
```

Чтобы отключить **Zswap** в работающей системе, необходимо сделать замену параметра с «**1**» на «**0**»:

```
echo 0 > /sys/module/zswap/parameters/enabled
```

Обратите внимание, что после перезагрузки операционной системы, значения параметров будут возвращены к величине по

умолчанию.

Проверка состояния производится командой:

```
cat /sys/module/zswap/parameters/enabled
```

Буква «**Y**» в выводе команды означает, что **Zswap** активирован.

Команды для включения и отключения модуля **Zswap** при старте операционной системы:

- команда для включения:

```
grubby --update-kernel ALL --args zswap.enabled=1
```

- команда для отключения:

```
grubby --update-kernel ALL --args zswap.enabled=0
```

Изменение параметров

Изменить размер пула (по умолчанию размер пула составляет 20% от всей оперативной памяти) можно, выполнив команду:

```
echo 15 > /sys/module/zswap/parameters/max_pool_percent
```

На системах с небольшим количеством оперативной памяти обычно устанавливается размер пула 5 - 15%, если оперативной памяти больше 2 Гб — 20 - 25%.

Убедитесь, что размер пула изменился:

```
cat /sys/module/zswap/parameters/max_pool_percent
```

Для изменения алгоритма управления памятью необходимо выполнить команду:

```
echo zsmalloc > /sys/module/zswap/parameters/zpool
```

По умолчанию **Zswap** использует алгоритм сжатия **lzo**, также может использовать любой алгоритм, поддерживаемый **api** ядра (например, lz4, zstd, deflate, lz4hc, lzo-rle), но для этого должен быть установлен модуль сжатия.

Проверьте наличие модуля **lz4** в системе командой:

```
modprobe lz4
```

Если команда ничего не выводит, значит модуль загружен, если выводится сообщение об ошибке — модуль отсутствует в ядре.

Чтобы изменить алгоритм сжатия на **lz4**, используйте команду:

```
echo lz4 > /sys/module/zswap/parameters/compressor
```

После перезагрузки операционной системы значения параметров, в которые были внесены изменения, будут возвращены к величине по умолчанию.

Сохранить внесенные изменения после перезагрузки можно следующим способом, для этого выполните команду:

```
grubby --update-kernel ALL --args "zswap.enabled=1 zswap.compressor=lz4 zswap.max_pool_percent=10 zswap.zpool=zsmalloc"
```

После выполнения команд **grubby** нужно обновить файл конфигурации **grub2** для применения настроек:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Выполните перезагрузку операционной системы:

```
reboot
```

Если необходимо получить статистику использования **Zswap**, используйте команду:

```
grep -r . /sys/kernel/debug/zswap
```

Поддержка оборудования в ядре ОС

Поддержка железа
Поддержка звука
Поддержка сети

Некоторые модели поддерживаемого оборудования указаны в разделе «Оборудование, совместимое с РЕД ОС».

Вопрос поддержки оборудования ядром и драйверами актуален всегда. Для того чтобы понять, как именно осуществляется проверка поддержки, рассмотрим основные инструменты и ссылки.

Для получения краткой сводки о комплектующих вашего ПК выполните команду:

```
loginfo.sh --hw-id
```

Предварительно **loginfo** должен быть обновлен до актуальной версии:

```
dnf update loginfo
```

Поддержка железа

Одним из популярных сайтов, в котором собраны ID устройств, является https://linux-hardware.org.

Однако, чтобы определить, какие **Vendor ID** (**VID**) и **Device ID** (**DID**) требуется вводить для понимания поддержки, воспользуйтесь утилитой **inxi**.

```
inxi -F -v 8
```

пример ID для **USB Bluetooth** / **USB Wi-Fi,** которые потребуются для эксперимента:

```
...

Device-2: 1-4:2 info: Realtek Bluetooth Radio type: Bluetooth driver: rtk_btusb interfaces: 2 rev: 1.1
speed: 12 Mb/s chip ID: 0bda:8771 serial: 00E04C239987
Device-3: 1-6:3 info: Realtek RTL8188EUS 802.11n Wireless Network Adapter type: Network driver: 8188eu
interfaces: 1 rev: 2.0 speed: 480 Mb/s chip ID: 0bda:8179 serial: 00E04C0001

...
```

В выводе отображаются 2 интересующих нас ID:

- Bluetooth - **0bda:8771**;
- Wi-Fi - **0bda:8179**.

Также рассмотрим альтернативу *linux-hardware.org* — **https://cateee.net**

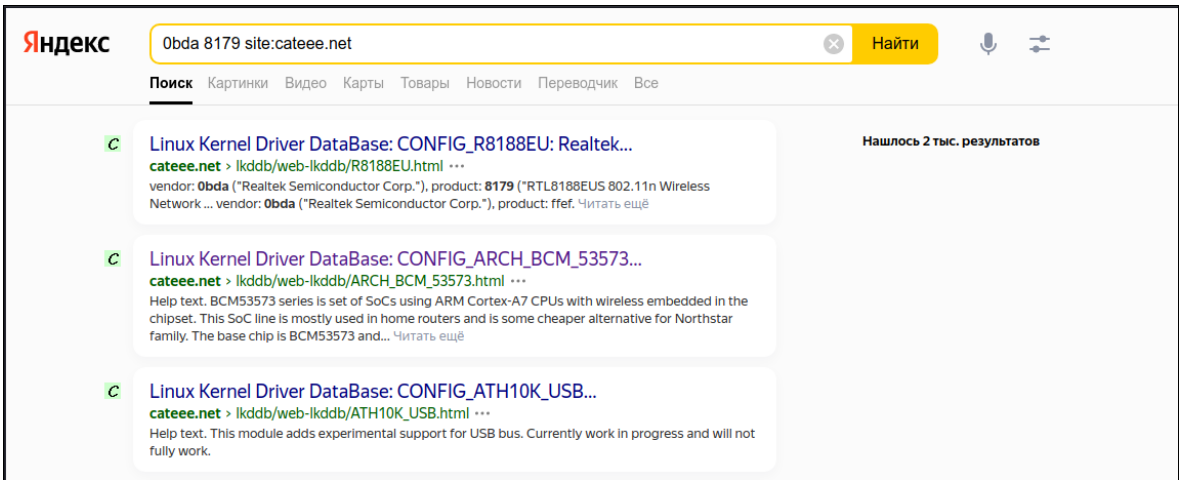
Данный сайт осуществляет поиск аналогично по ID. Для этого в поисковой строке требуется задать запрос вида:

<VID> <DID> site:cateee.net

или по одному из нужных ID.

Попробуем найти **0bda 8179** (**Wi-Fi**).

Имеется ряд результатов, в которых описывается, какой именно драйвер требует устройство:



Стоит упомянуть еще пару полезных ссылок для определения поддержки железа ядром:

- https://wireless.wiki.kernel.org/en/users/drivers
- https://h-node.org/hardware/catalogue/en

Также обращаем внимание на пункт **Driver** в выводе **inxi** - если он имеет значение отличное от **n/a**, значит у вас имеется поддержка устройства драйвером. Что это означает? Это значит, что вы можете найти данное устройство в заявленных драйвером через **modinfo**.

Bluetooth:

```
modinfo rtk_btusb | grep -i 0BDA

alias: usb:v0BDAp*d*dc*dsc*dp*icE0isc01ip01in*
```

В выводе показано, что есть метка **alias (алиас)**, являющаяся маской, по которой драйвер применяется к тому или иному устройству.

Аналогичную картину можно наблюдать для **Wi-Fi** адаптера:

```
modinfo 8188eu | grep -i 0BDA

alias: usb:v0BDAp8179d*dc*dsc*dp*ic*isc*ip*in*
```

Теперь рассмотрим проверку ядра на наличие интересующего драйвера.

Сначала проверим, установлен ли уже драйвер:

```
find /lib/modules/$(uname -r) -name *.ko | grep -i 8188eu

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/net/wireless/8188eu.ko
/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/staging/r8188eu/r8188eu.ko

find /lib/modules/$(uname -r) -name *.ko | grep -i rtk_btusb

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/bluetooth/rtk_btusb.ko
```

Как видно из вывода консоли, для ядра **5.15.10-3** данные драйвера имеются.

Существует также способ просмотра параметров ядра, с которыми оно было собрано. Для проверки того, какие были выбраны опции для драйвера, выполните команду:

```
cat /boot/config-$(uname -r) | grep -i 8188

CONFIG_RTL8188EE=m
CONFIG_R8188EU=m
```

А вот для bluetooth-драйвера вывод может выглядеть сомнительно:

```
cat /boot/config-$(uname -r) | grep -i BTUSB
```

```
CONFIG_BT_HCIBTUSB=m
CONFIG_BT_HCIBTUSB_AUTOSUSPEND=y
CONFIG_BT_HCIBTUSB_BCM=y
# CONFIG_BT_HCIBTUSB_MTK is not se t
CONFIG_BT_HCIBTUSB_RTL=y
```

Для того чтобы развеять сомнения, имеется ли драйвер - проверим его наличие следующим образом:

```
dnf provides *rtk_btusb.ko
```

Из полученного списка необходимо выбрать драйвер под свое ядро:

```
rtl8761b_5.15.10-3.el7.x86_64-1.0-8.el7.3.x86_64 : Kernel module for RTL8761B
Репозиторий        : kernels
Совпадения с:
Другое       : *rtk_btusb.ko
```

В случае, если драйвер отсутствует и в ядре, и в репозитории, существует вариант поиска необходимого драйвера на **github**.

Для этого необходимо в поиске по репозиториям **github** знать название нужного драйвера и попробовать найти интересующий. Так, к примеру, драйвер **8188eu** имеет множество разветвлений, которые охватывают широкий спектр устройств - примеры двух популярных вариаций драйвера:

- https://github.com/drygdryg/rtl8188eus;
- https://github.com/lwfinger/rtl8188eu.

Поддержка звука

Для проверки поддержки звука необходимо выполнить команду:

```
inxi -a -A

Audio:
 Device-1: NVIDIA vendor: ASUSTeK driver: snd_hda_intel v: kernel
 bus ID: 01:00.1 chip ID: 10de:10fa
 Device-2: AMD Family 17h HD Audio vendor: ASUSTeK driver: snd_hda_intel
 v: kernel bus ID: 05:00.6 chip ID: 1022:15e3
 Sound Server: ALSA v: k5.15.35-1.el7.3.x86_64

modinfo snd_hda_intel | grep -i 10de

alias:          pci:v0000 10DEd*sv*sd*bc04sc03i00*
```

Также можно попробовать поиск через легкое регулярное выражение, когда «**:**» заменяется на «**.***», что означает любые символы.

```
modinfo snd_hda_intel | grep -i 1022.*15e3

alias:          pci:v0000 1022d000015E3sv*sd*bc*sc*i*
```

Поддержка сети

Для проверки поддержки сети выполните команду:

```
inxi -a -N

Network:
 Device-1: Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet
 vendor: ASUSTeK driver: r8169 v: kernel port: e000 bus ID: 02:00.0
 chip ID: 10ec:8168
 Device-2: Realtek RTL8821CE 802.11ac PCIe Wireless Network Adapter
 vendor: AzureWave driver: rtw_8821ce v: N/A modules: rtw88_8821ce
 port: d000 bus ID: 04:00.0 chip ID: 10ec:c821

modinfo r8169 | grep -iE 10ec.*8168
```

```
alias:          pci:v000010ECd00008168sv*sd*bc*sc*i*
```

Бывают случаи, когда поле **driver** не определено (driver = N/A), но присутствует поле **module**, тогда стоит производить проверку по данному полю:

```
modinfo rtw88_8821ce | grep -iE 10ec.*c821

alias:          pci:v000010ECd0000C821sv*sd*bc*sc*i*
```

kernel-manager - утилита управления ядрами

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kernel-manager-0.1-7

В репозитории РЕД ОС доступна специальная утилита для управления ядрами операционной системы - **kernel-manager**.

Утилита содержит список всех доступных в репозитории версий ядра.

Вы можете подробнее ознакомиться с работой утилиты управления ядрами **kernel-manager**, просмотрев наши обучающие видео:

- на **RuTube** — kernel manager - утилита управления ядрами;
- в **Яндекс.Дзен** — kernel manager - утилита управления ядрами;
- в **VK Видео** — kernel manager - утилита управления ядрами.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

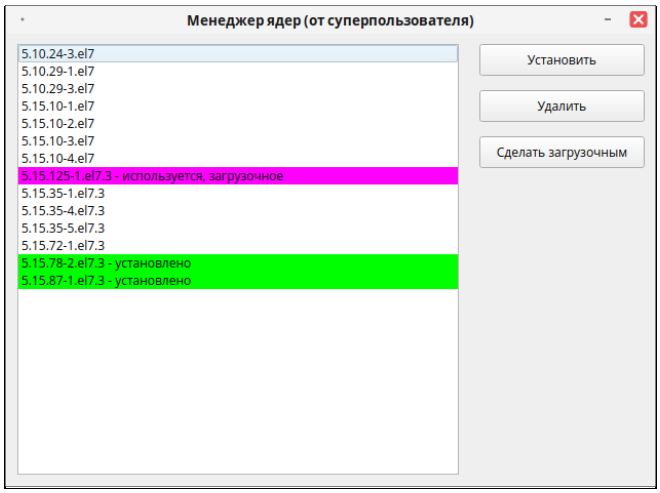
```
dnf install kernel-manager
```

После установки запуск утилиты доступен из «**Главного меню**» - «**Стандартные**» - «**Менеджер ядер**» или через терминал командой:

```
kernel-manager
```

Для работы с утилитой необходимы права суперпользователя **root**.

Окно утилиты выглядит следующим образом:

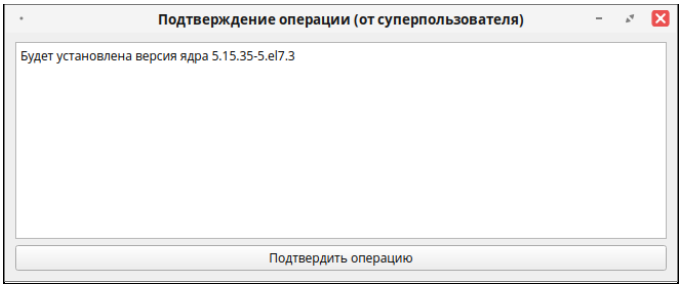


В списке слева отображаются все доступные в репозитории версии ядра. Розовым цветом подсвечивается используемое в данный момент операционной системой ядро. Зеленым цветом подсвечиваются установленные в системе версии ядра. Версии ядра без подсветки — не установлены в системе.

Справа доступны три кнопки действий:

- **Установить** — можно установить любую еще не установленную версию ядра из списка;
- **Удалить** — можно удалить любую установленную версию ядра, кроме используемой в данный момент;
- **Сделать загрузочным** — любую установленную версию ядра можно сделать загрузочной. При следующей загрузке системы использоваться будет именно она.

Для исключения случайного выполнения какого-либо действия выводится специальная форма с описанием операции, где необходимо нажать кнопку «**Подтвердить операцию**» в случае согласия или закрыть окно, в случае если действие выполнять не требуется.


Подтверждение операции (от суперпользователя)
Будет установлена версия ядра 5.15.35-5.el7.3
Подтвердить операцию

kdump — инструмент для анализа причин сбоев ядра

Минимальные требования
Запуск служб и проверка работы

Kdump — это стандартный механизм для создания дампа содержимого памяти компьютера при сбое ядра.

Минимальные требования

Минимальные требования к окружению:

- набор инструментов dracut – **dracut-056-9** и выше;
- механизм kexec – **kexec-tools-2.0.27** и выше.

Если в системе используются пакеты более ранних версий, обновите их:

```
dnf update
```

Если в системе пакеты не установлены, выполните команду:

```
dnf install dracut kexec-tools
```

Затем задайте размер для дампа ядра (в примере выделено **256 Мб** памяти). Для этого в файле **/etc/default/grub** добавьте в конец строки `GRUB_CMDLINE_LINUX=` параметр `crashkernel=256M` как показано в примере:

```
GRUB_CMDLINE_LINUX="rhgb quiet crashkernel=256M"
```

После внесения изменений необходимо обновить конфигурацию загрузчика **grub2**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Перезагрузите систему:

```
reboot
```

Запуск служб и проверка работы

В **dmesg** проверьте, что выделенная под дампы ядра память была зарезервирована:

```
dmesg | grep crashkernel

[    0.002111] Reserving 256MB of memory at 3312MB for crashkernel (System RAM: 4095MB)

kdumpctl status

Kdump: Kdump is not operational
```

Для оценки выделенной памяти используйте команду:

```
kdumpctl estimate
```

Далее запустите службу **kdump**и добавьте ее в автозагрузку:

```
kdumpctl start
systemctl enable kdump.service --now
```

Проверьте статус службы:

```
kdumpctl status
systemctl status kdump.service
```

В выводе должно быть **active (running)**.

Для проверки работы можно выполнить команду вызова паники ядра:

```
echo c > /proc/sysrq-trigger
```

Если настройка выполнена верно, в каталоге **/var/crash/<timestamp>** будут располагаться файлы дампов **kexec-dmesg.log**, **vmcore** и **vmcore-dmesg.txt**.

grubby - утилита настройки загрузчика ОС

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** grubby-8.40-72

GRUB является эталонной реализацией загрузчика, соответствующего спецификации Multiboot, и может загрузить любую совместимую с ней операционную систему. Кроме того GRUB может по цепочке передавать управление другому загрузчику, что позволяет ему загружать, например, ОС Windows, установленную рядом с РЕД ОС.

После настройки GRUB при включении компьютера пользователь видит список операционных систем, которые установлены на его компьютер и которые можно загрузить, выбрав подходящую и нажав «**Enter**».

GRUB позволяет при загрузке задавать произвольные параметры и передавать их в ядро Multiboot-совместимой ОС для дальнейшей обработки. GRUB — самый популярный загрузчик для Linux и является загрузчиком по умолчанию в большинстве известных дистрибутивов.

Здесь и далее под названием загрузчика GRUB подразумевается GRUB 2, который используется в Linux-системах, до него использовался GRUB первой версии, в настоящее время известный как GRUB Legacy. GRUB 2 полностью переписан с нуля и не имеет ничего общего с GRUB Legacy, разработка которого была остановлена в пользу более совершенного и мощного GRUB 2.

grubby является утилитой командной строки для настройки, отображения и обновления конфигураций загрузчика GRUB. По умолчанию **grubby** предустановлен в РЕД ОС.

Если в вашей системе утилита не установлена, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install grubby
```

Работа с утилитой **grubby** предоставляет множество преимуществ, включая простоту и согласованность во многих дистрибутивах. Для использования **grubby** не требуется обладать глубокими знаниями о файлах конфигурации утилиты.

Для генерации файла конфигурации GRUB 2 используется команда:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

После внесения изменений в файл конфигурации необходимо перезагрузить систему, чтобы изменения вступили в силу.

Для получения информации о работающем ядре системы выполните команду:

```
grubby --default-kernel

/boot/vmlinuz-6.6.6-1.red80.x86_64
```

Более подробную информацию о текущем ядре можно получить, выполнив команду:

```
grubby --info /boot/vmlinuz-$(uname -r)

kernel="/boot/vmlinuz-6.6.51-1.red80.x86_64"
args="ro rhgb quiet"
root="UUID=2df23883-b2e5-48ff-8144-48c54c172222"
initrd="/boot/initramfs-6.6.51-1.red80.x86_64.img"
title="RED OS (6.6.51-1.red80.x86_64) 8.0"
```

Для просмотра информации обо всех имеющихся версиях ядра используйте команду:

```
grubby --info ALL
```

С другими доступными опциями можно ознакомиться, выполнив:

```
grubby --help
```

Также можно отфильтровать вывод всех имеющихся версий ядра командой:

```
grubby --info=ALL | grep ^kernel

kernel="/boot/vmlinuz-6.6.51-1.red80.x86_64"
kernel="/boot/vmlinuz-6.6.6-1.red80.x86_64"
kernel="/boot/vmlinuz-0-rescue-459f810c15234e11b12a56eab4701744"
```

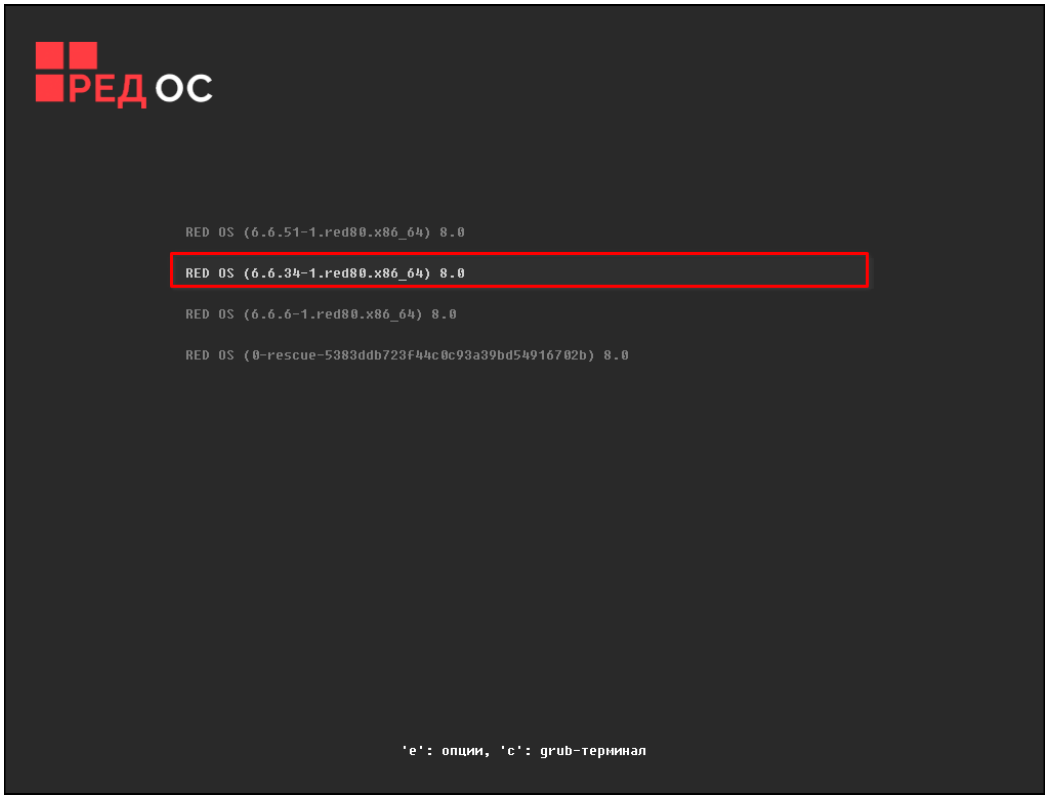
Для добавления новой записи в загрузчик выполните:

```
grubby --add-kernel=/boot/vmlinuz-6.6.34-1.red80.x86_64 --initrd=/boot/initramfs-6.6.34-1.red80.x86_64.img --copy-default
```

Проверьте, добавлена ли новая запись:

```
grubby --info=ALL | grep -E "^kernel|^index"

index=0
kernel="/boot/vmlinuz-6.6.51-1.red80.x86_64"
index=1
kernel="/boot/vmlinuz-6.6.34-1.red80.x86_64"
index=2
kernel="/boot/vmlinuz-6.6.6-1.red80.x86_64"
index=3
kernel="/boot/vmlinuz-0-rescue-5383ddb723f44c0c93a39bd54916702b"
```

После перезагрузки новая запись доступна для выбора в загрузчике.



Также можно добавить аргументы в ядро, чтобы загрузчик мог их обработать, командой:

```
grubby --update-kernel=current_kernel --args="kernel_args"
```

Например, для добавления новых записей и исключения **IPv6**:

```
grubby --update-kernel=/boot/vmlinuz-$(uname -r) --remove-args="ipv6.disable=1" --args="console=ttys0"
```

Загрузчик во время загрузки передает параметры ядру в буфер памяти, файл **/proc/cmdline** в псевдо-файловой системе **/proc** также содержит копию данных параметров. Проверить это можно при помощи команды:

```
cat /proc/cmdline

BOOT_IMAGE=/vmlinuz-6.6.51-1.red80.x86_64 root=UUID=2df23883-b2e5-48ff-8144-48c54c1722b9 ro resume=UUID=928c2360-1e08-49b5-b9a0-5fb19a04dd0a rhgb quiet
```

grub-customizer - утилита редактирования загрузчика ОС

GRUB (**Grand Unified Bootloader**) – программа-загрузчик операционной системы, которая позволяет выбирать и загружать операционные системы, установленные на компьютере. Помимо этого **grub** инициализирует параметры ядра системы и подготавливает систему к загрузке.



Настройка и редактирование загрузчика **grub** могут быть произведены с помощью графической утилиты **grub-customizer**. Данный вариант является довольно удобным и понятным.

Вы можете подробнее ознакомиться с установкой и настройкой утилиты **grub-customizer**, просмотрев наши обучающие видео:

- на **RuTube** — Удаление старых ядер из системы;
- в **Яндекс.Дзен** — Удаление старых ядер из системы;
- в **VK Видео** — Удаление старых ядер из системы.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты **grub-customizer** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install grub-customizer
```

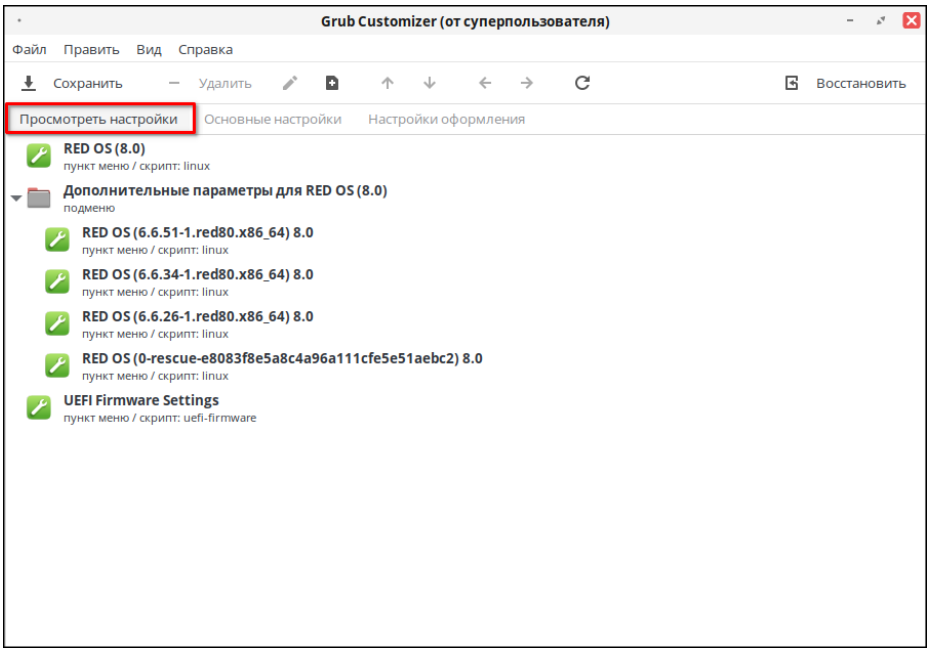
После установки запуск утилиты доступен из «**Главного меню**» - «**Администрирование**» - «**Настройки загрузчика**» или через консоль командой:

```
grub-customizer
```

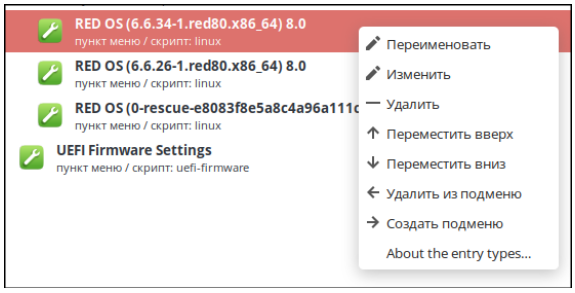
Перед запуском утилиты потребуется ввести пароль, так как для редактирования загрузчика операционной системы требуются права администратора.

Настройка утилиты

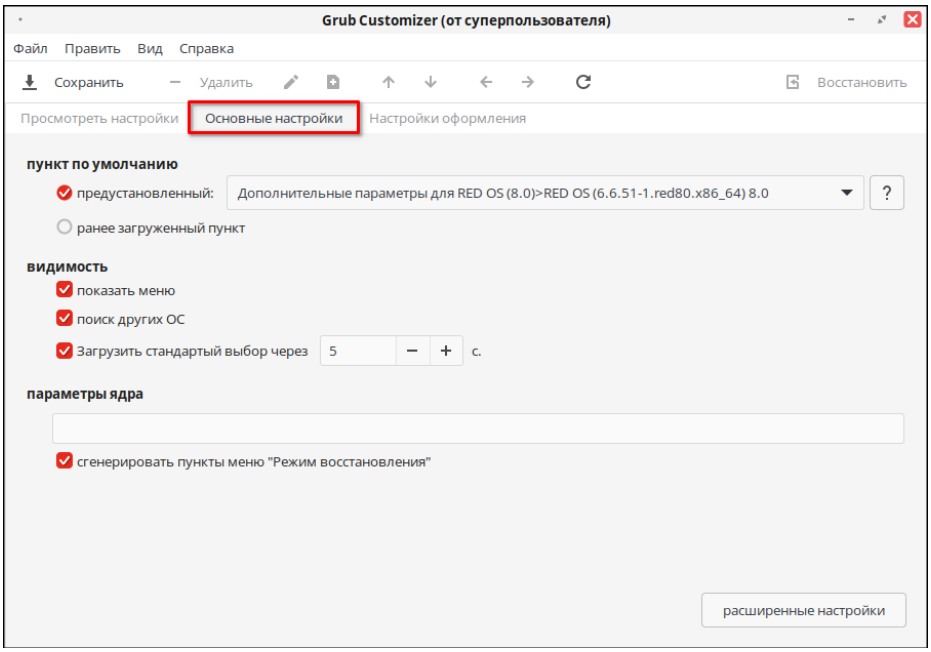
В главном окне программы отображается список доступных операционных систем, а в случае, если установлена одна ОС, то список представляет собой доступные версии ядра для загрузки.



В контекстном меню, вызываемом нажатием правой кнопкой мыши по требуемой ОС или версии ядра, есть возможность переименовать, отредактировать или переместить конфигурацию каждой ОС.

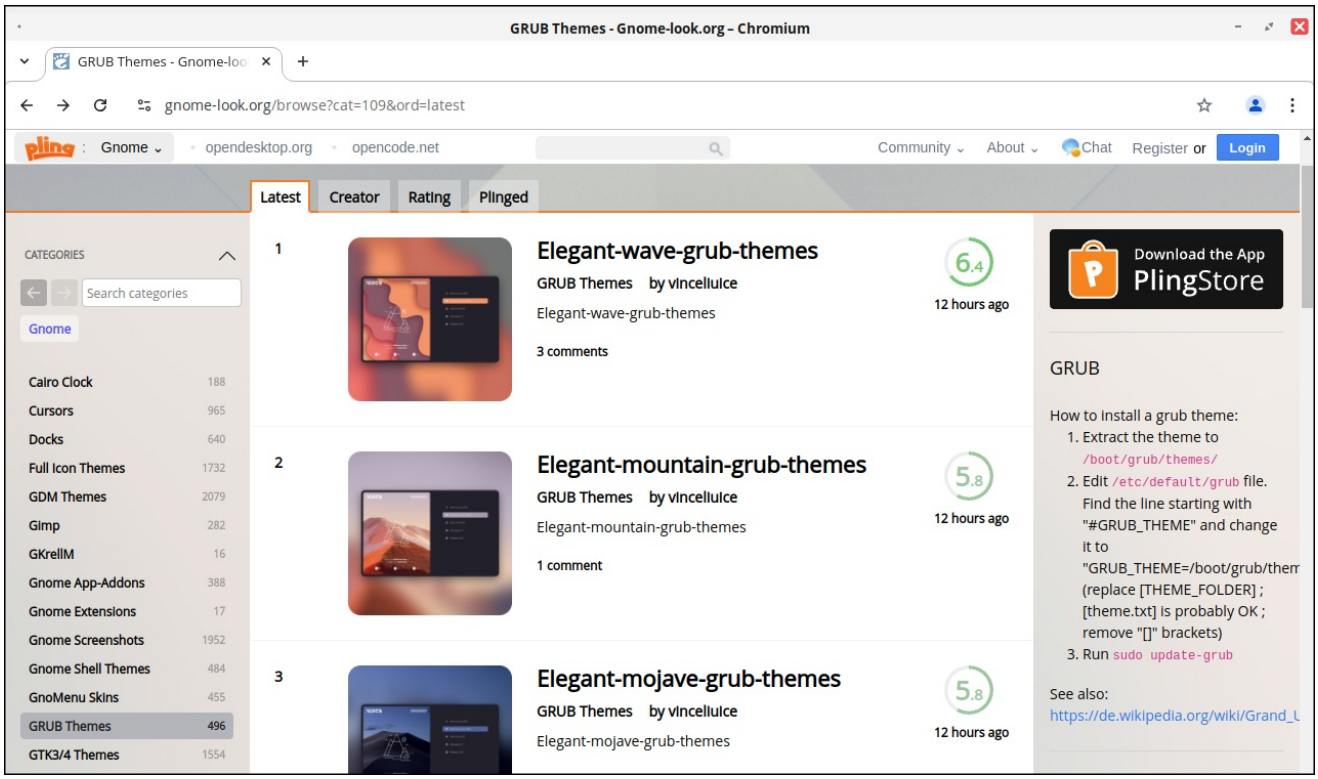


На вкладке «**Основные настройки**» можно выбрать необходимый пункт загрузчика, который будет использоваться по умолчанию, время, на протяжении которого будет отображаться меню **grub**, и параметры ядра для каждого пункта по умолчанию.



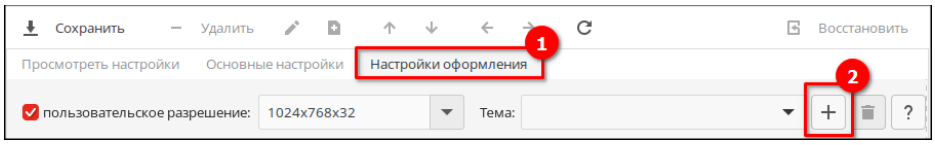
Вкладка «**Настройки оформления**» позволяет настроить отображение меню **grub**, а именно — цвет текста и фон. Также можно добавлять различные темы и устанавливать удобное разрешение экрана.

Для установки темы необходимо скачать архив понравившегося оформления меню **grub** с сайта gnome-look.org.

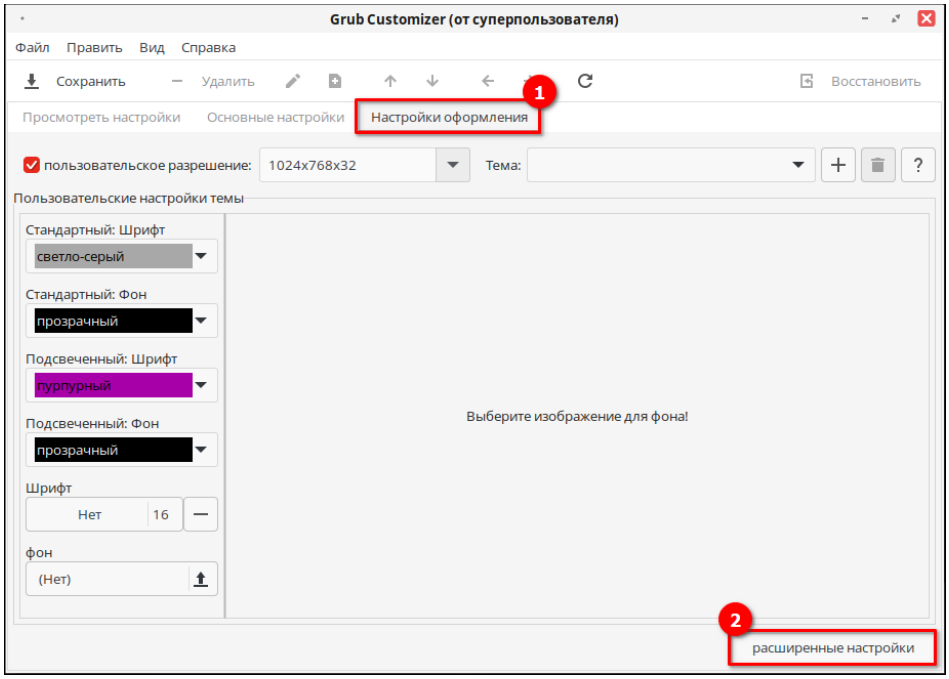


После того как архив выбранной темы будет скачан, с ним необходимо провести следующие преобразования: извлечь из архива папку с названием темы и заархивировать её отдельно. Данные действия необходимы для архивов, в которых помимо основной папки есть файл с разрешением **.sh**.

Для того чтобы добавить тему через утилиту **grub-customizer**, необходимо нажать на знак «**+**» рядом с раскрывающимся списком тем.

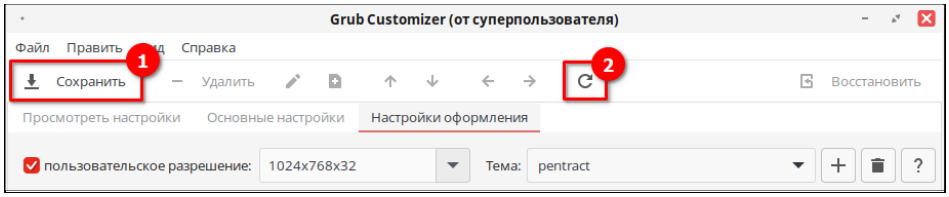


Кроме того, внизу экрана есть кнопка «**Расширенные настройки**».



В открывшемся окне можно более детально настроить значения переменных из конфигурационного файла **/etc/default/grub**.

Когда настройка **grub** будет завершена, необходимо нажать кнопки «**Сохранить**» и «**Обновить**» на верхней панели инструментов.



При следующей перезагрузке системы меню **grub** будет выглядеть в соответствии с выбранной и настроенной темой.



Назначение пароля на загрузчик GRUB2

Вы можете подробнее ознакомиться с возможностью назначения пароля на загрузчик **grub2**, просмотрев наши обучающие видео:

- на **RuTube** — Назначение пароля на загрузчик GRUB2;
- в **Яндекс.Дзен** — Назначение пароля на загрузчик GRUB2;
- в **VK Видео** — Назначение пароля на загрузчик GRUB2.

На наших каналах вы также сможете найти много другой полезной информации.

Для защиты от несанкционированных изменений и прерывания нормальной загрузки ОС рекомендуется установить пароль на загрузчик GRUB.

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

Затем выполните команду, в ответе которой назначьте новый пароль и, для исключения ошибок ввода, повторите его:

```
grub2-setpassword

Enter password: <новый_пароль_для_grub2>
Confirm password: <повторите_пароль>
```

На системах с загрузкой посредством **UEFI** команду необходимо выполнить в таком варианте:

```
grub2-setpassword -o /boot/efi/EFI/redos/
```

Для применения настроек перезагрузите систему:

```
reboot
```

Далее при запуске системы нажмите клавишу «**e**».

Будет открыта форма для авторизации:

```
Введите имя пользователя:
root
Введите пароль:
<новый_пароль_для_grub2>
```

Если необходимо убрать с определенного пункта меню GRUB запрос пароля, в конфигурационном файле **/boot/grub2/grub.cfg** откройте файл на редактирование:

```
sudo nano /boot/grub2/grub.cfg
```

Найдите загрузочную строку и добавьте параметр **--unrestricted**.

```
### BEGIN /etc/grub.d/10_linux ###
menuentry 'RED OS (8.0)' --class red --class gnu-linux --class gnu --class os --unrestricted $menuentry_id_option 'gnulinux-s>
        load_video
        set gfxpayload=1024x768x32
        insmod gzio
        insmod part_gpt
        insmod ext2
        set root='hd0,gpt2'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 --hint-efi=hd0,gpt2 --hint-baremetal=ahci0,gpt2 --hint>
        else
          search --no-floppy --fs-uuid --set=root 71d17031-5a26-4d30-ba25-d2cacfa16a91
        fi
        echo    'Загружается Linux 6.6.51-1.red80.x86_64 …'
        linux   /vmlinuz-6.6.51-1.red80.x86_64 root=UUID=5b25f5f1-2ee8-4ee2-8b0d-524f3cde5e1e ro resume=UUID=cd77454c-60a6-44>
        echo    'Загружается начальный виртуальный диск …'
        initrd  /initramfs-6.6.51-1.red80.x86_64.img
}
```

Для систем с **UEFI** файл конфигурации располагается в по адресу **/boot/efi/EFI/redos/grub.cfg**.

Восстановление загрузчика GRUB2

Восстановление загрузчика для систем, использующих BIOS
Восстановление загрузчика для систем, использующих UEFI

Вы можете подробнее ознакомиться с восстановлением загрузчика **grub2** и восстановлением для систем, просмотрев наши обучающие видео:

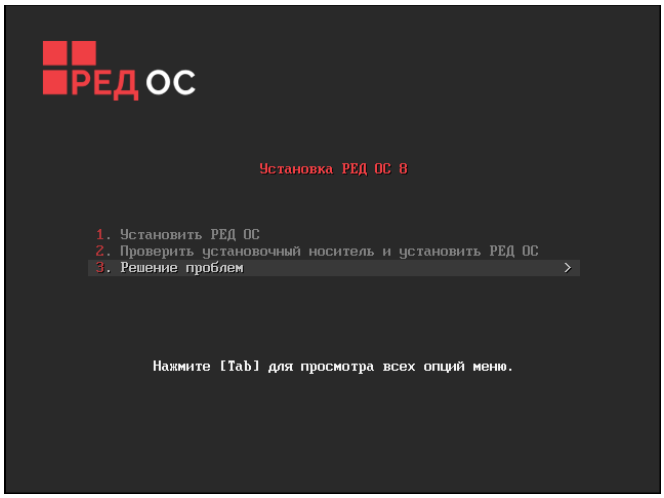
- на **RuTube** — Восстановление загрузчика GRUB2;
- в **Яндекс.Дзен** — Восстановление загрузчика GRUB2;
- в **VK Видео** — Восстановление загрузчика GRUB2.

На наших каналах вы также сможете найти много другой полезной информации.

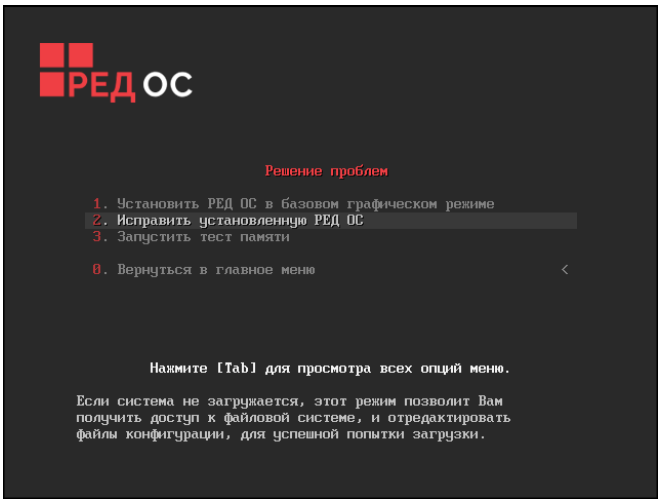
Для восстановления необходимо загрузиться с установочного образа вашей версии РЕД ОС, поставив ваш носитель первым в списке предпочтения загрузки.

Восстановление загрузчика для систем, использующих BIOS

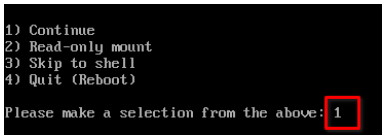
В появившемся меню следует выбрать пункт «**Решение проблем**».



Далее нужно выбрать пункт «**Исправить установленную RED OS**»:



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***:



Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Для определения диска, на котором установлена система, можно использовать следующую команду:

```
lsblk
```

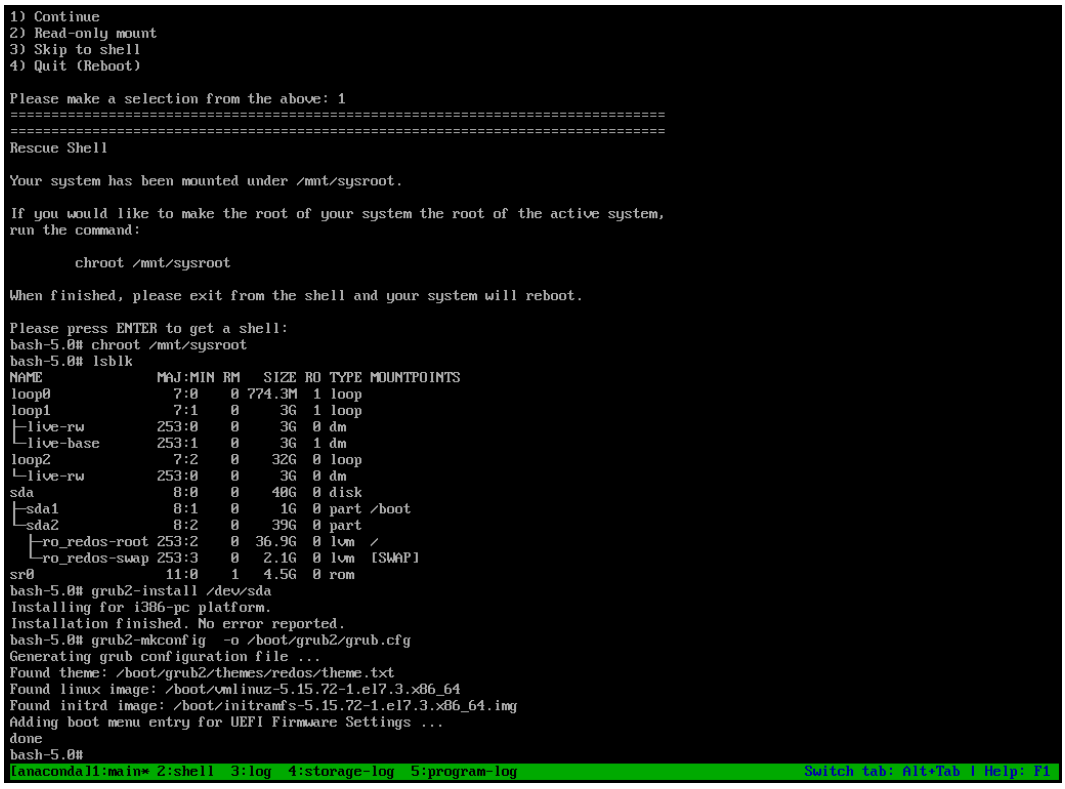
Далее выполните установку загрузчика командой (в конце указывается нужный диск):

```
grub2-install /dev/sda
```

Теперь создайте новый конфигурационный файл загрузчика с помощью команды:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Восстановление загрузчика для систем, использующих UEFI

В появившемся меню следует выбрать пункт «**Решение проблем**».



Далее нужно выбрать пункт «**Исправить установленную РЕД ОС**».



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***:

Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему

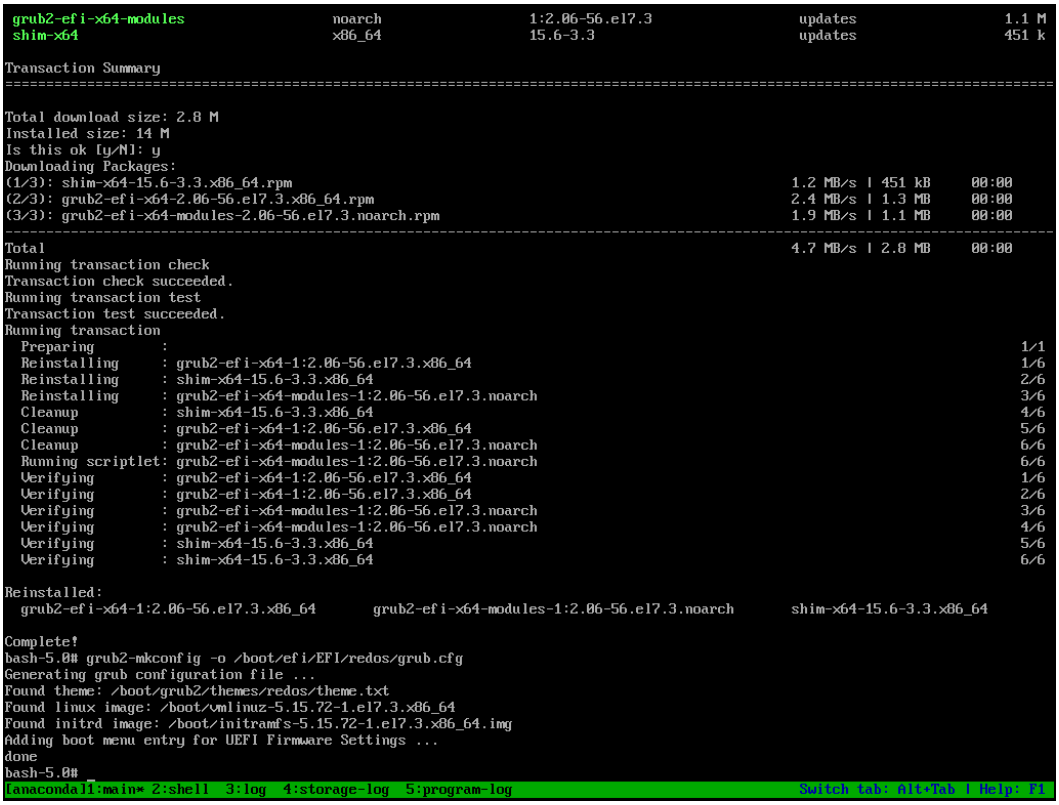
корневой средой):

```
chroot /mnt/sysroot
```

Затем потребуется обновить конфигурацию загрузчика с помощью команд:

```
dnf reinstall grub2-efi-x64  shim-x64 grub2-efi-x64-modules
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Описание процесса разметки диска

Так же, как и в других файловых системах, все данные хранятся на диске по определенным адресам. Эти адреса сохранены в метаданных. И тут уже начинаются различия. Все метаданные организованны в виде B-деревьев. Это дает большую производительность при работе с файловой системой, а также позволяет добавлять неограниченное количество файлов.

Когда вы перезаписываете файл, данные не перезаписываются, а лишь модифицированная часть копируется в новое место. Затем просто обновляются метаданные. Это позволяет создавать мгновенные снимки файловой системы, которые не занимают места на диске, пока не было внесено много изменений. Если же старый блок больше не нужен, потому что он не является частью какого-либо снимка, то он автоматически удаляется.

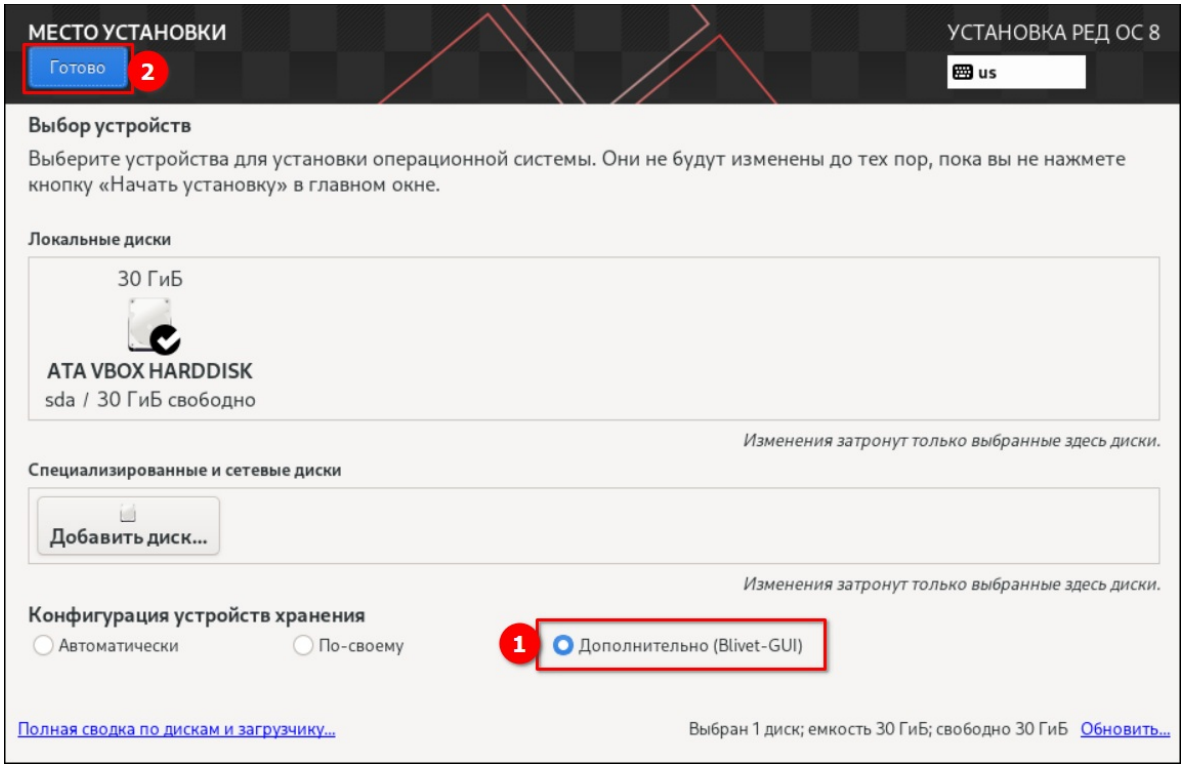
Каждый диск, независимо от его размера, делится на блоки по **1 Гб** для данных и **256 Мб** для метаданных. Затем эти блоки собираются в группы, каждая из которых может храниться на разных устройствах, количество таких блоков в группе может зависеть от уровня RAID для группы. Менеджер томов уже интегрирован в файловую систему, поэтому больше никакое дополнительное ПО использовать не нужно.

Защита и сжатие данных также поддерживается на уровне файловой системы, так что здесь вам тоже не нужны дополнительные программы. Также файловая система btrfs поддерживает зеркалирование данных на нескольких носителях. Вот другие особенности btrfs, которые можно упомянуть:

- Поддержка снимков файловой системы, только для чтения или для записи;
- Контрольные суммы для данных и метаданных с помощью алгоритма **crc32**. Таким образом, можно очень быстро определить любые повреждения блока;
- Сжатие с помощью **Zlib** и **LZO**;
- Оптимизация для работы с **SSD**, файловая система автоматически определяет **ssd** и начинает вести себя по-другому;
- Фоновый процесс для обнаружения и исправления ошибок, а также дефрагментации и дедупликации в реальном времени;
- Поддерживается преобразование из **ext4** и **ext3**.

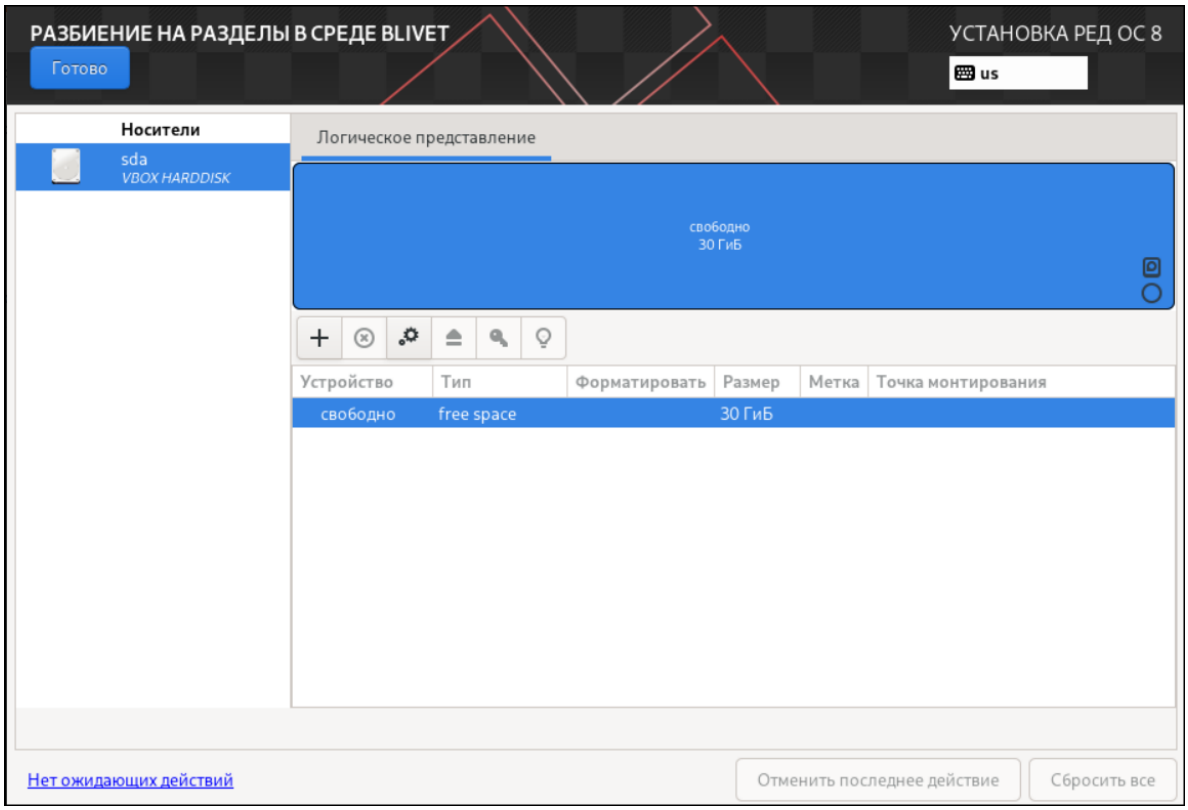
Создание тома при установке ОС (через blivet-gui)

При установке ОС для создания тома при помощи **blivet-gui**, нужно в «**Конфигурации устройств хранения**» выбрать пункт «**Дополнительно (Blivet-GUI)**», после чего нажать кнопку «**Готово**», которая находится сверху слева.

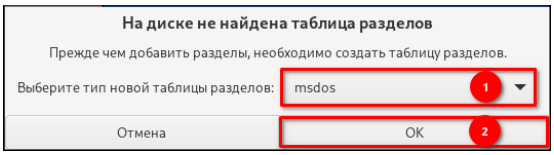


Далее происходит переход в раздел «**Разбиение на разделы в среде BLIVET**», где уже можно создать необходимые тома и подтома.

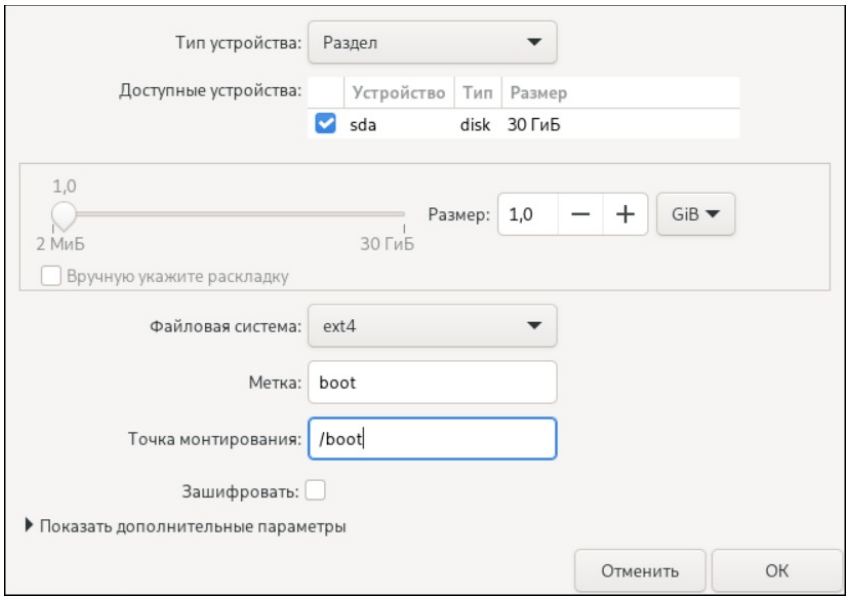
Для создания раздела нужно нажать на кнопку «**+**».



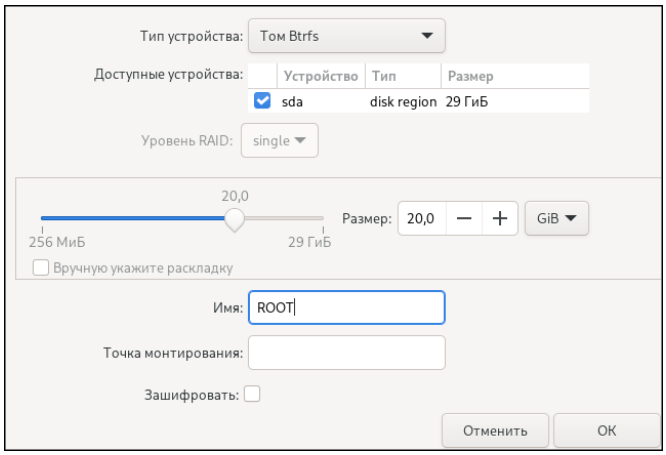
Установите тип новой таблицы разделов msdos и нажмите «OK».



Сначала необходимо создать раздел с местом установщика системы, нажав на кнопку «+».



Для создания тома необходимо выбрать носитель, на котором будут создаваться тома, и нажать на кнопку «+». После чего появится окно:



В данном окне предлагается выбрать тип устройства, размер, выделяемый на это устройство, файловую систему и точку монтирования.

Для создания тома с файловой системой **btrfs**:

- измените пункт «**Тип устройства**» на «**Том Btrfs**»;
- измените размер тома на необходимый;
- укажите имя тома;
- поле «**Точка монтирования**» оставьте без изменений;
- нажмите «**OK**».

Создастся новый том со своим названием.

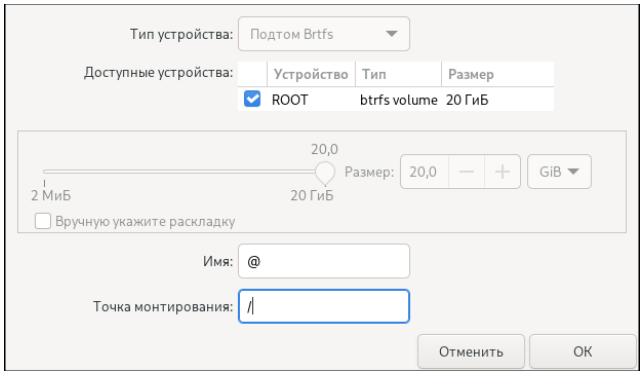


Для того чтобы создать подтом, нужно нажать на новый том и снова нажать на кнопку «**+**», после чего появится окно редактирования настроек.

При создании можно выбрать необходимый из доступных томов, чтобы в нём создать подтом.

Также в данном окне необходимо задать имя подтома и точку монтирования. В данном случае в поле «**Точка монтирования**» задано значение «**/**», которое включает в себя корневая директорию, содержащая всю файловую иерархию.

После чего нажиманием «**OK**».



После чего в списке устройств, можно увидеть созданный том и подтом.

Работа с квотами диска

Сначала можно посмотреть список доступных **subvolume** командой:

```
sudo btrfs subvolume list /

ID 256 gen 4371 top level 5 path @
ID 261 gen 4354 top level 256 path var/lib/portables
```

Для создания **subvolume** требуется ввести команду:

```
sudo btrfs subvolume create /@QUOTA

Create subvolume '//@QUOTA'
```

Для включения поддержки квот выполните команду:

```
sudo btrfs quota enable /@QUOTA
```

Для просмотра списка доступных **subvolume**, на которые можно ввести ограничения, требуется выполнить команду:

```
sudo btrfs qgroup show /

qgroupid         rfer         excl
--------         ----         ----
0/5         16.00Kib     16.00Kib
0/256        5.85Kib      5.85Kib
0/261       16.00Kib     16.00Kib
0/266       16.00Kib     16.00Kib
```

Для выбора нужного **ID** необходимо провести аналогию с выводом из команды btrfs subvolume list /, и на основе сопоставления **qgroupid** и **ID** назначать квоту.

В данном случае **ID** - **0/266** является только что созданной **subvolume** - **/@QUOTA**.

Для того чтобы ввести ограничения на **subvolume**, нужно выполнить:

```
sudo btrfs qgroup limit 1G /@QUOTA/
```

findmnt - получение информации о подключенных файловых системах

Findmnt – это утилита командной строки, используемая для отображения списка подключенных файловых систем или поиск файлов системы в **/etc/fstab**, **/etc/mtab** или **/proc/self/mountinfo**. Если устройство или точка монтирования не заданы, будут обнаружены все регистрируемые файловые системы.

Для отображения списка подключенных файловых систем выполните команду:

```
findmnt

TARGET                   SOURCE     FSTYPE  OPTIONS
/                        /dev/mapper/ro_redos-root
│                                   ext4    rw,relatime,seclabel
├─/sys                   sysfs      sysfs   rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/kernel/security securityfs securit rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/cgroup       cgroup2    cgroup2 rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/pstore       pstore     pstore  rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/bpf          bpf        bpf     rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/selinux      selinuxfs  selinux rw,relatime
│ ├─/sys/kernel/debug    debugfs    debugfs rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/kernel/tracing  tracefs    tracefs rw,nosuid,nodev,noexec,relatime,
│ ├─/sys/fs/fuse/connections fusectl    fusectl rw,nosuid,nodev,noexec,relatime
│ └─/sys/kernel/config   configfs   configf rw,nosuid,nodev,noexec,relatime
├─/proc                  proc       proc    rw,nosuid,nodev,noexec,relatime
│ └─/proc/sys/fs/binfmt_misc systemd-1  autofs  rw,relatime,fd=30,pgrp=1,timeout
├─/dev                   devtmpfs   devtmpf rw,nosuid,noexec,seclabel,size=4
│ ├─/dev/shm             tmpfs      tmpfs   rw,nosuid,nodev,seclabel,inode64
│ ├─/dev/pts             devpts     devpts  rw,nosuid,noexec,relatime,seclab
│ ├─/dev/hugepages       hugetlbfs  hugetlb rw,relatime,seclabel,pagesize=2M
│ └─/dev/mqueue          mqueue     mqueue  rw,nosuid,nodev,noexec,relatime,
├─/run                   tmpfs      tmpfs   rw,nosuid,nodev,seclabel,size=19
│ ├─/run/user/42         tmpfs      tmpfs   rw,nosuid,nodev,relatime,seclabe
│ ├─/run/user/1000       tmpfs      tmpfs   rw,nosuid,nodev,relatime,seclabe
│ │ └─/run/user/1000/gvfs    gvfsd-fuse fuse.gv rw,nosuid,nodev,relatime,user_id
│ └─/run/media/user/redos-MUROM-7.3 x86_64
│                         /dev/sr0   iso9660 ro,nosuid,nodev,relatime,nojolie
├─/boot                  /dev/sda1  ext4    rw,relatime,seclabel
└─/var/lib/nfs/rpc_pipefs  sunrpc     rpc_pip rw,relatime
```

В выводе отображается точка монтирования **TARGET**, исходное устройство **SOURCE**, тип файловой системы **FSTYPE** и дополнительные параметры **OPTIONS** для каждой файловой системы.

По умолчанию команда findmntвыводит данные в древовидном формате. Чтобы отобразить информацию в виде списка, используйте опцию **-l** :

```
findmnt -l

TARGET                        SOURCE                FSTYPE          OPTIONS
/sys                          sysfs                 sysfs           rw,nosuid,nodev,noexec,relatime,seclabel
/proc                         proc                  proc            rw,nosuid,nodev,noexec,relatime
/dev                          devtmpfs              devtmpfs        rw,nosuid,noexec,seclabel,size=4096k,nr_inodes=65536,mode=755,inode64
/sys/kernel/security          securityfs            securityfs      rw,nosuid,nodev,noexec,relatime
/dev/shm                      tmpfs                 tmpfs           rw,nosuid,nodev,seclabel,inode64
/dev/pts                      devpts                devpts          rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000
/run                          tmpfs                 tmpfs           rw,nosuid,nodev,seclabel,size=199140k,nr_inodes=819200,mode=755,inode64
/sys/fs/cgroup                cgroup2               cgroup2         rw,nosuid,nodev,noexec,relatime,seclabel,nsdelegate
/sys/fs/pstore                pstore                pstore          rw,nosuid,nodev,noexec,relatime,seclabel
/sys/fs/bpf                   bpf                   bpf             rw,nosuid,nodev,noexec,relatime,mode=700
/                             /dev/mapper/ro_redos-root ext4        rw,relatime,seclabel
/sys/fs/selinux               selinuxfs             selinuxfs       rw,relatime
/proc/sys/fs/binfmt_misc      systemd-1             autofs
rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=17271
/dev/hugepages                hugetlbfs             hugetlbfs       rw,relatime,seclabel,pagesize=2M
/dev/mqueue                   mqueue                mqueue          rw,nosuid,nodev,noexec,relatime,seclabel
/sys/kernel/debug             debugfs               debugfs         rw,nosuid,nodev,noexec,relatime,seclabel
/sys/kernel/tracing           tracefs               tracefs         rw,nosuid,nodev,noexec,relatime,seclabel
/sys/fs/fuse/connections      fusectl               fusectl         rw,nosuid,nodev,noexec,relatime
/sys/kernel/config            configfs              configfs        rw,nosuid,nodev,noexec,relatime
/boot                         /dev/sda1             ext4            rw,relatime,seclabel
/var/lib/nfs/rpc_pipefs       sunrpc                rpc_pipefs      rw,relatime
/run/user/42                  tmpfs                 tmpfs
rw,nosuid,nodev,relatime,seclabel,size=99568k,nr_inodes=24892,mode=700,uid=42,gid=42,inode64
```

```
/run/user/1000                  tmpfs                  tmpfs
rw,nosuid,nodev,relatime,seclabel,size=99568k,nr_inodes=24892,mode=700,uid=1000,gid=1000,inode64
/run/user/1000/gvfs             gvfsd-fuse             fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=1000,group_id=1000
/run/media/user/redos-MUROM-7.3 x86_64 /dev/sr0        iso9660
ro,nosuid,nodev,relatime,nojoliet,check=s,map=n,blocksize=2048,uid=1000,gid=1000,dmode=500,fmode=400,iocharset=utf8
```

Для отображения только определенной файловой системы используется параметр **-t**, в качестве аргумента которому необходимо передать тип файловой системы. Например:

```
findmnt -t ext4

TARGET  SOURCE                  FSTYPE OPTIONS
/       /dev/mapper/ro_redos-root ext4   rw,relatime,seclabel
└─/boot /dev/sda1               ext4   rw,relatime,seclabel
```

Найти файловую систему также можно, используя точку монтирования. Например, команда `findmnt --fstab /boot` отобразит все файловые системы **/etc/fstab**, где каталогом точки монтирования является **/boot**.

```
findmnt --fstab /boot

TARGET SOURCE                                FSTYPE OPTIONS
/boot  UUID=890a40d8-ab34-44b8-9632-6f6026dcb78e ext4   defaults
```

Чтобы вывести все файловые системы **/etc/fstab** и преобразовать теги *LABEL* и *UUID* в реальные имена устройств, необходимо в команду добавить ключ **--evaluate**.

```
findmnt --fstab /boot --evaluate

TARGET SOURCE    FSTYPE OPTIONS
/boot  /dev/sda1 ext4   defaults
```

Findmnt также позволяет отслеживать действия по монтированию и размонтированию в файловой системе. Для этого используется команда:

```
findmnt -p
```

Для отображения определенных событий следует указать точку монтирования, например, **/mnt/test**:

```
findmnt --poll --mountpoint /mnt/test
```

Для проверки правильности точек проверки следует контрольная команда (с правами администратора системы или суперпользователя **root**):

```
findmnt --verify

Success, no errors or warnings detected
```

Для получения более подробной информации в выводе используется параметр **--verbose** :

```
findmnt --verify --verbose

/
   [ ] target exists
   [ ] source /dev/mapper/ro_redos-root exists
   [ ] FS type is ext4
/boot
   [ ] target exists
   [ ] UUID=890a40d8-ab34-44b8-9632-6f6026dcb78e translated to /dev/sda1
   [ ] source /dev/sda1 exists
   [ ] FS type is ext4
none
   [ ] source /dev/mapper/ro_redos-swap exists
   [ ] FS type is swap
Success, no errors or warnings detected
```

Проверка файловой системы на наличие ошибок

Параметры fsck
Пример проверки диска на ошибки с помощью fsck
Запуск автоматической проверки и исправления найденных ошибок
Ручное добавление параметров в меню GRUB при загрузке ОС
Добавление параметров в меню GRUB с помощью утилиты grubby
Создание файла /forcefsck
Запуск проверки в ручном режиме
Использование загрузочного диска/flash для проверки файловой системы на ошибки
Проверка LVM-разделов с помощью утилиты fsck

В определенных случаях (в результате сбоя или некорректного завершения работы) на файловой системе могут накапливаться ошибки. В РЕД ОС для проверки файловой системы и исправления ошибок имеется утилита **fsck** ("file system consistency check").

Инструмент fsck обладает следующим функционалом:

- проверка файловой системы при возникновении проблем (не загружается система/поврежденные файлы) или в качестве профилактического обслуживания;
- диагностика состояния внешних накопителей, таких как SD-карты или USB-накопители.

Базовый синтаксис соответствует следующему шаблону:

```
fsck <опции> <файловая_система>
```

В качестве *файловой системы* может быть устройство, точка монтирования или раздел, в том числе LVM.

Вы можете подробнее ознакомиться с возможностями проверки файловой системы на наличие ошибок, просмотрев наши обучающие видео:

- на **RuTube** — Проверка файловой системы на наличие ошибок;
- в **Яндекс.Дзен** — Проверка файловой системы на наличие ошибок;
- в **VK Видео** — Проверка файловой системы на наличие ошибок.

На наших каналах вы также сможете найти много другой полезной информации.

Параметры fsck

fsck –p – утилита автоматически исправит найденные ошибки.

Вывод аналогичен простой проверке.

fsck –c – проверка файловой системы на поврежденные сектора.

```
bash-5.2# fsck –c
fsck from util-linux 2.38.1
e2fsck 1.46.3 (27-Jul-2021)
Checking for bad blocks (read-only test): done
/dev/sda4: Updating bad block inode.
Pass 1: Checking inides, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information

/dev/sda4: *****FILE SYSTEM WAS MODIFIED *****
/dev/sda4: *****REBOOT SYSTEM *****
/dev/sda4: 358151/1114112 files (0.1% non-contiguous), 2377380/4455680 blocksbash-5.2#
```

Для получения списка команд наберите **fsck –-help** или **fsck –h.**

Опция	Описание
-a	Устаревшая опция. Указывает исправлять все найденные ошибки без одобрения пользователя.
-r	Применяется для файловых систем ext. Указывает fsck спрашивать пользователя перед исправлением каждой ошибки

-n	Выполняет только проверку ФС, без исправления ошибок. Используется также для получения информации о ФС
-c	Применяется для файловых систем ext3/4. Помечает все повреждённые блоки для исключения последующей записи в них
-f	Принудительно проверяет ФС, даже если ФС исправна
-y	Автоматически подтверждает запросы к пользователю
-b	Задаёт адрес суперблока
-p	Автоматически исправлять найденные ошибки. Заменяет устаревшую опцию -a
-A	Проверяет все ФС
-C [<fd>]	Показывает статус выполнения. Здесь fd – дескриптор файла при отображении через графический интерфейс
-l	Блокирует устройство для исключительного доступа
-M	Запрещает проверять примонтированные ФС
-N	Показывает имитацию выполнения, без запуска реальной проверки
-P	Проверять вместе с корневой ФС
-R	Пропускает проверку корневой ФС. Может использоваться только совместно с опцией -A
-r [<fd>]	Выводит статистику для каждого проверенного устройства
-T	Не показывать заголовок при запуске
-t <тип>	Задаёт ФС для проверки. Можно задавать несколько ФС, перечисляя через запятую
-V	Выводит подробное описание выполняемых действий

Пример проверки диска на ошибки с помощью fsck

Запуск автоматической проверки и исправления найденных ошибок

Существует несколько способов запуска автоматической проверки на ошибки:

1. Ручное добавление параметров в меню **GRUB** при загрузке ОС.

2. Добавление параметров в меню **GRUB** с помощью утилиты **grubby**.

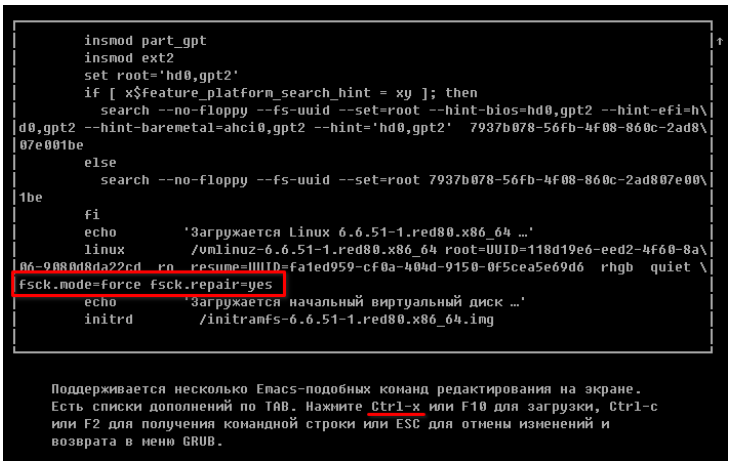
3. Создание файла **/forcefsck**.

1. Ручное добавление параметров в меню GRUB при загрузке ОС

Первый вариант проверки и исправления ошибок на разделах жесткого диска.

В меню **GRUB** перейдите в режим редактирования загрузочной строки, нажав при этом клавишу **e**. Добавьте параметры в конце строки, которая начинается на **linux**:

```
fsck.mode=force fsck.repair=yes
```



Нажмите **Ctrl+X** для запуска ОС с этими параметрами, во время запуска будет произведена проверка разделов диска, и при наличии ошибок произведено их исправление.

2. Добавление параметров в меню GRUB с помощью утилиты grubby

Существует еще один способ добавления параметров ядра для принудительной проверки файловой системы на ошибки и их исправления. Добавить параметры можно командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --args="fsck.mode=force fsck.repair=yes"
```

Удалить установленные параметры можно следующей командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --remove-args="fsck.mode=force fsck.repair=yes"
```

3. Создание файла /forcefsck

Бывают ситуации, когда систему необходимо проверить на наличие ошибок в *незапланированный* момент. Для этого можно **принудительно** запустить утилиту **fsck** для проверки при следующей перезагрузке. Запуск осуществляется командой:

```
sudo touch /forcefsck
```

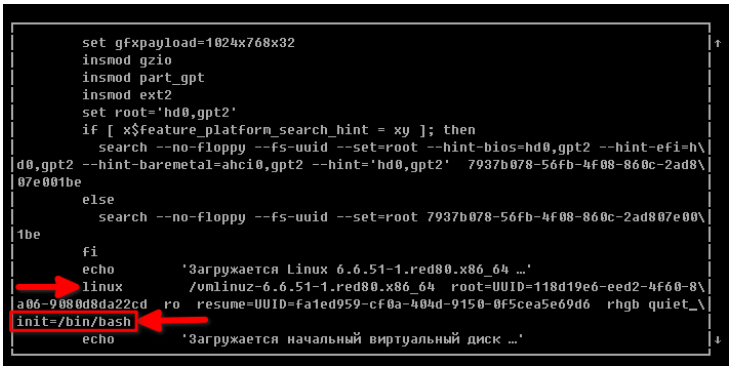
Команда **sudo** (после ввода пароля) предоставит права для создания с помощью **touch** пустого файла в корне диска **/forcefsck**, который послужит сигналом (флагом) для **fsck**, что нужно проверить диски.

Останется только перезагрузить компьютер и **fsck** начнет проверять все жесткие диски, указанные в **/etc/fstab**.

Запуск проверки в ручном режиме

Следующий метод относится к проверке диска, когда операционная система загружена в режиме **single mode**.

1. Запустим ОС в **single mode**, для этого пропишите в меню загрузки grub параметр init=/bin/bash в конце строки, которая начинается на linux, см. рисунок.



Также данная строка может начинаться с linuxefi, этот параметр характерен для систем с загрузкой в **UEFI**. Нажмите **"ctrl+x"** для запуска с этим параметром(init=/bin/bash).

2. Запустите проверку выполнив команду:

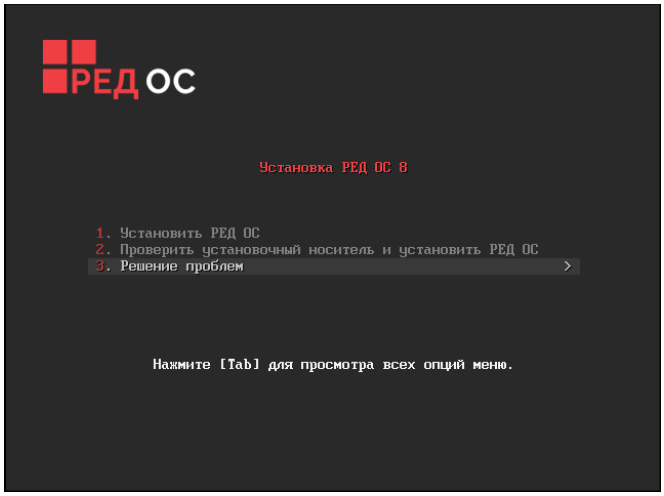
```
/usr/sbin/fsck -ACVfyv
```

Во время проверки на экране появится отчет о выполненных операциях, если отчет длинный, то можно его можно пролистать вверх сочетанием клавиш shift+PageUp. После проверки дисков перезагрузите компьютер, нажав на кнопку на системном блоке.

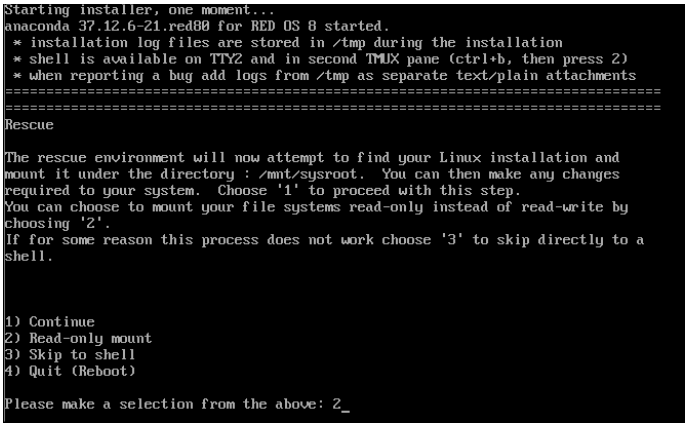
Наглядное видео примера проверки диска на ошибки:

Использование загрузочного диска/flash для проверки файловой системы на ошибки.

Загрузившись в режим восстановления операционной системы РЕД ОС с помощью загрузочного диска или съемного накопителя с установленным образом операционной системы РЕД ОС. Выберите пункт: **«Решение проблем» -> «Исправить установленную RED OS»**.



Система перезагрузится в режим восстановления. Введите «**2**» и нажмите 2 раза **Enter**. Так вы смонтируете операционную систему в режим «**Только для чтения**»



Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Потом введите команду:

```
# chroot /mnt/sysimage
```

После этого можете вводить **fsck**:

```
# fsck -ACVfyv
```

Если проверка завершится с такой ошибкой:

```
[путь_к_файловой_системе] is mounted
```

Введите:

```
umount [путь_к_файловой_системе]
```

И еще раз запустите утилиту **fsck**:

```
# fsck -ACVfyv
fsck from util-linux 2.38.1
…
```

Если система не выявит ошибок, то получится такой вывод:

```
[путь_к_файловой_системе] clean …
```

Чтобы выйти из режима восстановления, вы должны смонтировать все разделы, которые были отмонтированы командой **umount**, с помощью команды **mount**, нажать сочетание клавиш **ctrl+d**, а затем ввести команду **reboot**, которая перезапустит вашу операционную систему.

```
# reboot
```

По умолчанию, утилита **fsck** при проверке будет использовать разделы, указанные в **/etc/fstab/**, сформированные при установке операционной системы РЕД ОС.

Проверка LVM-разделов с помощью утилиты fsck

Перед проведением проверки необходимо найти устройство и размонтировать его.

Для просмотра всех подключенных устройств и проверки расположения диска выполните команду:

```
lsblk

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 20G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 19G 0 part
├─ro_redos-root 253:0 0 17G 0 lvm /
└─ro_redos-swap 253:1 0 2G 0 lvm [SWAP]
sr0 11:0 1 4,3G 0 rom /run/media/user/redos-MUROM-7.3.1 x86_64
```

При попытке запустить проверку на смонтированном диске или разделе в консоли появляется предупреждение о том, что невозможно продолжить проверку, так как диск смонтирован.

```
fsck -nf /dev/ro_redos/root

fsck из util-linux 2.38.1
e2fsck 1.46.3 (27-Jul-2021)
Warning! /dev/mapper/ro_redos-root is mounted.
```

Для того чтобы размонтировать диск, следует использовать команду:

```
umount <файловая_система>
```

Однако попытка выполнить данную процедуру на работающей ОС ни к чему не приведет.

```
umount /dev/ro_redos/root

umount: /: target is busy.
```

Также проблемой при попытке проверить LVM-разделы может быть и то, что они являются не активными. Для проверки следует использовать команду:

```
lvscan

ACTIVE '/dev/ro_redos/swap' [2,00 GiB] inherit
ACTIVE '/dev/ro_redos/root' [<17,00 GiB] inherit
```

Для активации раздела служит команда:

```
vgchange –ay <раздел>
```

Таким образом, можно сделать вывод, что проверка LVM-разделов через консоль с использованием утилиты **fsck** невозможна. Но это не значит, что LVM-разделы совсем не подлежат проверке. Существует как минимум два способа, позволяющие провести диагностику LVM-разделов.

Первым способом является проведение проверки через консоль загрузчика операционной системы **GRUB**.

А вторым - запуск утилиты **fsck** в **live-сессии** системы.

Очевидным плюсом при проверке дисковых пространств, в том числе LVM-разделов, через live-сессию является то, что разделы там по умолчанию являются не смонтированными. Поэтому проверка LVM-раздела будет выполнена с первого раза.

fsck /dev/ro_redos/root

```
fsck из util-linux 2.38.1
e2fsck 1.46.3 (27-Jul-2021)
/dev/mapper/ro_redos-root: recovering journal
Clearing orphaned inode 423398 (uid=0, gid=0, mode=0100644, size=229605)
Clearing orphaned inode 172559 (uid=0, gid=0, mode=0100644, size=24992)
Clearing orphaned inode 387 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 386 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 384 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 296594 (uid=1000, gid=1000, mode=0100644, size=9059)
Setting free inodes count to 890417 (was 890569)
Setting free inodes count to 2578845 (was 2585477)
/dev/mapper/ro_redos-root: clean, 223695/11141112 files, 1876579/4455424 blocks
```

Получение сведений о процессах в РЕД ОС

Содержимое каталога /proc

Назначение файлов в каталогах процессов /proc/<PID>

Структура каталога /proc/sys

Процесс — это экземпляр запущенной программы. Каждый раз, когда в терминале выполняется какая-либо команда, система создает новый процесс. Процессы в операционной системе имеют числовой идентификатор, называемый **PID**.

Программы пространства пользователя в РЕД ОС не могут обращаться к ядру системы напрямую. Однако для получения информации от ядра были созданы некоторые специальные каталоги, с помощью которых любая программа или пользователь может получить данные о состоянии компьютера и ядра – это каталоги **/proc** и **/sys**.

Вы можете подробнее ознакомиться с назначением каталога **/proc** и файловой системы **procfs**, просмотрев наши обучающие видео:

- на **RuTube** — Файловая система procfs;
- в **Яндекс.Дзен** — Файловая система procfs.
- в **VK Видео** — Файловая система procfs.

На наших каналах вы также сможете найти много другой полезной информации.

С дополнительной информацией о работе с процессами можно ознакомиться в нашей статье «Процессы в РЕД ОС».

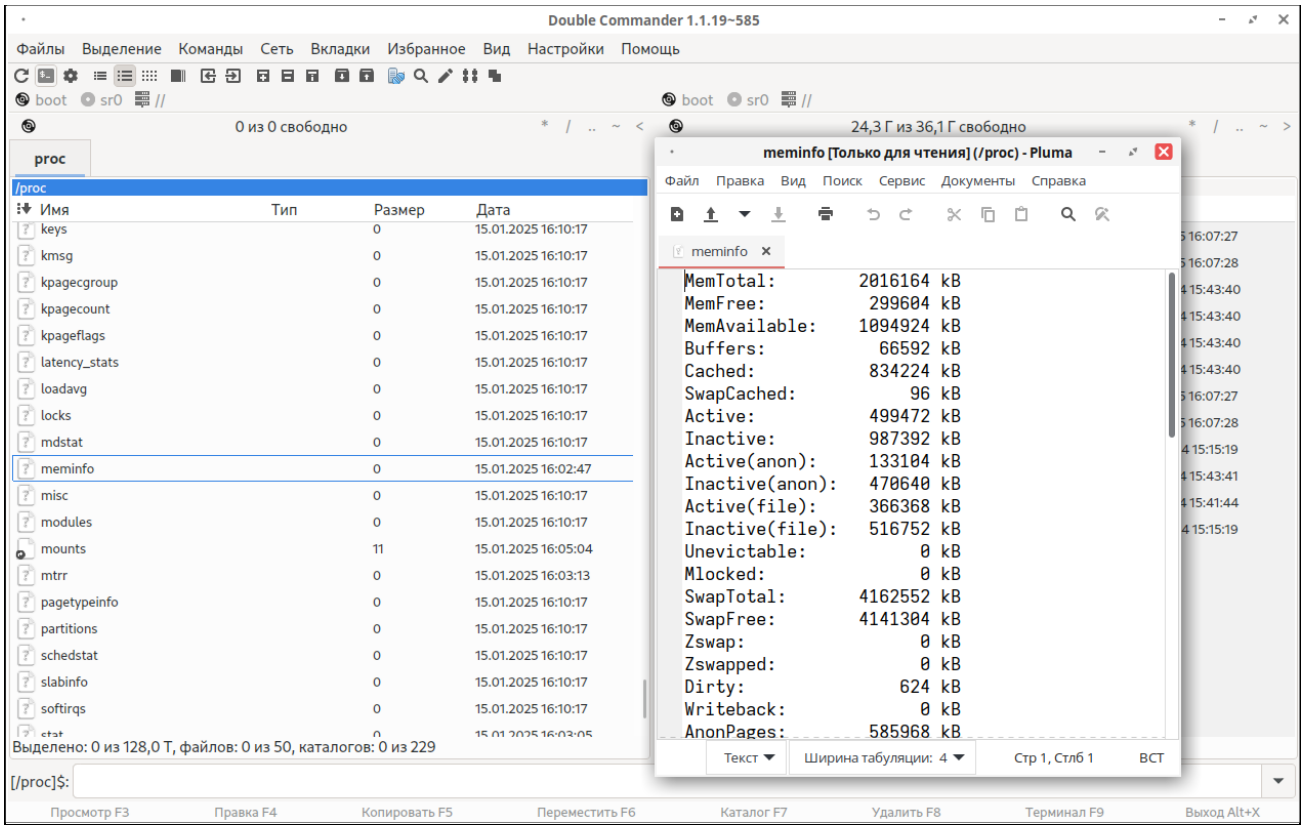
В рамках текущей статьи будет рассмотрен механизм получения сведений о процессах, на котором основаны все программы, позволяющие работать с процессами – работа с каталогом **/proc**.

В каталог **/proc** монтируется специальная файловая система **procfs**.

procfs — специальная файловая система, используемая в UNIX-подобных операционных системах, позволяющая получить доступ к информации из ядра о системных процессах, необходима для выполнения таких команд, как `ps`, `w`, `top`.

На самом деле каталог **/proc** – это не обычный каталог. Все подкаталоги, файлы и хранящаяся в них информация генерируются ядром «на лету», как только пользователь ее запрашивает. Работа построена таким образом, что пользователь может не заметить разницы между обычной файловой системой и **proc**, если откроет ее с помощью файлового менеджера.

Каталог **/proc** содержит файлы нулевого размера, у каждого файла отображается текущая дата создания. Например, файл **/proc/meminfo** будет содержать разные данные при каждом открытии, поскольку использование памяти постоянно изменяется.



С помощью такого механизма разработчики придерживаются главной концепции Unix: «Всё – есть файл». Все файлы доступны для изменения любым редактором, и все они представлены в простом текстовом формате, но для того чтобы проанализировать весь

каталог, необходимы права суперпользователя (**root**).

Большинство файлов в каталоге **/proc** доступны только для чтения, с их помощью можно только просмотреть информацию. Однако существуют и доступные для записи файлы, в частности – каталог **/proc/sys**, с помощью которого можно настраивать различные параметры ядра.

Содержимое каталога /proc

/proc/buddyinfo – файл отображает информацию о фрагментации памяти в ядре системы. Чаще всего используется для диагностики проблем с фрагментацией памяти.

```
cat /proc/buddyinfo
Node 0, zone      DMA      3      2      3      4      4      4      4      2      3      1      0
Node 0, zone    DMA32   3091   2531   1857    728    273    119     59     25      6      3      8
```

/proc/cmdline – файл отображает информацию о параметрах, которые были указаны в строке запуска ядра загрузчиком **grub**. Может быть полезно при поиске и устранении проблем с загрузкой ядра или в случае необходимости выявления файла, использованного для загрузки.

```
cat /proc/cmdline
BOOT_IMAGE=/vmlinuz-6.6.51-1.red80.x86_64 root=UUID=5b25f5f1-2ee8-4ee2-8b0d-524f3cde5e1e ro resume=UUID=cd77454c-60a6-4495-98e2-568a5279db77 rhgb quiet
```

/proc/consoles – файл отображает информацию о зарегистрированных в ядре символических устройствах для системной консоли **/dev/console**.

```
cat /proc/consoles
tty0                 -WU (EC p  )    4:2
```

/proc/cpuinfo – файл отображает очень подробную информацию о процессоре. Здесь можно просмотреть производителя, количество ядер, объем кеша, активные ядра, частоту, поддерживаемые расширения и многое другое. Ту же информацию можно получить с помощью специальных команд, однако все скрипты, выводящие информацию о процессоре, берут ее из каталога **/proc**.

```
cat /proc/cpuinfoprocessor : 0
vendor_id : GenuineIntel
cpu family : 6
model  : 158
model name : Intel(R) Core(TM) i5-9400 CPU @ 2.90GHz
stepping : 13
microcode : 0xea
cpu MHz  : 2903.998
cache size : 16384 KB
physical id : 0
siblings : 1
core id  : 0
cpu cores : 1
apicid  : 0
initial apicid : 0
fpu  : yes
fpu_exception : yes
cpuid level : 22
wp  : yes
[...]
```

/proc/devices – файл отображает информацию о различных блочных и символических устройствах, подключенных к системе, кроме тех, для которых не загружены модули ядра. Устройства разделены на *символические* и *блочные*. У символических устройств нет буфера хранения, поэтому они отправляют ядру данные определенного размера. Блочные устройства имеют буфер для данных и предназначены для сохранения информации, например, на жесткие диски.

```
cat /proc/devicesCharacter devices:
  1 mem
  2 pty
  3 ttyp
  4 /dev/vc/0
  4 tty
  4 ttyS
  5 /dev/tty
  5 /dev/console
```

```
  5 /dev/ptmx
  7 vcs
 10 misc
 13 input
 14 sound
 21 sg
 29 fb
116 alsa
128 ptm
136 pts
180 usb
188 ttyUSB
[...]
```

/proc/fb – файл отображает информацию об устройствах фреймбуфера (экраны), а также используемые графические драйверы. Файл является одним из способов просмотра используемого драйвера видеокарты.

```
cat /proc/fb
0 qxldrmfb
```

/proc/filesystems – файл содержит список файловых систем, которые на данный момент поддерживаются ядром. Значение **nodev** показывает, что это файловая система специального назначения, и она не используется для хранения данных на носителях.

```
cat /proc/filesystems
nodev sysfs
nodev tmpfs
nodev bdev
nodev proc
nodev cgroup
nodev cgroup2
nodev cpuset
nodev devtmpfs
nodev configfs
nodev debugfs
nodev tracefs
nodev securityfs
nodev sockfs
nodev bpf
nodev pipefs
nodev ramfs
nodev hugetlbfs
nodev devpts
 ext3
 ext2
 ext4
[...]
```

/proc/kcore – это все содержимое оперативной памяти, представленное в одном файле. В отличие от других у этого файла есть размер – объем ОЗУ плюс 4 Кб. Для доступа к файлу необходимы права суперпользователя (**root**). Перед работой с файлом его необходимо скопировать в другой каталог, а затем выполнять требуемые действия.

```
cat /proc/kcore
[...]
PAGESIZE=4096
SYMBOL(init_uts_ns)=ffffffff862b4fe0
OFFSET(uts_namespace.name)=0
SYMBOL(node_online_map)=ffffffff8631a3c0
SYMBOL(swapper_pg_dir)=ffffffff8601c000
SYMBOL(_stext)=ffffffff84000000
SYMBOL(vmap_area_list)=ffffffff861c8f30
SYMBOL(mem_section)=ffff9c9f7ffb1000
LENGTH(mem_section)=2048
SIZE(mem_section)=16
OFFSET(mem_section.section_mem_map)=0
NUMBER(SECTION_SIZE_BITS)=27
NUMBER(MAX_PHYSMEM_BITS)=46
SIZE(page)=64
SIZE(pglist_data)=175424
SIZE(zone)=1728
SIZE(free_area)=104
SIZE(list_head)=16
```

```
SIZE(nodemask_t)=128
OFFSET(page.flags)=0
OFFSET(page._refcount)=52
[...]
```

/proc/kmsg – файл накапливает и сохраняет сообщения ядра. Сообщения можно посмотреть также с помощью утилиты **dmesg**. Для доступа к файлу потребуются права суперпользователя (**root**).

```
cat /proc/kmsg
[...]
<6>[    1.469422] Freeing unused decrypted memory: 2028K
<6>[    1.471034] Freeing unused kernel image (initmem) memory: 4392K
<6>[    1.471067] Write protecting the kernel read-only data: 32768k
<6>[    1.472590] Freeing unused kernel image (rodata/data gap) memory: 1548K
<6>[    1.504398] x86/mm: Checked W+X mappings: passed, no W+X pages found.
<6>[    1.504415] rodata_test: all tests were successful
<6>[    1.504430] Run /init as init process
<7>[    1.504434]   with arguments:
<7>[    1.504436]     /init
<7>[    1.504437]     rhgb
<7>[    1.504438]   with environment:
<7>[    1.504439]     HOME=/
<7>[    1.504440]     TERM=linux
<7>[    1.504441]     BOOT_IMAGE=/vmlinuz-6.6.51-1.red80.x86_64
[...]
```

/proc/loadavg – файл позволяет оценить среднюю нагрузку на систему. Первые три цифры показывают нагрузку на процессор в данный момент времени, 5 минут назад и 15 минут назад, следующие два столбца показывают количество активных процессов и общее количество запущенных процессов. Последняя цифра — это идентификатор последнего процесса (**PID**).

```
cat /proc/loadavg
0.04 0.19 0.56 1/487 5764
```

/proc/meminfo – файл отображает всю доступную информацию об оперативной памяти и пространстве подкачки.

```
cat /proc/meminfo
MemTotal:        2016164 kB
MemFree:           88360 kB
MemAvailable:     181764 kB
Buffers:            7920 kB
Cached:           206472 kB
SwapCached:         6240 kB
Active:           972320 kB
Inactive:         595760 kB
Active(anon):     814268 kB
Inactive(anon):   553056 kB
Active(file):     158052 kB
Inactive(file):    42704 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:       4162552 kB
SwapFree:        3227384 kB
Zswap:                 0 kB
Zswapped:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:       1350020 kB
Mapped:            95860 kB
Shmem:             13636 kB
```

/proc/modules – файл содержит список всех загруженных модулей ядра. Ту же информацию можно увидеть, выполнив команду **lsmod**.

```
cat /proc/modules
uinput 20480 1 - Live 0x0000000000000000
snd_seq_dummy 12288 0 - Live 0x0000000000000000
snd_hrtimer 12288 1 - Live 0x0000000000000000
qrtr 49152 2 - Live 0x0000000000000000
rfkill 28672 3 - Live 0x0000000000000000
sunrpc 839680 1 - Live 0x0000000000000000
snd_hda_codec_generic 110592 1 - Live 0x0000000000000000
```

```
ledtrig_audio 12288 1 snd_hda_codec_generic, Live 0x0000000000000000
snd_hda_intel 61440 2 - Live 0x0000000000000000
intel_rapl_msr 20480 0 - Live 0x0000000000000000
intel_rapl_common 36864 1 intel_rapl_msr, Live 0x0000000000000000
snd_intel_dspcfg 36864 1 snd_hda_intel, Live 0x0000000000000000
snd_intel_sdw_acpi 16384 1 snd_intel_dspcfg, Live 0x0000000000000000
snd_hda_codec 204800 2 snd_hda_codec_generic,snd_hda_intel, Live 0x0000000000000000
snd_hda_core 135168 3 snd_hda_codec_generic,snd_hda_intel,snd_hda_codec, Live 0x0000000000000000
kvm_intel 409600 0 - Live 0x0000000000000000
snd_hwdep 16384 1 snd_hda_codec, Live 0x0000000000000000
kvm 1302528 1 kvm_intel, Live 0x0000000000000000
[...]
```

/proc/mounts – файл содержит все точки монтирования и все подключенные файловые системы.

```
cat /proc/mountsproc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
sysfs /sys sysfs rw,seclabel,nosuid,nodev,noexec,relatime 0 0
devtmpfs /dev devtmpfs rw,seclabel,nosuid,size=4096k,nr_inodes=1048576,mode=755,inode64 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,seclabel,nosuid,nodev,inode64 0 0
devpts /dev/pts devpts rw,seclabel,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,seclabel,nosuid,nodev,size=403236k,nr_inodes=819200,mode=755,inode64 0 0
cgroup2 /sys/fs/cgroup cgroup2 rw,seclabel,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,seclabel,nosuid,nodev,noexec,relatime 0 0
bpf /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
/dev/sda4 / ext4 rw,seclabel,relatime 0 0
[...]
```

/proc/partitions – в файле отображены все подключенные к системе разделы жестких дисков или других запоминающих устройств.

```
cat /proc/partitions
major minor  #blocks  name

   8        0   41943040 sda
   8        1       1024 sda1
   8        2    1048576 sda2
   8        3    2147328 sda3
   8        4   38744064 sda4
  11        0    1048575 sr0
 252        0    2015232 zram0
```

Назначение файлов в каталогах процессов /proc/<PID>

Для отображения файлов какого-либо процесса следует открыть каталог с номером необходимого процесса. В каждом каталоге более 50 файлов.

Далее будет рассмотрено назначение некоторых файлов:

- **cmdline** – содержит команду, с помощью которой был запущен процесс, а также переданные ей параметры;
- **cwd** – символическая ссылка на текущий рабочий каталог процесса;
- **exe** – ссылка на исполняемый файл;
- **root** – ссылка на каталог суперпользователя (**root**);
- **environ** – переменные окружения, доступные для процесса;
- **fd** – содержит файловые дескрипторы, файлы и устройства, которые использует процесс;
- **maps**, **statm**, и **mem** – информация о памяти процесса;
- **stat**, **status** – состояние процесса.

Структура каталога /proc/sys

Каталог **/proc/sys** содержит файлы с параметрами ядра. Файлы доступны не только для чтения, но и для редактирования с целью передачи ядру ОС новых значений параметров.

Каталог содержит подкаталоги, разделённые по типам хранимых параметров. Далее будет рассмотрено назначение некоторых

файлов:

- **debug** – содержит отладочную информацию, она будет полезна для разработчиков ядра;
- **dev** – содержит параметры различных устройств, подключенных к системе;
- **fs** – содержит всю информацию о файловой системе;
- **kernel** – позволяет напрямую настраивать ядро;
- **net** – позволяет настраивать различные параметры сети;
- **vm** – содержит ряд файлов и подкаталогов, соответствующих переменным ядра с подсистемой виртуальной памяти.

Более подробную информацию о каталоге **/proc** также можно просмотреть, выполнив команду:

```
man proc
```

Изменение приоритета процесса

Изменение приоритетов процессов с помощью терминала
Изменение приоритетов процессов с помощью графических средств

Изменение приоритетов процессов с помощью терминала

Утилита nice — программа, предназначенная для запуска процессов с изменённым приоритетом nice. Приоритет nice (целое число) процесса используется планировщиком процессов ядра ОС при распределении процессорного времени между процессами

Приоритет nice — число, указывающее планировщику процессов ядра ОС приоритет, который пользователь хотел бы назначить процессу.

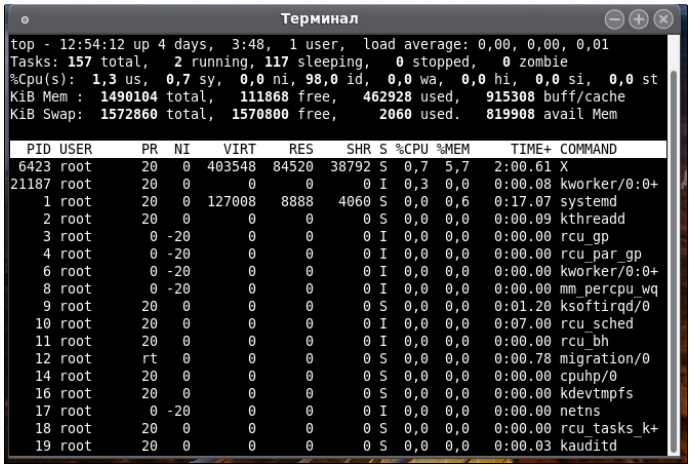
Утилита nice, запущенная без аргументов, выводит приоритет nice, унаследованный от родительского процесса. nice принимает аргумент «смещение» в диапазоне от -20 (наивысший приоритет) до +19 (низший приоритет). Если указать смещение и путь к исполняемому файлу, утилита nice получит приоритет своего процесса, изменит его на указанное смещение и использует системный вызов семейства exec() для замещения кода своего процесса кодом из указанного исполняемого файла. Команда nice сделает то же, но сначала выполнит системный вызов семейства fork() для запуска дочернего процесса (англ. sub-shell). Если смещение не указано, будет использовано смещение +10. Привилегированный пользователь (root) может указать отрицательное смещение.

Приоритет nice и приоритет планировщика процессов ядра ОС — разные числа. Число nice — приоритет, который пользователь хотел бы назначить процессу. Приоритет планировщика — действительный приоритет, назначенный процессу планировщиком. Планировщик может стремиться назначить процессу приоритет, близкий к nice, но это не всегда возможно, так как в системе может выполняться множество процессов с разными приоритетами. Приоритет nice является атрибутом процесса и, как и другие атрибуты, наследуется дочерними процессами. В выводе утилит top, ps, htop и др. приоритет nice называется «NI» — сокращение от «nice», а приоритет планировщика — «PRI» — сокращение от «priority». Обычно, NI = PRI - 20, но это верно не всегда. По умолчанию NI=0, соответственно PRI=20.

Планировщик процессов ядра ОС Linux поддерживает приоритеты от 0 (реальное время) до 139 включительно. Приоритеты -20...+19 утилиты или команды nice соответствуют приоритетам 100...139 планировщика процессов. Другие приоритеты планировщика процессов можно установить командой chrt из пакета util-linux.

Посмотреть приоритет процессов можно например с помощью утилиты **top**, для этого в терминале нужно выполнить:

```
top
```



Для просмотра приоритета уже запущенного конкретного процесса существует команда:

```
ps -o pid,comm,nice -C [name]
```

Например:

```
ps -o pid,comm,nice -C top

PID COMMAND NI
21244 top 0
```

nice

Синтаксис:

```
nice [-n смещение] [--adjustment=смещение] [команда [аргумент...]]
```

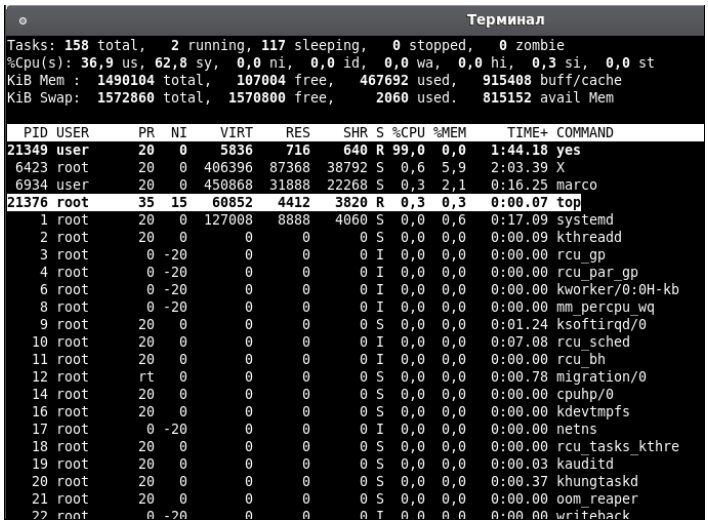
Параметры:

```
-n <смещение>
--adjustment=<смещение>
```

Установить приоритет nice, равный сумме текущего приоритета nice и указанного числа «смещение». Если этот аргумент не указан, будет использовано число 10.

Для примера зададим приоритет 15 при старте процесса top:

```
nice -n 15 top
```



Чтобы установить значение nice ниже нуля, требуются права суперпользователя. В противном случае будет установлено значение 0. Попробуем задать значение nice -1 без прав root:

```
nice -n -1 yes > /dev/null &nice: cannot set niceness: Permission denied
```

Поэтому, чтобы задать значение nice меньше 0, необходимо запускать программу как root, или использовать sudo.

renice

Для того, чтобы изменить приоритет у существующего процесса (т.е. такого процесса, который ранее был уже запущен), необходимо воспользоваться командой:

```
renice [значение приоритета] -p [id процесса]
```

У запущенной программы с помощью команды renice можно изменить назначенный приоритет. Предположим, что есть работающая программа yes со значением nice 10. Чтобы изменить его значение, можно использовать команду renice со значением nice и PID процесса. Изменим значение nice на 15:

```
renice -n 15 -p 21349
21349 (process ID) old priority 0, new priority 15
```

Согласно правилам, обычный пользователь может только увеличивать значение nice (уменьшать приоритет) любого процесса. Если попробовать изменить значение nice с 15 до 10, мы получим следующее сообщение об ошибке:

```
renice -n 10 -p 21349
renice: failed to set priority for 5645 (process ID): Permission denied
```

Также, команда renice позволяет суперпользователю изменять значение nice процессов любого пользователя. Это делается с помощью ключа -u. Следующая команда изменяет значение приоритета всех процессов пользователя на -19:

```
renice -n -19 -u lubos
1000 (user ID) old priority 0, new priority -19
```

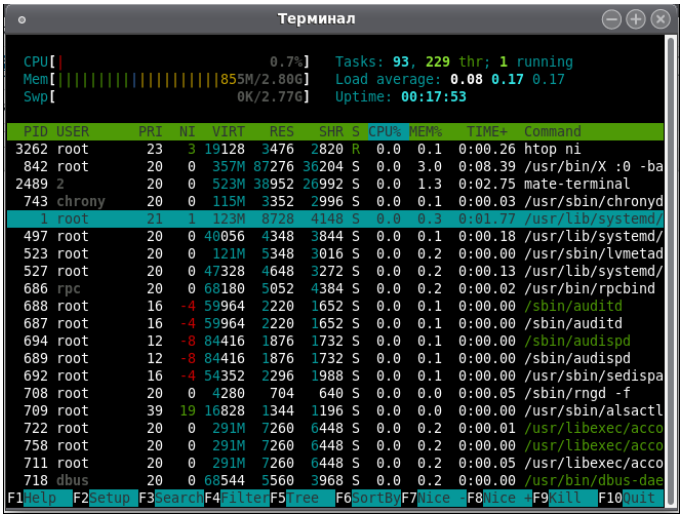
htop

htop представляет собой продвинутый монитор процессов, аналог **top.** В отличие от top, htop показывает все процессы в системе. Также показывает время непрерывной работы, использование процессоров и памяти. htop часто применяется в тех случаях, когда информации даваемой утилитой top недостаточно, например при поиске утечек памяти в процессах. htop написан на языке Си и использует для отображения библиотеку Ncurses.

Устанавливается командой:

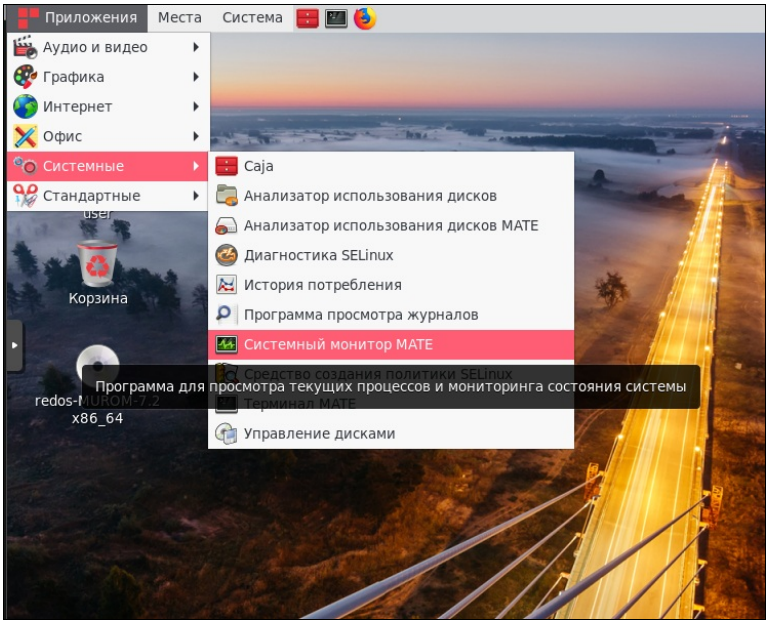
```
dnf install htop
```

На нижней панели интерфейса отображены основные действия. Переключаться межуд процессами можно кнопками «Вверх» и «Вниз». При нажатии F7 и F8 на выбранном процессе изменяется приоритет вниз и вверх соответственно.



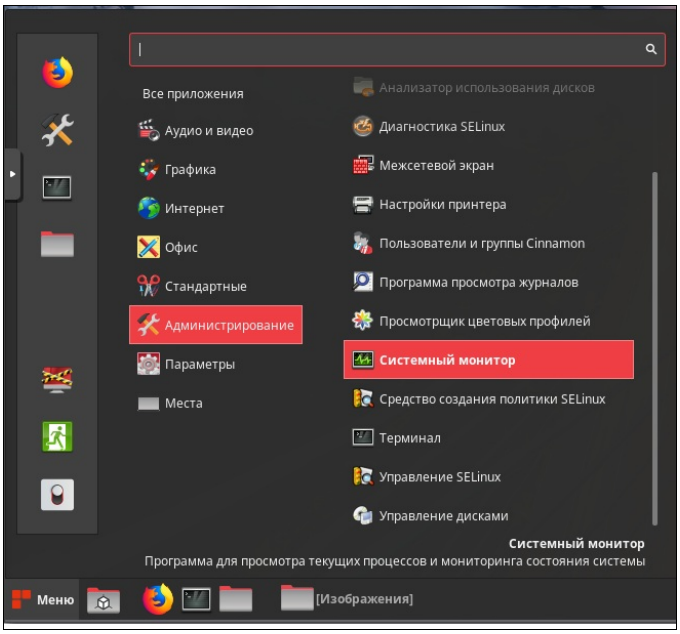
Изменение приоритетов процессов с помощью графических средств

Изменять приоритеты процессов можно с помощью утилиты **Системный монитор**.

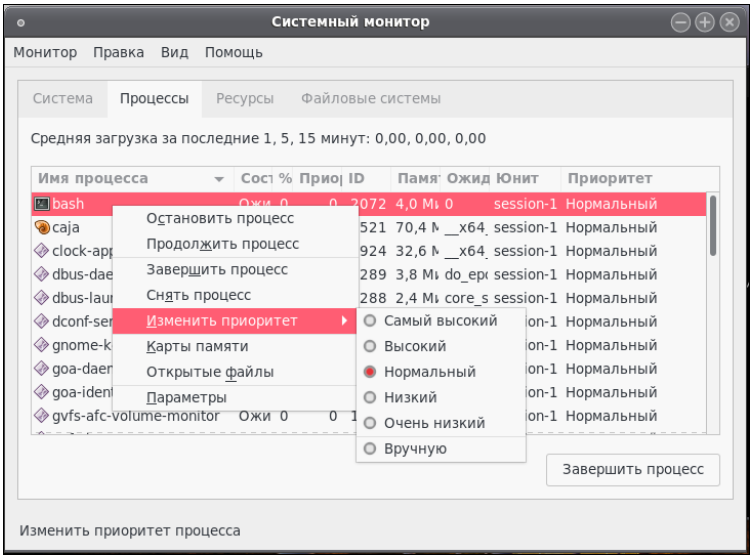


Для Cinnamon необходимо установить отдельно:

```
dnf install gnome-system-monitor.x86_64
```



Перейдите на вкладку Процессы. Выберите процесс, щелкните правой кнопкой мыши по нему и выберите в выпадающем меню пункт Изменить приоритет. Выберите нужный приоритет и выберите его.



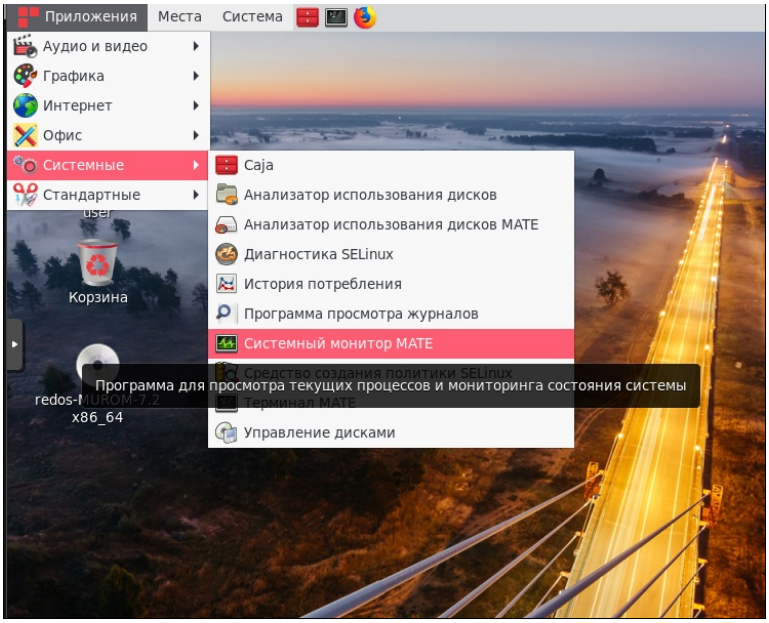
Системный монитор

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

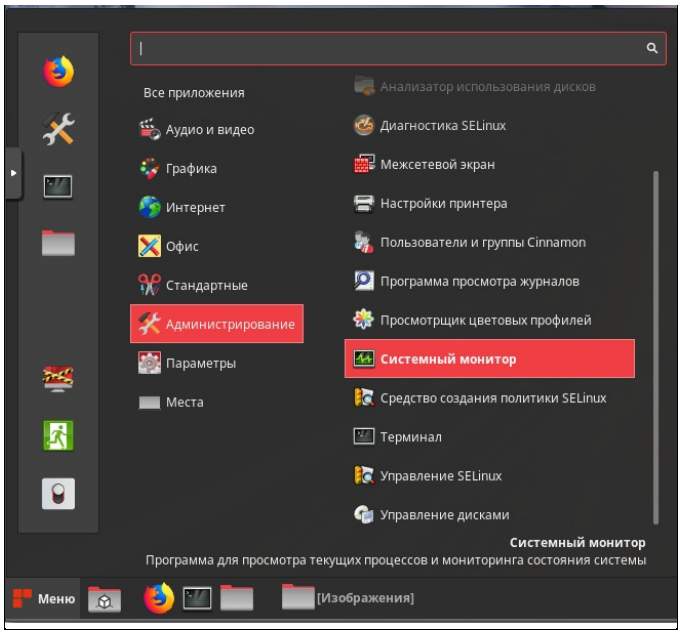
Утилита «**Системный монитор**» - аналогия диспетчера задач в Windows.



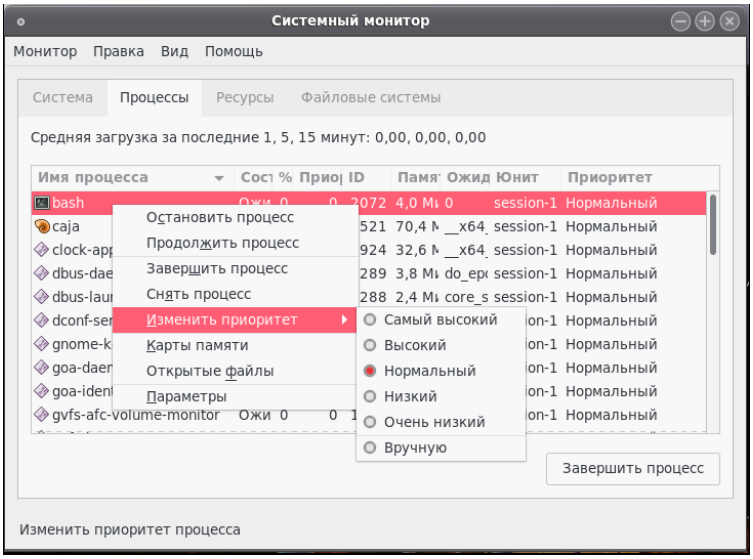
Для **Cinnamon** необходимо установить отдельно:

```
sudo dnf install gnome-system-monitor
```

Расположение утилиты в **Cinnamon**:



Графический интерфейс утилиты интуитивно понятен, вся информация распределена по четырем вкладкам (Cinamon — 3 вкладки). Выглядит следующим образом:



Вкладка **«Система»** - выводится базовая минимальная информация о системе.

Вкладка **«Процессы»** - можно просматривать и управлять, работающими процессами. Каждый процесс можно приостановить, остановить, изменить приоритет.

Вкладка **«Ресурсы»** - утилита выводит в виде графиков информацию в реальном времени о ресурсах использования процессора, использование оперативной памяти и файла подкачки, и использование сети.

Вкладка **«Файловые системы»** - отображает информацию о имеющихся устройствах хранения информации.

top

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер минимальный, Сервер графический

top — утилита, с помощью которой можно вывести список работающих в системе процессов и информацию о них. Данная утилита установлена в РЕД ОС по умолчанию.

С утилитой **top** вы можете подробнее ознакомиться, просмотрев наши обучающие видео:

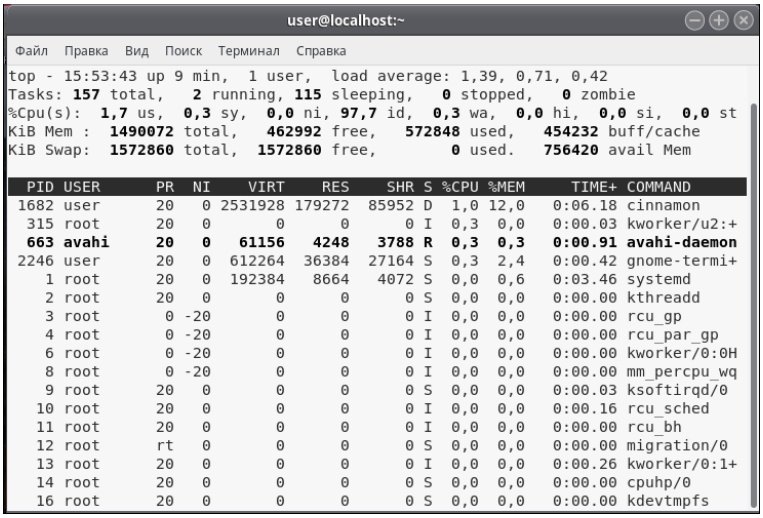
- на **RuTube** — Утилита мониторинга процессов top;
- в **Яндекс.Дзен** — Утилита мониторинга процессов top;
- в **VK Видео** — Утилита мониторинга процессов top.

На наших каналах вы также сможете найти много другой полезной информации.

Для запуска утилиты необходимо в терминале выполнить команду (с правами обычного **непривилегированного** пользователя):

```
top
```

После запуска в терминале можно увидеть вывод, примерно следующего содержания:



Где первая строка:

- текущее время (**15:53:43**);
- время работы системы (**up 9 min**);
- количество открытых пользовательских сессий (**1 users**);
- среднюю загрузку системы (**load average: 1.39, 0.71, 0.42**).

Вторая строка:

- общее количество процессов в системе (**157 total**);
- количество работающих в данный момент процессов (**2 running**);
- количество ожидающих событий процессов (**115 sleeping**);
- количество остановленных процессов (**0 stopped**);
- количество процессов, ожидающих родительский процесс для передачи статуса завершения (**0 zombie**).

Третья строка выводит информацию о работе процессора:

- использование центрального процессора (в процентах) пользовательскими процессам (**1.7 us**);
- использование центрального процессора (в процентах) системными процессами (**0.3 sy**);
- использование центрального процессора (в процентах) процессами с приоритетом, повышенным при помощи вызова nice (0.0 ni);
- время (в процентах), когда центральный процессор не используется (**97,7 id**);
- использование центрального процессора (в процентах) процессами, ожидающими завершения операций ввода-вывода (**0.3 wa**);
- использование центрального процессора (в процентах) обработчиками аппаратных прерываний (**0.0 hi - Hardware IRQ** (аппаратные прерывания));
- использование центрального процессора (в процентах) обработчиками программных прерываний (**0.0 si - Software Interrupts** (программные прерывания));
- количество ресурсов центрального процессора "заимствованных" у виртуальной машины гипервизором для других задач (таких, как запуск другой виртуальной машины), это значение будет равно нулю на настольных компьютерах и серверах, не

использующих виртуальные машины (**0.0 st - Steal Time** (заимствованное время)).

Четвертая и пятая строка показывает информацию об использовании физической оперативной памяти и раздела подкачки (swap):

- общее количество памяти (в килобайтах);
- количество используемой памяти (в килобайтах);
- количество свободной памяти (в килобайтах);
- количество памяти в кэше буферов (в килобайтах).

Далее идет список процессов, отсортированных по величине использования центрального процессора:

- **PID** – идентификатор процесса;
- **USER** - имя пользователя, который является владельцем процесса;
- **PR** - приоритет процесса;
- **NI** - значение "NICE", влияющие на приоритет процесса;
- **VIRT** - объем виртуальной памяти, используемый процессом;
- **RES** - объем физической памяти, используемый процессом;
- **SHR** - объем разделяемой памяти процесса;
- **S** - указывает на статус процесса:
  - S=sleep (ожидает событий);
  - R=running (работает);
  - Z=zombie (ожидает родительский процесс);

- **%CPU** - процент использования центрального процессора данным процессом;
- **%MEM** - процент использования оперативной памяти данным процессом;
- **TIME+** - общее время активности процесса;
- **COMMAND** - имя процесса.

Далее приведено описание наиболее часто используемых интерактивных команд, которые вы можете выполнять во время работы программы:

- **h** - вывод справки по утилите;
- **q (Ctrl+C)** - выход из **top**;
- **A** - выбор цветовой схемы;
- **d** или **s** - изменить интервал обновления информации;
- **H** - выводить потоки процессов;
- **k** - послать сигнал завершения процессу;
- **W** - записать текущие настройки программы в конфигурационный файл;
- **Y** - посмотреть дополнительные сведения о процессе, открытые файлы, порты, логи и т д;
- **Z** - изменить цветовую схему;
- **l** - скрыть или вывести информацию о средней нагрузке на систему;
- **m** - выключить или переключить режим отображения информации о памяти;
- **x** - выделять жирным колонку, по которой выполняется сортировка;
- **y** - выделять жирным процессы, которые выполняются в данный момент;
- **z** - переключение между цветным и одноцветным режимами;
- **c** - переключение режима вывода команды, доступен полный путь и только команда;
- **F** - настройка полей с информацией о процессах;
- **o** - фильтрация процессов по произвольному условию;
- **u** - фильтрация процессов по имени пользователя;
- **V** - отображение процессов в виде дерева;
- **i** - переключение режима отображения процессов, которые сейчас не используют ресурсы процессора;
- **n** - максимальное количество процессов, для отображения в программе;
- **L** - поиск по слову;
- **<>** - перемещение поля сортировки вправо и влево.

Примечание.

Обратите внимание, что для использования интерактивных команд, обозначаемых заглавными буквами (A, H, W, Y, Z и т.д.), необходимо одновременно нажимать клавишу *Shift* и соответствующую букву. Например, для выполнения интерактивной команды **A** следует использовать сочетание *Shift+a*.

Для получения более подробной справки необходимо нажать клавишу «**h**» во время работы утилиты.

Использование top в пакетном режиме

Утилита **top** также поддерживает использование опций командной строки. Большинство из этих опций соответствуют рассмотренным выше интерактивным командам — для их использования перед буквой требуется поставить дефис.

Также утилита **top** может использоваться в пакетном режиме. Для запуска утилиты в пакетном режиме применяется опция `-b`. Данный режим полезен для отправки выходных данных утилиты в другую программу или в файл. В пакетном режиме утилита **top** не

принимает ввод и работает до достижения заданного опцией `-n` предела повторений. Например, запуск команды **top** в пакетном режиме с одним обновлением информации будет выглядеть следующим образом:

```
top -b -n 1
```

Для сохранения результатов команды **top** в файл в *текущей директории* используйте следующую команду:

```
top -n 1 -b > top-output.txt
```

htop

Установка
Работа с утилитой
Горячие клавиши htop

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Рабочая станция, Сервер минимальный, Сервер графический.
- **Версия ПО**: htop-3.3.0-1

htop — утилита командной строки, позволяющая пользователю интерактивно отслеживать жизненно важные ресурсы системы или процессы в режиме реального времени. **htop** поддерживает работу с мышью, использует цвет в своих выходных данных и дает визуальные указания об использовании процессора.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Основные параметры:

- `-d`, `--delay=<число>` – задержка между обновлениями в секундах;
- `-C`, `--no-color`, `--no-colour` – запуск в монохромном режиме;
- `--directory=<путь_к_каталогу>` – директория, используемая для тестирования **I/O**;
- `-h`, `--help` – вывод справки;
- `-p`, `--pid=<PID>,<PID>...` – отображение только процессов с указанными **PID**;
- `-s`, `--sort-key` – сортировка таблицу по указанному столбцу;
- `-u`, --user=<имя_пользователя> – отображение только процессов заданного пользователя;
- `-v`, `--version` – вывод версии утилиты;
- `-t`, `--tree` – отображение процессов в виде дерева.

Установка

Установка утилиты выполняется командой (потребуются права **администратора**):

```
sudo dnf install htop
```

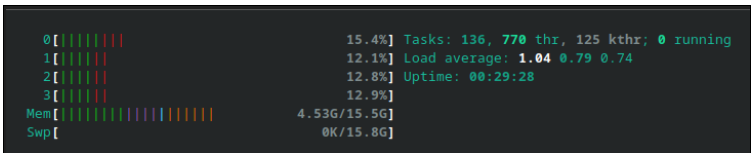
Работа с утилитой

Для запуска утилиты используется команда (с правами обычного **непривилегированного** пользователя):

```
htop
```

Общая информация

При запуске утилиты выводится общая информация о загруженности системы:

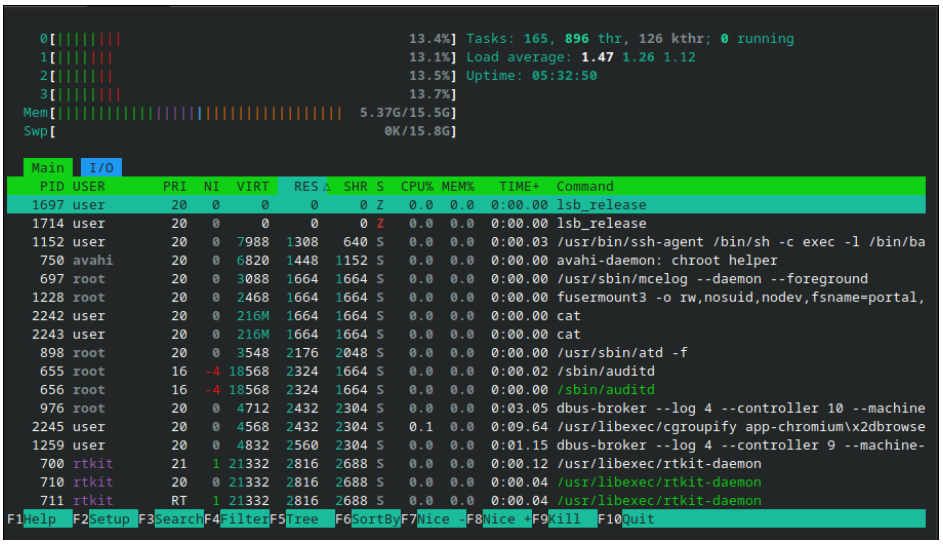


где:

- 0, 1, 2, 3 ... – нагрузка на каждое ядро процессора;
- Mem – используемая оперативная память и её общий объем;
- Swp – уровень заполненности раздела подкачки;
- Tasks/running – количество процессов и сколько из них активны;
- Load average – средняя загрузка системы за последние 1, 5, 15 минут;
- Uptime – время непрерывной работы системы.

Таблица main

На вкладке **main** выводится информация о запущенных процессах:



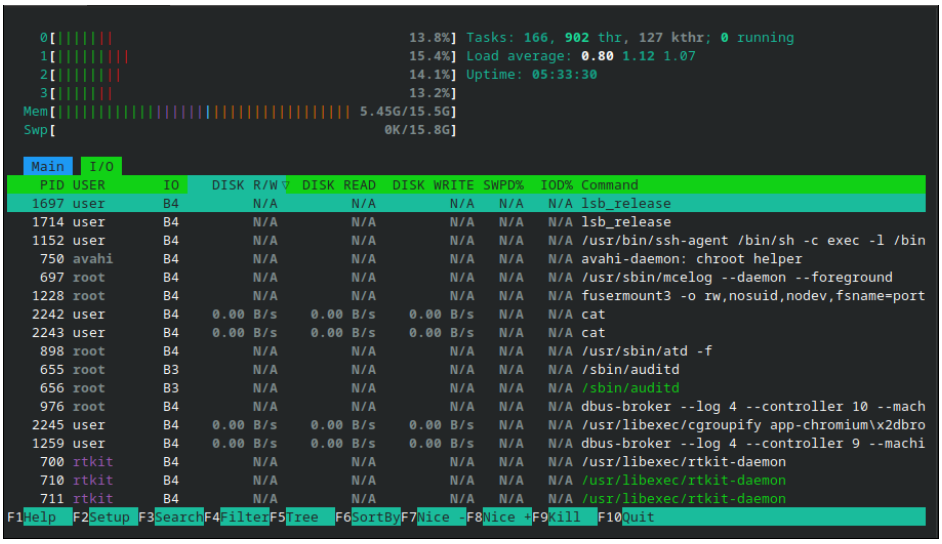
где:

- PID – уникальный идентификатор процесса;
- User – владелец процесса;
- PRI – приоритет в пространстве ядра;
- NI – приоритет процесса в пространстве пользователя (-20 самый высокий приоритет, 19 – самый низкий);
- VIRT – общее количество виртуальной памяти, занимаемое процессом;
- RES – физическая память, используемая процессом;
- SHR – объём памяти, который может быть использован совместно с другими процессами;
- S – состояние процесса:
  - R – процесс готов к выполнению и ожидает выделения процессорного времени;
  - S – процесс находится в состоянии сна, ожидая события (например, завершения ввода-вывода, сигнала таймера или другого процесса);
  - D – процесс находится в состоянии сна, ожидая ввода-вывода с диска;
  - Z – процесс завершился, но его запись в таблице процессов существует, пока родительский процесс не получит информацию о завершении;
  - T – процесс остановлен с помощью сигнала;
  - t – процесс остановлен для отладки (трассировки);
  - X – процесс завершился и его запись удалена из таблицы процессов;
  - W – процесс ожидает подкачки данных в RAM;

- CPU% – процент процессорного времени, который процесс использует в данный момент;
- MEM% – процент оперативной памяти, который процесс использует в данный момент;
- TIME+ – задержки ввода-вывода для достижения заданной цели;
- Command – имя выполняемой программы и аргументы.

Таблица I/O

На вкладке **I/O** отображаются данные о выполняемых операциях ввода/вывода:



где:

- IO – класс планирования ввода-вывода, за которым следует приоритет, если класс его поддерживает:
  - R – класс реального времени; процессам этого класса первым предоставляется доступ к диску;
  - B – класс планирования; процессы этого класса получают доступ к диску в порядке приоритета;
  - id – класс простоя; процессы этого класса получают доступ к диску только когда его не используют другие процессы;
- DISK R/W – сумма скорости ввода-вывода для чтения и для записи;
- DISK READ – скорость ввода-вывода для данного процесса при чтении;
- DISK WRITE – скорость ввода-вывода для данного процесса при записи;
- SWPD% – процент времени, затраченного на подкачку страниц;
- IOD% – процент времени, затраченного на ожидание завершения синхронного блочного ввода-вывода.

Горячие клавиши htop

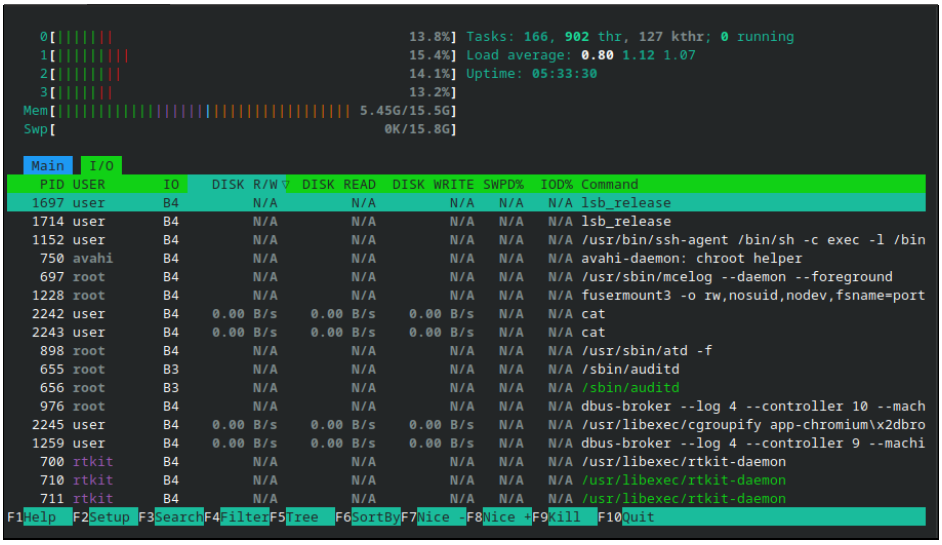
Клавиши навигации и выделения процессов

Для навигации и выбора нужных процессов используются следующие клавиши:

- курсорные клавиши (←, →, ↑, ↓) – прокрутка списка процессов;
- **PgUp**, **PgDn** – прокрутка списка вверх и вниз;
- **Home** – прокрутка к началу списка;
- **End** – прокрутка к концу списка;
- **Ctrl-a**, **^** – прокрутка к началу строки;
- **Ctrl-e**, **$** – прокрутка к концу строки;
- **Пробел** – выбор нескольких процессов. После этого введённые команды, такие как **kill (f9)** или изменение приоритета, будут применяться к группе выделенных процессов вместо подсвеченного в данный момент;
- **Shift-u** – снятие выделения со всех процессов;
- **l** – вывод файлов, открытых выделенным процессом. Для работы этой функции должна быть установлена утилита **lsof**.

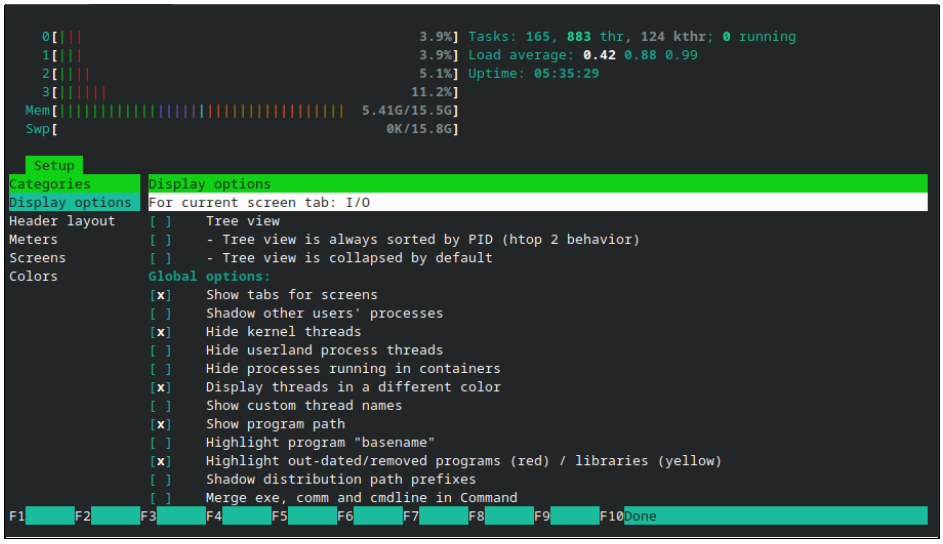
F1 Help

Выводит на экран сообщение помощи:



F2 Setup

Открывает экран настройки утилиты, в котором можно сконфигурировать счетчики, отображаемые в верхней части экрана – настройки отображения, выбор цветовой палитры, столбцы и их порядок.



F3 Search

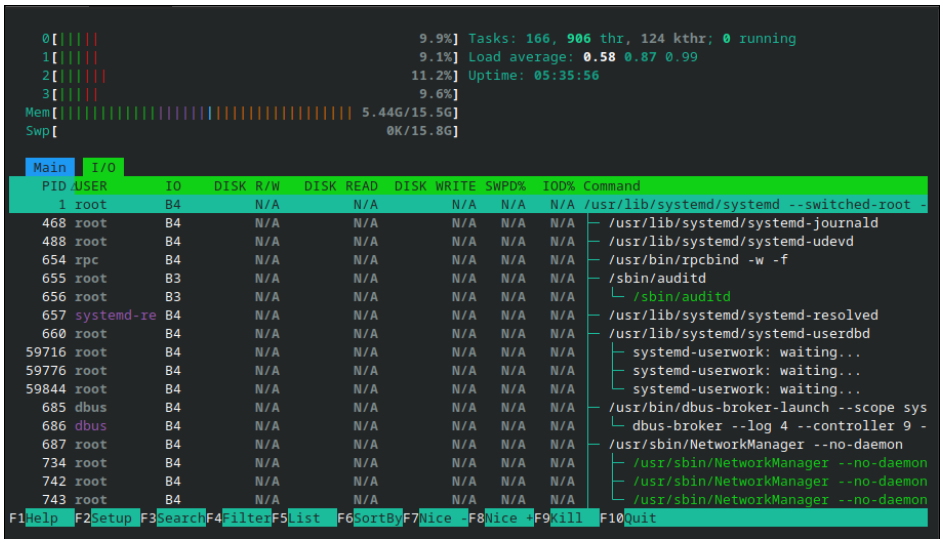
Поэтапный поиск в командах всех отображаемых процессов. Выбранная в данный момент (выделенная) команда будет обновляться по мере ввода. В режиме поиска нажатие клавиши **F3** приведет к цикличному просмотру подходящих процессов.

F4 Filter

Фильтрация процессов. Будут отображены только те процессы, названия которых содержат указанный фрагмент.

F5 Tree

Отображение процессов в виде дерева. При запуске нового процесса, процесс, который его запускает, принято называть *родительским* или просто *родителем*. Таким образом, новый процесс – это дочерний процесс родительского. Эти отношения образуют структуру в виде дерева.



F6 SortBy

Сортировка процессов по выбранному столбцу таблицы.

F7 Nice – и F8 Nice +

Увеличивает и уменьшает приоритет процесса.

F9 Kill

Системный вызов, который может послать сигнал процессу**.** Работает аналогично команде **kill**.

F10 Quit

Выход из утилиты.

atop

atop — интерактивный полноэкранный монитор производительности. Является аналогом **top**, но в отличие от него выводит только новые изменения об активных системных процессах. Основным преимуществом утилиты **atop** является функция ведения логов.

В состав пакета входит утилита **atopsar** — встроенный анализатор логов **atop**, который позволяет быстро найти проблему и просмотреть лог за определенный промежуток времени. Подробнее об утилите **atopsar** см. в нашей статье «atopsar — встроенный анализатор логов atop».

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

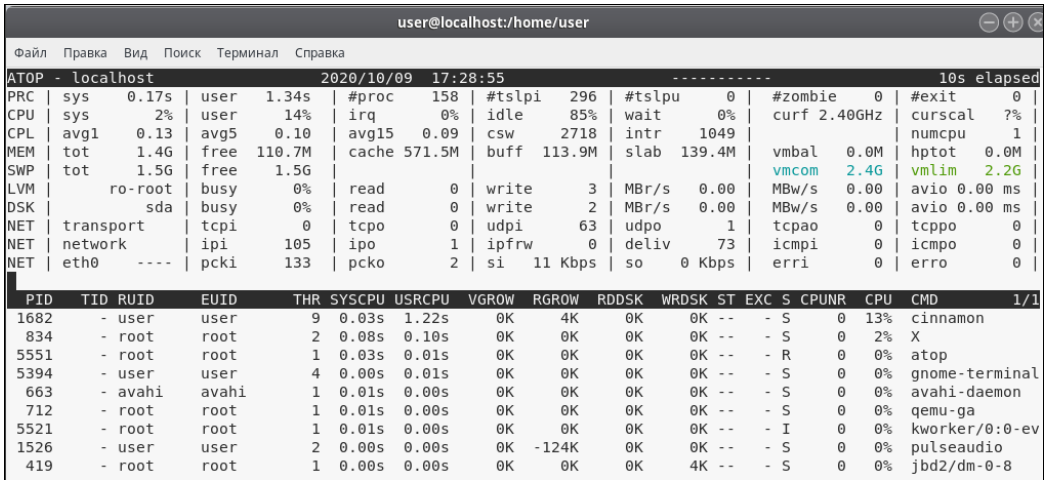
Установить **atop** можно командой (потребуются права **администратора**):

```
$ sudo dnf install atop
```

Для запуска утилиты необходимо в терминале выполнить команду:

```
$ atop
```

После запуска в терминале можно увидеть вывод, примерно следующего содержания:



Описание столбцов вывода **atop**:

- **PID** - идентификатор процесса;
- **RUID** — реальный UID, под которым обрабатывается процесс;
- **EUID** — эффективный UID, под которым обрабатывается процесс (Обычно реальный и эффективный идентификаторы совпадают, т.е. процесс имеет в системе те же права, что и пользователь, запустивший его.);
- **THR** - общее количество потоков для процесса;
- **SYSCPU** - потребление CPU за последний интервал в режиме system. (обычно системные вызовы);
- **USRCPU** - потребление CPU за последний интервал в режиме user;
- **VGROW** - рост виртуальной памяти в течении последнего интервала;
- **RGROW** - резидентный(реальный, занятый процессом ОП) рост памяти в течении последнего интервала. Может быть отрицательным, если процесс выгружается из памяти в swap;
- **RDDSK** - показывает кол обращений к физическому диску для считывания с него данных(минуя кеш);
- без установленного патча - количество данных считаные с диск(минуя кеш);
- **WRDSK** - показывает кол обращений к физическому диску для записи на него данных(минуя кеш);
- **ST** - статус процесса (N в первой позиции говорит, что процесс был запущен во время последнего интервала. Вторая позиция показывает закончился ли процесс за время последнего интервала: E — exit, S - прекращено, C - прекращено но остался core dump);
- **EXC** - код выхода процесса;
- **S** - состояние процесса. (S=sleep (ожидает событий) R=running (работает) Z=zombie (ожидает родительский процесс);
- **CPUNR** - идентифицирует CPU который обрабатывает процесс;
- **CPU** - процент занятости выбранного ресурса;
- **CMD** - имя процесса.

Далее приведено описание наиболее часто используемых интерактивных команд, которые вы можете выполнять во время работы программы:

- **m** — отсортирует процессы по занятой памяти;
- **d** — отсортирует процессы по использованию диска;
- **n** — отсортирует процессы по использованию сети (доступно только с установленным патчем);
- **v** — покажет более подробную информацию о процессах (пользователя, дату и время начала процесса);
- **u** — отсортирует таблицу по пользователям. Использование **shift**+(**d,m,n**) выстроит текущий список по выше указанным параметрам;
- **i** — изменение времени проверки, по умолчанию 10 секунд;
- **g** — вернет все в дефолтный вывод;
- **c** - вывести полный путь запущенного процесса (столбец **COMMAND**).

Для посуточного ведения логов необходимо отредактировать конфигурационный файл **atop**:

```
vi /etc/sysconfig/atop
```

Добавьте в конец файл следующие строки:

```
# Имя файла логов

OUTFILE="$LOGPATH/$CURDAY.log"
```

Общий вид конфига будет следующего содержания:

```
# sysconfig atop
#

# Current Day format
CURDAY=`date +%Y%m%d`
# Log files path
LOGPATH=/var/log/atop
# Binaries path
BINPATH=/usr/bin
# PID File
PIDFILE=/var/run/atop.pid
# interval (default 10 minutes)
INTERVAL=600
# Имя файла логов
OUTFILE="$LOGPATH/$CURDAY.log"
```

По умолчанию **atop** делает снимок раз в 10 минут, это значение регулируется параметром **INTERVAL** в конфиге **/etc/sysconfig/atop**, указывается в секундах, при необходимости поменяйте данный параметр.

После внесения изменений перезапустите **atop**:

```
sudo systemctl restart atop.service
```

Для просмотра дневного лога необходимо в терминале выполнить команду:

```
atop -r /var/log/atop/atop_20201009
```

где **/var/log/atop/atop_20201009** путь до нужного лога.

Для навигации по времени в дневном логе используются клавиши:

- **t** - перейти вперед по времени;
- **Shift + t** - перейти назад по времени.

Для остановки сбора логов необходимо выполнить:

```
sudo systemctl stop atop.service
```

atopsar — встроенный анализатор логов atop

atopsar — встроенный анализатор логов **atop**, который позволяет быстро найти проблему и смотреть лог за определенный промежуток времени. Входит в состав пакета утилиты **atop**.

Подробнее об **atop** см. в нашей статье «Интерактивные утилиты динамического мониторинга процессов. Atop».

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install atop
```

Дальнейшая работа с утилитой выполняется с правами **непривилегированного** пользователя. Выйдите из сеанса пользователя **root**:

```
exit
```

Все логи сохраняются в каталоге по пути **/var/log/atop/**, файлы именуются по формату `atop_<дата>`.

Основные ключи:

- **-r** — считывание данных из файла;
- **-b** — с какого времени вывести лог;
- **-e** — до какого времени вывести лог.

Дополнительные опции для анализа:

- **-d** — нагрузка на каждый диск;
- **-m** — нагрузка на оперативную память и **swap**;
- **-c** — нагрузка на процессор, отдельно по каждому ядру;
- **-p** — количество процессов и потоков;
- **-w** — нагрузка на сетевой трафик;
- **-i** — нагрузка на интерфейс;
- **-O** — топ-3 процессов по использованию процессора;
- **-G** — топ-3 процессов по использованию памяти;
- **-D** — топ-3 процессов по использованию диска;
- **-N** — топ-3 процессов по использованию сети;
- **-A** — все возможные отчеты.

Например, можно смотреть нагрузку на диск по анализу логов за определенный день и время, используя ключ **-d**:

```
atopsar -r /var/log/atop/atop_20231130 -d -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -d -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02  disk           busy read/s KB/read  writ/s KB/writ avque avserv _dsk_
14:18:02  sda              4%    1.8    95.3    10.3    24.9  32.1   3.39766 ms
14:28:02  sda              7%    4.7    61.7    11.7    24.5  35.9   4.07435 ms
14:38:02  sda              5%    5.1   108.5    10.1    24.3  32.5   3.02773 ms
14:48:02  sda              4%    1.6    99.0    10.0    20.1  37.0   3.54848 ms
14:58:02  sda              6%    2.9    79.1    11.0    23.2  31.2   4.16561 ms
15:08:02  sda              6%    6.1    48.0    10.3    22.9  28.2   3.52879 ms
15:18:02  sda              8%   15.8    71.4    10.9    29.7  17.9   2.97726 ms
15:28:02  sda              4%    5.3    96.6    10.4    23.2  30.2   2.34367 ms
15:38:02  sda              5%    3.7    89.0     9.7    23.1  36.4   3.47787 ms
15:48:02  sda              7%    4.6   114.6     9.2    21.6  31.5   5.42570 ms
15:58:02  sda              6%    3.3    99.6    10.0    22.5  32.9   4.68405 ms
```

где:

- **busy** — процент занятости ресурса;
- **read/s** — количество запросов чтения в секунду;
- **KB/read** — объем прочитанных данных в секунду;
- **writ/s** — количество запросов на запись в секунду;
- **KB/writ** — объем записанных данных в секунду;
- **avque** — среднее число запросов;
- **avserv** — среднее время обработки запроса.

Используя ключ **-m**, можно посмотреть, как изменялись значения ОЗУ в указанном диапазоне времени:

```
atopsar -r /var/log/atop/atop_20231130 -m -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -m -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02  memtotal memfree buffers cached dirty slabmem  swptotal swpfree _mem_
14:18:02      954M     64M      4M   301M    0M    102M     1843M   1211M
14:28:02      954M     64M      9M   328M    3M    102M     1843M   1180M
14:38:02      954M     63M      2M   344M    9M    102M     1843M   1160M
14:48:02      954M     72M      3M   336M    2M    101M     1843M   1157M
14:58:02      954M     69M      3M   351M    1M    101M     1843M   1138M
15:08:02      954M     65M      6M   367M    6M    101M     1843M   1120M
15:18:02      954M     78M      4M   376M    5M    102M     1843M   1064M
15:28:02      954M     85M      3M   387M    0M    102M     1843M   1048M
15:38:02      954M     70M      3M   400M    0M    102M     1843M   1034M
15:48:02      954M     67M      3M   410M    0M    101M     1843M   1024M
15:58:02      954M     71M      3M   405M    2M    102M     1843M   1013M
```

где:

- **memtotal** — общий объем оперативной памяти;
- **memfree** — доступный объем оперативной памяти;
- **buffers** — объем буферной памяти;
- **cached** — объем кэш-памяти;
- **dirty** — объем памяти в кэше страниц, который еще нужно сбросить на диск;
- **slabmem** — объем динамической памяти, выделяемой ядром;
- **swptotal** — общий объем памяти подкачки (**swap**);
- **swpfree** — доступный объем памяти подкачки (**swap**).

Узнать, какие топ-3 приложения потребляют память, можно используя ключ **-G**:

```
atopsar -r /var/log/atop/atop_20231130 -G -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -G -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02    pid command  mem% |   pid command  mem% |   pid command  mem%_top3_
14:18:02   8954 rdbserve  26% |   989 Xorg       7% |  1794 mate-scr   4%
14:28:02   8954 rdbserve  24% |   989 Xorg       7% |  1794 mate-scr   4%
14:38:02   8954 rdbserve  22% |   989 Xorg       8% |  1794 mate-scr   4%
14:48:02   8954 rdbserve  22% |   989 Xorg       7% |  1794 mate-scr   4%
14:58:02   8954 rdbserve  22% |   989 Xorg       7% |  1794 mate-scr   4%
15:08:02   8954 rdbserve  20% |   989 Xorg       7% |  1794 mate-scr   4%
15:18:02   8954 rdbserve  18% |   989 Xorg       7% |  1794 mate-scr   4%
15:28:02   8954 rdbserve  16% |   989 Xorg       7% |  1794 mate-scr   3%
15:38:02   8954 rdbserve  17% |   989 Xorg       6% |  1794 mate-scr   3%
15:48:02   8954 rdbserve  16% |   989 Xorg       7% |  1794 mate-scr   4%
15:58:02   8954 rdbserve  16% |   989 Xorg       6% |  1794 mate-scr   4%
```

где:

- **pid** — идентификатор процесса;
- **command** — наименование процесса;
- **mem%** — процент использования памяти процессом.

Аналогично, можно получить топ-3 приложения по загрузке процессора, выполняя команду с ключом **-O**, и по использованию диска с ключом **-D**:

```
atopsar -r /var/log/atop/atop_20231130 -D -O -b 14:00 -e 16:00
```

```
[user@localhost ~]$ atopsar -r /var/log/atop/atop_20231130 -D  -O -b 14:00 -e 16:00

localhost  6.1.38-2.el7.3.x86_64  #1 SMP PREEMPT_DYNAMIC Wed Jul 12 15:59:00 MSK 2023  x86_64  2023/12/04

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02    pid command  cpu% |   pid command  cpu% |   pid command  cpu%_top3_
14:18:02   8954 rdbserve  99% |   609 qemu-ga    0% |    47 kswapd0    0%
14:28:02   8954 rdbserve  98% |  9265 dnf        0% |   609 qemu-ga    0%
14:38:02   8954 rdbserve  99% |   609 qemu-ga    0% |  9288 gdbus      0%
14:48:02   8954 rdbserve  99% |   609 qemu-ga    0% |  1981 dnfdrago   0%
14:58:02   8954 rdbserve  99% |   609 qemu-ga    0% |    47 kswapd0    0%
15:08:02   8954 rdbserve  99% |   989 Xorg       0% |  9346 mate-scr   0%
15:18:02   8954 rdbserve  97% |  9433 dnfdaemo   0% |    47 kswapd0    0%
15:28:02   8954 rdbserve  99% |  9461 dnf        0% |   609 qemu-ga    0%
15:38:02   8954 rdbserve  98% |   609 qemu-ga    0% |    47 kswapd0    0%
15:48:02   8954 rdbserve  98% |   609 qemu-ga    0% |  9491 mate-scr   0%
15:58:02   8954 rdbserve  98% |   609 qemu-ga    0% |    47 kswapd0    0%

------------------------- analysis date: 2023/11/30 -------------------------

14:08:02    pid command  dsk% |   pid command  dsk% |   pid command  dsk%_top3_
14:18:02   8954 rdbserve  94% |  1005 systemd-   3% |   480 systemd-   2%
14:28:02   8954 rdbserve  79% |     1 systemd   16% |  1005 systemd-   2%
14:38:02   8954 rdbserve  56% |  1794 mate-scr  37% |   480 systemd-   2%
14:48:02   8954 rdbserve  90% |  1005 systemd-   5% |   480 systemd-   3%
14:58:02   8954 rdbserve  95% |  1005 systemd-   2% |   480 systemd-   1%
15:08:02   8954 rdbserve  66% |  1794 mate-scr  20% |   989 Xorg       4%
15:18:02   8954 rdbserve  57% |     1 systemd   29% |  1470 systemd    8%
15:28:02   8954 rdbserve  60% |     1 systemd   31% |   914 master     5%
15:38:02   8954 rdbserve  91% |  9476 pickup     4% |     1 systemd    2%
15:48:02   8954 rdbserve  53% |  1794 mate-scr  38% |  1005 systemd-   2%
15:58:02   8954 rdbserve  98% |  9519 systemd-   1% |     1 systemd    0%
```

iotop - утилита мониторинга использования диска

Установка
Основные опции программы
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** iotop 0.6-15

Утилита **iotop** позволяет просмотреть сведения об общем и текущем количестве операций обращения к диску.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

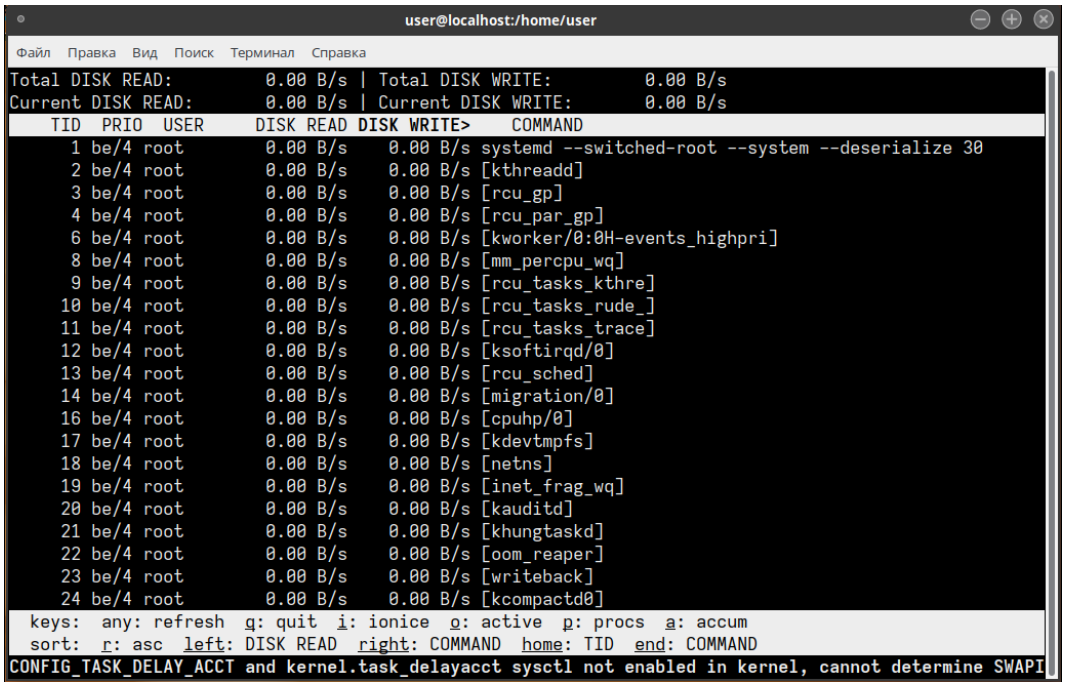
```
su -
```

и выполните команду:

```
dnf install iotop
```

Запустите утилиту через терминал, выполнив:

```
iotop
```



Основные опции программы

Опции для работы в программе описаны в таблице ниже.

Опции	Описание
--version	показать номер версии программы и выйти
-h, --help	показать данное справочное сообщение и выйти
-o, --only	отображать только процессы, которые в данный момент выполняют операции I/O с диском (по умолчанию — отображаются все активные процессы)
-b, --batch	неинтерактивный режим
-n <число>, --iter=<число>	количество итераций до окончания [бесконечно]
-d <сек>, --delay=<сек>	задержка между итерациями [1 секунда]
-p <PID_процесса>, --pid= <PID_процесса>	PID процесса, который нужно отслеживать
-u <имя_пользователя>, --user= <имя_пользователя>	имя пользователя, которого нужно отследить
-P, --processes	отображать только процессы (по умолчанию — все процессы и потоки)
-a, --accumulated	показывать накопленный ввод-вывод вместо пропускной способности
-k, --kilobytes	отображать информацию в КБ
-t, --time	добавить отображение времени выполнения проверки
-q, --quiet	уменьшить количество выводимой информации (подразумевается --batch)

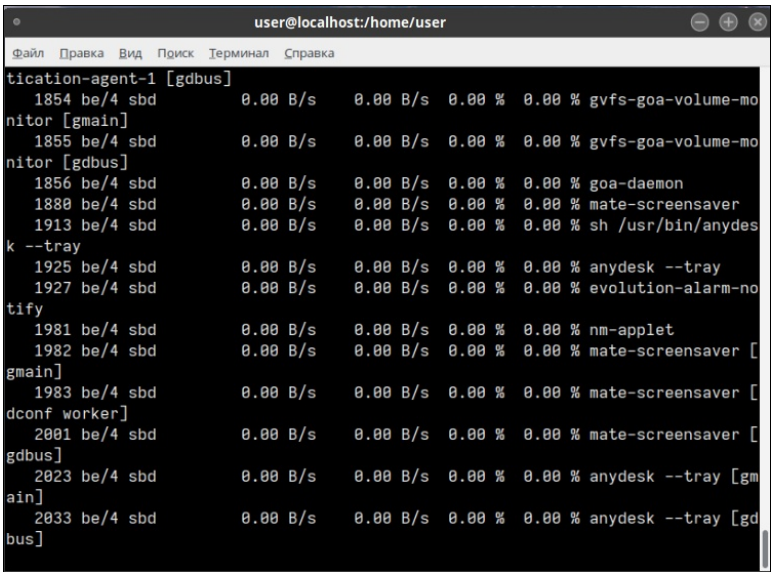
Также **iotop** поддерживает некоторое управление клавиатуры:

- стрелки **влево**-**вправо** — изменить сортировку колонок;
- **r** — изменить сортировку строк в выбранной колонке на обратную (a-z > z-a);
- **i** — изменить nice процесса (утилитой **ionice**);

Пример работы

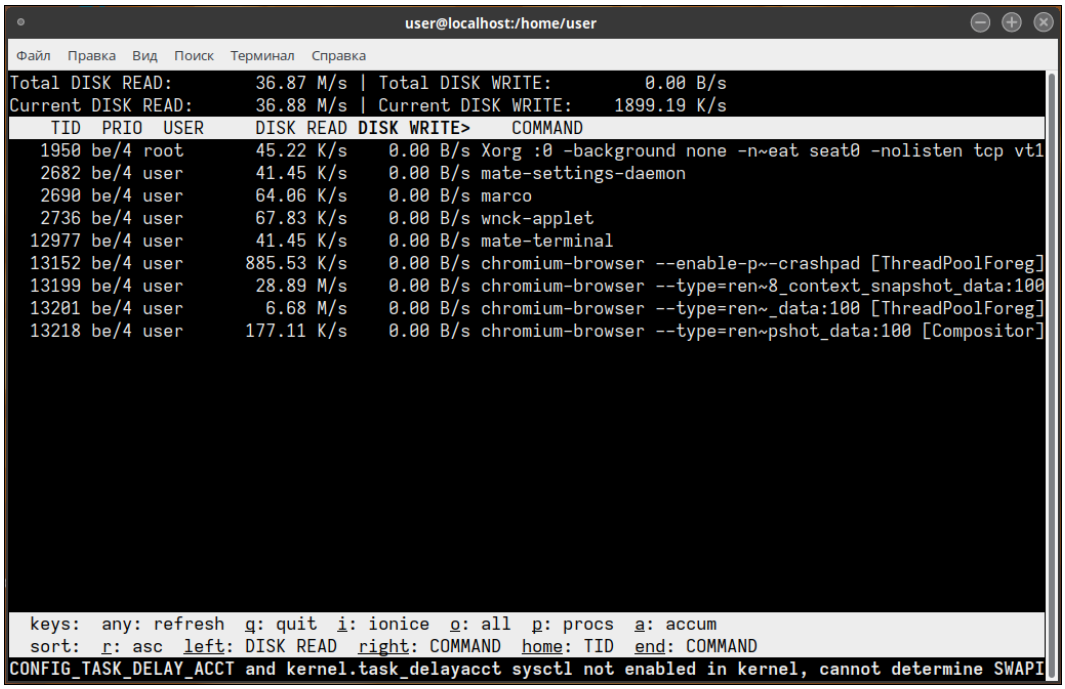
Для отключения интерактивного вида используйте:

```
iotop -b
```



Для отображения только процессов, которые в данный момент выполняют операции I/O с диском:

```
iotop -o
```

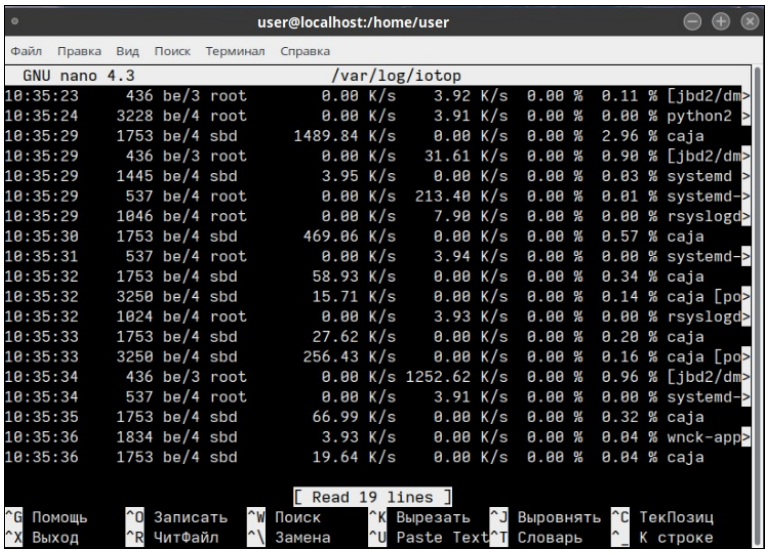


Программа позволяет не только выводить информацию, но и записывать ее для решения проблем в будущем.

Пример команды:

```
iotop -botqqqk --iter=60 >> /var/log/iotop
```

Результат можно посмотреть в указанном файле:



sar

Установка
Синтаксис
Параметры
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: sysstat-12.5.4-4

Sar (System Activity Report) — утилита для сбора статистической информации о производительности системы. **Sar** позволяет наблюдать за производительностью различных подсистем в реальном времени.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Утилита **sar** входит в пакет **sysstat**, для установки выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install sysstat
```

Дальнейшая работа в программе производится с правами непривилегированного пользователя.

Для получения дополнительной информации выполните команду:

```
man sar
```

Список опций можно получить с помощью параметра **--help**:

```
sar --help
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
sar [<параметры>] [<интервал>[<счётчик>]]
```

Параметры

Основные параметры утилиты:

- **-B** — статистика обмена страниц;
- **-b** — статистика ввода-вывода и скорости передачи;
- **-d** — статистика блочных устройств;
- **-F [MOUNT]** — статистика файловых систем;
- **-H** — статистика использования **hugepages** (больших страниц оперативной памяти);
- **- I { <список> | SUM | ALL }** — статистика прерываний;

- **-m { <ключ> | ALL }** — статистика управления питанием. Возможные значения:
  - **CPU** — текущая частота работы ЦП;
  - **FAN** — скорость вращения вентиляторов;
  - **FREQ** — средняя частота работы ЦП;
  - **IN** — входные напряжения;
  - **TEMP** — температура устройств;
  - **USB** — подключенные USB-устройства.
- **-n { <ключ> | ALL }** — сетевая статистика. Возможные значения:
  - **DEV** — статистика сетевых интерфейсов, включая количество принятых и переданных пакетов;
  - **EDEV** — статистика ошибок сетевых интерфейсов;
  - **NFS** — статистика клиента NFS;
  - **NFSD** — статистика сервера NFS;
  - **SOCK** — сокеты;
  - **IP** — IP-трафик;
  - **EIP** — ошибки IP-трафика;
  - **ICMP** — ICMP-трафик;
  - **EICMP** — ошибки ICMP-трафика;
  - **TCP** — TCP-трафик;
  - **ETCP** — ошибки TCP-трафика;
  - **UDP** — UDP-трафик;
  - **SOCK6** — сокеты IPv6;
  - **IP6** — IP-трафик IPv6;
  - **EIP6** — ошибки IP-трафика IPv6;
  - **ICMP6** — ICMP-трафик IPv6;
  - **EICMP6** — ошибки ICMP-трафика IPv6;
  - **UDP6** — UDP-трафик IPv6;
  - **FC** — адаптер Fibre channel;
  - **SOFT** — программная сетевая обработка.
- **-q [<ключ> | PSI | ALL]** — статистика по загрузке и провалов нагрузки системы. Возможные значения ключа:
  - **LOAD** — статистика длины очереди и средней загрузки;
  - **CPU** — статистика провалов нагрузки ЦП CPU;
  - **IO** — статистика провалов нагрузки ВВ/ВЫВ;
  - **MEM** — статистика провалов нагрузки памяти;
- **-r [ALL]** — статистика использования памяти;
- **-S** — статистика использования области подкачки;
- **-u [ALL]** — статистика использования ЦП;
- **-v** — статистика таблиц ядра;
- **-W** — статистика раздела подкачки;
- **-w** — статистика создания задач и системных переключений;
- **-y** — статистика устройств TTY.

Примеры использования

1. Сбор и отображение полной статистики работы процессора в течение 5 циклов с интервалом 2 секунды:

```
sar -u ALL 2 5
```

Пример вывода:

```
15:24:40      CPU    %usr   %nice    %sys %iowait  %steal   %irq  %soft  %guest  %gnice   %idle
15:24:42      all    0,50    0,00    0,25    0,00    0,00   1,50   2,51    0,00    0,00   95,24
15:24:44      all    0,25    0,00    0,00    0,00    0,00   1,50   2,26    0,00    0,00   95,99
15:24:46      all    1,25    0,00    0,50    0,75    0,00   1,75   2,01    0,00    0,00   93,73
15:24:48      all    0,25    0,00    0,25    0,00    0,00   1,51   2,02    0,00    0,00   95,97
15:24:50      all    0,75    0,00    0,50    0,00    0,00   1,51   2,26    0,00    0,00   94,97
Среднее:      all    0,60    0,00    0,30    0,15    0,00   1,56   2,21    0,00    0,00   95,18
```

где:

- **%usr** — процент времени, затраченного процессором на выполнение кода, запущенного на уровне пользователя;
- **%nice** — процент времени, затраченного процессором на выполнение кода в пользовательском пространстве с пониженным приоритетом;
- **%sys** — процент времени, затраченного процессором на выполнение кода в системном пространстве;
- **%iowait** — процент времени, затраченного процессором на ожидание завершения операций ввода/вывода;
- **%steal** — процент времени, проведенного в вынужденном ожидании виртуальным процессором или ЦПУ, пока гипервизор обслуживал другой виртуальный процессор;
- **%irq** — процент времени, затраченного процессором на обслуживание аппаратных прерываний;
- **%soft** — процент времени, затраченного процессором на обслуживание системных прерываний;
- **%guest** — процент времени, затраченного процессором на выполнение кода, запущенного внутри виртуальной машины;
- **%gnice** — процент времени, затраченного процессором на выполнение кода, запущенного с помощью команды nice внутри виртуальной машины;
- **%idle** — процент времени, когда процессор простаивает и не выполняет никаких задач.

Анализ результатов статистики состояния процессора:

- **idle < 20%** — указывает на высокую загрузку процессора. Необходимо определить, обусловлена ли нагрузка пользовательскими приложениями (user) или системными процессами (system);
- **usr > 70%** — процессор перегружен пользовательскими приложениями. Используйте инструменты, такие как **top**, **htop**, или **pidstat**, чтобы найти самые ресурсозатратные процессы;
- **sys > 30%** — высокая системная нагрузка, ядро работает слишком интенсивно, система перегружена системными вызовами, прерываниями, драйверами; проверьте работу драйверов или включите диагностику через **iostat** и **vmstat;**
- **iowait > 10%** — процессоры ждут операций ввода-вывода, указывая на проблемы с подсистемой хранения данных (диск или сеть), используйте **iostat** или **sar -d** для диагностики подсистемы ввода-вывода;
- **steal > 5%** — в виртуальной среде это говорит о конкуренции за **CPU** с другими виртуальными машинами.

2. Сбор и вывод статистики по свободной и занятой памяти:

```
sar -r 2 5 --human
```

где:

--human — отображение результата в удобочитаемом формате.

Пример вывода:

```
17:17:48    kbmemfree   kbavail kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
17:17:50      473,6M      1,3G    339,9M     17,3%    22,6M   1004,0M      3,4G     86,4%    811,0M    463,1M    104,0k
17:17:52      345,2M      1,2G    438,6M     22,4%    22,9M      1,0G      4,9G    124,4%    931,3M    463,3M    848,0k
17:17:54      285,9M      1,2G    463,1M     23,6%    22,9M      1,0G      5,0G    126,8%    988,0M    463,6M     1,4M
17:17:56      193,9M      1,1G    554,6M     28,3%    23,0M      1,0G      5,8G    146,7%      1,0G    465,2M     2,5M
17:17:58      184,3M      1,1G    563,1M     28,7%    23,2M      1,0G      6,4G    161,6%      1,0G    468,5M     3,2M
Среднее:      296,6M      1,2G    471,9M     24,1%    22,9M      1,0G      5,1G    129,2%    974,1M    464,7M     1,6M
```

где:

- **kbmemfree** — свободная память;
- **kbavail** — доступная память;

- **kbmemused** — использованная память;
- **%memused** — процент использованной памяти;
- **kbbuffers** — память, используемая ядром как буфер;
- **kbcached** — память, используемая ядром для кеширования данных;
- **kbcommit** — память, необходимая для текущей рабочей нагрузки;
- **%commit** — процент памяти, необходимый для рабочей нагрузки;
- **kbactive** — память, использовавшаяся недавно;
- **kbinact** — память, использовавшаяся давно;
- **kbdirty** — память, ожидающая перезаписи.

3. Сбор и вывод статистики по использованию устройств ввода/вывода:

```
sar -b 2 5
```

Пример вывода:

```
15:37:53        tps     rtps     wtps     dtps   bread/s   bwrtn/s   bdscd/s
15:37:55       0,00     0,00     0,00     0,00      0,00      0,00      0,00
15:37:57       0,00     0,00     0,00     0,00      0,00      0,00      0,00
15:37:59      37,50    37,50     0,00     0,00  69324,00      0,00      0,00
15:38:01     104,50   101,00     3,50     0,00 154636,00    128,00      0,00
15:38:03     191,50   187,50     4,00     0,00 154880,00    208,00      0,00
Среднее:     66,70    65,20     1,50     0,00  75768,00     67,20      0,00
```

где:

- **tps** — общее число передач в секунду, отправленных на физические устройства;
- **rtps** — число запросов на чтение (в сек.), отправленных на физические устройства;
- **wtps** — число запросов на запись (в сек.), отправленных на физические устройства;
- **dtps** — число запросов на удаление (в сек.), отправленных на физические устройства;
- **bread/s** — количество блоков, прочитанных (в сек.);
- **bwrtn/s** — количество блоков, записанных (в сек.);
- **bdscd/s** — количество блоков, отброшенных (в сек.).

4. Сбор и вывод статистики по трафику IPv4:

```
sar -n SOCK 3 5
```

Пример вывода:

```
15:41:48     totsck   tcpsck   udpsck   rawsck  ip-frag   tcp-tw
15:41:51       869       34        8        1        0        1
15:41:54       927       55       18        1        0        2
15:41:57       930       59       12        1        0        2
15:42:00       964       81       15        1        0        2
15:42:03       976       97       12        1        0        4
Среднее:       933       65       13        1        0        2
```

где:

- **totsck** — общее количество сокетов в системе;
- **tcpsck** — количество сокетов TCP (Transmission Control Protocol);
- **udpsck** — количество сокетов UDP (User Datagram Protocol);
- **rawsck** — количество сокетов RAW (сокеты, которые используются для передачи данных без использования транспортного протокола);
- **ip-frag** — количество фрагментов IP-пакетов, которые ожидают сборки;
- **tcp-tw** — количество сокетов TCP, находящихся в состоянии TIME-WAIT (ожидание закрытия соединения).

5. Сбор и вывод статистики по средней загрузке:

```
sar -q 2 5
```

Пример вывода:

```
15:45:06     runq-sz  plist-sz   ldavg-1   ldavg-5  ldavg-15   blocked
15:45:08           1       532      0,45      0,34      0,16         0
15:45:10           0       532      0,58      0,37      0,17         0
15:45:12           2       562      0,58      0,37      0,17         0
15:45:14           4       579      1,17      0,49      0,22         1
15:45:16           3       582      1,17      0,49      0,22         0
Среднее:           2       557      0,79      0,41      0,19         0
```

где:

- **runq-sz** — количество задач, ожидающих начала выполнения;
- **plist-sz** — количество задач в списке задач;
- **ldavg-1** — средняя загрузка системы за последнюю минуту;
- **ldavg-5** — средняя загрузка системы за последние 5 минут;
- **ldavg-15** — средняя загрузка системы за последние 15 минут;
- **blocked** — количество задач, заблокированных в данный момент.

6. Сбор статистики ввода-вывода на уровне устройств:

```
sar -d 2 4
```

Пример вывода:

```
09:06:07       DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:09       sda      3,98      0,00     35,82      0,00      9,00      0,00      0,62      0,05
09:06:09       sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
09:06:09     zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

09:06:09       DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:11       sda      4,50      0,00    482,00      0,00    107,11      0,01      1,22      0,50
09:06:11       sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
09:06:11     zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

09:06:11       DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:13       sda      1,00      0,00     44,00      0,00     44,00      0,01      3,00      0,25
09:06:13       sdb      1,50      0,00      8,00      0,00      5,33      0,07     21,67      3,25
09:06:13     zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

09:06:13       DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
09:06:15       sda     28,00      0,00    126,00      0,00      4,50      0,12      4,12      0,50
09:06:15       sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
09:06:15     zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00

Среднее:       DEV       tps     rkB/s     wkB/s     dkB/s   areq-sz    aqu-sz     await     %util
Среднее:       sda      9,36      0,00    171,79      0,00     18,35      0,03      3,37      0,32
Среднее:       sdb      0,37      0,00      2,00      0,00      5,33      0,02     21,67      0,81
Среднее:     zram0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
```

где:

- **DEV** — имя устройства, для которого собирается статистика (например, **sda**, **sdb** или **nvme0n1**);
- **tps** — количество операций ввода-вывода в секунду на устройство;
- **rkB/s** — скорость чтения данных с устройства в КБ/сек.;
- **wkB/s** — скорость записи данных на устройство в КБ/сек.;
- **dkB/s** — скорость операций **discard** (освобождения места) в КБ/сек.;
- **areq-sz** — средний размер операций ввода-вывода в КБ;
- **aqu-sz** — среднее количество операций ввода-вывода, ожидающих выполнения;

- **await** — среднее время (в миллисекундах), которое запросы ввода-вывода ожидали выполнения;
- **%util** — процент времени, в течение которого устройство было занято обработкой запросов.

Как интерпретировать статистику:

- высокие значения **tps**, **rkB/s**, **wkB/s** указывают на активную загрузку устройства;
- высокий **%util** (>70-80%) указывает на то, что устройство может стать узким местом;
- высокий **await** говорит о задержках в обработке операций, что может быть вызвано очередями или высокой нагрузкой.

pmap

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Команда **pmap** предоставляет подробную карту памяти, используемой процессом. Для работы с этой командой необходимо сначала найти идентификатор нужного процесса. Его можно получить командой **ps**, или даже командой **top**, если речь идет о процессе, потребляющем много процессорного времени.

Для запуска утилиты необходимо в терминале выполнить команду:

```
pmap <параметр> <идентификатор процесса>
```

Например:

```
[root@localhost ~]# pmap -x 34770
34770:   bash
Address           Kbytes     RSS   Dirty Mode  Mapping
0000000000400000    1036     952       0 r-x-- bash
0000000000702000       4       4       4 r---- bash
0000000000703000      36      36      36 rw--- bash
000000000070c000      40      28      28 rw---   [ anon ]
0000000000b1d000    1452    1352    1352 rw---   [ anon ]
00007f1219258000      44      44       0 r-x-- libnss_files-2.28.so
00007f1219263000    2048       0       0 ----- libnss_files-2.28.so
00007f1219463000       4       4       4 r---- libnss_files-2.28.so
00007f1219464000       4       4       4 rw--- libnss_files-2.28.so
00007f1219465000      24       0       0 rw---   [ anon ]
00007f121946b000      40      40       0 r-x-- libnss_sss.so.2
00007f1219475000    2044       0       0 ----- libnss_sss.so.2
00007f1219674000       4       4       4 r---- libnss_sss.so.2
00007f1219675000       4       4       4 rw--- libnss_sss.so.2
00007f1219676000  212648     512       0 r---- locale-archive
```

Основные параметры:

- **-x** - эта опция используется для отображения карты памяти в расширенном формате.
- **-p** - эта опция используется для отображения полного пути к файлам.
- **-d** - эта опция используется для отображения формата устройства.
- **-q** - эта опция используется для игнорирования имен столбцов при отображении отчета карты памяти.
- **-A** - эта опция используется для отображения результатов в заданном диапазоне. Обратите внимание, что аргументы **low** и **high** — это одна строка, разделенная запятой.
- **-XX** - эта опция используется для отображения всего, что предоставляет ядро.
- **-n** - эта опция используется для создания новой конфигурации.
- **-c** - эта опция используется для чтения конфигурации по умолчанию.
- **-h** - эта опция используется для отображения текста справки.
- **-v** - эта опция используется для отображения информации о версии и выхода.

nmon

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

nmon — это утилита измерения и настройки производительности для системных администраторов. Она может отображать информацию о ЦП, оперативной памяти, сети, дисках (в виде мини графиков или числовых данных), файловых системах, NFS, самых нагружающих процессах, ресурсах (версия Linux и процессоры).

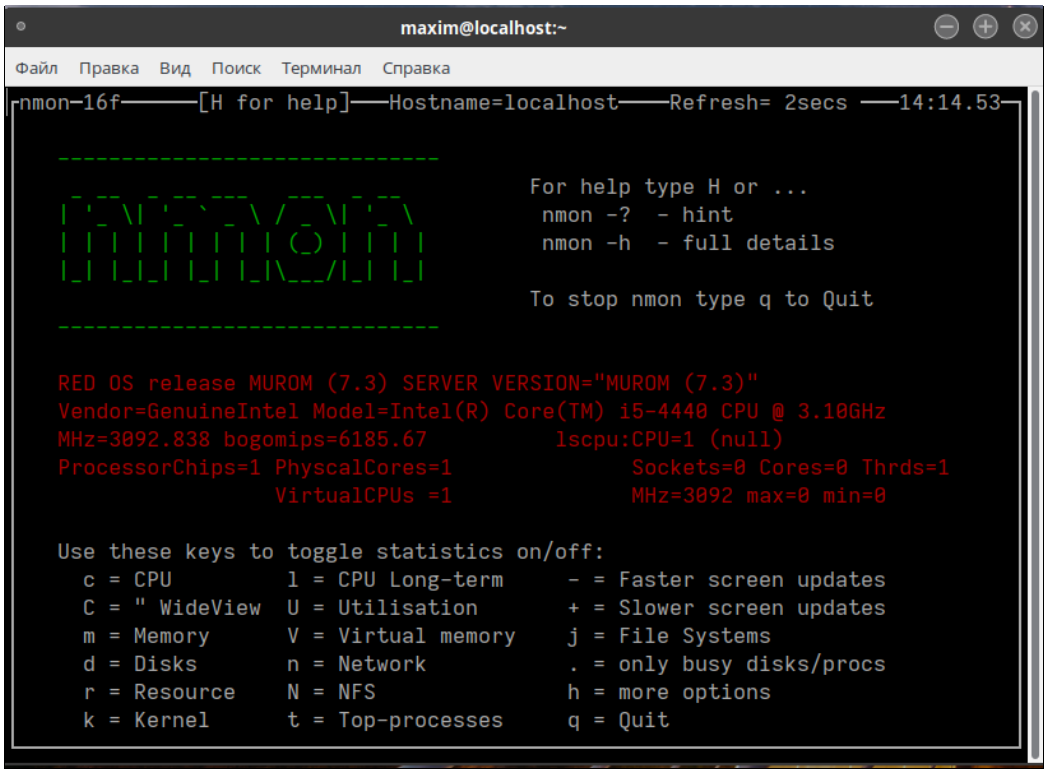
Устанавливается командой:

```
sudo dnf install nmon
```

Для запуска утилиты необходимо в терминале выполнить команду:

```
nmon
```

После запуска в терминале можно увидеть вывод, примерно следующего содержания:



Для отображения информации по определенному ресурсу используются следующие клавиши:

- **c = CPU** - Показывает нагрузку каждого ядра процессора и среднюю нагрузку процессора, загруженность системой, пользователем и ожидание.
- **m = Memory** - Показывает общее количество оперативной памяти, занятой в мегабайтах и процентах, файла подкачки, кэшированной памяти, буфера и другу информацию о состоянии памяти.
- **d = Disks** - Показывает информацию о состоянии дисков и их разделов (информация файла /proc/diskstats). Информация представлена в виде таблицы и графика, в котором показаны имя физического диска и томов, количество занятой памяти, текущее чтение и запись с раздела диска (в килобайтах), для каждого раздела существует график со шкалой от 0 до 100 процентов, для визуальной наглядности загруженности дисков. Также присутствует информация о суммарной скорости чтения и записи.
- **r = Resources** - Показывает информацию о версии и типе ядра, процессоре, архитектуре компьютера, операционной системе и ее версии.
- **k = Kernel** - Показывает информацию о ядре в виде таблицы, запущенных очередях, форках, прерываниях, переключениях. Также показывает среднюю нагрузку, холостой ход, длительность полной работы системы и средней нагрузки ядра на процессор.
- **j = Filesystems** - Показывает информацию о файловой системе в виде таблицы, имя раздела (путь к папке), полный размер (MB),

свободное и занятое место (MB), тип файловой системы и точка монтирования.

- **n = Network** - Показывает информацию о сетевых интерфейсах, количестве и размеру отправленных/полученных пакетов, также уведомляет об сетевых ошибках в виде аккуратной таблицы.
- **N = NFS** - Показывает информацию о сетевой файловой системе (NetworkFileSystem), загруженности сети, клиентом и сервером, в моем случае NFS версии 2 и 3.
- **t = Top processes** - Показывает список процессов в виде таблицы (очень похоже на команду top), столбцы: PID процесса, нагрузка на процессор, количество занятой оперативной памяти и т. д.
- **V = Virtual memory** - Показывает информацию о виртуально памяти, в частности о разделе подкачки.
- **v = Verbose hints** - Показывает информацию о ресурсах в плане безопасности, степень предупреждения и опасности (в процентах).
- **l = CPU long-term** - Показывает наглядный график загруженности процессора.

vmstat

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

vmstat – утилита для определения производительности системы. Она является эффективным средством для оценки необходимого объема ресурсов, предоставляя информацию о загруженности процессора, интенсивности операций дискового ввода-вывода и использовании оперативной памяти.

Устанавливается командой (если утилита не установлена):

```
sudo dnf install sysstat
```

Простой запуск без ключей будет выглядеть так:

```
vmstat
```

```
[root@localhost user]# vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0  36068 177128  13656 353808    0   66  1676   291  214  395  6  3 86  6  0
```

Значения каждой колонки:

Procs

- **r**: количество запущенных процессов (работающих или ожидающих выполнения).
- **b**: количество спящих процессов.

Memory

- **swpd**: объем используемой виртуальной памяти.
- **free**: объем свободной памяти.
- **buff**: количество памяти, используемой в качестве буферов.
- **cache**: объем памяти, используемой в качестве кеша.
- **inact**: количество неактивной памяти (опция -a).
- **active**: количество активной памяти. (опция -a).

Swap

- **si**: объем памяти, выгруженный с диска (/s).
- **so**: объем памяти, перенесенный на диск (/s).

IO

- **bi**: блоки, полученные от блочного устройства (blocks/s).
- **bo**: блоки, отправленные на блочное устройство (blocks/s).

System

- **in**: количество прерываний в секунду, включая часы.
- **cs**: количество переключений контекста в секунду.

CPU

Здесь проценты от общего времени процессора.

- **us**: время, потраченное на запуск кода, не относящегося к ядру (время пользователя).
- **sy**: время, потраченное на выполнение кода ядра (системное время).
- **id**: время бездействия. До версии Linux 2.5.41 это включает время ожидания ввода-вывода.
- **wa**: время, проведенное в ожидании ввода/вывода
- **st**: время, украденное из виртуальной машины.

Опции vmstat

- **-a** — переключение колонки memory в active/inactive значение вместо buff/cache (active — память, реально используемая в данный момент определённым процессом, inactive — память, выделенная ранее какому-то процессу, которого уже нет);
- **-f** — информация о количестве системных вызовов fork, vfork и rfork, выполненных с момента старта системы, и количество страниц виртуальной памяти, задействованных каждым из них;
- **-m** — использование динамической памяти ядра, выделенной с использованием malloc;
- **-n** — задаёт интервал выполнения в секундах;
- **-s** — изменение вида отображение результатов (в две колонки);
- **-d** — статистика использования дисков;
- **-w** — увеличивает визуальный размер поля для больших объемов;
- **-p** [partition name] — с указанием имени раздела, информация по конкретном разделу (read/writes);
- **-t** – добавляление временной метки к каждой выходной строке;
- **-d** – отображение статистики диска
- **-D** – сделать отчет об активности диска;
- **-S [k | K | m | M]** — с указанием в чем выводить информацию (килобиты, килобайты, мегабиты, мегабайты соответственно);
- **-V** — версия vmstat. Кроме того, после указания опций можно задать две цифры — интервал между выполнением, и количество повторов:

```
vmstat 2 5 -t
```

```
[root@localhost user]# vmstat 2 5 -t
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu----- -----timestamp-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st                 MSK
 2  0   9464  87188  19860 403008    0   13   991    51  125  275  2  2 92  5  0 2021-05-11 10:54:49
 0  0   9464  87156  19860 403008    0    0     0    78  111  239  1  1 98  0  0 2021-05-11 10:54:51
 1  0   9464  87156  19868 403008    0    0     0    22   75  125  1  1 97  2  0 2021-05-11 10:54:53
 0  0   9464  87164  19868 403008    0    0     0     0   71  151  1  0 99  0  0 2021-05-11 10:54:55
 0  0   9464  87196  19868 403008    0    0     0     0   69  130  1  0 99  0  0 2021-05-11 10:54:57
```

vmstat выполнен 5 раз с интервалом в 2 секунды.

dstat

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

dstat - инструмент для мониторинга состояния системы.

Установка в РЕД ОС 7.3:

```
dnf install dstat
```

Использование.

Отображение информации по процессу и статистики записи/чтения на диски:

```
python3 /usr/bin/dstat -s -d -top-bio
```

Пример по использованию памяти:

```
python3 /usr/bin/dstat -g -l -m -s -top-mem
```

Потребление ресурсов процессора:

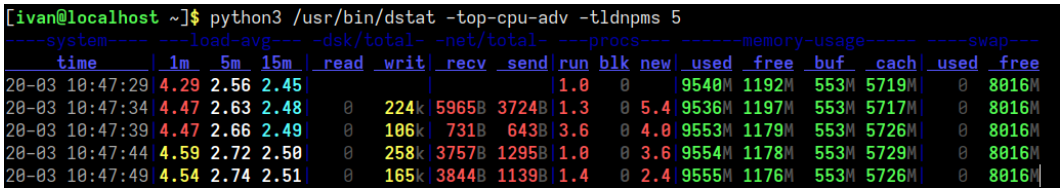
```
python3 /usr/bin/dstat -c -y -l -proc-count -top-cpu
```

или

```
python3 /usr/bin/dstat -c -top-cpu -d -top-bio -top-latency
```

Еще одна комбинация:

```
python3 /usr/bin/dstat -top-cpu-adv -tldnpms 5
```



Описание параметров:

- **l** - средняя загрузка системы;
- **d** - использования дисков;
- **n** - загрузка сетевых устройств;
- **p** - активность процессов;
- **m** - использование памяти;
- **s** - использование подкачки;
- **5** - интервалов в 5 секунд;
- **t** - вывод текущего времени;
- **-top-cpu-adv** - показать самый "дорогой" процесс ввода-вывода (включая pid и другую статистику).

SysMonTask - диспетчер задач РЕД ОС

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: SysMonTask - 1.3.9-2

SysMonTask — утилита, которая в режиме реального времени предоставляет информацию о процессах, выполняемых на компьютере, а также используемых ими ресурсах (об оперативной памяти, процессоре и др.).

SysMonTask имеет схожий с диспетчером задач Windows интерфейс.

Вы можете подробнее ознакомиться с работой диспетчера задач **SysMonTask**, просмотрев наши обучающие видео:

- на **RuTube** — Альтернативный диспетчер задач в РЕД ОС. Sysmontask;
- в **Яндекс.Дзен** — Альтернативный диспетчер задач в РЕД ОС. Sysmontask;
- в **VK Видео** — Альтернативный диспетчер задач в РЕД ОС. Sysmontask.

На наших каналах вы также сможете найти много другой полезной информации.

Установка SysMonTask

Для установки **SysMonTask** используется команда:

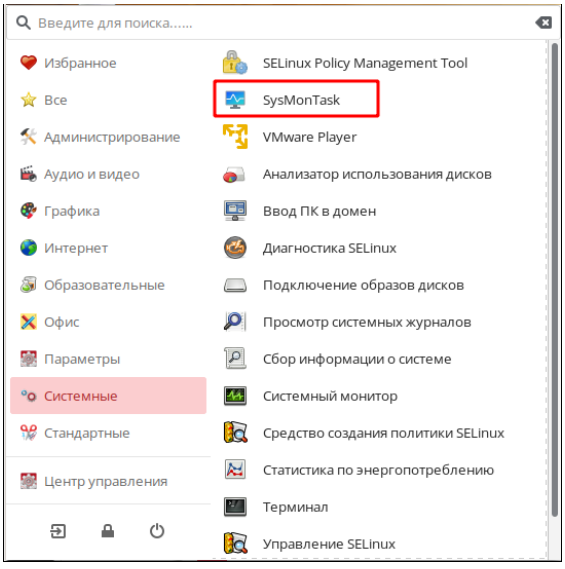
```
dnf install sysmontask
```

Использование SysMonTask

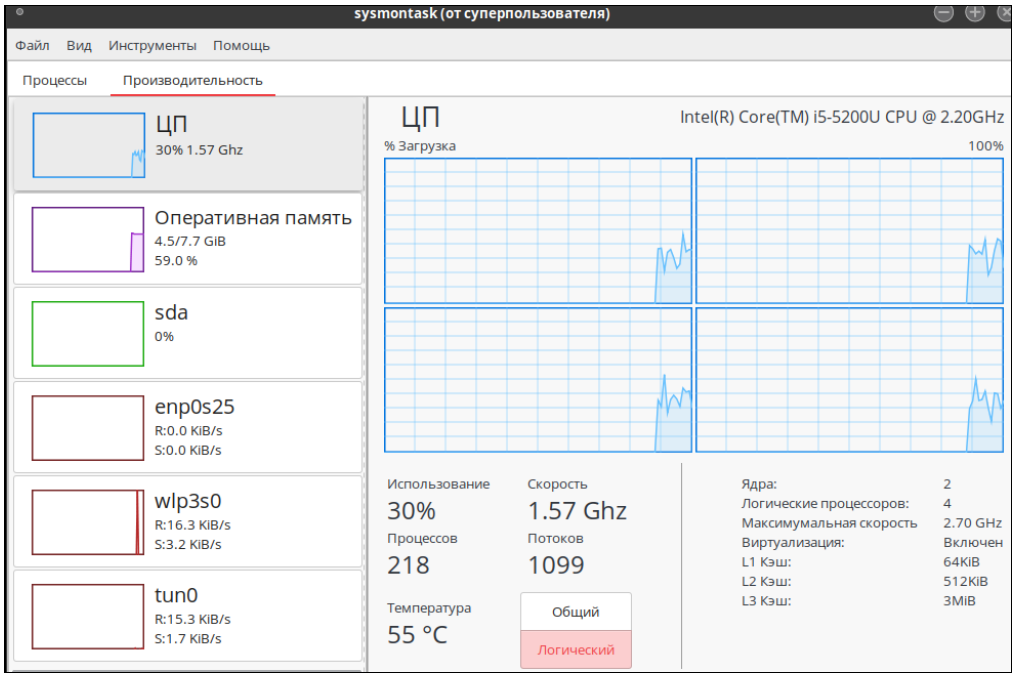
SysMonTask можно открыть из терминала командой:

```
sysmontask
```

или через пользовательский интерфейс из пункта меню «**Системные**».

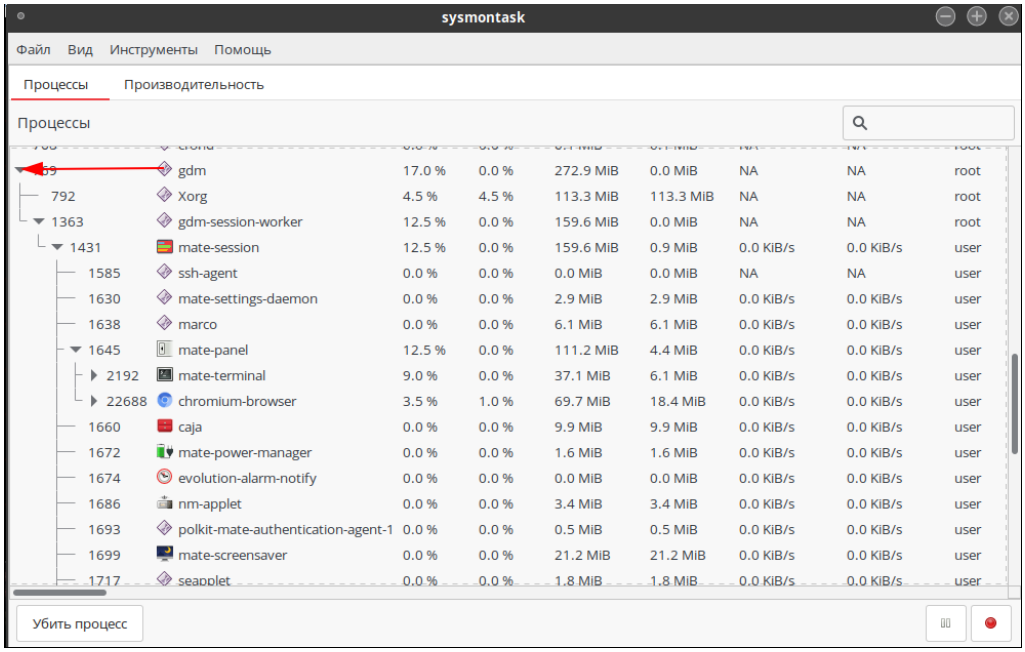


Во вкладке «**Производительность**» отображается общее потребление аппаратных ресурсов:



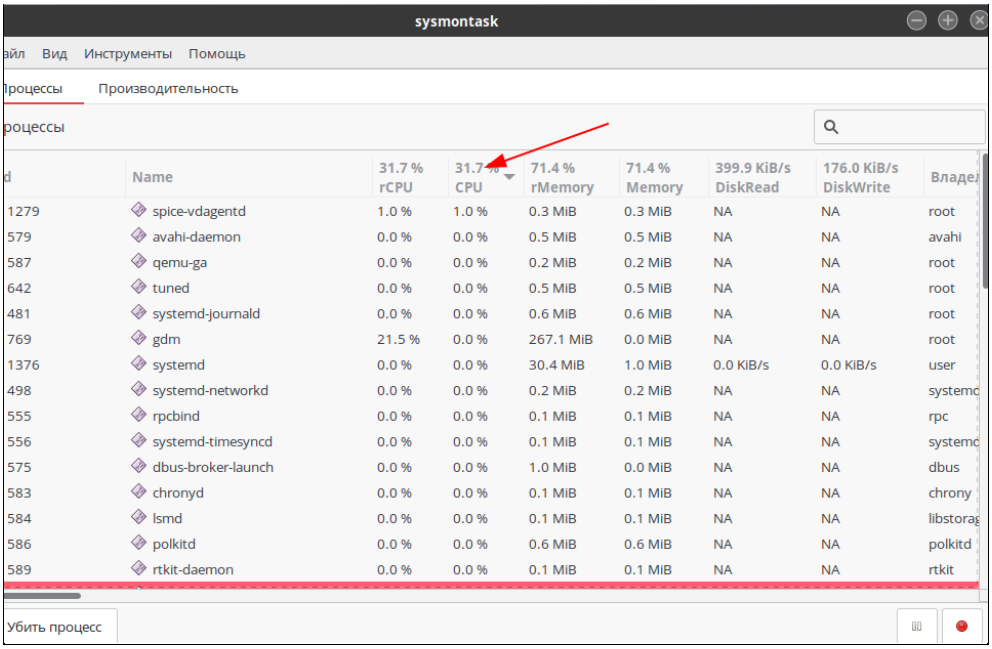
Во вкладке «**Процессы**» отображаются все выполняющиеся в данный момент процессы.

Если вы не находите какой-либо процесс, то скорее всего он является подпроцессом, чтобы его увидеть, необходимо развернуть дерево процессов.

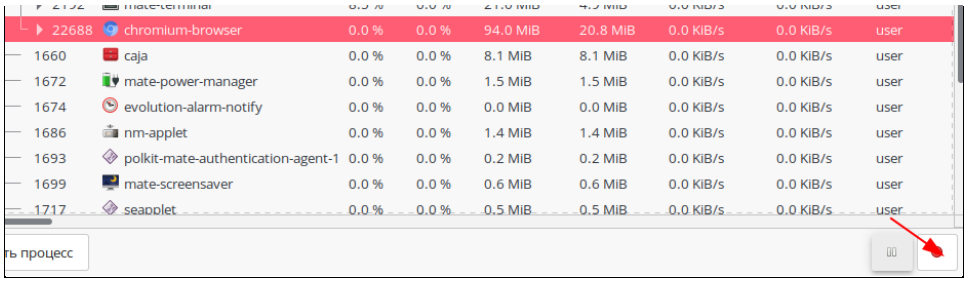


Кнопка «**Убить процесс**» завершает выбранный процесс.

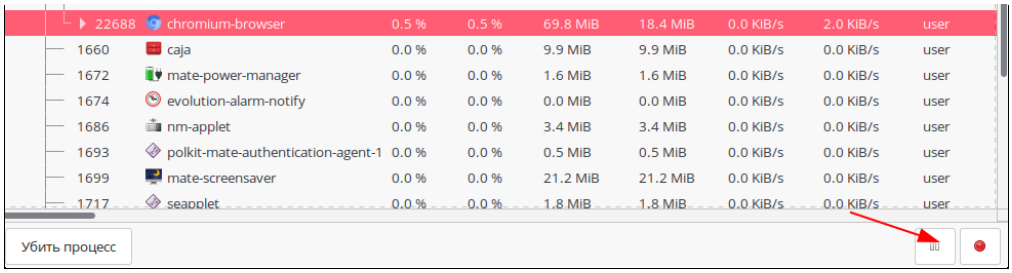
Чтобы отсортировать процессы по какому-либо параметру, необходимо нажать на заголовок столбца:



SysMonTask позволяет записывать потребление ресурсов, для этого необходимо нажать на кнопку записи в правом нижнем углу окна.



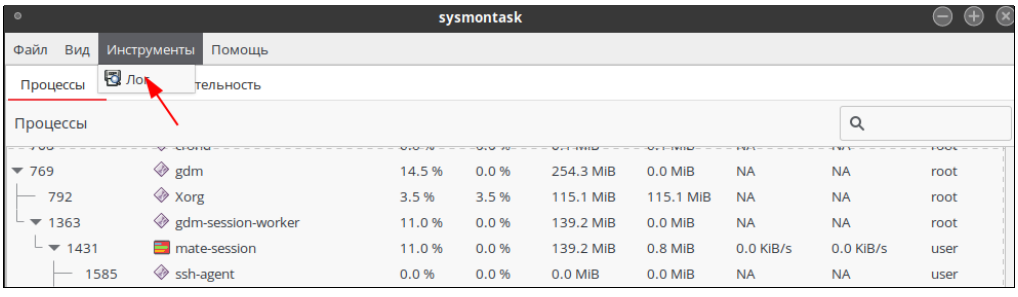
Запись можно приостановить нажав на кнопку паузы в правом нижнем углу окна.



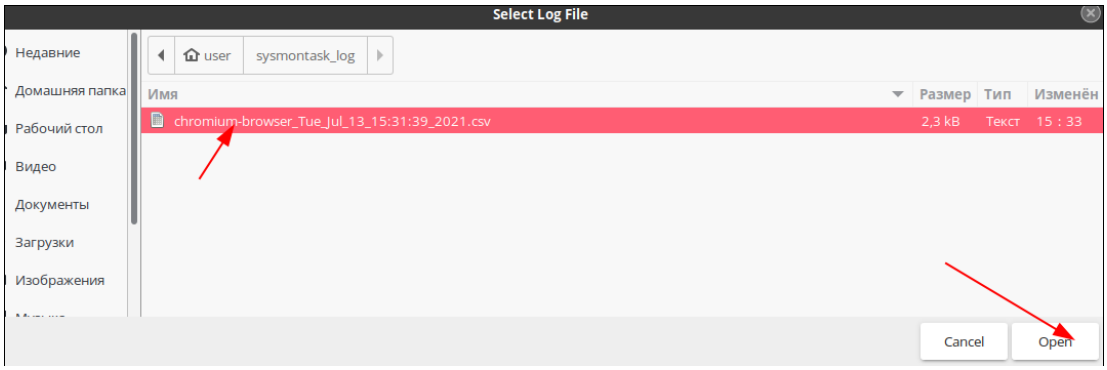
Для того чтобы просмотреть запись, должна быть установлена библиотека **matplotlib**, для этого используем следующую команду:

```
pip3 install matplotlib
```

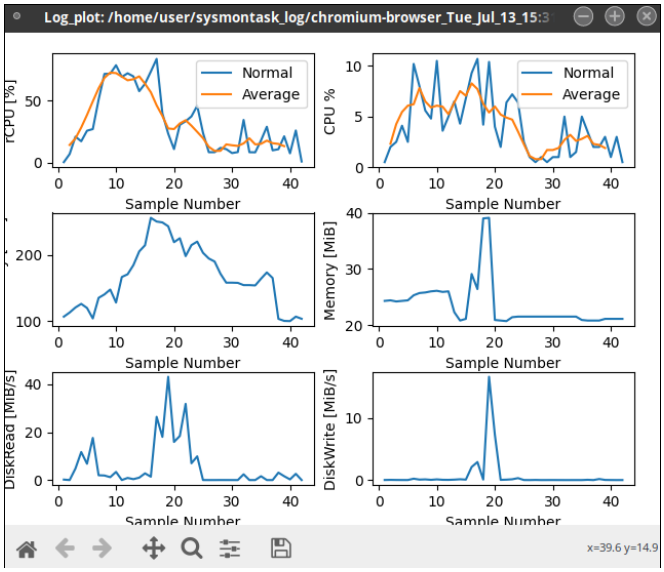
Далее в **SysMonTask** для открытия записи необходимо в меню «**Инструменты**» выбрать «**Лог**».



Выбираем нужную запись и нажимаем «**Открыть**»:

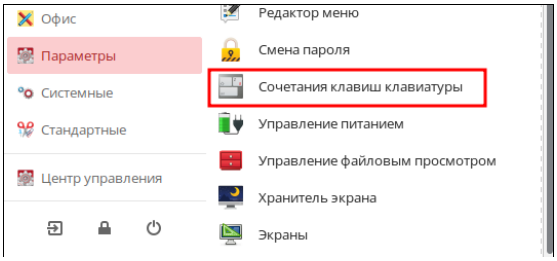


В результате отобразится график использования ресурсов.



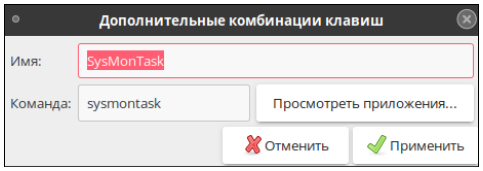
Можно настроить вызов **SysMonTask** с помощью сочетания клавиш «**Ctrl+Alt+Delete**», как в Windows.

Для этого в меню «**Параметры**» выбираем «**Сочетания клавиш клавиатуры**».

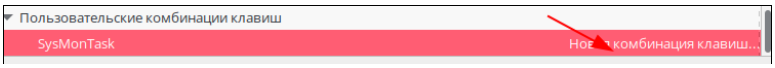


Нажимаем кнопку «**Добавить**».

Вписываем имя процедуры и команду «**sysmontask**», затем «**Применить**».



Далее выбираем поле «**Сочетание клавиш**» напротив **SysMonTask**:



И нажимаем «**Ctrl+Alt+Delete**».

Systemd-analyze - анализ системных процессов

Systemd-analyze — утилита, которая используется для просмотра отчетов о производительности системы. С помощью **systemd-analyze** можно получить информацию о том, сколько времени потребовалось для загрузки системы, а также сколько времени потребовалось для запуска каждого модуля.

Для просмотра информации о количестве времени, которое затрачивается при загрузке системы с разбивкой на ядро и пользовательское пространство, необходимо выполнить следующую команду:

```
systemd-analyze

Startup finished in 1.557s (kernel) + 4.996s (initrd) + 45.794s (userspace) = 52.348s
graphical.target reached after 45.780s in userspace
```

Также можно просмотреть подробную информацию о затраченном времени каждым блоком (процессом) в отдельности, для этого используется следующая команда:

```
systemd-analyze blame

25.298s plymouth-quit-wait.service
17.432s dnf-makecache.service
15.769s accounts-daemon.service
13.800s udisks2.service
 9.440s postfix.service
 5.744s vmware.service
 5.604s initrd-switch-root.service
 4.708s NetworkManager-wait-online.service
 4.668s systemd-udev-settle.service
 3.925s avahi-daemon.service
 3.546s lvm2-monitor.service
 3.343s lm_sensors.service
 3.108s smartd.service
 2.957s usbsrvd.service
 2.721s sshd.service
 2.216s ModemManager.service
 2.212s NetworkManager.service
 2.143s chronyd.service
 1.830s systemd-homed.service
 1.826s sysstat.service
 1.814s systemd-logind.service
 1.789s upower.service
 1.596s rtkit-daemon.service
 ...
```

С помощью полученной информации можно оптимизировать время загрузки системы. Список отсортирован по затраченному времени в порядке убывания.

Так как список процессов может быть довольно большим, существует возможность отсортировать вывод при помощи команды head (обычно первых 10 записей достаточно, чтобы найти требующие большого количества времени службы):

```
systemd-analyze blame | head
```

Также можно просмотреть подробную информацию в виде дерева критической по времени цепочки событий. Для этого необходимо выполнить команду:

```
systemd-analyze critical-chain

The time when unit became active or started is printed after the "@" character.
The time the unit took to start is printed after the "+" character.

graphical.target @45.780s
└─multi-user.target @45.780s
  └─plymouth-quit-wait.service @20.481s +25.298s
    └─systemd-user-sessions.service @20.211s +156ms
      └─remote-fs.target @20.176s
        └─remote-fs-pre.target @20.176s
          └─nfs-client.target @16.448s
            └─gssproxy.service @15.158s +1.266s
              └─network.target @15.140s
                └─wpa_supplicant.service @42.982s +143ms
                  └─basic.target @11.186s
```

```
└─dbus-broker.service @10.563s +618ms
  └─dbus.socket @10.556s
    └─sysinit.target @10.548s
      └─systemd-userdbd.service @31.778s +78ms
        └─systemd-userdbd.socket @4.150s
          └─system.slice
            └─-.slice
```

В выводе можно увидеть цепочку событий, отсортированных по времени (когда служба стала активной) в порядке убывания.

Значение после символа «**@**» в каждом событии - это время, когда служба стала активной.

Значение после символа «**+**» в каждом блоке показывает время, которое потребовалось для запуска службы.

Из полученной выше информации можно установить, какие службы запускаются дольше и, в свою очередь, вызывают медленную загрузку системы.

Такие службы можно отключить, если они не требуются для запуска при загрузке. Кроме того, можно отключить все службы, которые занимают меньше времени, но не требуются при загрузке, поскольку они также влияют на время загрузки системы.

Для того чтобы отключить какую-либо службу, необходимо выполнить следующую команду:

```
systemctl disable <имя_службы>
```

Systemd-analyze также позволяет получить и другие данные о состоянии и трассировке системы. Для ознакомления с дополнительной информацией о работе с утилитой и ее возможностях просмотрите справку:

```
man systemd-analyze
```

Pidstat — утилита для мониторинга и отчётности по статистике производительности процессов

Установка
Синтаксис
Параметры
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: sysstat-12.3.1-1, sysstat-12.5.4-4

Pidstat (Process ID Statistic) — утилита, используемая для мониторинга и отчётности по статистике производительности процессов. Она может контролировать либо конкретный процесс, либо все запущенные процессы в системе.

Установка

Утилита **pidstat** входит в пакет **sysstat**, для установки выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install sysstat
```

Дальнейшая работа в программе производится с правами непривилегированного пользователя. Для получения дополнительной информации выполните команду:

```
man pidstat
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
pidstat [<параметры> ] [ <интервал> [ <счётчик> ] ] [ -e <программа> <аргументы> ]
```

Параметры

Основные параметры утилиты:

-d — вывод статистики ввода вывода;

-H — отображение статистики ввода/вывода с использованием удобного формата;

-h — справка;

-I — статистика прерываний;

-l — вывод пути до программы.

-R — статистика страниц памяти;

-r — вывод статистики сбоя страниц и использования памяти;

-s — статистика операций записи;

-t — статистика по зависимым процессам в формате дерева;

-U [<имя_пользователя>] — статистика процессов, принадлежащих указанному пользователю;

-u — статистика процессов в режиме пользователя;

-V — версия программы;

-v — вывод подробной статистики процессов;

-w — статистика процессов, которые находятся в состоянии ожидания;

-C <команда> — статистика процессов, запущенных с указанной командой;

-G <имя_процесса> — вывод статистики по имени процесса;

-p { <идентификатор_процесса> [,...] | SELF | ALL } — вывод статистики для выбранного процесса;

-T { TASK | CHILD | ALL } — статистика процессов в зависимости от типа (задача, дочерний процесс или все процессы);

--dec={ 0 | 1 | 2 } — устанавливает формат вывода чисел (0 - по умолчанию, 1 - с запятой, 2 - с точкой);

--human — вывод статистики в удобном формате.

Пример работы

1. Команда для вывода статистики по всем процессам:

```
pidstat -p ALL
```

Результат:

```
[user@localhost ~]$ pidstat -p ALL
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:48:51      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:48:51        0         1    0,03    0,03    0,00    0,02    0,06     1  systemd
23:48:51        0         2    0,00    0,00    0,00    0,00    0,00     1  kthreadd
23:48:51        0         3    0,00    0,00    0,00    0,00    0,00     0  pool_workqueue_release
23:48:51        0         4    0,00    0,00    0,00    0,00    0,00     0  kworker/R-rcu_g
23:48:51        0         5    0,00    0,00    0,00    0,00    0,00     0  kworker/R-rcu_p
23:48:51        0         6    0,00    0,00    0,00    0,00    0,00     0  kworker/R-slub_
23:48:51        0         7    0,00    0,00    0,00    0,00    0,00     0  kworker/R-netns
23:48:51        0        10    0,00    0,00    0,00    0,00    0,00     0  kworker/0:0H-events_highpri
23:48:51        0        11    0,00    0,00    0,00    0,00    0,00     0  kworker/u4:0-ext4-rsv-conversion
23:48:51        0        12    0,00    0,00    0,00    0,00    0,00     0  kworker/R-mm_pe
23:48:51        0        13    0,00    0,00    0,00    0,00    0,00     0  rcu_tasks_kthread
23:48:51        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:48:51        0        15    0,00    0,00    0,00    0,00    0,00     0  rcu_tasks_trace_kthread
23:48:51        0        16    0,00    0,00    0,00    0,00    0,00     0  ksoftirqd/0
23:48:51        0        17    0,00    0,01    0,00    0,05    0,01     0  rcu_preempt
23:48:51        0        18    0,00    0,00    0,00    0,00    0,00     0  migration/0
23:48:51        0        19    0,00    0,00    0,00    0,00    0,00     0  idle_inject/0
```

где:

- **UID** — идентификатор пользователя, от имени которого работает процесс;
- **PID** — идентификационный номер отслеживаемой задачи (процесса);
- **%usr** — процент ресурсов процессора, затраченных на выполнение пользовательских приложений;
- **%system** — процент ресурсов процессора, затраченных выполнение системных задач;
- **%guest** — процент ресурсов процессора, затраченных на работу виртуального процессора;
- **%wait** — процент ресурсов процессора, израсходованных задачей во время ожидания запуска;
- **%CPU** — общий процент процессорного времени, используемого задачей;
- **CPU** — номер процессора, к которому привязана задача;
- **Command** — имя команды процесса.

2. Вывод статистики о работе определённого процесса 6 раз каждые 5 секунд:

```
pidstat -p 14 5 6
```

Результат:

```
[user@localhost ~]$ pidstat -p 14 5 6
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:51:59      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:52:04        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:09        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:14        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:19        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:24        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
23:52:29        0        14    0,00    0,00    0,00    0,00    0,00     1  rcu_tasks_rude_kthread
Среднее:        0        14    0,00    0,00    0,00    0,00    0,00     -  rcu_tasks_rude_kthread
```

3. Вывод статистики процесса по имени:

```
pidstat -C 'kworker'
```

Результат:

```
[user@localhost ~]$ pidstat -C 'kworker'
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:58:03      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:58:03        0        11    0,00    0,00    0,00    0,00    0,00     0  kworker/u4:0-ext4-rsv-conversion
23:58:03        0        28    0,00    0,00    0,00    0,00    0,00     1  kworker/u6:0-events_unbound
23:58:03        0        53    0,00    0,00    0,00    0,00    0,00     0  kworker/0:1H-kblockd
23:58:03        0        67    0,00    0,02    0,00    0,01    0,02     1  kworker/1:2-events
23:58:03        0       221    0,00    0,00    0,00    0,00    0,00     1  kworker/1:1H-kblockd
23:58:03        0       448    0,00    0,01    0,00    0,02    0,01     0  kworker/0:5-events
23:58:03        0      2452    0,00    0,00    0,00    0,00    0,00     1  kworker/u5:4-flush-8:0
23:58:03        0      2512    0,00    0,00    0,00    0,00    0,00     0  kworker/u5:0-events_unbound
23:58:03        0      2658    0,00    0,00    0,00    0,00    0,00     1  kworker/u6:3-flush-8:0
23:58:03        0      3138    0,00    0,00    0,00    0,00    0,00     1  kworker/1:0-ata_sff
```

4. Статистика ввода-вывода (I/O) для процесса с PID 14, обновляемая каждую секунду:

```
pidstat -p 14 -d 1
```

Результат:

```
[user@localhost ~]$ pidstat -p 14 -d 1
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     11.08.2024      _x86_64_        (2 CPU)

23:59:57      UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
23:59:58        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
23:59:59        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:00        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:01        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:02        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:03        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:04        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:05        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
00:00:06        0        14     -1,00     -1,00     -1,00       0  rcu_tasks_rude_kthread
```

где:

- **kB_rd/s** — скорость (КБ в секунду), с которой процесс читает с диска;
- **kB_wr/s** — скорость (КБ в секунду), с которой процесс записывает на диск;
- **kB_ccwr/s** — скорость (КБ в секунду), с которой запись на диск была отменена процессом;
- **Iodelay** — задержка ввода/вывода блока контролируемого процесса, измеряемая в тактах.

5. Сбор и вывод статистики по свободной и занятой памяти:

```
pidstat -p 14 -r 1
```

Результат:

```
[user@localhost ~]$ pidstat -p 14 -r 1
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:02:25      UID       PID  minflt/s  majflt/s     VSZ     RSS   %MEM  Command
00:02:26        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:27        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:28        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:29        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:30        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:31        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:32        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:33        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:34        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:35        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:36        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
00:02:37        0        14      0,00      0,00       0       0   0,00  rcu_tasks_rude_kthread
```

где:

- **minflt/s** — общее количество незначительных ошибок, совершенных процессом за секунду, которые не требовали загрузки страницы памяти с диска;
- **majflt/s** — общее количество значительных ошибок, совершенных процессом за секунду, которые требовали загрузки страницы памяти с диска;
- **VSZ** — виртуальная память (КБ), используемая задачей;
- **RSS** — физическая память (КБ), используемая задачей;
- **%MEM** — процент доступной физической памяти, используемой процессором.

6. Вывод статистики производительности всех процессов, имя которых содержит org_kde_powerde (заменить на необходимое):

```
pidstat -C org_kde_powerde -l
```

Результат:

```
[user@localhost ~]$ pidstat -C org_kde_powerde -l
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:19:30      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
00:19:30     1000      2368    0,01    0,01    0,00    0,05    0,02     0  /usr/libexec/org_kde_powerdevil
[user@localhost ~]$ pidstat -C dnfdragora-upda -l
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:20:45      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
00:20:45     1000      2169    0,02    0,01    0,00    0,02    0,03     1  /usr/bin/python3 /usr/bin/dnfdragora-updater --qt
```

7. Вывод статистики по родительским и дочерним процессам:

```
pidstat -T CHILD
```

Результат:

```
[user@localhost ~]$ pidstat -T CHILD
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:15:13      UID       PID    usr-ms system-ms  guest-ms  Command
00:15:13        0         1      4900      4870         0  systemd
00:15:13        0        11         0        20         0  kworker/u4:0-ext4-rsv-conversion
00:15:13        0        16         0        40         0  ksoftirqd/0
00:15:13        0        17         0       320         0  rcu_preempt
00:15:13        0        18         0        10         0  migration/0
00:15:13        0        23       140         0         0  migration/1
00:15:13        0        24         0        40         0  ksoftirqd/1
00:15:13        0        37         0        40         0  kcompactd0
00:15:13        0        53         0       110         0  kworker/0:1H-kblockd
00:15:13        0        54         0       100         0  kswapd0
00:15:13        0        67         0      1010         0  kworker/1:2-events
00:15:13        0       221         0        80         0  kworker/1:1H-kblockd
00:15:13        0       301         0        10         0  scsi_eh_1
```

где:

- **usr-ms** — общее количество миллисекунд, затраченных процессом и его производными на пользовательские задачи;

- **system-ms** — общее количество миллисекунд, затраченных процессом и его производными на системные задачи;
- **guest-ms** — общее количество миллисекунд, затраченных процессом и его производными на задачи виртуальной машины.

8. Вывод статистики в формате дерева:

```
pidstat -t
```

Результат:

```
[user@localhost ~]$ pidstat -t
Linux 6.6.26-1.red80.x86_64 (localhost.localdomain)     12.08.2024      _x86_64_        (2 CPU)

00:16:33      UID      TGID       TID    %usr %system  %guest   %wait    %CPU   CPU  Command
00:16:33        0         1         -    0,02    0,02    0,00    0,02    0,04     1  systemd
00:16:33        0         -         1    0,02    0,02    0,00    0,02    0,04     1  |__systemd
00:16:33        0        11         -    0,00    0,00    0,00    0,00    0,00     0  kworker/u4:0-ext4-rsv-conversion
00:16:33        0         -        11    0,00    0,00    0,00    0,00    0,00     0  |__kworker/u4:0-ext4-rsv-conversion
00:16:33        0        16         -    0,00    0,00    0,00    0,00    0,00     0  ksoftirqd/0
00:16:33        0         -        16    0,00    0,00    0,00    0,00    0,00     0  |__ksoftirqd/0
00:16:33        0        17         -    0,00    0,01    0,00    0,05    0,01     0  rcu_preempt
00:16:33        0         -        17    0,00    0,01    0,00    0,05    0,01     0  |__rcu_preempt
00:16:33        0        18         -    0,00    0,00    0,00    0,00    0,00     0  migration/0
00:16:33        0         -        18    0,00    0,00    0,00    0,00    0,00     0  |__migration/0
00:16:33        0        23         -    0,00    0,00    0,00    0,00    0,00     1  migration/1
00:16:33        0         -        23    0,00    0,00    0,00    0,00    0,00     1  |__migration/1
00:16:33        0        24         -    0,00    0,00    0,00    0,00    0,00     1  ksoftirqd/1
00:16:33        0         -        24    0,00    0,00    0,00    0,00    0,00     1  |__ksoftirqd/1
```

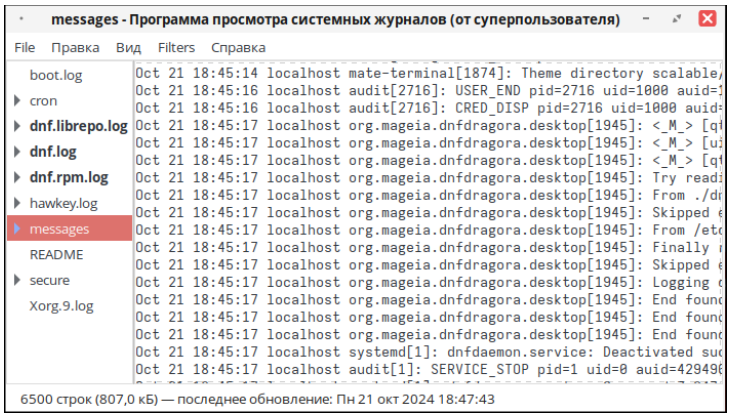
где:

- **TGID** — идентификационный номер главного процесса;
- **TID** — идентификационный номер контролируемого процесса.

Просмотр системных журналов с помощью графического интерфейса

При работе в РЕД ОС **с графической оболочкой MATE** для просмотра системных логов требуется открыть **«Меню» -> «Системные» -> «Просмотр системных журналов»**.

После ввода root-пароля откроется следующее окно:



Здесь можно выбрать нужный вам раздел, также здесь присутствуют фильтры, которые можно настроить под свой запрос:

Утилита tail

tail — это утилита, используемая для вывода N-го количества последних строк файла. Обычно она показывает в стандартном выводе 10 последних строк. Команда tail позволяет также выводить новые строки в интерактивном режиме. Вывод последних 10 строк файла производится следующей командой:

```
tail /var/log/messages
Oct 17 10:42:27 localhost audit[36545]: CRED_ACQ pid=36545 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 res=success'
Oct 17 10:42:27 localhost audit[36545]: USER_START pid=36545 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct="root" exe="/usr/bin/su" hostname=?
addr=? terminal=/dev/pts/0 res=success'
Oct 17 10:42:28 localhost audit: BPF prog-id=90 op=LOAD
Oct 17 10:42:28 localhost audit: BPF prog-id=91 op=LOAD
Oct 17 10:42:28 localhost audit: BPF prog-id=92 op=LOAD
Oct 17 10:42:28 localhost systemd[1]: Starting systemd-hostnamed.service - Hostname Service...
Oct 17 10:42:28 localhost systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Oct 17 10:42:28 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=systemd-hostnamed comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
```

Увеличить количество выводимых строк можно с помощью опции -n:

```
tail -n 100 /var/log/messages
Oct 17 10:45:27 localhost NetworkManager[573]: <info>  [1729151127.7574] dhcp4 (ens3): state changed new lease,
address=192.168.122.49
Oct 17 10:45:27 localhost systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
Oct 17 10:45:27 localhost systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Oct 17 10:45:27 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=NetworkManager-dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Oct 17 10:45:37 localhost systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
```

Для просмотра логов в реальном времени используется опция -f:

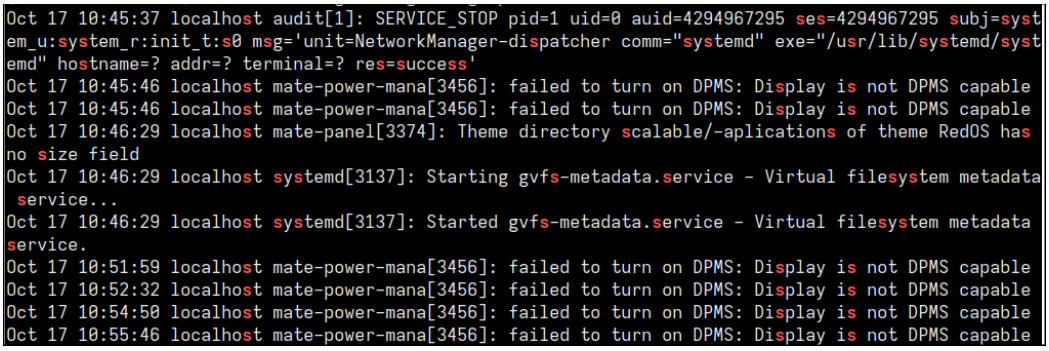
```
tail -f /var/log/messages
Oct 17 10:45:27 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=NetworkManager-dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Oct 17 10:45:37 localhost systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Oct 17 10:45:37 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=NetworkManager-dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Oct 17 10:45:46 localhost mate-power-mana[3456]: failed to turn on DPMS: Display is not DPMS capable
Oct 17 10:45:46 localhost mate-power-mana[3456]: failed to turn on DPMS: Display is not DPMS capable
Oct 17 10:46:29 localhost mate-panel[3374]: Theme directory scalable/-aplications of theme RedOS has no size field
Oct 17 10:46:29 localhost systemd[3137]: Starting gvfs-metadata.service - Virtual filesystem metadata service...
Oct 17 10:46:29 localhost systemd[3137]: Started gvfs-metadata.service - Virtual filesystem metadata service.
```

Вы можете открыть несколько файлов одновременно, перечислив их в параметрах:

```
tail /var/log/messages /var/log/Xorg.9.log
==> /var/log/messages <==
Oct 17 10:45:27 localhost systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service...
Oct 17 10:45:27 localhost systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
Oct 17 10:45:27 localhost audit[1]: SERVICE_START pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=NetworkManager-dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Oct 17 10:45:37 localhost systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Oct 17 10:45:37 localhost audit[1]: SERVICE_STOP pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=NetworkManager-dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
Oct 17 10:45:46 localhost mate-power-mana[3456]: failed to turn on DPMS: Display is not DPMS capable
...
==> /var/log/Xorg.9.log <==
[    17.563] (II) This device may have been added with another device file.
[    72.903] (II) event0  - Power Button: device removed
[    72.905] (II) event2  - QEMU QEMU USB Tablet: device removed
[    72.914] (II) event1  - AT Translated Set 2 keyboard: device removed
[    72.917] (II) event3  - ImExPS/2 Generic Explorer Mouse: device removed
[    72.930] (II) UnloadModule: "libinput"
[    72.930] (II) UnloadModule: "libinput"
[    72.930] (II) UnloadModule: "libinput"
[    72.930] (II) UnloadModule: "libinput"
[    72.939] (II) Server terminated successfully (0). Closing log file.
```

Для удобства, вы можете выбирать не все строки, а отфильтровать интересующие вас с помощью опции grep:

```
tail /var/log/messages | grep s
```



Основные опции tail

- ***-c*** - выводить указанное количество байт с конца файла;
- ***-f*** - обновлять информацию по мере появления новых строк в файле;
- ***-n*** - выводить указанное количество строк из конца файла;
- ***--pid*** - используется с опцией -f, позволяет завершить работу утилиты, когда завершится указанный процесс;
- ***-q*** - не выводить имена файлов;
- ***--retry*** - повторять попытки открыть файл, если он недоступен;
- ***-v*** - выводить подробную информацию о файле.

Утилита less

less — утилита командной строки, которая отображает содержимое файла или вывод команды по одной странице за раз.

Открыть содержимое файла можно следующей командой:

```
less /var/log/Xorg.9.log

 X.Org X Server 1.20.14
 X Protocol Version 11, Revision 0
 [    10.002] Current Operating System: Linux localhost.localdomain 6.6.6-1.red80.x86_64 #1 SMP PREE
 MPT_DYNAMIC Tue Dec 12 00:01:24 MSK 2023 x86_64
 [    10.002] Kernel command line: BOOT_IMAGE=/vmlinuz-6.6.6-1.red80.x86_64 root=UUID=5b25f5f1-2ee8-4ee2-8b0d- 524f3cde5e1e ro
resume=UUID=cd77454c-60a6-4495-98e2-568a5279db77 rhgb quiet
 [    10.002] Build Date: 13 December 2023  12:00:00AM
 [    10.002] Build ID: xorg-x11-server 1.20.14-11.red80
 [    10.002] Current version of pixman: 0.40.0
 [    10.002]    Before reporting problems, check http://wiki.x.org
        to make sure that you have the latest version.
 [    10.002] Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
 [    10.002] (==) Log file: "/var/log/Xorg.9.log", Time: Fri Sep 27 15:27:09 2024
 [    10.719] (==) Using config directory: "/etc/X11/xorg.conf.d"
 [    10.719] (==) Using system config directory "/usr/share/X11/xorg.conf.d"
 [    10.773] (==) No Layout section.  Using the first Screen section.
 [    10.773] (==) No screen section available. Using defaults.
...
```

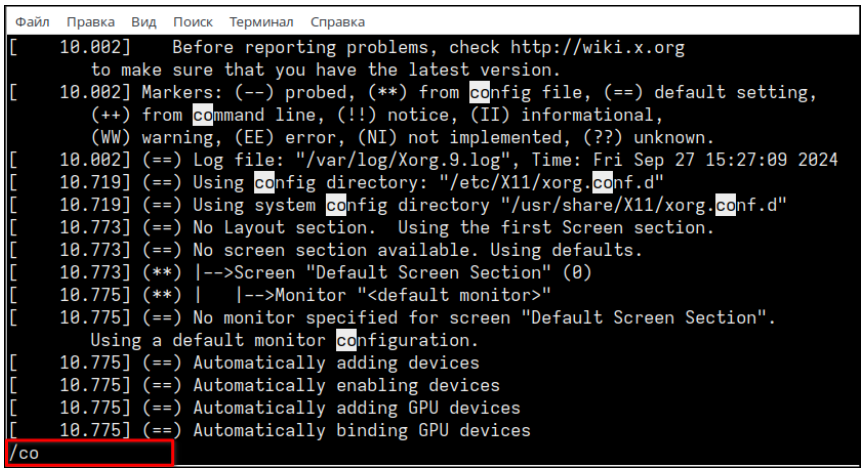
Командная строка исчезнет, а в окне терминала откроется указанный вами документ. После этого его можно читать, пользуясь для прокручивания строк вперед и назад клавишами **Enter** и **Y**.

Внизу окна вы увидите поле с мигающим курсором — здесь можно напечатать какую-либо внутреннюю команду, например, задать утилите паттерн поиска.

Для открытия файла могут задаваться определённые опции, их список представлен ниже:

- ***-a*** — не осуществлять поиск в тексте, который в данный момент отображен на экране;
- ***-bn*** — задать размер буфера памяти;
- ***-c*** — листать текст, полностью стирая содержимое экрана (построчная прокрутка работать не будет);
- ***-Dxcolor*, *--color=xcolor*** — задать цвет отображаемого текста;
- ***-E*** — выйти, когда утилита достигнет конца файла;
- ***-e*** — выйти, когда утилита второй раз достигнет конца файла;
- ***-F*** — выйти, если содержимое файла помещается на одном экране;
- ***-f*** — открыть специальный файл;
- ***-hn*** — задать максимальное количество строк для прокрутки назад;
- ***-yn*** — задать максимальное количество строк для прокрутки вперёд;
- ***-i*** — игнорировать регистр;
- ***-I*** — игнорировать регистр, даже если паттерн для поиска содержит заглавные буквы;
- ***-jn*** — указать, в какой строке должна быть выведена искомая информация;
- ***-J*** — пометить строки, соответствующие результатам поиска;
- ***-n*** — не выводить номера строк;
- ***-N*** — вывести номера строк;
- ***-s*** — заменить множество идущих подряд пустых строк одной пустой строкой;
- ***-w*** — выделить первую строку нового фрагмента текста.

Если вам нужно найти то или иное слово, напечатайте в поле с мигающим курсором **/текст** (для поиска вниз по тексту) или **?текст** (для поиска вверх по тексту) и нажмите **Enter**:

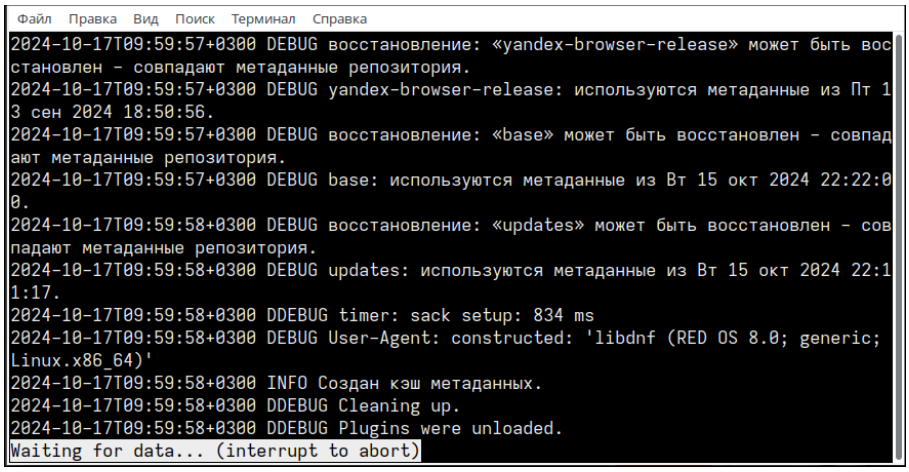


Less позволяет просматривать одновременно несколько файлов, переключаясь между ними, для этого нужно после команды less написать название двух файлов, чтобы просмотреть следующий файл, нажмите «:», а затем нажмите «n»:

```
less /var/log/Xorg.9.log /var/log/messagesSep 27 15:57:17 localhost kernel: Kernel command line: BOOT_IMAGE=/vmlinuz-6.6.34-
1.red80.x86_64 root>
Sep 27 15:57:17 localhost kernel: Unknown kernel command line parameters "rhgb BOOT_IMAGE=/vmlinuz-6.>
Sep 27 15:57:17 localhost kernel: random: crng init done
Sep 27 15:57:17 localhost kernel: Dentry cache hash table entries: 262144 (order: 9, 2097152 bytes, l>
Sep 27 15:57:17 localhost kernel: Inode-cache hash table entries: 131072 (order: 8, 1048576 bytes, li>
Sep 27 15:57:17 localhost kernel: Fallback order for Node 0: 0
Sep 27 15:57:17 localhost kernel: Built 1 zonelists, mobility grouping on. Total pages: 515808
Sep 27 15:57:17 localhost kernel: Policy zone: DMA32
Sep 27 15:57:17 localhost kernel: mem auto-init: stack:off, heap alloc:on, heap free:off
Sep 27 15:57:17 localhost kernel: Memory: 1988372K/2096632K available (18432K kernel code, 3220K rwda>
Sep 27 15:57:17 localhost kernel: SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=2, Nodes=1
Sep 27 15:57:17 localhost kernel: ftrace: allocating 51756 entries in 203 pages
Sep 27 15:57:17 localhost kernel: ftrace: allocated 203 pages with 5 groups
Sep 27 15:57:17 localhost kernel: Dynamic Preempt: voluntary
```

Для просмотра содержимого файла изменений в режиме реального времени используется опция +F:

```
less +F /var/log/dnf.log
```



При открытии файла с большим количеством текста в нём могут встречаться множество идущих подряд пустых строк. При открытии файла с опцией -s, множество пробелов сокращается до одного пробела между строками:

```
less -s /var/log/dnf.log
```

Во время просмотра содержимого файла утилитой можно управлять при помощи внутренних команд, набирая их на клавиатуре. Наиболее часто используемые из них:

- ***h, H*** — справка;
- ***Space, Ctrl+V, f, Ctrl+F*** — прокрутить текст на один экран вперёд;
- ***Enter, Return, Ctrl+N, e, Ctrl+E, j, Ctrl+J*** — прокрутить текст на n строк вперед, по умолчанию n=1;
- ***y, Ctrl+Y, Ctrl+P, k, Ctrl+K*** — прокрутить текст на n строк назад, по умолчанию n=1;
- ***Ctrl+→*** — прокрутить текст по горизонтали в конец строки;

- ***Ctrl+←*** — прокрутить текст по горизонтали в начало строки;
- ***:d*** — удалить текущий файл из списка файлов;
- ***Ctrl+G, :f*** — вывести основную информацию о файле;
- ***q, Q, :q, :Q, ZZ*** — выход.

Настройка журналов с помощью утилиты journalctl

Ограничение размера журнала
Удаление журналов
Вывод лога в текстовый файл
Фильтрация по приоритету
Сокращение или расширение области вывода
Запись логов в стандартный вывод
Справка по утилите

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Вы можете подробнее ознакомиться с работой утилиты **journalctl**, просмотрев наши обучающие видео:

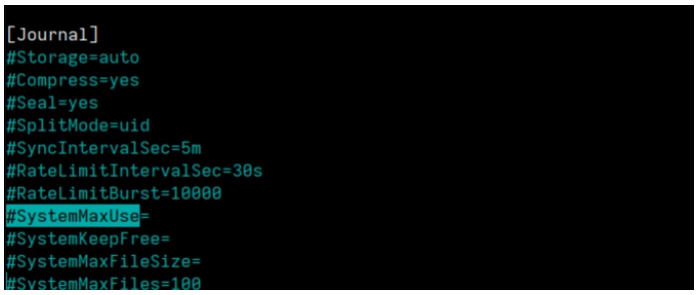
- на **RuTube** — Работа с журналами в РЕД ОС. Journalctl;
- в **Яндекс.Дзен** — Работа с журналами в РЕД ОС. Journalctl;
- в **VK Видео** — Работа с журналами в РЕД ОС. Journalctl.

На наших каналах вы также сможете найти много другой полезной информации.

Ограничение размера журнала

Если **journald** настроен, чтобы сохранять журналы после перезагрузки, то по умолчанию размер журнала ограничен 10% от объема файлового раздела и максимально может занять 4 Гб дискового пространства.

Максимальный объем журнала можно скорректировать, раскомментировав и отредактировав следующий параметр в файле конфигурации **/etc/systemd/journald.conf**.



В блоке **[journal]** надо изменить параметр **SystemMaxUse**, например **SystemMaxUse=50M**. Допустимые обозначения единиц - **K, M, G, T, P, E**.

Удаление журналов и определение текущего использования дискового пространства

Удалить файлы архивных журналов, можно вручную с помощью rm или использовать **journalctl**.

Удалить журналы, оставив только последние *100 Мб*:

```
journalctl --vacuum-size=100M
```

Удалить журналы, оставив журналы только за последние *7 дней*:

```
journalctl --vacuum-time=7d
```

Определить, сколько места занимает журнал на диске, используя флаг *--disk-usage*:

```
journalctl --disk-usage
```

Вывод лога в текстовый файл

Если необходимо вывести лог в текстовый формат, используйте конструкцию `<команда> > <путь_к_текстовому_файлу>`

Например:

```
journalctl -b > /home/user/loginfo.log
```

Фильтрация по приоритету

Фильтрация может применяться к приоритету сообщения, если вы хотите отфильтровать конкретное сообщение, такое как “**warning**” или “**error**” и т.д.

В таблице ниже перечислены все уровни приоритета:

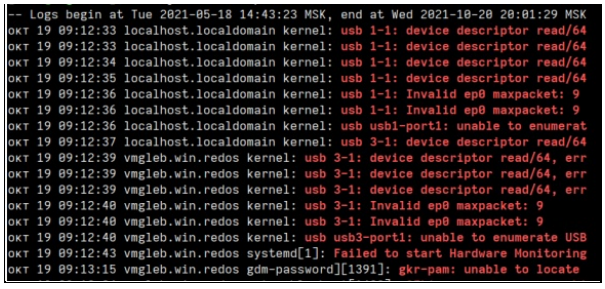
Приоритет	Код
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

Например:

```
journalctl -p 3 –b
```

или

```
sudo journalctl -p err –b
```

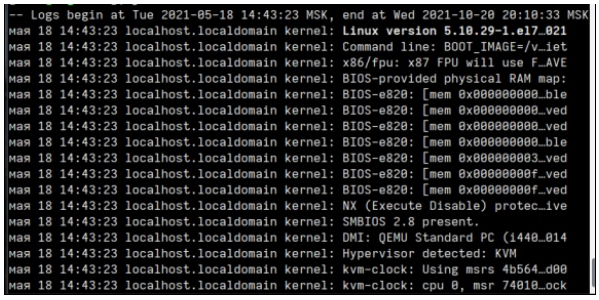


Сокращение или расширение области вывода

По умолчанию **journalctl** выводит на страничном модуле всю запись целиком так, что записи доходят до правого края экрана. Если вы предпочитаете урезать вывод, где удалена информация, вы можете использовать опцию **--no-full**.

Например:

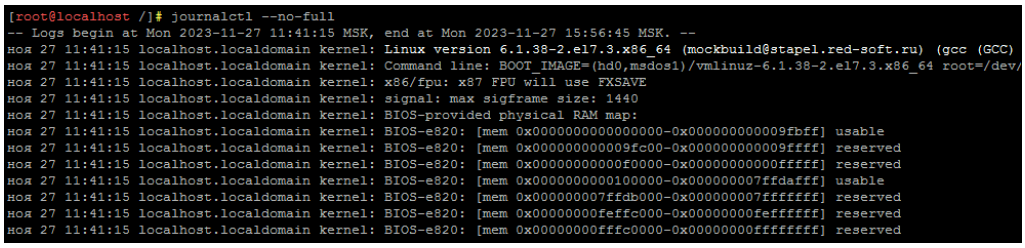
```
journalctl --no-full
```



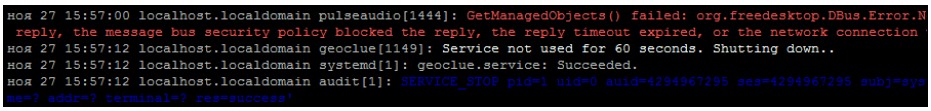
Запись логов в стандартный вывод

По умолчанию **journalctl** использует для вывода утилиту **less**. В этом случае к данным нельзя применять стандартные утилиты для обработки текстовых данных. При добавлении опции `--no-pager` все сообщения будут записываться в стандартный вывод.

Например:



С добавлением опции `--no-pager`:



Справка по утилите

Получить актуальные ключи команды:

```
journalctl --help
```

Чтение всех логов:

```
journalctl
```

Логи с момента запуска системы:

```
journalctl -b
```

Показывать записи журнала с момента запуска системы с расшифровкой ошибок:

```
journalctl -xb
```

Показать самые последние записи журнала и продолжать печатать новые записи при добавлении их в журнал:

```
journalctl -f
```

Просмотр информации о недавних событиях:

```
journalctl -n
```

По умолчанию на консоль выводится информация о последних 10 событиях. С опцией `-n` можно указать необходимое число событий:

```
journalctl -n 20
```

Для фильтрации по дате и времени важны два ключа

- `--since` - вывод от такого-то момента времени;
- `--until` - вывод до такого-то момента времени.

В качестве значений для этих ключей могут использоваться:

- Формат **YYYY-MM-DD HH:MM:SS**:

```
journalctl --since "2019-05-05 00:01" --until "2019-05-06 01:40"
```

- Слова «**yesterday**», «**today**», «**tomorrow**», «**now**»:

```
journalctl --since "yesterday" --until "2019-05-06 01:40"
```

Показывать в реальном времени все записи, независимо от их размера и кодировки:

```
journalctl -af
```

Просмотр сообщений ядра:

```
journalctl -k
```

Все сообщение конкретной утилиты, например, **systemd**:

```
journalctl /usr/lib/systemd/systemd
```

Все сообщения конкретного процесса:

```
journalctl _PID=1
```

Все сообщения конкретного приложения или службы:

```
journalctl -u netcfg
```

Все сообщения процессов, запущенных от имени конкретного пользователя:

```
journalctl _UID=33
```

Для справки в таблице ниже приведено расположение файлов журналов некоторых наиболее часто используемых служб:

Сервис	Путь
WEB-сервер Apache	/var/log/httpd/
Система управления печатью Cups	/var/log/cups/
Антивирус kaspersky	/var/log/kaspersky/
Системный журнал Syslog	/var/log/anaconda/syslog*
Samba	/var/log/samba/
X server	/var/log/Xorg.*.log
Графический менеджер gdm	/var/log/gdm/
Основной список логов	/var/log/messages

Средство просмотра журналов Log File Navigator (LNAV)

Установка и запуск
Параметры
Синтаксис
Навигация
Фильтры

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** lnav-0.11.2-1

lnav (**Log File Navigator**) – является расширенным средством просмотра файлов журналов, которое использует любую семантическую информацию, которую можно почерпнуть из просматриваемых файлов, таких как отметки времени и уровни журналов. Используя эту дополнительную семантическую информацию, *lnav* может делать такие вещи, как чередование сообщений из разных файлов, генерация гистограмм сообщений с течением времени и предоставление горячих клавиш для навигации по файлу.

Навигатор журналов *lnav* понимает ряд форматов файлов:

- */var/log/messages* – глобальный системный журнал, в котором пишутся сообщения с момента запуска системы, от ядра Linux, различных служб, обнаруженных устройств, сетевых интерфейсов и много другого;
- */var/log/secure* – информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации;
- */var/log/dmesg* – информация о драйверах устройств. Одноименной командой можно просмотреть вывод содержимого файла. Размер журнала ограничен; когда файл достигнет своего предела, старые сообщения будут перезаписаны более новыми;
- */var/log/anaconda/anaconda.log* – записи, зарегистрированные во время установки системы;
- */var/log/audit/audit* – записи, созданные службой аудита **auditd**;
- */var/log/boot.log* – информация, которая пишется при загрузке операционной системы;
- */var/log/cron* – отчет службы **crond** об исполняемых командах и сообщения от самих команд;
- */var/log/cups* – информация обо всем, что связано с печатью и принтерами;
- */var/log/maillog/* – журнал почтового сервера, используемого на ОС;
- */var/log/samba/* – логи файлового сервера **Samba**, который используется для доступа к общим папкам Windows и предоставления доступа пользователям Windows к общим папкам Linux;
- */var/log/spooler* – для представителей старой школы, содержит сообщения **USENET**. Чаще всего бывает пустым и заброшенным;
- */var/log/Xorg.0.log* – логи X-сервера. Чаще всего бесполезны, но если в них есть строки начинающиеся с **EE**, то следует обратить на них внимание;
- */var/log/lastlog* – последняя сессия пользователей;
- произвольные записи с временными отметками;
- gzip, bzip;
- журнал VMWare ESXi/vCenter.

Установка и запуск

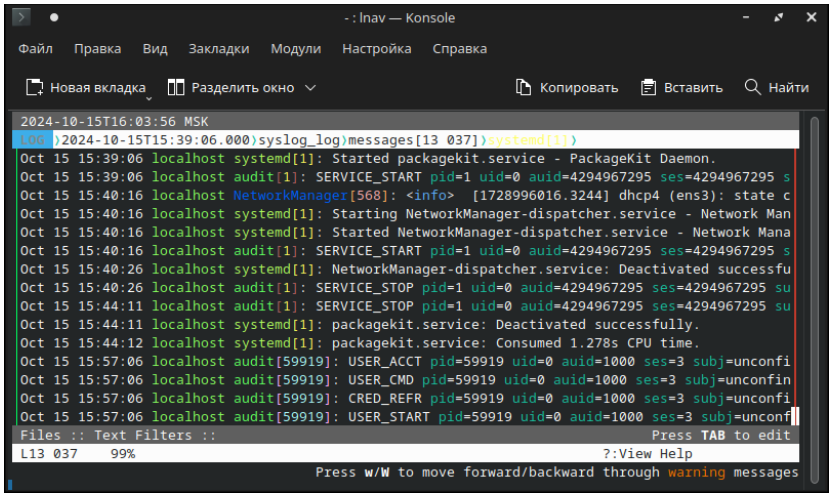
Для установки *lnav* выполните команду (потребуются права **администратора**):

```
sudo dnf install lnav
```

Дальнейшая работа с утилитой должна производиться с правами **администратора**, если не указано иное.

Запуск *lnav* производится командой:

```
lnav
```



При вводе команды без параметров *lnav* автоматически отображает информацию в реальном времени из файла */var/log/messages* на основе самых последних отметок времени из всех файлов журналов.

Параметры

Для того чтобы посмотреть информацию об отдельном файле, нужно использовать команду с определёнными параметрами (опциями). Список параметров представлен ниже:

- *-h* – распечатать сообщение и выйти;
- *-H* – показать на дисплее справку;
- *-I <путь>* – дополнительный каталог;
- *-i* – установить данный формат файла и выйти;
- *-C* – проверить конфигурацию и выйти;
- *-d <имя_файла>* – написать отладочные сообщения в указанный файл;
- *-V* – распечатать информацию версии;
- *-a* – загрузить самый последний файл журнала типов;
- *-r* – загрузка старого *rotated* журнала;
- *-t* – добавление метки к линиям данных, чтение в стандартном вводе;
- *-w <имя_файла>* – содержимое стандартного ввода в файл;
- *-c <команда>* – выполнить команду после того, как файлы были загружены;
- *-f <путь_к _файлу>* – выполнить команды в указанный файл;
- *-n* – работать без пользовательского интерфейса *UI*;
- *-q* – не печатать сообщения журнала после выполнения всех команд, или когда *lnav* читает из **stdin**;

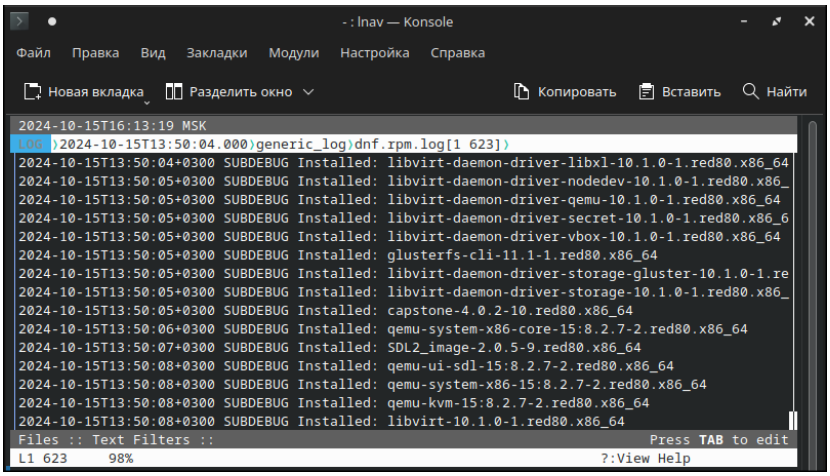
Синтаксис

Синтаксис утилиты выглядит следующим образом:

```
lnav <опция> <log_файл_1> <log_файл_2>
```

Например, просмотрим информацию из файла */var/log/dnf.rpm.log*:

```
lnav /var/log/dnf.rpm.log
```

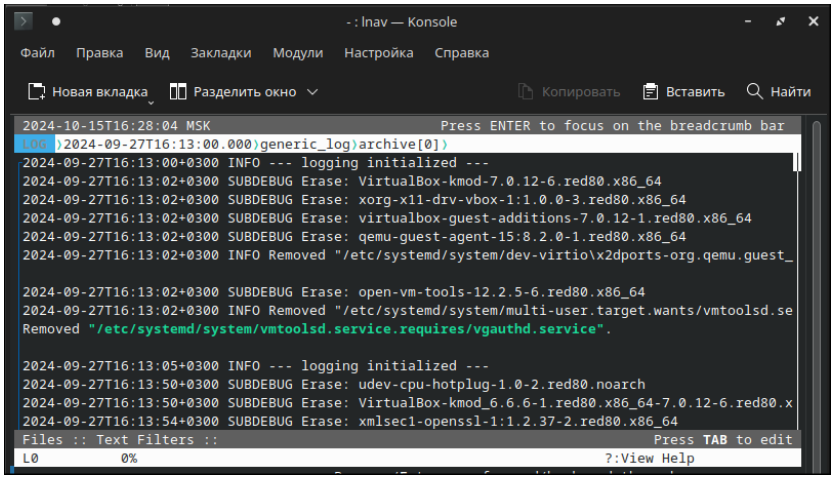


Так же в *lnav* можно открывать несколько файлов сразу и переключаться между ними:

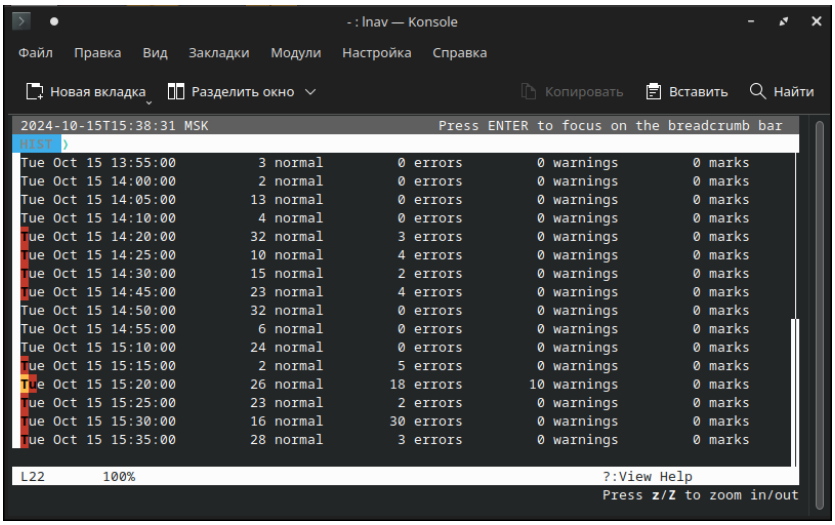
```
lnav /var/log/dnf.rpm.log /var/log/hawkey.log
```

Программа умеет напрямую открывать архивный файл:

```
lnav -r /mnt/archive.tar.gz
```



Программа показывает гистограмму информативных сообщений, предупреждений и ошибок, если нажать клавишу «**i**»:



Навигация

Список горячих клавиш для работы с *lnav*:

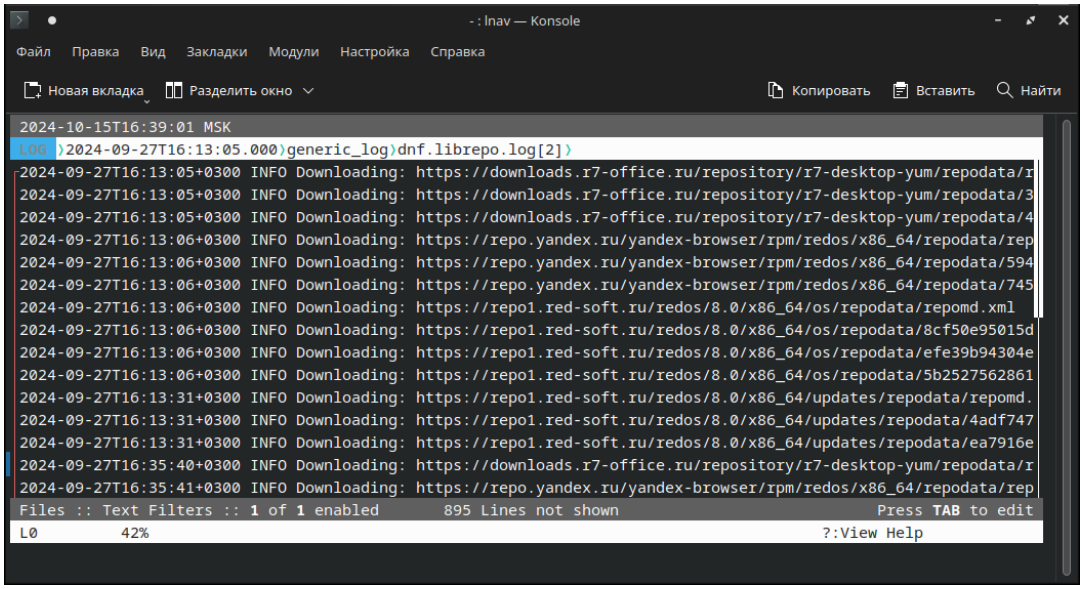
- *Shift + D* – вперед/назад на 24 часа;
- *Shift + [1-6]* – следующая/предыдущая *n*-я десятая минута часа;
- *Shift + 0* – следующий/предыдущий день;
- *Shift + R* – вперед/назад по относительному времени, которое в последний раз использовалось с командой **goto**;
- *M* – отметить/снять отметку с верхней строки;
- *Shift + M* – отметить/снять отметку с диапазона строк от последней отмеченной до верхней;
- Shift + J – отметить/снять отметку со следующей строки после ранее отмеченной;
- Shift + W – вернуться к предыдущему предупреждающему сообщению;
- *Shift + E* – перейти к последнему сообщению об ошибке;
- *Shift + K* – отметить/снять отметку с предыдущей строки;
- *C* – скопировать отмеченные строки в буфер обмена;
- *Shift + C* – очистить отмеченные линии;
- *?* – просмотр/выход из встроенной справки;
- *Q* – возврат к предыдущему виду/выход;
- *Shift + P* – переключится в/из отображаемого журнала или текстовых файлов;
- *Shift + T* – отображать прошедшее время между строками;
- *T* – переключиться в/из просмотра текстового файла;
- *I* – переключиться в/из просмотра гистограммы;
- *Shift + I* – переключиться в/из просмотра гистограммы;
- *V* – переключиться в/из представления результатов *sql*;
- *Shift + V* – переключиться в/из представления результатов *SQL* и перейти к соответствующему столбцу **log_line**;
- *P* – переключить отображение результата парсера журнала;

- *Tab* – циклический переход от столбцов к графику в представлении результатов *SQL*;
- *Ctrl + L* – переключиться в режим **li-fi**. Отображаемые строки журнала будут выгружены на терминал без каких-либо украшений, чтобы их можно было легко скопировать;
- */* – поиск регулярного выражения;
- *;* – выполнить SQL-запрос;
- *:* – выполнить внутреннюю команду;
- *Ctrl +]* – прервать.

Фильтры

Если вы хотите отображать только строки, соответствующие определенному шаблону, вы можете сделать это с помощью фильтров. Сначала войдите в командный режим, нажав двоеточие, а затем введите нужный текст с фильтром **filter-in**, чтобы отображались только строки, содержащие необходимый текст. Например:

```
filter-in repodata
```



Точно так же вы можете использовать фильтрацию, чтобы показать все данные, кроме отфильтрованных строк, для этого введите текст с фильтром **filter-out**.

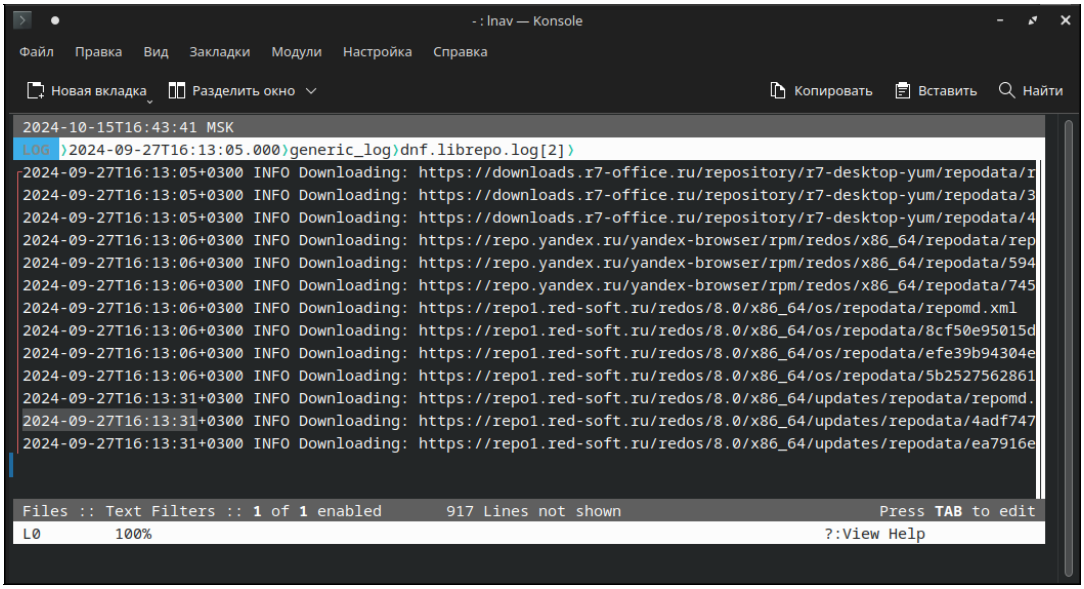
```
filter-out repodata
```

После применения фильтра данные с текстом «repodata» выводиться не будут.

Также можно использовать фильтры **hide-lines-after** и **hide-lines-before**.

Фильтр **hide-lines-after** скрывает строки, которые записаны *позже* заданного времени.

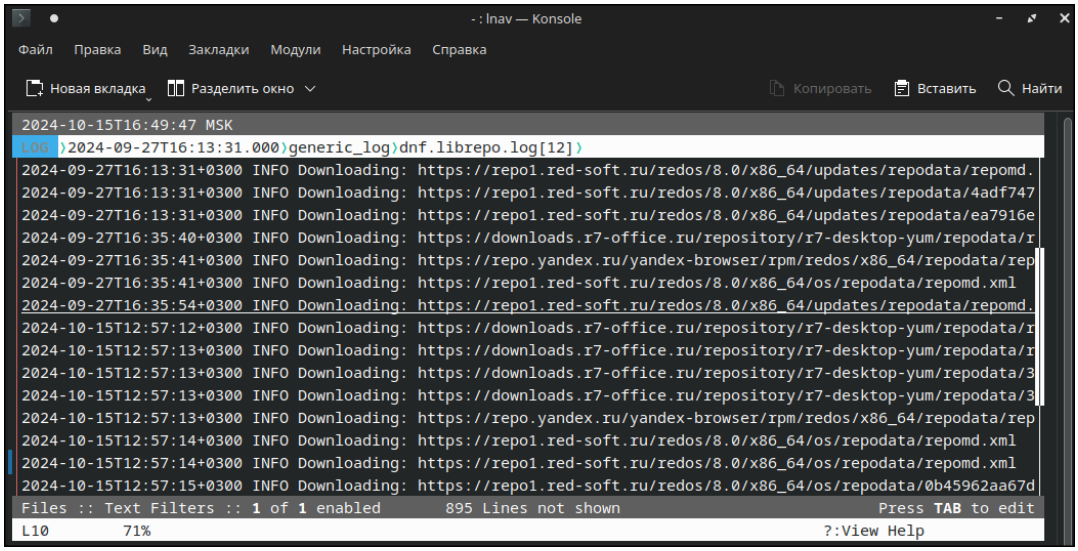
```
hide-lines-after 2024-09-27T16:13:31
```



Фильтр **hide-lines-before** скрывает строки, которые записаны *раньше* заданного времени.

```
hide-lines-before 2024-09-27T16:13:31
```

Скрытые строки можно снова показать с помощью команды **show-lines-before-and-after**.



Эти фильтры будут применяться ко всему файлу, поэтому, пока вы не отмените их (с помощью **Ctrl + R**), любые другие действия будут выполняться с отфильтрованным журналом, а не с журналом в целом.

Утилита incron

Установка
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: incron-0.5.12-19

Утилита **incron** предназначена для мониторинга событий в файловой системе и выполнения указанных действий при их обнаружении.

Основные функции утилиты:

- возможность задания разнообразных событий;
- возможность выполнения необходимых действий при обнаружении заданного события.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install incron
```

Запустите службу **incrond** и добавьте ее в автозагрузку:

```
systemctl enable incrond --now
```

Работа с утилитой производится через терминал с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

Для запуска утилиты необходимо выполнить команду **incrontab** с добавлением ключей.

Список ключей, с которыми может быть запущена утилита:

- `-e` — редактировать таблицу мониторинга текущего пользователя.

Редактирование таблицы мониторинга выполняется через редактор **nano**. Также доступно использование любого другого удобного текстового редактора, для смены редактора по умолчанию выполните команду:

```
export EDITOR="/usr/bin/vi"
```

- `-r` — удалить таблицу текущего пользователя;
- `-l` — вывести таблицу текущего пользователя.

Например, для редактирования таблицы мониторинга текущего пользователя выполните:

```
incrontab -e
```

Редактирование таблицы выполняется построчно для текущего пользователя, в таблицу необходимо добавить строку вида:

```
<объект> <событие> <команда>
```

где:

- `<объект>` — полный путь к файлу или директории, за которыми нужно наблюдать (рекурсивное наблюдение за директориями не поддерживается);

- `<событие>` — событие, на предмет наступления которого нужно наблюдать за объектом. Если событий несколько, они разделяются между собой запятой без пробела;
- `<команда>` — команда или скрипт, которые необходимо выполнить при наступлении события.

Доступные события приведены в таблице ниже.

Событие	Значение
IN_ACCESS	Файл был прочитан
IN_ATTRIB	Метаданные изменены (разрешения, временные метки, расширенные атрибуты и т. д.)
IN_CLOSE_WRITE	Файл, открытый для записи, был закрыт
IN_CLOSE_NOWRITE	Файл, не открытый для записи, был закрыт
IN_CLOSE	**IN_CLOSE_WRITE** или **IN_CLOSE_NOWRITE**
IN_CREATE	Создан файл или каталог
IN_DELETE	Удален файл или каталог
IN_DELETE_SELF	Удален файл или каталог, который мониторится
IN_MODIFY	Файл изменен
IN_MOVE_SELF	Файл или каталог, который мониторится, был перемещен
IN_MOVED_FROM	Файл был перемещен из каталога, который мониторится
IN_MOVED_TO	Файл перемещен в каталог, который мониторится
IN_MOVE	**IN_MOVED_FROM** или **IN_MOVED_TO**
IN_MOVED_TO	Файл был открыт
IN_ALL_EVENTS	Все перечисленные события

Примеры использования

В таблице мониторинга строка вида:

```
/etc/passwd IN_MODIFY cp /etc/passwd /tmp
```

означает, что при изменении файла **/etc/passwd**, например, при авторизации, файл будет скопирован в каталог **/tmp**.

В таблице мониторинга строка вида:

```
/etc/ssh/sshd_config IN_MODIFY systemctl restart sshd
```

означает, что при изменении конфигурации файла **sshd_config** будет перезагружен **sshd**-сервер.

Утилиты inotifywatch и inotifywait

Утилита inotifywatch
Установка
Примеры использования

Утилита inotifywait
Установка
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: inotify-tools-3.14-25

Утилита inotifywatch

Утилита **inotifywatch** предназначена для наблюдения за событиями файловой системы. Утилита выводит суммарное количество событий, произошедших с каждым файлом или директорией. Собранные данные отображаются только по завершении работы утилиты, выводятся на стандартный вывод в виде таблицы с одним столбцом для каждого вида события и одной строкой для каждого наблюдаемого файла или директории. Таблица отображает, сколько раз указанное событие произошло с каждым из файлов или каталогов.

Установка

Утилита входит в состав пакета **inotify-tools**.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install inotify-tools
```

Работа с утилитой производится через терминал с правами **непривилегированного** пользователя, выйдите из сеанса суперпользователя **root**:

```
exit
```

Синтаксис утилиты имеет вид:

```
inotifywatch [<опции>] <файл_1> [<файл_2>] [ ... ]
```

где:

- `<опции>` – необходимые для работы утилиты опции;
- `<файл_1>`, `<файл_2>` … – путь к файлу, мониторинг которого необходимо производить.

Для запуска утилиты необходимо выполнить команду **inotifywatch** с добавлением необходимых опций.

Список опций, с которыми может быть запущена утилита:

- `-h` – вывести справку по работе с утилитой;
- `-r` – рекурсивное наблюдение за всеми подкаталогами указанного каталога;
- `-t <время>` – время мониторинга в секундах, в течение которого будет производиться наблюдение (если опция не указана, мониторинг будет производиться непрерывно);
- `-e <событие>` – наблюдение только за указанными событиями.

Примеры использования

Для мониторинга файла **/etc/passwd** выполните:

```
inotifywatch /etc/passwd
```

Для мониторинга файла **/etc/passwd** в течение **10 секунд** на события типа **ACCESS** выполните:

```
inotifywatch -t 10 -e access /etc/passwd
```

Утилита inotifywait

Утилита **inotifywait** предназначена для наблюдения за событиями файловой системы. Утилита отображает в реальном времени информацию о наступлении запрашиваемых событий.

Установка

Утилита входит в состав пакета **inotify-tools**.

Для установки пакета перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install inotify-tools
```

Работа с утилитой производится через терминал с правами **непривилегированного** пользователя, выйдите из сеанса суперпользователя **root**:

```
exit
```

Синтаксис утилиты имеет вид:

```
inotifywait [<опции>] <файл_1> [<файл_2>] [ ... ]
```

где:

- `<опции>` – необходимые для работы утилиты опции;
- `<файл_1>`, `<файл_2>`... – путь к файлу, мониторинг которого необходимо производить.

Для запуска утилиты необходимо выполнить команду **inotifywait** с добавлением необходимых опций.

Список опций, с которыми может быть запущена утилита:

- `-h` – вывести справку по работе с утилитой;
- `-m` – не останавливать мониторинг после наступления первого события, продолжать мониторинг до остановки пользователем;
- `-o` – вывести события в файл;
- `-r` – рекурсивное наблюдение за всеми поддиректориями;
- `-t` – время мониторинга в секундах, в течение которого будет производиться наблюдение;
- `-e` – наблюдение за определенными событиями;
- `--format <формат_вывода>` – задать формат вывода:
    - **%w** – указать имя наблюдаемого файла или директории;
    - **%f** – если событие происходит с файлом внутри наблюдаемой директории, указать имя этого файла;
    - **%e** – указать наименование произошедшего события, наименования разделяются запятыми;
    - **%T** – указать текущее время в формате **ЧЧ:ММ:СС**;

- **--timefmt <формат_вывода>** – установить формат времени.

Примеры использования

Для наблюдения за файлом **/etc/passwd**, не завершая наблюдение после наступления первого события и используя пользовательский формат вывода, добавляющий текущее время к каждому событию, выполните команду:

```
inotifywait -m --format %T\ %w%f\ %e --timefmt %T /etc/passwd
```

где:

- **inotifywait -m** – не прерывать выполнение после первого события;
- **--format %T\ %w%f\ %e** – задать формат вывода, где:
  - **%w** – указать имя отслеживаемого файла,
  - **%f** – при отслеживании директории указать имя файла, в котором произошли изменения,
  - **%e** – показать события, которые произошли.
  - **--timefmt %T /etc/passwd** – добавить текущее время.

Результат выполнения команды:

```
[root@localhost /]# inotifywait -m --format %T\ %w%f\ %e --timefmt %T /etc/passwd
Setting up watches.
Watches established.
12:54:44 /etc/passwd OPEN
12:54:44 /etc/passwd ACCESS
12:54:44 /etc/passwd CLOSE_NOWRITE,CLOSE
```

Для рекурсивного наблюдения за директорией **/etc**, не завершая наблюдение после наступления первого события, используя пользовательский формат вывода, добавляющий текущее время к каждому событию, и записывая вывод в файл **/tmp/inotifywait**, выполните команду:

```
inotifywait -m --format %T\ %w%f\ %e --timefmt %T -o /tmp/inotifywait -r /etc/ &
```

Утилита fswatch

Установка
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: fswatch-1.17.1-1

Утилита **fswatch** предназначена для мониторинга изменений файлов и каталогов в реальном времени.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fswatch
```

Работа с утилитой производится через терминал. Права для работы с утилитой определяются установленным доступом к отслеживаемому каталогу или файлу.

Синтаксис утилиты имеет вид:

```
fswatch [<опции>] [<путь>]
```

где:

- `<опции>` – необходимые для работы утилиты опции;
- `<путь>` – путь к каталогу или файлу, мониторинг которого необходимо производить.

Для запуска утилиты необходимо выполнить команду **fswatch** с добавлением необходимых ключей.

Список основных ключей, с которыми может быть запущена утилита:

- `-h`, `--help` – вывод справки по утилите;
- `--event=<событие>` – отслеживать только указанные события;
- `-e <шаблон>`, `--exclude=<шаблон>` – исключение каталогов/файлов, совпадающих с шаблоном, из мониторинга;
- `-f` – вывод времени события в заданном формате;
- `-l` – интервал мониторинга;
- `-r` – рекурсивный просмотр каталогов;
- `-v` – печать подробного вывода.

Примеры использования

Для вывода изменений каталога **/tmp** с интервалом **20 секунд** выполните команду вида:

```
fswatch -l 20 /tmp
```

где

- **-l 20** – время мониторинга в секундах;
- **/tmp** – каталог мониторинга.

Результат выполнения команды:

```
 fswatch -l 20 /tmp

/tmp
/tmp/ test
/tmp
/tmp/ test
/tmp
/tmp/ test
/tmp
```

В каталоге был создан и удален каталог **/test**.

Для вывода времени изменения файла **/test.sh** с интервалом **2 секунды** выполните команду вида:

```
fswatch -t -l 2 /test.sh
```

где:

- **-t** – вывод времени наступления события.

Результат выполнения команды:

```
 fswatch -t -l 2 /test.sh

Пн 29 янв 2024 09:30:13 /test.sh
Пн 29 янв 2024 09:30:15 /test.sh
Пн 29 янв 2024 09:30:15 /test.sh
Пн 29 янв 2024 09:30:15 /test.sh
Пн 29 янв 2024 09:30:22 /test.sh
Пн 29 янв 2024 09:30:22 /test.sh
```

Для вывода времени изменения каталога **/** с интервалом **2 секунды** с указанием производимых действий выполните команду:

```
fswatch -x -t -l 2 /
```

где:

- **-x** – вывод произошедших изменений.

Результат выполнения команды:

```
 fswatch -x -t -l 2 /

Пн 29 янв 2024 09:33:44 / IsDir
Пн 29 янв 2024 09:33:44 //test Created
Пн 29 янв 2024 09:33:47 / IsDir
Пн 29 янв 2024 09:33:47 //test PlatformSpecific
Пн 29 янв 2024 09:33:49 / IsDir
Пн 29 янв 2024 09:33:49 //test PlatformSpecific
Пн 29 янв 2024 09:33:49 / IsDir
Пн 29 янв 2024 09:33:49 //test Removed
```

Rsyslog – сервис управления системными журналами

Содержимое конфигурационного файла rsyslog.conf
Создание правил в системе
Другие варианты написания правил
Отправка лог-сообщений на удаленный сервер

Rsyslog — это очень быстрый, расширяемый сервис для управления логами с огромным количеством возможностей. Среди его возможностей можно отметить поддержку фильтрации контента, а также передачу логов по сетям. Основные возможности:

- Многопоточность;
- TCP, SSL, TLS, RELP;
- Поддержка MySQL, PostgreSQL, Oracle;
- Фильтрация журналов;
- Полностью настраиваемый формат вывода.

Вы можете подробнее ознакомиться с работой сервиса управления логами **Rsyslog**, просмотрев наши обучающие видео:

- на **RuTube** — Rsyslog - сервис управления логами;
- в **Яндекс.Дзен** — Rsyslog - сервис управления логами;
- в **VK Видео** — Rsyslog - сервис управления логами.

На наших каналах вы также сможете найти много другой полезной информации.

Каталогом по умолчанию для хранения логов является каталог **/var/log**, в файлы которого записывается вся информация о состоянии системы и используемых программ, а также информация об ошибках. Лог-файлы можно просмотреть, выполнив команду:

```
ls -l /var/log/
```

Содержимое конфигурационного файла rsyslog.conf

Главным конфигурационным файлом сервиса **rsyslog** является **rsyslog.conf**. Для просмотра содержимого конфигурационного файла можно воспользоваться командой:

```
nano /etc/rsyslog.conf
```

Файл разделен на 3 основных секции:

- Modules — содержит параметры, предназначенные для настройки методов работы сервиса с лог-сообщениями;
- Global derectives — содержит глобальные параметры работы службы **rsyslog**;
- Rules — содержит правила сортировки логов.

Секция Modules

В секции Modules загружаются все необходимые модули программы. Секция имеет следующим вид:

```
#### MODULES ####

module(load="imuxsock"    # provides support for local system logging (e.g. via logger command)
  SysSock.Use="off")      # Turn off message reception via local log socket;
                          # local messages are retrieved through imjournal now.
module(load="imjournal"   # provides access to the systemd journal
  StateFile="imjournal.state")     # File to store the position in the journal
#module(load="imklog")    # reads kernel messages (the same are read from journald)
#module(load"immark")     # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp")     # needs to be done just once
#input(type="imudp" port="514")
```

```
# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp")     # needs to be done just once
#input(type="imtcp" port="514")
```

Существует четыре типа модулей:

- *Модули ввода* — можно рассматривать, как способ сбора информации из различных источников, начинаются с **im**;
- *Модули вывода* — позволяют отправлять сообщения в файлы, по сети или в базу данных, начинаются с **om**;
- *Модули фильтрации* — позволяют отфильтровывать сообщения по разным параметрам, начинаются с **fm**;
- *Модули парсинга* — предоставляют расширенные возможности для синтаксического анализа сообщения, начинаются с **pm**.

Модуль **imuxsock** позволяет сервису получать сообщения от приложений, работающих в локальной системе. По умолчанию отключено прослушивание сокета **/dev/log** из-за параметра `SysSock.Use="off"`.

Модуль **imjournal** предоставляет возможность импорта сообщений структурированного журнала из журнала *systemd* в системный журнал. Обратите внимание, что этот модуль читает базу данных журнала, что считается относительно интенсивной операцией. Таким образом, производительность конфигурации с использованием этого модуля может быть заметно ниже, чем при использовании **imuxsock**. По умолчанию ограничение скорости активировано и позволяет обрабатывать 20 000 сообщений в течение 10 минут, чего должно быть достаточно для большинства случаев использования. Если импорт структурированных данных необходим, используйте **imjournal**, в противном случае следует задействовать модуль **imuxsock**.

Модуль **imklog** предназначен для получения сообщений ядра.

Модуль **immark** позволяет маркировать соединения или выводить сообщения о том, что **syslog** все еще работает.

Секция Global directives

Глобальные директивы используются для настройки службы **rsyslog**. Как правило, они указывают значение для конкретной предопределенной переменной, которая влияет на функциональность правил или самой службы **rsyslog**.

Секция **Global directives** имеет следующий вид:

```
#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")
```

Описание переменных:

- `global(workDirectory="/var/lib/rsyslog")` — задает директорию, которая будет использоваться для рабочих файлов службы **rsyslog**;
- `module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")` — задает стандартный формат хранения времени, в секундах с 1970 года;
- `include(file="/etc/rsyslog.d/*.conf" mode="optional")` — задает директорию, которая будет использоваться для дополнительных файлов конфигурации.

Секция Rules

Данный раздел содержит правила сортировки логов. Каждое правило имеет свой синтаксис: сначала идет *источник* и *приоритет*, затем *действие*. Если источник и приоритет совпадают, сообщение отправляется в указанный файл. *Источников* и *приоритетов* может быть несколько, их можно разделять точкой с запятой.

Содержимое секции имеет следующий вид:

```
#### RULES ####
```

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure

# Log all the mail messages in one place.
mail.*                                          -/var/log/maillog

# Log cron stuff
cron.*                                          /var/log/cron

# Everybody gets emergency messages
*.emerg                                         :omusrmsg:*
# Save news errors of level crit and higher in a special file.

uucp,news.crit                                  /var/log/spooler

# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
```

Источниками являются места, откуда поступают сообщения.

Источники могут принимать следующие значения:

- **auth** — все, что связано с авторизацией пользователей, например, *login* и *su* (безопасность/права доступа);
- **authpriv** — то же самое, что и **auth**, однако сообщения этой категории записываются в файл, который могут читать лишь некоторые пользователи (категория выделена, потому что принадлежащие ей сообщения могут содержать открытые пароли пользователей, которые не должны попадать на глаза посторонним людям, и, следовательно, файлы протоколов должны иметь соответствующие права доступа);
- **cron** — сообщения от системного планировщика;
- **daemon** — сообщения от системных служб, которые в отличие от FTP или LPR не имеют специально-выделенных категорий;
- **kern** — сообщения ядра;
- **lpr** — сообщения от системы печати;
- **mail** — сообщения от почтовой системы;
- **mark** — присваивается отдельным сообщениям, формируемым службой syslog;
- **security** — эквивалентно auth;
- **syslog** — система протоколирования может протоколировать сообщения от самой себя;
- **uucp** — копирование файлов между компьютерами (Unix-to-Unix CoPy);
- **user** — сообщения пользовательских программ;
- **local0 ... local7** — зарезервированные категории для использования администратором системы. Категория local7 обычно используется для сообщений, генерируемых на этапе загрузки системы;
- ***** — Выбор всех источников.

Приоритетом является степень важности сообщения.

Приоритеты могут принимать следующие значения:

- **emerg** (раньше *panic*) — чрезвычайная ситуация, система неработоспособна;
- **alert** — тревога, требуется немедленное вмешательство;
- **crit** — критическая ошибка (критическое состояние);
- **error** (раньше *err*) — сообщение об ошибке;
- **warn** (раньше *warning*) — предупреждение;
- **notice** — информация о каком-либо нормальном, но важном событии;
- **info** — информационное сообщение;

- **debug** — сообщения, формируемые в процессе отладки;
- ***** — выбор всех приоритетов;
- **none** — сообщения от источника с любым приоритетом будут исключены для действия.

Действием является отправка сообщений, которые подходят под заданные ранее параметры в заданное место.

Действия могут принимать следующие значения:

- **/путь/к/файлу** — отправка сообщений в обычный файл;
- **/dev/console** — отправка сообщений в терминал или консоль;
- **@xx.xx.xx.xx:514** — отправка сообщений на удаленную машину с помощью **UDP**;
- **@@xx.xx.xx.xx:514** — отправка сообщений на удаленную машину с помощью **TCP**;
- **user,user2,root** — отправка сообщений пользователям на терминал (разделенный запятыми список пользователей, получающих сообщения).

Создание правил в системе

В общем случае синтаксис правил выглядит следующим образом:

```
<источник>.<приоритет> <действие>
```

В качестве примера разберем правило:

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

Первым *источником* событий являются все сообщения с приоритетом **info**. Также к *источникам* добавляются и другие сообщения, разделенные между собой точкой с запятой. Из правил следует, что *источники* **mail**, **authpriv**, **cron** будут исключены, так как имеют *приоритет* **none**. *Действием* для данного правила является отправка сообщений в файл **/var/log/messages**.

Другие варианты написания правил

Фильтрация на основе свойств сообщения

Фильтрация данного вида имеет следующий синтаксис:

```
:<переменная>, <операция_сравнения>, "<искомое_значение>" <действие>
```

Переменные могут принимать значение:

- **msg** — тело сообщения;
- **hostname** — имя хоста/IP-адреса из сообщения;
- **fromhost** — имя хоста, от которого пришло сообщение;
- **fromhost-ip** — адрес хоста, от которого пришло сообщение (127.0.0.1 для локальных сообщений);
- **syslogtag** — имя и номер процесса (`"rsyslogd[12125]:"`), который выдал сообщение (извлекается из сообщения);
- **programname** — имя процесса, который выдал сообщение (извлекается из сообщения);
- **pri** — источник и приоритет, в виде числа;
- **pri-text** — декодированные источник и приоритет (`facility.priority`, например `syslog.emer`);
- **syslogfacility** — только источник в виде числа;
- **syslogfacility-text** — только декодированный источник (`"local0"`);
- **syslogseverity** — только приоритет в виде числа;
- **syslogseverity-text** — только декодированный уровень (`"debug"`);
- **timegenerated** — время получения (с высоким разрешением);
- **timereported** — время, извлечённое из сообщения;
- **inputname** — имя входного модуля;

- **$hour, $minute** — текущее время;
- **$myhostname** — имя хоста обработки.

Операция сравнения может принимать значение:

- **contains** — проверяет соответствие `<искомое_значение>` с любой частью строки в переменная;
- **isequal** — проверяет, совпадает (целиком) ли `<искомое_значение>` с переменной;
- **isempty** — проверяет, является ли переменная пустой;
- **startswith** — проверяет, начинается ли переменная с `<искомое_значение>`;
- **regex** — сравнивает поле с регулярным выражением.

Искомое значение может принимать значение имени программы, службы или источника (источники были рассмотрены ранее в данной статье).

Действие принимает значения, рассмотренные ранее в статье.

Теперь можно составить правило для логирования приложения. Пример составления правила:

```
:syslogtag, isequal, "wireguard:" /var/log/wireguard.log
 &stop
```

& stop необходим для того, чтобы остановить регистрацию сообщения после его совпадения.

Фильтрация RainerScript

Фильтрация данного вида имеет следующий синтаксис:

```
if $<переменная> <операция_сравнения> "<искомое_значение>" then <действие>
```

Операция сравнения может принимать значения:

- **==** — равно;
- **!=** — не равно.

Пример правила для логирования приложения будет выглядеть следующим образом:

```
if $syslogtag == "wireguard" then /var/log/wireguard.log
```

Отправка лог-сообщений на удаленный сервер

Настройка сервера, который будет принимать лог-сообщения

Если на сервере используется брандмауэр, необходимо открыть порты **TCP/UDP 514**. На примере **iptables** открытие портов производится командами:

```
iptables -A INPUT -p tcp --dport 514 -j ACCEPT
iptables -A INPUT -p udp --dport 514 -j ACCEPT
```

Затем настройте SELinux, если он используется:

```
semanage port -m -t syslogd_port_t -p tcp 514
semanage port -m -t syslogd_port_t -p udp 514
```

Для разрешения серверу принимать соединение по **TCP** и **UDP** в конфигурационном файле **/etc/rsyslog.conf** раскомментируйте строки в секции **Modules**:

```
module(load="imudp") # needs to be done just once
 input(type="imudp" port="514")

 module(load="imtcp") # needs to be done just once
 input(type="imtcp" port="514")
```

Не обязательно открывать соединение по обоим протоколам, можно выбрать только тот, который необходим именно вам.

В эту же секцию после модулей для TCP- и UDP-соединения необходимо добавить следующее:

```
$template RemoteLogs,"/var/log/rsyslog/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~
```

Таким образом создается шаблон, по которому лог-сообщения от любого источника с любым уровнем будут сохраняться в каталог сервера **/var/log/rsyslog/<имя_компьютера-отправителя_лога>/<приложение-отправитель_лога>.log**.

После проделанных настроек необходимо перезагрузить службу **rsyslog** командой:

```
systemctl restart rsyslog.service
```

Настройка сервера на этом закончена. Для проверки открытия порта выполните команду:

```
netstat -pnltu
```

```
[root@localhost ~]# netstat -pnltu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3831/sshd: /usr/sbi
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1016/master
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN      99121/cupsd
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      107443/rsyslogd
tcp6       0      0 :::22                   :::*                    LISTEN      3831/sshd: /usr/sbi
tcp6       0      0 :::631                  :::*                    LISTEN      99121/cupsd
tcp6       0      0 :::514                  :::*                    LISTEN      107443/rsyslogd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1016/master
udp        0      0 127.0.0.1:323           0.0.0.0:*                           668/chronyd
udp        0      0 0.0.0.0:45131           0.0.0.0:*                           656/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           656/avahi-daemon: r
udp6       0      0 ::1:323                 :::*                                668/chronyd
udp6       0      0 :::41782                :::*                                656/avahi-daemon: r
udp6       0      0 :::5353                 :::*                                656/avahi-daemon: r
[root@localhost ~]#
```

Настройка клиента, который будет отправлять лог-сообщения

Для создания правила на клиенте воспользуйтесь директорией **rsyslog.d**, которая является дополнительной для конфигурационных файлов.

Создайте конфигурационный файл, который будет отправлять на сервер сообщения от *источника* **auth** с любым *приоритетом*. Для этого выполните команду:

```
nano /etc/rsyslog.d/auth.conf
```

И добавьте правило:

```
auth.* @@xx.xx.xx.xx:514
```

где **@@xx.xx.xx.xx:514** — адрес сервера и его порт для протокола **TCP**. Для протокола **UDP** нужно указывать действие в виде **@xx.xx.xx.xx:514**.

Сохраните изменения и перезагрузите службу **rsyslog** командой:

```
systemctl restart rsyslog.service
```

При корректной настройке на сервере в каталоге **/var/log/rsyslog** должна появиться директория с именем (hostname) ПК, который отправляет лог-файлы, и, непосредственно, лог-файлы.

```
ll /var/log/rsyslog/итого 4
drwx------. 2 root root 4096 окт 14 15:37 localhost
```

```
ll /var/log/rsyslog/localhost/-rw-------. 1 root root       100 окт 14 15:36 at-spi-bus-launcher.log
```

```
-rw-------. 1 root root       6904 окт 14 15:38 audit.log
-rw-------. 1 root root         98 окт 14 15:36 dbus-broker-launch.log
-rw-------. 1 root root        239 окт 14 15:36 plasmashell.log
-rw-------. 1 root root       2008 окт 14 15:37 rsyslogd.log
-rw-------. 1 root root        174 окт 14 15:37 su.log
-rw-------. 1 root root       1671 окт 14 15:37 systemd.log
```

Logrotate – настройка ротации (хранения) системных журналов

Основные параметры для настройки
Вспомогательные настройки
Проверка конфигурации

В РЕД ОС большинство сервисов и программ, которые работают в фоне, записывают информацию о своем состоянии, результатах работы и ошибках в файлы, называемые **журналами**. Стандартное расположение журналов или, как их еще называют, **логов** - в папке **/var/log**.

С помощью анализа этих файлов можно понять, что работает не так, почему произошла ошибка и как решить возникшую проблему. Однако существует некоторая проблема - размер журналов постоянно растет, они занимают все больше и больше места на диске, поэтому необходимо вовремя удалять устаревшие записи, чтобы они не мешали нормальной работе компьютера. Делать это можно вручную или воспользоваться утилитой **logrotate**.

Утилита **logrotate** предназначена для автоматизации обработки журналов. Она может выполнять необходимые действия в зависимости от определенных условий и правил соответствия. Например, можно сжимать журналы в архив или отправлять на другой сервер, когда они достигают определенного размера, возраста или других параметров.

Проверку условий можно настроить ежедневно, еженедельно или ежемесячно - это позволяет создать схему ротации логов, удобную именно для вас и вашего сервера.

Logrotate — популярная утилита, поэтому в большинстве дистрибутивов она поставляется по умолчанию.

Вы можете подробнее ознакомиться с возможностью настройки ротации логов при помощи утилиты **logrotate**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка ротации логов: logrotate;
- в **Яндекс.Дзен** — Настройка ротации логов: logrotate;
- в **VK Видео** — Настройка ротации логов: logrotate.

На наших каналах вы также сможете найти много другой полезной информации.

В дистрибутиве РЕД ОС программа также является предустановленной, поэтому даже установка ОС подробно записывается в журнал:

```
ls /var/log/anaconda/

anaconda.log     journal.log            program.log          X.log
dbus.log         ks-script-y8l57qzl.log  redos-postinstall.log
dnf.librepo.log  lorax-packages.log      storage.log
hawkey.log       packaging.log          syslog
```

Все основные настройки программы находятся в файле **/etc/logrotate.conf**.

Для дополнительных настроек в основном файле указана папка **/etc/logrotate.d**. Собственные настройки лучше сохранять именно в данном каталоге, так ими будет проще управлять.

```
sudo nano /etc/logrotate.conf

# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

Основные параметры для настройки

Чтобы указать частоту выполнения проверок на совпадение условий, используются следующие директивы:

- **hourly** — каждый час;
- **daily** — каждый день;
- **weekly** — каждую неделю;
- **monthly** — каждый месяц;
- **yearly** — каждый год.

По умолчанию настроена еженедельная (*weekly*) проверка.

Рассмотрим основные параметры управления и обработки журналов:

- **rotate** — указывает, сколько старых логов нужно хранить (в параметрах передается количество);
- **create** — создание пустого файла лога после перемещения старого;
- **dateext** — перед заголовком старого лога добавляется дата ротации;
- **compress** — сжатие логов;
- **delaycompress** — не сжимать последний и предпоследний журнал;
- **extension** — сохранять оригинальный лог-файл после ротации, если у него указано расширение;
- **mail** — отправлять e-mail после завершения ротации;
- **maxage** — выполнять ротацию журналов, если они старше, чем указано;
- **missingok** — не выдавать ошибки, если лог-файла не существует;
- **olddir** — перемещать старые логи в отдельную папку;
- **postrotate/endscript** — выполнить произвольные команды после ротации;
- **start** — номер, с которого будет начинаться нумерация старых логов;
- **size** — размер лога, когда он будет перемещен.

По умолчанию настроено хранение четырех старых файлов журналов, создание нового пустого файла журнала после перемещения старых и использование даты ротации при создании файлов журнала.

Вспомогательные настройки

В каталоге дополнительных настроек **/etc/logrotate.d** находятся несколько файлов, по названиям и содержимому которых можно определить, к журналам какой программы они относятся:

```
ls /etc/logrotate.d/

afick  bootlog  chrony  firebird   glusterfs    libreswan  psacct   samba  wpa_supplicant
aide   btmp     dnf     firewalld  iscsiuiolog  ppp        rsyslog  sssd   wtmp
```

В файлах содержатся правила обработки отдельных журналов.

В качестве примера рассмотрим параметры файла конфигурации **bootlog**:

```
cat /etc/logrotate.d/bootlog

    /var/log/boot.log
    {
1.      missingok
2.      daily
3.      copytruncate
4.      rotate 7
5.      notifempty
    }
```

Файл состоит из одной записи, которая, в свою очередь, разделена на две части:

- *имя файла*, который нужно обрабатывать (**/var/log/boot.log**);
- *параметры обработки*, указанные в фигурных скобках.

Описание параметров обработки:

1. **missingok** – не выдавать ошибки, если лог-файла не существует;
2. **daily** – обрабатывать журнал каждый день;
3. **copytruncate** – обрезать оригинальный файл до нулевого размера после создания копии вместо переименования оригинального файла и создания нового.
4. **rotate** 7 – необходимо хранить 7 старых файлов журналов;
5. **notifempty** – не ротировать файл лога, если он пуст.

Рассмотрим ещё один файл конфигурации - **sssd**.

```
cat /etc/logrotate.d/sssd

/var/log/sssd/*.log {
    weekly
    missingok
    notifempty
    sharedscripts
    rotate 2
    compress
    delaycompress
    postrotate
        /bin/kill -HUP `cat /var/run/sssd.pid  2>/dev/null`  2> /dev/null || true
    endscript
```

Здесь та же структура, но в конфигураторе дополнительно указана команда терминала, заключенная в postrotate и endscript. Строки, находящиеся между данными служебными словами, каждое из которых должно находиться в отдельной строке, выполняются с использованием **/bin/sh** после ротации файла журнала.

Проверка конфигурации

После настройки какого-либо файла конфигурации **logrotate** желательно проверить его корректность. Для этого необходимо запустить утилиту **logrotate** с опцией **-d**, она выведет все, что планируется сделать, но не будет изменять файлы на диске.

Рассмотрим действие утилиты на примере файла **/var/log/bootlog**:

```
logrotate -d /etc/logrotate.d/bootlog

 WARNING: logrotate in debug mode does nothing except printing debug messages!  Consider using verbose mode (-v) instead if this is not what you want.

reading config file /etc/logrotate.d/bootlog
Reading state from file: /var/lib/logrotate/logrotate.status
Allocating hash table for state file, size 64 entries

Handling 1 logs

rotating pattern: /var/log/boot.log
 after 1 days (7 rotations)
empty log files are not rotated, old logs are removed
considering log /var/log/boot.log
  Now: 2024-11-15 11:46
  Last rotated at 2024-11-15 11:00
  log does not need rotating (log is empty)
```

Если сообщений об ошибках нет, можно считать, что настройка завершена успешно.

Сбор диагностической информации о РЕД ОС (loginfo)

Графический интерфейс
Консольный вариант

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** loginfo-0.15-1

loginfo – утилита сбора технической информации о РЕД ОС для технической поддержки.

Вы можете подробнее ознакомиться с работой утилиты **loginfo**, просмотрев наши обучающие видео:

- на **RuTube** — Сбор диагностической информации о РЕД ОС;
- в **Яндекс.Дзен** — Сбор диагностической информации о РЕД ОС;
- в **VK Видео** — Сбор диагностической информации о РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

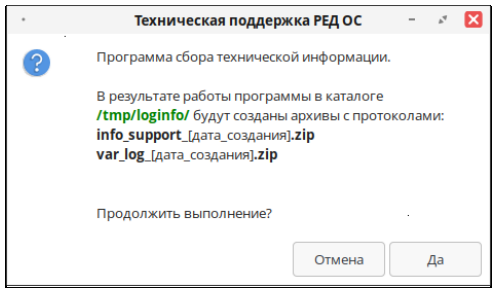
и выполните команду:

```
dnf install loginfo
```

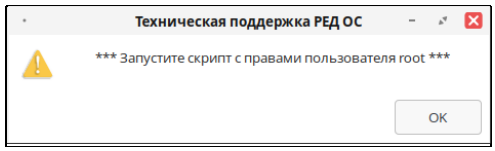
Графический интерфейс

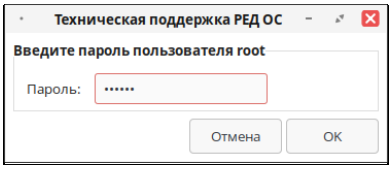
Запуск утилиты доступен из «**Главного меню**» - «**Системные**» - «**Сбор информации о системе**».

При инициализации утилиты вы увидите следующее диалоговое окно:

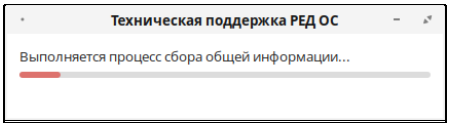


Т.к. для работы в программе необходимы права пользователя **root**, будет выведено следующее предупреждение и произведен запрос на ввод пароля пользователя **root**.



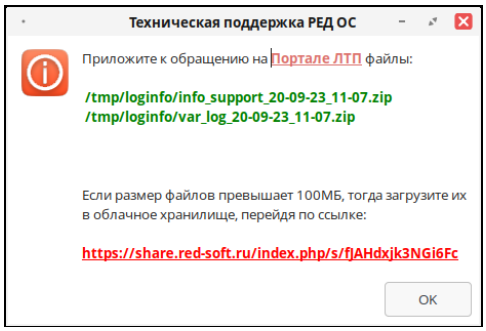


Будет запущен процесс сбора информации.



После сбора информации будет выведено информационное сообщение с контактами для отправки собранных данных в техническую поддержку.

Архивные файлы будут сформированы по пути **/tmp/loginfo**.



Консольный вариант

Для работы с утилитой необходимы права пользователя **root**:

```
su -
```

Для запуска процесса сбора информации выполните:

```
loginfo.sh
```

Loginfo также поддерживает дополнительный функционал, для просмотра выполните:

```
loginfo.sh --help
```

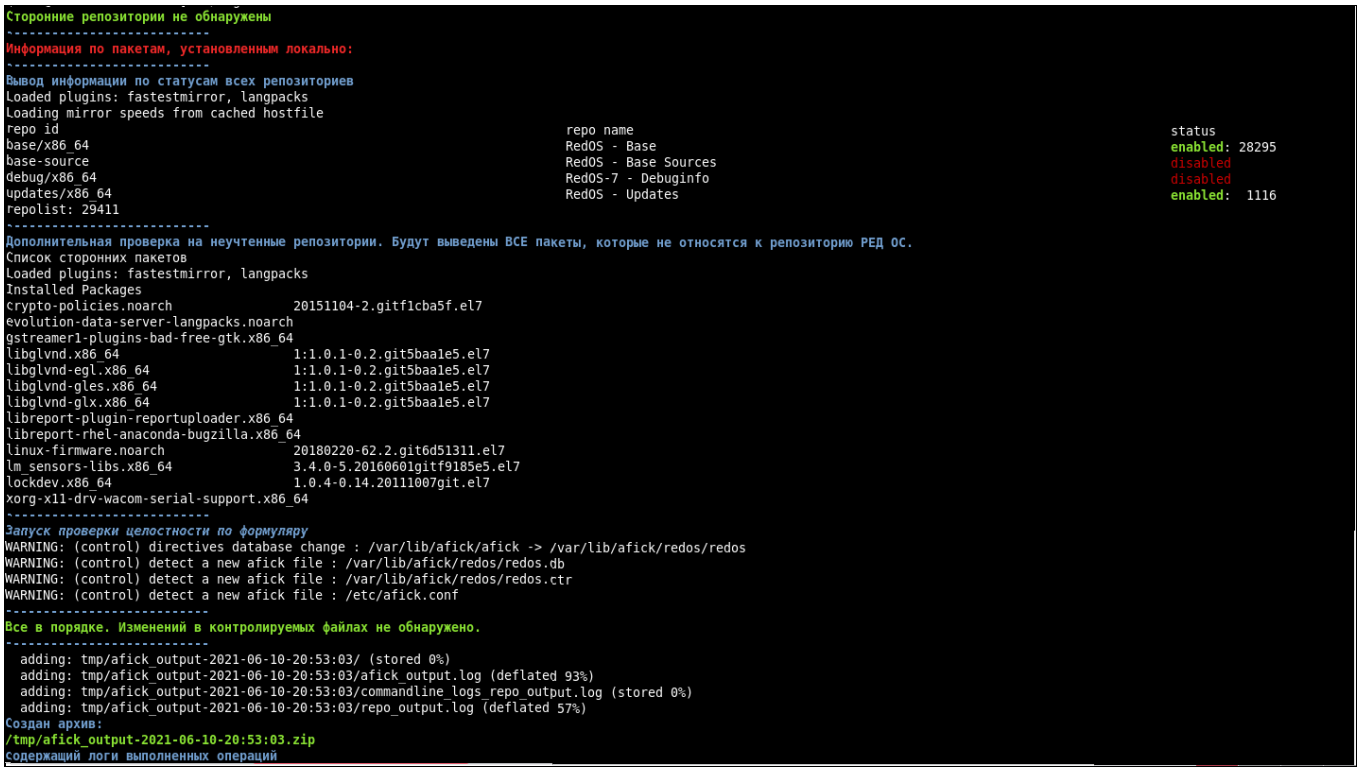
Для примера выполним дополнительную диагностику ОС.

Создание краткой сводки по аппаратным характеристикам:

```
loginfo.sh --hw-id

Создан файл /tmp/loginfo/hw-id-2022-06-21-11-50-35.txt
```

Проверка целостности сертифицированной редакции РЕД ОС:

```
loginfo.sh --afick
```



Контроль целостности системы РЕД ОС также осуществляется с помощью утилиты **afick**. Подробнее см. в нашей статье «Afick - утилита контроля целостности системы».

Настройка systemd-coredump для автоматического сбора дампов

Настройка сбора дампов
Изменение места сохранения дампов
Проверка работоспособности создания дампа
Чтение дампов ядра
Настройка сбора дампов в СУБД Ред База Данных

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: systemd-246.10-16

Дамп памяти (*core dump*) — содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы, например, значения регистров процессора и содержимое стека. Многие операционные системы позволяют сохранять дамп памяти для отладки программы. Как правило, дамп памяти процесса сохраняется автоматически, когда процесс завершается из-за критической ошибки (например, из-за ошибки сегментации). Дамп также можно сохранить вручную через отладчик или любую другую специальную программу.

Настройка сбора дампов

В РЕД ОС 7.3 для автоматического сбора дампов используется обработчик дампов **systemd-coredump** — он собирает информацию о процессе при аварийном завершении программы. Для проверки сбора дампов выполните команду:

```
cat /proc/sys/kernel/core_pattern
|/usr/lib/systemd/systemd-coredump %P %u %g %s %t %c %h
```

Размер дампов определяется в файле конфигурации **/etc/systemd/coredump.conf**. Для изменения размера дампов в секции [Coredump] необходимо раскомментировать следующие параметры:

```
Compress=yes
ProcessSizeMax=<максимальный_размер_дампов>
ExternalSizeMax=<максимальный_размер_сжатого_дампа>
```

Далее будут подробнее рассмотрены параметры конфигурационного файла:

- Storage — определяет место хранения дампа процесса, может принимать одно из значений: *none*, *external*, *journal*.
  - *none* — дампы ядра записываются (включая обратную трассировку, если возможно), но не сохраняются;
  - *external* — значение по умолчанию, дампы сохраняются в каталоге **/var/lib/systemd/coredump/**;
  - *journal* — дампы будут храниться в журнале и перезаписываться в соответствии со стандартными принципами ротации журналов.
- Compress — используется для сжатия дампов ядра. Принимает логический аргумент — *yes* или *no*:
  - *yes* — дампы сжимаются при сохранении (значение по умолчанию);
  - *no* — дампы сохраняются без сжатия.
- ProcessSizeMax — определяет максимальный размер дампа процесса, который может быть сохранен. Если размер дампа превышает значение этого параметра, то дамп сохранен не будет. Это позволяет ограничить размер дампов и избежать переполнения дискового пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *до 1ГБ* — в 32-битных системах, *32ГБ* — в 64-битных системах. Параметры Storage=none и ProcessSizeMax=0 отключает всю обработку дампа памяти, за исключением записи журнала.
- ExternalSizeMax и JournalSizeMax — определяет максимальный (сжатый или несжатый) размер дампа процесса, который будет сохранен на диске (по умолчанию *1 ГБ* — в 32-разрядных системах, *2 ГБ* — в 64-разрядных системах), или в журнале системы (по умолчанию 10M).
- MaxUse — определяет максимальный объем общего дискового пространства, который может быть использован для хранения дампов процессов. Если общий размер всех дампов превышает значение этого параметра, старые дампы будут удаляться для освобождения места для новых. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию ограничение равно *10% от общего размера диска*.
- KeepFree — определяет минимальный объем свободного дискового пространства, который должен оставаться на диске при хранении дампов. Если свободного места на диске становится меньше указанного значения, новые дампы не будут создаваться

до тех пор, пока не будет предоставлено достаточного объема свободного пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *15% от общего размера диска* должно оставаться свободным. Старые дампы ядра также удаляются в зависимости от времени с помощью **systemd-tmpfiles**.

Изменение места сохранения дампов

Дампы по умолчанию будут создаваться в каталоге **/var/lib/systemd/coredump**. Служба **systemd-coredump** не имеет параметра конфигурации для изменения каталога, в котором будут храниться дампы.

Для смены каталога создания дампов необходимо использовать **bind-mount**:

1. В файле **/etc/fstab** пропишите монтирование нужной директории для сохранения дампов следующим образом:

```
/каталог/для/дампов /var/lib/systemd/coredump none defaults,bind 0 0
```

2. Примонтируйте каталог:

```
mount /var/lib/systemd/coredump
```

3. Перезапустите службу **systemd** для применения изменений:

```
systemctl daemon-reload
```

Проверка работоспособности создания дампа

Для проверки создания дампа необходимо выполнить в терминале:

```
sleep 3600 &
kill -11 %1
```

Проверьте создание дампа с помощью утилиты **coredumpctl**:

```
coredumpctl
```

Рассмотрим дополнительные опции **coredumpctl**:

- **list** — список доступных дампов ядра;
- **info <PID>** — вывод подробной информации об указанном дампе ядра;
- **gdb <файл>** — запускает отладчик **gdb** (GNU Debugger) для анализа дампа ядра;
- **dump <PID>** — создает дамп ядра с указанным идентификатором (PID). Дамп ядра будет передан на стандартный вывод, если не указан выходной файл с помощью **--output=**;
- **debug <PID>** — запуск процесса с указанным PID в режиме отладки. По умолчанию используется **gdb**. Отладчик может быть изменен с помощью параметра **--debugger=** или переменной среды **$SYSTEM_DEBUGGER**. Для передачи отладчику дополнительных аргументов командной строки используется параметр **--debugger-arguments=**.

Чтение дампов ядра

Сводную информацию о дампе ядра, соответствующем определенному процессу, в котором произошел сбой, можно получить, выполнив команду:

```
coredumpctl info _PID=<PID_процесса,по_которому_создан_дамп>
```

```
[user@localhost ~]$ coredumpctl info _PID=2772
           PID: 2759 (bash)
           UID: 1000 (user)
           GID: 1000 (user)
        Signal: 6 (ABRT)
     Timestamp: Fri 2023-03-31 11:46:40 MSK (20min ago)
  Command Line: bash 1212.sh
    Executable: /usr/bin/bash
 Control Group: /user.slice/user-1000.slice/session-2.scope
          Unit: session-2.scope
         Slice: user-1000.slice
       Session: 2
     Owner UID: 1000 (user)
       Boot ID: df6eee73274847bf9b977b2b77d47391
    Machine ID: 1e8ddb949cf549d8a2785068c77b85cd
      Hostname: localhost.localdomain
       Storage: /var/lib/systemd/coredump/core.bash.1000.df6eee73274847bf9b977b2b77d47391.2759.16802
       Message: Process 2759 (bash) of user 1000 dumped core.

                Stack trace of thread 2759:
                #0  0x00007fe88a6e715b __waitpid (libc.so.6 + 0xcc15b)
                #1  0x0000000000451619 waitchld.isra.12 (bash + 0x51619)
                #2  0x000000000052dfa wait_for (bash + 0x52dfa)
                #3  0x000000000043fbd7 execute_command_internal (bash + 0x3fbd7)
                #4  0x000000000043fe76 execute_command (bash + 0x3fe76)
                #5  0x0000000000426a21 reader_loop (bash + 0x26a21)
                #6  0x0000000000425144 main (bash + 0x25144)
                #7  0x00007fe88a642413 __libc_start_main (libc.so.6 + 0x27413)
                #8  0x00000000004256ce _start (bash + 0x256ce)
lines 1-28/28 (END)
```

Для полного чтения дампа необходимо установить утилиту **gdb**, выполнив команду (с правами суперпользователя **root** или администратора системы):

```
dnf install gdb
```

Запустите анализ дампа, выполнив команду:

```
coredumpctl gdb _PID=<PID_процесса,по_которому_создан_дамп>
```

```
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/bash...

warning: Unable to open "librpm.so.8" (librpm.so.8: cannot open shared object file: No such file or d
irectory), missing debuginfos notifications will not be displayed
Missing separate debuginfo for /usr/bin/bash
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/58/dbe494d53a3772d3e6f32b6c97e5b573
228ef.debug
Reading symbols from .gnu_debugdata for /usr/bin/bash...
(No debugging symbols found in .gnu_debugdata for /usr/bin/bash)
[New LWP 2759]
Missing separate debuginfo for /lib64/libiniparser.so.1
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/8c/f382586277a70f91a9befa609e0e1393
4ee12.debug
Missing separate debuginfo for /lib64/libtinfo.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/b7/b929fb355f28f374b5054d3191fc05a7
b5802.debug
Missing separate debuginfo for /lib64/libdl.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/e7/e6d7db0bca11a7f7da45896c9165d369
d14ab.debug
Missing separate debuginfo for /lib64/libc.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/75/b55efed6938ccb77e0e40fff7571aae0
ffcc0.debug
Missing separate debuginfo for /lib64/ld-linux-x86-64.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/73/db0afd7ec02589302cf7bd90ae12d482
6a6e3.debug
Core was generated by `bash 1212.sh'.
Program terminated with signal SIGABRT, Aborted.
#0  0x00007fe88a6e715b in waitpid () from /lib64/libc.so.6
(gdb)
```

Настройка сбора дампов в СУБД Ред База Данных

Для сбора дампов *СУБД Ред База Данных* необходимо в файл службы **/usr/lib/systemd/system/firebird.service** в секцию [Service] добавить строку:

```
LimitCORE=infinity
```

Для этого необходимо воспользоваться редактированием модуля юнита с помощью команды:

```
systemctl edit firebird
```

И добавить следующие строки:

```
[Service]
LimitCORE=infinity
```

После сохранения сформируется файл **/etc/systemd/system/firebird.service.d/override.conf**.

При загрузке модуля **systemd** в памяти соединит фрагмент сформированного файла (**/etc/systemd/system/firebird.service.d/override.conf**) с полным файлом модуля (**/usr/lib/systemd/system/firebird.service**). Директивы фрагмента получат приоритет над найденными директивами в оригинальном файле модуля. Для проверки всех подгружаемых фрагментов необходимо выполнить:

```
systemctl cat firebird
```

Если СУБД при работе потребляет большой объем памяти (настроен большой страничный кэш), то создание дампа на диске после падения может продолжаться некоторое время. В конфигурационном файле службы **coredump** может быть настроен таймаут работы, после которого она будет остановлена. Для того чтобы времени на создание дампа было достаточно, необходимо увеличить таймаут, например, до 30 минут, изменив значение параметра `RuntimeMaxSec` в файле **/usr/lib/systemd/system/systemd-coredump@.service**:

```
RuntimeMaxSec=30min
```

ВАЖНО!

Дампы ядра полезны для устранения неполадок, однако могут являться причиной “утечки” конфиденциальных данных. Рекомендуется отключать дампы ядра и включать их только тогда, когда это действительно необходимо.

Для отключения сбора дампов ядра необходимо остановить службу **systemd-coredump**:

```
systemctl disable systemd-coredump
systemctl stop systemd-coredump
```

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС

Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

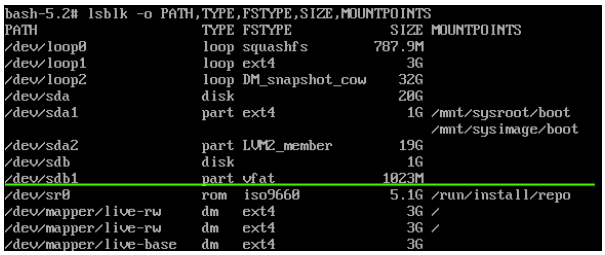
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

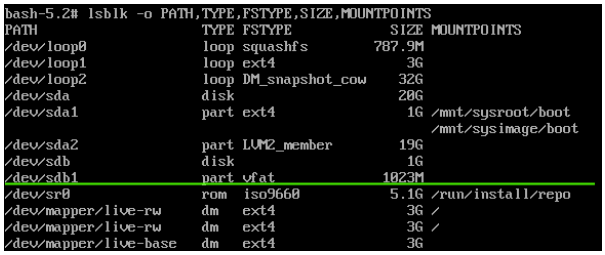
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Рекомендации по анализу журналов и дампов

1. Системные журналы событий ОС находятся в каталоге **/var/log/**, также можно использовать утилиту **journalctl** для просмотра журналов.

Подробную информацию по работе с утилитой **journalctl** см. в нашей статье «Работа с логами (утилита journalctl)».

Пример фильтрации содержимого журнала по типу ошибок:

```
journalctl -p err
journalctl -p alert
```

2. При анализе логов следует обращать внимание на ключевые слова, которые фигурируют в строках журналов:

- **failed** – обычно указывает на неудачное выполнение какой-либо операции или задачи. Например, сообщение вида authentication failed означает, что аутентификация завершилась неудачно;
- **error** – указывает на наличие ошибки. Далее может быть расшифровка ошибки и представлен ее код;
- **panic** – может появиться в записях, связанных с *Kernel Panic*, ошибками ядра Linux;
- **exception** – указывает на исключения (нештатную ситуацию или ошибку, которую программа или ядро не может обработать) в приложениях или ядре;
- **segfault** – ошибка сегментации, указывает на попытку доступа к памяти, к которой нет разрешения;
- **denied** – указывает на отказ в доступе, например, сообщение вида permission denied может быть связано с проблемами в правах доступа;
- **unable** – такие записи могут указывать на неспособность системы выполнить какое-либо определенное действие;
- **timeout** – задержки и таймауты могут указывать на проблемы с сетью или системными ресурсами;
- **crash** – аварийное завершение приложений или служб;
- **warning** – предупреждение о потенциальных проблемах, которые не вызывают сбоев, но требуют внимания;
- **critical** – критические события;
- **fatal** – критическая ошибка, которая приводит к сбою;
- **corruption** – обычно указывает на повреждение данных или файлов.

3. После определения кода или названия ошибки, которая связана со сбоем, уточняется ее более подробное описание, возможные причины возникновения, способы устранения. Поиск осуществляется в общедоступных поисковых системах, в системах отслеживания ошибок (*Bug tracking system*) по исследуемому компоненту или программе, а также соответствующим запросом в Техническую Поддержку программного продукта, в котором произошел инцидент.

4. Инструкция по работе с **coredump** — «Настройка systemd-coredump для автоматического сбора дампов».

5. Инструменты для анализа логов:

- средство просмотра файлов журналов **lnav** — «Средство просмотра журналов Log File Navigator (LNAV)»;
- веб-приложение для просмотра логов **loganalyzer** — «LogAnalyzer – веб-приложение для просмотра системных журналов».

Командные оболочки (интерпретаторы)

Для управления ОС используется командные интерпретаторы (shell). Зайдя в систему, пользователь увидит приглашение - строку, содержащую символ «$» (далее этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора - передавать команды пользователя операционной системе. При помощи командных интерпретаторов можно писать небольшие программы - сценарии (скрипты). Оболочкой по умолчанию в РЕД ОС является «**Bash**» (Bourne Again Shell) Чтобы проверить, какая оболочка используется, необходимо выполнить команду:

```
echo $SHELL
```

Вы можете подробнее ознакомиться с возможностями работы **bash**, просмотрев наши обучающие видео:

- на **RuTube**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **Яндекс.Дзен**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.
- в **VK Видео**:
    - Что такое bash;
    - Команды в bash;
    - Понятие о сценариях оболочки bash;
    - Ветвления, циклы, функции в сценариях bash.

На наших каналах вы также сможете найти много другой полезной информации.

Командная оболочка Bash

В bash имеется несколько приемов для работы со строкой команд. Например, используя клавиатуру, можно:

- **Ctrl + A** - перейти на начало строки;
- **Ctrl + U** - удалить текущую строку;
- **Ctrl + C** - остановить текущую задачу.

Можно использовать «;» для того, чтобы ввести несколько команд одной строкой. Клавиши «вверх» и «вниз», позволяют вам перемещаться по истории команд.

Для того чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, необходимо набрать:

Ctrl + R

Команды, присутствующие в истории, отображаются в списке пронумерованными. Для того, чтобы запустить конкретную команду, наберите:

```
! <номер_команды>
```

если ввести:

```
!!
```

запустится последняя из набранных команд. Иногда имена программ и команд слишком длинны. Bash сам может завершать имена. Нажав клавишу [TAB], можно завершить имя команды, программы или каталога. Например, предположим, что необходимо использовать программу декомпрессии bunzip2. Для этого нужно набрать:

```
bu
```

затем нажать [TAB]. Если ничего не происходит, то, вероятно, существует несколько возможных вариантов завершения команды.

Нажав клавишу [TAB] еще раз, пользователь получит список имен, начинающихся с «bu». Например, может быть:

```
bu buildhash builtin bunzip2
```

Если далее добавить:

n

(bunzip - это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу [TAB], оболочка дополнит имя и остается лишь нажать «Enter», чтобы запустить команду. Программу, вызываемую из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH.

По умолчанию, в этот перечень каталогов не входит текущий каталог, обозначаемый «./» (точка слэш), поэтому для запуска программы **prog** из текущего каталога, надо дать команду:

```
./prog
```

Базовые команды оболочки Bash

Все команды, приведенные ниже, могут быть запущены в режиме консоли. Для получения более подробной информации используйте команду **man.**Пример:

```
man ls
```

Команда su

Позволяет получить права администратора. Когда пользователь набирает su, оболочка запрашивает пароль суперпользователя (root). Необходимо ввести пароль и нажать **Enter**. Чтобы вернуться к правам основного пользователя, необходимо набрать **exit**.

Команда cd

Позволяет сменить каталог. Она работает как с абсолютными, так и с относительными путями. Предположим, что, находясь в своем домашнем каталоге, пользователь хочет перейти в его подкаталог **docs/**. Для этого нужно ввести относительный путь:

```
cd docs/
```

Чтобы перейти в каталог **/usr/bin** , нужно набрать (абсолютный путь):

```
cd /usr/bin/
```

Некоторые варианты команды:

```
cd ..
```

позволяет сделать текущим родительский каталог,

```
cd -
```

позволяет вернуться в предыдущий каталог. Команда cd без параметров переводит в домашний каталог.

Команда ls

ls (list) выдает список файлов в текущем каталоге. Синтаксис:

```
ls
```

Две основные опции:

- -a - просмотр всех файлов, включая скрытые,
- -l - отображение более подробной информации.

Команда rm

Эта команда используется для удаления файлов. Синтаксис:

```
rm <имя_файла>
```

У данной программы существует ряд параметров. Самые часто используемые:

- -i - запрос на удаление файла,
- -r - рекурсивное удаление (т.е. удаление, включая подкаталоги и скрытые файлы).

Команды mkdir и rmdir

Команда **mkdir** позволяет создать каталог, тогда как **rmdir** удаляет каталог, при условии, что он пуст. Синтаксис:

```
mkdir <имя_каталога>
```

```
rmdir <имя_каталога>
```

Команда **rmdir** часто заменяется командой **rm-rf** , которая позволяет удалять каталоги, даже если они не пусты.

Команда less

less позволяет постранично просматривать текст.

Синтаксис:

```
less <имя_файла>
```

Для выхода нужно нажать q.

Команда grep

Данная команда имеет много опций и предоставляет возможности поиска символьной строки в файле.

Синтаксис:

```
grep <шаблон_поиска> <файл>
```

Команда ps

Отображает список текущих процессов. Колонка команд указывает имя процесса, колонка PID (идентификатор процесса) - номер процесса (этот номер используется для операций с процессом, например чтобы «убить» его командой **kill**).

Синтаксис:

```
ps <аргументы>
```

Аргумент -u предоставляет больше информации, а -x позволяет просмотреть те процессы, которые не принадлежат пользователю (такие как те, что были запущены во время процесса загрузки).

Команда kill

Если программа перестала отвечать или зависла, необходимо использовать данную команду, чтобы её завершить.

Синтаксис:

```
kill <PID_номер>
```

Иногда необходимо будет использовать **kill -9** (когда обычная команда **kill** не дает желательного эффекта). Номер PID выясняется при помощи команды **ps**.

Горячие комбинации клавиш в Bash

Для удобства запоминания сочетания клавиш сгруппированы по действию. Обратите внимание, что **в комбинациях следует использовать левую клавишу Alt**, т.к. правая Alt Gr используется как клавиша Compose (специальная клавиша, позволяющая вводить символы с помощью определённых комбинаций клавиш).

Перемещение по тексту

Сочетание	Действие
Ctrl+a, Home	Переместить курсор в начало командной строки
Ctrl+e, End	Переместить курсор в конец командной строки
Ctrl+b, ←	Переход на один символ назад от курсора
Ctrl+f, →	Переход на один символ вперёд от курсора
Alt+b, Esc+b	Переместить курсор назад на одно слово
Alt+f, Esc+f	Переместить курсор вперёд на одно слово
Ctrl+xx	Переход от курсора в начало строки и обратно

Редактирование строки

Сочетание	Действие
Alt+?, Tab+Tab	Автодополнение команды или имени файла
Ctrl+u	Удалить все символы от курсора до начала командной строки
Ctrl+k	Удалить все символы от курсора до конца командной строки
Ctrl+w	Удалить символы от курсора до пробела слева
Alt+Backspace	Удалить символы от курсора до начала слова
Alt+d, Esc+d	Удалить символы от курсора до конца слова
Ctrl+y	Вставить символ, слово или текст, которые были удалены при помощи сочетаний клавиш, приведенных выше
Alt+y	Просмотреть буфер удалённых слов и вставить интересующее. Работает после нажатия Ctrl+y
Ctrl+h	Удалить перед курсором один символ
Ctrl+d	Удалить под курсором один символ
Alt+	Удалить любое количество пробелов вокруг курсора
Ctrl+_	Откатить редактирование
Alt+r, Esc+r	Отменить все изменения содержимого строки
Alt+c	Заменяет под курсором букву на заглавную и переводит курсор в конец слова
Alt+u	Переводит все буквы от курсора и до конца слова в заглавные
Alt+l	Переводит все буквы от курсора и до конца слова в нижний регистр
Alt+t	Замена текущего слова под курсором на предыдущее слово
Ctrl+t	Замена символа перед курсором на предыдущий символ

История команд

Сочетание	Действие
Ctrl+r	Искать команду по истории

Ctrl+g	Выйти из режима поиска в истории
Ctrl+p, ↑	Предыдущая команда в истории
Ctrl+n, ↓	Следующая команда в истории
Alt+<	Переход к первой команде в буфере истории
Alt+., Esc+.	Вставить последний аргумент предыдущей команды
Ctrl+o	Выполняет введённую команду и оставляет её же в командной строке

Выполнение и вывод на экран

Сочетание	Действие
Ctrl+l	Очистка экрана
Ctrl+s	Остановить вывод на экран
Ctrl+q	Возобновить вывод на экран, если он был приостановлен указанной выше командой
Ctrl+c	Прервать выполнение текущей команды
Ctrl+z	Приостановить выполнение текущей команды (для возобновления выполните fg)
Ctrl+d	Выйти из командной оболочки Bash

Информационный вывод

Сочетание	Действие
***+Alt+?, *+Tab+Tab**	Показать каталоги, кроме скрытых
$+Alt+?, $+Tab+Tab	Показать все системные переменные

Специальные клавиши

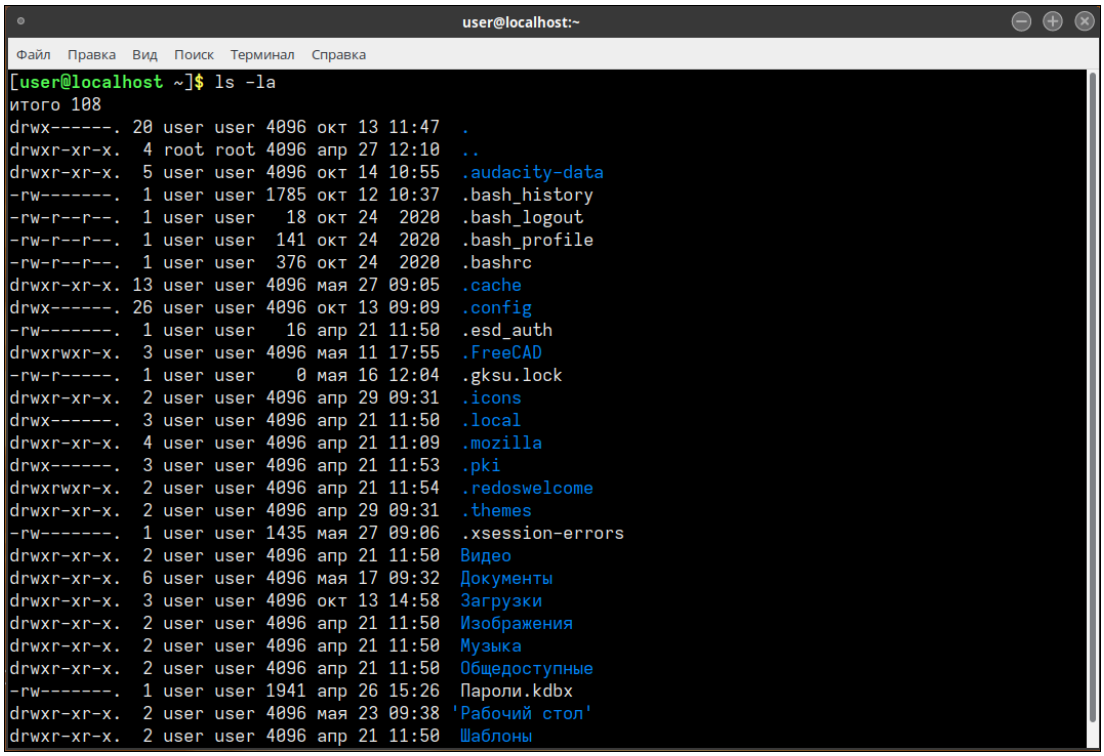
Сочетание	Действие
Ctrl+i	Tab
Ctrl+m	Enter
Ctrl+[	Esc

Основные утилиты в консоли РЕД ОС

ls

Утилита для просмотра содержимого каталогов. По умолчанию показывает содержимое текущего каталога. Если в параметрах указан путь к каталогу, она перечислит содержимое конечного каталога. Полезные опции:

- **-l** (list) - форматирует вывод в виде списка с более подробной информацией;
- **-a** (--all) - включает показ скрытых файлов;
- **--help** - вывести справку по использованию утилиты.

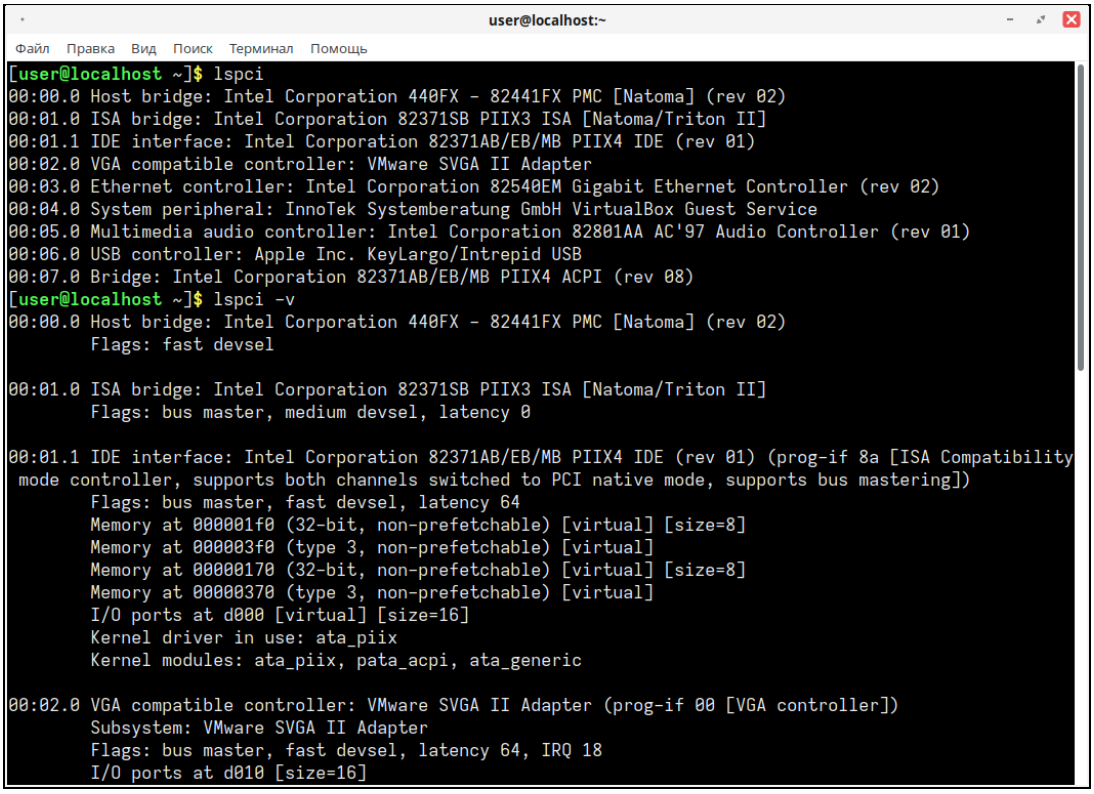


lspci

Команда **lspci** позволяет задействовать одноименную утилиту, предназначенную для вывода информации о PCI-шинах и подключенных к ним устройствах. Она поддерживает все разновидности PCI-шин: классическую шину **PCI** (Peripheral Component Interconnect), ее серверный вариант **PCI-X** и ее современный вариант **PCIe** (PCI-Express). Обычно к данной шине подключаются такие устройства, как графические, звуковые и сетевые карты, Wi-Fi и Bluetooth-адаптеры, SSD-накопители, а также множество других устройств.

Наиболее полезные опции:

- **-m** и **-mm** — для вывода установленных производителем идентификаторов устройств;
- **-t** — для вывода информации в древовидном формате;
- **-v** — для вывода подробной информации об устройствах;
- **-n** — для вывода идентификаторов устройств;
- **-s** и **-d** — для вывода информации об устройствах в заданных слотах и с заданными идентификаторами соответственно.



lsusb

Команда lsusb позволяет задействовать одноименную утилиту, предназначенную для вывода информации о USB-шинах и подключенных к ним устройствах. Каждое из устройств имеет пару 16-битных идентификаторов: идентификатор производителя (**Vendor ID**) и идентификатор устройства (**Device ID**), которые следует использовать для идентификации устройств и поиска драйверов в случае их отсутствия в ядре ОС, а также несколько дополнительных идентификаторов, устанавливаемых производителем.

```
[user@localhost ~]$ lsusb
Bus 002 Device 003: ID 062a:4101 MosArt Semiconductor Corp. Wireless Keyboard/Mouse
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
[user@localhost ~]$
```

lsmod

Команда **lsmod** показывает, какие модули ядра загружены в системе в данный момент.

```
[user@localhost ~]$ lsmod
Module                  Size  Used by
snd_hrtimer            16384  1
nf_conntrack_netlink    53248  0
xt_addrtype            16384  2
br_netfilter           32768  0
xt_conntrack           16384  3
ipt_REJECT             16384  4
nf_reject_ipv4         16384  1 ipt_REJECT
nft_compat             20480  18
nft_chain_nat          16384  4
nf_tables             294912  337 nft_compat,nft_chain_nat
nfnetlink              20480  4 nft_compat,nf_conntrack_netlink,nf_tables
xt_CHECKSUM            16384  3
iptable_mangle         16384  1
xt_MASQUERADE          20480  8
xt_comment             16384  8
iptable_nat            16384  1
nf_nat                 57344  3 nft_chain_nat,iptable_nat,xt_MASQUERADE
nf_conntrack          167936  4 xt_conntrack,nf_nat,nf_conntrack_netlink,xt_MASQUERADE
nf_defrag_ipv6         24576  1 nf_conntrack
nf_defrag_ipv4         16384  1 nf_conntrack
bridge                360448  1 br_netfilter
stp                    16384  1 bridge
```

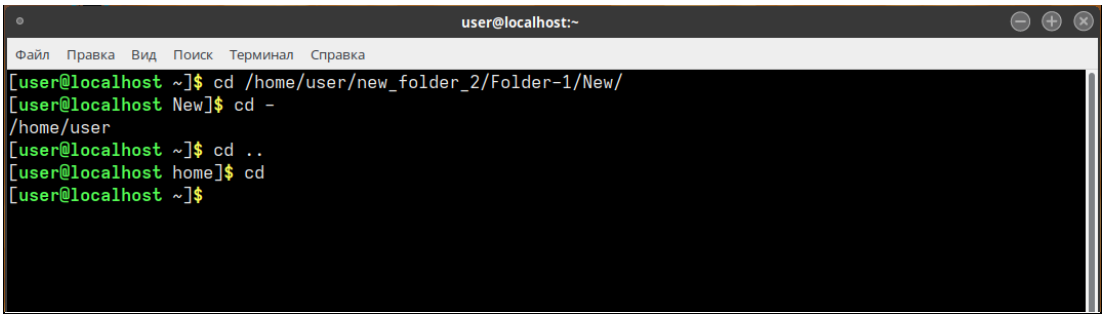
cat

Печатает содержимое файла, переданного в параметре, в стандартный вывод. Если передать несколько файлов, команда объединит их. Также можно перенаправить вывод в ещё один файл с помощью символа « **>** ».



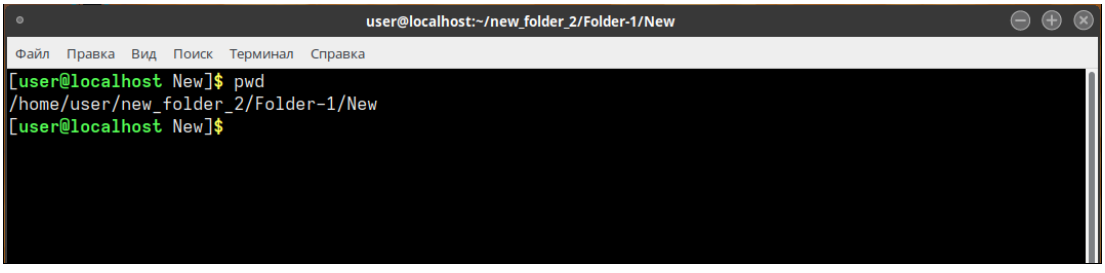
cd

Позволяет перейти из текущего каталога в указанный. Если запустить без параметров - возвращает в домашний каталог. Вызов с двумя точками (**cd ..**) - возвращает на уровень выше относительно текущего каталога. Вызов с тире (**cd -**) возвращает к предыдущему каталогу.



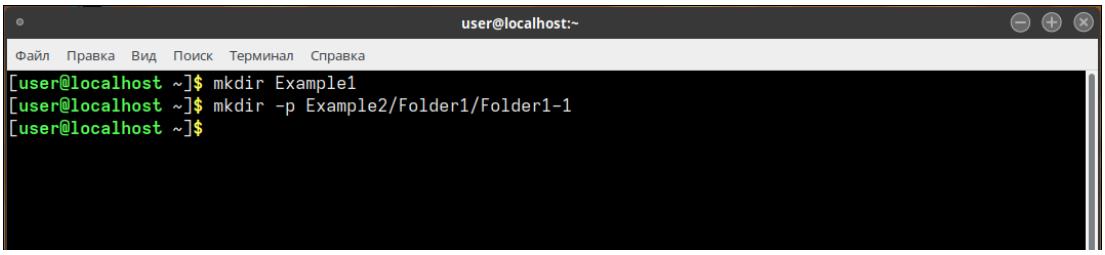
pwd

Выводит полный путь к текущему/рабочему каталогу.



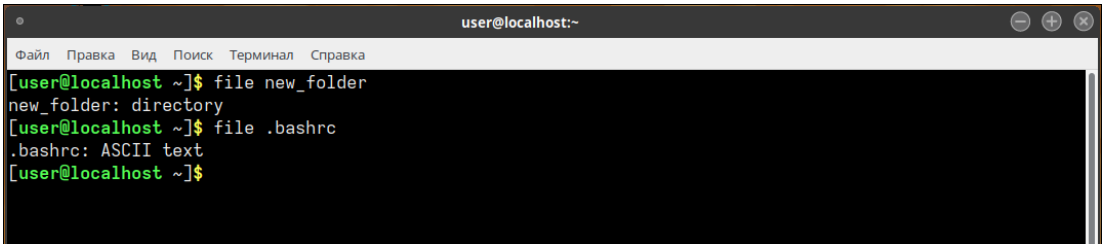
mkdir

Создание новых каталогов. Наиболее удобная опция **-p** (parents), позволяет создать всю структуру подкаталогов одной командой, даже если они ещё не существуют.



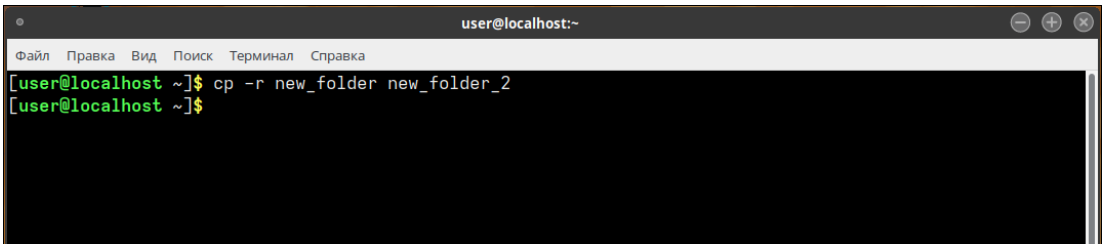
file

Показывает тип файла. В Linux файлы не обязаны всегда иметь расширения для того, чтобы с ними работать. Поэтому пользователю иногда трудно определить, какой именно перед ним файл. Данная утилита решает такую проблему.



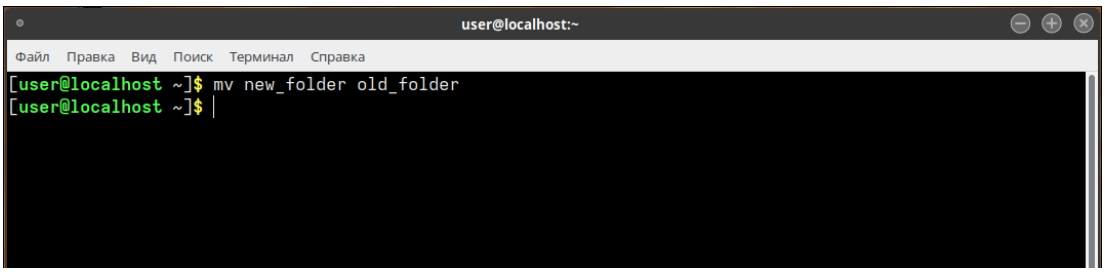
cp

Копирование файлов и каталогов. Утилита по умолчанию не копирует каталоги рекурсивно, поэтому необходимо добавить опцию **-r** (recursive) или **-a** (archive). Последняя включает режим сохранения атрибутов, владельца и временного штампа в дополнение к рекурсивному копированию.



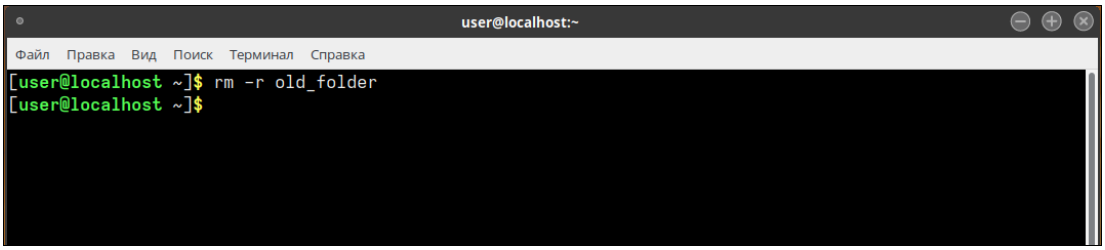
mv

Перемещение или переименование файлов и каталогов. В Linux это одна и та же операция. Переименование - это перемещение файла в ту же папку с другим именем.



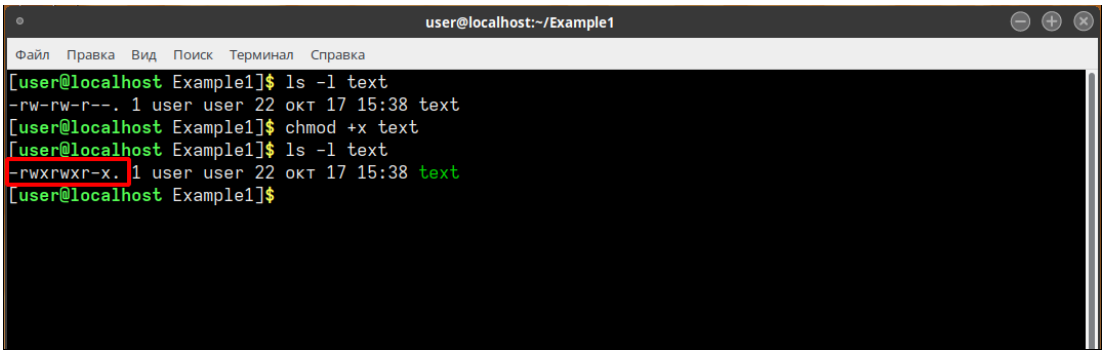
rm

Удаляет файлы и папки. Если нужно рекурсивное удаление, используйте опцию **-r**. **Rm** удаляет файлы не в корзину, из которой потом данные можно будет восстановить, а полностью их стирает. Действия оператора **rm** необратимы.



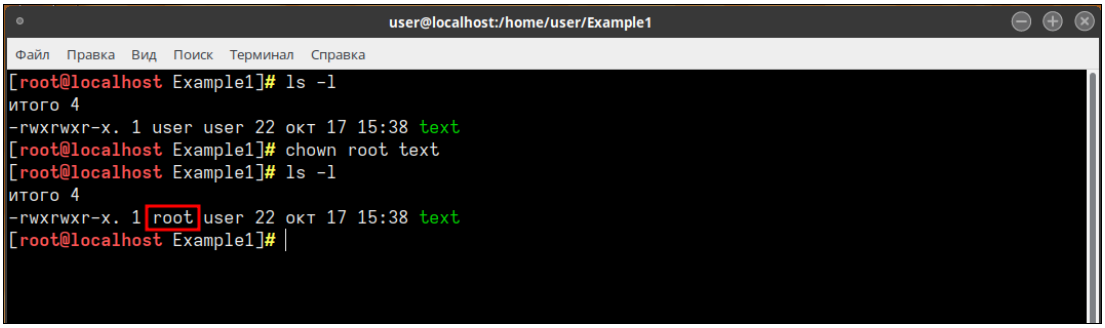
chmod

Изменяет права доступа к файлу - чтение, запись и выполнение. Каждый пользователь может изменять права для своих файлов.



chown

Изменяет владельца файла. Только суперпользователь может изменять владельцев. Для рекурсивного изменения используйте опцию **-R**.

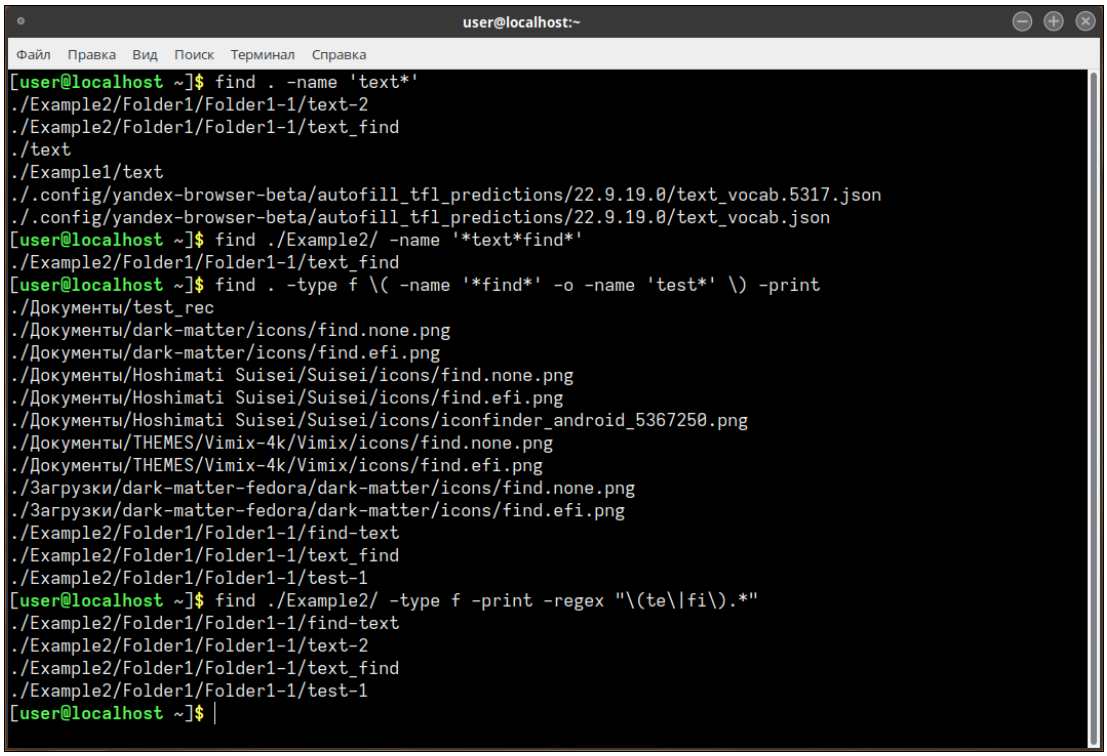


find

Очень гибкая и мощная команда Linux не только из-за своих способностей удобного поиска, но и благодаря возможности выполнять произвольные команды для найденных файлов. Поиск может осуществляться как в одном, так и в нескольких каталогах, имеется поддержка регулярных выражений для более точного поиска.

Основные опции:

- **-type** [f=файл, d=каталог (directory), l=ссылка (link), p=канал (pipe), s=сокет] - поиск по типу файла;
- **-name** '<имя_файла>' - поиск по имени файла, можно использовать как полное имя, так и его часть ('text' или 'te*');
- **-regex** "<регулярное_выражение>" - поиск файлов по регулярному выражению;
- **-print** - показать на экране найденные файлы.

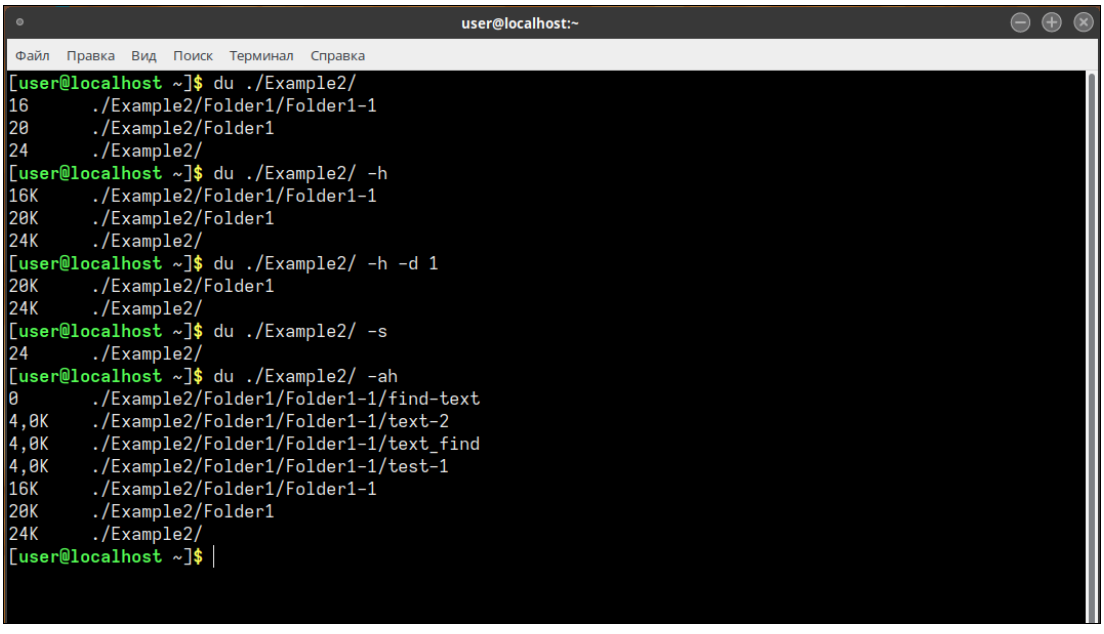


du

Показывает размер файла или каталога для оценки занимаемого файлового пространства.

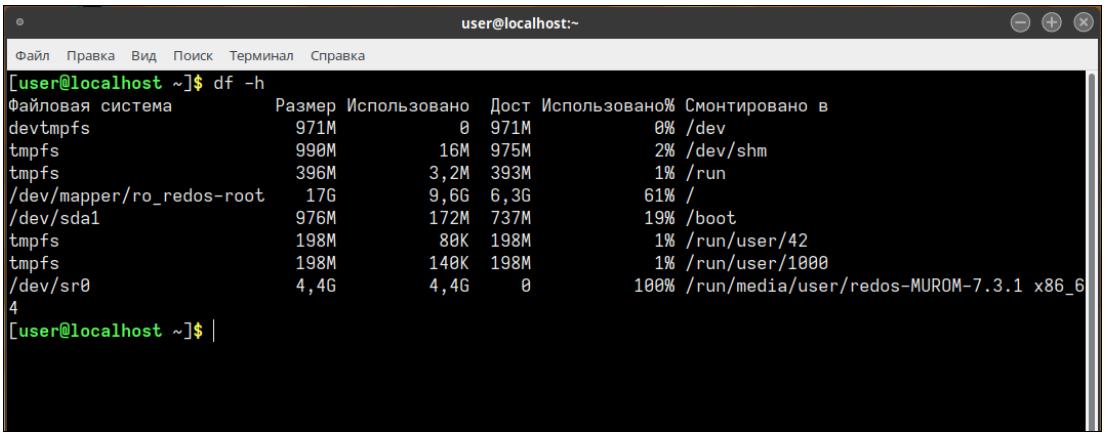
Полезные опции:

- **-a** (--all) - выводить размер для всех файлов, а не только для директорий, по умолчанию размер выводится только для папок;
- **-d** (--max-depth) - максимальная глубина вложенности директорий;
- **-h** (--human-readable) - преобразует размеры файлов в удобный формат;
- **-s** (--summarize) - выводит минимум данных.



df

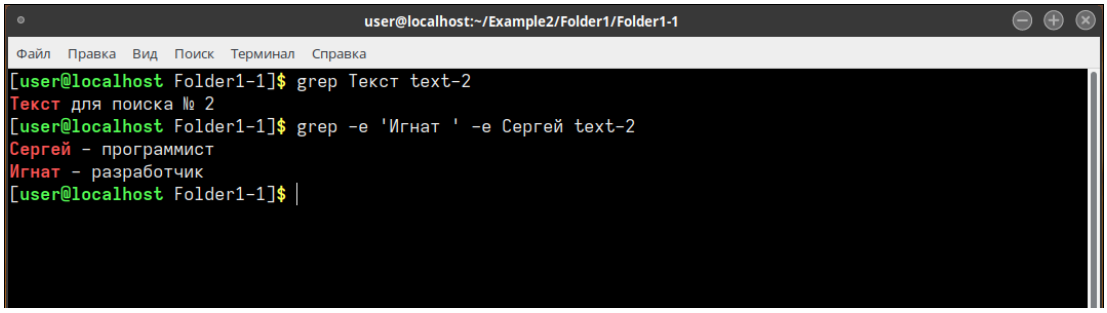
Используется для получения полной сводной информации о доступном и используемом дисковом пространстве файловой системы. По умолчанию вывод достаточно подробный: перечислены все файловые системы, их размер, количество использованного и свободного пространства. Для удобства можно использовать опцию **-h**, которая отобразит размеры удобными для чтения.



grep

Утилита **grep** ищет заданный шаблон или регулярное выражение из стандартного ввода или файла и печатает соответствующие заданным критериям строки. Утилита может вывести как полностью совпадающие, так и частично совпадающие строки и их контекст.

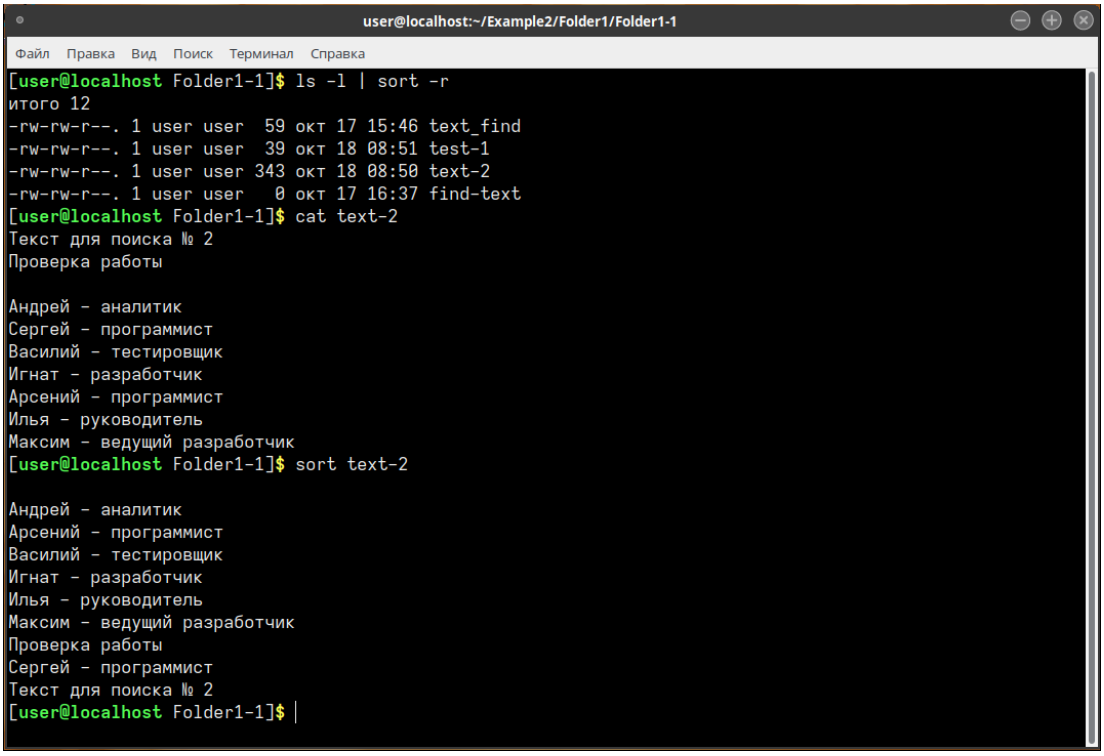
Команде **grep** также можно передавать и несколько параметров. Для этого перед каждым аргументом пишется ключ **-e**. Эту команду система понимает, как "или-или" и выводит все вхождения указанных слов. Кавычками выделяются только строки, содержащие пробел.

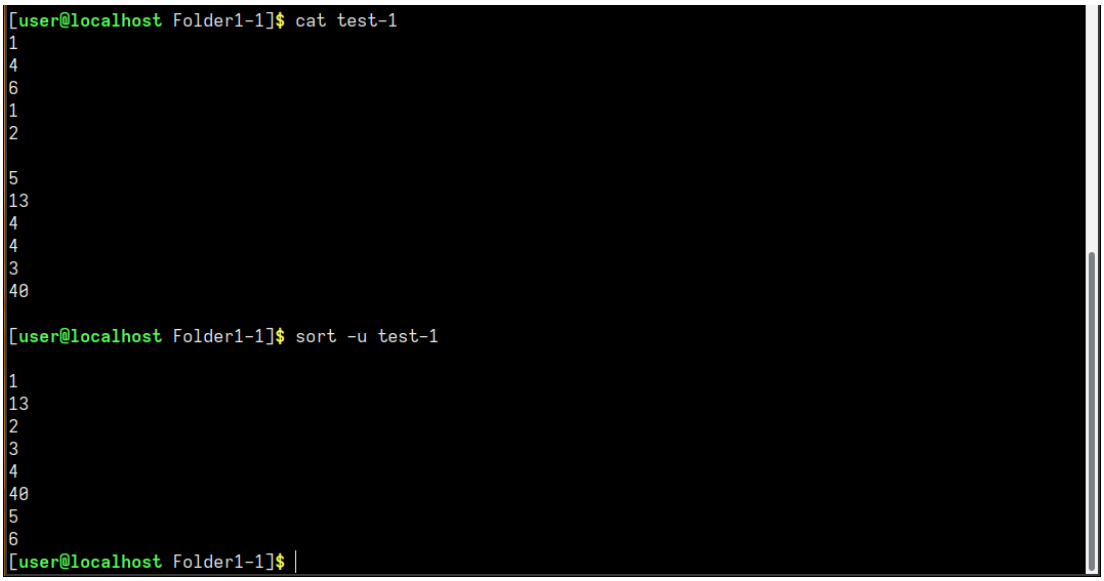


sort

Сортировка строк текста из одного или нескольких файлов по различным критериям, также может быть выполнена сортировка для вывода какой-либо команды. Наиболее полезные опции:

- **-b** - не учитывать пробелы;
- **-c** - проверить был ли отсортирован файл;
- **-n** (numeric) - сортирует по числовому значению;
- **-o** - вывести результат в файл;
- **-u** - игнорировать повторяющиеся строки
- **-r** (reverse) - сортирует в обратном порядке.



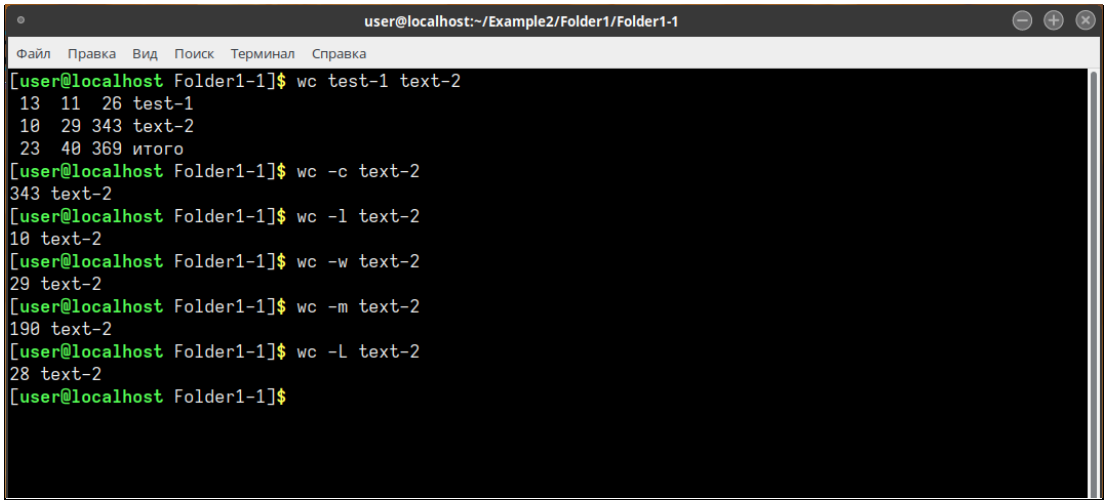


wc

Выводит число переводов строк, слов и байт для каждого указанного файла и итоговую строку, если было задано несколько файлов.

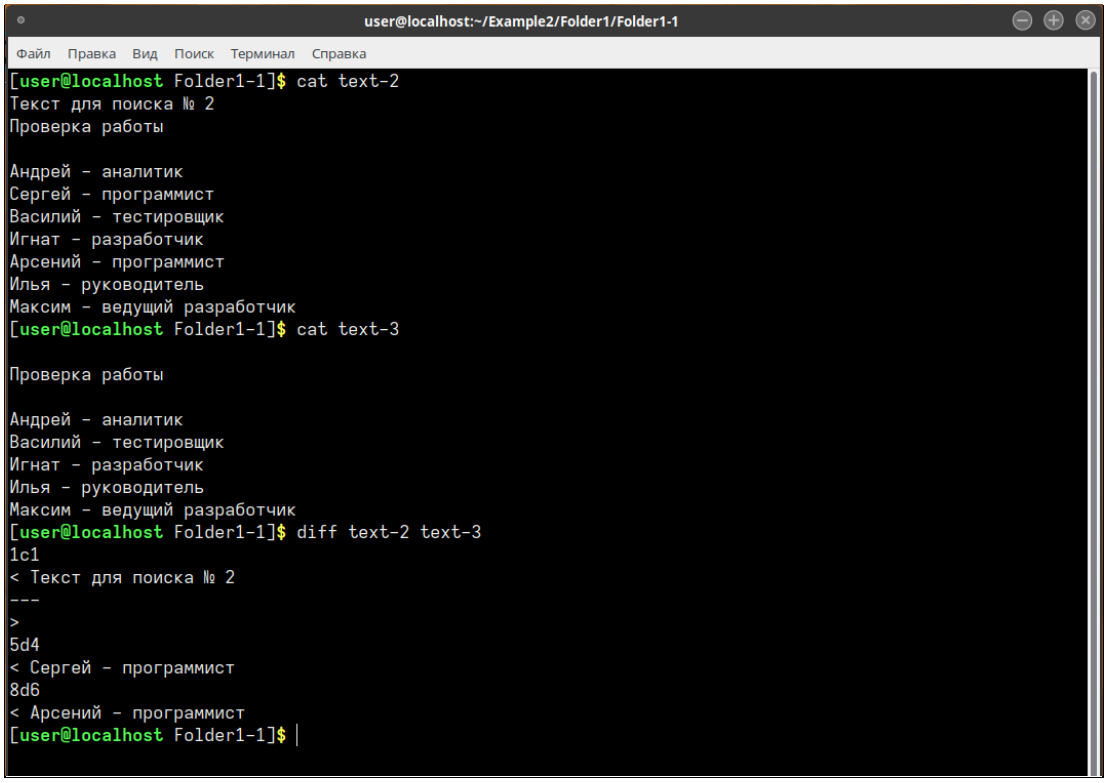
Основные опции:

- **-c**, **--bytes** – вывод размера файла в байтах;
- **-m**, **--chars** – вывод числа символов в файле;
- **-l**, **--lines** – вывод числа строк в файле;
- **-L**, **--max-line-length** – вывод максимальной длины строки в файле;
- **-w**, **--words** – вывод числа слов в файле.

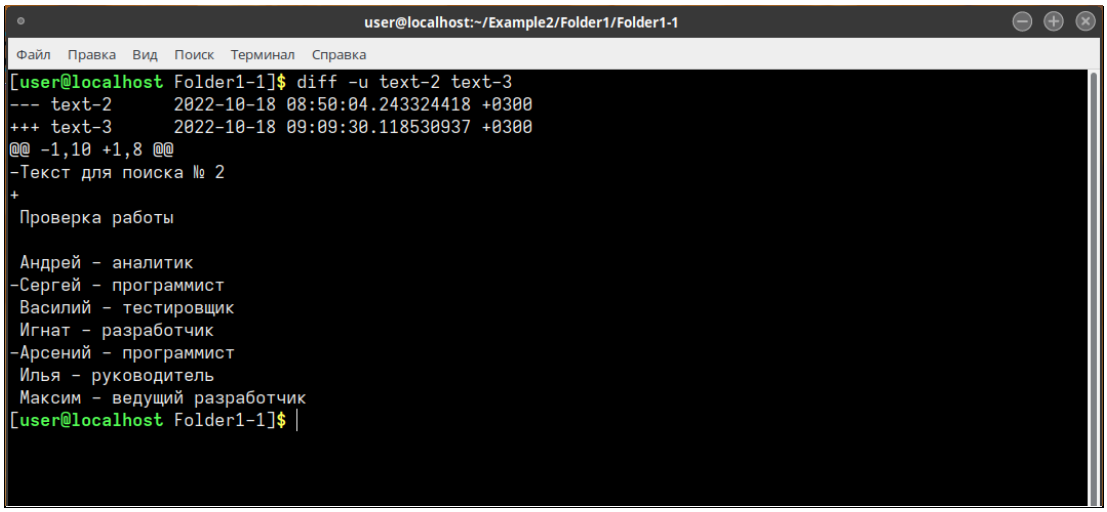


diff

Показывает различия между двумя файлами в построчном сравнении. Причём выводятся только строки, в которых обнаружены отличия. Измененные строки отмечаются символом «**c**», удаленные - «**d**», а новые - «**a**». Добавленные и удаленные строки обозначаются с помощью символов **>** и **<** соответственно.



Для вывода информации о различиях в унифицированном формате можно использовать опцию **-u**:



ps / pgrep

Предназначена для просмотра списка процессов. Чтобы завершить/приостановить какой-либо процесс, необходим его идентификатор. Один из способов получить его - утилита **ps**. Для отображения всех запущенных процессов можно использовать опцию **a**. Следует обратить внимание, что это только снимок состояния на момент вызова, информация не будет обновляться.

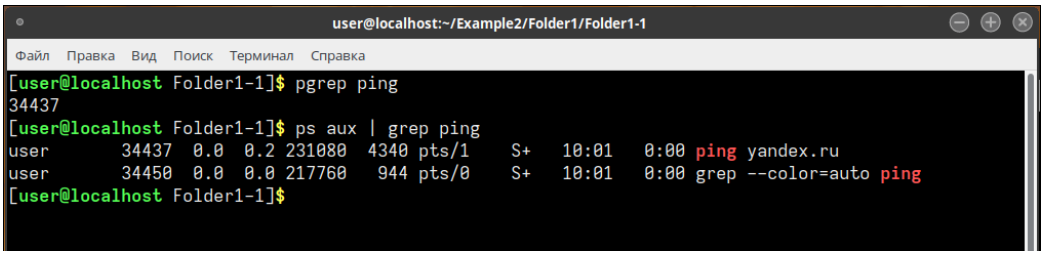
Для получения полной информации о процессах и определения идентификатора процесса (**PID**) выполните команду:

```
ps aux
```

Для конкретизации поиска определенного процесса рекомендуется использовать утилиту grep, например:

```
ps aux | grep ping
```

Утилита **pgrep** работает следующим образом: вы задаете имя процесса, а утилита показывает его идентификатор.



kill / xkill / pkill / killall

Данные команды служат для завершения процессов, однако они принимают различные параметры для идентификации процессов. **Kill** - нужен PID процесса, **xkill** - достаточно кликнуть по окну, чтобы закрыть его, **killall** и **pkill** - принимают имя процесса. Можно использовать любую из утилит, которая будет удобна в определенной ситуации.

Для определения идентификатора процесса (**PID**) воспользуйтесь утилитами ps или pgep, описанными выше.

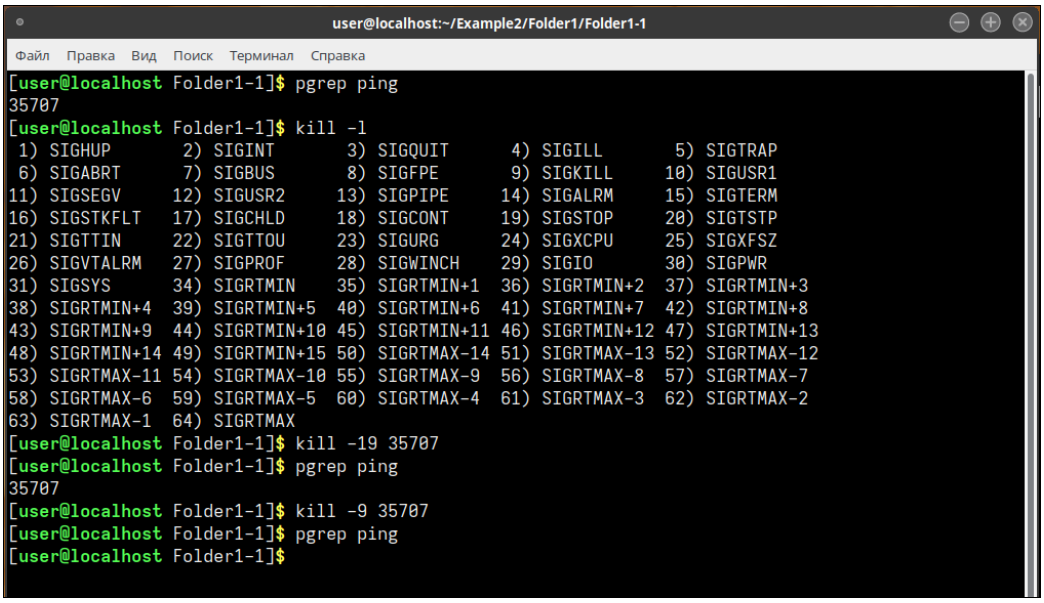
Для утилит kill и killall доступно несколько сигналов, которые также можно использовать для прерывания, завершения или приостановки процессов:

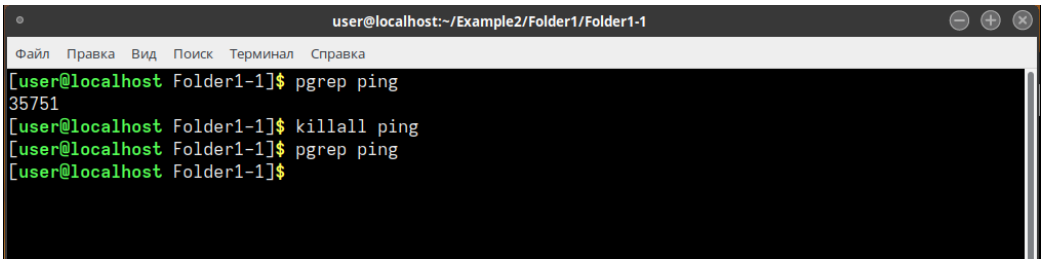
```
kill -l
killall -l
```

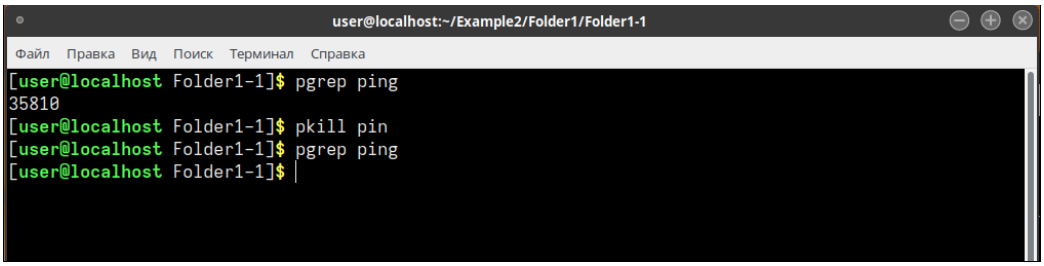
Принудительно завершить процесс можно, используя команды:

```
kill <PID_процесса>
killall <имя_процесса>
pkill <шаблон>
```

Утилита pkill может использовать как полное имя процесса для его завершения, так и часть имени. Утилита сопоставляет переданное ей имя процесса и может по ошибке завершить процесс с похожим именем, поэтому работу с утилитой следует проводить с осторожностью.

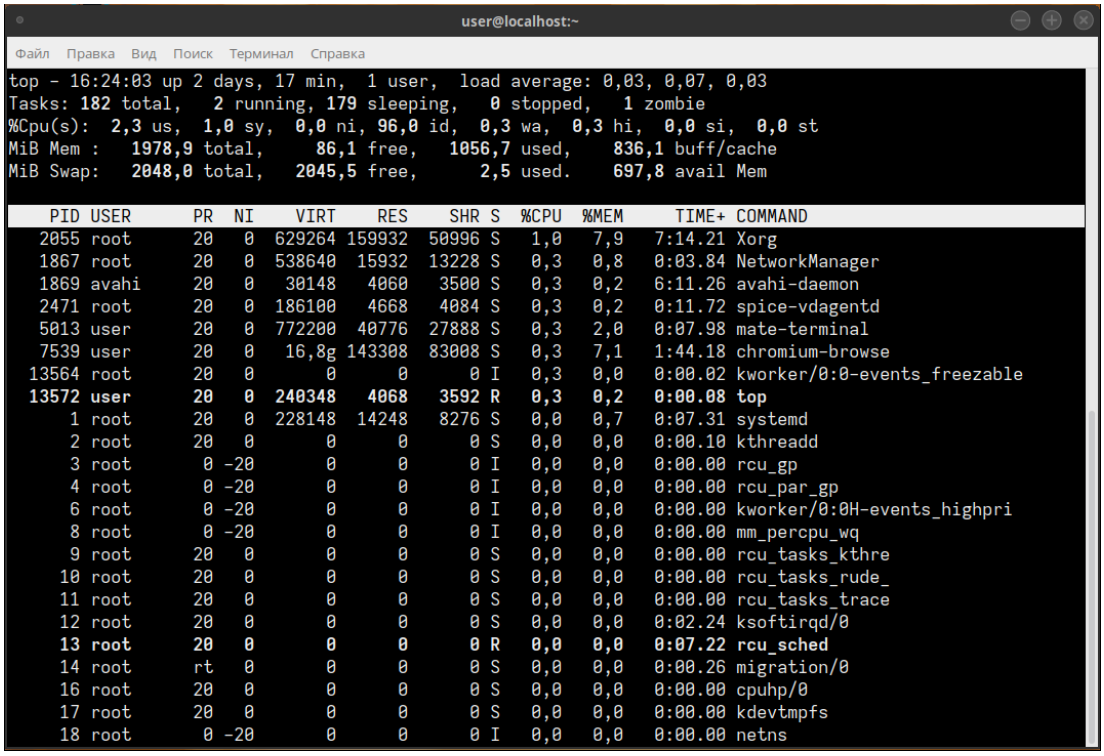






top / htop

Обе команды похожи, обе отображают процессы и могут быть использованы как консольные системные мониторы. **htop** - это улучшенная версия **top**. Вы сможете не только просматривать, но и контролировать процессы через его интерактивный интерфейс.



date

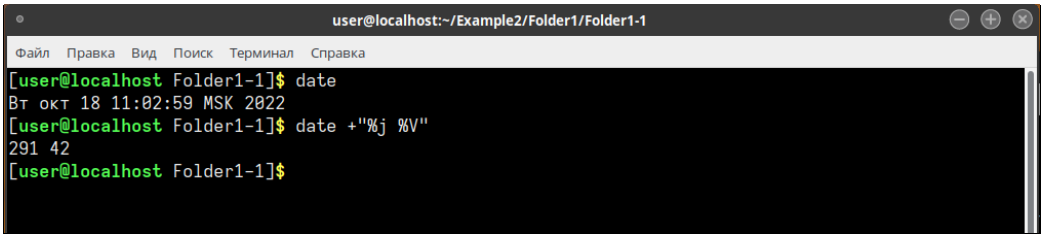
В отличие от **time**, выводит текущую дату и время в различных форматах и позволяет устанавливать системное время. Его можно форматировать в зависимости от ваших потребностей: вывести год, месяц, день, установить 12-ти или 24-ти часовой формат, получить наносекунды или номер недели. Например, **date +"%j %V"** выведет день в году и номер недели в формате ISO.

Установка системных даты и времени производится с правами администратора или суперпользователя (**root**) системы командой:

```
date ММДДччмм[[ВВ]ГГ][.сс]
```

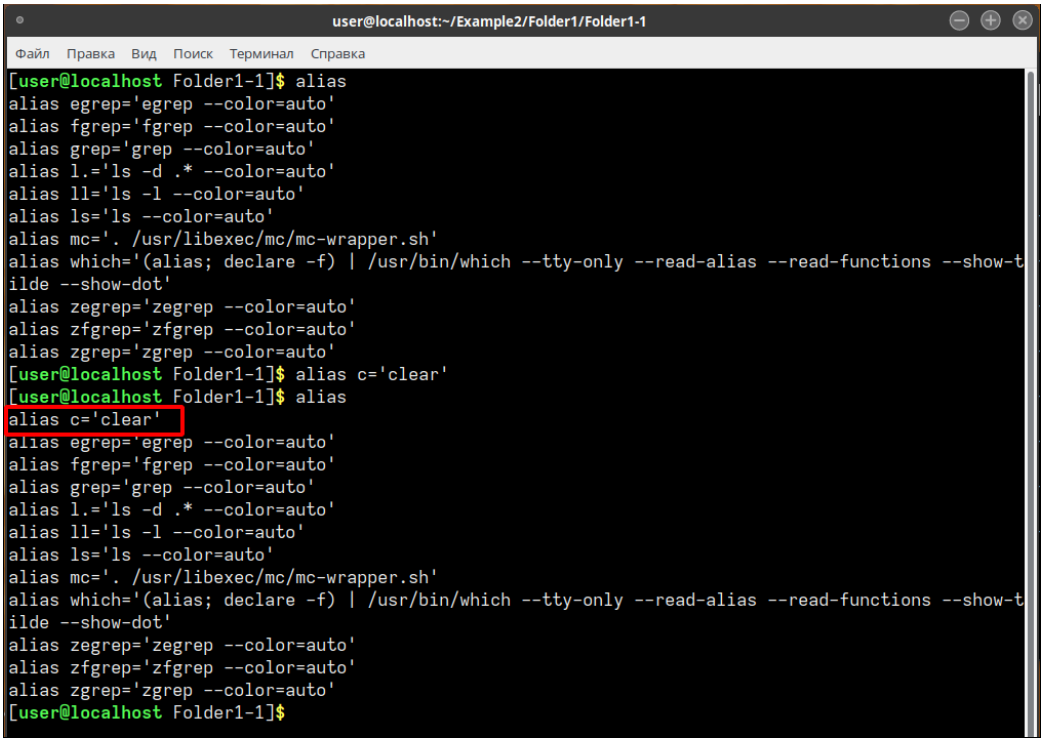
где:

- ММ - Месяц (от 01 до 12);
- ДД - День (от 01 до 28, 29, 30 или 31 в зависимости от месяца);
- чч - Часы (от 00 до 24);
- мм - Минуты (от 00 до 59);
- ГГ - Две последние цифры года (от 00 до 99, не обязательно);
- ВВ - Век (от 00 до 99, используется вместе с предыдущим элементом, не обязательно);
- .сс - Секунды (от 00 до 59 с символом точки, не обязательно).



alias

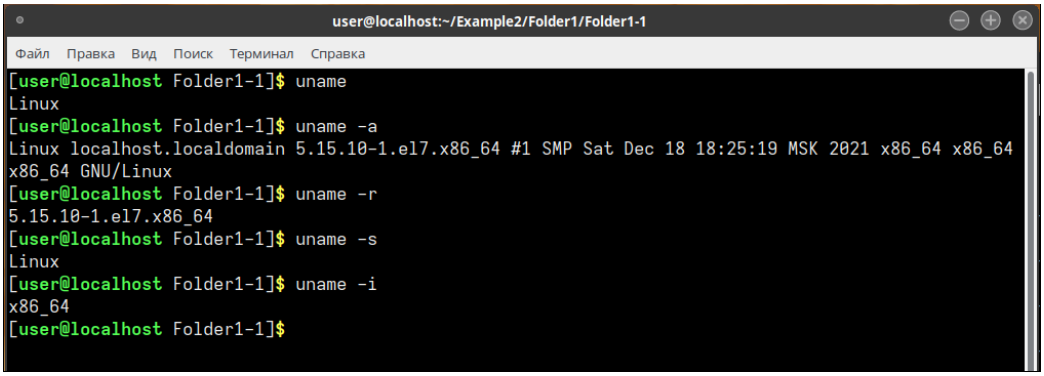
Команда создаёт синонимы для других команд Linux. То есть вы можете создать новые команды или группы команд, а также переименовывать существующие. Это очень удобно для сокращения длинных названий команд, которые вы часто используете, или создания более понятных имен для команд, которые вы используете нечасто или не можете запомнить.



uname

Выводит основную информацию о системе. Основные опции:

- **-a** (all) - информация о ядре, имени хоста и архитектуре процессора;
- **-i** - имя аппаратной реализации (платформы);
- **-r** - информация о релизе системы;
- **-s** - имя операционной системы, опция используется по умолчанию.

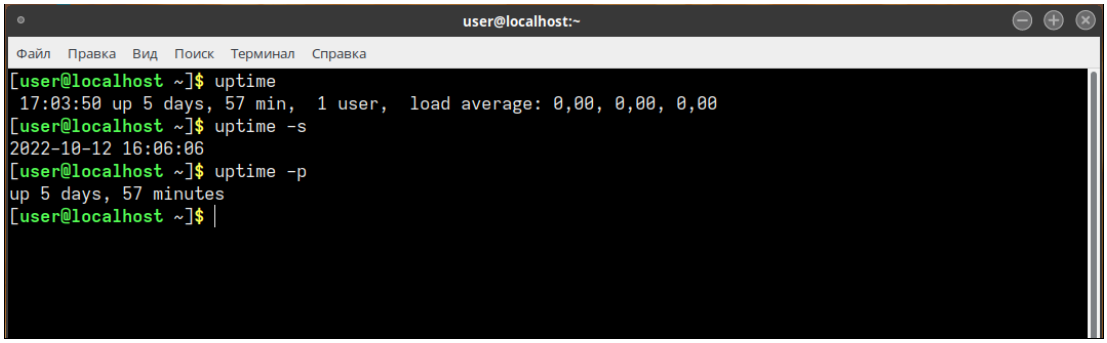


uptime

Выводит время работы системы, количество текущих в данный момент пользователей и среднюю загрузку системы за последние 1, 5 и 15 минут.

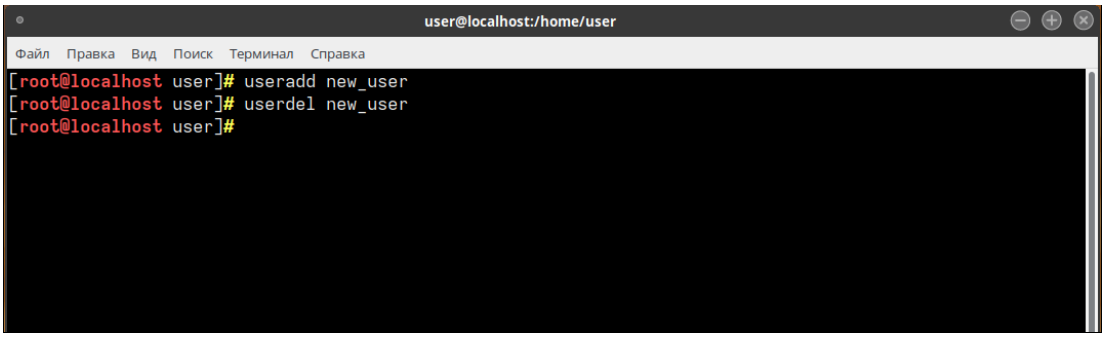
Можно использовать опции:

- **-s** (--since) - вывести время запуска системы. Это время, начиная с которого, отсчитывается время работы системы. Время выводится в формате YYYY-MM-DD HH:MM:SS;
- **-p** (--pretty) - вывести только время работы системы.



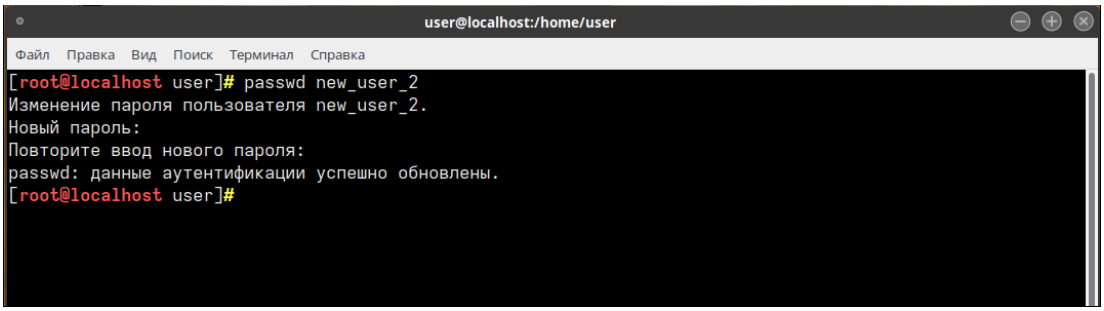
+ useradd / userdel / usermod

Эти команды позволяют добавлять, удалять и изменять учетные записи пользователей, для использования команд необходимы права администратора или суперпользователя (**root**) системы.



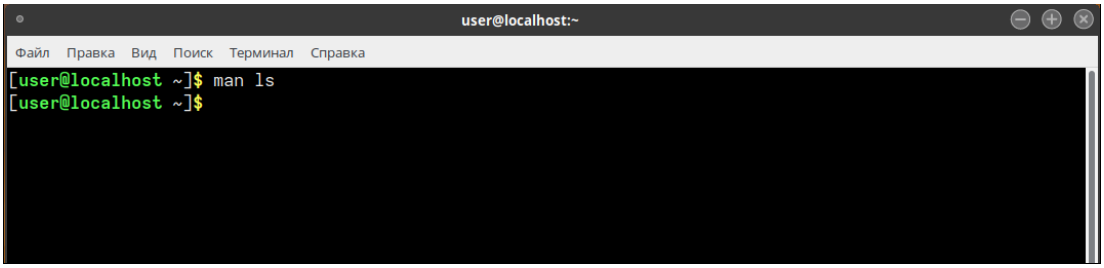
+ passwd

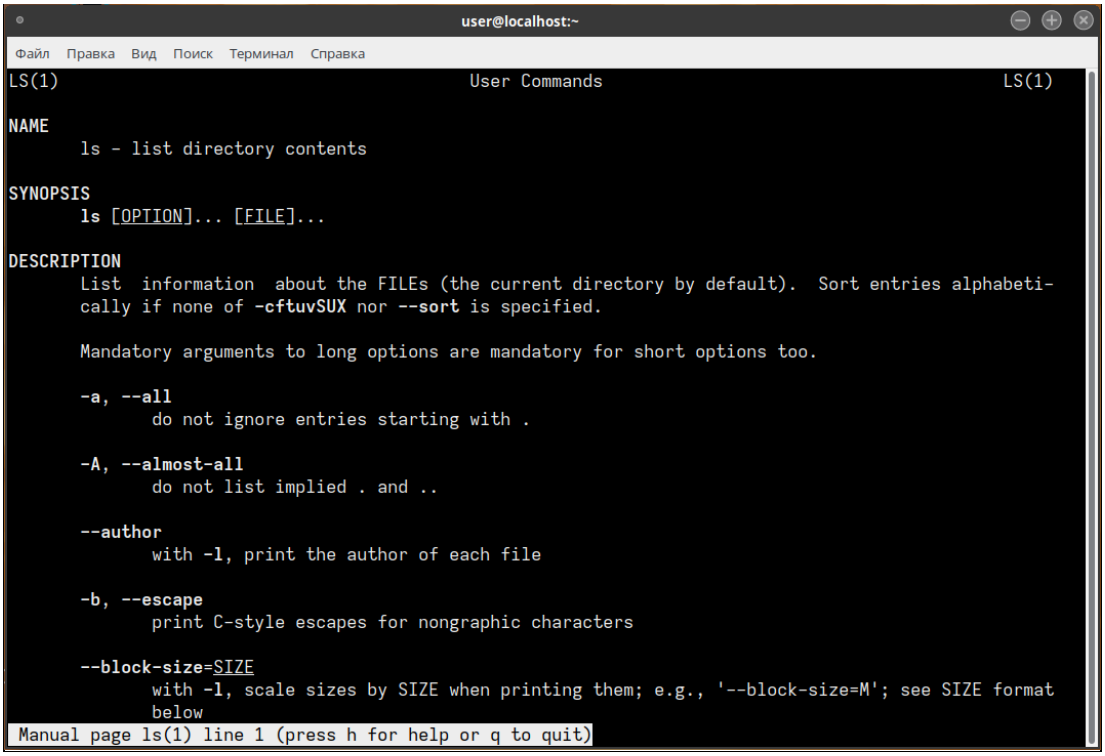
Эта команда позволяет изменить пароль учетной записи пользователя. Для использования команды необходимы права администратора или суперпользователя (**root**) системы.

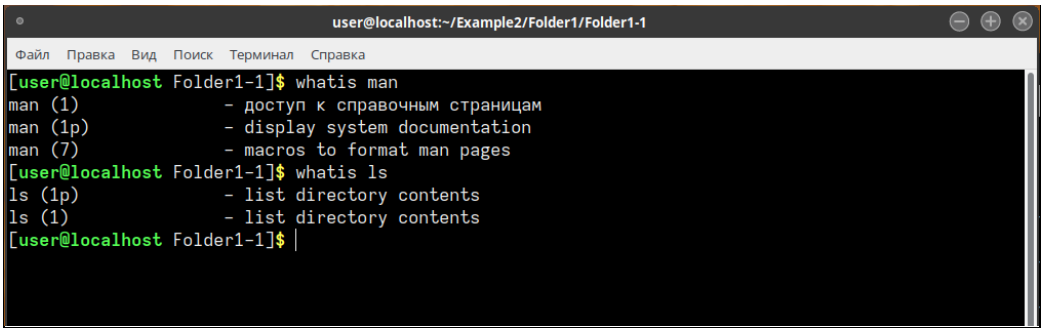


+ man / whatis

Команда **man** открывает руководство по определённой команде. Для всех основных команд Linux есть **man**-страницы. **Whatis** показывает, какие разделы руководств есть для данной команды.

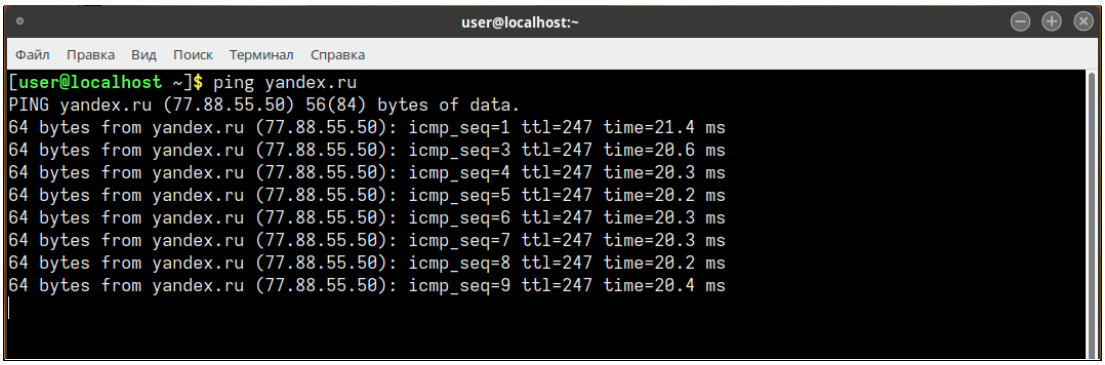






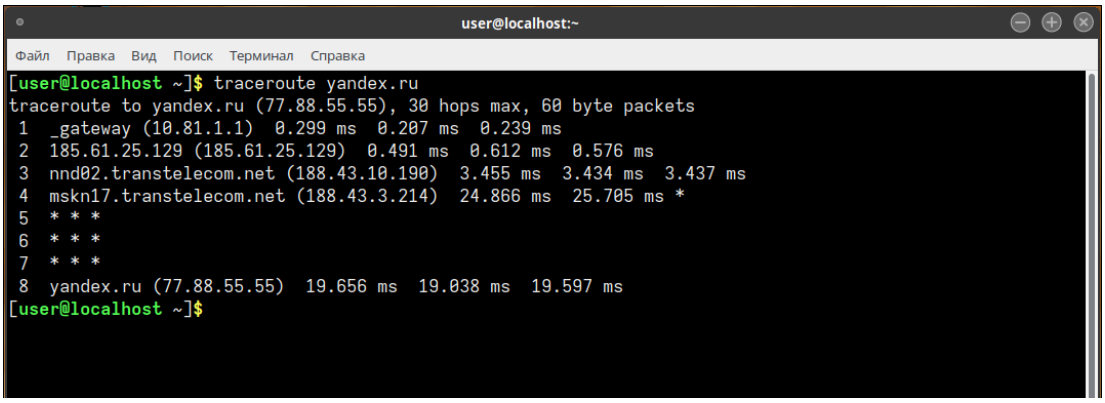
ping

Утилита **ping** может быть очень полезным диагностическим инструментом. Она поможет быстро проверить, подключены ли вы к маршрутизатору или к интернету, и дает некоторое представление о качестве этой связи.



traceroute

Это усовершенствованная версия **ping**. Мы можем увидеть не только полный маршрут сетевых пакетов, но и доступность узла, а также время доставки этих пакетов на каждый из узлов.



journalctl

journald — системная служба, отвечающая за сбор, хранение и управление данными журналов в ОС, также выполняет ротацию, сжатие и индексацию лог-файлов. **journalctl** позволяет просматривать и фильтровать данные, собираемых службой **journald**.

Полезные опции:

- **-f** — показать последние записи журнала и продолжить вывод новых записей при добавлении их в журнал;
- **-xb** — вывод записей журнала с момента запуска текущей сессии с расшифровкой ошибок.

```
[user@localhost ~]$ journalctl -f
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal', 'wheel' can see all messages.
      Pass -q to turn off this notice.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-tmpfiles-setup.service: Suc
ceeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped Create User's Volatile File
s and Directories.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus-broker.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Stopped D-Bus User Message Bus.
окт 25 14:44:49 localhost.localdomain systemd[71632]: dbus.socket: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Closed D-Bus User Message Bus Socke
t.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Shutdown.
окт 25 14:44:49 localhost.localdomain systemd[71632]: systemd-exit.service: Succeeded.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Finished Exit the Session.
окт 25 14:44:49 localhost.localdomain systemd[71632]: Reached target Exit the Session.
```

ip

ip — утилита командной строки из пакета **iproute2**, которая позволяет выполнять настройку сетевой подсистемы и является заменой таких утилит, как *ifconfig*, *route*, *arp*.

```
[user@localhost ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
00
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group d
efault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
 qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    altname enp0s25
    inet [redacted] brd [redacted] scope global dynamic noprefixroute eno1
       valid_lft 90149sec preferred_lft 90149sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever
4: anbox0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group de
fault qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet [redacted] scope global anbox0
       valid_lft forever preferred_lft forever
```

netstat

netstat — утилита командной строки, выводящая состояние TCP-соединений (как входящих, так и исходящих), таблицы

маршрутизации, число сетевых интерфейсов и сетевую статистику по протоколам.

```
[root@localhost user]# netstat --inet -pl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:46825         0.0.0.0:*               LISTEN      1088/containerd
tcp        0      0 0.0.0.0:ideafarm-door   0.0.0.0:*               LISTEN      1055/vmware-authdla
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      1086/sshd: /usr/sbi
tcp        0      0 localhost:54329         0.0.0.0:*               LISTEN      1113/postgres
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2133/dnsmasq
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      1078/cupsd
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN      1258/master
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN      2180/dnsmasq
udp        0      0 0.0.0.0:40848           0.0.0.0:*                           791/avahi-daemon: r
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2180/dnsmasq
udp        0      0 localhost.locald:domain 0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2180/dnsmasq
udp        0      0 0.0.0.0:bootps          0.0.0.0:*                           2133/dnsmasq
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*                           1/systemd
udp        0      0 localhost:323           0.0.0.0:*                           848/chronyd
```

df

Утилита **df** — консольная утилита, которая позволяет проверить использование дискового пространства в операционной системе. Эта команда отображает информацию об общем, свободном и используемом объеме памяти файловых систем. Утилита **df** предоставляет множество опций, которые позволяют настроить ее вывод.

```
[root@localhost user]# df
Файловая система 1K-блоков Использовано  Доступно Использовано% Смонтировано в
devtmpfs              4096            0      4096            0% /dev
tmpfs              4011852       608496   3403356           16% /dev/shm
tmpfs              1604744         3632   1601112            1% /run
/dev/sdb1        234213368    181416340  40826880           82% /
/dev/sda4        530945160    134478724 369422392           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1          106496       106496         0          100% /var/lib/snapd/snap/core/16928
/dev/loop0          108032       108032         0          100% /var/lib/snapd/snap/core/16574
/dev/loop2           57088        57088         0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3           57088        57088         0          100% /var/lib/snapd/snap/core18/2812
/dev/loop4           73088        73088         0          100% /var/lib/snapd/snap/webinar/7
/dev/loop6             128          128         0          100% /var/lib/snapd/snap/bare/5
/dev/loop7          168832       168832         0          100% /var/lib/snapd/snap/gnome-3-28-1804/198
/dev/loop5          382848       382848         0          100% /var/lib/snapd/snap/anbox/186
/dev/loop8           93952        93952         0          100% /var/lib/snapd/snap/gtk-common-themes/1535
/dev/loop9           72960        72960         0          100% /var/lib/snapd/snap/webinar/6
tmpfs               802368          160    802208            1% /run/user/1000
[root@localhost user]# df -h
Файловая система Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs           4,0M            0  4,0M            0% /dev
tmpfs              3,9G          595M  3,3G           16% /dev/shm
tmpfs              1,6G          3,6M  1,6G            1% /run
/dev/sdb1          224G          174G   39G           82% /
/dev/sda4          507G          129G  353G           27% /mnt/291c1faf-ec60-4019-afb2-9b24e608c5ba
/dev/loop1         104M          104M     0          100% /var/lib/snapd/snap/core/16928
/dev/loop0         106M          106M     0          100% /var/lib/snapd/snap/core/16574
/dev/loop2          56M           56M     0          100% /var/lib/snapd/snap/core18/2796
/dev/loop3          56M           56M     0          100% /var/lib/snapd/snap/core18/2812
```

free

Команда **free** предоставляет информацию об общем объеме физической памяти и памяти подкачки, а также о свободной и используемой памяти.

```
[user@localhost ~]$ free
               total        used        free      shared  buff/cache   available
Mem:         8023704     6372008      367168      575088     1284528      781116
Swap:        5122228     4663944      458284
[user@localhost ~]$ free -m
               total        used        free      shared  buff/cache   available
Mem:            7835        6225         355         561        1254         760
Swap:           5002        4554         447
[user@localhost ~]$ free -h
               total        used        free      shared  buff/cache   available
Mem:           7,7Gi       6,1Gi       355Mi       565Mi       1,2Gi       759Mi
Swap:          4,9Gi       4,4Gi       447Mi
[user@localhost ~]$
```

Получение справочной информации об использовании утилит с помощью man

Установка
Навигация
Разделы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО:** man-db-2.9.4-4, man-pages-5.12-4

man — утилита, предназначенная для форматирования и вывода справочных страниц. Каждая страница справки является самостоятельным документом и пишется разработчиками соответствующего программного обеспечения.

Установка

В РЕД ОС по умолчанию утилита уже установлена. Однако, если по каким-либо причинам она отсутствует, ее можно установить. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install man man-pages
```

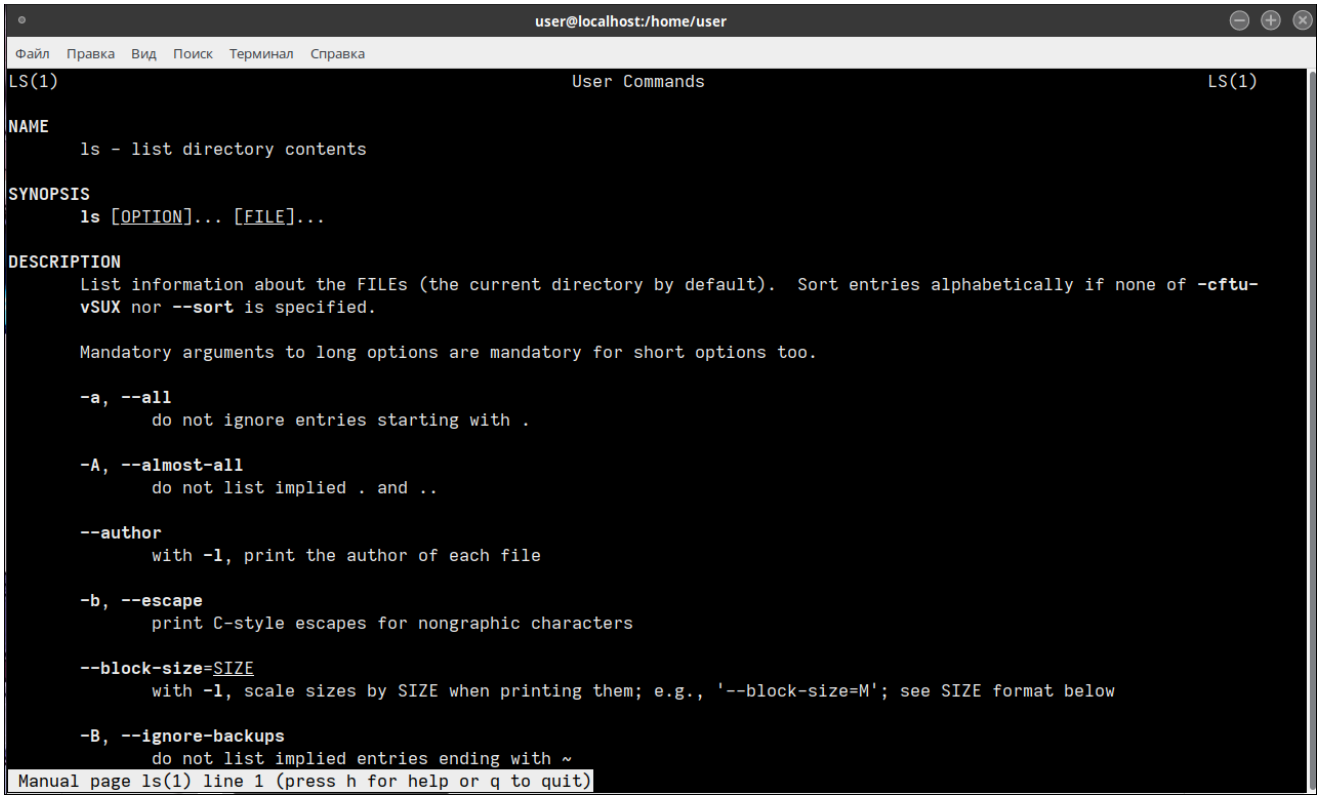
Далее команды будут выполняться с правами **локального пользователя**, если не указано иное.

Для вывода справочного руководства по какой-либо команде или пакету с возможностью запуска в терминале необходимо выполнить команду вида:

```
man <команда>
```

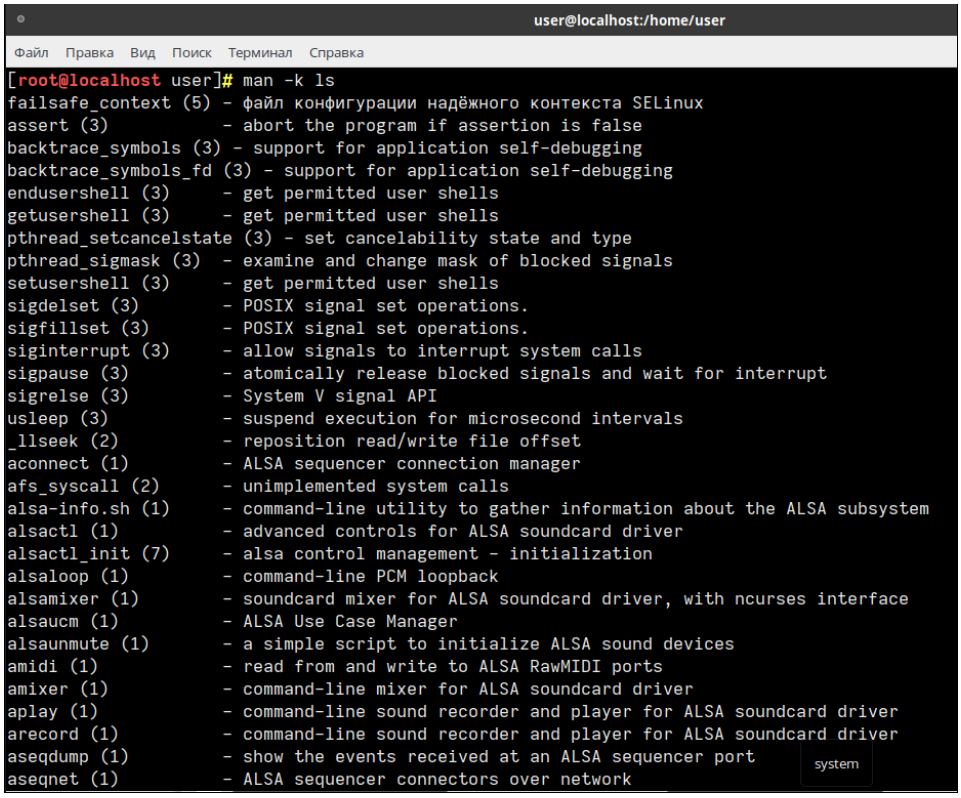
Например:

```
man ls
```



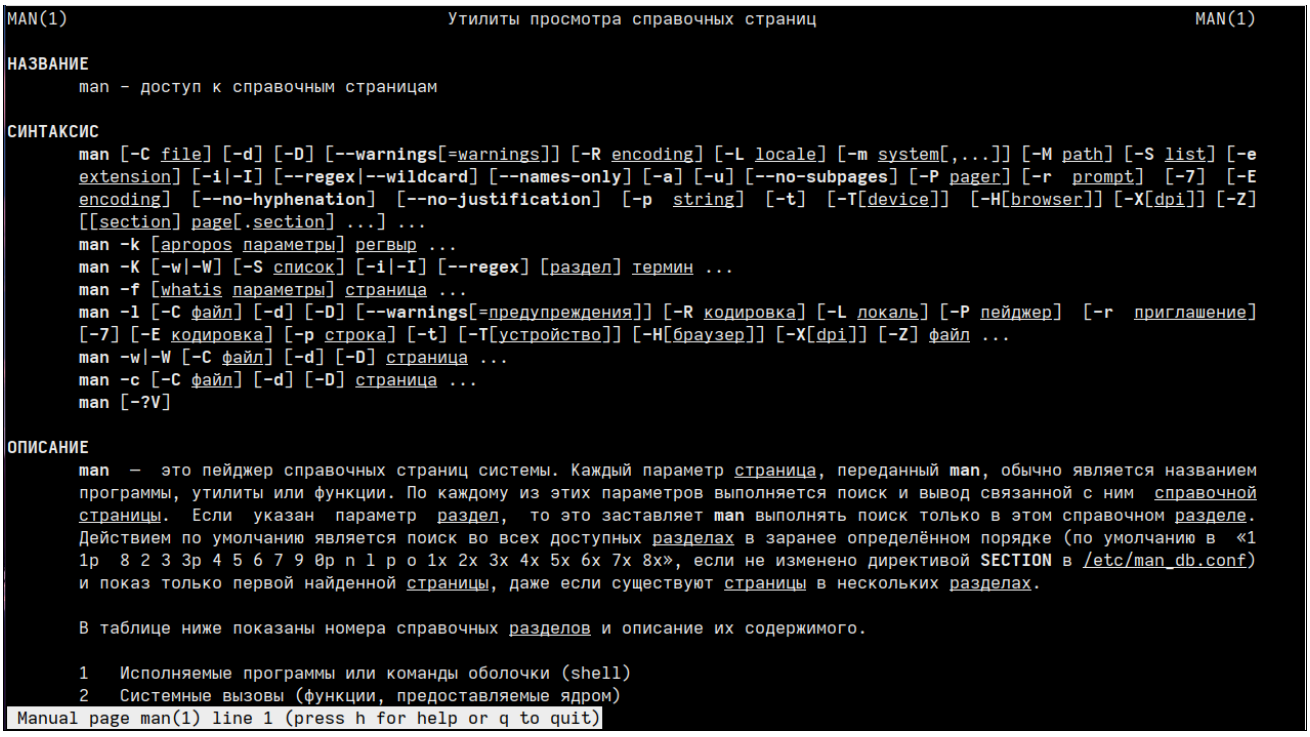
Опция **-k** выполняет поиск и выводит список man-страниц, в которых встречается искомый запрос.

```
man -k ls
```



Другие полезные опции утилиты **man** можно посмотреть командой:

```
man man
```



Навигация

Для навигации по страницам руководства используются следующие сочетания клавиш:

- ↑ и ↓ — для построчного перехода по руководству;
- **PgUp** и **PgDown** — для постраничного перехода по руководству;

- **/** — поиск по странице; введите **/** и искомое слово, затем нажмите **Enter**;
- **?** — поиск в обратном направлении (снизу вверх); введите **?** и искомое слово, затем нажмите **Enter**;
- **n** — переход к следующему подсвеченному вхождению;
- **Shift+n** — переход к предыдущему подсвеченному вхождению;
- **&** — поиск внутри страницы; выводятся только строки, где было найдено искомое слово;
- **h** — открыть справку по командам и горячим клавишам, для закрытия справки нажмите **q**;
- **q** — закрыть man-страницу.

Разделы

Справочные страницы поделены на 8 стандартных разделов и один дополнительный. Каждый из разделов соответствует той или иной тематике.

Раздел	Краткое описание
1	Прикладные программы и команды оболочки
2	Системные вызовы ядра (функции языка Си)
3	Библиотечные вызовы (функции различных библиотек, установленных в систему)
4	Специальные файлы (находящиеся обычно в каталоге **/dev**)
5	Форматы файлов и соглашения
6	Игры
7	Различные описания, соглашения и прочее
8	Команды администрирования системы, которые обычно запускаются от имени суперпользователя
9	Ядро операционной системы (нестандартный раздел)

Номер раздела в команде **man** указывается вторым аргументом, перед названием справочной страницы. Если номер раздела опущен, то поиск справочной страницы ведётся по всем разделам по порядку.

```
man kill  # раздел 1
man 1 kill  # раздел 1
man 2 kill  # раздел 2
```

Менеджер сервисов systemd

Файл сервиса systemd
Типы служб
Замещение файла юнита
Компоненты system
Запуск сервисов после подключения к сети

Systemd – менеджер системы и сервисов в операционной системе РЕД ОС.

Systemd приносит концепцию юнитов **systemd**. Юниты представлены конфигурационными файлами, размещенными в одной из директорий:

- **/usr/lib/systemd/system/** – юниты из установленных пакетов RPM.
- **/run/systemd/system/** – юниты, созданные в рантайме. Этот каталог приоритетнее каталога с установленными юнитами из пакетов.
- **/etc/systemd/system/** – юниты, созданные и управляемые системным администратором. Этот каталог приоритетнее каталога юнитов, созданных в рантайме.

Юниты содержат информацию о системных сервисах, прослушиваемых сокетах, сохраненных снапшотах состояний системы и других объектах, относящихся к системе инициализации.

Типы юнитов **systemd**:

- *.service* – системный сервис,
- *.target* – группа юнитов **systemd**,
- *.automount* – точка автомонтирования файловой системы,
- *.device* – файл устройства, распознанного ядром,
- *.mount* – точка монтирования файловой системы,
- *.path* – файл или директория в файловой системе,
- *.scope* – процесс, созданный извне,
- *.slice* – группа иерархически организованных юнитов, управляющая системными процессами,
- *.snapshot* – сохраненное состояние менеджера **systemd**,
- *.socket* – сокет межпроцессного взаимодействия,
- *.swap* – свап-устройство или свап-файл (файл подкачки),
- *.timer* – таймер **systemd**.

Во время загрузки **systemd** прослушивает сокеты для всех системных сервисов, поддерживает этот тип активации и передает сокеты этим сервисам сразу после старта сервисов. Это позволяет **systemd** не только запускать сервисы параллельно, но также дает возможность перезапускать сервисы без потери любых отправленных им сообщений, пока сервисы были недоступны. Соответствующий сокет остается доступным и все сообщения выстраиваются в очередь.

Системные сервисы, использующие D–Bus для межпроцессного взаимодействия, могут быть запущены по требованию, когда клиентское приложение пытается связаться с ними.

Системные сервисы, поддерживающие активацию, основанную на устройствах, могут быть запущены, когда определенный тип оборудования подключается или становится доступным.

Системные сервисы могут поддерживать этот вид активации, если изменяется состояние папки или директории.

Система может сохранять состояние всех юнитов и восстанавливать предыдущее состояние системы.

Systemd отслеживает и управляет точками монтирования и автомонтирования.

Агрессивная параллелизация **Systemd** запускает системные сервисы параллельно из-за использования активации, основанной на сокетах. В комбинации с сервисами, поддерживающими активацию по требованию, параллельная активация значительно уменьшает время загрузки системы.

До активации и деактивации юнитов **systemd** вычисляет их зависимости, создает временную транзакцию и проверяет целостность этой транзакции. Если транзакция не целостная, systemd автоматически пытается исправить ее и удалить не требующиеся задания из нее до формирования сообщения об ошибке.

Systemd полностью поддерживает скрипты инициализации **SysV**, как описано в спецификации Linux Standard Base (LSB), что упрощает переход на systemd.

По способу использования сервисные юниты *.service* напоминают скрипты инициализации. Для просмотра, старта, остановки, перезагрузки, включения или выключения системных сервисов используется команда systemctl. Команды service и chkconfig по-прежнему включены в систему, но только для обеспечения совместимости.

При использовании **systemctl** указывать расширение файла не обязательно.

Основные команды *systemctl*:

systemctl start name.service – запуск сервиса,
systemctl stop name.service — остановка сервиса,
systemctl restart name.service — перезапуск сервиса,
systemctl try-restart name.service — перезапуск сервиса только, если он запущен,
systemctl reload name.service — перезагрузка конфигурации сервиса,
systemctl status name.service — проверка, запущен ли сервис с детальным выводом состояния сервиса,
systemctl is-active name.service — проверка, запущен ли сервис с простым ответом: active или inactive,
systemctl list-units --type service --all – отображение статуса всех сервисов,
systemctl --failed – отображение списка юнитов, которые не удалось запустить,
systemctl enable name.service – активирует сервис (позволяет стартовать во время запуска системы),
systemctl disable name.service – деактивирует сервис,
systemctl reenable name.service – деактивирует сервис и сразу активирует его,
systemctl is-enabled name.service – проверяет, активирован ли сервис,
systemctl list-unit-files --type service – отображает все сервисы и проверяет, какие из них активированы,
systemctl cat name.service – позволит просмотреть содержимое файла юнита и связанных с ним drop-in сниппетов,
systemctl mask name.service – заменяет файл сервиса симлинком на /dev/null, делая юнит недоступным для systemd,
systemctl unmask name.service – возвращает файл сервиса, делая юнит доступным для systemd.

Файлы целей **systemd .target** предназначены для группировки вместе других юнитов systemd через цепочку зависимостей. Например, юнит **graphical.target**, использующийся для старта графической сессии, запускает системные сервисы GNOME Display Manager (*gdm.service*) и Accounts Service (*accounts-daemon.service*) и активирует **multi-user.target**. В свою очередь **multi-user.target** запускает другие системные сервисы, такие как Network Manager (*NetworkManager.service*) или D-Bus (*dbus.service*) и активирует другие целевые юниты **basic.target**.

В РЕД ОС присутствуют предопределенные цели, похожие на стандартный набор уровней запуска. Для обеспечения совместимости они также имеют псевдонимы на эти цели, которые напрямую отображаются в уровнях запуска *SysV*.

poweroff.target (runlevel0.target) – завершение работы и отключение системы
rescue.target (runlevel1.target) – настройка оболочки восстановления
multi-user.target (runlevel2.target, runlevel3.target, runlevel4.target) – настройка неграфической многопользовательской системы
graphical.target (runlevel5.target) – настройка графической многопользовательской системы
reboot.target (runlevel6.target) – выключение и перезагрузка системы

Команды **runlevel** и **telinit** по-прежнему доступны в системе для обеспечения совместимости, однако рекомендуется использовать **systemctl** для изменения или настройки системных целей.

Для определения, какой целевой юнит используется по умолчанию, полезна следующая команда:

```
systemctl get-default
```

Для просмотра всех загруженных целевых юнитов воспользуйтесь командой:

```
systemctl list-units --type target
```

а для просмотра вообще всех целевых юнитов командой:

```
systemctl list-units --type target --all
```

Для изменения цели по умолчанию поможет команда:

```
systemctl set-default name.target
```

Для изменения текущей цели:

```
systemctl isolate name.target
```

Команда запустит целевой юнит и все его зависимости и немедленно остановит все остальные.

В РЕД ОС *systemctl* заменяет значительное количество команд управления питанием. Прежние команды сохранены для совместимости, но рекомендуется использовать *systemctl*:

- **systemctl halt** – останавливает систему,
- **systemctl poweroff** – выключает систему,
- **systemctl reboot** – перезагружает систему,
- **systemctl suspend** – переводит систему в режим ожидания,

- **systemctl hibernate** – переводит систему в спящий режим,
- **systemctl hybrid-sleep** – переводит систему в режим гибридного сна.

Systemd позволяет управлять удаленной машиной по SSH. Для управления используйте команду:

```
systemctl --host <user_name>@<host_name> <command>
```

где **user_name** – имя пользователя, **host_name** – имя хоста, которым осуществляется удаленное управление, а **command** – выполняемая команда **systemd**. Подробная информация о всех параметрах файла *.service* есть в соответствующем разделе документации по **systemd**.

Файл сервиса systemd

```
[Unit]
Description=Daemon to detect crashing apps
After=syslog.target

[Service]
ExecStart=/usr/sbin/abrtd
Type=forking

[Install]
WantedBy=multi-user.target
```

Давайте посмотрим на секцию **[Unit]**. Она содержит общую информацию о сервисе. Такая секция есть не только в сервис-юнитах, но и в других юнитах (например, при управлении устройствами, точками монтирования и т.д.). В примере мы даем описание сервиса и указываем на то, что демон должен быть запущен после **Syslog**.

В следующей секции **[Service]** непосредственно содержится информация о нашем сервисе. Используемый параметр *ExecStart* указывает на исполняемый файл нашего сервиса. В *Type* мы указываем, как сервис уведомляет **systemd** об окончании запуска.

Финальная секция **[Install]** содержит информацию о цели, в которой сервис должен стартовать. В данном случае мы говорим, что сервис должен быть запущен, когда будет активирована цель *multi–user.target*. Это минимальный работающий файл сервиса **systemd**. Написав свой, для тестирования скопируйте его в **/etc/systemd/system/.service**. Выполните команду:

```
systemctl daemon-reload
```

Systemd узнает о сервисе и вы сможете его запустить.

Типы служб

Службы различаются по типу запуска, что следует учитывать при написании юнитов. Тип определяется параметром **Type=** в разделе [**Service**]:

- **Type=simple** (по умолчанию): systemd запустит эту службу незамедлительно. Процесс при этом не должен разветвляться (fork). Если после данной службы должны запускаться другие, то этот тип использовать не стоит (исключение — служба использует сокетную активацию).
- **Type=forking**: systemd считает службу запущенной после того, как процесс разветвляется с завершением родительского процесса. Используется для запуска классических демонов за исключением тех случаев, когда в таком поведении процесса нет необходимости. Укажите параметр **PIDFile=**, чтобы systemd мог отслеживать основной процесс.
- **Type=oneshot**: удобен для сценариев, которые выполняют одно задание и завершаются. Если задать параметр **RemainAfterExit=yes**, то systemd будет считать процесс активным даже после его завершения.
- **Type=notify**: идентичен параметру **Type=simple**, но с уточнением, что демон пошлет systemd сигнал готовности. Реализация уведомления находится в библиотеке **libsystemd-daemon.so**.
- **Type=dbus**: служба считается находящейся в состоянии готовности после появления указанного **BusName** в системной шине DBus.
- **Type=idlel**: systemd отложит выполнение двоичного файла службы до окончания запуска остальных ("более срочных") задач. В остальном поведение аналогично **Type=simple**.

Замещение файла юнита

Можно полностью заместить файл юнита /usr/lib/systemd/system/<юнит>. Для этого необходимо создать файл с таким же именем

/etc/systemd/system/<юнит> и включить заново юнит для обновления символических ссылок.

```
systemctl edit --full <юнит>
```

Эта команда откроет файл **/etc/systemd/system/<юнит>** в текстовом редакторе (если файл ещё не существует, будет скопирован оригинал) и автоматически перезагрузит юнит после завершения редактирования.

Компоненты system

- **systemd-boot** – простой менеджер загрузки для UEFI;
- **systemd-firstboot** – инициализация системных настроек при первой загрузке;
- **systemd-homed** – переносимые аккаунты пользователей;
- **systemd-logind** – управление сеансами;
- **systemd-networkd** – управление сетевыми настройками;
- **systemd-nspawn** – приложение для контейнеризации процессов;
- **systemd-resolved** – разрешение сетевых имён;
- **systemd-sysusers** – создание системных пользователей/групп и добавление пользователей в группы при установке пакетов и загрузке системы;
- **systemd-timesyncd** – синхронизация системных часов по сети;
- **systemd/Журнал** – системные логи;
- **systemd/Таймеры** – таймеры для управления событиями и службами, альтернатива *cron*.

Запуск сервисов после подключения к сети

Для того чтобы запускать сервис только после подключения к сети, добавьте такие зависимости в **.service**-файле:

```
nano /etc/system/system/foo.service

[Unit]
…
Wants=network-online.target
After = network-online.target
…
```

Управление задачами в командной строке

РЕД ОС является многозадачной системой, способной одновременно выполнять несколько задач (или процессов). На самом деле одно ядро процессора может выполнять только один процесс в определённый момент времени. Но ядро Linux управляет задачами и чередует их выполнение на процессоре так, что пользователю кажется их выполнение одновременным. Всеми процессами можно управлять из командной строки.

Существует множество команд для управления процессами из командной строки, рассмотрим некоторые из них:

- **ps** — список запущенных процессов на компьютере;
- **kill** — отправка сигнала одному или нескольким процессам;
- **jobs** — просмотр списка собственных задач сеанса оболочки;
- **bg** — выполнение задачи в фоновом режиме;
- **fg** — возврат задачи из фонового режима.

Вы можете подробнее ознакомиться со способами управления задачами, просмотрев наши обучающие видео:

- на **RuTube** — Управление задачами в bash;
- в **Яндекс.Дзен** — Управление задачами в bash;
- в **VK Видео** — Управление задачами в bash.

На наших каналах вы также сможете найти много другой полезной информации.

Для примера будет использоваться утилита ping с отправкой запросов каждые 9 секунд:

```
ping -i 9 red-soft.ru
```

Таким образом, активирован процесс, привязанный к данному терминалу, из-за чего работа с командной строкой становится невозможной. Но, поскольку командная строка необходима для дальнейшей работы, прервём выполнение команды «горячими» клавишами оболочки — «**Ctrl+C**» и запустим данную команду в фоновом режиме, для этого в конце команды необходимо добавить символ «**&**»:

```
ping -i 9 red-soft.ru &
```

Теперь командная строка доступна для работы, и каждые 9 секунд демонстрируется результат команды ping. И хотя процесс не занимает собой командную строку оболочки, он всё равно привязан к текущему терминалу. В таком случае говорят, что процесс стал собственной задачей текущего сеанса оболочки.

Для отображения списка задач в текущем сеансе оболочки можно воспользоваться командой jobs:

```
jobs [1]+ Запущен ping -i 9 red-soft.ru
```

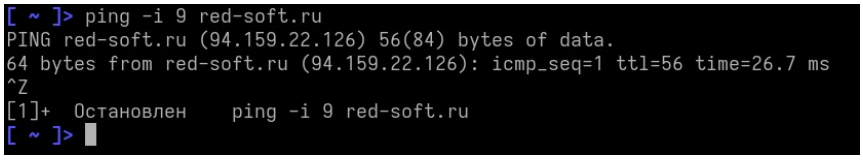
В квадратных скобках указан номер задачи в текущем терминале, его можно использовать в том числе и для завершения процесса утилитой kill, но в отличие от идентификатора процесса, который указывается «обычным» цифровым значением, перед номером задачи ставится знак «**%**». Например:

```
kill %1
```

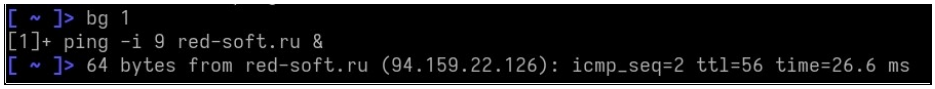
Для возвращения фонового процесса обратно в интерактивный режим необходимо использовать утилиту fg (**foreground**). Данную команду необходимо выполнять с переданным в качестве аргумента номером фоновой задачи (получить его можно из вывода команды **jobs**):

```
fg 1
```

Клавиатурное сочетание «**Ctrl+Z**» отправляет задачу в фон и ставит её выполнение на паузу. Иными словами, процесс не получает ресурсов центрального процессора для своего выполнения и находится в режиме ожидания.



Когда понадобится продолжить выполнение остановленной задачи, можно воспользоваться утилитой fg, описанной выше, или другой командой — bg (**background**). Утилита bg пробуждает задачу и отправляет её в фон:



В выводе команды отображаются результаты отправки ICMP-пакета (основная задача **ping**) и выводятся на экран — это значит, что процесс снова работает на заднем плане, не взаимодействуя с командной строкой.

Добавление команд в автозагрузку

Добавление через управление автозапускаемыми приложениями
Добавление через сервис
Добавление команды в crontab
Выполнение команд через desktop-файлы

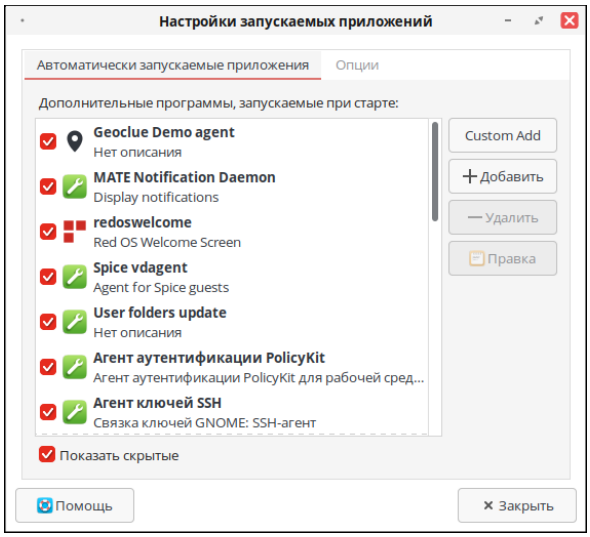
Вы можете подробнее ознакомиться с добавлением команд в автозагрузку, просмотрев наши обучающие видео:

- на **RuTube** — Добавление команд в автозагрузку;
- в **Яндекс.Дзен** — Добавление команд в автозагрузку;
- в **VK Видео** — Добавление команд в автозагрузку.

На наших каналах вы также сможете найти много другой полезной информации.

Добавление через управление автозапускаемыми приложениями

В графической оболочке **MATE** для добавления приложения или команды в автозагрузку требуется перейти в «**Главное меню**» — «**Параметры**» — «**Запуск приложений**». Будет показан текущий список автозагрузок пользователя.



Добавление приложения осуществляется нажатием кнопки «**Добавить**», добавление пользовательской команды осуществляется нажатием кнопки «**Custom Add**».

В случае приложения — будет доступен список установленных приложений, которые можно добавить в автозагрузку.

В случае команды пользователя — указывается имя команды, путь к ней и, если требуется, комментарий с задержкой выполнения команды.

Добавление через службу

Выберите скрипт, который будет запускаться через созданную службу, в примере используется **/etc/default/script**.

Создайте новую службу. Пример содержимого новой службы приведен ниже:

```
nano /etc/systemd/system/testservice.service
```

Содержимое службы:

```
[Unit]
 Description=service description
 After=gdm.service
 [Service]
 ExecStart=/etc/default/script
 Type=oneshot
 User=root
 RemainAfterExit=yes
 [Install]
```

```
WantedBy=multi-user.target
```

Также с помощью следующих команд можно указать, от имени какого именно пользователя будет проходить выполнение, в примере — **root**:

```
chmod 664 /etc/systemd/system/testservice.service
systemctl daemon-reload
systemctl enable testservice.service
systemctl start testservice.service
```

Добавление команды в crontab

Добавление скрипта в **crontab** происходит следующим образом:

1. В консоли выполните команду:

```
crontab -e
```

Откроется окно редактирования.

2. Введите команду, например:

```
0 * * * * /etc/default/script
```

Формат ввода данных представлен ниже:

```
* * * * * Команда, которая будет выполнена- - - - -
| | | | |
| | | | - День недели 0 - 7) (воскресенье = 0 или 7)
| | | --- Месяц (1 - 12)
| | --- День месяца (1 - 31)
| ---- Час (0 - 23)
----- Минута (0 - 59)
```

3. Сохраните отредактированный файл с заданием.

4. Для удаления заданий введите:

```
crontab -r
```

5. Для вывода списка текущих заданий выполните:

```
crontab -l
```

Подробную информацию о **crontab** см. в нашей инструкции «Планировщик заданий crontab».

Выполнение команд через desktop-файлы

Для выполнения команд через **desktop**-файлы необходимо:

1. Создать файл запуска со следующим содержимым (потребуются права пользователя **root** или **администратора** системы):

```
nano /etc/xdg/autostart/test.desktop
```

```
[Desktop Entry]
Type=Application
Exec=/home/user/test.sh
Hidden=false
Name=MyAutostart
```

где Exec=**<путь_к_файлу>**/test.sh — это команда/скрипт, которую требуется выполнить.

2. Создать скрипт **/test.sh** со следующим содержимым:

```
nano /home/user/test.sh
```

```
#!/usr/bin/bash
 if [ -f /home/user/test.sh ]; then
 v_date=`date "+%m.%d.%y %k:%M:%S"`
 echo "Время запуска скрипта: "$v_date >> ${HOME}/test.log
 fi
```

3. Назначить скрипту права на выполнение:

```
chmod +x /home/user/test.sh
```

4. Выполнить проверку.

Выйдите и войдите в сеанс пользователя либо перезагрузите систему.

В домашнем каталоге пользователя будет создан файл **test.log**, в который будут записаны дата и время исполнения скрипта.

```
cat /home/user/test.log

Время запуска скрипта: 10.10.24 11:34:57
```

Создание псевдонимов команд с помощью alias

Alias - псевдоним, который позволяет пользователю запускать любую команду или группу команд, в том числе с опциями, параметрами и файлами, вводом всего одного слова или даже символа.

Вы можете подробнее ознакомиться с работой **Alias**, просмотрев наши обучающие видео:

- на **RuTube** — Alias - создание псевдонимов команд;
- в **Яндекс.Дзен** — Alias - создание псевдонимов команд;
- в **VK Видео** — Alias - создание псевдонимов команд.

На наших каналах вы также сможете найти много другой полезной информации.

Проверить уже заданные псевдонимы можно вводом команды **alias** без параметров.

```
alias

alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mc='. /usr/libexec/mc/mc-wrapper.sh'
alias vi='vim'
alias view='vim -R'
alias which='(alias; declare -f) | /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot'
alias zegrep='zegrep --color=auto'
alias zfgrep='zfgrep --color=auto'
alias zgrep='zgrep --color=auto'
```

Команда показывает все псевдонимы для текущего пользователя.

Синтаксис **alias**:

```
alias <имя_псевдонима>=“<значение>/<команда> <аргумент>/<путь_к_файлу>”
```

Созданные псевдонимы сохраняются и будут работать только в данном терминале и только до его закрытия.

Пример создания алиаса для частоиспользуемой команды очистки вывода терминала **clear**:

```
alias c="clear"
alias

alias c='clear'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mc='. /usr/libexec/mc/mc-wrapper.sh'
alias vi='vim'
alias view='vim -R'
alias which='(alias; declare -f) | /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot'
alias zegrep='zegrep --color=auto'
alias zfgrep='zfgrep --color=auto'
alias zgrep='zgrep --color=auto'
```

Для очистки терминала в таком случае можно использовать только символ **c**.

Команда **unalias** удаляет созданный псевдоним.

```
unalias c
alias

alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
```

```
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mc='. /usr/libexec/mc/mc-wrapper.sh'
alias vi='vim'
alias view='vim -R'
alias which='(alias; declare -f) | /usr/bin/which --tty-only --read-alias --read-functions --show-tilde --show-dot'
alias zegrep='zegrep --color=auto'
alias zfgrep='zfgrep --color=auto'
alias zgrep='zgrep --color=auto'
```

Т.к. псевдонимы сохраняются только до закрытия терминала, необходимо их создавать в начале каждой терминальной сессии. Для этого можно добавить все необходимые команды в файл **~/.bashrc** , который представляет собой обычный bash-скрипт, исполняемый каждый раз при открытии терминала.

```
[user@localhost pub]$ cat ~/.bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]
then
    PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
```

Для удобства можно создать отдельный файл - **~/.bash_aliases**, в котором будут храниться все псевдонимы. Также это позволит уменьшить риск работы с **~/.bashrc**.

Для этого в конец файла **~/.bashrc** нужно добавить строки:

```
if [ -f ~/.bash_aliases ]; then
. ~/.bash_aliases
fi
```

Далее создать отдельный файл **~/.bash_aliases** командой:

```
nano ~/.bash_aliases
```

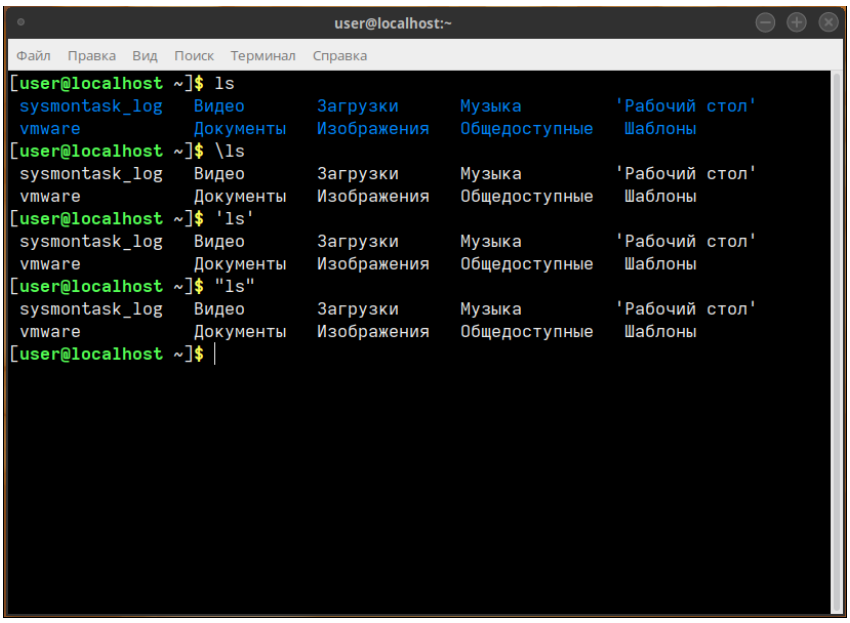
И вписать туда все нужные псевдонимы, например:

```
#Custom aliases XD
alias c=“clear“
alias cr=“cd /“
alias .=“cd ../“
alias up=“dnf update && dnf upgrade“
```

После обновления файла **~/.bashrc** (его исполнения или перезапуска терминала) все псевдонимы будут доступны при каждом входе в систему.

Чтобы временно отключить работу **alias** (например, когда созданный псевдоним совпадает с именем команды), при этом его не удаляя, необходимо перед командой поставить «\» либо использовать кавычки, например:

```
\c
“c“
'c'
```


user@localhost:~
Файл Правка Вид Поиск Терминал Справка
[user@localhost ~]$ ls
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$ \ls
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$ 'ls'
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$ "ls"
sysmontask_log Видео Загрузки Музыка 'Рабочий стол'
vmware Документы Изображения Общедоступные Шаблоны
[user@localhost ~]$

Утилита записи терминальной сессии asciinema

Установка
Запись терминальных сессий
Воспроизведение записанного сеанса
Выгрузка записанного сеанса

Asciinema — простая и эффективная утилита командной строки, которая запускает запись терминальной сессии.

Asciinema использует псевдотерминал, чтобы сохранить все символы, которые выводятся в консоль, а также информацию о времени. Записанный файл занимает очень мало места.

При воспроизведении все сохраненные символы повторно отображаются на экране с установленными интервалами. При этом все вводимые и выводимые символы при необходимости можно скопировать в буфер обмена.

Установка

Для установки **asciinema** перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

```
dnf install asciinema
```

Запись терминальных сессий

Для начала записи с сохранением в локальный файл выполните команду:

```
asciinema rec <имя_файла>
```

После этого действия в терминале записываются и сохраняются в файле под указанным названием (в примере — test_rec) в текущем рабочем каталоге.

Для того чтобы закончить запись, необходимо нажать комбинацию клавиш «Ctrl+d» или ввести команду exit. Когда запись будет завершена, на экране отобразится соответствующее сообщение.

Например:

```
asciinema rec test_rec

asciinema: recording asciicast to test_rec
asciinema: press <ctrl-d> or type "exit" when you're done

lsb_release -a

LSB Version: :core-4.1-amd64:core-4.1-noarch
Distributor ID: RED SOFT
Description: RED OS release MUROM (7.3.1) DESKTOP Standard Edition
Release: 7.3.1
Edition: Standard
Codename: MUROM

mkdir test_dir
ls -l

drwxrwxr-x. 2 user user 4096 апр 26 10:05 test_dir
-rw-rw-r--. 1 user user 2997 апр 26 10:05 test_rec

exit

exit
asciinema: recording finished
asciinema: asciicast saved to test_rec
```

Воспроизведение записанного сеанса

Для воспроизведения ранее записанного сеанса в терминале выполните команду:

```
asciinema play <имя_файла>
```

Выгрузка записанного сеанса

Локальную запись терминального сеанса можно выгрузить на сервер asciinema.org, для того чтобы можно было поделиться этой записью с другими людьми.

Для этого необходимо выполнить команду:

```
asciinema upload <имя_файла>
```

Например:

```
asciinema upload test_rec

View the recording at:

https://asciinema.org/a/5yyTPW5jud4nqhlUzPd3uCby3

This installation of asciinema recorder hasn't been linked to any asciinema.org
account. All unclaimed recordings (from unknown installations like this one)
are automatically archived 7 days after upload.

If you want to preserve all recordings made on this machine, connect this
installation with asciinema.org account by opening the following link:

https://asciinema.org/connect/da5948fa-55c2-4c21-a87d-4d63fd4be02a
```

В результате будет предоставлена ссылка, перейдя по которой можно просмотреть запись. Также в плеере можно скопировать в буфер обмена все, что вводится и выводится в терминале.

Существует возможность выгрузки записи сразу после ее окончания (без предварительного локального сохранения). Для этого выполните команду без указания имени файла:

```
asciinema rec

asciinema: recording asciicast to /tmp/tmp6imx6gtm-ascii.cast
asciinema: press <ctrl-d> or type "exit" when you're done

uname -r

5.15.10-1.el7.x86_64

exit

exit
asciinema: recording finished
asciinema: press <enter> to upload to asciinema.org, <ctrl-c> to save locally

View the recording at:

https://asciinema.org/a/TyRdslPzDQtAmJZQH0zfXUOzX

This installation of asciinema recorder hasn't been linked to any asciinema.org
account. All unclaimed recordings (from unknown installations like this one)
are automatically archived 7 days after upload.

If you want to preserve all recordings made on this machine, connect this
installation with asciinema.org account by opening the following link:

https://asciinema.org/connect/da5948fa-55c2-4c21-a87d-4d63fd4be02a
```

После окончания записи будет предложено 2 варианта:

- нажать «**Enter**», чтобы выгрузить запись на сервер;
- нажать комбинацию «**Ctrl+c**», чтобы сохранить запись локально.

Screen - запуск виртуальных терминалов в режиме сессий

Screen – это приложение, позволяющее запускать несколько виртуальных терминалов в режиме сессий. После того как сессия создана, от неё можно отключиться, а позже — снова подключиться, причём с любого другого хоста, на котором установлен SSH-клиент.

Процессы, запущенные в **screen**, продолжают выполняться и после того, как пользователь отключается от сессии или вообще от хоста в целом. Это ещё одна причина (кроме повышения удобства работы в командной строке вследствие использования возможности перехода между окнами), по которой используется **screen**.

Если соединение с интернетом ненадёжное, или у пользователя нет возможности поддерживать постоянное соединение, или существует необходимость запустить выполнение процесса в офисе, а остановить – дома, то использование **screen** – способ решить подобные проблемы.

Вы можете подробнее ознакомиться с информацией о работе терминальных мультиплексоров, просмотрев наши обучающие видео:

- на **RuTube** — Многооконность в консоли;
- в **Яндекс.Дзен** — Многооконность в консоли;
- в **VK Видео** — Многооконность в консоли.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки программы **screen** выполните команду:

```
dnf install screen
```

Для запуска новой сессии **screen** выполните команду:

```
screen
```

Все управляющие команды начинаются с комбинации клавиш «**Ctrl + a**», затем следует буква или сочетание клавиш. Буквы разных регистров выполняют разные команды. Также сочетания можно заменять текстом. Для его ввода нажмите «**Ctrl + a**» и «**:**», после чего вводите текст.

Команда **screen** обладает большим набором горячих клавиш. Полный их список можно посмотреть с помощью комбинации клавиш «**Ctrl+a ?**».

Рассмотрим основные из них:

- «**Ctrl+a c**» - Создать новое окно;
- «**Ctrl+a n**» - Перейти к следующем окну;
- «**Ctrl+a p**» - Перейти к предыдущему окну;
- «**Ctrl+a a**» - Изменить имя окна;
- «**Ctrl+a k**» - Закрыть текущее окно;
- «**Ctrl+a 1**» - Перейти к окну с номером 1 (можно использовать цифры от 0 до 9);
- «**Ctrl+a “**» - Вывести список окон, стрелками выбрать необходимую для перехода;
- «**Ctrl+a S**» - Разделить экран по горизонтали;
- «**Ctrl+a |**» - Разделить экран по вертикали;
- «**Ctrl+a Tab**» - Переключение между окнами;
- «**Ctrl+a d**» - Отключиться от сессии screen (при этом процессы и приложения запущенные в сессии продолжают выполняться).

При создании новой сессии **screen** можно задать для нее название с помощью ключа **-S <имя>**:

```
screen -S session1
```

Просмотреть список активных сессий можно командой:

```
screen -ls
```

Чтобы подключиться к существующей сессии, выполните команду:

```
screen -x <имя_сессии> | <ID_сессии>
```

Рассмотрим пример использования утилиты при работе на удаленном хосте через ssh-соединение.

После подключения к удаленному хосту создайте новую сессию screen с названием **session1**:

```
screen -S session1
```

Затем выполните на хосте необходимые действия и команды. Для примера запустим **ping** до ресурса **ya.ru**:

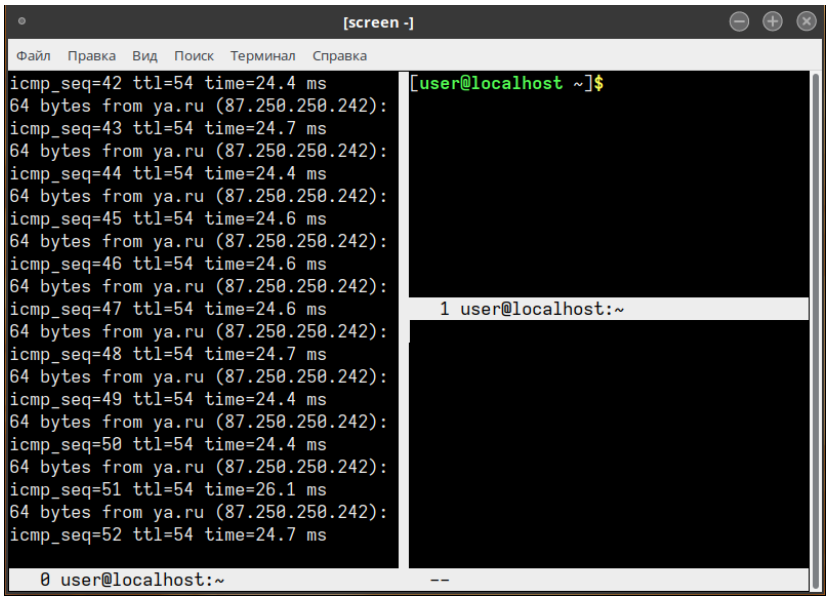
```
ping ya.ru
```

Для отключения от сессии нажмите сочетание «**Ctrl+a d**». При этом процесс **ping** продолжит выполнение, даже если разорвать ssh-подключение к удаленной машине. Чтобы вернуться в нашу сессию выполним команду:

```
screen -r session1
```

Можно увидеть, что утилита **ping** все еще работает.

Для того чтобы разделить экран терминала пополам, нужно сначала нажать комбинацию «**Ctrl+a**», а затем «**S**» или «|» (т.е. «**Shift + **»). При разделении окон новая оболочка не запускается на вновь созданной панели, для этого необходимо перейти в новое пространство с помощью «**Ctrl+a+Tab**» и вызвать новый экземпляр оболочки вручную с помощью «**Ctrl+a+C**».



Менеджер терминалов tmux

Tmux - это аналог утилиты **screen**, который имеет больше функций.

Вы можете подробнее ознакомиться с информацией о работе терминальных мультиплексоров, просмотрев наши обучающие видео:

- на **RuTube** — Многооконность в консоли;
- в **Яндекс.Дзен** — Многооконность в консоли;
- в **VK Видео** — Многооконность в консоли.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты выполните команду:

```
dnf install tmux
```

Чтобы создать новую сессию выполните команду:

```
tmux
```

Также можно создать сессию с указанием имени:

```
tmux new-session -s <имя_сессии>
```

По умолчанию для активации сочетания клавиш нужно нажать «**Ctrl+b**», отпустить, а потом нажать нужную клавишу.

Основные сочетания клавиш **tmux**:

- «**Ctrl+b c**» - создать новое окно;
- «**Ctrl+b w**» - выбрать окно из списка;
- «**Ctrl+b 0-9**» - открыть окно по его номеру;
- «**Ctrl+b ,**» - переименовать текущее окно;
- «**Ctrl+b %**» - разделить текущую панель по вертикали;
- «**Ctrl+b "**» - разделить текущую панель по горизонтали;
- «**Ctrl+b <стрелка>**» - перейти на панель, находящуюся в стороне, куда указывает стрелка;
- «**Ctrl+b Ctrl+<стрелка>**» - изменить размер текущей панели;
- «**Ctrl+b o**» - перейти на следующую панель;
- «**Ctrl+b ;**» - переключаться между текущей и предыдущей панелью;
- «**Ctrl+b x**» - закрыть текущую панель;
- «**Ctrl+b [**» - войти в режим копирования (подробнее ниже);
- «**Ctrl+b]**» - вставить из внутреннего буфера обмена **tmux**;
- «**Ctrl+b d**» - отключится от текущей сессии;
- «**Ctrl+b :**» - открыть командную строку.

По умолчанию поддержка мыши в **tmux** отключена, но если вы работаете в графическом окружении, можно её включить. Это даст несколько преимуществ: вы сможете выбирать активную панель мышкой, копировать текст во внутренний буфер обмена, менять размер панелей, использовать прокрутку для просмотра истории вывода и т.д. Для включения поддержки мыши откройте файл **~/.tmux.conf**:

```
nano ~/.tmux.conf
```

и добавьте следующие строки:

```
set-option -g -q mouse on bind-key -T root WheelUpPane if-shell -F -t = "#{alternate_on}" "send-keys -M" "select-pane -t =; copy-mode -e; send-keys -M" bind-key -T root WheelDownPane if-shell -F -t = "#{alternate_on}" "send-keys -M" "select-pane -t =; send-keys -M"
```

В сессии **tmux** нажмите сочетание «**Ctrl+b :**», чтобы открыть командную строку, и введите команду:

```
source-file ~/.tmux.conf
```

Теперь поддержка мыши включена.

Основные команды **tmux** для управления сессиями:

- **attach-session (attach)** - подключиться к уже существующей сессии. В параметре необходимо передать опцию **-t** и идентификатор сессии;
- **detach-session (detach)** - отключить всех клиентов (или переданного с помощью опции **-t**) от сессии, переданной в опции **-s**;
- **has-session** - проверить существует ли сессия, аналогично, надо передать идентификатор сессии;
- **kill-server** - остановить все запущенные сессии;
- **kill-session** - завершить сессию, переданную в параметре **-t**;
- **list-clients (lsc)** - посмотреть клиентов, подключенных к сессии **-t**;
- **list-sessions (ls)** - вывести список всех запущенных сессий;
- **new-session (new)** - создать новую сессию, можно передать имя сессии в опции **-s** и стартовую директорию в опции **-c**;
- **rename-session** - переименовать сессию, нужно передать идентификатор сессии и новое имя.

Принцип работы с **tmux** аналогичен работе со **screen**.

Создайте на хосте новую сессию:

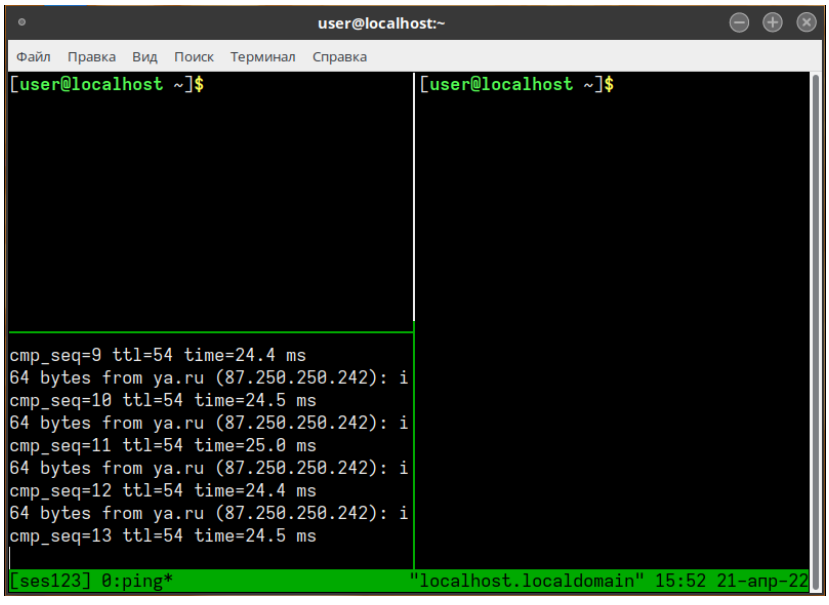
```
tmux new -s session1
```

Выполните необходимые действия. Отключитесь от сессии через комбинацию «**Ctrl+a d**».

Чтобы вернуться в сессию, выполните команду:

```
tmux attach -t session1
```

В рамках одной сессии может быть задействовано неограниченное количество окон; каждое из них может быть, в свою очередь, разделено на части.



Эмулятор терминала terminator

Установка
Функционал
Основные комбинации клавиш

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: terminator-2.1.1

Terminator — эмулятор терминала в РЕД ОС, который имеет возможность отображения нескольких терминалов в одном окне. Новые терминалы можно добавлять, разбивая текущее окно по горизонтали и по вертикали. **Terminator** позволяет экономить рабочее пространство, предоставляя возможность работы в одном окне.

Вы можете подробнее ознакомиться с информацией о работе терминальных мультиплексоров, просмотрев наши обучающие видео:

- на **RuTube** — Многооконность в консоли;
- в **Яндекс.Дзен** — Многооконность в консоли;
- в **VK Видео** — Многооконность в консоли.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

По умолчанию **terminator** предустановлен в РЕД ОС.

Если по каким-либо причинам утилита отсутствует в вашей системе, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду установки:

```
dnf install terminator
```

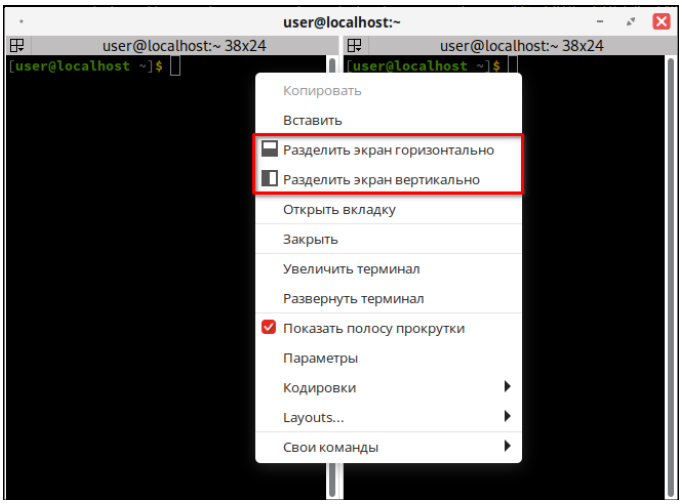
Работа в **terminator** не отличается от работы в **mate-terminal** и **gnome-terminal**.

Для запуска утилиты через терминал введите команду:

```
terminator
```

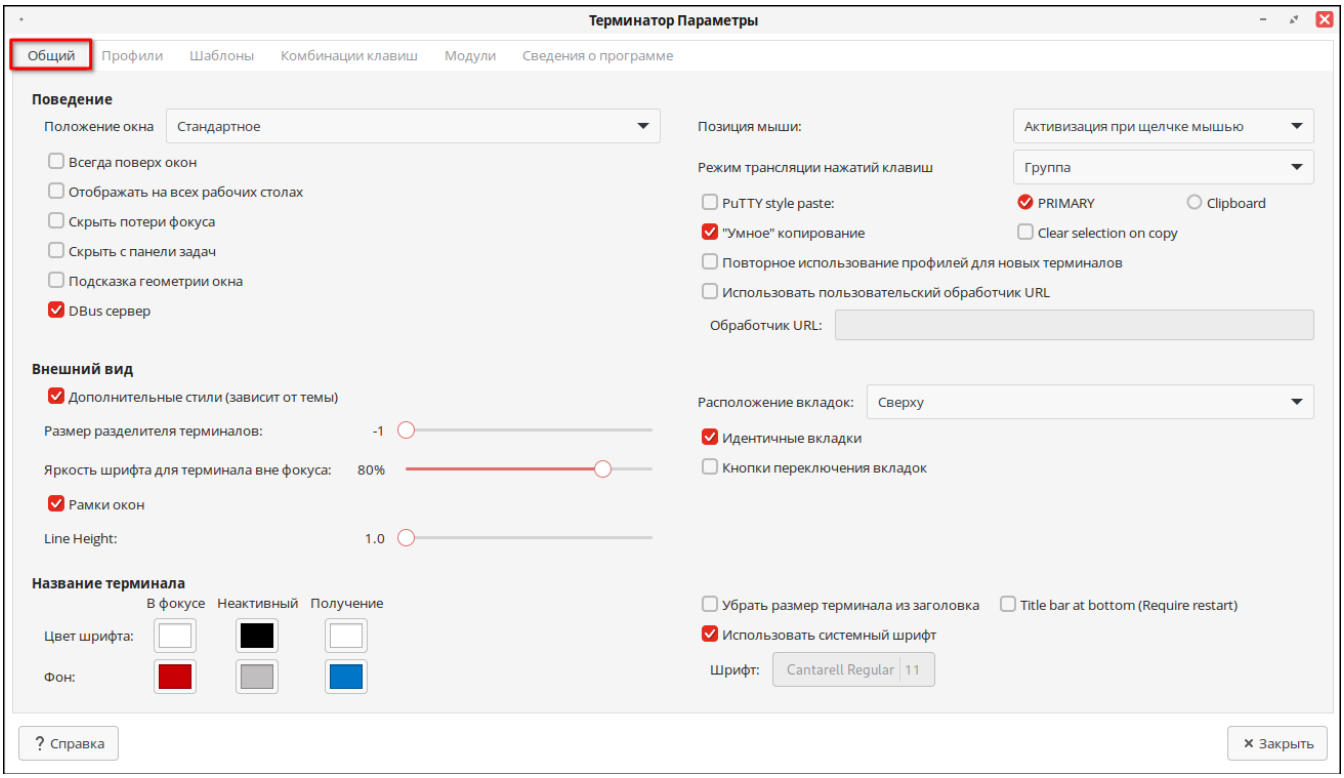
Функционал

Одной из отличительных особенностей **terminator** является разделение экрана на несколько окон. Сделать это можно, нажав ПКМ по пустому пространству окна и выбрав соответствующие опции.

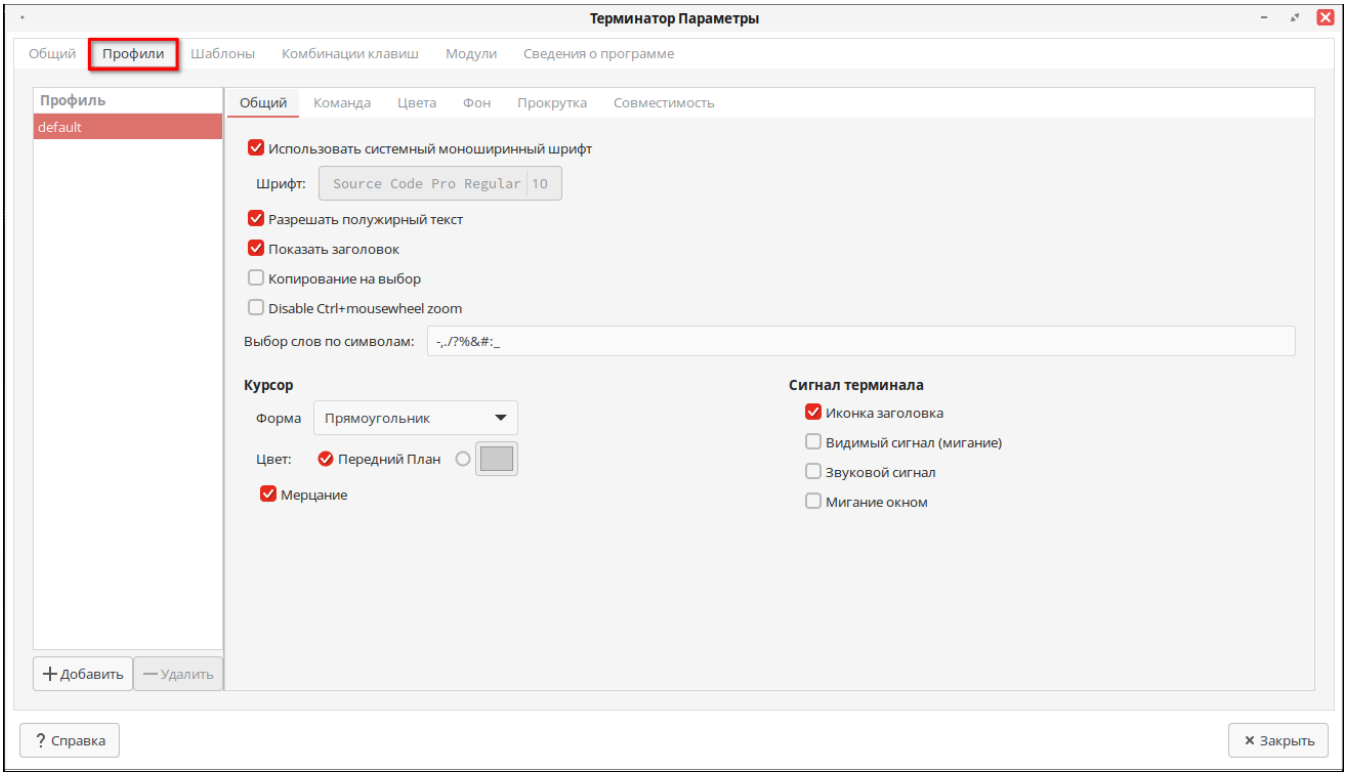


Утилита поддерживает большое количество настроек, которые можно определить индивидуально, для этого нажмите ПКМ по пустому пространству окна и перейдите в раздел «**Параметры**».

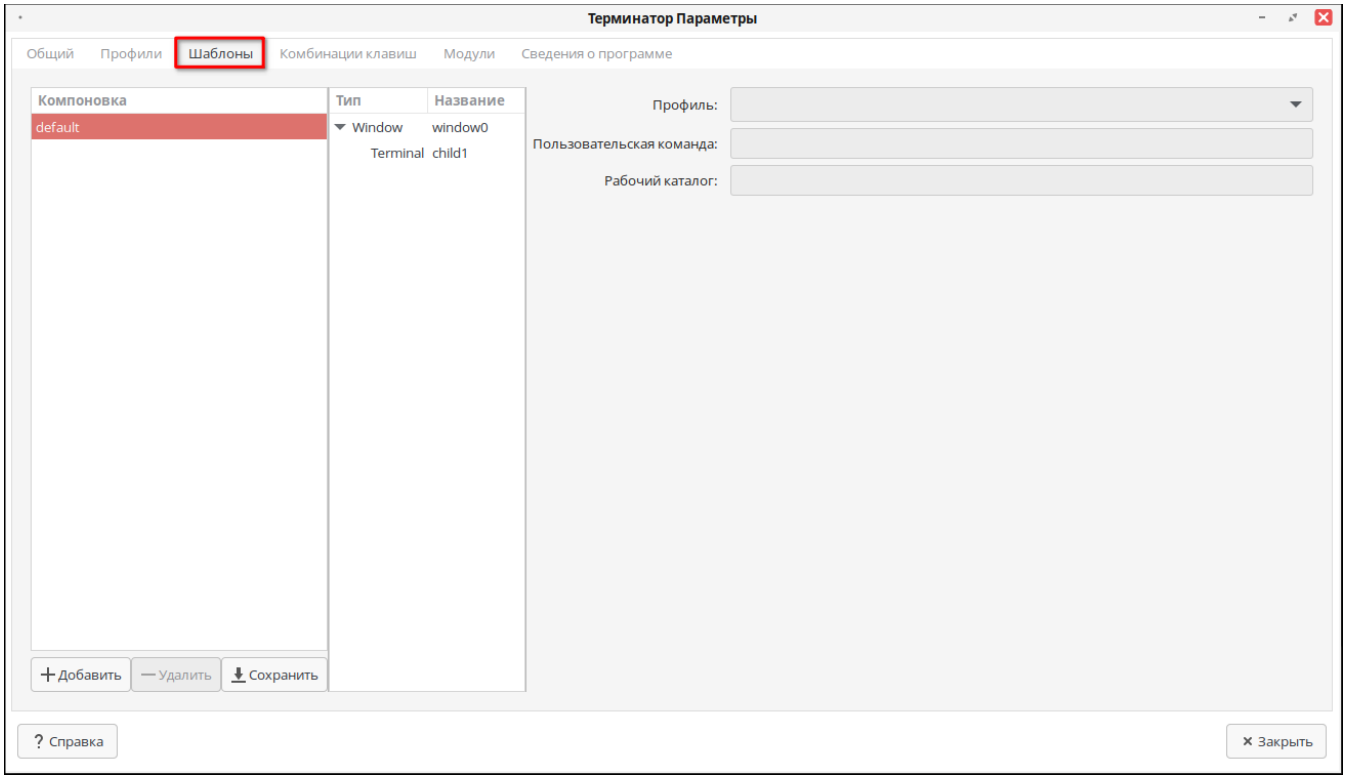
На вкладке «**Общий**» настраиваются основные параметры терминала. Здесь можно выбрать шрифт и размер шрифта по умолчанию, включить или отключить различные функции, такие как прокрутка назад или мигающий текст, а также указать размер и положение окна по умолчанию.



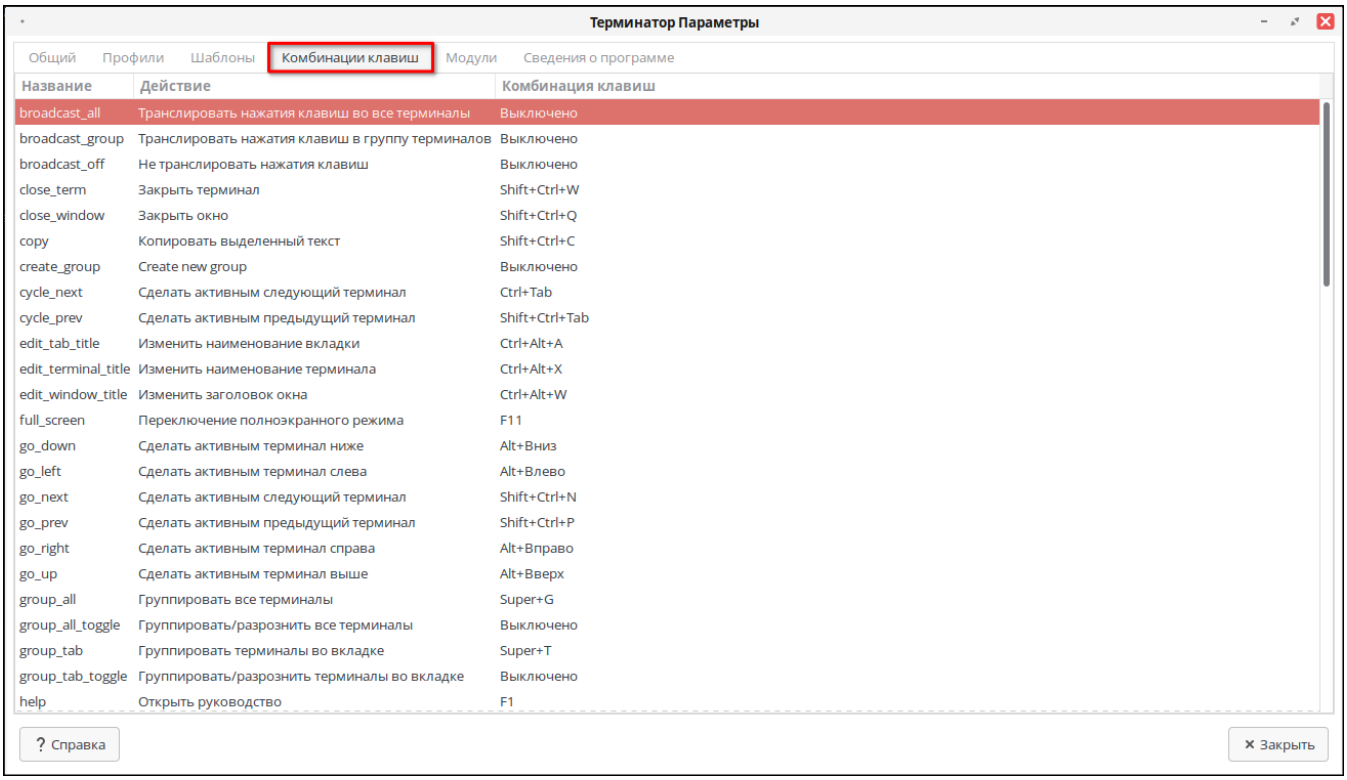
На вкладке «**Профили**» можно создавать и управлять профилями терминала. Профили можно дублировать и удалять, также есть возможность установить профиль по умолчанию при открытии новых окон и задать различные настройки для каждого профиля, такие как цветовая схема терминала, начальный рабочий каталог и команда, запускаемая при старте терминала.



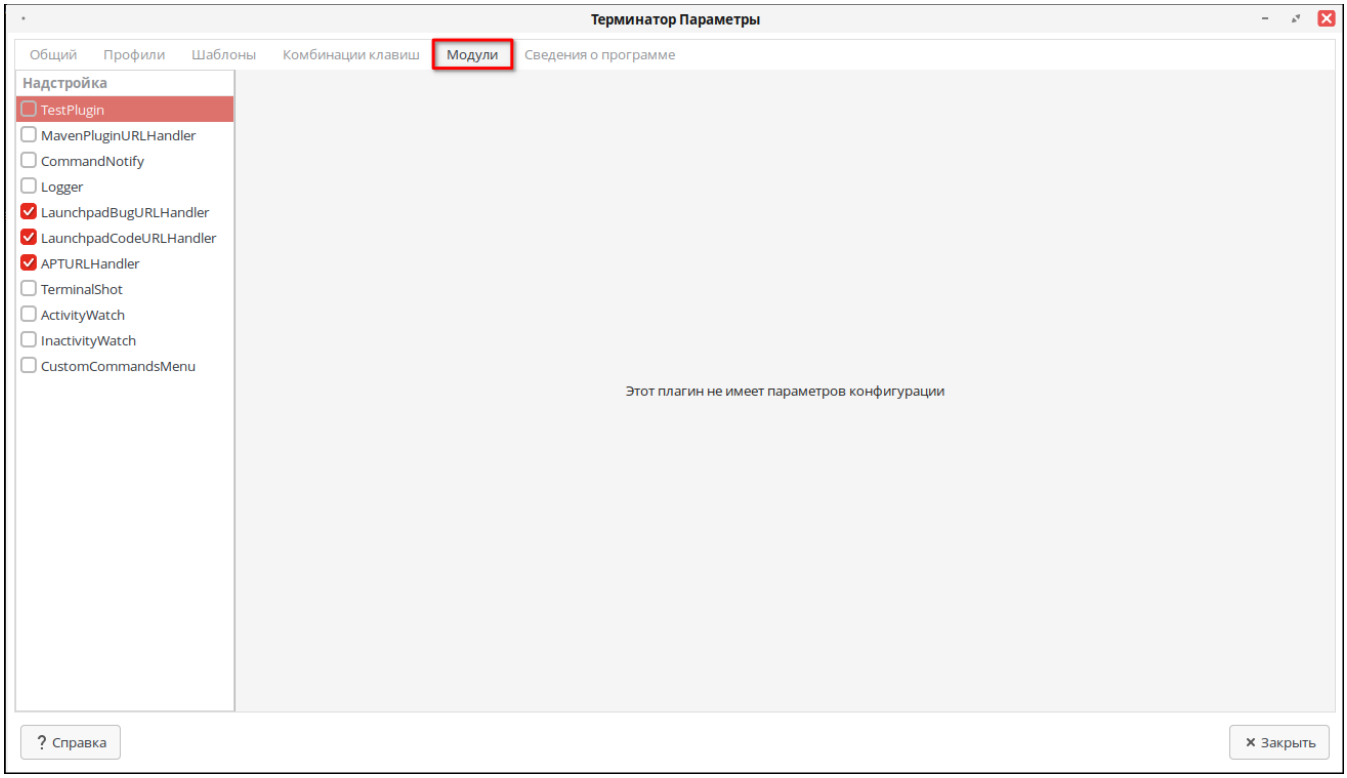
На вкладке «**Шаблоны**» настраивается макет окна **terminator**, включая количество рядов и столбцов терминалов, их размер и положение, а также то, как они должны быть расположены — горизонтально или вертикально. Здесь также можно сохранять и загружать различные конфигурации макета для быстрого переключения между различными вариантами расположения терминалов.



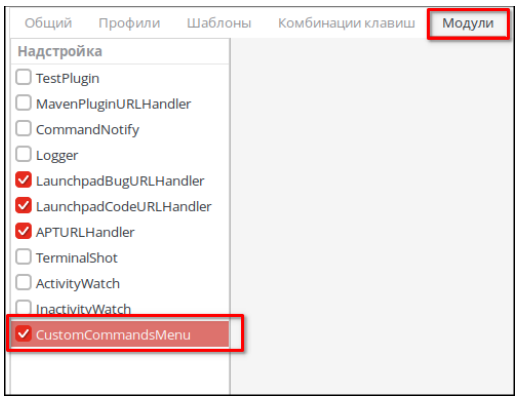
На вкладке «**Комбинации клавиш**» можно настроить существующие сочетания клавиш или создать новые для выполнения определенных действий, таких как разделение текущего терминала по вертикали или горизонтали, переключение между терминалами или переход в полноэкранный режим.



Утилита поддерживает различные модули, которые добавляют дополнительные возможности и функциональность. На вкладке «**Модули**» можно управлять и настраивать эти модули. Также можно включить или отключить определенные модули, указать специфические настройки модуля.

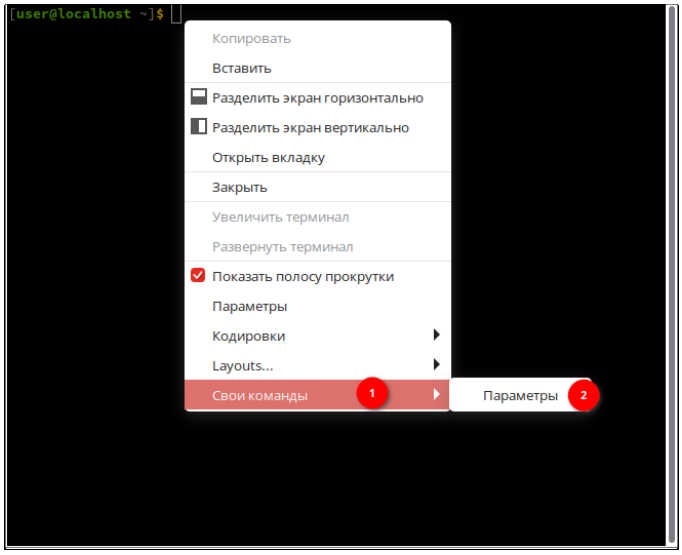


В качестве примера рассмотрим работу модуля **CustomCommandsMenu**, который добавляет пользовательские команды для быстрого доступа в контекстное меню терминала. Для этого в параметрах терминала на вкладке «**Модули**» включите модуль **CustomCommandsMenu**, установив на нем галочку.

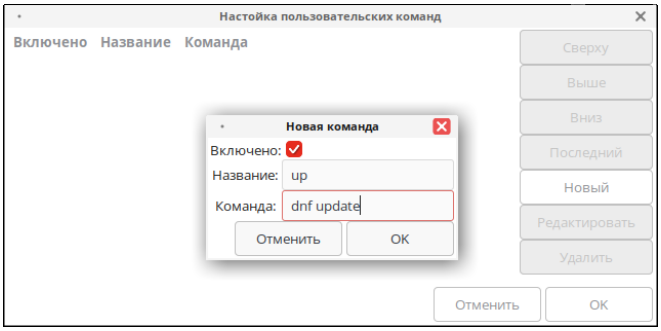


Закройте окно настроек.

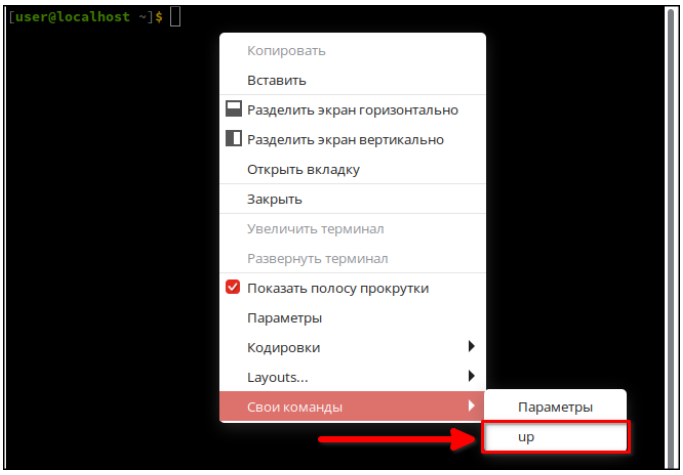
После этого нажмите ПКМ по свободной части окна терминала и в контекстном меню выберите «**Свои команды**» (1) — «**Параметры**» (2).



В открывшемся окне нажмите «**Новый**» для создания нового профиля команды. В окне «**Новая команда**» в поле «**Включено**» установите галочку, затем укажите название команды и пропишите непосредственно команду, которую должен будет выполнять терминал. Для сохранения изменений нажмите «**Да**».



После выполнения вышеперечисленных действий команда станет доступна из контекстного меню терминала. Для ее вызова нажмите ПКМ по свободной части окна терминала, в контекстном меню выберите «**Свои команды**» — «**up**».



Если все настроено верно, команда будет выполнена.

Основные комбинации клавиш

Следующие сочетания клавиш клавиатуры установлены по умолчанию и являются самыми часто используемыми в **terminator**:

- **«Ctrl + Shift + O»** — разделение окна терминала по горизонтали;
- **«Ctrl + Shift + E»** — разделение окна терминала по вертикали;
- **«Alt + ←|↑|→|↓»** — изменение фокуса терминала;
- **«Ctrl + Tab»** — перемещение между терминалами;
- **«F11»** — переход в полноэкранный режим;
- **«Ctrl + колесо мыши»** — увеличение и уменьшение шрифта;
- **«Ctrl + 0»** — сброс настроек до исходного состояния;
- **двойной клик ЛКМ по красной строке** — изменение имени окон.

expect - инструмент для автоматизации и тестирования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: expect-5.45.4-1

Expect — инструмент для автоматизации и тестирования, входящий в состав РЕД ОС. Предназначен для интерактивных приложений, таких как *telnet*, *ftp*, *passwd*, *fsck*, *rlogin*, *tip*, *ssh* и других.

Для установки **expect** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install expect
```

Для проверки работоспособности инструмента будет создан небольшой bash-скрипт, которому потребуется взаимодействие с пользователем. Для примера скрипт будет назван **questions**.

nano ./questions

```
#!/bin/bash
echo "Hello, what's your name?"
read $REPLY
echo "Can I ask you some question?"
read $REPLY
echo "What's your favorite OS?"
read $REPLY
```

Затем будет создан expect-скрипт, который запустит скрипт **questions** и ответит на его вопросы:

nano ./answerbot

```
#!/usr/bin/expect -f
set timeout -1
spawn ./questions
expect "Hello, what's your name?\r"
send -- "Im Dmitry\r"
expect "Can I ask you some question?\r"
send -- "Sure\r"
expect "What's your favorite OS?\r"
send -- "RedOS\r"
expect eof
```

В начале скрипта находится строка идентификации, которая (в данном примере) содержит путь к **expect**, т. к. интерпретацией скрипта будет заниматься именно **expect**. Во второй строке отключается тайм-аут путем присвоения переменной **timeout** значения **-1**. Остальная часть кода – это и есть автоматизация работы с bash-скриптом.

Сначала с помощью команды **spawn** запускается bash-скрипт с указанием пути к нему. Вместо пути к скрипту можно указать любую другую утилиту командной строки. Далее задана последовательность вопросов, поступающих от bash-скрипта, и ответов, которые дает expect-скрипт. Получив вопрос от подпроцесса, **expect** выдает ему заданный ответ и ожидает получения следующего вопроса.

В последней строке expect ожидает признака конца файла и скрипт, выполнив все действия до этой команды, завершается.

Рассмотрим данный пример на практике. Назначим скриптам права на исполнение с помощью команд:

```
chmod +x ./answerbot
chmod +x ./questions
```

и вызовем answerbot:

./answerbot

```
spawn ./questions
Hello, what's your name?
```

```
Im Dmitry
Can I ask you some question?
Sure
What's your favorite OS?
RedOS
```

Обратите внимание, что после запуска скрипта **answerbot** всё происходит полностью в автоматическом режиме. То же самое можно проделать для любой утилиты командной строки. Здесь необходимо отметить, что bash-скрипт в примере устроен очень просто, мы точно знаем, какие именно данные он выводит, поэтому написать expect-скрипт для взаимодействия с ним несложно.

Задача усложняется при работе с программами, которые написаны другими разработчиками. Однако здесь на помощь приходит средство для автоматизированного создания expect-скриптов.

Autoexpect — автоматизированное создание expect-скриптов

Autoexpect позволяет запускать программы, которые необходимо автоматизировать, после чего записывает то, что они выводят, и то, что пользователь вводит, отвечая на их вопросы. Вызовем **autoexpect** для нашего скрипта командой:

```
autoexpect ./questions

autoexpect started, file is script.exp
Hello, what's your name?
Dmitry
Can I ask you some question?
Sure
What's your favorite OS?
RED OS
autoexpect done, file is script.exp
```

В этом режиме взаимодействие с bash-скриптом ничем не отличается от обычного – мы сами вводим ответы на его вопросы.

После завершения работы с bash-скриптом **autoexpect** сообщит о том, что собранные данные записаны в файл **script.exp**. Проверим содержимое этого файла.

```
cat ./script.exp

set timeout -1
spawn ./questions
match_max 100000
expect -exact "Hello, what's your name?\r
"
send -- "Dmitry\r"
expect -exact "Dmitry\r
Can I ask you some question?\r
"
send -- "Sure\r"
expect -exact "Sure\r
What's your favorite OS?\r
"
send -- "RED OS\r"
expect eof
```

В целом, за исключением некоторых деталей, перед нами такой же скрипт, который мы написали самостоятельно. Если запустить этот скрипт, результат будет тем же.

Таким образом, можно автоматизировать работу практически любого bash-скрипта.

Общая информация

РЕД ОС, как и любой UNIX – многопользовательская операционная система. Также имеются группы пользователей, основное предназначение которых - облегчить управление большим количеством пользователей, а также более точно распределить права доступа к различным объектам системы. Пользователи и группы внутри системы обозначаются цифровыми идентификаторами - UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие еще группы входит пользователь, введите команду **id**, вывод ее может быть примерно следующим:

```
id

uid=1000(test) gid=1000(test) группы=1000(test),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Такая запись означает, что пользователь *test* (цифровой идентификатор 1000) входит в группы *test* и *wheel*. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

Вы можете подробнее ознакомиться с информацией по управлению пользователями в системе, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

ВНИМАНИЕ!

В связи с тем, что в дистрибутивах РЕД ОС большинство привилегированных системных утилит имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги.

Роли пользователей

Роль sysadm - администратор системы
Роль — пользователь системы

В ОС пользователи по умолчанию сопоставляются SELinux-пользователю <**unconfined_u**>. SELinux-пользователь <**unconfined_u**>, в свою очередь, сопоставлен ролям <**unconfined_r**> и <**system_r**>.

Обе роли <**unconfined_r**> и <**system_r**> сопоставляются доменам безопасности SELinux. Домены безопасности SELinux - это определённые окружения безопасности для процессов.

Неограниченный домен безопасности <**unconfined_t**> - зарезервированное окружение для процессов, которые в значительной степени освобождены от ограничений SELinux. Роль <**system_r**> сопоставляется доменам безопасности для системных процессов.

SELinux-пользователь <**unconfined_u**> имеет доступ к роли <**system_r**>, чтобы иметь возможность запускать системные процессы в своих доменах безопасности. SELinux-пользователь <**unconfined_u**> работает в домене безопасности <**unconfined_t**> через роль <**unconfined_r**>, которой он сопоставлен.

Команда «semanage» позволяет добавлять, изменять и удалять сопоставления между ОС- и SELinux-пользователями, так же как и другие настройки, касающиеся управления SELinux.

Чтобы с помощью команды «semanage» посмотреть какому SELinux- пользователю по умолчанию сопоставлены пользователи ОС, наберите:

```
semanage login -l | grep default
```

В примере выше пользователи по умолчанию сопоставлены SELinux- пользователю <**unconfined_u**>.

Чтобы изменить это и сопоставить пользователей по умолчанию ограниченному SELinux-пользователю с именем <**user_u**>, просто наберите:

```
semanage login -m -s user_u "__default__"
```

В результате все новые пользователи будут по умолчанию сопоставляться ограниченному SELinux-пользователю <**user_u**>.

Вы можете переопределить данное сопоставление при добавлении пользователей командой «**useradd**» используя опцию «**-Z**». Эта опция определяет, какому SELinux-пользователю должен быть сопоставлен пользователь ОС.

Например, наберите:

```
useradd -Z guest_u joe
```

В результате будет создан новый пользователь с именем **joe**, который будет сопоставлен SELinux-пользователю <**guest_u**>, вместо определённого по умолчанию SELinux-пользователя.

Также для изменения сопоставления между пользователем и SELinux-пользователем может быть использована команда «**usermod**» с опцией «**-Z**».

Существует несколько предопределённых профилей SELinux-пользователей. Список данных профилей можно вывести командой «**semanage**», наберите:

```
semanage user -l
```

SELinux-пользователь <**unconfined_u**> - это среда, в которой по умолчанию работают все пользователи. Этот пользователь в значительной степени освобождён от ограничений, накладываемых SELinux. Если Вы хотите повысить безопасность вашей системы, тогда не следует сопоставлять реальных пользователей, не пользователя root, SELinux-пользователю <**unconfined_u**>.

Вход пользователя root должен быть запрещён. Root должен иметь возможность войти с терминала только в случае крайней необходимости. Чтобы повысить безопасность использования root, можно сопоставить пользователя root SELinux-пользователю <**sysadm_u**>.

Ролевой доступ SELinux используется для обеспечения возможности назначения нескольких ограниченных окружений SELinux одному SELinux-пользователю.

В SELinux роли пользователя (*User Roles*) - это домены пользователя или пользовательские домены (*User Domains*). Когда упоминаются роли, часто имеется в виду дополнительный (*secondary*) пользовательский домен пользователя SELinux. Часто роли, предназначенные для использования в качестве дополнительных доменов пользователя, отличаются от основных (*primary*) доменов. Это объясняется тем, что пользователи ОС фактически не используют для входа в систему роли, созданные как дополнительные домены пользователя. Вместо этого пользователи Linux, используя команду «**sudo**» или комбинацию команд «**su**» и «**newrole**», осуществляют переключение домена или доменный переход (*Domain Transition*) к их дополнительной роли.

Роль sysadm - администратор системы

Пример роли, предназначенной для использования в качестве основного домена пользователя. SELinux пользователь <**sysadm_u**> сопоставлен роли <**sysadm_r**>. Это сопоставление можно увидеть, выполнив команду:

```
semanage user -l | grep sysadm_u
```

По умолчанию пользователи ОС, сопоставленные пользователю SELinux <**sysadm_u**>, работают с ролью <**sysadm_r**>. В этом случае <**sysadm_r**> — это основной домен пользователя.

SELinux пользователь <**staff_u**> также сопоставлен роли <**sysadm_r**>. Основным пользовательским доменом пользователя SELinux <**staff_u**> является (роль) <**staff_r**>. Контексты по умолчанию, обозначенные в **/etc/selinux/targeted/contexts/users/staff_u**, определяют, с какими пользовательскими доменами пользователи будут подключаться по умолчанию и с какими пользовательскими доменами пользователи могут войти, указав домен пользователя при входе.

По умолчанию SELinux пользователь <**staff_u**> входит в систему в домен пользователя <**staff_t**>. Роль <**sysadm_r**>, предназначенная для использования в качестве основного домена пользователя, может быть использована при входе, например, следующим образом:

```
ssh joe/sysadm_r@localhost.localdomain.tld
```

Также роль <**sysadm_r**> может быть использована при переходе домена выполнением команд «**sudo**» и «**su**» вместе с «**newrole**», как это предусмотрено для дополнительных доменов пользователей.

Пользовательский домен <**sysadm_t**> является окружением по умолчанию для SELinux-пользователя <**sysadm_u**> и предназначен для использования в качестве дополнительного окружения для SELinux-пользователя <**staff_u**>, хотя даже SElinux-пользователь <**staff_u**> может настроить подключаемый модуль аутентификации (*Pluggable Authentication Module*) <**pam_selinux**> для использования <**sysadm_t**> в качестве его основного домена пользователя.

Роль <user_r> — пользователь системы

Пользовательский домен, используемый только в качестве основного. Описание пользователя SELinux <**user_u**> приведено ранее.

Какие-то домены пользователей могут использоваться пользователями для входа в систему, потому что эти домены, например, имеют полномочия по доступу к домашней директории пользователя. Такие домены в предыдущей части назывались основными (*primary*) пользовательскими доменами. Другие домены созданы в качестве дополнительных. Пользователи, используя команды «**sudo**» или «**su**» вместе с «**newrole**», могут осуществить доменный переход (*Domain Transition*) к этим дополнительным доменам.

Дополнительные домены не могут использоваться для входа в систему. Далее будет продемонстрировано как создаётся такой дополнительный пользовательский домен. Целью является реализовать привилегированную роль SELinux, которой предоставлены полномочия по управлению DNS службой Bind.

Начнём с создания нового дополнительного домена пользователя с названием «**bindadm**», основанного на предустановленном домене SELinux <**webadm_t**>. Новый домен пользователя основан на двух файлах с исходным текстом политики SELinux (SELinux Source Policy):

- webadm.te;
- webadm.if.

Файлы исходных текстов политики SELinux с расширением "**.te**" называются Type Enforcement файлы. Файлы с расширением "**.if**" называются интерфейсными (Interface files). Файлы *Type Enforcement* содержат описания (*Declarations*) и политику (*Policy*), персональные или локальные для данного домена (*Domain*). Интерфейсные файлы содержат описания и политики, общие для этого домена и других доменов, желающими взаимодействовать с данным доменом.

```
mkdir ~/bindadm; cd ~/bindadm
echo "policy_module(bindadm, 0.0.1)" >> bindadm.te
echo "role bindadm_r" >> bindadm.te
echo "userdom_base_user_template(bindadm)" >> bindadm.te
echo "allow bindadm_t self:capability { dac_override dac_read_search kill sys_ptrace sys_nice" >> bindadm.te
echo "files_dontaudit_search_all_dirs(bindadm_t)" >> bindadm.te
echo "files_manage_generic_locks(bindadm_t)" >> bindadm.te
echo "files_list_var(bindadm_t)" >> bindadm.te
echo "selinux_get_enforce_mode(bindadm_t)" >> bindadm.te
echo "seutil_domtrans_setfiles(bindadm_t)" >> bindadm.te
echo "logging_send_syslog_msg(bindadm_t)" >> bindadm.te
echo "userdom_dontaudit_search_user_home_dirs(bindadm_t)" >> bindadm.te
```

Это основное содержимое для привилегированного дополнительного домена пользователя. Исключена политика, специфичная для управления службой Apache.

Теперь добавим политику, специфичную для управления службой Bind. Можно позаимствовать эту политику из исходных текстов политики для Bind. Как уже отмечалось, общая политика располагается в интерфейсных файлах. Это значит, что если мы хотим включить общую политику, относящуюся к Bind, можно посмотреть в соответствующем файле политики **bind.if**. Для включения этой политики в наш Type Enforcement файл требуется всего лишь добавить вызов этого интерфейса:

```
echo "bind_admin(bindadm_t, bindadm_r)" >> bindadm.te
```

На этом Type Enforcement файл bindadm заканчивается. Далее необходимо обеспечить другим доменам возможность взаимодействия с нашим доменом <**bindadm_t**>. Реализуем эту часть политики, взяв за основу файл **webadm.if**.

```
echo "## Bind administrator role" > bindadm.if
echo "########################################" >> bindadm.if
echo "##" >> bindadm.if
echo "## Change to the bind administrator role." >> bindadm.if
echo "##" >> bindadm.if
echo '##' >> bindadm.if
echo "##" >> bindadm.if
echo "## Role allowed access." >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "##" >> bindadm.if
echo "#" >> bindadm.if
echo "interface(\`bindadm_role_change',\`" >> bindadm.if
echo " gen_require(\`" >> bindadm.if
echo " role bindadm_r;" >> bindadm.if
echo " ')" >> bindadm.if
echo " allow  $1 bindadm_r;" >> bindadm.if
echo "')" >> bindadm.if
```

Позже общая политика администратора **Bind** (Bind Administrator Shared policy) будет использоваться в нашем основном специально созданном пользовательском домене SELinux.

Следующим шагом будет создание специализированного пользовательского домена SELinux для обслуживания Bind, разрешающего данному домену осуществлять переход к роли <**bindadm_r**> вызовом интерфейса <**bindadm_role_change**>. Создаваемый домен SELinux будет основан на пользовательском домене <**staff_t**>, описание политики смотрим в файле **staff.te**.

```
echo "policy_module(bindguy, 0.0.1)" > bindguy.te
echo "role bindguy_r;" >> bindguy.te
echo "userdom_unpriv_user_template(bindguy)" >> bindguy.te
echo "sudo_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "ssh_role_template(bindguy, bindguy_r, bindguy_t)" >> bindguy.te
echo "kernel_read_ring_buffer(bindguy_t)" >> bindguy.te
echo "kernel_getattr_core_if(bindguy_t)" >> bindguy.te
echo "kernel_getattr_message_if(bindguy_t)" >> bindguy.te
echo "kernel_read_software_raid_state(bindguy_t)" >> bindguy.te
echo "auth_domtrans_pam_console(bindguy_t)" >> bindguy.te
echo "libs_manage_shared_libs(bindguy_t)" >> bindguy.te
echo "seutil_run_newrole(bindguy_t, bindguy_r)" >> bindguy.te
echo "netutils_run_ping(bindguy_t, bindguy_r)" >> bindguy.te
echo "domain_read_all_domains_state(bindguy_t)" >> bindguy.te
echo "domain_getattr_all_domains(bindguy_t)" >> bindguy.te
echo "domain_obj_id_change_exemption(bindguy_t)" >> bindguy.te
echo "files_read_kernel_modules(bindguy_t)" >> bindguy.te
echo "kernel_read_fs_sysctls(bindguy_t)" >> bindguy.te
echo "modutils_read_module_config(bindguy_t)" >> bindguy.te
echo "modutils_read_module_deps(bindguy_t)" >> bindguy.te
echo "miscfiles_read_hwdata(bindguy_t)" >> bindguy.te
echo "term_use_unallocated_ttys(bindguy_t)" >> bindguy.te
```

Чтобы разрешить домену <**bindguy_t**> осуществлять переход в ограниченное окружение SELinux <**bindadm_t**>, добавим вызов интерфейса <**bindadm_role_change**>, определённого в нашем интерфейсном файле **bindadm.if**:

```
echo "bindadm_role_change(bindguy_r)" >> bindguy.te
```

Можно также автоматически создать сопоставление пользователя SELinux с именем <**bindguy_u**> ролям <**bindguy_r**>, <**bindadm_r**> и <**system_r**>. Роль <**system_r**> включается, чтобы <**bindadm_t**> мог остановить, запустить и перезапустить системную службу **bind**.

```
echo "gen_user(bindguy_u, user, bindguy_r system_r bindadm_r, s0,  s0 - mls_systemhigh,
mcs_allcats)" >> bindguy.te
```

Чтобы программы входа знали, что bindguy допустимый пользователь, добавим контексты по умолчанию для этого пользователя, взяв за основу контексты по умолчанию пользователя <**staff_u**>:

```
cp /etc/selinux/targeted/contexts/users/staff_u
/etc/selinux/targeted/contexts/users/bindguy_u
sed -i 's/staff/bindguy/g'
/etc/selinux/targeted/contexts/users/bindguy_u
```

Теперь можно собрать и установить обе политики bindguy и bindadm:

```
make -f /usr/share/selinux/devel/Makefile
semodule -i bindguy.pp bindadm.pp
```

Далее командой «**useradd**», опцией «**-Z**» и параметром <**bindguy_u**> можно создать нового пользователя Linux:

```
useradd -Z bindguy_u bindguy
```

Для того чтобы разрешить пользователю *bindguy* использовать команду «**sudo**» для автоматического перехода к пользователю root и SELinux-домену <**bindadm_t**>, добавим в **/etc/sudoers**:

```
echo "bindguy ALL=(ALL) ROLE=bindadm_r TYPE=bindadm_t ALL" » /etc/sudoers
```

При входе пользователя bindguy в систему он оказывается в пользовательском домене <**bindguy_t**>, основанном на домене <**staff_t**>. Домен <**bindguy_t**> может осуществлять переход в домен <**bindadm_t**>, используемый с правами root и позволяющий управлять службой Bind.

Например, выполнив следующую команду, пользователь bindguy сможет перезапустить службу bind:

```
systemctl restart named
```

Также пользователю *bindguy* разрешается редактировать различные конфигурационные файлы и файлы информационного наполнения Bind. При этом, например, пользователь *bindguy* не имеет прав изменить пароль пользователя root.

Подведём итог. Процессы и файлы маркируются метками - контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально). Когда SELinux включён, вся эта информация используется для принятия решения о предоставлении доступа.

В контексте SELinux используется следующий синтаксис SELinux:

```
<user>:<role>:<type>:<level>:<пользователь_SELinux>
```

<**Пользователь_SELinux**> - это сущность, определённая в политике, которая отвечает за определённый набор ролей и за определённый набор MLS-уровней. Каждый пользователь ОС сопоставлен пользователю SELinux посредством политики SELinux. Это позволяет пользователям наследовать ограничения, установленные на пользователей SELinux. Сопоставленные сущности пользователей SELinux используются в контексте SELinux для процессов в сессии, в порядке определения, для каких ролей и уровней они применимы.

Роль - это часть модели безопасности Ролевого управления доступом **Role-Based Access Control** (RBAC). Роль - это атрибут RBAC. Пользователи SELinux авторитетны для ролей, а роль авторитетна для доменов. Каждая конкретная роль определяет, какие домены могут быть доступны для пользователей с этой ролью. Роль служит промежуточным звеном между доменами и пользователями SELinux. Роль, которой обладает пользователь, определяет, в какие домены может попасть пользователь - фактически, этот механизм управляет доступностью объектов. Таким образом, уменьшается риск, связанный с уязвимостью повышения привилегий в системе. По умолчанию пользователям назначена неопределённая роль, не накладывающая ограничений на пользователя. Но есть и предопределённые роли пользователя и администратора системы, которые могут быть назначены администратором для повышения безопасности системы.

Тип - это атрибут *Type Enforcement*. Тип определяет домен для процессов и тип для файлов. Правила политики SELinux определяют, как типы взаимодействуют друг с другом, является ли тип доменом, получающим доступ к типу, или доменом, получающим доступ к другому домену. Доступ разрешается, только если существует определённое правило политики SELinux, позволяющее данное действие.

Контекст безопасности записывается в атрибуты файла (в файловой системе) и создаётся при установке SELinux (операция **labeling**). Уже присвоенный контекст безопасности может быть впоследствии изменён - операцией «**transition**».

Пароли пользователей

/etc/passwd — файл, содержащий в текстовом формате список пользовательских учётных записей (аккаунтов).

Является первым и основным источником информации о правах пользователя операционной системы. Существует в большинстве версий и вариантов UNIX-систем. Обязан присутствовать в POSIX-совместимой операционной системе.

Принцип:

```
login : password : UID : GID : GECOS : home : shell
```

Каждая строка файла описывает одного пользователя и содержит семь полей, разделённых двоеточиями:

- регистрационное имя или логин;
- хеш пароля;
- идентификатор пользователя;
- идентификатор группы по умолчанию;
- информационное поле GECOS;
- начальный (он же домашний) каталог;
- регистрационная оболочка, или shell.

Вы можете подробнее ознакомиться с информацией о файле **/etc/passwd**, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Основным назначением **/etc/passwd** является сопоставление логина и идентификатора пользователя (UID). Изначально поле пароля содержало хеш пароля и использовалось для аутентификации. Однако, в связи с ростом вычислительных мощностей процессоров появилась серьёзная угроза применения простого перебора для взлома пароля. Поэтому все пароли были перенесены в специальные файлы, такие как **/etc/shadow**. Эти файлы недоступны для чтения обычным пользователям. Такой подход называется механизмом скрытых паролей.

Регистрационные имена должны быть уникальными и представлять собой строки не длиннее 32 символов (любые, кроме двоеточия и символа новой строки). По сути, имя пользователя — это его короткий и легко запоминаемый псевдоним, который используется при входе в систему и часто включается в адреса электронной почты.

Идентификатор пользователя — это число от 0 до 2^{32}-1. Пользователь с идентификатором «0» (обычно *root*) называется суперпользователем и имеет право на выполнение любых операций в системе. Принято соглашение о выделении «специальным» пользователям (*bin, daemon*), назначение которых — только запуск определённых программ, маленьких идентификаторов (меньше 100 или, в некоторых дистрибутивах Linux, меньше 500).

В UNIX пользователь может принадлежать к одной или нескольким группам, которые используются для задания прав более чем одного пользователя на тот или иной файл. Максимальное количество групп, в которых может состоять один пользователь, разное в разных вариантах системы.

Список групп с их участниками задаётся в **/etc/group**. В файле же **/etc/passwd** указывается идентификатор группы по умолчанию.

Всем файлам, созданным пользователем после регистрации в системе, будет автоматически присвоен этот номер группы (исключение — если для каталога, в котором создаётся файл, установлен в правах бит SGID, то будет присвоена такая же группа, как у самого каталога).

/etc/group содержит записи обо всех группах в системе. Каждая его строка содержит:

- символьное имя группы;
- пароль группы — устаревшее поле, сейчас не используется. В нём обычно стоит «x»;
- идентификатор группы, или GID;
- список имён участников, разделённых запятыми.

Пример записи:

```
bin:x:1:root,bin,daemon
```

Здесь сообщается, что группа *bin* имеет *GID=1*, а входят в неё пользователи *root, bin и daemon*.

GECOS

Поле GECOS хранит вспомогательную информацию о пользователе (номер телефона, адрес, полное имя и так далее). Оно не имеет чётко определённого синтаксиса.

Тем не менее, демон **fingerd** предполагает, что в нём содержатся следующие элементы, разделённые запятыми:

- полное имя;
- адрес офиса или домашний адрес;
- рабочий телефон;
- домашний телефон.

С помощью утилиты **chfn** можно изменять эту информацию, а с помощью **finger** — узнать, например, полное имя любого пользователя в системе (или даже на другом компьютере сети).

Пример строки с заполненным полем GECOS:

```
tester:x:210:8:Edward Chernenko,Marx Street 10,4554391,5454221:/home/ed:/bin/bash
```

После входа в систему пользователь оказывается в своём домашнем каталоге. Исторически сложилось так, что домашний каталог пользователя *root* называется **/root**, а остальные имеют вид **/home/**. Но могут применяться и другие схемы.

Если на момент входа в систему домашний каталог отсутствует, то система выдаёт сообщение об ошибке и отказывается допустить пользователя к командной строке. Такое поведение НЕ характерно для GNU/Linux; в большинстве дистрибутивов этой ОС просто выводится предупреждение, после чего пользователь попадает в каталог «/». Это можно изменить посредством установки параметра **DEFAULT_HOME** в файле **/etc/login.defs** в значение «**no**».

Следует отметить, что при использовании графического интерфейса (KDE, GNOME) пользователь не увидит предупреждения или сообщения об ошибке, но просто будет выведен из системы безо всяких объяснений (так как оконный менеджер не сможет выполнить запись в нужный каталог, такой как **~/.gnome**).

В поле регистрационной оболочки задаётся **shell**, то есть интерпретатор командной строки. Здесь может быть указана любая программа, и пользователь может сам выбирать для себя наиболее подходящую при помощи команды **chsh**. Тем не менее, некоторые системы в целях безопасности требуют, чтобы суперпользователь явно разрешил использовать приложение в качестве интерпретатора командной строки. Для этого используется специальный файл **/etc/shells**, содержащий список «допустимых» оболочек.

vipw - запускает текстовый редактор, указанный в переменной среды *EDITOR* (или редактор по умолчанию, обычно *vi*), загружая в него копию файла **/etc/passwd**. После закрытия редактора переносит временную копию в сам файл. Не позволяет двум пользователям выполнять редактирование одновременно.

В файле **/etc/shadow** хранятся хеши паролей всех пользователей в системе. Процессы суперпользователя могут читать его напрямую, а для остальных создана специальная библиотека PAM. Она позволяет непривилегированным приложениям спрашивать у неё, правильный ли пароль ввёл пользователь, и получать ответ. Библиотека PAM как правило действует с привилегиями вызвавшего процесса. Таким образом, хеш не попадает «в чужие руки».

В ранних UNIX пароль шифровался с помощью одного из вариантов DES, теперь используется MD5-хеширование или blowfish-хеширование (bcrypt). MD5-хеши всегда записываются после префикса «**1**».

Перед хешированием к паролю добавляются случайные символы — «*salt*» (соль, от англ. add salt to something — сделать что-либо более интересным; в русскоязычных источниках иногда используется термин «затравка»). *Salt* также приписывается к началу полученного хеша. Благодаря *salt* нельзя при простом просмотре файла обнаружить пользователей с одинаковыми паролями.

Кроме имени (первое поле каждой строки) и хеша (второе поле) в файле **/etc/shadow** также хранятся:

- дата последнего изменения пароля;
- через сколько дней можно будет поменять пароль;
- через сколько дней пароль устареет;
- за сколько дней до того, как пароль устареет, начать напоминать о необходимости смены пароля;
- через сколько дней после того, как пароль устареет, заблокировать учётную запись пользователя;
- дата, при достижении которой учётная запись блокируется;
- зарезервированное поле.

Даты обозначаются как число дней с *1 января 1970 года* (начало эпохи UNIX).

Обязательная регулярная смена паролей — это популярная административная мера, призванная сделать учётные записи более защищёнными. К сожалению, многие пользователи после принудительного изменения возвращают себе старый пароль.

Утилита passwd

Окружение

- **Версия РЕД ОС**: 8
- **Версия ПО:** passwd 0.80-9

Утилита **passwd** поддерживает традиционные опции *passwd* и утилит *shadow*.

Синтаксис:

```
passwd
```

Вы можете подробнее ознакомиться с информацией о работе с утилитой **passwd**, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Возможные опции:

Опция	Значение опции
-d,- -delete	Удалить пароль для указанной записи.
-f,- -force	Форсировать операцию.
-k,- -keep-tokens	Сохранить не устаревшие пароли.
-l,- -lock	Блокировать указанную запись.
--stdin	Прочитать новые пароли из стандартного ввода.
-S,- -status	Дать отчет о статусе пароля в указанной записи.
-u,- -unlock	Разблокировать указанную запись.
-?,- -help	Показать справку и выйти.
--usage	Дать короткую справку по использованию.
-V,- -version	Показать версию программы и выйти.

Код выхода:

При успешном завершении **passwd** заканчивает работу с кодом выхода **0**. Код выхода **1** означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

Примеры:

Удаление пароля пользователя:

```
passwd -d <имя_пользователя>
```

Добавление пароля из стандартного ввода:

```
passwd --stdin <имя_пользователя>
```

Блокировка пароля:

```
passwd -l <имя_пользователя>
```

Разблокировать пароль:

```
passwd -u <имя_пользователя>
```

Создать новый пароль:

```
passwd <имя_пользователя>
```

Добавление нового пользователя

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Для добавления нового пользователя используйте команды **useradd** и **passwd**.

Вы можете подробнее ознакомиться с информацией по добавлению новых пользователей, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

В примере в качестве первоначально введенного пароля указана последовательность символов «*123*», затем введен надежный пароль:

```
useradd test1
passwd test1

Изменение пароля пользователя test1.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

В результате описанных действий в системе появился пользователь *test1* с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды **passwd** - но если он попытается поставить слабый пароль, система откажет ему (в отличие от **root**) в изменении.

В дистрибутивах ОС для проверки паролей на слабость используется модуль PAM **passwdqc**.

Программа **useradd** имеет множество параметров, которые позволяют менять ее поведение по умолчанию. Например, можно принудительно указать, какой будет **UID** или какой группе будет принадлежать пользователь.

Синтаксис:

```
useradd [-u <идентификатор> [-o] [-i]] [-g <группа>] [-G <группа>[[,<группа>] . . .]] [-d <каталог>] [-s <shell>] [-c <комментарий>] [-m [-k <skel_dir>]] [-f <inactive>] [-e <expire>] [-p <passgen>] [-a <событие>[, . . .]] <per_имя>
```

Опции:

Опция	Значение опции
-u <идентификатор>	Идентификационный номер пользователя (**UID**). Этот номер должен быть неотрицательным целым числом, не превосходящим **MAXUID**, определенным в **sys/param.h**. По умолчанию используется следующий доступный (уникальный) не устаревший **UID**, больший 99. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (**NIS**).
-o	Опция позволяет дублировать **UID** (сделать его не уникальным). Поскольку защита системы в целом, а также целостность контрольного журнала (**audit trail**) и учетной информации (**accounting information**) в частности, зависит от однозначного соответствия каждого **UID** определенному лицу, использовать эту опцию не рекомендуется (чтобы обеспечить учет действий пользователей). Опция действительна только с использованием опции -u.
-g <группа>	Имя или числовой идентификатор первичной группы пользователя. Группа с таким именем должна существовать. Опция задает основную группу (**primary group**) для нового пользователя. По умолчанию используется стандартная группа, указанная в файле **/etc/default/useradd**. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (**NIS**).
-G <группа>[[,<группа>] . . .]	Список дополнительных групп, членом которых также является пользователь. Каждая группа отделяется от следующей запятой без пробелов. На группы распространяются те же ограничения, что и на группу, указанную с параметром -g. По умолчанию пользователь принадлежит только к начальной группе. Опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (**NIS**).
-d <каталог>	Начальный каталог (**home directory**) нового пользователя. Длина этого поля не должна превышать 256 символов. По умолчанию используется **HOMEDIR/a**, где **HOMEDIR** - базовый каталог для начальных каталогов новых пользователей, **a** - регистрационное имя нового пользователя.
-s <shell>	Полный путь к программе, используемой в качестве начального командного интерпретатора для пользователя сразу после регистрации. Длина этого поля не должна превышать 256 символов. По умолчанию это поле - пустое, что заставляет систему использовать стандартный командный интерпретатор **/usr/bin/sh**. В качестве значения **shell** должен быть указан существующий выполняемый файл.

Опция	Значение опции
-c <комментарий>	Любая текстовая строка. Обычно, здесь коротко описывается учётная запись, и в настоящее время используется как поле для имени и фамилии пользователя. Информация хранится в записи пользователя в файле **/etc/passwd**. Длина этого поля не должна превышать 128 символов.
-m	Создает начальный каталог нового пользователя, если он еще не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу.
-k <skel_dir>	Основной каталог, содержащий файлы и каталоги, которые будут скопированы в домашнюю директорию пользователя, когда домашняя директория создается с помощью **useradd**. Этот параметр действителен только в том случае, если задан параметр `-m` (или `--create-home`). Если этот параметр не задан, основной каталог определяется переменной SKEL в **/etc/default/useradd** или, по умолчанию, **/etc/skel**.
-f <inactive>	Срок действия учетной запсии. Если значение равно 0, учетная запись блокируется сразу после того, как пароль устареет, а если значение равно -1, то эта функция не используется. Если значение не указано, **useradd** будет использовать срок действия по умолчанию, указанный переменной `INACTIVE` в файле **/etc/default/useradd**, или -1 по умолчанию.
-e <expire>	Дата, с которой учетная запись пользователя будет отключена. Дата указывается в формате **ГГГГ-ММ-ДД**. Если значение не указано, **useradd** будет использовать дату истечения срока действия по умолчанию, указанную переменной `EXPIRE` в файле **/etc/default/useradd**, или пустую строку (без истечения срока действия) по умолчанию.
<рег_имя>	Строка печатных символов, задающая регистрационное имя для нового пользователя. В ней не должно быть двоеточий (:) и символов перевода строки (\n). Она также не должна начинаться с прописной буквы.

Редактирование имеющихся пользовательских записей

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Для модификации уже имеющихся пользовательских записей применяется утилита **usermod**:

```
usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь *test1* - теперь это audio, rpm, test1.

```
usermod -l test2 test1
```

Будет произведена смена имени пользователя с *test1* на *test2*.

Вы можете подробнее ознакомиться с информацией по изменению имеющихся пользовательских записей, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Команды **usermod -L test2** и **usermod -U test2** соответственно временно блокируют возможность входа в систему пользователю *test2* и возвращают все на свои места.

> **Примечание.**
>
> Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используйте утилиту **chpasswd**. На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как **<имя>:<пароль>**.

Удаление пользователей

Удаление локальных пользователей
Удаление доменных пользователей

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Удаление локальных пользователей

Для удаления локальных пользователей используется утилита **userdel**. Например:

```
userdel test2
```

Данная команда удалит пользователя **test2** из системы. Если будет дополнительно задан параметр **-r**, будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он еще работает в системе.

Вы можете подробнее ознакомиться с информацией по удалению пользователей из системы, просмотрев наши обучающие видео:

- на **RuTube** — Создание и управление пользователями;
- в **Яндекс.Дзен** — Создание и управление пользователями;
- в **VK Видео** — Создание и управление пользователями.

На наших каналах вы также сможете найти много другой полезной информации.

Утилиты **vigr** и **vipw** используются для ручного редактирования файлов **/etc/passwd** и **/etc/group**, в которых хранятся основные записи о пользователях и группах в системе.

> Не рекомендуется создавать пользователей с правами сверх необходимых. Предпочтительнее создать серию новых групп и включить в них требуемого пользователя. А для данных групп установить соответствующие права на объектах файловой системы (утилиты **chmod** и **chown**).

Удаление доменных пользователей

Для удаления доменного пользователя из системы необходимо:

1. Удалить домашний каталог доменного пользователя:

```
rm -rf /home/<имя_пользователя>
```

2. Удалить его учетную запись с экрана входа в систему:

```
rm /var/lib/AccountsService/users/<имя_пользователя>
```

Управление пользователями и группами из консоли

Просмотреть всех локальных пользователей:

```
cat /etc/passwd
```

Просмотреть все локальные группы:

```
cat /etc/group
```

Посмотреть группы, в которых состоит пользователь.

Формат вывода: `<основная_группа> : <группы>`

```
groups user
```

Для добавления нового пользователя используйте команды `useradd` и `passwd`. В примере в качестве первоначально введенного пароля указана последовательность символов «123», затем введен надежный пароль:

```
useradd test1
passwd test1

Смена пароля для пользователя test1
Новый пароль:
Повторите ввод нового пароля:
passwd: все токены проверки подлинности успешно обновлены.
```

Добавить пользователя в группу:

```
usermod <опции> <имя_пользователя>
```

Опции:

- **-G** - дополнительные группы, в которые нужно добавить пользователя;
- **-g** - изменить основную группу для пользователя;

```
usermod -a -G <имя_группы> <имя_пользователя>
```

Для смены имени пользователя с *test1* на *test2*.

```
usermod -l test2 test1
```

Чтобы включить пользователя в группу, для основной группы используется опция *-g*:

```
sudo usermod -g test sergiy
```

Удалить пользователя из группы можно той же командой с опцией *-G*, перечислив список групп, куда пользователь должен входить (через запятую и без пробелов):

```
sudo usermod -G <группа_1>,<группа_2>,<группа_3> <пользователь>
```

После выполнения данной команды пользователь будет входить только в указанные группы, а из остальных будет удален.

Для удаления пользователей используйте **userdel**.

```
userdel test2
```

Для удаления группы выполните:

```
groupdel user
```

Автоматическая авторизация пользователя (автовход)

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция

Для активации автоматического входа пользователя (автовход) в GDM без ввода пароля при загрузке ОС, необходимо в файл **/etc/gdm/custom.conf** в секцию **[daemon]** добавить 2 строки:

```
AutomaticLogin=<имя_пользователя>
 AutomaticLoginEnable=True
```

При использовании этой конфигурации, при завершении сеанса пользователя, произойдет обратный автоматический вход в текущего пользователя.

Чтобы иметь возможность переключиться в сеанс другого пользователя, приведите в файле **/etc/gdm/custom.conf** секцию **[daemon]** к виду:

```
[daemon]
 WaylandEnable=false
 TimedLoginEnable = true
 TimedLogin = <имя_пользователя>
 TimedLoginDelay = 10
```

здесь в параметре **TimedLoginDelay** указывается время (в секундах) ожидания до автоматического входа в пользователя.

За это время можно успеть войти в рабочий стол другого пользователя.

Создание и настройка собственного default-профиля пользователя при помощи SKEL

Настройка браузера по умолчанию для всех пользователей
Примеры создания default-профиля пользователя
Настройка ярлыков рабочего стола
Создание шаблонов документов
Установка плагинов в браузеры
Настройка профиля skel
Создание профиля Wine
Настройка профиля skel с Wine

Для запуска домашнего каталога при первом создании пользователя в РЕД ОС используется каталог **/etc/skel/**. В нем можно задавать и хранить настройки новых пользователей, в частности для этого используется файл **.bashrc**. Доступ к файлу осуществляется с правами администратора.

Вы можете подробнее ознакомиться с возможностью создания эталонного пользователя, просмотрев наши обучающие видео:

- на **RuTube** — Создание универсального профиля пользователя;
- в **Яндекс.Дзен** — Создание универсального профиля пользователя;
- в **VK Видео** — Создание универсального профиля пользователя.

На наших каналах вы также сможете найти много другой полезной информации.

В файле **.bashrc** в секции «**# User specific aliases and functions**» необходимо прописать функции и настройки, которые будут применяться к каждому новому пользователю.

```
nano /etc/skel/.bashrc

# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
  . /etc/bashrc
fi

# User specific environment
if ! [[ "$PATH" =~ "$HOME/.local/bin:$HOME/bin:" ]]
then
PATH="$HOME/.local/bin:$HOME/bin:$PATH"
fi
export PATH

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions

alias cls=clear
alias diskspace='df -h'
alias data
```

После сохранения внесенных изменений можно создавать нового пользователя (создание новых пользователей осуществляется с правами суперпользователя) следующей командой:

```
useradd <имя_пользователя>
```

С помощью данной команды будет создан новый профиль пользователя, параметры для которого будут взяты из папки **/etc/skel/**.

Примечание.

Каталог **/skel** определен в файле **/etc/default/useradd**.

```
nano /etc/default/useradd

# useradd defaults file
GROUP=100
```

```
HOME=/home

INACTIVE=-1
EXPIRE=
SHELL=/bin/bash

SKEL=/etc/skel

CREATE_MAIL_SPOOL=yes
```

Местоположение **SKEL** по умолчанию можно установить любое, которое удобно. Также можно изменить и базовый домашний каталог **HOME** на любой другой.

Настройка браузера по умолчанию для всех пользователей

Добавьте в файл **/etc/skel/.bashrc** в секцию «**# User specific aliases and functions**» следующую команду (в зависимости от необходимого вам браузера):

Яндекс.Браузер:

```
if ! [ $(xdg-settings get default-web-browser | grep yandex) ]; then xdg-settings set default-web-browser yandex-browser-beta.desktop; fi
```

Opera:

```
if ! [ $(xdg-settings get default-web-browser | grep opera) ]; then xdg-settings set default-web-browser opera.desktop; fi
```

Vivaldi:

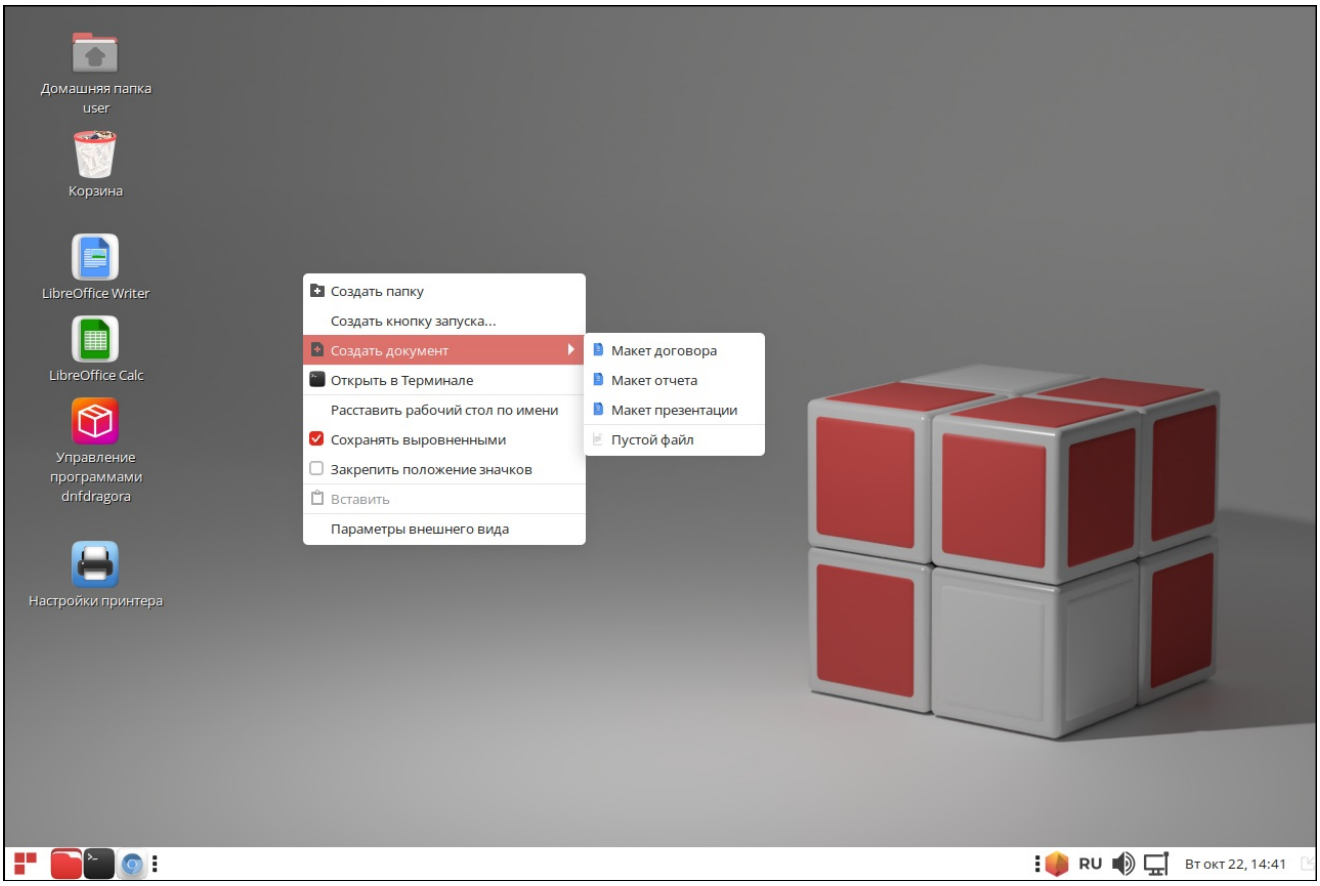
```
if ! [ $(xdg-settings get default-web-browser | grep vivaldi) ]; then xdg-settings set default-web-browser vivaldi-stable.desktop; fi
```

После сохранения внесенных изменений каждый новый созданный пользователь будет использовать указанный вами браузер, как браузер по умолчанию.

Примеры создания default-профиля пользователя

Настройка ярлыков рабочего стола

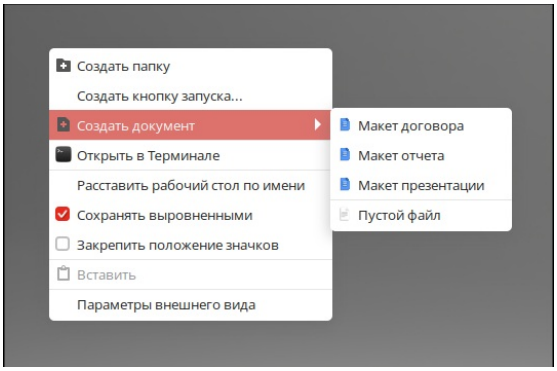
На **Рабочем столе** можно создать необходимые пользователям для работы ярлыки. Проще всего создать ярлыки через «**Главное меню**» – выбрать нужное приложение, нажать **ПКМ** – «**Переместить на Рабочий стол**».



Создание шаблонов документов

Можно создать шаблоны, например, макеты договоров, презентаций и отчетов. Для этого в офисном пакете необходимо создать и сохранить частично заполненные документы в папку **~/Шаблоны**.

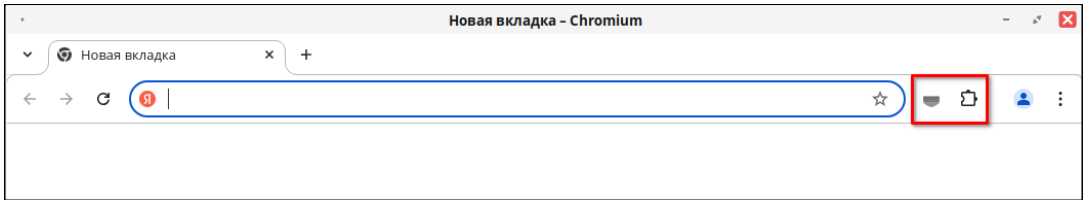
Проверьте, что созданные шаблоны доступны из контекстного меню при нажатии **ПКМ** по **Рабочему столу**.



Установка плагинов в браузеры

В качестве примера будет установлен плагин **Госуслуг**.

Установка стандартная, перейдите по ссылке и нажмите кнопку «**Установить**».



Настройка профиля skel

Необходимо создать файл, который будет служить для изменения старых путей пользователя на новые.

Примечание.

Обратите внимание на строку WHO="/home/user", вместо **/home/user** – пропишите путь до **вашего** домашнего каталога.

```
nano ~/.reconfigure_profile.sh
```

```
#!/bin/bash
WHO="/home/user"
NEW_NAME=$(whoami)
grep -rlE "$WHO" ~ > ~/.output_grep
while read line; do
sed -i "s|$WHO|/home/$NEW_NAME|g" "$line";
done < ~/.output_grep
rm -rf ~/.output_grep
```

Далее необходимо произвести синхронизацию необходимых каталогов домашнего пользователя с **/etc/skel**, для этого создайте скрипт:

```
nano ~/sync_path.sh
```

```
WHO="/home/user"
mkdir -p /etc/skel/.mozilla/ /etc/skel/.config/
cp -rfu $WHO/.{local,pki,redoswelcome}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/{Видео,Документы,Загрузки,Изображения,Музыка,Общедоступные,Рабочий\ стол,Шаблоны}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/.mozilla/{extensions,plugins}/ /etc/skel/.mozilla/ 2>/dev/null || :
cp -rfu $WHO/.config/{caja,caja-actions,chromium,dconf,mate,mate-session}/ /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.config/{monitors.xml,user-dirs.dirs} /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.{reconfigure_profile.sh,bash_logout,bash_profile,bashrc} /etc/skel/ 2>/dev/null || :
```

Запустите созданный скрипт (с правами администратора):

```
bash ./sync_path.sh
```

Отредактируйте файл **/etc/skel/.bashrc**, чтобы при первом входе нового пользователя произошел вызов вашего скрипта. В конец файла допишите:

```
if [ -f ~/.reconfigure_profile.sh ]; then
bash ~/.reconfigure_profile.sh
rm -rf ~/.reconfigure_profile.sh
fi
```

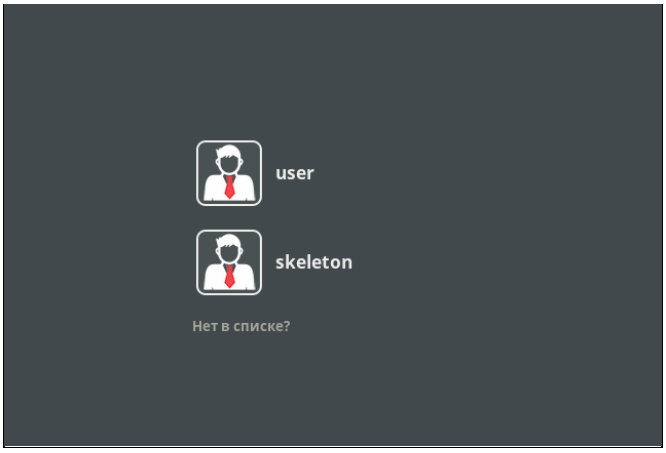
Примечание.

Чем больше будет размер **/etc/skel**, тем дольше будет происходить создание нового пользователя.

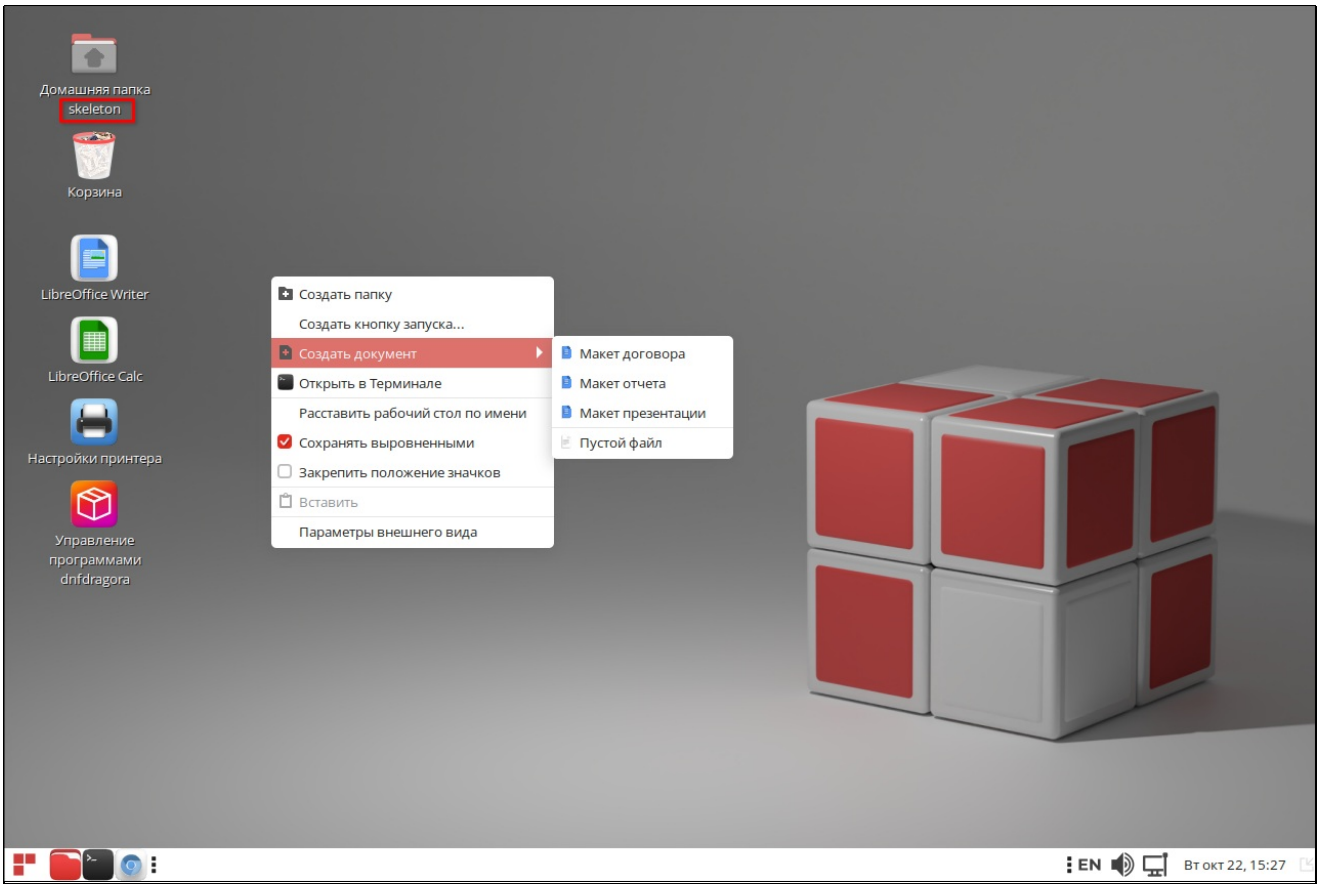
Для проверки работоспособности создайте нового пользователя:

```
useradd skeleton
passwd skeleton
```

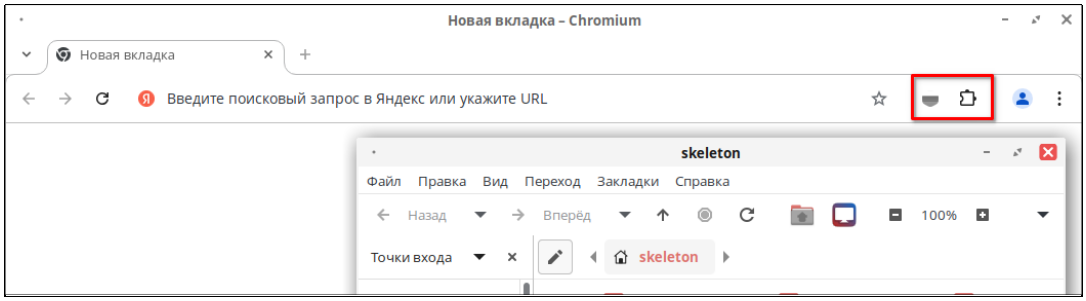
Выйдите из текущей сессии и авторизуйтесь под учетной записью нового пользователя.



Рабочий стол и **Домашняя папка** успешно созданы.



Проверьте браузер на наличие плагина Госуслуг:



Создание профиля Wine

В данном примере будет произведена базовая инициализация wine на примере notepad.

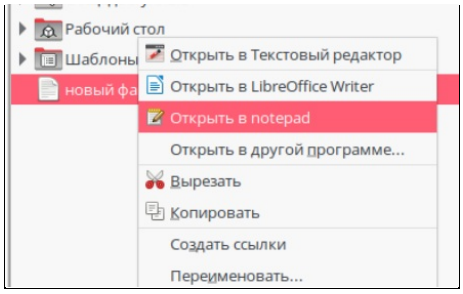
Перейдите в сеанс пользователя root:

```
su -
```

и установите wine и winetricks командой:

```
dnf install wine winetricks
```

После установки в **Главном меню** появится раздел **Wine**, который включает в себя несколько программ, в том числе **notepad**.



Настройка профиля skel с Wine

Необходимо создать файл, который будет служить для изменения старых путей пользователя на новые.

> **Примечание.**
>
> Обратите внимание на строку WHO="/home/user", вместо **/home/user** – пропишите путь до **вашего** домашнего каталога.

```
nano ~/.reconfigure_profile.sh
```

```
#!/bin/bash
WHO="/home/user"
NEW_NAME=$(whoami)
grep -rlE "$WHO" ~ > ~/.output_grep
while read line; do
sed -i "s|$WHO|/home/$NEW_NAME|g" "$line";
done < ~/.output_grep
rm -rf ~/.output_grep

NAME=$(sed -e 's|\"||g' <<< $(sed -e 's|.*\"USERNAME\"\=\"||g' <<< $(grep -rnE '"USERNAME"="' ~/.wine)))
grep -rlE '\\{2}'$NAME'\\{2}' ~/.wine | xargs sed -i 's|\\\\'$NAME'\\\\|\\\\'$NEW_NAME'\\\\|g'
grep -rlE '\\{2}'$NAME'\"' ~/.wine | xargs sed -i 's|\\\\'$NAME'\"|\\\\'$NEW_NAME'\"|g'
grep -rlE '"="'$NAME'"' ~/.wine | xargs sed -i 's|\"\=\"'$NAME'\"|\"\=\"'$NEW_NAME'\"|g'
mv ~/.wine/drive_c/users/$NAME ~/.wine/drive_c/users/$NEW_NAME
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Desktop ~/Рабочий\ стол
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Documents ~/Документы
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Downloads ~/Загрузки
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Music ~/Музыка
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Pictures ~/Изображения
ln -sf ~/.wine/drive_c/users/$NEW_NAME/Videos ~/Видео
```

Далее необходимо произвести синхронизацию необходимых каталогов домашнего пользователя с **/etc/skel**, для этого создайте скрипт:

```
nano ~/sync_path.sh
```

```
WHO="/home/user"
mkdir -p /etc/skel/.mozilla/ /etc/skel/.config/
cp -rfu $WHO/.{local,pki,redoswelcome,wine}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/{Видео,Документы,Загрузки,Изображения,Музыка,Общедоступные,Рабочий\ стол,Шаблоны}/ /etc/skel/ 2>/dev/null || :
cp -rfu $WHO/.mozilla/{extensions,plugins}/ /etc/skel/.mozilla/ 2>/dev/null || :
cp -rfu $WHO/.config/{caja,caja-actions,chromium,dconf,mate,mate-session}/ /etc/skel/.config/ 2>/dev/null || :
```

```
cp -rfu $WHO/.config/{monitors.xml,user-dirs.dirs} /etc/skel/.config/ 2>/dev/null || :
cp -rfu $WHO/.{reconfigure_profile.sh,bash_logout,bash_profile,bashrc} /etc/skel/ 2>/dev/null || :
```

Запустите созданный скрипт (с правами администратора):

```
bash ./sync_path.sh
```

Отредактируйте файл **/etc/skel/.bashrc**, чтобы при первом входе нового пользователя произошел вызов вашего скрипта. В конец файла допишите:

```
if [ -f ~/.reconfigure_profile.sh ]; then
bash ~/.reconfigure_profile.sh
rm -rf ~/.reconfigure_profile.sh
fi
```

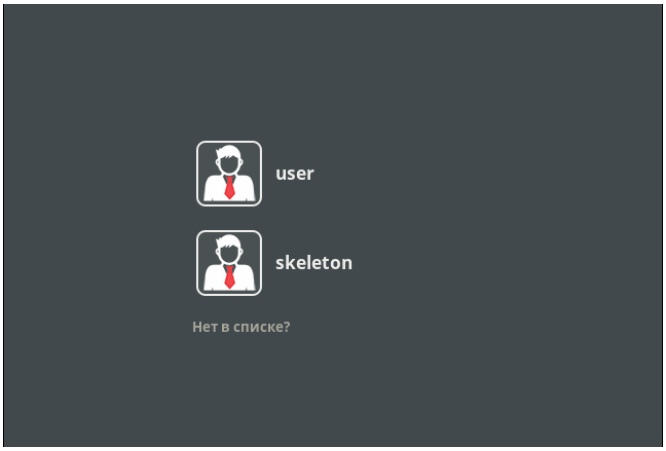
Примечание.

Чем больше будет размер **/etc/skel**, тем дольше будет происходить создание нового пользователя.

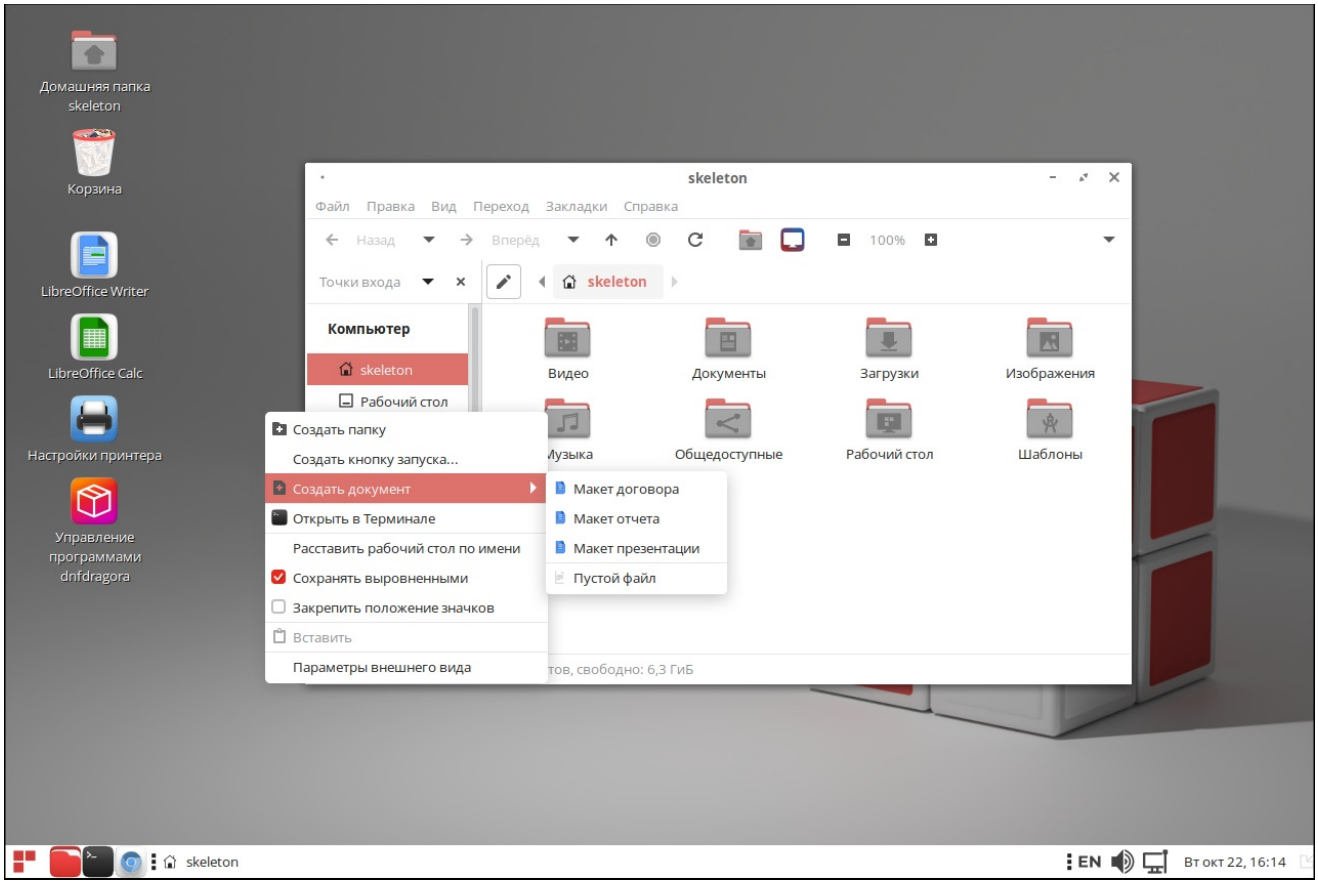
Для проверки работоспособности создайте нового пользователя:

```
useradd skeleton
passwd skeleton
```

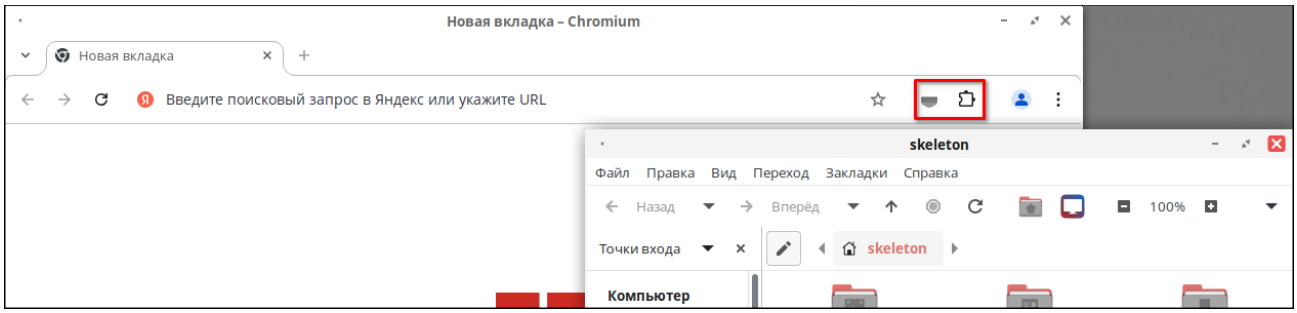
Выйдите из текущей сессии и авторизуйтесь под учетной записью нового пользователя.



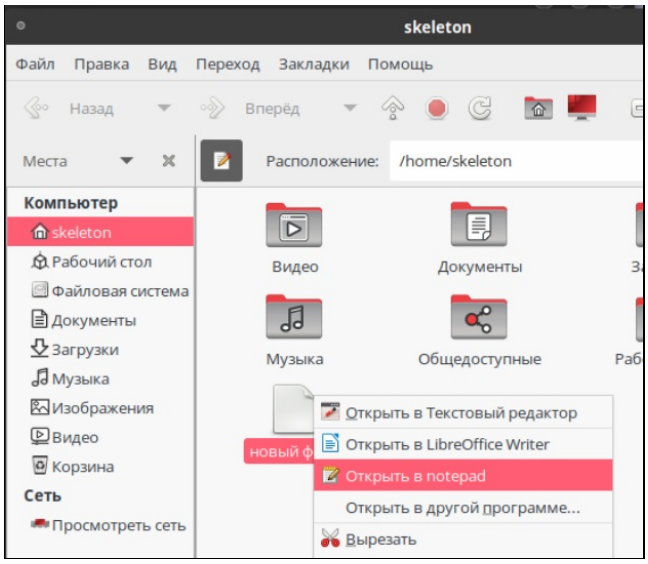
Рабочий стол и **Домашняя папка** успешно созданы.



Проверьте браузер на наличие плагина Госуслуг:



Префикс **Wine** также будет скопирован вместе с пунктом **notepad** в контекстном меню.



Управление сеансами пользователей с помощью systemd-logind

Systemd-logind — системная служба, которая управляет сеансами пользователей в операционной системе.

Файлом конфигурации службы **systemd-logind** является **logind.conf**. Для редактирования файла необходимы права **суперпользователя root**.

Откройте файл командой:

```
nano /etc/systemd/logind.conf
```

Содержимое файла выглядит следующим образом:

```
[Login]
#NAutoVTs=6
#ReserveVT=6
#KillUserProcesses=no
#KillOnlyUsers=
#KillExcludeUsers=root
#InhibitDelayMaxSec=5
#HandlePowerKey=poweroff
#HandleSuspendKey=suspend
#HandleHibernateKey=hibernate
#HandleLidSwitch=suspend
#HandleLidSwitchExternalPower=suspend
#HandleLidSwitchDocked=ignore
#PowerKeyIgnoreInhibited=no
#SuspendKeyIgnoreInhibited=no
#HibernateKeyIgnoreInhibited=no
#LidSwitchIgnoreInhibited=yes
#HoldoffTimeoutSec=30s
#IdleAction=ignore
#IdleActionSec=30min
#RuntimeDirectorySize=10%
#RuntimeDirectoryInodes=400k
RemoveIPC=no
#InhibitorsMax=8192
#SessionsMax=8192
```

Основные моменты настройки **systemd-logind**:

Параметр **NAutoVTs** отвечает за количество виртуальных терминалов, предоставляемых по умолчанию (к ним можно обращаться с использованием сочетания клавиш «*Ctrl+Alt+F[2-6]*»). В РЕД ОС предоставляется 6 виртуальных терминалов. Для изменения их количества необходимо раскомментировать данную строку и указать требуемое число терминалов. Например:

```
NAutoVTs=3
```

Параметр **ReserveVT** определяет один виртуальный терминал, который будет зарезервирован и останется доступным, даже если он не входит в диапазон параметра **NAutoVTs**.

Параметр **KillUserProcesses** отвечает за работу процессов пользователей, которые вышли из системы. Может принимать значения:

- **yes** — все процессы пользователя будут завершены при выходе из системы;
- **no** — процессы пользователя продолжат свою работу даже после завершения сеанса.

По умолчанию данный параметр установлен в значение **no**.

Параметры **KillOnlyUsers**, **KillExcludeUsers** переопределяют параметр **KillUserProcesses** и принимают в качестве значения разделенные пробелами имена пользователей.

Параметр **KillExcludeUsers** (при **KillUserProcesses=yes**) отменяет завершение процессов указанных пользователей после выхода из сеанса.

Параметр **KillOnlyUsers** завершает процессы только указанных пользователей после выхода из сеанса. Если значение параметра не задано, будет применяться параметр **KillUserProcesses**.

Параметр **InhibitDelayMaxSec** задает максимальное время задержки запроса на выключение системы или переход в спящий режим. Значение по умолчанию равно 5 секунд.

Параметры **HandlePowerKey**, **HandleSuspendKey**, **HandleHibernateKey**, **HandleLidSwitch**, **HandleLidSwitchExternalPower**, **HandleLidSwitchDocked** отображают, каким образом **logind** обрабатывает запросы включения системы, перезагрузки и перехода в спящий режим, а также выключения и приостановки работы системы. Параметры могут принимать значения *ignore*, *poweroff*, *reboot*, *halt*, *kexec*, *suspend*, *hibernate*, *hybrid-sleep*, *suspend-then-hibernate*, *lock* и *factory-reset*.

Параметры **PowerKeyIgnoreInhibited**, **SuspendKeyIgnoreInhibited**, **HibernateKeyIgnoreInhibited**, **LidSwitchIgnoreInhibited** определяют, подлежат ли блокировке действия клавиш управления питанием, перехода в спящий режим или перезагрузки. Параметры могут принимать значения *no* (действия блокируются) или *yes* (действия не блокируются).

Параметр **HoldoffTimeoutSec** задает время ожидания после запуска системы или возобновления работы системы, в течение которого система не реагирует на события. Такая задержка необходима для обнаружения системой устройств с горячий подключением. Значение по умолчанию 30 секунд.

Параметр **IdleAction** отображает действие, которое необходимо выполнять, пока система находится в режиме ожидания. Может принимать такие значения, как *ignore*, *poweroff*, *reboot*, *halt*, *kexec*, *suspend*, *hibernate*, *hybrid-sleep*, *suspend-then-hibernate* и *lock*. Значение по умолчанию *ignore*.

Параметр **IdleActionSec** задает время, по истечении которого настроенное действие в **IdleAction** будет выполняться.

Параметр **RuntimeDirectorySize** отвечает за максимальный размер временных каталогов, создаваемых для пользователей во время работы системы. Принимает размер в байтах, но можно использовать стандартные суффиксы K, M, G и T. Также значение может быть отображено в процентном соотношении. По умолчанию используется 10% физической памяти, но ее можно увеличить. Этот параметр может быть полезен для контроля использования дискового пространства и предотвращения переполнения диска.

Параметр **RemoveIPC** отвечает за удаление межпроцессного взаимодействия (IPC) при выходе пользователя из системы. Если параметр установлен в значение yes, то все IPC-объекты, созданные пользователем, будут удалены при его выходе из системы.

Параметр **InhibitorsMax** определяет максимальное количество процессов, которые могут быть заблокированы одновременно. Эти процессы могут быть заблокированы для предотвращения перезагрузки или выключения системы во время их выполнения. Если значение параметра указано 0, то блокировка процессов отключена. Если значение параметра установлено как отрицательное число, то количество заблокированных процессов не ограничено.

Параметр **SessionsMax** определяет максимальное количество одновременных сеансов пользователя. Если значение параметра установлено в 0, то количество сеансов не ограничено. Если значение параметра больше 0, то это означает максимальное количество сеансов, которые пользователь может открыть одновременно. Если пользователь пытается открыть новый сеанс, когда уже достигнуто максимальное количество сеансов, то ему будет выдано сообщение об ошибке. Этот параметр может быть полезен для ограничения количества одновременных сеансов пользователей и повышения безопасности системы.

С подробной информацией об остальных параметрах файла можно ознакомиться, выполнив команду:

```
man logind.conf
```

По окончании редактирования конфигурационного файла для применения внесенных изменений следует перезагрузить ПК или перезапустить службу **systemd-logind** командой:

```
systemctl restart systemd-logind
```

Ограничение ресурсов пользователя

Для ограничения ресурсов, доступных пользователю, используется конфигурационный файл **/etc/security/limits.conf**. Для включения лимитов необходимо добавить библиотеку **PAM pam_limits.so** в соответствующем модуле. Например:

```
session required pam_limits.so
```

в файле **/etc/pam.d/login**.

Для изменения лимитов редактируем файл **/etc/security/limits.conf**. Формат файла:

```
<группа/пользователь>  <лимит>(жёсткий/мягкий)  <параметр>  <значение>
```

Описание параметров:

- *core* - размер core-файлов (KB);
- *data* - максимальный размер данных (KB);
- *fsize* - максимальный размер файла (KB);
- *memlock* - максимальное заблокированное адресное пространство (KB);
- *nofile* - максимальное количество открытых файлов;
- *rss* - максимальный размер памяти для резидент-программ (KB);
- *stack* - максимальный размер стека (KB);
- *cpu* - максимальное процессорное время (MIN);
- *nproc* - максимальное количество процессов;
- *as* - ограничение адресного пространства (KB);
- *maxlogins* - максимальное число одновременных регистраций в системе;
- *maxsyslogins* - максимальное количество учётных записей;
- *priority* - приоритет запущенных процессов;
- *locks* - максимальное количество блокируемых файлов пользователем;
- *sigpending* - максимальное количество сигналов, которые можно передать процессу;
- *msgqueue* - максимальный размер памяти для очереди POSIX-сообщений (bytes);
- *nice* - максимальный приоритет, который можно выставить: [-20, 19];
- *rtprio* - максимальный приоритет времени выполнения;
- *chroot* - изменить корневой каталог (Debian-specific).

Вместо можно использовать групповой символ «*» (для всех) и групповой символ «**%**» для wildcast'а групп.

Ограничение полномочий пользователей по использованию виртуальных терминалов

Ограничение полномочий пользователей по использованию виртуальных терминалов можно настроить следующим образом:

Перейдите в сеанс пользователя **root**:

```
su -
```

и добавьте строку в файл **/etc/security/limits.conf**:

```
petrov hard maxlogins 2
```

Добавить строку можно следующей командой:

```
echo "petrov hard maxlogins 2" >> /etc/security/limits.conf
```

где `petrov` - имя пользователя, которому необходимо ограничить число запускаемых виртуальных терминалов.

Затем для ограничения количества запускаемых виртуальных терминалов **для группы пользователей** добавьте в файл **/etc/security/limits.conf** следующую строку:

```
@users hard maxlogins 2
```

где **@users**- это название группы пользователей (для обозначения группы перед её названием используется символ '**@**').

После добавления правила, ограничивающего число сеансов для пользователя *petrov* равным 2, при попытке открыть 3 сеанс в виртуальном терминале возникает ошибка вида:

```
Слишком много регистраций в системе для «petrov».
Доступ запрещен
```

Для ограничения количества допустимых **tty** (в том числе и отключение их) для всех пользователей, следует изменить содержимое файла **/etc/systemd/logind.conf**:

```
nano  /etc/systemd/logind.conf
```

раскомментировать строку и указать число 1:

```
NAutoVTs=1
```

после перезагрузки доступ к остальным **tty** будет закрыт, вы увидите только черный экран.

Управление дисковыми квотами

Система **diskquota** обеспечивает механизм для управления используемым дисковым пространством. Ограничения могут быть установлены для каждого пользователя в отдельности, для любой или для всех файловых систем. Система ограничений (**quota**) будет предупреждать пользователей, когда они превысят свой дозволенный лимит, но будет позволять использовать некоторое дополнительное пространство для текущей работы. Система ограничений (**quota system**) является частью ядра LINUX.

Вы можете подробнее ознакомиться с управлением дисковыми квотами, просмотрев наши обучающие видео:

- на **RuTube** — Управление дисковыми квотами;
- в **Яндекс.Дзен** — Управление дисковыми квотами;
- в **VK Видео** — Управление дисковыми квотами.

На наших каналах вы также сможете найти много другой полезной информации.

Команда **quota** позволяет просмотреть любые ограничения дискового пространства для каждого пользователя.

Доступны два типа ограничений, которые могут быть наложены на пользователя, обычно, если используется одно из ограничений, то и второе тоже будет использоваться. Ограничение может быть установлено как **на все дисковое пространство пользователя**, которое используется этим пользователем, так и **на число файлов** (**inodes**), которыми он может владеть.

Quota обеспечивает информацию на ограничения, которые были установлены системным администратором на каждую из областей, которые используются в данный момент. Ограничения по **inodes** и **block** накладываются как на **uid** (идентификатор пользователя), так и на **gid** (идентификатор группы). Если вы входите в группу, которая превысила наложенное на нее ограничение, то вы не сможете использовать дисковое пространство, даже если вы все еще можете использовать его как пользователь.

Существуют четыре числа для каждого ограничения:

- используемое в данное время ограничение;
- "мягкое" ограничение (softlimit);
- "жесткое" ограничение (hardlimit);
- промежуток времени, после истечения которого "мягкое" ограничение интерпретируется как "жесткое".

"Мягкое" ограничение определяет максимальное количество блоков размером 1Кбайт, которое пользователь может немного превысить. "Жесткое" ограничение не может быть превышено ни при каких обстоятельствах. Если пользователь пытается превысить это ограничение, то он получает сообщение о невозможности сделать это. При этом ядро возвращает код ошибки **EDQUOT**. После того как пользователь превысит доступное для него "мягкое" ограничение (softlimit) устанавливается время, после истечения которого "мягкое" ограничение становится "жестким" (hardlimit). Обычно срок этого периода истекает после 7 дней (1 неделя). В этот период времени пользователь может удалить ненужные ему файлы, после чего он вновь может использовать "мягкое" ограничение до момента истечения указанного промежутка времени. После истечения указанного промежутка времени "мягкое" ограничение становится "жестким" и у пользователя больше нет ресурсов для создания новых файлов.

Для того чтобы установить систему ограничений дискового пространства (quota) в ОС, системному администратору необходимо сделать несколько шагов:

- выбрать файловую систему, на которую будут накладываться ограничения;
- разрешить (включить) систему ограничений;
- произвести проверку файловой системы на ограничения дискового пространства;
- произвести проверку ограничений дискового пространства как для пользователей, так и для групп;
- запретить ограничения для пользователей и групп.

В первую очередь необходимо решить, на какую файловую систему необходимо наложить ограничения (quotas). Чаще всего ограничения накладываются на файловую систему, в которой располагаются домашние каталоги пользователей, или на файловую систем, которая смонтирована в каталог **/usr**, и пользователи имеют право записывать на нее информацию. Для того чтобы разрешить ограничения на дисковое пространство на необходимой файловой системе, отредактируйте файл **/etc/fstab**, добавив к указанной системе опции для ограничения дискового пространства (как для пользователей, так и для групп). Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
nano /etc/fstab
```

Предварительно рекомендуется создать резервную копию:

```
cp /etc/fstab /etc/fstab_backup
```

Отредактированный файл **/etc/fstab** может иметь вид:

```
#
```

```
# /etc/fstab
#
/dev/hda1       /           ext2    defaults       1 1
/dev/hda2       none          swap    sw       0 0
/dev/hda3       /usr          ext2    defaults       1 1
/dev/hdb1       /usr/users      ext2    defaults,usrquota,grpquota       0 0 /dev/hdb2           /usr/src       ext2    defaults,usrquota       0
0
```

Зарезервированное слово "**usrquota**" в поле опций включает ограничение дискового пространства (quotas) для пользователей (userquota) на данном устройстве. Зарезервированное слово "**grpquota**" включает ограничение дискового пространства для групп (groupquota) на данном устройстве. Во то время, когда вы используете опции "usrquota" и "grpquota" без '=', ваши файлы ограничений (quotafile) будут находиться в корневом каталоге каждой файловой системы, в которой используются ограничения на дисковое пространство. Файл, называемый "**aquota.user**", будет использоваться для ограничений пользователей, а файл "**aquota.group**" будет использоваться для ограничений групп. Однако вы сами можете определить ваши файлы ограничений. Например, строка "**usrquota=/usr/adm/quotasrc.user**" установит файл ограничений для пользователей в каталоге **/usr/adm**, который будет называться "**quotarc.user**". Однако будьте внимательны и отслеживайте длину строки в файле **/etc/fstab** (смотрите ее определение в файле **mntent.h**).

Периодически (в основном после некорректной перезагрузки системы и во время первого разрешения ограничений на дисковое пространство) записи, содержащиеся в файле ограничений, должны быть проверены на целостность действительного числа блоков и файлов, выделенных для пользователя. Для выполнения этой операции может быть использована команда **quotacheck**.

Данную команду необязательно выполнять для неподмонтированных файловых систем или на файловых системах, на которых отключено ограничение на дисковое пространство (quotas). Для проверки файловой системы на число блоков, используемых пользователем, а так же для установки и изменения всех файлов ограничений (quotafiles), выполните команду:

```
quotacheck -favugm
```

Вы можете вставить данную команду в один из rc-скриптов и запускать ее на файловой системе так же, как и **fsck**, только тогда, когда не установлен флаг **fastreboot**. Данная программа не поддерживает одновременную параллельную проверку нескольких файловых систем. Для того чтобы включить систему ограничений на дисковое пространство на вашем компьютере, добавьте строку **/usr/bin/quotaon -avug** в один из ваших **/etc/rc-файлов**. Данная команда будет включать поддержку ограничений дискового пространства во время загрузки вашей системы.

Только суперпользователь может использовать команду quota для проверки используемых ограничений любого пользователя и команду repquota для проверки используемого пространства и ограничений для всех пользователей на данной файловой системе.

Для того чтобы получить информацию об ограничениях, наложенных на всех пользователей, необходимо выполнить команду:

```
repquota -ua
```

после чего на экране можно будет видеть таблицу, в которой указаны ограничения, наложенные на каждого пользователя.

Содержимое экрана после выполнения выше приведенной команды может иметь вид:

```
                Block limits            File limits
User            used    soft    hard  grace    used  soft  hard  grace
root      --  487082       0       0        12147     0     0
daemon    --     399       0       0            2     0     0
news      --     626       0       0           46     0     0
```

Для получения информации о группах необходимо выполнить команду:

```
repquota -ga
```

Для редактирования ограничения дискового пространства необходимо использовать программу **edquota**. Для редактирования ограничений дискового пространства для конкретного пользователя необходимо использовать программу **edquota** с опцией **-u**, а для группы необходимо использовать ту же программу, но с опцией **-g**. Редактировать необходимо только число , которое следует за словом *hard* или *soft*. Например, после выполнения команды:

```
edquota -u <user>
```

содержимое экрана может иметь вид:

```
Quotas for user <user>:
/dev/hdb3: blocks in use: 345, limits (soft = 1, hard = 0)
        inodes in use: 94, limits (soft = 0, hard = 0)
```

После чего вы можете изменить значения, указанные после слов hard и soft. При редактировании используется редактор, который

указывается в переменной окружения **EDITOR**.

Для каждой файловой системы, имеющей ограничение на дисковое пространство, вы видите две строки. Слово **soft** означает, что на данную файловую систему наложено "мягкое" ограничение (softlimit), при этом пользователь или группа имеют некоторый интервал времени (grace period), в течении которого они могут превысить указанное значение. Данный интервал времени можно изменить с помощью команды **edquota -t**.

Например, после выполнения команды:

```
edquota -t
```

содержимое экрана может иметь вид:

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem             Block grace period     Inode grace period
  /dev/sda4                     7days                  7days
```

После чего вы можете изменить значения, указанные по умолчанию. Если пользователь или группа не удалят лишних файлов в течении указанного периода времени, то данные файлы переходят в разряд "жестких" ограничений. Слово **hard** означает, что на данную файловую систему наложено "жесткое" ограничение. "Жесткое" ограничение является максимальным значением, которое может иметь пользователь или группа на данной файловой системе. Пользователь/группа не может иметь больше файлов или inodes, чем указано в **hard**.

Строка:

```
/dev/hdb3: blocks in use: 345, limits (soft = 1, hard = 0)
```

сообщает, какое число блоков может быть выделено для данного пользователя или группы.

Строка:

```
inodes in use: 94, limits (soft = 0, hard = 0)
```

сообщает, какое число **inode** (файлов, устройств, поименованных каналов и т.д.) может быть выделено для данного пользователя или группы.

В большинстве случаев вам приходится иметь группу пользователей, которые должны иметь одинаковые ограничения на дисковое пространство на указанной файловой системе. Самый быстрый путь - отредактировать ограничения на дисковое пространство для этих пользователей и создать прототип одного из пользователей или группы для всех других. С помощью команды:

```
edquota -u <имя_пользователя/группы_который_станет_прототипом>
```

отредактировать ограничения на дисковое пространство, после чего с помощью команды:

```
edquota -p <имя_прототипа> *
```

отредактировать ограничения для всех оставшихся пользователей.

Например, для того чтобы в качестве ограничений дискового пространства (quota) для пользователя <ola> использовались ограничения, наложенные на пользователя <user>, вам необходимо выполнить команду:

```
edquota -p <user> <ola>
```

Для проверки ограничений дискового пространства для пользователя и группы используется программа quota.

Синтаксис этой программы:

```
quota [-guqv]
quota [-qv] -u username
quota [-qv] -g groupname
```

Используйте опцию **-v** для вывода информации о:

- файловых системах, которые не имеют включенными ограничения на дисковое пространство (quota);
- файловых системах, на которых вы уже установили систему ограничения дискового пространства, но на которых еще не занят ни один блок.

Используйте опцию **-q** для просмотра файловых систем, на которых превышено значение "мягкого" (softlimit) и "жесткого" (hardlimit)

ограничения.

Опция **-g** дает вам возможность просмотреть все ограничения, которые наложены на группы, членом которых вы являетесь.

Например, с помощью команды:

```
quota -u <user>
```

вы можете получить информацию об ограничениях дискового пространства, которые наложены на пользователя user. Содержимое экрана после выполнения данной команды может иметь вид:

```
Disk quotas for user <user> (uid 1002):
 Filesystem  blocks   quota   limit   grace   files   quota   limit  grace
 /dev/hdb3     345*      1       0    none      94       0       0
```

Если вы захотели запретить ограничения, наложенные на какого-то пользователя или на группу, то вам необходимо воспользоваться программой **edquota** для редактирования значений **hard** и **soft**. Установите эти значения в 0. После чего для данного пользователя или группы не будет существовать ограничений на дисковое пространство, и он/она сможет создавать неограниченное количество файлов (ограниченное только дисковым пространством).

Настройка прав доступа к файлам и каталогам

Поскольку Linux — система многопользовательская, вопрос об организации разграничения доступа к файлам и каталогам является одним из существенных вопросов, которые должна решать операционная система.

В основе механизмов разграничения доступа лежат имена пользователей и имена групп пользователей. В Linux каждый пользователь имеет уникальное имя, под которым он входит в систему (логируется). Кроме того, в системе создается некоторое число групп пользователей, причем каждый пользователь может быть включен в одну или несколько групп. Создает и удаляет группы суперпользователь, он же может изменять состав участников той или иной группы. Члены разных групп могут иметь разные права по доступу к файлам, например, группа администраторов может иметь больше прав, чем группа программистов.

Вы можете подробнее ознакомиться с назначением прав доступа к файлам и каталогам, просмотрев наши обучающие видео:

- на **RuTube**:
  - Атрибуты файлов и каталогов в РЕД ОС;
  - Расширенные права доступа.
- в **Яндекс.Дзен**:
  - Атрибуты файлов и каталогов в РЕД ОС;
  - Расширенные права доступа.
- в **VK Видео**:
  - Атрибуты файлов и каталогов в РЕД ОС;
  - Расширенные права доступа.

На наших каналах вы также сможете найти много другой полезной информации.

В индексном дескрипторе каждого файла записаны имя так называемого владельца файла и группы, которая имеет права на этот файл. Первоначально при создании файла его владельцем объявляется тот пользователь, который этот файл создал. Точнее, тот пользователь, от чьего имени запущен процесс, создающий файл. Группа тоже назначается при создании файла по идентификатору группы процесса, создающего файл. Владельца и группу файла можно поменять в ходе дальнейшей работы с помощью команд **chown** и **chgrp**.

Выполним команду **ls -l**. Но зададим ей в качестве дополнительного параметра имя конкретного файла, например, файла, задающего саму команду **ls**.

```
$ ls -l /bin/ls
-rwxr-xr-x 1 root root 49940 Sep 12 1999 /bin/ls
```

В данном случае владельцем файла является пользователь *root* и группа *root*. Но нас сейчас в выводе этой команды больше интересует первое поле, определяющее тип файла и права доступа к файлу. Это поле в приведенном примере представлено цепочкой символов **-rwxr-xr-x**. Эти символы можно условно разделить на 4 группы.

Первая группа, состоящая из единственного символа, определяет тип файла. Этот символ в соответствии с возможными типами файлов может принимать такие значения:

- **-** — обычный файл;
- **d** — каталог;
- **b** — файл блочного устройства;
- **c** — файл символьного устройства;
- **s** — доменное гнездо (socket);
- **p** — именованный канал (pipe);
- **l** — символическая ссылка (link).

Далее следуют **три группы** по три символа, которые и определяют права доступа к файлу соответственно:

- для владельца файла;
- для группы пользователей, которая сопоставлена данному файлу;
- для всех остальных пользователей системы.

В нашем примере права доступа для владельца определены как **rwx**, что означает, что владелец (root) имеет право читать файл (**r**), производить запись в этот файл (**w**), и запускать файл на выполнение (**x**). Замена любого из этих символов прочерком будет означать, что пользователь лишается соответствующего права. В том же примере мы видим, что все остальные пользователи (включая и тех, которые вошли в группу root) лишены права записи в этот файл, т. е. не могут файл редактировать и вообще как-то изменять.

Права доступа и информация о типе файла в UNIX-системах хранятся в индексных дескрипторах в отдельной структуре, состоящей из двух байтов, т. е. из 16 бит. Четыре бита из этих 16-ти отведены для кодированной записи о типе файла. Следующие три бита задают особые свойства исполняемых файлов. И, наконец, оставшиеся 9 бит определяют права доступа к файлу. Эти 9 бит разделяются на 3 группы по три бита. Первые три бита задают права пользователя, следующие три бита — права группы, последние 3 бита определяют права всех остальных пользователей (т. е. всех пользователей, за исключением владельца файла и группы файла).

При этом, если соответствующий бит имеет значение 1, то право предоставляется, а если он равен 0, то право не предоставляется. В символьной форме записи прав единица заменяется соответствующим символом (r, w или x), а 0 представляется прочерком.

Право на чтение (**r**) файла означает, что пользователь может просматривать содержимое файла с помощью различных команд просмотра, например, командой more или с помощью любого текстового редактора. Но, подредактировав содержимое файла в текстовом редакторе, вы не сможете сохранить изменения в файле на диске, если не имеете права на запись (**w**) в этот файл. Право на выполнение (**x**) означает, что вы можете загрузить файл в память и попытаться запустить его на выполнение как исполняемую программу. Конечно, если в действительности файл не является программой (или скриптом shell), то запустить этот файл на выполнение не удастся, но, с другой стороны, даже если файл действительно является программой, но право на выполнение для него не установлено, то он тоже не запустится.

Если выполнить ту же команду **ls -l**, но в качестве последнего аргумента ей указать не имя файла, а имя каталога, мы увидим, что для каталогов тоже определены права доступа, причем они задаются теми же самыми символами rwx. Например, выполнив команду **ls –l /**, мы увидим, что каталогу bin соответствует строка:

```
drwxr-xr-x 2 root root 2048 Jun 21 21:11 bin
```

Естественно, что по отношению к каталогам трактовка понятий «право на чтение», «право на запись» и «право на выполнение» несколько изменяется. Право на чтение по отношению к каталогам легко понять, если вспомнить, что каталог — это просто файл, содержащий список файлов в данном каталоге. Следовательно, если вы имеете право на чтение каталога, то вы можете просматривать его содержимое (этот самый список файлов в каталоге). Право на запись тоже понятно — имея такое право, вы сможете создавать и удалять файлы в этом каталоге, т. е. просто добавлять в каталог или удалять из него запись, содержащую имя какого-то файла и соответствующие ссылки. Право на выполнение в данном случае означает право переходить в этот каталог. Если вы, как владелец, хотите дать доступ другим пользователям на просмотр какого-то файла в своем каталоге, вы должны дать им право доступа в каталог, т. е. дать им «право на выполнение каталога». Более того, надо дать пользователю право на выполнение для всех каталогов, стоящих в дереве выше данного каталога. Поэтому в принципе для всех каталогов по умолчанию устанавливается право на выполнение как для владельца и группы, так и для всех остальных пользователей. И, уж если вы хотите закрыть доступ в каталог, то лишите всех пользователей (включая группу) права входить в этот каталог.

После прочтения предыдущего абзаца может показаться, что право на чтение каталога не дает ничего нового по сравнению с правом на выполнение. Однако разница в этих правах все же есть. Если задать только право на выполнение, вы сможете войти в каталог, но не увидите там ни одного файла (этот эффект особенно наглядно проявляется в том случае, если вы пользуетесь каким-то файловым менеджером, например, программой Midnight Commander). Если вы имеете право доступа в каком-то из подкаталогов этого каталога, то вы можете перейти в него (командой **cd**), но, как говорится «вслепую», по памяти, потому что списка файлов и подкаталогов текущего каталога вы не увидите.

Алгоритм проверки прав пользователя при обращении к файлу можно описать следующим образом. Система вначале проверяет, совпадает ли имя пользователя с именем владельца файла. Если эти имена совпадают (т. е. владелец обращается к своему файлу), то проверяется, имеет ли владелец соответствующее право доступа: на чтение, на запись или на выполнение (не удивляйтесь, суперпользователь может лишить некоторых прав и владельца файла). Если право такое есть, то соответствующая операция разрешается. Если же нужного права владелец не имеет, то проверка прав, предоставляемых через группу или через группу атрибутов доступа для остальных пользователей, уже даже не проверяются, а пользователю выдается сообщение о невозможности выполнения затребованного действия (обычно что-то вроде «Permission denied»).

Если имя пользователя, обращающегося к файлу, не совпадает с именем владельца, то система проверяет, принадлежит ли владелец к группе, которая сопоставлена данному файлу (далее будем просто называть ее группой файла). Если принадлежит, то для определения возможности доступа к файлу используются атрибуты, относящиеся к группе, а на атрибуты для владельца и всех остальных пользователей внимания не обращается. Если же пользователь не является владельцем файла и не входит в группу файла, то его права определяются атрибутами для остальных пользователей. Таким образом, третья группа атрибутов, определяющих права доступа к файлу, относится ко всем пользователям, кроме владельца файла и пользователей, входящих в группу файла.

Для изменения прав доступа к файлу используется команда **chmod**. Ее можно использовать в двух вариантах. В первом варианте вы должны явно указать, кому какое право даете или кого этого права лишаете:

```
chmod wXp <имя_файла>
```

где вместо символа **w** подставляется:

- либо символ **u** (т. е. пользователь, который является владельцем);
- либо **g** (группа);
- либо **o** (все пользователи, не входящие в группу, которой принадлежит данный файл);
- либо **a** (все пользователи системы, т. е. и владелец, и группа, и все остальные).

Вместо **X** ставится:

- либо **+** (предоставляем право);
- либо **–** (лишаем соответствующего права);

- либо **=** (установить указанные права вместо имеющихся).

Вместо **p** — символ, обозначающий соответствующее право:

- **r** (чтение);
- **w** (запись);
- **x** (выполнение).

Вот несколько примеров использования команды chmod:

```
chmod a+x <имя_файла>
```

предоставляет всем пользователям системы право на выполнение данного файла.

```
chmod go-rw <имя_файла>
```

удаляет право на чтение и запись для всех, кроме владельца файла.

```
chmod ugo+rwx <имя_файла>
```

дает всем права на чтение, запись и выполнение.

Если опустить указание на то, кому предоставляется данное право, то подразумевается, что речь идет вообще обо всех пользователях, т. е. команду:

```
chmod a+x <имя_файла>
```

можно записать таким способом:

```
chmod +x <имя_файла>
```

Второй вариант задания команды **chmod** (он используется чаще) основан на цифровом представлении прав. Для этого мы кодируем символ *r* цифрой 4, символ *w* — цифрой 2, а символ *x* — цифрой 1. Для того, чтобы предоставить пользователям какой-то набор прав, надо сложить соответствующие цифры. Получив, таким образом, нужные цифровые значения для владельца файла, для группы файла и для всех остальных пользователей, задаем эти три цифры в качестве аргумента команды **chmod** (ставим эти цифры после имени команды перед вторым аргументом, который задает имя файла). Например, если надо дать все права владельцу (4+2+1=7), право на чтение и запись — группе (4+2=6), и не давать никаких прав остальным, то следует дать такую команду:

```
chmod 760 <имя_файла>
```

Если вы знакомы с двоичным кодированием восьмеричных цифр, то вы поймете, что цифры после имени команды в этой форме ее представления есть не что иное, как восьмеричная запись тех самых 9 бит, которые задают права для владельца файла, группы файла и для всех пользователей.

Выполнять смену прав доступа к файлу с помощью команды **chmod** может только сам владелец файла или суперпользователь. Для того, чтобы иметь возможность изменить права группы, владелец должен дополнительно быть членом той группы, которой он хочет дать права на данный файл.

Надо рассказать еще о трех возможных атрибутах файла, устанавливаемых с помощью той же команды **chmod**. Это те самые атрибуты для исполняемых файлов, которые в индексном дескрипторе файла в двухбайтовой структуре, определяющей права на файл, занимают позиции 5-7, сразу после кода типа файла.

Первый из этих атрибутов — так называемый "бит смены идентификатора пользователя". Смысл этого бита состоит в следующем.

Обычно, когда пользователь запускает некоторую программу на выполнение, эта программа получает те же права доступа к файлам и каталогам, которые имеет пользователь, запустивший программу. Если же установлен "бит смены идентификатора пользователя", то программа получит права доступа к файлам и каталогам, которые имеет владелец файла программы (таким образом, рассматриваемый атрибут лучше называть "битом смены идентификатора владельца"). Это позволяет решать некоторые задачи, которые иначе было бы трудно выполнить. Самый характерный пример — команда смены пароля **passwd**. Все пароли пользователей хранятся в файле **/etc/passwd**, владельцем которого является суперпользователь **root**. Поэтому программы, запущенные обычными пользователями, в том числе команда **passwd**, не могут производить запись в этот файл. А, значит, пользователь как бы не может менять свой собственный пароль. Но для файла **/usr/bin/passwd** установлен "бит смены идентификатора владельца", каковым является пользователь root. Следовательно, программа смены пароля **passwd** запускается с правами **root** и получает право записи в файл **/etc/passwd** (уже средствами самой программы обеспечивается то, что пользователь может изменить только одну строку в этом файле).

Установить "бит смены идентификатора владельца" может суперпользователь с помощью команды

```
chmod +s <имя_файла>
```

Аналогичным образом работает "бит смены идентификатора группы".

Еще один возможный атрибут исполняемого файла — это "бит сохранения задачи" или "*sticky bit*" (дословно — "бит прилипчивости"). Этот бит указывает системе, что после завершения программы надо сохранить ее в оперативной памяти. Удобно включить этот бит для задач, которые часто вызываются на выполнение, так как в этом случае экономится время на загрузку программы при каждом новом запуске. Этот атрибут был необходим на старых моделях компьютеров. На современных быстродействующих системах он используется редко.

Если используется цифровой вариант задания атрибутов в команде **chmod**, то цифровое значение этих атрибутов должно предшествовать цифрам, задающим права пользователя:

```
chmod 4775 <имя_файла>
```

При этом веса этих битов для получения нужного суммарного результата задаются следующим образом:

4 — "бит смены идентификатора пользователя",

2 — "бит смены идентификатора группы",

1 — "бит сохранения задачи (sticky bit)".

Если какие-то из этих трех битов установлены в 1, то несколько изменяется вывод команды **ls -l** в части отображения установленных атрибутов прав доступа. Если установлен в 1 "бит смены идентификатора пользователя", то символ "x" в группе, определяющей права владельца файла, заменяется символом "s". Причем, если владелец имеет право на выполнение файла, то символ "x" заменяется на маленькое "s", а если владелец не имеет права на выполнение файла (например, файл вообще не исполняемый), то вместо "x" ставится "S". Аналогичные замены имеют место при задании "бита смены идентификатора группы", но заменяется символ "x" в группе атрибутов, задающих права группы. Если равен 1 "бит сохранения задачи (sticky bit)", то заменяется символ "x" в группе атрибутов, определяющей права для всех остальных пользователей, причем "x" заменяется символом "t", если все пользователи могут запускать файл на выполнение, и символом "T", если они такого права не имеют.

Таким образом, хотя в выводе команды **ls -l** не предусмотрено отдельных позиций для отображения значений битов смены идентификаторов и бита сохранения задачи, соответствующая информация выводится. Вот небольшой пример того, как это будет выглядеть:

```
ls -l prim1
-rwSrwsrwT 1 kos root 12 Dec 18 23:17 prim1
```

umask (от англ. user file creation mode mask — маска режима создания пользовательских файлов) — функция среды POSIX, изменяющая права доступа, которые присваиваются новым файлам и директориям по умолчанию. Права доступа файлов, созданных при конкретном значении **umask**, вычисляются при помощи следующих побитовых операций (umask обычно устанавливается в восьмеричной системе счисления): побитовое «**И**» между унарным дополнением аргумента (используя побитовое «**НЕ**») и режимом полного доступа.

Фактически, **umask** указывает, какие биты следует сбросить в выставляемых правах на файл — каждый установленный бит **umask** запрещает выставление соответствующего бита прав. Исключением из этого запрета является бит исполняемости, который для обычных файлов зависит от создающей программы (трансляторы ставят бит исполняемости на создаваемые файлы, другие программы — нет), а для каталогов следует общему правилу. **umask 0** означает, что следует (можно) выставить все биты прав (rwxrwxrwx), **umask 777** запрещает выставление любых прав.

Допустим, что значение **umask** равняется **174**, тогда каждый новый файл будет иметь права доступа 602, а каждая новая директория 603.

Режим Киоска в РЕД ОС

Включение режима киоска
Выключение режима киоска

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: redos-kiosk-utils-0.16-1

Режим киоска представляет собой рабочую среду для пользователя или группы пользователей с четко ограниченным функционалом – пользователи имеют доступ только к тем приложениям, которые явно указаны для их профиля.

Режим киоска в РЕД ОС реализуется с помощью доработанной командной оболочки *Bash* и окружения рабочего стола *MATE*.

Базовый функционал киоска реализован в нескольких пакетах и находится в выключенном состоянии. Режим киоска с утилитами для его настройки становится доступным после установки пакета **redos-kiosk-utils**.

Вы можете подробнее ознакомиться с организацией режима киоска в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Режим Киоска в РЕД ОС;
- в **Яндекс.Дзен** — Режим Киоска в РЕД ОС;
- в **VK Видео** — Режим Киоска в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки пакета **redos-kiosk-utils** выполните команду (потребуются права **администратора**):

```
sudo dnf install redos-kiosk-utils
```

В текущей версии для настройки режима киоска имеются только консольные утилиты, которые должны выполняться **с правами суперпользователя root**.

При включенном режиме киоска пользователю становятся недоступны:

- запуск программ с графическим интерфейсом, кроме явно разрешённых (ярлыки таких приложений находятся на *Рабочем столе*);
- выполнение сценариев на любом языке при явном их запуске пользователем;
- запуск на выполнение файлов с установленным битом *SUID*;
- изменение свойств и содержимого главной панели на *Рабочем столе*;
- изменение содержимого *Рабочего стола* (создание/удаление/изменение ярлыков, создание/удаление/изменение иных файлов);
- автоматическое монтирование внешних накопителей;
- смена виртуальной консоли по сочетанию клавиш **Ctrl+Alt+F*n***.

Также имеются следующие ограничения в режиме киоска:

- главная панель *Рабочего стола* в режиме киоска не имеет кнопки главного меню (типа «Пуск») и пиктограмм быстрого запуска приложений. Кнопки выхода из сессии, блокировки экрана и выключения/перезагрузки ПК вынесены на главную панель слева;
- Центр управления *MATE* недоступен, но, даже в случае его ручного запуска, приложение блокируется;
- блокирован запуск *Терминала MATE*;
- из консольных утилит блокированы **dconf** и **gsettings** с целью исключения изменений настроек как *MATE*, так и графической системы;
- просмотр справочной системы недоступен как при вызове по клавише **F1**, так и по нажатию кнопки «**Помощь**», также блокируется в ряде апплетов показ диалогового окна «**О программе**»;
- дополнительное усечение прав и возможностей пользователя путём запуска приложений в «песочнице» (**Firejail**).

Включение режима киоска

Для *включения режима киоска* конкретному пользователю применяется команда **kiosk-mode-on** с указанием имени этого пользователя (опция `-u` или `--username`) и перечнем приложений (опция `-a` или `--appname`), которые разрешаются к запуску пользователем в данном режиме. Также доступны следующие опции:

- `-t`, `--timelock` – указание времени (в минутах) бездействия в сессии перед включением хранителя экрана и блокировки экрана; по умолчанию, а также при указании значения 0 минут блокировка экрана отключается;
- `-b`, `--blockbtn` – отображение кнопки блокирования экрана на главной панели (по умолчанию кнопка не отображается);
- `-i`, `--autohide` – включение автоматического скрытия главной панели *Рабочего стола* (по умолчанию она постоянно отображается);
- `-f`, `--firejail` – при необходимости запуска разрешённых приложений в «песочнице» для более значимых ограничений (проект использует пакет **Firejail**). Если требуется задать какую-либо опцию для **firejail** (согласно его официальной документации), то данные ключи можно привести в двойных кавычках либо сразу после опции, либо после знака равенства;
- `-q` или `--quiet` – подавление вывода на экран (например, для использования в сценариях оболочки). Подавляется вывод не только информационных сообщений, но и сообщений об ошибках.

Например:

- для пользователя **sidorov** разрешить запуск текстового редактора **LibreOffice Writer** и почтового клиента **Mozilla Thunderbird** с блокировкой экрана после **5 минут** бездействия:

```
kiosk-mode-on -u sidorov -a libreoffice-writer,thunderbird -t 5
```

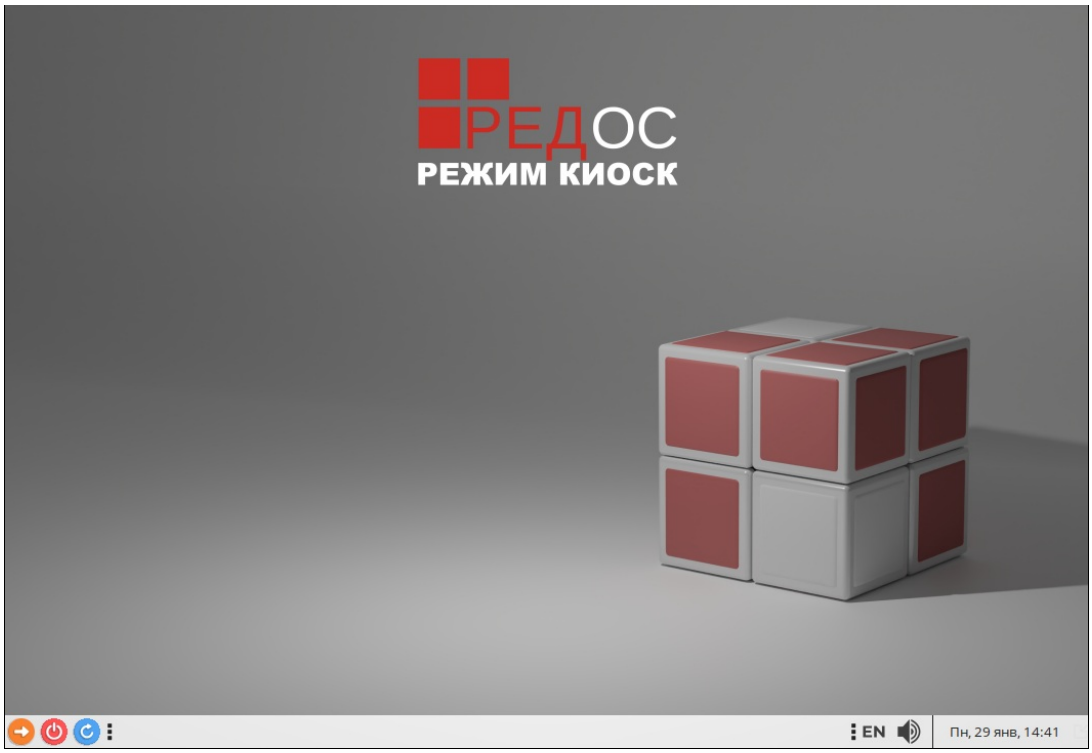
- для пользователя **ivanov** разрешить запуск только интернет-браузера **Firefox** с подключением по сетевому интерфейсу **enp1s3**:

```
kiosk-mode-on -u ivanov -a firefox --firejail="--net=enp1s3"

  или
kiosk-mode-on -u ivanov -a firefox -f"--net=enp1s3"
```

Обе команды равнозначны.

Приложения указываются путём перечисления имён *desktop*-файлов, имеющихся в каталоге **/usr/share/applications** без указания суффикса «**.desktop**». Иные приложения не допускаются к разрешению в режиме киоска.

По умолчанию на главной панели *Рабочего стола* имеются кнопки выключения, перезагрузки системы и завершения сеанса/смены пользователя, причём для перезагрузки или выключения системы потребуется ввести пароль администратора (**root**).



Выключение режима киоска

Для *выключения режима киоска* и возврата настроек пользователя к обычному состоянию используется команда **kiosk-mode-off** с указанием имени этого пользователя (`-u` или `--username`). Например:

```
kiosk-mode-off -u sidorov
```

Особенности служб синхронизации времени

Chrony и ntpsec
Chrony и systemd-timesyncd
Сравнительная таблица

Chrony и ntpsec

Преимущества **chrony**:

- **chrony** может эффективно работать в среде, где доступ к временной привязке прерывистый, в то время как **ntpsec** нуждается в регулярном опросе сервера для стабильной работы;
- **chrony** синхронизирует часы быстрее и с большей точностью;
- **chrony** быстро адаптируется к внезапным изменениям частоты тактовых импульсов (например, из-за изменения температуры кварцевого осциллятора). **ntpsec** может потребоваться много времени, чтобы снова синхронизироваться;
- **chrony** может работать при перегруженной сети, даже если она перегружена длительное время;
- **chrony** никогда не изменяет время в конфигурации по умолчанию, чтобы не нарушать работу других запущенных программ. В **ntpsec** можно произвести настройку так, чтобы он никогда не изменял время, но в таком случае должны использоваться другие средства настройки часов, что может отрицательно сказаться на точности времени;
- **chrony** использует меньше памяти и задействует процессор только при необходимости, что лучше экономит энергию.

Уникальные особенности **chrony**:

- поддержка механизма аутентификации *Network Time Security* (**NTS**);
- поддержка аппаратно-временной метки в системе для обеспечения стабильной и точной синхронизации в локальной сети;
- просмотр исправленных ошибок в обновлениях для определения скорости, с которой компьютер выигрывает или теряет время, и использования этой оценки для последующего сжатия времени компьютера;
- поддержка определения коэффициента усиления или потери времени, когда компьютер выключен. chrony может использовать эти данные при загрузке системы для установки системного времени на основе исправленной версии часов реального времени.

Уникальные особенности **ntpsec**:

- поддержка большинства режимов работы **RFC 5905**, включая широковещательный, многоадресный и сервер/клиент. Однако некоторые режимы, такие как 5 (Broadcast) и 6 (Broadcast client), больше не реализованы в **ntpsec**, так как их невозможно обеспечить безопасностью;
- поддержка протокола NTS (Network Time Security);
- **ntpsec** импортирован на различные операционные системы;
- поддержка большого количества драйверов для различных аппаратных эталонных часов. Например, в нём есть драйвер SHM (Shared Memory Driver), который может работать на системах без часов реального времени (RTC, Real Time Clock).

Chrony и systemd-timesyncd

systemd-timesyncd — служба для синхронизации локальных системных часов с удаленным сервером по протоколу сетевого времени (**NTP**). В отличие от реализации **chrony** **systemd-timesyncd** реализует только клиентскую часть, сосредоточившись на запросе времени с одного удаленного сервера и синхронизации локальных часов с ним.

В systemd-timesyncd также имеются цели, имитирующие общие уровни запуска **SystemVinit**, поэтому можно переключаться между целями, используя команду:

```
telinit <уровень_выполнения>
```

Преимущества **chrony**:

- использование NTP-сервером другого доступного хоста для синхронизации времени;
- получение информации о синхронизации NTP из нескольких источников;
- получение информации о синхронизации с локальных часов.

Chrony — реализует клиентский и серверный режимы полного протокола NTPv4.

Systemd-timesyncd - реализует только клиентский режим протокола **SNTP**, сложные варианты использования не охватываются **systemd-timesyncd**.

Например, SNTP не может сделать его более точным, извлекая время из нескольких источников, как это делает **ntpsec** по умолчанию. В результате **systemd-timesyncd** не может обеспечить точную синхронизацию времени, как **chrony**.

Сравнительная таблица служб синхронизации времени

	chrony	**ntpsec**	**systemd-timesyncd**
Базовая характеристика			
Лицензия	GPLv2	MIT + BSD	CC-BY-SA-3.0
Размер рабочего демона	287 KB	889 KB	192 KB
Источники времени			
NTP	+	+	+
Эталонные часы	+	+	+
Ручной ввод	+	+	+
Отслеживание источника			
Фиксированная фильтрация сэмпла	+	+	+
Адаптивная фильтрация сэмпла	+	-	-
Взвешивание выборки	+	-	-
Отслеживание частоты	+	-	-
Восстановить состояние из файла	+	-	-
Часовая дисциплина			
Независимая регулировка фазы и частоты	+	-	-
Разрешенный случайный интервал обновления	+	-	+
Максимальная скорость нарастания	100000 (настраивается)	500	500
Температурная компенсация	+	-	-
NTP-режимы			
Сервер	+	+	-
Клиент	+	+	+
Сервер трансляции	+	+	-
Клиент трансляции	-	+	+
Чередующийся сервер	+	-	-
Чередующийся клиент	+	-	-
Аутентификация по протоколу NTP			
Симметричный ключ	+	+	-
Автоключ (небезопасный)	-	-	-
Безопасность сетевого времени	+	+	-
MS-SNTP через Samba	+	+	+
Хэш-функции MAC	MD5, SHA-1, SHA-2	MD5, SHA-1, SHA-2	-
Шифры CMAC	AES-128, AES-256	AES-256, AES-384, AES-512	-

Установка и настройка ntpsec

Установка
Настройка
Просмотр статуса

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ntpsec-1.2.1-10

NTPsec — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Службой **NTPsec** является **ntpd.service**, она вычисляет отклонения системных часов и регулярно их корректирует.

Преимущества **ntpd**:

- поддержка всех режимов работы RFC 5905, включая широковещательный и многоадресный сервер/клиент;
- поддержка большого количества драйверов для различных аппаратных эталонных часов.

Недостатки **ntpd**:

- необходимость регулярного опроса источника для стабильной работы;
- необходимость некоторого количества времени для синхронизации.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **ntpsec** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ntpsec
```

Настройка

Для добавления/удаления серверов необходимо отредактировать конфигурационный файл **/etc/ntp.conf**.

```
nano /etc/ntp.conf
```

По умолчанию указаны следующие серверы:

```
server ntp1.vniiftri.ru
 server ntp2.vniiftri.ru
 server ntp3.vniiftri.ru
 server ntp4.vniiftri.ru

 driftfile VARNTP/drift
 restrict default nomodify noquery
 restrict 127.0.0.1
```

```
restrict ::1

disable monitor
logfile /var/log/ntp.log
```

Параметры:

server	Список серверов для синхронизации времени.
driftfile	Задает адрес файла, в котором хранится история изменений времени во время синхронизации. Если по каким-то причинам синхронизация времени с внешними источниками станет невозможна, служба времени изменит системные часы в соответствии с записями в этом файле.
restrict 127.0.0.1	Указывает, что пользоваться нашим сервером времени можно только непосредственно с локального интерфейса. Если вам необходимо разрешить другим компьютерам в вашей локальной сети синхронизировать время с текущей машины, то укажите в данном параметре адрес вашей сети, например: **restrict 192.168.10.0 mask 255.255.255.0**
restrict default nomodify notrap nopeer noquery	Параметры указывают на то, что клиентам данного сервиса времени запрещено изменять его настройки, получать его статус. Они могут только забрать с него значения точного времени.
disable monitor	Данный параметр повышает безопасность, предотвращая использования одной из уязвимостей сервиса ntpd, которую можно использовать для проведения DDoS атак.
logfile	Указывает путь к файлу с логами сервиса.

Если необходимо добавить собственные адреса серверов, следует заменить строки ntp[1-4].vniiftri.ru.

Для применения изменений необходимо запустить службу:

```
systemctl start ntpd
```

Проверяем запустился ли сервер:

```
netstat -tulnp | grep 123
```

Все в порядке, служба слушает положенный **порт 123**. Проверим на всякий случай системные логи используемой ОС:

```
cat /var/log/messages | grep ntpd
cat /var/log/ntp.log
```

Теперь настроим автозапуск службы **ntp** вместе с загрузкой используемой ОС:

```
systemctl enable ntpd
```

Просмотр статуса

Для просмотра дополнительной информации используется ntpq, например:

```
 ntpq -p

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+ntp1.vniiftri.ru    .MRS.          1 u   30  128  153  24.6955   0.7295  19.4495
 ntp2.vniiftri.ru    .MRS.          1 u  159  128    2  24.9635   1.4861   2.1827
 ntp3.vniiftri.ru    .MRS.          1 u   90  128  115  20.0448   3.6854  26.5434
*ntp4.vniiftri.ru    .MRS.          1 u  404  128   10  19.8532   3.6181   8.3031
```

Данные вывода:

remote	Адрес удаленного эталона времени, с которого была синхронизация.
refid	Указывает, откуда каждый эталон получает точное время. Это могут быть другие сервера времени, система GPS и другое.
st	Уровень (Stratum) это число от 1 до 16, которое указывает на точность эталона. 1- максимальная точность, 16 — сервер недоступен. Уровень вашего сервера будет равен уровню наименее точного удаленного эталона плюс 1.
poll	Интервал в секундах между опросами.
reach	Восьмеричное представление массива из 8 бит, отражающего результаты последних восьми попыток соединения с эталоном. Бит выставлен, если удаленный сервер ответил.

delay	Время задержки ответа на запрос о точном времени.
offset	Разница между вашим и удаленным сервером
jitter	Дисперсия (Jitter) — это мера статистических отклонений от значения смещения (поле offset) по нескольким успешным парам запрос-ответ. Чем меньше значение дисперсии, тем лучше, поскольку позволяет точнее синхронизировать время.

Утилита синхронизации времени ntpdate

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Программа **ntpdate** — позволяет разово синхронизировать локальное время с эталонным сервером времени в интернете. Подобных эталонов существует достаточно много. Для примера можно воспользоваться одним из них — **pool.ntp.org**.

Запускаем синхронизацию времени:

```
ntpdate pool.ntp.org
```

Утилита провела синхронизацию, в результате которой к системному времени было добавлено число секунд, необходимое для приближения к эталонному. Если в результате работы синхронизации возникает ошибка: «**no server suitable for synchronization found**», то попробуйте в работе утилиты использовать непривилегированный порт. По-умолчанию ntpdate работает по 123 порту. Если он закрыт на **firewall**, то помочь в синхронизации поможет следующий параметр:

```
ntpdate -u pool.ntp.org
```

Если у вас запуск ntpdate завершается ошибкой — «**the NTP socket is in use, exiting**», значит у вас уже установлена и запущена служба ntpd, которая заняла необходимый udp-порт, необходимый для работы ntpdate.

Установка и настройка chrony

Установка и запуск
Настройка
Управление Chronyd

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** chrony-4.1-5

Chrony – альтернативный клиент и сервер протокола сетевого времени **NTP**. **Chrony** может быстрее синхронизировать системные часы с лучшей точностью времени, и он может быть особенно полезен для систем, которые не работают в сети все время.

Основные преимущества:

- эффективная работа в среде, где доступ к временной связке прерывистый;
- адаптация к внезапным изменениям частоты тактовых импульсов;
- работа в перегруженной сети, даже если перегрузка продолжается длительное время;
- время в конфигурации по умолчанию никогда не изменяется, чтобы не нарушать работу других запущенных программ;
- использование меньшего объема памяти и запуск процессов только при необходимости в целях экономии энергии.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Установка и запуск

Действия по установке и настройке требуется производить под пользователем **root** или пользователем с правами администратора.

Chrony доступен по умолчанию в репозитории РЕД ОС.

Для установки **Chrony** необходимо выполнить следующую команду:

```
dnf install chrony
```

После установки необходимо добавить сервис chronyd.service в автозагрузку и запустить его командой:

```
systemctl enable --now chronyd.service
```

Настройка

Клиенты **NTP** должны знать, с какими серверами **NTP** они должны связаться, чтобы получить текущее время. Серверы **NTP** могут быть указаны в директиве **server** в файле конфигурации **NTP**.

Отредактируйте конфигурационный файл **/etc/chrony.conf** для добавления/удаления серверов.

Данные по умолчанию:

```
# Use public servers from the pool. ntp. org project.
 # Please consider joining the pool (http: //www. pool. ntp. org/join.html).
 server ntp1.vniiftri.ru iburst
 server ntp2.vniiftri.ru iburst
 server ntp3.vniiftri.ru iburst
 server ntp4.vniiftri.ru iburst
```

Параметр **iburst** используется для ускорения начальной синхронизации.

Управление Chronyd

Для **chrony** есть утилита командной строки с именем **chronyc** для управления и мониторинга сервиса **chrony (chronyd)**.

Для проверки синхронизации **chrony**, можно использовать команду tracking, как показано ниже:

```
chronyc tracking
```

Вывод должен выглядеть следующим образом:

```
Reference ID    : 596DFB17 (ntp3.vniiftri.ru)
Stratum         : 2
Ref time (UTC)  : Wed May 24 08:18:40 2023
System time     : 0.000260688 seconds fast of NTP time
Last offset     : +0.000226291 seconds
RMS offset      : 0.001286364 seconds
Frequency       : 8.707 ppm slow
Residual freq   : +0.024 ppm
Skew            : 3.054 ppm
Root delay      : 0.016705679 seconds
Root dispersion : 0.000947660 seconds
Update interval : 64.9 seconds
Leap status     : Normal
```

Перечисленные пункты содержат следующую информацию:

- **Reference ID** — идентификатор и имя сервера, с которым компьютер в настоящее время синхронизирован;
- **Stratum** — количество переходов к серверу с установленными эталонными часами;
- **Ref time** — время по Гринвичу, в которое было выполнено последнее измерение из эталонного источника;
- **System time** — задержка системных часов от синхронизированного сервера;
- **Last offset** — расчетное смещение последнего обновления часов;
- **RMS offset** — долгосрочное среднее арифметическое значения смещения;
- **Frequency** — частота, на которой часы системы будут работать неправильно, если хронограф не проведет коррекцию. Она выражена в ppm — ч/м (частей на миллион);
- **Residual freq** — остаточная частота указывает на разницу между измерениями от опорного источника и используемой в настоящее время частотой;
- **Skew** — расчетная погрешность, связанная с погрешностью частоты;
- **Root delay** — суммарная задержка сетевого пути к опорному серверу, с которым синхронизируется компьютер;
- **Leap status** — статус скачка (изменения) времени, который может иметь одно из следующих значений:
- *«Normal»* – означает нормальную корректировку времени;
- *«Insert second»* – означает, что произведена корректировка времени добавлением дополнительной секунды в последнюю минуту текущего месяца;
- *«Delete second»* – означает, что произведена корректировка времени удалением дополнительной секунды из последней минуты текущего месяца;
- *«Not synchronised»* – означает, что компьютер в данный момент времени не синхронизирован.

Также есть возможность проверить текущие источники времени, которые использует **chrony**:

```
chronyc sources
```

Вывод должен выглядеть следующим образом:

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^+ ntp1.vniiftri.ru              1   6   272   271   -264us[ +347us] +/- 7394us
^+ ntp2.vniiftri.ru              1   6   377    77  +2910us[+3321us] +/- 9806us
^* ntp3.vniiftri.ru              1   6   377    13   +848us[+1296us] +/- 6958us
^+ ntp4.vniiftri.ru              1   6   377    11   +895us[ +895us] +/- 6879us
```

Утилита **Chronyc** может находить статистику каждого источника, например, скорость дрейфа и процесс оценки смещения, используя команду **sourcestats**:

```
chronyc sourcestats
```

Вывод должен выглядеть следующим образом:

```
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
==============================================================================
ntp1.vniiftri.ru            7   5   517     -1.228      4.945  -1149us   242us
ntp2.vniiftri.ru            7   5   388     +4.855     22.098  +1466us  1091us
ntp3.vniiftri.ru           11   9   646     +1.307      6.637  -5544ns  1036us
ntp4.vniiftri.ru           11   7   647     +1.544      3.566   +599us   501us
```

Чтобы сообщить **Chrony**, что вы больше не подключены к глобальной сети Интернет, выполните следующие действия:

```
chronyc offline
```

Для проверки статуса источников **NTP**, необходимо запустить следующую команду:

```
chronyc activity
```

Вывод должен выглядеть следующим образом:

```
200 OK
4 sources online
0 sources offline
0 sources doing burst (return to online)
0 sources doing burst (return to offline)
0 sources with unknown address
```

Когда система будет вновь подключена к Интернету, необходимо сообщить об этом **chrony**, используя команду:

```
chronyc online
```

Для более подробного объяснения всех параметров следует руководствоваться *Справочными страницами*.

```
man chronyc
man chronyd
```

Настройка systemd-timesyncd

systemd-timesyncd – это системная служба, которую можно использовать для синхронизации локальных системных часов с удаленным сервером по протоколу сетевого времени (**NTPsec**). В отличие от служб **chronyd** или **ntpd**, которые могут предоставлять время для клиентов, служба **systemd-timesyncd** реализует только клиентскую часть **SNTP**. Этот сервис способен регулировать системные часы для больших смещений по времени или медленно настраивает их для меньших дельт.

Преимущества:

- реализация только клиентского режима протокола SNMP;
- поддержка большого количества сервисов, многие из которых не являются обязательными, поэтому их можно отключить.

Недостатки:

- сложные варианты использования не охватываются systemd-timesyncd;
- невозможность обеспечения точной синхронизации времени.

Вы можете подробнее ознакомиться с настройкой синхронизации времени, просмотрев наши обучающие видео:

- на **RuTube** — Настройка синхронизации времени;
- в **Яндекс.Дзен** — Настройка синхронизации времени;
- в **VK Видео** — Настройка синхронизации времени.

На наших каналах вы также сможете найти много другой полезной информации.

Чтобы перейти к настройке службы **systemd-timesyncd** предварительно необходимо проверить статус служб **ntpd** и **chronyd**. Если они запущены (имеют статус `active(running)`), исключите их из автозапуска с помощью команд:

```
systemctl disable ntpd --now
systemctl disable chronyd --now
```

Такие действия необходимы для корректной синхронизации через **systemd-timesyncd**.

Настройка

Настройка **systemd-timesyncd** производится через файл конфигурации **/etc/systemd/timesyncd.conf**.

Чтобы указать список серверов времени для синхронизации, добавьте в файл **/etc/systemd/timesyncd.conf** в раздел **[Time]** параметр «`NTP`»:

```
NTP=ntp0.vniiftri.ru ntp1.vniiftri.ru ntp2.vniiftri.ru ntp3.vniiftri.ru
```

Параметр «`FallbackNTP`» определит список резервных серверов времени:

```
FallbackNTP=ntp1.niiftri.irkutsk.ru
```

В итоге файл конфигурации должен выглядеть примерно следующим образом:

```
[Time]
NTP=ntp0.vniiftri.ru ntp1.vniiftri.ru ntp2.vniiftri.ru ntp3.vniiftri.ru
FallbackNTP=ntp1.niiftri.irkutsk.ru
```

Для применения изменений необходимо перезапустить службу:

```
systemctl restart systemd-timesyncd
```

Для проверки текущего статуса синхронизации времени выполните команду:

```
timedatectl status

               Local time: Чт 2024-10-10 16:21:46 MSK
         Universal time: Чт 2024-10-10 13:21:46 UTC
               RTC time: Чт 2024-10-10 13:21:46
              Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
```

```
RTC in local TZ: no
```

Детальную информацию о состоянии синхронизации времени можно посмотреть командой:

```
timedatectl timesync-status

       Server: 89.109.251.23 (ntp3.vniiftri.ru)
Poll interval: 2min 8s (min: 32s; max 34min 8s)
         Leap: normal
      Version: 4
      Stratum: 1
    Reference: MRS
    Precision: 4us (-18)
Root distance: 183us (max: 5s)
       Offset: +1.923ms
        Delay: 39.369ms
       Jitter: 2.683ms
 Packet count: 1
    Frequency: +7,516ppm
```

Утилита настройки системной локали localectl

Синтаксис
Основные команды
Опции утилиты
Примеры работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: localectl v246.10-17

Locale (локаль) – это региональные настройки операционной системы.

Каждая операционная система поставляется с конкретными региональными настройками. Эти настройки влияют на язык:

- интерфейса;
- сообщений об ошибках;
- справочной информации;
- вывода консольных утилит.

Также локаль влияет на формат чисел, даты и времени, денежной валюты и пр.

Для получения и изменения региональных настроек в РЕД ОС используется утилита командной строки **localectl**. Она позволяет просматривать и настраивать текущую локаль и список доступных раскладок клавиатуры, а также устанавливать новые значения.

Localectl может быть полезна для пользователей, которые работают в многоязычных средах или на компьютерах с разными макетами клавиатуры.

Синтаксис

Синтаксис утилиты имеет вид:

```
localectl [<опции>...] <команда>
```

Основные команды

Команды утилиты:

- **status** – показать текущие настройки локали;
- **set-locale <локаль>** – установить системную локаль;
- **list-locales** – вывести список доступных локалей;
- **set-keymap <раскладка_клавиатуры>** – установить раскладку клавиатуры для консоли;
- **list-keymaps** – вывести доступные раскладки клавиатуры виртуальной консоли;
- **set-x11-keymap <раскладка_клавиатуры>** – установить раскладку для X11;
- **list-x11-keymap-models** – вывести список доступных моделей раскладок для X11;
- **list-x11-keymap-layouts** – вывести список доступных раскладок для X11;
- **list-x11-keymap-variants [<раскладка_клавиатуры>]** – вывести список доступных вариантов раскладок для X11;
- **list-x11-keymap-options** – вывести список доступных опций для раскладок X11.

Опции утилиты

Основные опции утилиты:

- `-h`, `--help` – вывести справочную информацию;

- `--version` – вывести версию утилиты;
- `--no-ask-password` – не запрашивать пароль администратора при выполнении операций, которым необходимы дополнительные привилегии;
- `-H`, `--host=[<имя_пользователя>@]<имя_хоста>[:<порт>]` – выполнить команду на удаленном хосте;
- `-M`, `--machine=<контейнер>` – выполнить операцию в локальном контейнере;
- `--no-convert` – не преобразовывать раскладку клавиатуры из консоли в X11 и наоборот.

Примеры работы

Примеры работы утилиты:

- просмотр текущих настроек локали:

```
localectl

System Locale: LANG=ru_RU.UTF-8
VC Keymap: ru
X11 Layout: ru,us
X11 Variant: ,
X11 Options: grp:alt_shift_toggle
```

- просмотр списка доступных локалей:

```
localectl list-locales

C.UTF-8
aa_DJ.UTF-8
aa_ER.UTF-8
aa_ER.UTF-8@saaho
aa_ET.UTF-8
af_ZA.UTF-8
agr_PE.UTF-8
ak_GH.UTF-8
am_ET.UTF-8
an_ES.UTF-8
anp_IN.UTF-8
ar_AE.UTF-8
…
```

- просмотр списка доступных раскладок клавиатуры:

```
localectl list-keymaps

ANSI-dvorak
al
al-plisi
amiga-de
amiga-us
apple-a1048-sv
apple-a1243-sv
apple-a1243-sv-fn-reverse
apple-internal-0x0253-sv
apple-internal-0x0253-sv-fn-reverse
applkey
…
```

Для добавления поддержки русского языка выполните команду:

```
localectl set-locale LANG=ru_RU.UTF-8
```

Для добавления раскладки клавиатуры выполните следующую команду:

```
localectl set-keymap --no-convert ctrl_shift
```

Пример установки английской и русской раскладки, которые будут переключаться сочетанием клавиш *Ctrl+Shift*:

```
localectl --no-convert set-x11-keymap us,ru "" "" grp:ctrl_shift_toggle
```

Для применения настроек выполните:

```
systemctl restart display-manager
```

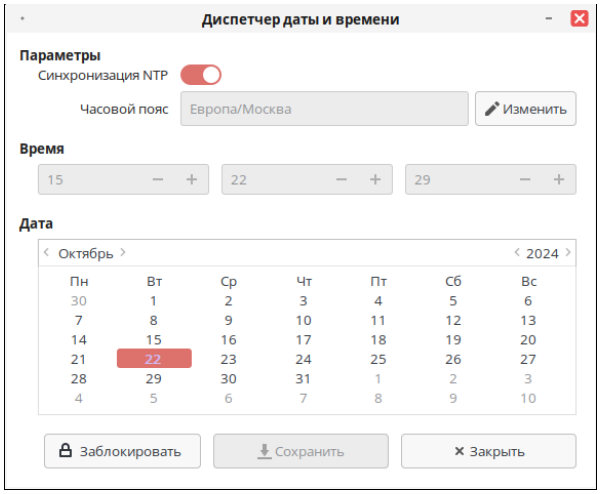
Localectl также может быть использован с другими утилитами командной строки, такими как **systemctl** и **timedatectl**, для управления системными настройками.

Диспетчер настройки даты и времени

Диспетчер настройки даты и времени в MATE
Диспетчер настройки даты и времени в GNOME
Диспетчер настройки даты и времени в KDE

Диспетчер настройки даты и времени в MATE

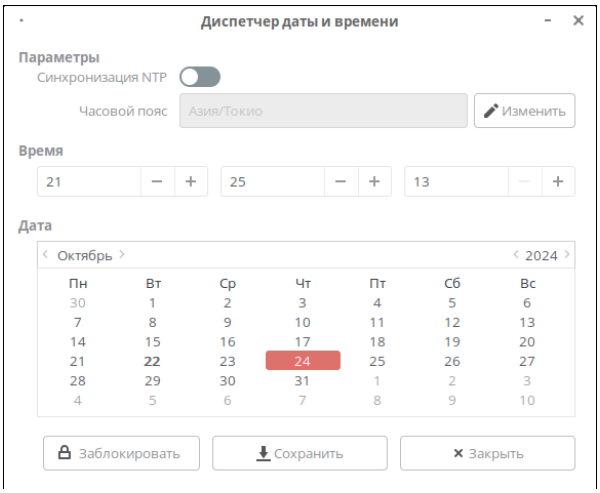
Для настройки даты и времени в РЕД ОС с графическим окружением **MATE** по умолчанию доступна графическая утилита «**Диспетчер даты и времени**», которая располагается в «**Главном меню**» - «**Администрирование**» - «**Дата и время**».



По умолчанию включена синхронизация по NTP, поэтому настройка даты и времени вручную отключена, доступна только смена часового пояса.

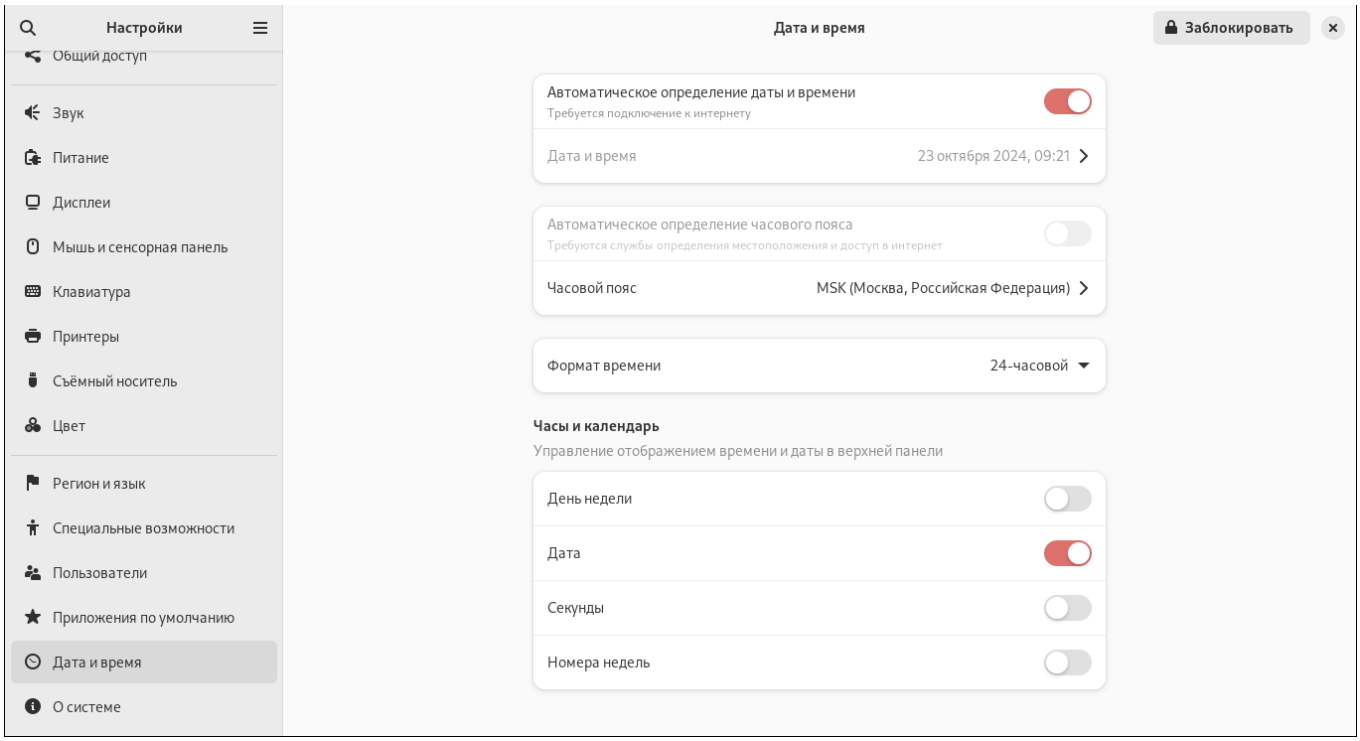


Для изменения настроек отключите синхронизацию по NTP, выберите часовой пояс, установите время и дату, для применения изменений нажмите кнопку «**Сохранить**».

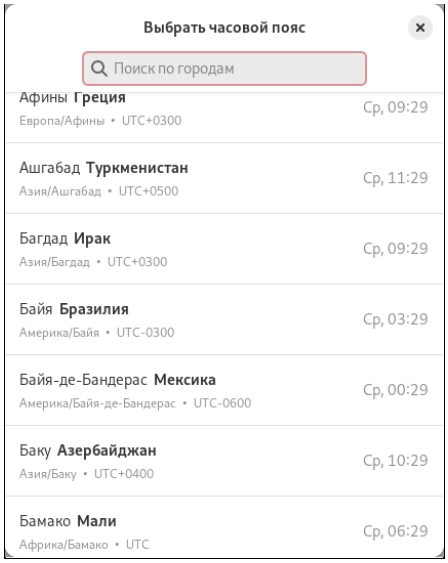


Диспетчер настройки даты и времени в GNOME

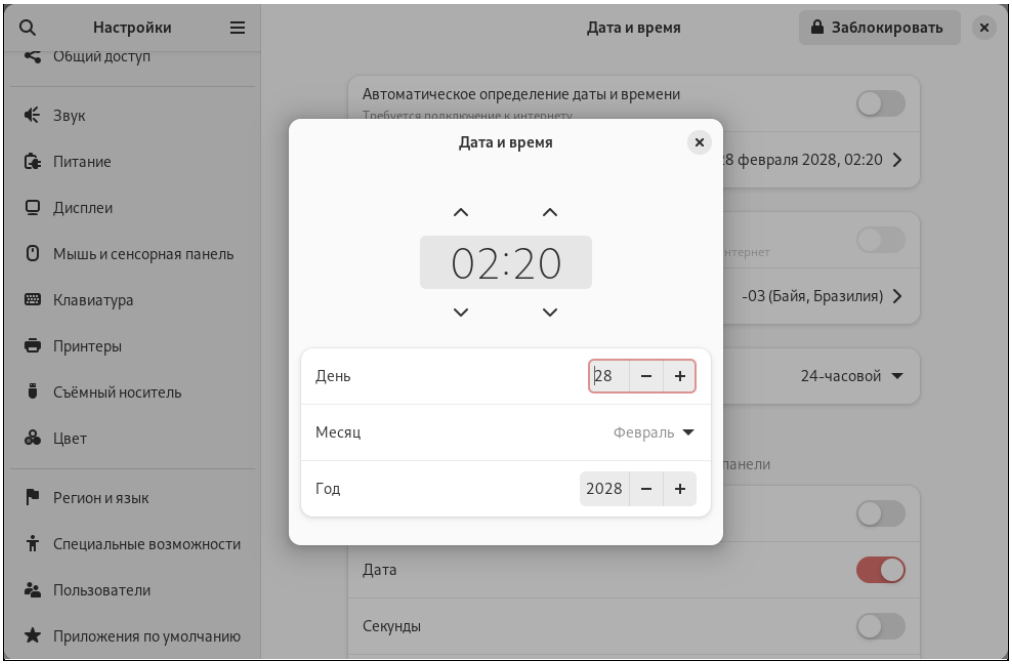
Изменение даты и времени в РЕД ОС с графическим окружением **GNOME** по умолчанию производится в разделе «**Дата и время**» системных настроек («**Показать приложения**» — «**Настройки**»).



По умолчанию включено **автоматическое определение даты и времени** (синхронизация по NTP), поэтому настройка даты и времени вручную отключена, доступна только смена часового пояса.



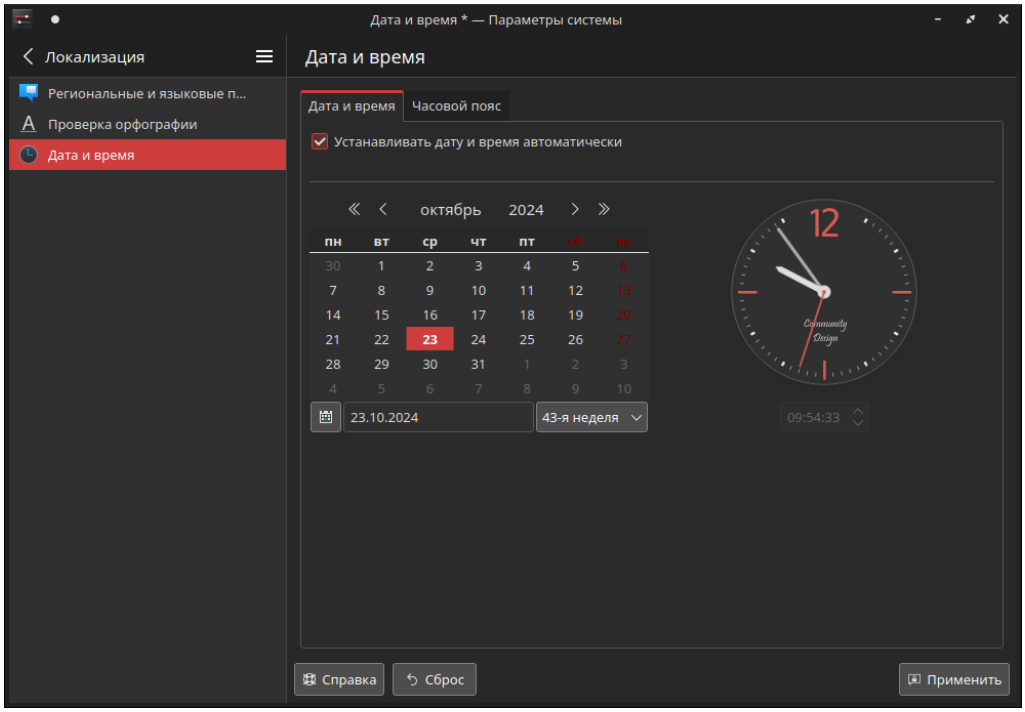
Для изменения настроек отключите автоматическое определение даты и времени (синхронизацию по NTP) и установите время и дату. Изменения будут применены автоматически.



Также доступно управление форматом отображения даты и времени в верхней панели — формат времени (12-часовой/24-часовой), день недели, дата, секунды и номера недель.

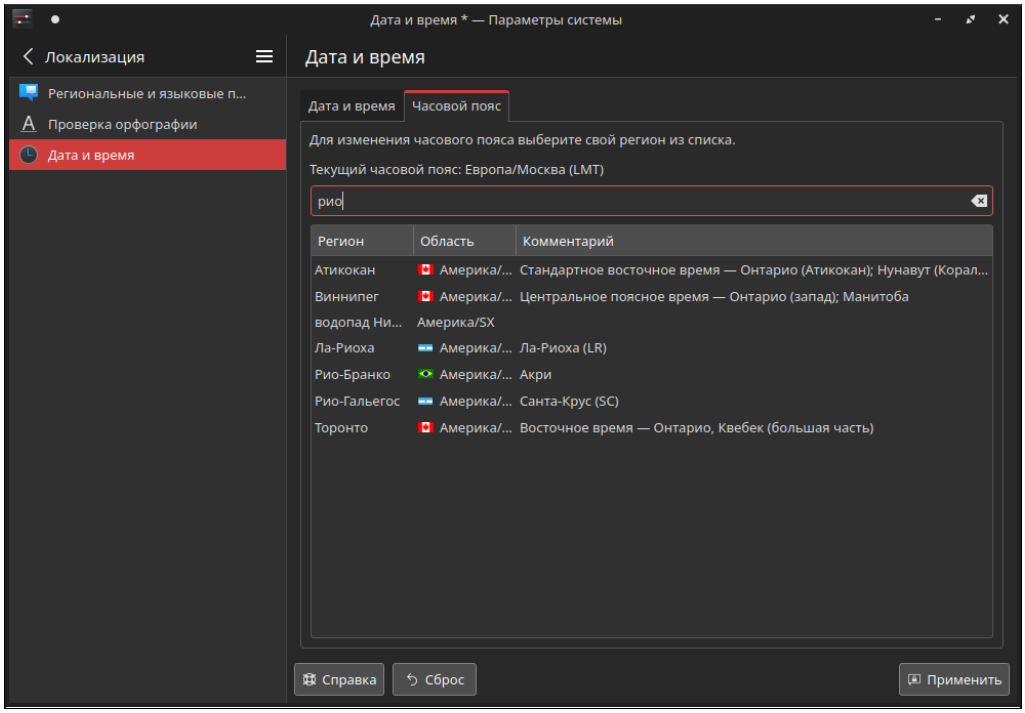
Диспетчер настройки даты и времени в KDE

Изменение даты и времени в РЕД ОС с графическим окружением **KDE** по умолчанию производится в разделе «**Дата и время**» системных настроек («**Параметры системы**» — «**Локализация**»).



По умолчанию включен параметр «**Устанавливать дату и время автоматически**», поэтому настройка даты и времени вручную отключена. Для изменения настроек отключите автоматическую установку даты и времени и установите собственные значения для соответствующих параметров. Для применения внесенных изменений нажмите «**Применить**».

Для изменения часового пояса перейдите на вкладку **Часовой пояс** и выберите свой регион из списка или воспользуйтесь строкой поиска. Для применения изменений нажмите «**Применить**».



Утилита настройки даты и времени timedatectl

Изменение часового пояса
Изменение даты и времени
Графические утилиты настройки даты и времени

Изменение часового пояса

Для подробного вывода информации об установленных дате, времени и выбранном часовом поясе, а также их настройке, используется утилита **timedatectl**.

Просмотр текущих настроек осуществляется командой:

```
timedatectl

               Local time: Вт 2022-11-15 11:36:46 MSK
           Universal time: Вт 2022-11-15 08:36:46 UTC
                 RTC time: Вт 2022-11-15 08:36:46
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

здесь:

- **Local time** (местное время) — это время, которое применяется в определенном географическом регионе или месте. Оно основано на солнечном времени и связано с часовым поясом данной местности;
- **Universal time** (универсальное время) — известно также как координированное всемирное время (UTC), универсальное время является международным стандартом времени, применяемым во всем мире. UTC не зависит от географического положения и не имеет смещения;
- **RTC time** (Real-Time Clock time) — это время, которое хранится во встроенных часах реального времени (RTC) компьютера или устройства. RTC используется для отслеживания текущего времени, даже когда устройство отключено от источника питания. **RTC time** используется при запуске системного времени и может быть синхронизировано с локальным временем операционной системы.
- **Time Zone** — установленная временная зона или часовой пояс;
- **System clock synchronized** — синхронизация системного времени с сервером **ntp**, принимает значения - *yes* (синхронизация производится) и *no* (синхронизация отключена);
- **NTP service** — доступность службы **ntp**;
- **RTC in local TZ** — синхронизация RTC с локальным временем операционной системы, принимает значения - *yes* (синхронизация производится) и *no* (синхронизация отключена).

Если часовой пояс указан неверно, его можно задать без перезагрузки системы с помощью команды:

```
tzselect

Please identify a location so that time zone rules can be set correctly.
Please select a continent, ocean, "coord", or "TZ".
 1) Africa
 2) Americas
 3) Antarctica
 4) Asia
 5) Atlantic Ocean
 6) Australia
 7) Europe
 8) Indian Ocean
 9) Pacific Ocean
10) coord - I want to use geographical coordinates.
11) TZ - I want to specify the time zone using the Posix TZ format.

#? 7
```

Будет предложено выбрать континент (в данном случае выбран вариант **7 - Europe**).

Затем потребуется выбрать страну (в примере выбран вариант **38 - Russia**) и регион (в примере выбран вариант **23 - Magadan**).

```
Please select a country whose clocks agree with yours.
```

```
 1) Albania    18) Guernsey      35) Poland
 2) Andorra    19) Hungary       36) Portugal
 3) Austria    20) Ireland       37) Romania
 4) Belarus    21) Isle of Man   38) Russia
 5) Belgium    22) Italy         39) San Marino
 6) Bosnia & Herzegovina  23) Jersey      40) Serbia
 7) Britain (UK)   24) Latvia      41) Slovakia
 8) Bulgaria    25) Liechtenstein     42) Slovenia
 9) Croatia    26) Lithuania      43) Spain
10) Czech Republic   27) Luxembourg     44) Svalbard & Jan Mayen
11) Denmark    28) Malta      45) Sweden
12) Estonia    29) Moldova       46) Switzerland
13) Finland    30) Monaco      47) Turkey
14) France    31) Montenegro     48) Ukraine
15) Germany    32) Netherlands     49) Vatican City
16) Gibraltar    33) North Macedonia     50) Åland Islands
17) Greece    34) Norway
#? 38

Please select one of the following time zone regions.
 1) MSK-01 - Kaliningrad  15) MSK+04 - Kemerovo
 2) MSK+00 - Moscow area  16) MSK+04 - Krasnoyarsk area
 3) Crimea    17) MSK+05 - Irkutsk, Buryatia
 4) MSK+00 - Kirov    18) MSK+06 - Zabaykalsky
 5) MSK+01 - Astrakhan    19) MSK+06 - Lena River
 6) MSK+01 - Volgograd    20) MSK+06 - Tomponsky, Ust-Maysky
 7) MSK+01 - Saratov    21) MSK+07 - Amur River
 8) MSK+01 - Ulyanovsk    22) MSK+07 - Oymyakonsky
 9) MSK+01 - Samara, Udmurtia  23) MSK+08 - Magadan
10) MSK+02 - Urals    24) MSK+08 - Sakhalin Island
11) MSK+03 - Omsk    25) MSK+08 - Sakha (E); North Kuril Is
12) MSK+04 - Novosibirsk  26) MSK+09 - Kamchatka
13) MSK+04 - Altai    27) MSK+09 - Bering Sea
14) MSK+04 - Tomsk
#? 23
```

После этого будет предложено проверить установленные параметры и, если все верно, подтвердить свой выбор.

```
The following information has been given:

 Russia
 MSK+08 - Magadan

Therefore TZ='Asia/Magadan' will be used.
Selected time is now: Tue Nov 15 19:38:15 +11 2022.
Universal Time is now: Tue Nov 15 08:38:15 UTC 2022.
Is the above information OK?
1) Yes
2) No
#? 1

You can make this change permanent for yourself by appending the line
 TZ='Asia/Magadan'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
Asia/Magadan
```

Далее для применения настроек перейдите в домашний каталог пользователя (в примере **/home/user/**) и создайте файл **.profile**:

```
cd /home/user/
nano .profile
```

Добавьте в него строку, указанную в выводе команды `tzselect` (выделена зеленым цветом):

```
TZ='Asia/Magadan'; export TZ
```

Сохраните изменения в файле и перезапустите сеанс пользователя.

Еще один способ изменения часового пояса доступен через утилиту **timedatectl**. Список доступных часовых поясов выводится командой:

```
timedatectl list-timezones
```

Чтобы выбрать нужный часовой пояс, используется команда:

```
timedatectl set-timezone <часовой_пояс>
```

Например:

```
timedatectl set-timezone America/Los_Angeles
timedatectl status

               Local time: Чт 2022-01-13 04:05:00 PST
         Universal time: Чт 2022-01-13 12:05:00 UTC
               RTC time: Чт 2022-01-13 12:05:00
              Time zone: America/Los_Angeles (PST, -0800)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Изменение даты и времени

Для изменения даты и времени используется команда:

```
timedatectl -- set-time "<дата> <время>"
```

Однако при попытке вноса изменений может возникнуть следующая ошибка:

```
timedatectl -- set-time "2002-08-28 00:00:00"

Failed to set time: Automatic time synchronization is enabled
```

Она означает, что в системе включена автоматическая синхронизация. Отключить ее можно следующей командой:

```
timedatectl set-ntp no
```

Проверка статуса синхронизации:

```
timedatectl status

               Local time: Ср 2002-08-28 00:00:03 MSD
         Universal time: Вт 2002-08-27 20:00:03 UTC
               RTC time: Вт 2002-08-27 20:00:04
              Time zone: Europe/Moscow (MSD, +0400)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

После этого необходимо повторить запрос на изменение даты и времени. Чтобы убедиться, что изменения вступили в силу, можно еще раз вывести статус настроек:

```
timedatectl -- set-time "2002-08-28 00:00:00"
timedatectl status

               Local time: Ср 2002-08-28 00:00:03 MSD
         Universal time: Вт 2002-08-27 20:00:03 UTC
               RTC time: Вт 2002-08-27 20:00:04
              Time zone: Europe/Moscow (MSD, +0400)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

С помощью данной команды дату и время можно изменять как в совокупности, так и отдельно. Для этого в команде следует указывать только один из параметров.

```
timedatectl -- set-time "2002-08-28"

  или

timedatectl -- set-time "15:30:00"
```

Графические утилиты настройки даты и времени

Подробную информацию о смене часового пояса и настройке системных даты и времени в графических утилитах см. в инструкциях «Диспетчер даты и времени» и «system-config-date».

Настройка и использование systemd-таймеров

Системные таймеры и чтение информации о них
Примеры использования таймеров
Создание таймеров
Преимущества и недостатки работы с таймерами

Таймеры — файлы юнитов **systemd**, имя которых имеет суффикс **.timer**; они позволяют контролировать файлы **.service** или определенные события. Эти таймеры могут быть использованы в качестве замены **cron**. Таймеры имеют встроенную поддержку календарных и регулярных событий и могут запускаться в асинхронном режиме.

Вы можете подробнее ознакомиться с созданием и настройкой systemd-таймеров, просмотрев наши обучающие видео:

- на **RuTube** — Настраиваем таймеры systemd вместо заданий cron;
- в **Яндекс.Дзен** — Настраиваем таймеры systemd вместо заданий cron;
- в **VK Видео** — Настраиваем таймеры systemd вместо заданий cron.

На наших каналах вы также сможете найти много другой полезной информации.

Системные таймеры и чтение информации о них

Когда система РЕД ОС устанавливается на компьютер, создается несколько системных таймеров, являющихся частью процедур обслуживания системы.

Чтобы увидеть, какие таймеры работают на данный момент, введите команду:

```
systemctl status *timer
● fstrim.timer - Discard unused blocks once a week
     Loaded: loaded (/usr/lib/systemd/system/fstrim.timer; enabled; preset: enabled)
     Active: active (waiting) since Thu 2024-12-19 08:27:01 MSK; 5h 33min ago
    Trigger: Mon 2024-12-23 01:09:54 MSK; 3 days left
   Triggers: ● fstrim.service
       Docs: man:fstrim

дек 19 08:27:01 localhost systemd[1]: Started fstrim.timer - Discard unused blocks once a week.● logrotate.timer - Daily rotation of log files
     Loaded: loaded (/usr/lib/systemd/system/logrotate.timer; enabled; preset: enabled)
     Active: active (waiting) since Thu 2024-12-19 08:27:01 MSK; 5h 33min ago
    Trigger: Fri 2024-12-20 00:18:40 MSK; 10h left
   Triggers: ● logrotate.service
       Docs: man:logrotate(8)
             man:logrotate.conf(5)

дек 19 08:27:01 localhost systemd[1]: Started logrotate.timer - Daily rotation of log files.● dnf-makecache.timer - dnf makecache --timer
     Loaded: loaded (/usr/lib/systemd/system/dnf-makecache.timer; enabled; preset: enabled)
     Active: active (waiting) since Thu 2024-12-19 08:27:01 MSK; 5h 33min ago
    Trigger: Thu 2024-12-19 15:49:48 MSK; 1h 49min left
   Triggers: ● dnf-makecache.service

дек 19 08:27:01 localhost systemd[1]: Started dnf-makecache.timer - dnf makecache --timer.● systemd-tmpfiles-clean.timer - Daily Cleanup
of Temporary Directories
     Loaded: loaded (/usr/lib/systemd/system/systemd-tmpfiles-clean.timer; static)
     Active: active (waiting) since Thu 2024-12-19 08:27:01 MSK; 5h 33min ago
    Trigger: Fri 2024-12-20 08:42:17 MSK; 18h left
   Triggers: ● systemd-tmpfiles-clean.service
       Docs: man:tmpfiles.d(5)
             man:systemd-tmpfiles(8)

дек 19 08:27:01 localhost systemd[1]: Started systemd-tmpfiles-clean.timer - Daily Cleanup of Temporary Directories.
```

С каждым таймером связано, по меньшей мере, шесть строк, содержащих сведения о нём:

1. Имя файла таймера и короткое описание цели существования этого таймера (но не всегда).
2. Сведения о состоянии таймера - загружен ли таймер, полный путь к файлу таймера, состояние **vendor preset** (**disabled** или **enabled**).
3. Сведения об активности таймера, куда входят данные о том, когда именно таймер был активирован.
4. Дата и время следующего запуска таймера и примерное время, оставшееся до его запуска.

5. Имя сервиса или события, вызываемого таймером.
6. Некоторые (но не все) таймеры содержат указатели на документацию.

Примеры использования таймеров

Самым простым примером использования таймеров можно считать системный таймер **systemd-tmpfiles-clean**. Как следует из названия, данный таймер раз в некоторое время производит очистку временных файлов системы.

```
● systemd-tmpfiles-clean.timer - Daily Cleanup of Temporary Directories
   Loaded: loaded (/usr/lib/systemd/system/systemd-tmpfiles-clean.timer; stati
   Active: active (waiting) since Thu 2024-12-19 08:27:01 MSK; 5h 33min ago
  Trigger: Fri 2024-12-20 08:42:17 MSK; 18h left
 Triggers: ● systemd-tmpfiles-clean.service
     Docs: man:tmpfiles.d(5)
           man:systemd-tmpfiles(8)
```

Данный таймер является системным и включен по умолчанию.

Создание таймеров

В системе РЕД ОС юниты **systemd** располагаются в следующих директориях:

- **/usr/lib/systemd/system** — юниты, поставляемые вместе с системой и устанавливаемыми приложениями;
- **/etc/systemd/system** — юниты системного администратора.

Для примера будет создан простой файл конфигурации сервиса, запускающий команду **free** (утилита, выводящая информацию об использовании оперативной памяти). Это может пригодиться, если необходимо регулярно отслеживать объём свободной памяти.

Создайте **unit**-файл с именем **ramMonitor.service** в папке **/etc/systemd/system**.

```
sudo nano /etc/systemd/system/ramMonitor.service
```

И добавьте в него следующие строки:

```
[Unit]
Description=Monitors RAM # Описание сервиса
Wants=ramMonitor.timer # Зависимость, отсылается к таймеру (будет создан позже)

[Service]
Type=oneshot # Тип службы, означающий выполнение одного задания и завершение
ExecStart=/usr/bin/free # Указывается полный путь к исполняемому файлу программы

[Install]
WantedBy=multi-user.target # Указывается, на каком уровне происходит запуск сервиса. Параметр multi-user.target указывает на запуск в многопользовательском режиме без графики
```

Данный файл можно назвать простейшим файлом конфигурации сервиса.

После проведенных манипуляций, проверьте состояние вашего сервиса командой:

```
systemctl status ramMonitor.service

● ramMonitor.service - Monitors RAM
   Loaded: loaded (/etc/systemd/system/ramMonitor.service; disabled; preset: disabled)
   Active: inactive (dead)
```

Сервис существует, но не активен. Запустите сервис и проверьте его статус:

```
systemctl start ramMonitor.service
systemctl status ramMonitor.service

● ramMonitor.service - Monitors RAM
    Loaded: loaded (/etc/systemd/system/ramMonitor.service; disabled; preset: disabled)
```

```
     Active: inactive (dead)

дек 19 14:39:45 localhost.localdomain systemd[1]: Starting Monitors RAM...
дек 19 14:39:45 localhost.localdomain systemd[1]: ramMonitor.service: Succeeded.
дек 19 14:39:45 localhost.localdomain systemd[1]: Finished Monitors RAM.
дек 19 14:39:45 localhost.localdomain free[3288]:              total        used
дек 19 14:39:45 localhost.localdomain free[3288]: Mem:        2016164      871644
дек 19 14:39:45 localhost.localdomain free[3288]: Swap:       4162552      384768
```

При включении сервиса в терминале не выводится никаких сообщений. Это происходит, потому что по умолчанию стандартный вывод (**stdout**) от программ, запускаемых **systemd**, перенаправляется в журнал **systemd**.

Чтобы проверить этот журнал, воспользуйтесь командой:

```
journalctl -u ramMonitor.service

дек 19 14:39:45 localhost.localdomain systemd[1]: Starting Monitors RAM...
дек 19 14:39:45 localhost.localdomain systemd[1]: ramMonitor.service: Succeeded.
дек 19 14:39:45 localhost.localdomain systemd[1]: Finished Monitors RAM.
дек 19 14:39:45 localhost.localdomain free[3288]:              total        use
дек 19 14:39:45 localhost.localdomain free[3288]: Mem:        2016164      871644
дек 19 14:39:45 localhost.localdomain free[3288]: Swap:       4162552      384768
```

С помощью ключа -S вы можете указать временной период, за который утилита **journalctl** будет искать записи. Например, `journalctl -S today -u ramMonitor.service` выведет записи, сделанные за сегодня.

Убедившись в работоспособности сервиса, создайте для него таймер. Для этого необходимо создать в той же папке файл с названием ramMonitor.timer.

```
nano /etc/systemd/system/ramMonitor.timer
```

В файл добавьте следующее содержимое:

```
[Unit]
Description=Monitors RAM
Requires=ramMonitor.service # Указание строгой зависимости

[Timer]
Unit=ramMonitor.service # Ссылка на сервис
OnCalendar=*-*-* *:*:00 # Срабатывание таймера по условию календаря. В данном случае – каждую минуту

[Install]
WantedBy=timers.target
```

В секции **[Timer]** указываются условия запуска. Таймеры могут быть двух типов: событийные и монотонные. Первые активируются по событию, вторые выполняются периодически. Из событий таймеров можно выделить **OnBootSec**, срабатывающий через определенное время после запуска системы. Из монотонных следует выделить:

- **OnUnitActiveSec** — срабатывает через указанное время после активации целевого юнита;
- **OnUnitInactiveSec** — срабатывает так же, как **OnUnitActiveSec**, только время отсчитывается с момента прекращения работы целевого юнита, хорошо подходит для «длительных» задач, например, бекапов.
- **OnCalendar** — срабатывает по условию календаря.

В качестве формата даты для календаря используется формат:

```
DOW YYYY-MM-DD HH:MM:SS
```

(где **DOW** (**D**ay **O**f **W**eek) — *день недели*, необязательный параметр; за ним следует указание *года*, *месяца*, *дня* через дефис и *часы*, *минуты* и *секунды* через двоеточие. Для указания любого значения используется «*», перечисления делаются через запятую, а диапазоны через «**..**»).

После завершения настройки нужно запустить таймер и проверить его статус:

```
systemctl start ramMonitor.timer
systemctl status ramMonitor.timer
```

```
● ramMonitor.timer - Monitors RAM
     Loaded: loaded (/etc/systemd/system/ramMonitor.timer; disabled; vendor pres
     Active: active (waiting) since Thu 2024-12-19 14:39:45 MSK; 7s ago
    Trigger: Thu 2024-12-19 14:40:45 MSK; 29s left
   Triggers: ● ramMonitor.service

дек 24 14:39:45 localhost.localdomain systemd[1]: Started Monitors RAM.
```

Если все настроено верно, таймер будет иметь состояние **active (waiting)**, а ниже будет указано время до его запуска.

Преимущества и недостатки работы с таймерами

Основные преимущества:

- Задачи могут быть легко запущены сразу, независимо от их таймеров - это упрощает отладку.
- Каждая задача может быть настроена для работы в определенной среде.
- Задачи могут быть настроены в зависимости от других юнитов **systemd**.
- Задачи регистрируются в журнале **systemd**.

Единственным недостатком можно считать сложность создания таких таймеров: чтобы настроить задачу, запускаемую в определенное время при помощи **systemd**, нужно создать два файла и использовать команды **systemctl**. По сравнению с добавлением одной строки в crontab. Кроме того в **systemd** отсутствует встроенный аналог *cron*'овского **MAILTO** для отправки писем при сбоях.

Планировщик заданий crontab

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Crontab - таблицы, управляющие работой службы **cron**. Файл содержит инструкции службы *cron* в общей форме: запускать указанную команду в заданное время и в заданные дни. На компьютере обычно имеются общесистемный файл (**/etc/crontab**) и индивидуальные файлы (**/var/spool/cron/**) для пользователей системы. Таким образом, команды в файле будут выполняться с правами этих пользователей или, в случае общесистемного файла, с правами пользователя, указанного в командной строке при запуске службы. У служб **Uucp** и **News** обычно есть свои собственные *crontab*, устраняющие необходимость в явном запуске **su** в рамках команды *cron*.

> **Примечание!** Хотя **cron**, по сути, является обыкновенным текстовым файлом, он не должен редактироваться обычными средствами. Для создания, изменения и удаления следует использовать специальную утилиту - **crontab**.

Вы можете подробнее ознакомиться с работой службы **cron**, просмотрев наши обучающие видео:

- на **RuTube** — Планировщик задач в РЕД ОС. Cron;
- в **Яндекс.Дзен** — Планировщик задач в РЕД ОС. Cron;
- в **VK Видео** — Планировщик задач в РЕД ОС. Cron.

На наших каналах вы также сможете найти много другой полезной информации.

Пустые строки, ведущие пробелы и символы табуляции игнорируются. Строки, начинающиеся с символа «**#**», считаются комментариями и игнорируются. Заметьте, что комментарии не допускаются в тех же строках, где расположены команды *cron*, так как они будут распознаны как части команды. По этой же причине комментарии не разрешены в строках, задающих переменные среды.

Строка-директива представляет собой либо задание переменной среды, либо команду *cron*.

Задание переменной среды:

Можно определять среду (набор переменных среды), в которой будет выполняться команда. Задание переменной среды осуществляется в следующей форме:

```
<имя_переменной> = <значение>
```

где пробелы вокруг знака равенства («**=**») не обязательны, и любые пробелы после будут использованы как часть значения переменной . Строка может быть заключена в кавычки (одинарные или двойные) для возможности сохранения пробелов в начале и конце.

Несколько переменных среды устанавливаются автоматически службой *cron*. SHELL устанавливается в /**bin/sh**, а **LOGNAME** и **HOME** определяются по файлу **/etc/passwd** (в соответствии с владельцем *crontab*). Значения переменных HOME и SHELL можно переопределить директивами crontab.

В дополнение к *LOGNAME, HOME и SHELL* cron может использовать переменную **MAILTO** в случаях, если в данном crontab была указана отправка почты. Если MAILTO определена (и не пуста), электронная почта отправляется указанному в переменной пользователю. Если MAILTO определена, но пустая (MAILTO = ' '), электронная почта отправляться не будет. В противном случае, почта посылается владельцу crontab. Эта переменная полезна при запуске команд от псевдопользователей, для которых не определены почтовые адреса в системе.

Команды cron:

Существует две конфигурации cron: системная и пользовательская. Общесистемная настройка crontab работает безусловно для всех пользователей РЕД ОС. Пользовательская настройка является дополнительной и выполняется в сессиях пользователей.

Для редактирования файла необходимо ввести команду:

```
crontab -e
```

Для просмотра содержимого расписания:

```
crontab -l
```

Каждая стока в системной конфигурации cron, расположенной в каталоге **/etc**, состоит из шести полей и команды:

```
<минута> <час> <число> <месяц> <день_недели> <пользователь> <команда>
```

Каждая строка в пользовательской конфигурации cron, расположенной в домашнем каталоге пользователя, состоит из пяти полей и команды:

```
<минута> <час> <число> <месяц> <день_недели> <команда>
```

Поля отделяются друг от друга пробелами или символами табуляции. Команда может состоять из нескольких полей. Допустимые значения полей:

Поле	Допустимые значения
<минута>	* или 0-59
<час>	* или 0-23
<число>	* или 1-31
<месяц>	*, 1-12 или имя месяца (см. ниже)
<день_недели>	*, 0-7 или имя дня (воскресенье - это 0 и 7)
<пользователь>	имя существующего пользователя
<команда>	строка

Допустимо указание нескольких значений (и диапазонов через тире) через запятую. Примеры:

' '1 , 2, 5 , 9' ' ' '0-4, 8-12' '.

Диапазон указывается как два числа, разделенных дефисом. Указываемые числа включаются в диапазон. Например, значение поля <час> 8-11 приведёт к выполнению команды в 8, 9, 10 и 11 часов.

При указании диапазона можно пропускать некоторые его значения, указав шаг в форме **/<число>**. Например: «0-23/2» для поля означает запуск команды через два часа (по стандарту V7 пришлось бы указывать «0,2,4,6,8,10,12,14,16,18,20,22»). Шаг можно указывать также после звёздочки: «каждые два часа» соответствует значению «*/2».

Звёздочка («*****») без шага соответствует полному диапазону значений.

Для задания полей <месяц> и <день_недели> и можно использовать имена. Указывайте первые три буквы нужного дня или месяца на английском, регистр букв не имеет значения. Диапазоны или списки имён не разрешены.

Поле <команда> (остаток строки) определяет запускаемую по расписанию команду. Вся оставшаяся часть строки до символа перевода строки или символа «%», будет выполнен вызов **/bin/sh** или другой оболочки, определенной в переменной SHELL в crontab. Знак процента («%») в команде (если он не экранирован обратной косой чертой («\»)) будет соответствовать символу перевода строки и все данные после первого «%» будут посланы для команды на стандартный ввод.

Служба cron запускает команды, когда значения полей <минута>, <час>, <месяц> и хотя бы одно из полей <число> и <день_недели>, совпадают с текущим временем (см. замечание ниже). Служба cron сверяет директивы с текущим временем раз в минуту.

ЗАМЕЧАНИЕ

День выполнения команды может быть задан в двух полях - <число> и <день_недели>. Если оба поля определены (т.е. не равны «*»), то команда будет запущена, когда любое поле совпадёт с текущим временем. Например, запись:

30 4 1,15 * 5

приведёт к выполнении команды в 4:30 по полуночи первого и пятнадцатого числа каждого месяца, плюс в каждую пятницу.

Вместо первых пяти полей допустимо указание одного из восьми специальных триггеров:

Строка	Значение
@reboot	Выполнить команду один раз, при запуске cron(8).
@yearly	Выполнять команду каждое 1 января, "0 0 1 1*"
@annually	(эквивалентно @yearly).
@monthly	Выполнять команду в начале каждого месяца, "0 0 1 * *"
@weekly	Выполнять команду каждое воскресенье, "0 0 * * 0".
@daily	Выполнять команду в полночь, "0 0 * * *".
@midnight	(эквивалентно @daily).
@hourly	Выполнять команду раз в час, "0 * * * *".

Планировщик заданий at

Отправка задач с помощью at
Непосредственный ввод команд
Запуск скрипта
Утилита atq
Указание очереди
Формат ввода даты
Утилита atrm
Файлы конфигурации

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** at-3.1.23-1

Бывают ситуации, когда необходимо однократно выполнить команды или скрипт в определённое время. Такую задачу можно решить с помощью планировщика **at**, представленного службой **atd**.

Для использования службы **atd** сначала необходимо ее запустить:

```
systemctl start atd
```

Проверить статус службы можно командой:

```
systemctl status atd
```

Обратите внимание, что служба **atd** не имеет связанного терминала. Одной из определяющих характеристик службы **atd** является то, что она отказывается от связи с терминалом, который ее запустил.

Вы можете подробнее ознакомиться с настройкой утилиты **at**, просмотрев наши обучающие видео:

- на **RuTube** — Планировщик задач в РЕД ОС. Команда at;
- в **Яндекс.Дзен** — Планировщик задач в РЕД ОС. Команда at;
- в **VK Видео** — Планировщик задач в РЕД ОС. Команда at.

На наших каналах вы также сможете найти много другой полезной информации.

Отправка задач с помощью at

Команда **at** используется для отправки заданий и запуска в определенное время сервису **atd**. Задания, созданные с помощью **at** , выполняются только один раз.

Подробную информацию об утилите можно посмотреть с помощью команды:

```
man at
```

Справка по использованию утилиты доступна при выполнении команды:

```
at --help
```

Непосредственный ввод команд

Если выполнить **at** только с указанием времени, он предложит ввести необходимые к выполнению команды с помощью стандартного ввода (клавиатуры). После ввода последовательности команд нажмите сочетание клавиш «**Ctrl+D**», чтобы выйти и сохранить задание. При вводе непосредственно с терминала «**Ctrl+D**» указывает на "конец файла".

```
at 8:22

warning: commands will be executed using /bin/sh
at> echo "$(date)" > /home/user/at.txt
```

```
at>
job 1 at Thu Dec  8 08:22:00 2022
```

Запуск скрипта

Если необходимо разово в определенное время запустить скрипт, тогда кроме нужного времени потребуется указать путь к файлу сценария, используя ключ **-f**. Можно дополнительно указать ключ **-m**, чтобы получить системное сообщение на почту при любом исходе выполнения команды.

```
at -f <имя_файла> -m <время>
```

Например:

```
at -f /home/user/at.sh -m 10:30

warning: commands will be executed using /bin/sh
job 4 at Thu Dec  8 10:30:00 2022
```

Утилита atq

Проверка установленного для исполнения задач порядка и времени может осуществляться с помощью утилиты **atq** или команды `at -l`.

```
atq

2 Wed Dec  7 16:45:00 2022 a user
4 Thu Dec  8 10:30:00 2022 a user
1 Thu Dec  8 08:22:00 2022 a user
3 Thu Dec  8 10:30:00 2022 a user
```

В выводе перечислены все задания, по одному в каждой строке. Каждая строка включает *номер* задания, *дату*, *время*, *букву* очереди и *имя пользователя*.

Указание очереди

По умолчанию задания, созданные с помощью **at**, планируются в очереди с именем «**a**».

Запросы могут иметь имена от «**a**» ... «**z**» до «**A**» ... «**Z**». Очереди со строчными буквами имеют приоритет над очередями с прописными буквами.

Вы можете указать очередь с помощью опции **-q**. Например, чтобы установить задание в **M**-очередь, необходимо выполнить команду вида:

```
at monday +2 hours -q M
at -f /home/user/at.sh 10:30 -q M
atq

2 Wed Dec  7 16:45:00 2022 a user
5 Mon Dec 12 15:32:00 2022 M user
4 Thu Dec  8 10:30:00 2022 a user
1 Thu Dec  8 08:22:00 2022 a user
6 Thu Dec  8 10:30:00 2022 M user
3 Thu Dec  8 10:30:00 2022 a user
```

Формат ввода даты

При формировании команды необходимо указывать время запуска, однако также предусмотрено указание и даты.

Если дата не указана, то принимается текущая, а если указанное время в текущий день уже прошло, задача планируется на следующий день.

Время дня можно указать в формате **ЧЧ:ММ** с суффиксом «**am**» или «**pm**». Также могут использоваться термины «**midnight**», «**noon**», и «**teatime**».

Дата также может быть указана в нескольких форматах, включая **ММ/ДД/ГГ**.

Более подробное описание команды можно найти на странице справки:

```
man at
```

Утилита atrm

Запланированные к исполнению задачи могут быть удалены из очереди с помощью утилиты `atrm` или `at -r`. Для этого достаточно ввести команду и указать номер запланированной задачи.

Например:

```
atrm 5
atq

2 Wed Dec  7 16:45:00 2022 a user
4 Thu Dec  8 10:30:00 2022 a user
1 Thu Dec  8 08:22:00 2022 a user
6 Thu Dec  8 10:30:00 2022 M user
3 Thu Dec  8 10:30:00 2022 a user
```

Файлы конфигурации

Можно использовать файлы конфигурации **/etc/at.allow** и **/etc/at.deny** для четкого указания пользователей, которые могут или не могут планировать исполнение задач с помощью службы **atd**.

Файл **/etc/at.allow** содержит список пользователей, которым позволено осуществлять планирование исполнения задач с помощью службы **atd**. В том случае, если файла **/etc/at.allow** не существует, служба **atd** может использоваться любым пользователем, имя которого не внесено в файл **/etc/at.deny**.

Файл **/etc/at.deny** содержит список пользователей, которым запрещено осуществлять планирование исполнения задач с помощью службы **atd**.

В случае, если не существует ни одного из этих файлов, службу **atd** по прямому назначению может использовать любой пользователь.

Примечание.

Если вы планируете передать **at** команду, требующую прав **суперпользователя**, помните, что она будет выполняться без присмотра — sudo не будет работать, т.к. никто не может ввести пароль. Для возможности отслеживания действий сначала войдите в систему как пользователь **root**, либо используйте команду `sudo at`.

Планировщик заданий anacron

Описание работы
Пример использования
Файл настроек
Сравнение cron и anacron

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** cronie-anacron-1.5.6-1

Программа **anacron**, как и **cron**, используется для настройки команд на многократное или регулярное выполнение.

Cron — это служба, используемая для запуска запланированных задач. **Cron** хорошо подходит для запуска запланированных задач на машинах, которые будут работать непрерывно 24/7, таких как серверы. Причём, если в запланированное время компьютер будет выключен, задача выполнена не будет.

Anacron — асинхронный или анахроничный **cron**. Используется для периодического запуска команд с частотой, определенной в днях. Его работа несколько отличается от работы **cron**, предполагая, что машина не будет включена все время.

Anacron подходит для выполнения *ежедневных*, *еженедельных* и *ежемесячных* запланированных заданий на ноутбуках или ПК. Если используется **anacron**, можно быть уверенным, что при следующем включении компьютера или ноутбука запланированная задача обязательно будет выполнена.

Вы можете подробнее ознакомиться с настройкой **anacron**, просмотрев наши обучающие видео:

- на **RuTube** — Планировщик задач в РЕД ОС. Anacron;
- в **Яндекс.Дзен** — Планировщик задач в РЕД ОС. Anacron;
- в **VK Видео** — Планировщик задач в РЕД ОС. Anacron.

На наших каналах вы также сможете найти много другой полезной информации.

Описание работы

В РЕД ОС есть *man*-страница с информацией по использованию и применению **anacron**, вызываемая командой:

```
man anacron
```

Утилита **anacron**, как и **cron**, имеет таблицу планирования. Задания **anacron** перечислены в файле **/etc/anacrontab**, их можно запланировать в следующем формате (комментарии внутри файла **anacrontab** должны начинаться с **#**):

```
#period  delay  job-identifier  command
```

где:

- *period* – это частота выполнения задания, указанная в днях или в виде: **@daily**, **@weekly** или **@monthly** для одного раза в *день*, *неделю* или *месяц* соответственно. Также можно использовать числа: *1 – ежедневно*, *7 – еженедельно*, *30 – ежемесячно* и *N – количество дней*;
- *delay* – это количество минут ожидания перед выполнением задания. Желательно для каждого задания указывать разное время, чтобы несколько заданий не запускались одновременно;
- *job-id* – это отличительное имя для задания, записанное в файлах журнала. Это имя используется для создания файла контроля задания. Файл создаётся в папке **/var/spool/anacron/** и содержит сведения, позволяющие программе **anacron** контролировать выполнение задания;
- *command* – это команда или путь к сценарию оболочки, который будет выполнен.

Anacron использует не такие подробные параметры, как **cron**. Наименьший интервал, который существует в **anacron** – день. Это значит, что **anacron** нужно использовать как дополнение к **cron**, а не в качестве его замещения.

Anacron имеет следующий принцип работы — он проверяет, выполнено ли задание за указанный период в поле **period**. Если нет, **anacron** выполняет команду из поля **command** после ожидания определенного количества минут (**delay**).

После выполнения задания **anacron** записывает дату в файл метки времени в каталоге **/var/spool/anacron** с именем, указанным в поле

id задания (имя файла метки времени).

Пример использования

Приведенный пример будет запускать скрипт **/home/user/backup.sh** каждый день:

```
#period delay  job-identifier  command
@daily  10   example.daily   /bin/bash /home/user/backup.sh
```

Если машина выключена, когда ожидается выполнение задания **backup.sh**, anacron запустит выполнение этого задания через 10 минут после следующего включения машины, не ожидая еще 7 дней.

Файл настроек

В файле **anacrontab**, кроме запланированных заданий, также есть важные переменные, которые необходимо понимать:

```
cat /etc/anacrontab

# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# the maximal random delay added to the base delay of the jobs
RANDOM_DELAY=45

# the jobs will be started during the following hours only
START_HOURS_RANGE=3-22


#period in days    delay in minutes  job-identifier   command
1    5  cron.daily  nice run-parts /etc/cron.daily
7    25  cron.weekly  nice run-parts /etc/cron.weekly
@monthly    45  cron.monthly  nice run-parts /etc/cron.monthly
```

Здесь:

- **RANDOM_DELAY** — определяет максимальную случайную задержку в минутах, добавляемую к пользовательской задержке задания (по умолчанию 45 мин);
- **START_HOURS_RANGE** — задает временной интервал, в течение которого будут запускаться задания (т.е. задания будут выполнятся только в течение следующих часов).

Сравнение cron и anacron

Cron	Anacron
является службой	не является службой
подходит для серверных машин	подходит для ПК и ноутбуков
позволяет запускать запланированные задания каждую минуту	позволяет запускать запланированные задания только на ежедневной основе
если машина выключена, запланированное задание не выполняется	если машина выключена, когда запланировано задание, *anacron* выполнит запланированное задание при следующем включении машины
может использоваться как **локальными пользователями**, так и суперпользователем **root**	может использоваться **только** суперпользователем **root**, если не указано иное (включено для обычных пользователей с конкретными настройками)

Основное различие между **cron** и **anacron** заключается в том, что **cron** эффективно работает на машинах, которые будут работать непрерывно, в то время как **anacron** предназначен для машин, которые будут отключены через день или неделю.

Графическая утилита для планирования заданий zeit

Установка
Работа с утилитой

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: zeit-0.6.0-2

Cron — это служба, используемая для запуска запланированных задач. **Cron** подходит для запуска запланированных задач на машинах, которые могут работать непрерывно 24/7, таких как серверы. Причём, если в запланированное время компьютер будет выключен, задача выполнена не будет.

zeit – графическая утилита для планирования заданий cron.

К запланированным заданиям можно отнести такие операции, как резервное копирование, очистка дискового пространства и прочие задачи обслуживания системы.

Установка

Для установки утилиты **zeit** перейдите в сеанс пользователя **root**:

```
su -
```

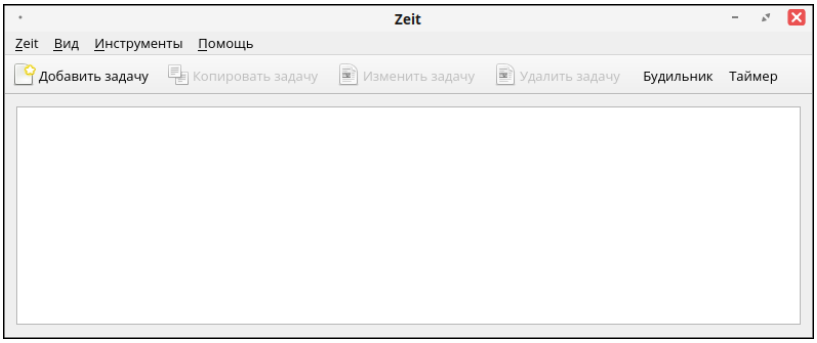
и выполните команду:

```
dnf install zeit
```

После установки запуск утилиты доступен из «**Главного меню**» – «**Системные**» – «**Планировщик заданий**» или через терминал (запуск производится с правами **непривилегированного** пользователя):

```
[ "$EUID" -ne 0 ] && zeit || echo "Команда не должна выполняться с правами пользователя root!"
```

Главное окно утилиты **zeit** выглядит следующим образом:

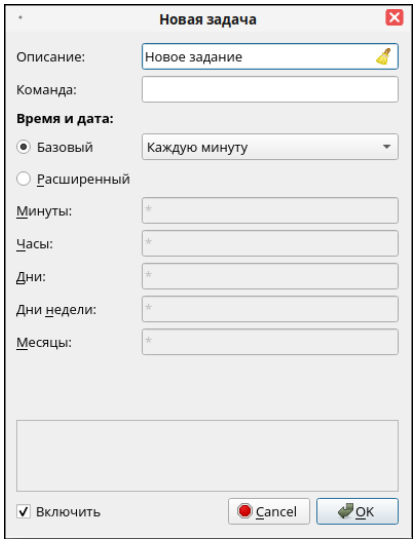


Интерфейс утилиты довольно прост и интуитивно понятен – здесь доступны:

- 4 основные опции:
  - Добавить;
  - Копировать;
  - Изменить;
  - Удалить;
- 2 дополнительные опции:
  - Будильник;
  - Таймер.

Работа с утилитой

Для создания нового запланированного задания нажмите кнопку «**Добавить задачу**».



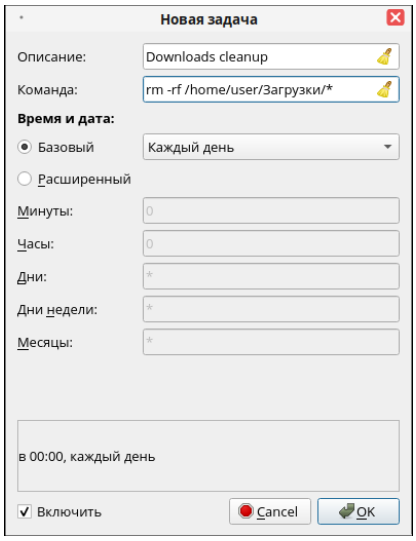
В появившемся окне задайте описание задания, непосредственно задание в виде команды **bash**, а также укажите временной интервал, по которому будет выполняться команда.

В списке **Базовый** предлагаются следующие параметры временного интервала:

- Каждую минуту;
- Каждый час;
- Каждый день;
- Каждую неделю;
- Каждый месяц;
- Кроме выходных.

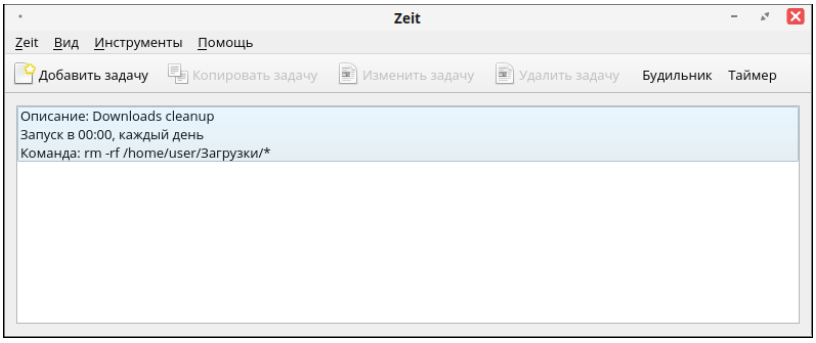
Если необходимо указать конкретную дату и время, выберите вариант **Расширенный** и установите собственные значения в соответствующих полях.

Для примера будет создана простая задача – ежедневная очистка каталога «**Загрузки**».



Нажмите **OK**, чтобы создать задание **cron**.

После этого созданное задание будет отображено в списке.



Для проверки активности задания выведите содержимое файла **crontab** с помощью команды:

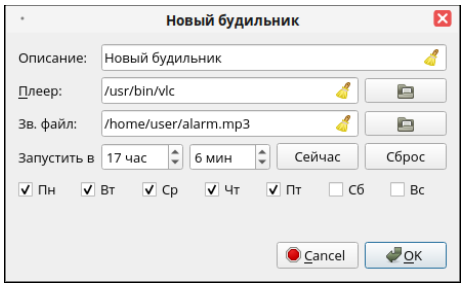
```
crontab -l

#Downloads cleanup
0 0 * * * rm -rf /home/user/Загрузки/*
```

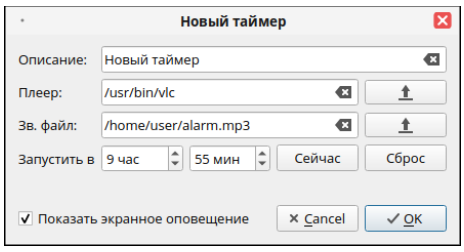
Задание будет выполняться каждый день в 0:00.

Для редактирования запланированного задания выберите его из списка утилиты и нажмите кнопку «**Изменить задачу**». Внесите необходимые изменения и нажмите **OK** для обновления задачи.

Для удаления запланированного задания выберите его из списка утилиты и нажмите кнопку «**Удалить задачу**».

В **zeit** также представлены две дополнительные опции: *будильник* и *таймер*. Будильник будет проигрывать звуковой сигнал в определенное время в выбранные дни недели, таймер будет проигрывать звуковой сигнал только в указанное время. Будильники/таймеры могут быть полезны для напоминания о чем-то важном.





Сервер электронной почты postfix

Работа в режиме SMTP-сервера
Пакеты postfix
Конфигурационные файлы
Доменная информация
Postfix на узлах с удалённым доступом к сети
Postfix на клиентской машине локальной сети
Почтовый сервер для небольших доменов и сетей
Алиасы и преобразования адресов
Защита от нежелательной корреспонденции
Прочие настройки
Использование Postfix

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** postfix-3.7.2-1

Сервер электронной почты **postfix** позволяет организовать обмен электронной почтой с Интернет и внутри локальной сети. postfix рекомендуется к установке в любой конфигурации РЕД ОС. Это объясняется тем, что в UNIX-подобных системах возможность отправлять почту с помощью вызова команды из командой оболочки практически обязательна. Некоторые программы (например, служба исполнения заданий по расписанию **crond**) пользуются этим для отправки сообщений пользователям.

Рекомендуется настраивать систему таким образом, чтобы доставкой всей электронной почты, проходящей через машину, занималась служба **MTA** (**Mail Transport Agent**), в нашем случае - postfix. Хотя многие почтовые программы способны отправлять сообщения на удалённый SMTP-сервер, имеет смысл поручить и эту задачу системному серверу электронной почты, чтобы не было необходимости следить за отсылкой отправленных писем.

Помимо postfix существуют и другие популярные реализации MTA, например, **qmail**, **exim** и даже ветеран Интернета **Sendmail**, хотя последний сейчас используется всё реже, поскольку неоправданно сложен в настройке. Однако по разным причинам, включая соображения безопасности, в любом дистрибутиве РЕД ОС по умолчанию в качестве MTA предлагается postfix.

Работа в режиме SMTP-сервера

Обратите внимание, что по умолчанию после установки postfix не работает в режиме SMTP-сервера. Для того, чтобы принимать сообщения по протоколу SMTP или ESMTP, как извне, так и локально, необходимо переключить службу postfix в режим работы **server** командой **control postfix server**. По умолчанию после установки служба postfix находится в режиме *local*, в котором postfix не принимает соединений из сети, ограничиваясь приёмом локальных соединений посредством сокетов семейства UNIX (UNIX-domain socket). Для большинства рабочих станций работа в режиме SMTP-сервера не требуется (и нежелательна с точки зрения безопасности), а в качестве SMTP-сервера должен использоваться какой-то внешний узел сети.

Пакеты postfix

Базовый RPM-пакет для установки сервера postfix в РЕД ОС носит, как нетрудно догадаться, имя postfix. Ряд дополнений, расширяющих возможности postfix, выделены в отдельные пакеты, полный список которых можно получить командой:

```
dnf search postfix-
```

Конфигурационные файлы

Файлы настройки postfix располагаются в каталоге **/etc/postfix**. Основные параметры определяются в файле **main.cf**; в частности, все параметры, о которых говорится далее в этом разделе, устанавливаются именно в этом файле, остальные случаи оговариваются специально.

Для простоты ориентации в настройке postfix в файле *main.cf* указываются только параметры, выставленные администратором системы, плюс некоторые из значений по умолчанию, которые администратору с большой вероятностью нужно будет изменить. Значения по умолчанию для всех остальных параметров перечислены в файле **main.cf.default** (этот файл не следует редактировать, он служит только для справок). Довольно полный список параметров с развёрнутыми комментариями и примерами приведён в файле **main.cf.dist**, а наиболее полную информацию по всем возможным параметрам следует искать в руководстве postconf.

Обратите внимание, что если вы изменили конфигурацию при запущенной службе postfix, новые настройки нужно активизировать командой **systemctl restart postfix**.

Доменная информация

Имя хоста и домена, которые считаются локальными при обработке email-адресов, необходимы для функционирования почтового сервера. Если эти имена для postfix должны отличаться от того, что выдаёт команда hostname, установите их с помощью параметров **myhostname** и **mydomain**.

Postfix на узлах с удалённым доступом к сети

Существует несколько проблем, возникающих при попытке отправки исходящей почты с машин, которые не являются полноценными узлами сети Интернет, например, в системах с модемным и другими непостоянными соединениями, не всегда возможно немедленно отправить сообщения удалённым адресатам по SMTP, и их приходится держать в очереди до тех пор, пока соединение не будет установлено. Для этого используется параметр **defer_transports**, например:

```
defer_transports = smtp
```

Доставка активизируется командой **/usr/sbin/sendmail -q**, которая в РЕД ОС исполняется автоматически при установке PPP-соединения.

Как любой полноценный MTA, postfix позволяет доставлять сообщения, связываясь напрямую с сервером, обслуживающим получателя письма. Тем не менее, для dialup-машин непосредственная доставка сообщений нежелательна, поскольку время соединения ограничено. К тому же это излюбленная тактика распространителей спама, поэтому многие почтовые серверы сверяют IP-адрес отправителя с базой известных адресов провайдерских пулов, после чего сообщения с таких адресов отвергаются. Поэтому целесообразно доверить доставку исходящей почты SMTP-серверу провайдера. Этим управляет параметр **relayhost**, например:

```
relayhost = [smtp.provider.net]
```

Postfix на клиентской машине локальной сети

Рабочие станции в локальной сети или машины в провайдерской сети, отделённой от Интернета с помощью межсетевого экрана/NAT, должны переправлять исходящую почту на почтовый сервер, обслуживающий данную сеть. Для этого также используется параметр **relayhost**, описанный выше. Если сервер задан IP-адресом, можно отключить использование DNS для ускорения работы:

```
disable_dns_lookups = yes
```

Для того чтобы в доменной части адреса отправителя фигурировал домен сети, а не имя конкретной машины в этой сети, установите параметр **myorigin** равным имени домена:

```
myorigin = $mydomain
```

Почтовый сервер для небольших доменов и сетей

Домены, для которых сервер получает почту, отличные от значения **mydomain** и не сконфигурированные как виртуальные домены postfix, нужно перечислить с помощью параметра **mydestination**, либо в дополнительном файле, на который ссылается этот параметр. Аналогичным образом параметр **mynetworks** описывает блоки IP-адресов, которые считаются внутренними и с которых разрешён приём исходящих сообщений. Не следует записывать в *mynetworks* блоки адресов, не принадлежащих сети, которую обслуживает сервер, поскольку этим могут воспользоваться распространители спама.

Для пользователей, желающих отправлять сообщения через данный сервер, когда они находятся вне пределов локальной сети, следует организовать SMTP-аутентификацию. В postfix для этой задачи следует использовать библиотеку SASL (начиная с версии 2.3 в postfix появилась возможность использовать разные реализации SASL). На текущий момент доступно две реализации: **Cyrus** (пакет postfix-cyrus) или **Dovecot** (пакет postfix-dovecot). Cyrus, кроме того, можно использовать в postfix для аутентификации в качестве клиента на удалённых SMTP-серверах.

Для шифрования соединений в этой схеме используется протокол *SSL/TLS*, для включения поддержки которого в postfix необходимо установить пакет **postfix-tls**. Используя postfix-tls следует принимать во внимание, что это расширение включает в postfix значительный объём исходных текстов, в меньшей степени проверенного в плане безопасности. Настройка аутентификации посредством *TLS/SASL* описана в файлах *TSL_README* и *SASL_README* в документации postfix.

Преобразование глобальных почтовых адресов в локальные адреса назначения устанавливается с помощью таблиц типа **virtual**:

```
virtual_alias_maps = cdb:/etc/postfix/virtual
```

Пример содержимого **/etc/postfix/virtual**:

```
domain1.ru # Домен в стиле postfix (текст здесь игнорируется) name1@domain1.ru user1 name2@domain2.ru user2@otherbox
@domain2.ru user3
```

После редактирования не забудьте активизировать изменения командой **systemctl restart postfix**.

Алиасы и преобразования адресов

Имена локальных адресатов либо совпадают с именами учётных записей пользователей системы, либо подставляются из таблицы **aliases**:

```
alias_maps = cdb:/etc/postfix/aliases
alias_database = cdb:/etc/postfix/aliases
```

При установке postfix «с нуля» в этой таблице создаётся алиас на имя root: вся корреспонденция, предназначенная администратору и поступающая на другие системные адреса, будет доставляться на имя реального пользователя, который осуществляет функции администратора. Изначально им становится первый зарегистрированный в системе реальный пользователь. Таблица алиасов отличается от остальных таблиц, используемых postfix; имена в поле слева (псевдонимы) отделяются от значений в поле справа (адреса доставки) двоеточиями. Адресаты в списке перечисляются через запятую. В качестве способа доставки можно использовать почтовые адреса, команды (обозначаются символом | в начале правой части; сообщение подаётся на стандартный поток ввода команды) и имена файлов:

```
John.Smith: john
chief: chief@bosscomputer
trio: stock, hausen, walkman
robot: | /usr/bin/robot --process-mail
filebox: /dir/file
```

Рабочий образ таблицы строится с помощью команды **newaliases**, а также при актуализации всех изменений посредством команды **systemctl restart postfix**.

При отправке сообщения postfix формирует адрес отправителя автоматически из имени учётной записи пользователя и значения собственного домена (или значения myorigin, если этот параметр выставлен). Даже если почтовый клиент выставил заголовок **From:**, этот адрес попадает в служебные заголовки сообщения и может быть использован получателем, что не всегда желательно. Преобразование адресов отправителей к глобальным адресам можно задать в таблице типа **canonical**:

```
sender_canonical_maps = cdb:/etc/postfix/sender_canonical
```

Аналогичная таблица **recipient_canonical** и соответствующий параметр **recipient_canonical_maps** могут быть использованы для преобразования адресов назначения. Для актуализации изменений таблиц используйте команду **systemctl restart postfix**.

Защита от нежелательной корреспонденции

Противодействие спаму (массовым рассылкам непрошеной корреспонденции) - отдельная большая тема, которую невозможно полностью раскрыть в этом руководстве; здесь даны лишь несколько практических советов применительно к конфигурации postfix. По умолчанию сервер сконфигурирован так, что отвергает попытки переслать сообщения извне на другие удалённые серверы. Со спамом, адресованным локальным получателям, дело обстоит сложнее.

В postfix предусмотрены возможности передачи почтовых сообщений на проверку на спам как внутренним фильтрам, так и внешним программам. Подробности о фильтрации почты см. в *FILTER_README* в документации postfix. Режим фильтрации почты включается в РЕД ОС командой **control postfix filter**.

Один из возможных способов - опираться на данные служб, организованных по принципу «чёрного списка» IP-адресов (MAPS RBL и ей подобные). Чтобы задействовать эти сервисы, предварительно ознакомившись с условиями их использования, занесите имена доменов, работающих по принципу RBL, в конфигурацию:

```
smtpd_client_restrictions = permit_mynetworks, reject_maps_rbl
maps_rbl_domains = relays.ordb.org, blackholes.mail-abuse.org
```

В некоторых случаях требуется адресная работа с отдельными нарушителями почтового этикета. Адресная работа заключается в блокировании SMTP-соединений с их адресов, сетей либо доменов. Для этого предусмотрены таблицы типа access:

```
smtpd_client_restrictions = permit_mynetworks, cdb:/etc/postfix/access
```

Пример таблицы:

```
1.2.3.4 550 No more canned meat, please

1.2.5 REJECT

goodguy.generallybad.com OK

.generallybad.com REJECT
```

Как и с другими таблицами, закончив редактирование, приведите новые настройки в действие командой **systemctl restart postfix**.

Прочие настройки

По умолчанию размер файла почтового ящика при локальной доставке ограничен 51200000 байтами. Это ограничение можно изменить с помощью параметра **mailbox_size_limit**. Установка параметра в 0 снимает ограничение.

Использование Postfix

После того, как postfix настроен и запущен как служба с предсказуемым именем postfix, в настройках почтовых клиентов можно указывать имя или адрес машины (например, localhost) в качестве SMTP-сервера. Для получения почты с удалённых серверов можно использовать программу **fetchmail**, которая работает в связке с postfix, опрашивая внешние почтовые ящики пользователей по протоколам POP3 или IMAP и передавая полученные сообщения системному MTA для локальной доставки. Подробнее о работе с fetchmail см. в документации соответствующего пакета. Файлы журналов postfix находятся в каталоге **/var/log/mail**.

Почтовый клиент Evolution

Установка Evolution
Основные функции

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: evolution-3.50.2

Evolution – свободно распространяемая программа для работы с электронной почтой, управления адресной книгой и функцией планировщика задач. Входит в состав среды рабочего стола **GNOME** в качестве поставляемой по умолчанию почтовой программы.

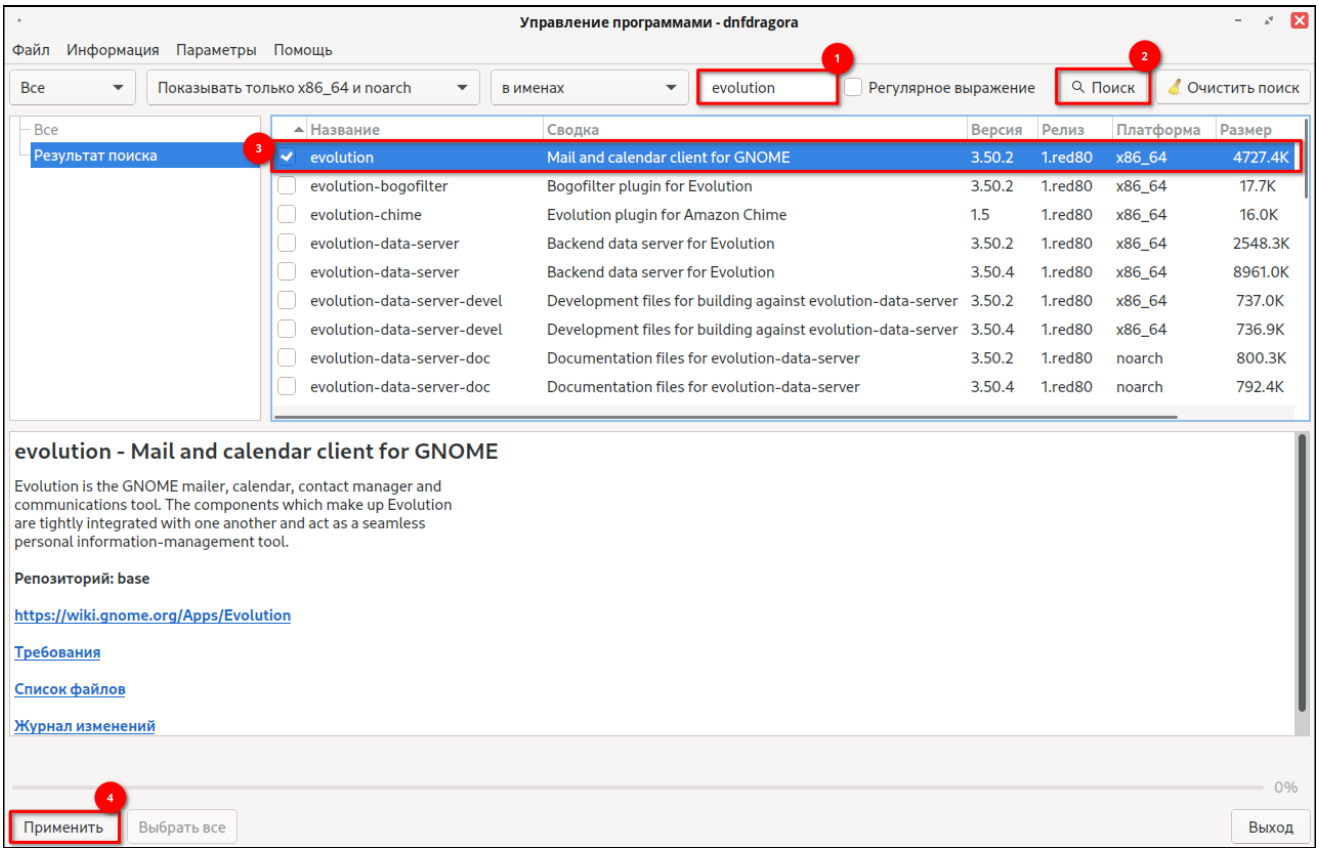
Evolution поддерживает следующие функции и протоколы:

- получение электронной почты по протоколам **POP3** и **IMAP** и её отправка по **SMTP**;
- поддержка расширений протокола **IMAP4** для быстрого обновления содержимого папок **Quick Resync** и уведомлений со стороны сервера **IMAP IDLE**;
- поддержка локальной почты на **UNIX**-системах;
- поддержка защищённых протоколов связи **SSL**, **TLS** и **STARTTLS**;
- шифрование переписки при помощи **GPG** и **S/MIME**;
- использование библиотеки **NSS** для управления сертификатами, что позволяет использовать общее хранилище между совместимыми программами, например, **Mozilla Firefox**, **Mozilla Thunderbird**, **LibreOffice** и пр;
- поиск по почтовым папкам и сортировка почты по критериям;
- автоматическая фильтрация спама с использованием **SpamAssassin** и **Bogofilter**;
- возможность работы с серверами **Microsoft Exchange Server**, **Novell GroupWise** и **Kolab**;
- календарь с поддержкой формата файлов **iCalendar** и протоколов **WebDAV**, **CalDAV** и возможностью подключения к **Google Calendar**;
- адресная книга с поддержкой локальных контактов, протоколов **CardDAV**, **LDAP** и контактов **Google**;
- интеграция адресной книги с **LibreOffice**;
- поддержка аватаров пользователей из адресной книги, из заголовков **X-Face**, **Face** и автоматический поиск их по хешу адреса электронной почты на сервисе **Gravatar**;
- поддержка расширений для чтения лент новостей **RSS**, синхронизации с мобильными устройствами и **VoIP** приложением **Ekiga**;
- импорт почты из архивов **Microsoft Outlook** (файлы с расширениями **.dbx**, **.pst**) и **Berkley Mailbox**.

Установка Evolution

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Evolution** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**evolution**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

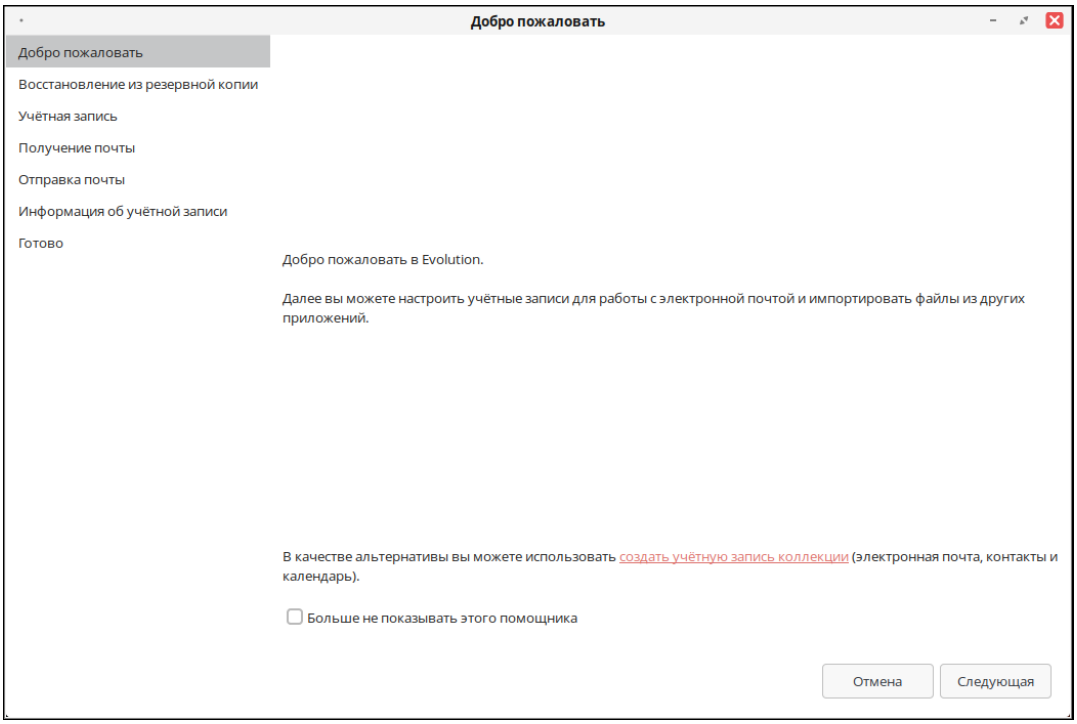
```
dnf install evolution
```

После установки **Evolution** будет доступен из «**Главного меню**» – «**Офис**» – «**Evolution**».

При первом запуске почтового клиента будет выведено окно с настройкой основных функций для работы программы. Здесь вы можете создать новую учетную запись или импортировать файлы из уже существующей, задать параметры почтового сервера, настроить параметры получения и отправки почты.

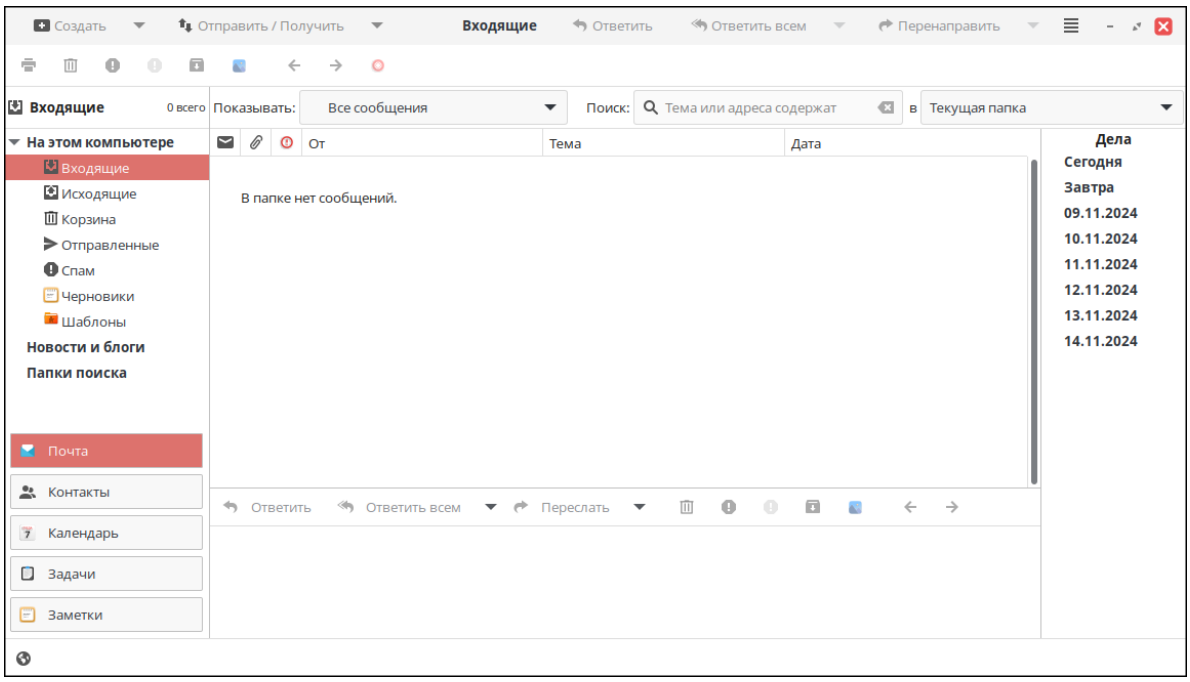
На шаге «**Информация об учетной записи**» необходимо проверить правильность введенных данных и указанных параметров почтового сервера. Если все настроено верно, перейдите к шагу «**Готово**» и начните пользоваться почтовым клиентом.

В противном случае нажмите «**Назад**» и внесите необходимые изменения в настройки клиента.

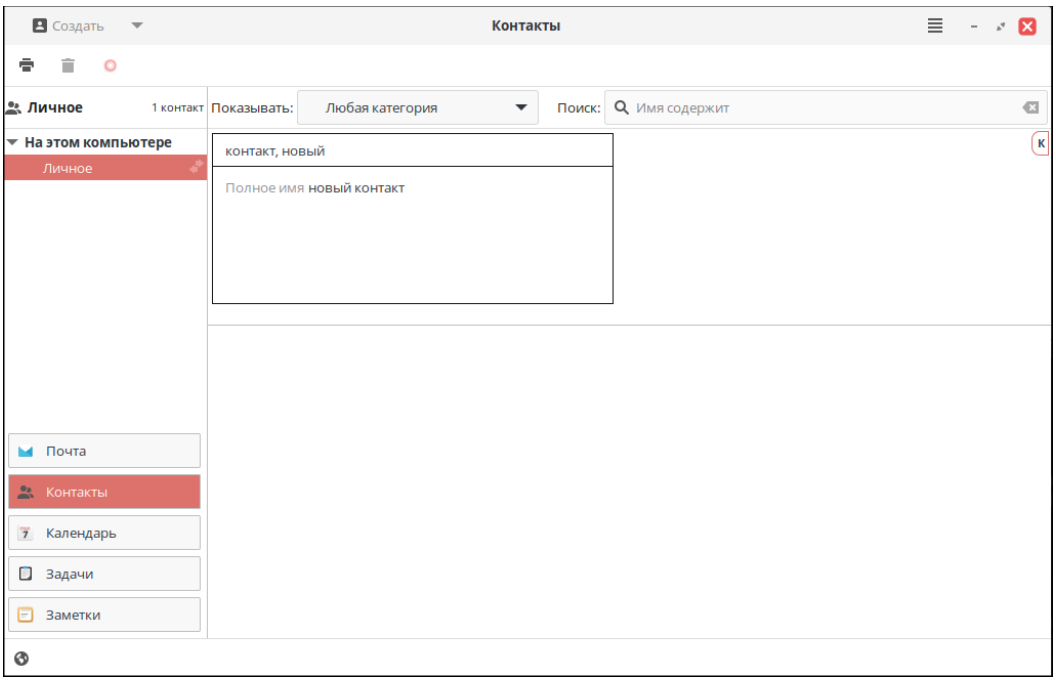


Основные функции

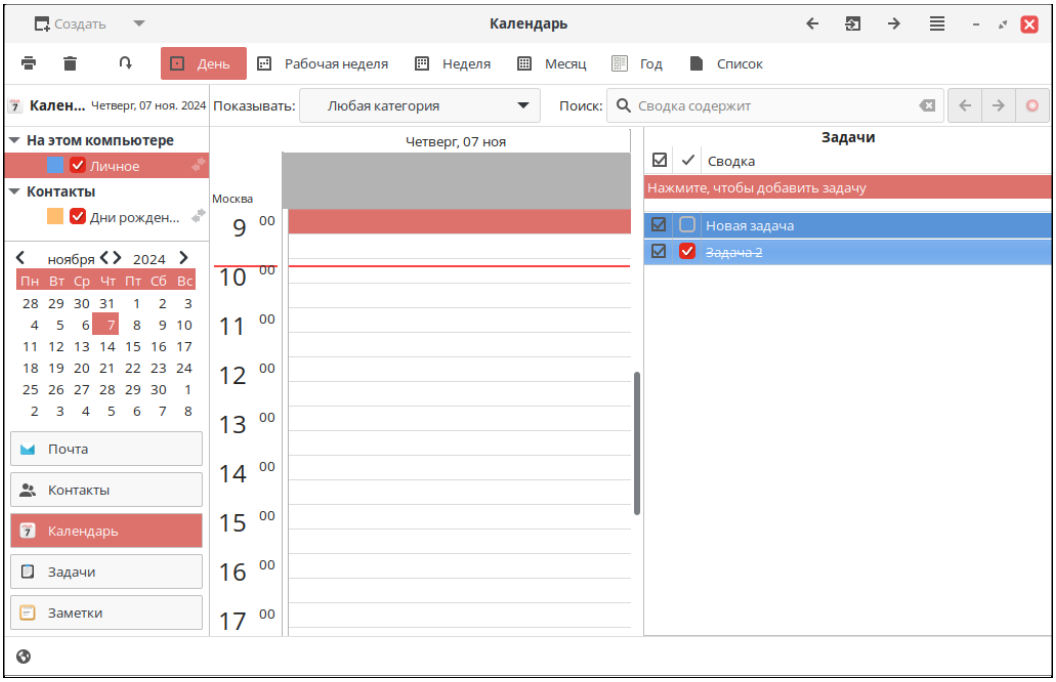
В **Evolution** реализованы стандартные функции почтового клиента – работа непосредственно с электронный почтой.



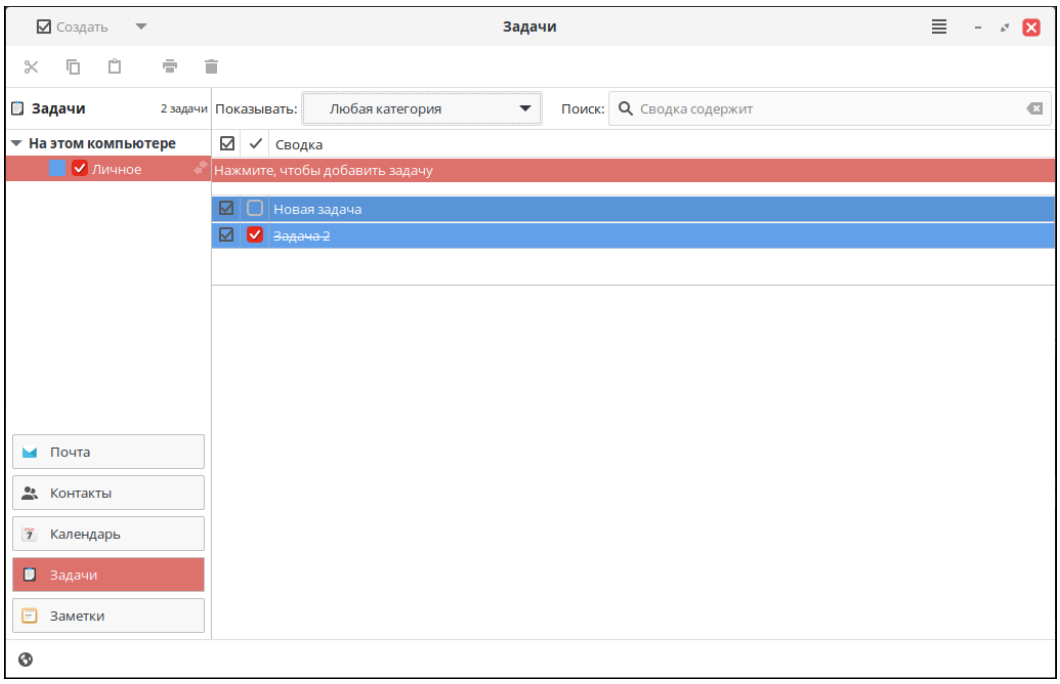
Отдельная вкладка для работы с контактами – добавьте новые контакты.



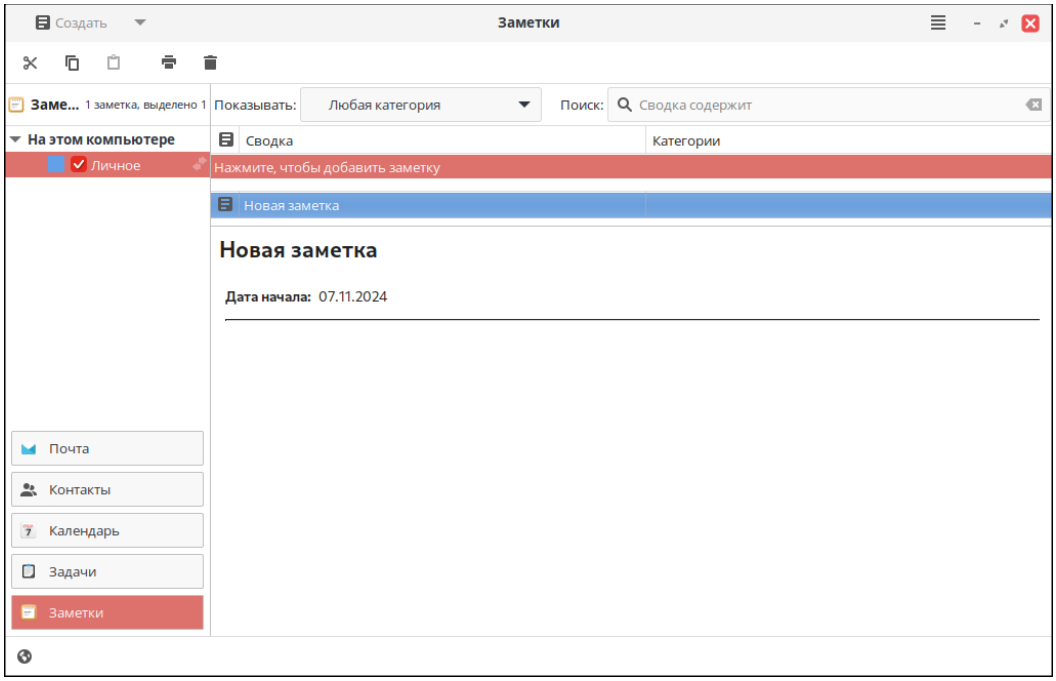
Календарь, в котором можно добавлять мероприятия на определенный день, настраивать оповещение о предстоящем мероприятии или событии.



Вкладка «**Задачи**» – возможность создавать задачи, устанавливать сроки их выполнения, приоритет и текущее состояние.



Также доступно ведение заметок.



Почтовый клиент Thunderbird

Установка
Основные возможности программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: thunderbird-102.15.0-1

Mozilla Thunderbird — это бесплатное приложение для работы с электронной почтой, разработанное командой *Mozilla Foundation*. Это один из самых популярных почтовых клиентов, который предоставляет широкие возможности для организации и управления электронной почтой.

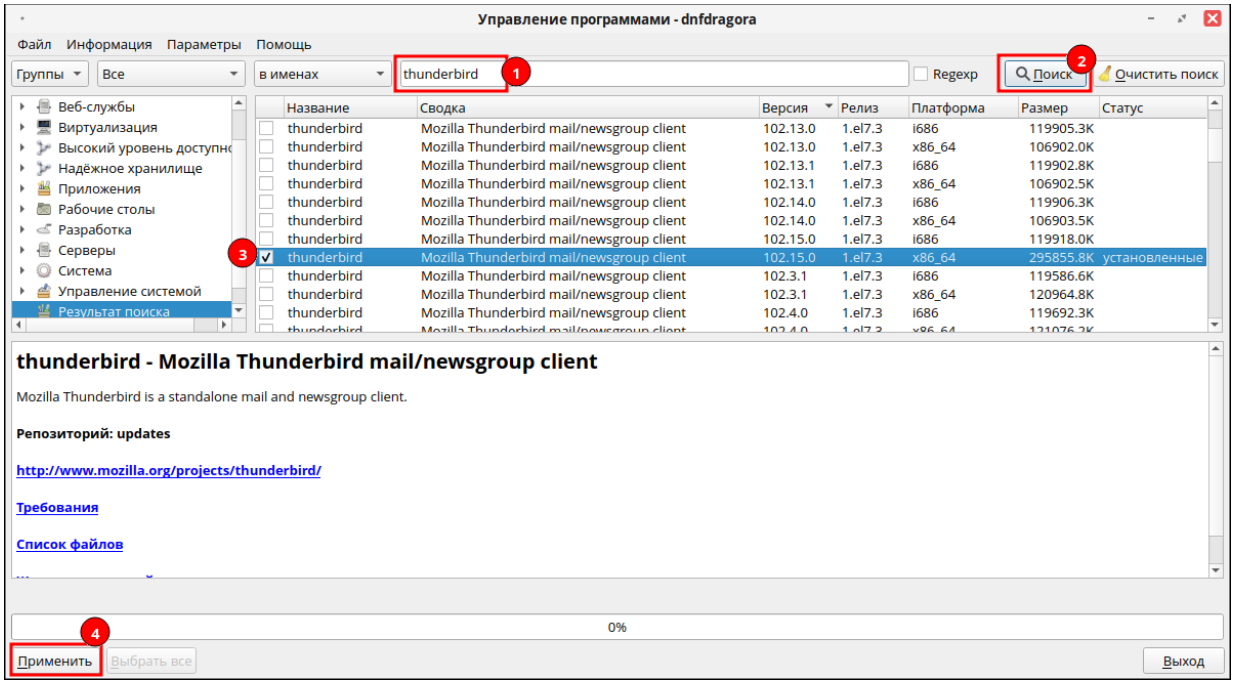
Thunderbird позволяет гибко настраивать учетную запись электронной почты, устанавливать и настраивать различные фильтры и правила, создавать папки для организации писем, устанавливать шаблоны и многое другое. Все письма и контакты хранятся локально на компьютере, обеспечивая безопасность и конфиденциальность данных.

Поддерживаются популярные почтовые протоколы, включая **POP3**, **IMAP** и **SMTP**. Есть возможность подключать почтовые ящики от разных провайдеров с автоматическим обнаружением настроек и управлять ими из одного интерфейса.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки **Thunderbird** через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**thunderbird**», выберите его и нажмите «**Применить**».



Для установки программы через терминал перейдите в сеанс пользователя **root**:

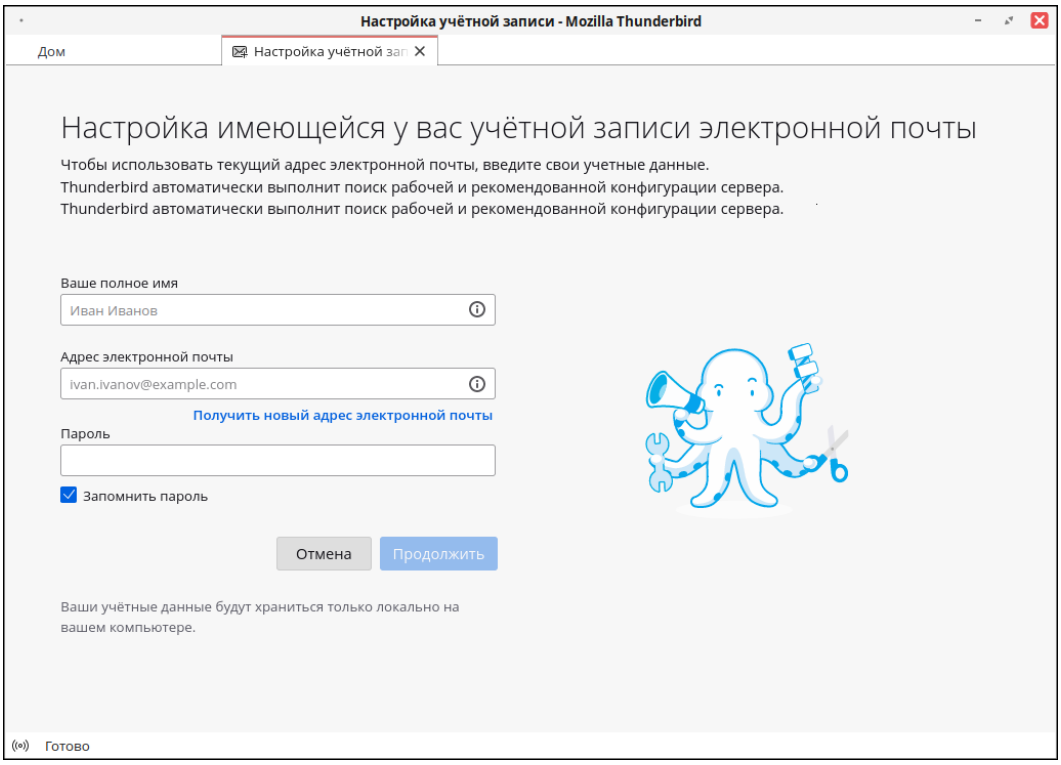
```
su -
```

и выполните команду:

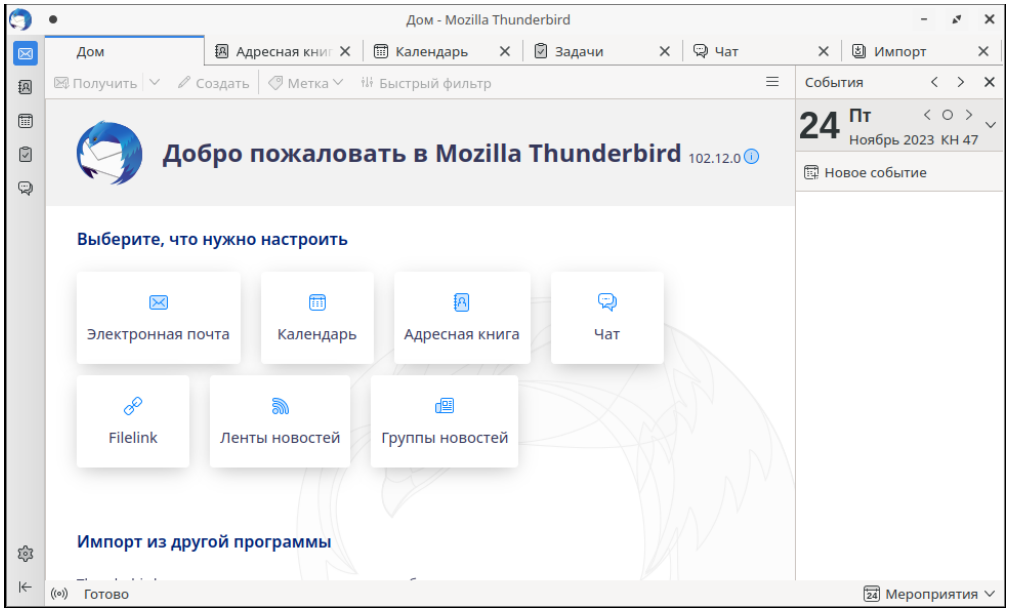
```
dnf install thunderbird
```

После установки **Thunderbird** будет доступен из «**Главного меню**» — «**Интернет**» — «**Почтовый клиент Thunderbird**».

При первом запуске почтового клиента будет предложено ввести данные существующей учетной записи для автоматического определения настроек сервера.

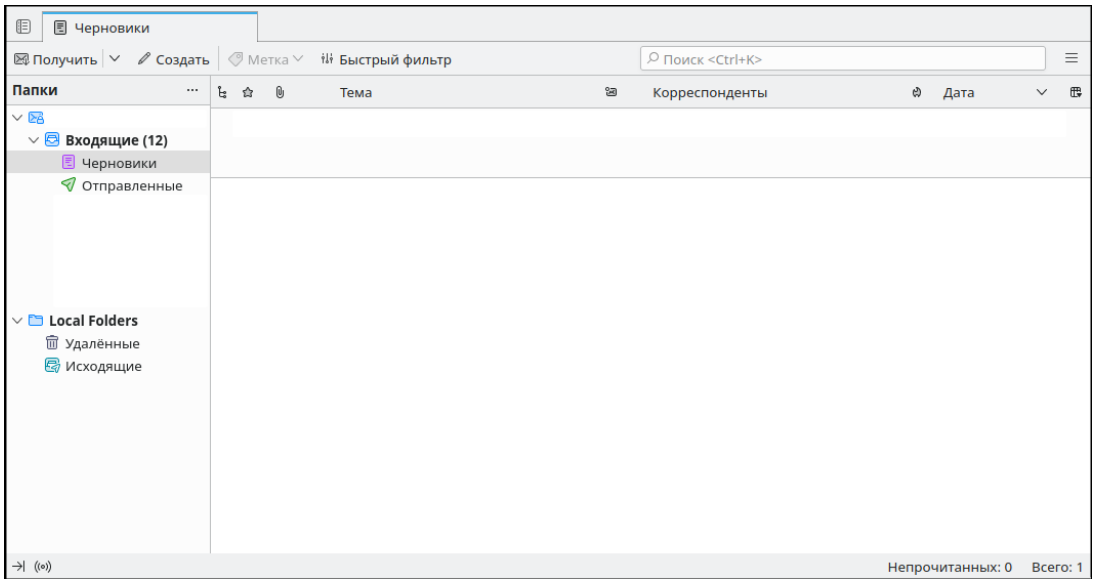


После входа в учетную запись будет открыта домашняя страница почтового клиента, где можно выбрать, что нужно настроить.



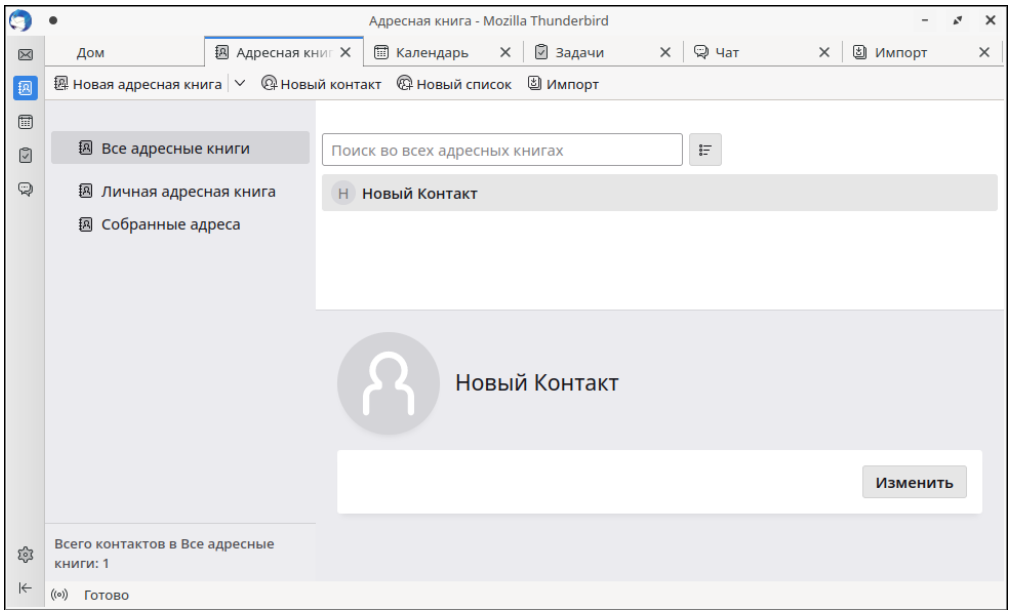
Основные возможности программы

Thunderbird имеет стандартный набор функций почтового клиента, основная из которых — работа с электронной почтой. Thunderbird умеет сохранять письма и вложения локально на компьютере, что обеспечивает доступ к ним даже без интернета. Кроме того, встроенный поиск позволяет быстро находить нужные сообщения.

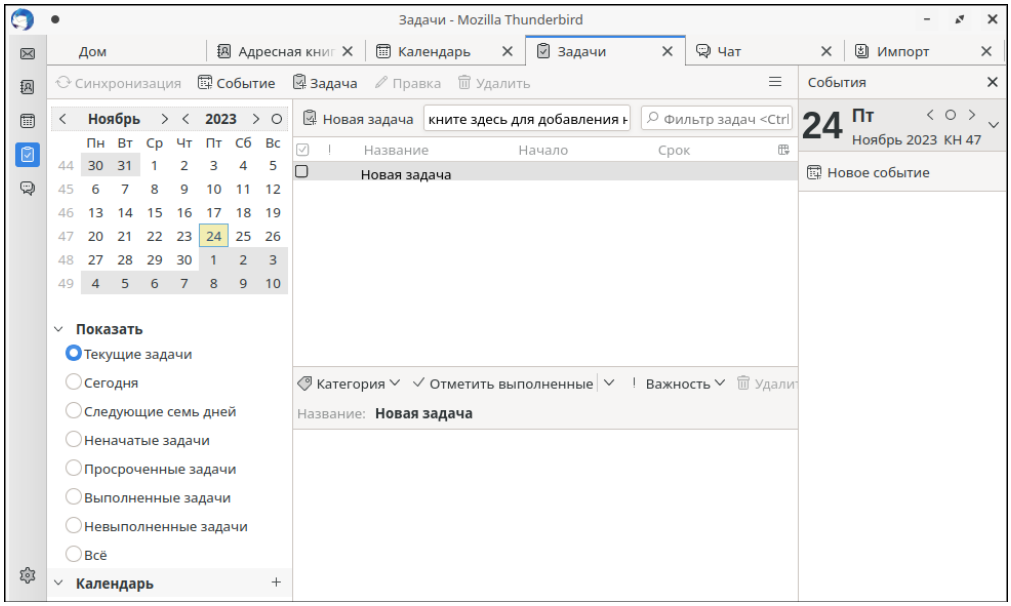


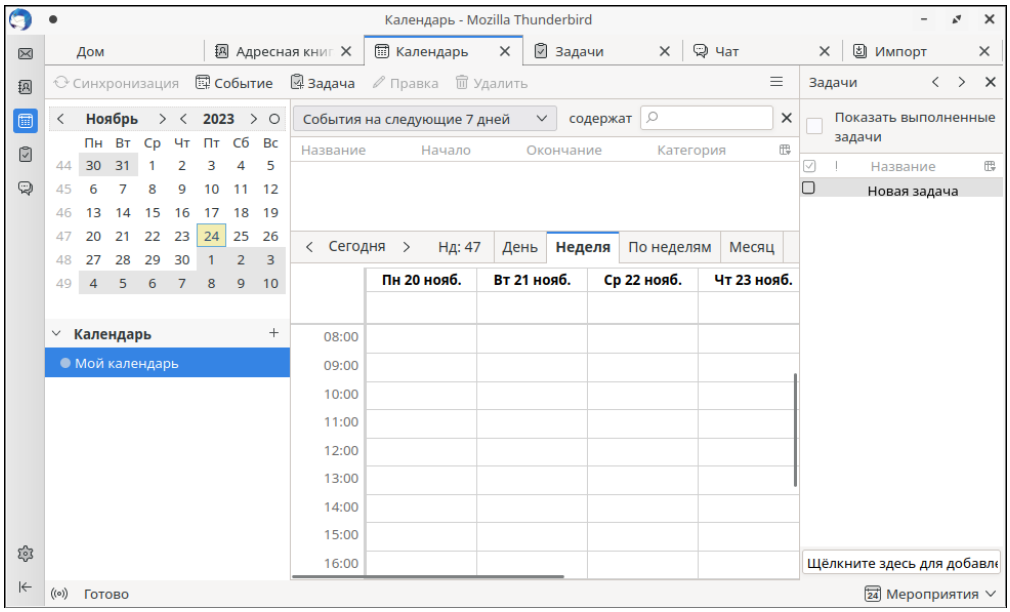
Thunderbird включает встроенные инструменты для борьбы со спамом и обнаружения вредоносных программ. Он также поддерживает шифрование и аутентификацию, чтобы обеспечить безопасность электронных писем.

Также доступна возможность работы с адресной книгой.

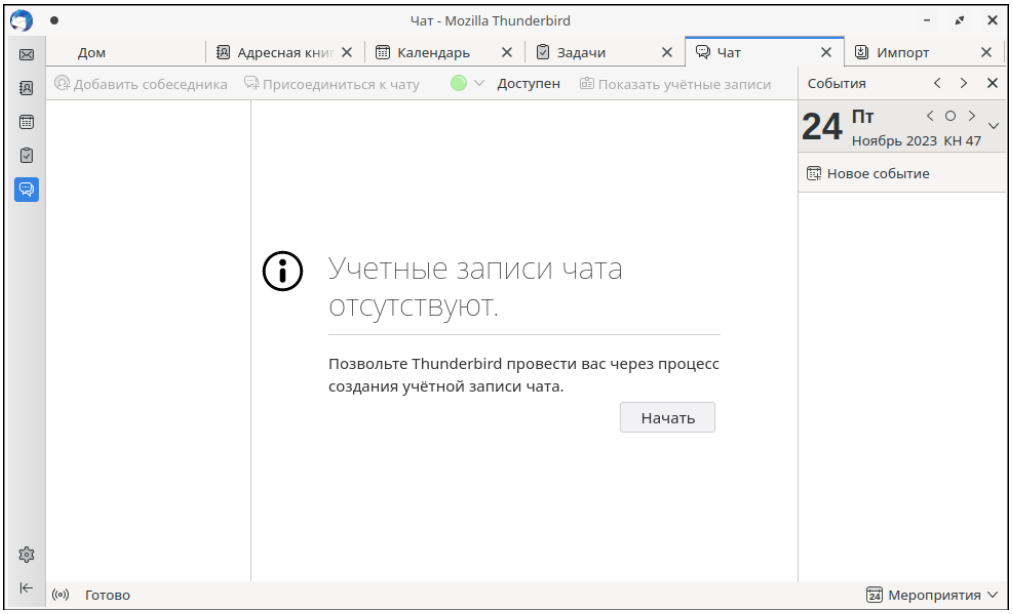


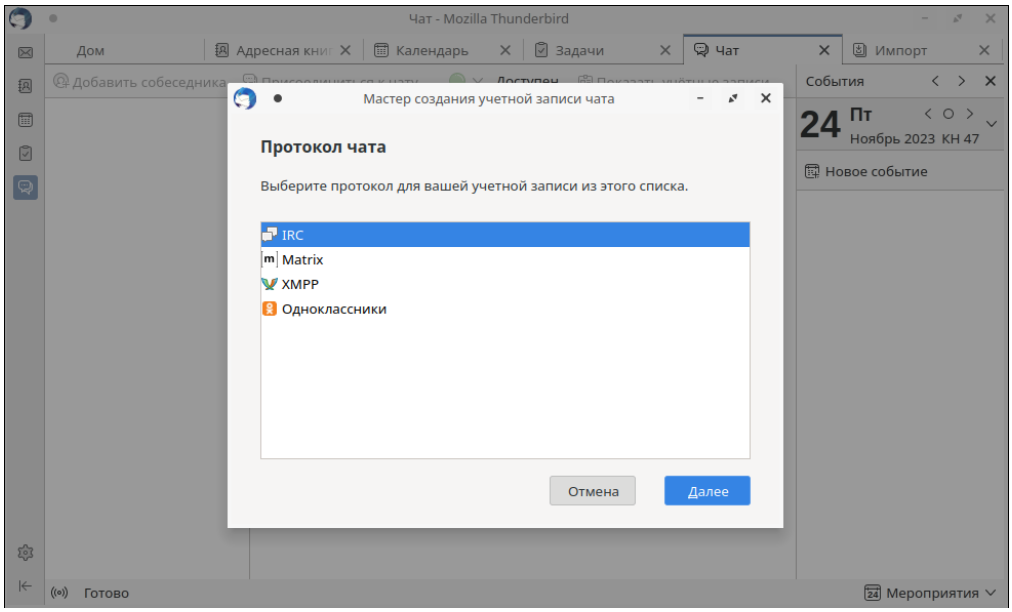
Присутствуют функции календаря, совмещенного с задачами, что позволяет управлять своим временем и не пропускать важные события.





Имеется возможность подключения учетной записи для чата, для выбора доступны такие протоколы, как **IRC**, **Matrix**, **XMPP**, **Одноклассники**.

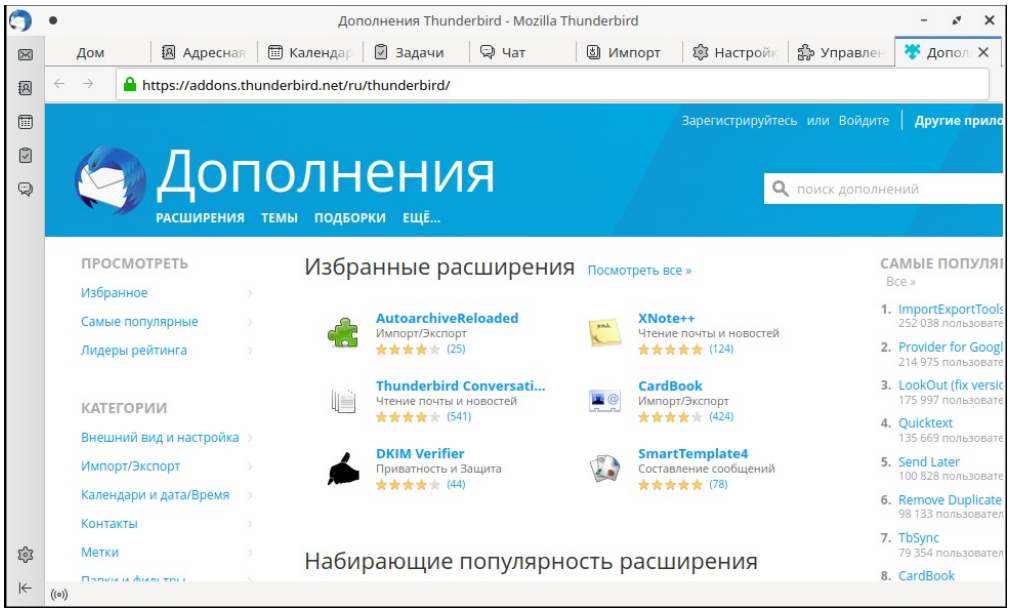




Thunderbird поддерживает подписку на новостные рассылки и чтение **RSS**-каналов, позволяя получать свежие новости и информацию из интересующих источников.

Главным достоинством **Thunderbird** можно назвать возможность установки различных дополнений, тем оформления, расширений. Это

позволяет гибко настраивать внешний вид почтового клиента под свой вкус, а также расширять функционал и возможности программы.



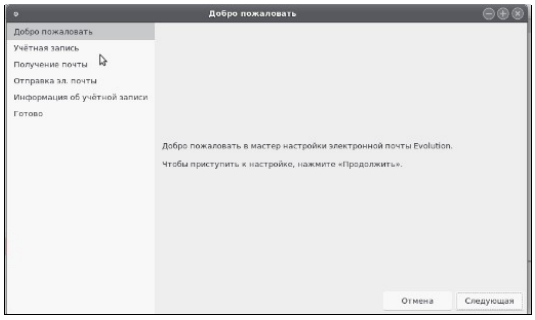
Настройка в Evolution подключения к MS Exchange

У вас должен быть установлен плагин для работы **EWS**. Установить его можно командой:

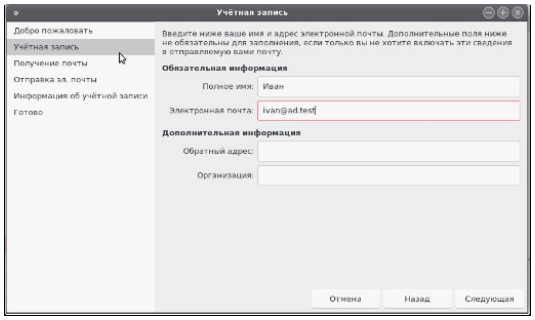
```
dnf install evolution-ews
```

Перейдите в меню «Файл > Создать > Учетная запись почты».

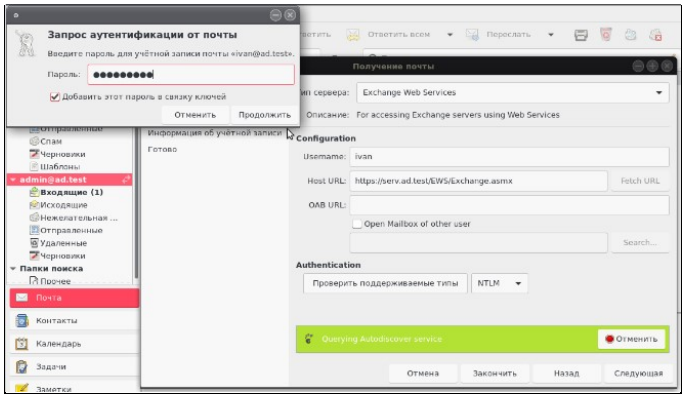
Откроется окно. Нажмите кнопку «Следующая».



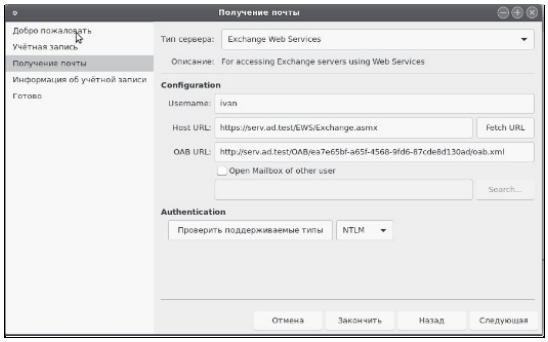
Введите имя и адрес электронной почты пользователя и нажмите кнопку «Следующая».



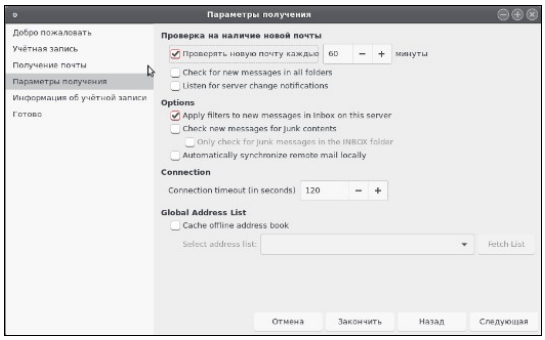
Выберете тип сервера Exchange Web Services. Введите правильный адрес к EWS и нажмите кнопку «Fetch URL».
Если все сделано правильно, откроется окно ввода пароля пользователя. Введите пароль и нажмите кнопку «Продолжить».



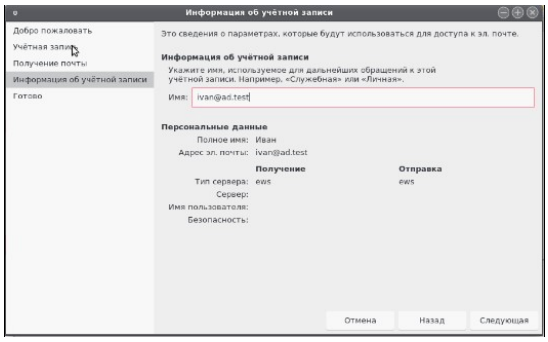
Если пароль введен верно, сервер вернет OAB URL, он отобразится в соответствующем окне. Нажмите кнопку «Следующая».



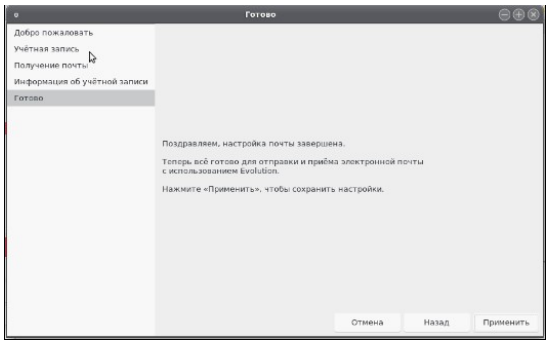
В следующем окне настройте параметры получения или оставьте их по умолчанию. Нажмите кнопку «Следующая».



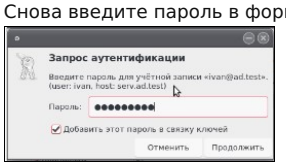
Укажите имя учетной записи для обращений или оставьте значение по умолчанию. Нажмите кнопку «Следующая».



Нажмите кнопку «Применить».



Снова введите пароль в форме ввода пароля.



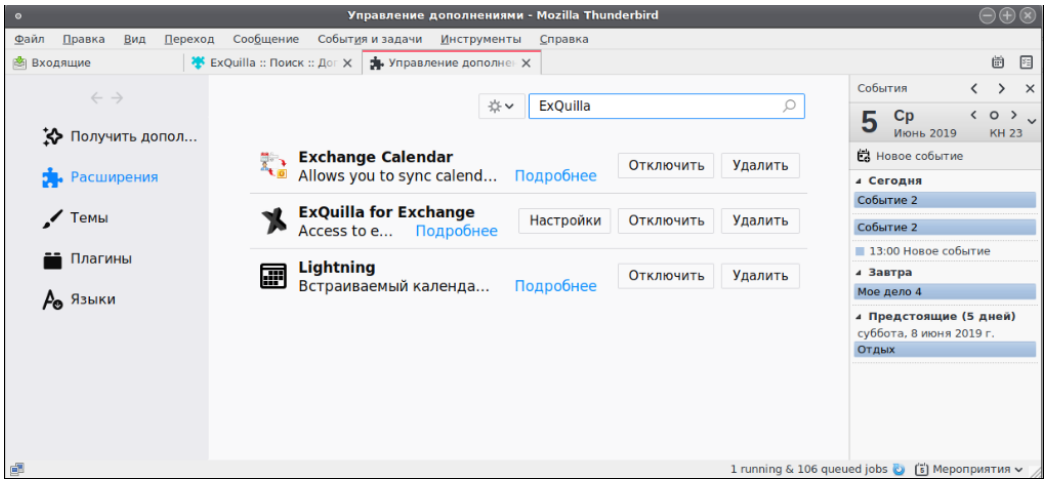
На этом почта подключена. Также автоматически подключен календарь, задачи, заметки. Есть возможность просмотра адресных книг.

Настройка календаря Exchange в Thunderbird

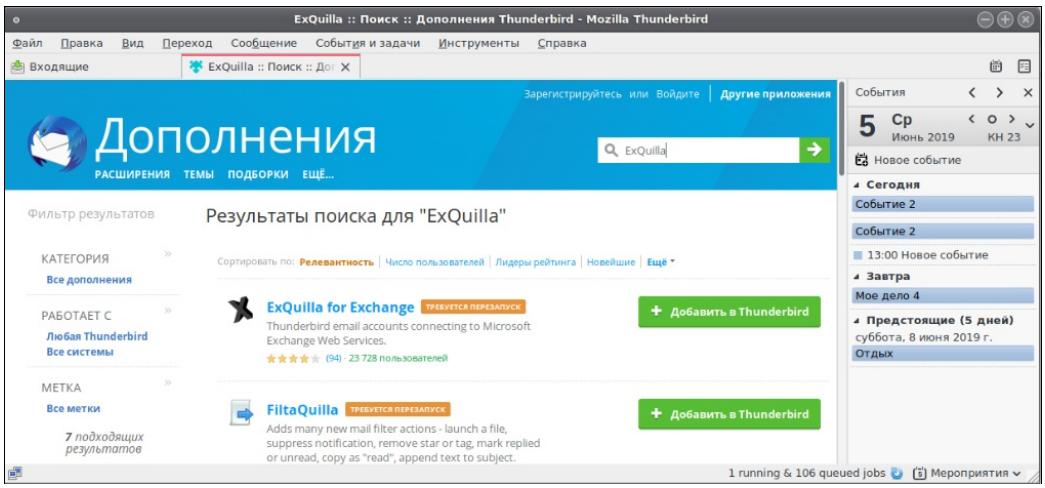
Настройка почты

Для подключения почты Exchange к Thunderbird скачайте и установите плагин ExQuilla for Exchange.

Для этого в меню нажмите Инструменты > Дополнения. В открывшемся окне выберите Расширения и в верхнем правом углу в строку поиска введите "ExQuilla".



В списке найденного нажмите кнопку "Добавить в Thunderbird" напротив плагина ExQuilla for Exchange. После установки перезагрузите почтовый клиент.

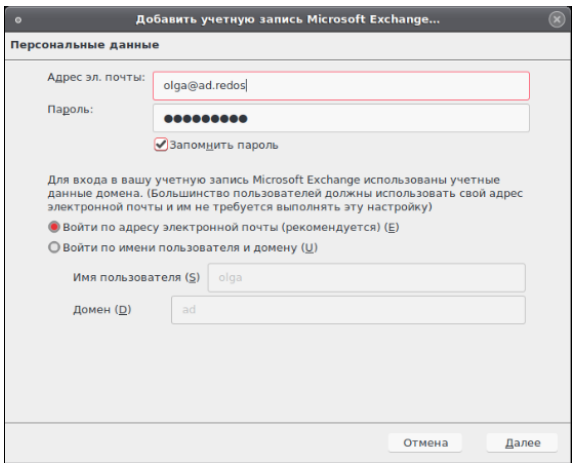


ВАЖНО

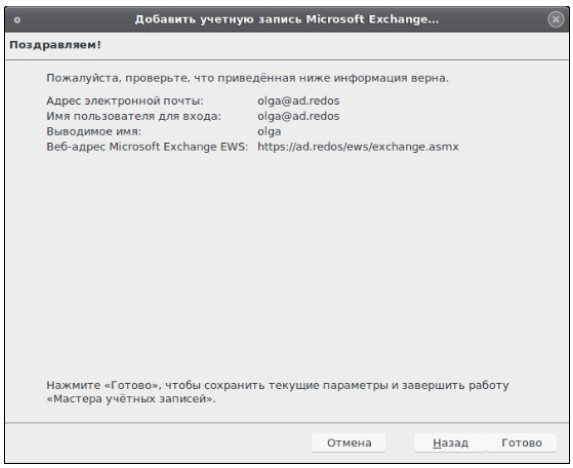
У вас должен быть установлен плагин Lighting

Далее подключите календарь. Выберите меню "Файл" > "Создать" > "Добавить учетную запись Microsoft Exchange".

В открывшемся окне введите адрес эл. почты, пароль и нажмите кнопку "Далее"

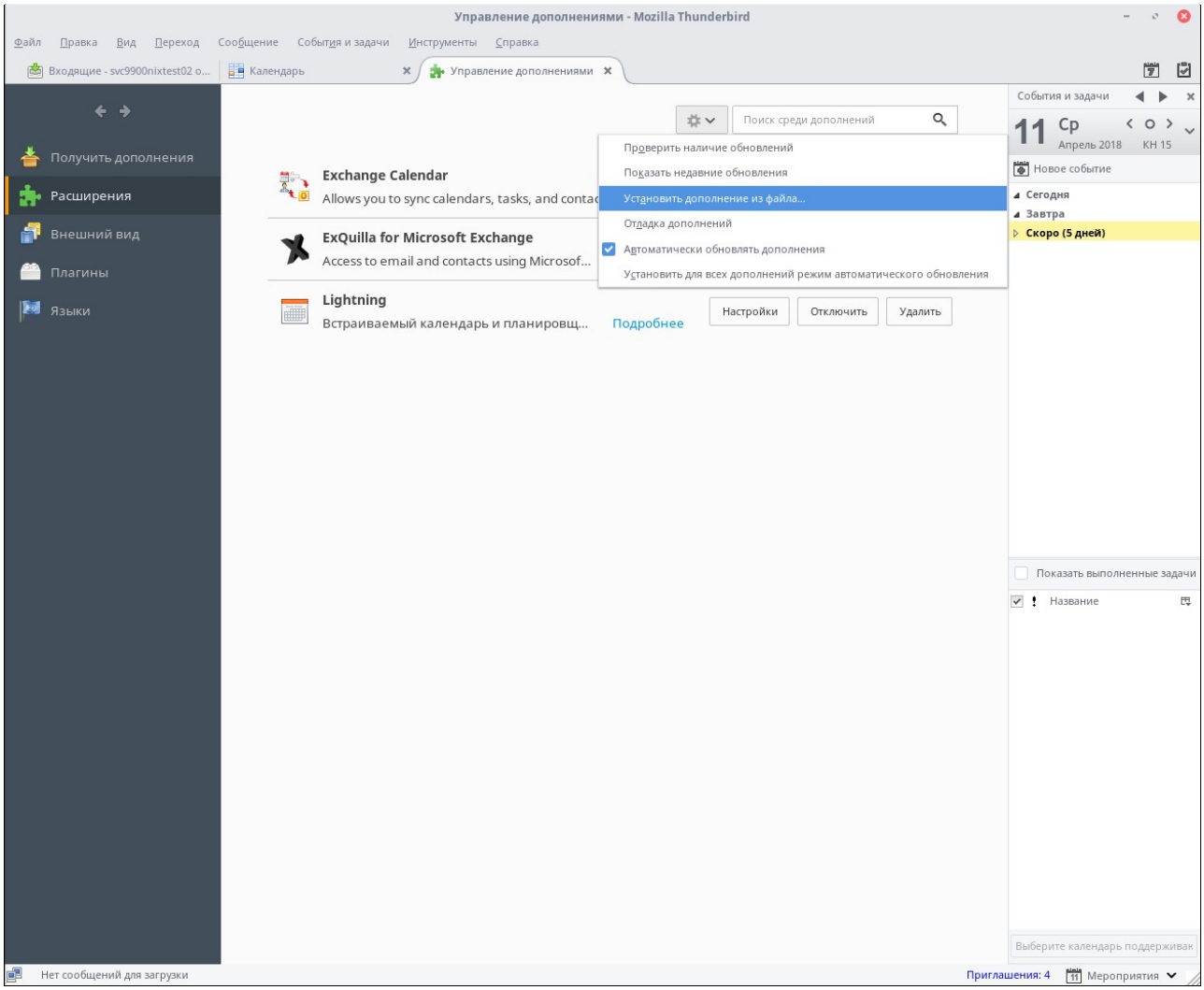


Должен автоматически определится адрес почтового сервера и появиться окно с успешным подключением. Остается только нажать кнопку "Готово".



Настройка календаря

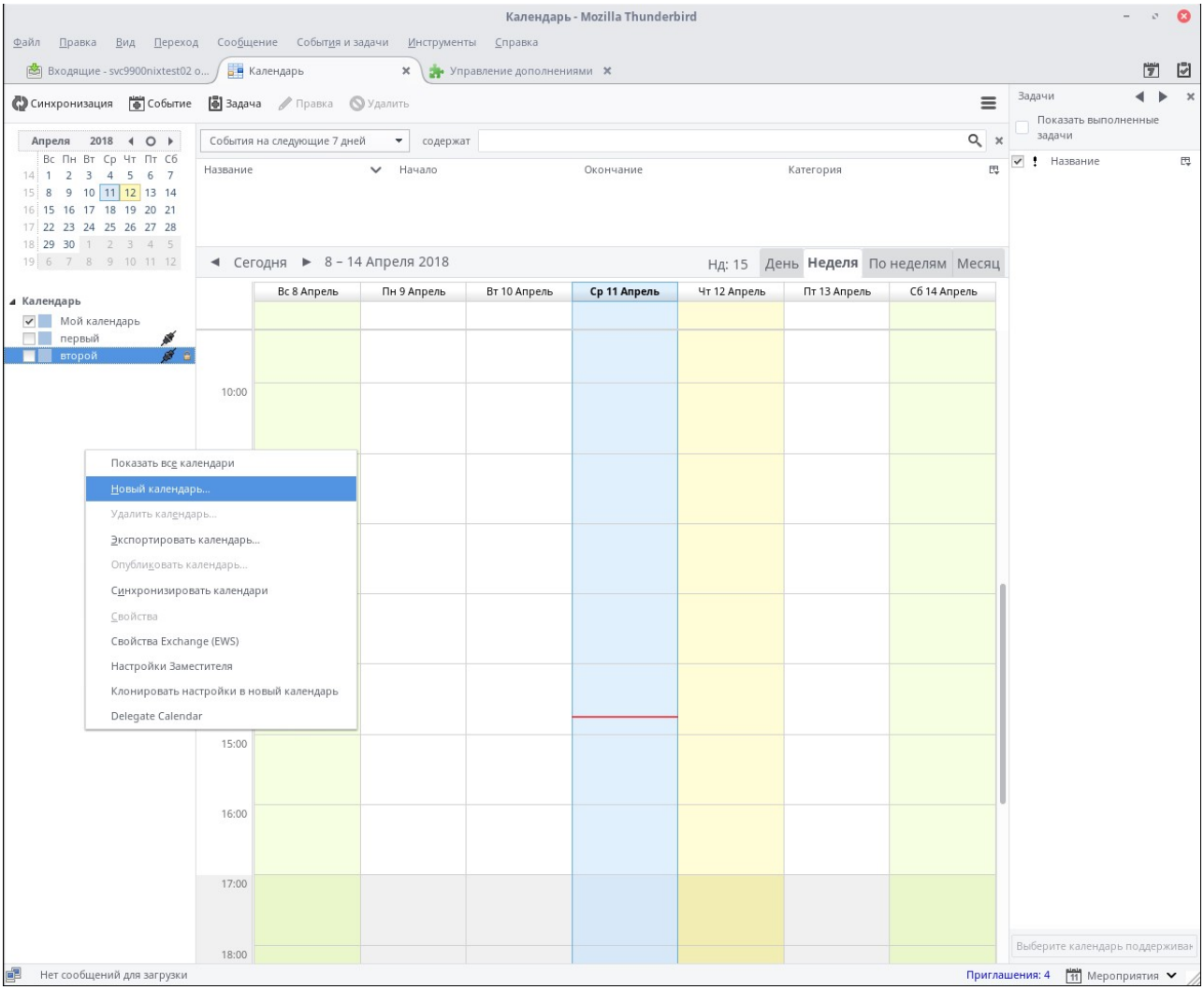
1. Скачайте дополнение ExchangeCalendar по ссылке:
https://github.com/ExchangeCalendar/exchangecalendar/releases
Откройте Thunderbird перейдите в меню и выберите пункт “Дополнения”.
Перейдите на вкладку “Расширения” и нажмите на шестеренку, затем выберите пункт “Установить дополнение из файла”.



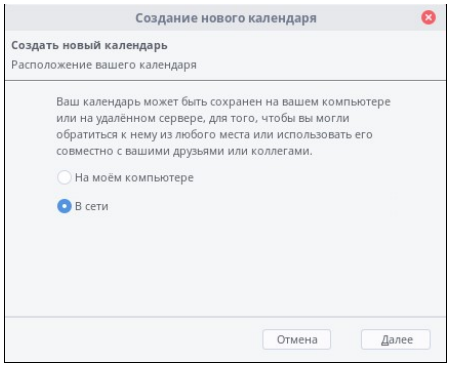
Выберите скачанный файл дополнения и нажмите “Ок”. Затем установите его и перезагрузите почтовый клиент.

2. Добавьте календарь.

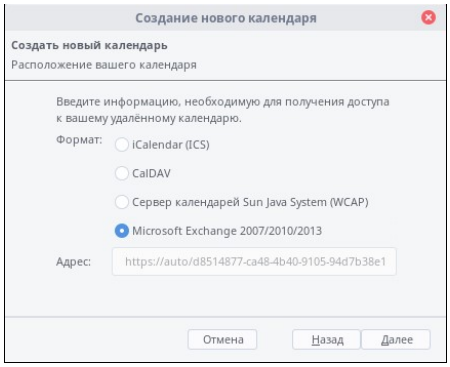
Откройте Thunderbird перейдите на вкладку “Календарь”.
В списке календарей нажмите на правую кнопку мыши и выберете “Новый календарь”.



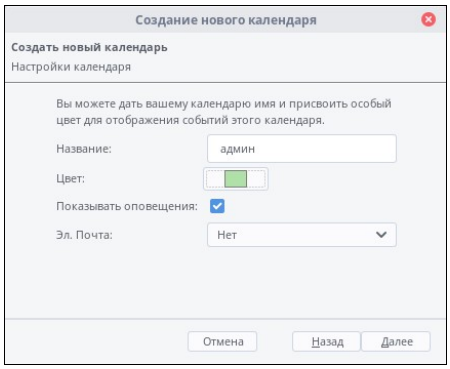
В открывшемся окне выберете “В сети” и нажмите кнопку “Далее”.



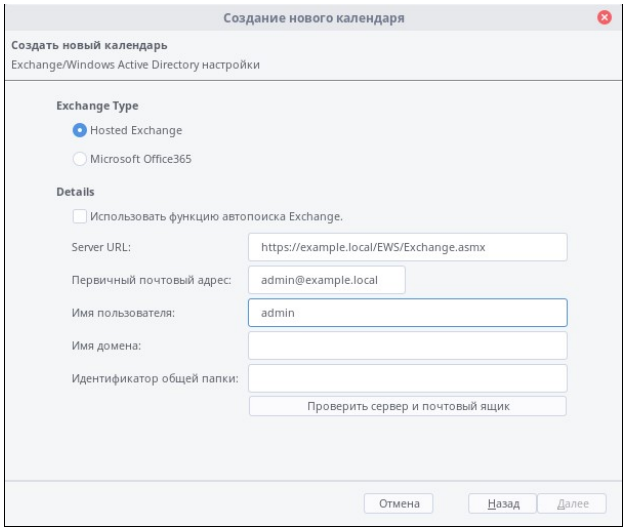
Выберите пункт “Microsoft Exchange 2007/2010/2013” и нажмите кнопку “Далее”.



Введите название календаря, выберите цвет, при выборе электронной почты укажите её или выберите “Нет” и нажмите кнопку “Далее”.



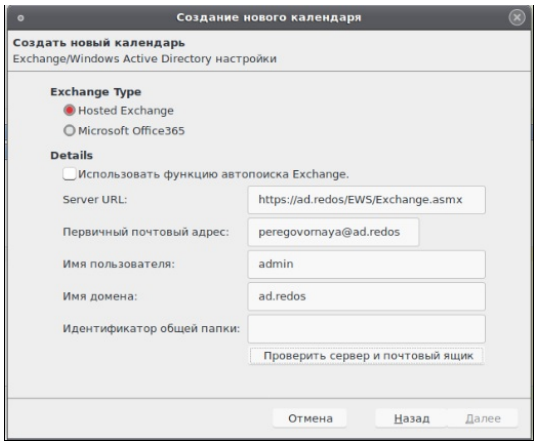
Выберите “Hosted Exchange”, введите Server URL. Обычно, адрес следующий https://<имя почтового сервера>/EWS/Exchange.asmx. Введите первичный почтовый адрес и имя пользователя, затем нажмите кнопку “Проверить сервер и аккаунт”.



В открывшемся окне введите пароль от аккаунта. Окно может появляться несколько раз.
Теперь нажмите кнопку “Далее” и “Готово”.
Календарь подключен.

Подключение общего календаря помещений или оборудования

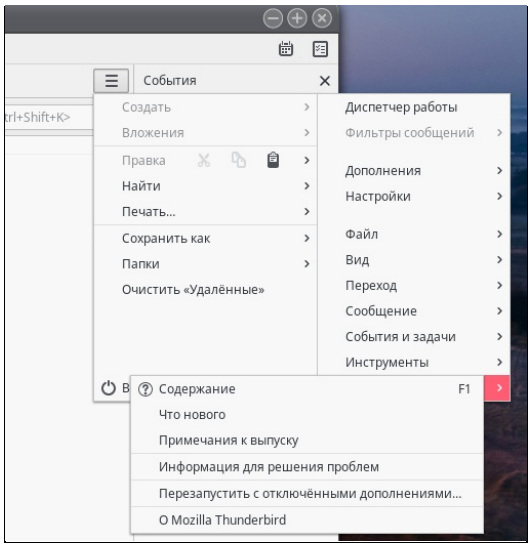
Для подключения любого общего календаря нужно при его подключении вписать в поле "Первичный почтовый адрес" адрес этого календаря. Пример на скриншоте ниже.

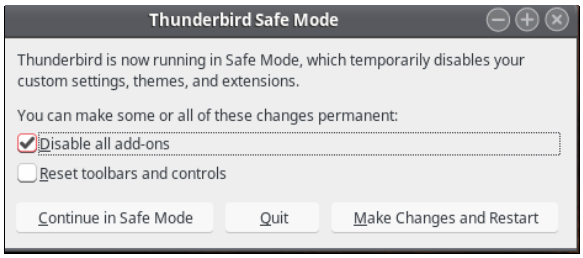


Thunderbird запуск Google-почты

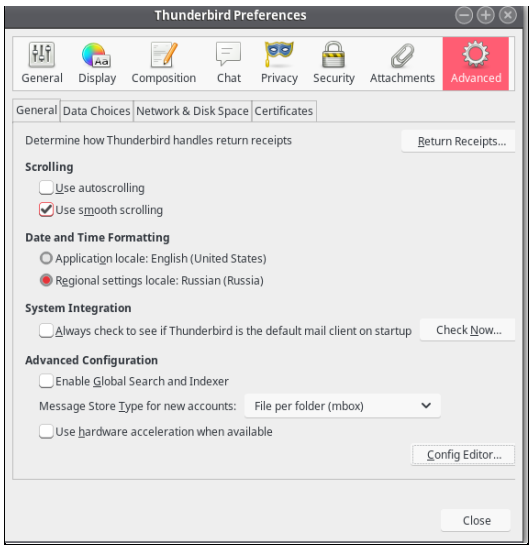
Настройка добавления Google аккаунта в ThunderBird при возникновении проблемы при авторизации с использованием OAuth2:

Включите Безопасный Режим Thunderbird для этого зайдите в Справку-> Перезапустить с отключенными дополнениями -> Disable all add-ons -> Continue in safe mode



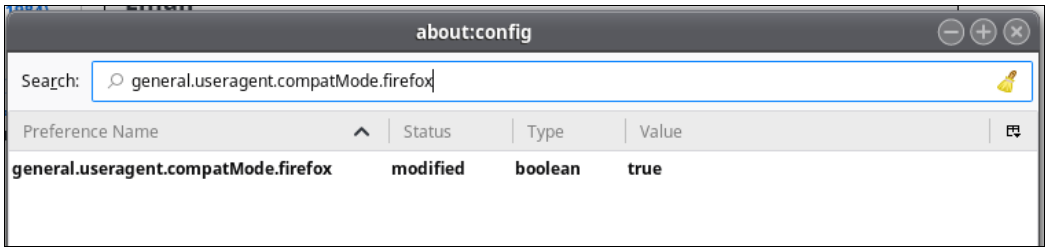


После запуска в безопасном режиме откройте Thunderbird Preferences -> Advanced -> General -> Config Editor -> согласитесь с уведомлением, откроется список доступных конфигураций



Воспользуйтесь поиском **general.useragent.compatMode.firefox** и измените значение на true.

Если параметр отсутствует, добавьте его с меткой boolean, значение true.



Выйдите из безопасного режима и попробуйте ввести данные Google аккаунта.

Настройка NextCloud с СУБД MySQL и ПО для веб-сервера Apache

Установка необходимых пакетов
Настройка SELinux
Настройка MySQL
Установка NextCloud
Настройка NextCloud

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** nextcloud-27.1.10-1, php-8.1.29-1, mariadb-3:10.11.6-2

Nextcloud — набор клиент-серверных программ для создания и использования облачного хранилища. *Nextcloud* можно установить как на хосте, так и на собственном сервере. По доступной функциональности похож на *Dropbox*.

В отличие от проприетарных сервисов, таких как *Dropbox*, открытая архитектура *Nextcloud* позволяет добавлять функциональность на сервер в виде приложений и дает возможность пользователям полностью контролировать свои данные.

Nextcloud позволяет совместно работать с офисными документами, файлами и информацией для планирования задач и мероприятий. Платформа также включает надстройки для доступа к электронной почте, обмена сообщениями, организации видеоконференций и чатов.

Аутентификация пользователей может производиться как по локальной базе, так и через интеграцию с *LDAP/Active Directory, Kerberos, IMAP*, в том числе с применением двухфакторной аутентификации, *SSO* (Single-sign-on) и привязки новых систем к учётной записи по QR-коду. Версионный контроль изменений позволяет отслеживать изменения в файлах, комментариях, правилах совместного доступа и тегах.

Также облачное хранилище поддерживает синхронизацию и обмен данными, предоставляет возможность просмотра и редактирования данных с любого устройства в любой точке сети. Доступ к данным может быть организован как при помощи web-интерфейса, так и с использованием протокола **WebDAV** и его расширений **CardDAV** и **CalDAV**.

Сервер *Nextcloud* можно развернуть на любом хостинге, поддерживающем выполнение PHP-скриптов и предоставляющем доступ к *SQLite, MariaDB/MySQL* или *PostgreSQL*.

Основные компоненты платформы Nextcloud:

1. **Files** - организация хранения, синхронизации, совместного доступа и обмена файлами. Доступ может быть осуществлён как через *Web*, так и при помощи клиентского ПО для настольных и мобильных систем. Предоставляются такие расширенные возможности, как полнотекстовый поиск, прикрепление файлов при отправке комментариев, выборочный контроль доступа, создание защищённых паролем ссылок для загрузки, интеграция с внешними хранилищами (*FTP, CIFS/SMB, SharePoint, NFS, Google Drive, Dropbox* и т.п.).
2. **Flow** - оптимизирует бизнес-процессы через автоматизацию выполнения типовых работ, таких как преобразование документов в PDF, отправка сообщений в чаты при загрузке новых файлов в определённые каталоги, автоматическое назначение тегов. Возможно создание собственных обработчиков, выполняющих действия в привязке к определённым событиям.
3. **Встроенные средства** совместного редактирования документов, электронных таблиц и презентаций на базе пакета *ONLYOFFICE*. Обеспечена полная интеграция *ONLYOFFICE* с остальными компонентами платформы, например, несколько участников могут одновременно редактировать один документ, параллельно обсуждая изменения в видеочате и оставляя заметки.
4. **Photos** - галерея изображений, упрощающая поиск, обмен и навигацию по совместной коллекции фотографий и изображений. Поддерживается ранжирование фотографий по времени, месту, тегам и частоте просмотра.
5. **Calendar** - календарь-планировщик, позволяющий координировать проведение встреч, планировать чаты и видеоконференции. Поддерживается загрузка событий с внешних ресурсов, поддерживающих протокол *WebCal*.
6. **Mail** - совместная адресная книга и web-интерфейс для работы с электронной почтой. Возможна привязка нескольких учётных записей к одному *inbox*. Поддерживается шифрование писем и прикрепление цифровых подписей на базе *OpenPGP*. Возможна синхронизация адресной книги при помощи *CalDAV*.
7. **Talk** - система обмена сообщениями и проведения web-конференций (чат, аудио и видео). Имеется возможность предоставления доступа к содержимому экрана и поддержка SIP-шлюзов для интеграции с обычной телефонией.

Установка необходимых пакетов

Необходимо подготовить систему для установки **NextCloud**, для этого установите следующие пакеты (потребуются права **администратора** системы):

```
sudo dnf install httpd php php-dom php-mbstring php-gd php-pdo php-json php-xml php-zip php-curl php-mcrypt php-pear setroubleshoot-server bzip2 php-ldap php-mysqlnd mariadb mariadb-server mod_auth_kerb php-fpm
```

Настройка SELinux

Настройте **SELinux**:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_graceful_shutdown 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P domain_can_mmap_files 1
setsebool -P daemons_dump_core 1
```

Настройка MySQL

В качестве базы данных используется **MySQl**.

Запустите и добавьте в автозагрузку службу **mariadb**:

```
sudo systemctl start mariadb && systemctl enable mariadb
```

Выполните скрипт **mysql_secure_installation**, чтобы защитить базу данных от злоумышленников:

```
sudo mysql_secure_installation
```

На первом шаге должен быть задан пароль **root**, по умолчанию пароль не задан, нажмите **Enter**.

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none): <нажмите_Enter>
OK, successfully used password, moving on...
```

Далее укажите свой пароль **root** и удалите анонимных пользователей:

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

Sett root password? [Y/n] y
New password: <задайте_пароль_root>
Re-enter new password: <повторите_пароль_root>
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!
```

Запретите удаленный вход для **root**, если необходимо:

```
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
```

Удалите тестовую базу данных и обновите таблицу привилегий:

```
By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
```

```
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Затем создайте базу данных и пользователя, которые будут использованы для дальнейшей работы.

Для подключения к базе используйте команду **mysql**:

```
mysql -u root -p

CREATE   DATABASE nextcloud;
CREATE USER 'nc_user'@'localhost' IDENTIFIED BY 'qwerqwer';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nc_user'@'localhost';
FLUSH PRIVILEGES;
quit
```

Установка NextCloud

Установите **NextCloud**, выполнив команду:

```
sudo dnf install nextcloud nextcloud-httpd nextcloud-mysql
```

Настройка NextCloud

Создайте виртуальный хост, для этого отредактируйте файл **/etc/httpd/conf.d/nextcloud.conf**:

```
nano /etc/httpd/conf.d/nextcloud.conf
```

Добавив в него следующее содержимое:

```
<VirtualHost *:80>
 ServerName localhost.localdomain
 ServerAdmin admin@localdomain
 DocumentRoot /usr/share/nextcloud
 <directory /usr/share/nextcloud>
 Require all granted
 AllowOverride All
 Options FollowSymLinks MultiViews
 SetEnv HOME /usr/share/nextcloud
 SetEnv HTTP_HOME /usr/share/nextcloud
 </directory>
 </VirtualHost>
```

где:

- **ServerName** - полное имя сервера.

Создайте пустой файл **CAN_INSTALL** для разрешения установки:

```
touch /usr/share/nextcloud/config/CAN_INSTALL
```

Назначьте владельцем каталога **nextcloud** пользователя **apache**:

```
sudo chown -R apache:apache /usr/share/nextcloud
```

Настройте SELinux:

```
chcon -R -t httpd_sys_rw_content_t /usr/share/nextcloud
```

Добавьте в автозагрузку службу **httpd** и запустите ее:

```
sudo systemctl enable httpd --now
```

Отредактируйте файл **/usr/share/nextcloud/config/config.php**.

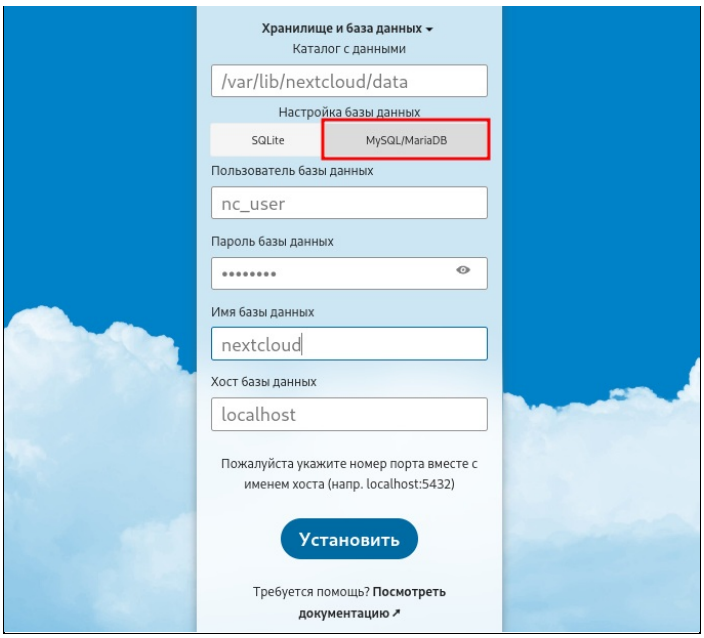
Создайте секцию **trusted_domains** в массиве и впишите IP-адрес этого сервера по образцу:

```
$CONFIG = array (
....
'trusted_domains' =>
  array (
    0 => '192.168.0.15',
),
...
)
```

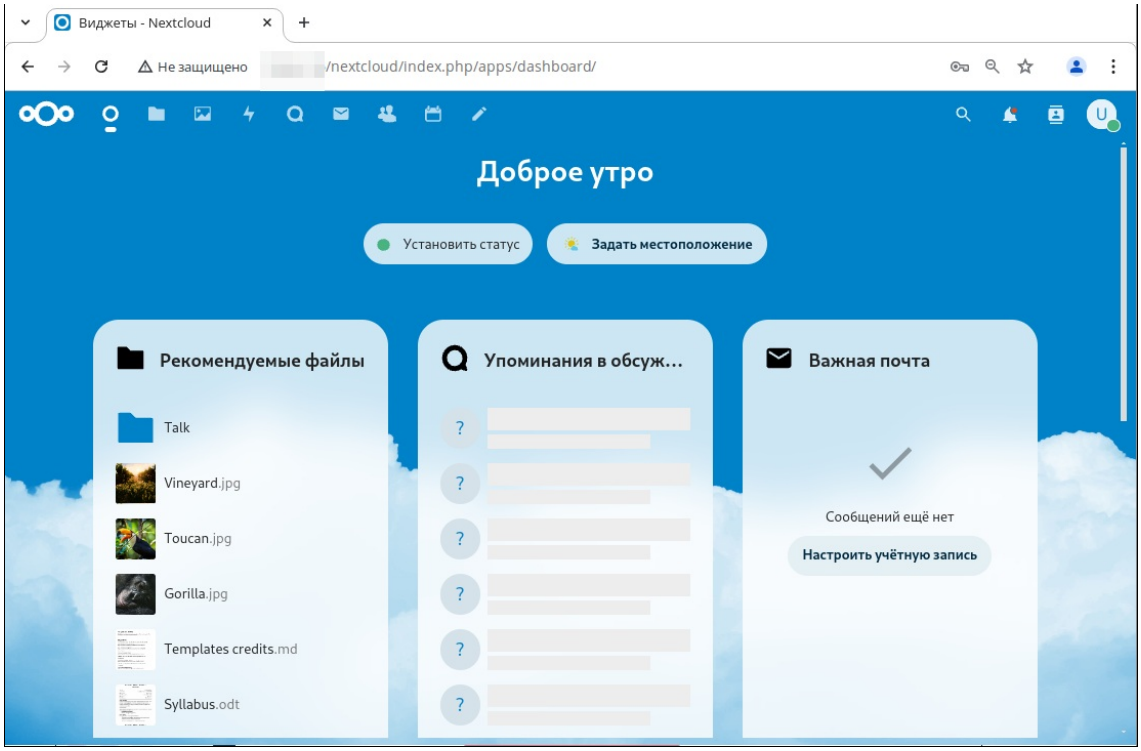
Далее, с помощью браузера, перейдите в веб-интерфейс по адресу - http://<IP-адрес_сервера>/nextcloud.

В открывшемся интерфейсе введите *имя* и *пароль* аккаунта будущего администратора сервера, а также выберите в качестве базы данных сервер **MySQL/MariaDB**. Введите ранее созданного пользователя **MySQL** и название базы данных:

- Пользователь: **nc_user**
- Пароль: **qwerqwer**
- Название базы: **nextcloud**
- Хост: **localhost**



Далее нажмите «**Установить**». Установка занимает некоторое время.



На данном этапе установка **NextCloud** завершена.

Настройка NextCloud с СУБД PostgreSQL и ПО для веб-сервера Ngnix

Предварительная подготовка сервера
Настройка SELinux
Установка Nextcloud
Установка PostreSQL14
Настройка PostreSQL
Настройка Nginx
Настройка Nextcloud

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** nextcloud-27.1.10-1, nginx-1:1.26.1-1, postgresql14-server-14.12-2

Nextcloud — набор клиент-серверных программ для создания и использования облачного хранилища. **Nextcloud** можно установить как на хосте, так и на собственном сервере.

Nextcloud позволяет совместно работать с офисными документами, файлами и информацией для планирования задач и мероприятий. Платформа также включает надстройки для доступа к электронной почте, обмена сообщениями, организации видеоконференций и чатов.

В **Nextcloud** есть выбор различных СУБД, в статье будет рассмотрена СУБД **PostgreSQL**, а в качестве ПО для веб-сервера будет выбран **Nginx**.

PostgreSQL — свободная объектно-реляционная система управления базами данных.

Nginx — это программное обеспечение с открытым исходным кодом, которое позволяет создавать веб-сервер.

Ранее мы также рассмотрели настройку **NextCloud** с СУБД **MySQL** и ПО для веб-сервера **Apache** в статье «Настройка NextCloud с СУБД MySQL и ПО для веб-сервера Apache».

Предварительная подготовка сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Настройка SELinux

Настройте **SELinux**:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_graceful_shutdown 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P domain_can_mmap_files 1
setsebool -P daemons_dump_core 1
```

Установка Nextcloud

Установка **nextcloud** для РЕД ОС осуществляется командой:

```
dnf install nextcloud nextcloud-postgresql nextcloud-nginx
```

Установка PostreSQL14

Установите **PostgreSQL**:

```
dnf install postgresql14-server
```

Настройка PostreSQL

Выполните инициализацию:

```
/bin/postgresql-14-setup initdb
```

Запустите сервер и добавьте в автозагрузку **PostgreSQL**, проверьте статус:

```
systemctl enable postgresql-14 --now
systemctl status postgresql-14
```

Зайдите под пользователем **PostgreSQL**:

```
su - postgres
```

Подключитесь к базе:

```
psql
```

Затем создайте пользователя и базу данных с именем **nextcloud** и предоставьте пользователю права на использование данной БД (**пароль укажите свой**):

```
CREATE ROLE nextcloud WITH NOSUPERUSER LOGIN PASSWORD 'nextcloudpassword';
CREATE DATABASE nextcloud WITH OWNER nextcloud;
GRANT ALL PRIVILEGES ON DATABASE nextcloud TO nextcloud;
```

Пример результата выполнения запросов:

```
postgres=# CREATE ROLE nextcloud WITH NOSUPERUSER LOGIN PASSWORD 'nextcloudpassword';
CREATE ROLE
postgres=# CREATE DATABASE nextcloud WITH OWNER nextcloud;
CREATE DATABASE
postgres=# GRANT ALL PRIVILEGES ON DATABASE nextcloud TO nextcloud;
GRANT
```

Тестовый запрос на получение списка баз данных:

```
\l
```

Выход из оболочки:

```
\q
```

Выйдите из текущей учетной записи:

```
exit
```

Добавьте разрешение для подключения:

```
nano /var/lib/pgsql/14/data/postgresql.conf
```

Приведите строку к следующему виду:

```
listen_addresses = '*'
```

Затем раскомментируйте строку:

```
#port = 5432
```

Отредактируйте файл **pg_hba.conf**, приведя строки **IPv4** и **IPv6** к следующему виду:

```
nano /var/lib/pgsql/14/data/pg_hba.conf
```

```
# or execute "SELECT pg_reload_conf()".
#
# Put your actual configuration here
# ----------------------------------
#
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.



# TYPE DATABASE USER ADDRESS METHOD

# "local" is for Unix domain socket connections only
local   all       all                   peer
# IPv4 local connections:
host    all       all    127.0.0.1/32    md5
# IPv6 local connections:
host    all       all    ::1/128         md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication    all                   peer
host    replication    all    127.0.0.1/32    scram-sha-256
host    replication    all    ::1/128         scram-sha-256
```

Затем выполните перезапуск демона **PostgreSQL**:

```
systemctl restart postgresql-14
```

Настройка Nginx

Запустите веб-сервер **Nginx**:

```
systemctl enable nginx  --now
systemctl status nginx
```

Приведите файл **nginx.conf** к следующему виду:

```
nano /etc/nginx/nginx.conf
```

```
....
  server {
    listen 80;
    listen [::]:80;
    server_name <ip_сервера>; #укажите IP-сервера
    proxy_connect_timeout 600s;
    proxy_send_timeout 600s;
    proxy_read_timeout 600s;
    fastcgi_send_timeout 600s;
    fastcgi_read_timeout 600s;
    sendfile on;
    root /usr/share/nginx/html;

    # Load configuration files for the default server block.
```

```
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
    location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
      location = /50x.html {
    }
}
```

Перезапустите веб-сервер:

```
systemctl restart nginx
```

Выполните проверку настроек **Nginx**:

```
nginx -t
```

Вывод должен быть вида:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Откройте файл **php.ini** и приведите параметры к следующему виду:

```
nano /etc/php.ini
```

```
;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;
max_execution_time = 3600
max_input_time = 3600
max_input_vars = 1000 #расскоментировать строку
memory_limit = 512M
;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;
upload_tmp_dir = /tmp/
```

Настройка Nextcloud

Создайте пустой файл **CAN_INSTALL** для разрешения установки:

```
touch /usr/share/nextcloud/config/CAN_INSTALL
```

Назначьте владельцем каталога **nextcloud** пользователя **apache**:

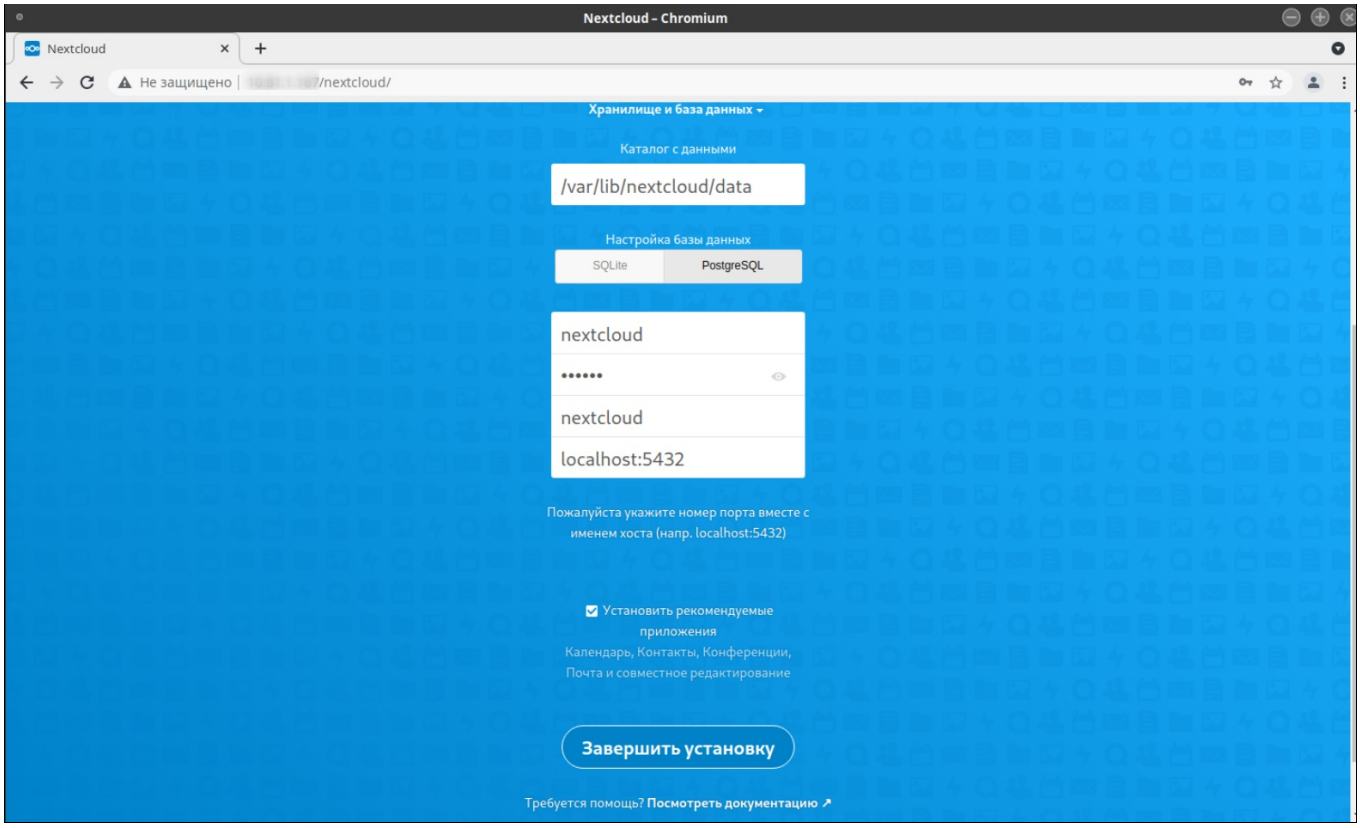
```
sudo chown -R apache:apache /usr/share/nextcloud
```

Настройте SELinux:

```
chcon -R -t httpd_sys_rw_content_t /usr/share/nextcloud
```

В браузере перейдите по ссылке вида http://<ip_сервера>/nextcloud.

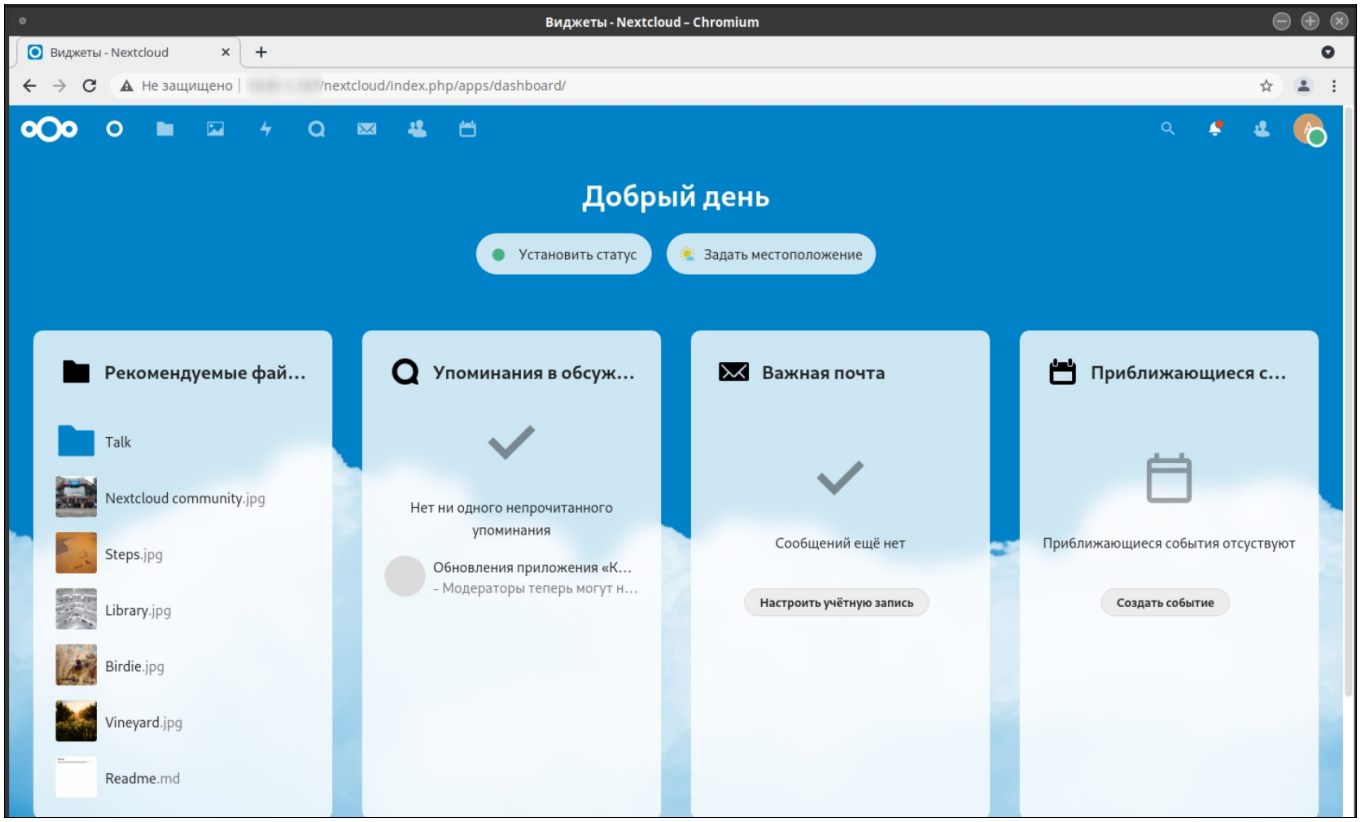
На данном этапе необходимо создать учетную запись администратора и выбрать в поле «**Хранилище и база данных**» - «**PostgreSQL**».



Укажите следующие данные для подключения:

- пользователь базы данных – **nextcloud**;
- пароль базы данных – **nextcloudpassword**;
- название базы данных – **nextcloud**;
- localhost – **localhost:5432**.

Далее нажмите «**Завершить установку**». Установка занимает некоторое время.



На данном этапе установка **Nextcloud** завершена.

Настройка автоматического входа в NextCloud в домене IPA

> Для автоматического входа сервер и клиенты **NextCloud** должны быть клиентами **IPA**. Должен быть выполнен вход под учетной записью IPA.

На сервере IPA получите kerberos-тикет администратора для создания сервиса HTTP и создайте его.

```
# kinit admin
# ipa service-add HTTP/nc.ipa.test
```

где, nc.ipa.test - это сервер NextCloud.

Сгенерируйте kerberos-тикет для сервера NextCloud.

```
# ipa-getkeytab -s dc.ipa.test -p HTTP/nc.ipa.test -k /etc/httpd/http.keytab
```

Назначьте необходимого владельца и права на файл тикета.

```
# chown root:apache /etc/httpd/http.keytab
# chmod 640 /etc/httpd/http.keytab
```

Отредактируйте конфигурационный файл NextCloud приведя его к следующему виду:

```
# nano /etc/httpd/conf.d/nextcloud.conf
Alias /nextcloud "/var/www/html/nextcloud/"
<Directory /var/www/html/nextcloud/>
  Options +FollowSymlinks
  AllowOverride All
<IfModule mod_dav.c>
  Dav off
</IfModule>
SetEnv HOME /var/www/html/nextcloud
SetEnv HTTP_HOME /var/www/html/nextcloud
</Directory>

<Location "/nextcloud/index.php/apps/user_saml/saml/login">
    AuthType Kerberos
    AuthName "Kerberos Login"
    KrbServiceName HTTP
    KrbMethodNegotiate On
    KrbLocalUserMapping On
    KrbMethodK5Passwd Off
    KrbSaveCredentials Off
    KrbVerifyKDC On
    KrbAuthRealms IPA.TEST
    Krb5KeyTab /etc/httpd/http.keytab
    Require valid-user
</Location>
```

Перезагрузите httpd

```
# systemctl restart httpd
```

Отредактируйте файл /usr/share/nextcloud/config/config.php

В секцию trusted_domains впишите hostname этого сервера по образцу:

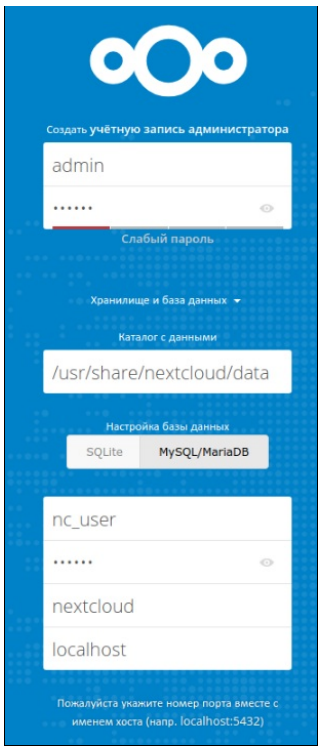
```
1 => 'nextc.ipa.test',
```

Далее, с помощью браузера, зайдите в веб интерфейс по адресу

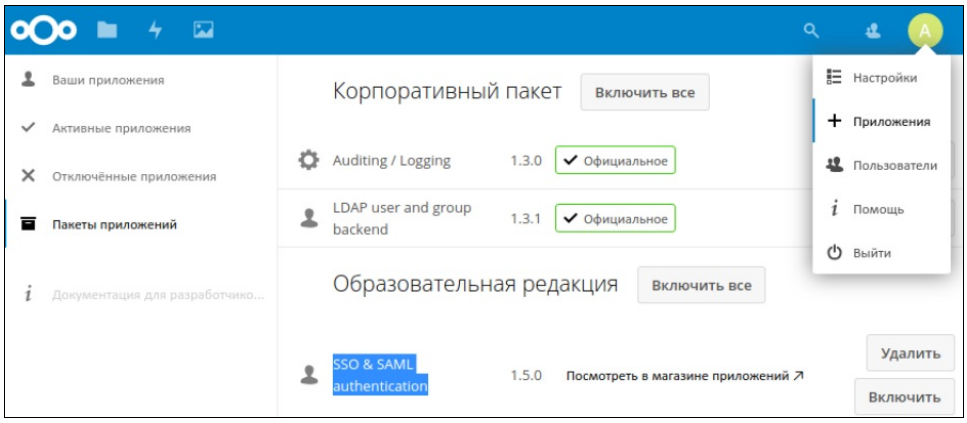
http://<ip адрес сервера>/nextcloud

В открывшемся интерфейсе введите имя и пароль аккаунта бедующего администратора сервера, а так же выберите в качестве базы данных сервер MySQL/MariaDB
Введите ранее созданного пользователя MySQL и название базы данных.
Пользователь: nc_user

Пароль: 12345
Название базы: nextcloud
Хост: localhost



Далее включите плагины для работы с LDAP и SSO. Для этого в правом верхнем углу выберите Приложения, в открывшемся окне, в меню выберите Пакеты приложений. Включите плагины LDAP user and group backend и SSO & SAML authentication.



Настройте доступ к LDAP.

Выберите в верхнем правом углу пункт Настройки, в открывшемся окне в меню пункт Интеграция LDAP/AD. Введите данные подключения.

Сервер: ldap://dc.ipa.test

Порт: 389

Пользователь DN: uid=admin,cn=users,cn=accounts,dc=ipa,dc=test

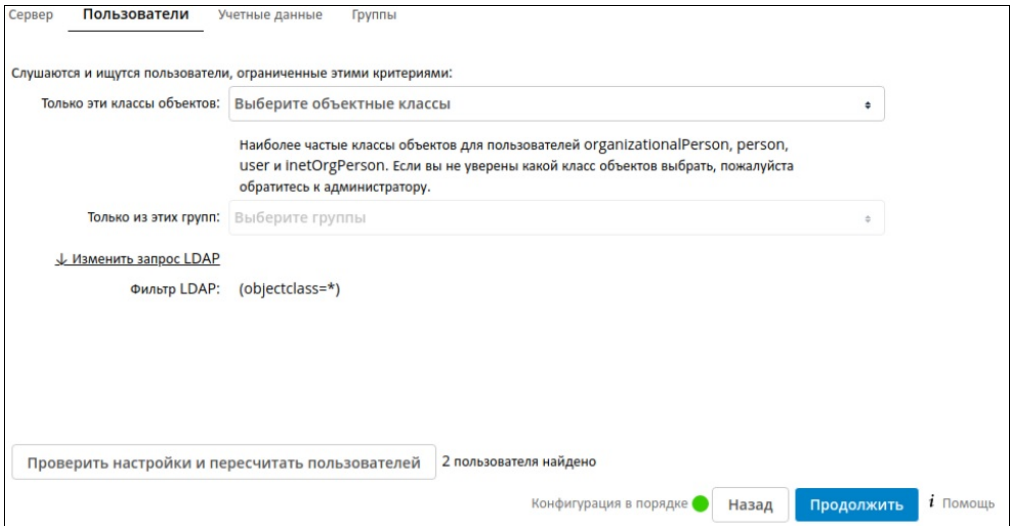
Пароль: qwerqwert12

База DN: dc=ipa,dc=test

Нажмите Проверить базу поиска DN

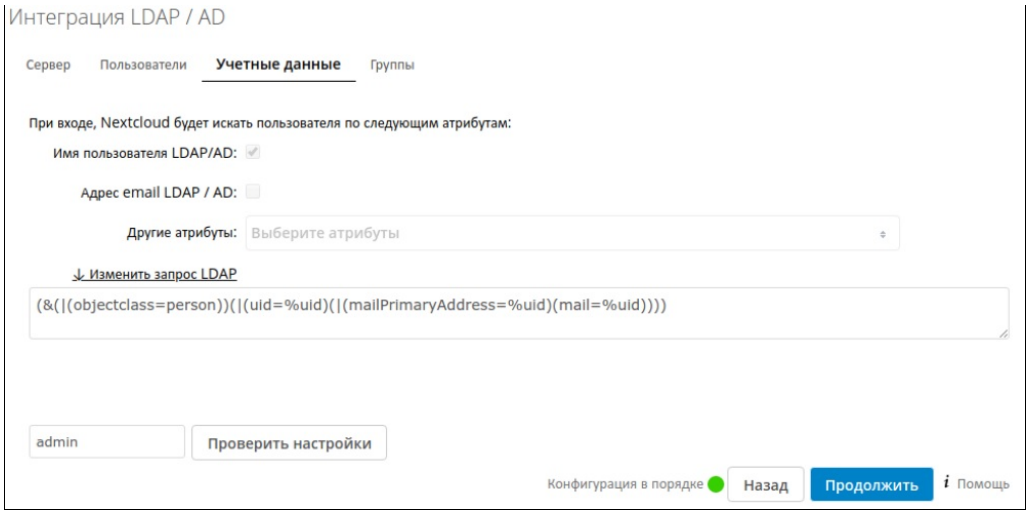
Если все хорошо, нажмите Продолжить.

Выставите все так, как на скриншоте ниже и нажмите "Проверить" и пересчитать пользователей.



В следующем окне измените запрос LDAP на
(&(|(objectclass=person))(|(uid=%uid)(|(mailPrimaryAddress=%uid)(mail=%uid))))

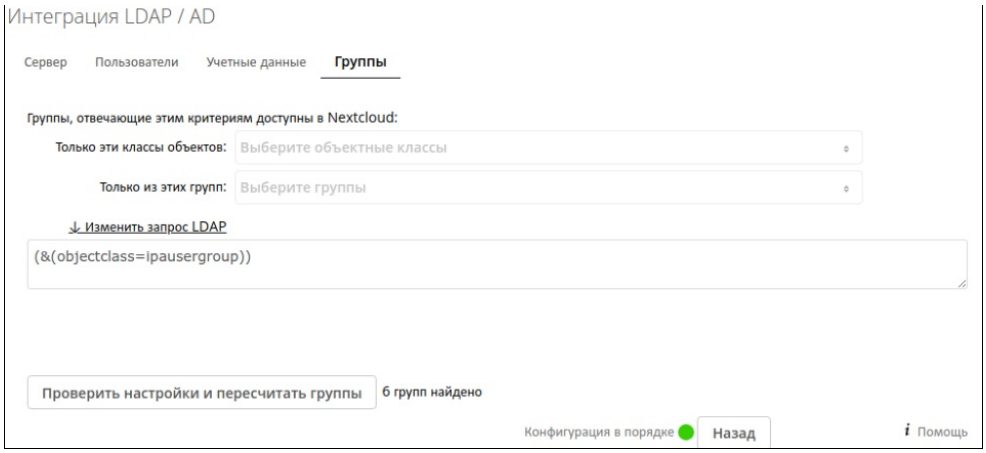
Впишите пользователя admin и проверьте настройки



В следующем окне измените запрос LDAP на

```
(&(objectclass=ipausergroup))
```

Нажмите Проверить базу поиска DN



На этом настройка LDAP завершена.

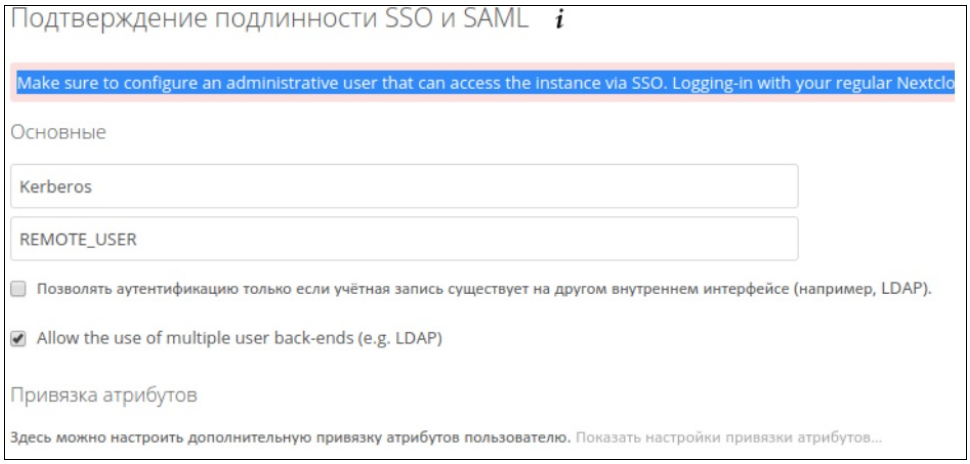
Перейдите к настройке SSO.

Перейдите в меню в пункт Подтверждение подлинности SSO и SAML

Выберите переменные окружения

Введите в верхнее поле отображаемое имя подключения, например Kerberos
В нижнее поле uid REMOTE_USER

Поставьте галку Allow the use of multiple user back-ends



На этом конфигурация закончена.

Настройка SSO на клиенте

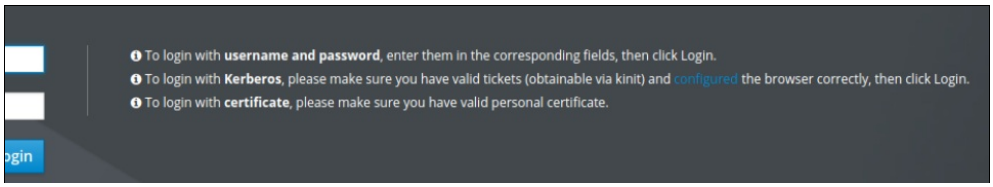
Зайдите на клиенте под учетной записью домена ipa.

Для работы с SSO нужно настроить браузер

Инструкцию по настройке можно найти в панель входа в ipa домен по адресу

https://<имя сервера ipa>

Нажать на ссылку Configured



Для Firefox

1. Импортируйте сертификат нажав на кнопку Import Certificate Authority certificate

Поставьте все три галки.

2. В адресной строке Firefox введите **about:config** для отображения списка текущих параметров конфигурации.
3. В поле «Поиск» введите, **negotiate**, чтобы ограничить список параметров.
4. Дважды щелкните запись network.negotiate-auth.trusted-uris, чтобы отобразить диалоговое окно «Введите значение(строка)».
5. Введите имя домена, в котором вы хотите выполнить аутентификацию, например, .ipa.test.
6. Перейдите на страницу Nextcloud в вашей сети и нажмите кнопку Kerberos. После этого вход будет произведен.

Подключение РЕД ОС к облачным сервисам

Веб-интерфейс
Специальная программа
WebDAV

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** yandex-disk-0.1.6.1080-1

В данной статье будут рассмотрены возможности подключения РЕД ОС к облачным сервисам на примере *Яндекс.Диска*.

Яндекс.Диск — это сервис, который позволяет вам хранить файлы на серверах Яндекса. Вы можете работать с файлами на Диске с любого устройства, подключенного к интернету.

Подключение к Диску можно осуществить тремя способами:

1. Через веб-интерфейс.

2. С помощью специальной программы.

3. С использованием протокола WebDAV.

Вы можете подробнее ознакомиться с возможностью подключения РЕД ОС к облачным сервисам, просмотрев наши обучающие видео:

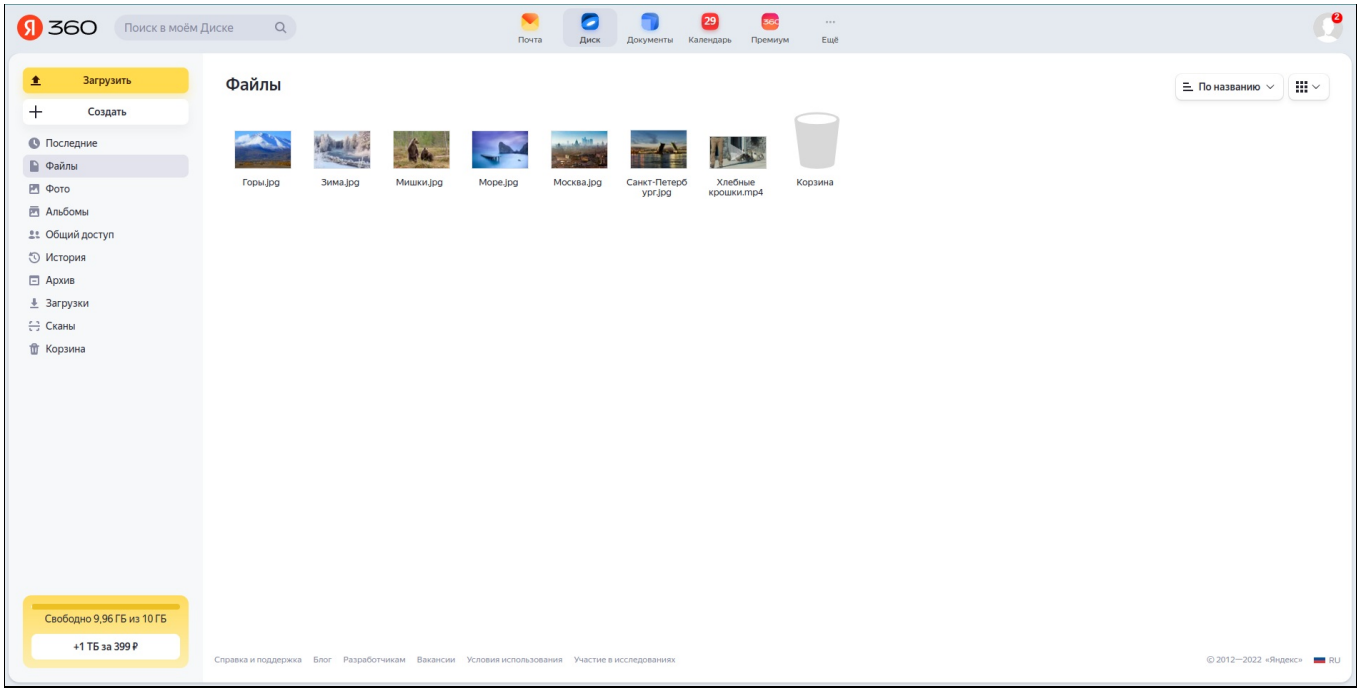
- на **RuTube** — Подключаем РЕД ОС (Linux) к облаку Яндекс.Диск. Web-Интерфейс, GUI программа или протокол WebDAV;
- в **Яндекс.Дзен** — Подключаем РЕД ОС (Linux) к облаку Яндекс.Диск. Web-Интерфейс, GUI программа или протокол WebDAV.
- в **VK Видео** — Подключаем РЕД ОС (Linux) к облаку Яндекс.Диск. Web-Интерфейс, GUI программа или протокол WebDAV.

На наших каналах вы также сможете найти много другой полезной информации.

Веб-интерфейс

Для подключения через веб-интерфейс необходимо в браузере перейти на страницу Яндекс.Диска и войти в свою учетную запись или создать новую. После авторизации будет открыто ваше облачное хранилище.

Веб-интерфейс прост и интуитивно понятен.



Специальная программа

Для использования *Яндекс.Диска* на компьютере необходимо установить специальную программу.

Перейдите на страницу Яндекс.Диска. В открывшемся списке доступных программ выберите «**yandex-disk-latest.x86_64**» в формате **.rpm**. Начнется загрузка пакета.

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

Затем откройте папку со скачанным пакетом:

```
cd /home/user/Загрузки/
```

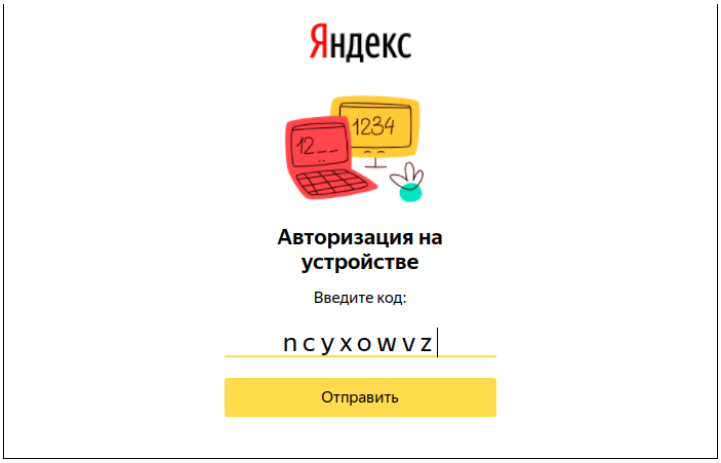
После этого запустите установку программы:

```
dnf install yandex-disk-latest.x86_64.rpm
```

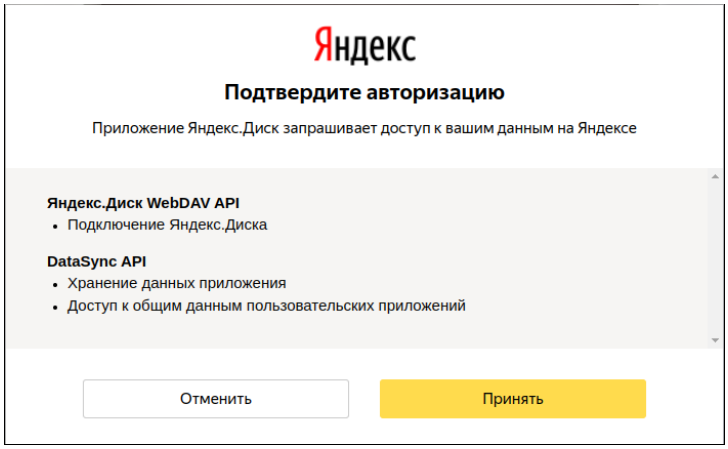
После установки программа сможет работать только в консольном режиме, поэтому необходимо открыть в терминал и выполнить команду:

```
yandex-disk setup

Использовать прокси-сервер? [y/N]: n
Авторизация
Если у вас ещё нет аккаунта на Яндексе, его можно завести по ссылке https://passport.yandex.ru/passport?mode=register

Откройте страницу 'https://ya.ru/device' и введите код ‘ncyxowvz’ в течение 300 секунд. Убедитесь, что вы авторизованы в браузере с нужным аккаунтом.
```

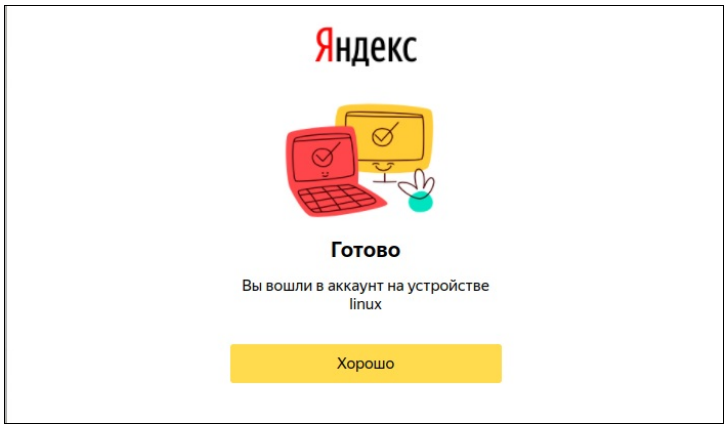
В выводе команды появится ссылка и код авторизации. В браузере перейдите по указанной ссылке и введите код. Убедитесь, что вы авторизованы в браузере с нужным аккаунтом.



Далее необходимо принять запрос на доступ к вашим данным на Диске.



Если все прошло успешно, появится следующее окно.



Проверить работу Яндекс.Диска можно командой:

```
yandex-disk status
```

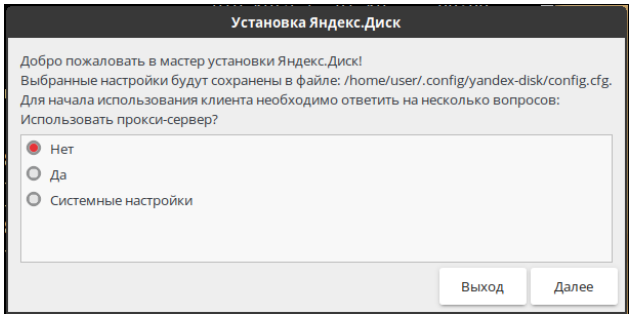
Для установки графической утилиты Диска, перейдите на страницу инструкции по установке «GUI для консольного клиента Linux». Для примера выбран вариант **YD-tools**. На открывшейся странице перейдите по ссылке с инструкцией и скачайте необходимый файл.

После этого откройте терминал, перейдите в папку со скачанным файлом и выполните установку утилиты:

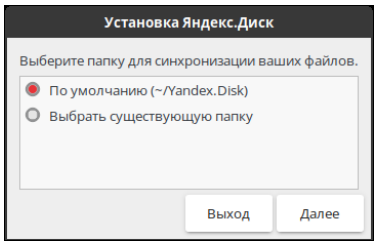
```
cd /home/user/Загрузки/
dnf install yandex-disk-indicator-1.11.0-1.noarch.rpm
```

После установки утилита будет доступна из «**Главного меню**» - «**Интернет**» - «**Индикатор Yandex.Disk**».

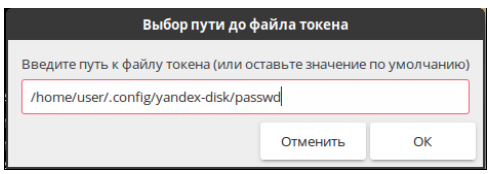
При первом запуске необходимо настроить сервис. На запрос использования прокси-сервера выберите «**Нет**».



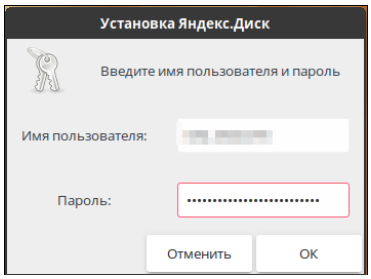
Далее необходимо указать папку, которая будет использоваться сервисом, в примере используется значение по умолчанию.



Затем необходимо указать путь к файлу, который будет хранить учетные данные для доступа к Яндекс.Диску.

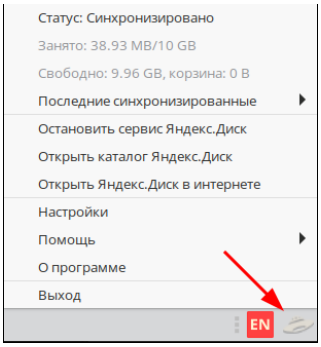


После этого необходимо указать логин и пароль вашей учетной записи на Яндекс.



На этом настройка сервиса завершена.

В системном трее появится соответствующий значок приложения, с помощью которого можно управлять всеми функциями Диска. При запуске программы автоматически будет запущена синхронизация Диска, данные будут сохранены в указанной вами папке при настройке консольной утилиты.

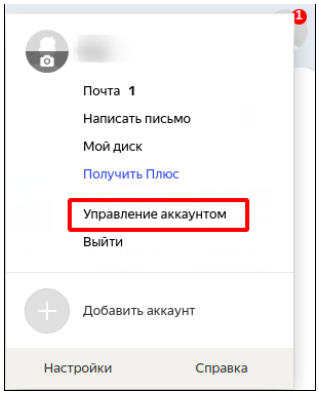


При наведении курсора на значок Яндекс.Диска в системном трее вы увидите надпись «**Синхронизировано**» - это означает, что Диск теперь подключен к компьютеру. Изменить параметры синхронизации можно в настройках.

WebDAV

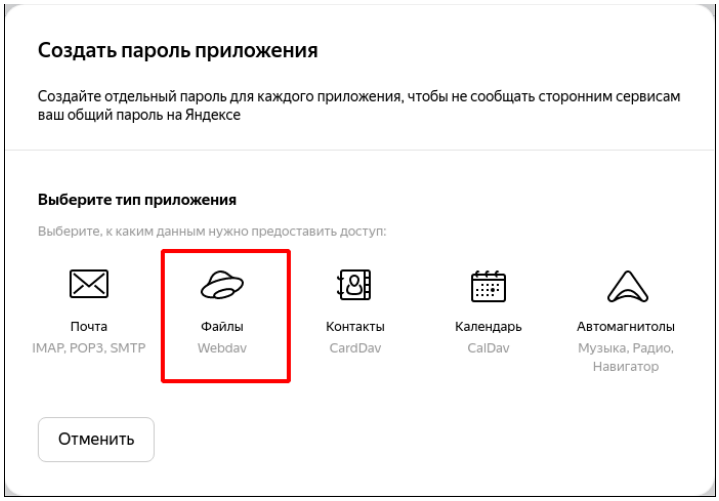
Существует также третий способ подключения РЕД ОС к облачному сервису — с использованием протокола **WebDAV**. Данный способ подключает облачный сервис как сетевой диск, некоторые возможности в таком режиме недоступны, однако работать с файлами удобнее, и требуется меньше ресурсов ОС.

Для того чтобы подключиться к Яндекс.Диску по протоколу **WebDAV**, необходимо создать пароль приложения. Для этого авторизуйтесь в своей учетной записи Яндекс и откройте страницу «**Управление аккаунтом**».

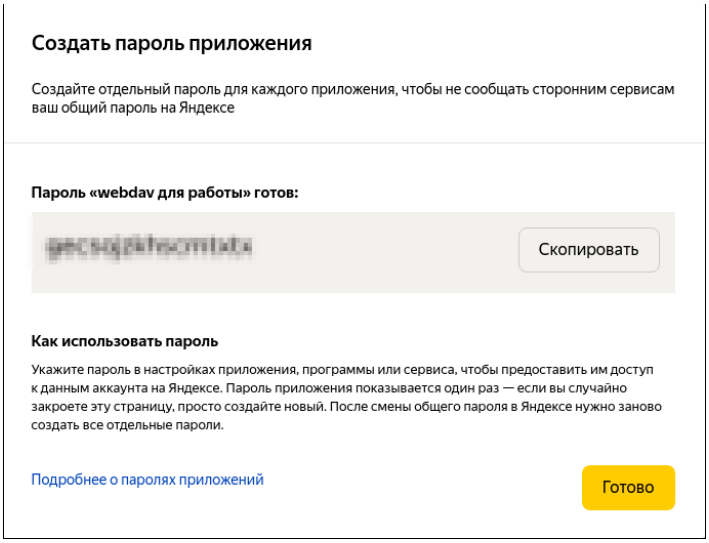


В разделе «Пароли и авторизация» выберите «**Включить пароли приложений**». Подтвердите действие и нажмите «**Создать новый пароль**».

Выберите тип приложения — **WebDAV**.



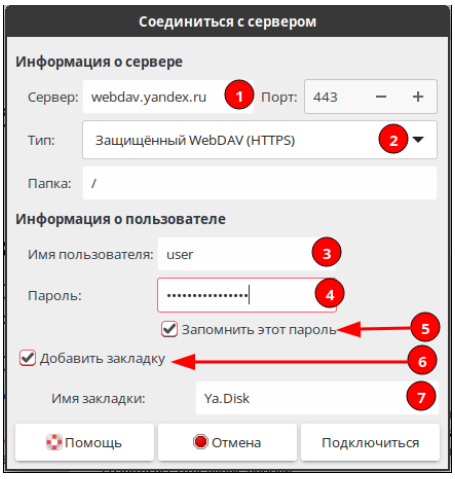
Введите понятное для вас название создаваемого пароля, например, «*webdav для работы*». Пароль с таким именем будет отображаться в списке. Нажмите кнопку «**Создать**». Пароль приложения отобразится во всплывающем окне.



Пароль приложения — это отдельный пароль, который будет создан специально для подключения вашего Яндекс.Диска по протоколу **WebDAV**. Такой пароль безопасен и не предоставит доступ к управлению вашим аккаунтом.

После создания отдельного защищенного пароля можно переходить к настройке подключения. Для этого откройте файловый менеджер *Caja*, перейдите в пункт меню «**Файл**» - «**Соединиться с сервером...**».

В появившемся окне введите следующие данные:



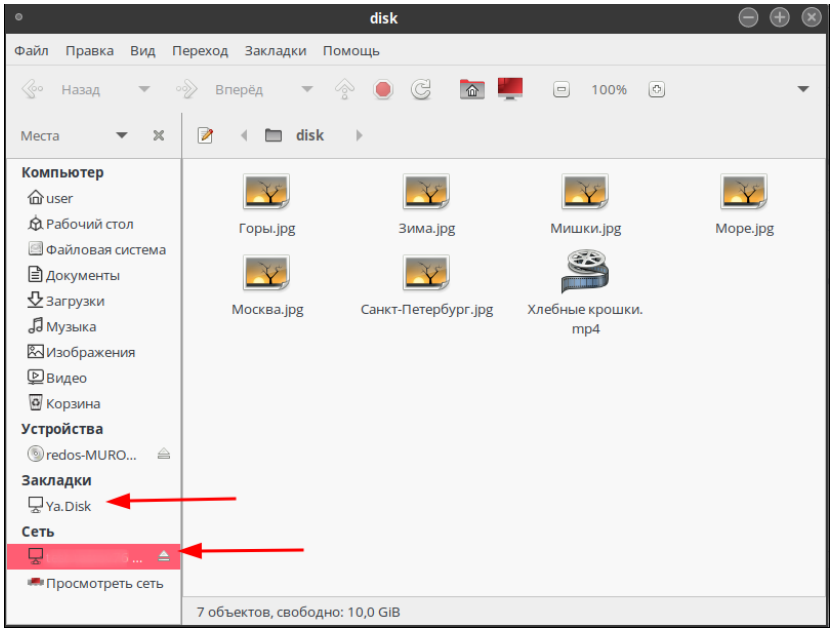
1. Имя сервера — **webdav.yandex.ru**.
2. Тип протокола для подключения — **Защищенный WebDAV (HTTPS)**.
3. **Имя** пользователя.
4. **Пароль** — созданный защищённый пароль.

5. Установить / снять флаг запоминания пароля.
6. Для восстановления подключения можно добавить закладку.
7. При добавлении закладки необходимо указать ее имя.

После этого нажмите «**Подключиться**».

После успешного подключения в группе **Сеть** будет активна запись, с правой стороны которой будет доступна кнопка **Извлечь** для отключения от Диска.

Если вы сохранили закладку, данная запись появится. Если закладку не сохраняли, то при активном соединении ее можно добавить через пункт меню «**Закладки**» - «**Добавить закладку**».



Облачные сервисы, которые поддерживают протокол **WebDAV**, настраиваются аналогичным образом.

WebDAV, neon и chezdav для настройки облачного сервиса

Утилита neon
Утилита chezdav
Синтаксис chezdav
Опции chezdav
WebDAV
Настройки облачного сервиса, поддерживающего протокол WebDAV

Окружение

- **Версия РЕД ОС**: 7.3, 8
- **Конфигурация**: Сервер графический
- **Версия ПО в РЕД ОС 7.3**: neon-0.32.1, chezdav-2.3
- **Версия ПО в РЕД ОС 8.0**: neon-0.32.2, chezdav-3.0

WebDAV (Web Distributed Authoring and Versioning) — это расширение протокола HTTP, которое позволяет клиентам выполнять удалённое управление и совместное использование файлов на веб-сервере. Оно предоставляет функции для работы с удалёнными файлами, включая создание, чтение, запись и удаление файлов, а также управление правами доступа и блокировками. Утилиты **neon** и **chezdav** являются клиентскими библиотеками, предназначенными для работы с WebDAV-серверами.

Утилита neon

Neon — клиентская библиотека HTTP и WebDAV, предоставляющая высокоуровневый интерфейс для методов HTTP и WebDAV, а также низкоуровневый интерфейс для обработки HTTP-запросов. Neon поддерживает постоянные подключения, прокси-серверы, базовую аутентификацию, Kerberos, SSL.

Neon предназначен для защиты от определённой модели угроз: использования вредоносного HTTP-сервера. В соответствии с этой моделью угроз против клиента возможен целый ряд атак, когда пользователя (или приложение) можно обманом заставить получить доступ к HTTP-серверу, который контролируется злоумышленником.

Возможности:

- Высокоуровневый интерфейс для общих методов **HTTP** и **WebDAV** позволяет отправлять GET- или MKCOL-запросы к ресурсу с помощью одного вызова функции;
- Низкоуровневый интерфейс для обработки HTTP-запросов, позволяющий реализовывать запросы с использованием произвольных методов и заголовков запросов, захватывать произвольные заголовки ответов и т. д.;
- Поддержка постоянного подключения — **neon** группирует набор запросов к серверу в "сеанс", запросы внутри этого сеанса могут использовать постоянно действующее соединение;
- Современная поддержка аутентификации, полная реализация нового стандарта аутентификации RFC2617, включая поддержку **Digest**, **Basic** и **Negotiate**;
- Сеанс может быть настроен на использование прокси-сервера, при этом аутентификация поддерживается как для прокси-сервера, так и для исходного сервера;
- Поддержка SSL/TLS с использованием OpenSSL или GnuTLS, предоставление уровня абстракции для проверки сертификатов сервера, обработки клиентских сертификатов и изучения свойств сертификатов;
- Полная поддержка SSL, простой интерфейс для включения SSL, скрывающий сложность прямого использования библиотеки SSL. Поддержка клиентских сертификатов, проверка сертификатов сервера на основе обратного вызова, а также функции для загрузки сертификатов доверенного центра сертификации. Клиентские сертификаты на основе смарт-карт поддерживаются через интерфейс-оболочку PKCS#11;
- Универсальный интерфейс синтаксического анализа XML для обработки содержимого XML-ответов с использованием SAX-подобных обратных вызовов;
- Поддержка WebDAV, включая блокировку, манипулирование свойствами и извлечение данных, поддержку ACL.

Для установки **neon** выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install neon
```

Основные функции:

- **ne_session *ne_session_create(const char *scheme, const char *hostname, unsigned int port)** — функция создаёт соединения с указанным хостом, принимает в качестве параметров схему, хост и порт, возвращает указатель на новый объект сеанса, который используется в других функциях для выполнения запросов;

- **int ne_get(ne_session *sess, const char *path, int fd)** — получение ресурса по пути path, результат записывается в указанный файловый дескриптор;
- **int ne_put(ne_session *sess, const char *path, int fd)** — изменение ресурса по пути path из файлового дескриптора;
- **int ne_copy(ne_session *sess, int overwrite, int depth, const char *src, const char *dest)** — копирует ресурс из src в dest;
- **int ne_move(ne_session *sess, int overwrite, const char *src, const char *dest)** — перемещает ресурс из src в dest;
- **int ne_delete(ne_session *sess, const char *uri)** — удаляет ресурс по указанному пути;
- **int ne_mkcol(ne_session *sess, const char *uri)** — создаёт директорию struct ne_lock *ne_lock_create(void);
- **int ne_lock(ne_session *sess, struct ne_lock *lock)** — создаёт блокировку на ресурс;
- **int ne_unlock(ne_session *sess, const struct ne_lock *lock)** — снимает блокировку с ресурса;
- **ne_lock** и **ne_unlock** — принимают структуру **ne_lock** в качестве аргумента, содержащую информацию о блокировке на ресурсы.

  Описание полей структуры **ne_lock**:

  - **ne_uri uri** — URI-ресурса, который требуется заблокировать;
  - **int depth** — глубина блокировки, определяющая, на каком уровне блокировки будет применяться операция;
  - **enum ne_lock_type type** — тип блокировки (**shared** — разделяемая блокировка, **exclusive** — исключительная блокировка);
  - **enum ne_lock_scope scope** — область видимости блокировки;
  - **char *token** — уникальный идентификатор блокировки;
  - **char *owner** — владелец блокировки;
  - **long timeout** — таймаут блокировки в секундах.

Утилита chezdav

Утилита **chezdav** также предоставляет возможность работы с WebDAV-серверами, но основной упор делается на удобство использования и предоставление более высокоуровневых функций. Утилита **chezdav** запускает сервер WebDAV. Это позволяет клиентам получать доступ к вашим файлам и изменять их. Для просмотра файлов достаточно простого веб-браузера. Общей папкой по умолчанию является домашний каталог, но вы можете указать другую папку с помощью опции **-P**.

Для установки **chezdav** выполните команду в терминале (потребуются права **администратора**):

```
sudo dnf install chezdav
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Для запуска webdav-сервера выполните в терминале команду:

```
chezdav
```

Для вывода списка доступных команд и опций утилиты **chezdav**, а также краткого описания их использования введите команду:

```
chezdav --help
```

Синтаксис chezdav

Утилита **chezdav** доступна для запуска через терминал при помощи команды следующего вида:

```
chezdav [<опции>]
```

Опции chezdav

Основные опции утилиты:

- **-h, --help** — показать параметры справки;
- **--version** — вывести версию программы;
- **-v, --verbose** — подробный вывод;

- **-p, --port** — порт для прослушивания (по умолчанию порт выделяется случайным образом);
- **--local** — слушать только локально;
- **--public** — слушать на всех интерфейсах;
- **-P, --path** — путь для экспорта;
- **-d, --htdigest** — путь к файлу htdigest;
- **-r, --readonly** — только чтение.

WebDAV

Подробную информацию о подключении к облачному сервису с использованием протокола **WebDAV** см. в нашей инструкции «Подключение РЕД ОС к облачным сервисам».

Настройки облачного сервиса, поддерживающего протокол WebDAV

1. Выполните установку **davfs2** в терминале (потребуются права **администратора**):

```
sudo dnf install davfs2
```

2. Создайте точку монтирования (например, **/mnt/webdav**):

```
sudo mkdir /mnt/webdav
```

3. Откройте файл конфигурации **/etc/davfs2/davfs2.conf** на редактирование:

```
sudo nano /etc/davfs2/davfs2.conf
```

Раскомментируйте (уберите символ "#" в начале строки) и установите значение "0" для отключения блокировок в параметре **use_locks**:

```
use_locks 0
```

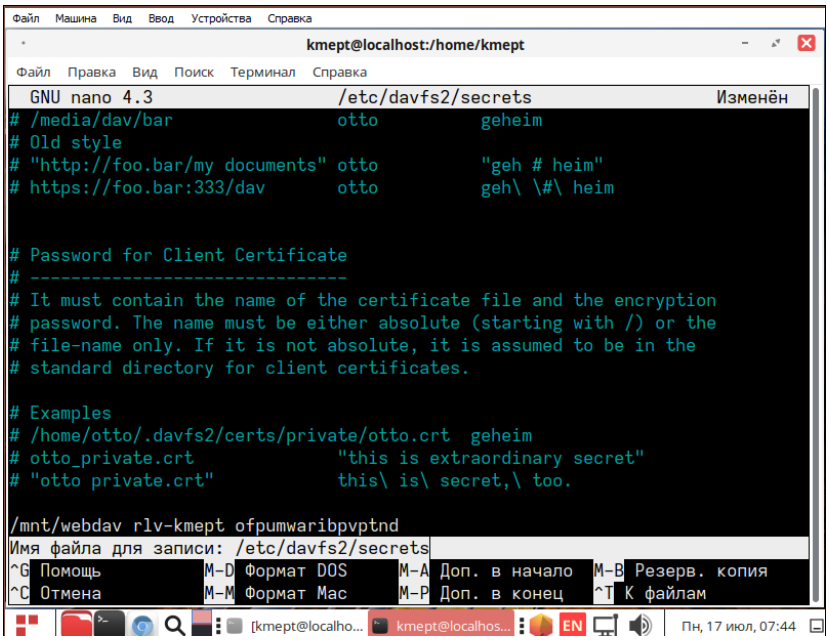
4. Создайте файл с учётными данными для аутентификации:

```
sudo nano /etc/davfs2/secrets
```

Добавьте строку в следующем формате (замените <имя_пользователя> и <пароль> на свои данные):

```
/mnt/webdav <имя_пользователя> <пароль>
```

Сохраните и закройте файл.



5. Установите права доступа для файла с учётными данными:

```
sudo chmod 600 /etc/davfs2/secrets
```

6. Добавьте свойства монтирования в файл **/etc/fstab** для автоматического монтирования при загрузке системы:

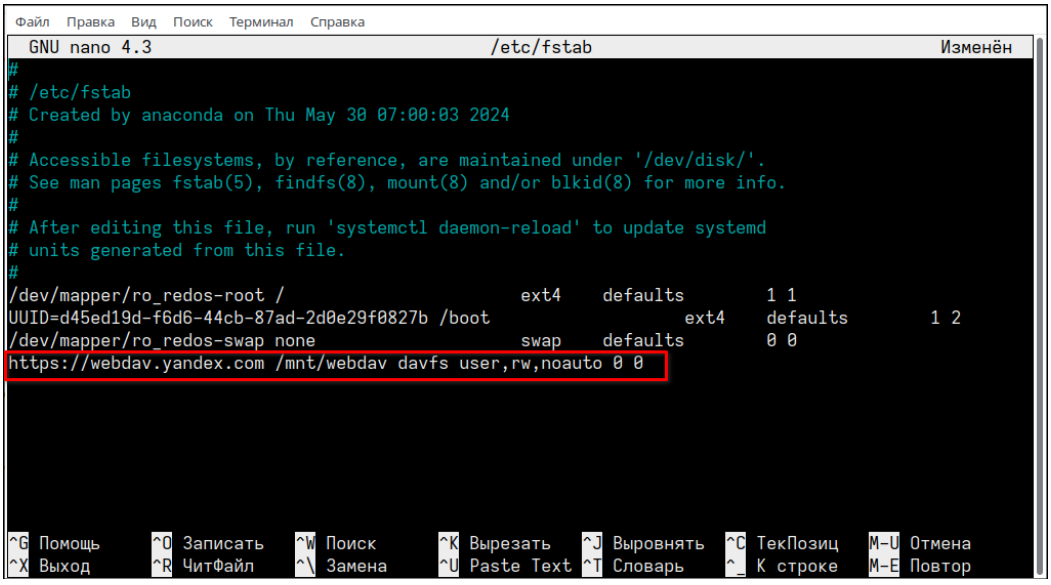
```
sudo nano /etc/fstab
```

Добавьте следующую строку в конец файла:

```
<URL_сервера_WebDAV> /mnt/webdav davfs user,rw,noauto 0 0
```

где:

<URL_сервера_WebDAV> необходимо заменить на URL вашего сервера WebDAV.

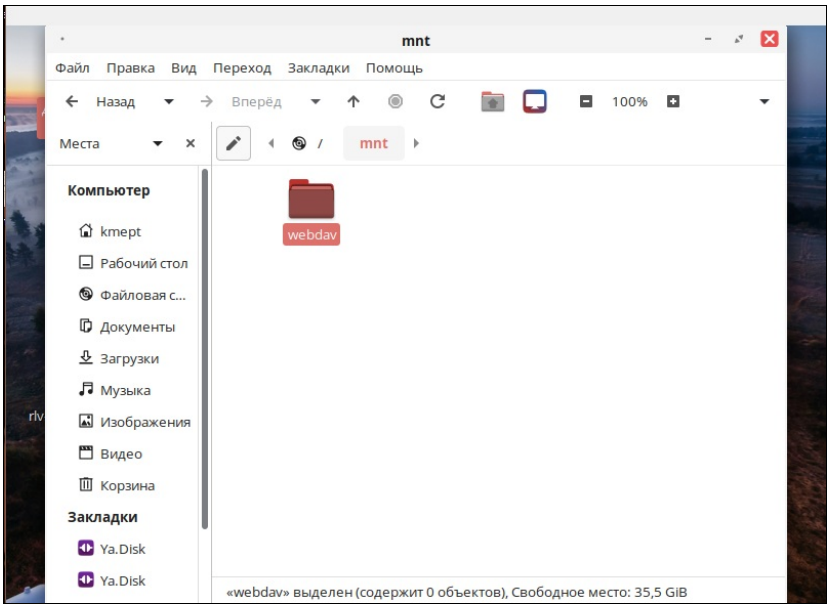


7. Сохраните и закройте файл.

8. Примонтируйте WebDAV-ресурс:

```
sudo mount /mnt/webdav
```

Теперь ваш WebDAV-ресурс должен быть успешно подключён и доступен для работы в каталоге **/mnt/webdav**.


mnt
Файл Правка Вид Переход Закладки Помощь
Назад
Вперёд
100%
Места
/
mnt
Компьютер
kmept
Рабочий стол
Файловая с...
Документы
Загрузки
Музыка
Изображения
Видео
Корзина
Закладки
Ya.Disk
Ya.Disk
webdav
«webdav» выделен (содержит 0 объектов), Свободное место: 35,5 GiB

Webmin - программный комплекс для удаленного администрирования

Установка и настройка
Обновление
Работа с Webmin
Файловый менеджер
Работа с консолью
Состояние сервера и служб
Резервное копирование конфигурационных файлов
Модуль «Пользователи в Webmin»
Bacula - резервное копирование системы
Ротация логов
Добавление и редактирование MIME типов
Read User Mail
Настройки Postfix
SSH Сервер
HTTP Tunnel
Protected Web Directories
Загрузка и сохранение
Команды пользователя
Модули Perl
Bandwidth Monitoring
TCP Wrappers
Запись на компакт-диски
Cluster Change Passwords
Cluster Copy Files
Cluster Shell Commands
Cluster Usermin Servers
Cluster Webmin Servers

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** webmin-1.981-4

Средство системного администрирования **Webmin** представляет собой бесплатное программное обеспечение, облегчающее работу системных администраторов операционных систем семейства Linux.

Webmin представляет собой простой веб-сервер, и несколько сотен скриптов, написанных на языке **Perl**, с помощью которых выполняются команды конфигурирования отдельных элементов системы, системных служб и самого Webmin. Практически, **Webmin** - это удобная панель управления, доступная через веб-браузер, а модули **Webmin** - это внешний интерфейс к консольным утилитам. При настройках по умолчанию, для доступа к **Webmin** достаточно в любом обозревателе открыть URL - https://host:10000

https://localhost:10000 - обычно, при настройках по умолчанию, доступ к средствам **Webmin** возможен только через петлевой интерфейс. После авторизации, пользователь получает доступ к настройкам как самого Webmin, так и тех составляющих операционной системы, поддержка которых реализована в его данной версии.

Webmin - это средство, облегчающее администрирование, упрощающее рутинные действия, позволяющее отображать данные в удобном для восприятия виде и выполнять настройки с меньшими затратами сил и средств.

Webmin работает фактически на всех *nix-платформах, включая Linux, AIX, HPUX, Solaris, OS X и другие. Он может работать практически на любом графическом браузере как локально так и удаленно. Данные, передаваемые между сервером и браузером, могут шифроваться при помощи SSL. Кроме того, для начинающего системного администратора Linux полезным свойством может быть то, что в **Webmin** имеется возможность изменить используемый язык и тему оформления.

Установка и настройка

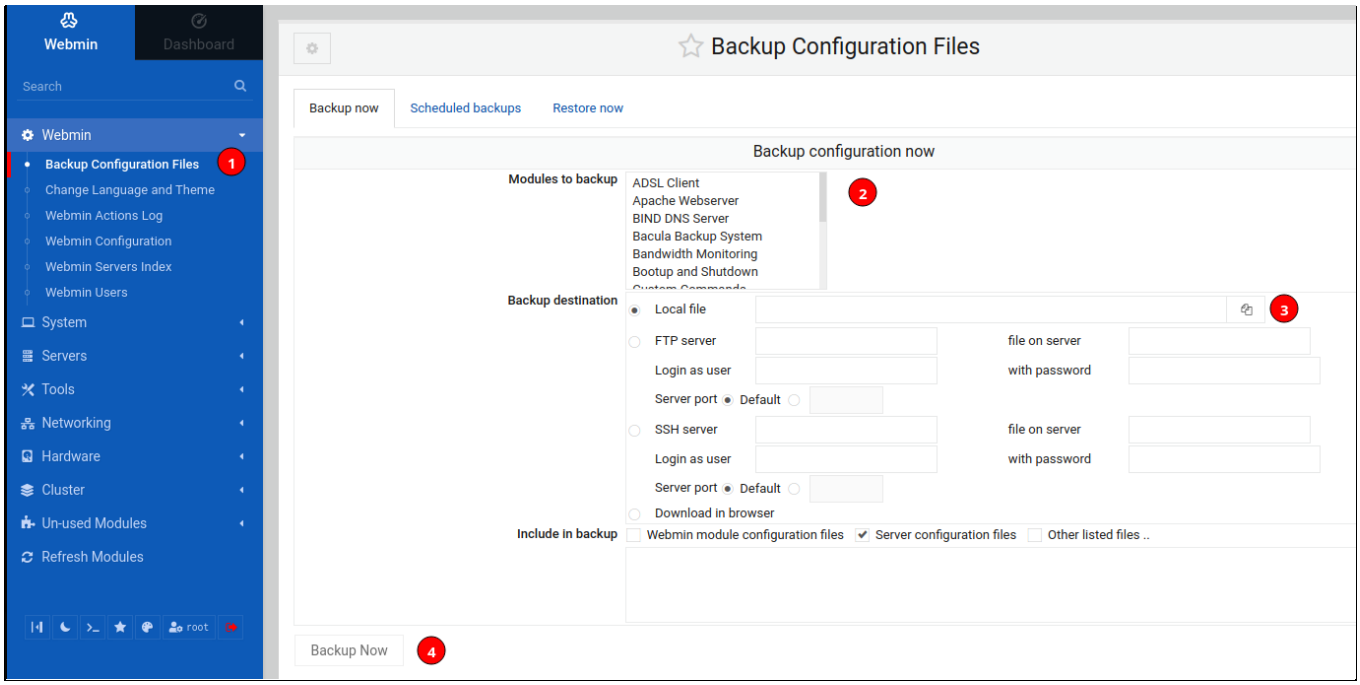
Установка должна выполняться под учетной записью суперпользователя и может быть выполнена в терминале с помощью команды:

```
dnf install webmin
```

Обновление

Для обновления уже установленной и настроенной системы webmin до актуальной версии необходимо выполнить следующие действия:

1. Создать резервную копию конфигурационных файлов webmin. Для этого в веб-интерфейсе во вкладке « **Webmin**» выберите модуль «**Backup Configuration Files**» (**1**).



Выделите модули, конфигурацию которых необходимо сохранить (**2**). Выберите место сохранения резервной копии и введите имя создаваемого архива (**3**). Обратите внимание, что расширение архива должно быть **tar.gz**. Затем нажмите на кнопку «**Backup Now**» (**4**).

2. Удалить установленную версию **webmin**:

```
dnf remove webmin
```

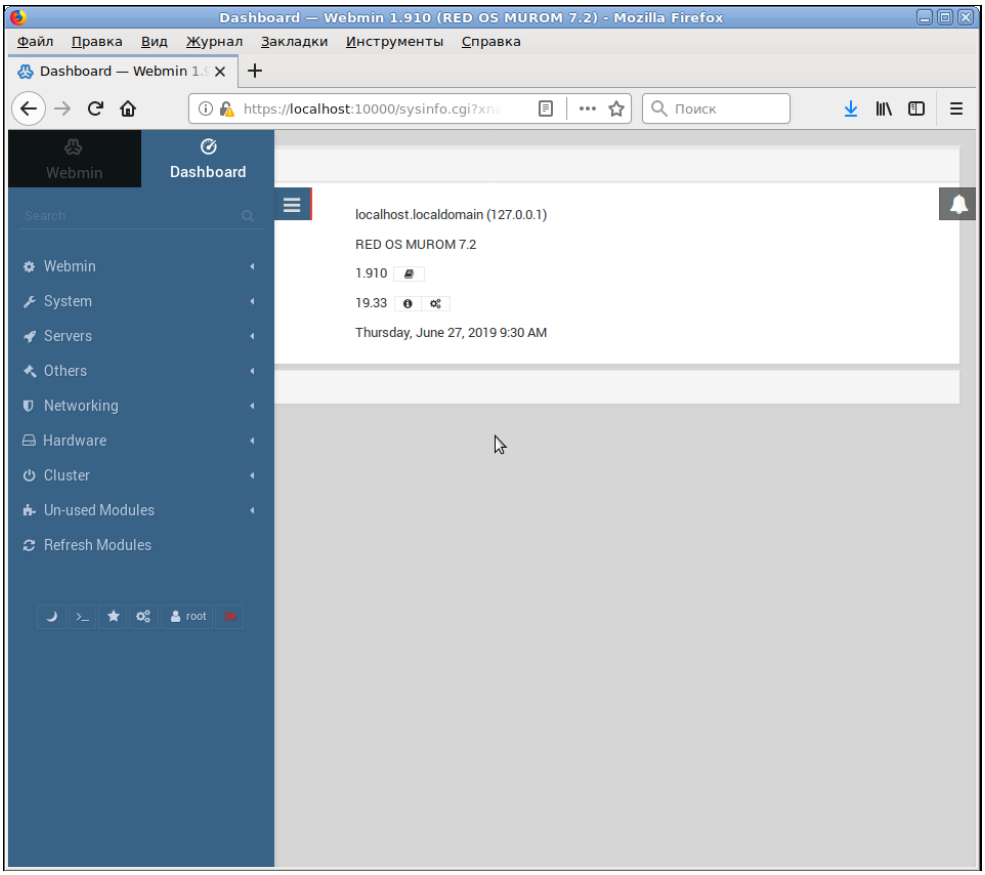
3. Установить актуальную версию из репозитория:

```
dnf install webmin
```

4. Перейти в веб-интерфейс **webmin**. Открыть модуль «**Backup Configuration Files**», во вкладке «**Restore now**» выполнить действия, аналогичные созданию резервной копии, и нажать кнопку «**Restore now**».

Работа с Webmin

В браузере открываем ссылку **https://localhost:10000/**. После ввода имени пользователя и пароля отобразится основное окно **Webmin**:



В правой части основного окна отображается информация о системе, в левой - разделы, доступные для настройки с использованием Webmin:

- **Webmin** - настройки модуля Webmin - настройка слушаемых сервером адресов и портов, настройки пользователей, язык и тема оформления, журналы действий, резервное копирование и т.п.
- **System** - информация и системные настройки - управление пользователями, процессами, службами, файловыми системами, системными журналами, резервное копирование и управление приложениями.
- **Servers** - настройки для установленных в системе серверов DNS, DHCP, FTP и т.п.
- **Others** - прочие инструменты для администрирования - командная оболочка, менеджер файлов, SSH-клиент и т.п.
- **Networking** - сетевые настройки, средства мониторинга сетевого трафика, брандмауэры и т.п.
- **Hardware** - системное время, средства управления принтерами, разделами на дисках, запись на CD/DVD.
- **Cluster** - управление несколькими системами, объединенными в кластер. Webmin устанавливается на одной из систем, входящих в кластер, и взаимодействие с остальными осуществляется через протокол удаленного вызова процедур RPC (Remote Procedure Call).
- **Un-used Modules** - неиспользуемые модули Webmin - модули которые были установлены, но в системе нет объектов для их использования. Если после установки Webmin выполнялась , например, установка сервера SSH, то для перевода его из категории неиспользуемых в категорию "Servers" (Серверы) необходимо выполнить обновление модулей (Refresh Modules в меню Webmin).
- **Search** - контекстный поиск в Webmin.
- **Refresh Modules** - обновить модули. Для того, чтобы изменения в составе модулей вступили в силу нужно завершить сеанс работы с Webmin (кнопка Logout) и повторно авторизоваться.
- **Logout** - выход из Webmin.

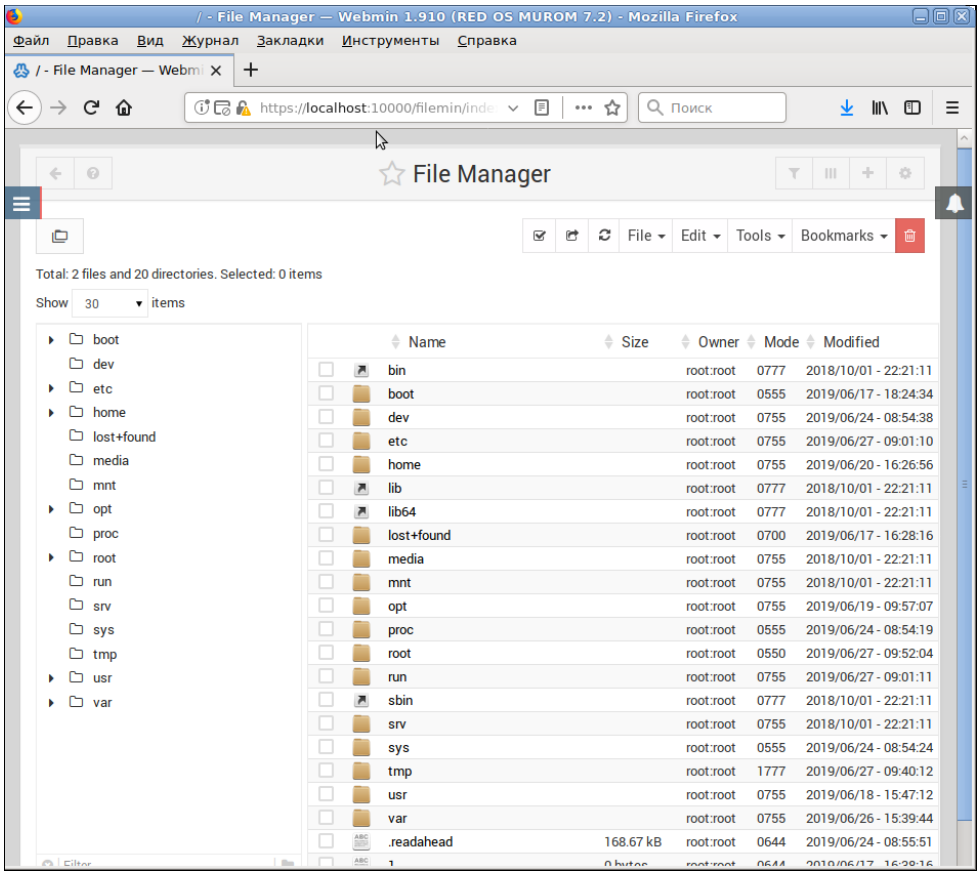
Для того, чтобы использовать Webmin с русским интерфейсом, нужно в меню **Webmin** выбрать пункт **Change Language and Theme** и установить персональный выбор **Personal choice** - русский язык **Russian (RU_UTF-8)**. После этого нажать кнопку **Make Changes**, выйти из Webmin и авторизоваться повторно.

При выполнении настроек с помощью Webmin необходимо учитывать тот факт, что в большинстве случаев, для того, чтобы установленные настройки вступили в силу, требуется нажатие кнопки "**Применить настройки**" (Apply Changes) и для некоторых сервисов - остановка и запуск. Многие модули Webmin, кроме собственных сценариев настроек позволяют выполнить прямое редактирование конфигурационных файлов, что позволяет выполнять настройки, не реализованные в текущей версии модуля.

Файловый менеджер

Файловый менеджер доступен по ссылке «**File Manager**» в разделе «**Прочее**» главного меню.

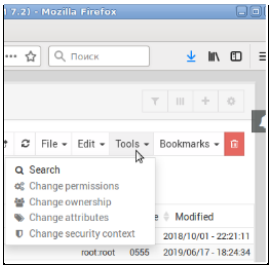
При открытии файлового менеджера отображается корневой каталог файловой системы. С помощью гиперссылок можно заходить в те или иные папки и открывать или загружать к себе на компьютер файлы.



Данный файловый менеджер позволяет выполнять лишь простейшие операции, такие как создание каталогов и текстовых файлов, редактирование текстовых файлов, создание архивов, распаковка архивов (при наличии, например, unzip), загрузка файлов с компьютера на сервер и наоборот.

Также стоит отметить возможность с помощью интерфейса файлового менеджера изменять владельцев файлов и папок и права доступа к ним.

Инструменты для изменения владельцев и прав доступны в меню «**Tools**».



Работа с консолью

Для работы с консолью служит страница «**Command Shell**» в разделе «**Прочее**». Поэтому, если необходим доступ к обычной консоли, Webmin предоставляет и такую возможность.

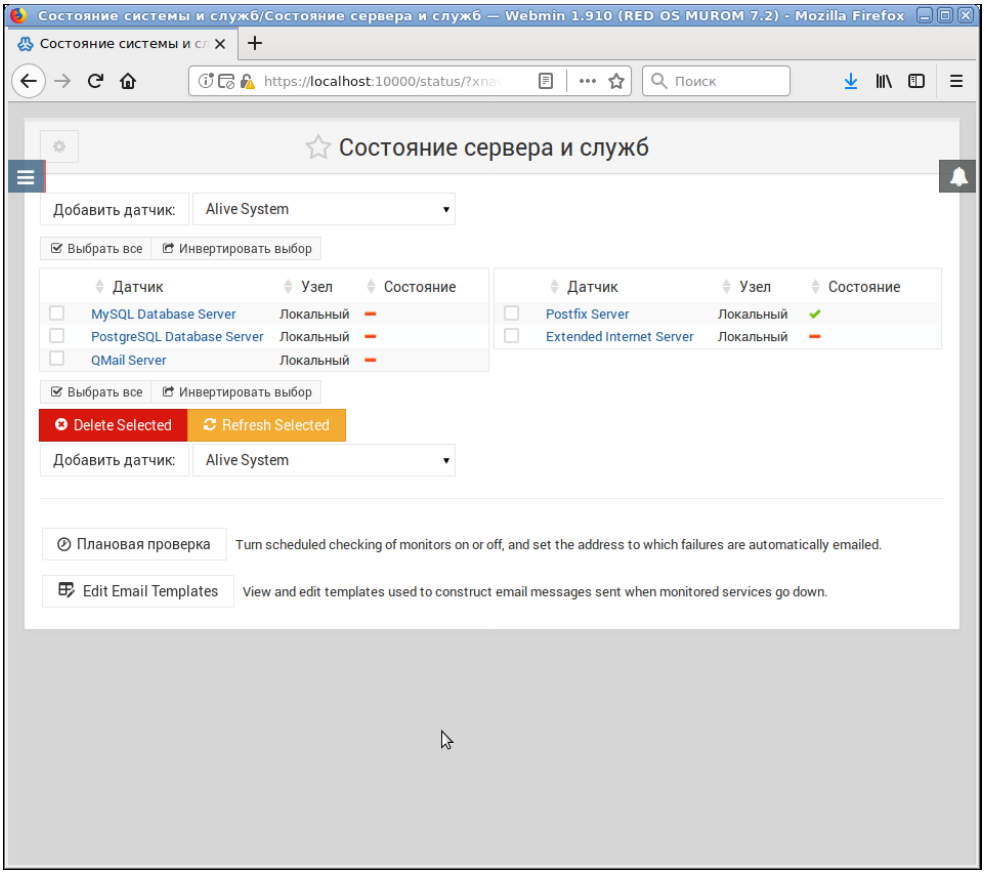
Состояние сервера и служб

Модуль доступен по ссылке «**Состояние сервера и служб**» в разделе «**Прочее**» главного меню.

Этот модуль позволяет отслеживать состояния выбранных серверов и запущенных демонов. С его помощью можно легко определить какие процессы выполняются должным образом или выявить те процессы, работа которых нарушена. Также можно сконфигурировать модуль таким образом, чтобы при проверке состояния сервера происходила отправка сообщения по e-mail или выполнялась какая-либо команда. Эта функция может быть полезна если система управляет серверами, от которых зависят другие люди, такими как Web или

DNS сервера.

Когда Вы входите в модуль «Состояние сервера и служб», то перед Вами появится главная страница, на которой отобразится таблица со всеми сконфигурированными мониторами. Несколько мониторов для общих серверов и служб будут определены по умолчанию, но Вы можете редактировать, удалять или добавлять их. На рисунке показан пример главной страницы модуля.



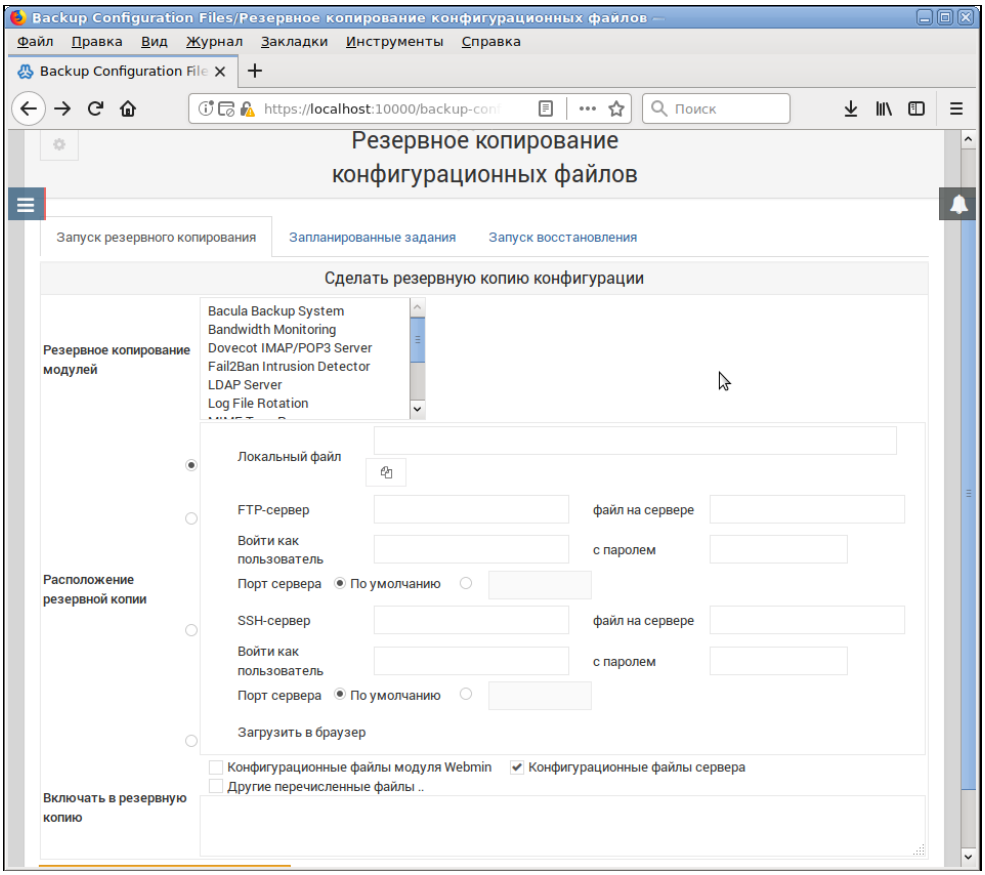
Каждый сервер или служба, за которым Вы хотите наблюдать, используя данный модуль, должен иметь свой монитор. Каждый монитор принадлежит к какому-либо типу, который указывает на то какие виды серверов им можно проверять, такие как Apache или BIND. Мониторы также имеют ряд дополнительных параметров, которые могут зависеть от типа. Модуль позволяет создавать множество различных типов мониторов, например, для проверки возможности запуска Sendmail или Squid путем наблюдения за интенсивностью использования сети или свободным дисковым пространством, или при помощи пингования или соединения с другим хостом.

Монитор может быть запущен, как в той же системе, в которой находится сам модуль, так и в другой системе, использующей Webmin. В последнем случае сервер должен быть определен в модуле **Webmin Server Index**. Также возможна проверка систем, на которых не установлен Webmin путем использования модулей типов remote TCP, HTTP и ping monitor.

По умолчанию состояния каждого монитора запрашиваются каждый раз при просмотре главной страницы модуля. Это может занять много времени, если запущено большое количество мониторов или происходит проверка статуса на удаленном хосте. Поэтому при необходимости в опциях конфигурации модуля можно установить запланированную проверку состояний. В этом случае при переходе на главную страницу будут отображаться состояния, полученные при проведении последней проверке.

Резервное копирование конфигурационных файлов

Резервное копирование и восстановление находится в разделе «**Система**».



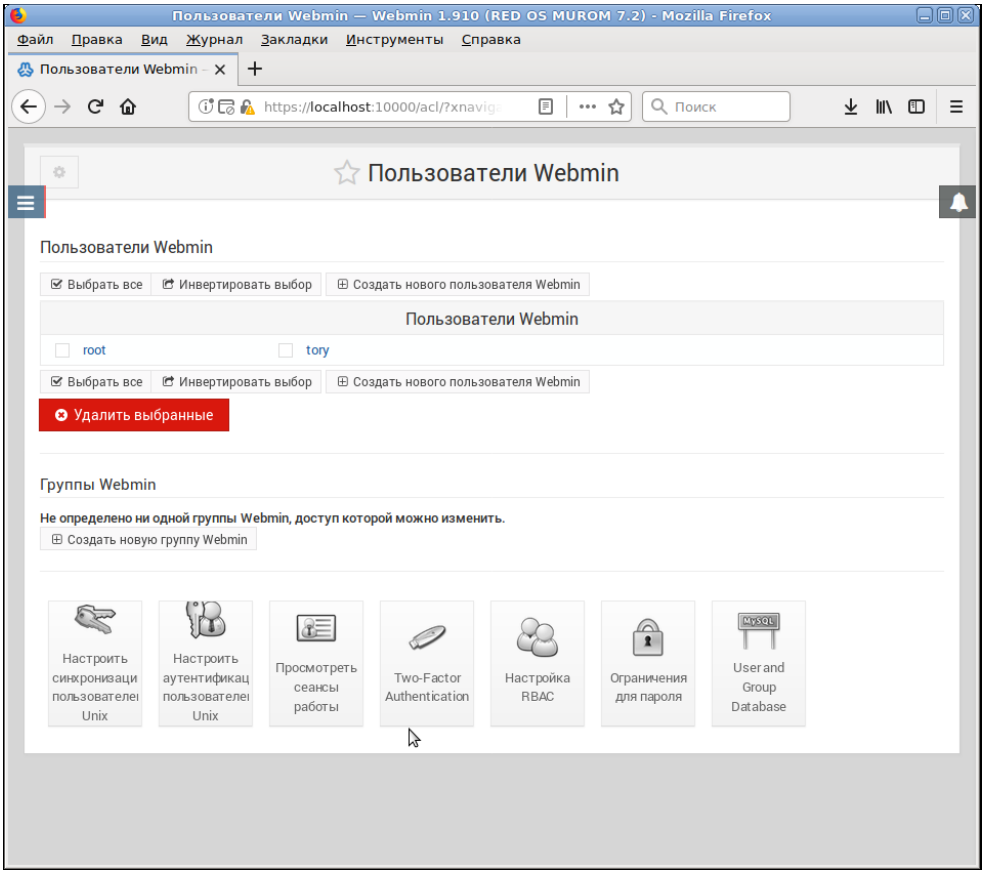
Здесь можно сделать резервное резервное копирование или восстановление, для этого следует выбрать необходимые модули, указать расположение резервной копии,и нажать кнопку «Запуск резервного копирования». Восстановление конфигурационных файлов проводится таким же образом.

Модуль «Пользователи в Webmin»

В Webmin, модуль **The Users and Groups** (Пользователи в Webmin), который находится в категории **System** (Система), может быть использован для создания, редактирования и удаления UNIX пользователей и групп в вашей системе. Нужно быть осторожным при использовании данного модуля для изменения существующих системных пользователей, таких как root и daemon, так как их изменение или удаление может вывести систему из строя. Некоторые пользователи имеют свою домашнюю директорию в корневом каталоге (/). Удаление таких пользователей вызовет удаление всех файлов вашей системы! Те пользователи, которых завели вы, обычно находятся в каталоге home.

В дополнение, к управлению UNIX пользователями в вашей системе, этот модуль также позволяет управлять пользователями, находящимися в других модулях. Например, Samba имеет свой собственный список пользователей и паролей, которые должны быть согласованы со списком паролей UNIX. Webmin может сделать это автоматически, используя функции других модулей, которые вызывают формы создания, редактирования и удаления пользователя. Однако, вы должны, разрешить это во всех модулях, которые хотите обновлять автоматически. По аналогии, в модуле также имеется опция согласования UNIX групп, например, с Samba группами. Но, поскольку эта функция работает только с Samba 3.0, которая все еще находится в стадии развития, это не включено в данную главу.

При открытии модуля, главная страница отображает в одной таблице список всех пользователей, а в другой – список всех групп, существующих в Вашей системе на данный момент. Если пользователей или групп слишком много, вместо таблиц отображаются небольшие формы, позволяющие выполнить поиск.



Bacula - резервное копирование системы

Bacula – пакет программ архитектуры «клиент-сервер» с открытым исходным кодом, предназначенный для создания резервных копий данных, находящихся на компьютерах с различными операционными системами, для восстановления и проверки хранящихся данных. Этот пакет имеет модульную архитектуру, легко масштабируется и может быть использован, как для небольшой локальной сети из нескольких компьютеров, так и для сети предприятия, состоящего из нескольких сотен компьютеров.

Система построена по технологии клиент-сервер, и для передачи данных использует протокол TCP. Резервные копии создаются в собственном, полностью открытом формате. Система резервирования данных Bacula состоит из четырёх основных элементов: *Director Daemon*, *Storage Daemon*, *File Daemon* и *Bacula Console*. Все эти элементы реализованы в виде самостоятельных приложений.

Director Daemon (DD) – это центральный элемент системы, осуществляющий управление её остальными компонентами. В его задачи входит управление процессом резервирования/восстановления данных, обеспечение интерфейса управления для администраторов и многое другое.

Storage Daemon (SD) – приложение, отвечающее за чтение/запись данных непосредственно на устройства хранения информации. Принимает управляющие команды от DD, а также резервируемые данные от/к File Daemon.

File Daemon (FD) – этот элемент ещё можно назвать Агентом. Ведь именно он работает в рамках операционной системы, данные которой необходимо резервировать. File Daemon выполняет всю рутину, осуществляя обращение к резервируемым файлам и их дальнейшую передачу к SD. Также на стороне FD выполняется шифрование резервных копий, если это определено конфигурацией.

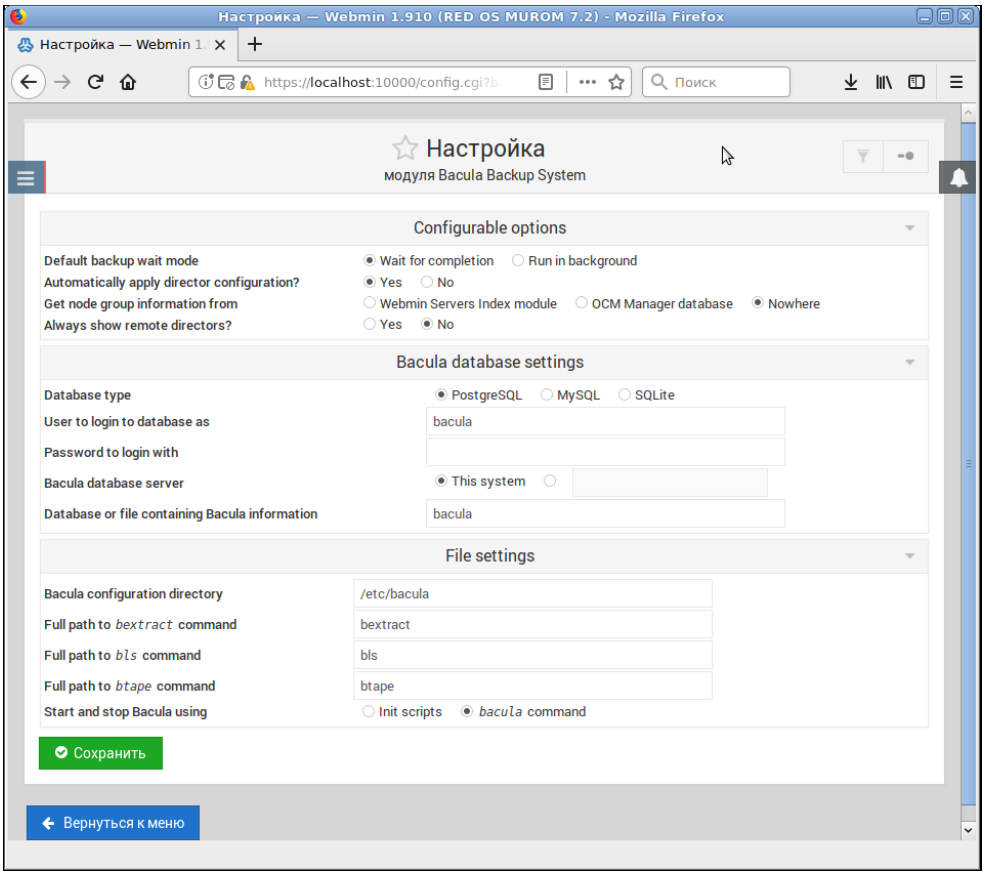
Bacula Console (BC) – интерфейс администратора системы. По своей сути, это командный интерпретатор для управления Bacula. Строго говоря, Bacula Console может быть расширена с помощью графических систем управления, которые, как правило, являются всего лишь надстройкой над BC. К таким системам можно отнести Tray Monitor и Bat. Первая устанавливается на компьютере администратора системы и осуществляет наблюдение за работой системы резервирования, а вторая обеспечивает возможность управления посредством графического интерфейса.

Bacula Catalog – база данных, в которой хранятся сведения обо всех зарезервированных файлах и их местонахождении в резервных копиях. Каталог необходим для обеспечения эффективной адресации к требуемым файлам. Поддерживаются MySql, PostgreSql и SqLite. Такое структурное деление позволяет организовать очень гибкую систему резервирования, когда Storage Daemon разворачивается на выделенном сервере с несколькими устройствами хранения данных. Также Bacula Director может управлять несколькими экземплярами SD, обеспечивая резервирование части данных на одно устройство хранения, а части – на другое.

Вы найдете системы резервного копирования Bacula в левой панели Webmin «**Система**» -> «**Bacula Backup System**». Если не находится там, попробуйте в разделе «**Неиспользуемые модули** (Un-used modules section)».

Нажмите на кнопку «**Резервное копирование системы Bacula**». Изначально сервер Bacula не включится автоматически. Для запуска Bacula сервера нажмите «**Настройки модуля**» - ссылку справа на странице «**Система резервного копирования Bacula**» (Bacula Backup System).

Заполняем все поля (вводим название БД, логин для нее и пользователя). Затем можно производить резервное копирование системы.



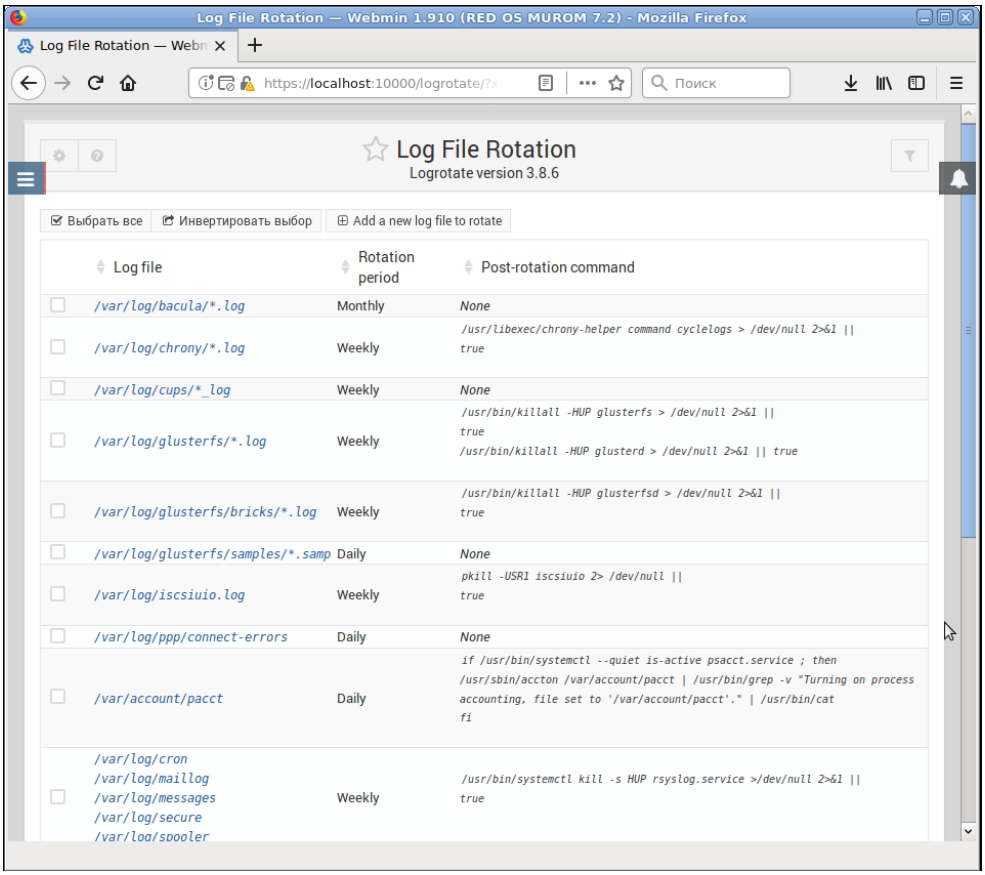
Ротация логов

В Linux, большинство сервисов и программ, которые работают в фоне, таких как Apache, Nginx, Postfix и других записывают информацию о своем состоянии, результатах работы и ошибках в лог файлы. Стандартное расположение логов или как их еще называют - журналов - в папке /var/log.

С помощью анализа логов вы можете понять что работает не так, почему произошла ошибка и как решить возникшую проблему. Но тут кроется одна проблема. Размер логов постоянно растет и они занимают все больше и больше места на диске, поэтому необходимо вовремя чистить логи и удалять устаревшие записи, чтобы они не мешали нормально работать.

Данная функция в Webmin предназначена для автоматизации обработки журналов. Она может выполнять с ними необходимые действия в зависимости от определенных условий и правил соответствия. Например, можно сжимать журналы в архив или отправлять на другой сервер когда они достигают определенного размера, возраста, или других параметров.

Вы найдете ротацию логов в левой панели Webmin консоли под **Система** -> **Log File Rotation**.

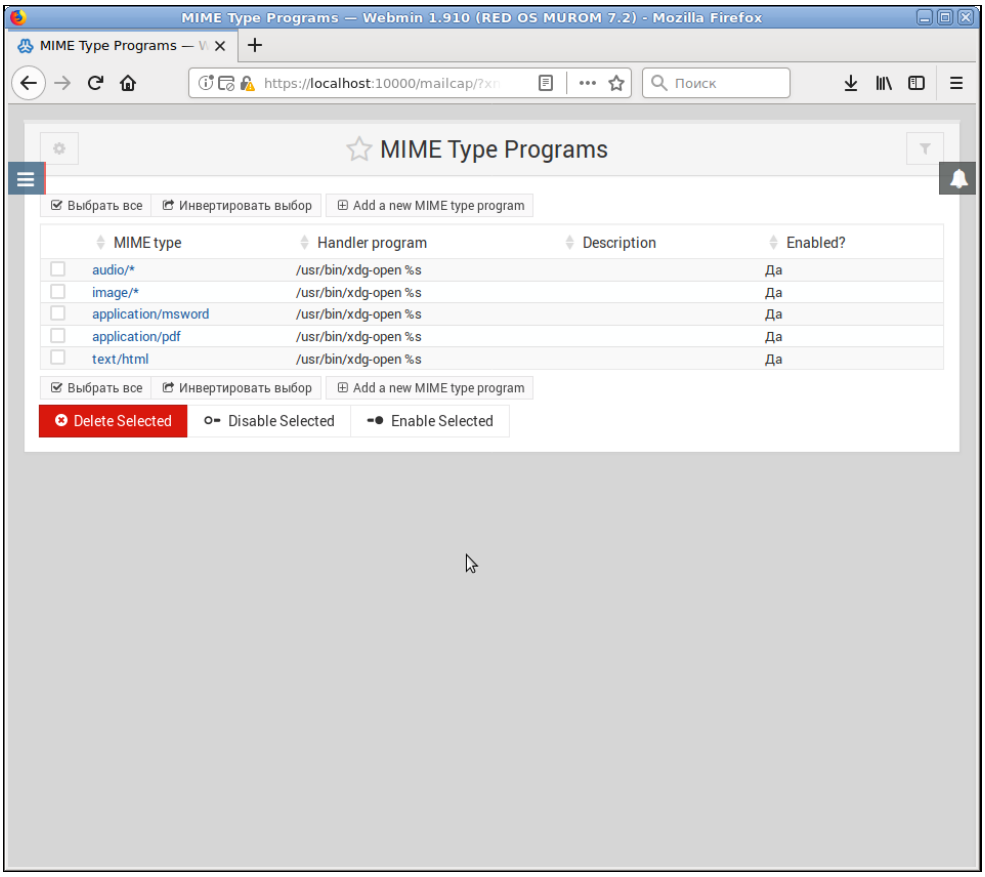


Проверку условий можно настроить ежедневно, еженедельно или ежемесячно. Это позволяет создать схему ротации логов, удобную именно для вас и вашего сервера. Также ротация логов может быть полезна на домашнем компьютере, но здесь она не так важна как на серверах, где только в логи Apache могут записываться до сотен тысяч строк ежедневно.

Добавление и редактирование MIME типов

MIME типы - это способ, который использует Apache, почтовые клиенты и многие другие программы для определения типа файлов или типа данных. MIME тип содержит два слова разделенные косой чертой. Например, text/html или video/mpeg. Как видно из примеров, первое слово это категория, а второе - реальное название типа содержимого.

Каждый ответ сервера Apache содержит запись о MIME типе, поэтому браузер "понимает" как показывать то или иное содержимое.



Apache имеет глобальный список MIME типов. Чтобы отредактировать его проделайте следующие шаги:

1. На главной странице модуля нажмите кнопку MIME Types(MIME типы).
2. Нажмите Add a new MIME type(Добавить новый MIME тип).
3. Введите имя вида text/foo в поле MIME type(MIME тип).
4. Введите расширения файлов, которые будут ассоциированы с этим типом, например .foo и .fo в поле Extensions(Расширения). Удостоверьтесь, что ни один другой MIME тип не связан с этими расширениями.
5. Нажмите кнопку Save(Сохранить).
6. Нажмите Apply Changes(Применить изменения), чтобы изменения вступили в силу.

MIME типы могут быть настроены для всех виртуальных серверов, для отдельного виртуального сервера или для отдельного каталога. Для этого выберите Сервер по умолчанию, отдельный виртуальный сервер или каталог соответственно.

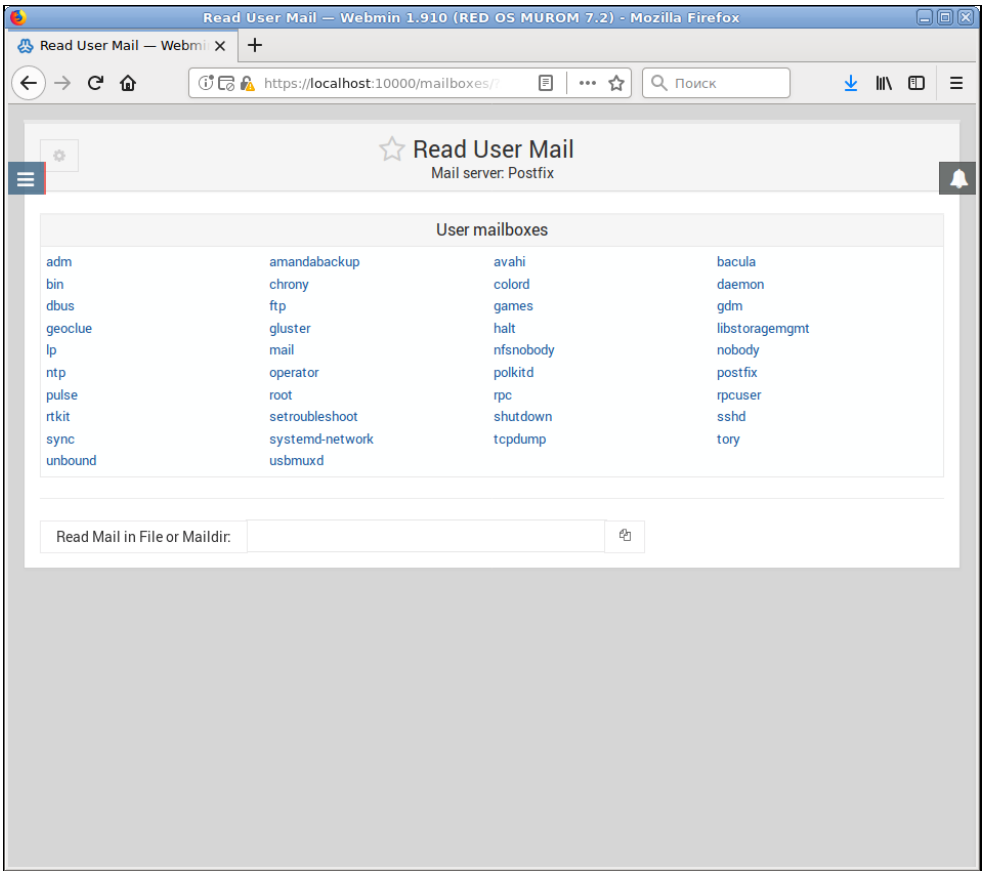
Чтобы отредактировать MIME тип или удалить его нажмите на его имя. После внесения изменений нажмите Save(Сохранить) и Apply Changes(Применить изменения). Чтобы удалить нажмите Delete(Удалить) на форме редактирования, затем Apply changes(Применить изменения), чтобы изменения вступили в силу.

На странице MIME типов есть очень полезное поле Default MIME тип(MIME тип по умолчанию). Если оно задано, то любое содержимое, которое Apache не может определить, будет отдано с этим значением.

Read User Mail

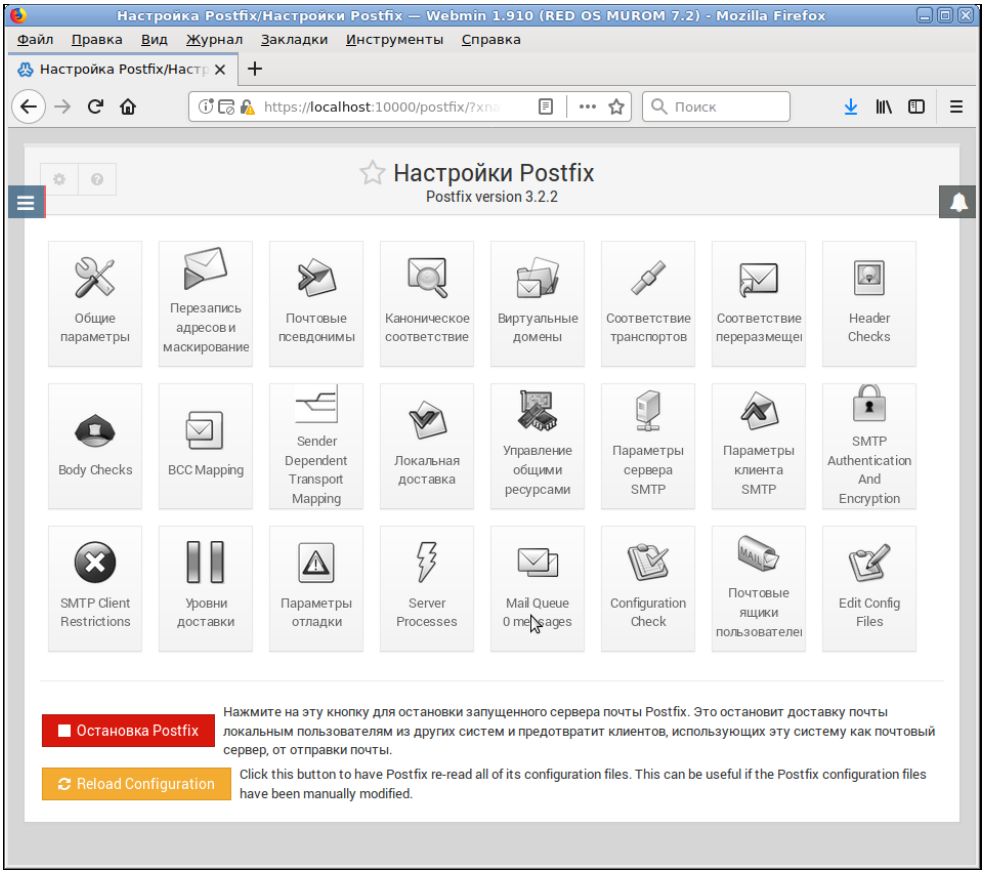
Webmin включает в себя очень полезный модуль, который позволяет администратору читать сообщения электронной почты любого пользователя. Модуль **Read User Mail** на самом деле является простым почтовым клиентом для доступа к почтовым ящикам пользователей почти для всех пользователей на сервере, и это один из стандартных модулей, установленных по умолчанию Webmin.

Выберите пользователя, у которого Вы хотите прочитать письма, или введите путь к почтовому файлу или MailDir, который Вы хотите прочитать. В почтовом ящике вы можете выбрать чтение писем из других папок.



Настройки Postfix

Postfix - это эффективный и многофункциональный почтовый сервер. Он был предназначен, чтобы быть заменой для популярного сервера. В то время как Sendmail был самым популярным почтовым сервером в течение многих лет, популярность Postfix, вероятно, выросла за пределы Sendmail из-за его простой конфигурации, исторически безопасной реализации и высокопроизводительной архитектуры. Кроме того, поскольку Postfix предназначен для внешнего поведения, как sendmail, это в основном замена для более старого, большого и медленного почтового сервера.



Настройка Postfix включает в себя следующие возможности:

1) Общие параметры

Страница общие параметры настраивает ряд параметров, касающихся общего поведения Postfix. В частности, здесь настраиваются большинство параметров конфигурации, влияющих на всех пользователей и все сообщения. Postfix, придерживаясь своей философии простоты, обычно требует всего нескольких изменений файла конфигурации, чтобы почтовый сервер работал эффективно и безопасно.

2) Перезапись адресов и маскирование

Postfix предлагает относительно простую в использовании и гибкую систему перезаписи адресов, позволяющую ей действовать как почтовый шлюз для большой сети или как шлюз между устаревшими почтовыми системами и интернетом в целом Переписывание адресов лежит в основе почтовой системы Postfix. Postfix переписывает адреса для самых разных целей. Некоторые из них просто косметические, а некоторые необходимы для доставки правильно отформатированной почты в нужное место назначения. Примерами переопределения адресов в постфикс являются:

- Преобразование неполного адреса в полный адрес. Например, превратить "имя пользователя" в "username@example.com" или преобразование "имя_пользователя@имя_хоста" в "username@hostname.example.com".

- Замена адреса эквивалентным адресом. Например, заменить "username@example.com" by "firstname.lastname@example.com" при отправке почты, и сделать обратное преобразование при получении почты.

- Замена внутреннего адреса на внешний адрес. Например, замените " username@localdomain.локальный "by" isp-аккаунт@isp.пример " при отправке почты с домашнего компьютера в интернет.

- Замена адреса несколькими адресами. Например, замените адрес псевдонима адресами, перечисленными под этим псевдонимом.

- Определение, как и куда доставлять почту по определенному адресу. Например, доставить почту для "username@example.com" с помощью агента доставки smtp на хосты, перечисленные в DNS в качестве почтовых серверов для домена "example.com".

3) Почтовые псевдонимы

Почтовые псевдонимы обеспечивают средства для перенаправления почты для локальных получателей. В частности, он позволяет доставлять почту, предназначенную для нескольких разных адресов, в один почтовый ящик. Обычно для этого используется прямая почта для пользователей, таких как postmaster, к реальному человеку. Эта страница разделена на две части. Верхний раздел с надписью Aliases Options содержит расположение и формат файлов псевдонимов, которые Postfix должен использовать для создания своих баз данных псевдонимов, и указывает тип используемой базы данных. В нижнем разделе представлен список всех настроенных псевдонимов в системе и сопоставление псевдонимов.

4)Каноническое соответствие

Каноническое сопоставление в Postfix используется для изменения почты во входящей очереди и изменяет как заголовки сообщений, так и информацию о конверте сообщения для локальной или удаленной почты. Это сопоставление может быть полезно для замены имен входа на Firstname, адреса стиля Lastname или для очистки нечетных адресов, созданных устаревшими почтовыми системами.

5) Виртуальные домены

Функциональность виртуальных доменов в Postfix предоставляет возможность перенаправлять сообщения в разные места, изменяя адрес конверта сообщения. Адрес заголовка не изменяется при сопоставлении виртуального домена. Хотя некоторые функции виртуальных доменов перекрываются с функциями, доступными в псевдонимах, виртуальные домены могут использоваться для локальных или нелокальных адресов, а псевдонимы могут использоваться только для локальных адресов.

6) Соответствие транспортов

Термин транспорт относится к механизму, используемому для доставки части электронной почты. В частности, SMTP и UUCP - это почтовые транспорты, поддерживаемые Postfix. Транспортное сопоставление может быть использовано для ряда целей, в том числе SMTP для UUCP gatewaying, работы Postfix на брандмауэре с переадресацией на внутренний почтовый сервер и т. д.

7) Соответствие переразмещения

С помощью этой опции можно уведомить отправителей, если локальный пользователь переехал на другой адрес. Например, если пользователь покидает организацию, но по-прежнему время от времени получает почту на свой локальный адрес, может быть удобно уведомить любого отправителя почты пользователю о переезде и новой контактной информации для этого пользователя.

8) Локальная доставка

Локальная доставка -это то, что Postfix делает, когда он достигает конца всего своего списка сопоставлений и элементов управления доступом и все еще находит, что сообщение разрешено и предназначено для пользователя на локальной машине (т.е. сопоставление может потенциально отправить сообщение в другое место для окончательной доставки, поэтому все сопоставления, а также различные проверки доступа выполняются до достижения этого этапа). На этой странице настраивается ряд параметров, связанных с тем, как Postfix обрабатывает доставку почты для локальных пользователей.

9) Управление общими ресурсами

Эта страница предоставляет доступ к различным ограничениям памяти и процессов для Постфиксных процессов. Редко требуется изменять значения на этой странице, за исключением высоконагруженных серверов или машин с очень низким ресурсом.

10) Параметры сервера SMTP

Эта страница настраивает большинство параметров, которые непосредственно влияют на поведение части сервера SMTP Postfix, в частности части Postfix, которые влияют на поведение сервера по отношению к клиенту SMTP, который подключается к серверу.

11) Параметры клиента SMTP

Параметры SMTP-клиента настраивают поведение Postfix при работе с другими почтовыми серверами в качестве клиента, т.е. при отправке почты от имени пользователя. Эта часть конфигурации в первую очередь определяет, как сервер будет реагировать на определенные ошибки.

12) Уровни доставки

Эта страница содержит параметры для установки скорости по умолчанию и ограничений параллелизма для всех компонентов Postfix. Эти скорости обычно могут быть переопределены в их соответствующих разделах конфигурации.

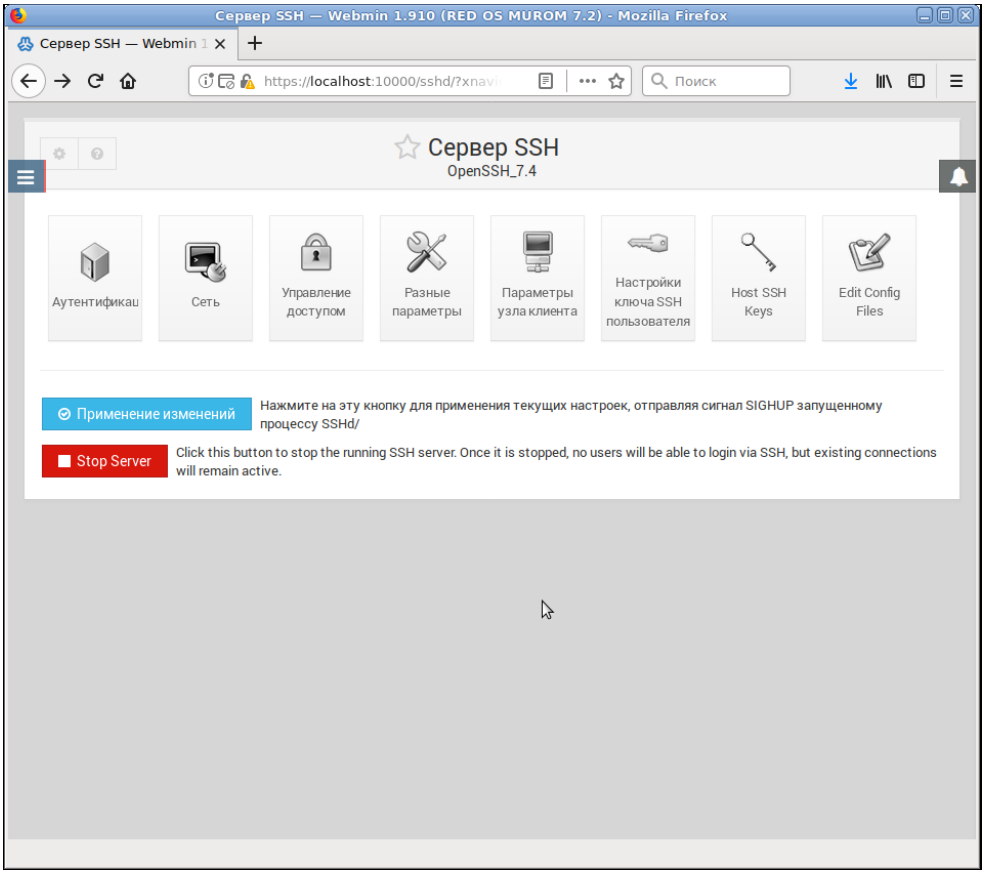
13) Параметры отладки

Postfix имеет два уровня ведения журнала. Первый уровень-обычный почтовый журнал, который сообщает обо всех обычных почтовых действиях, таких как полученная и отправленная почта, ошибки сервера, остановки и запуски. Второй уровень является более подробным и может быть настроен на ведение журнала действий, связанных с конкретными SMTP-клиентами, именами хостов или адресами. Эта страница содержит конфигурацию для второго уровня ведения журнала.

SSH Сервер

Настройки сервера SSH можно найти выбрав «**Службы**» → «**Сервер SSH**» в главном меню.

На главной странице всегда отображаются шесть значков, под каждым из которых находится форма, содержащая поля для настройки параметров, связанных с какой-либо категорией, например, аутентификация или сеть. В верхней части отображается реализация и версия установленного SSH, так что вы можете увидеть, какие из инструкций в этой главе относятся к вашей системе. В нижней части находится кнопка с надписью «**Применить изменения**», которые при нажатии сигнализируют SSH-серверу для повторного чтения файла конфигурации. Никакие изменения, внесенные в модуль вступят в силу, пока вы не нажмете эту кнопку.



1) Аутентификация

У всех реализаций SSH есть опции, связанные с тем, как клиенты аутентифицируются и сообщения, отображаемые им после входа в систему. В частности, вы можете разрешить или запретить аутентификацию по имени пользователя и паролю или по имени пользователя и сертификату, остановить вход в систему пользователя root и контролировать, являются ли файлы rrgin в стиле rlogin. Точные параметры довольно сильно различаются между версиями SSH, поэтому, что возможно с OpenSSH, может не быть, если вы используете коммерческий сервер SSH.

2) Управление доступом

По умолчанию любому пользователю Unix будет разрешено удаленно входить на сервер SSH в вашей системе или использовать его для загрузки и скачивания файлов. В системе почтового сервера или на том, на котором размещаются веб-сайты, это может быть неуместно - вместо этого вы можете разрешить большинству пользователей входить на серверы POP3, FTP или Usermin. Хотя этого можно добиться, предоставив им оболочку типа / bin / false, это может вызвать другие проблемы с заданиями пользователя Cron или At.

3) Сеть

SSH-сервер имеет несколько параметров, которые позволяют настроить IP-адрес, который он слушает, порт, который он использует, и различные параметры, связанные с протоколом.

4) Параметры узла клиента

Несмотря на то, что этот модуль предназначен в основном для настройки SSH-сервера, он также позволяет устанавливать параметры, которые применяются ко всем клиентским подключениям, выполненным из вашей системы с помощью команд ssh и scp. Параметры могут быть установлены для соединений со всеми хостами или только с определенным. Вы можете установить порт для подключения, протокол и локальный и удаленный порты для пересылки. Настройки, сделанные в этом модуле применяются ко всем пользователям в системе, но могут быть переопределены для отдельных пользователей, редактировать ~/.файлы ssh / config. Это можно сделать вручную или с помощью Usermin, который имеет клиентский модуль SSH с идентичным интерфейсом, описанным здесь для редактирования глобальных параметров клиента. Многие настройки не имеет большого смысла устанавливать для всех пользователей, хотя это можно сделать с помощью Webmin. По этой причине инструкции в этом разделе охватывают только поля, полезные на глобальном уровне.

5) Настройки ключа SSH пользователя

Прежде чем пользователь Unix сможет использовать проверку подлинности сертификата для входа на сервер SSH, он должен создать закрытый ключ с помощью команды ssh-keygen. Этот модуль можно настроить для работы с модулем пользователи и группы, чтобы выполнить эту команду для всех вновь созданных пользователей. Если в вашей сети используются домашние каталоги, смонтированные на NFS,это позволит новым пользователям входить на другие хосты без необходимости вводить пароль без дополнительной настройки.

6) Разные параметры

Эта страница содержит параметры, которые не входят ни в одну из других категорий. Некоторые из менее очевидных вариантов, но полезные :

- Разрешить пересылку соединения X11?

  Если установлено значение Да, пользователи, которые делают SSH-вход с машины Unix, смогут запускать X-приложения на сервере и туннелировать X-соединение обратно через SSH-соединение на свой локальный дисплей.

- Устройство для ведения системного журнала

  Средство системного журнала, которое используется для регистрации ошибок и информационных сообщений с сервера SSH. Это можно использовать в сочетании с модулем системных журналов для управления тем, в какой файл записываются SSH-сообщения.

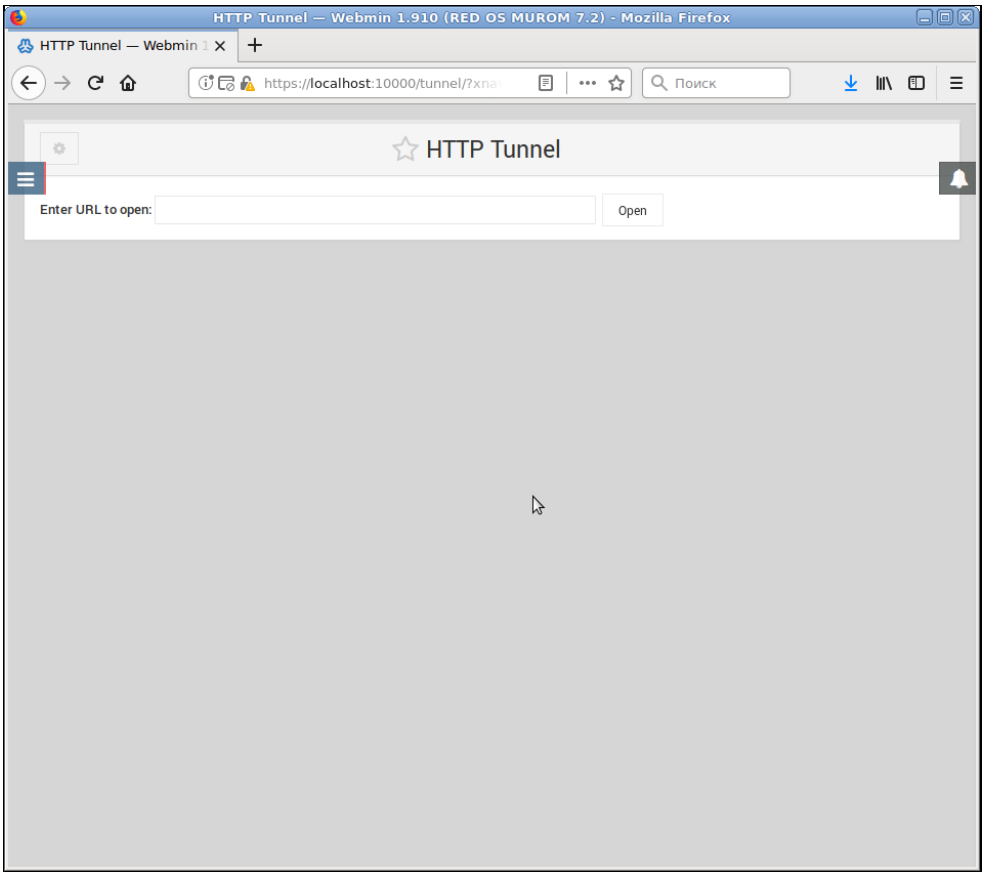
- Интервал регенерации ключа сервера

  Как часто сервер SSH повторно генерирует ключ, используемый для шифрования соединений.

HTTP Tunnel

Модуль доступен по ссылке «**HTTP Tunnel**» в разделе «**Прочее**» главного меню.

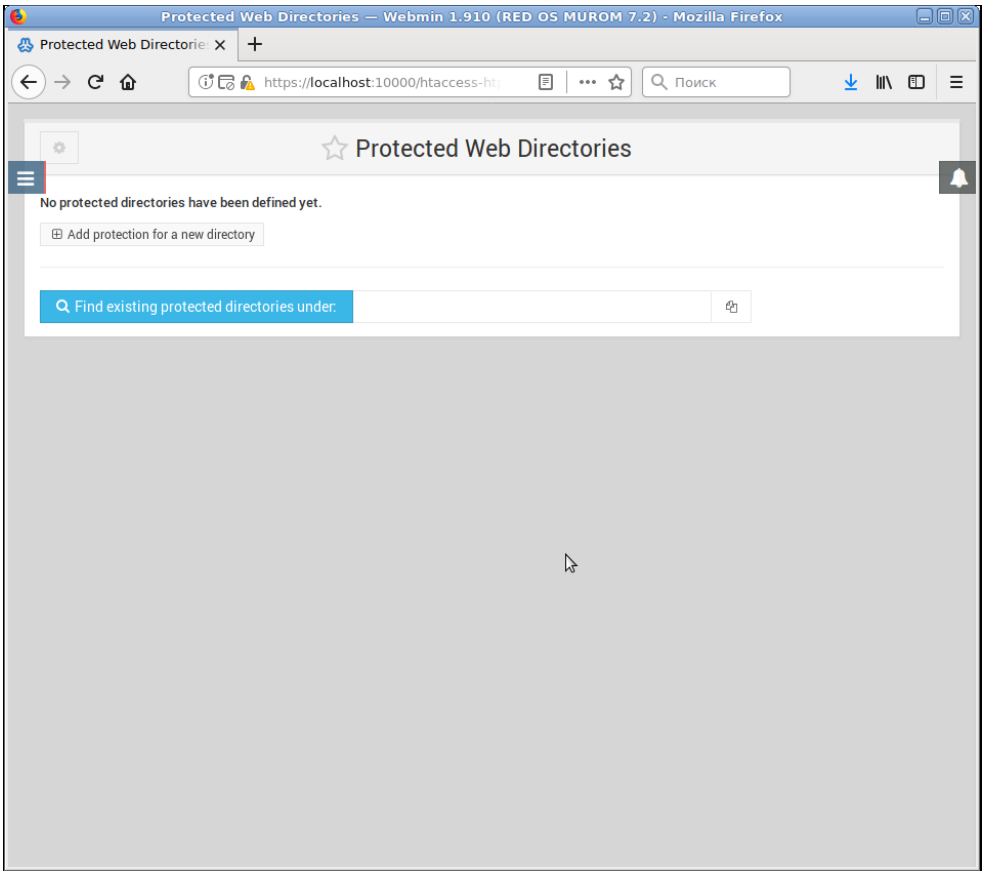
Модуль туннеля HTTP позволяет системному администратору создать значок в Usermin, который фактически соединяет пользователей с другим веб-сервером. Однако, вместо того, чтобы просто ссылаться на какой-либо URL-адрес, все запросы туннелируются через Usermin, и поэтому не появляются из браузера пользователя вообще. С точки зрения безопасности он абсолютно безвреден.



Protected Web Directories

Модуль доступен по ссылке «**Protected Web Directories**» в разделе «**Прочее**» главного меню.

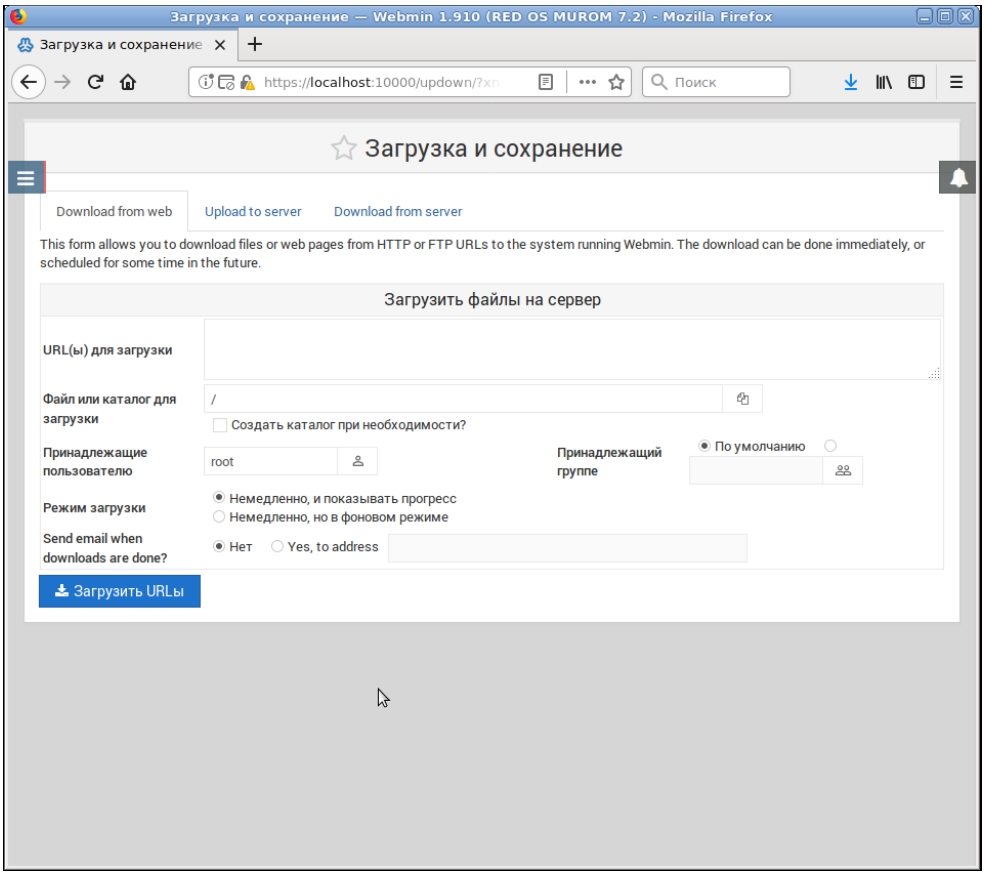
Модуль защищенных веб-каталогов позволяет управлять защищенными веб-каталогами **.htaccess** и **.htpasswd** файлов.



Загрузка и сохранение

Модуль доступен по ссылке «**Загрузка и сохранение**» в разделе «**Прочее**» главного меню.

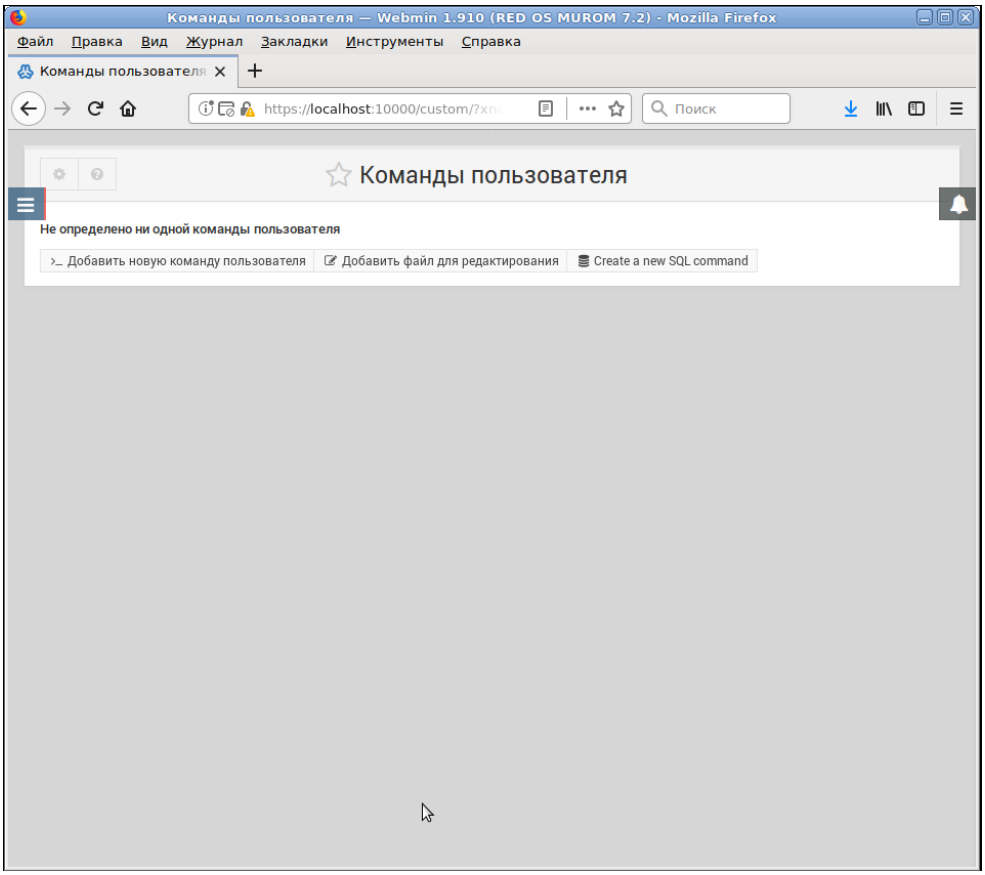
Эта форма позволяет загружать файлы или веб-страницы с URL-адресов HTTP или FTP в систему под управлением Webmin. Загрузка может быть выполнена немедленно или запланирована на некоторое время в будущем.



Команды пользователя

Вы найдете пункт «Команды пользователя» в левой панели Webmin консоли под **Прочее** -> **Команды пользователя**.

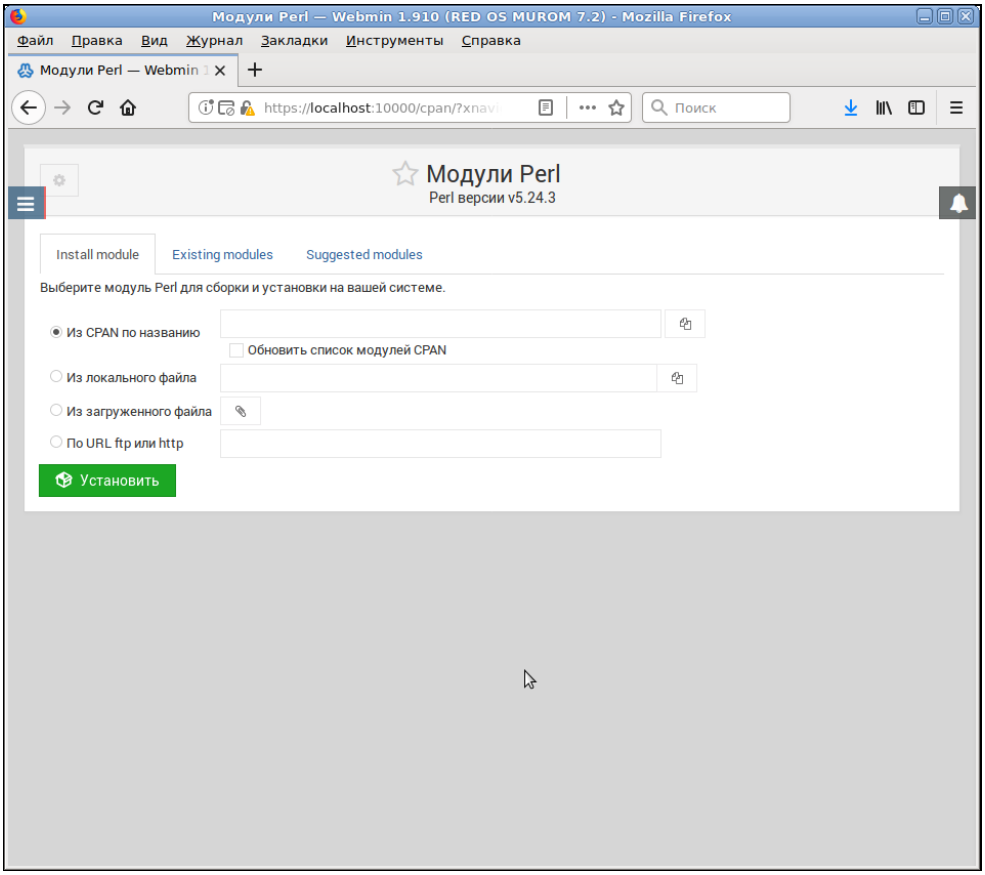
Позволяет неподготовленным пользователям выполнять команды или скрипты нажатием одной кнопки. Админу достаточно создать команду, заполнив соответствующие поля (прописать команду, задать параметры, пользователя, от имени которого будет выполняться команда, добавить описание и пр.). Здесь же во вкладке “**Прочее**” найдете и менеджер файлов (требует поддержки JAVA), который позволит получить доступ к файлам на удаленном компьютере в удобной графической оболочке.



Модули Perl

В категории другие в Webmin находится модуль **Perl Modules**, который можно использовать для просмотра, установки и удаления модулей Perl из вашей системы. Когда Вы вводите его, главная страница перечисляет все модули, которые в настоящее время установлены. Для каждого модуля отображается имя, краткое описание, дата установки и количество подмодулей. Подмодули - это термин Webmin для модулей Perl, включенных в tar дистрибутива.файл GZ вместе с основным модулем.

Поскольку Perl ведет себя одинаково во всех версиях Unix, этот модуль Webmin имеет одинаковый пользовательский интерфейс и функциональность во всех операционных системах.



Bandwidth Monitoring

Модуль мониторинга полосы пропускания может использоваться для создания простых отчетов об использовании полосы пропускания портом, хостом, протоколом и временем для трафика, отправляемого или маршрутизируемого через вашу систему. Это полезно как для автономных хостов, так и для тех, которые действуют как шлюз (возможно, с NAT) для сети.

Прежде чем его можно будет использовать, модуль должен настроить несколько правил брандмауэра и запись системного журнала для захвата трафика, отправленного и полученного через вашу систему. Во время установки необходимо выбрать внешний сетевой интерфейс системы, на котором будет отслеживаться трафик. Обычно это интерфейс PPP, используемый для подключения dialup или ADSL, или интерфейс Ethernet, подключенный к кабельному модему или вышестоящему маршрутизатору.

После захвата трафика продолжительностью не менее часа модуль может использоваться для создания отчетов, суммирующих трафик по одной из следующих категорий :

- *Час*. Дата и час получения данных.
- *День*. Дата, на которую эти данные были получены.
- *Хост*. Узел во внутренней сети или узел брандмауэра, который отправил или получил данные.
- *Внутренний порт*. Порт на внутреннем узле или узле брандмауэра, на который были отправлены данные. Этот режим полезен для определения объема трафика, генерируемого соединениями с каждым из серверов.
- *Внешний порт*. Порт на каком-либо сервере вне сети, на который были отправлены данные. С его помощью можно определить, к каким службам обращаются пользователи Сети.
- *Порт*. Как внутренние, так и внешние порты. Полезно для сравнения всего использования сети по типу службы.

Можно также ограничить отчет выбором узла, порта или протокола. Хост может быть введен по IP-адресу, имени хоста или сетевому адресу, например 192.168.1.0. Порт может быть введен по имени или номеру и будет соответствовать TCP и UDP.

Отчет также может быть ограничен трафиком, собранным между выбранными часами, используя поля для трафика после и для трафика до. Поскольку трафик суммируется по часам, нельзя ограничить отчет с большей точностью, чем по часам.

TCP Wrappers

Модуль TCP Wrappers использует простой язык управления доступом, основанный на шаблонах клиента (имя хоста/адрес, имя пользователя) и сервера (имя процесса, имя хоста/адрес).

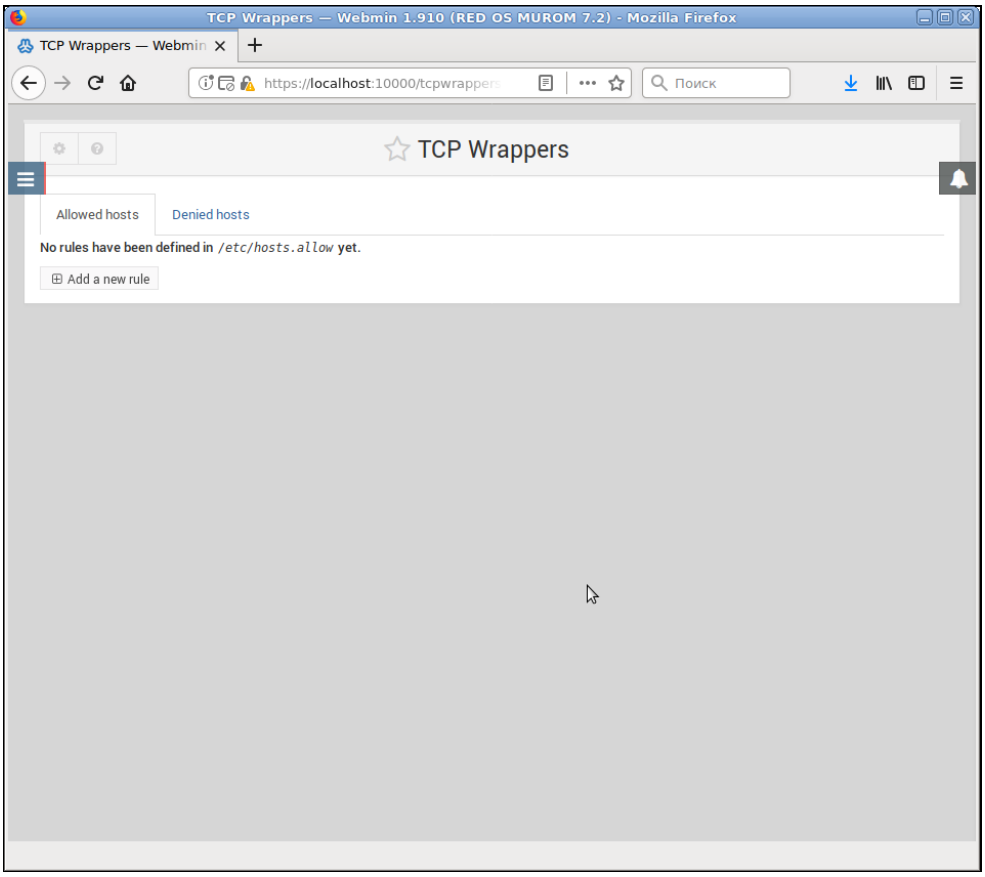
Расширенная версия языка управления доступом описана в документе **hosts_options**. Расширения включаются во время сборки программы с помощью команды - **PROCESS_OPTIONS**.

Контроль доступа к файлам

Программное обеспечение для контроля доступа использует шаблоны, описанные в двух файлах - **hosts.allow** и **hosts.deny**. Поиск шаблона будет остановлен при первом совпадении. Таким образом, вся цепочка будет выглядеть следующим образом:

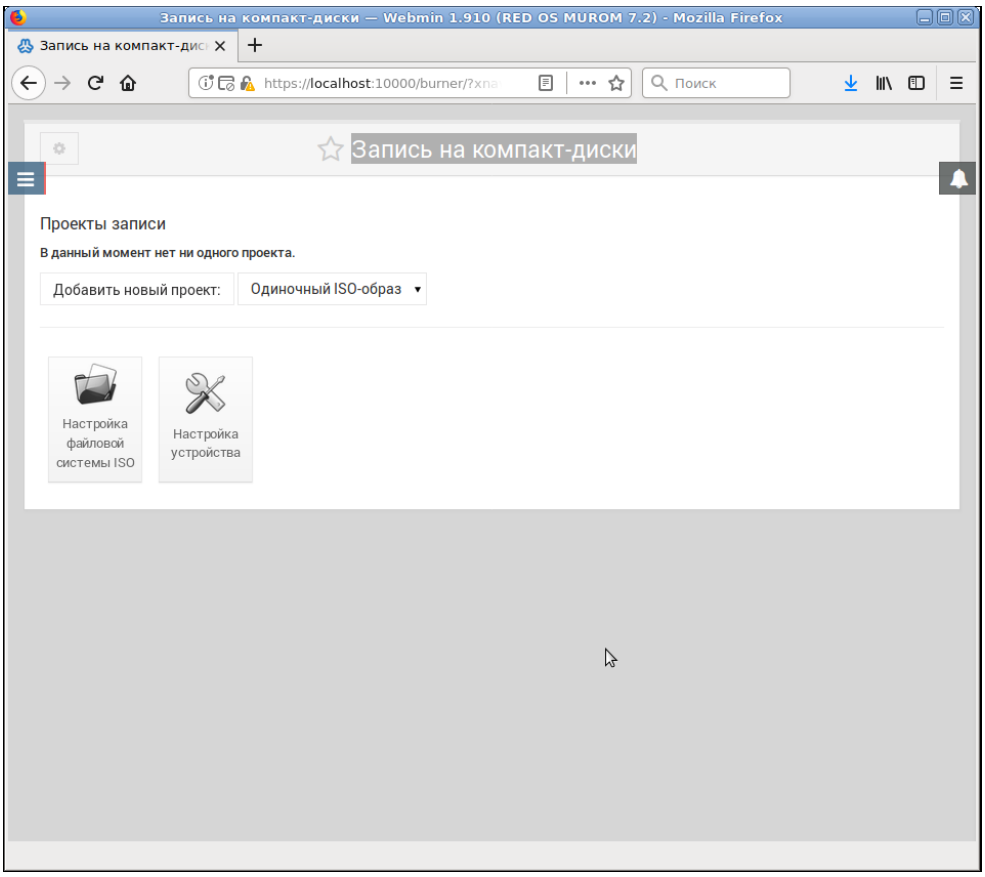
- сначала поиск осуществляется в файле **/etc/hosts.allow**. При совпадении пары (демон, клиент) доступ будет предоставлен;
- в случае, если в файле hosts.allow пара не найдена, поиск будет осуществлён в файле **/etc/hosts.deny**. Если поиск найдёт совпадение - доступ будет запрещён;
- в том случае, если поиск не найдёт совпадений в обоих файлах - доступ будет предоставлен.

В том случае если данных конфигурационных файлов в каталоге /etc не существует, они обрабатываются как "пустые". Таким образом, управление доступом можно отключить.



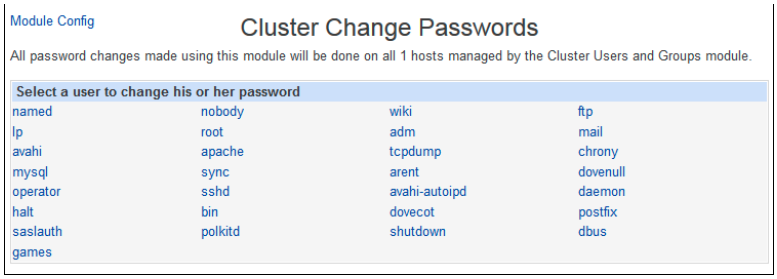
Запись на компакт-диски

Модуль диски находится в категории «**Оборудование**». Он предоставляет вам веб-интерфейс к CD / DVD burner, подключенному к Webmin-хосту.



Cluster Change Passwords

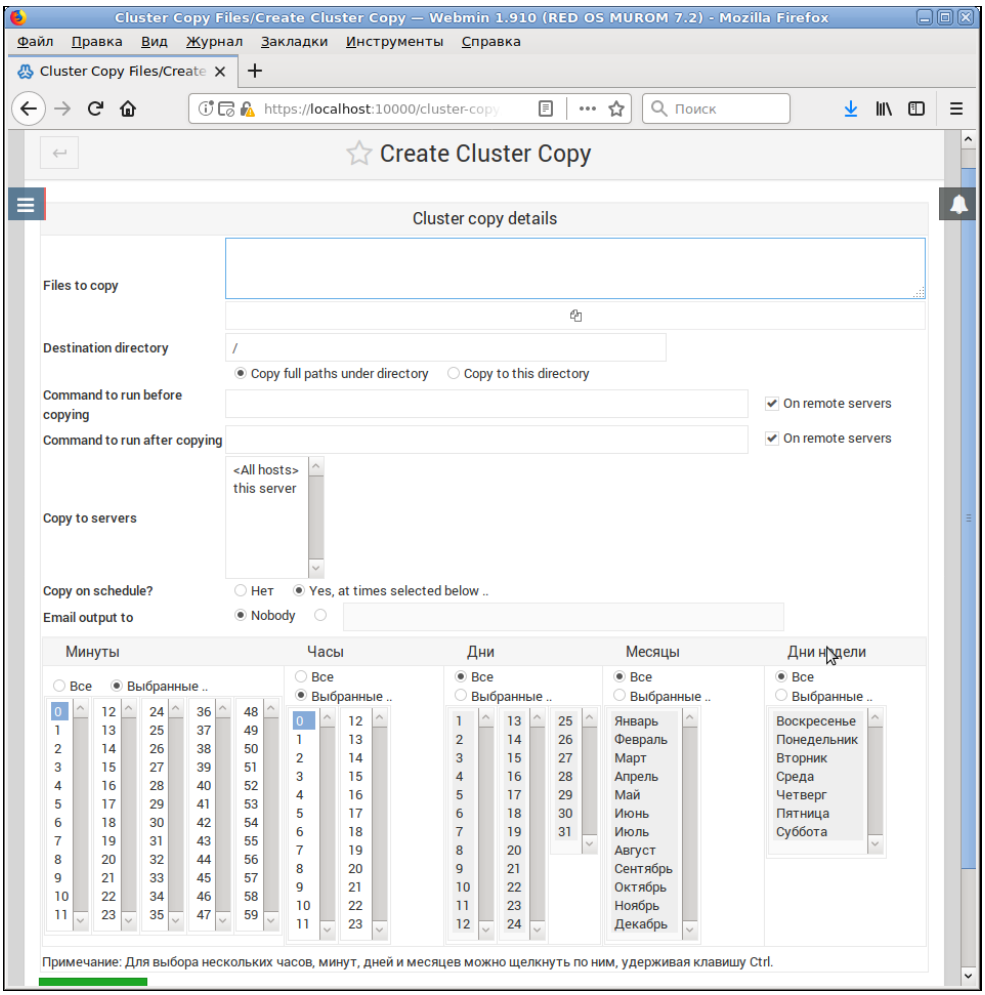
Модуль изменение паролей кластера-это способ изменить все пароли в кластере сразу.



Cluster Copy Files

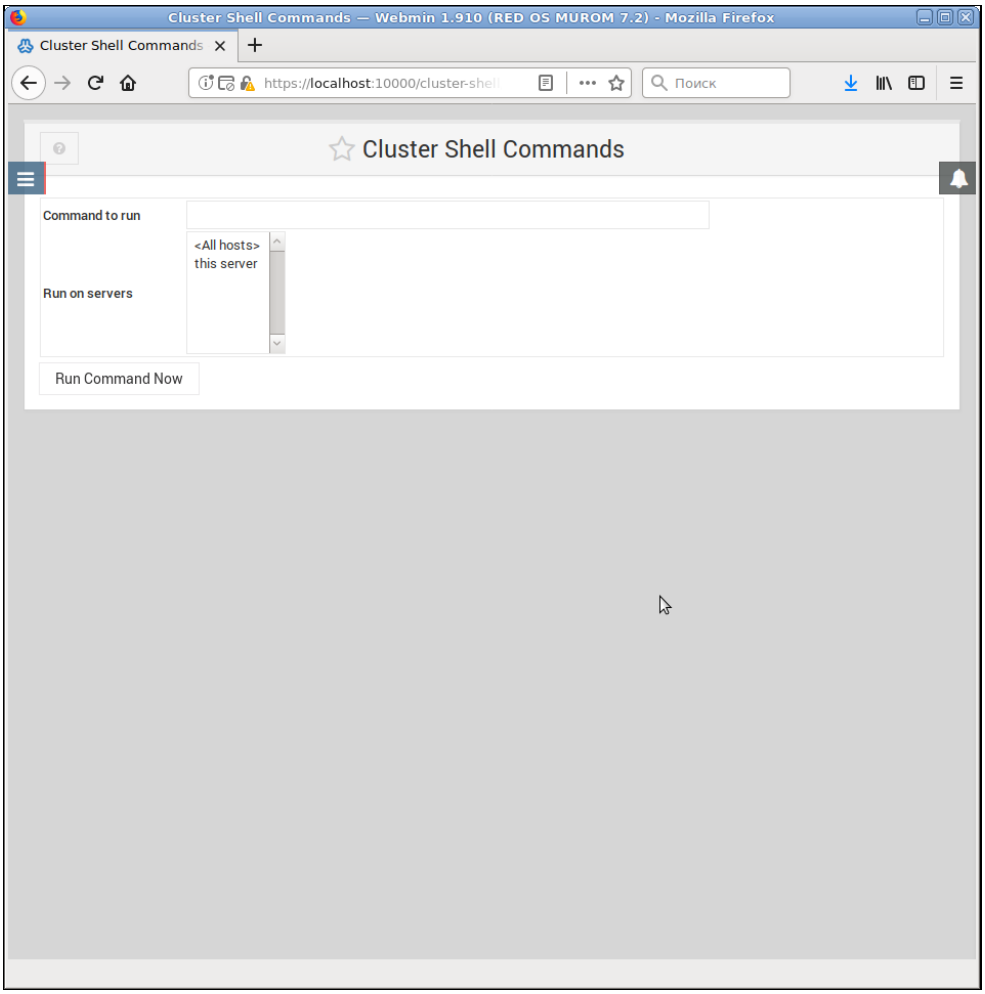
Модуль «**Копирование файлов кластера**» позволяет настроить запланированную передачу файлов с главного сервера на другие серверы кластера Webmin. Это может быть полезно для распространения файлов, таких как /etc/hosts, httpd.conf и другие, для которых нет сетевого протокола, такого как NIS или LDAP.

На главной странице модуля перечислены все определенные запланированные копии, и есть ссылка для создания новой. Для каждой копии можно определить исходные файлы, каталог назначения, целевые серверы и время выполнения. Целевые объекты должны быть сначала созданы в модуле индекса серверов Webmin с логином и паролем.



Cluster Shell Commands

Модуль команды оболочки кластера похож на командную оболочку, но позволяет выполнять простые команды на нескольких серверах одновременно, а не только на этом сервере. На главной странице можно ввести команду для запуска (или выбрать старую) и выбрать один или несколько серверов или групп для ее выполнения. В списке будут отображаться только серверы, созданные в модуле Webmin Servers Index с логином и паролем.



Cluster Usermin Servers

Модуль Cluster Usermin Servers позволяет управлять модулями, темами, пользователями и группами на нескольких серверах usermin с помощью одного интерфейса. Он сочетает в себе функции из модулей Usermin Configuration и Usermin Users с возможностью выполнения действий (таких как установка темы или создание пользователя) на нескольких серверах одновременно.

Управляемый сервер

В верхней части главной страницы под заголовком «Управляемые серверы» перечислены другие серверы Webmin, модули и пользователи которые управляются этим модулем. Чтобы добавить сервер в этот список, необходимо сначала добавить его в модуль серверы Webmin, указав имя пользователя и пароль для входа в Webmin на этом сервере. Затем можно выбрать сервер из списка рядом с кнопкой «Добавить сервер».

Когда сервер будет добавлен, он будет проверен, чтобы убедиться, что он работает под управлением поддерживаемой версии Usermin (0.985 или более поздней версии) и что на нем установлены необходимые модули. Списки всех модулей, тем, пользователей и групп с сервера будут загружены и кэшированы локально.

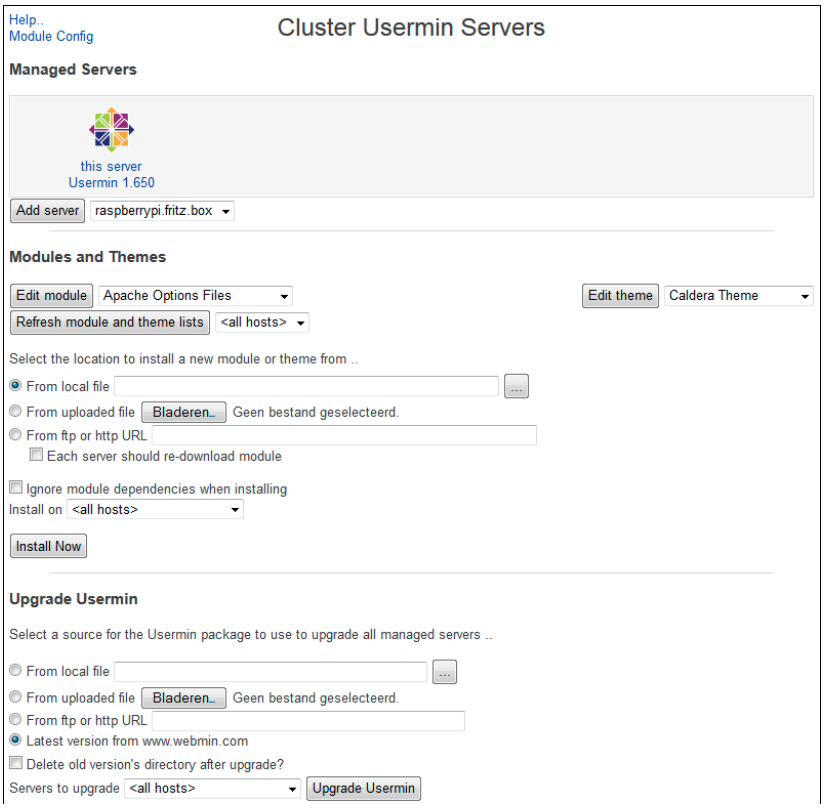
При наличии хотя бы одного значка в разделе управляемые серверы можно использовать кнопки в разделе «Пользователи и группы» для редактирования, создания или установки списков управления доступом для пользователей и групп на любом сервере. Пользователи и группы, которые вы создадите, будут созданы на всех управляемых серверах, но те, которые уже существуют, которые редактируются или удаляются, будут изменены только на серверах, на которых они уже существуют.

Модули и темы

В середине страницы в разделе модули и темы находятся кнопки для редактирования модулей и тем, установленных на любом управляемом сервере, и форма для установки нового модуля или темы на всех серверах.

Обновление Usermin

В нижней части страницы Вы можете обновить Usermin на всех управляемых серверах.

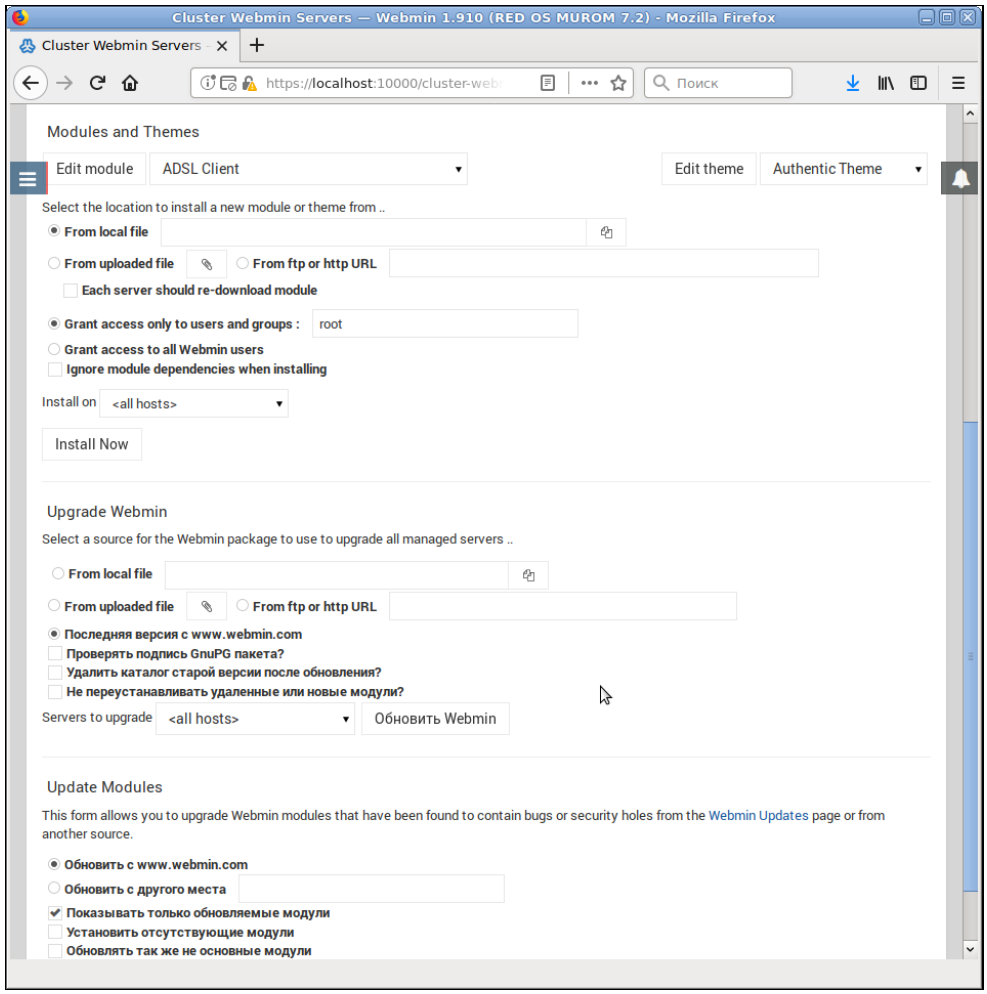


Cluster Webmin Servers

Модуль Cluster Webmin Configuration имеет две цели - управление пользователями и группами Webmin в нескольких системах, а также установка и удаление модулей и тем. Если в Вашей сети несколько серверов Webmin, этот модуль может быть очень полезен для синхронизации их списков пользователей и настроек контроля доступа. И это обеспечивает простой способ развертывания нового модуля на большом количестве серверов одновременно.

Как и другие кластерные модули, этот хранит списки модулей, тем, пользователей и групп с каждого управляемого сервера в главной системе. Это ускоряет поиск, но создает потенциал для несоответствий между тем, как настроены основные системы в других системах, и тем, какие они на самом деле. Например, если Вы устанавливаете модуль или обновляете управляемый хост, главная система не будет знать об этом, пока он не будет обновляться ежегодно, как объясняется в разделе «Обновление списков пользователей и модулей».

Если щелкнуть на значок модуля в категории «Кластер» в главном меню Webmin, отобразится главная страница. Вверху находится таблица значков, по одной для каждого из управляемых серверов. Под каждым значком указана версия Webmin, которую он в данный момент использует, определяется, когда он был добавлен в модуль или последний раз обновлен. Предполагая, что у вас есть несколько серверов в списке, под ними находятся формы для редактирования и добавления пользователей и групп, за которыми следуют дополнительные формы для установки и поиска модулей и тем.


Cluster Webmin Servers — Webmin 1.910 (RED OS MUROM 7.2) - Mozilla Firefox
Cluster Webmin Servers
https://localhost:10000/cluster-web
Поиск
Modules and Themes
Edit module
ADSL Client
Edit theme
Authentic Theme
Select the location to install a new module or theme from ..
From local file
From uploaded file
From ftp or http URL
Each server should re-download module
Grant access only to users and groups :
root
Grant access to all Webmin users
Ignore module dependencies when installing
Install on
<all hosts>
Install Now
Upgrade Webmin
Select a source for the Webmin package to use to upgrade all managed servers ..
From local file
From uploaded file
From ftp or http URL
Последняя версия с www.webmin.com
Проверять подпись GnuPG пакета?
Удалить каталог старой версии после обновления?
Не переустанавливать удаленные или новые модули?
Servers to upgrade
<all hosts>
Обновить Webmin
Update Modules
This form allows you to upgrade Webmin modules that have been found to contain bugs or security holes from the Webmin Updates page or from another source.
Обновить с www.webmin.com
Обновить с другого места
Показывать только обновляемые модули
Установить отсутствующие модули
Обновлять так же не основные модули

Ansible - система автоматизации настройки и развертывания ПО

Установка Ansible
Подключение клиентских хостов
Проверка подключения клиентских хостов
Создание плейбука и его выполнение
Выполнение одиночной команды
Обновление Ansible до версии 6.4.0

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** ansible-2.9.21-2, ansible-6.4.0-1

Ansible — система управления конфигурациями, написанная на Python, с использованием декларативного языка разметки для описания конфигураций. Используется для автоматизации настройки и развертывания программного обеспечения. Обычно используется для управления Linux-узлами, но Windows также поддерживается. Поддерживает работу с сетевыми устройствами, на которых установлен Python версии 2.4 и выше по SSH или WinRM соединению.

Установка Ansible

Для установки **Ansible** открываем терминал в режим суперпользователя командой:

```
su -
```

и выполните команду:

```
dnf install ansible
```

Подключение клиентских хостов

1) В файле **/etc/ansible/hosts** прописать все хосты, на которые будет распространяться конфигурация. Хосты можно разделить по группам, а так же, если у вас есть домен, то автоматически экспортировать список из домена. Можно прописывать как ip адреса так и имена хостов, если они резолвятся DNS ом в сети. Для теста пропишем 2 хоста.

```
[test]
10.10.1.111
10.10.1.74
```

2) Подключение к хостам осуществляется по протоколу **ssh** с помощью rsa ключей. Сгенерировать серверный ключ можно командой ниже. При её выполнении везде нажмите **Enter**.

```
ssh-keygen -C "$(whoami)@$(hostname)-$(date -I)"
```

3) Далее нужно распространить ключ на все подключенные хосты. Распространить ключи на хосты можно командой:

```
ssh-copy-id root@server
```

где:

- **root** - это пользователь, от имени которого будут выполняться плейбуки;
- **server** - IP-адрес хоста.

Пример: `root@10.10.1.74` .

Проверка подключения клиентских хостов

Пингуем удаленные хосты с помощью **Ansible**:

```
ansible test -m ping

test-1 | success >> {
    "changed": false, U
    "ping": "pong"
}

test-2 | success >> {
    "changed": false,
    "ping": "pong"
}
```

Где **test** - это группа хостов, указанная в файле **hosts**. В результате под каждым хостом должно быть написано `"ping": "pong"`.

Создание плейбука и его выполнение

Плейбуки являются сценариями, выполняемыми на удаленных хостах. Создаем каталог, для хранения наших **playbooks**, которые пишутся на языке **YAML**:

```
mkdir /etc/ansible/playbooks
```

Для примера создадим плейбук, устанавливающий программы. В каталоге **/etc/ansible/playbooks** создаем файл **install_programm.yml**:

```
touch /etc/ansible/playbooks/install_programm.yml
```

Содержимое файла следующее:

```
---
- hosts: all
tasks:
- name: Install programm
dnf:
name: "{{ packages }}"
vars:
packages:
- unrar
- p7zip
```

В данном примере для установки используется модуль **dnf**. Применяется массив **packages** для установки. В него вписываются необходимые для установки программы.

Если хотите, можно проверить, на каких хостах будет происходить работа, командой:

```
ansible-playbook /etc/ansible/playbooks/install_programm.yml --list-host
```

Запустить только что созданный набор инструкций можно следующей командой:

```
ansible-playbook /etc/ansible/playbooks/install_programm.yml
```

Выполнение одиночной команды

С помощью **Ansible** возможно сразу на всех клиентах выполнить команду **bash** без создания плейбуков. Просмотрим информацию об использовании оперативной памяти на удаленных хостах:

```
ansible test -a "free -h"

test-1 | success | rc=0 >>
             total       used       free     shared    buffers     cached
Mem:          7.6G       6.4G       1.2G       471M        64M       1.2G
-/+ buffers/cache:       5.2G       2.4G
Swap:         4.0G       616M       3.4G
```

```
test-2 | success | rc=0 >>
             total       used       free     shared    buffers     cached
Mem:          3.9G       3.3G       573M       333M       4.8M       442M
-/+ buffers/cache:       2.9G       1.0G
Swap:         4.0G       1.7G       2.3G
```

Обновление Ansible до версии 6.4.0

Пакеты **Ansible** версии **6.X** располагаются в подключаемом репозитории, поэтому порядок обновления несколько отличается от обычного.

Установка и обновление пакетов **Ansible** до версии **6.X** на **РЕД ОС 7.3** производится с помощью следующих команд (потребуются права пользователя **root**):

```
dnf install ansible6-release    # подключение репозитория
dnf clean all     # очистка метаданных
dnf makecache     # загрузка метаданных из всех репозиториев
dnf install ansible     # установка новой версии ansible 6.4
```

Puppet - централизованное управление конфигурацией ОС и ПО

Предварительная подготовка
Установка Puppet-сервера
Установка Puppet-клиента
Подключение клиента к серверу

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия puppet:** puppet-7.12.0-4

Puppet - это кроссплатформенная структура, позволяющая системным администраторам выполнять общие задачи с использованием кода. Код позволяет выполнять различные задачи от установки новых программ до проверки прав доступа файлов или обновлений пользовательских учетных записей. В большинстве случаев **puppet** используется в конфигурации клиент/сервер.

Вы можете подробнее ознакомиться с организацией централизованного управления конфигурацией ОС и ПО при помощи **Puppet**, просмотрев наши обучающие видео:

- на **RuTube** — Puppet - централизованное управление конфигурацией ОС и ПО;
- в **Яндекс.Дзен** — Puppet - централизованное управление конфигурацией ОС и ПО;
- в **VK Видео** — Puppet - централизованное управление конфигурацией ОС и ПО.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная подготовка

Сначала необходимо установить статические имена хостов на сервере и на клиенте соответственно:

```
hostnamectl set-hostname puppet.server --static
hostnamectl set-hostname puppet.client --static
```

Затем в базу данных доменных имен необходимо добавить имя и IP-адрес сервера Puppet, а также клиента Puppet:

```
echo '192.168.0.34 puppet.server' >> /etc/hosts
echo '192.168.0.35 puppet.client' >> /etc/hosts
```

Установка Puppet-сервера

На *серверной* машине установите пакет сервера Puppet:

```
dnf install puppetserver
```

Затем требуется отредактировать конфигурационный файл сервера Puppet **/etc/puppetlabs/puppet/puppet.conf**, добавив следующие настройки:

```
[main]
server =  puppet.server
ca_server =  puppet.server
[server]
vardir = /opt/puppetlabs/server/data/puppetserver
logdir = /var/log/puppetlabs/puppetserver
rundir = /var/run/puppetlabs/puppetserver
pidfile = /var/run/puppetlabs/puppetserver/puppetserver.pid
codedir = /etc/puppetlabs/code
dns_alt_names = puppet
```

dns_alt_names — список имен хостов, которые серверу разрешено использовать в качестве основного сервера. Имя хоста, которое ваши агенты используют в настройках своего сервера, должно быть включено либо в этот параметр, либо в параметр имени сертификата основного сервера. Этот параметр используется только при первоначальной генерации сертификата основного сервера.

Далее перезагрузите/запустите сервер Puppet:

```
systemctl restart puppetserver
```

Проверьте, что статус сервиса Puppet изменился на активный:

```
systemctl status puppetserver

● puppetserver.service - puppetserver Service
  Loaded: loaded (/usr/lib/systemd/system/puppetserver.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2021-12-07 12:09:44 MSK; 45s ago
 Main PID: 1084 (java)
   Tasks: 45 (limit: 4915)
  Memory: 1.2G
    CPU: 1min 47.001s
  CGroup: /system.slice/puppetserver.service
          └─1084 /usr/bin/java -Xms2g -Xmx2g -Djruby.logger.class=com.puppetlabs.jruby_utils.jruby.Slf4jLogger -
XX:+CrashOnOutOfMemoryError -XX:ErrorFile=/var/log/puppetlabs/puppetserver/p
```

Установка Puppet-клиента

На *клиентской* машине необходимо установить пакет клиента Puppet:

```
dnf install puppet
```

Затем требуется отредактировать конфигурационный файл клиента Puppet, добавив следующие настройки в файл **/etc/puppetlabs/puppet/puppet.conf**:

```
[main]
server = puppet.server
```

После этого запустите клиент Puppet:

```
systemctl start puppet
```

Проверьте, что статус клиента Puppet активен:

```
systemctl status puppet

● puppet.service - Puppet agent
  Loaded: loaded (/usr/lib/systemd/system/puppet.service; enabled; vendor preset: disabled)
  Active: active (running) since Tue 2021-12-07 12:16:36 MSK; 13s ago
 Main PID: 1321 (puppet)
   Tasks: 1 (limit: 1963)
  Memory: 52.0M
    CPU: 2.879s
  CGroup: /system.slice/puppet.service
          └─1321 /opt/puppetlabs/puppet/bin/ruby /opt/puppetlabs/puppet/bin/puppet agent --no-daemonize
```

Подключение клиента к серверу

Далее на *серверной* машине необходимо перечислить узлы клиента Puppet на сервере Puppet:

```
/opt/puppetlabs/bin/puppetserver ca list --all
```

Затем нужно добавить имя хоста Puppet-клиента к Puppet-серверу:

```
/opt/puppetlabs/bin/puppetserver ca sign --certname  puppet.client
```

После этого на *клиентской* машине необходимо запустить тест соединения с сервером Puppet:

```
/opt/puppetlabs/bin/puppet agent -t
```

```
Info: Using environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Caching catalog for puppet.agent-node
Info: Applying configuration version '1638876480'
Notice: Applied catalog in 0.28 seconds
```

Давайте проверим корректность работы Puppet-клиента и Puppet-сервера, установив пакет **httpd** с помощью манифеста.

Для этого сначала убедитесь, что на текущий момент на клиентской машине не установлен пакет **httpd**:

```
rpm -qa | grep -i httpd
```

Затем на серверной машине создайте манифест нового модуля **install_pkg** сервера Puppet, добавив задачу установки пакета **httpd** в файле **/etc/puppetlabs/code/environments/production/manifests/init.pp**:

```
class install_pkg {
  package { httpd:
  ensure => installed
  }
}
```

И создайте манифест, подключающий модуль **install_pkg** сервера Puppet в файле **/etc/puppetlabs/code/environments/production/manifests/site.pp**:

```
node default {
  include install_pkg
}
```

После этого на *клиентской* машине принудительно запустите агент сервера Puppet:

```
/opt/puppetlabs/bin/puppet agent -t
Info: Using environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Caching catalog for puppet.client
Info: Applying configuration version '1638877024'
Notice: /Stage[main]/Install_pkg/Package[httpd]/ensure: created
Notice: Applied catalog in 22.35 seconds
```

Убедитесь, что на *клиентской* машине пакет **httpd** был успешно установлен:

```
rpm -qa | grep -i httpd
httpd-tools-2.4.46-4.el7.x86_64
httpd-filesystem-2.4.46-4.el7.noarch
httpd-2.4.46-4.el7.x86_64
```

Проверка связи между сервером и клиентом прошла успешно.

Установка VirtualBox

Установка
Расширение размера диска виртуальной машины

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VirtualBox-7.0.20-1

Для установки **VirtualBox** у локального пользователя должны быть **права администратора** (пользователь должен входить в **sudoers**).

Вы можете подробнее ознакомиться с возможностями работы **VirtualBox**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с VirtualBox в РЕД ОС;
- в **Яндекс.Дзен** — Работа с VirtualBox в РЕД ОС;
- в **VK Видео** — Работа с VirtualBox в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Устанавливаем пакет **VirtualBox** с помощью утилиты **dnf**.

Установка **VirtualBox** вместе с гостевыми дополнениями и модулями ядра:

```
dnf install VirtualBox VirtualBox-guest-additions VirtualBox-kmod_$(uname -r)
```

В названии пакета **VirtualBox-kmod** добавляется **$(uname -r)** для того, чтобы установился модуль для текущей версии ядра, на которой загружена ОС.

После установки пакетов выполните перезагрузку ОС.

Для того чтобы **VirtualBox** поддерживал **Usb 3.0** и **Usb 2.0**, зайдите на страницу https://www.virtualbox.org/wiki/Downloads и скачайте **VirtualBox Extension Pack**. Для установки Extension Pack'а перейдите в "**Файл**" - "**Инструменты**" - "**Менеджер плагинов**", щелкните "**Установить**", найдите папку, в которую был скачан (обычно «Загрузки») Extension Pack, и двойным щелчком добавьте его.

ВНИМАНИЕ!

ДЛЯ ДОБАВЛЕНИЯ И УДАЛЕНИЯ ПЛАГИНОВ ТРЕБУЕТСЯ ПОЛЬЗОВАТЕЛЬ С **ПРАВАМИ АДМИНИСТРАТОРА**.

Для того чтобы в виртуальных машинах можно было использовать USB-устройства, подключённые к ПК, необходимо выполнить следующую команду:

```
usermod -a -G vboxusers user
```

где **user** - это пользователь, которому нужно разрешить проброс USB.

Затем перезайдите в сеанс пользователя **user**.

Расширение размера диска виртуальной машины

Применимо только к дискам формата **.VDI** и не работает с дисками форматов **.VHD** и **.VMDK**. Такие диски можно клонировать в диск формата **VDI**.

Данный метод актуален только для динамических дисков и не работает с дисками фиксированного размера. Однако такие диски можно клонировать в динамический диск.

Перед изменением размера диска необходимо выключить виртуальную машину и сделать клон диска.

Изменить размер диска можно из командной строки:

```
vboxmanage modifyhd YOUR_HARD_DISK.vdi --resize SIZE_IN_MB
```

или из меню графического менеджера виртуальных машин (если используемая версия Oracle VirtualBox поддерживает эту возможность: Меню "**Файл**" - "**Менеджер виртуальных носителей**".

Если на вашей машине содержится несколько снимков, то нужно изменить размер диска каждого диска Это можно сделать в графическом менеджере виртуальных носителей, или командой вида:

```
vboxmanage modifyhd YOUR_HARD_DISK.vdi --resize SIZE_IN_MB
for x in Snapshots/*.vdi ; do vboxmanage modifyhd $x --resize SIZE_IN_MB ; done
```

Изменение размера диска не изменяет размеры дисковых разделов. Для того, чтобы гостевая машина получила доступ к дополнительному дисковому пространству, нужно изменить размер дисковых разделов. Для этого нужно загрузить виртуальную машину с Live-CD, либо примонтировать диск к другой виртуальной машине. И в первом, и во втором случае изменение дисковых разделов можно сделать с помощью программы **GParted**.

Установка РЕД ОС в VirtualBox

Создание новой ВМ в VirtualBox
Установка РЕД ОС
Настройка виртуальной машины с помощью командной строки

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VirtualBox-7.0.20-1

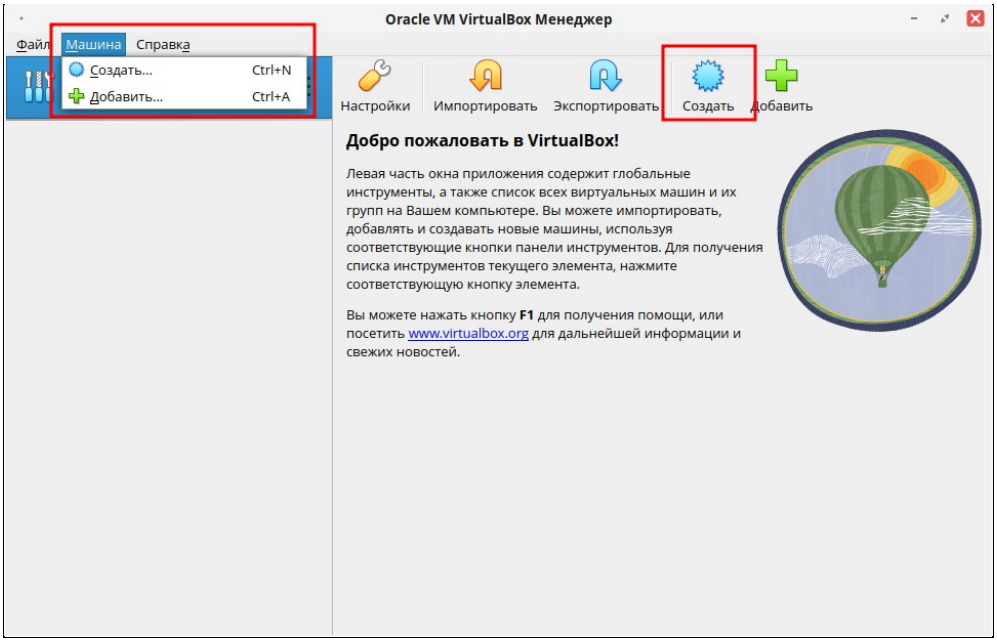
Вы можете подробнее ознакомиться с информацией по установке системы в VirtualBox, просмотрев наши обучающие видео:

- на **RuTube** — Установка РЕД ОС в виртуальных средах на примере Oracle VM VirtualBox ;
- в **Яндекс.Дзен** — Установка РЕД ОС в виртуальных средах на примере Oracle VM VirtualBox ;
- в **VK Видео** — Установка РЕД ОС в виртуальных средах на примере Oracle VM VirtualBox .

На наших каналах вы также сможете найти много другой полезной информации.

Создание новой ВМ в VirtualBox

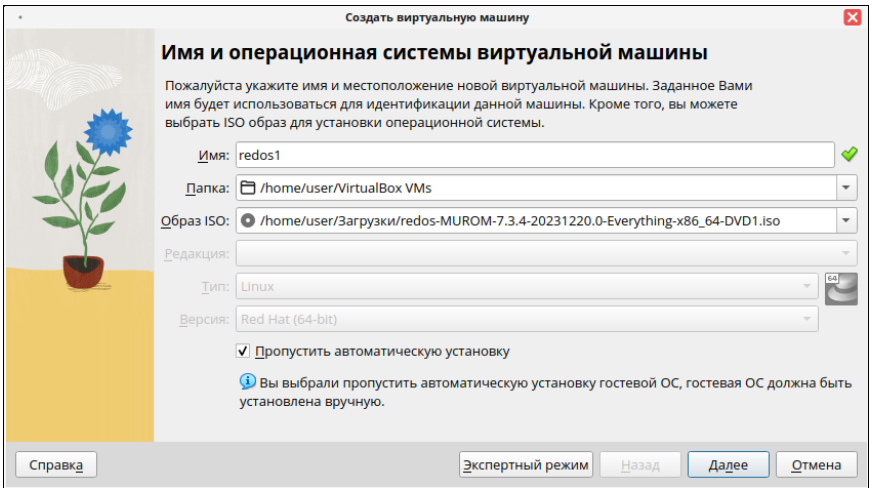
Для создания новой ВМ в окне приветствия **VirtualBox** нажмите «**Создать**» или выберите пункт меню «**Машина**» – «**Создать**».



В окне создания ВМ необходимо:

- задать имя будущей ВМ;
- указать каталог хранения данных ВМ;
- выбрать ISO-образ ОС;
- установить флаг пропуска автоматической установки ОС (по желанию).

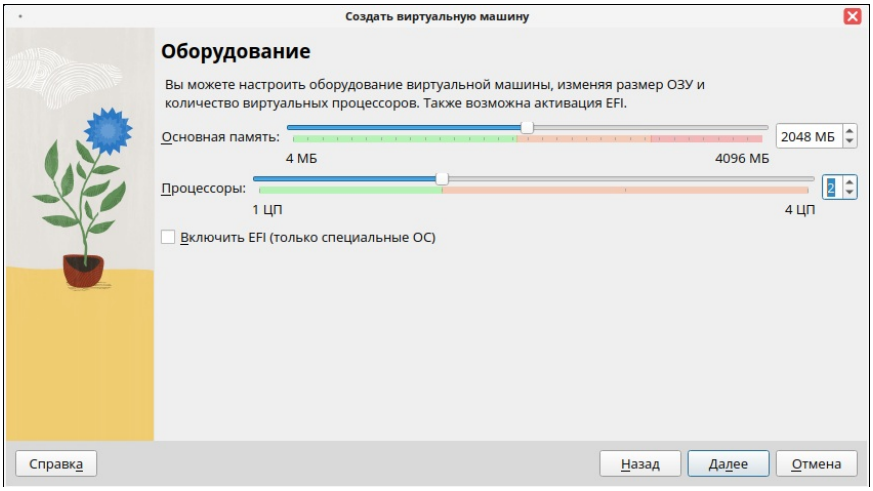
Нажмите «**Далее**».



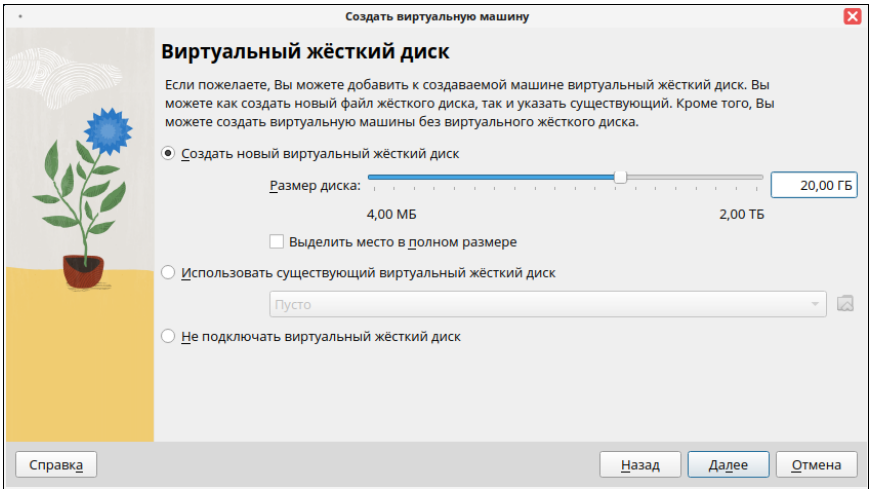
Выполните настройку оборудования:

- укажите объем ОЗУ (рекомендуется **не менее 2 ГБ**);
- укажите количество процессоров.

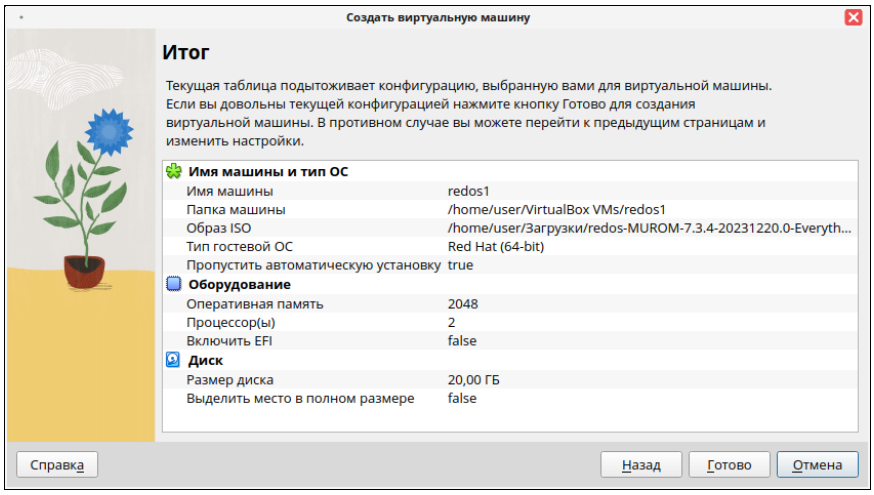
Нажмите «**Далее**».



Создайте новый виртуальный жесткий диск. Объем жесткого диска рекомендуется задать не менее 20 ГБ.



Проверьте параметры ВМ. Если все настроено верно, нажмите «**Готово**». В противном случае нажмите «**Назад**» и внесите необходимые изменения.



На данном этапе процесс создания новой ВМ завершен.

Для тонкой настройки ВМ перед ее запуском нажмите «**Настроить**» () и задайте необходимые параметры будущей системы по своему усмотрению.

Для запуска ВМ нажмите «**Запустить**» ().

Установка РЕД ОС

Установка ОС выполняется так же, как и на обычном ПК.

Определите необходимые настройки для стандартной установки РЕД ОС. Подробную информацию о настройке ОС перед установкой см. в нашей инструкции «Обзор установки».

Настройка виртуальной машины с помощью командной строки

Для создания виртуальной машины и регистрации её в системе выполните команду:

```
vboxmanage createvm --name RedOS --ostype Linux_64 --register
```

Для задания параметров созданной виртуальной машины выполните команду (укажите количество оперативной памяти, число процессоров и необходимые порты):

```
vboxmanage modifyvm RedOS --cpus 1 --memory 2048 --audio none --usb off --acpi on --boot1 dvd --nic1 nat
```

Для запуска виртуальной машины необходимо создать жёсткий и подключить его с помощью следующих команд:

```
vboxmanage createmedium \
--filename /home/user/virtualbox/RedOS/RedOS.vdi \
--size 12000
```

```
VBoxManage storagectl RedOS --name "SATA" --add sata
VBoxManage storagectl RedOS --name "IDE" --add ide
```

```
vboxmanage storageattach RedOS --storagectl "SATA" \
  --port 0 --device 0 --type hdd \
  --medium /home/user/virtualbox/RedOS/RedOS.vdi
```

Для установки виртуальной машины необходимо подключить к виртуальной машине ISO-образ, с которого будет происходить установка:

```
vboxmanage storageattach RedOS --storagectl "IDE" \
  --port 0 --device 1 --type dvddrive \
  --medium /home/user/data/iso/redos-MUROM-7.3-x86_64-DVD1.iso
```

Для запуска виртуальной машины выполните команду:

```
vboxmanage startvm RedOS
```

Экспортировать виртуальную машину можно командой:

```
vboxmanage export RedOS --output RedOS.ova
```

Импортировать виртуальную машину можно командой:

```
vboxmanage import RedOS.ova
```

Автостарт виртуальной машины в VirtualBox при запуске системы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** VirtualBox-7.0.20-1

Вы можете подробнее рассмотреть автоматический запуск ВМ в VirtualBox, просмотрев наши обучающие видео:

- на **RuTube** — Автостарт виртуальной машины в VirtualBox при запуске системы;
- в **Яндекс.Дзен** — Автостарт виртуальной машины в VirtualBox при запуске системы;
- в **VK Видео** — Автостарт виртуальной машины в VirtualBox при запуске системы.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка сервиса автозапуска виртуальной машины

Запустите терминал и выполните команду **с привилегиями пользователя root**:

```
echo -e "VBOXAUTOSTART_DB=/etc/vbox\nVBOXAUTOSTART_CONFIG=/etc/vbox/autostartvm.cfg" | sudo tee /etc/default/virtualbox
```

VBOXAUTOSTART_DB - определяет абсолютный путь к каталогу базы данных автозапуска, обычно это **/etc/vbox**.

VBOXAUTOSTART_CONFIG - определяет путь к конфигурации автозапуска виртуальной машины.

Для настройки конфигурации автостарта создайте файл:

```
sudo nano /etc/vbox/autostartvm.cfg
```

Содержимое файла (смените **user** - на вашего пользователя):

```
default_policy = deny
 user = {
allow = true
startup_delay = 10
}
```

- **default_policy** - определяет, разрешать или запрещать автоматический запуск виртуальной машины по умолчанию. В примере выше мы отказали кому-либо в автоматическом запуске виртуальной машины и явно разрешили одному пользователю user.
- **username (user)** - с помощью политики запрета по умолчанию вы можете определить конкретных пользователей, которым разрешено автоматически запускать виртуальную машину (allow = trues). Вы также можете определить, как долго задерживать запуск виртуальной машины. 10 секунд используется в этой демонстрации.

Определение владельца директории базы данных автозапуска

Для определения владельца директории базы данных автозапуска выполните следующие команды:

```
sudo usermod -aG vboxusers user
sudo chgrp vboxusers /etc/vbox
```

Назначьте группе разрешения на запись в каталоге базы данных автозапуска:

```
sudo chmod -R 777 /etc/vbox/
```

Как user, вы можете включить автозапуск для отдельных машин. Для этого необходимо сначала определить путь к каталогу базы данных.

```
VBoxManage setproperty autostartdbpath /etc/vbox/
```

Добавление виртуальной машины в автозапуск

```
vboxmanage modifyvm redos --autostart-enabled on
```

где redos - это UUID или имя вашей виртуальной машины.

Далее нужно создать скрипт для автозапуска машины:

```
sudo nano /etc/default/start
```

```
#!/bin/bash
VBoxAutostart --start -c /etc/vbox/autostartvm.cfg
```

Сделайте созданный файл исполняемым:

```
sudo chmod +x /etc/default/start
```

Проверьте, что файл выполняется успешно:

```
/etc/default/start
```

Пример вывода результата команды:

```
Oracle VM VirtualBox Autostart 6.1.16_REDSOFT
(C) 2021 Oracle Corporation
All rights reserved.

00:00:00.000404 main VirtualBox Autostart 6.1.16_REDSOFT r140961 linux.amd64 (Apr 12 2021 17:37:04) release log
00:00:00.000406 main Log opened 2021-05-24T06:54:30.722810000Z
00:00:00.000407 main Build Type: release
00:00:00.000411 main OS Product: Linux
00:00:00.000411 main OS Release: 5.10.29-1.el7.x86_64
00:00:00.000412 main OS Version: #1 SMP Mon Apr 12 13:55:18 MSK 2021
00:00:00.000445 main DMI Product Name: System Product Name
00:00:00.000452 main DMI Product Version: System Version
00:00:00.000457 main Firmware type: UEFI
00:00:00.001190 main Secure Boot: Disabled
00:00:00.001234 main Host RAM: 7826MB (7.6GB) total, 2378MB (2.3GB) available
00:00:00.001238 main Executable: /usr/lib64/virtualbox/VBoxAutostart
00:00:00.001239 main Process ID: 9566
00:00:00.001239 main Package type: LINUX_64BITS_GENERIC (OSE)
00:00:00.002388 main IPC socket path: /tmp/.vbox-wolandius-ipc/ipcd
```

Виртуальная машина должна будет запуститься в VirtualBox. Далее создайте сервис, который будет использоваться для автоматического запуска виртуальной машины (смените user — на вашего пользователя):

```
sudo nano /etc/systemd/system/vmsautostart.service
```

```
[Unit]
 Description=vms autostart
 Before=graphical.target

 [Service]
 ExecStart=/etc/default/start
 Type=oneshot
 Group=vboxusers
 User=user
 RemainAfterExit=yes

 [Install]
 WantedBy=multi-user.target
```

Предоставьте необходимые права следующей командой:

```
sudo chmod 664 /etc/systemd/system/vmsautostart.service
```

Добавьте сервис в автозагрузку и запустите его:

```
sudo systemctl daemon-reload
sudo systemctl enable vmsautostart.service
sudo systemctl start vmsautostart.service
```

При успешном старте сервиса проверьте VirtualBox на наличие работающей машины. При перезагрузке системы машина запустится до ввода пароля пользователя. Для отключения автозапуска виртуальной машины выполните команды:

```
vboxmanage modifyvm redos --autostart-enabled off
sudo systemctl disable vmsautostart.service
sudo systemctl stop vmsautostart.service
```

Установка эмулятора Android-x86

Создание новой ВМ

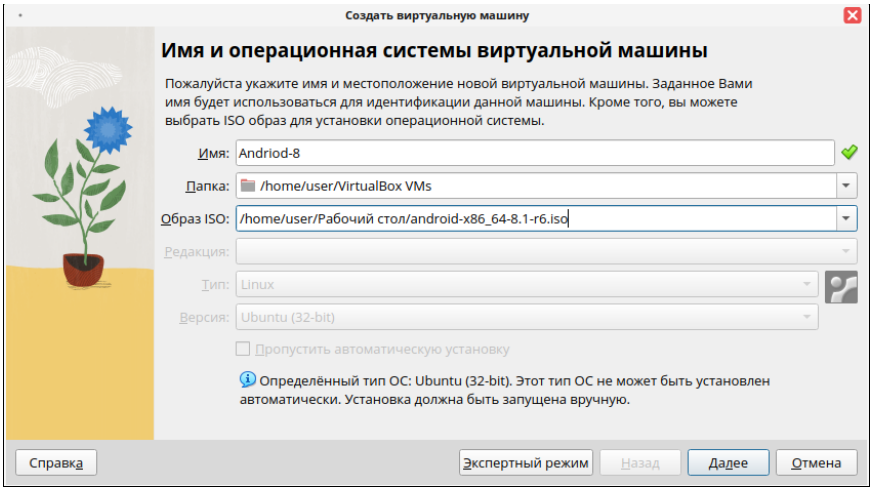
Для создания новой ВМ в окне приветствия **VirtualBox** нажмите «**Создать**» или выберите пункт меню «**Машина**» – «**Создать**».



В окне создания ВМ необходимо:

- задать имя будущей ВМ;
- указать каталог хранения данных ВМ;
- выбрать ISO-образ ОС;
- установить флаг пропуска автоматической установки ОС (по желанию).

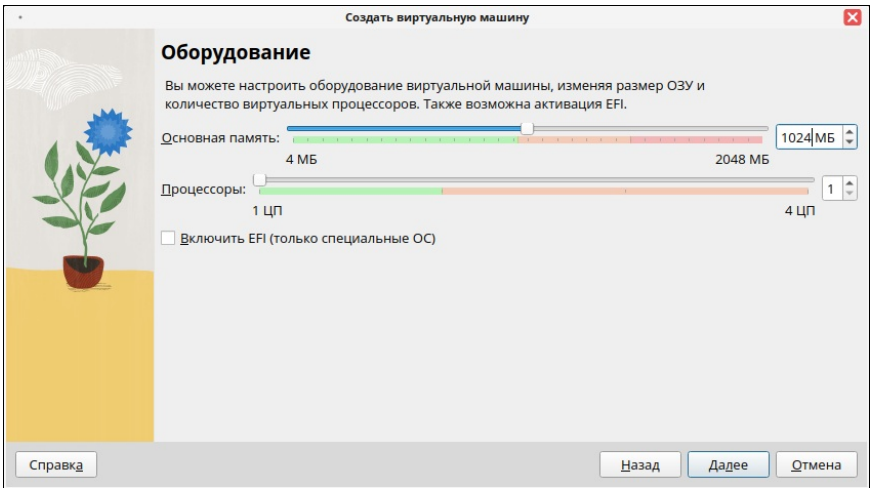
Нажмите «**Далее**».



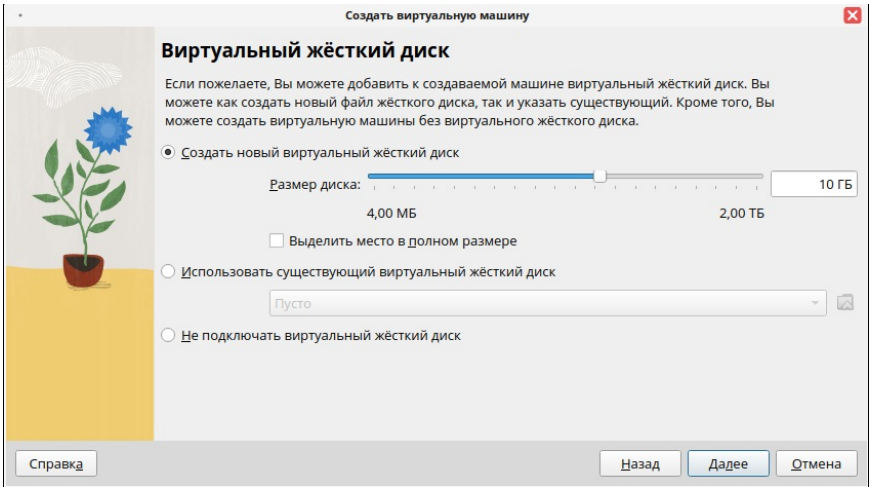
Выполните настройку оборудования:

- укажите объем ОЗУ (рекомендуется **не менее 512 МБ**);
- укажите количество процессоров.

Нажмите «**Далее**».



Создайте новый виртуальный жесткий диск. Объем жесткого диска рекомендуется задать **не менее 8 ГБ**. Если планируется устанавливать на Андроид приложения, необходимо выделить больше свободного места.



Проверьте параметры ВМ. Если все настроено верно, нажмите «**Готово**». В противном случае нажмите «**Назад**» и внесите необходимые изменения.

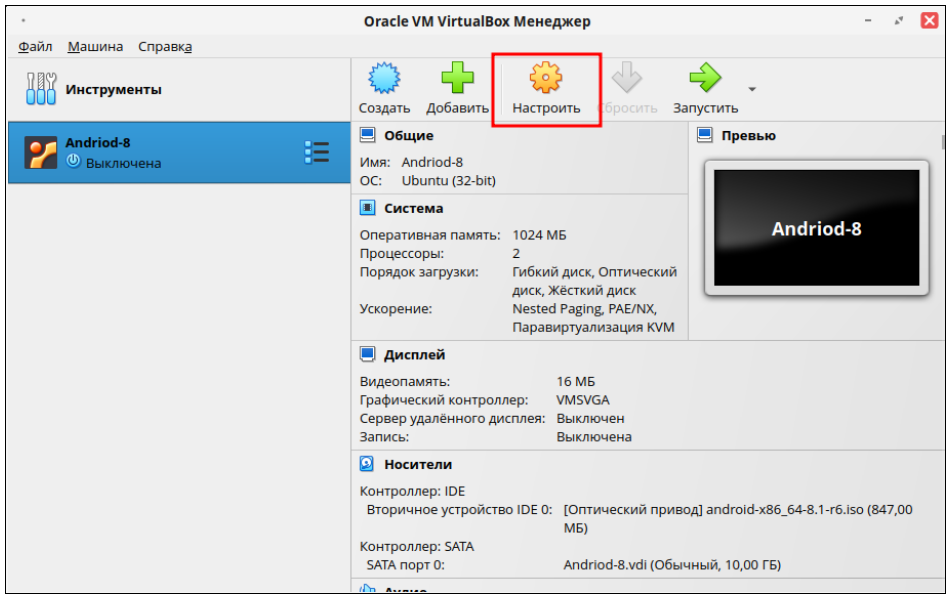


На данном этапе процесс создания новой ВМ завершен.

Настройка Android

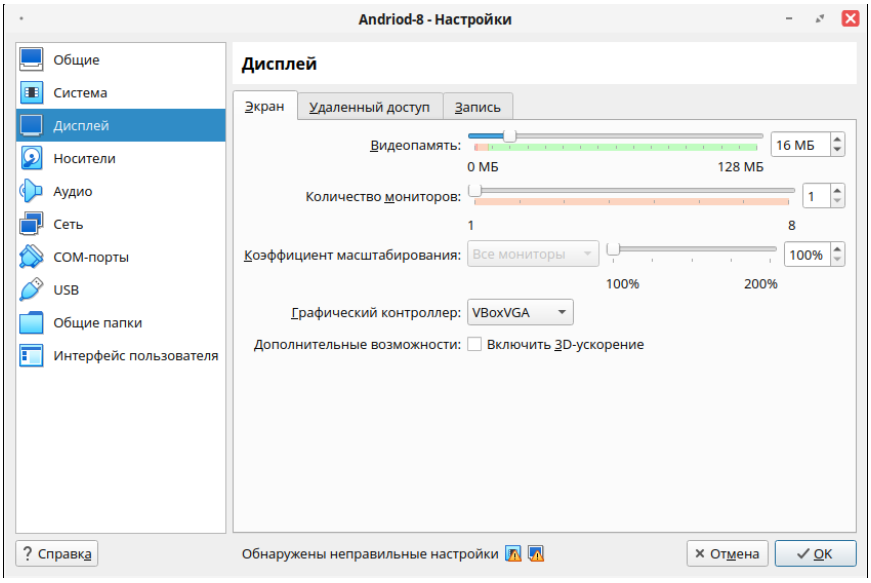
Перед запуском необходимо настроить Android.

Нажмите на кнопку **«Настроить»**.

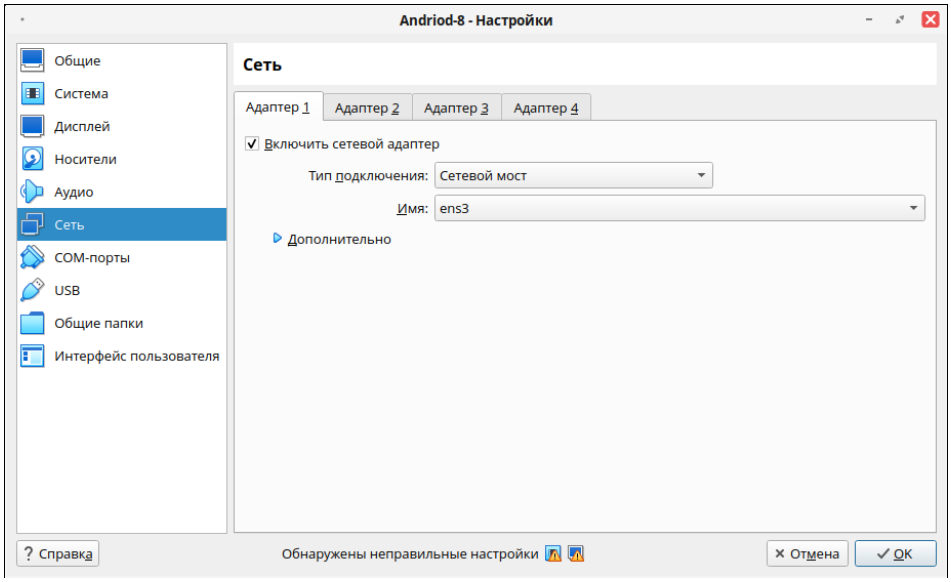


Зайдите в меню **«Система»** - **«Процессор»**, установите 4 ядра процессора и активируйте **PAE/NX**.

Затем перейдите в меню **«Дисплей»**, установите видеопамять **16 МБ** и выберите Графический контроллер **«VboxVGA»**.

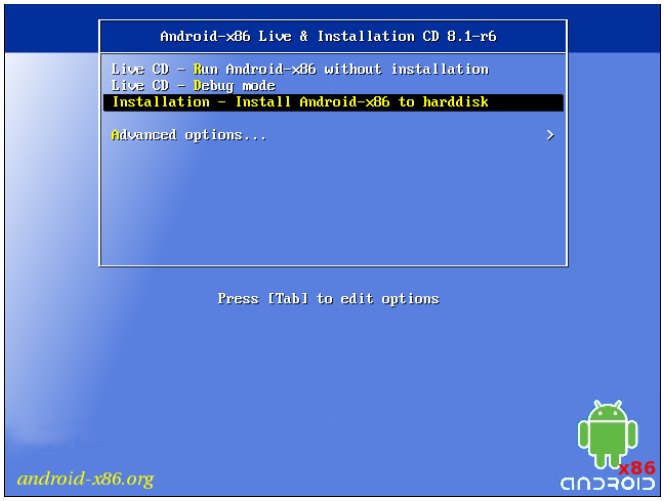


Перейдите в меню «**Сеть**» и выберите Тип подключения **«Сетевой мост»**.

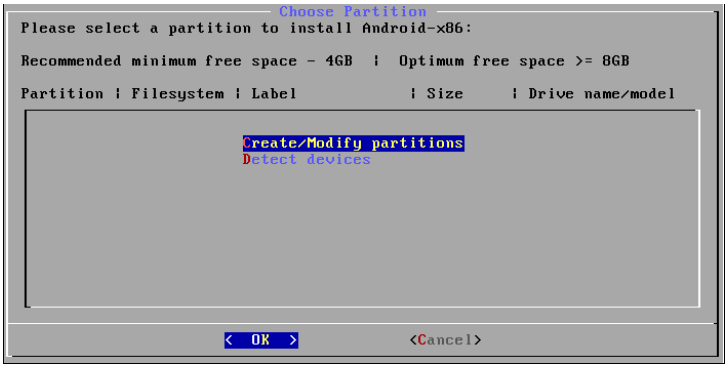


В VirtualBox Менеджере нажмите на кнопку **«Запустить»**.

Откроется boot-меню. Среди доступных способов выберите **«Installation - Install Android-x86 to harddisk»**.



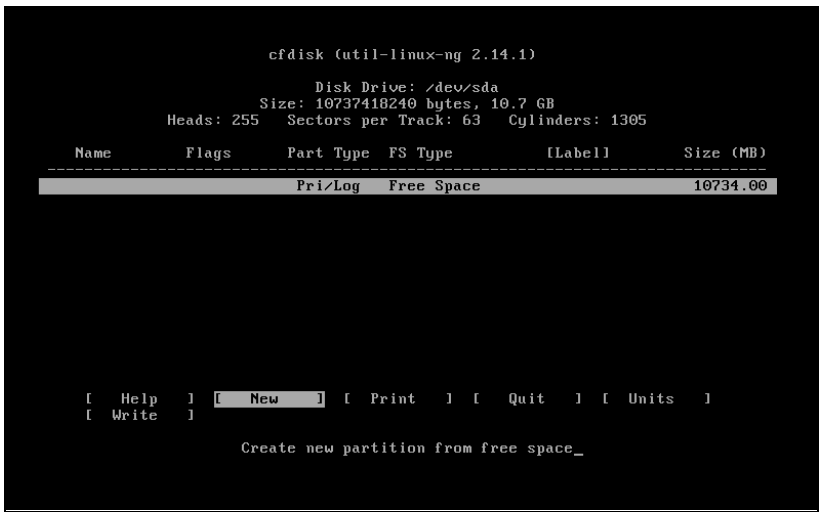
Вам будет предложено выбрать раздел для установки операционной системы. Нажмите на **«Create/Modify partitions»**.



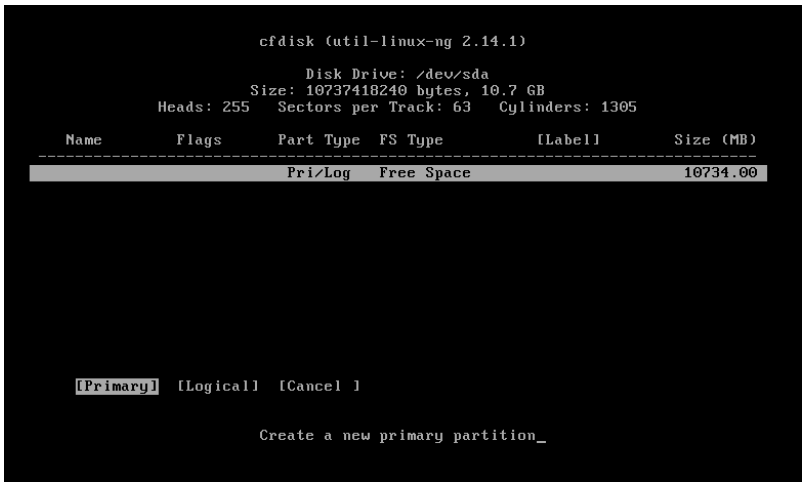
На предложение использовать GPT ответьте **«No»**.



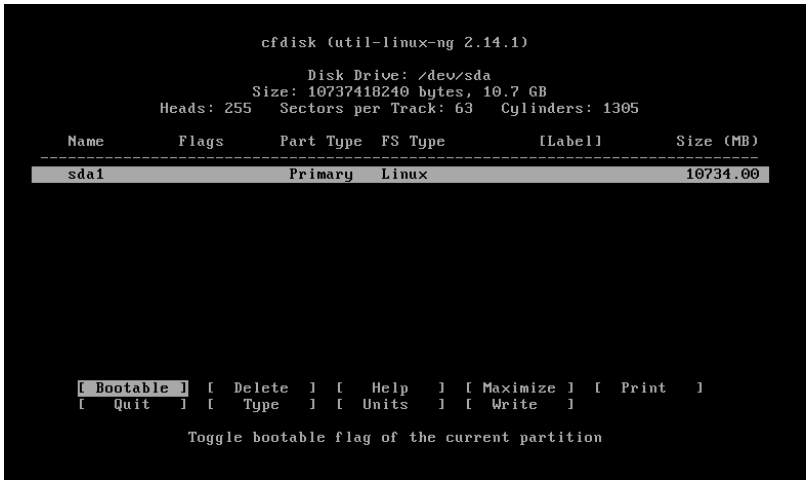
Загрузится утилита **cfdisk**, в которой необходимо будет создать раздел и задать ему некоторые параметры. Выберите **«New»** для создания раздела.



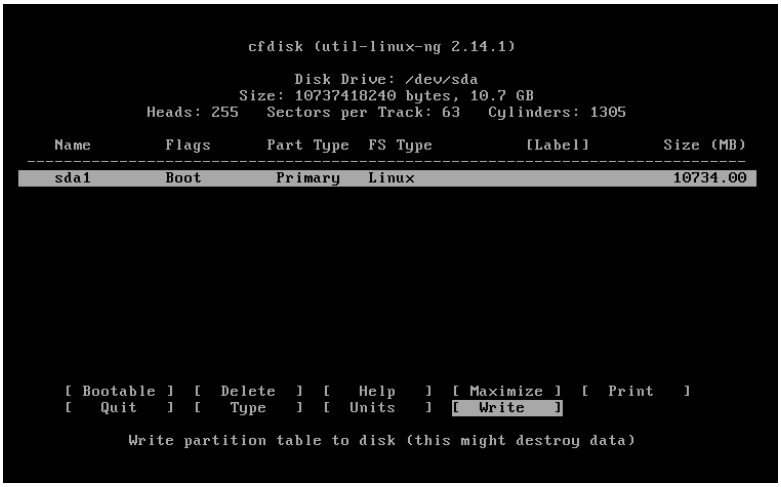
Назначьте раздел главным, выбрав **«Primary»**.



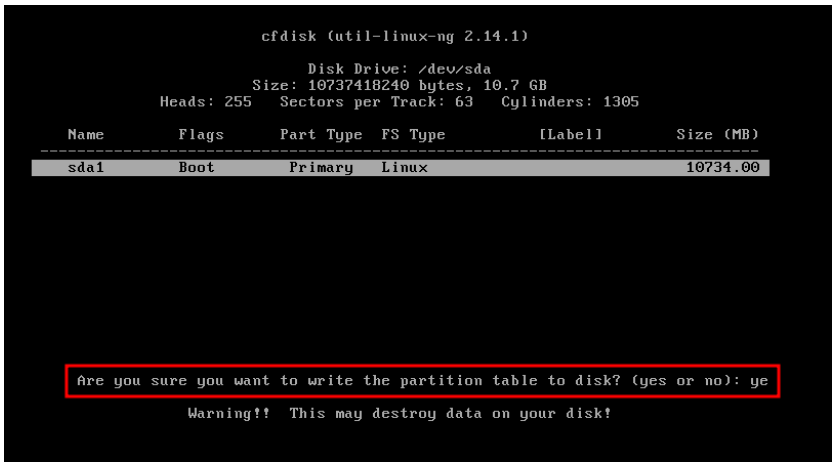
Сделайте раздел загрузочным, задав ему параметр **«Bootable»**.



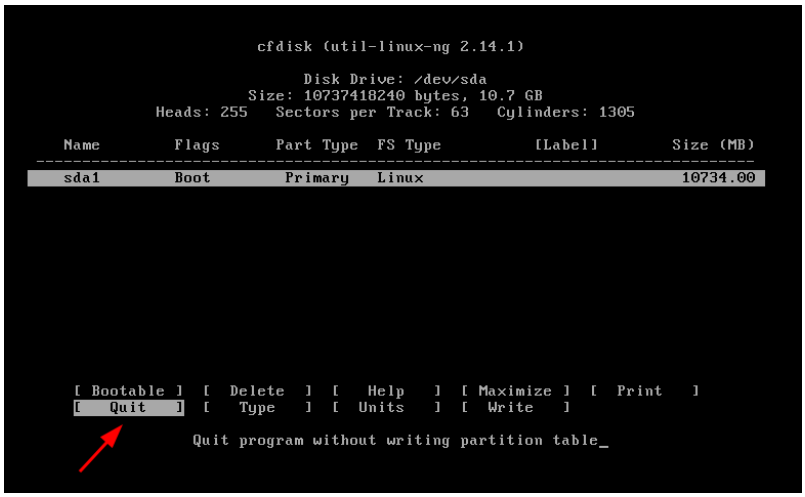
Примените все выбранные параметры, выбрав кнопку **«Write»**.



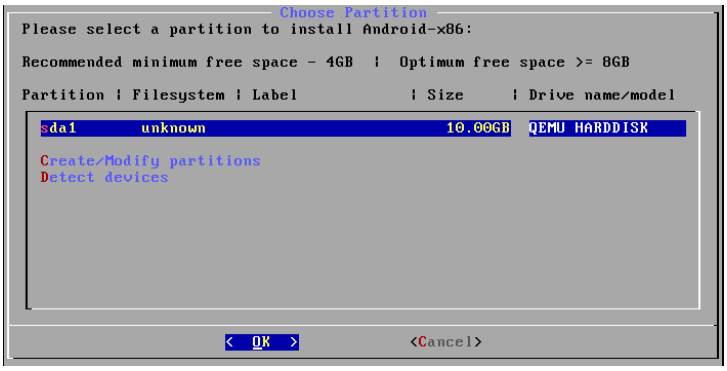
Для подтверждения записи диска необходимо ответить **«yes»** и нажать **Enter**.



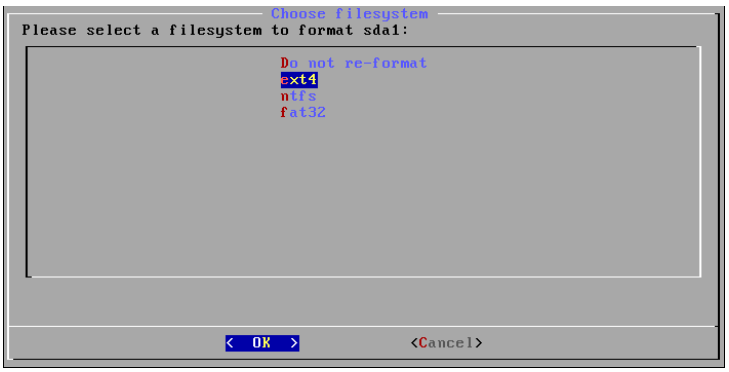
Чтобы выйти из утилиты **cfdisk**, выберите кнопку **«Quit»**.



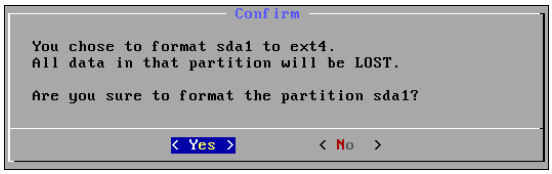
Вы снова попадете в окно установщика. Выберите созданный раздел — на него будет устанавливаться Андроид.



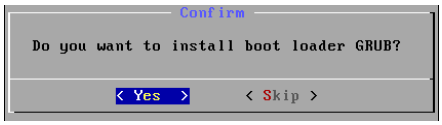
Установите для раздела в файловую систему **«ext4»**.



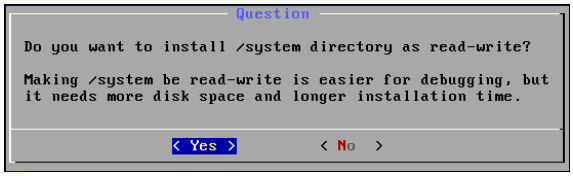
В окне с подтверждением форматирования выберите **«Yes»**.



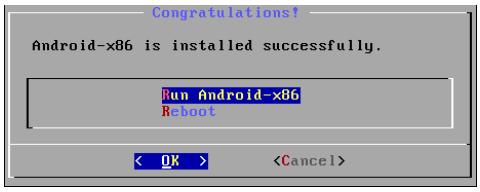
На предложение установить загрузчик GRUB ответьте **«Yes»**.



Устанавливаем директорию **\system** доступной для чтения\записи, отвечаем **«Yes»**.



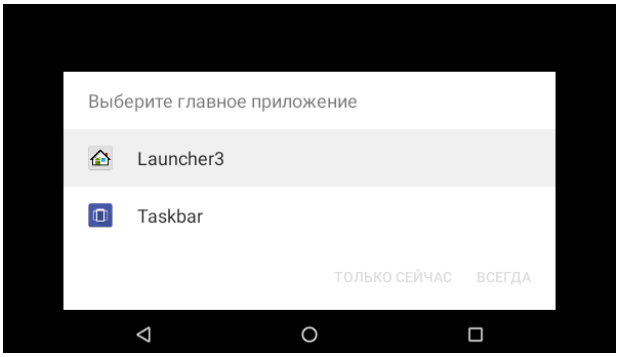
Когда установка будет завершена, будет предложено запустить систему или перезагрузить виртуальную машину. Выберите желаемый пункт.



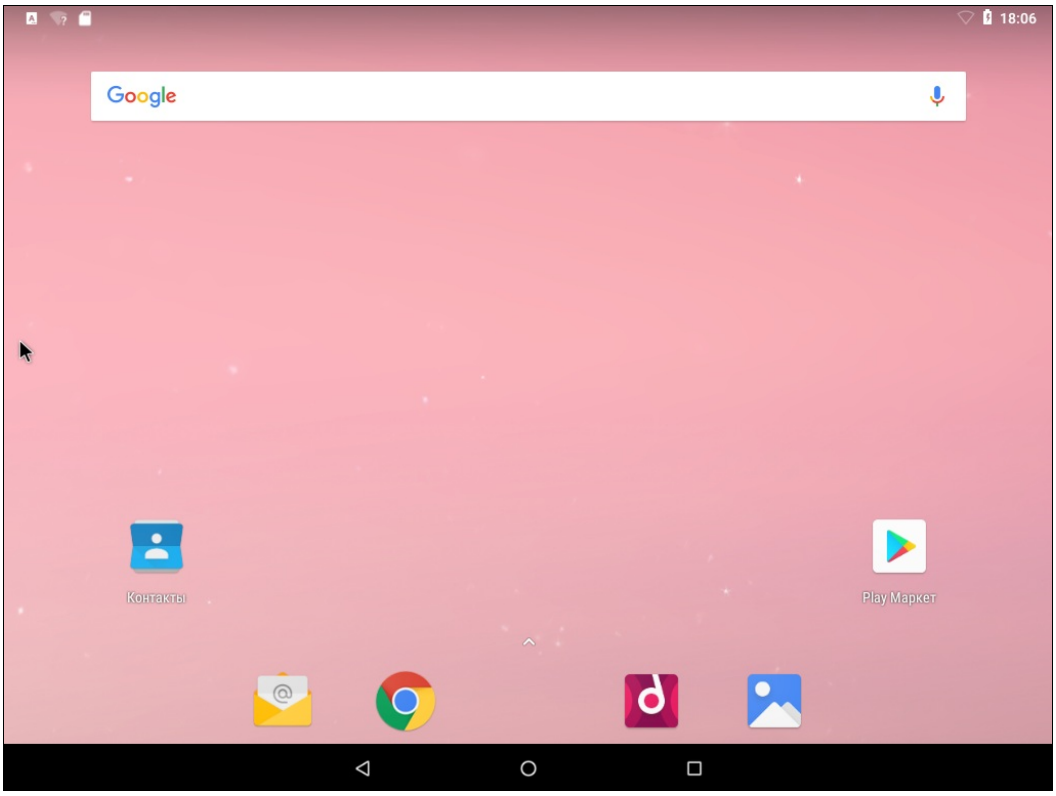
При запуске Android вы увидите фирменный логотип.



Далее систему нужно донастроить: выберите нужный язык, укажите имя пользователя, выполните настройку необходимых параметров и отключите те, которые вам не нужны, затем нажмите кнопку **«Принимаю»**.
Затем в качестве оболочки выбираем **«Launcher3»**.

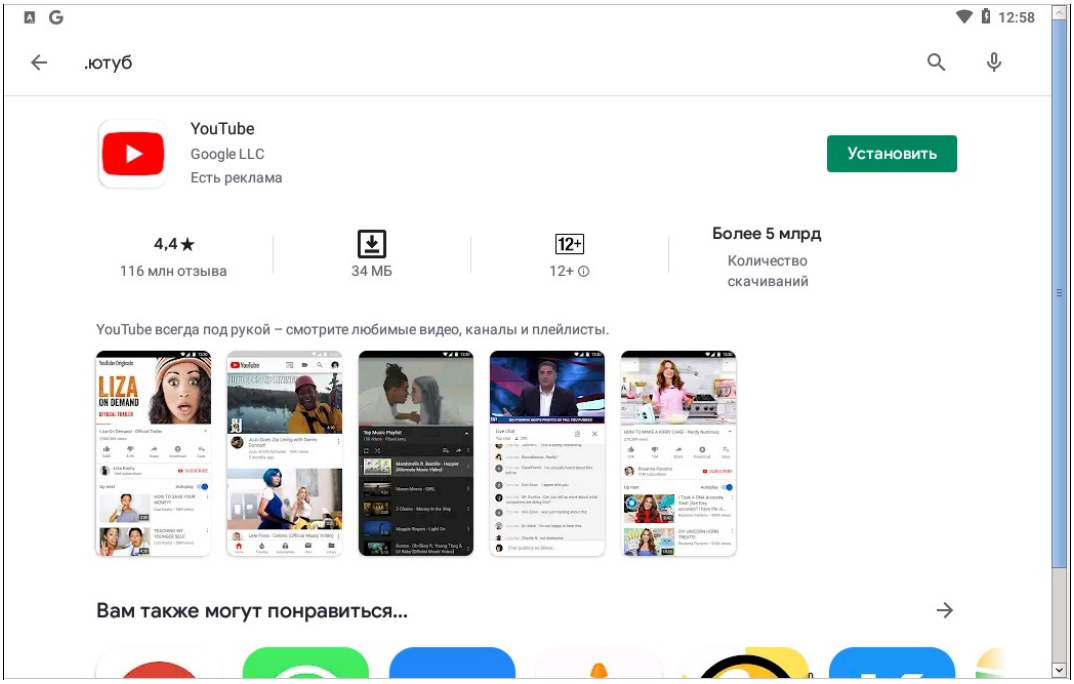


После успешной установки и настройки вы попадете на рабочий стол Android.

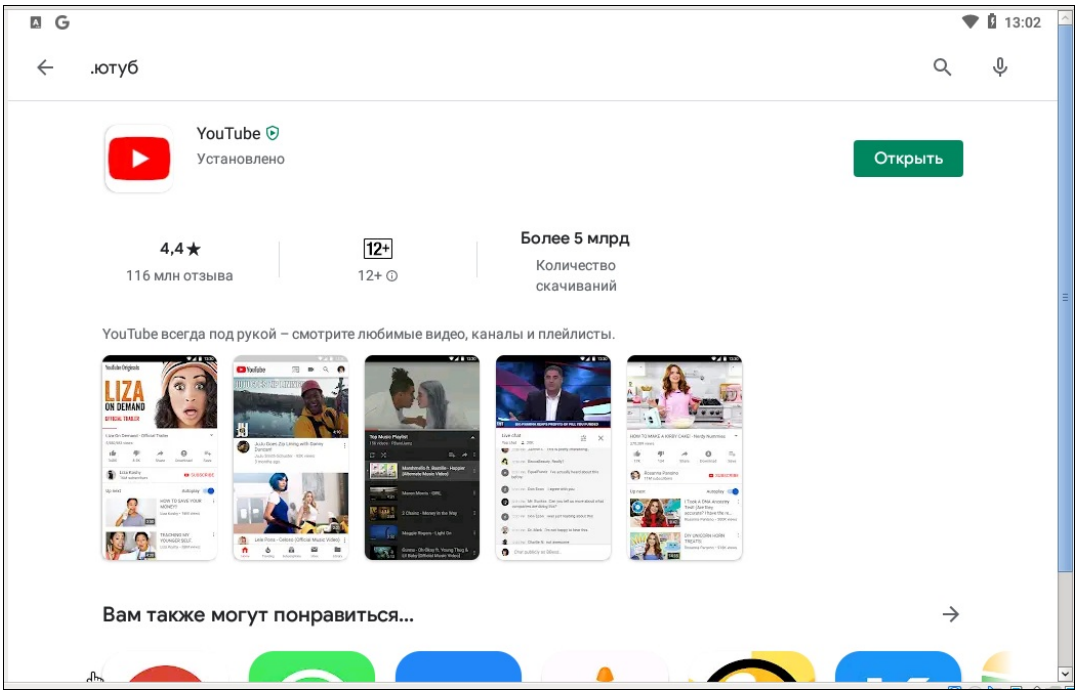


Установка приложения на Android

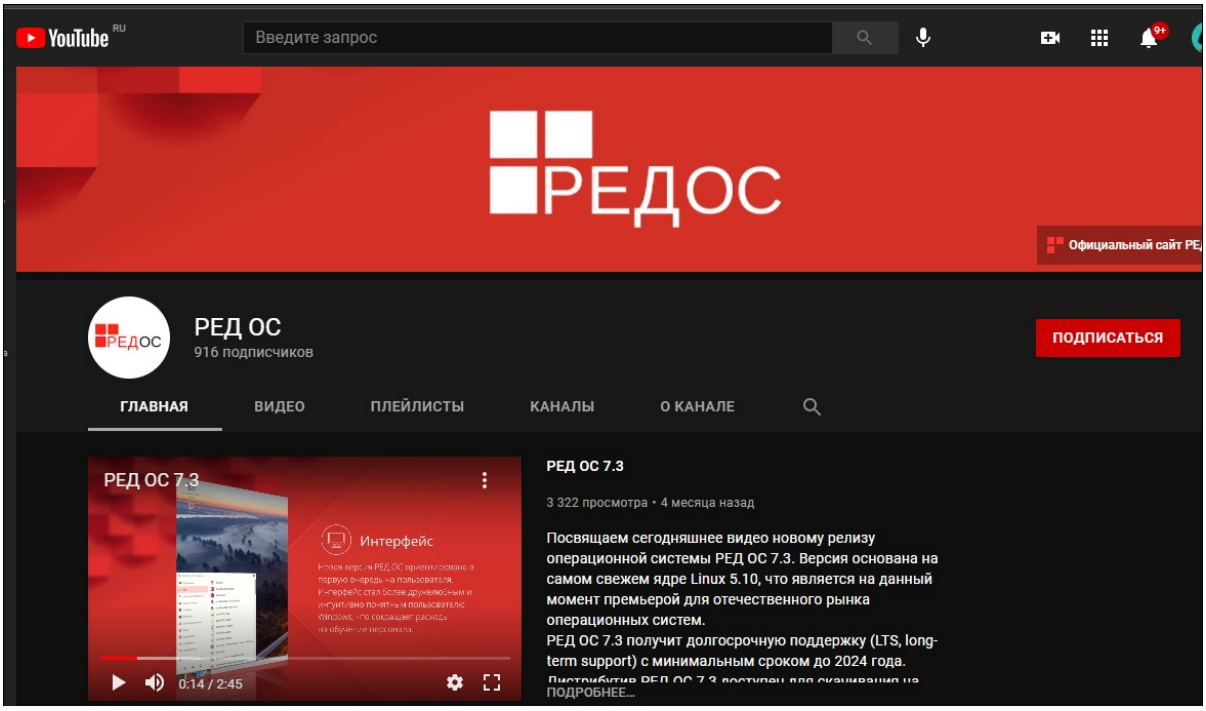
Заходим в *Play Market*, выбираем нужное приложение (для примера взят YouTube), нажимаем **«Установить»**.



После установки приложения нажимаем **«Открыть»**.



Приложение работает корректно.



Установка и настройка QEMU-KVM

Предварительная настройка
Установка и начальная настройка
Создание виртуальной машины
Управление ВМ
Управление ВМ через графический менеджер
Управление ВМ с помощью утилиты virsh
Клонирование виртуальных машин
Создание снапшотов
Решение возникающих проблем

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: libvirt-7.6.0-6, qemu-kvm-15:7.2.7-1, virt-manager-4.1.0-1

Виртуализация — предоставление набора вычислительных ресурсов или их логического объединения, независимое от аппаратной реализации и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.

Поддержка виртуализации в РЕД ОС обеспечивается технологией **KVM** (Kernel-based Virtual Machine). Программное обеспечение KVM состоит из загружаемого модуля ядра **kvm.ko**, предоставляющего базовый сервис виртуализации, процессорно-специфического загружаемого модуля **kvm-amd.ko** или **kvm-intel.ko** и компонентов пользовательского режима **QEMU**.

QEMU — средство эмуляции аппаратного обеспечения различных платформ, поддерживающее также аппаратную виртуализацию, основанную на технологии Intel-VT или AMD-V, на процессорах Intel и AMD.

Управление средой виртуализации в РЕД ОС осуществляется посредством набора инструментов **libvirt**, предоставляющего единый API к различным технологиям виртуализации. Главным компонентом сервера виртуализации является служба **libvirtd**.

Менеджер виртуальных машин **virt-manager** предоставляет графический интерфейс для доступа к гипервизорам и виртуальным машинам как в локальной, так и в удаленных системах.

Дополнительную информацию о настройке и работе с QEMU см. в **Руководстве администратора РЕД ОС**.

Вы можете подробнее ознакомиться с работой **QEMU**, просмотрев наши обучающие видео:

- на **RuTube** — Установка и настройка QEMU-KVM;
- в **Яндекс.Дзен** — Установка и настройка QEMU-KVM;
- в **VK Видео** — Установка и настройка QEMU-KVM.

На наших каналах вы также сможете найти много другой полезной информации.

Предварительная настройка

Сначала необходимо проверить, поддерживает ли ваш процессор аппаратную виртуализацию. Проверка осуществляется командой:

```
egrep '(vmx|svm)' /proc/cpuinfo

flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc aperfmperf eagerfpu pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm epb retpoline kaiser tpr_shadow vnmi flexpriority ept vpid fsgsbase smep erms xsaveopt dtherm ida arat pln pts
```

Если вывод команды не пуст, значит процессор поддерживает аппаратную виртуализацию.

В случае если у команды пустой вывод, возможно, процессор не поддерживает виртуализацию либо функция отключена в BIOS материнской платы.

После проверки можно приступать к развертыванию средства виртуализации.

Установка и начальная настройка

Для установки пакетов сервера виртуализации **libvirt** выполните команду:

```
dnf install libvirt qemu-kvm virt-install virt-manager openssh-askpass OVMF boost-random boost-program-options boost-regex
```

Затем запустите и добавьте в автозагрузку службу сервера **libvirtd**:

```
systemctl enable libvirtd --now
```

Проверьте статус службы сервера **libvirtd**:

```
systemctl status libvirtd
```

В статусе должно быть указано **active (running)**.

Перезагрузите компьютер для загрузки модулей ядра **kvm** (если используется процессор Intel, также должен загрузиться модуль **intel-kvm**).

После перезагрузки проверьте загрузку модулей.

```
lsmod | grep kvm

kvm_intel   196608   3
kvm         598016   1    kvm_intel
```

Дополнительно рекомендуется проверить сетевые подключения:

```
ifconfig
```

Должно появиться дополнительное подключение **virbr0**.

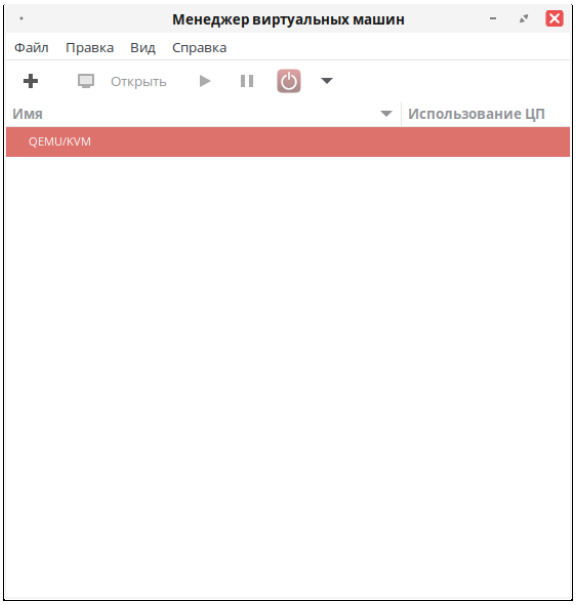
Добавьте пользователя (в примере **user**), используемого для управления виртуальными машинами, в группу **libvirt**.

```
usermod -a -G libvirt user
```

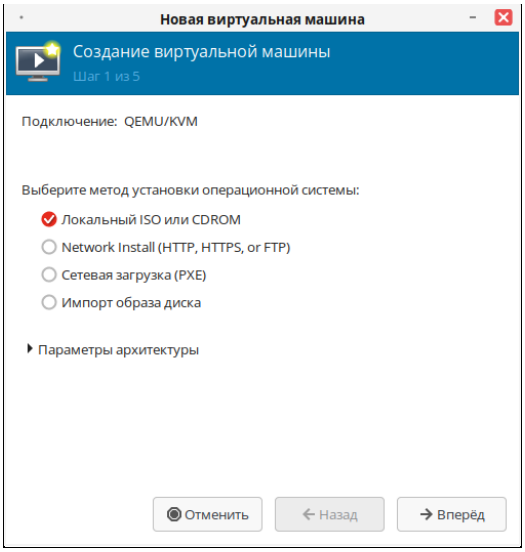
На этом установка и начальная настройка завершены.

Создание виртуальной машины

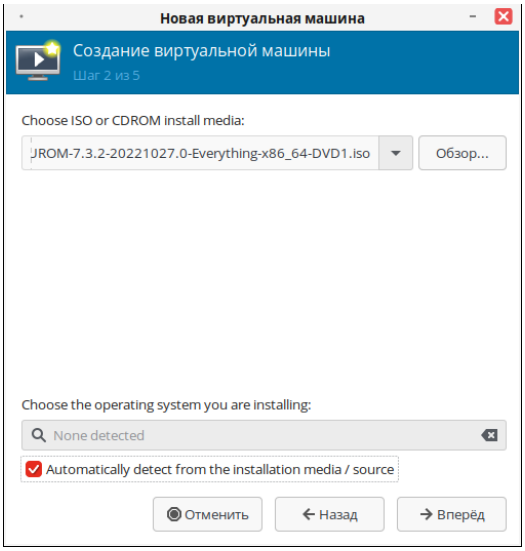
Для создания виртуальной машины можно воспользоваться графической утилитой **virt-manager**. Запуск утилиты доступен из «**Главного меню**» — «**Системные**» — «**Менеджер виртуальных машин**».



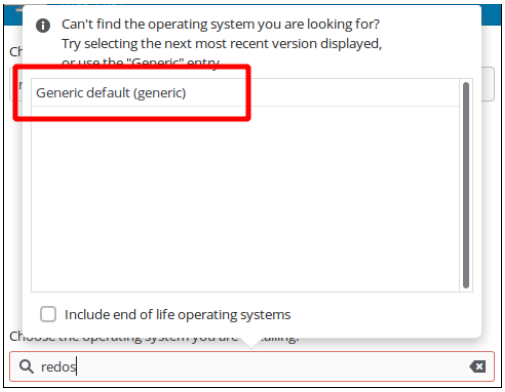
В меню **Файл** выберите **Создать виртуальную машину**. В открывшемся окне выберите метод, с помощью которого будет производиться установка операционной системы. В примере, установка производится из образа **iso**. Нажмите **Вперед**.



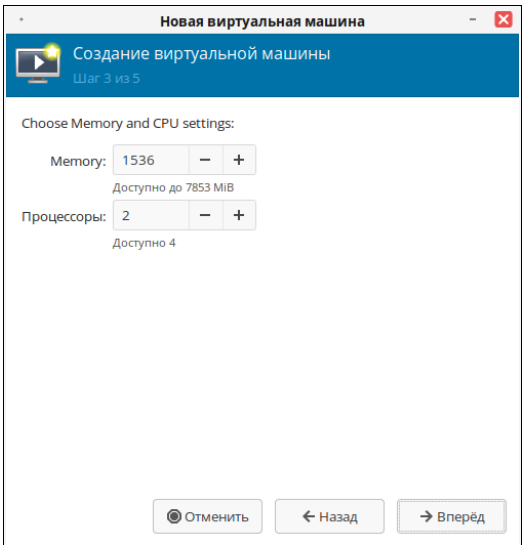
Далее необходимо указать путь к ISO-образу устанавливаемой системы, нажав кнопку «**Обзор...**».



Снимите флаг в поле «**Automatically detect from the installation media/source**» и в строке выбора типа ОС начните вводить ее название (в примере **redos**), будет выведен список доступных ОС, из которых потребуется выбрать нужную систему. Если нужной ОС нет в списке, выберите стандартную конфигурацию — **Generic**.

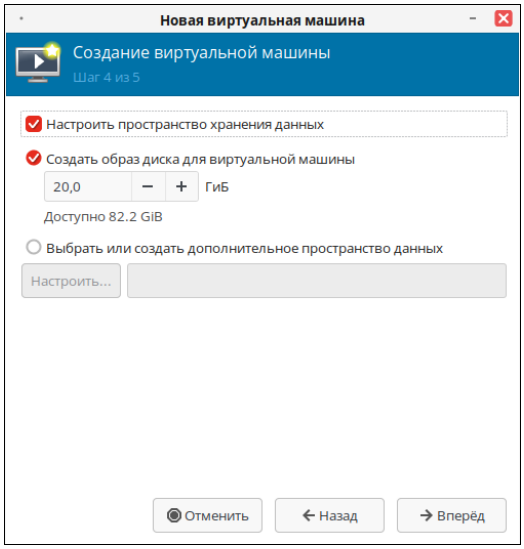


Определите оптимальное количество ОЗУ и процессоров, исходя из доступных данных. Виртуальной машине понадобится достаточный для ее работы объем оперативной памяти (как минимум 512 Мбайт). Стоит помнить, что ВМ используют физическую память. Выполнение слишком большого числа гостевых ОС или предоставление ОС недостаточного объема памяти может привести к повышенному использованию виртуальной памяти и области подкачки.



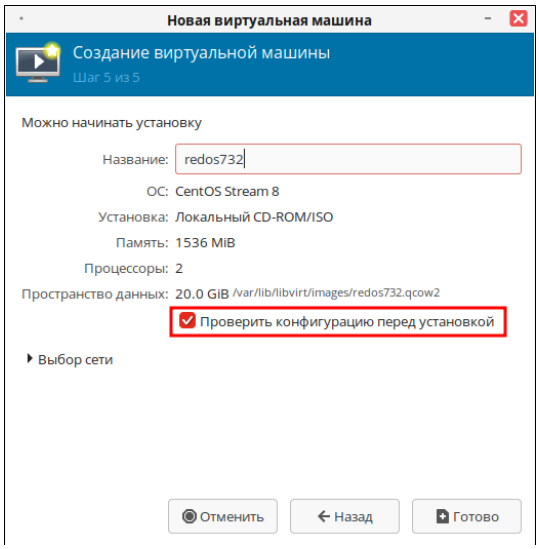
Далее необходимо настроить хранилище данных. Объем хранилища должен превышать минимально необходимый объем памяти, требуемый для установки системы. Минимально рекомендуемым объемом для РЕД ОС является **20 ГБ**.

Также, при желании, можно выделить дополнительное пространство для гостевой ОС.

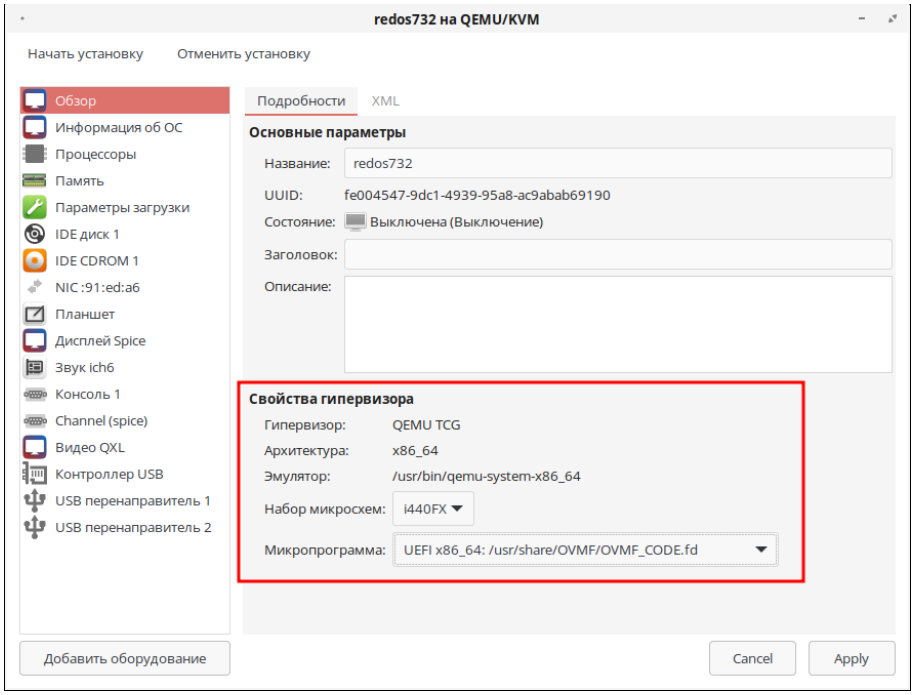


Проверьте правильность всех настроенных параметров. Если необходимо внести изменения, нажмите кнопку «**Назад**». Установите флаг в пункте «**Проверить конфигурацию перед установкой**».

Настройте сеть, если необходимо. Если все настроено верно, нажмите кнопку «**Готово**».

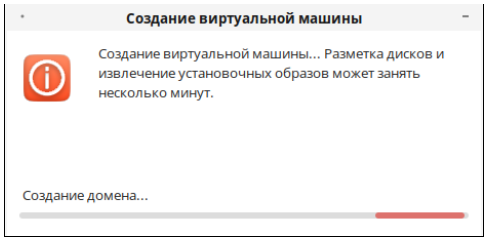


Будут открыты параметры виртуальной машины, где можно будет произвести дополнительные настройки. В свойствах гипервизора доступен выбор загрузчика системы — BIOS или UEFI. Для применения изменений нажмите «**Применить**».

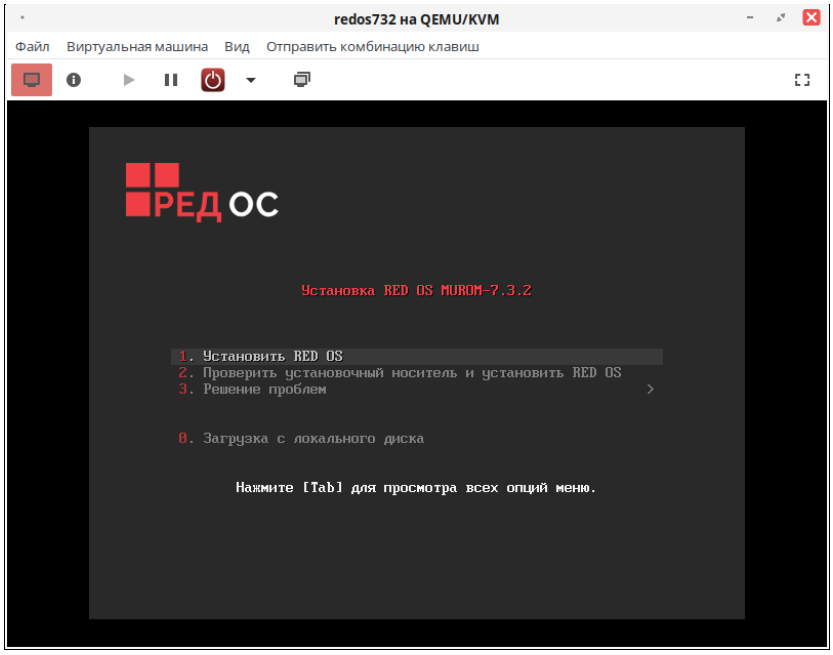


Если все необходимые настройки заданы, нажмите «**Начать установку**» в верхнем левом углу окна.

Будет запущен процесс создания ВМ.



После успешного создания ВМ будет открыта консоль, в которой можно приступить к стандартной установке ОС.



Управление ВМ

Под управлением ВМ подразумеваются такие действия, как:

- мониторинг состояния и ресурсов ВМ;
- управление питанием ВМ;
- создание снимков гостевой системы.

Управление ВМ через графический менеджер

Менеджер **virt-manager** предоставляет графический интерфейс для доступа к гипервизорам и виртуальным машинам в локальной и удаленных системах.

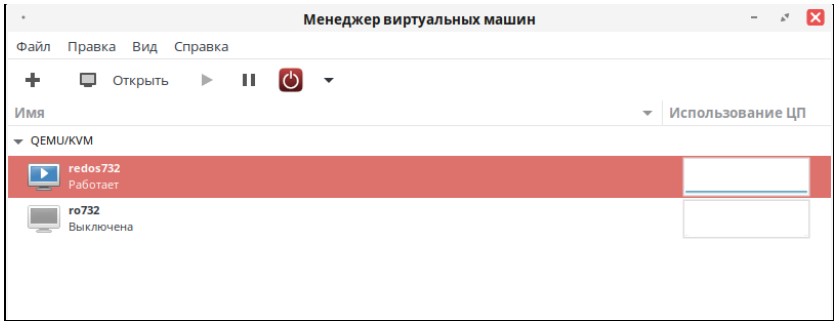
Кроме того, **virt-manager** выполняет управляющие функции:

- выделение памяти;
- выделение виртуальных процессоров;
- мониторинг производительности;
- сохранение и восстановление, приостановка и возобновление работы, запуск и завершение работы виртуальных машин;
- доступ к текстовой и графической консоли.

Просмотр информации о гостевой системе

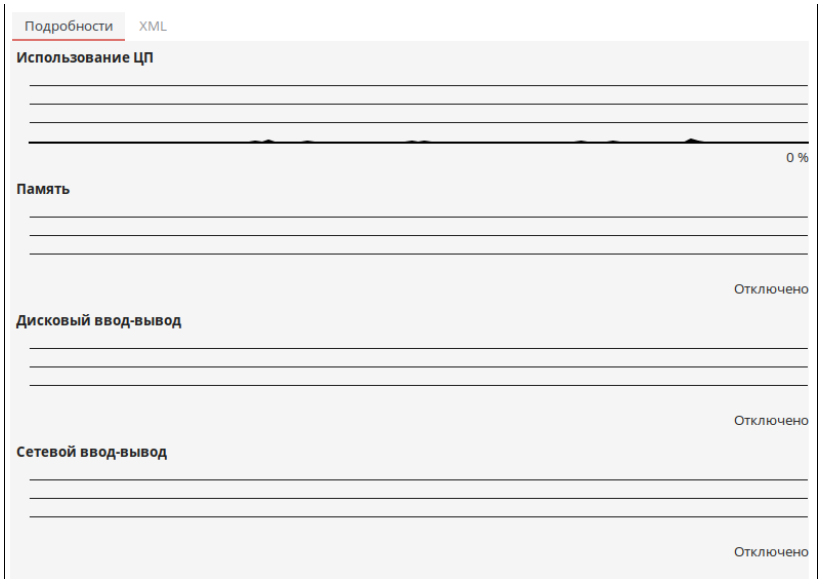
С помощью менеджера виртуальных машин можно получить доступ к подробной информации обо всех виртуальных машинах. Для этого выполните следующий алгоритм действий:

1. В главном окне менеджера выберите виртуальную машину.



2. В пункте меню «**Правка**» выберите «**Свойства виртуальной машины**» или дважды нажмите ЛКМ по имени ВМ.

Будет выведено окно с подробными сведениями о виртуальной машине, на вкладке «**Производительность**» будет доступна информация об использовании ресурсов процессора и памяти.

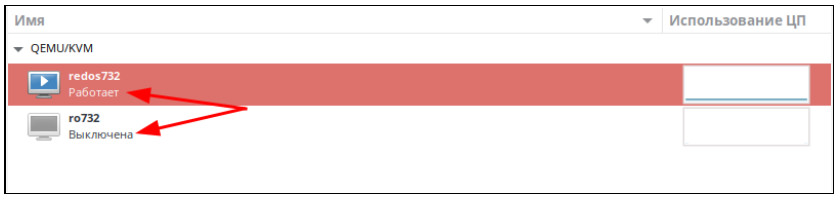


Просмотр состояния виртуальной машины

Состояния ВМ отображаются в главном окне менеджера в списке созданных ВМ под их названием.

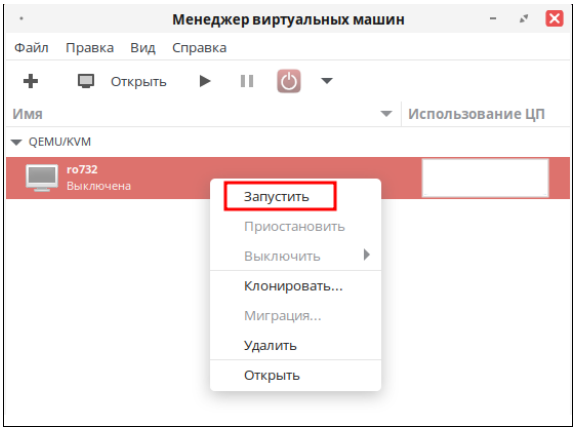
Состояния могут принимать следующие значения:

- работает;
- выключена;
- пауза;
- сохранено.



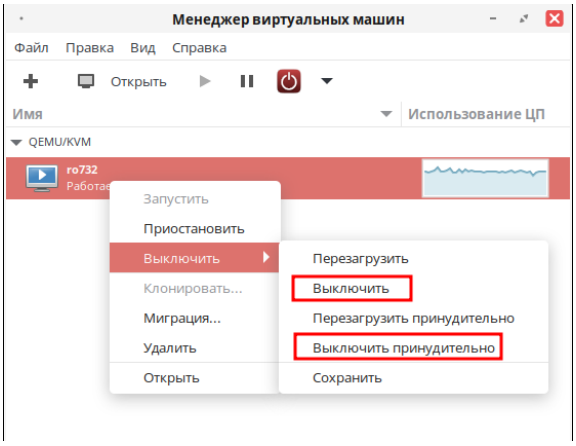
Запуск ВМ

Для запуска ВМ выберите ее в списке, нажмите ПКМ и выберите «**Запустить**».



Выключение ВМ

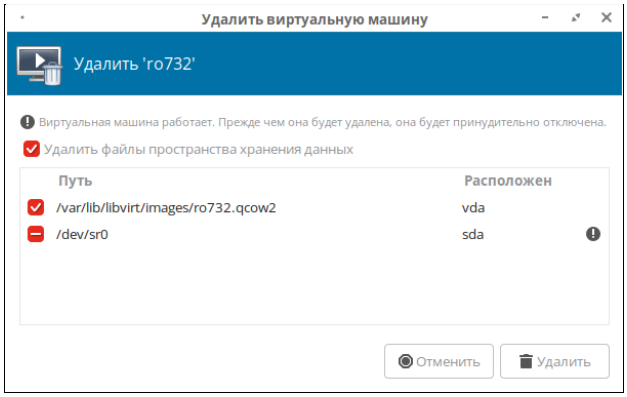
Для выключения ВМ выберите ее в списке, нажмите ПКМ и выберите «**Выключить**» — «**Выключить**» или «**Выключить**» — «**Выключить принудительно**».



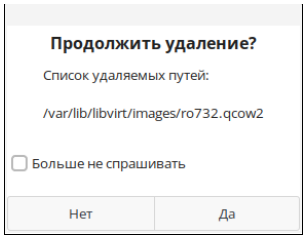
Удаление ВМ

Для удаления ВМ в менеджере необходимо выбрать нужную ВМ и нажать ПКМ по ее имени. В открывшемся контекстном меню выберите «**Удалить**».

Далее потребуется указать необходимость удаления пространства хранения данных. После определения всех настроек нажмите «**Удалить**».



Подтвердите удаление ВМ и всех ее данных.



После этого выбранная ВМ будет полностью удалена.

Управление ВМ с помощью утилиты virsh

Просмотр списка виртуальных машин ВМ

Для просмотра списка виртуальных машин и их состояния выполните:

```
virsh list
```

Можно добавить аргументы:

- `--inactive` — покажет список неактивных доменов (неактивным считается тот домен, который был определен, но в настоящий момент не является активным).
- `--all` — покажет все виртуальные машины независимо от их состояния.

Например:

```
 virsh list --all

ID    Имя       Состояние
----------------------------
1     ro732     работает
-     redos732  выключен
```

Столбец «**Состояние**» может содержать следующие значения:

- `работает` — работающие виртуальные машины, т.е. те машины, которые используют ресурсы процессора в момент выполнения команды;
- `заблокирован` — заблокированные, неработающие машины. Такой статус может быть вызван ожиданием ввода/вывода или пребыванием машины в спящем режиме;
- `приостановлен` — приостановленные домены. Данное состояние наступает, когда администратор нажал кнопку паузы в окне менеджера виртуальных машин или выполнил команду virsh suspend. В приостановленном состоянии гостевая ОС продолжает потреблять ресурсы, но не может занимать больше процессорных ресурсов;
- `выключен` — виртуальные машины, завершающие свою работу. При получении виртуальной машиной сигнала завершения работы, она начнет завершать все процессы. Стоит отметить, что некоторые операционные системы не отвечают на такие сигналы.

Запуск ВМ

Для запуска ВМ выполните команду вида:

```
virsh start <ID_домена, имя_домена, UUID_домена>
```

Приостановка ВМ

Для приостановки ВМ выполните команду вида:

```
virsh suspend <ID_домена, имя_домена, UUID_домена>
```

В этом состоянии виртуальная машина все еще продолжает использовать системную память, но освобождает ресурсы процессора. Операции ввода и вывода приостанавливаются. Работа виртуальной машины может быть возобновлена с помощью команды `resume`.

Возобновление работы ВМ

Для возобновления работы ВМ выполните команду вида:

```
virsh resume <ID_домена, имя_домена, UUID_домена>
```

Работа машины будет возобновлена немедленно.

Сохранение состояния ВМ

Для сохранения текущего состояния ВМ выполните команду:

```
virsh save <ID_домена, имя_домена, UUID_домена> <файл>
```

В результате выполнения данной команды виртуальная машина будет остановлена, а ее данные будут сохранены в заданный файл (это может занять некоторое время в зависимости от доступного гостевой ОС объема памяти). Состояние может быть позднее восстановлено с помощью команды `restore`.

Восстановление виртуальной машины

Чтобы восстановить виртуальную машину, ранее сохраненную с помощью команды `virsh save`, выполните команду:

```
virsh restore <файл>
```

Сохраненная машина будет восстановлена из файла и перезапущена, что может занять некоторое время. Имя и идентификатор **UUID** виртуальной машины останутся неизменными, но будет предоставлен новый идентификатор домена.

Завершение работы виртуальной машины

Для завершения работы ВМ выполните:

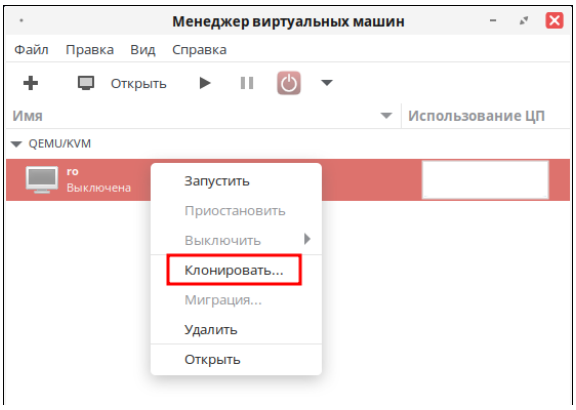
```
virsh shutdown <ID_домена, имя_домена, UUID_домена>
```

Поведение выключаемой гостевой ОС можно контролировать с помощью параметра `on_shutdown` в ее файле конфигурации.

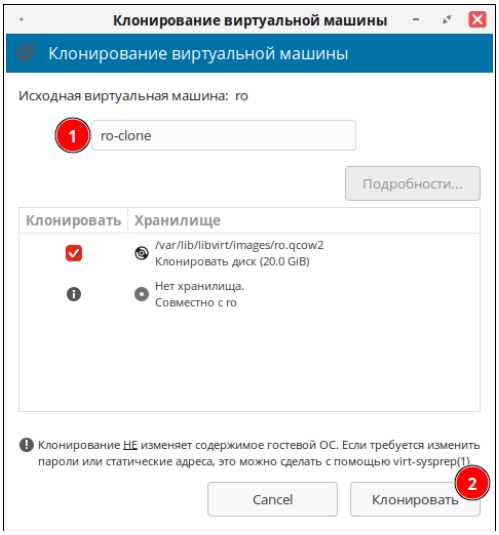
Клонирование виртуальных машин

Клонирование ВМ представляет собой процесс создания точной копии существующей ВМ. Этот метод устраняет необходимость ручной настройки каждой новой виртуальной машины, экономя значительное время и усилия системных администраторов. Клонирование может использоваться для различных целей, включая создание резервных копий, настройку тестовых сред, развертывание нескольких экземпляров одной и той же системы и облегчение разработки и тестирования программного обеспечения.

Для клонирования настроенной ВМ необходимо ее предварительно выключить. После этого в графическом менеджере виртуальных машин выберите необходимую ВМ и вызовите контекстное меню, нажав ПКМ по выбранном ВМ. В появившемся меню выберите «**Клонировать...**».



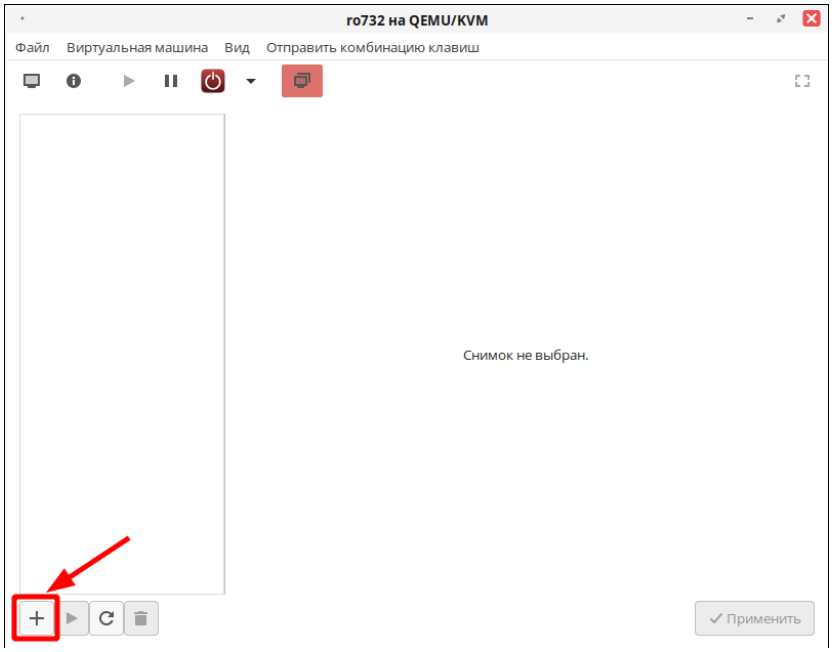
Укажите название новой ВМ и выберите клонируемое хранилище данных. Нажмите «**Клонировать**».



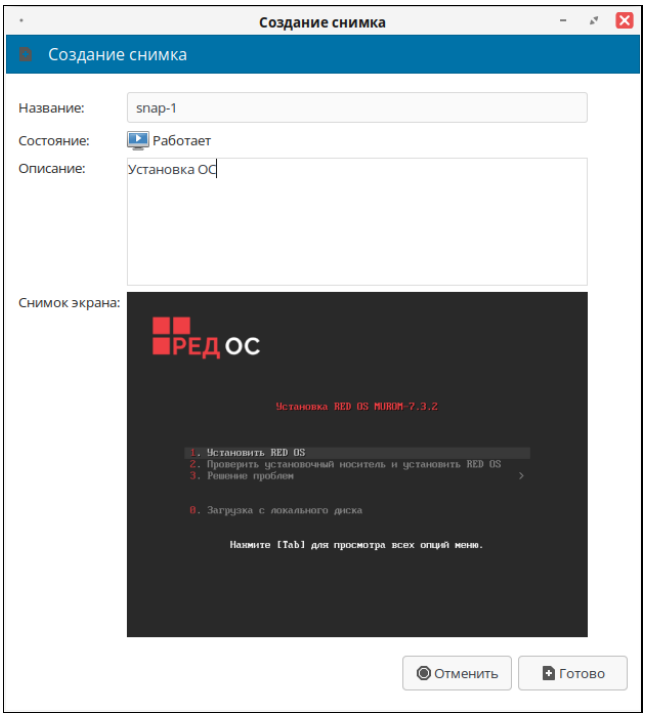
Создание снапшотов

Для создания снимка (снапшота) ВМ необходимо открыть консоль ВМ и перейти на вкладку «**Снимки**», нажав кнопку «**Управление снимками**» ( ).

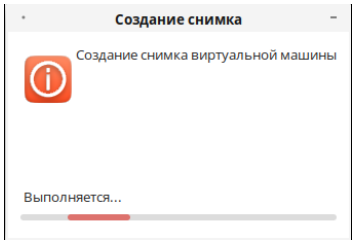
Для создания нового снимка ВМ нажмите кнопку «**Создать новый снимок**».



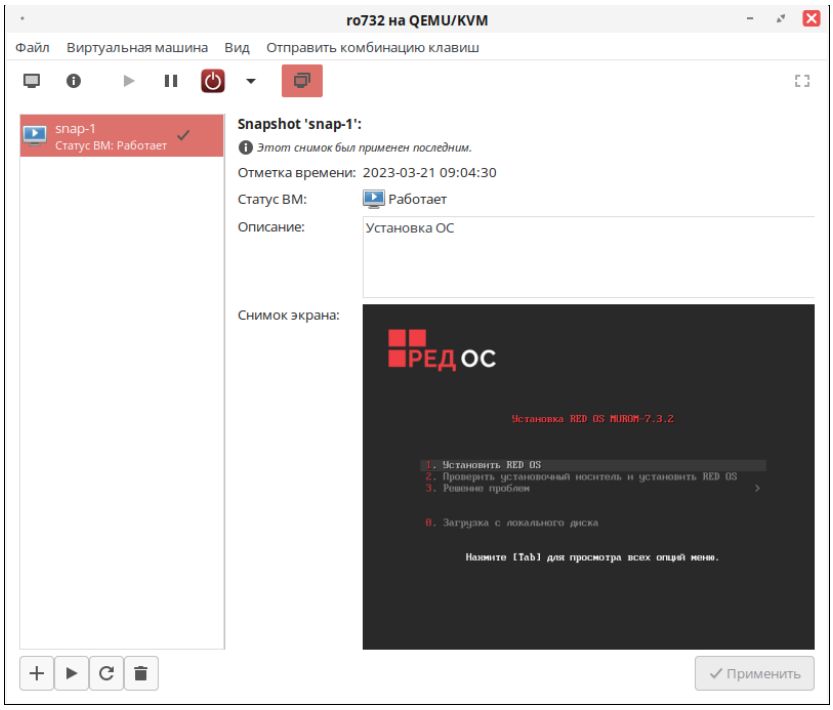
Будет открыто окно «**Создание снимка**», в котором необходимо указать название (обязательно) и описание (по желанию) снимка.



Нажмите кнопку «**Готово**» для запуска процесса создания снимка ВМ.



После этого снимок будет доступен в списке для дальнейшей работы. При выборе конкретного снимка будет отображена подробная информация о нем.



Снимки можно восстанавливать и удалять, нажав ПКМ по нужному снимку либо выбрав снимок и нажав одну из кнопок — «**Запуск выбранного снимка**» ( ) или «**Удалить выбранный снимок**» ( ).

Обновить список доступных снимков можно, нажав кнопку «**Refresh snapshot list**» ( ).

Снапшоты можно создавать как при включенной, так и при выключенной виртуальной машине.

Решение возникающих проблем

После обновления пакета **edk2-ovmf** ВМ (с загрузчиком UEFI) может не запуститься. Внешним признаком является высокая загрузка виртуального процессора (до 100%).

Данная проблема возникает из-за того, что пакет **edk2-ovmf** содержит *firmware* и шаблоны *NVRAM*. При создании виртуальных машин на основе шаблонов пакета **edk2-ovmf** формируются файлы **nvram**. После обновления пакета **edk2-ovmf** *firmware* обновляются, а файлы *nvram* остаются не обновленными. Совместимость нарушается.

Для решения данной проблемы необходимо в **XML** виртуальной машины в разделе `<os>` указать новое имя *nvram*-файла, чтобы он заново сформировался на основе нового шаблона.

Например, было: `<nvram>/var/lib/libvirt/qemu/nvram/myVM_VARS.fd</nvram>`.

Нужно задать новое имя, например: `<nvram>/var/lib/libvirt/qemu/nvram/redos733_VARS.fd</nvram>`.

Конвертация образа машины VirtualBox для KVM

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: qemu-kvm-15:8.2.7-2, libvirt-10.1.0-1, VirtualBox-7.0.20-1

Установите необходимый для виртуализации набор пакетов из стандартного репозитория. Для этого воспользуйтесь командой (потребуются права **администратора**):

```
sudo dnf install libvirt qemu-kvm virt-install virt-manager openssh-askpass OVMF boost-random boost-program-options boost-regex
```

Будет установлен **менеджер виртуальных машин**.

Затем установите **VirtualBox**, если он еще не установлен (потребуются права **администратора**):

```
sudo dnf install VirtualBox VirtualBox-guest-additions VirtualBox-kmod
```

Он будет доступен в **Главном меню** — «**Системные**» — «**Oracle VM VirtualBox**».

Вы можете подробнее ознакомиться с процессом конвертации образа машины **VirtualBox** для **KVM**, просмотрев наши обучающие видео:

- на **RuTube** — Конвертация образа машины VirtualBox для KVM;
- в **Яндекс.Дзен** — Конвертация образа машины VirtualBox для KVM;
- в **VK Видео** — Конвертация образа машины VirtualBox для KVM.

На наших каналах вы также сможете найти много другой полезной информации.

Затем **Менеджере VirtualBox** необходимо создать новый виртуальный образ ОС аналогично пункту «Создание новой ВМ в VirtualBox».

После успешного создания виртуального образа операционной системы *для конвертации* выполните команду:

```
qemu-img convert -f vdi -O qcow2 <название_образа_ВМ> <название_сконвертированного_образа_ВМ>.qcow2
```

Установка cloud-init, сценарии и использование в облачных средах

Установка cloud-init
Основные этапы работы и модули cloud-init
Сценарии для cloud-init
Локальный запуск cloud-init
Пример использования локальных сценариев
Примеры сценариев
Использование cloud-init в облачных средах
Отключение cloud-init

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: cloud-init-23.2

Cloud-init — программное обеспечение, разработанное для автоматической настройки виртуальных машин пользователя при первичном запуске. Виртуальные машины с помощью **cloud-init** автоматически конфигурируются при первой загрузке сетевыми настройками, ключами SSH, пакетами, новыми пользователями и другими системными аспектами.

Cloud-init позволяет системным администраторам экономить время и усилия по сравнению с ручной настройкой каждой виртальной машины.

Установка cloud-init

Предварительно пакет **cloud-init** должен быть установлен на виртуальной машине.

Для установки **cloud-init** выполните следующие действия:

1. Авторизуйтесь на виртуальной машине.

2. Установите пакет **cloud-init** на виртуальной машине, выполнив в терминале следующую команду с правами администратора:

```
sudo dnf install cloud-init
```

3. После установки службу **cloud-init** необходимо добавить в автозагрузку, чтобы она запускалась автоматически при старте системы. Таким образом, **cloud-init** начинает работать с момента запуска машины (**до подключения сети**), выполняя первоначальную конфигурацию.

Для запуска и добавления **cloud-init** и сопутствующих служб в гостевой системе в автозагрузку выполните команду:

```
sudo systemctl enable cloud-init cloud-config cloud-final --now
```

4. Для проверки текущего состояния служб используйте следующую команду:

```
sudo systemctl status cloud-init cloud-config cloud-final
```

При успешно выполненных настройках в статусе каждой службы должно отображаться **active (exited)**.

При возникновении проблем можно просмотреть логи **cloud-init**, которые могут помочь в диагностике:

```
sudo tail -f /var/log/cloud-init.log
```

```
sudo tail -f /var/log/cloud-init-output.log
```

Основные этапы работы и модули cloud-init

Работу **cloud-init** можно разделить на несколько ключевых этапов, каждый из которых выполняет определенные задачи для конфигурации системы. Эти этапы можно объединить в три основные фазы, каждая из которых активирует соответствующие службы **cloud-init**.

1. **Обнаружение** (**Detect**) и **локализация** (**Local**) — на этих этапах **cloud-init** определяет платформу виртуальной машины и находит

локальные источники данных. Также на этом этапе применяется сетевая конфигурация, включая резервную, и очищаются устаревшие настройки. Активные службы:

- **cloud-init-local.service**,
- **cloud-init.service**.

2. **Сетевой этап** (**Network**) и **этап конфигурации** (**Config**) — на этих этапах обрабатываются пользовательские данные, выполняются модули disk_setup и mounts, а также запускаются модули конфигурации. Активная служба:

- **cloud-config.service**.

3. **Финальный этап** (**Final**) — данный этап завершает процесс загрузки системы, начинается выполнение пользовательских задач, такие как установка пакетов, выполнение плагинов систем управления конфигурациями и запуск пользовательских скриптов. Активные службы:

- **cloud-final.service**,
- **cloud-init-hotplugd.service**.

В **cloud-init** доступно множество дополнительных модулей, расширяющих возможности конфигурации системы. Дополнительную информацию по модулям можно получить на официальном сайте. Модули можно добавлять или удалять. Они выполняются последовательно на каждом из этапов. Модули разделены на три группы в зависимости от этапа, на котором они запускаются:

- **cloud_init_modules** — модули, выполняемые на этапе инициализации, до подключения к сети;
- **cloud_config_modules** — модули, активируемые после подключения к сети на этапе конфигурации;
- **cloud_final_modules** — модули, выполняемые на финальном этапе.

Сценарии для cloud-init

При запуске системы **cloud-init** проверяет конфигурационные файлы, написанные в формате YAML, и выполняет указанные в них инструкции.

Основным конфигурационным файлом **cloud-init** является **/etc/cloud/cloud.cfg**.

Этот файл содержит ключевые настройки системы и представляет собой главный сценарий конфигурации, в котором прописываются директивы и их параметры. Каждая директива связана с конкретным модулем **cloud-init**, который выполняет определённую задачу. Конфигурационный файл можно редактировать, используя текстовый редактор.

Локальный запуск cloud-init

Для локального запуска **cloud-init** и проверки его работы можно использовать несколько команд. Эти команды помогут инициализировать, запустить модули и проверить результат работы **cloud-init**.

1. Для запуска **cloud-init** в локальном режиме используйте следующую команду:

```
sudo cloud-init init --local
```

Эта команда выполняет только локальные модули и сценарии, которые предназначены для выполнения **ДО** подключения к сети.

2. Запуск модулей **cloud-init**. Можно запускать различные модули **cloud-init** в зависимости от стадии инициализации. Команда запускает конфигурационные модули, которые предназначены для конфигурации системы, используя доступные сетевые ресурсы:

```
sudo cloud-init modules --mode=config
```

Для запуска финальных модулей, которые запускаются после полной конфигурации системы, используйте команду:

```
sudo cloud-init modules --mode=final
```

3. Для проверки текущего состояния **cloud-init** и корректного выполнения модулей используйте команду:

```
cloud-init status
```

Вывод `status: done` означает, что **cloud-init** завершил свою работу без ошибок.

Пример использования локальных сценариев

Подход позволяет автоматизировать задачи по конфигурации системы, задавая параметры на этапе запуска виртуальной машины. Сценарии могут включать установку пакетов, настройку пользователей, управление сервисами и многое другое.

Для настройки имени хоста при загрузке виртуальной машины выполните следующие действия:

1. Создайте новый файл конфигурации **my-cloud-config.cfg** в каталоге **/etc/cloud/cloud.cfg.d/**.

Все файлы с расширением ***.cfg** в этом каталоге будут прочитаны с помощью `#cloud-init`. Они читаются в лексическом порядке. Более поздние файлы перезаписывают значения в более ранних файлах.

```
sudo nano /etc/cloud/cloud.cfg.d/my-cloud-config.cfg
```

2. Вставьте следующее содержимое сценария в файл:

```
#cloud-config
hostname: my-server
fqdn: my-server.ru
manage_etc_hosts: true
```

где:

- **#cloud-config** — указывает на то, что это инструкции для cloud-init передаются в формате YAML;
- **hostname** — задает короткое имя хоста;
- **fqdn** — задает полное имя хоста;
- **manage_etc_hosts** — разрешает cloud-init управлять файлом **/etc/host.**

3. Сохраните и закройте файл, нажав `Ctrl+O`, затем `Enter`, чтобы сохранить, и `Ctrl+X`, чтобы выйти.

4. Проверьте конфигурацию. После создания или редактирования сценария можно проверить конфигурацию, запустив cloud-init в режиме проверки:

```
sudo cloud-init init --local
sudo cloud-init modules --mode=config
sudo cloud-init modules --mode=final
```

5. Примените изменения.

Для применения внесенных в конфигурацию изменений выполните:

```
sudo systemctl restart cloud-init
```

Для полной переинициализации cloud-init (Внимание! Это может привести к сбросу некоторых настроек!) выполните команды:

```
sudo cloud-init clean
sudo cloud-init init
```

6. В некоторых случаях может потребоваться перезагрузка системы:

```
reboot
```

7. Проверьте, что изменения были применены.

Например, для проверки имени хоста выполните команду:

```
hostname
```

Примеры сценариев

Пример 1. Настройка имени хоста.

```
#cloud-config
hostname: my-server
```

```
fqdn: my-server.ru
manage_etc_hosts: true
```

Пример 2. Установка пакетов.

```
#cloud-config
packages:
- git
- tox
- htop
```

Пример 3. Настройка сети.

```
#cloud-config
network:
version: 2
ethernets:
eth0:
dhcp4: true
```

При запуске новой виртуальной машины или физического сервера, система автоматически настраивает сетевой интерфейс eth0 для использования DHCPv4. Это означает, что интерфейс будет отправлять запросы на роутер или сервер DHCP в сети, чтобы получить IP-адрес и другие параметры сети.

Проверить применение настроек файла конфигурации можно с помощью команды:

```
ip addr
```

Пример 4. Запуск скриптов.

```
#cloud-config
runcmd:
- echo "Hello, World!" > /home/user/hello.txt
- systemctl start firebird.service
```

где:

- **echo "Hello, World!" > /home/user/hello.txt** — создает (или перезаписывает) файл **/home/user/hello.txt** с текстом "Hello, World!".
- **systemctl start firebird.service** — запускает службу Firebird, если она установлена на виртуальной машине.

Проверить применение настроек файла конфигурации можно с помощью команды:

```
cat /home/user/hello.txt
systemctl status firebird.service
```

Пример 5. Установка и настройка временной зоны.

```
#cloud-config
timezone: US/Eastern
```

где:

- **timezone** — настройка временной зоны.

Для проверки timezone используйте команду:

```
timedatectl           Local time: Пт 2024-09-20 06:34:40 EDT
      Universal time: Пт 2024-09-20 10:34:40 UTC
            RTC time: Пт 2024-09-20 10:34:40
           Time zone: US/Eastern (EDT, -0400)
System clock synchronized: yes
          NTP service: active
      RTC in local TZ: no
```

Пример 6. Запуск нескольких команд при первой загрузке.

Приведенный сценарий сохраняет содержимое веб-страницы в файл и запускает команду **echo** с аргументами.

```
#cloud-config
 runcmd:
- [ wget, "https://ya.ru/", -O, /tmp/index.html ]
- [ sh, -xc, "echo $(date) ': hello world!'" ]
```

где:

- **runcmd** — используется для указания списка команд, которые должны быть выполнены после завершения основной конфигурации cloud-init, но ДО первого входа в систему;
- **wget** — используется для загрузки веб-страницы https://ya.ru/ и сохранения ее содержимого в файл **/tmp/index.html**;
- **sh -xc** — запускает команду echo с аргументами **$(date) ': hello world!'**. Аргумент **-x** указывает, что команда должна быть выведена на экран перед выполнением, а **-c** указывает, что следующая строка — команда, которую нужно выполнить.

Проверьте содержимое файла **/tmp/index.html**. Если команда **wget** была выполнена успешно, то в этом файле должно быть сохранено содержимое веб-страницы. Можно просмотреть содержимое файла в терминале:

```
cat /tmp/index.html
```

Использование cloud-init в облачных средах

Применение в облачных средах:

1. **Развертывание масштабируемых приложений**.

В облачных средах для быстрого развертывания большого количества виртуальных машин **cloud-init** позволяет сократить время на настройку и конфигурацию серверов.

2. **Упрощение управления инфраструктурой**.

Вместо ручной конфигурации каждой виртуальной машины, администраторы могут создавать шаблоны конфигураций с помощью **cloud-init**. Шаблоны могут автоматически применяться к новым экземплярам виртуальных машин при их создании.

3. **Обеспечение единообразия окружения**.

Используя **cloud-init**, можно гарантировать, что каждая виртуальная машина будет иметь одинаковую базовую конфигурацию, что снижает вероятность ошибок, связанных с ручной настройкой.

Алгоритм для использования конфигурации с помощью облачного провайдера

1. **Создание конфигурационного файла**. Сохраните файл конфигурации, например, **/etc/cloud/cloud.cfg.d/my-cloud-config.cfg** в формате YAML.

2. **Использование cloud-init с образом ВМ**. Убедитесь, что ваш облачный провайдер поддерживает **cloud-init**. При создании нового экземпляра виртуальной машины в облаке загрузите созданный YAML-файл в качестве пользовательских данных.

3. **Запуск виртуальной машины**. Запустите экземпляр ВМ. **Cloud-init** автоматически выполнит конфигурацию при первом запуске.

Настройка cloud-init в облачных сервисах

В каждом облаке существует сервис, передающий виртуальной машине информацию о её окружении. Эта информация поступает в несколько типов данных, которые **cloud-init** использует в определённой последовательности.

1. **Пользовательские данные** (**user-data**). Это настройки и директивы, указанные в конфигурационном файле **/etc/cloud/cloud.cfg**. В них могут быть прописаны файлы для выполнения, пакеты для установки, скрипты оболочки и другие инструкции. Пользовательские данные, как правило, служат для настройки конкретного экземпляра виртуальной машины. Данные используются для автоматизации различных сценариев, таких как установка необходимого ПО, настройка сервера или управление конфигурациями. **Cloud-init** считывает пользовательские данные и, если они заданы в поддерживаемом формате, выполняет действия, описанные в этих данных.

2. **Метаданные** (**meta-data**). Информация об окружении виртуальной машины, такая как имя сервера, внутренний и публичный IP-адрес, идентификатор экземпляра, публичный SSH-ключ и тип виртуальной машины. Метаданные используются для настройки после применения пользовательских данных.

3 . **Данные поставщиков** (**vendor-data**). Информация, предоставляемая облачными провайдерами или разработчиками, которая помогает настроить образ виртуальной машины для корректной работы в облаке. Эти данные обычно задают конфигурации по умолчанию и применяются после метаданных.

Отключение cloud-init

В некоторых случаях, когда автоматическая настройка ВМ с использованием **cloud-init** не требуется, служба может быть отключена.

Для отключения **cloud-init** доступно несколько способов.

Способ 1. Файл отключения службы. Для отключения **cloud-init** необходимо создать пустой файл **/etc/cloud/cloud-init.disabled**:

```
sudo touch /etc/cloud/cloud-init.disabled
```

Во время загрузки система инициализации операционной системы проверит существование этого файла. Если он существует, **cloud-init** не будет запущен.

Способ 2. Отключение через конфигурацию загрузчика. Для отключения **cloud-init** необходимо добавить параметр **cloud-init=disabled** в конфигурацию загрузчика и применить настройки для загрузчика:

- для систем с **BIOS**:

```
sudo bash -c 'echo "GRUB_CMDLINE_LINUX=\"cloud-init=disabled\"" >> /etc/default/grub'
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем с **UEFI**:

```
sudo bash -c 'echo "GRUB_CMDLINE_LINUX=\"cloud-init=disabled\"" >> /etc/default/grub'
sudo grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Способ 3. Указание переменной окружения. Для отключения **cloud-init** также можно передать переменную окружения **KERNEL_CMDLINE=cloud-init=disabled** для каждого из процессов **cloud-init**:

```
sudo bash -c 'echo "DefaultEnvironment=KERNEL_CMDLINE=cloud-init=disabled" >> /etc/systemd/system.conf'
```

Установка VMware

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VMware-Player-17.6.0

Загрузите файл установки с официального сайта VMware.

После загрузки необходимо назначить файлу права на исполнение:

```
chmod +x /home/user/Загрузки/VMware-Player-17.6.0-24238078.x86_64.bundle
```

и установить дополнительные пакеты (с правами пользователя **root**):

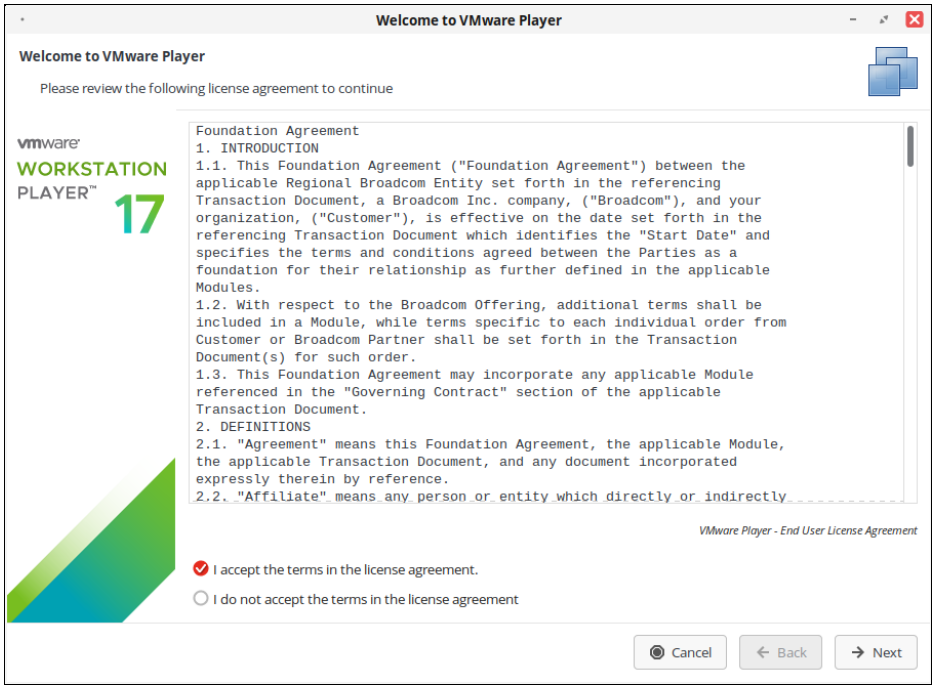
```
dnf install gcc kernel-lt-devel kernel-lt-headers
```

Перейдите в папку с загруженным файлом и выполните установку программы:

```
cd /home/user/Загрузки/
./VMware-Player-17.6.0-24238078.x86_64.bundle
```

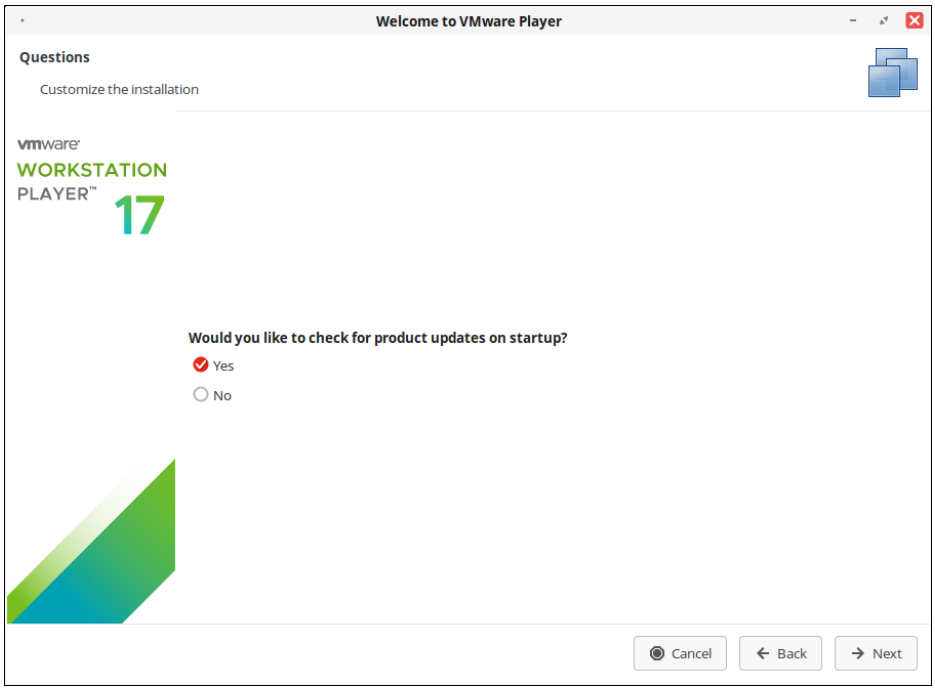
После успешной установки программу можно найти в «*Главном меню — Системные — VMware Player*».

Первый запуск программы будет выглядеть следующим образом:

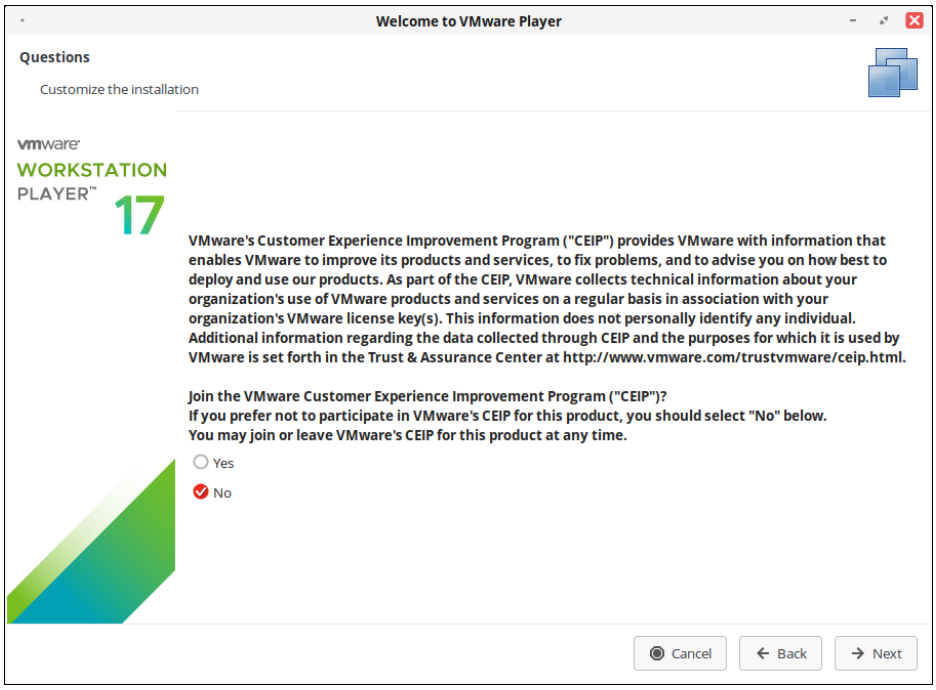


После запуска необходимо прочесть лицензионное соглашение, выбрать пункт «**I accept the terms in the license agreement**» и нажать кнопку «**Next**».

Далее необходимо указать, хотите ли вы проверять наличие обновлений при каждом последующем запуске программы. Выбираем пункт «**Yes**» (можно выбрать пункт «**No**», тогда проверка наличия обновлений будет производиться вручную).

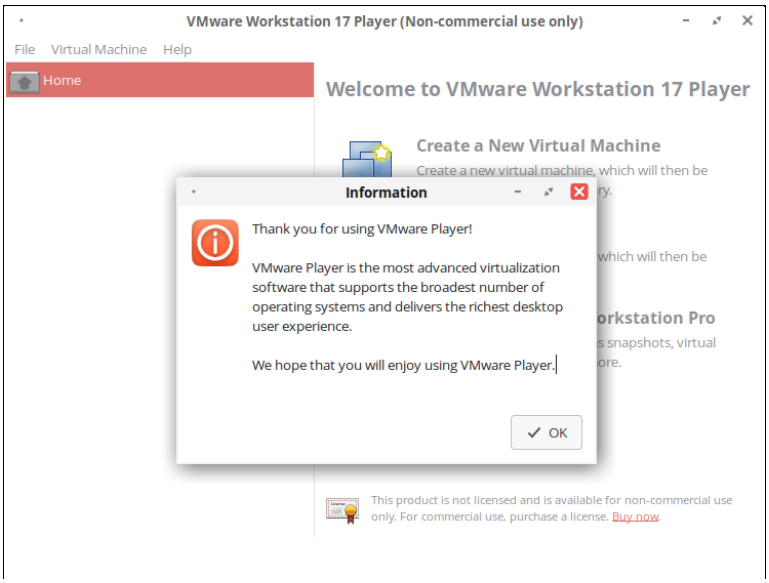


После нажатия кнопки «**Next**» установщик уточняет, хотите ли вы принимать участие в программе улучшения качества обслуживания клиентов. Это нужно для сбора технической информации об использовании VMware. Можно выбрать любой пункт, на ваше усмотрение. В данном случае выберем «**No**».



В завершении установки программа предложит ввести лицензионный ключ (при коммерческом использовании продукта) либо выбрать пункт «**Use VMware Player 17 for free for non-commercial use**» (бесплатное некоммерческое использование продукта). Выберите последний пункт и нажмите кнопку «**Finish**».

После этого откроется **VMware Workstation 17 Player** и приветственное окно.



Нажмите «**OK**» и после этого можно приступать к работе.

Установка РЕД ОС в VMware

Окружение

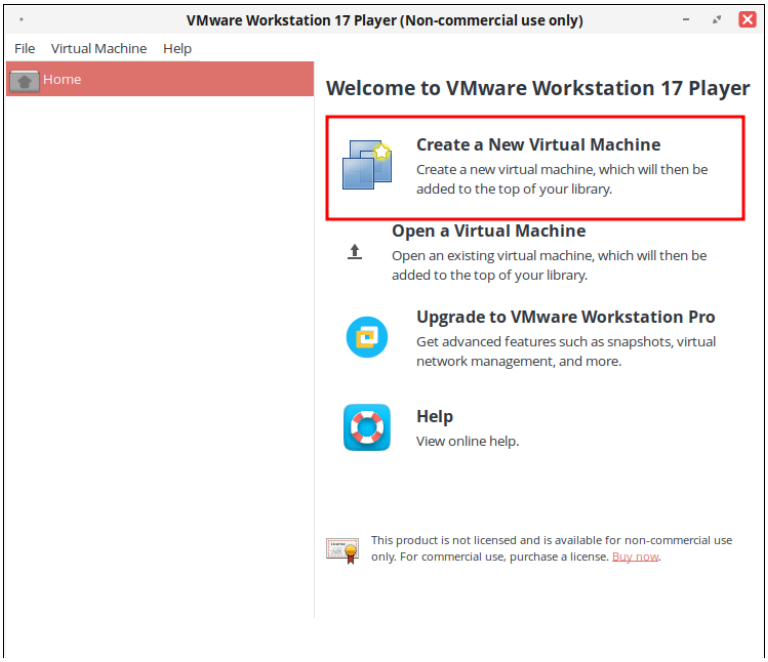
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: VMware-Player-17.6.0

Вы можете подробнее ознакомиться с информацией по установке системы в **VMware**, просмотрев наши обучающие видео:

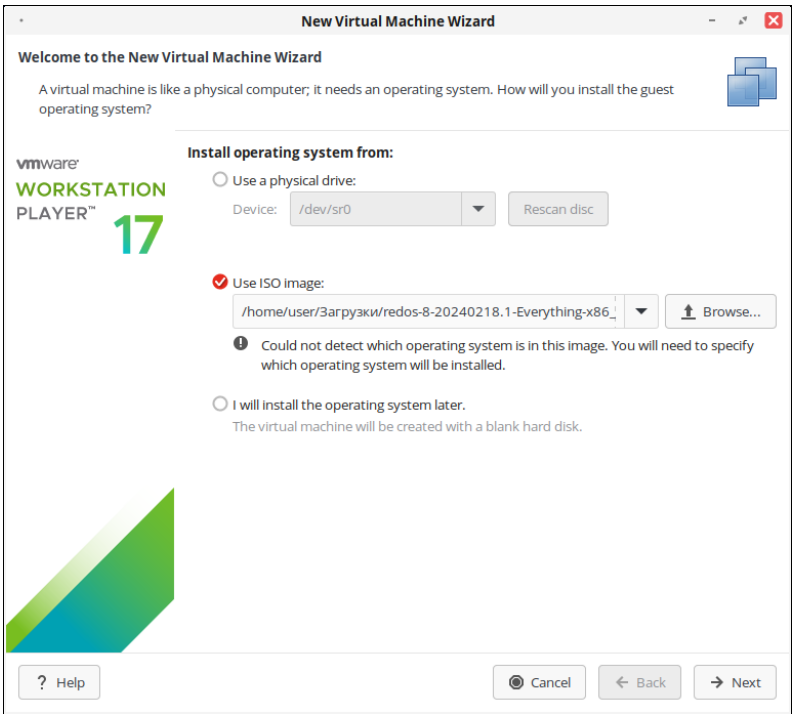
- на **RuTube** — Установка РЕД ОС в виртуальных средах на примере VMWare;
- в **Яндекс.Дзен** — Установка РЕД ОС в виртуальных средах на примере VMWare;
- в **VK Видео** — Установка РЕД ОС в виртуальных средах на примере VMWare.

На наших каналах вы также сможете найти много другой полезной информации.

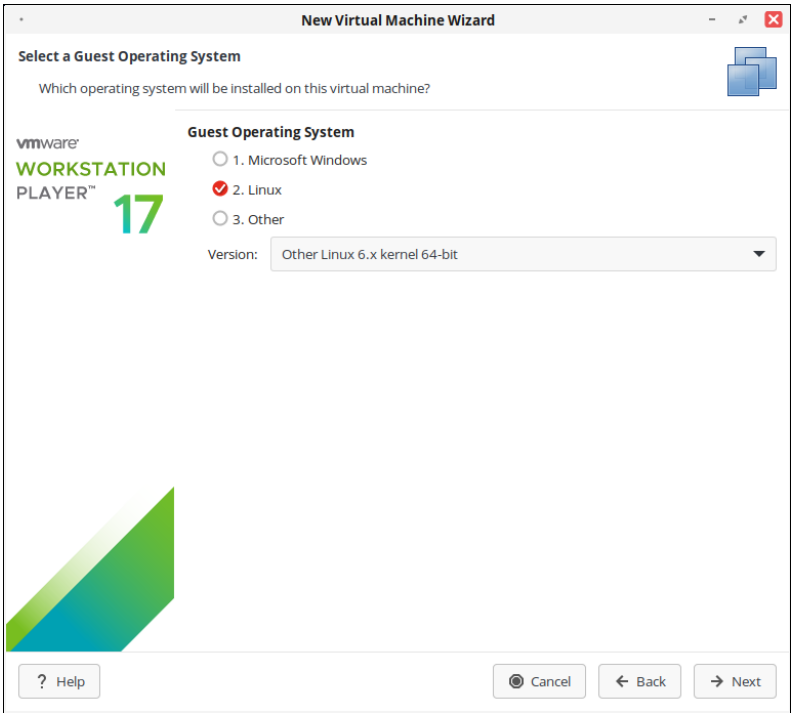
Для того чтобы начать работу в новой системе, необходимо создать новую виртуальную машину. Для этого выберите на домашней странице программы пункт «**Create a New Virtual Machine**».



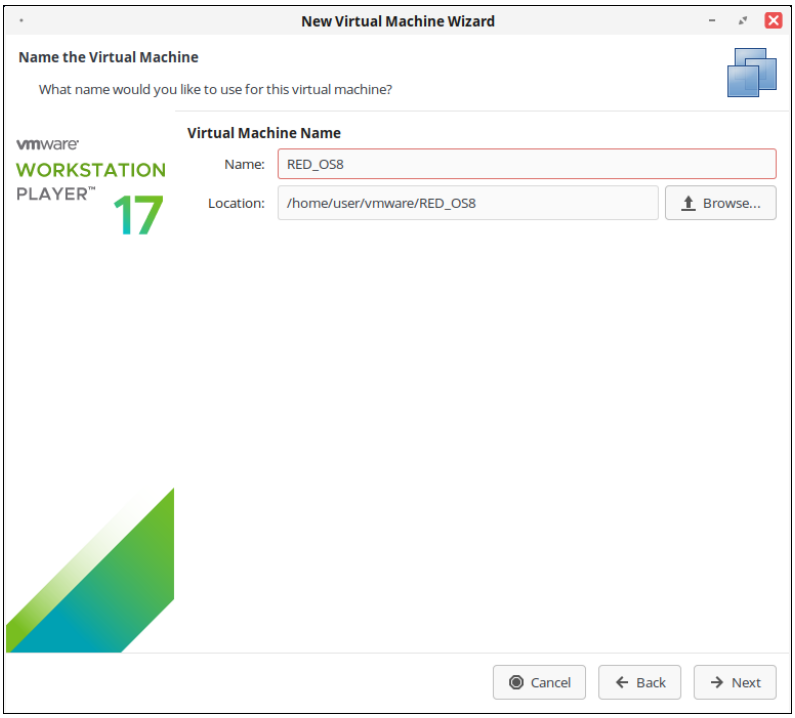
После этого откроется мастер установки, на начальном экране которого необходимо выбрать установочный диск для новой машины. Это может быть ISO-образ, сохраненный в файловой системе, или реальный привод оптических дисков.



Затем необходимо выбрать тип ОС и версию.

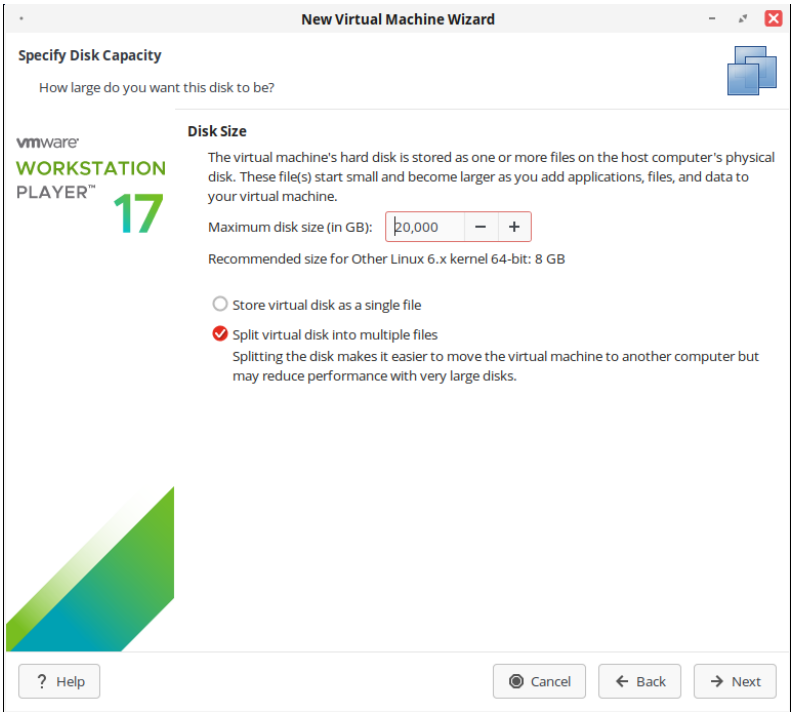


Указываем имя машины и ее расположение на диске основной системы.

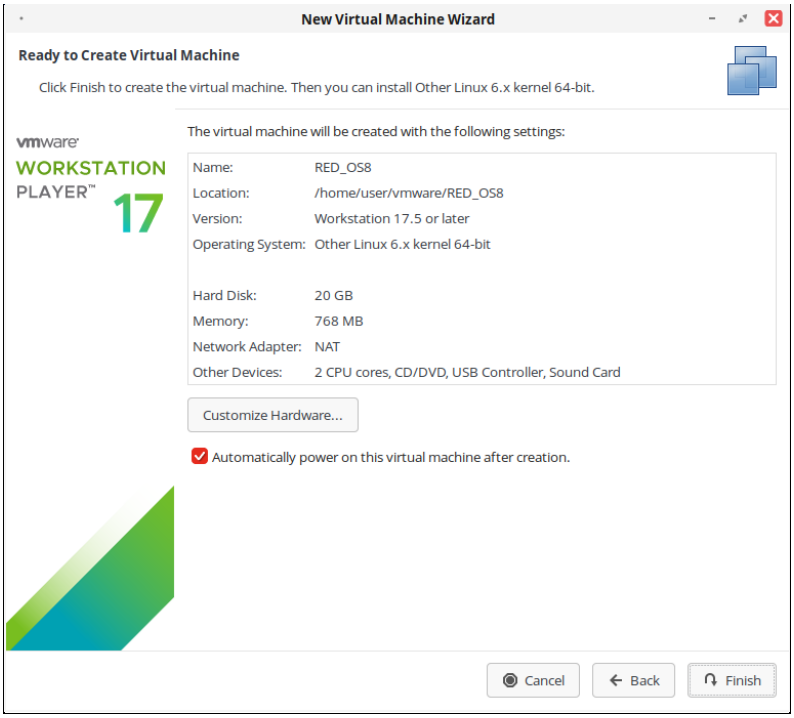


Затем необходимо установить максимальный размер жесткого диска, на который будет установлена система и будут храниться необходимые данные. Указанное значение не должно быть ниже минимально допустимого (более подробную информацию о системных требованиях см. по ссылке).

Также предлагается выбрать, разбивать ли на части жесткий диск. Обычно, если вы не планируете записывать его на небольшие носители, разбивать его не нужно.



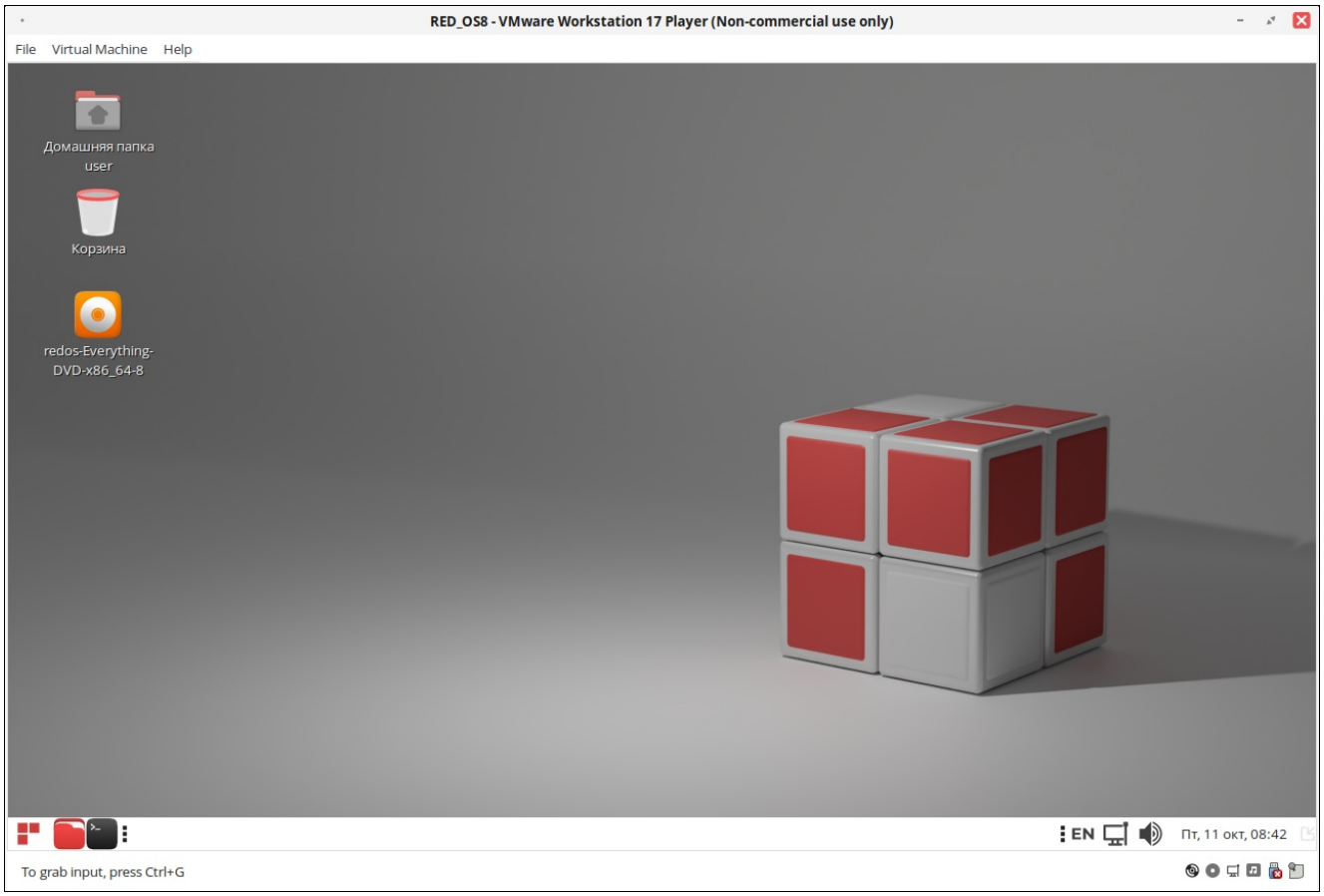
На последнем этапе предлагается просмотреть установленные данные для будущей системы, а также настроить (при необходимости) аппаратное обеспечение (кнопка «**Customize Hardware...**»).



После нажатия кнопки «**Finish**» будет произведен запуск новой виртуальной машины и можно будет начать установку непосредственно системы (подробную информацию об установке РЕД ОС см. по ссылке).



После успешной установки система будет автоматически запущена и готова к работе.


RED_OS8 - VMware Workstation 17 Player (Non-commercial use only)
File
Virtual Machine
Help
Домашняя папка user
Корзина
redos-Everything-DVD-x86_64-8
EN
Пт, 11 окт, 08:42
To grab input, press Ctrl+G

Установка VMware Tools

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: open-vm-tools-12.4.0-1, VMware-Player-17.6.0

VMWare tools — это набор специализированного программного обеспечения, который повышает производительность и обеспечивает дополнительные возможности по управлению гостевой операционной системой.

Основным преимуществом является возможность копировать/вставлять текст и перетаскивать файлы между хостом и гостевой ОС. Также в *VMware Tools* входят драйверы, необходимые для корректной работы гостевой ОС в среде виртуализации.

Установка *VMware Tools* возможна из дистрибутива с открытым исходным кодом (*Open VM Tools*).

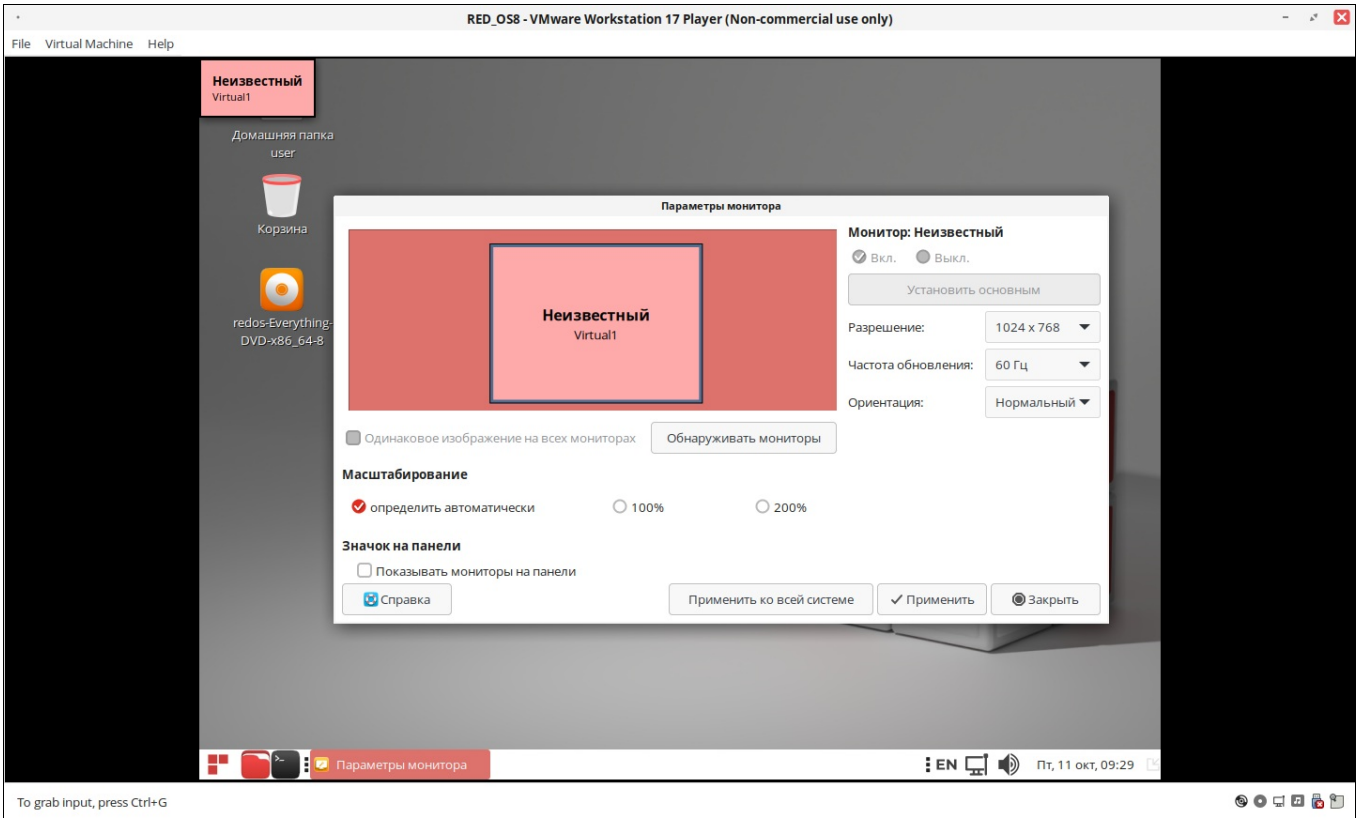
VMware рекомендует использовать дистрибутив с открытым исходным кодом, т.к. он прост в установке и обновлении, а также совместим практически со всеми популярными версиями Linux. Также он доступен в репозитории операционной системы РЕД ОС.

Вы можете подробнее ознакомиться с установкой специализированного ПО **VMware Tools**, просмотрев наши обучающие видео:

- на **RuTube** — Установка VMware Tools;
- в **Яндекс.Дзен** — Установка VMware Tools;
- в **VK Видео** — Установка VMware Tools.

На наших каналах вы также сможете найти много другой полезной информации.

Откройте *VMware* и запустите РЕД ОС.



В некоторых случаях отображение окна ВМ может производиться некорректно (остаются пустые места при разворачивании окна ВМ на весь экран), не копируется/вставляется текст между гостевой и хостовой ОС, отсутствует возможность копирования файлов простым перетаскиванием.

Для устранения данной проблемы необходимо установить пакет `open-vm-tools`.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**open-vm-tools**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.

Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install open-vm-tools open-vm-tools-desktop
```

Для того чтобы изменения вступили в силу, необходимо перезагрузить ВМ.

Для примера можно скопировать ссылку из браузера основной машины и вставить ее в браузер виртуальной машины.

Установка РЕД ОС в Hyper-V

Включение Hyper-V
Создание виртуальной машины
Настройка сети для ВМ
Настройка ВМ
Службы интеграции Hyper-V
Примечание

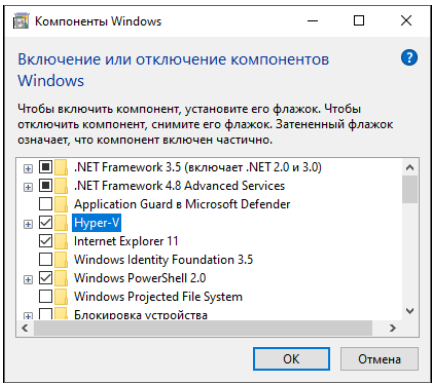
Вы можете подробнее ознакомиться с примером установки системы в Hyper-V, просмотрев наши обучающие видео:

- на **RuTube** — Установка РЕД ОС в виртуальных средах на примере Hyper-V;
- в **Яндекс.Дзен** — Установка РЕД ОС в виртуальных средах на примере Hyper-V;
- в **VK Видео** — Установка РЕД ОС в виртуальных средах на примере Hyper-V.

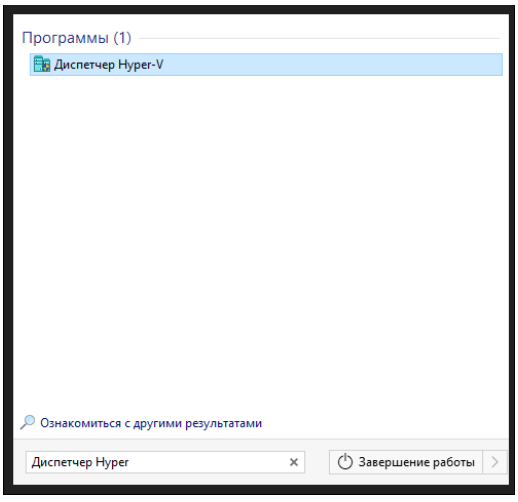
На наших каналах вы также сможете найти много другой полезной информации.

Включение Hyper-V

Убедитесь, что компоненты **Hyper-V** включены. Для этого перейдите в «**Панель управления**» - «**Программы и компоненты**» - «**Включение и отключение компонентов Windows**». Если не включены, установите флажок, нажмите «**OK**» и перезагрузите компьютер.

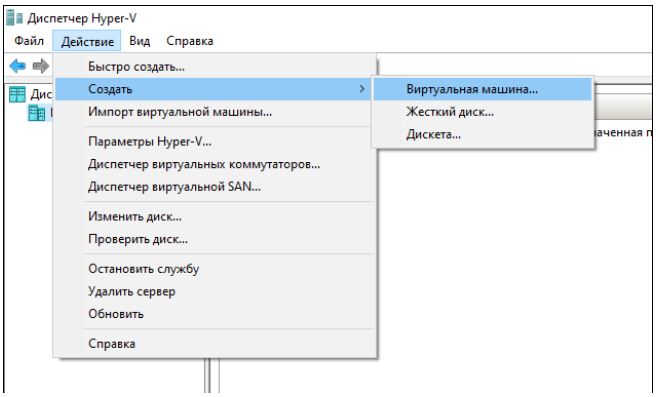


Запустите **Диспетчер Hyper-V**.

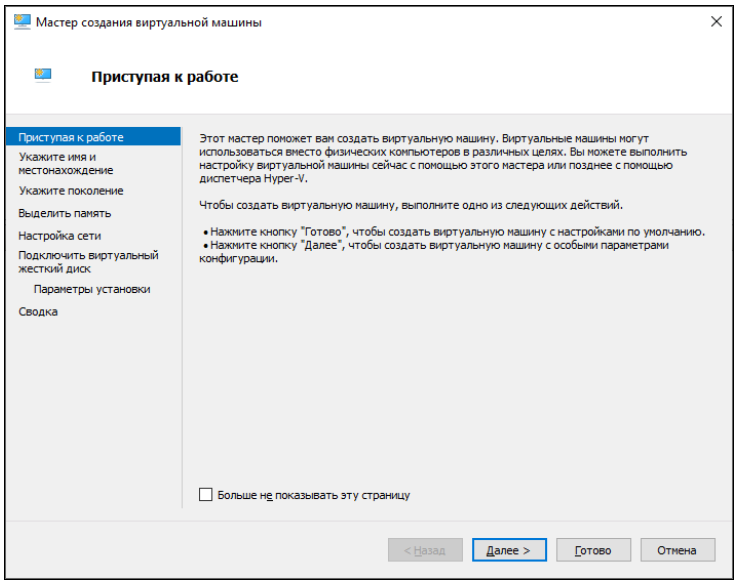


Создание виртуальной машины

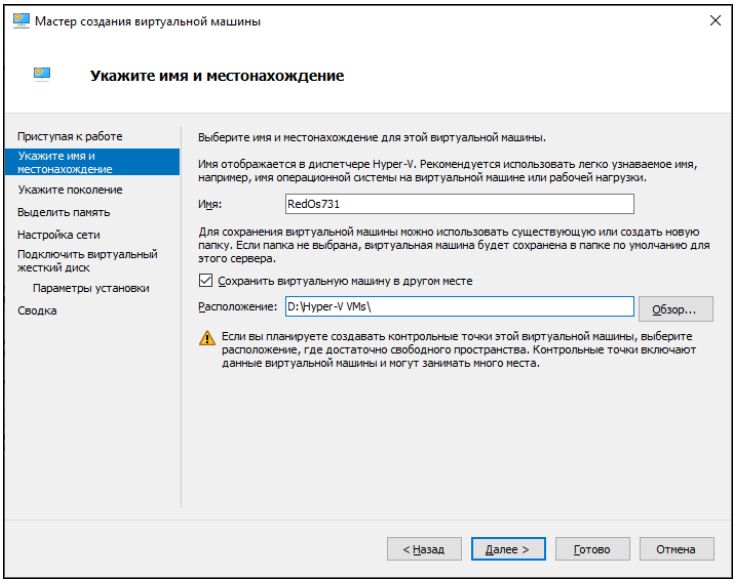
В **Диспетчере Hyper-V** нажмите на пункт меню «**Действие**» - «**Создать**» - «**Виртуальная машина**».



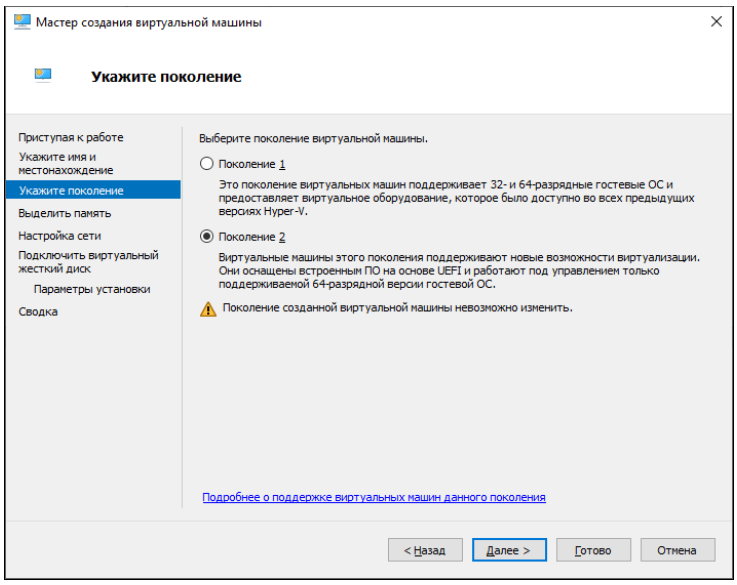
Откроется окно начальной настройки ВМ. Нажмите «**Далее**».



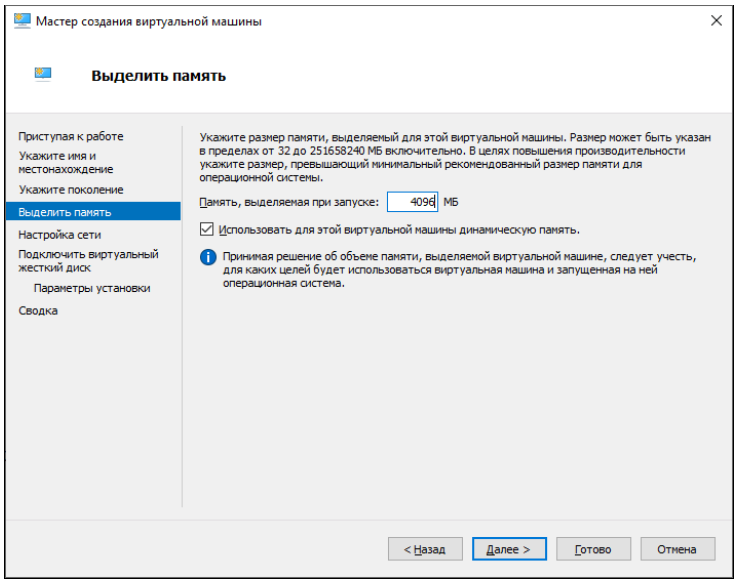
Укажите имя виртуальной машины и ее место расположения (по умолчанию она будет находиться на диске **C**). Нажмите «**Далее**».



Выберите «**Поколение 2**» виртуальной машины. Нажмите «**Далее**».

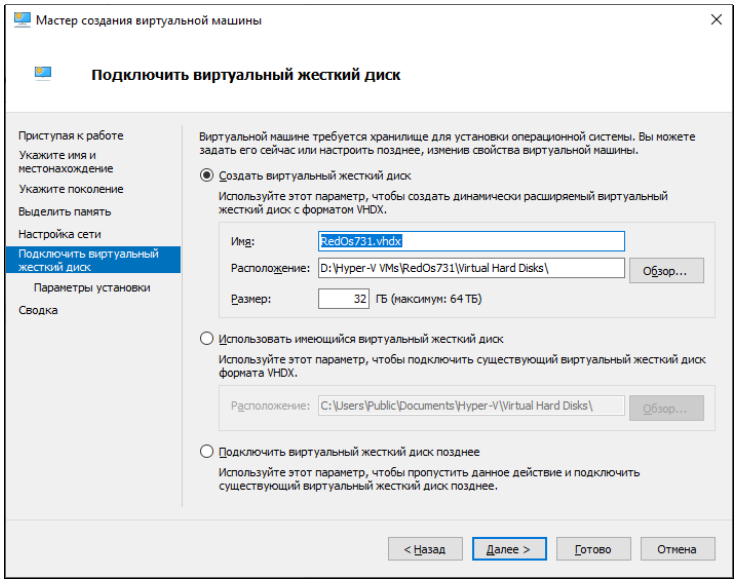


Установите максимальный объём оперативной памяти, который будет выделен для ВМ. С минимальными системными требованиями для установки РЕД ОС 8 можно ознакомиться по ссылке.

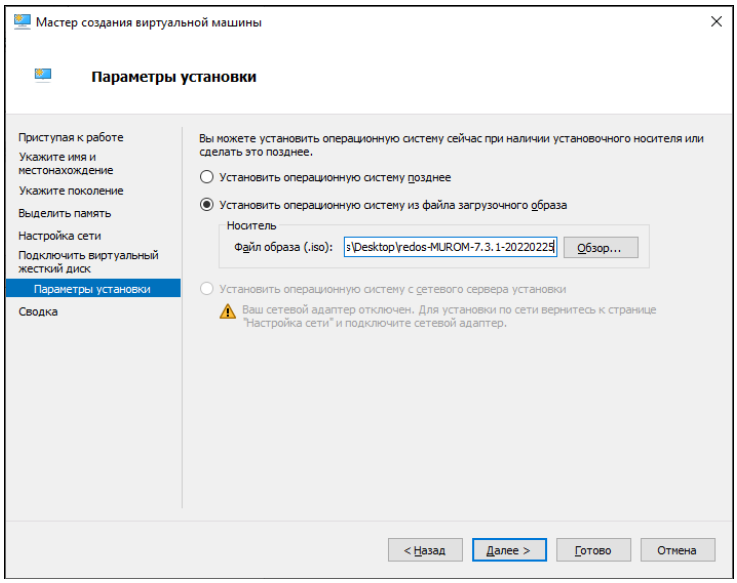


Пункт настроек сети временно пропустите.

Перейдите к настройке жесткого диска. Укажите имя жесткого диска, его место расположения и размер. Нажмите «**Далее**».



Укажите путь к установочному образу РЕД ОС. Нажмите «**Далее**».

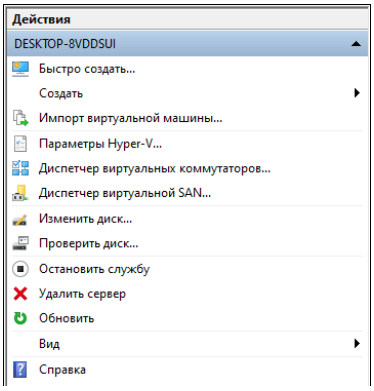


В «**Сводке**» проверьте настроенные данные и нажмите «**Готово**».

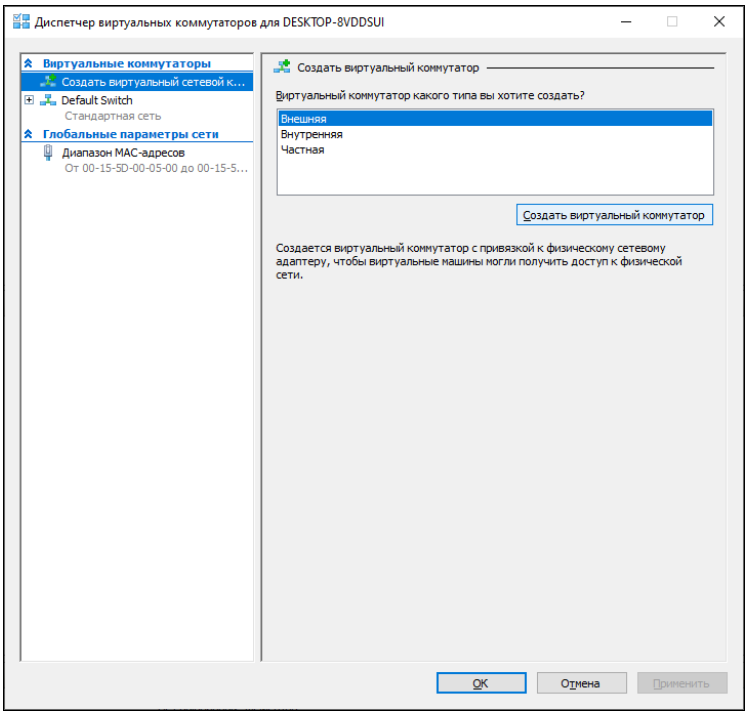
Настройка сети для ВМ

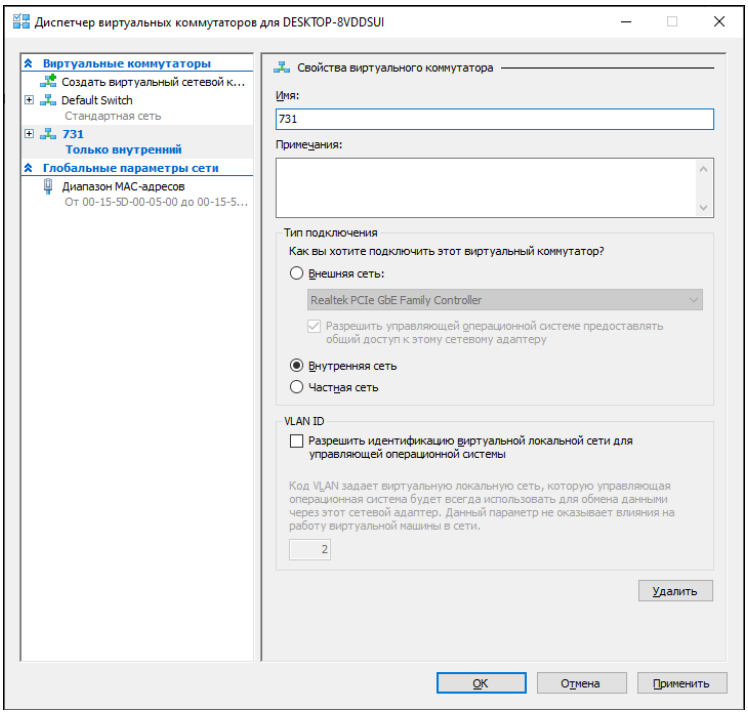
После создания ВМ настройте для нее сеть.

Для этого откройте «**Диспетчер виртуальных коммутаторов**».



Создайте виртуальный коммутатор.

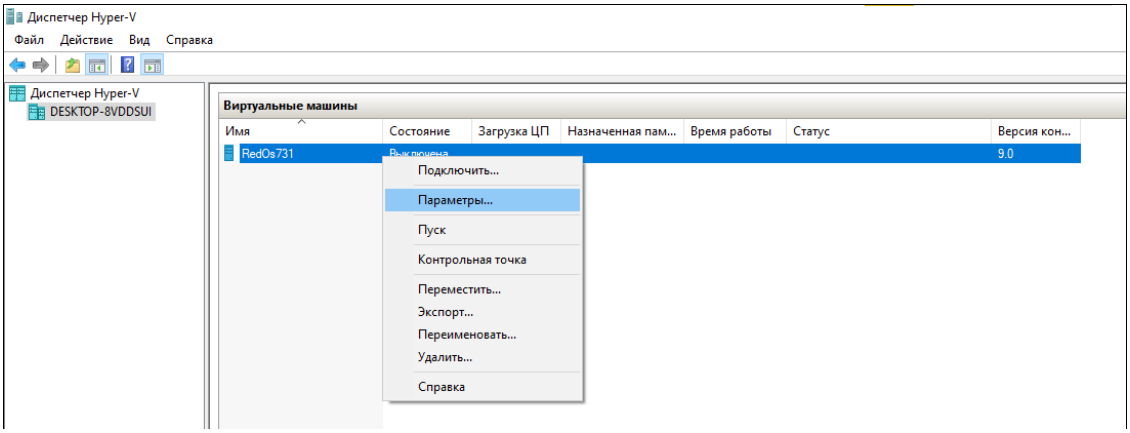




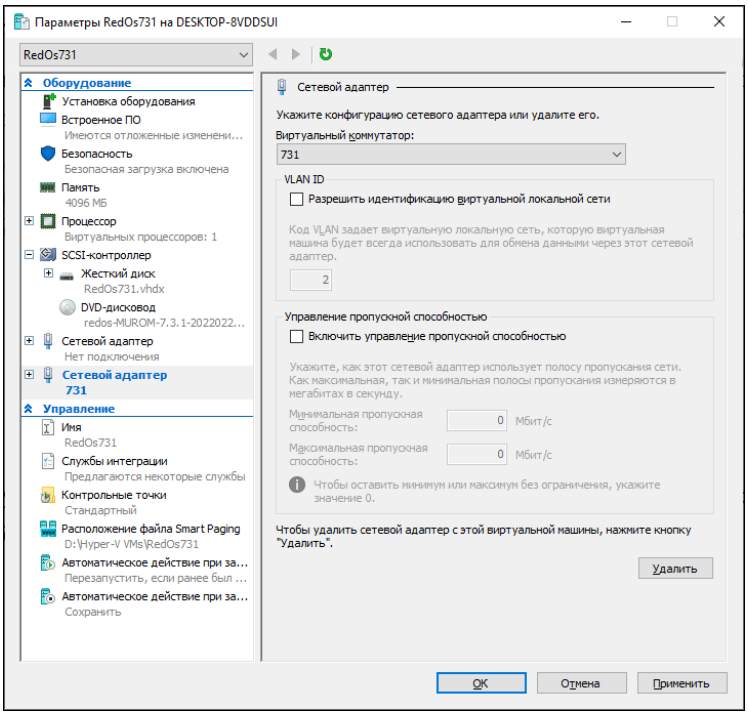
После этого закройте настройки коммутаторов и перейдите в настройки виртуальной машины.

Настройка ВМ

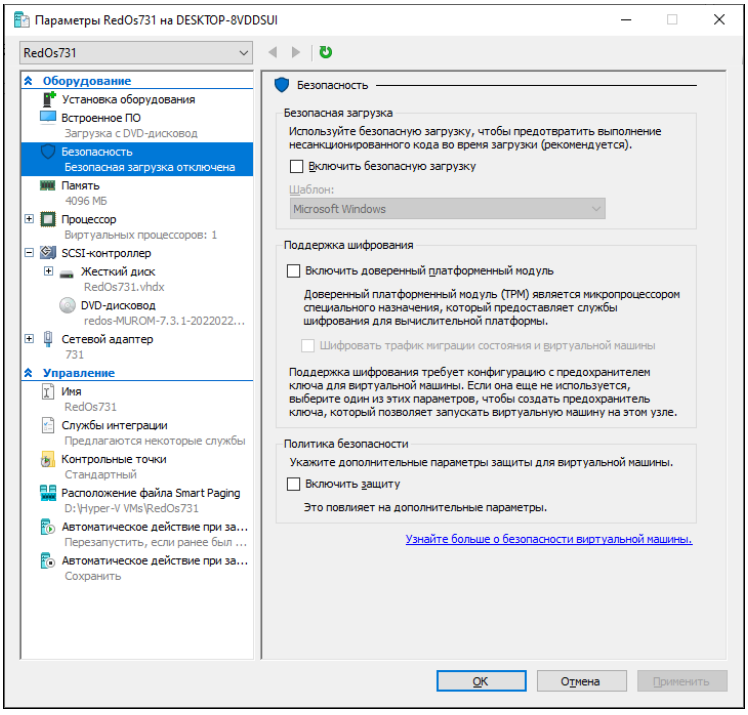
Кликните правой кнопки мыши по созданной виртуальной машине и выберите пункт «**Параметры**».



В пункте «**Установка оборудования**» выберите «**Сетевой адаптер**» и нажмите кнопку «**Добавить**». Выберите раннее созданный коммутатор.



В пункте «**Безопасность**» отключите безопасную загрузку.

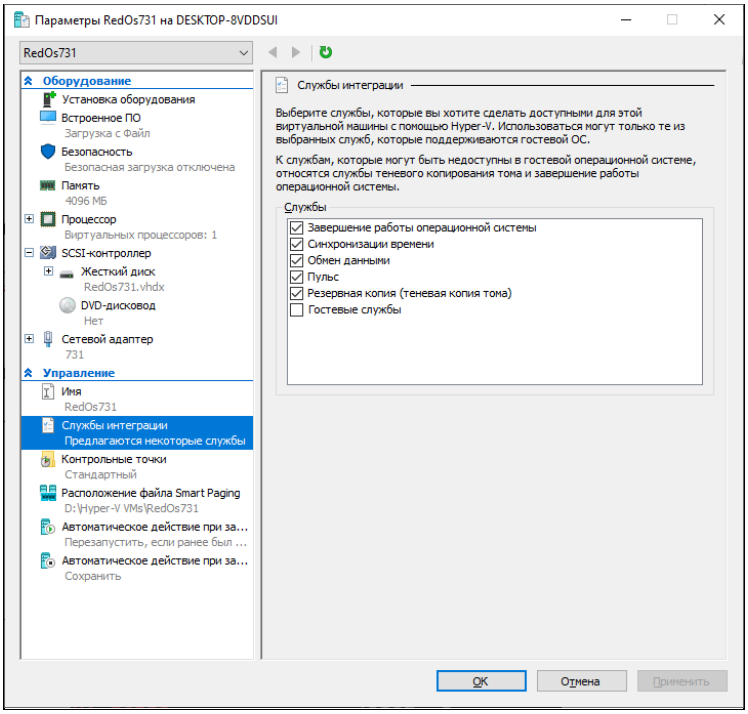


Службы интеграции Hyper-V

В РЕД ОС работают службы интеграции **Hyper-V**.

Службы интеграции - это службы, позволяющие виртуальной машине связываться с узлом **Hyper-V**.

Чтобы перейти к меню управления службами интеграции, нажмите правой кнопкой мыши по ВМ, далее «**Параметры**» - «**Службы интеграции**».

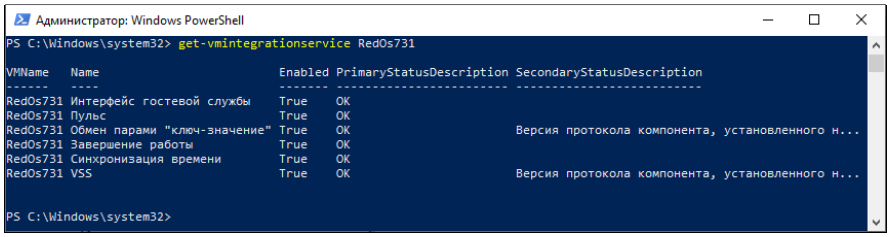


В данном меню можно включать или отключать службы интеграции.

Установите флажок в пункте «**Гостевые службы**».

Чтобы проверить состояние данных служб, в **PowerShell** введите команду:

```
get-vmintegrationservice <название_ВМ>
```

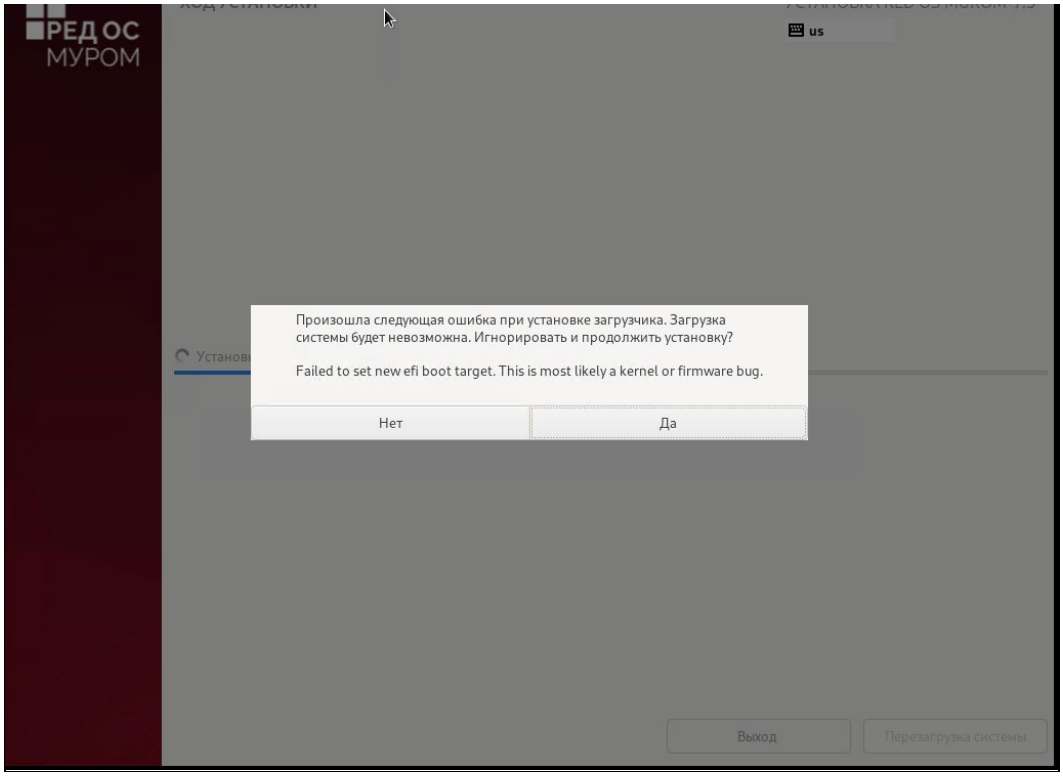


Все службы успешно работают.

После выполненных настроек запустите виртуальную машину и установите ОС в штатном режиме. Подробную информацию об установке системы см. по ссылке.

Примечание

В случае возникновения ошибки "Failed to set new efi boot target. This is most likely kernel or firmware bug. " ее можно проигнорировать и продолжить установку виртуальной машины:



На работоспособность ОС данная ошибка не влияет.

Взаимодействие Hyper-V с РЕД ОС

Изменение разрешения экрана
Служба обмена данными Hyper-V (KVP)
Служба запросов на теневое копирование томов Hyper-V
Интерфейс гостевой службы Hyper-V
Служба мониторинга состояния ВМ
Служба завершения работы в качестве гостя
Служба синхронизации времени

Изменение разрешения экрана

Чтобы изменить разрешение экрана, воспользуйтесь командой:

```
grubby --update-kernel=ALL --args="video=hyperv_fb:<разрешение_экрана>"
```

Перезапустите виртуальную машину.

Служба обмена данными Hyper-V (KVP)

Позволяет виртуальной машине и узлу обмениваться между собой простыми метаданными.

За работу службы обмена данными в системе РЕД ОС отвечает сервис **hypervkvpd.service**.

```
[user@localhost ~]$ systemctl status hypervkvpd.service
● hypervkvpd.service - Hyper-V KVP daemon
     Loaded: loaded (/usr/lib/systemd/system/hypervkvpd.service; static)
     Active: active (running) since Wed 2022-06-08 03:32:23 EDT; 1h 30min ago
   Main PID: 677 (hypervkvpd)
      Tasks: 1 (limit: 4667)
     Memory: 440.0K
        CPU: 3ms
     CGroup: /system.slice/hypervkvpd.service
             └─677 /usr/sbin/hypervkvpd -n

июн 08 03:32:23 localhost.localdomain systemd[1]: Started Hyper-V KVP daemon.
июн 08 03:32:24 localhost.localdomain KVP[677]: KVP starting; pid is:677
июн 08 03:32:24 localhost.localdomain KVP[677]: KVP LIC Version: 3.1
```

Служба запросов на теневое копирование томов Hyper-V

Позволяет службе теневого копирования томов выполнить резервное копирование виртуальной машины без ее выключения.

За работу данной службы в системе РЕД ОС отвечает сервис **hypervvssd.service**.

```
[user@localhost ~]$ systemctl status hypervvssd.service
● hypervvssd.service - Hyper-V VSS daemon
     Loaded: loaded (/usr/lib/systemd/system/hypervvssd.service; static)
     Active: active (running) since Wed 2022-06-08 03:32:23 EDT; 1h 32min ago
   Main PID: 678 (hypervvssd)
      Tasks: 1 (limit: 4667)
     Memory: 252.0K
        CPU: 866us
     CGroup: /system.slice/hypervvssd.service
             └─678 /usr/sbin/hypervvssd -n

июн 08 03:32:23 localhost.localdomain systemd[1]: Started Hyper-V VSS daemon.
июн 08 03:32:24 localhost.localdomain hypervvssd[678]: Hyper-V VSS: VSS starting; pid is:678
июн 08 03:32:24 localhost.localdomain hypervvssd[678]: Hyper-V VSS: VSS: kernel module version: 129
```

Интерфейс гостевой службы Hyper-V

Предоставляет интерфейс для узла **Hyper-V** для копирования файлов с виртуальной машины и на виртуальную машину.

За работу данной службы в системе РЕД ОС отвечает сервис **hypervfcopyd.service**.

```
[user@localhost ~]$ systemctl status hypervfcopyd.service
● hypervfcopyd.service - Hyper-V FCOPY daemon
     Loaded: loaded (/usr/lib/systemd/system/hypervfcopyd.service; static)
     Active: active (running) since Wed 2022-06-08 03:33:52 EDT; 1h 31min ago
   Main PID: 1459 (hypervfcopyd)
      Tasks: 1 (limit: 4667)
     Memory: 328.0K
        CPU: 2ms
     CGroup: /system.slice/hypervfcopyd.service
             └─1459 /usr/sbin/hypervfcopyd -n

июн 08 03:33:52 localhost.localdomain systemd[1]: Started Hyper-V FCOPY daemon.
июн 08 03:33:52 localhost.localdomain HV_FCOPY[1459]: starting; pid is:1459
июн 08 03:33:52 localhost.localdomain HV_FCOPY[1459]: kernel module version: 1
```

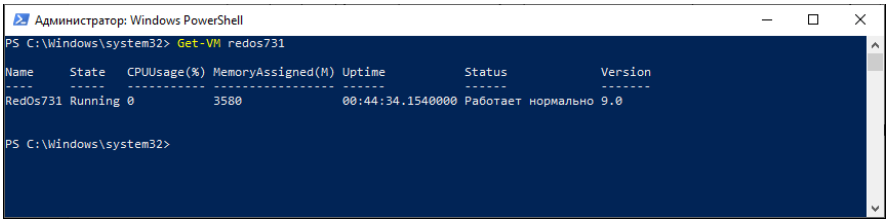
Служба мониторинга состояния ВМ

Сообщает узлу **Hyper-V**, что на виртуальной машине установлена операционная система и что она загрузилась надлежащим образом.

Чтобы увидеть статус виртуальной машины в **PowerShell** от имени администратора введите команду:

```
Get-VM <имя_виртуальной_машины>
```

За работу данной службы в системе РЕД ОС отвечает модуль **hv_utils**.



Служба завершения работы в качестве гостя

Позволяет узлу **Hyper-V** запрашивать завершение работы виртуальной машины. Компьютер виртуальной машины всегда может принудительно выключить виртуальную машину, но это похоже на нажатие кнопки выключения в отличие от корректного завершения работы.

У этой службы крайне высокая степень влияния на работу системы, т. к. при неработоспособности этой службы при каждом отключении узел не сможет корректно завершить работу ВМ, что может привести к потере или повреждению данных.

За работу данной службы в системе РЕД ОС отвечает модуль **hv_utils**.

Служба синхронизации времени

Синхронизирует системное время виртуальной машины с системным временем физического компьютера.

Эта служба также обладает высокой степенью влияния на работу, так как при каждом выключении ВМ время будет случайным образом меняться.

За работу данной службы в системе РЕД ОС отвечает модуль **hv_utils**.

Проверить, загружены ли модули, можно с помощью следующей команды:

```
lsmod | grep hv
```

```
[user@localhost ~]$ sudo lsmod|grep hv
hv_balloon             40960  0
hv_utils               49152  3
hv_netvsc              98304  0
hv_storvsc             24576  3
scsi_transport_fc      90112  1 hv_storvsc
hv_vmbus              143360  8 hv_balloon,hv_utils,hv_netvsc,hid_hyperv,hv_storvsc,hyperv_keyboard,
hyperv_drm,hyperv_fb
```

DOSBox - программный эмулятор DOS

Установка
Запуск программ
Примеры запущенных программ
Файл конфигурации
Список горячих клавиш
Автозапуск программ
Исправление проблем

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dosbox-staging-0.77.1-2

DOSBox - это программный эмулятор PC, создающий окружение **DOS**. Программа *DOSBox* является свободным программным обеспечением, которое позволяет запускать старые программы и игры на современных компьютерах и устройствах под управлением операционных систем *Windows, Linux, Android* и других.

Под *DOSBox* уверенно запустятся и будут работать различные файловые менеджеры времен **MS-DOS**, бухгалтерские и банковские программы, среды программирования, программы для радиолюбительских измерений и коммуникаций.

Установка

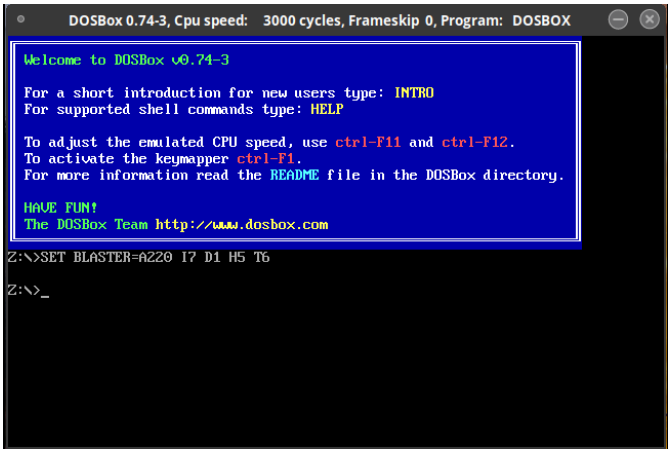
Установить *DOSBox* можно из репозитория РЕД ОС 7.3 командой:

```
dnf install dosbox
```

Запустить программу можно из *«Меню» → «Системные» → «DOSBox»* или из терминала командой:

```
dosbox
```

После запуска программы появится консоль *DOSBox*.



Запуск программ

Рассмотрим несколько вариантов запуска программ в эмуляторе *DOS*. Первый и самый простой способ запуска программы - это ввести в терминале внешней ОС команду **dosbox**, а в качестве атрибута указать *путь к запускаемому файлу*.

Пример:

```
dosbox /home/user/Program/Doom/DOOMS/SETUP.EXE
```



Второй способ - это запустить *DOSBox* и производить все манипуляции с файлами уже через его терминал.

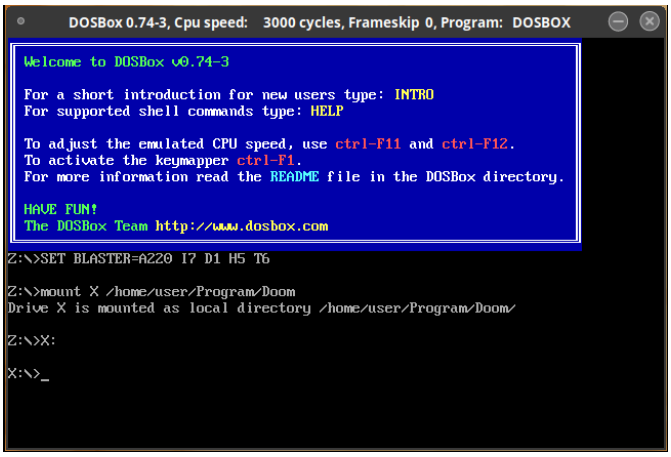
Для начала нам потребуется примонтировать каталог с программой, которую мы хотим запустить.

```
mount X /home/user/Program/Doom

Drive X is mounted as local directory /home/user/Program/Doom/
```

Перейти в смонтированый каталог можно, введя:

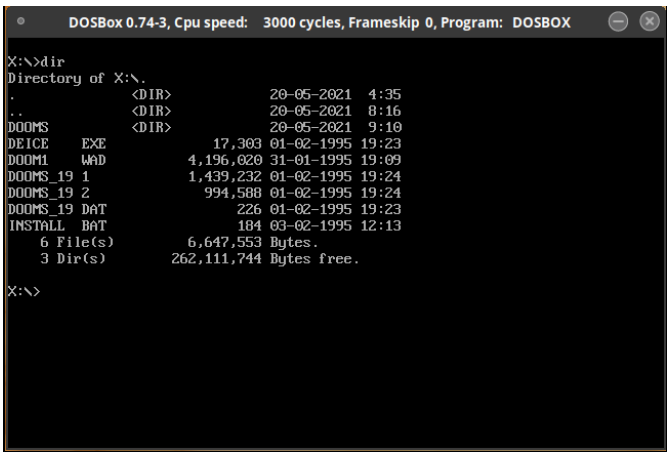
```
X:
```

где «X» - это имя диска, к которому был примонтирован каталог внешней ОС.



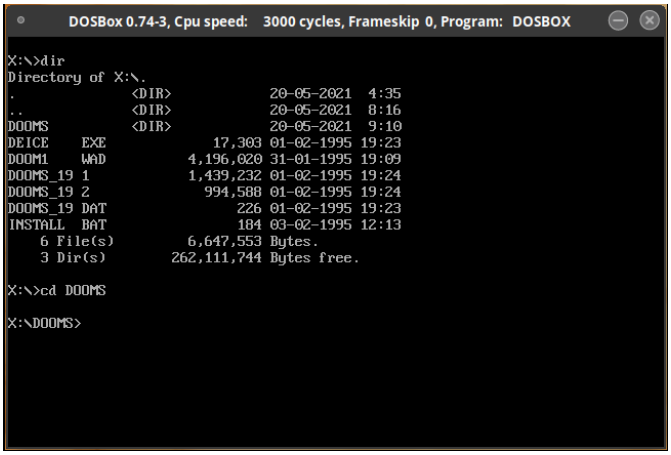
Вывод файлов в каталоге осуществляется командой:

```
dir
```



Перемещение по каталогам осуществляется командой **cd** . Например:

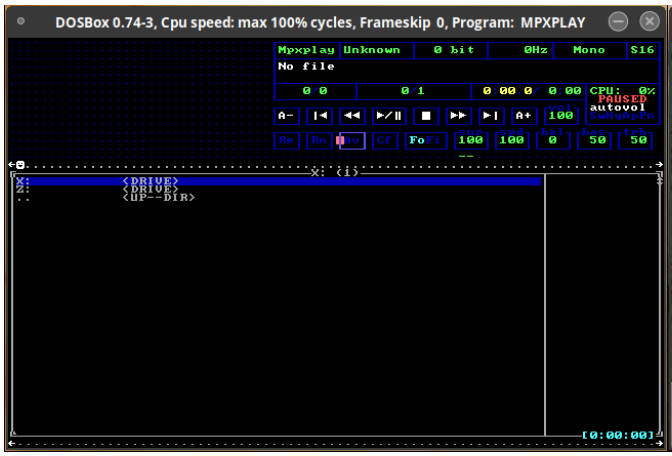
```
cd DOOMS
```



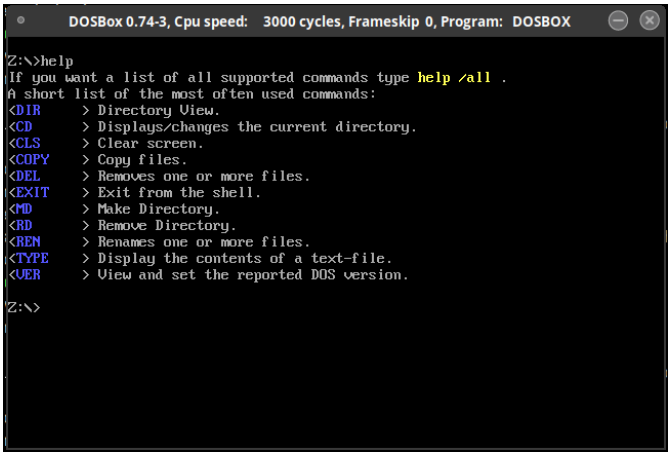
Для запуска программы необходимо ввести её название с расширением. В данном случае команда будет выглядеть следующим образом:

```
SETUP.EXE
```

Примеры запущенных программ



Также в DOSBox можно вывести список всех доступных команд. Для этого необходимо ввести **help**.



Файл конфигурации

Для каждой программы можно создать свой конфигурационный файл с уникальными для нее параметрами эмуляции.

После первого запуска *DOSBox* будет автоматически создан конфигурационный файл по умолчанию - **dosbox.conf**. Файл располагается **~/.dosbox**.

Для редактирования файлов конфигурации можно использовать любой текстовый редактор — **nano**, **pluma** и другие.

Чтобы запустить эмулятор с определенным конфигурационным файлом, нужно выполнить команду:

```
dosbox -conf  /
```

Например:

```
dosbox -conf  /home/user/Program/Doom/Dconf.conf
```

где **Dconf.conf** — имя конфигурационного файла.

Список горячих клавиш

Ниже приведен список основных горячих клавиш эмулятора:

1. «*ALT + ENTER*» - включение/выключение полноэкранного режима;
2. «*ALT + PAUSE*» - приостановка работы эмулятора *DosBox*;
3. «*CTRL + F1*» - запуск редактора горячих клавиш;
4. «*CTRL + F4*» - обновление кеша примонтированых директорий;
5. «*CTRL + ALT + F5*» - запуск и остановка захвата экрана с последующим сохранением в видеофайл;
6. «*CTRL + F5*» - захват и сохранение скриншота;
7. «*CTRL + F6*» - запуск и остановка записи звука в *Wav*-файл;
8. «*CTRL + ALT + F7*» - старт и остановка записи *OPL*-команд;
9. «*CTRL + ALT + F8*» - старт и остановка записи разных *MIDI*-команд;
10. «*CTRL + F7*» - уменьшить количество пропускаемых кадров;
11. «*CTRL + F8*» - увеличить количество пропускаемых кадров;
12. «*CTRL + F9*» - холодное выключение *DOSBox* (**kill**);
13. «*CTRL + F10*» - включение и отключение захвата мышки;
14. «*CTRL + F11*» - замедление эмулятора, уменьшение количества циклов микропроцессора;
15. «*CTRL + F12*» - ускорение эмулятора, увеличение количества циклов микропроцессора;
16. «*ALT + F12*» - отключение лимита скорости.

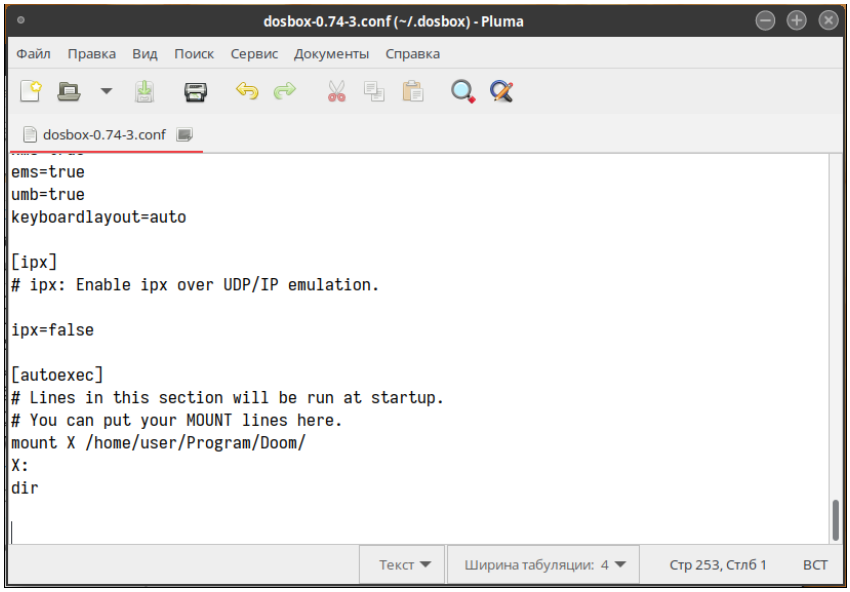
Автозапуск программ

Иногда полезно, чтобы при запуске эмулятора выполнялись определенные команды, например, монтирование каталога или запуск программ. В *DOSBox* это реализовано через файл конфигурации.

Чтобы задать команды для автостарта, в *DOSBox* нужно добавить список этих команд в конфигурационный файл в специальную секцию под названием **[autoexec]**.

Открываем в текстовом редакторе конфигурационный файл и ищем в конце секцию **[autoexec]** - все заданные там команды будут автоматически выполнены по порядку после запуска эмулятора.

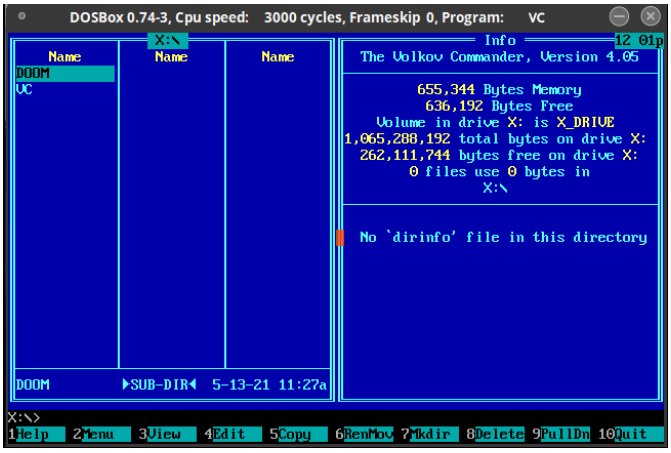
В примере настройка происходит в файле конфигурации **dosbox.conf**, используемом по умолчанию.



Для работы в более привычном формате можно добавить в автозагрузку оболочку типа **Volkov Commander** или **DOS Navigator**.

Распакуем *Volkov Commander* в директорию «*vc*», которая расположена в монтируемом каталоге *X*. Добавляем в конфигурационный файл примера, что приведен выше, строчку: «**x:/vc/vc.com**».

В показанном выше примере при запуске *DOSBox* автоматически примонтируется диск *X* и запустится *Volkov Commander*:



Исправление проблем

Для исправления неверного отображения символов кириллицы в *DOS* служат утилиты - руссификаторы клавиатуры.

В случае использования *DOSBox* достаточно добавить в конфигурационный файл в секцию **[autoexec]** строку:

```
keyb ru 866
```

После перезагрузки эмулятора проблема должна исчезнуть.

Flatpak - изолированная среда для запуска приложений

Добавление репозиториев
Поиск по репозиториям
Установка пакетов
Запуск программ flatpak
Удаление программ
Обновление программ
Поиск и установка программ с помощью Flathub

Flatpak - это утилита для развёртывания, управления пакетами и виртуализации для Linux. Предоставляет специально выделенную, изолированную среду, в которой пользователи могут запускать приложения без влияния на основную систему.

Для работы с утилитой *Flatpak* пакеты могут использовать как **Flathub** (репозиторий разработчика), так и сторонние репозитории. Библиотеки приложений могут находиться в одном пакете вместе с приложением или же в окружениях, общих для нескольких пакетов.

Для установки утилиты *flatpak* необходимо выполнить команду:

```
sudo dnf install flatpak
```

Добавление репозиториев

Для добавления репозитория *flathub* используется команда:

```
flatpak remote-add --user --if-not-exists flathub https://flathub.org/repo/flathub.flatpakrepo
```

Кроме того существует ещё несколько репозиториев, например:

- репозиторий программ *Gnome*:

```
flatpak remote-add --user --if-not-exists gnome-nightly https://nightly.gnome.org/gnome-nightly.flatpakrepo
```

- репозиторий программ *KDE*:

```
flatpak remote-add --user --if-not-exists kdeapps --from https://distribute.kde.org/kdeapps.flatpakrepo
```

Посмотреть все добавленные репозитории можно, выполнив команду:

```
flatpak remotes

 Name      Параметры
flathub    user
```

Поиск по репозиториям

Вы можете посмотреть все пакеты, которые есть в репозитории. Для этого следует выполнить команду **remote-ls** с переданным ей именем репозитория:

```
flatpak remote-ls --user flathub
```

```
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.12
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.13
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.14
QGnomePlatform-decorat… …Decoration.QGnomePlatform-decoration        5.15
Footprints              org.kicad.KiCad.Library.Footprints           stable
Packages3D              org.kicad.KiCad.Library.Packages3D           5.1
Packages3D              org.kicad.KiCad.Library.Packages3D           stable
Symbols                 org.kicad.KiCad.Library.Symbols              stable
Templates               org.kicad.KiCad.Library.Templates            stable
Help                    org.libreoffice.LibreOffice.Help             stable
Codecs                  org.pitivi.Pitivi.Codecs                     stable
bdj                     org.videolan.VLC.Plugin.bdj                  3-19.08
bdj                     org.videolan.VLC.Plugin.bdj                  3-20.08
fdkaac                  org.videolan.VLC.Plugin.fdkaac               3-19.08
fdkaac                  org.videolan.VLC.Plugin.fdkaac               3-20.08
makemkv                 org.videolan.VLC.Plugin.makemkv              3-19.08
makemkv                 org.videolan.VLC.Plugin.makemkv              3-20.08
```

Данная команда выводит полный список пакетов, входящих в репозиторий.

Для того чтобы найти нужный пакет по имени, используйте команду **flatpak search** . Рассмотрим на примере *pidgin*:

```
flatpak search pidgin
```

```
[user@master ~]$ flatpak search pidgin
Имя       Полное описание                          ID Приложения       Версия    Ветка     Удаленные репозитории
Pidgin    Клиент для мгновенного обмена сообщениями  im.pidgin.Pidgin    2.14.13   stable    flathub
```

Для установки программы вам понадобится имя пакета программы из колонки **Application ID** и имя репозитория из колонки **Remotes**.

Установка пакетов

Для установки пакета *flatpak* используйте команду **flatpak install** . Например, установим Pidgin, найденный предыдущей командой:

```
flatpak install flathub im.pidgin.Pidgin
```

```
[user@master ~]$ flatpak install flathub im.pidgin.Pidgin
Поиск похожих запросов...

Разрешения im.pidgin.Pidgin:
    ipc                 network               pulseaudio                  x11
    file access [1]     dbus access [2]       system dbus access [3]

    [1] xdg-download
    [2] org.freedesktop.Notifications
    [3] org.freedesktop.Avahi


        ID                        Ветка     Оп     Удалённый репозиторий   Загрузка
 1. [✓] im.pidgin.Pidgin.Locale   stable    i      flathub                 234,0 kB / 13,6 MB
 2. [/] im.pidgin.Pidgin          stable    i      flathub                   7,5 MB / 8,9 MB

Установка 2/2... ▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕▕ 100%  7,5 MB/s
```

Если вы не хотите добавлять репозиторий в систему, вы можете установить программу по ссылке из сети. Просто скопируйте ссылку на файл **.flatpakref** и передайте её программе:

```
flatpak install --user --from https://dl.flathub.org/repo/appstream/im.pidgin.Pidgin.flatpakref
```

Посмотреть все установленные программы можно выполнив команду:

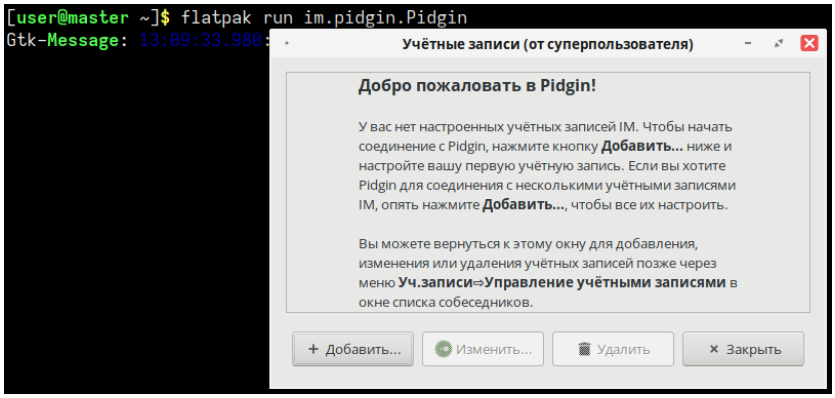
```
flatpak list
```

```
[user@master ~]$ flatpak list
Имя                                ID Приложения                          Версия    Ветка          Тип установки
Pidgin                             im.pidgin.Pidgin                       2.14.13   stable         user
Mesa                               org.freedesktop.Platform.GL.default    24.1.3    23.08          user
Mesa (Extra)                       org.freedesktop.Platform.GL.default    24.1.3    23.08-extra    user
openh264                           org.freedesktop.Platform.openh264      2.4.1     2.4.1          user
GNOME Application Platform version 46  org.gnome.Platform                            46             user
```

Запуск программ flatpak

Программы, установленные с помощью *flatpak*, можно запустить из главного меню. Для запуска с помощью терминала можно использовать команду **flatpak run**:

```
flatpak run im.pidgin.Pidgin
```



Удаление программ

Для удаления программы используйте команду **flatpak uninstall** , например, для Pidgin:

```
flatpak uninstall im.pidgin.Pidgin

   ID                  Ветка    Op
1. im.pidgin.Pidgin          stable   r
2. im.pidgin.Pidgin.Locale   stable   r
```

После удаления пакета можно удалить неиспользуемые компоненты, чтобы освободить место на диске:

```
flatpak uninstall --unused
```

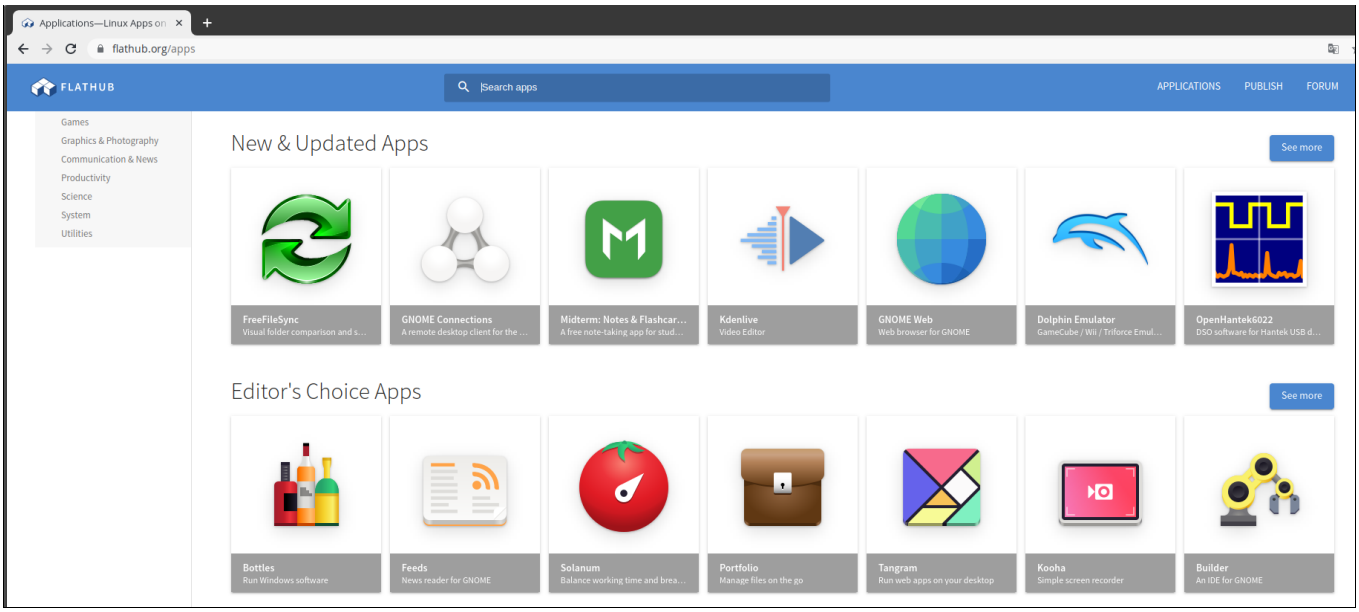
Обновление программ

Как и в любом другом пакетном менеджере, в *flatpak* можно обновлять установленные программы до самой новой версии. Для этого используется команда:

```
flatpak update
```

Поиск и установка программ с помощью Flathub

Несмотря на то, что *Flatpak* децентрализованный, большинство самых популярных пакетов вы можете найти на сайте *FlatHub*. Выберите нужную программу из списка на сайте https://flathub.org/apps:



Откройте её страницу и нажмите кнопку **Install** для установки программы с помощью центра приложений:



Кроме того внизу страницы есть инструкция, как установить программу с помощью терминала:



Для установки скачанного файла выполните команду:

```
flatpak install --user ~/Загрузки/org.freefilesync.FreeFileSync.flatpakref
```

```
org.freefilesync.FreeFileSync permissions:
    ipc       network               pulseaudio            wayland
    x11       file access [1]       dbus access [2]
        ID                                              Ветка            Op            Удалённый репозиторий            Download
 1. [✓] org.freefilesync.FreeFileSync.Locale            stable           i             flathub                            101,3 kB / 6,2 MB
 2. [|] org.gnome.Platform.Locale                       3.38             i             flathub                          < 326,2 MB (partial)
 3. [ ] org.gnome.Platform                              3.38             i             flathub                          < 346,5 MB
 4. [ ] org.freefilesync.FreeFileSync                   stable           i             flathub                           < 31,2 MB

Installing 2/4…
```

Snap - изолированная среда для запуска приложений

Установка
Работа со snap-пакетами. Установка пакетов
Работа со snap-пакетами. Обновление пакетов
Работа со snap-пакетами. Просмотр установленных пакетов
Работа со snap-пакетами. Поиск пакетов
Работа со snap-пакетами. Информация о пакете
Работа со snap-пакетами. Удаление пакетов
Работа со snap-пакетами. Откат обновления
Работа со snap-пакетами. Временно отключить пакет
Работа со snap-пакетами. Запуск snap-пакетов
Snap Store

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** snapd-2.65.1-1

Snap — это пакет, который помимо готовой сборки самого приложения, включает в себя все необходимые зависимости и может работать практически в любом дистрибутиве Linux.

Когда вы устанавливаете в систему приложение из Snap-пакета, установка не влияет на другие пакеты и приложения. То есть такое приложение работает в своей «программной среде», но при этом оно может взаимодействовать с другими программами в системе.

Вы можете подробнее ознакомиться с работой и настройкой изолированной программной среды **Snap**, просмотрев наши обучающие видео:

- на **RuTube** — Snap - изолированная среда для запуска приложений. Snap Store;
- в **Яндекс.Дзен** — Snap - изолированная среда для запуска приложений. Snap Store;
- в **VK Видео** — Snap - изолированная среда для запуска приложений. Snap Store.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для того чтобы установить пакет **snap**, необходимо сперва установить демон управления **snap**-пакетами — **snapd**. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install snapd
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

После установки модуль **systemd**, управляющий основным коммуникационным сокетом **snap**, должен быть включен:

```
systemctl enable --now snapd.socket
```

Чтобы включить поддержку классической привязки, введите следующую команду, чтобы создать символическую ссылку между **/var/lib/snapd/snap** и **/snap**:

```
ln -s /var/lib/snapd/snap /snap
```

После этого перезагрузите систему, чтобы убедиться, что пути **snap** были обновлены правильно.

Работа со snap-пакетами

Установка пакетов

Для установки пакетов используется команда вида **snap install <имя_пакета>**.

Пример установки графического редактора **GIMP** из **snap**-пакета:

```
snap install gimp
```

После установки программа доступна из «**Главного меню**» - «**Графика**» - «**GNU Image Manipulation Program**».

Обновление пакетов

Обновление всех установленных пакетов выполняется командой:

```
snap refresh
```

Обновление какого-либо определенного пакета выполняется командой вида **snap refresh <имя_пакета>**. Например:

```
snap refresh gimp
```

Просмотр установленных пакетов

Для просмотра списка установленных пакетов используется следующая команда:

```
snap list
```

```
Name               Version                    Rev    Tracking       Publisher     Notes
bare               1.0                        5      latest/stable  canonical✓    base
core18             20211215                   2284   latest/stable  canonical✓    base
gimp               2.10.28                    383    latest/stable  snapcrafters  -
gnome-3-28-1804    3.28.0-19-g98f9e67.98f9e67 161    latest/stable  canonical✓    -
gtk-common-themes  0.1-59-g7bca6ae            1519   latest/stable  canonical✓    -
snapd              2.53.4                     14295  latest/stable  canonical✓    snapd
```

Поиск пакетов

Для поиска пакетов используется команда вида **snap find <запрос>**. Например:

```
snap find gimp
```

```
Name                  Version  Publisher        Notes  Summary
gimp                  2.10.28  snapcrafters     -      GNU Image Manipulation Program
gutenprint-printer-app 1.0     openprinting✓    -      Gutenprint Printer Application
photogimp             2.10.20  pedro.ermarinho  -      Patch para o GIMP
djpdf                 0.1.6    unrud            -      Create small, searchable PDFs from scanned documents
lazpaint              7.1.6    chronoscz        -      Image editor with raster and vector layers.
```

Информация о пакете

Для получения информации о каком-либо пакете используется команда вида **snap info <имя_пакета>**. Например:

```
snap info gimp
```

Удаление пакетов

Для удаления пакетов используется команда вида **snap remove <имя_пакета>**. Например:

```
snap remove gimp
```

Откат обновления

Если по каким-то причинам вам необходимо отменить обновления, которые были выполнены над каким-либо snap-пакетом, можно

использовать команду вида snap revert <имя_пакета>, чтобы вернуть пакет к предыдущей версии.

Например:

```
snap revert gimp
```

Временно отключить пакет

Чтобы временно отключить пакет, используется команда вида **snap disable <имя_пакета>**. Например:

```
snap disable gimp
```

Запуск snap-пакетов

Для запуска snap-пакета можно использовать команду вида **snap run <имя_пакета>**. Например:

```
snap run gimp
```

Также приложения, установленные через **snap**, можно запускать через **Главное меню**.

Snap Store

Snap Store — это графическое приложение для обнаружения, установки и управления **snap**.

В **Snap Store** представлены избранные и популярные приложения с полезными описаниями, рейтингами, обзорами и скриншотами.

Приложения можно найти либо через просмотр категорий, либо через поиск.

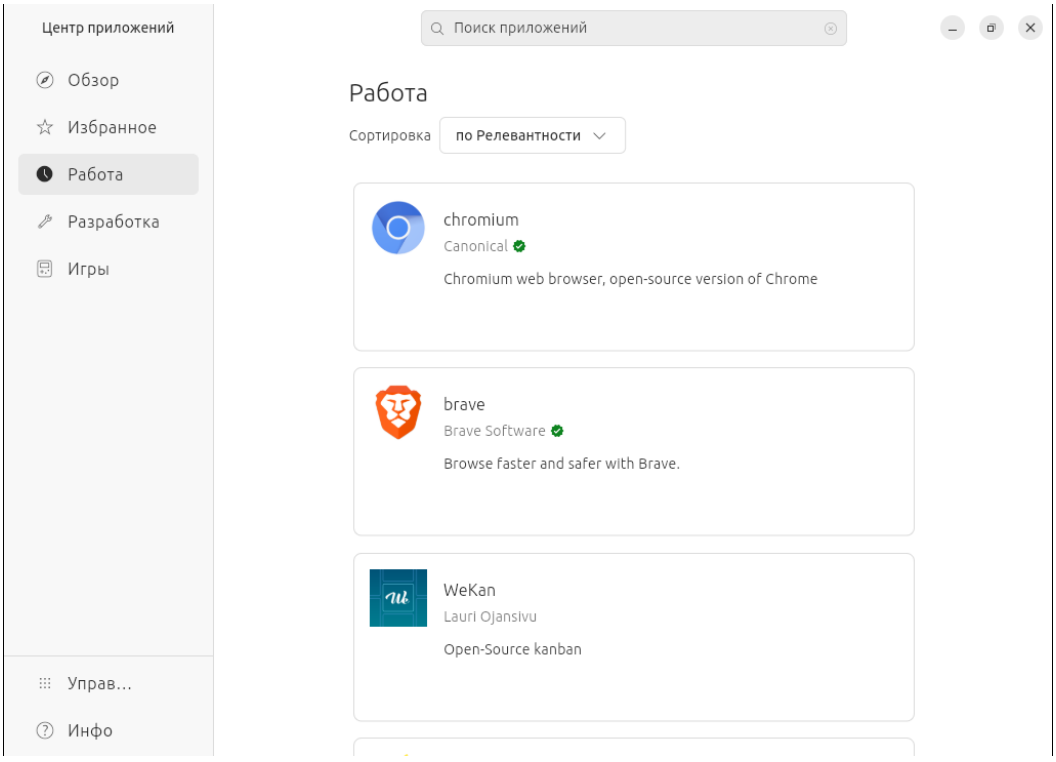
Snap Store также можно использовать для переключения каналов, просмотра и изменения разрешений привязки, а также для просмотра и отправки отзывов и оценок.

Snap Store основан на программном обеспечении **GNOME**, оптимизированном для работы со **snap**.

Для установки **Snap Store** выполните команду:

```
snap install snap-store
```

После установки программа будет доступна в «**Главном меню**» - «**Администрирование**» - «**Центр приложений**».



Firejail - система изолированного запуска приложений

Установка
Работа с утилитой
Дополнительные настройки

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** firejail 0.9.56

Firejail — это простая в использовании система изолированного выполнения графических, консольных и серверных приложений, которая снижает риск нарушений безопасности за счет ограничения рабочей среды потенциально уязвимых программ с использованием пространств имен (**namespaces**), фильтрации системных вызовов (**seccomp-bpf**) и возможностей **AppArmor**.

Вы можете подробнее ознакомиться с настройкой и работой системы **firejail**, просмотрев наши обучающие видео:

- на **RuTube** — firejail - система изолированного запуска приложений;
- в **Яндекс.Дзен** — firejail - система изолированного запуска приложений;
- в **VK Видео** — firejail - система изолированного запуска приложений.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **firejail** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install firejail
```

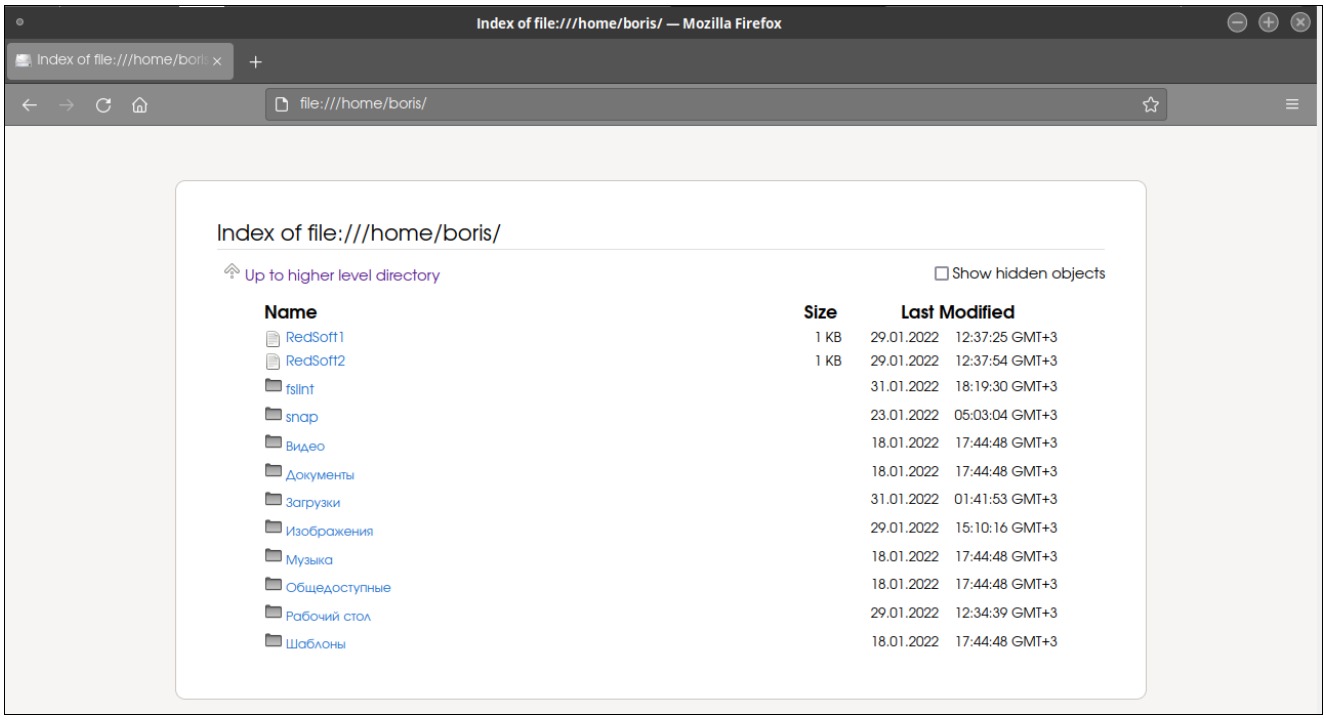
Работа с утилитой

Для того чтобы запустить приложение изолированно, нужно выполнить команду вида **firejail <имя_программы>**:

Например:

```
firejail firefox
```

При запуске браузера обычным способом доступны следующие данные пользователя:



При запуске браузера из контейнера доступ к большинству пользовательских данных ограничен.

Дополнительные настройки

Для просмотра доступных профилей приложений, которые поддерживает **firejail**, выполните:

```
ls /etc/firejail
```

```
[root@localhost firejail]# ls
0ad.profile                         lmms.profile
2048-qt.profile                     lobase.profile
7za.profile                         localc.profile
7z.profile                          lodraw.profile
7zr.profile                         loffice.profile
abrowser.profile                    lofromtemplate.profile
acat.profile                        login.users
adiff.profile                       loimpress.profile
akonadi_control.profile             lollypop.profile
akregator.profile                   lomath.profile
als.profile                         loweb.profile
amarok.profile                      lowriter.profile
amule.profile                       luminance-hdr.profile
android-studio.profile              lximage-qt.profile
anydesk.profile                     lxmusic.profile
aosp.profile                        lynx.profile
apack.profile                       lzcat.profile
apktool.profile                     lzcmp.profile
arch-audit.profile                  lzdiff.profile
archaudit-report.profile            lzegrep.profile
ardour4.profile                     lzfgrep.profile
ardour5.profile                     lzgrep.profile
arduino.profile                     lzip.profile
arepack.profile                     lzless.profile
aria2c.profile                      lzmadec.profile
ark.profile                         lzmainfo.profile
arm.profile                         lzma.profile
artha.profile                       lzmore.profile
```

Далее настройка будет выполняться на примере firefox.

Firejail имеет стандартные настройки по умолчанию. Даже если приложение находится в контейнере, каталог **~/Downloads** и каталоги плагинов в системе доступны. Для того чтобы добавить больше элементов в белый список, перейдите в раздел *whitelist* конфигурационного файла и пропишите свои собственные правила.

Откройте файл:

```
nano /etc/firejail/firefox.profile
```

В нем вы можете настроить доступ к файлам, вносить их в черный и белый списки.

```
# Firejail profile for firefox
 # Description: Safe and easy web browser from Mozilla
 # This file is overwritten after every install/update
 # Persistent local customizations
 include firefox.local
 # Persistent global definitions
 include globals.local

 noblacklist ${HOME}/.cache/mozilla
 noblacklist ${HOME}/.mozilla

 mkdir ${HOME}/.cache/mozilla/firefox
 mkdir ${HOME}/.mozilla
 whitelist ${HOME}/.cache/mozilla/firefox
 whitelist ${HOME}/.mozilla

 # firefox requires a shell to launch on Arch.
 #private-bin firefox,which,sh,dbus-launch,dbus-send,env,bash
 # private-etc must first be enabled in firefox-common.profile
 #private-etc firefox

 # Redirect
 include firefox-common.profile
```

Для того чтобы внести файл в белый список, необходимо прописать:

```
whitelist ~/<расположение_файла>
```

Например:

```
whitelist ~/Pictures
```

Для того чтобы внести файл в черный список, необходимо прописать:

```
blacklist ~/<расположение_файла>
```

Например:

```
blacklist ~/ secret/file/area
```

AppImage - запуск приложений без установки

AppImage — формат для распространения переносимых приложений для большинства систем. Программы в формате **AppImage** состоят всего из одного файла с расширением ***.AppImage**, например, **gimp.AppImage**. Для того чтобы **AppImage**-приложения работали, нужен пакет **fuse** (он уже установлен в систему по умолчанию).

Вы можете подробнее ознакомиться с возможностями **AppImage**, просмотрев наши обучающие видео:

- на **RuTube** — AppImage - запуск приложений без установки;
- в **Яндекс.Дзен** — AppImage - запуск приложений без установки;
- в **VK Видео** — AppImage - запуск приложений без установки.

На наших каналах вы также сможете найти много другой полезной информации.

Рассмотрим работу с **AppImage** на примере **kdenlive**.

Сначала необходимо скачать **kdenlive** с расширением ***.AppImage** с официального сайта.

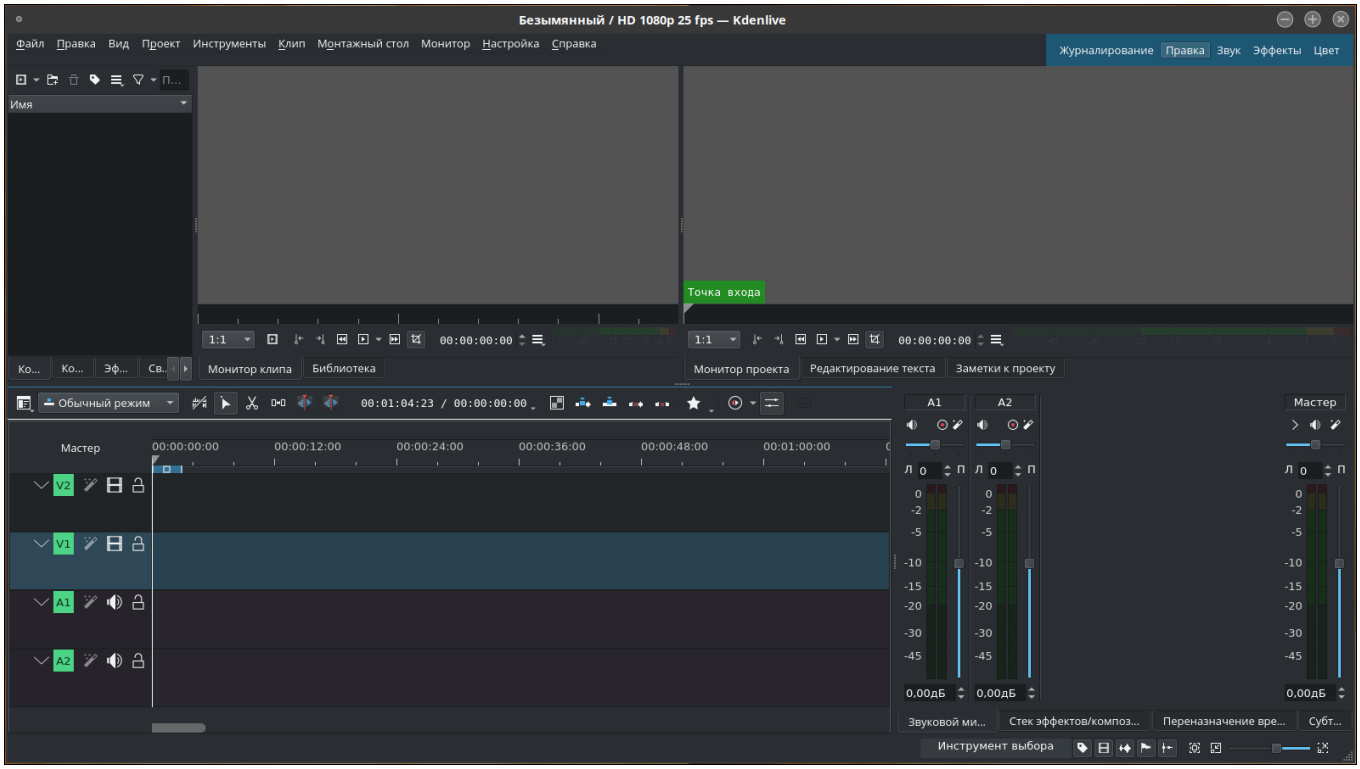
Затем нужно предоставить скачанному файлу права на исполнение. Для этого выполните следующие команды:

```
cd Загрузки
chmod +x kdenlive-21.12.3-x86_64.AppImage
```

После этого запустите программу либо двойным щелчком по файлу, либо прописав имя файла в консоли:

```
./kdenlive-21.12.3-x86_64.AppImage
```

Если всё было сделано правильно, программа успешно запустится.



Удаление пакетов .appimage

Для удаления программы **AppImage** достаточно удалить соответствующий файл с расширением ***.AppImage**.

PlayOnLinux - программа запуска приложений Windows

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: PlayOnLinux-4.4-8

PlayOnLinux — программа, позволяющая запускать *Windows*-приложения без эмуляции с помощью прослойки совместимости **Wine**.

PlayOnLinux — это графическая оболочка над **Wine**, которая очень облегчает использование программы. Она содержит готовые скрипты установки, разработанные пользователями. Эти скрипты содержат все необходимое для установки программы.

Вы можете подробнее ознакомиться с установкой и работой утилиты **PlayOnLinux**, просмотрев наши обучающие видео:

- на **RuTube** — PlayOnLinux - программа запуска приложений Windows;
- в **Яндекс.Дзен** — PlayOnLinux - программа запуска приложений Windows;
- в **VK Видео** — PlayOnLinux - программа запуска приложений Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**playonlinux**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.

Для установки **PlayOnLinux** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install playonlinux
```

Для запуска программы через терминал введите команду:

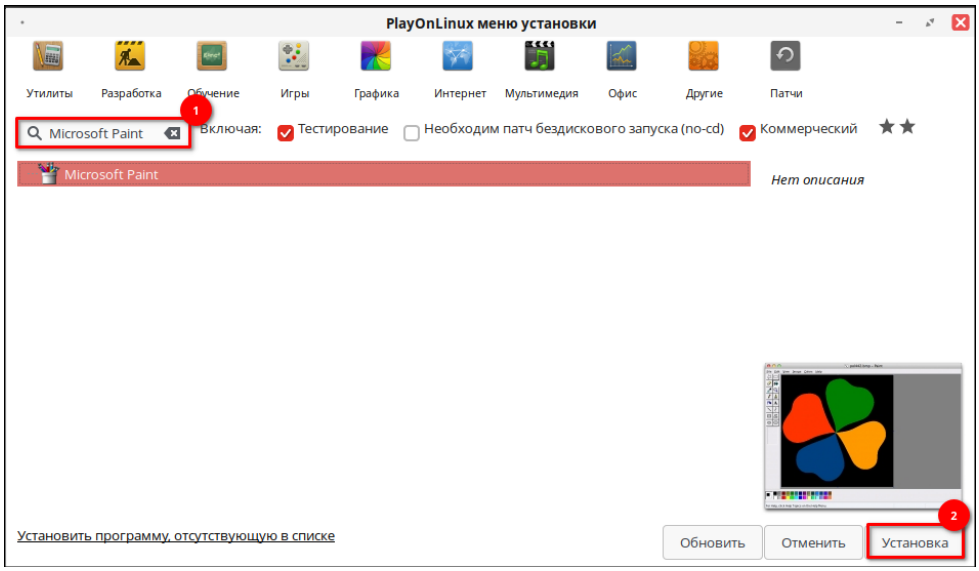
```
playonlinux
```

Для запуска в графическом режиме откройте **«Главное меню**» — «**Стандартные**» — «**PlayOnLinux**».

Интерфейс программы достаточно прост:

- Вверху окна находится **основное меню**, с помощью которого можно получить доступ к большинству функций программы;
- Чуть ниже находится **панель инструментов**, которые позволяют делать основные действия;
- Дальше окно разделено на две панели. На **левой** находятся ярлыки основных действий, например, для установки программ;
- На **правой панели** будет размещен список программ, которые были установлены;
- В нижней части окна находится **статус бар**, где отображается статус обновления или другие данные.

Для установки нужной программы необходимо выбрать в меню пункт «**Установить программу**». Для примера можно установить «**Microsoft Paint**».

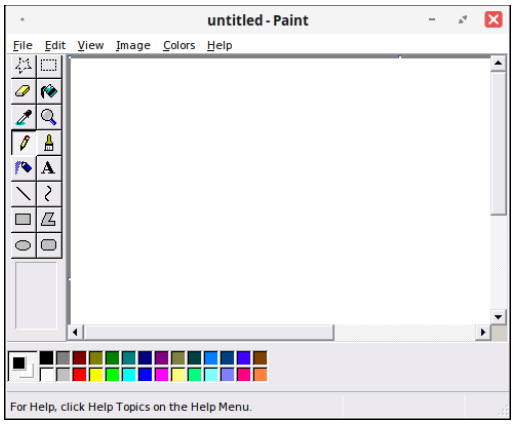


После нажатия на кнопку «**Установка**» откроется мастер установки. Нажмите «**Далее**».

Для загрузки необходимых компонентов и их распаковки нажмите кнопку «**Установить**».

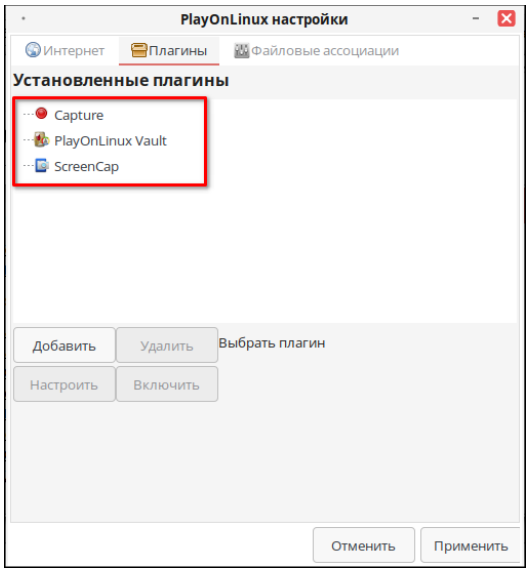
Затем программа предложит установить дополнительные компоненты, загрузить установщик программы **Microsoft Paint** и установить его в стандартном режиме *Windows*.

После всех выполненных действий программа будет готова к работе.



Также **PlayOnLinux** позволяет использовать различные плагины, например;

- **Capture** - позволяет записывать аудио *ALSA* и видео данные *OpenGL* от программы *Wine*, очень полезно для захвата видео;
- **PlayOnLinux Vault** - резервное копирование папок с программами и системными файлами *Wine* и их восстановление;
- **ScreenCap** - создание снимков экрана.



Объединённая служба каталога (LDAP)

Основные термины
Объекты и атрибуты
Установка и настройка
Настройка сервера
База данных ldbm
Настройка репликации
Настройка клиента
Использование LDAP

Служба каталога (Directory Service) — это программный комплекс для хранения и каталогизации информации. По своей сути это очень похоже на обычную базу данных, но с «уклоном» скорее на чтение данных, нежели на их добавление или изменение. Обычно служба каталога базируется на клиент-серверной архитектуре. Одна из наиболее известных таких систем — DNS (Domain Name Service): DNS-сервер производит взаимную «трансляцию» имён машин и их IP-адресов. Другие машины в сети могут обращаться к такому серверу за информацией о соответствии имени и адреса. Однако это очень простой пример каталогизации информации. Объекты в такой базе имеют ограниченное количество атрибутов — таких как имя, адрес и ещё несколько дополнительных параметров.

Протокол **LDAP** (Lightweight Directory Access Protocol) позволяет реализовать доступ по TCP/IP к службе каталогов и может легко расширяться.

Существует несколько реализаций данного протокола от различных фирм. Наиболее известные из них — Netscape Directory Service™, Novell Directory Service™ и Microsoft Active Directory™. Из некоммерческих реализаций LDAP наибольшее распространение получил проект **OpenLDAP**. Именно его мы и будем рассматривать в дальнейшем, хотя большинство понятий и определений применимо и к другим реализациям сервера LDAP.

Основные термины

Данные каталога хранятся в виде объектов или сущностей (от англ. entry), состоящих из специальных полей, называемых атрибутами (attributes). Набор атрибутов, их синтаксис и правила поиска определяются схемой каталога (scheme). Все объекты каталога идентифицируются специальным атрибутом — DN (Distinguished Name).

Данные в каталоге можно представить в виде древовидной структуры — *DIT* (Directory Information Tree). Это очень похоже на структуру, используемую многими файловыми системами. Вершиной такого дерева является корневой объект (*Root Entry*). DN корневого объекта одновременно является суффиксом каталога.

Каждый последующий объект в структуре каталога идентифицируется уникальным значением DN, который описывает путь к объекту в каталоге. Если продолжить аналогию с файловой системой, то DN любого объекта так же включает DN всех объектов, стоящих выше по иерархии. Отличие в данном случае только в том, что DN формируется не слева направо, как путь к файлу, а наоборот — справа налево.

DN администратора каталога (Root Distinguished Name) — это специальный объект, описывающий администратора каталога. Этот объект указывается в конфигурации сервера, но может отсутствовать в самом каталоге. К такому объекту не применяются списки доступа (ACL). В некоторых реализациях LDAP такой объект может не иметь суффикса.

База поиска (Base Distinguished Name) — объект каталога, начиная с которого производится поиск. Дело в том, что не всегда есть необходимость производить поиск по всему дереву каталога; ограничить область поиска можно указанием в запросе базы поиска. По умолчанию этот параметр соответствует суффиксу.

Объекты и атрибуты

Серверы LDAP могут поставляться с несколькими вариантами бэкенда (backend). Например, OpenLDAP имеет такие варианты, как **LDBM** — собственный формат хранения данных в текстовых файлах; **SHELL** — интерфейс к базе данных, использующий команды UNIX; **PASSWD** — простейшая база, использующая стандартные файлы **/etc/passwd** и **/etc/group**; **SQL** — интерфейс к любой базе данных, использующей SQL.
Для процедур импорта и экспорта данных всеми серверами LDAP поддерживается единый формат обмена данными — **LDIF**. Вот пример такого файла с описанием двух объектов:

```
dn: dc=example,dc=com
objectClass: top
objectClass: organization
o: example.com
o: Example Inc.

dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People
description: Example Inc. workers
description: Stuff area
```

Описание каждого объекта в таком файле начинается с атрибута DN. Специальный атрибут **objectClass** указывает, к каким классам относится данный объект и, следовательно, какие атрибуты он может иметь. В нашем случае принадлежность к классу **top** означает,

что объект обязательно должен иметь атрибут **objectClass**, а принадлежность к классу **organization** предполагает наличие нескольких атрибутов, из которых атрибут **o** является обязательным.

Второй объект находится на одну ступеньку ниже по иерархии и поэтому в его DN включён DN объекта верхнего уровня. Этот объект относится к классу **organizationalUnit** и поэтому имеет обязательный атрибут **ou**.

Можно заметить, что некоторые атрибуты (для которых это применимо) могут иметь несколько значений. В данном примере атрибут **description** имеет два значения. А вот для атрибута **dn** допустимо только одно значение.

Классы, характеризующие объекты, и атрибуты, составляющие классы, описываются схемой базы. Её пример приведён ниже.

```
attributetype ( 2.5.4.10 NAME ( 'o' 'organizationName' )
  SUP name
)
attributetype ( 2.5.4.13 NAME 'description'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024}
)
objectclass ( 2.5.6.4 NAME 'organization' SUP top STRUCTURAL
  MUST o
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
    x121Address $ registeredAddress $ destinationIndicator $
    preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
    telephoneNumber $ internationaliSDNNumber $
    facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
    postalAddress $ physicalDeliveryOfficeName $ st $ l $ description
  )
)
```

В данном фрагменте приводятся описания двух атрибутов и одного класса. Вот что означают эти записи:
Атрибут **o** (его можно также называть *organizationName*) является расширением атрибута **name**.
Атрибут **description** — это строка длиной до 1024 байт; при поиске в ней регистр символов не учитывается.
Класс **organization** является расширением класса **top** и, следовательно, он включает в себя все атрибуты, составляющие этот класс плюс дополнительные атрибуты, такие как **userPassword, businessAddress, street, postOfficeBox** и т.д. Кроме того, атрибут **o** является обязательным.

Установка и настройка

Процесс сборки и установки сервера OpenLDAP не отличается от установки другого программного обеспечения, поставляемого в виде готового пакета.

Настройка сервера

Сервер LDAP состоит из двух серверных процессов: **slapd** и **slurpd**. Процесс *slapd* занимается приёмом и обработкой запросов от клиентов; это основной процесс, который непосредственно работает с базой данных. Сервис *slurpd* используется в тех случаях, когда данные нужно реплицировать на другие сервера — он контролирует изменения в базе и, при необходимости, пересылает их на подчинённые сервера.

Приведём пример конфигурационного файла:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/nis.schema
```

В первых строках мы подключаем необходимые схемы; в поставке *OpenLDAP* их около полутора десятков. Подключите только те, которые будете использовать. В принципе, схемы являются частью конфигурационного файла, но для наглядности они вынесены в отдельные фрагменты.

```
LSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCertificateFile /etc/openldap/ssl/slapd.pem
TLSCertificateKeyFile /etc/openldap/ssl/slapd.pem
```

LDAP можно использовать для централизованной авторизации пользователей сети вместо **NIS+**. В таких случаях из каталога может запрашиваться конфиденциальная информация — например, пароль. Для предотвращения перехвата этих данных желательно использовать протокол LDAPS (LDAP via SSL/TLS).

База данных ldbm

В качестве способа хранения используется собственный формат LDBM. Если предполагается обычная конфигурация сервера, то данный формат предпочтителен.

```
suffix "dc=example,dc=com"
```

Корнем информационной структуры будет являться объект **dc=example, dc=com**. В принципе, суффикс для каталога можно взять любой, например, *o=Example Inc., c=RU* — это не накладывает абсолютно никаких ограничений на функциональность. Однако последнее время всё чаще используется именно первый вид суффикса, который подчёркивает, что информационная структура данного предприятия тесно связана со структурой его домена.

```
rootdn "cn=admin,dc=server,dc=com"
rootpw secret
```

DN, описывающий администратора и его пароль. В данном случае пароль записан в открытом виде, поэтому файл конфигурации сервера должен иметь соответствующие права доступа, ограничивающие его чтение обычными пользователями. Пароль можно записать и в виде хеша DES или MD5 — тогда строка будет иметь следующий вид:

```
rootpw {MD5}IFJFxyGN3Hap7xsJFBmeTA==
```

Эти опции нужны только на время первичной настройки базы. После того как структура создана и можно регулировать права доступа с помощью ACL, эти опции рекомендуется отключить.

```
index objectClass eq
```

Формат *ldbm* поддерживает простейшие индексы с целью ускорения операций поиска. Такие индексы желательно создавать по атрибутам, предполагающим наибольшее количество запросов. Последний параметр данной опции указывает по какому критерию создаётся индекс. Это могут быть **pres, eq, approx, sub, none** (present, equality, approximate, substring, no index).

```
access to attr=userPassword
  by dn=".*,ou=Admins,dc=example,dc=com" write
  by self write
  by anonymous auth
  by * none

access to * by * read
```

Данные каталога не всегда находятся в публичном доступе. Для управления доступом могут использоваться списки доступа (*access lists*). В данном примере приводятся два списка — в первом из них ограничивается доступ к атрибуту **userPassword** (полный доступ к нему могут иметь только сам объект либо администраторы базы; для всех остальных доступ запрещён). Второе правило гласит, что всем даётся доступ на чтение любых данных (кроме ограниченного предыдущим правилом).

После настройки можно сразу запустить процесс **slapd** — например, такой командой:

```
# service slapd start
```

Первый объект, который нужно создать в базе — корневой элемент (*root entry*), который указан в конфигурационном файле как **suffix**.

Настройка репликации

Одной из важных особенностей LDAP являются встроенные средства репликации данных. Этот механизм реализован в виде отдельного серверного процесса, контролирующего изменения в базе данных и пересылающего эти изменения на другие серверы. Прежде чем включить такую репликацию, необходимо убедиться в том, что соответствующие данные на обоих серверах идентичны. Это связано с тем, что *slurpd* пересылает именно изменения на текущем сервере — он не проверяет и не анализирует состояние данных на удалённом сервере. Настройки *slurpd* находятся в том же файле, что и настройки *slapd*, поэтому перечислим, что нужно добавить к перечисленным выше параметрам:

```
replica /var/log/slapd.replog
```

Прежде всего, укажем файл, в который *slapd* будет записывать все свои действия и из которого *slurpd* будет их читать.

```
replica uri=ldap://ldap2.example.com
  bindmethod=simple
  binddn="cn=slurpd,ou=Apps,dc=example,dc=com"
  credentials=secret
```

Реплика такого вида описывается для каждого подчинённого сервера. На подчинённом сервере нужно создать соответствующий объект и указать, что он имеет права на изменение информации. Это делается с помощью соответствующего списка доступа и параметров **updatedn** и **updateref**.

Настройка клиента

Существует огромное количество клиентов, работающих с LDAP. Это могут быть почтовые программы, которые обращаются к каталогу в поисках адреса электронной почты сотрудника или за информацией о маршрутизации почты, FTP-сервер, который берет информацию для авторизации своего клиента и многие другие программы — однако все они имеют схожие настройки. Прежде всего это адрес сервера и порт, на котором работает LDAP (обычно это 389 или, если сервер поддерживает протокол LDAPS, 636). Вторым важным параметром является база поиска (*Base DN*) — в большинстве случаев этот параметр соответствует суффиксу сервера, однако иногда имеет смысл сузить область поиска. Например, если мы ищем пользователя, чтобы авторизовать его на почтовом сервере, то вряд ли его нужно искать среди групп пользователей или списка компьютеров локальной сети. Третий важный параметр — фильтр поиска, т.е. критерий, по которому мы выбираем объект из базы. Кроме того, существуют параметры, позволяющие ограничить поиск снизу — например, только самой базой или базой и её подобъектами первого уровня, параметры, управляющие поиском в алиасах (*alias*), и т.п.

Трёх этих параметров (сервер, база поиска и фильтр) в большинстве случаев достаточно, чтобы выполнить запрос к любому серверу LDAP. Однако, если на сервере существуют ограничения на доступ к данным, может потребоваться авторизация. Авторизоваться в LDAP можно, указав DN одного из объектов базы данных LDAP; пароль для такого объекта будет искаться в его атрибуте **userPassword**.

Ниже приводится фрагмент настройки почтового сервера Postfix:

```
virtual_maps = ldap:virtual, hash:/etc/postfix/virtual
virtual_server_host = localhost
virtual_search_base = ou=People,dc=example,dc=ru
virtual_query_filter = (&(objectclass=inetLocalMailRecipient)(cn=%s))
virtual_result_attribute = mailLocalAddress,mailRoutingAddress
```

В данном фрагменте описывается, что при определении адреса получателя делается запрос в LDAP с целью найти объект, которому это письмо адресовано. Поиск делается по атрибуту **cn**. Результат берётся из атрибутов **mailLocalAddress** и **mailRoutingAddress**. Эти классы и атрибуты описаны схемой **misc**.

Использование LDAP

LDAP может использоваться в самых различных ситуациях. Здесь мы рассмотрим несколько наиболее распространённых его применений. Поскольку в LDAP хранится полная информация о сотрудниках предприятия, мы можем брать справочную информацию для почтовых программ прямо оттуда. Для начала настроим сервер:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/misc.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/openldap.schema

pidfile        /var/run/slapd.pid
argsfile       /var/run/slapd.args

loglevel 512

database       ldbm
directory      /var/lib/ldap/base/example.com
password-hash  {MD5}

suffix         "dc=example,dc=com"
#rootdn         "cn=admin,dc=example,dc=com"
#rootpw         secret

access to attr=userPassword
  by dn=".*,ou=Admins,dc=example,dc=com"
  by anonymous auth
  by self write
  by * none
access to * by * read

index objectClass,uid,uidNumber,gidNumber     eq
index cn,mail,surname,givenname               eq,sub
```

После этого создадим пользователя **ldap**, от имени которого будет работать наш сервер и запустим процесс **slapd** следующей командой:

```
# slapd -u ldap -h 'ldap://127.0.0.1/ ldap//ldap.example.com/ ldaps://ldap.example.com'
```

Теперь можно создать базу данных — например, с помощью утилиты ldapadd или slapadd:

```
# ldapadd -xWD cn=admin,ou=Admins,dc=example,dc=com -H ldaps://ldap.server.com -f initial.ldif
```

Или, если сервер не запущен:

```
# slapadd -b dc=example,dc=com -l initial.ldif # chown ldap:ldap /var/lib/ldap/bases/example.com/*
```

Содержимое файла **initial.ldif** будет такое:

```
dn: dc=example,dc=com
objectClass: top
objectClass: organization
o: Exapmle Inc.
o: exapmle.com

dn: ou=Admins,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Admins
description: Administrators

dn: cn=admin,ou=Admins,dc=example,dc=com
objectClass: top
objectClass: person
cn: admin
sn: Bender
givenName: Ostap
userPassword: secret
description: Our smart admin

dn: ou=People,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People
description: Stuff area

dn: uid=obender,ou=People,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
cn: Ostap Bender
sn: Bender
givenName: Ostap
uid: obender
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/obender
loginShell: /bin/bash
userPassword: {md5}$1$ION4SIII$EYyGEeYt4g2hEe9tjICac.
mail: obender@example.com
mail: obender@attiresandtoes.com

....

dn: ou=Groups,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Groups
description: Groups of users

dn: cn=obender,ou=Groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
cn: luser
gidNumber: 1000
description: Default group for users presented by LDAP
```

Проверим, что сервер работает, сделав к нему анонимный запрос:

```
$ ldapsearch -xLLL "(uid=obender)"
```

```
dn: uid=obender,ou=People,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
cn: Ostap Bender
sn: Bender
givenName: Ostap
uid: migor
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/obender
loginShell: /bin/bash
mail: obender@example.com
mail: obender@attiresandtoes.com
```

Поскольку, согласно нашим настройкам, доступ к атрибуту **userPassword** имеют только сам пользователь и администратор, то этот атрибут мы не получили.

Предварительная подготовка компьютера к вводу в домен

Описывается ввод в домены, организованные на версиях Windows Server 2008r2 и выше. Для ввода в домен на Windows server 2003 смотрите дополнительные примечания в тексте.

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.
Порты брандмауэра, необходимые для присоединения к домену AD
TCP 464 (Kerberos Password V5 – Used when user change their password from desktop)
TCP 636 (LDAP SSL)
TCP 53 (DNS)
TCP 88 (Kerberos Key Distribution Center)
TCP 135 (Remote Procedure Call)
TCP 139 (NetBIOS Session Service)
TCP 389 (LDAP)
TCP 445 (SMB,Net Logon)
UDP 389 (LDAP, DC Locator, Net Logon)
TCP 49152-65535 (Randomly allocated high TCP ports)

+ DNS-имена могут содержать только буквы (a–z), цифры (0–9), знак ''минус'' (-) и точку (.). Точки разрешено использовать только для разделения компонентов имен, заданных в формате доменных.

Имена узлов DNS не могут содержать следующие символы:

- Запятая (,)
- Тильда (~)
- Двоеточие (:)
- Восклицательный знак (!)
- Знак "@"
- Символ решетки (#)
- Знак доллара ($)
- Знак процента (%)
- Крышка (^)
- Амперсанд (&)
- Апостроф (')
- Точка (.)
- Круглые скобки (())
- Фигурные скобки ({})
- Символ подчеркивания (_)
- Пробел ( )

1. Измените имя компьютеру, **имя должно содержать домен**, то есть должно быть, например *client1.win.redos*

```
hostnamectl set-hostname <Имя компьютера>.<домен>
```

Например:

```
hostnamectl set-hostname client1.win.redos
```

2. Проверьте имя ПК

```
hostname
```

3. Для регистрации рабочей станции с РЕД ОС в домене **Active Directory** с автоматическим обновлением **DNS-записей** добавьте в файл **/etc/hosts** строку вида:

```
127.0.0.1 <Имя компьютера>.<домен> <Имя компьютера>
```

С помощью команды:

```
sudo sh -c "echo '127.0.0.1  `hostname -f` `hostname -s`' >> /etc/hosts"
```

Пример файла **/etc/hosts** (добавленная строка выделена жирным шрифтом):

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1  client1.win.redos client1
```

При выводе из домена эту строку нужно удалить

4. Проверьте настройку сети

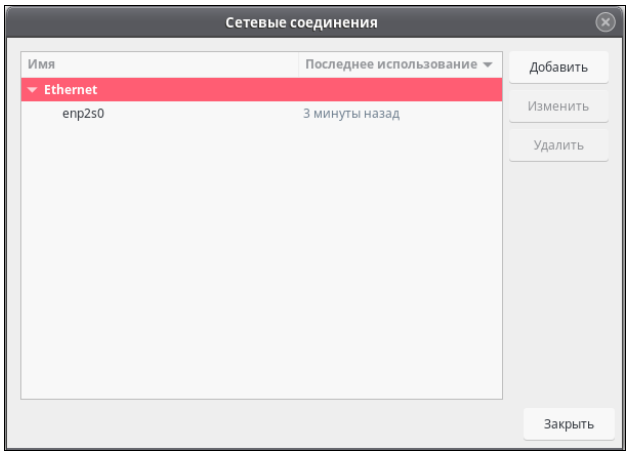
```
ifconfig
```

5. Проверьте работу сети

```
ping ya.ru -c 4
```

6. Настройте сетевой адаптер и проверьте, что первый DNS - это DNS контроллера домена, и укажите в качестве поискового домена домен MS AD.

Для настройки сетевого адаптера откройте утилиту **"Сетевые соединения"**, выберите доступное соединение и нажмите **"Изменить"**. Утилита находится по адресу:
"Меню" → "Параметры" → "Сетевые соединения"



Перейдите на вкладку **"Параметры IPv4"**. В поле **"Метод"** выберите **"Автоматический (DHCP, только адрес)"**, укажите нужные значения в полях **"Дополнительные серверы DNS"** и **"Дополнительные поисковые домены"**.

Нажмите кнопку "Сохранить" и перезапустите сервис **Network Manager**.

```
sudo systemctl restart NetworkManager
```

Проверьте, что введенные настройки сохранились.

```
resolvectl
```

В выводе команды должна быть запись вида:

```
# Generated by NetworkManager
search <название домена>
nameserver <IP контроллера домена>
```

ВАЖНО

В работе используются только 3 первые DNS-сервера.

7. Проверьте разрешение имен

```
nslookup <IP контроллера домена>
nslookup <FQDN имя контроллера домена>
```

Ввод РЕД ОС в домен MSAD с помощью утилиты join-to-domain

Графический режим работы программы ввода/вывода РЕД ОС из домена
Консольный режим работы программы ввода РЕД ОС в домен
Консольный режим работы join-to-domain с входными параметрами

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: join-to-domain-0.6.5

Перед вводом РЕД ОС в домен проверьте настройки сети. Контроллер домена должен быть доступен по имени, например, это можно проверить запустив команду **ping**:

```
ping -c 3 dc.win.redosPING dc.win.redos (10.81.1.196) 56(84) bytes of data.
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=1 ttl=128 time=0.320 ms
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=2 ttl=128 time=0.601 ms
64 bytes from dc.win.redos (10.81.1.196): icmp_seq=3 ttl=128 time=0.701 ms
```

Если ваш DHCP-сервер не раздает клиентам доменный суффикс, то укажите его в сетевых настройках, в поле «**Поисковый домен**».

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

В РЕД ОС имеется утилита **join-to-domain**, которая предназначена для ввода компьютера в домен *Windows* или домен на базе *SAMBA*. В РЕД ОС 7.3 программа **join-to-domain** предустановлена в системе по умолчанию, но перед использованием необходимо обновить утилиту до последней версии:

```
dnf update join-to-domain
```

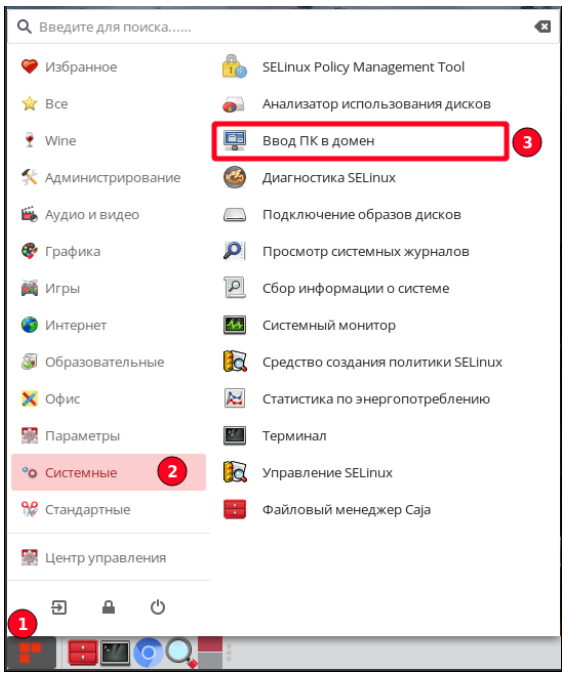
join-to-domain может выполняться в трех режимах:

- с графическим интерфейсом;
- в консоли (интерактивный режим);
- в консоли с входными параметрами.

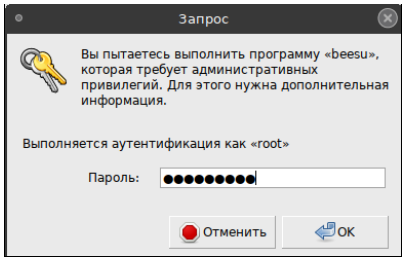
Графический режим работы программы ввода/вывода РЕД ОС из домена

В РЕД ОС для быстрого ввода компьютера в домен *Windows/SAMBA* используется утилита **join-to-domain**. Утилита может быть запущена в консольном (текстовом) и в графическом режиме. Описание работы **join-to-domain** в консоли будет рассмотрено ниже.

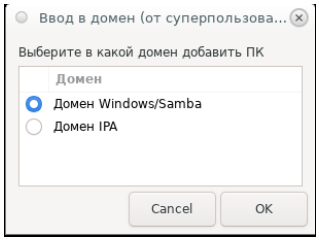
Для запуска **join-to-domain** в графическом режиме откройте «**Главное меню**» - «**Системные**» - «**Ввод ПК в домен**».



Запуск программы требует ввода пароля от пользователя **root**.



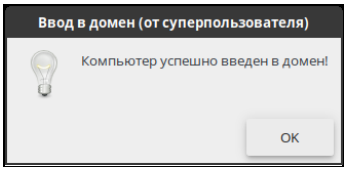
После успешной аутентификации откроется окно выбора типа домена на базе **SAMBA** или **FreeIPA**. Для ввода в домен **SAMBA** выберите пункт «**Домен Windows/SAMBA**».



После успешной аутентификации откроется основное окно, в котором необходимо заполнить все поля:

После нажатия на кнопку «**Да**» начнется процесс присоединения ПК к домену.

В случае успешного ввода в домен появится уведомление:

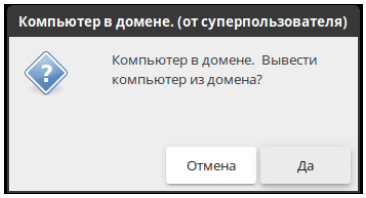


Перезагрузите компьютер и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

Процесс ввода в домен, а также возможные ошибки при работе протоколируются в файл **/var/log/join-to-domain.log**.

Для вывода ПК из домена *Windows*, следует снова запустить **join-to-domain** «**Главное меню**» - «**Системные**» - «**Ввод ПК в домен**».

В этот раз программа определит, что РЕД ОС введен в домен и предложит выйти из него.



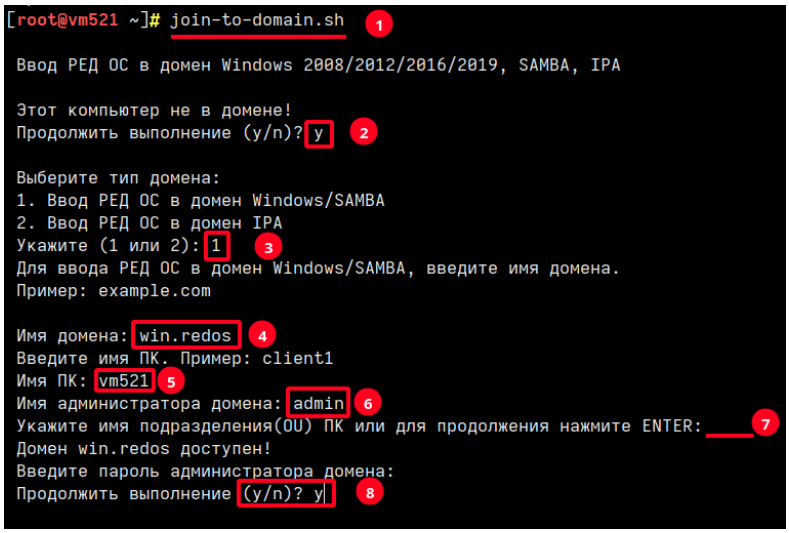
Консольный режим работы программы ввода РЕД ОС в домен

Откройте консоль и выполните запуск **join-to-domain.sh** с привилегиями суперпользователя **root**.

```
join-to-domain.sh
```

Программа запросит пользователя выбрать тип домена, к которому необходимо присоединить РЕД ОС, в данном случае необходимо выбрать первый пункт «**Ввод РЕД ОС в домен Windows/Samba**».

Введите имя домена, имя компьютера, имя администратора домена и подтвердите ваши действия для начала процесса ввода ПК в домен.

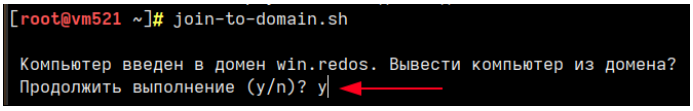


Протокол ввода в домен записывается в файл **/var/log/join-to-domain.log**.

Перезагрузите компьютер и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

Для вывода РЕД ОС из домена выполните в консоли команду с привилегиями суперпользователя **root**:

```
join-to-domain.sh
```



Подтвердите действие, после чего начнется процесс вывода из домена, по окончании всех действий перезагрузите ПК.

Консольный режим работы join-to-domain с входными параметрами

Пример №1 - ввод в домен Windows или SAMBA:

```
join-to-domain.sh -d win.redos -n client07 -u admin -p password
```

Пример №2 - ввод в домен с добавлением ПК в OU:

```
join-to-domain.sh -d example.com -n client1 -u admin -p password --ou "OU=МоиПК,OU=ОтделIT" -y
```

Пример №3 - удаление учетной записи ПК с подключением к определенному DC:

```
join-to-domain.sh --delete-computer -u <admin_login> -d <domain_name> --dc <domain_controller> -n <pc_name>
```

Пример №4 - вывод из домена. Выполните команду join-to-domain.sh, в результате программа определит, что данный ПК в домене и предложит выйти из него.

```
join-to-domain.sh

Компьютер введен в домен win.redos. Вывести компьютер из домена?
Продолжить выполнение (y/n)? y
Удаление учетной записи ПК из домена.
Введите имя контроллера домена или для продолжения нажмите ENTER:
Введите имя администратора домена: admin
Password for admin@WIN.REDOS:
```

Пример №5 - ввод в домен с поддержкой kerberos-аутентификации на SSH-сервере и предоставление прав доменной группе пользователей на использование sudo:

```
join-to-domain.sh -d <domain_name> -n <pc_name> -u <admin_login> -p <password> --sg "Администраторы домена" --sk -y
```

Описание параметров запуска:

Параметр	Описание параметра
-d	Имя домена
-n	Имя компьютера
-u	Имя администратора домена
-p	Пароль администратора домена
--ou	Имя подразделения компьютера (OU), формат ввода "**OU=МоиПК,OU=ОтделIT**". Порядок указания OU снизу вверх
--dc	Имя контроллера домена
-w	Позволяет ввести в домен, используя **Winbind** (по умолчанию применяется SSSD)
--sk	Включение поддержки kerberos-аутентификации на SSH-сервере при вводе в домен
--sg	Предоставление прав доменной группе пользователей использовать sudo, см. пример №5
-y	Автоматическое подтверждение запросов на выполнение действий при работе скрипта с параметрами
-f	Принудительный ввод в домен (вывод из домена) под своим прежним именем ПК (игнорируется существующая учетная запись ПК в домене)
--wg	Указать "**Имя домена (пред-Windows 2000)**" (необязательный ключ)
--delete-computer	Удаляет учётную запись ПК из домена (не выводит сам ПК из домена), см. пример №3
--sssd-lower-case	Принудительно устанавливает имя пользователя в нижнем регистре
-g	Запуск скрипта с графическим интерфейсом
-h, --help	Показать справку
-v	Вывод версии

Ввод РЕД ОС в домен MSAD с помощью консольных команд

Ввод в домен консольными командами
Список команд для быстрого ввода в домен через консоль
Ограничение доступа входа на ПК для доменных пользователей

ВАЖНО!

Имя ПК должно содержать только буквы (a–z), цифры (0–9), знак ''минус'' (-) и точку (.).

Данная инструкция не подходит для ПК, на которых установлено ПО SecretNet версии 1.9.

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Ввод в домен консольными командами

Подключаемся к домену Active Directory с помощью realmd.

Realmd (Realm Discovery) – это сервис, позволяющий производить настройку сетевой аутентификации и членства в домене MS AD без сложных настроек. Информация о домене обнаруживается автоматически. Для аутентификации и проверки учетных записей realmd использует SSSD (через Kerberos и LDAP) (также может использоваться и Winbind).

1. **Настройка NTP клиента**

Время на контроллере домена и на клиенте должно быть одинаково. Для синхронизации времени клиентского ПК с контроллером домена используйте клиент chrony. Откройте файл конфигурации NTP клиента CHRONY с помощью команды:

```
sudo nano /etc/chrony.conf
```

Удалите или закомментируйте в нем строки с серверами по умолчанию, а в качестве сервера времени укажите сервер контроллера домена:

```
server <FQDN_имя_контроллера_домена> iburst
```

После изменений конфигурационного файла вам надо перезапустить chronyd:

```
sudo systemctl restart chronyd
```

Проверьте работу chrony с помощью двух команд::

```
systemctl status chronyd
```

```
chronyc tracking
```

Пример вывода команды:

```
$ systemctl status chronyd
  chronyd.service - NTP client/server
    Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
    Active: active (running) since Вт 2019-07-09 11:13:49 MSK; 5min ago
  Process: 683 ExecStartPost=/usr/libexec/chrony-helper update-daemon (code=exited, status=0/SUCCESS)
  Process: 639 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 650 (chronyd)
    CGroup: /system.slice/chronyd.service
            └─650 /usr/sbin/chronyd
```

Пример вывода команды:

```
$ chronyc tracking
Reference ID    : 10.81.1.196 (dc.win.redos)
```

```
Stratum         : 4
Ref time (UTC)  : Wed Mar  4 09:44:17 2020
System time     : 0.000169261 seconds slow of NTP time
Last offset     : -0.000182217 seconds
RMS offset      : 0.000182217 seconds
Frequency       : 1.939 ppm slow
Residual freq   : -0.602 ppm
Skew            : 1.234 ppm
Root delay      : 0.047364 seconds
Root dispersion : 0.087531 seconds
Update interval : 64.7 seconds
Leap status     : Normal
```

2. **Установите необходимые пакеты, если они ещё не установлены**

```
sudo dnf install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation
```

3. **Выполните команду поиска домена**

```
realm discover < realm name >
```

ВАЖНО!

!!! Не рекомендовано использовать домен .local !!! Он зарезервирован для автоматически конфигурируемых сетей.

При использовании домена local

Если нужно получить доступ к ресурсам в уже существующей среде (Windows AD). То необходимо внести изменения в процесс разрешения хостов на linux машине. Отредактируйте /etc/nsswitch.conf. Изначально интересующий нас раздел содержит следующие записи:

```
hosts:          files mdns4_minimal [NOTFOUND=return] dns
```

Соответственно, в этом режиме сначала производится поиск в файле /etc/hosts, затем запрос идет к mdns, после чего возвращается ответ "не найдено". Mdns кэширует данные и работает с демоном Avahi. Модифицируйте эту "схему" к классическому виду:

```
hosts:          files dns
```

В РЕД ОС 7.3 изменять конфигурацию /etc/nsswitch.conf следует через файл

```
nano /etc/authselect/user-nsswitch.conf
```

после чего выполнить применение настроек:

```
authselect apply-changes
```

4. **Введите компьютер в домен, указав логин и пароль администратора домена**

```
sudo realm join -U -v <имя_администратора_домена> <realm_name>
```

Пример:

```
sudo realm join -U -v администратор win.redos
```

При успешном вводе ПК в домен, в конце вы увидите сообщение *"* Successfully enrolled machine in realm"*

5. **Теперь, если ввести команду realm list, то получим информацию о домене, а в консоли "Users and Computers" домена Active Directory появится новый компьютер.**

```
$ realm list
win.redos
```

```
type: kerberos
realm-name: WIN.REDOS
domain-name: win.redos
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
login-formats: %U@win.redos
login-policy: allow-realm-logins
```

6. **Некоторые действия и информацию можно получить с помощью утилиты** `adcli`**.**

```
$ adcli info win.redos
[domain]
domain-name = win.redos
domain-short = WIN
domain-forest = win.redos
domain-controller = dc.win.redos
domain-controller-site = Default-First-Site-Name
domain-controller-flags = pdc gc ldap ds kdc timeserv closest writable full-secret ads-web
domain-controller-usable = yes
domain-controllers = dc.win.redos
[computer]
computer-site = Default-First-Site-Name
```

7. **Откройте для редактирования файл** `/etc/sssd/sssd.conf`

```
sudo nano /etc/sssd/sssd.conf
```

Приведите строки к указанному ниже виду:

```
use_fully_qualified_names = False
ad_gpo_access_control = permissive
```

- use_fully_qualified_names = False - отключение режима полных имён для пользователей;
- ad_gpo_access_control = permissive - режим политики GPO входа пользователя в систему. В данном примере GPO оценивается, но не применяется.

8. **Разрешите доменным пользователям создавать домашние директории, для чего выполните команду:**

```
sudo authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

9. **Далее нужно отредактировать конфигурационный файл** ***/etc/krb5.conf***

Для доступа к сетевым ресурсам без запроса пароля (с помощью Kerberos) в файле /etc/krb5.conf нужно закомментировать строку

```
default_ccache_name = KEYRING:persistent:%{uid}
```

После нее вставить строку:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

Изменить значение параметра можно следующей командой:

```
sudo sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

В секцию `[libdefaults]` нужно добавить параметр `default_realm = REALM NAME`

Пример записи для домена **win.redos**:

```
default_realm = WIN.REDOS
```

Добавить параметр можно следующей командой (вместо `REALM NAME` укажите название своего домена ПРОПИСНЫМИ буквами):

```
sudo sed -i '/krb5cc_%{uid}/a default_realm = REALM NAME' /etc/krb5.conf
```

Этот параметр позволит пользователям при выполнении команды `kinit` не указывать полное имя пользователя (то есть можно использовать короткое имя пользователя *user* вместо *user@WIN.REDOS*).

Пример:

```
$ kinit user
Password for user@WIN.REDOS:
```

+ Для контроллера домена на базе Windows Server 2008 выполните дополнительные действия

  В связи с тем, что клиент Kerberos в Linux использует самый безопасный алгоритм шифрования при подключении к серверу Kerberos на MS AD, а 2008 версия windows не поддерживает его, вам придется явно указать, какими алгоритмами пользоваться клиенту. Отредактируйте файл /etc/krb5.conf. В секцию [libdefaults] впишите

  ```
  [libdefaults]
  ...
  default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
  default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
  preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
  ```

  Перезагрузите компьютер и попробуйте зайти под учетной записью доменного пользователя.

10. **Проверьте состояние службы sssd, в выводе статуса должно быть написано active (running)**

```
$ systemctl status sssd
 sssd.service - System Security Services Daemon
  Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset: disabled)
  Active: active (running) since Вт 2019-08-27 11:26:16 MSK; 2h 5min ago
Main PID: 31918 (sssd)
  CGroup: /system.slice/sssd.service
          ├─31918 /usr/sbin/sssd -i --logger=files
          ├─31919 /usr/libexec/sssd/sssd_be --domain implicit_files --uid 0 --gid 0 --logger=files
          ├─31920 /usr/libexec/sssd/sssd_be --domain win.redos --uid 0 --gid 0 --logger=files
          ├─31921 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --logger=files
          └─31922 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. **Пример настройки файла конфигурации /etc/samba/smb.conf**

Далее будут приведены примерные настройки конфигурационного файла **smb.conf**:

В блоке **[global]** указываются общие настройки.

Укажите свои данные домена для параметров **workgroup** и **realm**:

```
# Короткое имя домена в верхнем регистре
workgroup = WIN

# Домен в верхнем регистре
realm = WIN.REDOS
```

+ Остальные настройки можно оставить без изменений.

  ```
  # тип аутентификации, используемый для подключения к домену.
  security = ADS
  # определяет базу данных, которая будет использоваться для хранения учетных записей.
  passdb backend = tdbsam

  # определяет, будет ли winbind перечислять группы из домена.
  winbind enum groups = Yes
  # определяет, будет ли winbind перечислять пользователей из домена.
  winbind enum users = Yes
  ```

```
# определяет, будет ли winbind перечислять пользователей из домена.
winbind offline logon = Yes
# определяет, будет ли использоваться домен по умолчанию при входе в систему пользователей без указания имени домена.
winbind use default domain = No
# определяет, будет ли winbind обновлять билеты Kerberos.
winbind refresh tickets = Yes



# определяет время кэширования ID-отображений.
idmap cache time = 900
# настройки отображения ID между Windows и Unix.
idmap config * : backend = tdb
idmap config * : range = 10000-99999
idmap config SMBIND : backend = rid
idmap config SMBIND : range = 100000-999999

# минимальная версия SMB протокола клиента.
client min protocol = NT1
# максимально возможная версия SMB протокола клиента.
client max protocol = SMB3

# путь к файлу ключей Kerberos.
dedicated keytab file = /etc/krb5.keytab
# метод аутентификации Kerberos.
kerberos method = secrets and keytab

# время обновления пароля машины.
machine password timeout = 60
# определяет объекты VFS, используемые при монтировании файловой системы.
vfs objects = acl_xattr
# определяет, будет ли ACL-наследование применяться при создании файлов и каталогов.
map acl inherit = yes
# определяет, будут ли атрибуты DOS храниться в расширенных атрибутах файла.
store dos attributes = yes

printing = cups
printcap name = cups
load printers = yes
cups options = raw
```

Настройки блока **[global]** завершены.

Далее следует изменить блок **[homes]**, в котором необходимо указать настройки для доступа к папкам пользователей:

```
[homes]
comment = Home Directories
# "valid users" определеяет список пользователей или групп пользователей, которые имеют доступ к ресурсу.
# %S - подстановочный символ, который заменяется на имя текущей службы,
# %D - подстановочный символ, который заменяется на имя домена,
# %w - подстановочный символ, который заменяется на имя текущей машины.
valid users = %S, %D%w%S
# отключает/включает отображение данного ресурса в списке доступных ресурсов в проводнике или браузере файлов.
browseable = No
# разрешает запись на ресурс
read only = No
# позволяет унаследовать доступы на файлы и папки, если они не были явно настроены для данного ресурса.
inherit acls = Yes
```

В блоке **[printers]** укажите настройки для доступа к принтерам:

```
[printers]
comment = All Printers
path = /var/tmp
# устанавливает, что данная секция является принтером
printable = Yes
# права доступа для создания файлов
create mask = 0600
browseable = No
```

В блоке **[print$]** укажите параметры печати:

```
[print$]
comment = Printer Drivers
# путь к директории, которая будет использоваться для хранения драйверов принтеров
path = /var/lib/samba/drivers
# список пользователей/групп, имеющих права на запись
write list = @printadmin root
# устанавливает группу, которая будет установлена при создании файла/директории
force group = @printadmin
# устанавливает права доступа для создания файлов
create mask = 0664
# устанавливает права доступа для создания директорий
directory mask = 0775
```

Настройка файла **smb.conf** завершена. Обратите внимание, что приведены **примерные** настройки, которые могут быть изменены при необходимости.

12. **Также можно добавить новое правило в /etc/sudoers, чтобы доменный пользователь из группы администраторов домена мог получать права администратора локального компьютера:**Откройте файл /etc/sudoers для редактирования от пользователя root:

```
$ sudo nano /etc/sudoers
```

Добавьте в файл следующую строку, сохраните изменения и закройте редактор.

```
%администраторы\ домена ALL=(ALL) ALL
```

Данный параметр можно добавить командой:

```
sudo sh -c "echo '%администраторы\ домена ALL=(ALL) ALL' >> /etc/sudoers"
```

13. **Перезагрузите компьютер и войдите в ОС под учетной записью доменного пользователя.**

ВАЖНО!

Имя доменного пользователя должно состоять **из латинских символов** (кириллицу в имени пользователя использовать не рекомендуется).

Список команд для быстрого ввода в домен через консоль

В данном разделе собраны команды из раздела Ввод в домен консольными командами. Описание всех команд можно посмотреть в вышеуказанном подразделе. Не забудьте выполнить предварительную настройку ПК (задать имя и настроить сетевое соединение).

1. Настройте NTP-клиент

Здесь введите **своё FQDN имя контроллера домена**.

```
sudo sed -i 's/server/#server/g' /etc/chrony.conf
sudo sh -c "echo 'server <FQDN_имя_контроллера_домена> iburst' >> /etc/chrony.conf"
```

```
sudo systemctl restart chronyd
chronyc tracking
```

2. Установите необходимые пакеты, выполните поиск и настройку домена и введите компьютер в домен.

```
sudo dnf install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation
realm discover <имя_домена>
sudo realm join -U -v <имя_администратора_домена> <имя_домена>
```

При успешном вводе машины в домен вы увидите сообщение ***«* Successfully enrolled machine in realm»***

3. Отредактируйте файл sssd.conf и разрешите доменным пользователям создавать домашние директории.

```
sudo sed -i 's/use_fully_qualified_names = True/use_fully_qualified_names = False/g' /etc/sssd/sssd.conf
sudo sh -c "echo 'ad_gpo_access_control = permissive' >> /etc/sssd/sssd.conf"
sudo authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

4. Чтобы убрать предупреждение `"rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)"` **при выводе команды** `testparm -s`**:**

```
sudo sh -c "echo '*               -       nofile          16384' >> /etc/security/limits.conf"
sudo sh -c "echo 'root            -       nofile          16384' >> /etc/security/limits.conf"
```

+ Если контроллер домена основан на базе Windows Server 2008, то выполните следующую команду:

```
sudo sed -i '/\[libdefaults\]/a \    default_tkt_enctypes = RC4-HMAC, DES-CBC-CRC, DES3-CBC-SHA1,DES-CBC-MD5\n
default_tgs_enctypes = RC4-HMAC, DES-CBC-CRC, DES3-CBC-SHA1, DES-CBC-MD5' /etc/krb5.conf
```

5. **Для доступа доменных пользователей к сетевым ресурсам без запроса пароля (с помощью Kerberos) в файле /etc/krb5.conf нужно изменить параметр** `default_ccache_name`**:**

```
sudo sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

Добавление параметра `default_realm = REALM NAME` в секцию `[libdefaults]` позволит пользователям при выполнении команды `kinit` не указывать полное имя пользователя (то есть можно использовать короткое имя пользователя user вместо *user@WIN.REDOS*). Добавить параметр можно следующей командой (вместо `REALM NAME` укажите название своего домена ПРОПИСНЫМИ буквами):

```
sudo sed -i '/krb5cc_%{uid}/a default_realm = REALM NAME' /etc/krb5.conf
```

6. **Также можно добавить новое правило в /etc/sudoers, чтобы доменный пользователь из группы администраторов домена мог получать права администратора локального компьютера:**Данный параметр можно добавить командой:

```
sudo sh -c "echo '%администраторы\ домена ALL=(ALL) ALL' >> /etc/sudoers"
```

Ограничение доступа входа на ПК для доменных пользователей

Для данной настройки необходимо внести изменения в конфигурационный файл sssd.conf

```
access_provider = simple
simple_allow_users = user1@example.com, user2@example.com
simple_allow_groups = group@example.com
```

Параметр **access_provider = simple** определяет список доступа на основе имен пользователей или групп.

Настройка отображения общих ресурсов

> Данная инструкция применима для файловых ресурсов, находящихся в домене и развернутых на базе **Windows Server 2008r2** или **Windows Server 2012**.

Вы можете подробнее ознакомиться с информацией по вводу компьютера в домен, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Для отображения в файловом менеджере общих ресурсов, которые расположены в доменах **Microsoft Active Directory**, нужно отредактировать на клиентском ПК конфигурационный файл samba - **/etc/samba/smb.conf**, а также включить на сервере службу «*Браузер компьютеров*».

В качестве примера рассматривается: домен **win.redos**, имя контроллера домена - **dc.win.redos**

1) На сервере Windows нужно включить службу *«Браузер компьютеров»*. Укажите «Тип запуска» службы - «Автоматически», после чего произведите запуск службы.

2) В файле **/etc/samba/smb.conf** в секции [**global**] на клиенте нужно изменить некоторые параметры. По умолчанию в файле указываются параметры **workgroup = SAMBA** и **security = user**. Измените значения параметров или закомментируйте данные строки, добавив нужные параметры после них (если в конфигурационном файле один и тот же параметр указан несколько раз, то используется последний указанный параметр).

Пример настройки **/etc/samba/smb.conf** изменённые и добавленные параметры выделены жирным шрифтом):

```
[global]

security = ADS
workgroup = WIN
realm = win.redos
idmap config * : range = 10000-99999
client max protocol = NT1
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните команду проверки:

```
# testparm -s

Load smb config files fr om /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows lim it (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
```

Предупреждение **«rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)»** отображается в связи с тем, что в Linux по умолчанию установлен лимит на **1024** одновременно открытых файлов, а в Windows лимит равен **16384**. Чтобы убрать это предупреждение, добавьте в конец файла **/etc/security/limits.conf** строки:

```
*           -       nofile          16384
root        -       nofile          16384
```

3) В файле **/etc/krb5.conf** нужно закомментировать строку:

```
default_ccache_name = KEYRING:persistent:%{uid}
```

Вместо нее вставить параметр:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

4) Далее следует перезагрузить ПК.

После выполнения данных действий общие ресурсы будут отображаться в файловом менеджере.

В файловом менеджере **Caja (Mate)** в боковой панели слева нужно выбрать пункт *«Просмотреть сеть»*.

В файловом менеджере **Nemo (Cinnamon)** в боковой панели слева нужно выбрать пункт *«Сеть»*.

В целях безопасности на сервере Windows может быть отключен протокол **smb1**, в результате при подключении с РЕД ОС к серверу не будут видны общие сетевые ресурсы. Чтобы это исправить, в файле **/etc/samba/smb.conf** необходимо повысить версию протокола, указав **client max protocol = SMB2** или **client max protocol = SMB3**.

Создание кнопки запуска доступа к сетевому ресурсу

В MATE
В KDE
В GNOME

Окружение

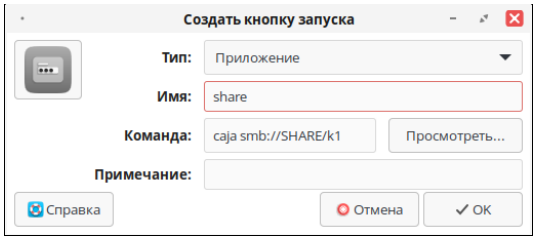
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

В разных графических окружениях процесс создания кнопки запуска к сетевому ресурсу отличается. Далее будет рассмотрена настройка для каждого графического окружения.

В MATE

Для создания кнопки запуска сетевого ресурса на рабочем столе нужно нажать правой кнопкой мыши по свободному месту рабочего стола и выбрать пункт «*Создать кнопку запуска...*».

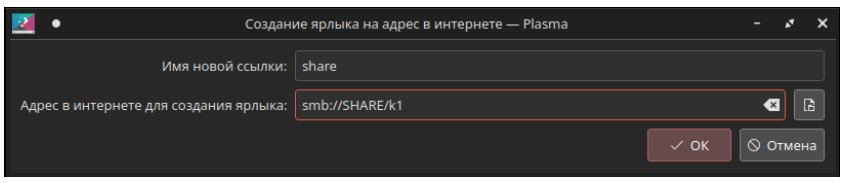
В открывшемся окне в поле «**Имя**» впишите отображаемое имя под кнопкой (название ярлыка). В поле «**Команда**» впишите `caja` и через пробел `путь к сетевому каталогу`. Его можно скопировать в адресной строке в файловом менеджере, находясь в нужном сетевом каталоге. Общий вид команды может быть, например, таким: `caja smb://SHARE/k1`. После всех действий нажмите кнопку «**ОК**».



В KDE

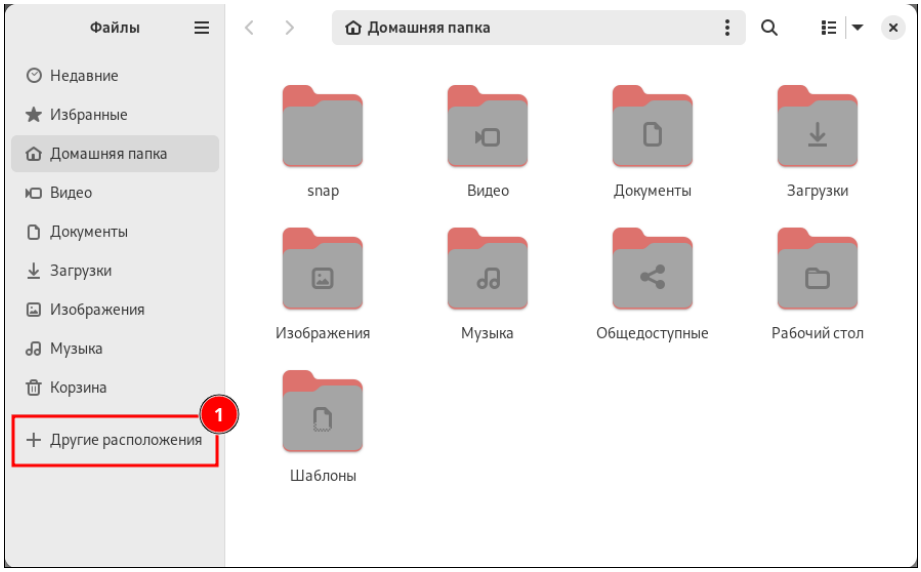
Для создания кнопки запуска сетевого ресурса на рабочем столе нужно нажать правой кнопкой мыши по свободному месту рабочего стола и выбрать пункт «*Создать*» — «*Ярлык для адреса в интернете (URL)...*».

В открывшемся окне в поле «**Имя новой ссылки**» впишите отображаемое имя под кнопкой (название ярлыка). В поле «**Адрес в интернете для создания ярлыка**» впишите путь к сетевому каталогу. Его можно скопировать в адресной строке в файловом менеджере, находясь в нужном сетевом каталоге. Общий вид команды может быть, например, таким `smb://SHARE/k1`. После всех действий нажмите кнопку «**ОК**».



В GNOME

Для создания кнопки запуска сетевого ресурса на рабочем столе необходимо открыть домашний каталог пользователя и в левом боковом меню выбрать «**Другие расположения**».



Далее необходимо перейти к нужному сетевому каталогу, кликнуть про нему ПКМ и выбрать в контекстном меню «**Присоединить**». Выбранный каталог будет отображаться на рабочем столе пользователя.

Отключение отображения определенного пользователя на экране входа в систему

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

MATE

Для отключения отображения определенного пользователя на экране входа в систему необходимо:

1. Перейти в каталог **/var/lib/AccountsService/users**:

```
sudo cd /var/lib/AccountsService/users
```

2. Создать файл настроек определенного пользователя, например, **user**:

```
sudo nano user
```

Для **MATE** добавить в файл следующие строки:

```
[User]
Language=
XSession=mate
SystemAccount=true
```

3. Для применения изменений перезагрузить ПК.

KDE Plasma

Для отключения отображения определенного пользователя на экране входа в систему необходимо:

1. Открыть на редактирование файл **/etc/sddm.conf**:

```
sudo nano /etc/sddm.conf
```

2. В разделе [Users] раскомментировать параметр **HideUsers=** и добавить в него пользователя, например, **user**:

```
[Users]
HideUsers=user
```

3. Для применения изменений перезагрузить ПК.

GNOME

Для отключения отображения определенного пользователя на экране входа в систему необходимо:

1. Перейти в каталог **/var/lib/AccountsService/users**:

```
sudo cd /var/lib/AccountsService/users
```

2. Создать файл настроек определенного пользователя, например, **user**:

```
sudo nano user
```

Для **GNOME** добавить в файл следующие строки:

```
[User]
Language=
XSession=gnome
SystemAccount=true
```

3. Для применения изменений перезагрузить ПК.

Предоставление права пользователям домена выполнять команды от пользователя root

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Выполните вход в РЕД ОС под доменным пользователем Active Directory.

Выведите список групп, в которых пользователь состоит, выполнив команду:

```
groups
```

Пример:

```
[admin@win.red-soft.ru]$ groups
"пользователи домена администраторы домена dnsadmins"
```

Запомните группу в выводе, к примеру **dnsadmins**.

Откройте файл /etc/sudoers для редактирования от пользователя **root**:

```
su
nano /etc/sudoers
```

Найдите строку:

```
%wheel  ALL=(ALL)    ALL
```

После этой строки вставьте название группы из AD по аналогии с предыдущей:

```
%dnsadmins ALL=(ALL)    ALL
```

Сохраните файл.

ВАЖНО!

Если в названии группы имеется **пробел**, то его необходимо экранировать с помощью обратного слеша — '\'.

Пример:

```
%администраторы\ домена ALL=(ALL) ALL
```

Данный параметр можно добавить командой:

```
sudo sh -c "echo '%администраторы\ домена ALL=(ALL) ALL' >> /etc/sudoers"
```

Примечание.

Если вы используете **winbind** при вводе ПК в домен, то в файл **/etc/sudoers** нужно добавлять пользователей и группы в следующем виде:

```
%DOMAIN\\group   ALL=(ALL) ALL
%DOMAIN\\user   ALL=(ALL) ALL
```

Теперь проверьте, что пользователю или группе пользователей можно выполнять команды от имени суперпользователя **root**. Выполните команду:

```
cat /etc/sudoers
cat: /etc/sudoers: Отказано в доступе
```

Но, если выполнить эту команду, добавив `sudo` и введя пароль пользователя, то `cat` выведет содержимое файла:

```
sudo cat /etc/sudoers
```

Вывод РЕД ОС из домена MSAD

Вывод из домена с помощью графической программы
Вывод из домена консольными командами

Вы можете подробнее ознакомиться с информацией по выводу компьютера из домена, просмотрев наши обучающие видео:

- на **RuTube** — Ввод ПК с РЕД ОС в домен Windows;
- в **Яндекс.Дзен** — Ввод ПК с РЕД ОС в домен Windows;
- в **VK Видео** — Ввод ПК с РЕД ОС в домен Windows.

На наших каналах вы также сможете найти много другой полезной информации.

Вывод из домена с помощью графической программы

Вывести компьютер из домена можно с помощью графической программы **join-to-domain**, установка данной программы:

```
sudo dnf install join-to-domain
```

После установки зайдите в меню, в разделе "*Администрирование*" выберите новый пункт *"Ввод ПК в домен"*.

Если ПК находится в домене, то при запуске утилиты она предложит вывести компьютер из домена. Для вывода из домена нужно подтвердить выполнение, дождаться окончания процесса и перезагрузить ПК.

Вывод из домена консольными командами

Для получения списка сконфигурированных доменов выполните:

```
realm list
```

Если в выводе присутствует одна запись:

```
sudo realm leave -v -U <username>@<domain>
```

Если в выводе присутствует две записи (две записи присутствуют при использовании двух client-software - winbind и sssd), тогда нужно выполнить две команды:

```
sudo realm leave -v --client-software=sssd -U <username>@<domain>
sudo realm leave -v --client-software=winbind -U <username>@<domain>
```

Нужно ввести пароль пользователя *<username>@<domain>*, который является Администратором домена. Для вывода из домена требуются права администратора. Поэтому при запросе пароля привилегированного пользователя нужно ввести пароль локального пользователя с правами администратора.

В конце вывода команды должно выдаваться сообщение об успешном выводе из домена:
`Successfully unenrolled machine from realm`

Проверить, успешно ли ПК был выведен из домена, можно командой `realm list` - в выводе не должно быть никаких записей

Если в окне входа в пользовательскую учетную запись после вывода из домена отображаются пользователи домена, выполните с привилегиями суперпользователя команду очистки кэша sssd

```
sudo sss_cache -E
```

Каталог общего сетевого доступа на РЕД ОС в домене MSAD

Графический вариант
Работа из файлового менеджера
Консольный вариант

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: share_directory 6.0-1

Рассмотрен механизм создания в РЕД ОС каталога с общим сетевым доступом по протоколу smb. РЕД ОС предварительно необходимо включить в домен *MS AD* согласно инструкциям текущего раздела «Работа с доменом MS AD».

Графический вариант

Утилита публикации сетевого ресурса в домене *Samba / MS AD* доступна в РЕД ОС.

Установите утилиту командой:

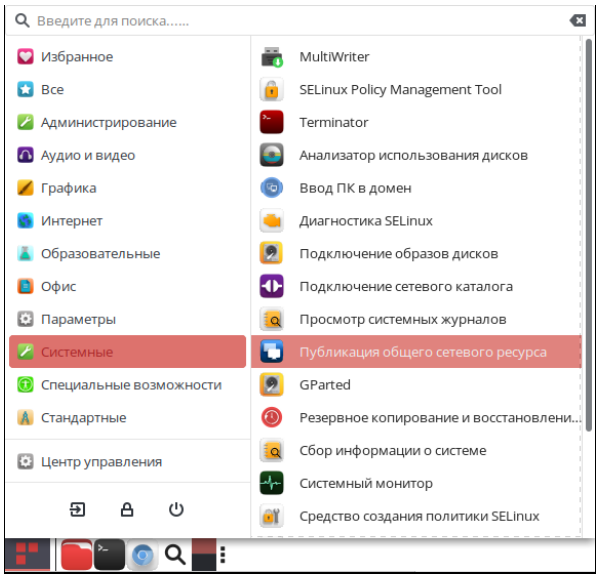
```
dnf install share_directory
```

От имени **root**-пользователя получите **kerberos ticket**:

```
su -
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

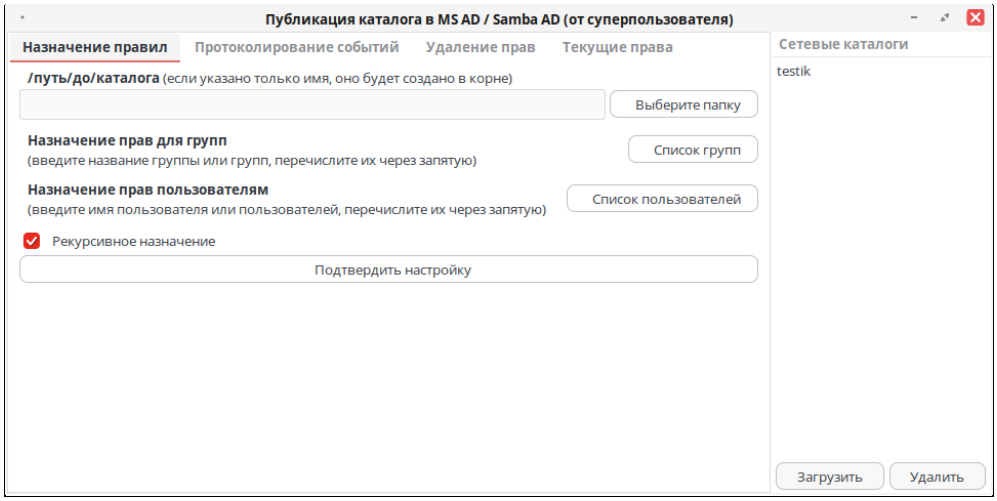
Запуск утилиты доступен через главное меню:



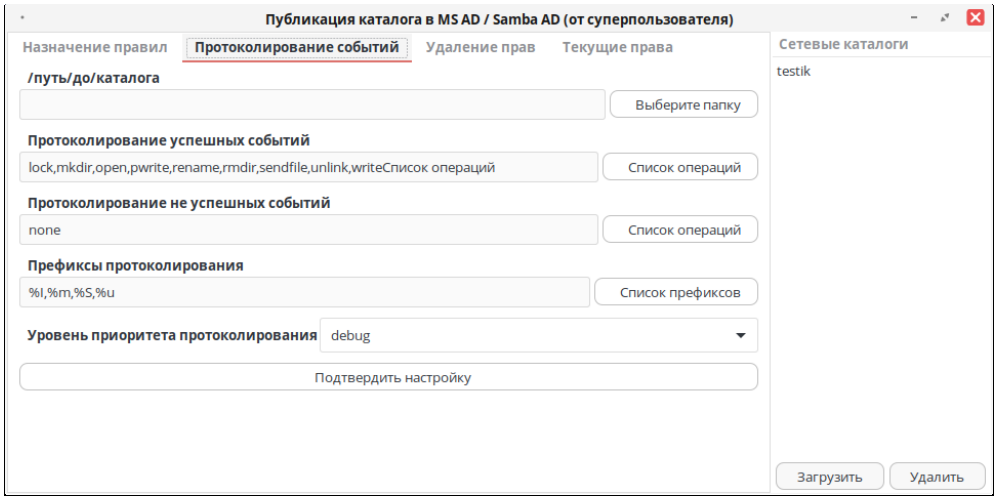
или через терминал:

```
share-directory
```

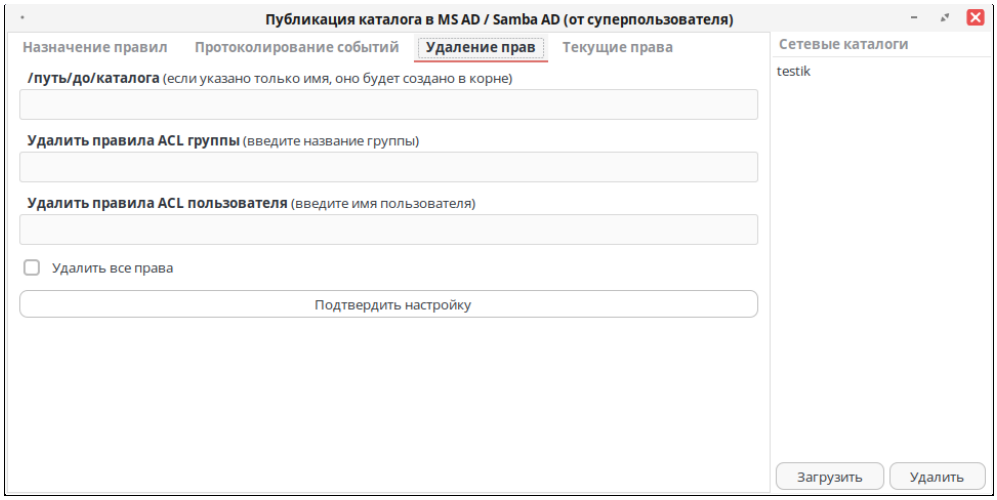
Для публикации сетевого ресурса в домене требуется задать путь к директории, пользователей и/или групп и соответствующие им права.



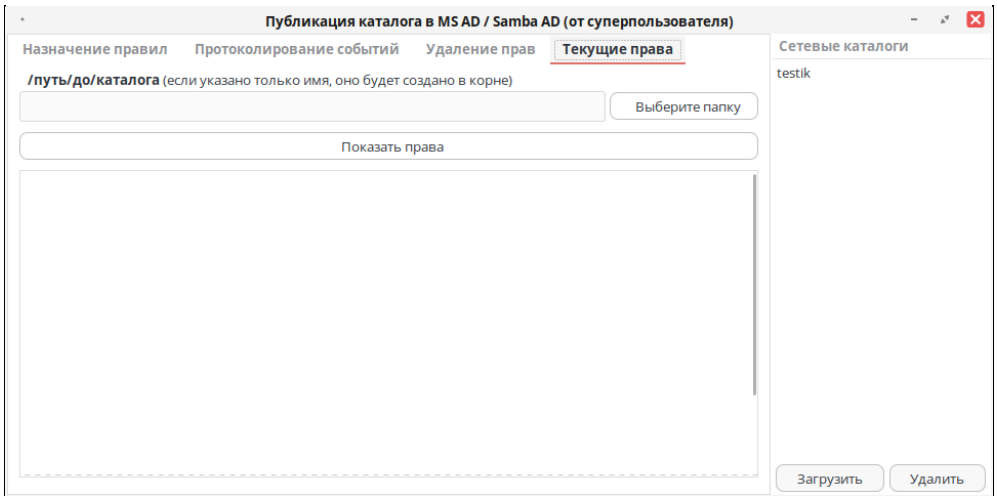
Для протоколирования событий предусмотрена соответствующая вкладка.



Для того чтобы *удалить права* с директории, требуется указать путь к ресурсу и прописать определенного пользователя или группу, которых требуется удалить. Так же доступно полное удаление ACL-прав с директории.



Для удобства *отслеживания прав* можно посмотреть текущие права директории, указав путь к интересующей.



Работа из файлового менеджера

Для включения быстрой настройки сетевой директории из файлового менеджера **caja** необходимо установить дополнительное расширение. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install share_directory-caja
```

Затем получите **kerberos ticket**:

```
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

Выйдите из учетной записи **root** командой:

```
exit
```

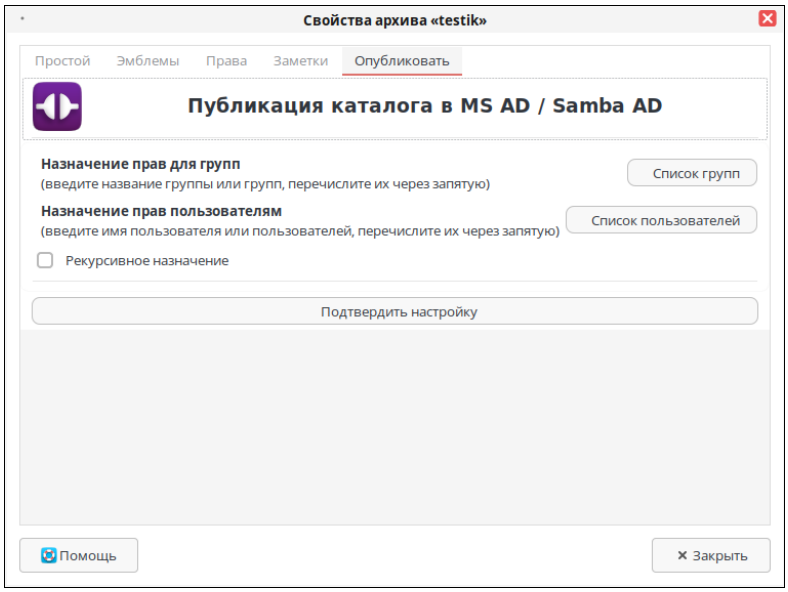
Затем обновите конфигурацию **caja** от имени **локального** пользователя:

```
caja -q
```

Или выполните выход из учетной записи пользователя и обратную авторизацию.

После обновления списка расширений **caja** станет доступен новый пункт в свойствах директории.

Вызовите контекстное меню правой кнопкой мыши для необходимой директории в файловом менеджере, затем выберите пункт «**Свойства**» – «**Опубликовать**».



Консольный вариант

Примечание.

Предполагается, что рабочая станция введена в домен посредством утилиты **join-to-domain** с выбором **sssd**.

Все указанные действия производятся от имени **суперпользователя** (**root**).

1. Добавьте параметр winbind в конце строк, начинающихся с group, passwd и shadow, в файле профиля *authselect* **/etc/authselect/custom/sssd_domain/nsswitch.conf** командой:

```
sed -i_bak '/^\(group:\|passwd:\|shadow:\)/ {s/\(winbind \)\(.*\)$/\2 winbind/; /winbind/ ! s/$/ winbind/}'
/etc/authselect/custom/sssd_domain/nsswitch.conf
```

2. Примените изменения профиля *authselect* командой:

```
authselect apply-changes
```

3. Проверьте возможность получения *kerberos*-билета для доменного пользователя:

```
kinit username
klist
```

4. Проверьте доступность входа доменного пользователя в систему:

```
su username
exit
```

5. Создайте каталог для общего доступа:

```
mkdir -p /share/
```

6. Назначьте права доступа. Пример для домена *wintest*:

```
chown -R root:"wintest\Пользователи домена" /share
chmod 2770 /share
setfacl -m default:group:"wintest\Администраторы домена":rwx /share/
setfacl -m default:group:"wintest\Пользователи домена":r-x /share/
setfacl -m default:other::--- /share/
```

В данном примере с помощью команды **setfacl** были выданы полные (rwx) права группе «**Администраторы домена**» на каталог **/share**.

Группе «**Пользователи домена**» домена *wintest* были выданы права только на чтение и выполнение (просмотр содержимого каталога).

7. Настройте политику *SELinux* для общего каталога и примените её:

```
semanage fcontext -a -t samba_share_t "/share(/.*)?"
restorecon -R -v /share
```

8. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) в секции [global] проверьте наличие следующих строк:

```
vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab
```

9. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) создайте раздел настроек общего ресурса [share] (с этим именем ресурс будет отображаться для клиентов):

```
[share]
 path = /share/
 read only = no
 browseable = yes
 create mask = 0664
 directory mask = 0775
```

10. Дополнительная настройка прав:

- установить полные права на каталог для группы:

```
setfacl -m g:"wintest\Группа_Пользователей":rwx /share
```

- установить полные права на каталог для пользователя:

```
setfacl -m u:"wintest\Пользователь":rwx /share
```

- удалить ACL для определённого пользователя:

```
setfacl -x u:alex /share
```

- удалить все ACL-права каталога:

```
setfacl -b /share
```

- просмотреть ACL-права на каталог:

```
getfacl /share
```

Подробное описание списков контроля доступа (ACL) и параметров команды **setfacl** доступно в нашей статье «Списки контроля доступа ACL»

11. Установите автоматический запуск служб *samba*:

```
systemctl enable smb --now
systemctl enable nmb --now
systemctl enable winbind --now
```

12. Перезагрузите рабочую станцию. Проверьте статус служб:

```
systemctl is-failed smb
systemctl is-failed nmb
systemctl is-failed winbind
```

При корректной настройке каждая команда должна вывести сообщение «active».

О домене IPA

Что такое домен IPA?

Домен IPA (FreeIPA) - это интегрированное решение идентификации и авторизации для РЕД ОС. Сервер FreeIPA обеспечивает централизованную аутентификацию, авторизацию и предоставление учетной информации путем хранения данных о пользователе, группах, хостах и других объектах, необходимых для управления аспектами безопасности компьютерной сети.

FreeIPA построена на основе хорошо известных Open Source компонентов и стандартных протоколов с очень сильной ориентацией на простоту управления и автоматизацию задач установки и настройки.

Несколько FreeIPA-серверов можно легко настроить в домене FreeIPA, чтобы обеспечить избыточность и масштабируемость. 389 Directory Server является основным хранилищем данных и предоставляет полный LDAPv3 мульти-мастер инфраструктуры каталогов. Аутентификация с использованием единого входа осуществляется через MIT Kerberos KDC. Возможности аутентификации дополняются интегрированным центром сертификации на основе проекта Dogtag . При желании можно управлять именами доменов с помощью интегрированного сервера DNS .

Управление полностью централизовано и управляется через веб - интерфейс или инструмент командной строки.

Вы можете подробнее ознакомиться с доменом IPA, просмотрев наши обучающие видео:

- на **RuTube** — Обзор домена FreeIPA;
- в **Яндекс.Дзен** — Обзор домена FreeIPA;
- в **VK Видео** — Обзор домена FreeIPA.

На наших каналах вы также сможете найти много другой полезной информации.

Зачем использовать домен IPA?

Для обеспечения эффективности, соблюдения и снижения рисков организациям необходимо централизованно управлять и сопоставлять важную информацию о безопасности, включая:

- **Идентификацию** (машин, пользователей, виртуальных машин, групп, учетных данных для проверки подлинности)
- **Политики** (управление доступом на основе хоста, правил sudo, пользовательских карт SELINUX)
- **SSO** - технология единого доступа к различным сервисам и ресурсам

Домен на основе IPA сфокусирован на том, чтобы информация о пользователе, политиках и аудите была легко централизованной, совместимой и управляемой. Так же, имеет возможность взаимодействовать с Windows доменами и многое другое.

Рекомендации по развертыванию

ВАЖНО!

Некоторые параметры и решения, не учтенные до развертывания IPA очень трудно изменить позже или даже невозможно. Поэтому в этом пункте приводятся важнейшие особенности и решения, необходимые для успешного развертывания.

Вы можете подробнее ознакомиться с доменом IPA, просмотрев наши обучающие видео:

- на **RuTube** — Обзор домена FreeIPA;
- в **Яндекс.Дзен** — Обзор домена FreeIPA;
- в **VK Видео** — Обзор домена FreeIPA.

На наших каналах вы также сможете найти много другой полезной информации.

DNS

DNS преднамеренно отображается первым, поскольку DNS играет важную роль в функциях управления идентификацией, особенно Kerberos.

Домен

IPA всегда должен иметь собственный основной домен, например example.ru или ipa.example.ru, который не должен использоваться совместно с другой системой управления идентификацией на основе Kerberos, поскольку в противном случае на уровне системы Kerberos будут возникать конфликты. Например, если IPA и Active Directory используют один и тот же домен, доверительные отношения никогда не будут возможны, а также автоматическое обнаружение клиентского сервера через DNS SRV-записи.

Избегайте коллизий имен. Мы настоятельно рекомендуем вам не использовать доменное имя, которое не делегировано вам, даже в частной сети. Например, вы не должны использовать доменное имя example.ru, если у вас нет действительного делегирования для него в общедоступном дереве DNS. Если это правило не соблюдается, доменное имя будет разрешено по-разному в зависимости от конфигурации сети. В результате сетевые ресурсы станут недоступными. Использование доменных имен, которые не делегированы вам, также затрудняет развертывание и обслуживание DNSSEC. Дополнительную информацию об этой проблеме можно найти в FAQ ICANN по вопросам коллизий доменных имен.

Клиентские машины не обязательно должны находиться в том же домене, что и IPA-серверы. Например, IPA может быть доменом ipa.example.ru и иметь клиентов в домене clients.example.ru, просто нужно иметь четкое сопоставление между доменом DNS и областью Kerberos. Стандартным методом для создания сопоставления являются записи TXT DNS (IPA DNS добавляет их автоматически).

ВАЖНО

!!! Не называйте свой домен .local !!! Он зарезервирован для автоматически конфигурируемых сетей.

Если нужно получить доступ к ресурсам в уже существующей среде (Windows AD). То необходимо внести изменения в процесс разрешения хостов на linux машине. Отредактируйте /etc/nsswitch.conf. Изначально интересующий нас раздел содержит следующие записи:

```
hosts:      files mdns4_minimal [NOTFOUND=return] dns
```

Соответственно, в этом режиме сначала производится поиск в файле /etc/hosts, затем запрос идет к mdns, после чего возвращается ответ "не найдено". Mdns кэширует данные и работает с демоном Avahi. Модифицируйте эту "схему" к классическому виду:

```
hosts:      files dns
```

Особенности для интеграции с Active Directory

Домен Active Directory - сложная система. Он включает в себя логически структурированный набор ресурсов (машины, пользователи, службы и т. д.), которые принадлежат потенциально нескольким доменам DNS. Несколько доменов DNS могут быть частью одного домена AD (где домен AD по определению совпадает с областью AD Kerberos). Несколько доменов AD можно объединить в лес. Самый

первый домен AD, созданный в лесу, называется **лесной корневой домен** . Верхнее имя основного домена DNS домена AD используется как имя домена Kerberos AD.

Домен IPA тоже представляет собой сложную систему. Он включает в себя логически структурированный набор ресурсов (машины, пользователи, службы и т. д.), которые принадлежат потенциально нескольким доменам DNS. В отличие от Active Directory у нас есть один домен / область IPA для развертывания, а для Active Directory этот единственный домен IPA выглядит как отдельный лес Active Directory. Active Directory считает основной домен DNS, используемый в качестве основы для области Kerberos IPA, как корневой домен леса для домена IPA (например, корневой домен леса для Active Directory).

Домен IPA может быть размещен в **любом** домене DNS, который не имеет прямого совпадения с любым доменом в лесу Active Directory. Он может быть, например, ipa.example.ru, если эта зона DNS не занята каким-либо другим доменом AD в том же лесу. Или может быть ipa.ad.example.ru, если нет перекрытий на одном уровне зоны DNS.

Доверие между двумя лесами Active Directory всегда устанавливается как доверие между корневыми доменами этих лесов. Если домен IPA использует ipa.ad.example.ru в качестве основной зоны DNS, мы будем говорить об установлении доверительного отношения к лесу между лесом Active Directory ad.example.ru и доменом IPA ipa.ad.example.ru. Если существует несколько зон DNS, принадлежащих домену IPA, рекомендуется размещать записи kerberos указывающие на имя области IPA в каждом из них для правильного обнаружения сетевых ресурсов клиентами IPA.

DNS-сервер

Домен IPA может обслуживаться либо интегрированной службой DNS, либо внешней службой. Рекомендуется использовать интегрированную службу DNS.

При использовании интегрированной службы DNS пакет bind-dyndb-ldap должен быть установлен перед разворачиванием IPA сервера.

При использовании внешнего сервера имен возможно использование функций управления идентификацией или доверия, однако конфигурация будет намного сложнее и подвержена ошибкам.

Имя области Kerberos

Когда вы начинаете устанавливать сервер IPA, вы всегда определяете имя области Kerberos для этой установки. При выборе названия области выполните следующие правила:

- Имя области не должно конфликтовать с любым другим существующим именем области Kerberos (например, имя, используемое Active Directory).
- Имя области должно быть верхним регистром (EXAMPLE.RU) основного DNS-имени домена (example.ru).
- Клиенты IPA из разных доменов DNS (example**.net**, example**.org,** example**.com**) могут быть объединены в единую область Kerberos (EXAMPLE**.RU**)
- Одна установка IPA всегда представляет собой единую область Kerberos.

ВАЖНО

Невозможно изменить основной домен и область IPA после установки. Продумайте его тщательно. Не ожидайте перехода от лабораторной / промежуточной среды к рабочей среде (например, сменить lab.example.ru на ipa.example.ru)

Множественное развертывание

Серверы и клиенты IPA могут распространяться в разных географических точках. Механизм местоположения DNS позволяет разделить топологию на отдельные области, называемые *местоположениями*. Клиенты, использующие записи DNS SRV (например, SSSD) в одном месте, используют близлежащие серверы IPA.

При планировании развертывания важно иметь в виду, что функции DNS в IPA требуют, по крайней мере, одного DNS-сервера в каждом месте. Если это необходимо, можно использовать несколько DNS-представлений на внешних DNS-серверах вместо развертывания DNS-сервера для каждого местоположения, но такие настройки обычно менее устойчивы.

PKI

Когда выполнена настройка PKI, хосты и службы IPA могут получать подписанные сертификаты от IPA CA. Затем сертификаты могут использоваться для аутентификации или проверки подлинности в настроенных службах.

В настоящее время существует 3 типа, настройки среды сертификатов IPA:

1. Без смешивания - IPA просто устанавливается с собственной службой PKI и самозаверяющим сертификатом ЦА
2. Внешний ЦА - IPA установлен с собственной PKI, но сертификат ЦА подписан внешним центром сертификации (служба сертификации Active Directory или другая пользовательская служба сертификации). Для этого требуется, чтобы внешний ЦС разрешил субцентры.
3. Установка без ЦА- IPA не настраивает собственный ЦС, но использует подписанные сертификаты хоста из внешнего ЦС.

ВАЖНО

После установки невозможно изменить базу данных сертификата IPA. Продумайте это тщательно. По умолчанию используется О

```
= $ REALM
```

Серверы/Реплики

Исключительность сервера IPA

Настоятельно рекомендуется избегать развертывания других приложений или служб на виртуальной машине IPA по нескольким основным причинам:

- Причины производительности - сервер IPA может быть ресурсозатратным для машины, особенно когда количество объектов LDAP велико;
- Стабильность - IPA интегрирована в систему, и если стороннее приложение меняет конфигурацию или службы IPA, домен может сломаться
- Легче перенести сервер IPA на более новую платформу

Количество серверов

IPA работает в реплицированной среде с несколькими мастерами. Количество серверов зависит от нескольких факторов:

- Сколько записей в системе?
- Сколько у вас разных географически распределенных центров обработки данных?
- Насколько активны приложения и клиенты в отношении аутентификации и поиска LDAP.

Как правило, рекомендуется иметь по меньшей мере 2-3 реплики в каждом центре обработки данных. В каждом центре обработки данных должна быть по крайней мере одна реплика с дополнительными службами IPA, такими как PKI или DNS, если они используются. Обратите внимание, что не рекомендуется иметь более 4 реплик в одном месте. В следующем примере показана рекомендуемая инфраструктура:

Клиенты

У каждого клиента для отказоустойчивости должно быть как минимум 2 DNS сервера, настроенных в /etc/resolv.conf. Обновите конфигурацию resolv.conf и *DHCPd* .

Для каждого клиента, использующего ipa-client-install, требуется доступ к порту 443 (HTTPS) на сервере IPA. Это связано с тем, что после регистрации клиент загружает собственные ключи SSH и выполняет несколько операций. IPI CLI также использует тот же порт для связи с ведущим IPA. Таким образом, требуется доступ к HTTPS (443) с клиентской стороны.

Интеграция с Active Directory

Чтобы настроить доверительные отношения, необходимо правильно настроить DNS, IPA должен иметь собственный первичный DNS-домен, и соответствующую ему область Kerberos. DNS-домен и область Kerberos должны отличаться от домена DNS Active Directory.

Еще одним важным требованием является стек IPv6. Рекомендуемым способом для современных сетевых приложений является только открытие сокетов IPv6 для прослушивания, поскольку IPv4 и IPv6 используют один и тот же диапазон локальных портов. IPA использует Samba как часть интеграции с Active Directory, а Samba **требует включенного стека IPv6** на машине.

НЕ используйте ipv6.disable = 1 в командной строке ядра: он отключает весь стек IPv6 и ломает Samba.

Если необходимо, добавьте ipv6.disable_ipv6 = 1, это будет поддерживать функциональность стека IPv6, но не будет назначать адреса IPv6 для ваших сетевых устройств. Это рекомендуемый подход для случаев, когда вы не используете сети IPv6.

Добавление следующих строк в /etc/sysctl.d/ipv6.conf, позволит не назначать адреса IPv6 для определенного сетевого интерфейса:

```
net.ipv6.conf.all.disable_ipv6 = 1
# Отключение «все» не применяется к интерфейсам, которые уже используются, когда применяются параметры sysctl.
net.ipv6.conf.<интерфейс0>.disable_ipv6 = 1
```

где *interface0* - ваш специализированный интерфейс. Обратите внимание, что все, что нам нужно, это то, чтобы стек IPv6 был включен на уровне ядра, это рекомендуется для разработки сетевых приложений уже давно.

SSL

Из-за CVE-2014-3566 протокол протокола Secure Socket Layer версии 3 (SSLv3) должен быть отключен в модуле mod_nss. Вы можете сделать это, выполнив следующие шаги:

1. Отредактируйте файл/etc/httpd/conf.d/nss.conf и установите параметр *NSSProtocol* (для обратной совместимости) и TLSv1.1.

```
NSSProtocol TLSv1.0, TLSv1.1
```

2. Перезапустите httpd-службу.

```
systemctl restart httpd
```

Установка сервера IPA

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер минимальный
- **Версия ПО:** ipa-server-4.10.3-1

Вы можете подробнее ознакомиться с информацией по установке в РЕД ОС сервера IPA, просмотрев наши обучающие видео:

- на **RuTube** — Установка и настройка FreeIPA в РЕД ОС;
- в **Яндекс.Дзен** — Установка и настройка FreeIPA в РЕД ОС;
- в **VK Видео** — Установка и настройка FreeIPA в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Подготовка сервера

Настройка синхронизации времени с помощью chronyd

Откройте файл конфигурации:

```
# nano /etc/chrony.conf
```

Если есть необходимость, то пропишите в файле сервера времени, перед стандартными серверами.

```
server ntp1.vniiftri.ru iburst
server ntp2.vniiftri.ru iburst
server ntp3.vniiftri.ru iburst
server ntp4.vniiftri.ru iburst
```

Отключите сервис:

```
# systemctl disable --now systemd-timesyncd
```

Установите часовой пояс:

```
# timedatectl set-timezone Europe/Moscow
```

Настройте сетевой адаптер

> **ВАЖНО!**
>
> IP-адрес сервера никогда не должен изменяться. Сделайте его статическим в вашей сети.

Более подробное описание конфигурирования сетевого адаптера вы можете найти в статье «Настройка сетевого адаптера».

Назначьте имя серверу

Используйте полное доменное имя. Имя серверу можно назначить командой

```
# hostnamectl set-hostname server.redosipa.ru
```

Установите ipa-server

Установите IPA сервер:

```
# dnf install bind bind-dyndb-ldap ipa-server ipa-server-dns ipa-server-trust-ad python3-packaging
```

> **ВАЖНО! ТОЛЬКО ДЛЯ РЕД ОС ВЕРСИИ 7.3**

Для того чтобы при установке избежать появления ошибки **"CA configuration failed"**, выполните следующие действия:
1. Убедитесь, что используется Java OpenJDK версии 8:

```
java -version
```

2. Если используется Java 11, то необходимо переключиться на 8-ую версию. Для этого выполните команды:

```
update-alternatives --config java
update-alternatives --config jre_openjdk
```

в каждой выберите нужную версию, указав ее порядковый номер. После чего нажмите *Enter*.

3. Удалите пакет:

```
rpm -e java-17-openjdk-headless --nodeps
```

Удалите пакет Java OpenJDK версии 11:

```
rpm -e java-11-openjdk-headless --nodeps
```

Настройка сервера

Есть два варианта настройки, интерактивный и автоматический.

ВАЖНО!

Невозможно изменить конфигурацию ЦС после создания домена, и невозможно перенести его из одной конфигурации в другую. Крайне важно, чтобы требования ЦС были рассмотрены до начала процесса установки.

Если каждая машина в домене будет клиентом IPA, добавьте адрес сервера IPA в конфигурацию DHCP.

Заметка

Сценарий ipa-replica-install включает в себя утилиту ipa-replica-conncheck, которая проверяет статус требуемых портов. Вы также можете запускать ipa-replica-conncheck отдельно для устранения неполадок.

+ Опции и параметры автоматической установки.

Основные параметры

-r *REALM_NAME*, **--realm**=*REALM_NAME (REALM имя)*

Имя области Kerberos для сервера IPA

-n *DOMAIN_NAME*, **--domain**=*DOMAIN_NAME* (*доменное имя)*

Ваше доменное имя DNS

-p *DM_PASSWORD*, **--ds-password**=*DM_PASSWORD (DM пароль)*

Пароль, который будет использоваться сервером каталогов для пользователя Менеджера каталогов

-P *MASTER_PASSWORD*,

--master-password=*MASTER_PASSWORD (мастер паролей)*

Главный пароль kerberos (обычно генерируемый автоматически)

-a *ADMIN_PASSWORD*,

--admin-password=*ADMIN_PASSWORD (пароль администратора*)

Пароль для пользователя admin IPA

--hostname=*HOST_NAME (имя хоста*)

Полное DNS-имя этого сервера. Если имя хоста не совпадает с именем системного хоста, системное имя хоста соответственно, будет обновляться, чтобы предотвратить сбои службы.

--ip-address=*IP_ADDRESS* (*IP адрес*)

IP-адрес этого сервера. Если этот адрес не соответствует адресу, который хост разрешает, и --setup-dns не выбран, установка завершится с ошибкой. Если имя хоста сервера не разрешимо, запись для имени хоста и IP_ADDRESS добавляется в / etc / hosts.

-N, **--no-ntp** *(нет **ntp**)*

Не настраивать NTP

--idstart=*IDSTART*

Начальный идентификатор пользователя и группы (по умолчанию случайный)

--idmax=*IDMAX*

Максимальный идентификатор пользователя и группы (по умолчанию: idstart + 199999). Если установлено равным нулю, будет использоваться значение по умолчанию.

--no_hbac_allow *(не разрешать hbac)*

Не устанавливайте правило allow_all (разрешить всё) HBAC. Это правило позволяет любому пользователю с любого хоста получать доступ к любой службе на любом другом хосте. Ожидается, что пользователи удалят это правило перед переходом на производство.

--no-ui-redirect *(не перенаправлять ui)*

Не следует автоматически перенаправлять веб-интерфейс,

--ssh-trust-dns *(ssh доверить dns)*

Настройте клиент OpenSSH для проверки записей DNS SSHFP,

--no-ssh *(нет ssh)*

Не настраивайте клиента OpenSSH,

--no-sshd *(нет sshd)*

Не настраивать сервер OpenSSH,

-d, **--debug** (*отладить*)

Включить ведение журнала отладки, когда требуется более подробный вывод,

-U, **--unattended** (*без запроса*)

Автоматическая установка, которая никогда не будет запрашивать,

для ввода пользователем.

Параметры системы сертификата

--external-ca

Генерировать CSR, который должен быть подписан внешним CA

--external_cert_file=*ФАЙЛ*

Файл, содержащий сертификат PKCS # 10

--external_ca_file= *ФАЙЛ*

Файл, содержащий PKCS # 10 внешней CA-цепи

--dirsrv_pkcs12= *ФАЙЛ*

Файл PKCS # 12, содержащий сертификат SSL сервера каталогов

***--http_pkcs12**= ФАЙЛ*

Файл PKCS # 12, содержащий сертификат SSL Apache Server

--dirsrv_pin=*DIRSRV_PIN*

Пароль файла PKCS # 12 сервера каталогов

--*http_pin*=*HTTP_PIN*

Пароль файла Apache Server PKCS # 12

--subject=*ПРЕДМЕТ*

База данных сертификата (по умолчанию O = REALM.NAME)

--selfsign

Настройте самозаверяющий экземпляр CA для выдачи сертификатов сервера вместо использования dogtag для сертификатов.

ПРЕДУПРЕЖДЕНИЕ. Использование этой опции ограничивает возможности управления сертификатами сервера. Пожалуйста, имейте в виду, что этот способ не меняется.

Опции (выбор) DNS

--setup-dns *(настройка DNS)*

Создайте зону DNS, если она еще не существует, и настройте DNS-сервер. Эта опция требует, чтобы вы либо указали по крайней мере один переадресатор DNS через параметр **--forwarder**, либо использовали параметр **--no-forwarders**.

Обратите внимание, что вы можете настроить DNS в любое время после установки первого сервера IPA, выполнив ipa-dns-install.

--forwarder=*IP_ADDRESS* (*IP адрес*)

Добавьте DNS-переадресацию в конфигурацию DNS. Вы можете использовать эту опцию несколько раз, чтобы указать больше пересылок, но по крайней мере один должен быть предоставлен, если не указана опция **--no-forwarders**.

--no-forwarders

Не добавляйте DNS-пересылок. Вместо этого будут использоваться корневые DNS-серверы.

--reverse-zone=*REVERSE_ZONE* (*обратная зона*)

Зона обратного использования DNS

--no-reverse *(без обратной зоны)*

Не создавать обратную зону DNS

--zonemgr *(зона mgr)*

Адрес электронной почты менеджера зоны DNS. По умолчанию hostmaster @ DOMAIN

--no-persistent-search *(нет постоянного поиска)*

Не включать механизм постоянного поиска для обновления списка зон DNS на сервере имен. Если постоянный поиск отключен, а параметр -zone-refresh не установлен на ненулевом значении, новые зоны не будут запускаться, пока сервер имен не будет перезагружен.

--zone-refresh=*ZONE_REFRESH* *(зона обновления)*

Если установлено ненулевое значение, механизм обновления постоянной зоны поиска будет отключен, а сервер имен будет использовать механизм опроса для загрузки новых зон DNS каждые секунды ZONE_REFRESH.

--no-host-dns *(нет хоста DNS)*

Не используйте DNS для поиска имени хоста во время установки

--no-dns-sshfp *(нет DNS sshfp)*

Нельзя автоматически создавать записи DNS SSHFP.

--no-serial-autoincrement *(нет последовательного автоматического увеличения)*

Не включайте функцию автоматического автообновления SOA. Последовательность SOA должна быть обновлена автоматически или другие функции DNS, такие как передача зоны, DNSSEC не будут работать должным образом. Для этой функции требуется постоянный механизм обновления зоны поиска.

Параметры удаления

--uninstall *(удаление, деинсталяция)*

Удалите существующую установку IPA

-U, **--unattended** *(без сопровождения*)

Автоматическая деинсталляция, которая никогда не будет

приглашение для ввода пользователем

Статус выхода

0, если установка (un) прошла успешно

1, если произошла ошибка

Интерактивная установка

```
# ipa-server-install --mkhomedir
```

Помимо аутентификации, IPA может управлять DNS-записями для хостов. Это может облегчить настройку и управление хостами.

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Далее нужно указать имя хоста сервера, доменное имя и пространство Kerberos.

```
Server host name [server.redosipa.ru]:
Please confirm the domain name [redosipa.ru]:
Please provide a realm name [REDOSIPA.RU]:
```

Затем создайте пароль для менеджера каталогов LDAP и пароль администратора IPA, который будет использоваться при аутентификации в IPA в качестве администратора.

Если нужно, добавляем ретранслятор службы имен (DNS relay). Этот шаг необязателен, и необходим в том случае, если у Вас предполагается использовать внешний сервер для обработки запросов службы имен DNS. Учитываете, что по-умолчанию, сервер IPA предполагает, что будет пользоваться собственным сервером имен, который развертывает локально.

```
Do you want to configure DNS forwarders? [yes]:
```

Выбирайте [yes] (да), в случае, если присутствует внешний ретранслятор службы имен, иначе, выбирайте [no] – нет. Далее впишите дополнительные реверс зоны, если они нужны.

```
Do you want to configure these servers as DNS forwarders?
```

Инициируем создание обратной зоны для службы имен.

```
Do you want to search for missing reverse zones? [yes]:
Do you want to create reverse zone for IP 192.168.1.123 [yes]:
Please specify the reverse zone name [1.168.192.in-addr.arpa.]:
```

и имя NetBIOS для домена IPA. По умолчанию он определяется на основе доменного имени DNS.

```
NetBIOS domain name:
```

Подтвердите конфигурацию. После этого запустится программа установки.

```
Continue to configure the system with these values? [no]: yes
```

Убедитесь, что сервер IPA работает:

```
kinit admin
ipa user-find admin
```

Установите оболочку по умолчанию для пользователей:

```
ipa config-mod --defaultshell=/usr/bin/bash
```

Подробную информацию о вводе хоста РЕД ОС в домен IPA см. в нашей инструкции «Ввод клиентских машин в домен IPA».

Настройка репликации IPA

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** ipa-4.8.10

Предварительная настройка сервера

Задайте хостнейм

Он должен быть в области домена IPA сервера. Например, если ваш домен example.ru, то хостнейм реплики может быть - rep1.example.ru

```
# hostnamectl set-hostname rep1.example.ru
```

Отредактируйте hosts

На уже созданном IPA сервере и на будущей реплике внесите в /etc/hosts адреса друг друга.

Открыть файл хостов можно в текстовом редакторе nano.

```
# nano /etc/hosts
10.81.1.181   ipa.example.ru
10.81.1.182   rep1.example.ru
```

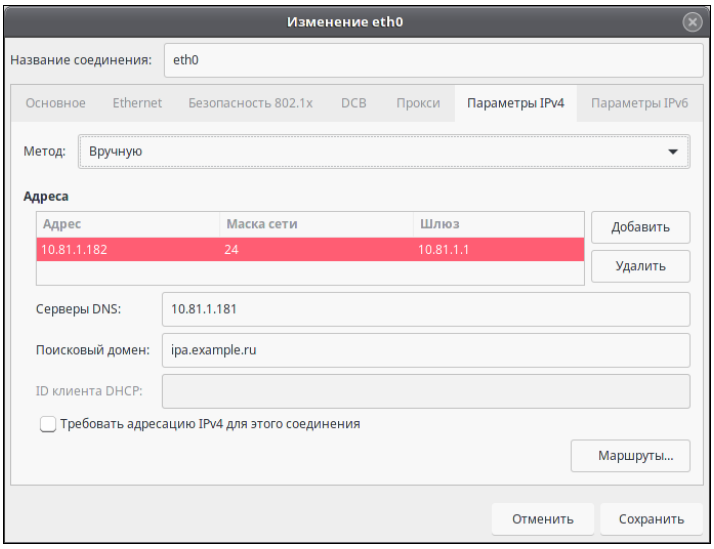
Настройте сетевой адаптер

ВАЖНО!

IP адрес сервера никогда не должен изменяться. Сделайте его статическим в вашей сети.

Пропишите настройки DNS, домена и поискового сервера по умолчанию в создаваемой реплике, укажите в качестве DNS ваш IPA сервер. Подробнее о настройке сети см. в нашей статье «Настройка сетевого адаптера».

Пример:



Перезагрузите сеть.

```
# systemctl restart NetworkManager
```

Проверка настроек

Проверьте заданные настройки в файле /etc/resolv.conf

```
# cat /etc/resolv.conf
search example.ru
domain example.ru
nameserver 10.81.1.181
```

Для корректной синхронизации реплики и сервера требуется на стороне сервера и реплики выполнить:

```
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
ntpdate time.yandex.ru
nano /etc/ntp.conf

добавьте строчку
server time.yandex.ru

закомментируйте строки:
#server ntp1.vniiftri.ru
#server ntp2.vniiftri.ru
#server ntp3.vniiftri.ru
#server ntp4.vniiftri.ru
```

Так же выполните команду:

```
# dig SRV _ldap._tcp.example.ru
```

в выводе нужно удостоверится, что SRV запись берется из DNS контроллера домена, в нашем случае с ipa.example.ru. Примерный вывод представлен ниже.

```
[root@localhost ~]# dig SRV _ldap._tcp.example.ru
; <<>> DiG 9.9.4-GosLinux-9.9.4-52.el7 <<>> SRV _ldap._tcp.example.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24642
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_ldap._tcp.ipa.murom.          IN      SRV
;; ANSWER SECTION:
_ldap._tcp.ipa.murom.   86400   IN      SRV     0 100 389 ipa.example.ru.
;; AUTHORITY SECTION:
example.ru.             86400   IN      NS      ipa.example.ru.
;; ADDITIONAL SECTION:
ipa.example.ru.         1200    IN      A       10.81.1.181
ipa.example.ru.         1200    IN      A       10.9.0.2
;; Query time: 1 msec
;; SERVER: 10.81.1.181#53(10.81.1.181)
;; WHEN: Вт дек 28 12:46:05 MSK 2017
;; MSG SIZE  rcvd: 112
```

Настройка синхронизации времени с помощью chronyd

После успешной синхронизации выполните

```
systemctl stop ntpd
systemctl disable ntpd
systemctl start chronyd
systemctl enable chronyd
```

Установка ipa-client

Установите ipa-client:

```
dnf install ipa-client ipa-server-dns
```

После установки, убедитесь что используется Java OpenJDK версии 8:

```
java -version
```

Если используется Java 11, то необходимо переключиться на 8-ую версию. Для этого выполните команды:

```
update-alternatives --config java
update-alternatives --config jre_openjdk
```

в каждой выберите нужную версию, указав ее порядковый номер. После чего нажмите Enter.

Настройте клиента.

Впишите в команду данные для вашей сети:

```
ipa-client-install -d --mkhomedir --enable-dns-updates
```

Скрипт установки должен автоматически найти настройки на ipa сервере, вывести их и спросить подтверждение для найденных параметров:

```
Continue to configure the system with these values? [no]:
```

Ответьте yes.

Затем введите имя администратора. Можно просто использовать администратора по умолчанию IPA, который был создан при установке сервера:

```
User authorized to enroll computers: admin
```

Введите пароль администратора IPA, который был установлен во время настройки сервера IPA.

После этого клиент IPA подготовит систему.

Если установка прошла успешно, в конце вывода вы увидите:

```
Client configuration complete.
The ipa-client-install command was successful
```

Далее нужно создать обратный адрес для реплики на DNS сервере основного сервера. Зайдите в веб управление и перейдите в Network Services > DNS > Зоны DNS. Выберете в таблице запись вашего домена, например org.lan. и в открывшемся списке откройте запись вашей реплики, например ipareplica0. Нажмите на ip адрес в поле A записи и на ссылку в открывшемся окне. Обратная запись создана.

После этого хост должен появиться в веб-интерфейсе.

Настройка обратной зоны DNS на сервере IPA

Если реплика находится в другой подсети, создайте для нее обратную зону и добавьте в неё PTR запись для реплики.

Если реплика находится в одной подсети с IPA сервером, достаточно просто создать PTR запись для реплики.

Настройка репликации

Перейдите к настройке репликации

Выполните:

```
ipa-replica-install
```

Введите пароль администратора:

```
Password for admin@EXAMPLE.RU:
```

Дождитесь установки и настройки репликации.

Установка CA сервера

Перейдите к установке CA сервера:

```
ipa-ca-install
```

Введите Directory Manager password:

```
Directory Manager (existing master) password:
```

После завершения зайтите на любой веб-интерфейс и проверьте топологию**:**

Настройте DNS-сервер на реплике

Выполните команду:

```
ipa-dns-install
```

Разрешите форвардеров.

У вас автоматически возьмутся днс сервера из файла /etc/resolv.conf, если там только один основной сервер ipa, укажите дополнительно основной DNS сервер в сети.

```
Enter an IP address for a DNS forwarder, or press Enter to skip:
```

Если вдруг ваша реплика находится в другом регионе, можно указать другие форвардеры.

Мониторинг запущенных процессов

Необходимо мониторить запущенные процессы, открытые порты и самое главное мониторить срок действия корневого CA-сертификата. Проверить сертификат можно в веб управлении IPA сервера.

Вывод клиента из домена Ipa

Для вывода клиента из домена Ipa выполните команду:

```
ipa-client-install --uninstall
```

Настройка резервного копирования домена IPA

Резервное копирование полного сервера IPA
Резервная копия только для данных
Создание резервной копии
Автоматизация резервного копирования
Восстановление резервной копии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер минимальный
- **Версия ПО:** ipa-server-4.8.10-12

IPA предлагает два варианта резервного копирования: резервное копирование полного сервера **IPA** и резервная копия только для данных.

Резервное копирование полного сервера IPA

Полное резервное копирование создает копию всех файлов сервера **IPA**, а также данных LDAP, что делает его автономной резервной копией. **IPA** затрагивает сотни файлов: файлы, сочетание целых каталогов и определенных файлов, таких как файлы конфигурации или файлы журналов. Они относятся непосредственно к **IPA** или к различным его службам.

Поскольку полносерверная резервная копия является копией необработанных файлов, она выполняется в автономном режиме. Скрипт, выполняющий полное серверное резервное копирование, останавливает все службы **IPA**, чтобы обеспечить безопасный ход процесса резервного копирования.

Резервная копия только для данных

Резервная копия только для данных создает копию данных **LDAP** и журнала изменений. Этот процесс поддерживает **IPA-REALM** и может также создавать резервные копии нескольких серверных частей или только одну; серверная часть включает **PA** и **CA Dogtag**. Этот тип резервного копирования также поддерживает запись содержимого **LDAP**, хранящегося в **LDIF**. Резервная копия данных может выполняться как в режиме онлайн, так и в автономном режиме.

Создание резервной копии

По умолчанию **IdM** хранит созданные резервные копии в каталоге **/var/lib/ipa/backup/**.

Для полного резервного копирования сервера **IPA** выполните команду:

```
ipa-backup
```

Например:

```
ipa-backup

Preparing backup on server.redosipa.ru
Local roles match globally used roles, proceeding.
Stopping IPA services
Backing up ipaca in REDOSIPA-RU to LDIF
Packing up userRoot in REDOSIPA-RU to LDIF
Backing up REDOSIPA-RU
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2823-87-04-16-35-31
The ipa-backup command was successful
```

Для резервной копии только данных без остановки сервера выполните:

```
ipa-backup --data --online
```

где:

- **--data** — выполняет резервное копирование только данных,
- **--online** — выполняет онлайн-резервное копирование этот параметр доступен только с резервными копиями только для данных.

Например:

```
ipa-backup --data --online

Preparing backup on server.redosipa.ru
Local roles match globally used roles, proceeding.
Backing up ipaca in REDOSIPA-RU to LDIF
Waiting for LDIF to finish
Backing up userRoot in REDOSIPA-RU to LDIF
Waiting for LDIF to finish
Backing up REDOSIPA-RU
Waiting for BAK to finish
Backed up to /var/lib/ipa/backup/ipa-data-2823-87-84-16-48-44
The ipa-backup command was successful
```

Автоматизация резервного копирования

Для автоматизации можно использовать **cron**. Отредактируйте файл **/etc/crontab**. Например для создания ежедневной копии только данных в 23.30 впишите следующую строку.

```
30 23 * * * root ipa-backup --data --online
```

Восстановление резервной копии

Для восстановления резервной копии необходимо, чтобы на ПК уже был установлен и настроен **IPA**-сервер по нашей инструкции «Установка сервера IPA».

Далее перейдите в каталог с резервной копией IPA-сервера и выполните команду восстановления:

```
ipa-restore <имя_РК>
```

Например:

```
cd /var/lib/ipa/backup
ipa-restore ipa-full-2023-07-04-21-40-49

SystemWide CA database updated.
Restoring from userRoot in REDOSIPA-RU
Restoring from ipaca in REDOSIPA-RU
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restarting IPA services
Restoring umask to 18
The ipa-restore command was successful
```

Создание доверительных отношений IPA и MSAD

Для примера создания доверительных отношений будут использоваться следующие данные:
Домен IPA - **redos.ipa**
Сервер IPA - **dc1.redos.ipa** - **10.81.1.67**
Домен MS AD - **win.redos**
Сервер MS AD - **dc.win.redos** - **10.81.1.196**

1 Настройки на IPA

1.1 Отключение проверки DNSSEC

Для этого в файле **/etc/named/ipa-options-ext.conf** приведите параметр к виду:

```
dnssec-validation no;
```

Перезагрузить сервер или службу IPA командой:

```
# systemctl restart ipa
```

Примечание.

На время настройки сервиса переведите **selinux** в режим уведомлений. Для этого измените содержимое конфигурационного файла:

```
nano /etc/selinux/config
```

Заменив текст SELINUX=enforcing на SELINUX=permissive

Выполните:

```
setenforce 0
```

Более подробно см.ссылку.

Не забудьте включить selinux после завершения настройки.

1.2 Отредактируйте /etc/hosts

Впишите туда адрес сервера MS AD и его хостнейм.

```
10.81.1.196 dc.win.redos dc
```

1.3 Настройка времени

На всех серверах и рабочих станциях время должно быть синхронизировано.

```
nano /etc/chrony.conf
```

Удалите все остальные строки, начинающиеся на **server**.

Вставьте следующие строки в файл:

```
server ntp1.stratum2.ru iburst
server ntp2.stratum2.ru iburst
server ntp3.stratum2.ru iburst
```

Укажите подсеть:

```
allow 10.81.1.0/24
```

Перезапустите сервис chronyd:

```
systemctl restart chronyd
```

Проверка:

```
chronyc sources
```

1.4 Настройка зоны перенаправления на IPA сервере

На сервере IPA добавьте условный сервер пересылки (зону пересылки dns) для домена Windows AD:

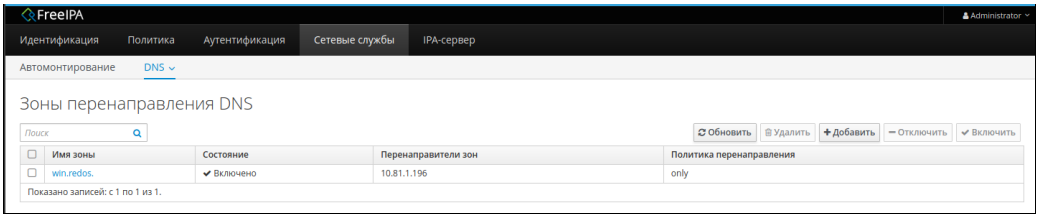
```
# kinit admin
# ipa dnsforwardzone-add win.redos --forwarder=10.81.1.196 --forward-policy=only
```

здесь **10.81.1.196** - windows server;

win.redos - имя домена windows.

С помощью web GUI в параметрах DNS-сервера IPA укажите ip-адрес перенаправителя, им должен быть сервер Windows.

У вас должно получится примерно следующее:



Проверьте, резолвится ли сервер MS AD. Воспользуйтесь командой:

```
# nslookup dc.win.redos
Server:      10.81.1.67
Address:     10.81.1.67#53
Non-authoritative answer:
Name:  dc.win.redos
Address: 10.81.1.196
```

Вам должен вернуться адрес вашего MS AD.

Так же проверьте SRV записи.

```
# dig SRV _ldap._tcp.redos.ipa

# dig SRV _ldap._tcp.win.redos
```

1.5 Переустановка samba-dc

Убедитесь, что установлена актуальная версия samba:

```
dnf update samba
```

Для корректной работы IPA сервера и MS AD требуется версия samba с поддержкой MIT Kerberos. Для ее установки выполните команду:

```
dnf dg samba
```

После этого перезапустите сервис **ipa**:

```
systemctl restart ipa.service
```

Проверьте **Samba** на наличие **MIT Kerberos**:

```
smbd -b | grep HAVE_KADM5SRV_MIT
```

Должны получить вывод:

```
HAVE_KADM5SRV_MIT
```

Для исключения пакетов samba из обновлений, в файл **/etc/dnf/dnf.conf** добавьте строку:

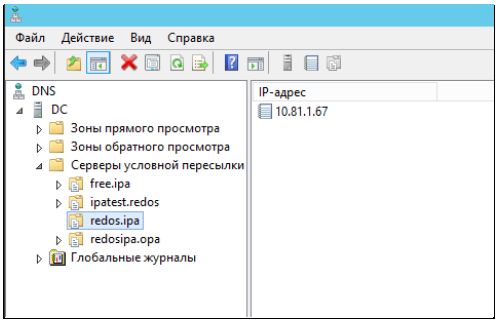
```
exclude=libsmbclient libwbclient python3-samba python3-samba-dc samba*
```

2 Настройка DNS на сервере Windows

Вам нужно сделать так, что бы доменом IPA сервера управлял DNS IPA.

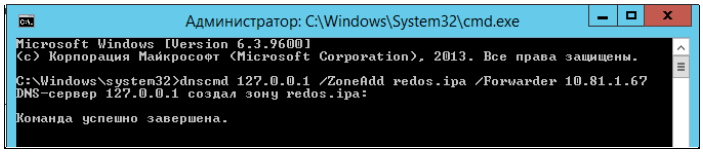
В случае разных доменов создайте сервер условной пересылки.

1. Откройте Диспетчер DNS и перейдите на вкладку «**Серверы условной пересылки**».
2. В контекстном меню выберите «**Создать сервер условной пересылки**».
3. Впишите DNS домен сервера IPA и его ip адрес.
4. Выберите «**Все DNS серверы в этом лесу**» и нажмите **OK**.
5. Ниже приведен примерный результат:

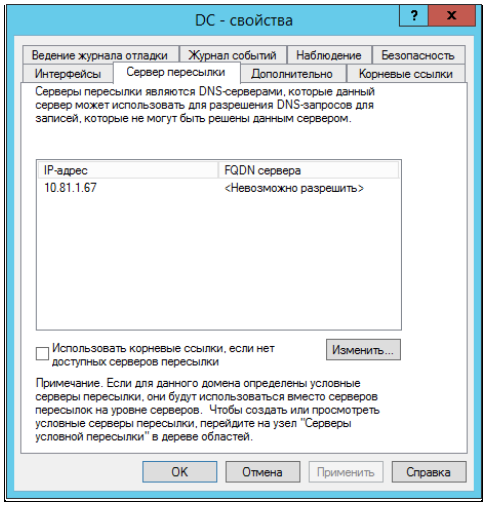


Также это можно сделать с помощью команды:

```
dnscmd 127.0.0.1 /ZoneAdd redos.ipa /Forwarder 10.81.1.67
```



Кроме этого необходимо добавить глобальный "**Сервер пересылки**" в свойствах dns сервера windows. Для этого в диспетчере DNS нажмите правой клавиши мыши на сервере DNS (SERV) и в выпадающем меню выберите "**Свойства**", перейдите на вкладку "**Сервер пересылки**", нажмите на кнопку "**Изменить**" и в открывшемся окне введите ip-адрес сервера IPA.



Также это можно сделать с помощью команды:

```
dnscmd 127.0.0.1 /ResetForwarders 10.81.1.67 /Slave
```

Проверьте конфигурацию DNS на сервере Windows.

Чтобы убедиться, что сервер AD может корректно видеть IPA, проверьте, правильно ли разрешены записи SRV.

```
C:\> nslookup
> set type=srv
> _ldap._tcp.win.redos
> _ldap._tcp.redos.ipa
> quit
```

3 Добавьте доверительные отношения между доменами

3.1 Сконфигурируйте сервер IPA для доверительных отношений с AD.

```
# ipa-adtrust-install
```

Отвечайте на все вопросы скрипта положительно (yes)

При доступе пользователей AD к IPA-клиентам обязательно запустите ipa-adtrust-install на каждом IPA-сервере, к которому будут подключаться клиенты IPA.

3.2 Добавьте доверительные отношения.

```
#ipa trust-add --type=ad win.redos --range-type ipa-ad-trust --admin admin --password --two-way=TRUE
```

На этом этапе будет установлено двустороннее доверие между **FreeIPA** и **Active Directory**. Для создания таких отношений используется опция **--two-way=true**.

При появлении запроса введите пароль администратора.

```
Пароль администратора домена Active Directory:
----------------------------------------------------------------------------
Добавлено отношение доверия Active Directory для области (realm) "win.redos"
----------------------------------------------------------------------------
Имя области (realm): win.redos
Имя домена NetBIOS: WIN
Идентификатор безопасности домена: ***
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Установлено и проверено
```

ВАЖНО!

Учетная запись пользователя, используемая при создании доверия (аргумент опции --admin в командеipa trust-add), должна быть членом группы Domain Admins. Имя учетной записи должно быть на английском языке.

3.3 После того, как установлена доверительное отношение на стороне AD, необходимо получить список доверенных доменов леса со стороны AD. Это делается с помощью следующей команды:

```
# ipa trust-fetch-domains "win.redos"
```

При успехе IPA получит информацию о доверенных доменах и создаст для них все необходимые идентификаторы.

Используйте «trustdomain-find», чтобы просмотреть список доверенных доменов из доверенного леса:

```
# ipa trustdomain-find "win.redos"
```

3.4 Создать внешнюю группу, сопоставленную с группой **posix freeipa**: это позволит предоставить право внешней группе. Затем **active directory** группа администраторов домена сопоставляется с группой **ad_admins**, которая принадлежит пользователю **admins**. В этом случае каждый администратор домена windows имеет некоторый грант администратора **freeipa**:

```
ipa group-add --desc='ad domain external map' ad_admins_external --external
ipa group-add --desc='ad domain users' ad_admins
ipa group-add-member ad_admins_external --external 'WIN.REDOS\Администраторы домена'
ipa group-add-member ad_admins --groups ad_admins_external
```

Ввод клиентских машин в домен IPA

Предварительная настройка РЕД ОС
Присоединение к домену IPA с помощью утилиты join-to-domain
Ручная установка IPA клиента и ввод в домен

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ipa-client-4.8.10-12

Предварительная настройка РЕД ОС

Задайте имя компьютера

Он должен быть в области домена IPA сервера. Например, если ваш домен example.ru, то хостнейм клиента должен быть - client.example.ru.

```
# hostnamectl set-hostname client.example.ru
```

Настройте DNS

Пропишите настройки DNS и домен в создаваемом клиенте, укажите в качестве DNS ваш IPA сервер и опцию, для того, что бы по DHCP не принимался DNS адрес.

Для этого, используйте утилиту **«Сетевые соединения»**, расположенную в **«Меню» → «Параметры» → «Сетевые соединения»** в графическом окружении **Cinnamon** или **«Система» → «Параметры» → «Сетевые соединения»** в графическом окружении **Mate**. Выберите ваше активное подключение, нажмите кнопку **«Изменить»,** перейдите на вкладку **«Параметры IPv4»**, поменяйте **«Метод»** н а **«Вручную»**, в поле «**Дополнительные серверы DNS**» напишите адрес **IPA-сервера** (например 172.16.0.11), в поле **«Дополнительные поисковые домены»** введите поисковый домен (например example.ru), нажмите применить и переподключитесь к сети.

Проверка настроек

Проверьте заданные настройки в файле /etc/resolv.conf:

```
cat /etc/resolv.conf

search  example.ru
nameserver 172.16.0.11
```

Так же выполните команду:

```
dig SRV _ldap._tcp. example.ru
```

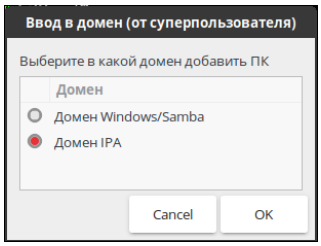
в выводе нужно удостоверится, что SRV запись берется из DNS контроллера домена Примерный вывод представлен ниже.

```
dig SRV _ldap._tcp. example.ru

; <<>> DiG 9.11.4-P2-RedOS-9.11.4-5.P2.el7 <<>> SRV _ldap._tcp. example.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24642
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_ldap._tcp.ipa.murom.          IN      SRV
;; ANSWER SECTION:
_ldap._tcp.ipa.example.   86400   IN      SRV     0 100 389 ipa.example.ru.
;; AUTHORITY SECTION:
example.ru.             86400   IN      NS
ipa.example.ru.
;; ADDITIONAL SECTION:
ipa.example.ru.         1200    IN      A       172.16.0.11
;; Query time: 1 msec
```

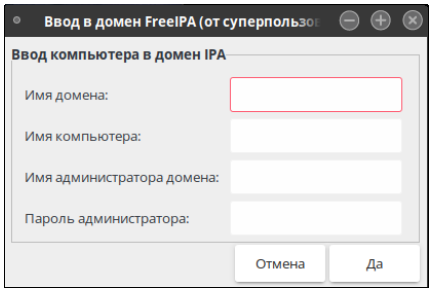
```
;; SERVER: 172.16.0.11#53(172.16.0.11)
;; WHEN: Ср май 06 10:47:20 MSK 2020
;; MSG SIZE  rcvd: 112
```

Присоединение к домену IPA с помощью утилиты join-to-domain

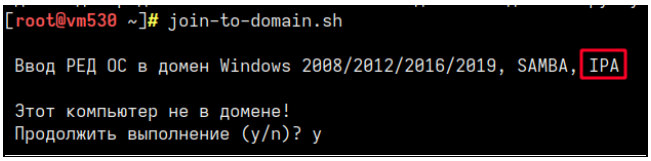
Откройте главное меню - «**Системные**» - «**Ввод ПК в домен**». Выберите «**Домен IPA**».



Заполните все поля:



Кроме графического варианта утилитой **join-to-domain** можно воспользоваться в терминале.



На следующем шаге нужно выбрать способ ввода, а именно "**2. Ввод РЕД ОС в домен IPA**"

Далее введите все предлагаемые значения. По окончании ПК будет введен в домен IPA.

Ручная установка IPA клиента и ввод в домен

```
dnf install ipa-client
```

Присоединение клиента к домену IPA

Впишите в команду данные для вашей сети:

```
ipa-client-install --mkhomedir --enable-dns-updates
```

Скрипт установки должен автоматически найти настройки на ipa сервере, вывести их и спросить подтверждение для найденных параметров:

```
Continue to configure the system with these values? [no]:
```

Ответьте **yes**.

Затем введите имя администратора. Можно просто использовать администратора по умолчанию IPA, который был создан при установке сервера:

```
User authorized to enroll computers: admin
```

Введите пароль администратора IPA, который был установлен во время настройки сервера IPA.

После этого клиент IPA подготовит систему.

Если установка прошла успешно, в конце вывода вы увидите:

```
Client configuration complete.
The ipa-client-install command was successful
```

После этого хост должен появиться в веб-интерфейсе ipa сервера.

Интеграция файлового сервера SAMBA с IPA

Установка необходимых пакетов на сервере SAMBA
Настройка серверов IPA и Samba
Настройка сетевого каталога на сервере Samba

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: ipa-client-4.10.3-6, samba-4.19.2-2h

Установка необходимых пакетов на сервере SAMBA

Для установки пакетов **samba** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ipa-client sssd-common samba samba-client ipa-client-samba
```

Установите имя хоста samba-сервера:

```
hostnamectl set-hostname samba.redosipa.ru
```

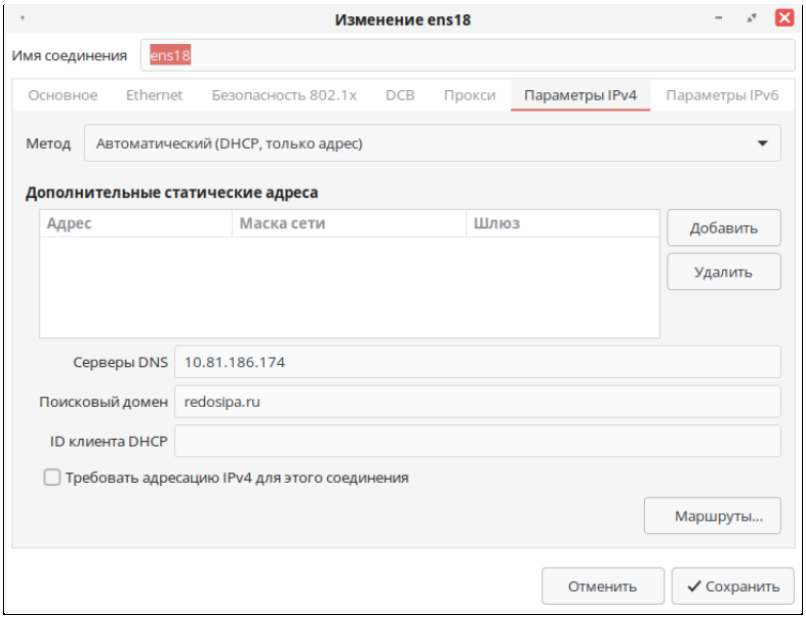
Добавьте запись в **/etc/hosts**, по какому IP обращаться к домену IPA, например:

```
10.81.186.174 server.redosipa.ru
```

Отключите службу:

```
systemctl disable --now systemd-timesyncd
```

В сетевых настройках укажите поисковый DNS IPA-сервера, например:



Присоедините файловый сервер к домену IPA:

```
join-to-domain.sh
```

Выполните автоматическую конфигурацию системных служб на сервере **samba** для работы в домене IPA:

```
authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

Настройка серверов IPA и Samba

Для правильного распределения DNS выполните следующие команды на сервере IPA:

```
kinit admin
ipa dnsrecord-add redosipa.ru --a-rec=samba --a-ip-address=10.81.186.124
```

Запустите настройку домена для обработки классов и атрибутов объектов, специфичных для **Samba**:

```
ipa-adtrust-install --add-sids
reboot
```

На сервере **samba** выполните ipa-client-samba, который создаст **cifs** и отредактирует **/etc/samba/smb.conf** для работы *samba* с **ipa**:

```
ipa-client-samba
```

Отредактируйте в файле **/etc/samba/smb.conf** значение netbios name, указав рабочую группу домена, в данном случае **smb.conf** будет выглядеть следующим образом:

```
...
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 ...
```

Далее отредактируйте секции по примеру из **smb.conf**:

```
[global]
 max smbd processes = 1000
 dedicated keytab file = FILE:/etc/samba/samba.keytab
 kerberos method = dedicated keytab
 log file = /var/log/samba/log.%m
 log level = 1
 server role = member server
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 idmap config * : range = 0 - 0
 idmap config * : backend = tdb


 idmap config REDOSIPA : range = 14000000 - 14199999
 idmap config REDOSIPA : backend = sss

 security = ads
 printing = cups
 printcap name = cups
 load printers = yes
 cups options = raw

 [homes]
 read only = no
 comment = Home Directories
 valid users = %S, %D%w%S
 browseable = No
 read only = No
 inherit acls = Yes
```

```
[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775
```

Создайте структуру ролей и привилегий для **samba**. Действия выполняются на контроллере домена **ipa**:

```
ipa permission-add "CIFS server can read user passwords" --attrs={ipaNTHash,ipaNTSecurityIdentifier} --type=user --right=
{read,search,compare} --bindtype=permission
ipa privilege-add "CIFS server privilege"
ipa privilege-add-permission "CIFS server privilege" --permission="CIFS server can read user passwords"
ipa role-add "CIFS server"
ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
ipa role-add-member "CIFS server" --services=cifs/samba.redosipa.ru
```

На samba-сервере внесите изменения в **/etc/krb5.conf**:

```
sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

Получите тикет и создайте **keytab**:

```
kinit admin
ipa-getkeytab -s server.redosipa.ru -p cifs/samba.redosipa.ru -k /etc/samba/samba.keytab
reboot
```

Настройка сетевого каталога на сервере Samba

На samba-сервере создайте каталог:

```
mkdir -p /share/
```

Назначьте права на созданный каталог:

```
chown -R :users /share
chmod -R 777 /share
setfacl -m default:user:"admin":rwx /share
setfacl -R -m default:user:"admin":rwx /share
```

Затем настройте метки SELinux:

```
semanage fcontext -a -t samba_share_t /share/
restorecon -R -v /share/
```

На контроллере домена **IPA** получите SID:

```
net getdomainsid
```

На файловом сервере **samba** настройте идентификатор безопасности (введите SID, полученный ранее):

```
 net setdomainsid <SID>
```

На сервере **samba** выполните:

```
net -s /dev/null groupmap add sid=S-1-5-32-546 unixgroup=nobody type=builtin
```

В **/etc/samba/smb.conf** укажите настройки для каталога:

```
[share]
 path = /share
 writable = yes
 browsable=yes
 valid users = admin
 read list = admin
 write list = admin
 guest ok = no
 inherit acls = Yes
 create mask = 0660
 directory mask = 0770
```

Добавьте в автозапуск службы **samba** и **winbind**, перезагрузите сервер **samba**:

```
systemctl enable smb winbind --now
reboot
```

Для проверки доступности сетевого каталога на сервере **samba** необходимо получить тикет (если он отсутствует) и выполнить команду подключения к сетевому каталогу:

```
kinit admin
smbclient //samba.redosipa.ru/share -N --use-kerberos=required
```

В случае, если все настроено верно, появится следующее сообщение:

```
Try "help" to get a list of possible commands.
 smb: \>
```

Основные понятия

Общие сведения о Samba

Данный продукт представляет собой комплект серверного и клиентского программного обеспечения для осуществления связи UNIX-машин с сетями **Microsoft** и **LanManager**, которые сами по себе представляют собой подклассы сетей **SMB**.

Samba использует протокол «**NetBIOS over TCP/IP**», что позволяет ей успешно взаимодействовать с такими реализациями **SMB**, как входящие в OS/2 3-4, Windows 9X-ME, NT3.5-4/2000/XP/Vista/7, UNIX-системами с Samba и, возможно, другими подобными. Samba не может работать без использования **TCP/IP** (на NetBIOS и NetBEUI). Об этом не стоит забывать при проектировании сетей.

Для работы в сетях SMB необходимы:

- клиент;
- сервер;
- средства администрирования.

Все это есть в пакетах **samba-client**, **samba-client-cups**, **samba-common**, **samba, samba-swat**, входящих в состав дистрибутива.

При использовании **SMB** доступны следующие ресурсы:

- сетевые диски;
- прямые пути к дискам;
- принтеры;
- доменная авторизация и управление.

Первые три пункта поддерживаются **Samba** в полном объеме, последний - частично, но это направление стремительно развивается и весьма полно реализовано в **Samba**, описанной ниже.

Также доступен весьма объемный комплект документации в пакете **samba-doc**; большинство ссылок данного раздела будут указывать именно на содержимое этого пакета.

Краткий обзор каталогов и файлов

Все файлы конфигурации и авторизации **Samba** расположены в каталоге **/etc/samba** и его подкаталогах. Рассмотрим их несколько подробнее.

Файл конфигурации	**Описание файла конфигурации**
MACHINE.SID	Системный идентификатор машины, формируется автоматически при старте сервера и предназначен для идентификации компьютера в домене сети Microsoft.
codepages/	Каталог, содержащий файлы с таблицами перекодировки.
Lmhosts	То же, что и **/etc/hosts**, но он предназначен для преобразования **IP<=>NetBIOS**. Как правило, содержит только одну запись: **127.1.0.1 localhost**, но туда можно заносить хосты из других подсетей (когда по ряду причин невозможно надежно провести преобразование **IP<=>NetBIOS** ни широковещательными запросами, ни с использованием **WINS**) или наоборот - ключевые сервера собственного домена.
secrets.tdb	Ключевой файл для идентификации машины в домене сети Microsoft. С точки зрения безопасности имеет ту же ценность, что и файлы **/etc/tcb/*/shadow** - а потому права доступа должны быть **root.root 0600**.
smb.conf	Основной конфигурационный файл **Samba**. Он нужен не только серверной части, но и всем остальным компонентам этой системы.
Smbpasswd	Аналог **/etc/passwd** и **/etc/tcb/*/shadow** - файл пользователей сервера **Samba** с паролями. С точки зрения безопасности имеет ту же ценность, что и **/etc/tcb/*/shadow** - а потому права доступа должны быть **root.root 0600**. Соответствие пользователей **Samba** и системных производится на основе общего **UID**; данный файл используется **Samba** при отсутствии данных о пользователе на **PDC** или при отсутствии самого **PDC**.
Smbusers	Файл соответствий имен сетевых и локальных пользователей **SMB**; это удобный метод для организации административных и гостевых входов на сервер. Соответствие пользователей **Samba** и системных производится на основе символьных имен.
/var/log/samba/*	Лог-файлы серверной части **Samba**. Из них **log.smbd**, **log.nmbd**, **log.winbind** - журналы соответствующих процессов, а все прочие - логи взаимодействия сервера с отдельными клиентскими хостами в формате именования по умолчанию **log.<Client_NetBIOS_NAME>**. При превышении заданного в smb.conf предела производится ротация логов и формируются файлы ***.old**.
/var/spool/samba	Каталог динамического спулинга печати сервера **Samba**. На не сильно загруженных серверах печати он обычно пуст; наличие там множества файлов в то время, когда ни один из клиентов не печатает - явный признак сбоев сервера печати.
/var/cache/samba/*	Файлы (как правило, двоичные базы данных), формируемые в процессе работы различных компонентов **Samba**.

Наиболее примечательны:

Файл конфигурации	Описание файла конфигурации
browse.dat и wins.dat	текстовые файлы, их названия говорят сами за себя;
winbindd*.tdb	базы данных доменных пользователей, формируемых **winbind**. Время от времени их необходимо архивировать: если при апгрейде, «переезде» или переустановке сервера **winbind** сгенерирует эти файлы с нуля, то соответствия системных и доменных символьных и числовых имен изменятся, и права доступа на восстановленные из архива файлы окажутся заведомо перепутанными. Поэтому настоятельно рекомендуется архивировать файлы **/var/cache/samba/winbindd*.tdb**;
/var/lib/samba/	служебные каталоги для администратора сервера.

Список выполняемых файлов **Samba** можно получить командой:

```
rpm -qa | grep samba | xargs rpm -ql | grep bin/
```

и подробно ознакомиться с каждым, прочитав соответствующие разделы документации.

Далее описаны самые важные и наиболее часто используемые компоненты.

Серверные компоненты:

Компонента	Описание компоненты
/usr/sbin/nmbd	сервер преобразования имен и адресов;
/usr/sbin/smbd	файловый сервер;
/usr/sbin/winbindd	сервер импорта пользователей и групп с PDC;
/usr/sbin/swat	средство конфигурирования Samba с web-интерфейсом;
/etc/init.d/smb и /etc/init.d/winbind	управляющие скрипты инициализации сервисов.

Следует отметить, что у скрипта **/etc/init.d/smb** есть два режима рестарта - **restart** и **reload**, которые радикально отличаются следующими особенностями.

restart производит полный рестарт процессов **smbd** и **nmbd** со сбросом текущих соединений. Как правило, клиенты сами производят автоматический реконнект к ресурсам, однако если в момент рестарта были открыты файлы, то возможны проблемы с клиентскими приложениями (например, MS Office и 1C).

reload заставляет **smbd** и **nmbd** только лишь перечитывать файлы конфигурации без рестарта и сброса соединений. При этом старые соединения продолжают существовать по старым правилам, а ко всем новым соединениям будут применены уже новые правила на основании файлов конфигурации.

Клиентские компоненты:

Компонента	Описание компоненты
/usr/bin/smbclient	интерактивное приложение для просмотра сетевых ресурсов;
/sbin/mount.smb, /sbin/mount.smbfs, /usr/bin/smbumount, /usr/sbin/smbmnt, /usr/bin/smbmount	средства монтирования/размонтирования сетевых файловых систем.

Утилиты:

Утилита	Описание утилиты
/usr/bin/smbpasswd	Управление пользователями и подключением к домену;
/usr/bin/wbinfo	Отображение списка пользователей, импортированных **winbindd**;
/usr/bin/testparm	Проверка синтаксиса конфигурационных файлов;
/usr/bin/smbstatus	Отображение статуса процессов **smbd** и **nmbd**;
/usr/bin/nmblookup	Программа разрешения имен **WINS** (аналог **nslookup** для DNS).

Настройка

В большинстве случаев настройка **Samba** заключается в редактировании основного конфигурационного файла **/etc/samba/smb.conf** и управлении пользователями с помощью **smbpasswd**.

Обычный сервер:

Под таковым понимается компьютер, предоставляющий в сеть файловые ресурсы. Фактически это простейший независимый файловый сервер, имеющий собственную базу авторизации пользователей.

Для того чтобы создать такой сервер, необходимо лишь немного подправить стандартный конфигурационный файл **smb.conf** (подставить требуемые имя рабочей группы и имена ресурсов) и создать учетные записи пользователей, как описано ниже, а также учесть рекомендации по безопасности, изложенные в конце раздела.

Вот основные записи в **smb.conf**, которые создадут нам «обычный сервер».

```
[global]
```

Секция [**global**] определяет общие настройки серверной части **Samba** в целом для всех ресурсов.

Имя рабочей группы:

```
OFFICE workgroup = OFFICE
```

Уровень определения прав доступа на уровне пользователей:

```
security = user
```

Приоритет данного сервера среди других компьютеров рабочей группы: определяет, кто именно будет главной машиной, отвечающей за отображение ресурсов сети.

Для сравнения, у **Win9X os level = 34**, а у **NT4 os level = 64**.

```
os level = 65
```

Очевидно, что раз нет домена - нет и мастера.

```
domain master = no
```

Не стоит становиться сервером паролей для окрестных машин.

```
domain logons = no
```

Обычно в простейшей сети **WINS** не нужен, мы его отключаем и у себя тоже.

```
wins support = no
```

Далее надо определить, какие именно каталоги предоставим в сеть. Для каждого ресурса существует отдельная секция.

Самый простейший вариант для обычных ресурсов - обычный каталог с именем **public**:

Имя ресурса, видимое в сети

```
[public]
```

Комментарий, видимый в сети как комментарий к ресурсу:

```
comment = Public Stuff
```

Путь к каталогу ресурса:

```
path = /home/samba/public
```

Отметка о доступе на чтение всем авторизованным пользователям (в том числе и гостевым, если они определены):

```
public = yes
```

Запрет работы на запись всем пользователям:

```
writable = no
```

Разрешение работы на запись всем пользователям, входящим в системную группу **staff**:

```
write list = @staff
```

Подобным образом можно создать различные сетевые ресурсы сервера с различными правами доступа.

Поскольку **Samba** исполняется не в **chroot**, внутри ресурсов можно использовать любые символические ссылки на расположенные локально и в сети (NFS, SMB, Coda и т.д.) файловые обьекты, что очень удобно в плане администрирования системы.

Особые ресурсы - например, домашние каталоги пользователей:

имя ресурса, которое автоматически будет заменено именем домашнего каталога пользователя, под которым подключился клиент и именно название его домашнего каталога будет отображено в сети как имя ресурса. Для получения доступа к этому ресурсу клиент должен предоставить серверу соответствующие имя и пароль, все прочие пользователи к этому ресурсу доступа не имеют вовсе.

```
[homes]
```

Комментарий, видимый в сети как комментарий к ресурсу:

```
comment = Home Directories
```

Признак невидимости - данный ресурс виден в сети только тому пользователю, который является его владельцем. К этому ресурсу можно обратиться непосредственно задав его имя, но в браузинге сети он будет виден только владельцу:

```
browseable = no
```

Разрешение на запись:

```
writable = yes
```

Принтеры:

Имя ресурса, которое будет видно в сети. Кроме него, в сети будут также видны и локальные принтеры под теми же именами, что и в системе по команде **lpq**.

```
[printers]
```

Комментарий, который игнорируется:

```
comment = All Printers
```

Путь к каталогу, в котором располагается спул принтеров, предоставляемых в сеть через **Samba**:

```
path = /var/spool/samba
```

Невидимость ресурса в браузинге, он подменяется системным ресурсом:

```
browseable = no
```

Разрешение на печать для гостевого захода:

```
guest ok = yes
```

Запрещение на запись, поскольку в спул пишет сама **Samba**, а не пользователь.

```
writable = no
```

Признак того, что это именно принтер, а не файловый ресурс:

```
printable = yes
```

Маска для создания файлов заданий на печать:

```
create mode = 0700
```

Команды, выполняемые **Samba** для того, чтобы напечатать документ.

Использование драйвера клиента, применяется для не-UNIX клиентов.

```
print command = lpr-cups -P %p -o raw %s -r
```

Использование драйвера **CUPS** на стороне сервера (на стороне клиентов используется generic **PostScript** драйвер):

```
; print command = lpr-cups -P %p %s
```

Следующие команды являются стандартными при установке **printing=cups**, их можно изменить в случае необходимости.

```
lpq command = lpq -P %p lprm command = cancel %p-%j
```

Сервер в составе существующего домена NT

Подключите вновь созданную машину **Samba** с именем **COMP** к существующему домену **DOM**, администратором которого является пользователь **Administrator** и **PDC** этого домена реализован на другом компьютере.

Первым делом необходимо убедиться, что машины с таким же именем, как и та, которую вы собираетесь подключить, в домене еще нет. В противном случае эту машину необходимо удалить из состава домена средствами самого **PDC** или выбрать другое имя.

На машине **COMP** в **/etc/samba/smb.conf** необходимо внести следующие изменения:

[global]

```
workgroup = DOM
netbios name = COMP
security = domain
password server = *
allow trusted domains = yes
nt acl support = yes
```

После чего необходимо остановить Samba-сервер, если он работает, командой:

```
service smb stop
```

Теперь необходимо послать запрос на **PDC** с целью авторизации нового члена домена с помощью следующей команды:

```
smbpasswd -j DOM -r DOMPDC -U Administrator
```

и в ответ на запрос ввести пароль пользователя **Administrator** - тот самый, с которым этот пользователь зарегистрирован в домене.

Если получено сообщение:

```
Joined domain DOM.
```

все работает; иначе в **smb.conf** надо написать:

```
[global] log level = 4,
```

повторить последнюю команду и по подробным логам разбираться, что не так. При таком уровне **log level** в **log.smbd** содержится подробный отчет об обмене с **PDC**. Вполне возможно, что были допущены ошибки в написании имен или ошибочно введен пароль; также возможны какие-либо неполадки на стороне **PDC**.

С этого момента, когда к **Samba** обратился пользователь «*user123*» с паролем «*passw*», она:

Сначала ищет его в **/etc/samba/smbpasswd**, если пароль и имя совпадают - пускает, иначе отказывает в авторизации или считает гостем (в зависимости от настройки);

- если такого имени в упомянутом файле нет - смотрит в **/etc/passwd** (проверив соответствия через файл **/etc/samba/smbusers**) и если такой пользователь есть - спрашивает **PDC**, числится ли за пользователем «*user123*» полученный пароль «*passw*»;
- если это так - пускает, иначе отказывает в авторизации либо переключает на гостевой заход, в соответствии с настройкой.

Обычно при работе в домене на рядовых рабочих станциях **/etc/samba/smbpasswd** должен быть абсолютно пустым либо содержать только административные учетные записи, с доменом никак не связанные.

Данная логика работы применима только в том случае, если не используется **winbind**. Для того, чтобы доменные пользователи автоматически оказывались в **/etc/passwd** при первом же удачном обращении (правильность паролей была подтверждена PDC), в **/etc/samba/smb.conf** необходимо написать одну строку:

[global]

```
add user script = /usr/sbin/useradd -d /home/domain/%u -g 600 -m -k /etc/skel_domain -s /bin/false %u
```

соответственно каталоги **/home/domain** и **/etc/skel_domain**, а также группа 600 должны уже существовать. Все конкретные имена и опции **useradd** можно менять в зависимости от конкретных применений.

По директиве **add user script**, которая активизируется в тех случаях, когда пользователь еще не зарегистрирован на данной машине, можно вызывать не только **/usr/sbin/useradd** с ключами, но и любые другие программы.

При этом не стоит забывать и о безопасности - программы, запущенные при помощи **add user script**, будут выполняться от всемогущего в пределах системы пользователя root, а параметры их вызова частично определяются пользователем, что потенциально опасно!

Теперь можно включить сервер **Samba** командой:

```
service smb start
```

и работать в домене сети Windows на правах рядового члена домена.

Сервер как PDC домена

Для создания **Primary Domain Controller** (PDC) необходимо в **smb.conf** внести/изменить следующие записи

[global]

Имя сервера, если данный параметр не определен, то он примет значение, соответствующее имени хоста:

```
netbios name = COOLSERVER
```

Имя домена:

```
workgroup = COOLDOMAIN
```

Режим работы системы авторизации сервера:

```
security = user
```

Разрешение на использование шифрованных паролей:

```
encrypt passwords = yes
```

Путь к локальному файлу паролей:

```
smb passwd file = /etc/samba/smbpasswd
```

Стать мастер-браузером для домена:

```
local master = yes
```

Быть PDC:

```
domain master = yes
```

Сразу при старте постараться стать мастер-браузером домена:

```
preferred master = yes
```

Быть сервером паролей домена:

```
domain logons = yes
```

Расположение профайла пользователей домена:

```
logon path = \\%L\Profiles\%U
```

Административная группа домена, присутствие в списке пользователя **administrator** весьма желательно, без этого данный пользователь не получит административных прав на клиентских машинах Windows:

```
domain admin group = root @wheel administrator
```

Быть WINS-сервером. WINS-сервер имеет смысл когда в сети более 10 машин, работающих по протоколу **SMB**. Наличие такого сервера в сложных сетях существенно снижает широковещательный трафик:

```
wins support = yes
```

Порядок разрешения имен **NetBIOS**, по аналогии с записью в **/etc/host.conf** для разрешения имен **DNS**. Значение wins имеет смысл только при наличии в сети wins-сервера, в противном случае оно замедлит работу:

```
name resolve order = wins lmhosts bcast
```

Также необходимо создать ресурсы для работы домена.

Ресурс **netlogon** необходим для работы **PDC** и домена в целом. Он просто должен существовать.

[netlogon]

```
comment = Network Logon Service
path = /var/lib/samba/netlogon
guest ok = yes
writable = no
write list = admin, administrator
```

Данный ресурс необходим для создания и хранения профайлов пользователей домена:

[Profiles]

```
path = /var/lib/samba/profiles
browseable = no
read only = no
create mask = 0600
directory mask = 0700
```

При создании пользователя домена в **/var/lib/samba/profiles** автоматически создается каталог с именем, идентичным имени создаваемого пользователя и принадлежащий ему (с правами 0700). В этом каталоге будут храниться личные настройки пользователя.

Для того чтобы включить клиентскую машину в домен, необходимо произвести следующие действия:

Первый метод - вручную.

Прежде всего, необходимо создать локального пользователя системы с именем, соответствующим NetBIOS-name подключаемой к домену машины. К имени на конце добавляется символ ''**$**''. Для добавления машины с именем **machine_name** необходимо от имени пользователя **root** выполнить следующие команды:

```
/usr/sbin/useradd -g machines -d /dev/null -c "machine nickname" -s /bin/false machine_name$
passwd -l machine_named$
```

Теперь, когда создан пользователь (символ ''**$**'' в конце имени означает что это NetBIOS-имя компьютера, а не имя пользователя), можно добавить его в домен, выполнив от имени **root** команду:

```
smbpasswd -a -m machine_name
```

Теперь компьютер подключен к домену.

Второй метод - автоматический.

Работу по созданию машинного акаунта можно переложить на Samba, включив в **smb.conf** следующую запись:

[global]

```
add user script = /usr/sbin/useradd -d /dev/null -g machines -s /bin/false -M %u
```

Теперь **Samba** будет принимать от клиентских машин запросы на включение в домен и автоматически регистрировать их аналогично **NT Server.**

С этого момента начинает существовать домен и PDC на базе Samba-сервера. Пользователи могут входить под своими именами и паролями с любой машины домена с сохранением настроек, а также самостоятельно менять свои пользовательские пароли без помощи администратора сети.

Учетные записи пользователей

Все учетные записи хранятся в файле /etc/samba/smbpasswd.

Учетные записи пользователей, используемые Samba, делятся на две категории:

- записи о компьютерах, входящих в домен;
- записи о пользователях, зарегистрированных на данном сервере.

Следует учитывать, что для того, чтобы создать и использовать любую учетную запись в **/etc/samba/smbpasswd**, предварительно необходимо создать соответствующую запись в **/etc/passwd**. Общее правило - для каждого пользователя в **/etc/samba/smbpasswd** обязательно должен существовать пользователь в **/etc/passwd**. Обратное утверждение неверно.

Для управления учетными записями предназначена утилита **smbpasswd**; полный список ее возможностей можно узнать из соответствующей man-страницы, здесь же рассмотрим наиболее частые методы использования.

Создание нового пользователя:

```
smbpasswd -a <User_name>
```

Смена пароля у существующего пользователя:

```
smbpasswd <User_name>
```

Удаление существующего пользователя:

```
smbpasswd -x <User_name>
```

Приостановление учетной записи без удаления:

```
smbpasswd -d <User_name>
```

Подключение данного компьютера к существующему домену:

```
smbpasswd -j <Domain_name> -U <Administrator_name>
```

Использование winbind

Сервис **winbind** является новым средством, предназначенным для более полной интеграции Samba в домены Windows; он появился, начиная с **Samba 2.2.0**. Данный сервис считывает свою конфигурацию из **/etc/samba/smb.conf** и динамически взаимодействует с PDC домена, автоматически синхронизируя списки пользователей и групп домена и машины **Samba**. Таким образом, **winbind** является весьма удобным средством для автоматического поддержания актуальности базы пользователей домена на рабочих станциях **Samba**.

Работа данного сервиса происходит без изменения содержимого каких-либо авторизационных файлов в **/etc** и при перезагрузке машины доменные пользователи появляются в системе только после запуска **winbindd**. Если во время работы остановить **winbindd**, то доменные пользователи и группы не исчезнут из системы до перезагрузки, однако динамического обновления списков имен и паролей происходить не будет.

Для того чтобы при рестарте компьютера (или только сервиса winbindd) не нарушались соответствия внутренних **UID** и доменных **SID**, он сохраняет текущее состояние списков в файлах **/var/cache/samba/winbindd*.tdb**.

Для нормального функционирования winbindd в файле /etc/samba/smb.conf обязательно должны быть обьявлены следующие директивы:

[global]

Диапазон номеров локальных пользователей, который будет использован для динамического создания пользователей домена:

```
winbind uid = 10000-20000
```

Диапазон номеров локальных групп пользователей, который будет использован для динамического создания групп пользователей домена:

```
winbind gid = 10000-20000
```

Символ-разделитель, используемый для составления доменных имен пользователей и располагающийся между именем домена и именем пользователя:

```
winbind separator = +
```

Интервал времени (в секундах) между запросами **winbind** к PDC в целях синхронизации списков пользователей и групп:

```
winbind cache time = 10
```

Шаблон имени домашних каталогов доменных пользователей, автоматически присваиваемых каждому пользователю. Сами каталоги, однако, динамически не создаются. Вместо переменой **%D** подставляется имя домена, а вместо **%U** подставляется имя пользователя:

```
template homedir = /home/%D/%U
```

Командный интерпретатор, назначаемый по умолчанию для пользователей, авторизованных через **winbindd**.

```
template shell = /bin/bash
```

Также необходимо внести изменения в файле **/etc/nsswich.conf** в разделы **passwd** и **group**, вписав директиву **winbind** - например, таким образом:

```
passwd: files winbind
group: files winbind
```

С этого момента можно использовать имена доменных пользователей в **/etc/samba/smb.conf** с целью разграничения доступа, в правах на файлы и каталоги, для подключения к сетевым ресурсам данного хоста со стороны других хостов.

Обычный клиент

Клиентские функции **Samba** представлены средствами просмотра сетевого окружения и монтирования файловых систем **/usr/bin/smbclient** и **/usr/bin/smbmount** соответственно. Также доступны **mount.smb** и **mount.smbfs**, являющиеся символическими ссылками на **/usr/bin/smbount**.

При запуске эти программы считывают текущую конфигурацию из файла **/etc/samba/smb.conf** и используют доменные функции в случае, если машина подключена к домену Windows.

Также файловые системы возможно монтировать системной командой mount, указав в качестве типа файловой системы **smbfs**, и использовать эти записи в /etc/fstab для автоматического монтирования при загрузке системы.

Например, для того что бы смонтировать в каталог **/mnt/disk** ресурс **public** с машины **SMALLSERVER** под именем **cooluser**, нужно выполнить команду:

```
smbmount //smallserver/public /mnt/disk -o username=cooluser
```

Регистр написания имен компьютеров, ресурсов и пользователей роли не играет. Для того, что бы получить список Samba-ресурсов данной машины и список машин рабочей группы или домена достаточно выполнить команду:

```
#smbclient -L localhost -N
```

Более подробные сведения можно прочесть в man-страницах по **smbclient** и **smbmount**.

Клиент в составе существующего домена NT

Подключение происходит аналогично рассмотренному подключению сервера в составе существующего домена NT. Далее вся работа происходит точно так же, как описано в предыдущем пункте.

Принт-сервер на CUPS

По умолчанию **Samba** сконфигурирована на использование **CUPS** в качестве спулера печати. Подразумевается, что **CUPS** уже настроен и запущен. В **/etc/samba/smb.conf** присутствуют следующие директивы:

[global]

```
printcap name = lpstat
load printers = yes
printing = cups
```

Также необходимо создать ресурс [**printers**] - его создание и назначение директив подробно описано в подпункте «**Обычный сервер**» в части «**Особые ресурсы**».

Особенности локализации клиента и сервера

Для того, чтобы все компоненты **Samba** правильно работали с русскими именами файловых объектов и ресурсов, в **/etc/samba/smb.conf** необходимо добавить следующие директивы:

[global]

```
client code page =
character set =
```

Далее приводятся наборы значений этих директив и системных кодировок, наиболее часто используемых в России, Белоруссии и на Украине:

```
$LANG = ru_RU.KOI8-R
client code page = 866
character set = koi8-r
$LANG = ru_RU.CP2151 client code page = 866 character set = 1251
$LANG = be_BY.CP1251 client code page = 866 character set = 1251
$LANG = uk_UA.KOI8-U client code page = 1125 character set = koi8-u
$LANG = uk_UA.CP1251 client code page = 1125 character set = 1251U
$LANG = ru_UA.CP1251 client code page = 1125 character set = 1251U
```

В двух последних случаях **1251U** - специальное обозначение внутри **Samba** для комбинации «**локально 1251 - удаленно 1125**». В **Samba** определение удаленной кодировки делается по имени локальной.

Также необходимо проследить, чтобы на тех компьютерах Windows, с которыми предполагается взаимодействие через **Samba**, были установлены соответствующие системные настройки локализации. В противном случае велика вероятность, что вместо кириллических символов будут отображены знаки ''**?**'' либо другие символы.

Указанные директивы **/etc/samba/smb.conf** воздействуют на работу всех компонентов **Samba** - и серверных, и клиентских. На данный момент поддерживаются кириллические написания имен - файлов, каталогов и ресурсов.

Некоторые вопросы безопасности

Данный раздел относится в основном к серверной части **Samba**.

Прежде всего необходимо определить, какие интерфейсы должны прослушиваться **Samba** в ожидании запроса на соединение (по умолчанию прослушиваются все имеющиеся в системе).

Например, для того чтобы ограничить прослушивание локальным хостом и первой сетевой картой, необходимо написать в **/etc/samba/smb.conf**:

[global]

```
interfaces = 127.0.0.1 eth0
bind interfaces only = Yes
```

Далее можно ограничить диапазоны адресов, с которых позволительно обращаться к данному серверу. Действие данных директив аналогично воздействию **/etc/hosts.allow** и **/etc/hosts.deny** на **xinetd** и **ssh**: если IP-адрес хоста не подпадает под разрешающее правило, то соединение не будет установлено вовсе. Для того, что бы ограничить доступ двумя подсетями и локальной системой, дополнительно исключив при этом один хост, можно написать:

[global]

```
hosts allow = 192.168.1. 192.168.2. 127.
hosts deny = 192.168.1.12
```

Все вышеперечисленные директивы ограничивают соединения на уровне интерфейсов и IP-адресов до какой либо авторизации.

Следующие директивы управляют режимом авторизации пользователей.

Во избежание перехвата чувствительных данных при передаче их по сети открытым текстом принято шифровать пароли. **Samba** и все версии Windows, начиная с версии Win98, по умолчанию используют шифрование паролей. Данная директива включает его в **Samba**:

[global]

```
encrypt passwords = yes
```

Файл переопределений имен пользователей является весьма мощным средством управления пользовательскими акаунтами, однако при неразумном использовании это средство опасно и поэтому по умолчанию отключено. Внимательно ознакомьтесь с содержимым файла **/etc/samba/smbusers** прежде, чем использовать его.

[global]

```
username map = /etc/samba/smbusers
```

Особенности использования samba 3.0

Samba 3.0 имеет заметные отличия от более ранних версий; наиболее выдающимися из них являются улучшенная по сравнению с версией 2.2 поддержка Unicode, поддержка гораздо большего количества кодовых страниц, новая утилита администрирования net, призванная заменить **smbpasswd**.

Задание кодовых страниц

Для задания кодировок используются следующие новые параметры **smb.conf**:

```
unix charset = <charset>
dos charset = <charset>
display charset = <charset>
```

где <**charset**> - любая кодировка, поддерживаемая **iconv**.

Список возможных кодировок можно узнать, выполнив команду:

```
iconv --list
```

Параметры **client code page** и **character set** больше не поддерживаются. Параметр **unix charset** указывает кодировку, в которой будут храниться файлы на диске, в которой заданы параметры в **smb.conf**.

Параметр **dos charset** указывает кодировку, в которой **Samba** будет общаться с клиентами, не поддерживающими **Unicode**. Все версии Windows, начиная с 95, понимают Unicode - но все же стоит установить **dos charset = cp866**, что соответствует **client code page = 866** в более старых версиях.

Параметр **display charset** указывает, в какой кодировке должны выводить информацию программы, непосредственно обменивающиеся информацией с пользователем, например **smbclient**, **net**, **wbinfo** и другие.

Утилита net

Утилита **net** призвана заменить **smbpasswd** и обеспечивает гораздо большие возможности по получению информации о сети и управлению сетью. Формат команд утилиты очень похож на формат одноименной команды Windows NT/2000.

Основные применения команды **net**:

- создание и удаление пользователей: **net user**;
- включение машины в домен: net ads join - Active Directory; **net rpc join - NT Domain**;
- получение информации о домене, машине, открытых файлах, сессиях: **net info**, **net ads status**, **net rpc status**;
- создание и удаление разделяемых ресурсов на удаленных машинах: **net share**;
- синхронизация времени с windows-сервером: **net time**.

Управление машиной с Samba из Microsoft Management Console

Начиная с версии **2.2**, **Samba** имеет возможнось удаленного администрирования из **MMC** (Microsoft Management Console). Эта возможность полезна, когда **Samba** является членом NT-домена или **AD**. Администратор домена может создавать, удалять и изменять

сетевые ресурсы на UNIX-машине с запущенной **Samba**.

Для управления ресурсами служат параметры **/etc/samba/smb.conf**:

[global]

```
add share command = <add script>
```

Параметр указывает скрипт, который будет вызван при попытке создания нового ресурса в **MMC**. Скрипту передается четыре параметра:

- имя конфигурационного файла (например, **/etc/samba/smb.conf**);
- имя создаваемого ресурса;
- путь к существующей директории на диске;
- комментарий.

Скрипт должен завершаться с кодом **0**, в случае успешного создания, и ненулевым - в случае ошибки.

```
change share command = <change script>
```

Параметр указывает скрипт, который будет вызван при попытке изменения существующего ресурса в MMC. Скрипту передается четыре параметра:

- имя конфигурационного файла (например, **/etc/samba/smb.conf**);
- имя создаваемого ресурса;
- путь к существующей директории на диске;
- комментарий.

Скрипт должен завершаться с кодом **0**, в случае успешного создания, и ненулевым - в случае ошибки.

```
delete share command = <delete script>
```

Параметр указывает скрипт, который будет вызван при попытке удаления существующего ресурса в MMC (Stop sharing). Скрипту передается два параметра:

- имя конфигурационного файла (например **/etc/samba/smb.conf**);
- имя создаваемого ресурса.

Скрипт должен завершаться с кодом **0**, в случае успешного создания, и ненулевым - в случае ошибки.

Чтобы скрипты могли изменять конфигурационные файлы **Samba**, они должны выполняться с правами **root**. Для этого нужно установить отображение пользователей домена, имеющих право изменять ресурсы, в **root**. Это можно сделать либо с помощью файла **/etc/samba/smbusers**, прописав там строку вида:

```
root = administrator <user 1> ... <user n>
```

либо с помощью параметра **admin users** в **/etc/samba/smb.conf**:

```
admin users = administrator
```

При создании нового ресурса Windows позволяет просматривать дерево директорий. Для этого в **/etc/samba/smb.conf** нужно задать служебные ресурсы, заканчивающиеся символом `'$'`, например:

```
[C$]
path = /drives/c
```

После этого при создании нового ресурса можно будет просматривать и выбирать все директории ниже **/drives/c**.

Работа в среде Active Directory

Для объединения компьютеров в домены Widows 2000 Server использует схему, отличную от NT- доменов, которая называется Active Directory; эта схема обладает гораздо большей масштабируемостью и позволяет централизованно администрировать машины, входящие в домен. Active Directory базируется на протоколе авторизации Kerberos, при котором имя пользователя и пароль не передаются по сети, а используется механизм так называемых билетов, выдаваемых сервером на определенное время. Получив билет, машина, входящая в домен, может авторизоваться на других машинах домена без участия сервера.

Установка Samba

Samba 3.0, в отличие от более ранних версий Samba, имеет возможность работать в сетях Wndows, работающих в режиме Active Directory (или Windows 2000 native mode). Если требуется эта функциональность, следует установить **samba3 samba2**.

Active Directory имеет другую схему именования доменов, компьютеров и пользователей, основанную на DNS. Допустим, существует сеть с именем **my.firm.com** и компьютерами **host1.my.firm.com**, **host2.my.firm.com**, **host3.my.firm.com**; тогда домен Active Directory будет называться **my.firm.com**, а пользователи Active Directory будут иметь имена вида user@my.firm.com.

Настройка

/etc/krb5.conf должен содержать, по крайней мере, следующие строки:

[realms]

```
MY.FIRM.COM = {
kdc = your.kerberos.server
}
```

г д е **MY.FIRM.COM** - имя домена (или «царства», в терминологии Kerberos; задается обязательно в верхнем регистре), а **your.kerberos.server** - имя или IP-адрес KDC (Kerberos Domain Controller), аналог PDC (Primary Domain Controller) в доменах Windows NT - например, **server.my.firm.com** или **192.168.117.11**.

Правильность указания параметров можно проверить, выполнив команду (замените имя пользователя на актуальное - например, administrator@MY.FIRM.COM):

```
kinit username@REALM
```

и убедившись, что пароль был принят сервером. REALM всегда задается в верхнем регистре.

Также нужно убедиться, что возможно получить имя KDC по его IP адресу (так называемый Reverse DNS lookup). Имя KDC должно либо совпадать с NetBIOS-именем компьютера (имя машины в сети Windows без указания домена) либо состоять из NetBIOS-имени и имени домена. Если получить имя KDC по адресу невозможно, вы получите ошибку "**local error**" при попытке войти в домен.

Если DNS не поддерживает Reverse **lookup** либо KDC не зарегистрирован в DNS, вы можете указать соответствие IP-адреса и имени в **/etc/hosts**.

Редактирование /etc/samba/smb.conf:

Для работы в Active Directory smb.conf должен содержать следующие параметры:

```
[global]

# Задаёт Kerberos realm, обычно совпадает с именем домена в
# верхнем регистре, например realm = MY.FIRM.COM
realm = <REALM>

# Это обычно часть реалма до первой точки, например
# workgroup = MY
workgroup = <WORKGROUP>

# Тип домена - Active Directory.
security = ADS

# В случае Active Directory пароли всегда шифруются.
encrypt passwords = true

# Обычно этот параметр указывать не обязательно, т.к. Samba сама
# определяет адрес KDC, если в сети есть WINS-сервер и он указан
# в smb.conf
ads server = <your.kerberos.server>
```

Регистрация компьютера в Active Directory домене

Убедитесь что **Samba** не запущена. Если запущена, ее нужно остановить:

```
service smb stop; service winbind stop
```

Чтобы включить компьютер в домен, выполните команду:

```
net ads join -U administrator
```

где **administrator** - имя пользователя домена, имеющего право создавать новые учетные записи.

Если не было выдано сообщение об ошибке, то машина успешно зарегистрирована в домене - иначе проверьте правильность задания параметров в **/etc/samba/smb.conf** и **/etc/krb5.conf**. Убедитесь, что пользователь, указанный после **-U** в **net ads join**, имеет необходимые права на создание новых учетных записей.

Теперь можно запустить необходимые службы:

```
service smb start; service winbind start
```

Проверка правильной работы в Active Directory

Для работы с компьютерами, зарегистрированными в Active Directory, не требуется указывать имя пользователя и пароль. Попробуйте выполнить команду:

```
smbclient -k -L <имя компьютера в домене>
```

Вы должны получить список доступных ресурсов, при этом **smbclient** не должен запрашивать имя пользователя и пароль.

Чтобы проверить, что доступ к ресурсам вашей машины возможен с других машин домена, вы можете попробовать выполнить все ту же команду:

```
smbclient -k -L <имя вашего компьютера в домене>
```

и получить список доступных ресурсов. Можно также попробовать открыть какой-нибудь ресурс на вашей машине с Windows-машины, входящей в домен. В любом случае, имя пользователя и пароль запрашиваться не должны.

Некоторые особенности работы в Active Directory

В отличие от доменов Windows NT, авторизация в Active Directory производится не по имени и паролю, а с помощью билетов протокола **Kerberos**. Из-за этого работа с **smbclient** может поначалу показаться необычной.

Во-первых, при вызове smbclient нужно указывать опцию **-k**. Во-вторых, билеты **Kerberos** даются на определенное время (обычно на сутки, но это зависит от настроек сервера). Поэтому их нужно периодически обновлять с помощью команды **kinit**:

```
kinit username@realm
```

где **username** - ваше имя в Active Directory домене **REALM**.

Так что если **smbclient** вдруг перестает подключаться к доменным ресурсам, попробуйте обновить билет - скорее всего, дело именно в этом.

Установка сервера SAMBA DC

Предварительная настройка сервера
Обновление пакетов
Установка необходимых пакетов
Отключение SELinux
Присваивание серверу доменного имени
Отключение DNS-службы systemd-resolved
Настройка сетевого интерфейса
Настройка сетевого интерфейса вручную
Настройка сетевого интерфейса с помощью утилиты nmtui
Создание нового домена под управлением контроллера домена Samba DC
Создание резервных копий файлов
Настройка конфигурации Kerberos
Первоначальное полуавтоматическое конфигурирование сервера с помощью утилиты samba-tool
Дополнительная настройка сервера
Запуск и проверка работоспособности службы samba

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: samba-4.17.5-2h, krb5-devel-1.20.1-1

Вы можете подробнее ознакомиться с установкой и настройкой **SAMBA**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка Samba как контроллера домена в РЕД ОС 7.2 ;
- в **Яндекс.Дзен** — Настройка Samba как контроллера домена в РЕД ОС 7.2 .

На наших каналах вы также сможете найти много другой полезной информации.

В обучающем видео рассмотрен пример установки и настройки сервера **SAMBA** на **РЕД ОС 7.2**. В настоящее время актуальными версиями ОС являются **РЕД ОС 7.3** и **РЕД ОС 8**, в которых используется пакетный менеджер **dnf** вместо **yum**.

Предварительная настройка сервера

Обновление пакетов

Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните обновление всех пакетов:

```
dnf makecache && dnf upgrade
```

Все дальнейшие действия выполняются с правами пользователя **root**, если не указано иное.

Установка необходимых пакетов

Для установки необходимых пакетов выполните:

```
dnf install samba* krb5*
```

Отключение SELinux

На время настройки переведите SELinux в режим уведомлений:

```
setenforce 0
```

Статус службы SELinux можно посмотреть командой **sestatus**.

Замените в файле конфигурации **/etc/selinux/config** режим `enforcing` на `permissive` командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

После перезагрузки системы служба SELinux будет запущена — в режиме, который указан в конфигурационном файле.

Присваивание серверу доменного имени

Сервер контроллера домена должен иметь собственное уникальное доменное имя и статический IP-адрес. Назначьте серверу полное доменное имя: например, если короткое имя сервера **dc1**, то для домена **skynet.murom** полное имя сервера имеет вид **dc1.skynet.murom**:

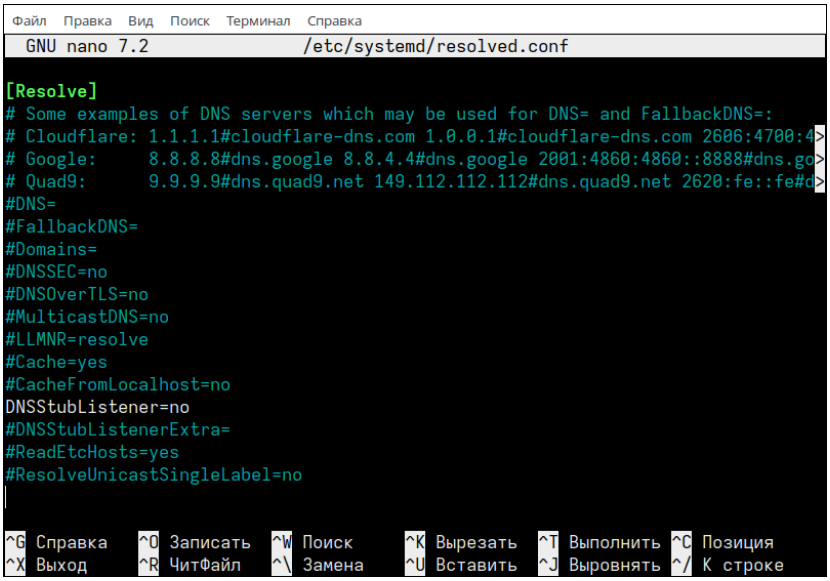
```
hostnamectl set-hostname dc1.skynet.murom
```

Отключение DNS-службы systemd-resolved

Откройте файл **/etc/systemd/resolved.conf**.

```
sudo nano /etc/systemd/resolved.conf
```

Установите параметр `DNSStubListener` в значение `no`, как показано в примере. Это необходимо, чтобы отключить прослушивание **systemd-resolved** на порту `53`.



После внесения изменений в файл необходимо перезапустить **systemd-resolved** и **NetworkManager** командой:

```
systemctl restart systemd-resolved.service NetworkManager
```

Проверьте изменения в настройках, выполните:

```
cat /etc/resolv.conf
```

В выводе должен быть указан адрес отличающийся от `127.0.0.53`. Например:

```
nameserver 192.168.1.96
 search skynet.murom
```

Настройка сетевого интерфейса

По умолчанию сетевой интерфейс настроен для получения IP-адреса по **DHCP**. Нужно установить серверу контроллера домена статический IP-адрес.

Настройку сетевого интерфейса можно выполнить несколькими способами, в данной статье рассматриваются два из них:

- вручную, путём редактирования файла настроек;
- с помощью графической консольной утилиты **nmtui**.

Настройка сетевого интерфейса вручную

Настройки хранятся в файле **/etc/NetworkManager/system-connections/<имя_сетевого_интерфейса>.nmconnection**. Именуются они, например, как **enp0s3** или **enp0s4**.

В данном примере сетевой интерфейс имеет имя **enp0s3**.

Откройте конфигурационный файл в текстовом редакторе:

```
nano /etc/NetworkManager/system-connections/enp0s3.nmconnection
```

Внесите следующие изменения:

1) измените тип соединения на статический:

```
method=manual
```

2) установите значение для игнорирования DNS из DHCP:

```
ignore-auto-dns=true
```

3) укажите IP-адрес контроллера, маску подсети и IP-адрес шлюза:

```
address1=192.168.1.96/24,192.168.1.1
```

4) укажите в качестве *DNS-сервера* IP-адрес создаваемого контроллера домена:

```
dns=192.168.1.96
```

5) впишите домен поиска (в данном примере это skynet.murom):

```
dns-search=skynet.murom;
```

Итоговый файл настройки должен иметь вид:

```
[connection]
id=enp0s3
uuid=97def639-603a-4167-9613-edd5bd902ef8
type=ethernet
interface-name=enp0s3
timestamp=1704763284

[ethernet]

[ipv4]
address1=192.168.1.96/24,192.168.1.1
dns=192.168.1.96;
dns-search=skynet.murom;
ignore-auto-dns=true
method=manual

[ipv6]
addr-gen-mode=eui64
method=auto

[proxy]
```

Перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Для проверки настроек статической IP-адресации воспользуйтесь командой ifconfig или ip addr.

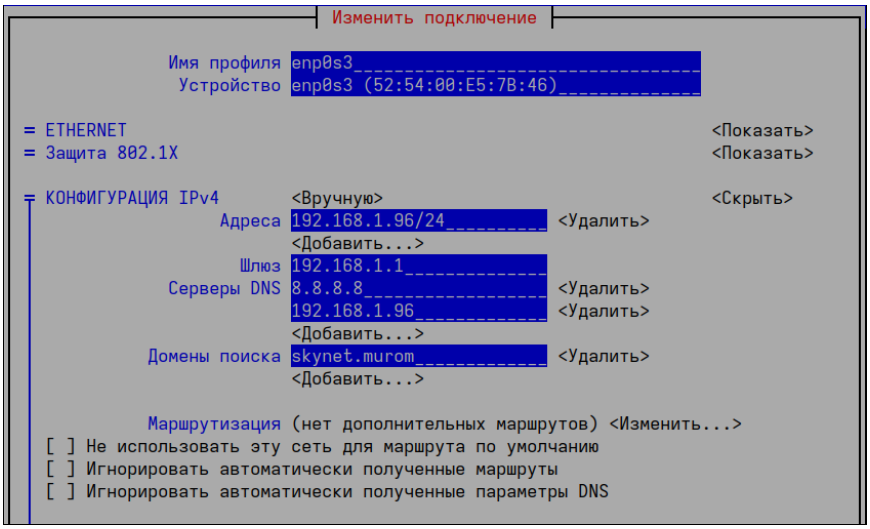
Настройка сетевого интерфейса с помощью утилиты nmtui

Запустите утилиту в консоли:

```
nmtui
```

В настройках сетевого интерфейса в конфигурации **IPv4** укажите следующие значения:

- тип конфигурирования – «**Вручную**»;
- IP-адрес создаваемого сервера и маску подсети – **192.168.1.96/24**;
- адрес шлюза – **192.168.1.1**;
- IP-адрес первого DNS-сервера – IP-адрес сервера с доступом к локальному репозиторию или интернету, например **8.8.8.8** (при добавлении контроллера домена РЕД АДМ в существующий домен указать IP-адрес контроллера домена существующего домена);
- IP-адрес второго DNS-сервера – IP-адрес создаваемого контроллера домена, **192.168.1.96**;
- домен поиска – **skynet.murom**.



Перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Проверьте доступные серверы имен, просмотрев файл **resolv.conf**:

```
cat /etc/resolv.conf
```

Вывод команды должен иметь примерно следующий вид:

```
nameserver 8.8.8.8
nameserver 192.168.1.96
search skynet.murom
```

Создание нового домена под управлением контроллера домена Samba DC

Создание резервных копий файлов

Переименуйте файл **/etc/smb.conf**, он будет создан позднее в процессе выполнения команды **samba-tool**. Наличие данного файла на момент запуска полуавтоматической конфигурации может вызвать ошибку.

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Создайте резервную копию используемого по умолчанию конфигурационного файла **kerberos**:

```
cp /etc/krb5.conf /etc/krb5.conf.bak
```

Настройка конфигурации Kerberos

Откройте файл **/etc/krb5.conf**:

```
nano /etc/krb5.conf
```

В секции [libdefaults] установите имя домена, используемое по умолчанию:

```
default_realm = SKYNET.MUROM
```

В ту же секцию добавьте время жизни тикета керберос:

```
ticket_lifetime = 24h
 forwardable = yes
```

Пример листинга конфигурации **krb5.conf**:

```
[libdefaults]
 default_realm = SKYNET.MUROM
 dns_lookup_realm = false
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 forwardable = yes

 [realms]
 SKYNET.MUROM = {
 kdc = dc1.skynet.murom
 admin_server = dc1.skynet.murom
 }

 [domain_realm]
 .skynet.murom = SKYNET.MUROM
 skynet.murom = SKYNET.MUROM
```

Откройте файл **/etc/krb5.conf.d/crypto-policies**:

```
nano /etc/krb5.conf.d/crypto-policies
```

и приведите его содержание к следующему виду:

```
[libdefaults]
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
    preferred_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 RC4-HMAC DES-CBC-CRC DES3-CBC-SHA1 DES-CBC-MD5
```

Первоначальное полуавтоматическое конфигурирование сервера с помощью утилиты samba-tool

Конфигурирование в интерактивном режиме выполняется командой:

```
samba-tool domain provision --use-rfc2307 --interactive
```

Описание некоторых опций (параметров) этой команды:

- use-rfc2307 – параметр добавляет POSIX атрибуты (UID / GID) на схеме AD. Он понадобится при аутентификации клиентов Linux,

BSD, или OS X (в том числе, на локальной машине), в дополнение к Microsoft Windows;

- interactive – запуск в интерактивном режиме;
- realm – указывает на полное DNS-имя домена, которое настроено в **/etc/hosts**, в верхнем регистре (в рассматриваемом примере это SKYNET.MUROM);
- Domain – краткое имя домена *NetBIOS* (в примере – **SKYNET**);
- Server Rules – роль сервера (например, DC – **domain controller**);
- DNS backend – DNS-сервер. Возможные значения – **SAMBA_INTERNAL** (внутренний DNS сервера), **BIND9_FLATFILE**, **BIND9_DLZ**, **NONE**;
- DNS forwarder IP address – данный параметр позволяет указать IP-адрес DNS-сервера, на который будут перенаправлены DNS-запросы, в том случае, когда сервер не сможет их разрешить.

Более подробная информация доступна в Wiki-справке проекта Samba по адресу https://wiki.samba.org, на странице "**Setting up Samba as an Active Directory Domain Controller**".

Пример сокращённого листинга настройки для тестового домена **skynet.murom**:

```
Realm [SKYNET.MUROM]:
Domain [SKYNET]:
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.1.96]: 192.168.1.1
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce uniqueness constraint on local domainSIDs
Adding DomainDN: DC=skynet,DC=muromAdding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=skynet,DC=muromCreating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with this one. Do not create a symlink!
Setting up fake yp server settings
Once the above files are installed, your Samba AD server will be ready to use
Server Role: active directory domain controller
...Hostname:dc1
...NetBIOS Domain:SKYNET
...DNS Domain: skynet.murom
...DOMAIN SID:S-1-5-21-4010603892-1310842104-1159347701
```

После запуска автоматической настройки файлы конфигурации будут созданы автоматически.

Дополнительная настройка сервера

Настройки сервера находятся в файле **/etc/samba/smb.conf**. Конфигурирование сервера выполняется путём внесения изменений в этот файл:

```
nano /etc/samba/smb.conf
```

Начиная с версии **3.3.0** в Samba есть модуль **acl_xattr**, который позволяет Samba корректно обрабатывать Windows ACL (Access Control List) и обеспечивает полноценную поддержку прав доступа к файлам.

Для подключения этого модуля добавьте в файл **/etc/samba/smb.conf** в секцию [global] следующие строки (либо отредактируйте существующие):

```
vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
```

Для включения автоматического обновления записей в DNS добавьте следующий параметр в секцию [global]:

```
allow dns updates = nonsecure
```

В секцию [global] добавьте поддержку расширений схемы Samba AD (Active Directory):

```
dsdb:schema update allowed = true
```

Пример содержания файла **/etc/samba/smb.conf** с внесёнными дополнительными изменениями:

```
cat /etc/samba/smb.conf
```

```
#Global parameters
 [global]
 netbios name = DC1
 realm= SKYNET.MUROM
 server role = active directory domain controller
 workgroup= SKYNET
 idmap_ldb:use rfc2307 = yes
 vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 dsdb:schema update allowed = true

 [sysvol]
 path = /var/lib/samba/sysvol
 read only = No

 [netlogon]
 path = /var/lib/samba/sysvol/skynet.murom/scripts
 read only = No
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните проверку:

```
testparm
```

Пример вывода команды:

```
Load smb config files from /etc/samba/smb.conf
vfs objects specified without required AD DC module: dfs_samba4
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
```

Запуск и проверка работоспособности службы samba

Запустите и добавьте в автозагрузку службу **samba**:

```
systemctl enable samba --now
```

Проверьте статус служб:

```
systemctl status samba
```

> **Примечание.**
>
> Не запускайте службу **winbind** вручную на контроллере домена Samba Active Directory. Служба запускается автоматически как подпроцесс **samba**.

Проверьте работу динамического обновления **DNS**:

```
samba_dnsupdate --verbose --all-names
```

Для более быстрой проверки рекомендуется отключить **IPv6**. Сделать это можно с помощью утилиты **nmtui**.

Администрирование контроллера SAMBA

Средства администрирования удаленного сервера от MS
Подготовка резервного контроллера домена
Добавление резервного контроллера в домен
Установка необходимых пакетов
Присоединение сервера в качестве вторичного контроллера домена
Дополнительная настройка сервера
Запуск служб
Настройка NTP на контроллере домена dc1.skynet.murom
Настройка NTP на резервном контроллере домена dc2.skynet.murom
Настройка двунаправленной репликации sysvol и netlogon с помощью Unison

Средства администрирования удаленного сервера от MS

Введение ПК с Windows в домен Samba производится точно так же, как и ввод компьютера в домен MS AD.

Для администрирования домена Samba установите **RSAT** - https://wiki.samba.org/index.php/Installing_RSAT.

Включите компоненты: «**Установка удаление программ**» - «**Включение отключение компонентов**» - «**Средства удаленного администрирования сервера**».

После настройки перезагрузите ПК.

В управлении DNS подключитесь к **dc1.skynet.murom**, добавьте обратную зону и PTR-запись для контроллера домена **dc1**. Кроме работы с DNS через оснастку Windows существует способ добавления обратной зоны dns с помощью команд в терминале.

Для этого, предварительно, получите kerberos-тикет:

```
kinit administrator@SKYNET.MUROM
```

Добавьте обратную зону:

```
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 1.81.10.in-addr.arpa
samba-tool dns add dc1.skynet.murom 1.81.10.in-addr.arpa 96 PTR dc1.skynet.murom -U administrator
```

в последней команде **96** - это последний октет (четвертый) в IP-адресе (**10.81.1.96**) сервера samba.

Следующие зоны, вероятно, создавать не обязательно, но такие зоны автоматически настроены на Windows srv:

```
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 0.in-addr.arpa
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 127.in-addr.arpa
samba-tool dns zonecreate -U Administrator dc1.skynet.murom 255.in-addr.arpa
```

Подготовка резервного контроллера домена

Настройте сеть, по примеру **DC1**.

Проверьте, что настройки применены, проверив содержимое файла **resolv.conf**:

```
 cat /etc/resolv.conf

nameserver 10.81.1.96
search skynet.murom
```

С помощью **hostnamectl** измените доменное имя машины на **dc2.skynet.murom**:

```
hostnamectl set-hostname dc2.skynet.murom
```

В **/etc/hosts** пропишите:

```
<IP-адрес-сервера-DC2> dc2.skynet.murom dc2
```

Добавление резервного контроллера в домен

Установка необходимых пакетов

Установите необходимые пакеты командой:

```
dnf install samba* krb5*
```

Присоединение сервера в качестве вторичного контроллера домена

Скопируйте конфигурации самбы с основного контроллера **/etc/samba/smb.conf** и **/etc/krb5.conf**.

Измените в **/etc/samba/smb.conf** значение следующего параметра:

```
netbios name=DC2
```

Получите билет:

```
# kinit Administrator
```

и проверьте вывод:

```
# klist
```

Добавьте **winbind** в файл **/etc/nsswitch.conf**.

Winbind будет использоваться как прокси между AD и связкой **PAM** и **NSS**. Для аутентификации AD **winbind** использует **kerberos**, а LDAP используется для получения информации.

```
nano /etc/nsswitch.conf

passwd: winbind sss files systemd
group:  winbind sss files systemd
shadow: winbind files sss
hosts:  files dns wins
```

Выполните команду присоединения к домену в роли "**backend**":

```
samba-tool domain join skynet.murom DC -U Administrator --dns-backend=SAMBA_INTERNAL --realm=skynet.murom
```

Введите пароль от доменного *Администратора контроллера домена*.

При этом в прямой зоне DNS должна появиться соответствующая A-запись.

Дополнительная настройка сервера

Выполните дополнительную настройку сервера аналогично тому, как это сделано в подразделе Дополнительная настройка основного сервера.

Отредактируйте файл **/etc/samba/smb.conf** и добавьте в секцию [global] следующие строки (либо отредактируйте существующие):

```
vfs objects = acl_xattr
 map acl inherit = yes
 store dos attributes = yes
 allow dns updates = nonsecure
 dns update command = /usr/sbin/samba_dnsupdate --all-names
 dsdb:schema update allowed = true
```

После внесения изменений в файл **/etc/samba/smb.conf** выполните проверку:

```
testparm
```

Пример вывода команды:

```
Load smb config files from /etc/samba/smb.conf
vfs objects specified without required AD DC module: dfs_samba4
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
```

Удалите из настроек сетевого интерфейса из списка DNS-серверов IP-адрес внешнего сервера, который был указан ранее. В данном примере это 8.8.8.8. Перезагрузите сетевой интерфейс.

Запуск служб

Запустите и добавьте в автозагрузку службы **samba**:

```
systemctl enable samba --now
```

Проверьте статус службы:

```
systemctl status samba
```

В DNS добавьте PTR-запись второго сервера в обратную зону.

Для проверки репликации выполните:

```
samba-tool drs showrepl
```

Предупреждение Warning: No NC replicated for Connection! можно проигнорировать (см. FAQ в Samba Wiki).

Для запуска принудительной репликации выполните:

```
samba-tool drs replicate dc2.skynet.murom dc1.skynet.murom dc=skynet,dc=murom
```

В качестве первого аргумента должен быть указан приемник, в качестве второго - источник.

По умолчанию автоматическая *внутрисайтовая репликация* в Windows AD занимает *5 сек*, *межсайтовая репликация - 15 мин*. Данные значения не регулируются. Без успешной двунаправленной репликации в течение *14 дней* DC исключается из Active Directory.

Настройка NTP на контроллере домена dc1.skynet.murom

Для установки NTP выполните:

```
dnf install ntp
```

Измените группу и права:

```
chgrp ntp /var/lib/samba/ntp_signd/
chmod 750 /var/lib/samba/ntp_signd/
```

Отредактируйте конфигурационный файл:

```
nano /etc/ntp.conf
```

Добавьте следующие строки:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
server 0.pool.ntp.org iburst prefer
server 1.pool.ntp.org iburst prefer
ntpsigndsocket /var/lib/samba/ntp_signd/
```

Закомментируйте строки:

```
#driftfile /var/lib/ntp/ntp.drift
#logfile /var/log/ntp
```

Описание параметров файла конфигурации NTP:

- **ntpsigndsocket /usr/local/samba/ntp_signd/** - позволит клиентским машинам отправлять NTP-запросы к серверу используя Active Directory;
- **Server** - указывает на сервера синхронизации времени;
- **restrict 127.0.0.1** - обмен данным с самим собой;
- **iburst** — отправлять несколько пакетов (повышает точность);
- **prefer** — указывает на предпочитаемый сервер времени;
- **server 127.127.1.0** — позволит, в случае отказа сети Интернет, брать время из своих системных часов.

Старт NTP и добавление в автозапуск:

```
systemctl disable chronyd --now
systemctl enable ntpd --now
```

Проверка статуса NTP:

```
systemctl status ntpd.service
```

Проверить состояние получения эталонного времени можно командой:

```
ntpq -p
```

Настройка NTP на резервном контроллере домена dc2.skynet.murom

Отключите службу **chrony**:

```
systemctl disable chronyd --now
```

Запустите службу **NTP**:

```
systemctl enable ntpd --now
```

В файл **/etc/ntp.conf** на резервном контроллере добавьте строки:

```
server dc1.skynet.murom iburst prefer
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
```

Проверка:

```
[root@dc2 ~]# ntpq -p
remote refid st t when poll reach   delay offset jitter
==============================================================================
*dc1.skynet.murom 62.33.136.11 2 u - 64 1 0.272 0.177 0.618
cello.corbina.n 194.58.202.20 2 u - 64 1 14.088 2.191 0.673
62.183.87.106 194.190.168.1 2 u 1 64 1 48.239 9.129 10.577
```

Настройка двунаправленной репликации sysvol и netlogon с помощью Unison

Информацию о настройке Samba на поддержку репликации SysVol через DFS-R или FRS см. по ссылке.

Папка **SYSVOL** содержит групповые политики и скрипты. Отсутствие репликации приведет к неправильной работе групповых политик и сценариев входа. Есть два варианта: однонаправленная синхронизации и двунаправленная. В первом случае, реплика снимается с основного контроллера и распространяется на все резервные.

Во втором работает в обе стороны. Используем для этого Rsync и Unison (программа двунаправленной синхронизации файлов).

Для установки пакетов выполните:

```
dnf install rsync unison
```

Создание для ssh rsa-ключей и копирование публичного ключ на **DC2**:

```
[root@dc1 ~]# ssh-keygen -t rsa
[root@dc1 ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub root@DC2.skynet.murom
```

Теперь без ввода пароля можно попасть по ssh с **DC1** на **DC2** выполнив команду:

```
ssh dc2.skynet.murom
```

При низких скоростях в сети, unison может некорректно работать, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
mkdir ~/.ssh/ctl
cat << EOF > ~/.ssh/ctl/config
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

Лог файл репликации (следим за размером лога!)

```
touch /var/log/sysvol-sync.log
chmod 640 /var/log/sysvol-sync.log
```

Создайте файла конфигурации unison, для этого создадим каталог **.unison**:

```
mkdir /root/.unison
```

а теперь создайте в нем файл конфигурации:

```
nano /root/.unison/default.prf
```

с содержимым:

```
root = /var/lib/samba
# Note that 2 x / behind DC2, it is required
root = ssh://root@DC2.skynet.murom//var/lib/samba
# Путь синхронизации
path = sysvol
#ignore = Path stats  ## ignores /var/www/stats
auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
copythreshold=0
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress --old-args
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace --compress --old-args
copyquoterem = true
copymax = 1
logfile = /var/log/sysvol-sync.log
```

Установка **rsync** и **unison** на DC2:

```
dnf install rsync unison
```

Сделайте **backup sysvol**, потом запустите команду синхронизации:

```
/usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol
root@dc2.skynet.murom:/var/lib/samba && /usr/bin/unison
&> /dev/null
```

в этой строке программа **rsync** создает структуры каталогов с расширенными атрибутами, а затем программа **Unison** копирует только эти расширенные атрибуты файлов.

Межсайтовая синхронизация настраивается через оснастку (*mmc*) "**Active Directory Sites and Services**" в Windows. Оснастка входит в пакет RSAT.

Настройка доверительных отношений SAMBA и MSAD

Исходные данные
Настройка сервера Samba
Настройка DNS на сервере Windows
Настройка доверительных отношений

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия Samba:** 4.15.9-2h
- **Версия Windows Server:** 2012 R2

Исходные данные

Для примера создания доверительных отношений будут использоваться следующие данные:

Сервер Samba - **dc.skynet.murom**, IP - **10.81.1.199**

Сервер MS AD – **dcms.msnet.murom**, IP - **10.81.1.210**

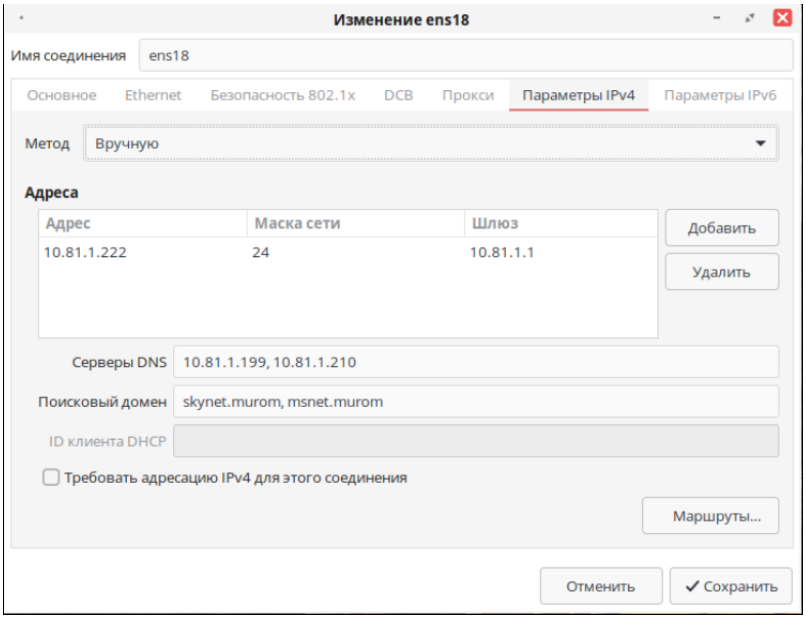
Предполагается, что сервер *Samba* был настроен по инструкции «Установка сервера Samba DC».

Настройка сервера Samba

В сетевых настройках сервера Samba требуется указать DNS адрес контроллера домена MS AD и поисковый домен MS AD. После применения настроек в файле **/etc/resolv.conf** должны содержаться следующее записи:

```
cat /etc/resolv.conf

# Generated by NetworkManager
search skynet.murom msnet.murom
nameserver 10.81.1.199
nameserver 10.81.1.210
```

Пример настройки DNS:



Далее потребуется изменить файл конфигурации:

```
nano /etc/samba/smb.conf
```

В строке dns forwarder пропишите IP-адрес *MS AD*:

```
dns forwarder = 10.81.1.210
```

Если доверительные отношения создаются с доменом **.local**, то в файле **/etc/nsswitch.conf** приведите строку, которая начинается на **hosts**, к виду:

```
hosts:      files dns resolve [!UNAVAIL=return] myhostname mdns4_minimal
```

Затем отредактируйте файл **/etc/krb5.conf**:

```
nano /etc/krb5.conf
```

Добавив строки в [**realms**], где нужно описать *kerberos* область Windows-домена:

```
MSNET.MUROM = {
kdc = dcms.msnet.murom
kdc = dcms2.msnet.murom
admin_server = dcms.msnet.murom
}
```

Если имеется резервный контроллер домена, то его также следует добавить. В примере это `kdc = dcms.msnet.murom.`

Пример вывода:

```
cat /etc/krb5.conf:

[libdefaults]
      default_realm = SKYNET.MUROM
      dns_lookup_realm = false
      dns_lookup_kdc = true
        ticket_lifetime = 24h
        forwardable = yes

[realms]
SKYNET.MUROM = {
      default_domain = skynet.murom
}
MSNET.MUROM = {
   kdc = dcms.msnet.murom
   kdc = dcms2.msnet.murom
   admin_server = dcms.msnet.murom
}

[domain_realm]
       dc = SKYNET.MUROM
```

Проверьте разрешения SRV-записей командой:

```
host -t srv _kerberos._tcp.msnet.murom

_kerberos._tcp.msnet.murom has SRV record 0 100 88 dcms.msnet.murom.
```

Запросите тикет Kerberos:

```
kinit admin@MSNET.MUROM
```

Проверьте, что тикет успешно получен:

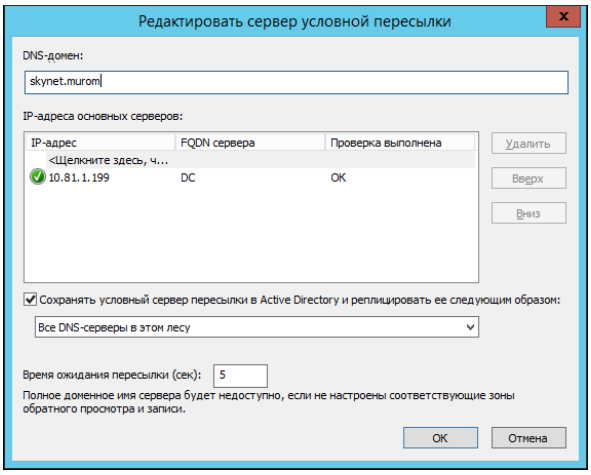
```
klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@MSNET.MUROM

Valid starting  Expires   Service principal
25.07.2022  15:19:37 26.07.2022  01:19:37 krbtgt/MSNET.MUROM@MSNET.MUROM
```

Настройка DNS на сервере Windows

Создайте сервер условной пересылки, для этого откройте **Диспетчер DNS** и перейдите на вкладку «**Серверы условной пересылки**».

В контекстном меню выберите «**Создать сервер условной пересылки**».

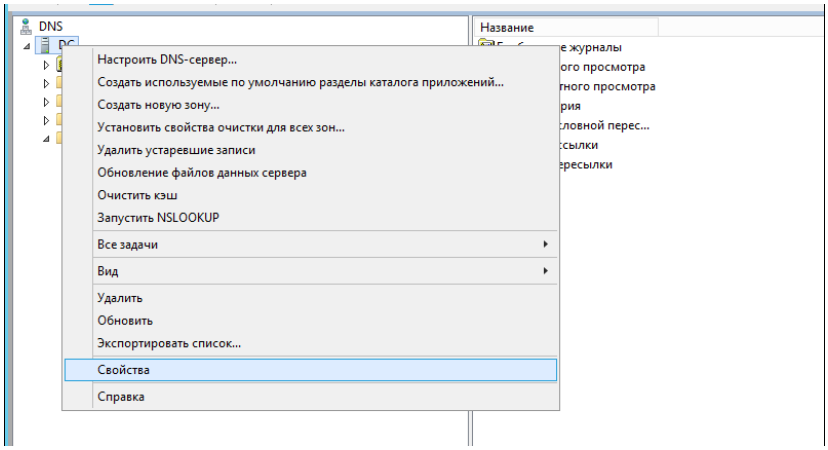
Впишите DNS домен сервера SAMBA и его IP-адрес. Выберите «**Все DNS серверы в этом лесу**» и нажмите **OK**.

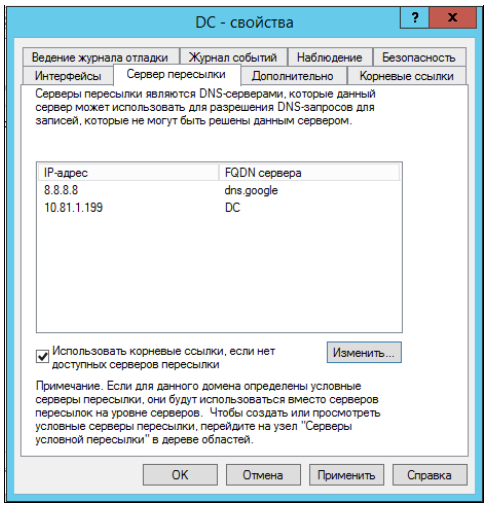


Также необходимо добавить глобальный «**Сервер пересылки**» в свойствах DNS сервера *Windows*.

Для этого в диспетчере DNS нажмите правой кнопкой мыши на сервере DNS (**SERV**) и в выпадающем меню выберите «**Свойства**», перейдите на вкладку «**Сервер пересылки**», нажмите на кнопку «**Изменить**» и в открывшемся окне введите IP-адрес сервера *SAMBA*.

Перейдите в свойства DNS сервера *MS AD*.





Чтобы убедиться, что сервер *AD* может корректно видеть *Samba*, проверьте, правильно ли разрешены записи *SRV*.

```
C:\> nslookup.exe
> set type=srv
> _ldap._tcp.msnet.murom
> _kerberos._tcp.msnet.murom
> exit
```

Настройка двухсторонних транзитивных доверительных отношений

Добавьте доверительные отношения командой:

```
samba-tool domain trust create msnet.murom --type=forest --direction=both --create-location=both -U admin@msnet.murom

LocalDomain Netbios[SKYNET] DNS[skynet.murom] SID[S-1-5-21-3278458734-1377290257-482432228]
RemoteDC Netbios[DC] DNS[dc.msnet.murom] ServerType[PDC, GC, LDAP, DS, KDC, TIMESERV, CLOSEST, WRITABLE, GOOD_TIMESERV,
FULL_SECRET_DOMAIN_6, SERVICE, DS_8, __unknown_00008000__]
```

где:

- `--type=external` - указывает тип доверительного отношения, может принимать значения *external* и *forest*.
    - **external** (внешнее) - означает, что доверительное отношение будет создано с внешним доменом;
    - **forest** (лес) - указывает, что доверительное отношение будет создано с другим лесом. В этом случае, доверительное отношение будет устанавливаться между вашим лесом и другим лесом.
- `--direction=incoming` - определяет направление доверительного отношения. Значение **incoming** указывает, что доверительное отношение будет установлено только для входящих запросов, и ваш сервер Samba будет доверять внешнему домену MS при получении запросов от него;
- `--create-location=local` - указывает место создания доверительного отношения. Значение **local** означает, что доверительное отношение будет создано локально на вашем сервере Samba, и ваш сервер Samba будет инициировать процесс создания доверительного отношения с внешним доменом MS;
- `--direction=both` - доверительное отношение будет устанавливаться в обоих направлениях. Ваш сервер Samba будет доверять другому лесу, и взаимно другой лес будет доверять вашему лесу. Таким образом, обе стороны смогут обмениваться аутентификационной информацией и ресурсами;
- `--create-location=both` - указывает, что доверительное отношение будет создаваться и на вашем сервере Samba, и на другом сервере в другом лесу. Таким образом, создание доверительного отношения происходит с обеих сторон, что обеспечивает взаимное доверие и возможность обмена информацией.

При появлении запроса введите пароль администратора. Если все настроено верно, будет установлено доверие к домену *AD*.

```
Password for [Admin@msnet.murom]:
RemoteDomain Netbios[MSNET] DNS[msnet.murom] SID[S-1-5-21-2219352354-104895378-3667193527]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Validating outgoing trust...
OK: LocalValidation: DC[\\dcms.msnet.murom] CONNECTION[WERR_OK] TRUST[WEER_OK] VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dcms.skynet.murom] CONNECTION[WERR_OK] TRUST[WEER_OK] VERIFY_STATUS_RETURNED
Success.
```

Проверить установленные доверительные отношения можно командой:

```
samba-tool domain trust show msnet.murom

LocalDomain Netbios[SKYNET] DNS[skynet.murom] SID[S-1-5-21-3278458734-1377290257-482432228]
TrustedDomain:

NetbiosName:MSNET
DnsName:msnet.murom
SID:   S-1-5-21-3278458734-1377290257-482432228
Type:    0x2 (UPLEVEL)
Direction:  0x3 (BOTH)
Attributes:   0x4 (QUARANTINED_DOMAIN)
PosixOffset:   0x00000000 (0)
```

```
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96)
```

Если между **samba** и **windows** установлены двухсторонние доверительные отношения с типом связи **Лес**, то рабочую станцию с РЕД ОС нужно вводить в домен **samba** через **winbind**.

Для ввода компьютера в домен Samba используйте следующую команду, которая введет ПК в домен через **windind**:

```
join-to-domain.sh -d  <ваш_домен_samba> -n  <имя_пк> -u  <имя_администратора_samba> -w
```

Если планируется создать односторонние доверительные отношения между Samba и Windows, то для этого на сервере Samba используется команда:

```
samba-tool domain trust create msnet.murom -U admin@msnet.murom
```

При такой связи устанавливаются не транзитивные доверительные отношения (*External Trust*) между двумя доменами Samba и Windows из разных лесов.

Ввод клиентских машин в домен SAMBA

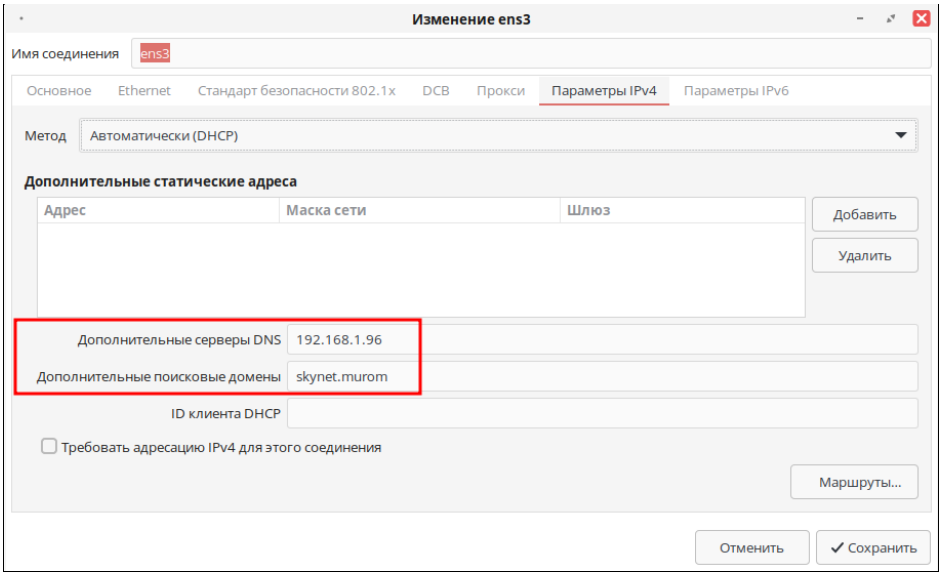
Предварительная подготовка компьютера к вводу в домен
Графический режим работы программы ввода РЕД ОС в домен SAMBA
Терминальный режим работы программы ввода РЕД ОС в домен SAMBA
Вывод РЕД ОС из домена SAMBA

Ввод РЕД ОС в домен **SAMBA** аналогичен вводу РЕД ОС в домен Windows, который описан в разделе «Ввод РЕД ОС в MS Active Directory».

Предварительная подготовка компьютера к вводу в домен

Важное условие для ввода в домен *SAMBA* – это доступность домена и контроллеров домена по их именам (**FQDN**). Обычно сетевые настройки распространяются через DHCP-сервер и сетевой карте вместе с IP-адресом присваивается DNS-сервер, а также поисковый домен.

Если необходимо указать другие настройки DNS и поискового домена, это можно выполнить в настройках сетевого соединения и указать свои значения DNS. Пример сетевых настроек:



Перед вводом в домен необходимо убедиться, что контроллер домена доступен с клиентского ПК, а в настройках сетевой карты назначен DNS-сервер домена.

Команда `nmcli` покажет действующие сетевые настройки:

```
nmcli

...
DNS configuration:
      servers: 192.168.1.96
      domains: skynet.murom
      interface: ens3
```

Для проверки доступности контроллера домена можно запустить команду `ping` и передать ей имя контроллера, например:

```
ping -c 3 dc1.skynet.murom

PING dc1.skynet.murom (192.168.1.96) 56(84) bytes of data.
64 bytes from 192.168.1.96 (192.168.1.96): icmp_seq=1 ttl=64 time=0.969 ms
64 bytes from 192.168.1.96 (192.168.1.96): icmp_seq=2 ttl=64 time=0.908 ms
64 bytes from 192.168.1.96 (192.168.1.96): icmp_seq=3 ttl=64 time=0.965 ms

--- dc1.skynet.murom ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.908/0.947/0.969/0.027 ms
```

Примечание.

Обращаем внимание, что «пинговать» нужно **имя**, а не IP-адрес, так вы сможете проверить, что на клиенте правильно обрабатываются DNS-имена домена.

Теперь можно приступить к вводу РЕД ОС в домен *SAMBA*.

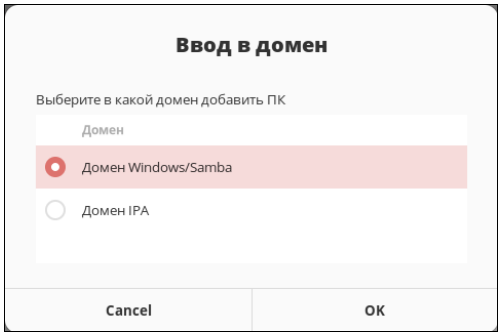
Графический режим работы программы ввода РЕД ОС в домен SAMBA

В РЕД ОС для быстрого ввода компьютера в домен SAMBA используется утилита join-to-domain. Утилита может быть запущена в консольном (текстовом) и в графическом режиме. Описание работы **join-to-domain** в консоли будет рассмотрено ниже.

Для запуска **join-to-domain** в графическом режиме откройте «**Главное меню**» - «**Системные**» - «**Ввод ПК в домен**».

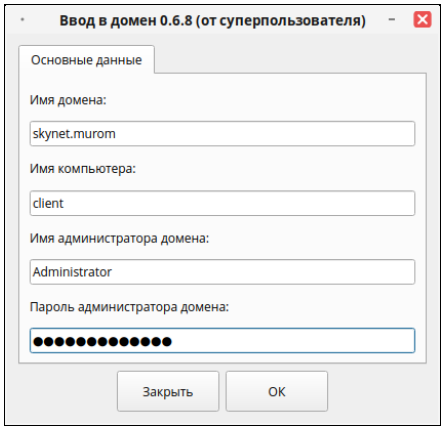
Запуск программы требует ввода пароля от пользователя **root**.

После успешной аутентификации откроется окно выбора типа домена на базе *SAMBA* или *FreeIPA*. Для ввода в домен SAMBA выберите пункт «**Домен Windows/SAMBA**».



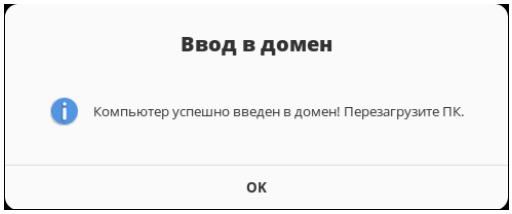
Будет открыто окно, в котором необходимо заполнить поля:

- имя домена;
- имя компьютера (это новое имя данного ПК);
- имя администратора домена;
- пароль администратора.



После нажатия на кнопку «**Да**» начнется процесс присоединения ПК к домену.

В случае успешного ввода в домен появится уведомление:



Перезагрузите компьютер и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

Процесс ввода в домен, а также возможные ошибки при работе протоколируются в файл **/var/log/join-to-domain.log**.

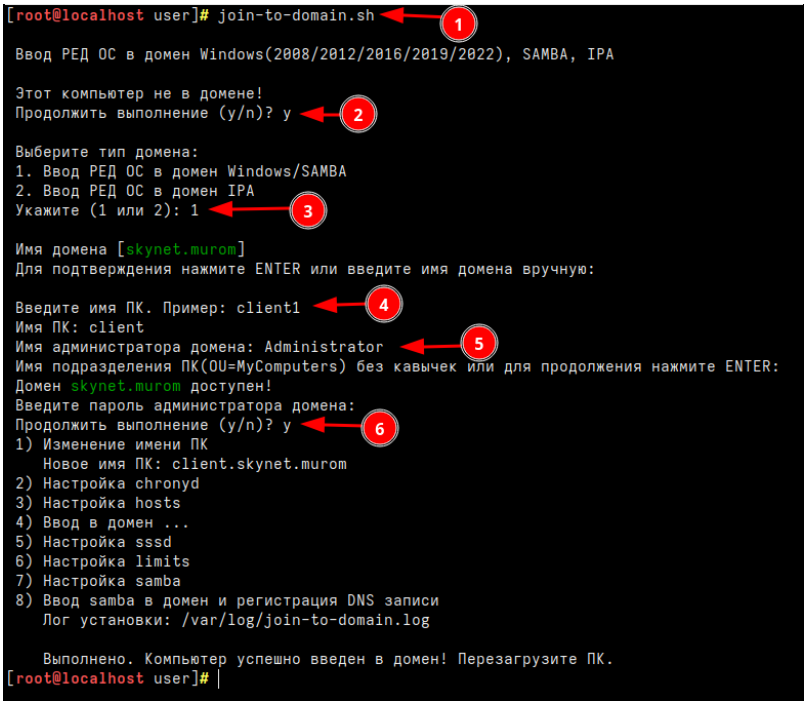
Терминальный режим работы программы ввода РЕД ОС в домен SAMBA

Откройте терминал и выполните запуск **join-to-domain.sh** с привилегиями суперпользователя **root**:

```
join-to-domain.sh
```

Программа запросит пользователя выбрать тип домена, к которому необходимо присоединить РЕД ОС, в данном случае необходимо выбрать первый пункт «**Ввод РЕД ОС в домен Windows/Samba**».

Введите имя домена, имя компьютера, имя администратора домена и подтвердите ваши действия для начала процесса ввода ПК в домен.



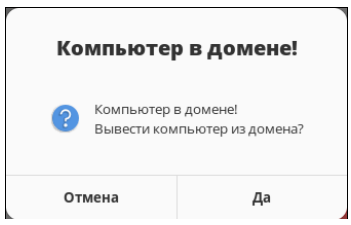
Перезагрузите ПК и войдите в РЕД ОС, используя *логин* и *пароль* пользователя домена.

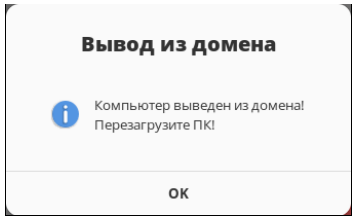
Протокол ввода в домен записывается в файл **/var/log/join-to-domain.log**.

Вывод РЕД ОС из домена SAMBA

Для вывода ПК из домена *SAMBA* следует снова запустить **join-to-domain** из «**Главного меню**» - «**Системные**» - «**Ввод ПК в домен**».

В этот раз программа определит, что РЕД ОС введена в домен и предложит выйти из него.

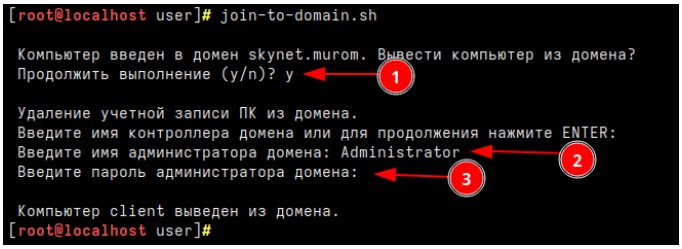




В режиме терминала вывод выполняется запуском команды с привилегиями суперпользователя **root**:

```
join-to-domain.sh
```

Если компьютер введен в домен, **join-to-domain** это обнаружит и предложит вывести его из домена.



Управление пользователями и группами в домене SAMBA DC

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** samba 4.15.9-2h

Управление пользователями и группами

Список пользователей:

```
samba-tool user list
```

Создадим пользователя в Active Directory и делаем тесты:

```
samba-tool user create PetrovDA
```

или

```
smbpasswd -a USERNAME
smbpasswd -e USERNAME
```

- **username** - имя нового пользователя в AD;
- ключ **-a** - создает пользователя;
- ключ **-e** - активирует пользователя

Удаление пользователя:

```
samba-tool user delete PetrovDA
```

Изменение пароля пользователя:

```
samba-tool user setpassword PetrovDA
```

Отключить пользователя:

```
samba-tool user disable PetrovDA
```

Список групп:

```
samba-tool group list
```

Добавление группы:

```
samba-tool group add MyGroup
```

Удаление группы:

```
samba-tool group delete MyGroup
```

Добавление пользователя в группу:

```
samba-tool group addmembers MyGroup PetrovDA
```

Удаление пользователя из группы:

```
samba-tool group removemembers MyGroup PetrovDA
```

Проверка подключения к samba ресурсам

Вывести список сетевых ресурсов **samba**:

```
smbclient -L localhost -U%
```

Вывод команды:

```
smbclient -L localhost -U%

members MyGroup PetrovDA
Sharename Type Comment
--------- ---- -------
netlogon Disk
sysvol Disk
IPC$ IPC IPC Service (Samba 4.15.9)
Reconnecting with SMB1 for workgroup listing.
Server Comment
--------- -------
Workgroup Master
```

Проверьте вход с помощью учетной записи администратора домена:

```
smbclient //localhost/netlogon -U Administrator -c 'ls'

Enter SKYNET\Administrator's password:
. D 0 Sun Nov 4 10:56:52 2018
..D 0 Sun Nov 4 10:56:57 2018
6486016 blocks of size 1024. 4496892 blocks available
```

Проверьте выдачу билета керберос:

```
kinit administrator@SKYNET.MUROM
klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SKYNET.MUROM
Valid starting Expires Service principal
04.11.2018 12:03:05 04.11.2018 22:03:05 krbtgt/SKYNET.MUROM@SKYNET.MUROM
renew until 05.11.2018 12:02:56
```

Просмотр пользователей:

```
wbinfo -u
```

Просмотр групп:

```
wbinfo -g
```

Доступ к предыдущим версиям файлов с помощью shadow_copy

На время настройки сервиса переведите selinux в режим уведомлений. Для этого измените содержимое конфигурационного файла:

```
nano /etc/selinux/config
```

Заменив текст `SELINUX=enforcing` на `SELINUX=permissive`
Выполните:

```
setenforce 0
```

Более подробно см.ссылку
Не забудьте включить selinux после завершения настройки.

Процедура настройки «теневых копий» делится на две части:

- предоставление клиентам Microsoft Shadow Copy возможности просматривать снимки файловой системы как «теневые копии» в сетевых каталогах Samba;
- механизм создания «теневых копий».

Настройка в samba механизма «теневых копий»

Samba позволяет вам организовать хранение предыдущих версий файла так, чтобы они были доступны механизму учёта предыдущих версий в Windows. Для этого предназначен специальный модуль `vfs object` с именем **shadow_copy2**. Для активации этого механизма со стороны Samba просто добавьте в блок, описывающий нужную вам шару, несколько строк. Для примера создадим шару **secure**. Добавьте в её блок параметр, активирующий **shadow_copy2**, и параметр **shadow:snapdir**, указывающий, где будут храниться снапшоты. В данном случае, они будут храниться в скрытом каталоге с именем самой шары.

```
[secure]

 vfs objects = shadow_copy2
 shadow:snapdir = /srv/.share
 path = /srv/share
 valid users = @secure
 guest ok = no
 writable = yes
 browsable = yes
```

Теперь добавьте настройки в секции `[global]`:

```
[global]

 wide links = yes
 unix extensions = no
 allow insecure wide links = no
```

- `wide links` разрешает samba проходить по символьным ссылкам;
- `unix extensions =` запрещает *nix клиентам создание символьных ссылок (и еще несколько возможностей, которые вам могут не понадобиться);
- `allow insecure wide links` — эту опцию включаем в `yes` только при включенных `unix extensions`, иначе `wide links` останутся недоступны.

На этом настройку можно закончить. Дополнительные параметры приведены на сайте samba.org и доступны по ссылке.

Пример настройки файлового хранилища SAMBA

Графический вариант
Работа из файлового менеджера
Консольный вариант

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** Samba 4.15.9, share_directory 6.0-1

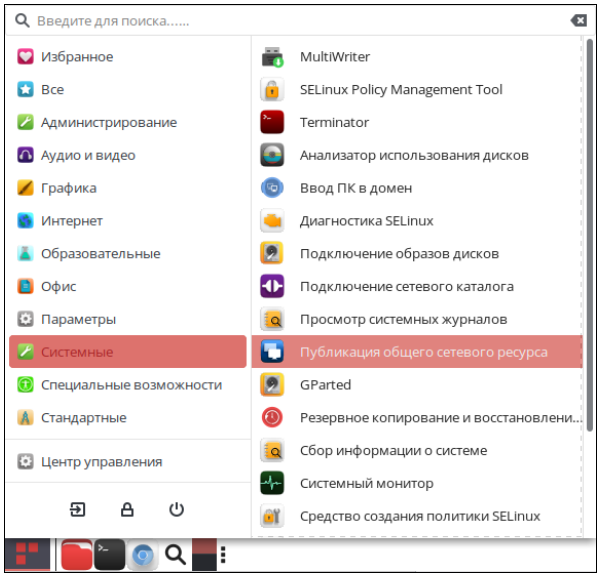
Графический вариант

Для публикации сетевого ресурса в рабочей группе в РЕД ОС доступна специальная утилита share_directory.

Установите утилиту командой:

```
dnf install share_directory
```

Запуск утилиты доступен через главное меню:

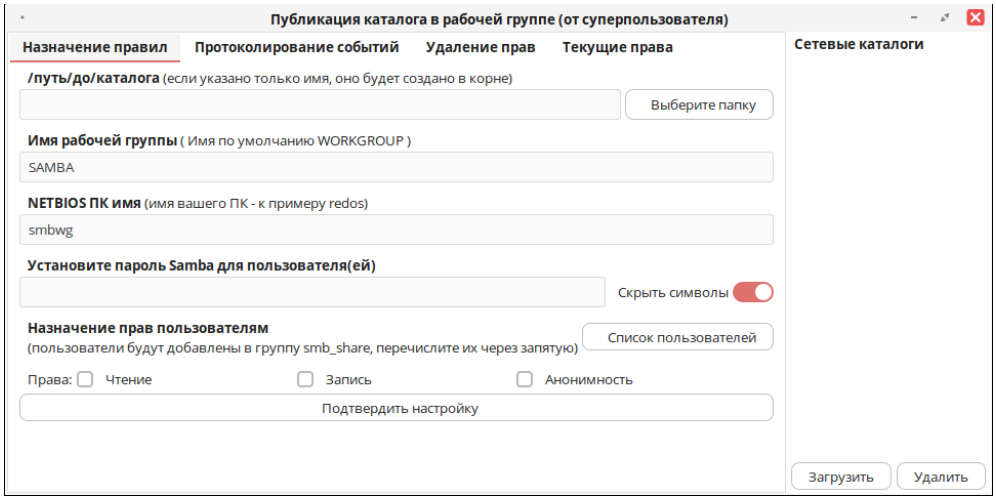


или через терминал:

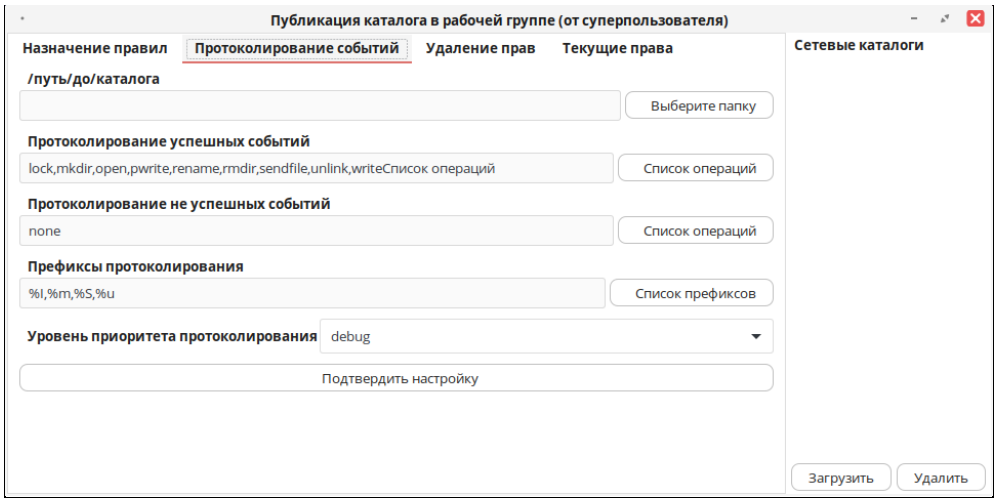
```
share-directory
```

Для того чтобы был запущен вариант утилиты по работе с рабочей группой, ПК не должен находиться в домене, в ином случае утилита запустится в режиме, указанном в данной инструкции «Каталог общего сетевого доступа на РЕД ОС в домене Windows» .

Для ***публикации*** сетевого ресурса в рабочей группе требуется задать путь к директории, задать Samba пароль и выбрать разрешенных пользователей с назначением соответствующих им прав.

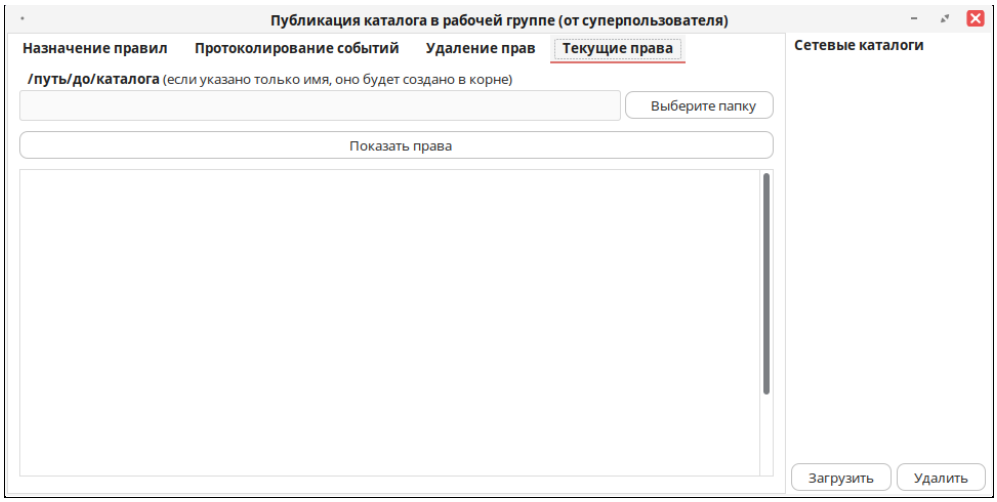


Для того чтобы назначить ***протоколирование событий*** директории, требуется указать путь к ресурсу и необходимые атрибуты.



Для того чтобы ***удалить права*** с директории, требуется указать путь к ресурсу и прописать определенного пользователя, которого требуется удалить. Также доступно полное удаление прав с директории.

Для удобства ***отслеживания прав*** можно посмотреть текущие права директории, указав путь к интересующей.



Работа из файлового менеджера

Для включения быстрой настройки сетевой директории из файлового менеджера **caja** необходимо установить дополнительное расширение. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install share_directory-caja
```

Выйдите из учетной записи **root** командой:

```
exit
```

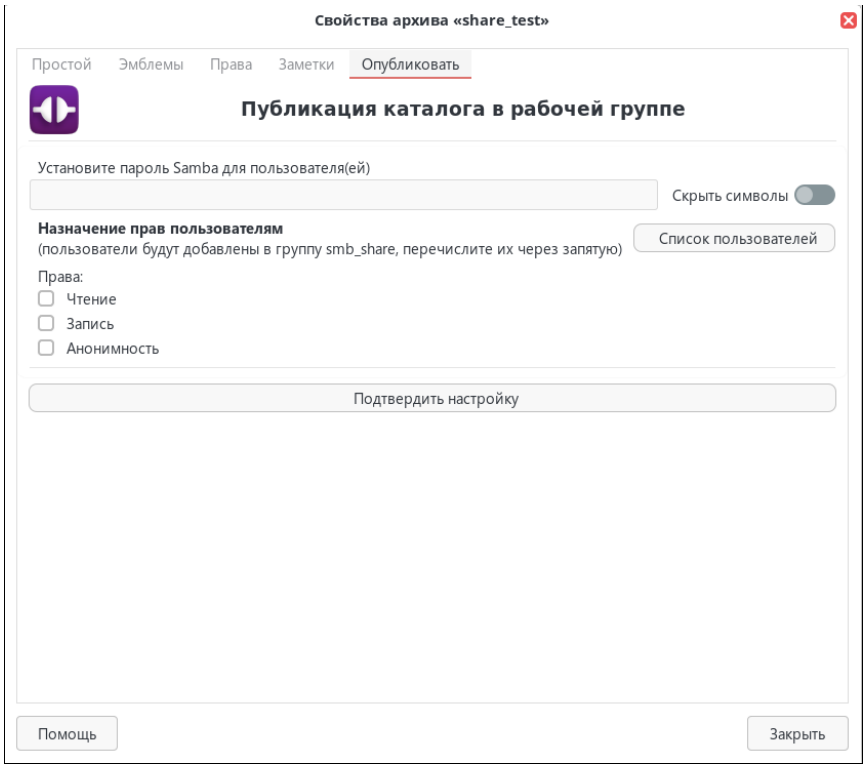
Затем обновите конфигурацию **caja** от имени **локального** пользователя:

```
[ "$EUID" -ne 0 ] && caja -q || echo "Команда не должна выполняться с правами пользователя root!"
```

Или выполните выход из учетной записи пользователя и обратную авторизацию.

После обновления списка расширений **caja** станет доступен новый пункт в свойствах директории.

Вызовите контекстное меню правой кнопкой мыши для необходимой директории в файловом менеджере, затем выберите пункт «**Свойства**» – «**Опубликовать**».



Далее потребуется назначить необходимые атрибуты доступа для директории и выбрать подтверждение настройки.

Консольный вариант

Данная конфигурация будет содержать общую папку obmen, в которую будут иметь доступ авторизованные пользователи. И каждый пользователь будет иметь свою папку, которая доступна только ему и администратору сервера.

Реализация

Автоматически права на пользовательские каталоги и файлы выставляются в 775, что означает – разрешать записывать читать и выполнять файлы только пользователю и группе, остальным только чтение.

Каждый новый пользователь включается в группу администратора для того, что бы он мог редактировать изменения администратора. Так же включаются в общую группу для доступа к общей папке. Администратор при создании новых пользователей включается в их группу для возможности редактирования файлов и каталогов пользователя. В каждый пользовательский сетевой каталог разрешается доступ пользователю и администратору.

Автоматически права на каталоги и файлы в общем каталоге выставляются в 777, что означает – все пользователи могут читать, записывать и выполнять файлы. Доступ к общей папке разрешается общей группе и администратору.

Создайте общий каталог.

```
mkdir /srv/obmen
```

Создайте приватный каталог пользователя:

```
mkdir /srv/user1
```

Создайте пользователя **user1** и **adminsmb**:

```
useradd -d /dev/null -s /usr/sbin/nologin user1
useradd -d /dev/null -s /usr/sbin/nologin adminsmb
```

Задайте пароль пользователю **user1** и adminsmb:

```
smbpasswd -a user1
smbpasswd -a adminsmb
```

Создайте общую группу пользователей:

```
groupadd obmen
```

Добавьте пользователя **user1** в группу **obmen**. Последующих пользователей также добавляйте в эту группу. Это позволит им подключаться к общей сетевой папке **obmen**. Пользователя **adminsmb** в группу пользователя **user1**.

```
usermod -a -G obmen user1
usermod -a -G user1 adminsmb
```

Проверьте успешное добавление:

```
groups user1
```

Установите группу **obmen** в качестве владельца папки **/srv/obmen** и предоставьте право на запись:

```
chown -R :obmen /srv/obmen
chmod 777 /srv/obmen
```

Так же установите права и группу на каталог пользователя **user1**.

```
chown -R user1 /srv/user1
chmod 777 /srv/user1
```

Проверить права и владельцев можно следующей командой:

```
ll /srv/
```

Настройка Selinux

SELinux позволяет **Samba** читать и записывать файлы, помеченные типом **samba_share_t**, если файл **/etc/samba/smb.conf** и разрешения Linux установлены соответствующим образом. Введите следующую команду от имени пользователя **root**, чтобы добавить изменение метки в конфигурацию файлового контекста.

```
semanage fcontext -a -t samba_share_t "/srv/obmen(/.*)?"
```

Используйте утилиту restorecon от имени пользователя **root**, чтобы применить изменения метки:

```
restorecon -R -v /srv/obmen
```

Повторите эти действия для остальных каталогов.

Настройка файла конфигурации SAMBA

В файл **/etc/samba/smb.conf** добавьте разделы для созданных сетевых папок.

```
nano /etc/samba/smb.conf
```

```
[global]
workgroup = WORKGROUP # имя рабочей группы
server string = Samba Server %v # описание сервера
netbios name = redos #netbios-имя сервера
security = user
passdb backend = tdbsam
# Создаем лог файл
log file = /var/log/samba/log.%m
max log size = 50

[obmen]
comment = Obmen share with authenticated access
path = /srv/obmen
browsable = yes
writable = yes
guest ok = no
valid users = @obmen adminsmb # указываем группу и конкретное имя пользователя для доступа
force directory mode = 0777
force create mode = 0676
vfs objects = full_audit

[user1]
comment = Private share with user #описание общей папки
path = /srv/user1
browsable = yes # «yes» — означает, что общая папка не будет скрытой
writable = yes # общая папка доступна для записи
guest ok = no # разрешен ли гостевой доступ
valid users = user1 adminsmb # указываем доступ для пользователей
force directory mode = 0775
force create mode = 0674
```

Перезагрузите службу **samba** для вступления изменений в силу.

```
systemctl restart smb
systemctl enable smb
```

Алгоритм создания новых пользователей

Создайте приватный каталог:

```
mkdir /srv/user2
```

Создайте самого пользователя:

```
useradd -d /dev/null -s /usr/sbin/nologin user2
```

Задайте пароль пользователю:

```
smbpasswd -a user2
```

Добавьте созданного пользователя в группу **obmen** и пользователя **adminsmb** в группу созданного пользователя.

```
usermod -a -G obmen user2
usermod -a -G user2 adminsmb
```

Так же установите права и группу на каталог пользователя.

```
chown -R user2. /srv/user2
chmod 777 /srv/user2
```

В файл **/etc/samba/smb.conf** добавьте раздел для созданной сетевой папки.

```
nano /etc/samba/smb.conf
```

```
[user2]
comment = Private share with user
path = /srv/user2
browsable = yes
writable = yes
guest ok = no
valid users = user2 adminsmb
force directory mode = 0775
force create mode = 0674
```

Перезагрузите службу **samba** для вступления изменений в силу.

```
systemctl restart smb
```

Анонимный доступ

- Создадим папку **/srv/guest** и настроим ее для анонимного доступа.

```
mkdir /srv/guest
```

- Назначим пользователя и группу **nobody** владельцем и группой для папки **/srv/guest**. Данный пользователь и группа автоматически присваиваются **samba** анонимным пользователям.

```
chown -R nobody:nobody /srv/guest
```

- Укажем права на директорию, разрешающие пользователю и группе читать и писать в папку.

```
chmod 775 /srv/guest
```

- Настройте конфигурацию **samba**. Файл конфигурации samba находится в **/etc/samba/smb.conf**. Он состоит из разделов. Приведите его к следующему виду:

```
[global]
workgroup = WORKGROUP
server string = Samba Server %v
netbios name = redos
security = user
passdb backend = tdbsam
# Опция bad user означает, что доступ будет предоставлен от имени пользователя nobody
map to guest = bad user

[guest]
comment = Share with anonymous access
path = /srv/guest
browsable = yes
writable = yes
guest ok = yes
```

Настройка Selinux для анонимного доступа:

```
semanage fcontext -a -t samba_share_t "/srv/guest(/.*)?"
restorecon -R -v /srv/guest
```

Каталог общего сетевого доступа на РЕД ОС в домене MSAD

Графический вариант
Работа из файлового менеджера
Консольный вариант

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: share_directory 6.0-1

Рассмотрен механизм создания в РЕД ОС каталога с общим сетевым доступом по протоколу smb. РЕД ОС предварительно необходимо включить в домен *MS AD* согласно инструкциям текущего раздела «Работа с доменом MS AD».

Графический вариант

Утилита публикации сетевого ресурса в домене *Samba / MS AD* доступна в РЕД ОС.

Установите утилиту командой:

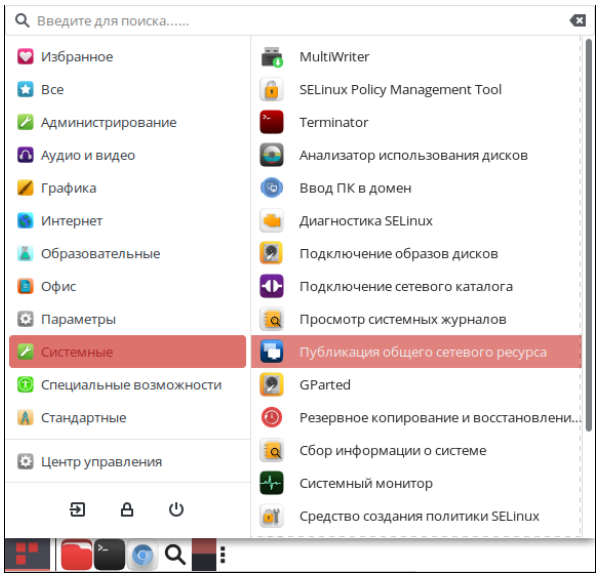
```
dnf install share_directory
```

От имени **root**-пользователя получите **kerberos ticket**:

```
su -
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

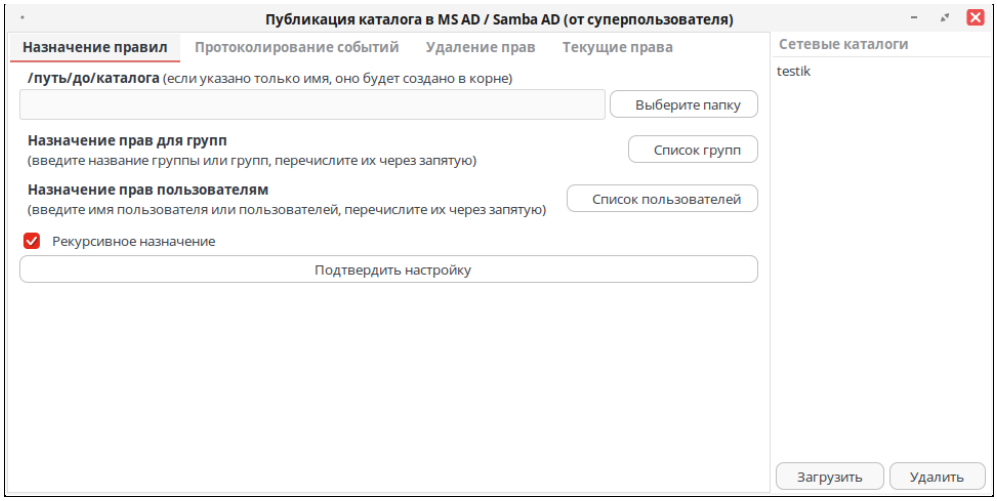
Запуск утилиты доступен через главное меню:



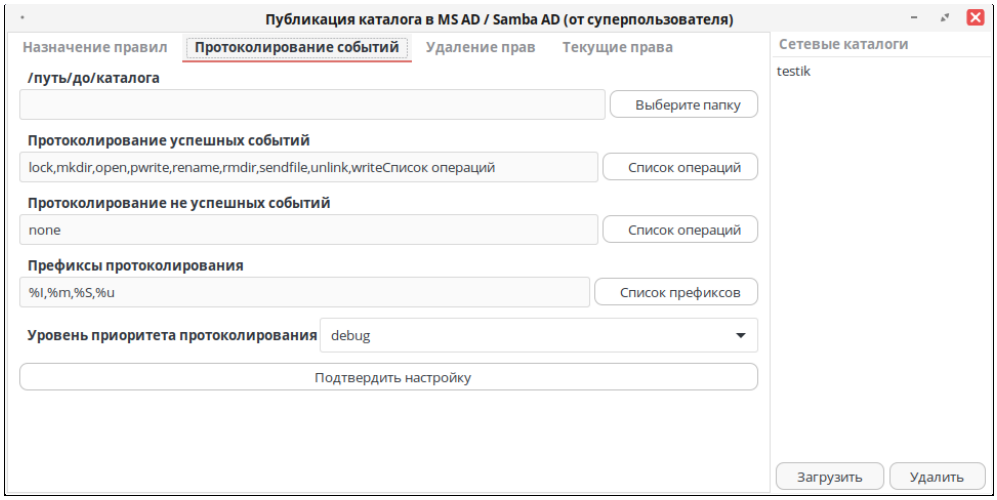
или через терминал:

```
share-directory
```

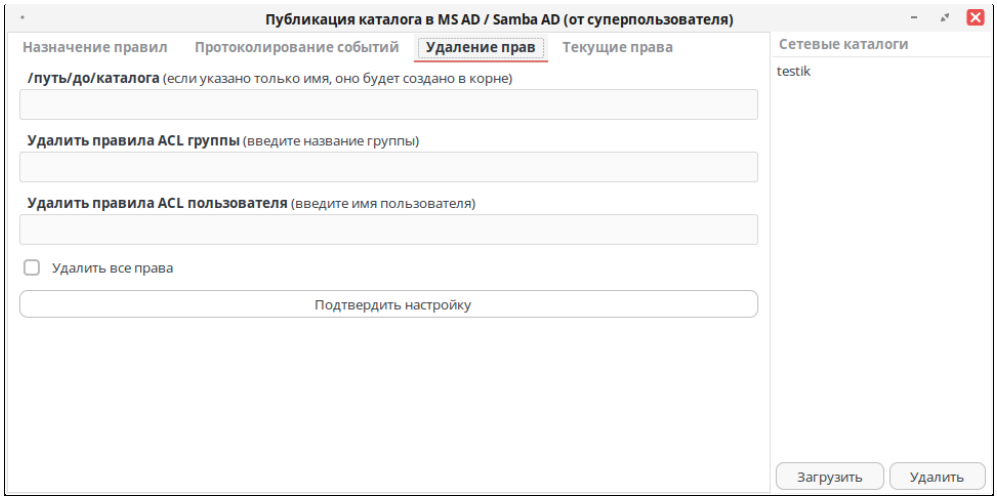
Для публикации сетевого ресурса в домене требуется задать путь к директории, пользователей и/или групп и соответствующие им права.



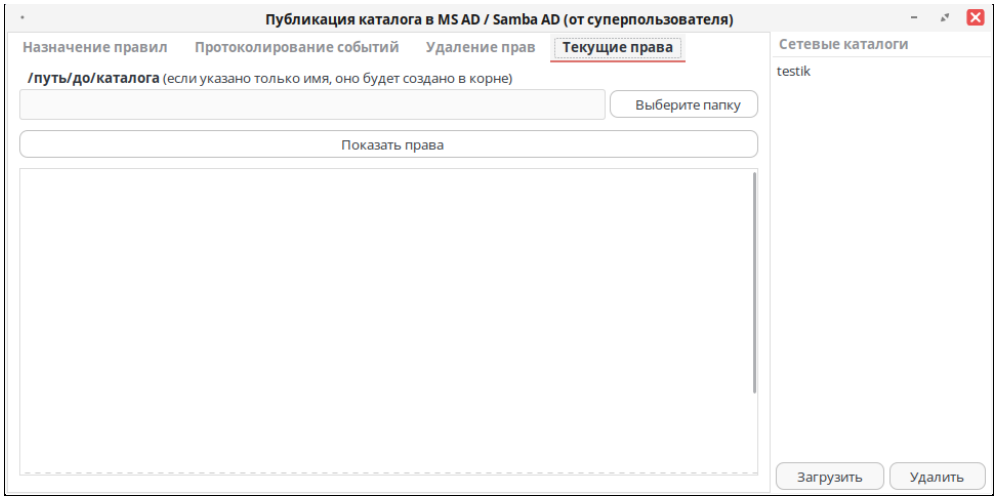
Для протоколирования событий предусмотрена соответствующая вкладка.



Для того чтобы *удалить права* с директории, требуется указать путь к ресурсу и прописать определенного пользователя или группу, которых требуется удалить. Так же доступно полное удаление ACL-прав с директории.



Для удобства *отслеживания прав* можно посмотреть текущие права директории, указав путь к интересующей.



Работа из файлового менеджера

Для включения быстрой настройки сетевой директории из файлового менеджера **caja** необходимо установить дополнительное расширение. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install share_directory-caja
```

Затем получите **kerberos ticket**:

```
kinit USERNAME
```

где вместо **USERNAME** - имя вашего пользователя.

Выйдите из учетной записи **root** командой:

```
exit
```

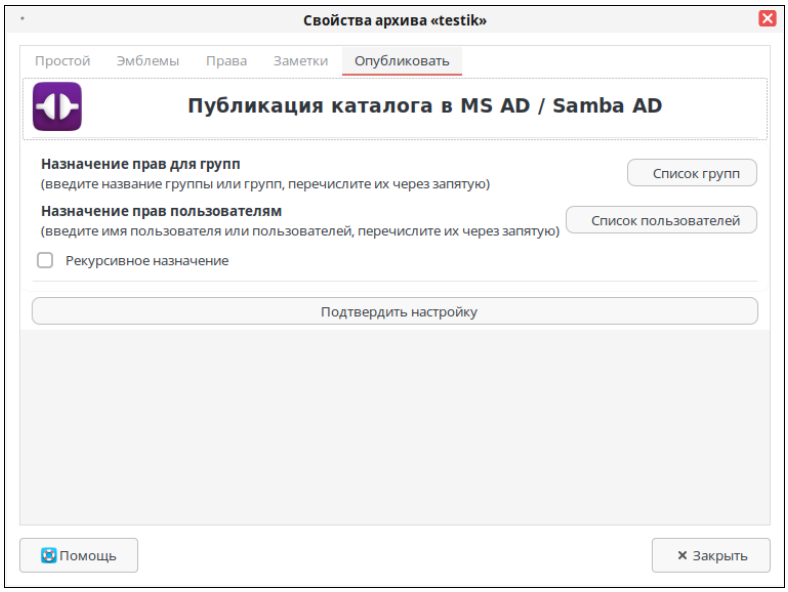
Затем обновите конфигурацию **caja** от имени **локального** пользователя:

```
caja -q
```

Или выполните выход из учетной записи пользователя и обратную авторизацию.

После обновления списка расширений **caja** станет доступен новый пункт в свойствах директории.

Вызовите контекстное меню правой кнопкой мыши для необходимой директории в файловом менеджере, затем выберите пункт «**Свойства**» – «**Опубликовать**».



Консольный вариант

Примечание.

Предполагается, что рабочая станция введена в домен посредством утилиты **join-to-domain** с выбором **sssd**.

Все указанные действия производятся от имени **суперпользователя** (**root**).

1. Добавьте параметр winbind в конце строк, начинающихся с group, passwd и shadow, в файле профиля *authselect* **/etc/authselect/custom/sssd_domain/nsswitch.conf** командой:

```
sed -i_bak '/^\(group:\|passwd:\|shadow:\)/ {s/\(winbind \)\(.*\)$/\2 winbind/; /winbind/ ! s/$/ winbind/}'
/etc/authselect/custom/sssd_domain/nsswitch.conf
```

2. Примените изменения профиля *authselect* командой:

```
authselect apply-changes
```

3. Проверьте возможность получения *kerberos*-билета для доменного пользователя:

```
kinit username
klist
```

4. Проверьте доступность входа доменного пользователя в систему:

```
su username
exit
```

5. Создайте каталог для общего доступа:

```
mkdir -p /share/
```

6. Назначьте права доступа. Пример для домена *wintest*:

```
chown -R root:"wintest\Пользователи домена" /share
chmod 2770 /share
setfacl -m default:group:"wintest\Администраторы домена":rwx /share/
setfacl -m default:group:"wintest\Пользователи домена":r-x /share/
setfacl -m default:other::--- /share/
```

В данном примере с помощью команды **setfacl** были выданы полные (rwx) права группе «**Администраторы домена**» на каталог **/share**.

Группе «**Пользователи домена**» домена *wintest* были выданы права только на чтение и выполнение (просмотр содержимого каталога).

7. Настройте политику *SELinux* для общего каталога и примените её:

```
semanage fcontext -a -t samba_share_t "/share(/.*)?"
restorecon -R -v /share
```

8. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) в секции [global] проверьте наличие следующих строк:

```
vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab
```

9. В конфигурационном файле *samba* (**/etc/samba/smb.conf**) создайте раздел настроек общего ресурса [share] (с этим именем ресурс будет отображаться для клиентов):

```
[share]
path = /share/
read only = no
browseable = yes
create mask = 0664
directory mask = 0775
```

10. Дополнительная настройка прав:

- установить полные права на каталог для группы:

```
setfacl -m g:"wintest\Группа_Пользователей":rwx /share
```

- установить полные права на каталог для пользователя:

```
setfacl -m u:"wintest\Пользователь":rwx /share
```

- удалить ACL для определённого пользователя:

```
setfacl -x u:alex /share
```

- удалить все ACL-права каталога:

```
setfacl -b /share
```

- просмотреть ACL-права на каталог:

```
getfacl /share
```

Подробное описание списков контроля доступа (ACL) и параметров команды **setfacl** доступно в нашей статье «Списки контроля доступа ACL»

11. Установите автоматический запуск служб *samba*:

```
systemctl enable smb --now
systemctl enable nmb --now
systemctl enable winbind --now
```

12. Перезагрузите рабочую станцию. Проверьте статус служб:

```
systemctl is-failed smb
systemctl is-failed nmb
systemctl is-failed winbind
```

При корректной настройке каждая команда должна вывести сообщение «active».

Интеграция файлового сервера SAMBA с IPA

Установка необходимых пакетов на сервере SAMBA
Настройка серверов IPA и Samba
Настройка сетевого каталога на сервере Samba

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: ipa-client-4.10.3-6, samba-4.19.2-2h

Установка необходимых пакетов на сервере SAMBA

Для установки пакетов **samba** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install ipa-client sssd-common samba samba-client ipa-client-samba
```

Установите имя хоста samba-сервера:

```
hostnamectl set-hostname samba.redosipa.ru
```

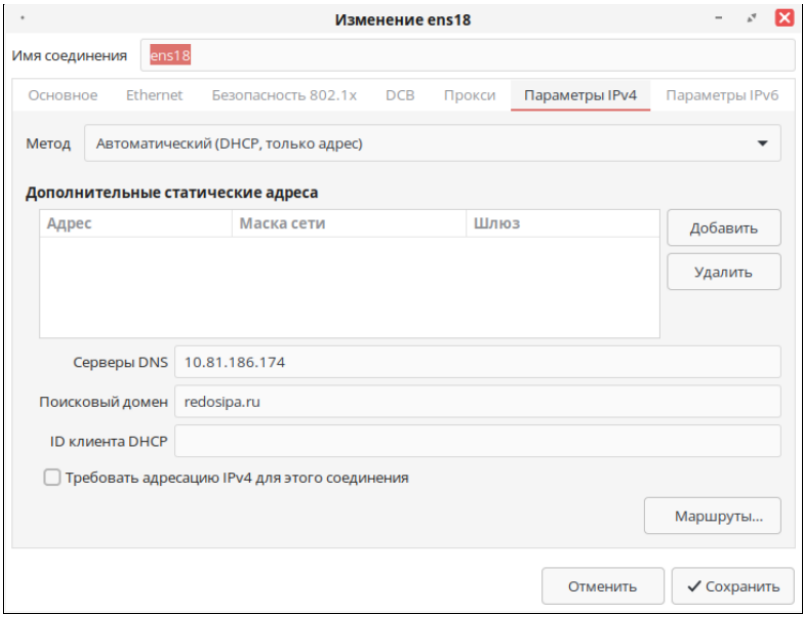
Добавьте запись в **/etc/hosts**, по какому IP обращаться к домену IPA, например:

```
10.81.186.174 server.redosipa.ru
```

Отключите службу:

```
systemctl disable --now systemd-timesyncd
```

В сетевых настройках укажите поисковый DNS IPA-сервера, например:



Присоедините файловый сервер к домену IPA:

```
join-to-domain.sh
```

Выполните автоматическую конфигурацию системных служб на сервере **samba** для работы в домене IPA:

```
authselect select sssd with-fingerprint with-gssapi with-mkhomedir with-smartcard --force
```

Настройка серверов IPA и Samba

Для правильного распределения DNS выполните следующие команды на сервере IPA:

```
kinit admin
ipa dnsrecord-add redosipa.ru --a-rec=samba --a-ip-address=10.81.186.124
```

Запустите настройку домена для обработки классов и атрибутов объектов, специфичных для **Samba**:

```
ipa-adtrust-install --add-sids
reboot
```

На сервере **samba** выполните ipa-client-samba, который создаст **cifs** и отредактирует **/etc/samba/smb.conf** для работы *samba* с **ipa**:

```
ipa-client-samba
```

Отредактируйте в файле **/etc/samba/smb.conf** значение netbios name, указав рабочую группу домена, в данном случае **smb.conf** будет выглядеть следующим образом:

```
...
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 ...
```

Далее отредактируйте секции по примеру из **smb.conf**:

```
[global]
 max smbd processes = 1000
 dedicated keytab file = FILE:/etc/samba/samba.keytab
 kerberos method = dedicated keytab
 log file = /var/log/samba/log.%m
 log level = 1
 server role = member server
 realm = REDOSIPA.RU
 netbios name = REDOSIPA
 workgroup = REDOSIPA
 idmap config * : range = 0 - 0
 idmap config * : backend = tdb


 idmap config REDOSIPA : range = 14000000 - 14199999
 idmap config REDOSIPA : backend = sss

 security = ads
 printing = cups
 printcap name = cups
 load printers = yes
 cups options = raw

 [homes]
 read only = no
 comment = Home Directories
 valid users = %S, %D%w%S
 browseable = No
 read only = No
 inherit acls = Yes
```

```
[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775
```

Создайте структуру ролей и привилегий для **samba**. Действия выполняются на контроллере домена **ipa**:

```
ipa permission-add "CIFS server can read user passwords" --attrs={ipaNTHash,ipaNTSecurityIdentifier} --type=user --right=
{read,search,compare} --bindtype=permission
ipa privilege-add "CIFS server privilege"
ipa privilege-add-permission "CIFS server privilege" --permission="CIFS server can read user passwords"
ipa role-add "CIFS server"
ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
ipa role-add-member "CIFS server" --services=cifs/samba.redosipa.ru
```

На samba-сервере внесите изменения в **/etc/krb5.conf**:

```
sed -i 's;default_ccache_name = KEYRING:persistent:%{uid};default_ccache_name = FILE:/tmp/krb5cc_%{uid};g' /etc/krb5.conf
```

Получите тикет и создайте **keytab**:

```
kinit admin
ipa-getkeytab -s server.redosipa.ru -p cifs/samba.redosipa.ru -k /etc/samba/samba.keytab
reboot
```

Настройка сетевого каталога на сервере Samba

На samba-сервере создайте каталог:

```
mkdir -p /share/
```

Назначьте права на созданный каталог:

```
chown -R :users /share
chmod -R 777 /share
setfacl -m default:user:"admin":rwx /share
setfacl -R -m default:user:"admin":rwx /share
```

Затем настройте метки SELinux:

```
semanage fcontext -a -t samba_share_t /share/
restorecon -R -v /share/
```

На контроллере домена **IPA** получите SID:

```
net getdomainsid
```

На файловом сервере **samba** настройте идентификатор безопасности (введите SID, полученный ранее):

```
 net setdomainsid <SID>
```

На сервере **samba** выполните:

```
net -s /dev/null groupmap add sid=S-1-5-32-546 unixgroup=nobody type=builtin
```

В **/etc/samba/smb.conf** укажите настройки для каталога:

```
[share]
 path = /share
 writable = yes
 browsable=yes
 valid users = admin
 read list = admin
 write list = admin
 guest ok = no
 inherit acls = Yes
 create mask = 0660
 directory mask = 0770
```

Добавьте в автозапуск службы **samba** и **winbind**, перезагрузите сервер **samba**:

```
systemctl enable smb winbind --now
reboot
```

Для проверки доступности сетевого каталога на сервере **samba** необходимо получить тикет (если он отсутствует) и выполнить команду подключения к сетевому каталогу:

```
kinit admin
smbclient //samba.redosipa.ru/share -N --use-kerberos=required
```

В случае, если все настроено верно, появится следующее сообщение:

```
Try "help" to get a list of possible commands.
 smb: \>
```

Журналирование событий SAMBA

Настройка протоколирования событий, связанных с файловым хранилищем *samba*, является довольно важным вопросом. Рассмотрим случай, когда на файловом сервере присутствуют сетевые папки, для которых необходимо организовать запись действий, которые пользователи производят в данной папке.

За настройку журналирования действий *samba* отвечает конфигурационный файл **/etc/samba/smb.conf**.

Рассмотрим пример сетевой папки, имеющей в своем теле конфигурацию для протоколирования событий.

Секция сетевой папки:

```
[share_domain]
path = /share_domain/
read only = no
browseable = yes
vfs objects = full_audit
full_audit:prefix = %u|%I|%m|%S
full_audit:failure = none
full_audit:success = lock write pwrite mkdirat open sendfile unlinkat write renameat
full_audit:facility = local5
full_audit:priority = debug
```

Рассмотрим детально, что означают данные параметры:

В параметре **vfs objects** указывается модуль **full_audit**, на основе которого будет происходить протоколирование событий.

Запись **full_audit:prefix = %u|%I|%m|%S** представляет из себя набор тех данных, которые будут записываться в логи при определенных действиях пользователей в сетевой папке.

▸ **Полный список допустимых переменных**

Параметры:

full_audit:failure = none

full_audit:success = lock write pwrite mkdirat open sendfile unlinkat write renameat

отвечают за протоколирование действий в случае успешного выполнения операции или неуспешного. Допустимо использование **none** - т.е. отсутствие протоколирования событий или команд.

▸ **Полный список допустимых команд**

Параметры:

full_audit:facility = local5 - категория событий *syslog*, в которую будут попадать записи.

Для того чтобы каждая сетевая папка вела свои собственные логи, требуется указывать отличные друг от друга значения, т.е. **local5**, **local6**, **local7** и т.д.

full_audit:priority = debug - категория событий *syslog*, в которую будут попадать записи.

Доступные приоритеты: **notice**, **debug**, **alert**

Необходимо помнить, для того чтобы настройки вступили в силу, требуется перезапустить сервис:

```
sudo -E systemctl restart smb
```

Настройка ведения логов в определенный файл

За пути логов отвечает конфигурационный файл **/etc/rsyslog.conf**, в конец файла вписывается для каждой сетевой папки свой параметр **local4**, **local5**, **local6** и т.д.:

```
local5.debug -/var/log/samba/audit.log
```

Вместо **debug** необходимо указать тот режим, который был указан в параметре **full_audit:priority**.

Также для удобства ведения логов можно назвать файл логов идентично имени сетевой папки, т.е.:

```
local5.debug -/var/log/samba/share_dir.log
```

Для применения изменений потребуется перезапустить сервис командой:

```
sudo -E systemctl restart rsyslog
```

Настройка ротации логов

За ротации логов отвечает конфигурационный файл **/etc/logrotate.d/samba**.

По умолчанию в системе уже настроена ротация логов *Samba* и конфигурационный файл имеет следующее содержимое:

```
/var/log/samba/log.* {
    compress
    dateext
    maxage 365
    rotate 99
    notifempty
    olddir /var/log/samba/old
    missingok
    copytruncate
}
```

Рассмотрим, за что отвечают параметры:

- **compress** - сжатие данных;
- **dateext** - добавляет дату ротации перед заголовком старого лога;
- **maxage** - значение, отвечающее за удаление логов старше X дней;
- **rotate** - параметр отвечает за частоту ротаций логов через X дней;
- **notifyempty** - не сдвигать журнал, если он пуст;
- **olddir /var/log/samba/old** - параметр отвечающий, куда сохранять старые логи;
- **missingok** - в случае отсутствия файла журнала перейти к обработке следующего, не выдавая сообщения об ошибке;
- **copytruncate** - после создания копии обрезать исходный файл журнала взамен перемещения старого файла журнала и создания нового. Данный параметр применяется в том случае, когда некоторой программе нельзя указать закрыть её журнал, и таким образом можно постоянно продолжать запись (добавление) в существующий файл журнала.

Запустить ротацию логов можно следующей командой:

```
sudo -E logrotate -v -f /etc/logrotate.conf
```

Резервное копирование домена SAMBA DC

Резервное копирование типа online
Резервное копирование типа offline
Восстановление домена из файла резервной копии
Обновление пакетов
Отключение SELinux
Присваивание серверу доменного имени
Настройка сетевого интерфейса
Установка необходимых пакетов
Создание резервных копий файлов
Процесс восстановления домена из резервной копии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: samba-4.17.5-2h, krb5-devel-1.20.1-1, bind-32:9.16.27-1

Резервное копирование **Samba** обеспечивает восстановление домена в случае серьезного сбоя.

Примечание.

Если в качестве файлового сервера используется DC, необходимо создать резервную копию для хранимых данных отдельно.

Существует два типа резервного копирования:

- **online** – создает клон базы данных работающего DC. По функциональности процесс похож на подключение нового DC к сети. Резервное копирование может быть произведено удаленно;
- **offline** (или локальное) — создает копию локальных файлов Samba, которые расположены на диске. Включает в себя метаданные репликации, которые являются локальными для данного DC. Резервное копирование выполняется только локально. При этом резервное копирование может быть выполнено на DC как в работающем, так и в не работающем состоянии.

Резервное копирование типа **online** лучше всего подходит для обеспечения долгосрочной замены домена. Его также можно использовать в качестве временной замены, но будет недоступно одновременное устранение неполадок с вышедшими из строя контроллерами домена. Выяснение причин сбоя домена Samba может занять много времени и быть технически сложной работой. В случае критичного сбоя домена, когда нет необходимости исследовать проблему и требуется просто вернуться к старой копии рабочего домена, данный вариант является оптимальным.

Резервное копирование типа **offline** лучше всего подходит для изучения информации о сбое, поскольку она содержит дополнительные данные, которые обычно не реплицируются. При резервном копировании типа **offline** быстрее выполняется автономное резервное копирование для большого домена, поскольку не возникает дополнительных затрат на отправку базы данных по сети и повторную запись ее на диск.

Два этих типа резервного копирования имеют несколько общих черт. Резервные копии создаются с использованием двух вариантов команды `samba-tool domain backup`. Каждая команда создает файл резервной копии ***.tar.bz2**, который содержит полную резервную копию домена (на основе данного DC). Затем файл резервной копии можно использовать для восстановления домена с помощью команды `samba-tool domain backup restore`.

Резервное копирование типа online

Для того чтобы запустить резервное копирование в режиме **online**, выполните команду:

```
samba-tool domain backup online --targetdir=<каталог_хранения_РК> --server=<имя_сервера_DC> -U Administrator
```

где:

- **--targetdir=** - путь до директории, в которую будет сохранен файл резервной копии в формате **tar.bz2**;
- **--server=** - доменное имя сервера, на котором будет производиться резервное копирование;
- **-U** - имя учетной записи администратора контроллера домена.

Команда может быть запущена как удаленно, так и локально на самом контроллере домена. Выполняя удаленное копирование, можно добавить параметр **--configfile** для включения в резервную копию правильных параметров файла **smb.conf** (т. е. локальный файл

smb.conf может не существовать или его параметры могут отличаться от используемого контроллера домена).

Пример команды:

```
samba-tool domain backup online --targetdir=<каталог_хранения_PK> --server=<имя_сервера_DC> -U Administrator --configfile
```

Полезно также будет скопировать содержание файла **/etc/krb5.conf**, для того чтобы скорректировать настройки **kerberos** при последующем восстановлении домена. Так как в резервную копию попадает лишь файл из **/var/lib/samba/private/krb5.conf**, который может отличаться от используемого файла в **/etc/krb5.conf**.

Резервное копирование типа offline

Для создания резервной копии в режиме **offline** войдите в систему, резервную копию которой необходимо создать, и укажите расположение целевого каталога для записи файла резервной копии. Пример:

```
samba-tool domain backup offline --targetdir=<каталог_хранения_PK>
```

где **--targetdir=** - путь до директории, в которую будет сохранен файл резервной копии в формате **tar.bz2**.

Во время выполнения копирования контроллер домена может находиться как в рабочем состоянии, так и в автономном (когда службы **samba** отключены).

Полезно также будет скопировать содержимое файла **/etc/krb5.conf**, для того чтобы скорректировать настройки **kerberos** при последующем восстановлении домена. Так как в резервную копию попадает лишь файл из **/var/lib/samba/private/krb5.conf**, который может отличаться от используемого файла в **/etc/krb5.conf**.

Восстановление домена из файла резервной копии

Будет рассмотрен пример восстановления домена из файла резервной копии на новом сервере.

Первые шаги восстановления похожи на установку нового сервера **Samba DC**.

Обновление пакетов

Перейдите в сеанс пользователя **root**:

```
su -
```

и выполните обновление всех пакетов:

```
dnf makecache && dnf update
```

Все дальнейшие действия выполняются с правами пользователя **root**, если не указано иное.

Отключение SELinux

На время настройки переведите SELinux в режим уведомлений:

```
setenforce 0
```

Статус службы SELinux можно посмотреть командой sestatus.

Замените в файле конфигурации **/etc/selinux/config** режим **enforcing** на **permissive** командой:

```
sed -i "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

После перезагрузки системы служба SELinux будет запущена в режиме, который указан в конфигурационном файле.

Присваивание серверу доменного имени

Сервер контроллера домена должен иметь собственное уникальное доменное имя и статический IP-адрес. Назначьте серверу полное

доменное имя: например, если короткое имя сервера **dc1**, то для домена **skynet.murom** полное имя сервера имеет вид **dc1.skynet.murom**:

```
hostnamectl set-hostname dc1.skynet.murom
```

ВАЖНО!

Сервер должен иметь новое доменное имя, не совпадающее с доменным именем сервера, с которого была снята резервная копия.

Настройка сетевого интерфейса

По умолчанию сетевой интерфейс настроен для получения IP-адреса по **DHCP**. Нужно установить серверу контроллера домена статический IP-адрес.

Также необходимо установить адрес первого DNS-сервера с доступом к интернету или локальному репозиторию и адрес второго DNS-сервера самого контроллера домена.

После проведенных настроек перезагрузите сетевой интерфейс для применения настроек:

```
systemctl restart NetworkManager
```

Проверьте доступные серверы имен, просмотрев файл **resolv.conf**:

```
cat /etc/resolv.conf
```

Вывод команды должен иметь примерно следующий вид:

```
# Generated by NetworkManager
search skynet.murom
nameserver 8.8.8.8
nameserver 10.81.1.96
```

Установка необходимых пакетов

Для установки необходимых пакетов выполните:

```
dnf install samba* krb5*
```

Создание резервных копий файлов

Переименуйте используемые по умолчанию конфигурационные файлы **samba** и **kerberos**, тем самым создав их резервную копию:

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
mv /etc/krb5.conf /etc/krb5.conf.bak
```

Переместите все файлы из каталога **/var/lib/samba** в новый, тем самым создав их резервную копию:

```
mkdir /var/lib/samba.bak
mv /var/lib/samba/* /var/lib/samba.bak/
```

Процесс восстановления домена из резервной копии

Скопируйте файл резервной копии в формате ***.tar.bz2** на сервер. Выполните команду для восстановления домена из резервной копии:

```
samba-tool domain backup restore --backup-file=/home/user/backup_file.tar.bz2 --newservername=dc1 --targetdir=/var/lib/samba
```

где:

- **--backup-file=** - путь до файла с резервной копией;
- **--newservername=** - новое доменное имя для контроллера домена, оно не должно совпадать с именем старого контроллера домена, с которого была снята резервная копия.

Успешное выполнение команды должно сопровождаться следующими сообщениями:

```
Backup file successfully restored to /var/lib/samba
Please check the smb.conf settings are correct before starting samba.
```

Перенесите конфигурационные файлы командами:

```
cp /var/lib/samba/etc/smb.conf /etc/samba/
cp /var/lib/samba/private/krb5.conf /etc/
```

При необходимости можно изменить конфигурацию файла **krb5.conf** в соответствии с файлом **krb5.conf** старого контроллера домена, содержание которого было скопировано на этапе создания резервной копии.

Запустите службы **samba** командой:

```
systemctl enable samba --now
```

Проверьте статус служб **samba** командой:

```
systemctl status samba --now
```

В статусе возможно появление ошибки **winbind**. Если ошибка появилась, выполните:

```
systemctl restart samba.service
```

Для того чтобы повторно добавить старые контроллеры домена в сеть, присоединив их к восстановленному контролеру домена, выполните команду:

```
samba-tool domain join <dns-realm> DC --server=<restored-dc>
```

где:

- **<dns-realm>** - имя области присоединяемого домена;
- **<restored-dc>** - имя восстановленного контроллера домена.

smbpass – графическая утилита изменения пароля доменного пользователя (MSAD или SAMBA)

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** smbpass-0.4.2-2

Smbpass – это утилита для изменения пароля пользователя в домене Windows или Samba.

Для установки программы перейдите в сеанс пользователя **root**:

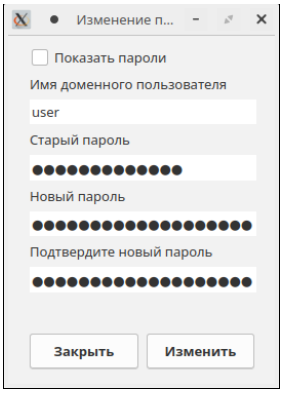
```
su -
```

и выполните команду:

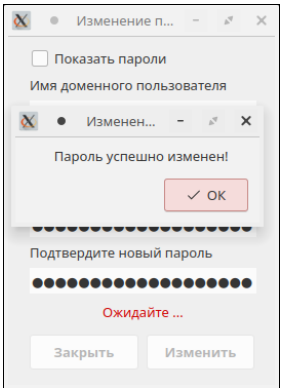
```
dnf install smbpass
```

После установки программа будет доступна из «**Главного меню**» – «**Системные**» - «**Изменение пароля доменного пользователя**».

Программа автоматически определит, от имени какого доменного пользователя произошел запуск, и подставит его *login* в поле «**Имя доменного пользователя**». Для изменения действующего пароля пользователя необходимо ввести текущий пароль и новый пароль с подтверждением.



Программа оповестит вас в случае успешного изменения пароля.



Сравнение функций Winbind и SSSD

Категория	Функция	Winbind	SSSD
Аутентификация	Аутентификация с использованием Kerberos	▭	▭
	Аутентификация с использованием LDAP	▭	▭
	Поддержка нескольких AD-доменов	▭	▭
	Поддержка AD-лесов	▭	▭
	Поддержка гетерогенных сред AD/FreeIPA	▬	▭
Безопасность	Простота настройки безопасной конфигурации	▬	▭
	Использование системы идентификации и ее ключа для защиты доступа к центральному серверу	▭	▭
	Поддержка NTLM	▭	▬
Поиск и сопоставление идентификаторов	Динамическое сопоставление идентификаторов AD (SID)	▭	▭
	Использование преимуществ конкретных расширений и протоколов AD	▭	▭
DNS	Обновление и очистка DNS AD	▬	▭
	Сайты DNS AD	▭	▭
Обмен файлами	Интеграция Samba FS	▭	▭
	Интеграция клиента CIFS	▭	▭
Служба печати	Сервер печати CUPS с использованием Kerberos	▭	▭
Политики	Централизованное управление контролем доступа на основе хоста через GPO	▬	▭
Интеграция на хосте с другими службами и приложениями	Интеграция с основными утилитами, такими как SSH, sudo, automount	▬	▭
	Расширенные интерфейсы идентификации по локальной шине сообщений D-Bus	▬	▭
	Специальные функции для приложений Docker, Cockpit, GSS Proxy и пр.	▬	▭

Настройка доступа к компьютеру по его сетевому имени

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Для подключения к компьютеру в сети удобнее обращаться к нему по сетевому имени, потому что IP-адрес компьютера может динамически измениться, если адрес был назначен DHCP-сервером.

Примечание.

Рабочая станция должна быть введена в домен. Инструкция по вводу доступна в разделе «**Работа с доменом MS AD**».

Если у вас не используется DNS-сервер для разрешения имен ПК, то включите разрешение имени **NetBIOS** — это процесс определения **IP-адреса** по имени.

Для этого откройте (от root) файл на редактирование /etc/nsswitch.conf, найдите строку с параметром `hosts` и приведите ее к следующему виду (добавив параметр `wins`):

```
hosts: files wins dns myhostname mdns4_minimal [NOTFOUND=return]
```

В РЕД ОС изменение конфигурации **/etc/nsswitch.conf** должно производиться через файл:

```
nano /etc/authselect/user-nsswitch.conf
```

после чего выполнить применение настроек:

```
authselect apply-changes
```

Включите службу **winbind**:

```
systemctl enable winbind
systemctl start winbind
```

Включите службу **nmb**:

```
systemctl enable nmb
systemctl start nmb
```

Проверьте работу:

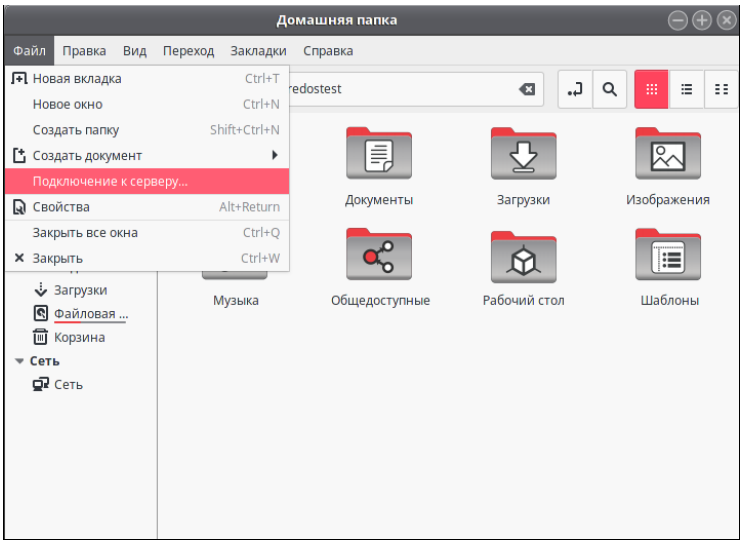
```
ping win10
```

где **win10** — это имя компьютера с ОС Windows.

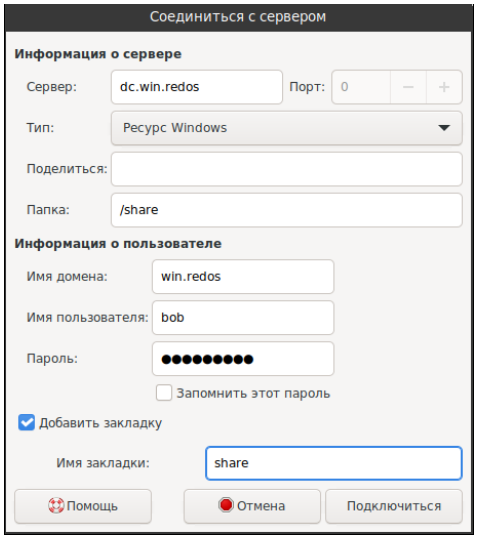
Подключение сетевых директорий с помощью графического приложения

Для авторизованного входа к сетевым ресурсам windows воспользуйтесь логином и паролем.

1. Откройте файловый менеджер, перейдите в меню «**Файл**» — «**Подключение к серверу**».



2. В открывшемся окне выберите тип подключения «**Общий ресурс Windows**». В разделе «**Информация о сервере**» в поле «**Сервер**» укажите IP-адрес сервера или доменное имя, в поле «**Папка**» впишите имя подключаемого сетевого каталога. В разделе «**Информация о пользователе**» заполните поля «**Имя домена**», «**Имя пользователя**» и «**Пароль**». Нажмите кнопку «**Соединиться**». При успешном соединении будет открыта сетевая папка.



Также можно установить флаг «**Добавить закладку**», чтобы ресурс появился в меню слева в файловом менеджере для быстрого доступа.

Подключение сетевых директорий с помощью fstab

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

1. Создайте файл с авторизационными данными:

```
# nano /root/.smbuser
```

```
username=имя_пользователя
password=пароль_пользователя
domain=ДОМЕН
```

Для безопасности ограничьте доступ к файлу с указанными данными:

```
# chmod 400 /root/.smbuser
```

2. Для подключения сетевой директории впишите в конец файла **/etc/fstab** её параметры.

Откройте его в текстовом редакторе:

```
# nano /etc/fstab
```

Синтаксис строки подключения для windows или samba-ресурсов следующий.

```
//<адрес_сервера>/<имя_сетевого_каталога> <каталог_для_монтирования> cifs
credentials=<путь_до_файла_с_авторизационными_данными>,iocharset=utf8,file_mode=0777,dir_mode=0777 0 0
```

При подключении используйте свои параметры.

В случае возникновения ошибки при монтировании общего ресурса, который находится на ПК с ОС Windows, нужно добавить в строку подключения следующий параметр:

```
vers=1.0
```

Пример:

```
//windows_pc/common /mnt/common/ cifs credentials=/root/.smbuser,vers=1.0,iocharset=utf8,file_mode=0777,dir_mode=0777 0 0
```

3. Создайте каталог, куда будет монтироваться папка и назначьте ей права.

```
# mkdir /mnt/common
# chmod 777 /mnt/common
```

Для удобства, можете создать ярлык каталога на рабочем столе, для этого выполните нижеследующую команду, вписав имя своего пользователя.

```
ln -s /mnt/common/ /home/<имя_пользователя>/Рабочий\ стол/Общая
```

4. Выполните монтирование каталога

```
mount -a
```

ВАЖНО!

В некоторых случаях, при загрузке компьютера монтирование происходит быстрее получения IP-адреса, тем самым, монтирование не происходит. Связано это с особенностями конфигурации сети. Для предотвращения подобных случаев можно вписать команду монтирования в файл **/etc/gdm/PreSession/Default**. Тогда монтирование будет происходить при входе пользователей в систему.

Откройте файл **/etc/gdm/PreSession/Default** и впишите в конец строку монтирования, после неё переведите курсор на новую строку и сохраните.

```
# nano /etc/gdm/PreSession/Default
...

mount -a &
```

ВАЖНО!

При подключении сетевой папки на windows server 2003 в опции монтирования надо дописать параметр `vers=1.0`, а так же логин и пароль не должны содержать кириллических символов.

Подключение сетевых директорий с использованием automount (autofs)

Автоматическое монтирование ресурсов CIFS
Автоматическое монтирование FTP-ресурсов
Автоматическое монтирование SSH-ресурсов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версии пакетов**: openssh-8.9p1-6, autofs-5.1.6-7

Установите или обновите пакет **cifs-utils** и **autofs**.

Для этого перейдите в сеанс пользователя **root** и запустите команду:

```
su -
dnf install cifs-utils autofs
```

Автоматическое монтирование ресурсов CIFS

1. Добавьте строку для монтирования в файл **/etc/auto.master**:

```
/mnt/samba    /etc/auto.samba    --ghost
```

- Первое поле - базовая точка монтирования, каталог /mnt/samba вручную создавать **не нужно**, он автоматически создается службой **autofs**.
- Второе поле - файл таблицы (map-файл), соответствующий этой точке монтирования.
- Третье поле необязательно и может содержать опции, которые будут применены ко всем записям таблицы.

2. Создайте файл **/etc/auto.samba** и впишите строку:

```
share    -fstype=cifs,rw,noperm,credentials=/root/.smbuser    ://win10/public
```

- Первое поле - имя автоматически создаваемой autofs папки, в которую монтируется шара.
- Второе поле - параметры подключения и путь к файлу с авторизационными данными.
- Третье поле - адрес сетевого каталога.

Если в пути имеются кириллические символы, то возьмите их в кавычки:
://win10/'мой каталог'

ВАЖНО!

При подключении сетевой папки на **windows server 2003** в опции монтирования надо дописать параметр **vers=1.0**.

Логин и пароль пользователя не должны содержать кириллических символов.

Версия **ядра** РЕД ОС должна быть **ниже 5.15.72**.

Проверьте, что компьютер доступен по имени, например, выполните команду:

```
ping <имя_пк>
```

если отклика нет, то запустите службу **winbind**:

```
systemctl enable winbind --now
```

а в файле **/etc/nsswitch.conf** приведите строку, начинающуюся с hosts, к виду:

```
hosts: files dns myhostname wins
```

Изменять конфигурацию **/etc/nsswitch.conf** следует через файл:

```
nano /etc/authselect/user-nsswitch.conf
```

после чего выполнить применение настроек:

```
authselect apply-changes
```

3. Создайте файл **/root/.smbuser** с логином и паролем пользователя для доступа к общему каталогу.

> **Примечание.**
>
> Если к общему каталогу разрешён анонимный доступ, тогда SMB-пароль задавать не нужно.
>
> Значения параметров в файле с реквизитам учётной записи /root/.smbuserзадавать тоже не нужно (после знака "=" ничего не указывать не надо).

> **ВАЖНО!**
>
> Задайте SMB-пароль пользователю (например, для ivan.ivanov):
>
> ```
> smbpasswd -a ivan.ivanov
> ```

```
nano /root/.smbuser
```

```
username=ivan.ivanov
password=12345678
domain=WORKGROUP
```

Если домена нет, то укажите в параметре domain имя рабочей группы windows.

Для безопасности ограничим доступ к файлу с нашими данными:

```
chmod 400 /root/.smbuser
```

4. Запустите **autofs** и добавьте его в автозагрузку.

```
systemctl enable autofs.service --now
```

Автоматическое монтирование FTP-ресурсов

С подробной информацией о возможности автоматического монтирования FTP-ресурсов можно ознакомиться в нашей статье «Настройка FTP-сервера».

Автоматическое монтирование SSH-ресурсов

1. Устанавливаем дополнительный пакет **sshfs**:

```
dnf install sshfs
```

2. Генерируем ключ ssh:

```
ssh-keygen
```

Когда генератор запросит фразу-пароль, просто нажмите **Enter**.

3. Копируем открытый ключ на удаленный сервер, доступ к которому необходимо настроить:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@10.10.1.7
```

где 10.10.1.7 - адрес удаленного сервера.

А закрытый ключ копируем в домашнюю директорию **root** (не требуется, если предыдущие действия выполнялись от root):

```
sudo cp ~/.ssh/id_rsa /root/.ssh/id_rsa
```

4. Редактируем файл **/etc/auto.master**:

```
nano /etc/auto.master

/mnt/ssh    /etc/auto.ssh    --ghost
```

5. Создаем файл:

```
nano /etc/auto.ssh
```

```
ssh -fstype=fuse,rw,allow_other,IdentityFile=/home/user/.ssh/id_rsa :sshfs\#user@10.10.1.7\:/home/user
```

6. Выполняем перезапуск сервиса **autofs**:

```
systemctl restart autofs
```

Подключение сетевых директорий с помощью fstab и механизма Kerberos

Установите необходимые пакеты:

```
dnf install cifs-utils samba-client krb5-workstation
```

ВАЖНО!

Рабочая станция должна быть введена в домен. Инструкция по вводу доступна в разделе «Работа с доменом MS AD».

Подключение сетевых директорий с помощью fstab

Для подключения сетевой директории впишите в конец файла /etc/fstab её параметры.

Откройте его в текстовом редакторе.

Пример:

```
# nano /etc/fstab
//win.ad.test/Public /mnt/pub/ cifs rw,users,sec=krb5,_netdev,nofail,domain=AD.TEST
```

где:
//win.ad.test/Public - доменное имя файлового сервера и каталог
/mnt/pub/ - каталог, в который будет произведено монтирование
cifs - тип монтируемой файловой системы
rw,users,noauto,sec=krb5 - параметры монтирования
domain=AD.TEST - имя домена

ВАЖНО

при подключении сетевой папки на windows server 2003 в опции монтирования надо дописать параметр vers=1.0, а так же логин и пароль не должны содержать кириллических символов

Создайте каталог, куда будет монтироваться папка и назначьте ей права.

```
# mkdir /mnt/pub
# chmod 777 /mnt/pub
```

Для удобства, можете создать ярлык каталога на рабочем столе, для этого выполните нижеследующую команду, вписав имя своего пользователя.

```
ln -s /mnt/pub/ /home/<имя пользователя>/Рабочий\ стол/Общая
```

Проверьте полученный билет керберос.

```
# klist
```

Если его нет, получите его

```
# kinit <имя-пользователя>
```

Разрешим выполнять mount от имени суперпользователя (root):

```
# chmod u+s /usr/sbin/mount.cifs
```

Выполните монтирование каталога

```
mount -a
```

Подключение сетевых директорий с использованием automount (autofs) и механизма Kerberos

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

autofs - это служба, которая автоматически монтирует файловые системы при их использовании, и отключает их позже, когда файловые системы перестают использоваться. **autofs** может работать с сетевыми файловыми системами, компакт-дисками и т. д.

ВАЖНО!

Рабочая станция должна быть введена в домен. Инструкции по вводу рабочей станции в домен доступны в разделе «Работа с доменом MS AD».

Вы можете подробнее ознакомиться с возможностью автоматического монтирования ресурсов и директорий, просмотрев наши обучающие видео:

- на **RuTube**:
  - Монтирование файловых систем в РЕД ОС;
  - Подключение сетевых директорий с помощью automount (autofs) и механизма Kerberos .
- в **Яндекс.Дзен**:
  - Монтирование файловых систем в РЕД ОС;
  - Подключение сетевых директорий с помощью automount (autofs) и механизма Kerberos .
- в **VK Видео**:
  - Монтирование файловых систем в РЕД ОС;
  - Подключение сетевых директорий с помощью automount (autofs) и механизма Kerberos .

На наших каналах вы также сможете найти много другой полезной информации.

1. Установите пакет **cifs-utils** и **autofs** (если они не установлены). Для этого перейдите в сеанс пользователя **root** или запустите команду от sudo-пользователя:

```
$ su -
# dnf install cifs-utils autofs
```

2. Войдите в систему **под учетной записью доменного пользователя** и проверьте билет Керберос командой (именно **от доменного пользователя**, а не от root):

```
$ klist
```

Пример вывода команды:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_51105
Default principal: u1@WIN.REDOS

Valid starting       Expires              Service principal
23.01.2020 15:41:54  24.01.2020 01:41:54  krbtgt/WIN.REDOS@WIN.REDOS
 renew until 30.01.2020 12:04:05
```

Для выполнения **всех** последующих действий перейдите в сеанс пользователя root (**su -**) или выполните действия от sudo-пользователя.

3. Добавьте строку для монтирования в файл **/etc/auto.master**

Для РЕД ОС 7.3 целесообразно создать точку монтирования сетевой папки в **/media**, потому что каталоги, созданные в **/media**, будут отображаться на рабочем столе и в файловых менеджерах *Nemo/Caja* (в левой колонке). В файловых менеджерах

Nemo/Caja монтировать данные каталоги можно будет одним кликом.

```
# nano /etc/auto.master
```

```
/media/samba    /etc/auto.samba    --ghost
```

- Первое поле (в примере - **/media/samba**) - базовая точка монтирования, которая выступает родительским каталогом для подключаемых общих сетевых ресурсов (они будут располагаться именно в этом каталоге)
- Второе поле (в примере - **/etc/auto.samba**) - файл таблицы (map-файл), соответствующий этой точке монтирования.
- Третье поле (в примере это –-**ghost**) необязательно и может содержать опции, которые будут применены ко всем записям таблицы.

4. Создайте файл **/etc/auto.samba** и впишите туда строку

```
# nano /etc/auto.samba
```

```
share    -fstype=cifs,multiuser,cruid=$UID,sec=krb5,iocharset=utf8,domain=WIN.REDOS ://dc.win.redos/share
```

- Первое поле (в примере - **share**) - имя автоматически создаваемой **autofs** папки, в которую монтируется общая папка **//dc2.wintest.redostest/share**.
- Второе поле (в примере - **-fstype**) - параметры подключения и указание на использования механизма *Kerberos.*
- Третье поле (в примере - **://dc.win.redos/share**) - адрес сетевого хранилища.
- Параметр **cruid** может принимать значение идентификатора пользователя или доменного имени пользователя.

ВАЖНО!

При подключении сетевой папки на *windows server 2003* в опции монтирования надо дописать параметр **vers=1.0**. Логин и пароль пользователя не должны содержать кириллических символов.

Для подключения скрытых сетевых каталогов необходимо экранировать символ **$**

```
share -fstype=cifs,multiuser,cruid=$UID,sec=krb5,iocharset=utf8,domain=WIN.REDOS ://dc.win.redos/share\$
```

Если в имени каталога имеются пробелы, то пробелы необходимо экранировать с помощью символа backslash(\):

```
share -fstype=cifs,multiuser,cruid=$UID,sec=krb5,iocharset=utf8,domain=WIN.REDOS ://dc.win.redos/Новая\ папка
```

5. Добавьте **autofs** в автозагрузку и запустите службу:

```
systemctl enable autofs --now
```

Теперь подключённые общие сетевые ресурсы будут автоматически монтироваться при обращении пользователя к каталогу-точке монтирования (по запросу пользователя, а не при загрузке ОС на ПК, что позволяет снизить нагрузку на сервер). В нашем примере точкой монтирования выступает каталог **/media/samba**.

Подключение сетевых директорий с помощью NFS

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

Для монтирования сетевой папки необходимо создать папку на локальном компьютере:

```
mkdir ~/test
```

Монтирование вручную

Для монтирования папки вручную необходимо выполнить в терминале команду:

```
sudo mount -t nfs -O uid=1000,iocharset=utf-8 *IP-сервера*:/data ~/test
```

ВАЖНО

Следует помнить, что, как в настройках сервера, так и в настройках клиента при монтировании, путь к общему каталогу указывается полный. Данный пример показывает, что каталог **/data** находится в корне файловой системы.

Монтирование с записью в fstab

Для большего удобства можно добавить запись с сетевой папкой в fstab.

Целесообразно создать точку монтирования сетевой папки в **/media**, потому что каталоги, созданные в **/media**, будут отображаться на рабочем столе и в файловых менеджерах Nemo/Caja (в левой колонке). В файловых менеджерах Nemo/Caja монтировать данные каталоги можно будет одним кликом.

```
sudo mkdir /media/test
```

В файл /etc/fstab добавляем подобную запись:

```
*IP-сервера*:/data /media/test nfs rsize=8192,wsize=8192,timeo=14,intr 0 0
```

Опция «noauto» запрещает автоматическое монтирование сетевого диска при старте системы.

Проблемы

Использование на ноутбуке
При монтировании удаленных папок NFS посредством fstab, в ситуации, когда сеть с сервером будет не доступна, ноутбук невозможно выключить или отправить в спящий режим. Для использования удаленных папок NFS на ноутбуке лучше воспользоваться монтированием при помощи autofs

Монтирование с помощью autofs

Данный способ монтирования позволяет автоматически монтировать папку после обращения к ней в Nemo, Caja (к примеру, через закладки) или в терминале и автоматически отмонтировать при отсутствии активности.
Для реализации данного способа необходимо установить пакет autofs (если он ещё не установлен):

```
dnf install autofs
```

Для настройки autofs в файле /etc/auto.master необходимо добавить строку

```
/nfs /etc/auto.nfs --timeout=60
```

Здесь --timeout=60
указывает системе отмонтировать раздел при отсутствии активности на нём более чем 60 секунд.
Создаем в корне файловой системы папку /nfs :

```
touch /etc/auto.nfs && mkdir /nfs
```

В файле */etc/auto.nfs* добавляем строку

```
server  -rw,soft,intr,rsize=8192,wsize=8192 *IP-адрес*:/path_to_share
```

где:
• **-rw,soft,intr,rsize=8192,wsize=8192** – параметры монтирования;
• **server** – папка, которая будет создаваться в каталоге /nfs при монтировании удаленных папок;
• ***IP-адрес*:/path_to_share** – IP-адрес и общая папка сервера.

Добавляем службу autofs в автозапуск и перезапускаем для применения настроек:

```
sudo systemctl enable autofs
```

```
sudo systemctl restart autofs
```

ВАЖНО

При подключении сетевой папки на windows server 2003 в опции монтирования надо дописать параметр vers=1.0. Логин и пароль не должны содержать кириллических символов.

Автоматическое монтирование ресурсов при входе пользователя с помощью pam_mount

Для автоматического монтирования разделяемых файловых ресурсов при входе пользователя используется PAM-модуль pam_mount, предоставляемый пакетом pam_mount, то есть для автоматического монтирования разделяемых файловых ресурсов на компьютере-клиенте должны быть установлены пакет **cifs-utils** и **pam_mount**:

```
dnf install cifs-utils pam_mount
```

Настройка модуля pam_mount осуществляется с помощью конфигурационного файла **/etc/security/pam_mount.conf.xml**.

Вы можете подробнее ознакомиться с возможностью автоматического монтирования ресурсов, просмотрев наши обучающие видео:

- на **RuTube** — Монтирование файловых систем в РЕД ОС;
- в **Яндекс.Дзен** — Монтирование файловых систем в РЕД ОС;
- в **VK Видео** — Монтирование файловых систем в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Описание возможностей модуля pam_mount и формат его конфигурационного файла приведены в руководстве man для pam_mount и pam_mount.conf.

Для монтирования с помощью pam_mount разделяемых файловых ресурсов в конфигурационном файле должны быть указаны параметра монтируемого тома, например:

```
<?xml version="1.0" encoding="utf-8" ?>
 <!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
 <!-- See pam_mount.conf(5) for a description.-->
 <pam_mount>
 <mntoptions allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow_other" />
 <mntoptions require="nosuid,nodev" />
 <mkmountpoint enable="1" remove="true" />
 <debug enable="0" />

 <logout wait="500000" hup="1" term="1" kill="1" />

 <cifsmount>
 mount.cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o %(OPTIONS)
 </cifsmount>

 <volume
 fstype="cifs"
 server="dc.example.ru"
 path="share-pam"
 mountpoint="~/share-pam"
 options="username=%(USER),uid=%(USERUID),pass=%(PASSWD),rw,setuids,sec=ntlmv2i"
 />

 <volume
 fstype="cifs"
 server="dc.example.ru"
 path="share-pam"
 mountpoint="~/share-pam"
 options="username=%(USER),cruid=%(USERUID),setuids,file_mode=0664,dir_mode=0775,sec=krb5i"
 />

 </pam_mount>
```

где:

- server — машина, откуда производится монтирование. Обычно, если сеть не является доменной структурой, допустимо использование IPv4-адреса;
- path — каталог, который необходимо смонтировать с сервера;

- mountpoint — точка монтирования, другими словами - куда монтировать ресурс;
- options — атрибуты монтирования.

После настройки **pam_mount.conf.xml** необходимо внести изменения в файл **postlogin** профиля **authselect** и применить новую конфигурацию.

Для этого выполните следующее:

1. Определите используемый профиль:

```
authselect current
```

1.1. В случае если компьютер введен в домен, но используется профиль **sssd**, создайте профиль **sssd_domain**:

```
authselect create-profile sssd_domain -b sssd
```

> **Примечание.**
>
> В опции -b указывается профиль, который будет основой для создаваемого.

1.2. В случае если компьютер введен в домен, но используется профиль **winbind**, создайте профиль **winbind_domain**:

```
authselect create-profile winbind_domain -b winbind
```

1.3. В случае если компьютер введен в домен и уже используется профиль **sssd_domain** или **winbind_domain**, создавать профиль не нужно.

2. Отредактируйте файл **/etc/authselect/<идентификатор_профиля>/postlogin**:

```
nano /etc/authselect/<идентификатор_профиля>/postlogin
```

где <идентификатор_профиля> может принимать следующие значения:

- для **sssd_domain** — custom/sssd_domain;
- для **winbind_domain** — custom/winbind_domain.

и добавьте в конец файла следующую строку:

```
session optional pam_mount.so
```

> **Примечание.**
>
> Модуль **pam_mount.so** с атрибутом disable_interactive допустим только при аутентификации через **krb5** и **krb5i**.

3. Примените отредактированный профиль:

```
authselect select <идентификатор_профиля>
```

Аутентификация через Kerberos при использовании модуля pam_mount

Для использования Kerberos-аутентификации на введенной в домен рабочей станции в конфигурационном файле **/etc/security/pam_mount.conf.xml** в строке с опциями монтирования укажите параметр аутентификации:

- **sec=krb5i** – предпочтительно с точки зрения безопасности, но требует больше ресурсов;
- **sec=krb5** – при монтировании будет использоваться текущий кеш Kerberos-пользователя.

Также можно добавить атрибут disable_interactive к модулю **pam_mount.so**, который позволяет авторизоваться на сетевом ресурсе без повторного ввода пароля (в файле **/etc/authselect/<идентификатор_профиля>/postlogin**). Для применения изменений, внесенных в профиль, выполните:

```
authselect select <идентификатор_профиля>
```

Примечание.

Обратите внимание, что настроенный автоматический вход в систему не производит автоматическую авторизацию сетевых ресурсов при использовании модуля **pam_mount.so** с атрибутом disable_interactive.

ВАЖНО!

При подключении сетевой папки на **windows server 2003** в опции монтирования необходимо дописать параметр vers=1.0. Логин и пароль **не должны** содержать кириллических символов. Обратите внимание, что начиная с версии ядра **5.15** в клиенте CIFS прекращена поддержка NTLM и менее надёжных алгоритмов аутентификации, основанных на алгоритме DES и используемых в протоколе SMB1.

При повторном вводе в домен внесенные изменения в профиль **authselect** будут удалены в связи с повторным конфигурированием профиля.

Подключение сетевых директорий через сервис systemd

Выполните в терминале команду:

```
systemctl enable NetworkManager-wait-online.service
```

ВАЖНО!

Пример настройки приведен для использования на ПК в домене. Если не используется домен, тогда опции надо использовать другие (описание опций можно посмотреть в мануале, для этого в терминале введите команду man mount).

Создайте сервис для монтирования:

```
nano /etc/systemd/system/mnt-pub.mount
```

где:

- **mnt-pub** — путь до точки монтирования (разделение указываются в этом случае через "дефис");
- **.mount** — расширение, указывающее на то, что данный модуль является опцией для монтирования.

ВАЖНО!

Имя файла должно соответствовать созданной точке монтирования, иначе сервис работать не будет.

Содержимое:

```
[Unit]
 Description=User's mount service
 Requires=network-online.target
 After=gdm.service

 [Mount]
 What=//dc1.winhost.ru/share
 Where=/mnt/pub
 Type=cifs
 Options=multiuser,cruid=$UID,sec=krb5,domain=WINHOST.RU

 [Install]
 WantedBy=multi-user.target
```

где:

- **cruid** — уникальный идентификатор пользователя, состоящий из последовательности цифр. Его можно увидеть в выводе команды:

```
id <имя_пользователя>
```

Параметр cruid = Arg устанавливает UID владельца кеша учетных данных. В первую очередь, эта опция полезна с sec = krb5. По умолчанию используется реальный идентификатор процесса, выполняющего монтирование. Установка этого параметра указывает upcall искать кеш учетных данных, принадлежащий этому пользователю.

Другой вариант создания сервиса с явным указанием *пользователя* и *пароля*:

```
[Unit]
 Description=User's mount service
 Requires=network-online.target
 After=gdm.service

 [Mount]
 What=//dc1.winhost.ru/share
 Where=/mnt/pub
```

```
Type=cifs
Options=rw,user=admin,password=password,domain=WINHOST.RU

[Install]
WantedBy=multi-user.target
```

где:

- **admin** — ваше имя пользователя;
- **password** — ваш пароль для указанного пользователя.

ВАЖНО!

При подключении сетевой папки на **windows server 2003** в опции монтирования надо дописать параметр **vers=1.0**, а так же логин и пароль не должны содержать кириллических символов.

Добавьте сервис в автозагрузку:

```
systemctl enable mnt-pub.mount
```

Создайте папку, в которую будет происходить монтирование, и назначьте права:

```
mkdir -p /mnt/pub && chmod 777 /mnt/pub
```

Выполните команду:

```
chmod u+s /usr/sbin/mount.cifs
```

Вывод ярлыка папки на рабочий стол:

```
ln -s /mnt/pub/ $HOME/Рабочий\ стол/Share
```

РЕД ОС в рабочей группе

Окружение

- **Версия РЕД ОС**: 8
- **Версия Kernel**: 5.15.10
- **Конфигурация**: Рабочая станция

Для включения РЕД ОС в рабочую группу, необходимо в конфигурационном файле samba, секцию **[global]** привести к виду:

```
# nano /etc/samba/smb.conf
```

```
[global]
workgroup = WORKGROUP
security = user
passdb backend = tdbsam
map to guest = bad user

netbios name = mycomputer
client min protocol = NT1
client max protocol = SMB3
wins support = yes

# UTF кодировка
unix charset = UTF-8
dos charset = cp1251
store dos attributes = yes
```

Включим сервис **smb** в автозагрузку и запустим его:

```
systemctl enable smb --now
```

Также поступим и с сервисом **nmb**:

```
systemctl enable nmb --now
```

nmb - сервер имен NetBIOS для предоставления клиентам услуг именования NetBIOS через IP.
Теперь машины с операционными системами Windows или Linux смогут найти ваш компьютер в сети.
Также и РЕД ОС в рабочей группе WORKGROUP сможет увидеть другие ПК.

Подключение сетевых директорий с помощью утилиты connectfolder

Окружение

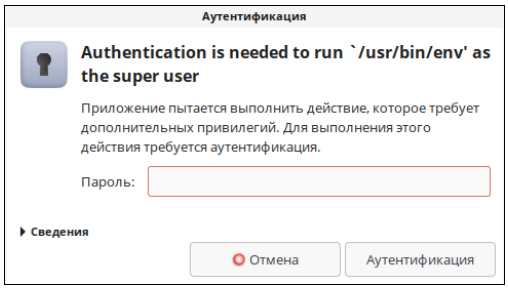
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** connectfolder 0.2.4

connectfolder - графическая утилита для подключения сетевых каталогов, открытых в общий доступ по протоколу *smb* в рабочей группе или домене *Windows/Samba*. Для монтирования сетевых директорий программа использует технологию **autofs**.

```
dnf install connectfolder
```

После установки программа доступна через «*Главное меню > Системные > Подключение сетевого каталога*».

Работа с *connectfolder* требует прав администратора, поэтому во время запуска программы необходимо ввести пароль пользователя **root**.

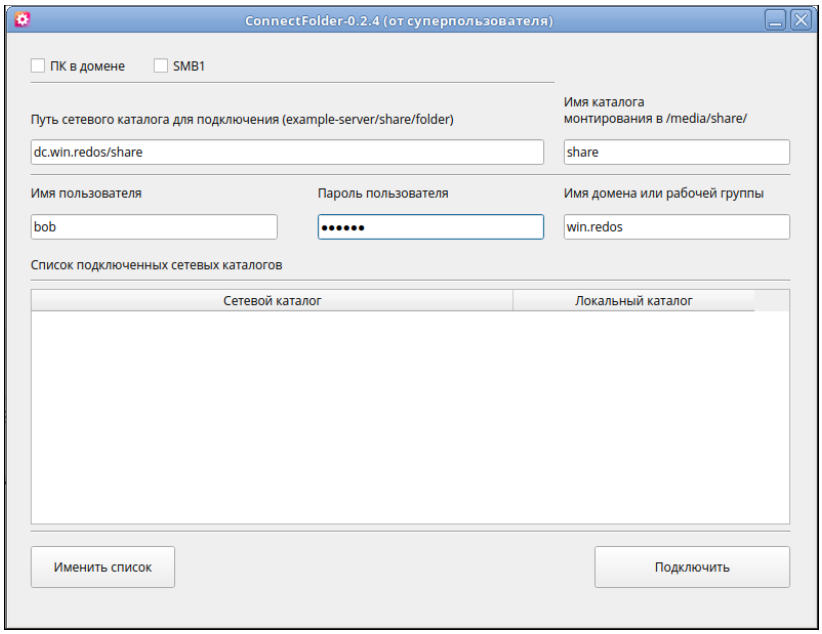


После успешной аутентификации откроется окно программы.

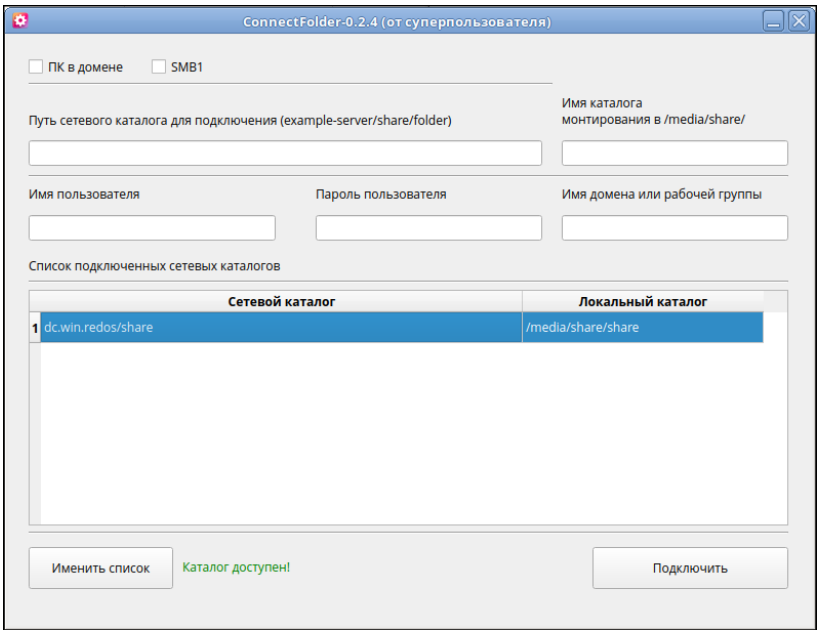
В первой строке указывается путь к сетевому каталогу, который необходимо подключить.

По умолчанию программа монтирует сетевые каталоги в локальную директорию **/media/share/** в предварительно указанный каталог. Этот каталог назначается в поле «*Имя каталога монтирования в /media/share/*».

При необходимости впишите *имя пользователя* для доступа к сетевому ресурсу, *пароль*, *имя рабочей группы или домена*.

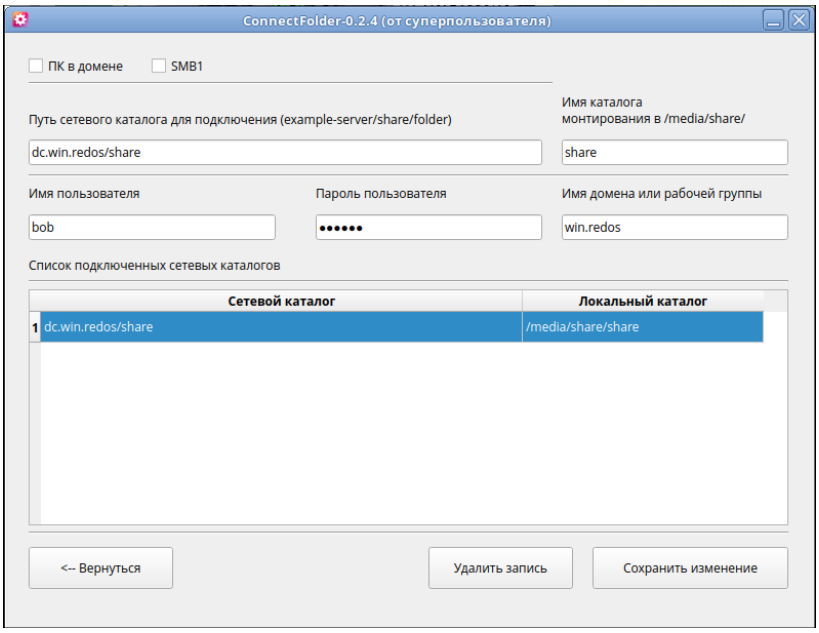


В данном примере после нажатия на кнопку «*Подключить*» инициализируется подключение (монтирование в linux) сетевого каталога «**dc.win.redos/share**» в локальную директорию **/media/share/share**. В случае успеха появится соответствующая запись в списке подключенных сетевых ресурсов.

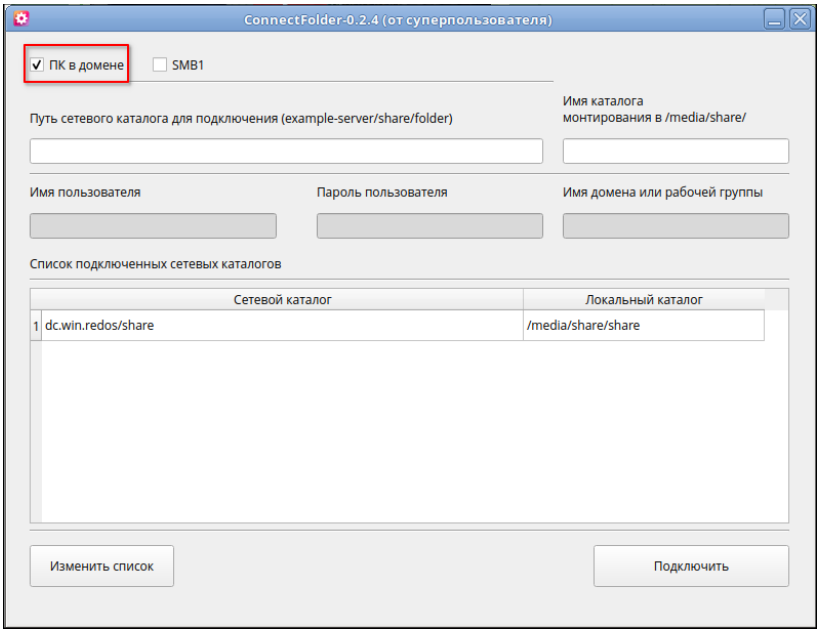


При выборе мышкой данной записи из списка будет произведен тест доступности каталога, и при успешном подключении появится надпись «*Каталог доступен*!».

При нажатии на кнопку «*Изменить список*» будет активирован режим редактирования, в котором можно изменять поля для подключения или совсем отключить подключенный сетевой ресурс, нажав на кнопку «*Удалить запись*», предварительно выбрав необходимую запись из списка.



Если ПК с РЕД ОС, на котором запускается *connectfolder*, введен в домен, то программа это автоматически обнаружит и установит флаг «*ПК в домене*». В таком случае поля «*Имя пользователя*», «*Пароль пользователя*» и «*Имя домена или рабочей группы*» будут автоматически не активны, т.к. для подключения к сетевому ресурсу будут использоваться права доступа доменного пользователя. При необходимости можно снять выбор «*ПК в домене*» и тогда ранее неактивные поля будут доступны для редактирования.



Переключатель «*SMB1*» активирует использование протокола версии **SMB1** при монтировании сетевого ресурса. Это может быть использовано при возникновении проблем с подключением к файловым серверам, которые продолжают работать на устаревшей версии протокола **SMB**.

Подключение сетевых директорий с помощью GIO

Установка и возможности GIO
Примеры использования
Автомонтирование сетевых ресурсов

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: gvfs-1.52.3-1

GIO (*GNOME Input/Output*) — это библиотека ввода-вывода, предоставляющая абстрактный интерфейс для работы с файлами, сетевыми соединениями, устройствами и другими ресурсами.

В РЕД ОС **gio** входит в состав пакета **gvfs**. **GVFS** предоставляет полную инфраструктуру виртуальной файловой системы и управления хранилищем.

Для идентификации **GIO** использует адреса на основе стандарта URI. Такие адреса имеют вид `<протокол>://user@server/path` и являются ключевой информацией, определяющей вид услуги и протокола, по которому воспроизводится передача данных. Для монтирования ресурсов используется **GVFS**.

GVFS монтирует съемные носители в каталог **/var/run/user/<uid_пользователя>/gvfs**.

Установка и возможности GIO

Пакет **gvfs** с **gio** по умолчанию предустановлен в РЕД ОС (в MATE, GNOME).

Если по каким-либо причинам пакет отсутствует в вашей системе, перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду установки:

```
dnf install gvfs
```

GIO предоставляет несколько команд, которые могут быть полезны для написания скриптов и тестирования. Команды описаны в таблице ниже.

Команда	Описание
help	Напечатать справку
version	Вывести номер версии
cat	Объединить файлы и вывести содержимое на стандартный вывод
copy	Копировать один или несколько файлов
info	Показать информацию о расположениях
list	Показать содержимое расположений
mime	Получить или установить обработчик для типа MIME
mkdir	Создать каталог
monitor	Отслеживать изменение файлов и каталогов
mount	Монтирование или размонтирование расположений
move	Переместить один или несколько файлов
open	Открыть файлы приложением по умолчанию
rename	Переименовать файл
remove	Удалить один или несколько файлов
save	Прочитать содержимое стандартного входа и сохранить
set	Установить атрибут файла

trash	Переместить файлы или каталоги в корзину
tree	Показать содержимое расположений в виде дерева

В РЕД ОС **gio** используется для монтирования распределенной файловой системы **DFS** (*Distributed File System*).

Примеры использования

Монтирование сетевого ресурса к доменному пользователю

В данном примере рассмотрено монтирование сетевого ресурса к пользователю в домене *Microsoft AD*.

Перед монтированием необходимо авторизоваться под доменным пользователем.

> **Примечание.**
>
> Пользователю должен быть разрешён доступ к монтируемому ресурсу.

Монтирование производится командой:

```
gio mount smb://<сервер>/<общий_ресурс>
```

Например:

```
gio mount smb://dc.win.redos/test
```

Монтирование сетевого ресурса к локальному пользователю

Для анонимного доступа к ресурсу применяется ключ **-a**:

```
gio mount -a smb://<сервер>/<общий_ресурс>/
```

При выполнении команды без ключа анонимного доступа будет запрошена аутентификационная информация:

```
gio mount smb://10.81.81.1
Требуется аутентификация
Введите пользователя и пароль для «10.81.81.1»:
User [user]:
Domain [SAMBA]:
Password:
```

Просмотр и копирование файлов с использованием ssh

Для просмотра файла на удалённом ресурсе используется операнд `cat`:

```
gio cat ssh://user@<ip-адрес>/home/user/test.txt
```

Для копирования файла с удалённого ресурса используется операнд `copy`:

```
gio copy ssh://user@<ip-адрес>/home/user/test.txt /<место_сохранения>/
```

Монтирование сетевого ресурса с использованием ftp

Для монтирования FTP-ресурса выполните команду:

```
gio mount ftp://<сервер>/<общий_ресурс>/
```

Автомонтирование сетевых ресурсов

Файл автозагрузки

Для автоматизации монтирования необходимо в директории **/etc/xdg/autostart** создать файл автозапуска с расширением **.desktop**:

```
nano /etc/xdg/autostart/gio.desktop
```

со следующим содержимым:

```
[Desktop Entry]
Name=GIO mount
Type=Application
Exec=gio mount smb://<сервер>/<общий_ресурс>/
Terminal=false
```

здесь:

- `gio mount smb://<сервер>/<общий_ресурс>/` — команда монтирования. Таким же образом можно настроить автомонтирование для FTP-ресурса.

Добавление параметра в .bashrc

Для автоматизации монтирования под доменным пользователем необходимо добавить команду в файл **.bashrc** в домашнем каталоге пользователя. Сделать это можно командой:

```
echo "timeout 4 gio mount smb://10.81.81.1 &> /dev/null" >> ./.bashrc
```

Организация отказоустойчивого кластера

Вводные данные
Предварительная подготовка кластера
Создание и настройка кластера
IPMI
STONITH

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: pcs - 0.10.14, pacemaker - 2.1.4, corosync - 3.1.6

Corosync - это программа с открытым исходным кодом, которая предоставляет возможности кластерного членства и обмена сообщениями, часто называемые уровнем обмена сообщениями, на клиентские серверы.

Pacemaker - это менеджер ресурсов кластера с открытым исходным кодом (CRM), который координирует ресурсы и службы, которые управляются и становятся доступными кластеру. По сути, *Corosync* позволяет серверам связываться как кластер, в то время как Pacemaker предоставляет возможность управлять тем, как ведет себя кластер.

Архитектура *pacemaker* состоит из трех уровней:

- *Кластеронезависимый уровень* - на этом уровне располагаются сами ресурсы и их скрипты, которыми они управляются, и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах.
- *Менеджер ресурсов* (Pacemaker), который реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Pacemaker, исходя из сложившейся ситуации, делает расчет наиболее оптимального состояния кластера и дает команды на выполнение действий для достижения этого состояния (остановка/перенос ресурсов или узлов).
- *Информационный уровень* - на этом уровне осуществляется сетевое взаимодействие узлов, т.е. передача сервисных команд (запуск/остановка ресурсов, узлов и т.д.), обмен информацией о полноте состава кластера (quorum) и т.д. На этом уровне работает Corosync.

Вводные данные

Администраторы самостоятельно определяют, какое количество нод необходимо для отказоустойчивого кластера в зависимости от ресурсов и задач. В данной статье в качестве примера будет рассмотрен кластер из двух узлов - **node1** и **node2**:

```
10.81.186.128 - node1
10.81.186.130 - node2
```

Предварительная подготовка кластера

Примечание.

Раздел «**Предварительная подготовка**» выполняется на каждом сервере.

Примечание.

Команды выполняются с правами пользователя **root**, если не указано иное.

1. Задайте имя ноды командой:

```
hostnamectl set-hostname <имя_ноды>
```

Например, задайте имя **node1**:

```
hostnamectl set-hostname node1
```

2. В файле **/etc/hosts** необходимо внести *IP* и *имя* каждой ноды, во избежание проблем с DNS, строкой вида:

```
127.0.0.1 <имя_ноды>
```

Пример файла **/etc/hosts** (добавленные строки выделены жирным шрифтом):

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

10.81.186.128 node1
10.81.186.130 node2
```

3. Установите необходимые компоненты:

```
dnf install pcs pacemaker corosync
```

4. Основная утилита управлением кластером - **pcs**. Данная утилита создает пользователя **hacluster**, для которого необходимо задать пароль:

```
passwd hacluster
```

5. Добавьте службы в автозапуск:

```
systemctl enable pcsd pacemaker corosync
```

6. Выполните запуск службы:

```
systemctl start pcsd
```

Создание и настройка кластера

1. Перед настройкой и первым запуском кластера необходимо однократно произвести авторизацию узлов в кластере:

```
pcs host auth node1 node2 -u hacluster -p password

node2: Authorized
node1: Authorized
```

2. Настройте кластер:

```
pcs cluster setup Cluster node1 node2

No addresses specified for host 'node1', using 'node1'
No addresses specified for host 'node2', using 'node2'
Destroying cluster on hosts: 'node1', 'node2'...
node2: Successfully destroyed cluster
node1: Successfully destroyed cluster
Requesting remove 'pcsd settings' from 'node1', 'node2'
node1: successful removal of the file 'pcsd settings'
node2: successful removal of the file 'pcsd settings'
Sending 'corosync authkey', 'pacemaker authkey' to 'node1', 'node2'
node2: successful distribution of the file 'corosync authkey'
node2: successful distribution of the file 'pacemaker authkey'
node1: successful distribution of the file 'corosync authkey'
node1: successful distribution of the file 'pacemaker authkey'
Sending 'corosync.conf' to 'node1', 'node2'
node1: successful distribution of the file 'corosync.conf'
node2: successful distribution of the file 'corosync.conf'
Cluster has been successfully set up.
```

3. Включите в автозагрузку и запустите кластер:

```
pcs cluster enable --all && pcs cluster start --all
```

```
node1: Cluster Enabled
node2: Cluster Enabled
node2: Starting Cluster...
node1: Starting Cluster...
```

4. Выполните следующие команды:

```
pcs property set stonith-enabled=false
pcs property set no-quorum-policy=ignore
```

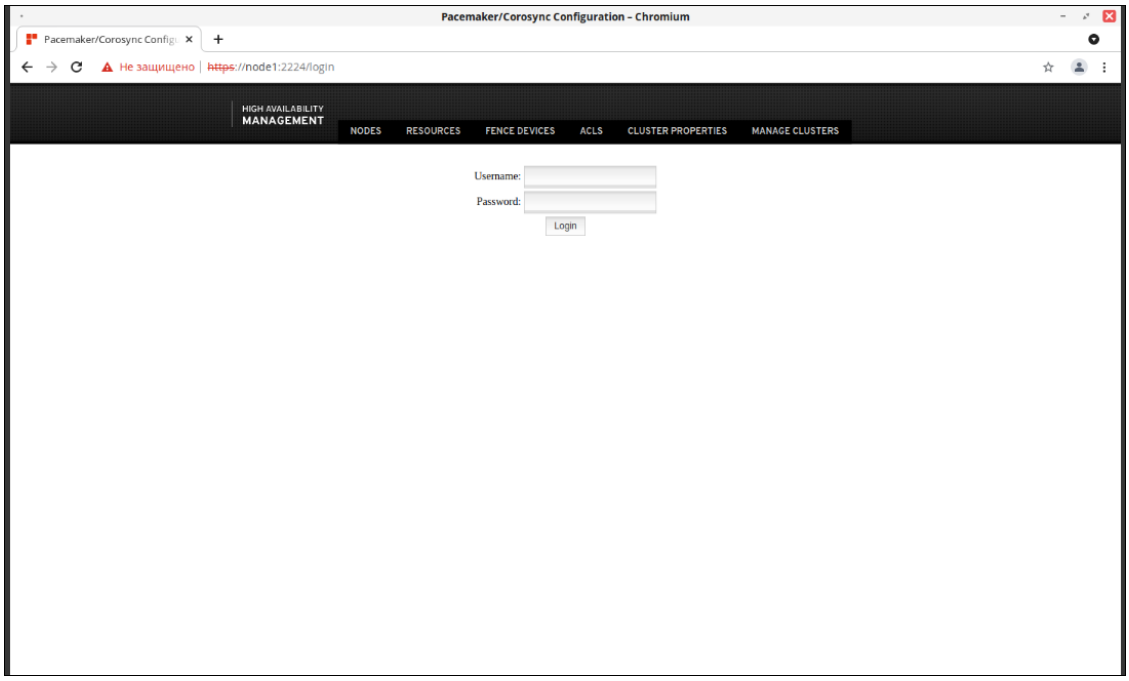
Если ноды разворачиваются на серверах с поддержкой **ipmi**, то в строке `pcs property set stonith-enabled` укажите значение `true`. **Stonith** используется для перезагрузки сервера в случае возникновения критической ошибки, которую не сможет устранить кластер.

Как настроить **ipmi** см. раздел «IPMI».

5. Проверьте состояние кластера командой:

```
pcs status

Cluster name: Cluster

WARNINGS:
No stonith devices and stonith-enabled is not false

Cluster Summary:
  * Stack: corosync
  * Current DC: node1 (version 2.1.4-1.el7-dc6eb4362e) - partition with quorum
  * Last updated: Tue Mar 28 22:17:57 2023
  * Last change:  Tue Mar 28 22:17:17 2023 by root via cibadmin on node1   * 2 nodes configured
  * 0 resource instances configured

Node List:
  * Online: [ node1 node2 ]

Full List of Resources:
  * No resources

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

Кроме консольных команд настройку кластеров можно производить также с панели администрирования, для этого в адресной строке браузера необходимо вписать **https://<имя_ноды>:2224** и авторизоваться пользователем **hacluster** с созданным ранее паролем.



IPMI

В случае возникновения критических неполадок серверов инженеры используют технологию **IPMI**. Данная технология позволяет удаленно реагировать на неполадки, вести мониторинг физического состояния оборудования и многое другое.

> **Примечание.**
>
> Настройка выполняется на каждом сервере.

Установите пакеты командой:

```
dnf install resource-agents fence-agents
```

Перед настройкой **IPMI** на серверах необходимо загрузить модули ядра. Для этого выполните следующие команды:

```
modprobe ipmi_devintf
modprobe ipmi_si
```

Затем необходимо настроить сеть на IPMI-интерфейсе в BIOS или через ОС.

Проверьте, что на интерфейсе используется статический адрес, выполните команду:

```
ipmitool lan print 1
```

Вывод команды должен иметь следующий вид:

```
IP Address Source : Static Address
```

Задайте сетевые параметры ipmi-интерфейсу, выполнив команды:

```
ipmitool lan set 1 ipsrc static <IP>
ipmitool lan set 1 netmask <netmask>
ipmitool lan set 1 defgw ipaddr <Gateway_IP>
```

Далее необходимо настроить **STONITH**.

STONITH

STONITH - метод изоляции отказавшего узла. **STONITH** изолирует неисправные узлы, перезагружая или отключая неисправный узел, чтобы он не вызывал нарушения работы кластера.

> **Примечание.**
>
> Настройка выполняется на каждом сервере.

Выведите список пользователей **ipmi** командой:

```
ipmitool user list 1

ID  Name     Callin  Link    Auth  IPMI Msg   Channel Priv Limit
2   ADMIN    false   false         true       ADMINISTRATOR
```

Вывод показывает, что существует пользователь с ID 2, следовательно, следующие идентификаторы свободны. Для примера будет создан пользователь **pcs** (по имени команды конфигурации кластера) с **ID 3** и с правами администратора для доступа. Для этого на сервере подсистем для *настройки привилегий пользователя root* необходимо выполнить следующие команды:

```
ipmitool user set name 3 pcs
ipmitool user set password 3 ipmitool channel setaccess 1 3 ipmi=on link=on callin=on privilege=4
ipmitool user priv 3 4 1
ipmitool user enable 3
```

где 3 - это **id** создаваемого пользователя и назначение ему привилегий.

Далее необходимо настроить **fence_ipmilan**, выполнив на сервере команды:

```
 pcs stonith create <имя_stonith_ресурса_для_node1> fence_ipmilan auth=md5 ipaddr=<ip> passwd=******** login=pcs action=reboot pcmk_host_list=<node1> pcmk_host_check=static-list
 pcs stonith create <имя_stonith_ресурса_для_node2> fence_ipmilan auth=md5 ipaddr=<ip> passwd=******** login=pcs action=reboot pcmk_host_list=<node2> pcmk_host_check=static-list
```

Для настройки **STONITH** также требуется осуществить привязку ресурсов к узлам кластера через **constraint**, которая жёстко задаёт ограничение запуска. Для этого на любом сервере выполните следующие команды:

```
 pcs constraint location <имя_stonith_ресурса_для_node1> avoids node1=INFINITY
 pcs constraint location <имя_stonith_ресурса_для_node2> avoids node2=INFINITY
```

Установка PostgreSQL

Установка и настройка PostgreSQL
Ключевые моменты по работе с PostgreSQL
Дополнительные возможности для PostgreSQL
Решение проблемы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: postgresql15-15.2-3

Для установки и настройки **postgresql** перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Примечание.

В наименовании пакетов и путях конфигурационных файлов для указания версии **PostgreSQL** используется число, выделенное в тексте статьи **красным цветом**.

Для **PostgreSQL 12** номер версии в названии пакета и путях к конфигурационным файлам отсутствует.

В репозитории РЕД ОС доступны следующие версии **PostgreSQL**:

- PostgreSQL 12;
- PostgreSQL 13;
- PostgreSQL 14;
- PostgreSQL 15.
- PostgreSQL 16.

Установка и настройка PostgreSQL

Для установки **postgresql** выполните команду:

```
dnf install postgresql15-server
```

Далее необходимо произвести инициализацию базы данных **postgresql**:

```
postgresql-15-setup initdb
```

После успешной инициализации запустите службу **postgresql** и добавьте ее в автозагрузку:

```
systemctl enable postgresql-15.service --now
```

Убедитесь, что служба запущена:

```
systemctl status postgresql-15.service
```

В статусе должно отображаться **active (running)**.

Ключевые моменты по работе с PostgreSQL

Авторизуйтесь пользователем **postgres**:

```
su - postgres
```

Для запуска **postgres shell** (запускается только от пользователя **postgres**) выполните:

```
psql
```

Тестовый запрос на получение списка баз данных производится командой (символ "\" также необходимо вводить):

```
\l
```

Тестовый запрос на получение списка таблиц производится командой:

```
\dt *
```

Для выхода из оболочки **postgres shell** выполните:

```
\q
```

Для выхода из текущей учетной записи **postgres** выполните:

```
exit
```

Дополнительные возможности для PostgreSQL

Для расширения возможностей **PostgreSQL** можно подключить каталог **contrib**. В нем содержатся модули, среди которых есть средства портирования, утилиты анализа и подключаемые функции, не включенные в состав основной системы **PostgreSQL**.

ВАЖНО!

Данные модули не включены в **PostgreSQL**, потому что они адресованы ограниченной аудитории или находятся в экспериментальном состоянии, не подходящем для основного дерева кода.

Для подключения каталога **contrib** выполните команду:

```
dnf install postgresql15-contrib
```

Решение проблемы: после установки не удается подключиться к PostgreSQL через pgadmin4

Откройте для редактирования файл **postgresql.conf**:

```
nano /var/lib/pgsql/15/data/postgresql.conf
```

Замените строку:

```
# listen_addresses = 'localhost'
```

на следующую:

```
listen_addresses = '*'
```

В файл **/var/lib/pgsql/15/data/pg_hba.conf** в качестве первой строки добавьте следующее:

```
host all all 0.0.0.0/0 md5
```

Данный параметр разрешает доступ ко всем базам данных для всех пользователей с зашифрованным паролем.

Далее необходимо задать пароль пользователю **postgres** для администрирования баз данных на сервере удаленно.

```
su - postgres
psql
ALTER USER postgres WITH ENCRYPTED PASSWORD 'yourpassword';
```

где вместо **yourpassword** укажите нужный пароль.

Для применения внесенных изменений в настройки требуется перезапустить службу **postgresql**:

```
systemctl restart postgresql-15.service
```

Для более гибкой настройки прав доступа рекомендуем обратиться к официальной документации разработчика программного обеспечения.

Установка Firebird

Установка Firebird 2.5
Установка Firebird 3.0

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** firebird 3.0.6.33328-1, firebird 2.5.9.27139.0-1

Установка Firebird 2.5

Установка осуществляется командой:

```
# dnf install firebird25
```

Для запуска **firebird** выполните команду:

```
# systemctl start firebird25-classic.socket
```

Проверка статуса службы выполняется командой:

```
$ systemctl status firebird25-classic.socket
```

Автозапуск **firebird** при запуске ОС осуществляется командой:

```
# systemctl enable firebird25-classic.socket
```

Основные файлы конфигурации будут находиться в каталоге **/etc/firebird25**, а утилиты в **/usr/lib64/firebird25/bin-classic**.

Установка Firebird 3.0

Для установки **firebird 3.0** выполните команду:

```
# dnf  install firebird
```

Для запуска **firebird** выполните команду:

```
# systemctl start firebird-superserver.service
```

Проверка статуса службы:

```
$ systemctl status firebird-superserver.service
```

Автозапуск **firebird** при запуске ОС осуществляется командой:

```
# systemctl enable firebird-superserver.service
```

Установка СУБД Ред База Данных

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** 3.0.10.0 RedDatabase

СУБД Ред База Данных (Red Database) – промышленная российская система управления базами данных с открытым кодом. Ядро СУБД Ред База Данных построено на основе одной из самых известных и распространенных в мире СУБД с открытым кодом – Firebird, которая используется в решениях.

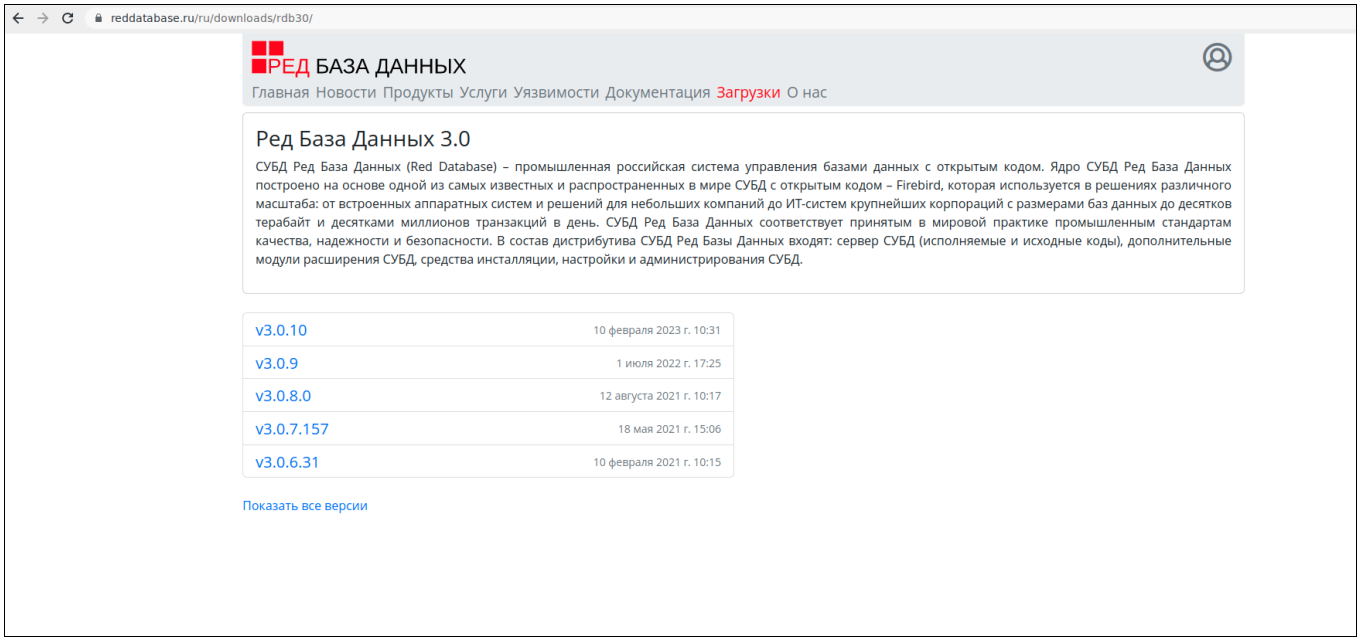
Вы можете подробнее ознакомиться с установкой **СУБД РЕД База Данных**, а также пройти обучающий курс по работе с **СУБД РЕД База Данных**, просмотрев наши обучающие видео:

- на **RuTube**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».
- в **Яндекс.Дзен**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».
- в **VK Видео**:
  - Установка СУБД Ред База Данных на РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Скачивание СУБД Ред База Данных

Скачать Red Database можно на официальном сайте - https://reddatabase.ru/downloads/rdb30/.



Для скачивания необходимо авторизоваться или зарегистрироваться.

Для установки на Linux необходимо скачать бинарный файл нужной разрядности и назначить на него права:

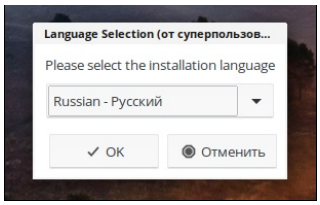
```
sudo chmod +x [путь до файла]
```

Для старта установки запускаем установочный бинарный файл:

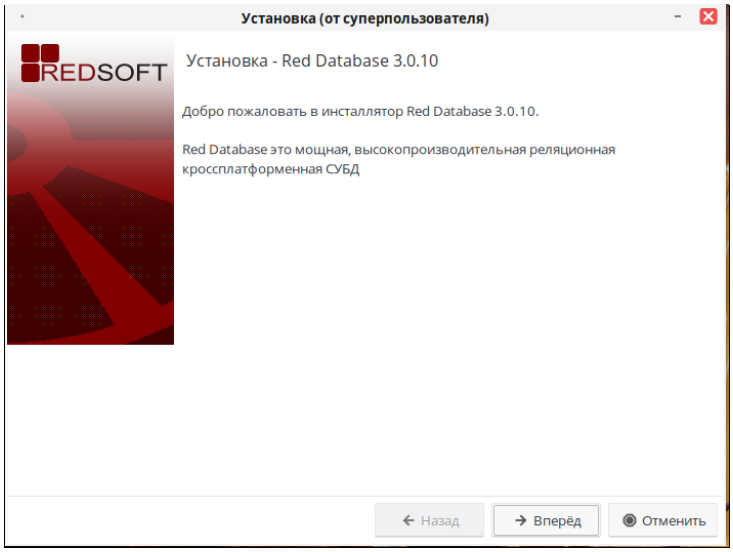
```
sudo ./rdb30-linux-x86_64-enterprise-3.0.10.bin
```

Установка

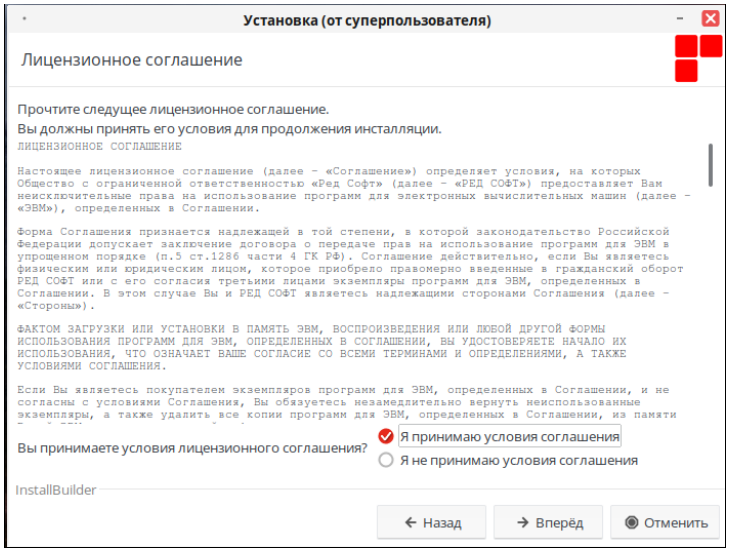
Выбор языка установки



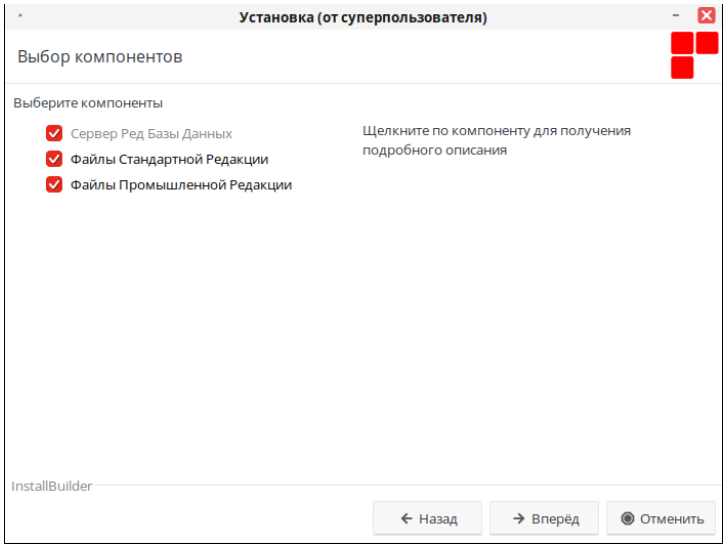
Нажмите вперед, для начала установки.



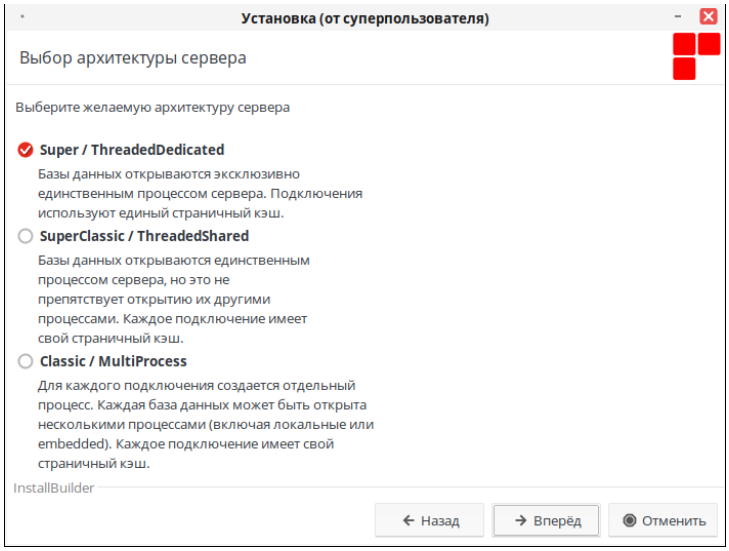
Необходимо принять условия лицензионного соглашения, перед этим прочитайте его.



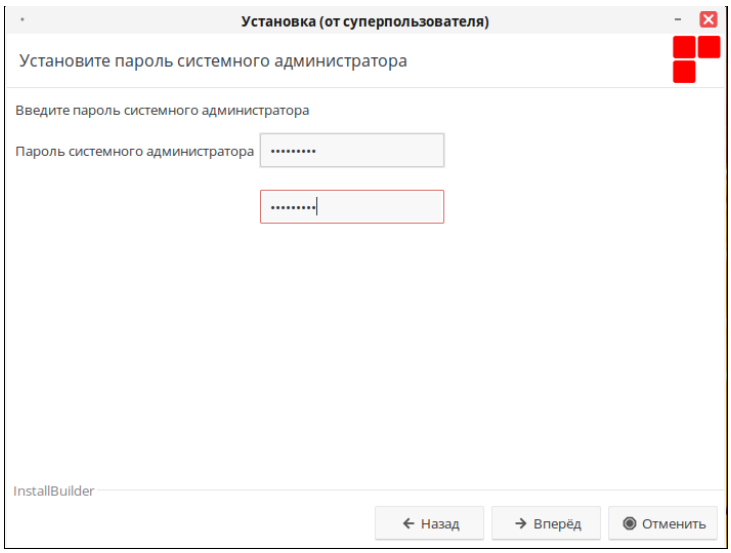
Выбор компонентов в зависимости от доступной редакции СУБД



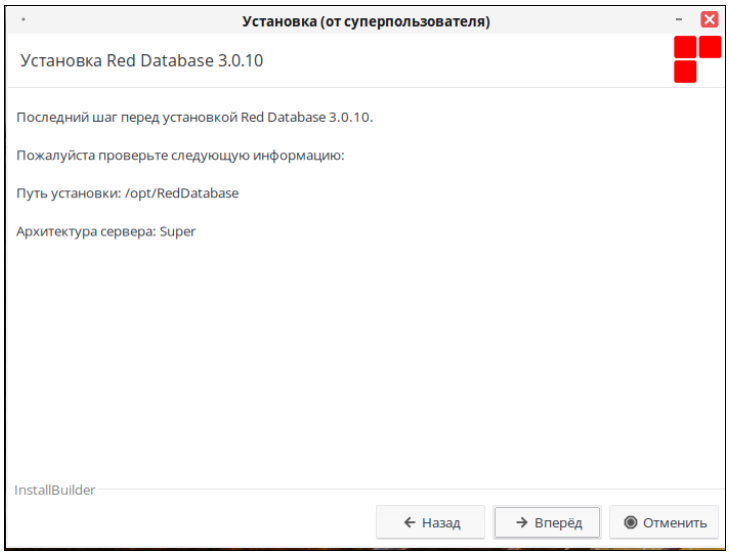
Выбор архитектуры



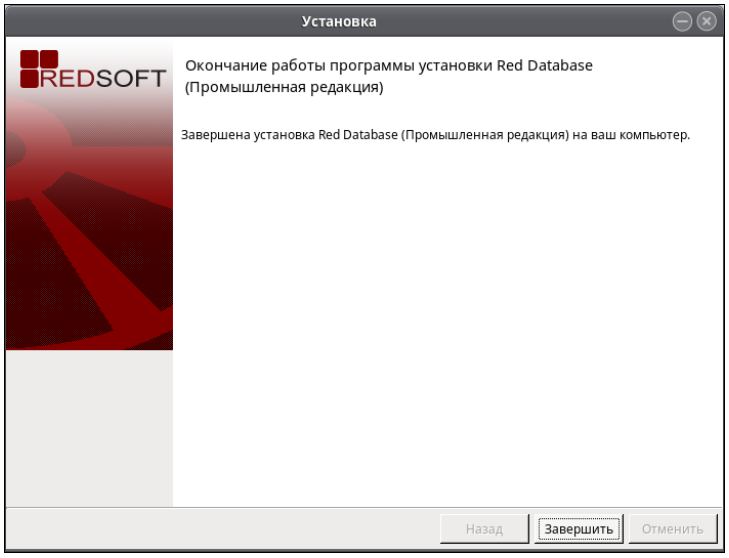
Пароль администратора, необходимо дважды указать пароль администратора.



Вывод выбранной информации.



После окончания установки необходимо нажать **"Завершить".**



Кратко об основных каталогах и файлах конфигурации.

По умолчанию все каталоги и файлы создаются в /opt/RedDatabase

/opt/RedDatabase/firebird.conf - Файл содержит параметры настройки сервера. Сервер читает все настройки с этого файла при старте (больше про настройку сервера можно прочитать в документации*)

/opt/RedDatabase/databases.conf – В этом текстовом файле можно задать алиас БД, чтобы затем в прикладных кодах использовать более короткий и удобный псевдоним для обращения к нужной базе данных. Также здесь указываются индивидуальные настройки для каждой конкретной базы данных.

Так же в каталоге /opt/RedDatabase/bin находятся утилиты для взаимодействия с БД и ее управлением.

pgAdmin4 - администрирование и разработка баз данных

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** pgadmin4-6.19-4

pgAdmin4 - это программный продукт для администрирования и разработки баз данных *PostgreSQL*. **pgAdmin4** позволяет выполнять задачи мониторинга, обслуживания, конфигурирования сервера *PostgreSQL*, а также создавать и выполнять SQL-запросы.

Для установки **pgAdmin4** перейдите в сеанс пользователя **root**:

```
su -
```

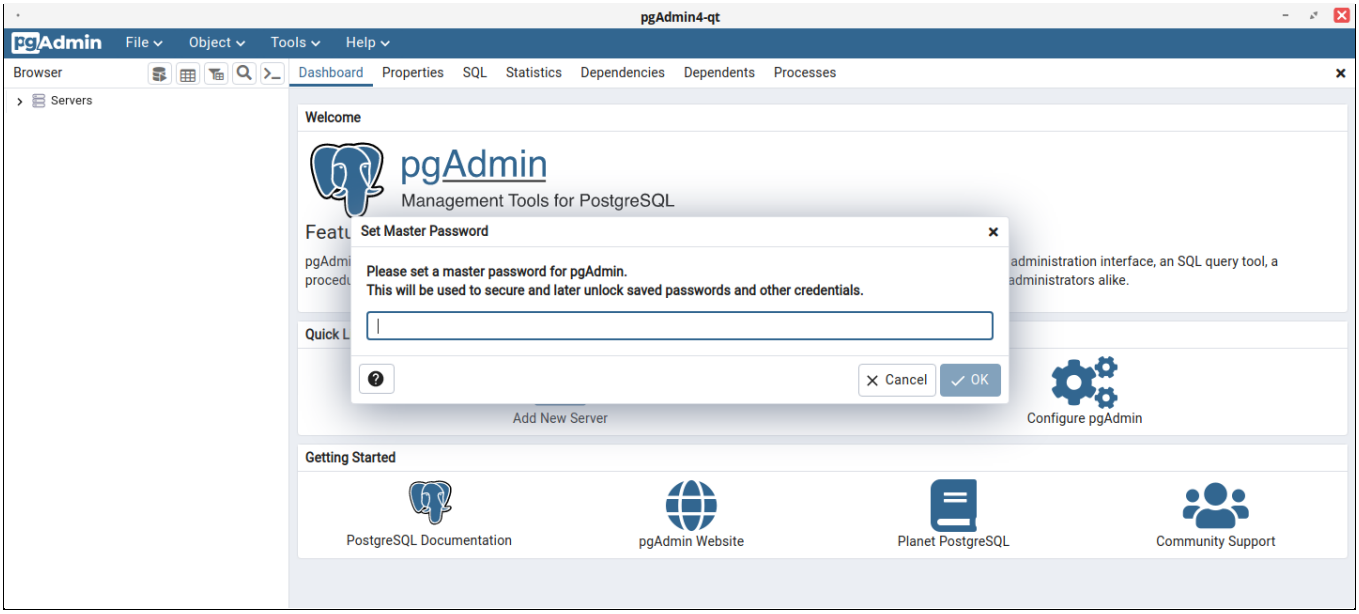
и выполните команду:

```
dnf install pgadmin4 pgadmin4-qt
```

В результате **pgAdmin4** будет доступен в **Главном меню** - «**Программирование**» - «**pgAdmin 4**».

При первом входе необходимо ввести пароль от учетной записи **root** или, при нажатии на кнопку «**Reset master Password**», установить собственный пароль для **pgadmin**.

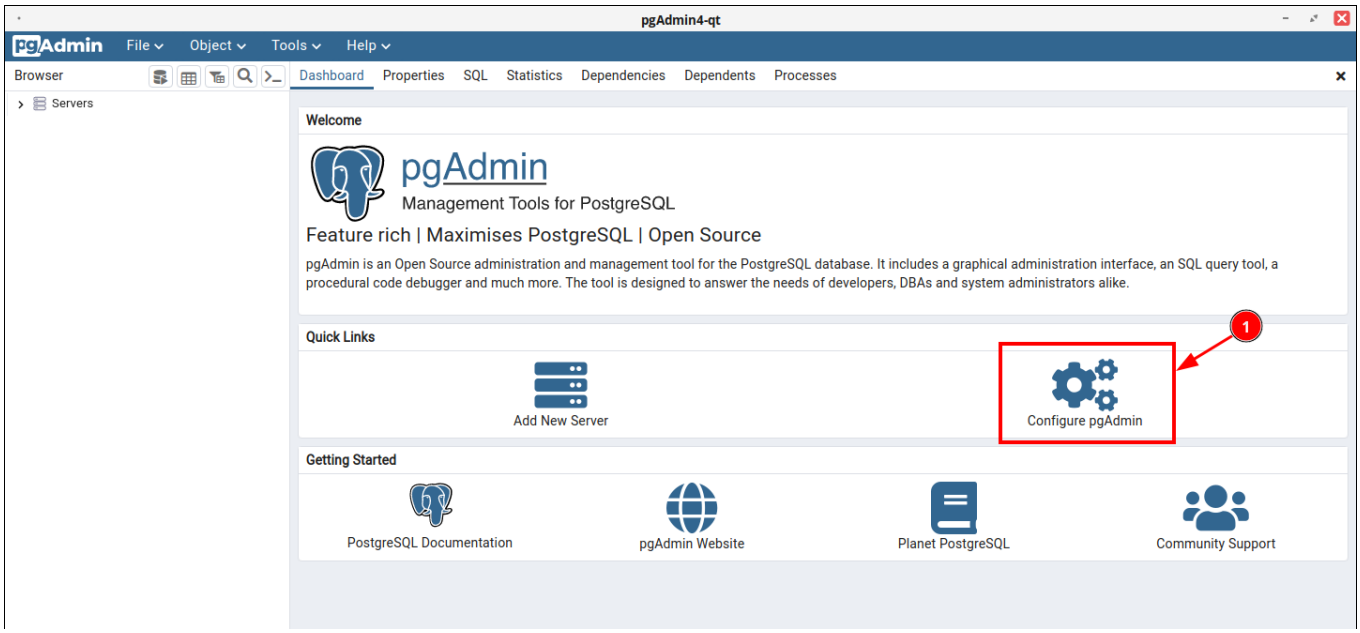
После авторизации в панели управления появится возможность настроить подключение к базам данных *PostgreSQL*.



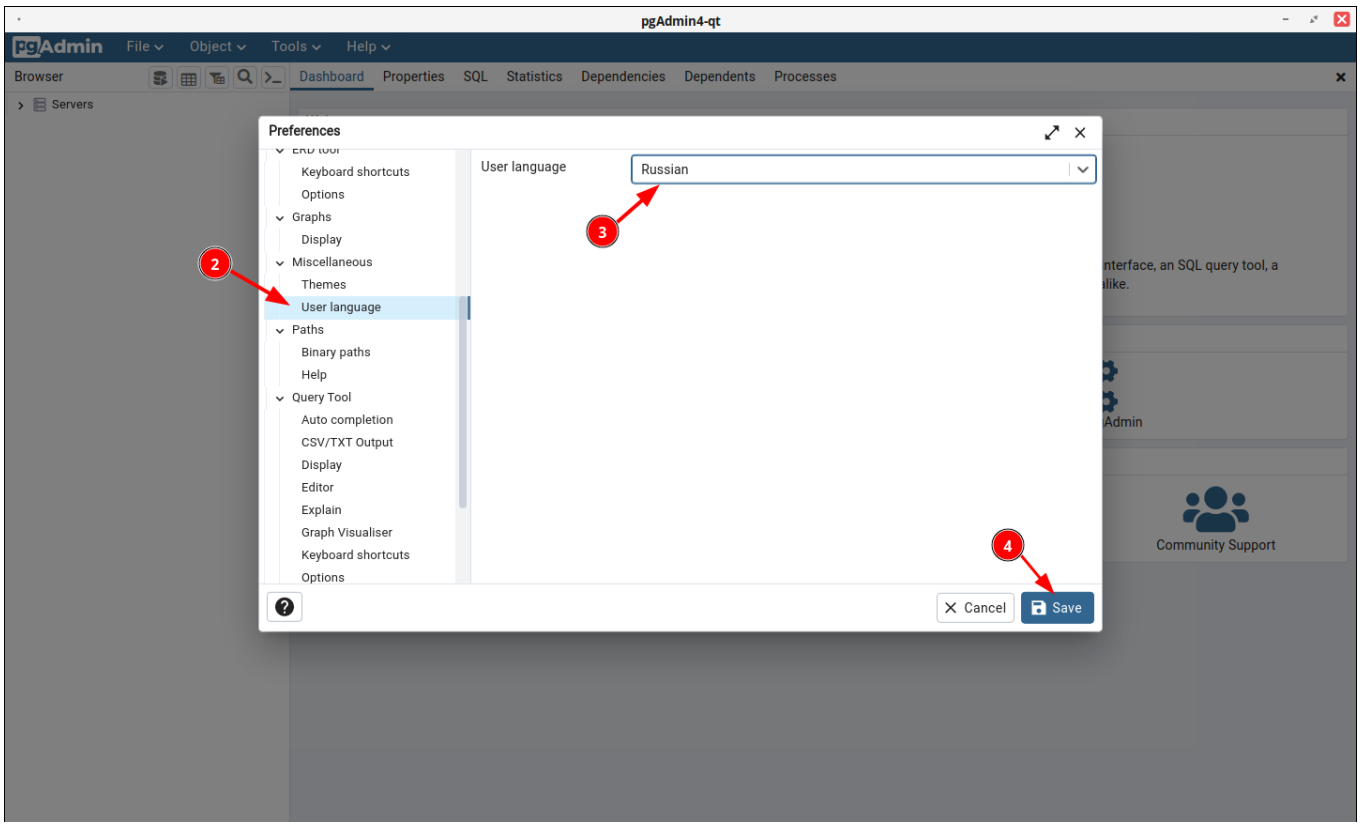
Для удобства работы можно изменить язык программы. Для этого сначала необходимо установить дополнительный пакет:

```
dnf install pgadmin4-langpack-ru
```

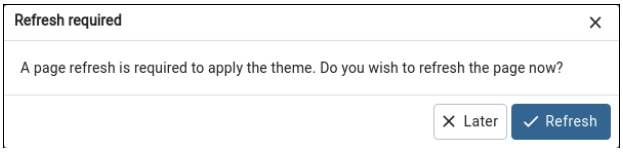
Затем на панели управления нужно выбрать «**Configure pgAdmin**».



И перейти на вкладку «**User language**», где в выпадающем списке выбрать русский язык.



После этого появится уведомление, и язык интерфейса изменится на выбранный.



В данной установке и настройке **pgAdmin4** работает только локально и нет возможности подключиться к нему с других ПК к панели администрирования.

Чтобы настроить **pgAdmin4** в качестве внешнего веб-сервиса с возможностью подключения к веб-панели **pgAdmin4** с других ПК, необходимо выполнить ряд настроек и установить дополнительные RPM-пакеты из репозитория РЕД ОС.

Настройка pgAdmin4 в качестве внешнего web-сервиса

Обратите внимание, что после настройки **pgAdmin4** в качестве внешнего веб-сервиса, графическое приложение **pgadmin4-qt** будет недоступно.

Установите дополнительные пакеты:

```
dnf install httpd python3-mod_wsgi pgadmin4-httpd
```

Создайте необходимые каталоги:

```
mkdir -p /var/log/pgadmin4/
```

Затем настройте **selinux**:

```
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_can_network_connect_db 1
semanage fcontext -a -t httpd_sys_rw_content_t "/var/lib/pgadmin4(/.*)?"
semanage fcontext -a -t httpd_sys_rw_content_t "/var/log/pgadmin4(/.*)?"
restorecon -R /var/lib/pgadmin4/
restorecon -R /var/log/pgadmin4/
```

Запустите сервис **httpd**:

```
systemctl enable httpd --now
```

Откройте файл конфигурации для редактирования:

```
nano /usr/lib/pgadmin4/config_local.py
```

и приведите его к следующему виду:

```
import os
 from config import *
 HELP_PATH = '/usr/share/doc/pgadmin4/html/'
 DATA_DIR = os.path.realpath(os.path.expanduser(u'/var/lib/pgadmin4'))
 LOG_FILE = os.path.join(DATA_DIR, 'pgadmin4.log')
 SQLITE_PATH = os.path.join(DATA_DIR, 'pgadmin4.db')
 SESSION_DB_PATH = os.path.join(DATA_DIR, 'sessions')
 STORAGE_DIR = os.path.join(DATA_DIR, 'storage')
 AZURE_CREDENTIAL_CACHE_DIR = os.path.join(DATA_DIR, 'azurecredentialcache')
 KERBEROS_CCACHE_DIR = os.path.join(DATA_DIR, 'krbccache')
 TEST_SQLITE_PATH = os.path.join(DATA_DIR, 'test_pgadmin4.db')
```

Выполните команду настройки **pgadmin4**, при этом нужно будет ввести *адрес почты* и *пароль*:

```
python /usr/lib/pgadmin4/setup.py
```

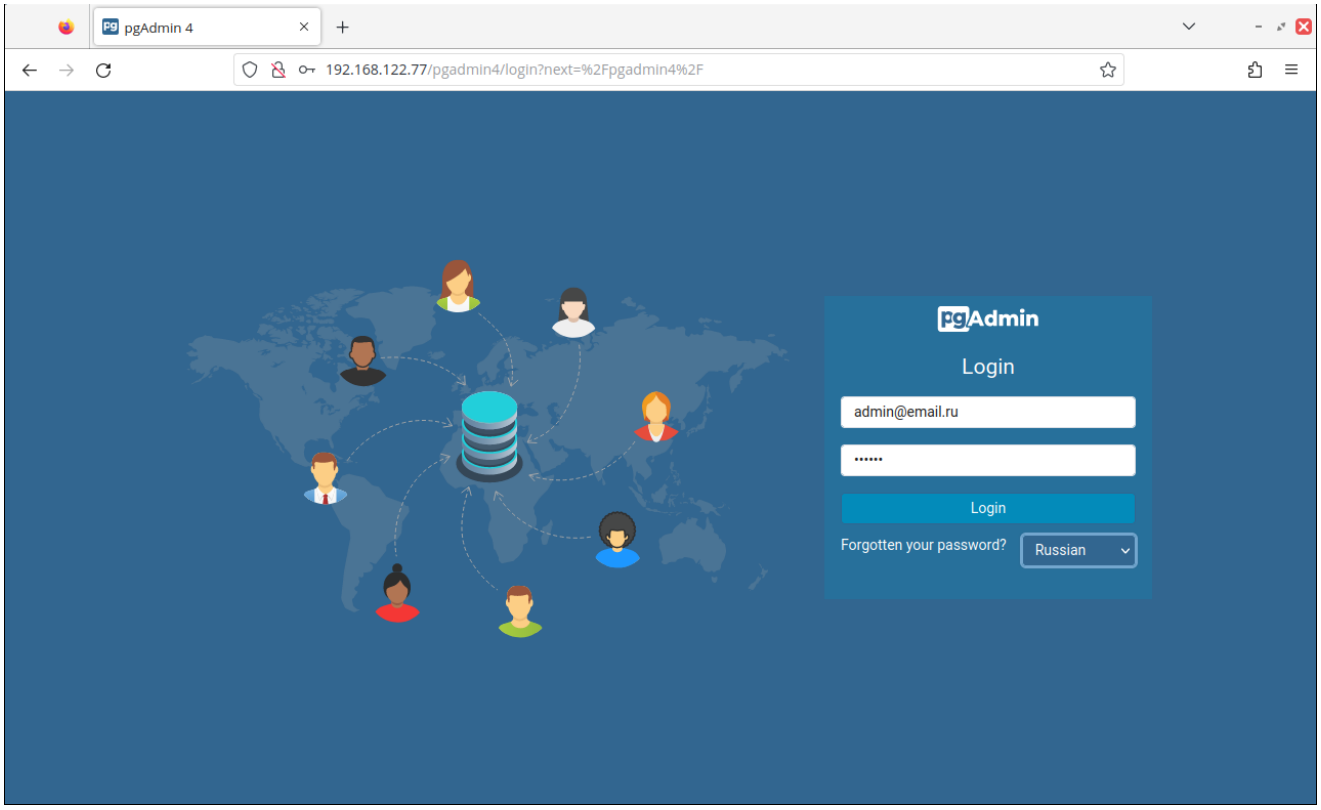
После этого выполните команду смены владельца для каталогов:

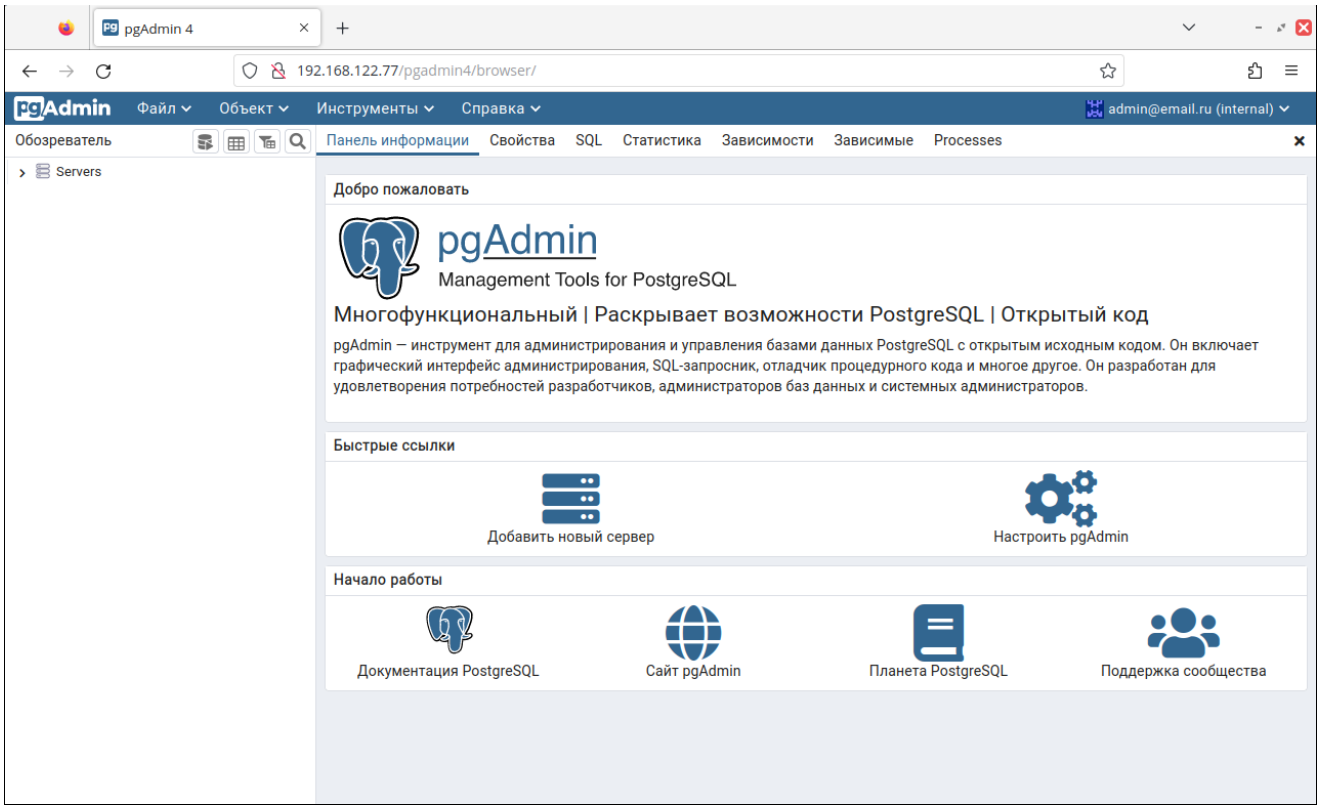
```
chown -R apache:apache /var/lib/pgadmin4 /var/log/pgadmin4
```

После чего перезапустите веб-службу:

```
systemctl restart httpd
```

После этих действий **pgadmin4** будет доступен в браузере через веб-интерфейс по адресу вашего сервера, например: http://<IP-адрес_сервера>/pgadmin4.


pgAdmin 4
192.168.122.77/pgadmin4/login?next=%2Fpgadmin4%2F
pgAdmin
Login
admin@email.ru
Login
Forgotten your password?
Russian


pgAdmin 4
192.168.122.77/pgadmin4/browser/
pgAdmin
Файл
Объект
Инструменты
Справка
admin@email.ru (internal)
Обозреватель
Servers
Панель информации
Свойства
SQL
Статистика
Зависимости
Зависимые
Processes
Добро пожаловать
pgAdmin
Management Tools for PostgreSQL
Многофункциональный | Раскрывает возможности PostgreSQL | Открытый код
pgAdmin — инструмент для администрирования и управления базами данных PostgreSQL с открытым исходным кодом. Он включает графический интерфейс администрирования, SQL-запросник, отладчик процедурного кода и многое другое. Он разработан для удовлетворения потребностей разработчиков, администраторов баз данных и системных администраторов.
Быстрые ссылки
Добавить новый сервер
Настроить pgAdmin
Начало работы
Документация PostgreSQL
Сайт pgAdmin
Планета PostgreSQL
Поддержка сообщества

Настройка Postgresql для 1С

Вы можете подробнее ознакомиться с настройкой **postgresql**, просмотрев наши обучающие видео:

- на **RuTube** — Настройка сервера баз данных для сервера 1С;
- в **Яндекс.Дзен** — Настройка сервера баз данных для сервера 1С;
- в **VK Видео** — Настройка сервера баз данных для сервера 1С.

На наших каналах вы также сможете найти много другой полезной информации.

Настройка postgresql

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Измените имя сервера:

```
hostnamectl set-hostname serv.1ctest.ru
```

где **serv.1ctest.ru** - нужное имя вашего сервера.

Отредактируйте **/etc/hosts**:

```
nano /etc/hosts
```

Добавьте строку:

```
127.0.0.1 serv.1ctest.ru
```

Установка

Установка **postgresql** для 1С:

```
dnf install postgresql-1c postgresql-1c-contrib postgresql-1c-libs postgresql-1c-plperl postgresql-1c-plpython3 postgresql-1c-pltcl postgresql-1c-server
```

Настройка **postgresql**:

```
su - postgres
```

Откройте файл, в котором будут заданы необходимые переменные окружения:

```
nano .bash_profile
```

> **Примечание.**
>
> Необходимо указать вашу версию **postgresql** (выделена красным цветом).

Добавляем в этот файл переменные:

```
export PATH=/usr/pgsql-14/bin:$PATH
export MANPATH=/usr/pgsql-14/share/man:$MANPATH
```

Пример листинга файла:

```
[ -f /etc/profile ] && source /etc/profile
PGDATA=/var/lib/pgsql/14/data export PGDATA
# If you want to customize your settings,
```

```
# Use the file below. This is not overridden
# by the RPMS.

export PATH=/usr/pgsql-14/bin:$PATH
export MANPATH=/usr/pgsql-14/share/man:$MANPATH

[ -f /var/lib/pgsql/.pgsql_profile ] && source /var/lib/pgsql/.pgsql_profile
```

Далее с правами того же пользователя **postgres** выполните команду инициализации БД:

> **Примечание.**
>
> **Минимальный объём** оперативной памяти для инициализации БД - **4 ГБ**.

```
initdb
```

Если команда не найдена, пропишите полный путь:

```
/usr/pgsql-14/bin/initdb
```

Выйдите из текущей учетной записи:

```
exit
```

Запуск и добавление в автозагрузку сервера **PostgreSQL**:

```
systemctl enable postgresql-14 --now
```

Проверка статуса сервиса:

```
systemctl status postgresql-14
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Изменение настроек сервера PostgreSQL

Для возможности пользователю **postgres** авторизоваться по паролю, внесите изменения в файл **/var/lib/pgsql/14/data/pg_hba.conf**:

```
nano /var/lib/pgsql/14/data/pg_hba.conf
```

```
host all all 0.0.0.0/0 trust

на

host all all 0.0.0.0/0 md5
```

Внесите изменения в файл **/var/lib/pgsql/14/data/postgresql.conf**, исходя из характеристик сервера:

```
nano /var/lib/pgsql/14/data/postgresql.conf
```

> **Примечание.**
>
> Подбор данных настроек производится индивидуально и зависит как от характеристик сервера, на котором будет работать сервер **PostgreSQL**, так и от характеристик информационных баз, которые будут обрабатываться на этом сервере.

Параметры, требующие настройки:

```
listen_addresses = '*'
```

```
password_encryption = md5
shared_buffers = 4096MB
temp_buffers = 256MB
work_mem = 128MB
maintenance_work_mem = 192MB
effective_cache_size = 4GB
```

Задайте пароль пользователю **postgres**, для того чтобы была возможность подключаться к серверу удаленно.

```
su - postgres
psql
ALTER USER postgres WITH ENCRYPTED PASSWORD 'yourpassword';
(вместо yourpassword поставьте нужный пароль)
```

Рестарт сервера **PostgreSQL**:

```
systemctl stop postgresql-14
systemctl start postgresql-14
systemctl status postgresql-14
```

1С-сервер для РЕД ОС

Установка 1С-сервера для РЕД ОС
Запуск сервиса для версии сервера 8.3.21.xxxx
Администрирование 1С

Вы можете подробнее ознакомиться с установкой и настройкой сервера 1С, просмотрев наши обучающие видео:

- на **RuTube** — Настройка сервера баз данных для сервера 1С;
- в **Яндекс.Дзен** — Настройка сервера баз данных для сервера 1С;
- в **VK Видео** — Настройка сервера баз данных для сервера 1С.

На наших каналах вы также сможете найти много другой полезной информации.

Установка 1С-сервера для РЕД ОС

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Перед началом установки сервера необходимо поставить последние обновления РЕД ОС.

```
dnf update
```

Примечание.

Для РЕД ОС **рекомендуется** использовать сервер 1С:Предприятия **8.3.20.xxxx и выше**.

Загрузите дистрибутив 1С, который был запрошен у производителя для linux (***данные пакеты не являются нашей разработкой и, соответственно, отсутствуют в репозитории РЕД ОС***).

Установите дополнительные пакеты шрифтов:

```
dnf install libxcrypt-compat msttcore-fonts-installer
```

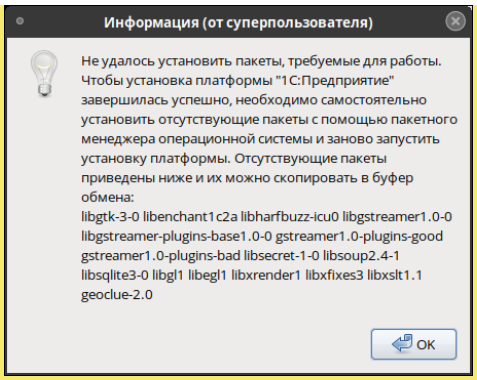
Начиная с версии **8.3.20.xxxx**, фирма 1С изменила формат распространения дистрибутива для Linux-систем. Теперь он распространяется в формате **run**. Для установки сервера run-файл требуется сделать исполняемым, запустить и доустановить пакеты из репозитория:

```
chmod +x setup-full-8.3.21.1197-x86_64.run
./setup-full-8.3.21.1197-x86_64.run --mode unattended --disable-components client_full --enable-components
server,ws,server_admin,config_storage_server,liberica_jre
```

Будет произведена установка всех необходимых компонентов и модулей без отображения диалоговых окон установщика.

Примечание.

Если вы используете графический вариант установки сервера 1С, будет выведено предупреждение о возможных отсутствующих дополнительных пакетах. **Данное сообщение не является ошибкой!**



Запуск сервиса для версии сервера 8.3.21.xxxx

После установки необходимо создать ссылку на сервис сервера 1С:

```
systemctl link /opt/1cv8/x86_64/8.3.21.1197/srv1cv8-8.3.21.1197@.service
```

Запустите сервис и добавьте его в автозагрузку командой:

```
systemctl enable srv1cv8-8.3.21.1197@default.service --now
```

Команда проверки статуса сервиса:

```
systemctl status srv1cv8-8.3.21.1197@default.service
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Администрирование 1С

Настройка 1С-сервера производится через консоль администратора 1С.

Сначала запустите кластер серверов 1С следующей командой:

```
/opt/1cv8/x86_64/8.3.21.1197/ras --daemon cluster
```

Для получения информации о кластере в терминале введите команду:

```
/opt/1cv8/x86_64/8.3.21.1197/rac cluster list
```

Листинг информации:

```
cluster : 163e5d4d-152a-4584-a176-48109eb261f6
 host : ro731serv1c83211197
 port : 1541
 name : "Локальный кластер"
 expiration-timeout : 60
 lifetime-limit : 0
 max-memory-size : 0
 max-memory-time-limit : 0
 security-level : 0
 session-fault-tolerance-level : 0
 load-balancing-mode : performance
 errors-count-threshold : 0
 kill-problem-processes : 1
 kill-by-memory-with-dump : 0
```

Для дальнейших операций сохраните себе название кластера «**163e5d4d-152a-4584-a176-48109eb261f6**». Вместо элементов,

выделенных красным цветом, вставьте свои параметры.

Добавление базы производится командой:

```
/opt/1cv8/x86_64/8.3.21.1197/rac infobase --cluster=163e5d4d-152a-4584-a176-48109eb261f6 create --create-database --name=test_bd --dbms=PostgreSQL --db-server=ro731serv1c83211197 --db-name=test_bd --locale=ru --db-user=postgres --db-pwd=yourpassword  --license-distribution=allow
```

При добавлении новой базы данных может появиться ошибка вида:

```
Ошибка операции администрирования
Сервер баз данных не обнаружен
authentication method 10 not supported
```

Для решения данной проблемы необходимо:

1. В конфигурационном файле **postgresql.conf** скорректировать настройку **password_encryption** на **md5** вместо **scram-sha-256**:

```
password_encryption = md5  # scram-sha-256 or md5
```

2) Перезапустить службу **postgresql**:

```
systemctl restart postgresql-14
```

где **postgresql-14** - служба для РЕД ОС.

3) Установить (Обновить) пароль пользователя, с правами которого настраивается подключение к **postgresql**. Ниже приведен пример для пользователя **postgres**:

```
su - postgres
psql
ALTER USER postgres WITH ENCRYPTED PASSWORD 'yourpassword';
```

где **yourpassword** - установленный вами пароль.

Краткая информация о параметрах команды:

Параметр	Описание
--create-database	При создании информационной базы создать базу данных
--name=<name>	(**обязательный**) имя информационной базы
--dbms=MSSQLServer | PostgreSQL | IBMDB2 | OracleDatabase	(**обязательный**) тип СУБД, в которой размещается информационная база: • *MSSQLServer* — MS SQL Server; • *PostgreSQL* — PostgreSQL; • *IBMDB2* — IBM DB2; • *OracleDatabase* — Oracle Database.
--db-server=<host>	(**обязательный**) имя сервера баз данных
--db-name=<name>	(**обязательный**) имя базы данных
--locale=<locale>	(**обязательный**) идентификатор национальных настроек информационной базы
--b-user=<name>	имя администратора базы данных
--db-pwd=<pwd>	пароль администратора базы данных
--descr=<descr>	описание информационной базы
--date-offset=<offset>	смещение дат в информационной базе
--security-level=<level>	уровень безопасности установки соединений с информационной базой
--scheduled-jobs-deny=on | off	управление блокировкой выполнения регламентных заданий: • *on* — выполнение регламентных заданий запрещено; • *off* — выполнение регламентных заданий разрешено.
--license-distribution=deny | allow	управление выдачей лицензий сервером 1С:Предприятия: • deny — выдача лицензий запрещена; • allow — выдача лицензий разрешена.

Для получения списка баз введите в терминале команду:

```
/opt/1cv8/x86_64/8.3.21.1197/rac infobase --cluster=163e5d4d-152a-4584-a176-48109eb261f6 summary list
```

Пример вывода:

```
infobase : 8a3f7235-37c7-403f-bd3c-bce5a8d9b40a
name : test_bd
descr :
```

Для удаления БД введите команду:

```
/opt/1cv8/x86_64/8.3.21.1197/rac infobase --cluster=163e5d4d-152a-4584-a176-48109eb261f6 drop --infobase=8a3f7235-37c7-403f-bd3c-bce5a8d9b40a
```

Не забудьте также удалить базу из **postgresql**:

```
su postgres
psql
\l
DR OP DATABASE test_bd;
\q
```

Публикация БД на web-сервере 1С

Подготовка веб-сервера
Установка 1С
Публикация БД

Примечание.

Для публикации базы на веб-сервере у вас уже должна быть подготовлена и настроена БД на сервере 1С.

Подготовка веб-сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Установите **apache**:

```
dnf install httpd
```

Настройте SELinux:

```
setsebool -P httpd_can_network_connect on
```

Добавьте в автозагрузку и запустите веб-сервер:

```
systemctl enable httpd --now
```

Статус службы веб-сервера можно проверить командой:

```
systemctl status httpd
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Далее необходимо проверить корректность работы **apache**. Для этого создайте в каталоге **/var/www/html/** файл **index.html** с любым содержанием, например, «**Page available**».

```
nano /var/www/html/index.html
```

Для сохранения внесенных изменений нажмите «**Ctrl+O**», «**Enter**» и для выхода из редактора - «**Ctrl+X**».

Установите имя веб-сервера:

```
hostnamectl set-hostname ro731webserv1c83211197
```

где **ro731webserv1c83211197** - нужное имя сервера.

Измените файл **/etc/hosts**, добавьте ip-адрес веб-сервера и его имя:

```
nano /etc/hosts
```

```
10.1.10.1 ro731webserv1c83211197
```

(вместо **10.1.10.1** введите IP-адрес вашего веб-сервера, а вместо **ro731webserv1c83211197** имя вашего веб-сервера).

Если БД находится на другом сервере, в **/etc/hosts** также необходимо прописать IP-адрес и имя сервера расположения базы.

Проверим доступность станицы http://ro731webserv1c83211197/ в браузере, где **ro731webserv1c83211197** - имя вашего веб-сервера.

Установка 1С

Загрузите дистрибутив 1С, который был запрошен у производителя для linux (***данные пакеты не являются нашей разработкой и, соответственно, отсутствуют в репозитории РЕД ОС***).

Установите дополнительные пакеты и назначьте run-файлу права на исполнение:

```
dnf install libxcrypt-compat msttcore-fonts-installer
chmod +x setup-full-8.3.21.1197-x86_64.run
```

Для запуска установки выполните команду:

```
./setup-full-8.3.21.1197-x86_64.run --mode unattended --disable-components client_full --enable-components
server,ws,server_admin,config_storage_server,liberica_jre
```

Публикация БД

После завершения установки перейдите в каталог 1С:

```
cd /opt/1cv8/x86_64/8.3.21.1197
```

Опубликуйте базу на веб-сервере командой:

```
./webinst -apache24 -wsdir test_bd -dir /var/www/test_bd -connstr "Srvr=ro731serv1c83211197;Ref=test_bd;" -confPath
/etc/httpd/conf/httpd.conf
```

(где **ro731serv1c83211197** - имя сервера расположения базы, которую вы хотите опубликовать, **test_bd** - имя вашей базы, которую вы хотите опубликовать, а **/var/www/test_bd** - каталог, в котором будет содержаться конфигурационный файл веб-клиента, он должен обязательно располагаться в **/var/www**).

Проверьте, что в конфигурационном файле **apache** появилась необходимая запись о загрузке:

```
nano /etc/httpd/conf/httpd.conf
```

Для версии **8.3.21.1197** запись в конце файла будет выглядеть:

```
LoadModule _1cws_module "/opt/1cv8/x86_64/8.3.21.1197/wsap24.so"
```

Добавьте в тот же файл строку:

```
ServerName ro731webserv1c8321119
```

(где **ro731webserv1c8321119** - имя вашего веб-сервера).

Параметры веб-сервера можно менять в файле **default.vrd**. В примере каталогом расположения данного файла будет **/var/www/test_bd**.

Проверка синтаксиса конфигурационных файлов **apache** осуществляется командой:

```
apachectl -t
```

Перезапустите **apache**:

```
systemctl restart httpd
```

Перезагрузите компьютер.

После перезагрузки сервера, если всё было настроено правильно, доступ к БД можно будет получить из браузера или через приложение, указав адрес http://ro731webserv1c8321119/test_bd, (где **ro731webserv1c8321119** - имя вашего веб-сервера, **test_bd** - имя вашей публикуемой базы).

1С-клиент

Установка клиента 1С
Подключение к БД
Установка драйвера ключа аппаратной лицензии
Решение возникающих проблем
Возможные проблемы при установке пакетов
Возможные проблемы при запуске программы

Вы можете подробнее ознакомиться с установкой и настройкой клиента 1С, просмотрев наши обучающие видео:

- на **RuTube** — Настройка сервера баз данных для сервера 1С;
- в **Яндекс.Дзен** — Настройка сервера баз данных для сервера 1С;
- в **VK Видео** — Настройка сервера баз данных для сервера 1С.

На наших каналах вы также сможете найти много другой полезной информации.

Установка клиента 1С

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

Загрузите дистрибутив 1С, который был запрошен у производителя для linux (***данные пакеты не являются нашей разработкой и, соответственно, отсутствуют в репозитории РЕД ОС***).

Установка производится командой:

```
dnf install 1c-enterprise-8.3.19.1522-client-8.3.19.1522.x86_64.rpm 1c-enterprise-8.3.19.1522-common-8.3.19.1522.x86_64.rpm 1c-enterprise-8.3.19.1522-server-8.3.19.1522.x86_64.rpm
```

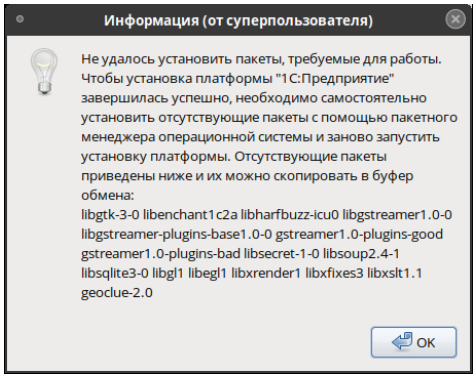
Начиная с версии **8.3.20.xxxx**, 1С:Предприятие для Linux распространяется в формате **run**, поэтому алгоритм установки отличается.

Для установки необходимо назначить run-файлу права на исполнение и запустить его:

```
chmod +x setup-full-8.3.21.1197-x86_64.run
./setup-full-8.3.21.1197-x86_64.run
```

Затем нужно следовать инструкциям в менеджере установки 1С.

При установке будет выведено предупреждение о возможных отсутствующих дополнительных пакетах (**не является ошибкой!**).



Установите необходимые шрифты:

```
dnf install msttcore-fonts-installer
```

Измените файл **/etc/hosts**, добавьте ip-адрес вашего сервера и его имя:

```
nano /etc/hosts
```

```
45.14.51.45 serv.1ctest.ru
```

где **45.14.51.45** - IP-адрес вашего сервера.

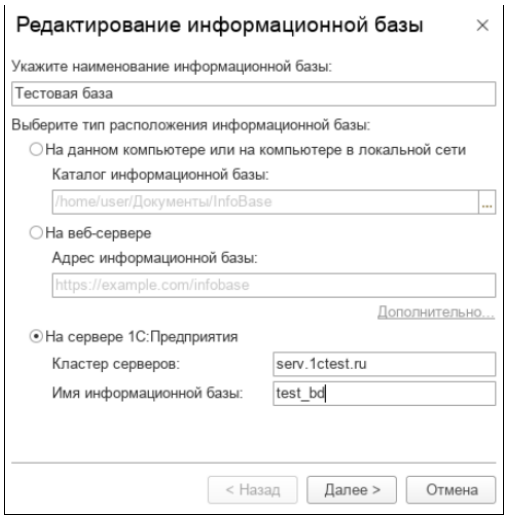
Перезагрузите систему. **После перезагрузки** установленная программа будет доступна в «**Главном меню**» - «**Офис**» - «**1С:Предприятие**».

Подключение к БД

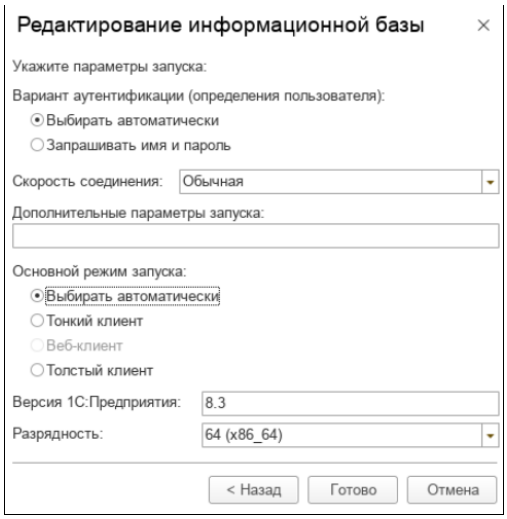
Для проверки подключения к базе данных, находящейся на сервере, запустите клиент 1С:Предприятия из «**Главного меню**» - «**Офис**» - «**1С:Предприятие**».

Выберите пункт «**Добавить**», затем «**Включение в список уже ранее созданной информационной базы**».

Введите **имя сервера** и **название информационной базы**:



После нажатия кнопки «**Далее**» необходимо выбрать **версию** 1С и **разрядность**:



При правильно введенных данных подключение к БД пройдет успешно.

Установка драйвера ключа аппаратной лицензии

Драйвер аппаратной лицензии можно скачать со страницы производителя:

https://thales-sentinel.ru/helpdesk/download-space/

Распакуйте архив в каталог удобным для вас способом и перейдите в него:

```
cd /home/user/Загрузки/Sentinel_LDK_RedHat_and_SuSE_RPM_Run-time_Installer
```

Внутри находятся пакеты под разные архитектуры. Установим **rpm** для **x86_64**:

```
dnf install aksusbd-8.43-1.x86_64.rpm
```

Статусы служб драйвера ключей и менеджера лицензий можно посмотреть следующими командами:

```
systemctl status aksusbd
systemctl status hasplmd
```

В выводе команды должно быть отображено **"Active: active (running)"**.

Решение возникающих проблем

Возможные проблемы при установке пакетов

Вариант 1. При попытке установки 1С-клиента может возникнуть ошибка вида:

```
 dnf install 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64

 Проблема: противоречивые запросы - nothing provides libwebkitgtk-3.0.so.0()(64bit) needed by 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64
```

Для решения данной проблемы выполните команду установки через менеджер пакетов RPM с выводом всех действий на экран и без контроля всех зависимостей:

```
rpm -ivh --nodeps 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64.rpm
```

Вариант 2. При попытке установки 1С-клиента ранних версий (например, **3.8.6**) может возникнуть ошибка вида:

```
 dnf install 1C_Enterprise83-client-8.3.6-2299.x86_64

 Проблема: противоречивые запросы - nothing provides libwebkitgtk-1.0.so.0()(64bit) needed by 1C_Enterprise83-client-8.3.6-2299.x86_64
```

где 8.3.6-2299 – используемая версия 1С-клиента.

Для решения данной проблемы необходимо установить пакет **libwebkitgtk-1.0**, выполнив команду:

```
dnf install libwebkitgtk1.00
```

После этого повторить попытку установки 1С-клиента.

Возможные проблемы при запуске программы

Вариант 1. При запуске 1С-клиента может возникнуть ошибка вида:

```
 /opt/1cv8/x86_64/8.3.24.1467/1cv8s

 /opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libwebkit2gtk-4.0.so.37)
 /opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libjavascriptcoregtk-4.0.so.18)
```

где 8.3.24.1467 – используемая версия 1С-клиента.

Для решения данной проблемы рекомендуется создать символическую ссылку на библиотеку, используя следующие команды:

```
mv /opt/1cv8/common/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6
mv /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6
```

где 8.3.24.1467 – используемая версия 1С-клиента.

После этого повторите запуск клиента.

Вариант 2. При запуске 1С-клиентов ранних версий (**до версии 8.3.20**) может возникать ошибка вида:

```
/opt/1cv8/common/1cestart

/opt/1C/v8.3/x86_64/1cestart: error while loading shared libraries: libwebkitgtk-3.0.so.0: cannot open shared object file: No such file or directory
```

Для решения данной проблемы необходимо проверить наличие установленных пакетов **webkit2gtk4.0** и **javascriptcoregtk4.0** в используемой системе:

```
rpm -qa | grep webkit2gtk4.0
rpm -qa | grep javascriptcoregtk4.0
```

По умолчанию пакеты установлены в РЕД ОС.

Если по каким-либо причинам пакеты в вашей системе не установлены, выполните команду:

```
dnf install webkit2gtk4.0 javascriptcoregtk4.0
```

Далее необходимо создать символические ссылки на библиотеки, выполнив команды:

```
ln -sf /usr/lib64/{libjavascriptcoregtk-4.0.so.18,libjavascriptcoregtk-3.0.so.0}
ln -sf /usr/lib64/{libjavascriptcoregtk-4.0.so.18,libjavascriptcoregtk-3.0.so.0.16.19}
ln -sf /usr/lib64/{libwebkit2gtk-4.0.so.37,libwebkitgtk-3.0.so.0}
ln -sf /usr/lib64/{libwebkit2gtk-4.0.so.37,libwebkitgtk-3.0.so.0.22.17}
```

После этого повторите запуск клиента.

1С-клиент. Установка нескольких версий

Установка
Решение возникающих проблем
Возможные проблемы при установке пакетов
Возможные проблемы при запуске программы

Установка

Примечание.

Данные действия необходимы только при использовании клиентов 1С:Предприятие версии **8.3.18.xxxx или более ранних** .

Если вы используете версии новее, то установка нескольких версий предусмотрена уже самой фирмой 1С.

В качестве примера будет рассмотрена установка клиентов версий **8.3.16.1359** и **8.3.17.1989**. Далее по тексту «Клиент 1» и «Клиент 2» соответственно.

Распакуйте скачанные заранее архивы клиентов в разные для каждой версии каталоги.

```
mkdir ~/Загрузки/8.3.17
cp <название_архива> ~/Загрузки/8.3.17
cd ~/Загрузки/8.3.17
tar xvzf <название_архива>
```

Создайте папку для распаковки **.rpm** в каталоге «Клиента 2» (в примере **1C_8.3.17.1989**) и перейдите в него:

```
mkdir ~/Загрузки/8.3.17/1C_8.3.17.1989
cd ~/Загрузки/8.3.17/1C_8.3.17.1989
```

Выполните команду распаковки от **локального** пользователя (не от администратора):

```
for i in ../*.rpm; do rpm2cpio $i | cpio -id; done
```

В директории появятся каталоги **opt** и **usr**.

Скопируйте папку **1C_8.3.17.1989** с распакованными файлами, например, в корень. Для копирования в корень требуются права администратора:

```
cp -r ~/Загрузки/8.3.17/1C_8.3.17.1989 /
```

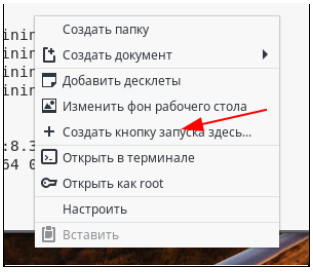
Затем установите «Клиент 1» 1С (в примере версия **8.3.16**):

```
cd ~/Загрузки
mkdir ~/Загрузки/8.3.16
cp <название_архива> ~/Загрузки/8.3.16
cd ~/Загрузки/8.3.16
tar xvzf <название_архива>
dnf install *.rpm
```

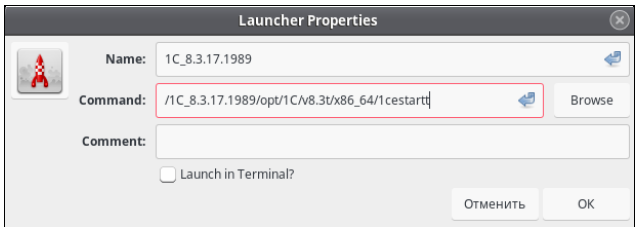
После всех выполненных действий можно запустить несколько версий платформы. Одну — через «**Главное меню**» - «**Офис**» (8.3.16), вторую — из каталога **1C_8.3.17**.

Можно создать кнопку для более удобного запуска «Клиента 2».

Нажмите правой кнопкой мыши по рабочему столу и выберите пункт «**Создать кнопку запуска здесь...**».



В открывшейся форме укажите **имя ярлыка** и **путь** до *1cestartt* (**/1C_8.3.17.1989/opt/1C/v8.3/x86_64/1cestartt**).



Решение возникающих проблем

Возможные проблемы при установке пакетов

При попытке установки 1С-клиента может возникнуть ошибка вида:

```
dnf install 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64

Проблема: противоречивые запросы - nothing provides libwebkitgtk-3.0.so.0()(64bit) needed by 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64
```

Для решения данной проблемы выполните команду установки через менеджер пакетов RPM с выводом всех действий на экран и без контроля всех зависимостей:

```
rpm -ivh --nodeps 1c-enterprise-8.3.18.1959-common-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-client-8.3.18-1959.x86_64.rpm 1c-enterprise-8.3.18.1959-server-8.3.18-1959.x86_64.rpm
```

Возможные проблемы при запуске программы

Вариант 1. При запуске 1С-клиента может возникнуть ошибка вида:

```
/opt/1cv8/x86_64/8.3.24.1467/1cv8s

/opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libwebkit2gtk-4.0.so.37)
/opt/1cv8/x86_64/8.3.24.1467/1cv8s: /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6: version `GLIBCXX_3.4.29' not found (required by /lib64/libjavascriptcoregtk-4.0.so.18)
```

где 8.3.24.1467 – используемая версия 1С-клиента.

Для решения данной проблемы рекомендуется создать символическую ссылку на библиотеку, используя следующие команды:

```
mv /opt/1cv8/common/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/common/libstdc++.so.6
mv /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6.old
ln -s /usr/lib/x86_64-linux-gnu/libstdc++.so.6 /opt/1cv8/x86_64/8.3.24.1467/libstdc++.so.6
```

где 8.3.24.1467 – используемая версия 1С-клиента.

После этого повторите запуск клиента.

Вариант 2. При запуске 1С-клиентов ранних версий (**до версии 8.3.20**) может возникать ошибка вида:

```
/opt/1cv8/common/1cestart

/opt/1C/v8.3/x86_64/1cestart: error while loading shared libraries: libwebkitgtk-3.0.so.0: cannot open shared object file: No such file or directory
```

Для решения данной проблемы необходимо проверить наличие установленных пакетов **webkit2gtk4.0** и **javascriptcoregtk4.0** в используемой системе:

```
rpm -qa | grep webkit2gtk4.0
```

```
rpm -qa | grep javascriptcoregtk4.0
```

По умолчанию пакеты установлены в РЕД ОС.

Если по каким-либо причинам пакеты в вашей системе не установлены, выполните команду:

```
dnf install webkit2gtk4.0 javascriptcoregtk4.0
```

Далее необходимо создать символические ссылки на библиотеки, выполнив команды:

```
ln -sf /usr/lib64/{libjavascriptcoregtk-4.0.so.18,libjavascriptcoregtk-3.0.so.0}
ln -sf /usr/lib64/{libjavascriptcoregtk-4.0.so.18,libjavascriptcoregtk-3.0.so.0.16.19}
ln -sf /usr/lib64/{libwebkit2gtk-4.0.so.37,libwebkitgtk-3.0.so.0}
ln -sf /usr/lib64/{libwebkit2gtk-4.0.so.37,libwebkitgtk-3.0.so.0.22.17}
```

После этого повторите запуск клиента.

Сбор логов сервера 1С

Для настройки сбора логов необходимо выполнить следующие действия:

1. Перейдите в пользователя **root**.

```
su -
```

2. Создайте папку для логов.

```
mkdir -p /var/log/log1c
```

3. Назначьте владельца.

```
chown usr1cv8:grp1cv8 /var/log/log1c
```

4. Создайте каталог **conf** в **/opt/1cv8/x86_64/current/**.

```
mkdir -p /opt/1cv8/x86_64/current/conf
```

5. Назначьте владельца каталогу **conf**.

```
chown usr1cv8:grp1cv8 /opt/1cv8/x86_64/current/conf
```

6. Создайте файл настроек технологического журнала 1С.

```
nano /opt/1cv8/x86_64/current/conf/logcfg.xml
```

Содержание файла:

```
<config xmlns="http://v8.1c.ru/v8/tech-log">
 <log location="/var/log/log1c" history="12">

 <event>
 <eq property="name" value="excp"/>
 </event>

 <event>
 <eq property="name" value="excpcntx"/>
 </event>

 <event>
 <eq property="name" value="admin"/>
 </event>

 <event>
 <eq property="name" value="clstr"/>
 </event>

 <event>
 <eq property="name" value="conn"/>
 </event>

 <event>
 <eq property="name" value="sesn"/>
 </event>

 <event>
 <eq property="name" value="proc"/>
 </event>
```

```
<event>
<eq property="name" value="DBPOSTGRS"/>
<ge property="Durationus" value="10000000"/>
</event>

<property name="all"/>
</log>
<plansql/>
</config>
```

7. Назначьте владельца файлу **logcfg.xml**.

```
chown usr1cv8:grp1cv8 /opt/1cv8/x86_64/current/conf/logcfg.xml
```

8. Подождите 1-2 минуты.

Данное условие связано с тем, что обнаружение файла настройки осуществляется опросом каталогов их возможного месторасположения в заданный промежуток времени.

9. Проверьте, что в **/var/log/log1c** начали появляться папки.

Если папки появляются – значит, все настроено верно.

Справочно-правовая система Консультант Плюс

Установка и настройка wine

Установите Wine.

```
dnf install wine winetricks
```

ВАЖНО!

Выполните следующую команду **от пользователя, для которого** устанавливается Консультант+ (**не из-под sudo или root**):

```
winetricks riched30 winhttp
```

Запустите конфигуратор wine, перейдя в меню по пути **Меню - Wine - Wine Configuration**.

ВАЖНО

Запускать конфигуратор Wine нужно **от того пользователя, под которым планируется работать в Консультант+**

Установите необходимые дополнительные библиотеки, которые попросит установить Wine.
На вкладке Графика уберите галочку в пункте "Разрешить менеджеру окон декорировать окна".

Настройка запуска Консультант+ на рабочей станции

Для запуска "Консультант Плюс" на рабочей станции подключите сетевой диск с "Консультантом", это можно сделать разными способами. Инструкции по подключению сетевых дисков вы можете прочитать по ссылке, используйте подходящий для вас вариант. Рекомендуется использовать **automount**.
Если клиентский ПК находится в домене, то для подключения сетевого каталога с К+ воспользуйтесь инструкцией по ссылке.

ВАЖНО!

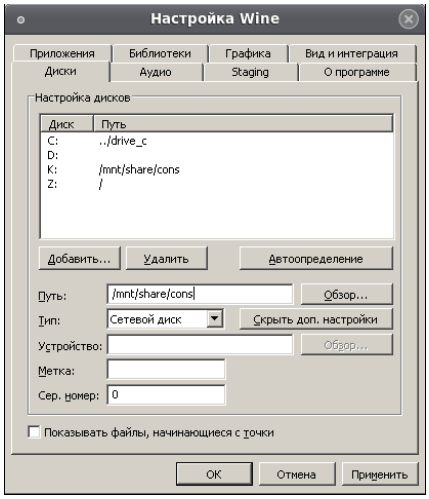
Дальнейшие команды выполняются **от того пользователя, под которым планируется работать в Консультант+** (**не от root**)

Проверьте, что команда whoami выдаёт имя вашего пользователя, а не *root*.

После того, как сетевой каталог с К+ был подключен, например в /mnt/share/cons/ , перейдем к настройке wine. Для Консультант Плюс в wine важно создать сетевой диск, для этого выполните команду в консоли от обычного пользователя:

```
winecfg
```

При этом откроется окно, в котором нужно создать сетевой диск, например K: и для него указать точку монтирования (каталог, в который был примонтирован Консультант+.), а тип диска обязательно выбрать "Сетевой диск".



Тогда, команда запуска Консультанта будет выглядеть следующим образом:

```
wine K:\cons.exe /linux /yes
```

Первый запуск Консультант+ производится долго, так как выполняется обновление конфигурации wine.

Далее должна запуститься процедура регистрации рабочей станции. Не закрывая окна обмена информацией с администратором, необходимо зарегистрировать рабочую станцию с машины администратора. Для регистрации рабочей станции с машины администратора, запустите Консультант+ с ключом /adm. Перейдите в меню на пункт ***Сервис > Регистрация новых пользователей***.

При успехе, на сервере и на клиенте будет увеличиваться прогресс регистрации в прогресс-баре.
В некоторых случаях могут возникать проблемы с регистрацией станций, т.е. при повторном запуске К+ снова просит зарегистрировать станцию. Это происходит из-за того, что у К+ есть ограничение по количеству различных прописываемых путей запуска К+ при регистрации станции. Их не может быть более пяти.
Т.е. если будет условно 50 станций, но у всех прописан одинаковый путь, то проблем с регистрацией быть не должно.

Создание ярлыка Консультант+

Если при установке Консультант+ автоматически не создался ярлык запуска, то создайте на рабочем столе файл с расширением .desktop и содержанием:

```
[Desktop Entry]
Name=ConsultantPlus
Exec=wine K:\cons.exe /linux /yes
Type=Application
StartupNotify=true
Comment=ConsultantPlus
Icon=/usr/share/icons/hicolor/cons.ico
StartupWMClass=cons.exe
```

В строке *"Exec=wine K:\cons.exe /linux /yes"* укажите свой каталог, в который был примонтирован Консультант+.
Переместите иконку cons.ico в /usr/share/icons/hicolor/ и укажите в параметрах ярлыка для значения **Icon** путь до него.

В случае замедленной работы можно добавить ключ /sprocess=0. При нормальной работе, не добавляйте этот ключ.
Ключ /yes необходим для подавления сообщения об ошибке [WNetGetUniversalName ...] : NO_NETWORK

Дополнительные ключи запуска КонсультантПлюс

Для регистрации

```
wine cons.exe /adm /reg
```

Для приема пополнения из RECEIVE

```
wine cons.exe /adm /receive /base*
```

Для приема пополнения через интернет

```
wine cons.exe /adm /receive_inet /base*
```

Для тестирования

```
wine cons.exe /adm /basetest /base*
```

Установка драйвера защиты "Консультант Плюс" для серверной части

Если **файл-серверная** часть "Консультант Плюс" будет располагаться на РЕД ОС, то для его работы нужно установить и запустить на РЕД ОС драйвер защиты conslin. Этот файл необходим для успешных регистрации и обновления баз. Для установки драйвера защиты "Консультант Плюс" требуется файл conslin с официального сайта Консультант+.
Поместите его в директорию /usr/local/bin. Переместить файл в этот каталог получится только с правами суперпользователя.

Перейдите в консоли в каталог с файлом conslin и выполните копирование:

```
# cp conslin /usr/local/bin
```

Владельцем conslin назначьте пользователя root и дайте права на выполнение:

```
# chown root:root /usr/local/bin/conslin
# chmod +x /usr/local/bin/conslin
```

Запустите conslin:

```
# /usr/local/bin/conslin
```

Результат успешного запуска conslin:

```
bind: Address already in use
```

Если conslin не запустился и выдал ошибку о том, что не нашел библиотек, установите дополнительно пакеты:

```
# dnf install glibc.i686 compat-libstdc++-33.x86_64 libstdc++.i686
```

Для автоматической загрузки драйвера защиты надо отредактировать файл rc.local

```
# nano /etc/rc.local
```

В конец файла добавить строку:

```
/usr/local/bin/conslin
```

Закрыть с сохранением файл и выполнить команду:

```
chmod a+x /etc/rc.local
```

Тест драйвера ККМ АТОЛ

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Драйвер ККТ - 10.9.3.1

ККМ АТОЛ — контрольно-кассовая техника ведущего российского производителя оборудования и разработчика ПО для решения задач, связанных с маркировкой товаров, **АТОЛ**.

В их линейке – более 20 онлайн-касс, соответствующих требованиям 54-ФЗ, принципиально новый класс контрольно-кассовой техники – «Ньюджеры», смарт-терминалы.

Облачный сервис компании «**АТОЛ Онлайн**» является первым и одним из самых крупных в РФ среди KaaS-решений («касса как сервис») по занимаемой доле рынка.

Также **АТОЛ** поставляет POS-оборудование и решения для автоматизации склада.

Для установки тестового приложения драйвера **ККТ АТОЛ** в Центре загрузок официального сайта компании необходимо открыть папку «**Контрольно-кассовая техника**» и скачать архив «**Драйвер ККТ 10.9.3.1**».

Распакуйте скачанный архив и перейдите в каталог с необходимыми для установки файлами:

```
unzip /home/user/Загрузки/10.9.3.1.zip
```

```
cd /home/user/Загрузки/10.9.3.1/installer/rpm
```

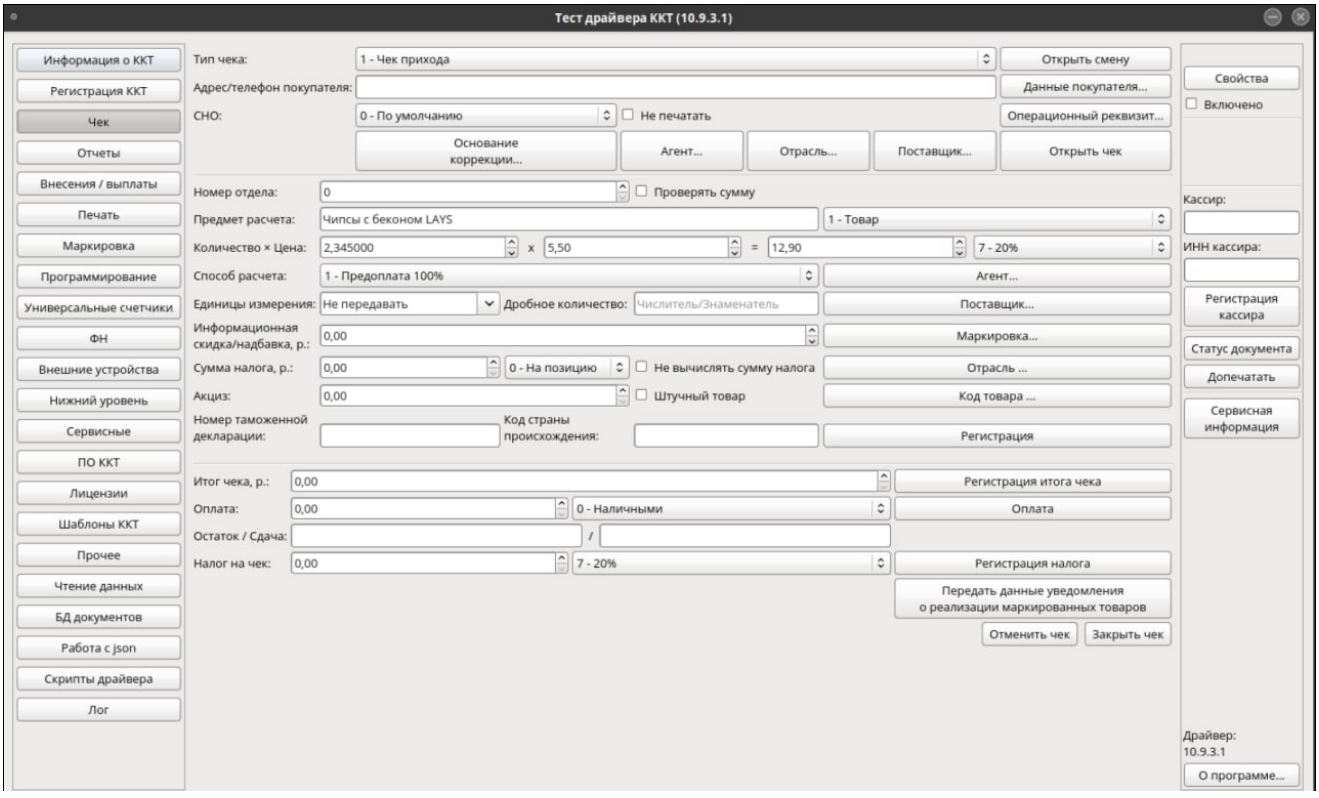
Для установки драйвера перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install libfptr10-gui-10.9.3.1-1.x86_64.rpm libfptr10-10.9.3.1-1.x86_64.rpm fptr10-test-util-10.9.3.1-1.x86_64.rpm
```

После установки программа будет доступна в «**Главном меню**» - «**Прочее**» - «**Тест драйвера ККТ v. 10**».



Установка ПО ГРАНД-Смета

Установка драйверов guardant
Предварительная подготовка
Установка ПО ГРАНД-Смета
Установка ПО ГРАНД-Смета через инсталлятор
Установка ПО ГРАНД-Смета через загрузчик

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: wine-9.0-1, autoconf-2.71-4, guardant-wine-0:0.5.8-1, smeta-2024.3.3

ГРАНД-Смета — программный комплекс для составления и проверки расчётов смет строительных работ, а также составления различных актов. Пользоваться программой может только обладатель уникального электронного ключа. Основными пользователями программного комплекса являются инженеры-сметчики. В составе ГРАНД-Сметы имеются различные базы, необходимые для работы инженера-сметчика.

Установка драйверов guardant

Guardant — семейство электронных ключей для защиты программного обеспечения от несанкционированного копирования и распространения. Разработаны российской компанией Актив.

В рамках данной статьи установка драйверов производится из репозитория РЕД ОС. Подробную информацию о драйверах **guardant** см. на официальной странице разработчика.

Предварительная подготовка

Установка пакетов

Для дальнейшей настройки необходимо установить дополнительные пакеты. Для этого перейдите в сеанс суперпользователя **root**:

```
su -
```

и выполните команду:

```
dnf install autoconf wine guardant-wine.i686
```

Выйдите из сеанса суперпользователя **root**:

```
exit
```

Дальнейшие действия выполняются с правами **локального пользователя**, если не указано иное.

Установка правил для udev

Скачайте архив с необходимыми правилами по ссылке.

После загрузки перейдите в каталог со скачанным архивом (в примере **/home/user/Загрузки**) и распакуйте его:

```
cd /home/user/Загрузки
tar -xvf udev-rules.tar.gz
```

Выполните установку правил (потребуются права **администратора системы**):

```
sudo ./install.sh
```

После успешной установки правил следует отсоединить электронный ключ от USB-порта и подсоединить его повторно.

Ключ готов к работе с защищенным приложением.

Настройка wine

В **wine** необходимо настроить 32-разрядную архитектуру:

```
export WINEARCH=win32
```

Убедитесь, что настройки применены:

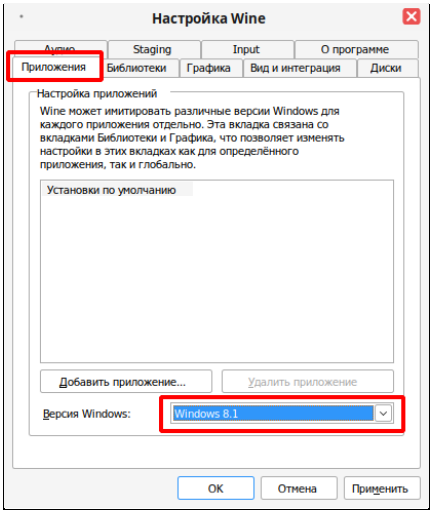
```
echo $WINEARCH

win32
```

Запустите конфигуратор **winecfg**:

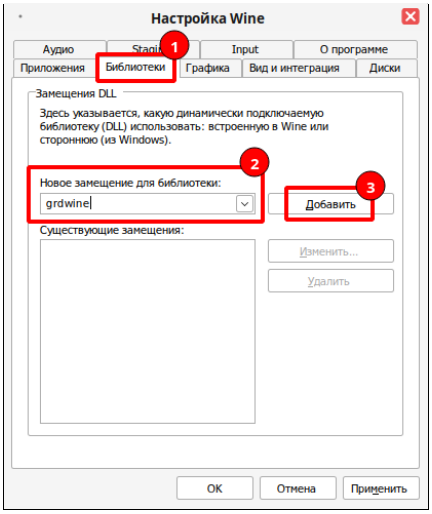
```
winecfg
```

> **Примечание.**
>
> Установка пакетов **mono** и **geco** не требуются для работы.

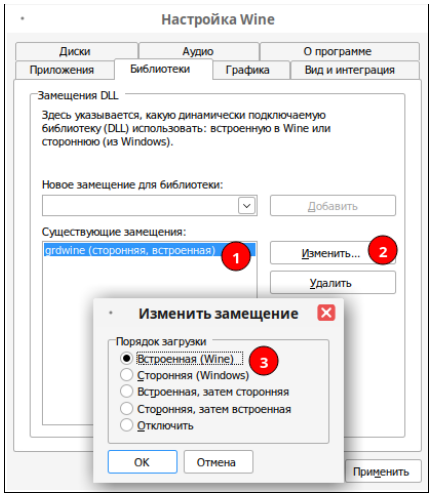
На вкладке **Приложения** выберите **Версию Windows** - *Windows 8.1*.



На вкладке **Библиотеки** введите **Новое замещение для библиотеки** - *grdwine*. Нажмите кнопку **Добавить**.



Затем выберите добавленную строку и нажмите **Изменить** для изменения порядка загрузки, установив значение - *Встроенная (Wine)*.



Нажмите **OK** для применения настроек.

Установка ПО ГРАНД-Смета

Подключите электронный ключ к компьютеру и запустите установку программы.

Установка ПО ГРАНД-Смета возможна двумя способами:

- через скачанный инсталлятор;
- через специальный загрузчик.

Установка ПО ГРАНД-Смета через инсталлятор

Перейдите на официальный сайт разработчика и запросите архив с необходимой версией **ПО ГРАНД-Смета** (в примере рассмотрена установка **ПО ГРАНД-Смета 2024.3.3**).

Перейдите в каталог со скачанным архивом (в примере **/home/user/Загрузки**) и распакуйте его:

```
cd /home/user/Загрузки
unzip smeta2024.3.3.zip -d ./smeta2024.3.3
```

Дополнительно для установки **ПО ГРАНД-Смета 2024.3** на РЕД ОС в **wine** необходимо использовать скрипт setup_run.sh.

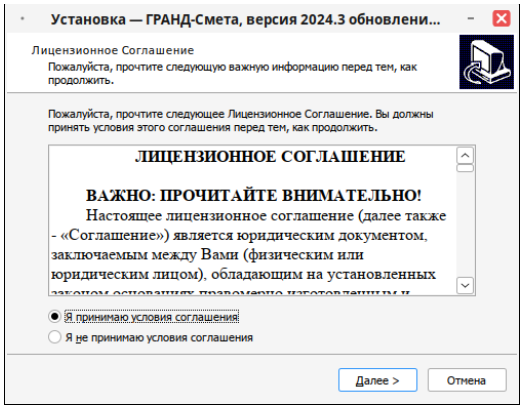
Скачайте скрипт **setup_run.sh** и поместите его в директорию с установочным файлом **Setup.exe** из распакованного архива, предоставьте скрипту права на исполнение:

```
mv setup_run.sh ./smeta2024.3.3
chmod +x ./smeta2024.3.3/setup_run.sh
```

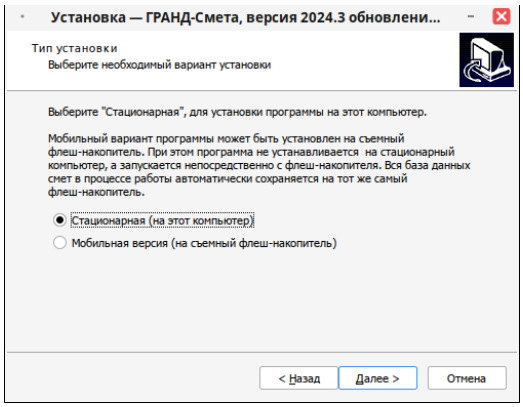
После этого запустите скрипт **setup_run.sh**:

```
./setup_run.sh Setup.exe
```

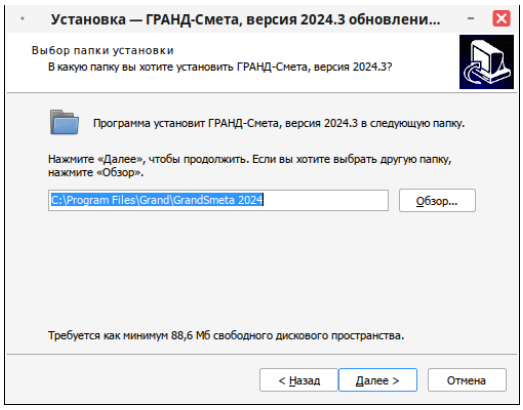
Для продолжения установки необходимо принять условия Лицензионного соглашения. Нажмите **Далее**.



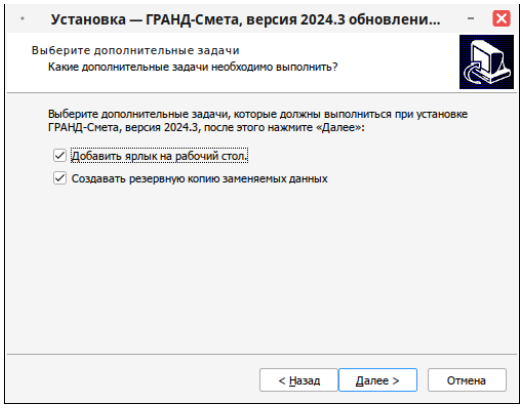
Выберите вариант установки — *Стационарная*. Нажмите **Далее**.



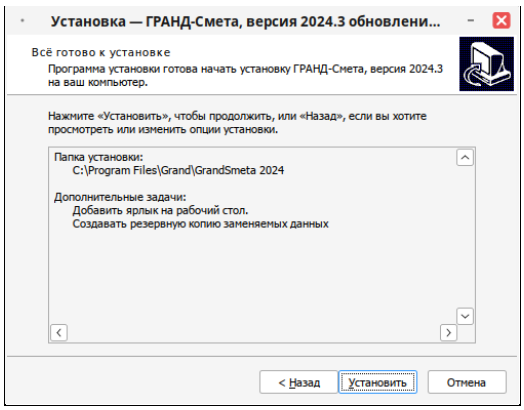
Выберите папку установки (можно оставить путь по умолчанию). Нажмите **Далее**.



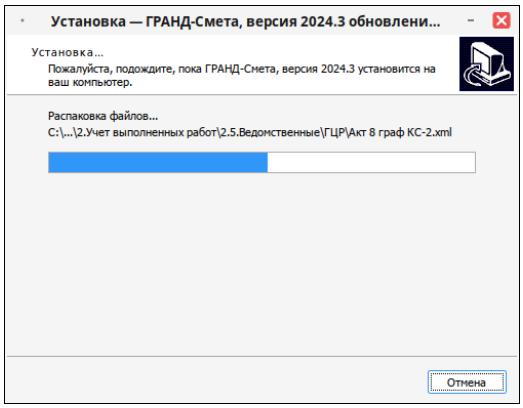
Установите дополнительные параметры. Нажмите **Далее**.



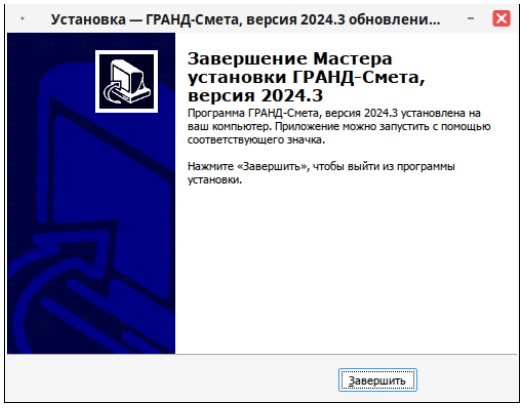
Проверьте правильность выбранных настроек и, если все верно, нажмите **Установить**.



Будет запущен процесс установки.



После окончания установки нажмите **Завершить** для выхода из программы установки.



Для завершения настройки выполните команду:

```
cp -rf /usr/lib/wine/i386-unix/grdwine.dll.so /home/user/.wine/drive_c/Program\ Files/Grand/GrandSmeta\ 2024/Client/grdwine.dll
```

На этом установка ПО ГРАНД-Смета завершена. На **Рабочем столе** появится ярлык для запуска программы.

Установка ПО ГРАНД-Смета через загрузчик

Перейдите на официальный сайт разработчика и скачайте **Утилиту загрузки программы ГРАНД-Смета**, нажав кнопку **Скачать и установить**.

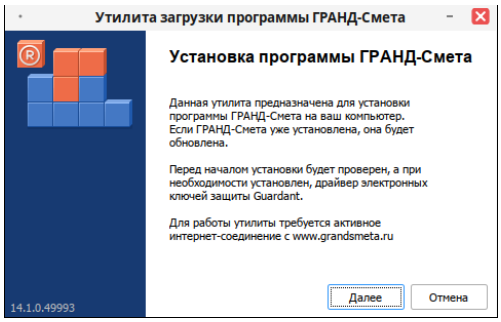
Перейдите в каталог со скачанным файлом (в примере **/home/user/Загрузки**):

```
cd /home/user/Загрузки
```

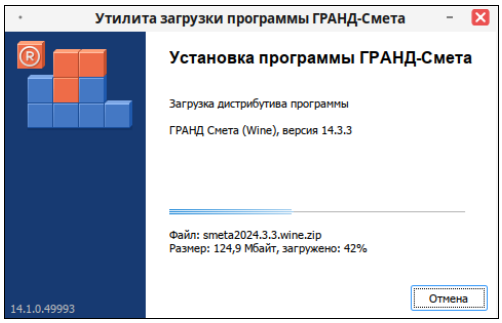
Для запуска установки выполните:

```
wine GrandSmetaDownloader.exe
```

Будет открыт загрузчик **ПО ГРАНД-Смета**. На приветственной странице нажмите **Далее**.

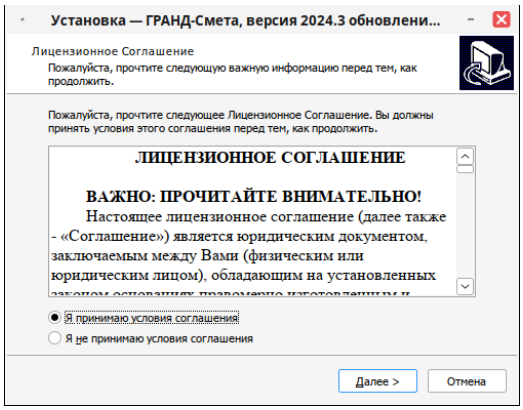


Будет произведена проверка драйверов электронных ключей. Если драйверы отсутствуют, они будут автоматически установлены. Также будет осуществлена проверка подключенного ключа защиты.

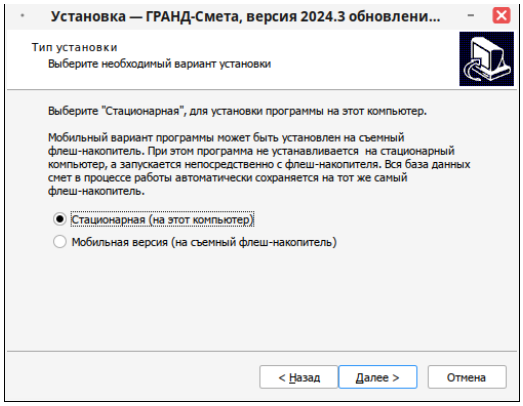


Затем будет загружен и распакован дистрибутив программы ГРАНД-Смета.

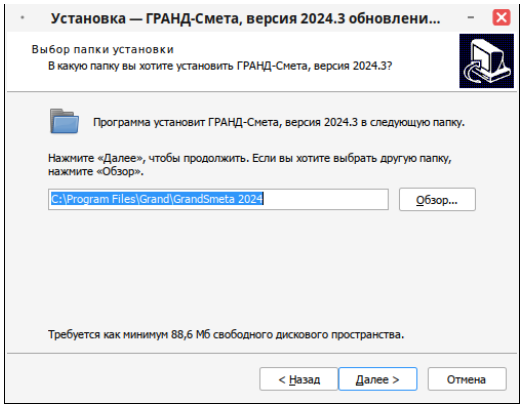
После распаковки дистрибутива будет открыто окно установщика, где необходимо принять условия Лицензионного соглашения.



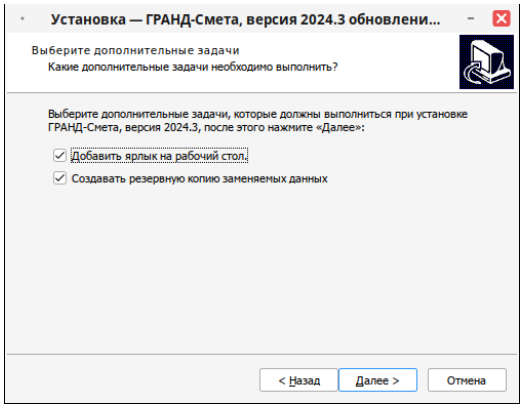
Выберите вариант установки — *Стационарная*. Нажмите **Далее**.



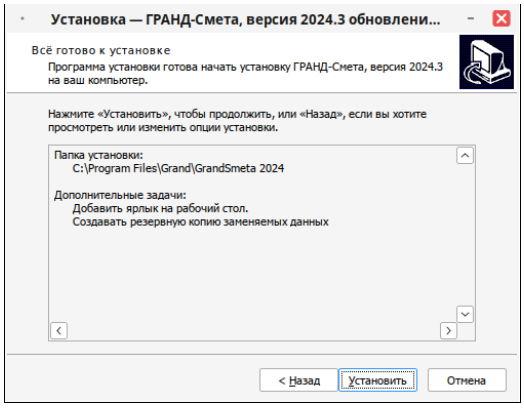
Выберите папку установки (можно оставить путь по умолчанию). Нажмите **Далее**.



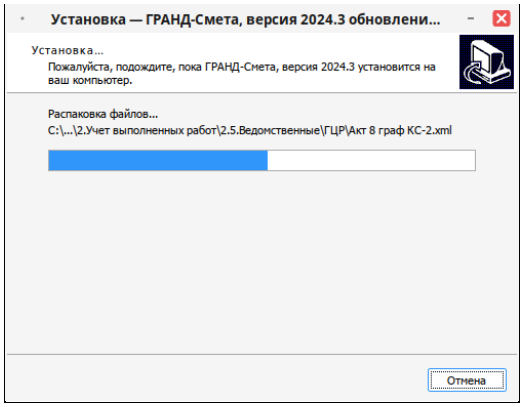
Установите дополнительные параметры. Нажмите **Далее**.



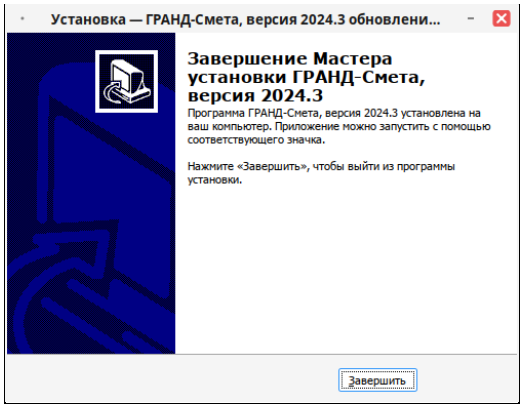
Проверьте правильность выбранных настроек и, если все верно, нажмите **Установить**.



Будет запущен процесс установки.



После окончания установки нажмите **Завершить** для выхода из программы установки.

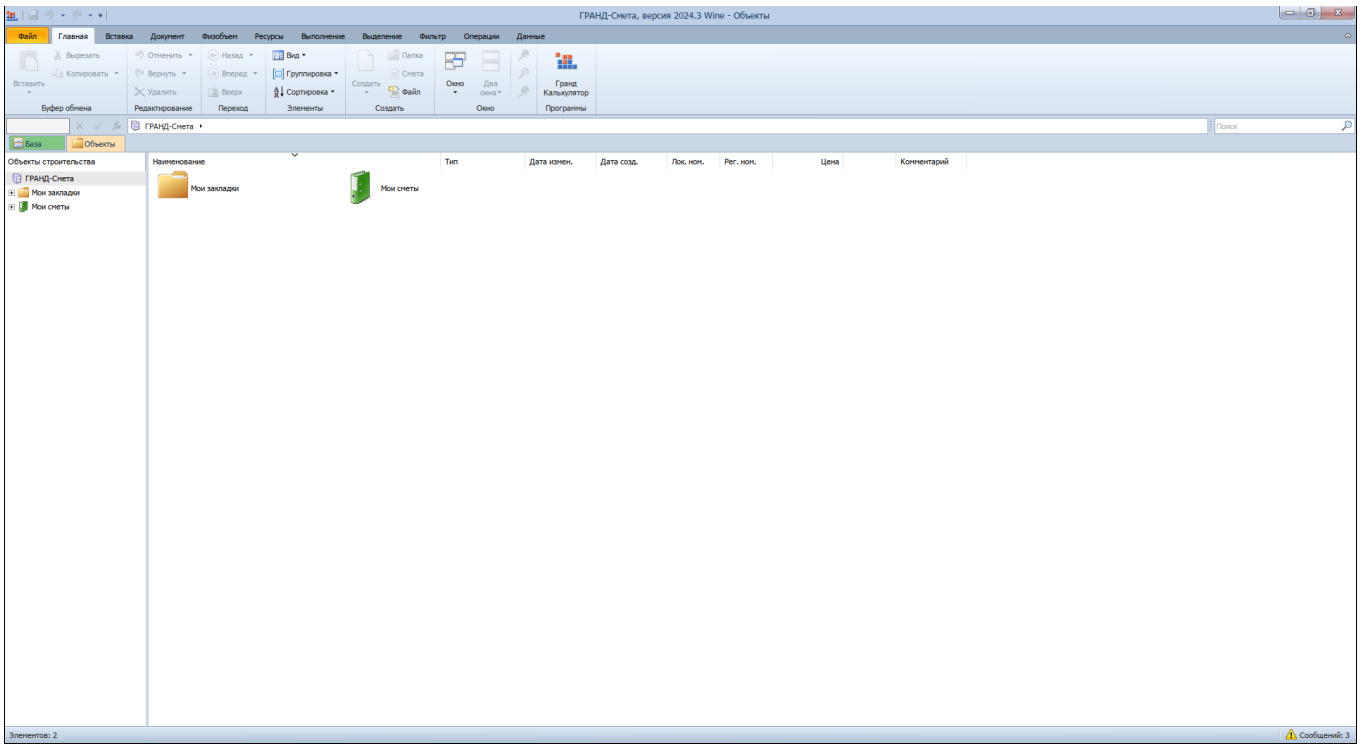


Для завершения настройки выполните команду:

```
cp -rf /usr/lib/wine/i386-unix/grdwine.dll.so /home/user/.wine/drive_c/Program\ Files/Grand/GrandSmeta\ 2024/Client/grdwine.dll
```

На **Рабочем столе** появится ярлык для запуска программы.

Окно программы выглядит следующим образом:


ГРАНД-Смета, версия 2024.3 Wine - Объекты
Файл
Главная
Вставка
Документ
Физобъем
Ресурсы
Выполнение
Выделение
Фильтр
Операции
Данные
Вставить
Вырезать
Копировать
Буфер обмена
Отменить
Вернуть
Удалить
Редактирование
Назад
Вперед
Вверх
Переход
Вид
Группировка
Сортировка
Элементы
Создать
Папка
Смета
Файл
Создать
Окно
Два окна
Окно
Гранд Калькулятор
Программы
ГРАНД-Смета
Поиск
База
Объекты
Объекты строительства
ГРАНД-Смета
Мои закладки
Мои сметы
Наименование
Тип
Дата измен.
Дата созд.
Лок. ном.
Рег. ном.
Цена
Комментарий
Мои закладки
Мои сметы
Элементов: 2
Сообщений: 3

Conky - программа для системного мониторинга

Графический менеджер conky

Conky - это системный монитор, который позволяет выводить на экран информацию о вашем процессоре, памяти, жестком диске, сетевом подключении, запущенных процессах и многом другом, что происходит в системе. Основная особенность *Conky* заключается в том, что данные выводятся на рабочий стол в виде виджета.

Вы можете подробнее ознакомиться с настройкой и работой утилиты **conky**, просмотрев наши обучающие видео:

- на **RuTube** — Conky - мощный и настраиваемый системный монитор;
- в **Яндекс.Дзен** — Conky - мощный и настраиваемый системный монитор;
- в **VK Видео** — Conky - мощный и настраиваемый системный монитор.

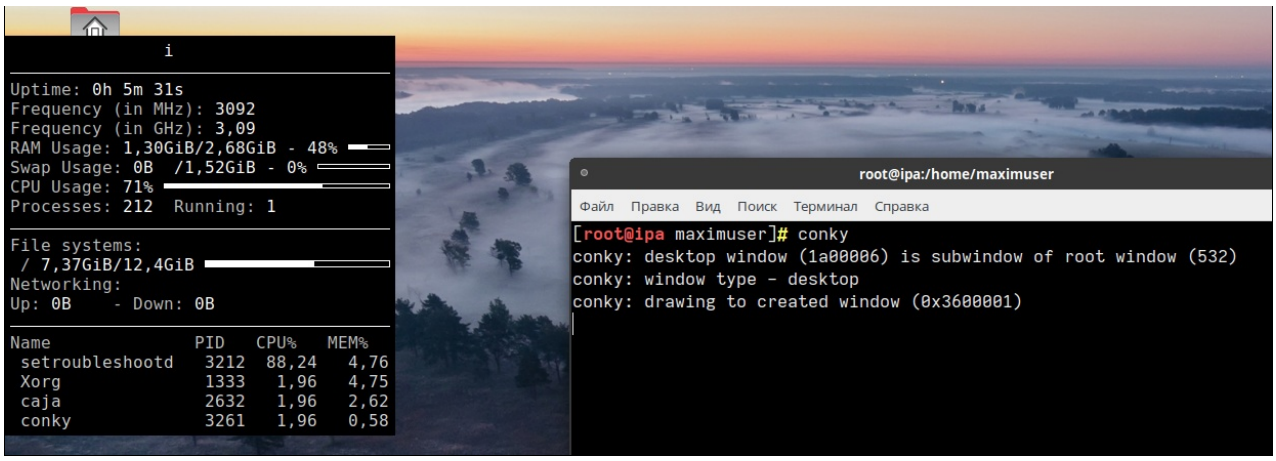
На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты необходимо выполнить команду:

```
dnf install conky
```

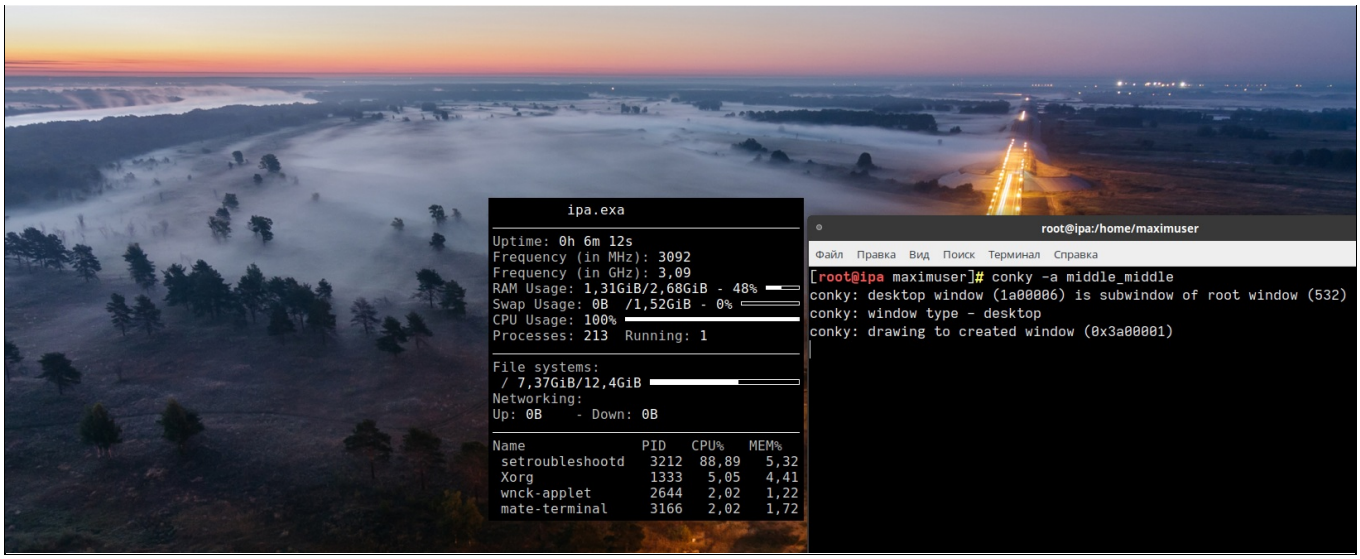
После установки запустим *conky* и увидим виджет с основной информацией о системе:

```
conky
```



Для того чтобы изменить положение виджета, необходимо использовать опцию **-a** и параметры **left, right, top, bottom, middle**, нужно указать положение по вертикали и по горизонтали. Например, установим виджет посередине:

```
conky -a middle_middle
```



При обновлении виджет мерцает, чтобы этого избежать, можно использовать двойную буферизацию. Для этого добавьте опцию **-b**:

```
conky -b -a middle_middle
```

Теперь перейдём к конфигурации виджета, для этого используется опция **-c**, она позволяет задать конфигурационный файл, из которого надо загружать тему. Так как мы будем изменять конфигурационный файл темы, чтобы не повредить стандартную тему, скопируйте его в домашнюю папку:

```
cp /etc/conky/conky.conf /etc/conky/conky.default
```

Перейдём в редактирование конфигурационного файла:

```
nano /etc/conky/conky.conf
```

По умолчанию любой конфигурационный файл *conky* делится на две секции - секция настроек и секция данных для вывода. Для начала изменим основные параметры секции настроек. Параметр **alignment = bottom_right** отвечает за расположение виджета, в данном случае - справа внизу. Параметр **gap_x = 50** используется для указания отступа от края по горизонтали, также можно указать отступ по вертикали - **gap_y**.

Сейчас окно чёрное, чтобы сделать его прозрачным, добавьте строку:

```
own_window_argb_visual = true
```

Затем можно настроить цвет и нужный уровень прозрачности с помощью следующих строк:

```
own_window_colour = '171717'
own_window_argb_value = 150
```

Цвет может быть практически любым. Значение прозрачности может быть от 0 до 255, где 0 - это полностью прозрачный и 255 - непрозрачный.

С помощью параметра **font** можно настраивать шрифт и его размер. Например, используем шрифт *Noto Mono, 13*:

```
font = 'Noto Mono:size=13'
```

За интервал обновления данных отвечает параметр **update_interval**, в данном случае - одна секунда, можно сделать полсекунды:

```
update_interval = 0.5
```

Если вы запустили программу без опции **-b**, то увидите, что при обновлении виджет немного мерцает. Чтобы этого избежать, включите двойную буферизацию, добавив строчку:

```
double_buffer = true
```

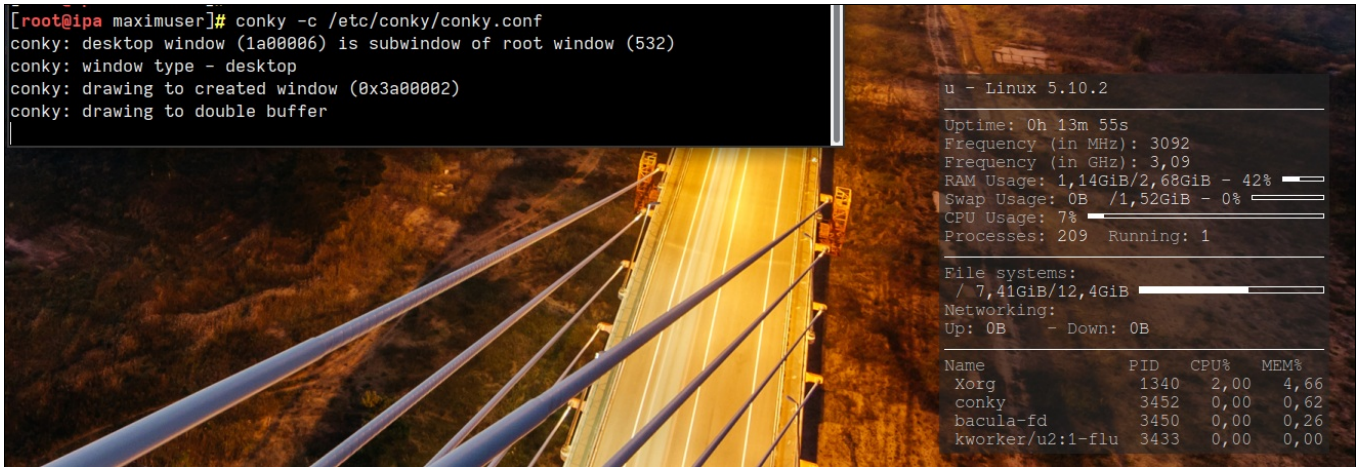
В секции настроек можно задать цвета, которые вы будете использовать потом в секции вывода. Это делать не обязательно, так как там можно сразу же указывать цвета, но это довольно удобно. Для установки цвета просто добавьте переменные *color1, color2, color3* и т.д.:

```
color1 = '#ff0000'
color2 = '#00ff00'
color3 = '#00ff00'
```

Теперь после изменения секции настроек она выглядит следующим образом:

```
conky.config = {
    alignment = 'bottom_right',
    background = false,
    border_width = 1,
    cpu_avg_samples = 2,
    default_color = 'white',
    default_outline_color = 'white',
    default_shade_color = 'white',
    draw_borders = false,
    draw_graph_borders = true,
    draw_outline = false,
    draw_shades = false,
    use_xft = true,
    font = 'Noto Mono:size=13',
    gap_x = 50,
    gap_y = 60,
    minimum_height = 5,
        minimum_width = 5,
    net_avg_samples = 2,
    no_buffers = true,
    out_to_console = false,
    out_to_stderr = false,
    extra_newline = false,
    own_window = true,
    own_window_class = 'Conky',
    own_window_type = 'desktop',
    own_window_argb_visual = true,
    own_window_colour = '171717',
    own_window_argb_value = 150,
    color1 = '#ff0000',
    color2 = '#00ff00',
    color3 = '#00ff00',
    stippled_borders = 0,
    update_interval = 0.5,
    double_buffer = true,
```

Сам виджет теперь выглядит так:



Перейдём к текстовой секции. В текстовой секции записывается текст, который будет выводиться в виджете. Синтаксис здесь следующий:

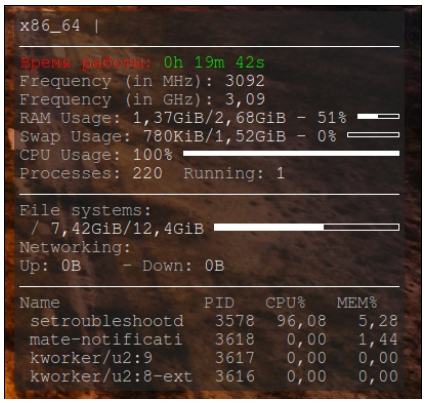
```
${<переменная> <параметр>}<текст>${<переменная> <параметр>}<текст>$<переменная>
```

Если для переменной нужны параметры, она пишется в скобках, если параметры не нужны, можно писать без скобок. Например:

```
${color1}Время работы:$color ${color2}$uptime$color
```

```
conky.text = [[
${scroll 16 $nodename - $sysname $kernel on $machine | }
$hr
${color1}Время работы:$color ${color2}$uptime$color
```

Теперь виджет выглядит следующим образом:



Все операции с выводом текста выполняются с помощью переменных. Основные переменные, которые вы можете использовать, можно посмотреть с помощью команды:

```
man conky
```

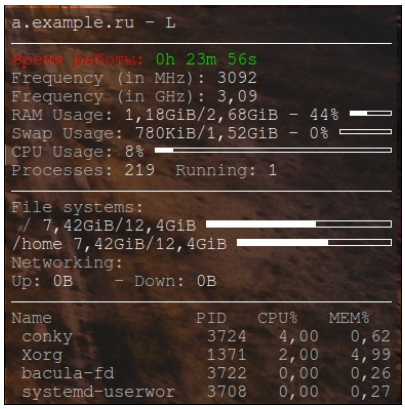
Примеры использования переменных

Для примера выведем свободное место в вашей домашней папке на виджет:

```
/home $color${fs_used /home}/${fs_size /home} ${fs_bar /home}
```

```
${color grey}File systems:
 / $color${fs_used /}/${fs_size /} ${fs_bar 6 /}
/home $color${fs_used /home}/${fs_size /home} ${fs_bar /home}
```

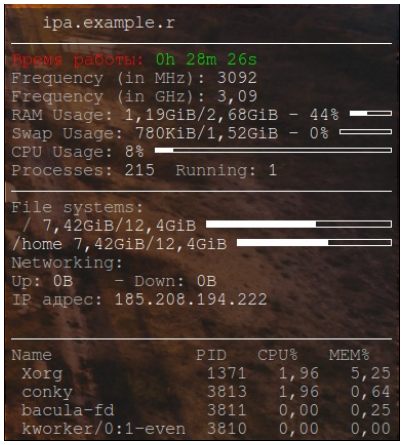
Теперь в разделе **File systems** выводится свободное место в домашней папке:



Аналогично можно сделать для необходимых каталогов. Чтобы показать ваш текущий IP-адрес, можно указать следующую строку:

```
${color grey}IP адрес: $alignr ${eval $${addrs ${gw_iface}}}
```

Теперь в разделе **Networking** выводится текущий IP-адрес:

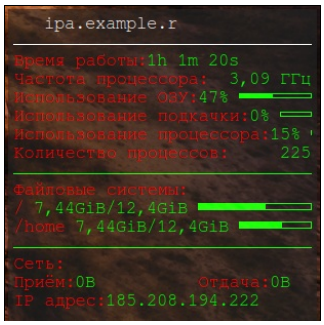


Зададим вывод данных на русском языке и изменим цвет выводимого текста:

```
${color1}Время работы:$color2${alignr}$uptime
${color1}Частота процессора:$color2${alignr}$freq_g ГГц
${color1}Использование ОЗУ:$color2$memperc% ${membar 4}
${color1}Использование подкачки:$color2$swapperc% ${swapbar 4}
${color1}Использование процессора:$color2$cpu% ${cpubar 4}
${color1}Количество процессов:$color2${alignr}$processes
${color1}Файловые системы:
${color1}/ $color2${fs_used /}/${fs_size /} ${fs_bar 6 /}
${color1}/home $color2${fs_used /home}/${fs_size /home} ${fs_bar /home}
${color1}Сеть:
${color1}Приём:$color2${upspeed enp24s0} ${color2} ${alignr} Отдача:$color2${downspeed enp24s0}
${color1}IP адрес:$color2${curl eth0.me}
```

```
conky.text = [[
${scroll 16 $nodename - $sysname $kernel on $machine | }
$hr
${color1}Время работы:$color${color2}$uptime$color
${color1}Частота процессора:$color2${alignr}$freq_g ГГц
${color1}Использование ОЗУ:$color2$memperc% ${membar 4}
${color1}Использование подкачки:$color2$swapperc% ${swapbar 4}
${color1}Использование процессора:$color2$cpu% ${cpubar 4}
${color1}Количество процессов:$color2${alignr}$processes
$hr
${color1}Файловые системы:
${color1}/ $color2${fs_used /}/${fs_size /} ${fs_bar 6 /}
${color1}/home $color2${fs_used /home}/${fs_size /home} ${fs_bar /home}
$hr
${color1}Сеть:
${color1}Приём:$color2${upspeed enp24s0} ${color1} ${alignr} Отдача:$color2${downspeed enp24s0}
${color1}IP адрес:$color2${curl eth0.me}
]]
```

Теперь виджет выглядит следующим образом:



Настройка *conky* завершена, у данного виджета присутствует множество вариаций оформления и выводимых данных, всё зависит от задаваемых параметров.

Графический менеджер conky

Утилита **conky** также имеет графический менеджер.

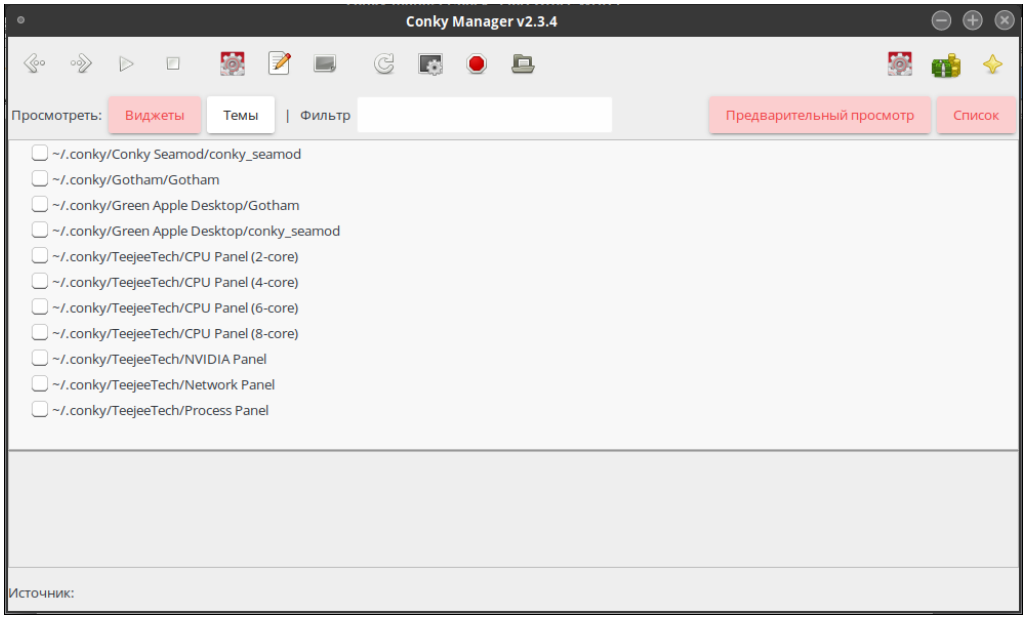
Для установки необходимо перейти в сеанс пользователя **root**:

```
su -
```

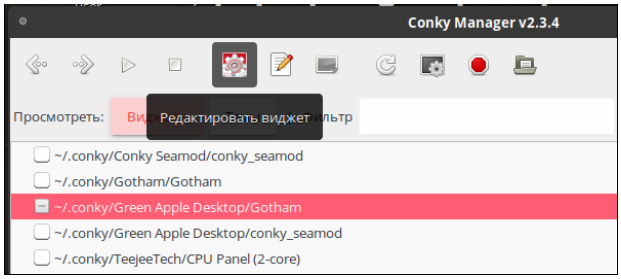
и выполнить команду:

```
dnf install conky-manager
```

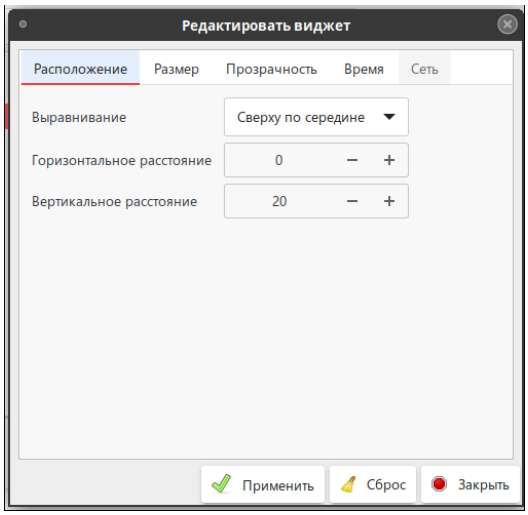
Запуск утилиты доступен из «**Главного меню**» – «**Стандартные**» – «**Conky Manager**».



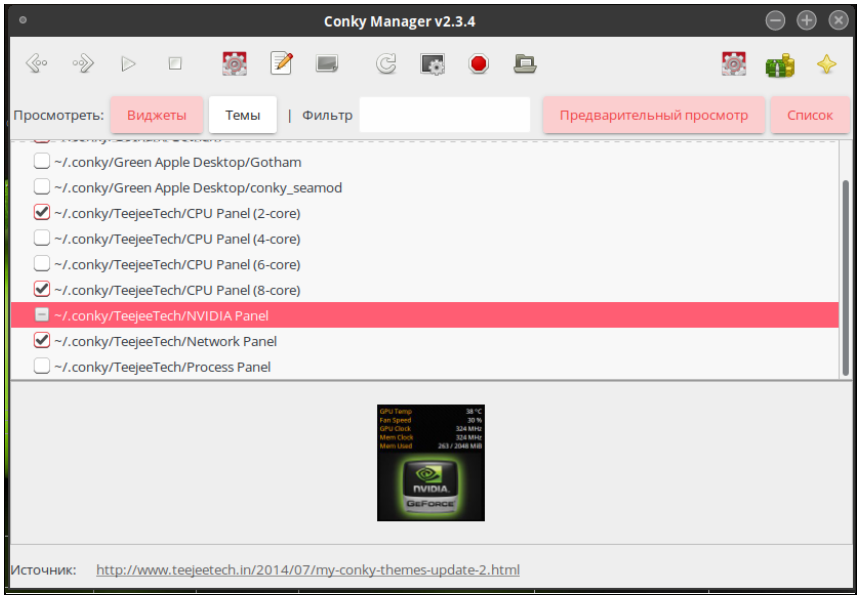
Утилита позволяет добавлять различные виджеты мониторинга системы, осуществлять предпросмотр этих виджетов на рабочем столе, а также редактировать их.



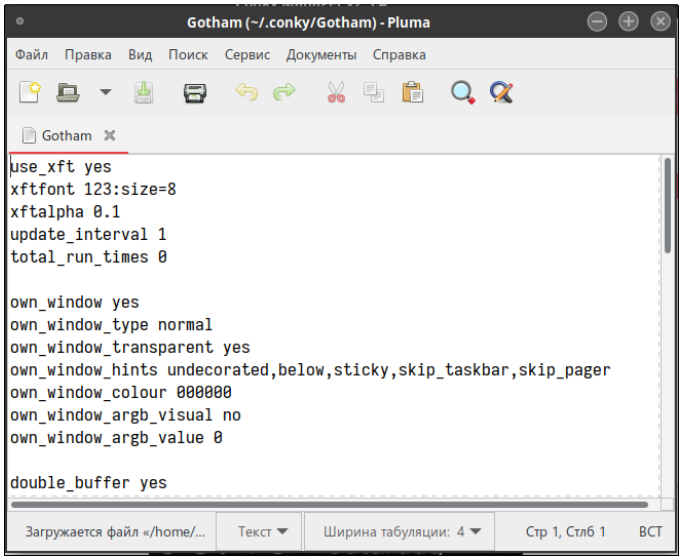
Можно отредактировать расположение виджета, его размер, цвет фона и прозрачность, формат отображаемого времени и сетевой интерфейс (если доступно).



В **conky-manager** существует возможность запуска нескольких виджетов одновременно.



А также можно запускать свои созданные конфигурации для виджетов или изменять существующие. Для изменения уже существующих конфигураций редактируются две секции – секция настроек и секция данных для вывода.



В графическом менеджере также можно создавать и сохранять новые или редактировать уже имеющиеся темы для рабочего стола.



Glances - инструмент для мониторинга системы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** glances-3.1.4.1-1

Glances — это кросплатформенный инструмент для мониторинга системы на основе командной строки, написанный на языке **Python**, использующий библиотеку **psutil** для получения информации о системе. Так вы можете отслеживать использование процессора, средней нагрузки, памяти, сетевых интерфейсов, дискового ввода/вывода, процессов и файловой системы.

Информация о системе которая может выводится **Glances**:

- Информация о процессоре (пользовательские приложения, системные программы и незанятые программы).
- Общая информация о памяти, включая RAM, Swap, Free memory и т. д.
- Средняя загрузка процессора за последние 1, 5 и 15 минут.
- Скорость загрузки/выгрузки по сети.
- Общее количество процессов, активных и спящих процессов и т. д.
- Информация о скорости дискового ввода/вывода (чтение или запись).
- Подключенные устройства, использующие диск в настоящее время.
- top-процессы с использованием ЦП/памяти, именами и местоположением приложения.
- Текущие дата и время.
- Подсветка процесса, который потребляет максимальные системные ресурсы, красным цветом.

Атрибуты Glances

Поле указания атрибутов открывается клавишей «**Enter**» во время работы программы. Все доступные атрибуты можно посмотреть, нажав «**h**»:

- **a** – сортировать процессы автоматически;
- **c** – сортировать процессы по **CPU%**;
- **m** – сортировать процессы по **MEM%**;
- **p** – сортировать процессы по имени;
- **i** – сортировать процессы по скорости ввода/вывода;
- **d** – показать/скрыть статистику дискового ввода-вывода;
- **f** – показать/скрыть статистику директорий и файлов;
- **n** – показать/скрыть сетевую статистику;
- **s** – показать/скрыть статистику датчиков;
- **y** – показать/скрыть статистику **hddtemp**;
- **l** – показать/скрыть логи;
- **b** – байты или биты для сетевых входов/выходов;
- **w** – удалить журналы предупреждений;
- **x** – удалить предупреждения и критические журналы;
- **1** – общая статистика ЦП;
- **h** – показать/скрыть этот экран справки;
- **t** – просмотреть сетевой ввод/вывод как комбинации;
- **u** – просмотреть совокупный сетевой ввод/вывод;
- **q** – выйти (**Esc** и **Ctrl+C** тоже работают).

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

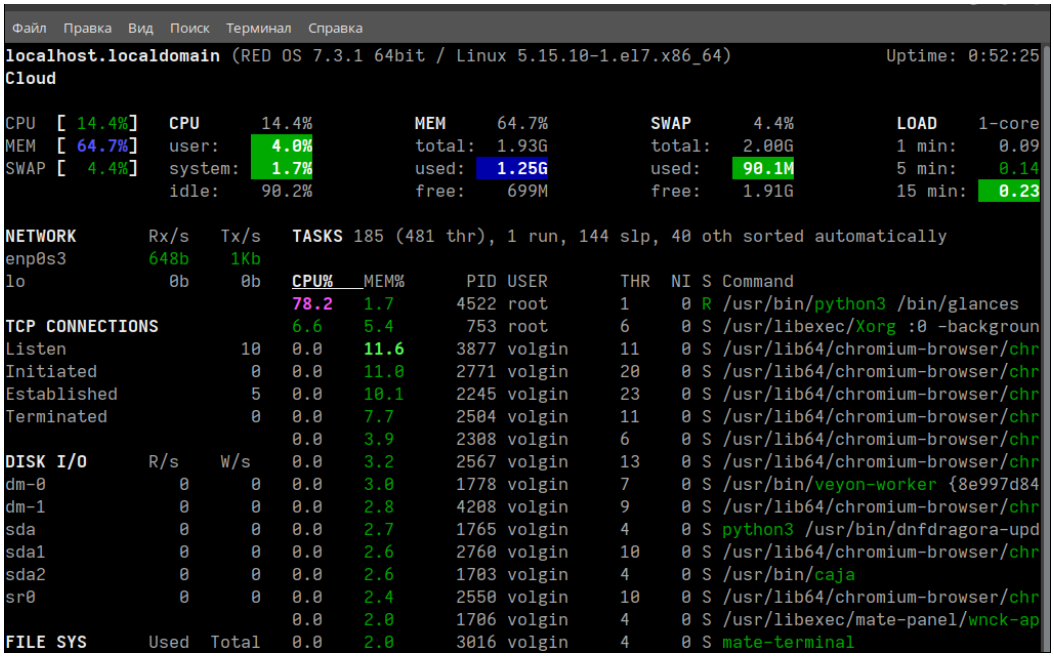
и выполните команду:

```
dnf install glances
```

Для запуска утилиты введите её название в терминале:

```
glances
```

Отображаемая по умолчанию информация:



iostat - утилита анализа загруженности системы

Установка
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** sysstat-12.3.1-1

Утилита **iostat** позволяет проанализировать загруженность системы. Она отображает основные параметры ввода/вывода данных на диск, скорость записи и чтения данных, а также объем записанных или прочитанных данных. Кроме того утилита выводит параметры загруженности процессора. Её можно использовать для оптимизации работы системы.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install sysstat
```

Основные опции утилиты:

- **-c** — отобразить только информацию об использовании процессора;
- **-d** — отобразить только информацию об использовании устройств;
- **-h** — выводить данные отчёта в удобном для чтения формате;
- **-k** — выводить статистику в килобайтах;
- **-m** — выводить статистику в мегабайтах;
- **-o JSON** — выводить статистику в формате JSON;
- **-p** — вывести статистику по устройству и всем его разделам;
- **-x** — вывести расширенную статистику;
- **-y** — отображать статистику с момента запуска утилиты, а не системы;
- **-z** — спрятать информацию о дисках, у которых нет активности.

Пример работы

Самый простой пример использования утилиты - это запуск без параметров:

```
iostat
```

```
Linux 5.15.10-1.el7.x86_64 (localhost.localdomain)      11.07.2022      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          1,15    0,01    0,91    0,25    0,03   97,65

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
dm-0             12,93       319,53        22,87         0,00    1156449      82756          0
dm-1              0,40         0,66         1,48         0,00       2384       5340          0
sda               7,31       322,56        24,38         0,00    1167410      88228          0
scd0              0,01         0,30         0,00         0,00       1072          0          0
```

В первой части отчёта находится информация о загруженности процессора. Здесь приведены следующие данные:

- **%user** — процент использования процессора программами, запущенными на уровне пользователя;
- **%nice** — процент использования процессора программами, запущенными в пространстве пользователя, но с изменённым приоритетом;
- **%system** — процент использования процессора ядром;
- **%iowait** — процент времени, затраченного на ожидание завершения операций ввода/вывода;

- **%steal** — процент простоя виртуального процессора во время передачи гипервизором мощности другому виртуальному процессору;
- **%idle** — процент времени простоя процессора (процессор не занят).

Для устройств ввода/вывода также отображается ряд данных со следующей информацией:

- **tps** — количество запросов на чтение или запись к устройству в секунду;
- **KB_read/s, MB_read/s** — количество килобайт или мегабайт, прочитанных с устройства за секунду;
- **KB_wrtn/s, MB_wrtn/s** — количество килобайт или мегабайт, записанных на устройство в секунду;
- **KB_dscd/s, MB_dscd/s** — скорость освобождения блоков данных на устройстве, килобайт или мегабайт в секунду;
- **KB_read, MB_read** — общее количество прочитанных данных с диска с момента загрузки системы;
- **KB_wrtn, MB_wrtn** — количество записанных данных с момента загрузки системы;
- **KB_dscd, MB_dscd** — количество освобождённых блоков на диске в результате выполнения операции **trim** в килобайтах или мегабайтах.

Для просмотра в более удобном формате выполните:

```
iostat -h
```

```
Linux 5.15.10-1.el7.x86_64 (localhost.localdomain)      11.07.2022      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0,6%    0,0%    0,6%    0,1%    0,0%   98,7%

     tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd Device
    5,82       135,9k        12,2k         0,0k       1,1G     102,0M       0,0k dm-0
    0,19         0,3k         0,7k         0,0k       2,8M       5,6M       0,0k dm-1
    3,36       137,2k        12,8k         0,0k       1,1G     107,7M       0,0k sda
    0,01         0,1k         0,0k         0,0k       1,0M       0,0k       0,0k scd0
```

Для отображения всей статистики выполните:

```
iostat -x
```

```
Linux 5.15.10-1.el7.x86_64 (localhost.localdomain)      11.07.2022      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0,56    0,01    0,55    0,13    0,03   98,72

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_awa
it wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz     f/s f_await  aqu-sz  %util
dm-0             4,21    135,48     0,00   0,00    2,04    32,18    1,60     12,13     0,00   0,00   16,
13     7,60    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,03   0,29
dm-1             0,03      0,33     0,00   0,00    4,67    12,87    0,16      0,66     0,00   0,00   25,
59     4,00    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,00   0,02
sda              2,31    136,72     2,01  46,45    1,55    59,14    1,04     12,81     0,72  40,98   16,
60    12,28    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,02   0,30
scd0             0,01      0,12     0,00   0,00    1,17    20,24    0,00      0,00     0,00   0,00    0,
00     0,00    0,00      0,00     0,00   0,00    0,00     0,00    0,00     0,00    0,00   0,00
```

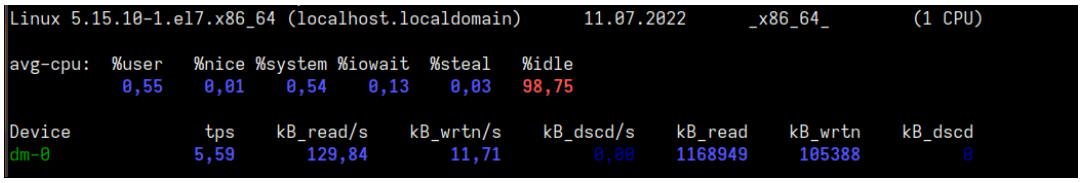
Описание вывода:

- **r/s** — количество запросов на чтение в секунду;
- **rKB/s** — скорость чтения с диска (КБ/сек);
- **rrqm/s** — обобщенное количество запросов на чтение в секунду;
- **%rrqm** — количество объединенных запросов чтения;
- **r_await** — среднее время (миллисекунды) на обработку запросов чтения к диску (включает в себя время, потраченное в очереди на обработку, и время на обработку запроса);
- **rareq-sz** — средний размер запроса для чтения;
- **w/s** — количество запросов на запись в секунду;
- **wKB/s** — скорость записи на диск (КБ/сек);
- **wrqm/s** — обобщенное количество запросов на запись в секунду;
- **%wrqm** — количество объединенных запросов записи;
- **w_await** — среднее время (миллисекунды) на обработку запросов записи к диску (включает в себя время, потраченное в очереди на обработку, и время на обработку запроса);

- **wareq-sz** — средний размер запроса для записи;
- **aqu-sz** — средняя длина очереди
- **%util** — % CPU, затраченный на передачу I/O запросов к диску («пропускная способность» диска).

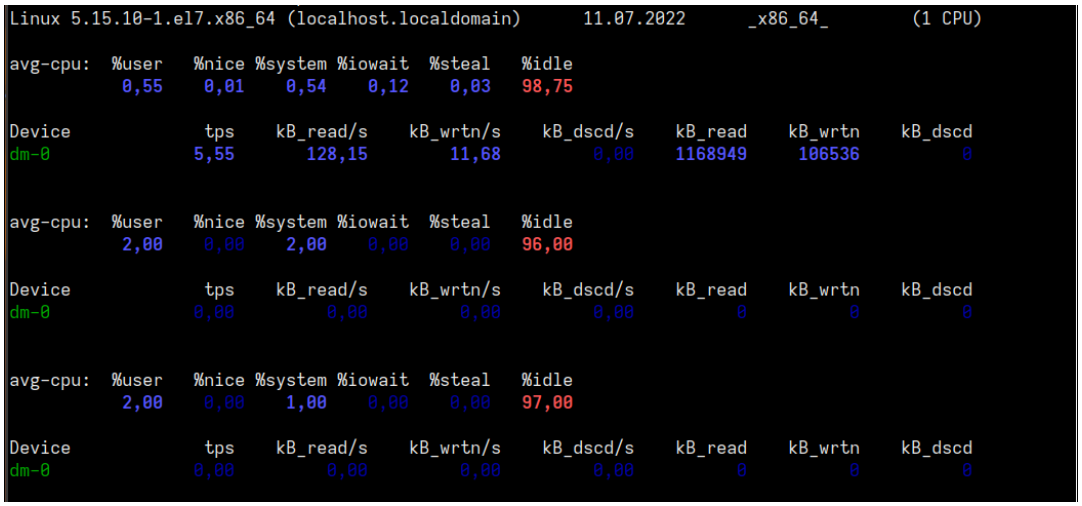
Можно просмотреть статистику по каждому разделу устройства, воспользовавшись опцией **-p**:

```
iostat -p /dev/dm-0
```



Чтобы утилита автоматически обновляла данные каждую секунду, необходимо добавить интервал (определяется в секундах):

```
iostat -p /dev/dm-0 1
```



iotop - утилита мониторинга использования диска

Установка
Основные опции программы
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** iotop 0.6-15

Утилита **iotop** позволяет просмотреть сведения об общем и текущем количестве операций обращения к диску.

Вы можете подробнее ознакомиться с интерактивными утилитами динамического мониторинга процессов, просмотрев наши обучающие видео:

- на **RuTube** — Интерактивные утилиты динамического мониторинга процессов;
- в **Яндекс.Дзен** — Интерактивные утилиты динамического мониторинга процессов;
- в **VK Видео** — Интерактивные утилиты динамического мониторинга процессов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки утилиты перейдите в сеанс пользователя **root**:

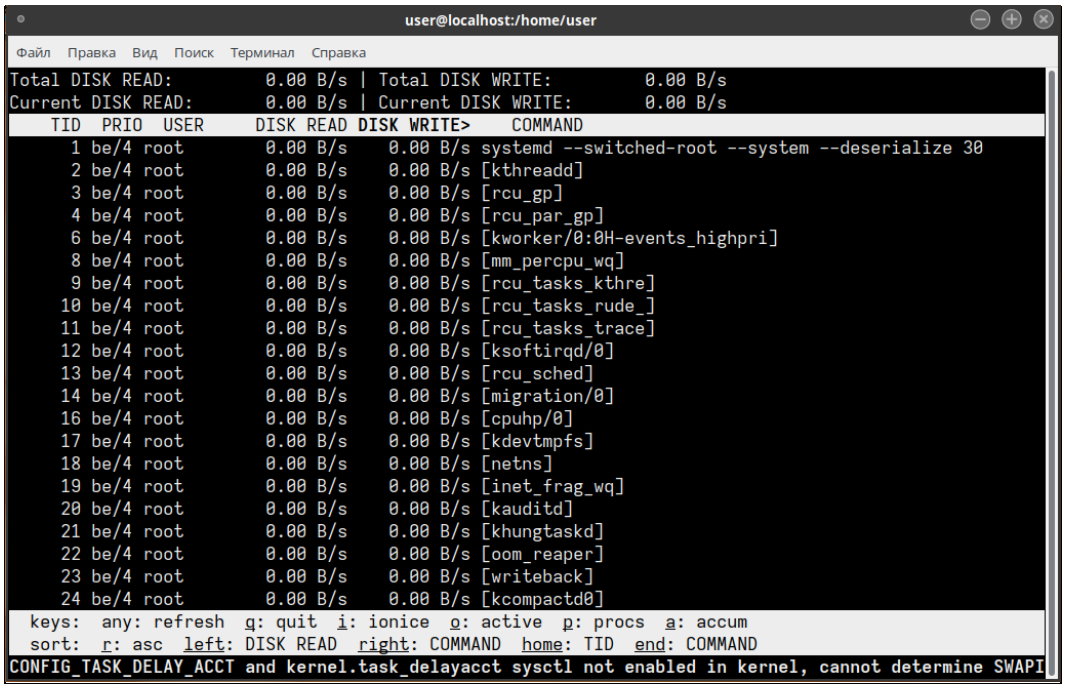
```
su -
```

и выполните команду:

```
dnf install iotop
```

Запустите утилиту через терминал, выполнив:

```
iotop
```



Основные опции программы

Опции для работы в программе описаны в таблице ниже.

Опции	Описание
--version	показать номер версии программы и выйти
-h, --help	показать данное справочное сообщение и выйти
-o, --only	отображать только процессы, которые в данный момент выполняют операции I/O с диском (по умолчанию — отображаются все активные процессы)
-b, --batch	неинтерактивный режим
-n <число>, --iter=<число>	количество итераций до окончания [бесконечно]
-d <сек>, --delay=<сек>	задержка между итерациями [1 секунда]
-p <PID_процесса>, --pid= <PID_процесса>	PID процесса, который нужно отслеживать
-u <имя_пользователя>, --user= <имя_пользователя>	имя пользователя, которого нужно отследить
-P, --processes	отображать только процессы (по умолчанию — все процессы и потоки)
-a, --accumulated	показывать накопленный ввод-вывод вместо пропускной способности
-k, --kilobytes	отображать информацию в КБ
-t, --time	добавить отображение времени выполнения проверки
-q, --quiet	уменьшить количество выводимой информации (подразумевается --batch)

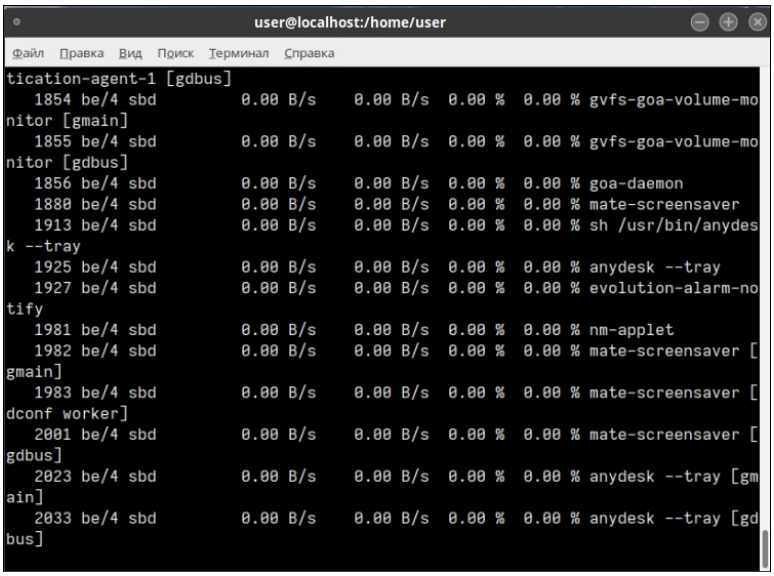
Также **iotop** поддерживает некоторое управление клавиатуры:

- стрелки **влево**-**вправо** — изменить сортировку колонок;
- **r** — изменить сортировку строк в выбранной колонке на обратную (a-z > z-a);
- **i** — изменить nice процесса (утилитой **ionice**);

Пример работы

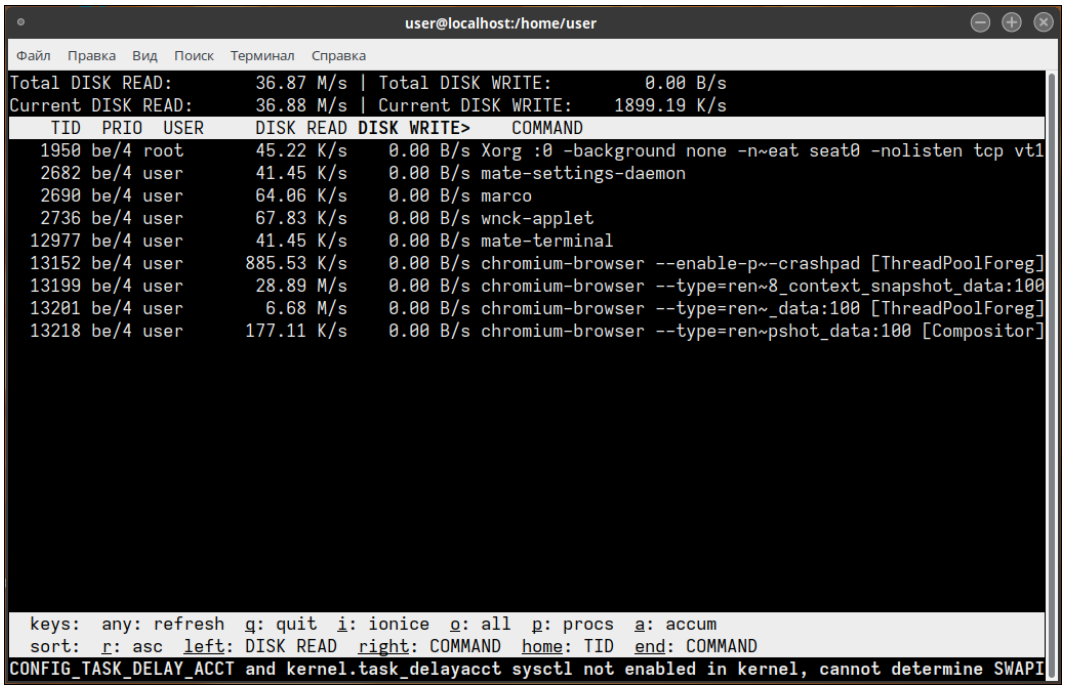
Для отключения интерактивного вида используйте:

```
iotop -b
```



Для отображения только процессов, которые в данный момент выполняют операции I/O с диском:

```
iotop -o
```

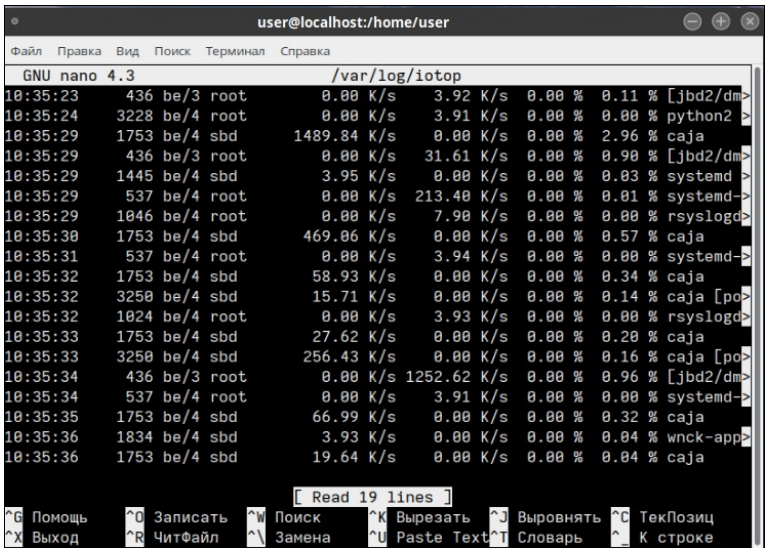


Программа позволяет не только выводить информацию, но и записывать ее для решения проблем в будущем.

Пример команды:

```
iotop -botqqqk --iter=60 >> /var/log/iotop
```

Результат можно посмотреть в указанном файле:



nfsiostat - утилита отображения статистики для файловых систем NFS

Синтаксис
Опции утилиты
Работа с утилитой

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: nfs-utils-1:2.5.2-0

nfsiostat – утилита отображения статистики операций ввода/вывода в файловых системах **NFS**.

Основные функции утилиты:

- отображение списка примонтированных NFS-каталогов;
- отслеживание скорости работы с каталогами;
- возможность просмотра статистики по определенному каталогу.

По умолчанию утилита предустановлена в РЕД ОС. Однако если по каким-либо причинам утилита отсутствует в вашей системе, для ее установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install nfs-utils
```

Для запуска утилиты перейдите в терминал и выполните команду (с правами **непривилегированного** пользователя):

```
nfsiostat
```

Синтаксис

Синтаксис утилиты имеет вид:

```
nfsiostat [ <интервал> [ <количество_отчетов> ] ] [ <опции> ] [ <точка_монтирования> ]
```

где:

- `<интервал>` – определяет интервал времени в секундах между каждым отчетом. Первый отчет содержит статистику за время с момента подключения файловой системы. Каждый последующий отчет содержит статистику, собранную за интервал времени, прошедший с момента предыдущего отчета. Отчет состоит из строки заголовка NFS, за которой следует строка статистики для каждой смонтированной сетевой файловой системы.
- `<количество_отчетов>` – определяет количество отчетов, созданных с интервалом в несколько секунд, можно указать вместе с параметром `<интервал>`. Если параметр `<интервал>` указан без параметра `<количество_отчетов>`, тогда утилита **nfsiostat** генерирует отчеты непрерывно.
- `<точка_монтирования>` – если указаны имена точек монтирования, будет отображаться статистика только для них. В противном случае перечисляются все точки монтирования NFS на клиенте.

Опции утилиты

Опции утилиты:

- **-h**, **--help** – вывод справки по утилите;
- **--version** – вывод версии утилиты.

Опции статистики:

- **-a**, **--attr** – отображать статистику, относящуюся к кешу атрибутов;

- **-d**, **--dir** – отображать статистику, относящуюся к операциям с каталогами;
- **-p**, **--page** – отображать статистику, относящуюся кешу страниц.

Опции формата отображения:

- **-s**, **--sort** – сортировать точки монтирования NFS по скорости работы;
- **-l <список>**, **--list=<список>** – выводить статистику только для первой точки монтирования в списке.

Работа с утилитой

Далее будут рассмотрены примеры работы с утилитой:

- вывод статистики с обновлением статистики каждые 5 секунд:

```
nfsiostat 5
```

где **5** – интервал обновления.

- вывод 10 отчетов с интервалом обновления статистики каждые 20 секунд:

```
nfsiostat 20 10
```

где:

- **20** – интервал обновления статистики;
- **10** – количество отчетов.
- запуск утилиты для определенной точки монтирования:

```
nfsiostat /home/test/
```

Пример:

На тестовом сервере примонтирован сетевой ресурс **/home/test** на источнике **10.81.186.174**. Запустим утилиту:

```
nfsiostat
```

```
[root@redos /]# nfsiostat

10.81.186.174:/home/test mounted on /home/test:

           ops/s       rpc bklog
           3.100           0.000

read:              ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                   0.000           0.000           0.000        0 (0.0%)           0.000           0.000           0.000        0 (0.0%)
write:             ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                   0.000           0.000           0.000        0 (0.0%)           0.000           0.000           0.000        0 (0.0%)
```

Утилита **nfsiostat** без параметров выведет список примонтированных ресурсов и текущую скорость работы с ними.

Запустим утилиту в момент копирования файла с источника.

Утилита **nfsiostat** покажет скорость загрузки.

```
[root@redos /]# nfsiostat

10.81.186.174:/home/test mounted on /home/test:

           ops/s       rpc bklog
          63.640           0.000

read:              ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                  63.430        8136.508         128.275        0 (0.0%)           0.399           0.496           0.027        0 (0.0%)
write:             ops/s            kB/s           kB/op         retrans    avg RTT (ms)    avg exe (ms)  avg queue (ms)          errors
                   0.000           0.000           0.000        0 (0.0%)           0.000           0.000           0.000        0 (0.0%)
```

В выводе утилиты также содержится важный параметр `avg RTT` – продолжительность времени с момента отправки ядром клиента запроса до момента получения ответа.

Высокий показатель `avg RTT` отражает высокую задержку в сети, которая влияет на производительность ввода-вывода, из-за чего могут возникнуть сложности работы с сетевым каталогом.

perf - анализ производительности ПО

Установка
Синтаксис
Опции
Команда bench
Команда stat
Команда top
Команда record
Команда report

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** perf 3.3.1-4

Perf - инструмент для анализа производительности программного обеспечения.

Через данную утилиту приложения могут использовать блок мониторинга производительности (PMU), точки трассировки и специальные счетчики в ядре для сбора статистики производительности.

Perf может не только анализировать проблемы производительности указанного приложения (для каждого потока), но и анализировать проблемы производительности ядра. Он также может анализировать код приложения и ядро одновременно, чтобы полностью понять узкие места производительности в приложении.

Установка

Для установки утилиты выполните команду:

```
sudo dnf install perf
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
perf [--version] [--help] [<опции>] <команда> [<аргументы>]
```

Опции

Основные опции утилиты:

- **--debug** — устанавливает для отладочных переменных значения от **0** до **10**, позволяя устанавливать следующие переменные:
    - **verbose** – базовые отладочные сообщения;
    - **ordered-events** – отладочные сообщения упорядоченных событий;
    - **data-convert** – отладочные сообщения команд преобразования данных;
    - **stderr** – запись отладочных сообщений (опция **-v**) на *stderr* в режиме браузера.

  Большее значение задает более подробный вывод.
- **--buildid-dir** — задает каталог кэширования идентификаторов сборки (эта опция имеет более высокий приоритет по сравнению с переменной buildid.dir в файле конфигурации);
- **-v, --version** — выводит версию программы *perf*;
- **-h, --help** — выводит справку о команде *perf*.

Команды утилиты

Команда bench

bench — общая база для тестов производительности.

Синтаксис

```
perf bench [<опции_общего_назначения>] <подсистемы> <тесты> [<опции_тестов>]
```

Опции общего назначения

- **-r, --repeat=<число>** - задаёт число повторения тестов (по умолчанию **10**);
- **-f, --format=<значение>** - задаёт стиль форматирования вывода:
  - **default** - принятый по умолчанию стиль, удобный для восприятия человеком;
  - **simple** - упрощённый стиль, удобный для обработки в программных сценариях.

Подсистемы

- **sched** - механизмы планировщиков и коммуникации между процессами (*IPC*);
- **mem** - производительность доступа к памяти;
- **numa** - планирование *NUMA* и производительность *MM*;
- **futex** -стрессовые тесты *Futex*;
- **epoll** - стрессовые тесты опроса событий (*epoll*);
- **all** - все подсистемы тестирования.

Тесты

Тесты для sched

messaging - набор тестов для оценки производительности механизмов планирования и IPC.

Опции *messaging*:

- **-p, --pipe** - использовать `pipe()` вместо `socketpair()`.
- **-t, --thread** - использовать множество потоков (`thread`) вместо множества процессов.
- **-g, --group=<число>** - задаёт число групп.
- **-l, --nr_loops=<число>** - задаёт число циклов.

pipe - тесты для системных вызовов `pipe()`.

Опции *pipe*:

- **-l, --loop=<число>** - задаёт число циклов.

Пример работы

```
 perf bench sched messaging

# Running 'sched/messaging' benchmark:
# 20 sender and receiver processes per group
# 10 groups == 400 processes run

     Total time: 2.886 [sec]

 perf bench sched messaging -t -g 20

# Running 'sched/messaging' benchmark:
# 20 sender and receiver threads per group
# 20 groups == 800 threads run
```

```
    Total time: 4.028 [sec]

 perf bench sched pipe

# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 9.023 [sec]

      9.023075 usecs/op
       110826 ops/sec

 perf bench sched pipe -l 1000

# Running 'sched/pipe' benchmark:
# Executed 1000 pipe operations between two processes

    Total time: 0.010 [sec]

     10.278000 usecs/op
        97295 ops/sec
```

Тесты для mem

memcpy - набор тестов для оценки скорости простых операций копирования в памяти различными способами.

Опции *memcpy*:

- **-s, --size** - размер копируемого блока (по умолчанию 1 Мбайт). Задаётся числом с суффиксом B, KB, MB, GB или TB (без учёта регистра символов).
- **-f, --function** - задаёт функцию копирования (по умолчанию **default**).
- **-l, --nr_loops** - задаёт повтор вызова memcpy указанное число раз.
- **-c, --cycles** - задаёт использование **perf** события `cpu-cycles` вместо системного вызова `gettimeofday`.

memset - набор тестов для оценки скорости простых операций установки памяти различными способами.

Опции для *memset*:

- **-s, --size** - размер копируемого блока (по умолчанию 1 Мбайт). Задаётся числом с суффиксом B, KB, MB, GB или TB (без учёта регистра символов).
- **-f, --function** - задаёт функцию копирования (по умолчанию **default**).
- **-l, --nr_loops** - задаёт повтор вызова memset указанное число раз.
- **-c, --cycles** - задаёт использование **perf** события `cpu-cycles` вместо системного вызова `gettimeofday`.

Пример работы

```
 perf bench mem memcpy

# Running 'mem/memcpy' benchmark:
# function 'default' (Default memcpy() provided by glibc)
# Copying 1MB bytes ...

      13.020833 GB/sec
# function 'x86-64-unrolled' (unrolled memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 1MB bytes ...

       9.765625 GB/sec
# function 'x86-64-movsq' (movsq-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 1MB bytes ...

       9.668936 GB/sec
# function 'x86-64-movsb' (movsb-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 1MB bytes ...
```

```
      9.964923 GB/sec


 perf bench mem memcpy -s 10MB -l 3

# Running 'mem/memcpy' benchmark:
# function 'default' (Default memcpy() provided by glibc)
# Copying 10MB bytes ...

     10.236504 GB/sec
# function 'x86-64-unrolled' (unrolled memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 10MB bytes ...

      3.372496 GB/sec
# function 'x86-64-movsq' (movsq-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 10MB bytes ...

      5.617809 GB/sec
# function 'x86-64-movsb' (movsb-based memcpy() in arch/x86/lib/memcpy_64.S)
# Copying 10MB bytes ...

      5.426352 GB/sec
```

Тесты для numa

mem - набор тестов для оценки выполнения заданий NUMA.

Тесты для futex

- **hash** - тесты для оценки хэш-таблиц;
- **wake** - тесты для оценки вызовов *wake*;
- **wake-parallel** - тесты для оценки параллельных вызовов *wake*;
- **requeue** - тесты для оценки вызовов requeue;
- **lock-pi** - тесты для оценки вызовов *futex lock_pi*.

Опции, применимые для всех тестов:

- **-S, --shared** - использовать вызовы общих *futex* вместо приватных;
- **-s, --silent** - без вывода данных и деталей;
- **-t, --threads <число>** - задаёт число потоков (*thread*).

Опции для отдельных тестов:

- **-f, --futexes <число>** - задаёт число вызовов *futex* на поток (только *hash*);
- **-r, --runtime <число>** - задаёт время работы в секундах (*hash* и *lock-pi*);
- **-w, --nwakes <число>** - задаёт число потоков для разового пробуждения (*wake* и *wake-parallel*);
- **-q, --nrequeue <число>** - задаёт число потоков для разового изменения очерёдности (только *requeue*);
- **-M, --multi** - использовать множество *futex* (только *lock-pi*).

Тесты для epoll

wait - тесты для оценки одновременных вызовов **epoll_wait**.

Опции для *wait*:

- **-B, --nonblocking** - неблокируемое поведение *epoll_wait;*
- **-E, --edge** - использовать интерфейс **Edge-triggered** (по умолчанию *LT*);
- **-m, --multiq** - использовать множество экземпляров epoll (по одному на поток);
- **-S, --oneshot** - использовать семантику *EPOLLONESHOT*.

ctl - тесты для оценки множества вызовов **epoll_ctl**.

Опции, применимые для всех тестов:

- **-f, --nfds <число>** - задаёт число файловых дескрипторов для отслеживания каждым потоком;
- **-N, --nested <число>** - задаёт уровень вложенности для иерархии *epoll* (по умолчанию без вложенности - **0**);
- **-n, --noaffinity** - отключает близость CPU (*affinity*);
- **-R, --randomize** - задаёт выполнение случайных операций на случайных дескрипторах файлов;
- **-r, --runtime <число>** - задаёт время работы в секундах;
- **-t, --threads <число>** - задаёт число потоков (*thread*).;
- **-v, --verbose** - расширенный вывод.

Команда stat

stat - выполняет указанную параметром команду, собирая статистику работы.

Синтаксис

```
perf stat [-e <EVENT> | --event=EVENT] [-a] <команда>
perf stat [-e <EVENT> | --event=EVENT] [-a] - <команда> [<опции>]
perf stat [-e <EVENT> | --event=EVENT] [-a] record [-o <файл>] - <команда> [<опции>]
perf stat report [-i <файл>]
```

Опции команды

- **<command>...** - любая команда, которая может быть выполнена в консоли;
- **-e, --event=<значение>** - задаёт событие PMU;
- **-i, --no-inherit** - дочерние задачи не наследуют счётчики;
- **-p, --pid=<pid>** - события для процесса с заданными идентификаторами (список разделённых запятыми значений);
- **-t, --tid=<tid>** - события для потоков (*thread*) с заданными идентификаторами (список разделённых запятыми значений);
- **-a, --all-cpus** - сбор в масштабе системы от всех CPU (используется по умолчанию, если цель не задана);
- **--no-scale** - отключает масштабирование и нормализацию значений счётчиков;
- **-d, --detailed** - задаёт уровень детализации вывода;
- **-r, --repeat=<значение>** - повтор команды заданное число раз (**не более 100**) с усреднением и указанием стандартного отклонения. **0** - означает бесконечный повтор;
- **-B, --big-num** - задаёт вывод больших чисел с отделением тысяч в соответствии с установками **locale**;
- **-C, --cpu=<значение>** - задаёт учёт лишь указанных CPU, которые можно задать номерами через запятые без пробелов (**0,1**) или как диапазон (**0-2**). В режиме учёта по потокам эта опция игнорируется. Для мониторинга в масштабе системы сохраняется актуальность опции **-a**. По умолчанию учитываются все процессоры;
- **-A, --no-aggr** - отключает агрегирование счётчиков для отслеживаемых CPU;
- **-n, --null** - пустой прогон без запуска счётчиков;
- **-v, --verbose** - задаёт подробный вывод (показывает ошибки открытия счётчиков и т. п.);
- **--table** - задаёт вывод времени для каждого запуска (опция **-r**) в форме таблицы.

Пример работы

```
perf stat --null -r 5 --table perf bench sched pipe

# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes
```

```
    Total time: 8.769 [sec]

      8.769539 usecs/op
       114031 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 8.799 [sec]

      8.799256 usecs/op
       113645 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 8.958 [sec]

      8.958335 usecs/op
       111627 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 9.020 [sec]

      9.020829 usecs/op
       110854 ops/sec
# Running 'sched/pipe' benchmark:
# Executed 1000000 pipe operations between two processes

    Total time: 9.080 [sec]

      9.080392 usecs/op
       110127 ops/sec

 Performance counter stats for 'perf bench sched pipe' (5 runs):

          # Table of individual measurements:
          8,7822 (-0,1613) #
          8,8164 (-0,1271) #
          8,9726 (+0,0291) #
          9,0432 (+0,0997) #
          9,1030 (+0,1595) #

          # Final result:
          8,9435 +- 0,0626 seconds time elapsed  ( +-  0,70% )
```

stat record - запись статистики в файл (по умолчанию **perf.data**).

Опции:

- **-i <файл>** - запись в выбранный файл.

stat raport - считывает файл данных **perf.data**, созданный командой perf record, и выводит профиль производительности, построенный по собранным ранее данным.

Опции:

- **-i <файл>, --input <файл>** - имя входного файла данных;
- **--per-socket** - объединение счётчиков по физическим процессорам для измерений в масштабе системы;
- **--per-core** - объединение счётчиков по ядрам одного физического процессора для измерений в масштабе системы;
- **-A, --no-aggr** - отключает объединение данных для всех отслеживаемых CPU.

Команда top

top - создание и вывод профиля производительности в реальном масштабе времени.

Синтаксис

```
perf top [-e <EVENT> | --event=EVENT] [<опции>]
```

Опции

- **-a, --all-cpus** - сбор данных на уровне системы в целом (используется по умолчанию);
- **-c <число>, --count=<число>** - период выборки событий;
- **-d <сек>, --delay=<сек>** - задает интервал обновления в секундах;
- **-v, --verbose** - задает подробный вывод (ошибки открытия счетчиков и т. п.).

Команда record

record - выполняет пользовательскую команду и записывает профиль работы в файл **perf.data**. Полученный файл можно затем использовать для подготовки отчёта с помощью perf report.

Синтаксис

```
perf record [-e <EVENT> | --event=EVENT] [-a] <команда>
perf record [-e <EVENT> | --event=EVENT] [-a] - <команда> [<опции>]
```

Опции

- **<command>...** - любая команда, которую можно выполнить в командном процессоре;
- **-c, --count=<число>** - период событий для выборки;
- **-o, --output=<файл>** - имя выходного файла;
- **-v, --verbose** - задаёт более подробный вывод (ошибки открытия счётчиков и т. п.);
- **-s, --stat** - задаёт запись счётчиков событий по потокам (*thread*). Для просмотра значений применяется команда perf report -T;
- **-d, --data** - запись виртуальных адресов выборок.

Команда report

report - считывает файл данных **perf.data**, созданный командой perf record, и выводит профиль производительности, построенный по собранным ранее данным.

Синтаксис

```
perf report [-i <файл> | --input=<файл>]
```

Опции

- **-i, --input=<файл>** - имя входного файла (по умолчанию **perf.data**, если *stdin* не является *fifo*);
- **-v, --verbose** - задаёт подробный вывод (адреса символов и т. п.);
- **-q, --quiet** - отменяет вывод сообщения, отменяя опцию **-v**;
- **-s, --sort=<ключ>** - задаёт сортировку гистограммы по указанным ключам.

tuned - служба оптимизации производительности системы

Tuned - это демон, который позволяет автоматически оптимизировать производительность системы под различные задачи, а также устанавливает системные параметры в соответствии с заданным профилем.

В службе **tuned** используются разные профили настроек для таких распространенных случаев использования, как высокая пропускная способность, низкая задержка или экономия энергии.

Служба **Tuned** по умолчанию предустановлена в РЕД ОС.

Вы можете подробнее ознакомиться с работой службы **tuned**, просмотрев наши обучающие видео:

- на **RuTube** — tuned - служба оптимизации производительности системы. Графическая утилита tuned-gtk;
- в **Яндекс.Дзен** — tuned - служба оптимизации производительности системы. Графическая утилита tuned-gtk;
- в **VK Видео** — tuned - служба оптимизации производительности системы. Графическая утилита tuned-gtk.

На наших каналах вы также сможете найти много другой полезной информации.

Включить **Tuned** можно командой:

```
systemctl enable --now tuned
```

Список профилей настроек:

Профиль	Описание профиля
balanced	Профиль для баланса между энергосбережением и производительностью
desktop	Профиль для повышения отклика графических приложений
throughput-performance	Профиль для установки максимальной пропускной способности
latency-performance	Профиль устанавливает низкую задержку за счет энергопотребления
network-latency	Профиль для установки дополнительных параметров настройки для обеспечения низкой задержки сети
network-throughput	Профиль для установки максимальной пропускной способности сети
powersave	Профиль для установки максимального энергосбережения
optimize-serial-console	Оптимизация для использования консоли
virtual-guest	Профиль оптимизации работы внутри гостевой системы при работе в среде виртуализации
virtual-host	Профиль оптимизации системы для максимальной производительности для запуска гостевых KVM
accelerator-performance	Настройка производительности с отключением состояний STOP с более высокой задержкой
hpc-compute	Оптимизация для вычислительных нагрузок HPC
intel-sst	Настройка для Intel Speed Select Technology (Intel SST)

Полный список **tuned** можно просмотреть при помощи команды:

```
tuned-adm list

Available profiles:
- accelerator-performance     - Throughput performance based tuning with disabled higher latency STOP states
- balanced                    - General non-specialized tuned profile
- desktop                     - Optimize for the desktop use-case
- hpc-compute                 - Optimize for HPC compute workloads
- intel-sst                   - Configure for Intel Speed Select Base Frequency
- latency-performance         - Optimize for deterministic performance at the cost of increased power consumption
- network-latency             - Optimize for deterministic performance at the cost of increased power consumption, focused on low latency
network performance
- network-throughput          - Optimize for streaming network throughput, generally only necessary on older CPUs or 40G+ networks
- optimize-serial-console     - Optimize for serial console use.
- powersave                   - Optimize for low power consumption
- throughput-performance      - Broadly applicable tuning that provides excellent performance across a variety of common server workloads
- virtual-guest               - Optimize for running inside a virtual guest
- virtual-host                - Optimize for running KVM guests
```

Проверка текущего профиля осуществляется командой:

```
tuned-adm active
```

```
No current active profile.
```

Для установки необходимого профиля нужно ввести команду:

```
tuned-adm profile <name>
```

где вместо **<name>** нужно указать необходимый профиль.

Далее следует проверить, что нужный профиль установлен, и подтвердить его командой:

```
tuned-adm active
```

Установите профиль максимальной производительности:

```
tuned-adm profile throughput-performance

tuned-adm active
Current active profile: throughput-perfomance
```

Для смены профиля на *сбалансированный* применяем аналогичные команды:

```
tuned-adm profile balanced
tuned-adm active Current active profile: balanced
```

Чтобы отключить данную службу нужно воспользоваться командами:

```
tuned-adm off
tuned-adm active No current active profile.
```

Графическая утилита tuned-gtk

Tuned можно настраивать через графическое приложение. Для установки пакета **tuned-gtk** перейдите в сеанс пользователя **root**:

```
su -
```

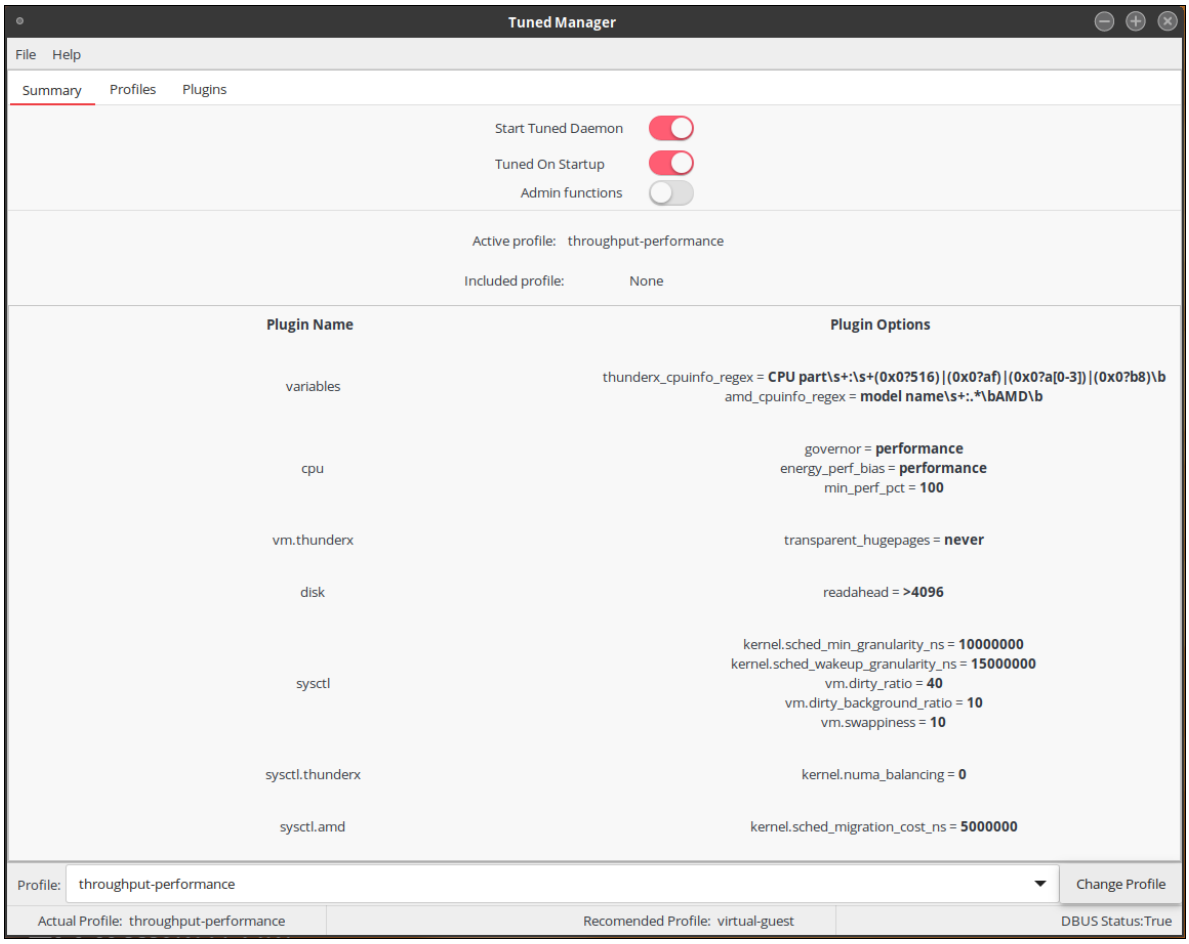
и выполните команду:

```
dnf install tuned-gtk
```

После установки утилита будет доступна из «**Главного меню**» — «**Параметры**» — «**tuned-gui**».

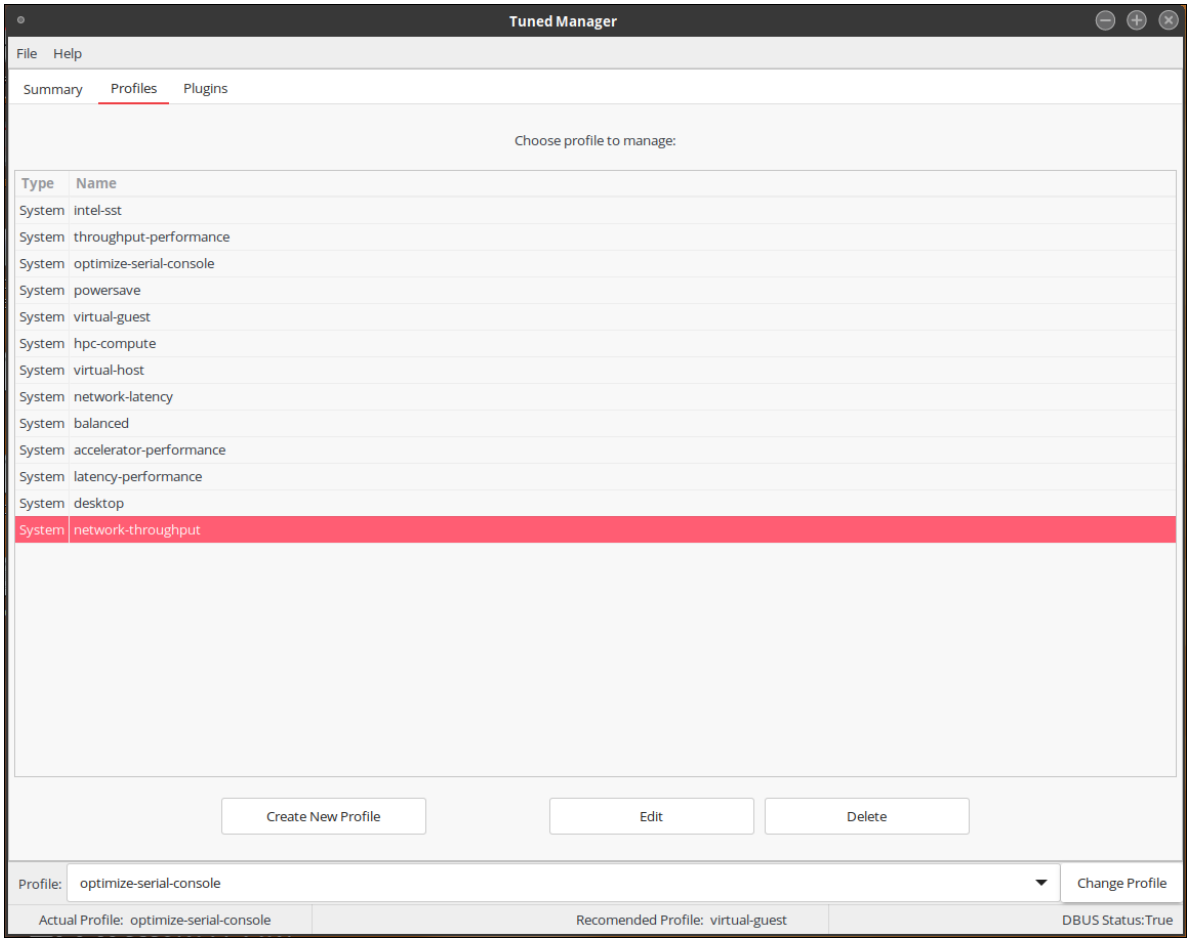
Обратите внимание, что перед использованием графической утилиты, необходимо сначала включить службу **Tuned** командой:

```
systemctl enable --now tuned
```

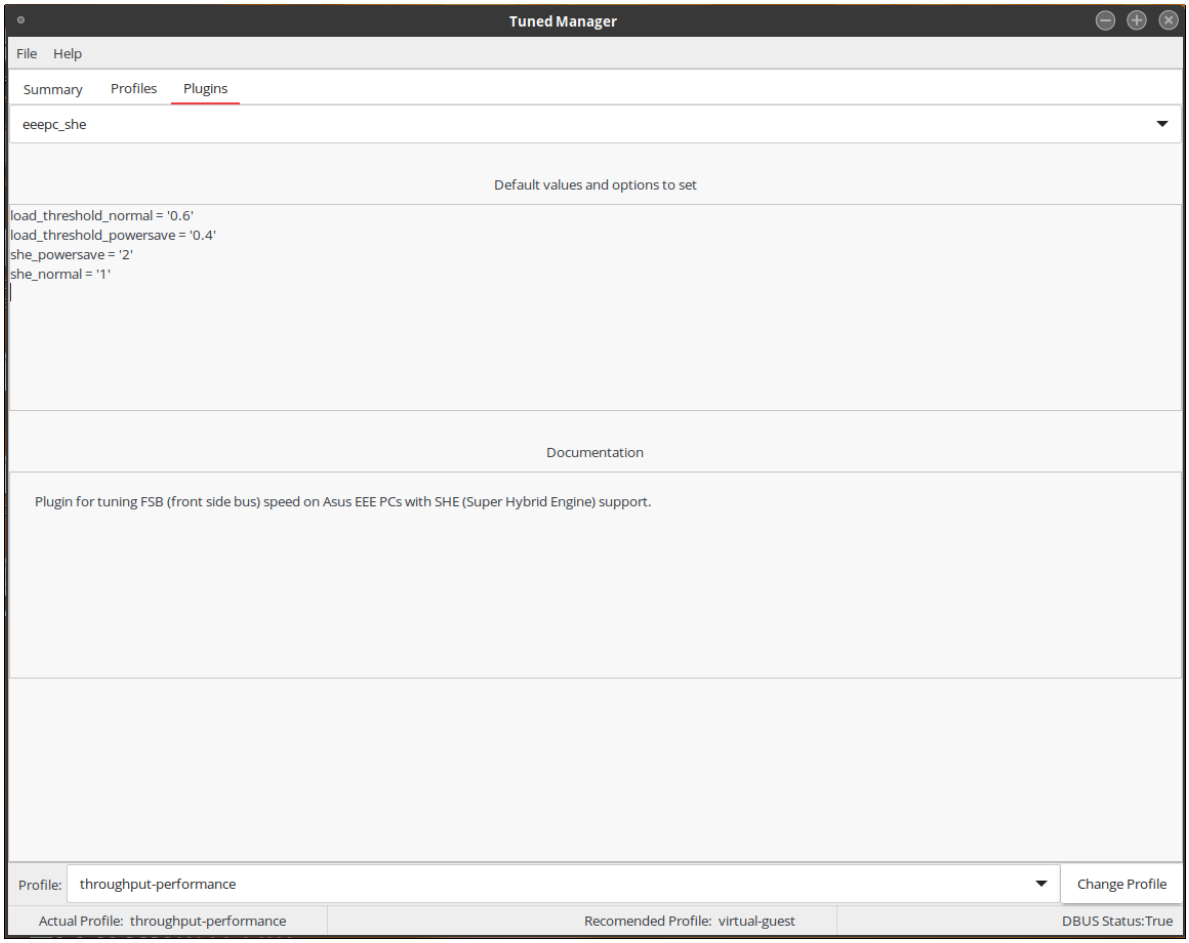


В приложении можно включить демон **tuned**, добавить его в автозапуск и выбрать необходимый профиль для работы системы. Изменить используемый профиль можно, выбрав профиль в списке «**Profile**» и затем нажав на кнопку «**Change Profile**».

На вкладке «**Profiles**» представлен список доступных профилей, а также есть возможность создать новый профиль, отредактировать или удалить уже имеющиеся профили.



Во вкладке «**Plugins**» в ниспадающем списке представлены имеющиеся плагины. При выборе любого из них будут выведены значения по умолчанию и поясняющая информация.



Тестирование производительности дисков с помощью fio

Установка
Синтаксис
Опции
Формат файла задания
Параметры файла задания
Примеры работы
Тесты производительности операций ввода-вывода в секунду
Тест скорости записи
Тест скорости чтения
Тест скорости чтения/записи
Тест пропускной способности
Использование файла задания
Тест с разными значениями iodepth
Удаление результатов тестирования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: fio-3.28-2

Fio (Flexible I/O Tester) — это инструмент, который позволяет запускать несколько потоков или процессов для выполнения операций ввода-вывода, заданных пользователем. Обычно **fio** используется для создания файла задания, описывающего нагрузку на ввод-вывод, которую необходимо смоделировать. Для получения точного результата тестирования производительности системы хранения данных важно учитывать несколько ключевых аспектов.

Выбор типов тестов и параметров **fio** является важным, поскольку такие настройки, как размер блока данных (**bs**) и количество задач (**numjobs**), могут существенно влиять на результаты. Изменение этих параметров может привести к получению различных данных о производительности. Поэтому следует стремиться к единообразию параметров на всех тестируемых стендах.

ВАЖНО!

Не запускайте тесты **fio** с рабочей нагрузкой на запись (**readwrite**, **randrw**, **write**, **trimwrite**) непосредственно на используемом устройстве. Для проведения таких тестов рекомендуется использовать тестовые среды или резервные устройства, чтобы избежать потери данных и негативных последствий для основного рабочего устройства.

Установка

Для установки утилиты выполните в терминале команду (потребуются права **администратора**):

```
sudo dnf install fio
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
fio [<Опции>] [<Файл задания>]
```

Опции

Основные опции **fio**:

- **--debug=<параметры>** — включает ведение журнала отладки;
- **--parse-only** — анализирует файл задания и выводит настройки, без операций ввода;
- **--merge-blktrace-only** — объединяет вывод **blktrace** (трассировка блоков) из предыдущих тестов;
- **--output=имя_файла** — указывает файл для записи результатов;

- **--output-format=формат** — устанавливает формат вывода;
- **--bandwidth-log** — включает ведение журнала пропускной способности;
- **--minimal** — выводит минимально необходимую информацию;
- **--append-terse** — дополняет короткий вывод предыдущих результатов;
- **--terse-version=версия** — указывает версию для короткого вывода;
- **--version** — выводит информацию о версии программы и завершает работу;
- **--help** — показывает справку по командам;
- **--cpuclock-test** — тестирует тактовую частоту процессора;
- **--crctest=[тест]** — запускает тест контрольной суммы;
- **--cmdhelp=команда** — выводит справку по указанной команде;
- **--enghelp=[ввод-вывод[,команда]]** — выводит справку по указанному механизму ввода-вывода и команде;
- **--showcmd** — показывает команду, которую нужно использовать для запуска текущей конфигурации;
- **--readonly** — работает в режиме только для чтения;
- **--eta=when** — показывает время до завершения (ETA) теста;
- **--eta-interval=время** — интервал обновления информации о ETA;
- **--eta-newline=время** — интервал добавления новой строки в вывод ETA;
- **--status-interval=время** — интервал обновления статуса;
- **--section=имя** — указывает конкретный раздел конфигурации для выполнения;
- **--alloc-size=kb** — устанавливает размер выделения памяти в КБ;
- **--warnings-fatal** — обрабатывает предупреждения как ошибки;
- **--max-jobs=номер** — максимальное количество параллельных задач;
- **--server=аргументы** — запускает **fio** в режиме сервера с указанными аргументами;
- **--daemonize=pid-файл** — запускает **fio** как фоновый процесс и записывает PID в файл;
- **--client=имя_хоста** — подключается к серверу **fio** на указанном хосте;
- **--remote-config=файл** — использует удалённый конфигурационный файл;
- **--idle-prof=опция** — формирует отчёт о простое процессора, опция может быть одной из следующих:
  - **calibrate** — выполняет калибровку и завершает работу;
  - **system** — показывает общий уровень простоя системы и единичную работу;
  - **percpu** — как system, но также показывает время простоя каждого процессора;
- **--inflate-log=журнал_регистрации** — увеличить размер лог-файла;
- **--trigger-file=файл** — выполняет команду запуска, когда файл существует;
- **--trigger-timeout=время** — время ожидания перед запуском триггера;
- **--trigger=команда** — устанавливает команду в качестве локального триггера;
- **--trigger-remote=команда** — устанавливает команду в качестве удалённого запуска;
- **--aux-path=путь** — вспомогательный путь для временных файлов вместо текущего рабочего каталога.

Формат файла задания

Любые параметры, следующие за **опциями**, будут считаться **файлами заданий**, если они не соответствуют параметру файла задания. В списке может быть несколько файлов заданий, и каждый файл задания будет рассматриваться как отдельная группа.

Fio принимает один или несколько файлов заданий, описывающих, что он должен делать. **Формат файла задания** — классический ini-файл, в котором имена, заключённые в квадратные скобки [], определяют название задания. Можно использовать любое имя в формате ASCII, кроме **global**, которое имеет предопределенное значение. После названия задания указывается последовательность из параметров, которые определяют поведение задания.

В разделе global устанавливаются значения по умолчанию для заданий, описанных в этом файле. Задание может переопределять параметр *global* section, а файл задания может также содержать несколько **глобальных параметров**.

Параметры файла задания

Для некоторых параметров используется параметр определённого типа, например, целое число или строка. Везде, где требуется числовое значение, можно использовать арифметическое выражение, при условии, что оно заключено в круглые скобки.

Поддерживаются следующие операции:

- сложение **(+)**,
- вычитание **(-)**,
- умножение **(*)**,
- деление **(/)**,
- модуль **(%)**,
- возведение в степень **(^)**.

Для значений времени в выражениях по умолчанию единицами измерения являются микросекунды.

Основные параметры для задания:

- **--name** — имя теста (можно изменить на любое другое);
- **--filename** — путь к файлу, который будет использоваться для тестирования I/O;
- **--directory** — каталог, который будет использоваться для тестирования I/O;
- **--size** — размер файла для теста;
- **--direct** — использование прямых I/O, обходящих кеш операционной системы;
- **--rw** — режим теста (чтение, запись или оба);
- **--bs** — размер блока ввода-вывода (I/O) для теста;
- **--ioengine** — механизм ввода-вывода, который будет использоваться для теста (например, libaio для асинхронного ввода-вывода);
- **--iodepth** — глубина очереди запросов на ввод-вывод для теста (количество одновременных запросов к файловой системе);
- **--runtime** — время выполнения теста;
- **--numjobs** — количество параллельных задач для теста;
- **--time_based** — время работы будет использоваться для определения длительности теста;
- **--group_reporting** — режим групповой отчётности (результаты будут отображаться для каждой группы рабочих нитей, а не для каждого рабочего потока);
- **--eta-newline** — интервал отображения прогресса выполнения теста и перевода строки.

Примеры работы

Тесты производительности операций ввода-вывода в секунду

Для тестирования пропускной способности используется одновременное чтение и запись небольшими блоками с использованием множества процессов. Тесты измеряют количество операций **чтения/записи**, которые система может выполнить за секунду.

Тесты являются показателем производительности хранилища данных или системы ввода-вывода и позволяют оценить **скорость обработки операций** ввода и вывода данных, независимо от их объёма. Чем выше значение **IOPS**, тем быстрее система может обрабатывать запросы на чтение и запись данных.

ВАЖНО!

При выполнении тестирования на запись в указанном файле данные перезаписываются. Поэтому не рекомендуется указывать в качестве файла блочное устройство с нужными данными.

Тест скорости записи

Перед выполнением теста убедитесь, что в указанной директории достаточно свободного места (более 5 ГБ) для завершения теста.

```
fio --name=fiotest --blocksize=4k --directory=/home/user --size=5g --ioengine=libaio --iodepth=256 --runtime=60 --rw=randwrite --direct=1
```

где:

- **--name=fiotest** — имя теста (можно изменить на любое другое);
- **--blocksize=4k** — размер блока данных для теста (4 КБ);
- **--directory=/home/user** — каталог, в котором будет проводиться тест;
- **--size=5g** — размер файла для теста (5 ГБ);
- **--ioengine=libaio** — использование libaio (асинхронный ввод-вывод);
- **--iodepth=256** — глубина очереди (256 запросов одновременно);
- **--runtime=60** — время выполнения теста (60 секунд);
- **--rw=randwrite** — режим теста (случайная запись);
- **--direct=1** — использование прямого доступа к устройству (чтобы избежать кеширования данных).

В результате запуска команды будет проведён тест производительности I/O на указанном каталоге с указанными параметрами.

Результат:

```
fiotest: (g=0): rw=randwrite, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
fio-3.28
Starting 1 process
fiotest: Laying out IO file (1 file / 5120MiB)
Jobs: 1 (f=1): [w(1)][100.0%][w=33.4MiB/s][w=8540 IOPS][eta 00m:00s]
fiotest: (groupid=0, jobs=1): err= 0: pid=3906: Tue Jul 30 12:05:52 2024
  write: IOPS=1354, BW=5418KiB/s (5548kB/s)(317MiB/60001msec); 0 zone resets
    slat (usec): min=4, max=7229.8k, avg=733.37, stdev=53817.01
    clat (usec): min=23, max=11931k, avg=188197.99, stdev=1188675.61
     lat (usec): min=89, max=11931k, avg=188931.83, stdev=1190998.57
    clat percentiles (msec):
     |  1.00th=[   10],  5.00th=[   12], 10.00th=[   12], 20.00th=[   13],
     | 30.00th=[   13], 40.00th=[   14], 50.00th=[   14], 60.00th=[   15],
     | 70.00th=[   20], 80.00th=[   27], 90.00th=[   75], 95.00th=[  184],
     | 99.00th=[ 7886], 99.50th=[11476], 99.90th=[11879], 99.95th=[11879],
     | 99.99th=[11879]
   bw (  KiB/s): min=    8, max=68669, per=100.00%, avg=17068.00, stdev=18091.84, samples=35
   iops        : min=    2, max=17167, avg=4266.94, stdev=4522.95, samples=35
  lat (usec)   : 50=0.01%, 100=0.01%, 250=0.01%, 500=0.02%, 750=0.02%
  lat (usec)   : 1000=0.02%
  lat (msec)   : 2=0.07%, 4=0.12%, 10=1.00%, 20=69.48%, 50=15.80%
  lat (msec)   : 100=5.15%, 250=4.88%, 500=0.76%, 750=0.08%, 1000=0.57%
  lat (msec)   : 2000=0.16%, >=2000=1.87%
  cpu          : usr=0.67%, sys=4.04%, ctx=77891, majf=0, minf=15
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=99.9%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=0,81270,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
  WRITE: bw=5418KiB/s (5548kB/s), 5418KiB/s-5418KiB/s (5548kB/s-5548kB/s), io=317MiB (333MB), run=60001-60001msec

Disk stats (read/write):
  sda: ios=3/77906, merge=0/1835, ticks=63/698196, in_queue=716266, util=95.37%
```

где:

- **slat** — время подачи операции ввода-вывода (задержка);
- **clat** — время от подачи до завершения операции ввода-вывода (задержка завершения);
- **lat** — полная задержка от создания до завершения операции;
- **bw** — пропускная способность: количество образцов и процент от общей пропускной способности;
- **iops** — IOPS-статистика операций в секунду;
- **lat (nsec/usec/msec)** — распределение задержек завершения операций ввода-вывода;
- **cpu** — использование процессора и количество переключений контекста, дефектов страниц;
- **IO depths** — распределение глубин ввода-вывода за время существования задания;
- **IO submit** — количество операций ввода-вывода, отправленных в одном вызове;
- **IO complete** — количество завершённых операций ввода-вывода;

- **IO issued rwt** — количество отправленных запросов на чтение/запись/обрезку, короткие или отброшенные;
- **IO latency** — задержки ввода-вывода для достижения заданной цели.

После того как каждый клиент был перечислен, появляются **статистические данные для группы**:

```
Run status group 0 (all jobs):
  WRITE: bw=5418KiB/s (5548kB/s), 5418KiB/s-5418KiB/s (5548kB/s-5548kB/s), io=317MiB (333MB), run=60001-60001msec
```

где:

- **WRITE** — указывает, что результаты относятся к операциям записи;
- **bw** — совокупная пропускная способность потоков в заданной группе, за которой следуют минимальная и максимальная пропускная способность всех потоков в группе. 5418KiB/s-5418KiB/s (5548kB/s-5548kB/s) — диапазон скоростей записи, достигнутых в ходе теста, является фиксированным;
- **io** — совокупный объём выполненных операций ввода-вывода всех потоков в группе;
- **run** — самое короткое и самое длинное время выполнения потоков в группе.

В конце выводится **статистика по дискам**:

```
Disk stats (read/write):
  sda: ios=3/77906, merge=0/1835, ticks=63/698196, in_queue=716266, util=95.37%
```

где:

- **ios** — количество операций ввода-вывода, выполненных всеми группами (**3** — количество операций чтения, **77906** — количество операций записи);
- **merge** — количество объединений, выполненных планировщиком ввода-вывода (иногда несколько операций могут быть объединены в одну, чтобы снизить нагрузку на систему). **0** — количество объединённых операций чтения, **1835** — количество объединённых операций записи.
- **ticks** — количество тактов, в течение которых диск был занят, **63** — время, затраченное на операции чтения (в миллисекундах), **698196** — время, затраченное на операции записи (в миллисекундах);
- **in_queue** — общее время, проведённое в очереди на выполнение (в миллисекундах);
- **util** — занятость устройства, отображаемая в процентах (**95.37%**). Значение, близкое к **100%**, может указывать на высокую загрузку диска и на необходимость оптимизации или добавления дополнительного оборудования.

Тест скорости чтения

Для корректного выполнения команды тестирования скорости чтения с приведёнными ниже параметрами необходимо выполнить следующие условия:

- для выполнения теста в директории /home/user автоматически будут созданы файлы для каждого задания, количество которых определяется параметром **--numjobs,** размер файлов определяется параметром **--size**;
- пользователь, под которым запускается команда **fio**, должен иметь права на чтение/запись файлов в директории /home/user.

```
fio --directory=/home/user --direct=1 --rw=randread --bs=4k --ioengine=libaio --iodepth=256 --runtime=60 --numjobs=3 --time_based --group_reporting --name=iops-test-job --eta-newline=1 --size=1G
```

где:

- **--directory=/home/user** — каталог /home/user, в котором будут созданы тестовые файлы;
- **--direct=1** — включает режим прямого ввода-вывода, обходя кеширование в операционной системе;
- **--rw=randread** — тип выполняемых операций ввода-вывода (randread означает случайное чтение). В режиме randread **fio** будет случайным образом выбирать блоки для чтения;
- **--bs=4k** — устанавливает размер блока ввода-вывода на 4 КБ, каждая операция чтения будет обрабатывать 4 КБ данных;
- **--ioengine=libaio** — указывает механизм ввода-вывода, **libaio** использует асинхронные операции ввода-вывода, позволяет одновременно запускать несколько запросов ввода-вывода, не дожидаясь завершения предыдущих;
- **--iodepth=256** — задаёт глубину очереди операций ввода-вывода, 256 операций могут находиться в очереди на выполнение одновременно;
- **--runtime=60** — устанавливает время выполнения теста в секундах;

- **--numjobs=3** — определяет количество параллельно выполняемых заданий, тест будет выполняться с тремя потоками;
- **--time_based** — указывает, что тест должен быть основан на времени, а не на объёме данных;
- **--group_reporting** — включает групповой отчёт, результаты всех заданий будут объединены и представлены как один общий результат;
- **--name=iops-test-job** — имя задания;
- **--eta-newline=1** — опция, которая указывает **fio** обновлять строку с расчётным оставшимся временем (ETA) каждую секунду.

Результат:

```
iops-test-job: (g=0): rw=randread, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
...
fio-3.28
Starting 3 processes
Jobs: 3 (f=3): [r(3)][4.9%][r=129MiB/s][r=33.1k IOPS][eta 00m:58s]
Jobs: 3 (f=3): [r(3)][6.6%][r=120MiB/s][r=30.7k IOPS][eta 00m:57s]
Jobs: 3 (f=3): [r(3)][9.8%][r=128MiB/s][r=32.8k IOPS][eta 00m:55s]
Jobs: 3 (f=3): [r(3)][13.1%][r=138MiB/s][r=35.4k IOPS][eta 00m:53s]
Jobs: 3 (f=3): [r(3)][14.8%][r=139MiB/s][r=35.6k IOPS][eta 00m:52s]
Jobs: 3 (f=3): [r(3)][16.4%][r=137MiB/s][r=35.0k IOPS][eta 00m:51s]
Jobs: 3 (f=3): [r(3)][18.0%][r=139MiB/s][r=35.6k IOPS][eta 00m:50s]
Jobs: 3 (f=3): [r(3)][19.7%][r=139MiB/s][r=35.7k IOPS][eta 00m:49s]
Jobs: 3 (f=3): [r(3)][21.3%][r=133MiB/s][r=34.0k IOPS][eta 00m:48s]
Jobs: 3 (f=3): [r(3)][24.6%][r=139MiB/s][r=35.7k IOPS][eta 00m:46s]
Jobs: 3 (f=3): [r(3)][27.9%][r=138MiB/s][r=35.3k IOPS][eta 00m:44s]
Jobs: 3 (f=3): [r(3)][29.5%][r=140MiB/s][r=35.8k IOPS][eta 00m:43s]
Jobs: 3 (f=3): [r(3)][32.8%][r=139MiB/s][r=35.5k IOPS][eta 00m:41s]
Jobs: 3 (f=3): [r(3)][36.1%][r=140MiB/s][r=35.8k IOPS][eta 00m:39s]
Jobs: 3 (f=3): [r(3)][40.0%][r=139MiB/s][r=35.5k IOPS][eta 00m:36s]
Jobs: 3 (f=3): [r(3)][41.0%][r=139MiB/s][r=35.7k IOPS][eta 00m:36s]
Jobs: 3 (f=3): [r(3)][44.3%][r=140MiB/s][r=35.7k IOPS][eta 00m:34s]
Jobs: 3 (f=3): [r(3)][47.5%][r=138MiB/s][r=35.4k IOPS][eta 00m:32s]
Jobs: 3 (f=3): [r(3)][50.8%][r=139MiB/s][r=35.7k IOPS][eta 00m:30s]
Jobs: 3 (f=3): [r(3)][53.3%][r=138MiB/s][r=35.2k IOPS][eta 00m:28s]
Jobs: 3 (f=3): [r(3)][54.1%][r=126MiB/s][r=32.4k IOPS][eta 00m:28s]
Jobs: 3 (f=3): [r(3)][57.4%][r=139MiB/s][r=35.7k IOPS][eta 00m:26s]
Jobs: 3 (f=3): [r(3)][60.0%][r=139MiB/s][r=35.6k IOPS][eta 00m:24s]
Jobs: 3 (f=3): [r(3)][60.7%][r=139MiB/s][r=35.7k IOPS][eta 00m:24s]
Jobs: 3 (f=3): [r(3)][63.9%][r=139MiB/s][r=35.7k IOPS][eta 00m:22s]
Jobs: 3 (f=3): [r(3)][65.6%][r=139MiB/s][r=35.7k IOPS][eta 00m:21s]
Jobs: 3 (f=3): [r(3)][68.9%][r=139MiB/s][r=35.7k IOPS][eta 00m:19s]
Jobs: 3 (f=3): [r(3)][70.5%][r=136MiB/s][r=34.9k IOPS][eta 00m:18s]
Jobs: 3 (f=3): [r(3)][73.8%][r=134MiB/s][r=34.2k IOPS][eta 00m:16s]
Jobs: 3 (f=3): [r(3)][78.3%][r=135MiB/s][r=34.5k IOPS][eta 00m:13s]
Jobs: 3 (f=3): [r(3)][80.3%][r=135MiB/s][r=34.5k IOPS][eta 00m:12s]
Jobs: 3 (f=3): [r(3)][83.6%][r=136MiB/s][r=34.7k IOPS][eta 00m:10s]
Jobs: 3 (f=3): [r(3)][85.2%][r=133MiB/s][r=34.2k IOPS][eta 00m:09s]
Jobs: 3 (f=3): [r(3)][86.9%][r=134MiB/s][r=34.3k IOPS][eta 00m:08s]
Jobs: 3 (f=3): [r(3)][88.5%][r=133MiB/s][r=34.1k IOPS][eta 00m:07s]
Jobs: 3 (f=3): [r(3)][91.8%][r=136MiB/s][r=34.8k IOPS][eta 00m:05s]
Jobs: 3 (f=3): [r(3)][95.1%][r=128MiB/s][r=32.6k IOPS][eta 00m:03s]
Jobs: 3 (f=3): [r(3)][96.7%][r=126MiB/s][r=32.2k IOPS][eta 00m:02s]
Jobs: 3 (f=3): [r(3)][100.0%][r=130MiB/s][r=33.2k IOPS][eta 00m:00s]
iops-test-job: (groupid=0, jobs=3): err= 0: pid=3593: Tue Jul 30 21:43:19 2024
  read: IOPS=34.7k, BW=136MiB/s (142MB/s)(8133MiB/60007msec)
    slat (nsec): min=1166, max=97127k, avg=75924.61, stdev=510067.56
    clat (usec): min=2, max=123674, avg=22035.95, stdev=4534.57
     lat (msec): min=6, max=123, avg=22.11, stdev= 4.54
    clat percentiles (msec):
     |  1.00th=[   16],  5.00th=[   18], 10.00th=[   19], 20.00th=[   20],
     | 30.00th=[   21], 40.00th=[   21], 50.00th=[   22], 60.00th=[   23],
     | 70.00th=[   24], 80.00th=[   24], 90.00th=[   26], 95.00th=[   27],
     | 99.00th=[   34], 99.50th=[   40], 99.90th=[   91], 99.95th=[  101],
     | 99.99th=[  117]
   bw (  KiB/s): min=103294, max=148248, per=100.00%, avg=138926.83, stdev=2412.68, samples=357
   iops        : min=25823, max=37062, avg=34731.20, stdev=603.19, samples=357
  lat (usec)   : 4=0.01%
  lat (msec)   : 10=0.03%, 20=27.34%, 50=72.31%, 100=0.25%, 250=0.06%
  cpu          : usr=2.31%, sys=13.81%, ctx=45133, majf=0, minf=805
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
```

```
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=2081938,0,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
   READ: bw=136MiB/s (142MB/s), 136MiB/s-136MiB/s (142MB/s-142MB/s), io=8133MiB (8528MB), run=60007-60007msec

Disk stats (read/write):
  sda: ios=2055328/37, merge=82/22, ticks=487922/130, in_queue=488058, util=80.34%
```

где:

- **iops** — среднее количество операций ввода/вывода в секунду (34,700 операций чтения в секунду);
- **bw** — средняя скорость передачи данных — 136 МБ/с;
- **latency** — среднее время, которое требуется для завершения одной операции чтения — 22.11 миллисекунды;
- **clat percentiles** — показывает, какое время задержки имеет определённый процент запросов:
  - 1% запросов имеют задержку менее 16 мс;
  - 50% запросов имеют задержку менее 22 мс;
  - 99% запросов имеют задержку менее 34 мс.
- **cpu** — процентное использование процессора: usr=2.31%, sys=13.81% (2.31% используется для пользовательских задач, 13.81% для системных задач);
- **IO depths** — все операции ввода/вывода были выполнены с глубиной очереди 64 или больше: >=64=100.0%;
- **общее количество данных прочитано**: 8133 МБ (8.528 ГБ);
- **средняя скорость чтения**: 136 МБ/с;
- **среднее количество операций чтения в секунду**: 34,700 IOPS;
- **процент выполнения операций**:
  - 50% операций завершены за 22 мс или меньше;
  - 95% операций завершены за 27 мс или меньше.

Результат показывает:

- выполнение операций чтения с пропускной способностью в 136 МБ/с и 34.7k IOPS;
- среднее время задержки в 22 мс и латентность в 100 мс для 99% операций демонстрируют, что задержки относительно стабильны и приемлемы для большинства операций;
- процент использования процессора относительно низкий, что указывает на то, что CPU не является узким местом в тесте.

Тест скорости чтения/записи

```
 fio --directory=/home/user --direct=1 --rw=randrw --bs=4k --ioengine=libaio --iodepth=256 --runtime=60 --numjobs=3 --time_based --group_reporting --name=iops-test-job --eta-newline=1
```

где:

- **--directory=/home/user** — директория, где будут производиться тесты ввода-вывода;
- **--direct=1** — активирует прямой ввод-вывод, что означает, что операции не будут кешироваться операционной системой;
- **--rw=randrw** — режим работы, тест будет одновременно выполнять операции чтения и записи в случайном порядке;
- **--bs=4k** — устанавливает размер блока для операций ввода-вывода, размер блока равен 4 КБ (4096 байт);
- **--ioengine=libaio** — механизм ввода-вывода, libaio — асинхронный ввод-вывод через библиотеку libaio;
- **--iodepth=256** — определяет глубину очереди ввода-вывода (256 — максимальное количество операций ввода-вывода, которые могут находиться в ожидании одновременно);
- **--runtime=60** — устанавливает время работы теста в секундах — 60 секунд (1 минута);
- **--numjobs=3** — количество задач, которые будут выполняться параллельно;
- **--time_based** — задаёт режим тестирования по времени, а не по количеству операций;
- **--group_reporting** — указывает, что результаты теста должны группироваться и выводиться в одном отчёте для всех задач, а не

по отдельности для каждой;

- **--name=iops-test-job** — задаёт имя теста, которое будет отображаться в результатах;
- **--eta-newline=1** — выводит оставшееся время в следующей строке в процессе выполнения теста.

Результат:

```
iops-test-job: (g=0): rw=randrw, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
...
fio-3.28
Starting 3 processes
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1053564928, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1066758144, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1072381952, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1066737664, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1039486976, buflen=4096
fio: io_u error on file /home/user/iops-test-job.1.0: No space left on device: write offset=1033895936, buflen=4096
fio: pid=3773, err=28/file:io_u.c:1845, func=io_u error, error=No space left on device
Jobs: 2 (f=2): [m(2),X(1)][4.9%][r=47.4MiB/s,w=46.8MiB/s][r=12.1k,w=12.0k IOPS][eta 00m:58s]
Jobs: 2 (f=2): [m(2),X(1)][8.2%][r=51.2MiB/s,w=50.3MiB/s][r=13.1k,w=12.9k IOPS][eta 00m:56s]
Jobs: 2 (f=2): [m(2),X(1)][9.8%][r=47.4MiB/s,w=48.7MiB/s][r=12.1k,w=12.5k IOPS][eta 00m:55s]
Jobs: 2 (f=2): [m(2),X(1)][11.5%][r=44.5MiB/s,w=44.5MiB/s][r=11.4k,w=11.4k IOPS][eta 00m:54s]
Jobs: 2 (f=2): [m(2),X(1)][13.1%][r=47.0MiB/s,w=46.6MiB/s][r=12.0k,w=11.9k IOPS][eta 00m:53s]
Jobs: 2 (f=2): [m(2),X(1)][16.4%][r=44.6MiB/s,w=45.0MiB/s][r=11.4k,w=11.5k IOPS][eta 00m:51s]
Jobs: 2 (f=2): [m(2),X(1)][18.0%][r=47.4MiB/s,w=47.5MiB/s][r=12.1k,w=12.2k IOPS][eta 00m:50s]
Jobs: 2 (f=2): [m(2),X(1)][21.3%][r=43.3MiB/s,w=43.6MiB/s][r=11.1k,w=11.2k IOPS][eta 00m:48s]
Jobs: 2 (f=2): [m(2),X(1)][23.0%][r=43.4MiB/s,w=43.7MiB/s][r=11.1k,w=11.2k IOPS][eta 00m:47s]
Jobs: 2 (f=2): [m(2),X(1)][26.2%][r=47.7MiB/s,w=47.3MiB/s][r=12.2k,w=12.1k IOPS][eta 00m:45s]
Jobs: 2 (f=2): [m(2),X(1)][29.5%][r=46.8MiB/s,w=47.2MiB/s][r=12.0k,w=12.1k IOPS][eta 00m:43s]
Jobs: 2 (f=2): [m(2),X(1)][32.8%][r=47.6MiB/s,w=47.4MiB/s][r=12.2k,w=12.1k IOPS][eta 00m:41s]
Jobs: 2 (f=2): [m(2),X(1)][36.1%][r=46.5MiB/s,w=47.1MiB/s][r=11.9k,w=12.1k IOPS][eta 00m:39s]
Jobs: 2 (f=2): [m(2),X(1)][40.0%][r=50.2MiB/s,w=49.8MiB/s][r=12.9k,w=12.7k IOPS][eta 00m:36s]
Jobs: 2 (f=2): [m(2),X(1)][41.0%][r=49.3MiB/s,w=49.1MiB/s][r=12.6k,w=12.6k IOPS][eta 00m:36s]
Jobs: 2 (f=2): [m(2),X(1)][44.3%][r=47.6MiB/s,w=47.6MiB/s][r=12.2k,w=12.2k IOPS][eta 00m:34s]
Jobs: 2 (f=2): [m(2),X(1)][47.5%][r=49.8MiB/s,w=49.7MiB/s][r=12.8k,w=12.7k IOPS][eta 00m:32s]
Jobs: 2 (f=2): [m(2),X(1)][49.2%][r=49.0MiB/s,w=48.8MiB/s][r=12.6k,w=12.5k IOPS][eta 00m:31s]
Jobs: 2 (f=2): [m(2),X(1)][53.3%][r=48.3MiB/s,w=49.3MiB/s][r=12.4k,w=12.6k IOPS][eta 00m:28s]
Jobs: 2 (f=2): [m(2),X(1)][56.7%][r=48.6MiB/s,w=49.0MiB/s][r=12.4k,w=12.5k IOPS][eta 00m:26s]
Jobs: 2 (f=2): [m(2),X(1)][60.0%][r=48.0MiB/s,w=47.8MiB/s][r=12.3k,w=12.2k IOPS][eta 00m:24s]
Jobs: 2 (f=2): [m(2),X(1)][60.7%][r=48.0MiB/s,w=48.1MiB/s][r=12.3k,w=12.3k IOPS][eta 00m:24s]
Jobs: 2 (f=2): [m(2),X(1)][63.9%][r=51.0MiB/s,w=50.6MiB/s][r=13.1k,w=13.0k IOPS][eta 00m:22s]
Jobs: 2 (f=2): [m(2),X(1)][67.2%][r=49.8MiB/s,w=49.5MiB/s][r=12.7k,w=12.7k IOPS][eta 00m:20s]
Jobs: 2 (f=2): [m(2),X(1)][70.5%][r=49.0MiB/s,w=50.3MiB/s][r=12.5k,w=12.9k IOPS][eta 00m:18s]
Jobs: 2 (f=2): [m(2),X(1)][73.8%][r=48.5MiB/s,w=49.4MiB/s][r=12.4k,w=12.7k IOPS][eta 00m:16s]
Jobs: 2 (f=2): [m(2),X(1)][78.3%][r=48.2MiB/s,w=47.3MiB/s][r=12.3k,w=12.1k IOPS][eta 00m:13s]
Jobs: 2 (f=2): [m(2),X(1)][80.3%][r=50.3MiB/s,w=49.4MiB/s][r=12.9k,w=12.7k IOPS][eta 00m:12s]
Jobs: 2 (f=2): [m(2),X(1)][83.6%][r=50.2MiB/s,w=49.0MiB/s][r=12.9k,w=12.5k IOPS][eta 00m:10s]
Jobs: 2 (f=2): [m(2),X(1)][85.2%][r=47.5MiB/s,w=47.7MiB/s][r=12.2k,w=12.2k IOPS][eta 00m:09s]
Jobs: 2 (f=2): [m(2),X(1)][86.9%][r=50.1MiB/s,w=49.5MiB/s][r=12.8k,w=12.7k IOPS][eta 00m:08s]
Jobs: 2 (f=2): [m(2),X(1)][90.2%][r=48.8MiB/s,w=49.6MiB/s][r=12.5k,w=12.7k IOPS][eta 00m:06s]
Jobs: 2 (f=2): [m(2),X(1)][93.4%][r=48.4MiB/s,w=47.4MiB/s][r=12.4k,w=12.1k IOPS][eta 00m:04s]
Jobs: 2 (f=2): [m(2),X(1)][96.7%][r=47.5MiB/s,w=48.7MiB/s][r=12.2k,w=12.5k IOPS][eta 00m:02s]
Jobs: 2 (f=2): [m(2),X(1)][98.4%][r=49.8MiB/s,w=49.5MiB/s][r=12.8k,w=12.7k IOPS][eta 00m:01s]
Jobs: 2 (f=2): [m(2),X(1)][100.0%][r=48.9MiB/s,w=47.9MiB/s][r=12.5k,w=12.3k IOPS][eta 00m:00s]
iops-test-job: (groupid=0, jobs=3): err=28 (file:io_u.c:1845, func=io_u error, error=No space left on device): pid=3771: Tue Jul 30 23:06:17
2024
  read: IOPS=12.3k, BW=48.1MiB/s (50.4MB/s)(2886MiB/60002msec)
    slat (nsec): min=1679, max=61519k, avg=57980.28, stdev=147149.84
    clat (usec): min=1126, max=163039, avg=20880.35, stdev=5236.80
     lat (usec): min=1188, max=163066, avg=20938.57, stdev=5236.55
    clat percentiles (usec):
     |  1.00th=[14746],  5.00th=[15664], 10.00th=[16057], 20.00th=[16581],
     | 30.00th=[17171], 40.00th=[17957], 50.00th=[18744], 60.00th=[21627],
     | 70.00th=[23200], 80.00th=[24773], 90.00th=[27132], 95.00th=[31327],
     | 99.00th=[36963], 99.50th=[39060], 99.90th=[49021], 99.95th=[51643],
     | 99.99th=[76022]
   bw (  KiB/s): min=35632, max=53506, per=100.00%, avg=49309.31, stdev=1275.25, samples=236
   iops        : min= 8907, max=13376, avg=12326.85, stdev=318.82, samples=236
  write: IOPS=12.3k, BW=48.1MiB/s (50.5MB/s)(2888MiB/60002msec); 0 zone resets
    slat (usec): min=2, max=112744, avg=98.70, stdev=586.77
```

```
    clat (usec): min=1013, max=162272, avg=20443.88, stdev=5185.99
     lat (usec): min=1125, max=163299, avg=20542.90, stdev=5202.03
    clat percentiles (usec):
     |  1.00th=[14353],  5.00th=[15401], 10.00th=[15795], 20.00th=[16319],
     | 30.00th=[16712], 40.00th=[17433], 50.00th=[18220], 60.00th=[21103],
     | 70.00th=[22938], 80.00th=[24249], 90.00th=[26608], 95.00th=[30802],
     | 99.00th=[36439], 99.50th=[38536], 99.90th=[48497], 99.95th=[51119],
     | 99.99th=[76022]
   bw (  KiB/s): min=37137, max=53249, per=100.00%, avg=49333.05, stdev=1188.12, samples=236
   iops        : min= 9283, max=13312, avg=12332.74, stdev=297.01, samples=236
  lat (msec)   : 2=0.01%, 4=0.01%, 10=0.02%, 20=56.72%, 50=43.18%
  lat (msec)   : 100=0.07%, 250=0.01%
  cpu          : usr=2.87%, sys=16.33%, ctx=447882, majf=0, minf=56
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=738903,739381,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
   READ: bw=48.1MiB/s (50.4MB/s), 48.1MiB/s-48.1MiB/s (50.4MB/s-50.4MB/s), io=2886MiB (3027MB), run=60002-60002msec
  WRITE: bw=48.1MiB/s (50.5MB/s), 48.1MiB/s-48.1MiB/s (50.5MB/s-50.5MB/s), io=2888MiB (3028MB), run=60002-60002msec

Disk stats (read/write):
  sda: ios=738033/738664, merge=43/87, ticks=767404/135599, in_queue=903136, util=72.27%
```

Тест пропускной способности

Для тестирования пропускной способности используется одновременное чтение и запись крупными блоками с использованием множества процессов. Эти тесты измеряют значение объёма данных, который может быть передан за определённое время. Чем выше значение пропускной способности, тем больше данных может быть передано или принято за единицу времени.

bw — основной параметр вывода для теста пропускной способности, означающий совокупную пропускную способность потоков в группе, за которой следуют минимальная и максимальная пропускная способность всех потоков.

> Перед выполнением теста убедитесь, что в указанной директории достаточно свободного места (более 10 ГБ) для завершения теста.

Тест чтения/записи:

```
fio --name=fiotest --blocksize=256k --directory=/home/user --size=10G --ioengine=psync --iodepth=1 --runtime=120 --rw=randrw --direct=1 --numjobs=25 --group_reporting
```

где:

• **--name=fiotest** — имя задания, используемое для отчётов;

• **--blocksize=256k** — устанавливает размер читаемого или записываемого блока данных на 256 КБ;

• **--directory=/home/user** — задаёт каталог /home/user, в котором будут созданы тестовые файлы;

• **--size=10G** — общий объем данных, который будет использоваться для каждого задания (10 ГБ);

• **--ioengine=psync** — устанавливает синхронный механизм ввода-вывода с использованием стандартных системных вызовов (pread/pwrite);

• **--iodepth=1** — глубина очереди ввода-вывода, которая равна 1, каждая операция будет дожидаться завершения перед началом следующей;

• **--runtime=120** — устанавливает время выполнения теста в 120 секунд;

• **--rw=randrw** — режим работы с диском: данные будут читаться и записываться случайным образом;

• **--direct=1** — включает режим прямого ввода-вывода, минуя кеширование в операционной системе;

• **--numjobs=25** — количество параллельно выполняемых заданий (25 заданий);

• **--group_reporting** — включает групповой отчёт, объединяющий результаты всех заданий.

Использование файла задания

Можно получить более последовательные результаты, если использовать файл задания вместо выполнения команды напрямую.

Для этого создайте файл задания **fiorandomreadwrite.fio**:

```
nano fiorandomreadwrite.fio
```

Добавьте в файл следующие строки:

```
[global]

name=fiotest
blocksize=4k
directory=/home/user
size=5g
ioengine=libaio
iodepth=256
runtime=60
rw=randwrite
direct=1
runtime=60
rw=randwrite
direct=1
[job1]
filename=directory=/home/user
```

Для выполнения файла задания используйте команду:

```
fio ./fiorandomreadwrite.fio
```

Результат:

```
job1: (g=0): rw=randwrite, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=256
fio-3.28
Starting 1 process
job1: Laying out IO file (1 file / 5120MiB)
Jobs: 1 (f=1): [w(1)][100.0%][w=53.5MiB/s][w=13.7k IOPS][eta 00m:00s]
job1: (groupid=0, jobs=1): err= 0: pid=4312: Tue Jul 30 12:29:40 2024
  write: IOPS=5104, BW=19.9MiB/s (20.9MB/s)(1197MiB/60001msec); 0 zone resets
    slat (usec): min=4, max=6968.9k, avg=192.75, stdev=21138.71
    clat (nsec): min=884, max=8563.0M, avg=49933698.53, stdev=420390411.52
     lat (usec): min=89, max=8563.0k, avg=50126.78, stdev=421252.44
    clat percentiles (msec):
     |  1.00th=[   11],  5.00th=[   12], 10.00th=[   12], 20.00th=[   13],
     | 30.00th=[   13], 40.00th=[   14], 50.00th=[   14], 60.00th=[   14],
     | 70.00th=[   14], 80.00th=[   18], 90.00th=[   25], 95.00th=[   43],
     | 99.00th=[  342], 99.50th=[ 2039], 99.90th=[ 7282], 99.95th=[ 8423],
     | 99.99th=[ 8423]
   bw (  KiB/s): min=    8, max=74003, per=100.00%, avg=38357.61, stdev=26329.13, samples=61
   iops        : min=    2, max=18500, avg=9589.21, stdev=6582.25, samples=61
  lat (nsec)   : 1000=0.01%
  lat (usec)   : 50=0.01%, 100=0.01%, 250=0.01%, 500=0.01%, 750=0.01%
  lat (usec)   : 1000=0.01%
  lat (msec)   : 2=0.01%, 4=0.04%, 10=0.45%, 20=82.69%, 50=12.38%
  lat (msec)   : 100=2.49%, 250=0.46%, 500=0.70%, 750=0.09%, 1000=0.01%
  lat (msec)   : 2000=0.16%, >=2000=0.50%
  cpu          : usr=1.00%, sys=15.06%, ctx=334602, majf=0, minf=16
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%, >=64=100.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued rwts: total=0,306304,0,0 short=0,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=256

Run status group 0 (all jobs):
```

```
  WRITE: bw=19.9MiB/s (20.9MB/s), 19.9MiB/s-19.9MiB/s (20.9MB/s-20.9MB/s), io=1197MiB (1255MB), run=60001-60001msec
Disk stats (read/write):
  sda: ios=4/304465, merge=0/6666, ticks=446/976801, in_queue=983934, util=84.55%
```

Тест с разными значениями iodepth

> Перед выполнением теста убедитесь, что в указанной директории достаточно свободного места (более 5 ГБ) для завершения теста.

Основная цель данного теста — измерить производительность дисковой подсистемы при различных значениях iodepth.

Значение iodepth определяет, сколько операций ввода-вывода может быть выполнено одновременно. Чем **выше значение** iodepth, тем **выше нагрузка** на систему, и тест позволяет увидеть, как это влияет на скорость чтения/записи.

Тест можно использовать для:

- оценки производительности устройства хранения;
- выявления пределов производительности для различных сценариев загрузки;
- сравнения различных устройств хранения;
- оптимизации конфигураций серверов/приложений, особенно при высокой нагрузке.

Скрипт для тестирования диска с разными значениями iodepth (разным количеством одновременных запросов):

Создайте файл **run_fio_tests.sh**:

```
nano run_fio_tests.sh
```

Добавьте в файл следующие строки:

```
#!/bin/bash
for i in 1 2 4 8 16 32 64 128 256 512 1024; do
  echo "Testing with iodepth=$i"
  fio --name=fiotest --ioengine=libaio --direct=1 --rw=randread --bs=4k --size=5G --randrepeat=0 --norandommap --fsync=1 --numjobs=1 --runtime=60 --group_reporting --directory=/base/fio_test --iodepth=$i
  echo ""
done
```

где:

- **--name=fiotest** — название теста;
- **--ioengine=libaio** — задаёт используемый механизм ввода-вывода. libaio — асинхронный механизм ввода-вывода, который позволяет программе выполнять ввод-вывод в неблокирующем режиме;
- **--direct=1** — ввод-вывод будет осуществляться непосредственно на устройство, минуя кеш операционной системы;
- **--rw=randread** — тип операции ввода-вывода (read/write). randread означает, что будут выполняться случайные операции чтения;
- **--bs=4k** — размер блока ввода-вывода 4 КБ;
- **--size=5G** — определяет общий размер файла — 5 ГБ, который будет использоваться в тестировании;
- **--randrepeat=0** — указывает, что не нужно повторять одно и то же случайное последовательности ввода-вывода;
- **--norandommap** — отключает создание карты случайных блоков;
- **--fsync=1** — после каждой записи необходимо синхронизировать данные с устройством хранения;
- **--numjobs=1** — определяет количество параллельных задач, которые будут запущены. В примере 1 задача;
- **--runtime=60** — определяет продолжительность теста в секундах. Тест будет выполняться 60 секунд;
- **--group_reporting** — результаты должны быть собраны и отображены глобально;
- **--directory=/home/user** — определяет директорию, где будет осуществляться тестирование;
- **--iodepth=$i** — глубина очереди ввода-вывода, которая будет варьироваться от 1 до 1024 в зависимости от текущего значения $i

в цикле.

Сделайте файл исполняемым:

```
chmod +x run_fio_tests.sh
```

Запустите скрипт:

```
./run_fio_tests.sh
```

Удаление результатов тестирования

Удалить файлы после тестирования можно с помощью следующей команды:

```
rm /home/user/fiotest*
```

где:

- **/home/user/fiotest*** — путь и шаблон имён файлов, которые нужно удалить.

Перед удалением можно проверить, что удаляются только нужные файлы:

```
ls /home/user/fiotest*
```

Примерный вывод:

```
/home/user/fiotest.0.0 /home/user/fiotest.1.0
```

Анализ производительности блочных устройств (blktrace) и построение графиков на основе собранных данных (iowatcher)

Установка
Возможности blktrace
Возможности iowatcher
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: blktrace-1.0.5-10, iowatcher-1.0-8

blktrace – это инструмент для трассировки событий блочного ввода/вывода, который использует трассировщик **blktrace** в ядре. Это низкоуровневый инструмент, отображающий множество событий для каждой операции ввода/вывода. **blktrace** используется в качестве вспомогательного инструмента в программных решениях, предназначенных для анализа и диагностики проблем производительности в системах хранения данных.

iowatcher – утилита, позволяющая анализировать данные, подготовленные с помощью **blktrace** и строить на основе этих данных графики (в том числе и анимированные). Т.е. инструмент **blktrace** позволяет записывать события в файлы трассировки для последующей визуализации с помощью утилиты **iowatcher**. Поэтому работу **iowatcher** не стоит рассматривать отдельно от **blktrace**.

С помощью **iowatcher** также можно запускать **blktrace** с последующим созданием графика трассировки одной командой.

Установка

Для установки утилит перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install blktrace iowatcher
```

Возможности blktrace

blktrace запускает трассировку драйвера блочного устройства в ядре и возвращает данные трассировки, которые можно обработать помимо **iowatcher** с помощью **blkparse**. Для удобства был также создан инструмент **btrace**, который запускает **blktrace** и **blkparse**, т.е. следующие команды дадут один и тот же вывод:

```
blktrace -d /dev/sda -o - | blkparse -i -
```

```
btrace /dev/sda
```

Ниже приведен пример трассировки события «*запись в файл на примере команды* `echo 1 > test.txt`».

```
btrace /dev/sdb

  8,16   5        1     0.000000000 193450 A RM  973080688 + 8 <- (8,17) 973078640
  8,16   5        2     0.000000744 193450  Q RM  973080688 + 8 [bash]
  8,16   5        3     0.000003993 193450 G RM  973080688 + 8 [bash]
  8,16   5        4     0.000004498 193450  P  N  [bash]
  8,16   5        5     0.000005205 193450  UT N  [bash] 1
  8,16   5        6     0.000005495 193450 I  RM  973080688 + 8 [bash]
  8,16   5        7     0.000014361   266 D RM  973080688 + 8 [kworker/5:1H]
  8,16   3        1     0.001309172     0  C  RM  973080688 + 8 [0]
  8,16   5        8     0.001354482 193450 A  W  976766976 + 8 <- (8,17) 976764928
  8,16   5        9     0.001354754 193450  Q  W  976766976 + 8 [bash]
  8,16   5       10     0.001356122 193450  G W  976766976 + 8 [bash]
  8,16   5       11     0.001356303 193450 P  N  [bash]
  8,16   5       12     0.001357581 193450 D  W  976766976 + 8 [bash]
```

```
  8,16  3      2    0.001417097    0  C  W  976766976 + 8 [0]
```

В выводе представлено несколько строк – по одной на каждое действие (событие), связанное с очередью блочного устройства или с самим устройством.

По умолчанию выводится семь столбцов:

1. Старший и младший номер устройства.

2. Идентификатор процессора.

3. Порядковый номер.

4. Время события в секундах от начала трассировки.

5. Идентификатор процесса.

6. Идентификатор действия: тип события.

7. Описание **RWBS**: флаги ввода/вывода.

Далее приведено описание идентификаторов из страницы справочного руководства для **blkparse**. Этот список показывает, какие события может наблюдать фреймворк **blktrace**:

- **A** – ввод/вывод был отображен на другое устройство;
- **B** – дополнительный ввод/вывод;
- **C** – ввод/вывод завершен;
- **D** – запрос передан драйверу;
- **F** – запрос добавлен в начало другого запроса, находившегося в очереди;
- **G** – выделение памяти для запроса;
- **I** – запрос добавлен в очередь планировщика ввода/вывода;
- **M** – запрос добавлен в конец другого запроса, находившегося в очереди;
- **P** – блокировка очереди для накопления нескольких запросов;
- **Q** – ввод/вывод передан коду, который управляет очередью;
- **S** – ожидание освобождения структуры для размещения запроса;
- **T** – разблокировка очереди по тайм-ауту;
- **U** – разблокировка очереди;
- **X** – запрос разделен.

Для нужд мониторинга ядро позволяет описать тип каждой операции ввода/вывода с помощью строки символов — rwbs. Она применяется в **blktrace** и в других инструментах трассировки, определена в функции ядра **blk_fill_rwbs()** и использует следующие символы:

- **R**: чтение (*read*);
- **W**: запись (*write*);
- **M**: метаданные (*metadata*);
- **S**: синхронная (*synchronous*);
- **A**: опережающее чтение (*read-ahead*);
- **F**: выталкивание на диск или принудительное обращение к блоку (*flush or force*);
- **D**: отмена (*discard*);
- **E**: стирание (*erase*);
- **N**: нет операции (none).

Символы могут комбинироваться. Например, «***WM***» означает «***запись метаданных***».

Возможности iowatcher

Наиболее часто используемые параметры запуска:

- **-d** – определяет, какое устройство отслеживать, параметр перенаправляется в **blktrace** для создания новой трассировки;
- **-p** – инициирует запуск другой программы во время снятия трассировки. Программа и аргументы ее запуска должны быть указаны после всех остальных параметров утилиты **iowatcher**;
- **-K** – сохраняет файлы **SVG** для создания анимированного графика;
- **-t** – определяет расположение и имя файла, в котором хранятся трассировки **blktrace**. Можно указывать только каталог с набором трассировок;
- **-l** – добавляет метки на графике;
- **-m** – создает анимированный график;
- **-T** – задает заголовок, который будет размещен в верхней части графика;
- **-o** – определяет расположение и имя файла для SVG или видео;
- **-h** – задает высоту графика;
- **-w** – задает ширину графика;
- **-c** – количество столбцов в графике;
- **-x** – ограничивает диапазон обрабатываемого времени;
- **-P** – различать процессы в графике ввода/вывода;
- **-O** – позволяет генерировать только необходимые графики (по умолчанию генерируются все);
- **-N** – противоположность параметра **-O**, определяет тот график, который нужно пропустить.

Варианты графиков – *io*, *tput*, *latency*, *queue_depth*, *iops*, *cpu-sys*, *cpu-io*, *cpu-irq*, *cpu-user*, *cpu-soft*.

Примеры использования

Для того чтобы снять показания с блочного устройства (диска) за определенный интервал времени, необходимо выполнить команду:

```
blktrace -w 600 -d /dev/sda1 -o- > trace.dump
```

где:

- `w 300` – интервал времени в секундах, в течение которого будут сниматься показания;
- `d /dev/sda` – устройство, с которого будет сниматься статистика ввода-вывода;
- `-o-` – вывод статистики в консоль;
- `trace.dump` – перенаправление из консоли в файл **trace.dump**.

Для создания графика используется утилита **iowatcher**.

```
iowatcher -t trace.dump -o trace.svg
```

Файл **trace.svg** можно открыть в браузере или любом другом графическом редакторе.

Дополнительные типовые примеры использования:

- Создать график из существующего файла трассировки:

```
iowatcher -t trace
```

- Пропустить график ввода/вывода в создаваемом файле **trace.svg**:

```
iowatcher -t trace.dump -o trace.svg -N io
```

- Сгенерировать график только с показаниями **latency** (задержка):

```
iowatcher -t trace.dump -o trace.svg -O latency
```

- Запустить тест **fio** и снять трассировку этого процесса через **blktrace** на устройстве **/dev/sda**, при этом **fio** будет запущен с

параметрами, которые указаны в `-p fio some_job_file`:

```
iowatcher -d /dev/sda -t trace.dump -T 'Fio Benchmark' -p 'fio some_job_file'
```

- Снять трассировку с диска **/dev/sdb** и сразу создать график:

```
iowatcher -d /dev/sdb -t trace -o trace.svg
```

- Анимированный график можно получить при помощи команды:

```
iowatcher -t trace.dump --movie -o trace.mp4
```

Настройка сервера на postgresql 13 и zabbix 6.4

Предварительная подготовка сервера
Настройка сервера на PostgreSQL 13
Установка и настройка zabbix 6
Настройка базы данных
Запуск процесса zabbix-сервера
Настройка из веб-интерфейса

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** postgresql13-13.16-1, zabbix-server-pgsql-1:6.4.18-2

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. **Zabbix** использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления практически для любого события и быстро реагировать на проблемы с серверами. **Zabbix** предлагает отличные функции отчетности и визуализации данных, основанные на данных истории. Это делает **zabbix** идеальным для планирования мощности и мониторинга состояния серверов.

Zabbix разделяется на два вида: **zabbix-agent** и **zabbix-server**.

Zabbix-server собирает данные со всех клиентов, обрабатывает их, выводя на экран в веб-интерфейсе, и рассылает уведомления.

Zabbix-agent установлен на серверах, с которых необходимо собирать информацию об их состоянии, таких агентов может быть множество.

Примечание.

Для **zabbix 6** требуется **postgresql 13 и выше**. В инструкции будет рассмотрен пример настройки сервера на **postgresql 13**.

Предварительная подготовка сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

1. Настройте политики безопасности с помощью команд:

```
setsebool -P httpd_can_network_connect on
setsebool -P httpd_can_network_connect_db on
```

2. Обновите систему.

```
dnf update
```

3. Установите следующие пакеты и добавьте пакет **httpd** в автозагрузку.

```
dnf install httpd zabbix-apache-conf zabbix-sql-scripts
systemctl enable httpd
```

Настройка сервера на PostgreSQL 13

1. Установите сервер баз данных **postgresql** и добавьте его в автозагрузку:

```
dnf install postgresql13 postgresql13-server
systemctl enable postgresql-13
```

2. Выполните инициализацию нового сервера баз данных **postgresql**:

```
/usr/bin/postgresql-13-setup initdb
```

3. Запустите **postgres**:

```
systemctl start postgresql-13
```

Установка и настройка zabbix 6

Установите **zabbix**:

```
dnf install zabbix-server-pgsql zabbix-web-pgsql zabbix-agent
```

Далее необходимо отредактировать файл **php.ini**:

```
nano /etc/php.ini
```

Приведите параметры к следующему виду:

```
date.timezone = Europe/Moscow      #обязательно укажите свой часовой пояс
post_max_size = 16M
max_execution_time = 300
max_input_time = 300
```

и сохраните изменения.

Настройка базы данных PostgreSQL

Сначала нужно создать пользователя и базу данных, для этого необходимо выполнить команду:

```
su postgres
```

и подключиться к серверу базы данных:

```
psql
```

Затем создайте пользователя и базу данных с именем **zabbix** и предоставьте пользователю права на использование данной БД (пароль укажите свой):

```
CREATE ROLE zabbix WITH NOSUPERUSER LOGIN PASSWORD 'zabbixpassword';
CREATE   DATABASE zabbix WITH OWNER zabbix;
GRANT ALL PRIVILEGES ON DATABASE zabbix TO zabbix;
```

Будет создан пользователь с именем **zabbix**, паролем **zabbixpassword** и база данных с именем **zabbix**.

При выполнении команд получится следующее:

```
postgres=# CREATE ROLE zabbix WITH NOSUPERUSER LOGIN PASSWORD 'zabbixpassword';
CREATE ROLE
postgres=# CREATE   DATABASE zabbix WITH OWNER zabbix;
CREATE   DATABASE
postgres=# GRANT ALL PRIVILEGES ON DATABASE zabbix TO zabbix;
GRANT
```

Проверьте, что таблицы создались:

```
\l
```

Отключитесь от базы:

```
\q
```

Завершите сессию пользователя **postgres**:

```
exit
```

Затем необходимо перенастроить сам сервер **postgresql**:

```
nano /var/lib/pgsql/13/data/postgresql.conf
```

Найдите строку:

```
listen_addresses = 'localhost'
```

и приведите ее к виду:

```
listen_addresses = '*'
```

Затем раскомментируйте строку:

```
#port = 5432
```

и сохраните изменения.

После этого необходимо предоставить права доступа пользователю **zabbix** к базе данных по паролю, для этого требуется отредактировать другой файл:

```
nano /var/lib/pgsql/13/data/pg_hba.conf
```

найдите строку:

```
host    replication     all             127.0.0.1/32            scram-sha-256
```

и перед ней добавьте запись, чтобы выглядело следующим образом:

```
host    zabbix  zabbix        127.0.0.1/32        password
host    replication     all             127.0.0.1/32            scram-sha-256
```

Далее замените все **scram-sha-256** на **md5**, конечный вариант файла:

```
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host zabbix        zabbix        127.0.0.1/32        password
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```

Перезапустите сервер **postgresql**:

```
systemctl restart postgresql-13
```

Импортируйте содержимое SQL-дампа в базу данных:

```
zcat /usr/share/zabbix-sql-scripts/postgresql/server.sql.gz | sudo -u zabbix psql zabbix
```

Сменить пароль **psql** можно так:

```
passwd postgres
```

На этом настройка базы данных закончена, осталось настроить **zabbix**-сервер.

Отредактируйте файл конфигурации сервера **zabbix**. Пропишите данные для подключения к базе данных:

```
nano /etc/zabbix/zabbix_server.conf
```

Измените строки (их нужно раскомментировать, если они закоментированы, и присвоить нужные значения, если их нет или они отличаются):

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbixpassword
```

Запуск процесса zabbix-сервера

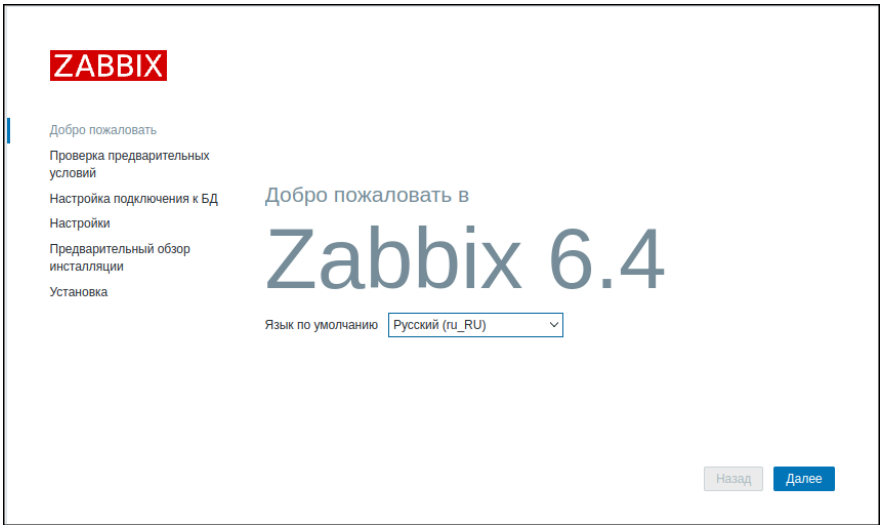
Запустите **zabbix**-сервер и добавьте его в автозагрузку:

```
systemctl restart zabbix-server
systemctl enable zabbix-server
systemctl restart zabbix-agent
systemctl enable zabbix-agent
systemctl restart httpd
```

Настройка из веб-интерфейса

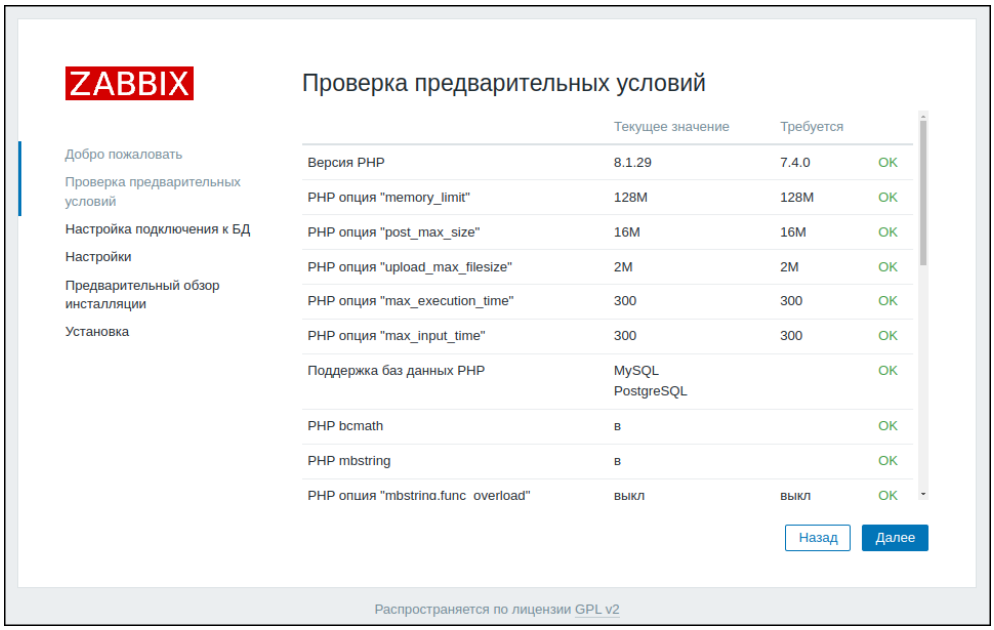
- Для того чтобы войти в веб-интерфейс, укажите в адресной строке браузера **http://<ip-адрес_сервера>/zabbix**.

Откроется страница приветствия.



Выберете язык и нажмите «**Далее**»

- Затем вы попадете на страницу преднастроек. Если вы ранее указали временную зону, то во всех пунктах должно быть « **OK**».



Нажмите «**Далее**».

- Укажите данные для подключения к ранее созданной базе данных.

В поле:

Database host — укажите адрес сервера **127.0.0.1**;

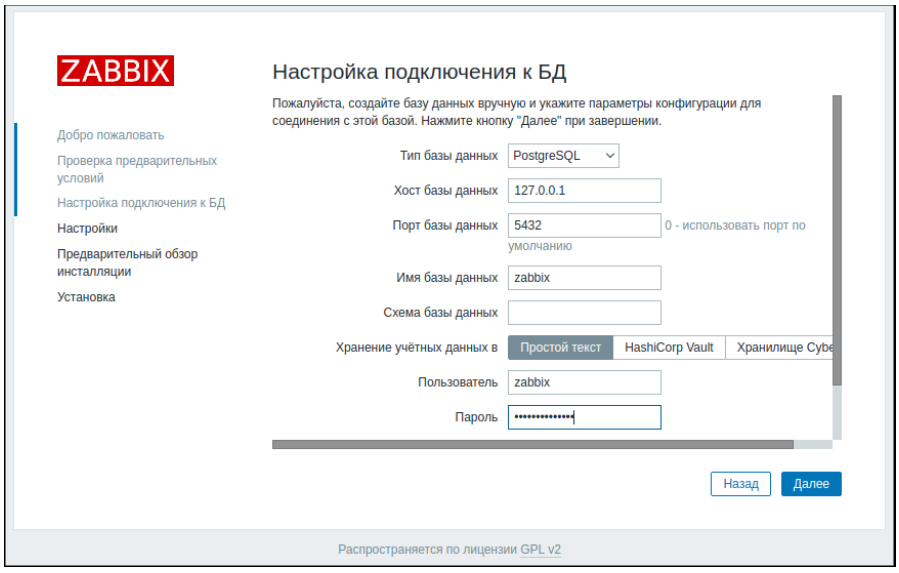
Database port — стандартный порт postgres **5432**;

Database name — имя базы данных **zabbix**;

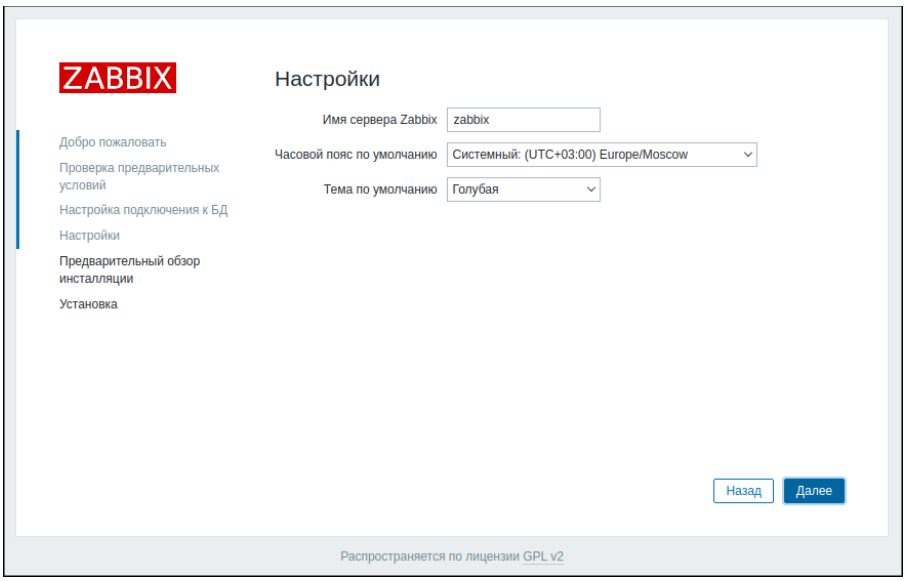
User — логин пользователя **zabbix**;

Password — пароль пользователя **zabbixpassword**.

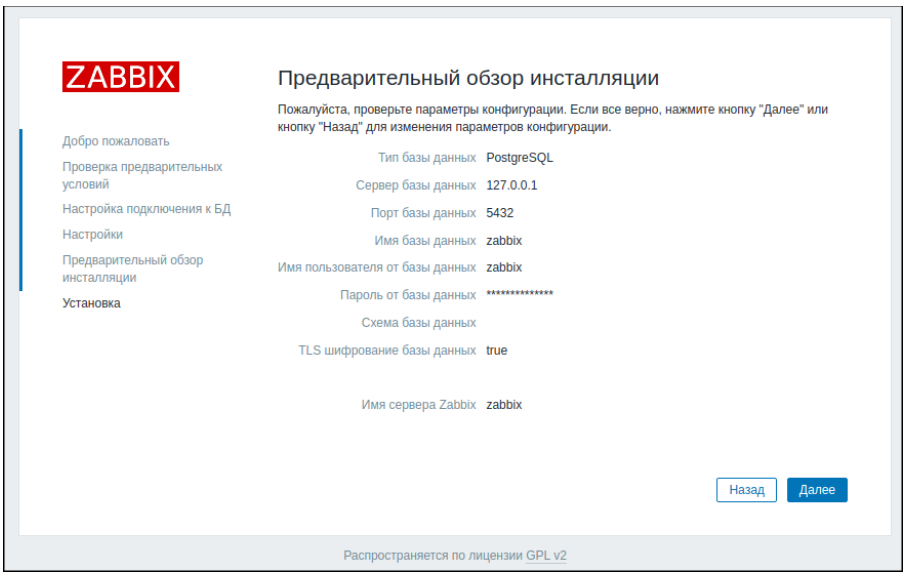
Нажмите «**Далее**». При неправильно указанных данных или неправильной конфигурации базы данных появится сообщение об ошибке подключения к базе.



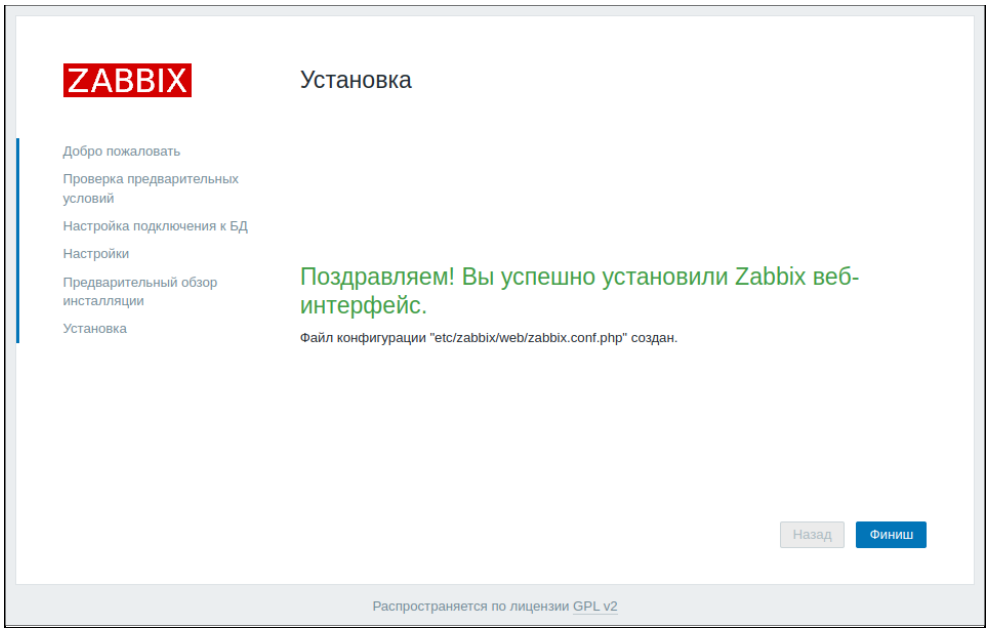
- В следующем окне нужно ввести имя сервера **Zabbix**. Проверьте часовой пояс и нажмите «**Далее**».



- Проверьте правильность введенных данных и нажмите «**Далее**».

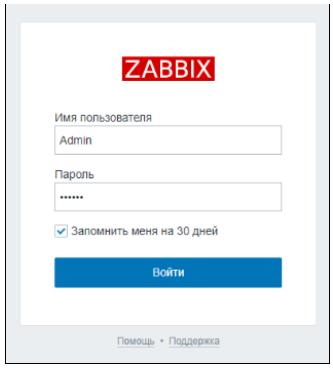


- При успешном окончании установки вы увидите следующую страницу.



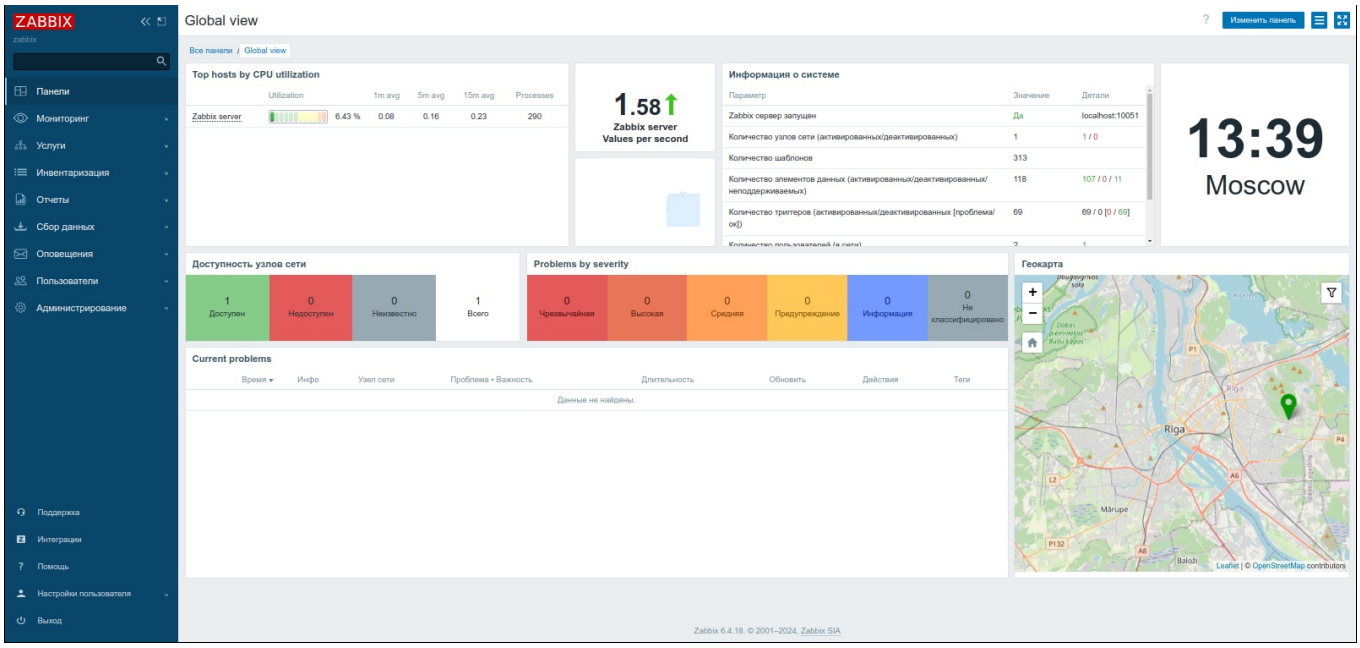
Нажмите «**Финиш**».

- Введите логин и пароль сервера **zabbix**. По умолчанию имя пользователя - **Admin** (регистр важен), пароль - **zabbix**.



Нажмите «**Войти**».

Вы попадете в панель управления. На этом настройка **zabbix** на **PSQL** завершена.



Настройка сервера на MySQL и Zabbix 6.4

Предварительная подготовка сервера
Настройка сервера на MYSQL
Настройка базы данных
Запуск процесса zabbix-сервера
Настройка из веб-интерфейса

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** mariadb-3:10.11.6-2, zabbix-server-mysql-1:6.4.18-2

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. **Zabbix** использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления практически для любого события и быстро реагировать на проблемы с серверами. **Zabbix** предлагает отличные функции отчетности и визуализации данных, основанные на данных истории. Это делает **zabbix** идеальным для планирования мощности и мониторинга состояния серверов.

Zabbix разделяется на два вида: **zabbix-agent** и **zabbix-server**.

Zabbix-server собирает данные со всех клиентов, обрабатывает их, выводя на экран в веб-интерфейсе, и рассылает уведомления.

Zabbix-agent установлен на серверах, с которых необходимо собирать информацию об их состоянии, таких агентов может быть множество.

Предварительная подготовка сервера

Перейдите в сеанс пользователя **root**:

```
su -
```

Здесь и далее команды будут выполняться с правами пользователя **root**, если не указано иное.

1. Настройте политики безопасности с помощью команд:

```
setsebool -P httpd_can_network_connect on
setsebool -P httpd_can_network_connect_db on
```

2. Обновите систему.

```
dnf update
```

3. Установите следующие пакеты и добавьте пакет **httpd** в автозагрузку.

```
dnf install httpd zabbix-apache-conf zabbix-sql-scripts
systemctl enable httpd
```

Настройка сервера на MYSQL

Установите необходимые пакеты для работы с БД:

```
dnf install mariadb mariadb-server zabbix-server-mysql zabbix-agent
```

Запустите и добавьте в автозагрузку службу **mariadb**:

```
sudo systemctl start mariadb && systemctl enable mariadb
```

Выполните скрипт **mysql_secure_installation**, чтобы защитить базу данных от злоумышленников:

```
sudo mysql_secure_installation
```

На первом шаге должен быть задан пароль **root** (это НЕ системный root), по умолчанию пароль не задан, нажмите **Enter**.

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none): <нажмите_Enter>
OK, successfully used password, moving on...
```

Далее укажите собственный пароль **root** и удалите анонимных пользователей:

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

Sett root password? [Y/n] y
New password: <задайте_пароль_root>
Re-enter new password: <повторите_пароль_root>
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!
```

Запретите удаленный вход для **root**, если необходимо:

```
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
```

Удалите тестовую базу данных и обновите таблицу привилегий:

```
By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Настройка базы данных MYSQL

Создайте базу данных и пользователя, которые будут использованы для дальнейшей работы. Для подключения к базе используйте команду **mysql**:

```
mysql -u root -p
Enter password: <пароль_root>

> create database zabbix character set utf8 collate utf8_bin;
> grant all privileges on zabbix.* to zabbix@localhost identified by 'zabpassword';
> quit;
```

Создается база данных в **/var/lib/mysql/zabbix**, где:

- **пароль_root** - пароль пользователя **root mysql**, это **НЕ системный root**;
- **zabpassword** - пароль пользователя **zabbix**, у которого полный доступ к базе **mysql zabbix**.

2. Импортируйте схему базы данных и начальные данные.

Импортируйте содержимое SQL-дампа в базу данных следующим образом:

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -pzabpassword zabbix
```

3. После этого отредактируйте файл конфигурации сервера **zabbix**. Пропишите данные для подключения к базе данных:

```
nano /etc/zabbix/zabbix_server.conf
```

Измените строки (их нужно раскоментировать, если они закоментированы, и присвоить нужные значения, если их нет или они отличаются):

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabpassword
```

4. Также необходимо отредактировать файл:

```
nano /etc/php.ini
```

Приведите параметры к следующему виду (аналогичные параметры есть в **/etc/httpd/conf.d/zabbix.conf** - они должны соответствовать):

```
date.timezone = Europe/Moscow      # обязательно укажите свой часовой пояс!
post_max_size = 16M
max_execution_time = 300
max_input_time = 300
```

5. Запустите **zabbix** и **httpd**:

```
systemctl restart httpd
systemctl restart zabbix-server
```

Произведите проверку логов на предмет ошибок:

```
cat /var/log/zabbix/zabbix_server.log
```

Запуск процесса zabbix-сервера

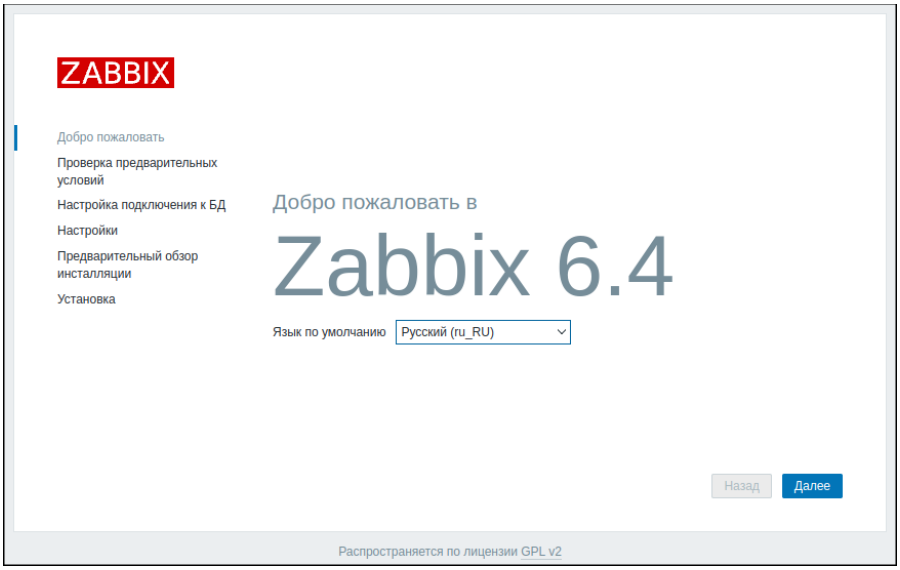
Запустите **zabbix**-сервер и добавьте его в автозагрузку:

```
systemctl restart zabbix-server
systemctl enable zabbix-server
systemctl restart zabbix-agent
systemctl enable zabbix-agent
systemctl restart httpd
```

Настройка из веб-интерфейса

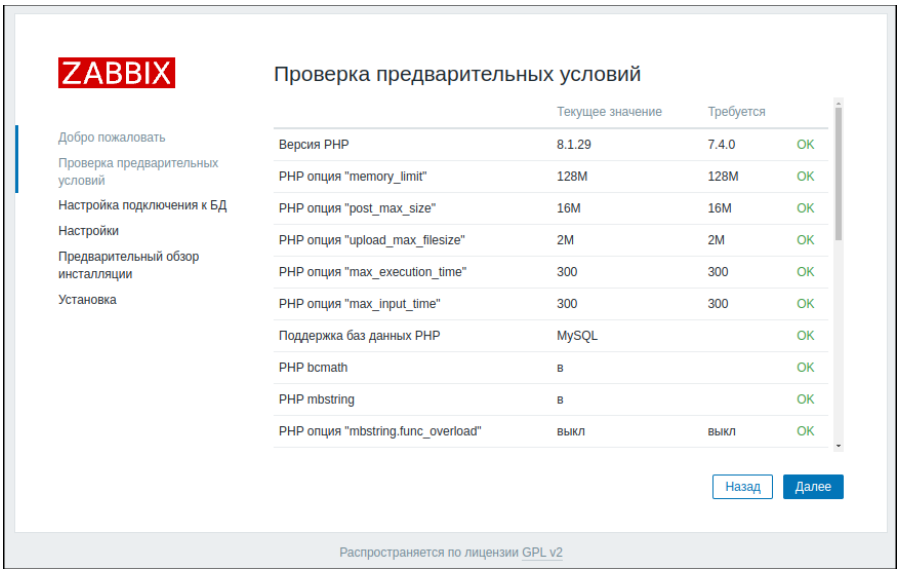
- Для того чтобы войти в веб-интерфейс, укажите в адресной строке браузера **http://<IP-адрес_сервера>/zabbix**.

Откроется страница приветствия.



Выберете язык и нажмите «**Далее**».

- Далее вы попадете на страницу преднастроек. Если вы ранее указали временную зону, то во всех пунктах должно быть « **OK**».



Нажмите «**Далее**».

- Укажите данные для подключения к ранее созданной базе данных.

В поле:

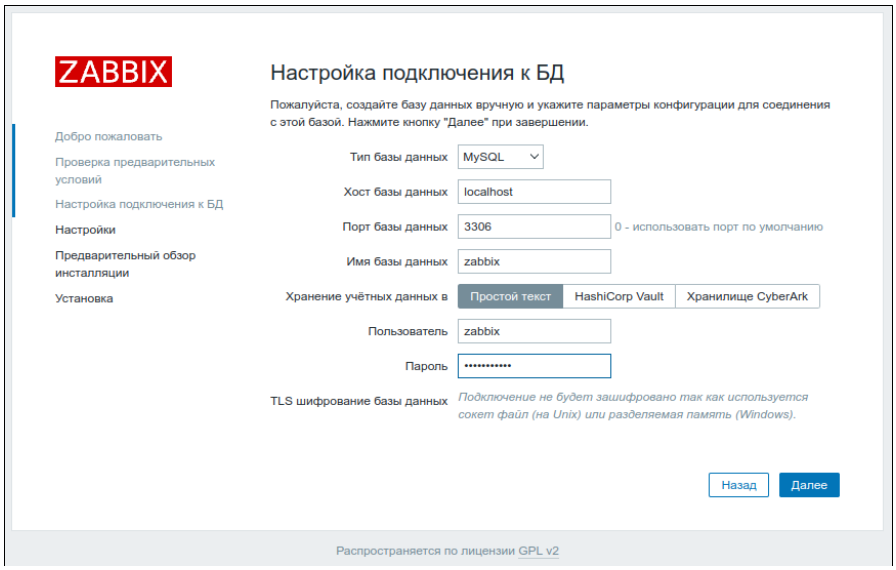
Database host — укажите адрес сервера **127.0.0.1** или **localhost**;

Database port — стандартный порт **MYSQL** (**3306**);

Database name — имя базы данных **zabbix**;

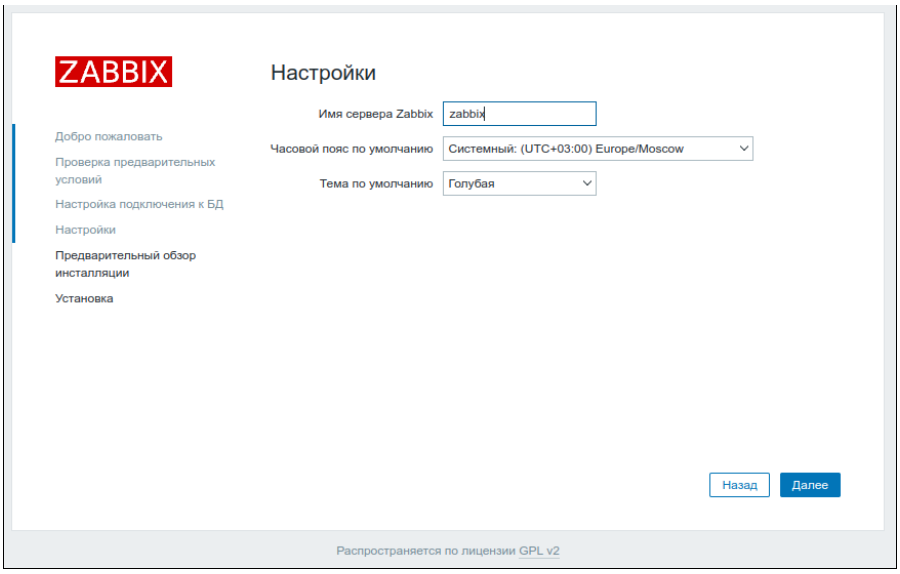
User — логин пользователя **zabbix**;

Password — пароль пользователя **zabpassword**.

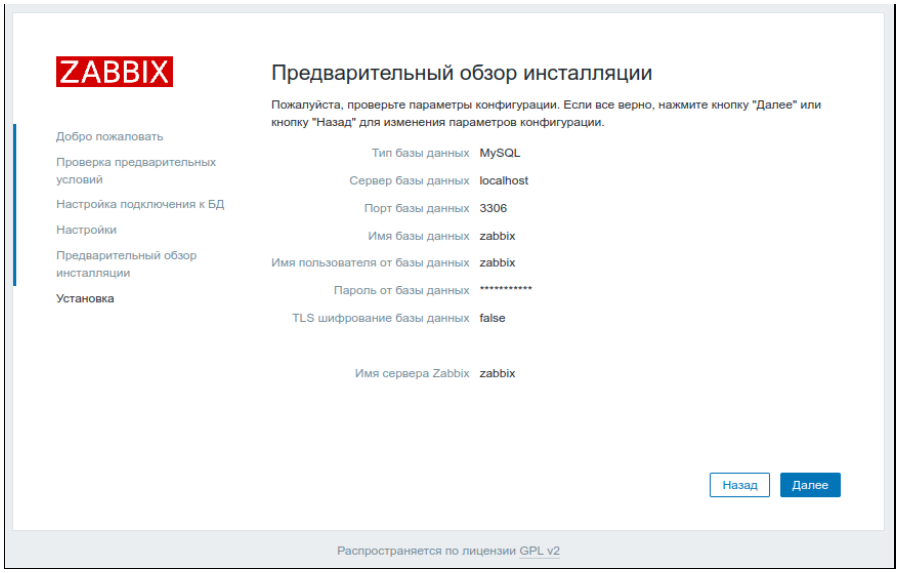


Нажмите «**Далее**». При неправильно указанных данных или неправильной конфигурации базы данных появится сообщение об ошибке подключения к базе.

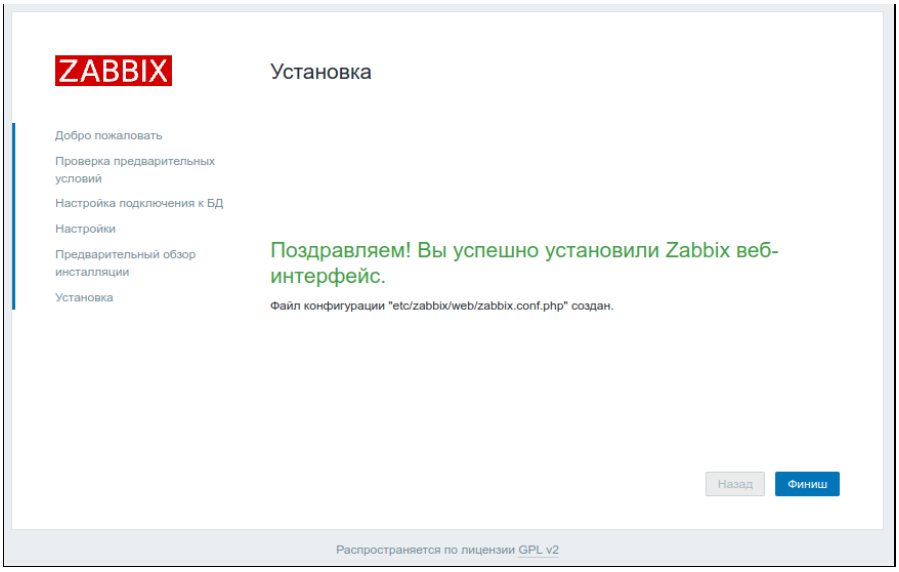
- В следующем окне нужно ввести имя сервера **zabbix** и проверить часовой пояс. Для продолжения нажмите «**Далее**».



- Проверьте правильность введенных данных и нажмите «**Далее**».

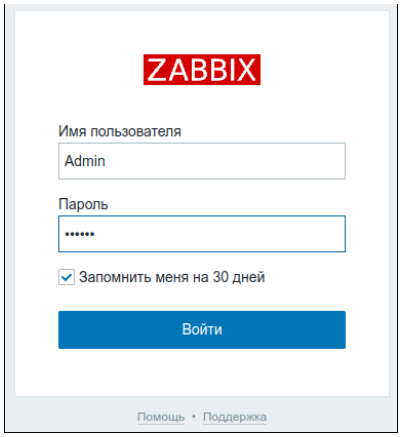


- При успешном окончании установки вы увидите следующую страницу.



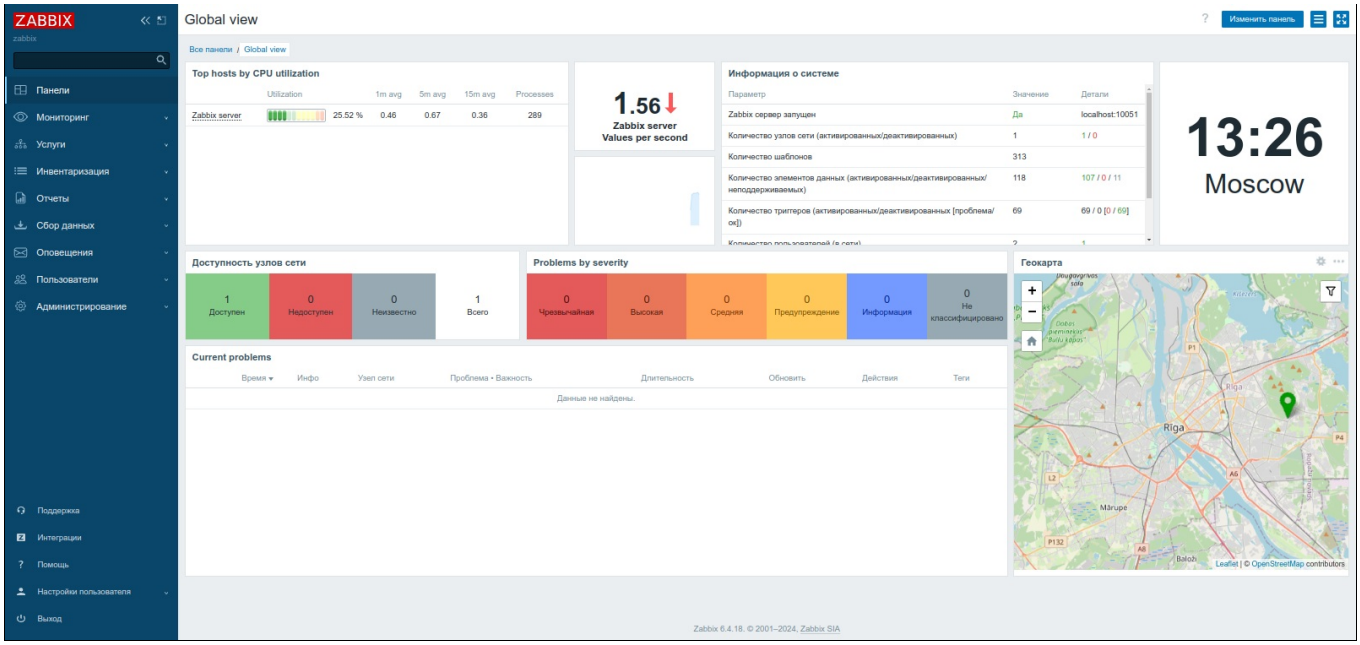
Нажмите «**Финиш**».

- Введите логин и пароль сервера **zabbix**. По умолчанию имя пользователя - **Admin** (регистр важен), пароль - **zabbix**.



Нажмите «**Войти**».

Вы попадете в панель управления. На этом настройка **zabbix** на **MYSQL** завершена.



Настройка агента zabbix

Настройка zabbix-agent
Добавление zabbix-agent

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** zabbix-agent-1:6.4.18-2

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. **Zabbix** использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления практически для любого события и быстро реагировать на проблемы с серверами. **Zabbix** предлагает отличные функции отчетности и визуализации данных, основанные на данных истории. Это делает **zabbix** идеальным для планирования мощности и мониторинга состояния серверов.

Zabbix разделяется на два вида: **zabbix-agent** и **zabbix-server**.

Zabbix-server собирает данные со всех клиентов, обрабатывает их, выводя на экран в веб-интерфейсе, и рассылает уведомления.

Zabbix-agent установлен на серверах, с которых необходимо собирать информацию об их состоянии, таких агентов может быть множество.

Настройка zabbix-agent

На сервере, который необходимо отслеживать, выполните следующие действия:

1. Установите **zabbix-agent**:

```
dnf install zabbix-agent
```

2. Настройте файл конфигурации:

```
nano /etc/zabbix/zabbix_agentd.conf
```

По умолчанию достаточно просто прописать IP-адрес сервера мониторинга:

```
Server=<ip-адрес_сервера>
```

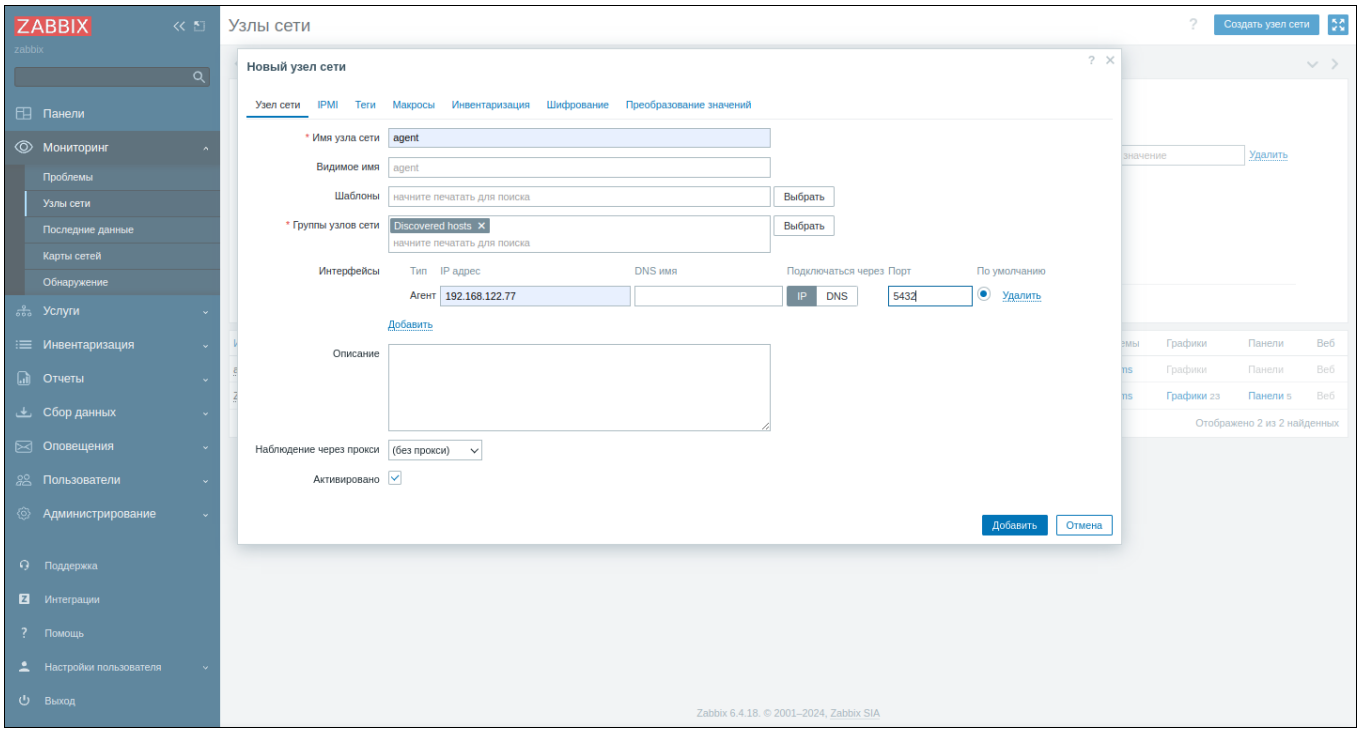
3. Запустите сервис и добавьте его в автозапуск:

```
systemctl enable zabbix-agent
systemctl start zabbix-agent
systemctl status zabbix-agent
```

Добавление zabbix-agent

В веб-интерфейсе **zabbix**-сервера добавьте новый узел в меню «**Мониторинг**» - «**Узлы сети**» - «**Создать узел сети**».

Далее впишите имя узла, укажите группу, в которой он должен состоять, для параметра «**Интерфейсы**» нажмите «**Добавить**», пропишите IP- или DNS-адрес узла и нажмите кнопку « **Добавить**».



На этом настройка **zabbix**-агента успешно завершена.

Более подробную информацию о **zabbix** можно найти на официальном сайте.

Настройка Prometheus с применением системы визуализации данных Grafana

Установка и настройка Prometheus на сервере
Установка экспортера на целевом (клиентском) сервере
Установка и настройка Grafana

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: grafana-11.2.4-1, golang-github-prometheus-2.49.1-1, prometheus-node_exporter-1.6.0-1

Prometheus — программное обеспечение с открытым исходным кодом, используемое для мониторинга различных систем (например, нагрузки на сервер). В **prometheus** происходит запись метрик в реальном времени в базу данных временных рядов.

Установка и настройка Prometheus на сервере

Для установки **prometheus** выполните команду:

```
dnf install golang-github-prometheus
```

Запустите **prometheus** и добавьте его в автозагрузку:

```
systemctl enable prometheus --now
```

Проверьте статус службы:

```
systemctl status prometheus
```

В статусе должно отображаться **active(running)**.

Мониторинг можно производить через веб-интерфейс, введя в адресную строку браузера http://**<IP-адрес_сервера>**:9090/graph.

Установка экспортера на целевом (клиентском) сервере

Экспортер — программное обеспечение (клиентская часть), задача которого заключается в экспорте информации о машине в формате, понятном **Prometheus**. Устанавливается и настраивается непосредственно на клиентском сервере.

Существует множество экспортеров для разных систем и сервисов. Большое количество экспортеров доступно на официальном сайте.

Установка node exporter из репозитория

В качестве примера будет рассмотрена настройка одного из самых популярных экспортеров — **Node Exporter**, который собирает множество системных метрик (процессор, память и т.д.) для оценки состояния сервера и его нагрузки. **Node Exporter** доступен в репозитории РЕД ОС.

Создайте пользователя **nodeusr**:

```
useradd -rs /bin/false nodeusr
```

Для установки экспортера выполните команду (потребуются права **администратора** системы):

```
sudo dnf install prometheus-node_exporter
```

Установка node exporter с внешнего ресурса

Однако не все из существующих экспортеров доступны для установки из репозитория РЕД ОС. Далее будет рассмотрен пример установки экспортера *node exporter* с официального сайта *Prometheus*. Согласно приведенному примеру можно устанавливать и другие экспортеры с официального сайта *Prometheus*.

Для установки экспортера скачайте последнюю версию программы на официальном сайте либо используйте команду:

```
wget https://github.com/prometheus/node_exporter/releases/download/v1.5.0/node_exporter-1.5.0.linux-amd64.tar.gz
```

Перейдите в каталог со скачанным архивом (в примере **/home/user/Загрузки**) и распакуйте его:

```
cd /home/user/Загрузки
tar -xvzf node_exporter-1.5.0.linux-amd64.tar.gz
```

Затем создайте пользователя **nodeusr**:

```
useradd -rs /bin/false nodeusr
```

Установите экспортер путем копирования:

```
mv node_exporter-1.5.0.linux-amd64/node_exporter /usr/bin/
```

Настройте политики безопасности SELinux:

```
restorecon -v /usr/bin/node_exporter
```

Настройка node exporter

Создайте службу для запуска:

```
nano /etc/systemd/system/node_exporter.service
```

со следующим содержимым:

```
[Unit]
Description=Node Exporter
After=network.target
[Service]
User=nodeusr
Group=nodeusr
Type=simple
ExecStart=/usr/bin/node_exporter
[Install]
WantedBy=multi-user.target
```

Запустите **node_exporter** и добавьте его в автозагрузку:

```
systemctl enable node_exporter --now
```

Проверьте статус службы:

```
systemctl status node_exporter
```

В статусе должно отображаться **active(running)**.

Для отображения метрик введите в адресную строку браузера http://**<IP-адрес_клиентского_сервера>**:9100/metrics.

На сервере откройте конфигурационный файл (необходимы права суперпользователя):

```
nano /etc/prometheus/prometheus.yml
```

и дополните секцию scrape_configs следующими строками:

```
  - job_name: 'node_1'
    static_configs:
      - targets: ['<IP-адрес_клиентского_сервера>:9100']
```

Для применения изменений перезапустите **prometheus**:

```
systemctl restart prometheus
```

> **Примечание.**
>
> Если после перезапуска **prometheus** в статусе отображается **failed**, необходимо проверить корректность заполнения файла конфигурации. Ошибки отображаются в журнале **/var/log/messages**.

Мониторинг можно производить через веб-интерфейс, указав в адресной строке браузера https://**<IP-адрес_сервера_Prometheus>**:9090/targets.

Установка и настройка Grafana

Grafana — платформа с открытым исходным кодом для визуализации, мониторинга и анализа данных. **Grafana** позволяет пользователям создавать дашборды с панелями, каждая из которых отображает определенные показатели в течение установленного периода времени. Каждый дашборд универсален, поэтому его можно настроить для конкретного проекта или с учетом любых потребностей разработки и/или бизнеса.

Установка Grafana

Для установки **Grafana** выполните команду:

```
dnf install grafana
```

Запустите **grafana-server** и добавьте его в автозагрузку:

```
systemctl enable grafana-server --now
```

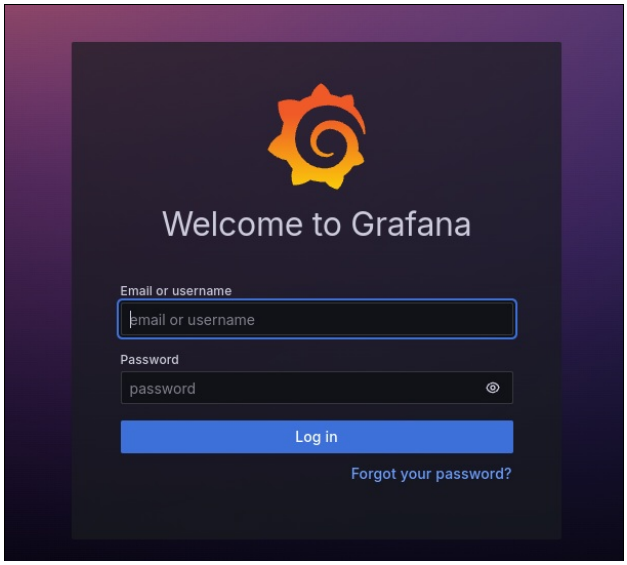
Проверьте статус сервера:

```
systemctl status grafana-server
```

В статусе должно отображаться **active(running)**.

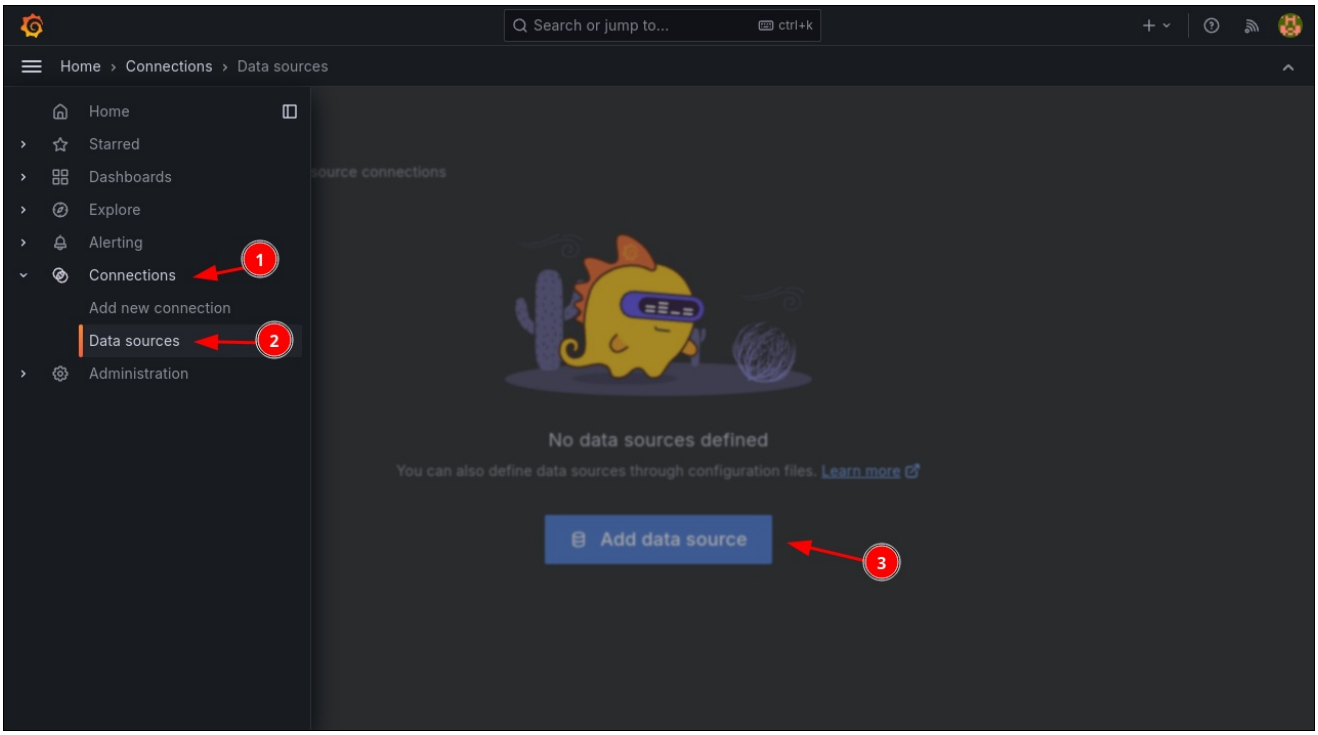
Настройка Grafana

Веб-интерфейс доступен по адресу http://**<IP-адрес_сервера>**:3000/.

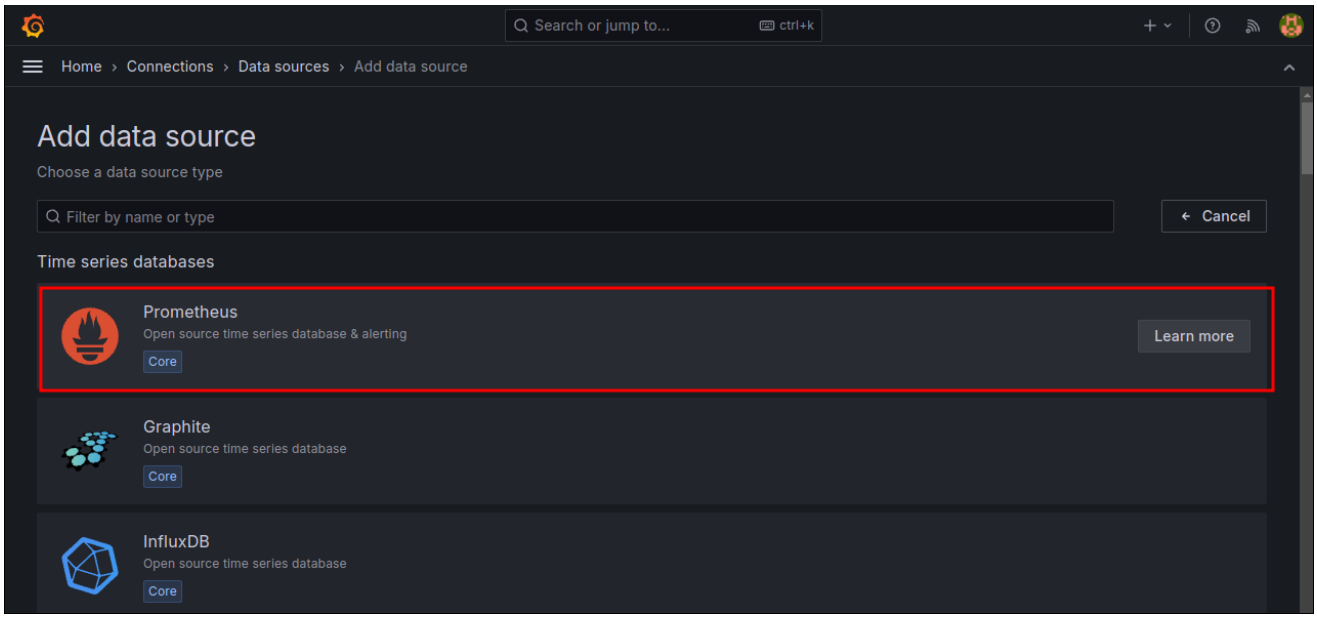


Логин и пароль для входа: **admin**/**admin**. При первом входе будет запрошена смена пароля.

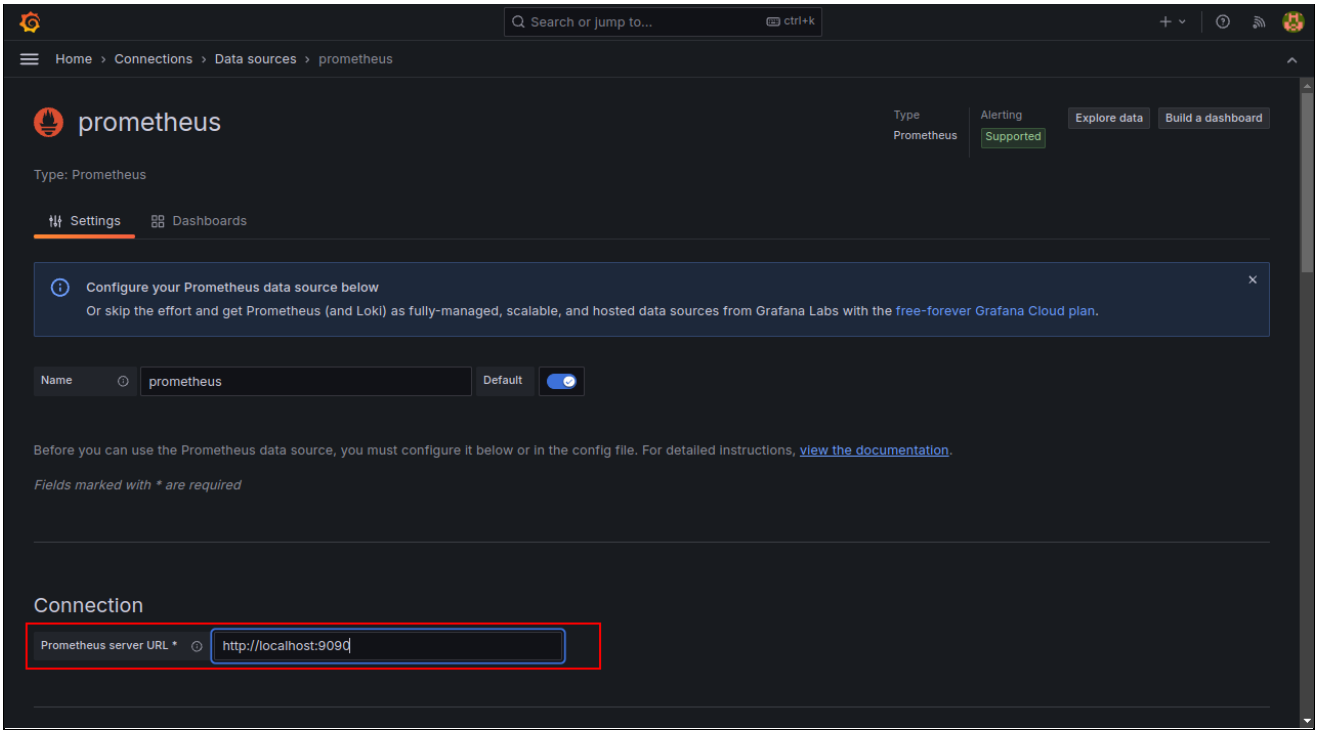
Далее добавьте источник данных для **Grafana**, выбрав **Home** - **Connections** - **Data Sources** - **Add data source**.

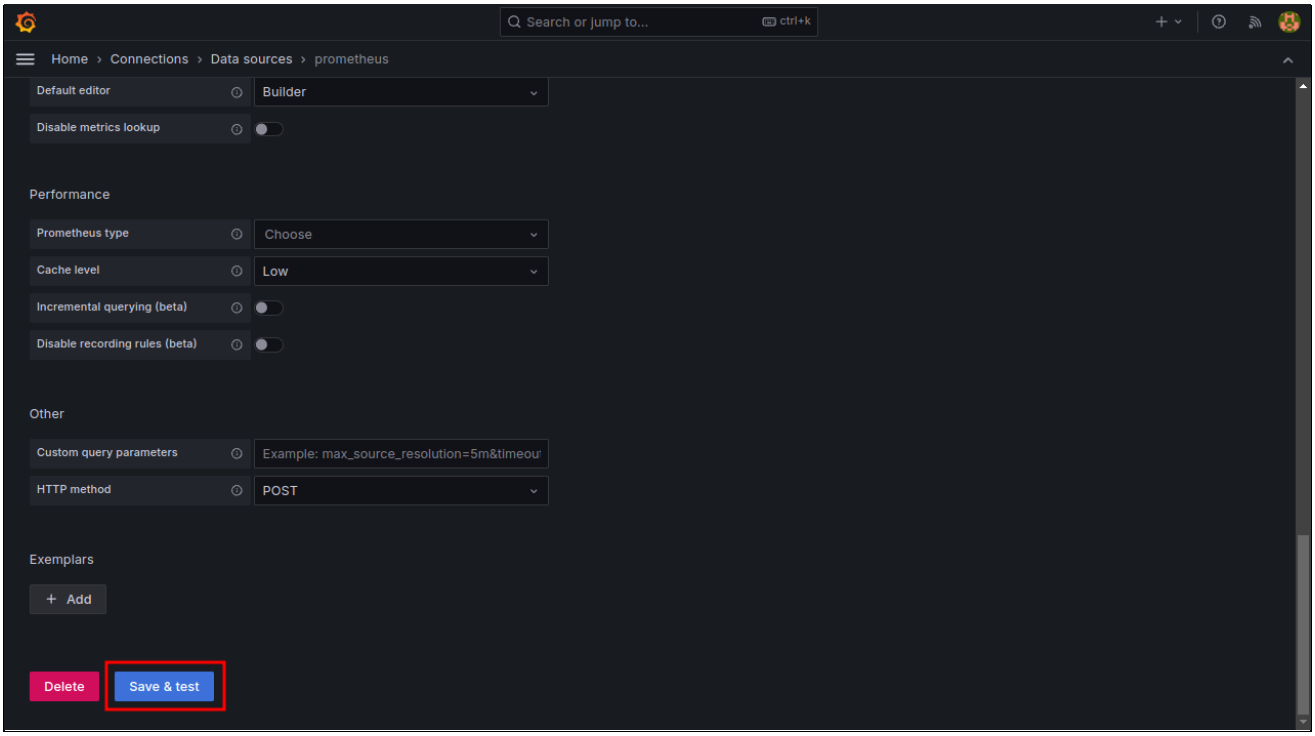


Выберите из списка **Prometheus**, кликнув по нему ЛКМ.



В настройках укажите *IP-адрес* и *порт* сервера с **Prometheus**, остальные настройки ситуативны и устанавливаются по желанию. Для сохранения настроек нажмите **Save & Test**.





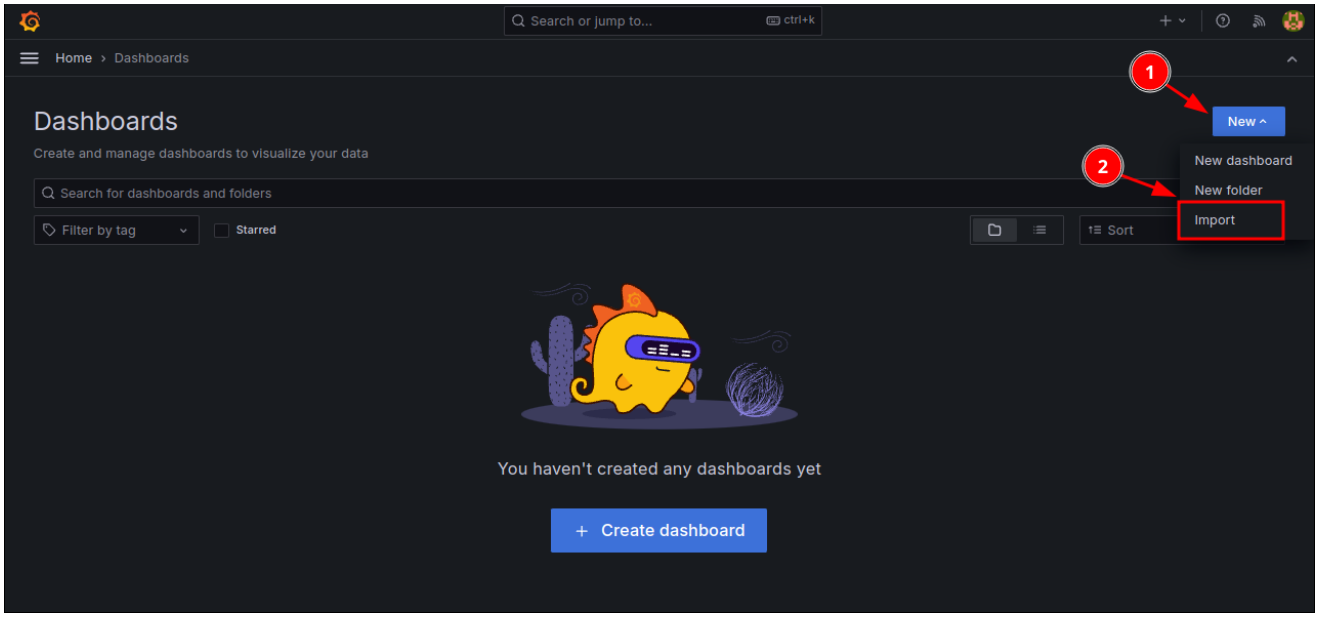
Загрузка дашбордов

Существует множество готовых дашбордов (в формате JSON), которые можно импортировать. Например, *id=9614* или *id=13978*. Наиболее универсальным является *id=1860*, его можно скачать по ссылке (в примере использована *ревизия 27*).

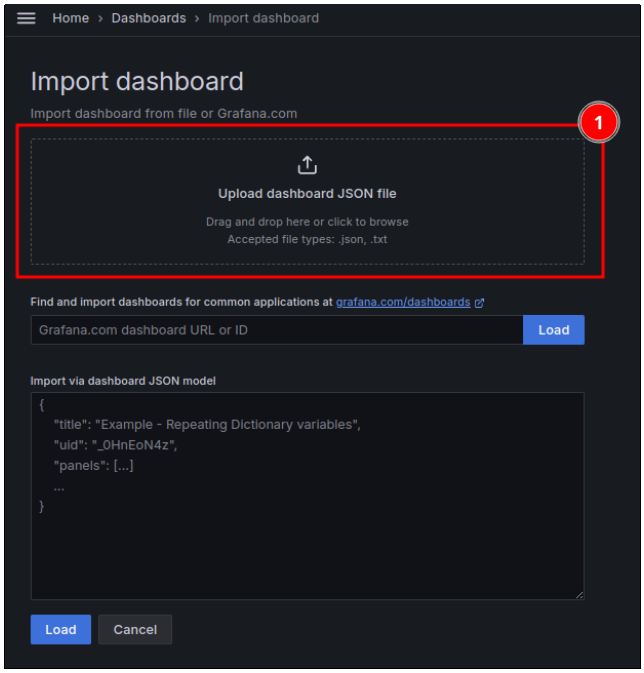
Примечание.

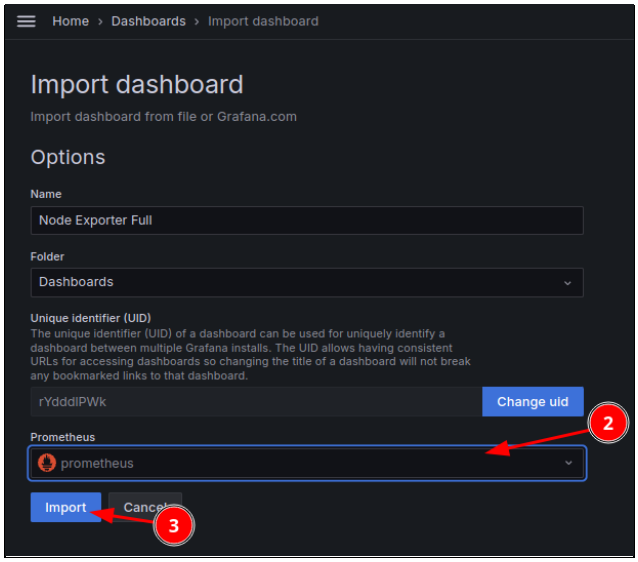
Для указанных в *Окружении* версий **Prometheus** и **Grafana** могут быть использованы дашборды с **ревизией 27 и ниже**. В случае использования *ревизий 28 и выше* при работе могут возникнуть ошибки.

Для импорта дашборда выберите **Home** - **Dashboards** и нажмите **New** - **Import**.

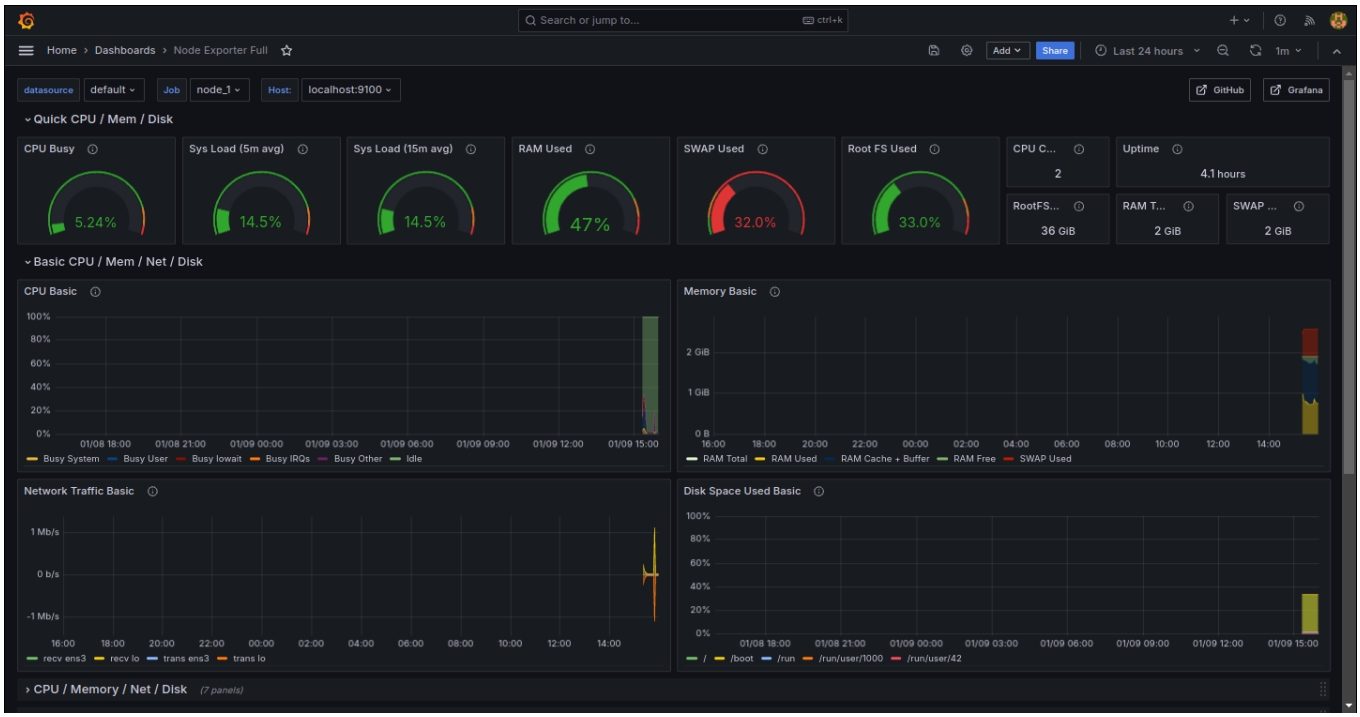


Далее, нажав **Upload dashboard JSON file**, выберите скачанный раннее JSON-файл. В появившемся окне **Options** выберите **Prometheus** и нажмите **Import**.





Загруженный *дашборд 1860* выглядит следующим образом:



Каталог с данными **prometheus** располагается по пути **/var/lib/prometheus**.

Настройка GLPI-сервера (для инвентаризации оборудования)

Установка GLPI
Настройка glpiinventory plugin на сервере
Настройка glpi-agent на клиенте
Установка дополнительных плагинов
Первичная настройка GLPI
Основные разделы GLPI. Заявки
Основные разделы GLPI. Уведомления
Основные разделы GLPI. Интерфейс
Основные разделы GLPI. Автоматические действия
Основные разделы GLPI. SLA
Основные разделы GLPI. Автоматическое назначение заявок
Основные разделы GLPI. Отчет

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** glpi-9.5.7-3

Gestionnaire libre de parc informatique (**GLPI**) - свободный менеджер ИТ-инфраструктуры - является системой работы с заявками и инцидентами, а также используется для инвентаризации компьютерного оборудования (компьютеры, программное обеспечение, принтеры и т.д.). Имеет расширенные функции, такие как работа системы отслеживания почты с уведомлением, методы для создания базы данных с основной информацией о топологии сети и т.д. *GLPI* - это веб-приложение, разрабатывающееся на PHP.

GLPI включает следующие возможности:

- инвентаризация компьютеров, периферийного оборудования, сетевых принтеров и связанных компонентов через интерфейс с OCS Inventory или FusionInventory;
- управление заявками и инцидентами;
- управление лицензиями, договорами (по стандарту ITIL);
- связывание пользователей и групп по географическому положению;
- управление деловой и финансовой информацией (договоры);
- управление статусом объектов;
- поддержка базы знаний и часто задаваемых вопросов (FAQ);
- генераторы отчетов;
- поддержка базы данных MySQL/MariaDB;
- поддержка UTF8;
- система оповещения о событиях.

GLPI позволяет увеличивать функциональность с помощью подключения плагинов.

Установка GLPI

Для установки необходимых пакетов откройте консоль и воспользуйтесь следующей командой (обратите внимание, что команды выполняются с правами администратора):

```
dnf install glpi mariadb mariadb-server php-pear-CAS php-ldap php-opcache php-apcu php-xmlrpc php-zip php-sodium
```

Выполните команду переразметки SELinux:

```
touch /.autorelabel
```

Инициализация БД – запомните пароль, создающийся для root-пользователя БД. На вопросы по умолчанию отвечайте «**Y**».

```
systemctl enable --now mariadb
```

```
/usr/bin/mysql_secure_installation
```

```
 mysql -u root -p
```

```
CREATE USER 'glpi'@'%' IDENTIFIED BY 'glpiDBSecret';
```

```
GRANT USAGE ON *.* TO 'glpi'@'%' IDENTIFIED BY 'glpiDBSecret';
CREATE     DATABASE IF NOT EXISTS `glpi` ;
GRANT ALL PRIVILEGES ON `glpi`.* TO 'glpi'@'%';
FLUSH PRIVILEGES;
EXIT
```

Проверка соединения с БД осуществляется командой:

```
mysql -uglpi -pglpiDBSecret glpi
```

```
exit
```

Далее запустите веб-сервис командой:

```
systemctl enable --now httpd
```

В файл конфигурации **/etc/httpd/conf/httpd.conf** добавьте строку:

```
Timeout 600
```

Перезапустите службу веб-сервиса для применения изменений:

```
systemctl restart httpd
```

Назначьте права на директорию:

```
chown -R apache /usr/share/glpi
```

Настройка SELinux

SELinux должен находиться в режиме **Enforcing**, если SELinux установлен в какой-либо другой режим работы, необходимо самостоятельно перевести его, выполнив команду:

```
nano /etc/selinux/config
```

Затем привести строку с установленным режимом к виду:

```
SELINUX=enforcing
```

Выполните команды:

```
setenforce 1
setsebool -P httpd_can_network_connect on
setsebool -P httpd_can_network_connect_db on
setsebool -P httpd_can_sendmail on
setsebool -P httpd_unified 1
setsebool -P httpd_read_user_content 1
```

Для настройки входа по IP-адресу выполните команду:

```
nano /etc/httpd/conf.d/glpi.conf
```

Добавьте в секцию **Require** ваш ip-адрес – в качестве примера «**192.168.1.56**»:

```
<IfModule mod_authz_core.c>
 # Apache 2.4
 Require local
 Require ip 192.168.1.56
 </IfModule>
```

Затем следует выполнить настройку защищенности файлов. Добавьте секцию:

```
<Directory /usr/share/glpi/files>
  <IfModule mod_authz_core.c>
```

```
Require all denied
</IfModule>
<IfModule !mod_authz_core.c>
deny from all
</IfModule>
</Directory>
```

+ Пример итогового конфигурационного файла:

```
Alias /glpi /usr/share/glpi
 <Directory /usr/share/glpi>
 Options None
 AllowOverride Limit Options FileInfo
 <IfModule mod_authz_core.c>
 Require local
 Require ip 192.168.1.56
 </IfModule>
 <IfModule !mod_authz_core.c>
 Order deny,allow
 Allow from all
 </IfModule>
 </Directory>
 <Directory /usr/share/glpi/install>
 <IfModule mod_authz_core.c>
 Require local
 </IfModule>
 <IfModule !mod_authz_core.c>
 Order Deny,Allow
 Deny from All
 Allow from 127.0.0.1
 Allow from ::1
 </IfModule>
 <IfModule mod_php5.c><
 php_value max_execution_time 0
 php_value memory_limit -1
 </IfModule>
 <IfModule mod_php7.c>
 php_value max_execution_time 0
 php_value memory_limit -1
 </IfModule>
 </Directory>
 <Directory /usr/share/glpi/config>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/locales>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/install/mysql>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/scripts>
 Order Allow,Deny
 Deny from all
 </Directory>
 <Directory /usr/share/glpi/files>
```

```
<IfModule mod_authz_core.c>
Require all denied
</IfModule>
<IfModule !mod_authz_core.c>
deny from all
</IfModule>
</Directory>
```

Перезапустите сервис для применения внесенных изменений:

```
systemctl restart httpd
```

Для обновления меток selinux необходимо перезагрузить ПК.

Вход через браузер будет производиться по адресу:

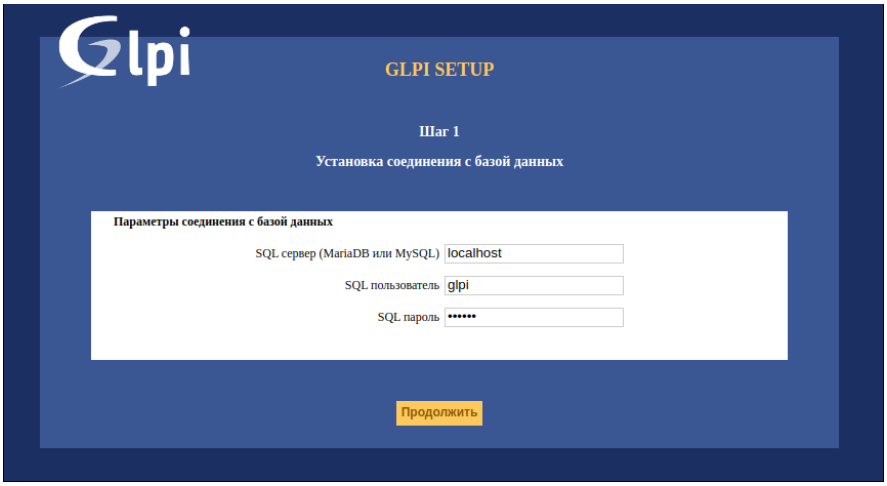
```
http://192.168.1.56/glpi/install/install.php
```

Статусы проверки должны быть успешными:

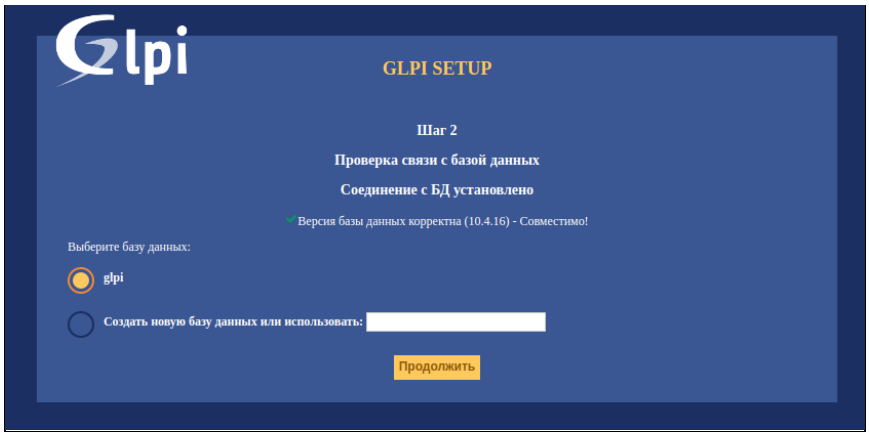


Настройка соединения с БД – требуется пароль, созданный для root-пользователя БД:

```
IP - 127.0.0.1
user - glpi
pass – {пароль glpi-пользователя БД}
```



Выберите Базу Данных GLPI:



После завершения установки вход в веб-форму администратора осуществляется по данным:

```
user - glpi
pass - glpi
```



Настройка glpiinventory plugin на сервере

Установите пакет:

```
dnf install glpi-plugin-glpiinventory
```

В браузере перейдите по ссылке:

```
http://192.168.1.56/glpi/front/plugin.php
```

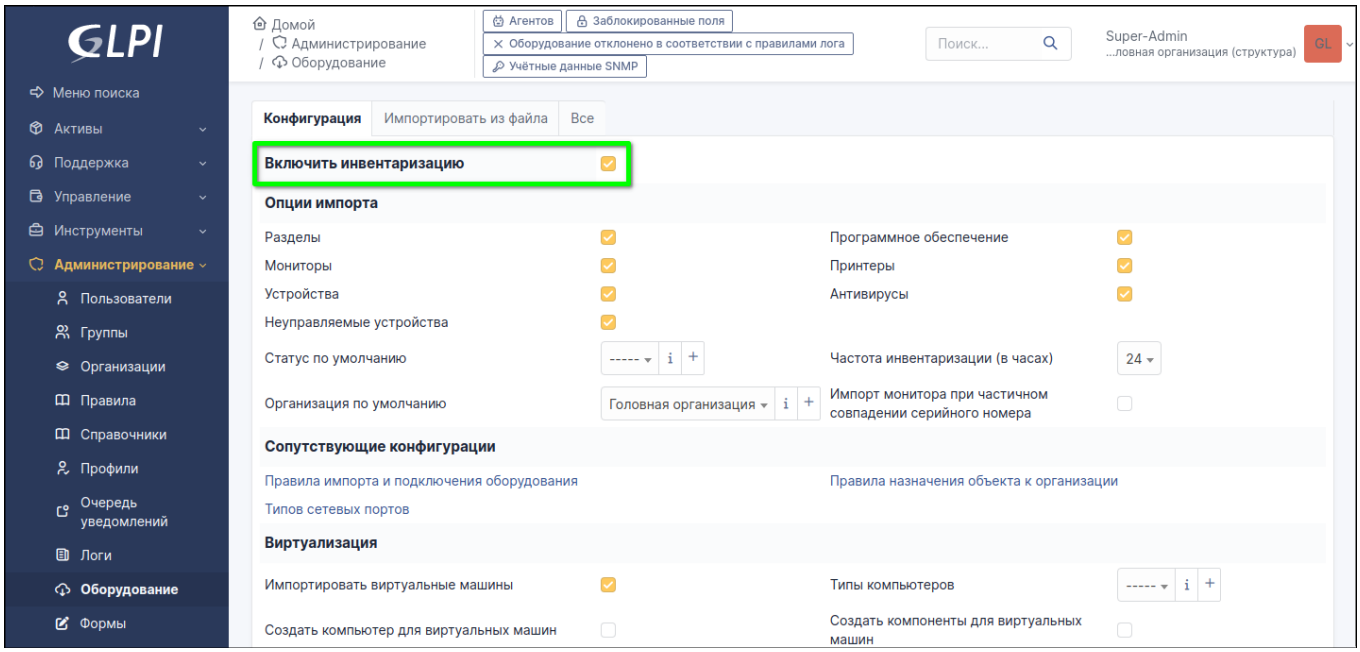
В списке плагинов должен отобразиться **GLPI Inverntory**, нажмите на иконку «**Установить**».



После этого плагин можно будет активировать.

Перейдите в пункт меню «**Администрирование**» — «**Оборудование**» либо по адресу: http://192.168.1.56/glpi/front/inventory.conf.php.

Включите инвентаризацию и сохраните изменения.



Настройка glpi-agent на клиенте

На клиентской машине установите пакет:

```
dnf install glpi-agent
```

Измените конфигурационный файл:

```
nano /etc/glpi-agent/agent.cfg
```

Впишите IP-сервера в строку, предварительно раскомментировав ее:

```
server = http://192.168.1.56/glpi/plugins/glpiinventory/
```

Выполните запуск службы:

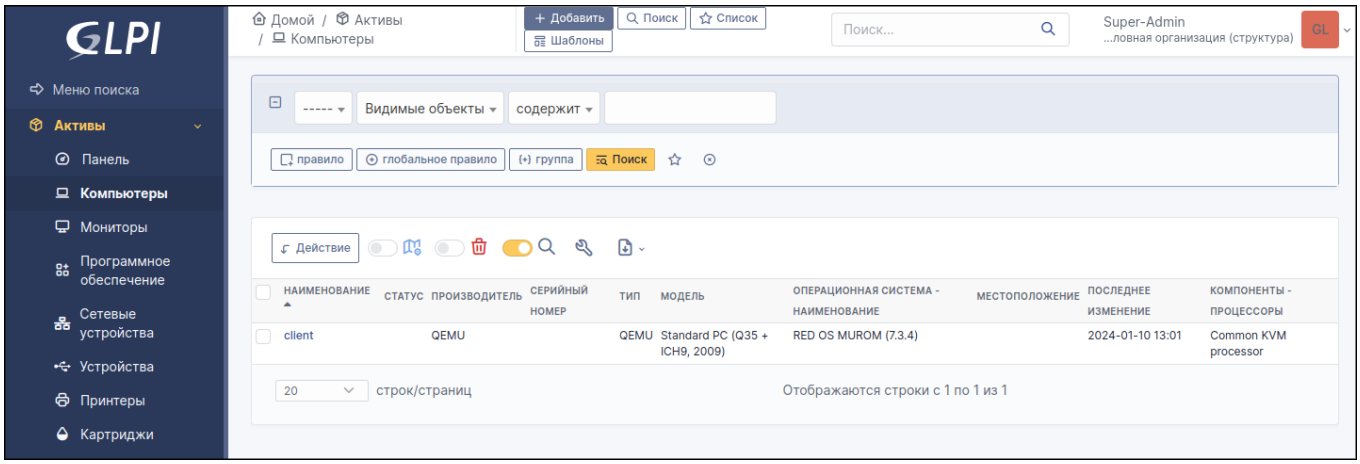
```
systemctl enable --now glpi-agent.service
```

По умолчанию инвентаризация будет запущена *через 1 час* после запуска службы. Этот параметр можно изменить, указав необходимое значение в секундах в строке delaytime в конфигурационном файле **/etc/glpi-agent/agent.cfg**.

Для ручного запуска инвентаризации на клиенте можно использовать команду:

```
glpi-agent -f --conf-file=/etc/glpi-agent/agent.cfg --daemon
```

После выполнения вышеперечисленных действий на сервере появится информация о ПК-клиенте:



Установка дополнительных плагинов

Список доступных плагинов в репозитории РЕД ОС можно получить, выполнив команду:

```
dnf search glpi-plugin
```

Для установки плагина необходимо выполнить команду вида:

```
dnf install glpi-plugin-<имя_плагина>
```

После установки пакета плагин будет отображаться в меню «**Настройки**» — «**Плагины**» веб-интерфейса сервера, где его можно будет установить и включить.

Первичная настройка GLPI

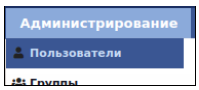
Удаление файла автонастройки install.php

После установки GLPI на главной странице появится уведомление о том, что надо удалить из корневой папки файл автонастройки **install/install.php**, удалите его командой:

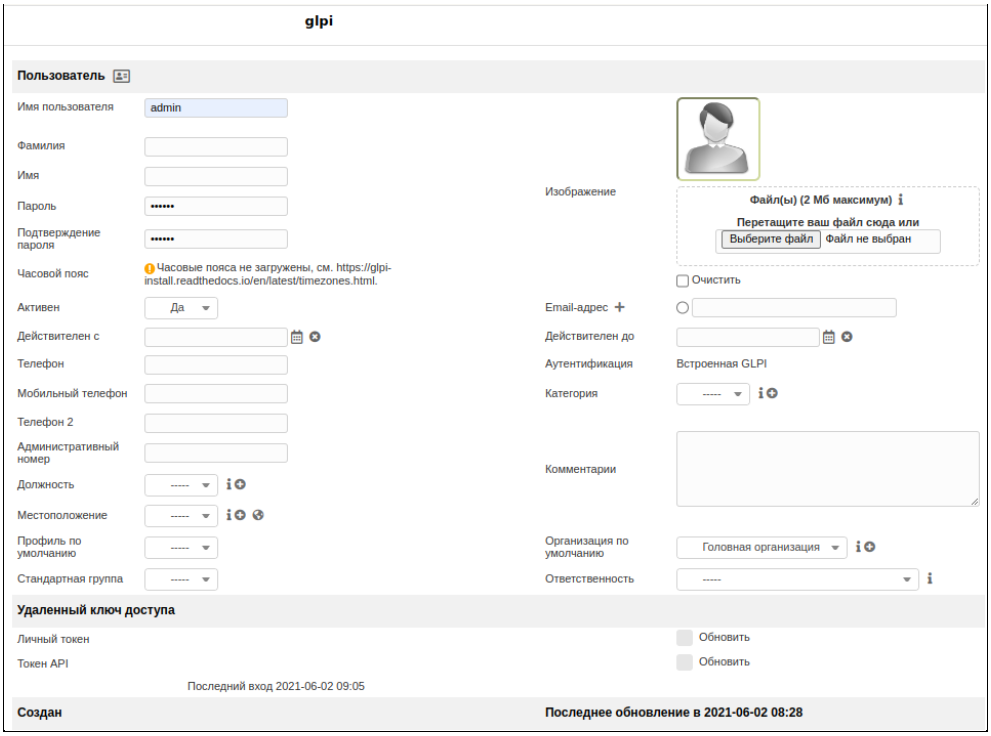
```
rm /usr/share/glpi/install/install.php
```

Переименовывание базовых пользователей

После завершения установки система автоматически создаст 4 учетных записи с паролем и логином по умолчанию. После входа в систему данные учетные записи нужно будет переименовать и сменить на них пароли. Для смены паролей необходимо перейти в *«Администрирование» -> «Пользователи»*:



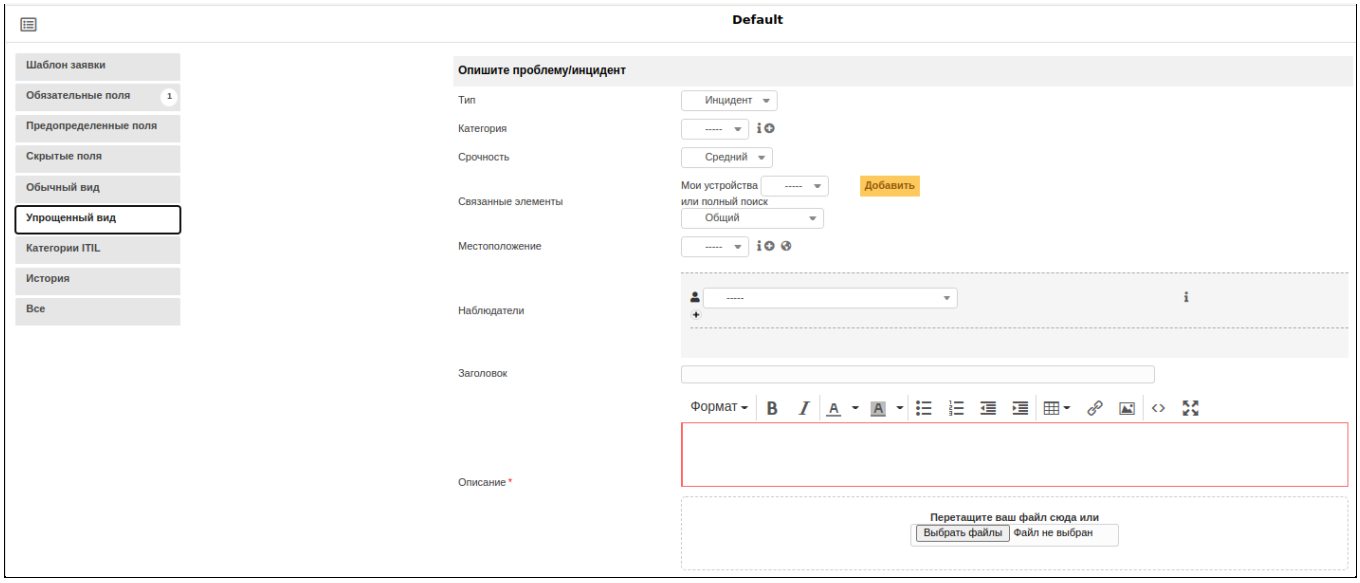
Переходим в настройки нужного пользователя и меняем необходимые данные:



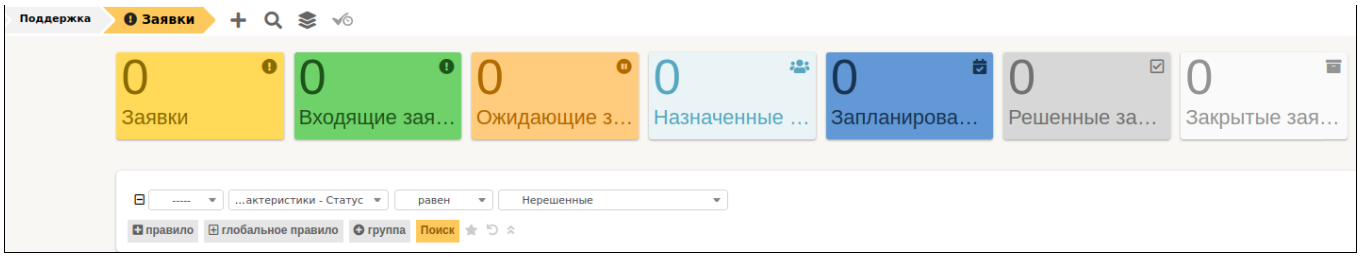
Основные разделы GLPI

Заявки

Для настройки заявок необходимо перейти в *«Поддержка» -> «Заявки» -> «Управление шаблонами»* (две горизонтальные линии с разрывом). Выбираем шаблон для настройки, в левой части находятся параметры данного шаблона:

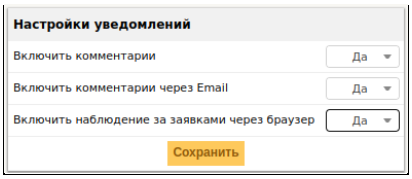


При переходе в меню заявок можно просмотреть список доступных заявок, создать собственную заявку или отсортировать список заявок:



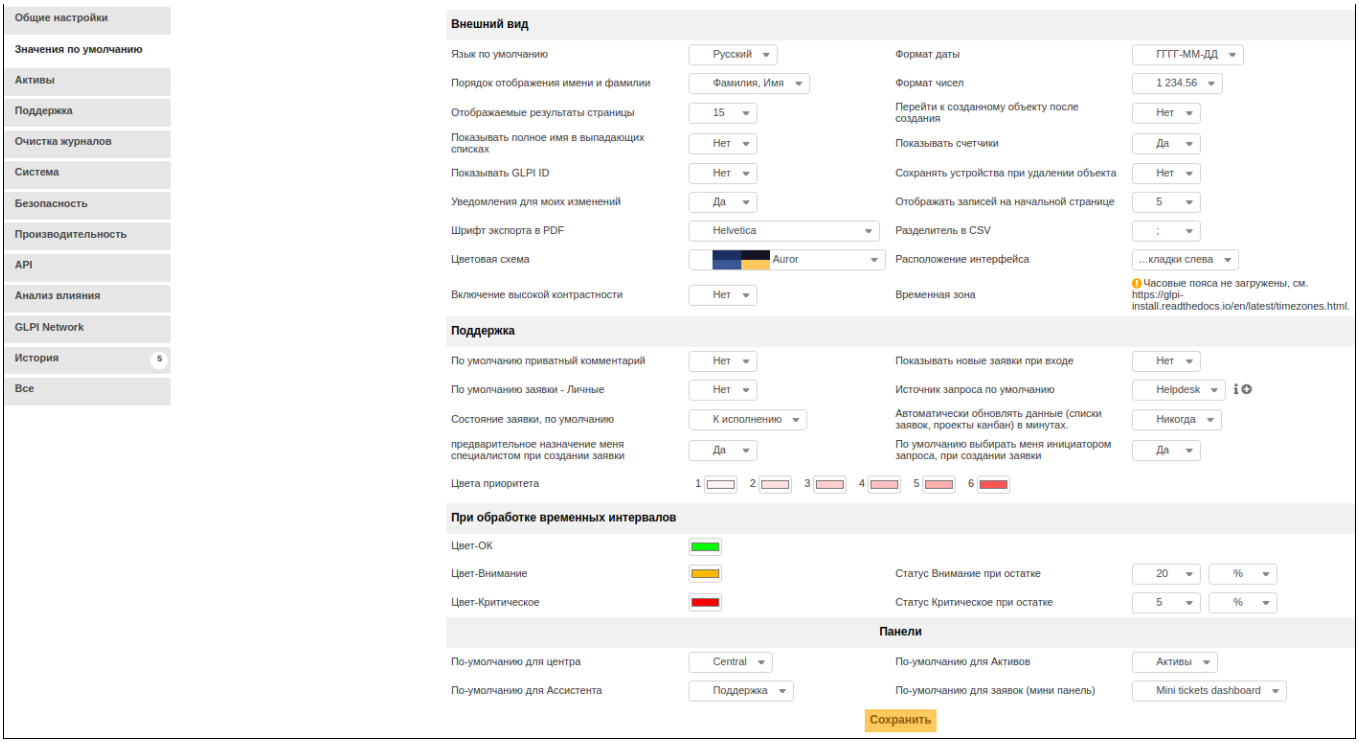
Уведомления

Для настройки уведомлений перейдите в *«Настройки» -> «Уведомления»* и включите уведомления о комментариях, уведомлениях по *e-mail* и браузерные оповещения:



Интерфейс

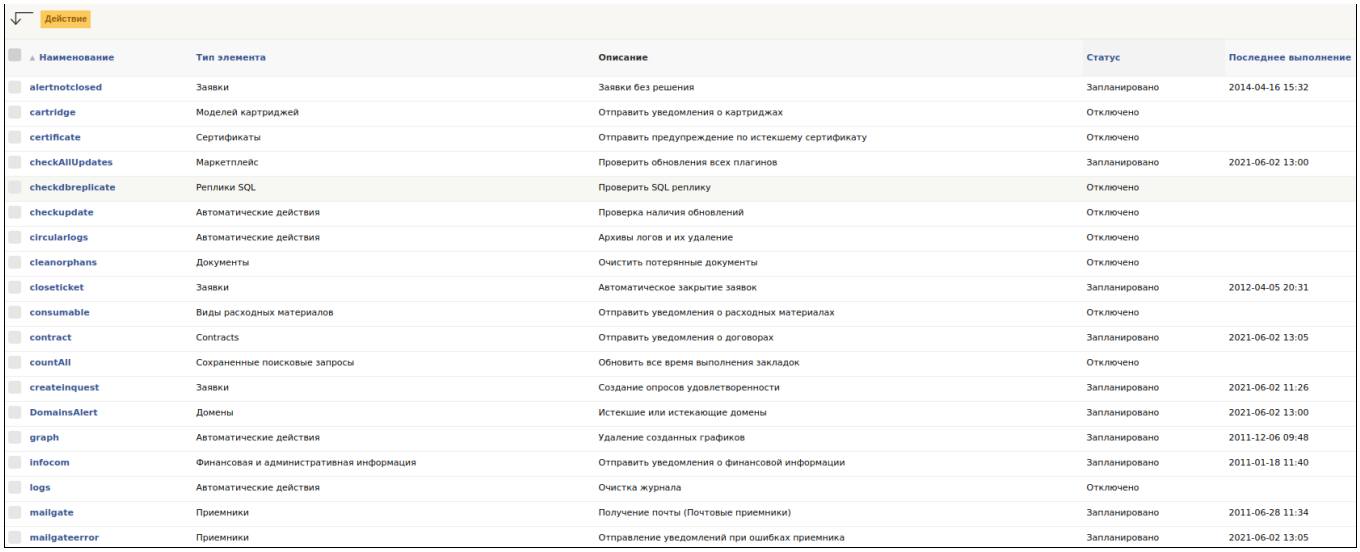
В GLPI есть несколько способов настроить отображаемый внешний вид вкладок и интерфейс. Для настройки первым способом перейдите в *«Настройки» -> «Общий» -> «Значения по умолчанию»*:



В открывшейся вкладке можно настроить интерфейс как вам удобно. Для настройки вторым способом (для конкретного пользователя) перейдите по имени профиля в правом верхнем углу -> *«Внешний вид»*.

Автоматические действия

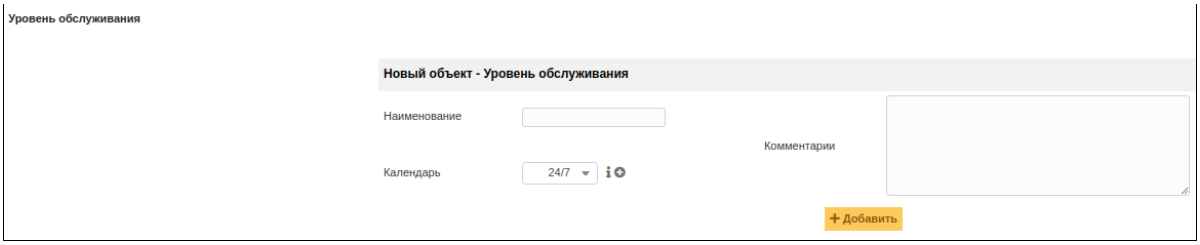
В GLPI имеется возможность запускать автоматически выполняемые команды. Для этого перейдите в *«Настройки» -> «Автоматические действия»*. С помощью действий можно настроить автоматическую отправку уведомлений, очистку журнала, закрытие заявок и т.д. Для данных команд можно настроить время запуска или при необходимости запустить вручную.



Наименование	Тип элемента	Описание	Статус	Последнее выполнение
alertnotclosed	Заявки	Заявки без решения	Запланировано	2014-04-16 15:32
cartridge	Моделей картриджей	Отправить уведомления о картриджах	Отключено	
certificate	Сертификаты	Отправить предупреждение по истекшему сертификату	Отключено	
checkAllUpdates	Маркетплейс	Проверить обновления всех плагинов	Запланировано	2021-06-02 13:00
checkdbreplicate	Реплики SQL	Проверить SQL реплику	Отключено	
checkupdate	Автоматические действия	Проверка наличия обновлений	Отключено	
circularlogs	Автоматические действия	Архивы логов и их удаление	Отключено	
cleanorphans	Документы	Очистить потерянные документы	Отключено	
closeticket	Заявки	Автоматическое закрытие заявок	Запланировано	2012-04-05 20:31
consumable	Виды расходных материалов	Отправить уведомления о расходных материалах	Отключено	
contract	Contracts	Отправить уведомления о договорах	Запланировано	2021-06-02 13:05
countAll	Сохраненные поисковые запросы	Обновить все время выполнения закладок	Отключено	
createinquest	Заявки	Создание опросов удовлетворенности	Запланировано	2021-06-02 11:26
DomainsAlert	Домены	Истекшие или истекающие домены	Запланировано	2021-06-02 13:00
graph	Автоматические действия	Удаление созданных графиков	Запланировано	2011-12-06 09:48
infocom	Финансовая и административная информация	Отправить уведомления о финансовой информации	Запланировано	2011-01-18 11:40
logs	Автоматические действия	Очистка журнала	Отключено	
mailgate	Приемники	Получение почты (Почтовые приемники)	Запланировано	2011-06-28 11:34
mailgateerror	Приемники	Отправление уведомлений при ошибках приемника	Запланировано	2021-06-02 13:05

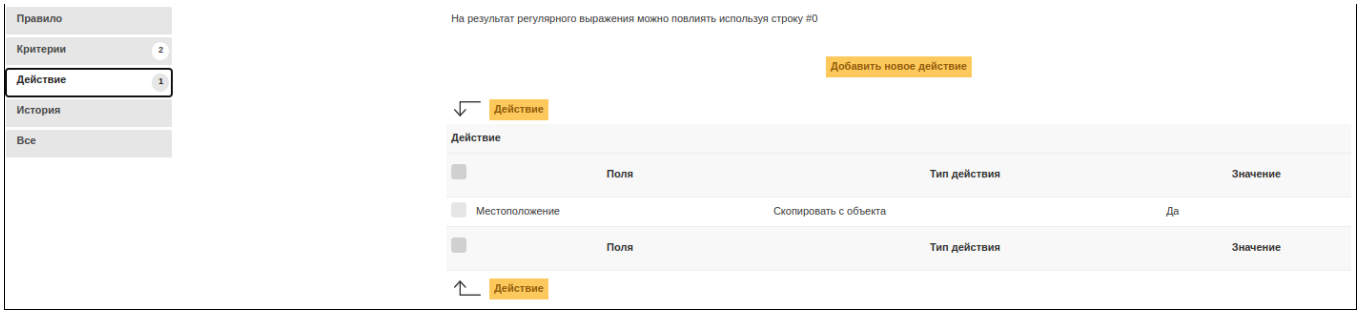
SLA

В GLPI имеется возможность добавления уровней обслуживания (SLA). Для этого перейдите в *«Настройки» -> «Уровни обслуживания»*, в открывшемся списке можно отсортировать имеющиеся уровни или добавить новый уровень, нажав на плюс в левой части панели:



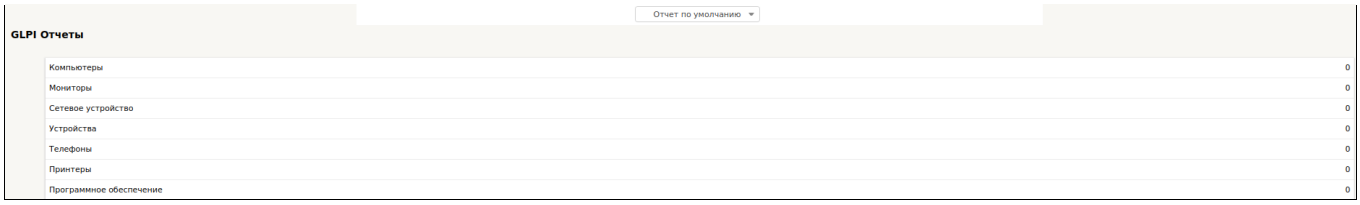
Автоматическое назначение заявок

Имеется возможность автоматического назначения заявки на сотрудника. Для этого перейдите в *«Администрирование» -> «Правила» -> «Бизнес-правила для заявок»*, в появившемся списке нужно выбрать правило и настроить его:



Отчет

Позволяет увидеть все, что происходит в системе, получить статистику и информацию по инвентаризации. Для просмотра отчёта переходим в *«Инструменты» -> «Отчет»* и выбираем необходимый тип отчёта:



OpenSearch — система распределенного поиска, сбора, анализа и визуализации данных

OpenSearch
Установка и настройка OpenSearch
OpenSearch Dashboards
Установка и настройка OpenSearch Dashboards
Logstash
Установка и настройка logstash
Beats
Установка и настройка filebeat
Установка и настройка auditbeat
Установка и настройка heartbeat
Установка и настройка metricbeat
Установка и настройка packetbeat
Отображение данных в OpenSearch Dashboards
Создание шаблона индексов
Создание информационной панели OpenSearch Dashboards
Использование Discover

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: opensearch-2.13.0, opensearch-dashboards-2.13.0, logstash-8.9.0, auditbeat-7.17.14, filebeat-7.17.14, heartbeat-7.17.14, metricbeat-7.17.14, packetbeat-7.17.14

OpenSearch стек (OpenSearch, Logstash, OpenSearch Dashboards) — это форк ELK стека (Elasticsearch, Logstash, Kibana). Конвейер обработки данных журнала состоит из трёх этапов: агрегация, обработка и хранение. В традиционном стеке обработка и агрегация данных осуществлялись с использованием **Logstash**. Из-за проблем с производительностью и сложностью обработки данных возникла потребность в использовании **Beats**.

Beats — это легковесные агенты сбора данных, каждый из которых предназначен для определенной задачи:

- **auditbeat** — сбор данных аудита безопасности;
- **filebeat** — мониторинг и сбор лог-файлов;
- **heartbeat** — проверка доступности служб;
- **metricbeat** — сбор метрик системы и служб;
- **packetbeat** — анализ трафика сетевых пакетов.

OpenSearch

Opensearch — это распределенная система полнотекстового поиска и анализа данных, работающая в режиме реального времени. После добавления данных в **opensearch** можно выполнять полнотекстовый поиск со сложными функциями: поиск по полю, поиск по нескольким индексам, повышение полей, ранжирование результатов по баллам, сортировка результатов по полю и агрегирование результатов.

Opensearch можно использовать в качестве серверной части для поискового приложения, система обеспечивает хорошую производительность и имеет возможность масштабироваться в зависимости от потребностей приложения.

Установка и настройка OpenSearch

Для установки **opensearch** выполните следующий алгоритм действий:

1. Выполните установку пакетов (потребуются права **администратора**).

Для установки **opensearch** необходимо определить собственный пароль администратора, чтобы настроить демонстрационную конфигурацию безопасности.

```
sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=<custom-admin-password> dnf install opensearch
```

где:

<custom-admin-password> — установите самостоятельно заданный пароль администратора длиной от 12 символов, содержащий прописные буквы (A-Z), строчные буквы (a-z), спецсимволы, цифры (0-9).

2. Перезагрузите конфигурацию диспетчера **systemd**:

```
sudo systemctl daemon-reload
```

3. Добавьте **opensearch** в автозагрузку и запустите службу:

```
sudo systemctl enable opensearch --now
```

4. Настройки **opensearch** находятся в файле ***/etc/opensearch/opensearch.yml***. Внесите изменения в конфигурационный файл:

```
sudo nano /etc/opensearch/opensearch.yml
```

5. Измените следующие строки:

```
network.host: 0.0.0.0
 discovery.seed_hosts: ["127.0.0.1", "[::1]"]
```

где:

- **0.0.0.0** — приём на всех интерфейсах;
- **["127.0.0.1", "[::1]"]** — локальный поиск хостов кластера.

Сохраните внесённые в конфигурацию изменения и перейдите в терминал.

6. Перезапустите службу **opensearch**:

```
sudo systemctl restart opensearch
```

7. Для проверки статуса службы **opensearch** можно использовать команду:

```
sudo systemctl status opensearch
```

При успешно выполненных настройках в статусе должно отображаться active (running).

8. Проверьте работу **opensearch**:

```
curl -X GET https://localhost:9200 -u 'admin:<custom-admin-password>' --insecure
```

В терминале должна отобразится информация приблизительно следующего содержания:

```
{
 "name" : "localhost.localdomain",
 "cluster_name" : "opensearch",
 "cluster_uuid" : "6c3fb4JuQJ2HJxQEfLiqIg",
 "version" : {
 "distribution" : "opensearch",
 "number" : "2.13.0",
 "build_type" : "tar",
 "build_hash" : "7ec678d1b7c87d6e779fdef94e33623e1f1e2647",
 "build_date" : "2024-05-13T00:00Z",
 "build_snapshot" : false,
 "lucene_version" : "9.10.0",
 "minimum_wire_compatibility_version" : "7.10.0",
 "minimum_index_compatibility_version" : "7.0.0"
 },
 "tagline" : "The OpenSearch Project: https://opensearch.org/"
 }
```

OpenSearch Dashboards

OpenSearch Dashboards — это веб-интерфейс для **opensearch**, предоставляющий комплексное решение для визуального анализа, обнаружения и запроса данных мониторинга. При работе с **opensearch** через консоль **OpenSearch Dashboards** использовать необязательно. Также вместо **OpenSearch Dashboards** в качестве веб-интерфейса можно использовать другие инструменты, например, **Grafana**.

Установка и настройка OpenSearch Dashboards

Для установки и настройки **opensearch-dashboards** выполните следующий алгоритм действий:

1. Выполните установку пакетов:

```
sudo dnf install opensearch-dashboards
```

2. Перезагрузите конфигурацию диспетчера **systemd**:

```
sudo systemctl daemon-reload
```

3. Затем запустите и добавьте в автозагрузку службу **opensearch-dashboards**:

```
sudo systemctl enable opensearch-dashboards --now
```

4. Откройте конфигурационный файл ***opensearch_dashboards.yml***:

```
nano /etc/opensearch-dashboards/opensearch_dashboards.yml
```

5. Добавьте строку для внешнего подключения к веб-панели:

```
server.host: "192.168.2.15"
```

где:

192.168.2.15 — IP-адрес хоста.

6. Перезапустите службу opensearch-dashboards:

```
sudo systemctl restart opensearch-dashboards
```

7. Проверьте статус службы opensearch-dashboards:

```
sudo systemctl status opensearch-dashboards
```

Отобразится текущий статус службы opensearch-dashboards, включая информацию о том, запущена ли служба, возникли ли ошибки или проблемы при запуске, а также последние записи журнала, связанные со службой. При успешном подключении в статусе должно отображаться: active (running).

Logstash

Logstash является механизмом обработки событий на стороне сервера. Утилита извлекает данные из широкого спектра источников, трансформирует их и отправляет в **opensearch** в реальном времени.

Возможности **logstash**:

- помогает централизовать данные из логов и метрик;
- выполняет обработку данных;
- формирует нужную пользователю выборку;
- позволяет строить масштабируемые контейнеры для сбора больших объемов разнообразных данных;
- нормализует и отправляет на хранение данные на различные ресурсы;
- обрабатывает все типы данных протоколирования;
- предоставляет фильтры ввода и плагины вывода.

Logstash принимает входные данные из следующих источников:

- STDIN,
- журналы,
- файлы,
- TCP / UDP,
- websocket,
- zeromq.

При наличии большого количества разрозненных данных их отправка напрямую в **opensearch** неудобна, в таких случаях можно использовать предобработку в **logstash**.

При использовании **logstash** на него отправляются данные со всех **beats** и настройки перемещаются в единый центр, где происходит управление, распределение индексов, изменение полей. При большой нагрузке есть возможность вынести **logstash** на отдельную машину.

Конвейер logstash состоит из трёх компонентов — **ввода**, **фильтров** и **вывода**. Таких блоков может быть любое количество.

```
input {
 input_plugin => {...}
 }

 filter {
 filter_plugin => {...}
 }

 output {
 output_plugin => {...}
 }
```

где:

- **input** — получает события из разных источников одновременно, используя коллекцию инструментов ввода с открытым исходным кодом под названием *beats* для сбора событий;
- **filter** — анализирует и обогащает события различными способами, располагает обширной коллекцией фильтров, которые преобразуют события и направляют их на вывод;
- **output** — отправляет отфильтрованные события в одно или несколько мест назначения.

Установка и настройка logstash

Для установки и настройки **logstash** выполните следующий алгоритм действий:

1. Выполните установку **logstash** (потребуются права **администратора**):

```
sudo dnf install logstash
```

2. Откройте для редактирования конфигурационный файл ***pipelines.yml***:

```
nano /etc/logstash/pipelines.yml
```

3. Добавьте следующие настройки:

```
- pipeline.id: main
 path.config: "/etc/logstash/conf.d/*.conf"
```

4. Создайте конфигурационный файл **input.conf**:

```
nano /etc/logstash/conf.d/input.conf
```

5. Добавьте в него следующие настройки:

```
input {
 beats {
 port => 5044
 }
 }
```

6. Создайте конфигурационный файл ***filter.conf***:

```
nano /etc/logstash/conf.d/filter.conf
```

7. Добавьте в него следующие настройки:

```
filter {
 if [type] == "syslog" {
 grok {
 match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%
{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }
 add_field => [ "received_at", "%{@timestamp}" ]
```

```
add_field => [ "received_from", "%{host}" ]
}
date {
match => [ "syslog_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]
}
}
}
```

8. Создайте файл ***output.conf***:

```
nano /etc/logstash/conf.d/output.conf
```

9. Добавьте в него следующие настройки:

```
output {
 opensearch {
 hosts => ["https://localhost:9200"]
 ssl => true
 ssl_certificate_verification => false
 user => "admin"
 password => "custom-admin-password"
 manage_template => false
 index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
 }
 }
```

10. Проверьте конфигурацию **logstash**:

```
sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t /usr/share/logstash/bin/logstash -f
```

Если конфигурация корректна, в ответе команды появится примерно следующее сообщение: Starting server on port: 5044. Если есть ошибки в конфигурации, будут показаны сообщения об ошибках, которые нужно исправить.

11. Добавьте службу **logstash** в автозагрузку:

```
systemctl enable logstash
```

12. Перезапустите службу **logstash**:

```
systemctl restart logstash
```

13. Проверьте статус **logstash**:

```
sudo systemctl status logstash
```

При успешном подключении появится статус: active (running).

Beats

Beats — это легковесные агенты для доставки данных с открытым исходным кодом, располагающиеся на стороне клиента. Их особенность заключается в задействовании небольшого количества ресурсов.

Beats содержит несколько пакетов, являющихся различными модулями системы обработки и анализа данных. Каждый из них предоставляет специальные возможности для сбора и анализа данных, что облегчает создание сквозных решений для анализа логов.

> **Примечание.**
>
> Компоненты **beats** и **logstash** являются взаимодополняемыми и в зависимости от задач можно использовать их либо вместе, либо по отдельности.

Установка и настройка filebeat

Модуль используется для сбора и доставки логов из локальных файлов в систему пользователя для мониторинга и анализа. Filebeat может мониторить различные источники данных, такие как логи приложений, системные журналы, а также JSON- и текстовые файлы.

1. Для установки программы **filebeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install filebeat
```

2. Откройте конфигурационный файл ***filebeat.yml***:

```
nano /etc/filebeat/filebeat.yml
```

3. В настройках укажите путь к файлам, которые необходимо собрать, и адрес, куда отправлять результаты.

В разделе Filebeat inputs включите опцию сбора лога:

```
filebeat.inputs:
 - type: log
 enabled: true
 paths:
 - /var/log/*.log
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

В разделе Logstash Output раскомментируйте следующие строки, вместо localhost укажите IP-адрес сервера:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

где:

- 192.168.2.15 – IP-адрес машины, на которой запущен logstash;
- 5044 – порт, который используется для подключения к logstash.

Сохраните изменения и закройте файл.

4. Активируйте модуль **logstash**:

```
sudo filebeat modules enable logstash
```

5. В файле **/etc/filebeat/modules.d/logstash.yml** измените настройки модуля. Вы должны включить хотя бы один набор файлов в модуле. По умолчанию наборы файлов отключены. Поменяйте значение **enabled: false** на **true**.

```
- module: logstash
  access:
    enabled: true
```

6. Перед запуском **filebeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo filebeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

7. Настройте автозагрузку **filebeat** и запустите службу:

```
sudo systemctl enable --now filebeat
```

8. Проверьте состояние **filebeat** с помощью команды:

```
sudo systemctl status filebeat
```

При успешно выполненных настройках в статусе службы должно отображаться active (running).

Установка и настройка auditbeat

Модуль системы обработки и анализа данных, предназначенный для мониторинга активности пользователей и процессов операционной системы. Он собирает данные об аудите безопасности, такие как журналы аудита, и отправляет их в **opensearch** или **logstash** для анализа и визуализации. **Auditbeat** отправляет эти события в режиме реального времени в opensearch для дальнейшего анализа. Можно следить за изменениями в определенных папках, идентифицировать потенциальные нарушения политики безопасности.

1. Для установки программы **auditbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install auditbeat
```

2. Настройте **auditbeat**:

```
sudo nano /etc/auditbeat/auditbeat.yml
```

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
  hosts: ["192.168.2.15:5044"]
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
  #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
  #hosts: ["localhost:9200"]
```

Сохраните изменения и закройте файл.

3. Перед запуском **auditbeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo auditbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

4. После настройки файла конфигурации необходимо запустить и настроить службу **auditbeat** для автозагрузки:

```
sudo systemctl enable --now auditbeat
```

5. Проверьте состояние **auditbeat** с помощью команды:

```
sudo systemctl status auditbeat
```

При успешно выполненных настройках в статусе должно отображаться active (running).

Установка и настройка heartbeat

Это модуль мониторинга доступности, предназначенный для проверки доступности и производительности служб и ресурсов. Он может мониторить HTTP-эндпоинты, TCP-службы, DNS-серверы и другие ресурсы, отправляя тестовые запросы и анализируя ответы. Heartbeat отслеживает доступность служб с помощью активного поиска. Получив список URL-адресов, **heartbeat** задаёт вопрос о доступности системы и отправляет эту информацию и время отклика в остальную часть стека для дальнейшего анализа.

Для установки программы **heartbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install heartbeat
```

1. Откройте конфигурационный файл ***heartbeat.yml***:

```
sudo nano /etc/heartbeat/heartbeat.yml
```

2. Настройте параметры в файле ***heartbeat.yml*** в соответствии с примером:

Включите монитор, который необходимо использовать.

```
heartbeat.monitors:
 - type: http
 urls: ["https://192.168.2.15:9200"]
 schedule: '@every 60s'
 id: dashboards
 name: 'Opensearch Dashboards'
 username: "admin"
 password: "custom-admin-password"
```

В разделе `Kibana` закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе `Elasticsearch Output` закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

В разделе `Logstash Output` раскомментируйте следующие строки:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

Сохраните изменения и закройте файл.

В этом примере файл ***heartbeat.yml*** настраивает параметры мониторинга и управления кластером из двух узлов с использованием **heartbeat** для обеспечения высокой доступности. В случае неисправности одного из узлов, другой узел возьмёт на себя его роль.

Перед запуском **heartbeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo heartbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

3. После настройки файла конфигурации необходимо запустить и настроить службу **heartbeat** для автозагрузки:

```
sudo systemctl enable --now heartbeat-elastic
```

4. Проверьте состояние **heartbeat** с помощью команды:

```
sudo systemctl status heartbeat-elastic
```

При успешно выполненных настройках в статусе должно отображаться active (running).

Установка и настройка metricbeat

Metricbeat — это модуль сбора метрик, предназначенный для сбора различных системных метрик и сервисной статистики. Он может собирать данные о производительности хостов, сетевого трафика, использования ресурсов контейнеров и многого другого. Применяется для мониторинга серверов/приложений.

Для установки программы **metricbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install metricbeat
```

Для настройки **metricbeat** выполните следующий алгоритм действий:

1. Откройте основной файл конфигурации ***/etc/metricbeat/metricbeat.yml*** для редактирования:

```
sudo nano /etc/metricbeat/metricbeat.yml
```

2. Измените настройки.

В разделе Modules configuration измените значение параметра reload.enabled на true.

```
metricbeat.config.modules:
 path: ${path.config}/modules.d/*.yml
 reload.enabled: true
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
 #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
 #hosts: ["localhost:9200"]
```

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
 hosts: ["192.168.2.15:5044"]
```

Сохраните изменения и закройте файл.

3. Откройте на редактирование конфигурационный файл ***metricbeat.reference.yml***:

```
sudo nano /etc/metricbeat/metricbeat.reference.yml
```

4. Заполните конфигурационный файл и сохраните настройки.

```
metricbeat.config.modules:
 path: ${path.config}/modules.d/*.yml
 reload.period: 10s

 reload.enabled: true
 metricbeat.max_start_delay: 10s

 metricbeat.modules:
 - module: system
 metricsets:
 - cpu
 - load
 - memory
 - network
 - process
 - process_summary
 - uptime
 - socket_summary
 enabled: true
 period: 10s
 processes: ['.*']
```

5. Перед запуском **metricbeat** рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo metricbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

6. После настройки файла конфигурации, необходимо запустить и активировать автозагрузку **metricbeat**:

```
sudo systemctl enable --now metricbeat
```

7. Проверьте статус **metricbeat**:

```
sudo systemctl status metricbeat
```

При успешно выполненных настройках в статусе должно отображаться active (running).

8. Для просмотра всех модулей выполните команду:

```
metricbeat modules list
```

9. Активируйте нужные модули:

```
metricbeat modules enable logstash
```

Установка и настройка packetbeat

Packetbeat — модуль для сбора метрик, предназначенный для мониторинга и анализа сетевого трафика протоколов уровня приложений в реальном времени. **Packetbeat** может анализировать различные протоколы, такие как HTTP, DNS, MySQL и другие службы, а также обнаруживать аномалии и атаки в сети. Мониторинг сетевого трафика имеет важное значение для управления инфраструктурой, обеспечивая высокий уровень производительности и безопасности.

На клиентской машине нужно настроить агент-отправитель. После сбора и обработки данных с хостов и контейнеров агент отправляет сгенерированные отчеты в **logstash** или **opensearch**.

Для установки программы **packetbeat** используйте команду (потребуются права **администратора**):

```
sudo dnf install packetbeat
```

После установки **packetbeat** нужно настроить. Основной файл конфигурации ***packetbeat.yml*** находится в каталоге ***/etc/packetbeat/***. Откройте его для редактирования:

```
sudo nano /etc/packetbeat/packetbeat.yml
```

Настройте сетевые интерфейсы, которые **packetbeat** будет использовать для мониторинга трафика, например:

```
packetbeat.interfaces.device: any
```

где:

any — означает мониторинг всех доступных интерфейсов. Можно указать конкретный интерфейс, например eth0.

Включите и настройте протоколы, которые **packetbeat** будет анализировать. Например:

```
packetbeat.protocols:
 - type: http
 ports: [80, 8080, 8000, 5000, 8002]
 - type: mysql
 ports: [3306]
 - type: dns
 ports: [53]
 - type: redis
 ports: [6379]
```

Этот пример включает анализ HTTP, MySQL, DNS и Redis трафика на указанных портах.

В разделе Logstash Output раскомментируйте следующие строки:

```
output.logstash:
  hosts: ["192.168.2.15:5044"]
```

В разделе Kibana закомментируйте следующие строки:

```
#setup.kibana:
  #host: "localhost:5601
```

В разделе Elasticsearch Output закомментируйте следующие строки:

```
#output.elasticsearch:
  #hosts: ["localhost:9200"]
```

Сохраните изменения и закройте файл.

Перед запуском packetbeat рекомендуется протестировать файл конфигурации на наличие ошибок:

```
sudo packetbeat test config
```

При успешных настройках появится сообщение: «**Config OK**».

После настройки файла конфигурации, необходимо запустить и настроить службу **packetbeat** для автозагрузки:

```
sudo systemctl enable --now packetbeat
```

Проверьте статус **packetbeat**:

```
sudo systemctl status packetbeat
```

При успешно выполненных настройках в статусе должно отображаться active (running).

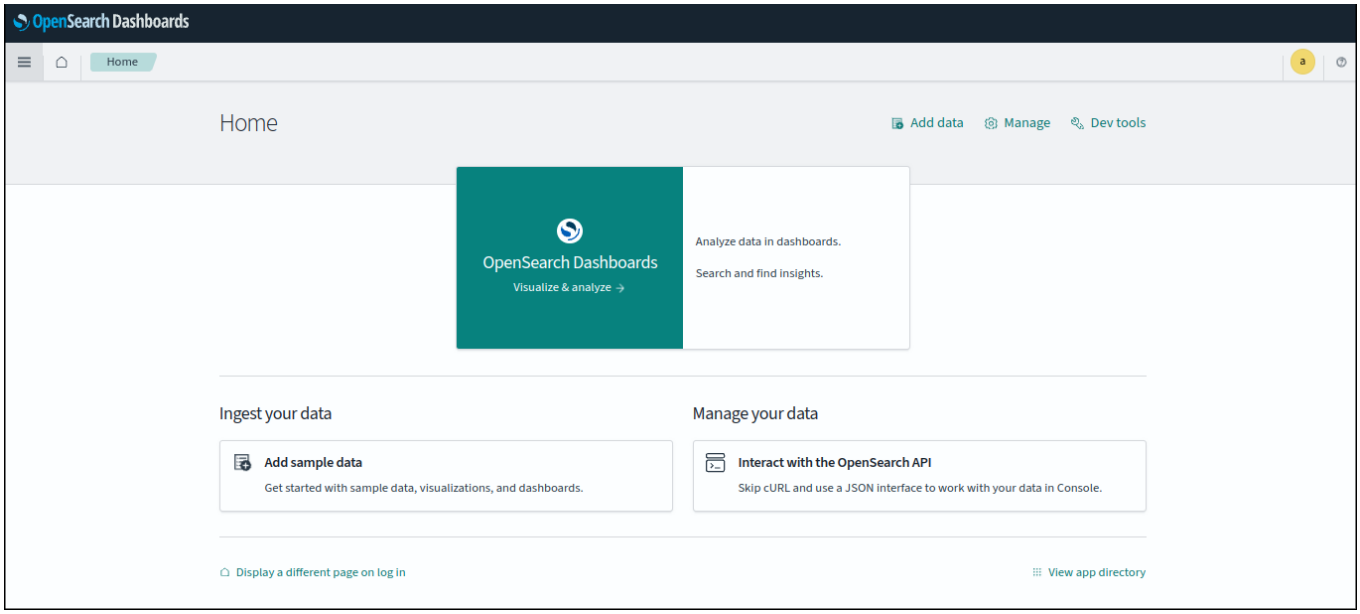
Отображение данных в OpenSearch Dashboards

Для просмотра данных в веб-панели **OpenSearch Dashboards** подключитесь через веб-браузер, используя IP-адрес машины, на которой развернут **logstash**:

```
http://192.168.2.15:5601
```

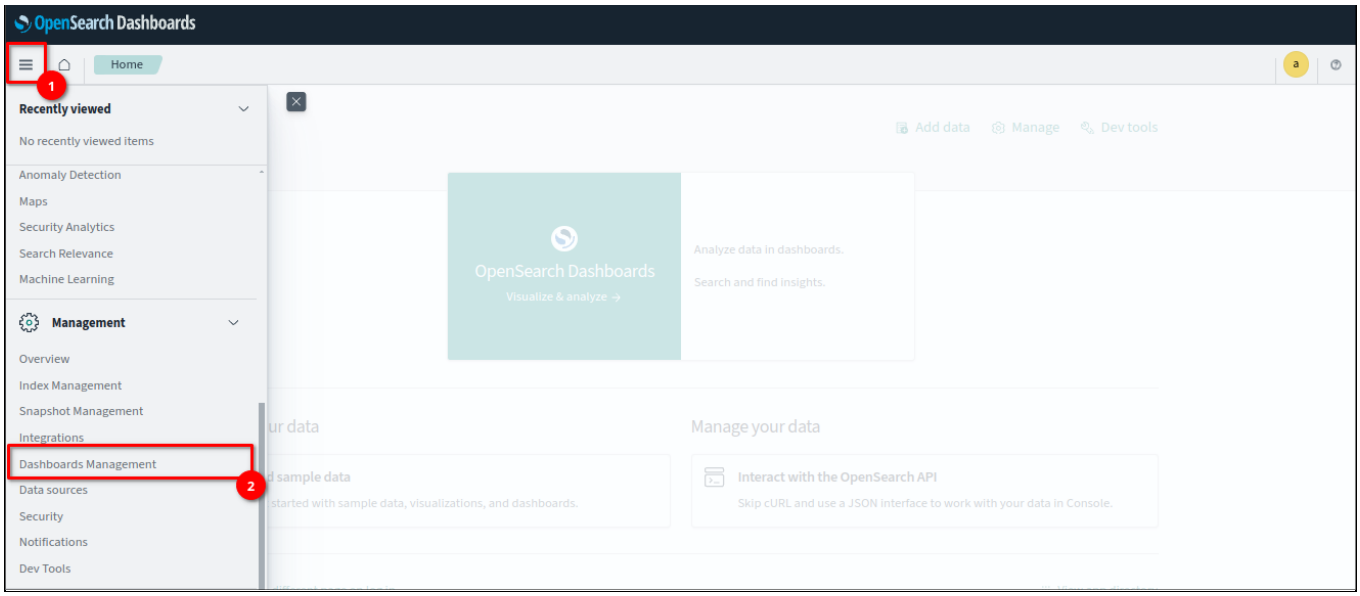


Введите аутентификационные данные, созданные при установке **opensearch**.

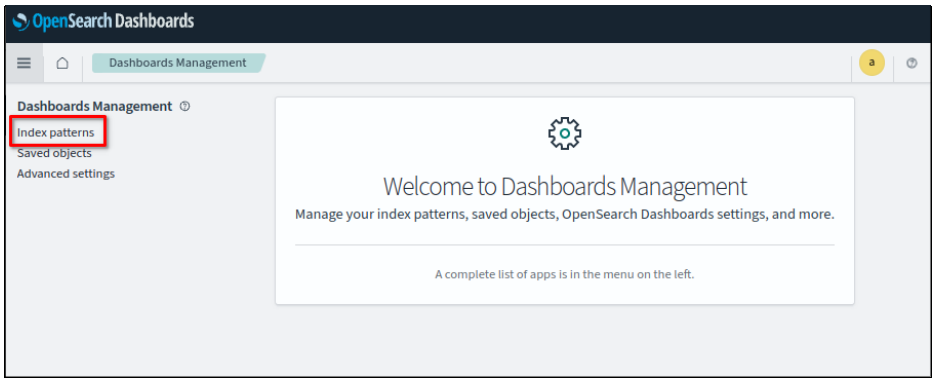


Создание шаблона индексов

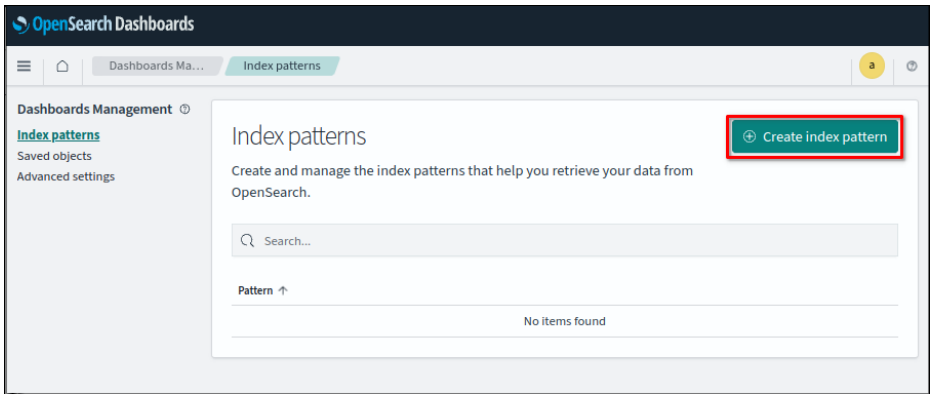
Для осуществления поиска данных с помощью **OpenSearch Dashboards** необходимо создать шаблон индексов. Перейдите в «**Основное меню**» (1) — «**Dashboards Management**» (2).



Выберите «**Index Pattern**».

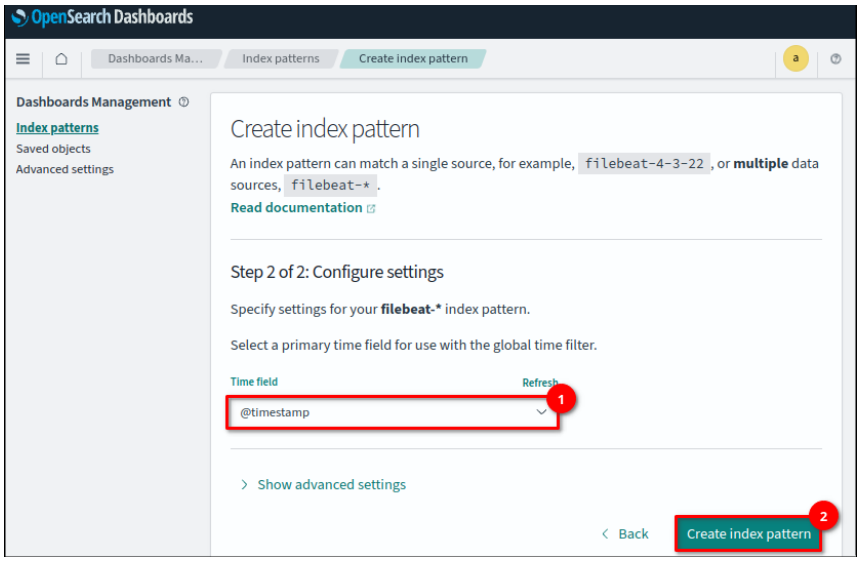


Нажмите кнопку «**Create index pattern**».



В поле «**Index pattern name**» (1) введите имя индекса «**filebeat-***» и нажмите «**Next step**» (2).

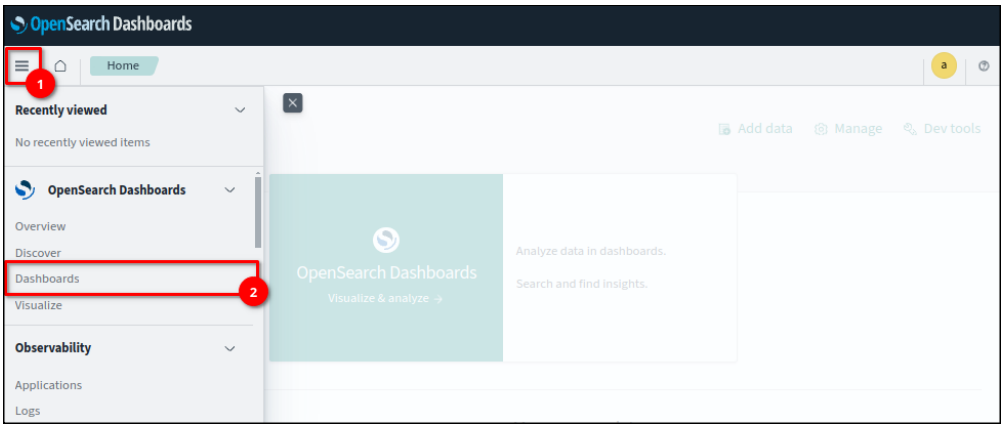
В поле «**Time field**» выберите значение «**@timestamp**» (1) и нажмите «**Create index pattern**» (2).



Аналогичным образом создаются индексы для **auditbeat-***, **heartbeat-***, **metricbeat-***, **packetbeat-*.**

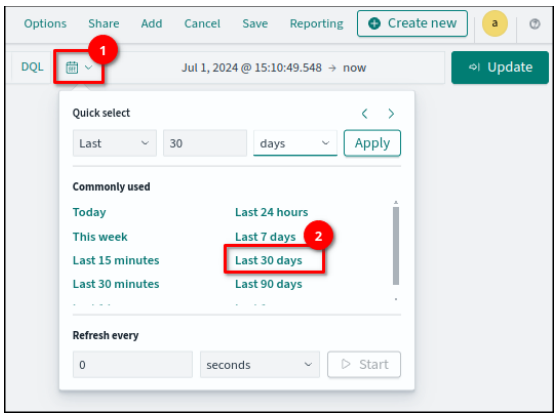
Создание информационной панели OpenSearch Dashboards

Для отображения данных в **OpenSearch Dashboards** необходимо создать информационную панель. Для этого перейдите в «**Основное меню**» (1) — «**Dashboards**» (2).

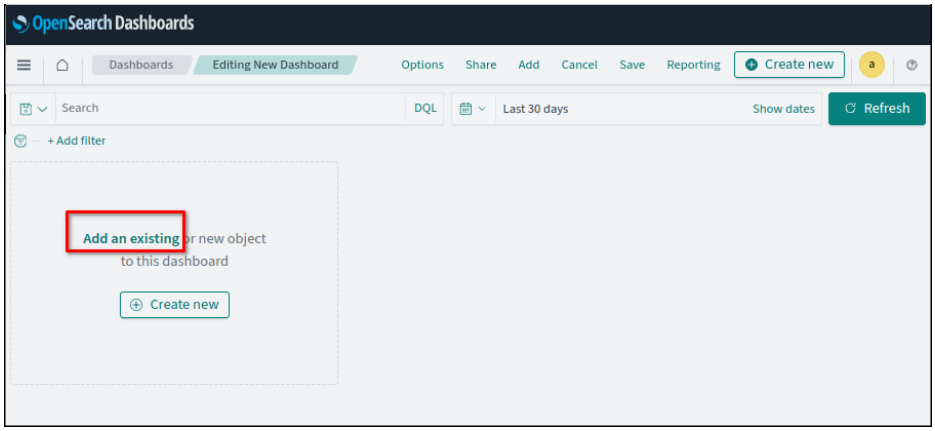


На панели «**Dashboards**» выберите «**Create**» — «**Dashboards**».

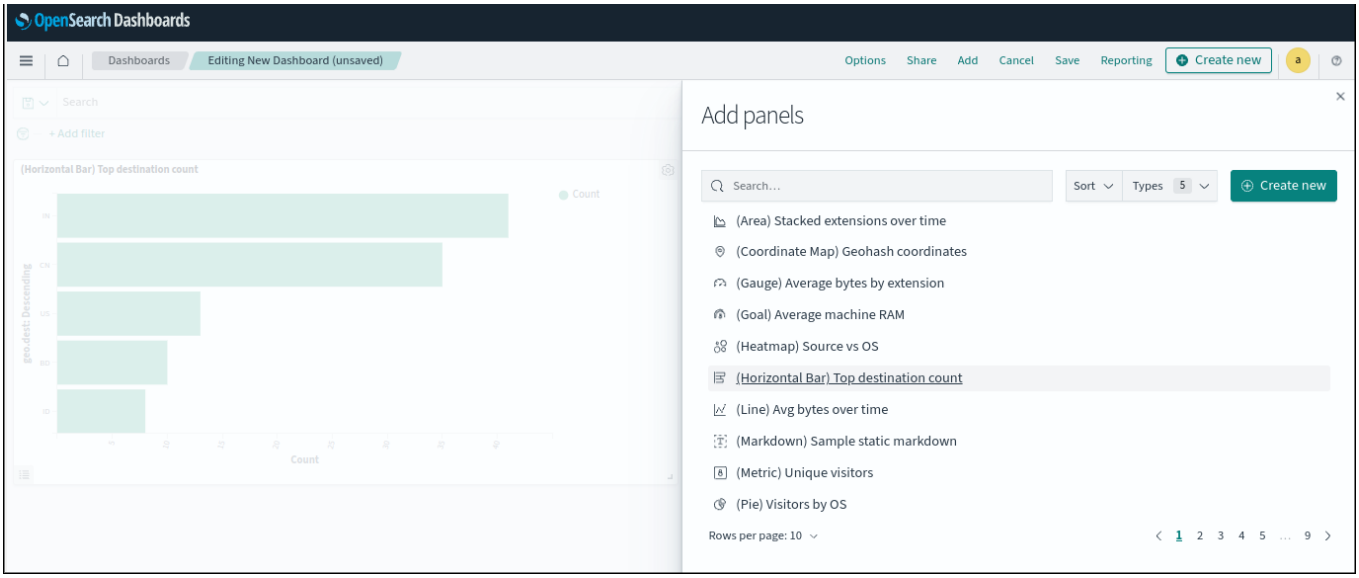
Выберите значок календаря и установите временной фильтр, например, 30 дней.



Выберите на панели «**Add an existing**» для добавления существующего объекта.



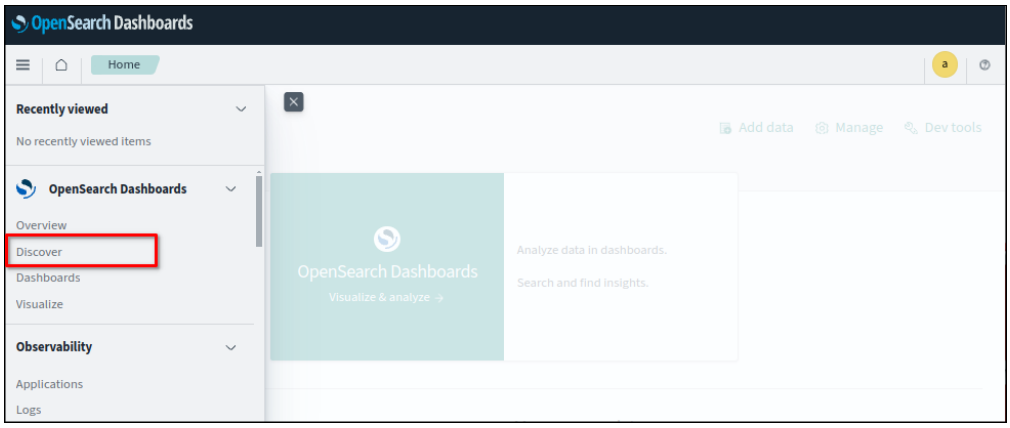
В окне **«Add panels»** выберите необходимую панель, а затем закройте панель. В результате будет создана базовая панель для мониторинга.



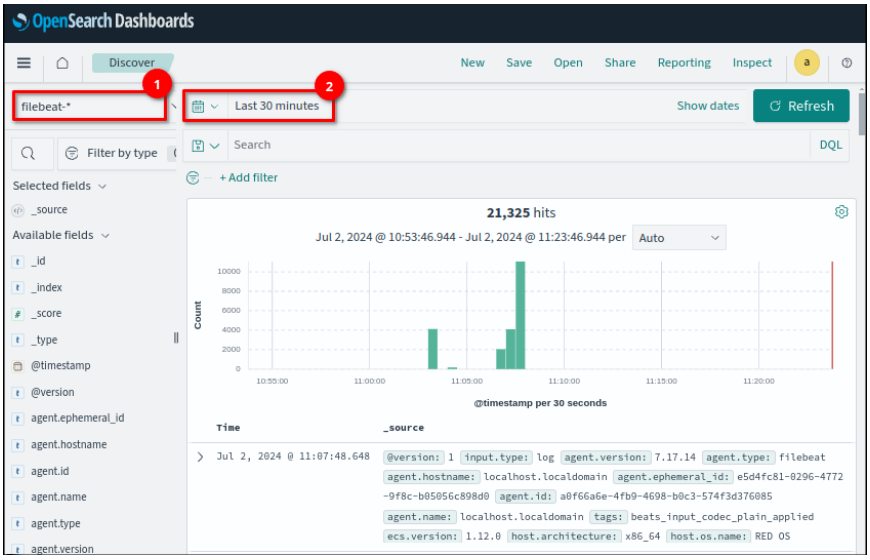
Использование Discover

С помощью раздела **Discover** можно выбирать данные для анализа, устанавливать временной диапазон для этих данных, выполнять поиск с помощью языка запросов Dashboards и фильтровать результаты.

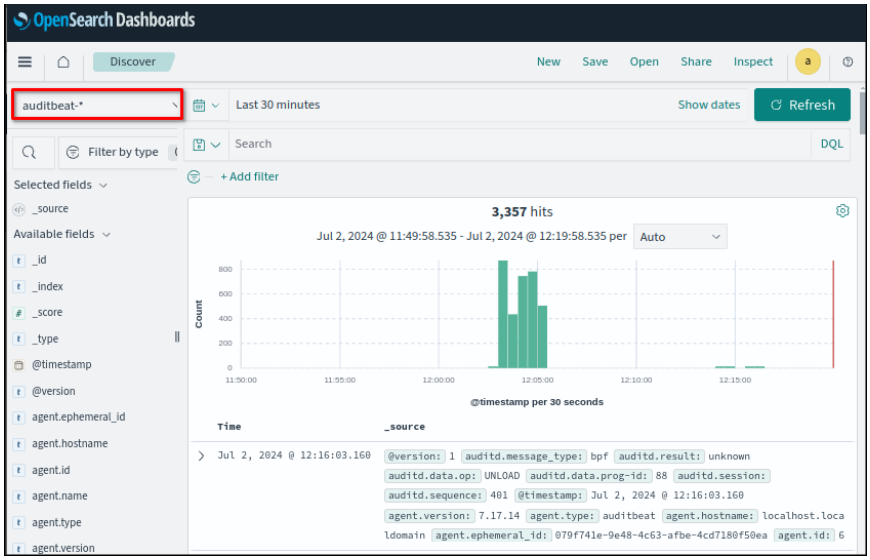
В навигационном меню **OpenSearch Dashboards** выберите раздел «**Discover**».



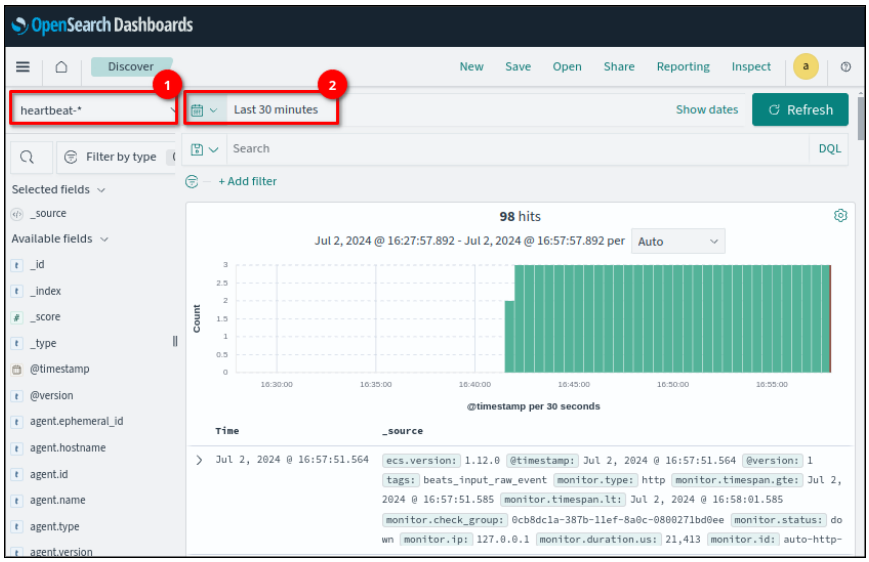
На странице **Discover** выберите шаблон индекса «**filebeat-***» (1) из выпадающего меню в левом верхнем углу. Выберите значок для изменения временного фильтра и установите значение «**Last 30 minutes**» (2).



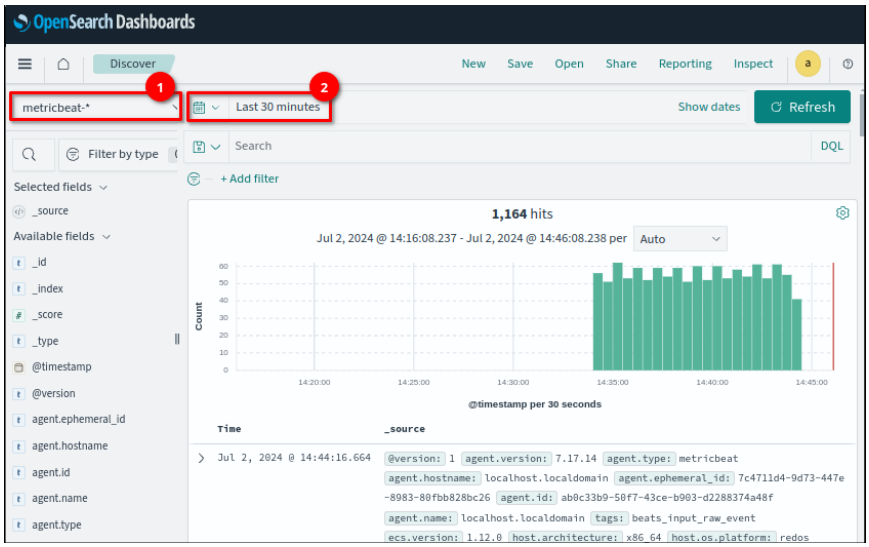
Результат для индекса «**auditbeat-***»:



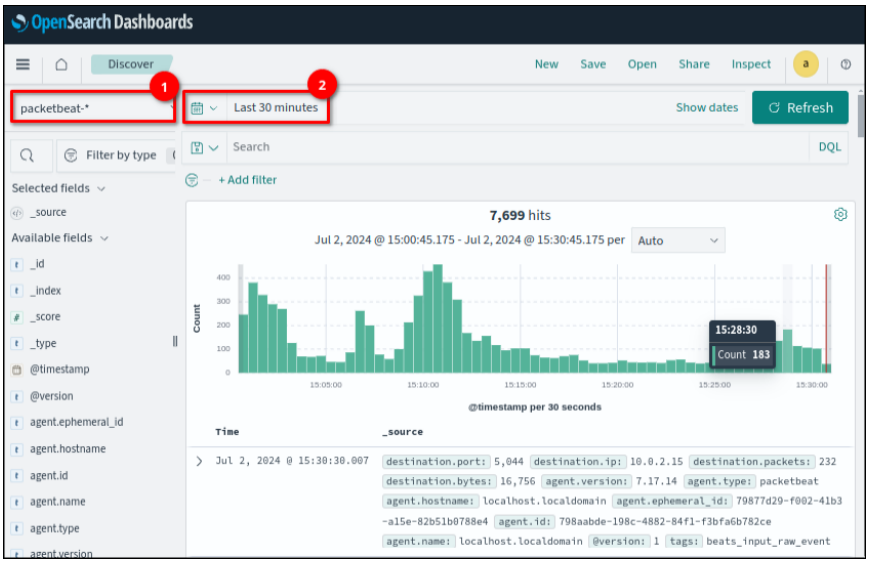
Результат для индекса «**heartbeat-***»:



Результат для индекса «**metricbeat-***»:



Результат для индекса «**packetbeat-***»:



Graylog — инструмент для централизированного сбора, хранения и анализа системных журналов

Установка Java 17
Установка MongoDB
Установка и настройка OpenSearch
Установка и настройка Graylog

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: graylog-server-5.2.9, java-17-openjdk-17.0.10, mongodb-org-7.0.8, opensearch-2.14.0

Graylog — это платформа для централизованного сбора, хранения, фильтрации, анализа и визуализации логов, которая помогает организациям получать ценные инсайты из своих данных.

Graylog предоставляет удобный интерфейс для работы с логами, позволяя администраторам и аналитикам быстро находить и устранять проблемы, а также отслеживать активность в реальном времени. Благодаря поддержке различных источников данных и гибким возможностям настройки **graylog** становится незаменимым инструментом для обеспечения безопасности и стабильности ИТ-инфраструктуры.

Graylog требует установки и настройки нескольких компонентов для полноценной работы.

1 . **Java 17** — обеспечивает совместимость и стабильность работы **graylog** (рекомендуется использовать последнюю стабильную версию для обеспечения безопасности и производительности).

2. **MongoDB** — база данных, которая используется **graylog** для хранения конфигурационных данных и метаданных.

3 . **OpenSearch** — поисковая и аналитическая система, которая позволяет обрабатывать большие объёмы данных, предоставляя обширные возможности для поиска и анализа логов.

4. **Сервер Graylog** — основной компонент, который собирает, обрабатывает и визуализирует логи.

Каждый из компонентов выполняет свою роль в общей системе управления логами.

Установка Java 17

Для установки **java-17** выполните следующие шаги:

1. Установите java-17, выполнив в терминале команду (потребуются права **администратора**):

```
sudo dnf install java-17-openjdk
```

2. Выберите версию по умолчанию 17:

```
update-alternatives --config java
```

Установка MongoDB

Для установки **mongodb** выполните следующий алгоритм действий:

1. Установите **mongodb**:

```
sudo dnf install mongodb-org
```

2. Перезагрузите конфигурацию системных служб:

```
sudo systemctl daemon-reload
```

3. Добавьте службу **mongod** в автозагрузку:

```
sudo systemctl enable mongod --now
```

4. Проверьте статус службы **mongod**:

```
sudo systemctl status mongod
```

В статусе должно отображаться active (running).

Установка и настройка OpenSearch

Для установки **opensearch** выполните следующий алгоритм действий:

1. Для установки **opensearch** необходимо определить собственный пароль администратора, чтобы настроить демонстрационную конфигурацию безопасности.

```
sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=<пароль> dnf install opensearch
```

где:

<пароль> — установите пароль администратора длиной от 12 символов, содержащий прописные буквы, строчные буквы, спецсимволы, цифры.

2. Настройки **opensearch** находятся в файле **/etc/opensearch/opensearch.yml**. Внесите изменения в конфигурационный файл:

```
sudo nano /etc/opensearch/opensearch.yml
```

3. Добавьте следующие строки:

```
cluster.name: graylog
 node.name: ${HOSTNAME}
 path.data: /var/lib/opensearch
 path.logs: /var/log/opensearch
 discovery.type: single-node
 network.host: 0.0.0.0
 action.auto_create_index: false
 plugins.security.disabled: true
```

4. Установите значение параметра виртуальной памяти vm.max_map_count:

```
sudo sysctl -w vm.max_map_count=262144
```

5. Добавьте параметр в файл конфигурации:

```
sudo echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

6. Перезагрузите конфигурацию системных служб, чтобы применить изменения:

```
sudo systemctl daemon-reload
```

7. Включите opensearch для автоматического запуска при загрузке системы:

```
sudo systemctl enable opensearch --now
```

8. Проверьте статус opensearch, чтобы убедиться, что он запущен и работает корректно:

```
sudo systemctl status opensearch
```

При успешно выполненных настройках в статусе должно отображаться active (running).

Установка и настройка Graylog

Для установки и настройки **graylog** выполните следующий алгоритм действий:

1. Установите **graylog**:

```
sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.rpm
```

2. Установите graylog-server:

```
sudo dnf install graylog-server
```

3. Создайте пароли для двух переменных **password_secret** и **root_password_sha2.** Без указанных переменных **graylog** не сможет запуститься.

Создайте хеш пароля администратора **graylog**. Используйте следующую команду, чтобы сгенерировать хеш для введенного `<пароля>`:

```
echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
```

Введите пароль:

```
Enter Password: <пароль>
```

В терминале отобразится хеш пароля:

```
<хеш_пароля>
```

Создайте секретный ключ password_secret:

```
< /dev/urandom tr -dc A-Z-a-z-0-9 | head -c${1:-96};echo;
```

В терминале отобразится секретный ключ:

```
<секретный_ключ>
```

Скопируйте полученные значения `<хеш_пароля>` и `<секретный_ключ>`.

4. Откройте конфигурационный файл **/etc/graylog/server/server.conf** на редактирование:

```
sudo nano /etc/graylog/server/server.conf
```

5. Измените следующие строки:

```
root_password_sha2 = <хеш_пароля>
 password_secret = <секретный_ключ>
 elasticsearch_hosts = http://localhost:9200
```

6. Перезагрузите конфигурацию системных служб:

```
sudo systemctl daemon-reload
```

7. Включение **graylog** для автоматического запуска:

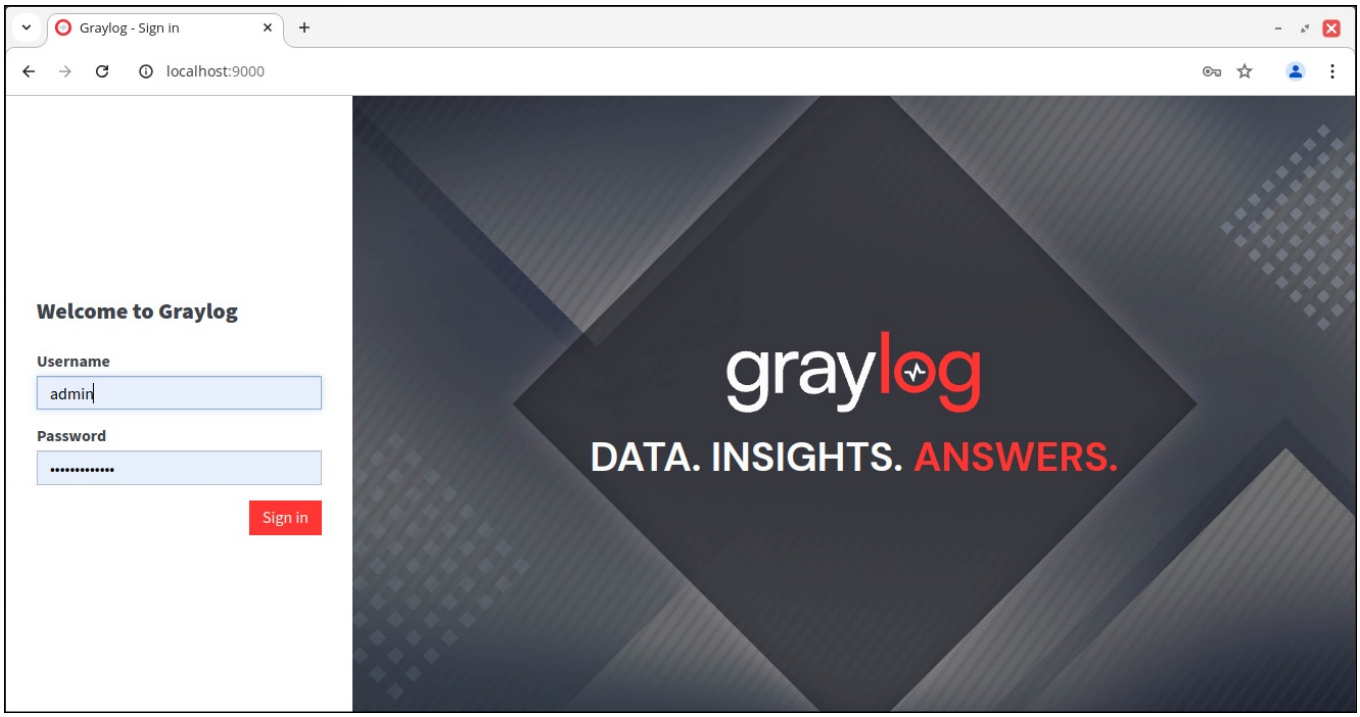
```
sudo systemctl enable graylog-server --now
```

8. Проверьте статус **graylog**:

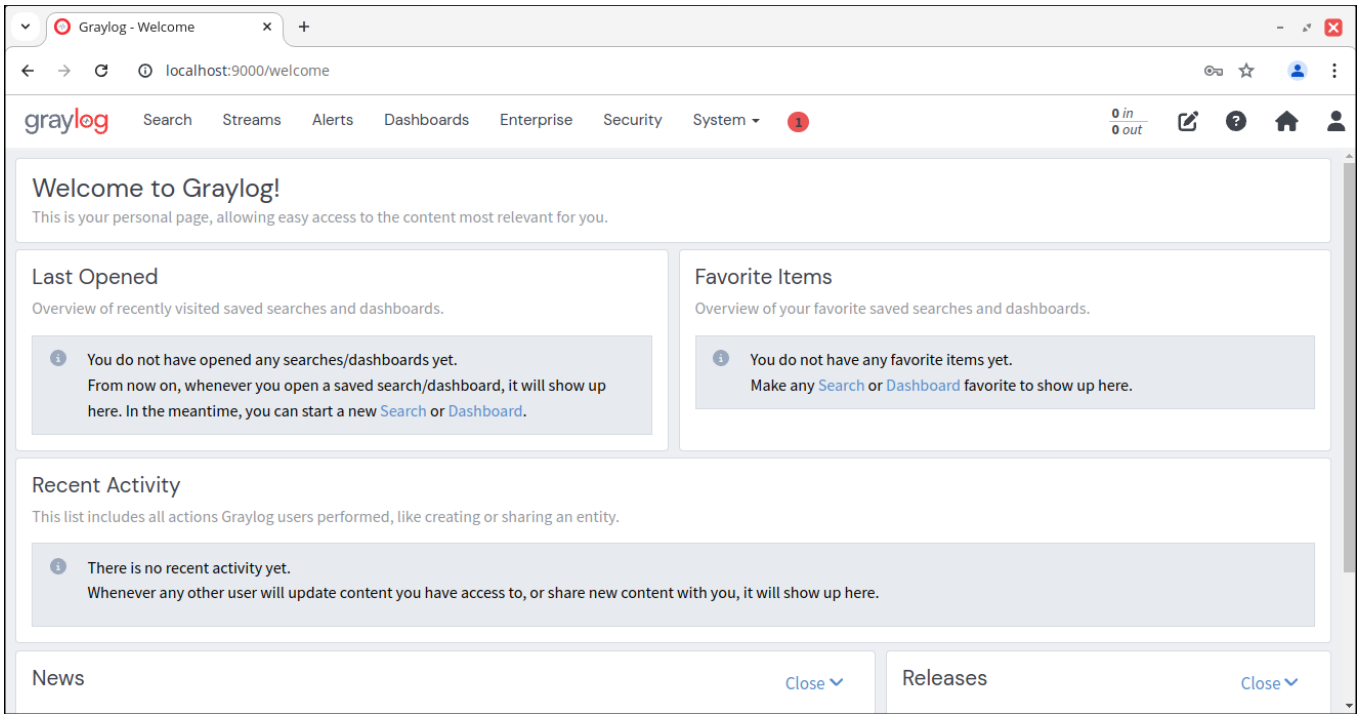
```
sudo systemctl --type=service --state=active | grep graylog
```

В случае успешного запуска сервера **graylog** в терминале отобразится сообщение: **loaded active running Graylog server**. Это означает, что сервер **Graylog** успешно запущен и работает.

9. Перейдите по адресу **http://localhost:9000** и войдите под учетной записью `admin:` `<пароль>`.



После входа в учетную запись отобразится веб-интерфейс **Graylog**. В этом интерфейсе можно управлять настройками **Graylog**, просматривать и анализировать логи, настраивать потоки данных, создавать дашборды и выполнять другие действия, связанные с мониторингом и анализом логов.



Создание резервных копий с помощью утилиты cp

Для создания резервных копий важных файлов пользователь может использовать команду **cp**.

cp — команда, предназначенная для копирования файлов из одного в другие каталоги (возможно, с другой файловой системой). Исходный файл остаётся неизменным, имя созданного файла может быть таким же, как у исходного, или изменится.

Чтобы скопировать файл

```
cp [ -f ] [ -h ] [ -i ] [ -p ][ -- ] исходный_файл целевой_файл
```

Чтобы скопировать файл или файлы в другой каталог

```
cp [-R] [-H | -L | -P] [-f | -i] [-pv] исходный_файл … целевая_директория
```

Чтобы скопировать каталог в другой каталог (должен быть использован флаг -r или -R)

```
cp [ -f ] [ -h ] [ -i ] [ -p ] [ -- ] { -r | -R } исходная_директория ... целевая_директория
```

Опции команды:

- **-R, -r, --recursive (recursive)** — копировать директории рекурсивно (то есть все поддиректории и все файлы в поддиректориях).
- **-f (force)** — разрешает удаление целевого файла, в который производится копирование, если он не может быть открыт для записи.
- **-H** — используйте этот ключ, чтобы копировать символические ссылки. По умолчанию команда переходит по символическим ссылкам и копирует файлы, на которые те указывают.
- **-i (interactive)** — команда будет запрашивать, следует ли перезаписывать конечный файл, имя которого совпадает с именем исходного, то есть если в параметре целевой_каталог или целевой_файл встречается такое же имя файла, какое было задано в параметре исходный_файл или исходная_директория, то запрашивается подтверждение. Для того, чтобы перезаписать файл, следует ввести у или его эквивалент для данной локали. Ввод любого другого символа приведёт к отмене перезаписи данного файла.
- **-n, --no-clobber** — не перезаписывать существующий файл (отменяет предыдущий параметр -i).
- **-v, --verbose** — выводит имя каждого файла перед его копированием.
- **-p (preserve)** — повторяет следующие свойства исходного файла или директории у целевого файла или директории:
  - время последнего изменения и последнего доступа,
  - идентификатор пользователя и группы,
  - права доступа и биты SUID и SGID.

Начало работы

Введение

fwbackups - многофункциональная программа для резервного копирования пользователей, которая позволяет вам легко создавать резервные копии ваших документов в любое время. Её простой, интуитивно понятный интерфейс предлагает следующие функции:

- каждый пользователь системы может настроить собственные резервные копии;
- по требованию или автоматическое резервное копирование файлов и папок с помощью наборов резервных копий;
- значок в трее, чтобы отслеживать текущий ход операций резервного копирования или восстановления;
- несколько резервных копий, включая сжатие и инкрементное резервное копирование;
- поддержка резервного копирования на удаленный хост через ssh / sftp;
- поддержка восстановления любых резервных копий.

Вы можете подробнее ознакомиться с работой утилиты **fwbackups**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с графической утилитой Fwbackups;
- в **Яндекс.Дзен** — Работа с графической утилитой Fwbackups;
- в **VK Видео** — Работа с графической утилитой Fwbackups.

На наших каналах вы также сможете найти много другой полезной информации.

Запуск fwbackups

Сначала установим программу.

```
dnf install fwbackups
```

Существует два способа запуска fwbackups:

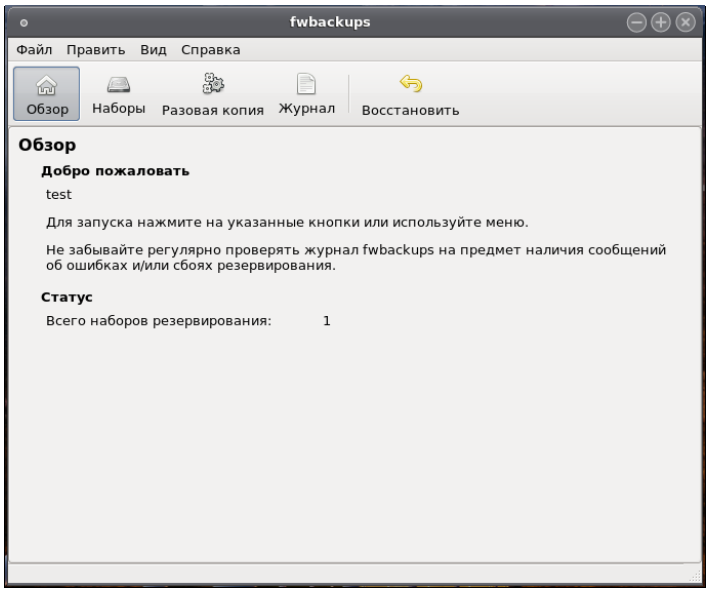
1. Графический (рекомендуется для большинства пользователей):

Выберите «**Приложения**» → «**Системные**» → «**fwbackups**» в меню;

2. Из интерфейса командной строки:

Запустите терминал, введите, **fwbackups** а затем нажмите клавишу «Enter» .

> Доступны дополнительные опции! Введите **fwbackups --help** все доступные параметры и их описания.



fwbackups открывает страницу «Обзор». Чтобы начать использовать **fwbackups**, просто нажмите одну из кнопок панели инструментов, чтобы переключать страницы.

Наборы

Создавайте, редактируйте или удаляйте наборы резервных копий, а также вручную запускайте заданную резервную копию.

Разовая копия

Выполнять «одноразовые» резервные копии (резервные копии, которые *не* планируется выполнять периодически).

Журнал

Отображает файл журнала, отображающий информацию о действиях **fwbackups** .

- Все сообщения журнала отформатированы следующим образом: *Month DD HH: MM: SS :: severity: message;*
- Сообщения из предыдущих сеансов отображаются фиолетовым цветом;
- Сообщения из текущего сеанса отображаются синим цветом;
- Ошибки и предупреждения отображаются красным и желтым цветом соответственно.

Восстановить

Позволяет восстановить любую резервную копию, которую вы ранее сделали с помощью **fwbackups**.

Использование fwbackups

Типы резервного копирования

fwbackups поддерживает два основных типа резервных копий: повторяющиеся резервные копии, которые автоматически резервируют ваши файлы по расписанию, и резервные копии, которые запускаются один раз и не запланированы снова. Они называются *резервными наборами* и *одноразовыми резервными копиями* соответственно.

Вы можете подробнее ознакомиться с работой утилиты **fwbackups**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с графической утилитой Fwbackups;
- в **Яндекс.Дзен** — Работа с графической утилитой Fwbackups;
- в **VK Видео** — Работа с графической утилитой Fwbackups.

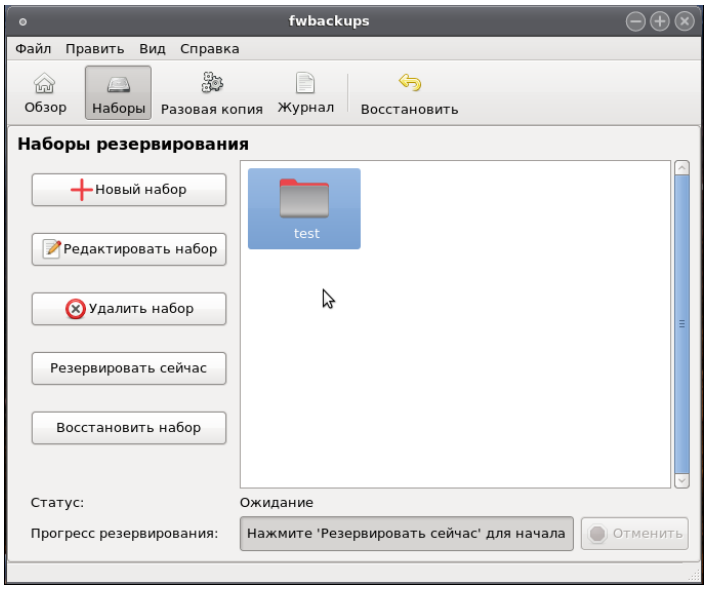
На наших каналах вы также сможете найти много другой полезной информации.

Вы сможете настроить любое количество наборов резервных копий, каждый из которых будет выполняться по регулярному графику в любое время по вашему выбору. Каждый набор работает независимо, поэтому, вы можете группировать файлы на два или более набора и производить их резервное копирование в разное время или в разные папки назначения. Вы также можете выполнять одноразовые операции, однако в этом случае резервное копирование не будет запланировано для запуска в будущем.

Когда использовать резервные наборы или одноразовые резервные копии

> Рекомендуется создать регулярные резервные копии для важных файлов, чтобы обеспечить сохранение резервной копии регулярно. Одноразовые резервные копии более подходят для создания резервных копий больших файлов, таких как музыкальная коллекция или видео, которые вы не хотите включать в набор резервных копий, который запускается ежедневно или еженедельно.

Создание набора резервных копий



Чтобы создать новый набор, нажмите «**Наборы»** на панели инструментов, а затем нажмите «**Новый набор»** слева.

Пути

Вкладка «Пути» позволяет выбрать, какие файлы и папки должны быть включены в резервную копию. Чтобы добавить файлы, нажмите «**Добавить файл »** или «**Добавить папку»**. Если вы хотите удалить файл или папку из резервной копии, выберите один или несколько путей из списка и нажмите «**Удалить»** .

Каждый путь в списке будет иметь либо зеленый, либо красный значок рядом с ним. Зеленый значок указывает, что **fwbackups** способен читать путь, а красный значок указывает, что файл отсутствует или не может прочитать путь, и он будет исключен из будущих резервных копий.

Добавление файлов или папок так же возможно с помощью перетаскивания из любого файлового менеджера в список путей.

Назначение

Вкладка назначения определяет, где будет сохранена ваша резервная копия. Вы можете выбрать резервное копирование на локальный диск, съемное хранилище или удаленный компьютер, поддерживающий протокол SFTP (если на вашем компьютере запущен сервер OpenSSH, он, скорее всего, поддерживает SFTP).

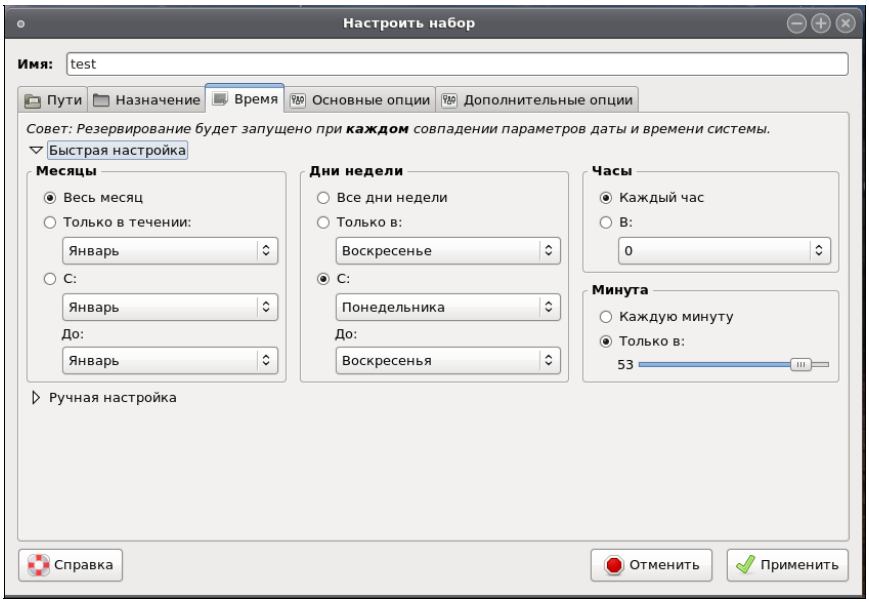
Не забудьте проверить настройки для удаленных пунктов назначения

Если вы решите сделать резервную копию на удаленном хосте, перед тем, как сохранить свой набор, обязательно нажмите «**Проверить настройки».** Опечатка в пароле (и в других полях) может сделать невозможным подключение к удаленному хосту, что приведет к неудачной резервной копии.

Время

Эта вкладка управляет временем и датой начала резервного копирования. Поддерживаются методы простой настройки и ручной настройки (crontab). Использование простой конфигурации рекомендуется для большинства пользователей.

Легкая конфигурация использует серию раскрывающихся списков и ползунков, чтобы определить, в какое время fwbackups должен запланировать резервное копирование. Резервное копирование набора выполняется каждый раз, когда дата соответствует выбранным параметрам. При этом будьте осторожны при выборе минуты для операции резервного копирования! Ошибка пользователя может вызвать резервирование **каждую минуту**. Вместо этого рекомендуется выбрать конкретную минуту, с которой начнется резервное копирование, например «0» (в начале часа) или «30» (в половине часа).



Если вы хотите дополнительно настроить время начала операции резервного копирования, вы можете использовать метод ручной настройки для этого. Он использует синтаксис crontab:

```
+ ------------- минута (0 - 59)
| + ------------ час (0 - 23)
| | + ---------- день месяца (1 - 31)
| | | + -------- месяц (1 - 12)
| | | | + ------ день недели (0 - 7) (воскресенье = 0 или 7)
| | | | | + ---- команда запуска
| | | | | |
* * * * * команда
```

Просто введите те же значения, что и в crontab, как указано выше, в обозначенные поля ввода. Обратите внимание, что вы не можете ввести все пять полей в одну строку. Кроме того, важно отметить, что в режиме ручной настройки проверка достоверности не выполняется при вводе пользователя, вы должны указать допустимые значения для полей. Шестое поле, используемое для команды, генерируется автоматически fwbackups.

- Используйте запятую (,), чтобы указать список значений

Пример 1. Использование запятой

2,4,5,7,8,9

- Используйте тире (-), чтобы указать диапазон значений

Пример 2. Использование тире

1-4 эквивалентна 1,2,3,4

- Используйте звездочку (*), чтобы указать все возможные значения

Пример 3. Использование звездочки

* в поле часов совпадает с 0-23 или 1,2,3, [...], 23

- Большинство версий cron поддерживают косую черту (/) для обозначения пропусков

Пример 4. Использование косой черты

* / 2 в поле минут эквивалентно 0,2,4,6,8, [...], 58

- В поле **дня недели**, как 0, так и 7 считаются воскресными.

Основные опции

Вкладка «**Основные опции»** позволяет вам установить параметры для вашей резервной копии. Кроме того, вкладка параметров позволяет вам выбрать формат резервного копирования и количество старых резервных копий для сохранения в любой момент времени.

Формат резервирования

Ваша резервная копия будет храниться по-разному в зависимости от выбранного формата резервного копирования.

Архивирование упаковывает все файлы в один (часто большой) архивный файл формата «tar». Архивные резервные копии не поддерживают инкрементное резервное копирование; каждый раз должен создаваться полный снимок. Также можно включить сжатие посредством gzip и bzip2. В этом случае к архиву будут приписаны .gz или .bz2 соответственно.

Уменьшение размера резервной копии при сжатии

> Включение сжатия будет использовать больше системных ресурсов во время резервного копирования, но приведет к меньшим размерам файлов. *gzip* - относительно легкое сжатие с хорошей степенью сжатия. Если вы хотите еще больше уменьшить размер своих резервных копий, подумайте о переходе на сжатие *bzip2* . Хотя он намного медленнее, чем gzip, bzip2 способен добиваться меньших размеров файлов.

При **прямом копировании** резервная копия будет просто копировать файлы и структуру папок как есть. Хотя этот тип резервного копирования не поддерживает сжатие, доступно инкрементное резервное копирование. Этот формат резервного копирования ранее назывался механизмом резервного копирования «rsync».

Увеличение скорости резервного копирования

> Включение параметра «**Прямое копирование файлов и папок» является инкрементным** вариантом, который будет выполнять инкрементную резервную копию вместо полной, копируя только изменения с момента последней резервной копии. В настоящее время инкрементные резервные копии не могут использоваться при резервном копировании на удаленный хост. Поддерживаются только полные прямые удаленные копии.
>
> Кроме того, при запуске инкрементного резервного копирования будет перезаписана папка бэкапа, поэтому старые резервные копии не будут сохранены.

Набор включен

Если этот параметр отключен, набор будет не запланирован для автоматического резервного копирования (недоступен в одноразовых резервных копиях).

Включая вложенные подпапки

Если выбрано, подпапки будут включены в резервную копию (рекомендуется). Если флажок снят, fwbackups будет делать только резервную копию файлов непосредственно внутри папок, указанных в разделе Пути, и не будет делать резервные копии файлов в подпапках.

Включая скрытые файлы

Если выбрано, скрытые файлы в системе (файлы и папки, начинающиеся с символа периода .) включены в резервную копию.

Следовать по ссылкам

Если выбрано, резервное копирование будет следовать символическим ссылкам и скопирует их цели, а не скопирует просто ссылку. Будьте осторожны с рекурсией ссылок!

Печатать информацию о геометрии диска в файле

Если выбрано, геометрия диска (включая разметку разделов) будет сохранена в файл, который будет добавлен в резервную копию.

Вывод установленных пакетов в текстовый файл

Если выбрано, список установленных имен и версий пакетов будет сохранен в текстовый файл, который будет добавлен в резервную копию. Этот параметр можно использовать для облегчения переустановки системы в неудачном случае сбоя или потери данных.

Сохраняется он в каталог tmp в бэкапе.

Эффективная поддержка разреженных файлов

Если выбрано, разреженные файлы на диске будут обработаны более эффективно.

Дополнительные опции

Вкладка «**Дополнительные опции**» включает технические или сложные параметры, которые можно использовать для настройки функций резервного копирования.

Команда для запуска до резервного копирования

Команда, введенная здесь, будет запущена в системной оболочке по умолчанию, прежде чем fwbackups начнет копировать файлы (недоступные в одноразовых резервных копиях).

Команда для запуска после резервного копирования

Команда, введенная здесь, будет запущена в системной оболочке по умолчанию после завершения резервного копирования fwbackups (недоступно в одноразовых резервных копиях).

Лексемы

Обе команды до и после резервного копирования поддерживают замену токенов. **fwbackups** заменит токены, которые вы используете в своих командах, с их соответствующими значениями:

[successful] Если резервная копия была успешно завершена без ошибок, этот токен будет заменен на 1. В случае ошибки сбоя или резервного копирования будет заменено 0.

[destination]

Целевая папка (см. Раздел «Назначение»). Если используется удаленный хост, то возвратится удаленная папка.

[set]

Имя набора

[date]

Дата в формате (YYYY-MM-DD_HH-MM) при запуске резервного копирования

[backup]

Имя файла резервной копии или папки, которая будет сохранена в месте назначения резервного копирования. По умолчанию *Backup-[set]-[date]*, плюс расширение архива, если это применимо.

[remote_host]

Имя хоста удаленного компьютера, на котором будет храниться резервная копия

[remote_port]

Порт для подключения к удаленному имени хоста

[remote_username]

Имя пользователя, используемое для подключения к удаленному хосту

[remote_password]

Пароль, используемый для подключения к удаленному хосту

> Используйте *[destination]/[backup],* если вам нужен абсолютный путь к новой папке или файлу резервной копии. Для экранирования одного из токенов (например, чтобы фактически использовать текст *[дата]* в команде), используйте обратную косую черту (\ *[дата]*).

Значение nice для процесса резервирования

Он контролирует приоритет резервного копирования (более низкое значение nice указывает более высокий приоритет). Только пользователь root может выбирать отрицательные nice значения.

Исключение из резервной копии

Файлы и папки, соответствующие шаблонам, перечисленным в этой текстовой записи, будут исключены из резервной копии. Файл, папка или шаблоны для исключения должны вводиться по одному в строке. Содержимое этой текстовой записи будет передаваться

непосредственно процессам tar или rsync при выполнении резервного копирования. В приведенном ниже примере все файлы в папке /home/username/Exclude, все файлы с расширением png, файл /home/username/foobar.jpg и, наконец, все имена файлов specificname.txt исключены из резервной копии.

Пример 5. Исключение файлов

/home/username/Exclude/*

*.png

/home/username/foobar.jpg

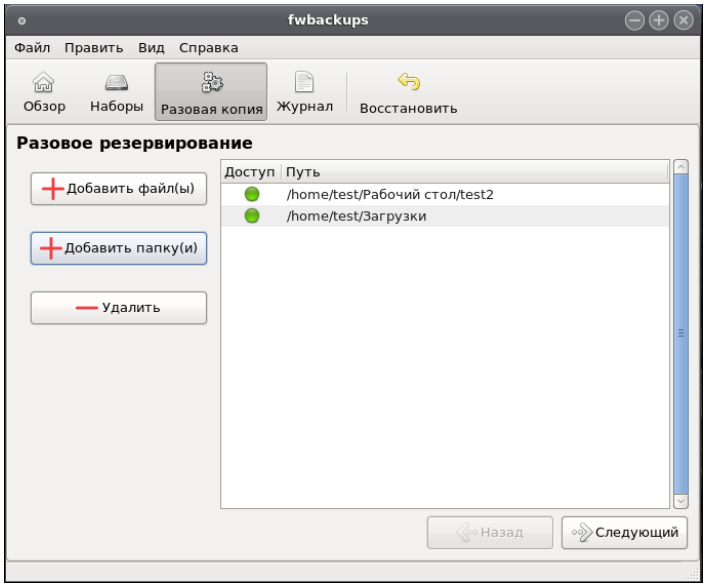
specificname.txt

Редактирование существующего набора

Перейдите на страницу «**Наборы резервирования»** и выберите нужный набор. Нажмите «**Редактировать набор»,** чтобы открыть диалоговое окно конфигурации резервного копирования. Вы можете настроить существующие наборы таким же образом, как и для нового набора (см. Раздел «Создание набора резервных копий»).

Запуск резервной копии только один раз

1. Переключитесь на страницу **разового резервного копирования**
2. Добавьте файлы и/или папки, которые вы хотите сделать резервными копиями. Вы можете использовать кнопки «**Добавить файлы» или «Добавить папки»**или просто перетащить файлы и папки в список. По завершении нажмите « **Далее»**.



3. Выберите варианты резервного копирования (см. Раздел «Основные опции»). По завершении нажмите «**Запуск резервирования»,**чтобы начать операцию.

Восстановление резервных копий

fwbackups может восстанавливать ваши файлы и папки из любого запланированного или одноразового резервного копирования.

1. Нажмите «**Восстановить»**на панели инструментов, чтобы открыть диалоговое окно восстановления.
2. Введите папку, в которую вы хотите восстановить свои файлы, в запись с надписью « **Восстановить в»**. Чтобы сделать выбор более удобным, вы можете использовать кнопку «**Обзор»**, чтобы открыть диалоговое окно браузера файлов. Зеленый значок указывает, что введенная папка доступна для записи, а красный значок указывает на то, что папка не может быть написана (необходимо выбрать другую и выполнить операцию восстановления).

Структура папок сохраняется в операциях восстановления, поэтому файлы будут восстановлены относительно их исходного местоположения. Например, восстановление резервной копии из **/home/myusername** для **/tmp** приведет к тому, что ваши файлы восстановятся в **/tmp/home/myusername**.

Установка места восстановления в корневой каталог приведет к восстановлению ваших файлов в их исходных местоположениях. Но при использовании такого варианта убедитесь что программа запущена с привилегиями суперпользователя.

3. Выберите, источник восстановления. Существует несколько возможных вариантов:

Набор резервирования

Используйте этот параметр для восстановления из созданных ранее резервных копий. Достаточно указать только набор и дату копирования.

Локальный архив

Используйте этот параметр для восстановления одноразовых архивных резервных копий, доступных на локальном хранилище (например, жестких дисках или съемных носителях). Нажмите «**Обзор»,** чтобы выбрать местоположение архивного файла для восстановления.

Локальная папка

Используйте этот параметр для восстановления одноразовых резервных копий как есть, доступных на локальном хранилище (таких как жесткие диски или съемные носители). Нажмите «**Обзор»** чтобы выбрать резервную папку для восстановления.

Удаленный архив (SSH)

То же, что и **локальный архив,** за исключением того, что архив будет извлечен с удаленного компьютера, после чего можно запустить восстановление из локального архива.

Удаленная папка (SSH)

То же, что и **локальная папка,** за исключением того, что папка будет извлекаться с удаленного компьютера, прежде чем восстановлена.

После того, как вы настроили операцию восстановления, нажмите «**Запуск восстановления»,** чтобы начать восстановление файлов. В зависимости от размера вашей резервной копии восстановление файлов может занять некоторое время.

Импорт или экспорт наборов

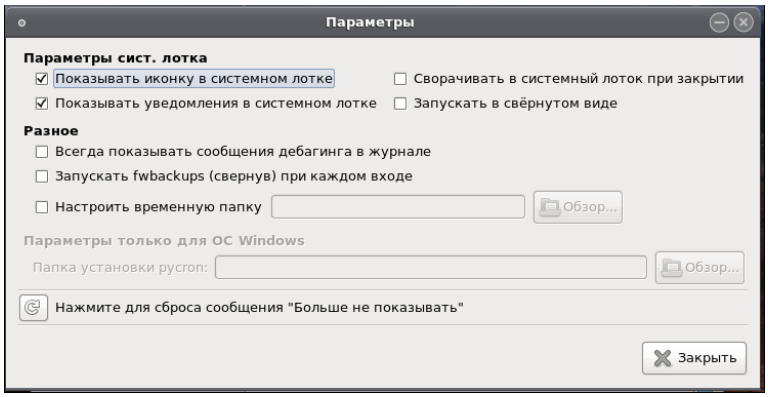
Чтобы импортировать установленные файлы конфигурации (**.conf** файлы), выберите «**Файл» → «Импорт наборов»,** а затем выберите файлы .conf, которые необходимо импортировать. Все версии **файлов** конфигурации **fwbackups** можно импортировать.

Чтобы экспортировать набор, выберите «**Файл» → «Экспорт наборов»** и выберите наборы, которые вы хотите экспортировать, установив флажок рядом с заданным именем. После выбора папки нажмите «**Экспортировать наборы»,** чтобы сохранить выбранные наборы в выбранную папку.

Местоположение, в котором хранятся установленные конфигурации, находится **~/.fwbackups/Sets.**

Изменение настроек программы

Выберите «**Править» → «Параметры»** в меню, чтобы открыть диалог настроек:



Показывать иконку в системном лотке

При переключении этого флажка будет отображаться или скрываться значок в трее.

Показывать уведомления в системном лотке

Выберите это, если вы хотите получать уведомления для важных событий.

Сворачивать в системный лоток при закрытии

При выборе этого флажка **fwbackups сворачивается** в трей при закрытии вместо выключения.

При нажатии на значок в трее откроется главное окно **fwbackups** .

Запускать в свёрнутом виде

Выберите, чтобы **fwbackups** отображал только значок в трее и скрывал главное окно при запуске.

Всегда показывать сообщения дебагинга в журнале

Эта опция позволяет отображать отладочные сообщения в средстве просмотра журналов. Используйте это, если вы пытаетесь устранить проблему.

Запуск fwbackups (свернув) при каждом входе

Выберите, чтобы fwbackups запускался свернутым при каждом входе в систему.

Настроить временную папку

Настройте временную папку для fwbackups.

«Больше не показывать»

Некоторые сообщения в **fwbackups** можно отключить, выбрав «**Больше не показывать**». Если вы хотите снова включить эти сообщения, нажмите кнопку.

Техническая информация

Вы можете подробнее ознакомиться с работой утилиты **fwbackups**, просмотрев наши обучающие видео:

- на **RuTube** — Работа с графической утилитой Fwbackups;
- в **Яндекс.Дзен** — Работа с графической утилитой Fwbackups;
- в **VK Видео** — Работа с графической утилитой Fwbackups.

На наших каналах вы также сможете найти много другой полезной информации.

Форматы резервного копирования

В этом разделе описывается, как fwbackups создает резервные копии и требования к хранилищу каждого типа.

Архивные/tar-архивы

Архивные резервные копии используют один из двух методов для создания резервного архива в зависимости от операционной системы. Программа tar вызывается непосредственно для создания стандартного архива tar, опционально со сжатием gzip или bzip2. Сжатие резервной копии применяется «на лету» без необходимости создания архива tar.

Поскольку резервная копия находится в формате стандартного tar-архива, если нет возможности восстановить бэкап с помощью fwbackups, то любая утилита, поддерживающая формат tar может использоваться для извлечения файлов из резервной копии.

Резервное копирование Direct Copy/rsync

fwbackups определяет параметры, а затем делает вызов **rsync** для копирования файлов (rsync быстрее, чем shutil и, следовательно, используется, если rsync установлен в системе).

Поскольку файлы были скопированы напрямую, если fwbackups не может восстановить ваши файлы, достаточно просто скопировать их из места назначения резервного копирования в нужное место с помощью перетаскивания в вашем браузере файлов.

Минимальные требования к хранению

В зависимости от формата резервного копирования и назначения, минимальные требования к хранилищу для резервного копирования могут изменяться.

Для локальных резервных копий, как **архивных** и **прямого копирования** система будет копировать файлы с исходного диска к месту назначения без необходимости временного хранения, даже если сжатие включено.

Резервные копии для удаленных получателей имеют разные требования к хранению. **Архивные** резервные копии с удаленным получателем создают архив локально, а затем загружают его через SFTP на удаленный хост. Следовательно, вы должны иметь свободное пространство, равное размеру резервных копий файлов (если не включено сжатие, и в этом случае потребуется немного меньше). В резервной копии с **прямым** копированием с удаленным получателем файлы загружаются непосредственно на удаленный компьютер, и поэтому можно создать резервную копию полного диска. Однако следует предупредить, что удаленная прямая копия значительно медленнее резервной копии архива.

Сохранение владения файлами и другие атрибуты

fwbackups использует внутренние файлы tarfile и shutil для восстановления файлов (и paramiko для взаимодействия с удаленными узлами через SFTP). Разрешения на файлы, время модификации и время доступа всегда сохраняются, как и символические ссылки.

Локальные резервные копии должны сохранять право собственности на Unix-подобные операционные системы, однако ОС обычно не позволяют обычным пользователям изменять права собственности на файлы, и, таким образом, резервное копирование нужно будет извлечь вручную с правами root, чтобы сохранить право собственности. Удаленные резервные копии не сохранят право собственности, так как любые файлы, загруженные через SFTP, предполагают владельца пользователя, используемого для подключения к удаленному компьютеру. Обратите внимание, что в случае резервного копирования архива на удаленный хост это относится только к фактическому архиву. Сам архив может содержать информацию о владельце файла, и как только он был получен с удаленного хоста, его можно извлечь вручную аналогично резервной копии локального архива, если пользователь хочет сохранить права собственности на файл.

Другие атрибуты файлов, xattrs или ACL могут быть сохранены в резервной копии (в зависимости от формата резервной копии, ОС, на которой была создана резервная копия, и файловой системы), однако fwbackups не будет пытаться их восстановить.

Ожидаемые уровни надежности

fwbackups - это программа резервного копирования пользователей и, соответственно, должна иметь возможность резервировать ваши пользовательские данные без проблем. Хотя можно использовать fwbackups для резервного копирования всей операционной системы, это не было его целью, и этот сценарий пока не проверен. Пользователи должны ожидать, что fwbackups будут успешно выполнять резервное копирование и восстановление своих данных, однако (как описано выше) дополнительные метаданные, такие как владение файлами, списки ACL и расширенные атрибуты, которые ОС может потребовать для правильной работы, не подлежат восстановлению вместе с фактическими файловыми данными.

Пользователям рекомендуется регулярно проверять журнал fwbackups, чтобы гарантировать отсутствие ошибок, а также

периодически проверять резервные копии.

Testdisk - утилита для восстановления утраченных данных

Утилита **testdisk** предназначена для восстановления утраченных разделов и/или данных, если эти проблемы вызваны программно, вредоносным ПО или ошибками человека.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install testdisk
```

После установки запуск утилиты доступен по команде (с правами пользователя **root**):

```
testdisk
```

Вы можете подробнее ознакомиться с работой утилиты **testdisk**, просмотрев наши обучающие видео:

- на **RuTube** — Восстановление файлов в РЕД ОС;
- в **Яндекс.Дзен** — Восстановление файлов в РЕД ОС;
- в **VK Видео** — Восстановление файлов в РЕД ОС.

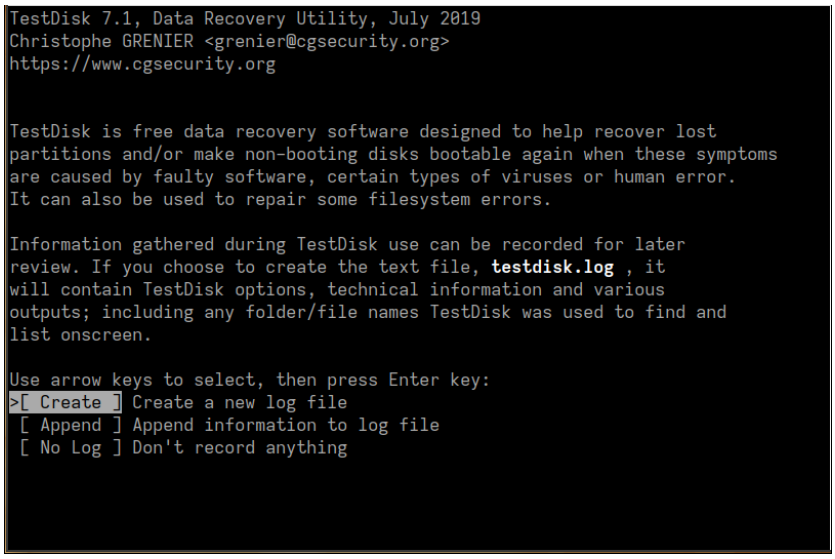
На наших каналах вы также сможете найти много другой полезной информации.

Утилита работает в окне терминала и имеет интуитивно понятный интерфейс.

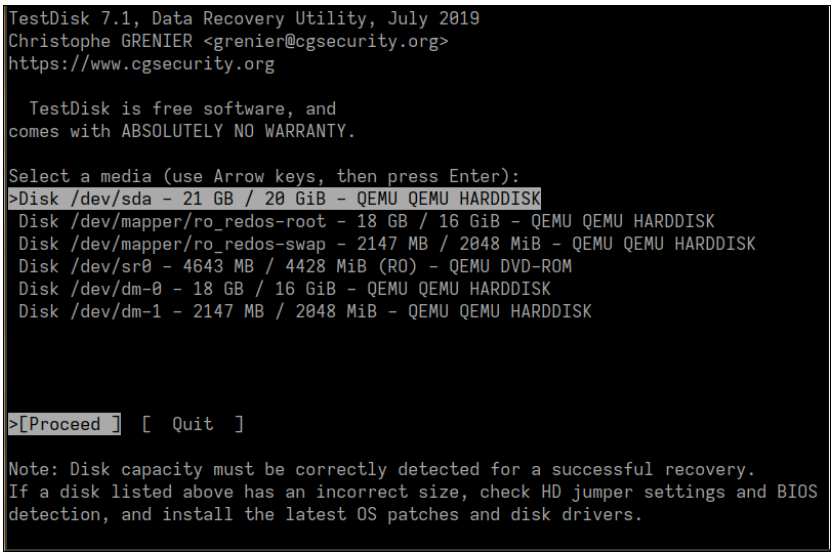
Сначала необходимо выбрать способ логирования данных:

- [**Create**] - создать новый файл журнала данных;
- [**Append**] - использовать существующий;
- [**No Log**] - ничего не регистрировать.

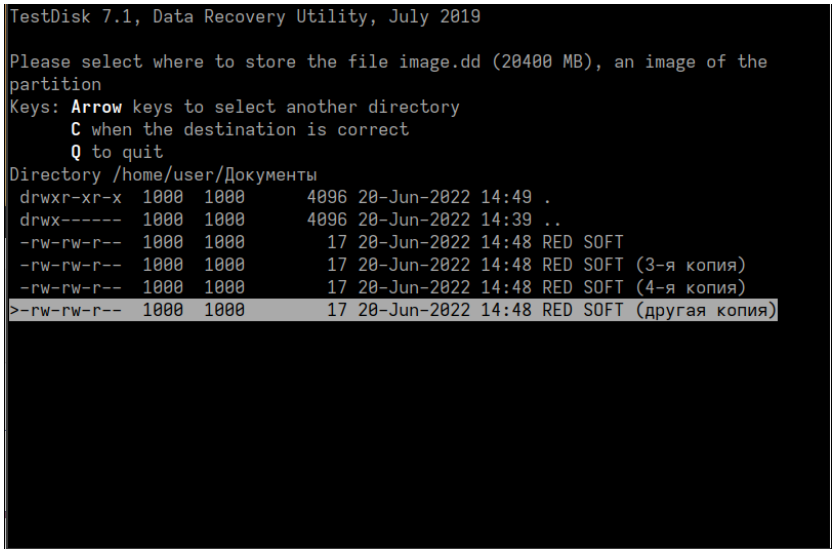
Выберите подходящий вам вариант.



Следующий шаг — выбор диска. Утилита отображает все диски, подключенные к системе, общий объем памяти каждого диска и его свободное пространство. Для продолжения работы необходимо выбрать диск, на котором хранится (хранилась) информация, подлежащая восстановлению.

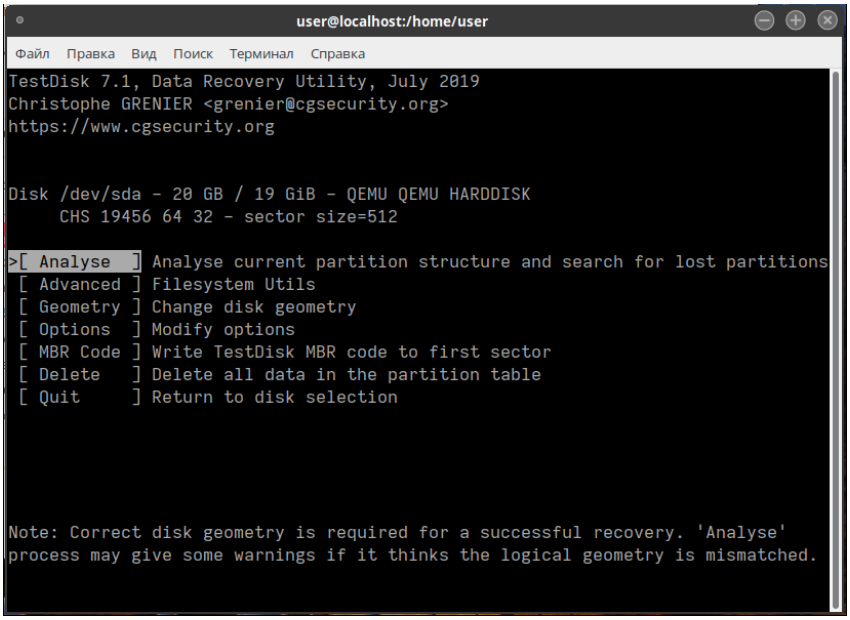


Перед тестированием утилиты было создано несколько файлов в папке «**Документы**». До момента их удаления они отображаются через утилиту **testdisk** в заданной папке, их также можно копировать в другие разделы и каталоги.

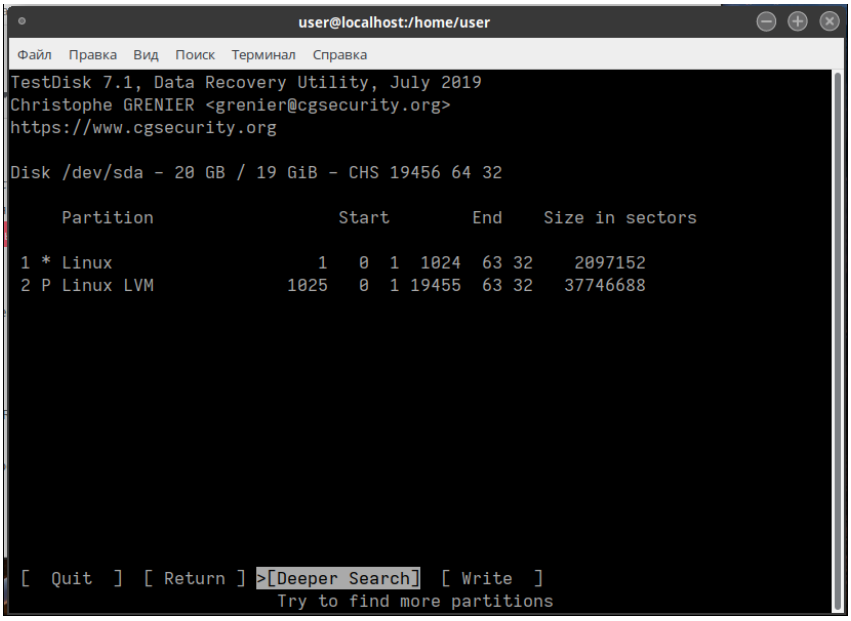


После того как некоторые документы были удалены, с помощью утилиты **testdisk** необходимо произвести анализ текущей структуры разделов необходимого диска.

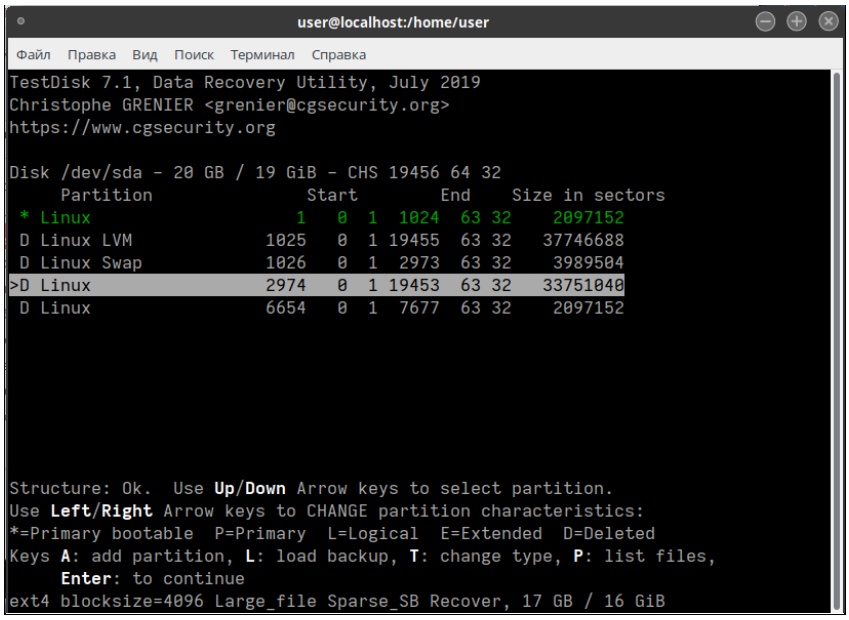
Для этого на требуемой таблице разделов необходимо выбрать из предложенных вариантов возможных действий — [**Analyse**], а затем нажать [**Quick Search**] для поиска разделов.



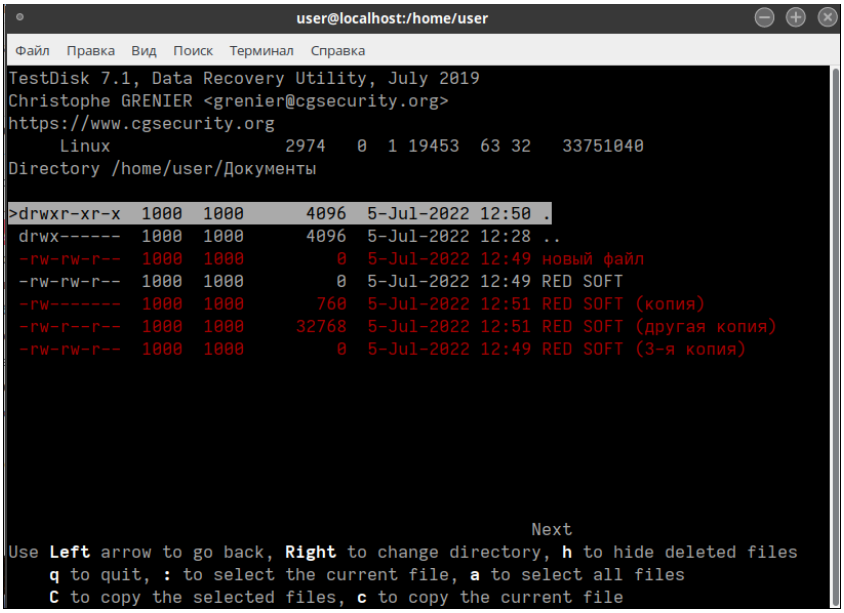
Утилита предложит выбрать раздел, который необходимо проанализировать. Для запуска анализа раздела нажмите [**Deeper Search**].



После завершения анализа будет выведена структура диска, где следует найти нужный раздел с содержимым.

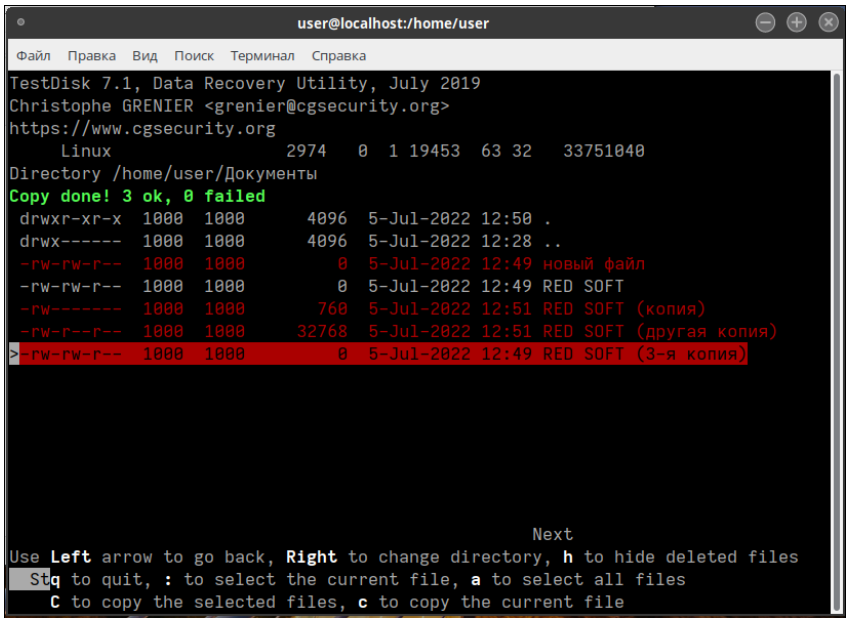


Нажмите **P** для отображения содержимого диска и перейдите в папку, из которой были удалены файлы. Удаленные файлы, подлежащие восстановлению, будут выделены красным цветом.

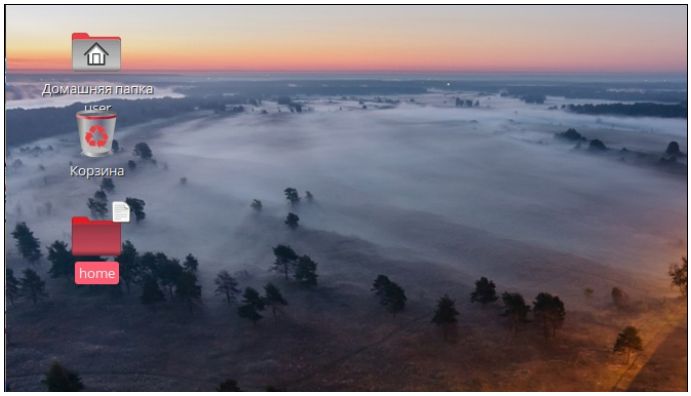


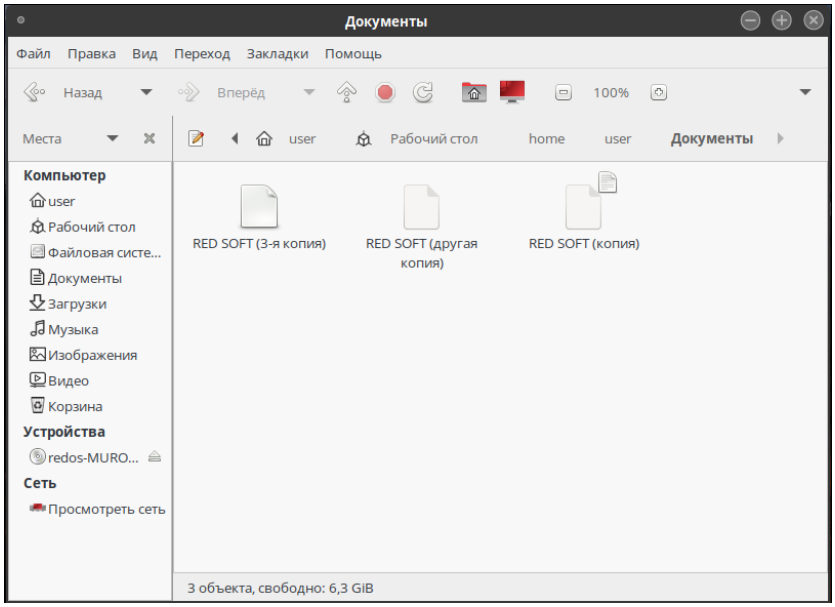
Внизу экрана даны инструкции по восстановлению данных. После копирования удаленных файлов появится список каталогов, в

которые его можно восстановить.



В данном примере файлы были восстановлены на «**Рабочий стол**». Восстановленные файлы отмечены специальным значком.





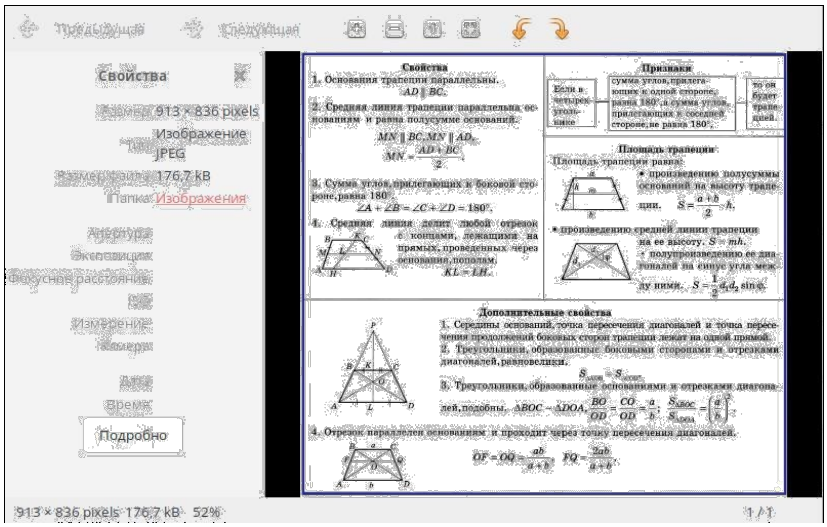
При работе со съемными носителями восстановление удаленных файлов производится несколько проще.

После выбора таблицы разделов диска необходимо выбрать пункт [**Advanced**] для работы с файловой системой. Выберите необходимый раздел и выполните [**Undelete**].

Будут показаны все файлы, содержащиеся на разделе, в том числе и удаленные (отмечены красным цветом).

Внизу экрана также описаны инструкции по восстановлению удаленных файлов. После копирования удаленного файла появится список каталогов, в которые его можно восстановить. В данном примере восстановление удаленного изображения производится в папку «**Изображения**».

```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
 1 * FAT32 LBA               0   2  1 14999  63 32   30719936 [RODIP]
Directory /2019-02-07_13-50-166.jpg
Copy done! 1 ok, 0 failed
 drwxr-xr-x     0     0         0  6-Apr-2022 13:00 System Volume Information
>-rwxr-xr-x     0     0    176658 16-Mar-2022 19:19 2019-02-07_13-50-166.jpg
 -rwxr-xr-x     0     0    141453 16-Mar-2022 19:19 _RAP.JPG
 -rwxr-xr-x     0     0   1911163  1-Feb-2022 21:28 Козко и Чирский - Задачи с парамет
 drwxr-xr-x     0     0         0  6-Apr-2022 10:01 .Trash-1000
```



Утилита **testdisk** - достаточно простой, но мощный инструмент для восстановления различных типов данных. Функционал утилиты также включает исправление таблицы разделов и восстановление загрузочного сектора. Обработке подлежат все типы дисков и разделов, включая LVM-разделы.

Timeshift. Работа со снимками ОС

Создание снимков ОС
Режим RSYNC
Режим BTRFS
Восстановление снимка ОС
Работа с timeshift в командной строке

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: timeshift-21.09.1-1

Timeshift — программа для автоматического периодического создания копий системы (снимков/snapshots).

Timeshift предназначен прежде всего для создания снимков системных файлов и настроек. Пользовательские данные по умолчанию не архивируются, поэтому в случае сбоя системы восстанавливаются системные файлы, а данные пользователей остаются в актуальном состоянии (при условии, что они не были повреждены).

Резервные копии не могут быть восстановлены на уровне отдельных файлов, восстановление всегда происходит в полном объеме настроек **Timeshift**.

Стоит учитывать, что **Timeshift** не предназначена для клонирования ОС с одного ПК на другой путем восстановления из снимка другого ПК.

Timeshift имеет 2 режима работы:

- RSYNC;
- BTRFS.

Вы можете подробнее ознакомиться с работой утилиты **timeshift**, просмотрев наши обучающие видео:

- на **RuTube** — Создание резервных копий и восстановление системы с помощью TimeShift;
- в **Яндекс.Дзен** — Создание резервных копий и восстановление системы с помощью TimeShift;
- в **VK Видео** — Создание резервных копий и восстановление системы с помощью TimeShift.

На наших каналах вы также сможете найти много другой полезной информации.

Создание снимков ОС

Для установки **timeshift** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install timeshift
```

После установки утилита доступна из «**Главного меню**» - «**Системные**» - «**Резервное копирование и восстановление**».

Режим RSYNC

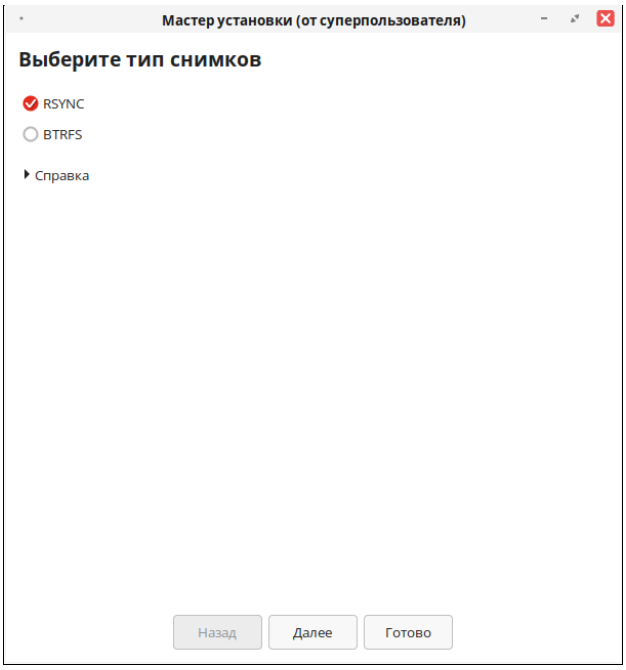
Первый режим является универсальным для всех файловых систем. Основные особенности режима **RSYNC**:

- снимки создаются путём копирования системных файлов при помощи *RSYNC* и создания жёстких ссылок на неизмененные файлы из предыдущего снимка;
- все файлы копируются при создании первого снимка, последующие снимки являются инкрементальными. Неизмененные файлы будут связаны с предыдущим снимком, если он доступен;
- создание первого снимка может занять до *10 минут*;
- системный раздел может быть отформатирован в любой файловой системе. Резервный раздел может быть отформатирован в любой файловой системе Linux, поддерживающей жесткие ссылки. Сохранение снимков на несистемный или внешний диск

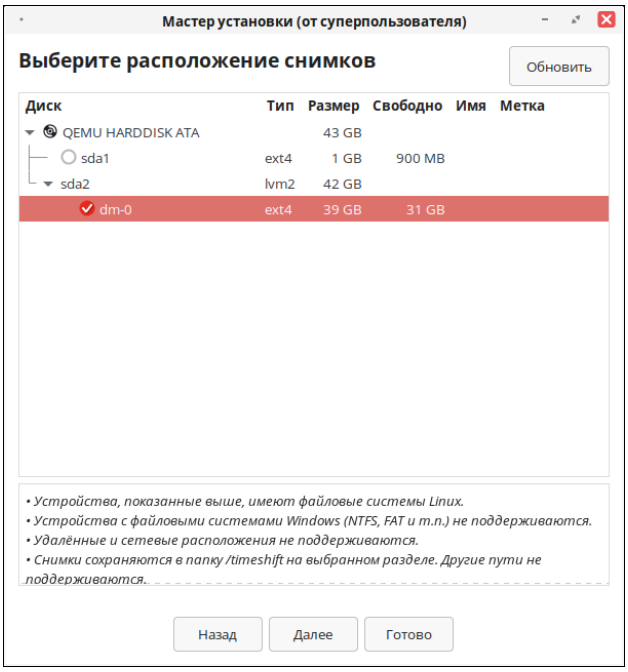
позволяет восстановить систему, даже если системный диск повреждён;

- можно задать исключения для файлов и каталогов для экономии дискового пространства;
- систему необходимо перезагрузить после восстановления снимка.

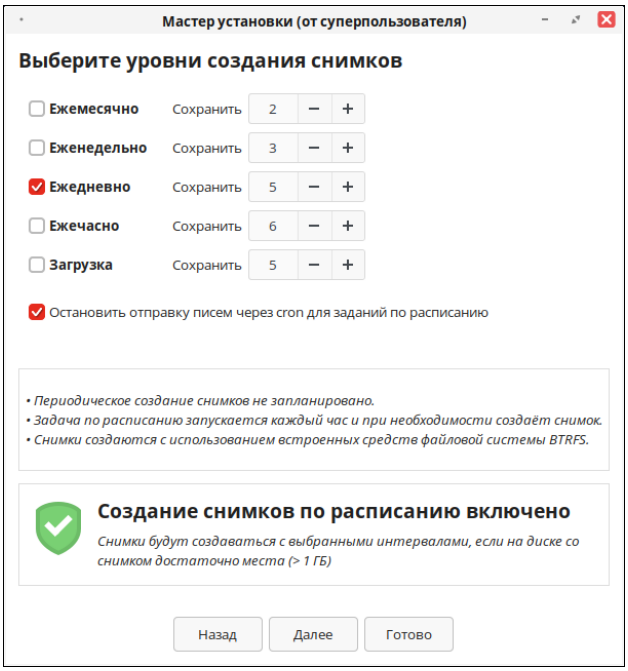
При запуске утилиты **timeshift** выберите тип снимков **RSYNC**.



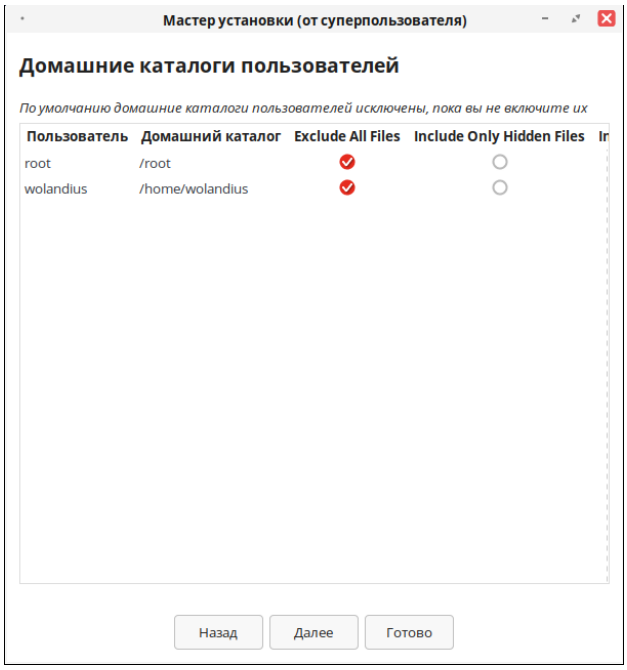
Выберите расположение снимков.



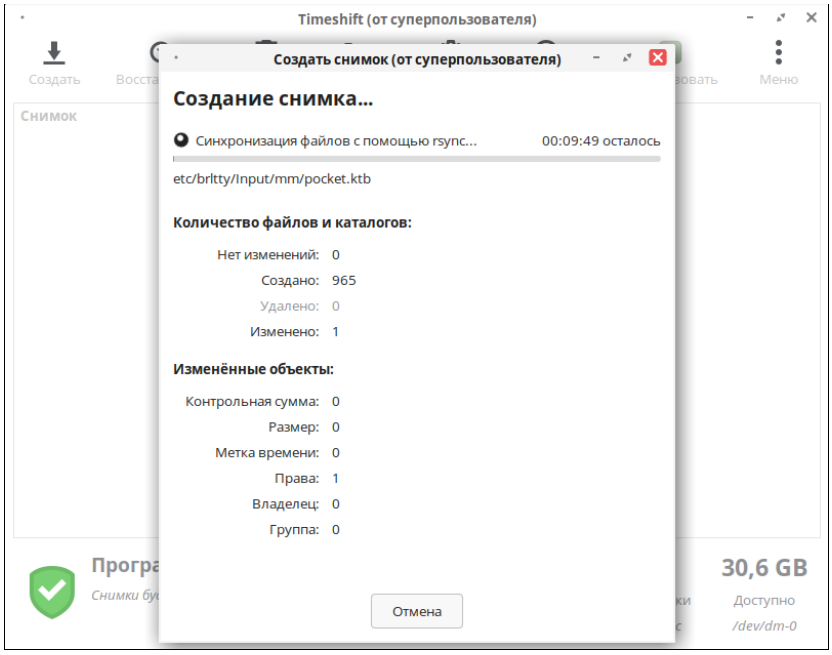
Настройте периодичность создания снимков.



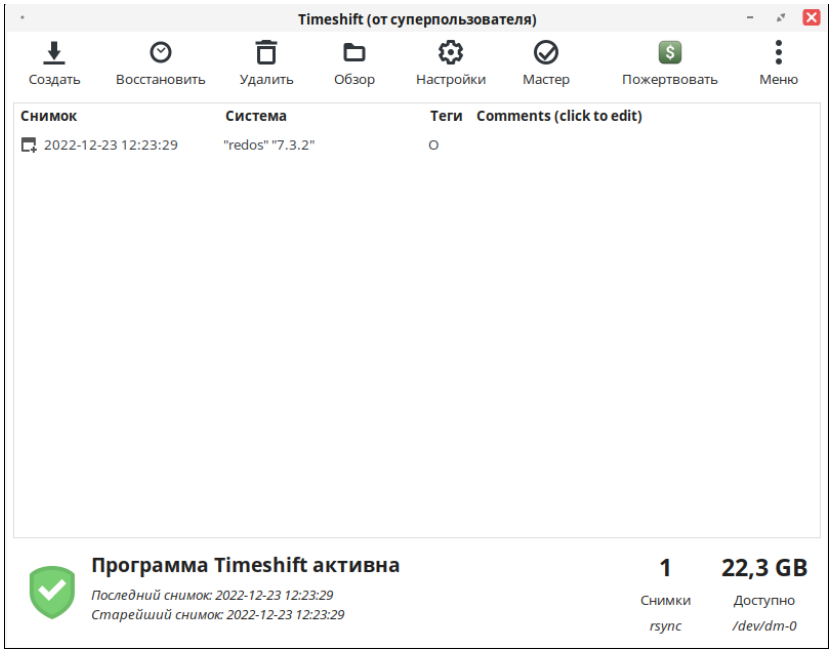
Включите ведение снимков для домашних каталогов пользователей.



Выберите пункт «**Создать**».



После завершения создания снимок появится в списке.



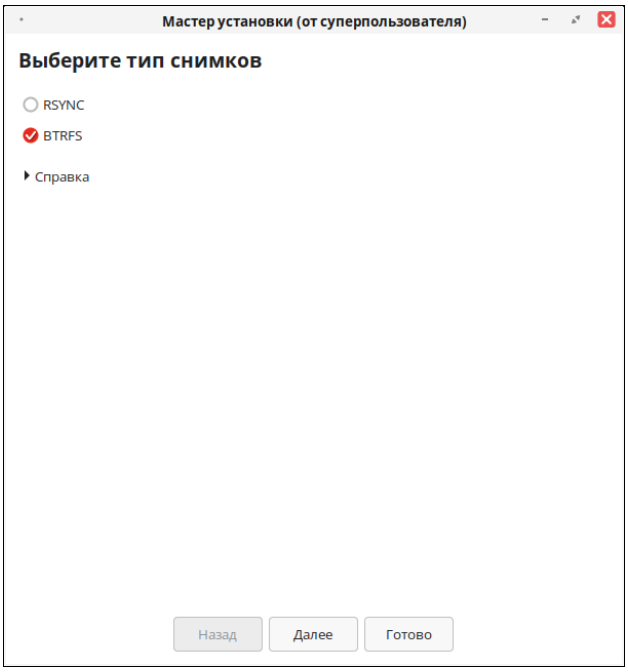
Режим BTRFS

Основные особенности режима **BTRFS**:

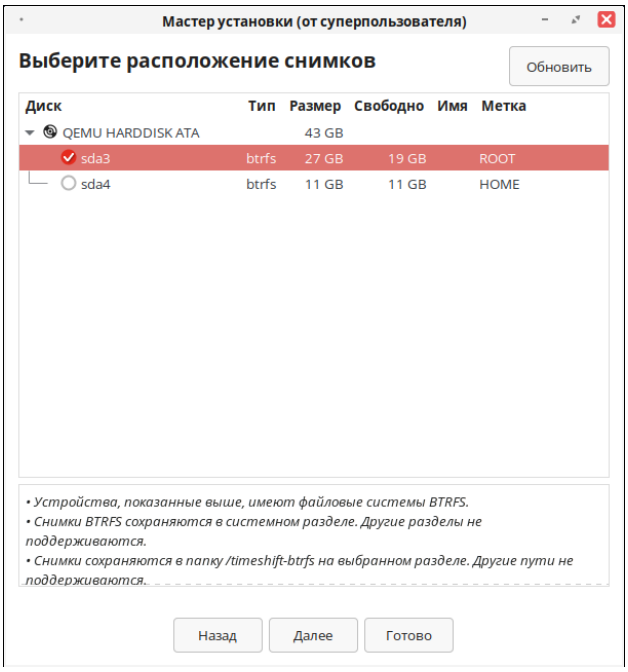
- снимки создаются с использованием встроенных средств файловой системы *BTRFS*;
- снимки создаются и восстанавливаются мгновенно (создание снимков — это атомарная транзакция на уровне файловой системы);
- снимки восстанавливаются путём замены системных подразделов. Поскольку файлы никогда не копируются, не удаляются и не перезаписываются, риск потери данных отсутствует. Существующая система сохраняется как новый снимок после восстановления;
- снимки сохраняются на том же диске, с которого они созданы (системном диске). Хранение на других дисках не поддерживается. Если системный диск выйдет из строя, снимки, хранящиеся на нём, будут потеряны вместе с системой;
- нет возможности исключать файлы и каталоги;
- размер снимков *BTRFS* изначально равен нулю. При изменении системных файлов, данные записываются в новые блоки, которые занимают дисковое пространство (копирование при записи). Файлы в снимке продолжают указывать на исходные блоки данных;
- ОС должна быть установлена на раздел *BTRFS* с разбивкой на подразделы **@** и **@home** (см. Описание процесса разметки диска). Другие виды разделов не поддерживаются;

- снимки можно восстановить без немедленной перезагрузки запущенной системы.

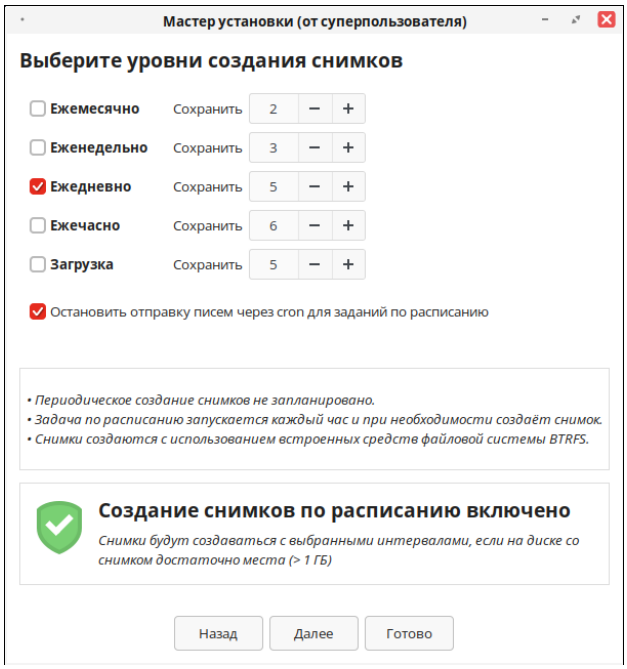
При запуске утилиты **timeshift** выберите тип снимков **BTRFS**.



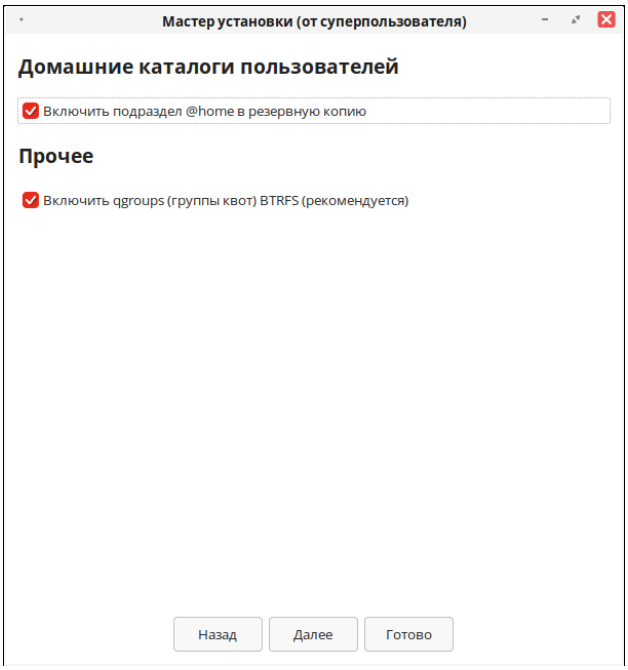
Выберите расположение снимков на том диске, где расположен подтом **@**.



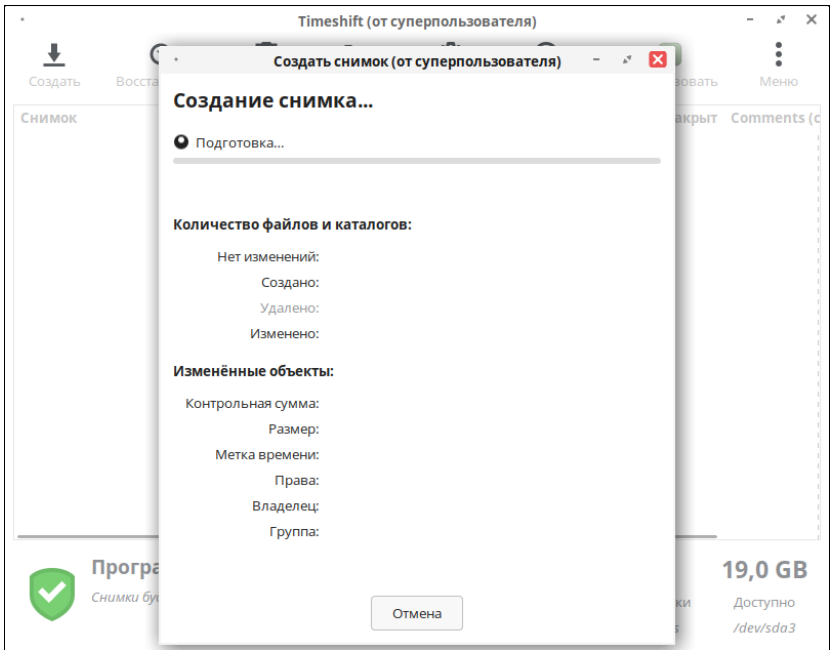
Настройте периодичность создания снимков.



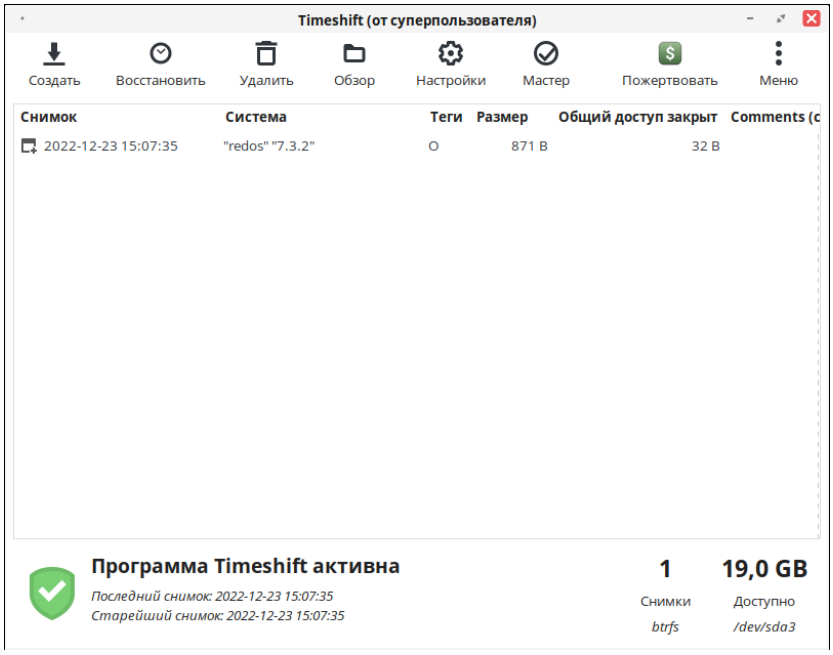
Включите ведение снимков для домашних каталогов пользователей.



Выберите пункт «**Создать**».

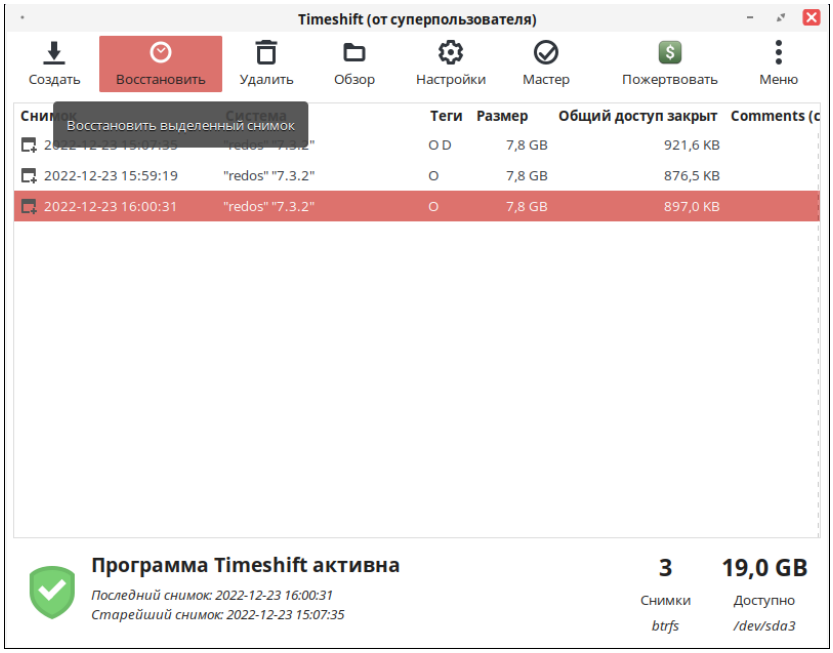


После завершения создания снимок появится в списке.



Восстановление снимка ОС

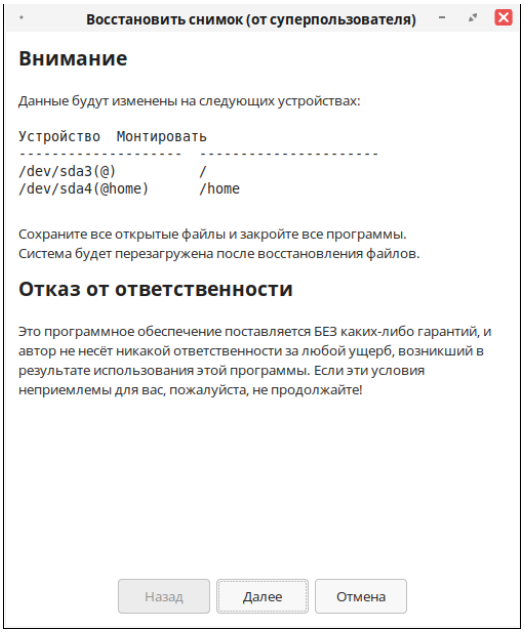
Для восстановления снимка ОС необходимо выбрать нужный снимок ОС и нажать кнопку «**Восстановить**».



Если также необходимо восстановить домашний каталог пользователя, установите соответствующий флаг в открывшемся окне.



После этого будет выведена информация о восстанавливаемых дисках. Нажмите «**Далее**» для запуска процесса восстановления снимка.



После перезагрузки ОС ПК будет работать на выбранном вами снимке ОС.

Работа с timeshift в командной строке

Работа с **timeshift** выполняется с правами администратора системы или суперпользователя root.

Вывод справки о команде осуществляется командой (возможно выполнение с правами локального пользователя):

```
timeshift
```

Если параметры не указаны, например, при создании снимка, значения по умолчанию будут загружены из конфигурации приложения.

Просмотр списка снимков:

```
timeshift --list

/dev/sda3 is mounted at: /run/timeshift/backup, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

/dev/sda4 is mounted at: /run/timeshift/backup-home, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

Device : /dev/sda3
UUID   : f58e67fe-03f2-44e9-8251-f3c7db87b6bf
Path   : /run/timeshift/backup
Mode   : BTRFS
Status : OK
2 snapshots, 19.0 GB free

Num     Name                 Tags  Description
------------------------------------------------------------------------------
0    >  2022-12-23_15-07-35  O
1    >  2022-12-23_15-59-19  O
```

Создание снимка:

```
timeshift --create

Using system disk as snapshot device for creating snapshots in BTRFS mode

/dev/sda3 is mounted at: /run/timeshift/backup, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

/dev/sda4 is mounted at: /run/timeshift/backup-home, options: rw,seclabel,relatime,space_cache,subvolid=5,subvol=/

Creating new backup...(BTRFS)
Saving to device: /dev/sda3, mounted at path: /run/timeshift/backup
Saving to device: /dev/sda4, mounted at path: /run/timeshift/backup-home
Created directory: /run/timeshift/backup/timeshift-btrfs/snapshots/2022-12-23_16-00-31
```

```
Created subvolume snapshot: /run/timeshift/backup/timeshift-btrfs/snapshots/2022-12-23_16-00-31/@
Created directory: /run/timeshift/backup-home/timeshift-btrfs/snapshots/2022-12-23_16-00-31
Created subvolume snapshot: /run/timeshift/backup-home/timeshift-btrfs/snapshots/2022-12-23_16-00-31/@home
Created control file: /run/timeshift/backup/timeshift-btrfs/snapshots/2022-12-23_16-00-31/info.json
BTRFS Snapshot saved successfully (0s)
Tagged snapshot '2022-12-23_16-00-31': ondemand ------------------------------------------------------------------------------
```

Создание снимка, если он запланирован (есть в расписании):

```
timeshift --check
```

Восстановить снимок (параметры будут запрошены в интерактивном режиме):

```
timeshift --restore
```

Восстановить снимок:

```
timeshift --restore --snapshot '2022-12-23_16-00-31'
```

Восстановить определенный снимок в необходимый раздел (для **rsync**):

```
timeshift --restore --snapshot 1 --target /dev/sda2
```

Удалить снимок:

```
timeshift --delete --snapshot '2022-12-23_16-00-31'
```

SyncThing — утилита для синхронизации файлов

Установка
Синтаксис
Команды
Опции
Пример работы

Окружение

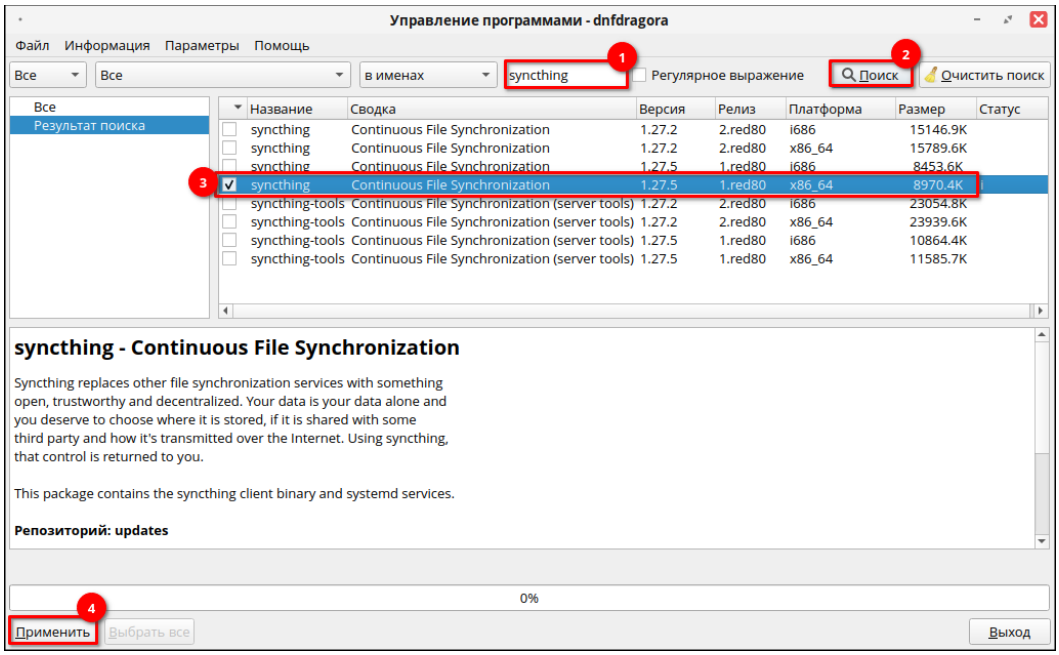
- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: syncthing-1.27.5-1

Syncthing позволяет синхронизировать файлы в двух направлениях на нескольких устройствах. Создание, изменение или удаление файлов на одном компьютере будет автоматически реплицировано на другие устройства. **Syncthing** обменивается данными между компьютерами, когда они одновременно подключаются к сети.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**syncthing**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install syncthing
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
syncthing [<команда>] [<опции>]
```

Команды

Основные команды утилиты:

- **serve** — запустить синхронизацию;
- **generate** — сгенерировать ключ и конфигурацию, затем выйти;
- **decrypt** — расшифровать или проверить зашифрованную папку;
- **cli** — интерфейс командной строки для синхронизации;
- **install-completions** — печать команд для установки дополнений оболочки.

Опции

Основные опции утилиты:

- **--allow-newer-config** — загрузить конфигурационный файл с более новой версией программы;
- **--audit** — записать события в файл аудита с отметками времени в формате ГГГГММДД-ЧЧММСС.log;
- **--auditfile=<file|-|-->** — использовать файл или поток для событий аудита;
- **--browser-only** — открыть веб-интерфейс в браузере для работающего экземпляра syncthing;
- **--device-id** — вывести идентификатор устройства;
- **--generate=<dir>** — сгенерировать ключ и конфигурацию в указанном каталоге;
- **--gui-address=<address>** — переопределить адрес прослушивания графического интерфейса;
- **--gui-apikey=<string>** — переопределить ключ API, необходимый для доступа к GUI/REST API;
- **--gui-password=<password|->** — установить новый пароль аутентификации графического интерфейса для обновления файла конфигурации;
- **--gui-user=<username>** — установить новое имя пользователя для аутентификации графического интерфейса для обновления файла конфигурации;
- **--help, -h** — вывести справку;
- **--home=<dir>** — установить новую конфигурацию и каталог данных;
- **--config=<dir>** — установить каталог конфигурации;
- **--data=<dir>** — установить каталог данных;
- **--logfile=<filename>** — задать имя файла назначения для регистрации;
- **--logflags=<flags>** — выбрать информацию в префиксе строки журнала;
- **--log-max-old-files=<num>** — количество старых файлов, которые нужно сохранить;
- **--log-max-size=<num>** — задать максимальный размер любого файла журнала;
- **--no-browser** — запустить браузер;
- **--no-console** — консольное окно;
- **--no-default-folder** — не создавать папку по умолчанию при создании начальной конфигурации/первом запуске;
- **--no-restart** — не перезапускать syncthing после его закрытия;
- **--no-upgrade** — отключить автоматическое обновление;
- **--paths** — распечатать пути, используемые для конфигурации, ключей, базы данных, переопределений графического интерфейса, папки синхронизации по умолчанию и файла журнала;
- **--paused** — запуск устройства и пауза;
- **--reset-database** — удалить все данные из базы данных и возвратить ее к исходному состоянию, выполнив полное повторное сканирование и повторную синхронизацию;
- **--reset-deltas** — сбросить все изменения или обновления, которые были внесены в систему с момента последнего сброса;
- **--skip-port-probing** — пропустить сканирование портов при выполнении операций;
- **--unpaused** — запустить или выполнить действие без ожидания;
- **--upgrade** — обновить программу до новой версии;
- **--upgrade-check** — проверить наличие обновлений или новых версий;
- **--upgrade-to=<url>** — обновить до указанного URL;
- **--verbose** — выводить подробные сообщения или логи для отладки;
- **--version** — показать текущую версию syncthing;
- **--to=<dir>** — указать каталог или директорию для перемещения или копирования;
- **--verify-only** — выполнять только проверку или верификацию, без выполнения операции;
- **--password=<pw>** — установить пароль для аутентификации или доступа;
- **--folder-id=<id>** — указать идентификатор папки для операции;
- **--token-path=<file>** — указать путь к файлу токена для доступа или аутентификации;
- **--continue** — продолжить выполнение операции или действия без прерывания.

Пример работы

Для запуска сервера выполните следующий алгоритм действий:

1. Создайте файл **/etc/systemd/system/syncthing@.service** (потребуются права **администратора**):

```
nano /etc/systemd/system/syncthing@.service
```

2. Заполните файл следующим содержанием и сохраните его:

```
[Unit]
Description=Syncthing - Open Source Continuous File Synchronization for %I
Documentation=man:syncthing(1)
```

```
After=network.target

[Service]
User=%i
ExecStart=/usr/bin/syncthing -no-browser -gui-address="0.0.0.0:8384" -no-restart -logflags=0
Restart=on-failure
SuccessExitStatus=3 4
RestartForceExitStatus=3 4

# Hardening
ProtectSystem=full
PrivateTmp=true
SystemCallArchitectures=native
MemoryDenyWriteExecute=true
NoNewPrivileges=true

[Install]
WantedBy=multi-user.target
```

3. Перезагрузите список служб systemd:

```
sudo systemctl daemon-reload
```

4. Запустите службу синхронизации (если запуск службы необходимо разрешить только определенному пользователю, замените $USER на имя пользователя):

```
sudo systemctl start syncthing@$USER
```

5. Добавьте службу синхронизации в автозагрузку:

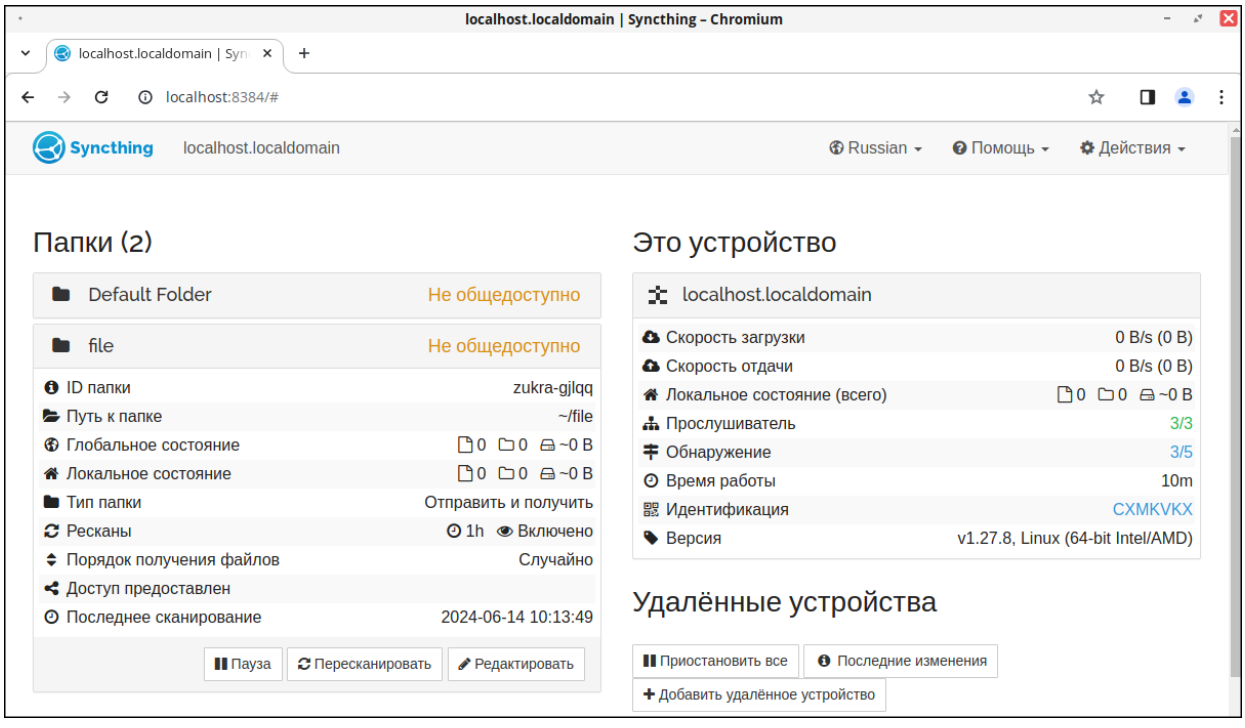
```
sudo systemctl enable syncthing@$USER
```

6. Проверьте работу службы синхронизации:

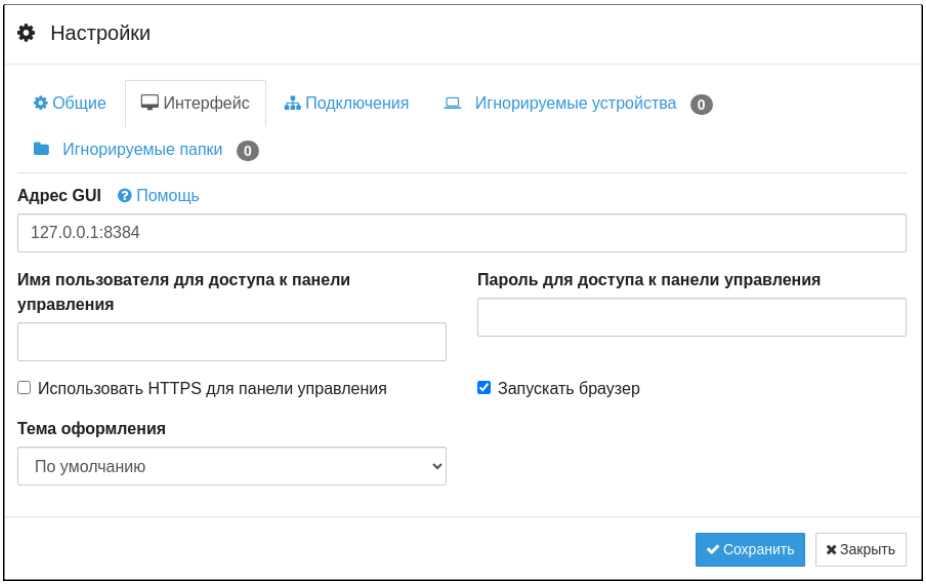
```
sudo systemctl status syncthing@$USER
```

В статусе должно отображаться active (running).

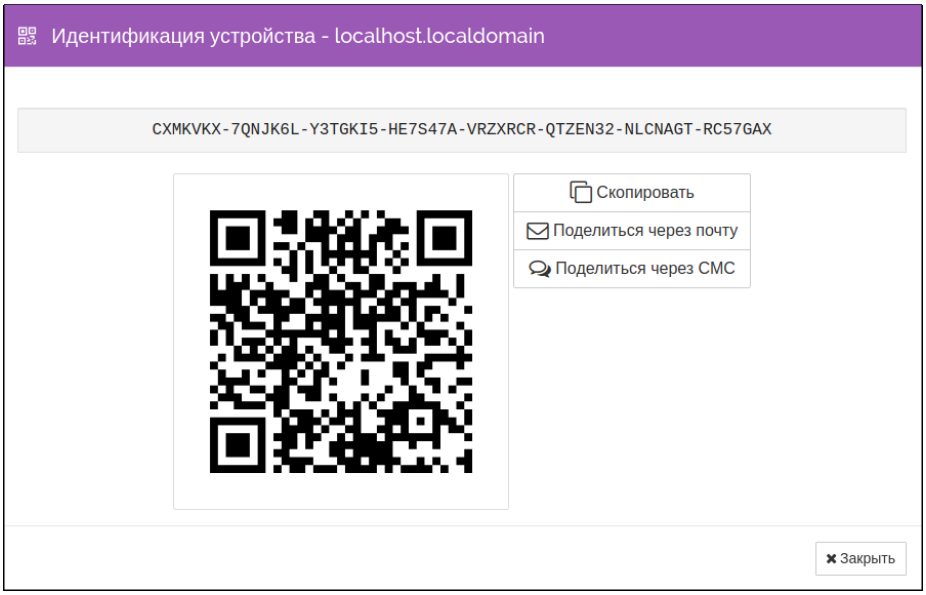
7. Перейдите в браузер. По умолчанию служба доступна по адресу: localhost:8384.



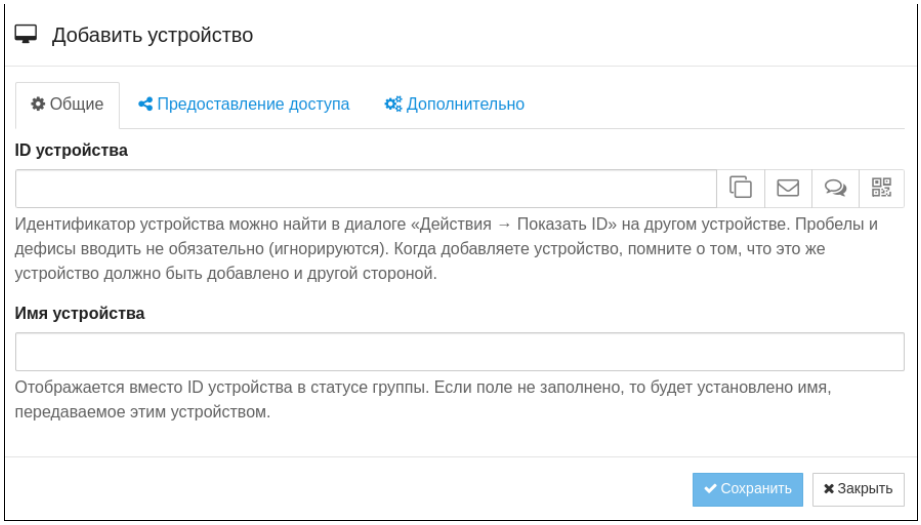
8. В целях безопасности обязательно установите имя пользователя и пароль для доступа к панели управления: «**Действия**» — «**Настройки**» — «**Интерфейс**».



9. Для добавления удаленного устройства определите его ID. Для этого на удаленном компьютере нажмите: «**Действия**» — «**Показать ID**».

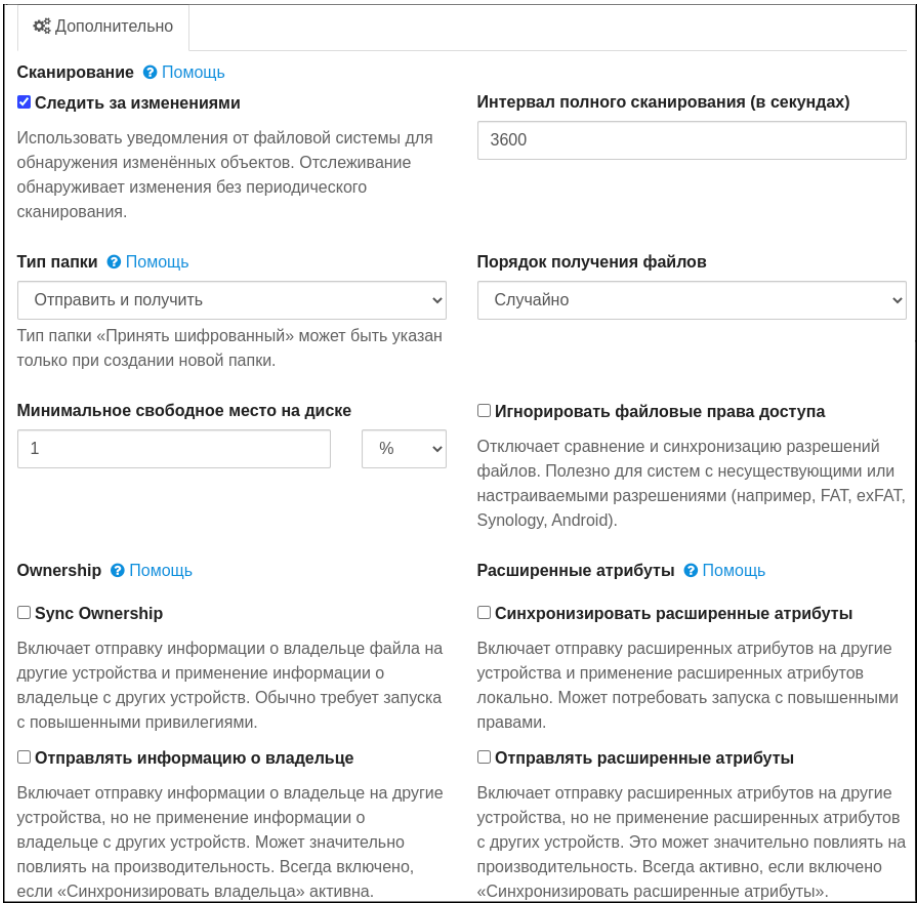


10. Укажите данные нового устройства в соответствующих полях на сервере и нажмите «**Сохранить**». После этого на удаленном устройстве появится запрос на добавление. Для связки двух устройств примите запрос.



По умолчанию создается общая папка ~/Sync. Для папок можно настроить разграничение доступа, управление версиями, шаблоны игнорирования, режим синхронизации (только принимать/отправлять или всё вместе) и другие. Программа способна сама найти кратчайший путь до удаленного устройства. Она может выполнять поиск в глобальной сети с помощью релеев или в локальной сети.

Можно настроить свой релей и не связываться с публичными серверами.



Burp - программа резервного копирования

Возможности
Установка
Синтаксис
Опции сервера
Опции клиента
Конфигурационные файлы
Запуск сервера
Создание и настройка клиента
Отключение клиента
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: burp-server-3.1.4-2, burp-client-3.1.4-2

Burp — это программа сетевого резервного копирования и восстановления данных. Она экономит сетевой трафик и объем пространства, используемого каждой резервной копией, с помощью *librsync*. Программа имеет клиент-серверную архитектуру. Сервер в **burp** представляет собой центральное хранилище резервных копий, а клиенты выполняют резервное копирование и восстановление данных через сервер.

С документацией можно ознакомиться на официальном сайте.

Возможности

Основные возможности **burp**:

- серверный режим;
- клиентский режим;
- дельта-дифференцирование с помощью *librsync*;
- сетевые резервные копии;
- ограничение скорости работы сети;
- создание резервных копий и восстановление файлов, каталогов, символических ссылок, жёстких ссылок, fifos, узлов, разрешений и временных меток;
- сжатие хранилища и сети с использованием zlib;
- возможность продолжения прерванного резервного копирования;
- шифрование связи между клиентом и сервером с помощью SSL;
- автоматическая подпись центра сертификации SSL и клиентского сертификата;
- шифрование файлов на стороне клиента;
- планирование;
- уведомления об успешном/неудачном резервном копировании по электронной почте;
- оперативный мониторинг ncurses на сервере;
- поддержка чтения/записи Fifo;
- клиентские скрипты до/после резервного копирования/восстановления;
- несколько периодов хранения;
- дедупликация данных хранилища;
- автоматическое обновление клиента.

Установка

Установить burp можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**burp**» и отметьте флагом пакеты **burp-client** и **burp-server** последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.

Для установки **burp-client** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install burp-client
```

Для установки **burp-server** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install burp-server
```

Установите зависимости:

```
sudo dnf install uthash-devel make gcc librsync-devel openssl-devel libacl-devel ncurses-devel zlib-devel autoconf automake libtool
```

Синтаксис

Программа доступна для запуска через терминал при помощи команды следующего вида:

```
burp [<опции>]
```

Опции сервера

Основные опции сервера:

- **-c <path>** — указать путь к файлу конфигурации (по умолчанию используется **/etc/burp/burp.conf)**;
- **-d <path>** — указать путь к клиенту в мониторе состояния;
- **-o <option>** — переопределить указанную конфигурационную опцию;
- **-F** — запустить сервер в режиме переднего плана (сервер перейдет в фоновый режим, если не указывать эту опцию);
- **-g** — сгенерировать исходные сертификаты центра сертификации и завершить работу;
- **-h** — вывести справку;
- **-i** — вывести индекс символов и завершить работу;
- **-n** — не создавать дочерних процессов (подразумевает -F);
- **-Q** — не выводить журналирование в stdout;
- **-t** — запустить проверку синтаксиса файла конфигурации (тестовый запуск);
- **-v** — вывести записи журнала в *stdout*;
- **-V** — вывести версию.

При использовании опции ''**-a c**'':

- **-C <client>** — запустить сервер, разделенный через подключение от клиента.

Опции клиента

Основные опции клиента:

- **-a <action>** — выбрать дополнительные действия:
    - **b** — создать резервную копию;
    - **delete** — удалить;
    - **d** — показать различия;
    - **e** — провести оценку;
    - **l** — показать список;
    - **L** — показать длинный список;
    - **m** — провести мониторинг интерфейса;
    - **p** — показать список в формате для парсинга;
    - **r** — восстановить;
    - **R** — восстановить (с учетом порядка путей из стандартного потока ввода);
    - **s** — монитор состояния;
    - **S** — снимок монитора состояния;
    - **t** — резервное копирование по времени;
    - **T** — проверить таймер резервного копирования;
    - **v** — проверить;
    - **V** — проверить (с учетом порядка путей из стандартного потока ввода);
- **-b <number>** — указать номер резервной копии, по умолчанию используется последняя;
- **-c <path>** — указать путь к файлу конфигурации, стандартно /etc/burp/burp.conf;
- **-d <directory>** — установить директорию для восстановления или просмотра;
- **-o <option>** — установить переопределение опции конфигурации;
- **-f** — установить разрешение на перезапись файлов при восстановлении;
- **-h** — вывести справку;
- **-i** — вывести индекс символов;
- **-q <max secs>** — установить задержку перед началом запланированного резервного копирования;
- **-Q** — отключить логирования в stdout;
- **-r|-R <regex>** — указать регулярное выражение для выбора файлов;

- **-s <number>** — удалить пути для использования при восстановлении;
- **-t** — проверить синтаксис файла конфигурации;
- **-V** — вывести версию программы;
- **-v** — вывести логи на стандартный вывод.

Дополнительные опции для использования с ''**-a S**'':

- **-C <client>** — отобразить информацию о клиенте;
- **-b <number>** — просмотреть файлы, доступные для списка в определенной резервной копии;
- **-d <path>** — просмотреть путь в резервной копии;
- **-l <path>** — файл лога для монитора статуса;
- **-z <file>** — вывести файл лога из резервной копии.

Конфигурационные файлы

Конфигурационные файлы и директории для программы **burp** играют ключевую роль в настройке процесса резервного копирования и восстановления.

В конфигурационном файле **/etc/burp/burp-server.conf** содержатся настройки сервера, такие как порт сервера, пути к директориям для хранения резервных копий и политики резервного копирования.

В папке **/etc/burp/clientconfdir/*** содержатся настройки резервного копирования для каждого клиента.

В конфигурационном файле **/etc/burp/burp.conf** содержатся настройки клиента для подключения к серверу. Директории для резервной копии указываются с помощью команды **include** в конфигурационном файле клиента: **/etc/burp/burp.conf**.

Резервные копии хранятся в папке **/var/spool/burp**.

Запуск сервера

Сервер **burp** используется для хранения резервных копий данных. Для запуска burp-сервера используйте команду (можно указывать свои конфигурационные файлы):

```
sudo burp -c /etc/burp/burp-server.conf
```

После выполнения команды сервер готов к подключению клиентов. Клиенты и сервер могут находиться как на одной машине, так и на разных.

Создание и настройка клиента

Клиенты отправляют свои данные на сервер для создания резервных копий и для восстановления информации в случае потери данных или необходимости восстановления системы.

Для создания клиента выполните следующий алгоритм действий:

1. Каждый клиент представлен файлом в каталоге **/etc/burp/clientconfdir** на сервере. Для добавления клиента с именем <имя_клиента> необходимо создать на сервере файл с именем **/etc/burp/clientconfdir/<имя_клиента>**.

```
nano /etc/burp/clientconfdir/<имя_клиента>
```

2. Задайте пароль клиенту в этом файле, добавив строку:

```
password = <пароль>
```

3. У клиента в файле **/etc/burp/burp.conf** в параметре **cname** укажите имя клиента, в параметре **password** — пароль, в параметре **server** — адрес сервера.

```
server = localhost:4971 password = <пароль> cname = <имя_клиента>
```

4. При первом подключении нового клиента к серверу он выполнит обмен SSL-сертификатами.

Отключение клиента

Для отключения клиента от сервера удалите файл **/etc/burp/clientconfdir/<имя_клиента>**:

```
rm /etc/burp/clientconfdir/<имя_клиента>
```

Примеры использования

1. Запустить резервное копирование:

```
sudo burp -a b
```

2. Вывести список резервных копий с датами:

```
sudo burp -a l
```

3. Показать файлы второй резервной копии:

```
sudo burp -a l -b 2
```

4. Восстановить все файлы из второй резервной копии в корневую папку:

```
sudo burp -a r -b 2 -d /
```

5. Восстановить файлы второй резервной копии, принудительно перезаписывая одноимённые файлы, в корневую папку:

```
sudo burp -a r -b 2 -d / -f
```

6. Восстановить файлы, которые соответствуют регулярному выражению "a_*" (начинаются на «a_»), из второй резервной копии в корневую папку:

```
sudo burp -a r -b 2 -r a_* -d /
```

7. Настройки резервного копирования очень разнообразные, можно исключать из резервной копии файлы, у которых путь соответствует регулярному выражению, или исключать файлы с заданными расширениями.

Можно настроить резервное копирование по расписанию с помощью crontab:

```
MAILTO="" 0,20,40 * * * * root /usr/sbin/burp -a b
```

После настройки каждые 20 минут будет производиться резервное копирование и отправляться сообщение владельцу файла *crontab*.

Создание бэкапов с помощью Butterfly Backup

Возможности
Установка
Синтаксис
Команды
Опции
Пример использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО**: butterfly-backup-1.12-2

Butterfly Backup — это инструмент для резервного копирования (РК), который использует **rsync** для синхронизации и сохранения файлов на сервере. Он обеспечивает гибкость в настройке заданий РК.

Butterfly Backup позволяет выполнять полные и инкрементные резервные копии, а также предоставляет возможность восстановления данных.

Возможности

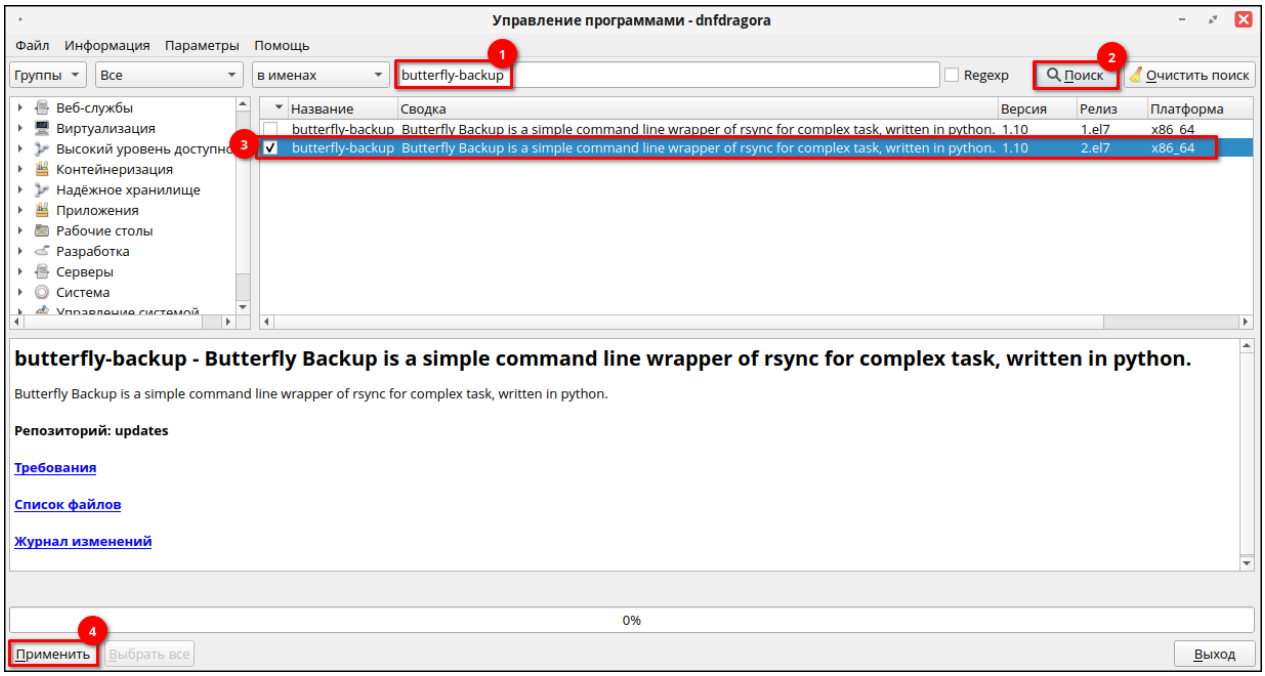
Основные возможности:

- **автоматизация заданий** — позволяет настроить автоматическое выполнение РК в определённое время с использованием cron или других планировщиков заданий;
- **управление версиями** — сохраняет историю изменений файлов, что позволяет восстановить предыдущие версии файлов при необходимости;
- **фильтрация данных** — предоставляет возможность исключать из РК определённые файлы или директории с помощью фильтров;
- **логирование** — записывает подробные логи операций, что облегчает отслеживание процесса РК и устранение возможных проблем;
- **централизованное хранение** — использует центральный сервер для сбора и хранения резервных копий от различных клиентов;
- **резервное копирование и восстановление системы** — позволяет выполнять РК всей системы и её восстановление на другом оборудовании или виртуальной машине;
- **просмотр содержимого резервных копий** — предоставляет возможность детально просматривать содержимое каждой резервной копии;
- **шифрование** — обеспечивает безопасность данных путём шифрования резервных копий перед их передачей на сервер или хранением.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**butterfly-backup**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install butterfly-backup
```

Для вывода справочной информации о доступных опциях и аргументах **butterfly-backup** воспользуйтесь командой:

```
bb --help
```

Для получения документации через man воспользуйтесь командой:

```
man bb
```

Синтаксис

Программа доступна для запуска через терминал при помощи команды следующего вида:

```
bb [<команды>] [<опции>]
```

Команды

Основные команды:

- **config** — настройка параметров конфигурации;
- **backup** — запуск процесса РК;
- **restore** — восстановление данных из резервной копии;
- **archive** — архивация, сжатие и упаковка данных для долгосрочного хранения;
- **list** — список доступных резервных копий или архивов;
- **export** — экспорт данных или настроек.

Опции

Опции команды config

Основные опции команды **config**:

Инициализация конфигурации:

- **--new, -n** — сгенерировать новую конфигурацию;
- **--remove, -r** — удалить существующую конфигурацию;
- **--init <каталог>, -i <каталог>** — изменить местоположение резервных копий;
- **--delete-host <каталог>, -D <каталог>** — удалить все записи для конкретного хоста в каталоге;
- **--clean <каталог>, -c <каталог>** — очистить каталог, если он поврежден, установив значения по умолчанию;
- **--delete-backup -b** — удалить определенный идентификатор РК из каталога.

Развертывание конфигурации:

- **--deploy <хост>, -d <хост>** — развернуть конфигурацию на удаленном хосте, указав его имя или IP-адрес;
- **--user <имя_пользователя>, -u <имя_пользователя>** — указать пользователя удаленного хоста.

Опции команды backup

Основные опции команды **backup**:

- **--computer <хост>, -c <хост>** — имя хоста или IP-адрес для РК;
- **--list <список>, -L <список>** — файл со списком удаленных хостов или IP-адресов для резервного копирования;
- **--destination <каталог>, -d <каталог>** — каталог назначения для РК;
- **--mode <значение>** — режим РК. Возможные значения:
  - **full** — полное резервное копирование;
  - **incremental** — добавочное РК выполняется на основе последней резервной копии;
  - **differential** — добавочное РК выполняется на основе последней полной резервной копии;
  - **mirror** — режим зеркалирования, при котором структура каталогов источника будет точно воспроизведена в пункте назначения.
- **--data <значение>, -D <значение>** — тип данных для РК. Возможные значения:
  - **user** — пользовательские данные;
  - **config** — конфигурационные файлы;
  - **log** — журналы;
  - **application** — данные приложений;
  - **system** — система.
- **--custom-data <путь>, -D <путь>** — пользовательский каталог для РК;
- **--user <имя_пользователя>, -u <имя_пользователя>** — имя пользователя для авторизации на удаленном хосте;
- **--type <тип_ОС>, -t <тип_ОС>** — тип операционной системы для РК. Возможные значения:
  - **unix** — все ос UNIX (Linux, BSD, Solaris);
  - **windows** — Windows Vista или более поздней версии;
  - **macos** — MacOSX 10.8 или выше.
- **--compress, -z** — сжимать данные;
- **--retention [<дни> [<количество>], -r [<дни> [<количество>]** — период хранения резервных копий (в днях) и минимальное количество хранимых резервных копий;
- **--parallel <количество>, -p <количество>** — количество параллельных заданий;
- **--timeout <значение>**, **-T <значение>** — задержка ввода/вывода в секундах;
- **--skip-error**, **-e** — пропускать ошибки;
- **--rsync-path <путь>, -R <путь>** — пользовательский путь для РК;
- **--bwlimit, -b** — ограничение пропускной способности в КБ/с;
- **--ssh-port, -P** — пользовательский SSH-порт;
- **--exclude <шаблон>, -E <шаблон>** — шаблон для исключения файлов;

- **--start-from <ID>, -s <ID>** — новая резервная копия на основании другой резервной копии по ее ID.

Опции команды restore

Основные опции команды **restore**:

- **--catalog <каталог>, -C <каталог>** — указать каталог, где хранятся резервные копии;
- **--backup-id <ID>, -i <ID>** — указать ID резервной копии для восстановления;
- **--last, -L** — использовать последнюю доступную резервную копию;
- **--user <имя_пользователя>, -u <имя_пользователя>** — имя пользователя для авторизации на удаленном хосте, где происходит восстановление;
- **--computer <имя_хоста>, -c <имя_хоста>** — указать имя хоста или IP-адрес для выполнения восстановления;
- **--type <тип_ОС>** — указать тип операционной системы для выполнения восстановления: Unix, Windows или MacOS;
- **--timeout <значение>, -T <значение>** — указать задержку ввода/вывода в секундах;
- **--mirror, -m** — режим зеркалирования, при котором структура каталогов источника будет точно воспроизведена в пункте назначения;
- **--skip-error, -e** — пропускать ошибки;
- **--rsync-path <путь>, -R <путь>** — пользовательский путь к резервной копии;
- **--bwlimit, -b** — ограничение пропускной способности в КБ/с;
- **--ssh-port, -P** — указать пользовательский SSH-порт;
- **--exclude <шаблон>, -E <шаблон>** — указать шаблон для исключения файлов;
- **--files <файлы>, -f <файлы>** — восстанавливать только указанные файлы.

Опции команды archive

Основные опции команды **archive:**

- **--catalog <каталог>, -C <каталог>** — каталог с резервной копией;
- **--days <дни>, -D <дни>** — количество дней для хранения архива;
- **--destination <каталог>, -d <каталог>** — каталог назначения для архива.

Опции команды list

Основные опции команды **list**:

- **--catalog <каталог>, -C <каталог>** — отобразить список резервных копий из указанного каталога;
- **--backup-id <ID>, -i <ID>** — выводить ID резервной копии;
- **--archived, -a** — показывать только архивированные резервные копии;
- **--cleaned, -c** — отобразить только очищенные резервные копии;
- **--computer <имя_хоста>, -H <имя_хоста>** — выводить только совпадающие имена хоста или IP-адреса;
- **--detail <ID>, -d <ID>** — отобразить подробную информацию о файлах и папках для указанного ID резервной копии;
- **--oneline, -o** — выводить информацию в одной строке.

Опции команды export

Основные опции команды **export:**

- **--catalog <каталог>, -C <каталог>** — каталог с резервной копией;
- **--backup-id <ID>, -i <ID>** — идентификатор конкретной резервной копии для экспорта;
- **--all, -A** — экспортирует все резервные копии;
- **--destination <каталог>, -d <каталог>** — каталог назначения, куда будут экспортированы данные;

- **--mirror, -m** — режим зеркалирования, при котором структура каталогов источника будет точно воспроизведена в пункте назначения;
- **--cut, -c** — удалить исходные данные после экспорта;
  --include <шаблон>, -I <шаблон> — паттерны включения определенных файлов или каталогов в экспорт;
- **--exclude <шаблон>, -E <шаблон>** — паттерны исключения определенных файлов или каталогов из экспорта;
- **--timeout <значение> , -T <значение>** — задержка ввода/вывода в секундах;
- **--skip-error, -e** — пропускать ошибки во время экспорта;
- **--rsync-path <путь>, -R <путь>** — пользовательский путь для экспорта;
- **--bwlimit, -b** — ограничение пропускной способности в КБ/с;
- **--ssh-port, -P** — пользовательский порт SSH для подключения.

Дополнительные опции

Дополнительные опции:

- **-h, --help** — отобразить справку;
- **--verbose, -v** — включить подробный режим;
- **--log, -l** — создать журналы логов;
- **--dry-run, -N** — режим предварительного запуска;
- **-version, -V** — показать версию.

Пример использования

Рассмотрим настройку сервера и удаленного хоста для создания РК с помощью **bb**.

1. Генерация SSH ключей. Сгенерируйте пару ключей:

```
ssh-keygen -t rsa Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa
Your public key has been saved in /home/user/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:7L7L6TLN6Lqj6L7PLkLVLPL/LDLFL/iaLA9Bc user@localhost.localdomain
```

В процессе генерации SSH ключей будут заданы следующие вопросы:

- **Enter file in which to save the key (/home/user/.ssh/id_rsa)**: укажите, куда сохранить файл закрытого ключа. По умолчанию он будет сохранен в папку **~/.ssh** с именем **id_rsa**. Имя файла можно изменить.
- **Enter passphrase (empty for no passphrase)**: установите пароль для ключа. Пароль используется для дополнительной защиты ключа. Если пароль не требуется, нажмите Enter.
- **Enter same passphrase again**: если пароль был задан, его необходимо повторить, чтобы избежать возможных опечаток.

2. Передача **SSH-ключей на удаленный хост.** После генерации ключей необходимо передать открытый ключ на удаленный хост. Для этого выполните команду вида:

```
bb config --deploy <IP-адрес> --user <имя_пользователя>
```

где:

<IP-адрес> — IP-адрес удаленного хоста;

<имя_пользователя> — имя пользователя, с правами которого будет выполняться РК.

```
 bb config --deploy 192.168.2.15 --user userCopying configuration to 192.168.2.15; write the password:
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/id_rsa.pub"
The authenticity of host ' 192.168.2.15 (192.168.2.15)' can't be established.
ED25519 key fingerprint is SHA256:PK4OB5HgQpPel67ag9bvi2YgVpD1xaIayo/A.
```

```
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
user@192.168.2.15's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'user@192.168.2.15'"
and check to make sure that only the key(s) you wanted were added.success: Configuration copied successfully on 192.168.2.15!
```

3. Резервное копирование домашнего каталога пользователя. В качестве примера создайте резервную копию каталога /home на удаленном хосте <IP-адрес> от имени пользователя user. Убедитесь, что каталог ~/backups существует, или создайте его перед выполнением команды.

```
bb backup --computer 192.168.2.15 --data user --type unix --destination ~/backups --user user# 10.81.101.178:22 SSH-2.0-
OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
# 10.81.101.178:22 SSH-2.0-OpenSSH_9.6
Start backup  192.168.2.15success: Command rsync -ah --no-links user@192.168.2.15:/home /backups/192.168.2.15/2024_08_27__15_54
```

4. Просмотр списка резервных копий. Для просмотра списка резервных копий используйте следующую команду, заменив ~/backups на фактический путь к папке резервных копий:

```
bb list --catalog ~/backups BUTTERFLY BACKUP CATALOG

Backup id: f0e0b12c-656d-11ef-beea-080027d4cbd8
Hostname or ip:  192.168.2.15
Timestamp: 2024-08-28 21:47:13

Backup id: 0f442602-656f-11ef-83c6-080027d4cbd8
Hostname or ip:  192.168.2.15
Timestamp: 2024-08-28 21:55:14

(END)
```

5. Для получения подробной информации о резервной копии используйте команду:

```
bb list --catalog ~/backups --backup-id f0e0b12c-656d-11ef-beea-080027d4cbd8 Backup id: f0e0b12c-656d-11ef-beea-
080027d4cbd8
Hostname or ip:  192.168.2.15
Type: full
Timestamp: 2024-08-28 21:47:13
Start: 2024-08-28 21:47:13
Finish: 2024-08-28 21:47:28
OS: unix
ExitCode: 0
Path: /home/user/backups/ 192.168.2.15/2024_08_28__21_47
List: home
```

где:

- f0e0b12c-656d-11ef-beea-080027d4cbd8 — это идентификатор РК, который был получен на предыдущем шаге.

6. Для просмотра файлов в конкретной РК используйте команду:

```
bb list --catalog ~/backups --detail f0e0b12c-656d-11ef-beea-080027d4cbd8
```

7. Для восстановления файлов из определённой резервной копии, используйте команду:

```
bb restore --catalog ~/backups --last --user user --computer 192.168.2.15 --type unix--verbose debug: Build a rsync command
debug: Command flags are: rsync -ahu --no-perms --no-owner --no-group -vP --log-file=/home/user/backups/
192.168.2.15/2024_08_28__21_47/restore.log
Want to do restore path /home/user/backups/192.168.2.15/2024_08_28__21_47/home/*?
To continue? [y/N] y
Start restore  192.168.2.15
debug: rsync command: rsync -ahu --no-perms --no-owner --no-group -vP --log-
file=/home/user/backups/192.168.2.15/2024_08_28__21_47/restore.log /home/user/backups/192.168.2.15/2024_08_28__21_47/home/*
```

```
user@192.168.2.15:/home
 sending incremental file list
 user/.cache/
 user/.config/
 user/.local/share/

 sent 269,43K bytes  received 711 bytes  180,09K bytes/sec
 total size is 891,06M  speedup is 3.298,53
 success: Command rsync -ahu --no-perms --no-owner --no-group -vP --log-
file=/home/user/backups/192.168.2.15/2024_08_28__21_47/restore.log /home/user/backups/192.168.2.15/2024_08_28__21_47/home/* user@
192.168.2.15:/home
```

8. Для архивации старых резервных копий, которые старше определённого количества дней, используйте:

```
bb archive --catalog ~/backups --days 365 --destination
```

9. Для копирования всех резервные копий в другую папку используйте:

```
bb export --catalog <каталог_с_РК> --all --destination <каталог_для_экспорта> Start export all_backup success: Command rsync -
ahu --no-perms --no-owner --no-group --safe-links /home/user/backups/ /home/user/backups1
```

Rescuezilla - программа для создания и восстановления резервных копий

Установка
Создание резервной копии
Восстановление резервной копии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: rescuezilla-2.4.2-64bit

Rescuezilla – программное обеспечение для резервного копирования и восстановления случайно удалённых файлов в разделах операционной системы. Поддерживает выполнение автоматического поиска и подключения сетевых разделов, которые можно использовать для размещения резервных копий.

Графический интерфейс программы основан на оболочке **LXDE**. Формат создаваемых резервных копий полностью совместим с дистрибутивом Clonezilla.

При восстановлении поддерживается работа с образами *Clonezilla*, *Redo Rescue*, *Foxclone* и *FSArchiver*.

Установка

Скачайте образ **Rescuezilla** командой:

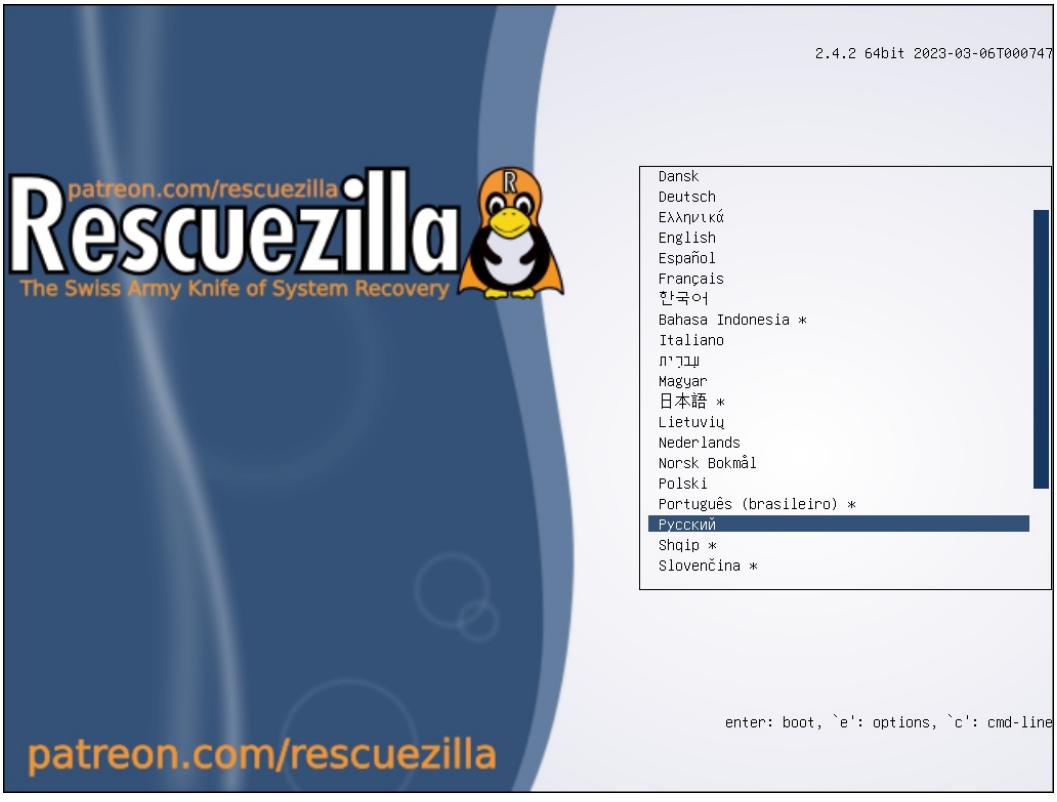
```
wget https://github.com/rescuezilla/rescuezilla/releases/download/2.4.2/rescuezilla-2.4.2-64bit.jammy.iso
```

Запишите образ на носитель. Рекомендуется использовать balenaEtcher.

Создание резервной копии

Загрузитесь с носителя, на который был записан образ **Rescuezilla**.

Выберите необходимый язык интерфейса.

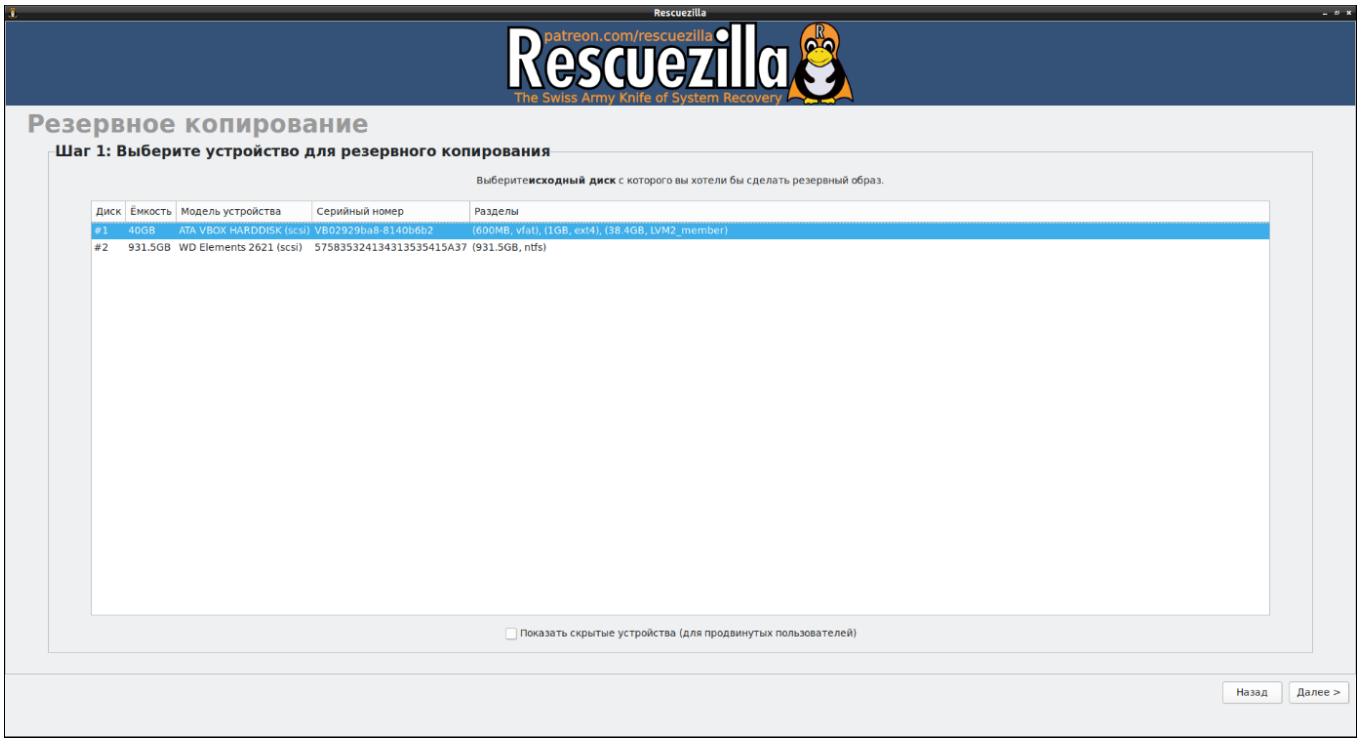


Сразу после загрузки рабочего стола откроется программа **Rescuezilla**.



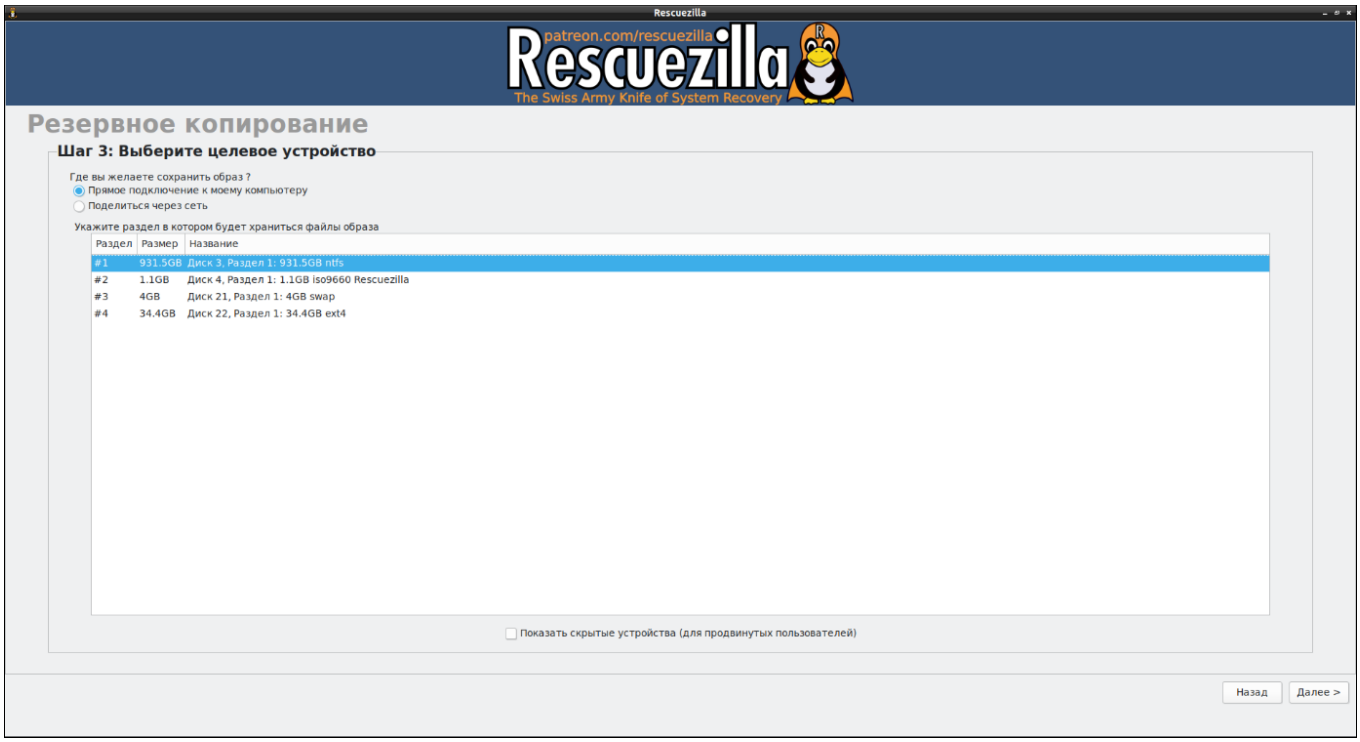
Для создания резервной копии нажмите «**Резервное копирование**».

Выберите диск и разделы на нем, которые необходимо включить в резервную копию.





Выберите диск, на который будет сохранена резервная копия.



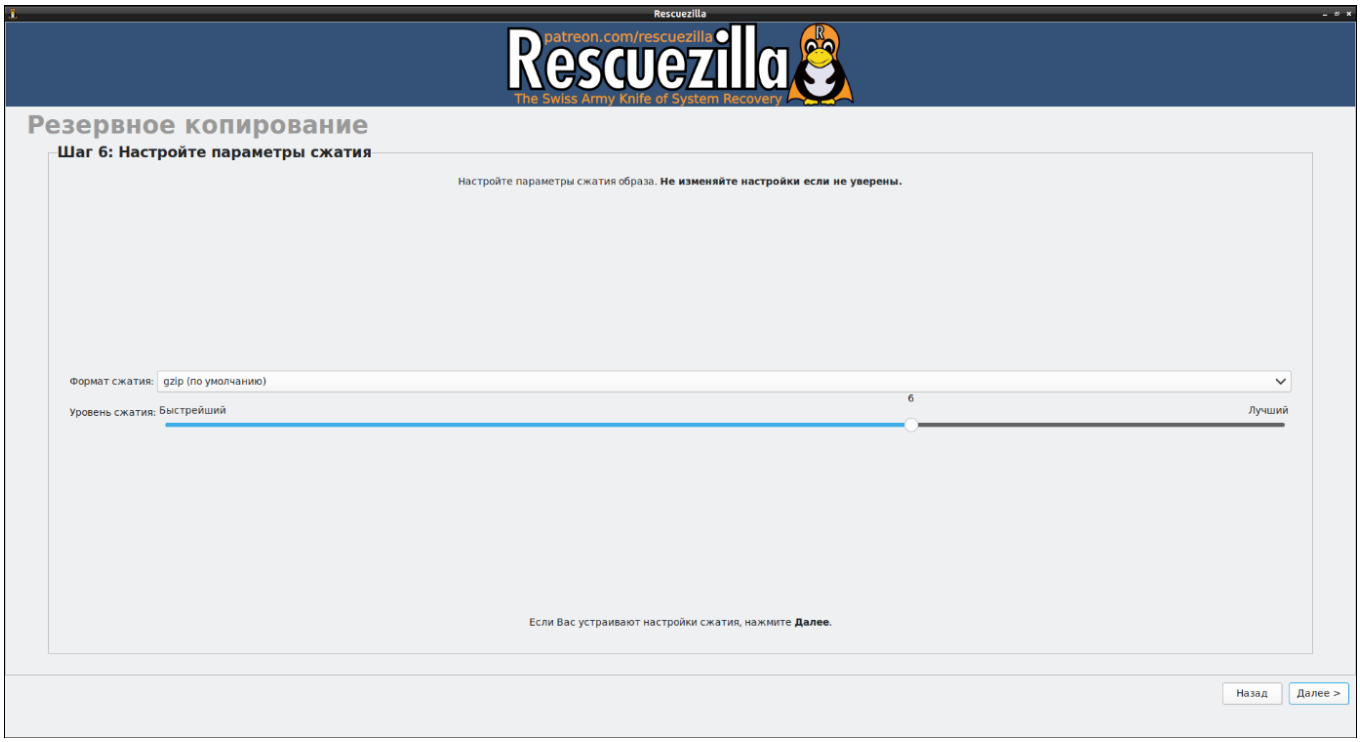
Укажите каталог хранения резервной копии.



Укажите название создаваемой резервной копии.



Определите параметры сжатия. Можно оставить настройки по умолчанию.



Проверьте указанные параметры и, если все указано верно, подтвердите изменения, нажав «**Далее**». В противном случае нажмите «**Назад**» для редактирования необходимых параметров.

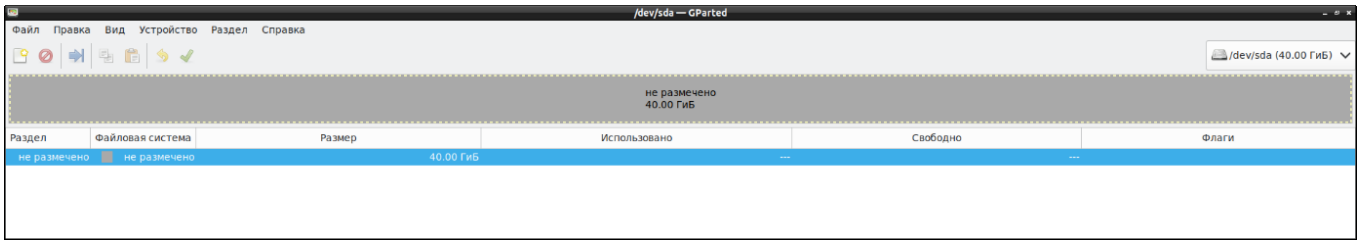


Начнется процесс резервного копирования. По завершении создания резервной копии будет выведено соответствующее сообщение.



Восстановление резервной копии

Для примера будут удалены все разделы на системном диске через GParted.

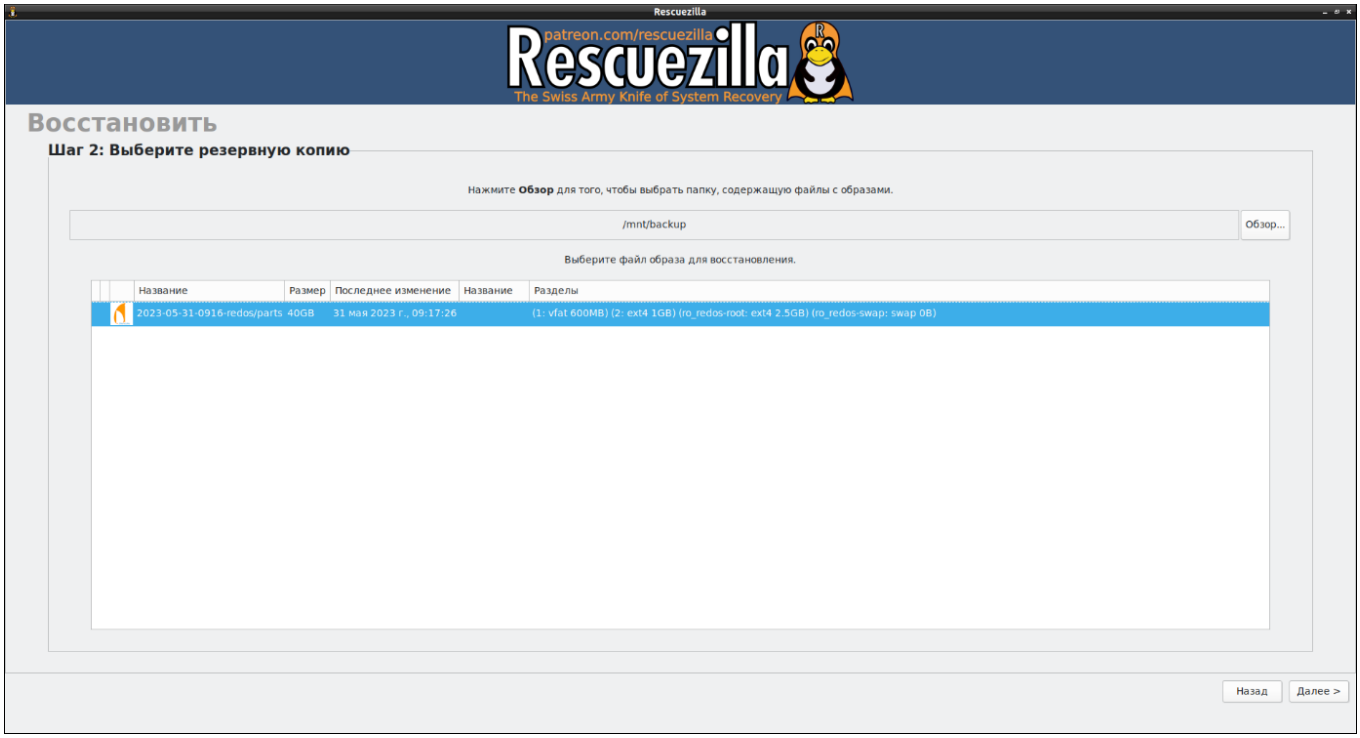


Откройте программу **Rescuezilla** и нажмите «**Восстановить**».

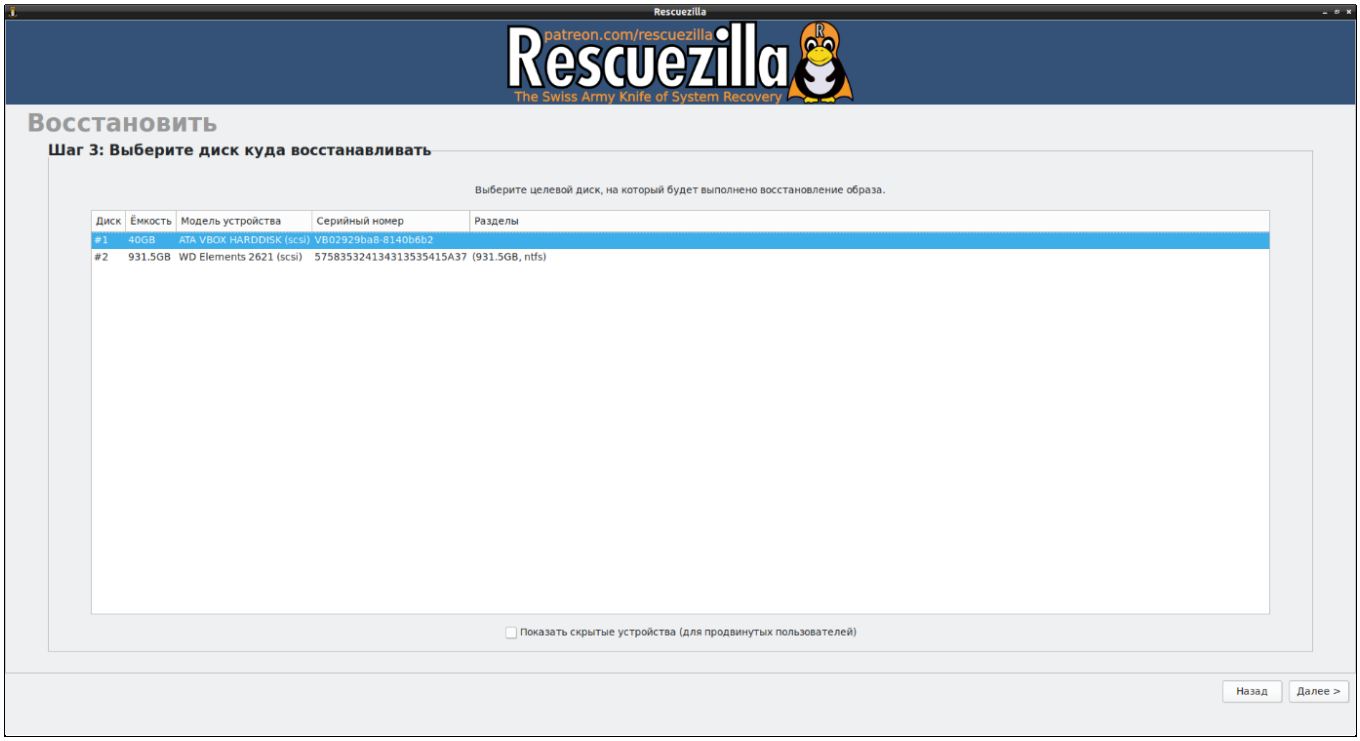
Укажите раздел, содержащий резервную копию.



Укажите каталог с сохраненной резервной копией и выберите ее.



Укажите диск, на который необходимо восстановить данные.



Укажите разделы, которые необходимо восстановить, и требуется ли перезаписать таблицу разделов.



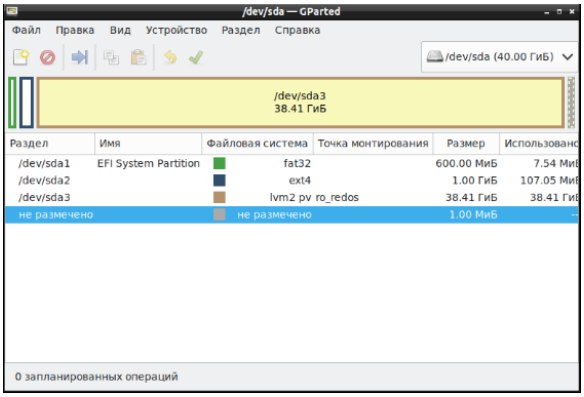
Проверьте указанные параметры и, если все указано верно, подтвердите изменения, нажав «**Далее**». В противном случае нажмите «**Назад**» для редактирования необходимых параметров.



Начнется процесс восстановления резервной копии. По завершении восстановления резервной копии будет выведено соответствующее сообщение.



Для проверки восстановления удаленных разделов откройте **GParted**.

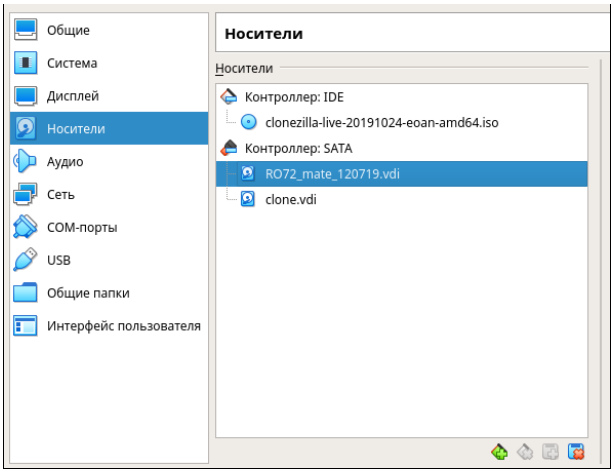


Системный диск успешно восстановлен.

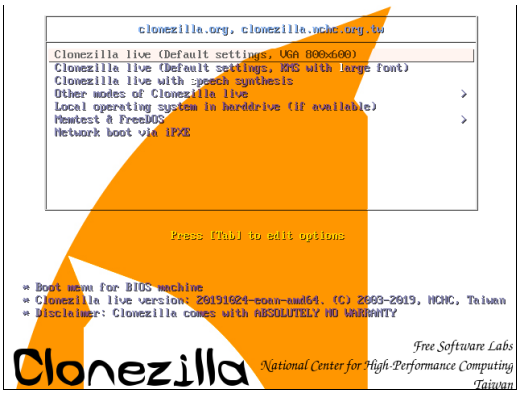
Локальное клонирование жесткого диска

СОЗДАНИЕ ОБРАЗА СИСТЕМЫ

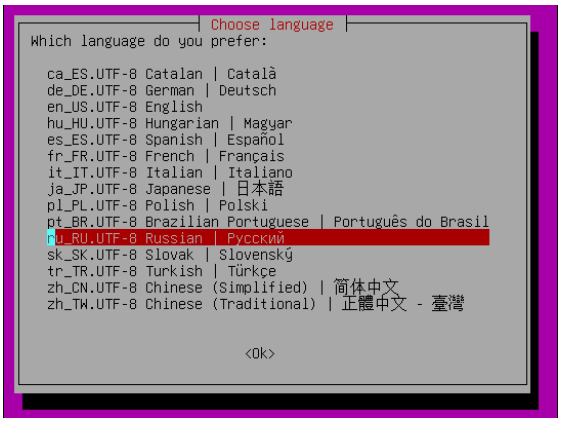
Для примера в VirtaulBox создан дополнительный диск clone.vdi на которой будет сохранен образ системы с помощью clonezilla для последующего восстановления. Вместо этого диска можно использовать Flash-накопитель.



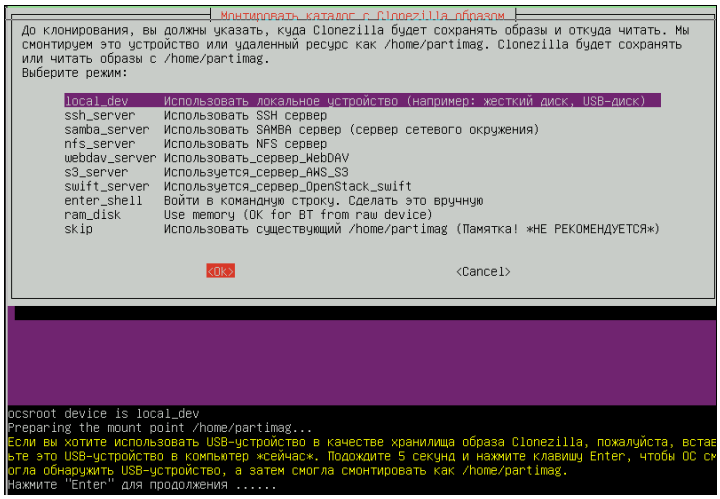
1. Загружаемся с загрузочного образа clonezilla, в меню загрузки выбрав первый пункт.



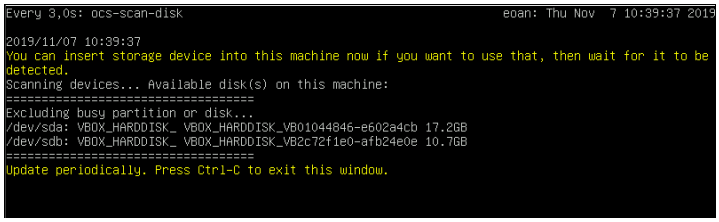
Программа предложит выбрать язык интерфейса



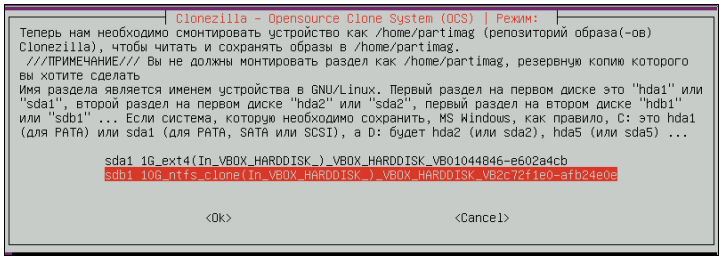
Выбираем место куда будет сохранен образ системы.
Выбираем режим для работы с диском.



Для продолжения нажмите Enter. Далее нажмите ctrl+c



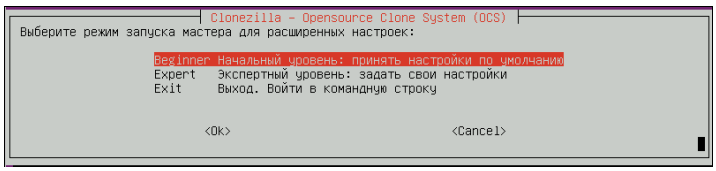
Выбираем диск на который будет сохранен образ, в нашем случае это второй подключенный диск.



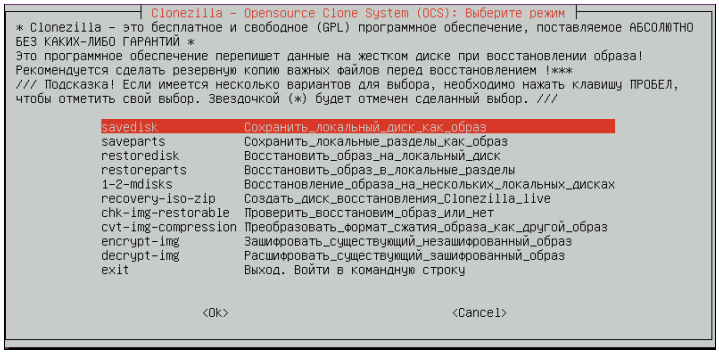
Здесь происходит выбор директории для сохранения образа, т.к диск пустой, сохраним образ в корень.



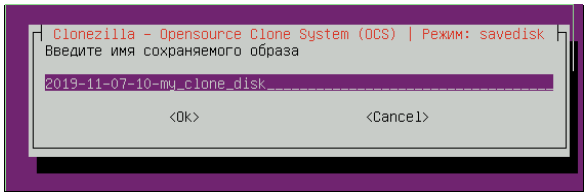
Нажмите «Done»
Режим мастера клонирования, оставим Beginner.



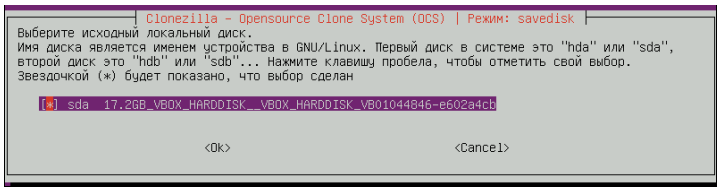
Выбираем необходимое действие, нас интересует «Сохранить локальный диск как образ»



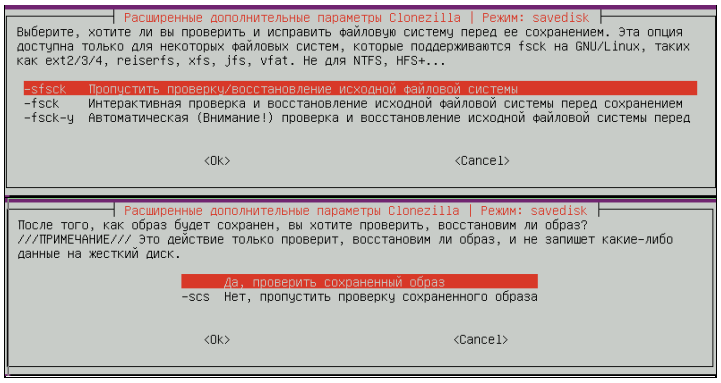
Далее предлагается ввести имя образу диска



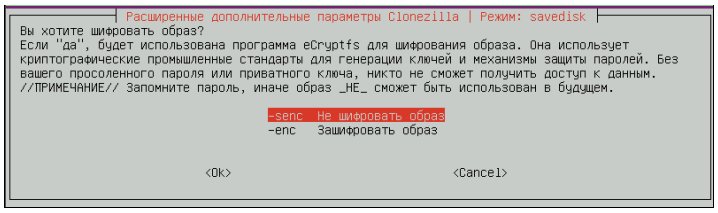
Укажите диск для клонирования



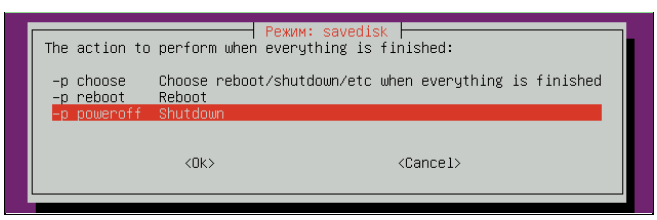
Далее предлагается проверить и исправить файловую систему перед началом клонирования диска.



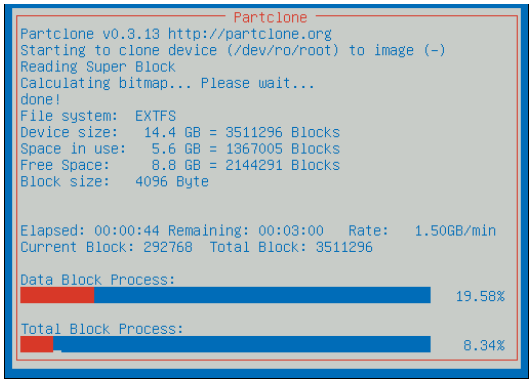
Имеется возможность зашифровать образ.



На следующем шаге предлагается запланировать действие после завершения клонирования, выберете необходимое

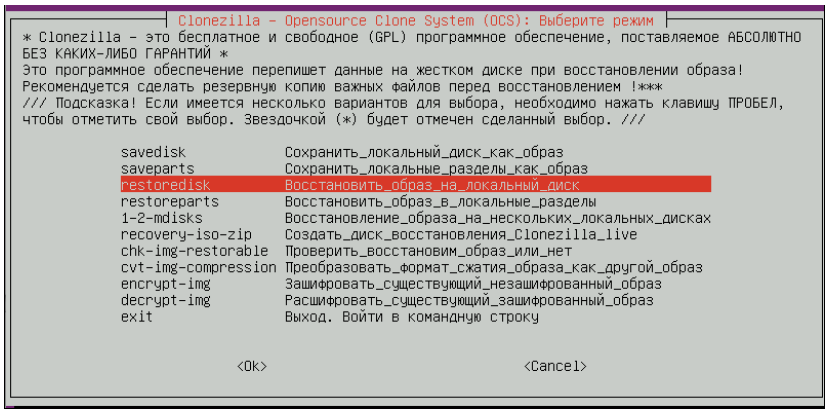


После этого начнется процесс клонирования

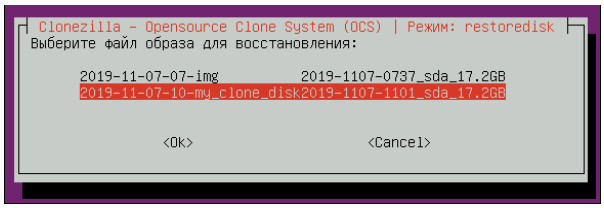


ВОССТАНОВЛЕНИЕ ОБРАЗА СИСТЕМЫ

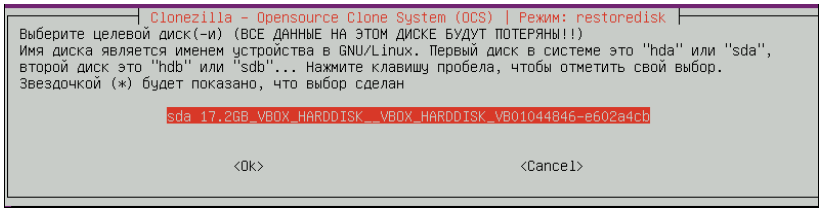
Для восстановления необходимо пройти те же шаги как и в начале клонирования, но дойдя до пункта, где выбирается сохранение и восстановление образов необходимо выбрать «Восстановить образ на локальный диск»



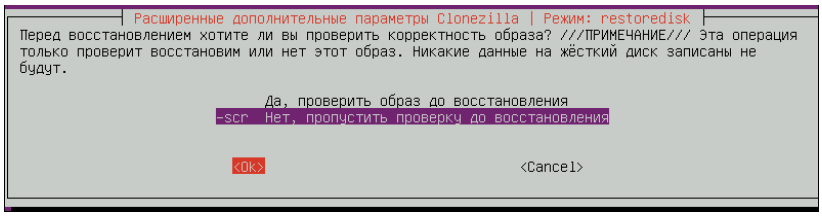
Выбираем файл образа для восстановления



Указываем физический диск на который будет разворачиваться образ



Предлагается проверить образ на ошибки



После этого начнется восстановление образа на диск.
После того, как система восстановится, загрузите РЕД ОС и выполните команду от пользователя root:

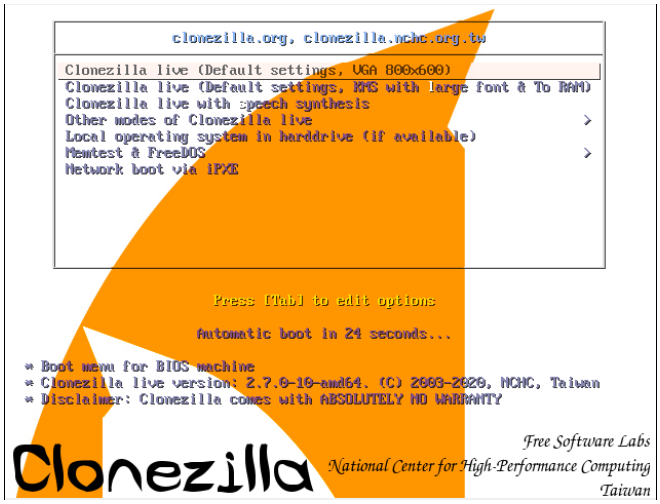
```
dracut -f -v
```

это необходимо для того, чтобы избежать возможных ошибок при использовании функции спящего режима в РЕД ОС.

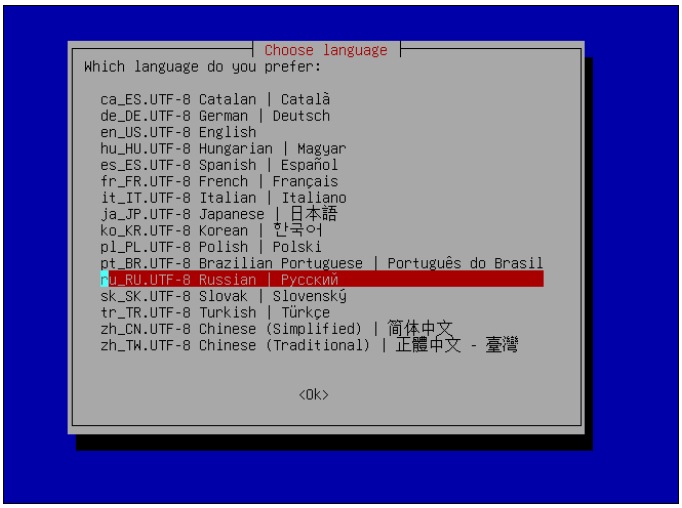
Клонирование жесткого диска на SAMBA-сервер

Создание образа системы

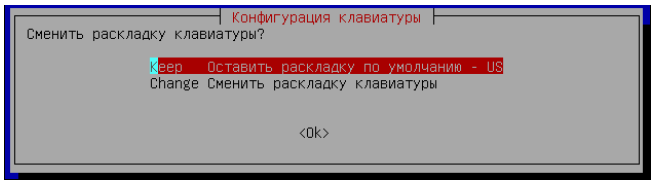
1. Необходимо загрузиться с загрузочного образа **clonezilla**. На экране появится окно загрузчика. В нем необходимо выбрать первый пункт. Для подтверждения выбора следует нажать «**Enter**».



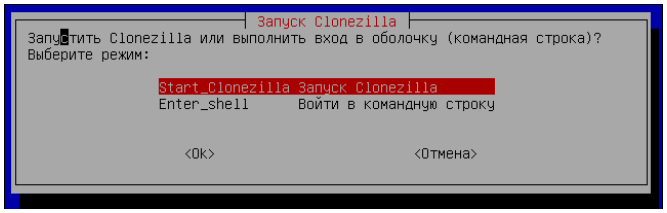
2. Затем программа предложит выбрать язык интерфейса.



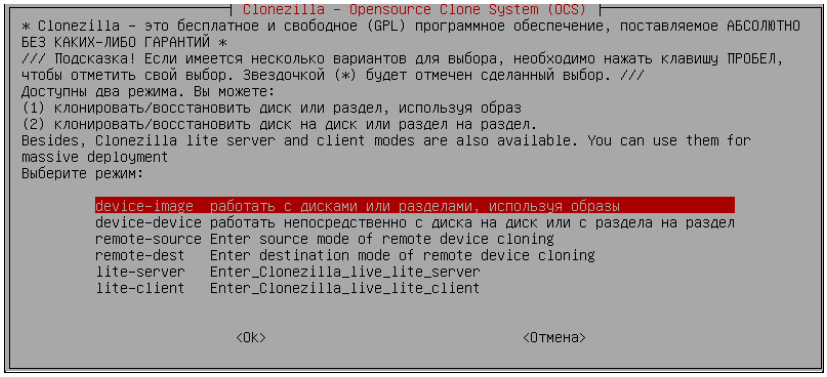
3. Далее программа предлагает сменить раскладку клавиатуры.



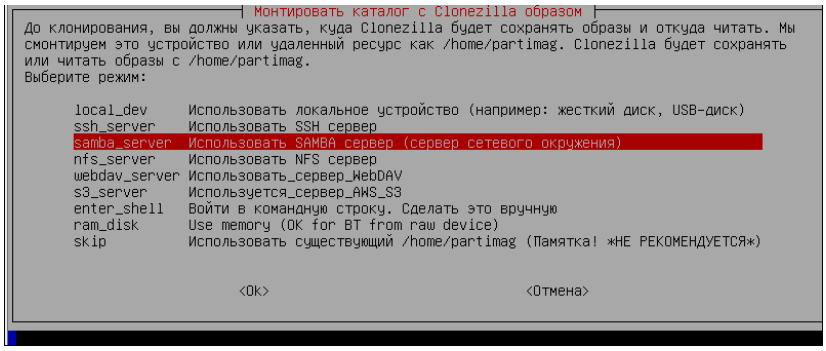
4. В следующем окне предлагается запустить **Clonezilla** или перейти в командную строку. Выберите вариант «**Start_Clonezilla**».



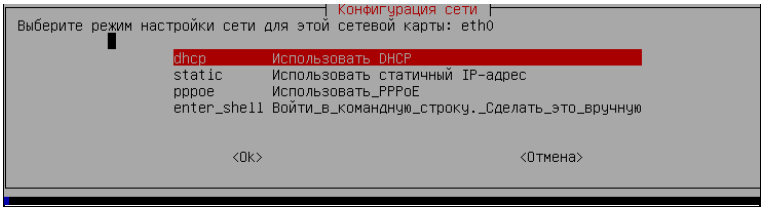
5. Затем необходимо настроить режим для работы с диском. Выберите пункт «**device-image**».



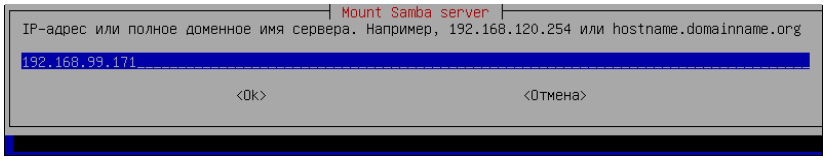
6. Местом сохранения образа в данном случае выберите «**samba_сервер**».



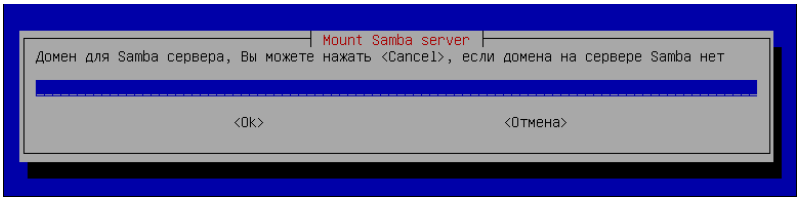
7. Далее выберите режим настройки сети — «**dhcp**».



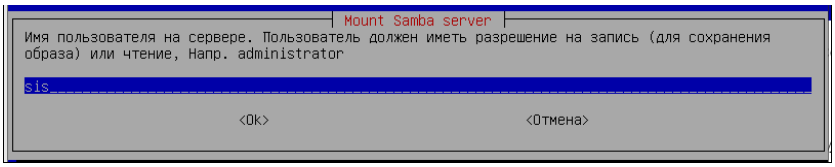
8. После выбора режима сети необходимо ввести *IP-адрес* или *полное имя* Samba-сервера.



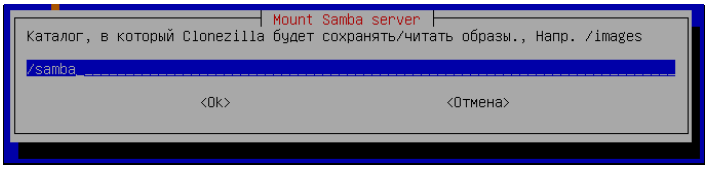
9. Затем требуется ввести домен для Samba-сервера. Однако если домена нет, нужно нажать «**Отмена**».



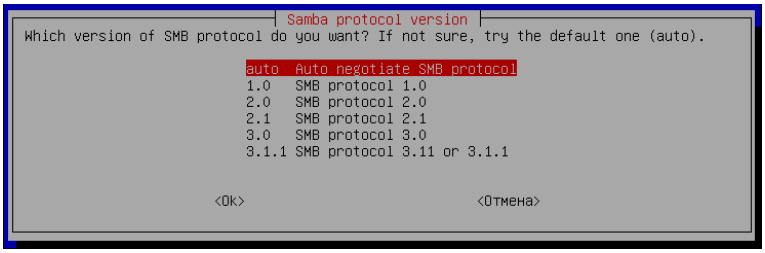
10. Далее нужно ввести *имя пользователя* Samba-сервера.



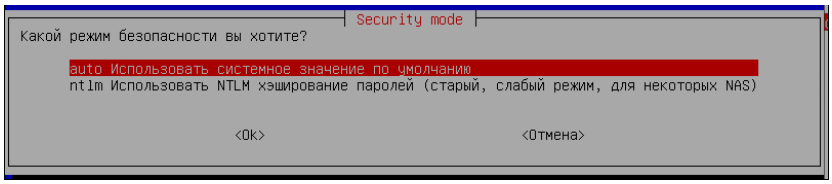
11. Определите *каталог*, в который будете сохранять/читать образы, введите его *название*.



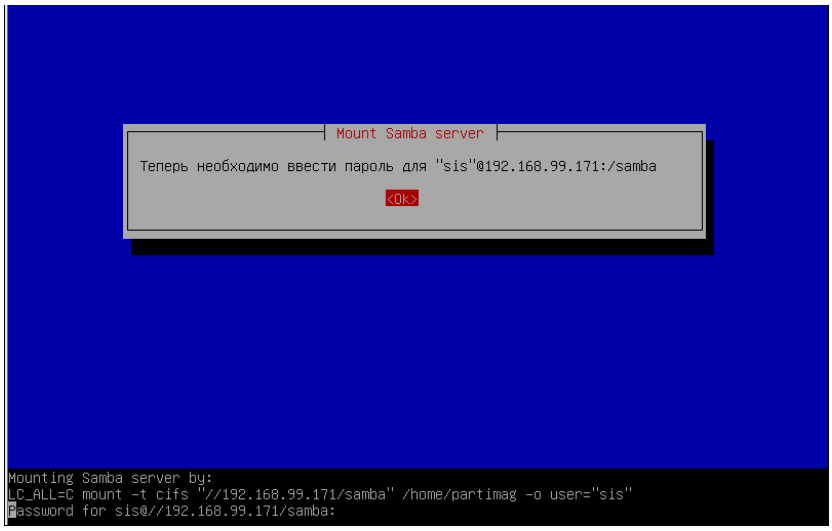
12. Затем необходимо выбрать версию протокола **SMB**.



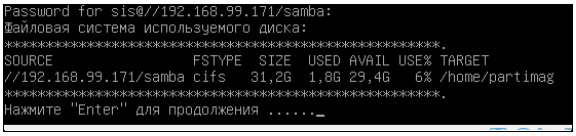
13. Режим безопасности установите «**auto**».



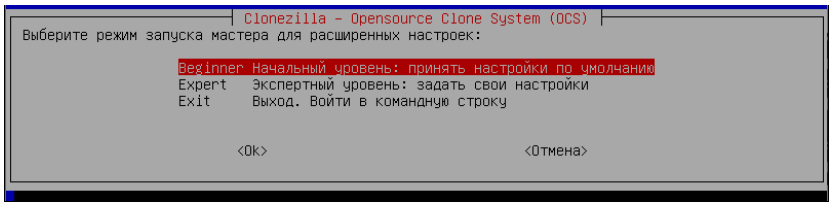
14. Введите пароль пользователя Samba-сервера.



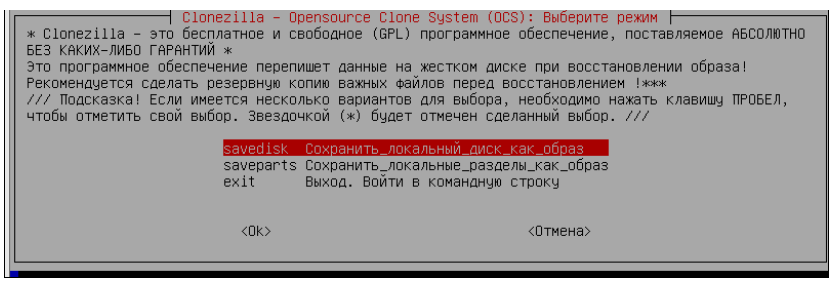
15. Подтвердите свой выбор нажатием «**Enter**».



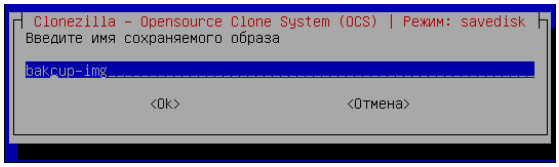
16. Затем нужно выбрать режим запуска мастера для расширенных настроек.



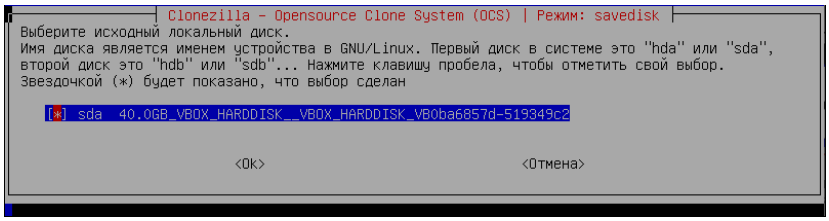
17. В нем необходимо выбрать пункт «**savedisk — Сохранить локальный диск как образ**».



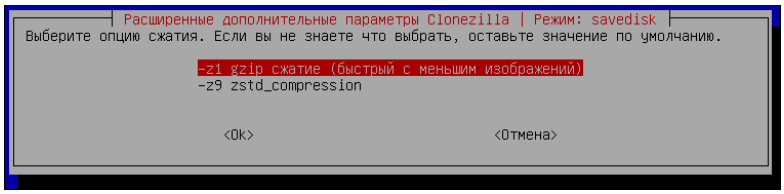
18. Затем введите *имя* сохраняемого *образа*.



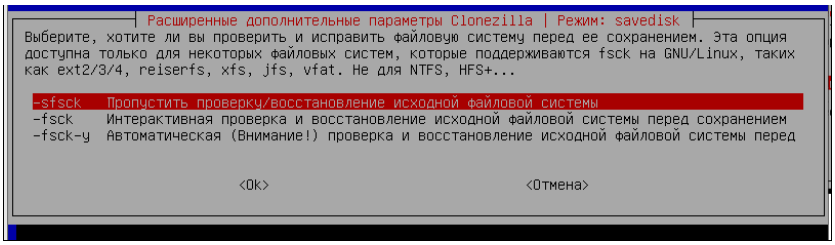
19. Выберите *диск*, который хотите сохранить.



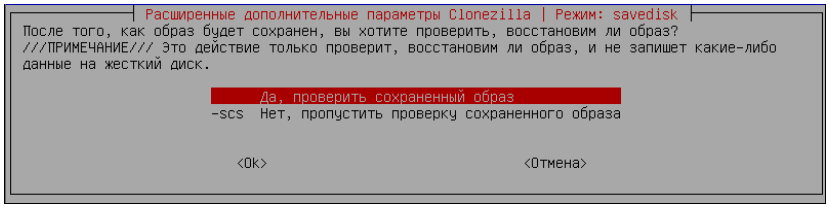
20. Далее предлагается выбрать опцию сжатия данных. Можно оставить *значение по умолчанию*.



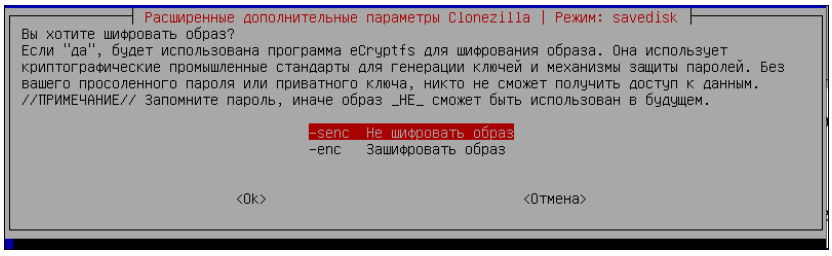
21. Затем требуется указать, нужно ли проверять файл перед сохранением.



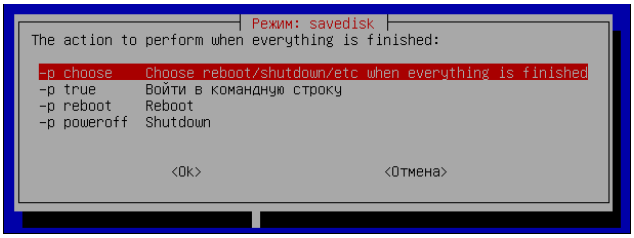
22. Следующее окно предлагает выбрать, хотите ли вы включить проверку сохраненного образа на восстановление. Выберите пункт «**Да, проверить сохраненный образ**».



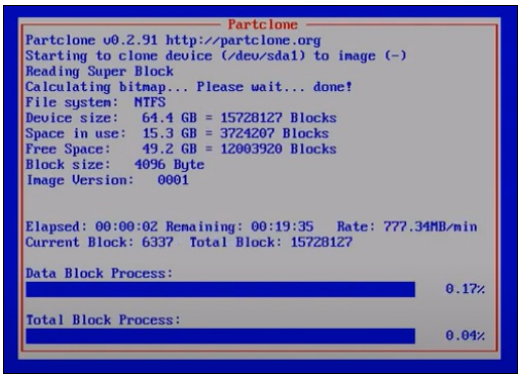
23. Выберите, нужно ли шифровать ваш образ.



24. Затем необходимо выбрать *дальнейшее действие* после завершения клонирования.



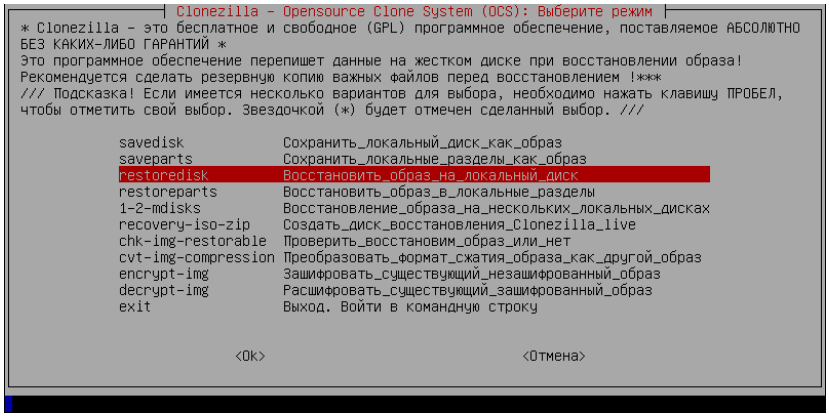
После выполнения всех вышеуказанных действий **образ диска на Samba-сервере** будет успешно **создан**.



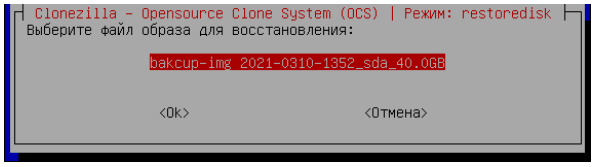
Восстановление диска

Для восстановления диска необходимо проделать описанные выше пункты **1-16**.

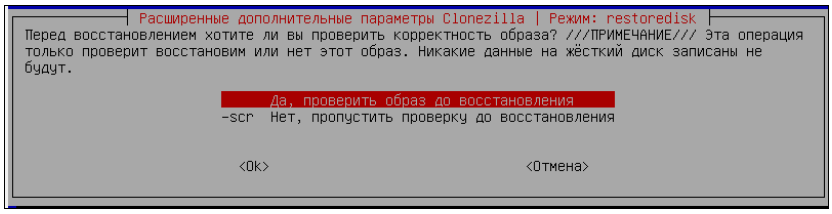
После этого необходимо выбрать действие с диском «**restoredisk — Восстановить образ на локальный диск**».



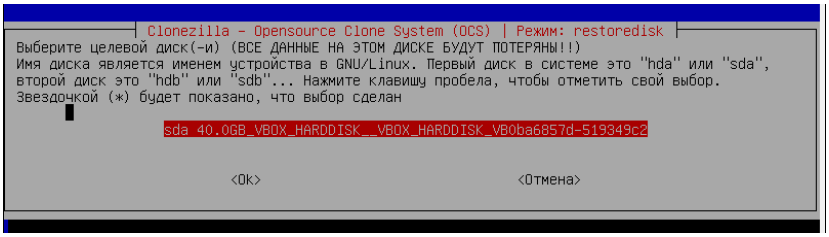
Выберите нужный *файл образа*.



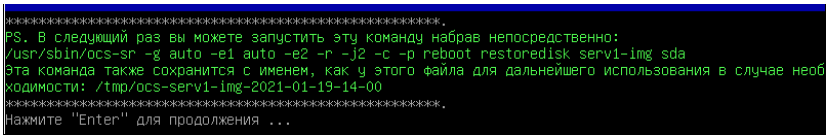
Включите *проверку образа* перед восстановлением.



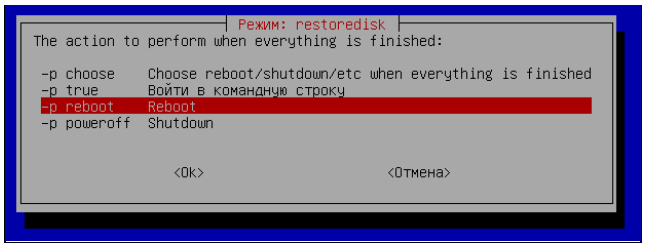
Затем выберите *диск*, на который будет установлен образ.



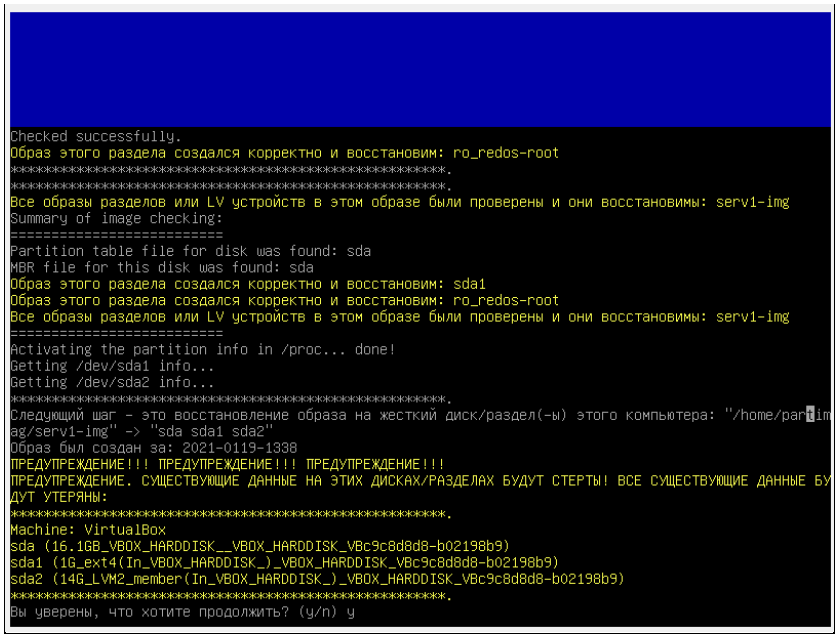
Подтвердите действия нажатием «**Enter**».



Далее выберите *действие после завершения* восстановления диска.



Будет выполнена проверка возможности восстановления диска и представлены данные о нем. Для подтверждения действия необходимо будет нажать «**y**». После этого пойдет процесс восстановления и диск будет восстановлен.



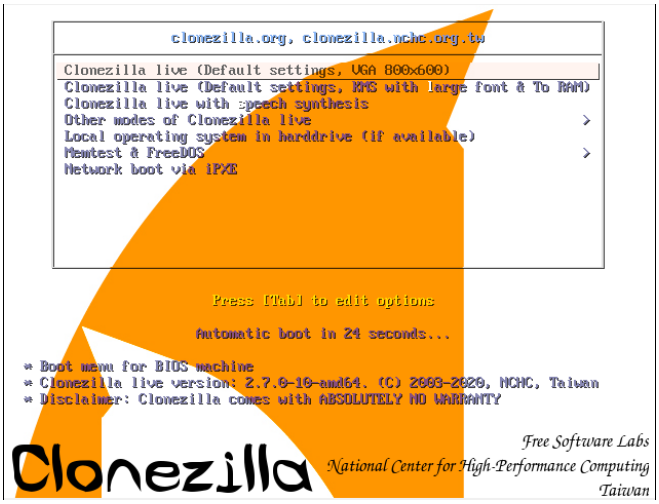
Клонирование жесткого диска на SSH-сервер

Окружение

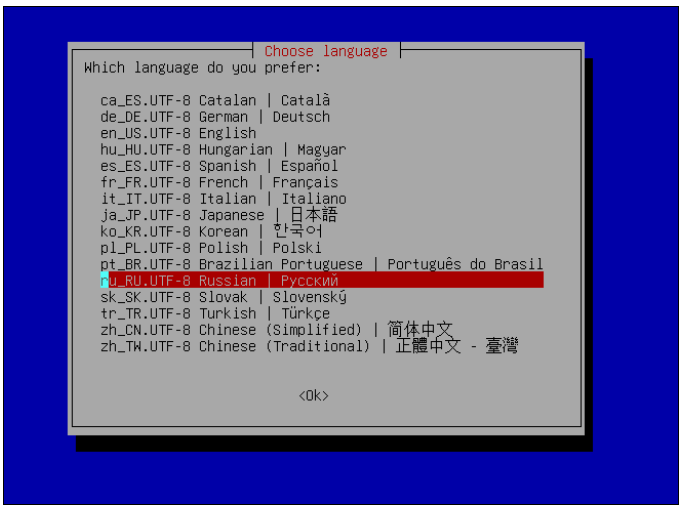
- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:**: Clonezilla 3.0.1-8

Создание образа системы

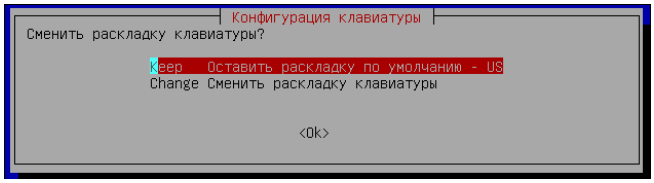
1. Необходимо загрузиться с загрузочного образа **clonezilla**. На экране появится окно загрузчика. В нем необходимо выбрать первый пункт. Для подтверждения выбора следует нажать «**Enter**».



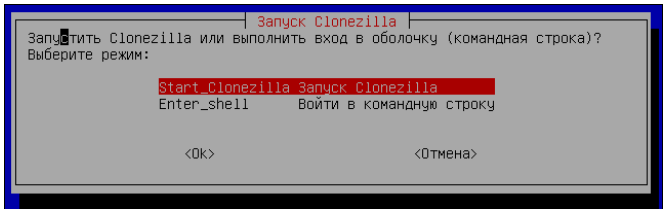
2. Затем программа предложит выбрать *язык интерфейса*.



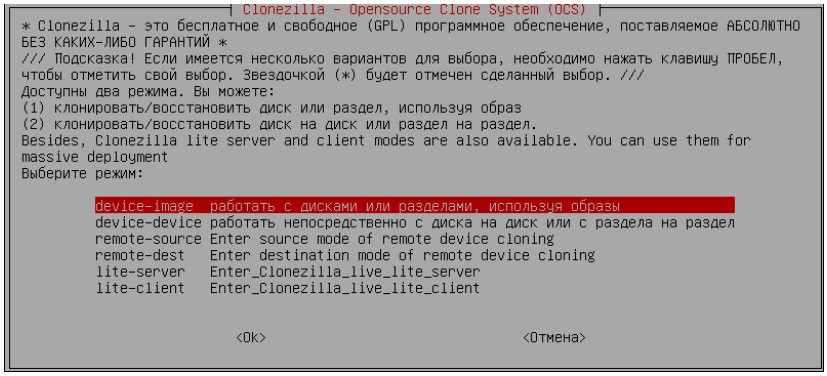
3. Далее программа предлагает сменить *раскладку* клавиатуры.



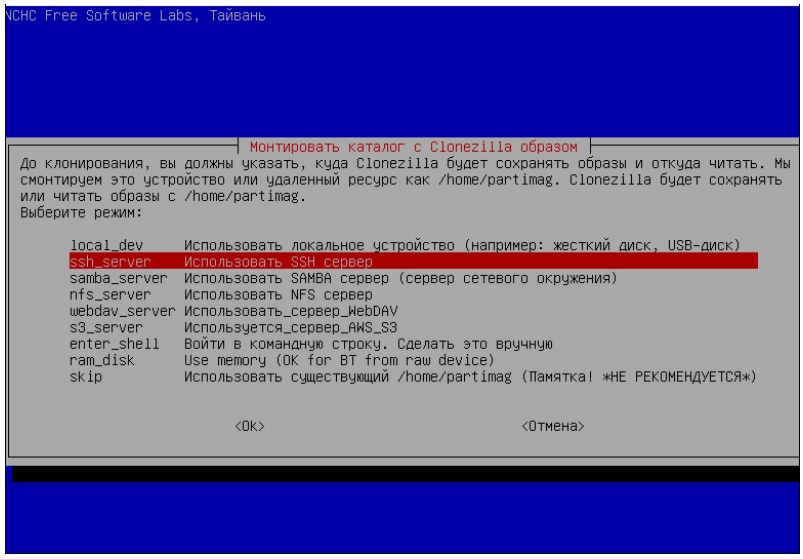
4. В следующем окне предлагается запустить **Clonezilla** или перейти в командную строку. Выберите вариант «**Start_Clonezilla**».



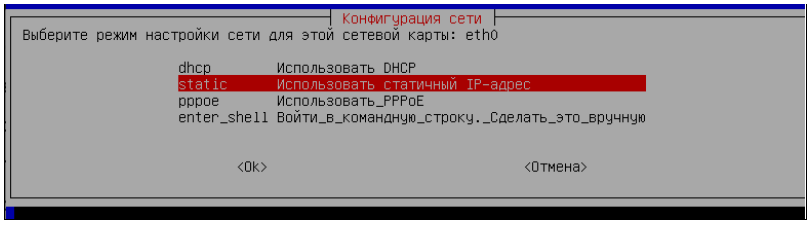
5. Затем необходимо настроить режим для работы с диском. Выберите пункт «**device-image**».



6. *Местом* сохранения образа в данном случае выберите «**ssh_сервер**».

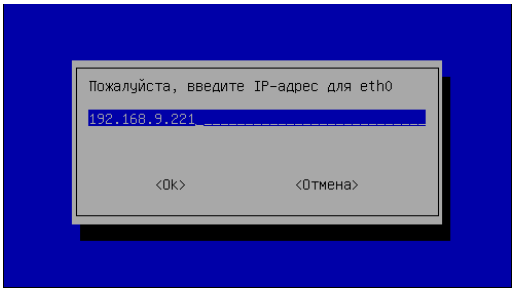


7. Далее выберите *режим* настройки сети — «**static**».

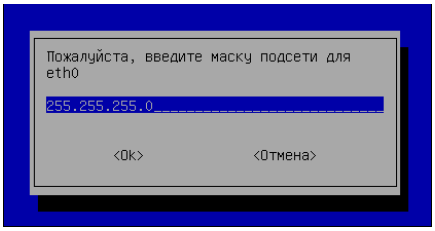


Так как было выбрано использовать *статический* ip-адрес, необходимо его прописать.

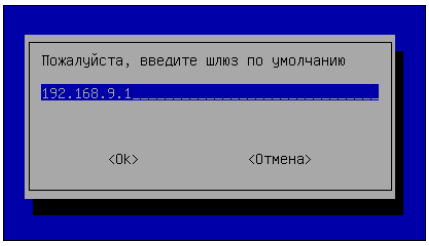
8. Введите *IP-адрес* устройства, с которого клонируется диск.



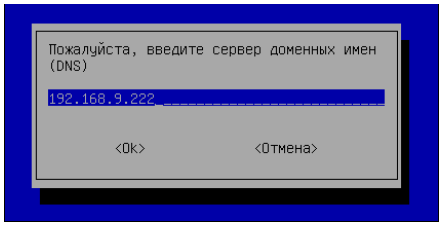
9. Введите *маску* подсети.



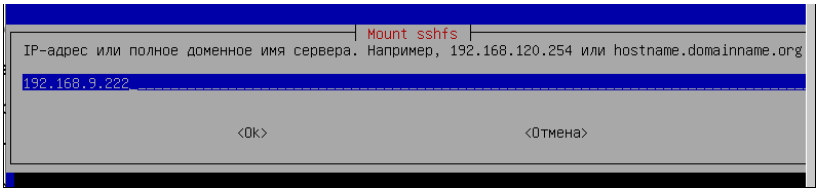
10. Затем введите *шлюз* по умолчанию.



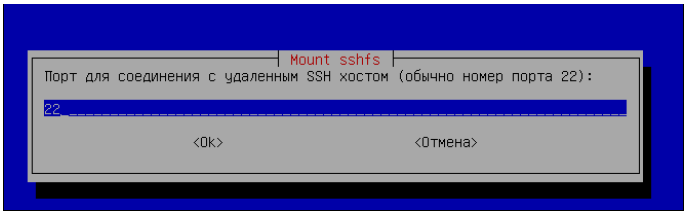
11. А также *IP-адрес DNS*.



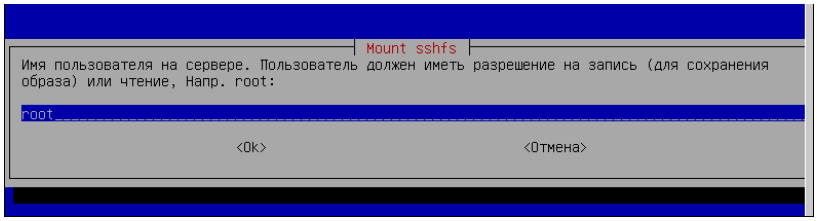
12. Затем введите *IP-адрес* или *полное имя* SSH сервера.



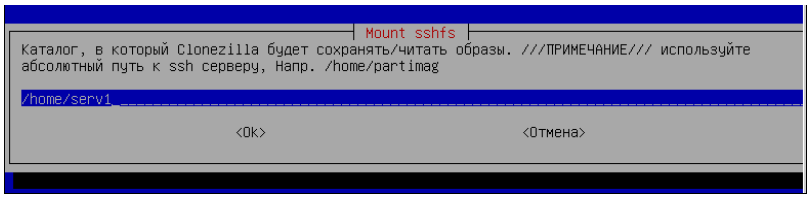
13. Введите используемый *порт* для соединения с удаленным хостом.



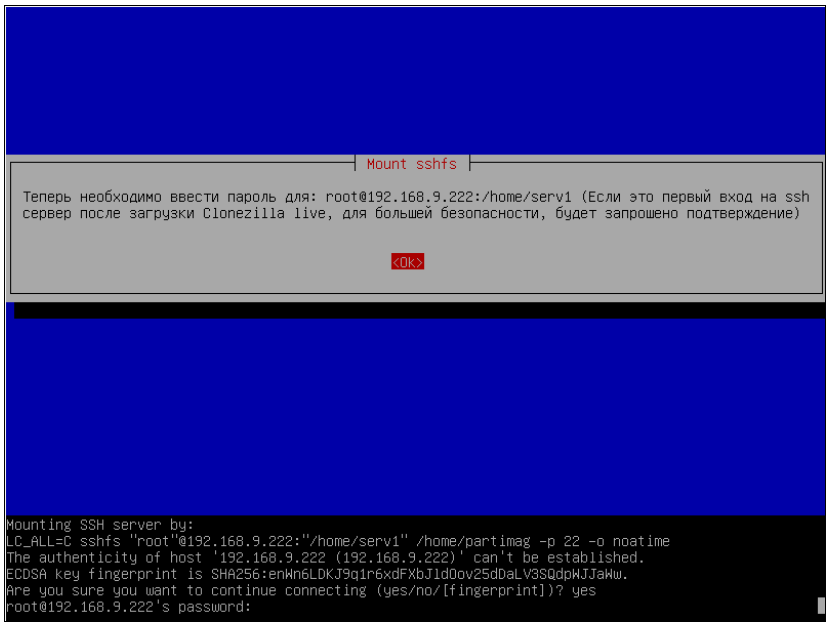
14. Далее нужно ввести *имя пользователя* SSH сервера.



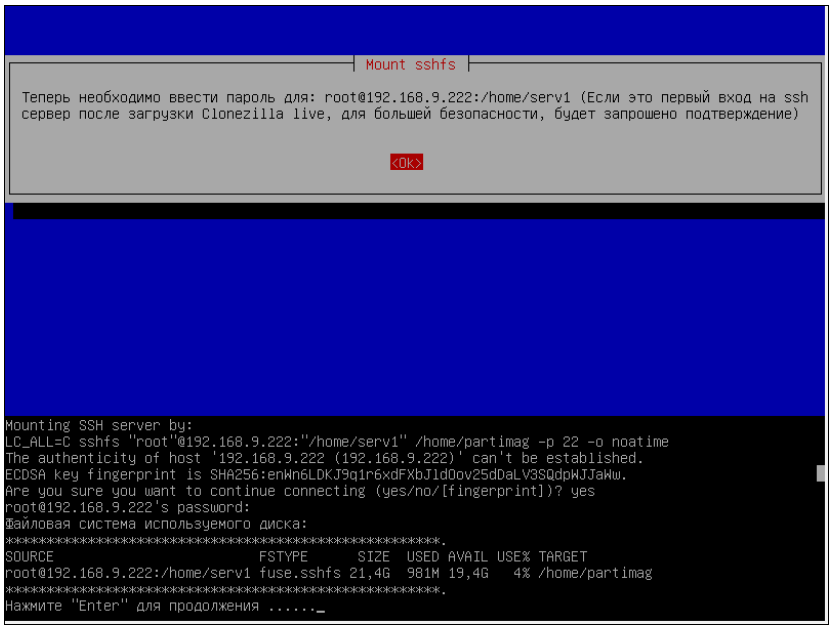
15. Определите *каталог*, в который будете сохранять/читать образы, введите *его название*.



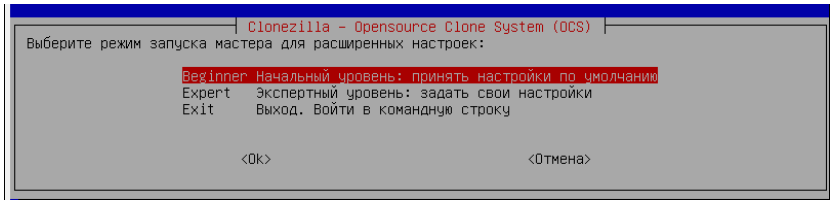
16. Введите *пароль пользователя*.



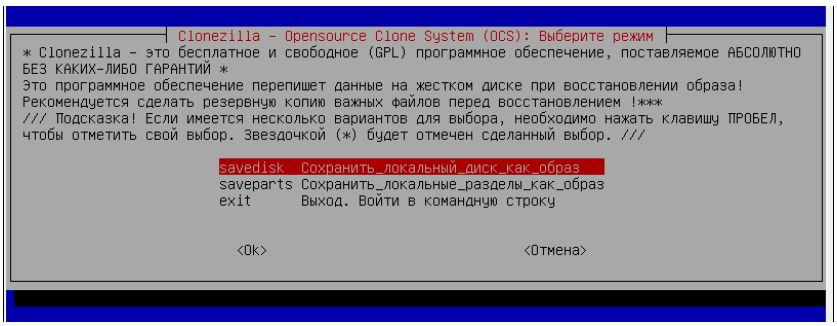
17. Подтвердите свой выбор нажатием «**Enter**».



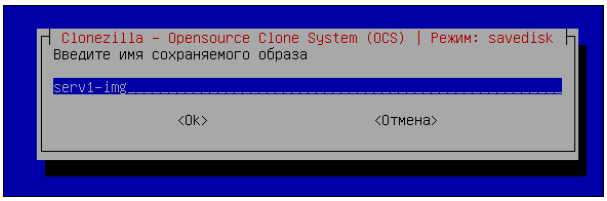
18. Затем нужно выбрать *режим запуска* мастера для расширенных настроек.



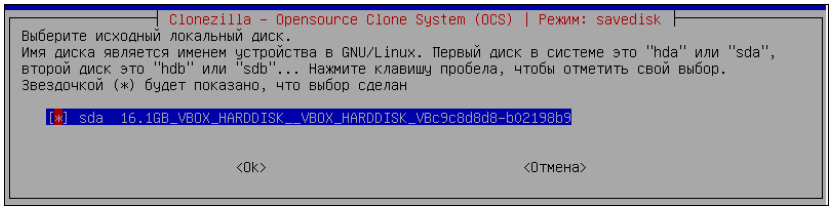
19. В нем необходимо выбрать пункт «**savedisk — Сохранить локальный диск как образ**».



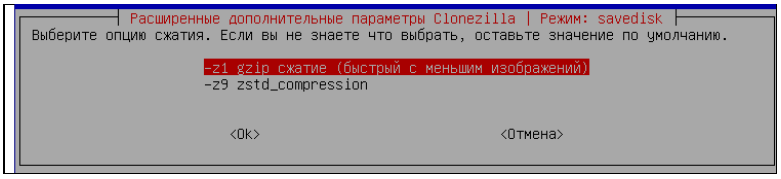
20. Затем введите *имя* сохраняемого *образа*.



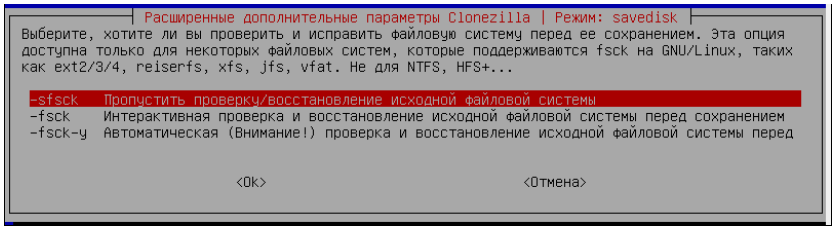
21. Выберите *диск*, который хотите сохранить.



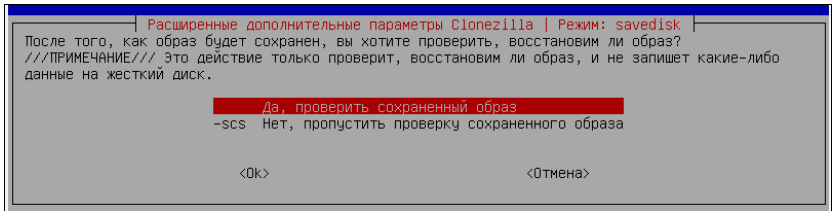
22. Далее предлагается выбрать *опцию сжатия* данных. Можно оставить значение *по умолчанию*.



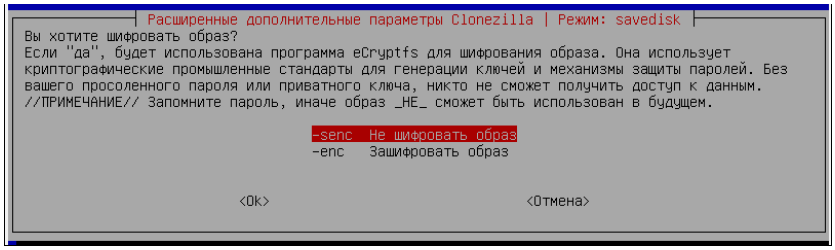
23. Затем требуется указать, нужно ли *проверять* файл перед сохранением.



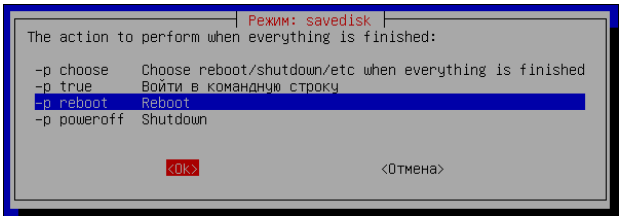
24. Следующее окно предлагает выбрать, хотите ли вы включить *проверку* сохраненного *образа* на восстановление. Выберите пункт «**Да, проверить сохраненный образ**».



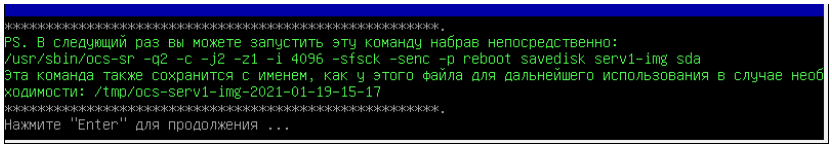
25. Выберите, нужно ли *шифровать* ваш образ.



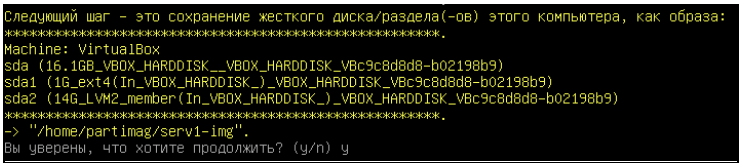
26. Затем необходимо выбрать *дальнейшее действие* после завершения клонирования.



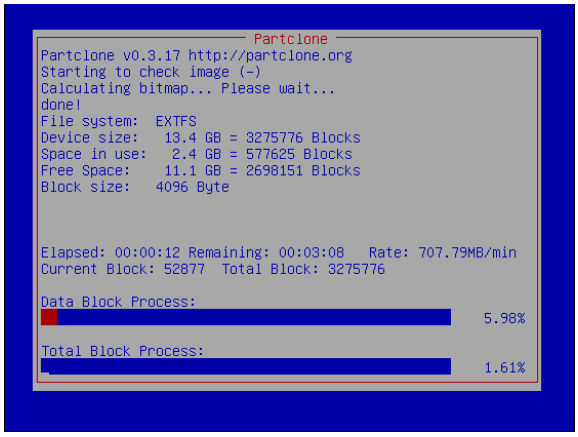
27. Подтвердите свой выбор нажатием «**Enter**».



28. Затем необходимо подтвердить сохранение диска, как образа.



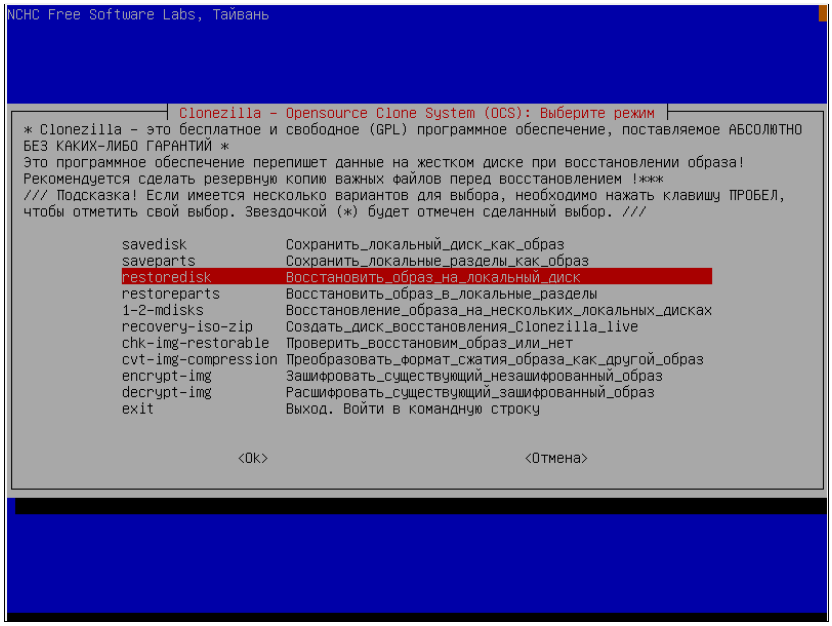
После выполнения всех перечисленных выше действий образ диска на SSH сервере создан.



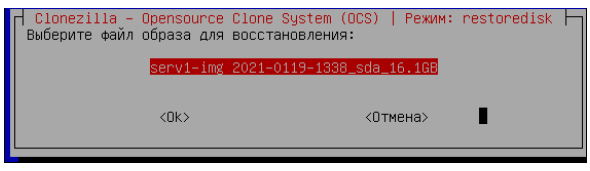
Восстановление диска

Для восстановления диска необходимо проделать описанные выше пункты **1-18**.

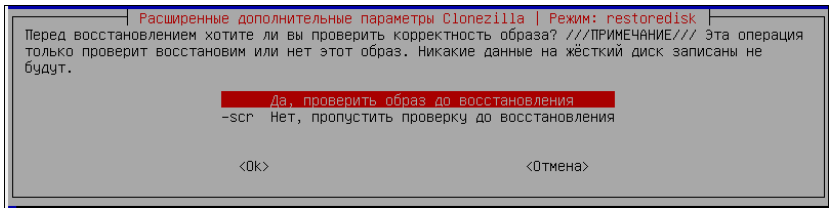
После этого необходимо выбрать действие с диском «**restoredisk — Восстановить образ на локальный диск**». Данный пункт будет доступен, если Clonezilla обнаружит сохраненный ранее образ на SSH-сервере.



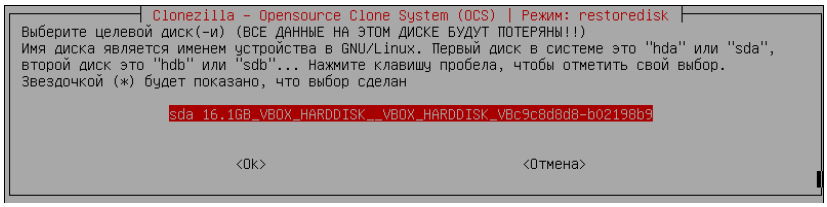
Выберите нужный *файл образа*.



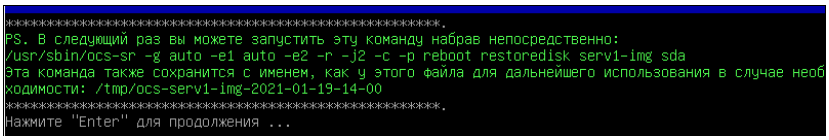
Включите *проверку образа* перед восстановлением.



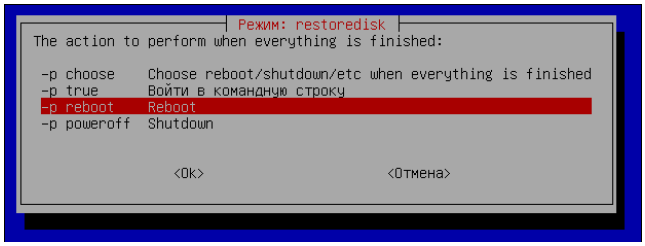
Затем выберите *диск*, на который будет установлен образ.



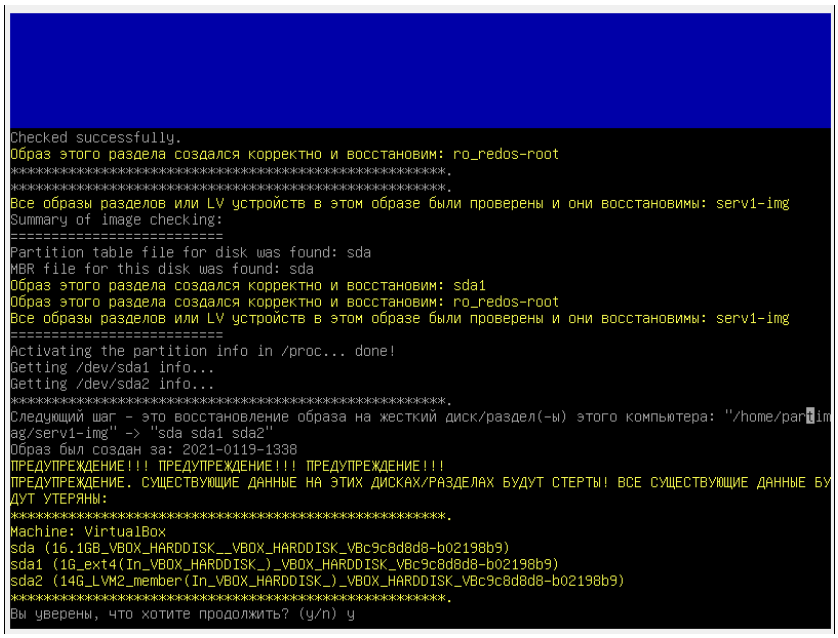
Подтвердите действия нажатием «**Enter**».



Далее выберите *действие после завершения* восстановления диска.



Будет выполнена проверка возможности восстановления диска и представлены данные о нем. Для подтверждения действия необходимо будет нажать «**y**». После этого пойдет процесс восстановления и диск будет восстановлен.



Создание резервных копий в Кибер Бекап

Обзор
Установка
Установка сервера управления
Установка агента
Создание плана выполнения резервной копии

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Сервер графический
- **Версия ПО:** CyberBackup_17

Обзор

Кибер Бэкап — коммерческое программное обеспечение, предназначенное для создания резервного копирования и восстановления данных. Скачать пробную версию или приобрести продукт можно на официальном сайте компании Киберпротект.

Управление утилитой осуществляется из web-формы. Через нее можно задать расписание, по которому будет выполняться резервное копирование, просматривать доступные резервные копии, просматривать уведомления и отчеты о прошедших операциях, добавлять или удалять хранилища. Для первого подключения к web-форме нужен пароль от учетной записи суперпользователя. Впоследствии можно добавить других пользователей.

Установка

Для корректной установки **CyberBackup** необходимо установить ряд дополнительных пакетов. Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install kernel-lt-headers kernel-lt-devel gcc make dkms elfutils-libelf-devel
```

Здесь и далее работа с программой будет выполняться с правами пользователя **root**, если не указано иное.

Перейдите в директорию, куда был скачан файл, и назначьте ему права на исполнение:

```
cd /<путь_до_папки_с_файлом>/
chmod +x CyberBackup_17_64-bit.x86_64
```

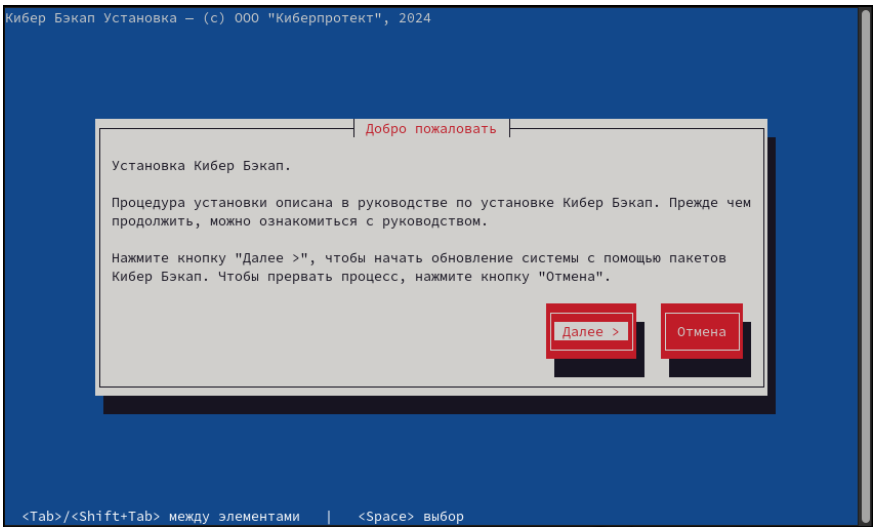
Выполните команду для запуска утилиты:

```
./CyberBackup_17_64-bit.x86_64
```

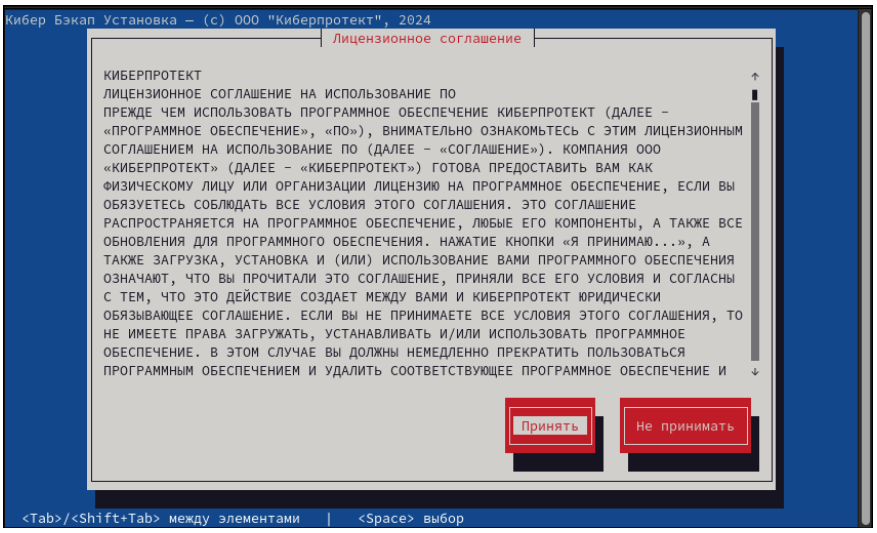
Дальнейшие действия выполняются в установщике программы.

Установка сервера управления

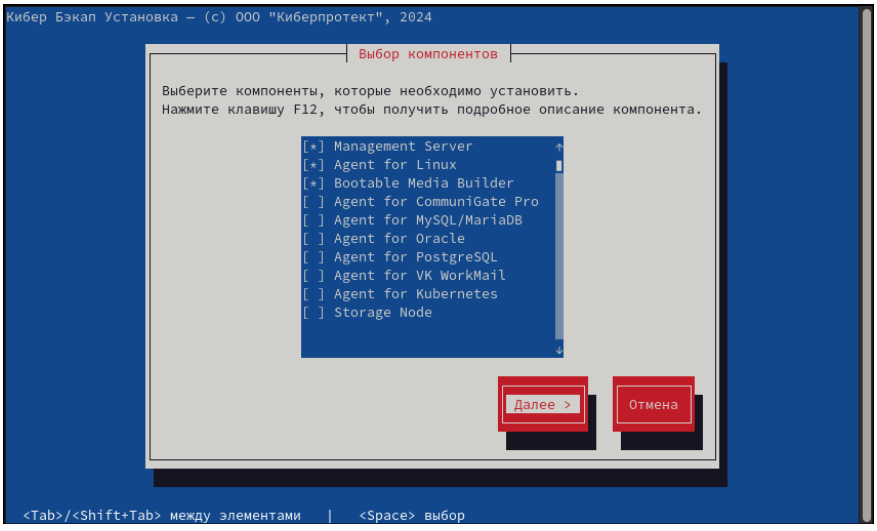
После запуска установки будет открыто окно установщика. Нажмите **Далее**.



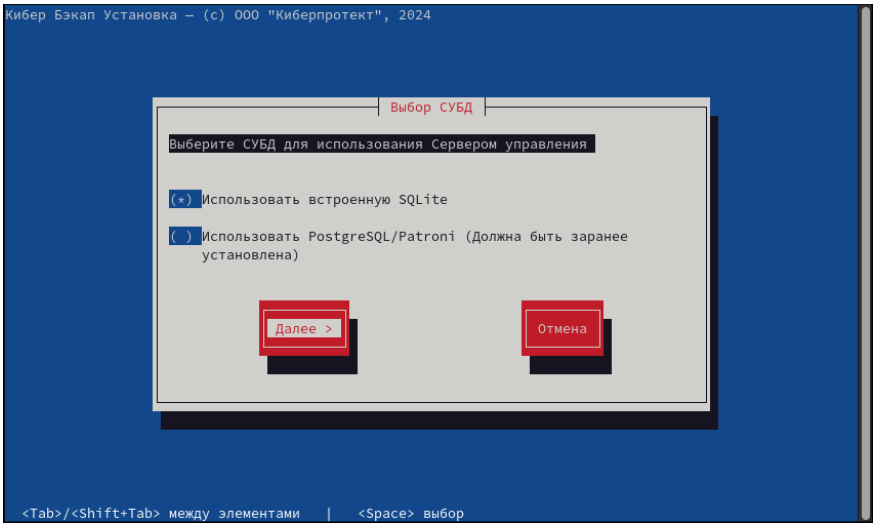
Ознакомьтесь и примите лицензионное соглашение.



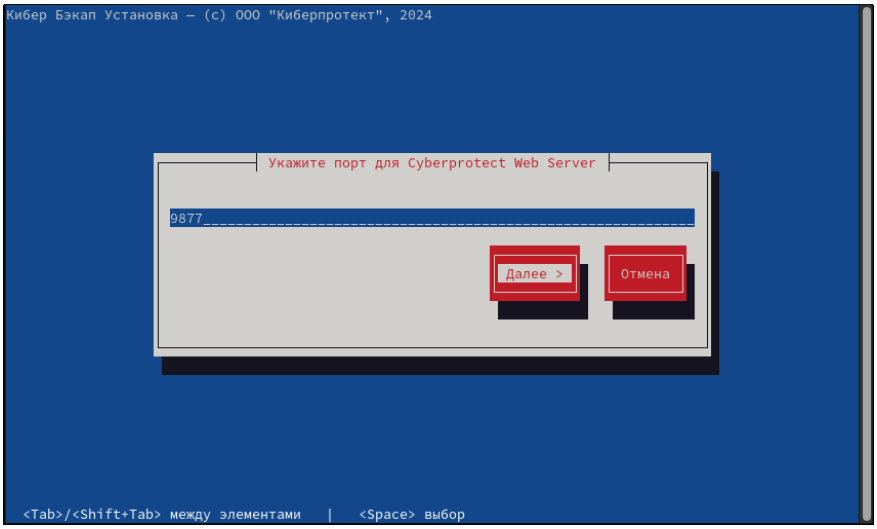
Выберите компоненты для установки.



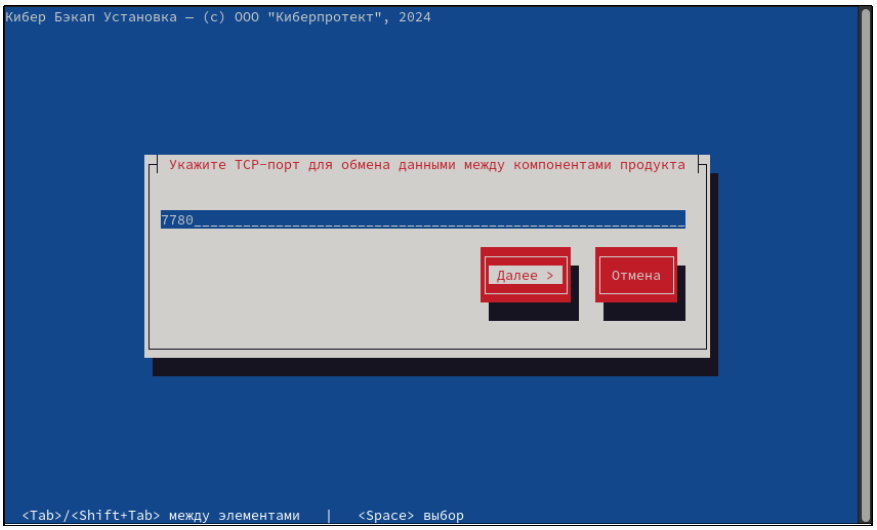
Укажите СУБД.



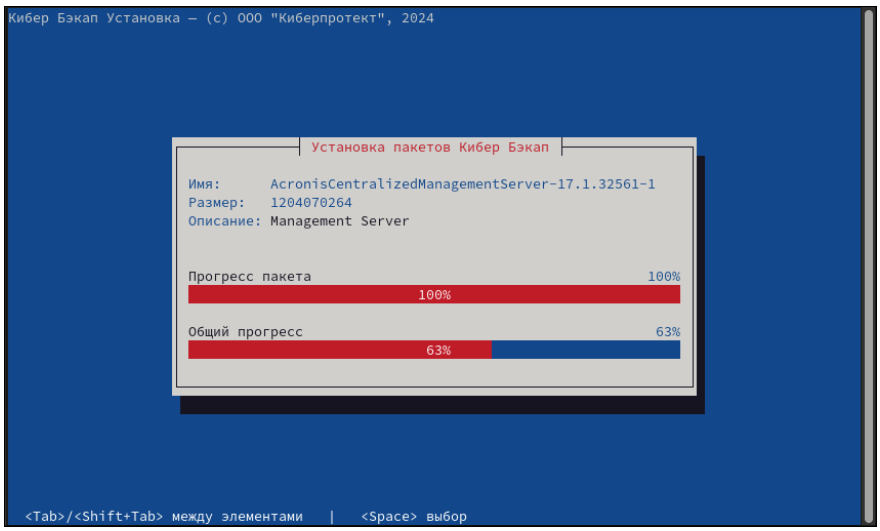
Укажите порт для **Cyberprotect Web Server**.



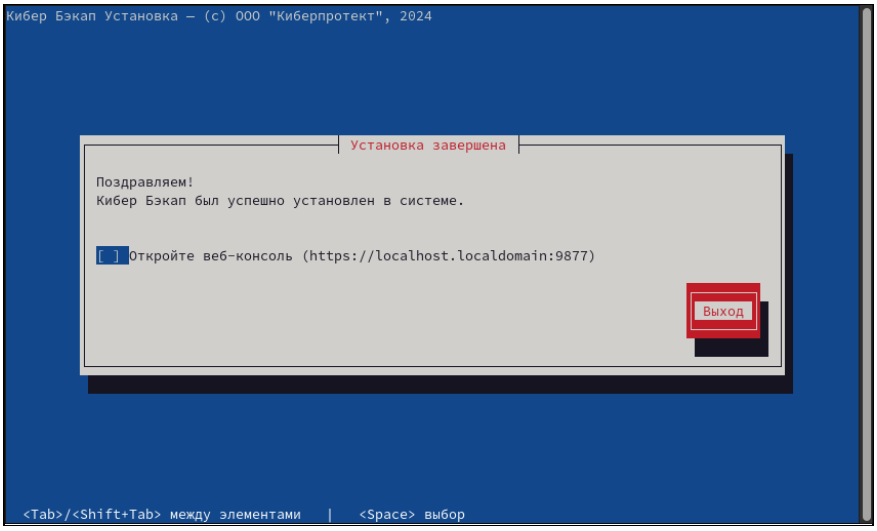
Укажите TCP-порт для обмена данными между компонентами продукта.



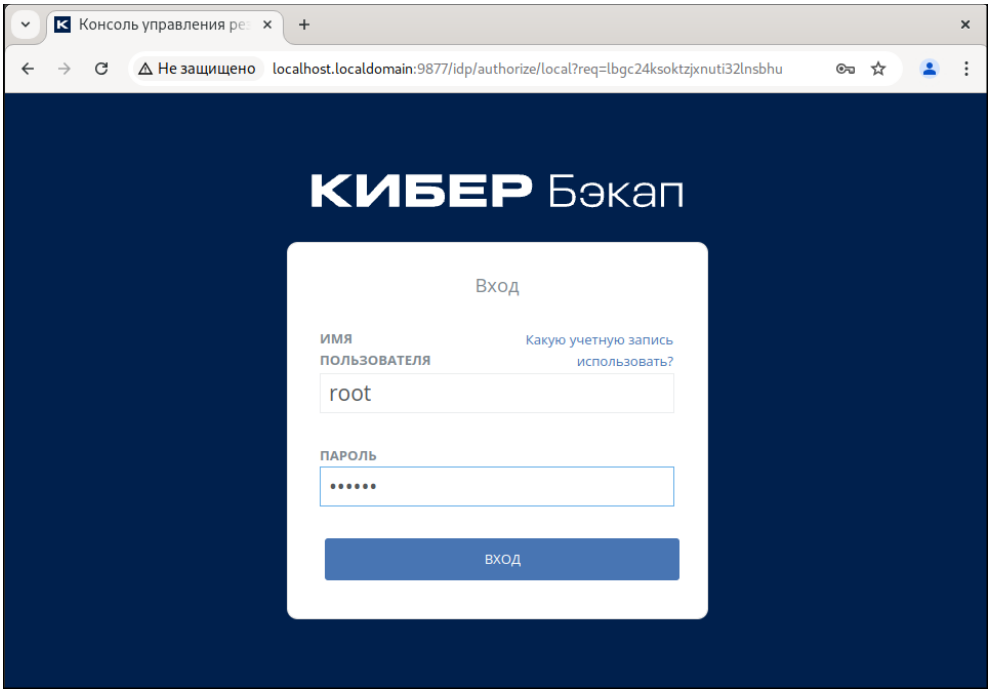
Затем будет запущен процесс установки пакетов.



После завершения установки можно выбрать пункт «**Откройте веб-консоль**», а затем нажать **Выход**. В таком случае, веб-консоль **Cyber Protect** откроется в вашем веб-браузере, установленном по умолчанию.



Вы также можете самостоятельно открыть нужный браузер и перейти по адресу https://localhost.localdomain:9877. Для входа введите имя пользователя и пароль.



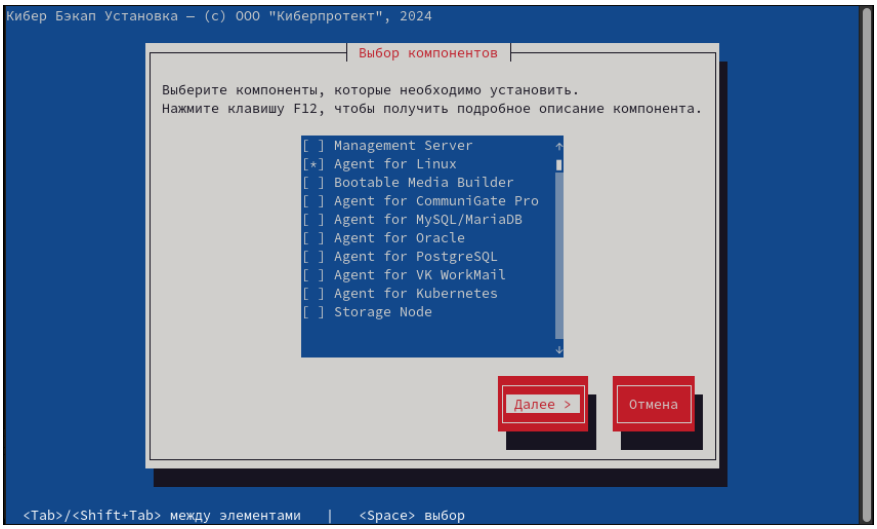
Проведите проверку работы модуля командой, в выводе которой должны отобразиться диски, разделы, массивы и тома LVM, выполнив команду:

```
/usr/lib/Acronis/BackupAndRecovery/dsk_supp_test
```

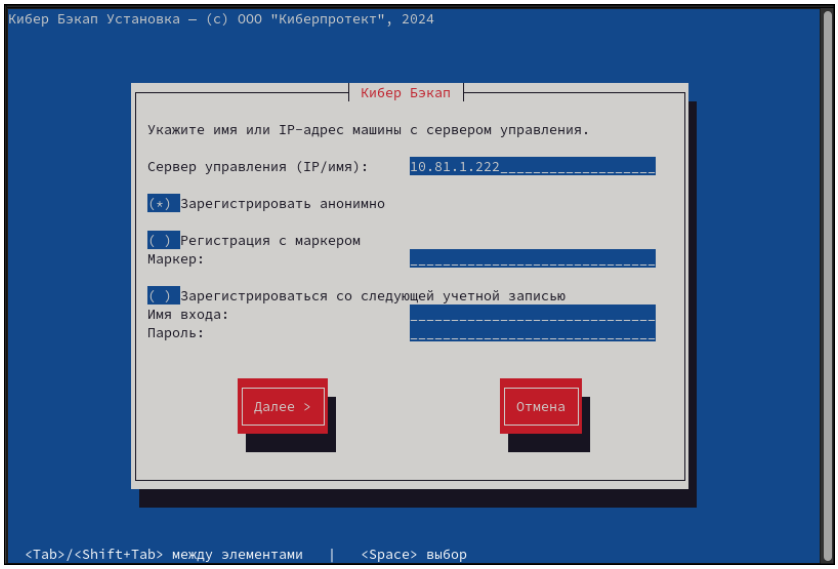
Установка агента

Агенты устанавливаются на локальных машинах и должны быть подключены к серверу управления для создания резервных копий.

Для установки **CyberBackup Агент** выберите соответствующий компонент на этапе выбора компонентов.

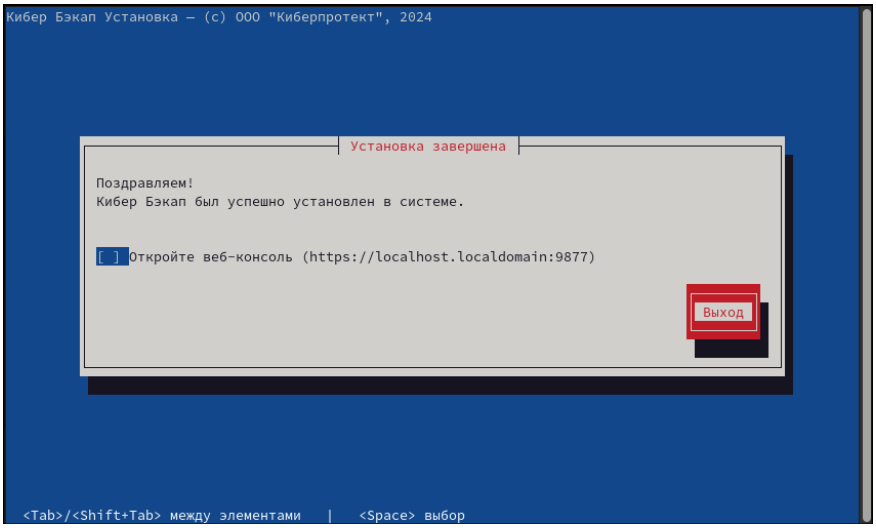


Далее необходимо настроить подключение, указав **имя** или **IP-адрес** машины с установленным сервером управления.

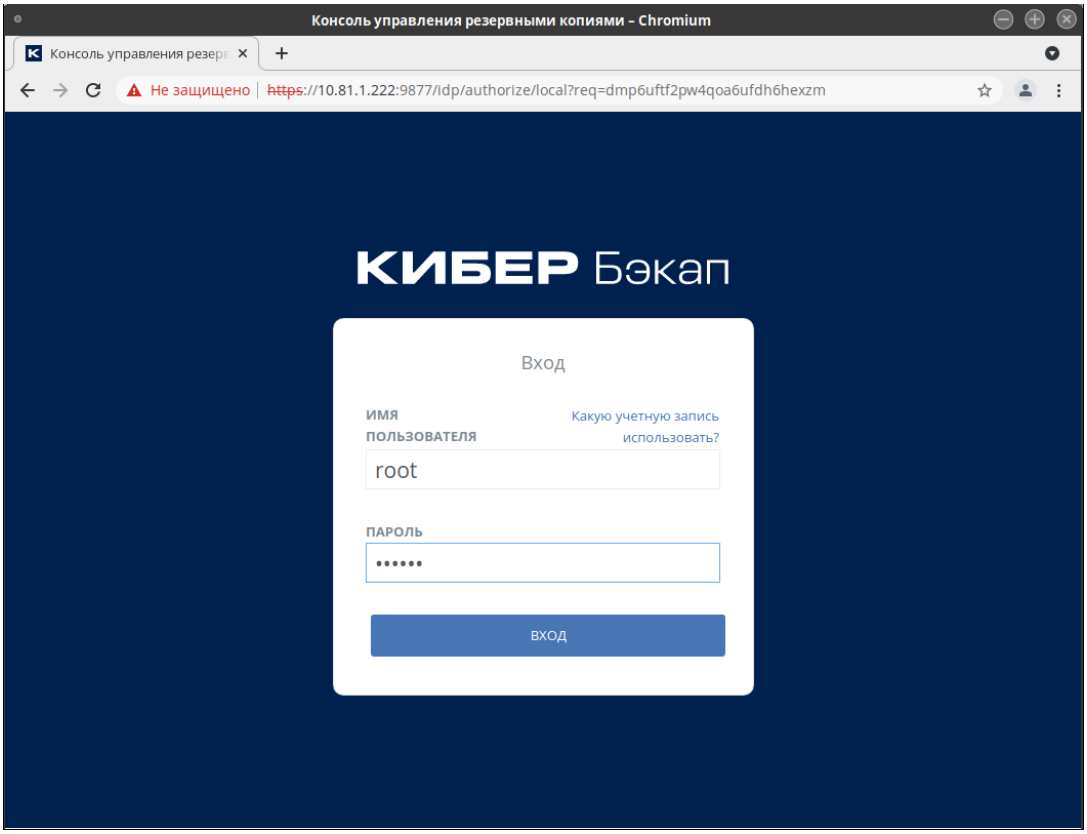


При нажатии на кнопку **Далее** начнется процесс установки агента.

После завершения установки можно выбрать пункт «**Откройте веб-консоль**», а затем нажать **Выход**. В таком случае, веб-консоль **Cyber Protect** откроется в вашем веб-браузере, установленном по умолчанию.



Вы также можете самостоятельно открыть нужный браузер и перейти по адресу https://10.81.1.222:9877. Для входа введите имя пользователя и пароль.



Создание плана выполнения резервной копии

Прежде чем создавать план, нужно добавить хранилище. Для этого выберите пункт **«Резервные копии»** — **«Добавить хранилище»**. Выберите и настройте один из предложенных вариантов.

Далее создайте план, выбрав в правом меню пункт **«Планы»**. Их может быть несколько типов:

- **«Резервное копирование»** — отвечает за создание резервной копии;
- **«Репликация резервной копии»** — создание дополнительной копии синхронизированной с основной для восстановления в случае, если исходная копия недоступна или повреждена.
- **«Проверка»** — план проверок созданных резервных копий
- **«Очистка»** — план удаления ранних резервных копий для освобождения места под новые.
- **«Преобразование в ВМ»** — перевод созданной резервной копии диска в виртуальную машину.
- **«Репликация ВМ»** — создание дополнительной виртуальной машины синхронизированной с основной для повышения надежности хранения.

Выберите **«Резервное копирование»** и нажмите **«Создать план».** Настройте план, указав расписание его выполнения, устройства, с которых будет создаваться резервная копия, место хранения (ранее добавленное хранилище) и срок его хранения. Дополнительно можно указать использование шифрования. Указав вышеперечисленные данные — нажмите **«Создать»**. Созданный сразу появится в списке выбора. Его можно запустить сразу, изменить его параметры или посмотреть историю его выполнения, где отображается результат его работы.

Дополнительную документацию по программе и более подробное описание функций можно посмотреть в официальной документации, нажав на знак вопроса в правом верхнем углу и выбрав пункт **«Документация».**

Для использования функциональных возможностей **CyberBackup** необходимо приобрести лицензию.

ПО для образовательного процесса – redos-education

Установка утилиты
Возможности утилиты
Информация о пакетах

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: redos-education-1.7-3

Redos-education – программное обеспечение для образовательного процесса, созданное компанией РЕД СОФТ для удобного управления рядом пакетов из репозитория РЕД ОС.

Вы можете подробнее ознакомиться с установкой и работой утилиты **redos-education**, просмотрев наши обучающие видео:

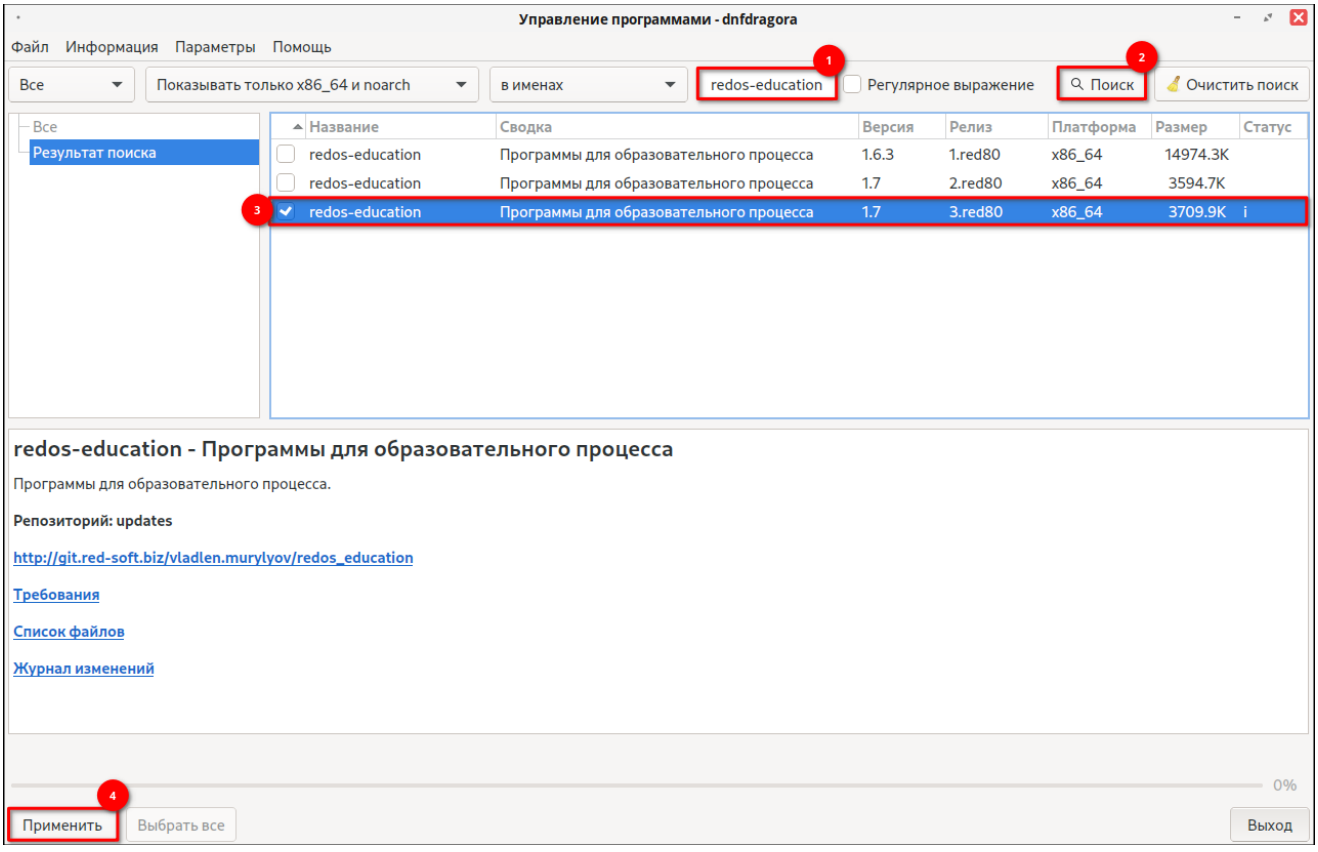
- на **RuTube** — ПО для образовательного процесса в РЕД ОС;
- в **Яндекс.Дзен** — ПО для образовательного процесса в РЕД ОС;
- в **VK Видео** — ПО для образовательного процесса в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка утилиты

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**redos-education**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

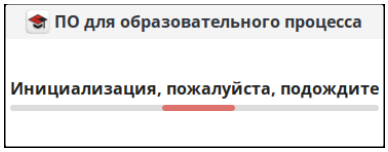
и выполните команду:

```
dnf install redos-education
```

Дальнейшая работа в программе выполняется от локального пользователя.

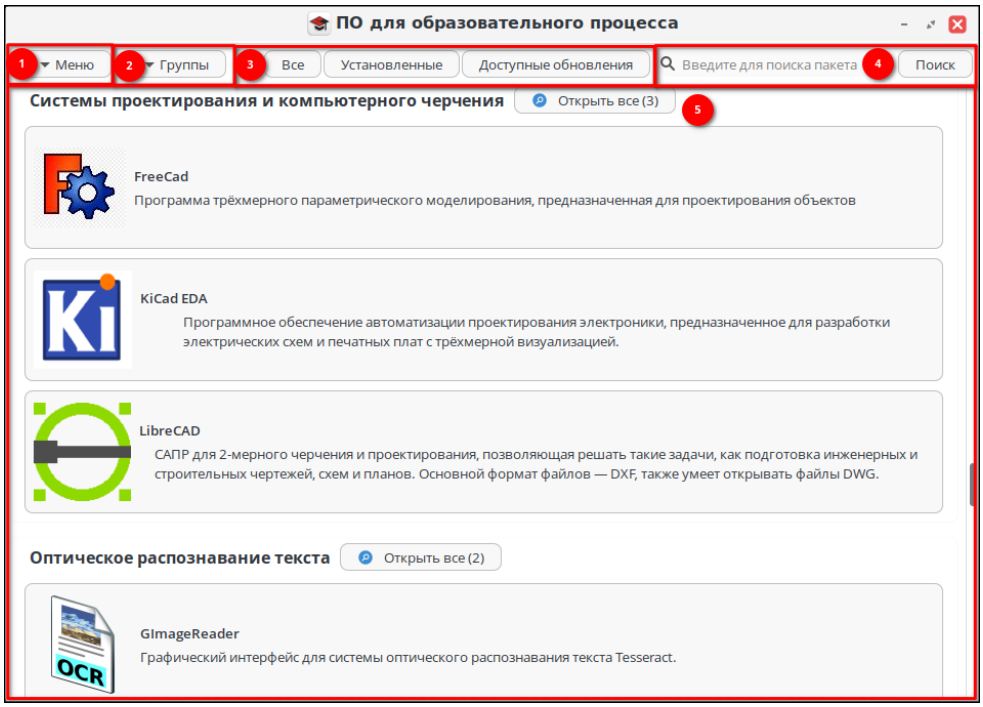
После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**ПО для образовательного процесса**».

При запуске утилиты будет открыто окно инициализации.



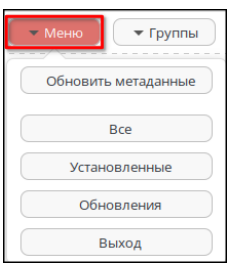
Возможности утилиты

Окно программы выглядит следующим образом:



1. **Меню программы** — представляет собой выпадающий список, здесь доступны такие действия, как:

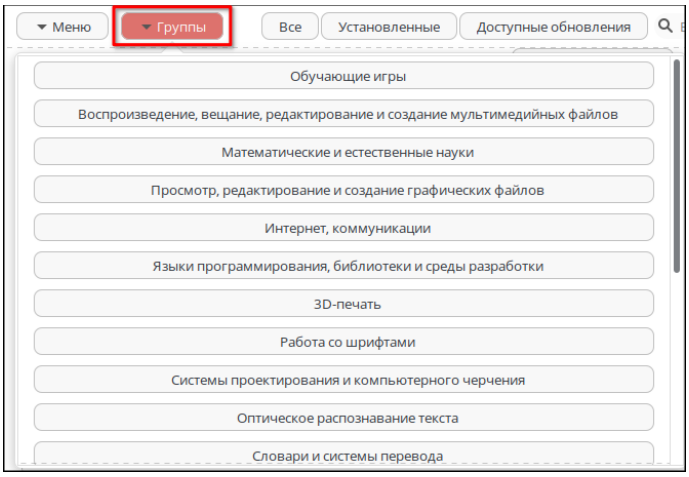
- обновление метаданных;
- отображение всех доступных утилит;
- отображение только установленных пакетов;
- отображение пакетов, требующих обновления;
- выход из программы.



2 . **Группы** — представляет собой выпадающий список доступных групп, в которые объединены утилиты, список служит навигационным меню для быстрого перехода между группами приложений:

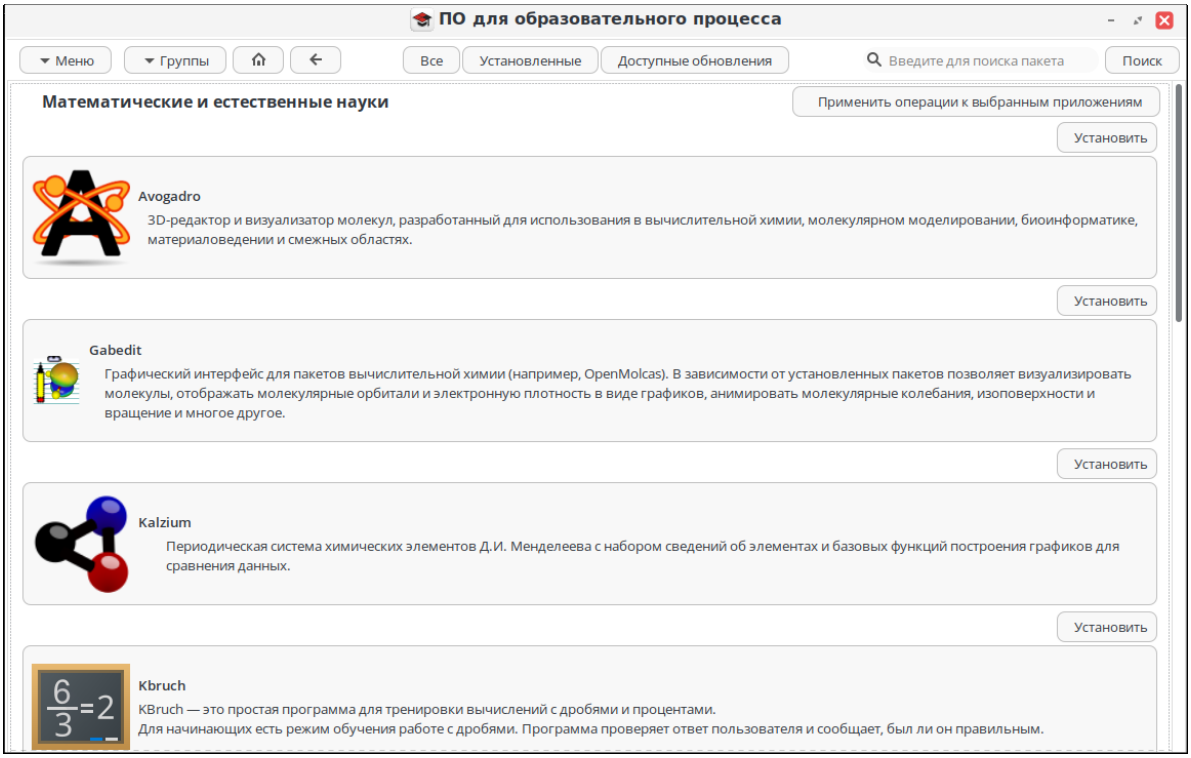
- системы проектирования и черчения;
- словари и системы перевода;
- работа с дисками;

- работа с документами;
- работа со шрифтами и т.д.



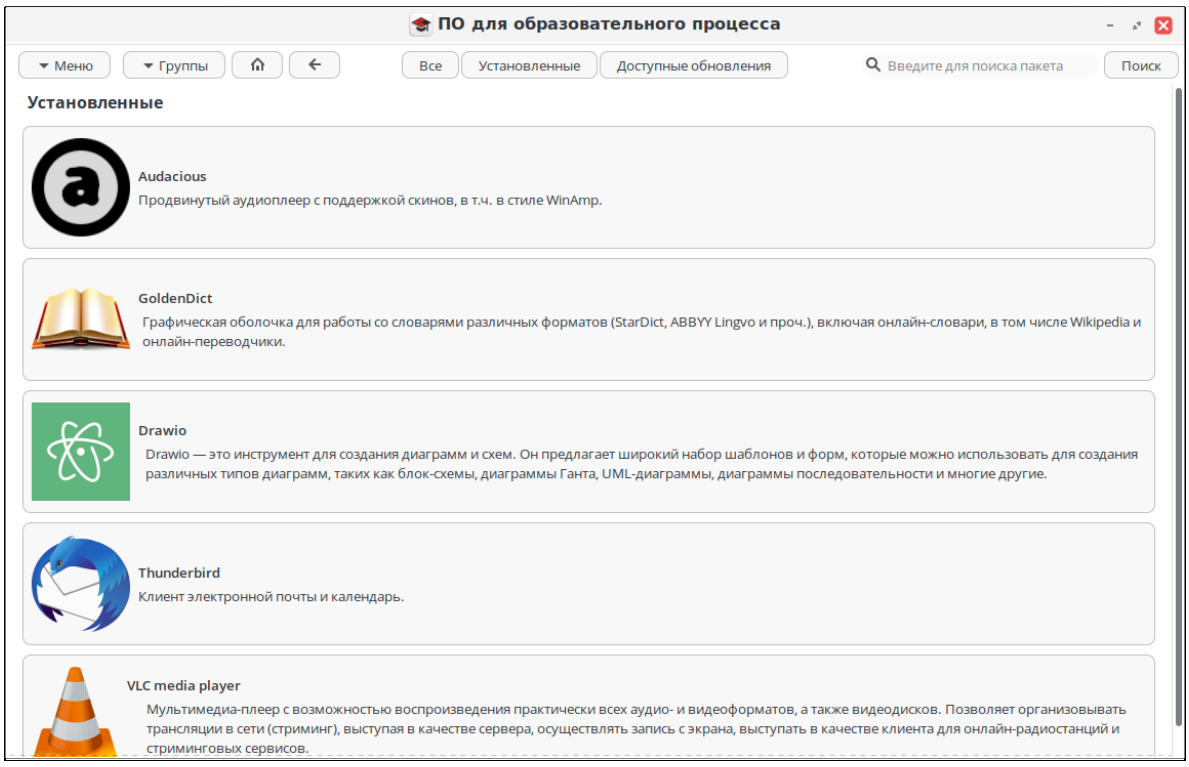
При выборе любого из пунктов будет открыта соответствующая ему страница приложения с перечнем утилит, которые входят в данную группу.

Пример отображения содержимого группы «**Математические и естественные науки**»:

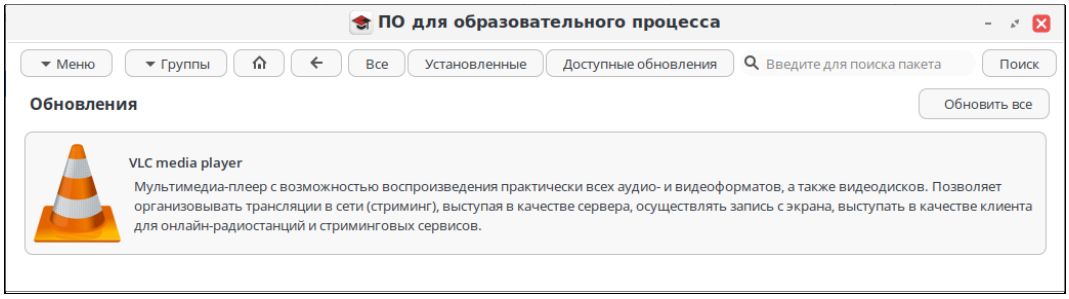


3. **Секции приложений** — отображение всех доступных утилит, отображение только установленных утилит или отображение утилит, требующих обновлений.

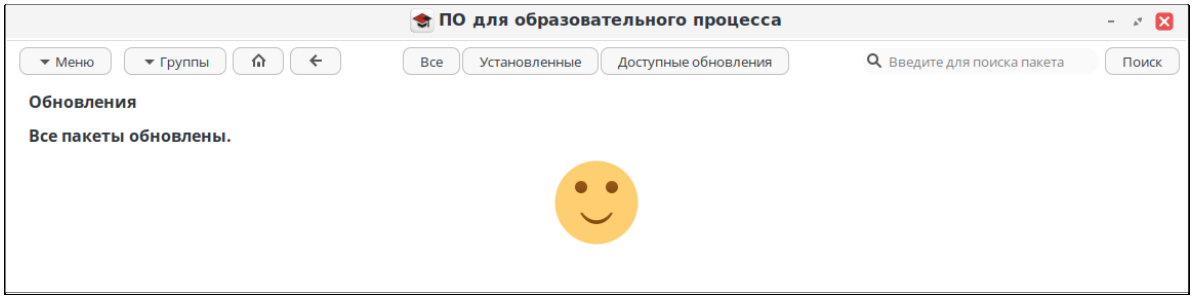
Отображение установленных утилит выглядит следующим образом:



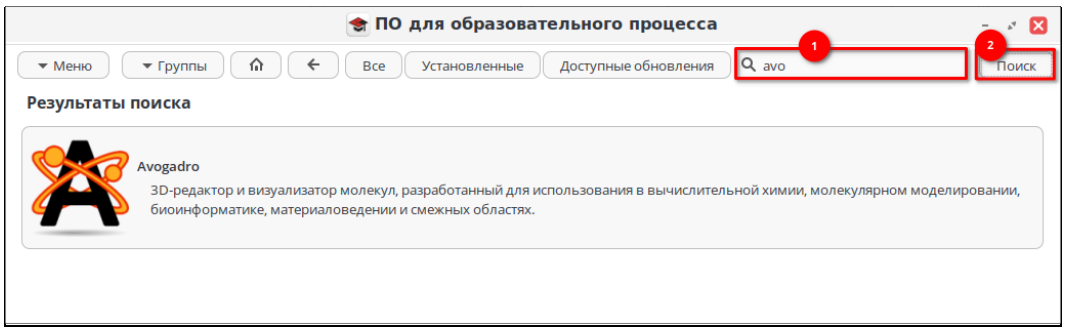
Отображение утилит, требующих обновлений, выглядит следующим образом:



В случае отсутствия доступных обновлений будет выведено сообщение:



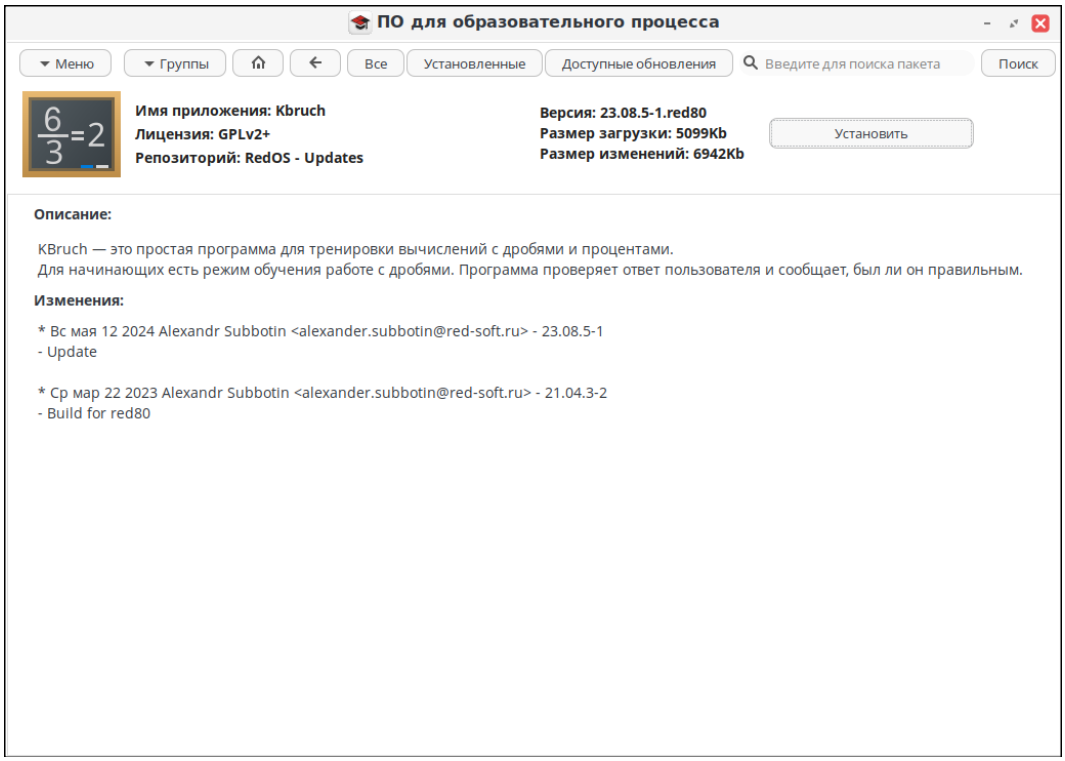
4. **Поиск утилит** — в строке поиска необходимо ввести название программы (1) и нажать кнопку «**Поиск**» (2).



5. **Поле** для непосредственного **отображения утилит** и информационных сообщений.

Информация о пакетах

Для открытия справочной информации, описания и списка изменений определенного приложения необходимо просто кликнуть по нужной утилите.



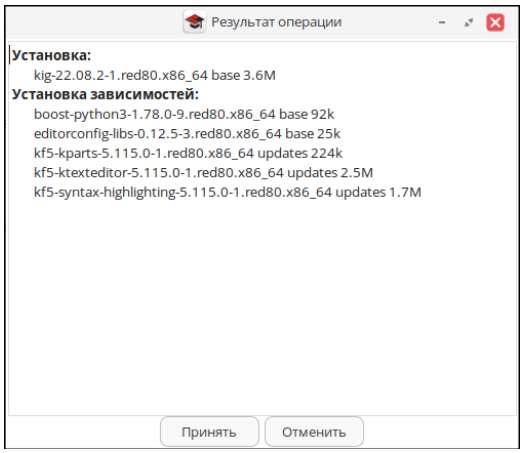
На данной странице можно ознакомиться со следующей информацией:

- имя rpm-пакета;
- лицензия, под которой распространяется данная утилита;
- имя репозитория, который предоставляет данный пакет;
- версия утилиты;
- размер загрузки и изменений в ОС после установки;
- описание утилиты;
- скриншоты работы в утилите;
- список изменений.

Список команд, которые можно выполнить с выбранной утилитой:

- установка утилиты;
- удаление утилиты;
- обновление утилиты;
- запуск утилиты после установки в ОС.

При выборе команды установки, удаления или обновления появится окно транзакции, которое оповещает пользователя о затрагиваемых зависимостях. Стоит обращать внимание на то, какие зависимости выдаются в данном окне транзакции. Если пользователь согласен с изменениями, которые будут внесены в ОС, то следует согласиться с результатами транзакции, в ином случае — отклонить.


Результат операции
Установка:
kig-22.08.2-1.red80.x86_64 base 3.6M
Установка зависимостей:
boost-python3-1.78.0-9.red80.x86_64 base 92k
editorconfig-libs-0.12.5-3.red80.x86_64 base 25k
kf5-kparts-5.115.0-1.red80.x86_64 updates 224k
kf5-ktexteditor-5.115.0-1.red80.x86_64 updates 2.5M
kf5-syntax-highlighting-5.115.0-1.red80.x86_64 updates 1.7M
Принять
Отменить

OpenBoard - программа для работы с интерактивными досками

Установка
Обзор программы
Запись экрана

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: OpenBoard-1.6.1-1

OpenBoard – кроссплатформенное приложение для интерактивной доски с открытым исходным кодом. Приложение может быть использовано как с интерактивными досками, так и с сенсорным или дополнительным экраном либо проектором.

Вы можете подробнее ознакомиться с работой программы **OpenBoard**, просмотрев наши обучающие видео:

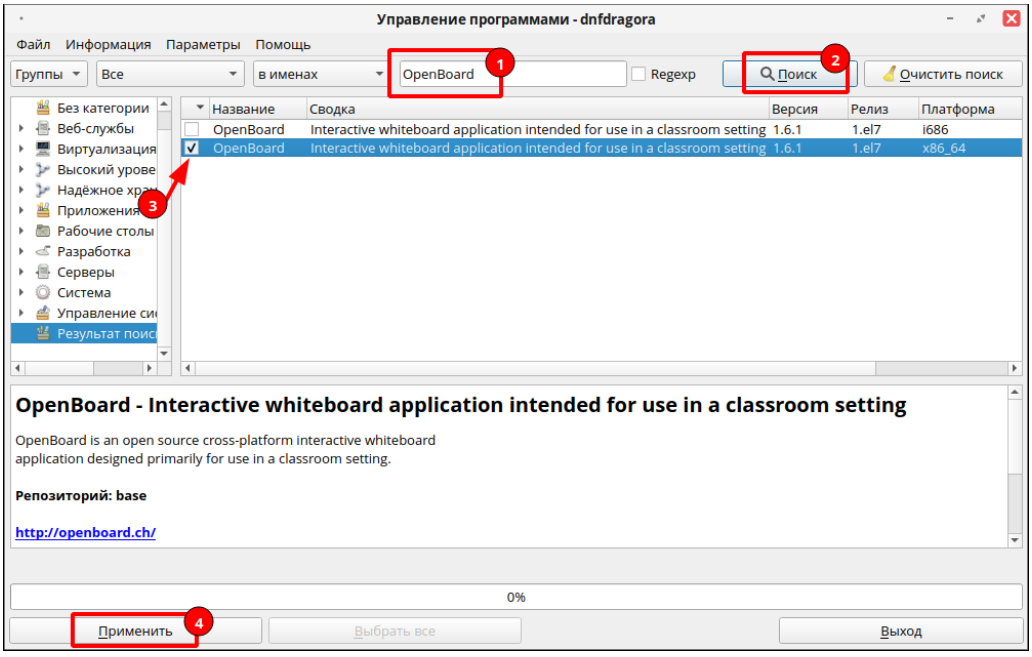
- на **RuTube** — Работа с интерактивными досками в РЕД ОС. OpenBoard;
- в **Яндекс.Дзен** — Работа с интерактивными досками в РЕД ОС. OpenBoard;
- в **VK Видео** — Работа с интерактивными досками в РЕД ОС. OpenBoard.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**OpenBoard**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

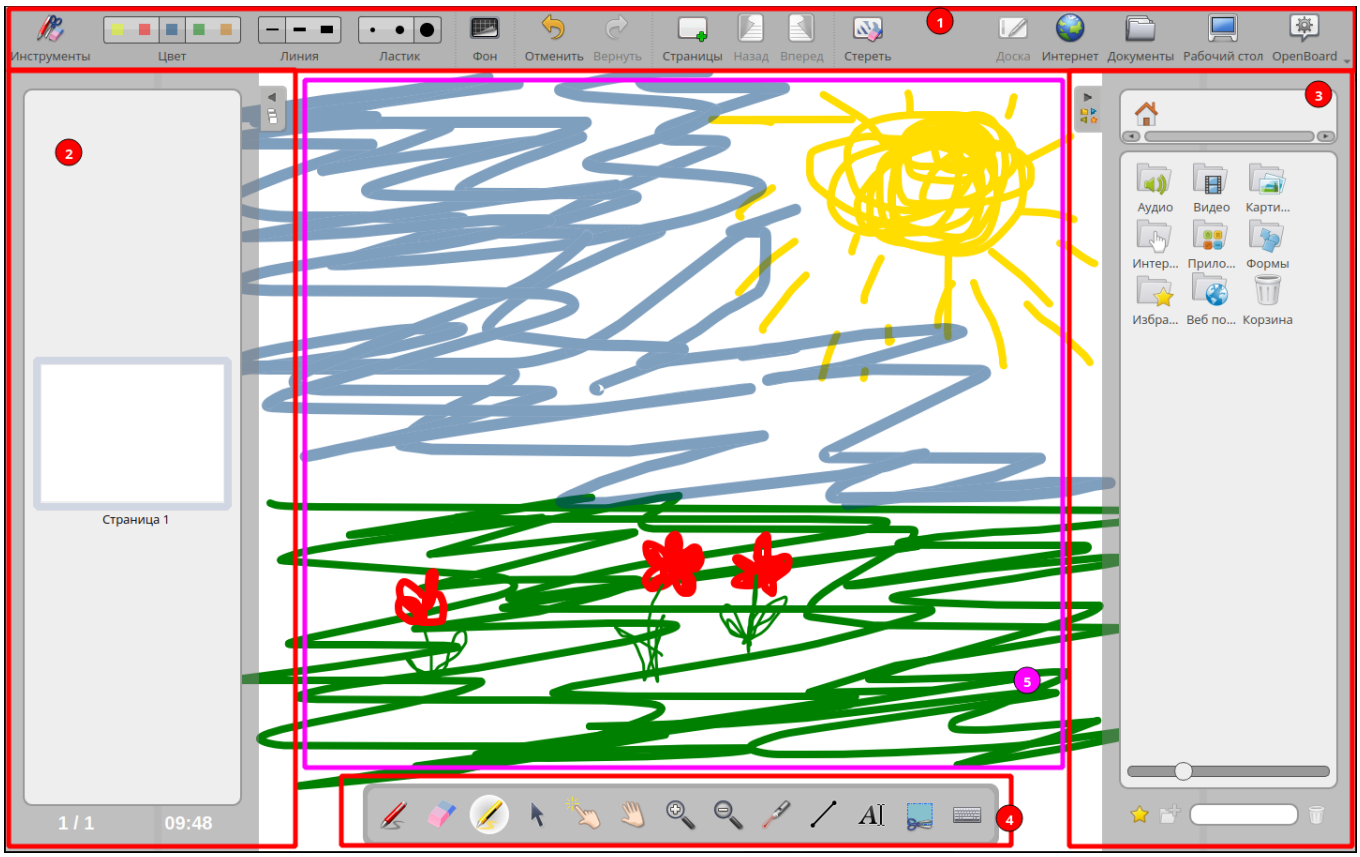
```
dnf install OpenBoard
```

Дальнейшая работа в программе выполняется от локального пользователя.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**OpenBoard**».

Описание программы

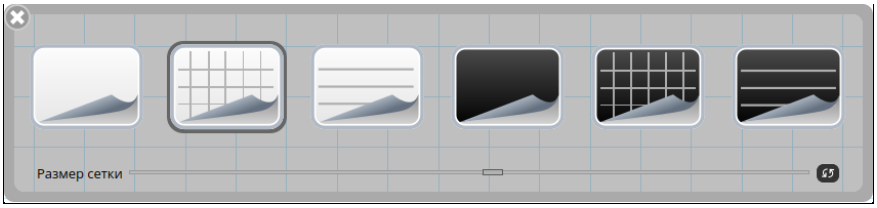
Интерфейс программы довольно прост и разделён на несколько типовых элементов. По умолчанию **OpenBoard** открывается в режиме доски на весь экран.



1. *Панель управления* – здесь доступны основные действия для быстрой работы с программой.

Можно сменить цвет линии, толщину линии, размер ластика.

Доступна смена фона – пустой белый или темный фон, фон с горизонтальными линиями, фон с сеткой, также можно изменить размер сетки.



Далее доступны кнопки для *отмены* или *возврата* выполненных действий, добавление новой пустой страницы и кнопки навигации по страницам (*Назад* и *Вперед*).

Кнопка «**Стереть**» очищает все рабочее пространство.

Далее представлены следующие кнопки:

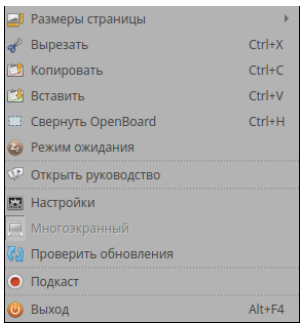
- *Интернет* – встроенный в **OpenBoard** браузер;
- *Документы* – для навигации по документам. Можно загрузить готовую презентацию и, для наглядности, выделять важные моменты и рисовать на слайдах.

  Поддерживаемые форматы программы **OpenBoard**:

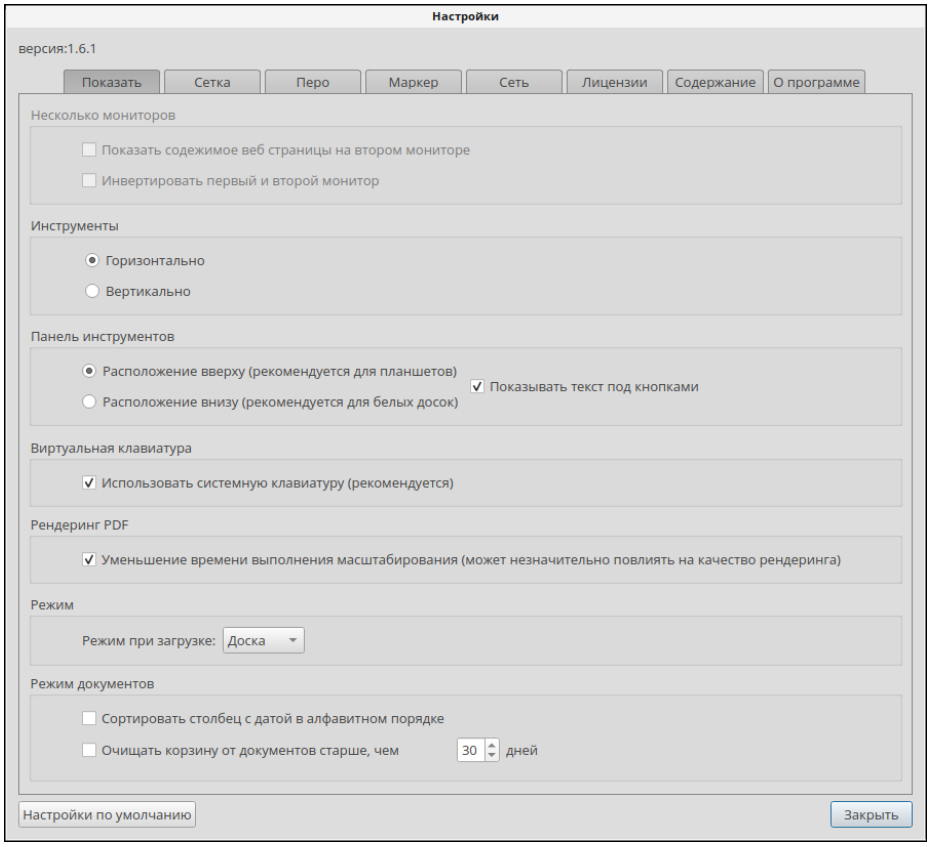
  - файлы, созданные в OpenBoard;
  - файлы в формате **PDF**;
  - изображения в формате **PNG** и **JPG**.

- *Рабочий стол* – кнопка переключения на рабочий стол. В таком режиме панель инструментов **OpenBoard** будет доступна в левой части экрана. Для демонстрации можно открыть браузер или собственный документ и использовать все необходимые инструменты.

- *OpenBoard* – контекстное меню программы с некоторыми дополнительными действиями, такими как выбор размеров страницы, вырезать, копировать, вставить, свернуть программу, перейти в режим ожидания, открыть руководство по программе, пункт настроек программы, проверка обновлений, запись подкаста и выход из программы.

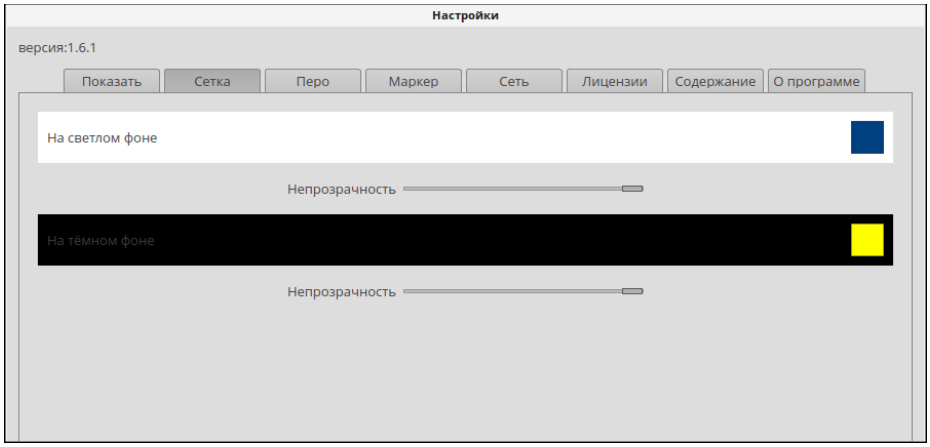


Для детальной настройки программы необходимо открыть пункт меню «**Настройки**».



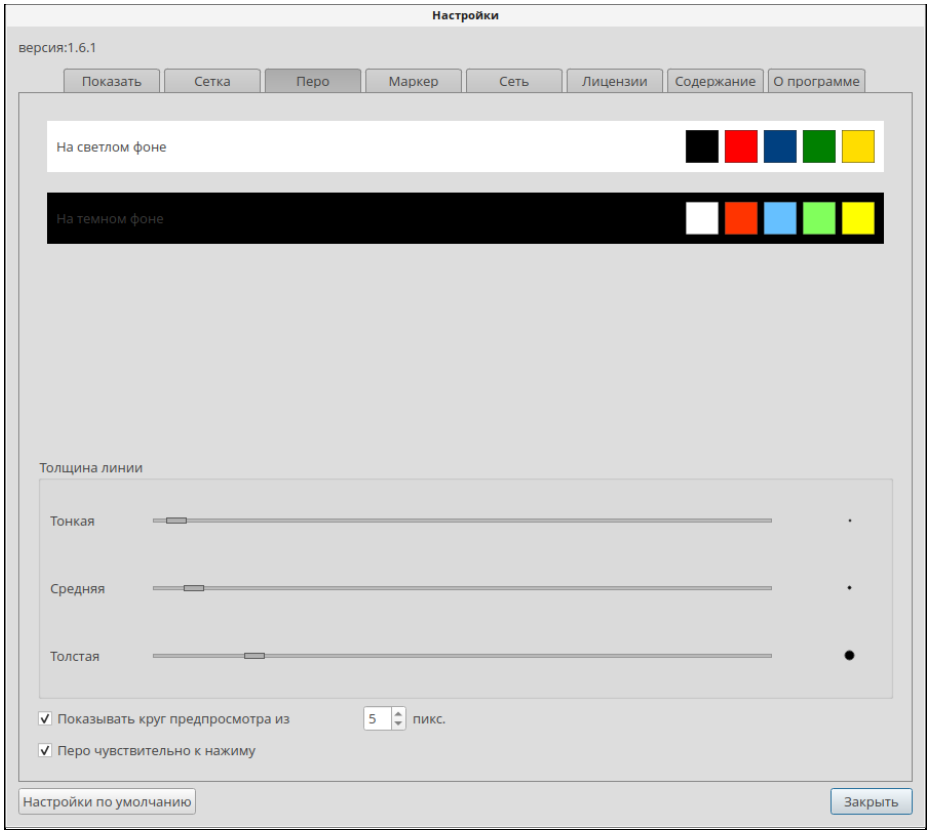
На вкладке «**Показать**» можно изменить отображение инструментов с горизонтального на вертикальное. Если доска висит высоко, полезной функцией будет смена положения панели инструментов. Если требуется компактность, можно убрать текст под кнопками панели инструментов. Далее расположены настройки *системной клавиатуры* и *рендеринг PDF*. Затем можно выбрать режим при загрузке – доска или десктоп.

На вкладке «**Сетка**» доступны настройки линий сетки на белом и темном фоне – непрозрачность и цвет линий.

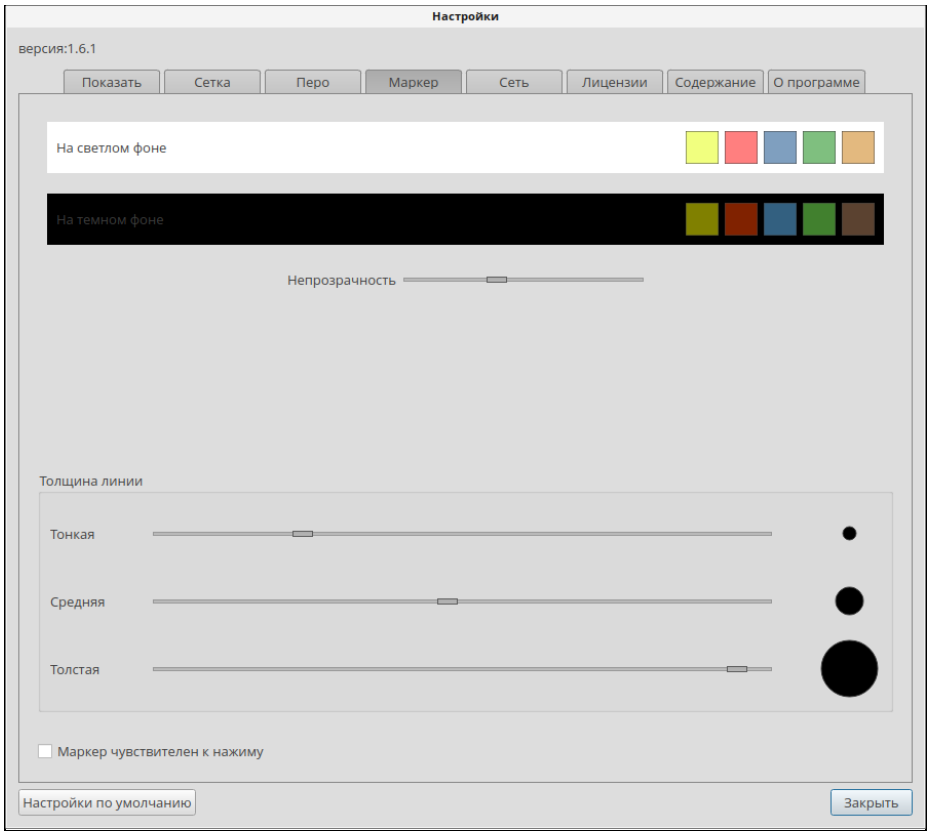


На вкладке «**Перо**» можно настроить доступные в панели инструментов цвета пера на белом и темном фоне, а также задать толщину

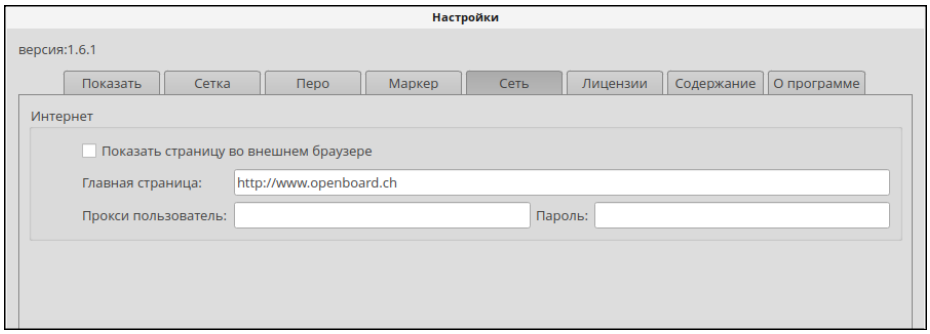
линии для вариантов *тонкая*, *средняя* и *толстая*.



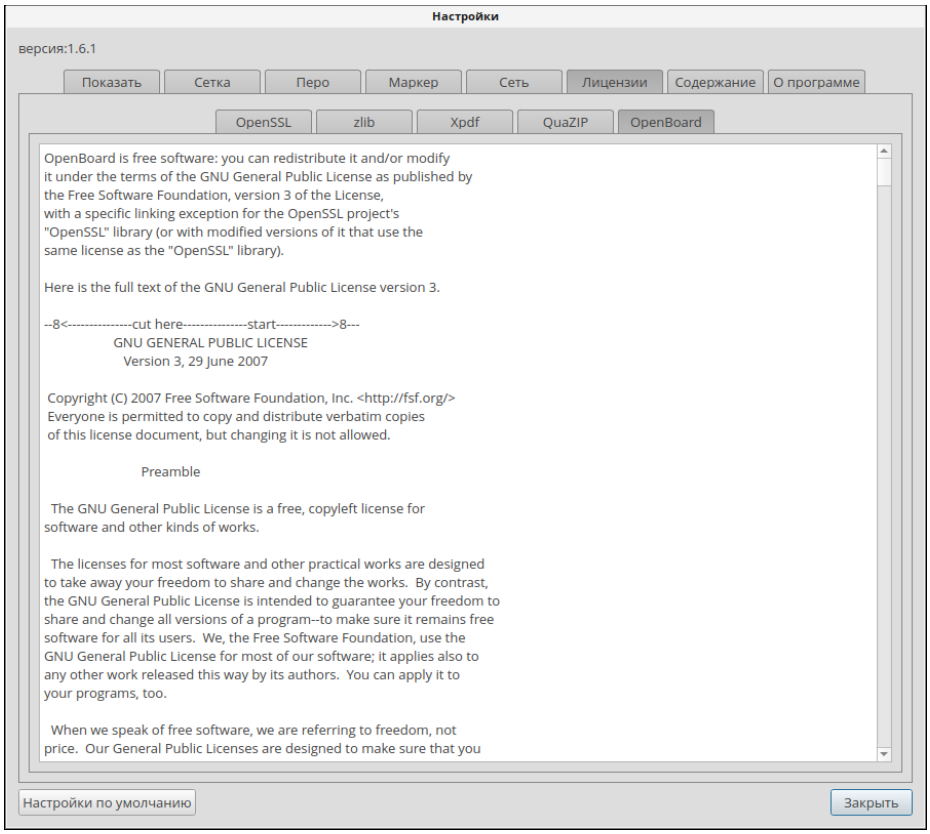
На вкладке «**Маркер**» производится настройка маркера – доступные цвета на светлом и темном фоне доски, непрозрачность, а также задается толщина линии для вариантов *тонкая*, *средняя* и *толстая*.



На вкладке «**Сеть**» задается адрес главной страницы, возможность открытия страниц во внешнем браузере, а также прокси пользователь и его пароль при наличии.



На вкладке «**Лицензии**» доступны необходимые лицензионные соглашения.



На вкладках «**Содержание**» и «**О программе**» приведены благодарности команде и общие сведения о программе.

При нажатии на кнопку «**Настройки по умолчанию**» будут отменены все установленные тонкие настройки и возвращены значения настроек по умолчанию.

2 . *Панель навигации* – здесь отображаются миниатюры открытых страниц. Для перехода к странице выберите соответствующую миниатюру. При наведении указателя на миниатюру страницы появятся кнопки «**Удалить**» и «**Копировать**».

3. *Библиотека встроенных материалов* – объекты распределены по каталогам в соответствии с форматом и тематикой. Для добавления объекта из библиотеки материалов необходимо открыть каталог и выбрать любой нужный объект, затем перенести его с помощью мыши на рабочую область.

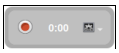
4. *Панель с инструментами для работы в режиме доски* – панель не закреплена, поэтому ее можно перенести в любое удобное место. Доступные инструменты:

- **Карандаш** — отвечает за добавление рукописного объекта;
- **Ластик** — удаление объектов с рабочей области. Размер ластика можно регулировать;
- **Маркер** для выделения — полупрозрачный маркер для выделения текста или другого объекта;
- **Курсор** — позволяет выделить отдельную область, элемент или группу элементов. При нажатии курсором по объекту будут открыты дополнительные настройки, например, изменение размера объекта, изменение положения, растягивание или поворот.
- **Взаимодействие с элементами** (палец) — перемещение объекта по рабочему полю;
- **Ладонь** — прокручивание страницы;
- **Масштаб** — увеличение или уменьшение масштаба рабочей области;

- **Указка** — указывание на объект без перемещения и выделения;
- **Отрезок** — создание отрезка любой длины и цвета;
- **Текст** — ввод текста с клавиатуры;
- **Выделение области** — выделение области для копирования на текущую или новую страницу. Работает аналогично скриншоту. Выделенную область также можно сохранить как файл в библиотеке;
- **Экранная клавиатура** — вызов экранной клавиатуры для ввода текста и навигации. Данный инструмент полезен в режиме рабочего стола.

5. *Основная рабочая область*.

Запись экрана

Полезной опцией для работы также является запись экрана (**OpenBoard** — **Подкаст**). При активации подкаста рядом с нижней панелью инструментов появится инструмент для записи видео (

).

При нажатии на кнопку конфигурирования записи подкаста () будет открыто контекстное меню с выбором использования микрофона при записи экрана, публикация видео в интранете или на Youtube.

Для записи видео необходимо нажать на кнопку «**Начать запись экрана**» ().

Для завершения записи необходимо нажать на кнопку «**Завершить запись экрана**» (). По умолчанию видеозаписи сохраняются на рабочий стол.

Veyon - программа управления компьютерным классом

Настройка сервера
Настройка клиента
Проверка работоспособности

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: veyon-4.5.7

Veyon - это программа для мониторинга и управления компьютерами. Она в основном используется в учебных заведениях для виртуальных тренингов или удаленной поддержки.

Вы можете подробнее ознакомиться с работой утилиты **veyon**, просмотрев наши обучающие видео:

- на **RuTube** — Veyon - программа управления компьютерным классом;
- в **Яндекс.Дзен** — Veyon - программа управления компьютерным классом;
- в **VK Видео** — Veyon - программа управления компьютерным классом.

На наших каналах вы также сможете найти много другой полезной информации.

Veyon предлагает множество функций, которые позволяют вам контролировать и получать доступ к компьютерам. Все функции доступны через кнопки на панели инструментов, а также из контекстного меню отдельных компьютеров.

Функции программы:

Функция	Описание
Режим мониторинга	По умолчанию **Veyon** работает в режиме мониторинга. В этом режиме у вас есть обзор всех компьютеров и содержимого их экранов в виде миниатюр. Содержимое экрана обновляется практически в режиме реального времени, поэтому вы можете отслеживать всю активность на выбранных компьютерах. Пока нет подключения, вместо содержимого экрана отображается значок компьютера. После запуска программы значок изначально окрашен в серый цвет. Как только программа обнаруживает, что компьютер недоступен или доступ запрещен, цвет меняется на красный.
Демонстрационный режим	Вы можете использовать демонстрационный режим, чтобы начать презентацию. В этом режиме содержимое вашего экрана или экрана учащегося транслируется на все компьютеры и отображается в режиме реального времени. Вы можете выбрать между полноэкранной и оконной демонстрацией.
Блокировка экранов	Еще один способ привлечь внимание студентов - использовать функцию блокировки экрана. Как и во время полноэкранного показа, все устройства ввода на компьютерах учеников заблокированы. Компьютеры больше не могут быть использованы учениками. Кроме того, отображается символ блокировки, чтобы не отвлекать внимание от открытых приложений.
Удалённый просмотр и удаленное управление	Функции удаленный просмотр и удаленное управление очень похожи. В обоих режимах доступа экран удаленного компьютера отображается в полном размере в отдельном окне. В отличие от режима мониторинга, вы можете детально наблюдать за действиями на компьютере в отдельном окне или вмешиваться самостоятельно.
Включение, перезагрузка и выключение компьютеров	Функции включения, перезагрузки и выключения питания полезны как для административных целей, так и для подготовки и последующего прохождения курсов и экзаменов. Используя эти функции, вы можете удаленно включать, перезагружать или выключать компьютеры.
Вход в систему	Функция входа в систему позволяет удаленно входить в систему определенному пользователю на всех компьютерах.
Послать текстовое сообщение	Еще одна возможность взаимодействия с пользователем - отправить текстовое сообщение отдельным или всем участникам курса. Текстовое сообщение отображается на компьютерах в виде окна сообщения.
Запустить программу	Если определенная программа должна быть запущена на всех компьютерах, вы можете использовать функцию «Запуск программы» на панели инструментов.
Открыть веб-сайт	Если вы хотите, чтобы все учащиеся открывали определенный веб-сайт, вы можете автоматически разрешить открытие этого веб-сайта на всех компьютерах.
Передача файлов	Используя функцию передачи файлов, вы можете легко передавать файлы всем учащимся и, при необходимости, открывать переданные файлы впоследствии.
Скриншот	Veyon позволяет сохранять текущее содержимое экрана одного или всех компьютеров в файлах изображений.

Настройка сервера

Для установки veyon перейдите в сеанс пользователя root:

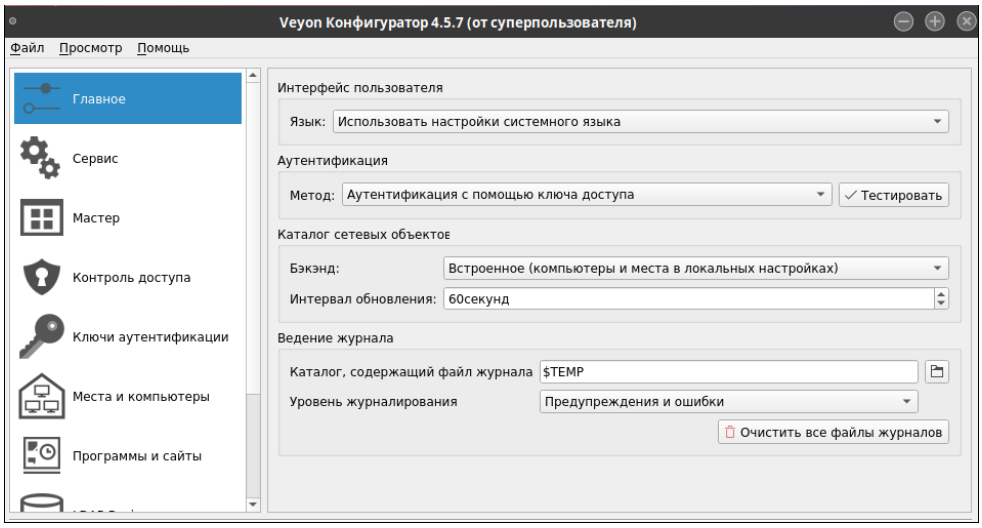
```
su -
```

и выполните команду:

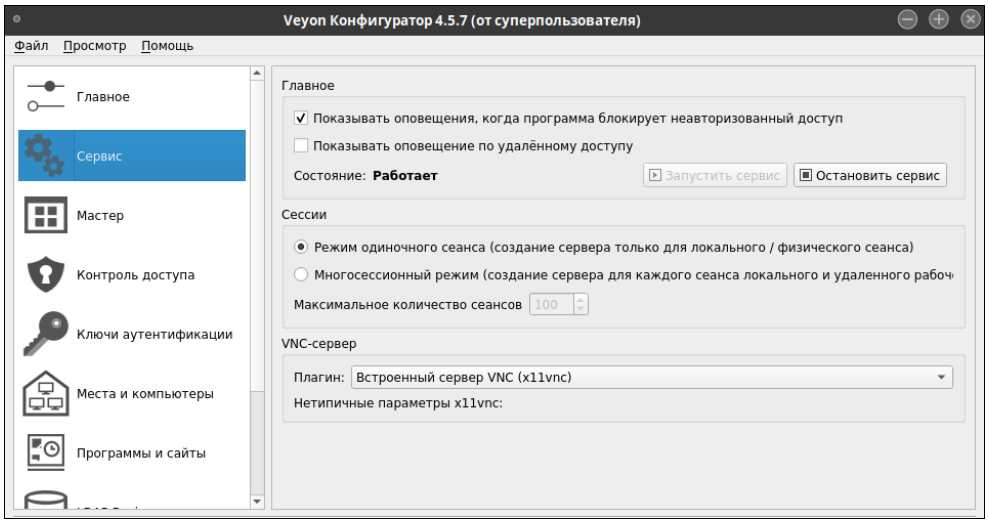
```
dnf install veyon
```

После завершения установки откройте конфигуратор **veyon**. Его можно найти в «**Главном меню**» - «**Администрирование**» - «**Настройка Veyon**».

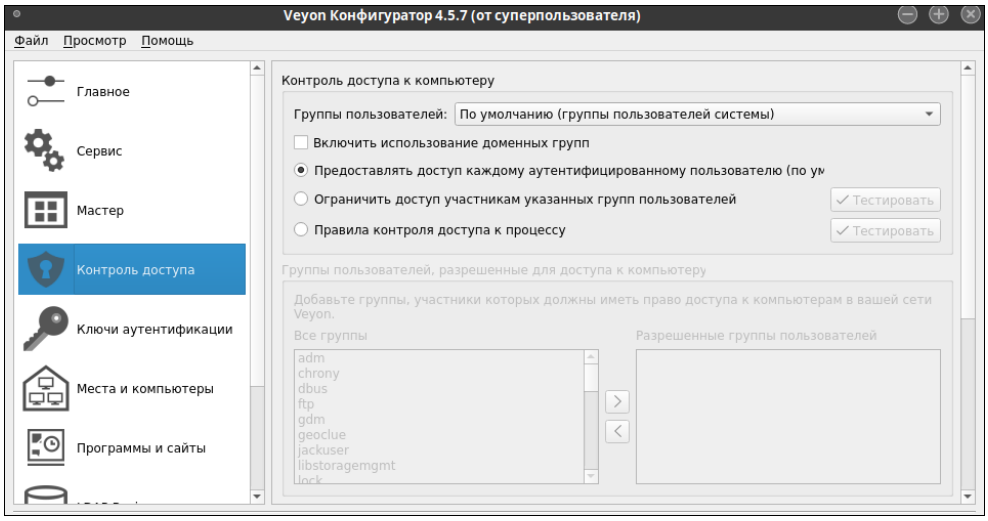
Приступим к настройке. На вкладке «**Главное**» выберите метод аутентификации: «**Аутентификация с помощью ключа доступа**», бэкэнд: «**Встроенное**».



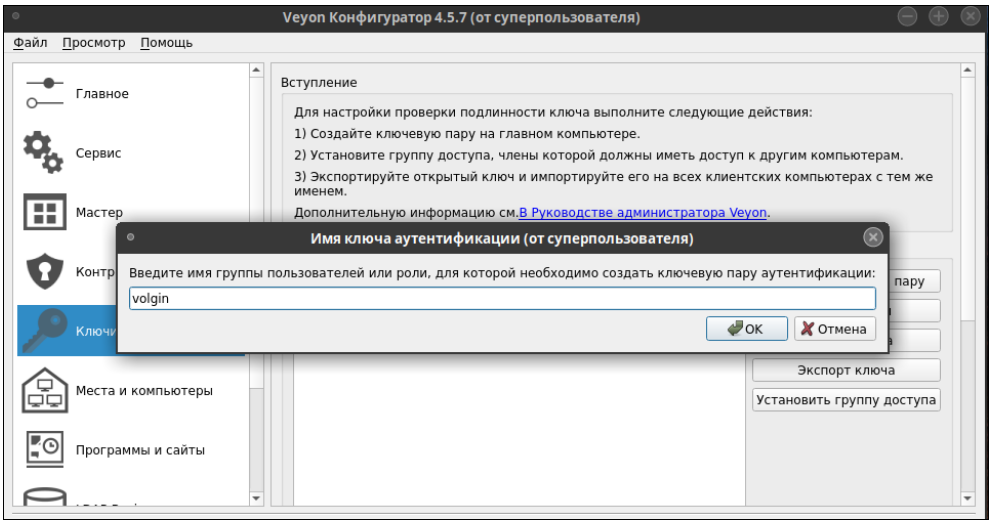
Перейдите во вкладку «**Сервис**», переключите сессии в «**Режим одиночного сеанса**» и запустите сервис.



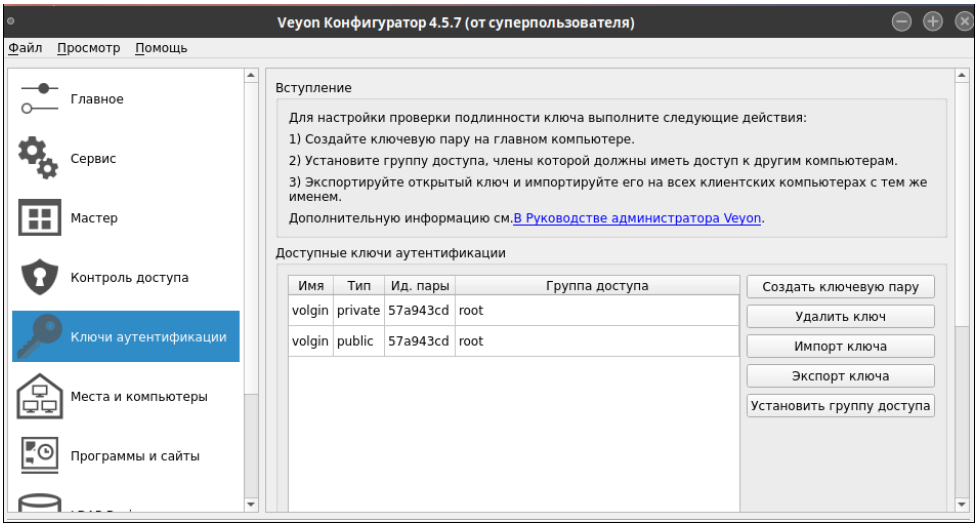
Далее на вкладке «**Контроль доступа**» выставьте группы пользователей: «**По умолчанию**».



На вкладке «**Ключи аутентификации**» нажмите на кнопку «**Создать ключевую пару**» и введите её название.



Будет создано 2 ключа с типом **private** и **public**. Необходимо экспортировать ключ с типом **public** на внешний накопитель. Это нужно для того, чтобы можно было подключиться к клиентскому компьютеру.



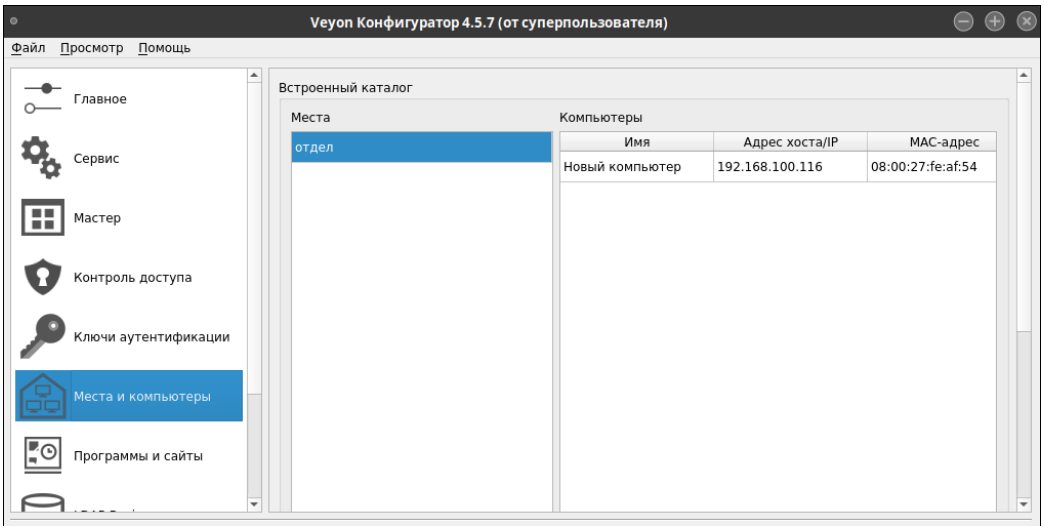
Примечание.

По умолчанию открытый и закрытый ключ будут доступны на чтение всем пользователям (все пользователи будут иметь возможность запускать *Veyon Master*). Чтобы ограничить доступ, необходимо установить группу доступа для закрытого ключа. Пользователи, которым разрешен доступ к компьютерам с помощью *Veyon Master*, должны быть членами группы доступа, заданной для закрытых ключей. Открытый ключ должен быть доступен для чтения всем пользователям.

Для изменения группы доступа следует выбрать ключ и нажать кнопку «**Установить группу доступа**». В открывшемся окне выбрать/указать группу пользователей.

Далее перейдите во вкладку «**Места и компьютеры**». Создайте новое место, дайте ему название, для этого с низу страницы нажмите на «**+**».

Далее добавьте то количество компьютеров клиентов, которое вам требуется. Задайте им имя и укажите **ip**- и **MAC**-адреса.



После этого примените настройки.

Настройка клиента

Для установки veyon перейдите в сеанс пользователя **root**:

```
su -
```

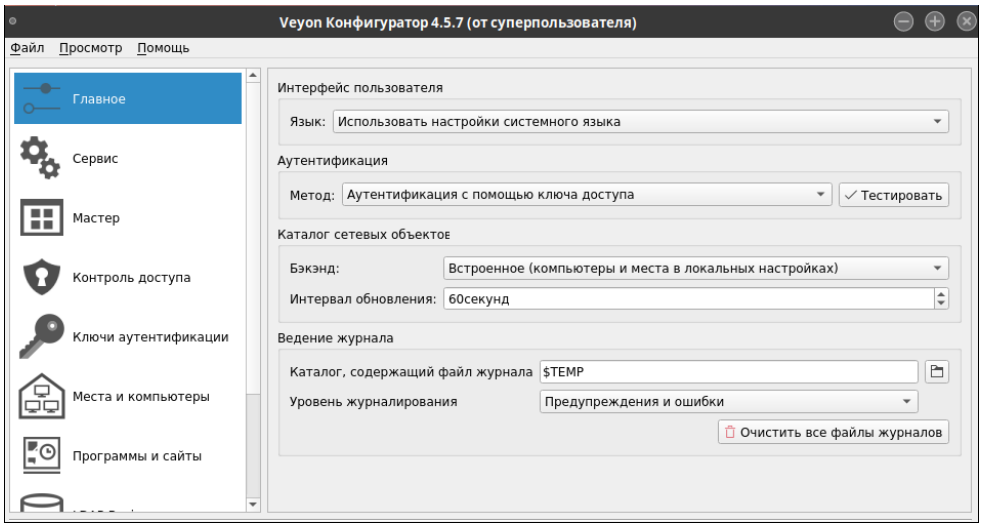
и выполните команду:

```
dnf install veyon
```

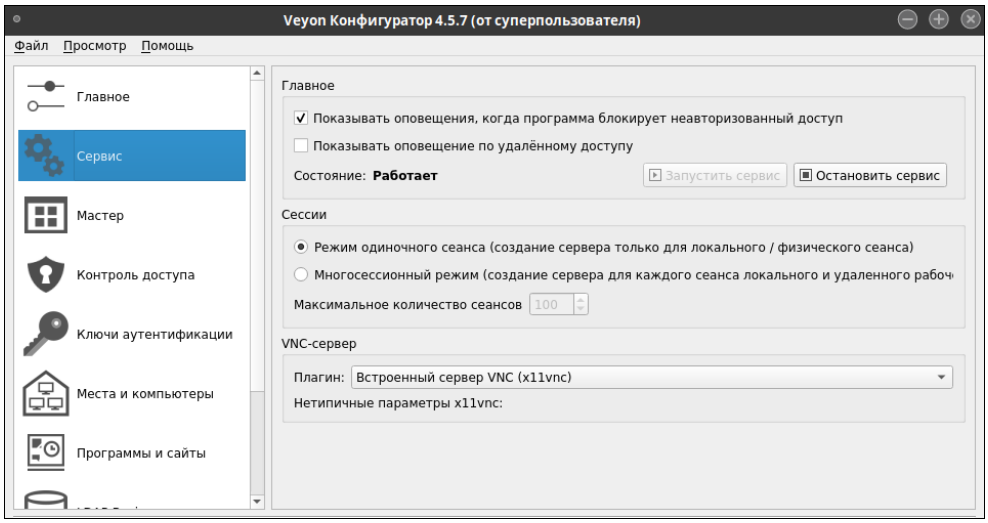
После завершения установки откройте конфигуратор **veyon**. Его можно найти в «**Главном меню**» - «**Администрирование**» - «**Настройка Veyon**».

Откройте «**Настройки Veyon**» и начните настройку программы.

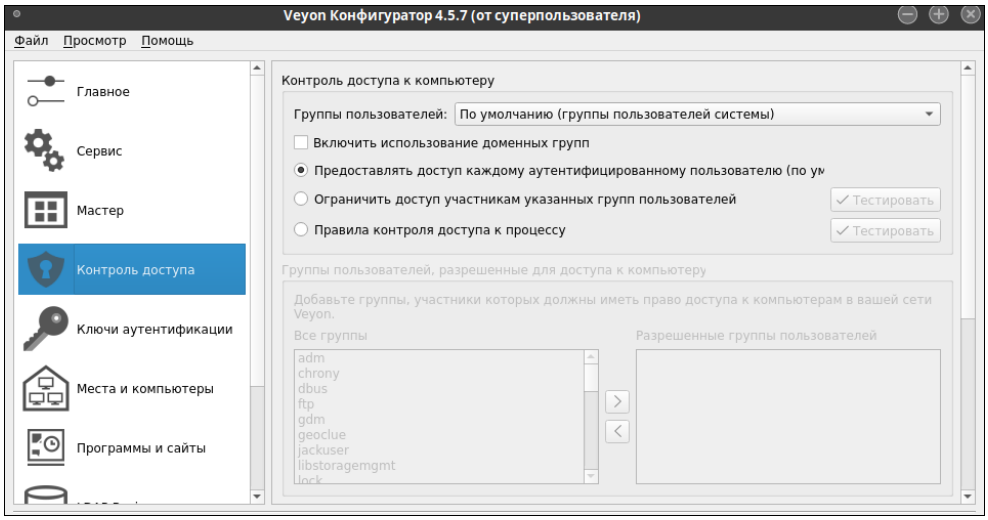
Приступим к настройке. На вкладке «**Главное**» выберите метод аутентификации: «**Аутентификация с помощью ключа доступа**», бэкэнд: «**Встроенное**».



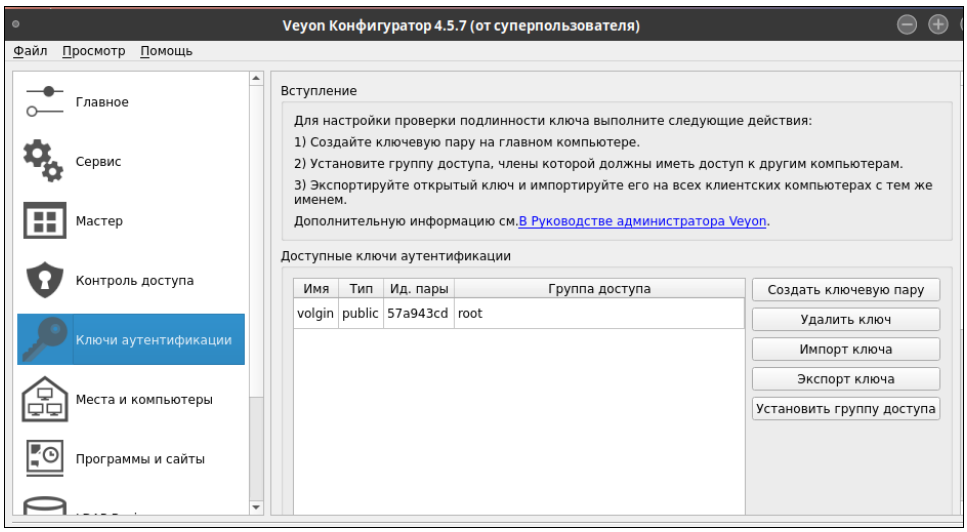
Перейдите во вкладку «**Сервис**», переключите сессии в «**Режим одиночного сеанса**» и запустите сервис.



Далее на вкладке «**Контроль доступа**» выставите группы пользователей: «**По умолчанию**».



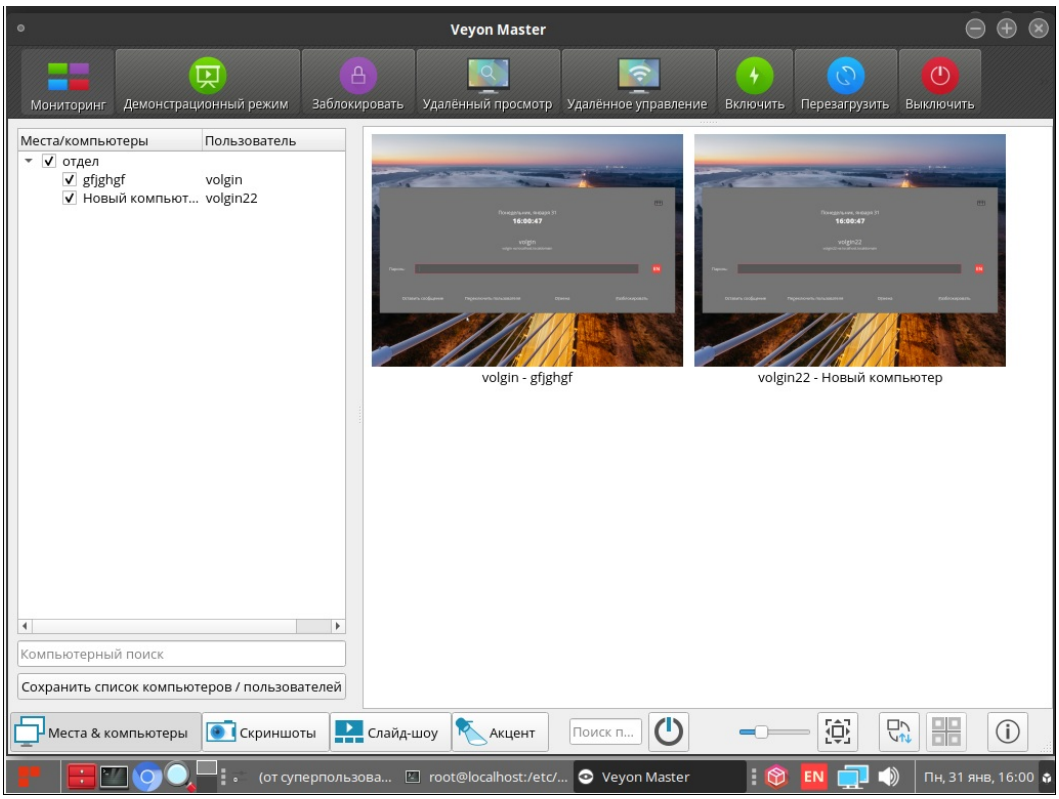
Затем перейдите во вкладку «**Ключи аутентификации**» и импортируйте ключ с внешнего носителя, который вы сгенерировали на сервере.



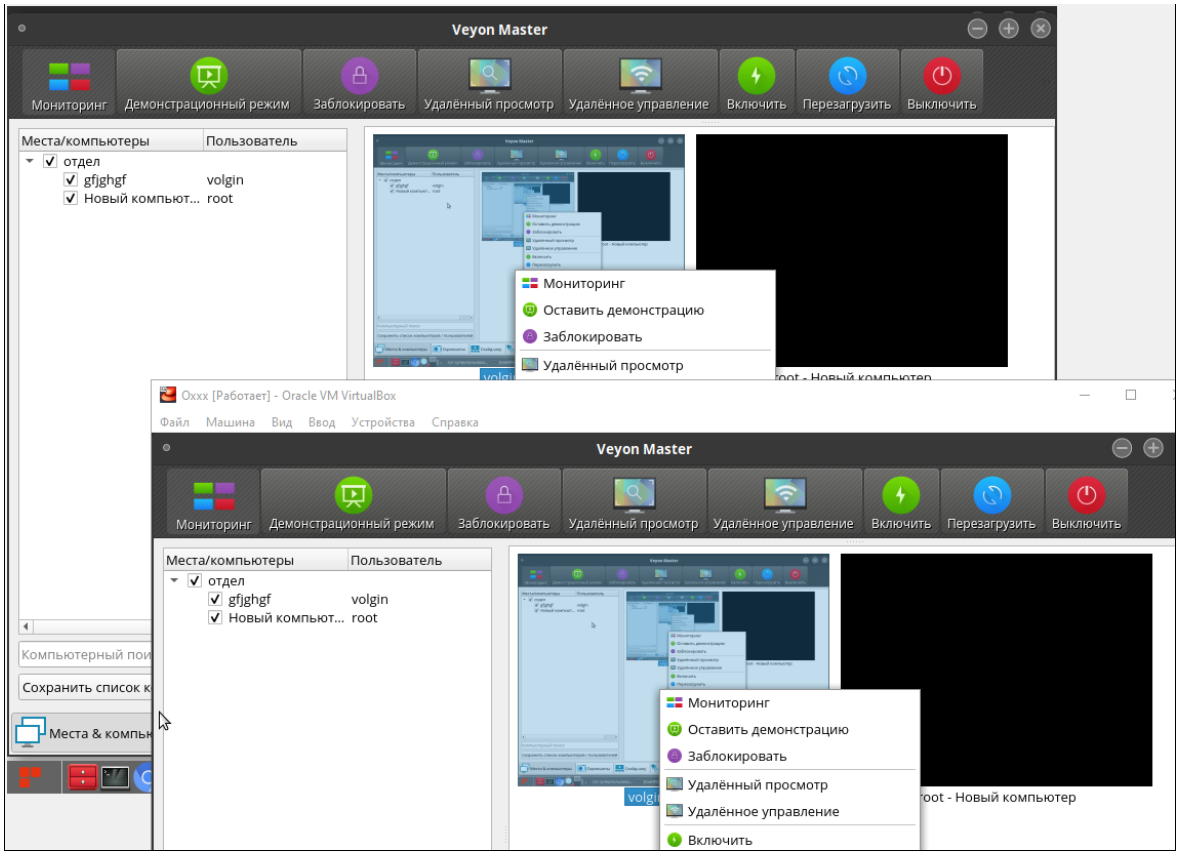
Примените настройки. На этом настройка клиента **veyon** заканчивается.

Проверка работоспособности

Теперь, когда всё настроено, войдите на сервере в «**Монитор Veyon**». Он располагается в «**Главном меню**» - «**Образовательные**» - «**Монитор Veyon**». На вкладке «**Мониторинг**» должны появиться клиентские рабочие места, если компьютеры включены, и всё настроено правильно.



Проверим работоспособность, включив демонстрационный режим.



OpenBabel – программа для работы с химическими структурами и молекулярными системами

Установка OpenBabel
Интерфейс программы и ее основные элементы
Конвертация химических форматов файлов
Разработка на языках программирования C++ и Python
Рекомендации по использованию программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: openbabel-3.1.1-12

OpenBabel — экспертная система анализа химических данных, предоставляющая набор инструментов для преобразования многих форматов химических данных. Она позволяет пользователям искать, преобразовывать, хранить и анализировать данные молекулярного моделирования, химии, твердотельных материалов, биохимии или смежных областей.

OpenBabel имеет функции чтения, записи и преобразования более 110 форматов химических файлов, что делает ее универсальным инструментом для работы с молекулярными данными. Она интегрируется с другими программами для химической инженерии и моделирования, такими как Avogadro, GROMACS, XDrawChem, JMol и другими.

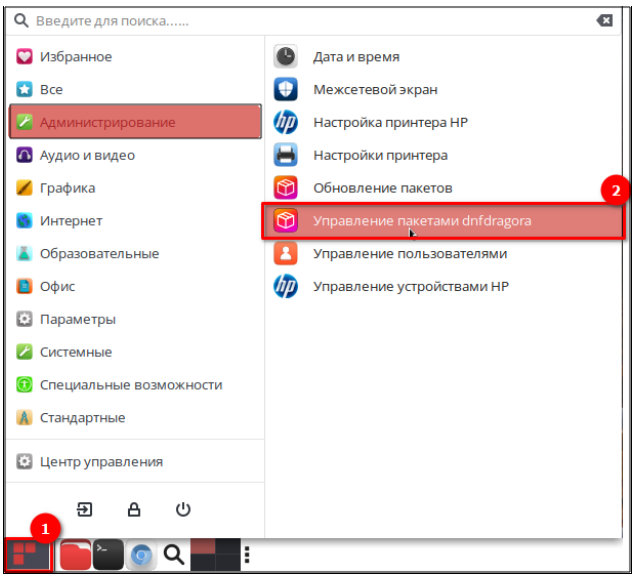
Основные возможности **OpenBabel**:

- конвертация файлов между различными форматами;
- визуализация молекул в 2D и 3D;
- расчет молекулярных свойств, таких как энергия, энтальпия, свободная энергия и т.д.;
- преобразование координат молекул из одной системы в другую;
- интеграция с другими программами и инструментами для химической инженерии;
- поддержка различных типов атомов и связей;
- работа с большими молекулярными сетями;
- поддержка работы с квантово-механическими методами;
- разработка на языках программирования C++ и Python.

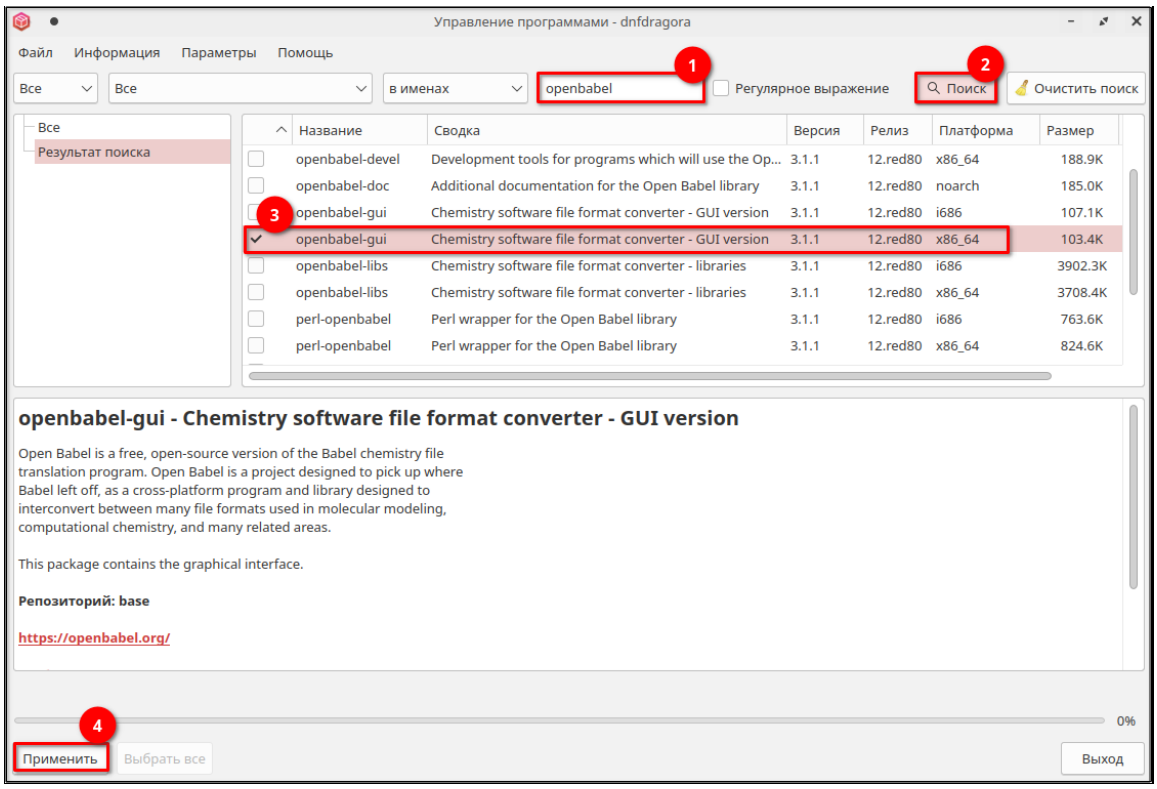
Установка OpenBabel

Программу можно установить через графический менеджер пакетов (**dnfdragora**) или с помощью команд в терминале.

Для установки программы через графический менеджер пакетов перейдите в «**Главное меню**» (1) — «**Администрирование**» — «**Управление пакетами dnfdragora**» (2).



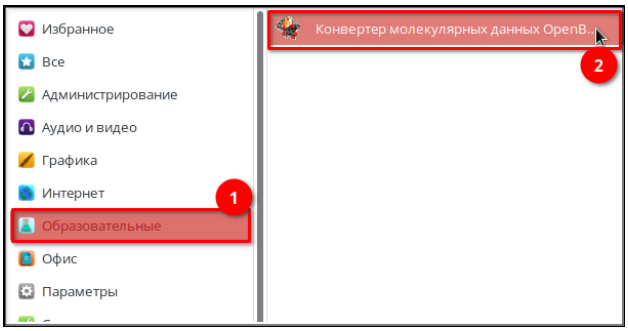
В поисковой строке менеджера пакетов введите ключевое слово «**openbabel**» (1), нажмите кнопку «**Поиск**» (2), выберите пакет «**openbabel-gui**» последней версии для платформы **x86_64**, отметьте флагом (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



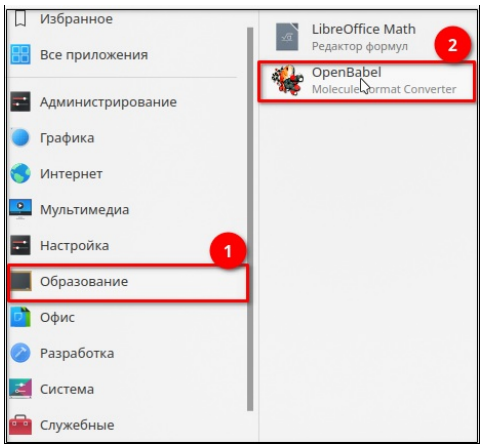
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install openbabel-gui
```

После установки программа будет доступна из «**Главного меню**» – «**Образовательные**» (1) – «**Конвертер молекулярных данных OpenBabel**» (2). (РЕД ОС 7.3)

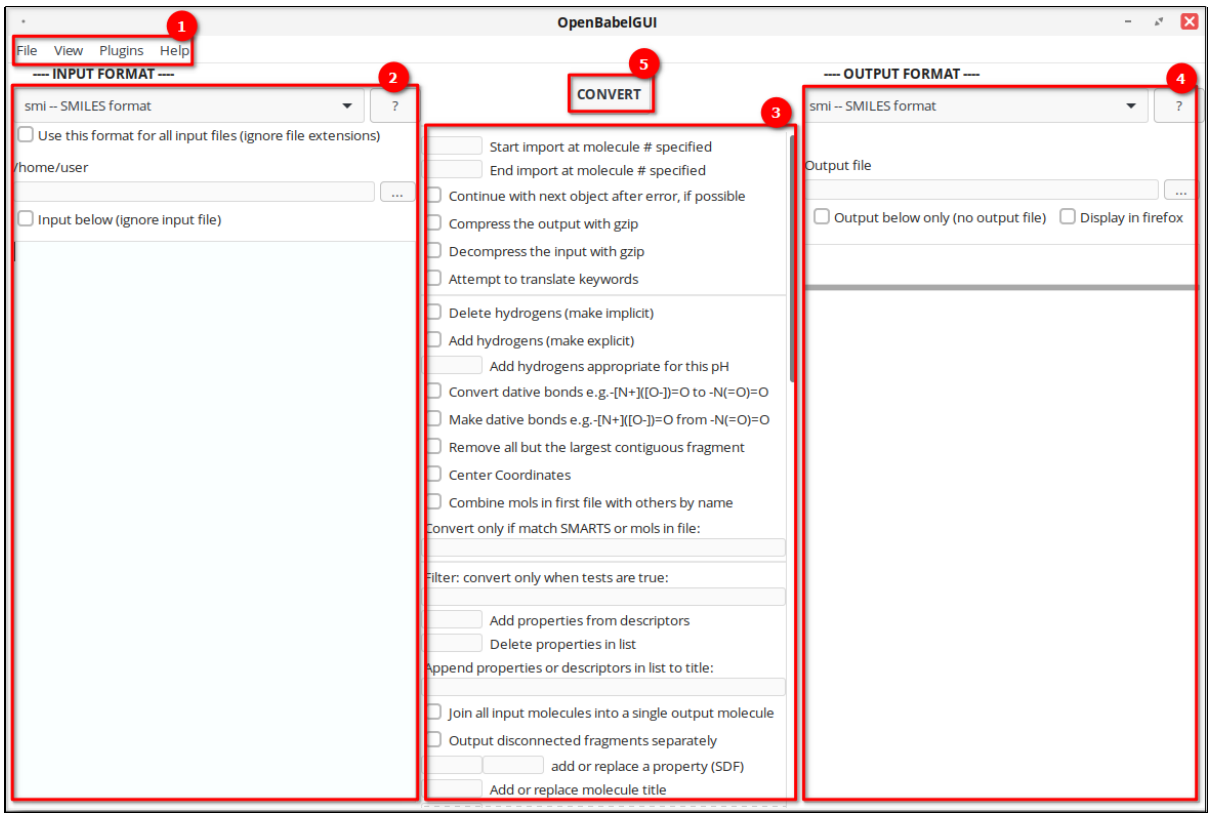


После установки программа будет доступна из «**Главного меню**» – «**Образование**» (1) – «**OpenBabel**» (2). (РЕД ОС 8)



Интерфейс программы и ее основные элементы

Программа **OpenBabel** имеет простой и понятный интерфейс. Главное окно программы содержит следующие элементы: главное меню (1), область формата входных данных (2), область выбора параметров (3), область формата выходных данных (4), кнопка конвертирования (5).



1. Главное меню включает:

- меню «**File**» («**Файл**») - здесь можно копировать, конвертировать, сохранить данные или конфигурацию экрана;
- меню «**View**» («**Вид**») - настраивает вид области для выбора параметров, можно отключить или подключить панели выбора параметров;
- меню «**Plugins**» («**Плагины**») - можно подключать дополнительные функции (например, различные методы определения частичных или парциальных зарядов, индексацию линейных фрагментов, канонически закрепить порядок атомов, генерирование двумерных и трехмерных координат);
- меню «**Help**» («**Помощь**») - позволяет просмотреть информацию о программе.

2. Область формата входных данных «**INPUT FORMAT**».

Выберите тип типа входного файла из раскрывающегося списка (например, **SD**, **SMILES**, **VMOL**, **XML**, **SDF**, **PNG**, **MPC**, **MRV**, **PDB** или другие форматы)

Нажмите кнопку ... и выберите файл, который необходимо конвертировать.

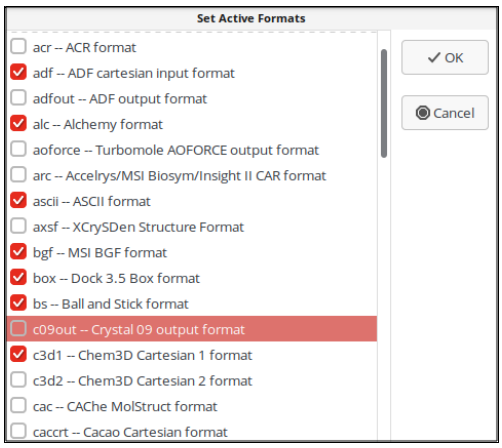
Вы можете выбрать несколько входных файлов в диалоговом окне.

Содержимое файла отобразится в текстовом поле ниже.

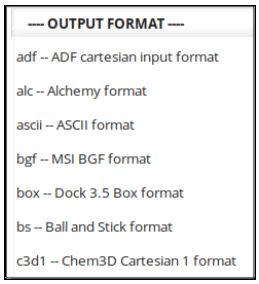
3. Область формата выходных данных «**OUTPUT FORMAT**».

Аналогичным образом выберите выходной формат и файл, в который необходимо преобразовать данные.

Если необходимо использовать только часть большого количества форматов, поддерживаемых **OpenBabel**, вы можете ограничить выбор, предлагаемый в раскрывающихся списках, что упрощает рутинный выбор. В раскрывающемся меню «**View**» нажмите кнопку «**Select set of formats**» («**Выбрать набор форматов**») для изменения отображаемых форматов. Отметьте флагами нужные форматы.



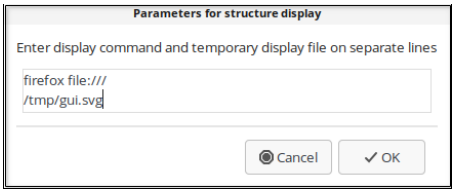
Впоследствии нажатие кнопки «**Use restricted set of formats**» («**Использовать ограниченный набор форматов**») в меню «**View**» включает и выключает эту функцию. Выбранные форматы отобразятся в областях входных и выходных данных.



Включив подстановочный знак * в имена входных и выходных файлов, вы можете выполнить пакетное преобразование (например, ***.smi**, ***.mol** и др.). Если имя выходного файла было **File_*.mol**, то выходные файлы будут иметь имя **File_first.mol** и т. д.

Вы можете отобразить выходные данные ниже в рабочей области, не выбирая при этом выходной файл. Для этого нужно установить флаг «**Output below only (no output file)**».

Преобразуемые химические структуры могут отображаться (в формате **SVG**) во внешней программе. По умолчанию используется **Firefox**, но его можно изменить в пункте меню « **View**» - «**Configure structure display**» (например, на **Opera** или **Chrome**).



Если установлен флаг «**Display in firefox**»» (под именем выходного файла), структуры будут отображаться на новой вкладке **Firefox**.

При наличии нескольких молекул изображение можно масштабировать (с помощью колеса мыши) и панорамировать (перетаскиванием нажатой левой кнопкой мыши). Довольно быстро обрабатывается до 100 молекул одновременно, при большем количестве молекул система конвертации работает медленнее.

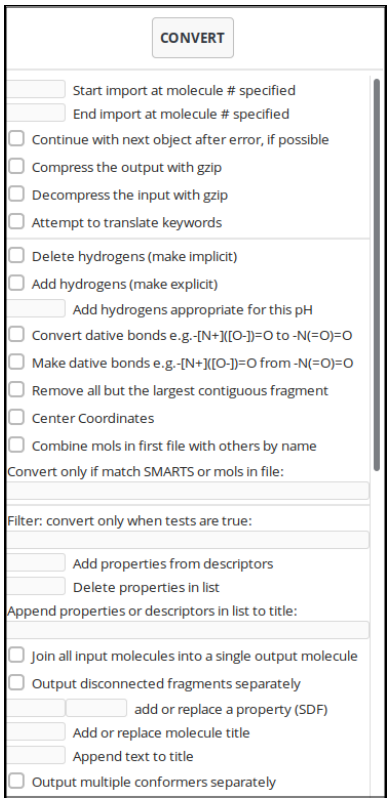
Генерация также может производиться медленнее при вычислении двумерных координат атомов. Новая вкладка браузера **Firefox** будет открываться каждый раз при нажатии кнопки «**CONVERT**» («**Преобразовать**»).

4. Область выбора параметров.

Опции параметров соответствуют типу преобразуемого химического объекта (молекула или реакция), а также форматам ввода и вывода. Вы можете отключить отображение любого из различных типов параметров с помощью меню «**View**».

Можно задать дополнительные параметры:

- сжать данные с помощью **zip**;
- распаковать данные;
- удалить или добавить водород;
- удалить самые крупные смежные фрагменты;
- отцентрировать координаты соединения;
- добавить или заменить название молекулы;
- добавить заголовок или текст;
- сгенерировать трехмерные или двухмерные координаты.



5. Кнопка «**CONVERT**» конвертирует данные выбранных форматов.

В окне сообщений под кнопкой будет указано количество преобразованных молекул, а также отобразится содержимое выходного файла.

По умолчанию все молекулы во входном файле преобразуются, если выходной формат допускает несколько молекул.

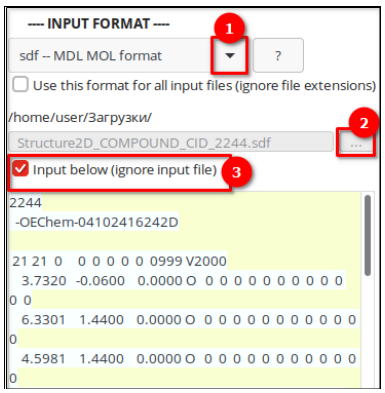
Конвертация химических форматов файлов

Наиболее распространенным применением **Open Babel** является преобразование химических форматов файлов. Ниже приведены примеры использования данной функции. Предварительно файлы для преобразования необходимо загрузить из банка данных химических веществ (например, **Pubchem**) или программ редактирования молекул (**Avogadro**, **GROMACS**, **XDrawChem** и др.).

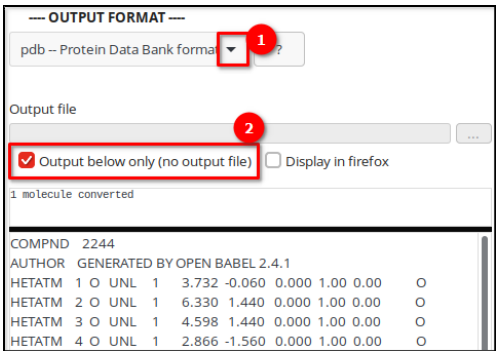
ПРИМЕР 1

Для конвертации файла формата **SDF** в формат **PDB** выполните следующие действия:

1. Установите формат входного файла **SDF** (1), загрузите файл (2), установите флаг «**Input below (ignore input file)**» (3) для считывания входных данных.



2. Установите формат выходного файла **PDB** (1) – формат банка данных трехмерных структур белков и нуклеиновых кислот. Установите флаг «**Output below only (no output file)**» (2) для вывода информации о преобразовании в поле ниже.



3. Установите дополнительные параметры при необходимости.

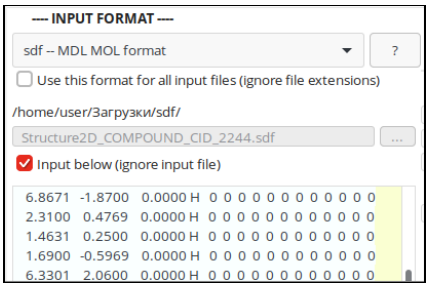
4. Выполните конвертирование, нажав «**CONVERT**».

ПРИМЕР 2

Рассмотрим пример конвертации файла формата **SDF** в **SMI** формат:

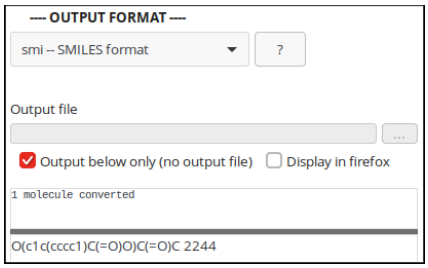
1. В области «**INPUT FORMAT**» выберите формат **SDF,** далее укажите путь к файлу.

2. Установите флаг «**Input below (ignore input file)**» для считывания входных данных.



3. В области «**OUTPUT FORMAT**» в качестве выходного формата выберите «**SMI — SMILES format**» и отметьте флагом параметр для вывода информации о преобразовании в поле ниже «**Output below only (no output file)**».

4. В информационном поле отобразится описание состава и структуры молекулы.



Разработка на языках программирования C++ и Python

Если у вас есть опыт программирования на **C++** или **Python**, вы можете использовать **OpenBabel** как основу для создания своих приложений или скриптов.

Интерфейс **Python** для **OpenBabel** предоставляет два модуля, которые можно использовать для доступа к функциональности набора инструментов:

1. Модуль **OpenBabel** - он содержит стандартные привязки **Python**, автоматически созданные из **API C++**.

2. Модуль **Pybel** - это оболочка классов и методов модуля **openbabel**. Pybel предоставляет более удобные способы доступа к набору инструментов **Open Babel**.

Для отображения 2D-форматов с помощью **Pybel** необходимо установить библиотеки **Pillow** (python3-pillow) и **Tkinter** (python3-tkinter). Обычно данные библиотеки установлены по умолчанию. В случае если они были отключены, их можно подключить через менеджер пакетов **dnfdragora** или через **терминал**.

Для установки библиотеки **Pillow** через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install python3-pillow
```

Для установки библиотеки **Tkinter** выполните команду:

```
sudo dnf install python3-tkinter
```

Модуль openbabel обеспечивает прямой доступ к библиотеке **C++ Open Babel** из **Python**. Такая привязка создается с помощью пакета **SWIG** и обеспечивает доступ практически ко всем интерфейсам **Open Babel** через **Python**, включая базовые классы **OBMol**, **OBAtom**, **OBBond** и **OBResidue**, а также платформу преобразования **OBConversion**.

Рекомендации по использованию программы

1. Большинство параметров интерфейса, таких как выбранный формат, размер и положение окна, сохраняются между сеансами.
2. Конвертацию можно проводить без файлов. Вместо использования входных и выходных файлов можно вставить содержимое химического формата файла в поле ввода и просмотреть результаты преобразования в поле вывода.
3. При работе с другими программами рекомендуется интегрировать OpenBabel для удобства использования и получения более точных результатов.
4. При работе с большими молекулярными сетями необходимо учитывать ограничения программы и использовать дополнительные инструменты для оптимизации работы.
5. Рекомендуется регулярно обновлять программу, чтобы получить доступ к новым функциям и улучшениям.

XDrawChem – программа для рисования и анализа химических структур и реакций

Установка XDrawChem
Описание программы
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** XDrawChem-1.10.2

XDrawChem — это графическое приложение для рисования и анализа химических веществ, схем реакций. Программа предоставляет возможность редактирования химических структур в 2D-формате, а также анализа и хранения химических данных молекулярного моделирования, биохимии, твердотельных материалов или смежных областей. **XDrawChem** позволяет создавать химические структуры с фиксированными длинами связей и углами, автоматически рисует кольцевые системы, выравнивает структуры в реакциях и генерирует структурные диаграммы.

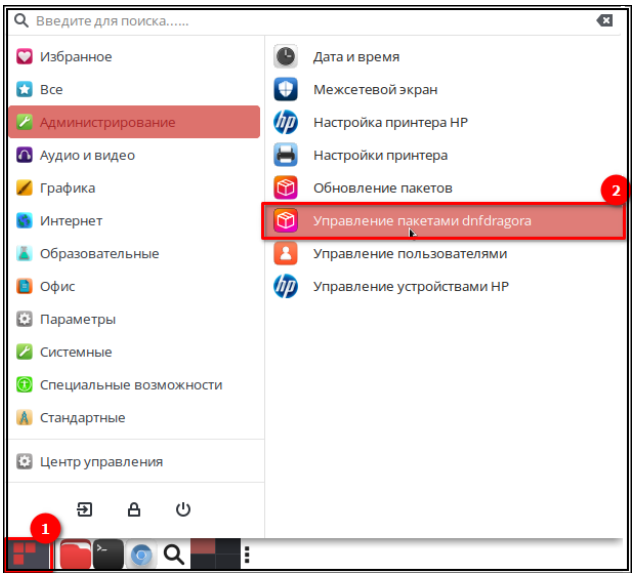
XDrawChem может работать с собственным файловым форматом, совместим с файлами **Chemdraw** и форматами, поддерживаемыми пакетом **OpenBabel** (***.cml**, ***.mdl**, ***.cif**, ***.mol**, ***.sd**, ***.sdf** и **др.**), а также позволяет экспортировать изображения в форматы: **PNG**, **BMP**, **EPS** и **SVG**.

XDrawChem предоставляет *прогнозы 13C-ЯМР* и *1H-ЯМР*, простое *ИК-прогнозирование*, простую *оценку pKa*, оценку *коэффициента распределения октанол-вода*, а также проводить *анализ реакций*, включая оценку изменения *энтальпии в газовой фазе* и сравнение *ЯМР 1H* и *ЯМР 13C*.

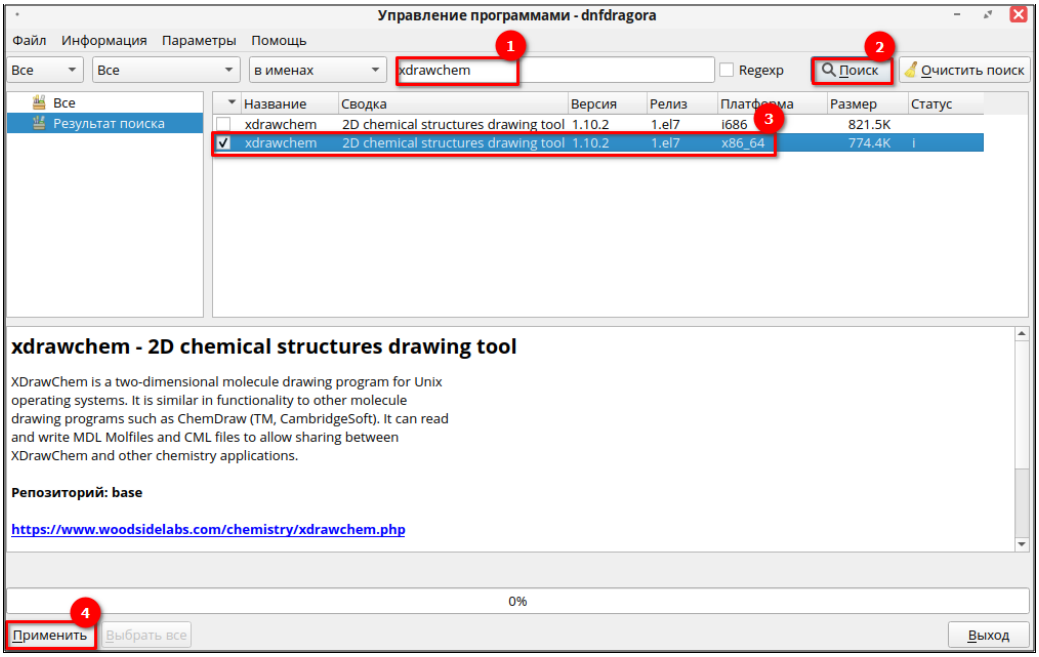
Установка XDrawChem

Программу можно установить через графический менеджер пакетов (**dnfdragora**) или с помощью команд в терминале.

Для установки программы через графический менеджер пакетов перейдите в «**Главное меню**» (1) — «**Администрирование**» — «**Управление пакетами dnfdragora**» (2).



В поисковой строке менеджера пакетов введите ключевое слово «**xdrawchem**» (1), нажмите кнопку «**Поиск**» (2) и отметьте флагом пакет последней версии для платформы **x86_64** (3). После этого нажмите кнопку «**Применить**» (4) и дождитесь окончания установки пакетов.



Для установки программы через **терминал** (**Ctrl+Alt+T**) перейдите в сеанс пользователя **root**:

```
su -
```

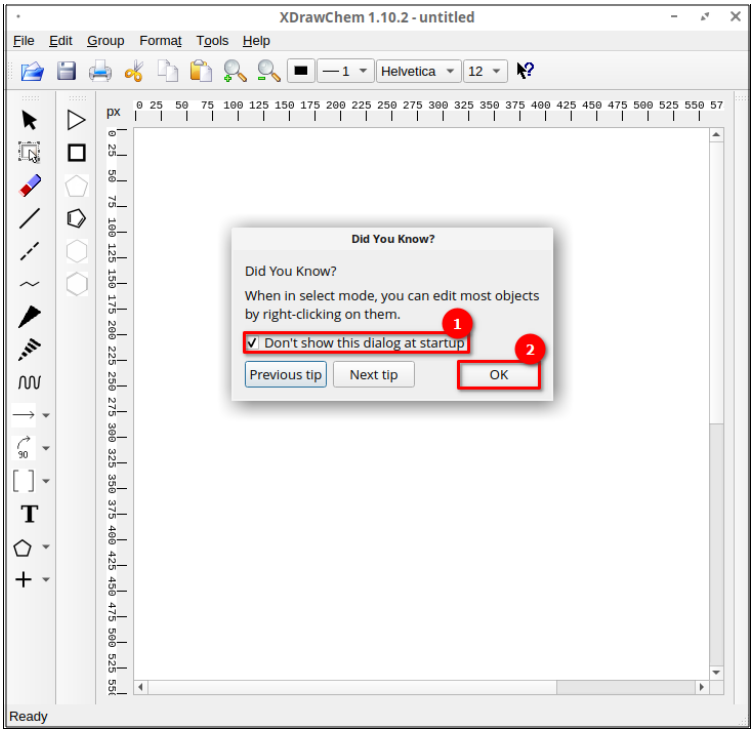
Далее выполните команду установки:

```
dnf install xdrawchem
```

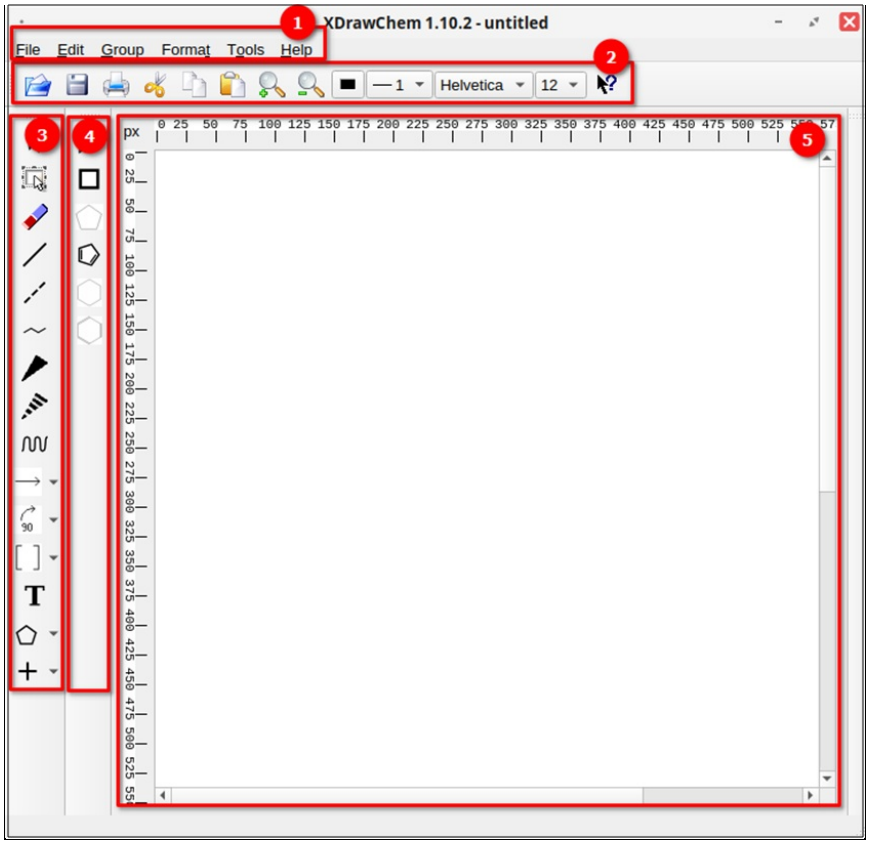
После установки программа будет доступна из «**Главного меню**» – «**Образовательные**» – «**Рисование хим. формул**».

Описание программы

При первом запуске появляется окно с различными подсказками по использованию программы. Для отключения данного окна при запуске программы поставьте флаг рядом с надписью «**Не показывать это диалоговое окно**» (1) и нажмите кнопку «**OK**» (2).



Окно программы выглядит следующим образом:



Интерфейс программы **XDrawChem** представлен в стандартном виде и состоит из следующих основных элементов:

1. Основное меню программы: содержит различные команды и опции, позволяющие управлять функциями программы, открывать и сохранять файлы, настраивать параметры и многое другое. Главные пункты меню включают:

- **Файл** (File): создание, открытие, поиск в интернете, сохранение, экспорт, настройка страницы, печать, закрытие, выход.
- **Редактирование** (Edit): отмена, вырезать, копировать, вставить, удалить, отменить выбор, повернуть, масштабировать.
- **Группа** (Group): выбор реактанта, выбор продукта реакции, очистка одной или всех групп.
- **Формат** (Format): установка цвета фона, настройки рисования, переключение сетки, отрисовка с фиксированными длинами отрезков и углами, настройки XDC.
- **Инструменты** (Tools): информация о молекуле, автоматическое распределение, *прогнозы 13C-* и *1H-ЯМР*, *простое ИК-прогнозирование*, простая оценка pKa, оценка коэффициента распределения октанол-вода, анализ реакций.
- **Помощь** (Help): дополнительная информация о программе.

2. Панель инструментов: стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы, таким как создать, сохранить, напечатать, вырезать, копировать, вставить и др.

3. Панель инструментов для рисования:

 Инструмент «Выбрать» (Select) предназначен для выбора и перемещения элементов внутри рамки. Можно выбрать несколько элементов, вырезать, копировать, перемещать и вращать их.

 Инструмент для создания лассо (Lasso) используется для выбора и перемещения элементов, рисуя петлю вокруг них. Доступны к выбору также несколько элементов.

 Инструмент «Стереть» (Erase) предназначен для удаления отдельных элементов.

 Линейный инструмент (Draw Line) используется для рисования связей. Обведите существующие связи, чтобы создать двойные и тройные связи.

 Инструмент «Пунктирная линия» (Draw dashed line) позволяет провести поверх существующих связей пунктирные линии.

 Инструмент «Цепи» (Draw aliphatic chain) дает возможность нарисовать ациклические (или алифатические) соединения.

 Инструмент для создания стереофонической восходящей линии (Draw stereo-up line) позволяет нарисовать дополнительные линии.

 Инструмент для создания стереофонической нисходящей линии (Draw stereo-down line) используется для отображения нисходящих линий.

Инструмент для создания волнистых линий (Draw wavy bond).

Инструмент «Стрелка» (Regular Arrow) позволяет рисовать простые стрелки. При нажатии и удержании можно выбирать из списка доступные стрелки.

Инструмент для рисования изогнутых стрелок используется для создания изогнутых стрелок и кубической кривой Безье.

«Квадратная скобка» (Square bracket) позволяет добавлять квадратные скобки к химическим структурам.

«Надпись» (Draw or edit text) предоставляет возможность создавать или редактировать текстовые блоки в редакторе химических структур.

Инструмент химических элементов (Chemical elements) предназначен для добавления или редактирования химических элементов.

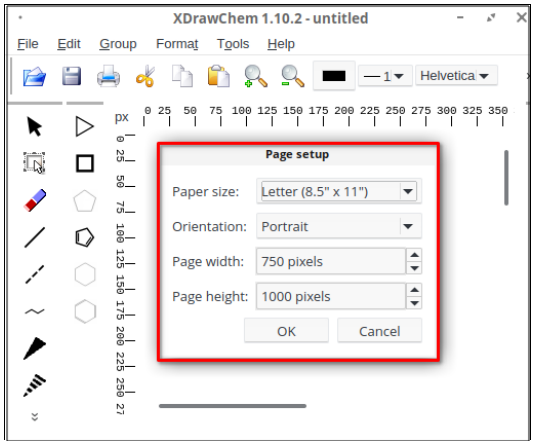
Инструмент для создания символов (Symbol tool) используется для добавления различных символов к химическим структурам.

4. Дополнительная панель инструментов: содержит инструменты для создания и редактирования химических структур.

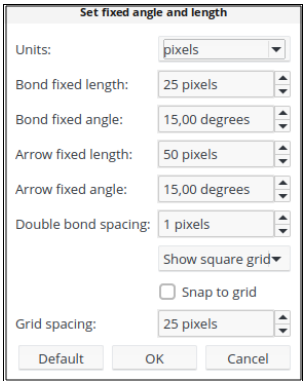
5. Рабочая область: здесь отображается сама химическая структура, которую вы создаете или редактируете, а также другие графические объекты.

XDrawChem обладает гибким пользовательским интерфейсом, который позволяет перемещать и отключать панели инструментов.

Для настройки страницы перейдите в «**File**» - «**Page setup**» и выберите необходимые опции.

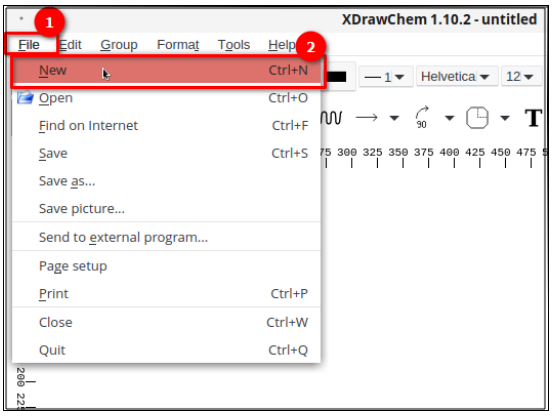


Для настройки рисования перейдите в «**Format**» - «**Drawing settings...**» и установите фиксированный угол и длину отрезка.



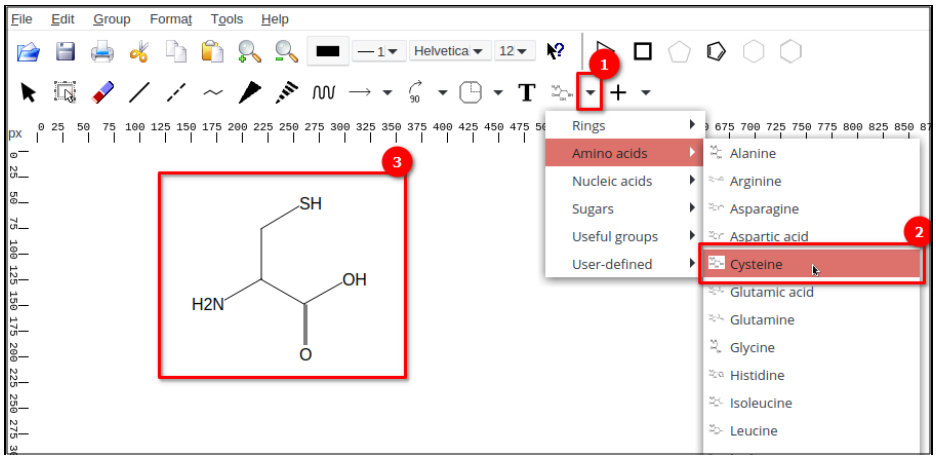
Пример работы

1. Для создания нового проекта необходимо перейти в основное меню программы в «**File**» (1) - «**New**» (2) или воспользоваться комбинацией клавиш «**Ctrl + N**».

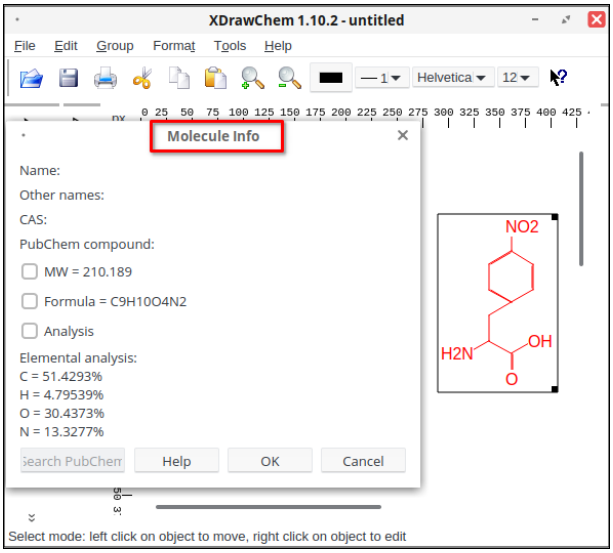


2. Взаимодействие с инструментами.

В **XDrawChem** доступны все стандартные аминокислоты и нуклеиновые кислоты во встроенной библиотеке. Например, для того чтобы разместить в рабочей области схему аминокислоты цистеина, необходимо открыть выпадающий список химических веществ (1), выбрать «**Amino acids**» - «**Cysteine**» (2), кликнуть ЛКМ в рабочей области (3). Изображение можно увеличить, повернуть и переместить.

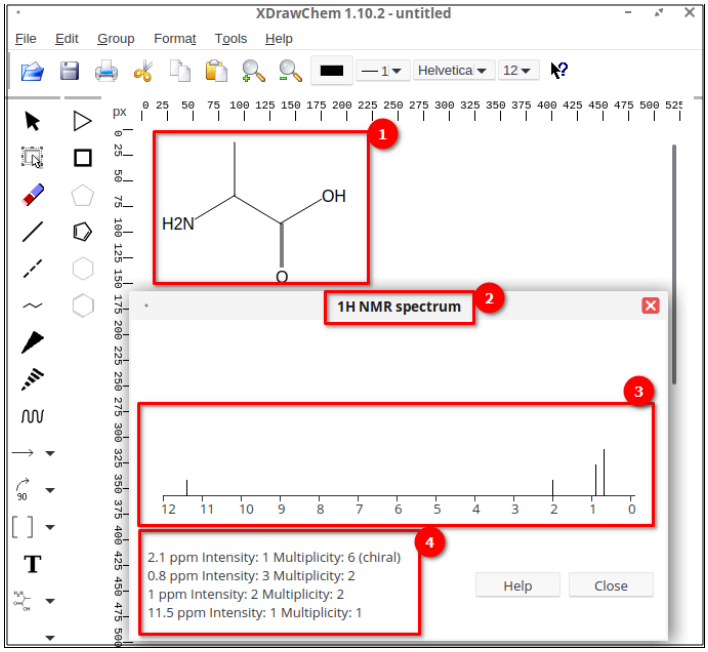


Для получения детальной информации о любом веществе в рабочей области необходимо его выделить, перейти в меню «**Tools**» - «**Molecule information...**» или воспользоваться сочетанием клавиш (**Ctrl + I**). Отобразится информация о средневесовой молекулярной массе (**MW**), формула вещества, элементарный анализ.

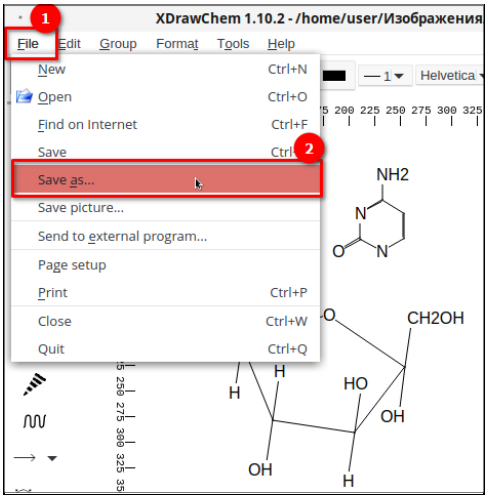


Для получения *1H ЯМР* анализа перейдите в главное меню в «**Tools**» - «**Predict 1H NMR**» и выделите соединение в рабочей области (1). Инструмент *1H NMR spectrum* (2) выведет спектр (3) и структуру соединения (4).

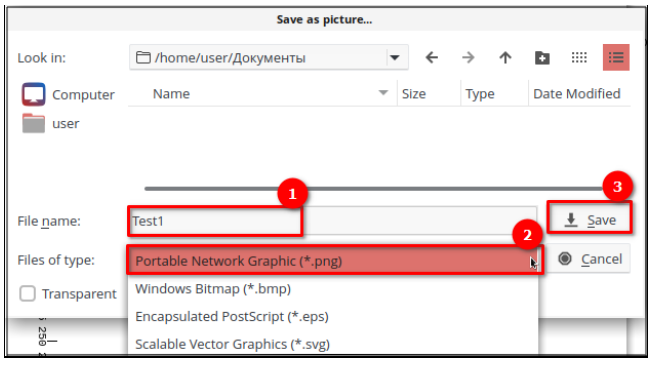
Например, спектр *1H ЯМР* аланина представляет собой 4 сигнала с химическими сдвигами 0.8, 1, 2.1 и 11.5 м. д.:



3. Для сохранения проекта необходимо перейти в пункт меню «**File**» (1) - «**Save as...**» (2). В диалоговом окне ввести имя, выбрать тип файла, директорию для сохранения.



Для сохранения изображения перейдите в пункт меню «**File**» - «**Save picture...**». Укажите имя файла (1), выберите один из доступных форматов: **PNG**, **BMP**, **EPS** и **SVG** (2), нажмите «**Save**» (3).



Kalzium - периодическая система химических элементов

Установка
Описание программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** kalzium-19.12.1-2

Kalzium — удобное графическое приложение для работы с *Периодической системой химических элементов*.

Периодическая система химических элементов имени Дмитрия Ивановича Менделеева (периодическая система, таблица Менделеева) — классификация химических элементов, устанавливающая зависимость различных свойств элементов от заряда атомного ядра. Система является графическим выражением периодического закона, открытого в 1869 году русским учёным энциклопедистом Дмитрием Ивановичем Менделеевым.

Kalzium прост в использовании, ориентирован на учащихся любого возраста в качестве маленькой и быстрой базы данных. Приложение можно использовать для изучения сведений о периодической системе.

Вы можете подробнее ознакомиться с возможностями работы программы **Kalzium**, просмотрев наши обучающие видео:

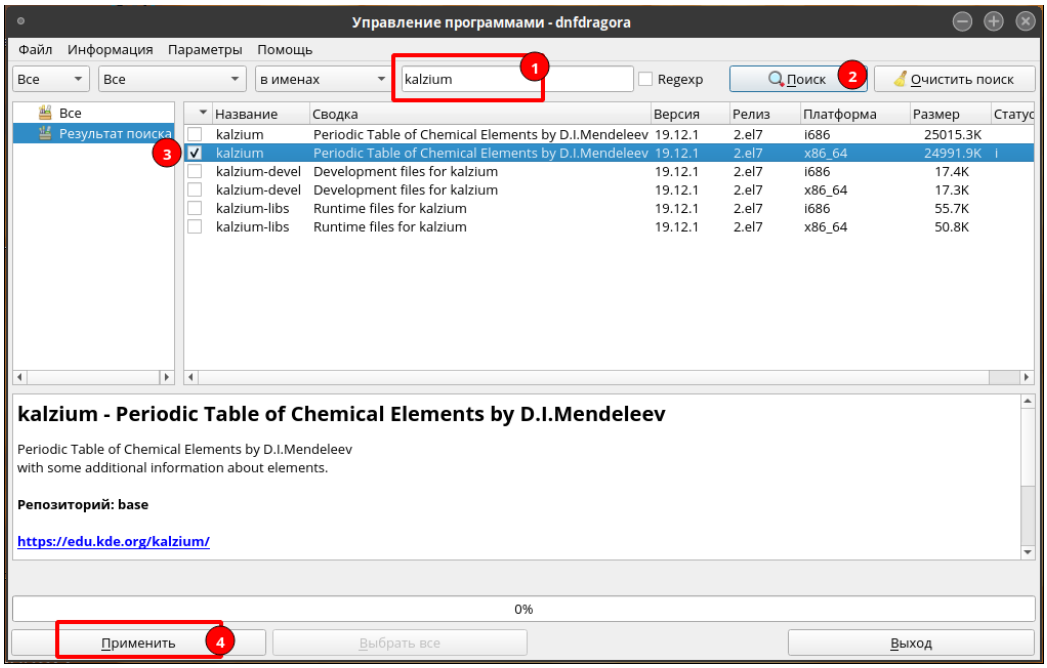
- на **RuTube** — Kalzium. Периодическая система химических элементов;
- в **Яндекс.Дзен** — Kalzium. Периодическая система химических элементов;
- в **VK Видео** — Kalzium. Периодическая система химических элементов.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kalzium**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install kalzium
```

Выйдите из сеанса пользователя **root**:

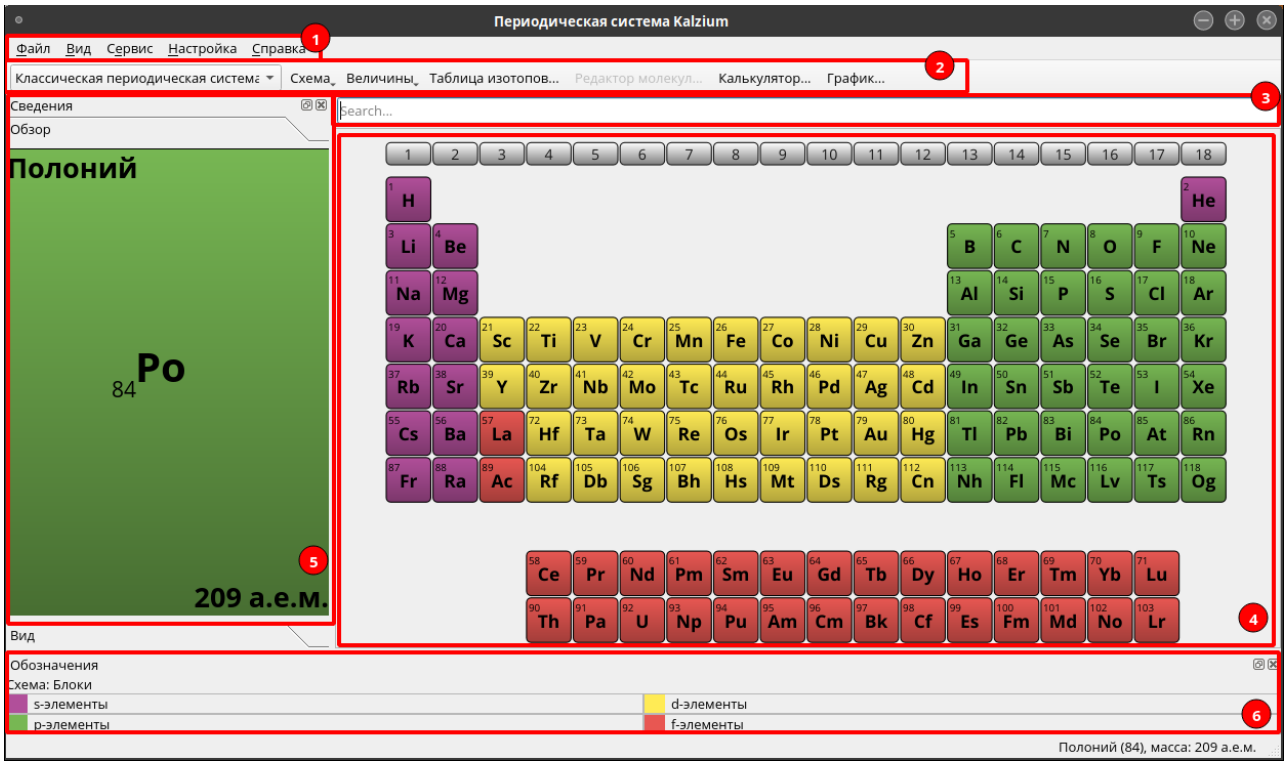
```
exit
```

Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**Периодическая система Kalzium**».

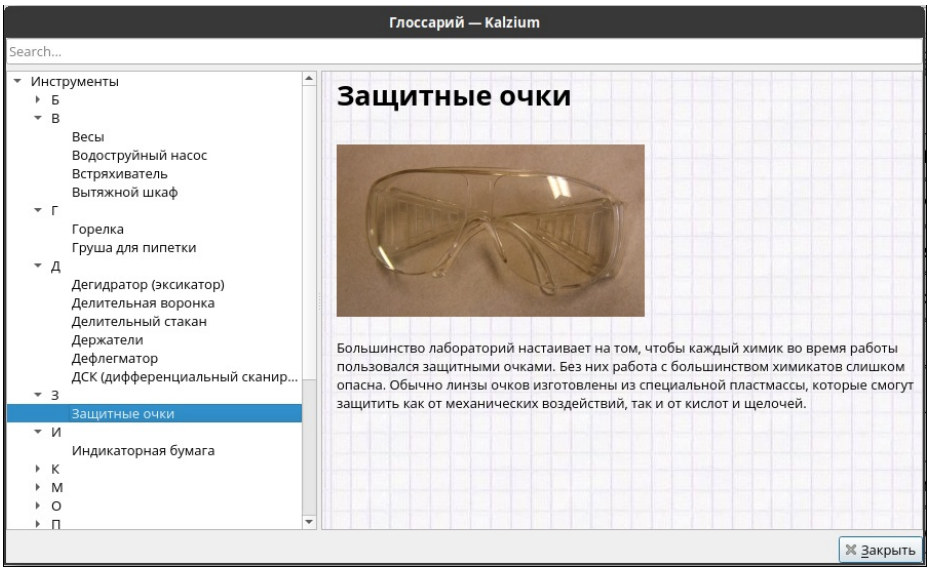
Описание программы

Интерфейс программы довольно прост и разделён на несколько типовых элементов.

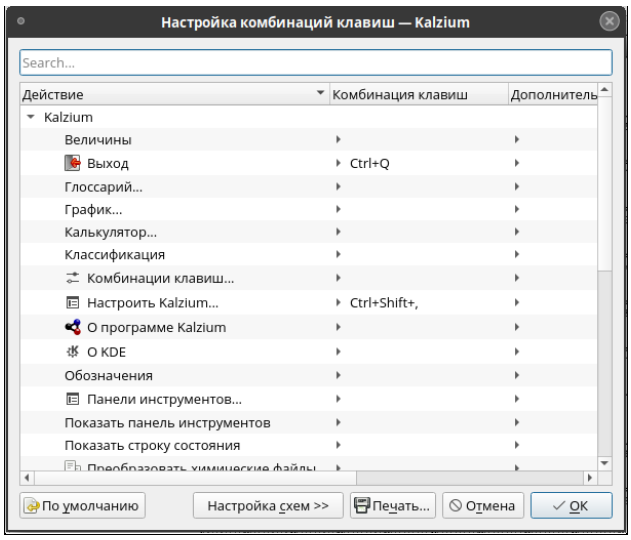


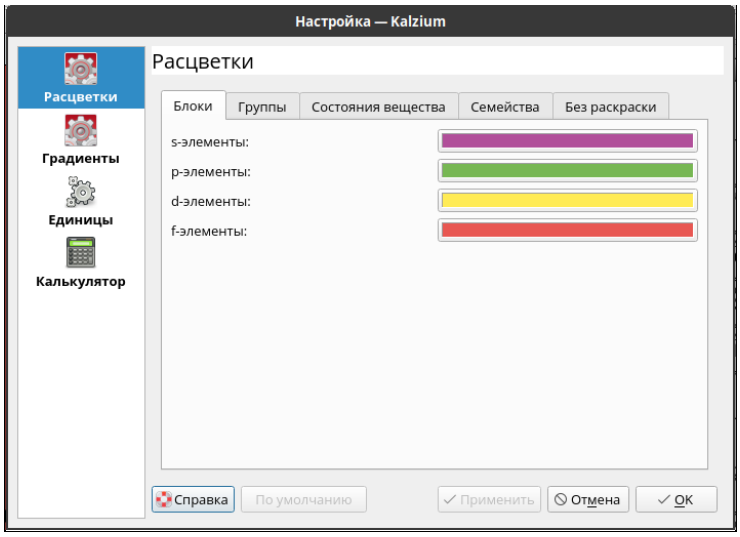
1. *Основное меню* – здесь доступны основные возможности программы.

Одним из наиболее интересных пунктов является «**Сервис**» - «**Глоссарий**», в котором собраны пояснения для большинства химических терминов, а также названия инструментов и краткое описание к ним.

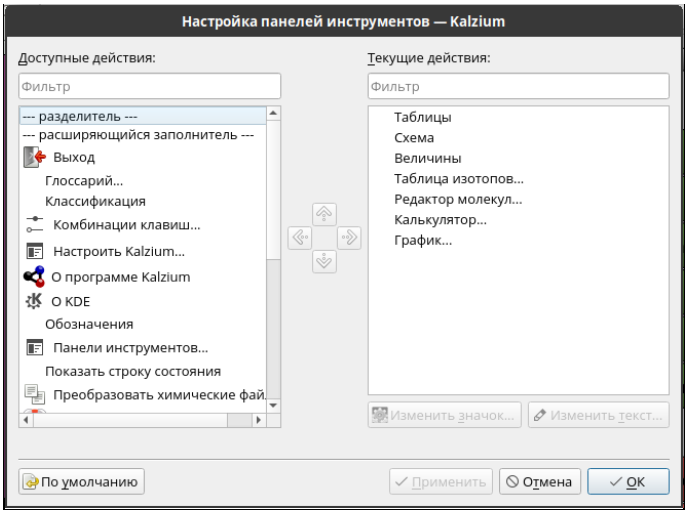


В пункте меню «**Настройка**» доступно изменение внешнего вида программы, языка интерфейса, а также просмотр и настройка используемых горячих клавиш.





2. *Панель инструментов* – нужна для быстрого доступа к основным возможностям программы. Кнопки этой панели можно настраивать через пункт меню «**Настройка**» — «**Панели инструментов**».

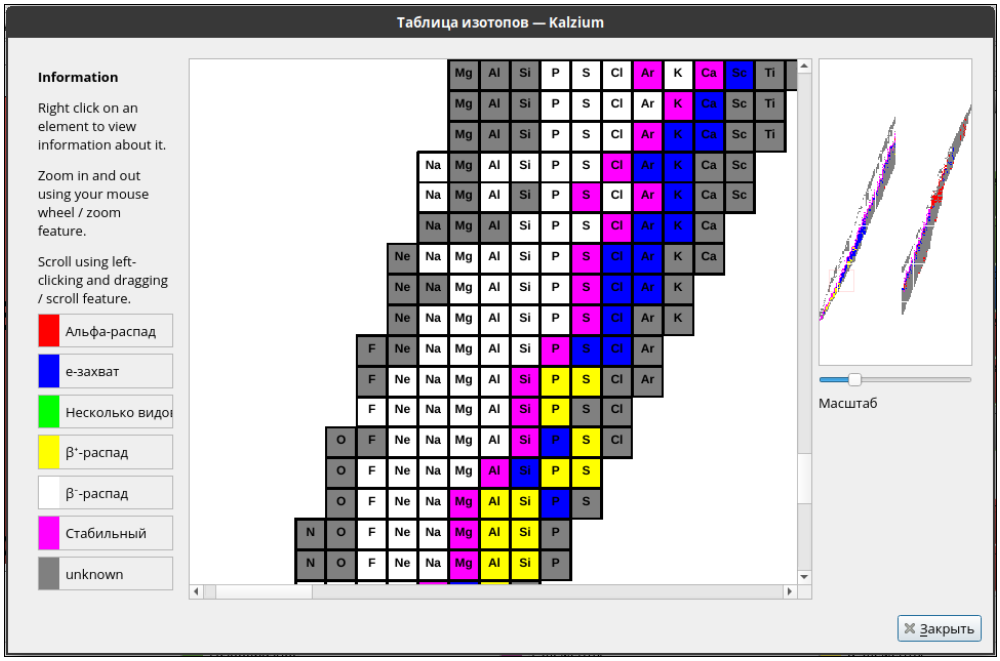


В панели инструментов также имеются некоторые дополнительные инструменты, такие как:

- *Таблица изотопов*;
- *Калькулятор*;
- *График*.

Таблица изотопов

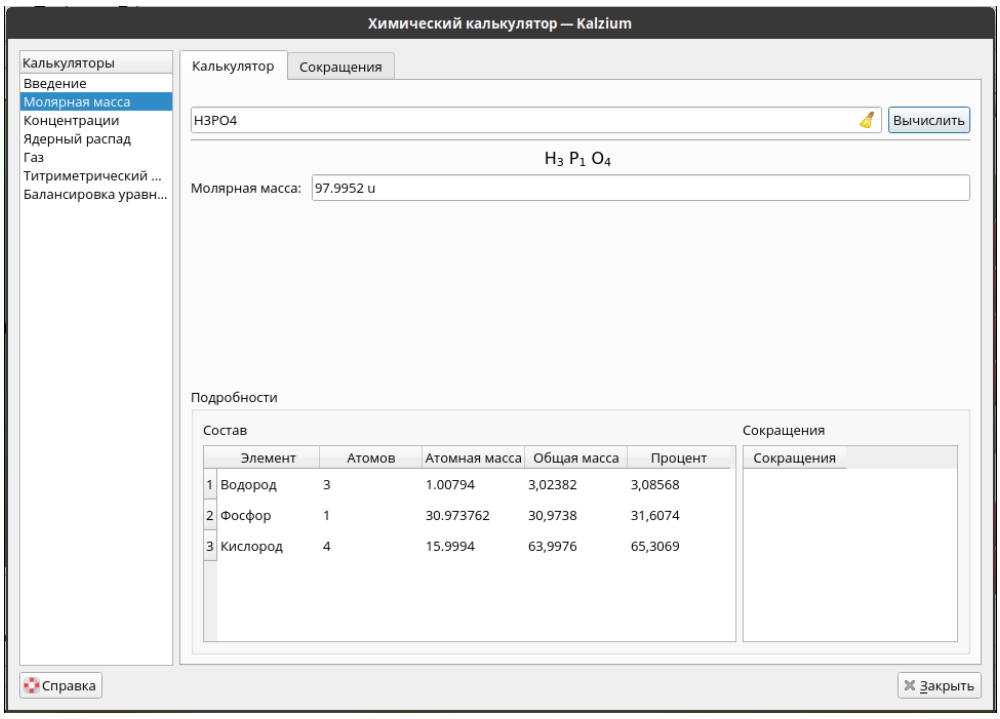
В таблице отображается информация об изотопах всех химических элементов.



Калькулятор

Химический калькулятор для расчёта значений различных свойств:

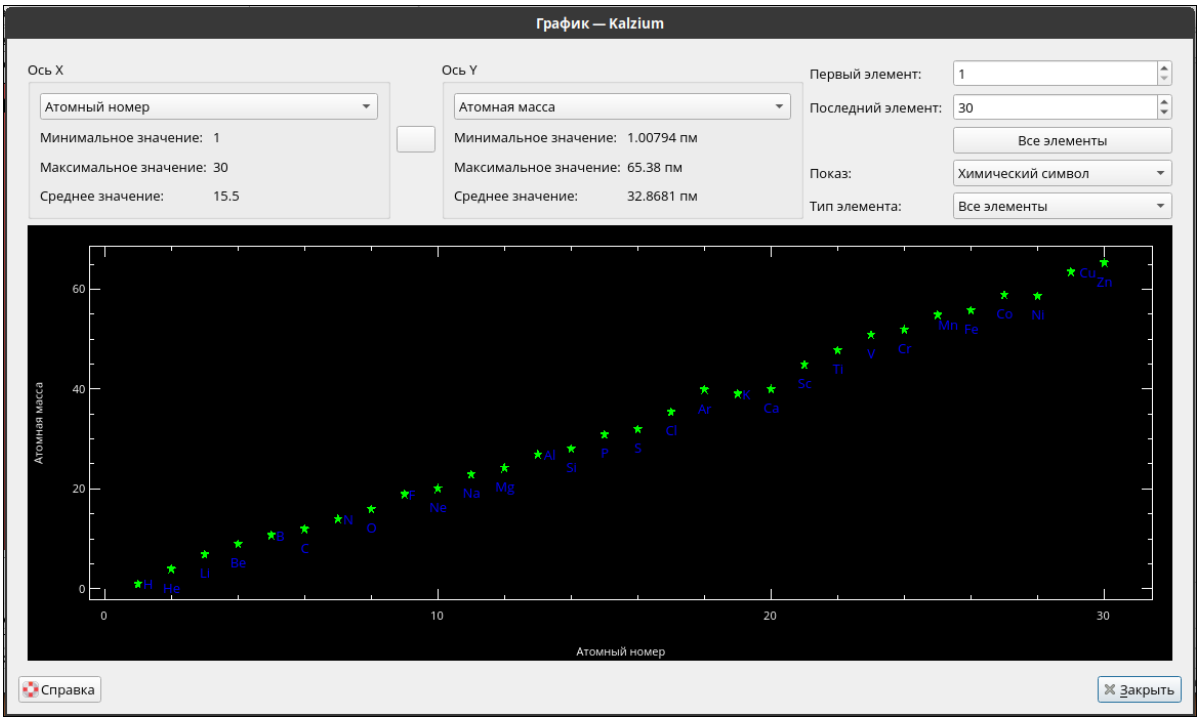
- молярной массы молекул;
- концентраций;
- титриметрического анализа;
- ядерных распадов;
- газов;
- балансировки химических уравнений.



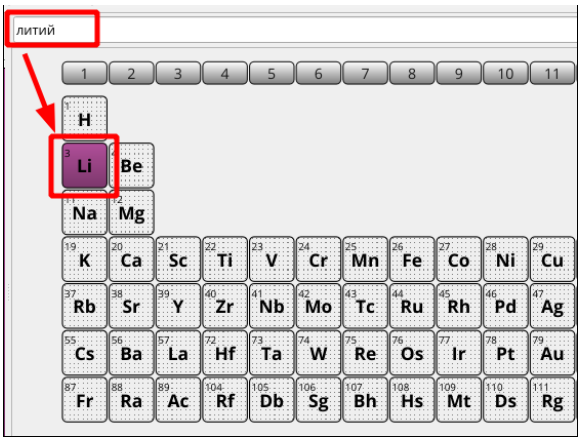
График

Kalzium позволяет построить график диапазона элементов по различным свойствам (температура кипения, атомная масса и др.). Такие

графики можно использовать, например, при наглядном отображении *закона Мозли*.



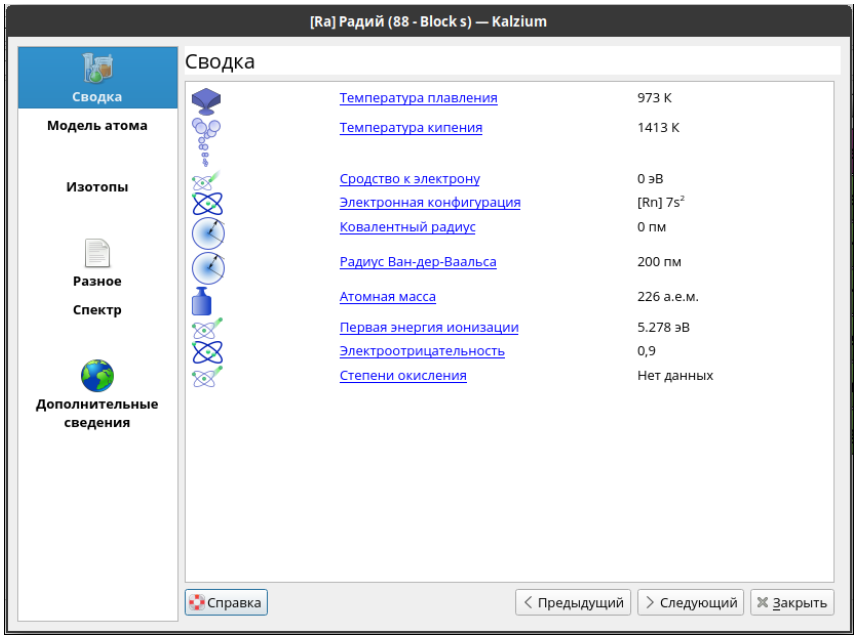
3. *Панель быстрого поиска элементов*. При поиске цветом выделяется только искомый элемент, остальные элементы становятся прозрачными.



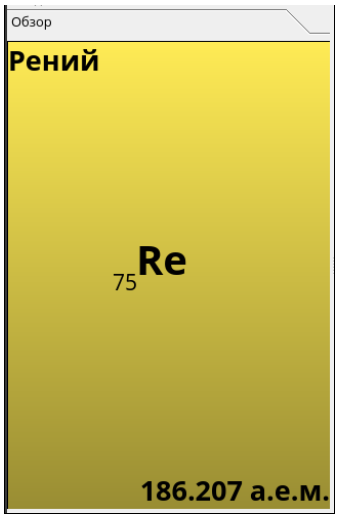
4. *Таблица элементов*. Внешний вид таблицы можно изменять через основное меню программы или через кнопки на панели инструментов (**2**).

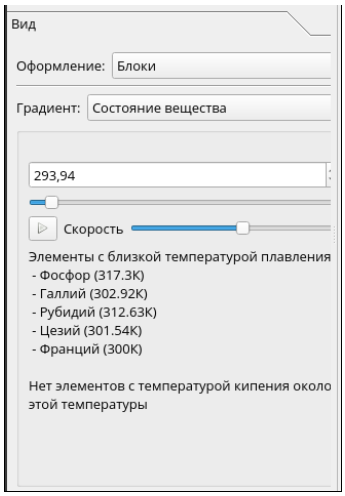
Kalzium может отображать периодическую таблицу различными способами (группами, блоками и семействами) и изменять её вид на короткую или длинную, можно также использовать различные схемы классификации, показывать элементы, сгруппированные по ряду свойств, например, кристаллической структуре и т.д.

В таблице отображаются краткое название химического элемента и его атомный номер. Для получения дополнительной информации о конкретном элементе нужно выбрать его в таблице. В открывшемся окне будет предоставлена расширенная информация о выбранном элементе: температура плавления, температура кипения, конфигурация электронных оболочек, электроотрицательность, ссылка на статью об элементе, краткая история открытия элемента, список его изотопов и модель атома.

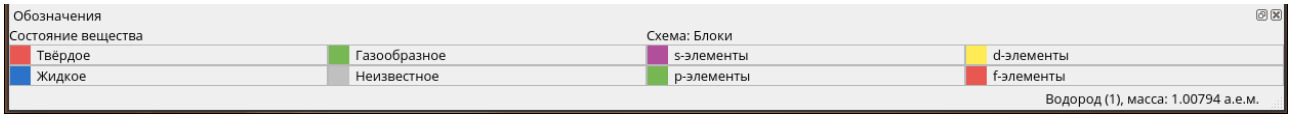


5. *Панель отображения дополнительной информации о выбранном элементе*. Тут можно показать либо обзор элемента, либо настройку общего вида таблицы.





6. *Панель легенды* с пояснениями цветовых обозначений элементов.



Kalzium может быть успешно использован как на уроках, так и при самостоятельном изучении химии.

InChI — химический идентификатор на основе молекулярной структуры

Установка
Синтаксис
Опции
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: inchi-1.0.6

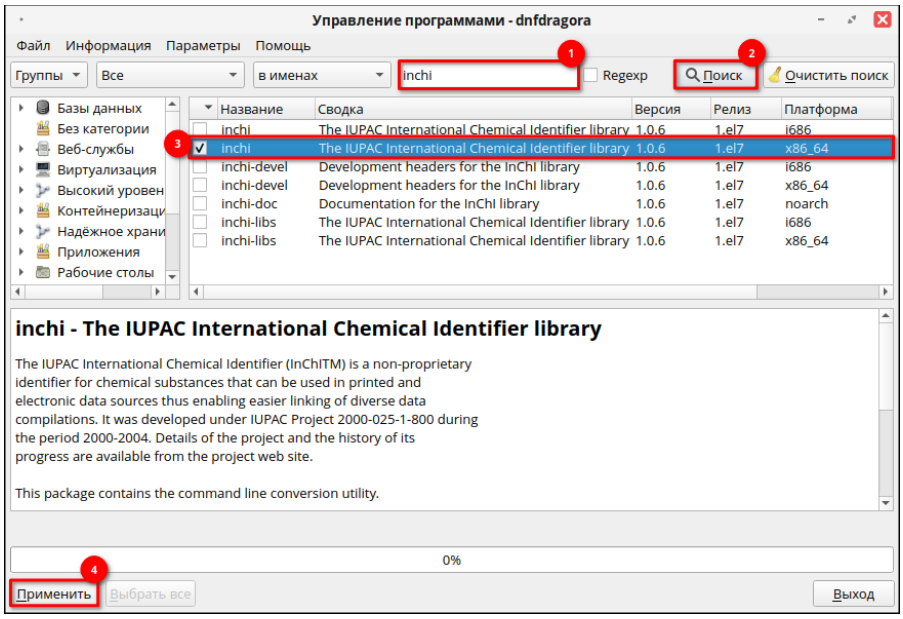
InChI — международный текстовый химический идентификатор. Предназначен для однозначного обозначения молекул. Он обеспечивает универсальный метод для облегчения поиска молекулярной информации в различных базах данных и в Интернете.

InChI и его компактная форма, **InChIKey**, являются открытыми стандартами, не ограниченными патентами. Эти идентификаторы преобразуют химические структуры в строки, которые могут быть использованы для описания, систематизации и поиска химических соединений.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**inchi**» и отметьте флагом пакет последней версии. Далее нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install inchi
```

Данный пакет предоставляет утилиту для командной строки **inchi-1**. Утилита применяется для пакетной обработки нескольких структурированных файлов, в первую очередь файлов SDF. Список опций утилиты можно вывести, запустив её без аргументов:

```
inchi-1
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
inchi-1 inputFile [outputFile [logFile [problemFile]]] [-option[ -option ...]]
```

где:

- **inchi-1** — название утилиты;
- **inputFile** — путь к входному файлу с химическими структурами, который нужно конвертировать;
- **outputFile** (необязательно) — путь к файлу, куда будет сохранён результат конвертации;
- **logFile** (необязательно) — путь к файлу логов, где будут записаны сообщения о ходе выполнения;
- **problemFile** (необязательно) — путь к файлу, куда будут записаны проблемные случаи;
- **[-option[-option ...]]** — одна или несколько опций, модифицирующих процесс конвертации.

```
inchi-1 inputFiles... -AMI [-option[ -option...]]
```

где:

- **inputFiles...** — список входных файлов для обработки;
- **-AMI** — опция, указывающая на использование дополнительного режима или модуля;
- **[-option[-option...]]** — дополнительные опции, настраивающие процесс.

Опции

Основные опции утилиты:

1. Опции ввода.

- **STDIO** — использовать стандартные потоки ввода/вывода;
- **InpAux** — ввод структур в формате дополнительной информации inchi;
- **SDF:DataHeader** — читать из входного SD-файла идентификатор под этим заголовком данных;
- **START:n** — начать с n-й входной структуры;
- **END:n** — остановиться после n-й входной структуры;
- **RECORD:n** — обработать только n-ю входную структуру;
- **AMI** — разрешить множественные входные файлы (поддержка шаблонов);
- **AMIOutStd** — записывать вывод в стандартный поток вывода (в режиме AMI);
- **AMILogStd** — записывать логи в стандартный поток ошибок (в режиме AMI);
- **AMIPrbNone** — подавить создание файлов с проблемами (в режиме AMI).

2. Опции вывода.

- **NoLabels** — не включать номер структуры, DataHeader и ID в вывод inchi;
- **NoWarnings** — подавить все предупреждающие сообщения;
- **AuxNone** — не включать дополнительную информацию;
- **SaveOpt** — сохранить пользовательские опции создания inchi (нестандартный inchi);
- **Tabbed** — разделить номер структуры, inchi и AuxInfo с помощью табуляции;
- **MergeHash** — объединить inchikey с дополнительными хешами, если они присутствуют;
- **NoInChI** — не печатать саму строку inchi;
- **OutErrInChI** — при ошибке печатать пустую строку inchi (по умолчанию ничего);
- **OutputSDF** — преобразовать inchi, созданный с дополнительной информацией по умолчанию, в SD-файл;
- **SdfAtomsDT** — выводить изотопы водорода в SD-файле как атомы D и T.

3. Опции структуры.

- **SNon** — исключить стереохимию (по умолчанию включить абсолютные стереохимические свойства);
- **NEWPSOFF** — оба конца клина указывают на стереоцентры;
- **LooseTSACheck** — ослабить критерии неоднозначного рисунка для тетраэдрической стереохимии в кольце;
- **DoNotAddH** — все атомы водорода являются явными (по умолчанию добавлять H в соответствии с обычными валентностями).

4. Модификаторы восприятия стереохимических свойств (нестандартный inchi).

- **SRel** — относительная стереохимия;
- **SRac** — рацемическая стереохимия;
- **SUCF** — использовать флаг хиральности: включено означает абсолютную стереохимию, выключено — относительную стереохимию.

5. Опции настройки создания inchi (нестандартный inchi).

- **SUU** — всегда включать опущенные неизвестные/неопределённые стереохимические свойства;
- **SLUUD** — делать метки для неизвестных и неопределённых стереохимических свойств различными;
- **RecMet** — включать результаты с реконнектированными металлами;
- **FixedH** — включать слой фиксированного водорода;
- **KET** — учитывать кето-енольный таутомеризм (экспериментально);
- **15T** — учитывать 1,5-таутомеризм (экспериментально).

6. Опции генерации.

- **Wnumber** — установить тайм-аут на структуру в секундах (W0 означает неограниченно);
- **WMnumber** — установить тайм-аут на структуру в миллисекундах (WM0 означает неограниченно);
- **LargeMolecules** — обрабатывать молекулы до 32766 атомов (экспериментально);
- **WarnOnEmptyStructure** — предупреждать и производить пустой inchi для пустой структуры;
- **Polymers** — разрешить обработку полимеров (экспериментально);
- **Polymers105** — разрешить обработку полимеров (экспериментально, устаревший режим версии 1.05);
- **FoldCRU** — складывать CRU-полимера, если внутри повторяются;
- **NoFrameShift** — отключить сдвиг рамки CRU-полимера;
- **NoEdits** — отключить сдвиг рамки и складывание CRU-полимера;
- **NPZz** — разрешить Zz-атомы, не связанные с полимерами (псевдоэлементы-заполнители);
- **SAtZz** — разрешить стереохимию у атомов, связанных с Zz (по умолчанию отключено);
- **Key** — генерировать inchikey;
- **XHash1** — генерировать расширение хеша (до 256 бит) для первого блока inchikey;
- **XHash2** — генерировать расширение хеша (до 256 бит) для второго блока inchikey.

7. Опции преобразования.

- **InChI2Struct** — преобразовать строку inchi обратно в структуру молекулы, восстановить исходную структуру молекулы из ее уникального идентификатора **inchi**;
- **InChI2InChI** — преобразовать строку inchi в другую строку inchi с использованием разных опций или стандартов, необходимо для сравнения и анализа различных представлений одной и той же молекулы.

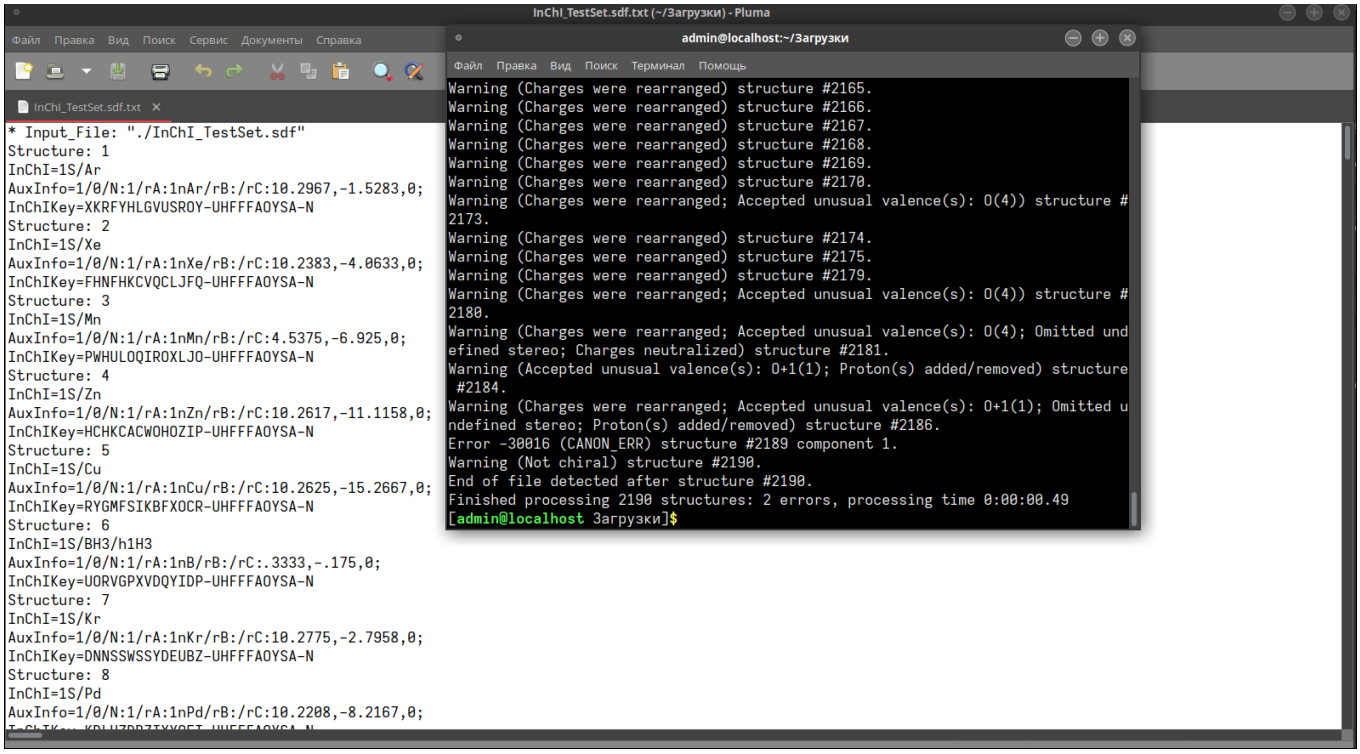
Примеры использования

Перед выполнением данных примеров создайте файл **InChI_TestSet.sdf**, содержащий необходимые химические структуры для преобразования.

> **Примечание.**
>
> Для создания и редактирования sdf-файлов можно использовать молекулярные редакторы, например:
>
> Avogadro - программа просмотра и редактирования молекул.
>
> XDrawChem – программа для рисования и анализа химических структур и реакций .

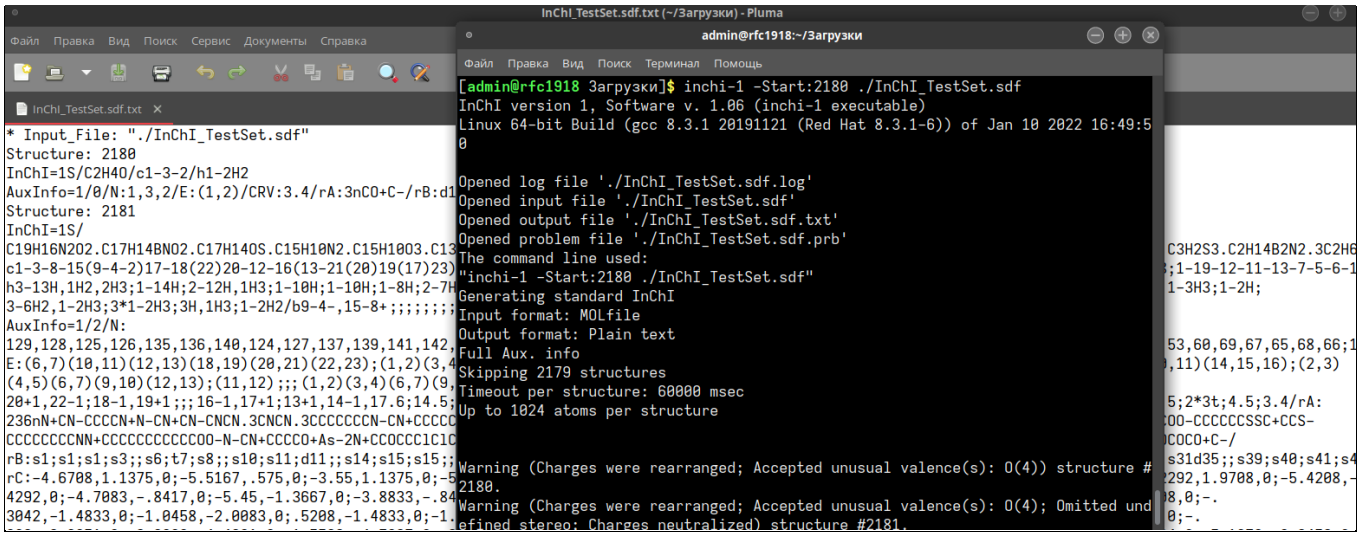
1. Преобразование sdf-файла в txt-файл со строками inchi и inchikey с использованием опции **-Key**:

```
inchi-1 -Key ./InChI_TestSet.sdf
```



2. Опции **-Start:n**, **-End:n**, **Record:n** позволяют обрабатывать структуры в файле, начиная с определённой структуры, либо заканчивая или обрабатывая только её.

```
inchi-1 -Start:2180 ./InChI_TestSet.sdf
```



OpenMolcas — программа для квантовой химии

Установка
Синтаксис
Опции
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: OpenMolcas-21.10

OpenMolcas — это утилита для квантовой химии, которая используется для моделирования и анализа молекулярных систем. Она предназначена для выполнения расчетов в различных областях теоретической и вычислительной химии, включая молекулярную структуру, термодинамику, спектроскопию и фотохимические процессы. Ее ключевой особенностью является мультиконфигурационный подход с использованием таких методов, как **CASSCF** (*Complete Active Space Self-Consistent Field* — метод полного самосогласованного поля активного пространства) и **CASPT2** (*Complete Active Space Perturbation Theory to second order* — полная теория возмущений активного пространства второго порядка).

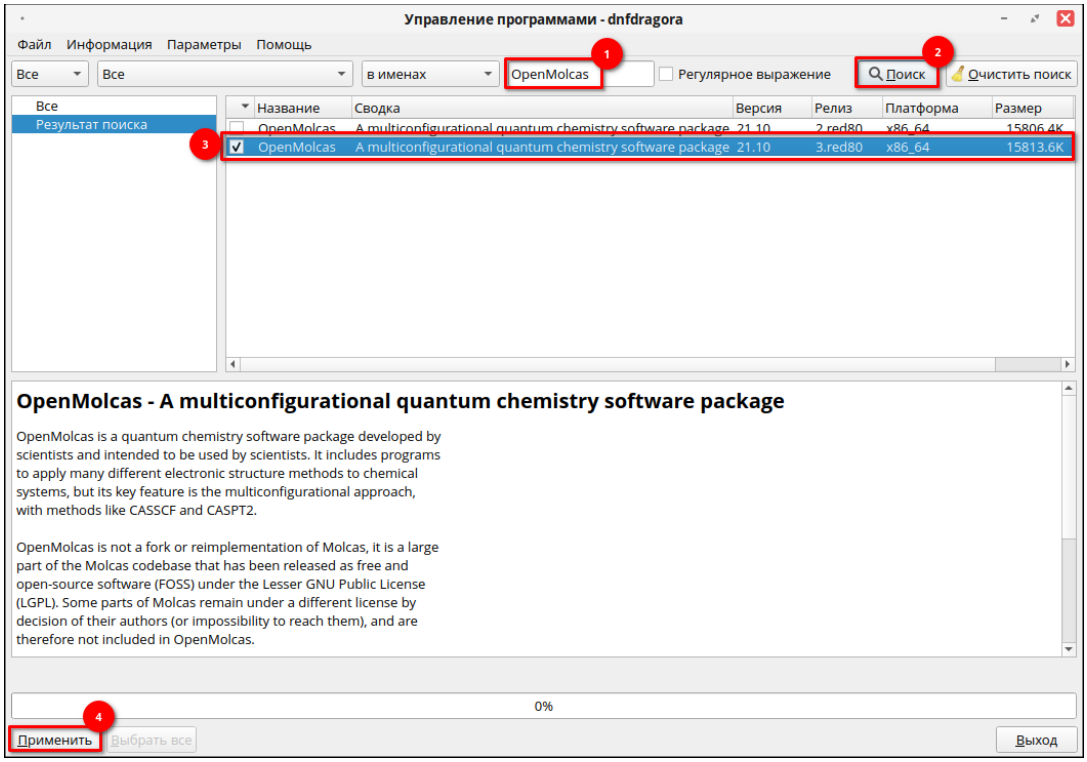
OpenMolcas предоставляет широкий спектр функций для проведения квантово-химических расчётов:

- **расчёт электронной структуры молекул** — позволяет рассчитывать электронную структуру молекул с использованием различных методов, таких как метод Хартри-Фока, метод функционала плотности и другие;
- **расчёт свойств молекул** — позволяет рассчитывать различные свойства молекул, такие как энергии, дипольные моменты, магнитные моменты и другие;
- **оптимизация геометрии молекул** — позволяет оптимизировать геометрию молекул с целью достижения минимума энергии;
- **изучение реакционной способности молекул** — позволяет изучать реакционную способность молекул с использованием методов теории возмущений.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**OpenMolcas**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install OpenMolcas
```

Синтаксис

Утилита доступна для запуска через терминал при помощи команды следующего вида:

```
pymolcas [<опции>] [<входной_файл> | <сценарий>]
```

Опции

Основные опции утилиты:

- **<входной_файл> | <сценарий>** — входной файл сценария или сценарий;
- **-h, --help** — показать справку;
- **-s, --setup** — настроить molcas;
- **-env, --environment** — отобразить информацию о расположении molcas;
- **-clean, --clean_scratch** — очистить рабочую область после расчета;
- **-new, --new_scratch** — очистить рабочую область перед расчетом;
- **-old, --old_scratch** — повторно использовать рабочую область;
- **-ign, --ignore_environment** — запустить, игнорируя файлы ресурсов;
- **-val, --validate** — проверить только ввод;
- **-np [<количество_процессов>], --nprocs [<количество_процессов>]** — указать количество параллельных (MPI) процессов;
- **-v, --version** — вывести версию;
- **-o [<файл>], --output [<файл>]** — перенаправить выходной поток в указанный файл;
- **-e [<файл>], --error [<файл>]** — перенаправить поток ошибок в указанный файл;
- **-oe [<файл>], -eo [<файл>], --outputerror [<файл>]** — перенаправить потоки вывода и ошибок в указанный файл;
- **-f, --files** — перенаправить потоки вывода/ошибок в стандартные файлы (***.log** и ***.err**);
- **-b [<размер_буффера>], --buffer [<размер_буффера>]** — указать размер буфера для файлов ввода/ошибок;
- **--banner** — вывод информативного баннера;
- **--not-here** — не пытаться найти molcas в текущем каталоге (и родительских).

Пример работы

Для примера будет выполнен полный расчёт поля реакции с использованием модели Кирквуда. **SCF** будет вычислять поле реакции, в то время как **MRCI** — добавлять эффект в виде постоянного возмущения.

Для этого будет создан файл **example.input** с настройками для вычисления квантовой химии:

```
nano example.input
```

```
&GATEWAY
 Title = HF molecule
 Symmetry
 X Y
 Basis set
 F.ANO-S...3S2P.
 F 0.00000 0.00000 1.73300
 End of basis
 Basis set
 H.ANO-S...2S.
 H 0.00000 0.00000 0.00000
 End of basis
 Well integrals
 4
 1.0 5.0 6.75
 1.0 3.5 7.75
 1.0 2.0 9.75
 1.0 1.4 11.75
```

```
RF-Input
Reaction field
80.0 4.75 4
End of RF-Input

&SEWARD

&SCF
Occupied = 3 1 1 0

&MOTRA
LumOrb
Frozen = 1 0 0 0
RFPert

&GUGA
Electrons = 8
Spin = 1
Inactive = 2 1 1 0
Active = 0 0 0 0
CiAll = 1

&MRCI
SDCI
```

где:

1. **&GATEWAY** — блок используется для задания различных параметров и опций, которые определяют расчет базисного набора, тип расчета и настройки реакционного поля. *Параметры:*

- **Title = HF molecule** — заголовок расчёта указывает на то, что рассматривается молекула фтороводорода (**HF**);
- **Basis set** — определение базисного набора для каждого типа атома в молекуле, для водорода используется набор **ANOS-S...2S**, а для фтора — **ANOS-S...3S2P**;
- **Well integrals** — настройки для вычисления интегралов, связанные с потенциальной энергией и волновыми функциями в пространственной области;
- **RF-Input** — используется для определения различных параметров реакционного поля (**RF**), которые могут быть использованы в расчетах.

2. **&SCF** — настройка для **SCF-метода** (**Self-Consistent Field**). *Настройка включает:*

- **Occupied = 3 1 1 0** — определение занятых орбиталей, где 3 означает три занятые орбитали в первом представлении, 1 — одну занятую орбиталь во втором и третьем представлениях, и 0 указывает на отсутствие занятых орбиталей в четвертом представлении.

3. **&MOTRA** — настройки для многоконфигурационных методов. *Параметры:*

- **LumOrb** — учет люминесцентных свойств молекулярных орбиталей;
- **Frozen = 1 0 0 0** — включение только первого порядка теории возмущений для коррекции энергии и волновых функций, отключая все более высокие порядки возмущения;
- **RFPert** — учет эффектов спин-орбитального взаимодействия и других релятивистских эффектов.

4. **&GUGA** — настройки для **GVB-метода**. *Параметры:*

- **Electrons = 8** — общее количество электронов;
- **Spin = 1** — общее количество спиновых орбиталей;
- **Inactive = 2 1 1 0** — определение неактивных орбиталей;
- **Active = 0 0 0 0** — определение активных орбиталей;
- **CiAll = 1** — включение полного конфигурационного смешения (**Full Configuration Interaction**).

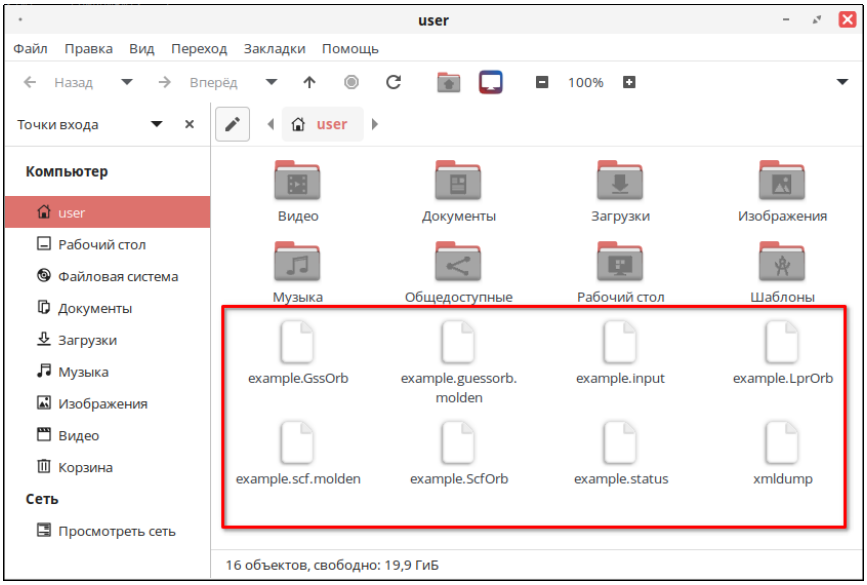
5. **&MRCI** — настройки для метода точного описания электронной структуры молекул с сильными корреляционными эффектами (**Multi-Reference Configuration Interaction**). *Настройка включает:*

- **SDCI** — расчёт с использованием **SDCI** (**Singles and Doubles Configuration Interaction**) метода в рамках блока настроек **&MRCI**.

Для запуска расчета используется команда:

```
pymolcas '/home/user/example.input'
```

Результаты работы можно посмотреть в каталоге **/home/user/**:



Более подробную информацию и расширенные возможности программы см. в официальном руководстве.

Работа со словарями

GoldenDict
StarDict
Translate-shell

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** stardict-3.0.6-1, goldendict-1.5-0.1, translate-shell-0.9.6.12-1

Словарями называют справочные издания, которые содержат упорядоченный перечень языковых единиц (слов, словосочетаний, фраз, терминов, знаков с краткими характеристиками или переводом на другой язык).

Вы можете подробнее ознакомиться с работой словарей и переводчиков в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Словари и переводчики в РЕД ОС;
- в **Яндекс.Дзен** — Словари и переводчики в РЕД ОС;
- в **VK Видео** — Словари и переводчики в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

GoldenDict

GoldenDict — оболочка для электронных словарей, поддерживающая форматы программ-словарей *ABBYY Lingvo*, *StarDict*, *Babylon*, *Dictd*.

Особенности:

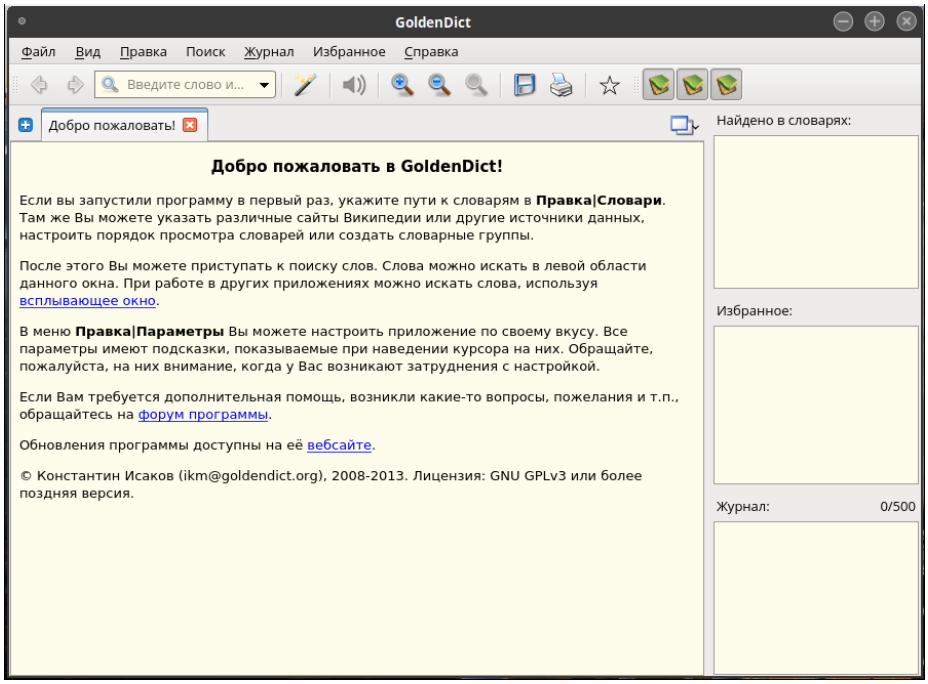
1. Вывод отформатированных статей со ссылками и картинками с помощью движка **WebKit**;
2. При поиске слов с ошибками используется система морфологии на основе свободной программы для проверки орфографии **Hunspell**;
3. Индексирование каталогов со звуковыми файлами для формирования словарей с произношением слов;
4. При поиске перевода пробелы, знаки пунктуации, диакритические знаки и регистр символов, содержащиеся в поисковой фразе, не учитываются;
5. После выделения текста появляется всплывающее окно, содержащее перевод выделенного текста;
6. Программа может показывать статьи с веб-сайтов, работающих на движке **MediaWiki** (таких как Википедия, Викисловарь и др.).

На сайте программы можно скачать русско-английский и англо-русский словари, а также словарь произношения английских слов.

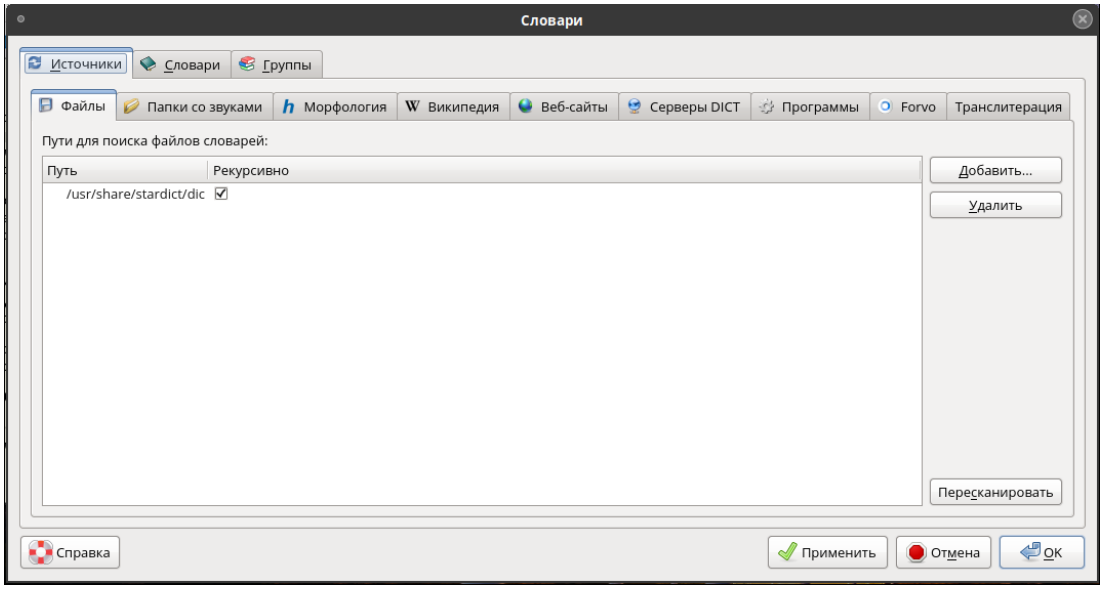
Режим всплывающего перевода

Вы можете получать перевод интересующего слова, не выходя из приложения, в котором работаете. Это осуществимо благодаря возможности программы работать в режиме *всплывающего перевода*. Чтобы посмотреть перевод интересующего слова, необходимо вызвать всплывающий перевод способом, установленным в настройках словаря. Другие способы вызова всплывающего перевода можно настроить в пункте меню «**Правка**» - «**Параметры**» - «**Всплывающее окно**».

GoldenDict по умолчанию установлен в РЕД ОС и находится в « **Главном меню**» - «**Офис**» - «**Мультиязычный словарь**».



Вы можете скачать любой словарь с официального сайта **GoldenDict**. Чтобы добавить новый словарь, распакуйте содержимое скачанного архива в **/usr/share/stardict/dic** либо укажите собственный каталог на вкладке «**Правка**» - «**Словари**» - «**Источники**». Нажмите «**Пересканировать**» и «**Применить**», все скачанные словари будут добавлены в **GodenDict**.



StarDict

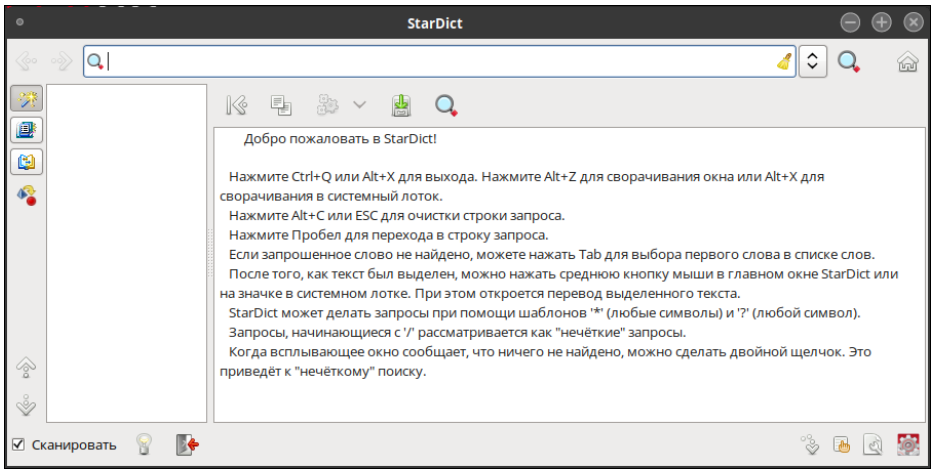
StarDict — свободная оболочка для электронных словарей с открытым исходным кодом, способная, кроме вывода статей, осуществлять перевод, озвучивать слова, использовать нечёткие запросы и шаблоны, поиск в онлайновых словарях.

Для установки **StarDict** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install stardict
```



После установки **StarDict** можно запустить из «**Главного меню**» - «**Офис**» - «**Словарь-переводчик StarDict**».

Translate-shell

Translate-shell - переводчик командной строки через **Google Translate** (по умолчанию), **Bing Translator**, **Яндекс.Переводчик** и **Apertium**. Данный инструмент позволяет получить доступ к одной из этих систем перевода прямо из терминала.

Для установки перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install translate-shell
```

Для перевода откройте терминал, напишите команду **trans** и необходимое для перевода слово. Данный инструмент может автоматически определять язык исходного текста. По умолчанию он переводит исходный текст на русский язык.

```
 trans dictionary

dictionary
/'dikSHə,nerē/ толковый словарь
(tolkovyy slovar')

dictionary – определения
[ English -> Русский ]

имя существительное
   словарь
      dictionary, vocabulary, glossary, lexicon, thesaurus, wordbook

dictionary
   толковый словарь, Словарь, словарик
```

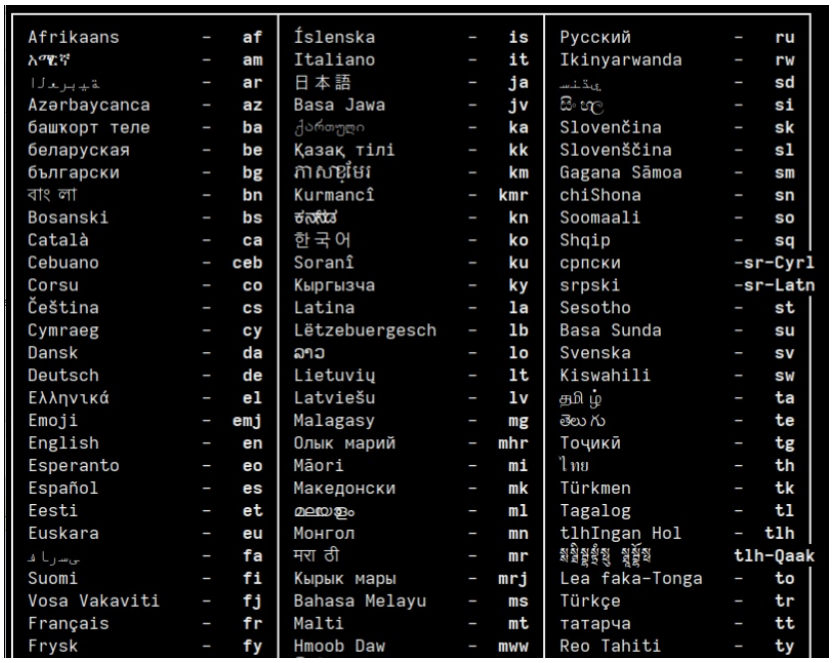
Чтобы перевести слово на другой язык надо явно указать идентификатор языка после команды **trans**, например:

```
 trans :de dictionary

dictionary
/'dikSHə,nerē/ Wörterbuch

dictionary – определения
[ English -> Deutsch ]

имя существительное
   (das) Wörterbuch
      dictionary, lexicon, thesaurus
   (das) Lexikon
      lexicon, encyclopedia, dictionary, encyclopaedia
   (der) Diktionär
      dictionary
```

```
dictionary
   Wörterbuch, Lexikon
```

Для просмотра доступных языков добавьте опцию **-T** после **trans**:

```
trans -T
```



Afrikaans	-	af	Íslenska	-	is	Русский	-	ru
አማርኛ	-	am	Italiano	-	it	Ikinyarwanda	-	rw
العربية	-	ar	日本語	-	ja	سنڌي	-	sd
Azərbaycanca	-	az	Basa Jawa	-	jv	සිංහල	-	si
башкорт теле	-	ba	ქართული	-	ka	Slovenčina	-	sk
беларуская	-	be	Қазақ тілі	-	kk	Slovenščina	-	sl
български	-	bg	ភាសាខ្មែរ	-	km	Gagana Sāmoa	-	sm
বাংলা	-	bn	Kurmancî	-	kmr	chiShona	-	sn
Bosanski	-	bs	ಕನ್ನಡ	-	kn	Soomaali	-	so
Català	-	ca	한국어	-	ko	Shqip	-	sq
Cebuano	-	ceb	Soranî	-	ku	српски	-	sr-Cyrl
Corsu	-	co	Кыргызча	-	ky	srpski	-	sr-Latn
Čeština	-	cs	Latina	-	la	Sesotho	-	st
Cymraeg	-	cy	Lëtzebuergesch	-	lb	Basa Sunda	-	su
Dansk	-	da	ລາວ	-	lo	Svenska	-	sv
Deutsch	-	de	Lietuvių	-	lt	Kiswahili	-	sw
Ελληνικά	-	el	Latviešu	-	lv	தமிழ்	-	ta
Emoji	-	emj	Malagasy	-	mg	తెలుగు	-	te
English	-	en	Олык марий	-	mhr	Тоҷикӣ	-	tg
Esperanto	-	eo	Māori	-	mi	ไทย	-	th
Español	-	es	Македонски	-	mk	Türkmen	-	tk
Eesti	-	et	മലയാളം	-	ml	Tagalog	-	tl
Euskara	-	eu	Монгол	-	mn	tlhIngan Hol	-	tlh
فارسی	-	fa	मराठी	-	mr	[illegible]		tlh-Qaak
Suomi	-	fi	Кырык мары	-	mrj	Lea faka-Tonga	-	to
Vosa Vakaviti	-	fj	Bahasa Melayu	-	ms	Türkçe	-	tr
Français	-	fr	Malti	-	mt	татарча	-	tt
Frysk	-	fy	Hmoob Daw	-	mww	Reo Tahiti	-	ty

Для перевода слов на несколько языков, все необходимые языки указываются через «**+**», например:

```
 trans :de+fr dictionary

dictionary
/ˈdikSHəˌnerē/Wörterbuchdictionary – определения
[ English -> Deutsch ]

имя существительное
   (das) Wörterbuch
      dictionary, lexicon, thesaurus
   (das) Lexikon
      lexicon, encyclopedia, dictionary, encyclopaedia
   (der) Diktionär
      dictionary

dictionary
   Wörterbuch, Lexikon

dictionary
/ˈdikSHəˌnerē/dictionnaire

dictionary – определения
[ English -> Français ]

имя существительное
   (le) dictionnaire
      dictionary, thesaurus

dictionary
   dictionnaire
```

Для того чтобы перевести фразу, её необходимо прописывать в кавычках:

```
trans “Who ate my sandwich?”
```

Также есть возможность перевода файла. Команда в таком случае будет выглядеть следующим образом:

```
trans file:///home/user/text.txt
```

Чтобы определить язык введённого слова, требуется указать ключ **-identify**:

```
trans -identify dictionary

English
Name                English
Family              Indo-European
Writing system      Latin
Code                en
ISO 639-3           eng
SIL                 https://iso639-3.sil.org/code/eng
Glottolog           https://glottolog.org/resource/languoid/id/stan1293
Wikipedia           https://en.wikipedia.org/wiki/ISO_639:eng
```

Перевод слова или фразы также можно прослушать, указав ключ **-p**:

```
trans -p "Welcome to RED OS, we wish You productive work!"

Welcome to RED OS, we wish You productive work!

Добро пожаловать в РЕД ОС, желаем Вам плодотворной работы!
(Dobro pozhalovatʹ v RED OS, zhelayem Vam plodotvornoy raboty!)

Welcome to RED OS, we wish You productive work!: варианты перевода
[ English -> Русский ]

Welcome to RED OS, we wish You productive work!
    Добро пожаловать в РЕД ОС, желаем Вам плодотворной работы!, Добро пожаловать в РЕД ОС, желаем Вам
продуктивной работы!
```

ПО для машинного перевода документов Promt Translation Server и PROMT Agent

Конфигурация веб-сервиса Nginx
Установка PROMT Agent

ВНИМАНИЕ!

Для установки утилиты необходимы дополнительные пакеты:

```
sudo dnf install coreutils tar gzip curl glibc libgcc libstdc++ libcurl libuuid zlib nginx mono-core mono-data fcgi
```

Promt Translation Server (PTS) — проприетарное программное обеспечение машинного перевода текста. Для использования **PTS** необходимо получить и активировать лицензию, отослав службе поддержки компании ПРОМТ идентификатор компьютера.

Для получения идентификатора, перейдите в каталог с **run-файлом** и выполните команду:

```
sh ptsu36.run +h
```

Создайте папки **ptsu_bin** и **ptsu_data** и распакуйте в них содержимое архивов:

```
sudo mkdir -p <путь_к_папке>/ptsu_bin
sudo mkdir -p <путь_к_папке>/ptsu_data
tar zxvf ptsu_bin.tar.gz -C <путь_к_папке>
tar zxvf ptsu_data.tar.gz -C <путь_к_папке>
```

После получения файла лицензии, его необходимо скопировать в корень папки с исполняемыми файлами:

```
cp <файл_лицензии> <путь_к_папке_ptsu_bin>
```

В файле настроек укажите путь до папки **ptsu_data** и до **FastCGI** сокета:

```
SocketPath=<путь_до_fcgisocket>
DataPath=<путь_до_папки_ptsu_data>
```

Конфигурация веб-сервиса Nginx

Перед конфигурацией **веб-сервиса** создайте две папки:

```
sudo mkdir /etc/nginx/sites-enabled /etc/nginx/sites-available
```

Следом создайте в папке **/etc/nginx/sites-available** конфигурационный файл виртуального хоста:

```
touch pts.conf
```

Заполните его следующем содержимом:

```
server {  listen 80;  server_name ptsu;  access_log /var/log/nginx/ptsu.access.log;  error_log /var/log/nginx/ptsu.error.log;  root /var/www/ptsu_bin/ui/;  rewrite ^/$ /pts redirect; client_max_body_size 1024m;  location /pts { root /var/www/ptsu_bin/ui/;  location /pts/service {  rewrite /pts/service/(.*) /pts/translator/$1 break;  proxy_pass http://127.0.0.1:9001;  proxy_connect_timeout 12000;  proxy_read_timeout 3600;  proxy_set_header Host $host;  }  location /pts/translator { fastcgi_pass unix:/home/test/fcgisocket;  fastcgi_connect_timeout 3600;  fastcgi_read_timeout 3600;  include fastcgi_params;  fastcgi_param HOST $host;  }}}
```

После чего создайте **символьную ссылку** на файл в каталог **/etc/nginx/sites-enabled**:

```
ln -s /etc/nginx/sites-available/pts.conf /etc/nginx/sites-enabled/pts.conf
```

Переместите каталог **ptsu_bin** в **/var/www/**

Сотрите все содержимое файла **/etc/nginx/nginx.conf** и вставьте туда следующее:

```
include /etc/nginx/modules-enabled.d/*.conf; include /etc/nginx/conf-enabled.d/*.conf; worker_processes 10; events { worker_connections 1024;  } http {  error_log /var/log/nginx/error.log warn;  access_log /var/log/nginx/access.log; include /etc/nginx/mime.types; include /etc/nginx/sites-enabled/*.conf; default_type application/octet-stream; sendfile on; gzip on; gzip_types text/plain text/css text/xml application/x-javascript application/atom+xml; }
```

Окончив конфигурацию веб-сервиса — запустите сервисы **PTS**, перейдя в папку **/var/www/ptsu_bin/bin64**:

```
./dcs -d
./transfcgid -d
./transfcgid -b -d
```

После запуска сервисов, веб-интерфейс будет доступен по адресу: http://localhost/pts

А сам веб-сервис: http://localhost/pts/service

Установка PROMT Agent

Для установки **PROMT Agent** распакуйте архив и запустите исполняемый файл командами:

```
tar -zxvf ptsu_agent.tar.gz
cd ptsu_agent
chmod +x PromtAgent.run
./PromtAgent.run
```

По умолчанию, **PROMT Agent** использует адрес подключения к серверу http://localhost/pts/service. Его можно изменить в настройках программы.

QGIS — геоинформационная система

Просмотр данных
Исследование данных и создание карт
Управление данными
Анализ данных
Публикация карт в сети Интернет
Внешние модули
Установка

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** qgis-3.34.7-1

Quantum GIS (**QGIS**)— свободная кроссплатформенная геоинформационная система, состоящая из настольной и серверной части:

- **QGIS Desktop** — настольная ГИС для создания, редактирования, визуализации, анализа и публикации геопространственной информации. Под «*QGIS*» часто имеют в виду именно *QGIS Desktop*.
- **QGIS Server** и **QGIS Web Client** — серверные приложения для публикации в сети проектов, созданных в *QGIS Desktop*, через сервисы, совместимые с OGC-стандартами (например, *WMS* и *WFS*).

QGIS позволяет использовать большое количество распространенных ГИС функций, обеспечиваемых встроенными инструментами и модулями. Основные возможности рассмотрим ниже.

Просмотр данных

Можно просматривать и накладывать друг на друга векторные и растровые данные в различных форматах и проекциях без преобразования во внутренний или общий формат.

Поддерживаются следующие основные форматы:

- пространственные таблицы и представления *PostGIS, SpatiaLite* и *MSSQL Spatial*, векторные форматы, поддерживаемые установленной библиотекой *OGR*, включая *shape*-файлы *ESRI, MapInfo, SDTS (Spatial Data Transfer Standard), GML (Geography Markup Language)* и многие другие;
- форматы растров и графики, поддерживаемые библиотекой *GDAL* (Geospatial Data Abstraction Library), такие, как *GeoTIFF, Erdas IMG, ArcInfo ASCII Grid, JPEG, PNG* и многие другие;
- растровый и векторный форматы GRASS (область/набор данных);
- пространственные данные, публикуемые в сети Интернет с помощью *OGC*-совместимых (Open Geospatial Consortium) сервисов *Web Map Service* (WMS) или *Web Feature Service* (WFS);
- данные *OpenStreetMap* (OSM).

Исследование данных и создание карт

С помощью удобного графического интерфейса можно создавать карты и исследовать пространственные данные. Графический интерфейс включает в себя множество полезных инструментов, например:

- браузер QGIS;
- перепроецирование «на лету»;
- компоновщик карт;
- панель обзора;
- пространственные закладки;
- определение/выборка объектов;
- редактирование/просмотр/поиск атрибутов;
- подписывание объектов;
- изменение символики векторных и растровых слоев;
- добавление слоя координатной сетки — средствами расширения *fTools* и в виде элемента оформления;
- добавление к макету карты стрелки севера, линейки масштаба и знака авторского права;
- сохранение и загрузка проектов.

Управление данными: создание, редактирование и экспорт

В QGIS можно создавать и редактировать векторные данные, а также экспортировать их в разные форматы. Чтобы иметь возможность редактировать и экпортировать в другие форматы растровые данные, необходимо сначала импортировать их в GRASS.

QGIS предоставляет следующие возможности работы с данными, в частности:

- инструменты оцифровки для форматов, поддерживаемых библиотекой OGR, и векторных слоев GRASS;
- создание и редактирование shape-файлов и векторных слоев GRASS;
- геокодирование изображений с помощью модуля пространственной привязки;
- инструменты GPS для импорта и экспорта данных в формате **GPX**, преобразования прочих форматов GPS в формат **GPX** или скачивание/загрузка непосредственно в прибор GPS;
- визуализация и редактирование данных *OpenStreetMap*;
- создание слоёв PostGIS из shape-файлов с помощью плагина **SPIT**;
- обработка слоёв PostGIS;
- управление атрибутами векторных данных с помощью новой таблицы атрибутов или модуля *Table Manager*;
- сохранение снимков экрана как изображений с пространственной привязкой.

Анализ данных

Вы можете анализировать векторные пространственные данные в PostgreSQL / PostGIS и других форматах, поддерживаемых OGR, используя модуль *fTools*, написанный на языке программирования Python.

В настоящее время QGIS предоставляет возможность использовать инструменты анализа, выборки, геопроцессинга, управления геометрией и базами данных. Также можно использовать интегрированные инструменты GRASS, которые включают в себя функциональность более чем 400 модулей GRASS.

Публикация карт в сети Интернет

QGIS может использоваться для экспорта данных в **map**-файл и публикации его в сети Интернет, используя установленный веб-сервер **Mapserver**.

Кроме того, QGIS может использоваться как клиент WMS, WMS-C, WFS и WFS-T и как сервер WMS или WFS.

Внешние модули

QGIS может быть адаптирована к особым потребностям благодаря расширяемой модульной архитектуре.

QGIS предоставляет библиотеки, которые могут использоваться для создания модулей. Можно создавать отдельные приложения, используя языки программирования *C++* или *Python*.

Основные модули:

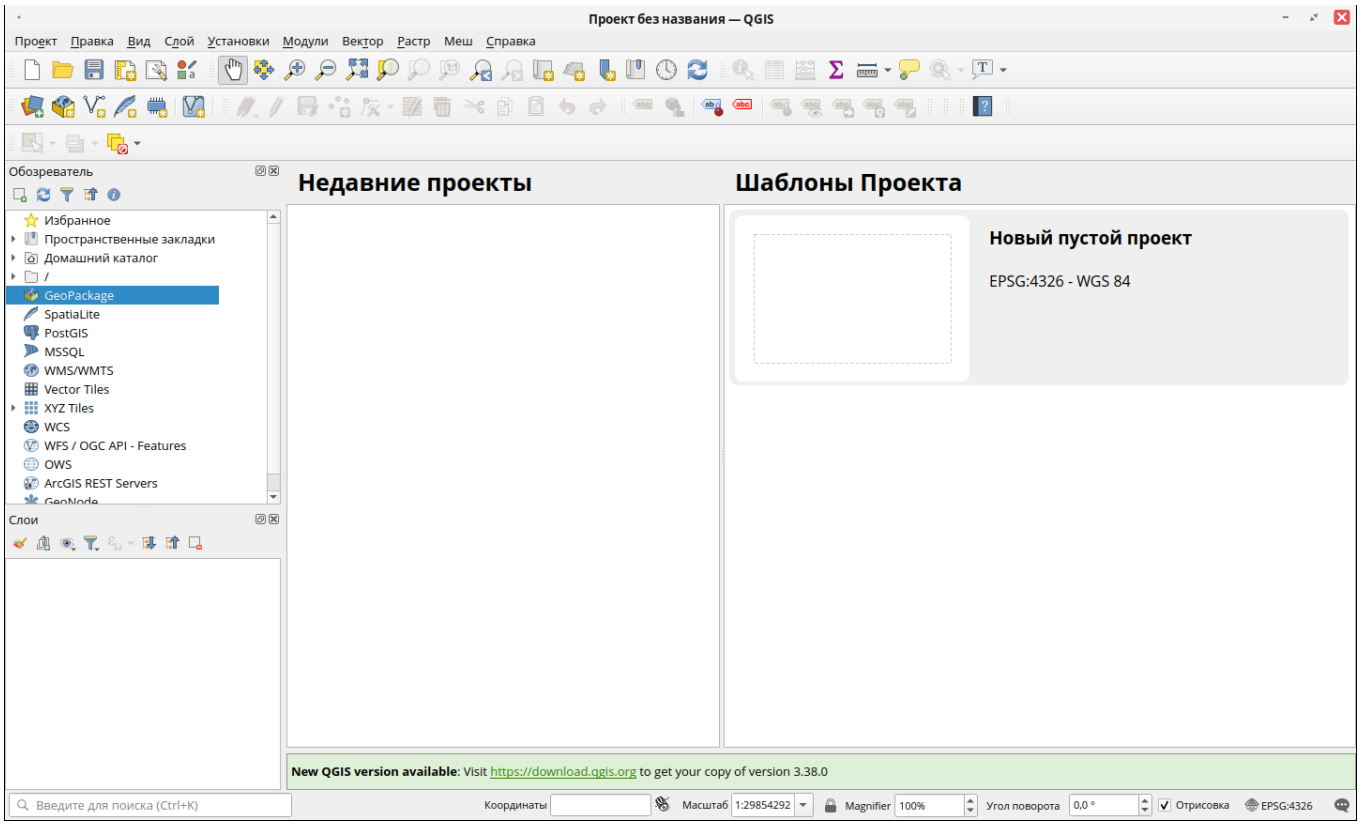
1. *Добавить слой* из текста с разделителями - загружает и выводит текстовые файлы, содержащие координаты x, y.
2. *Захват координат* - получает координаты мыши в различных системах координат.
3. *DB Manager* - импорт/экспорт, редактирование и просмотр слоёв и таблиц, выполнение SQL-запросов.
4. *Наложение диаграмм* - наложение диаграмм на векторные слои.
5. *Преобразователь Dxf2Shp* - преобразование файлов DXF в shape-файлы.
6. *Инструменты GPS* - загрузка и импорт данных GPS.
7. *GRASS* - поддержка ГИС GRASS.
8. *Инструменты GDAL* - интеграция инструментов GDAL в QGIS.
9. *Привязка растров GDAL* - географическая привязка растров.
10. *Теплокарта* - создание растровой теплокарты из точечных данных.
11. *Модуль интерполяции* - интерполяция векторных данных.
12. *Экспорт в Mapserver* - экспорт проекта QGIS в map-файл Mapserver.
13. *Оффлайновое редактирование* - оффлайновое редактирование слоёв и синхронизация с базами данных.
14. *Модуль OpenStreetMap* - просмотр и редактирование данных OpenStreetMap.
15. Доступ к данным *Oracle Spatial GeoRaster*.
16. *Установщик модулей Python* - загрузка и установка модулей QGIS.
17. *Морфометрический анализ* - морфометрический анализ растровых слоев.
18. *Road graph* - поиск кратчайшего маршрута.
19. *SPIT* - инструмент импорта shape-файлов в PostgreSQL/PostGIS.
20. *SQL Anywhere* - работа с векторными слоями в БД SQL Anywhere.
21. *Зональная статистика* - расчет количества, суммы, среднего значения ячеек растра в пределах заданных полигонов.
22. *Пространственные запросы* - пространственные запросы для векторных слоёв.
23. *eVIS* - инструмент визуализации событий — показ изображений, связанных с векторными объектами.
24. *fTools* - инструменты для управления векторными данными и их анализа.

Установка

Установка программы в РЕД ОС осуществляется командой:

```
dnf install qgis
```

Стартовое окно программы выглядит следующим образом:



Подробную информацию о работе в QGIS см. в официальной документации.

Weasis — программа просмотра диагностических изображений в формате DICOM

Установка Weasis
Смена языка интерфейса
Открытие изображений

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: weasis-4.0.3-1

Примечание.

Данная статья актуальна **только** для РЕД ОС **Стандартной редакции**.

Weasis — средство для просмотра диагностических изображений в формате **DICOM** (**.dcm**), которые используются в здравоохранении.

Является бесплатным программным обеспечением с открытым исходным кодом. Weasis поддерживает многопоточность, что позволяет выполнять высококачественный рендеринг с высокой производительностью за счет **OpenCV**-библиотеки.

Также программа имеет удобный пользовательский интерфейс и работает на экранах с высоким разрешением.

Основные особенности, заявленные разработчиками программы:

- отображение всех типов файлов DICOM (включая многокадровые, расширенные, *MPEG-2*, *MPEG-4*, *SR*, *PR*, *KOS*, *AU*, *RT* и *ЭКГ*);
- средство просмотра распространенных форматов изображений (*TIFF*, *BMP*, *GIF*, *JPEG*, *PNG*, *RAS*, *HDR* и *PNM*);
- манипуляции с изображением (панорамирование, масштабирование, управление окнами, вращение, отражение, прокрутка);
- отображение и поиск по всем атрибутам *DICOM*;
- отображение поперечных линий;
- инструменты измерения и аннотации;
- гистограмма значений модальности;
- сохранение измерений и аннотаций в файле *DICOM PR* или *XML*;
- импорт CD/DVD и локальных файлов *DICOM*;
- экспорт *DICOM* с несколькими вариантами (*DICOMDIR*, *ZIP*, файл образа *ISO*, создание новых *UID*, транскодирование, *TIFF*, *JPEG*, *PNG*...);
- стеклянная лупа с расширенными параметрами отображения;
- печать и печать *DICOM*;
- чтение изображения *DICOM*, содержащего плавающие или двойные данные (параметрическая карта);
- программа просмотра *ЭКГ DICOM*;
- модуль **Dicomizer** для преобразования стандартных изображений в формат *DICOM*.

Вы можете подробнее ознакомиться с настройкой и работой утилиты **weasis**, просмотрев наши обучающие видео:

- на **RuTube** — Weasis — программа просмотра диагностических изображений в формате DICOM;
- в **Яндекс.Дзен** — Weasis — программа просмотра диагностических изображений в формате DICOM;
- в **VK Видео** — Weasis — программа просмотра диагностических изображений в формате DICOM.

На наших каналах вы также сможете найти много другой полезной информации.

Установка Weasis

Перейдите в сеанс пользователя **root**:

```
su -
```

Сначала необходимо подключить репозиторий **redos-3rdparty-weasis** командой:

```
dnf install redos-3rdparty-weasis
```

Далее выполните команду установки **Weasis**:

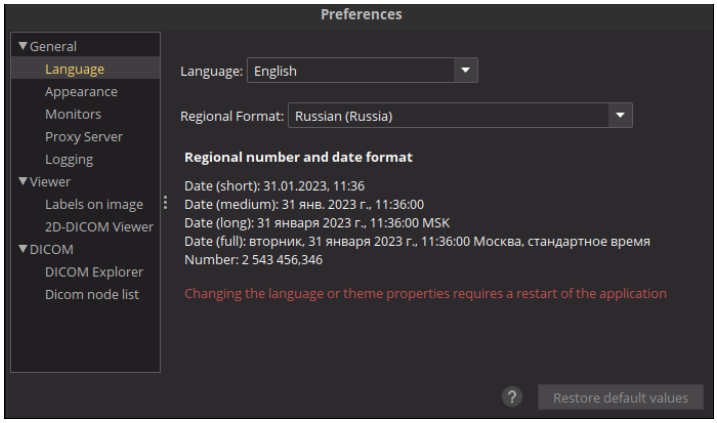
```
dnf install weasis
```

После установки программа доступна из «**Главного меню**» – «**Графика**» – «**Weasis**».

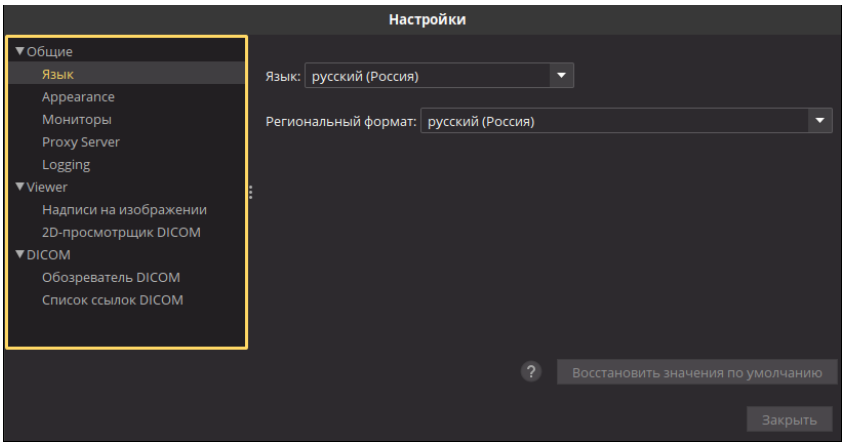
Смена языка интерфейса

Для смены языка программы выберите пункт меню «**File**» - «**Preferences...**», в открывшемся окне настроек откройте пункт **General** – **Language** и выберите из списка необходимый язык.

Интерфейс настроек на английском языке выглядит следующим образом:

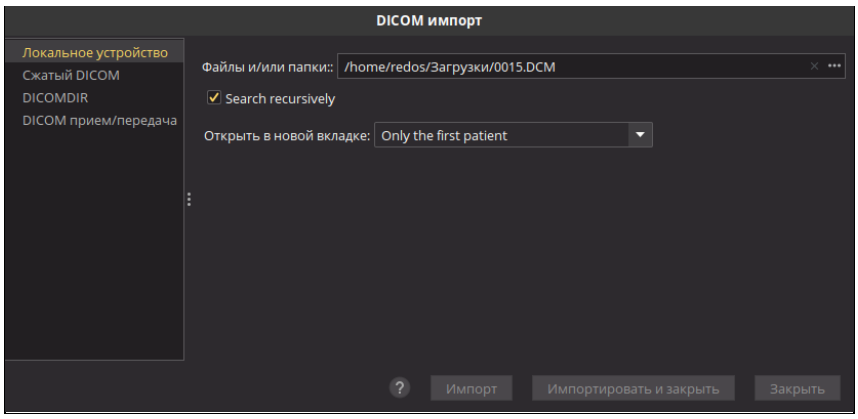


Интерфейс настроек на русском языке выглядит следующим образом (для изменения языка интерфейса необходимо перезапустить программу):

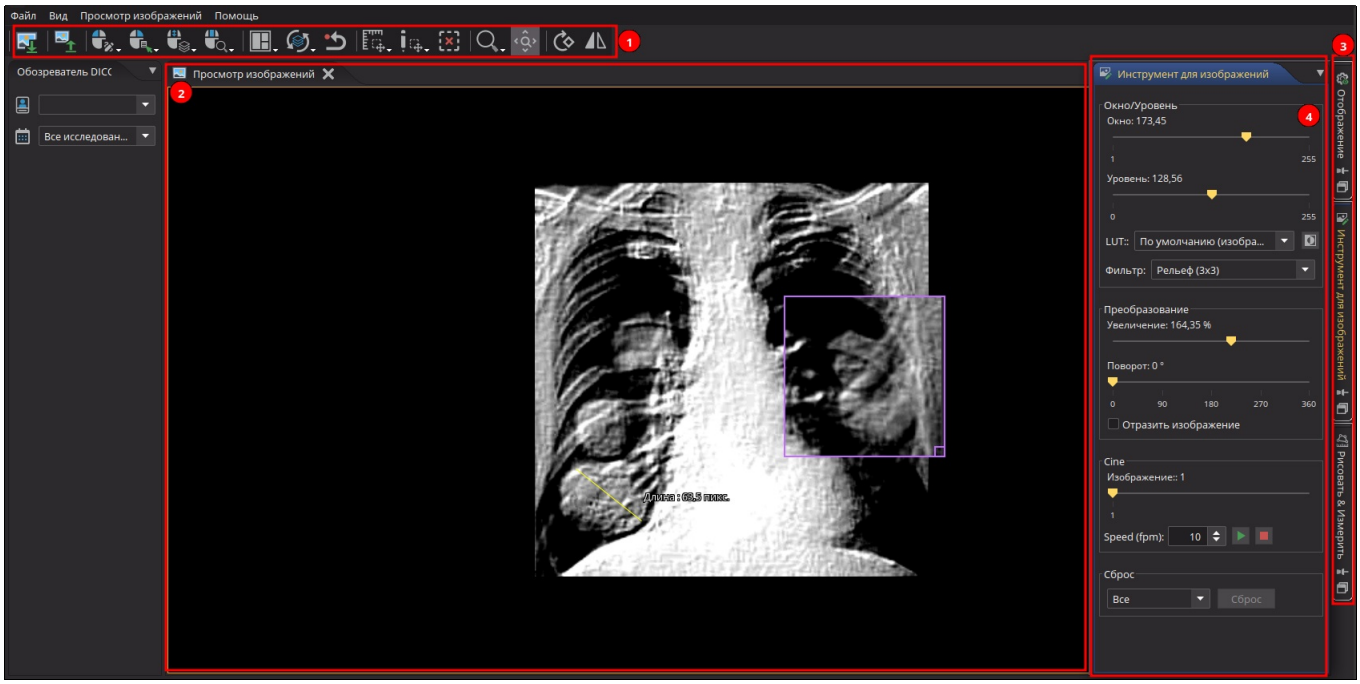


Открытие изображений

Для открытия DICOM-файла в меню программы выберите **Файл** – **Импорт** – **Dicom**.



Диагностическое изображение будет загружено в программу и доступно для детального изучения:



После загрузки изображения станут доступны инструменты для работы. Рассмотрим их подробнее:

1. Панели инструментов.

Здесь располагаются основные инструменты для работы с изображением, такие как *Импорт*, *Экспорт*, *Панель настраиваемых функций мыши*, *Панель расположения изображений*, *Панель инструментов увеличения изображения*, *Панель инструментов вращения* и т. д.

2. Основное окно программы для просмотра изображений.

3. Панель вкладок дополнительных инструментов.

Здесь сгруппированы инструменты *Отображения*, *Измерения* и *Обработки изображений*.

4. Подробное отображение дополнительных инструментов.

При выборе определенной вкладки дополнительных инструментов будет открыта их детальная настройка.

Клавиатурный тренажер KTouch

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** ktouch-19.12.2-1

Клавиатура является наиболее часто используемым устройством ввода на любом компьютере. Большинство задач, которые пользователи выполняют с помощью мыши или трекпада, можно выполнить намного быстрее с помощью клавиатуры и некоторых сочетаний клавиш и сенсорного ввода.

Сенсорный ввод текста - это техника, которая помогает печатать тесты быстрее, помещая пальцы на определенные части клавиатуры и нажимая на клавиши, не глядя на клавиатуру.

Несколько причин для освоения навыка сенсорного ввода:

- уменьшение усталости пальцев, поскольку все клавиши находятся рядом;
- повышенная точность по мере развития мышечной памяти;
- улучшение осанки, поскольку не нужно смотреть на клавиатуру;
- быстрое исправление ошибок.

KTouch — это тренажёр для обучения методу слепой печати текста. Он предоставляет текст для тренировки и подстраивается под разные уровни навыков пользователя. Программа отображает клавиатуру и указывает, какую клавишу следует нажать следующей и какой палец при этом использовать.

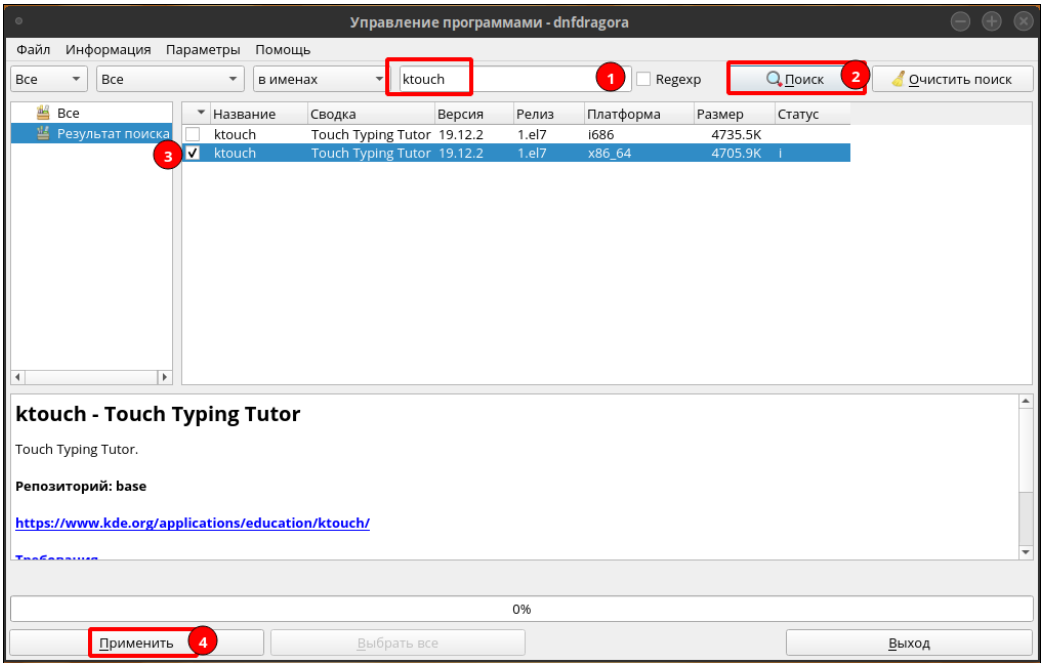
Вы можете подробнее ознакомиться с работой на тренажере **Ktouch**, просмотрев наши обучающие видео:

- на **RuTube** — Клавиатурный тренажер KTouch;
- в **Яндекс.Дзен** — Клавиатурный тренажер KTouch;
- в **VK Видео** — Клавиатурный тренажер KTouch.

На наших каналах вы также сможете найти много другой полезной информации.

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**ktouch**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

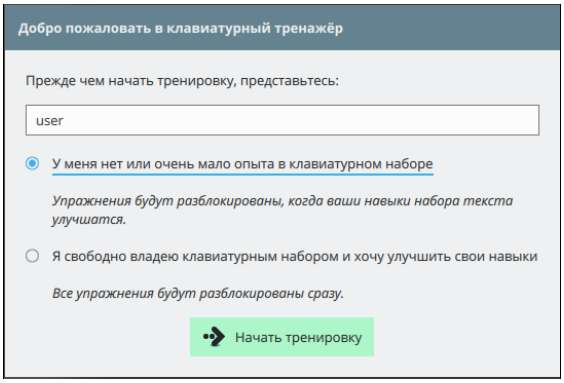
и выполните команду:

```
dnf install ktouch
```

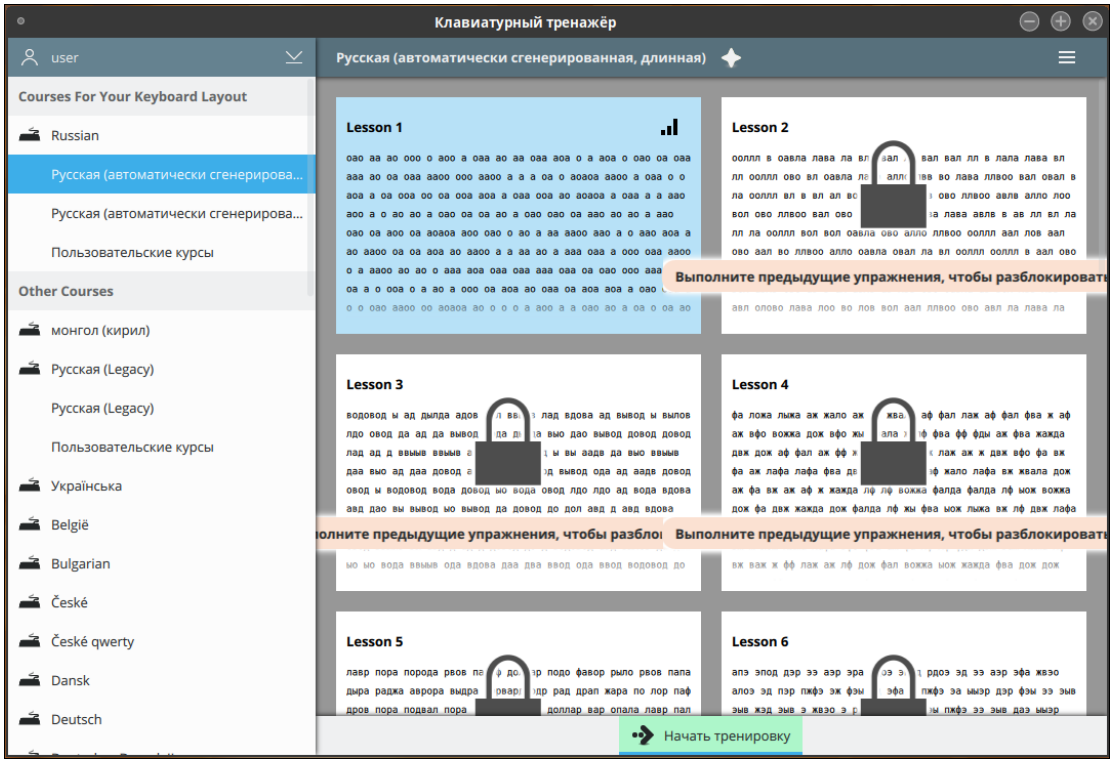
Дальнейшая работа в программе выполняется **от локального пользователя**.

После установки программа будет доступна из «**Главного меню**» - «**Образовательные**» - «**Ktouch**».

При первом запуске программы будет предложено ввести имя пользователя и выбрать уровень владения клавиатурным набором.

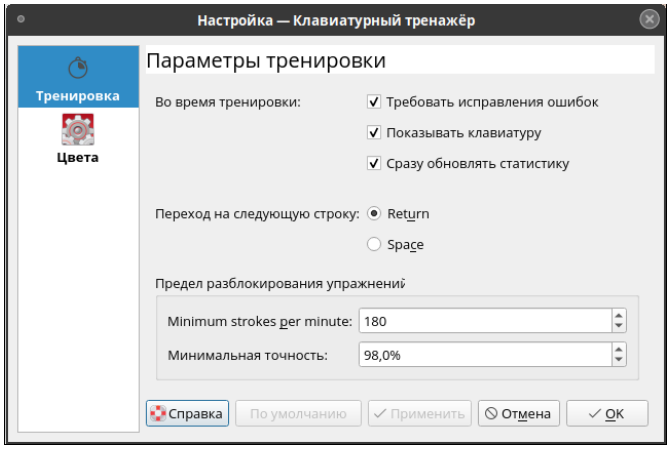


При выборе *начального уровня* — задания будут разблокированы по мере выполнения, при выборе *профессионального уровня* — все упражнения будут разблокированы сразу.



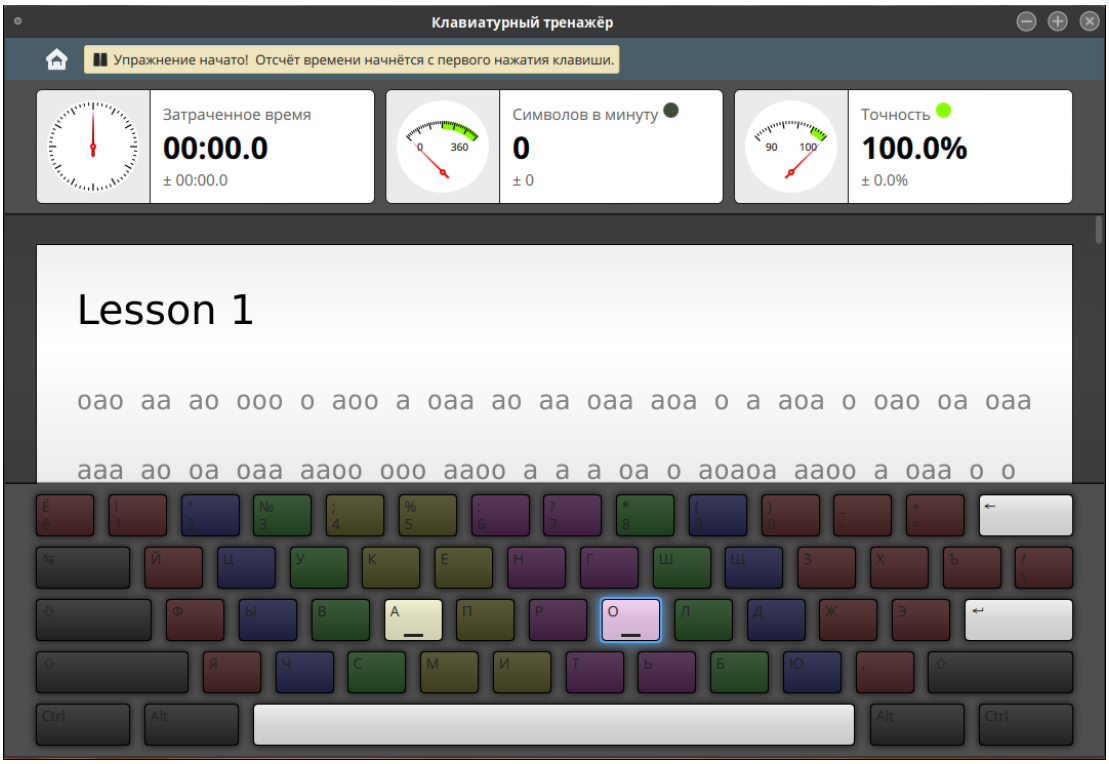
В списке слева можно выбрать любой язык для тренировок.

В **Настройках** есть возможность задать параметры тренировки — требовать ли исправления ошибок, указать минимальную точность и скорость печати в минуту. Также есть возможность задать параметры цвета. Во время упражнений перед Вами будет располагаться клавиатура с соответствующими цветами для подсказки.

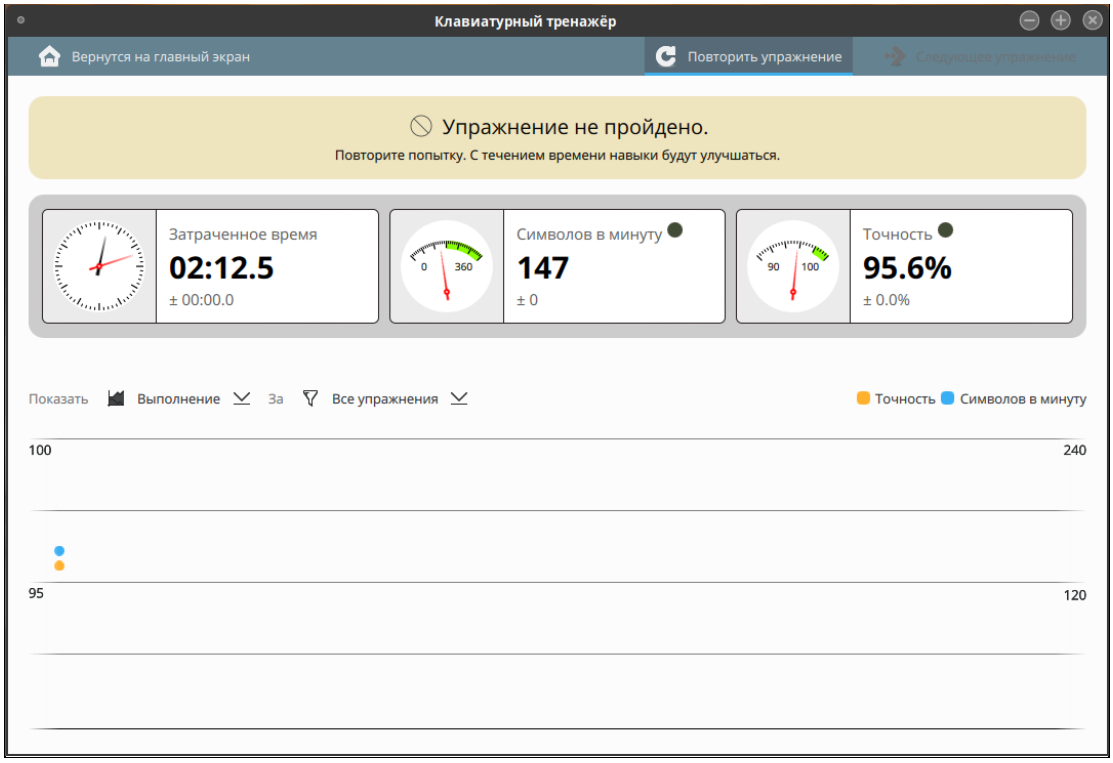


Выберите первый урок и нажмите «**Начать тренировку**».

Каждый урок длится несколько минут и представляет вам различные комбинации клавиш. По мере выполнения, если будут встречаться ошибки, *ktouch* подчеркнет их красным цветом. Добравшись до конца строки, не забудьте нажать **Enter**, а если допустили ошибку - используйте клавишу **Bakspase**.



В конце каждого урока *KTouch* представляет отчет о проделанной работе и статус — **Пройденный** или **Неудачный**.


Клавиатурный тренажёр
Вернутся на главный экран
Повторить упражнение
Следующее упражнение
Упражнение не пройдено.
Повторите попытку. С течением времени навыки будут улучшаться.
Затраченное время
02:12.5
± 00:00.0
Символов в минуту
147
± 0
Точность
95.6%
± 0.0%
Показать
Выполнение
За
Все упражнения
Точность
Символов в минуту
100
240
95
120

LibreCAD

Установка LibreCAD
Описание программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: librecad-2.2.0-0.11

LibreCAD – это мощный и бесплатный проект с открытым исходным кодом для проектирования 2D-технологий. Он предлагает широкий набор инструментов, позволяющих создавать высококачественные чертежи. Этот инструмент имеет простой и интуитивно понятный пользовательский интерфейс, что делает его идеальным выбором для начинающих пользователей, которые хотят освоить искусство компьютерного проектирования, а также для профессионалов, которым нужен надежный инструмент для работы с 2D-моделями.

Особенности **LibreCAD**:

- Кроссплатформенность – **LibreCAD** доступен на операционных системах Windows, macOS и Linux, что делает его универсальным инструментом для пользователей всех типов систем.
- Интерфейс и инструменты – программа предлагает широкий набор инструментов для создания точных чертежей. Он включает в себя создание линий, окружностей, дуг, текста, а также специализированные инструменты для работы с размерами и слоями.
- Поддержка форматов – **LibreCAD** поддерживает широкий спектр форматов файлов, включая **DXF**, поэтому пользователи могут легко импортировать и экспортировать свои чертежи в/из других CAD-систем.
- Сообщество и поддержка – благодаря своему статусу OpenSource-проекта, **LibreCAD** имеет активное сообщество пользователей и разработчиков, что обеспечивает постоянное обновление и улучшение программы.

LibreCAD нашел широкое применение в различных областях, включая архитектуру, инженерное дело, и даже в образовательных целях. Программа позволяет пользователям создавать точные чертежи различной сложности, начиная от простых эскизов и заканчивая более сложными техническими чертежами.

Установка LibreCAD

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

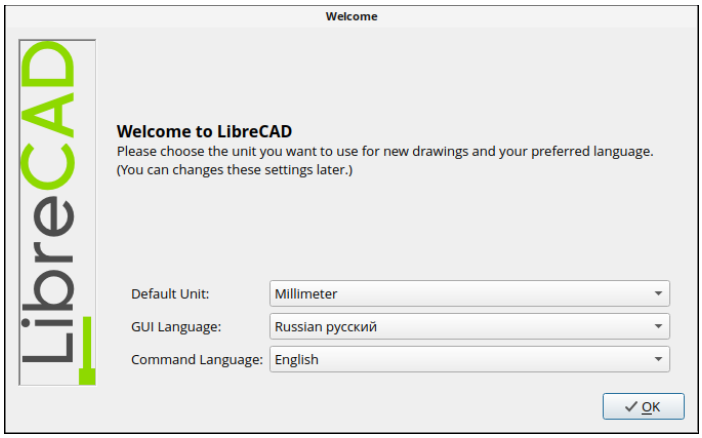
и выполните команду:

```
dnf install librecad
```

Запуск программы доступен из «**Главного меню**» – «**Графика**» – «**LibreCAD**».

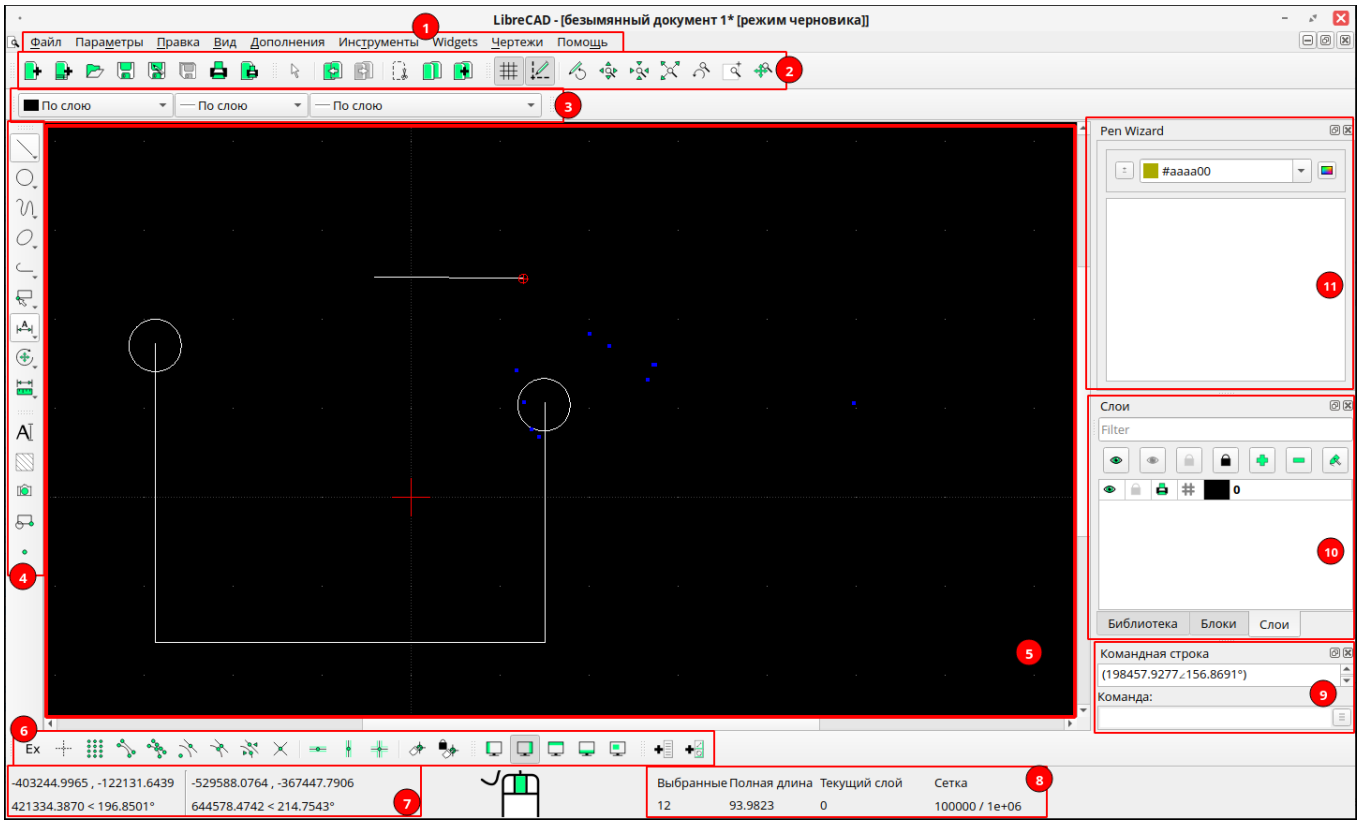
При первом запуске необходимо выбрать систему измерения по умолчанию, язык интерфейса и язык команд.

Выберите необходимые параметры и нажмите «**OK**».



Описание программы

Главное окно программы выглядит следующим образом:



1. *Основное меню* программы, где доступны все действия по настройке и работе программы.

2. *Панель инструментов* – здесь доступны основные действия над проектом, такие как создание нового проекта, сохранение проекта, печать проекта, масштабирование, добавление сетки для удобства и пр.

3. *Панель настройки линий* – цвет, ширина, тип.

4. *Боковая панель* инструментов с основными инструментами для создания проекта, такими как создание линий, окружностей, кривых, измерение расстояния, выбор блоков, добавление текста и пр.

5. *Рабочая область*, где создается проект.

6. *Нижняя панель* – здесь настраивается привязка объектов, ограничения, положение относительного нуля, отображение панелей и добавление нового меню и новых панелей инструментов.

7. *Координаты* положения курсора.

8. *Данные* о выбранных точках (объектах).

9. *Командная строка* – здесь доступно выполнение каких-либо команд над объектом.

10. *Панель слоев* – здесь можно отображать/скрывать слои для удобства работы, а также защищать от модификации объекты чертежа.

11. *Панель* для задания *цвета* выбранному объекту.

Программа имеет интуитивно понятный интерфейс. В случае если возникают какие-либо сложности в работе, доступна онлайн-справка по работе. Для ее вызова в основном меню программы выберите «**Помощь**» – «**Онлайн**».

NanoCAD 24.1

Модульный состав программы
Системные требования
Установка NanoCAD
Установка Платформы nanoCAD из репозитория
Установка Платформы nanoCAD из установочных пакетов
Лицензионное соглашение
Активация локальной лицензии
Запрос и активация локальной лицензии онлайн
Активация локальной лицензии оффлайн при помощи сохранения лицензионного запроса
Активация локальной лицензии оффлайн при помощи файла лицензии
Сервер лицензий
Установка сервера лицензий Нанософт из репозитория
Установка сервера лицензий Нанософт из установочного пакета
Активация сетевой лицензии оффлайн при помощи файла сетевой лицензии
Запрос и активация сетевой лицензии онлайн
Подключение к серверу лицензий
Состояние лицензии
Проверка подключения к локальным базам данных PostgreSQL СПДС и Механика
Установка Сервера лицензий в РЕД ОС конфигурации Сервер минимальный
Установка баз данных PostgreSQL СПДС и Механика на сервер
Дополнительная информация

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: NanoCAD-24.1-x86_64

NanoCAD представляет собой универсальный векторный редактор, а также графическую платформу для целого ряда вертикальных приложений – систем автоматизированного проектирования (САПР) в различных областях проектирования.

NanoCAD предоставляет проектировщикам полный набор современных инструментов для создания и редактирования векторных примитивов, трехмерных объектов, блоков, размеров, таблиц как в пространстве модели, так и в пространстве листа посредством видовых экранов, а также для подготовки, оформления и выпуска графической технической документации.

NanoCAD предназначается как для работы индивидуального пользователя, так и для работы проектных коллективов, с использованием функционала внешних ссылок и возможностью интеграции в системы инженерного документооборота, в том числе в системы **PDM/PLM**.

NanoCAD поддерживает импорт и экспорт векторных данных в различные 3D и 2D форматы.

Модульный состав программы

Помимо основного функционала, платформа **nanoCAD** включает в себя несколько независимо лицензируемых встроенных модулей:

- **Модуль СПДС**. Модуль позволяет быстро и точно оформлять проектно-конструкторскую документацию по общетехническим требованиям нормативных документов, применяемых в строительной отрасли. Планы, фасады, разрезы, сечения, виды, узлы и другие чертежи выполняются «на лету» с помощью инструментов, создающих динамические «умные» чертежи.
- **Модуль Механика**. Модуль предназначен для проектирования машиностроительных изделий и оформления конструкторской и технологической документации в полном соответствии с требованиями ГОСТ (ЕСКД и ЕСТД) и основными зарубежными стандартами. Наличие параметрических объектов и средств автоматизированного проектирования среднего уровня делают это программное решение одним из самых удобных инструментов создания и оформления чертежей.
- **Модуль Растр** расширяет возможности работы платформы с различными растровыми изображениями, включая сканированные документы – чертежи, планы, схемы и т.п. Базовая конфигурация платформы *nanoCAD* предоставляет возможность использовать такого рода данные лишь в качестве подложки, сопровождая это набором из нескольких инструментов по 4-х точечной коррекции, выравниванию, обрезке и настройке параметров отображения растровых изображений. В состав модуля **Растровое редактирование** входит широкий набор инструментов по улучшению качества изображений, их преобразованию, интеллектуальному анализу и редактированию, извлечению семантической информации (векторизации), полуавтоматической трассировке векторных примитивов и распознаванию текстов, а также растеризации произвольного вида данных, поддерживаемых *nanoCAD*.
- **Модуль 3D на ядре C3D**, включающий в себя функционал **2D** и **3D Зависимостей**. Модуль позволяет при помощи инструментов трехмерного проектирования формировать сложные трехмерные сцены любой геометрической формы. С помощью функции создания сечений можно получать автоматически обновляемые двумерные виды.

- **Модуль Организация** – централизованное управление настройками рабочих мест *nanoCAD* на предприятии.
- **Модуль Топоплан** предназначен для создания цифровой модели местности и подготовки чертежа к выпуску топографических планов. В модуль включена поддержка объектов **Civil 3D**. Если открыть чертёж, содержащий такие объекты, то они будут отображаться как объекты чертежа (а не в виде прокси-графики), будет доступно отображение их свойств, переключение стилей, управление элементами стилей.

На время триального (пробного) периода все модули доступны. По окончании триального периода для активации любого модуля необходимо получить соответствующую лицензию.

Существует три варианта платформ *nanoCAD*:

- платформа ***nanoCAD*** с бесплатным пробным периодом 30 дней;
- платформа ***nanoCAD Standart*** для представителей малого и среднего бизнеса;
- платформа ***nanoCAD Pro*** с максимальной конфигурацией для крупных и корпоративных клиентов.

Актуальные цены на платформы *nanoCAD* приведены на официальном сайте разработчика ПО.

Системные требования

Перед установкой *NanoCAD* убедитесь, что ваша система выполняет условия минимальных системных требований.

Оптимальная производительность и более высокая стабильность работы *NanoCAD* может быть достигнута, когда используемая операционная система выполняет условия рекомендуемых системных требований.

	Минимальные требования	**Рекомендуемые требования**
Процессор	2 ГГц	3 ГГц и выше
Оперативная память	4 Гб	16 Гб и выше
Видеоадаптер	Графический процессор с поддержкой 3D-ускорения, объемом видеопамяти 1 Гб	Графический процессор с поддержкой 3D-ускорения, объемом видеопамяти 4 Гб (поддерживающий OpenGL 2.1)
Разрешение экрана	1920 x 1080	до 3840 x 2160
Свободное место на диске	7 Гб и более	
Сеть	На сервере лицензий и всех рабочих станциях, где будут работать приложения, использующие сетевое лицензирование, должен быть запущен протокол **TCP/IP.**	
Интерфейсы	Видеовыход **HDMI** или **Displayport**, устройство для чтения DVD-дисков или USB-порт	

Установка NanoCAD

Установка Платформы nanoCAD из репозитория

Предварительно необходимо подключить репозиторий платформы при помощи скрипта:

```
sudo wget -qO- https://repo.nanodev.ru/r24.1/get_ncad.sh | sudo bash
```

Для автоматической установки платформы NanoCAD совместно с локальным сервером БД Механика и СПДС на запрос скрипта «Желаете установить nanoCAD? [д/Н]:» ответьте yes. Если установка и настройка будет производиться вручную, ответьте no.

Для ручной установки платформы БЕЗ локального сервера PostgreSQL баз данных СПДС и Механика выполните команды:

```
sudo dnf check-update
sudo dnf install ncad24-1
```

Затем выполните настройку сервера и подключения к серверу PostgreSQL на клиенте согласно п. «Установка баз данных PostgreSQL СПДС и Механика на сервер».

Для ручной установки СОВМЕСТНО с локальным сервером PostgreSQL баз данных СПДС и Механика выполните команды:

```
sudo dnf check-update
sudo dnf install ncad-pgsql
sudo dnf install ncad24-1
```

Подключение к локальному серверу баз данных СПДС и Механики будет настроено автоматически. При необходимости, выполните проверку подключения к локальному серверу баз данных PostgreSQL СПДС и Механика согласно п. «Проверка подключения к локальным базам данных PostgreSQL СПДС и Механика».

Если пакет `ncad-data24-1` был установлен раньше, чем `ncad-pgsql`, для установки и настройки баз необходимо выполнить:

```
ncad-db-install24-1
```

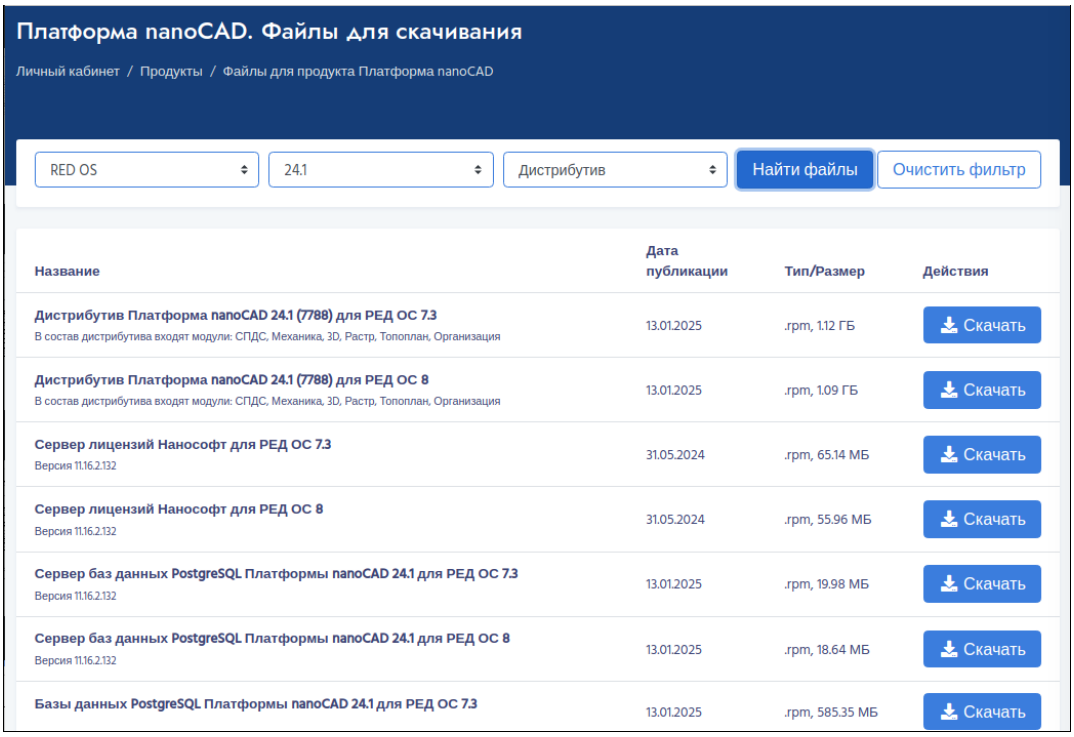
Установка Платформы nanoCAD из установочных пакетов

ВАЖНО!

Для доступа к загрузке дистрибутивов необходимо предварительно зарегистрироваться или авторизоваться в Личном кабинете.

Для загрузки инсталляционных пакетов перейдите по ссылке. На странице задайте фильтр для списка доступных дистрибутивов:

- выберите ОС – **RED OS**;
- выберите версию продукта – **24.1**;
- выберите тип файлов – **дистрибутив**.



Загрузите необходимые пакеты, нажав «**Скачать**».

Для установки БЕЗ локального сервера БД Механика и СПДС загрузите:

- Базы данных платформы NanoCAD для РЕД ОС 8 – ncad-data24-1.red80.x86_64.rpm;
- Платформа NanoCAD для РЕД ОС 8 – ncad24-1.red80.x86_64.rpm.

Для установки СОВМЕСТНО с локальным сервером БД Механикка и СПДС загрузите:

- Сервер БД платформы NanoCAD для РЕД ОС 8 – ncad-pgsql.red80.x86_64.rpm;
- Базы данных платформы NanoCAD для РЕД ОС 8 – ncad-data24-1.red80.x86_64.rpm;
- Платформа NanoCAD для РЕД ОС 8 – ncad24-1.red80.x86_64.rpm.

Затем перейдите в каталог со скачанными файлами – «**Загрузки**» (по умолчанию).

Для установки локальных БД и сервера БД **Механика** и **СПДС** выберите соответствующие инсталляционные пакеты (согласно указанной последовательности установки) и запустите их выполнение двойным кликом ЛКМ. В открывшемся окне «**Аутентификация**» введите пароль администратора. Нажмите **Аутентификация**.

В окне «**Результат транзакции**» будет выведен список устанавливаемых пакетов, нажмите **Хорошо** для продолжения установки.

По окончании установки нажмите **Выход**.

Повторите те же действия для пакета платформы NanoCAD **ncad24.1_x86_64.rpm**.

Примечание.

В случае если по каким-либо причинам пакет **ncad-data24-1.red80.x86_64.rpm** был установлен раньше, чем пакет **ncad-pgsql.red80.x86_64.rpm**, для установки и настройки баз необходимо выполнить:

```
ncad-db-install24-1
```

После успешной установки ярлыки будут созданы в «**Главном меню**» – «**NanoCAD 24.1**». При необходимости, можно создать ярлыки приложений на рабочем столе через контекстное меню. Для этого нажмите ПКМ на нужном приложении и выберите **Поместить на Рабочий стол**.

Лицензионное соглашение

Для дальнейшей работы в программе *NanoCAD* необходимо принять условия Лицензионного соглашения. Для этого из **Главного меню** запустите **Мастер регистрации** или **Платформу nanoCAD 24.1**.

В появившемся окне «**Установка Платформа nanoCAD x64 24.1 — Лицензионное соглашение**» внизу окна установите флаг «**Я принимаю условия Лицензионного соглашения**». Нажмите **Да**.



Активация локальной лицензии

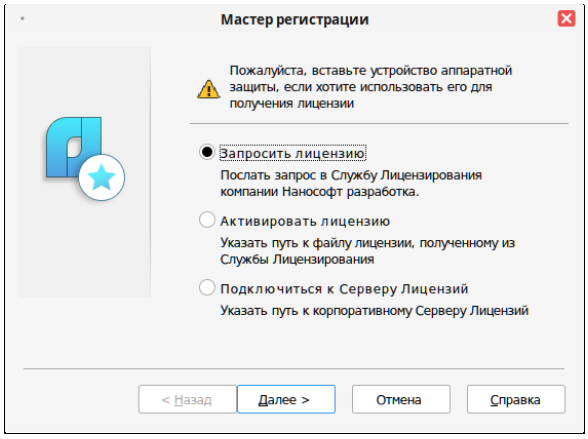
Доступно несколько способов активации лицензии:

- запрос и активация лицензии онлайн;
- активация лицензии оффлайн при помощи сохранения лицензионного запроса;
- активация лицензии оффлайн при помощи файла лицензии.

Для активации лицензии запустите **Мастер регистрации**, который доступен из «**Главного меню**» — «**nanoCAD 24.1**».

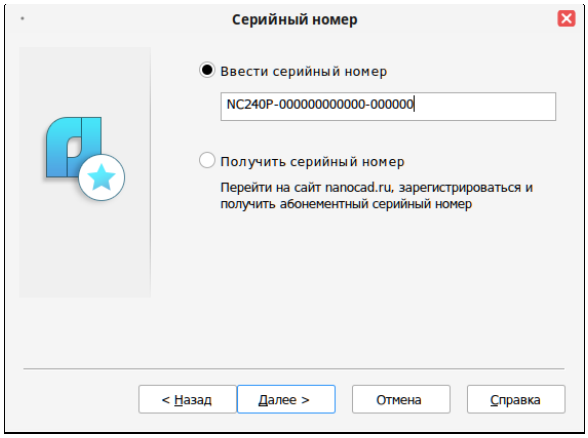
Запрос и активация локальной лицензии онлайн

После запуска **Мастера регистрации** выберите «**Запросить лицензию**» и нажмите **Далее**.



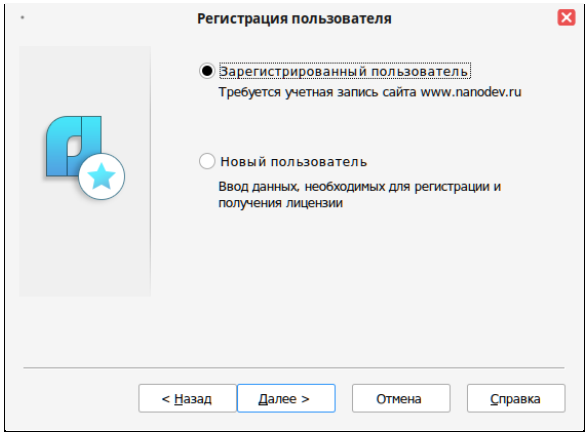
В открывшемся окне «**Серийный номер**» введите серийный номер (если у вас нет серийного номера, выберите пункт « **Получить серийный номер**»). Серийный номер имеет вид *NC240P-000000000000-000000*.

Нажмите **Далее**.



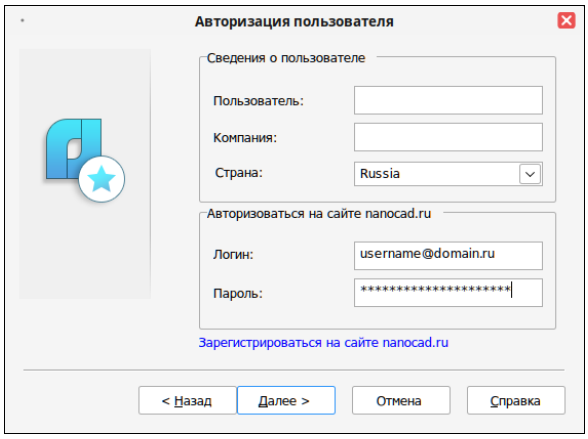
Будет открыто окно «**Регистрация пользователя**».

Если у вас уже есть учетная запись в личном кабинете на сайте https://lk.nanocad.ru, выберите пункт **Зарегистрированный пользователь**. В противном случае, необходимо зарегистрироваться в личном кабинете на сайте https://lk.nanocad.ru перед продолжением процедуры запроса лицензии.



В окне «**Авторизация пользователя**» поля **Логин** и **Пароль** следует заполнять теми значениями, которые были использованы при регистрации в личном кабинете на сайте https://lk.nanocad.ru.

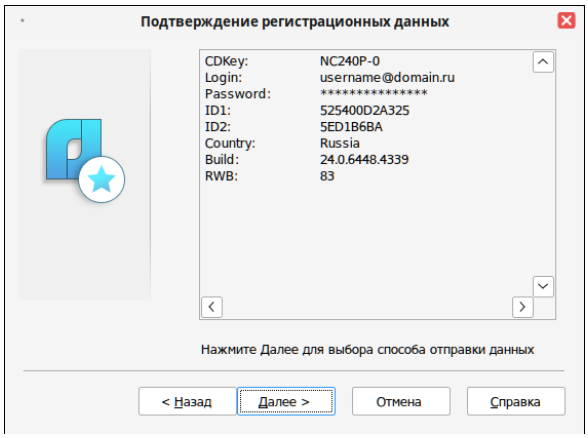
Если вы не зарегистрированы в личном кабинете на сайте https://lk.nanocad.ru, нажмите на ссылку **Зарегистрироваться на сайте www.nanodev.ru**. После регистрации введите ваши регистрационные данные в полях **Логин** и **Пароль**.



Опционально можно заполнить поля **Пользователь** и **Компания**. Информация из этих полей будет отображаться при запуске программного обеспечения.

Заполните необходимые поля и нажмите **Далее**.

В окне подтверждения регистрационных данных отображаются данные, которые будут отправлены в **ООО «Нанософт разработка»** для получения локальной лицензии.

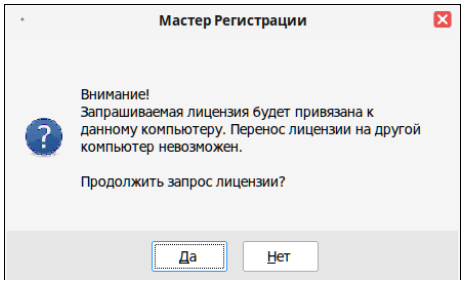


Проверьте введенные данные и подтвердите их нажатием кнопки **Далее**. В случае обнаружения ошибки нажмите **Назад** и исправьте информацию в тех полях, где это необходимо.

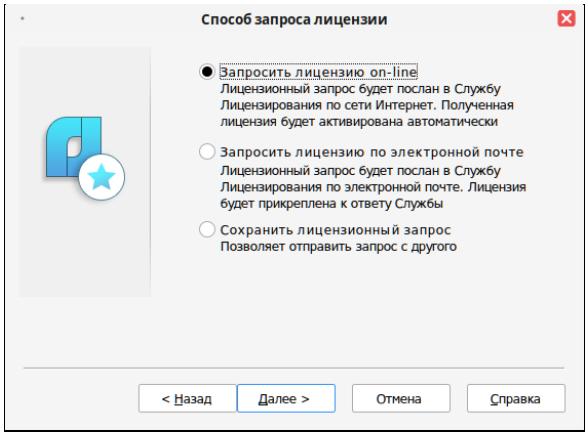
ВАЖНО!

Внимательно проверяйте указанные регистрационные данные. При неверном заполнении регистрационных полей разработчик программного обеспечения **ООО «Нанософт разработка»** может отказать в выдаче лицензии.

Подтвердите привязку лицензии к компьютеру, нажав **Да** в появившемся запросе **Мастера регистрации**.

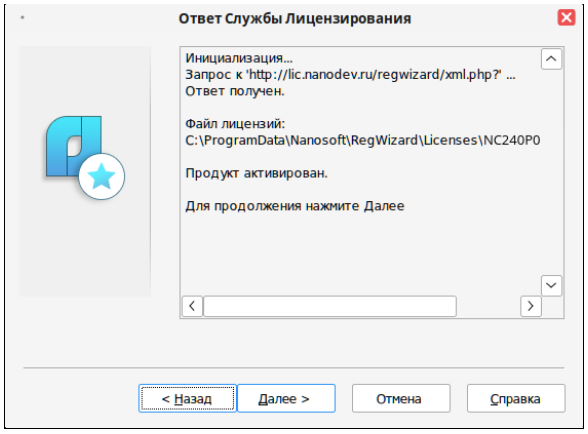


После подтверждения запроса лицензии будет открыто окно «**Способ запроса лицензии**».



Запрос лицензии онлайн производится только с компьютера, имеющего выход в сеть Интернет.

При запросе лицензии онлайн **Мастер регистрации** автоматически соединится с **Сервером лицензий**, сохранит и активирует лицензию.



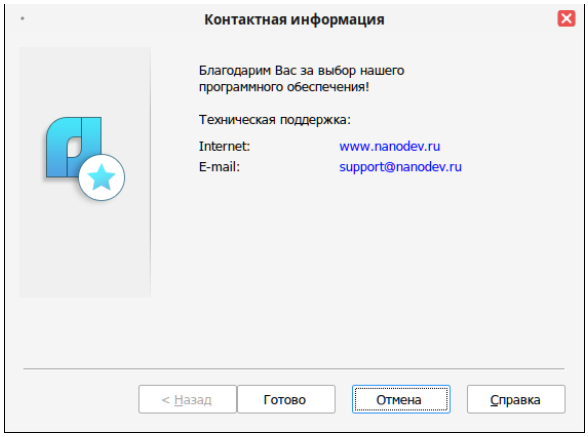
Примечание.

Все файлы лицензий, полученные таким способом, помещаются в следующую директорию **/home/<username>/.ncad_24.1x64/drive_c/ProgramData/Nanosoft/RegWizard/Licenses**.

Результатом запроса лицензии онлайн может быть:

- успешное получение лицензии;
- отказ в выдаче лицензии;
- неудачное соединение.

В случае *успешного* завершения нажмите **Далее** и в следующем окне, содержащем контактную информацию, нажмите **Готово**.



На этом процесс лицензирования продукта **ООО «Нанософт разработка»** успешно завершен. Никаких других действий по лицензированию установленного продукта производить не требуется.

Запустите **Платформу nanoCAD**.

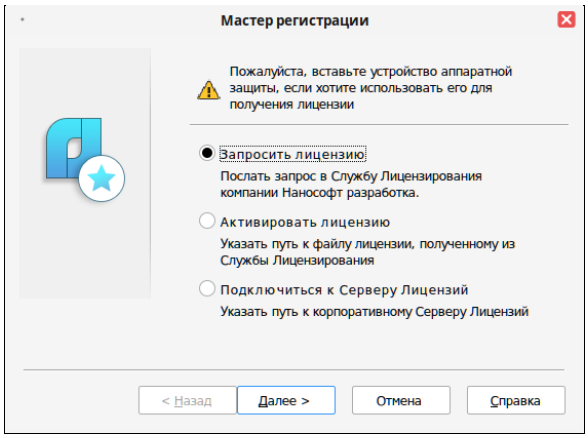
Если по той или иной причине **Сервер** отказал в выдаче локальной лицензии, нажмите **Далее** и в следующем окне, содержащем контактную информацию, нажмите **Готово**, завершив работу.

В случае неудачного соединения с **Сервером**, а также при невозможности получить локальную лицензию выбранным способом нажмите **Далее** и, вернувшись в окно «**Способ запроса лицензии**», выберите другой вариант осуществления запроса.

Дождитесь ответа службы лицензирования.

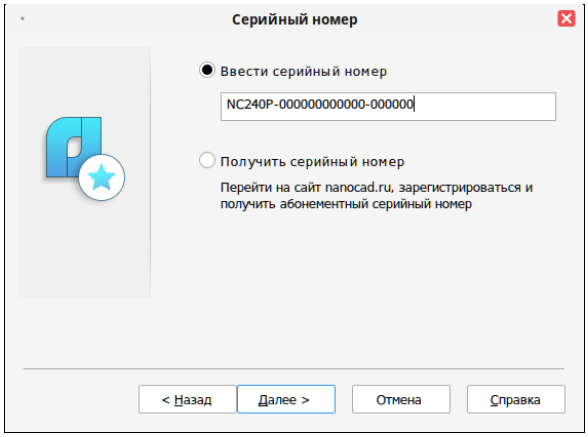
Активация локальной лицензии оффлайн при помощи сохранения лицензионного запроса

После запуска **Мастера лицензий** выберите «**Запросить лицензию**» и нажмите **Далее**.



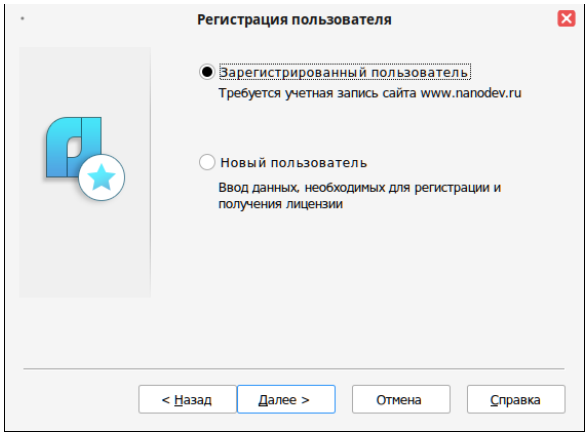
В открывшемся окне «**Серийный номер**» введите серийный номер (если у вас нет серийного номера, выберите пункт « **Получить серийный номер**»). Серийный номер имеет вид *NC240P-000000000000-000000*.

Нажмите **Далее**.



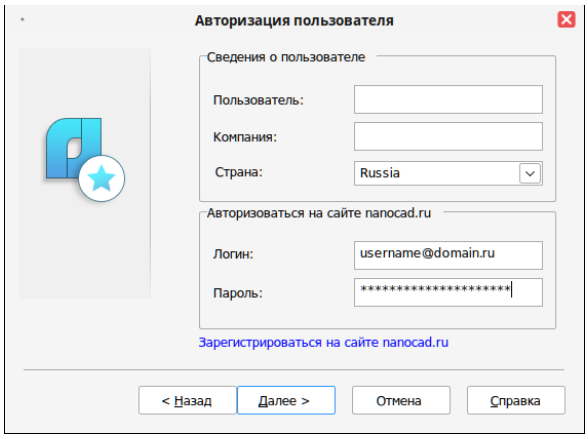
Будет открыто окно «**Регистрация пользователя**».

Если у вас уже есть учетная запись в личном кабинете на сайте https://lk.nanocad.ru, выберите пункт **Зарегистрированный пользователь**. В противном случае, необходимо зарегистрироваться в личном кабинете на сайте https://lk.nanocad.ru перед продолжением процедуры запроса лицензии.



В окне «**Авторизация пользователя**» поля **Логин** и **Пароль** следует заполнять теми значениями, которые были использованы при регистрации в личном кабинете на сайте https://lk.nanocad.ru.

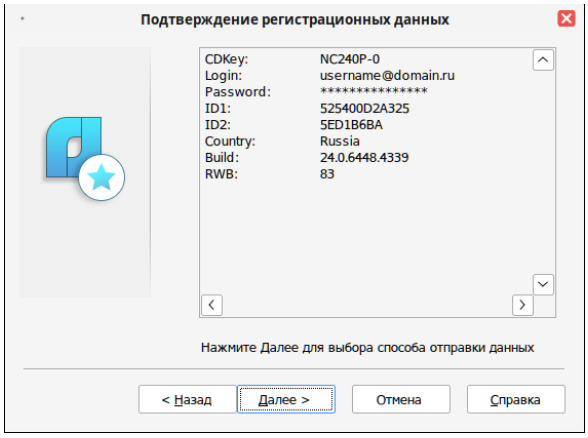
Если вы не зарегистрированы в личном кабинете на сайте https://lk.nanocad.ru, нажмите на ссылку **Зарегистрироваться на сайте www.nanodev.ru**. После регистрации введите ваши регистрационные данные в полях **Логин** и **Пароль**.



Опционально можно заполнить поля **Пользователь** и **Компания**. Информация из этих полей будет отображаться при запуске программного обеспечения.

Заполните необходимые поля и нажмите **Далее**.

В окне подтверждения регистрационных данных отображаются данные, которые будут отправлены в **ООО «Нанософт разработка»** для получения локальной лицензии.

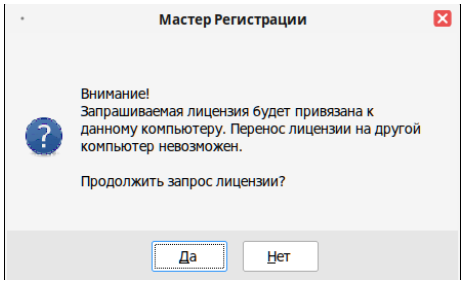


Проверьте введенные данные и подтвердите их нажатием кнопки **Далее**. В случае обнаружения ошибки нажмите **Назад** и исправьте информацию в тех полях, где это необходимо.

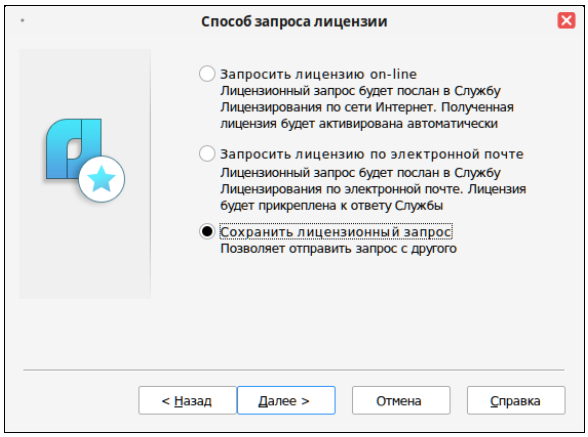
ВАЖНО!

Внимательно проверяйте указанные регистрационные данные. При неверном заполнении регистрационных полей разработчик программного обеспечения **ООО «Нанософт разработка»** может отказать в выдаче лицензии.

Подтвердите привязку лицензии к компьютеру, нажав **Да** в появившемся запросе **Мастера регистрации**.



После подтверждения запроса лицензии будет открыто окно «**Способ запроса лицензии**».



Если компьютер, с которого производится запрос лицензии, не подключен к сети Интернет, необходимо выбрать пункт **Сохранить лицензионный запрос**.

При выборе этого пункта программа автоматически создаст шаблон электронного письма.

Для продолжения процедуры лицензирования необходимо отправить сформированное письмо с компьютера, имеющего выход в сеть Интернет, в службу лицензирования **ООО «Нанософт разработка»**.

ВАЖНО!

Не изменяйте тему и содержимое сохранённого лицензионного запроса при отправке письма. Изменение содержимого может привести к отказу в выдаче лицензионного файла.

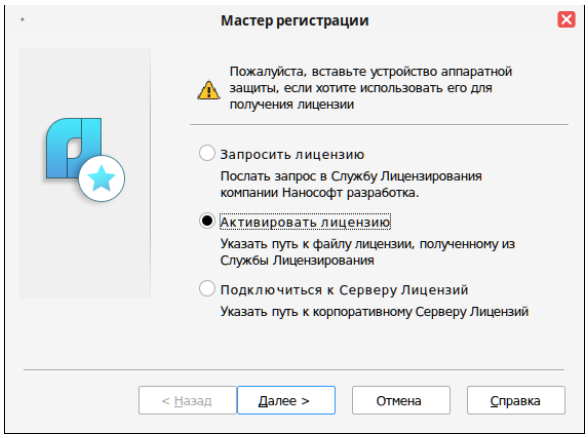
Результатом запроса лицензии при помощи электронной почты будет ответ службы лицензирования с файлом лицензии. Для активации **Платформы nanoCAD** при помощи файла локальной лицензии перейдите к пункту «Активация локальной лицензии оффлайн при помощи файла лицензии».

Активация локальной лицензии оффлайн при помощи файла лицензии

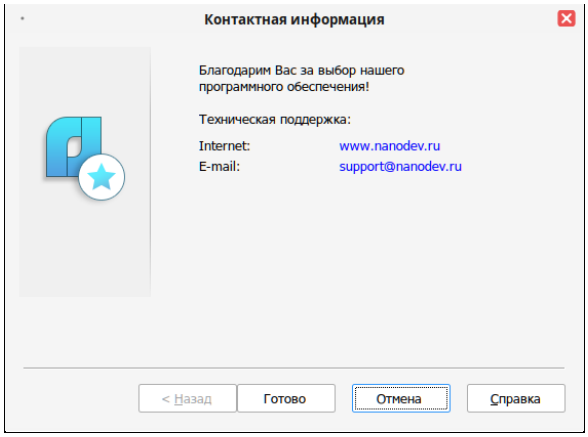
Скопируйте полученный от службы лицензирования **ООО «Нанософт разработка»** файл лицензии на компьютер, где установлен программный продукт, требующий лицензирования.

Запустите Мастер регистрации, который доступен из «**Главного меню**» — «**nanoCAD 24.1**».

В открывшемся окне **Мастера регистрации** программного обеспечения выберите пункт **Активировать лицензию** и нажмите **Далее**.



Укажите путь к файлу лицензии, нажав «**Обзор...**». Нажмите **Далее**.



На этом процесс лицензирования продукта **ООО «Нанософт разработка»** успешно завершен. Никаких других действий по лицензированию установленного продукта производить не требуется.

Запустите **Платформу nanoCAD**.

Сервер лицензий

Установка сервера лицензий Нанософт из репозитория

Примечание.

В случае если ранее платформа **NanoCAD** была автоматически установлена с помощью скрипта согласно пункту «Установка Платформы nanoCAD из репозитория» данный шаг следует пропустить.

Предварительно необходимо подключить репозиторий при помощи скрипта:

```
sudo wget -qO- https://repo.nanodev.ru/r24.1/get_ncad.sh | sudo bash
```

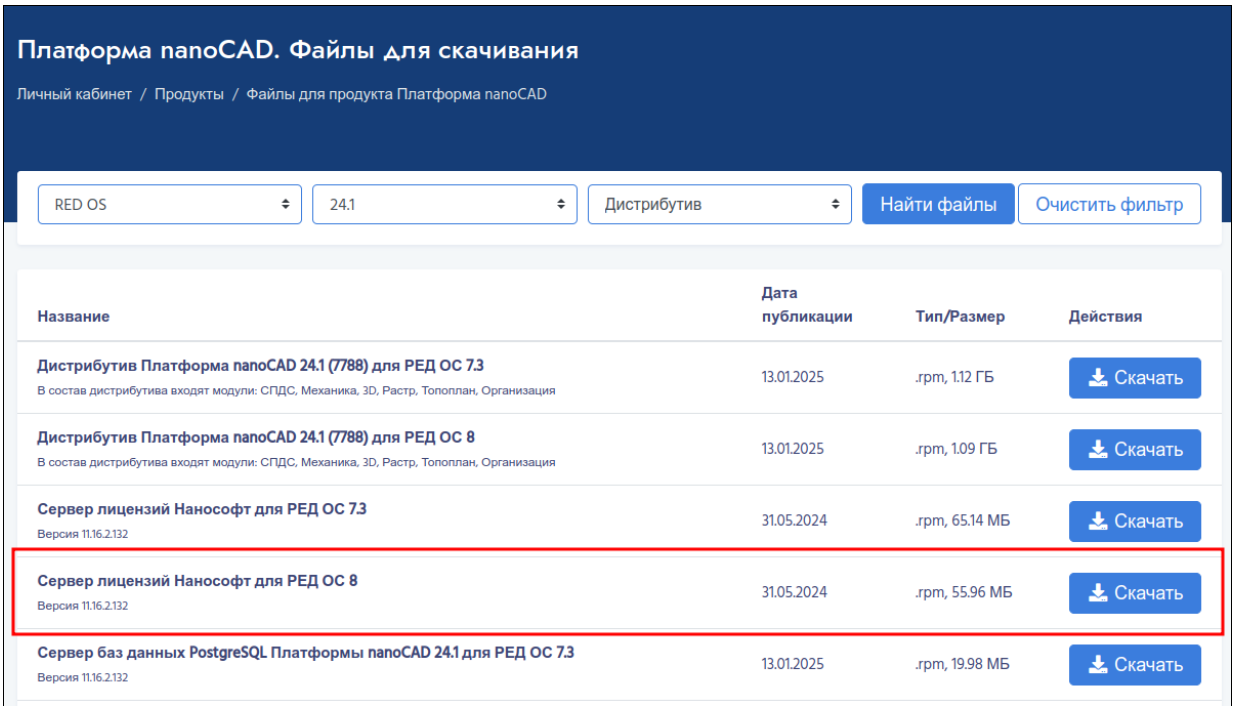
Выполните установку сервера лицензий Нанософт:

```
sudo dnf check-update
sudo dnf install ncad-licsrv
```

Установка сервера лицензий Нанософт из установочного пакета

Для загрузки инсталляционных пакетов перейдите по ссылке. На странице задайте фильтр для списка доступных дистрибутивов:

- выберите ОС – **RED OS**;
- выберите версию продукта – **24.1**;
- выберите тип файлов – **дистрибутив**.



Загрузите **Сервер лицензий Нанософт для РЕД ОС 8**, нажав «**Скачать**». Затем перейдите в каталог со скачанным файлом – «**Загрузки**» (по умолчанию).

Для установки **Сервера лицензий** выберите инсталляционный пакет **ncad-licsrv.rpm** и запустите его выполнение двойным кликом ЛКМ. В открывшемся окне **Аутентификация** введите пароль администратора. Нажмите **Аутентификация**.

В открывшемся окне **Результат транзакции** будет выведен список устанавливаемых пакетов, нажмите **Хорошо** для продолжения установки.

По окончании установки нажмите **Выход**.

Активация сетевой лицензии оффлайн при помощи файла сетевой лицензии

Примечание.

Если служба лицензирования уже запущена, перед добавлением лицензии остановите службу следующей командой (потребуются права **администратора** системы):

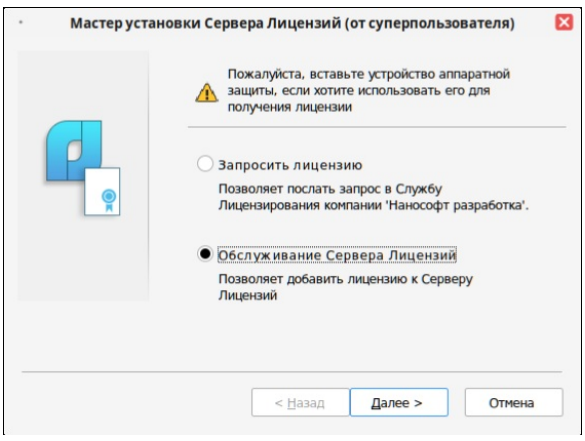
```
sudo systemctl stop ncad-licsrv
```

Если это первый запуск **Мастера установки Сервера лицензий**, пропустите данное предупреждение.

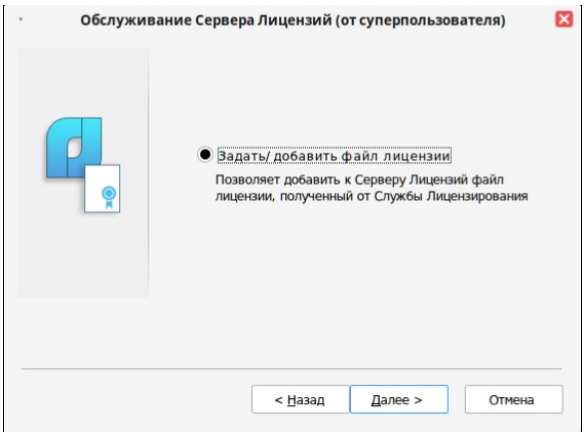
Откройте терминал и запустите **Мастер установки Сервера Лицензий** с правами **администратора** системы:

```
sudo ncad-licreq
```

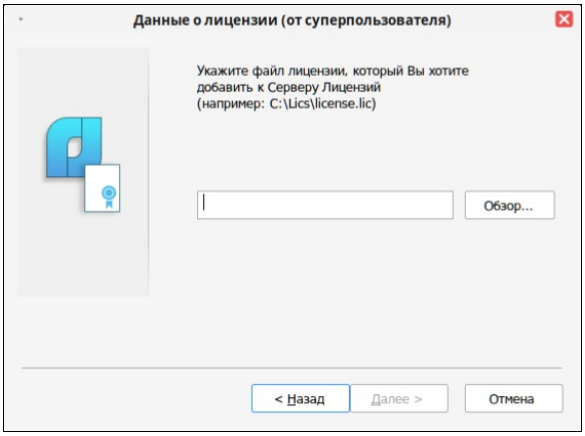
В открывшемся окне выберите «**Обслуживание Сервера Лицензий**». Нажмите **Далее**.



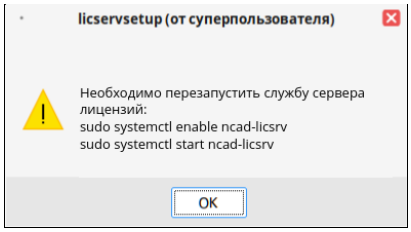
В следующем окне выберите «**Задать/добавить файл лицензии**» и нажмите **Далее**.



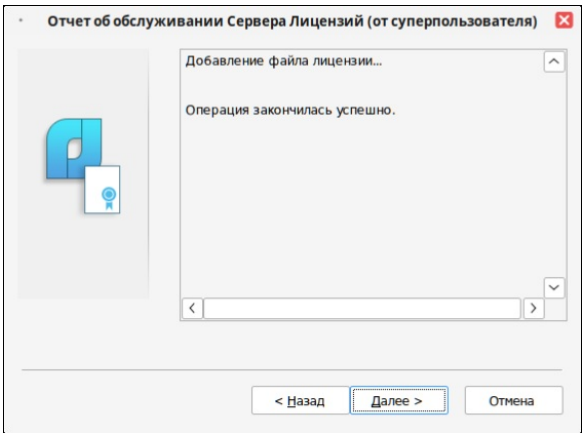
Укажите путь к файлу лицензии с расширением **.lic**, нажав «**Обзор...**». Затем нажмите **Далее**.



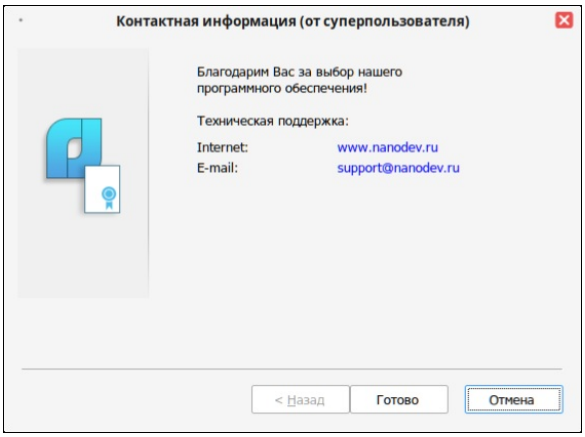
После добавления файла лицензии будет отображено информационное окно с командой запуска службы лицензирования. Нажмите **OK**.



В случае успешного добавления файла лицензии в окне **Отчета об обслуживании Сервера Лицензий** отображается информация об успешном окончании операции. Нажмите Далее.



В окне «**Контактная информация**» нажмите **Готово**.



Откройте терминал и запустите службу лицензирования с правами суперпользователя:

```
systemctl start ncad-licsrv
```

Проверьте работу службы лицензирования командой:

```
systemctl status ncad-licsrv
```

В случае если все шаги по установке и настройке были выполнены верно, в статусе службы лицензирования будет отображаться **active (running)**.

Запрос и активация сетевой лицензии онлайн

Примечание.

Если служба лицензирования уже запущена, перед добавлением лицензии остановите службу следующей командой (потребуются права администратора системы):

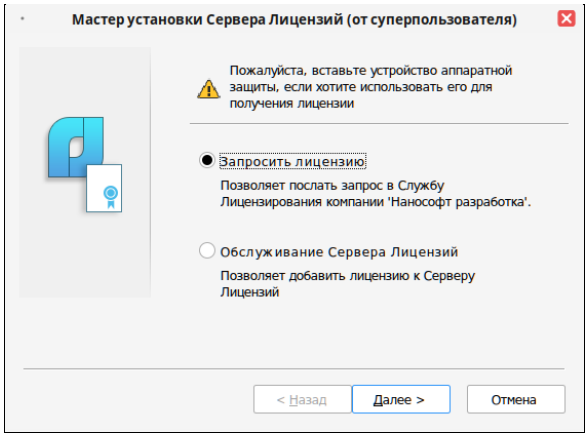
```
sudo systemctl stop ncad-licsrv
```

Если это первый запуск **Мастера установки Сервера лицензий**, пропустите данное предупреждение.

Откройте терминал и запустите **Мастер установки Сервера Лицензий** с правами администратора системы:

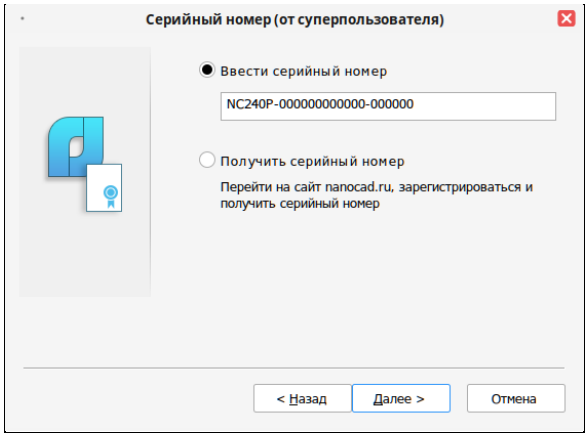
```
sudo ncad-licreq
```

После запуска **Мастера установки Сервера Лицензий** выберите «**Запросить лицензию**» и нажмите **Далее**.



В открывшемся окне «**Серийный номер**» введите серийный номер (если у вас нет серийного номера, выберите пункт « **Получить серийный номер**»). Серийный номер имеет вид *NC240P-000000000000-000000*.

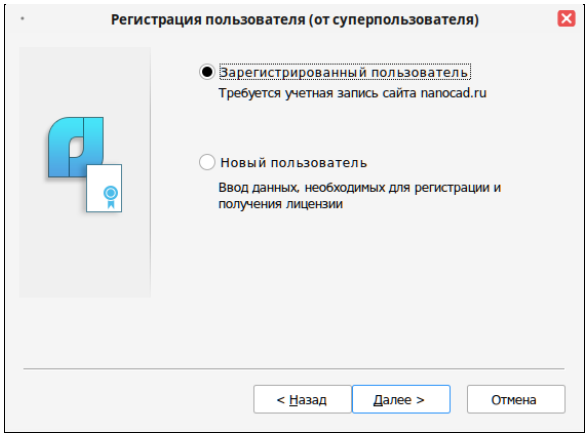
Нажмите **Далее**.



Будет открыто окно «**Регистрация пользователя**».

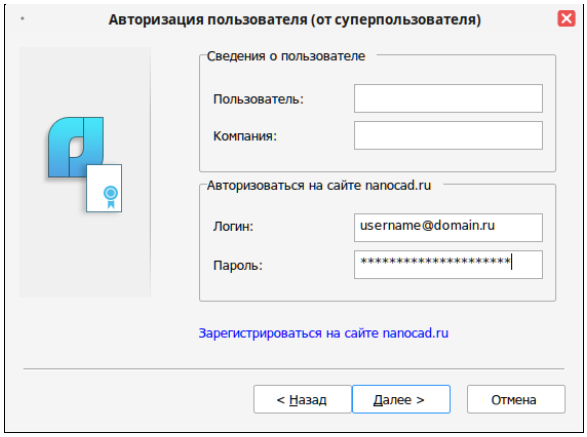
Если у вас уже есть учетная запись в личном кабинете на сайте https://lk.nanocad.ru, выберите пункт **Зарегистрированный пользователь**.

В противном случае выберите пункт «**Новый пользователь**». Сервер лицензий позволяет зарегистрироваться в качестве нового пользователя.



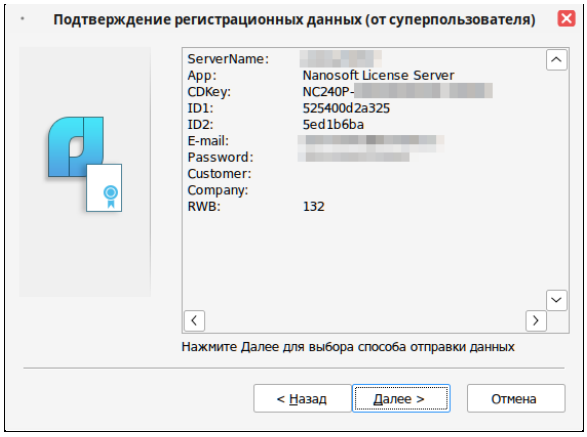
В окне «**Авторизация пользователя**» поля **Логин** и **Пароль** следует заполнять теми значениями, которые были использованы при регистрации в личном кабинете на сайте https://lk.nanocad.ru.

Если вы не зарегистрированы в личном кабинете на сайте https://lk.nanocad.ru, нажмите на ссылку **Зарегистрироваться на сайте www.nanodev.ru**. После регистрации введите ваши регистрационные данные в полях **Логин** и **Пароль**.



Опционально можно заполнить поля **Пользователь** и **Компания**. Нажмите **Далее**.

В окне подтверждения регистрационных данных отображаются данные, которые будут отправлены в **ООО «Нанософт разработка»** для получения сетевой лицензии.

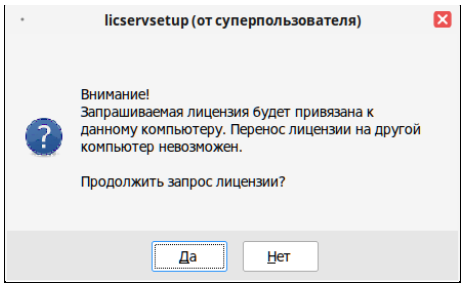


Проверьте введенные данные и подтвердите их нажатием кнопки **Далее**. В случае обнаружения ошибки нажмите **Назад** и исправьте информацию в тех полях, где это необходимо.

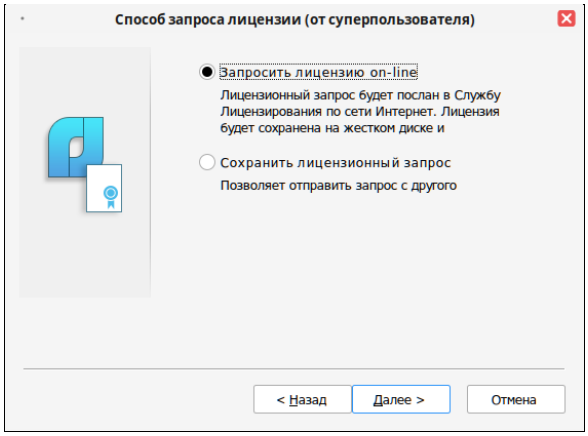
ВАЖНО!

Внимательно проверяйте указанные регистрационные данные. При неверном заполнении регистрационных полей разработчик программного обеспечения **ООО «Нанософт разработка»** может отказать в выдаче лицензии.

Подтвердите привязку лицензии к серверу, нажав **Да** в появившемся запросе **Мастера установки Сервера Лицензий**.

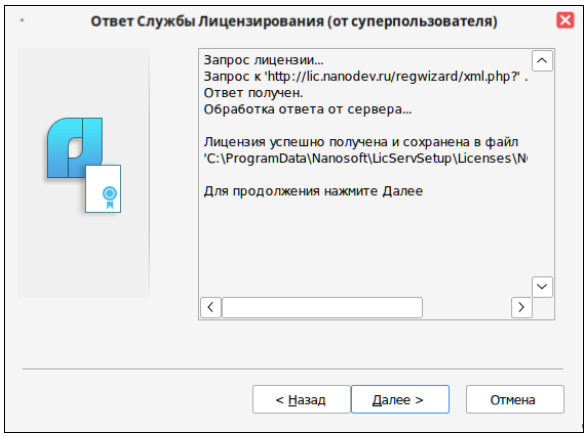


После подтверждения запроса лицензии будет открыто окно «**Способ запроса лицензии**».



Запрос лицензии онлайн производится только с компьютера, имеющего выход в сеть Интернет.

При запросе лицензии онлайн **Мастер установки Сервера Лицензий** автоматически соединится с **Сервером лицензий**, сохранит и активирует лицензию.



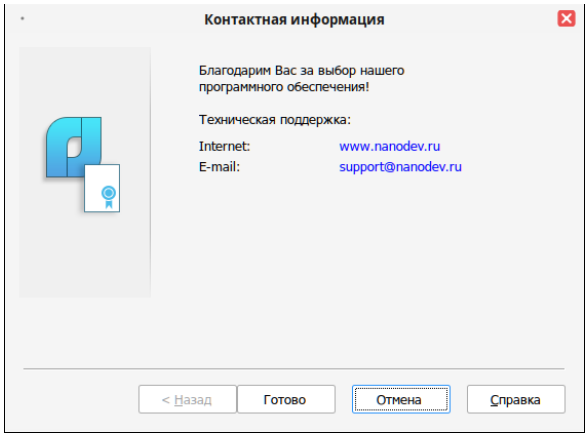
Примечание.

Все файлы лицензий, полученные таким способом, помещаются в директорию **/opt/nanosoft/licsrv/xnhome/drive_c/ProgramData/Nanosoft/LicServSetup/Licenses/**.

Результатом запроса лицензии онлайн может быть:

- успешное получение лицензии;
- отказ в выдаче лицензии;
- неудачное соединение.

В случае успешного завершения нажмите **Далее** и в следующем окне, содержащем контактную информацию, нажмите **Готово**.



Откройте терминал и запустите службу лицензирования с правами **суперпользователя**:

```
systemctl restart ncad-licsrv
```

Проверьте статус службы лицензирования командой:

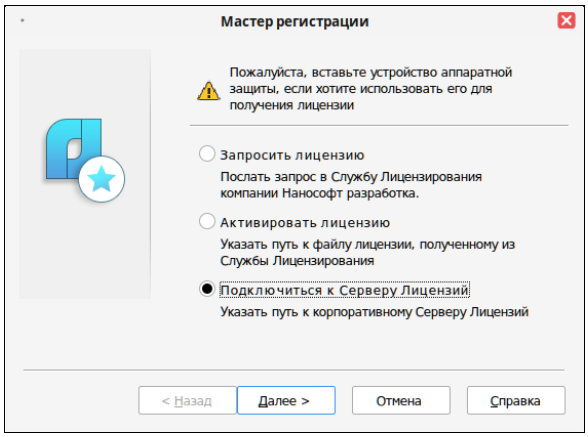
```
systemctl status ncad-licsrv
```

В случае если все шаги по установке и настройке были выполнены верно, в статусе службы лицензирования будет отображаться **active (running)**.

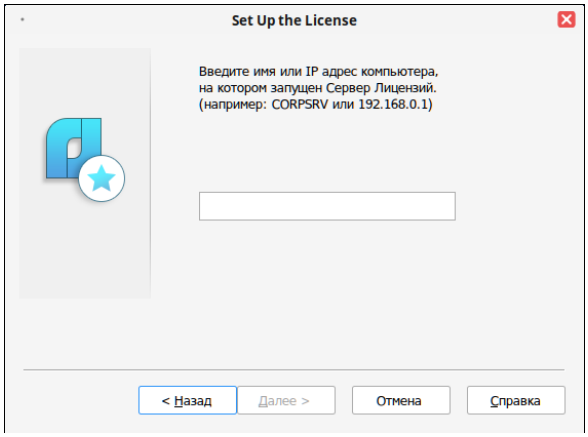
Подключение к серверу лицензий

Для подключения к **Серверу лицензий** с целью активации программного обеспечения *NanoCAD* запустите **Мастер регистрации** из «**Главного меню**» – «**nanocad 24.1**».

В открывшемся окне **Мастера регистрации** программного обеспечения выберите пункт «**Подключиться к серверу лицензий**» и нажмите **Далее**.

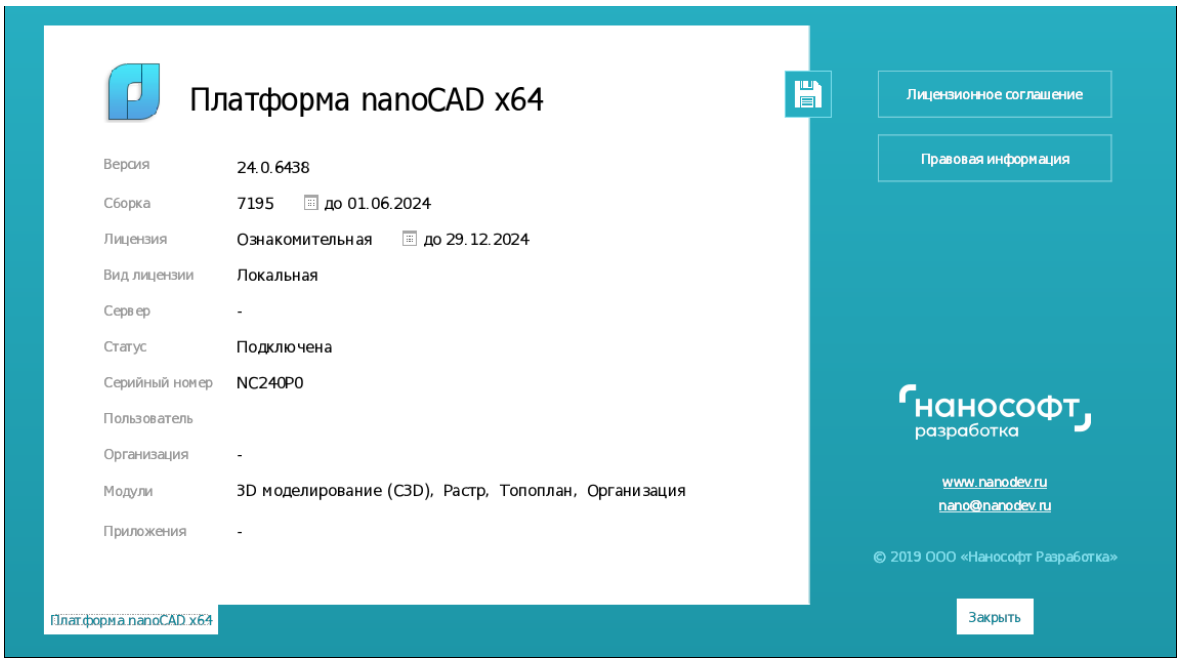


На следующем шаге введите IP-адрес компьютера, на котором установлен **Сервер лицензий** (например, *192.168.0.1*), или укажите NetBIOS-имя машины (например, *CORPSRV*). Если для подключений используются нестандартные порты, укажите запись следующего вида `<порт>@<имя_сервера>` (например, *270010@CORPSRV*).



Состояние лицензии

Уточнить информацию о состоянии имеющейся лицензии можно в меню «**Справка**» – «**О программе**».



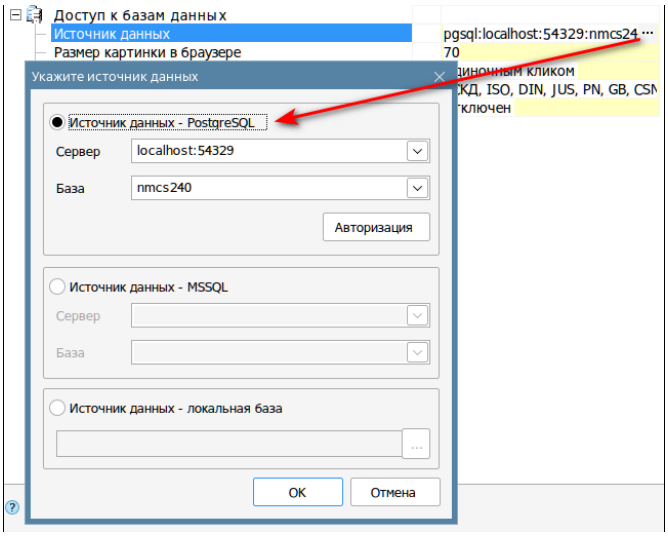
Проверка подключения к локальным базам данных PostgreSQL СПДС и Механика

Для проверки подключения запустите модуль из «**Главного меню**» – «**nanoCAD 24.1**» – «**Механика 24.1**».

В командной строке выполните:

```
params
```

Перейдите в раздел **Источник данных** и настройте локальную БД.



где:

- localhost:54329 – сервер БД:
  - localhost – имя сервера (в примере – локальный сервер);
  - 54329 – номер порта, на котором работает БД;
- имя БД:
  - nmcs240 – имя БД (для модуля Механика);
  - nspds240 – имя БД (для модуля СПДС).

Для авторизации используются следующие данные:

- логин – mclogin;
- пароль – mclogin.

Проверьте доступность порта 54329, т. к. **postgresql** работает на порту 54329:

```
ss -tulpn | grep 54329

tcp   LISTEN   0  244  127.0.0.1:54329   0.0.0.0:*
tcp   LISTEN   0  244      [::1]:54329      [::]:*
```

Для проверки статуса службы БД PostgreSQL выполните:

```
systemctl status ncad-pgsql
```

В статусе должно отображаться **active (running)**.

Установка Сервера лицензий в РЕД ОС конфигурации Сервер минимальный

Предварительная подготовка

1. Убедитесь, что на клиенте используется X11-сервер (*Wayland* или *Xorg*), выполнив команду:

```
echo $XDG_SESSION_TYPE
```

2. На сервере установите и настройте SSH-сервер. Подробную информацию об установке и настройке см. в нашей статье «Работа с клиентом и сервером SSH».

3. На сервере установите **xauth** (потребуются права **администратора**):

```
sudo dnf install xorg-x11-xauth
```

4. На сервере в файле **/etc/ssh/sshd_config** должен быть активен параметр для включения туннелирования X11 при аутентификации – X11Forwarding. Подробную информацию о параметрах конфигурационного файла **/etc/ssh/sshd_config** см. в нашей статье «Конфигурационный файл SSHD_CONFIG».

5. Пользователь, для которого настраивается аутентификация, должен быть включен в группу **wheel** (*sudoers*):

```
usermod -a -G wheel <имя_пользователя>
```

Подключение к серверу

Примечание.

Нижеприведенные действия необходимо выполнять при каждом подключении к серверу.

1. Выполните переподключение к серверу с помощью команды вида:

```
ssh -Y <имя_пользователя>@<IP-адрес_сервера>
```

2. Получите данные авторизации дисплея **X11**:

```
xauth list $DISPLAY
```

3. Авторизуйте дисплей для сессии пользователя:

```
sudo xauth add <вывод_предыдущей_команды>
```

Установка и настройка Сервера лицензий Нанософт

Предварительно загрузите на сервер файл дистрибутива **Сервера лицензий** командой:

```
wget https://download.nanodev.ru/products/nanocad_platform/24.1/ncad-licsrv-11.16.2.132-51+1735141935.red80.x86_64.rpm
```

Для установки Сервера лицензий Нанософт выполните команду (команда выполняется после подключения к серверу по **SSH** с правами **администратора** системы):

```
sudo dnf install ./ncad-licsrv-11.16.2.132-51+1735141935.red80.x86_64.rpm
```

Примечание.

Если служба лицензирования уже запущена, перед добавлением лицензии остановите службу следующей командой (потребуются права **администратора** системы):

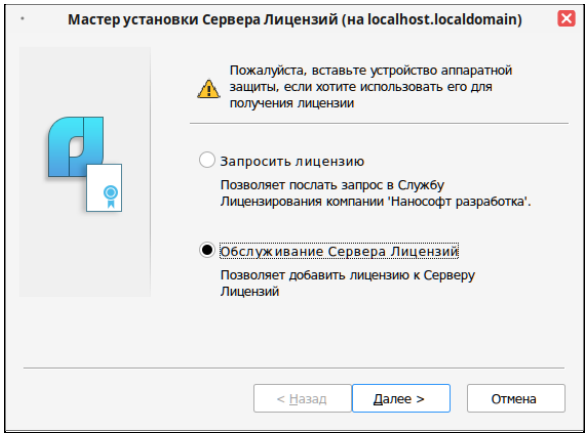
```
sudo systemctl stop ncad-licsrv
```

Если это первый запуск **Мастера установки Сервера лицензий**, пропустите данное предупреждение.

Затем запустите **Мастер установки Сервера Лицензий** с правами **администратора** системы:

```
sudo ncad-licreq
```

Будет открыто окно мастера установки Сервера лицензий:



Дальнейшая настройка и управление **Сервером лицензий** Нанософт осуществляется согласно описанным в разделе «Сервер лицензий» процедурам.

Установка баз данных PostgreSQL СПДС и Механика на сервер

Настройка сервера

На сервере выполните установку **базы данных (БД) модулей Механика и СПДС**, предварительно загрузив пакет с официального сайта разработчика:

```
wget https://download.nanodev.ru/products/nanocad_platform/24.1/ncad-pgsql-12.18-25+1729178738.red80.x86_64.rpm
```

```
sudo dnf install ./ncad-pgsql-12.18-25+1729178738.red80.x86_64.rpm
```

Для настройки подключения **к серверу PostgreSQL** необходимо выполнить следующий алгоритм действий:

1. Разрешить удаленные подключения к серверу. Для этого откройте файл **pg_hba.conf**:

```
sudo nano /opt/nanosoft/postgresql/ncad-database/ncad-data/pg_hba.conf
```

и добавьте в него строку:

```
host all all 0.0.0.0/0 trust
```

2. Разрешить прослушивание запросов на всех IP-адресах (*). Для этого откройте файл **postgresql.conf**:

```
sudo nano /opt/nanosoft/postgresql/ncad-database/ncad-data/postgresql.conf
```

и добавьте в него строку:

```
listen_addresses = '*'
```

3. Для применения настроек перезапустить службу **ncad-pgsql**:

```
sudo systemctl restart ncad-pgsql
```

4. Проверьте статус службы **ncad-pgsql**:

```
sudo systemctl status ncad-pgsql
```

В статусе должно отображаться **active (running)**.

5. Проверить доступность порта 54329, т. к. **postgresql** работает на порту 54329:

```
ss -tulpn | grep 54329

tcp   LISTEN   0  244  127.0.0.1:54329   0.0.0.0:*
tcp   LISTEN   0  244      [::1]:54329      [::]:*
```

Настройка клиента

На клиенте запустите модуль **Механика** из «**Главного меню**» – «**nanoCAD 24.1**».

Перейдите в пункт меню **Механика** – **Настройки** или выполните в командной строке:

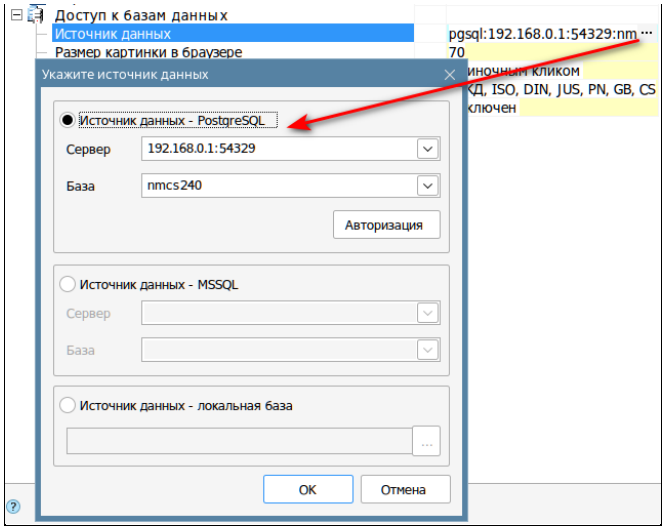
```
mcparams
```

На вкладке «**Главное настройки**» раскройте список «**Доступ к базам данных**» и выберите **Источник данных**.

В разделе **Источник данных** — **PostgreSQL** укажите сервер в формате `<IP-адрес_сервера>:<порт>` и имя базы:

- `nmcs240` – имя БД (для модуля Механика);
- `nspds240` – имя БД (для модуля СПДС).

Для сохранения настроек нажмите **OK**.



Дополнительная информация

В случае возникновения дополнительных вопросов по настройке платформы **NanoCAD** рекомендуется обращаться к официальной документации разработчика продукта, задав на странице загрузок фильтр:

- выберите ОС – **RED OS**;
- выберите версию продукта – **24.1**;
- выберите тип файлов – **инструкции**.

КОМПАС-3D

Установка WINE@Etersoft
Установка КОМПАС-3D

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** KOMPAS-3D_v21

КОМПАС-3D – это российская импортонезависимая система трехмерного проектирования.

КОМПАС-3D широко используется для проектирования изделий основного и вспомогательного производств в таких отраслях промышленности, как машиностроение (транспортное, сельскохозяйственное, энергетическое, нефтегазовое, химическое и т.д.), приборостроение, авиастроение, судостроение, станкостроение, вагоностроение, металлургия, промышленное и гражданское строительство, товары народного потребления и т. д.

В настоящее время использование *КОМПАС-3D* возможно в связке с приложением **WINE@Etersoft** от компании Этерсофт. Данный программный продукт обеспечивает полную поддержку работы *КОМПАС-3D* в РЕД ОС.

Вы можете подробнее ознакомиться с настройкой и работой **КОМПАС-3D**, просмотрев наши обучающие видео:

- на **RuTube** — Установка КОМПАС-3D в РЕД ОС 7.3;
- в **Яндекс.Дзен** — Установка КОМПАС-3D в РЕД ОС 7.3;
- в **VK Видео** — Установка КОМПАС-3D в РЕД ОС 7.3.

На наших каналах вы также сможете найти много другой полезной информации.

Установка WINE@Etersoft

Программный продукт *WINE@Etersoft* позволяет использовать Windows-приложения в операционных системах семейства GNU/Linux.

Продукт *WINE@Etersoft* основан на коде свободного проекта **Wine**. Компания *Etersoft* занимается доработкой *Wine*, чтобы обеспечить полноценную работу в Linux наиболее востребованных в России приложений для бизнеса.

Для установки *WINE@Etersoft* необходимо запросить дистрибутив с официального сайта разработчика. Продукт представлен в двух версиях — **Enterprise** (для корпоративных клиентов) и **Local** (для частного использования).

После запроса продукта на электронную почту будет отправлено письмо с указанием индивидуальных ссылок для скачивания установочных пакетов. Найдите ссылку для скачивания скрипта установки **wine-etersoft-install.sh** и загрузите его на компьютер.

После загрузки откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

Перейдите в каталог со скачанным скриптом установки (в примере **/home/user/Загрузки/**) программы и запустите установку:

```
cd /home/user/Загрузки/
bash wine-etersoft-install.sh
```

Скрипт автоматически установит все необходимые для работы пакеты.

После установки *WINE@Etersoft* выйдите из сеанса суперпользователя:

```
exit
```

Установка КОМПАС-3D

Для установки *КОМПАС-3D* необходимо запросить дистрибутив на официальном сайте разработчика. Для ознакомления с программным обеспечением доступно использование бесплатной пробной версии, работающей без ограничения функционала в течение 30 дней.

После запроса продукта на электронную почту будет отправлено письмо с указанием индивидуальной ссылки для скачивания архива.

После загрузки архива распакуйте его командой в терминале (в примере **/home/user/Загрузки/**):

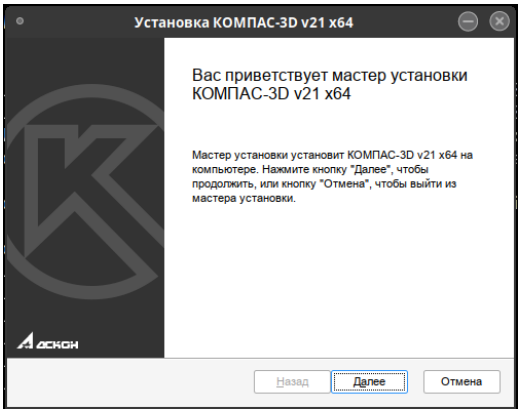
```
unzip -d /home/user/Загрузки/KOMPAS-3D_v21_x64.zip
```

Когда архив будет распакован, перейдите в каталог с дистрибутивом *КОМПАС-3D* и выполните команду (с правами **локального пользователя**):

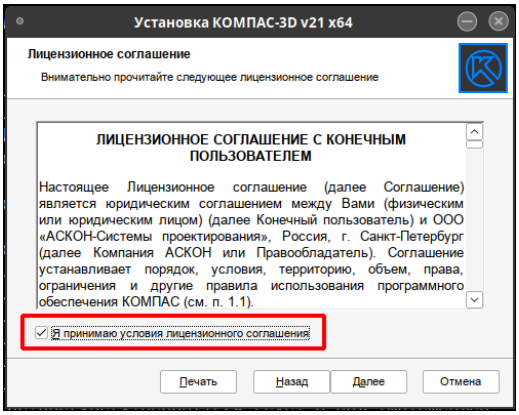
```
cd /home/user/Загрузки/KOMPAS-3D_v21_x64
wine_install_kompas
```

Будет запущен скрипт подготовки окружения для работы ПО, а затем мастер установки.

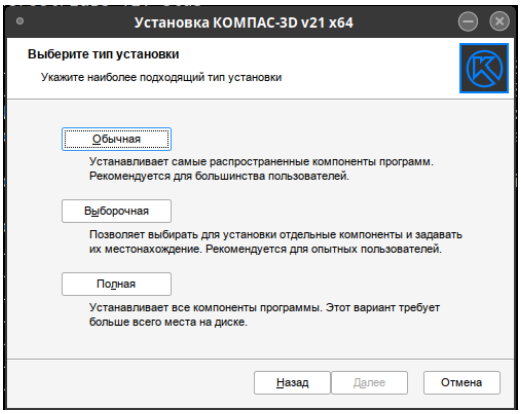
В приветственном окне нажмите «**Далее**».



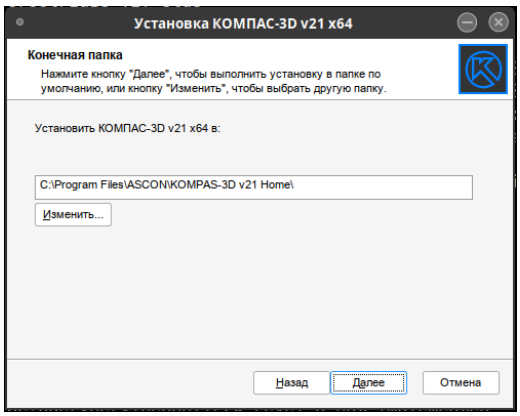
Ознакомьтесь и примите условия лицензионного соглашения, нажмите «**Далее**».



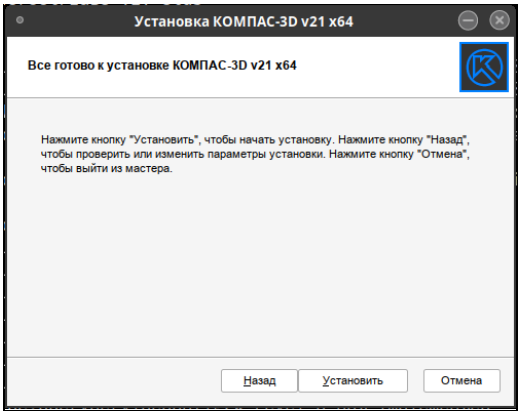
Выберите тип установки.



Выберите папку для установки программы (в примере оставлена папка по умолчанию), нажмите «**Далее**».

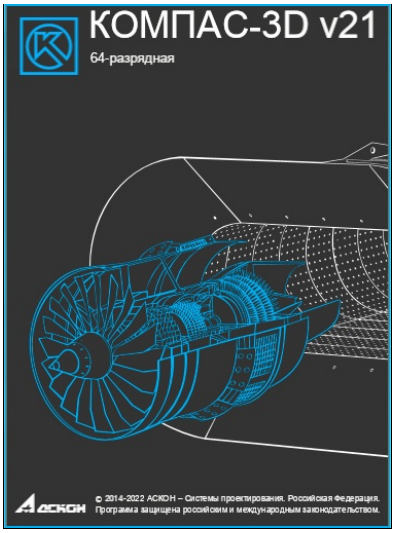


Подтвердите начало установки, нажав кнопку «**Установить**».

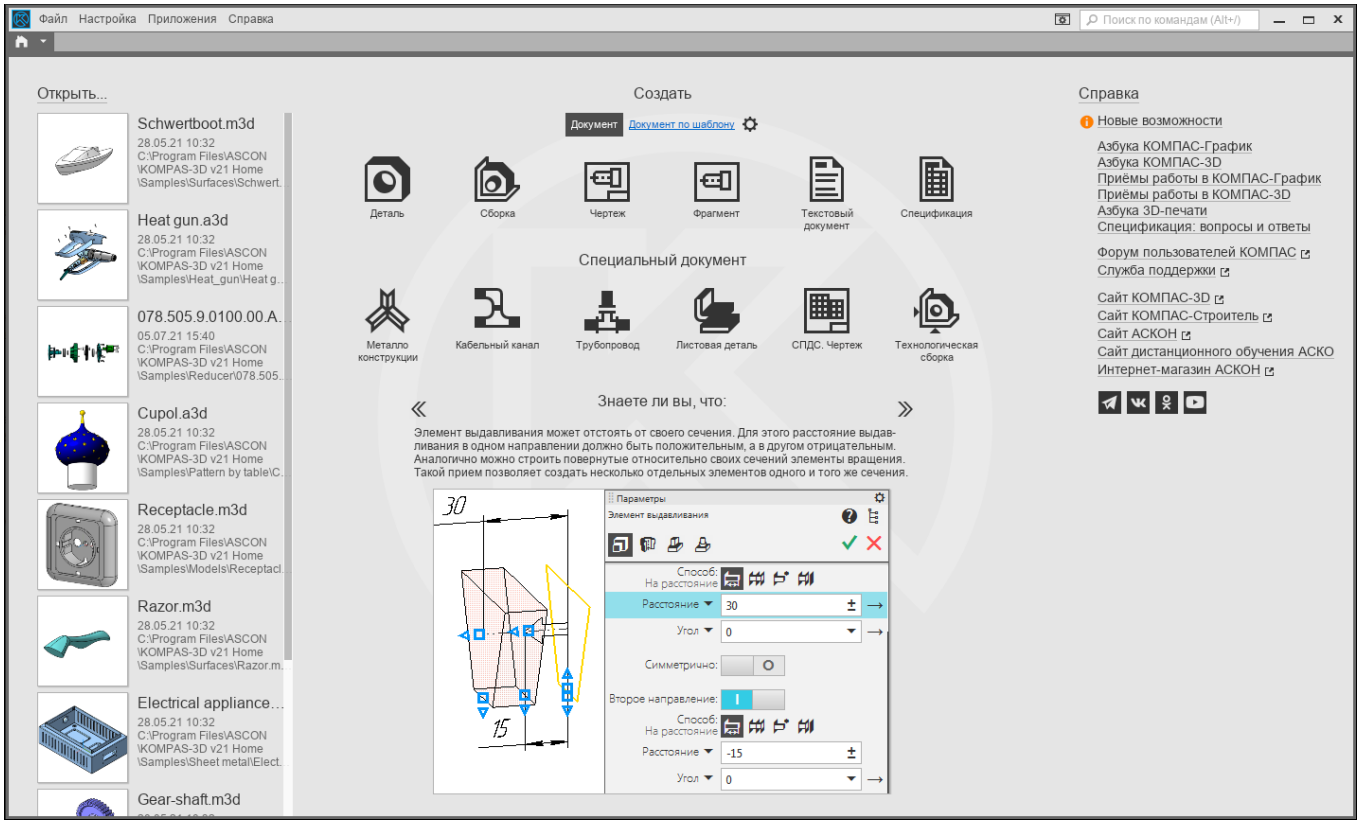


После установки ПО будет доступно из «**Главного меню**» - «**Wine**» - «**КОМПАС-3D v21**», а также появится ярлык на **Рабочем столе**.

Запуск программы выглядит следующим образом:



Главное окно программы выглядит следующим образом:


Файл Настройка Приложения Справка
Поиск по командам (Alt+/)
Открыть...
Schwertboot.m3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Surfaces\Schwert...
Heat gun.a3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Heat_gun\Heat g...
078.505.9.0100.00.A...
05.07.21 15:40
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Reducer\078.505...
Cupol.a3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Pattern by table\C...
Receptacle.m3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Models\Receptacl...
Razor.m3d
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Surfaces\Razor.m...
Electrical appliance...
28.05.21 10:32
C:\Program Files\ASCON\KOMPAS-3D v21 Home\Samples\Sheet metal\Elect...
Gear-shaft.m3d
Создать
Документ
Документ по шаблону
Деталь
Сборка
Чертеж
Фрагмент
Текстовый документ
Спецификация
Специальный документ
Металло конструкции
Кабельный канал
Трубопровод
Листовая деталь
СПДС. Чертеж
Технологическая сборка
Знаете ли вы, что:
Элемент выдавливания может отстоять от своего сечения. Для этого расстояние выдавливания в одном направлении должно быть положительным, а в другом отрицательным. Аналогично можно строить повернутые относительно своих сечений элементы вращения. Такой прием позволяет создать несколько отдельных элементов одного и того же сечения.
30
15
Параметры
Элемент выдавливания
Способ:
На расстояние
Расстояние
30
Угол
0
Симметрично:
Второе направление:
Способ:
На расстояние
Расстояние
-15
Угол
0
Справка
Новые возможности
Азбука КОМПАС-График
Азбука КОМПАС-3D
Приёмы работы в КОМПАС-График
Приёмы работы в КОМПАС-3D
Азбука 3D-печати
Спецификация: вопросы и ответы
Форум пользователей КОМПАС
Служба поддержки
Сайт КОМПАС-3D
Сайт КОМПАС-Строитель
Сайт АСКОН
Сайт дистанционного обучения АСКО
Интернет-магазин АСКОН

Marble — виртуальный глобус

Основные функции
Установка
Описание программы
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: marble-22.12.2-1

Marble — это удобное программное обеспечение, представляющее виртуальный глобус, который позволяет масштабировать карту и исследовать Землю или Луну с разных позиций.

Marble предлагает огромное количество возможностей для исследования различных географических объектов, таких как горы, реки, океаны и т.д. Также пользователи могут путешествовать по различным планетам, изучая их поверхность и географию.

Основные функции

Основные функции **marble** включают:

1. **Просмотр карт —** marble предоставляет возможность просмотра и исследования различных видов карт, включая физическую карту, политическую карту, облачную карту и другие;

2. **Интерактивность** — пользователи могут вращать глобус, изменять масштаб и перемещаться по карте, что делает процесс обучения более интересным и наглядным;

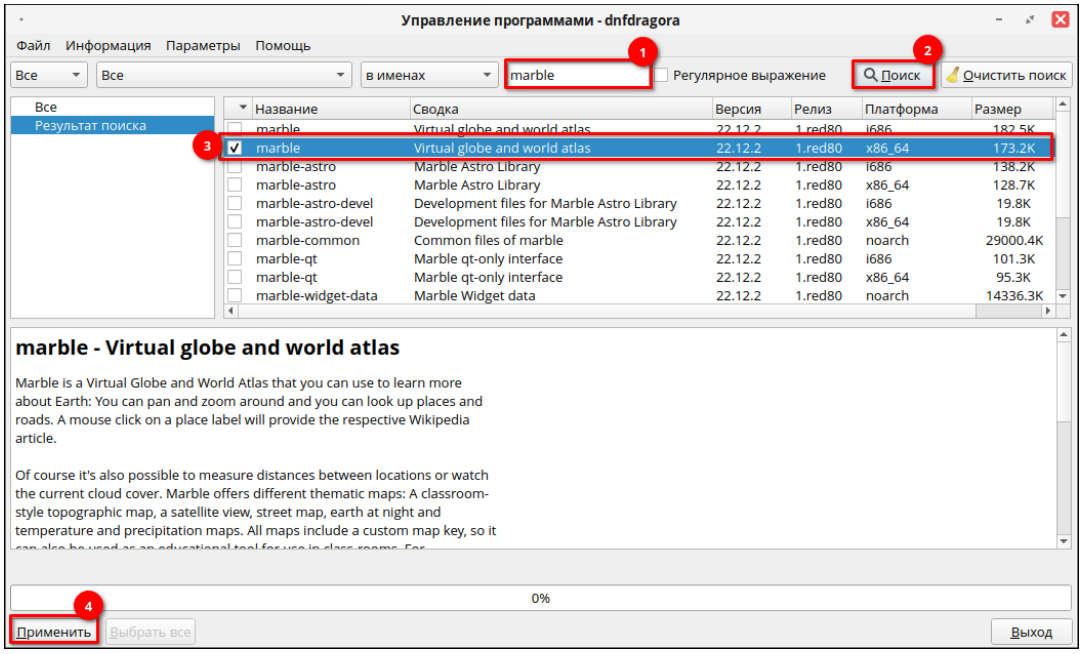
3 . **3D-моделирование —** marble использует технологию 3D-моделирования для создания высококачественных изображений поверхности планет, спутников и других небесных объектов;

4. **Информацию о географических объектах —** marble предлагает подробную информацию о различных географических объектах, таких как горы, океаны, реки, столицы и многое другое.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**marble**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



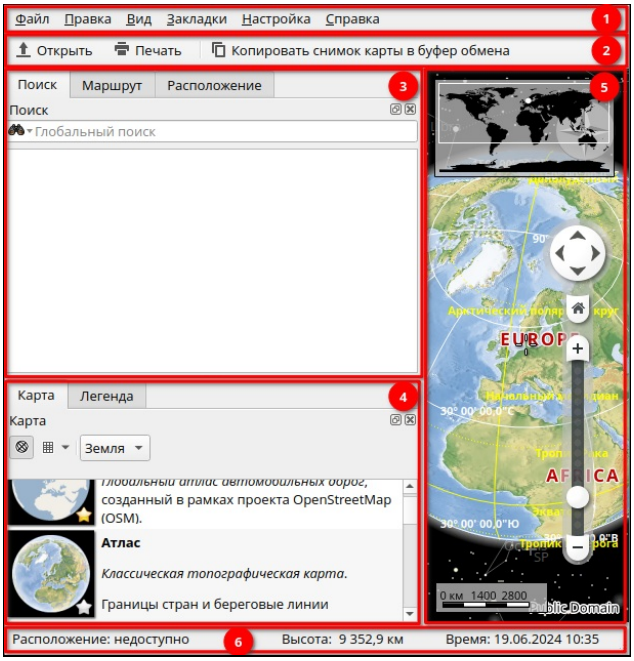
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install marble
```

После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**KDE Marble**».

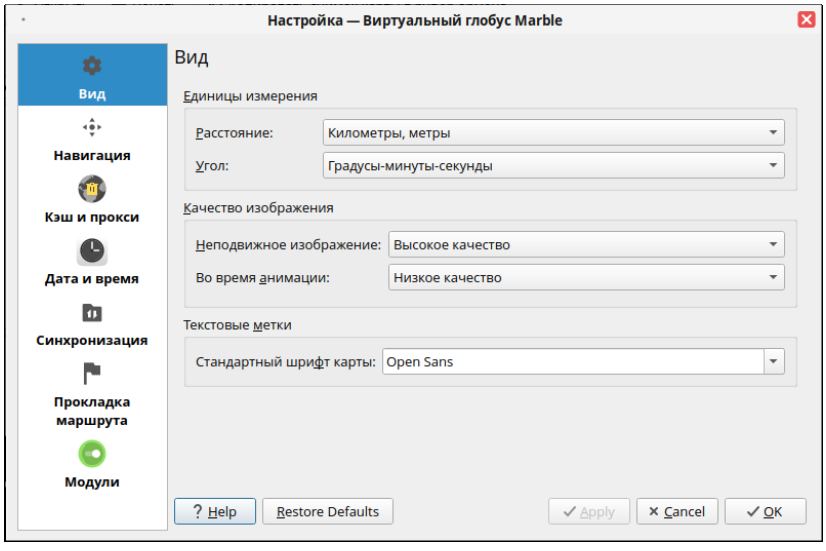
Описание программы

Интерфейс программы стандартный и состоит из нескольких типовых частей.



1. **Основное меню программы.** Позволяет выполнять различные действия с картой, а также настраивать как саму программу, так и панель инструментов.

Одним из наиболее важных пунктов является «**Настройка**» — «**Настроить Виртуальный глобус Marble...**», который позволяет настраивать внешний вид глобуса и его основные параметры, чтобы оптимизировать визуализацию и функциональность глобуса.

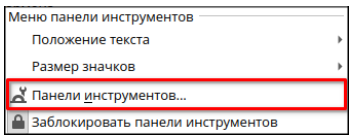


В пункте меню «**Справка**» — «**Руководство пользователя Виртуальный глобус Marble**» можно ознакомиться с более подробной пользовательской инструкцией.

2. **Основная панель инструментов.** Это панель инструментов с кнопками быстрого доступа к основным возможностям программы. Содержит кнопки справочной информации о программе, открытия файла, печати, копирования снимка, выбора языка.



Кнопки можно скрывать и отображать через контекстное меню, щёлкнув ПКМ по области панели и выбрав пункт «**Панели инструментов...**»



3. **Панель поиска.** Позволяет искать места и объекты на выбранной карте.

4. **Панель выбора карты.** Даёт возможность выбирать различные карты. По умолчанию marble предлагает 15 вариантов просмотра:

- атлас;
- OpenStreetMap;
- вид со спутника;
- Земля ночью;
- глобус Бехайма 1492 года;
- спутниковая карта Sentinel-2;
- историческая карта 1689 года;
- политическая карта;
- обычная карта;
- осадки в декабре;
- осадки в июле;
- температура в декабре;
- температура в июле;
- векторная карта OSM;
- Луна.

Также есть возможность создать новую карту и загрузить карту.

5. **Основное рабочее поле.** Основная область интерфейса, где отображается карта или глобус.

Для лучшей ориентации в левом нижнем углу рабочего поля находится масштабная линейка.



В правом верхнем углу рабочего поля находится компас.



Для навигации и управления видом возможно использовать инструменты панели навигации в правой части рабочего поля.



Используйте стрелки вправо и влево для вращения Земли вокруг оси и стрелки вверх и вниз для наклона оси Земли назад или вперёд.

Масштабирование производится перемещением ползунка вверх и вниз. В зависимости от масштаба будут отображаться различные детали.

Для возврата к первоначальным настройкам нажмите на значок  .

6. **Строка состояния.** Отображается информация о расположении, высоте, текущем уровне масштаба тайлов, индикатор выполнения загрузки данных карт. Щелчок ПКМ по строке состояния открывает контекстное меню, в котором возможно изменить её внешний вид.

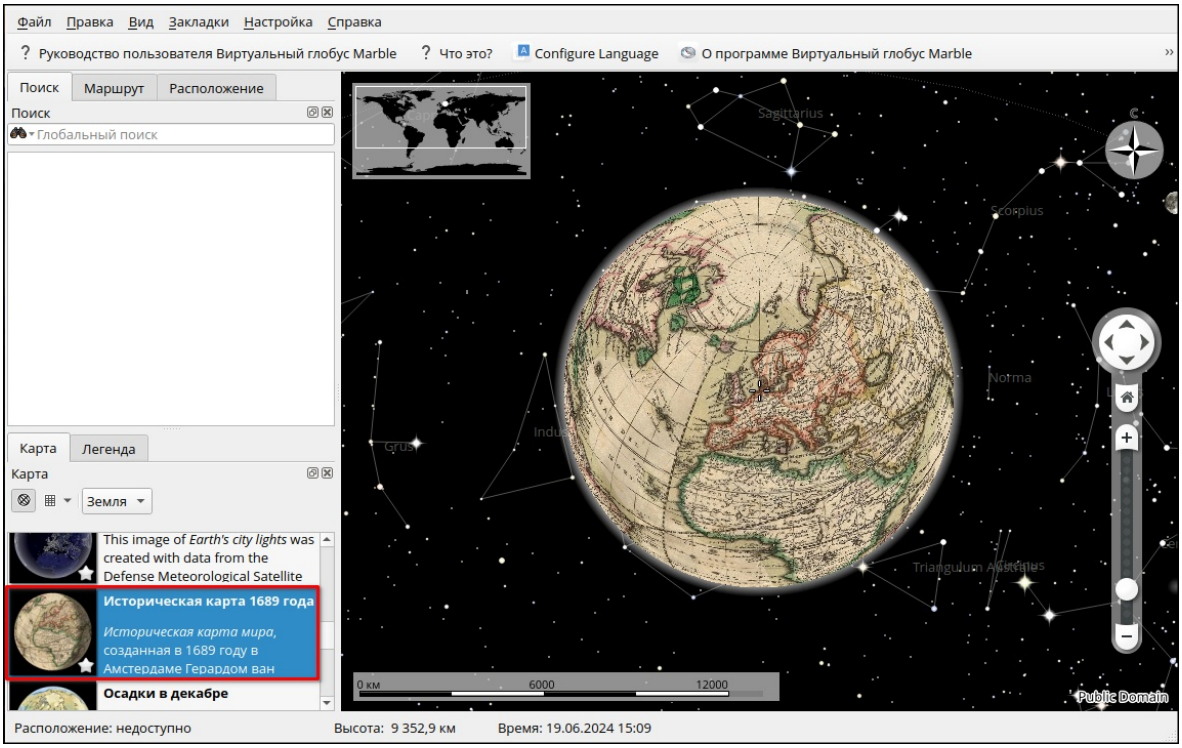
Пример работы

Для поиска информации о географическом объекте воспользуйтесь следующим алгоритмом действий:

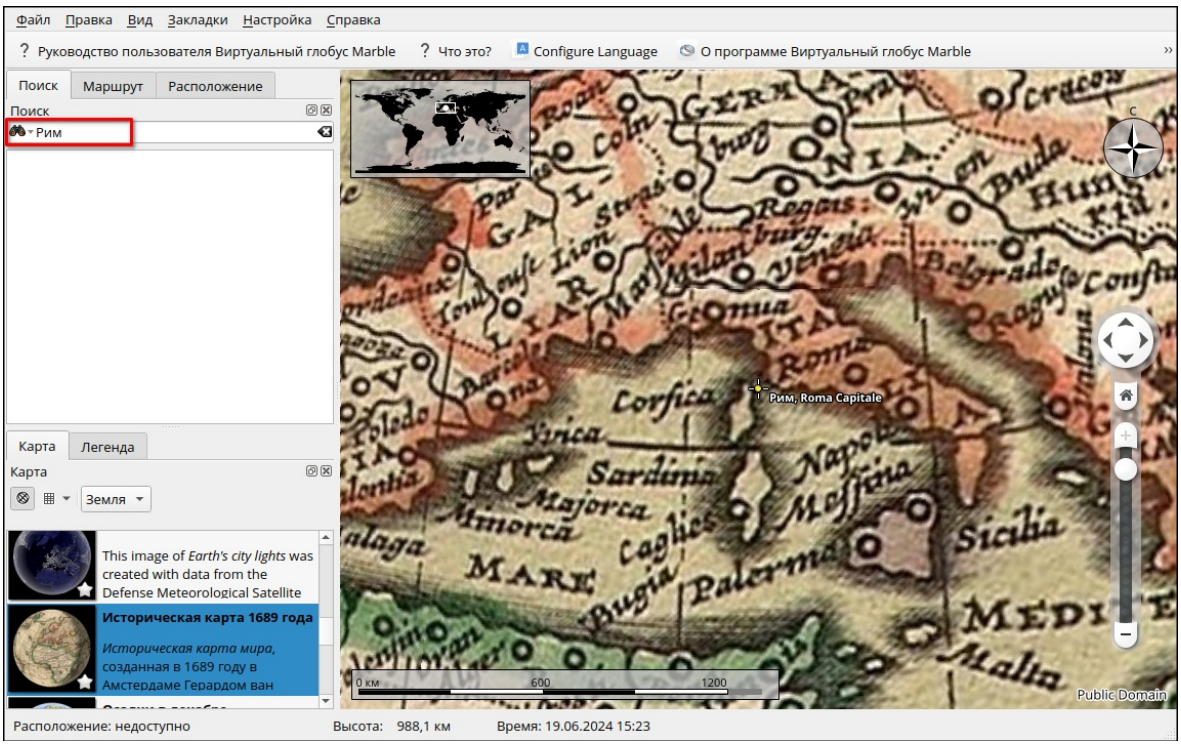
1. На панели выбора карты выберите вид глобуса или выберите режим просмотра, который хотите использовать (например, на плоскости).



2. Выберите карту. Например, историческая карта мира 1689 года.



3. Используйте панель поиска для ввода названия интересующего географического объекта. При нажатии клавиши Enter будет выполнен поиск для вывода более подробной информации.



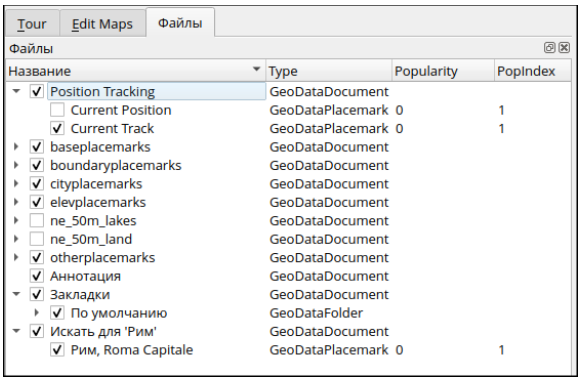
4. После того, как объект найден, используйте мышь или панель инструментов для навигации — увеличения, уменьшения или перемещения по карте.



5. Кликните по объекту, чтобы открыть панель информации, где можно узнать больше о выбранном месте.



6. Активируйте различные слои на панели слоёв, чтобы увидеть дополнительную информацию, такую как погодные условия, физическая география или спутниковые снимки.

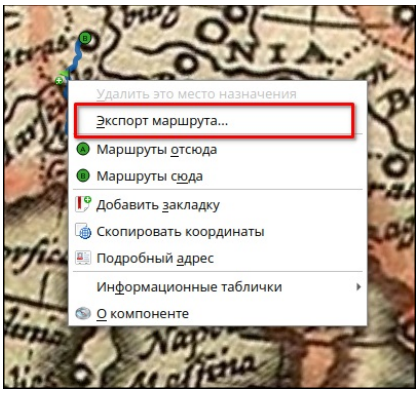


7. Проложите маршрут. Для выбора начальной точки маршрута щёлкните по желаемому местоположению ПКМ и выберите из контекстного меню «**Маршруты отсюда**». Для выбора конечной точки щёлкните по другому местоположению ПКМ и выберите «**Маршруты сюда**».

После выполненных действий маршрут отобразится на карте:



8. Возможно сохранять маршруты в формате **.kml** (Keyhole Markup Language) и загружать их на том же самом или на другом компьютере с установленным приложением Marble. Для сохранения маршрута в файл с расширением **.kml** используйте функцию экспорта маршрута в файл через контекстное меню, щёлкнув ПКМ по маршруту. Открывшийся диалог сохранения позволит указать имя сохраняемого файла.



Система программирования КуМир

Установка
Конфигурации
Описание конфигурации «Кумир»
Исполнитель «Робот»
Установка стартовой обстановки
Окно наблюдения
Ручное управление
Исполнитель «Чертежник»
Исполнитель «Кузнечик»
Описание конфигураций «Кумир для учителей» и «Кумир-Про»
Примеры работы
Пример 1 (вычисление факториала)
Пример 2 (исполнитель «Робот»)
Пример 3 (исполнитель «Чертежник»)
Пример 4 (исполнитель «Кузнечик»)

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: kumir2-2.1.0

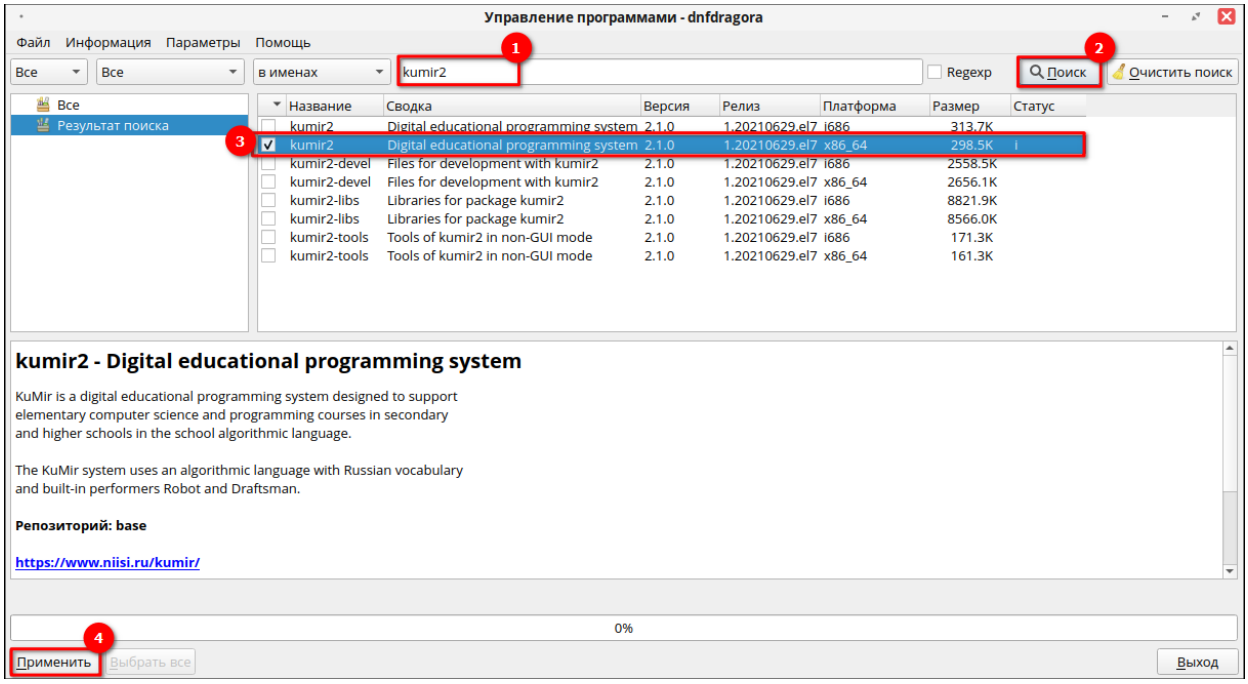
КуМир (Комплект Учебных МИРов) — это цифровая образовательная система программирования, предназначенная для поддержки начальных курсов информатики и программирования в средних и высших школах на школьном алгоритмическом языке.

Система **КуМир** использует алгоритмический язык с русской лексикой и встроенными исполнителями.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**kumir2**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



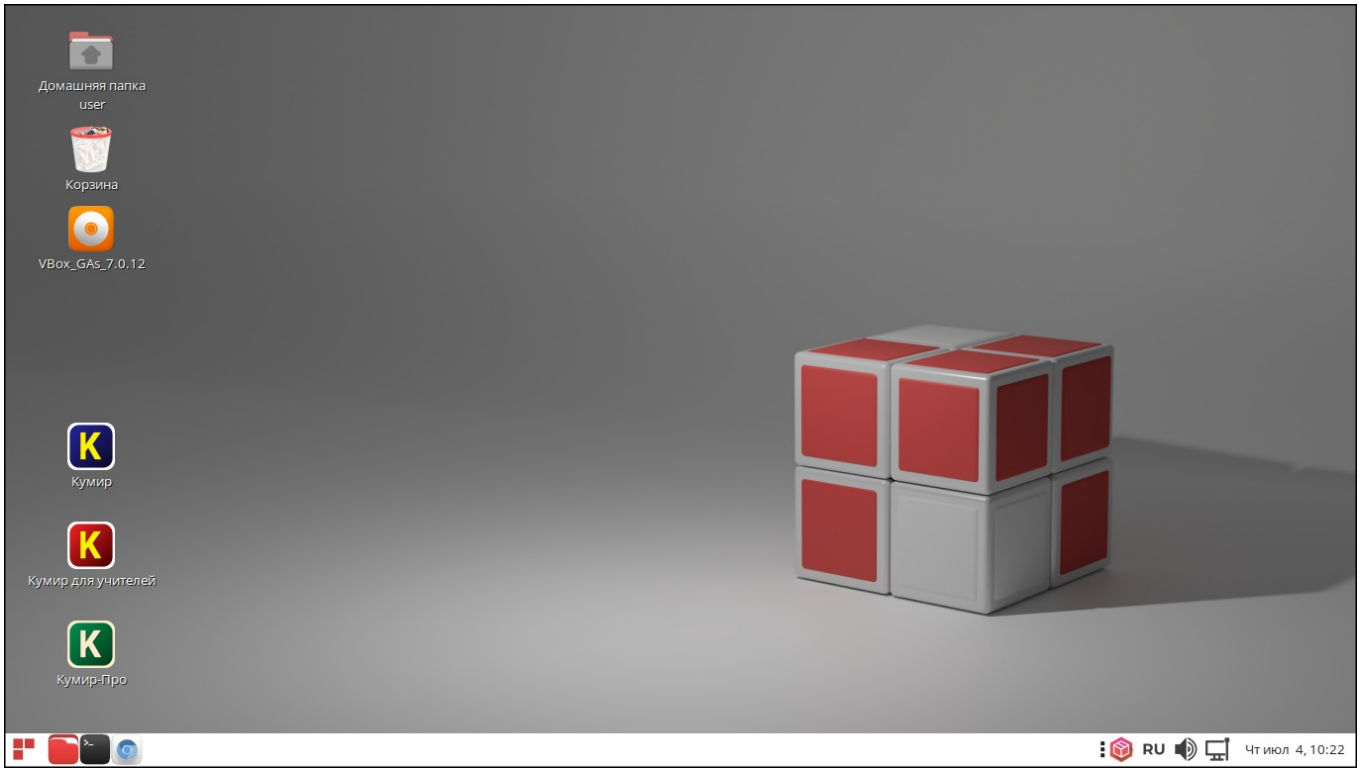
Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install kumir2
```

После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**Кумир**» («**Кумир для учителей**»,

«**Кумир-Про**»).

Для размещения значка программы **Кумир** на рабочем столе наведите мышь на программу в «**Главном меню**» и, нажав ПКМ, выберите в контекстном меню «**Поместить на Рабочий стол**». Теперь значок **Кумир** доступен для быстрого запуска.



Конфигурации

Выбор между доступными конфигурациями зависит от целей и задач.

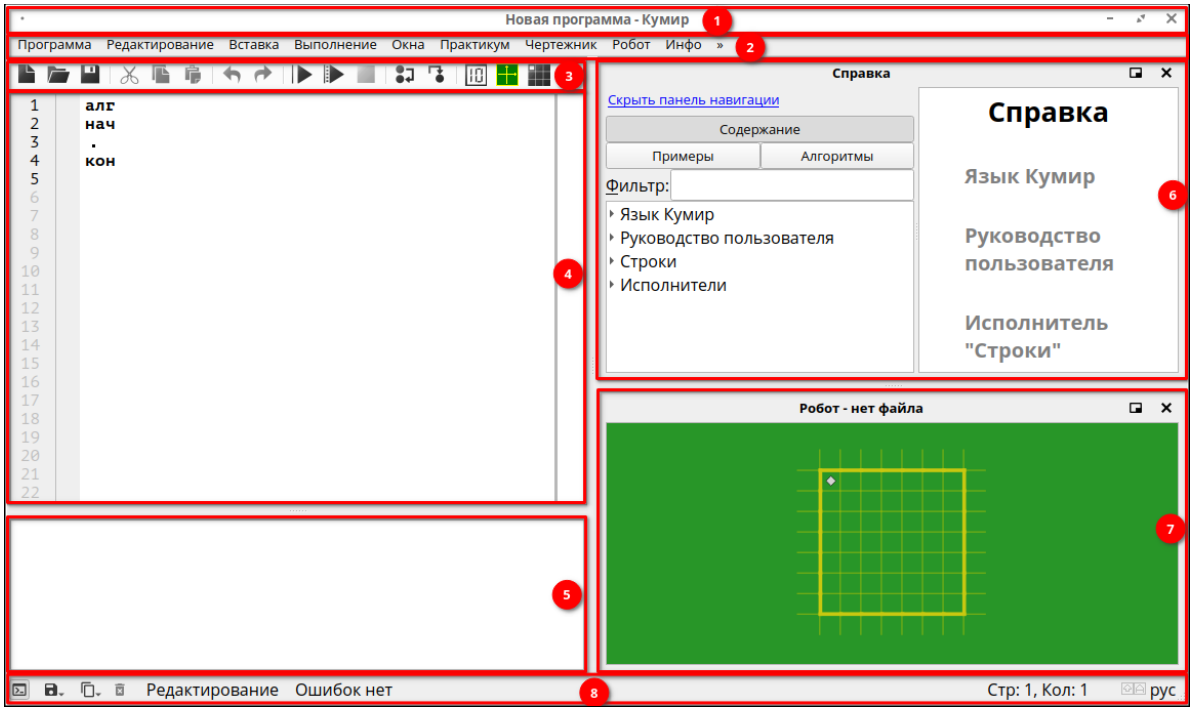
1. Конфигурация «**Кумир**» — предназначена для первичного школьного обучения.

2. Конфигурация «**Кумир для учителей**» — предназначена для подготовки заданий и практикумов.

3. Конфигурация «**Кумир-Про**» — профессиональная версия, предназначенная для более глубокой работы с программированием и разработки сложных проектов.

Описание конфигурации «Кумир»

После запуска программы в конфигурации для учащихся на экране появляется главное окно системы Кумир:



Интерфейс программы стандартный и состоит из нескольких типовых частей.

1. **Системный заголовок главного окна** — отображает название программы.

2. **Главное меню** — содержит семь основных пунктов и несколько дополнительных пунктов.

3. **Панель инструментов** — стандартная панель инструментов с кнопками быстрого доступа к основным функциям программы.

4. **Рабочая область** — область для написания и редактирования кода. Она поддерживает подсветку синтаксиса и имеет номера строк для удобства навигации.

5. **Область ввода-вывода программы** — отображаются результаты выполнения программы, а также можно вводить данные, если программа этого требует.

6. **Справочные руководства** — раздел, где можно найти информацию о языке программирования, функциях системы **Кумир** и примеры кода (Меню «**Инфо**» — «**Справочные руководства**» или горячая клавиша **F1**).

7. **Окно исполнителя** — визуализирует выполнение программы, если она включает графический или анимационный вывод.

8. **Строка состояния** — отображает информацию об ошибках.

Главное меню

Главное меню системы содержит несколько пунктов.

Меню «**Программа**» содержит действия для работы с файлами, имеющими формат **.kum***. С его помощью можно создать новую программу, новый текст, загрузить, сохранить файлы, закрыть рабочую вкладку.

Меню «**Редактирование**» обеспечивает стандартные средства редактирования текстов, например, ввод символов в режиме вставки или замены, удаление символов, выделение/копирование/вставку/удаление фрагмента текста, отмену/возврат последних действий, поиск по тексту.

Меню «**Вставка**» содержит операции вставки конструкций используемого языка программирования / операции выполнения записанных ранее последовательностей нажатий клавиш.

Элементами меню «**Выполнение**» являются действия по запуску и остановке выполнения текущей программы.

Меню «**Окна**» содержит действия отображения дополнительных окон, которые реализуются исполнителями, отображает или скрывает нижнюю часть главного окна с областью ввода-вывода, отображает дополнительное окно практикума.

Меню «**Практикум**» позволяет загрузить курс, открыть список тетрадей/курсов, запустить проверку заданий, сохранить тетрадь, вернуть исполнителей к исходному состоянию.

Модуль поддержки практикумов позволяет учителю создавать, а ученику выполнять учебные курсы по информатике на базе системы **Кумир**.

Курсы представляют:

- систему заданий, которую должен выполнить ученик;
- методику, которая описывает рекомендованный порядок выполнения заданий.

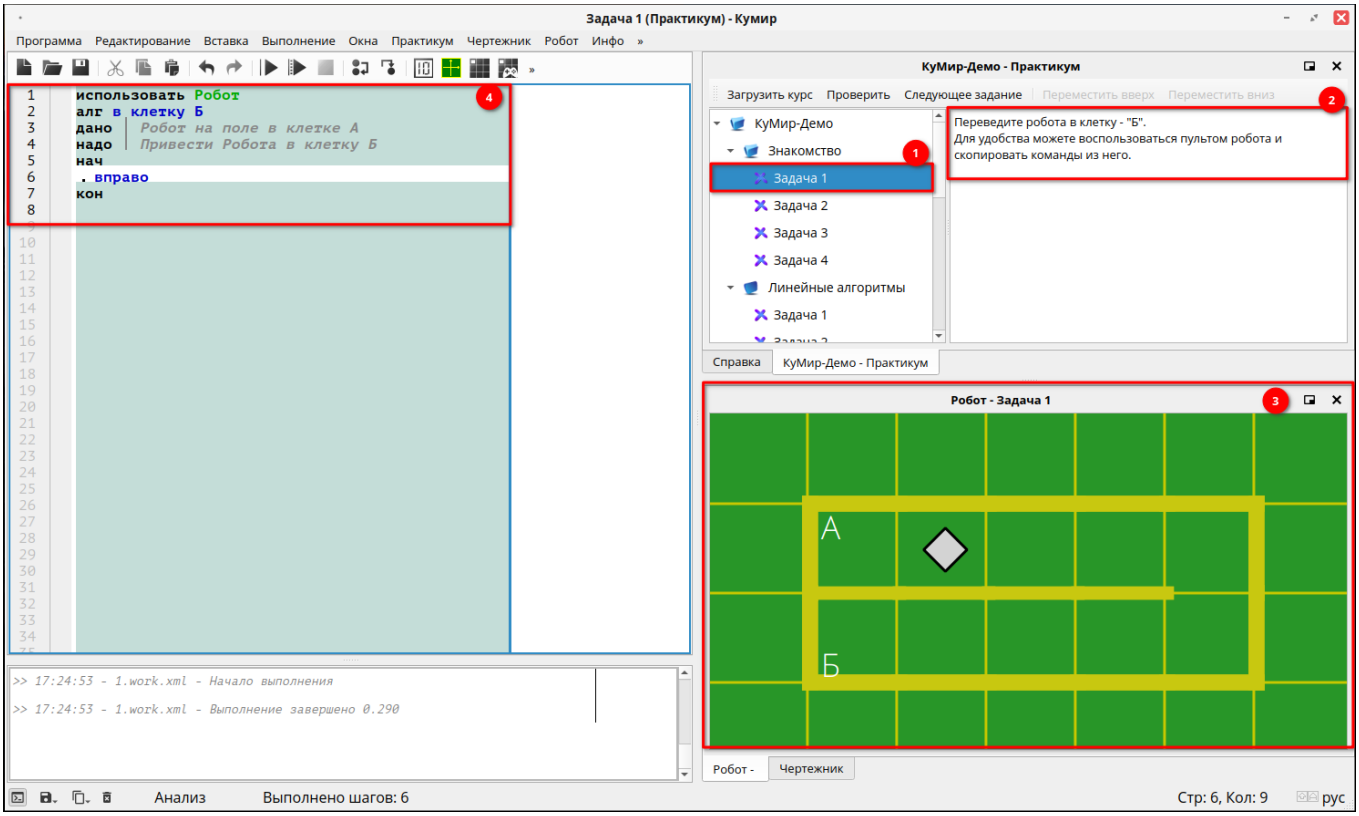
Задание предлагает ученику написать программу. Задание включает в себя:

- текстовое описание задания;
- шаблон программы и, если нужно, обстановку исполнителя;
- программу тестирования, обстановки, используемые при тестировании.

В меню «**Практикум»** ученик выбирает пункт «**Загрузить курс**» или выбирает «**Недавние тетради/курсы...**».

В исходном состоянии ученику доступно только одно действие – загрузить курс. После того, как курс выбран, ученику предлагается создать тетрадь, в которой будут сохраняться результаты его работы. В левой части окна показывается *список заданий* (1).

Ученик поочерёдно выбирает задачу в списке заданий, открывая ветви дерева, нажимая на  . После выбора задачи появляется словесное *описание текущего задания* (2), а в поле программы окна системы **Кумир** устанавливается окно исполнителей (3) и начальный текст программы (4). Результаты выполненных заданий автоматически сохраняются в тетрадь.



Различные исполнители системы Кумир могут иметь свои одноимённые меню, которые располагаются в главном окне между меню «**Практикум**» и «**Инфо**».

В среде программирования **Кумир** существует множество различных исполнителей, каждый из которых предназначен для выполнения определённых задач:

1. Исполнитель «Робот» — выполняет команды по перемещению и манипуляции объектами в лабиринте.

2. Исполнитель «Чертежник» — рисует геометрические фигуры и линии на плоскости.

3. Исполнитель «Кузнечик» — перемещается по клетчатому полю, прыгая через заданное количество клеток.

4. Исполнитель «Вертун» — вращается вокруг своей оси и выполняет команды, связанные с поворотами.

5. Исполнитель «Клавиатура» — обрабатывает ввод с клавиатуры и выполняет команды на основе введённых данных.

6. Исполнитель «Водолей» — перемещает воду между сосудами, выполняя задачи по переливанию.

7. Исполнитель «Рисователь» — создаёт рисунки и изображения на экране.

8. Исполнитель «Черепаха» — рисует линии и фигуры, перемещаясь по экрану.

Меню «**Инфо**» (сокращение от «Информация») содержит элементы, вызов которых приводит к отображению информационных окон.

Панель инструментов

Сверху от редактора находится панель инструментов, которая дублирует часто используемые действия главного меню:

 — создаёт новый файл программы;

 — открывает существующий файл программы;

 — сохраняет текущий файл программы;

 — удаляет выделенный текст и помещает его в буфер обмена;

 — копирует выделенный текст в буфер обмена;

 — вставляет текст из буфера обмена в текущее место курсора;

 — отменяет последнее изменение в тексте программы;

 — повторяет последнее отменённое изменение;

 — выполняет программу без отображения дополнительной информации на полях;

 — запускает выполнение программы в обычном режиме;

 — прерывает выполнение программы;

 — выполняет один шаг программы;

 — выполняет программу шаг за шагом;

 — открывает окно с заданиями и упражнениями;

 — запускает исполнителя «Чертежник», с помощью которого можно программировать движения виртуального рисовальщика для создания графических изображений;

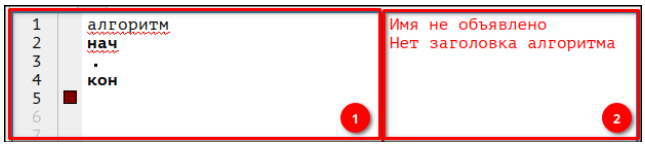
 — запускает исполнителя «Робот», позволяет программировать виртуального робота;

 — открывает пульт управления Роботом, что даёт возможность управлять роботом в режиме реального времени, а не через предварительно написанный код;

 — открывает окно, в котором можно выбрать, какие кнопки показывать в строке, а какие — скрыть.

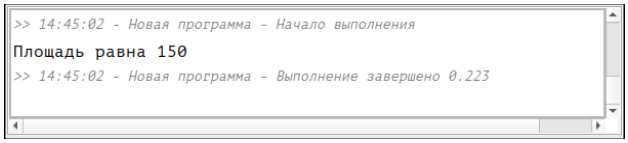
Рабочая область

Рабочая область программы делится на две части: *область редактирования текста программы* (1) и *поле редактора* (2).



Область ввода-вывода программы

Область ввода/вывода автоматически появляется при выполнении операторов или во время выполнения программы. Она может быть полностью скрыта.



Справочные руководства

Справочные руководства представляют собой документацию, которая помогает пользователям понять основы работы с программой, её функции и язык программирования. Руководства содержат примеры кода, объяснения команд и методики решения типичных задач.

Окно исполнителя

В окне исполнителя отображается процесс выполнения программы. Здесь пользователи могут наблюдать за выполнением команд и взаимодействием программы с виртуальными объектами, такими как «**Чертежник**» или «**Робот**».

Строка состояния

Строка состояния отображает информацию о текущем состоянии программы, данные о номере выполняемой строки, статусе исполнения и сообщения об ошибках. Это помогает пользователям отслеживать процесс выполнения программы и быстро находить и исправлять ошибки.



В левой части строки состояния находятся следующие кнопки:

 – отображает область ввода/вывода;

 – отображает всплывающее меню сохранения содержимого окна ввода-вывода;

 – отображает всплывающее меню копирования содержимого окна ввода-вывода в буфер обмена;

 – эта кнопка становится доступной только при наличии текста в области ввода-вывода, её нажатие приводит к очистке данной области.

Исполнитель «Робот»

Среда исполнителя «**Робот**» — прямоугольное клетчатое поле, между клетками которого могут стоять стены. Окно «**Робота**» выглядит следующим образом:



Робот находится в **текущей обстановке**, которая изменяется при выполнении команд Робота. Выполнение программы начинается со **стартовой обстановки**.

Обстановка «**Робота**» представляет собой прямоугольное поле, окружённое забором и разбитое на клетки.

Обстановка описывается следующими величинами:

- размеры обстановки — количество строк (1–128) и количество столбцов (1–255);
- характеристики каждой клетки:
    - наличие стен вокруг клетки;
    - признак закрашенности;
    - уровень радиации (может принимать любое вещественное значение от 0 до 99 у. е.);
    - температура (может принимать любое целое значение от -273 до +233 градусах Цельсия).

«**Робот**» изображается в клетке  . «**Робот**» может измерить температуру и радиацию, но не может распознать символы в клетках. Для изменения масштаба изображения окружающей обстановки перейдите в окно наблюдения за «**Роботом**» и используйте колёсико мыши.

Команды исполнителя Робот

Основными командами исполнителя «**Робот**» являются:

- **стартовая команда** — программа, управляющая «Роботом», должна начинаться со строки использовать «Робот». При выполнении этой строки **Кумир** помещает «Робота» в стартовую обстановку.
- **команды-действия** — влево, вправо, вверх, вниз, закрасить;

  Пример:

```
использовать Робот
 алг
 нач
 вправо
```

```
вниз
влево
вверх
закрасить
кон
```

- **команды проверки условий** — сверху стена/свободно, снизу стена/свободно, слева стена/свободно, справа стена/свободно, закрашена, чистая;

  Пример:

```
алг лог справа стена
```

- **команды измерения** — измеряет температуру, радиацию в клетке, где находится «Робот».

  Пример:

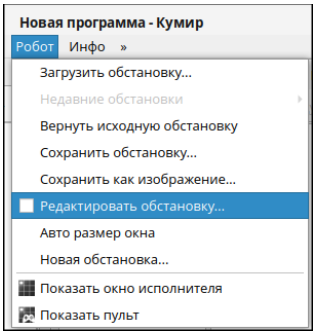
```
алг вещ радиация
 алг вещ температура
```

Исполнитель «**Робот**» двигается по клеткам. Получая простую команду, «**Робот**» выполняет движение на одну клетку и ждёт следующей команды.

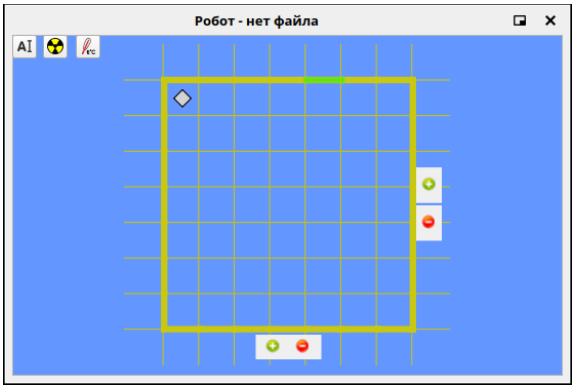
С принципами работы остальных исполнителей можно ознакомиться в меню «**Инфо**» — «**Справочные руководства**».

Установка стартовой обстановки

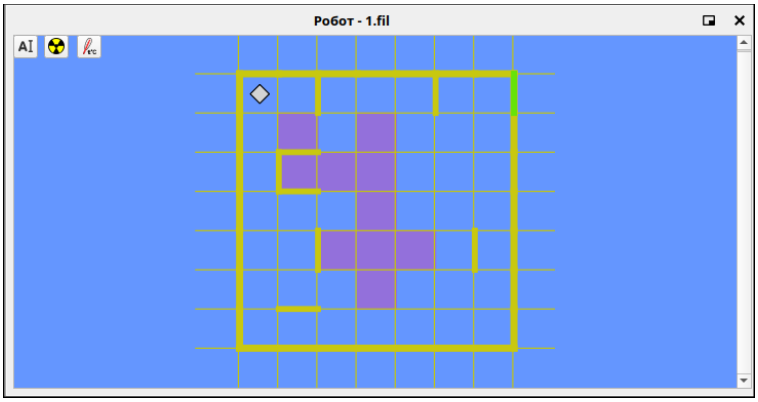
В системе **Кумир** есть средства, с помощью которых можно задать нужную стартовую обстановку. Для этого откройте меню « **Робот**» — «**Редактировать обстановку...**».



Диалоговое окно обстановки «**Робот**» становится синего цвета, также появляются кнопки управления, с помощью которых можно добавить или убрать клетки поля.

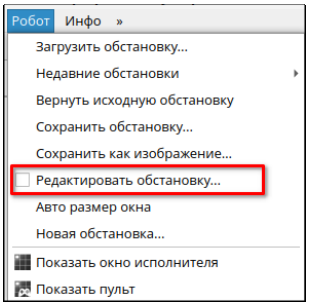


Затем, щёлкая ЛКМ, выставите препятствия для «**Робота**» или закрасьте клетки.



Для сохранения обстановки перейдите в меню «**Робот**» — «**Сохранить обстановку...**». В открывшемся диалоговом окне задайте параметры сохранения файла и сохраните его.

Для выхода из режима редактирования перейдите в меню «**Робот**» и снимите флаг с пункта «**Редактировать обстановку...**».



Для загрузки обстановки перейдите в меню «**Робот**» — «**Загрузить обстановку...**». Нажмите «**Open**».

Окно наблюдения

Окно наблюдения за «Роботом» создаётся в момент начала сеанса работы системы **Кумир** и доступно до окончания сеанса. Во время сеанса работы окно может находиться в одном из двух состояний — видимо или скрыто.

Для отображения окна наблюдения можно нажать на кнопку  или выбрать пункт в меню «**Окна**» — «**Робот**».

Окно наблюдения появится автоматически при запуске программы, содержащей команду:

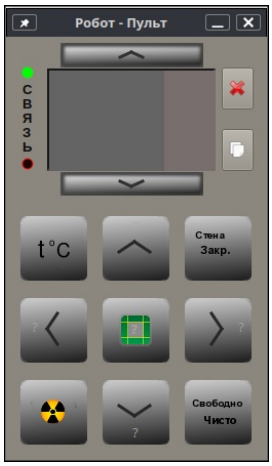
```
использовать Робот
```

Окно наблюдения за «Роботом» может находится в двух режимах:

- **обычном** – применяется при наблюдении за Роботом во время исполнения программ или управлении с пульта,
- **редактирования** – применяется при редактировании стартовой обстановки Робота.

Ручное управление

Окно пульта ручного управления «Роботом» выглядит следующим образом:



Пульт позволяет вручную управлять «Роботом» – выдавать команды, входящие в систему команд «Робота». Использовать пульт можно в интервал времени, когда выполнение программы приостановлено. Перейти к управлению через пульт можно из меню «**Окна**» — «**Робот-Пульт**» или, нажав на панели инструментов кнопку  .

Исполнитель «Чертежник»

Функции «**Чертежника**» не являются частью языка программирования. Для его использования необходимо в программе явно указать использование данного исполнителя:

```
использовать Чертежник
```

В программе отобразится поле исполнителя:

Команды исполнителя «Чертежник»

Основными командами исполнителя «**Чертежник**» являются:

1. **Опустить перо** — опускает перо и при дальнейшем перемещении оставляет след.

Синтаксис:

```
алг опустить перо
```

2. **Поднять перо** — поднимает перо и при дальнейшем перемещении не оставляет след.

Синтаксис:

```
алг поднять перо
```

3. **Выбрать чернила** — устанавливает цвет чернил (цвет *a*).

Синтаксис:

```
алг выбрать чернила(цвет a)
```

4. Сместиться в точку — смещает перо в заданную точку:

- x — абсцисса точки,
- y — её ордината.

Синтаксис:

```
алг сместиться в точку(вещ x, вещ y)
```

5. **Сместиться на вектор** — смещает перо на вектор (dx, dy). Иными словами, если до выполнения команды перо находилось в точке (x, y), то после её выполнения, оно будет находиться в точке (x + dx, y + dy).

Синтаксис:

```
алг сместиться на вектор(вещ dx, вещ dy)
```

6. **Написать** — пишет строку, растянутую или сжатую до заданной ширины:

- ширина — ширина строки,
- текст — текст строки.

Синтаксис:

```
алг написать(вещ ширина, лит текст)
```

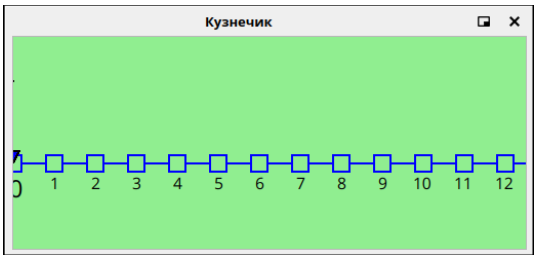
Исполнитель «Кузнечик»

«**Кузнечик**» живёт на числовой прямой и обозначается синим треугольником.

Для использования исполнителя «**Кузнечик**» необходимо в программе явно указать его использование:

```
использовать Кузнечик
```

В программе отобразится поле исполнителя:



Команды исполнителя «Кузнечик»

Основными командами исполнителя «**Кузнечик**» являются:

1. **Вперёд** — сделать прыжок длины **x** вперёд.

Синтаксис:

```
алг вперед x
```

2. **Назад** — сделать прыжок длины **x** назад.

Синтаксис:

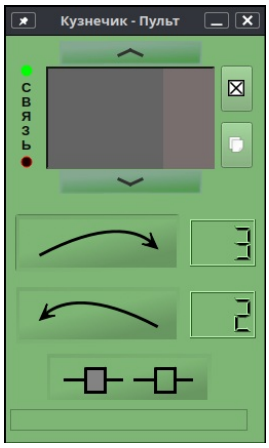
```
алг назад x
```

3. **Перекрасить** — меняет цвет клетки, в которой в данный момент находится «Кузнечик». Если клетка была чистая, закрашивает её. Если закрашена — снимает закраску.

Синтаксис:

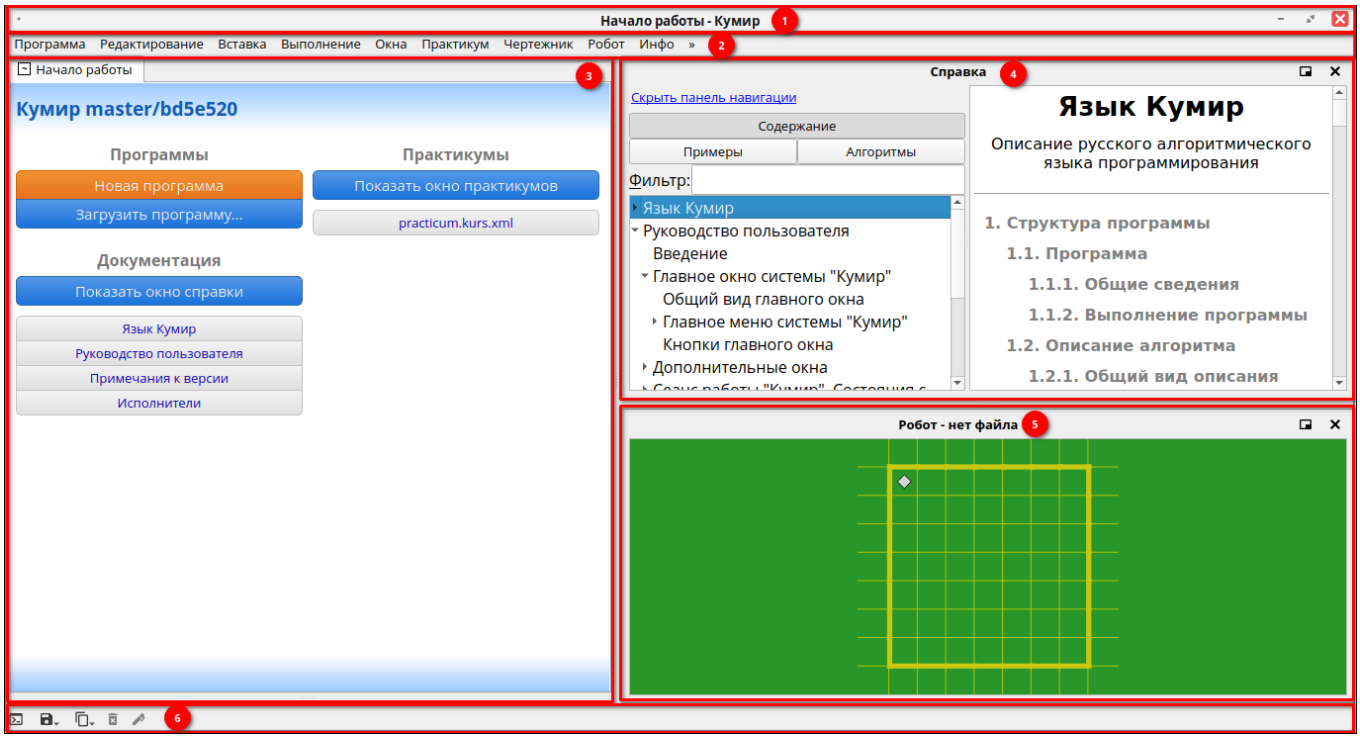
```
алг перекрасить
```

Программу для исполнителя «**Кузнечик**» можно писать также через пульт. Для управления исполнителем «**Кузнечик**» перейдите в меню «**Окна**» — «**Кузнечик-Пульт**»:



Описание конфигураций «Кумир для учителей» и «Кумир-Про»

Главное окно программы в конфигурациях «**Кумир для учителей**» и «**Кумир-Про**» выглядит следующим образом:



Интерфейс программы стандартный и состоит из нескольких типовых частей:

1. **Системный заголовок главного окна** — отображает название программы.

2. **Главное меню** — содержит семь основных пунктов и несколько дополнительных пунктов.

3. **Стартовая страница «Начало работы»** — расположены кнопки доступа к программам, практикумам, документации.

4. **Справочные руководства** — раздел, где можно найти информацию о языке программирования, функциях системы **Кумир** и примеры кода (Меню «**Инфо**» — «**Справочные руководства**» или горячая клавиша **F1**).

5. **Окно исполнителя** — визуализирует выполнение программы, если она включает графический или анимационный вывод.

6. **Строка состояния** — отображает информацию об ошибках.

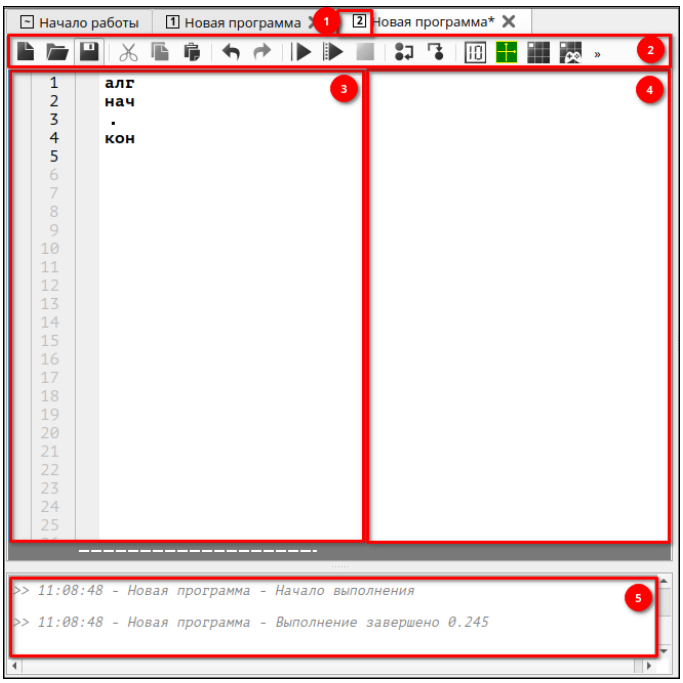
После запуска отображается стартовая страница «**Начало работы**», на которой отображаются ссылки для быстрого доступа к последним файлам, практикумам, книгам справочной системы, а также крупные кнопки, дублирующие некоторые пункты меню программы. Начальную вкладку закрыть нельзя.

Для начала работы с системой необходимо создать или загрузить существующую программу либо открыть практикум.

Слева от заголовка вкладки (1) отображается номер от 1 до 9 для быстрого доступа с помощью клавиатурного сочетания: CTRL+1..9 , где 1..9 – это номер вкладки. Доступ к стартовой странице обеспечивается комбинацией клавиш CTRL+~ .

Программа имеет две основные области: *рабочую область* и *область ввода-вывода* (4).

Рабочая область делится на две части: *область редактирования текста программы* (2) и *поле редактора* (3).



Система Кумир поддерживает преподавание по учебникам:

1. Основы информатики и вычислительной техники: Пробный учеб. для средних учебных заведений / А. П. Ершов, А. Г. Кушниренко, Г. В. Лебедев, А. Л. Семенов, А. Х. Шень. — М.: Просвещение, 1998. — 207 с.

2. Основы информатики и вычислительной техники: Учеб. для 10-11 кл. общеобразоват. учреждений / А. Г. Кушниренко, Г. В. Лебедев, Р. А. Сворень. — 4-е изд. — М.: Просвещение, 1996. — 223 с.

3. Информатика: 7-9 кл.: Учеб. для общеобразоват. учр. / А. Г. Кушниренко, Г. В. Лебедев, Я. Н. Зайдельман. — 4-е изд., стер. — М.: Дрофа, 2003. — 335 с.

4. Информационная культура. Кодирование информации. Информационные модели: 9-10 кл.: Учеб. для общеобразоват. учр. / А. Г. Кушниренко, А. Г. Леонов, М. Г. Эпиктетов и др. — 6-е изд., стер. — М.: Дрофа, 2003. — 199 с.

5. Информатика: алгоритмика: Учеб. для 6 кл. общеобразоват. учр. / А. К. Звонкин, С. К. Ландо, А. Л. Семенов. — М.: Просвещение, 2006. — 237 с.

6. Информатика: алгоритмика: Учеб. для 7 кл. общеобразоват. учр. / С. К. Ландо, А. Л. Семенов, М. Н. Вялый. — М.: Просвещение, 2008. — 207 с.

7. Информатика. 10 класс. Углубленный уровень: Учебник. в 2 частях / К. Ю. Поляков, Е. А. Еремин. — М.: Бином, 2013. — 648 с.

8. Информатика. 11 класс. Углубленный уровень: Учебник. в 2 частях / К. Ю. Поляков, Е. А. Еремин. — М.: Бином, 2013. — 532 с.

Система **Кумир** поддерживает также разработку практикумов по программированию с автоматизированной проверкой.

Примеры работы

Пример 1 (вычисление факториала)

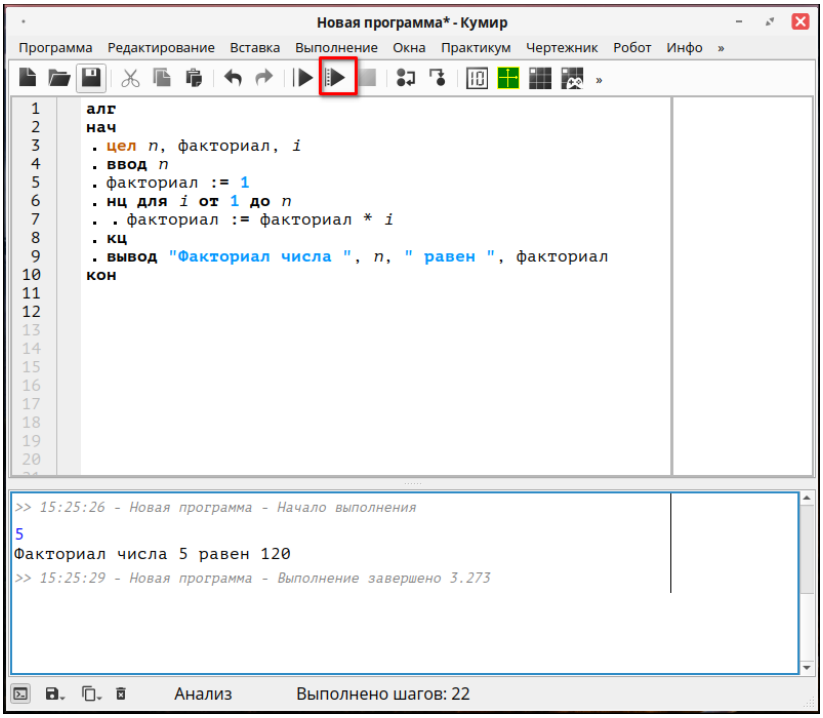
Для вычисления факториала числа, введённого пользователем, введите код в рабочей области:

```
алг
 нач
 цел n, факториал, i
 ввод n
 факториал := 1
 нц для i от 1 до n
 факториал := факториал * i
 кц
 вывод "Факториал числа ", n, " равен ", факториал
 кон
```

Алгоритм работы программы:

- Сначала программа запрашивает у пользователя число n.
- Затем она инициализирует переменную факториал значением 1.
- После этого программа входит в цикл от 1 до n, на каждом шаге умножая текущее значение факториала на номер итерации i.
- В конце программа выводит результат вычисления факториала.

Запустите код, нажав «**Обычное выполнение**». В области ввода-вывода введите любое число, далее отобразится результат выполнения программы.

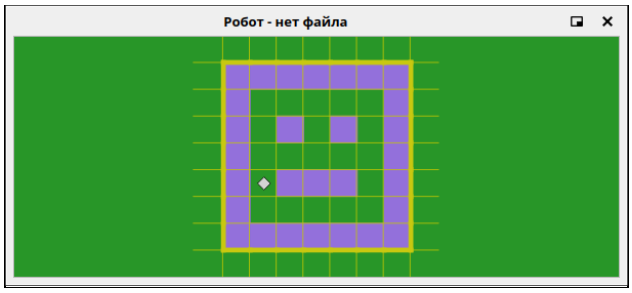


Пример 2 (исполнитель «Робот»)

Для выполнения задачи рисования на виртуальном поле с использованием «**Робота**» введите в рабочей области следующий код:

```
использовать Робот
алг
нач
нц пока справа свободно
закрасить; вправо
кц
нц пока снизу свободно
закрасить; вниз
кц
нц пока слева свободно
закрасить; влево
кц
нц пока сверху свободно
закрасить; вверх
кц
вниз; вниз; вправо; вправо
закрасить
вправо; вправо
закрасить
вниз; вниз
нц 3 раз
закрасить; влево
кц
кон
```

Результат выполнения:

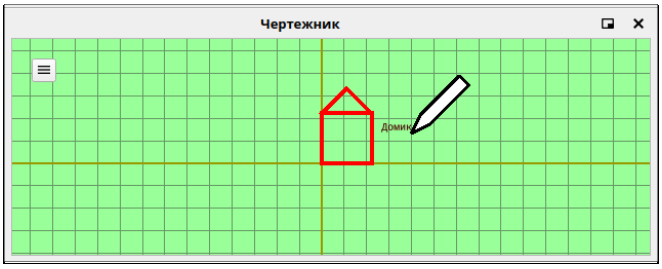


Пример 3 (исполнитель «Чертежник»)

Для выполнения задачи рисования на виртуальном поле с использованием «Чертежника» введите в рабочей области следующий код:

```
использовать Чертежник
 алг
 нач
 выбрать чернила(красный)
  опустить перо
  сместиться на вектор(0, 5)
  сместиться на вектор(5, 0)
  сместиться на вектор(0, -5)
  сместиться на вектор(-5, 0)
  поднять перо
  сместиться на вектор(5, 5)
  опустить перо
  сместиться на вектор(-2.5, 2.5)
  сместиться на вектор(-2.5, -2.5)
  поднять перо
  сместиться в точку(0, 0)
  сместиться на вектор(6, 3)
  написать(3, "Домик")
 кон
```

Результат выполнения:



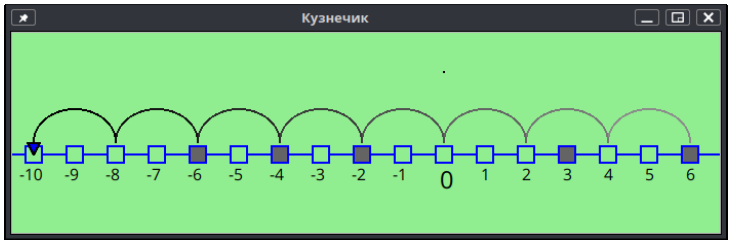
Пример 4 (исполнитель «Кузнечик»)

Для выполнения задачи перемещения «Кузнечика» с перекрашиванием клеток с использованием «Кузнечика» введите в рабочей области следующий код:

```
использовать Кузнечик
 алг
 нач
 вперед 3
   перекрасить
   вперед 3
   перекрасить
```

```
  назад 2
  назад 2
  назад 2
  назад 2
  перекрасить
  назад 2
  перекрасить
  назад 2
  перекрасить
  назад 2
  назад 2
кон
```

Результат выполнения:



GNU Octave — программа для математических вычислений

Установка
Описание программы
Начало работы
Примеры использования

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: octave-6:6.3.0

GNU Octave — свободная программная система для математических вычислений, использующая совместимый с MATLAB язык высокого уровня, предназначенный для решения задач вычислительной математики.

GNU Octave представляет удобный интерактивный командный интерфейс для решения линейных и нелинейных математических задач и для выполнения других численных экспериментов.

Язык Octave оперирует арифметикой вещественных и комплексных скаляров и матриц, имеет расширения для:

- решения линейных алгебраических задач;
- нахождения корней систем нелинейных алгебраических уравнений;
- работы с полиномами;
- решения различных дифференциальных уравнений;
- интегрирования систем дифференциальных и дифференциально-алгебраических уравнений первого порядка;
- интегрирования функций на конечных и бесконечных интервалах.

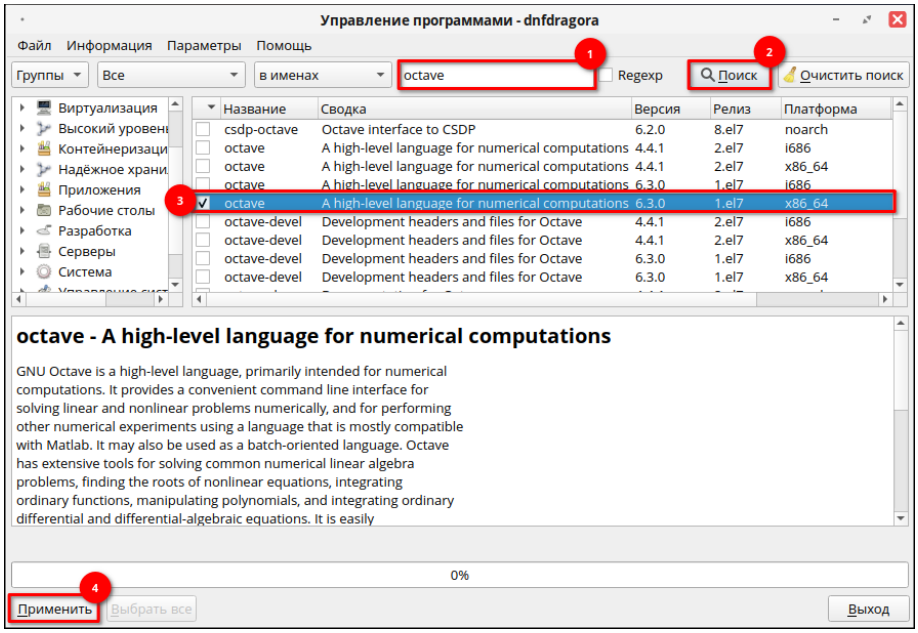
Характеристики:

- GNU Octave написана на языке C++ с использованием библиотеки STL;
- для запуска скриптов octave используется интерпретатор;
- GNU Octave можно дополнять динамически подгружаемыми модулями;
- GNU Octave является кроссплатформенной;
- существуют онлайн-сервисы, позволяющие выполнять скрипты octave и отображать полученные результаты в браузере.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов dnfdragora перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**octave**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки.



Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install octave
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя. Для запуска программы через терминал введите команду:

```
octave
```

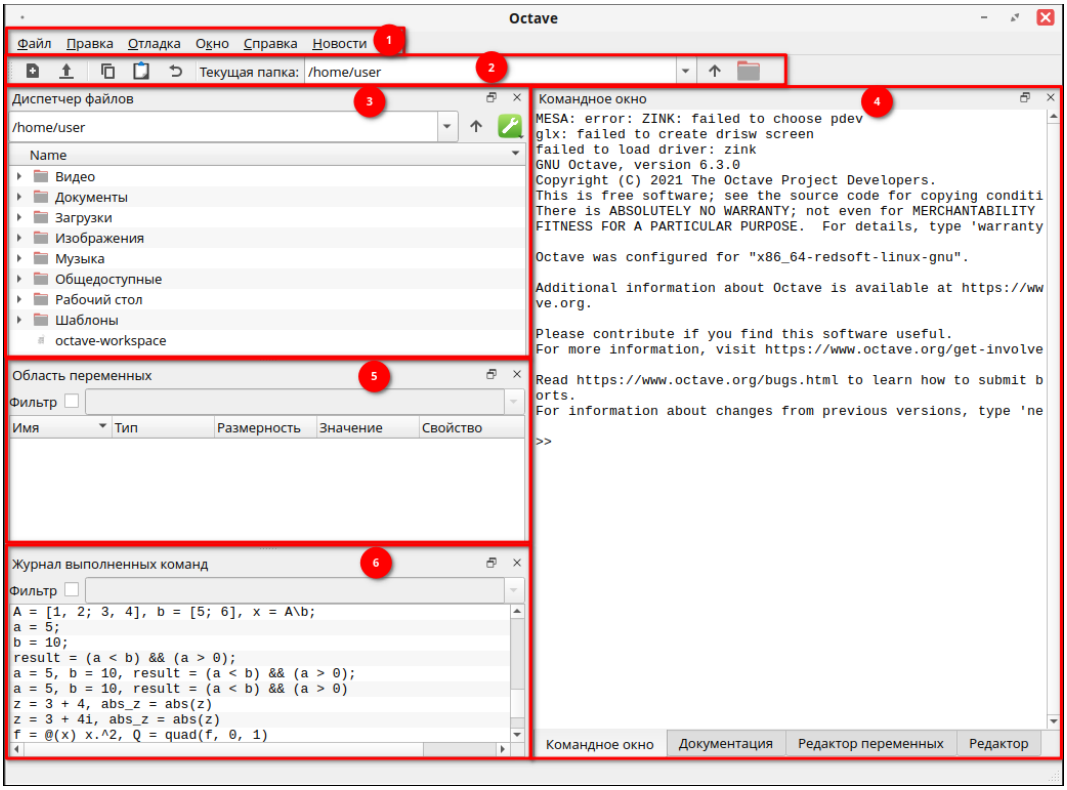
Для выхода из Octave введите **quit** или **exit** в командной строке. После установки программа будет доступна из «**Главного меню**» — «**Образовательные**» — «**GNU Octave**».

Можно запустить программу также с помощью кнопки запуска (ярлыка) на рабочем столе. Для размещения кнопки запуска (ярлыка) программы на рабочем столе в «**Главном меню**» — «**Образовательные**» щелкните ПКМ на **GNU Octave** и выберите в контекстном меню «**Поместить на Рабочий стол**».



Описание программы

Главное окно программы выглядит следующим образом:



1. **Основное меню** содержит различные функции для управления файлами, редактирования кода, настройки интерфейса и доступа к справочной информации. Основное меню включает:

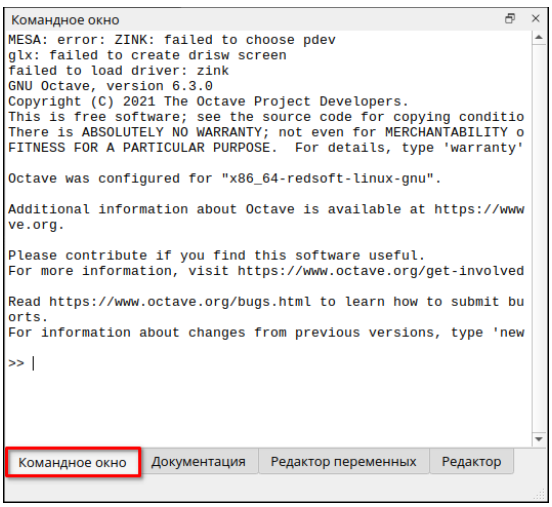
- **Файл** — работа с файлами и областью переменных;
- **Правка** — инструменты редактирования документа и операции с буфером обмена;
- **Отладка** — средство отладки кода;
- **Окно** — управление интерфейсом пользователя;
- **Справка** — доступ к справочной системе;
- **Новости** — примечания к выпуску и последние обновления.

2 . **Панель инструментов** содержит кнопки для быстрого доступа к часто используемым командам, таким как создать сценарий, открыть существующий файл в редакторе, копировать, вставить.

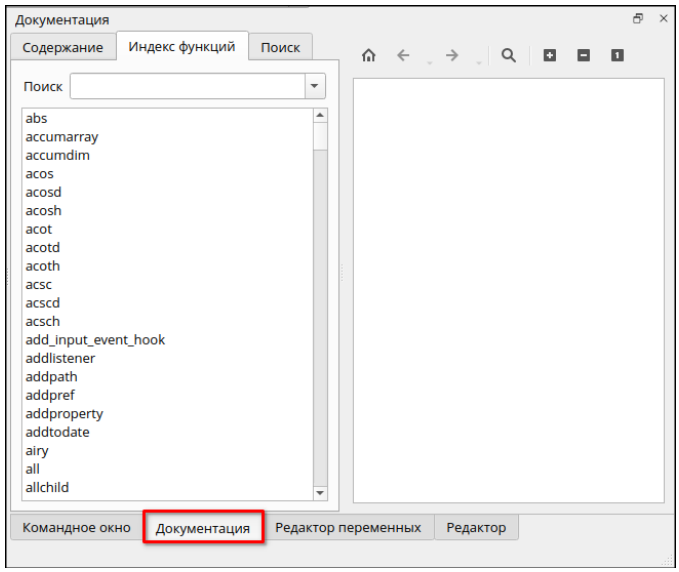
3 . **Диспетчер файлов** позволяет управлять файлами и каталогами на компьютере пользователя. Можно использовать его для открытия, сохранения, перемещения и копирования файлов, а также для просмотра содержимого файлов.

4. **Рабочая область** имеет четыре вкладки, каждая из которых выполняет определённую функцию. Переключение между вкладками позволяет управлять просмотром документации, редактированием переменных или написанием кода.

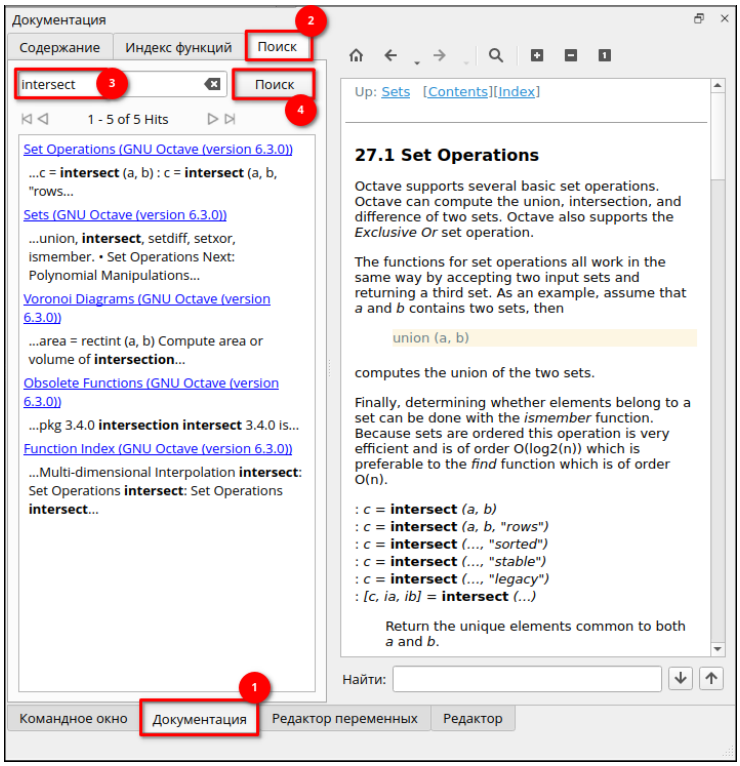
- **Командное окно** вкладка является активной по умолчанию и представляет собой панель ввода, где можно вводить команды и выражения, а также просматривать результаты их выполнения. Командное окно отображает сообщения об ошибках, если они возникают при выполнении команд.



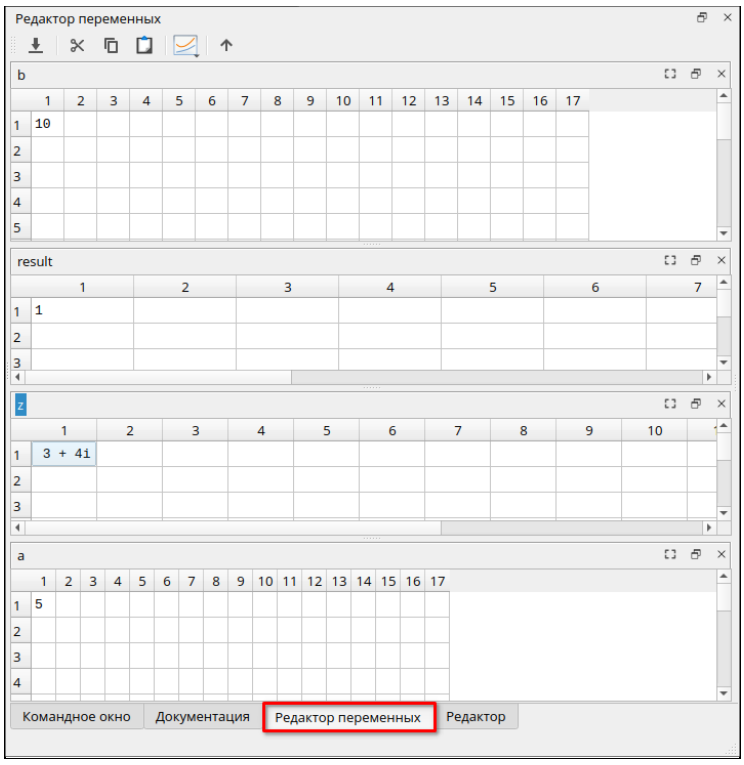
- **Документация** отображает справочную информацию о функциях, переменных и других объектах в **Octave**.



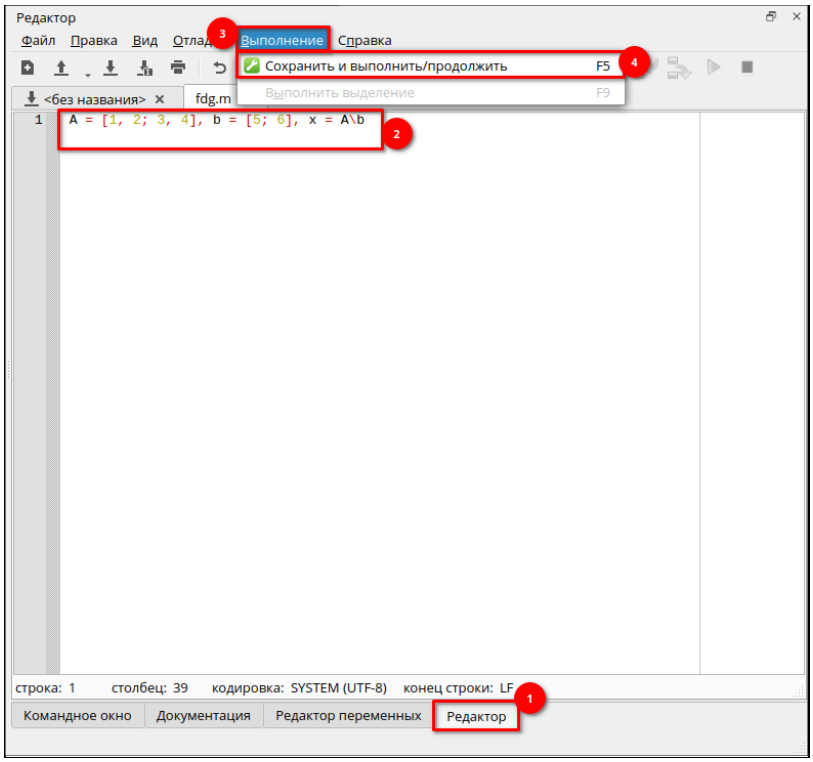
Для просмотра документации по определённому объекту перейдите на вкладку «**Документация**» (1) — «**Поиск**» (2). Введите в строке поиска нужный объект (3) и выполните поиск (4).



- **Редактор переменных** позволяет просмотреть и изменить значения переменных в текущей сессии Octave без повторного ввода всей команды, создающей переменную. После ввода команды, создающей переменную, можно переключиться на вкладку «**Редактор переменных**» и увидеть список текущих переменных. Щёлкнув по имени переменной, можно отредактировать её значение. Для отображения выбранных данных на графике доступен инструмент  .



- **Редактор** (1) позволяет работать в программном режиме. Он представляет собой текстовый редактор, в котором можно писать и редактировать скрипты и программы на языке **Octave**. Скрипты доступны для сохранения и загрузки для дальнейшей работы. После редактирования кода в редакторе (2) можно выполнить его, перейдя в меню «**Выполнение**» (3) — «**Сохранить и выполнить/продолжить**» (4) или используя горячую клавишу **F5**.



В редакторе присутствует дополнительная панель инструментов:



5 . **Область переменных** отображает текущие переменные в текущей сессии Octave. Можно просмотреть, изменить или удалить переменные из этой области.

6. **Журнал выполненных команд** отображает историю введённых команд и результатов их выполнения. Журнал также может быть сохранен как файл для дальнейшего использования или обмена с другими пользователями.

Начало работы

В **Octave** существуют два режима работы.

1 . **Терминальный режим** позволяет пользователю вводить команды в диалоговом режиме, система выполняет их и выводит результаты на экран.

2. **Программный режим** позволяет создавать текстовые файлы с расширением ***.m** и запускать файлы в среде **Octave**. Для работы в программном режиме перейдите на вкладку «**Редактор**».

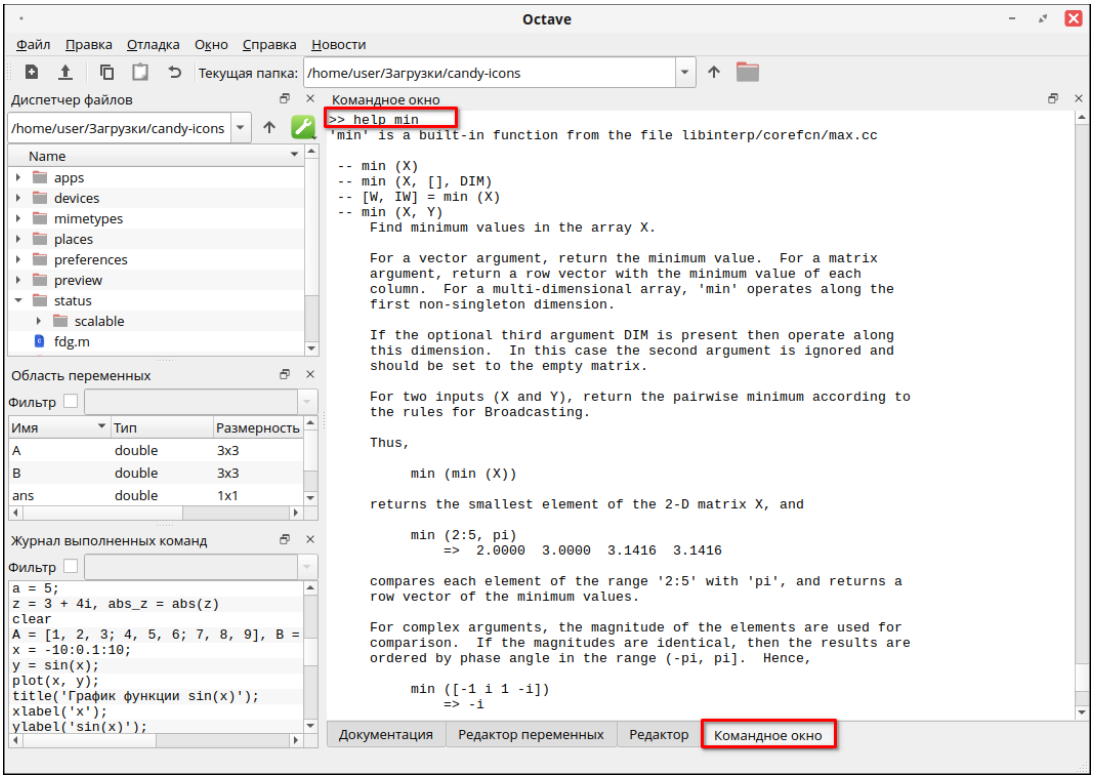
В настройках можно изменить параметры интерфейса командного окна, редактора и устанавливать комбинации клавиш.

Признаком начала работы является наличие знака **>>** в командном окне.

Octave имеет справочную базу на английском языке. Документация доступна из командной строки в онлайн-режиме и печатном варианте.

Для получения справочной информации в командном окне введите **help** и <название_команды>. Например, для вызова справки о функции **min()** введите команду:

```
help min
```



При работе в командном окне нажатие клавиши **Enter** инициирует выполнение введённой команды и выводит результат на экран.

Во время выполнения сложных вычислений, когда не требуется выводить промежуточные результаты, чтобы отменить вывод результата на экран, можно поставить символ "**;**" в конце строки после команды. В противном случае, если символ "**;**" не указан, результаты будут выведены на экран.

Сообщения об ошибке при выполнении кода помогают пользователю проследить, на каком этапе он допустил ошибку.

Octave можно использовать для базовых числовых расчётов. **Octave** поддерживает арифметические операции (**+**, **-**, ***, /**), возведение в степень (**^**), натуральные логарифмы и показатели (**log**, **exp**), тригонометрические функции (**sin**, **cos** и т.д.). **Octave** работает с действительными или мнимыми числами (**i**, **j**). Некоторые математические константы, например, основание натурального логарифма (**e**) и отношение длины окружности к её диаметру (**pi**), также заранее определены в **Octave**.

Примеры использования

Пример 1. Для выполнения арифметических операций введите в командном окне последовательность команд и нажмите **Enter**:

```
a=43;
b=2;
sum= a + b,
diff = a - b,
prod = a * b,
quot = a / b,
```

```
rem = a % b,
pow = a ^ bsum = 45
diff = 41
prod = 86
quot = 21.500
rem = 43
pow = 1849
```

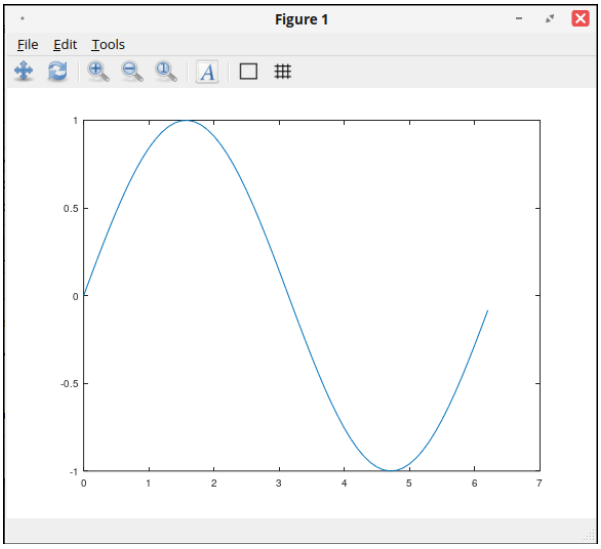
где:

- **sum = a + b** — складывает значения **a**, **b** и сохраняет результат в переменной **sum**;
- **diff = a - b** — вычитает значение **b** из значения **a** и сохраняет результат в переменной **diff**;
- **prod = a * b** — перемножает значения **a**, **b** и сохраняет результат в переменной **prod**;
- **quot = a / b** — делит значение **a** на значение **b** и сохраняет результат в переменной **quot**;
- **rem = a % b** — вычисляет остаток от деления значения **a** на значение **b** и сохраняет результат в переменной **rem**;
- **pow = a ^ b** — возводит значение **a** в степень **b** и сохраняет результат в переменной **pow**.

Пример 2. Для построения графика синусоиды введите следующую команду:

```
t = 0:0.1:2*pi;
y = sin(t);
plot(t, y)
```

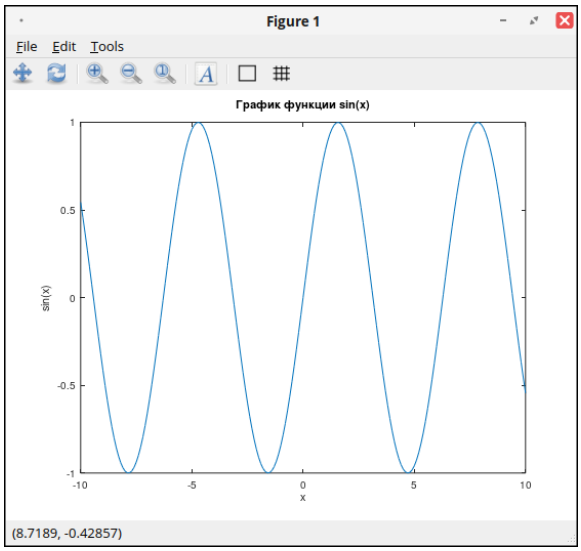
Отобразится окно с графиком.



Пример 3. Для построения графика функции создайте вектор **x** от **-10** до **10** с шагом **0.1**, затем вычислите соответствующие значения функции **sin(x)**:

```
x = -10:0.1:10;
y = sin(x);
plot(x, y);
title('График функции sin(x)');
xlabel('x');
ylabel('sin(x)');
```

Отобразится график:



Пример 4. Введите следующую команду для создания матрицы A и умножения каждого элемента на 2:

```
A = [1, 2, 3; 4, 5, 6; 7, 8, 9], B = A * 2A =
   1   2   3
   4   5   6
   7   8   9

B =
    2    4    6
    8   10   12
   14   16   18
```

Пример 5. Введите матрицу коэффициентов **A**, вектор свободных членов **b** и найдите решение системы линейных уравнений **x** с помощью обратной матрицы **A**:

```
A = [1, 2; 3, 4], b = [5; 6], x = A\bA =
   1   2
   3   4
b =
   5
   6
x =
  -4.0000
   4.5000
```

Пример 6. Введите переменные **a**, **b** и выполните логические операции:

```
a = 5, b = 10, result = (a < b) && (a > 0)a = 5
b = 10
result = 1
```

Пример 7. Введите комплексное число **z** и найдите его модуль:

```
z = 3 + 4i, abs_z = abs(z)z =  3 + 4i
abs_z = 5
```

Пример 8. Определите функцию **f** и найдите площадь под кривой **f(x) = x^2** от **0** до **1** с помощью функции **quad**:

```
f = @(x) x.^2, Q = quad(f, 0, 1)f =
@(x) x .^ 2
Q = 0.3333
```

Установка Geany

Установка
Замена терминала
Простая программа на языке pascal

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: geany-1.36

Geany — среда разработки программного обеспечения, написанная на языке **C** с использованием библиотеки **GTK+**. Отличие **Geany** в том, что это быстрая и легкая среда разработки.

Geany совмещает в себе редактор исходного кода, который поддерживает подсветку синтаксиса большого числа языков и базовые возможности по автодополнению ключевых слов, инструменты для компиляции и запуска программ.

Работать с ней очень удобно и приятно, к тому же она не ограничивает пользователя только одним языком. Всего поддерживается более **60 языков** программирования.

Вы можете подробнее ознакомиться с работой **Geany**, просмотрев наши обучающие видео:

- на **RuTube** — Geany - программировать просто. Первая программа на Pascal;
- в **Яндекс.Дзен** — Geany - программировать просто. Первая программа на Pascal;
- в **VK Видео** — Geany - программировать просто. Первая программа на Pascal.

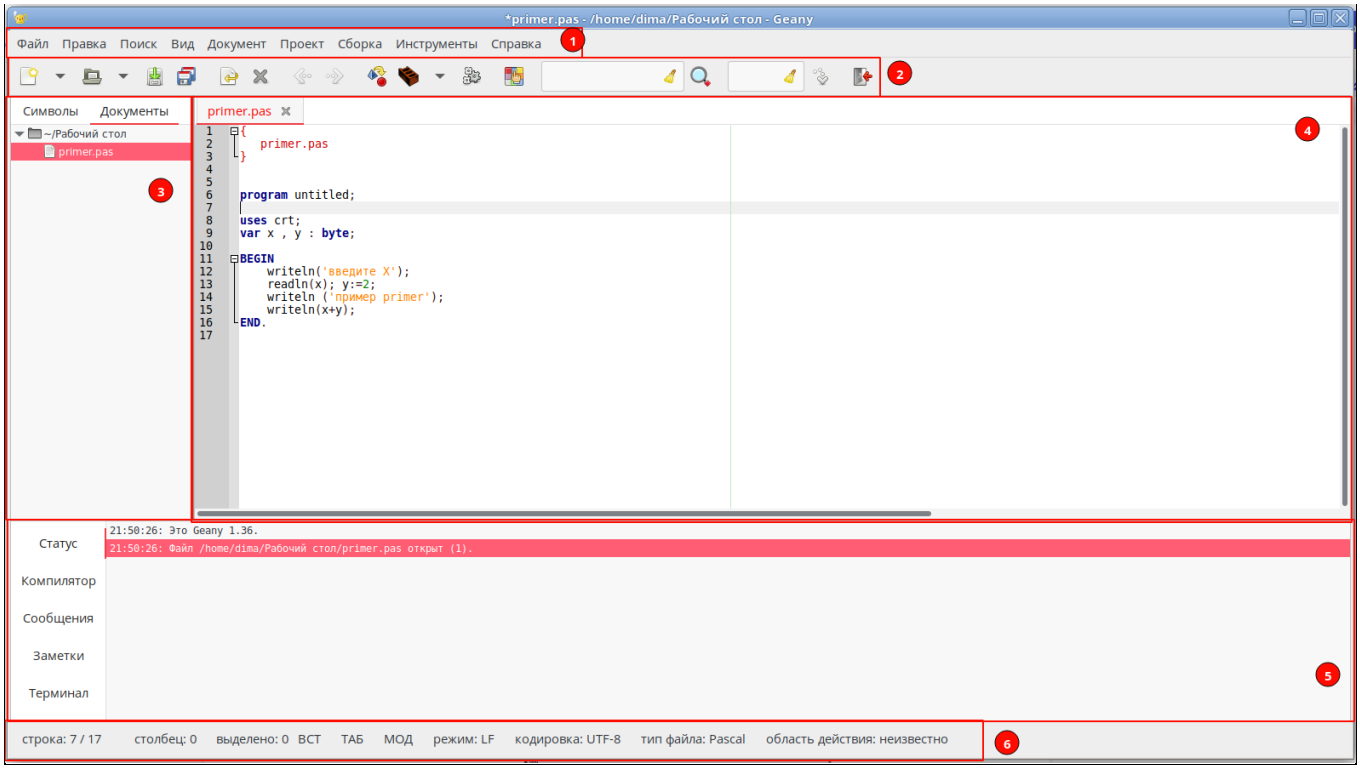
На наших каналах вы также сможете найти много другой полезной информации.

Основные функции **Geany**:

- подсветка синтаксиса;
- поддержка большого количества кодировок;
- сворачивание блоков кода;
- автозавершение имён;
- работа со сниппетами (фрагментами кода);
- автоматическое закрытие тегов *xml* и *html*;
- поддержка языков *c*, *java*, *php*, *html*, *python*, *perl*, *pascal* и других;
- списки имен;
- навигация по коду;
- отладка (требуется плагин **geanygdb**);
- использование контекстной документации **man**, **devhelp**;
- сборка — система для компиляции и исполнения кода;
- простое управление проектом;
- интерфейс для модулей.

Основное окно редактора состоит из *6 основных блоков*:

1. Строка основного меню.
2. Панель инструментов с кнопками.
3. Боковая панель.
4. Основное поле редактора.
5. Панель сообщений.
6. Панель состояний.



Установка

Для установки необходимо перейти в сеанс пользователя root:

```
su -
```

и выполнить команду:

```
dnf install geany
```

также необходимо установить компилятор языка Pascal:

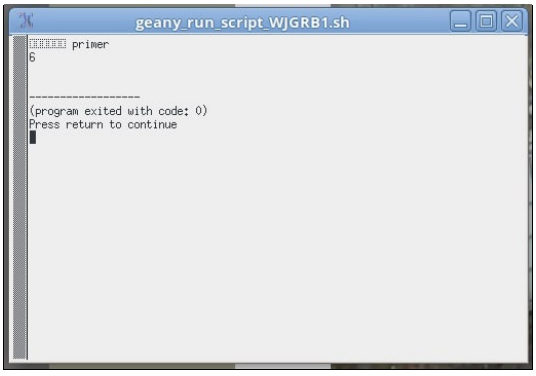
```
dnf install fpc
```

Запуск доступен из «**Меню**» - «**Программирование**» - «**Среда разработки Geany**».

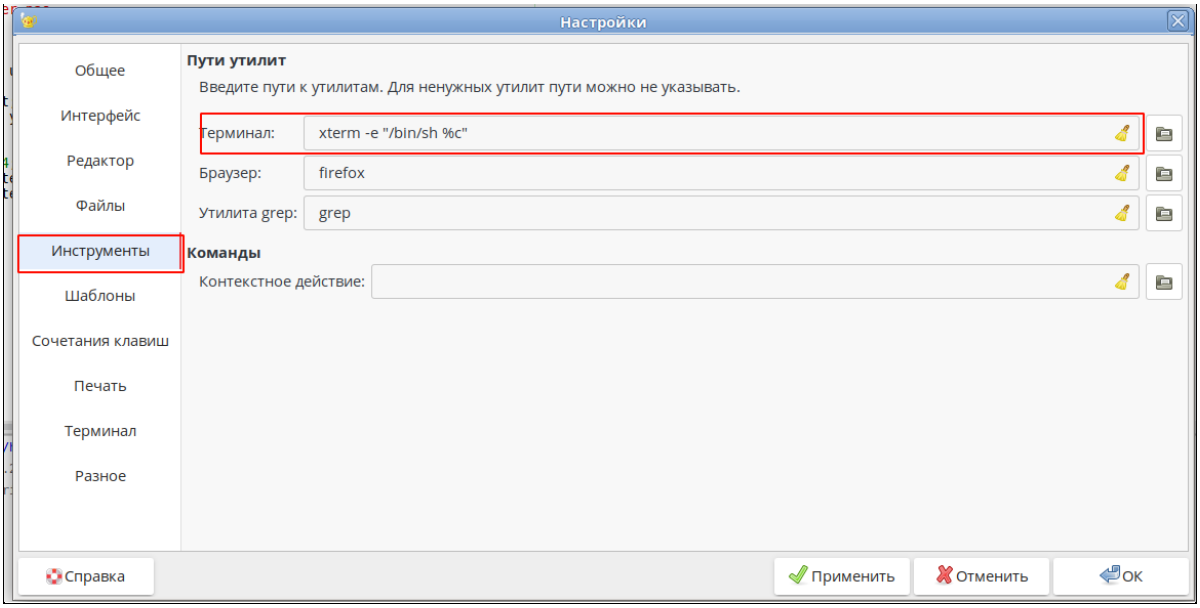
Замена терминала

По умолчанию для запуска скомпилированной программы используется программа **xterm**. Если она не установлена, это можно сделать командой:

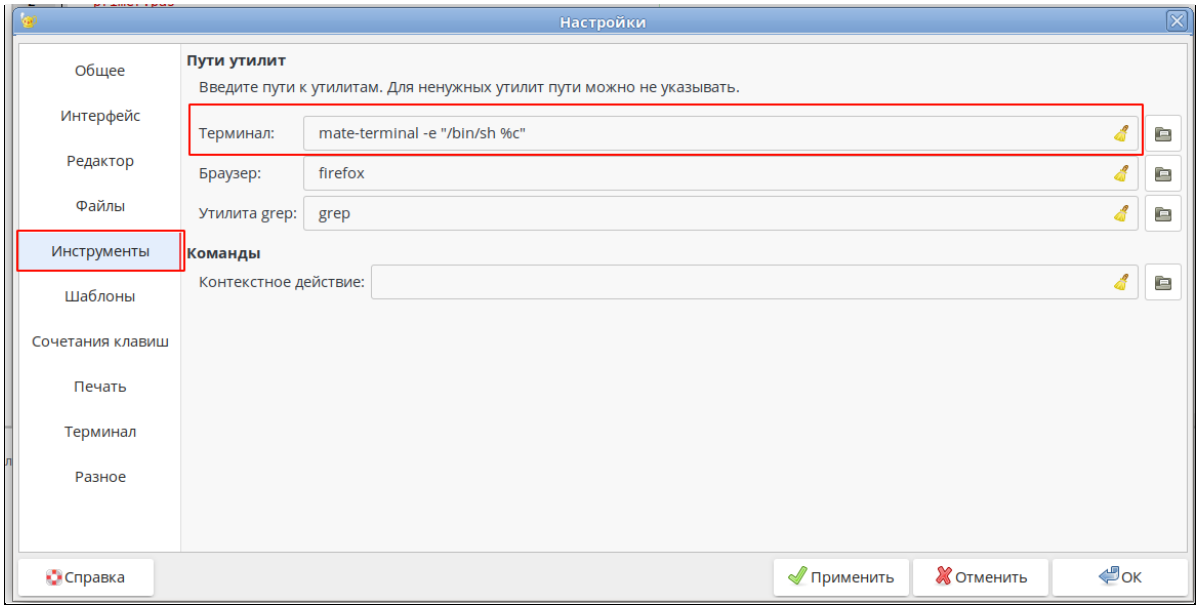
```
dnf install xterm
```



Терминал можно заменить на стандартный. Для этого необходимо перейти в **Настройки** («**Правка**» - «**Настройки**»). В появившемся окне в пункте «**Инструменты**», в поле «**Терминал**» необходимо заменить **xterm** на **mate-terminal**.

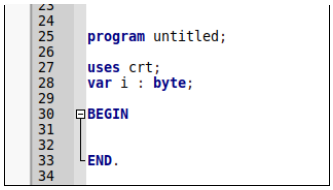


После сохранения внесенных изменений программа по умолчанию будет запускаться в стандартном для **MATE** терминале.



Простая программа на языке pascal

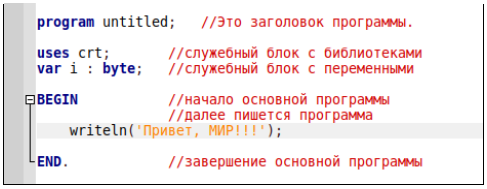
Для создания новой программы в **Geany** необходимо выбрать пункт меню «**Файл**» - «**Создать из шаблона**» - «**program.pas**». Откроется шаблон для написания кода:



```
24
25  program untitled;
26
27  uses crt;
28  var i : byte;
29
30  BEGIN
31
32
33  END.
34
```

Затем необходимо сохранить файл программы («**Файл**» - «**Сохранить**»).

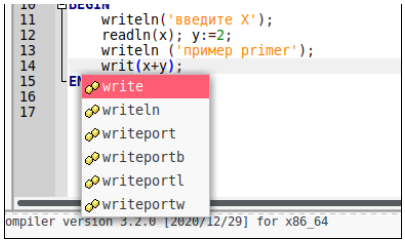
Далее следует написать основной код программы. Т.к. рассматривается простейшая программа, можно использовать в качестве основного кода программы вывод текстовой строки «*Привет, МИР!!!*» в терминал.



```
program untitled;   //Это заголовок программы.

uses crt;           //служебный блок с библиотеками
var i : byte;       //служебный блок с переменными

BEGIN               //начало основной программы
                    //далее пишется программа
    writeln('Привет, МИР!!!');

END.                //завершение основной программы
```

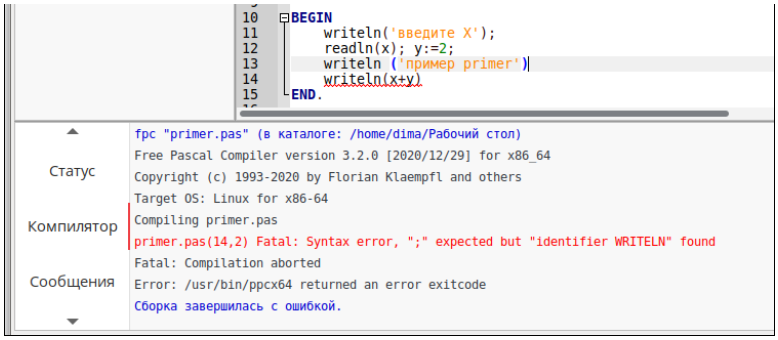
В процессе написания текста программы постоянно отображаются подсказки. Если необходимая команда есть в подсказке, можно

выбрать её двойным нажатием *ЛКМ* или клавишами *вверх/вниз + Enter*.



После того как программа написана, необходимо ее преобразовать в понятный процессору набор команд. Для этого существует компилятор. Одновременно с компиляцией происходит проверка текста программы на наличие ошибок. Компиляция запускается в пункте меню «**Сборка**» - «**Скомпилировать**».

Если в тексте программы есть синтаксические ошибки, компилятор сообщит об этом и подчеркнет строку с ошибкой красной линией.



Ошибку необходимо исправить и повторить компиляцию. Данные действия выполняются до тех пор, пока все ошибки не будут исправлены и компиляция не будет завершена успешно.

После успешной компиляции можно проверить работу программы. Запустите её на исполнение «**Сборка**» - «**Выполнить**».

Откроется окно терминала и программа начнет выполняться. Останется только проконтролировать правильность выполнения написанной программы, при необходимости исправить и повторить компиляцию.

Установка Lazarus

Установка
Обзор программы
Пример работы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: lazarus-2.2.2

Lazarus – это интегрированная среда разработки (IDE) и компилятор для языка программирования **Pascal**, который строится на основе библиотеки компонентов Free Pascal (FPC).

Особенности **Lazarus**:

- **Кроссплатформенность**. *Lazarus* позволяет разрабатывать приложения, которые могут работать в различных операционных системах, таких как *Windows*, *Linux*, *macOS* и других без изменений в исходном коде. Данная возможность поддерживается благодаря использованию *Free Pascal Compiler*.
- **Визуальное программирование**. *Lazarus* предоставляет визуальный редактор форм, который позволяет разработчикам создавать интерфейс приложения методом перетаскивания. Этот подход значительно упрощает создание пользовательских интерфейсов и улучшает процесс разработки.
- **Компонентная модель**. *Lazarus* предоставляет богатую библиотеку компонентов, которые можно использовать для создания различных элементов интерфейса и функциональности приложения. Компоненты могут быть переиспользованы, что способствует повышению производительности и уменьшению объема кода.
- **Отладка**. *Lazarus* предоставляет возможности для отладки кода, что помогает выявлять и устранять ошибки в процессе разработки.
- **Поддержка множества стандартов**. *Lazarus* соответствует различным стандартам *Pascal*, включая **Turbo Pascal** и **Delphi**, что делает его подходящим для разработчиков, знакомых с данными окружениями.

Lazarus популярен среди разработчиков, которые хотят использовать язык **Pascal** для создания кроссплатформенных приложений с удобным визуальным редактором форм и богатыми возможностями компонентной модели. Он особенно популярен среди разработчиков, знакомых с **Borland Delphi**, так как предоставляет схожий опыт разработки и привычный интерфейс.

Установка

Для установки **Lazarus** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install lazarus
```

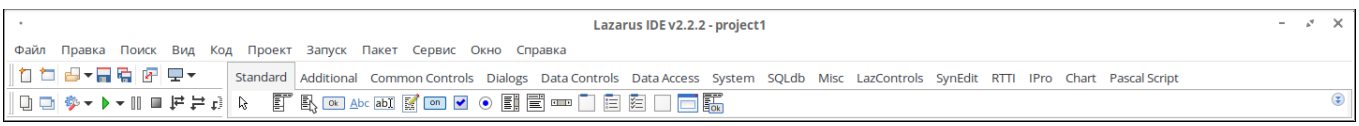
После установки запуск программы доступен из «**Главного меню**» — «**Программирование**» — «**Lazarus**» или через терминал (с правами **непривилегированного** пользователя) командой:

```
startlazarus
```

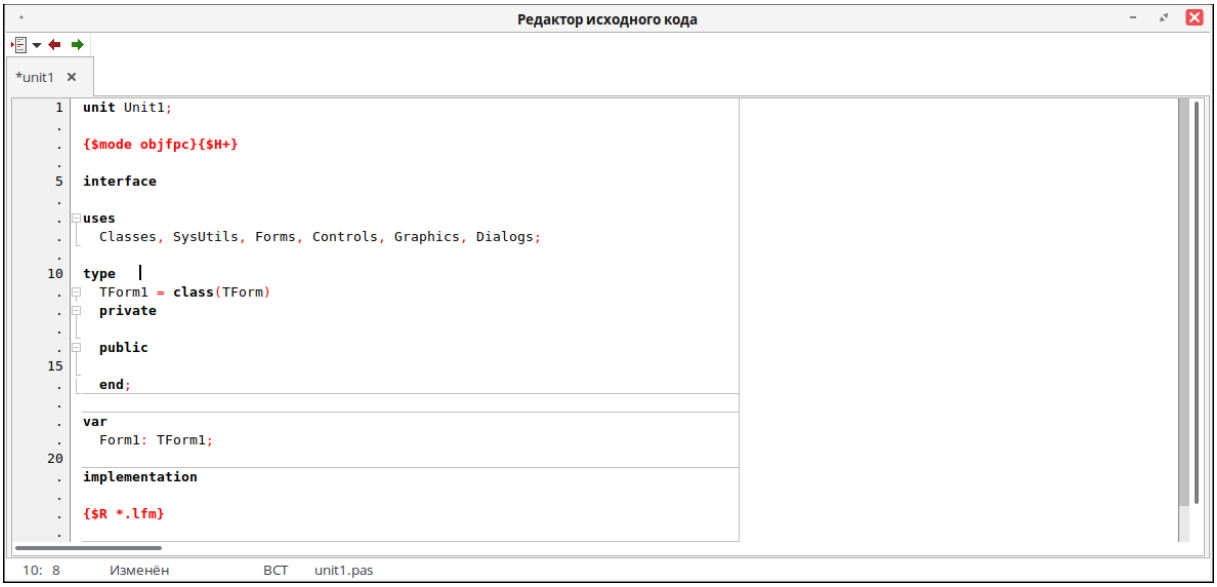
Обзор программы

Программа состоит из нескольких основных компонент:

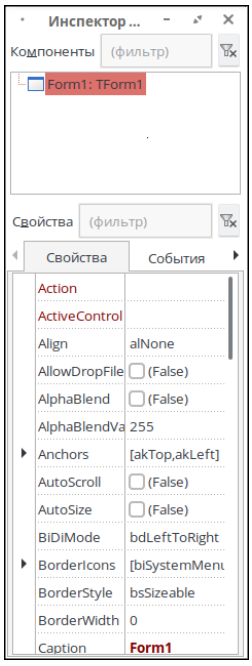
1. **Главное меню** – содержит основное меню, панели инструментов и область для работы с проектами и файлами кода. Здесь можно создавать, открывать и редактировать проекты, а также управлять компонентами и кодом приложения.



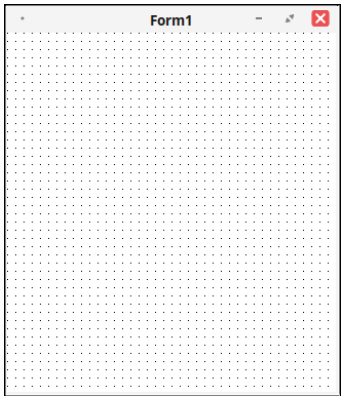
2 . **Редактор кода** – предназначен для написания и редактирования исходного кода приложения. Он обеспечивает подсветку синтаксиса, автозавершение и другие функции для облегчения работы с кодом.



3 . **Инспектор объектов** (панель объектов) – предоставляет доступ к свойствам и событиям выбранного компонента. Здесь можно настраивать свойства компонентов и устанавливать обработчики событий.

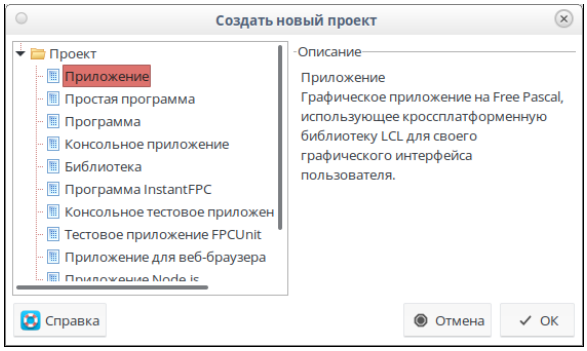


4. **Окно форм** – позволяет создавать и редактировать пользовательские формы, на которых размещаются графические компоненты для создания интерфейса приложения.



Пример работы

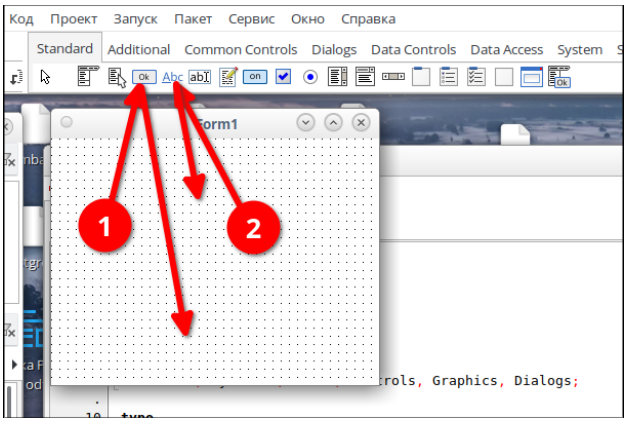
Для создания нового проекта в главном меню выберите «**Проект**» – «**Создать проект**». Появится окно, в котором предлагается выбрать тип проекта.



Для создания графического приложения выберите «**Приложение**» и нажмите «**OK**».

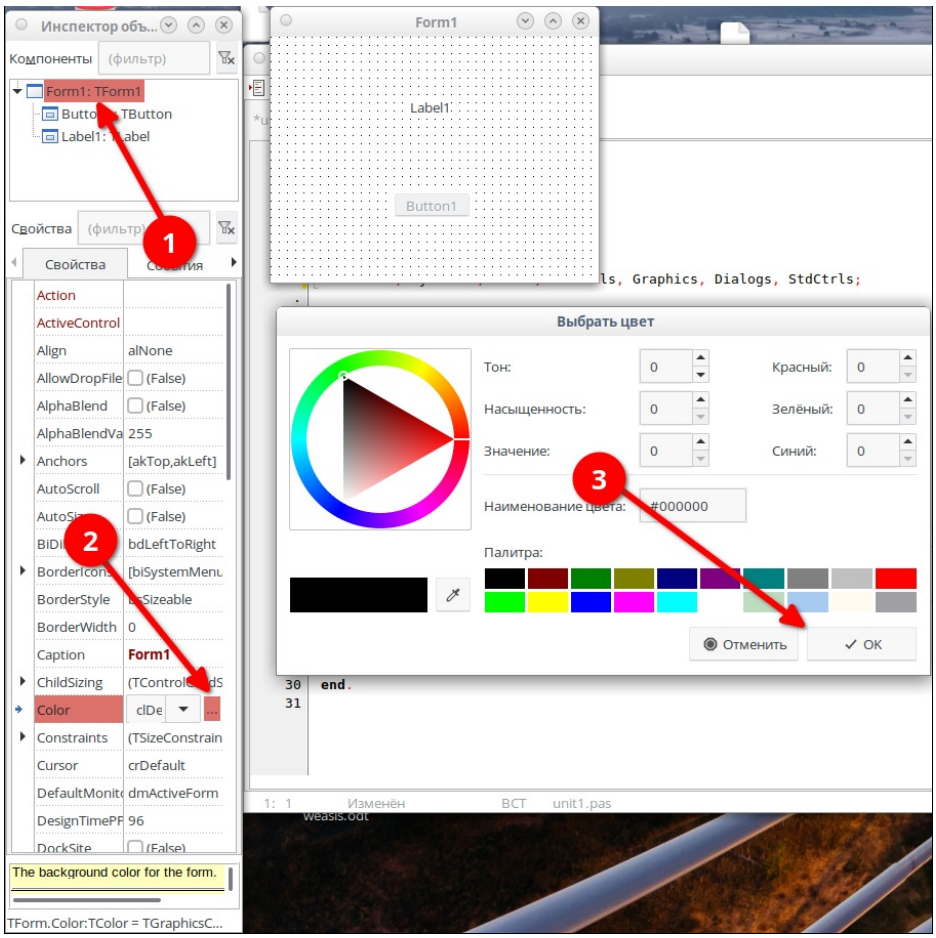
В меню с объектами выберите необходимые объекты:

- 1 – кнопка (*button*);
- 2 – текстовое поле для вывода информации (*label*).

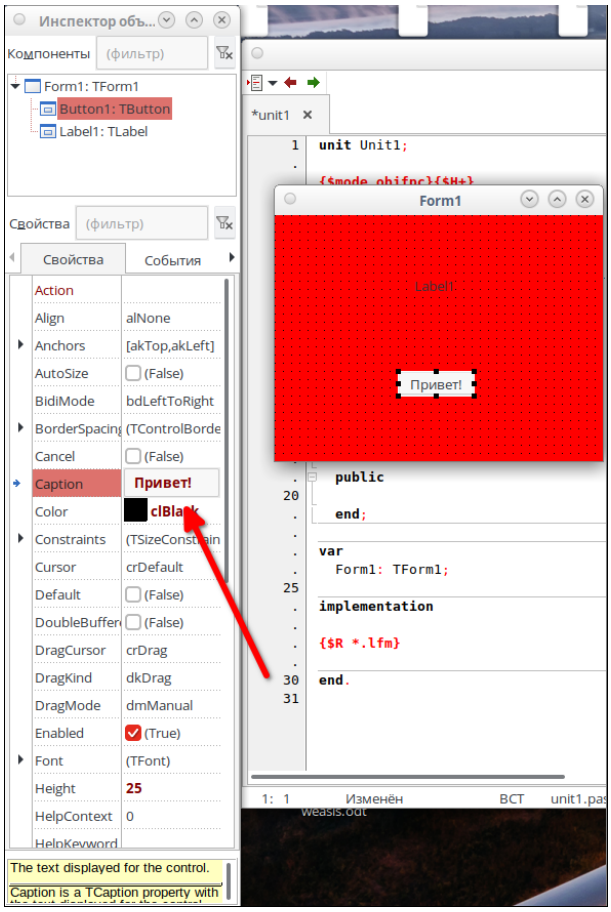


Доступно изменение размера и положения объектов.

В инспекторе объектов можно определить различные настройки для объектов, в примере будет изменен цвет фона. Для этого в окне инспектора объектов в дереве объектов выберите **Form1**, для параметра **Color** выберите необходимый цвет.



Измените надпись на кнопке. В окне инспектора объектов выберите **Button1** и в разделе «**Свойства**» укажите собственное название кнопки в параметре **Caption**.

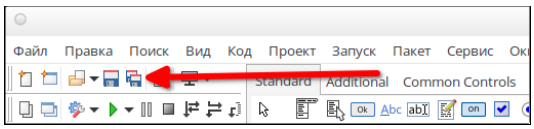


Для **Label1** удалите содержимое параметра **Caption**.

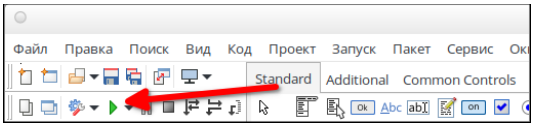
После этого можно создать код для кнопки – дважды щелкните по кнопке, откроется редактор кода. Напишите программный код для действия, например:

```
procedure TForm1.Button1Click(Sender: TObject);
begin
 Label1.Caption:='Привет мир!';
end;
```

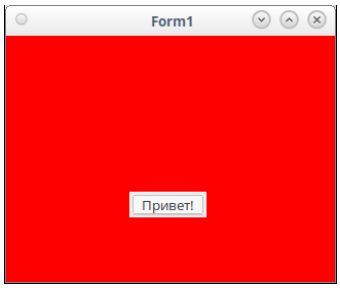
Сохраните проект – в главном меню нажмите «**Сохранить все**» или комбинацию клавиш **Shift+Ctrl+S**. Проект рекомендуется сохранять в отдельный каталог.



Запустите программу – в главном меню нажмите «**Запуск**» или клавишу **F9**.



При удачной компиляции будет открыто окно созданной программы.



Нажмите на кнопку – результат работы отобразится на экране.

В данном примере было рассмотрено создание простейшей программы для начала работы пользователя с **Lazarus**.

С помощью **Lazarus** можно разрабатывать разнообразные приложения – от простых оконных до сложных программ с графическим интерфейсом.

Установка QT Creator

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Qt Creator - 6.0.2

Qt Creator — кроссплатформенная свободная *IDE* для разработки на **C**, **C++**, **QML** и **python**. Разработана **Trolltech** для работы с фреймворком **Qt**.

Включает в себя графический интерфейс отладчика и визуальные средства разработки интерфейса как с использованием **QtWidgets**, так и **QML**.

Для установки **qtcreator** перейдите в сеанс пользователя root:

```
su -
```

Установка **qtcreator** в РЕД ОС осуществляется следующей командой:

```
dnf install qt-creator libdrm
```

Для использования **QML** необходимо установить дополнительные библиотеки следующей командой:

```
dnf install qt5-qtquickcontrols2 qt5-qtquickcontrols2-devel
```

Запуск *IDE* доступен из «**Меню**» - «**Программирование**» - «**Qt Creator**» или выполнить команду от локального пользователя:

```
qtcreator
```

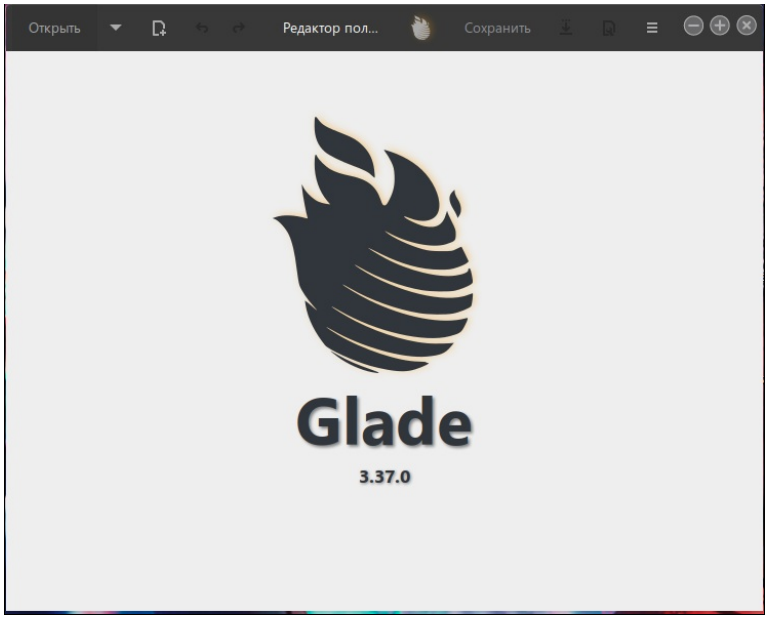


Установка Glade

Glade - это приложение для визуального создания графических интерфейсов на **GTK+**.

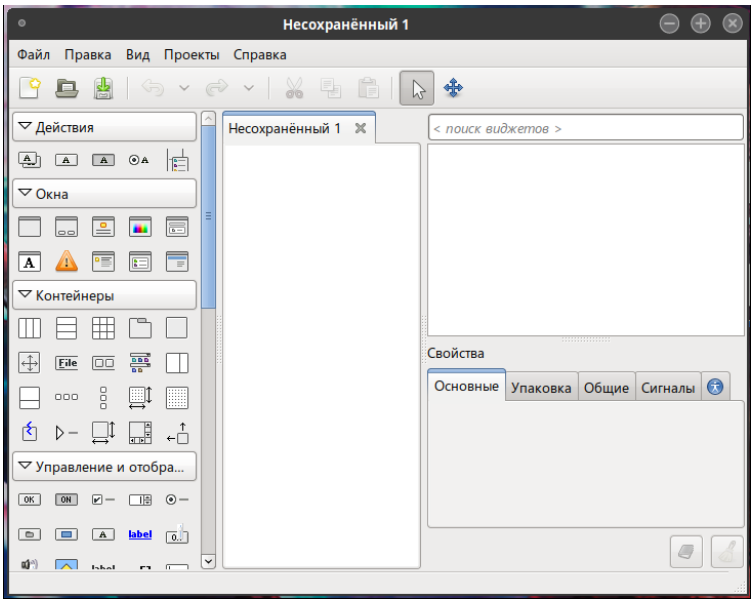
Установка производится командой:

```
dnf install glade
```



Также для поддержки старого типа **ui** файлов **GTK2** в РЕД ОС есть возможность поставить **glade** следующей командой:

```
dnf install glade3
```



Запуск доступен из «**Меню**» - «**Программирование**» - «**Glade**».

Установка Code::Blocks

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** Codeblocks - 20.03

Code::Blocks — свободная кроссплатформенная среда разработки.

Code::Blocks написана на **C++** и использует библиотеку **wxWidgets**. Имея открытую архитектуру, может масштабироваться за счёт подключаемых модулей. Поддерживает языки программирования **C**, **C++**, **D**, **Fortran**.

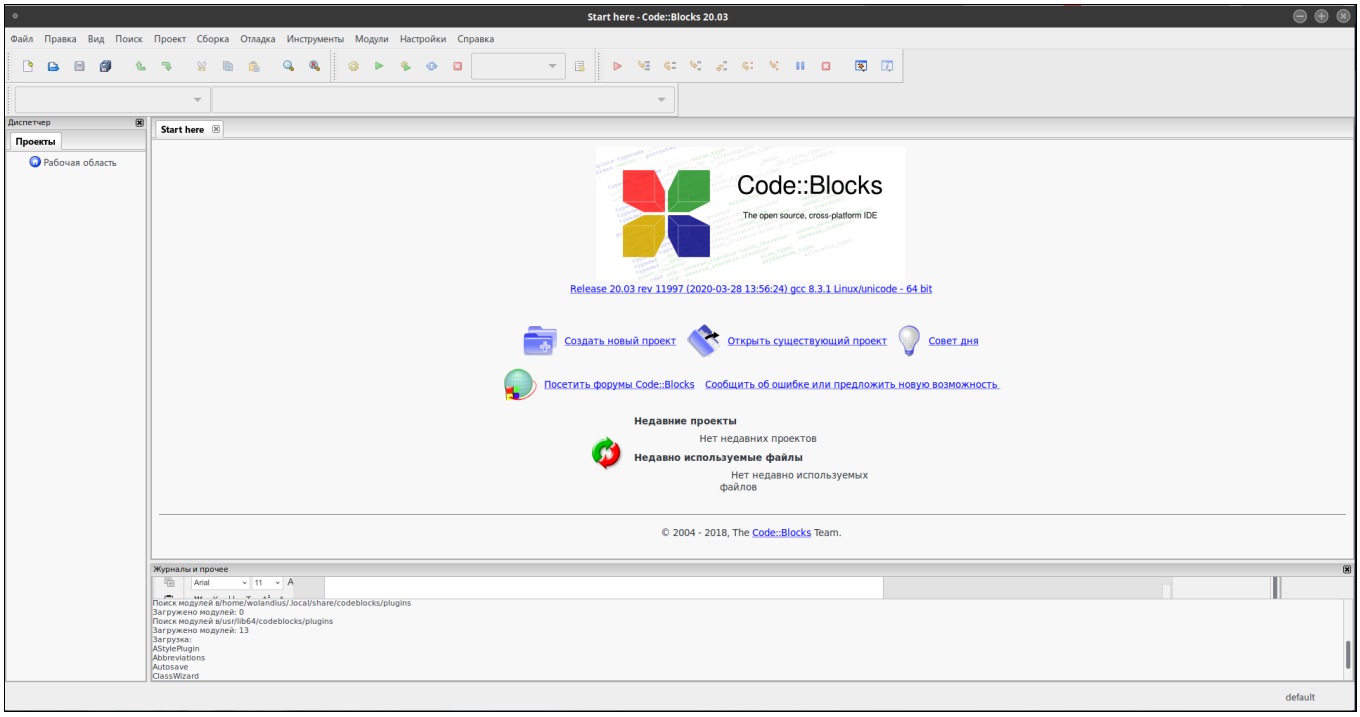
Для установки программы перейдите в сеанс пользователя root:

```
su -
```

и выполните команду:

```
dnf install codeblocks
```

Запуск *IDE* доступен из «**Меню**» - «**Программирование**» - «**Среда разработки Code::Blocks**».



Установка Visual Studio Code

Вариант 1. Установка с помощью менеджера пакетов
Вариант 2. Установка с помощью flatpak

Для установки **Visual Studio Code** выберите один из вариантов в зависимости от ваших предпочтений.

Вариант 1. Установка с помощью менеджера пакетов

Для установки **Visual Studio Code** выполните следующие действия:

1. Импортируйте ключ (для проверки подлинности пакетов):

```
sudo rpm --import https://packages.microsoft.com/keys/microsoft.asc
```

2. Создайте файл подключения репозитория **Visual Studio Code**:

```
sudo nano /etc/yum.repos.d/vscode.repo
```

Добавьте в него следующий текст:

```
[code]
name=Visual Studio Code
baseurl=https://packages.microsoft.com/yumrepos/vscode
enabled=1
gpgcheck=1
gpgkey=https://packages.microsoft.com/keys/microsoft.asc
```

3. Обновите кеш пакетов:

```
sudo dnf check-update
```

4. Установите пакет **Visual Studio Code**:

```
sudo dnf install code
```

5. После установки запустите **Visual Studio Code** из «**Меню**» — «**Программирование**» либо запустите программу, выполнив команду в терминале:

```
code
```

Вариант 2. Установка с помощью flatpak

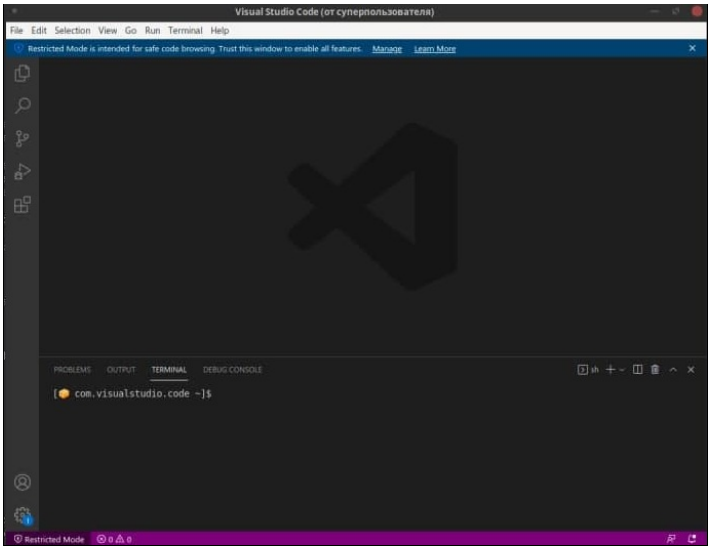
Для установки данной многофункциональной среды разработки потребуется установить **flatpak** в соответствии с инструкцией «Flatpak - изолированная среда для запуска приложений» и добавить репозиторий **flathub** с помощью команды, указанной в п. «Добавление репозиториев».

Следующим шагом является установка **vscode**, для этого потребуется выполнить следующее действие:

```
flatpak install flathub com.visualstudio.code
```

Дождитесь завершения загрузки и запустите **vscode** из «**Меню**» — «**Программирование**» либо запустите программу, выполнив команду в терминале:

```
flatpak run com.visualstudio.code
```


Visual Studio Code (от суперпользователя)
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
com.visualstudio.code ~]$
Restricted Mode

Установка VSCodium

Установка
Изменение языка интерфейса
Установка плагинов

Окружение

- **Версия РЕД ОС:** 8
- **Конфигурация:** Рабочая станция
- **Версия ПО:** codium-1.91.1

VSCodium - это ответвление популярного редактора кода **Microsoft Visual Studio**. Он построен с использованием наработок проекта **Atom** и платформы **Electron**, основанной на кодовой базе **Chromium** и **Node.js**. Редактор предоставляет встроенный отладчик, инструменты для работы с **Git**, средства рефакторинга, навигации по коду, автодополнения типовых конструкций и контекстной подсказки. Поддерживается более 100 языков программирования и технологий. Для расширения функциональности **Visual Studio Codium** предоставляется возможность установки дополнений.

Вы можете подробнее ознакомиться с установкой и работой в **VSCodium**, просмотрев наши обучающие видео:

- на **RuTube** — Установка IDE VSCodium в РЕД ОС;
- в **Яндекс.Дзен** — Установка IDE VSCodium в РЕД ОС;
- в **VK Видео** — Установка IDE VSCodium в РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки **vscodium** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install codium
```

После установки запуск программы доступен из «**Меню**» — «**Программирование**» — «**VSCodium**» или через терминал (с правами локального пользователя) командой:

```
codium
```

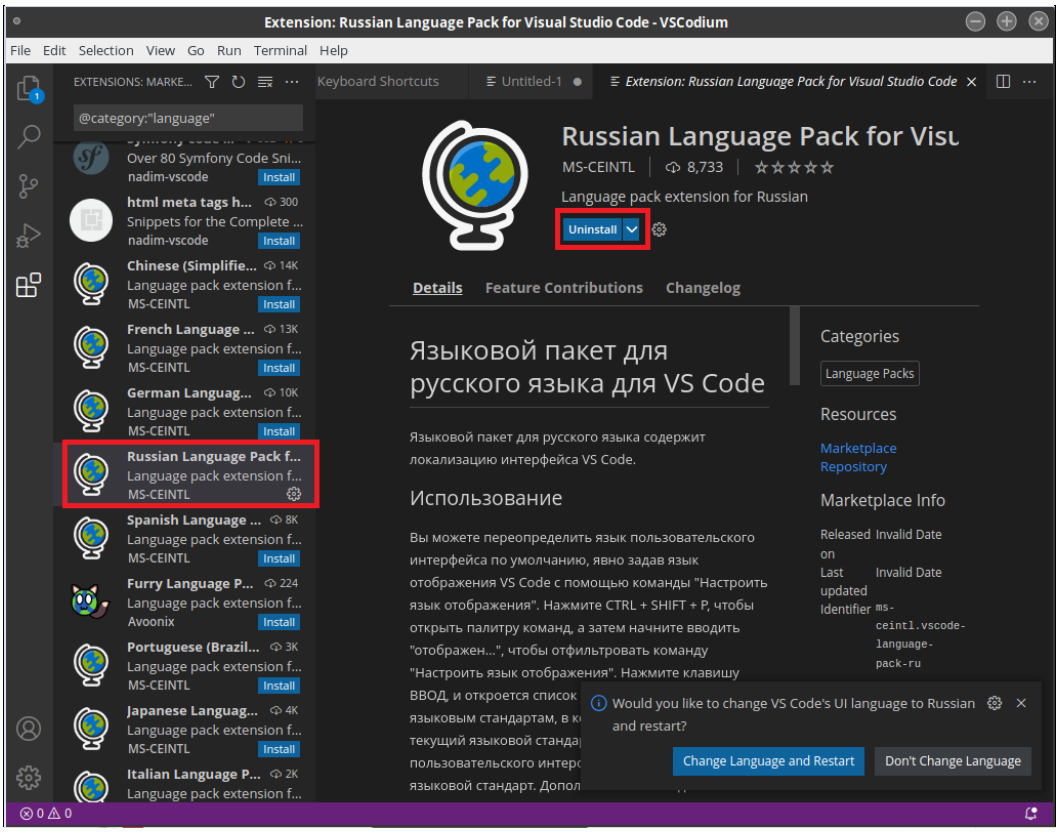
При первом запуске появится окно настройки оформления.

Изменение языка интерфейса

Для изменения языка интерфейса откройте меню **Command Palette** на вкладке **View** и введите **Configure Display Language**.

В появившемся списке выберите нужный пакет языков. Если он отсутствует, нажмите **Install additional languages**.

В строке поиска введите название языкового пакета, например «**Russian Language Pack**» и нажмите **install**.



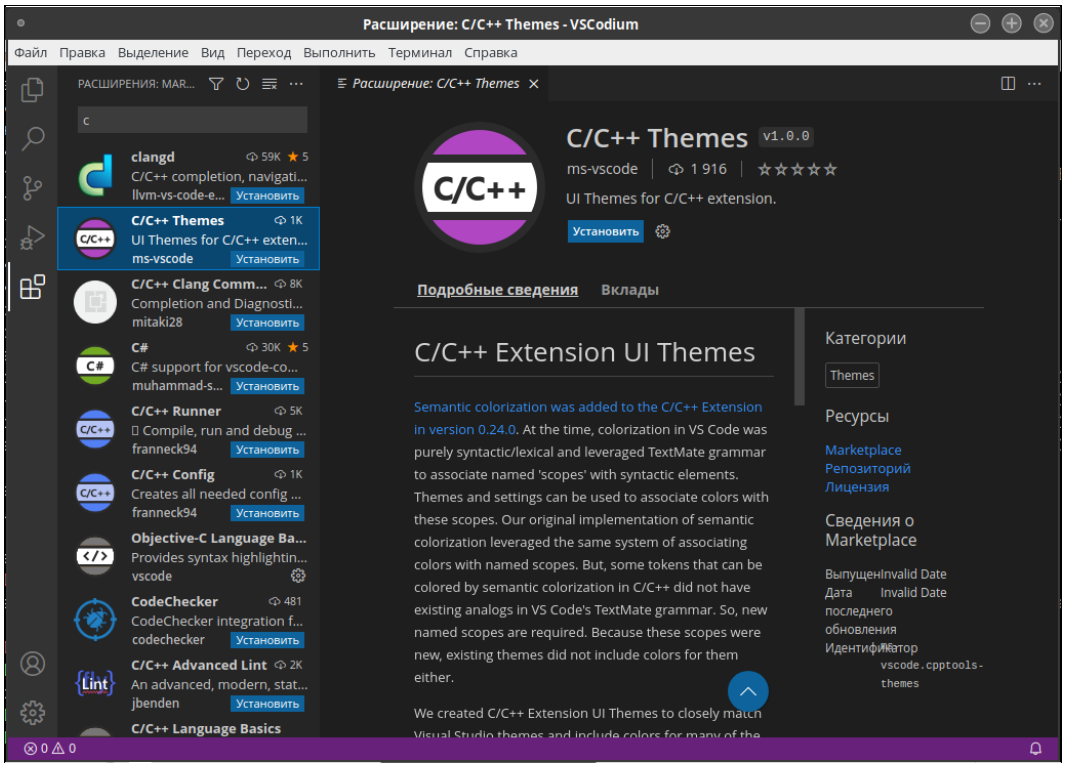
После завершения установки нажмите на кнопку **Change Language and Restart**, чтобы перезапустить **VSCodium**. После перезагрузки программы будет применён выбранный язык.

Установка плагинов

Для установки и просмотра плагинов выберите пункт **Расширения** на панели слева или нажмите сочетание клавиш **Ctrl+Shift+X**.

Введите название плагина в строке поиска, выберите дополнение и нажмите **install**.

Каждое расширение в списке включает краткое описание, имя издателя, количество загрузок и пятизвездочный рейтинг.



Установка Arduino IDE

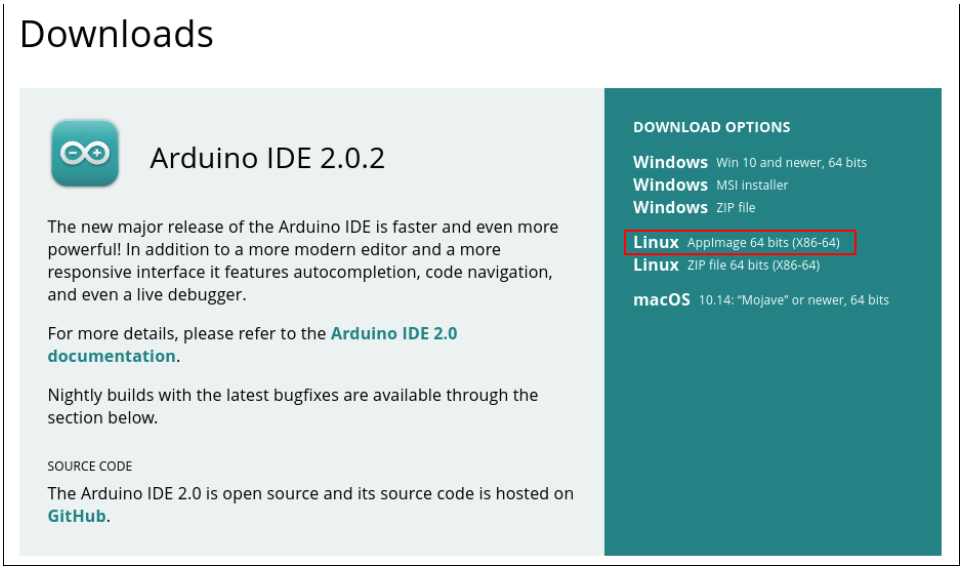
Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** arduino IDE 2.0.2

Arduino IDE — интегрированная среда разработки, предназначенная для создания и загрузки программ на платформу **Arduino**.

Для установки **Arduino IDE** перейдите на официальный сайт разработчика.

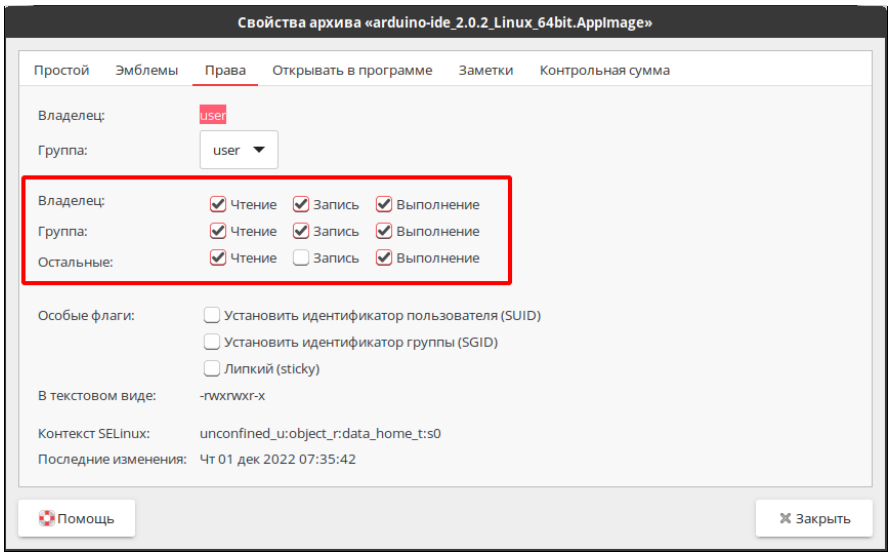
В разделе **Downloads** выберите «**Linux AppImage 64 bits (x86-64)**» и скачайте приложение.



Для запуска приложений в формате *Applimage* необходимо назначить файлу права на исполнение. Сделать это можно двумя способами:

1. Через графический интерфейс.

Перейдите в папку с загруженным файлом, вызовите контекстное меню, нажав по файлу ПКМ, выберите пункт «**Свойства**». После этого во вкладке «**Права**» активируйте флаг пункта «**Выполнение**» для необходимых пользователей и групп.



2. Через командную строку (потребуются права администратора или суперпользователя системы).

В терминале перейдите в папку с загруженным файлом (в примере **/home/user/Загрузки/**):

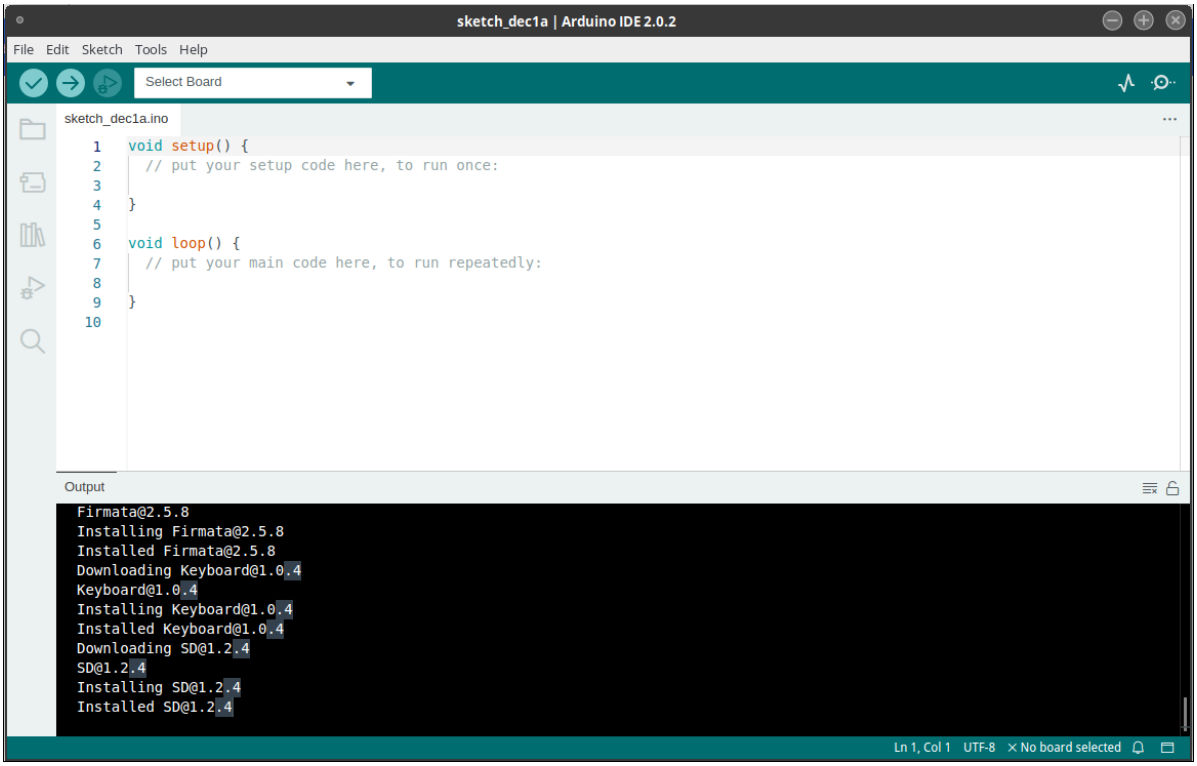
```
cd /home/user/Загрузки/
```

и выполните команду:

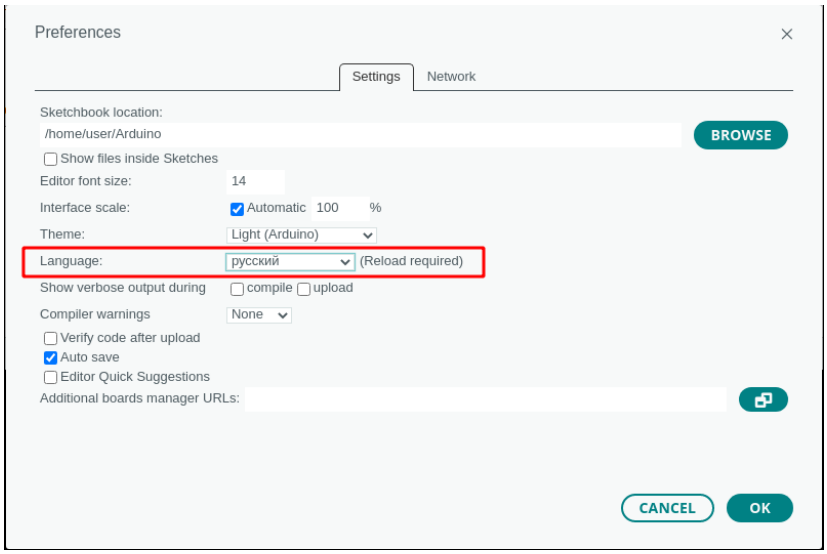
```
chmod +x arduino-ide_2.0.2_Linux_64bit.AppImage
```

Теперь приложение можно запустить, кликнув ЛКМ по файлу формата **.Applimage** или набрав в командной строке (с правами локального пользователя):

```
./arduino-ide_2.0.2_Linux_64bit.AppImage
```



Для смены языка программы выберите пункт меню «**File**» - «**Preferences...**», в открывшемся окне настроек выберите из списка необходимый язык (параметр **Language**).

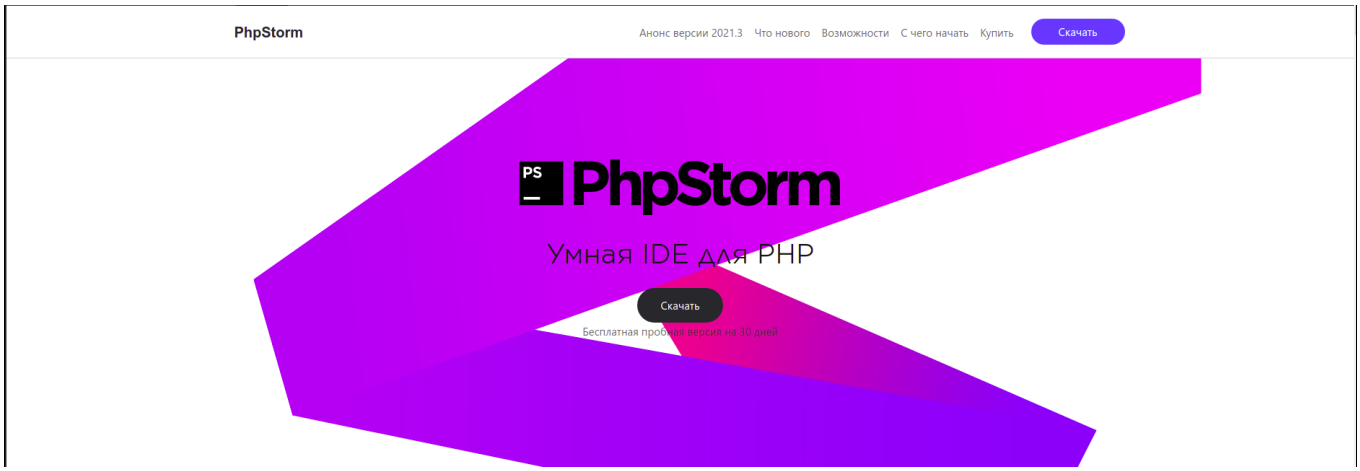


Здесь также доступны общие настройки интерфейса программы.

Установка PhpStorm

PhpStorm — коммерческая кросс-платформенная интегрированная среда разработки для **PHP**. Разрабатывается компанией **JetBrains** на основе платформы **IntelliJ IDEA**.

Скачать данную *IDE* можно по ссылке с официального сайта.



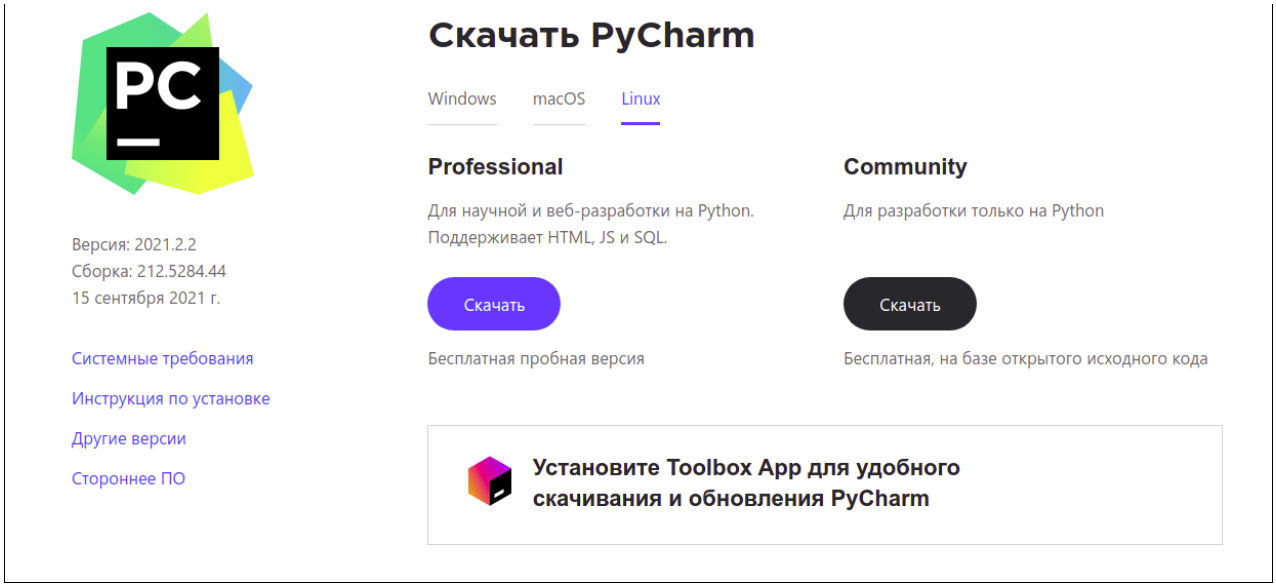
После скачивания необходимо распаковать архив **PhpStorm-202x.x.x.tar.gz**.

Для запуска перейдите в папку **PhpStorm-<версия>/bin** и запустите файл **phpstorm.sh**.

Установка PyCharm

Для установки данной многофункциональной среды разработки вам потребуется перейти на сайт разработчика данного ПО.

Выберите **community** или **professional** версию, нажмите кнопку «**Скачать**» и дождитесь завершения загрузки **tar.gz** архива.



Затем распакуйте архив в удобную для вас директорию.

Перейдите по пути **<путь_к_директории>/pycharm-202x.x/bin** в файловом менеджере или в терминале с помощью команды, например:

```
cd /home/user/Загрузки/pycharm-community-2022.1.3/bin/
```

Для начала установки вам потребуется запустить файл **pycharm.sh**:

```
./pycharm.sh
```

BlueFish - ПО для создания и редактирования интернет-приложений

Установка
Описание программы
Пример работы
Настройка CSS

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** bluefish-2.2.12-1

BlueFish — это текстовый редактор, представляющий собой интегрированную среду разработки (IDE). **BlueFish** основан на программе **KompoZer**, которую выпускало сообщество Mozilla как редактор для создания HTML-страниц или статичных сайтов. **BlueFish** стал полнофункциональным редактором для разработчиков программного обеспечения с поддержкой **HTML**, **CSS**, **JavaScript**, **PHP**, а также **C**, **C++** и ещё ряда языков программирования, однако, в первую очередь, он нацелен на создание веб-контента.

Основные возможности и достоинства **BlueFish**:

- поддержка большого количества открытых вкладок и документов;
- поддержка менеджмента проектов;
- мощный поиск и замена, позволяющие использовать регулярные выражения;
- неограниченное количество отмены и возврата совершенных действий;
- настраиваемая подсветка синтаксиса с поддержкой как пользовательских шаблонов, так и предустановленных шаблонов подсветки для **HTML**, **JavaScript**, **PHP**, **CSS**, **SQL**, **XML**, **Ruby**, **Python** и многих других языков;
- поддержка различных кодировок, по умолчанию работает в **UTF8**;
- хороший мастер для HTML-документов: таблицы, слои, фреймы и пр.;
- подсказки для HTML- и CSS-тегов со всеми их атрибутами;
- функциональные диалоги вставки различных объектов в документы;
- генератор большого количества превью для быстрого создания фотоальбомов или скриншотов страниц;
- настраиваемая пользователем панель инструментов для быстрого доступа к часто используемым функциям;
- автозакрытие тегов для HTML и XML-документов.

Вы можете подробнее ознакомиться с работой редактора **BlueFish**, просмотрев наши обучающие видео:

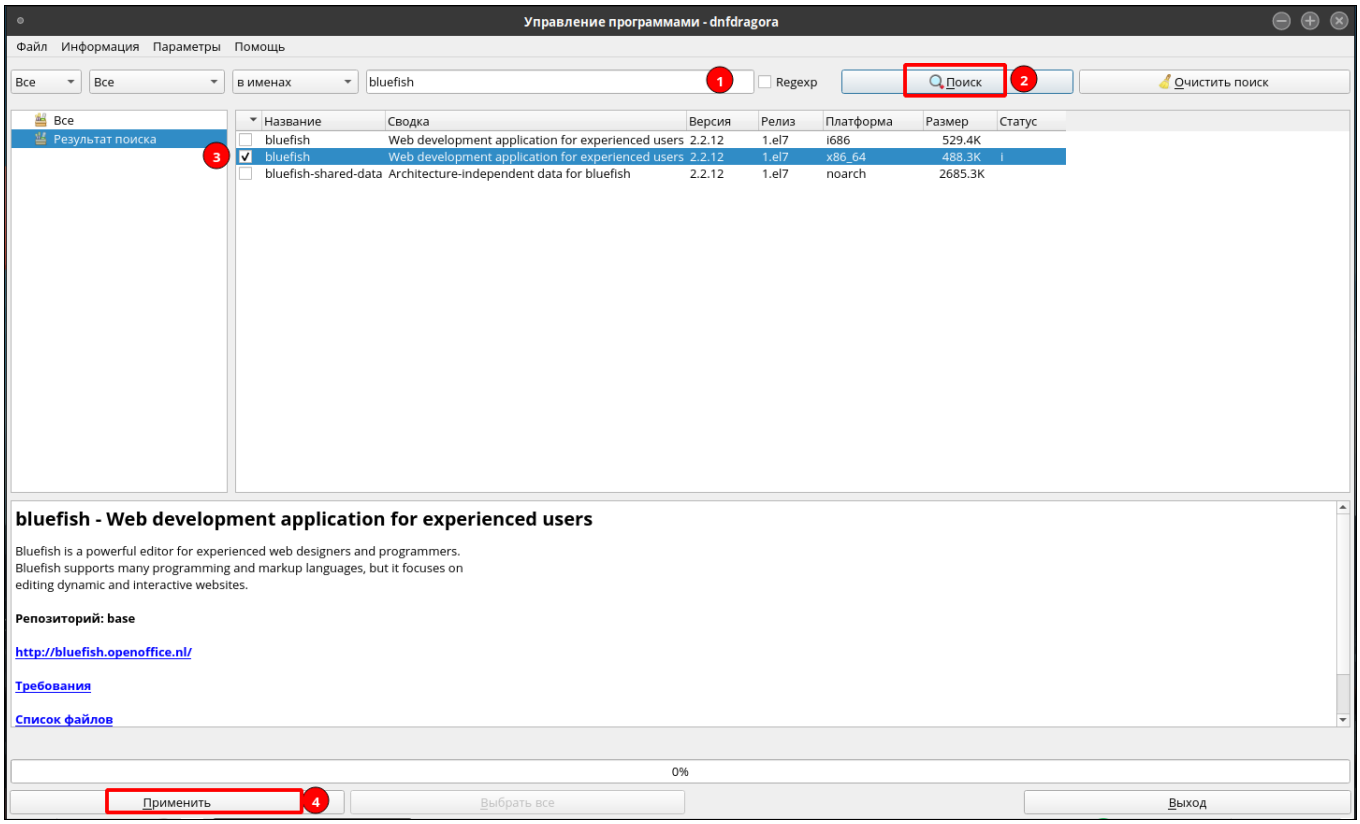
- на **RuTube** — Визуальный редактор для веб-страниц и простых сайтов BlueFish;
- в **Яндекс.Дзен** — Визуальный редактор для веб-страниц и простых сайтов BlueFish;
- в **VK Видео** — Визуальный редактор для веб-страниц и простых сайтов BlueFish.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Установить программу можно либо через графический менеджер пакетов, либо через терминал.

Для установки программы через графический менеджер пакетов **dnfdragora** перейдите в «**Главное меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**», выполните поиск необходимого пакета по ключевому слову «**bluefish**» и отметьте флагом пакет последней версии. После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



Для установки программы через терминал перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install bluefish
```

Дальнейшая работа в программе выполняется от **локального пользователя**.

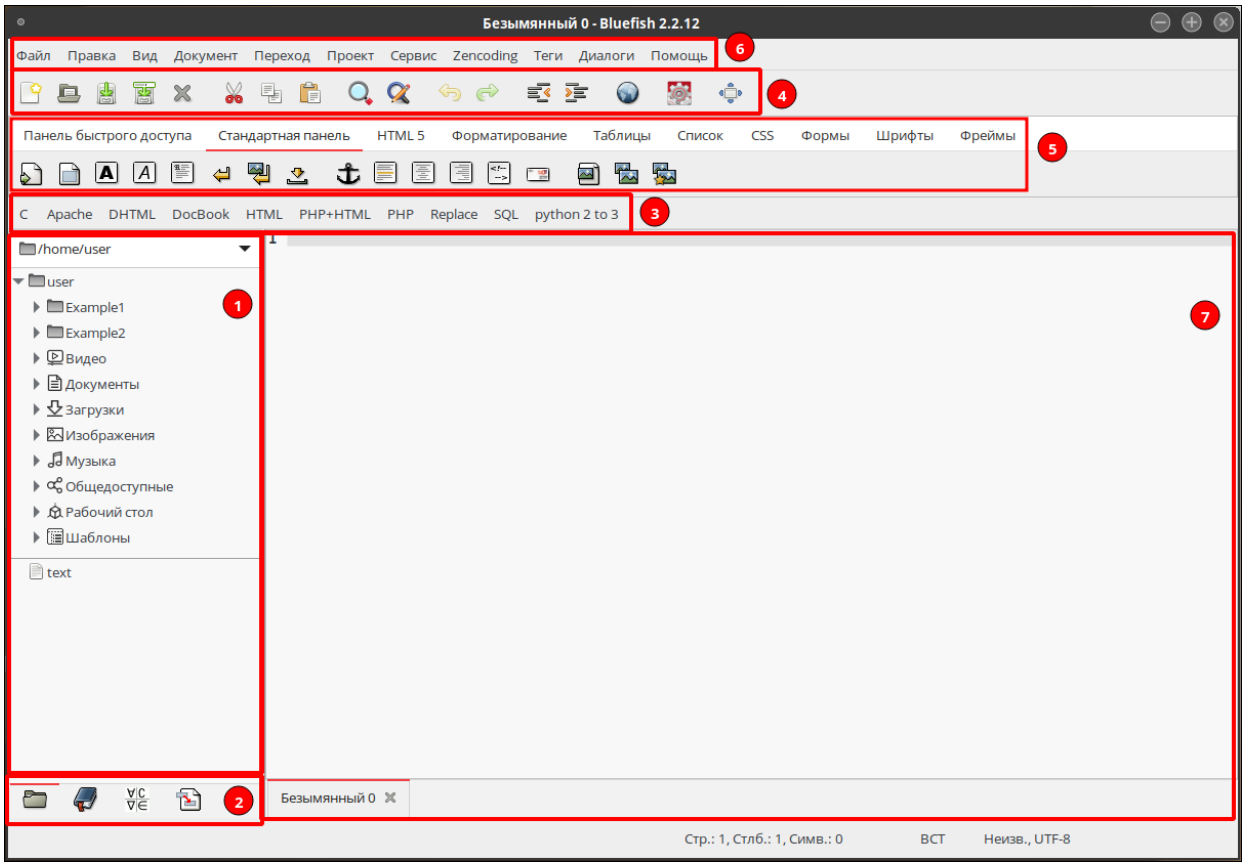
Завершите сеанс пользователя **root**:

```
exit
```

После установки программа будет доступна из «**Главного меню**» - «**Программирование**» - «**Веб-редактор BlueFish**». Если по каким-либо причинам раздел «**Программирование**» не появился в «**Главном меню**», перезагрузите систему.

Описание программы

Главное окно программы выглядит следующим образом:



1 - быстрый доступ к ряду возможностей программы, переключаемых вкладками панели **2**.

2 - панель, позволяющая переключать содержимое блока:

- панель обеспечения быстрого доступа к файловой системе для работы с файлами и каталогами (открывается по умолчанию);
- панель поиска;
- панель визуального выбора символов;
- панель выбора наиболее часто использующихся операций (дублируется на панели **3**).

3 - панель выбора наиболее часто использующихся операций;

4 - главная панель приложения;

5 - панель пиктограмм для определенных действий. В основном действия на данной панели относятся именно к созданию веб-страниц, как статических (на HTML), так и динамических (на PHP и/или JavaScript).

6 - главное меню программы, в котором собраны практически все возможности. Можно убрать показ всех верхних панелей, оставив только главное меню, и осуществлять доступ к каким-либо действиям или возможностям только через него - это может пригодиться в качестве альтернативы полноэкранному режиму - места на экране под текст больше, но и быстрый доступ ко всему функционалу программы остаётся.

7 - рабочая область программы, в котором отображается содержимое файлов проекта, с которым производится работа, и в котором и происходят основные события.

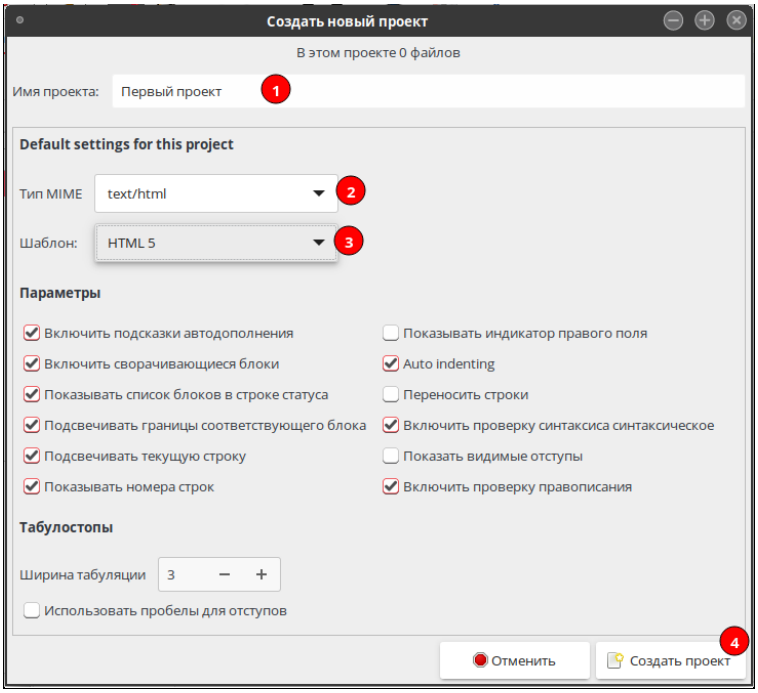
Пример работы

В качестве примера будет рассмотрено создание простейшего проекта с элементарной веб-страницей.

Для создания нового проекта в главном меню выберите «**Проект**» - «**Новый проект**». Откроется окно с базовыми параметрами нового проекта, в котором для HTML-страницы необходимо будет задать некоторые начальные значения:

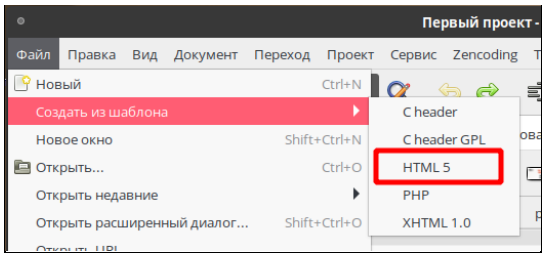
- в поле **Имя проекта** необходимо установить название для проекта;
- в поле **Тип MIME** - выбрать тип создаваемой страницы, в примере **text/html**;
- в поле **Шаблон** - выбрать тип шаблона для страницы, в примере **HTML5**;
- остальные параметры пока оставьте по умолчанию.

После этого нажмите **Создать проект**.

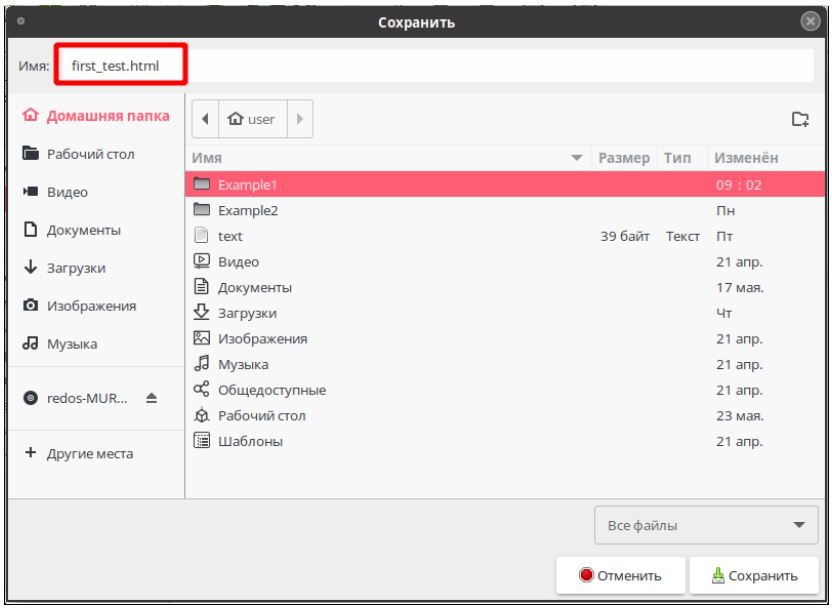


Откроется диалоговое окно с запросом имени файла — программа предлагает сразу сохранить проект. Можно оставить имя, заданное в настройках проекта, можно указать другое имя, также можно выбрать определённый каталог для проекта. После выбора каталога и имени нажмите **Сохранить**. Файл проекта будет иметь расширение **.bfproject**.

Затем в созданный проект необходимо добавить файл, для чего в главном меню выберите «**Файл**» - «**Создать из шаблона**» - «**HTML 5**».



Далее нужно сохранить () созданный файл, явно указав суффикс **.html**, поскольку редактор автоматически не присваивает расширения.



После всех выполненных действий перед вами будет открыта заготовка будущей веб-страницы. Графического способа создания веб-страниц данный редактор не имеет, поэтому работа с **BlueFish** требует хотя бы базовых знаний языка разметки HTML. В остальном редактор будет выводить всплывающие подсказки и описания тех или иных тегов.

Название страницы указывается в тегах `<title>` **Имя страницы** `</title>`.

Основное содержание страницы прописывается в тегах <body> **Содержание страницы** </body>.

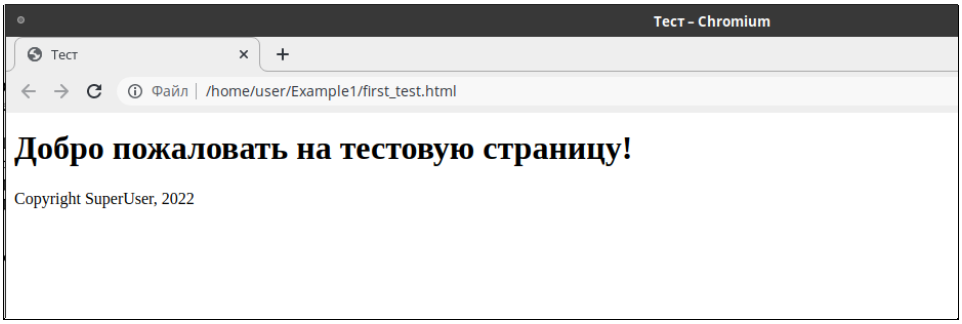
Для примера на страницу будет добавлен заголовок (теги <h1> **Заголовок** </h1>) и некоторый текст (**Текст**), а также авторские права (<footer> **Текст** </footer>).

Теги можно как прописать вручную, так и проставить, используя пункт главного меню «**Теги**» или вкладку **HTML** панели выбора наиболее часто использующихся операций.

Итоговый код страницы будет выглядеть следующим образом:

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title> Тест </title>
</head>
<body>
<h1> Добро пожаловать на тестовую страницу! </h1>
</body>
<footer> Copyright SuperUser, 2022 </footer>
</html>
```

Чтобы проверить, как страница выглядит в браузере, необходимо сначала сохранить внесенные в HTML-файл изменения, а затем в главном меню выбрать «**Сервис**» - «**Команды**» - «**Chromium**» (можно выбрать любой другой установленный в системе браузер).



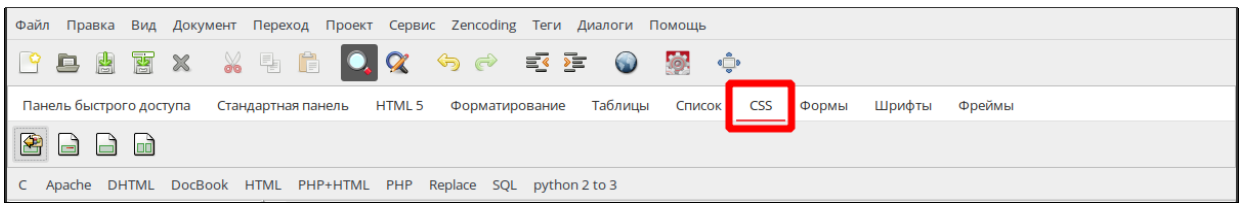
Настройка CSS

Для оформления страницы также можно применять различные стили. Для этого необходимо подключить таблицу стилей. Таблица стилей будет иметь расширение **.css**.

В качестве примера будет рассмотрено создание цветного фона для текста с авторскими правами (*Copyright SuperUser, 2022*).

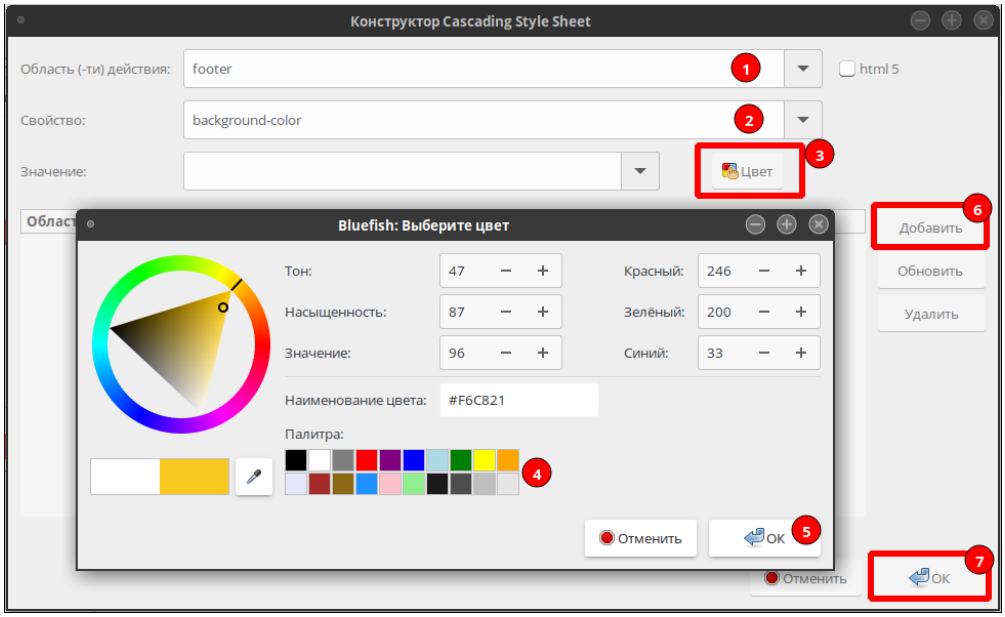
Для этого необходимо создать новый файл в проекте («**Файл**» - «**Новый**») и сохранить его с именем, например, **test.css**. Создание нового безымянного файла происходит сразу из HTML-шаблона, поэтому шаблонное содержимое можно просто удалить.

Для создания цвета фона для тега <footer> в панели быстрого доступа переключитесь на вкладку « **CSS**».



На панели выберите первую пиктограмму «**Создать таблицу стилей**» (), после чего откроется окно создания таблицы.

Укажите в «**Области действия**» тег footer, в поле «**Свойство**» из выпадающего списка выберите background-color, кнопка «**Цвет**» станет активной. Нажмите на кнопку «**Цвет**» для удобного выбора нужного цвета из палитры.



Нажмите«**ОК**». Заполнив все поля в окне, нажмите на кнопку « **Добавить**», затем «**ОК**».

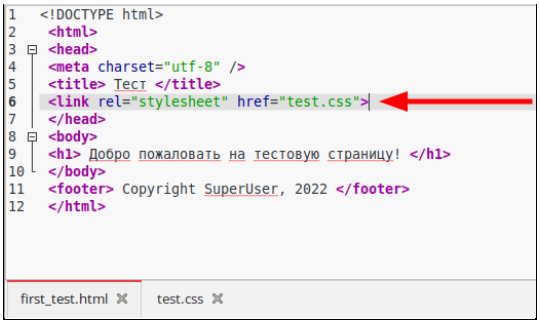
После этого в файл с таблицей стилей будет добавлена запись.

```
footer {
background-color: #F6C820;
}
```

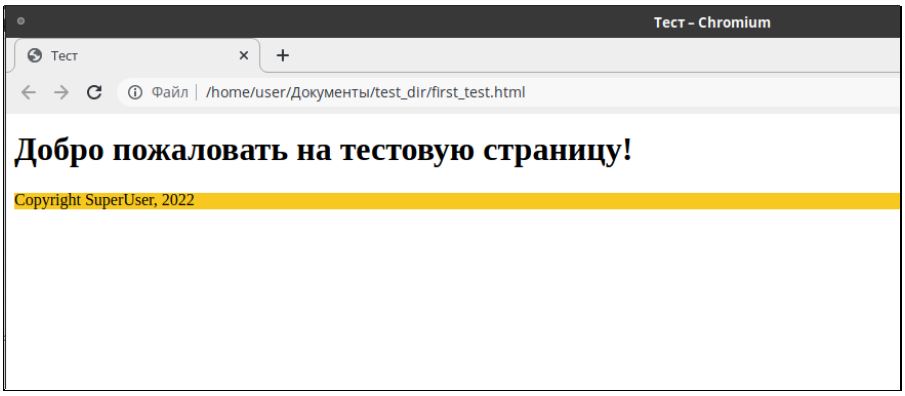
Сохраните CSS-файл.

Для того чтобы созданный стиль применился для созданного ранее HTML-файла, необходимо указать внешнюю таблицу в свойствах гипертекстового документа. Для этого переключитесь на вкладку с файлом HTML и в блоке head добавьте новую строку со следующим содержимым:

```
<link rel="stylesheet" href="test.css">
```



Сохраните документ, перейдите в браузер и обновите веб-страницу.



Основные понятия

Менеджер пакетов **RPM** (**RPM Package Manager**) — это система управления пакетами программного обеспечения, используемая в ряде операционных систем семейства GNU/Linux.

Пакет RPM состоит из архива **cpio**, содержащего файлы, и заголовка RPM, содержащего метаданные о пакете. Менеджер пакетов RPM использует эти метаданные для определения зависимостей, места установки файлов и другой информации.

Заголовок файла RPM имеет следующие записи:

- идентификатор файла как RPM-архива,
- цифровая подпись для проверки целостности и подлинности,
- данные о пакете (версия, архитектура, список файлов и т. д.).

После всего этого идёт сам архив с файлами пакета.

Архиватор **cpio** может использовать различные алгоритмы сжатия из имеющихся в системе, например: **lzma**, **xz**, **zstd**.

Существует два типа пакетов RPM:

- исходный пакет (**source RPM**, **SRPM**);
- двоичный пакет (**binary RPM**).

SRPM и двоичный RPM имеют общий формат файла и инструментарий, но имеют разное содержимое и служат разным целям:

- SRPM содержит исходный код, исправления (**patches**) к нему при необходимости и файл спецификации, в котором описывается, как построить (собрать) из исходного кода двоичный пакет;
- двоичный RPM содержит двоичные файлы, созданные из исходных текстов и патчей согласно спецификации. Именно в двоичных пакетах распространяется готовое программное обеспечение среди пользователей.

Файл спецификации (spec-файл) в русскоязычной ИТ-литературе также называют сценарием сборки пакета.

Для работы с пакетами в РЕД ОС используются следующие пакетные менеджеры:

- универсальная утилита **rpm**,
- пакетный менеджер **dnf**.

Преимущества RPM

RPM упрощает распространение, управление и обновление программного обеспечения, созданного для РЕД ОС. Многие поставщики программного обеспечения распространяют своё ПО с помощью обычного архивного файла (например, **tar**-файла). Тем не менее, есть несколько преимуществ в упаковке программного обеспечения в пакеты RPM:

1) *Установка, переустановка, удаление, обновление и проверка пакетов.*

Пользователи могут использовать стандартные инструменты управления пакетами для установки, переустановки, удаления, обновления и проверки пакетов.

2) *Использование базы данных установленных пакетов.*

Поскольку RPM поддерживает базу данных установленных пакетов и их файлов, пользователи могут легко запрашивать информацию и проверять пакеты в своей системе.

3) *Использование метаданных.*

Каждый пакет RPM содержит метаданные, описывающие компоненты пакета, версию, релиз, размер, URL проекта, инструкции по установке и так далее.

4) *Упаковка исходных текстов программного обеспечения в исходные и двоичные пакеты*.

RPM позволяет брать исходные тексты из источников программного обеспечения и упаковывать их в исходные и двоичные пакеты для пользователей. В исходных пакетах имеются нетронутые исходные тексты вместе с любыми патчами (если таковые требуются и применяются при сборке), а также полные инструкции по сборке. Такая конструкция облегчает обслуживание пакетов по мере выпуска новых версий программного обеспечения.

5) *Добавление пакетов в репозитории.*

Можно добавить свой пакет в репозиторий, который позволит клиентам легко находить, развёртывать и обновлять программное обеспечение.

6) *Цифровая подпись ваших пакетов.*

Используя ключ подписи **GPG**, можно подписать пакет цифровой подписью, чтобы пользователи могли проверить подлинность программного обеспечения.

Поименование пакетов

Каждый пакет имеет своё собственное уникальное имя, которое складывается из нескольких составляющих (полей) строго в соответствии со следующими принципами:

1) Разделителем полей является символ «**-**» (минус);

2) Первое поле — имя или название (**Name**) программного обеспечения, может совпадать с названием проекта, но возможно задавать и собственное имя, если это обусловлено какими-либо корпоративными принципами или во избежание совпадений имён с уже существующими пакетами в репозитории дистрибутива.

Окончанием имени в названии файла пакета считается первый символ «**-**», за которым следует цифра. Например (здесь имя выделено зеленым цветом):

```
openssl-3.1.5-5.red80
openssl1.1-1.1.1q-1.red80
```

3) Второе поле — версия (**Version**) программного обеспечения. Окончанием значения данного поля является первый символ «**-**». Например (здесь версия выделена зеленым цветом):

```
openssl-3.1.5-5.red80
openssl1.1-1.1.1q-1.red80
```

Как видно из примеров, в репозитории могут находиться пакеты с различным названием, но содержащие в себе программное обеспечение с одной и той же версией;

4) Третье поле — релиз (**Release**) пакета. Например (здесь поле релиза выделено зеленым цветом):

```
openssl-3.1.5-5.red80 openssl1.1-1.1.1q-1.red80
```

Цифра до точки задаётся сборщиком пакета. Значение после первой точки в релизе называют суффиксом релиза (в данных примерах — **red80**), который показывает принадлежность пакета к какому-то семейству дистрибутивов. Суффикс релиза можно опускать, хотя это и нежелательно.

Первые три поля названия пакета (имя–версия–релиз) в документации и технической литературе для краткости часто обозначают первыми буквами английских терминов — **NVR** (Name–Version–Release).

Полное имя файла пакета завершается строго определённой строкой:

- для исходных пакетов — **.src.rpm**. Например:

```
openssl-3.1.5.red80.src.rpm
openssl1.1-1.1.1q-1.red80.src.rpm
```

- для бинарных пакетов — **.<ARCH>.rpm**, где **<ARCH>** — обозначение архитектуры, под которую собран пакет, т. е. скомпилирован бинарный код, содержащихся в пакете файлов. Различают большой ряд архитектур, из которых наиболее часто используются в РЕД ОС следующие:

```
i686, x86_64, aarch64, noarch
```

В случае **noarch**-пакетов в них располагаются архитектурно-независимые файлы, такие как документация, скрипты, изображения и пр.

Например:

```
openssl-3.1.5.red80.i686.rpm
openssl-3.1.5.red80.x86_64.rpm
globus-openssl-module-doc-5.2-4.red80.noarch.rpm
```

Значения всех параметров, заносимых в поля имени пакета, определяются в файле спецификации.

Сборочное окружение

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Прежде чем приступать к написанию спецификации и дальнейшей сборке пакета необходимо убедиться, что в системе установлены следующие пакеты:

```
rpm-build rpm-sign rpmdevtools diffutils patch make python-srpm-macros
```

являющие собой минимально необходимый набор, требуемый для обработки сценариев сборки.

Конечно, для сборки реальных проектов могут потребоваться и набор компиляторов **gcc**, и интерпретаторы **python** или **perl**, и многие другие инструменты разработчика, а также дополнительные утилиты по обслуживанию пакетов, в том числе и репозитория. Потребность в дополнительных пакетах определяется или самим разработчиком проекта (если собирается пакет программного обеспечения собственного написания), или согласно документации к программному обеспечению.

ВАЖНО!

Собирая пакеты, **не работайте** под учётными записями с повышенными привилегиями, особенно администратора **root**!

Первым шагом на пути создания пакета RPM является создание структуры каталогов, в которых будут находиться файлы проекта, для чего необходимо выполнить команду:

```
rpmdev-setuptree
tree ~/rpmbuild/

/home/user/rpmbuild/
|-- BUILD
|-- RPMS
|-- SOURCES
|-- SPECS
`-- SRPMS

5 directories, 0 files
```

В результате чего получим в домашней директории пользователя необходимое дерево каталогов. Во время запуска сборки пакета будет создан ещё один подкаталог в этом дереве — **BUILDROOT**. Каждый подкаталог в сборочной директории имеет своё предназначение.

Каталог	Предназначение
BUILD	Директория сборочных каталогов, их содержимое бывает полезно при расследовании неудачной сборки, если выходные данные журналов не содержат достаточной информации.
BUILDROOT	В данной директории формируются псевдо-корневые каталоги, в которые происходит установка скомпилированного ПО для дальнейшего формирования двоичного пакета.
RPMS	Собранные двоичные RPM записываются в подкаталогах для разных архитектур данного каталога.
SOURCES	В данном каталоге размещаются архивы исходного кода, патчи и другие файлы, необходимые для сборки.
SPECS	Каталог для файлов спецификаций.
SRPMS	В данный каталог сохраняются собранные исходные пакеты.

Файл спецификации

Преамбула
Тело спецификации

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Файл спецификации можно рассматривать как «рецепт», согласно которому утилита **rpmbuild** создаёт готовый пакет. В спецификации задаются команды для системы сборки, определяются инструкции в ряде разделов. Фактически спецификация представляет собой сценарий, выраженный языком макросов. Написание спецификации является важнейшим этапом при создании двоичных пакетов программного обеспечения.

Макрос RPM — это прямая текстовая подстановка, осуществляемая на основе раскрытия заданных выражений и условий, реализованная на базе встроенной функциональности сборочной системы. Иными словами, макросы являются псевдонимами для часто используемых фрагментов текста, применение которых сокращает не только объём ввода, но и делает спецификацию легче читаемой и воспринимаемой. Имена макросов начинаются с символа «**%**».

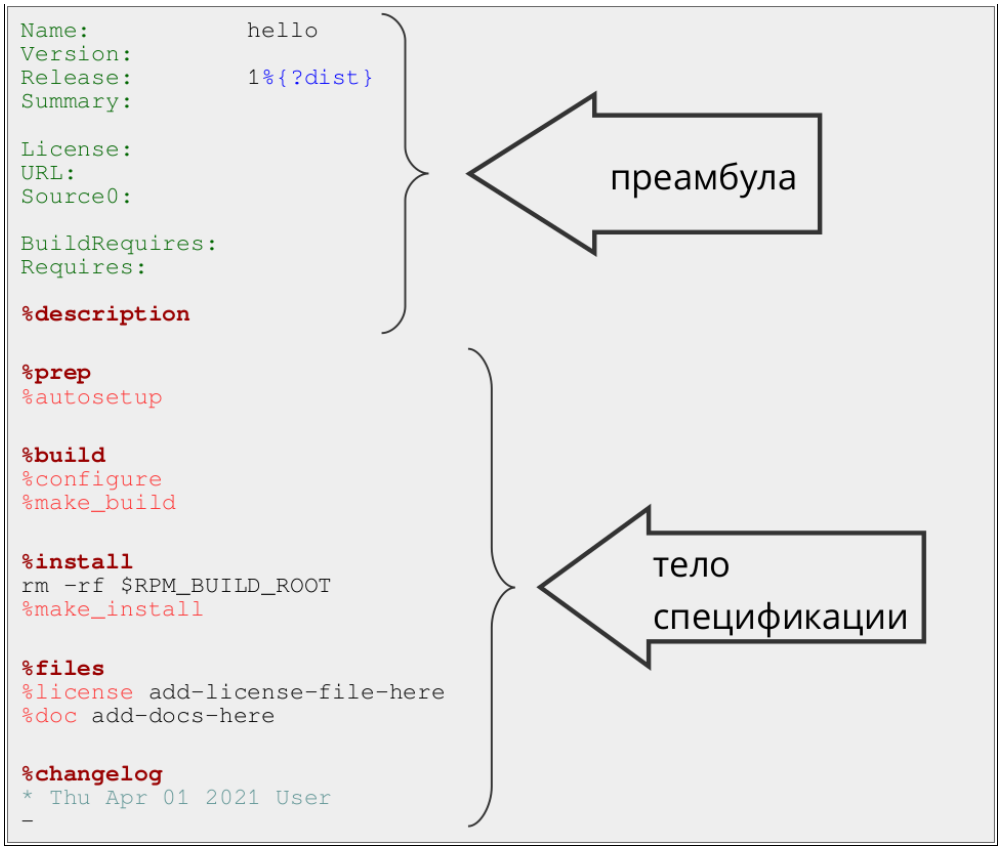
Файл спецификации разделяют на **преамбулу**, содержащую ряд элементов метаданных, которые используются в дальнейшем тексте, и **текст (тело) спецификации**, в котором содержится основная часть инструкций. В русскоязычных источниках преамбулу также называют заголовком спецификации.

Каждый из этих двух разделов сценария сборки содержит как обязательные, так и опциональные подразделы и элементы.

В случае написания спецификации «с нуля» можно создать её заготовку с типовыми блоками с помощью утилиты **rpmdev-newspec**, которой в качестве аргумента указывается имя нового проекта:

```
rpmdev-newspec hello
hello.spec created; type minimal, rpm version >= 4.13.
```

Созданный файл **hello.spec** будет иметь следующее содержимое:



Преамбула

В нижеприведенной таблице перечислены элементы, используемые в преамбуле файла спецификации RPM, которые называются **директивами** или **тэгами**. В таблице жирным шрифтом выделены **обязательные** директивы.

Директивы	Определение
Name	Базовое имя пакета, которое должно совпадать с именем файла спецификации
Version	Номер версии программного обеспечения
Release	Количество раз, когда данная версия программного продукта была собрана. Как правило, при первой сборке конкретной версии пакета значение устанавливается равным 1 и увеличивается на единицу с каждой новой сборкой пакета. После цифры указывают суффикс макросом **%{?dist}**
Epoch	Способ определения взвешенных зависимостей на основе номеров версий. Если директива явно не задана, то значение по умолчанию равно 0. Данный параметр влияет на полную версию пакета при построении зависимостей в базе данных RPM или в репозитории Полная версия выглядит как **Epoch:Version-Release**
Summary	Краткое, однострочное описание пакета
License	Лицензия на упаковываемое программное обеспечение
URL	Полный URL (адрес) для получения дополнительной информации о программе. Обычно это веб-сайт проекта для упаковываемого программного обеспечения
Source[X]	Путь (абсолютный или относительный) или URL-адрес к исходным файлам проекта. Директива может указывать как на сжатые архивы исходных кодов, так и на отдельные файлы. Проект может содержать несколько исходных файлов, тогда для их нумерации вместо **[X]** указывается цифра, например: **Source3**. Если имеется только один исходный файл, то нумерацию можно опустить, указав просто **Source**.
Patch[X]	Файлы патчей, которые при необходимости будут применены к исходному коду. Проект может содержать несколько патчей, тогда вместо **[X]** указывают их номер, например: **Patch2**. Если патч единственный, то номер можно не присваивать (**Patch**)
BuildArch	Явное указание архитектуры, под которую собирается двоичный пакет. Если параметр не задан, то пакет автоматически наследует архитектуру машины, на которой он собран. В случае с архитектурно-независимыми пакетами указание данной директивы обязательно: **BuildArch: noarch**
ExcludeArch	Если программное обеспечение, для которого собирается двоичный пакет, не может работать на определённой архитектуре процессора, то можно исключить эту архитектуру данной директивой
BuildRequires	Список пакетов, разделённых запятыми или пробелами либо указанных по одному в строке с данной директивой, необходимых для компиляции/создания программы или формирования пакета
Requires	Список пакетов, разделённых запятыми или пробелами, необходимых программному обеспечению для запуска после установки. В файле спецификации может быть несколько записей **Requires**, каждая из которых находится в отдельной строке

Provides	Указание дополнительных имён, библиотек или иных сущностей, которые предоставляет данный пакет. Используется для создания псевдонимов пакета, которые можно использовать как в тэгах спецификаций при сборке других пакетов, так и для установки пакета через пакетный менеджер
Obsoletes	Перечисление имён пакетов, которые данный пакет делает устаревшими. При установке данного пакета устаревшие пакеты будут автоматически удалены из системы пакетным менеджером
Confilcts	Перечисление имён пакетов, с которыми конфликтует данный пакет, т. е. все эти пакеты не могут быть одновременно установлены в системе

ВАЖНО!

Каждая директива обязательно разделяется от её значения символом «**:**», между директивой и двоеточием **не должно быть пробелов**!

Например:

```
Name: openssl
Version: 1.0.2
Release: 4%{?dist}
```

Завершается преамбула обязательным блоком описания назначения пакета, идущим после тэга **%description**, в котором, в отличие от директивы **Summary**, даётся развёрнутая информация о пакете. Описание может занимать любое количество строк и быть разбито на абзацы по желанию автора спецификации.

ВАЖНО!

В **одном** файле спецификации может быть описано **несколько** двоичных пакетов!

В таком случае один проект будет представлен несколькими двоичными RPM-файлами. Заголовки других пакетов в подобной спецификации должны начинаться с макроса **%package <ИМЯ_ПАКЕТА>**, причём имя другого пакета тэгом **Name** задавать не нужно — оно будет сформировано из опций указанного макроса. Также можно не указывать версию и релиз, если они совпадают (или должны совпадать по задумке автора спецификации) со значениями таковых же директив всего проекта. Например:

```
Name: superproj
Version: 1.0
Release: 1%{?dist}
Summary: Super Project
...
%description
This is the Super Project from our Company for all people.

%package devel
Summary: Development files for Super Project
...
%descrtiption devel
This package contains libraries and header files for development
with Super Project.
...
```

В результате успешного завершения сборки согласно данной спецификации будут получены два пакета, например (для архитектуры **x86_64**):

```
superproj-1.0-1.el7.x86_64.rpm  и  superproj-devel-1.0-1.el7.x86_64.rpm
```

Тело спецификации

В таблице ниже перечислены основные блоки, используемые в тексте (теле) спецификации, причём **все** они, **кроме %check**, **являются обязательными**.

Важно заметить, что сколько бы двоичных пакетов не было описано в спецификации, **все** ниже приведённые директивы, **кроме**

%files, фигурируют в тексте **только один раз** — разделение на разные двоичные RPM происходит именно в блоках **%files** согласно преамбуле.

Блоки	Определение
%prep	Команды для подготовки программного обеспечения к сборке, например, распаковка архива, указанного в **Source** или **Source0**.
%build	Команды для фактической сборки программного обеспечения в машинный код (для компилируемых языков) или байт-код (для некоторых интерпретируемых языков)
%install	Команды установки/копирования файлов из сборочного каталога в псевдо-корневую директорию
%check	Команды для тестирования программного обеспечения. Данный блок обычно включают в себя модульные тесты
%files	Список файлов для каждого двоичного пакета (если их создаётся несколько по одной спецификации), которые будут установлены в системе конечного пользователя
%changelog	Список изменений, произошедших в пакете между сборками разных версий или релизов

Командами внутри блоков могут быть как макросы сборочной системы RPM, так и вызовы внешних приложений, включая сценарии оболочки.

Если при сборке какого-либо пакета нет необходимости в каком-то блоке, всё равно его название необходимо указать в спецификации. Например, упаковывается тема пиктограмм и компилировать просто нечего при сборке двоичного пакета, то в спецификации такого пакета блок **%build** будет пустым.

Основные макросы

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Как уже говорилось ранее, **макрос RPM** — это прямая текстовая подстановка. Имеется ряд основных макросов, как явно заданных в установленной сборочной системе, так и задаваемых по мере обработки спецификации.

Получить значение заданного в сборочной системе макроса можно с помощью команды

```
rpm --eval %{<ИМЯ_МАКРОСА>}
```

Например, получим значение уже упомянутого выше макроса **%{?dist}**:

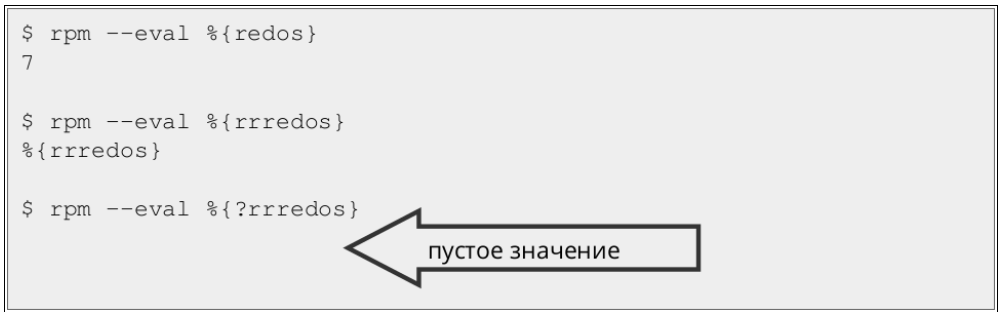
```
rpm --eval %{?dist}

.red80
```

ВАЖНО!

Тип значения макроса как переменной считается строковым (по аналогии с переменными в сценариях оболочки)!

С целью избежания нештатных ситуаций в случаях, когда макрос не определён, рекомендуется в конструкциях, где он используется как переменная, содержащая какое-либо значение, после открывающей скобки его имени ставить символ «**?**». Такая форма обращения к не определённому макросу при подстановке возвратит пустое значение, без знака вопроса — строку с именем данного макроса.

Например:



Макросы можно использовать внутри других макросов. Так, например, если название архива исходных текстов проекта формируется из его имени и версии (директивы **Name** и **Version** транслируются в определённые макросы, о чём будет рассказано ниже), то директива задания пути к файлу может выглядеть следующим образом:

```
Source0: %{name}-%{version}.tar.gz
```

Пути к системным каталогам и каталогам сборочного окружения могут быть получены в спецификации через заданные макросы, представленные в таблицах ниже.

Таблица 1. Макросы путей системных каталогов

Макрос	Определение
%{_sysconfdir}	/etc
%{_lib}	lib64 (для 64-битных платформ) lib (для 32-битных платформ)

%{_prefix}	/usr
%{_includedir}	%{_prefix}/include = /usr/include
%{_bindir}	%{_prefix}/bin = /usr/bin
%{_libdir}	%{_prefix}/%{_lib} = /usr/%{_lib}
%{_libexecdir}	%{_prefix}/libexec = /usr/lubexec
%{_sbindir}	%{_prefix}/sbin = /usr/sbin
%{_datadir}	%{_prefix}/share = /usr/share
%{_infodir}	%{_datadir}/info = /usr/share/info
%{_mandir}	%{_datadir}/man = /usr/share/man
%{_docdir}	%{_datadir}/doc = /usr/share/doc
%{_rundir}	/run
%{_localstatedir}	/var
%{_sharedstatedir}	/var/lib

Таблица 2. Макросы путей каталогов сборочного окружения

Макрос	Определение
%{_topdir}	%{getenv:HOME}/rpmbuild
%{_buildrootdir}	%{_topdir}/BUILDROOT
%{buildroot}	%{_buildrootdir}/%{name}-%{version}-%{release}.%{_arch}
%{_builddir}	%{_topdir}/BUILD
%{_rpmdir}	%{_topdir}/RPMS
%{_sourcedir}	%{_topdir}/SOURCES
%{_specdir}	%{_topdir}/SPECS
%{_srcrpmdir}	%{_topdir}/SRPMS

Значения, определяемые директивами преамбулы, транслируются для данной сборки в стандартные макросы. Связь директив и макросов дана в следующей таблице.

Таблица 3. Связь директив преамбулы и некоторых макросов

Директива	Соответствующий макрос
Name	%{name}
Version	%{version}
Release	%{release}
Epoch	%{epoch}
URL	%{url}
SourceX	%{SOURCEX} или %{S:X}

С целью сокращения написания часто требуемых команд при сборке пакета в блоках тела спецификации существует ряд полезных встроенных макросов:

1) **%setup** — используется в блоке **%prep** и выполняет следующие действия:

- переходит в дерево сборки;
- распаковывает архив с исходным кодом (с ключом **-q** подавляет подробный вывод при распаковке архива);
- изменяет владельца и права доступа к файлам с исходным кодом;
- переходит в распакованный каталог.

По умолчанию распаковывается первый архив с исходным кодом (т. е. который имеет номер 0), для любых других необходимо

использовать дополнительный параметр **-a X**, где **X** — номер, совпадающий с таковым у **Source**.

По умолчанию считается, что рабочим каталогом сборки в **BUILD** является тот, у которого имя совпадает с именем архива без суффикса (**.tar.gz** и пр.), если каталог с исходными текстами имеет другое название, то его указывают с ключом **-n** (например: **%setup -n %{name}-master**).

2) **%patch[X]** — используется в блоке **%prep** и выполняет применение указанного патча (здесь **X** — номер патча, такой же, как и при их описании в преамбуле, если патчей несколько). Применение патчей производится от текущего сборочного каталога, при необходимости обрезать часть пути к изменяемому файлу, можно использовать ключ **-p** (как и у самой утилиты **patch**). Например:

```
%patch3 -p1
```

3) **%autopatch** — применение всех патчей в порядке возрастания их номера в имени. Макрос также поддерживает использование ключа **-p**.

4) **%autosetup** — макрос, объединяющий функционал **%setup** и **%autopatch**; поддерживает все ключи, применимые в этих двум макросах.

5) **%configure** — применяется в блоке **%build** для выполнения сценария **configure** с подстановкой преднастроенных значений (обычно имён каталогов). Макрос принимает любые аргументы, которые при его раскрытии будут переданы скрипту **configure**.

6) **%make_build** — используется в блоке **%build** для выполнения команды **make** с установленными значениями **%{?_smp_mflags} %{_make_verbose}**. Здесь **%{?_smp_mflags}** раскрывается в **-j <ЧИСЛО_ПОТОКОВ>** и **%{_make_verbose}** — в **V=1 VERBOSE=1**.

Данный макрос также может принимать любые аргументы, которые при его раскрытии будут переданы утилите **make**.

7) **%make_install** — применяется в блоке **%install**, и представляет собой запуск утилиты **make** с ключом **install**, указанием каталога для установки (**DESTDIR=%{buildroot}**) и рядом других ключей.

Макрос также может принимать любые аргументы, которые при его раскрытии будут переданы утилите **make**.

8) **%dir** — макрос, используемый в блоке **%files**, указывающий, что путь является каталогом, который должен принадлежать этому RPM. Это указание важно для того, чтобы манифест файла RPM точно знал, какие каталоги нужно очистить при удалении пакета;

9) **%doc** — макрос, используемый в блоке **%files**, обеспечивающий создание каталога документации (**%{_docdir}/%{name}-%{version}**) и копирование в него указанных в качестве аргументов файлов. Пути к файлам строятся относительно каталога сборки проекта.

Например: **%doc README docs/Changelog**

10) **%license** — макрос, применяемый в блоке **%files**, аналогичный **%doc**, но копирует файлы лицензий в соответствующий каталог.

Скриптлеты

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

В спецификации RPM существует ряд директив, которые можно использовать для внесения необходимых или желаемых изменений в систему во время установки или удаления пакета. Такие директивы называются **скриптлетами**.

Некоторыми из основных примеров того, когда это может понадобиться, являются:

- установка пакетом системной службы, которая предоставляет файл модуля **systemd**, после чего нужно будет уведомить **systemd** о появлении нового модуля, возможно и запустить его. Обратная ситуация: при удалении пакета, содержащего модуль **systemd**, необходимо остановить выполнение сервиса и проинформировать **systemd** об удалении модуля;
- установка или удаление библиотек с последующей перестройкой их кэша;
- установка или удаление элементов графического интерфейса или схем **GLib**, после чего необходимо перестраивать кэши или перекомпилировать схемы;
- создание или удаление системных пользователей и/или групп при установке или удалении пакетов.

Количество стандартных (встроенных) скриптлетов весьма невелико, все они похожи на блоки тела спецификации, такие как **%build** или **%install**, в том, что определяются многострочными сегментами кода, представляющим собой стандартный сценарий оболочки (но могут быть использованы и некоторые скриптовые языки, например, Lua).

В своём роде, скриптлеты являют собой дополнительные блоки в теле спецификации, предоставляющие расширенные возможности при работе уже с двоичными пакетами.

Далее приведены встроенные скриптлеты сборочной системы в РЕД ОС.

Скриптлеты поддерживают специальный флаг **-p**, который позволяет напрямую вызывать одну указанную программу, а не создавать сеанс оболочки для вызова программ (например, **%post -p /sbin/ldconfig**):

- **%pretrans** - выполняется до начала любых операций по установке пакета;
- **%pre** - выполняется непосредственно перед установкой файлов из пакета;
- **%post** - выполняется сразу после завершения установки файлов из пакета;
- **%preun** - выполняется непосредственно перед удалением пакета;
- **%postun** - выполняется после завершения удаления файлов пакета;
- **%posttrans** - выполняется после завершения всех операций при удалении пакета.

При вызове скриптлетов им всегда передаётся аргумент, доступ к которому осуществляется через переменную **$1** (для сценариев оболочки), — это количество пакетов с этим именем, которые останутся в системе после завершения действия.

Скриптлет	Установка (install)	Обновление (upgrade)	Удаление (uninstall)
%pretrans	$1 == 0	$1 == 0	(N/A)
%pre	$1 == 1	$1 == 2	(N/A)
%post	$1 == 1	$1 == 2	(N/A)
%preun	(N/A)	$1 == 1	$1 == 0
%postun	(N/A)	$1 == 1	$1 == 0
%posttrans	$1 == 0	$1 == 0	(N/A)

Таким образом, анализируя аргумент внутри скриптлета, можно точно идентифицировать действие, которое выполняется в системе, а также определить, имеются ли в системе пакеты с таким же именем, что бывает необходимо знать при обновлении с целью

сохранения имеющихся настроек, а не их перезаписью.

Условные операторы

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Условные операторы сборочной системы RPM позволяют включать различные разделы файла спецификации в зависимости от указанных условий.

Чаще всего условные операции имеют дело с:

- разделами, относящиеся к версиям пакетов или операционной системы;
- разделами, относящиеся к архитектуре;
- существованием и определением макросов.

Синтаксис условного оператора следующий:

```
%if <УСЛОВИЕ>
...
%else
...
%endif
```

В случае необходимости выполнить только действия с истинным условием, можно использовать сокращённый вариант оператора:

```
%if <УСЛОВИЕ>
...
%endif
```

Существует форма записи данного оператора для случая проверки архитектуры, под которую собирается пакет:

```
%ifarch <АРХИТЕКТУРА>
...
%endif
```

Также имеется вариант, который проверяет условие «**если НЕ указанная архитектура**»:

```
%ifnarch <АРХИТЕКТУРА>
...
%endif
```

Например, задание переменной окружения **CFLAGS** в зависимости от архитектуры сборки пакета:

```
%ifarch %ix86 x86_64
export CFLAGS="$CFLAGS -msse2 -mfpmath=sse"
%endif
```

Чтобы избежать нештатных ситуаций при обработке условия, когда переменная (макрос) не определена, рекомендуется перед именем макроса ставить, например, символ «**0**»:

```
%if 0%{?redos} == 7
Requires: clang-devel
%endif
```

В директивах преамбулы **BuildRequires** и **Requires** для указания ограничений на версию требуемого пакета допускается краткое написание условного оператора, например:

```
BuildRequires: ffmpeg-devel >= 4.0
...
Requires: ffmpeg >= 4.0
```

Здесь в логической конструкции важно указывать такое же количество позиций у версии, как и у используемого пакета, то есть нельзя взять, например, только мажорную версию или добавить ещё одну цифру в конце.

Сборка исходных и двоичных пакетов

Сборка исходных пакетов
Сборка двоичных пакетов

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Пакеты RPM создаются с помощью утилиты **rpmbuild**. Различные сценарии и желаемые результаты сборки пакетов требуют различных комбинаций аргументов для **rpmbuild**. В этом разделе описаны два основных сценария:

- построение исходного пакета;
- построение двоичного пакета.

Команда **rpmbuild** работает с определённой структурой каталогов и файлов, которая была рассмотрена в нашей статье « Сборочное окружение». Таким образом, приступать к сборке пакетов можно при наличии всех требуемых исходных файлов, патчей к ним (в случае необходимости) и файла спецификации, размещённых в дереве каталогов сборочного окружения.

Построение двоичного пакета можно осуществить и без настроенной сборочного структуры каталогов и файлов, если имеется исходный пакет.

Сборка исходных пакетов

Основными задачами создания исходных пакетов (**SRPM**) являются:

- сохранение точного источника, включающего в себя точный файл спецификации, исходный код и все соответствующие исправления. Наличие **SRPM** бывает полезно для просмотра истории изменений и для отладки;
- возможность создавать двоичный пакет на другой аппаратной платформе или архитектуре.

Создание исходного пакета выполняется с помощью команды:

```
rpmbuild -bs <SPECFILE>
```

где <**SPECFILE**> — имя файла спецификации; ключ **-bs** является сокращением от словосочетания «**build source**». Имя файла может быть как абсолютным, так и относительным путём.

В результате безошибочного выполнения команды сборки исходного пакета в папке **~/rpmbuilds/SRPMS** появится SRPM-файл.

Сборка двоичных пакетов

Существует два метода построения двоичных пакетов:

- перестроить его из **SRPM** с помощью команды **rpmbuild --rebuild**;
- создать его из файла спецификации с помощью команды **rpmbuild -bb**. Опция **-bb** расшифровывается как «**build binary**».

Если имеется исходный пакет, то для получения двоичного необходимо выполнить команду:

```
rpmbuild --rebuild <ИМЯ>.src.rpm
```

В случае выполнения указанной команды будут реализованы следующие шаги:

1) создание сборочной структуры каталогов **~/rpmbuild** и установка в них содержимого исходного пакета;

2) сборка двоичного пакета согласно спецификации. Полученные файлы пакетов будут размещены в **~/rpmbuild/RPMS** в подкаталогах по именам архитектуры;

3) очистка содержимого каталогов **SPECS** и **SOURCES** в сборочном окружении.

Исходный пакет можно установить:

```
rpm -i <ИМЯ>.src.rpm
```

и после чего осуществить сборку двоичного пакета командой:

```
rpmbuild -bb <SPEC-ФАЙЛ>
```

Имя файла спецификации может быть как абсолютным, так и относительным путём.

С помощью последней команды можно собрать пакет, если имеется развёрнутое сборочное окружение со всеми необходимыми каталогами и файлами.

Цифровая подпись пакета

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Подписание пакета — это способ защитить пакет для конечного пользователя, чтобы убедиться, что никакая третья сторона не изменяла его содержимое при передаче от автора к пользователю.

В большинстве случаев пакеты создаются без подписи, которая уже позже добавляется непосредственно перед размещением файлов RPM в репозитории или ином способе передачи пользователям.

Чтобы добавить подпись к пакету, используется опция **--addsign** утилиты **rpm**. Например:

```
rpm --addsign superproj-1.0-1.el7.x86_64.rpm

 Enter pass phrase:

Pass phrase is good.
superproj-1.0-1.el7.x86_64.rpm:
```

Пакет может быть подписан несколькими различными подписями — наличие нескольких подписей позволяет отслеживать путь владения пакетом от разработчика до конечного пользователя.

Чтобы изменить открытый ключ у пакета, который уже подписан другой подписью, используется опция **--resign**:

```
rpm --resign superproj-1.0-1.el7.x86_64.rpm

 Enter pass phrase:

Pass phrase is good.
superproj-1.0-1.el7.x86_64.rpm:
```

Чтобы подписать пакет во время сборки, используется команда **rpmbuild** с параметром **--sign**, причём парольная фраза запрашивается перед сборкой пакета, а не по её окончании:

```
rpmbuild -bb --sign superproj.spec

 Enter pass phrase:

Pass phrase is good.
* Package: superproj
...
Binary Packaging: superproj-1.0-1
Finding dependencies...
...
Generating signature: 1002
Wrote: /home/user/rpmbuild/RPMS/x86_64/superproj-1.0-1.el7.x86_64.rpm
```

Сборка пакета стороннего ПО

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Рассмотрим сборку пакета на примере проекта **libfakekey**.

1) Получите исходные тексты программы, скачав архив актуальной версии по следующей ссылке.

2) Получив исходный архив, распакуйте его командой:

```
tar -xf libfakekey-0.3.tar.gz
```

3) В полученном дереве исходного кода найдите файл **INSTALL**, в случае его отсутствия — **README**. В них, как правило, описаны инструкции по сборке проекта.

В данном случае файл **INSTALL** отсутствует, а **README** имеет нулевую длину, но имеется сценарий **autogen.sh** со следующим содержимым:

```
#! /bin/sh
autoreconf -v --install || exit 1
./configure --enable-maintainer-mode "$@"
```

Значит, необходимые файлы могут быть сгенерированы с помощью утилиты **autoreconf**, для чего необходимо установить в систему пакеты **autoconf** и **automake**, если они отсутствуют. Находясь в каталоге исходных текстов, выполните следующую команду:

```
autoreconf -fiv
```

4) Поскольку в РЕД ОС сборка бинарных файлов осуществляется с использованием динамического связывания, то можно для сценария конфигурации использовать опцию отключения сборки статической версии (**--disable-static**). Также нужно указать, что при сборке проекта скомпилированные библиотеки необходимо компоновать с библиотеками X Window, для чего утилите **make** передайте указание на это (**AM_LDFLAGS=-lX11**).

5) Затем следует определиться с пакетами, необходимыми для сборки. Откройте файл **fakekey/fakekey.h**, в котором будет интересовать секция **#include**, находящаяся в его начале:

```
#ifndef _HAVE_LIBFAKEKEY_H
#define _HAVE_LIBFAKEKEY_H

#include <stdio.h>
#include <stdlib.h>
#include <X11/X.h>
#include <X11/Xlib.h>
#include <X11/Xlibint.h>
#include <X11/Xutil.h>
#include <X11/cursorfont.h>
#include <X11/keysymdef.h>
#include <X11/keysym.h>
#include <X11/extensions/XTest.h>
#include <X11/Xos.h>
#include <X11/Xproto.h>

#ifdef __cplusplus
extern "C" {
```

```
#endif
```

Здесь представляют интерес заголовочные файлы системы **X11**. Проверьте, какими пакетами они поставляются, для чего выполните операцию поиска по репозиторию, например:

```
dnf provides "*X11/Xlib.h"
```

Использование джокерного символа «*» обязательно, поскольку в метаданных пакета может храниться полный путь к файлу, а утилита **dnf** выводит результаты поиска при условии полного совпадения строк.

Таким образом, проверив все **.h**-файлы, будет выведен список из следующих пакетов: libX11-devel, libXi-devel, libXtst-devel, xorg-x11-proto-devel.

6) Имея полученную информацию, перед тем как приступить к написанию спецификации пакета, создайте структуру сборочных каталогов (см. статью «Сборочное окружение»):

```
rpmdev-setuptree
```

В каталог **SOURCES** скопируйте исходный архив, затем перейдите в директорию **SPECS** и создайте в нём заготовку спецификации (см. статью «Файл спецификации»):

```
rpmdev-newspec libfakekey libfakekey.spec created; type minimal, rpm version >= 4.13.
```

7) Откройте на редактирование файл **libfakekey.spec** в любом текстовом редакторе и начните заполнять преамбулу. Учтите, что пакет устанавливает в систему не только двоичные компоненты, но и файлы, необходимые для разработки программного обеспечения. Считается «хорошим тоном» файлы для разработчиков выносить в отдельный двоичный пакет — отразите это в спецификации.

```
0 # spec file for package libfakekey
1 Name: libfakekey
2 Version: 0.3
3 Release: 1%{?dist}
4 Summary: Library for converting characters to X key-presses
5 License: LGPLv2+
6 URL: http://projects.o-hand.com/matchbox/
7 Source0: %{name}-%{version}.tar.gz
8 BuildRequires: gcc
9 BuildRequires: make
10 BuildRequires: autoconf
11 BuildRequires: automake
12 BuildRequires: libX11-devel
13 BuildRequires: libXi-devel
14 BuildRequires: libXtst-devel
15 BuildRequires: xorg-x11-proto-devel
16 BuildRequires: pkgconfig
17
18 %description
19 libfakekey is a simple library for converting UTF-8 characters
20 into 'fake' X key-presses.
21
22 %package devel
23 Summary: Development files for %{name}
24 Requires: %{name} = %{version}-%{release}
25 Requires: libX11-devel
26 Requires: libXi-devel
27 Requires: libXtst-devel
28 Requires: xorg-x11-proto-devel
29 Requires: pkgconfig
30
31 %description devel
32 The %{name}-devel package contains libraries and header files for
33 developing applications that use %{name}.
34
```

Здесь в строке **№ 0** находится комментарий. В спецификации к таковым относится вся символьная последовательность от «**#**» до конца строки.

В строке **№ 4** даётся краткое описание, а в строках **18–20** — развёрнутое описание пакета, которые можно взять, например, с сайта проекта.

Имя исходного архива в строке **№ 7** задаётся через макросы (как показывалось в статье «Основные макросы»), что будет удобным при обновлении пакета до новой версии, так как директиву **Source0** исправлять не придётся — достаточно будет изменить только версию пакета в директиве **Version** в начале файла.

В строках **с 8 по 16** находится перечисление пакетов по одному в строке, которые необходимы для сборки данного пакета. Здесь пакет **pkgconfig** необходим для обработки файла **libfakekey.pc.in**, имеющегося в дереве исходного кода проекта.

С 22 по 33 строки производится описание второго двоичного пакета, который получит имя **libfakekey-devel**, с файлами для разработчиков. В секции его описания дополнительно указываются те пакеты, которые будут необходимы для его использования при разработке программного обеспечения — они заданы директивами **Requires**. Содержимое **%description** определяются самостоятельно, исходя из общего описания в предыдущей подобной директивы, с указанием на то, что здесь содержатся файлы для разработки.

8) Далее перейдем к телу спецификации (нумерация строк сквозная, с продолжением после преамбулы):

```
35 %prep
36 %setup -q
37
38 %build
39 autoreconf -fiv
40 %configure --disable-static
41 %make_build AM_LDFLAGS=-lX11
42
43 %install
44 %make_install
45 rm -f %{buildroot}%{_libdir}/libfakekey.la
46
47 %ldconfig_scriptlets
48
49 %files
50 %license COPYING
51 %{_libdir}/libfakekey.so.*
52
53 %files devel
54 %{_includedir}/fakekey/
55 %{_libdir}/libfakekey.so
56 %{_libdir}/pkgconfig/libfakekey.pc
57
58 %changelog
59 * Tue Jan 19 2021 Rodion Alexeev - 0:0.3-1
60 - Initial build
70
```

Со строки **№ 35** начинается блок подготовки к сборке, в нём с помощью макроса **%setup** производится распаковка архива с подавлением вывода на экран информации об извлечение файлов.

Со строки **№ 38** следует блок сборки проекта. Согласно файлу **autogen.sh**, требуется выполнить **autoreconf**, а после него — сгенерированный **configure**. Необходимо выполнить данные действия, но лучше это сделать не запуском сценария, а явным указанием этих команд в спецификации, поэтому в строке **№ 39** осуществляется выполнение утилиты **autoconf**, а в строке **№ 40** — **configure** посредством соответствующего макроса. После всего этого выполните сборку проекта утилитой **make** также посредством макроса (строка **№ 41**).

Собранный проект необходимо установить, т. е. инсталлировать, за что отвечает блок **%install** со строки **№ 43**. Типовая установка (**make install**) осуществляется посредством соответствующего макроса (строка **№ 44**), а затем из дерева установки удаляется файл **Libtool Archive** (**.la**) за ненадобностью. Обращаем внимание, что все пути указаны как абсолютные и с помощью макросов!

Поскольку в пакете будет поставляться динамическая библиотека, то при её установке или удалении необходимо перестраивать кэш библиотек утилитой **ldconfig** — данные действия осуществляются с помощью скриптлетов **%post** и **%postun**, соответственно. Можно это оформить в следующем виде:

```
%post -p /sbin/ldconfig
%postun -p /sbin/ldconfig
```

В РЕД ОС имеется скриптлет, объединяющий вышеуказанные действия, он использован в строке **№ 47**.

Затем следуют блоки описания файлов, размещаемых в двоичных пакетах. Поскольку необходимо разделить проект на два RPM-файла, то и блоков **%files** у нас тоже два — со строки **№ 49** для **libfakekey**, со строки **№ 53** — для **libfakekey-devel**. В строке **№ 50** используется макрос для копирования и описания файла лицензии, в остальных строках (**№ 51, 54–56**) идёт перечисление файлов, которые будут принадлежать тому или иному пакету.

В данном примере количество двоичных файлов не велико и их названия и расположение можно посмотреть в **Makefile**, но в случае больших проектов это, скорее всего, не поможет в заполнении данного блока.

При написании спецификации «с нуля» можно поступить следующим образом — блоки **%files** оставить пустыми, перейти к заполнению следующего раздела, после выполнить первую сборку пакета. В конце сборки будет показано сообщение об ошибке, что имеются неупакованные в RPM файлы с выводом их полного списка. Из данного списка уже можно взять имена файлов и их местоположение и внести в блок **%files**, не забывая заменять реальные имена каталогов на макросы, их обозначающие.

Последний раздел тела спецификации — журнал изменений (**%changelog**) — начинается со строки **№ 58**. Здесь указаны дата сборки пакета, автор сборки, а также список изменений (оно в данном примере одно — **Initial build**). Допускается (и считается «хорошим тоном») после имени автора указывать его адрес электронной почты в виде **<box@domain.tld>**.

Обратите внимание на окончание строки **№ 59: 0:0.3-1**. Первая цифра до двоеточия — это эпоха (**Epoch**), которая явно в преамбуле не задана, и по умолчанию принимается равной 0. После двоеточия до символа «-» идёт указание версии пакета (**Version**), а после «-» — указание релиза (**Release**) без суффикса. Часто опускают указание эпохи, если она нулевая. Можно опустить и всю данную цифровую конструкцию, но не рекомендуется этого делать, поскольку становится не понятным, к какой конкретно сборке относится запись в журнале изменений.

9) Завершив редактирование файла спецификации, приступаем к сборке двоичного пакета командой:

```
rpmbuild -bb libfakekey.spec
```

Вывод информации на экран при работе данной команды весьма обширный, приведём только некоторые выдержки из него:

- начало сборки, выполнение блока **%prep**:

```
rpmbuild -bb libfakekey.spec

Выполняется(%prep): /bin/sh -e /var/tmp/rpm-tmp.yqu3Ha
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd /home/user/rpmbuild/BUILD
+ rm -rf libfakekey-0.3
+ /usr/bin/gzip -dc /home/user/rpmbuild/SOURCES/libfakekey-0.3.tar.gz
+ /usr/bin/tar -xof -
+ STATUS=0
+ '[' 0 -ne 0 ']'
+ cd libfakekey-0.3
+ /usr/bin/chmod -Rf a+rX,u+w,g-w,o-w .
+ exit 0
...
```

- начало блока **%build**:

```
Выполняется(%build): /bin/sh -e /var/tmp/rpm-tmp.Im8Y8n
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd libfakekey-0.3
+ autoreconf -fiv
...
```

продолжение **%build** — запуск макроса **%configure**:

```
...
+ ./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix= --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64 --libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/share/man --infodir=/usr/share/info --disable-static
```

запуск макроса **%make_build** и завершение блока **%build**:

```
+ make -j2 AM_LDFLAGS=-lX11
make  all-recursive
make[1]: Entering directory '/home/user/rpmbuild/BUILD/libfakekey-0.3'
...
+ exit 0
...
```

- начало блока **%install**:

```
Выполняется(%install): /bin/sh -e /var/tmp/rpm-tmp.Y0WCvw
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ '[' /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64 '!=' / ']'
+ rm -rf /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
++ dirname /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
+ mkdir -p /home/user/rpmbuild/BUILDROOT
+ mkdir /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
+ cd libfakekey-0.3
+ make install DESTDIR=/home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
Making install in fakekey
make[1]: Entering directory '/home/user/rpmbuild/BUILD/libfakekey-0.3/fakekey'
...
```

- блок **%files**:

```
Processing files: libfakekey-0.3-1.el7.x86_64
Выполняется(%license): /bin/sh -e /var/tmp/rpm-tmp.W2BVTI
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd libfakekey-0.3
+ LICENSEDIR=/home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64/usr/share/licenses/libfakekey
+ export LC_ALL=C
+ LC_ALL=C
+ export LICENSEDIR
+ /usr/bin/mkdir -p /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64/usr/share/licenses/libfakekey
+ cp -pr COPYING /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64/usr/share/licenses/libfakekey
+ exit 0
...
```

- после завершения всех действий, заданных в спецификации, сборочная система начинает анализировать полученные в ходе сборки файлы на предмет определения зависимостей (**Requires**), которые будут добавлены в метаданные пакета, чтобы пакетные менеджеры при установке данных RPM знали, что должно присутствовать в системе к моменту установки пакета, а в случае отсутствия — установить из репозитория. Также на данном этапе записывается в метаданные информация о компонентах, которые предоставляет пакет (**Provides**):

```
Provides: libfakekey = 0.3-1.el7 libfakekey(x86-64) = 0.3-1.el7 libfakekey.so.0()(64bit)
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Requires: libX11.so.6()(64bit) libXtst.so.6()(64bit) libc.so.6()(64bit) libc.so.6(GLIBC_2.2.5)(64bit) libc.so.6(GLIBC_2.4)(64bit) rtld(GNU_HASH)
Processing files: libfakekey-devel-0.3-1.el7.x86_64
Provides: libfakekey-devel = 0.3-1.el7 libfakekey-devel(x86-64) = 0.3-1.el7 pkgconfig(libfakekey) = 0.3
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Requires: /usr/bin/pkg-config
Processing files: libfakekey-debuginfo-0.3-1.el7.x86_64
Provides: libfakekey-debuginfo = 0.3-1.el7 libfakekey-debuginfo(x86-64) = 0.3-1.el7
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Проверка на неупакованный(е) файл(ы): /usr/lib/rpm/check-files /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
Записан: /home/user/rpmbuild/RPMS/x86_64/libfakekey-0.3-1.el7.x86_64.rpm
Записан: /home/user/rpmbuild/RPMS/x86_64/libfakekey-devel-0.3-1.el7.x86_64.rpm
Записан: /home/user/rpmbuild/RPMS/x86_64/libfakekey-debuginfo-0.3-1.el7.x86_64.rpm
...
```

- успешное завершение сборки пакета:

```
...
Выполняется(%clean): /bin/sh -e /var/tmp/rpm-tmp.hlC2sW
+ umask 022
+ cd /home/user/rpmbuild/BUILD
+ cd libfakekey-0.3
+ /usr/bin/rm -rf /home/user/rpmbuild/BUILDROOT/libfakekey-0.3-1.el7.x86_64
```

```
+ exit 0
```

В случае успешного завершения сборки в каталоге **~/rpmbuild/RPMS** будут созданы подкаталоги с именами архитектур, под которые собрались RPM-файлы. В этих подкаталогах будут размещены двоичные пакеты:

```
ls -1Rp ~/rpmbuild/RPMS

/home/user/rpmbuild/RPMS:
x86_64/

/home/user/rpmbuild/RPMS/x86_64:
libfakekey-0.3-1.el7.x86_64.rpm
libfakekey-debuginfo-0.3-1.el7.x86_64.rpm
libfakekey-devel-0.3-1.el7.x86_64.rpm
```

Здесь видно, что собрано три пакета, хотя в спецификации описывалось два. Дело в том, что перед упаковкой файлов в архив **cpio** сборочная система извлекает из двоичных файлов отладочную информацию, которая затем помещается в отдельный файл RPM, что отражается в его названии:

```
libfakekey-debuginfo-0.3-1.el7.x86_64.rpm
```

Данные пакеты не нужны рядовым пользователям, они востребованы разработчиками для отладки работы программного обеспечения.

10) После успешного завершения сборки двоичных пакетов необходимо собрать исходный пакет:

```
rpmbuild -bs libfakekey.spec

Записан: /home/user/rpmbuild/SRPMS/libfakekey-0.3-1.el7.src.rpm
```

На этом процесс сборки проекта **libfakekey** завершён — в результате созданы как исходный, так и двоичные пакеты. Двоичные RPM можно передавать кому-либо для использования/установки, перед этим желательно подписать их своей цифровой подписью.

Сборка мета-пакета

Консультации и оказание технической поддержки по данной статье **не предоставляются**.

Вы можете подробнее ознакомиться с принципами сборки пакетов для РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Курс по принципам сборки пакетов для РЕД ОС;
- в **Яндекс.Дзен** — Курс по принципам сборки пакетов для РЕД ОС;
- в **VK Видео** — Курс по принципам сборки пакетов для РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Определим, что такое «мета-пакет», хотя однозначного, стандартизованного толкования данного понятия не существует. В общих словах, мета-пакет — это «пустой» пакет. Под термином «пустой» понимают как отсутствие исходных файлов при сборке пакета (в спецификации нет директив **Source**), так и отсутствие файлов в архиве **cpio** двоичного пакета (блок **%files** пустой).

Может возникнуть вопрос: зачем такой пакет, который ничего не устанавливает в систему? Дело в том, что ценность пакета может быть не только в файлах, в нём содержащихся, но и в его метаданных. Иными словами, после инсталляции мета-пакета в базе данных установленных пакетов появляются записи относительно каких-то новых имён, зависимостей и прочего, имеющих значение в целом для системы.

В каких случаях это может понадобиться? Например, имеется программный проект, представленный большим числом RPM файлов, каждый из которых устанавливает в систему какой-то логически законченный набор файлов. Полная установка всего этого ПО потребует устанавливать все эти пакеты — для упрощения данной процедуры можно создать мета-пакет, который при установке всего лишь потребует от пакетного менеджера установить весь перечень пакетов этого программного проекта.

Например, имеется следующий список двоичных пакетов:

```
superproj-libs-1.0-1.el7
superproj-devel-1.0-1.el7
superproj-bin-1.0-1.el7
superproj-server-1.0-1.el7
superproj-client-1.0-1.el7
superproj-tools-1.0-1.el7
superproj-docs-1.0-1.el7
```

Создадим мета-пакет для установки всех этих пакетов. Спецификация для такого пакета будет выглядеть следующим образом:

```
1 %define debug_package %{nil}
2 Name: superproj-all
3 Version: 1.0
4 Release: 1%{?dist}
5 Summary: Meta-package for SuperProj
6 License: GPL2+
7 URL: https://super.proj/
8 Requires: superproj-libs = %{version}-%{release}
9 Requires: superproj-devel = %{version}-%{release}
10 Requires: superproj-bin = %{version}-%{release}
11 Requires: superproj-server = %{version}-%{release}
12 Requires: superproj-client = %{version}-%{release}
13 Requires: superproj-tools = %{version}-%{release}
14 Requires: superproj-docs = %{version}-%{release}
15
16 %description
17 Meta-package for installing all packages of SuperProj.
18
19 %prep
20
21 %build
22
23 %install
```

```
24
25 %files
26
27 %changelog
28 * Tue Jan 19 2021 Rodion Alexeev - 0:1.0-1
29 - Initial build
```

Здесь надо обратить внимание на строку **№ 1:** **%define** в общем случае задаёт значение макроса, а в данном случае — переопределяет значение стандартного макроса **debug_package**, устанавливая его в пустое значение (**%nil**). Такая конструкция говорит сборочной системе, что не надо извлекать отладочную информацию из конечных файлов (в данном мета-пакете извлекать нечего и не из чего!) и не формировать **debuginfo**-пакет.

Блоки **%prep**, **%build**, **%install**, **%files** в данной спецификации пустые, но они всё равно должны быть явно обозначены.

После выполнения команды **rpmbuild** будет создан пакет под заданную архитектуру, который сам в виде файлов ничего не будет поставлять в систему, но потребует от пакетного менеджера установить все пакеты, которые у него перечислены в зависимостях (директивы **Requires**).

Установка .NET

Установка
Работа в программе
Создание простого консольного приложения
Создание простого веб-приложения

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: dotnet-sdk-6.0-6.0.105-1

.NET (ранее известна как *.NET Core*) — бесплатная модульная платформа с открытым исходным кодом для разработки программного обеспечения. Поддерживает следующие языки программирования:

- **C#** — это современный, объектно-ориентированный и типобезопасный язык программирования. Он имеет свои корни в семействе языков C – *C*, *C++*, *Java* и *JavaScript*.
- **F#** — это язык программирования взаимодействия для написания краткого, надежного и эффективного кода. Программирование **F#** ориентировано на данные, где код включает преобразование данных с помощью функций.
- **Visual Basic** использует более подробный синтаксис, который близок к обычному человеческому языку. Это наиболее простой язык для начинающих программистов.

Платформа **.NET** основана на высокопроизводительной среде выполнения, которая используется в рабочей среде многими высокомасштабируемыми приложениями.

Установка

Платформа **.NET** в РЕД ОС включает в себя следующие пакеты:

- **dotnet-sdk** – пакет SDK позволяет разрабатывать приложения с помощью **.NET**;
- **aspnetcore-runtime** – среда выполнения **ASP.NET Core** позволяет запускать веб-приложения, включает в себя пакет **dotnet-runtime**;
- **dotnet-runtime** – альтернатива среде выполнения **ASP.NET Core**, позволяет запускать **.NET**-приложения.

В рамках текущей статьи будет рассмотрена установка **.NET** в составе пакета **dotnet-sdk**, т.к. он включает в себя сразу всю платформу.

Перед началом установки перейдите в сеанс пользователя **root**:

```
su -
```

Далее выполните команду установки платформы:

```
dnf install dotnet-sdk-6.0
```

Для проверки установленных **SDK** воспользуйтесь следующей командой:

```
dotnet --list-sdks

6.0.105 [/usr/lib64/dotnet/sdk]
```

Для проверки установленных сред выполнения воспользуйтесь командой:

```
dotnet --list-runtimes

Microsoft.AspNetCore.App 6.0.5 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
Microsoft.NETCore.App 6.0.5 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]
```

Подробную информацию о доступных опциях и командах выполните команду:

```
dotnet --help
```

Работа в программе

Для проверки работы будут созданы два приложения – консольное и веб-приложение.

Создание простого консольного приложения

Создайте отдельный каталог для проектов (в примере **Projects**) и перейдите в созданный каталог:

```
mkdir Projects
cd Projects
```

Создайте новое консольное приложение (в примере **TestApp**) и перейдите в каталог приложения:

```
dotnet new console -o TestApp

Шаблон "Консольное приложение" успешно создан.

Идет обработка действий после создания...
Выполнение "dotnet restore" для /home/user/Projects/TestApp/TestApp.csproj...
  Determining projects to restore...
  Restored /home/user/Projects/TestApp/TestApp.csproj (in 309 ms).
 cd TestApp
```

Затем скомпилируйте или запустите скомпилированное приложение – в выводе должно отобразиться «Hello, world!».

```
dotnet run
Hello, World!
 dotnet bin/Debug/net6.0/TestApp.dll
Hello, World!
```

Создание простого веб-приложения

Создайте отдельный каталог для проектов (в примере **Projects**) и перейдите в созданный каталог:

```
mkdir Projects
cd Projects
```

Создайте новое веб-приложение (**TestWebApp**) и перейдите в каталог приложения:

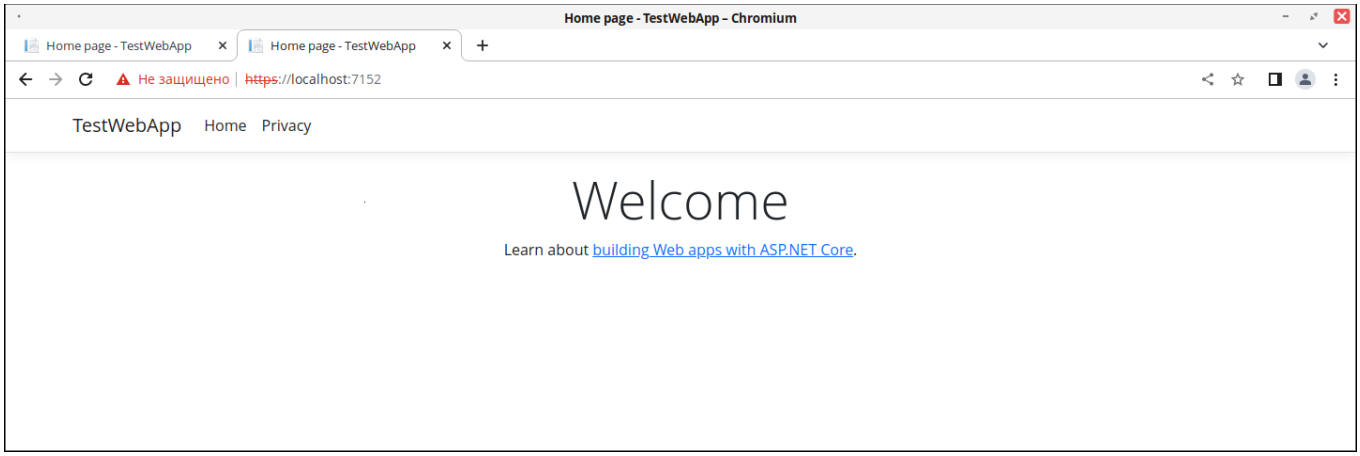
```
dotnet new webapp -o TestWebApp

Шаблон "ASP.NET Core Web App" успешно создан.
Этот шаблон содержит технологии сторонних производителей, кроме Майкрософт. Дополнительные сведения см. в разделе
https://aka.ms/aspnetcore/6.0-third-party-notices.

Идет обработка действий после создания...
Выполнение "dotnet restore" для /home/user/Projects/TestWebApp/TestWebApp.csproj...
  Determining projects to restore...
  Restored /home/user/Projects/TestWebApp/TestWebApp.csproj (in 289 ms).
Восстановление выполнено.cd TestWebApp
```

Затем скомпилируйте или запустите скомпилированное приложение.

```
dotnet run

Сборка...
info: Microsoft.Hosting.Lifetime[14]
      Now listening on: https://localhost:7152
info: Microsoft.Hosting.Lifetime[14]
      Now listening on: http://localhost:5274
info: Microsoft.Hosting.Lifetime[0]
      Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
```

```
      Hosting environment: Development
info: Microsoft.Hosting.Lifetime[0]
      Content root path: /home/user/Projects/TestWebApp/
```

В результате будет сформировано 2 адреса – для *HTTP*- и *HTTPS*-соединений. Запустите браузер и в адресной строке введите любой из указанных адресов – созданное веб-приложение должно быть доступно.



FPC – компилятор для разработки программ на языке Pascal

Установка
Создание и редактирование исходного кода
Создание простейшей программы на Pascal
Пример работы программы

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: fpc-3.2.0-1

FPC (*Free Pascal Compiler*) – это бесплатный компилятор программного обеспечения, предназначенный для языка программирования **Pascal**. *FPC* предоставляет возможность создания кроссплатформенных приложений – это означает, что можно написать программу один раз и скомпилировать ее для различных операционных систем, таких как *Windows*, *Linux*, *macOS* и даже для некоторых встраиваемых платформ.

Основные особенности *FPC*:

- **Поддержка платформ**. *FPC* поддерживает широкий спектр платформ, включая **x86**, **x86-64**, **ARM**, **PowerPC**, **SPARC** и многие другие. Это позволяет разрабатывать приложения для различных архитектур и операционных систем.
- **Полная совместимость с Turbo Pascal**. *FPC* стремится быть полностью совместимым с **Turbo Pascal** и поддерживает множество синтаксических расширений и возможностей языка.
- **Объектно-ориентированное программирование**. *FPC* поддерживает объектно-ориентированное программирование (ООП) и предоставляет возможности для создания классов, наследования, полиморфизма и инкапсуляции.
- **Модульность**. FPC позволяет разбивать программы на модули, что упрощает организацию и структурирование кода.
- **Расширения для системного программирования**. *FPC* предоставляет возможность обращения к низкоуровневым функциям и библиотекам операционной системы, что делает его подходящим для системного программирования.
- **Поддержка множества стандартов**. *FPC* соответствует многим стандартам, включая **ISO Pascal**, **Borland Pascal**, **Delphi**, **Mac Pascal** и другие.

FPC широко используется для разработки приложений, особенно в сообществах, где **Pascal** остается популярным языком программирования, таких как образование и некоторые научные области. Он также применяется для создания кроссплатформенных приложений, программирования микроконтроллеров и встроенных систем.

Установка

Для установки **fpc** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install fpc
```

После установки компилятор не требует дополнительной настройки. Работа с компилятором производится с правами **непривилегированного** пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

Синтаксис утилиты имеет вид:

```
fpc [<опции>] <файл> [<опции>]
```

Полезные опции:

- `-a` – не удалять файл ассемблера;
- `-al` – включить строки исходного кода в файл ассемблера в качестве комментариев;

- `-Cs<n>[<,m>]` – `<n>` задает минимальный размер кучи (стека данных) в байтах (от 1023 до 67107840), `[<,m>]` – максимальный размер кучи (необязательный параметр);
- `-Ct` – сгенерировать код проверки стека;
- `-s` – не вызывать ассемблер и компоновщик; вместо этого компилятор генерирует сценарий **ppas.sh**, который затем может быть выполнен для создания исполняемого файла;
- `-sh` – компилятор генерирует сценарий, который можно использовать для сборки и компоновки на хосте.

Для получения подробной информации о работе *FPC* выполните:

```
fpc -h
```

Создание и редактирование исходного кода

Перед началом работы создайте новый текстовый файл с расширением **.pas** и откройте его в любом удобном текстовом редакторе, например, nano. В этом файле будет располагаться исходный код программы на языке **Pascal**.

```
nano <имя_файла>.pas
```

> **Примечание.**
>
> Здесь и далее **<имя_файла>** замените на имя вашего файла.

Создание простейшей программы на Pascal

В примере будет написан и сохранен простейший код программы на языке **Pascal**.

Пример файла:

```
program Hello_world;
 begin
 writeln ('Hello World');
 end.
```

Компиляция программы

Теперь, когда есть исходный код, можно скомпилировать его с помощью **fpc**. Перейдите в каталог, где сохранен исходный файл, и выполните следующую команду:

```
fpc <имя_файла>.pas
```

В процессе выполнения компилятор создаст исполняемый файл с таким же именем, но без расширения **.pas**.

Запуск программы

После успешной компиляции программу можно запустить, указав в терминале имя исполняемого файла.

```
./<имя_файла>
```

Теперь программа должна запуститься и выполняться в соответствии с созданным исходным кодом.

Обратите внимание, что это базовая информация о том, как начать работать с *Free Pascal*.

Pascal – это мощный язык программирования с богатыми возможностями. Разработчик может использовать различные функции языка и библиотеки для создания разнообразных приложений. При желании, можно изучить дополнительные ресурсы и примеры для более продвинутого использования языка **Pascal** и компилятора *Free Pascal*.

Пример работы программы

Создадим исходный код программы:

```
nano test.pas
```

```
program ProgramTest;
 var a,i,n: integer;
 begin
  writeln('Введите высоту башни:');
  readln(a);
  for i:=1 to a do
  begin
   writeln();
   for n:=1 to I do
   write('*');
  end;
 writeln();
 end.
```

Выполним компиляцию программы:

```
fpc test.pas

Free Pascal Compiler version 3.2.0 [2020/12/29] for x86_64
Copyright (c) 1993-2020 by Florian Klaempfl and others
Target OS: Linux for x86-64
Compiling test.pas
Linking test
13 lines compiled, 0.1 sec
```

Запустим программу:

```
./test

Введите высоту башни:9

*
**
***
****
*****
******
*******
********
*********
```

Установка Julia

Установка
Работа в программе

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: julia-1.5.3-1

Julia – это высокоуровневый, динамический, функциональный и высокоэффективный язык программирования, который был разработан для научных вычислений и общего назначения. Он был представлен в 2012 году и стал популярным среди исследователей, инженеров, аналитиков данных и разработчиков благодаря своим мощным возможностям и простому синтаксису.

Некоторые ключевые особенности и характеристики языка программирования **Julia**:

- *Производительность*. **Julia** известен своей выдающейся производительностью. Он использует **Just-In-Time** (JIT) компиляцию, что позволяет достигать скорость, близкую к языкам низкого уровня, таким как **C** или **Fortran**. Это делает его отличным выбором для научных вычислений и других задач, где требуется высокая производительность.
- *Простота синтаксиса*. Синтаксис **Julia** интуитивен и легко читаем. Он похож на синтаксис **Matlab** и **Python**, что упрощает процесс изучения и использования языка.
- *Многопоточность*. **Julia** поддерживает параллельное программирование с помощью многопоточности. Это позволяет эффективно использовать многопроцессорные системы и ускорять выполнение вычислений.
- *Встроенная поддержка для распределенных вычислений*. Julia предоставляет удобные средства для распределенных вычислений на кластерах и удаленных системах, что делает его привлекательным для задач с высокой степенью параллелизма.
- *Обширная библиотека*. **Julia** имеет обширную библиотеку пакетов, включая инструменты для работы с матрицами, статистическими данными, машинным обучением, визуализацией данных и многое другое. Это облегчает решение различных задач без необходимости переходить к другим языкам программирования.
- *Открытый исходный код*. **Julia** является языком с открытым исходным кодом, что позволяет пользователям адаптировать его под свои потребности и вносить вклад в развитие языка.

Julia представляет собой мощный и гибкий язык программирования, который может быть использован для различных задач, особенно в области научных исследований, вычислений и анализа данных.

Установка

Для установки **Julia** перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install julia
```

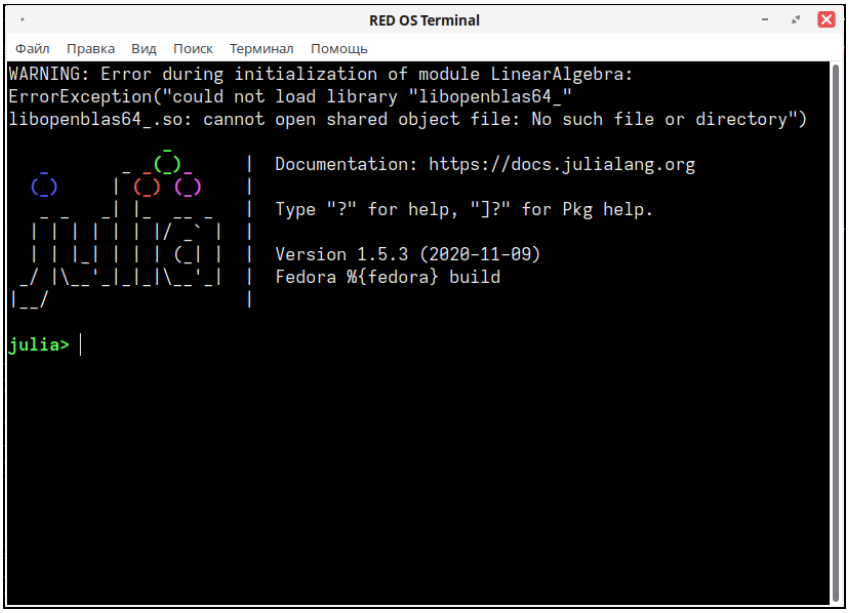
Дальнейшая работа в программе производится с правами непривилегированного пользователя, выйдите из сеанса пользователя **root**:

```
exit
```

После установки запуск программы доступен из «**Главного меню**» — «**Программирование**» — «**Julia**» или через терминал (с правами непривилегированного пользователя) командой:

```
julia
```

При запуске программы открывается привычный терминал РЕД ОС:



Для выхода используйте сочетание клавиш **Ctrl+D**.

Работа в программе

В **Julia** нет прямого аналога команды man, как в некоторых других языках программирования или в операционных системах Unix/Linux. Однако в **Julia** доступна встроенная функция help?, которая предоставляет доступ к справке и информации о функциях и объектах в **REPL** (Read-Eval-Print Loop – интерактивная среда командной строки **Julia**).

Чтобы получить справку по функции, объекту или пакету в **Julia**, введите символ вопроса ? и имя функции или объекта, о котором необходимо получить информацию.

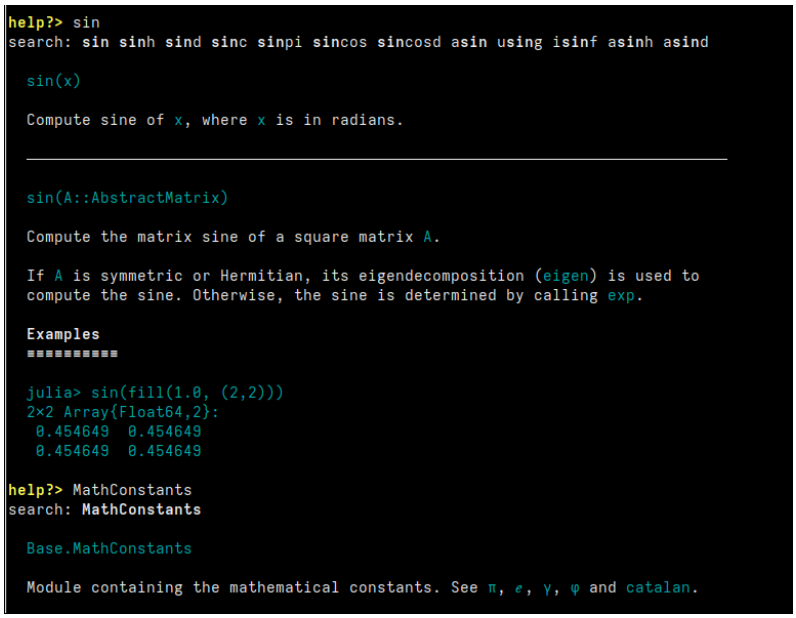
Например, для вывода справки о функции sin(), которая вычисляет синус угла, выполните:

```
?help?> sin
```

Для вывода справки о пакете или модуле также используется help?:

```
?help?> MathConstants
```

Пример вывода справки:



Справочную информацию о функции или пакете можно также получить с помощью @doc.

@doc – это макрос, который позволяет получить справку о функции, модуле или другом объекте. Для использования макроса введите команду вида:

```
@doc <имя_функции_или_объекта>
```

Например:

```
@doc sin
```

```
julia> @doc sin
  sin(x)

  Compute sine of x, where x is in radians.

  sin(A::AbstractMatrix)

  Compute the matrix sine of a square matrix A.

  If A is symmetric or Hermitian, its eigendecomposition (eigen) is used to compute the sine. Otherwise, the sine is determined by calling exp.

  Examples
  ==========

  julia> sin(fill(1.0, (2,2)))
  2×2 Array{Float64,2}:
   0.454649  0.454649
   0.454649  0.454649
```

Пример написания простого кода в программе и результаты его выполнения:

```
[user@localhost ~]$ julia
WARNING: Error during initialization of module LinearAlgebra:
ErrorException("could not load library "libopenblas64_"
libopenblas64_.so: cannot open shared object file: No such file or directory")
               _
   _       _ _(_)_     |  Documentation: https://docs.julialang.org
  (_)     | (_) (_)    |
   _ _   _| |_  __ _   |  Type "?" for help, "]?" for Pkg help.
  | | | | | | |/ _` |  |
  | | |_| | | | (_| |  |  Version 1.5.3 (2020-11-09)
 _/ |\__'_|_|_|\__'_|  |  Fedora %{fedora} build
|__/                   |

julia> bar() = (x = "Hello, Mars!"; return x)
bar (generic function with 1 method)

julia> function foo()
                    x = "Hello, "; x *= "World!"
                    return x
                end
foo (generic function with 1 method)

julia> foo()
"Hello, World!"

julia> bar()
"Hello, Mars!"
```

Tarantool — оптимизированный интерпретатор Lua

Возможности
Установка tarantool
Основные каталоги и файлы конфигурации
Интерактивная консоль
Создание базы данных с использованием Lua
Пример запуска Lua-скрипта в консоли tarantool
Пример работы с SQL
Управление экземплярами с помощью tarantoolctl
Исправление ошибок

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: tarantool-2.4.2.68-8

Tarantool — это одновременно резидентная база данных (размещаемая в оперативной памяти) и сервер приложений с поддержкой языка Lua.

Tarantool позволяет хранить и обрабатывать данные, разрабатывать приложения и ускорять работу системы. **Tarantool** можно использовать для работы с данными любого типа, копировать, сегментировать, распределяя большие объёмы данных по нескольким серверам и сочетая результаты, полученные от них, для создания отказоустойчивых кластеров. **Tarantool** подходит для серверов очередей, кешей, веб-приложений с отслеживанием состояния.

Возможности

Основные возможности сервера приложений:

- оптимизированный интерпретатор Lua, поддерживающий быстрый отслеживающий JIT-компилятор;
- совместная многозадачность, неблокирующий ввод-вывод;
- встроенная поддержка очередей задач;
- сегментирование данных и задач;
- встроенные средства для управления кластерами и развертывания приложений;
- коннекторы для взаимодействия с внешними базами данных;
- набор встроенных и автономных модулей.

Основные возможности базы данных:

- формат данных MessagePack и протокол клиент-сервер;
- два механизма хранения данных: хранение в оперативной памяти с полной сохраняемостью и собственная реализация LSM-tree, которая оптимизирована для работы с большими объёмами данных;
- несколько типов индексов: HASH, TREE, RTREE, BITSET;
- индексы путей в формате JSON;
- асинхронная и синхронная репликация;
- автоматическое избрание лидера с использованием алгоритма RAFT;
- аутентификация и контроль доступа;
- поддержка ANSI SQL;
- коннекторы для различных языков программирования.

Установка tarantool

Для установки программы через терминал выполните команду (потребуются права **администратора**):

```
sudo dnf install tarantool
```

Дальнейшая работа с программой должна выполняться с правами обычного (непривилегированного) пользователя.

Основные каталоги и файлы конфигурации

По умолчанию создаются каталоги:

- **/etc/tarantool** — каталог для хранения всей конфигурации;
- **/var/log/tarantool** — каталог для хранения журналов;
- **/var/lib/tarantool** — каталог для хранения данных, которые распределяются между экземплярами.
- **/etc/tarantool/instances.available/*.lua** — файл инициализации **tarantool** по умолчанию с простыми в использовании примерами конфигурации, включая репликацию, сегментирование и все основные функции.

Интерактивная консоль

Для запуска интерактивной консоли **tarantool** введите команду:

```
tarantool
```

Примерный вывод:

```
Tarantool 2.4.2-68-g17621b0
type 'help' for interactive help
tarantool>
```

В консоли можно работать с языком Lua и SQL.

Создание базы данных с использованием Lua

1. Настройка конфигурации. Выполните настройку сервера с базовыми параметрами:

```
box.cfg{
    listen = 3301,  -- порт для подключения клиентов     memtx_memory = 1024 * 1024 * 256  -- размер памяти для хранения данных
(256 МБ) }
```

Результат:

```
2024-08-09 09:51:46.499 [6465] main/103/interactive C> Tarantool 2.4.2-68-g17621b0
2024-08-09 09:51:46.500 [6465] main/103/interactive C> log level 5
2024-08-09 09:51:46.501 [6465] main/103/interactive I> mapping 268435456 bytes for memtx tuple arena...
2024-08-09 09:51:46.504 [6465] main/103/interactive I> mapping 134217728 bytes for vinyl tuple arena...
2024-08-09 09:51:46.514 [6465] main/103/interactive I> instance uuid e753c2aa-3d14-4a8e-9c03-7b4412a87011
2024-08-09 09:51:46.514 [6465] iproto/101/main I> binary: bound to 0.0.0.0:3301
2024-08-09 09:51:46.514 [6465] main/103/interactive I> initializing an empty data directory
2024-08-09 09:51:46.570 [6465] main/103/interactive I> assigned id 1 to replica e753c2aa-3d14-4a8e-9c03-7b4412a87011
2024-08-09 09:51:46.570 [6465] main/103/interactive I> cluster uuid 21f5b9e0-775c-467e-9872-e3be40b06f0a
2024-08-09 09:51:46.572 [6465] snapshot/101/main I> saving snapshot `./00000000000000000000.snap.inprogress'
2024-08-09 09:51:46.589 [6465] snapshot/101/main I> done
2024-08-09 09:51:46.589 [6465] main/103/interactive I> ready to accept requests
2024-08-09 09:51:46.589 [6465] main/105/checkpoint_daemon I> scheduled next checkpoint for Fri Aug  9 11:08:02 2024
2024-08-09 09:51:46.590 [6465] main/103/interactive I> set 'listen' configuration option to "3301" ---
...
```

После выполнения команды сервер будет инициализирован.

2. Создание нового пространства имён:

```
box.schema.space.create('my_space')
```

где:

- my_space - это имя вашей первой базы данных.

Вывод:

```
---
- engine: memtx
  before_replace: 'function: 0x40736f18'
  on_replace: 'function: 0x40736ef0'
  ck_constraint: []
  field_count: 0
```

```
  temporary: false
  index: []
  is_local: false
  enabled: false
  name: my_space
  id: 514
- created
...
```

где:

- **engine: memtx** - движок хранения (memtx), используемый для этого пространства;
- **before_replace** и **on_replace** - функции, которые вызываются перед и после замены данных в этом пространстве;
- **ck_constraint** - ограничения, накладываемые на данные в этом пространстве (в данном случае пустой список);
- **field_count** - количество полей в этом пространстве (0);
- **temporary** - флаг, указывающий, является ли это пространство временным;
- **index** - список индексов, созданных для этого пространства;
- **is_local** - флаг, указывающий, является ли это пространство локальным;
- **enabled** - флаг, указывающий, включено ли это пространство;
- **name** - имя пространства ("my_space");
- **id** - идентификатор пространства (514);
- **- created** - подтверждает, что пространство успешно создано.

3. Создание индекса с именем primary для базы данных:

```
box.space.my_space:create_index('primary', {
    type = 'tree',
    parts = {1, 'unsigned'}
})
```

Результат:

```
---
- unique: true
  parts:
  - type: unsigned
    is_nullable: false
    fieldno: 1
  id: 0
  space_id: 512
  type: TREE
  name: primary
...
```

4. Добавление данных в базу данных:

```
box.space.my_space:insert{1, 'example data'}
```

Результат:

```
---
- [1, 'example data']
...
```

5. Выбор данных:

```
local result = box.space.my_space:select{}
for _, row in ipairs(result) do
    print(row[1], row[2])
end
```

Результат:

```
---
- [1, 'example data']
...
```

6. Удаление записи из пространства имен:

```
box.space.my_space:delete{1}
```

Результат:

```
---
- [1, 'example data']
...
```

Пример запуска Lua-скрипта в консоли tarantool

1. В терминале создайте файл **app.lua** с помощью текстового редактора:

```
nano app.lua
```

2. Напишите код Lua-скрипта в файле:

```lua
-- app.lua

-- Настройка конфигурации
box.cfg{
listen = 3301,
memtx_memory = 1024 * 1024 * 256
}

-- Проверка существования пространства и создание, если оно не существует
local space_name = 'example_space'
local space = box.space[space_name]

if not space then
space = box.schema.space.create(space_name)
space:create_index('primary', { type = 'tree', parts = {1, 'unsigned'} })
print('Space and index created.')
else
print('Space already exists.')
end

-- Добавление данных, если они ещё не существуют
local count = space:count()
if count == 0 then
space:insert{1, 'Hello, Tarantool!'}
print('Data inserted.')
else
print('Data already exists.')
end

-- Выбор данных и вывод
local result = space:select{}
print('Selected data:')
for _, row in ipairs(result) do
print(row[1], row[2])
end
```

Сохраните файл и закройте редактор. Для этого нажмите **Ctrl + O**, затем **Enter** для сохранения, и **Ctrl + X** для выхода.

3. Запустите консоль **tarantool**:

```
tarantool
```

4. В консоли **tarantool** выполните Lua-скрипт:

```
dofile('app.lua')
```

Результат:

```
Hello, Tarantool!
```

Пример работы с SQL

Tarantool поддерживает SQL-запросы. Для использования функций SQL, используя tarantool в качестве клиента, выполните:

1. Включение SQL-режима:

```
box.cfg{listen = 3301}
```

2. Для создания таблицы используйте команду **CREATE TABLE**:

```
box.execute('CREATE TABLE employees (id INTEGER PRIMARY KEY, name TEXT)')
```

Если SQL-запрос был выполнен успешно и затронул одну строку **- row_count: 1**, то таблица была успешно создана.

3. Чтобы вставить данные в таблицу, выполните команду **INSERT INTO**:

```
box.execute('INSERT INTO employees (id, name) VALUES (1, \'John Doe\')')
box.execute('INSERT INTO employees (id, name) VALUES (2, \'Jane Smith\')')
box.execute('INSERT INTO employees (id, name) VALUES (3, \'Alice Johnson\')')
```

Вывод **--- ...** после выполнения команды **box.execute()** в консоли **tarantool** указывает на то, что запрос был выполнен успешно, но подробная информация о результате не отображается в текущем выводе.

4. Для выбора данных из таблицы используйте команду **SELECT**:

```
local result = box.execute('SELECT * FROM employees')
for _, row in ipairs(result.rows) do
    print(row[1], row[2])
end
```

Вывод:

```
1       John Doe
2       Jane Smith
3       Alice Johnson
```

Для выхода из консоли используйте команду:

```
os.exit()
```

Управление экземплярами с помощью tarantoolctl

Tarantoolctl позволяет управлять экземплярами **tarantool**, выполнять команды SQL, подключаться к удаленным серверам и др.

Основные команды и опции, которые можно использовать с **tarantoolctl** для управления экземплярами **tarantool**:

1. Запуск экземпляра **tarantool** (example - замените на любое имя экземпляра):

```
sudo tarantoolctl start example
```

2. Остановка экземпляра **tarantool**:

```
sudo tarantoolctl stop example
```

3. Проверка состояния сервера:

```
sudo tarantoolctl status example
```

4. Перезапуск экземпляра:

```
sudo tarantoolctl restart example
```

5. Ротация логов:

```
tarantoolctl logrotate example
```

6. Проверка экземпляра:

```
tarantoolctl check example
```

7. Вход в командную строку интерфейса **tarantool**:

```
tarantoolctl enter example [--language=<language>]
```

8. Выполнение Lua-скрипта:

```
tarantoolctl eval example <FILE>
```

9. Выполнение команд через стандартный ввод:

```
<команда> | tarantoolctl eval example
```

10. Подключение к серверу **tarantool** по адресу example.com и порту 3301:

```
tarantoolctl connect tcp://example.com:3301
```

11. Передача команд через стандартный ввод на удаленный экземпляр:

Например, у вас есть сервер **tarantool**, работающий на хосте example.com и порту 3301. Вы хотите выполнить команду SQL, которая добавляет запись в таблицу, и затем получить результат.

```
echo "box.execute('INSERT INTO employees (id, name) VALUES (4, \'Jane Doe\')')" | tarantoolctl connect tcp://example.com:3301
```

12. Для получения информации об установленном **tarantoolctl** выполните:

```
tarantoolctl --help
```

13. Для определения списка запущенных на узле экземпляров класса **tarantool** используйте:

```
ls /etc/tarantool/instances.available
```

Исправление ошибок

При возникновении ошибки:

```
can't initialize storage: Failed to lock WAL directory . and hot_standby mode is off
```

В терминале выполните поиск запущенных процессов tarantool. Утилита **pgrep** работает следующим образом: вы задаете имя процесса, а утилита показывает его идентификатор:

```
sudo pgrep -f tarantool
```

Примерный вывод:

```
4143 5046 5181 5190
```

Принудительно завершить процессы можно, используя команду **kill -9**:

```
sudo kill -9 4143 sudo kill -9 5046 sudo kill -9 5181 sudo kill -9 5190
```

Java OpenJDK в РЕД ОС

В репозитории РЕД ОС доступно использование нескольких версий **Java OpenJDK**. Даже если у вас установлена последняя актуальная версия, некоторые программы могут устанавливать в качестве зависимостей другие (например, более старые) версии **JDK**, поэтому существует возможность иметь несколько версий **JDK** без возникновения конфликтов.

В РЕД ОС по умолчанию уже установлена **OpenJDK** версии **8**. Проверить это можно командой:

```
java -version

openjdk version "1.8.0_275"
OpenJDK Runtime Environment (build 1.8.0_275-b01)
OpenJDK 64-Bit Server VM (build 25.275-b01, mixed mode)
```

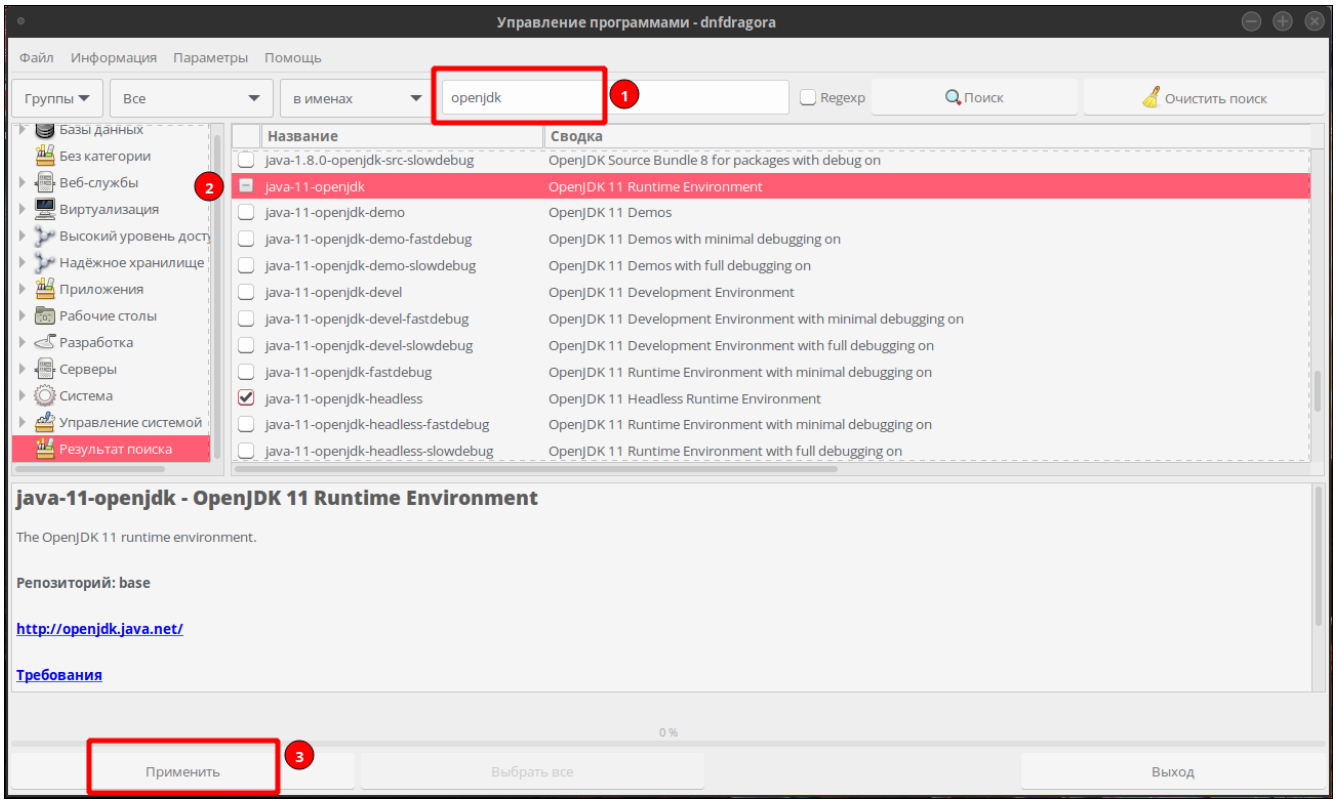
При необходимости можно установить более новую версию **Java**. В качестве примера установим **Java 11**. Сделать это можно двумя способами:

- 1 способ — через графический менеджер пакетов **dnfdragora**.

В «**Главном меню**» — «**Администрирование**» — «**Управление пакетами dnfdragora**» выполните поиск необходимых пакетов по ключевому слову «**openjdk**» и отметьте галочками пакеты:

- **java-11-openjdk**;
- **java-11-openjdk-headless**.

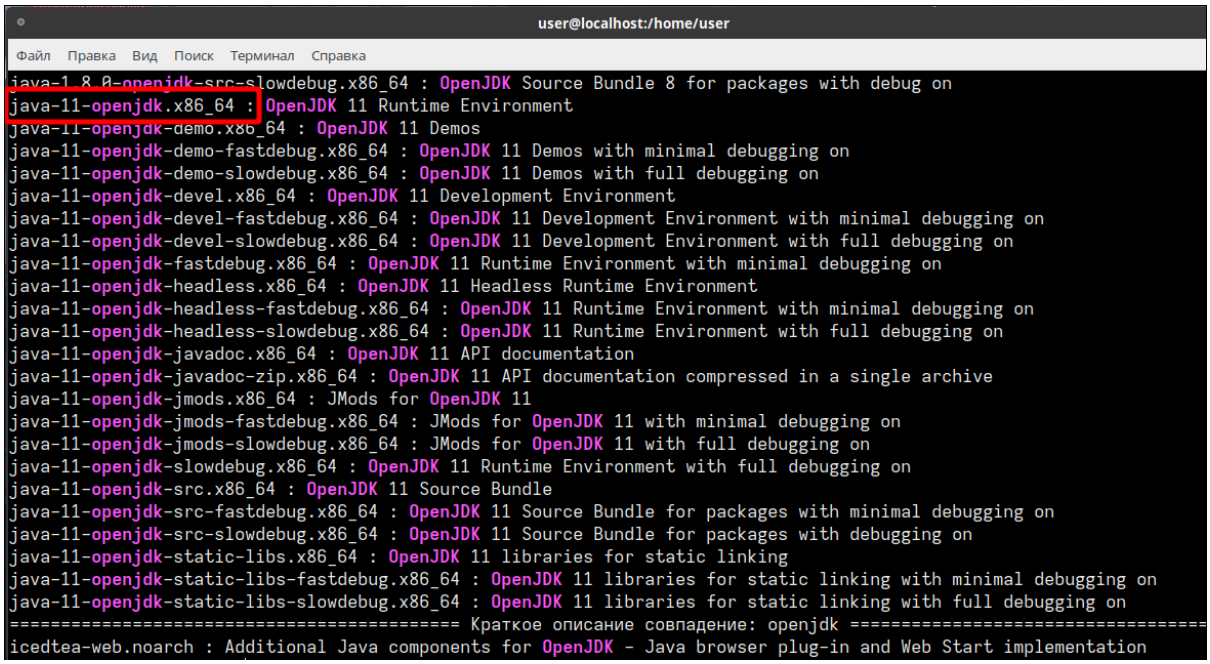
После этого нажмите кнопку «**Применить**» и дождитесь окончания установки пакетов.



- 2 способ — через терминал.

Для этого необходимо проверить доступные для установки пакеты с помощью команды:

```
dnf search openjdk
```



Затем из полученного списка нужно установить файл вида «**java-<версия>-openjdk**».

Для этого перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install java-11-openjdk
```

После установки новой версии по умолчанию будет использоваться именно она. Проверить используемую версию можно следующей командой:

```
java -version

openjdk version "11.0.10" 2021-01-19 LTS
OpenJDK Runtime Environment 18.9 (build 11.0.10+9-LTS)
OpenJDK 64-Bit Server VM 18.9 (build 11.0.10+9-LTS, mixed mode, sharing)
```

Для того чтобы при необходимости переключаться на ту или иную версию **OpenJDK**, выполните команду:

```
alternatives --config java

Имеется 2 программ, которые предоставляют 'java'.

  Выбор    Команда
-----------------------------------------------
   1           java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.275.b01-1.el7.x86_64/jre/bin/java)
*+ 2           java-11-openjdk.x86_64 (/usr/lib/jvm/java-11-openjdk-11.0.10.0.9-1.el7.x86_64/bin/java)

Enter - сохранить текущий выбор[+], или укажите номер: 1
```

Знаком «**+**» выделена версия, используемая по умолчанию. Для переключения на необходимую для работы версию следует указать ее порядковый номер или нажать **Enter**, если нужная версия выбрана.

Проверим установленный выбор командой:

```
java -version

openjdk version "1.8.0_275"
OpenJDK Runtime Environment (build 1.8.0_275-b01)
OpenJDK 64-Bit Server VM (build 25.275-b01, mixed mode)
```

PHP 8.X на РЕД ОС

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: php-8.1, php82-release, php83-release

Установка **PHP** версии **8.1** производится командой (потребуются права пользователя **root**):

```
sudo dnf install php
```

Пакеты **PHP** версии **8.2, 8.3** располагаются в подключаемых репозиториях, поэтому порядок обновления несколько отличается от обычного.

Обновление пакетов **PHP** до версии **8.X** на **РЕД ОС** производится с помощью следующих команд (потребуются права пользователя **root**):

```
sudo dnf install php8X-release
sudo dnf clean all
sudo dnf makecache
sudo dnf update php*
```

где X — номер необходимой для установки версии.

Сбор диагностической информации о РЕД ОС (loginfo)

Графический интерфейс
Консольный вариант

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО:** loginfo-0.15-1

loginfo – утилита сбора технической информации о РЕД ОС для технической поддержки.

Вы можете подробнее ознакомиться с работой утилиты **loginfo**, просмотрев наши обучающие видео:

- на **RuTube** — Сбор диагностической информации о РЕД ОС;
- в **Яндекс.Дзен** — Сбор диагностической информации о РЕД ОС;
- в **VK Видео** — Сбор диагностической информации о РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Для установки утилиты перейдите в сеанс пользователя **root**:

```
su -
```

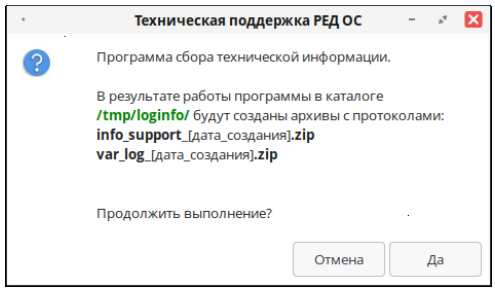
и выполните команду:

```
dnf install loginfo
```

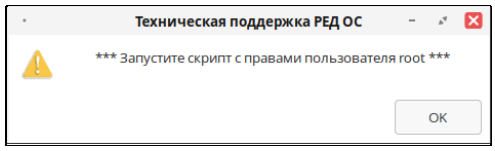
Графический интерфейс

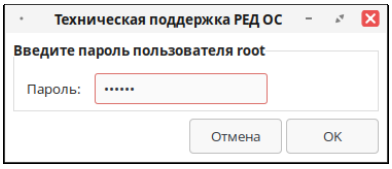
Запуск утилиты доступен из «**Главного меню**» - «**Системные**» - «**Сбор информации о системе**».

При инициализации утилиты вы увидите следующее диалоговое окно:

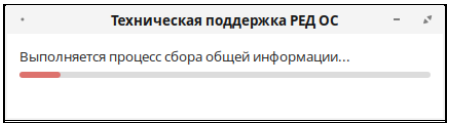


Т.к. для работы в программе необходимы права пользователя **root**, будет выведено следующее предупреждение и произведен запрос на ввод пароля пользователя **root**.



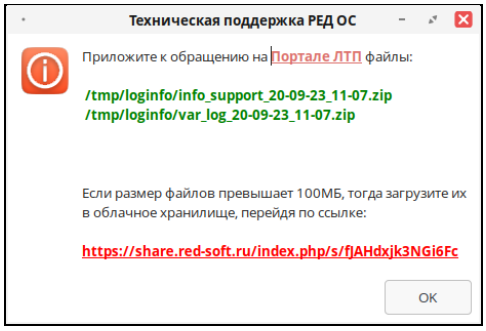


Будет запущен процесс сбора информации.



После сбора информации будет выведено информационное сообщение с контактами для отправки собранных данных в техническую поддержку.

Архивные файлы будут сформированы по пути **/tmp/loginfo**.



Консольный вариант

Для работы с утилитой необходимы права пользователя **root**:

```
su -
```

Для запуска процесса сбора информации выполните:

```
loginfo.sh
```

Loginfo также поддерживает дополнительный функционал, для просмотра выполните:

```
loginfo.sh --help
```

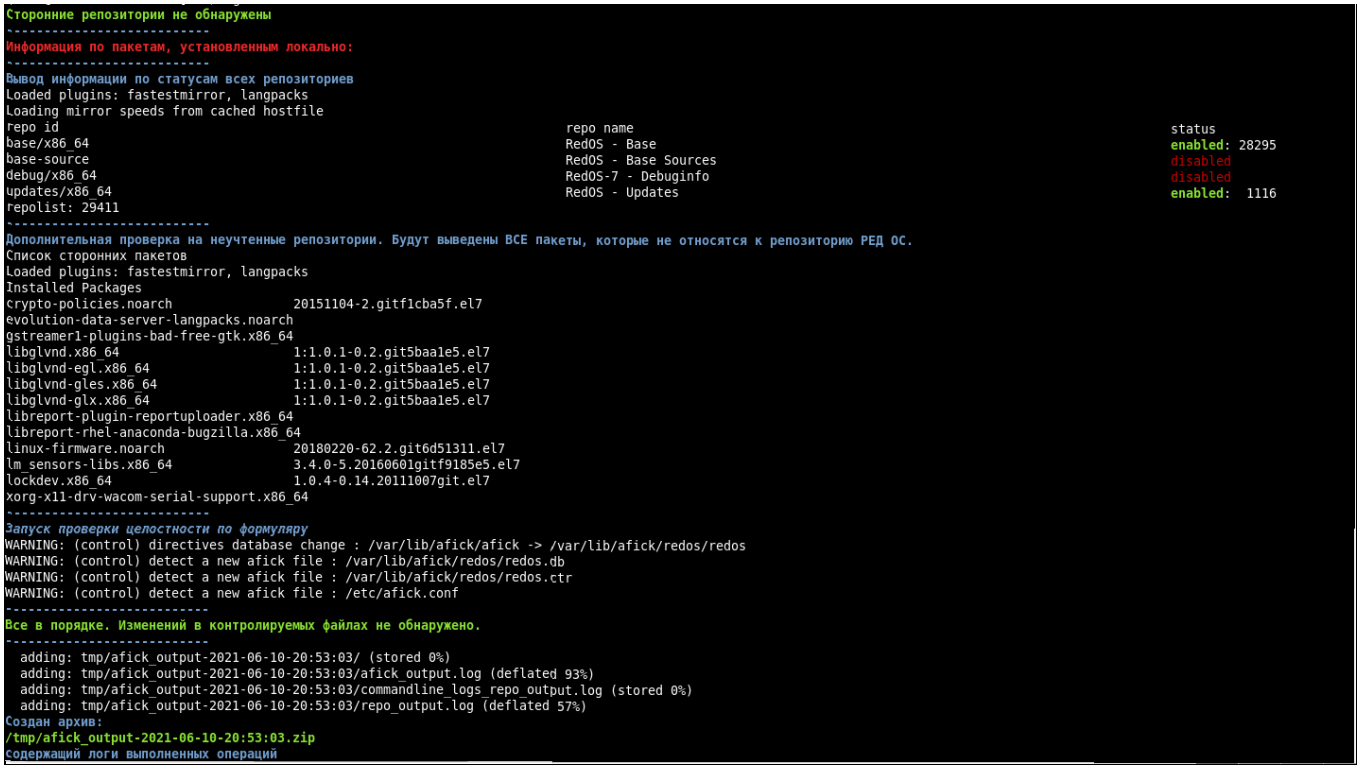
Для примера выполним дополнительную диагностику ОС.

Создание краткой сводки по аппаратным характеристикам:

```
loginfo.sh --hw-id

Создан файл /tmp/loginfo/hw-id-2022-06-21-11-50-35.txt
```

Проверка целостности сертифицированной редакции РЕД ОС:

```
loginfo.sh --afick
```



Контроль целостности системы РЕД ОС также осуществляется с помощью утилиты **afick**. Подробнее см. в нашей статье «Afick - утилита контроля целостности системы».

Проверка файловой системы на наличие ошибок

Параметры fsck
Пример проверки диска на ошибки с помощью fsck
Запуск автоматической проверки и исправления найденных ошибок
Ручное добавление параметров в меню GRUB при загрузке ОС
Добавление параметров в меню GRUB с помощью утилиты grubby
Создание файла /forcefsck
Запуск проверки в ручном режиме
Использование загрузочного диска/flash для проверки файловой системы на ошибки
Проверка LVM-разделов с помощью утилиты fsck

В определенных случаях (в результате сбоя или некорректного завершения работы) на файловой системе могут накапливаться ошибки. В РЕД ОС для проверки файловой системы и исправления ошибок имеется утилита **fsck** ("file system consistency check").

Инструмент fsck обладает следующим функционалом:

- проверка файловой системы при возникновении проблем (не загружается система/поврежденные файлы) или в качестве профилактического обслуживания;
- диагностика состояния внешних накопителей, таких как SD-карты или USB-накопители.

Базовый синтаксис соответствует следующему шаблону:

```
fsck <опции> <файловая_система>
```

В качестве *файловой системы* может быть устройство, точка монтирования или раздел, в том числе LVM.

Вы можете подробнее ознакомиться с возможностями проверки файловой системы на наличие ошибок, просмотрев наши обучающие видео:

- на **RuTube** — Проверка файловой системы на наличие ошибок;
- в **Яндекс.Дзен** — Проверка файловой системы на наличие ошибок;
- в **VK Видео** — Проверка файловой системы на наличие ошибок.

На наших каналах вы также сможете найти много другой полезной информации.

Параметры fsck

fsck –p – утилита автоматически исправит найденные ошибки.

Вывод аналогичен простой проверке.

fsck –c – проверка файловой системы на поврежденные сектора.

```
bash-5.2# fsck –c
fsck from util-linux 2.38.1
e2fsck 1.46.3 (27-Jul-2021)
Checking for bad blocks (read-only test): done
/dev/sda4: Updating bad block inode.
Pass 1: Checking inides, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information

/dev/sda4: *****FILE SYSTEM WAS MODIFIED *****
/dev/sda4: *****REBOOT SYSTEM *****
/dev/sda4: 358151/1114112 files (0.1% non-contiguous), 2377380/4455680 blocksbash-5.2#
```

Для получения списка команд наберите **fsck –-help** или **fsck –h.**

Опция	Описание
-a	Устаревшая опция. Указывает исправлять все найденные ошибки без одобрения пользователя.
-r	Применяется для файловых систем ext. Указывает fsck спрашивать пользователя перед исправлением каждой ошибки

-n	Выполняет только проверку ФС, без исправления ошибок. Используется также для получения информации о ФС
-c	Применяется для файловых систем ext3/4. Помечает все повреждённые блоки для исключения последующей записи в них
-f	Принудительно проверяет ФС, даже если ФС исправна
-y	Автоматически подтверждает запросы к пользователю
-b	Задаёт адрес суперблока
-p	Автоматически исправлять найденные ошибки. Заменяет устаревшую опцию -a
-A	Проверяет все ФС
-C [<fd>]	Показывает статус выполнения. Здесь fd – дескриптор файла при отображении через графический интерфейс
-l	Блокирует устройство для исключительного доступа
-M	Запрещает проверять примонтированные ФС
-N	Показывает имитацию выполнения, без запуска реальной проверки
-P	Проверять вместе с корневой ФС
-R	Пропускает проверку корневой ФС. Может использоваться только совместно с опцией -A
-r [<fd>]	Выводит статистику для каждого проверенного устройства
-T	Не показывать заголовок при запуске
-t <тип>	Задаёт ФС для проверки. Можно задавать несколько ФС, перечисляя через запятую
-V	Выводит подробное описание выполняемых действий

Пример проверки диска на ошибки с помощью fsck

Запуск автоматической проверки и исправления найденных ошибок

Существует несколько способов запуска автоматической проверки на ошибки:

1. Ручное добавление параметров в меню **GRUB** при загрузке ОС.

2. Добавление параметров в меню **GRUB** с помощью утилиты **grubby**.

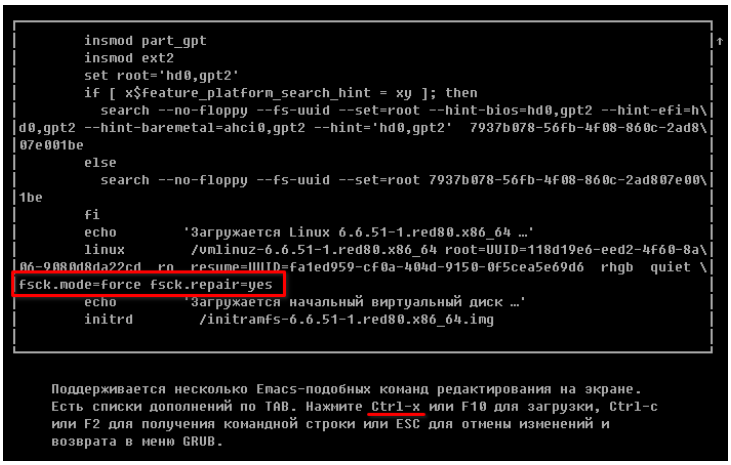
3. Создание файла **/forcefsck**.

1. Ручное добавление параметров в меню GRUB при загрузке ОС

Первый вариант проверки и исправления ошибок на разделах жесткого диска.

В меню **GRUB** перейдите в режим редактирования загрузочной строки, нажав при этом клавишу **e**. Добавьте параметры в конце строки, которая начинается на **linux**:

```
fsck.mode=force fsck.repair=yes
```



Нажмите **Ctrl+X** для запуска ОС с этими параметрами, во время запуска будет произведена проверка разделов диска, и при наличии ошибок произведено их исправление.

2. Добавление параметров в меню GRUB с помощью утилиты grubby

Существует еще один способ добавления параметров ядра для принудительной проверки файловой системы на ошибки и их исправления. Добавить параметры можно командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --args="fsck.mode=force fsck.repair=yes"
```

Удалить установленные параметры можно следующей командой:

```
grubby --update-kernel /boot/vmlinuz-$(uname -r) --remove-args="fsck.mode=force fsck.repair=yes"
```

3. Создание файла /forcefsck

Бывают ситуации, когда систему необходимо проверить на наличие ошибок в *незапланированный* момент. Для этого можно **принудительно** запустить утилиту **fsck** для проверки при следующей перезагрузке. Запуск осуществляется командой:

```
sudo touch /forcefsck
```

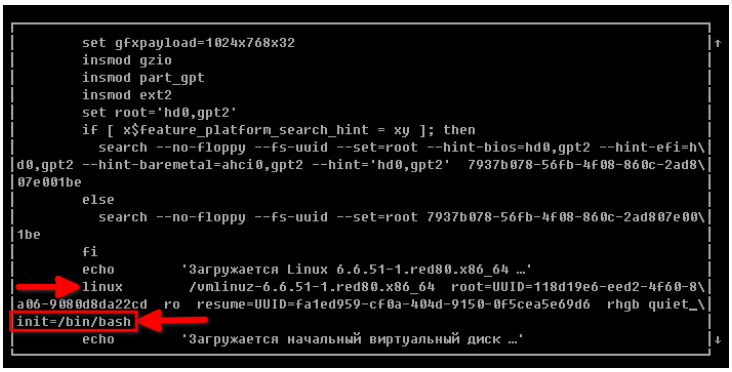
Команда **sudo** (после ввода пароля) предоставит права для создания с помощью **touch** пустого файла в корне диска **/forcefsck**, который послужит сигналом (флагом) для **fsck**, что нужно проверить диски.

Останется только перезагрузить компьютер и **fsck** начнет проверять все жесткие диски, указанные в **/etc/fstab**.

Запуск проверки в ручном режиме

Следующий метод относится к проверке диска, когда операционная система загружена в режиме **single mode**.

1. Запустим ОС в **single mode**, для этого пропишите в меню загрузки grub параметр init=/bin/bash в конце строки, которая начинается на linux, см. рисунок.



Также данная строка может начинаться с linuxefi, этот параметр характерен для систем с загрузкой в **UEFI**. Нажмите **"ctrl+x"** для запуска с этим параметром(init=/bin/bash).

2. Запустите проверку выполнив команду:

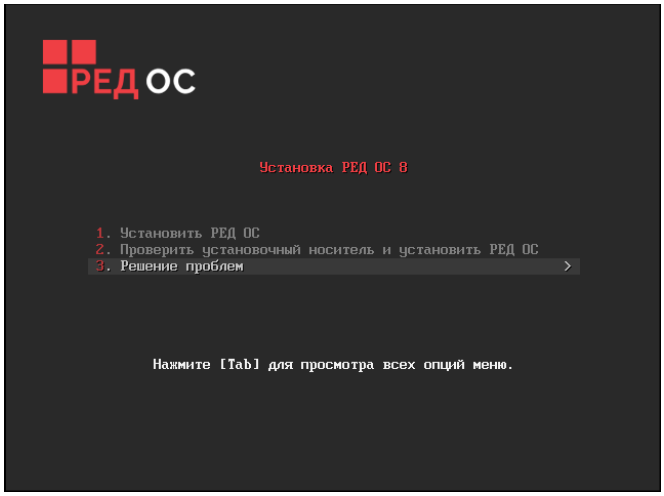
```
/usr/sbin/fsck -ACVfyv
```

Во время проверки на экране появится отчет о выполненных операциях, если отчет длинный, то можно его можно пролистать вверх сочетанием клавиш shift+PageUp. После проверки дисков перезагрузите компьютер, нажав на кнопку на системном блоке.

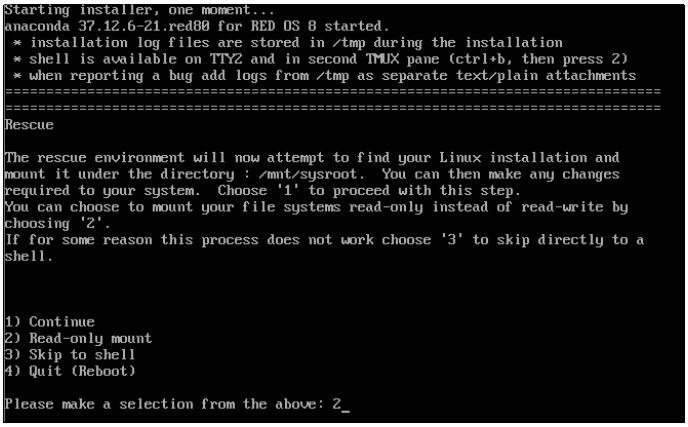
Наглядное видео примера проверки диска на ошибки:

Использование загрузочного диска/flash для проверки файловой системы на ошибки.

Загрузившись в режим восстановления операционной системы РЕД ОС с помощью загрузочного диска или съемного накопителя с установленным образом операционной системы РЕД ОС. Выберите пункт: **«Решение проблем» -> «Исправить установленную RED OS»**.



Система перезагрузится в режим восстановления. Введите «**2**» и нажмите 2 раза **Enter**. Так вы смонтируете операционную систему в режим «**Только для чтения**»



Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Потом введите команду:

```
# chroot /mnt/sysimage
```

После этого можете вводить **fsck**:

```
# fsck -ACVfyv
```

Если проверка завершится с такой ошибкой:

```
[путь_к_файловой_системе] is mounted
```

Введите:

```
umount [путь_к_файловой_системе]
```

И еще раз запустите утилиту **fsck**:

```
# fsck -ACVfyv
fsck from util-linux 2.38.1
...
```

Если система не выявит ошибок, то получится такой вывод:

```
[путь_к_файловой_системе] clean ...
```

Чтобы выйти из режима восстановления, вы должны смонтировать все разделы, которые были отмонтированы командой **umount**, с помощью команды **mount**, нажать сочетание клавиш **ctrl+d**, а затем ввести команду **reboot**, которая перезапустит вашу операционную систему.

```
# reboot
```

По умолчанию, утилита **fsck** при проверке будет использовать разделы, указанные в **/etc/fstab/**, сформированные при установке операционной системы РЕД ОС.

Проверка LVM-разделов с помощью утилиты fsck

Перед проведением проверки необходимо найти устройство и размонтировать его.

Для просмотра всех подключенных устройств и проверки расположения диска выполните команду:

lsblk

```
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 20G 0 disk
├─sda1 8:1 0 1G 0 part /boot
└─sda2 8:2 0 19G 0 part
├─ro_redos-root 253:0 0 17G 0 lvm /
└─ro_redos-swap 253:1 0 2G 0 lvm [SWAP]
sr0 11:0 1 4,3G 0 rom /run/media/user/redos-MUROM-7.3.1 x86_64
```

При попытке запустить проверку на смонтированном диске или разделе в консоли появляется предупреждение о том, что невозможно продолжить проверку, так как диск смонтирован.

fsck -nf /dev/ro_redos/root

```
fsck из util-linux 2.38.1
e2fsck 1.46.3 (27-Jul-2021)
Warning! /dev/mapper/ro_redos-root is mounted.
```

Для того чтобы размонтировать диск, следует использовать команду:

```
umount <файловая_система>
```

Однако попытка выполнить данную процедуру на работающей ОС ни к чему не приведет.

umount /dev/ro_redos/root

```
umount: /: target is busy.
```

Также проблемой при попытке проверить LVM-разделы может быть и то, что они являются не активными. Для проверки следует использовать команду:

lvscan

```
ACTIVE '/dev/ro_redos/swap' [2,00 GiB] inherit
ACTIVE '/dev/ro_redos/root' [<17,00 GiB] inherit
```

Для активации раздела служит команда:

```
vgchange –ay <раздел>
```

Таким образом, можно сделать вывод, что проверка LVM-разделов через консоль с использованием утилиты **fsck** невозможна. Но это не значит, что LVM-разделы совсем не подлежат проверке. Существует как минимум два способа, позволяющие провести диагностику LVM-разделов.

Первым способом является проведение проверки через консоль загрузчика операционной системы **GRUB**.

А вторым - запуск утилиты **fsck** в **live-сессии** системы.

Очевидным плюсом при проверке дисковых пространств, в том числе LVM-разделов, через live-сессию является то, что разделы там по умолчанию являются не смонтированными. Поэтому проверка LVM-раздела будет выполнена с первого раза.

fsck /dev/ro_redos/root

```
fsck из util-linux 2.38.1
e2fsck 1.46.3 (27-Jul-2021)
/dev/mapper/ro_redos-root: recovering journal
Clearing orphaned inode 423398 (uid=0, gid=0, mode=0100644, size=229605)
Clearing orphaned inode 172559 (uid=0, gid=0, mode=0100644, size=24992)
Clearing orphaned inode 387 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 386 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 384 (uid=1000, gid=1000, mode=0100700, size=4096)
Clearing orphaned inode 296594 (uid=1000, gid=1000, mode=0100644, size=9059)
Setting free inodes count to 890417 (was 890569)
Setting free inodes count to 2578845 (was 2585477)
/dev/mapper/ro_redos-root: clean, 223695/11141112 files, 1876579/4455424 blocks
```

Проверка состояния жесткого диска

Smartmontools
Gsmartcontrol
Gnome disk utility
BadBlocks

Smartmontools

Smartmontools — утилита, предназначенная для проверки состояния жесткого диска. Чтобы посмотреть количество установленных жестких дисков наберите команду:

```
$ sudo smartctl --scan
```

На запрос пароля привилегированного пользователя, введите пароль локального пользователя с правами администратора.

Чтобы посмотреть информацию о жестком диске, а также узнать, поддерживает ли он технологию анализа SMART и включена ли она, наберите команду:

```
smartctl -i /dev/sda

smartctl 6.6 2018-08-10 r4748 [x86_64-linux-4.19.56-2.el7.x86_64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org
=== START OF INFORMATION SECTION ===
Model Family: Seagate Barracuda 3.5
Device Model: ST1000DM010-2EP102
Serial Number: ZN179JYJ
LU WWN Device Id: 5 000c50 0b6491aa4
Firmware Version: CC43
User Capacity: 1 000 204 886 016 bytes [1,00 TB]
Sector Sizes: 512 bytes logical, 4096 bytes physical
Rotation Rate: 7200 rpm
Form Factor: 3.5 inches
Device is: In smartctl database [for details use: -P show]
ATA Version is: ATA8-ACS T13/1699-D revision 4
SATA Version is: SATA 3.0, 6.0 Gb/s (current: 3.0 Gb/s)
Local Time is: Thu Aug 22 14:01:23 2019 MSK
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

В данном выводе указана информация о вашем жестком диске.

SMART support is: Available - device has SMART capability — жесткий диск поддерживает технологию анализа SMART. Если технология не поддерживается, вместо слова **Available** будет **Unavailable**.

SMART support is: Enabled — технология анализа SMART включена. Если она выключена у вас, то для включения введите:

```
smartctl -s on /dev/sda
```

Для выключения:

```
smartctl -s off /dev/sda
```

Для вывода атрибутов SMART введите:

```
smartctl -A /dev/sda
```

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 10
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
  1 Raw_Read_Error_Rate     0x000f   080   072   006    Pre-fail  Always       -       110427890
  3 Spin_Up_Time            0x0003   097   097   000    Pre-fail  Always       -       0
  4 Start_Stop_Count        0x0032   100   100   020    Old_age   Always       -       25
  5 Reallocated_Sector_Ct   0x0033   100   100   010    Pre-fail  Always       -       0
  7 Seek_Error_Rate         0x000f   100   253   045    Pre-fail  Always       -       716102
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       42
 10 Spin_Retry_Count        0x0013   100   100   097    Pre-fail  Always       -       0
 12 Power_Cycle_Count       0x0032   100   100   020    Old_age   Always       -       25
183 Runtime_Bad_Block       0x0032   100   100   000    Old_age   Always       -       0
184 End-to-End_Error        0x0032   100   100   099    Old_age   Always       -       0
187 Reported_Uncorrect      0x0032   100   100   000    Old_age   Always       -       0
188 Command_Timeout         0x0032   100   100   000    Old_age   Always       -       0 0 0
189 High_Fly_Writes         0x003a   100   100   000    Old_age   Always       -       0
190 Airflow_Temperature_Cel 0x0022   070   059   040    Old_age   Always       -       30 (Min/Max 24/30)
193 Load_Cycle_Count        0x0032   100   100   000    Old_age   Always       -       25
194 Temperature_Celsius     0x0022   030   021   000    Old_age   Always       -       30 (0 21 0 0 0)
195 Hardware_ECC_Recovered  0x001a   003   003   000    Old_age   Always       -       110427890
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   200   200   000    Old_age   Always       -       0
240 Head_Flying_Hours       0x0000   100   253   000    Old_age   Offline      -       42h+36m+02.609s
241 Total_LBAs_Written      0x0000   100   253   000    Old_age   Offline      -       85113048
242 Total_LBAs_Read         0x0000   100   253   000    Old_age   Offline      -       25314842
```

В данном выводе стоит смотреть на значения в колонке **RAW_VALUE**.

Наиболее важные атрибуты отмечены как **pre_fail** в колонке **TYPE**.
1 Raw_Read_Error_Rate — количество ошибок чтения. На дисках Seagate и Samsung большие значения - норма.

2 Spin_Up_Time — время раскрутки диска из состояния покоя до рабочей скорости. Растет при износе диска.

5 Rellocated Sector Count — количество переназначенных секторов. Если диск обнаружил ошибку чтения/записи он перенесет сектор в резерв. Чем меньше значение, тем лучше.

7 Seek Error Rate — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики или поверхности жёсткого диска.

196 Rellocation Event Count - число операций переназначения. **Raw Value** хранит общее число попыток переноса информации с переназначенных секторов в резервную область как успешных так и провальных.
Более подробную информацию можно найти на странице википедии.

Для того, чтобы провести тест самодиагностики, наберите команду:

```
smartctl -t <тип_теста> /dev/sda
```

Тип теста может быть:

- **long** — расширенный;
- **short** — короткий;
- **conveyance** — тест на выявления ошибок при записи/чтении.

Тесты выполняются в фоновом режиме. Чтобы просмотреть результат, наберите:

```
smartctl -l selftest /dev/sda

=== START OF READ SMART DATA SECTION ===
SMART Self-test log structure revision number 1
Num Test_Description Status Remaining LifeTime(hours) LBA_of_first_error
# 1 Conveyance offline Self-test routine in progress 60% 43 -
# 2 Short offline Completed without error 00% 42 -
# 3 Short offline Aborted by host 90% 42 -
# 4 Short captive Completed without error 00% 41 -
# 5 Short offline Completed without error 00% 41 -
```

Completed without error означает, что тест завершился без ошибок.

Для просмотра полной информации, включающей в себя показатели атрибутов SMART, информацию о жестком диске и результаты диагностических тестов, наберите:

```
$ sudo smartctl -a /dev/sda
```

Gsmartcontrol

Gsmartcontrol — это графическая утилита к **smartctl**, позволяющая оценивать состояние и работоспособность жёсткого диска или

твердотельного накопителя по показаниям S.M.A.R.T.

Основными возможностями программы являются:

- вывод информации об ошибках работы дисков;
- отображение информации о дисках, атрибутов, статистики;
- включение/выключение автоматического сбора данных о состоянии дисков;
- выполнение тестов «SMART self-tests»;
- включение/выключение SMART;
- создание отчетов по проведенным тестам.

Вы можете подробнее ознакомиться с информацией о проверке состояния жесткого диска, просмотрев наши обучающие видео:

- на **RuTube** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **Яндекс.Дзен** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска;
- в **VK Видео** — Gsmartcontrol - графическая утилита для проверки состояния жесткого диска.

На наших каналах вы также сможете найти много другой полезной информации.

Установка

Для установки программы перейдите в сеанс пользователя **root**:

```
su -
```

и выполните команду:

```
dnf install gsmartcontrol
```

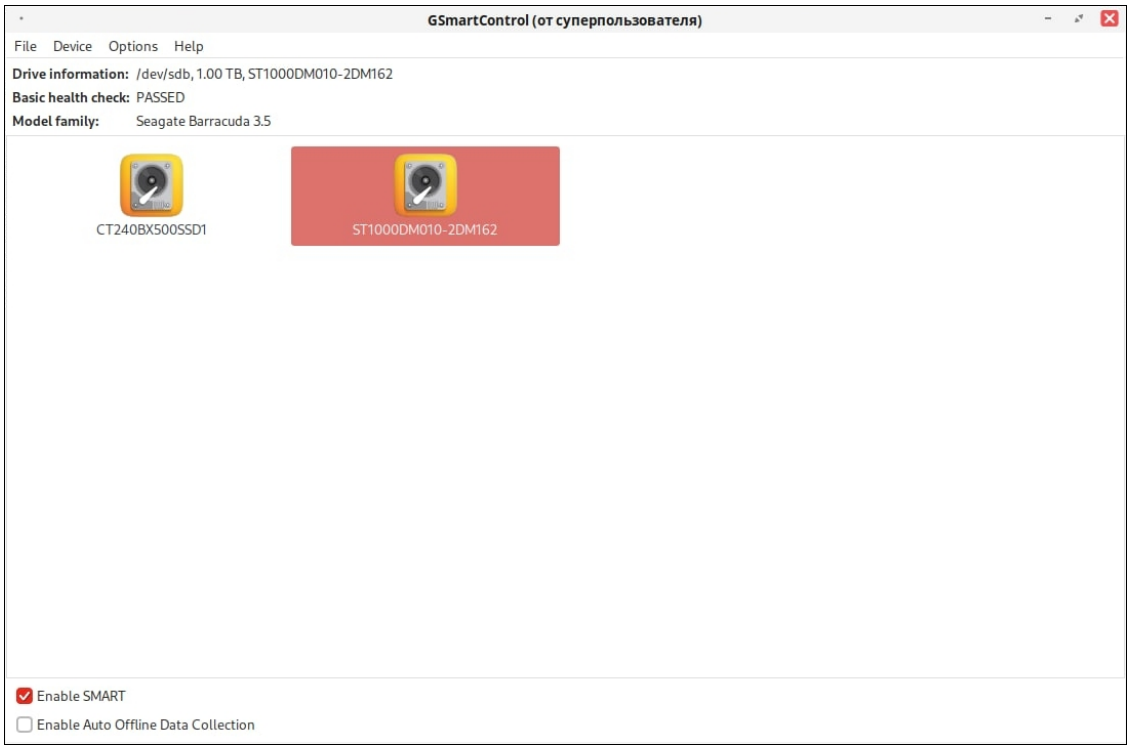
После установки программа будет доступна из «**Главного меню**» - «**Системные**» - «**Контроль S.M.A.R.T.**» или при помощи команды в терминале:

```
gsmartcontrol
```

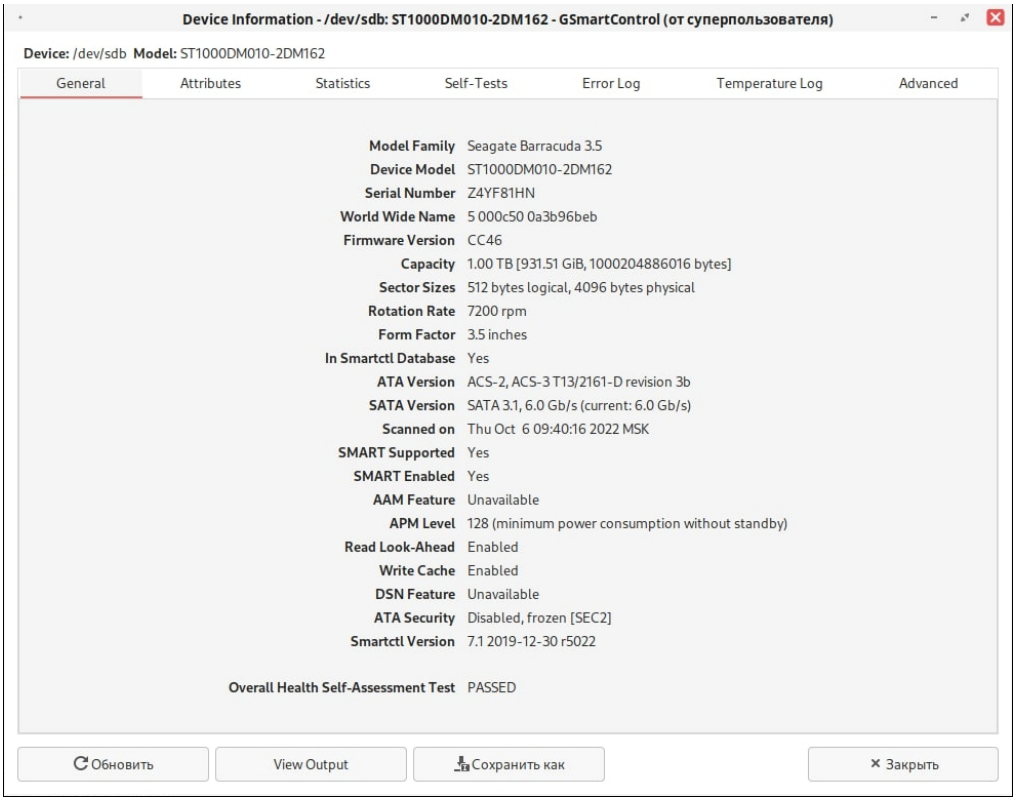
Обратите внимание, что для работы с утилитой необходимы права администратора или суперпользователя (**root**) системы.

Работа с утилитой

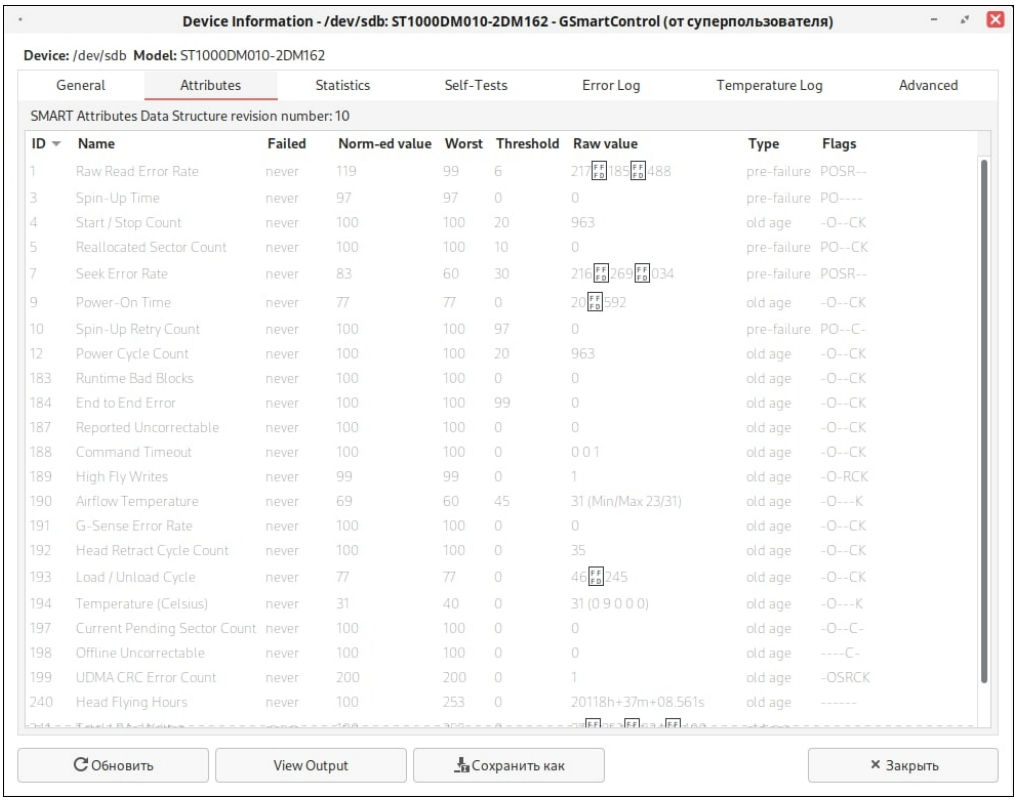
При запуске программа выглядит следующим образом:



Здесь отображены все диски, доступные для сканирования. При нажатии ПКМ на нужный диск выберите «**View details**», на вкладке «**General**» будет выведена вся информация о диске.



На вкладке «**Attributes**» указаны атрибуты проверки, нормальное, плохое и пороговое значение для каждого атрибута для удобного ориентирования по выявленным значениям в ходе проверок диска.



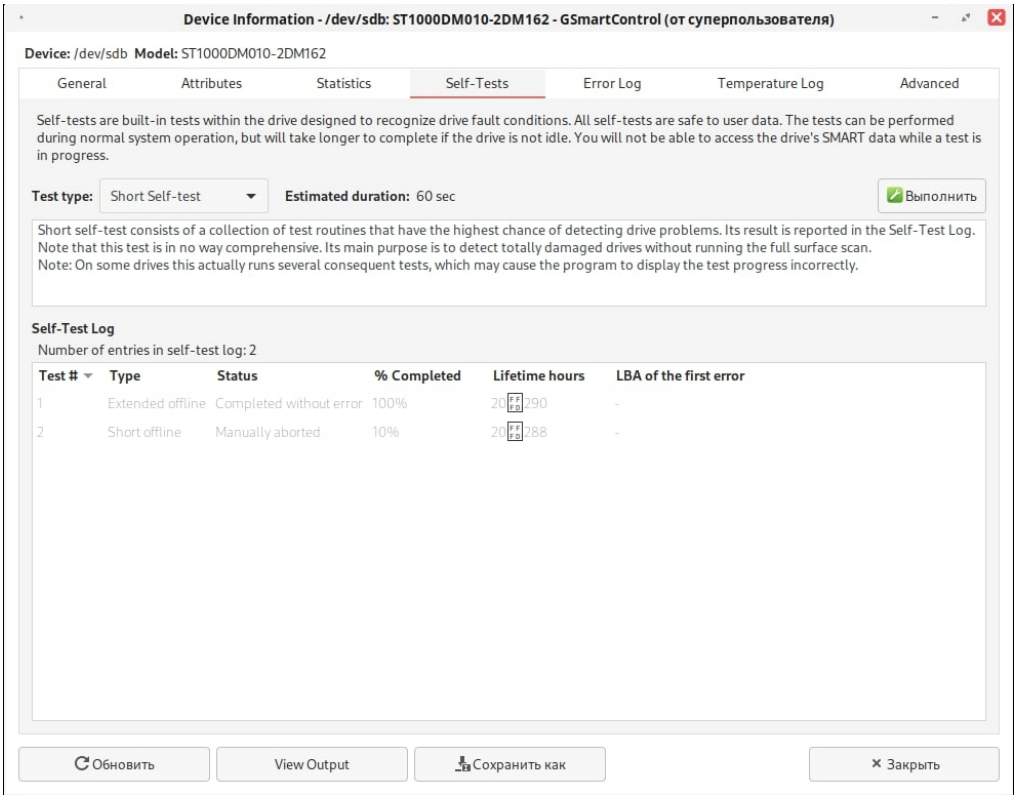
Часто используемые атрибуты:

- **Raw Read Error Rate** — частота ошибок при чтении данных с диска, происхождение которых обусловлено аппаратной частью диска, если значение большое, значит ошибки встречаются редко;
- **Spin-Up Time** — время раскрутки пакета дисков из состояния покоя до рабочей скорости, значение возрастает при износе диска;
- **Start/Stop Count** — полное число циклов запуск-остановка шпинделя. У дисков некоторых производителей (например, Seagate) — счётчик включения режима энергосбережения. В поле raw value хранится общее количество запусков/остановок диска;
- **Reallocated Sectors Count** — число операций переназначения секторов. Когда диск обнаруживает ошибку чтения/записи, он помечает сектор «переназначенным» и переносит данные в специально отведённую резервную область. Чем больше значение, тем хуже состояние поверхности дисков. Поле raw value содержит общее количество переназначенных секторов;
- **Seek Error Rat**e — частота ошибок при позиционировании блока магнитных головок. Чем их больше, тем хуже состояние механики и/или поверхности жёсткого диска;
- **Power-On Time** — число часов (минут, секунд — в зависимости от производителя), проведённых во включенном состоянии;
- **Spin-Up Retry Count** — число повторных попыток раскрутки дисков до рабочей скорости в случае, если первая попытка была неудачной. Если значение атрибута увеличивается, то велика вероятность неполадок с механической частью;
- **Power Cycle Count** — количество полных циклов включения-выключения диска;
- **End-to-End error** — данный атрибут - часть технологии HP SMART IV - означает, что после передачи данных через кэш-память чётность данных между хостом и жестким диском не совпадает;
- **Reported Uncorrectable** — ошибки, которые не могли быть восстановлены, используя методы устранения ошибки аппаратными средствами;
- **Command Timeout** — количество прерванных операций в связи с HDD тайм-аут. Обычно это значение атрибута должно быть равно нулю, и, если значение гораздо выше нуля, то, скорее всего, там будут какие-то серьезные проблемы с питанием или окисленные кабели для передачи данных;
- **Airflow Temperature** — температура воздуха внутри корпуса жёсткого диска;
- **G-sense Error Rate** — количество ошибок, возникающих в результате ударных нагрузок. Атрибут хранит показания встроенного акселерометра, который фиксирует все удары, толчки, падения и даже неаккуратную установку диска в корпус компьютера;
- **Load/Unload Cycle** — количество циклов перемещения блока магнитных головок в парковочную зону / в рабочее положение;
- **Temperature** — температура жёсткого диска;
- **Current Pending Sector Count** — число секторов, являющихся кандидатами на замену. Они пока не определены как плохие, но считывание с них отличается от чтения стабильного сектора, это так называемые подозрительные или нестабильные сектора;
- **Head flying hours** — время позиционирования головок.

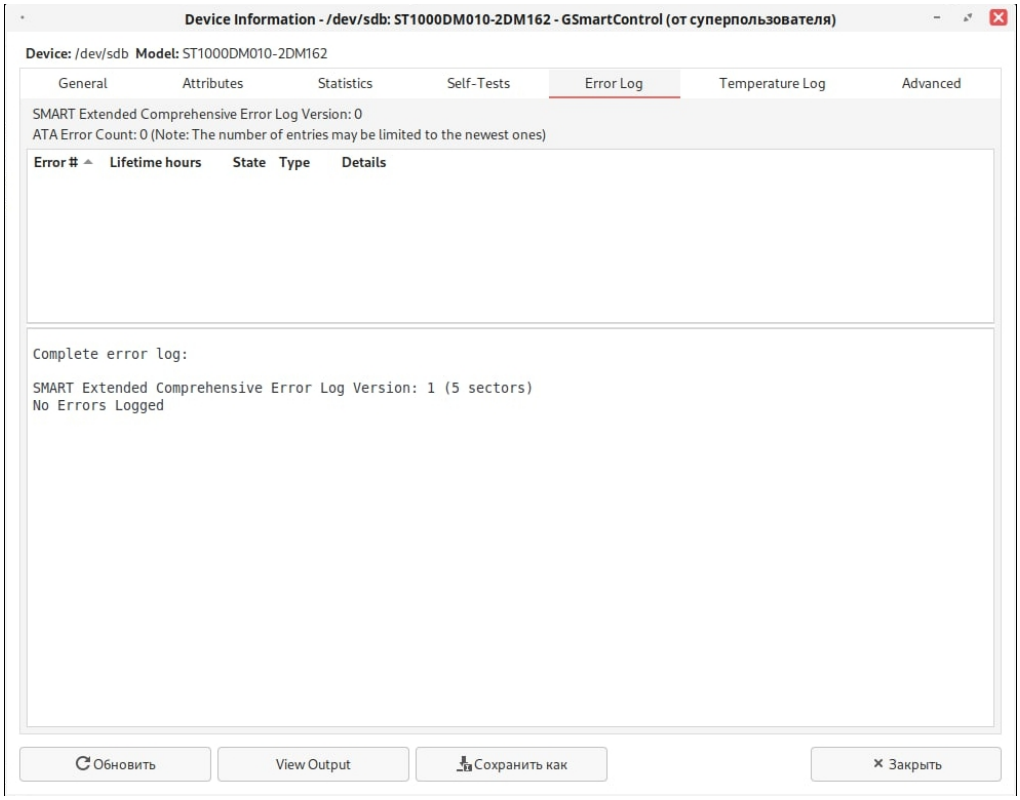
На вкладке «**Statistics**» выводится статистика использования диска.

На вкладке «**Self-Tests**» можно выполнять проверки жесткого диска. Доступно три варианта проверки:

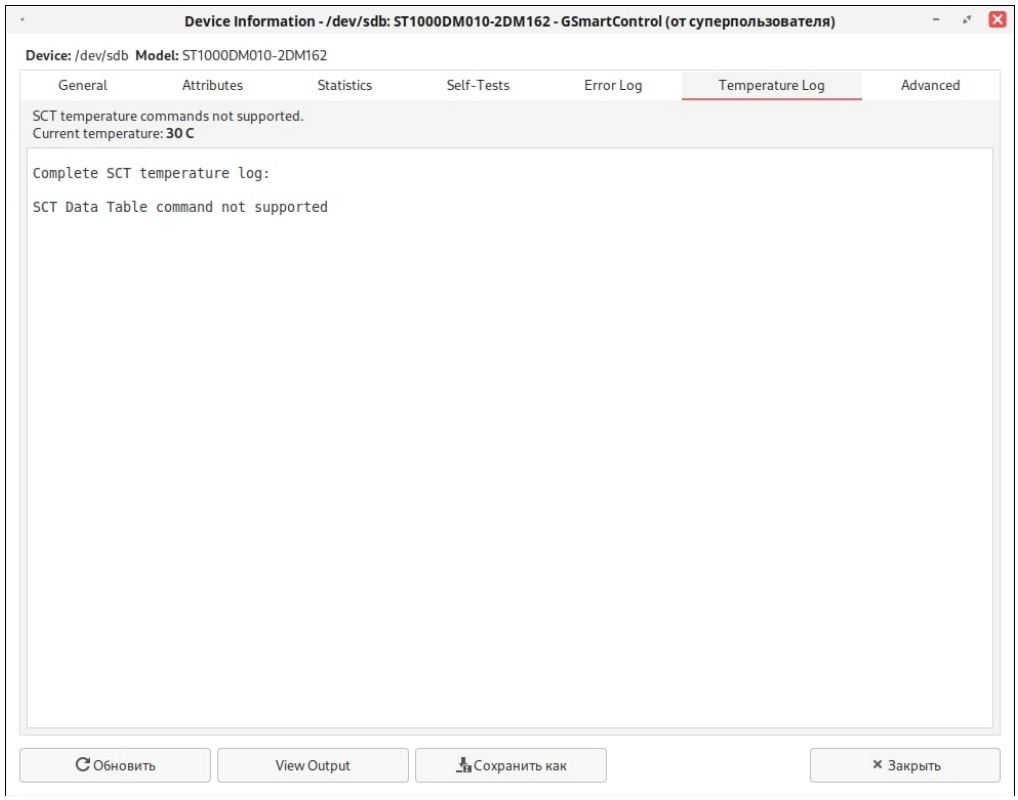
- **Быстрый тест** — продолжительностью 1 мин.
- **Расширенный тест** — продолжительностью более 1 часа, полный тест с процедурами проверки и пр.
- **Тест передачи** — продолжительностью 2 мин., тест подходит для обнаружения физических сбоев.



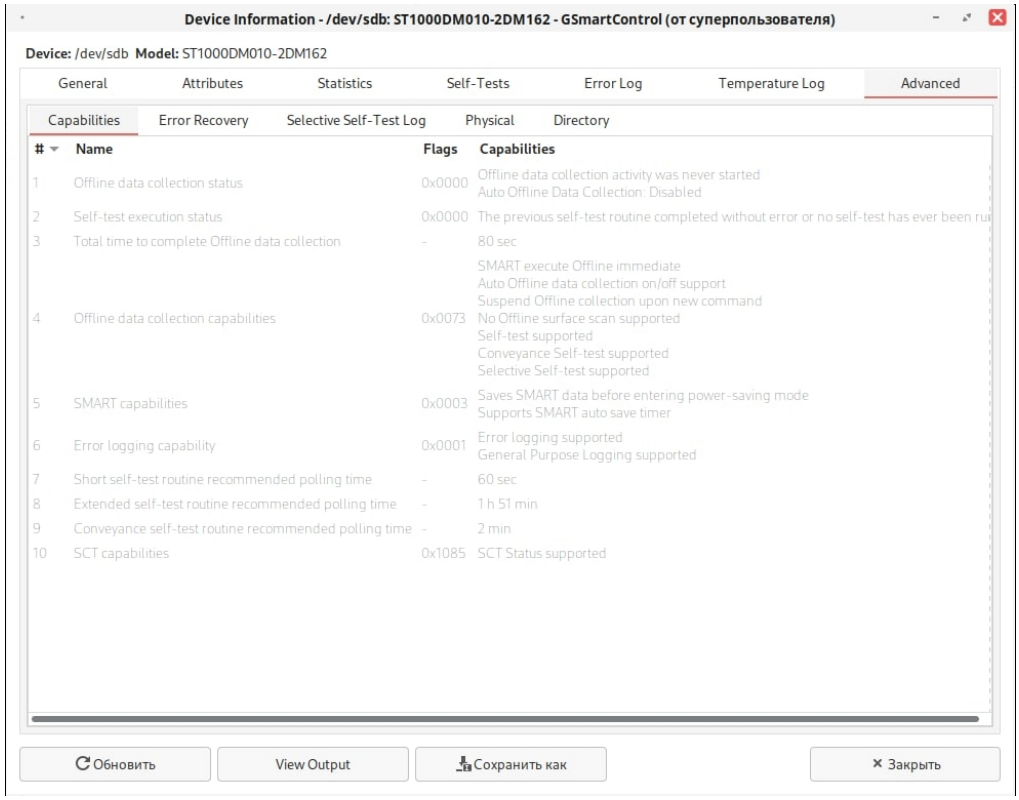
На вкладке «**Error Log**» ведется журнал ошибок с указанием деталей и подробным описанием при выборе любой из выявленных ошибок.



На вкладке «**Temperature Log**» ведется учет температурного режима используемого диска (если поддерживается).



На вкладке «**Advanced**» отображаются дополнительные параметры.



Все представленные утилитой результаты проверок можно сохранить в текстовом формате, например, для передачи информации о состоянии диска в сервисные центры или техническую поддержу.

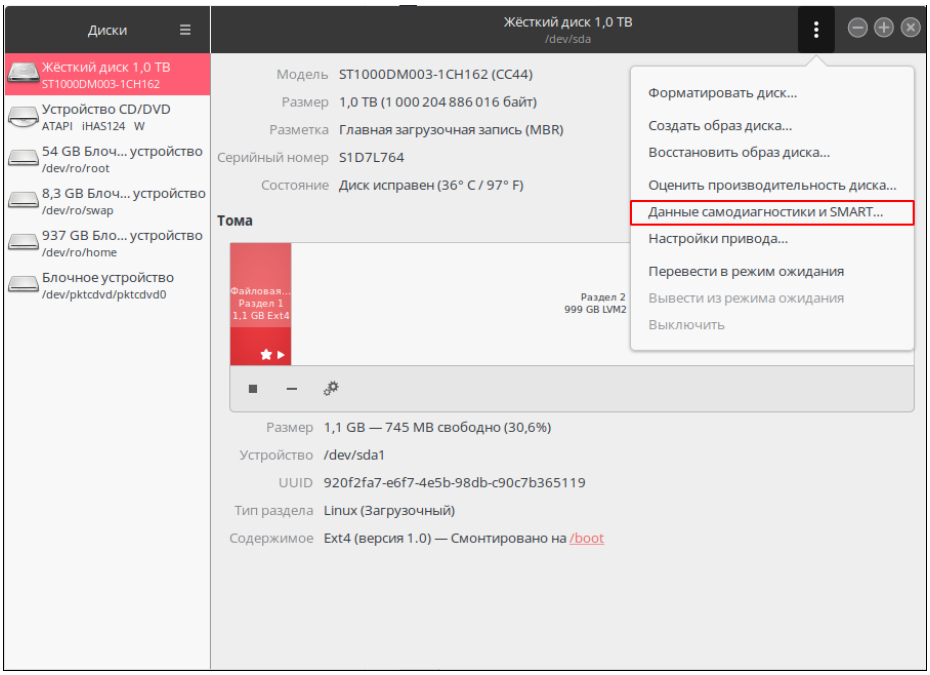
Gnome disk utility

Gnome disk utility — утилита с графической оболочкой для просмотра информации атрибутов SMART и тестирования диска. Для установки воспользуйтесь утилитой **yum** или **dnf** в зависимости от используемой версии РЕД ОС.

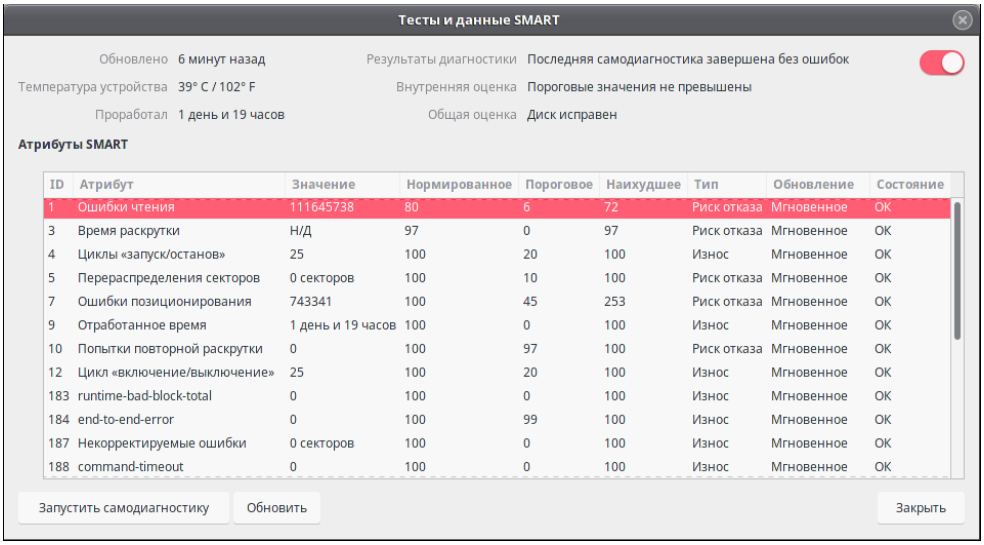
```
dnf install gnome-disk-utility
```

После установки утилита находится в **«Меню» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой Cinnamon и в **«Приложения» → «Стандартные» → «Диски»** в РЕД ОС с графической оболочкой MATE.

После запуска приложения, выберите жесткий диск на панели справа, и нажмите на значок дополнительного меню, там выберите данные самодиагностики SMART.



В открывшемся окне вы можете просмотреть значения атрибутов SMART, температуры жесткого диска, результат последнего теста самодиагностики и запустить новый тест. Доступные тесты аналогичные таковым из утилиты **smartmontools**.



BadBlocks

Утилита **badblocks** используется для поиска сбойных блоков на устройстве (в разделе диска, например, */dev/sda1*).

Синтаксис утилиты:

```
badblocks [-<параметры>] <устройство> [<конечный_блок>] [<начальный_блок>]
```

Параметры [**<конечный_блок>**], [**<начальный_блок>**] являются необязательными и указывают диапазон проверяемых блоков. Если они не указаны, тогда (по умолчанию) проверке подлежат все блоки, начиная с самого первого блока и заканчивая самым последним блоком, которые используются на устройстве.

Основные параметры:

- **-b** - размер блока (в байтах);

- **-c** - порция блоков (по умолчанию 64 блока);
- **-f** - принудительный запуск теста с помощью чтения/записи;
- **-i** - входной файл (читает список уже существующих сбойных блоков);
- **-o** - исходящий файл (сохраняет список сбойных блоков в указанный файл);
- **-p** - число раз поиска (по умолчанию только одна проверка);
- **-n** - принудительное использование режима чтения-записи (только в размонтированной системе);
- **-s** - отображение хода процесса проверки;
- **-v** - подробные сообщения о проверке;
- **-w** - использование режима реальной записи (приводит к уничтожению информации на диске).

Пример использования утилиты

1. Выберите раздел жесткого диска для проверки. Для просмотра всех подключенных устройств и проверки расположения диска можно воспользоваться командой:

```
fdisk -l <имя_раздела>

  или

lsblk
```

2. Запустите проверки с помощью утилиты:

```
badblocks -v /dev/sda1Checking blocks 0 to 1048575
Checking for bad blocks (read-only test): done

Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Из вывода консоли видно, что проверка происходит только для чтения. При попытке использовать параметр **-n** (проверка чтения/записи) возникает следующее предупреждение:

```
/dev/ro_redos/root is mounted; it's not safe to run badblocks!
```

Поэтому для проверки дисков на чтение/запись рекомендуется использовать **live-сессию**.

```
badblocks -v /dev/sda1

Checking for bad blocks in non-destructive read-write mode
From block 0 to 1048575
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

```
badblocks -v /dev/ro_redos/root

Checking for bad blocks in non-destructive read-write mode
From block 0 to 17821695
Testing with random pattern:
Pass completed, 0 bad blocks found. (0/0/0 errors)
```

Восстановление загрузчика GRUB2

Восстановление загрузчика для систем, использующих BIOS
Восстановление загрузчика для систем, использующих UEFI

Вы можете подробнее ознакомиться с восстановлением загрузчика **grub2** и восстановлением для систем, просмотрев наши обучающие видео:

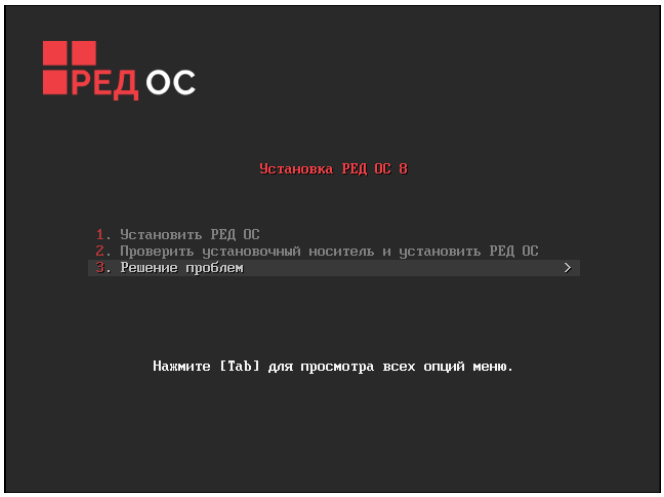
- на **RuTube** — Восстановление загрузчика GRUB2;
- в **Яндекс.Дзен** — Восстановление загрузчика GRUB2;
- в **VK Видео** — Восстановление загрузчика GRUB2.

На наших каналах вы также сможете найти много другой полезной информации.

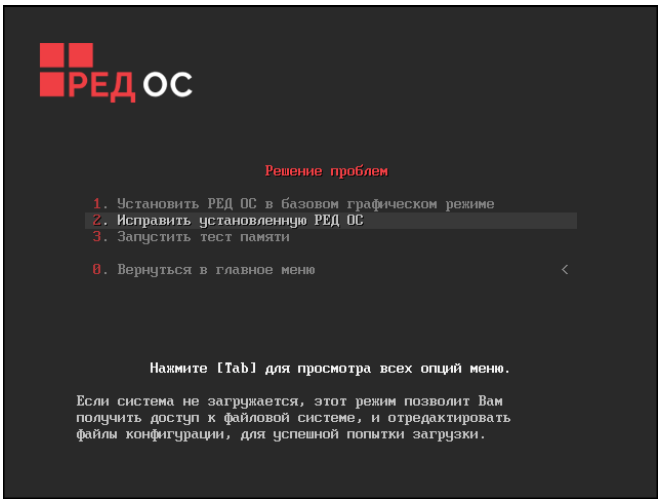
Для восстановления необходимо загрузиться с установочного образа вашей версии РЕД ОС, поставив ваш носитель первым в списке предпочтения загрузки.

Восстановление загрузчика для систем, использующих BIOS

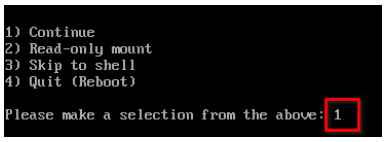
В появившемся меню следует выбрать пункт «**Решение проблем**».



Далее нужно выбрать пункт «**Исправить установленную RED OS**»:



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***:



Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Для определения диска, на котором установлена система, можно использовать следующую команду:

```
lsblk
```

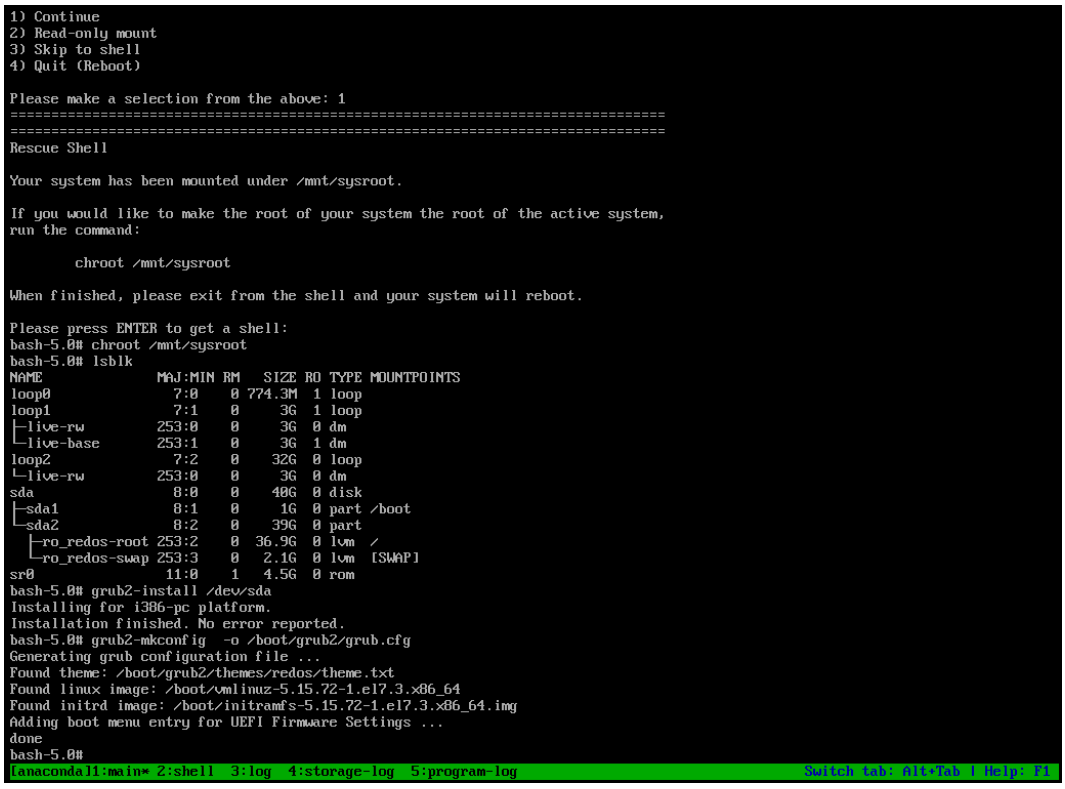
Далее выполните установку загрузчика командой (в конце указывается нужный диск):

```
grub2-install /dev/sda
```

Теперь создайте новый конфигурационный файл загрузчика с помощью команды:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Восстановление загрузчика для систем, использующих UEFI

В появившемся меню следует выбрать пункт «**Решение проблем**».



Далее нужно выбрать пункт «**Исправить установленную РЕД ОС**».



В появившемся списке выберите пункт «**Continue**», введя цифру **1** и нажав ***Enter***:

Примечание.

Для корректного отображения в терминале кириллических символов введите команду:

```
setfont cyr-sun16
```

Следующим шагом является изменение корневого каталога на **/mnt/sysroot** с помощью команды **chroot** (это сделает вашу систему

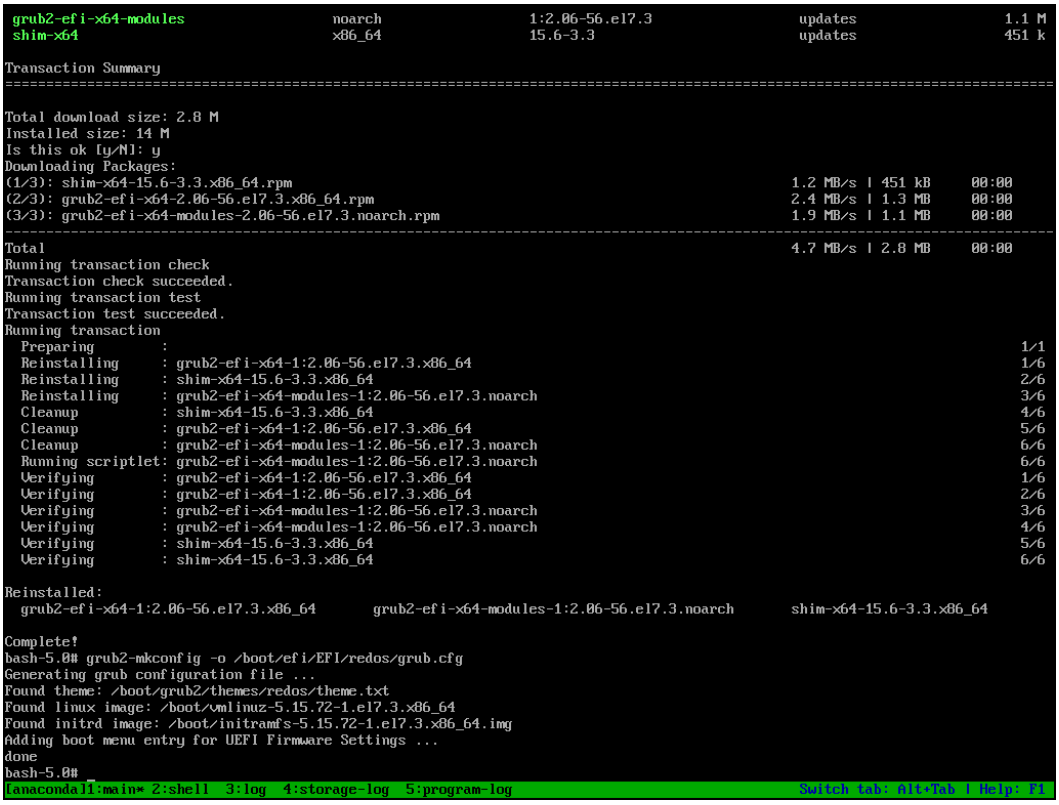
корневой средой):

```
chroot /mnt/sysroot
```

Затем потребуется обновить конфигурацию загрузчика с помощью команд:

```
dnf reinstall grub2-efi-x64  shim-x64 grub2-efi-x64-modules
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Вывод команд будет выглядеть следующим образом:



После выполнения команд выйдите из окружения **chroot**:

```
exit
```

Уберите загрузочный диск или флешку и выполните перезагрузку командой:

```
reboot
```

Проблемы с монтированием домашнего каталога /home

Рассмотрим проблему, из-за которой система не запускает графический менеджер **GDM** и вместо этого переходит в режим **emergency mode**. Суть данной проблемы заключается в том, что происходит сбой при монтировании домашнего каталога **/home**. При загрузке системы можно увидеть следующие предупреждения:

```
Warning: dev/mapper/ro-root does not exist
Warning: dev/ro/root does not exist
Warning: dev/ro/swap does not exist
```

В результате система входит в **emergency mode**. При входе будет предложено воспользоваться командной оболочкой для диагностики проблемы:

```
Entering emergency mode. Exit the shell to continue.
Type “journalctl“ to view system logs.
You might want to save “/run/initramfs/rdsosreport.txt“ to a USB stick or /boot after mounting then and attach it to a bug report.
```

Можно просмотреть журналы системы, введя команду:

```
journalctl
```

Запустите следующую команду, чтобы увидеть ошибки, связанные с домашним каталогом:

```
dmesg
```

В выводе должны присутствовать ошибки вида:

```
/dev/sda3, run e2fsck manually
```

где **/dev/sda3** - home-раздел.

Для того чтобы узнать, за каким разделом закреплен **/home**, необходимо проверить файл **/etc/fstab**. Найдите строчку, относящуюся к **/home**, чтобы определить, за каким устройством он закреплен.

```
cat /etc/fstab
```

Проверка файловой системы осуществляется через утилиту **fsck**. Запустите **fsck** для автоматической проверки (замените /dev/sda3 на ваш корректный раздел):

```
fsck -a /dev/sda3
```

где ключ **-a** отвечает за автоматическую коррекцию ошибок файловой системы.

Следуйте инструкциям. Если утилита сообщает о наличии ошибок, позвольте ей исправить их. Если некоторые ошибки не могут быть исправлены автоматически, утилита предложит вам выполнить их исправление вручную. После успешной проверки необходимо перезагрузить компьютер.

```
reboot
```

После этого графический менеджер GDM должен запуститься, и пользователь должен увидеть окно авторизации.

Пользователь забыл свой пароль и пароль root

Решением данной проблемы является сброс пароля **root**, согласно инструкции. Инструкцию предоставляет техническая поддержка, обратиться за инструкцией вы можете по ссылке.

Система не монтирует корневой раздел

Решение проблемы. Загрузка из более старого ядра
Неверное имя корневого раздела GRUB

Проблема монтирования корневого раздела выглядит следующим образом:

```
[ 1.719701] Hardware name: ECS IC780M-A2/IC780M-A2, BIOS 080015 11/03/2010
[ 1.719749] 0000000000000000 ffff88022c0b7df0 ffffffff8176cf38 ffffffff81a65048
[ 1.719951 0000000000008001 ffff88022c0b7e68 ffffffff81765306 ffffffff00000010
[ 1.720152] ffff88022c0b7e78 ffff88022c0b7e18 ffffffff81765e74 ffff88022c0b7e88
[ 1.720353] Call Trace:
[ 1.720402] [] dump_stack+0x64/0x82
[ 1.720449] [] panic+0xc8/0x206
[ 1.720494] [] ? printk+0x67/0x69
[ 1.720541] [] mount_block_root+0x225/0x2b0
[ 1.720587] [] mount_root+0x53/0x56
[ 1.720633] [] prepare_namespace+0x16c/0x1a4
[ 1.720679] [] kernel_init_freeable+0x1e1/0x1ee
[ 1.720725] [] ? initcall_blacklist+0xba/0xba
[ 1.720771] [] ? rest_init+0x80/0x80
[ 1.720817] [] kernel_init+0xe/0xf0
[ 1.720862] [] rest_from_fork+058/0x90
[ 1.720908] [] ? rest_init+0x80/0x80
[ 1.720974] Kernel Offset: 0x0 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 1.721043] ---[ end Kernel panic — not syncing: VFS: Unable to mount root fs on unknown-block (0,0)
_
```

Сообщение об ошибке «vfs unable to mount root fs on unknown block» может встречается во время загрузки Linux. Оно означает, что ядро не может примонтировать корневую файловую систему, и, следовательно, дальнейшая загрузка невозможна. Ошибка довольно серьёзная и, не исправив её, вы не сможете полноценно работать в своей операционной системе.

Все ситуации, в которых может появиться сообщение «error: vfs unable to mount root fs» можно разделить на два вида:

- Загрузка с жёсткого диска — вы загружаете свою основную операционную систему после внесения изменений в таблицу разделов, обновления или других действий, которые могли задеть диски;
- Вы загружаете LiveCD-систему с оптического диска или флешки.

Второй вариант сразу же отбросим. Здесь исправлять нечего. Ошибка означает, что либо образ был битый, либо он был неверно записан на диск. А вот первый случай интереснее, рассмотрим основные причины, которые могут его вызывать:

- Корневой раздел был переименован и теперь называется по-другому;
- Повреждена **initramfs**;
- Ядро не поддерживает файловую систему корневого раздела;
- Ошибка в конфигурации загрузчика, например, из-за недостаточного количества свободного места в папке **/boot**;
- Файловая система корневого раздела повреждена.

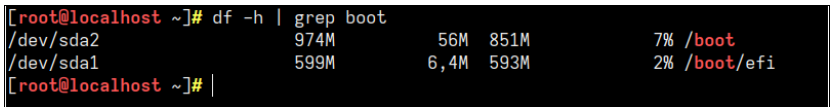
Рассмотрим возможные пути решения проблемы.

Решение проблемы. Загрузка из более старого ядра

После того, как система выдаст эту ошибку, случится **Kernel Panic** и компьютер перезагрузится. Вы снова окажетесь в меню загрузчика **GRUB**. Сначала следует попытаться загрузиться с помощью более старого ядра. Для этого выберите пункт «**Дополнительные параметры**» и выберите одно из более старых ядер.

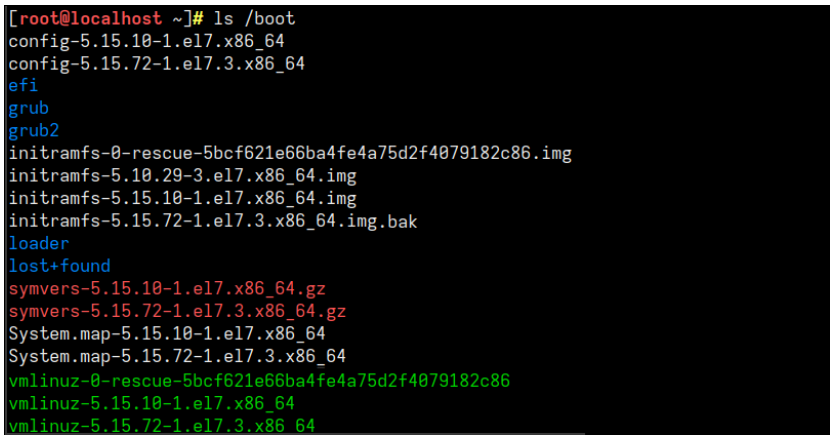
Если система в этом случае загрузится, то можно сделать вывод, что не работает только новое ядро. Если вы собирали его сами, то, возможно, вы не включили в него все необходимые для работы файловые системы. Если это ядро из репозиториев, и система загрузилась с более старым ядром, то можно предположить, что у вас повреждена **initramfs** для нового ядра. Это тоже могло произойти из-за недостатка памяти при обновлении системы. Чтобы всё исправить, вам достаточно освободить место в каталоге **/boot/** и создать новую **initramfs**. Проверьте и освободите место в папке **/boot**, если его там мало:

```
df -h | grep boot
```



На данном скриншоте занято только 7%, если будет 100% — надо освобождать. Для создания **initramfs** необходимо выполнить следующие действия:

```
cp -p /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak
dracut -f -v --regenerate-all
ls /boot
```



Обновите конфигурацию загрузчика **grub**:

- если используется **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- если используется **UEFI**:

```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

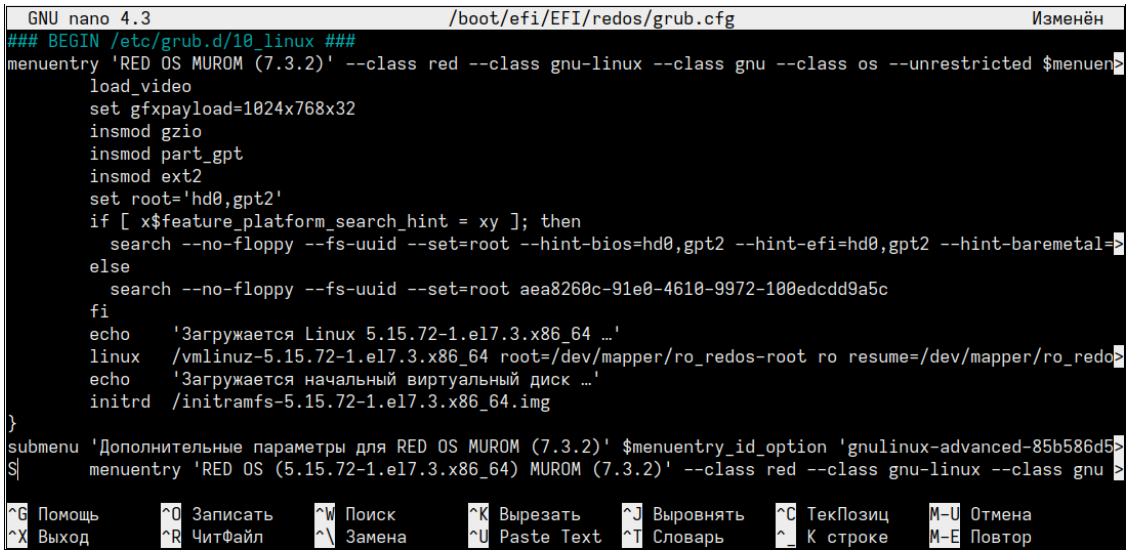
Если вы думаете, что проблема именно в свободном пространстве и **initramfs**, но загрузиться с помощью более старого ядра не можете, то попробуйте другой **LiveCD**-дистрибутив и попытайтесь всё исправить в *chroot*-окружении.

Неверное имя корневого раздела GRUB

Сейчас, в большинстве дистрибутивов, в конфигурационном файле **GRUB** имя корневого раздела передается ядру в формате **UUID**. И с этим обстоятельством есть одна проблема. Если вы каким-либо образом измените корневой раздел, например, измените его размер, то **UUID** изменится. И если вы выполните перезагрузку, не обновив конфигурацию **GRUB**, то система больше не загрузится, потому что ядро попросту не сможет найти нужного раздела.

Но попытаться решить проблему можно. Если вы точно знаете, на каком разделе у вас находится корень, то можно непосредственно в меню **GRUB** исправить конфигурацию. Для этого в меню выберете стрелками вверх и вниз нужный пункт, а затем нажмите кнопку **E**. Откроется редактор конфигурации. Вам нужно найти строчку, похожую на следующую:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro quiet splash
```



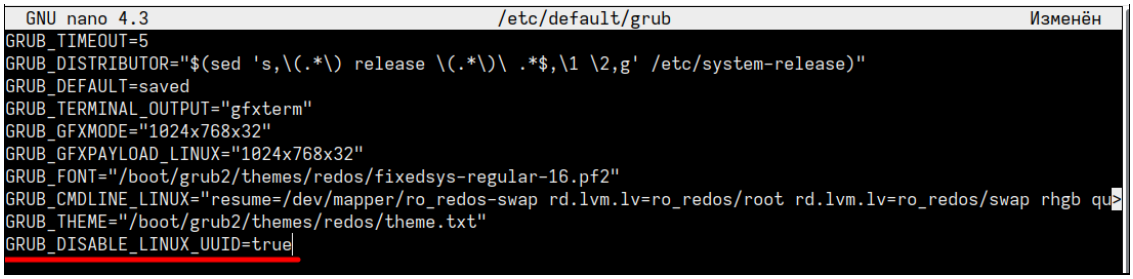
В ней надо заменить UUID=9d8d92de-74a6-4e64-8281-b8548c690e0c на обычное имя вашего корневого раздела, например, **/dev/sda2**. Для начала загрузки нажмите **F10**. Если система загрузится, значит проблема была именно в этом. В дальнейшем, можно просто обновить конфигурацию **GRUB**:

```
grub2-mkconfig
```

Или даже попросить **GRUB** больше не использовать **UUID** для обозначения корневого раздела:

```
nano /etc/default/grub
```

```
GRUB_DISABLE_LINUX_UUID=true
```



Далее необходимо снова обновить конфигурацию **GRUB**, используя команду **grub2-mkconfig**.

Если ошибка исчезла, но система всё ещё не загружается, обратите внимание, что **systemd** всё ещё использует файл **/etc/fstab** для монтирования файловых систем. И если корневая файловая система (и не корневая тоже) там указана неверно, система не загрузится. Для исправления этой проблемы можно использовать режим восстановления. Здесь тоже надо заменить **UUID** на обычную запись или же на правильный **UUID**. Такая проблема очень часто становится причиной медленной загрузки Linux.

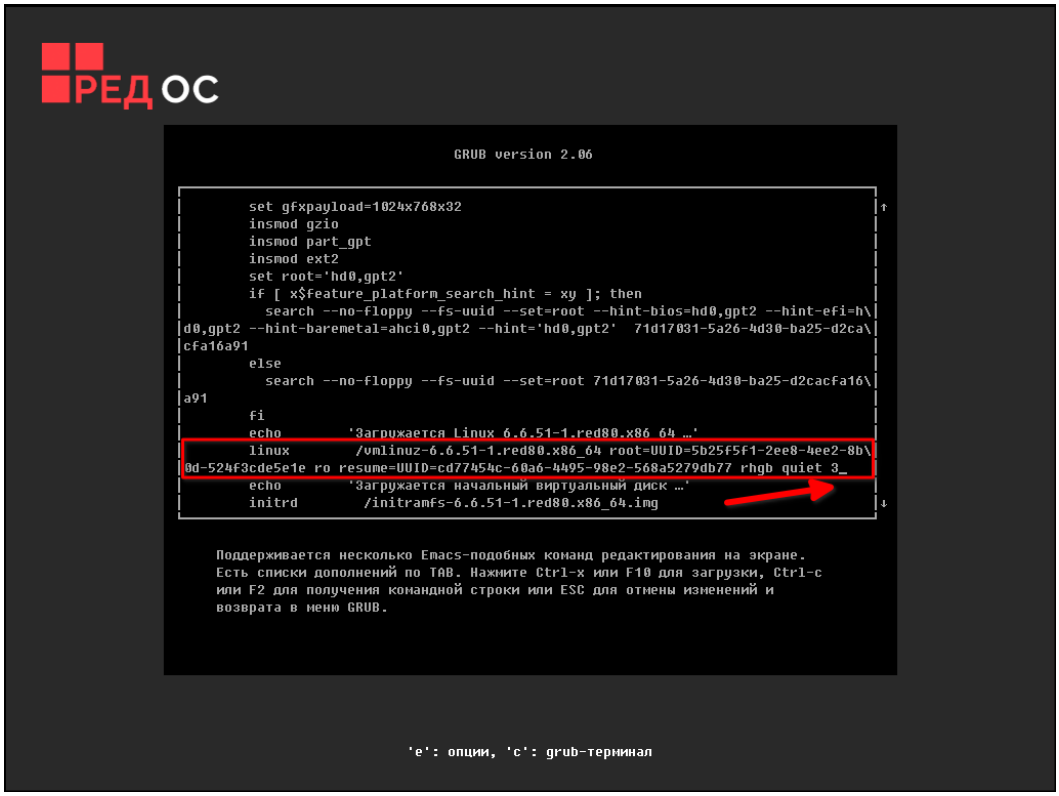
В этом же режиме можно проверить корневой раздел на ошибки, но для проверки диска лучше использовать **LiveCD**.

Если файловая система корневого раздела повреждена, её необходимо проверить, исправить согласно инструкции «Проверка файловой системы на наличие ошибок».

ОС запускается, но зависает на экране загрузки

Скорее всего данное поведение может быть связано с некорректным поведением X-сервера и графических драйверов. Для диагностики ситуации и сбора информации с ПК вы можете запустить ПК в консольном режиме. Для этого вам потребуется перезагрузить ПК и на этапе выбора ядра для загрузки нажать «**e**».

Далее необходимо найти примерно такую строку (см. скриншот) и добавить в конец «**3**».



После этого для продолжения загрузки необходимо нажать сочетание клавиш «**Ctrl+X**», ОС будет запущена в текстовом режиме.

Следующим этапом потребуется собрать отладочную информацию через утилиту loginfo для дальнейшего изучения проблемы.

Не загружается РЕД ОС из-за неправильного UUID раздела SWAP

Диагностика проблемы
Устранение проблемы

Проблема характеризуется тем, что во время загрузки операционной системы РЕД ОС на экране появляется ошибка вида:

```
A start job is running for /dev/disk/by-uuid/03a83c83-3827-4fa3-8352-bdfb4d99a15b (10min 6s / no limit)
```

Загрузить операционную систему в безопасном режиме также не удается.

Диагностика проблемы

Ошибка «A start job is running for /dev/disk/by-uuid/...» связанна с разделом диска, который используется в системе. Операционная система не может подключить раздел, который имеет номер **UUID**, указанный в ошибке.

Для того чтобы узнать, с каким именно разделом имеются проблемы при загрузке, требуется проверить параметры загрузчика системы **grub**.

Чтобы увидеть параметры загрузки grub, нужно на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /vmlinuz-6.6.51-1.red80.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> rhgb quiet
```

В строке видно, что в параметре resume=UUID= записан тот номер **UUID**, из-за которого возникает проблема с запуском системы.



Параметр resume отвечает за указание файла подкачки (раздел **SWAP**) для возобновления работы системы после перехода в спящий режим. Из этого можно сделать вывод, что проблема связана с разделом **SWAP**.

Необходимо узнать, совпадает ли номер **UUID** раздела **SWAP**, который указан в параметрах grub, с его актуальным на данный момент **UUID**-номером.

Номер **UUID** всех разделов диска можно узнать с помощью команды:

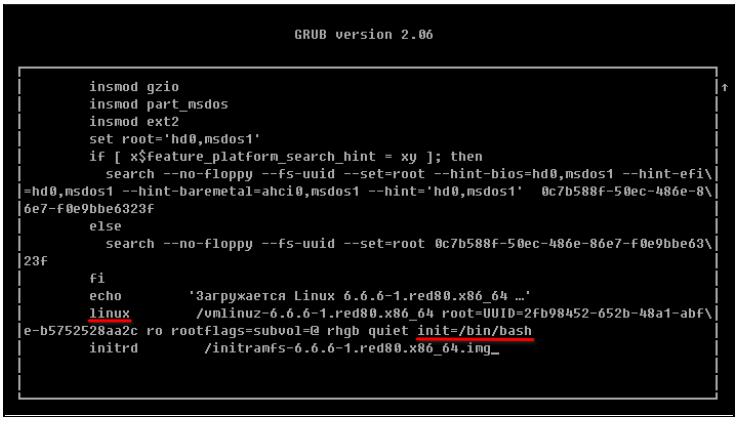
```
lsblk -o +uuid,name
```

Но т. к. операционная система РЕД ОС не может быть загружена ни в обычном, ни в безопасном режиме, то нужно выполнить загрузку системы сразу в командный интерпретатор **/bin/bash**.

Для этого необходимо открыть параметры загрузки **grub** — на этапе выбора ядра нажать клавишу «**e**». Далее найти строку примерно следующего вида:

```
linux /vmlinuz-6.6.51-1.red80.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> rhgb quiet
```

В строке необходимо удалить полностью параметр resume=UUID=<номер_uuid> и добавить параметр init=/bin/bash:



Для продолжения загрузки с введенными параметрами необходимо нажать сочетание клавиш **Ctrl+x** или **F10**.

Система сразу загрузится в командную оболочку **bash**.

Авторизуйтесь с правами пользователя **root** командой:

```
su root
```

Далее выполните монтирование корневого раздела командой:

```
mount -o remount,rw /
```

Нужно узнать **UUID**-номер, который имеет раздел **SWAP** в данный момент. Для этого необходимо выполнить команду:

```
lsblk -o +uuid,name
```

Вывод команды должен быть примерно следующим:

```
nvme0n1
│   259:0    0 476,9G  0 disk                                  nvme0n1
├─nvme0n1p1
│   259:1    0   600M  0 part /boot/efi   050C-89A6                    nvme0n1p1
├─nvme0n1p2
│   259:2    0     1G  0 part /boot      bef54c6a-a584-4147-9178-4218be5daedc   nvme0n1p2
└─nvme0n1p3
   259:3    0 475,4G  0 part           lA0CXd-ZuHw-7mqu-uhkH-igMU-c7wt-QBESxa nvme0n1p3
  ├─ro_redos-root
  │ 253:0    0    70G  0 lvm  /        832a877b-0293-4eec-a5f0-6a8d080aac03   ro_redos-srv-root
  ├─ro_redos-swap
  │ 253:1    0   7,5G  0 lvm  [SWAP]     fc46bf73-2759-4d70-a2d3-ab1f664ebf12   ro_redos-srv-swap
  └─ro_redos-home
    253:2    0 397,8G  0 lvm  /home      e5411e74-97de-4b84-aecd-e7f86e16ad5e   ro_redos-home
```

В данном примере раздел **SWAP** имеет **UUID - fc46bf73-2759-4d70-a2d3-ab1f664ebf12**.

Таким образом, можно сделать вывод, что номер **UUID** раздела **SWAP**, который записан в параметрах загрузки grub, и его актуальный **UUID** номер отличаются.

Устранение проблемы

Для устранения проблемы необходимо заменить неактуальный **UUID**-номер в параметрах загрузки **grub** на его актуальный номер, который был получен в результате диагностики.

Изменение параметра resume загрузчика GRUB

1. На этапе выбора ядра нажмите клавишу «**e**». Будут открыты параметры загрузки **grub**.

2. Замените старый номер **UUID**, прописанный в параметре `resume=UUID=`, на актуальный, который был получен в результате диагностики командой `lsblk -o +uuid,name`.

В строке:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=UUID=<номер_uuid> ro resume=UUID=<номер_uuid> quiet splash
```

3. Для продолжения загрузки с введенными параметрами нажмите сочетание клавиш **Ctrl+x** или **F10**.

Система должна загрузиться без ошибок.

Сохранение конфигурации загрузчика GRUB

При таком способе редактирования параметров загрузки **grub** введенные параметры не будут сохранены при следующей загрузке. Для сохранения внесенных изменений на постоянной основе измените параметр `resume=UUID=` в файле **/etc/default/grub**.

Для запуска терминала необходимо использовать сочетание клавиш **Ctrl+Alt+T** или запустить утилиту из **Главного меню** – **Системные** – **Терминал**.

Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

Откройте файл **/etc/default/gru**b с помощью текстового редактора командой:

```
nano /etc/default/grub
```

Найдите строку следующего вида:

```
GRUB_CMDLINE_LINUX="resume=UUID=..."
```

Номер **UUID** параметра `resume=UUID=` должен быть заменен на актуальный, с помощью которого удалось запустить систему.

Далее обновите файл загрузчика **grub** командой:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

После выполнения этих действий параметры загрузи **grub** будут сохранены для постоянного использования.

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

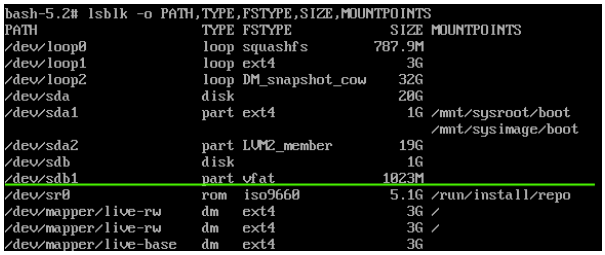
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

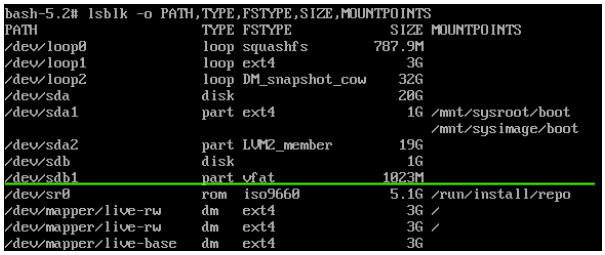
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

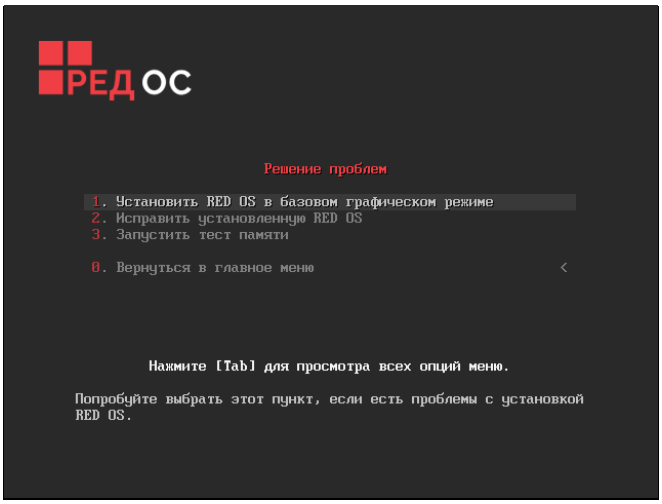
Проблемы при установке ОС

Установка ОС зависает на начальном этапе
ОС не запускается после установки с LiveUSB

Установка ОС зависает на начальном этапе

Бывают случаи, когда установка ОС зависает на этапе первичной загрузки до запуска окна *Anaconda*. В таких случаях рекомендуется произвести установку ОС в **базовом графическом режиме**, который также называется **nomodeset**.

Для загрузки ОС в режиме **nomodeset**, использующих **BIOS**, выберите пункт «**Решение проблем**» – «**Установить RED OS в базовом графическом режиме**».



Для загрузки ОС в режиме **nomodeset**, использующих **UEFI**, выберите пункт «**Решение проблем**» – «**Установить РЕД ОС в базовом графическом режиме**».



ОС не запускается после установки с LiveUSB

Иногда бывают случаи, что после установки ОС с *LiveUSB* не происходит загрузка установленной ОС. Для таких случаев необходимо загрузиться обратно в Live-сессию и скопировать файл **initramfs** с установочного носителя на диск с ОС. Для этого выполните следующий алгоритм действий:

1. Откройте терминал и перейдите в сеанс пользователя **root**:

```
su -
```

2. Проверьте названия разделов установленной ОС командой:

```
lsblk
```

В ответе команды будут указаны разделы ОС и загрузчика.

```
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   40G  0 disk
├─sda1   8:1    0    1M  0 part
├─sda2   8:2    0    1G  0 part /boot
├─sda3   8:3    0    2G  0 part [SWAP]
└─sda4   8:4    0 36,9G  0 part /
sr0     11:0    1  6,3G  0 rom  /run/initramfs/live
```

3. Примонтируйте разделы установленной ОС следующими командами:

```
mkdir /newboot
mount /dev/sda2 /newboot
```

4. Скопируйте образ **initrd.img** с **liveUsb** на раздел **/boot** диска с установленной системой:

```
cp /run/initramfs/live/images/pxeboot/initrd.img /newboot/initramfs-6.6.51-1.red80.x86_64.img
```

5. Назначьте необходимые права:

```
chmod 600 /newboot/initramfs-6.6.51-1.red80.x86_64.img
chown root. /newboot/initramfs-6.6.51-1.red80.x86_64.img
```

6. Отмонтируйте разделы установленной ОС:

```
umount /newboot
```

7. Перезагрузите ПК в установленную ОС:

```
reboot
```

Сбор диагностической информации при проблемах установки или загрузки РЕД ОС

Сбор логов при установке РЕД ОС
Сбор логов в случае невозможности запуска РЕД ОС

Вы можете подробнее ознакомиться с возможностью сбора диагностической информации в РЕД ОС, просмотрев наши обучающие видео:

- на **RuTube** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **Яндекс.Дзен** — Сбор журналов при проблемах установки или загрузки РЕД ОС;
- в **VK Видео** — Сбор журналов при проблемах установки или загрузки РЕД ОС.

На наших каналах вы также сможете найти много другой полезной информации.

Сбор логов при установке РЕД ОС

Если во время установки ОС возникает ошибка, и установка не продолжается, необходимо получить доступ к логам установки, которые находятся в каталоге **/tmp**, для дальнейшей передачи их в службу технической поддержки (https://support.red-soft.ru).

Перейдите в терминал с помощью нажатия сочетания клавиш «**CTRL+ALT+F2**».

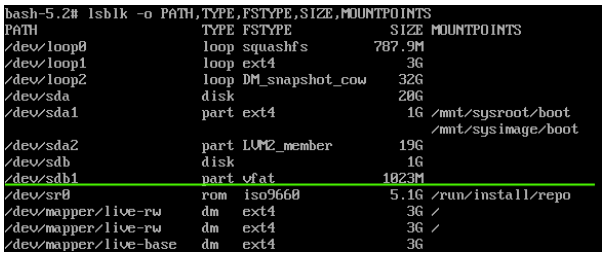
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /tmp/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/setup_logs.tgz /tmp/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **setup_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /tmp/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /tmp/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

Сбор логов в случае невозможности запуска РЕД ОС

Если ОС установлена, но не загружается, необходимо получить доступ к логам. Для данного варианта потребуется установочный носитель РЕД ОС, который подготавливается одним из способов, описанных в статье «Создание загрузочных носителей».

Загрузка среды восстановления

1. Подготовленный загрузочный носитель установите первым в очередности загрузки в настройках **BIOS**/**UEFI** и выполните перезагрузку.

2. В появившемся меню **Grub** произведите последовательный выбор пунктов: «**Решение проблем**» – «**Исправить установленную REDOS**». Начнется загрузка среды восстановления.

3. Дождитесь предложения выбора дальнейших действий (Please make a selection from the above:), нажмите **2** и **Enter**. Таким образом выбирается пункт «**Read-only mount**», соответствующий попытке монтирования разделов установленной РЕД ОС в каталог **/mnt/sysroot/** в режиме «**Только чтение**».

4. При успешном монтировании появится сообщение «Your system has been mounted under /mnt/sysroot/» и предложение перейти в оболочку «Please press ENTER to get a shell:». Перейдите в оболочку, нажав **Enter**.

Копирование логов

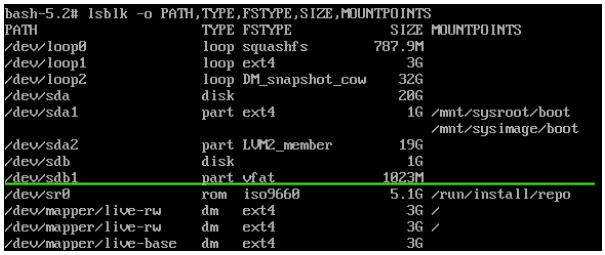
Способ 1. Копирование логов на USB-накопитель

1. Подключите USB-накопитель, на который будет скопирован архив с логами. Накопитель должен содержать отформатированный раздел, подготовленный для монтирования.

2. Определите путь подключенного накопителя с помощью команды:

```
lsblk -o PATH,TYPE,FSTYPE,SIZE,MOUNTPOINTS
```

Пример:



Данная информация поможет идентифицировать накопитель (по типу файловой системы, объему и отсутствию точки монтирования). Вам потребуется запомнить путь устройства (в примере: **/dev/sdb1**).

3. Создайте каталог и смонтируйте в него раздел накопителя (пример для **/dev/sdb1**):

```
mkdir /mnt/usb/
mount /dev/sdb1 /mnt/usb/
```

4. Рекомендуется оценить размер логов, которые необходимо скопировать, и объем свободного пространства на накопителе (поле *Avail*):

```
du -sh /mnt/sysroot/var/log/
df -h /dev/sdb1
```

5. Создайте архив логов с помощью команды (может занять продолжительное время):

```
tar -czf /mnt/usb/redos_logs.tgz /mnt/sysroot/var/log/
```

6. Перед извлечением накопителя отмонтируйте устройство командой:

```
umount /mnt/usb/
```

7. Подключите USB-накопитель к другой рабочей станции (или серверу) и отправьте архив **redos_logs.tgz** в службу технической поддержки.

Способ 2. Копирование логов посредством ssh

1. Оцените размер копируемых логов командой:

```
du -sh /mnt/sysroot/var/log/
```

2. Запустите команду копирования посредством клиента **SSH**:

```
scp -r /mnt/sysroot/var/log/ <имя_пользователя_SSH>@<адрес_назначения>:<каталог_назначения>
```

Опции и примеры использования утилиты **scp** приведены в статье «Работа с клиентом и сервером SSH» (раздел «Копирование файлов SCP»). Выполнение команды может занять продолжительное время.

3. Заархивируйте логи из каталога назначения на удаленном сервере любым удобным способом и направьте архив в службу технической поддержки.

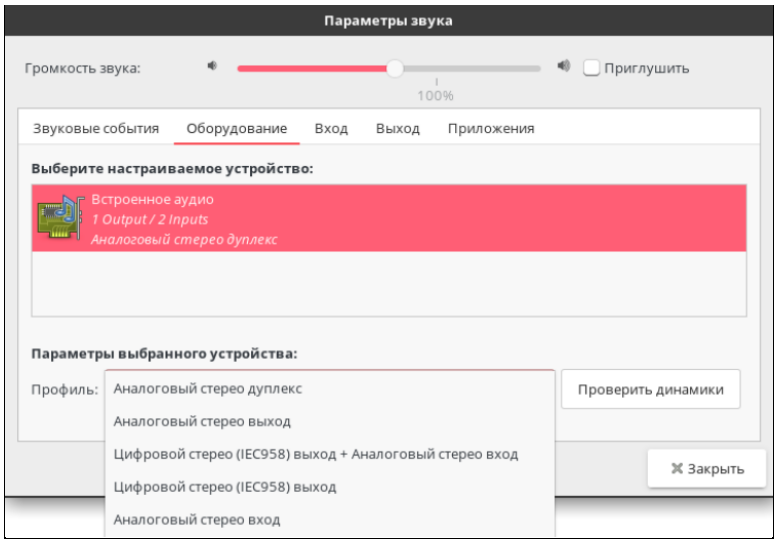
Решение проблем со звуком

Выбор оборудования
Отсутствует оборудование в списке доступных
Выбор оборудования через alsamixer
Проверка поддержки устройства ядром
Отсутствует звук у доменного пользователя

При возникновении проблем, связанных со звуком, существует несколько вариантов их решения.

Выбор оборудования

Бывают ситуации, когда необходимо вручную выбрать, какое именно устройство должно использоваться в ОС для ввода и вывода аудио-информации. Для этого выберите устройство в списке оборудования и установите для него необходимые параметры.

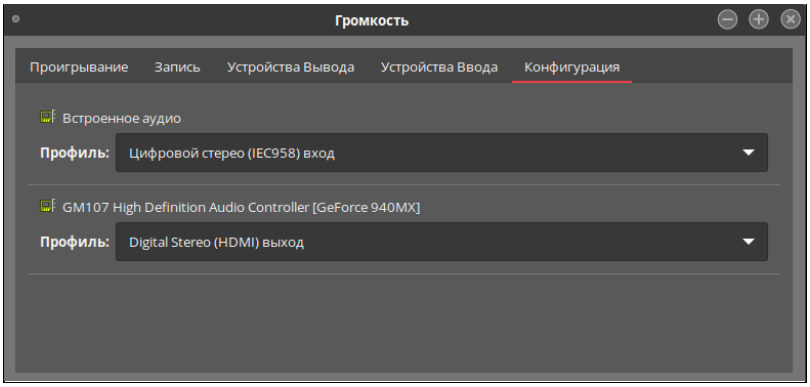


Отсутствует оборудование в списке доступных

Для решения данной проблемы на некоторых моделях ПК может подойти установка дополнительного пакета (потребуются права администратора):

```
dnf install alsa-sof-force
```

После установки необходимо перезагрузить ПК и проверить наличие аудиовыходов в параметрах звука.



Также не стоит забывать о системных обновлениях, соответственно, необходимо проверить работу оборудования на актуальных пакетах ОС. Для этого выполните следующие команды (потребуются права администратора):

```
dnf makecache
dnf update
dracut -f -v --regenerate-all
```

Затем для корректной загрузки необходимо обновить конфигурацию **GRUB**:

- для систем, использующих **BIOS**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- для систем, использующих **UEFI**:

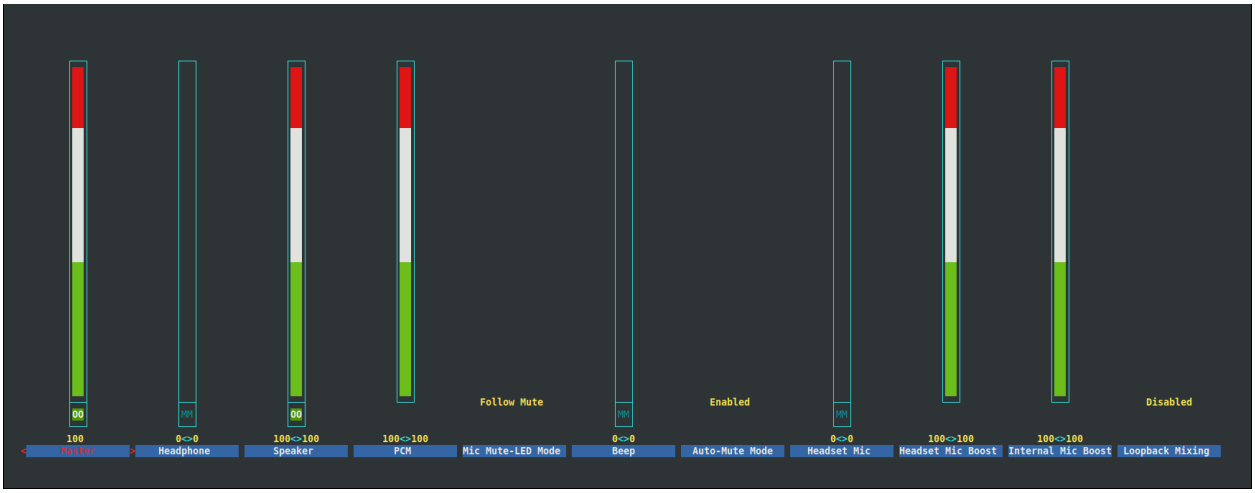
```
grub2-mkconfig -o /boot/efi/EFI/redos/grub.cfg
```

Для применения настроек потребуется перезагрузить ПК:

```
reboot
```

Выбор оборудования через alsamixer

В решении проблем со звуком также может помочь вариант с выбором звуковой карты из консоли через утилиту **alsamixer**.



С помощью клавиши **F6** можно выбрать необходимую звуковую карту.

Проверка поддержки устройства ядром

С выходом нового оборудования при возникновении проблем стоит обратить внимание на поддержку такого оборудования ядром. Проверить поддержку можно по нашей инструкции «Поддержка звука».

Отсутствует звук у доменного пользователя

Если звук отсутствует у доменного пользователя, в первую очередь необходимо проверить наличие файла **/var/lib/AccountsService/users/<доменный_пользователь>**. Если файл отсутствует, его необходимо создать по примеру файла локального пользователя.

Также попробуйте добавить пользователя в группу *audio*:

```
usermod -aG audio <доменный_пользователь>@<домен>
```

Если предложенные рекомендации не помогли с решением проблемы, необходимо собрать диагностическую информацию с помощью утилиты loginfo для дальнейшего ее изучения.

Realtek RTL8821CE

Для решения возможной проблемы с wi-fi адаптерами на базе микроконтроллера **Realtek RTL8821CE**, убедитесь в том, что у вас именно такой адаптер. Для этого выполните команду:

```
lspci | grep Network02:00.0 Network controller: Realtek Semiconductor Co., Ltd. RTL8821CE 802.11ac PCIe Wireless Network Adapter
```

Есть вероятность, что система использует драйверы **rtw88_***. Проверка производится командой:

```
lsmod | grep rtw
```

Если вывод команды показал, что используются именно эти драйверы, то нужно внести их в черный список (подробнее см. по ссылке) модулей ядра. Для этого необходимо создать конфигурационный файл:

```
nano /etc/modprobe.d/wifi.conf
```

и запретить загрузку «ненужных» модулей ядра (драйверов):

```
blacklist rtw88_8821ce /bin/true
blacklist rtw88_8821c /bin/true
blacklist rtw88_pci /bin/true
blacklist rtw88_core /bin/true
modprobe rtl8821ce
```

Обратите внимание на последнюю строку, в ней предопределяется модуль для загрузки, входящий в пакет, который еще не установлен. Установите пакет с работоспособным модулем (драйвером):

- для РЕД ОС версии 7.3 и старше выполните команду:

```
dnf install rtl8821ce_$(uname -r)
```

После этого нужно произвести перезагрузку системы командой:

```
reboot
```

После выполнения вышеуказанных действий проблема с wi-fi адаптерами на базе микроконтроллера **Realtek RTL8821CE** должна исчезнуть.

Intel i915

Ошибка в журнале сообщений ядра
Мерцание экрана
Отключение аппаратного ускорения
Включение поддержки графики
Зависания компьютера

Для решения возможной проблемы, связанной со встроенной графикой **Intel** последних поколений, требуется указать ядру дополнительные параметры, чтобы драйвер **i915** был применен принудительно к определенным версиям графического контроллера.

Ниже представлены примеры принудительного применения параметров для ядра. Применить параметры можно на этапе загрузки ОС для разового использования, т.е. на этапе выбора ядра необходимо нажать клавишу «**e**» и в строку примерно следующего вида:

```
linux /boot/vmlinuz-5.15.72-1.el7.3.x86_64 root=/dev/mapper/ro_redos-root ro quiet splash
```

и вписать параметры в **GRUB**:

- для **UHD Graphics 730**:

```
i915.force_probe=4692 i915.modeset=1
```

- для **UHD Graphics 750**:

```
i915.force_probe=4c8b i915.modeset=1
```

- для **UHD Graphics 770**:

```
i915.force_probe=4680 i915.modeset=1
```

В итоге должна получиться примерно следующая строка загрузки:



Стоит обратить внимание, что некоторые ID железа могут отличаться и уточнить их следует, как показано в инструкции «Поддержка железа».

Если указанные параметры помогли в решении проблемы, их можно добавить в ядро для постоянного использования. Для этого необходимо прописать параметры в файл **/etc/default/grub** в строку, начинающуюся со слов:

```
GRUB_CMDLINE_LINUX=
```

В конец строки дописываются **ваши** параметры.

Далее обновите файлы загрузчика:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Примеры использования

При возникновении таких проблем, как:

- мерцание экрана монитора,
- произвольные выключения монитора на небольшие промежутки времени,
- произвольные выключения монитора на большие промежутки времени (при этом во всех случаях система продолжает работать, экран монитора через какое-то время восстанавливается в работе),

необходимо в конфигурационный файл **grub** внести соответствующие изменения. Далее будут рассмотрены основные возникающие проблемы и способы их решения.

Ошибка в журнале сообщений ядра

При отображении в выводе журнала сообщений ядра ОС ошибки примерно следующего вида:

```
dmesg | grep i915

i915 0000:00:02.0: [drm] *ERROR* CPU pipe A FIFO underrun
```

необходимо открыть конфигурационный файл **grub**:

```
nano /etc/default/grub
```

и добавить в строку **GRUB_CMDLINE_LINUX** следующие значения:

```
...
 GRUB_CMDLINE_LINUX="resume=/dev/mapper/ro_redos-swap rd.lvm.lv=ro_redos/root rd.lvm.lv=ro_redos/swap rhgb quiet
i915.enable_psr=0 intel_idle.max_cstate=2"
 ...
```

Мерцание экрана

Для исправления проблем с мерцанием экрана в файл **/etc/default/grub** в строку, начинающуюся со слов:

```
GRUB_CMDLINE_LINUX="..."
```

в конце допишите:

```
i915.enable_psr=0 intel_idle.max_cstate=4 i915.enable_dc=0 i915.enable_fbc=0
```

Далее выставите иной режим энергосбережения:

```
tuned-adm profile latency-performance
```

Обновите файлы загрузчика:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Перезагрузите систему и проверьте работу.

Отключение аппаратного ускорения

Для отключения аппаратного ускорения используются следующие параметры (в зависимости от производителя):

Вендор	Параметр
Intel	`i915.modeset=0` или `nomodeset`
AMD	`radeon.modeset=0` или `amdgpu.dc=0` (для новых ядер)
Nvidia	`nomodeset` (или `nouveau.modeset=0`)

Пример отключения аппаратного ускорения для **Intel**:

```
grubby --update-kernel ALL --args="nomodeset"
```

Для удаления параметра выполните:

```
grubby --update-kernel ALL --remove-args nomodeset
```

Дополнительные опции:

- `text` — загрузка в текстовом режиме;
- `xforcevesa` — загрузка видеодрайвера **vesa**.

Также настройку можно выполнить через редактирование файла **/etc/default/grub**, добавив соответствующий параметр в конец строки **GRUB_CMDLINE_LINUX=**, после этого потребуется обновить конфигурацию **grub**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Включение поддержки графики

Через ID

Для загрузки графики и возможности выбора любого поддерживаемого разрешения используется опция загрузчика — `i915.force_probe=<ID_видеокарты>`.

Например:

```
i915.force_probe=9a49
 i915.force_probe=4c8a
 i915.force_probe=4e71
 i915.force_probe=9a78
```

Стоит обратить внимание, что некоторые ID железа могут отличаться и уточнить их следует, как показано в инструкции «Поддержка железа».

Также для включения поддержки графики можно использовать конфигурационный файл **/etc/modprobe.d/i915.conf**.

Параметры прописываются следующим образом:

```
options i915 force_probe=4c8a
```

С помощью активации альфа-драйвера

Запустите ОС, перейдите в консольный режим с помощью сочетания клавиш *Ctrl+Alt+F2*.

Выполните команду:

```
grubby --update-kernel ALL --args i915.alpha_support=1
```

Включение через опцию modeset

Поддержку графики также можно активировать с помощью опции **modeset**. Для этого выполните команду:

```
grubby --update-kernel ALL --args modeset=1
```

Зависания компьютера

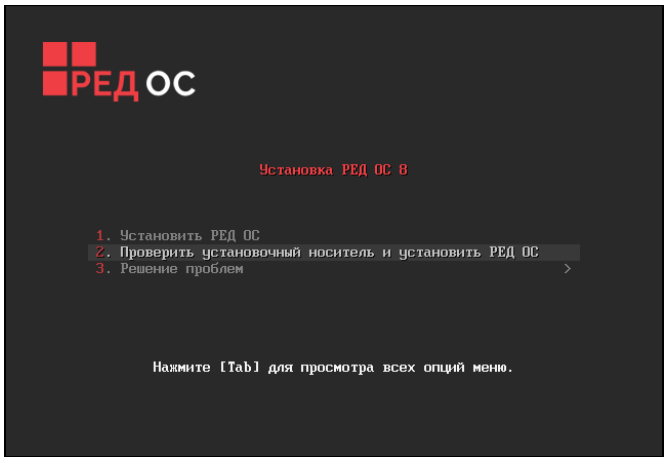
Если происходят периодические зависания компьютера без видимых причин, можно попробовать добавить параметр ядру `intel_idle.max_cstate=1` командой:

```
grubby --update-kernel ALL --args intel_idle.max_cstate=1
```

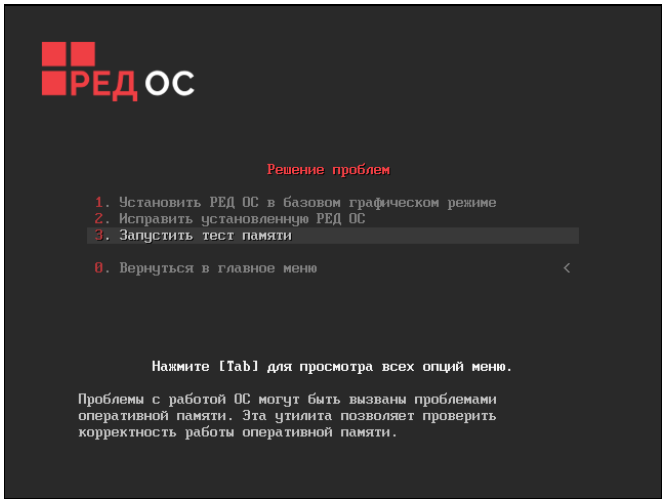
Тестирование оперативной памяти

Чтобы протестировать оперативную память на ошибки нужно запустить ОС с загрузочной флешки или диска.

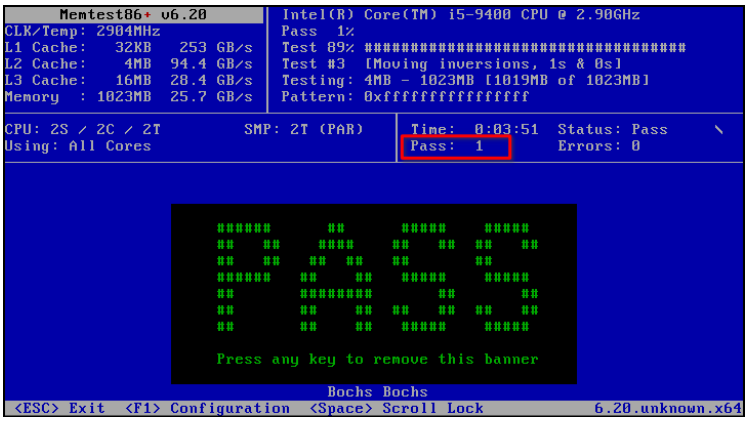
В открывшемся меню необходимо выбрать третий пункт «**Решение проблем**».



Затем выбрать третий пункт «**Запустить тест памяти**».



Запустится тест памяти. Данный процесс будет выполняться бесконечно, пока вы не остановите его. Вам нужно дождаться окончания хотя бы одного цикла проверки (значение **Pass** должно быть **>= 1**). В случае обнаружения ошибки она отобразится в списке.



Поддержка оборудования в ядре ОС

Поддержка железа
Поддержка звука
Поддержка сети

Некоторые модели поддерживаемого оборудования указаны в разделе «Оборудование, совместимое с РЕД ОС».

Вопрос поддержки оборудования ядром и драйверами актуален всегда. Для того чтобы понять, как именно осуществляется проверка поддержки, рассмотрим основные инструменты и ссылки.

Для получения краткой сводки о комплектующих вашего ПК выполните команду:

```
loginfo.sh --hw-id
```

Предварительно **loginfo** должен быть обновлен до актуальной версии:

```
dnf update loginfo
```

Поддержка железа

Одним из популярных сайтов, в котором собраны ID устройств, является https://linux-hardware.org.

Однако, чтобы определить, какие **Vendor ID** (**VID**) и **Device ID** (**DID**) требуется вводить для понимания поддержки, воспользуйтесь утилитой **inxi**.

```
inxi -F -v 8
```

пример ID для **USB Bluetooth** / **USB Wi-Fi,** которые потребуются для эксперимента:

```
...

Device-2: 1-4:2 info: Realtek Bluetooth Radio type: Bluetooth driver: rtk_btusb interfaces: 2 rev: 1.1
speed: 12 Mb/s chip ID: 0bda:8771 serial: 00E04C239987
Device-3: 1-6:3 info: Realtek RTL8188EUS 802.11n Wireless Network Adapter type: Network driver: 8188eu
interfaces: 1 rev: 2.0 speed: 480 Mb/s chip ID: 0bda:8179 serial: 00E04C0001

...
```

В выводе отображаются 2 интересующих нас ID:

- Bluetooth - **0bda:8771**;
- Wi-Fi - **0bda:8179**.

Также рассмотрим альтернативу *linux-hardware.org* — **https://cateee.net**

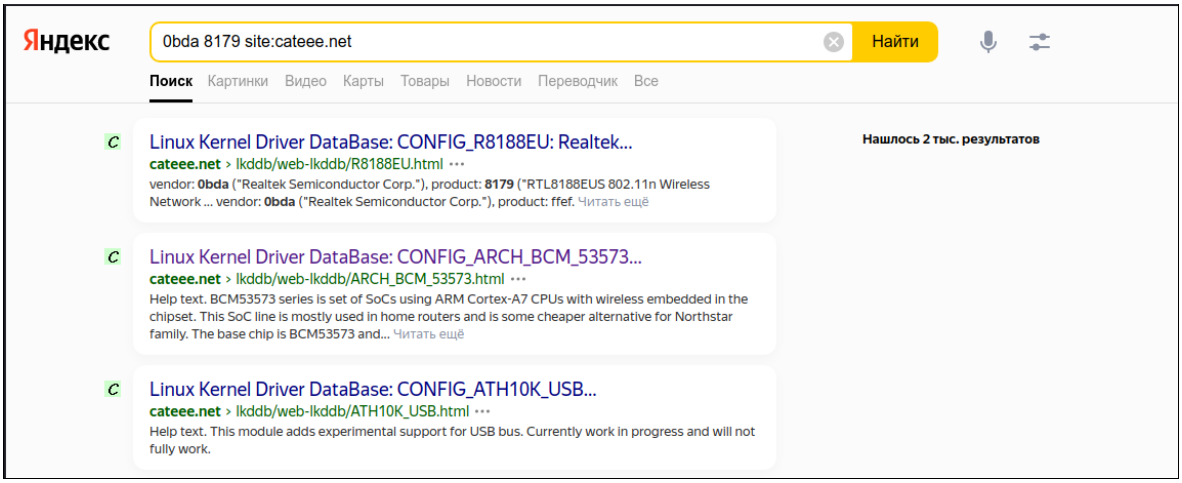
Данный сайт осуществляет поиск аналогично по ID. Для этого в поисковой строке требуется задать запрос вида:

<VID> <DID> site:cateee.net

или по одному из нужных ID.

Попробуем найти **0bda 8179** (**Wi-Fi**).

Имеется ряд результатов, в которых описывается, какой именно драйвер требует устройство:



Стоит упомянуть еще пару полезных ссылок для определения поддержки железа ядром:

- https://wireless.wiki.kernel.org/en/users/drivers
- https://h-node.org/hardware/catalogue/en

Также обращаем внимание на пункт **Driver** в выводе **inxi** - если он имеет значение отличное от **n/a**, значит у вас имеется поддержка устройства драйвером. Что это означает? Это значит, что вы можете найти данное устройство в заявленных драйвером через **modinfo**.

Bluetooth:

```
modinfo rtk_btusb | grep -i 0BDA

alias: usb:v0BDAp*d*dc*dsc*dp*icE0isc01ip01in*
```

В выводе показано, что есть метка **alias (алиас)**, являющаяся маской, по которой драйвер применяется к тому или иному устройству.

Аналогичную картину можно наблюдать для **Wi-Fi** адаптера:

```
modinfo 8188eu | grep -i 0BDA

alias: usb:v0BDAp8179d*dc*dsc*dp*ic*isc*ip*in*
```

Теперь рассмотрим проверку ядра на наличие интересующего драйвера.

Сначала проверим, установлен ли уже драйвер:

```
find /lib/modules/$(uname -r) -name *.ko | grep -i 8188eu

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/net/wireless/8188eu.ko
/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/staging/r8188eu/r8188eu.ko

find /lib/modules/$(uname -r) -name *.ko | grep -i rtk_btusb

/lib/modules/5.15.10-3.el7.x86_64/kernel/drivers/bluetooth/rtk_btusb.ko
```

Как видно из вывода консоли, для ядра **5.15.10-3** данные драйвера имеются.

Существует также способ просмотра параметров ядра, с которыми оно было собрано. Для проверки того, какие были выбраны опции для драйвера, выполните команду:

```
cat /boot/config-$(uname -r) | grep -i 8188

CONFIG_RTL8188EE=m
CONFIG_R8188EU=m
```

А вот для bluetooth-драйвера вывод может выглядеть сомнительно:

```
cat /boot/config-$(uname -r) | grep -i BTUSB
```

```
CONFIG_BT_HCIBTUSB=m
CONFIG_BT_HCIBTUSB_AUTOSUSPEND=y
CONFIG_BT_HCIBTUSB_BCM=y
# CONFIG_BT_HCIBTUSB_MTK is not se t
CONFIG_BT_HCIBTUSB_RTL=y
```

Для того чтобы развеять сомнения, имеется ли драйвер - проверим его наличие следующим образом:

```
dnf provides *rtk_btusb.ko
```

Из полученного списка необходимо выбрать драйвер под свое ядро:

```
rtl8761b_5.15.10-3.el7.x86_64-1.0-8.el7.3.x86_64 : Kernel module for RTL8761B
Репозиторий        : kernels
Совпадения с:
Другое       : *rtk_btusb.ko
```

В случае, если драйвер отсутствует и в ядре, и в репозитории, существует вариант поиска необходимого драйвера на **github**.

Для этого необходимо в поиске по репозиториям **github** знать название нужного драйвера и попробовать найти интересующий. Так, к примеру, драйвер **8188eu** имеет множество разветвлений, которые охватывают широкий спектр устройств - примеры двух популярных вариаций драйвера:

- https://github.com/drygdryg/rtl8188eus;
- https://github.com/lwfinger/rtl8188eu.

Поддержка звука

Для проверки поддержки звука необходимо выполнить команду:

```
inxi -a -A

Audio:
 Device-1: NVIDIA vendor: ASUSTeK driver: snd_hda_intel v: kernel
 bus ID: 01:00.1 chip ID: 10de:10fa
 Device-2: AMD Family 17h HD Audio vendor: ASUSTeK driver: snd_hda_intel
 v: kernel bus ID: 05:00.6 chip ID: 1022:15e3
 Sound Server: ALSA v: k5.15.35-1.el7.3.x86_64

modinfo snd_hda_intel | grep -i 10de

alias:          pci:v0000 10DEd*sv*sd*bc04sc03i00*
```

Также можно попробовать поиск через легкое регулярное выражение, когда «**:**» заменяется на «**.***», что означает любые символы.

```
modinfo snd_hda_intel | grep -i 1022.*15e3

alias:          pci:v0000 1022d000015E3sv*sd*bc*sc*i*
```

Поддержка сети

Для проверки поддержки сети выполните команду:

```
inxi -a -N

Network:
 Device-1: Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet
 vendor: ASUSTeK driver: r8169 v: kernel port: e000 bus ID: 02:00.0
 chip ID: 10ec:8168
 Device-2: Realtek RTL8821CE 802.11ac PCIe Wireless Network Adapter
 vendor: AzureWave driver: rtw_8821ce v: N/A modules: rtw88_8821ce
 port: d000 bus ID: 04:00.0 chip ID: 10ec:c821

modinfo r8169 | grep -iE 10ec.*8168
```

```
alias:          pci:v000010ECd00008168sv*sd*bc*sc*i*
```

Бывают случаи, когда поле **driver** не определено (driver = N/A), но присутствует поле **module**, тогда стоит производить проверку по данному полю:

```
modinfo rtw88_8821ce | grep -iE 10ec.*c821

alias:          pci:v000010ECd0000C821sv*sd*bc*sc*i*
```

Настройка systemd-coredump для автоматического сбора дампов

Настройка сбора дампов
Изменение места сохранения дампов
Проверка работоспособности создания дампа
Чтение дампов ядра
Настройка сбора дампов в СУБД Ред База Данных

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция
- **Версия ПО**: systemd-246.10-16

Дамп памяти (*core dump*) — содержимое рабочей памяти одного процесса, ядра или всей операционной системы. Также может включать дополнительную информацию о состоянии программы или системы, например, значения регистров процессора и содержимое стека. Многие операционные системы позволяют сохранять дамп памяти для отладки программы. Как правило, дамп памяти процесса сохраняется автоматически, когда процесс завершается из-за критической ошибки (например, из-за ошибки сегментации). Дамп также можно сохранить вручную через отладчик или любую другую специальную программу.

Настройка сбора дампов

В РЕД ОС 7.3 для автоматического сбора дампов используется обработчик дампов **systemd-coredump** — он собирает информацию о процессе при аварийном завершении программы. Для проверки сбора дампов выполните команду:

```
cat /proc/sys/kernel/core_pattern
|/usr/lib/systemd/systemd-coredump %P %u %g %s %t %c %h
```

Размер дампов определяется в файле конфигурации **/etc/systemd/coredump.conf**. Для изменения размера дампов в секции [Coredump] необходимо раскомментировать следующие параметры:

```
Compress=yes
ProcessSizeMax=<максимальный_размер_дампов>
ExternalSizeMax=<максимальный_размер_сжатого_дампа>
```

Далее будут подробнее рассмотрены параметры конфигурационного файла:

- Storage — определяет место хранения дампа процесса, может принимать одно из значений: *none*, *external*, *journal*.
  - *none* — дампы ядра записываются (включая обратную трассировку, если возможно), но не сохраняются;
  - *external* — значение по умолчанию, дампы сохраняются в каталоге **/var/lib/systemd/coredump/**;
  - *journal* — дампы будут храниться в журнале и перезаписываться в соответствии со стандартными принципами ротации журналов.
- Compress — используется для сжатия дампов ядра. Принимает логический аргумент — *yes* или *no*:
  - *yes* — дампы сжимаются при сохранении (значение по умолчанию);
  - *no* — дампы сохраняются без сжатия.
- ProcessSizeMax — определяет максимальный размер дампа процесса, который может быть сохранен. Если размер дампа превышает значение этого параметра, то дамп сохранен не будет. Это позволяет ограничить размер дампов и избежать переполнения дискового пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *до 1ГБ* — в 32-битных системах, *32ГБ* — в 64-битных системах. Параметры Storage=none и ProcessSizeMax=0 отключает всю обработку дампа памяти, за исключением записи журнала.
- ExternalSizeMax и JournalSizeMax — определяет максимальный (сжатый или несжатый) размер дампа процесса, который будет сохранен на диске (по умолчанию *1 ГБ* — в 32-разрядных системах, *2 ГБ* — в 64-разрядных системах), или в журнале системы (по умолчанию 10M).
- MaxUse — определяет максимальный объем общего дискового пространства, который может быть использован для хранения дампов процессов. Если общий размер всех дампов превышает значение этого параметра, старые дампы будут удаляться для освобождения места для новых. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию ограничение равно *10% от общего размера диска*.
- KeepFree — определяет минимальный объем свободного дискового пространства, который должен оставаться на диске при хранении дампов. Если свободного места на диске становится меньше указанного значения, новые дампы не будут создаваться

до тех пор, пока не будет предоставлено достаточного объема свободного пространства. Значение параметра указывается в байтах, также возможно использование суффиксов (B, K, M, G, T, P и E). По умолчанию *15% от общего размера диска* должно оставаться свободным. Старые дампы ядра также удаляются в зависимости от времени с помощью **systemd-tmpfiles**.

Изменение места сохранения дампов

Дампы по умолчанию будут создаваться в каталоге **/var/lib/systemd/coredump**. Служба **systemd-coredump** не имеет параметра конфигурации для изменения каталога, в котором будут храниться дампы.

Для смены каталога создания дампов необходимо использовать **bind-mount**:

1. В файле **/etc/fstab** пропишите монтирование нужной директории для сохранения дампов следующим образом:

```
/каталог/для/дампов /var/lib/systemd/coredump none defaults,bind 0 0
```

2. Примонтируйте каталог:

```
mount /var/lib/systemd/coredump
```

3. Перезапустите службу **systemd** для применения изменений:

```
systemctl daemon-reload
```

Проверка работоспособности создания дампа

Для проверки создания дампа необходимо выполнить в терминале:

```
sleep 3600 &
kill -11 %1
```

Проверьте создание дампа с помощью утилиты **coredumpctl**:

```
coredumpctl
```

Рассмотрим дополнительные опции **coredumpctl**:

- **list** — список доступных дампов ядра;
- **info <PID>** — вывод подробной информации об указанном дампе ядра;
- **gdb <файл>** — запускает отладчик **gdb** (GNU Debugger) для анализа дампа ядра;
- **dump <PID>** — создает дамп ядра с указанным идентификатором (PID). Дамп ядра будет передан на стандартный вывод, если не указан выходной файл с помощью **--output=**;
- **debug <PID>** — запуск процесса с указанным PID в режиме отладки. По умолчанию используется **gdb**. Отладчик может быть изменен с помощью параметра **--debugger=** или переменной среды **$SYSTEM_DEBUGGER**. Для передачи отладчику дополнительных аргументов командной строки используется параметр **--debugger-arguments=**.

Чтение дампов ядра

Сводную информацию о дампе ядра, соответствующем определенному процессу, в котором произошел сбой, можно получить, выполнив команду:

```
coredumpctl info _PID=<PID_процесса,по_которому_создан_дамп>
```

```
[user@localhost ~]$ coredumpctl info _PID=2772
           PID: 2759 (bash)
           UID: 1000 (user)
           GID: 1000 (user)
        Signal: 6 (ABRT)
     Timestamp: Fri 2023-03-31 11:46:40 MSK (20min ago)
  Command Line: bash 1212.sh
    Executable: /usr/bin/bash
 Control Group: /user.slice/user-1000.slice/session-2.scope
          Unit: session-2.scope
         Slice: user-1000.slice
       Session: 2
     Owner UID: 1000 (user)
       Boot ID: df6eee73274847bf9b977b2b77d47391
    Machine ID: 1e8ddb949cf549d8a2785068c77b85cd
      Hostname: localhost.localdomain
       Storage: /var/lib/systemd/coredump/core.bash.1000.df6eee73274847bf9b977b2b77d47391.2759.16802
       Message: Process 2759 (bash) of user 1000 dumped core.

                Stack trace of thread 2759:
                #0  0x00007fe88a6e715b __waitpid (libc.so.6 + 0xcc15b)
                #1  0x0000000000451619 waitchld.isra.12 (bash + 0x51619)
                #2  0x000000000052dfa wait_for (bash + 0x52dfa)
                #3  0x000000000043fbd7 execute_command_internal (bash + 0x3fbd7)
                #4  0x000000000043fe76 execute_command (bash + 0x3fe76)
                #5  0x0000000000426a21 reader_loop (bash + 0x26a21)
                #6  0x0000000000425144 main (bash + 0x25144)
                #7  0x00007fe88a642413 __libc_start_main (libc.so.6 + 0x27413)
                #8  0x00000000004256ce _start (bash + 0x256ce)
lines 1-28/28 (END)
```

Для полного чтения дампа необходимо установить утилиту **gdb**, выполнив команду (с правами суперпользователя **root** или администратора системы):

```
dnf install gdb
```

Запустите анализ дампа, выполнив команду:

```
coredumpctl gdb _PID=<PID_процесса,по_которому_создан_дамп>
```

```
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/bash...

warning: Unable to open "librpm.so.8" (librpm.so.8: cannot open shared object file: No such file or d
irectory), missing debuginfos notifications will not be displayed
Missing separate debuginfo for /usr/bin/bash
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/58/dbe494d53a3772d3e6f32b6c97e5b573
228ef.debug
Reading symbols from .gnu_debugdata for /usr/bin/bash...
(No debugging symbols found in .gnu_debugdata for /usr/bin/bash)
[New LWP 2759]
Missing separate debuginfo for /lib64/libiniparser.so.1
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/8c/f382586277a70f91a9befa609e0e1393
4ee12.debug
Missing separate debuginfo for /lib64/libtinfo.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/b7/b929fb355f28f374b5054d3191fc05a7
b5802.debug
Missing separate debuginfo for /lib64/libdl.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/e7/e6d7db0bca11a7f7da45896c9165d369
d14ab.debug
Missing separate debuginfo for /lib64/libc.so.6
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/75/b55efed6938ccb77e0e40fff7571aae0
ffcc0.debug
Missing separate debuginfo for /lib64/ld-linux-x86-64.so.2
Try: yum --enablerepo='*debug*' install /usr/lib/debug/.build-id/73/db0afd7ec02589302cf7bd90ae12d482
6a6e3.debug
Core was generated by `bash 1212.sh'.
Program terminated with signal SIGABRT, Aborted.
#0  0x00007fe88a6e715b in waitpid () from /lib64/libc.so.6
(gdb)
```

Настройка сбора дампов в СУБД Ред База Данных

Для сбора дампов *СУБД Ред База Данных* необходимо в файл службы **/usr/lib/systemd/system/firebird.service** в секцию [Service] добавить строку:

```
LimitCORE=infinity
```

Для этого необходимо воспользоваться редактированием модуля юнита с помощью команды:

```
systemctl edit firebird
```

И добавить следующие строки:

```
[Service]
LimitCORE=infinity
```

После сохранения сформируется файл **/etc/systemd/system/firebird.service.d/override.conf**.

При загрузке модуля **systemd** в памяти соединит фрагмент сформированного файла (**/etc/systemd/system/firebird.service.d/override.conf**) с полным файлом модуля (**/usr/lib/systemd/system/firebird.service**). Директивы фрагмента получат приоритет над найденными директивами в оригинальном файле модуля. Для проверки всех подгружаемых фрагментов необходимо выполнить:

```
systemctl cat firebird
```

Если СУБД при работе потребляет большой объем памяти (настроен большой страничный кэш), то создание дампа на диске после падения может продолжаться некоторое время. В конфигурационном файле службы **coredump** может быть настроен таймаут работы, после которого она будет остановлена. Для того чтобы времени на создание дампа было достаточно, необходимо увеличить таймаут, например, до 30 минут, изменив значение параметра RuntimeMaxSec в файле **/usr/lib/systemd/system/systemd-coredump@.service**:

```
RuntimeMaxSec=30min
```

ВАЖНО!

Дампы ядра полезны для устранения неполадок, однако могут являться причиной “утечки” конфиденциальных данных. Рекомендуется отключать дампы ядра и включать их только тогда, когда это действительно необходимо.

Для отключения сбора дампов ядра необходимо остановить службу **systemd-coredump**:

```
systemctl disable systemd-coredump
systemctl stop systemd-coredump
```

kdump — инструмент для анализа причин сбоев ядра

Минимальные требования
Запуск служб и проверка работы

Kdump — это стандартный механизм для создания дампа содержимого памяти компьютера при сбое ядра.

Минимальные требования

Минимальные требования к окружению:

- набор инструментов dracut – **dracut-056-9** и выше;
- механизм kexec – **kexec-tools-2.0.27** и выше.

Если в системе используются пакеты более ранних версий, обновите их:

```
dnf update
```

Если в системе пакеты не установлены, выполните команду:

```
dnf install dracut kexec-tools
```

Затем задайте размер для дампа ядра (в примере выделено **256 Мб** памяти). Для этого в файле **/etc/default/grub** добавьте в конец строки `GRUB_CMDLINE_LINUX=` параметр `crashkernel=256M` как показано в примере:

```
GRUB_CMDLINE_LINUX="rhgb quiet crashkernel=256M"
```

После внесения изменений необходимо обновить конфигурацию загрузчика **grub2**:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Перезагрузите систему:

```
reboot
```

Запуск служб и проверка работы

В **dmesg** проверьте, что выделенная под дампы ядра память была зарезервирована:

```
dmesg | grep crashkernel

[    0.002111] Reserving 256MB of memory at 3312MB for crashkernel (System RAM: 4095MB)

kdumpctl status

Kdump: Kdump is not operational
```

Для оценки выделенной памяти используйте команду:

```
kdumpctl estimate
```

Далее запустите службу **kdump**и добавьте ее в автозагрузку:

```
kdumpctl start
systemctl enable kdump.service --now
```

Проверьте статус службы:

```
kdumpctl status
systemctl status kdump.service
```

В выводе должно быть **active (running)**.

Для проверки работы можно выполнить команду вызова паники ядра:

```
echo c > /proc/sysrq-trigger
```

Если настройка выполнена верно, в каталоге **/var/crash/<timestamp>** будут располагаться файлы дампов **kexec-dmesg.log**, **vmcore** и **vmcore-dmesg.txt**.

Рекомендации по анализу журналов и дампов

1. Системные журналы событий ОС находятся в каталоге **/var/log/**, также можно использовать утилиту **journalctl** для просмотра журналов.

Подробную информацию по работе с утилитой **journalctl** см. в нашей статье «Работа с логами (утилита journalctl)».

Пример фильтрации содержимого журнала по типу ошибок:

```
journalctl -p err
journalctl -p alert
```

2. При анализе логов следует обращать внимание на ключевые слова, которые фигурируют в строках журналов:

- **failed** – обычно указывает на неудачное выполнение какой-либо операции или задачи. Например, сообщение вида authentication failed означает, что аутентификация завершилась неудачно;
- **error** – указывает на наличие ошибки. Далее может быть расшифровка ошибки и представлен ее код;
- **panic** – может появиться в записях, связанных с *Kernel Panic*, ошибками ядра Linux;
- **exception** – указывает на исключения (нештатную ситуацию или ошибку, которую программа или ядро не может обработать) в приложениях или ядре;
- **segfault** – ошибка сегментации, указывает на попытку доступа к памяти, к которой нет разрешения;
- **denied** – указывает на отказ в доступе, например, сообщение вида permission denied может быть связано с проблемами в правах доступа;
- **unable** – такие записи могут указывать на неспособность системы выполнить какое-либо определенное действие;
- **timeout** – задержки и таймауты могут указывать на проблемы с сетью или системными ресурсами;
- **crash** – аварийное завершение приложений или служб;
- **warning** – предупреждение о потенциальных проблемах, которые не вызывают сбоев, но требуют внимания;
- **critical** – критические события;
- **fatal** – критическая ошибка, которая приводит к сбою;
- **corruption** – обычно указывает на повреждение данных или файлов.

3. После определения кода или названия ошибки, которая связана со сбоем, уточняется ее более подробное описание, возможные причины возникновения, способы устранения. Поиск осуществляется в общедоступных поисковых системах, в системах отслеживания ошибок (*Bug tracking system*) по исследуемому компоненту или программе, а также соответствующим запросом в Техническую Поддержку программного продукта, в котором произошел инцидент.

4. Инструкция по работе с **coredump** — «Настройка systemd-coredump для автоматического сбора дампов».

5. Инструменты для анализа логов:

- средство просмотра файлов журналов **lnav** — «Средство просмотра журналов Log File Navigator (LNAV)»;
- веб-приложение для просмотра логов **loganalyzer** — «LogAnalyzer – веб-приложение для просмотра системных журналов».

Ошибка HTTPS-соединения

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция

При попытке установить защищенное соединение (**HTTPS**) может возникнуть ошибка вида:

```
POST https://XX.XX.XX.150/
 Attempting to connect to server XXXXXXXXXXX
 Connected to XXXXXXXXXXXXX
 SSL negotiation with XXXXXXXXXXXXXXXX
 SSL connection failure
 C0A63FE5747F0000:error:0A000152:SSL routines:final_renegotiate:unsafe legacy renegotiation disabled:ssl/statem/extensions.c:892:
 Failed to open HTTPS connection to XXXXXXXXXXX
```

Данная ошибка возникает из-за повторного согласования соединения по протоколу **TLSv1.2**. Для того чтобы фиксированная версия повторного согласования работала, ее должен поддерживать как клиент, так и сервер.

Для решения данной проблемы в конфигурационный файл **/etc/ssl/openssl.cnf** необходимо добавить блок `[system_default_sect]` со следующим содержимым:

```
[system_default_sect]
 Options = UnsafeLegacyRenegotiation
```

Данная настройка добавляет небезопасное повторное согласование как опцию для соединения на клиентской машине, поскольку сервер его не поддерживает.

После сохранения изменений в файле конфигурации необходимо перезагрузить машину:

```
reboot
```

и повторить попытку соединения.

Проверка работоспособности DNS с помощью nslookup

Синтаксис утилиты
Примеры использования утилиты
Получение IP-адреса
Обратное преобразование
Запись NS
Запись MX

nslookup – утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе **DNS**. Позволяет задавать различные типы запросов и опрашивать произвольно указываемые серверы для проверки работоспособности **DNS**, просмотра IP-адреса сервера, скорости его работы и т.д.

С помощью данной утилиты также можно не только получить IP-адрес по доменному имени, но и выполнить обратное преобразование, а также проверить необходимые записи **DNS**.

По умолчанию утилита **nslookup** предустановлена в РЕД ОС.

Синтаксис утилиты

Синтаксис утилиты имеет следующий вид:

```
nslookup [-опции] [домен] [сервер]
```

Основные опции **nslookup**:

- **-type** – тип информации, которую требуется получить, возможные типы: *txt*, *soa*, *ptr*, *ns*, *mx*, *mr*, *minfo*, *mg*, *mb*, *hinfo*, *gid*, *cname*, *a*, *any*;
- **-port** – использовать другой порт DNS-сервера (порт по умолчанию **53**);
- **-recurse** – рекурсивный запрос (информация запрашивается у других серверов, если она недоступна или отсутствует на указанном сервере);
- **-retry** – количество попыток опроса сервера;
- **-timeout** – время ожидания ответа от сервера (в секундах);
- **-fail** – опросить другой сервер имен, если указанный вернул ошибку.

Примеры использования утилиты

Получение IP-адреса

Для определения IP-адреса сервера по его доменному имени необходимо выполнить команду вида:

```
nslookup <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
Name: ya.ru
Address: 77.88.55.242
Name: ya.ru
Address: 5.255.255.242
Name: ya.ru
Address: 2a02:6b8::2:242
```

В строке **Server** выводится IP-адрес сервера, в строке **Address** – IP-адрес сервера и порт, с которого был отправлен запрос к **ya.ru**.

Далее отображается информация о запросе. В строке **Name** выводится доменное имя сервера, на который был отправлен запрос. В строке **Address** выводится IP-адрес, который принадлежит доменному имени сервера. Из примера видно, что доменному имени может

принадлежать несколько IP-адресов.

Обратное преобразование

Также с помощью утилиты **nslookup** может быть выполнено обратное преобразование IP-адреса в доменное имя. Для этого используется команда вида:

```
nslookup <IP-адрес>
```

Пример команды и ее вывода:

```
nslookup 77.88.55.242

242.55.88.77.in-addr.arpa name = ya.ru.

Authoritative answers can be found from:
55.88.77.in-addr.apra nameserver = ns3.yandex.ru.
55.88.77.in-addr.apra nameserver = ns4.yandex.ru.
ns3.yandex.ru internet address = 87.250.250.1
ns3.yandex.ru has AAAA address = 2a02:6b8::1001
ns4.yandex.ru internet address = 77.88.21.1
ns4.yandex.ru has AAAA address = 2a02:6b8:0:1::1:1
```

Запись NS

Первоисточником информации о домене являются его **NS**-серверы. Получить их можно, используя опцию `-type=ns` в команде следующего вида:

```
nslookup -type=ns <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=ns ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru nameserver = ns2.yandex.ru.
ya.ru nameserver = ns1.yandex.ru.

Authoritative answers can be found from:
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

Команда выведет список используемых серверов имен, в приведенном примере это **ns1.yandex.ru**.

Запись MX

Также можно получить **MX**-запись для домена, установив тип запроса **mx** в команде следующего вида:

```
nslookup -type=mx <доменное_имя>
```

Пример команды и ее вывода:

```
nslookup -type=mx ya.ru

Server:  192.168.31.1
Address: 192.168.31.1#53

Non-authoritative answer:
ya.ru mail exchanger = 10 mx.yandex.ru.
```

```
Authoritative answers can be found from:
ya.ru nameserver = ns1.yandex.ru.
ya.ru nameserver = ns2.yandex.ru.
ns1.yandex.ru internet address = 213.180.193.1
ns1.yandex.ru has AAAA address = 2a02:6b8::1
ns2.yandex.ru internet address = 93.158.134.1
ns2.yandex.ru has AAAA address = 2a02:6b8:0:1::1
```

В выводе команды будут отображены все настроенные почтовые серверы, у каждого сервера есть свой приоритет – 15, 10 или 5. Чем меньше число, тем выше приоритет адреса. В приведенном примере почтовый сервер – **mx.yandex.ru** имеет приоритет **10**.

Обновление РЕД ОС с 7.3 на 8

Для получения инструкции по **обновлению** стандартной редакции РЕД ОС 7.3 **до РЕД ОС 8**, пожалуйста, обратитесь в **Техническую поддержку** (https://support.red-soft.ru).

Инструкция предоставляется пользователям с **действующим** сертификатом на техническую поддержку.

Обновление ядра Linux до версии 5.15 в РЕД ОС 7.3

Окружение:

- **Версия РЕД ОС:** 7.3
- **Конфигурация:** Сервер графический, Сервер минимальный, Рабочая станция
- **Ядро:** 5.15.72-1

Примечание.
Инструкция является общей для стандартной и сертифицированной редакции.

Процедуру обновления ядра системы необходимо выполнять под учётной записью **root**. Для этого наберите в терминале:

```
su -
```

Потребуется ввести пароль пользователя **root**.

Перед установкой новой версии ядра обновите систему, выполнив в терминале команду:

```
dnf update
```

После окончания процесса обновления пакетов операционной системы установите пакет для подключения раздела репозитория **kernels**:

```
dnf install redos-kernels-release
```

При установке этого пакета автоматически будет подключен репозиторий с ядром Linux версии 5.15 для Ред ОС 7.3, поэтому вам не потребуется вручную добавлять его в конфигурационный файл.

Затем выполните команду для обновления кэша пакетов:

```
dnf makecache
```

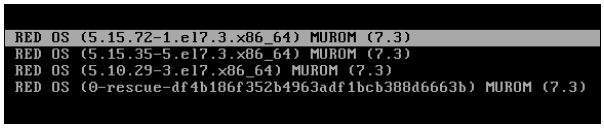
Выполните команду для обновления ядра и ядрозависимых пакетов:

```
dnf update
```

После этого перезагрузите ПК:

```
reboot
```

Теперь система будет по умолчанию автоматически загружаться с новой версией ядра **5.15.72**:



Для **удаления** устаревших версий ядра из системы можно воспользоваться утилитой управления ядрами kernel-manager.

Обновление ядра Linux до версии 6.1 в РЕД ОС 7.3

Окружение

- **Версия РЕД ОС**: 7.3
- **Конфигурация**: Сервер графический, Сервер минимальный, Рабочая станция
- **Версия ПО**: 6.1

> **Примечание.**
>
> Инструкция является общей для стандартной и сертифицированной редакции РЕД ОС 7.3.

Вы можете подробнее ознакомиться с процедурой обновления ядра до версии 6.1, просмотрев наши обучающие видео:

- на **RuTube** — Обновление ядра Linux до версии 6.1 в РЕД ОС 7.3 ;
- в **Яндекс.Дзен** — Обновление ядра Linux до версии 6.1 в РЕД ОС 7.3 .

На наших каналах вы также сможете найти много другой полезной информации.

Процедуру обновления ядра системы необходимо выполнять под учётной записью **root**. Для этого наберите в терминале:

```
su -
```

Потребуется ввести пароль пользователя **root**.

Перед установкой новой версии ядра обновите систему, выполнив в терминале команду:

```
dnf update
```

После окончания процесса обновления пакетов операционной системы установите пакет для подключения раздела репозитория **kernels6**:

```
dnf install redos-kernels6-release
```

При установке этого пакета автоматически будет подключен репозиторий с ядром Linux версии 6.1 для Ред ОС 7.3, поэтому вам не потребуется вручную добавлять его в конфигурационный файл.

Затем выполните команду для обновления кэша пакетов:

```
dnf makecache
```

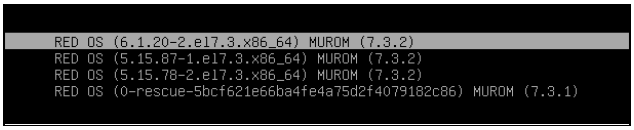
Выполните команду для обновления ядра и ядрозависимых пакетов:

```
dnf update
```

После этого перезагрузите ПК:

```
reboot
```

Теперь система будет по умолчанию автоматически загружаться с актуальной минорной версией 6-го ядра:



> Для **удаления** устаревших версий ядра из системы можно воспользоваться утилитой управления ядрами kernel-manager.

Установка realtime-ядра в РЕД ОС 8

Окружение

- **Версия РЕД ОС**: 8
- **Конфигурация**: Рабочая станция, Сервер графический, Сервер минимальный
- **Версия ПО**: redos-kernel-rt-release-1.0-1, kernel-rt-6.6.52-1

Ядро реального времени (*real-time kernel*, *kernel-rt*) представляет собой специализированную версию стандартного ядра, используемого в РЕД ОС. Однако важным отличием ядра реального времени от стандартного является обеспечение *предсказуемости* или *детерминированности* поведения системы в различных внешних условиях.

Real-time kernel включает в себя более жесткие правила планирования и управления ресурсами, чтобы свести к минимуму задержки и время реакции, что часто является критически важным условием в некоторых системах.

К основным функциям *real-time kernel* относятся:

- *планирование задач* – ядро должно поддерживать различные алгоритмы планирования для управления выполнением задач;
- *обработка прерываний* – быстрая реакция на внешние события через обработку прерываний;
- *управление памятью* – эффективное распределение и управление памятью для обеспечения быстрого доступа к данным;
- *синхронизация* – механизмы для предотвращения конфликтов при доступе к общим ресурсам.

По времени реакции на события ядра реального времени можно разделить на два типа – **hard real-time** и **soft real-time**.

Hard real-time (ядра с жесткими ограничениями) не допускают задержек реакции системы, так как это может привести к потере актуальности результатов, большим финансовым потерям или даже авариям и катастрофам. Ситуация, в которой обработка событий происходит за время, большее предусмотренного, считается фатальной ошибкой. При возникновении такой ситуации ядро прерывает операцию и блокирует её, чтобы, насколько возможно, не пострадала надёжность и готовность остальной части системы. Примерами систем жёсткого реального времени могут быть бортовые системы управления (на самолёте, космическом аппарате, корабле и пр.), системы аварийной защиты, регистраторы аварийных событий.

Soft real-time (ядра с мягкими ограничениями) не гарантируют выполнение задач в строгие сроки, но стараются минимизировать задержки. Задержка реакции считается восстановимой ошибкой, которая может привести к увеличению стоимости результатов и снижению производительности, но не является фатальной. Примером может служить работа компьютерной сети – если система не успела обработать очередной принятый пакет, это приведёт к остановке на передающей стороне и повторной посылке (в зависимости от протокола). Данные при этом не теряются, но производительность сети снижается.

Выбор типа ядра зависит от специфических требований приложения и его временных ограничений.

В РЕД ОС используется *ядро* с *мягким* типом ограничений (*soft real-time*) и патчем **PREEMPT_RT**, реализующим POSIX real-time API.

Установка

Процедуру установки **RT**-ядра в ОС необходимо выполнять под учётной записью **root**. Для этого выполните в терминале:

```
su -
```

Потребуется ввести пароль пользователя **root**.

Перед установкой ядра обновите систему, выполнив в терминале команду:

```
dnf update
```

После окончания процесса обновления пакетов ОС установите пакет для подключения раздела репозитория **kernel-rt**:

```
dnf install redos-kernel-rt-release
```

Затем выполните команду установки **RT**-ядра:

```
dnf install kernel-rt
```

Выполните команду для обновления ядрозависимых пакетов:

```
dnf update
```

После этого перезагрузите систему:

```
reboot
```

Для проверки версии ядра, с которым загружена система, выполните:

```
uname -vr

6.6.52-1.red80.x86_64-rt43 #1 SMP PREEMPT_RT Mon Sep 30 16:52:27 MSK 2024
```

Обновление системы в рамках корректирующих релизов РЕД ОС 7.3

Корректирующие релизы РЕД ОС собраны на пакетной базе репозитория 7.3 и включают в себя пакеты последних версий со всеми исправлениями, улучшениями и обновлениями безопасности, накопленными с момента выпуска РЕД ОС 7.3.

С момента выпуска РЕД ОС 7.3 было опубликовано несколько корректирующих релизов. Подробнее ознакомиться с графиком выпуска корректирующих релизов и списками изменений в каждом из них можно в нашей статье «Версии РЕД ОС и сроки поддержки».

Все пользователи РЕД ОС 7.3 *стандартной редакции* могут перейти на актуальный корректирующий релиз (на данный момент РЕД ОС 7.3.4) штатным обновлением системы с использованием команды:

```
sudo dnf update
```

Однако в некоторых частных случаях могут возникнуть ситуации, когда при обновлении системы происходит ошибка зависимостей вида:

```
Ошибка: проверка транзакции на разрешение зависимостей:
rpmlib(CaretInVersions) <= 4.15.0-1 нужен для systemd-249.12-2.el7.x86_64
```

В данном случае необходимо предварительно обновить пакетный менеджер **rpm** до версии **не ниже указанной** (в примере *4.15.0-1*) командой:

```
sudo dnf update rpm
```

А затем запустить штатное обновление системы:

```
sudo dnf update
```

Также при возникновении каких-либо конфликтов при обновлении ОС можно передать команде дополнительные параметры:

- `--allowerasing` – разрешить удаление установленных пакетов для разрешения зависимостей;
- `--skip-broken` – разрешить проблемы зависимостей, пропустив пакеты;
- `-b, --best` – попытаться использовать наиболее подходящие версии пакетов в транзакциях;
- `--nobest` – не ограничивать транзакцию наилучшим кандидатом.

Ознакомиться с полным списком доступных параметров и способами их использования можно, выполнив команду:

```
dnf update --help
```

Версии РЕД ОС и сроки поддержки

Сроки поддержки версий РЕД ОС
Стандартная редакция
Сертифицированная редакция

Версии РЕД ОС нумеруются двумя цифрами: **A.B**, где **A** - мажорная версия, **B** - минорная версия. На ноябрь 2024 года выпущено 4 версии РЕД ОС: 7.1, 7.2, 7.3 и 8.

РЕД ОС имеет 2 редакции: **стандартную** и **сертифицированную**. Обе редакции в рамках одной версии имеют общую пакетную базу. Сертифицированная редакция РЕД ОС проходит регулярные сертификационные испытания в системе сертификации ФСТЭК России.

Каждая версия и редакция РЕД ОС имеет свой репозиторий пакетов. В период поддержки версии РЕД ОС в репозитории публикуются обновления безопасности и обновления функционала.

Сроки поддержки версий РЕД ОС

Каждая версия РЕД ОС (начиная с 7.3) поддерживается минимум 5 лет. При окончании поддержки:

- прекращается выпуск обновлений безопасности и обновлений функционала;
- установочный образ остается доступен на сайте РЕД ОС в архиве, репозиторий остается открытым;
- услуги технической поддержки оказываются только в рамках поддерживаемых версий РЕД ОС.

Стандартная редакция

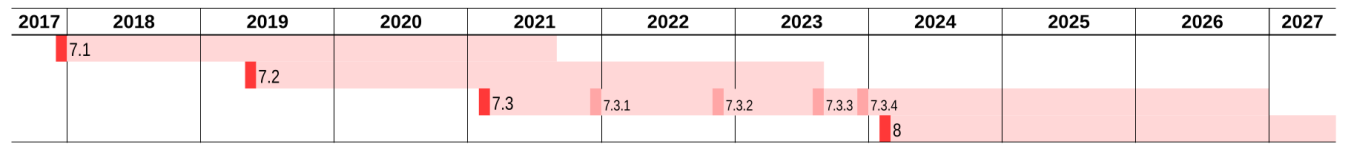
В период поддержки версии РЕД ОС стандартной редакции, начиная с версии 7.3, выпускаются **корректирующие релизы**, которые нумеруются тремя цифрами: **A.B.x**, где **x** - номер корректирующего релиза в рамках версии **A.B**. Корректирующий релиз представляет собой установочный образ, который включает в себя обновления, накопленные с момента предыдущего релиза. На ноябрь 2024 года актуальным корректирующим релизом для версии 7.3 является релиз 7.3.4.

Пользователям, которые уже используют версию РЕД ОС 7.3, нет необходимости заново скачивать установочный образ и переустанавливать ОС. Штатный процесс регулярных обновлений обеспечивает автоматическую эволюцию ОС, приводя ее в соответствие с последним выпуском 7.3.x. Использование нового корректирующего релиза позволяет сэкономить время и сетевой трафик, которые уходят на обновление ОС после её установки. Особенно эта экономия заметна в тех случаях, когда обновления устанавливаются нечасто.

История выхода версий РЕД ОС стандартной редакции:

Версия	Номер релиза	Список изменений	Дата релиза	Срок поддержки версии
7.1	7.1		Дек. 2017	31.08.2021
7.2	7.2		Май 2019	31.08.2023
7.3	7.3		Фев. 2021	31.12.2026
	7.3.1	Список изменений в 7.3.1	Дек. 2021	
	7.3.2	Список изменений в 7.3.2	Ноя. 2022	
	7.3.3	Список изменений в 7.3.3	Авг. 2023	
	7.3.4	Список изменений в 7.3.4	Дек. 2023	
8	8	Список изменений в 8	Фев. 2024	31.12.2028

График выхода версий РЕД ОС стандартной редакции



где:

-  - Релиз новой версии РЕД ОС;

- - Корректирующий релиз в рамках версии РЕД ОС;
- - Общий период поддержки версии РЕД ОС.

Сертифицированная редакция

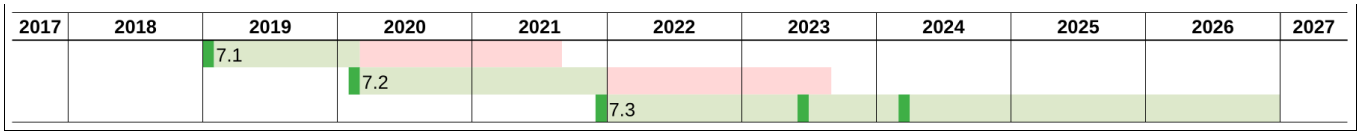
Сертификат ФСТЭК России №4060 от 12.01.2019 распространяет свое действие на единственную версию РЕД ОС. На август 2023 года сертификат №4060 распространяется на РЕД ОС версии 7.3. Однако с момента переоформления сертификата на новую версию РЕД ОС продолжают выпускаться обновления безопасности в рамках общего срока поддержки для предыдущей версии РЕД ОС.

В период поддержки версии РЕД ОС сертифицированной редакции выпускаются обновления безопасности, которые публикуются в репозитории. Бюллетени безопасности публикуются в соответствующем разделе сайта: https://redos.red-soft.ru/support/secure/. Для прохождения очередных сертификационных испытаний формируется установочный образ, включающий в себя все накопленные ранее обновления безопасности и обновления функционала.

История выхода версий РЕД ОС сертифицированной редакции

Версия	Дата получения/переоформления сертификата	Событие
7.1	12.01.2019	Получение сертификата на версию 7.1
7.2	18.02.2020	Переоформление сертификата на версию 7.2
7.3	16.12.2021	Переоформление сертификата на версию 7.3
	23.06.2023	Переоформление сертификата на версию 7.3 на соответствие требованиям ФСТЭК России к средствам виртуализации и контейнеризации
	Мар. 2024	Продление срока действия сертификата на версию 7.3 до 12.01.2029

График выхода версий РЕД ОС сертифицированной редакции



где:

- - Получение/переоформление сертификата ФСТЭК России;
- - Период поддержки версии РЕД ОС в рамках сертификата ФСТЭК России;
- - Общий период поддержки версии РЕД ОС.

Рекомендации по организации процесса тестирования и установки обновлений РЕД ОС

Общая информация о версиях РЕД ОС
Типы выпускаемых обновлений для РЕД ОС
Риски и важность тестирования перед внедрением обновления
Рекомендации по тестированию обновлений
Общий подход в организации тестовых репозиториев
Общая схема организации репозиториев в тестовой и продуктивной среде
Полезные ссылки

Общая информация о версиях РЕД ОС

Информация о принципах нумерации версий РЕД ОС, редакциях и истории выхода версий приведена в Базе знаний на официальном сайте РЕД ОС в статье «Версии РЕД ОС и сроки поддержки».

Типы выпускаемых обновлений для РЕД ОС

1. Обновления безопасности.

Обновления выпускаются по мере обнаружения и устранения уязвимостей. Публикуются в репозитории РЕД ОС. Каждое обновление безопасности сопровождается бюллетенем на сайте в разделе «Обновления безопасности». Обновление безопасности может производиться применением определенного патча безопасности для устранения уязвимостей или других критических проблем, связанных с безопасностью. Кроме этого допустимы обновления на новую версию пакета, с целью закрытия найденных угроз безопасности в предыдущих версиях.

Периодичность обновления может варьироваться от ежедневной до более редкой в зависимости от активности в выявлении и устранении уязвимостей.

2. Обновления функционала.

Обновления функционала публикуются в репозитории в виде новых версий rpm-пакетов. Как правило, обновления связаны с потребностью заказчиков в более новой версии определенного пакета и/или с решением какой-либо известной проблемы. Вместе с обновлением функционала автоматически может быть применено обновление безопасности.

Периодичность обновления может варьироваться от ежедневной до более редкой в зависимости от активности добавления нового функционала в программный продукт и потребности заказчика в новом функционале.

3. Новая версия РЕД ОС.

Информация о выпуске новых версии публикуется на официальном сайте РЕД ОС. Предусматривается возможность “мягкого” обновления (без обязательной “чистой” установки системы) текущей версии РЕД ОС на следующую версию.

График выпуска версий представлен в статье «Версии РЕД ОС и сроки поддержки».

4. Корректирующие релизы.

Выпуск корректирующего релиза сопровождается подробным списком изменений, который публикуется на сайте в Базе Знаний в разделе «Обновление РЕД ОС». Использование корректирующих релизов позволяет избежать длительного обновления системы после ее установки.

Периодичность выпуска корректирующих релизов — несколько раз в год (зависит от количества накопленных обновлений в репозитории).

Риски и важность тестирования перед внедрением обновления

Разработчиками РЕД ОС выполняется тестирование всех публикуемых обновлений. Пакеты обновлений проверяются на установку, удаление, обновление, а также выполняется базовое функциональное тестирование наиболее востребованных, часто используемых программ и компонентов ОС.

Учитывая разнообразие конфигураций и компонентов ИТ-инфраструктуры, возможны ситуации, когда обновления РЕД ОС могут вызвать разного рода конфликты в работе компонентов операционной системы и/или прикладного ПО. Поэтому настоятельно рекомендуется проводить тестирование обновлений в изолированной тестовой среде перед их внедрением в продуктивную среду

(рабочую среду). Такой подход поможет предотвратить возможные сбои и обеспечить бесперебойную работу в продуктивной среде.

Риски невыполнения предварительного тестирования:

1. Обновления пакетов могут вызвать конфликты с существующими настройками системы и/или приложениями, что может привести к некорректной работе прикладного ПО, а также к ошибкам и сбоям в работе самой ОС. Необходимость предварительного тестирования вызвана особенностью инфраструктуры и программного окружения заказчика, что не всегда может быть учтено при тестировании обновлений разработчиком ОС.

2. Обновления пакетов могут повлиять на работу приложений. Например, в новых версиях пакетов может быть удалена определенная функция, которая активно используется в рабочей среде, что потенциально может вызвать проблемы в работе приложения.

3. Внедрение обновлений без предварительного тестирования может вызвать потребность в разрешении множества проблем и привести к дополнительным трудозатратам при проведении восстановительных работ.

Рекомендации по тестированию обновлений

Продуктивная среда (также известная как рабочая среда или продакшн среда) — это окружение, в котором выполняются и обрабатываются основные бизнес-процессы и операции организации или предприятия.

Общие рекомендации по установке обновлений:

1. Обновления безопасности рекомендуется устанавливать в обязательном порядке для нивелирования угроз безопасности, которые могут быть использованы злоумышленником через известные уязвимости.

2. Рекомендуется применять обновления функциональности, исходя из актуальности новых версий программного обеспечения и необходимости устранения известных ошибок.

3. В общем случае рекомендуется устанавливать и обновления безопасности, и обновления функционала.

4. Использование корректирующих релизов рекомендуется для новых инсталляций РЕД ОС. Это позволяет сократить время и ресурсы, необходимые на установку обновлений после установки системы.

Частота применения обновлений зависит от внутренних бизнес-процессов заказчика, но важно помнить, что отсрочка в установке обновлений может привести к накоплению большого объема необходимых обновлений.

Организация тестирования и установки обновлений:

1. Для проверки обновлений в продуктивной среде рекомендуется создание тестового контура. Тестовый контур должен быть разделен на серверную группу и группу рабочих станций (АРМ).

2. В соответствии с установленными стандартами для продуктивной среды (например, при наличии различных типов рабочих мест (АРМ)), рекомендуется включить в тестовую среду минимум по одной рабочей станции каждого типа АРМ. Аналогично необходимо поступить и с серверами. Это поможет обеспечить более полное тестирование обновлений.

3. Для стандартных рабочих мест (АРМ) рекомендуется проверить установку стандартного программного обеспечения и выполнение типовых операций.

4. Для тестирования обновлений в тестовом контуре необходимо развернуть зеркало репозиториев РЕД ОС. Синхронизация тестовых репозиториев с официальными репозиториями должна выполняться по мере необходимости и с периодичностью, определенной самим заказчиком.

5. В случае использования ПО, обновление которого необходимо выполнять по определенным правилам и алгоритмам (например, при обновлении СУБД нужно будет выполнить бекап БД, остановить службы, обновить СУБД, восстановить БД, запустить службы), необходимо пользоваться рекомендациями к обновлению данного ПО.

Для обеспечения безопасного обновления РЕД ОС в продуктивной среде также рекомендуется настраивать ***предпродуктивные*** тестовые зеркала. ***Предпродуктивное*** тестовое зеркало репозитория — это вторичная копия тестового зеркала, содержащая только успешно протестированные обновления, готовые к внедрению в продуктивное зеркало. Это позволит контролировать процесс синхронизации обновлений и тестирования перед их внедрением в продуктивную среду.

Общий подход в организации тестовых репозиториев

Тестовое зеркало:

- Создать зеркало репозиториев для тестирования обновлений.
- Синхронизировать это зеркало с официальными репозиториями, чтобы обеспечить доступ к актуальным обновлениям для тестирования.
- Синхронизацию с официальными репозиториями следует обязательно выполнять вручную — для контроля успешного завершения синхронизации.
- В тестовом зеркале проводить первичные тесты без воздействия на продуктивную среду.

Предпродуктивное Тестовое Зеркало:

- Создать второе зеркало репозиториев, которое будет синхронизировано с тестовым зеркалом после успешных тестов обновлений.
- Это зеркало содержит только те обновления, которые успешно прошли тестирование.

Продуктивное Зеркало:

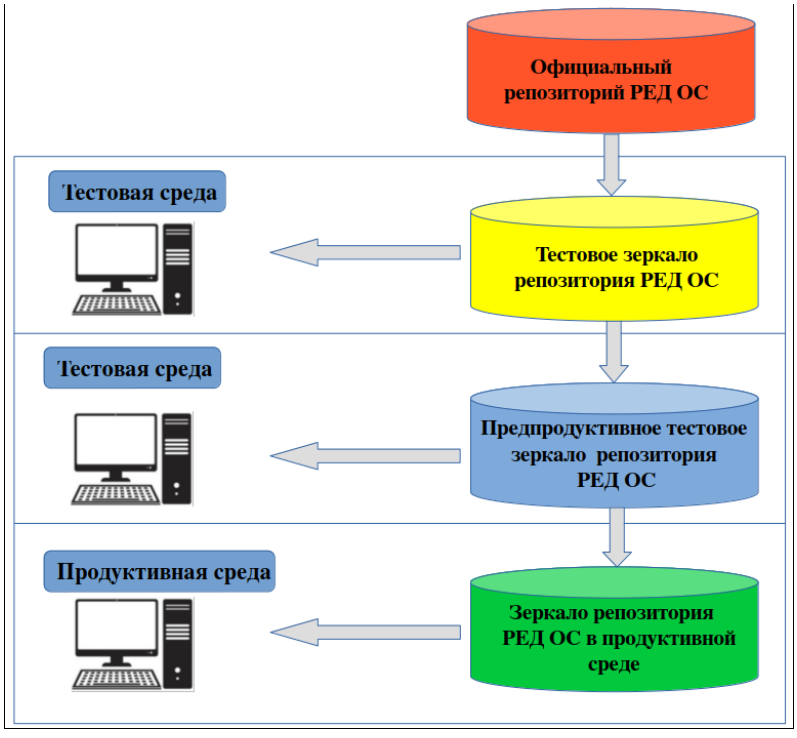
- Настроить продуктивное зеркало, которое будет синхронизироваться с "Предпродуктивным тестовым зеркалом"
- В продуктивном зеркале будут содержаться только проверенные и безопасные обновления, готовые для внедрения в рабочую среду.

В итоге для организации локальных репозиториев рекомендуется настроить и использовать в работе **3 сервера**.

К ним относятся:

- Тестовое зеркало;
- Предпродуктивное Тестовое Зеркало;
- Продуктивное Зеркало

Общая схема организации репозиториев в тестовой и продуктивной среде



Полезные ссылки

- Портал технической поддержки РЕД ОС: https://support.red-soft.ru/.

- Информация об обновлениях безопасности публикуется в соответствующем разделе сайта: https://redos.red-soft.ru/support/secure/.
- Списки изменений в корректирующих релизах РЕД ОС: https://redos.red-soft.ru/base/update/.
- Инструкции по обновлению версии ядра Linux приводится в статьях БЗ:
  - *Обновление ядра Linux до версии 5.15 в РЕД ОС 7.3* — https://redos.red-soft.ru/base/update/update-kernel-5-15-7-3/;
  - *Обновление ядра Linux до версии 6.1 в РЕД ОС 7.3* — https://redos.red-soft.ru/base/update/update-kernel-6-1/.
- Общая информация о работе системы управления пакетами DNF приведена в соответствующем разделе БЗ:
  - для РЕД ОС 7.3 —https://redos.red-soft.ru/base/redos-7_3/7_3-base-consept/7_3-sys-dnf/;
  - для РЕД ОС 8 — https://redos.red-soft.ru/base/redos-8_0/8_0-base-consept/8_0-sys-dnf/.
- Информацию о создании локального репозитория и настройке синхронизации размещена в статьях БЗ:
  - для РЕД ОС 7.3 — https://redos.red-soft.ru/base/redos-7_3/7_3-administation/7_3-repo/;
  - для РЕД ОС 8 — https://redos.red-soft.ru/base/redos-8_0/8_0-administation/8_0-repo/.

Список изменений в РЕД ОС 7.3.1

РЕД ОС 7.3.1 является обновлением РЕД ОС 7.3. Дистрибутив собран на пакетной базе репозитория 7.3 и включает в себя пакеты последних версий со всеми исправлениями, улучшениями и обновлениями безопасности, накопленными за 2021 год.

Все пользователи РЕД ОС 7.3 стандартной редакции могут перейти на 7.3.1 через штатное обновление системы (**dnf update**), ядро Linux обновляется опционально (https://redos.red-soft.ru/base/update/update-kernel-5-15-7-3/).

Основные изменения в **РЕД ОС 7.3.1**:

- LTS-ядро Linux **5.15**.
- Отдельный образ **LiveUSB** с предустановленной конфигурацией «Рабочая станция».
- В «Рабочую станцию» добавлено окно приветствия, которое поможет начинающему пользователю ознакомиться с системой и настроить ее «под себя».
- Отключено сообщение о последних попытках входа в систему.
- Утилита **lsb_release** теперь выводит подробную информацию о версии, редакции и конфигурации установленной ОС.
- Исправлены выявленные ошибки в установщике **Anaconda**.
- В составе РЕД ОС 7.3.1 по-умолчанию идут такие пакеты как:
    - *Timeshift* для снимков системы;
    - *gnome-multi-writer* для записи ISO;
    - *hplip, hplip-gui* и *foo2zjs* для работы с принтерами;
    - *python3-smbc* для обзора принтеров в сети;
    - *GParted* для работы с дисками;
    - редактор меню *brisk-menu* был заменен на *mozo*;
    - *libreoffice-filters* для понимания форматов MS Office (docx/xlsx/pptx) самых последних версий, а также ряда иных форматов (Adobe Pagemaker/InDesin, *QuarkXPress* и пр.).
- Внесены улучшения и исправления в графическом окружении MATE: исправлен набор пиктограмм, добавлена темная тема, расширено контекстное меню для работы с файлами и каталогами (копирование/перемещение файлов в указанный каталог, защищенное преобразование файлов).
- Добавлена экранная клавиатура **Onboard**, в том числе в окно блокировки сессии.
- Обновлен пакет **dnfdragora** и исправлены выявленные ошибки в его работе.
- Добавлена утилита **dnfdragora-updater**, которая уведомляет пользователя о доступных обновлениях.
- Устранена ошибка при установке rpm-пакетов «двойным кликом».
- Решены проблемы с «двойной» авторизацией в **GDM**.
- Исправлены выявленные проблемы в графическом окружении **Cinnamon**.
- Обновлены до актуальных версий браузеры **Chromium**, **Firefox** и почтовый клиент **Thunderbird**.
- **LibreOffice** обновлён до версии **7.2.4**.

Репозиторий 7.3 получил обновления пакетов и пополнился новыми решениями для построения серверной инфраструктуры:

- Инструмент управления жизненным циклом, развертывания, настройки и мониторинга физических и виртуальных серверов **Foreman** версии **3.0.0**.
- Системы управления конфигурациями **Ansible 2.9.21** и **Puppet 7.12.0**.
- Распределенная файловая система **Ceph 15.2.14**.
- Обновлены **Samba** до версии **4.14.6** и **FreeIPA** до версии **4.8.10**.
- Эмулятор **QEMU/KVM** обновлен до версии **6.1.0**.
- Платформа контейнеризации **Docker CE 20.10.10** и инструмент для работы с многоконтейнерными приложениями **Docker Compose 1.29.2**.
- Сервер управления облачной инфраструктурой **NextCloud** обновлен до **23.0.0**.

Репозиторий 7.3 пополнился набором ПО для образования:

- Система управления учебным классом **Veyon**.
- Среда разработки **Gambas** для языка **Basic**.
- Среда программирования **КУМИР**.
- Среда разработки **Code::Blocks**.
- ПО для создания и редактирования интернет-приложений **Bluefish**.
- Пакеты для создания слайд-шоу и видео-роликов **Imagination** и **Ffdiaporama**.
- Программа для создания 2D-анимации **SynfigStudio**.
- Видеоредакторы **Shotcut** и **Kdenlive**.
- Клавиатурный тренажер **Ktouch**.

Список изменений в РЕД ОС 7.3.2

РЕД ОС 7.3.2 является обновлением РЕД ОС 7.3. Дистрибутив собран на пакетной базе репозитория 7.3 и включает в себя пакеты последних версий со всеми исправлениями, улучшениями и обновлениями безопасности, накопленными за 2022 год. Все пользователи РЕД ОС 7.3 стандартной редакции могут перейти на 7.3.2 через штатное обновление системы (**dnf update**).

Вы можете подробнее ознакомиться с основными обновлениями, имеющимися в РЕД ОС 7.3.2, просмотрев наши обучающие видео:

- на **RuTube** — Обзор обновления РЕД ОС 7.3;
- в **Яндекс.Дзен** — Обзор обновления РЕД ОС 7.3.

На наших каналах вы также сможете найти много другой полезной информации.

Основные изменения в установочном образе РЕД ОС 7.3.2:

- **Ядро** Linux обновлено до версии **5.15.72**.
- Обновлен загрузчик **GRUB** (закрыты уязвимости «Boot Hole» и «Secure Boot Bypass 2021»).
- Решена проблема с определением видеодрайверов Intel UHD на этапе установки РЕД ОС (обновлён пакет **linux-firmware**).
- Обновлен дизайн оформления рабочего стола - появилось 2 новые темы. Желаемую тему можно выбрать в окне приветствия при первом входе в систему.
- Из окна приветствия теперь можно установить **Яндекс.Браузер** - нажатием кнопки выполнится загрузка и установка rpm-пакета штатными средствами (через **dnfdragora**).
- GPG-ключ подписи пакетов РЕД ОС теперь установлен в системе по умолчанию и не требует установки при первом обращении к репозиторию.
- Предустановлен TLS-сертификат удостоверяющего центра Минцифры России для беспрепятственного доступа пользователей к важным Интернет-сервисам и сайтам, которые перешли на российские сертификаты.
- Часовой пояс в установщике Anaconda теперь по умолчанию выставлен MSK (UTC+3), а для автоматического определения местоположения используется Российский сервис **GeoIP**.
- В установщике появилась опция “Средства облачной настройки” (выполняет установку пакета **cloud-init**), обеспечивающая возможность автоматического конфигурирования РЕД ОС в средах виртуализации.
- В системе предустановлены пакеты **orca**, **atop**, **gnome-disk-utility**, а также драйверы **rtw89** и **rtl8821ce**, исключены устаревшие версии **openjdk - 1.6 и 1.7**.
- Обновлены основные офисные приложения: **LibreOffice 7.4.2.3**, **Thunderbird 102.4.0** и др.

Репозиторий РЕД ОС 7.3 обновился и пополнился следующими пакетами:

Пользовательское ПО:

- Обновлен офисный пакет **LibreOffice** до версии **7.4.2.3**.
- Обновлены браузер **Firefox 102.4.0** и почтовый клиент **Thunderbird 102.4.0**.
- Инструмент для запуска Windows приложений **Wine 7.16**.
- Система управления проектами **ProjectLibre 1.9.3**.
- Обновлен клиент мгновенного обмена сообщениями **Pidgin** до версии **2.14.8**.
- Графический планировщик заданий **Zeit 0.6.0**.
- Менеджер паролей **KeePassXC 2.6.6**.
- Обновлена программа чтения с экрана **Orca 42.0** и речевой синтезатор **speech-dispatcher 0.11.2**.
- ПО для управления питанием **TLP** и **TLPUI 1.5.0**.
- Программа для создания скриншотов **Ksnip 1.10.0**.
- Обновлены пакеты для создания слайд–шоу **Sox 14.4.2** и **Imagination 3.6**.
- Программа для освобождения места на диске **Bleachbit 4.4.0**.
- ПО для поиска дубликатов файлов **Fslint 2.47**.
- Программы для создания и печати штрих-кодов **Zint 2.11.0** и **gLabels 3.4.1**.

ПО для работы с файловыми системами:

- Криптографические файловые системы **EncFS** (**fuse-encfs 1.9.5**) и **eCryptfs** (**ecyptfs-utils 111**).
- Обновлены пакеты виртуальной файловой системы GNOME **GVFS 1.48.2**.
- Пакеты для поддержки файловой системы **ZFS 2.1.5**.
- Обновлены пакеты для монтирования сетевых файловых систем CIFS **cifs-utils 6.15**.
- Программа для монтирования сетевых хранилищ **Davfs2 1.6.1**.
- Инструмент для работы с облачными образами ВМ **Cloud-utils 0.31**.
- ПО для синхронизации файлов **Unison 2.51.5**.

Серверное и системное ПО:

- Обновлён **Zabbix** до версии **6.2.1**.
- Пересобран **Nginx** с дополненными модулями **GeoIP2** и **ModSecurity**.
- **Ansible** обновлен до версии **6.4** (размещен в подключаемом репозитории, пакет ansible6-release), добавлена поддержка РЕД ОС для работы распространенных плейбуков (идентифицирующих ОС по атрибуту ansible_os_family и другим).
- Обновлен почтовый сервер **Postfix** до версии **3.7.2** и сервер печати **Cups** до версии **2.3.3op**.
- FTP-сервер **Proftpd 1.3.6e**.
- DNS-сервер **NSD 4.3.9**.
- Обновлен прокси-сервер **Squid** до версии **5.5**.
- Обновлена платформа компьютерной телефонии **Asterisk** до версии **18.4.0**.
- Обновлен программный брокер сообщений **RabbitMQ 3.10.6**.
- Программа для вывода диалоговых окон **Yad 10.1**.
- Инструмент управления и запуска контейнеров OCI **Podman 3.4.0**.
- Пакеты для работы с LXC контейнерами **Lxcfs 4.0.12**, **LXD 4.17** и **Distrobuilder 1.3**.
- Набор инструментов для виртуализации **Libvirt 7.6.0**.
- Обновлена графическая консоль управления машинами KVM **Virt Viewer** до версии **11.0**.
- ПО для организации VPN **WireGuard** версии **1.0.20210914**.
- Система предотвращения вторжений **SSHGuard 2.4.2**.
- Балансировщик нагрузки DNS **DNSDist 1.7.1** и подключений к удаленному рабочему столу **X2gobroker 0.0.4.3**.
- Обновлены балансировщики нагрузки **Keepalived** до версии **2.2.7** и **Haproxy** до версии **2.6.0**.
- Обновлены системы мониторинга **Nagios 4.4.7** и **Dstat 0.7.4**.
- Инструмент реализации сетевой маршрутизации **Frr 8.2.2**.
- Программа для работы с сетевыми протоколами **Putty 0.77**.
- Обновлена библиотека **OpenSSL** до версии **1.1.1q**.
- ПО для управления сеансами SSH **Redial 0.6**.
- Пакет для управления портами **Knock 0.8**.
- Обновлен пакет для сканирования IP-сетей **Nmap** до версии **7.80**.
- Графический интерфейс для подключения удаленных USB-устройств **USBIP-GUI** версии **20210429** и для редактирования конфигураций Conky **conky-manager 2.3.4**.
- Обновлен пакет для обработки ввода с сенсорных устройств **libinput 1.21.0**.
- Платформа для визуализации анализа данных **Grafana 7.5.11**.
- Система полнотекстового поиска и анализа данных **OpenElasticSearch 1.13.2** (включая **Kibana**), а также инструмент сбора данных **Logstash** и поставщик данных **Filebeat** версий **7.10.2**.
- Пакеты для работы кластера **corosync-qdevice 3.0.1** и **corosync-qnetd 3.0.1**.
- Обновлен инструмент анализа дампа памяти **Crash** до версии **8.0.1**.

- Библиотеки для работы со статическими данными **Whitenoise 6.2.0**.
- Программа создания зеркала репозитория **Debmirror 2.36**.
- Инструменты для автоматизации процесса загрузки Linux **Dracut 056.2**.
- Обновлен видеокодек **Dirac** до версии **1.0.2**.
- Программа для конфигурирования отображения кнопок устройств ввода **Key Mapper 1.2.1**.

ПО для работы с СУБД:

- Объектно-реляционная СУБД **PostgreSQL 14**.
- Менеджер бэкапов для серверов PostgreSQL **Barman 3.0.1**.
- Пакеты для поддержки географических объектов в PostgreSQL **PostGIS 2.5.5**.
- Обновлен драйвер **ODBC для PostgreSQL** до версии **13.01**.
- Инструмент для работы кластера PostgreSQL **Patroni 2.1.3**.
- Обновлена библиотека для доступа к базе данных Microsoft SQL **FreeTds** до версии **1.3.12**.

Средства разработки:

- Обновлен **PHP** до версии **8.1.9** (размещен в подключаемом репозитории, пакет php81-release).
- Обновлен пакет **OpenJDK** (**Java**) до версии **13**.
- Пакеты для языка программирования Go **Golang 1.18.2**.
- Обновлен **.NET** до версии **6.0**.
- Инструмент для создания Flatpak-приложений **Flatpak Builder 1.2.2**.
- Обновлена среда разработки для Python **Thonny 3.3.14**.
- Многофункциональная среда разработки и аналог редактора кода Virtual Studio **Codium 1.66.1**.
- Обновлен многофункциональный текстовый редактор для программирования **Geany 1.38**.
- Обновлена среда разработки на основе компилятора Free Pascal **Lazarus 2.2.2**.
- Образовательная среда программирования **Kturtle 20.04.3**.

ПО для образования:

- Программа для работы с интерактивными досками **OpenBoard 1.6.1** и инструмент поддержки жестов на сенсорных панелях **touchegg 2.04.14**.
- Программный комплекс для разработки электрических схем и печатных плат **KiCAD 6.0.0**.
- ПО для эконометрического моделирования **Gretl** и отдельный пакет для процессоров, не поддерживающих технологию AVX **gretl-lite** версий **2022a**.
- Программа для создания графических структур формул химических веществ **XDrawChem 1.10.2**.
- Редактор и визуализатор молекулярных структур **Avogadro 1.2.0**.
- Электронная периодическая система химических элементов **Kalzium 19.12.1**.
- Пакеты для работы с химическими данными и молекулярными вычислениями в графическом интерфейсе **Gabedit 2.5.1**.
- Химическая экспертная система **OpenBabel 2.4.1**.
- Программный пакет квантовой химии **OpenMolcas 21.10**.
- Библиотека для кристаллохимических вычислений и обработки соответствующих данных **spglib 1.16.1**.
- Пакет для вычислений электронных состояний в атомах и молекулах **libint 1.2.1**.
- Библиотека международных идентификаторов ИЮПАК **inchi 1.0.6**.

Драйверы устройств:

- Обновлены драйверы видеоадаптеров **Nvidia** до версии **510.60.02**.

- Обновлены драйверы для принтеров **Canon** (**в частности для BP311**).
- Драйверы для термопринтеров **Godex**.
- Собраны драйверы для Wi-Fi-адаптеров **MediaTek MT7961**, **RTL8812AU/21AU**, **RTL8814AU**, **RTL8188 EU/EUS**, **Edimax EW-7822ULC**.
- Драйвер сетевого адаптера **Huawei Hi1822**.
- Собраны драйверы речевого кодека **G.729** (**asterisk-g72x 1.4.3**) и драйверы телефонных карт потоков **Digium**, **Sangoma** (**dahdi-linux 2.11.1**).
- Обновлены и собраны пакеты для работы звуковой карты **Everest ESSX8336**.
- Драйвер преобразователя интерфейсов MOXA NPort **npreal2 5.1**.

Список изменений в РЕД ОС 7.3.3

РЕД ОС 7.3.3 является корректирующим релизом РЕД ОС версии 7.3 стандартной редакции. Дистрибутив собран на пакетной базе репозитория 7.3 и включает в себя пакеты последних версий со всеми исправлениями, улучшениями и обновлениями безопасности, накопленными с момента выпуска РЕД ОС 7.3.2. Все пользователи РЕД ОС 7.3 стандартной редакции могут обновиться до 7.3.3 через штатное обновление системы (**dnf update**), ядро Linux обновляется опционально (инструкция «Обновление ядра Linux до версии 6.1 в РЕД ОС 7.3»). Узнать подробнее об истории версий и релизов РЕД ОС можно в статье « Версии РЕД ОС и сроки поддержки».

Основные изменения в установочном образе РЕД ОС 7.3.3:

- Актуальная LTS-версия ядра Linux **6.1**.
- Среда рабочего стола MATE обновлена до версии **1.26**.
- Офисный пакет **LibreOffice** самой актуальной на сегодня версии **7.6.0**.
- По умолчанию подключен репозиторий **Яндекс.Браузера** для его установки и последующего обновления. Теперь установить Яндекс.Браузер на РЕД ОС можно простой командой **dnf install yandex-browser-stable** или нажав соответствующую кнопку в окне приветствия. Яндекс.Браузер был специальным образом собран под пакетную базу РЕД ОС и не использует внешние источники для загрузки кодеков - теперь используются кодеки из репозитория РЕД ОС.
- В установщике появилась опция «**ПО для образовательного процесса**», которая добавит в ОС “магазин приложений” (пакет redos-education) с программами, необходимыми в образовательном процессе – системы проектирования и черчения, геоинформационные системы, графические редакторы, программы для математических и химических вычислений, среды разработки, программы для работы с мультимедиа, словари, программа для мониторинга и управления компьютерным классом и многое другое. Теперь преподаватель сможет легко найти нужную программу, ознакомиться с ее описанием и установить на РЕД ОС нажатием одной кнопки, без помощи администратора.
- В дистрибутив интегрировано большое количество Wi-Fi-драйверов, что обеспечит работу Wi-Fi-адаптера на ноутбуке сразу после установки РЕД ОС.

Репозиторий РЕД ОС 7.3 с момента выпуска 7.3.2 обновился и пополнился следующими пакетами:

Пользовательское ПО:

- Инструмент для запуска Windows-приложений **Wine** обновлен до версии 8.2.
- Добавлен GUI-индикатор для Яндекс.Диска **yandex-disk-indicator 1.11**.
- В репозитории появились мини-игры – тетрис, сапер, судоку, шахматы и др.
- Добавлен менеджер ядер с возможностью просмотра имеющихся версий, установки и переключения между ними – **Kernel-Manager 0.1**.
- Обновлен инструмент виртуализации **VirtualBox** до версии **6.1.42**.
- Обновлен векторный графический редактор **Inkscape** до версии **1.2.2**.
- Обновлен просмотрщик и каталогизатор изображений **Pix** до версии **2.8.9**.
- Добавлен проигрыватель мультимедиа **DeaDBeef 1.9.4**.
- Добавлен инструмент записи с экрана в GIF-формат **Peek 1.5.1**.
- **Double Commander** обновлен до версии **1.0.3**.
- Добавлено средство конвертации изображений формата jpeg в ASCII **jp2a 1.1.1**.
- Добавлено ПО для передачи файлов с iPhone **ifuse 1.1.4**.
- Добавлен синтезатор речи **RHVoice 1.8.0** с общедоступными голосами.
- Добавлено средство запуска Android-приложений **Anbox**.
- Обновлена программа систематизации и ведения заметок **CherryTree** до версии **0.99.51**.
- Добавлена программа финансового учета **KmyMoney 5.1.3**.
- Добавлена программа просмотра диагностических изображений в формате DICOM **Weasis** (размещена в подключаемом репозитории, пакет **redos-3rdparty-weasis**).

Серверное и системное ПО:

- В репозиторий включен сервер и клиент системы централизованного управления информационной инфраструктурой **РЕД АДМ Стандартной редакции**.
- Обновлены **Samba** до версии **4.17.5** и **FreeIPA** до версии **4.10.1**.

- Обновлен сервер каталогов 389 Directory Server **389-ds-base** до версии **2.1.7**.
- Обновлён **Zabbix** до версии **6.4.2**.
- Обновлено ПО для инвентаризации и управления активами организации **GLPI** до версии **9.5.7**.
- Обновлено ПО для удаленного администрирования **Webmin** до версии **2.001** с поддержкой модуля **Disk Quotas**.
- Обновлена система полнотекстового поиска и анализа данных **OpenSearch** до версии **2.8.0**, которая является заменой общеизвестного ElasticSearch.
- Обновлен сервер для совместной работы **Sogo** до версии **5.8.0**.
- Добавлены системы мониторинга **Xymon 4.3.30** и **Prometheus 2.30.0**.
- Добавлены пакеты для мониторинга системы **prometheus-node_exporter 1.6.0**, экземпляров кластера PostgreSQL **prometheus-postgres_exporter 0.12.1** и Nginx **nginx-prometheus-exporter 0.11.0** в формате, доступном Prometheus.
- Добавлен инструмент для работы с зашифрованными Bitlocker разделами дисков **Dislocker 0.7.3**.
- Добавлены средство диагностики жестких дисков **WHDD 3.0.1** и инструмент восстановления данных **Ddrescue 1.27**.
- Обновлен RADIUS-сервер **Freeradius** до версии **3.0.26**.
- Добавлен инструмент для синхронизации данных **lsyncd 2.3.1**, обновлен **rsync** до версии **3.2.7**.
- Обновлены средства организации кластера **Coronsync** до версии **3.1.6** и **Pacemaker** до версии **2.1.4**.
- Обновлен брокер сообщений **RabbitMQ** до версии **3.11.18**.
- Обновлен **OpenVPN** до версии **2.6.0**.
- Обновлен **Network Manager** до версии **1.32.12** и добавлен пакет для настройки IPsec/IKEv2 **strongswan 1.6.0**.
- Добавлен сетевой сканирующий инструмент **Hping3**.
- Добавлено средство для маршрутизации TCP/IP **Bird 2.0.12**.
- Обновлено средство фильтрации сетевых пакетов **iptables** до версии **1.8.7**.
- Добавлен пакет для работы с DNS **dnstop 20140915**, обновлены **pdns** и **pdns-recursor** до версии **4.7.2**.
- Обновлен **Nginx** до версии **1.22.1**.
- Добавлен DHCP-сервер **Kea 1.9.8**.
- Добавлен инструмент автоматического запуска сеанса SSH **autossh 1.4b**.
- Обновлен пакет для управления доступом к удаленным каталогам и механизмам аутентификации **sssd** до версии **2.8.2**.
- Добавлено средство развертывания приложений Shiny **shinyproxy 2.6.1**.
- Обновлен контейнер сервлетов **Tomcat** до версии **9.0.74**.
- Добавлены пакеты для работы с TMP-модулем **tpm2-pkcs11 1.7.0** и **tpm2-tss-engine 1.2.0**.
- Обновлена конфигурация DNF – теперь при недоступности одного из репозиториев, операция продолжается с использованием остальных (опция **skip_if_unavailable**).

Средства контейнеризации и оркестрации:

- **Docker-ce** обновлен до **20.10.24**, **Docker-compose** обновлен до **2.11.2**.
- Создан общедоступный **реестр базовых образов РЕД ОС**.
- **Kubernetes** обновлен до версии **1.24.12** (по умолчанию в качестве среды выполнения контейнеров использует **containerd**).
- Добавлена среда выполнения контейнеров Kubernetes **cri-o 1.24.0**.
- Для возможности использования Docker в качестве среды выполнения контейнеров в Kubernetes, начиная с версии 1.24, был добавлен пакет **cri-dockerd 0.3.2**.
- **Podman** обновлен до **4.4**, **Podman-compose** обновлен до **1.0.6**.
- Добавлено ПО для работы с контейнерами **skopeo 1.8.0**.

Появился стек ПО от HashiCorp:

- **Consul 1.13.1** – инструмент для обнаружения и настройки множества различных сервисов.
- **Terraform 1.2.7** – инструмент для подготовки и управления облачной инфраструктурой.

- **Packer 1.8.3** – инструмент создания образов для виртуальных машин.
- **Nomad 1.3.3** – инструмент для управления контейнерами и не контейнерными приложениями.
- **Vault 1.11.2** – инструмент для хранения секретов и безопасного доступа к ним.

ПО для работы с базами данных:

- Добавлена резидентная СУБД **Tarantool 2.10.3**.
- Обновлены NoSQL-СУБД - **MongoDB** до версии **6.0.6**, **KeyDB** до версии **6.3.2**.
- Добавлена реляционная СУБД **PostgreSQL** версии **15**.
- Обновлена реляционная СУБД **MariaDB** до версии **10.11**, добавлен прокси-сервер для MySQL **proxysql 2.4.8**.
- Обновлены инструменты для работы кластера PostgreSQL и MariaDB - **Patroni** до версии **3.0.2** и **Galera** до версии **26.4.11**.
- Добавлен многопоточный пул подключений PostgreSQL и маршрутизатор запросов **Odyssey 1.3**.
- Добавлен пакет для работы с файлами OGR в PostgreSQL **ogr_fdw 1.1.3**.
- Добавлен инструмент мониторинга производительности PosgreSQL в реальном времени **pg_top 4.0.0**.
- Обновлены пакеты для поддержки географических объектов в PostgreSQL **PostGIS 3.2.2**.
- Добавлен инструмент управления резервным копированием и восстановлением кластеров баз данных PostgreSQL **pg_probackup 2.5.8**.
- Обновлено средство переноса данных из базы данных Oracle в базу данных PostgreSQL **ora2prg** до версии **23.2**.
- Добавлен планировщик заданий для баз данных PostgreSQL **pg_cron 1.5.2**.
- Обновлен пакет для объединения подключений, репликации и балансировки нагрузки PostgreSQL **pgpool-II 4.3.3**.

Средства разработки:

- Обновлена реализация Microsoft .NET Framework **Mono** до версии **6.12.0**.
- Обновлен инструмент для создания установочных образов **Lorax** до версии **38.6**.
- Появилась среда разработки для языка программирования R **RStudio 1.4.1717**.
- Обновлена среда разработки **Geany** до версии **1.38**.
- Появился инструмент для разработки интерфейсов GTK3 и GTK4 **Cambalache 0.10.3**.
- Обновлено средство автоматизации сборки из исходного кода **CMake 3.19.7**.
- Обновлен инструмент создания сетевых приложений **node.js** до версии **18.14.2**.
- Пересобран **Zenity** с дополнительной поддержкой **webkit**.

ПО для образования:

- Визуально-блочная событийно-ориентированная среда программирования для детей **Scratch 1.4.0.7**.
- Игра для развития памяти **Blinken 0.9.29** и игра по отгадыванию анаграмм **Kanagram 21.12.2**.
- Репетитор по математике **TuxMath 2.0.3**, репетитор набора текста для детей **TuxType2 1.8.1** и программа для рисования **TuxPaint 0.9.29**.

Драйверы устройств:

- Драйверы **NVIDIA** обновлены до версии **530.41.03**.
- Разработан пакет **nvidia-primus** для переключения между видеокартами **Intel** и **NVIDIA** на ноутбуках.
- Драйверы для поддержки МФУ **Pantum** размещены в подключаемом репозитории (пакет **redos-3rdparty-pantum**).
- Добавлен драйвер для поддержки принтеров GoDEX - **GoDEX-drivers-cups** версии **1.1.2**.
- Обновлено ПО для устройств сканирования **SANE** до версии **1.2.1**.
- Обновлено ПО для поддержки bluetooth-устройств **bluez** до версии **5.66**.
- Обновлен пакет драйверов для считывателей и смарт-карт **pcsc-lite-ccid** до версии **1.5.2**.

- Добавлен пакет для работы токенов по OpenID Connect **pam_oidc 0.0.5**.
- Добавлен драйвер для Wi-Fi-адаптеров **RTL8188FU**.

Список изменений в РЕД ОС 7.3.4

РЕД ОС 7.3.4 является корректирующим релизом РЕД ОС версии 7.3 стандартной редакции. Дистрибутив собран на пакетной базе репозитория 7.3 и включает в себя пакеты последних версий со всеми исправлениями, улучшениями и обновлениями безопасности, накопленными с момента выпуска **РЕД ОС 7.3.3**. Все пользователи РЕД ОС 7.3 стандартной редакции могут перейти на **7.3.4** штатным обновлением системы (`dnf update`). Узнать подробнее об истории версий и релизов РЕД ОС можно в статье « Версии РЕД ОС и сроки поддержки».

Обновление РЕД ОС 7.3.4 представлено в виде 3-х установочных образов:

- **Классический ISO-образ** РЕД ОС с тремя конфигурациями: “Рабочая станция”, “Сервер с графическим окружением” и “Сервер минимальный”.
- **LiveUSB-образ** (конфигурации “Рабочая станция”). Позволяет запустить систему без установки, опробовать ее в работе, и непосредственно из Live-режима установить систему на диск.
- **OEM-образ** (конфигурации “Рабочая станция”), для установки на диск без какой-либо предварительной настройки. Установщик делает автоматическую разбивку диска, пользователь root по умолчанию заблокирован. При первом запуске системы достаточно принять лицензионное соглашение, задать логин и пароль для пользователя (будет по умолчанию администратором) и приступить к работе с системой.

Основные изменения в установочном образе РЕД ОС 7.3.4:

- LTS-версия **ядра** Linux **6.1.52**.
- Исправлена проблема установки на программный **RAID**, обеспечена корректная установка на **Intel VROC**.
- Обновлена конфигурация **D N F** – теперь при удалении пакета не удаляются неиспользуемые зависимости (опция `clean_requirements_on_remove=false`).
- Набор компиляторов **GCC** обновлен до версии **11**.
- Браузер **Chromium** обновлен до версии **119**.
- Обновлены прочие пакеты в связи с исправлением ошибок и устранением уязвимостей.

Репозиторий:

- Появился **Foreman** версии **3.7** (находится в подключаемом репозитории http://repo.red-soft.ru/redos/7.3/x86_64/extras/foreman37-73/), а также версии **3.6**, **3.5**, **3.4** для возможности ступенчатого перехода с версии **3.3**.
- Обновлена версия **OpenSearch** до **2.11**.
- Появился **OpenJDK** версии **17**.
- Добавлен **OpenSSL** версии **3.2.0** (пакет **openssl3** - может быть установлен совместно с версией **1.1.1**).
- Драйверы **NVIDIA** обновлены до версии **535.113.01**.
- В пакет **nvidia-primus** добавлена графическая утилита для переключения видеокарт.
- Обновилась версия **GlusterFS** до **11.1**.
- Обновилась версия **Ceph** до **17.2.7**.

Список изменений в РЕД ОС 7.3.5

Опубликован обновленный установочный образ РЕД ОС 7.3 x86_64 (7.3.5). Основные изменения в установочном образе:

- **ядро Linux** обновлено до версии **6.1.110**, применены многие рекомендации ФСТЭК России для несертифицированных ОС, а также патчи безопасности, исправления и улучшения, разрабатываемые в рамках Технологического центра исследования безопасности ядра Linux при ИСП РАН;
- обновлен набор драйверов и прошивок **linux-firmware** до версии **20240709**;
- в хранилище корневых сертификатов добавлены TLS-сертификаты ТЦИ («Технического центра Интернет») с методами шифрования ECDSAи ГОСТ(пакет **ca-certificates-ru**). Подробнее про работу с сертификатами ТЦИ см. в нашей статье «Поддержка российских сертификатов безопасности»;
- обновлено графическое окружение **MATE** до версии **1.28**;
- обновлен браузер **Chromium** до версии **128**;
- обновлен офисный пакет **Thunderbird** до версии **115.15.0**;
- менеджер входа **GDM** (используемый в MATE и GNOME) доработан для корректного отображения длинных имен пользователей (больше 25 символов);
- обновлено оформление приветственной страницы браузера (file:///usr/share/doc/HTML/index.html);
- исправлены известные ошибки, связанные с установкой и работой системы.

Важные обновления в репозитории:

- обновлены драйвера **NVIDIA** до версии **555.58**;
- добавлена программа **EnvyControl 3.4.0** для управления режимами работы гибридной графики;
- добавлена LTS-версия **Zabbix 7** (пакет **zabbix7-lts**);
- добавлены версии PHP 8.2 и 8.3.

Прочие обновления в репозитории:

Пользовательское ПО:

- добавлен **Xournalpp** версии **1.2.2**;
- добавлен **Lutris** версии **0.5.17**;
- добавлен **Yate** версии **6.1.1**;
- добавлен **Diff-so-fancy** версии **1.4.4**;
- добавлен **Loganalyzer** версии **4.1.13**;
- добавлен **Mumble** версии **1.4**;
- обновлен **Firefox** до версии **115.15.0**;
- обновлен **Cherrytree** до версии **1.1.4**;
- обновлен **VLC** до версии **3.0.21**.

Специализированное ПО:

- Для радиоэфира:
  - обновлен **SoapySDR** до версии **0.8.1**;
  - обновлен **CubicSDR** до версии **0.2.7**.
- Для работы с геоданными:
  - добавлен **Fiona** версии **1.9.6**;
  - обновлен **Gdal** до версии **3.8.2**;
  - обновлен **Proj** до версии **9.4.1**.
- Для разработки электрических схем и печатных плат:

    - обновлен **Kicad** до версии **8.0.1**.
- Для работы с программаторами:
    - обновлен **Imsprog** до версии **1.4.1**.
- Для работы с интерактивными досками:
    - обновлен **OpenBoard** до версии **1.7**.
- Для моделирования архитектуры предприятия, её анализа и визуализации:
    - добавлен пакет **Archi** версии **5.2.0**.

Системное и серверное ПО:

- обновлен **Systemd** до версии **249.17**;
- обновлен **Rsyslog** до версии **8.2102.0**;
- обновлен **Sudo** до версии **1.9.15p5**;
- обновлен **Nftables** до версии **1.0.9**;
- обновлен **OpenSSL** до версии **1.1.1w**;
- обновлен **Etckeeper** до версии **1.18.21**;
- обновлены **Nvme-cli** до версии **2.7.1** и **Libnvme** до версии **1.7.1**;
- обновлены **libburn** до версии **1.5.6** и **libisofs** до версии **1.5.6**;
- обновлен **Atop** до версии **2.10.0**;
- обновлен **Opentelemetry-collector-contrib** до версии **0.100.0**;
- обновлен **Mercurial** до версии **6.2.3**;
- обновлен **Tmux** до версии **3.4**;
- обновлен **Syncthing** до версии **1.27.9**;
- обновлен **Tuned** до версии **2.22.1**;
- обновлен **Stress-ng** до версии **0.17.08**;
- обновлен **Loginfo** до версии **0.19**;
- обновлены **Bash** до версии **5.2.15** и **Bash-completion** до версии **2.14**;
- обновлен **xorg-x11-server** до версии **1.20.14**;
- обновлен **Hwdata** до версии **0.383**;
- обновлен **Protobuf** до версии **3.19.6**;
- обновлен **Nethogs** до версии **0.8.7**;
- обновлен **Keepalived** до версии **2.3.1**;
- обновлен **OpenvSwitch** до версии **2.17.10**;
- обновлен **Debmirror** до версии **2.39**;
- обновлен **ZFS** до версии **2.1.14**;
- обновлен **pymemcache** до версии **4.0.0**;
- обновлен **rtslib** до версии **2.1.76**;
- обновлен **Supervisor** до версии **4.2.5**;
- обновлен **PowerShell** до версии **7.4.1**;
- обновлен **Authselect** до версии **1.5.0**;
- обновлен **Etcd** до версии **3.5.15**;
- добавлен **MyConnector** версии **2.5.2**;
- обновлен **Grafana** до версии **11.1.3**;
- добавлен **Loki** версии **2.9.4**;

- добавлен **Promtail** версии **2.9.4**;
- добавлен **uCarp** версии **1.5.2**;
- добавлен **Kamailio** версии **5.5.2**;
- добавлен **Ocsinventory** версии **2.12.1**;
- обновлен **NFS-Ganesha** до версии **5.7**;
- обновлен **PowerDNS** до версии **4.8.3**;
- обновлен **Nginx** до версии **1.26.2** ;
- обновлен **BIND** до версии **9.18.28**;
- обновлен **dhcp** до версии **4.4.3**;
- обновлен **IPA** до версии **4.10.3**;
- обновлен **FreeRDP** до версии **3.4.0**;
- обновлен **Prometheus** до версии **2.49.1**;
- обновлен **Openfire** до версии **4.7.5**;
- обновлен **OpenSearch** до версии **2.15.0**;
- обновлен **Clevis** до версии **20**;
- обновлен **Salt** до версии **3006.8**;
- обновлен **FreeRADIUS** до версии **3.2.3**;
- обновлен **DRBD** до версии **9.22.0**;
- обновлен **Rear** до версии **2.7**;
- добавлен **OpenVAS** версии **22.7.9**;
- добавлены **Trufflehog** версии **3.68.4** и **detect-secrets** версии **1.4.0**;
- обновлен **GnuTLS** до версии **3.6.16**;
- обновлен **Vault** до версии **1.17.5**;
- обновлен **Keepassxc** до версии **2.8.7**;
- обновлен **Libxcrypt** до версии **4.4.36**;
- обновлен **OpenScap** до версии **1.3.9**;
- обновлен **Fail2Ban** до версии **1.0.2**.

Средства виртуализации и контейнеризации:

- обновлен **QEMU** до версии **7.2.14**;
- обновлен **Cloud-init** до версии **23.2**;
- обновлен **Containerd** до версии **1.7.17**;
- обновлен **Lxd** до версии **4.24**;
- обновлен **Lxc** до версии **4.0.12**;
- обновлен **Shinyproxy** до версии **3.1.1**.

ПО для работы с базами данных:

- добавлены версии **Firebird 4** и **5** (опубликованы в extras-репозиториях, подключаются пакетами **redos-firebird4-release** и **redos-firebird5-release**);
- обновлен **PostgreSQL** до версии **16.4**;
- добавлены и обновлены вспомогательные пакеты для **PostgreSQL**:
  - **TimescaleDB 2.14.12**;
  - **Patroni 3.2.2**;
  - **Stolon 0.17.0**;

    - **Pgloader 3.6.9**;
    - **Pgpool-II 4.5.2**;
    - **Plpgsql_check 2.7.6**.
- обновлен пакет **postgresql-1c** до версии **14.15**;
- обновлен **KeyDB** до версии **6.3.4**;
- обновлен **MongoDB** до версии **7.0.8**;
- обновлен **Cassandra** до версии **4.1.5**;
- обновлен **DBeaver** до версии **24.0.2**.

Средства разработки:

- обновлен **Git** до версии **2.44.1**;
- добавлен **Thefuzz** версии **0.19.0**;
- добавлен **Drf-yasg** версии **1.21.5**;
- добавлен **Flux** версии **0.195.1** и **Influxdb** версии **1.11.5**;
- добавлен **Loguru** версии **0.7.2**;
- добавлен **Or-tools** версии **9.0**;
- добавлен **Upx** версии **4.2.4**;
- обновлен **Mock** до версии **2.1**;
- обновлен **Codium** до версии **1.91.1**;
- обновлен **Nomad** до версии **1.8.3**;
- обновлен **Packer** до версии **1.11.1**;
- обновлен **NodeJS** до версии **18.20.4**;
- обновлен **OpenCV** до версии **4.5.0**;
- обновлен **Liborc** до версии **1.7.9**;
- обновлены **Asciidoc** до версии **10.2.0** и **Asciidoctor** до версии **2.0.23**;
- обновлен **Rstudio** до версии **2024.04.2+764**;
- обновлен **Golist** до версии **0.10.4**;
- обновлен **Lld** до версии **17.0.6**;
- обновлен **Clang** до версии **17.0.6**;
- обновлены **Rustdesk** до версии **1.3.0** и **Rustdesk-server** до версии **1.1.11**.

Список изменений в РЕД ОС 8

РЕД ОС 8 является новой мажорной версией РЕД ОС, выпущенной в феврале 2024 года. Узнать подробнее об истории версий и релизов РЕД ОС можно в статье «Версии РЕД ОС и сроки поддержки».

Обновиться до РЕД ОС 8 возможно с версии 7.3 без переустановки системы. Инструкция предоставляется пользователям с действующей ТП.

Описание изменений

Ядро Linux:

- LTS-версия 6.6.

Пользовательские окружения:

- В установочном образе 3 окружения:
  - **MATE 1.26** (с оконным менеджером **Marco**);
  - **KDE Plasma 5**;
  - **GNOME 44**.
- В качестве DM используются:
  - **GDM** (для MATE и GNOME)
  - **SDDM** (для KDE).
- По умолчанию все окружения работают на графическом сервере **XOrg**. Графический сервер **Wayland** доступен в репозитории для **GNOME** и **KDE**. Инструкция по установке доступна по ссылке.

Пользовательские окружения предоставляют специальные возможности:

- Экранный диктор для чтения текста с экрана;
- Высококонтрастные темы оформления рабочего стола;
- Экранная лупа, клавиатура и другие функции доступности.

Узнать обо всех специальных возможностях РЕД ОС можно в разделе «Специальные возможности РЕД ОС».

В MATE реализованы 4 компоновки панелей на выбор пользователя:

- Однопанельный интерфейс в стиле “Windows XP” (идет по умолчанию, условное обозначение **ventanaXP**);
- Однопанельный интерфейс в стиле “Windows 7” (**ventana7**);
- Интерфейс с верхней и Dock-панелью в стиле “macOS” (**vespanamaca**);
- Двухпанельный интерфейс в стиле “GNOME 2” (**oldschool**).

В MATE реализован режим Киоска.

При включенном режиме Киоска пользователю становятся недоступными:

- запуск программ с графическим интерфейсом, кроме явно разрешенных (ярлыки таковых приложений находятся на Рабочем столе),
- выполнение сценариев на любом языке при явном их запуске пользователем,
- запуск на выполнение файлов с установленным битом SUID,
- изменение свойств и содержимого главной панели на Рабочем столе,
- изменение содержимого Рабочего стола (создание/удаление/изменение ярлыков, создание/удаление/изменение иных файлов),
- автоматическое монтирование внешних накопителей,
- смена виртуальной консоли по сочетанию клавиш Ctrl+Alt+Fn.

Узнать обо всех возможностях Киоска в РЕД ОС можно в статье «Режим Киоска в РЕД ОС».

Основные компоненты системы:

- Пакетный менеджер **DNF** версии **4.17.0**.
- Система принудительного контроля доступа **SELinux** версии **3.4**.

- Система управления службами **Systemd** версии **251.13**.
- Криптографическая библиотека **OpenSSL** версии **3.1.4**.
- Межсетевой экран **Firewalld** версии **2.0.0** (вместо **iptables** в 7.3).
- Сервер времени **Chrony** версии **4.1** (вместо **ntp** в 7.3).
- Звуковой сервер **PipeWire** версии **1.0.3** (вместо **PulseAudio** в 7.3).

Диск и установщик:

- Разметка диска по умолчанию “**Стандартная**” (вместо **LVM** в 7.3).
- Во всех конфигурациях предустановлена утилита **loginfo** (для сбора диагностической информации и передачи в ТП).
- В конфигурациях с графическим окружением предустановлены утилиты работы с доменом (**join-to-domain**, **connectfolder**, **share_directory**, **smbpass**) и с USB-интерфейсами (**usb_rules**).
- В конфигурациях с графическим окружением по умолчанию устанавливаются офисный пакет **LibreOffice**, браузер **Chromium** (с поддержкой криптографических алгоритмов ГОСТ и выключенной синхронизацией с сервисами Google), почтовый клиент **Thunderbird**. На этапе установки ОС можно отказаться от установки этих компонент (сняв галочку).
- Предустановлены сертификаты Минцифры России.
- По умолчанию подключены репозитории **Яндекс.Браузер** и **Р7 Офис**.

Версии ПО в РЕД ОС 8

Средства разработки:

- glibc - 2.36;
- gcc - 12.2.1;
- clang/llvm - 11, 12, 13, 14, 15;
- python - 2.7, 3.8, 3.9, 3.10, 3.11 (по умолчанию 3.11);
- openjdk (java) - 1.8, 11, 17, 21 (все LTS);
- dotnet - 6.0, 7.0, 8.0;
- php - 8.1.24;
- mono - 6.12.0;
- perl - 5.36.0;
- rust - 1.72.0;
- golang - 1.21.6.

Средства виртуализации:

- qemu - 8.2.0;
- libvirt - 9.7.0.

Средства контейнеризации:

- docker - 24.0.7;
- docker-compose - 2.11.2;
- podman - 4.8.1;
- podman-compose - 1.0.6;
- cri-o - 1.28.2;
- containerd - 1.6.24.

Базовые Docker-образы РЕД ОС 8 представлены в реестре **registry.red-soft.ru/ubi8**.

Средства оркестрации:

- kubernetes - 1.28.3.

Контроллеры домена:

- samba - 4.19.0;

- freeipa - 4.10.1.

СУБД:

- firebird - 4.0;
- mariadb - 10.11 (LTS);
- postgresql - 12, 13, 14, 15, 16 (все LTS).

Системы управление конфигурациями:

- puppet 8.3;
- ansible 8.4.

Офисный пакет:

- libreoffice - 7.6.

Браузеры:

- chromium - 120 (выключена синхронизация с сервисами Google);
- firefox - 102.15.0.

Почтовые клиенты:

- thunderbird - 102.15.0;
- evolution - 3.50.2.

Менеджеры приложений:

- wine - 9.0;
- snapd - 2.58.3;
- flatpak - 1.14.4.

Список изменений в РЕД ОС 8 (декабрь 2024)

Опубликован обновленный установочный образ РЕД ОС 8 x86_64. Основные изменения в установочном образе:

- **ядро Linux** обновлено до версии **6.6.51**, применены многие рекомендации ФСТЭК России для несертифицированных ОС, а также патчи безопасности, исправления и улучшения, разрабатываемые в рамках Технологического центра исследования безопасности ядра Linux при ИСП РАН;
- обновлен набор драйверов и прошивок **linux-firmware** до версии **20240513**;
- в хранилище корневых сертификатов добавлены TLS-сертификаты ТЦИ («Технического центра Интернет») с методами шифрования ECDSAи ГОСТ(пакет **ca-certificates-ru**). Подробнее про работу с сертификатами ТЦИ см. в нашей статье «Поддержка российских сертификатов безопасности»;
- обновлены графические окружения: **MATE 1.28**, **KDE Plasma 5.27.11** и **GNOME 45**;
- обновлен **OpenSSH** до версии **9.9p1**;
- обновлен браузер **Chromium** до версии **128**;
- обновлен почтовый клиент **Thunderbird** до версии **115.15.0**;
- обновлен офисный пакет **LibreOffice** до версии **24.2.4**;
- в конфигурации для рабочих станций по умолчанию входит программа сканирования **NAPS2**;
- доработан менеджер входа в систему **SDDM** (используемый в KDE) – позволяет запоминать и отображать доменных пользователей, а также менять пароль пользователя при входе в систему;
- менеджер входа **GDM** (используемый в MATE и GNOME) доработан для корректного отображения длинных имен пользователей (больше 25 символов);
- обновлено оформление приветственной страницы браузера (file:///usr/share/doc/HTML/index.html);
- обновлен дизайн установщика **Anaconda**;
- исправлены известные ошибки, связанные с установкой и работой системы.

Важные обновления в репозитории:

- обновлены драйвера **NVIDIA** до версии **555.58**;
- добавлена программа Envycontrol 3.4.0 для управления режимами работы гибридной графики;
- добавлена LTS-версия **Zabbix 7** (пакет **zabbix7-lts**);
- добавлены версии PHP 8.2 и 8.3;
- обновлен **Docker** до версии **27.2.1**;
- обновлен **Podman** до версии **5.2**.

В репозитории РЕД ОС 8 x86_64 появилось **ядро реального времени** (realtime-ядро). Версия ядра **6.6.52** собрана с патчем **PREEMPT-RT**, обеспечивающим «мягкое реальное время». Подробнее про установку realtime-ядра в РЕД ОС 8 см. в нашей статье « Установка realtime-ядра в РЕД ОС 8».

Прочие обновления в репозитории:

Пользовательское ПО:

- добавлен **Wine** версии **9.17** (в extras-репозитории, подключается пакетом **wine-unstable-release**);
- добавлен **Nmonchart** версии **42;**
- добавлен **Mumble** версии **1.4.287**;
- добавлен **Fastfetch** версии **2.16.0**;
- обновлен **Remmina** до версии **1.4.35**;
- обновлен **Blender** до версии **4.1.1**;
- обновлен **Firefox** до версии **115.15.0**;
- обновлен **7-Zip** до версии **24.07**;
- обновлен **OBS-Studio** до версии **30.1.0**;
- обновлен **VLC** до версии **3.0.21**;

- обновлен **Krita** до версии **5.2.2**;
- обновлен **Shotcut** до версии **24.02.29**;
- обновлен **Zathura** до версии **0.5.4**;
- обновлен **Gajim** до версии **1.7.3**;
- обновлен **Lutris** до версии **0.5.17**;
- обновлен **Recoll** до версии **1.37.5**;
- обновлен **GIMP** до версии **2.10.38**;
- обновлен **Mangohud** до версии **0.7.1**;
- обновлен **Vips** до версии **8.15.2**;
- обновлен **Cherrytree** до версии **1.1.4**.

Специализированное ПО:

- Для радиоэфира:
  - обновлен **SoapySDR** до версии **0.8.1**.
- Для работы с геоданными:
  - добавлен **Fiona** версии **1.9.6**;
  - добавлен **Proj** версии **9.4.1**;
  - обновлен **Qgis** до версии **3.34.7**;
  - обновлен **Gdal** до версии **3.8.2**.
- Для разработки электрических схем и печатных плат:
  - обновлен **Kicad** до версии **8.0.1**.
- Для черчения и проектирования:
  - обновлен **Librecad** до версии **2.2.0.2**.
- Для работы с программаторами:
  - обновлен **Imsprog** до версии **1.4.1**.

Системное и серверное ПО:

- обновлен **Systemd** до версии **251.20**;
- обновлен **OpenVPN** до версии **2.6.11**;
- обновлен **Rsyslog** до версии **8.2310.0**;
- обновлен **Sudo** до версии **1.9.15p5**;
- обновлен **Nftables** до версии **1.0.9**;
- обновлен **OpenSSL** до версии **3.1.5**;
- обновлен **K3b** до версии **23.08.5**;
- обновлен **Dconf-editor** до версии **45.0.1**;
- обновлен **Realmd** до версии **0.17.1**;
- обновлен **p11-kit** до версии **0.25.3**;
- обновлен **Irqbalance** до версии **1.9.2**;
- обновлен **GdkPixbuf** до версии **2 2.42.11**;
- обновлен **Libheif** до версии **1.17.5**;
- обновлен **OpenTelemetryCollectorContrib** до версии **0.100.0**;
- обновлен **Tmux** до версии **3.4**;

- обновлен **Syncthing** до версии **1.27.9**;
- обновлен **Tuned** до версии **2.22.1**;
- обновлен **Stress-ng** до версии **0.17.08**;
- обновлен **Bash-completion** до версии **2.14**;
- обновлен **Xorg-x11-server** до версии **1.20.14**;
- обновлен **Hwdata** до версии **0.383**;
- обновлен **Protobuf** до версии **3.19.6**;
- обновлен **NetHogs** до версии **0.8.7**;
- обновлен **Keepalived** до версии **2.3.1**;
- обновлен **OpenvSwitch** до версии **2.17.10**;
- обновлен **PyMemcache** до версии **4.0.0**;
- обновлен **Supervisor** до версии **4.2.5**;
- обновлен **PowerShell** до версии **7.4.1**;
- обновлен **Authselect** до версии **1.5.0**;
- обновлен **Etcd** до версии **3.5.15**;
- добавлены **Stork-server** версии **1.17.0** и **Stork-agent** версии **1.17.0**;
- добавлен **Kamailio** версии **5.5.7**;
- добавлен **Ocsinventory** версии **2.12.1**;
- добавлен **Tomcat-native** версии **1.29**;
- добавлен **PostfixAdmin** версии **3.3.13**;
- добавлен **Apache-jmeter** версии **5.6.3**;
- добавлен **Fprobe** версии **1.2**;
- обновлен **Arpwatch** до версии **3.3**;
- обновлен **FreeRDP** до версии **3.4.0**;
- обновлен **Clevis** до версии **20**;
- обновлен **FreeRADIUS** до версии **3.2.3**;
- обновлен **Grafana** до версии **11.1.3**;
- обновлен **PCP** до версии **6.2.0**;
- обновлен **Collectd** до версии **5.12.0**;
- обновлен **Prometheus** до версии **2.49.1**;
- обновлен **MTR** до версии **0.95**;
- обновлен **Haproxy** до версии **3.0.4**;
- обновлен **Netmiko** до версии **4.3.0**;
- обновлен **GLPI** до версии **10.0.16** и связанные пакеты;
- обновлен **Nginx** до версии **1.26.2**;
- обновлен **BIND** до версии **9.18.28**;
- обновлен **SpamAssassin** до версии **4.0.1**;
- обновлен **OpenSearch** до версии **2.15.0**;
- обновлен **Vip-manager** до версии **2.5.0**;
- обновлен **ExaBGP** до версии **4.2.21**;
- обновлен **Salt** до версии **3006.8**;
- обновлен **Openfire** до версии **4.7.5**;
- обновлен **MinIO** до версии **20240803T043323Z**;
- добавлены **Trufflehog** версии **3.68.4** и **detect-secrets** версии **1.4.0**;

- добавлены **LAPS4-client** и **LAPS4-runner** версии **1.8.0**;
- обновлен **XCA** до версии **2.7.0**;
- обновлен **Stunnel** до версии **5.69**;
- обновлен **KeePassXC** до версии **2.7.8**;
- обновлен **Fail2Ban** до версии **1.0.2**;
- обновлен **GnuTLS** до версии **3.6.16**;
- обновлен **ButterflyBackup** до версии **1.12**;
- обновлен **Vault** до версии **1.17.5**.

Средства виртуализации и контейнеризации:

- обновлен **QEMU** до версии **8.2.7**;
- обновлен **Cloud-init** до версии **23.2**;
- обновлен **Containerd** до версии **1.7.17**;
- обновлен **Lxd** до версии **5.14**;
- обновлен **ShinyProxy** до версии **3.1.1**;
- обновлен **gns3-server** до версии **2.2.46**.

ПО для работы с базами данных:

- добавлены версии **Firebird 3** и **5** (опубликованы в extras-репозиториях, подключаются пакетами **redos-firebird3-release** и **redos-firebird5-release**);
- обновлен **PostgreSQL** до версии **16.4**;
- добавлены и обновлены вспомогательные пакеты для **PostgreSQL**:
    - **TimescaleDB 2.14.12**;
    - **Patroni 3.2.2**;
    - **Stolon 0.17.0**;
    - **Pgloader 3.6.9**;
    - **Pgpool-II 4.5.2**;
    - **Plpgsql_check 2.7.6**.
- обновлен пакет **postgresql-1c** до версии **14.15**;
- обновлен **KeyDB** до версии **6.3.4**;
- обновлен **MongoDB** до версии **7.0.8**;
- обновлен **DBeaver** до версии **24.0.2**.

Средства разработки:

- обновлен **Git** до версии **2.44.1**;
- добавлен **Drf-yasg** версии **1.21.5**;
- добавлен **Flux** версии **0.195.1** и **Influxdb** версии **1.11.5**;
- добавлен **Loguru** версии **0.7.2**;
- добавлен **Or-tools** версии **9.0**;
- добавлен **Upx** версии **4.2.4**;
- добавлен **Clang** версии **17.0.6**;
- обновлен **DotNet** до версии **8.0.108**;
- обновлен **MuParser** до версии **2.3.4**;

- обновлен **OpenCV** до версии **4.6.0**;
- обновлен **BeIr** до версии **5.2.45**;
- обновлен **Libdxfrw** до версии **1.1.0**;
- обновлен **RustDesk** до версии **1.3.0** и **RustDesk Server** до версии **1.1.11**;
- обновлен **Crudini** до версии **0.9.5**;
- обновлен **GStreamer** до версии **1.22.12**;
- обновлен **RubyGem-thor** до версии **1.2.2**;
- обновлен **Codium** до версии **1.91.1**;
- обновлен **Nomad** до версии **1.8.3**;
- обновлен **Packer** до версии **1.11.1**;
- обновлен **G2Plot** до версии **2.4.31**;
- обновлен **Flake8** до версии **7.1.1**;
- обновлен **Rstudio** до версии **2024.04.2+764**;
- обновлен **Lld** до версии **17.0.6**.

Список пользовательского ПО

В данном разделе представлен список пользовательского программного обеспечения, который доступен для установки и использования в репозитории РЕД ОС 7.3.

В файле указано описание каждого пакета, наименование пакетов для установки и использования, а также добавлены ссылки на сайты проектов.

Список пользовательского программного обеспечения

Информацию о группах пакетов, входящих в установочный диск для конфигурации «Рабочая станция», можно просмотреть здесь.

Список серверного ПО

Серверное программное обеспечение (Серверное ПО) – специальные приложения, предназначенные для предоставления определенных услуг и обеспечивающие их выполнение. К Серверному ПО относятся программы, предоставляющие пользователю различные услуги по обработке, передаче, хранению информации (серверы протоколов, почтовые серверы, серверы приложений, серверы печати и прочие).

По сертификату технической поддержки для конфигурации "Сервер" оказывается помощь для всех программных продуктов, которые входят в состав РЕД ОС.

По сертификату технической поддержки для конфигурации "Рабочая станция" не оказывается помощь по серверному ПО. За исключением вопросов, которые относятся к настройке клиентских приложений для серверного ПО.

Консультация сотрудников технической поддержки для пользователей без сертификата технической поддержки для сервера по вопросам, связанными с серверным ПО, рассматривается службой технической поддержки в индивидуальном порядке и зависит от конфигурации оборудования АРМ.

Список серверного программного обеспечения

Информацию о группах пакетов, входящих в установочный диск для конфигурации «Сервер», можно просмотреть здесь.

Оборудование, совместимое с РЕД ОС

Поддерживаемые процессорные архитектуры и чипсеты
Поддерживаемые звуковые карты
Поддерживаемые видеокарты
Поддерживаемые сетевые карты
Совместимое печатающее оборудование
Поддерживаемое сканирующее оборудование
Совместимое оборудование и программное обеспечение
Дополнительно

Примечание.

Составить единый список поддерживаемого в РЕД ОС оборудования невозможно, так как производителей и моделей оборудования очень много.

В этом разделе Базы знаний РЕД ОС можно найти информацию о поддержке различных устройств аппаратного обеспечения и периферии.

Некоторые способы определения поддержки оборудования операционной системой перечислены в наших инструкциях:

- для РЕД ОС 7.3 — «Поддержка оборудования в ядре ОС»;
- для РЕД ОС 8 — «Поддержка оборудования в ядре ОС».

Поддерживаемые процессорные архитектуры и чипсеты

Операционная система РЕД ОС функционирует на электронно-вычислительных машинах с процессорной архитектурой и чипсетами под них:

- x86 и x86_64 Intel;
- AMD;
- aarch64.

Поддерживаемые звуковые карты

Список звуковых карт, поддерживаемых РЕД ОС:

- Производитель Realtek – все модели;
- Производитель intel - ICH southbridge AC97 audio – все модели.

Поддерживаемые видеокарты

Доступные драйверы для видеокарт для РЕД ОС можно посмотреть на сайтах производителей (следует выбирать rpm-совместимые ОС. Такие, как, например, RedHat/RHEL/Centos/Oracle/Linux 64bit):

- https://www.amd.com/ru/graphics/radeon-rx-graphics;
- https://www.nvidia.com/Download/index.aspx;
- https://www.intel.ru/.

Поддерживаемые сетевые карты

Со списком поддерживаемых сетевых карт для РЕД ОС можно ознакомиться на странице «Список сетевых карт, поддерживаемых РЕД ОС».

Совместимое печатающее оборудование

Списки совместимого с РЕД ОС печатающего оборудования приведены на данных страницах:

- Печатающие устройства производства Alps, Anitech, Apollo, Apple
- Печатающие устройства производства Brother
- Печатающие устройства производства Canon
- Печатающие устройства производства CIAAT, Citizen, Compaq
- Печатающие устройства производства Dai Nippon, DatamaxONeil, DEC, Dell
- Печатающие устройства производства Epson
- Печатающие устройства производства Fuji, Genicom
- Печатающие устройства производства Gestetner
- Печатающие устройства производства Heidelberg, Hitachi,HP
- Печатающие устройства производства IBM, Imagen, Imagistics, infoPrint
- Печатающие устройства производства Kodak, Konica Minolta
- Печатающие устройства производства Kyocera
- Печатающие устройства производства Lanier
- Печатающие устройства производства Lexmark
- Печатающие устройства производства Minolta, Mitsubishi, NEC
- Печатающие устройства производства NRG
- Печатающие устройства производства Oce, Oki
- Печатающие устройства производства Olivetti, Olympus, Panasonic, PCPI, QMS, Raven
- Печатающие устройства производства Ricoh
- Печатающие устройства производства Samsung
- Печатающие устройства производства Savin
- Печатающие устройства производства Sharp
- Печатающие устройства производства Seiko, Shinko, Sinfonia, SiPix, Sony
- Печатающие устройства производства Tally, Tektronix, Texas Instruments, Toshiba
- Печатающие устройства производства Xante, Xerox
- Печатающие и сканирующие устройства производства Hewlett-Packard

Списки совместимых устройств для **РЕД ОС** версии **7.3 и выше** также можно посмотреть на данных сайтах:

- http://www.openprinting.org/drivers
- http://www.openprinting.org/printers
- https://www.openprinting.org/driver/Postscript/
- https://www.brother.ru/printers/all-printers
- https://www.canon.ru/printers/
- https://epson.ru/catalog/printers/
- https://www8.hp.com/ru/ru/printers/view-all-printers.html
- https://www.orgprint.com/printeri/IBM/
- https://prophotos.ru/devices/printer/kodak
- https://www.kyoceradocumentsolutions.ru/index/products/printers.html
- https://www.lanier.com/en/products/pl/equipment-printers-and-copiers/_/N-1q
- https://www.lexmark.com/en_us.html
- https://oce.ru/
- https://pro.sony/ru_UZ/products/medical-printers

Поддерживаемое сканирующее оборудование

Поддерживаемое сканирующее оборудование можно посмотреть на странице «Сканеры, поддерживаемые РЕД ОС».

Совместимое оборудование и программное обеспечение

Ознакомиться со списком оборудования и программным обеспечением, совместимость с которым официально подтверждена, можно на нашей странице «Совместимое оборудование и программное обеспечение».

Дополнительно

Дополнительные списки ресурсов, на которых можно проверить совместимость различных аппаратных компонентов с Linux, можно посмотреть на http://wiki.opennet.ru/HardwareCompatibilityLists.

Печатающее и сканирующее оборудование, совместимое с РЕД ОС (из практики)

Производитель	Модель
BROTHER	HL-l5100dn
	HL-L2340DWR
	QL-800
CANON	6020
	MF210
	MF211
	i-Sensys MF4410
EPSON	L566
	M1170
Godex	Godex EZ-DT-4 (пакет *GoDEX-drivers-cups*)
HP	LaserJet mfc m227 sdn
	LaserJet professional 1102
	Color LaserJet 3600
	LaserJet 2015
	LaserJet Pro M225rdn
	LaserJet Pro M426fdn
	LaserJet Pro M227sdn
	LaserJet 1522
	HP1102
KONICA-MINOLTA	c658
KYOCERA	FS-1120d
	TASKaifa 4501i
	M4132idn
LEXMARK	X862de
PANTUM	2200
	M6550NW
	BM5100adn
	P3010D
	M6700
RICOH	SP210
SAMSUNG	M2020
	SCX-3400
XEROX	Phaser 3020

Печатающее и сканирующее оборудование, несовместимое с РЕД ОС (из практики)

Производитель	Модель
Avision	AD130
Brother	DCP-1612WR
	7440nr
Canon	image Runner 2530i
	lbp 6030B
	MF3228
Custom	TG2480
Fujitsu	fi-5750c
	fi-6230
	fi-7700s
	fi-6770
HP	LaserJet P2055d
Kodak	Scanmate i1150
Toshiba	E-2505h
	E-STUDIO5018A
	E-Studio 257
Xerox	Phaser 3100
	Work Centre 5222SD

Сканеры, поддерживаемые РЕД ОС

Производитель	Модель
Abaton	Scan 300/GS
Across Technologies	FS-1130
Adlib	JetScan630
AGFA	Focus Color
AGFA	Focus Color Plus
Agfa	Arcus II
Agfa	StudioScan
Agfa	StudioScan II
Agfa	StudioScan IIsi
Agfa	Studiostar
Agfa	DuoScan
Agfa	Snapscan Touch
AGFA	SnapScan
AGFA	SnapScan 300
AGFA	SnapScan 310
AGFA	SnapScan 600
AGFA	Arcus 1200
AGFA	SnapScan 1236s
AGFA	SnapScan 1236u
AGFA	SnapScan 1212U
AGFA	SnapScan 1212U_2
AGFA	SnapScan e10
AGFA	SnapScan e20
AGFA	SnapScan e25
AGFA	SnapScan e26
AGFA	SnapScan e40
AGFA	SnapScan e42
AGFA	SnapScan e50
AGFA	SnapScan e52
Ambir	Visigo A4
Apple	Apple Scanner
Apple	OneScanner
Apple	Color OneScanner
Apple	Color OneScanner 600/27
Aries	Scan-It Pro 4800
Artec/Ultima	AT3
Artec/Ultima	A6000C
Artec/Ultima	A6000C PLUS
Artec/Ultima	AT6
Artec/Ultima	AT12
Artec/Ultima	AM12S
Artec/Ultima	E+ 48U
Artec/Ultima	E+ Pro
Artec/Ultima	AS6E

Производитель	Модель
Artec/Ultima	Ultima 2000
Artec/Ultima	Ultima 2000 e+
avision	AV120
avision	AV121
avision	AV122
avision	AV122 C2
avision	AV210
avision	AV210
avision	AV210C2
avision	AV210C2-G
avision	AV210D2+
avision	AV220
avision	AV220C2
avision	AV220D2
avision	AV220+
avision	AV220C2-G
avision	AV220C2-B
avision	AV220-G
avision	AV610
avision	AV600U Plus
avision	AV610C2
avision	AM3000 Series
avision	DS610CU Scancopier
avision	AV620CS
avision	AV620CS Plus
avision	AV630CS
avision	AV6240
avision	AV600U
avision	AV820C
avision	AV820C Plus
avision	AV830C
avision	AV3200C
avision	AV3200SU
avision	AV3730SU
avision	AV3750SU
avision	AV3800C
avision	AV3850SU
avision	FB6000E
avision	FB6080E
avision	FB2080E
avision	AV8000S
avision	AV8050U
avision	AV8300
avision	AV8350
avision	IT8300

Производитель	Модель
avision	@V5100
avision	AVA3
Bell and Howell	COPISCAN II 6338
Bell and Howell	COPISCAN II 2137(A)
Bell+Howell	2000F
BenQ	5550
Benq (Acer)	300f
Benq (Acer)	310s
Benq (Acer)	610s
Benq (Acer)	610plus
Benq (Acer)	620s
Benq (Acer)	ScanWit 2720s
Benq (Acer)	310U
Benq (Acer)	320U
Benq (Acer)	340U
Benq (Acer)	620U
Benq (Acer)	620UT
Benq (Acer)	640U
Benq (Acer)	640bu
Benq (Acer)	640BT
Benq (Acer)	1240
Benq (Acer)	3300
Benq (Acer)	3300
Benq (Acer)	4300
Benq (Acer)	4300
Benq (Acer)	5000E
Benq (Acer)	5000U
Benq (Acer)	5000
Benq (Acer)	5150
Benq (Acer)	5250
Benq (Acer)	5300
BlackWidow	BW4800SP
Boeder	Sm@rtScan Slim Edition
BrightScan	BrighScan OpticPro
Canon	CanoScan 300
Canon	CanoScan 600
Canon	CanoScan 620S
Canon	CanoScan 1200S
Canon	CanoScan 2700F
Canon	CanoScan 2710S
Canon	IX-4015
Canon	DR-2010C
Canon	DR-2050C
Canon	DR-2080C
Canon	DR-2510C

Производитель	Модель
Canon	DR-2580C
Canon	DR-3010C
Canon	DR-4010C
Canon	DR-5020
Canon	DR-5060F
Canon	DR-6050C
Canon	DR-6080
Canon	DR-7080C
Canon	DR-7090C
Canon	DR-7580
Canon	DR-9050C
Canon	DR-9080C
Canon	DR-C125
Canon	DR-G1100
Canon	DR-M140
Canon	DR-M160
Canon	P-208
Canon	P-215
Canon	P-215
Canon	CanoScan FB320P
Canon	CanoScan FB620P
Canon	CanoScan FB330P
Canon	CanoScan FB630P
Canon	CanoScan N340P
Canon	CanoScan N640P
Canon	CanoScan N640P ex
Canon	CanoScan LiDE 35
Canon	CanoScan LiDE 40
Canon	CanoScan LiDE 50
Canon	CanoScan LiDE 60
Canon	CanoScan LiDE 80
Canon	CanoScan LiDE 100
Canon	CanoScan LiDE 110
Canon	CanoScan LiDE 200
Canon	CanoScan LiDE 210
Canon	CanoScan LiDE 220
Canon	CanoScan 700F
Canon	PIXMA MG2100 Series
Canon	PIXMA MG2200 Series
Canon	PIXMA MG2400 Series
Canon	PIXMA MG2500 Series
Canon	PIXMA MG2900 Series
Canon	PIXMA MG3100 Series
Canon	PIXMA MG3200 Series
Canon	PIXMA MG3500 Series

Производитель	Модель
Canon	PIXMA MG4200 Series
Canon	PIXMA MG5100 Series
Canon	PIXMA MG5200 Series
Canon	PIXMA MG5300 Series
Canon	PIXMA MG5500 Series
Canon	PIXMA MG5600 Series
Canon	PIXMA MG6100 Series
Canon	PIXMA MG6200 Series
Canon	PIXMA MG6300 Series
Canon	PIXMA MG6400 Series
Canon	PIXMA MG7100 Series
Canon	PIXMA MG7500 Series
Canon	PIXMA MG8200 Series
Canon	PIXMA MP140
Canon	PIXMA MP150
Canon	PIXMA MP160
Canon	PIXMA MP170
Canon	PIXMA MP180
Canon	PIXMA MP190
Canon	PIXMA MP210
Canon	PIXMA MP220
Canon	PIXMA MP230
Canon	PIXMA MP240
Canon	PIXMA MP250
Canon	PIXMA MP260
Canon	PIXMA MP270
Canon	PIXMA MP280
Canon	PIXMA MP360
Canon	PIXMA MP370
Canon	PIXMA MP390
Canon	PIXMA MP450
Canon	PIXMA MP460
Canon	PIXMA MP470
Canon	PIXMA MP480
Canon	PIXMA MP490
Canon	PIXMA MP500
Canon	PIXMA MP510
Canon	PIXMA MP520
Canon	PIXMA MP530
Canon	PIXMA MP540
Canon	PIXMA MP550
Canon	PIXMA MP560
Canon	PIXMA MP600
Canon	PIXMA MP600R
Canon	PIXMA MP610

Производитель	Модель
Canon	PIXMA MP620
Canon	PIXMA MP630
Canon	PIXMA MP640
Canon	PIXMA MP700
Canon	PIXMA MP710
Canon	PIXMA MP730
Canon	PIXMA MP750
Canon	PIXMA MP760
Canon	PIXMA MP770
Canon	PIXMA MP780
Canon	PIXMA MP790
Canon	PIXMA MP800
Canon	PIXMA MP800R
Canon	PIXMA MP810
Canon	PIXMA MP830
Canon	PIXMA MP960
Canon	PIXMA MP970
Canon	PIXMA MP980
Canon	PIXMA MP990
Canon	PIXMA MX300
Canon	PIXMA MX310
Canon	PIXMA MX330
Canon	PIXMA MX340
Canon	PIXMA MX350
Canon	PIXMA MX360
Canon	PIXMA MX370 Series
Canon	PIXMA MX410
Canon	PIXMA MX420
Canon	PIXMA MX470 Series
Canon	PIXMA MX510 Series
Canon	PIXMA MX520 Series
Canon	PIXMA MX530 Series
Canon	PIXMA MX700
Canon	PIXMA MX720 Series
Canon	PIXMA MX850
Canon	PIXMA MX860
Canon	PIXMA MX870
Canon	PIXMA MX880 Series
Canon	PIXMA MX882
Canon	PIXMA MX885
Canon	PIXMA MX890 Series
Canon	PIXMA MX920 Series
Canon	PIXMA MX7600
Canon	imageCLASS D420
Canon	imageCLASS D480

Производитель	Модель
Canon	imageCLASS D530
Canon	i-SENSYS MF3010
Canon	imageCLASS MF3110
Canon	imageCLASS MF3240
Canon	imageCLASS MF4010
Canon	imageCLASS MF4018
Canon	imageCLASS MF4120
Canon	imageCLASS MF4122
Canon	imageCLASS MF4140
Canon	imageCLASS MF4150
Canon	imageCLASS MF4270
Canon	I-SENSYS MF4320d
Canon	I-SENSYS MF4330d
Canon	imageCLASS MF4350d
Canon	imageCLASS MF4370dn
Canon	imageCLASS MF4380dn
Canon	imageCLASS MF4410
Canon	imageCLASS MF4430
Canon	i-SENSYS MF4500 Series
Canon	imageCLASS MF4570dw
Canon	imageCLASS MF4660
Canon	imageCLASS MF4690
Canon	i-SENSYS MF4700 Series
Canon	i-SENSYS MF4800 Series
Canon	imageCLASS MF5730
Canon	imageCLASS MF5770
Canon	imageCLASS MF6500 series
Canon	imageCLASS MF6550
Canon	i-SENSYS MF8200C Series
Canon	i-SENSYS MF8300 Series
Canon	imageRUNNER 1020/1024/1025
Canon	CanoScan 8800F
Canon	CanoScan 9000F
Canon	CanoScan 9000F Mark II
Canon	CanoScan N650U/N656U
Canon	CanoScan N1220U
Canon	CanoScan N670U/N676U/LiDE20
Canon	CanoScan N1240U/LiDE30
Canon	CanoScan LiDE25
Canon	CanoScan D660U
Compaq	S4-100
Corex	800c
Corex	600c
Cybercom	9352
DCT	DocketPort 487

Производитель	Модель
Dell	1600n
Dell	A920
Dell	Dell MFP Laser Printer 1815dn
Dell	Dell 1235cn
Devcom	9636PRO
Dextra	DF-600P
Dexxa	4800
Epson	GT-5000
Epson	Actionscanner II
Epson	GT-6000
Epson	ES-300C
Epson	ES-300GS
Epson	GT-5500
Epson	GT-6500
Epson	ES-600C
Epson	ES-1200C
Epson	GT-7000
Epson	GT-8000
Epson	ES-8500
Epson	Perfection 636S
Epson	Perfection 636
Epson	Perfection 636U
Epson	Perfection 610
Epson	Perfection 640
Epson	Perfection 1200S
Epson	Perfection 1200U
Epson	Perfection 1200Photo
Epson	Perfection 1240
Epson	Perfection 1640
Epson	Perfection 1650
Epson	Perfection 1660
Epson	Perfection 2400
Epson	Perfection 2450
Epson	Perfection 3200
Epson	Perfection 4870
Epson	Perfection 4990
Epson	Expression 636
Epson	Expression 800
Epson	Expression 1600
Epson	Expression 1680
Epson	CX-3200
Epson	CX-3600
Epson	CX-3650
Epson	CX-4600
Epson	CX-4800

Производитель	Модель
Epson	CX-5000
Epson	CX-5200
Epson	CX-5400
Epson	CX-5400
Epson	CX-6300
Epson	CX-6400
Epson	CX-6500
Epson	CX-6600
Epson	RX-500
Epson	RX-600
Epson	RX-425
Epson	RX-700
Epson	RX-620
Epson	DX-3850
Epson	CX-3700
Epson	CX-3800
Epson	CX-4200
Epson	DX-3800
Epson	DX-5000
Epson	DX-5050
Epson	DX-6000
Epson	DX-7400
Epson	DX-4050
Epson	AcuLaser CX11
Epson	AcuLaser CX11NF
Epson	V700
Epson	V750
Epson	AL-MX300DN Series
Epson	AL-MX300DNF Series
Epson	Actionscanner II
Epson	AcuLaser CX11
Epson	AcuLaser CX11NF
Epson	AcuLaser CX21
Epson	AcuLaser MX20DN
Epson	AcuLaser MX20DNF
Epson	AcuLaser MX21DNF
Epson	Artisan 635
Epson	Artisan 700
Epson	Artisan 710 Series
Epson	Artisan 725
Epson	Artisan 730 Series
Epson	Artisan 800
Epson	Artisan 810 Series
Epson	Artisan 835
Epson	Artisan 837

Производитель	Модель
Epson	CC-570L
Epson	CC-600PX
Epson	EP-702A
Epson	EP-703A
Epson	EP-704A
Epson	EP-705A
Epson	EP-706A
Epson	EP-707A
Epson	EP-774A
Epson	EP-775A
Epson	EP-775AW
Epson	EP-776AB
Epson	EP-776AW
Epson	EP-777A
Epson	EP-801A
Epson	EP-802A
Epson	EP-803A
Epson	EP-803AW
Epson	EP-804A
Epson	EP-804AR
Epson	EP-804AW
Epson	EP-805A
Epson	EP-805AR
Epson	EP-805AW
Epson	EP-806AB
Epson	EP-806AR
Epson	EP-806AW
Epson	EP-807AB
Epson	EP-807AR
Epson	EP-807AW
Epson	EP-901A
Epson	EP-901F
Epson	EP-902A
Epson	EP-903A
Epson	EP-903F
Epson	EP-904A
Epson	EP-904F
Epson	EP-905A
Epson	EP-905F
Epson	EP-906F
Epson	EP-907F
Epson	EP-976A3
Epson	EP-977A3
Epson	ES-300C
Epson	ES-300GS

Производитель	Модель
Epson	ES-600C
Epson	ES-800C
Epson	ES-1200C
Epson	ES-2000
Epson	ES-2200
Epson	ES-6000
Epson	ES-6000H
Epson	ES-6000HS
Epson	ES-7000H
Epson	ES-8500
Epson	ES-9000H
Epson	ES-10000G
Epson	ES-G11000
Epson	ES-H300
Epson	ES-H7200
Epson	Expression 636
Epson	Expression 800
Epson	Expression 1600
Epson	Expression 1640XL
Epson	Expression 1680
Epson	Expression 10000XL
Epson	Expression 11000XL
Epson	FilmScan 200
Epson	GT-2500
Epson	GT-5000
Epson	GT-5400
Epson	GT-5500
Epson	GT-6000
Epson	GT-6500
Epson	GT-6600U
Epson	GT-6700U
Epson	GT-7000S
Epson	GT-7000U
Epson	GT-7600S
Epson	GT-7600U
Epson	GT-7600UF
Epson	GT-7700U
Epson	GT-8000
Epson	GT-8200U
Epson	GT-8200UF
Epson	GT-8300UF
Epson	GT-8700
Epson	GT-8700F
Epson	GT-9000
Epson	GT-9300UF

Производитель	Модель
Epson	GT-9500
Epson	GT-9600
Epson	GT-9700F
Epson	GT-9800F
Epson	GT-10000
Epson	GT-10000+
Epson	GT-15000
Epson	GT-20000
Epson	GT-30000
Epson	GT-X700
Epson	GT-X800
Epson	GT-X900
Epson	GT-X970
Epson	GT-X980
Epson	K200 Series
Epson	K300 Series
Epson	L200 Series
Epson	L210 Series
Epson	L350
Epson	L351
Epson	L355
Epson	L358
Epson	L550 Series
Epson	L850 Series
Epson	LP-A500
Epson	LP-M5000
Epson	LP-M5300 Series
Epson	LP-M5500
Epson	LP-M5500F
Epson	LP-M5600
Epson	LP-M6000
Epson	LP-M8040
Epson	LP-M8040A
Epson	LP-M8040F
Epson	M200 Series
Epson	ME 200
Epson	ME 300
Epson	ME 320 Series
Epson	ME 330 Series
Epson	ME 340 Series
Epson	ME OFFICE 510
Epson	ME OFFICE 520 Series
Epson	ME OFFICE 535
Epson	ME OFFICE 560W Series
Epson	ME OFFICE 570W Series

Производитель	Модель
Epson	ME Office 600F
Epson	ME OFFICE 620F Series
Epson	ME OFFICE 650FN Series
Epson	ME Office 700FW
Epson	ME OFFICE 900WD Series
Epson	ME OFFICE 940FW Series
Epson	ME OFFICE 960FWD Series
Epson	ME-101
Epson	ME-301
Epson	ME-303
Epson	ME-401
Epson	PM-A700
Epson	PM-A750
Epson	PM-A820
Epson	PM-A840
Epson	PM-A840S
Epson	PM-A850
Epson	PM-A870
Epson	PM-A890
Epson	PM-A900
Epson	PM-A920
Epson	PM-A940
Epson	PM-A950
Epson	PM-A970
Epson	PM-T960
Epson	PM-T990
Epson	PX-045A
Epson	PX-046A
Epson	PX-047A
Epson	PX-1600F
Epson	PX-1700F
Epson	PX-401A
Epson	PX-402A
Epson	PX-403A
Epson	PX-404A
Epson	PX-405A
Epson	PX-434A
Epson	PX-435A
Epson	PX-436A
Epson	PX-437A
Epson	PX-501A
Epson	PX-502A
Epson	PX-503A
Epson	PX-504A
Epson	PX-505F

Производитель	Модель
Epson	PX-535F
Epson	PX-601F
Epson	PX-602F
Epson	PX-603F
Epson	PX-605F
Epson	PX-673F
Epson	PX-675F
Epson	PX-A550
Epson	PX-A620
Epson	PX-A640
Epson	PX-A650
Epson	PX-A720
Epson	PX-A740
Epson	PX-B750F
Epson	PX-FA700
Epson	PX-M350F
Epson	PX-M5040F
Epson	PX-M5041F
Epson	PX-M650A
Epson	PX-M650F
Epson	PX-M740F
Epson	PX-M741F
Epson	PX-M840F
Epson	Perfection 610
Epson	Perfection 636S
Epson	Perfection 636U
Epson	Perfection 640U
Epson	Perfection 1200S
Epson	Perfection 1200U
Epson	Perfection 1200U PHOTO
Epson	Perfection 1240U
Epson	Perfection 1640SU
Epson	Perfection 1640SU PHOTO
Epson	Perfection 1650
Epson	Perfection 1650 PHOTO
Epson	Perfection 1660 PHOTO
Epson	Perfection 2400 PHOTO
Epson	Perfection 2450 PHOTO
Epson	Perfection 3200 PHOTO
Epson	Perfection 4870 PHOTO
Epson	Perfection 4990 PHOTO
Epson	Perfection V700 Photo
Epson	Perfection V750 Photo
Epson	Perfection V800 Photo
Epson	Perfection V850 Pro

Производитель	Модель
Epson	Stylus CX2800
Epson	Stylus CX2900
Epson	Stylus CX3100
Epson	Stylus CX3200
Epson	Stylus CX3500
Epson	Stylus CX3600
Epson	Stylus CX3650
Epson	Stylus CX3700
Epson	Stylus CX3800
Epson	Stylus CX3810
Epson	Stylus CX3900
Epson	Stylus CX4100
Epson	Stylus CX4200
Epson	Stylus CX4500
Epson	Stylus CX4600
Epson	Stylus CX4700
Epson	Stylus CX4800
Epson	Stylus CX4900
Epson	Stylus CX5000
Epson	Stylus CX5100
Epson	Stylus CX5200
Epson	Stylus CX5300
Epson	Stylus CX5400
Epson	Stylus CX5900
Epson	Stylus CX6000
Epson	Stylus CX6300
Epson	Stylus CX6400
Epson	Stylus CX6500
Epson	Stylus CX6600
Epson	Stylus CX7300
Epson	Stylus CX7400
Epson	Stylus CX7700
Epson	Stylus CX7800
Epson	Stylus CX8300
Epson	Stylus CX8400
Epson	Stylus CX9300F
Epson	Stylus CX9400Fax
Epson	Stylus DX3800
Epson	Stylus DX3850
Epson	Stylus DX4000
Epson	Stylus DX4200
Epson	Stylus DX4800
Epson	Stylus DX4850
Epson	Stylus DX5000
Epson	Stylus DX6000

Производитель	Модель
Epson	Stylus DX7400
Epson	Stylus DX8400
Epson	Stylus DX9400F
Epson	Stylus Office BX300F
Epson	Stylus Office BX305F
Epson	Stylus Office BX305FW
Epson	Stylus Office BX305FW Plus
Epson	Stylus Office BX310FN Series
Epson	Stylus Office BX320FW Series
Epson	Stylus Office BX535WD
Epson	Stylus Office BX630FW Series
Epson	Stylus Office BX525WD
Epson	Stylus Office BX600FW
Epson	Stylus Office BX610FW Series
Epson	Stylus Office BX625FWD
Epson	Stylus Office BX635FWD
Epson	Stylus Office BX925FWD
Epson	Stylus Office BX935FWD
Epson	Stylus Office TX300F
Epson	Stylus Office TX320F Series
Epson	Stylus Office TX510FN Series
Epson	Stylus Office TX525FW
Epson	Stylus Office TX600FW
Epson	Stylus Office TX610FW Series
Epson	Stylus Office TX620FWD Series
Epson	Stylus Photo PX650 Series
Epson	Stylus Photo PX660 Series
Epson	Stylus Photo PX700W
Epson	Stylus Photo PX710W Series
Epson	Stylus Photo PX720WD Series
Epson	Stylus Photo PX730WD Series
Epson	Stylus Photo PX800FW
Epson	Stylus Photo PX810FW Series
Epson	Stylus Photo PX820FWD Series
Epson	Stylus Photo PX830FWD Series
Epson	Stylus Photo RX420
Epson	Stylus Photo RX425
Epson	Stylus Photo RX430
Epson	Stylus Photo RX500
Epson	Stylus Photo RX510
Epson	Stylus Photo RX520
Epson	Stylus Photo RX530
Epson	Stylus Photo RX560
Epson	Stylus Photo RX585
Epson	Stylus Photo RX580

Производитель	Модель
Epson	Stylus Photo RX595
Epson	Stylus Photo RX590
Epson	Stylus Photo RX600
Epson	Stylus Photo RX610
Epson	Stylus Photo RX620
Epson	Stylus Photo RX630
Epson	Stylus Photo RX640
Epson	Stylus Photo RX650
Epson	Stylus Photo RX680
Epson	Stylus Photo RX685
Epson	Stylus Photo RX690
Epson	Stylus Photo RX700
Epson	Stylus Photo TX650 Series
Epson	Stylus Photo TX700W
Epson	Stylus Photo TX710W Series
Epson	Stylus Photo TX720WD Series
Epson	Stylus Photo TX730WD Series
Epson	Stylus Photo TX800FW
Epson	Stylus Photo TX820FWD Series
Epson	Stylus NX100
Epson	Stylus NX110 Series
Epson	Stylus NX125
Epson	Stylus NX127
Epson	Stylus NX130 Series
Epson	Stylus NX200
Epson	Stylus NX210 Series
Epson	Stylus NX220 Series
Epson	Stylus NX230 Series
Epson	Stylus NX300 Series
Epson	Stylus NX330 Series
Epson	Stylus NX400
Epson	Stylus NX410 Series
Epson	Stylus NX420 Series
Epson	Stylus NX430W Series
Epson	Stylus NX510 Series
Epson	Stylus NX530 Series
Epson	Stylus NX625
Epson	Stylus NX635
Epson	Stylus SX100
Epson	Stylus SX110 Series
Epson	Stylus SX125
Epson	Stylus SX130 Series
Epson	Stylus SX200
Epson	Stylus SX205
Epson	Stylus SX210 Series

Производитель	Модель
Epson	Stylus SX218
Epson	Stylus SX230 Series
Epson	Stylus SX235W
Epson	Stylus SX400
Epson	Stylus SX405
Epson	Stylus SX410 Series
Epson	Stylus SX420W Series
Epson	Stylus SX430W Series
Epson	Stylus SX440W Series
Epson	Stylus SX510W Series
Epson	Stylus SX525WD
Epson	Stylus SX535WD
Epson	Stylus SX600FW
Epson	Stylus SX610FW Series
Epson	Stylus SX620FW Series
Epson	Stylus TX100
Epson	Stylus TX110 Series
Epson	Stylus TX120 Series
Epson	Stylus TX130 Series
Epson	Stylus TX200
Epson	Stylus TX203
Epson	Stylus TX209
Epson	Stylus TX210 Series
Epson	Stylus TX220 Series
Epson	Stylus TX230W Series
Epson	Stylus TX235
Epson	Stylus TX400
Epson	Stylus TX410 Series
Epson	Stylus TX420W Series
Epson	Stylus TX430W Series
Epson	Stylus TX435W
Epson	Stylus TX550W Series
Epson	Stylus TX560WD Series
Epson	WF-2510 Series
Epson	WF-2520 Series
Epson	WF-2530 Series
Epson	WF-2540 Series
Epson	WF-2630 Series
Epson	WF-2650 Series
Epson	WF-2660 Series
Epson	WF-3520 Series
Epson	WF-3530 Series
Epson	WF-3540 Series
Epson	WF-3620 Series
Epson	WF-3640 Series

Производитель	Модель
Epson	WF-4630 Series
Epson	WF-4640 Series
Epson	WF-5620 Series
Epson	WF-5690 Series
Epson	WF-7510 Series
Epson	WF-7520 Series
Epson	WF-7610 Series
Epson	WF-7620 Series
Epson	WF-M1560 Series
Epson	WF-M5690 Series
Epson	WF-R4640 Series
Epson	WF-R5690 Series
Epson	WP-4511
Epson	WP-4515
Epson	WP-4521
Epson	WP-4525
Epson	WP-4530 Series
Epson	WP-4540 Series
Epson	WP-4590 Series
Epson	WorkForce 310 Series
Epson	WorkForce 320 Series
Epson	WorkForce 435
Epson	WorkForce 500
Epson	WorkForce 520 Series
Epson	WorkForce 545
Epson	WorkForce 600
Epson	WorkForce 610 Series
Epson	WorkForce 625
Epson	WorkForce 630 Series
Epson	WorkForce 645
Epson	WorkForce 840 Series
Epson	WorkForce 845
Epson	WorkForce K301
Epson	XP-100 Series
Epson	XP-200 Series
Epson	XP-211
Epson	XP-212
Epson	XP-215
Epson	XP-225
Epson	XP-300 Series
Epson	XP-310 Series
Epson	XP-320 Series
Epson	XP-400 Series
Epson	XP-410 Series
Epson	XP-420 Series

Производитель	Модель
Epson	XP-600 Series
Epson	XP-510 Series
Epson	XP-520 Series
Epson	XP-610 Series
Epson	XP-620 Series
Epson	XP-700 Series
Epson	XP-710 Series
Epson	XP-720 Series
Epson	XP-750 Series
Epson	XP-760 Series
Epson	XP-800 Series
Epson	XP-810 Series
Epson	XP-820 Series
Epson	XP-850 Series
Epson	XP-860 Series
Epson	XP-950 Series
Epson	Epson ME 350
Epson	WP-M4525, WP-M4521, PX-K751F, WP-M4595
Epson	DS-60000
Epson	DS-510
Epson	Perfection 1250
Epson	Perfection 1250Photo
Epson	Perfection 1260
Epson	Perfection 1260Photo
Epson	Perfection 660
Epson	Perfection 1270
Epson	Perfection 1670
Epson	Perfection 2480
Epson	Perfection 2580
Epson	Perfection 3490
Epson	Perfection 3590
Epson	Stylus CX-1500
Epson	Perfection 600
Escom	Image Scanner 256
Fujitsu	ScanPartner 620C
Fujitsu	fi-5015C
Fujitsu	fi-60F
Fujitsu	ScanSnap S300
Fujitsu	ScanSnap S300M
Fujitsu	ScanSnap S1100
Fujitsu	ScanSnap S1300
Fujitsu	ScanSnap S1300i
Fujitsu	fi-65F
Fujitsu	M3091DC
Fujitsu	M3092DC

Производитель	Модель
Fujitsu	fi-4120C
Fujitsu	fi-4120C2
Fujitsu	fi-4220C
Fujitsu	fi-4220C2
Fujitsu	fi-5110C
Fujitsu	fi-5110EOX/2
Fujitsu	fi-5110EOX3
Fujitsu	fi-5110EOXM
Fujitsu	fi-5120C
Fujitsu	fi-5220C
Fujitsu	ScanSnap S500
Fujitsu	ScanSnap S500M
Fujitsu	ScanSnap S510
Fujitsu	ScanSnap S510M
Fujitsu	fi-6130
Fujitsu	fi-6230
Fujitsu	fi-6130Z
Fujitsu	fi-6230Z
Fujitsu	ScanSnap S1500
Fujitsu	ScanSnap S1500M
Fujitsu	fi-6110
Fujitsu	fi-7160
Fujitsu	fi-7260
Fujitsu	ScanSnap iX500
Fujitsu	ScanSnap iX100
Fujitsu	M3093DG
Fujitsu	M3093GX
Fujitsu	M3096GX
Fujitsu	M3097G+
Fujitsu	M3097DG
Fujitsu	fi-4340C
Fujitsu	fi-4530C
Fujitsu	fi-4640S
Fujitsu	fi-4750C
Fujitsu	fi-5530C
Fujitsu	fi-6140
Fujitsu	fi-6240
Fujitsu	fi-6140Z
Fujitsu	fi-6240Z
Fujitsu	fi-5530C2
Fujitsu	fi-7180
Fujitsu	fi-7280
Fujitsu	M3099G
Fujitsu	M3099GH
Fujitsu	M3099GX

Производитель	Модель
Fujitsu	M4097D
Fujitsu	M4099D
Fujitsu	fi-4750L
Fujitsu	fi-4860C
Fujitsu	fi-4860C2
Fujitsu	fi-4990C
Fujitsu	fi-5650C
Fujitsu	fi-5750C
Fujitsu	fi-5900C
Fujitsu	fi-6670
Fujitsu	fi-6670A
Fujitsu	fi-6770
Fujitsu	fi-6770A
Fujitsu	1200CUS
Fujitsu	ScanPartner 15C
Fujitsu	ScanPartner 600C
Gallery	4800
Genius	Colorpage SF600
Genius	Colorpage Vivid3x
Genius	Colorpage Vivid3 V2
Genius	Colorpage Vivid3xe
Genius	Colorpage Vivid4
Genius	Colorpage Vivid4x
Genius	Colorpage Vivid4xe
Genius	Colorpage Vivid 1200 X
Genius	Colorpage Vivid 1200 XE
Genius	FS-1130 Colorpage Scanner
Genius	Colorpage-SP2
Genius	ColorPage-EP
Genius	Colorpage HR6 V2
Genius	Colorpage HR6 V2
Genius	Colorpage HR7
Genius	Colorpage Vivid III V2
Genius	Colorpage Vivid Pro II Film
Genius	Colorpage HR6X EPP
Genius	ColorPage HR6 V1
Genius	ColorPage-HR5 (Pro)
Genius	ColorPage-Life Pro
Googlegear	2000
Guillemot / Hercules	Maxi Scan A4 Deluxe (SCSI)
Guillemot / Hercules	Scan@home Touch 1248 (USB)
Guillemot / Hercules	Maxi Scan A4 USB 640U
Guillemot / Hercules	Maxi A4 36 bit
Hewlett-Packard	ScanJet 5300C
Hewlett-Packard	ScanJet 5370C

Производитель	Модель
Hewlett-Packard	ScanJet 7400c
Hewlett-Packard	ScanJet 7450c
Hewlett-Packard	ScanJet 7490c
Hewlett-Packard	ScanJet 8200
Hewlett-Packard	ScanJet 8250
Hewlett-Packard	ScanJet 8270
Hewlett-Packard	ScanJet 8290
Hewlett-Packard	ScanJet 8300
Hewlett-Packard	ScanJet 8350
Hewlett-Packard	ScanJet 8390
Hewlett-Packard	ScanJet 2300C
Hewlett-Packard	ScanJet 2400C
Hewlett-Packard	ScanJet G2410
Hewlett-Packard	ScanJet 3670C
Hewlett-Packard	ScanJet 3690C
Hewlett-Packard	ScanJet 4850C
Hewlett-Packard	ScanJet G4010
Hewlett-Packard	ScanJet G4050
Hewlett-Packard	ScanJet Plus
Hewlett-Packard	ScanJet IIc
Hewlett-Packard	ScanJet IIp
Hewlett-Packard	ScanJet IIcx
Hewlett-Packard	ScanJet 3c
Hewlett-Packard	ScanJet 3p
Hewlett-Packard	ScanJet 4c
Hewlett-Packard	ScanJet 4p
Hewlett-Packard	ScanJet 4100C
Hewlett-Packard	ScanJet 5p
Hewlett-Packard	ScanJet 5100C
Hewlett-Packard	ScanJet 5200C
Hewlett-Packard	ScanJet 6100C
Hewlett-Packard	ScanJet 6200C
Hewlett-Packard	ScanJet 6250C
Hewlett-Packard	ScanJet 6300C
Hewlett-Packard	ScanJet 6350C
Hewlett-Packard	ScanJet 6390C
Hewlett-Packard	PhotoSmart PhotoScanner
Hewlett-Packard	ScanJet 3500C
Hewlett-Packard	ScanJet 3530C
Hewlett-Packard	ScanJet 3570C
Hewlett-Packard	ScanJet 3800
Hewlett-Packard	ScanJet 3970c
Hewlett-Packard	ScanJet 4070 Photosmart
Hewlett-Packard	ScanJet 4370
Hewlett-Packard	ScanJet G2710

Производитель	Модель
Hewlett-Packard	ScanJet G3010
Hewlett-Packard	ScanJet G3110
Hewlett-Packard	ScanJet 4200C
Hewlett-Packard	ScanJet 4200Cxi
Hewlett-Packard	ScanJet 4200Cse
Hewlett-Packard	ScanJet 5400c
Hewlett-Packard	ScanJet 5470c
Hewlett-Packard	ScanJet 5490c
Hewlett-Packard	ScanJet 4500C
Hewlett-Packard	ScanJet 4570C
Hewlett-Packard	ScanJet 5550C
Hewlett-Packard	ScanJet 5590
Hewlett-Packard	ScanJet 7650
Hewlett-Packard	LaserJet M1005 MFP
Hewlett-Packard	LaserJet M1120 MFP
Hewlett-Packard	LaserJet M1120n MFP
Hewlett-Packard	ScanJet 5s
Hewlett-Packard	ScanJet 3300c
Hewlett-Packard	ScanJet 3400c
Hewlett-Packard	ScanJet 4300c
Hewlett-Packard	ScanJet 4300c/Silitek
Hewlett-Packard	ScanJet 2100C
Hewlett-Packard	ScanJet 2200C
Hewlett-Packard	scanjet 4470c
Hewlett-Packard	scanjet 4400c
Hewlett-Packard	Scanjet 3200C
IBM	2456
Kodak	i40
Kodak	i80
Kodak	i1860 Scanner
Kodak	ESP 2170
Kodak	ESP 5200
Kodak	Hero Office 6.1
Kodak	Hero 9.1
KONICA MINOLTA	magicolor 1690MF
KONICA MINOLTA	magicolor 4690MF
LEO	LEOScan S3
Lexmark	X70
Lexmark	X73
Lexmark	X1130
Lexmark	X1150
Lexmark	X1170
Lexmark	X1180
Lexmark	X1185
Lexmark	X74

Производитель	Модель
Lexmark	X12xx
Linotype Hell	Jade
Linotype Hell	Jade
Linotype Hell	Jade2
Linotype Hell	Saphir2
Linotype Hell	Saphir3
Linotype Hell	Saphir Ultra II
Linotype Hell	Opal2
Linotype Hell	Linoscan 1400
Medion/Lifetec/Tevion/Cytron	MD9693
Medion/Lifetec/Tevion/Cytron	MD9705
Medion/Lifetec/Tevion/Cytron	MD4394
Medion/Lifetec/Tevion/Cytron	MD5345
Medion/Lifetec/Tevion/Cytron	MD6228
Medion/Lifetec/Tevion/Cytron	MD6471
Medion/Lifetec/Tevion/Cytron	MD 4394
Medion/Lifetec/Tevion/Cytron	MD/LT 9385
Medion/Lifetec/Tevion/Cytron	LT 9452
Medion/Lifetec/Tevion/Cytron	MD 9458
Medion/Lifetec/Tevion/Cytron	MD 9848
Medion/Lifetec/Tevion/Cytron	MD 9806
Medion/Lifetec/Tevion/Cytron	MD/LT 935x
Medion/Lifetec/Tevion/Cytron	MD/LT 985x
Medion/Lifetec/Tevion/Cytron	MD/LT 9890
Memorex	MEM 48U
Micromaxx	MM-9851
Microstar	MR 9791
Microtek	Scanmaker E6
Microtek	Scanmaker E3
Microtek	Scanmaker E2
Microtek	Scanmaker 35t+
Microtek	Scanmaker 45t
Microtek	Scanmaker 35
Microtek	Scanmaker III
Microtek	Scanmaker IISP
Microtek	Scanmaker IIHR
Microtek	Scanmaker IIG
Microtek	Scanmaker II
Microtek	Scanmaker 600G(S)
Microtek	Color PageWiz
Microtek	ScanMaker E3plus
Microtek	ScanMaker E3plus
Microtek	ScanMaker X6
Microtek	ScanMaker X6EL
Microtek	ScanMaker X6USB

Производитель	Модель
Microtek	ScanMaker V300
Microtek	ScanMaker V300
Microtek	ScanMaker V310
Microtek	ScanMaker V310
Microtek	ScanMaker V600
Microtek	ScanMaker V600
Microtek	ScanMaker 330
Microtek	ScanMaker 630
Microtek	ScanMaker 636
Microtek	ScanMaker 6400XL
Microtek	ScanMaker 9600XL
Microtek	ScanMaker 9800XL
Microtek	Phantom 330CX
Microtek	SlimScan C3
Microtek	Phantom 636
Microtek	Phantom 636CX
Microtek	SlimScan C6
Microtek	ScanMaker V6UPL
Microtek	ScanMaker V6USL
Microtek	ScanMaker V6USL
Microtek	ScanMaker V6USL
Microtek	ScanMaker X12USL
Microtek	ScanMaker 3600
Microtek	ScanMaker 3600
Microtek	ScanMaker 3600
Microtek	ScanMaker 3700
Microtek	ScanMaker 3700
Microtek	ScanMaker 3750
Microtek	ScanMaker 3840
Microtek	ScanMaker 4800
Minolta	Dimage Scan Dual I
Minolta	Dimage Scan Dual II
Minolta	Dimage Scan Dual III
Minolta	Dimage Scan Elite 5400
Minolta-QMS	SC-215
Mitsubishi	SS600
Mitsubishi	Diamondview 648UT
Mitsubishi	Diamondview 650U
Mustek	BearPaw 1200 CS
Mustek	BearPaw 1200 CU
Mustek	BearPaw 1200 CU Plus
Mustek	BearPaw 1200 CU Plus
Mustek	BearPaw 1200 TA
Mustek	BearPaw 1248 CU
Mustek	BearPaw 2400 CS Plus

Производитель	Модель
Mustek	BearPaw 2400 CU
Mustek	BearPaw 2400 CU Plus
Mustek	BearPaw 2400 TA
Mustek	BearPaw 2400 TA Plus
Mustek	BearPaw 2448 CS Plus
Mustek	BearPaw 2448 TA Plus
Mustek	Plug-n-Scan 2400 MT
Mustek	Plug-n-Scan 2400 M
Mustek	ScanExpress 1200 UB Plus
Mustek	ScanExpress 1248 UB
Mustek	ScanExpress 2400 USB
Mustek	ScanExpress A3 USB
Mustek	ScanMagic 1200 UB Plus
Mustek	BearPaw 1200 F
Mustek	Paragon MFS-6000CX
Mustek	Paragon MFS-12000CX
Mustek	Paragon MFC-600S
Mustek	Paragon 600 II CD
Mustek	Paragon 600 II EP
Mustek	ScanMagic 600 II SP
Mustek	TwainScan II SP
Mustek	Paragon MFC-800S
Mustek	Paragon 800 II SP
Mustek	Paragon MFS-6000SP
Mustek	Paragon MFS-8000SP
Mustek	Paragon MFS-1200SP
Mustek	Paragon MFS-12000SP
Mustek	ScanExpress 6000SP
Mustek	ScanExpress 12000SP
Mustek	ScanExpress 12000SP Plus
Mustek	Paragon 1200 III SP
Mustek	Paragon 1200 LS
Mustek	ScanMagic 9636S
Mustek	ScanMagic 9636S Plus
Mustek	ScanExpress A3 SP
Mustek	Paragon 1200 SP Pro
Mustek	Paragon 1200 A3 Pro
Mustek	Paragon 600 II N
Mustek	ScanExpress 6000 P
Mustek	ScanExpress 600 SEP
Mustek	ScanMagic 4800 P
Mustek	600 III EP Plus
Mustek	96 CP
Mustek	ScanExpress 600 CP
Mustek	ScanMagic 600 CP

Производитель	Модель
Mustek	ScanExpress 1200 CP
Mustek	ScanExpress 1200 CP+
Mustek	ScanExpress 600 CU
Mustek	ScanExpress 1200 CU
Mustek	ScanExpress 1200 CU Plus
Mustek	ScanExpress 1200 UB
Mustek	BearPaw 2448TA Pro
Mustek	BearPaw 1200
Mustek	BearPaw 1200
Mustek	BearPaw 2400
NeatReceipts	Mobile Scanner
NEC	PC-IN500/4C
Network	Easy Plus 30 Bit
Nikon	LS-20
Nikon	LS-30
Nikon	LS-2000
Nikon	LS-1000
Nikon	LS 30
Nikon	LS 2000
Nikon	LS 40 ED
Nikon	LS 4000 ED
Nikon	LS 50 ED
Nikon	Coolscan V ED
Nikon	LS 8000 ED
Nikon	LS 30
Nikon	Coolscan III
Nikon	LS 40 ED
Nikon	Coolspan IV
Nikon	LS 50 ED
Nikon	Coolscan V ED
Nikon	LS 2000
Nikon	LS 4000 ED
Nikon	LS 8000 ED
Nikon	AX-210
OKI	S700 Scancopier
Packard Bell	Diamond 1200
Packard Bell	Diamond 1200 Plus
Packard Bell	Diamond 1200 Plus
Packard Bell	Diamond 2450
Panasonic	KV-SS080
Panasonic	KV-S1020C
Panasonic	KV-S1025C
Panasonic	KV-S1045C
Panasonic	KV-SS25
Panasonic	KV-SS25D

Производитель	Модель
Panasonic	KV-SS55EX
Panasonic	KV-S2025C
Panasonic	KV-S2045C
Panasonic	KV-S2065L
Pentax	DSmobile 600
Pentax	DSmobile 600
PIE	ScanAce 1236S
PIE	ScanAce 1230S
PIE	ScanAce III
PIOTECH	Splendeur 3024
Plustek	OpticPro 19200S
Plustek	OpticBook 3600
Plustek	OpticPro 1248U
Plustek	OpticPro 1248U
Plustek	OpticPro U16B
Plustek	OpticPro U16B+
Plustek	OpticPro S12
Plustek	OpticPro S24
Plustek	OpticSlim 1200
Plustek	OpticSlim 2400
Plustek	OpticSlim 2400 plus
Plustek	Iriscan Express 2
Plustek	OpticSlim M12
Plustek	OpticPro U12
Plustek	OpticPro UT12
Plustek	OpticPro UT12
Plustek	OpticPro UT16
Plustek	OpticPro U24
Plustek	OpticPro U24
Plustek	OpticPro UT24
Plustek	OpticPro 4800P
Plustek	OpticPro 4830P
Plustek	OpticPro 600P/6000P
Plustek	OpticPro 4831P
Plustek	OpticPro 9630P
Plustek	OpticPro 9630PL
Plustek	OpticPro 9600P
Plustek	OpticPro 1236P
Plustek	OpticPro 12000P/96000P
Plustek	OpticPro 9636P
Plustek	OpticPro 9636P+/Turbo
Plustek	OpticPro 9636T
Plustek	OpticPro 12000T
Plustek	OpticPro AI3
Plustek	OpticPro P12

Производитель	Модель
Plustek	OpticPro PT12
Plustek	OpticPro U12
Plustek	OpticPro UT12
Plustek	OpticPro 1212U
Portable Peripheral Co., Ltd.	Q-Scan USB001 (A4 portable scanner)
Portable Peripheral Co., Ltd.	Q-Scan USB201 (A6 portable scanner)
Primax	Compact 4800 SCSI
PRIMAX	PagePartner
Primax	Compact 4800 Direct
Primax	Compact 4800 Direct-30
Primax	Compact 9600 Direct-30
Primax	Jewel 4800
Primax	Profi 9600
Primax	Profi 19200
Reflecta	Reflecta ProScan 7200
Reflecta	Reflecta CrystalScan 7250
Reflecta	Reflecta DigitDia 6000 Multiple Slide Scanner
Relisys	RELI 2412
Relisys	AVEC 2400
Relisys	RELI 4830
Relisys	AVEC 2412
Relisys	RELI 4816
Relisys	AVEC II S3
Relisys	SCORPIO Super 3
Relisys	APOLLO Express 3
Relisys	APOLLO Express 6
Relisys	SCORPIO Pro
Relisys	Infinity Scorpio
RevScan	19200i
RevScan	RevScan Orange R48Ti
Ricoh	IS450
Ricoh	IS-420
Ricoh	Ricoh IS50
Ricoh	Ricoh IS60
Samsung	SCX-4100
Samsung	SCX-4200
Samsung	SCX4725-FN
Samsung	CLX-2160
Samsung	SCX-4500
Samsung	SCX-6x55
Samsung	CLX-3170fn (CLX-3170 Series)
Samsung	CLX-3175FW
Samsung	SCX-4500W
Samsung	SCX-4824 (SCX-4x24 Series)
Samsung	SCX-4828FN (SCX-4x28 Series)

Производитель	Модель
Samsung	SCX-4300
Samsung	SCX-5835_5935
Samsung	SCX-4600
Samsung	SCX-4623
Samsung	SCX-6545
Samsung	CLX-6220
Samsung	SCX-4825FN (SCX-4x25 Series)
Samsung	CLX-3185
Samsung	SCX-4623FW
Samsung	SCX-3205W (SCX-3200 Series)
Samsung	SCX-6545X
Samsung	SCX-6x55X
Samsung	CLX-8385X
Samsung	SCX-5835_5935X
Samsung	SCX-4833FD
Samsung	SCX-4835FD
Samsung	SCX-3405W
Samsung	SCX-3400
Samsung	SCX-4729FD
Samsung	CLX-6260
Samsung	CLX-3300 Series
Samsung	CLX-4190
Samsung	M337x 387x 407x Series
Scanport	SQ300
Scanport	SQ2030
Scanport	SQ4836
Sceptre	Vividscan S1200
Sharp	JX-610
Sharp	JX-250
Sharp	JX-320
Sharp	JX-330
Sharp	JX-350
Siemens	9036 Flatbed scanner
Siemens	ST400
Siemens	ST800
Syscan	DocketPort 485
Syscan	DocketPort 665
Syscan	DocketPort 685/ Ambir DS685
Syscan	TravelScan 460/464
Syscan	TravelScan 662
Tamarack	Artiscan 6000C
Tamarack	Artiscan 8000C
Tamarack	Artiscan 12000C
Targa	Funline TS12 EP
Targa	Funline TS6 EP

Производитель	Модель
TriGem	PowerScanII
Trust	Easy Webscan 19200
Trust	240H Easy Webscan Gold
Trust	Easy Scan 9600 Plus
Trust	240TH Easy Webscan Gold
Trust	Compact Scan USB 19200
Trust	Direct WebScan 19200
Trust	Flat Scan USB 19200
Trust	Imagery 1200
Trust	Imagery 1200 SP
Trust	Imagery 4800 SP
Trust	SCSI Connect 19200
Trust	SCSI excellence series 19200
Trust	Easy Connect 9600+
Trust	Easy Connect 19200+
Trust	Compact Scan USB 19200
Trust	Office Scan USB 19200
Trust	Imagery 2400 SP
Trust	Imagery 4800 SP+
UMAX	AstraSlim SE
UMAX	AstraSlim 1200 SE
UMAX	Astra 4900
Umax	UMAX 3400
Umax	UMAX 3400
Umax	UMAX Astranet ia101
Umax	UMAX 3450
Umax	UMAX 5400
UMAX	Astra 4400
UMAX	Vista S6
UMAX	Vista S6E
UMAX	UMAX S-6E
UMAX	UMAX S-6EG
UMAX	Vista-S8
UMAX	Supervista S-12
UMAX	UMAX S-12
UMAX	UMAX S-12G
UMAX	Astra 600S
UMAX	Astra 610S
UMAX	Astra 1200S
UMAX	Astra 1220S
UMAX	Astra 2100S
UMAX	Astra 2200 (SU)
UMAX	Astra 2200 (SU)
UMAX	Astra 2400S
UMAX	Astra MX3

Производитель	Модель
UMAX	Astra MX3
UMAX	Mirage D-16L
UMAX	Mirage II
UMAX	Mirage IIse
UMAX	PSD
UMAX	PowerLook
UMAX	PL-II
UMAX	PowerLook III
UMAX	PowerLook 2000
UMAX	PowerLook 2100XL
UMAX	PowerLook 3000
UMAX	Gemini D-16
UMAX	Vista-T630
UMAX	UC 630
UMAX	UG 630
UMAX	UG 80
UMAX	UC 840
UMAX	UC 1200SE
UMAX	UC 1260
UMAX	Astra 1220U
UMAX	Astra 1600U
UMAX	Astra 2000U
UMAX	Astra 2100U
UMAX	Astra 1220P
UMAX	Astra 2000P
UMAX	Astra 1600P
UMAX	Astra 610P
Visioneer	Strobe XP 450
Visioneer	Strobe XP 450-G
Visioneer	Strobe XP 470
Visioneer	Strobe XP 470-G
Visioneer	9320
Visioneer	9450
Visioneer	9450-G
Visioneer	9550
Visioneer	9650
Visioneer	9650-G
Visioneer	9750
Visioneer	9750-G
Visioneer	Patriot 430
Visioneer	Patriot 470
Visioneer	Patriot 680
Visioneer	Patriot 780
Visioneer	Strobe XP 100,r3
Visioneer	Strobe XP 200

Производитель	Модель
Visioneer	Strobe XP 300
Visioneer	Roadwarrior
Visioneer	Visioneer OneTouch 7100
Visioneer	OneTouch 7300
Visioneer	Strobe XP 100
Viviscan	Compact II
Vobis	Highscreen Realscan
Vobis	HighScan
Vobis	Highscreen Scanboostar Premium
Xerox	DocuMate150
Xerox	DocuMate152
Xerox	DocuMate162
Xerox	DocuMate250
Xerox	DocuMate250-G
Xerox	DocuMate252
Xerox	DocuMate252-G
Xerox	DocuMate232
Xerox	DocuMate262
Xerox	DocuMate262-G
Xerox	DocuMate262i
Xerox	Travel Scanner 100
Xerox	2400 Onetouch
Xerox	Phaser 6110MFP
Xerox	Phaser 3200MFP
Xerox	WorkCentre 3119 Series
Xerox	WorkCentre 4118 Series
Xerox	WorkCentre 3210
Xerox	WorkCentre 3220
Yakumo	Scan50

Список видеокарт, поддерживаемых РЕД ОС

Модуль ядра	Производитель	Марка оборудования
radeon	ATI Technologies Inc	M24 1P [Radeon Mobility X600]
radeon	ATI Technologies Inc	M24 [FireMV 2400]
radeon	ATI Technologies Inc	M22 [Radeon Mobility X300]
radeon	ATI Technologies Inc	M24GL [Mobility FireGL V3200]
radeon	ATI Technologies Inc	RV380 0x3e50 [Radeon X600]
radeon	ATI Technologies Inc	RV380 0x3e54 [FireGL V3200]
radeon	ATI Technologies Inc	Radeon IGP 320 M
radeon	ATI Technologies Inc	Radeon IGP330/340/350
radeon	ATI Technologies Inc	R300 AD [Radeon 9500 Pro]
radeon	ATI Technologies Inc	R300 AE [Radeon 9700 Pro]
radeon	ATI Technologies Inc	R300 AF [Radeon 9700 Pro]
radeon	ATI Technologies Inc	R300 AG [FireGL Z1/X1]
radeon	ATI Technologies Inc	R350 AH [Radeon 9800]
radeon	ATI Technologies Inc	R350 AI [Radeon 9800]
radeon	ATI Technologies Inc	R350 AJ [Radeon 9800]
radeon	ATI Technologies Inc	R350 AK [FireGL X2]
radeon	ATI Technologies Inc	RV350 AP [Radeon 9600]
radeon	ATI Technologies Inc	RV350 AQ [Radeon 9600]
radeon	ATI Technologies Inc	RV350 AR [Radeon 9600]
radeon	ATI Technologies Inc	RV350 AS [Radeon 9550]
radeon	ATI Technologies Inc	RV350 AT [FireGL T2]
radeon	ATI Technologies Inc	RV350 AU [FireGL T2]
radeon	ATI Technologies Inc	RV350 AV [FireGL T2]
radeon	ATI Technologies Inc	Radeon 7000 IGP
radeon	ATI Technologies Inc	R200 BB [Radeon All in Wonder 8500DV]
radeon	ATI Technologies Inc	R200 BC [Radeon All in Wonder 8500]
radeon	ATI Technologies Inc	Radeon Mobility U1
radeon	ATI Technologies Inc	Radeon IGP 330M/340M/350M
mach64	ATI Technologies Inc	215CT [Mach64 CT]
mach64	ATI Technologies Inc	210888CX [Mach64 CX]
radeon	ATI Technologies Inc	Radeon Mobility 7000 IGP
mach64	ATI Technologies Inc	210888ET [Mach64 ET]
mach64	ATI Technologies Inc	3D Rage Pro AGP 1X/2X
mach64	ATI Technologies Inc	3D Rage Pro AGP 1X
mach64	ATI Technologies Inc	3D Rage Pro
mach64	ATI Technologies Inc	Rage XC
mach64	ATI Technologies Inc	Rage XL AGP 2X
mach64	ATI Technologies Inc	Rage XC AGP
mach64	ATI Technologies Inc	Rage XL
mach64	ATI Technologies Inc	3D Rage Pro 215GP
mach64	ATI Technologies Inc	3D Rage Pro 215GQ
mach64	ATI Technologies Inc	Rage XL
mach64	ATI Technologies Inc	Rage XC
mach64	ATI Technologies Inc	3D Rage I/II 215GT [Mach64 GT]

mach64	ATI Technologies Inc	3D Rage II+ 215GTB [Mach64 GTB]
mach64	ATI Technologies Inc	3D Rage IIC 215IIC [Mach64 GT IIC]
mach64	ATI Technologies Inc	3D Rage IIC AGP
mach64	ATI Technologies Inc	210888GX [Mach64 GX]
mach64	ATI Technologies Inc	3D Rage IIC
mach64	ATI Technologies Inc	3D Rage IIC AGP
radeon	ATI Technologies Inc	Radeon RV250 If [Radeon 9000]
radeon	ATI Technologies Inc	Radeon RV250 Ig [Radeon 9000]
radeon	ATI Technologies Inc	R420 JH [Radeon X800]
radeon	ATI Technologies Inc	R420 JI [Radeon X800PRO]
radeon	ATI Technologies Inc	R420 JJ [Radeon X800SE]
radeon	ATI Technologies Inc	R420 JK [Radeon X800]
radeon	ATI Technologies Inc	R420 JL [Radeon X800]
radeon	ATI Technologies Inc	R420 JM [FireGL X3]
radeon	ATI Technologies Inc	M18 JN [Radeon Mobility 9800]
radeon	ATI Technologies Inc	Radeon X800 SE (R420) (AGP)
radeon	ATI Technologies Inc	R420 JP [Radeon X800XT]AO
radeon	ATI Technologies Inc	R480 [Radeon X850XT]
radeon	ATI Technologies Inc	Radeon X850 SE (R480) (AGP)
radeon	ATI Technologies Inc	R480 [Radeon X850Pro]
radeon	ATI Technologies Inc	R481 [Radeon X850XT-PE]
mach64	ATI Technologies Inc	3D Rage LT Pro AGP-133
mach64	ATI Technologies Inc	3D Rage LT Pro AGP-66
r128	ATI Technologies Inc	Rage Mobility M3 AGP
r128	ATI Technologies Inc	Rage Mobility M3 AGP 2x
mach64	ATI Technologies Inc	3D Rage LT-G 215LG
mach64	ATI Technologies Inc	3D Rage LT Pro
mach64	ATI Technologies Inc	Rage Mobility P/M AGP 2x
mach64	ATI Technologies Inc	Rage Mobility L AGP 2x
mach64	ATI Technologies Inc	3D Rage LT Pro
mach64	ATI Technologies Inc	3D Rage LT Pro
mach64	ATI Technologies Inc	Rage Mobility P/M
mach64	ATI Technologies Inc	Rage Mobility L
radeon	ATI Technologies Inc	Radeon Mobility M7 LW [Radeon Mobility 7500]
radeon	ATI Technologies Inc	Radeon RV200 LX [Mobility FireGL 7800 M7]
radeon	ATI Technologies Inc	Radeon Mobility M6 LY
radeon	ATI Technologies Inc	Radeon Mobility M6 LZ
radeon	ATI Technologies Inc	Radeon RV250 Ld [Radeon Mobility 9000 M9]
radeon	ATI Technologies Inc	Mobility Radeon 9000
radeon	ATI Technologies Inc	Radeon RV250 [Mobility FireGL 9000]
radeon	ATI Technologies Inc	Radeon RV250 Lg [Radeon Mobility 9000 M9]
r128	ATI Technologies Inc	Rage Mobility M4 AGP
r128	ATI Technologies Inc	Rage Mobility M4 AGP
radeon	ATI Technologies Inc	Radeon R300 ND [Radeon 9700 Pro]
radeon	ATI Technologies Inc	Radeon R300 NE [Radeon 9500 Pro]
radeon	ATI Technologies Inc	R300 NF [Radeon 9600 TX]

radeon	ATI Technologies Inc	Radeon R300 NG [FireGL X1]
radeon	ATI Technologies Inc	Radeon R350 [Radeon 9800 Pro]
radeon	ATI Technologies Inc	Radeon R350 [Radeon 9800]
radeon	ATI Technologies Inc	R360 NJ [Radeon 9800 XT]
radeon	ATI Technologies Inc	R350 NK [FireGL X2]
radeon	ATI Technologies Inc	RV350 [Mobility Radeon 9600 M10]
radeon	ATI Technologies Inc	M10 NQ [Radeon Mobility 9600]
radeon	ATI Technologies Inc	RV350 [Mobility Radeon 9600 M10]
radeon	ATI Technologies Inc	M10 NS [Radeon Mobility 9600]
radeon	ATI Technologies Inc	M10 NT [FireGL Mobility T2]
radeon	ATI Technologies Inc	M11 NV [FireGL Mobility T2e]
r128	ATI Technologies Inc	Rage 128 PA/PRO
r128	ATI Technologies Inc	Rage 128 PB/PRO AGP 2x
r128	ATI Technologies Inc	Rage 128 PC/PRO AGP 4x
r128	ATI Technologies Inc	Rage 128 PD/PRO TMDS
r128	ATI Technologies Inc	Rage 128 PE/PRO AGP 2x TMDS
r128	ATI Technologies Inc	Rage 128 PF/PRO AGP 4x TMDS
r128	ATI Technologies Inc	Rage 128 PG/PRO
r128	ATI Technologies Inc	Rage 128 PH/PRO AGP 2x
r128	ATI Technologies Inc	Rage 128 PI/PRO AGP 4x
r128	ATI Technologies Inc	Rage 128 PJ/PRO TMDS
r128	ATI Technologies Inc	Rage 128 PK/PRO AGP 2x TMDS
r128	ATI Technologies Inc	Rage 128 PL/PRO AGP 4x TMDS
r128	ATI Technologies Inc	Rage 128 PM/PRO
r128	ATI Technologies Inc	Rage 128 PN/PRO AGP 2x
r128	ATI Technologies Inc	Rage 128 PO/PRO AGP 4x
r128	ATI Technologies Inc	Rage 128 PP/PRO TMDS [Xpert 128]
r128	ATI Technologies Inc	Rage 128 PQ/PRO AGP 2x TMDS
r128	ATI Technologies Inc	Rage 128 PR/PRO AGP 4x TMDS
r128	ATI Technologies Inc	Rage 128 PS/PRO
r128	ATI Technologies Inc	Rage 128 PT/PRO AGP 2x
r128	ATI Technologies Inc	Rage 128 PU/PRO AGP 4x
r128	ATI Technologies Inc	Rage 128 PV/PRO TMDS
r128	ATI Technologies Inc	Rage 128 PW/PRO AGP 2x TMDS
r128	ATI Technologies Inc	Rage 128 PX/PRO AGP 4x TMDS
radeon	ATI Technologies Inc	Radeon R100 QD [Radeon 7200]
radeon	ATI Technologies Inc	Radeon R100 QE
radeon	ATI Technologies Inc	Radeon R100 QF
radeon	ATI Technologies Inc	Radeon R100 QG
radeon	ATI Technologies Inc	Radeon R200 QH [Radeon 8500]
radeon	ATI Technologies Inc	Radeon R200 QL [Radeon 8500 LE]
radeon	ATI Technologies Inc	Radeon R200 QM [Radeon 9100]
radeon	ATI Technologies Inc	Radeon RV200 QW [Radeon 7500]
radeon	ATI Technologies Inc	Radeon RV200 QX [Radeon 7500]
radeon	ATI Technologies Inc	Radeon RV100 QY [Radeon 7000/VE]
radeon	ATI Technologies Inc	Radeon RV100 QZ [Radeon 7000/VE]

radeon	ATI Technologies Inc	ES1000
r128	ATI Technologies Inc	Rage 128 RE/SG
r128	ATI Technologies Inc	Rage 128 RF/SG AGP
r128	ATI Technologies Inc	Rage 128 RG
r128	ATI Technologies Inc	Rage 128 RK/VR
r128	ATI Technologies Inc	Rage 128 RL/VR AGP
r128	ATI Technologies Inc	Rage 128 SE/4x
r128	ATI Technologies Inc	Rage 128 SF/4x AGP 2x
r128	ATI Technologies Inc	Rage 128 SG/4x AGP 4x
r128	ATI Technologies Inc	Rage 128 SH
r128	ATI Technologies Inc	Rage 128 SK/4x
r128	ATI Technologies Inc	Rage 128 SL/4x AGP 2x
r128	ATI Technologies Inc	Rage 128 SM/4x AGP 4x
r128	ATI Technologies Inc	Rage 128 4x
r128	ATI Technologies Inc	Rage 128 Pro Ultra TF
r128	ATI Technologies Inc	Rage 128 Pro Ultra TL
r128	ATI Technologies Inc	Rage 128 Pro Ultra TR
r128	ATI Technologies Inc	Rage 128 Pro Ultra TS
r128	ATI Technologies Inc	Rage 128 Pro Ultra TT
r128	ATI Technologies Inc	Rage 128 Pro Ultra TU
radeon	ATI Technologies Inc	M22 [Mobility Radeon X300]
radeon	ATI Technologies Inc	M24 [Radeon Mobility X600]
radeon	ATI Technologies Inc	M22 [FireGL GL]
radeon	ATI Technologies Inc	R423 UH [Radeon X800 (PCIE)]
radeon	ATI Technologies Inc	R423 UI [Radeon X800PRO (PCIE)]
radeon	ATI Technologies Inc	R423 UJ [Radeon X800LE (PCIE)]
radeon	ATI Technologies Inc	R423 UK [Radeon X800SE (PCIE)]
radeon	ATI Technologies Inc	Radeon X800 XTP (R430) (PCIE)
radeon	ATI Technologies Inc	R430 [Radeon X800 XL] (PCIe)
radeon	ATI Technologies Inc	Radeon X800 SE (R430) (PCIE)
radeon	ATI Technologies Inc	R430 [Radeon X800 (PCIE)]
radeon	ATI Technologies Inc	R423 [FireGL V7100]
radeon	ATI Technologies Inc	R423 [FireGL V5100 (PCIE)]
radeon	ATI Technologies Inc	R423 UR [FireGL V5100 (PCIE)]
radeon	ATI Technologies Inc	R423 UT [FireGL V7100 (PCIE)]
radeon	ATI Technologies Inc	M26 [Mobility FireGL V5000]
radeon	ATI Technologies Inc	M26 [Mobility FireGL V5000]
radeon	ATI Technologies Inc	M26 [Radeon Mobility X700 XL (PCIE)]
radeon	ATI Technologies Inc	M26 [Radeon Mobility X700]
radeon	ATI Technologies Inc	Radeon Mobility X700 (PCIE)
mach64	ATI Technologies Inc	264VT [Mach64 VT]
mach64	ATI Technologies Inc	264VT3 [Mach64 VT3]
mach64	ATI Technologies Inc	264VT4 [Mach64 VT4]
radeon	ATI Technologies Inc	Radeon X550/X700 Series (RV410)
radeon	ATI Technologies Inc	Radeon 9100 IGP
radeon	ATI Technologies Inc	RS300M AGP [Radeon Mobility 9100IGP]

radeon	ATI Technologies Inc	RS480 [Radeon Xpress 200G Series]
radeon	ATI Technologies Inc	Radeon XPRESS 200M 5955 (PCIE)
radeon	ATI Technologies Inc	RV280 [Radeon 9200 PRO]
radeon	ATI Technologies Inc	RV280 [Radeon 9200]
radeon	ATI Technologies Inc	RV280 [Radeon 9200]
radeon	ATI Technologies Inc	RV280 [Radeon 9200 SE]
radeon	ATI Technologies Inc	RV280 [FireMV 2200 PCI]
radeon	ATI Technologies Inc	ES1000
radeon	ATI Technologies Inc	RS482 [Radeon Xpress 200]
radeon	ATI Technologies Inc	RS482 [Radeon Xpress 200M]
radeon	ATI Technologies Inc	RS400 [Radeon Xpress 200]
radeon	ATI Technologies Inc	RS400 [Radeon Xpress 200M]
radeon	ATI Technologies Inc	RC410 [Radeon Xpress 200]
radeon	ATI Technologies Inc	RC410 [Radeon Xpress 200M]
radeon	ATI Technologies Inc	RV370 5B60 [Radeon X300 (PCIE)]
radeon	ATI Technologies Inc	RV380 [Radeon X600 (PCIE)]
radeon	ATI Technologies Inc	RV370 [Sapphire X550 Silent]
radeon	ATI Technologies Inc	RV370 5B64 [FireGL V3100 (PCIE)]
radeon	ATI Technologies Inc	RV370 5B65 [FireGL D1100 (PCIE)]
radeon	ATI Technologies Inc	M9+ 5C61 [Radeon Mobility 9200 (AGP)]
radeon	ATI Technologies Inc	M9+ 5C63 [Radeon Mobility 9200 (AGP)]
radeon	ATI Technologies Inc	M28 [Radeon Mobility X800XT]
radeon	ATI Technologies Inc	M28 [Mobility FireGL V5100]
radeon	ATI Technologies Inc	Mobility Radeon X800
radeon	ATI Technologies Inc	Radeon X850 (PCIE)
radeon	ATI Technologies Inc	R480 [Radeon X850XT Platinum (PCIE)]
radeon	ATI Technologies Inc	Radeon X850 SE (R480) (PCIE)
radeon	ATI Technologies Inc	R480 [Radeon X800 GTO (PCIE)]
radeon	ATI Technologies Inc	FireGL V7200 (R480) (PCIE)
radeon	ATI Technologies Inc	R480 [Radeon X850XT (PCIE)] (Primary)
radeon	ATI Technologies Inc	R423 5F57 [Radeon X800XT (PCIE)]
radeon	ATI Technologies Inc	RV410 [FireGL V5000]
radeon	ATI Technologies Inc	RV410 [Radeon X700XT]
radeon	ATI Technologies Inc	RV410 [Radeon X700 Pro (PCIE)]
radeon	ATI Technologies Inc	RV410 [Radeon X700SE]
radeon	ATI Technologies Inc	RV410 [Radeon X700 (PCIE)]
radeon	ATI Technologies Inc	RV410 [Radeon X700]
radeonhd	ATI Technologies Inc	R520 [Radeon X1800]
radeon	ATI Technologies Inc	R520 [Radeon X1800]
radeonhd	ATI Technologies Inc	M58 [Radeon Mobility X1800]
radeon	ATI Technologies Inc	M58 [Radeon Mobility X1800]
radeonhd	ATI Technologies Inc	M58 [Mobility FireGL V7200]
radeon	ATI Technologies Inc	M58 [Mobility FireGL V7200]
radeonhd	ATI Technologies Inc	R520GL [FireGL V7200] (Primary)
radeon	ATI Technologies Inc	R520GL [FireGL V7200] (Primary)
radeonhd	ATI Technologies Inc	R520 [FireGL]

radeon	ATI Technologies Inc	R520 [FireGL]
radeonhd	ATI Technologies Inc	M58 [Mobility FireGL V7100]
radeon	ATI Technologies Inc	M58 [Mobility FireGL V7100]
radeonhd	ATI Technologies Inc	M58 [Radeon Mobility X1800]
radeon	ATI Technologies Inc	M58 [Radeon Mobility X1800]
radeonhd	ATI Technologies Inc	R520 [Radeon X1800]
radeon	ATI Technologies Inc	R520 [Radeon X1800]
radeonhd	ATI Technologies Inc	R520 [Radeon X1800]
radeon	ATI Technologies Inc	R520 [Radeon X1800]
radeonhd	ATI Technologies Inc	R520 [Radeon X1800]
radeon	ATI Technologies Inc	R520 [Radeon X1800]
radeonhd	ATI Technologies Inc	R520 [Radeon X1800]
radeon	ATI Technologies Inc	R520 [Radeon X1800]
radeonhd	ATI Technologies Inc	RV515 [Radeon X1600]
radeon	ATI Technologies Inc	RV515 [Radeon X1600]
radeonhd	ATI Technologies Inc	RV515 PRO [Radeon X1300/X1550 Series]
radeon	ATI Technologies Inc	RV515 PRO [Radeon X1300/X1550 Series]
radeonhd	ATI Technologies Inc	RV505 [Radeon X1550 Series]
radeon	ATI Technologies Inc	RV505 [Radeon X1550 Series]
radeonhd	ATI Technologies Inc	Radeon Mobility X1400
radeon	ATI Technologies Inc	Radeon Mobility X1400
radeonhd	ATI Technologies Inc	RV515 [Radeon X1300]
radeon	ATI Technologies Inc	RV515 [Radeon X1300]
radeonhd	ATI Technologies Inc	RV505 [Radeon X1550 64-bit]
radeon	ATI Technologies Inc	RV505 [Radeon X1550 64-bit]
radeonhd	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeon	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeonhd	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeon	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeonhd	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeon	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeonhd	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeon	ATI Technologies Inc	M52 [Mobility Radeon X1300]
radeonhd	ATI Technologies Inc	RV515 [Radeon X1300]
radeon	ATI Technologies Inc	RV515 [Radeon X1300]
radeonhd	ATI Technologies Inc	RV515LE [Radeon X1300]
radeon	ATI Technologies Inc	RV515LE [Radeon X1300]
radeonhd	ATI Technologies Inc	RV515GL [FireGL V3300] (Primary)
radeon	ATI Technologies Inc	RV515GL [FireGL V3300] (Primary)
radeonhd	ATI Technologies Inc	RV515GL [FireGL V3350]
radeon	ATI Technologies Inc	RV515GL [FireGL V3350]
radeonhd	ATI Technologies Inc	RV515 [Radeon X1300]
radeon	ATI Technologies Inc	RV515 [Radeon X1300]
radeonhd	ATI Technologies Inc	RV505 CE [Radeon X1550 64-bit]
radeon	ATI Technologies Inc	RV505 CE [Radeon X1550 64-bit]
radeonhd	ATI Technologies Inc	RV516 [Radeon X1300/X1550 Series]

radeon	ATI Technologies Inc	RV516 [Radeon X1300/X1550 Series]
radeonhd	ATI Technologies Inc	RV516 XT Radeon X1600 Series (Primary)
radeon	ATI Technologies Inc	RV516 XT Radeon X1600 Series (Primary)
radeonhd	ATI Technologies Inc	RV516 [Radeon X1300/X1550 Series]
radeon	ATI Technologies Inc	RV516 [Radeon X1300/X1550 Series]
radeonhd	ATI Technologies Inc	RV515 [Radeon Mobility X1450]
radeon	ATI Technologies Inc	RV515 [Radeon Mobility X1450]
radeonhd	ATI Technologies Inc	RV516 [Radeon X1300/X1550 Series]
radeon	ATI Technologies Inc	RV516 [Radeon X1300/X1550 Series]
radeonhd	ATI Technologies Inc	M64-S [Mobility Radeon X2300]
radeon	ATI Technologies Inc	M64-S [Mobility Radeon X2300]
radeonhd	ATI Technologies Inc	Mobility Radeon X2300
radeon	ATI Technologies Inc	Mobility Radeon X2300
radeonhd	ATI Technologies Inc	!M62CSP64 [Mobility Radeon X1350]
radeon	ATI Technologies Inc	!M62CSP64 [Mobility Radeon X1350]
radeonhd	ATI Technologies Inc	!M64CSP128 [Mobility Radeon X1450]
radeon	ATI Technologies Inc	!M64CSP128 [Mobility Radeon X1450]
radeonhd	ATI Technologies Inc	RV516 [Radeon X1550 Series]
radeon	ATI Technologies Inc	RV516 [Radeon X1550 Series]
radeonhd	ATI Technologies Inc	RV516 [Mobility Radeon X1350]
radeon	ATI Technologies Inc	RV516 [Mobility Radeon X1350]
radeonhd	ATI Technologies Inc	FireMV 2250
radeon	ATI Technologies Inc	FireMV 2250
radeonhd	ATI Technologies Inc	RV516LE [Radeon X1550 64-bit]
radeon	ATI Technologies Inc	RV516LE [Radeon X1550 64-bit]
radeonhd	ATI Technologies Inc	RV530 [Radeon X1600]
radeon	ATI Technologies Inc	RV530 [Radeon X1600]
radeonhd	ATI Technologies Inc	Radeon X1650 Pro
radeon	ATI Technologies Inc	Radeon X1650 Pro
radeonhd	ATI Technologies Inc	RV530 [Radeon X1600]
radeon	ATI Technologies Inc	RV530 [Radeon X1600]
radeonhd	ATI Technologies Inc	M56GL [Mobility FireGL V5200]
radeon	ATI Technologies Inc	M56GL [Mobility FireGL V5200]
radeonhd	ATI Technologies Inc	M56P [Radeon Mobility X1600]
radeon	ATI Technologies Inc	M56P [Radeon Mobility X1600]
radeonhd	ATI Technologies Inc	RV530LE [Radeon X1600/X1650 PRO]
radeon	ATI Technologies Inc	RV530LE [Radeon X1600/X1650 PRO]
radeonhd	ATI Technologies Inc	RV535 [Radeon X1650 Series]
radeon	ATI Technologies Inc	RV535 [Radeon X1650 Series]
radeonhd	ATI Technologies Inc	RV530LE [Radeon X1600]
radeon	ATI Technologies Inc	RV530LE [Radeon X1600]
radeonhd	ATI Technologies Inc	M56GL [Mobility FireGL V5250]
radeon	ATI Technologies Inc	M56GL [Mobility FireGL V5250]
radeonhd	ATI Technologies Inc	M66-P [Mobility Radeon X1700]
radeon	ATI Technologies Inc	M66-P [Mobility Radeon X1700]
radeonhd	ATI Technologies Inc	M66-XT [Mobility Radeon X1700]

radeon	ATI Technologies Inc	M66-XT [Mobility Radeon X1700]
radeonhd	ATI Technologies Inc	RV530LE [Radeon X1600]
radeon	ATI Technologies Inc	RV530LE [Radeon X1600]
radeonhd	ATI Technologies Inc	M71 [Mobility Radeon X2100]
radeon	ATI Technologies Inc	M71 [Mobility Radeon X2100]
radeonhd	ATI Technologies Inc	M71 [Mobility Radeon X2100] (Secondary)
radeon	ATI Technologies Inc	M71 [Mobility Radeon X2100] (Secondary)
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900 XT] (Primary)
radeon	ATI Technologies Inc	R580 [Radeon X1900 XT] (Primary)
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [Radeon X1900]
radeon	ATI Technologies Inc	R580 [Radeon X1900]
radeonhd	ATI Technologies Inc	R580 [AMD Stream Processor]
radeon	ATI Technologies Inc	R580 [AMD Stream Processor]
radeonhd	ATI Technologies Inc	RV570 [Radeon X1950 Pro]
radeon	ATI Technologies Inc	RV570 [Radeon X1950 Pro]
radeonhd	ATI Technologies Inc	Radeon X1950 GT
radeon	ATI Technologies Inc	Radeon X1950 GT
radeonhd	ATI Technologies Inc	Radeon X1650 XT (Primary) (PCIE)
radeon	ATI Technologies Inc	Radeon X1650 XT (Primary) (PCIE)
radeonhd	ATI Technologies Inc	Radeon X1650 Series
radeon	ATI Technologies Inc	Radeon X1650 Series
radeon	ATI Technologies Inc	Radeon 9100 PRO IGP
radeon	ATI Technologies Inc	Radeon Mobility 9200 IGP
radeonhd	ATI Technologies Inc	RS690 [Radeon X1200 Series]
radeon	ATI Technologies Inc	RS690 [Radeon X1200 Series]
radeonhd	ATI Technologies Inc	RS690M [Radeon X1200 Series]

radeon	ATI Technologies Inc	RS690M [Radeon X1200 Series]
radeonhd	ATI Technologies Inc	RS600 [Radeon Xpress 1200 Series]
radeon	ATI Technologies Inc	RS600 [Radeon Xpress 1200 Series]
radeonhd	ATI Technologies Inc	RS600 [Radeon Xpress 1200 Series]
radeon	ATI Technologies Inc	RS600 [Radeon Xpress 1200 Series]
radeonhd	ATI Technologies Inc	Radeon Xpress 1250
radeon	ATI Technologies Inc	Radeon Xpress 1250
radeonhd	ATI Technologies Inc	Radeon 2100
radeon	ATI Technologies Inc	Radeon 2100
radeonhd	ATI Technologies Inc	R600 [Radeon HD 2900 Series]
radeon	ATI Technologies Inc	R600 [Radeon HD 2900 Series]
radeonhd	ATI Technologies Inc	R600GL [Fire GL V8650]
radeon	ATI Technologies Inc	R600GL [Fire GL V8650]
radeonhd	ATI Technologies Inc	R600GL [Fire GL V8600]
radeon	ATI Technologies Inc	R600GL [Fire GL V8600]
radeonhd	ATI Technologies Inc	Radeon HD 2400 XT
radeon	ATI Technologies Inc	Radeon HD 2400 XT
radeonhd	ATI Technologies Inc	RV610 video device [Radeon HD 2400 PRO]
radeon	ATI Technologies Inc	RV610 video device [Radeon HD 2400 PRO]
radeonhd	ATI Technologies Inc	RV610 LE AGP [Radeon HD 2400 PRO AGP]
radeon	ATI Technologies Inc	RV610 LE AGP [Radeon HD 2400 PRO AGP]
radeonhd	ATI Technologies Inc	Radeon HD 2400 XT
radeon	ATI Technologies Inc	Radeon HD 2400 XT
radeonhd	ATI Technologies Inc	Mobility Radeon HD 2400
radeon	ATI Technologies Inc	Mobility Radeon HD 2400
radeonhd	ATI Technologies Inc	Radeon E2400
radeon	ATI Technologies Inc	Radeon E2400
radeonhd	ATI Technologies Inc	RV 610LE PCI [Radeon HD 2400]
radeon	ATI Technologies Inc	RV 610LE PCI [Radeon HD 2400]
radeonhd	ATI Technologies Inc	Radeon HD 3870
radeon	ATI Technologies Inc	Radeon HD 3870
radeonhd	ATI Technologies Inc	RV670PRO [Radeon HD 3850]
radeon	ATI Technologies Inc	RV670PRO [Radeon HD 3850]
radeonhd	ATI Technologies Inc	RV670 [Radeon HD 3850]
radeon	ATI Technologies Inc	RV670 [Radeon HD 3850]
radeonhd	ATI Technologies Inc	R680 [Radeon HD 3870 x2]
radeon	ATI Technologies Inc	R680 [Radeon HD 3870 x2]
radeonhd	ATI Technologies Inc	RV670 [FireGL 7700]
radeon	ATI Technologies Inc	RV670 [FireGL 7700]
radeonhd	ATI Technologies Inc	RV670 AGP [Radeon HD 3850]
radeon	ATI Technologies Inc	RV670 AGP [Radeon HD 3850]
radeonhd	ATI Technologies Inc	RV670 [FireStream 9170]
radeonhd	ATI Technologies Inc	M76 [Radeon Mobility HD 2600 Series]
radeon	ATI Technologies Inc	M76 [Radeon Mobility HD 2600 Series]
radeonhd	ATI Technologies Inc	RV 630 XT AGP [Radeon HD 2600 XT AGP]
radeon	ATI Technologies Inc	RV 630 XT AGP [Radeon HD 2600 XT AGP]

radeonhd	ATI Technologies Inc	RV630 PRO AGP [Radeon HD 2600 PRO AGP]
radeon	ATI Technologies Inc	RV630 PRO AGP [Radeon HD 2600 PRO AGP]
radeonhd	ATI Technologies Inc	RV630 [Radeon HD 2600XT]
radeon	ATI Technologies Inc	RV630 [Radeon HD 2600XT]
radeonhd	ATI Technologies Inc	RV630 [Radeon HD 2600 Series]
radeon	ATI Technologies Inc	RV630 [Radeon HD 2600 Series]
radeonhd	ATI Technologies Inc	RV630GL [FireGL v5600]
radeon	ATI Technologies Inc	RV630GL [FireGL v5600]
radeon	ATI Technologies Inc	Mobilitiy Radeon HD 3650
radeon	ATI Technologies Inc	Radeon Mobility HD 3670
radeonhd	ATI Technologies Inc	RV635 PRO AGP [Radeon HD 3650]
radeon	ATI Technologies Inc	RV635 PRO AGP [Radeon HD 3650]
radeonhd	ATI Technologies Inc	Mobilitiy Radeon HD 3600 Series
radeon	ATI Technologies Inc	Mobilitiy Radeon HD 3600 Series
radeonhd	ATI Technologies Inc	Mobilitiy Radeon HD 3470
radeon	ATI Technologies Inc	Mobilitiy Radeon HD 3470
radeonhd	ATI Technologies Inc	Mobilitiy Radeon HD 3400 Series
radeon	ATI Technologies Inc	Mobilitiy Radeon HD 3400 Series
radeonhd	ATI Technologies Inc	Mobilitiy Radeon HD 3450
radeon	ATI Technologies Inc	Mobilitiy Radeon HD 3450
radeon	ATI Technologies Inc	Radeon HD 3200 Graphics
radeon	ATI Technologies Inc	Radeon 3100 Graphics
radeon	ATI Technologies Inc	RS780M/RS780MN [Radeon HD 3200 Graphics]
radeon	ATI Technologies Inc	RS780MC [Radeon HD 3100 Graphics]
nsc	National Semiconductor Corporation	SCx200 Video
tseng	Tseng Labs Inc	ET4000/W32p rev A
tseng	Tseng Labs Inc	ET4000/W32p rev B
tseng	Tseng Labs Inc	ET4000/W32p rev C
tseng	Tseng Labs Inc	ET4000/W32p rev D
tseng	Tseng Labs Inc	ET6000
tga	Digital Equipment Corporation	DECchip 21030 [TGA]
tga	Digital Equipment Corporation	PBXGB [TGA2]
cirrus	Cirrus Logic	GD 7548
cirrus	Cirrus Logic	GD 5430/40 [Alpine]
cirrus	Cirrus Logic	GD 5434-4 [Alpine]
cirrus	Cirrus Logic	GD 5434-8 [Alpine]
cirrus	Cirrus Logic	GD 5436 [Alpine]
cirrus	Cirrus Logic	GD 5446
cirrus	Cirrus Logic	GD 5480
cirrus	Cirrus Logic	GD 5462
cirrus	Cirrus Logic	GD 5464 [Laguna]
cirrus	Cirrus Logic	GD 5464 BD [Laguna]
cirrus	Cirrus Logic	GD 5465 [Laguna]
trident	Trident Microsystems	CyberBlade XP4m32
trident	Trident Microsystems	!CyberBlade/i7
trident	Trident Microsystems	!CyberBlade/i7d

trident	Trident Microsystems	!CyberBlade/i1
trident	Trident Microsystems	CyberBlade i1
trident	Trident Microsystems	!CyberBlade/i1
trident	Trident Microsystems	CyberBlade XPAi1
trident	Trident Microsystems	TGUI 9320
trident	Trident Microsystems	Cyber 9388
trident	Trident Microsystems	Cyber 9397
trident	Trident Microsystems	Cyber 9397DVD
trident	Trident Microsystems	TGUI 9420
trident	Trident Microsystems	TGUI 9440
trident	Trident Microsystems	Cyber 9520
trident	Trident Microsystems	Cyber 9525
trident	Trident Microsystems	Cyber 9540
trident	Trident Microsystems	TGUI 9660/938x/968x
trident	Trident Microsystems	3DImage 9750
trident	Trident Microsystems	3DImage 9850
trident	Trident Microsystems	Blade 3D PCI/AGP
trident	Trident Microsystems	!CyberBlade/XP
mga	Matrox Graphics, Inc.	MGA 2064W [Millennium]
mga	Matrox Graphics, Inc.	MGA 1064SG [Mystique]
mga	Matrox Graphics, Inc.	MGA 2164W [Millennium II]
mga	Matrox Graphics, Inc.	MGA 2164W [Millennium II] AGP
mga	Matrox Graphics, Inc.	MGA G200
mga	Matrox Graphics, Inc.	MGA G200 AGP
mga	Matrox Graphics, Inc.	MGA G200e [Pilot] ServerEngines (SEP1)
mga	Matrox Graphics, Inc.	MGA G400/G450
mga	Matrox Graphics, Inc.	MGA G100 [Productiva]
mga	Matrox Graphics, Inc.	MGA G100 [Productiva] AGP
mga	Matrox Graphics, Inc.	MGA G550 AGP
chips	Chips and Technologies	F69000 !HiQVideo
chips	Chips and Technologies	F65545
chips	Chips and Technologies	F65548
chips	Chips and Technologies	F65550
chips	Chips and Technologies	F65554
chips	Chips and Technologies	F65555 !HiQVPro
chips	Chips and Technologies	F68554 !HiQVision
chips	Chips and Technologies	F69030
sis	Silicon Integrated Systems [SiS]	5597/5598/6326 VGA
sis	Silicon Integrated Systems [SiS]	300/305 PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	315H PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	315PRO PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	330 [Xabre] PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	SiS540 PCI Display Adapter
sis	Silicon Integrated Systems [SiS]	550 PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	630/730 PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	530/620 PCI/AGP VGA Display Adapter

sis	Silicon Integrated Systems [SiS]	65x/M650/740 PCI/AGP VGA Display Adapter
sis	Silicon Integrated Systems [SiS]	86C326 5598/6326
sis	Silicon Integrated Systems [SiS]	661/741/760 PCI/AGP or 662/761Gx PCIE VGA Display Adapter
glint	Texas Instruments	TVP4010 [Permedia]
glint	Texas Instruments	TVP4020 [Permedia 2]
i128	Number 9 Computer Company	Imagine 128
i128	Number 9 Computer Company	Imagine 128-II
i128	Number 9 Computer Company	Imagine 128 T2R [Ticket to Ride]
i128	Number 9 Computer Company	Revolution 4
cyrix	Cyrix Corporation	5510 [Grappa]
cyrix	Cyrix Corporation	5520 [Cognac]
cyrix	Cyrix Corporation	5530 Video [Kahlua]
neomagic	Neomagic Corporation	NM2070 [MagicGraph 128]
neomagic	Neomagic Corporation	NM2090 [MagicGraph 128V]
neomagic	Neomagic Corporation	NM2093 [MagicGraph 128ZV]
neomagic	Neomagic Corporation	NM2160 [MagicGraph 128XD]
neomagic	Neomagic Corporation	NM2200 [MagicGraph 256AV]
neomagic	Neomagic Corporation	NM2360 [MagicMedia 256ZX]
neomagic	Neomagic Corporation	NM2380 [MagicMedia 256XL+]
neomagic	Neomagic Corporation	NM2230 [MagicGraph 256AV+]
neomagic	Neomagic Corporation	NM2093 [MagicGraph 128ZV+]
nv	Nvidia	NV4 [RIVA TNT]
nv	Nvidia	NV5 [RIVA TNT2/TNT2 Pro]
nv	Nvidia	NV5 [RIVA TNT2 Ultra]
nv	Nvidia	NV5 [Riva TNT2]
nv	Nvidia	NV6 [Vanta/Vanta LT]
nv	Nvidia	!NV5M64 [RIVA TNT2 Model 64/Model 64 Pro]
nv	Nvidia	NV40 [GeForce 6800 Ultra]
nv	Nvidia	NV40 [GeForce 6800]
nv	Nvidia	NV40.2 [GeForce 6800 LE]
nv	Nvidia	NV40.3 [GeForce 6800 XE]
nv	Nvidia	NV40 [GeForce 6800 XT]
nv	Nvidia	NV40 [GeForce 6800 GT]
nv	Nvidia	NV40 [GeForce 6800 GT]
nv	Nvidia	NV40 [GeForce 6800 GS]
nv	Nvidia	NV40 [GeForce 6800 XT]
nv	Nvidia	NV40GL [Quadro FX 4000]
nv	Nvidia	G70 [GeForce 7800 GTX]
nv	Nvidia	G70 [GeForce 7800 GTX]
nv	Nvidia	G70 [GeForce 7800 GT]
nv	Nvidia	G70 [GeForce 7800 GS]
nv	Nvidia	GeForce 7800 SLI
nv	Nvidia	G70 [GeForce Go 7800]
nv	Nvidia	G70 [GeForce Go 7800 GTX]
nv	Nvidia	G70GL [Quadro FX 4500]
nv	Nvidia	NV5 [Aladdin TNT2]

nv	Nvidia	NV41 [GeForce 6800 GS]
nv	Nvidia	NV41.1 [GeForce 6800]
nv	Nvidia	NV41.2 [GeForce 6800 LE]
nv	Nvidia	NV42 [GeForce 6800 XT]
nv	Nvidia	NV41.8 [GeForce Go 6800]
nv	Nvidia	NV41.9 [GeForce Go 6800 Ultra]
nv	Nvidia	NV41 [Quadro FX Go1400]
nv	Nvidia	NV41 [Quadro FX 3450/4000 SDI]
nv	Nvidia	NV41GL [Quadro FX 1400]
nv	Nvidia	NV10 [GeForce 256 SDR]
nv	Nvidia	NV10DDR [GeForce 256 DDR]
nv	Nvidia	NV10GL [Quadro]
nv	Nvidia	NV11 [GeForce2 MX/MX 400]
nv	Nvidia	NV11DDR [GeForce2 MX200]
nv	Nvidia	NV11 [GeForce2 Go]
nv	Nvidia	NV11GL [Quadro2 MXR/EX/Go]
nv	Nvidia	NV43 [GeForce 6600 GT]
nv	Nvidia	NV43 [GeForce 6600]
nv	Nvidia	NV43 [GeForce 6600 LE]
nv	Nvidia	NV43 [GeForce 6600 VE]
nv	Nvidia	NV43 [GeForce Go 6600]
nv	Nvidia	NV43 [GeForce 6610 XL]
nv	Nvidia	NV43 [Geforce Go 6600TE/6200TE]
nv	Nvidia	GeForce 6700 XL
nv	Nvidia	NV43 [GeForce Go 6600]
nv	Nvidia	NV43 [GeForce Go 6600 GT]
nv	Nvidia	Quadro FX 540 MXM
nv	Nvidia	NV43GL [Quadro FX 550]
nv	Nvidia	NV43GL [Quadro FX 540]
nv	Nvidia	NV43 [GeForce 6200]
nv	Nvidia	NV15 [GeForce2 GTS/Pro]
nv	Nvidia	NV15DDR [GeForce2 Ti]
nv	Nvidia	NV15BR [GeForce2 Ultra, Bladerunner]
nv	Nvidia	NV15GL [Quadro2 Pro]
nv	Nvidia	GeForce 6500
nv	Nvidia	NV44 [GeForce 6200 TurboCache(TM)]
nv	Nvidia	NV44 [GeForce 6200SE TurboCache (TM)]
nv	Nvidia	NV44 [GeForce 6200 LE]
nv	Nvidia	NV44 [GeForce Go 6200]
nv	Nvidia	NV44 [Quadro NVS 285]
nv	Nvidia	NV43 [GeForce Go 6400]
nv	Nvidia	NV43 [GeForce Go 6200/6400]
nv	Nvidia	NV43 [GeForce Go 6200/6400]
nv	Nvidia	GeForce 6250
nv	Nvidia	NV17 [GeForce4 MX 460]
nv	Nvidia	NV17 [GeForce4 MX 440]

nv	Nvidia	NV17 [GeForce4 MX 420]
nv	Nvidia	NV17 [GeForce4 MX 440-SE]
nv	Nvidia	NV17 [GeForce4 440 Go]
nv	Nvidia	NV17 [GeForce4 420 Go]
nv	Nvidia	NV17 [GeForce4 420 Go 32M]
nv	Nvidia	NV17 [GeForce4 460 Go]
nv	Nvidia	NV17GL [Quadro4 550 XGL]
nv	Nvidia	NV17 [GeForce4 440 Go 64M]
nv	Nvidia	NV17GL [Quadro NVS]
nv	Nvidia	NV17GL [Quadro4 500 GoGL]
nv	Nvidia	NV17 [GeForce4 410 Go 16M]
nv	Nvidia	NV18 [GeForce4 MX 440 AGP 8x]
nv	Nvidia	NV18 [GeForce4 MX 440SE AGP 8x]
nv	Nvidia	NV18 [GeForce4 MX 420 AGP 8x]
nv	Nvidia	NV18 [GeForce4 MX 4000]
nv	Nvidia	NV18M [GeForce4 448 Go]
nv	Nvidia	NV18M [GeForce4 488 Go]
nv	Nvidia	NV18GL [Quadro4 580 XGL]
nv	Nvidia	NV18GL [Quadro NVS 280 SD]
nv	Nvidia	NV18GL [Quadro4 380 XGL]
nv	Nvidia	NV18GL [Quadro NVS 50 PCI]
nv	Nvidia	NV18M [GeForce4 448 Go]
nv	Nvidia	G80 [GeForce 8800 GTX]
nv	Nvidia	G80 [GeForce 8800 GTS]
nv	Nvidia	GeForce 8800 Ultra
nv	Nvidia	G80 [Quadro FX 5600]
nv	Nvidia	G80 [Quadro FX 4600]
nv	Nvidia	NVCrush11 [GeForce2 MX Integrated Graphics]
nv	Nvidia	GeForce 7350 LE
nv	Nvidia	G72 [GeForce 7300 LE]
nv	Nvidia	G72 [GeForce 7300 SE]
nv	Nvidia	GeForce Go 7200
nv	Nvidia	G72M [Quadro NVS 110M/!?GeForce Go 7300]
nv	Nvidia	G72M [GeForce Go 7400]
nv	Nvidia	G72M [Quadro NVS 110M]
nv	Nvidia	Quadro NVS 120M
nv	Nvidia	G72GL [Quadro FX 350M]
nv	Nvidia	G72 [GeForce 7500 LE]
nv	Nvidia	G72GL [Quadro FX 350]
nv	Nvidia	G71 [GeForce 7300 GS]
nv	Nvidia	NV18 [GeForce4 MX - nForce GPU]
nv	Nvidia	NV20 [GeForce3]
nv	Nvidia	NV20 [GeForce3 Ti 200]
nv	Nvidia	NV20 [GeForce3 Ti 500]
nv	Nvidia	NV20DCC [Quadro DCC]
nv	Nvidia	NV40 [GeForce 6800]

nv	Nvidia	NV40 [GeForce 6800 LE]
nv	Nvidia	NV40 [GeForce 6800 GT]
nv	Nvidia	NV40 [GeForce 6800 XT]
nv	Nvidia	NV44A [GeForce 6200]
nv	Nvidia	GeForce 6200 A-LE
nv	Nvidia	C51PV [GeForce 6150]
nv	Nvidia	C51 [GeForce 6150 LE]
nv	Nvidia	C51G [GeForce 6100]
nv	Nvidia	C51 [Geforce 6150 Go]
nv	Nvidia	MCP51 PCI-X GeForce Go 6100
nv	Nvidia	NV25 [GeForce4 Ti 4600]
nv	Nvidia	NV25 [GeForce4 Ti 4400]
nv	Nvidia	NV25 [GeForce4 Ti 4200]
nv	Nvidia	NV25GL [Quadro4 900 XGL]
nv	Nvidia	NV25GL [Quadro4 750 XGL]
nv	Nvidia	NV25GL [Quadro4 700 XGL]
nv	Nvidia	NV28 [GeForce4 Ti 4800]
nv	Nvidia	NV28 [GeForce4 Ti 4200 AGP 8x]
nv	Nvidia	NV28 [GeForce4 Ti 4800 SE]
nv	Nvidia	NV28 [GeForce4 Ti 4200 Go AGP 8x]
nv	Nvidia	NV28GL [Quadro4 980 XGL]
nv	Nvidia	NV28GL [Quadro4 780 XGL]
nv	Nvidia	NV28GLM [Quadro4 Go700]
nv	Nvidia	G71 [GeForce 7900 GTX]
nv	Nvidia	G71 [GeForce 7900 GT/GTO]
nv	Nvidia	G71 [GeForce 7900 GS]
nv	Nvidia	GeForce Go 7900 GS
nv	Nvidia	GeForce Go 7900 GTX
nv	Nvidia	G71 [Quadro FX 2500M]
nv	Nvidia	G71 [Quadro FX 1500M]
nv	Nvidia	G71 [Quadro FX 5500]
nv	Nvidia	G71GL [Quadro FX 3500]
nv	Nvidia	G71 [Quadro FX 1500]
nv	Nvidia	G70 [Quadro FX 4500 X2]
nv	Nvidia	NV30 [GeForce FX]
nv	Nvidia	NV30 [GeForce FX 5800 Ultra]
nv	Nvidia	NV30 [GeForce FX 5800]
nv	Nvidia	NV30GL [Quadro FX 2000]
nv	Nvidia	NV30GL [Quadro FX 1000]
nv	Nvidia	NV31 [GeForce FX 5600 Ultra]
nv	Nvidia	NV31 [GeForce FX 5600]
nv	Nvidia	NV31 [GeForce FX 5600XT]
nv	Nvidia	NV31M [GeForce FX Go5600]
nv	Nvidia	NV31M [GeForce FX Go5650]
nv	Nvidia	Quadro FX Go700
nv	Nvidia	NV34 [GeForce FX 5200]

nv	Nvidia	NV34 [GeForce FX 5200 Ultra]
nv	Nvidia	NV34 [GeForce FX 5200]
nv	Nvidia	NV34 [GeForce FX 5200LE]
nv	Nvidia	NV34M [GeForce FX Go5200 64M]
nv	Nvidia	NV34M [GeForce FX Go5250]
nv	Nvidia	NV34 [GeForce FX 5500]
nv	Nvidia	NV34 [GeForce FX 5100]
nv	Nvidia	NV34M [GeForce FX Go5200 32M/64M]
nv	Nvidia	NV34M [GeForce FX Go5200]
nv	Nvidia	NV34GL [Quadro NVS 280 PCI]
nv	Nvidia	NV34GL [Quadro FX 500/600 PCI]
nv	Nvidia	NV34GLM [GeForce FX Go 5300]
nv	Nvidia	NV34 [GeForce FX Go5100]
nv	Nvidia	NV35 [GeForce FX 5900 Ultra]
nv	Nvidia	NV35 [GeForce FX 5900]
nv	Nvidia	NV35 [GeForce FX 5900XT]
nv	Nvidia	NV38 [GeForce FX 5950 Ultra]
nv	Nvidia	NV35 [GeForce FX 5900ZT]
nv	Nvidia	NV35GL [Quadro FX 3000]
nv	Nvidia	NV35GL [Quadro FX 700]
nv	Nvidia	NV36.1 [GeForce FX 5700 Ultra]
nv	Nvidia	NV36.2 [GeForce FX 5700]
nv	Nvidia	NV36 [GeForce FX 5700LE]
nv	Nvidia	NV36.4 [GeForce FX 5700VE]
nv	Nvidia	NV36 [GeForce FX Go5700]
nv	Nvidia	NV36 [GeForce FX Go5700]
nv	Nvidia	NV36 [Quadro FX Go1000]
nv	Nvidia	NV36GL [Quadro FX 1100]
nv	Nvidia	GeForce 7650 GS
nv	Nvidia	G70 [GeForce 7600 GT]
nv	Nvidia	G70 [GeForce 7600 GS]
nv	Nvidia	G70 [GeForce 7300 GT]
nv	Nvidia	G70 [GeForce 7600 LE]
nv	Nvidia	G70 [GeForce 7300 GT]
nv	Nvidia	GeForce Go 7700
nv	Nvidia	G70 [GeForce Go 7600]
nv	Nvidia	GeForce Go 7600 GT
nv	Nvidia	GeForce Go 7900 SE
nv	Nvidia	Quadro FX 550M
nv	Nvidia	G73GL [Quadro FX 560]
nv	Nvidia	GeForce 6150SE nForce 430
nv	Nvidia	GeForce 8600 GTS
nv	Nvidia	GeForce 8600GT
nv	Nvidia	GeForce 8600 GT
nv	Nvidia	GeForce 8400 GS
nv	Nvidia	GeForce 9500M GS

nv	Nvidia	GeForce 8600M GT
nv	Nvidia	GeForce 9650M GS
nv	Nvidia	GeForce 8700M GT
nv	Nvidia	Quadro FX 370
nv	Nvidia	Quadro NVS 320M
nv	Nvidia	Quadro FX 570M
nv	Nvidia	Quadro FX 1600M
nv	Nvidia	Quadro FX 570
nv	Nvidia	Quadro FX 1700
nv	Nvidia	GeForce 8400 SE
nv	Nvidia	GeForce 8500 GT
nv	Nvidia	GeForce 8400 GS
nv	Nvidia	GeForce 8300 GS
nv	Nvidia	GeForce 8400 GS
nv	Nvidia	GeForce 8600M GS
nv	Nvidia	G86M [GeForce 8400M GT]
nv	Nvidia	GeForce 8400M GS
nv	Nvidia	GeForce 8400M G
nv	Nvidia	Quadro NVS 140M
nv	Nvidia	Quadro NVS 130M
nv	Nvidia	Quadro NVS 135M
nv	Nvidia	Quadro FX 360M
nv	Nvidia	GeForce 9300M G
nv	Nvidia	Quadro NVS 290
nv	Nvidia	GeForce 8800 GTS 512
nv	Nvidia	GeForce 8800 GT 512
nv	Nvidia	GeForce 9800 GX2
nv	Nvidia	GeForce 8800 GS
nv	Nvidia	GeForce 8800M GTS
nv	Nvidia	GeForce 8800M GTX
nv	Nvidia	GeForce 8800 GS
nv	Nvidia	GeForce 9600 GSO
nv	Nvidia	GeForce 8800 GT
nv	Nvidia	GeForce 9800 GTX
nv	Nvidia	Quadro FX 3700
nv	Nvidia	Quadro FX 3600M
nv	Nvidia	G94 [GeForce 9600 GT]
nv	Nvidia	GeForce 9600M GT
nv	Nvidia	GeForce 9600M GS
nv	Nvidia	GeForce 9600M GT
nv	Nvidia	GeForce 9500M G
nv	Nvidia	GeForce 8400 GS
nv	Nvidia	GeForce 9300M GS
nv	Nvidia	GeForce 9200M GS
nv	Nvidia	GeForce 9300M GS
imstt	Integrated Micro Solutions Inc.	IMS9128 [Twin turbo 128]

via	VIA Technologies, Inc.	!K8M800/!K8N800/!K8N800A [S3 UniChrome Pro]
via	VIA Technologies, Inc.	CN400/PM800/PM880/PN800/PN880 [S3 UniChrome Pro]
via	VIA Technologies, Inc.	VT8623 [Apollo CLE266] integrated CastleRock graphics
via	VIA Technologies, Inc.	CN700/!?P4M800 Pro/!?P4M800 CE/VN800 [S3 UniChrome Pro]
via	VIA Technologies, Inc.	KM400/KN400/!?P4M800 [S3 UniChrome]
apm	Alliance Semiconductor Corporation	ProVideo 6422
apm	Alliance Semiconductor Corporation	ProVideo 6424
apm	Alliance Semiconductor Corporation	ProMotion AT3D
rendition	Rendition	Verite 1000
rendition	Rendition	Verite V2000/V2100/V2200
voodoo	3Dfx Interactive, Inc.	Voodoo
voodoo	3Dfx Interactive, Inc.	Voodoo 2
tdfx	3Dfx Interactive, Inc.	Voodoo Banshee
tdfx	3Dfx Interactive, Inc.	Voodoo 3
tdfx	3Dfx Interactive, Inc.	Voodoo 4 / Voodoo 5
siliconmotion	Silicon Motion, Inc.	SM710 LynxEM
siliconmotion	Silicon Motion, Inc.	SM712 LynxEM+
siliconmotion	Silicon Motion, Inc.	SM720 Lynx3DM
siliconmotion	Silicon Motion, Inc.	SM731 Cougar3DR
siliconmotion	Silicon Motion, Inc.	SM810 LynxE
siliconmotion	Silicon Motion, Inc.	SM820 Lynx3D
siliconmotion	Silicon Motion, Inc.	SM910
nv	NVidia / SGS Thomson (Joint Venture)	Riva128
vmware	VMware Inc	Abstract SVGA II Adapter
vmware	VMware Inc	Abstract SVGA Adapter
glint	3DLabs	GLINT 300SX
glint	3DLabs	GLINT 500TX
glint	3DLabs	GLINT Delta
glint	3DLabs	Permedia
glint	3DLabs	GLINT MX
glint	3DLabs	3D Extreme
glint	3DLabs	GLINT Gamma G1
glint	3DLabs	Permedia II 2D+3D
glint	3DLabs	GLINT R3
glint	3DLabs	GLINT R3 [Oxygen VX1]
glint	3DLabs	GLint R4 rev A
glint	3DLabs	GLINT Gamma G2
s3virge	S3 Inc.	86c325 [ViRGE]
s3	S3 Inc.	86c764/765 [Trio32/64/64V+]
s3	S3 Inc.	86cM65 [Aurora64V+]
s3	S3 Inc.	86c767 [Trio 64UV+]
s3virge	S3 Inc.	86c988 [ViRGE/VX]
s3	S3 Inc.	86c964 [Vision 964 VRAM] vers 0
s3	S3 Inc.	86c964 [Vision 964 VRAM] vers 1
s3	S3 Inc.	86c968 [Vision 968 VRAM] rev 0
s3	S3 Inc.	86c775/86c785 [Trio 64V2/DX or /GX]

s3virge	S3 Inc.	Trio 64 3D
s3virge	S3 Inc.	ViRGE/DX or /GX
s3virge	S3 Inc.	ViRGE/GX2
s3virge	S3 Inc.	86c368 [Trio 3D/2X]
savage	S3 Inc.	86c794 [Savage 3D]
savage	S3 Inc.	86c390 [Savage 3D/MV]
savage	S3 Inc.	Savage 4
savage	S3 Inc.	ProSavage PM133
savage	S3 Inc.	ProSavage KM133
s3virge	S3 Inc.	ViRGE/MX
s3virge	S3 Inc.	ViRGE/MX+MV
savage	S3 Inc.	86C270-294 Savage/MX-MV
savage	S3 Inc.	82C270-294 Savage/MX
savage	S3 Inc.	86C270-294 Savage/IX-MV
savage	S3 Inc.	86C270-294 Savage/IX
savage	S3 Inc.	SuperSavage MX/128
savage	S3 Inc.	SuperSavage MX/64
savage	S3 Inc.	SuperSavage MX/64C
savage	S3 Inc.	SuperSavage IX/128 SDR
savage	S3 Inc.	SuperSavage IX/128 DDR
savage	S3 Inc.	SuperSavage IX/64 SDR
savage	S3 Inc.	SuperSavage IX/64 DDR
savage	S3 Inc.	SuperSavage IX/C SDR
savage	S3 Inc.	SuperSavage IX/C DDR
savage	S3 Inc.	86C380 [!ProSavageDDR K4M266]
savage	S3 Inc.	VT8636A [ProSavage KN133] AGP4X VGA Controller (TwisterK)
savage	S3 Inc.	VT8751 [!ProSavageDDR P4M266]
savage	S3 Inc.	VT8375 [ProSavage8 KM266/KL266]
savage	S3 Inc.	86C410 Savage 2000
intel	Intel Corporation	82815 815 Chipset Host Bridge and Memory Controller Hub
intel	Intel Corporation	82815 Chipset Graphics Controller (CGC)
intel	Intel Corporation	82845G/GL[Brookdale-G]/GE/PE DRAM Controller/Host-Hub Interface
intel	Intel Corporation	82845G/GL[Brookdale-G]/GE Chipset Integrated Graphics Device
intel	Intel Corporation	82865G/PE/P DRAM Controller/Host-Hub Interface
intel	Intel Corporation	82865G Integrated Graphics Controller
intel	Intel Corporation	82915G/P/GV/GL/PL/910GL Memory Controller Hub
intel	Intel Corporation	82915G/P/GV/GL/PL/910GL Memory Controller Hub
intel	Intel Corporation	82915G/GV/910GL Integrated Graphics Controller
intel	Intel Corporation	E7221 Integrated Graphics Controller
intel	Intel Corporation	Mobile 915GM/PM/GMS/910GML Express Processor to DRAM Controller
intel	Intel Corporation	Mobile 915GM/GMS/910GML Express Graphics Controller
intel	Intel Corporation	82945G/GZ/P/PL Memory Controller Hub
intel	Intel Corporation	82945G/GZ Integrated Graphics Controller
intel	Intel Corporation	Mobile 945GM/PM/GMS, 943/940GML and 945GT Express Memory Controller Hub
intel	Intel Corporation	Mobile 945GM/GMS, 943/940GML Express Integrated Graphics Controller
intel	Intel Corporation	Mobile 945GME Express Memory Controller Hub

intel	Intel Corporation	Mobile 945GME Express Integrated Graphics Controller
intel	Intel Corporation	82946GZ/PL/GL Memory Controller Hub
intel	Intel Corporation	82946GZ/GL Integrated Graphics Controller
intel	Intel Corporation	82G35 Express DRAM Controller
intel	Intel Corporation	82G35 Express Integrated Graphics Controller
intel	Intel Corporation	82Q963/Q965 Memory Controller Hub
intel	Intel Corporation	82Q963/Q965 Integrated Graphics Controller
intel	Intel Corporation	82P965/G965 Memory Controller Hub
intel	Intel Corporation	82G965 Integrated Graphics Controller
intel	Intel Corporation	82Q35 Express DRAM Controller
intel	Intel Corporation	82Q35 Express Integrated Graphics Controller
intel	Intel Corporation	82G33/G31/P35/P31 Express DRAM Controller
intel	Intel Corporation	82G33/G31 Express Integrated Graphics Controller
intel	Intel Corporation	82Q33 Express DRAM Controller
intel	Intel Corporation	82Q33 Express Integrated Graphics Controller
intel	Intel Corporation	Mobile PM965/GM965/GL960 Memory Controller Hub
intel	Intel Corporation	Mobile GM965/GL960 Integrated Graphics Controller
intel	Intel Corporation	Mobile GME965/GLE960 Memory Controller Hub
intel	Intel Corporation	Mobile GME965/GLE960 Integrated Graphics Controller
intel	Intel Corporation	Mobile 4 Series Chipset Memory Controller Hub
intel	Intel Corporation	Mobile 4 Series Chipset Integrated Graphics Controller
intel	Intel Corporation	Eaglelake DRAM Controller
intel	Intel Corporation	Eaglelake Integrated Graphics Controller
intel	Intel Corporation	Eaglelake DRAM Controller
intel	Intel Corporation	Eaglelake Integrated Graphics Controller
intel	Intel Corporation	Eaglelake DRAM Controller
intel	Intel Corporation	Eaglelake Integrated Graphics Controller
intel	Intel Corporation	82830 830 Chipset Host Bridge
intel	Intel Corporation	82830 CGC [Chipset Graphics Controller]
intel	Intel Corporation	82852/82855 GM/GME/PM/GMV Processor to I/O Controller
intel	Intel Corporation	82852/855GM Integrated Graphics Device
intel	Intel Corporation	82810 GMCH (Graphics Memory Controller Hub)
intel	Intel Corporation	82810 (CGC) Chipset Graphics Controller
intel	Intel Corporation	82810 DC-100 (GMCH) Graphics Memory Controller Hub
intel	Intel Corporation	82810 DC-100 (CGC) Chipset Graphics Controller
intel	Intel Corporation	82810E DC-133 (GMCH) Graphics Memory Controller Hub
intel	Intel Corporation	82810E DC-133 (CGC) Chipset Graphics Controller
i740	Intel Corporation	82740 (i740) AGP Graphics Accelerator
ark	ARK Logic Inc	1000PV [Stingray]
ark	ARK Logic Inc	2000PV [Stingray]
ark	ARK Logic Inc	2000MT

Список сетевых карт, поддерживаемых РЕД ОС

Производитель	Марка оборудования
SpeedStream	1012 PCMCIA 10/100 Ethernet Card [RTL81xx]
LSI Logic / Symbios Logic	83C885 NT50 DigitalScape Fast Ethernet
LSI Logic / Symbios Logic	Yellowfin G-NIC gigabit ethernet
National Semiconductor Corporation	DP83815 (MacPhyter) Ethernet Controller
National Semiconductor Corporation	DP83815 (MacPhyter) Ethernet Controller
National Semiconductor Corporation	DP83820 10/100/1000 Ethernet Controller
National Semiconductor Corporation	DP83065 [Saturn] 10/100/1000 Ethernet Controller
Digital Equipment Corporation	Farallon PN9000SX Gigabit Ethernet
AT&T GIS (NCR)	100VG ethernet
Advanced Micro Devices [AMD]	AMD-8111 Ethernet
Silicon Integrated Systems [SiS]	190 Ethernet Adapter
Silicon Integrated Systems [SiS]	191 Gigabit Ethernet Adapter
Silicon Integrated Systems [SiS]	SiS900 PCI Fast Ethernet
Silicon Integrated Systems [SiS]	SiS7016 PCI Fast Ethernet Adapter
STMicroelectronics	21x4x DEC-Tulip compatible 10/100 Ethernet
STMicroelectronics	21x4x DEC-Tulip compatible 10/100 Ethernet
Apple Computer Inc.	Tigon3 Gigabit Ethernet NIC (BCM5701)
QLogic Corp.	ISP4022-based Ethernet NIC
QLogic Corp.	ISP4032-based Ethernet IPv6 NIC
Sun Microsystems Computer Corp.	Happy Meal 10/100 Ethernet [hme]
Sun Microsystems Computer Corp.	RIO 10/100 Ethernet [eri]
Sun Microsystems Computer Corp.	GEM 10/100/1000 Ethernet [ge]
Sun Microsystems Computer Corp.	Multithreaded 10 Gigabit Ethernet Network Controller
Silicon Graphics, Inc.	AceNIC Gigabit Ethernet
3Com Corporation	3c900B-TPO Etherlink XL [Cyclone]
3Com Corporation	3c900B-Combo Etherlink XL [Cyclone]
3Com Corporation	3c900B-TPC Etherlink XL [Cyclone]
3Com Corporation	3c905B-T4 Fast EtherLink XL [Cyclone]
3Com Corporation	3c905B Deluxe Etherlink 10/100/BNC [Cyclone]
3Com Corporation	3c905B-FX Fast Etherlink XL FX 100baseFx [Cyclone]
3Com Corporation	3C920B-EMB Integrated Fast Ethernet Controller [Tornado]
3Com Corporation	3Com 3C920B-EMB-WNM Integrated Fast Ethernet Controller
3Com Corporation	3C920B-EMB-WNM Integrated Fast Ethernet Controller
3Com Corporation	3c980-TX Fast Etherlink XL Server Adapter [Cyclone]
Standard Microsystems Corp [SMC]	83c170 EPIC/100 Fast Ethernet Adapter
Standard Microsystems Corp [SMC]	83c170 EPIC/100 Fast Ethernet Adapter
Standard Microsystems Corp [SMC]	83c175 EPIC/100 Fast Ethernet Adapter
ALi Corporation	M5261 Ethernet Controller
ALi Corporation	ULi 1689,1573 integrated ethernet.
nVidia Corporation	MCP04 Ethernet Controller
nVidia Corporation	MCP04 Ethernet Controller
nVidia Corporation	CK804 Ethernet Controller
nVidia Corporation	CK804 Ethernet Controller
nVidia Corporation	nForce2 Ethernet Controller

Производитель	Марка оборудования
nVidia Corporation	MCP2A Ethernet Controller
nVidia Corporation	MCP2A Ethernet Controller
nVidia Corporation	nForce3 Ethernet
nVidia Corporation	CK8S Ethernet Controller
nVidia Corporation	CK8S Ethernet Controller
nVidia Corporation	nForce Ethernet Controller
nVidia Corporation	MCP51 Ethernet Controller
nVidia Corporation	MCP51 Ethernet Controller
nVidia Corporation	MCP55 Ethernet
nVidia Corporation	MCP55 Ethernet
nVidia Corporation	MCP61 Ethernet
nVidia Corporation	MCP61 Ethernet
nVidia Corporation	MCP61 Ethernet
nVidia Corporation	MCP61 Ethernet
nVidia Corporation	MCP65 Ethernet
nVidia Corporation	MCP65 Ethernet
nVidia Corporation	MCP65 Ethernet
nVidia Corporation	MCP65 Ethernet
nVidia Corporation	MCP67 Ethernet
nVidia Corporation	MCP67 Ethernet
nVidia Corporation	MCP67 Ethernet
nVidia Corporation	MCP67 Ethernet
nVidia Corporation	MCP78S [GeForce 8200] Ethernet
nVidia Corporation	MCP77 Ethernet
nVidia Corporation	MCP77 Ethernet
nVidia Corporation	MCP77 Ethernet
nVidia Corporation	MCP73 Ethernet
nVidia Corporation	MCP73 Ethernet
nVidia Corporation	MCP73 Ethernet
nVidia Corporation	MCP73 Ethernet
nVidia Corporation	MCP79 Ethernet
nVidia Corporation	MCP79 Ethernet
nVidia Corporation	MCP79 Ethernet
nVidia Corporation	MCP79 Ethernet
Realtek Semiconductor Co., Ltd.	RTL8101E/RTL8102E PCI Express Fast Ethernet controller
Realtek Semiconductor Co., Ltd.	RT8139 (B/C) Cardbus Fast Ethernet Adapter
Realtek Semiconductor Co., Ltd.	RTL-8110SC/8169SC Gigabit Ethernet
Realtek Semiconductor Co., Ltd.	RTL8111/8168B PCI Express Gigabit Ethernet controller
Realtek Semiconductor Co., Ltd.	RTL-8169 Gigabit Ethernet
VIA Technologies, Inc.	VT6120/VT6121/VT6122 Gigabit Ethernet Adapter
Accton Technology Corporation	EN-1216 Ethernet Adapter
Accton Technology Corporation	EN-1217 Ethernet Adapter
Accton Technology Corporation	21x4x DEC-Tulip compatible Fast Ethernet
SysKonnect	SK-9872 Gigabit Ethernet Server Adapter (SK-NET GE-ZX dual link)
SysKonnect	SK-9871 V2.0 Gigabit Ethernet 1000Base-ZX Adapter, PCI64, Fiber ZX/SC

Производитель	Марка оборудования
SysKonnect	SK-9Dxx Gigabit Ethernet Adapter
SysKonnect	SK-9Mxx Gigabit Ethernet Adapter
Xircom	Cardbus Ethernet 10/100
D-Link System Inc	DL10050 Sundance Ethernet
D-Link System Inc	DL10050 Sundance Ethernet
D-Link System Inc	DL10050 Sundance Ethernet
D-Link System Inc	DL10050 Sundance Ethernet
D-Link System Inc	DL10050 Sundance Ethernet
D-Link System Inc	RTL8139 Ethernet
D-Link System Inc	DL2000-based Gigabit Ethernet
D-Link System Inc	DL2000-based Gigabit Ethernet
D-Link System Inc	DGE-550SX PCI-X Gigabit Ethernet Adapter
D-Link System Inc	DGE-528T Gigabit Ethernet Adapter
D-Link System Inc	DGE-560T PCI Express Gigabit Ethernet Adapter
D-Link System Inc	DGE-530T Gigabit Ethernet Adapter (rev 11)
D-Link System Inc	DGE-560SX PCI Express Gigabit Ethernet Adapter
D-Link System Inc	DGE-550T Gigabit Ethernet Adapter V.B1
D-Link System Inc	Gigabit Ethernet Adapter
Marvell Technology Group Ltd.	88E8001 Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8021 PCI-X IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8022 PCI-X IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8061 PCI-E IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8062 PCI-E IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8021 PCI-X IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8022 PCI-X IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8061 PCI-E IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8062 PCI-E IPMI Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8035 PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88E8036 PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88E8038 PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88E8039 PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88E8040 PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88E8040T PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88EC033 Ethernet Controller
Marvell Technology Group Ltd.	88E8048 PCI-E Fast Ethernet Controller
Marvell Technology Group Ltd.	88E8052 PCI-E ASF Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8050 PCI-E ASF Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8053 PCI-E Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8055 PCI-E Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8056 PCI-E Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8070 based Ethernet Controller
Marvell Technology Group Ltd.	88EC036 PCI-E Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88EC032 Ethernet Controller
Marvell Technology Group Ltd.	88EC034 Ethernet Controller
Marvell Technology Group Ltd.	88EC042 Ethernet Controller

Производитель	Марка оборудования
Marvell Technology Group Ltd.	Marvell Yukon 88E8058 PCI-E Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8071 PCI-E Gigabit Ethernet Controller
Marvell Technology Group Ltd.	88E8075 PCI-E Gigabit Ethernet Controller
Lite-On Communications Inc	LNE100TX [Linksys EtherFast 10/100]
Compex	RL100TX Fast Ethernet
Allied Telesyn International	RTL81xx Fast Ethernet
Allied Telesyn International	RTL81xx Fast Ethernet
Allied Telesyn International	21x4x DEC-Tulip compatible 10/100 Ethernet
Asix Electronics Corporation	AX88141 Fast Ethernet Controller
Davicom Semiconductor, Inc.	Ethernet 100/10 MBit
Davicom Semiconductor, Inc.	21x4x DEC-Tulip compatible 10/100 Ethernet
Davicom Semiconductor, Inc.	21x4x DEC-Tulip compatible 10/100 Ethernet
Davicom Semiconductor, Inc.	21x4x DEC-Tulip compatible 10/100 Ethernet
Davicom Semiconductor, Inc.	21x4x DEC-Tulip compatible 10/100 Ethernet
Davicom Semiconductor, Inc.	Ethernet 100/10 MBit
Alteon Networks Inc.	AceNIC Gigabit Ethernet
Alteon Networks Inc.	AceNIC Gigabit Ethernet (Copper)
Alteon Networks Inc.	Farallon PN9100-T Gigabit Ethernet
Holtek Microelectronics Inc	PCI NE2K Ethernet
Holtek Microelectronics Inc	PCI NE2K Ethernet
ADMtek	21x4x DEC-Tulip compatible 10/100 Ethernet
ADMtek	NC100 Network Everywhere Fast Ethernet 10/100
ADMtek	21x4x DEC-Tulip compatible 10/100 Ethernet
ADMtek	21x4x DEC-Tulip compatible 10/100 Ethernet
Packet Engines Inc.	GNIC-II PCI Gigabit Ethernet [Hamachi]
Netgear	GA620 Gigabit Ethernet
Netgear	GA630 Gigabit Ethernet
Abocom Systems Inc	ADMtek Centaur-C rev 17 [D-Link DFE-680TX] CardBus Fast Ethernet Adapter
Abocom Systems Inc	21x4x DEC-Tulip compatible 10/100 Ethernet
Abocom Systems Inc	RTL8139 [FE2000VX] CardBus Fast Ethernet Attached Port Adapter
Abocom Systems Inc	21x4x DEC-Tulip compatible 10/100 Ethernet
Sundance Technology Inc / IC Plus Corp	IC Plus IP100A Integrated 10/100 Ethernet MAC + PHY
Sundance Technology Inc / IC Plus Corp	ST201 Sundance Ethernet
Sundance Technology Inc / IC Plus Corp	TC9020 Gigabit Ethernet
Sundance Technology Inc / IC Plus Corp	TC9020 Gigabit Ethernet
Sundance Technology Inc / IC Plus Corp	IP1000 Family Gigabit Ethernet
Chelsio Communications Inc	10GbE Ethernet Adapter
Edimax Computer Co.	RTL81xx Fast Ethernet
Broadcom Corporation	NetXtreme BCM5752 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5752M Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme II BCM5709 Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5709S Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5700 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5701 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5702 Gigabit Ethernet

Производитель	Марка оборудования
Broadcom Corporation	NetXtreme BCM5703 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5704 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5704S_2 Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5706 Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5706 Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5706 Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5708 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5702FE Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5705 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5705_2 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5720 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5721 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5722 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5723 Gigabit Ethernet PCIe
Broadcom Corporation	NetXtreme BCM5705M Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5705M_2 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5714 Gigabit Ethernet
Broadcom Corporation	NetXtreme 5714S Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5780 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5780S Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5754M Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5755M Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5756ME Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5750 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5751 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5715 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5715S Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5754 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5755 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5750M Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5751M Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5751F Fast Ethernet PCI Express
Broadcom Corporation	NetLink BCM5787F Fast Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5761e Gigabit Ethernet PCIe
Broadcom Corporation	NetXtreme BCM5761 Gigabit Ethernet PCIe
Broadcom Corporation	NetXtreme BCM5764M Gigabit Ethernet PCIe
Broadcom Corporation	NetLink BCM5787M Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5782 Gigabit Ethernet
Broadcom Corporation	NetLink BCM5784M Gigabit Ethernet PCIe
Broadcom Corporation	NetLink BCM5786 Gigabit Ethernet PCI Express
Broadcom Corporation	NetLink BCM5787 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5788 Gigabit Ethernet
Broadcom Corporation	NetLink BCM5789 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5702X Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5703X Gigabit Ethernet

Производитель	Марка оборудования
Broadcom Corporation	NetXtreme BCM5704S Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5706S Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5706S Gigabit Ethernet
Broadcom Corporation	NetXtreme II BCM5708S Gigabit Ethernet
Broadcom Corporation	NetXtreme !BCM5702A3 Gigabit Ethernet
Broadcom Corporation	NetXtreme BCM5703 Gigabit Ethernet
Broadcom Corporation	NetLink BCM5781 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5753 Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5753M Gigabit Ethernet PCI Express
Broadcom Corporation	NetXtreme BCM5753F Fast Ethernet PCI Express
Broadcom Corporation	NetLink BCM5906 Fast Ethernet PCI Express
Broadcom Corporation	NetLink BCM5906M Fast Ethernet PCI Express
Planex Communications, Inc	FNW-3603-TX CardBus Fast Ethernet
Planex Communications, Inc	RTL81xx RealTek Ethernet
Planex Communications, Inc	FNW-3602-TX CardBus Fast Ethernet
DELTA Electronics, Inc	RTL81xx RealTek Ethernet
MYSON Technology Inc	MTD-8xx 100/10M Ethernet PCI Adapter
MYSON Technology Inc	SURECOM EP-320X-S 100/10M Ethernet PCI Adapter
MYSON Technology Inc	MTD-8xx 100/10M Ethernet PCI Adapter
TDK Semiconductor Corp.	RTL81xx Fast Ethernet
NetEffect	NE020 10Gb Accelerated Ethernet Adapter (iWARP RNIC)
Linksys	21x4x DEC-Tulip compatible 10/100 Ethernet
Linksys	21x4x DEC-Tulip compatible 10/100 Ethernet
Altima (nee Broadcom)	AC1000 Gigabit Ethernet
Altima (nee Broadcom)	AC1001 Gigabit Ethernet
Altima (nee Broadcom)	AC9100 Gigabit Ethernet
Altima (nee Broadcom)	AC1003 Gigabit Ethernet
Peppercon AG	ROL/F-100 Fast Ethernet Adapter with ROL
Hawking Technologies	PN672TX 10/100 Ethernet
S2io Inc.	Xframe 10 Gigabit Ethernet PCI-X
S2io Inc.	Xframe II 10Gbps Ethernet
Ammasso	AMSO 1100 iWARP/RDMA Gigabit Ethernet Coprocessor
Hangzhou Silan Microelectronics Co., Ltd.	SC92031 PCI Fast Ethernet Adapter
Hangzhou Silan Microelectronics Co., Ltd.	RTL8139D [Realtek] PCI 10/100BaseTX ethernet adaptor
Attansic Technology Corp.	L1e Gigabit Ethernet Adapter
Attansic Technology Corp.	L1 Gigabit Ethernet Adapter
Addtron Technology Co, Inc.	RTL8139 Ethernet
NetXen Incorporated	NXB-10GXSR 10 Gigabit Ethernet PCIe Adapter with SR-XFP optical interface
NetXen Incorporated	NXB-10GCX4 10 Gigabit Ethernet PCIe Adapter with CX4 copper interface
NetXen Incorporated	NXB-4GCU Quad Gigabit Ethernet PCIe Adapter with 1000-BASE-T interface
NetXen Incorporated	BladeCenter-H 10 Gigabit Ethernet High Speed Daughter Card
Intel Corporation	21145 Fast Ethernet
Intel Corporation	82542 Gigabit Ethernet Controller (Fiber)
Intel Corporation	82543GC Gigabit Ethernet Controller (Fiber)
Intel Corporation	82543GC Gigabit Ethernet Controller (Copper)

Производитель	Марка оборудования
Intel Corporation	82544EI Gigabit Ethernet Controller (Copper)
Intel Corporation	82544EI Gigabit Ethernet Controller (Fiber)
Intel Corporation	82544GC Gigabit Ethernet Controller (Copper)
Intel Corporation	82544GC Gigabit Ethernet Controller (LOM)
Intel Corporation	82540EM Gigabit Ethernet Controller
Intel Corporation	82545EM Gigabit Ethernet Controller (Copper)
Intel Corporation	82546EB Gigabit Ethernet Controller (Copper)
Intel Corporation	82545EM Gigabit Ethernet Controller (Fiber)
Intel Corporation	82546EB Gigabit Ethernet Controller (Fiber)
Intel Corporation	82541EI Gigabit Ethernet Controller
Intel Corporation	82541ER Gigabit Ethernet Controller
Intel Corporation	82540EM Gigabit Ethernet Controller (LOM)
Intel Corporation	82540EP Gigabit Ethernet Controller (Mobile)
Intel Corporation	82540EP Gigabit Ethernet Controller
Intel Corporation	82541EI Gigabit Ethernet Controller
Intel Corporation	82547EI Gigabit Ethernet Controller
Intel Corporation	82547EI Gigabit Ethernet Controller (Mobile)
Intel Corporation	82546EB Gigabit Ethernet Controller
Intel Corporation	82540EP Gigabit Ethernet Controller (Mobile)
Intel Corporation	82545GM Gigabit Ethernet Controller
Intel Corporation	82545GM Gigabit Ethernet Controller
Intel Corporation	82545GM Gigabit Ethernet Controller
Intel Corporation	82559 Ethernet Controller
Intel Corporation	82559 Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VE (LOM) Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VE (LOM) Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VE Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VE Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VM (LOM) Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VM (LOM) Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VM Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VM Ethernet Controller
Intel Corporation	82801CAM (ICH3)/82562EH (LOM) Ethernet Controller
Intel Corporation	82801CAM (ICH3) 82562EH Ethernet Controller
Intel Corporation	82801CAM (ICH3) Chipset Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VM (KM) Ethernet Controller
Intel Corporation	82801CAM (ICH3) PRO/100 VM (KM) Ethernet Controller
Intel Corporation	82801DB PRO/100 VE (LOM) Ethernet Controller
Intel Corporation	82801DB PRO/100 VE (LOM) Ethernet Controller
Intel Corporation	82801DB PRO/100 VE (CNR) Ethernet Controller
Intel Corporation	82801DB PRO/100 VE (CNR) Ethernet Controller
Intel Corporation	82801DB PRO/100 VM (LOM) Ethernet Controller
Intel Corporation	82801DB PRO/100 VM (LOM) Ethernet Controller
Intel Corporation	82801DB PRO/100 VM (CNR) Ethernet Controller
Intel Corporation	82801DB PRO/100 VM (CNR) Ethernet Controller

Производитель	Марка оборудования
Intel Corporation	82801DB PRO/100 VE (MOB) Ethernet Controller
Intel Corporation	82801DB PRO/100 VE (MOB) Ethernet Controller
Intel Corporation	82801DB PRO/100 VM (MOB) Ethernet Controller
Intel Corporation	82801DB PRO/100 VM (MOB) Ethernet Controller
Intel Corporation	82597EX 10GbE Ethernet Controller
Intel Corporation	82562EZ 10/100 Ethernet Controller
Intel Corporation	82562EZ 10/100 Ethernet Controller
Intel Corporation	82551QM Ethernet Controller
Intel Corporation	82551QM Ethernet Controller
Intel Corporation	82571EB Gigabit Ethernet Controller
Intel Corporation	82571EB Gigabit Ethernet Controller
Intel Corporation	82571EB Gigabit Ethernet Controller
Intel Corporation	82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller
Intel Corporation	82562ET/EZ/GT/GZ - PRO/100 VE Ethernet Controller
Intel Corporation	82562 EM/EX/GX - PRO/100 VM (LOM) Ethernet Controller
Intel Corporation	82562 EM/EX/GX - PRO/100 VM Ethernet Controller
Intel Corporation	82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller Mobile
Intel Corporation	82562EM/EX/GX - PRO/100 VM (LOM) Ethernet Controller Mobile
Intel Corporation	82562G - PRO/100 VE (LOM) Ethernet Controller
Intel Corporation	82562G - PRO/100 VE Ethernet Controller Mobile
Intel Corporation	82547GI Gigabit Ethernet Controller
Intel Corporation	82541GI Gigabit Ethernet Controller
Intel Corporation	82541GI Gigabit Ethernet Controller
Intel Corporation	82541ER Gigabit Ethernet Controller
Intel Corporation	82546GB Gigabit Ethernet Controller
Intel Corporation	82546GB Gigabit Ethernet Controller
Intel Corporation	82546GB Gigabit Ethernet Controller
Intel Corporation	82541PI Gigabit Ethernet Controller
Intel Corporation	82572EI Gigabit Ethernet Controller (Copper)
Intel Corporation	82572EI Gigabit Ethernet Controller (Fiber)
Intel Corporation	82572EI Gigabit Ethernet Controller
Intel Corporation	82546GB Gigabit Ethernet Controller
Intel Corporation	82573V Gigabit Ethernet Controller (Copper)
Intel Corporation	82573E Gigabit Ethernet Controller (Copper)
Intel Corporation	80003ES2LAN Gigabit Ethernet Controller (Copper)
Intel Corporation	80003ES2LAN Gigabit Ethernet Controller (Serdes)
Intel Corporation	82546GB Gigabit Ethernet Controller (Copper)
Intel Corporation	82573L Gigabit Ethernet Controller
Intel Corporation	82597EX 10GbE Ethernet Controller
Intel Corporation	82571EB Gigabit Ethernet Controller
Intel Corporation	82571EB Gigabit Ethernet Controller (Fiber)
Intel Corporation	82546GB Gigabit Ethernet Controller (Copper)
Intel Corporation	82572EI Gigabit Ethernet Controller (Copper)
Intel Corporation	80003ES2LAN Gigabit Ethernet Controller (Copper)
Intel Corporation	80003ES2LAN Gigabit Ethernet Controller (Serdes)

Производитель	Марка оборудования
Intel Corporation	82571EB Gigabit Ethernet Controller (Copper)
Intel Corporation	8255xER/82551IT Fast Ethernet Controller
Intel Corporation	8255xER/82551IT Fast Ethernet Controller
Intel Corporation	82865 EtherExpress PRO/100A
Intel Corporation	82557/8/9/0/1 Ethernet Pro 100
Intel Corporation	82557/8/9/0/1 Ethernet Pro 100
Intel Corporation	82597EX 10GbE Ethernet Controller
Intel Corporation	82597EX 10GbE Ethernet Controller
Intel Corporation	82801BA/BAM/CA/CAM Ethernet Controller
Intel Corporation	82801BA/BAM/CA/CAM Ethernet Controller
Intel Corporation	82801E Ethernet Controller 0
Intel Corporation	82801E Ethernet Controller 0
Intel Corporation	82801E Ethernet Controller 1
Intel Corporation	82801E Ethernet Controller 1
Intel Corporation	EtherExpress PRO/100 Intelligent Server
Intel Corporation	EtherExpress PRO/100 Intelligent Server

Печатающие устройства производства Alps, Anitech, Apollo, Apple

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Alps	
Alps MD-1000	OpenPrintingPPDs-ghostscript
Alps MD-1300	OpenPrintingPPDs-ghostscript
Alps MD-1500	OpenPrintingPPDs-ghostscript
Alps MD-2000	OpenPrintingPPDs-ghostscript
Alps MD-4000	OpenPrintingPPDs-ghostscript
Alps MD-5000	OpenPrintingPPDs-ghostscript
Anitech	
Anitech M24	OpenPrintingPPDs-ghostscript
Apollo	
Apollo P-1200	OpenPrintingPPDs-ghostscript
Apollo P-1220 Barbie	OpenPrintingPPDs-ghostscript
Apollo P-1250	OpenPrintingPPDs-ghostscript
Apollo P-2100	OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2150	OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2200	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2250	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2500	OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2550	OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2600	OpenPrintingPPDs-hpijs gutenprint-ppd
Apollo P-2650	OpenPrintingPPDs-hpijs gutenprint-ppd
Apple	
Apple 12/640ps	OpenPrintingPPDs-postscript
Apple Color StyleWriter 4100	gutenprint-ppd
Apple Color StyleWriter 4500	gutenprint-ppd
Apple Color StyleWriter 6500	gutenprint-ppd
Apple LaserWriter Select 360	gutenprint-ppd
Apple ImageWriter	OpenPrintingPPDs-ghostscript
Apple ImageWriter II	OpenPrintingPPDs-ghostscript
Apple ImageWriter LQ	OpenPrintingPPDs-ghostscript
Apple LaserWriter 16/600	OpenPrintingPPDs-postscript
Apple LaserWriter 4/600	OpenPrintingPPDs-postscript
Apple LaserWriter IIg	OpenPrintingPPDs-postscript
Apple LaserWriter IINTX	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Apple LaserWriter NT	OpenPrintingPPDs-ghostscript
Apple LaserWriter Pro 630	OpenPrintingPPDs-postscript
Apple LaserWriter Select 360	OpenPrintingPPDs-ghostscript
Apple LaserWriter Select 360	OpenPrintingPPDs-postscript

Печатающие устройства производства Brother

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother DCP-1200	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother DCP-7010	OpenPrintingPPDs-ghostscript
Brother DCP-7020	OpenPrintingPPDs-ghostscript
Brother DCP-7025	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother DCP-7045N	OpenPrintingPPDs-postscript
Brother DCP-8020/8025D	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother DCP-8040	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother DCP-8045D	manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
Brother DCP-8080DN/8085DN	OpenPrintingPPDs-postscript
Brother DCP-9010CN	OpenPrintingPPDs-postscript
Brother DCP-9040CN/9045CDN	OpenPrintingPPDs-postscript
Brother HJ-400	OpenPrintingPPDs-ghostscript
Brother HL-10h	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-10V	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother HL-1020	OpenPrintingPPDs-ghostscript
Brother HL-1030	OpenPrintingPPDs-ghostscript
Brother HL-1040	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother HL-1050 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-1060	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-1070 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-1230 series	OpenPrintingPPDs-ghostscript
Brother HL-1240 series	OpenPrintingPPDs-ghostscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother HL-1250 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-1260	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-1270N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-1430 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Brother HL-1440 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-1450 series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-1470N series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-1650/1660e/1670N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-1850/1870N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-2030 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-2040 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-2060	gutenprint-ppd
Brother HL-2070N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother HL-2140 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Brother HL-2170W	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Brother HL-2250DN	gutenprint-ppd
Brother HL-2400CeN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Brother HL-2460 series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-2600CN series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Brother HL-2700CN series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother HL-3070CW	OpenPrintingPPDs-postscript
Brother HL-3260N series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Brother HL-3400CN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Brother HL-3450CN series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Brother HL-4Ve	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother HL-4000CN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Brother HL-4040CN	OpenPrintingPPDs-ghostscript
Brother HL-4050CDN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Brother HL-4070CDW	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Brother HL-5030/5040	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother HL-5050 series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-5070N series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-5140 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-5150D series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-5170DN series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-5240 series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother HL-5250DN series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother HL-5270DN series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother HL-5350DN series	OpenPrintingPPDs-postscript
Brother HL-5370DW series	OpenPrintingPPDs-postscript
Brother HL-5380DN series	OpenPrintingPPDs-postscript
Brother HL-630	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother HL-660	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother HL-6050/6050D_DN series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother HL-720	OpenPrintingPPDs-ghostscript
Brother HL-730	OpenPrintingPPDs-ghostscript
Brother HL-760	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother HL-7050 series	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-7050N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
Brother HL-8	OpenPrintingPPDs-ghostscript
Brother HL-820	OpenPrintingPPDs-ghostscript
Brother HL-8050N series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother HL-960	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Brother MC-3000	OpenPrintingPPDs-ghostscript
Brother MFC 7150C	OpenPrintingPPDs-ghostscript
Brother MFC-6550MC	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother MFC-7225N	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-7450	OpenPrintingPPDs-postscript
Brother MFC-7820N	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-7840N/7840W	OpenPrintingPPDs-postscript
Brother MFC-8220	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-8300	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother MFC-8370DN	OpenPrintingPPDs-postscript
Brother MFC-8380DN	OpenPrintingPPDs-postscript
Brother MFC-8420	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-8440	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-8480DN	OpenPrintingPPDs-postscript
Brother MFC-8600	OpenPrintingPPDs-ghostscript
Brother MFC-8640D	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-8670DN series	OpenPrintingPPDs-postscript
Brother MFC-8680DN	OpenPrintingPPDs-postscript
Brother MFC-8820D	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-8840D	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-8880DN	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother MFC-8890DW	OpenPrintingPPDs-postscript
Brother MFC-9010CN	OpenPrintingPPDs-postscript
Brother MFC-9050	OpenPrintingPPDs-ghostscript
Brother MFC-9100c	OpenPrintingPPDs-ghostscript
Brother MFC-9120CN	OpenPrintingPPDs-postscript
Brother MFC-9320CW	OpenPrintingPPDs-postscript
Brother MFC-9420CN series	manufacturer-PPDs OpenPrintingPPDs-postscript
Brother MFC-9440CN	OpenPrintingPPDs-postscript
Brother MFC-9450CDN	OpenPrintingPPDs-postscript
Brother MFC-9500	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother MFC-9600	OpenPrintingPPDs-ghostscript gutenprint-ppd
Brother MFC-9840CDW	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Brother MFC-P2500	OpenPrintingPPDs-ghostscript
Brother HL-L5000D	OpenPrintingPPDs-postscript
Brother HL-L5100DN	OpenPrintingPPDs-postscript
Brother HL-L5200DW	OpenPrintingPPDs-postscript
Brother DCP-L5500DN	OpenPrintingPPDs-postscript
Brother MFC-L5750DW	OpenPrintingPPDs-postscript
Brother HL-L6250DN	OpenPrintingPPDs-postscript
Brother HL-L6300DW	OpenPrintingPPDs-postscript
Brother HL-L6400DW	OpenPrintingPPDs-postscript
Brother DCP-L6600DW	OpenPrintingPPDs-postscript
Brother MFC-L6800DW	OpenPrintingPPDs-postscript
Brother MFC-L6900DW	OpenPrintingPPDs-postscript
Brother MFC-L6950DW	OpenPrintingPPDs-postscript
Brother HL-L2300D	OpenPrintingPPDs-postscript
Brother HL-L2340DW	OpenPrintingPPDs-postscript
Brother HL-L2360DN	OpenPrintingPPDs-postscript
Brother HL-L2365DW	OpenPrintingPPDs-postscript
Brother HL-L2371DN	OpenPrintingPPDs-postscript
Brother DCP-L2500D	OpenPrintingPPDs-postscript
Brother DCP-L2520DW	OpenPrintingPPDs-postscript
Brother DCP-L2540DN	OpenPrintingPPDs-postscript
Brother DCP-L2551DN	OpenPrintingPPDs-postscript
Brother DCP-L2560DW	OpenPrintingPPDs-postscript
Brother MFC-L2700DW	OpenPrintingPPDs-postscript
Brother MFC-L2700DN	OpenPrintingPPDs-postscript
Brother MFC-L2720DW	OpenPrintingPPDs-postscript
Brother MFC-L2740DW	OpenPrintingPPDs-postscript
Brother MFC-L2751DW	OpenPrintingPPDs-postscript
Brother HL-L8260CDW	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Brother HL-L8360CDW	OpenPrintingPPDs-postscript
Brother HL-L9200CDW	OpenPrintingPPDs-postscript
Brother HL-L9310CDW	OpenPrintingPPDs-postscript
Brother DCP-L8410CDW	OpenPrintingPPDs-postscript
Brother MFC-L8650CDW	OpenPrintingPPDs-postscript
Brother MFC-L8690CDW	OpenPrintingPPDs-postscript
Brother MFC-L8900CDW	OpenPrintingPPDs-postscript
Brother MFC-L9550CDW	OpenPrintingPPDs-postscript
Brother MFC-L9570CDW	OpenPrintingPPDs-postscript
Brother QL-800	OpenPrintingPPDs-postscript
Brother QL-810W	OpenPrintingPPDs-postscript
Brother QL-820W	OpenPrintingPPDs-postscript

Печатающие устройства производства Canon

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon BJ-5	OpenPrintingPPDs-ghostscript
Canon BJ-10e	OpenPrintingPPDs-ghostscript
Canon BJ-10v	OpenPrintingPPDs-ghostscript
Canon BJ-15v	OpenPrintingPPDs-ghostscript
Canon BJ-20	OpenPrintingPPDs-ghostscript
Canon BJ-30	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJ-35v	OpenPrintingPPDs-ghostscript
Canon BJC-50	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-55	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-70	OpenPrintingPPDs-ghostscript
Canon BJC-80	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-85	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJ-100	OpenPrintingPPDs-ghostscript
Canon BJ-200	OpenPrintingPPDs-ghostscript
Canon BJC-210	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-240	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-250	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJ-300	OpenPrintingPPDs-ghostscript
Canon BJ-330	OpenPrintingPPDs-ghostscript
Canon BJC-600	OpenPrintingPPDs-ghostscript
Canon BJC-610	OpenPrintingPPDs-ghostscript
Canon BJC-620	OpenPrintingPPDs-ghostscript
Canon BJC-800	OpenPrintingPPDs-ghostscript
Canon BJC-880J	OpenPrintingPPDs-ghostscript
Canon BJC-1000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-2000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-2010	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-2100	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-210SP	OpenPrintingPPDs-ghostscript
Canon BJC-2110	OpenPrintingPPDs-ghostscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon BJC-3000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-4000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-4100	OpenPrintingPPDs-ghostscript
Canon BJC-4200	OpenPrintingPPDs-ghostscript
Canon BJC-4300	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-4310SP	OpenPrintingPPDs-ghostscript
Canon BJC-4400	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-4550	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-5100	gutenprint-ppd
Canon BJC-5500	gutenprint-ppd
Canon BJC-5500J	gutenprint-ppd
Canon BJC-6000	gutenprint-ppd
Canon BJC-6100	gutenprint-ppd
Canon BJC-6200	gutenprint-ppd
Canon BJC-6500	gutenprint-ppd
Canon BJC-7000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-7004	OpenPrintingPPDs-ghostscript
Canon BJC-7100	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-8200	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon BJC-8500	gutenprint-ppd
Canon CP-10	gutenprint-ppd
Canon CP-100	gutenprint-ppd
Canon CP-200	gutenprint-ppd
Canon CP-220	gutenprint-ppd
Canon CP-300	gutenprint-ppd
Canon CP-330	gutenprint-ppd
Canon E400 series	gutenprint-ppd
Canon E460 series	gutenprint-ppd
Canon E480 series	gutenprint-ppd
Canon E500 series	gutenprint-ppd
Canon E510 series	gutenprint-ppd
Canon E560 series	gutenprint-ppd
Canon E600 series	gutenprint-ppd
Canon E610 series	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon GP 335	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Canon GP 405	OpenPrintingPPDs-postscript
Canon i70	gutenprint-ppd
Canon i80	gutenprint-ppd
Canon i450	gutenprint-ppd
Canon i450	OpenPrintingPPDs-ghostscript
Canon i450X	gutenprint-ppd
Canon i455	gutenprint-ppd
Canon i455X	gutenprint-ppd
Canon i470D	gutenprint-ppd
Canon i475D	gutenprint-ppd
Canon i550	gutenprint-ppd
Canon i550X	gutenprint-ppd
Canon i560	gutenprint-ppd
Canon i560X	gutenprint-ppd
Canon i6100	gutenprint-ppd
Canon i6500	gutenprint-ppd
Canon i850	gutenprint-ppd
Canon i860	gutenprint-ppd
Canon i865	gutenprint-ppd
Canon i900D	gutenprint-ppd
Canon i905D	gutenprint-ppd
Canon i9100	gutenprint-ppd
Canon i950	gutenprint-ppd
Canon i960	gutenprint-ppd
Canon i965	gutenprint-ppd
Canon i990	gutenprint-ppd
Canon i9900	gutenprint-ppd
Canon i9950	gutenprint-ppd
Canon iB4000 series	gutenprint-ppd
Canon imageRunner 330s	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Canon imageRunner 1023	OpenPrintingPPDs-ghostscript
Canon imageRunner 1023iF	OpenPrintingPPDs-ghostscript
Canon imageRunner 1023N	OpenPrintingPPDs-ghostscript
Canon imageRunner 2016	OpenPrintingPPDs-ghostscript
Canon imageRunner 2016i	OpenPrintingPPDs-ghostscript
Canon imageRunner 2018	OpenPrintingPPDs-ghostscript
Canon imageRunner 2020	OpenPrintingPPDs-ghostscript
Canon imageRunner 2020i	OpenPrintingPPDs-ghostscript
Canon imageRunner 2022	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon imageRunner 2200	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 2230	OpenPrintingPPDs-ghostscript
Canon imageRunner 2270	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 2800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 3025	OpenPrintingPPDs-ghostscript
Canon imageRunner 3300	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 3570	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 4570	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 5000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 5570	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 6000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 6570	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 7086	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 7095	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 7105	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 8070	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner 8500	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C2550	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner C2570	OpenPrintingPPDs-hpijs penPrintingPPDs-postscript
Canon imageRunner C2570i	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C2620N	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C3100	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C3170	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon imageRunner C3170i	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C3200	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner C5058	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner C5068	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner C5180	OpenPrintingPPDs-ghostscript
Canon imageRunner C5185	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner C5185i	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon imageRunner C5800	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C5870U	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C6800	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon imageRunner C6870U	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Canon iP90 series	gutenprint-ppd
Canon iP100 series	gutenprint-ppd
Canon iP110 series	gutenprint-ppd
Canon iP2000 series	gutenprint-ppd
Canon iP2700 series	gutenprint-ppd
Canon iP2800 series	gutenprint-ppd
Canon iP3300 series	gutenprint-ppd
Canon iP3500 series	gutenprint-ppd
Canon iP3600 series	gutenprint-ppd
Canon iP4200 series	gutenprint-ppd
Canon iP4300 series	gutenprint-ppd
Canon iP4500 series	gutenprint-ppd
Canon iP4600 series	gutenprint-ppd
Canon iP4700 series	gutenprint-ppd
Canon iP4800 series	gutenprint-ppd
Canon iP4900 series	gutenprint-ppd
Canon iP5200R series	gutenprint-ppd
Canon iP6600D series	gutenprint-ppd
Canon iP6700D series	gutenprint-ppd
Canon iP7200 series	gutenprint-ppd
Canon iP8700 series	gutenprint-ppd
Canon iR3225 UFR II	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon iR3225 UFR II	OpenPrintingPPDs-postscript
Canon iX5000 series	gutenprint-ppd
Canon iX6500 series	gutenprint-ppd
Canon iX6700 series	gutenprint-ppd
Canon iX6800 series	gutenprint-ppd
Canon iX7000 series	gutenprint-ppd
Canon LBP-4+	OpenPrintingPPDs-ghostscript
Canon LBP-4sx	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon LBP-4U	OpenPrintingPPDs-ghostscript
Canon LBP-8A1	OpenPrintingPPDs-ghostscript
Canon LBP-310	OpenPrintingPPDs-ghostscript
Canon LBP-320 Pro	OpenPrintingPPDs-ghostscript
Canon LBP-350	OpenPrintingPPDs-ghostscript
Canon LBP-430	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Canon LBP-470	OpenPrintingPPDs-ghostscript
Canon LBP-1000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Canon LBP-1260	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Canon LBP-1760	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Canon LBP-3360	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Canon LBP-3460	OpenPrintingPPDs-ghostscript
Canon LBP-5360	OpenPrintingPPDs-ghostscript
Canon LBP-5960	OpenPrintingPPDs-ghostscript
Canon LBP-5970	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon LBP-5975	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Canon LIPS-II+	OpenPrintingPPDs-ghostscript
Canon LIPS-III	OpenPrintingPPDs-ghostscript
Canon LIPS-IV	OpenPrintingPPDs-ghostscript
Canon LIPS-IVv	OpenPrintingPPDs-ghostscript
Canon MAXIFY iB4010	gutenprint-ppd
Canon MAXIFY iB4020	gutenprint-ppd
Canon MAXIFY iB4030	gutenprint-ppd
Canon MAXIFY iB4040	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon MAXIFY iB4050	gutenprint-ppd
Canon MAXIFY iB4060	gutenprint-ppd
Canon MAXIFY iB4070	gutenprint-ppd
Canon MAXIFY iB4080	gutenprint-ppd
Canon MAXIFY MB2010	gutenprint-ppd
Canon MAXIFY MB2020	gutenprint-ppd
Canon MAXIFY MB2030	gutenprint-ppd
Canon MAXIFY MB2040	gutenprint-ppd
Canon MAXIFY MB2050	gutenprint-ppd
Canon MAXIFY MB2060	gutenprint-ppd
Canon MAXIFY MB2320	gutenprint-ppd
Canon MAXIFY MB2330	gutenprint-ppd
Canon MAXIFY MB2340	gutenprint-ppd
Canon MAXIFY MB2350	gutenprint-ppd
Canon MAXIFY MB2360	gutenprint-ppd
Canon MAXIFY MB2390	gutenprint-ppd
Canon MAXIFY MB5020	gutenprint-ppd
Canon MAXIFY MB5030	gutenprint-ppd
Canon MAXIFY MB5040	gutenprint-ppd
Canon MAXIFY MB5050	gutenprint-ppd
Canon MAXIFY MB5060	gutenprint-ppd
Canon MAXIFY MB5070	gutenprint-ppd
Canon MAXIFY MB5080	gutenprint-ppd
Canon MAXIFY MB5090	gutenprint-ppd
Canon MAXIFY MB5310	gutenprint-ppd
Canon MAXIFY MB5320	gutenprint-ppd
Canon MAXIFY MB5330	gutenprint-ppd
Canon MAXIFY MB5340	gutenprint-ppd
Canon MAXIFY MB5350	gutenprint-ppd
Canon MAXIFY MB5360	gutenprint-ppd
Canon MAXIFY MB5370	gutenprint-ppd
Canon MAXIFY MB5390	gutenprint-ppd
Canon MB2000 series	gutenprint-ppd
Canon MB2300 series	gutenprint-ppd
Canon MB5000 series	gutenprint-ppd
Canon MB5300 series	gutenprint-ppd
Canon MG2100 series	gutenprint-ppd
Canon MG2200 series	gutenprint-ppd
Canon MG2400 series	gutenprint-ppd
Canon MG2500 series	gutenprint-ppd
Canon MG2900 series	gutenprint-ppd
Canon MG3100 series	gutenprint-ppd
Canon MG3200 series	gutenprint-ppd
Canon MG3500 series	gutenprint-ppd
Canon MG3600 series	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon MG4100 series	gutenprint-ppd
Canon MG4200 series	gutenprint-ppd
Canon MG5100 series	gutenprint-ppd
Canon MG5200 series	gutenprint-ppd
Canon MG5300 series	gutenprint-ppd
Canon MG5400 series	gutenprint-ppd
Canon MG5500 series	gutenprint-ppd
Canon MG5600 series	gutenprint-ppd
Canon MG5700 series	gutenprint-ppd
Canon MG6100 series	gutenprint-ppd
Canon MG6200 series	gutenprint-ppd
Canon MG6300 series	gutenprint-ppd
Canon MG6400 series	gutenprint-ppd
Canon MG6500 series	gutenprint-ppd
Canon MG6600 series	gutenprint-ppd
Canon MG6700 series	gutenprint-ppd
Canon MG6800 series	gutenprint-ppd
Canon MG6900 series	gutenprint-ppd
Canon MG7100 series	gutenprint-ppd
Canon MG7500 series	gutenprint-ppd
Canon MG7700 series	gutenprint-ppd
Canon MG8100 series	gutenprint-ppd
Canon MG8200 series	gutenprint-ppd
Canon Mommy Photo MG5670	gutenprint-ppd
Canon Mommy Photo MG5790	gutenprint-ppd
Canon Mommy Photo MG6670	gutenprint-ppd
Canon Mommy Photo MG7570	gutenprint-ppd
Canon MP140 series	gutenprint-ppd
Canon MP150 series	gutenprint-ppd
Canon MP160 series	gutenprint-ppd
Canon MP170 series	gutenprint-ppd
Canon MP180 series	gutenprint-ppd
Canon MP190 series	gutenprint-ppd
Canon MP210 series	gutenprint-ppd
Canon MP220 series	gutenprint-ppd
Canon MP230 series	gutenprint-ppd
Canon MP240 series	gutenprint-ppd
Canon MP250 series	gutenprint-ppd
Canon MP260 series	gutenprint-ppd
Canon MP270 series	gutenprint-ppd
Canon MP280 series	gutenprint-ppd
Canon MP360 series	gutenprint-ppd
Canon MP370 series	gutenprint-ppd
Canon MP390 series	gutenprint-ppd
Canon MP450 series	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon MP460 series	gutenprint-ppd
Canon MP470 series	gutenprint-ppd
Canon MP480 series	gutenprint-ppd
Canon MP490 series	gutenprint-ppd
Canon MP500 series	gutenprint-ppd
Canon MP510 series	gutenprint-ppd
Canon MP520 series	gutenprint-ppd
Canon MP530 series	gutenprint-ppd
Canon MP540 series	gutenprint-ppd
Canon MP550 series	gutenprint-ppd
Canon MP560 series	gutenprint-ppd
Canon MP600 series	gutenprint-ppd
Canon MP610 series	gutenprint-ppd
Canon MP620 series	gutenprint-ppd
Canon MP630 series	gutenprint-ppd
Canon MP640 series	gutenprint-ppd
Canon MP700 series	gutenprint-ppd
Canon MP710 series	gutenprint-ppd
Canon MP730 series	gutenprint-ppd
Canon MP740 series	gutenprint-ppd
Canon MP750 series	gutenprint-ppd
Canon MP760 series	gutenprint-ppd
Canon MP770 series	gutenprint-ppd
Canon MP780 series	gutenprint-ppd
Canon MP790 series	gutenprint-ppd
Canon MP800 series	gutenprint-ppd
Canon MP810 series	gutenprint-ppd
Canon MP830 series	gutenprint-ppd
Canon MP900 series	gutenprint-ppd
Canon MP950 series	gutenprint-ppd
Canon MP960 series	gutenprint-ppd
Canon MP970 series	gutenprint-ppd
Canon MP980 series	gutenprint-ppd
Canon MP990 series	gutenprint-ppd
Canon MultiPASS C2500	OpenPrintingPPDs-ghostscript
Canon MultiPASS C3000	OpenPrintingPPDs-ghostscript
Canon MultiPASS C3500	OpenPrintingPPDs-ghostscript
Canon MultiPASS C5000	OpenPrintingPPDs-ghostscript
Canon MultiPASS C5500	OpenPrintingPPDs-ghostscript
Canon MultiPASS MP360	gutenprint-ppd
Canon MultiPASS MP370	gutenprint-ppd
Canon MultiPASS MP390	gutenprint-ppd
Canon MultiPASS MP700	gutenprint-ppd
Canon MultiPASS MP730	gutenprint-ppd
Canon MX300 series	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon MX310 series	gutenprint-ppd
Canon MX320 series	gutenprint-ppd
Canon MX330 series	gutenprint-ppd
Canon MX340 series	gutenprint-ppd
Canon MX350 series	gutenprint-ppd
Canon MX360 series	gutenprint-ppd
Canon MX370 series	gutenprint-ppd
Canon MX390 series	gutenprint-ppd
Canon MX410 series	gutenprint-ppd
Canon MX420 series	gutenprint-ppd
Canon MX430 series	gutenprint-ppd
Canon MX450 series	gutenprint-ppd
Canon MX470 series	gutenprint-ppd
Canon MX490 series	gutenprint-ppd
Canon MX510 series	gutenprint-ppd
Canon MX520 series	gutenprint-ppd
Canon MX530 series	gutenprint-ppd
Canon MX700 series	gutenprint-ppd
Canon MX710 series	gutenprint-ppd
Canon MX720 series	gutenprint-ppd
Canon MX850 series	gutenprint-ppd
Canon MX860 series	gutenprint-ppd
Canon MX870 series	gutenprint-ppd
Canon MX880 series	gutenprint-ppd
Canon MX890 series	gutenprint-ppd
Canon MX920 series	gutenprint-ppd
Canon MX7600 series	gutenprint-ppd
Canon PIXMA E400	gutenprint-ppd
Canon PIXMA E401	gutenprint-ppd
Canon PIXMA E404	gutenprint-ppd
Canon PIXMA E408	gutenprint-ppd
Canon PIXMA E409	gutenprint-ppd
Canon PIXMA E460	gutenprint-ppd
Canon PIXMA E461	gutenprint-ppd
Canon PIXMA E464	gutenprint-ppd
Canon PIXMA E468	gutenprint-ppd
Canon PIXMA E480	gutenprint-ppd
Canon PIXMA E481	gutenprint-ppd
Canon PIXMA E484	gutenprint-ppd
Canon PIXMA E488	gutenprint-ppd
Canon PIXMA E489	gutenprint-ppd
Canon PIXMA E500	gutenprint-ppd
Canon PIXMA E510	gutenprint-ppd
Canon PIXMA E514	gutenprint-ppd
Canon PIXMA E518	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA E560	gutenprint-ppd
Canon PIXMA E568	gutenprint-ppd
Canon PIXMA E569	gutenprint-ppd
Canon PIXMA E600	gutenprint-ppd
Canon PIXMA E608	gutenprint-ppd
Canon PIXMA E610	gutenprint-ppd
Canon PIXMA E618	gutenprint-ppd
Canon PIXMA iP90	gutenprint-ppd
Canon PIXMA iP90v	gutenprint-ppd
Canon PIXMA iP100	gutenprint-ppd
Canon PIXMA iP110	gutenprint-ppd
Canon PIXMA iP2000	gutenprint-ppd
Canon PIXMA iP2700	gutenprint-ppd
Canon PIXMA iP2701	gutenprint-ppd
Canon PIXMA iP2702	gutenprint-ppd
Canon PIXMA iP2740	gutenprint-ppd
Canon PIXMA iP2760	gutenprint-ppd
Canon PIXMA iP2770	gutenprint-ppd
Canon PIXMA iP2772	gutenprint-ppd
Canon PIXMA iP2780	gutenprint-ppd
Canon PIXMA iP2788	gutenprint-ppd
Canon PIXMA iP2810	gutenprint-ppd
Canon PIXMA iP2820	gutenprint-ppd
Canon PIXMA iP2840	gutenprint-ppd
Canon PIXMA iP2850	gutenprint-ppd
Canon PIXMA iP2870	gutenprint-ppd
Canon PIXMA iP2872	gutenprint-ppd
Canon PIXMA iP2880	gutenprint-ppd
Canon PIXMA iP2890	gutenprint-ppd
Canon PIXMA iP3000	gutenprint-ppd
Canon PIXMA iP3100	gutenprint-ppd
Canon PIXMA iP3300	gutenprint-ppd
Canon PIXMA iP3500	gutenprint-ppd
Canon PIXMA iP3600	gutenprint-ppd
Canon PIXMA iP3680	gutenprint-ppd
Canon PIXMA iP4000	gutenprint-ppd
Canon PIXMA iP4000R	gutenprint-ppd
Canon PIXMA iP4100	gutenprint-ppd
Canon PIXMA iP4100R	gutenprint-ppd
Canon PIXMA iP4200	gutenprint-ppd
Canon PIXMA iP4300	gutenprint-ppd
Canon PIXMA iP4500	gutenprint-ppd
Canon PIXMA iP4600	gutenprint-ppd
Canon PIXMA iP4680	gutenprint-ppd
Canon PIXMA iP4700	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA iP4760	gutenprint-ppd
Canon PIXMA iP4800	gutenprint-ppd
Canon PIXMA iP4810	gutenprint-ppd
Canon PIXMA iP4820	gutenprint-ppd
Canon PIXMA iP4840	gutenprint-ppd
Canon PIXMA iP4850	gutenprint-ppd
Canon PIXMA iP4870	gutenprint-ppd
Canon PIXMA iP4880	gutenprint-ppd
Canon PIXMA iP4900	gutenprint-ppd
Canon PIXMA iP4910	gutenprint-ppd
Canon PIXMA iP4920	gutenprint-ppd
Canon PIXMA iP4940	gutenprint-ppd
Canon PIXMA iP4950	gutenprint-ppd
Canon PIXMA iP4970	gutenprint-ppd
Canon PIXMA iP4980	gutenprint-ppd
Canon PIXMA iP5000	gutenprint-ppd
Canon PIXMA iP5200	gutenprint-ppd
Canon PIXMA iP5200R	gutenprint-ppd
Canon PIXMA iP5300	gutenprint-ppd
Canon PIXMA iP6000D	gutenprint-ppd
Canon PIXMA iP6100D	gutenprint-ppd
Canon PIXMA iP6210D	gutenprint-ppd
Canon PIXMA iP6220D	gutenprint-ppd
Canon PIXMA iP6310D	gutenprint-ppd
Canon PIXMA iP6320D	gutenprint-ppd
Canon PIXMA iP6600D	gutenprint-ppd
Canon PIXMA iP6700D	gutenprint-ppd
Canon PIXMA iP7100	gutenprint-ppd
Canon PIXMA iP7210	gutenprint-ppd
Canon PIXMA iP7220	gutenprint-ppd
Canon PIXMA iP7240	gutenprint-ppd
Canon PIXMA iP7250	gutenprint-ppd
Canon PIXMA iP7260	gutenprint-ppd
Canon PIXMA iP7270	gutenprint-ppd
Canon PIXMA iP7280	gutenprint-ppd
Canon PIXMA iP7500	gutenprint-ppd
Canon PIXMA iP7810	gutenprint-ppd
Canon PIXMA iP8100	gutenprint-ppd
Canon PIXMA iP8500	gutenprint-ppd
Canon PIXMA iP8600	gutenprint-ppd
Canon PIXMA iP8720	gutenprint-ppd
Canon PIXMA iP8740	gutenprint-ppd
Canon PIXMA iP8750	gutenprint-ppd
Canon PIXMA iP8760	gutenprint-ppd
Canon PIXMA iP8770	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA iP8780	gutenprint-ppd
Canon PIXMA iP9910	gutenprint-ppd
Canon PIXMA iX4000	gutenprint-ppd
Canon PIXMA iX5000	gutenprint-ppd
Canon PIXMA iX6500	gutenprint-ppd
Canon PIXMA iX6510	gutenprint-ppd
Canon PIXMA iX6520	gutenprint-ppd
Canon PIXMA iX6540	gutenprint-ppd
Canon PIXMA iX6550	gutenprint-ppd
Canon PIXMA iX6560	gutenprint-ppd
Canon PIXMA iX6580	gutenprint-ppd
Canon PIXMA iX6770	gutenprint-ppd
Canon PIXMA iX6780	gutenprint-ppd
Canon PIXMA iX6810	gutenprint-ppd
Canon PIXMA iX6820	gutenprint-ppd
Canon PIXMA iX6840	gutenprint-ppd
Canon PIXMA iX6850	gutenprint-ppd
Canon PIXMA iX6860	gutenprint-ppd
Canon PIXMA iX6870	gutenprint-ppd
Canon PIXMA iX6880	gutenprint-ppd
Canon PIXMA iX7000	gutenprint-ppd
Canon PIXMA MG2100	gutenprint-ppd
Canon PIXMA MG2110	gutenprint-ppd
Canon PIXMA MG2120	gutenprint-ppd
Canon PIXMA MG2140	gutenprint-ppd
Canon PIXMA MG2150	gutenprint-ppd
Canon PIXMA MG2160	gutenprint-ppd
Canon PIXMA MG2170	gutenprint-ppd
Canon PIXMA MG2180	gutenprint-ppd
Canon PIXMA MG2210	gutenprint-ppd
Canon PIXMA MG2220	gutenprint-ppd
Canon PIXMA MG2240	gutenprint-ppd
Canon PIXMA MG2250	gutenprint-ppd
Canon PIXMA MG2260	gutenprint-ppd
Canon PIXMA MG2270	gutenprint-ppd
Canon PIXMA MG2280	gutenprint-ppd
Canon PIXMA MG2400	gutenprint-ppd
Canon PIXMA MG2410	gutenprint-ppd
Canon PIXMA MG2420	gutenprint-ppd
Canon PIXMA MG2440	gutenprint-ppd
Canon PIXMA MG2450	gutenprint-ppd
Canon PIXMA MG2460	gutenprint-ppd
Canon PIXMA MG2470	gutenprint-ppd
Canon PIXMA MG2490	gutenprint-ppd
Canon PIXMA MG2510	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MG2520	gutenprint-ppd
Canon PIXMA MG2540	gutenprint-ppd
Canon PIXMA MG2550	gutenprint-ppd
Canon PIXMA MG2560	gutenprint-ppd
Canon PIXMA MG2570	gutenprint-ppd
Canon PIXMA MG2570S	gutenprint-ppd
Canon PIXMA MG2580	gutenprint-ppd
Canon PIXMA MG2580S	gutenprint-ppd
Canon PIXMA MG2590	gutenprint-ppd
Canon PIXMA MG2910	gutenprint-ppd
Canon PIXMA MG2920	gutenprint-ppd
Canon PIXMA MG2922	gutenprint-ppd
Canon PIXMA MG2924	gutenprint-ppd
Canon PIXMA MG2940	gutenprint-ppd
Canon PIXMA MG2950	gutenprint-ppd
Canon PIXMA MG2960	gutenprint-ppd
Canon PIXMA MG2970	gutenprint-ppd
Canon PIXMA MG2980	gutenprint-ppd
Canon PIXMA MG2990	gutenprint-ppd
Canon PIXMA MG3100	gutenprint-ppd
Canon PIXMA MG3110	gutenprint-ppd
Canon PIXMA MG3120	gutenprint-ppd
Canon PIXMA MG3122	gutenprint-ppd
Canon PIXMA MG3140	gutenprint-ppd
Canon PIXMA MG3150	gutenprint-ppd
Canon PIXMA MG3160	gutenprint-ppd
Canon PIXMA MG3170	gutenprint-ppd
Canon PIXMA MG3180	gutenprint-ppd
Canon PIXMA MG3210	gutenprint-ppd
Canon PIXMA MG3220	gutenprint-ppd
Canon PIXMA MG3222	gutenprint-ppd
Canon PIXMA MG3240	gutenprint-ppd
Canon PIXMA MG3250	gutenprint-ppd
Canon PIXMA MG3260	gutenprint-ppd
Canon PIXMA MG3270	gutenprint-ppd
Canon PIXMA MG3510	gutenprint-ppd
Canon PIXMA MG3520	gutenprint-ppd
Canon PIXMA MG3522	gutenprint-ppd
Canon PIXMA MG3540	gutenprint-ppd
Canon PIXMA MG3550	gutenprint-ppd
Canon PIXMA MG3560	gutenprint-ppd
Canon PIXMA MG3570	gutenprint-ppd
Canon PIXMA MG3580	gutenprint-ppd
Canon PIXMA MG3610	gutenprint-ppd
Canon PIXMA MG3620	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MG3640	gutenprint-ppd
Canon PIXMA MG3650	gutenprint-ppd
Canon PIXMA MG3670	gutenprint-ppd
Canon PIXMA MG3680	gutenprint-ppd
Canon PIXMA MG4100	gutenprint-ppd
Canon PIXMA MG4110	gutenprint-ppd
Canon PIXMA MG4120	gutenprint-ppd
Canon PIXMA MG4140	gutenprint-ppd
Canon PIXMA MG4150	gutenprint-ppd
Canon PIXMA MG4160	gutenprint-ppd
Canon PIXMA MG4170	gutenprint-ppd
Canon PIXMA MG4180	gutenprint-ppd
Canon PIXMA MG4210	gutenprint-ppd
Canon PIXMA MG4220	gutenprint-ppd
Canon PIXMA MG4240	gutenprint-ppd
Canon PIXMA MG4250	gutenprint-ppd
Canon PIXMA MG4260	gutenprint-ppd
Canon PIXMA MG4270	gutenprint-ppd
Canon PIXMA MG4280	gutenprint-ppd
Canon PIXMA MG5100	gutenprint-ppd
Canon PIXMA MG5120	gutenprint-ppd
Canon PIXMA MG5140	gutenprint-ppd
Canon PIXMA MG5150	gutenprint-ppd
Canon PIXMA MG5170	gutenprint-ppd
Canon PIXMA MG5180	gutenprint-ppd
Canon PIXMA MG5200	gutenprint-ppd
Canon PIXMA MG5210	gutenprint-ppd
Canon PIXMA MG5220	gutenprint-ppd
Canon PIXMA MG5240	gutenprint-ppd
Canon PIXMA MG5250	gutenprint-ppd
Canon PIXMA MG5270	gutenprint-ppd
Canon PIXMA MG5280	gutenprint-ppd
Canon PIXMA MG5300	gutenprint-ppd
Canon PIXMA MG5310	gutenprint-ppd
Canon PIXMA MG5320	gutenprint-ppd
Canon PIXMA MG5340	gutenprint-ppd
Canon PIXMA MG5350	gutenprint-ppd
Canon PIXMA MG5370	gutenprint-ppd
Canon PIXMA MG5380	gutenprint-ppd
Canon PIXMA MG5410	gutenprint-ppd
Canon PIXMA MG5420	gutenprint-ppd
Canon PIXMA MG5422	gutenprint-ppd
Canon PIXMA MG5440	gutenprint-ppd
Canon PIXMA MG5450	gutenprint-ppd
Canon PIXMA MG5460	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MG5470	gutenprint-ppd
Canon PIXMA MG5480	gutenprint-ppd
Canon PIXMA MG5510	gutenprint-ppd
Canon PIXMA MG5520	gutenprint-ppd
Canon PIXMA MG5522	gutenprint-ppd
Canon PIXMA MG5540	gutenprint-ppd
Canon PIXMA MG5550	gutenprint-ppd
Canon PIXMA MG5560	gutenprint-ppd
Canon PIXMA MG5570	gutenprint-ppd
Canon PIXMA MG5580	gutenprint-ppd
Canon PIXMA MG5610	gutenprint-ppd
Canon PIXMA MG5620	gutenprint-ppd
Canon PIXMA MG5622	gutenprint-ppd
Canon PIXMA MG5640	gutenprint-ppd
Canon PIXMA MG5650	gutenprint-ppd
Canon PIXMA MG5660	gutenprint-ppd
Canon PIXMA MG5670	gutenprint-ppd
Canon PIXMA MG5680	gutenprint-ppd
Canon PIXMA MG5710	gutenprint-ppd
Canon PIXMA MG5720	gutenprint-ppd
Canon PIXMA MG5721	gutenprint-ppd
Canon PIXMA MG5722	gutenprint-ppd
Canon PIXMA MG5740	gutenprint-ppd
Canon PIXMA MG5750	gutenprint-ppd
Canon PIXMA MG5751	gutenprint-ppd
Canon PIXMA MG5752	gutenprint-ppd
Canon PIXMA MG5753	gutenprint-ppd
Canon PIXMA MG5770	gutenprint-ppd
Canon PIXMA MG5780	gutenprint-ppd
Canon PIXMA MG5790	gutenprint-ppd
Canon PIXMA MG5795	gutenprint-ppd
Canon PIXMA MG6100	gutenprint-ppd
Canon PIXMA MG6110	gutenprint-ppd
Canon PIXMA MG6120	gutenprint-ppd
Canon PIXMA MG6140	gutenprint-ppd
Canon PIXMA MG6150	gutenprint-ppd
Canon PIXMA MG6170	gutenprint-ppd
Canon PIXMA MG6180	gutenprint-ppd
Canon PIXMA MG6200	gutenprint-ppd
Canon PIXMA MG6210	gutenprint-ppd
Canon PIXMA MG6220	gutenprint-ppd
Canon PIXMA MG6240	gutenprint-ppd
Canon PIXMA MG6250	gutenprint-ppd
Canon PIXMA MG6270	gutenprint-ppd
Canon PIXMA MG6280	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MG6310	gutenprint-ppd
Canon PIXMA MG6320	gutenprint-ppd
Canon PIXMA MG6340	gutenprint-ppd
Canon PIXMA MG6350	gutenprint-ppd
Canon PIXMA MG6360	gutenprint-ppd
Canon PIXMA MG6370	gutenprint-ppd
Canon PIXMA MG6380	gutenprint-ppd
Canon PIXMA MG6400	gutenprint-ppd
Canon PIXMA MG6410	gutenprint-ppd
Canon PIXMA MG6420	gutenprint-ppd
Canon PIXMA MG6440	gutenprint-ppd
Canon PIXMA MG6450	gutenprint-ppd
Canon PIXMA MG6470	gutenprint-ppd
Canon PIXMA MG6610	gutenprint-ppd
Canon PIXMA MG6620	gutenprint-ppd
Canon PIXMA MG6622	gutenprint-ppd
Canon PIXMA MG6640	gutenprint-ppd
Canon PIXMA MG6650	gutenprint-ppd
Canon PIXMA MG6660	gutenprint-ppd
Canon PIXMA MG6670	gutenprint-ppd
Canon PIXMA MG6680	gutenprint-ppd
Canon PIXMA MG6810	gutenprint-ppd
Canon PIXMA MG6820	gutenprint-ppd
Canon PIXMA MG6821	gutenprint-ppd
Canon PIXMA MG6822	gutenprint-ppd
Canon PIXMA MG6840	gutenprint-ppd
Canon PIXMA MG6850	gutenprint-ppd
Canon PIXMA MG6851	gutenprint-ppd
Canon PIXMA MG6852	gutenprint-ppd
Canon PIXMA MG6853	gutenprint-ppd
Canon PIXMA MG6870	gutenprint-ppd
Canon PIXMA MG6880	gutenprint-ppd
Canon PIXMA MG7110	gutenprint-ppd
Canon PIXMA MG7120	gutenprint-ppd
Canon PIXMA MG7140	gutenprint-ppd
Canon PIXMA MG7150	gutenprint-ppd
Canon PIXMA MG7170	gutenprint-ppd
Canon PIXMA MG7180	gutenprint-ppd
Canon PIXMA MG7510	gutenprint-ppd
Canon PIXMA MG7520	gutenprint-ppd
Canon PIXMA MG7540	gutenprint-ppd
Canon PIXMA MG7550	gutenprint-ppd
Canon PIXMA MG7560	gutenprint-ppd
Canon PIXMA MG7570	gutenprint-ppd
Canon PIXMA MG7580	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MG7710	gutenprint-ppd
Canon PIXMA MG7720	gutenprint-ppd
Canon PIXMA MG7740	gutenprint-ppd
Canon PIXMA MG7750	gutenprint-ppd
Canon PIXMA MG7751	gutenprint-ppd
Canon PIXMA MG7752	gutenprint-ppd
Canon PIXMA MG7753	gutenprint-ppd
Canon PIXMA MG7770	gutenprint-ppd
Canon PIXMA MG7780	gutenprint-ppd
Canon PIXMA MG7790	gutenprint-ppd
Canon PIXMA MG8100	gutenprint-ppd
Canon PIXMA MG8120	gutenprint-ppd
Canon PIXMA MG8120B	gutenprint-ppd
Canon PIXMA MG8140	gutenprint-ppd
Canon PIXMA MG8150	gutenprint-ppd
Canon PIXMA MG8170	gutenprint-ppd
Canon PIXMA MG8180	gutenprint-ppd
Canon PIXMA MG8200	gutenprint-ppd
Canon PIXMA MG8220	gutenprint-ppd
Canon PIXMA MG8240	gutenprint-ppd
Canon PIXMA MG8250	gutenprint-ppd
Canon PIXMA MG8270	gutenprint-ppd
Canon PIXMA MG8280	gutenprint-ppd
Canon PIXMA mini220	gutenprint-ppd
Canon PIXMA mini320	gutenprint-ppd
Canon PIXMA mini360	gutenprint-ppd
Canon PIXMA MP140	gutenprint-ppd
Canon PIXMA MP145	gutenprint-ppd
Canon PIXMA MP150	gutenprint-ppd
Canon PIXMA MP160	gutenprint-ppd
Canon PIXMA MP170	gutenprint-ppd
Canon PIXMA MP180	gutenprint-ppd
Canon PIXMA MP190	gutenprint-ppd
Canon PIXMA MP198	gutenprint-ppd
Canon PIXMA MP210	gutenprint-ppd
Canon PIXMA MP218	gutenprint-ppd
Canon PIXMA MP220	gutenprint-ppd
Canon PIXMA MP228	gutenprint-ppd
Canon PIXMA MP230	gutenprint-ppd
Canon PIXMA MP236	gutenprint-ppd
Canon PIXMA MP237	gutenprint-ppd
Canon PIXMA MP240	gutenprint-ppd
Canon PIXMA MP245	gutenprint-ppd
Canon PIXMA MP250	gutenprint-ppd
Canon PIXMA MP252	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MP258	gutenprint-ppd
Canon PIXMA MP259	gutenprint-ppd
Canon PIXMA MP260	gutenprint-ppd
Canon PIXMA MP268	gutenprint-ppd
Canon PIXMA MP270	gutenprint-ppd
Canon PIXMA MP272	gutenprint-ppd
Canon PIXMA MP276	gutenprint-ppd
Canon PIXMA MP280	gutenprint-ppd
Canon PIXMA MP282	gutenprint-ppd
Canon PIXMA MP287	gutenprint-ppd
Canon PIXMA MP288	gutenprint-ppd
Canon PIXMA MP360	gutenprint-ppd
Canon PIXMA MP370	gutenprint-ppd
Canon PIXMA MP375R	gutenprint-ppd
Canon PIXMA MP390	gutenprint-ppd
Canon PIXMA MP450	gutenprint-ppd
Canon PIXMA MP460	gutenprint-ppd
Canon PIXMA MP470	gutenprint-ppd
Canon PIXMA MP476	gutenprint-ppd
Canon PIXMA MP480	gutenprint-ppd
Canon PIXMA MP486	gutenprint-ppd
Canon PIXMA MP490	gutenprint-ppd
Canon PIXMA MP492	gutenprint-ppd
Canon PIXMA MP493	gutenprint-ppd
Canon PIXMA MP495	gutenprint-ppd
Canon PIXMA MP496	gutenprint-ppd
Canon PIXMA MP497	gutenprint-ppd
Canon PIXMA MP498	gutenprint-ppd
Canon PIXMA MP499	gutenprint-ppd
Canon PIXMA MP500	gutenprint-ppd
Canon PIXMA MP510	gutenprint-ppd
Canon PIXMA MP520	gutenprint-ppd
Canon PIXMA MP530	gutenprint-ppd
Canon PIXMA MP540	gutenprint-ppd
Canon PIXMA MP545	gutenprint-ppd
Canon PIXMA MP550	gutenprint-ppd
Canon PIXMA MP558	gutenprint-ppd
Canon PIXMA MP560	gutenprint-ppd
Canon PIXMA MP568	gutenprint-ppd
Canon PIXMA MP600	gutenprint-ppd
Canon PIXMA MP600R	gutenprint-ppd
Canon PIXMA MP610	gutenprint-ppd
Canon PIXMA MP620	gutenprint-ppd
Canon PIXMA MP620B	gutenprint-ppd
Canon PIXMA MP628	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MP630	gutenprint-ppd
Canon PIXMA MP638	gutenprint-ppd
Canon PIXMA MP640	gutenprint-ppd
Canon PIXMA MP640R	gutenprint-ppd
Canon PIXMA MP648	gutenprint-ppd
Canon PIXMA MP700	gutenprint-ppd
Canon PIXMA MP710	gutenprint-ppd
Canon PIXMA MP730	gutenprint-ppd
Canon PIXMA MP740	gutenprint-ppd
Canon PIXMA MP750	gutenprint-ppd
Canon PIXMA MP760	gutenprint-ppd
Canon PIXMA MP770	gutenprint-ppd
Canon PIXMA MP780	gutenprint-ppd
Canon PIXMA MP790	gutenprint-ppd
Canon PIXMA MP800	gutenprint-ppd
Canon PIXMA MP800R	gutenprint-ppd
Canon PIXMA MP810	gutenprint-ppd
Canon PIXMA MP830	gutenprint-ppd
Canon PIXMA MP900	gutenprint-ppd
Canon PIXMA MP950	gutenprint-ppd
Canon PIXMA MP960	gutenprint-ppd
Canon PIXMA MP970	gutenprint-ppd
Canon PIXMA MP980	gutenprint-ppd
Canon PIXMA MP988	gutenprint-ppd
Canon PIXMA MP990	gutenprint-ppd
Canon PIXMA MP996	gutenprint-ppd
Canon PIXMA MX300	gutenprint-ppd
Canon PIXMA MX308	gutenprint-ppd
Canon PIXMA MX310	gutenprint-ppd
Canon PIXMA MX318	gutenprint-ppd
Canon PIXMA MX320	gutenprint-ppd
Canon PIXMA MX328	gutenprint-ppd
Canon PIXMA MX330	gutenprint-ppd
Canon PIXMA MX338	gutenprint-ppd
Canon PIXMA MX340	gutenprint-ppd
Canon PIXMA MX347	gutenprint-ppd
Canon PIXMA MX348	gutenprint-ppd
Canon PIXMA MX350	gutenprint-ppd
Canon PIXMA MX357	gutenprint-ppd
Canon PIXMA MX358	gutenprint-ppd
Canon PIXMA MX360	gutenprint-ppd
Canon PIXMA MX366	gutenprint-ppd
Canon PIXMA MX368	gutenprint-ppd
Canon PIXMA MX370	gutenprint-ppd
Canon PIXMA MX371	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MX372	gutenprint-ppd
Canon PIXMA MX374	gutenprint-ppd
Canon PIXMA MX375	gutenprint-ppd
Canon PIXMA MX376	gutenprint-ppd
Canon PIXMA MX377	gutenprint-ppd
Canon PIXMA MX378	gutenprint-ppd
Canon PIXMA MX391	gutenprint-ppd
Canon PIXMA MX392	gutenprint-ppd
Canon PIXMA MX394	gutenprint-ppd
Canon PIXMA MX395	gutenprint-ppd
Canon PIXMA MX396	gutenprint-ppd
Canon PIXMA MX397	gutenprint-ppd
Canon PIXMA MX398	gutenprint-ppd
Canon PIXMA MX410	gutenprint-ppd
Canon PIXMA MX416	gutenprint-ppd
Canon PIXMA MX418	gutenprint-ppd
Canon PIXMA MX420	gutenprint-ppd
Canon PIXMA MX426	gutenprint-ppd
Canon PIXMA MX428	gutenprint-ppd
Canon PIXMA MX430	gutenprint-ppd
Canon PIXMA MX431	gutenprint-ppd
Canon PIXMA MX432	gutenprint-ppd
Canon PIXMA MX434	gutenprint-ppd
Canon PIXMA MX435	gutenprint-ppd
Canon PIXMA MX436	gutenprint-ppd
Canon PIXMA MX437	gutenprint-ppd
Canon PIXMA MX438	gutenprint-ppd
Canon PIXMA MX439	gutenprint-ppd
Canon PIXMA MX451	gutenprint-ppd
Canon PIXMA MX452	gutenprint-ppd
Canon PIXMA MX454	gutenprint-ppd
Canon PIXMA MX455	gutenprint-ppd
Canon PIXMA MX456	gutenprint-ppd
Canon PIXMA MX457	gutenprint-ppd
Canon PIXMA MX458	gutenprint-ppd
Canon PIXMA MX459	gutenprint-ppd
Canon PIXMA MX471	gutenprint-ppd
Canon PIXMA MX472	gutenprint-ppd
Canon PIXMA MX474	gutenprint-ppd
Canon PIXMA MX475	gutenprint-ppd
Canon PIXMA MX476	gutenprint-ppd
Canon PIXMA MX477	gutenprint-ppd
Canon PIXMA MX478	gutenprint-ppd
Canon PIXMA MX479	gutenprint-ppd
Canon PIXMA MX490	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MX492	gutenprint-ppd
Canon PIXMA MX494	gutenprint-ppd
Canon PIXMA MX495	gutenprint-ppd
Canon PIXMA MX496	gutenprint-ppd
Canon PIXMA MX497	gutenprint-ppd
Canon PIXMA MX498	gutenprint-ppd
Canon PIXMA MX499	gutenprint-ppd
Canon PIXMA MX510	gutenprint-ppd
Canon PIXMA MX511	gutenprint-ppd
Canon PIXMA MX512	gutenprint-ppd
Canon PIXMA MX514	gutenprint-ppd
Canon PIXMA MX515	gutenprint-ppd
Canon PIXMA MX516	gutenprint-ppd
Canon PIXMA MX517	gutenprint-ppd
Canon PIXMA MX518	gutenprint-ppd
Canon PIXMA MX521	gutenprint-ppd
Canon PIXMA MX522	gutenprint-ppd
Canon PIXMA MX524	gutenprint-ppd
Canon PIXMA MX525	gutenprint-ppd
Canon PIXMA MX526	gutenprint-ppd
Canon PIXMA MX527	gutenprint-ppd
Canon PIXMA MX528	gutenprint-ppd
Canon PIXMA MX531	gutenprint-ppd
Canon PIXMA MX532	gutenprint-ppd
Canon PIXMA MX534	gutenprint-ppd
Canon PIXMA MX535	gutenprint-ppd
Canon PIXMA MX536	gutenprint-ppd
Canon PIXMA MX537	gutenprint-ppd
Canon PIXMA MX538	gutenprint-ppd
Canon PIXMA MX700	gutenprint-ppd
Canon PIXMA MX710	gutenprint-ppd
Canon PIXMA MX711	gutenprint-ppd
Canon PIXMA MX712	gutenprint-ppd
Canon PIXMA MX714	gutenprint-ppd
Canon PIXMA MX715	gutenprint-ppd
Canon PIXMA MX721	gutenprint-ppd
Canon PIXMA MX722	gutenprint-ppd
Canon PIXMA MX725	gutenprint-ppd
Canon PIXMA MX726	gutenprint-ppd
Canon PIXMA MX727	gutenprint-ppd
Canon PIXMA MX728	gutenprint-ppd
Canon PIXMA MX7600	gutenprint-ppd
Canon PIXMA MX850	gutenprint-ppd
Canon PIXMA MX860	gutenprint-ppd
Canon PIXMA MX868	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXMA MX870	gutenprint-ppd
Canon PIXMA MX876	gutenprint-ppd
Canon PIXMA MX880	gutenprint-ppd
Canon PIXMA MX882	gutenprint-ppd
Canon PIXMA MX884	gutenprint-ppd
Canon PIXMA MX885	gutenprint-ppd
Canon PIXMA MX886	gutenprint-ppd
Canon PIXMA MX888	gutenprint-ppd
Canon PIXMA MX890	gutenprint-ppd
Canon PIXMA MX892	gutenprint-ppd
Canon PIXMA MX894	gutenprint-ppd
Canon PIXMA MX895	gutenprint-ppd
Canon PIXMA MX897	gutenprint-ppd
Canon PIXMA MX898	gutenprint-ppd
Canon PIXMA MX922	gutenprint-ppd
Canon PIXMA MX924	gutenprint-ppd
Canon PIXMA MX925	gutenprint-ppd
Canon PIXMA MX926	gutenprint-ppd
Canon PIXMA MX927	gutenprint-ppd
Canon PIXMA MX928	gutenprint-ppd
Canon PIXMA P200	gutenprint-ppd
Canon PIXMA Pro9000	gutenprint-ppd
Canon PIXMA Pro9000mk2	gutenprint-ppd
Canon PIXMA Pro9500	gutenprint-ppd
Canon PIXMA Pro9500mk2	gutenprint-ppd
Canon PIXUS 50i	gutenprint-ppd
Canon PIXUS 80i	gutenprint-ppd
Canon PIXUS 450i	gutenprint-ppd
Canon PIXUS 455i	gutenprint-ppd
Canon PIXUS 550i	gutenprint-ppd
Canon PIXUS 560i	gutenprint-ppd
Canon PIXUS 850i	gutenprint-ppd
Canon PIXUS 860i	gutenprint-ppd
Canon PIXUS 865R	gutenprint-ppd
Canon PIXUS 900PD	gutenprint-ppd
Canon PIXUS 950i	gutenprint-ppd
Canon PIXUS 960i	gutenprint-ppd
Canon PIXUS 990i	gutenprint-ppd
Canon PIXUS 470PD	gutenprint-ppd
Canon PIXUS 475PD	gutenprint-ppd
Canon PIXUS 6100i	gutenprint-ppd
Canon PIXUS 6500i	gutenprint-ppd
Canon PIXUS 9100i	gutenprint-ppd
Canon PIXUS 9900i	gutenprint-ppd
Canon PIXUS iP100	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXUS iP110	gutenprint-ppd
Canon PIXUS iP2000	gutenprint-ppd
Canon PIXUS iP2700	gutenprint-ppd
Canon PIXUS iP3100	gutenprint-ppd
Canon PIXUS iP3300	gutenprint-ppd
Canon PIXUS iP3500	gutenprint-ppd
Canon PIXUS iP3600	gutenprint-ppd
Canon PIXUS iP4100	gutenprint-ppd
Canon PIXUS iP4100R	gutenprint-ppd
Canon PIXUS iP4200	gutenprint-ppd
Canon PIXUS iP4300	gutenprint-ppd
Canon PIXUS iP4500	gutenprint-ppd
Canon PIXUS iP4600	gutenprint-ppd
Canon PIXUS iP4700	gutenprint-ppd
Canon PIXUS iP4830	gutenprint-ppd
Canon PIXUS iP4930	gutenprint-ppd
Canon PIXUS iP5200R	gutenprint-ppd
Canon PIXUS iP6100D	gutenprint-ppd
Canon PIXUS iP6600D	gutenprint-ppd
Canon PIXUS iP6700D	gutenprint-ppd
Canon PIXUS iP7100	gutenprint-ppd
Canon PIXUS iP7230	gutenprint-ppd
Canon PIXUS iP7500	gutenprint-ppd
Canon PIXUS iP8100	gutenprint-ppd
Canon PIXUS iP8600	gutenprint-ppd
Canon PIXUS iP8730	gutenprint-ppd
Canon PIXUS iP90	gutenprint-ppd
Canon PIXUS iP90v	gutenprint-ppd
Canon PIXUS iP9910	gutenprint-ppd
Canon PIXUS iX5000	gutenprint-ppd
Canon PIXUS iX6530	gutenprint-ppd
Canon PIXUS iX6830	gutenprint-ppd
Canon PIXUS iX7000	gutenprint-ppd
Canon PIXUS MG2130	gutenprint-ppd
Canon PIXUS MG3130	gutenprint-ppd
Canon PIXUS MG3230	gutenprint-ppd
Canon PIXUS MG3530	gutenprint-ppd
Canon PIXUS MG3630	gutenprint-ppd
Canon PIXUS MG4130	gutenprint-ppd
Canon PIXUS MG4230	gutenprint-ppd
Canon PIXUS MG5130	gutenprint-ppd
Canon PIXUS MG5230	gutenprint-ppd
Canon PIXUS MG5330	gutenprint-ppd
Canon PIXUS MG5430	gutenprint-ppd
Canon PIXUS MG5530	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXUS MG5630	gutenprint-ppd
Canon PIXUS MG5730	gutenprint-ppd
Canon PIXUS MG6130	gutenprint-ppd
Canon PIXUS MG6230	gutenprint-ppd
Canon PIXUS MG6330	gutenprint-ppd
Canon PIXUS MG6530	gutenprint-ppd
Canon PIXUS MG6730	gutenprint-ppd
Canon PIXUS MG6930	gutenprint-ppd
Canon PIXUS MG7130	gutenprint-ppd
Canon PIXUS MG7530	gutenprint-ppd
Canon PIXUS MG7530F	gutenprint-ppd
Canon PIXUS MG7730	gutenprint-ppd
Canon PIXUS MG7730F	gutenprint-ppd
Canon PIXUS MG8130	gutenprint-ppd
Canon PIXUS MG8230	gutenprint-ppd
Canon PIXUS mini220	gutenprint-ppd
Canon PIXUS mini360	gutenprint-ppd
Canon PIXUS MP55	gutenprint-ppd
Canon PIXUS MP170	gutenprint-ppd
Canon PIXUS MP270	gutenprint-ppd
Canon PIXUS MP280	gutenprint-ppd
Canon PIXUS MP360	gutenprint-ppd
Canon PIXUS MP370	gutenprint-ppd
Canon PIXUS MP375R	gutenprint-ppd
Canon PIXUS MP390	gutenprint-ppd
Canon PIXUS MP450	gutenprint-ppd
Canon PIXUS MP460	gutenprint-ppd
Canon PIXUS MP470	gutenprint-ppd
Canon PIXUS MP480	gutenprint-ppd
Canon PIXUS MP490	gutenprint-ppd
Canon PIXUS MP493	gutenprint-ppd
Canon PIXUS MP500	gutenprint-ppd
Canon PIXUS MP510	gutenprint-ppd
Canon PIXUS MP520	gutenprint-ppd
Canon PIXUS MP540	gutenprint-ppd
Canon PIXUS MP550	gutenprint-ppd
Canon PIXUS MP560	gutenprint-ppd
Canon PIXUS MP600	gutenprint-ppd
Canon PIXUS MP610	gutenprint-ppd
Canon PIXUS MP620	gutenprint-ppd
Canon PIXUS MP630	gutenprint-ppd
Canon PIXUS MP640	gutenprint-ppd
Canon PIXUS MP700	gutenprint-ppd
Canon PIXUS MP710	gutenprint-ppd
Canon PIXUS MP730	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon PIXUS MP740	gutenprint-ppd
Canon PIXUS MP770	gutenprint-ppd
Canon PIXUS MP790	gutenprint-ppd
Canon PIXUS MP800	gutenprint-ppd
Canon PIXUS MP810	gutenprint-ppd
Canon PIXUS MP830	gutenprint-ppd
Canon PIXUS MP900	gutenprint-ppd
Canon PIXUS MP950	gutenprint-ppd
Canon PIXUS MP960	gutenprint-ppd
Canon PIXUS MP970	gutenprint-ppd
Canon PIXUS MP980	gutenprint-ppd
Canon PIXUS MP990	gutenprint-ppd
Canon PIXUS MX350	gutenprint-ppd
Canon PIXUS MX420	gutenprint-ppd
Canon PIXUS MX513	gutenprint-ppd
Canon PIXUS MX523	gutenprint-ppd
Canon PIXUS MX7600	gutenprint-ppd
Canon PIXUS MX850	gutenprint-ppd
Canon PIXUS MX860	gutenprint-ppd
Canon PIXUS MX870	gutenprint-ppd
Canon PIXUS MX883	gutenprint-ppd
Canon PIXUS MX893	gutenprint-ppd
Canon PIXUS MX923	gutenprint-ppd
Canon PIXUS Pro9000	gutenprint-ppd
Canon PIXUS Pro9000mk2	gutenprint-ppd
Canon PIXUS Pro9500	gutenprint-ppd
Canon PIXUS Pro9500mk2	gutenprint-ppd
Canon Pro9000 Mk.II series	gutenprint-ppd
Canon Pro9000 series	gutenprint-ppd
Canon Pro9500 Mk.II series	gutenprint-ppd
Canon Pro9500 series	gutenprint-ppd
Canon S100	gutenprint-ppd
Canon S100SP	OpenPrintingPPDs-ghostscript
Canon S200	gutenprint-ppd
Canon S300	gutenprint-ppd
Canon S330	gutenprint-ppd
Canon S330 Photo	OpenPrintingPPDs-ghostscript
Canon S400	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon S450	gutenprint-ppd
Canon S500	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon S520	gutenprint-ppd
Canon S530D	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon S600	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon S630	OpenPrintingPPDs-ghostscript gutenprint-ppd
Canon S750	gutenprint-ppd
Canon S800	gutenprint-ppd
Canon S820	gutenprint-ppd
Canon S830D	gutenprint-ppd
Canon S900	gutenprint-ppd
Canon S4500	gutenprint-ppd
Canon S9000	gutenprint-ppd
Canon SELPHY CP400	gutenprint-ppd
Canon SELPHY CP500	gutenprint-ppd
Canon SELPHY CP510	gutenprint-ppd
Canon SELPHY CP520	gutenprint-ppd
Canon SELPHY CP530	gutenprint-ppd
Canon SELPHY CP600	gutenprint-ppd
Canon SELPHY CP710	gutenprint-ppd
Canon SELPHY CP720	gutenprint-ppd
Canon SELPHY CP730	gutenprint-ppd
Canon SELPHY CP740	gutenprint-ppd
Canon SELPHY CP750	gutenprint-ppd
Canon SELPHY CP760	gutenprint-ppd
Canon SELPHY CP770	gutenprint-ppd
Canon SELPHY CP780	gutenprint-ppd
Canon SELPHY CP790	gutenprint-ppd
Canon SELPHY CP800	gutenprint-ppd
Canon SELPHY CP810	gutenprint-ppd
Canon SELPHY CP820	gutenprint-ppd
Canon SELPHY CP900	gutenprint-ppd
Canon SELPHY CP910	gutenprint-ppd
Canon SELPHY CP1000	gutenprint-ppd
Canon SELPHY CP1200	gutenprint-ppd
Canon SELPHY DS700	gutenprint-ppd
Canon SELPHY DS810	gutenprint-ppd
Canon SELPHY ES1	gutenprint-ppd
Canon SELPHY ES2	gutenprint-ppd
Canon SELPHY ES3	gutenprint-ppd
Canon SELPHY ES20	gutenprint-ppd
Canon SELPHY ES30	gutenprint-ppd
Canon SELPHY ES40	gutenprint-ppd
Canon SmartBase MP360	gutenprint-ppd
Canon SmartBase MP360S	gutenprint-ppd
Canon SmartBase MP370	gutenprint-ppd
Canon SmartBase MP390	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Canon SmartBase MP700	gutenprint-ppd
Canon SmartBase MP730	gutenprint-ppd
Canon SmartBase MPC400	gutenprint-ppd
Canon SmartBase MPC600F	gutenprint-ppd

Печатающие устройства производства CIAAT, Citizen, Compaq

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
CIAAT	
CIAAT CIAAT Brava 21	gutenprint-ppd
Citizen	
Citizen CW-01	gutenprint-ppd
Citizen CW-02	gutenprint-ppd
Citizen CX	gutenprint-ppd
Citizen CX-W	gutenprint-ppd
Citizen CY	gutenprint-ppd
Citizen OP900	gutenprint-ppd
Citizen OP900II	gutenprint-ppd
Citizen ProJet II	gutenprint-ppd
Citizen ProJet II	OpenPrintingPPDs-ghostscript
Citizen ProJet IIc	OpenPrintingPPDs-ghostscript
Compaq	
Compaq IJ1200	gutenprint-ppd
Compaq IJ750	OpenPrintingPPDs-ghostscript
Compaq IJ900	OpenPrintingPPDs-ghostscript

Печатающие устройства производства Dai Nippon, DatamaxONeil, DEC, Dell

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Dai Nippon	
Dai Nippon Printing DS40	gutenprint-ppd
Dai Nippon Printing DS80	gutenprint-ppd
Dai Nippon Printing DS80DX	gutenprint-ppd
Dai Nippon Printing DS620	gutenprint-ppd
Dai Nippon Printing DS820	gutenprint-ppd
Dai Nippon Printing DSRX1	gutenprint-ppd
Dai Nippon Printing SL10	gutenprint-ppd
DatamaxONeil	
Datamax-ONeil E4204B Mark III	gutenprint-ppd
Datamax-ONeil E4205A Mark III	gutenprint-ppd
Datamax-ONeil E4206L Mark III	gutenprint-ppd
Datamax-ONeil E4206P Mark III	gutenprint-ppd
Datamax-ONeil E4304B Mark III	gutenprint-ppd
Datamax-ONeil E4305A Mark III	gutenprint-ppd
Datamax-ONeil E4305L Mark III	gutenprint-ppd
Datamax-ONeil E4305P Mark III	gutenprint-ppd
Datamax-ONeil H8308p	gutenprint-ppd
Datamax-ONeil I4212e Mark II	gutenprint-ppd
Datamax-ONeil I4310e Mark II	gutenprint-ppd
Datamax-ONeil I4606e Mark II	gutenprint-ppd
Datamax-ONeil p1115	gutenprint-ppd
Datamax-ONeil p1115s	gutenprint-ppd
Datamax-ONeil p1120n	gutenprint-ppd
Datamax-ONeil p1125	gutenprint-ppd
Datamax-ONeil p1725	gutenprint-ppd
Datamax-ONeil RL3e	gutenprint-ppd
Datamax-ONeil RL4e	gutenprint-ppd
Datamax-ONeil w1110	gutenprint-ppd
DEC	
DEC 1800	OpenPrintingPPDs-ghostscript
DEC 1800	gutenprint-ppd
DEC LN17	gutenprint-ppd
DEC DECwriter 110i	OpenPrintingPPDs-ghostscript
DEC DECWriter 500i	OpenPrintingPPDs-ghostscript
DEC DECwriter 520ic	OpenPrintingPPDs-ghostscript
DEC LA50	OpenPrintingPPDs-ghostscript
DEC LA70	OpenPrintingPPDs-ghostscript
DEC LA75	OpenPrintingPPDs-ghostscript
DEC LA75 Plus	OpenPrintingPPDs-ghostscript
DEC LJ250	OpenPrintingPPDs-ghostscript
DEC LN03	OpenPrintingPPDs-ghostscript
DEC LN07	OpenPrintingPPDs-postscript
DEC LN17	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
DEC LN17	OpenPrintingPPDs-hpijs
Dell	
Dell 1355	foo2zjs
Dell C1765	foo2zjs
Dell Laser Printer 1110	OpenPrintingPPDs-ghostscript
Dell Laser Printer 3000cn	OpenPrintingPPDs-ghostscript
Dell Laser Printer 3100cn	OpenPrintingPPDs-ghostscript
Dell M5200	OpenPrintingPPDs-postscript
Dell S2500	OpenPrintingPPDs-postscript

Печатающие устройства производства Epson

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson ActionLaser 1100	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson ActionLaser II	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson ActionPrinter 3250	OpenPrintingPPDs-ghostscript
Epson AL-2600	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson AL-C1900	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Epson AL-C1900 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Epson AL-C2000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson AL-C2000 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson AL-C2600	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson AL-C2800	OpenPrintingPPDs-postscript
Epson AL-C3800	OpenPrintingPPDs-postscript
Epson AL-C4000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Epson AL-C4000 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Epson AL-C4100	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Epson AL-C4200	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson AL-C8500	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Epson AL-C8500 PS3	manufacturer-PPDs
Epson AL-C8500PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson AL-C8600	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Epson AL-C8600 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Epson AL-C9000	manufacturer-PPDs
Epson AL-C9100	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson AL-C9200	OpenPrintingPPDs-postscript
Epson AL-CX17NF	foo2zjs
Epson AL-CX21	OpenPrintingPPDs-postscript
Epson AL-M1400	foo2zjs
Epson AL-M2000	OpenPrintingPPDs-postscript
Epson AL-M2010	OpenPrintingPPDs-postscript
Epson AL-M2400	OpenPrintingPPDs-postscript
Epson AL-M2410	OpenPrintingPPDs-postscript
Epson AL-M4000	OpenPrintingPPDs-postscript
Epson AL-M8000	OpenPrintingPPDs-postscript
Epson AL-MX20	OpenPrintingPPDs-postscript
Epson AL-MX21	OpenPrintingPPDs-postscript
Epson AL-C8500	gutenprint-ppd
Epson AL-C8500PS	gutenprint-ppd
Epson AL-C8600	gutenprint-ppd
Epson AL-C8600 PS3	gutenprint-ppd
Epson Artisan 50	gutenprint-ppd
Epson Artisan 700	gutenprint-ppd
Epson Artisan 710	gutenprint-ppd
Epson Artisan 800	gutenprint-ppd
Epson Artisan 810	gutenprint-ppd
Epson Artisan 835	gutenprint-ppd
Epson B-300	gutenprint-ppd
Epson B-308	gutenprint-ppd
Epson B-310	gutenprint-ppd
Epson B-310N	gutenprint-ppd
Epson B-500DN	gutenprint-ppd
Epson B-508DN	gutenprint-ppd
Epson B-510DN	gutenprint-ppd
Epson CL 700	gutenprint-ppd
Epson CL 750	gutenprint-ppd
Epson CL 760	gutenprint-ppd
Epson E 100	gutenprint-ppd
Epson E 150	gutenprint-ppd
Epson E 200	gutenprint-ppd
Epson E 300	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson E 500	gutenprint-ppd
Epson E 520	gutenprint-ppd
Epson E 700	gutenprint-ppd
Epson E 720	gutenprint-ppd
Epson EM 900C	gutenprint-ppd
Epson EM 930C	gutenprint-ppd
Epson EP 302	gutenprint-ppd
Epson EP 702A	gutenprint-ppd
Epson EP 801A	gutenprint-ppd
Epson EP 901A	gutenprint-ppd
Epson EP 901F	gutenprint-ppd
Epson EPL-5200	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson EPL-5200+	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson EPL-5700	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-5700PS	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson EPL-5800	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-5800PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson EPL-5900	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-5900 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson EPL-6100	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-6100 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson EPL-6200	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson EPL-7100	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson EPL-C8200 PS3	manufacturer-PPDs
Epson EPL-N1600	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Epson EPL-N1600PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Epson EPL-N2050	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson EPL-N2050 PS	manufacturer-PPDs gutenprint-ppd
Epson EPL-N2050+	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson EPL-N2050 PS+	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson EPL-N2120	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-N2500	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-N2500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Epson EPL-N2550	OpenPrintingPPDs-postscript
Epson EPL-N2700	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson EPL-N2750	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Epson EPL-N2750 PS	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson EPL-N3000	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson EPL-N4000 PS	manufacturer-PPDs
Epson EPL-N4000+ PS3	manufacturer-PPDs
Epson EPL-N7000	manufacturer-PPDs OpenPrintingPPDs-postscript
Epson GT-S55	All-in-one package
Epson L120	gutenprint-ppd
Epson L1300	gutenprint-ppd
Epson L1800	gutenprint-ppd
Epson L210	gutenprint-ppd
Epson L-1000	OpenPrintingPPDs-ghostscript
Epson LP-2000	OpenPrintingPPDs-ghostscript
Epson LP-3000	OpenPrintingPPDs-ghostscript
Epson LP-7000	OpenPrintingPPDs-ghostscript
Epson LP-7000G	OpenPrintingPPDs-ghostscript
Epson LP-8000	OpenPrintingPPDs-ghostscript
Epson LP-8300CPD	OpenPrintingPPDs-postscript
Epson LP-8500CPD	OpenPrintingPPDs-postscript
Epson LP-9600SPD	OpenPrintingPPDs-postscript
Epson LQ-24	OpenPrintingPPDs-ghostscript
Epson LQ-500	OpenPrintingPPDs-ghostscript
Epson LQ-570+	OpenPrintingPPDs-ghostscript
Epson LQ-850	OpenPrintingPPDs-ghostscript
Epson LQ-2550	OpenPrintingPPDs-ghostscript
Epson LX-300+	OpenPrintingPPDs-ghostscript
Epson LX-1050	OpenPrintingPPDs-ghostscript
Epson MachJet	OpenPrintingPPDs-ghostscript
Epson MC 2000	gutenprint-ppd
Epson MC 5000	gutenprint-ppd
Epson MC 7000	gutenprint-ppd
Epson MC 9000	gutenprint-ppd
Epson MC 10000	gutenprint-ppd
Epson ME 300	gutenprint-ppd
Epson ME 320	gutenprint-ppd
Epson ME Office 70	gutenprint-ppd
Epson ME Office 80W	gutenprint-ppd
Epson ME Office 82WD	gutenprint-ppd
Epson ME Office 85ND	gutenprint-ppd
Epson ME Office 360	gutenprint-ppd
Epson ME Office 600F	gutenprint-ppd
Epson ME Office 620F	gutenprint-ppd
Epson ME Office 700FW	gutenprint-ppd
Epson ME Office 900WD	gutenprint-ppd
Epson ME Office 940FW	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson ME Office 960FWD	gutenprint-ppd
Epson ME Office 1100	gutenprint-ppd
Epson MJ 520C	OpenPrintingPPDs-ghostscript
Epson MJ 930C	gutenprint-ppd
Epson MJ 5100C	gutenprint-ppd
Epson MJ 6000C	gutenprint-ppd
Epson MJ 8000C	gutenprint-ppd
Epson Offirio PX B300	gutenprint-ppd
Epson Offirio PX B500	gutenprint-ppd
Epson PictureMate	gutenprint-ppd
Epson PictureMate 100	gutenprint-ppd
Epson PictureMate 200	gutenprint-ppd
Epson PictureMate 210	gutenprint-ppd
Epson PictureMate 215	gutenprint-ppd
Epson PictureMate 240	gutenprint-ppd
Epson PictureMate 250	gutenprint-ppd
Epson PictureMate 260	gutenprint-ppd
Epson PictureMate 270	gutenprint-ppd
Epson PictureMate 280	gutenprint-ppd
Epson PictureMate 290	gutenprint-ppd
Epson PictureMate 500	gutenprint-ppd
Epson PictureMate 2005	gutenprint-ppd
Epson PictureMate Dash	gutenprint-ppd
Epson PictureMate Deluxe	gutenprint-ppd
Epson PictureMate Flash	gutenprint-ppd
Epson PictureMate Pal	gutenprint-ppd
Epson PictureMate Snap	gutenprint-ppd
Epson PM 670C	gutenprint-ppd
Epson PM 700C	gutenprint-ppd
Epson PM 730C	gutenprint-ppd
Epson PM 740C	gutenprint-ppd
Epson PM 750C	gutenprint-ppd
Epson PM 760C	gutenprint-ppd
Epson PM 770C	gutenprint-ppd
Epson PM 780C	gutenprint-ppd
Epson PM 790PT	gutenprint-ppd
Epson PM 800C	gutenprint-ppd
Epson PM 850PT	gutenprint-ppd
Epson PM 870C	gutenprint-ppd
Epson PM 880C	gutenprint-ppd
Epson PM 930C	gutenprint-ppd
Epson PM 940C	gutenprint-ppd
Epson PM 950C	gutenprint-ppd
Epson PM 970C	gutenprint-ppd
Epson PM 980C	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson PM 2000C	gutenprint-ppd
Epson PM 2200C	gutenprint-ppd
Epson PM 3000C	gutenprint-ppd
Epson PM 3300C	gutenprint-ppd
Epson PM 3500C	gutenprint-ppd
Epson PM 3700C	gutenprint-ppd
Epson PM 5000C	gutenprint-ppd
Epson PM 7000C	gutenprint-ppd
Epson PM 9000C	gutenprint-ppd
Epson PM 10000	gutenprint-ppd
Epson PM 4000PX	gutenprint-ppd
Epson PM A650	gutenprint-ppd
Epson PM A750	gutenprint-ppd
Epson PM A820	gutenprint-ppd
Epson PM A890	gutenprint-ppd
Epson PM A900	gutenprint-ppd
Epson PM A940	gutenprint-ppd
Epson PM A950	gutenprint-ppd
Epson PM D600	gutenprint-ppd
Epson PM D750	gutenprint-ppd
Epson PM D770	gutenprint-ppd
Epson PM D800	gutenprint-ppd
Epson PM D870	gutenprint-ppd
Epson PM D1000	gutenprint-ppd
Epson PM G700	gutenprint-ppd
Epson PM G720	gutenprint-ppd
Epson PM G730	gutenprint-ppd
Epson PM G800	gutenprint-ppd
Epson PM G820	gutenprint-ppd
Epson PM G850	gutenprint-ppd
Epson PM G4500	gutenprint-ppd
Epson PM T960	gutenprint-ppd
Epson PX 7V	gutenprint-ppd
Epson PX 101	gutenprint-ppd
Epson PX 1001	gutenprint-ppd
Epson PX 1200	gutenprint-ppd
Epson PX 1600F	gutenprint-ppd
Epson PX 1700F	gutenprint-ppd
Epson PX 201	gutenprint-ppd
Epson PX 203	gutenprint-ppd
Epson PX 204	gutenprint-ppd
Epson PX 401A	gutenprint-ppd
Epson PX 503A	gutenprint-ppd
Epson PX 504A	gutenprint-ppd
Epson PX 601F	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson PX 603F	gutenprint-ppd
Epson PX 5500	gutenprint-ppd
Epson PX 7000	gutenprint-ppd
Epson PX 9000	gutenprint-ppd
Epson PX A650	gutenprint-ppd
Epson PX G5000	gutenprint-ppd
Epson PX G5300	gutenprint-ppd
Epson PX G5600	gutenprint-ppd
Epson PX G900	gutenprint-ppd
Epson PX G920	gutenprint-ppd
Epson PX V500	gutenprint-ppd
Epson PX V600	gutenprint-ppd
Epson PX V630	gutenprint-ppd
Epson PX V780	gutenprint-ppd
Epson SQ 1170	OpenPrintingPPDs-ghostscript
Epson Stylus 800	OpenPrintingPPDs-ghostscript
Epson Stylus C20	gutenprint-ppd
Epson Stylus C20SX	gutenprint-ppd
Epson Stylus C20UX	gutenprint-ppd
Epson Stylus C40	gutenprint-ppd
Epson Stylus C40SX	gutenprint-ppd
Epson Stylus C40UX	gutenprint-ppd
Epson Stylus C41	gutenprint-ppd
Epson Stylus C41SX	gutenprint-ppd
Epson Stylus C41UX	gutenprint-ppd
Epson Stylus C42	gutenprint-ppd
Epson Stylus C42SX	gutenprint-ppd
Epson Stylus C42UX	gutenprint-ppd
Epson Stylus C43	gutenprint-ppd
Epson Stylus C43SX	gutenprint-ppd
Epson Stylus C43UX	gutenprint-ppd
Epson Stylus C44	gutenprint-ppd
Epson Stylus C44SX	gutenprint-ppd
Epson Stylus C44UX	gutenprint-ppd
Epson Stylus C45	gutenprint-ppd
Epson Stylus C46	gutenprint-ppd
Epson Stylus C48	gutenprint-ppd
Epson Stylus C50	gutenprint-ppd
Epson Stylus C60	gutenprint-ppd
Epson Stylus C61	gutenprint-ppd
Epson Stylus C62	gutenprint-ppd
Epson Stylus C63	gutenprint-ppd
Epson Stylus C64	gutenprint-ppd
Epson Stylus C65	gutenprint-ppd
Epson Stylus C66	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus C68	gutenprint-ppd
Epson Stylus C70	gutenprint-ppd
Epson Stylus C79	gutenprint-ppd
Epson Stylus C80	gutenprint-ppd
Epson Stylus C82	gutenprint-ppd
Epson Stylus C83	gutenprint-ppd
Epson Stylus C84	gutenprint-ppd
Epson Stylus C85	gutenprint-ppd
Epson Stylus C86	gutenprint-ppd
Epson Stylus C87	gutenprint-ppd
Epson Stylus C88	gutenprint-ppd
Epson Stylus C92	gutenprint-ppd
Epson Stylus C110	gutenprint-ppd
Epson Stylus C120	gutenprint-ppd
Epson Stylus Color I	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color II	gutenprint-ppd
Epson Stylus Color IIs	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color PRO	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 8	gutenprint-ppd
Epson Stylus Color 200	OpenPrintingPPDs-ghostscript
Epson Stylus Color 300	OpenPrintingPPDs-ghostscript
Epson Stylus Color 400	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 440	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 460	gutenprint-ppd
Epson Stylus Color 480	gutenprint-ppd
Epson Stylus Color 500	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 580	gutenprint-ppd
Epson Stylus Color 600	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 640	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 660	gutenprint-ppd
Epson Stylus Color 670	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 680	gutenprint-ppd
Epson Stylus Color 740	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 760	gutenprint-ppd
Epson Stylus Color 777	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus Color 800	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 850	gutenprint-ppd
Epson Stylus Color 860	gutenprint-ppd
Epson Stylus Color 880	gutenprint-ppd
Epson Stylus Color 900	gutenprint-ppd
Epson Stylus Color 980	gutenprint-ppd
Epson Stylus Color 1160	gutenprint-ppd
Epson Stylus Color 1500	gutenprint-ppd
Epson Stylus Color 1520	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Color 3000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus CX1500	gutenprint-ppd
Epson Stylus CX3100	gutenprint-ppd
Epson Stylus CX3200	gutenprint-ppd
Epson Stylus CX3500	gutenprint-ppd
Epson Stylus CX3600	gutenprint-ppd
Epson Stylus CX3650	gutenprint-ppd
Epson Stylus CX3700	gutenprint-ppd
Epson Stylus CX3800	gutenprint-ppd
Epson Stylus CX3805	gutenprint-ppd
Epson Stylus CX3810	gutenprint-ppd
Epson Stylus CX3900	gutenprint-ppd
Epson Stylus CX4100	gutenprint-ppd
Epson Stylus CX4200	gutenprint-ppd
Epson Stylus CX4400	gutenprint-ppd
Epson Stylus CX4500	gutenprint-ppd
Epson Stylus CX4600	gutenprint-ppd
Epson Stylus CX4700	gutenprint-ppd
Epson Stylus CX4800	gutenprint-ppd
Epson Stylus CX4900	gutenprint-ppd
Epson Stylus CX5000	gutenprint-ppd
Epson Stylus CX5000F	gutenprint-ppd
Epson Stylus CX5100	gutenprint-ppd
Epson Stylus CX5200	gutenprint-ppd
Epson Stylus CX5300	gutenprint-ppd
Epson Stylus CX5400	gutenprint-ppd
Epson Stylus CX5500	gutenprint-ppd
Epson Stylus CX5600	gutenprint-ppd
Epson Stylus CX5700	gutenprint-ppd
Epson Stylus CX5800	gutenprint-ppd
Epson Stylus CX6000	gutenprint-ppd
Epson Stylus CX6300	gutenprint-ppd
Epson Stylus CX6400	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus CX6500	gutenprint-ppd
Epson Stylus CX6600	gutenprint-ppd
Epson Stylus CX7000F	gutenprint-ppd
Epson Stylus CX7300	gutenprint-ppd
Epson Stylus CX7400	gutenprint-ppd
Epson Stylus CX7700	gutenprint-ppd
Epson Stylus CX7800	gutenprint-ppd
Epson Stylus CX8300	gutenprint-ppd
Epson Stylus CX8400	gutenprint-ppd
Epson Stylus CX9300F	gutenprint-ppd
Epson Stylus CX9400	gutenprint-ppd
Epson Stylus CX9400F	gutenprint-ppd
Epson Stylus CX9475F	gutenprint-ppd
Epson Stylus D68	gutenprint-ppd
Epson Stylus D78	gutenprint-ppd
Epson Stylus D88	gutenprint-ppd
Epson Stylus D92	gutenprint-ppd
Epson Stylus D120	gutenprint-ppd
Epson Stylus DX3800	gutenprint-ppd
Epson Stylus DX3850	gutenprint-ppd
Epson Stylus DX4000	gutenprint-ppd
Epson Stylus DX4050	gutenprint-ppd
Epson Stylus DX4200	gutenprint-ppd
Epson Stylus DX4250	gutenprint-ppd
Epson Stylus DX4400	gutenprint-ppd
Epson Stylus DX4450	gutenprint-ppd
Epson Stylus DX4800	gutenprint-ppd
Epson Stylus DX4850	gutenprint-ppd
Epson Stylus DX7000F	gutenprint-ppd
Epson Stylus DX7400	gutenprint-ppd
Epson Stylus DX7450	gutenprint-ppd
Epson Stylus DX8400	gutenprint-ppd
Epson Stylus DX8450	gutenprint-ppd
Epson Stylus DX9400F	gutenprint-ppd
Epson Stylus NX100	gutenprint-ppd
Epson Stylus NX105	gutenprint-ppd
Epson Stylus NX115	gutenprint-ppd
Epson Stylus NX200	gutenprint-ppd
Epson Stylus NX215	gutenprint-ppd
Epson Stylus NX300	gutenprint-ppd
Epson Stylus NX400	gutenprint-ppd
Epson Stylus NX415	gutenprint-ppd
Epson Stylus NX420	gutenprint-ppd
Epson Stylus NX515	gutenprint-ppd
Epson Stylus NX530	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus NX625	gutenprint-ppd
Epson Stylus NX630	gutenprint-ppd
Epson Stylus NX635	gutenprint-ppd
Epson Stylus NX645	gutenprint-ppd
Epson Stylus Office B1100	gutenprint-ppd
Epson Stylus Office B30	gutenprint-ppd
Epson Stylus Office B33	gutenprint-ppd
Epson Stylus Office B40W	gutenprint-ppd
Epson Stylus Office B42WD	gutenprint-ppd
Epson Stylus Office BX300F	gutenprint-ppd
Epson Stylus Office BX525WD	gutenprint-ppd
Epson Stylus Office BX535WD	gutenprint-ppd
Epson Stylus Office BX600FW	gutenprint-ppd
Epson Stylus Office BX625FWD	gutenprint-ppd
Epson Stylus Office BX630FW	gutenprint-ppd
Epson Stylus Office BX635FWD	gutenprint-ppd
Epson Stylus Office SX600FW	gutenprint-ppd
Epson Stylus Office SX620FW	gutenprint-ppd
Epson Stylus Office T30	gutenprint-ppd
Epson Stylus Office T33	gutenprint-ppd
Epson Stylus Office T40W	gutenprint-ppd
Epson Stylus Office T1100	gutenprint-ppd
Epson Stylus Office T1110	gutenprint-ppd
Epson Stylus Office TX300F	gutenprint-ppd
Epson Stylus Office TX600FW	gutenprint-ppd
Epson Stylus Office TX620FWD	gutenprint-ppd
Epson Stylus Photo 700	gutenprint-ppd
Epson Stylus Photo 720	gutenprint-ppd
Epson Stylus Photo 750	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus Photo 780	gutenprint-ppd
Epson Stylus Photo 785	gutenprint-ppd
Epson Stylus Photo 790	gutenprint-ppd
Epson Stylus Photo 810	gutenprint-ppd
Epson Stylus Photo 820	gutenprint-ppd
Epson Stylus Photo 825	gutenprint-ppd
Epson Stylus Photo 830	gutenprint-ppd
Epson Stylus Photo 830U	gutenprint-ppd
Epson Stylus Photo 870	gutenprint-ppd
Epson Stylus Photo 875	gutenprint-ppd
Epson Stylus Photo 890	gutenprint-ppd
Epson Stylus Photo 895	gutenprint-ppd
Epson Stylus Photo 900	gutenprint-ppd
Epson Stylus Photo 915	gutenprint-ppd
Epson Stylus Photo 925	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus Photo 935	gutenprint-ppd
Epson Stylus Photo 950	gutenprint-ppd
Epson Stylus Photo 960	gutenprint-ppd
Epson Stylus Photo 1200	gutenprint-ppd
Epson Stylus Photo 1270	gutenprint-ppd
Epson Stylus Photo 1280	gutenprint-ppd
Epson Stylus Photo 1290	gutenprint-ppd
Epson Stylus Photo 1290s	gutenprint-ppd
Epson Stylus Photo 1400	gutenprint-ppd
Epson Stylus Photo 1410	gutenprint-ppd
Epson Stylus Photo 2000P	gutenprint-ppd
Epson Stylus Photo 2100	gutenprint-ppd
Epson Stylus Photo 2200	gutenprint-ppd
Epson Stylus Photo EX	gutenprint-ppd
Epson Stylus Photo EX3	gutenprint-ppd
Epson Stylus Photo P50	gutenprint-ppd
Epson Stylus Photo PX650	gutenprint-ppd
Epson Stylus Photo PX700W	gutenprint-ppd
Epson Stylus Photo PX710W	gutenprint-ppd
Epson Stylus Photo PX800FW	gutenprint-ppd
Epson Stylus Photo PX810FW	gutenprint-ppd
Epson Stylus Photo R200	gutenprint-ppd
Epson Stylus Photo R210	gutenprint-ppd
Epson Stylus Photo R220	gutenprint-ppd
Epson Stylus Photo R230	gutenprint-ppd
Epson Stylus Photo R240	gutenprint-ppd
Epson Stylus Photo R245	gutenprint-ppd
Epson Stylus Photo R260	gutenprint-ppd
Epson Stylus Photo R265	gutenprint-ppd
Epson Stylus Photo R270	gutenprint-ppd
Epson Stylus Photo R280	gutenprint-ppd
Epson Stylus Photo R285	gutenprint-ppd
Epson Stylus Photo R290	gutenprint-ppd
Epson Stylus Photo R300	gutenprint-ppd
Epson Stylus Photo R310	gutenprint-ppd
Epson Stylus Photo R320	gutenprint-ppd
Epson Stylus Photo R340	gutenprint-ppd
Epson Stylus Photo R350	gutenprint-ppd
Epson Stylus Photo R360	gutenprint-ppd
Epson Stylus Photo R380	gutenprint-ppd
Epson Stylus Photo R390	gutenprint-ppd
Epson Stylus Photo R800	gutenprint-ppd
Epson Stylus Photo R1800	gutenprint-ppd
Epson Stylus Photo R1900	gutenprint-ppd
Epson Stylus Photo R2000	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus Photo R2400	gutenprint-ppd
Epson Stylus Photo R2880	gutenprint-ppd
Epson Stylus Photo R3000	gutenprint-ppd
Epson Stylus Photo RX400	gutenprint-ppd
Epson Stylus Photo RX420	gutenprint-ppd
Epson Stylus Photo RX425	gutenprint-ppd
Epson Stylus Photo RX430	gutenprint-ppd
Epson Stylus Photo RX500	gutenprint-ppd
Epson Stylus Photo RX510	gutenprint-ppd
Epson Stylus Photo RX560	gutenprint-ppd
Epson Stylus Photo RX580	gutenprint-ppd
Epson Stylus Photo RX585	gutenprint-ppd
Epson Stylus Photo RX590	gutenprint-ppd
Epson Stylus Photo RX595	gutenprint-ppd
Epson Stylus Photo RX600	gutenprint-ppd
Epson Stylus Photo RX610	gutenprint-ppd
Epson Stylus Photo RX620	gutenprint-ppd
Epson Stylus Photo RX630	gutenprint-ppd
Epson Stylus Photo RX640	gutenprint-ppd
Epson Stylus Photo RX650	gutenprint-ppd
Epson Stylus Photo RX680	gutenprint-ppd
Epson Stylus Photo RX685	gutenprint-ppd
Epson Stylus Photo RX690	gutenprint-ppd
Epson Stylus Photo RX700	gutenprint-ppd
Epson Stylus Photo TX700W	gutenprint-ppd
Epson Stylus Photo TX710W	gutenprint-ppd
Epson Stylus Photo TX800FW	gutenprint-ppd
Epson Stylus Photo TX810FW	gutenprint-ppd
Epson Stylus Pro 3800	gutenprint-ppd
Epson Stylus Pro 3880	gutenprint-ppd
Epson Stylus Pro 3885	gutenprint-ppd
Epson Stylus Pro 4000	gutenprint-ppd
Epson Stylus Pro 4800	gutenprint-ppd
Epson Stylus Pro 4880	gutenprint-ppd
Epson Stylus Pro 5000	gutenprint-ppd
Epson Stylus Pro 5500	gutenprint-ppd
Epson Stylus Pro 7000	gutenprint-ppd
Epson Stylus Pro 7500	gutenprint-ppd
Epson Stylus Pro 7600	gutenprint-ppd
Epson Stylus Pro 7700	gutenprint-ppd
Epson Stylus Pro 7800	gutenprint-ppd
Epson Stylus Pro 7880	gutenprint-ppd
Epson Stylus Pro 7890	gutenprint-ppd
Epson Stylus Pro 7900	gutenprint-ppd
Epson Stylus Pro 9000	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus Pro 9500	gutenprint-ppd
Epson Stylus Pro 9600	gutenprint-ppd
Epson Stylus Pro 9700	gutenprint-ppd
Epson Stylus Pro 9800	gutenprint-ppd
Epson Stylus Pro 9880	gutenprint-ppd
Epson Stylus Pro 9890	gutenprint-ppd
Epson Stylus Pro 9900	gutenprint-ppd
Epson Stylus Pro 10000	gutenprint-ppd
Epson Stylus Pro 11800	gutenprint-ppd
Epson Stylus Pro 11880	gutenprint-ppd
Epson Stylus Pro XL	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus S20	gutenprint-ppd
Epson Stylus S21	gutenprint-ppd
Epson Stylus S50	gutenprint-ppd
Epson Stylus Scan 2000	gutenprint-ppd
Epson Stylus Scan 2500	OpenPrintingPPDs-ghostscript gutenprint-ppd
Epson Stylus SX100	gutenprint-ppd
Epson Stylus SX105	gutenprint-ppd
Epson Stylus SX110	gutenprint-ppd
Epson Stylus SX115	gutenprint-ppd
Epson Stylus SX200	gutenprint-ppd
Epson Stylus SX205	gutenprint-ppd
Epson Stylus SX210	gutenprint-ppd
Epson Stylus SX215	gutenprint-ppd
Epson Stylus SX400	gutenprint-ppd
Epson Stylus SX405	gutenprint-ppd
Epson Stylus SX410	gutenprint-ppd
Epson Stylus SX415	gutenprint-ppd
Epson Stylus SX420	gutenprint-ppd
Epson Stylus SX445W	gutenprint-ppd
Epson Stylus SX510W	gutenprint-ppd
Epson Stylus SX515	gutenprint-ppd
Epson Stylus SX525	gutenprint-ppd
Epson Stylus SX535FW	gutenprint-ppd
Epson Stylus SX600FW	gutenprint-ppd
Epson Stylus SX610FW	gutenprint-ppd
Epson Stylus SX615	gutenprint-ppd
Epson Stylus SX630	gutenprint-ppd
Epson Stylus SX635	gutenprint-ppd
Epson Stylus SX645	gutenprint-ppd
Epson Stylus SX650	gutenprint-ppd
Epson Stylus T13	gutenprint-ppd
Epson Stylus T20	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson Stylus T21	gutenprint-ppd
Epson Stylus T22	gutenprint-ppd
Epson Stylus T22E	gutenprint-ppd
Epson Stylus T26	gutenprint-ppd
Epson Stylus T30	gutenprint-ppd
Epson Stylus T40W	gutenprint-ppd
Epson Stylus T42WD	gutenprint-ppd
Epson Stylus T50	gutenprint-ppd
Epson Stylus T59	gutenprint-ppd
Epson Stylus T60	gutenprint-ppd
Epson Stylus TX100	gutenprint-ppd
Epson Stylus TX101	gutenprint-ppd
Epson Stylus TX102	gutenprint-ppd
Epson Stylus TX103	gutenprint-ppd
Epson Stylus TX104	gutenprint-ppd
Epson Stylus TX105	gutenprint-ppd
Epson Stylus TX106	gutenprint-ppd
Epson Stylus TX109	gutenprint-ppd
Epson Stylus TX110	gutenprint-ppd
Epson Stylus TX125	gutenprint-ppd
Epson Stylus TX200	gutenprint-ppd
Epson Stylus TX210	gutenprint-ppd
Epson Stylus TX300F	gutenprint-ppd
Epson Stylus TX400	gutenprint-ppd
Epson Stylus TX410	gutenprint-ppd
Epson Stylus TX420	gutenprint-ppd
Epson Stylus TX510FN	gutenprint-ppd
Epson Stylus TX550W	gutenprint-ppd
Epson Stylus TX560WD	gutenprint-ppd
Epson Stylus TX610FW	gutenprint-ppd
Epson Stylus TX615	gutenprint-ppd
Epson Stylus TX630	gutenprint-ppd
Epson Stylus TX635	gutenprint-ppd
Epson Stylus TX645	gutenprint-ppd
Epson Stylus TX650	gutenprint-ppd
Epson Stylus TX659	gutenprint-ppd
Epson Stylus XP100	gutenprint-ppd
Epson SureColor P400	gutenprint-ppd
Epson SureColor P600	gutenprint-ppd
Epson SureColor P800	gutenprint-ppd
Epson SureColor P6000	gutenprint-ppd
Epson SureColor P7000	gutenprint-ppd
Epson SureColor P7000 Commercial Edition	gutenprint-ppd
Epson SureColor P8000	gutenprint-ppd
Epson SureColor P9000	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Epson SureColor P9000 Commercial Edition	gutenprint-ppd
Epson SureColor P10000	gutenprint-ppd
Epson SureColor P20000	gutenprint-ppd
Epson WF-7010 Series	gutenprint-ppd
Epson WF-7011 Series	gutenprint-ppd
Epson WF-7015 Series	gutenprint-ppd
Epson WF-7018 Series	gutenprint-ppd
Epson WF-7510 Series	gutenprint-ppd
Epson WF-7511 Series	gutenprint-ppd
Epson WF-7515 Series	gutenprint-ppd
Epson WF-7520 Series	gutenprint-ppd
Epson WF-7521 Series	gutenprint-ppd
Epson WF-7525 Series	gutenprint-ppd
Epson WorkForce 30	gutenprint-ppd
Epson WorkForce 40	gutenprint-ppd
Epson WorkForce 60	gutenprint-ppd
Epson WorkForce 310	gutenprint-ppd
Epson WorkForce 315	gutenprint-ppd
Epson WorkForce 500	gutenprint-ppd
Epson WorkForce 545	gutenprint-ppd
Epson WorkForce 600	gutenprint-ppd
Epson WorkForce 610	gutenprint-ppd
Epson WorkForce 615	gutenprint-ppd
Epson WorkForce 625	gutenprint-ppd
Epson WorkForce 630	gutenprint-ppd
Epson WorkForce 633	gutenprint-ppd
Epson WorkForce 635	gutenprint-ppd
Epson WorkForce 645	gutenprint-ppd
Epson WorkForce 1100	gutenprint-ppd
Epson XP-820	gutenprint-ppd

Печатающие устройства производства Fuji, Genicom

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Fuji	
Fuji Xerox DocuPrint CM205	foo2zjs
Fuji Xerox DocuPrint CM215	foo2zjs
Fuji Xerox DocuPrint CM305 df	OpenPrintingPPDs-postscript
Fuji Xerox DocuPrint M215	foo2zjs
Fuji Xerox DocuPrint P205	foo2zjs
Fujifilm ASK-300	gutenprint-ppd
Fujifilm FinePix-NX-500	gutenprint-ppd
Fujifilm Printpix-CX-400	gutenprint-ppd
Fujifilm Printpix-CX-550	gutenprint-ppd
Fujitsu 1200	OpenPrintingPPDs-ghostscript
Fujitsu 2400	OpenPrintingPPDs-ghostscript
Fujitsu 3400	OpenPrintingPPDs-ghostscript
Fujitsu FMLBP2xx Page Printer	OpenPrintingPPDs-ghostscript
Fujitsu FMPR	OpenPrintingPPDs-ghostscript
Fujitsu PrintPartner 10V	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Fujitsu PrintPartner 16DV	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Fujitsu PrintPartner 20W	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Fujitsu PrintPartner 8000	OpenPrintingPPDs-ghostscript gutenprint-ppd
Genicom	
Genicom LN45	OpenPrintingPPDs-postscript
Genicom microLaser 12	OpenPrintingPPDs-postscript
Genicom microLaser 210	OpenPrintingPPDs-postscript
Genicom ML450	OpenPrintingPPDs-postscript

Печатающие устройства производства Gestetner

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner 10512	gutenprint-ppd
Gestetner 10512 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 2212	gutenprint-ppd
Gestetner 2212 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 2712	gutenprint-ppd
Gestetner 2712 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 3212	gutenprint-ppd
Gestetner 3212 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 3502	gutenprint-ppd
Gestetner 3502 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 3532/4235g	gutenprint-ppd
Gestetner 3532/4235g PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 4502	gutenprint-ppd
Gestetner 4502 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 4532/4245g	gutenprint-ppd
Gestetner 4532/4245g PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 6002	gutenprint-ppd
Gestetner 6002 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 7502	gutenprint-ppd
Gestetner 7502 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner 9002	gutenprint-ppd
Gestetner 9002 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner C7010 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7116 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7416 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7417 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7425dn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7435n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7521n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7526dn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7528n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7531dn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7535n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner C7640nD PS3	OpenPrintingPPDs-postscript
Gestetner C8140ND PS3	OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Gestetner CS555 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc1020 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc1025 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc1030 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc1045 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc1060 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc224 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc232 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc328 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner DSc332 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc338 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc38 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc38u PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc424 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc428 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc432 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc435 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc445 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc460 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSc524 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSc532 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner DSm1525 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm1530 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm1533 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm415	gutenprint-ppd
Gestetner DSm415 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm615	gutenprint-ppd
Gestetner DSm615 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm616	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner DSm616 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm618	gutenprint-ppd
Gestetner DSm618 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm618d	gutenprint-ppd
Gestetner DSm618d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm620	gutenprint-ppd
Gestetner DSm620 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm620d	gutenprint-ppd
Gestetner DSm620d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm622	gutenprint-ppd
Gestetner DSm622 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm627	gutenprint-ppd
Gestetner DSm627 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm635/635G	gutenprint-ppd
Gestetner DSm635/635G PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm645/645G	gutenprint-ppd
Gestetner DSm645/645G PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm651	gutenprint-ppd
Gestetner DSm651 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm660	gutenprint-ppd
Gestetner DSm660 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm675	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner DSm675 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm725	gutenprint-ppd
Gestetner DSm725 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm730	gutenprint-ppd
Gestetner DSm730 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm735/735G	gutenprint-ppd
Gestetner DSm735/735G PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner DSm745/745G	gutenprint-ppd
Gestetner DSm745/745G PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner F9199/9199nf PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner GWD2004 PS3	OpenPrintingPPDs-postscript
Gestetner GWD2006 PS3	OpenPrintingPPDs-postscript
Gestetner GWD3006 PS3	OpenPrintingPPDs-postscript
Gestetner GWD5100 PS3	OpenPrintingPPDs-postscript
Gestetner GWD7140 PS3	OpenPrintingPPDs-postscript
Gestetner MP 161/DSm416	gutenprint-ppd
Gestetner MP 161/DSm416 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 171 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 301 PS3	OpenPrintingPPDs-postscript
Gestetner MP C300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C305 PS3	OpenPrintingPPDs-postscript
Gestetner MP C400 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2510/DSm725e	gutenprint-ppd
Gestetner MP 2510/DSm725e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2550	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner MP 2550 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2550B	gutenprint-ppd
Gestetner MP 2550B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2553 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 2851 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 3010/DSm730e	gutenprint-ppd
Gestetner MP 3010/DSm730e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 3053 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 3350	gutenprint-ppd
Gestetner MP 3350 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 3350B	gutenprint-ppd
Gestetner MP 3350B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 3351 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 3353 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 4000	gutenprint-ppd
Gestetner MP 4000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 4000B	gutenprint-ppd
Gestetner MP 4000B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 4001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 4002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 5000	gutenprint-ppd
Gestetner MP 5000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 5000B	gutenprint-ppd
Gestetner MP 5000B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 5001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 5002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner MP 6000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 6001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 6002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 7000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 7001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 7502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 8000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 8001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 9001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP 9002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2050 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2051 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2550 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2551 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C2800 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C300SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C3001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C3002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C3003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C3300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner MP C3501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C3502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C3503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C400SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C4000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C4501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C4501A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C4502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C4502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C4503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C5000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C5501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C5501A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C5502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C5502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C5503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C6000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C6003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C6501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C6502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C7500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP C7501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner MP C8002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP CW2200 PS3	OpenPrintingPPDs-postscript
Gestetner MP1100/DSm7110	gutenprint-ppd
Gestetner MP1100/DSm7110 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP1350/DSm7135	gutenprint-ppd
Gestetner MP1350/DSm7135 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP1600/DSm716	gutenprint-ppd
Gestetner MP1600/DSm716 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP2000/DSm721d	gutenprint-ppd
Gestetner MP2000/DSm721d PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP2352/DSm923 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP2500/DSm625	gutenprint-ppd
Gestetner MP2500/DSm625 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP2852/DSm928 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP3352/DSm933 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP3500/DSm735e	gutenprint-ppd
Gestetner MP3500/DSm735e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP4500/DSm745e	gutenprint-ppd
Gestetner MP4500/DSm745e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP5500/DSm755	gutenprint-ppd
Gestetner MP5500/DSm755 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP6500/DSm765	gutenprint-ppd
Gestetner MP6500/DSm765 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP7500/DSm775	gutenprint-ppd
Gestetner MP7500/DSm775 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MP9000/DSm790	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner MP9000/DSm790 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MPC1500/GS106 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MPC2500/DSc525 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MPC3000/DSc530 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MPC3500/DSc535 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner MPC4500/DSc545 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner P7026 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7026n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7031n PS3	OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Gestetner P7032 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7035n PS3	OpenPrintingPPDs-postscript
Gestetner P7126 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7126n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7132n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7145 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7245 PS3	OpenPrintingPPDs-postscript
Gestetner P7325 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7325n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7431cn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7527 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7527n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Gestetner P7535n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7575 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Gestetner P7675 PS3	OpenPrintingPPDs-postscript
Gestetner Pro 1106EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner Pro 1107EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner Pro 1356EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner Pro 1357EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner Pro 906EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner Pro 907EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Gestetner SP 4210N PS3	OpenPrintingPPDs-postscript
Gestetner SP 6330N PS3	OpenPrintingPPDs-postscript
Gestetner SP 8200DN PS3	OpenPrintingPPDs-postscript
Gestetner SP C320DN PS3	OpenPrintingPPDs-postscript
Gestetner SP C420DN PS3	OpenPrintingPPDs-postscript
Gestetner SP C430DN PS3	OpenPrintingPPDs-postscript
Gestetner SP C431DN PS3	OpenPrintingPPDs-postscript
Gestetner SP W2470 PS3	OpenPrintingPPDs-postscript

Печатающие устройства производства Heidelberg, Hitachi, HP

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Heidelberg	OpenPrintingPPDs-ghostscript
Heidelberg Digimaster 9110	OpenPrintingPPDs-postscript
Hitachi	OpenPrintingPPDs-postscript
Hitachi DDP 70 with MicroPress	OpenPrintingPPDs-postscript
HP Business Inkjet 2200	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Business Inkjet 2230	gutenprint-ppd
HP Business Inkjet 2250	gutenprint-ppd
HP Business Inkjet 2250	manufacturer-PPDs
HP Business Inkjet 2250	hplip OpenPrintingPPDs-postscript
HP Business Inkjet 2250TN	gutenprint-ppd
HP Business Inkjet 2280	manufacturer-PPDs gutenprint-ppd
HP Business Inkjet 2280	hplip OpenPrintingPPDs-postscript
HP Business Inkjet 2300	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Business Inkjet 2600	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Business Inkjet 2800	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Business Inkjet 3000	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
HP CM8050 Color MFP	OpenPrintingPPDs-postscript
HP CM8060 Color MFP	hplip OpenPrintingPPDs-postscript
HP Color Inkjet Printer CP1160	gutenprint-ppd
HP Color Inkjet Printer CP1700	gutenprint-ppd
HP Color LaserJet 5	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Color LaserJet 5M	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 1500	foo2zjs

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Color LaserJet 1600	foo2zjs
HP Color LaserJet 2500	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 2550 series	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 2600n	foo2zjs
HP Color LaserJet 2605/dn/dtn	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 2700	hplip
HP Color LaserJet 2800 series	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 3000	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 3700	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 3800	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 4500	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 4550	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 4600	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 4610	hplip manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Color LaserJet 4650	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 4700	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 4730mfp	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 5000	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Color LaserJet 5500	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 5550	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 8500	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 8550	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet 8550GN	gutenprint-ppd
HP Color LaserJet 9500	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP Color LaserJet 9500 MFP	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP Color LaserJet CM1015/CM1017	hplip
HP Color LaserJet CM1312/f/nfi/wb/wi MFP	hplip
HP Color LaserJet CM2320n/nf/xi/wb/wbb/wi MFP	hplip
HP Color LaserJet CM3530 MFP	hplip
HP Color LaserJet CM4540 MFP	hplip
HP Color LaserJet CM4730 MFP	hplip
HP Color LaserJet CM6030 MFP	hplip
HP Color LaserJet CM6040 MFP	hplip
HP Color LaserJet CM6049 MFP	hplip
HP Color LaserJet CP1215	foo2zjs
HP Color LaserJet CP1515n/ni	hplip
HP Color LaserJet CP2024/CP2025/CP2026/CP2027/n	hplip
HP Color LaserJet CP2024/CP2025/CP2026/CP2027/n	hplip

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Color LaserJet CP3505	hplip
HP Color LaserJet CP3525	hplip
HP Color LaserJet CP4005	hplip
HP Color LaserJet CP4020/CP4520 Series	hplip
HP Color LaserJet CP5221/CP5223/CP5225/CP5227/CP5229/n/dn	hplip
HP Color LaserJet CP5520 Series	hplip
HP Color LaserJet CP6015	hplip
HP Color LaserJet E65050	hplip
HP Color LaserJet Flow MFP M680	hplip
HP Color LaserJet flow MFP M880	hplip
HP Color LaserJet M452dn/nw/dw	hplip
HP Color LaserJet M552	hplip
HP Color LaserJet M553	hplip
HP Color LaserJet M651	hplip
HP Color LaserJet M652/M653	hplip
HP Color LaserJet M750	hplip
HP Color LaserJet M855	hplip
HP Color LaserJet MFP E67550/E67560	hplip
HP Color LaserJet MFP E77822/E77825/E77830	hplip
HP Color LaserJet MFP E87640/E87650/E87660	hplip
HP Color LaserJet MFP M274n	hplip
HP Color LaserJet MFP M277n/c1/c2/c3/c4/c5/c6/c7c/8c/9/c10	hplip
HP Color LaserJet MFP M377dw	hplip
HP Color LaserJet MFP M476dn/dw/nw	hplip
HP Color LaserJet MFP M477fdn/fdw/fnw	hplip
HP Color LaserJet MFP M577	hplip
HP Color LaserJet MFP M680	hplip
HP Color LaserJet MFP M681/M682	hplip
HP Color LaserJet Pro M252n/c1/c2/c3/c4/c5/c6/c7c/8c/9/c10	hplip
HP DesignJet 30	OpenPrintingPPDs-ghostscript
HP DesignJet 70	OpenPrintingPPDs-ghostscript
HP DesignJet 90	OpenPrintingPPDs-ghostscript
HP DesignJet 100	OpenPrintingPPDs-ghostscript
HP DesignJet 100plus	OpenPrintingPPDs-ghostscript
HP DesignJet 110	OpenPrintingPPDs-ghostscript
HP DesignJet 120	OpenPrintingPPDs-ghostscript
HP DesignJet 130	OpenPrintingPPDs-ghostscript
HP DesignJet 230	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP DesignJet 250C	gutenprint-ppd
HP DesignJet 350C	OpenPrintingPPDs-ghostscript
HP DesignJet 430	gutenprint-ppd
HP DesignJet 455CA	gutenprint-ppd
HP DesignJet 488CA	gutenprint-ppd
HP DesignJet 500	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP DesignJet 500ps	OpenPrintingPPDs-ghostscript
HP DesignJet 650C	OpenPrintingPPDs-ghostscript
HP DesignJet 700	gutenprint-ppd
HP DesignJet 750C	gutenprint-ppd
HP DesignJet 750C Plus	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP DesignJet 800	OpenPrintingPPDs-ghostscript
HP DesignJet 800PS	manufacturer-PPDs OpenPrintingPPDs-postscript
HP DesignJet 1050C	manufacturer-PPDs OpenPrintingPPDs-postscript
HP DesignJet 1055CM	manufacturer-PPDs OpenPrintingPPDs-postscript
HP DesignJet 2500CP	manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP DesignJet 3500CP	manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP Designjet 4000ps	hplip
HP Designjet 4020ps	hplip
HP Designjet 4500mfp	hplip
HP Designjet 4500ps	hplip
HP DesignJet 450C	gutenprint-ppd
HP Designjet 4520mfp	hplip
HP Designjet 4520ps	hplip
HP DesignJet 5000	OpenPrintingPPDs-ghostscript
HP DesignJet 5000PS	manufacturer-PPDs
HP DesignJet 5500	OpenPrintingPPDs-ghostscript
HP DesignJet 5500PS	manufacturer-PPDs OpenPrintingPPDs-postscript
HP DesignJet ColorPro CAD	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Designjet D5800ps Photo	hplip
HP Designjet T1100ps	hplip
HP Designjet T1100ps	hplip
HP Designjet T1120ps	hplip
HP Designjet T1120ps	hplip
HP Designjet T1200 PostScript	hplip
HP Designjet T1300 PostScript	hplip
HP Designjet T1500 PostScript	hplip
HP Designjet T2300 PostScript	hplip
HP Designjet T2500 PostScript	hplip
HP Designjet T3500ps	hplip
HP Designjet T7100ps	hplip

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Designjet T7100ps Monochrome	hplip
HP Designjet T7200ps	hplip
HP Designjet T770 PostScript	hplip
HP Designjet T770ps	hplip
HP Designjet T790ps	hplip
HP Designjet T790ps	hplip
HP Designjet T795ps	hplip
HP Designjet T920 PostScript	hplip
HP Designjet Z5200 PostScript	hplip
HP Designjet Z5400 PostScript	hplip
HP Designjet Z6100ps 42in Photo	hplip
HP Designjet Z6100ps 60in Photo	hplip
HP Designjet Z6200ps 42in Photo	hplip
HP Designjet Z6200ps 60in Photo	hplip
HP Designjet Z6600ps	hplip
HP Designjet Z6800ps Photo	hplip
HP Deskjet 200	OpenPrintingPPDs-ghostscript
HP Deskjet 310	OpenPrintingPPDs-ghostscript
HP Deskjet 320	OpenPrintingPPDs-ghostscript
HP Deskjet 340	OpenPrintingPPDs-ghostscript
HP Deskjet 340C	gutenprint-ppd
HP Deskjet 350	OpenPrintingPPDs-ghostscript
HP Deskjet 400	gutenprint-ppd
HP Deskjet 400	OpenPrintingPPDs-ghostscript
HP Deskjet 420C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 450	gutenprint-ppd
HP Deskjet 500	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 500C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 505J Plus	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 510	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 520	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 540	OpenPrintingPPDs-ghostscript
HP Deskjet 540C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 550C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 560C	OpenPrintingPPDs-ghostscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Deskjet 600	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 600C	gutenprint-ppd
HP Deskjet 610C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 610CL	gutenprint-ppd
HP Deskjet 612C	gutenprint-ppd
HP Deskjet 640C	gutenprint-ppd
HP Deskjet 648C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 660C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 670C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 670TV	gutenprint-ppd
HP Deskjet 672C	gutenprint-ppd
HP Deskjet 680C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 682C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 690C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 692C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 693C	gutenprint-ppd
HP Deskjet 694C	gutenprint-ppd
HP Deskjet 695C	gutenprint-ppd
HP Deskjet 697C	gutenprint-ppd
HP Deskjet 810C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 812C	gutenprint-ppd
HP Deskjet 815C	gutenprint-ppd
HP Deskjet 816C	gutenprint-ppd
HP Deskjet 825C	gutenprint-ppd
HP Deskjet 830C	gutenprint-ppd
HP Deskjet 832C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 840C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 841C	gutenprint-ppd
HP Deskjet 842C	gutenprint-ppd
HP Deskjet 843C	gutenprint-ppd
HP Deskjet 845C	OpenPrintingPPDs-ghostscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Deskjet 850C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 855C	gutenprint-ppd
HP Deskjet 870C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 880C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 882C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 890C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 895C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 916C	gutenprint-ppd
HP Deskjet 920C	gutenprint-ppd
HP Deskjet 930C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 932C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 933C	gutenprint-ppd
HP Deskjet 934C	gutenprint-ppd
HP Deskjet 935C	gutenprint-ppd
HP Deskjet 940C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 948C	gutenprint-ppd
HP Deskjet 950C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 952C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 955C	gutenprint-ppd
HP Deskjet 957C	gutenprint-ppd
HP Deskjet 959C	gutenprint-ppd
HP Deskjet 960C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 970C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 975C	gutenprint-ppd
HP Deskjet 980C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 990C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 995C	gutenprint-ppd
HP Deskjet 1100C	OpenPrintingPPDs-ghostscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Deskjet 1120C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 1125C	gutenprint-ppd
HP Deskjet 1200C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 1220C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Deskjet 1600C	gutenprint-ppd
HP Deskjet 1600CM	OpenPrintingPPDs-postscript gutenprint-ppd
HP Deskjet 2000	gutenprint-ppd
HP Deskjet 2500	gutenprint-ppd
HP Deskjet 2500CM	gutenprint-ppd
HP Deskjet 3810	gutenprint-ppd
HP Deskjet 3816	gutenprint-ppd
HP Deskjet 3820	gutenprint-ppd
HP Deskjet 3822	gutenprint-ppd
HP Deskjet 5550	gutenprint-ppd
HP Deskjet 5551	gutenprint-ppd
HP Deskjet 6122	gutenprint-ppd
HP Deskjet 6127	gutenprint-ppd
HP Deskjet 9300	gutenprint-ppd
HP Deskjet Plus	OpenPrintingPPDs-ghostscript
HP Deskjet Portable	OpenPrintingPPDs-ghostscript
HP e-printer e20	gutenprint-ppd
HP Fax	hplip
HP Fax2	hplip
HP Fax3	hplip
HP Fax4	hplip
HP LaserJet 2	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 2D	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 2P	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 2P Plus	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 3	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 3D	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 3P w/ PCL5	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 3P w/PS	OpenPrintingPPDs-ghostscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 4	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 4 Plus	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4L	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 4M	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4ML	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4MP	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP LaserJet 4P	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 4Si	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4V	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4V/4LJ Pro	OpenPrintingPPDs-ghostscript
HP LaserJet 5	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 5L	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 5M	manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 5MP	OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 5P	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 5Si	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 6	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 6L	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 6MP	OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 6P	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 100/M175a/M175b/M175c/M175e/ /M175nw/M175p/M175q/M175r colorMFP	hplip
HP LaserJet 200 color M251n/M251b/M251e/ /M251g/M251j/M251k/M251nw/M251p/M251q/M251r/M251u/M251v	hplip
HP LaserJet 200 colorMFP M275nw/M275s/M275t/M275u	hplip
HP LaserJet 200 colorMFP M276n/M276b/M276e/ /M276g/M276j/M276k/M276nw/M276p/M276q/M276r/M276u/M276v	hplip
HP LaserJet 300/400 color M351a/M451nw/M451dn/M451dw	hplip
HP LaserJet 300/400 colorMFP M375nw/M475dn/M475dw	hplip
HP LaserJet 400 M401a/M401d/M401n/M401dn/M401dw	hplip
HP LaserJet 400 M401dne	hplip
HP LaserJet 400 MFP M425dn/M425dw	hplip
HP LaserJet 500 color M551	hplip
HP LaserJet 500 colorMFP M575	hplip
HP LaserJet 500 colorMFP M570dn/M570dw	hplip
HP LaserJet 500 MFP M525	hplip
HP LaserJet 600 M601/M602/M603	hplip
HP LaserJet 700 color MFP M775	hplip
HP LaserJet 700 M712	hplip
HP LaserJet 1000	foo2zjs
HP LaserJet 1005	foo2zjs
HP LaserJet 1010	gutenprint-ppd
HP LaserJet 1012	gutenprint-ppd
HP LaserJet 1015	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 1018	foo2zjs

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 1020	foo2zjs
HP LaserJet 1022	foo2zjs gutenprint-ppd
HP LaserJet 1022n/nw	foo2zjs
HP LaserJet 1100	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 1100A	gutenprint-ppd
HP LaserJet 1150	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 1160	gutenprint-ppd
HP LaserJet 1200	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 1300/1300n	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 1320 series	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 2100	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 2100M	gutenprint-ppd
HP LaserJet 2200	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 2300/L	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 2410	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 2420	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 2430	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3015	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3020/3030	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3030	OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3050	hplip manufacturer-PPDs gutenprint-ppd
HP LaserJet 3052/3055	hplip manufacturer-PPDs gutenprint-ppd
HP LaserJet 3200	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3200m	hplip OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3200se	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP LaserJet 3300 MFP	gutenprint-ppd
HP LaserJet 3300/3310/3320	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3320N MFP	gutenprint-ppd
HP LaserJet 3330	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 3380	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3390	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 3392	gutenprint-ppd
HP LaserJet 4000 Series	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4050 Series	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4100 MFP	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4200/4200L	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4240/4240N	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4250/4250L	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4300	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 4345 mfp	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 4350/4350L	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 5000	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 5100 Series	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 5200	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 5200L	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 5200LX	hplip
HP LaserJet 8000	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 8100	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 8150 Series	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 9000 Series	hplip manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet 9000/9000L MFP	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP LaserJet 9040/9040 MFP	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 9050/9050 MFP	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP LaserJet 9055mfp/9065mfp	hplip manufacturer-PPDs OpenPrintingPPDs-postscript
HP LaserJet CM1415fn/CM1411fn/CM1412fn/ /CM1413fn/CM1415fnw /CM1416fnw/CM1417fnw/CM1418fnw	hplip
HP LaserJet Color Flow MFP M575	hplip
HP LaserJet CP1525N/CP1521n/CP1522n/ /CP1523n/CP1525nw/CP1526nw/CP1527nw/CP1528nw	hplip
HP LaserJet E60055/E60065/E60075	hplip
HP LaserJet Flow MFP M525	hplip
HP LaserJet Flow MFP M630	hplip
HP LaserJet Flow MFP M830	hplip
HP LaserJet M203-M206	hplip
HP LaserJet M402d/M403d/M402dw/M403dw/M402dn/M403dn	hplip
HP LaserJet M402n	hplip
HP LaserJet M506	hplip
HP LaserJet M604/M605/M606	hplip
HP LaserJet M607/M608/M609	hplip
HP LaserJet M806	hplip
HP LaserJet M1005 MFP	foo2zjs
HP LaserJet M1120 MFP	foo2zjs
HP LaserJet M1319 MFP	foo2zjs
HP LaserJet M1522/M1522n/M1522nf	hplip OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
HP LaserJet M1536dnf/M1537dnf/M1538dnf/M1539dnf MFP	hplip
HP LaserJet M2727/M2727nf/M2727nf/M2727nfs MFP	hplip
HP LaserJet M3027 MFP	hplip gutenprint-ppd
HP LaserJet M3035 MFP	hplip gutenprint-ppd
HP LaserJet M4345 MFP	hplip gutenprint-ppd
HP LaserJet M4349 MFP	hplip

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet M4555 MFP	hplip
HP LaserJet M5025 MFP	hplip gutenprint-ppd
HP LaserJet M5035 MFP	hplip gutenprint-ppd
HP LaserJet M9050/M9040 MFP	hplip
HP LaserJet M9059 MFP	hplip
HP LaserJet MFP E62555/E62565/E62575 (Flow)	hplip
HP LaserJet MFP E72525/E72530/E72535 (Flow)	hplip
HP LaserJet MFP E82540/E82550/E82560 (Flow)	hplip
HP LaserJet MFP M227-M231	hplip
HP LaserJet MFP M426dw/M427dw/M426fdn/ /M426fdw/M427fdn/M427fdw	hplip
HP LaserJet MFP M527	hplip
HP LaserJet MFP M630	hplip
HP LaserJet MFP M631/M632/M633 (Flow)	hplip
HP LaserJet MFP M725	hplip
HP LaserJet P1005	foo2zjs
HP LaserJet P1006	foo2zjs
HP LaserJet P1007	foo2zjs
HP LaserJet P1008	foo2zjs
HP LaserJet P1505/P1505n MFP	foo2zjs
HP LaserJet P2010	gutenprint-ppd
HP LaserJet P2014/P2014n	foo2zjs
HP LaserJet P2015 Series	hplip gutenprint-ppd
HP LaserJet P2035/P2035n	foo2zjs
HP LaserJet P2055/P2055n/P2055d/P2055dn/P2055x	hplip
HP LaserJet P3004	hplip gutenprint-ppd
HP LaserJet P3005	hplip gutenprint-ppd
HP LaserJet P3010/P3011/P3015	hplip
HP LaserJet P4014/P4015	hplip
HP LaserJet Pro CP1025nw	foo2zjs
HP LaserJet Pro M201n/M201c1/M201c2/c3/M201c4/ /M201c5/M201c6/M201c7/M201c8/M201c9/M201c10/ /M201dw/M202n/M202dw	hplip
HP LaserJet Pro M501n/dn	hplip
HP LaserJet Pro M701a/n	hplip
HP LaserJet Pro M706n	hplip
HP LaserJet Pro MFP M225dn/M225rdn/M225c1/ /M225c2/M225c3/M225c4/M225c5/M225c6/M225c7/ /M225c8/M225dw/M226dn/M226dw	hplip
HP LaserJet Pro MFP M435nw	hplip

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP LaserJet Pro MFP M521dn/M521dw/M521dx/M521dz	hplip
HP LaserJet Pro MFP M1212	foo2zjs
HP LaserJet Pro P1102/P1102w	foo2zjs
HP LaserJet Pro P1566	foo2zjs
HP LaserJet Pro P1606dn	foo2zjs
HP Mopier 240	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP Mopier 320	hplip manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
HP Officejet 300	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 330	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 350	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 500	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 520	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 570	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 580	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 590	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 600	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 610	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 625	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 630	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 635	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet 700	gutenprint-ppd
HP Officejet 710	gutenprint-ppd
HP Officejet 720	gutenprint-ppd
HP Officejet 725	gutenprint-ppd
HP Officejet 5105	gutenprint-ppd
HP Officejet 5110	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Officejet 5110xi	gutenprint-ppd
HP Officejet 6105	gutenprint-ppd
HP Officejet 6110	gutenprint-ppd
HP Officejet 7110	gutenprint-ppd
HP Officejet 7130	gutenprint-ppd
HP Officejet 7140	gutenprint-ppd
HP Officejet 9100 series	manufacturer-PPDs OpenPrintingPPDs-postscript
HP Officejet Color MFP X585	hplip
HP Officejet Color X555	hplip
HP Officejet D125	gutenprint-ppd
HP Officejet D135	gutenprint-ppd
HP Officejet D145	gutenprint-ppd
HP Officejet D155	gutenprint-ppd
HP Officejet G55	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet G85	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet G95	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet K60	gutenprint-ppd
HP Officejet K60xi	gutenprint-ppd
HP Officejet K80	gutenprint-ppd
HP Officejet K80xi	gutenprint-ppd
HP Officejet LX	gutenprint-ppd
HP Officejet Pro 1150C	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet Pro 1170C Series	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet Pro 1175C	gutenprint-ppd
HP Officejet Pro 251dw Printer	hplip
HP Officejet Pro 276dw MFP	hplip
HP Officejet Pro 8000	hplip
HP Officejet Pro 8210	hplip
HP Officejet Pro 8730	hplip
HP Officejet Pro 8732M	hplip
HP Officejet Pro 8740	hplip
HP Officejet Pro X451dn/X451dw/X551dw Printer	hplip
HP Officejet Pro X476dn/X476dw/X576dw MFP	hplip
HP Officejet R40	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet R45	gutenprint-ppd
HP Officejet R60	gutenprint-ppd
HP Officejet R65	gutenprint-ppd
HP Officejet R80	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP Officejet T45	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet T65	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP Officejet V40	gutenprint-ppd
HP Officejet V40xi	gutenprint-ppd
HP PageWide Color 556	hplip
HP PageWide Color E55650	hplip
HP PageWide Color Flow MFP 586	hplip
HP PageWide Color MFP 586	hplip
HP PageWide Color MFP E58650	hplip
HP PageWide MFP P57750	hplip
HP PageWide MFP P77740-60zs	hplip
HP PageWide P55250	hplip
HP PageWide P75050-60	hplip
HP PageWide Pro 352dn/352dw Printer	hplip
HP PageWide Pro 377dn/377dw MFP	hplip
HP PageWide Pro 452dn/452dw Printer	hplip
HP PageWide Pro 477dn/477dw MFP	hplip
HP PageWide Pro 552 Printer	hplip
HP PageWide Pro 577 MFP	hplip
HP PageWide Pro 750	hplip
HP PageWide Pro MFP 772-777	hplip
HP PaintJet XL300	OpenPrintingPPDs-ghostscript
HP PhotoSmart 100	OpenPrintingPPDs-ghostscript
HP PhotoSmart 1115	OpenPrintingPPDs-ghostscript
HP PhotoSmart 1218	OpenPrintingPPDs-ghostscript
HP PhotoSmart 1315	OpenPrintingPPDs-ghostscript
HP PhotoSmart 7150	gutenprint-ppd
HP PhotoSmart 7345	gutenprint-ppd
HP PhotoSmart 7350	gutenprint-ppd
HP PhotoSmart 7550	gutenprint-ppd
HP PhotoSmart P100	gutenprint-ppd
HP PhotoSmart P130	gutenprint-ppd
HP PhotoSmart P230	gutenprint-ppd
HP PhotoSmart P1000	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP PhotoSmart P1100	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP PhotoSmart P1115	gutenprint-ppd
HP PhotoSmart P1215	OpenPrintingPPDs-ghostscript gutenprint-ppd
HP PhotoSmart P1218	gutenprint-ppd
HP PhotoSmart P1315	gutenprint-ppd
HP PSC 370	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
HP PSC 380	gutenprint-ppd
HP PSC 500	hplip OpenPrintingPPDs-ghostscript gutenprint-ppd
HP PSC 750	gutenprint-ppd
HP PSC 950	gutenprint-ppd
HP PSC 950xi	gutenprint-ppd
HP PSC 2110	gutenprint-ppd
HP PSC 2150	gutenprint-ppd
HP PSC 2210	gutenprint-ppd

Печатающие устройства производства IBM, Imagen, Imagistics, infoPrint

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
IBM	
IBM 3853 JetPrinter	OpenPrintingPPDs-ghostscript
IBM 4019	OpenPrintingPPDs-ghostscript gutenprint-ppd
IBM 4029 030 LaserPrinter 10	OpenPrintingPPDs-ghostscript gutenprint-ppd
IBM 4029 10P	OpenPrintingPPDs-postscript/
IBM 4303 Network Color Printer	OpenPrintingPPDs-postscript
IBM 4312	OpenPrintingPPDs-ghostscript gutenprint-ppd
IBM Execjet 4072	OpenPrintingPPDs-ghostscript
IBM 3112 Page Printer	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
IBM Infoprint 12	gutenprint-ppd
IBM Infoprint 1226tn	OpenPrintingPPDs-postscript
IBM Infoprint 1422	OpenPrintingPPDs-postscript
IBM Infoprint 1532 Express	OpenPrintingPPDs-postscript
IBM Infoprint 1540 MFP	OpenPrintingPPDs-postscript
IBM Infoprint 1560 MFP	OpenPrintingPPDs-postscript
IBM Infoprint 1570 MFP	OpenPrintingPPDs-postscript
IBM Infoprint 1572 MFP	OpenPrintingPPDs-postscript
IBM Infoprint 1580 MFP	OpenPrintingPPDs-postscript
IBM Infoprint 1585n	OpenPrintingPPDs-postscript
IBM Infoprint 1650 MFP	OpenPrintingPPDs-postscript
IBM Page Printer 3112	gutenprint-ppd
IBM ProPrinterII	OpenPrintingPPDs-ghostscript
Imagen	
Imagen ImPress	OpenPrintingPPDs-ghostscript
Imagistics	
Imagistics im8530	OpenPrintingPPDs-postscript
InfoPrint	
InfoPrint Pro 1107EX PS3	OpenPrintingPPDs-ghostscript
InfoPrint Pro 1107EX PS3	OpenPrintingPPDs-postscript
InfoPrint Pro 1357EX PS3	OpenPrintingPPDs-ghostscript
InfoPrint Pro 1357EX PS3	OpenPrintingPPDs-postscript
InfoPrint Pro 907EX PS3	OpenPrintingPPDs-ghostscript
InfoPrint Pro 907EX PS3	OpenPrintingPPDs-postscript

Печатающие устройства производства Kodak, Konica Minolta

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Kodak	
Kodak DigiSource 9110	OpenPrintingPPDs-postscript
Kodak IS 70 CPII	OpenPrintingPPDs-postscript
Kodak 305	gutenprint-ppd
Kodak 605	gutenprint-ppd
Kodak 805	gutenprint-ppd
Kodak 1400	gutenprint-ppd
Kodak 6800	gutenprint-ppd
Kodak 6850	gutenprint-ppd
Kodak 7000	gutenprint-ppd
Kodak 7010	gutenprint-ppd
Kodak 7015	gutenprint-ppd
Kodak 8500	gutenprint-ppd
Kodak 8800	gutenprint-ppd
Kodak 8810	gutenprint-ppd
Kodak 9810	gutenprint-ppd
Kodak EasyShare-G600-Printer-Dock	gutenprint-ppd
Kodak Easyshare-Printer-Dock	gutenprint-ppd
Kodak PD-4000	gutenprint-ppd
Kodak PD-6000	gutenprint-ppd
Kodak Photo-Printer	gutenprint-ppd
Kodak Photo-Printer-500	gutenprint-ppd
Kodak Printer-Dock-Plus	gutenprint-ppd
Kodak Printer-Dock-Plus-S3	gutenprint-ppd
Konica Minolta	
Konica Minolta 1050	OpenPrintingPPDs-postscript
Konica Minolta 500/420/360	OpenPrintingPPDs-postscript
Konica Minolta 750/600	OpenPrintingPPDs-postscript
Konica Minolta C250	OpenPrintingPPDs-postscript
Konica Minolta C252	OpenPrintingPPDs-postscript
Konica Minolta C351	OpenPrintingPPDs-postscript
Konica Minolta C352/C300	OpenPrintingPPDs-postscript
Konica Minolta C450	OpenPrintingPPDs-postscript
Konica Minolta C451	OpenPrintingPPDs-postscript
Konica Minolta C550	OpenPrintingPPDs-postscript
Konica Minolta magicolor 1600W	foo2zjs
Konica Minolta magicolor 1680MF	foo2zjs
Konica Minolta magicolor 1690MF	foo2zjs
Konica Minolta magicolor 2480MF	foo2zjs
Konica Minolta magicolor 2490MF	foo2zjs
Konica Minolta magicolor 4690MF	foo2zjs
Konica Minolta magicolor 2430 DL	foo2zjs
Konica Minolta magicolor 2530 DL	foo2zjs

Печатающие устройства производства Kyocera

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Kyocera Ci-1100	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-250ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-300ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-400ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-500ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1650	manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-1815	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-2050	manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-3050ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-3550ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C2525E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C3225E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C3232E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C4035E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript

Модели (серий) устройств	RPM-Pakete-PPDs-дверский для данного устройства
Kyocera C-1200	OpenPrintingPPDs-ghostscript
Kyocera F-1000	OpenPrintingPPDs-ghostscript
Kyocera F-1010	OpenPrintingPPDs-hpijs gutenprint-ppd OpenPrintingPPDs-postscript
Kyocera F-1200	OpenPrintingPPDs-ghostscript
Kyocera F-1200S	OpenPrintingPPDs-hpijs
Kyocera F-1800	OpenPrintingPPDs-postscript
Kyocera F-2000	OpenPrintingPPDs-ghostscript
Kyocera F-2010	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript
Kyocera F-2200	OpenPrintingPPDs-postscript
Kyocera F-2200S	OpenPrintingPPDs-ghostscript
Kyocera F-3000	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript
Kyocera F-3010	OpenPrintingPPDs-postscript
Kyocera F-3300	OpenPrintingPPDs-ghostscript
Kyocera F-5000	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript
Kyocera FS-400	OpenPrintingPPDs-postscript
Kyocera CS-1650	OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera FS-600	OpenPrintingPPDs-postscript manufacturer-PPDs
Kyocera CS-1815	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-680	gutenprint-ppd manufacturer-PPDs
Kyocera CS-2050	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera CS-3050ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs gutenprint-ppd OpenPrintingPPDs-postscript
Kyocera FS-800	manufacturer-PPDs
Kyocera CS-3550ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C2525E	OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs
Kyocera FS-850	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C3225E	OpenPrintingPPDs-ghostscript
Kyocera FS-920	manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera CS-C3232E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs gutenprint-ppd
Kyocera FS-1000	manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-C4035E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript gutenprint-ppd
Kyocera F-800T	OpenPrintingPPDs-ghostscript

Модели устройств	RPM-пакеты с драйверами для данного устройства
Kyocera Ci-1100	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-2010 Kyocera CS-2510i	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-300ci Kyocera FS-1018MFP	OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-400ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-500ci Kyocera FS-1020D	gutenprint-ppd OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1650	OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1815 Kyocera FS-1030D	gutenprint-ppd manufacturer-PPDs OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs gutenprint-ppd OpenPrintingPPDs-postscript
Kyocera CS-2050 Kyocera FS-1050	gutenprint-ppd manufacturer-PPDs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-3050ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-3550ci Kyocera FS-1118MFP	gutenprint-ppd OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C2525E Kyocera FS-1135MFP	OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs gutenprint-ppd OpenPrintingPPDs-postscript
Kyocera CS-C3225E	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C3232E Kyocera FS-1500	OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-C4035E Kyocera FS-1550	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera F-800 Kyocera FS-1350+	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera F-800T	OpenPrintingPPDs-ghostscript

Kyocera FS-1600/1600+	OpenPrintingPPDs-ghostscript
Kyocera Ci-1100	manufacturer-PPDs OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera FS-1700/1700+	manufacturer-PPDs
Kyocera CS-250ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-300ci Kyocera FS-1714M	gutenprint-ppd manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-400ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-1750 Kyocera CS-500ci	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1650	manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-1800/1800+ Kyocera CS-1815	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-1900 Kyocera CS-2050	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-3050ci	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-1920 Kyocera CS-3550ci	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C2525E Kyocera FS-2000D	OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-C3225E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C3232E Kyocera FS-2100D	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-C4035E Kyocera FS-2100DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera F-800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Kyocera F-800T	OpenPrintingPPDs-ghostscript

Kyocera FS-3400/3400+	OpenPrintingPPDs-ghostscript
Kyocera Ci-1100	manufacturer-PPDs
Kyocera FS-3500	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
Kyocera FS-3600/3600+	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
Kyocera CS-300ci	gutenprint-ppd
Kyocera FS-3700/3700+/3718M	manufacturer-PPDs
	OpenPrintingPPDs-postscript
Kyocera CS-400ci	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
	gutenprint-ppd
Kyocera CS-3050ci	manufacturer-PPDs
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
Kyocera CS-1650	manufacturer-PPDs
	gutenprint-ppd
Kyocera CS-1815	manufacturer-PPDs
	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
	gutenprint-ppd
Kyocera CS-2050	manufacturer-PPDs
	OpenPrintingPPDs-ghostscript
Kyocera CS-3050ci	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
	gutenprint-ppd
Kyocera CS-3550ci	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
Kyocera CS-C2525E	OpenPrintingPPDs-ghostscript
	gutenprint-ppd
Kyocera FS-4000DN	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
	manufacturer-PPDs
Kyocera CS-C3225E	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-postscript
Kyocera CS-C3232E	OpenPrintingPPDs-ghostscript
	gutenprint-ppd
Kyocera FS-4100DN/4200DN/4300DN	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-postscript
Kyocera CS-C4035E	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-ghostscript
Kyocera FS-5500	OpenPrintingPPDs-postscript
	OpenPrintingPPDs-hpijs
	OpenPrintingPPDs-ghostscript
	OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript

Kyocera F-800T	OpenPrintingPPDs-ghostscript

Kyocera FS-5900C/5900C	manufacturer-PPDs
Kyocera Ci-1100	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-2020/6026	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-300ci Kyocera FS-6300/6500/6500+	OpenPrintingPPDs-ghostscript gutenprint-ppd manufacturer-PPDs
Kyocera CS-400ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-500ci Kyocera FS-6700/6750	OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-1650	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1815 Kyocera FS-6900/6950DN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-2050 Kyocera FS-7000/7000+/7028M	gutenprint-ppd manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-3050ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-3550ci Kyocera FS-8000C	OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-C2525E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd OpenPrintingPPDs-postscript
Kyocera FS-9100DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C3232E Kyocera FS-9120DN	OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C4035E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript
Kyocera F-800T	OpenPrintingPPDs-ghostscript

Модели устройств	Драйверы для данного устройства
Kyocera FS-9130DN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera Ci-1100	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera FS-9500DN/9530DN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-300ci Kyocera FS-9520DN	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript gutenprint-ppd OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-400ci Kyocera FS-C5015N	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-500ci Kyocera FS-C5016N	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-1650	OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-1815 Kyocera FS-C5025N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript gutenprint-ppd OpenPrintingPPDs-ghostscript
Kyocera CS-2050	OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-3050ci	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-3550ci Kyocera FS-C5100DN/C5200DN/C5300DN/C5350DN	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C2525E Kyocera FS-C5400DN	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C3225E Kyocera FS-C8008N	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-C3232E Kyocera FS-C8026N	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-C4035E Kyocera FS-C8100DN/C8100DN+	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera F-800T	OpenPrintingPPDs-ghostscript

Модели принтеров	Рекомендуемые драйверами для данного устройства
Kyocera Ci-1100	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppds
Kyocera CS-1505 Kyocera KM-1650	foo2zjs OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1810/1815	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-400ci Kyocera KM-1820	OpenPrintingPPDs-ghostscript gutenprint-ppds OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-500ci	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppds
Kyocera CS-2030 Kyocera CS-2050	manufacturer-PPDs manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-1815 Kyocera KM-2035 Kyocera KM-2050	OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-ghostscript gutenprint-ppds OpenPrintingPPDs-hpijs foo2zjs OpenPrintingPPDs-postscript gutenprint-ppds manufacturer-PPDs
Kyocera CS-2050 Kyocera KM-2530	manufacturer-PPDs OpenPrintingPPDs-postscript manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-3050ci	**OpenPrintingPPDs-ghostscript** **OpenPrintingPPDs-hpijs** **OpenPrintingPPDs-postscript**
Kyocera CS-3550ci Kyocera KM-2550	gutenprint-ppds OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-3225E Kyocera KM-3050	manufacturer-PPDs manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-C3225E	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppds
Kyocera CS-3232E	manufacturer-PPDs manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-C4035E Kyocera KM-4030/4035	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript gutenprint-ppds OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera F-800T	OpenPrintingPPDs-ghostscript

Модели устройств	Драйверы для данного устройства
Kyocera KM-4050	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera Ci-1100 Kyocera KM-4230	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-250ci	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-300ci Kyocera KM-4230/5230	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-400ci Kyocera KM-4530	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-500ci	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-1650 Kyocera KM-5035	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-1815 Kyocera KM-5050	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-2030 Kyocera KM-5230	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-3050ci Kyocera KM-5530	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-3550ci	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-C2525E Kyocera KM-6030/6230	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-C3225E Kyocera KM-6330	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-C3232E Kyocera KM-7530	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera CS-C4035E Kyocera KM-8030	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera F-800	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Kyocera F-800T	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Kyocera KM-C830/C850	manufacturer-PPDs
Kyocera Ci-1100	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera KM-C2520	manufacturer-PPDs
Kyocera CS-250ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-300ci Kyocera KM-C2525E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-400ci Kyocera KM-C2630	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-500ci Kyocera KM-C3225	OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Kyocera CS-1650	OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-1815 Kyocera KM-C3225E Kyocera KM-C3232	OpenPrintingPPDs-ghostscript manufacturer-PPDs OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript manufacturer-PPDs OpenPrintingPPDs-postscript gutenprint
Kyocera CS-2050	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs manufacturer-PPDs OpenPrintingPPDs-postscript
Kyocera CS-3050ci Kyocera KM-C3232E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera CS-3550ci Kyocera KM-C4035E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Kyocera P-2000/2002	OpenPrintingPPDs-ghostscript
Kyocera CS-C2525E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera TASKalfa 250ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-C3225E	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera TASKalfa 300ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-C3232E	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera TASKalfa 400ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera CS-C4035E	OpenPrintingPPDs-hpijs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript OpenPrintingPPDs-hpijs
Kyocera TASKalfa 500ci	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera F-800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Kyocera F-800T	OpenPrintingPPDs-ghostscript

Печатающие устройства производства Lanier

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier 2132 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier 2138 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier 2145 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier 5622	gutenprint-ppd
Lanier 5622 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier 5627	gutenprint-ppd
Lanier 5627 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier 5632	gutenprint-ppd
Lanier 5632 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier 5635	gutenprint-ppd
Lanier 5635 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier 5645	gutenprint-ppd
Lanier 5645 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LC155 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD 130C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD 130CSR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD 140C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD 140CSR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD 620C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD 625C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD0105	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier LD0105 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD015	gutenprint-ppd
Lanier LD015 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD024c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LD032c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LD035	gutenprint-ppd
Lanier LD035 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD045	gutenprint-ppd
Lanier LD045 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD060	gutenprint-ppd
Lanier LD060 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD075	gutenprint-ppd
Lanier LD075 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD090	gutenprint-ppd
Lanier LD090 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD115	gutenprint-ppd
Lanier LD115 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD116	gutenprint-ppd
Lanier LD116 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD118	gutenprint-ppd
Lanier LD118 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD118d	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier LD118d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD120	gutenprint-ppd
Lanier LD120 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD120d	gutenprint-ppd
Lanier LD120d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD122	gutenprint-ppd
Lanier LD122 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD124c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD127	gutenprint-ppd
Lanier LD127 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD132	gutenprint-ppd
Lanier LD132 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD132c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD135	gutenprint-ppd
Lanier LD135 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD145	gutenprint-ppd
Lanier LD145 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD151	gutenprint-ppd
Lanier LD151 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD160	gutenprint-ppd
Lanier LD160 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier LD160c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD175	gutenprint-ppd
Lanier LD175 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD225	gutenprint-ppd
Lanier LD225 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD228c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LD230	gutenprint-ppd
Lanier LD230 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD232c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LD235	gutenprint-ppd
Lanier LD235 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD238c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LD245	gutenprint-ppd
Lanier LD245 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD328c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD335c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LD345c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier LF510/515e PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP 020c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP 036c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier LP025/LP026 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP025N/LP026N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP031c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP032 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP116c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP122c/LP121c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP124w PS3	OpenPrintingPPDs-postscript
Lanier LP125cx/LP126cn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP127n/LP128n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP128 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP131n/LP131nL PS3	OpenPrintingPPDs-postscript
Lanier LP135n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP136n/LP137CN PS3	OpenPrintingPPDs-postscript
Lanier LP138c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP142CN PS3	OpenPrintingPPDs-postscript
Lanier LP145n/SP 8100DN PS3	OpenPrintingPPDs-postscript
Lanier LP150dn/SP8200DN PS3	OpenPrintingPPDs-postscript
Lanier LP175/LP175hdn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP222cn/LP221c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP226c/SP C410 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP231c/SP C411 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP235c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Lanier LP331cn/SP C420 PS3	OpenPrintingPPDs-postscript
Lanier LP332c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP335c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Lanier LP37N PS3	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier LP440c/SP C811DN PS3	OpenPrintingPPDs-postscript
Lanier LP540C/SPC820DN PS3	OpenPrintingPPDs-postscript
Lanier LP550C/SPC821DN PS3	OpenPrintingPPDs-postscript
Lanier LW324/LW326 PS3	OpenPrintingPPDs-postscript
Lanier LW426 PS3	OpenPrintingPPDs-postscript
Lanier LW5100 PS3	OpenPrintingPPDs-postscript
Lanier LW7140 PS3	OpenPrintingPPDs-postscript
Lanier MP 1100/LD1100	gutenprint-ppd
Lanier MP 1100/LD1100 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 1350/LD1135	gutenprint-ppd
Lanier MP 1350/LD1135 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 1600/LD316	gutenprint-ppd
Lanier MP 1600/LD316 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 161/LD016	gutenprint-ppd
Lanier MP 161/LD016 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 171/LD 117 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2000/LD320d	gutenprint-ppd
Lanier MP 2000/LD320d PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 201/LD 220 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2510/LD325	gutenprint-ppd
Lanier MP 2510/LD325 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2550/LD425	gutenprint-ppd
Lanier MP 2550/LD425 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2550B/LD425B	gutenprint-ppd
Lanier MP 2550B/LD425B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2553 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier MP 2851/LD528 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 2852 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 301 PS3	OpenPrintingPPDs-postscript
Lanier MP 3010/LD330	gutenprint-ppd
Lanier MP 3010/LD330 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3053 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3350/LD433	gutenprint-ppd
Lanier MP 3350/LD433 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3350B/LD433B	gutenprint-ppd
Lanier MP 3350B/LD433B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3351/LD533 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3353 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 3500/LD335	gutenprint-ppd
Lanier MP 3500/LD335 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 4000/LD040	gutenprint-ppd
Lanier MP 4000/LD040 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 4000B/LD040B	gutenprint-ppd
Lanier MP 4000B/LD040B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 4001/LD140 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 4002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 4500/LD345	gutenprint-ppd
Lanier MP 4500/LD345 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 5000/LD050	gutenprint-ppd
Lanier MP 5000/LD050 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 5000B/LD050B	gutenprint-ppd
Lanier MP 5000B/LD050B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier MP 5001/LD150 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 5002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 5500/LD255	gutenprint-ppd
Lanier MP 5500/LD255 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 6000/LD260 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 6001/LD360 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 6002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 6500/LD265	gutenprint-ppd
Lanier MP 6500/LD265 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 7000/LD270 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 7001/LD370 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 7500/LD275	gutenprint-ppd
Lanier MP 7500/LD275 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 7502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 8000/LD280 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 8001/LD380 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 9000/LD190	gutenprint-ppd
Lanier MP 9000/LD190 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 9001/LD390 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP 9002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C305 PS3	OpenPrintingPPDs-postscript
Lanier MP C400 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier MP C2003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C2050/LD520C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C2500/LD425c PS3	manufacturer-PPDs
Lanier MP C2500/LD425c PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C2503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C2550/LD525C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C2800/LD528C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3000/LD430c PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3001/LD630C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C300SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3300/LD533C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3500/LD435c PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3501/LD635C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C3503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C4000/LD540C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C400SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C4500/LD445c PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C4501/LD645C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C4502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C4502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier MP C4503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C5000/LD550C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C5501/LD655C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C5502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C5502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C5503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C6000/LD260c PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C6003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C6501/LD365C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C6502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C7500/LD275c PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C7501/LD375C PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP C8002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MP CW2200 PS3	OpenPrintingPPDs-postscript
Lanier MP2500/LD125	gutenprint-ppd
Lanier MP2500/LD125 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MPC1500/LD215c PS3	manufacturer-PPDs
Lanier MPC1500/LD215c PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MPC4501A/LD645CA PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier MPC5501A/LD655CA PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 1106EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 1107EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 1356EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 1357EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lanier Pro 8100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 8110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 8120S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 906EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro 907EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro C5100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier Pro C5110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lanier SG3110DN	OpenPrintingPPDs-ghostscript
Lanier SG3110DNw	OpenPrintingPPDs-ghostscript
Lanier SG3110SFNw	OpenPrintingPPDs-ghostscript
Lanier SP 4100N PS3	OpenPrintingPPDs-postscript
Lanier SP 4100NL PS3	OpenPrintingPPDs-postscript
Lanier SP 4110N PS3	OpenPrintingPPDs-postscript
Lanier SP 4210N PS3	OpenPrintingPPDs-postscript
Lanier SP 4310N PS3	OpenPrintingPPDs-postscript
Lanier SP 5200DN PS3	OpenPrintingPPDs-postscript
Lanier SP 5200S PS3	OpenPrintingPPDs-postscript
Lanier SP 5210DN PS3	OpenPrintingPPDs-postscript
Lanier SP 5210SF PS3	OpenPrintingPPDs-postscript
Lanier SP 5210SR PS3	OpenPrintingPPDs-postscript
Lanier SP 6330N PS3	OpenPrintingPPDs-postscript
Lanier SP 8300DN PS3	OpenPrintingPPDs-postscript
Lanier SP 9100/LP275 PS3	OpenPrintingPPDs-postscript
Lanier SP C320DN PS3	OpenPrintingPPDs-postscript
Lanier SP C400DN PS3	OpenPrintingPPDs-postscript
Lanier SP C430DN PS3	OpenPrintingPPDs-postscript
Lanier SP C431DN PS3	OpenPrintingPPDs-postscript
Lanier SP C730DN PS3	OpenPrintingPPDs-postscript
Lanier SP C830DN PS3	OpenPrintingPPDs-postscript
Lanier SP C831DN PS3	OpenPrintingPPDs-postscript

Печатающие устройства производства Lexmark

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lexmark MB2236adw	Lexmark-AEX-PPD-Files-1.0-01242019.x86_64.rpm
Lexmark 1020 Business	OpenPrintingPPDs-ghostscript
Lexmark 7000	OpenPrintingPPDs-ghostscript
Lexmark C500	foo2zjs
Lexmark C500n	OpenPrintingPPDs-postscript
Lexmark C510	OpenPrintingPPDs-postscript
Lexmark C510b	OpenPrintingPPDs-postscript
Lexmark C530dn	OpenPrintingPPDs-postscript
Lexmark C532dn	OpenPrintingPPDs-postscript
Lexmark C532n	OpenPrintingPPDs-postscript
Lexmark C534dn	OpenPrintingPPDs-postscript
Lexmark C534dtn	OpenPrintingPPDs-postscript
Lexmark C534n	OpenPrintingPPDs-postscript
Lexmark C720n	OpenPrintingPPDs-ghostscript
Lexmark C720n	OpenPrintingPPDs-postscript
Lexmark C750	OpenPrintingPPDs-postscript
Lexmark C752	OpenPrintingPPDs-postscript
Lexmark C752b	OpenPrintingPPDs-postscript
Lexmark C770dtn	OpenPrintingPPDs-postscript
Lexmark C770n	OpenPrintingPPDs-postscript
Lexmark C772dn	OpenPrintingPPDs-postscript
Lexmark C772n	OpenPrintingPPDs-postscript
Lexmark C780dn	OpenPrintingPPDs-postscript
Lexmark C780dtn	OpenPrintingPPDs-postscript
Lexmark C780n	OpenPrintingPPDs-postscript
Lexmark C782dn	OpenPrintingPPDs-postscript
Lexmark C782dtn	OpenPrintingPPDs-postscript
Lexmark C782n	OpenPrintingPPDs-postscript
Lexmark C910	OpenPrintingPPDs-postscript
Lexmark C912	OpenPrintingPPDs-postscript
Lexmark C920n	OpenPrintingPPDs-postscript
Lexmark C935dn	OpenPrintingPPDs-postscript
Lexmark C935dtn	OpenPrintingPPDs-postscript
Lexmark C935hdn	OpenPrintingPPDs-postscript
Lexmark E210	OpenPrintingPPDs-ghostscript
Lexmark E320	OpenPrintingPPDs-ghostscript
Lexmark E450dn	OpenPrintingPPDs-ghostscript
Lexmark E450dn	OpenPrintingPPDs-postscript
Lexmark IBM LaserPrinter 4039 plus	OpenPrintingPPDs-postscript
Lexmark 3000 Color Jetprinter	OpenPrintingPPDs-ghostscript
Lexmark 3200	OpenPrintingPPDs-ghostscript
Lexmark 4076	gutenprint-ppd
Lexmark 5700	OpenPrintingPPDs-ghostscript
Lexmark 6500e	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lexmark 6500e Series	OpenPrintingPPDs-postscript
Lexmark C2100 Series	OpenPrintingPPDs-postscript
Lexmark C2132	OpenPrintingPPDs-postscript
Lexmark C510	OpenPrintingPPDs-postscript
Lexmark C520	OpenPrintingPPDs-postscript
Lexmark C522	OpenPrintingPPDs-postscript
Lexmark C524	OpenPrintingPPDs-postscript
Lexmark C540	OpenPrintingPPDs-postscript
Lexmark C543	OpenPrintingPPDs-postscript
Lexmark C544	OpenPrintingPPDs-postscript
Lexmark C546	OpenPrintingPPDs-postscript
Lexmark C734	OpenPrintingPPDs-postscript
Lexmark C736	OpenPrintingPPDs-postscript
Lexmark C740 Series	OpenPrintingPPDs-postscript
Lexmark C746	OpenPrintingPPDs-postscript
Lexmark C748	OpenPrintingPPDs-postscript
Lexmark C750	OpenPrintingPPDs-postscript
Lexmark C752	OpenPrintingPPDs-postscript
Lexmark C780	OpenPrintingPPDs-postscript
Lexmark C782	OpenPrintingPPDs-postscript
Lexmark C790 Series	OpenPrintingPPDs-postscript
Lexmark C792	OpenPrintingPPDs-postscript
Lexmark C910	OpenPrintingPPDs-postscript
Lexmark C912	OpenPrintingPPDs-postscript
Lexmark C920 Series	OpenPrintingPPDs-postscript
Lexmark C925	OpenPrintingPPDs-postscript
Lexmark C930	OpenPrintingPPDs-postscript
Lexmark C935	OpenPrintingPPDs-postscript
Lexmark C950	OpenPrintingPPDs-postscript
Lexmark CS310 Series	OpenPrintingPPDs-postscript
Lexmark CS310dn	OpenPrintingPPDs-postscript
Lexmark CS310n	OpenPrintingPPDs-postscript
Lexmark CS410 Series	OpenPrintingPPDs-postscript
Lexmark CS410dn	OpenPrintingPPDs-postscript
Lexmark CS410n	OpenPrintingPPDs-postscript
Lexmark CS510 Series	OpenPrintingPPDs-postscript
Lexmark CS510de	OpenPrintingPPDs-postscript
Lexmark CX310 Series	OpenPrintingPPDs-postscript
Lexmark CX310dn	OpenPrintingPPDs-postscript
Lexmark CX310n	OpenPrintingPPDs-postscript
Lexmark CX410 Series	OpenPrintingPPDs-postscript
Lexmark CX410de	OpenPrintingPPDs-postscript
Lexmark CX410e	OpenPrintingPPDs-postscript
Lexmark CX510 Series	OpenPrintingPPDs-postscript
Lexmark CX510de	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lexmark E120	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Lexmark E120n	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Lexmark E230	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Lexmark E238	OpenPrintingPPDs-ghostscript
Lexmark E260	OpenPrintingPPDs-postscript
Lexmark E260d	OpenPrintingPPDs-postscript
Lexmark E260dn	OpenPrintingPPDs-postscript
Lexmark E321	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Lexmark E350d	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lexmark E352dn	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Lexmark E360d	OpenPrintingPPDs-postscript
Lexmark E360dn	OpenPrintingPPDs-postscript
Lexmark E460dn	OpenPrintingPPDs-postscript
Lexmark E460dw	OpenPrintingPPDs-postscript
Lexmark E462dtn	OpenPrintingPPDs-postscript
Lexmark EG460dn	OpenPrintingPPDs-postscript
Lexmark M1100 Series	OpenPrintingPPDs-postscript
Lexmark M1140	OpenPrintingPPDs-postscript
Lexmark M1140 Plus	OpenPrintingPPDs-postscript
Lexmark M1145	OpenPrintingPPDs-postscript
Lexmark M3100 Series	OpenPrintingPPDs-postscript
Lexmark M3150	OpenPrintingPPDs-postscript
Lexmark M5100 Series	OpenPrintingPPDs-postscript
Lexmark M5155	OpenPrintingPPDs-postscript
Lexmark M5163	OpenPrintingPPDs-postscript
Lexmark M5170	OpenPrintingPPDs-postscript
Lexmark MS310 Series	OpenPrintingPPDs-postscript
Lexmark MS310d	OpenPrintingPPDs-postscript
Lexmark MS310dn	OpenPrintingPPDs-postscript
Lexmark MS312dn	OpenPrintingPPDs-postscript
Lexmark MS315dn	OpenPrintingPPDs-postscript
Lexmark MS410 Series	OpenPrintingPPDs-postscript
Lexmark MS410d	OpenPrintingPPDs-postscript
Lexmark MS410dn	OpenPrintingPPDs-postscript
Lexmark MS415dn	OpenPrintingPPDs-postscript
Lexmark MS510 Series	OpenPrintingPPDs-postscript
Lexmark MS510dn	OpenPrintingPPDs-postscript
Lexmark MS610 Series	OpenPrintingPPDs-postscript
Lexmark MS610de	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lexmark MS610dn	OpenPrintingPPDs-postscript
Lexmark MS710	OpenPrintingPPDs-postscript
Lexmark MS711	OpenPrintingPPDs-postscript
Lexmark MS810	OpenPrintingPPDs-postscript
Lexmark MS811	OpenPrintingPPDs-postscript
Lexmark MS812	OpenPrintingPPDs-postscript
Lexmark MX310 Series	OpenPrintingPPDs-postscript
Lexmark MX310dn	OpenPrintingPPDs-postscript
Lexmark MX410 Series	OpenPrintingPPDs-postscript
Lexmark MX410de	OpenPrintingPPDs-postscript
Lexmark MX510 Series	OpenPrintingPPDs-postscript
Lexmark MX510de	OpenPrintingPPDs-postscript
Lexmark MX511de	OpenPrintingPPDs-postscript
Lexmark MX511dhe	OpenPrintingPPDs-postscript
Lexmark MX610 Series	OpenPrintingPPDs-postscript
Lexmark MX610de	OpenPrintingPPDs-postscript
Lexmark MX611de	OpenPrintingPPDs-postscript
Lexmark MX611dhe	OpenPrintingPPDs-postscript
Lexmark MX6500e	OpenPrintingPPDs-postscript
Lexmark MX710	OpenPrintingPPDs-postscript
Lexmark MX711	OpenPrintingPPDs-postscript
Lexmark MX810	OpenPrintingPPDs-postscript
Lexmark MX811	OpenPrintingPPDs-postscript
Lexmark MX812	OpenPrintingPPDs-postscript
Lexmark Optra C710	OpenPrintingPPDs-postscript
Lexmark Optra Color 40	OpenPrintingPPDs-postscript
Lexmark Optra Color 45	OpenPrintingPPDs-postscript
Lexmark Optra Color 1200	OpenPrintingPPDs-postscript
Lexmark Optra Color 1275	OpenPrintingPPDs-postscript
Lexmark Optra E	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Lexmark Optra E+ LaserPrinter	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Lexmark Optra E220	gutenprint-ppd
Lexmark Optra E310	OpenPrintingPPDs-postscript
Lexmark Optra E312	OpenPrintingPPDs-postscript
Lexmark Optra E321	gutenprint-ppd
Lexmark Optra E323	gutenprint-ppd
Lexmark Optra Ep LaserPrinter	OpenPrintingPPDs-postscript
Lexmark Optra K 1220	OpenPrintingPPDs-postscript
Lexmark Optra LaserPrinter	OpenPrintingPPDs-postscript
Lexmark Optra M410	OpenPrintingPPDs-postscript
Lexmark Optra M412	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lexmark Optra S 1250	OpenPrintingPPDs-postscript
Lexmark Optra S 1855	OpenPrintingPPDs-postscript
Lexmark Optra Se 3455	OpenPrintingPPDs-postscript
Lexmark Optra T610	OpenPrintingPPDs-postscript
Lexmark Optra T612	OpenPrintingPPDs-postscript
Lexmark Optra T614	OpenPrintingPPDs-postscript
Lexmark Optra T616	OpenPrintingPPDs-postscript
Lexmark Optra W810	OpenPrintingPPDs-postscript
Lexmark T430	OpenPrintingPPDs-postscript
Lexmark T640	OpenPrintingPPDs-postscript
Lexmark T642	OpenPrintingPPDs-postscript
Lexmark T644	OpenPrintingPPDs-postscript
Lexmark T650	OpenPrintingPPDs-postscript
Lexmark T652	OpenPrintingPPDs-postscript
Lexmark T654	OpenPrintingPPDs-postscript
Lexmark T656	OpenPrintingPPDs-postscript
Lexmark TG654	OpenPrintingPPDs-postscript
Lexmark Valuewriter 300	OpenPrintingPPDs-ghostscript gutenprint-ppd
Lexmark W812	OpenPrintingPPDs-postscript
Lexmark W840	OpenPrintingPPDs-postscript
Lexmark W850	OpenPrintingPPDs-postscript
Lexmark Winwriter 400	OpenPrintingPPDs-ghostscript
Lexmark X73	gutenprint-ppd
Lexmark X203n	OpenPrintingPPDs-postscript
Lexmark X204n	OpenPrintingPPDs-postscript
Lexmark X264dn	OpenPrintingPPDs-postscript
Lexmark X342n	OpenPrintingPPDs-ghostscript
Lexmark X363dn	OpenPrintingPPDs-postscript
Lexmark X364dn	OpenPrintingPPDs-postscript
Lexmark X364dw	OpenPrintingPPDs-postscript
Lexmark X463de	OpenPrintingPPDs-postscript
Lexmark X464de	OpenPrintingPPDs-postscript
Lexmark X466de	OpenPrintingPPDs-postscript
Lexmark X466dte	OpenPrintingPPDs-postscript
Lexmark X466dwe	OpenPrintingPPDs-postscript
Lexmark X543	OpenPrintingPPDs-postscript
Lexmark X544	OpenPrintingPPDs-postscript
Lexmark X546	OpenPrintingPPDs-postscript
Lexmark X548	OpenPrintingPPDs-postscript
Lexmark X560n	OpenPrintingPPDs-postscript
Lexmark X642e	OpenPrintingPPDs-ghostscript
Lexmark X651de	OpenPrintingPPDs-postscript
Lexmark X652de	OpenPrintingPPDs-postscript
Lexmark X654de	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Lexmark X656de	OpenPrintingPPDs-postscript
Lexmark X658de	OpenPrintingPPDs-postscript
Lexmark X734de	OpenPrintingPPDs-postscript
Lexmark X736de	OpenPrintingPPDs-postscript
Lexmark X738de	OpenPrintingPPDs-postscript
Lexmark X740 Series	OpenPrintingPPDs-postscript
Lexmark X746	OpenPrintingPPDs-postscript
Lexmark X748	OpenPrintingPPDs-postscript
Lexmark X790 Series	OpenPrintingPPDs-postscript
Lexmark X792	OpenPrintingPPDs-postscript
Lexmark X860de	OpenPrintingPPDs-postscript
Lexmark X862de	OpenPrintingPPDs-postscript
Lexmark X864de	OpenPrintingPPDs-postscript
Lexmark X920 Series	OpenPrintingPPDs-postscript
Lexmark X925	OpenPrintingPPDs-postscript
Lexmark X940e	OpenPrintingPPDs-postscript
Lexmark X945e	OpenPrintingPPDs-postscript
Lexmark X950	OpenPrintingPPDs-postscript
Lexmark X952	OpenPrintingPPDs-postscript
Lexmark X954	OpenPrintingPPDs-postscript
Lexmark XC2100 Series	OpenPrintingPPDs-postscript
Lexmark XC2130	OpenPrintingPPDs-postscript
Lexmark XC2132	OpenPrintingPPDs-postscript
Lexmark XM1100 Series	OpenPrintingPPDs-postscript
Lexmark XM1135	OpenPrintingPPDs-postscript
Lexmark XM1140	OpenPrintingPPDs-postscript
Lexmark XM1145	OpenPrintingPPDs-postscript
Lexmark XM3100 Series	OpenPrintingPPDs-postscript
Lexmark XM3150	OpenPrintingPPDs-postscript
Lexmark XM5100 Series	OpenPrintingPPDs-postscript
Lexmark XM5163	OpenPrintingPPDs-postscript
Lexmark XM5170	OpenPrintingPPDs-postscript
Lexmark XM7100 Series	OpenPrintingPPDs-postscript
Lexmark XM7155	OpenPrintingPPDs-postscript
Lexmark XM7163	OpenPrintingPPDs-postscript
Lexmark XM7170	OpenPrintingPPDs-postscript
Lexmark Z22-Z32	OpenPrintingPPDs-ghostscript
Lexmark Z42	gutenprint-ppd
Lexmark Z43	gutenprint-ppd
Lexmark Z52	gutenprint-ppd
Lexmark Z53	gutenprint-ppd

Печатающие устройства производства Minolta, Mitsubishi, NEC

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Minolta	
Minolta magicolor 3100	OpenPrintingPPDs-postscript
Minolta PagePro 6	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Minolta PagePro 6e	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Minolta PagePro 6ex	gutenprint-ppd
Minolta PagePro 8	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Minolta PagePro 8L	OpenPrintingPPDs-ghostscript gutenprint-ppd
Minolta PagePro 1100	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Minolta PagePro 1250E	OpenPrintingPPDs-postscript
Minolta QMS PagePro 9100N	OpenPrintingPPDs-postscript
Mitsubishi	
Mitsubishi CP50 Color Printer	OpenPrintingPPDs-ghostscript
Mitsubishi CP-3020D	gutenprint-ppd
Mitsubishi CP-3020DA	gutenprint-ppd
Mitsubishi CP-3020DAE	gutenprint-ppd
Mitsubishi CP-3020DE	gutenprint-ppd
Mitsubishi CP-3020DU	gutenprint-ppd
Mitsubishi CP-3800DW	gutenprint-ppd
Mitsubishi CP-9500DW	gutenprint-ppd
Mitsubishi CP-9550D	gutenprint-ppd
Mitsubishi CP-9550DW	gutenprint-ppd
Mitsubishi CP-9550DW-S	gutenprint-ppd
Mitsubishi CP-9550DZ	gutenprint-ppd
Mitsubishi CP-9600DW	gutenprint-ppd
Mitsubishi CP-9800D	gutenprint-ppd
Mitsubishi CP-9800DW	gutenprint-ppd
Mitsubishi CP-9800DW-S	gutenprint-ppd
Mitsubishi CP-9800DZ	gutenprint-ppd
Mitsubishi CP-9810D	gutenprint-ppd
Mitsubishi CP-9810DW	gutenprint-ppd
Mitsubishi CP-D70DW	gutenprint-ppd
Mitsubishi CP-D80DW	gutenprint-ppd
Mitsubishi CP-D90DW	gutenprint-ppd
Mitsubishi CP-D707DW	gutenprint-ppd
Mitsubishi CP-K60DW-S	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Mitsubishi P95D	gutenprint-ppd
NEC	
NEC MultiWriter	OpenPrintingPPDs-ghostscript
NEC SuperScript 660i	gutenprint-ppd
NEC SuperScript 860	gutenprint-ppd
NEC SuperScript 870	gutenprint-ppd
NEC SuperScript 1260	gutenprint-ppd
NEC SuperScript 1400	gutenprint-ppd
NEC SuperScript 1800	gutenprint-ppd
NEC P2X	OpenPrintingPPDs-ghostscript
NEC PC-PR150	OpenPrintingPPDs-ghostscript
NEC PC-PR201	OpenPrintingPPDs-ghostscript
NEC PC-PR1000	OpenPrintingPPDs-ghostscript
NEC PC-PR2000	OpenPrintingPPDs-ghostscript
NEC PICTY180	OpenPrintingPPDs-ghostscript
NEC PinWriter P6	OpenPrintingPPDs-ghostscript
NEC PinWriter P6 plus	OpenPrintingPPDs-ghostscript
NEC PinWriter P7	OpenPrintingPPDs-ghostscript
NEC PinWriter P7 plus	OpenPrintingPPDs-ghostscript
NEC Pinwriter P20	OpenPrintingPPDs-ghostscript
NEC PinWriter P60	OpenPrintingPPDs-ghostscript
NEC PinWriter P70	OpenPrintingPPDs-ghostscript
NEC Silentwriter 95f	OpenPrintingPPDs-postscript
NEC SilentWriter LC 890	OpenPrintingPPDs-postscript
NEC Silentwriter2 model 290	OpenPrintingPPDs-postscript
NEC Silentwriter2 S60P	OpenPrintingPPDs-postscript
NEC SuperScript 100C	OpenPrintingPPDs-ghostscript
NEC SuperScript 150C	OpenPrintingPPDs-ghostscript
NEC SuperScript 650C	OpenPrintingPPDs-ghostscript
NEC SuperScript 660i	OpenPrintingPPDs-ghostscript
NEC SuperScript 660i	OpenPrintingPPDs-hpijs
NEC SuperScript 750C	OpenPrintingPPDs-ghostscript
NEC SuperScript 860	OpenPrintingPPDs-ghostscript
NEC SuperScript 870	OpenPrintingPPDs-ghostscript
NEC SuperScript 1260	OpenPrintingPPDs-ghostscript
NEC SuperScript 1400	OpenPrintingPPDs-ghostscript
NEC SuperScript 1400	OpenPrintingPPDs-hpijs
NEC SuperScript 1800	OpenPrintingPPDs-ghostscript
NEC SuperScript 1800	OpenPrintingPPDs-hpijs
NEC SuperScript 4600N	OpenPrintingPPDs-postscript

Печатающие устройства производства NRG

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG 10515/10518/10512 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 2205/2238/2212 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 2705/2738/2712 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 3205/3238/3212 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 3525/3508/3502 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 3545/3518/3532 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 4525/4508/4502 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 4545/4518/4532 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 6002/6005/6008 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 7502/7505/7508 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG 9005/9008/9002 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG C7010 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7116 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7416 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7425dn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7425hdn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7435n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7521n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7528n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG C7535hdn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG CC7417 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG CS555 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG DSc224 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc232 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc328 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc332 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc338 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc38 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc38u PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG DSc424 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG DSc428 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG DSc432 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG DSc435 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG DSc445 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG DSc460 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG DSm415 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm615 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm616 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm618 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm618d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm620 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm620d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm622 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm627 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG DSm632 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm635 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm645 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm651 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm660 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm675 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm725 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm730 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm735 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG DSm745 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG MP 161 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG MP 171 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG MP 201 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 301 PS3	OpenPrintingPPDs-postscript
NRG MP 1100 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG MP 1350 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG MP 1600 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG MP 2000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
NRG MP 2001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2500	gutenprint-ppd
NRG MP 2500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2510	gutenprint-ppd
NRG MP 2510 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2550	gutenprint-ppd
NRG MP 2550 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2550B	gutenprint-ppd
NRG MP 2550B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2553 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2851 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 2852 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3010	gutenprint-ppd
NRG MP 3010 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG MP 3053 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3350	gutenprint-ppd
NRG MP 3350 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3350B	gutenprint-ppd
NRG MP 3350B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3351 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3353 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 3500	gutenprint-ppd
NRG MP 3500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 4000	gutenprint-ppd
NRG MP 4000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 4000B	gutenprint-ppd
NRG MP 4000B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 4001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 4002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 4500	gutenprint-ppd
NRG MP 4500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 5000	gutenprint-ppd
NRG MP 5000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 5000B	gutenprint-ppd
NRG MP 5000B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 5001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 5002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 5500	gutenprint-ppd
NRG MP 5500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG MP 6000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 6001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 6002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 6500	gutenprint-ppd
NRG MP 6500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 7000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 7001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 7500	gutenprint-ppd
NRG MP 7500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 7502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 8000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 8001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 9000	gutenprint-ppd
NRG MP 9000 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 9001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP 9002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C300SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C305 PS3	OpenPrintingPPDs-postscript
NRG MP C400 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C400SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C1500sp PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG MP C2003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2003Z PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2050 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2051 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2503Z PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2550 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2551 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C2800 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3000 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C3503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C4000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C4500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C4501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG MP C4501A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C4502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C4502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C4503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C5000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C5501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C5501A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C5502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C5502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C5503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C6000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C6003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C6501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C6502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C7500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C7501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP C8002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG MP CW2200 PS3	OpenPrintingPPDs-postscript
NRG MP W2400 PS3	OpenPrintingPPDs-postscript
NRG MP W2401 PS3	OpenPrintingPPDs-postscript
NRG MP W3600 PS3	OpenPrintingPPDs-postscript
NRG MP W3601 PS3	OpenPrintingPPDs-postscript
NRG MP W5100 PS3	OpenPrintingPPDs-postscript
NRG MP W7140 PS3	OpenPrintingPPDs-postscript
NRG P7026 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG P7026N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7032 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7126 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7126N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7132N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7145 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7325 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7325N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7431cn PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7527 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7527n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7535n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG P7575 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG Pro 906EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 907EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 1106EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 1107EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 1356EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 1357EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 8100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 8110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro 8120S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
NRG Pro C5100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
NRG Pro C5110S PS3	OpenPrintingPPDs-ghostscript penPrintingPPDs-postscript
NRG SG3110DN	OpenPrintingPPDs-ghostscript
NRG SG3110DNw	OpenPrintingPPDs-ghostscript
NRG SG3110SFNw	OpenPrintingPPDs-ghostscript
NRG SP 4100N PS3	OpenPrintingPPDs-postscript
NRG SP 4100NL PS3	OpenPrintingPPDs-postscript
NRG SP 4110N PS3	OpenPrintingPPDs-postscript
NRG SP 4210N PS3	OpenPrintingPPDs-postscript
NRG SP 4310N PS3	OpenPrintingPPDs-postscript
NRG SP 5200DN PS3	OpenPrintingPPDs-postscript
NRG SP 5200S PS3	OpenPrintingPPDs-postscript
NRG SP 5210DN PS3	OpenPrintingPPDs-postscript
NRG SP 5210SF PS3	OpenPrintingPPDs-postscript
NRG SP 5210SR PS3	OpenPrintingPPDs-postscript
NRG SP 6330N PS3	OpenPrintingPPDs-postscript
NRG SP 8100DN PS3	OpenPrintingPPDs-postscript
NRG SP 8200DN PS3	OpenPrintingPPDs-postscript
NRG SP 8300DN PS3	OpenPrintingPPDs-postscript
NRG SP 9100DN PS3	OpenPrintingPPDs-postscript
NRG SP C320DN PS3	OpenPrintingPPDs-postscript
NRG SP C410DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG SP C411DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
NRG SP C420DN PS3	OpenPrintingPPDs-postscript
NRG SP C430DN PS3	OpenPrintingPPDs-postscript
NRG SP C431DN PS3	OpenPrintingPPDs-postscript
NRG SP C730DN PS3	OpenPrintingPPDs-postscript
NRG SP C811DN PS3	OpenPrintingPPDs-postscript
NRG SP C820DN PS3	OpenPrintingPPDs-postscript
NRG SP C821DN PS3	OpenPrintingPPDs-postscript
NRG SP C830DN PS3	OpenPrintingPPDs-postscript
NRG SP C831DN PS3	OpenPrintingPPDs-postscript
NRG SP W2470 PS3	OpenPrintingPPDs-postscript

Печатающие устройства производства Oce, Oki

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oce	
Oce 25C-1	OpenPrintingPPDs-postscript
Oce 3145	OpenPrintingPPDs-postscript
Oce 3155	OpenPrintingPPDs-postscript
Oce 3165	OpenPrintingPPDs-postscript
Oce 9050	OpenPrintingPPDs-ghostscript
Oce cm2510	OpenPrintingPPDs-postscript
Oce cm3521	OpenPrintingPPDs-postscript
Oce cm4010	OpenPrintingPPDs-postscript
Oce cm4520	OpenPrintingPPDs-postscript
Oce cm4521	OpenPrintingPPDs-postscript
Oce cm5520	OpenPrintingPPDs-postscript
Oce cm6520	OpenPrintingPPDs-postscript
Oce fx2080	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce fx3000	OpenPrintingPPDs-postscript
Oce im2330	OpenPrintingPPDs-postscript
Oce im2830	OpenPrintingPPDs-postscript
Oce im3512	OpenPrintingPPDs-postscript
Oce im3530	OpenPrintingPPDs-postscript
Oce im4512	OpenPrintingPPDs-postscript
Oce im4530	OpenPrintingPPDs-postscript
Oce im5530	OpenPrintingPPDs-postscript
Oce im6020	OpenPrintingPPDs-postscript
Oce im6030	OpenPrintingPPDs-postscript
Oce im7230	OpenPrintingPPDs-postscript
Oce im7520	OpenPrintingPPDs-postscript
Oce im8530	OpenPrintingPPDs-postscript
Oce im9220	OpenPrintingPPDs-postscript
Oce 3145	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce 3155	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce 3165	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce 8445	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce 8465	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce 9230	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oce 9245	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce 9260	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 3073	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 3074	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 3093	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 3094	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 3113	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 3114	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 5115	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce PPC for 5160	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce VarioPrint 2045	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce VarioPrint 2050	manufacturer-PPDs OpenPrintingPPDs-ghostscript
Oce VarioPrint 2050	OpenPrintingPPDs-postscript
Oce VarioPrint 2055	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce VarioPrint 2060	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce VarioPrint 2065	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce VarioPrint 2070	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce VarioPrint 2090 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce VarioPrint 2100 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce VarioPrint 2110 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Oce VP2105 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oce PPC3073	OpenPrintingPPDs-postscript
Oce PPC3074	OpenPrintingPPDs-postscript
Oce PPC3093	OpenPrintingPPDs-postscript
Oce PPC3094	OpenPrintingPPDs-postscript
Oce PPC3113	OpenPrintingPPDs-postscript
Oce PPC3114	OpenPrintingPPDs-postscript
Oce PPC5115	OpenPrintingPPDs-postscript
Oce PPC5160	OpenPrintingPPDs-postscript
Oce sx1480	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oce sx2100	OpenPrintingPPDs-postscript
Oce VarioPrint 2045	OpenPrintingPPDs-postscript
Oce VarioPrint 2055	OpenPrintingPPDs-postscript
Oce VarioPrint 2065	OpenPrintingPPDs-postscript
Oce VarioPrint 2100	OpenPrintingPPDs-postscript
Oce VarioPrint 2110	OpenPrintingPPDs-postscript
Oki	
Oki B401d	gutenprint-ppd
Oki B410	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Oki B430	gutenprint-ppd
Oki B2400	OpenPrintingPPDs-ghostscript
Oki B2540 MFP	OpenPrintingPPDs-postscript
Oki B4200	OpenPrintingPPDs-ghostscript
Oki B4250	OpenPrintingPPDs-ghostscript
Oki B4300	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki B4350	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Oki B4400	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Oki B4545 MFP	OpenPrintingPPDs-postscript
Oki B4600	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Oki B4600 PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki B6200	OpenPrintingPPDs-postscript
Oki B6250	OpenPrintingPPDs-postscript
Oki B6300	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki B6500	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oki B8300	manufacturer-PPDs
Oki-C110	foo2zjs
Oki-C301dn	foo2zjs
Oki-C310dn	foo2zjs
Oki-C511dn	foo2zjs
Oki C710	OpenPrintingPPDs-postscript
Oki-C810	foo2zjs
Oki-C3100	foo2zjs
Oki-C3200	foo2zjs
Oki-C3300	foo2zjs
Oki-C3400	foo2zjs
Oki-C3530 MFP	foo2zjs
Oki-C5100	foo2zjs
Oki-C5200	foo2zjs
Oki C5300	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Oki C5400	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Oki C5450	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki-C5500	foo2zjs OpenPrintingPPDs-postscript
Oki-C5600	foo2zjs
Oki-C5650	foo2zjs
Oki C5700	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C5750	OpenPrintingPPDs-postscript
Oki-C5800	foo2zjs
Oki C5900	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C6000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C6050	OpenPrintingPPDs-postscript
Oki C6100	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C6150	OpenPrintingPPDs-postscript
Oki C7100	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C7200	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oki C7300	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Oki C7350	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C7400	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C7500	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C7550	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C8800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C9200	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Oki C9300	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C9400	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Oki C9500	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C9600	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki C9650	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C9800	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Oki C9800 MFP	OpenPrintingPPDs-postscript
Oki DP 5000	OpenPrintingPPDs-ghostscript
Oki Microline 18NR	manufacturer-PPDs
Oki Microline 22NR	manufacturer-PPDs
Oki Microline 182	OpenPrintingPPDs-ghostscript
Oki Microline 192+	OpenPrintingPPDs-ghostscript
Oki Microline 600CL	OpenPrintingPPDs-ghostscript
Oki Microline 620CL	OpenPrintingPPDs-ghostscript
Oki Microline 1032PS	manufacturer-PPDs
Oki Microline 1035PS	manufacturer-PPDs
Oki Microline 1055PS	manufacturer-PPDs
Oki Microline 2020/N	manufacturer-PPDs
Oki Microline 2030N	manufacturer-PPDs

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oki Microline 3010c	manufacturer-PPDs
Oki Microline 3020c	manufacturer-PPDs
Oki Microline 3020cV	manufacturer-PPDs
Oki Microline 3050c	manufacturer-PPDs
Oki Microline 3050cV	manufacturer-PPDs
Oki Microline 5300	manufacturer-PPDs
Oki Microline 5400	manufacturer-PPDs
Oki Microline 7300PS	manufacturer-PPDs
Oki Microline 9055c	manufacturer-PPDs
Oki Microline 9055cV	manufacturer-PPDs
Oki Microline 9300PS	manufacturer-PPDs
Oki Microline 9500PS	manufacturer-PPDs
Oki Microline 9500PS-F	manufacturer-PPDs
Oki Microline IBM compatible 9 pin	OpenPrintingPPDs-ghostscript
Oki ML 321	OpenPrintingPPDs-ghostscript
Oki ML 380	OpenPrintingPPDs-ghostscript
Oki ML320/1TURBO	OpenPrintingPPDs-ghostscript
Oki ML703N3	manufacturer-PPDs
Oki ML802PSII	manufacturer-PPDs
Oki ML803PSII	manufacturer-PPDs
Oki ML803PSIIV	manufacturer-PPDs
Oki ML905PSIII	manufacturer-PPDs
Oki Okijet 2500	OpenPrintingPPDs-ghostscript
OKI Okipage 4w	OpenPrintingPPDs-ghostscript
Oki Okipage 4w+	OpenPrintingPPDs-ghostscript
Oki Okipage 6e	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki Okipage 6ex	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki Okipage 6w	OpenPrintingPPDs-ghostscript
Oki Okipage 8c	OpenPrintingPPDs-postscript
Oki Okipage 8p	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki Okipage 8w	OpenPrintingPPDs-ghostscript
Oki Okipage 8w Lite	OpenPrintingPPDs-ghostscript
Oki Okipage 8z	OpenPrintingPPDs-ghostscript
Oki Okipage 10e	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki Okipage 10ex	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Oki Okipage 12i	OpenPrintingPPDs-postscript
Oki Okipage 14ex	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki Okipage 14i	manufacturer-PPDs OpenPrintingPPDs-postscript
Oki Okipage 20DXn	OpenPrintingPPDs-postscript
Oki OL400	OpenPrintingPPDs-ghostscript gutenprint-ppd
Oki OL400e	OpenPrintingPPDs-ghostscript gutenprint-ppd
Oki OL400ex	OpenPrintingPPDs-ghostscript gutenprint-ppd
Oki OL400w	OpenPrintingPPDs-ghostscript
Oki OL410e	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki OL600e	OpenPrintingPPDs-ghostscript gutenprint-ppd
Oki OL610e/PS	OpenPrintingPPDs-postscript
Oki OL610e/S	OpenPrintingPPDs-ghostscript gutenprint-ppd
Oki OL800	OpenPrintingPPDs-ghostscript gutenprint-ppd
Oki OL810e/PS	OpenPrintingPPDs-postscript
Oki OL810ex	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Oki OL830Plus	OpenPrintingPPDs-postscript
Oki Super 6e	gutenprint-ppd

Печатающие устройства производства Olivetti, Olympus, Panasonic, Pantum, PCPI, QMS, Raven

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Olivetti	
Olivetti d-Color P160W	foo2zjs
Olivetti JP350S	OpenPrintingPPDs-ghostscript gutenprint-ppd
Olivetti JP450	OpenPrintingPPDs-ghostscript
Olivetti JP470	OpenPrintingPPDs-ghostscript
Olivetti PG 306	OpenPrintingPPDs-ghostscript gutenprint-ppd
Olympus	
Olympus P-10	gutenprint-ppd
Olympus P-11	gutenprint-ppd
Olympus P-200	gutenprint-ppd
Olympus P-300	gutenprint-ppd
Olympus P-300E	gutenprint-ppd
Olympus P-300U	gutenprint-ppd
Olympus P-330E	gutenprint-ppd
Olympus P-330NE	gutenprint-ppd
Olympus P-400	gutenprint-ppd
Olympus P-440	gutenprint-ppd
Olympus P-S100	gutenprint-ppd
Panasonic	
Panasonic DP-180	OpenPrintingPPDs-ghostscript
Panasonic DP-2330	OpenPrintingPPDs-ghostscript
Panasonic DP-4510	OpenPrintingPPDs-ghostscript
Panasonic DP-4520	OpenPrintingPPDs-ghostscript
Panasonic DP-8016P	OpenPrintingPPDs-ghostscript
Panasonic DP-8020E	OpenPrintingPPDs-ghostscript
Panasonic DP-8045	OpenPrintingPPDs-ghostscript
Panasonic DP-8060	OpenPrintingPPDs-ghostscript
Panasonic DP-C213	OpenPrintingPPDs-ghostscript
Panasonic DP-C262	OpenPrintingPPDs-ghostscript
Panasonic DP-C264	OpenPrintingPPDs-ghostscript
Panasonic DP-C265	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Panasonic DP-C305	OpenPrintingPPDs-ghostscript
Panasonic DP-C322	OpenPrintingPPDs-ghostscript
Panasonic DP-C354	OpenPrintingPPDs-ghostscript
Panasonic DP-C405	OpenPrintingPPDs-ghostscript
Panasonic KX-P1123	OpenPrintingPPDs-ghostscript
Panasonic KX-P1124	OpenPrintingPPDs-ghostscript
Panasonic KX-P1150	OpenPrintingPPDs-ghostscript
Panasonic KX-P1624	OpenPrintingPPDs-ghostscript
Panasonic KX-P2023	OpenPrintingPPDs-ghostscript
Panasonic KX-P2123	OpenPrintingPPDs-ghostscript
Panasonic KX-P2135	OpenPrintingPPDs-ghostscript
Panasonic KX-P2150	OpenPrintingPPDs-ghostscript
Panasonic KX-P4410	OpenPrintingPPDs-ghostscript gutenprint-ppd
Panasonic KX-P4450	OpenPrintingPPDs-ghostscript gutenprint-ppd
Panasonic KX-P5400	OpenPrintingPPDs-postscript
Panasonic KX-P6150	OpenPrintingPPDs-ghostscript gutenprint-ppd
Panasonic KX-P6500	OpenPrintingPPDs-ghostscript gutenprint-ppd
Panasonic KX-P8420	OpenPrintingPPDs-postscript
Panasonic KX-P8475	OpenPrintingPPDs-postscript
Pantum	
Pantum CM7000DN/FDN series	
Pantum CP2500DN Series	
Pantum M5100/5200/5300 all Series	
Pantum M6200/6500/6550/6600/6700/6760/6800/6860 all Series	
Pantum M7100/7160/7200/7300/7600 all Series	
Pantum MS6000/6550/6600 all Series	
Pantum P1000 all Series	
Pantum P2000/2200/2500/2550/2600/2650 all Series	
Pantum P3000/3010/3060/3100/3300/3307/3500/3508 all Series	
Pantum P4000 all Series	
Pantum P5000 all Series	
Pantum P9500DN series	

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Pantum S2000 Series	
PCPI	
PCPI 1030	OpenPrintingPPDs-ghostscript gutenprint-ppd
QMS	
QMS 2425 Turbo EX	OpenPrintingPPDs-postscript
QMS LPK-100	OpenPrintingPPDs-ghostscript
QMS magicolor 2+	OpenPrintingPPDs-postscript
QMS ps-810	OpenPrintingPPDs-postscript
Raven	
Raven LP-410	OpenPrintingPPDs-ghostscript gutenprint-ppd

Печатающие устройства производства Ricoh

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh 4081	OpenPrintingPPDs-ghostscript
Ricoh 4801	OpenPrintingPPDs-ghostscript
Ricoh 6000	OpenPrintingPPDs-ghostscript
Ricoh Aficio 220	OpenPrintingPPDs-ghostscript
Ricoh Aficio 220	OpenPrintingPPDs-hpijs
Ricoh Aficio 401	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Ricoh Aficio 700	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Ricoh Aficio 5206	OpenPrintingPPDs-postscript
Ricoh Aficio AP2000	OpenPrintingPPDs-postscript
Ricoh Aficio SP C222SF	OpenPrintingPPDs-postscript
Ricoh DDP 70	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh DDP 92	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh EMP156	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh GelSprinter GX 3050N	OpenPrintingPPDs-ghostscript
Ricoh GelSprinter GX 3050SFN	OpenPrintingPPDs-ghostscript
Ricoh GelSprinter GX 5050N	OpenPrintingPPDs-ghostscript
Ricoh GelSprinter GX e3350N	OpenPrintingPPDs-ghostscript
Ricoh GelSprinter GX e5550N	OpenPrintingPPDs-ghostscript
Ricoh Aficio 401	gutenprint-ppd
Ricoh Aficio 700	gutenprint-ppd
Ricoh Aficio 1022	gutenprint-ppd
Ricoh Aficio 1022 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1027	gutenprint-ppd
Ricoh Aficio 1027 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1032	gutenprint-ppd
Ricoh Aficio 1032 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1035	gutenprint-ppd
Ricoh Aficio 1035 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1045	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio 1045 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1060	gutenprint-ppd
Ricoh Aficio 1060 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1075	gutenprint-ppd
Ricoh Aficio 1075 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 1224C PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio 1232C PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio 1515	gutenprint-ppd
Ricoh Aficio 1515 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2015	gutenprint-ppd
Ricoh Aficio 2015 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2016	gutenprint-ppd
Ricoh Aficio 2016 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2018	gutenprint-ppd
Ricoh Aficio 2018 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2018D	gutenprint-ppd
Ricoh Aficio 2018D PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2020	gutenprint-ppd
Ricoh Aficio 2020 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2020D	gutenprint-ppd
Ricoh Aficio 2020D PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2022	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio 2022 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2027	gutenprint-ppd
Ricoh Aficio 2027 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2032	gutenprint-ppd
Ricoh Aficio 2032 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2035	gutenprint-ppd
Ricoh Aficio 2035 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2035e	gutenprint-ppd
Ricoh Aficio 2035e PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2045	gutenprint-ppd
Ricoh Aficio 2045 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2045e	gutenprint-ppd
Ricoh Aficio 2045e PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2051	gutenprint-ppd
Ricoh Aficio 2051 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2060	gutenprint-ppd
Ricoh Aficio 2060 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2075	gutenprint-ppd
Ricoh Aficio 2075 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2090	gutenprint-ppd
Ricoh Aficio 2090 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 2105	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio 2105 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 220	gutenprint-ppd
Ricoh Aficio 2228C PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio 2232C PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio 2238C PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio 3025	gutenprint-ppd
Ricoh Aficio 3025 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3030	gutenprint-ppd
Ricoh Aficio 3030 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3035	gutenprint-ppd
Ricoh Aficio 3035 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3045	gutenprint-ppd
Ricoh Aficio 3045 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3224C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3228C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3232C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3235C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3245C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio 3260C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio AP2600 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio AP2600N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP2610 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP2610N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP3200 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP3800C PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP400 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP400N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP410 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP410N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP4510 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP600N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP610N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio AP900 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL1000N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL2000 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL3000 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL3000e PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL3100 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL3500N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL4000DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL4000HDN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL5000 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio CL7000 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL7100 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL7200 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio CL7300 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio Color5560 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 1100	gutenprint-ppd
Ricoh Aficio MP 1100 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 1350	gutenprint-ppd
Ricoh Aficio MP 1350 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 1600	gutenprint-ppd
Ricoh Aficio MP 1600 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 161	gutenprint-ppd
Ricoh Aficio MP 161 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 171 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2000	gutenprint-ppd
Ricoh Aficio MP 2000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 201 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2500	gutenprint-ppd
Ricoh Aficio MP 2500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2510	gutenprint-ppd
Ricoh Aficio MP 2510 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2550	gutenprint-ppd
Ricoh Aficio MP 2550 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2550B	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio MP 2550B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2851 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 2852 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 301 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP 3010	gutenprint-ppd
Ricoh Aficio MP 3010 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 3350	gutenprint-ppd
Ricoh Aficio MP 3350 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 3350B	gutenprint-ppd
Ricoh Aficio MP 3350B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 3351 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 3352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 3500	gutenprint-ppd
Ricoh Aficio MP 3500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 4000	gutenprint-ppd
Ricoh Aficio MP 4000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 4000B	gutenprint-ppd
Ricoh Aficio MP 4000B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 4001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 4002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 4500	gutenprint-ppd
Ricoh Aficio MP 4500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 5000	gutenprint-ppd
Ricoh Aficio MP 5000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 5000B	gutenprint-ppd
Ricoh Aficio MP 5000B PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 5001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio MP 5002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 5500	gutenprint-ppd
Ricoh Aficio MP 5500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 6000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 6001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 6002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 6500	gutenprint-ppd
Ricoh Aficio MP 6500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 7000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 7001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 7500	gutenprint-ppd
Ricoh Aficio MP 7500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 7502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 8000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 8001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 9000	gutenprint-ppd
Ricoh Aficio MP 9000 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 9001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP 9002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C2050 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C2051 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C2500 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio MP C2550 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C2551 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C2800 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C3000 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C3001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C3002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C300SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C305 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP C3300 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C3500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C3501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C3502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C400 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C4000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C400SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C4500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C4501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C4501A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C4502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C4502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C5000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C5501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio MP C5501A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C5502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C5502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C6000 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C6501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C7500 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP C7501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Aficio MP W2400 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP W2401 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP W3600 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP W3601 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP W5100 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio MP W7140 PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SG3110DN	OpenPrintingPPDs-ghostscript
Ricoh Aficio SG3110DNw	OpenPrintingPPDs-ghostscript
Ricoh Aficio SG3110SFNw	OpenPrintingPPDs-ghostscript
Ricoh Aficio SP 4100N PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 4100NL PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 4110N PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 4210N PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 4310N PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 5200DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 5200S PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 5210DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 5210SF PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 5210SR PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 6330N PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 8100DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 8200DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 8300DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP 9100DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C320DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C400DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C410DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio SP C411DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh Aficio SP C420DN PS3	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh Aficio SP C430DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C431DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C730DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C811DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C820DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C821DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C830DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP C831DN PS3	OpenPrintingPPDs-postscript
Ricoh Aficio SP W2470 PS3	OpenPrintingPPDs-postscript
Ricoh ColorLaser AP828 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh FAX5510L/5510NF PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh LASER AP2600 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh LASER AP2600N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh LASER AP2610 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh LASER AP2610N PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Ricoh MP 2001 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP 2501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP 2553 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP 3053 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP 3353 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C1500/615C PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C2003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C2003Z PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C2503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C2503Z PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C3003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Ricoh MP C3503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C4503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C5503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C6003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C6502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP C8002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh MP CW2200 PS3	OpenPrintingPPDs-postscript
Ricoh Pro 1106EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 1107EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 1356EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 1357EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 8100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 8110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 8120S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 906EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro 907EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro C5100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh Pro C5110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Ricoh SG3120BSFNw	OpenPrintingPPDs-ghostscript
Ricoh SP 112	foo2zjs
Ricoh SP 201Nw	foo2zjs
Ricoh RPDL I Laser Printer	OpenPrintingPPDs-ghostscript
Ricoh RPDL II Laser Printer	OpenPrintingPPDs-ghostscript
Ricoh RPDL III Laser Printer	OpenPrintingPPDs-ghostscript
Ricoh RPDL IV Laser Printer	OpenPrintingPPDs-ghostscript

Печатающие устройства производства Samsung

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Samsung 6050	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Samsung CLP-300	foo2zjs
Samsung CLP-310	foo2zjs
Samsung CLP-315	foo2zjs
Samsung CLP-325	foo2zjs
Samsung CLP-350 Series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-365	foo2zjs
Samsung CLP-410 Series	OpenPrintingPPDs-postscript
Samsung CLP-550	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-550N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-600	foo2zjs
Samsung CLP-610 Series	foo2zjs OpenPrintingPPDs-ghostscript
Samsung CLP-620 Series	foo2zjs OpenPrintingPPDs-ghostscript
Samsung CLP-650	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-650N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-660 Series	OpenPrintingPPDs-postscript
Samsung CLP-660N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-660ND	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung CLP-670 Series	OpenPrintingPPDs-postscript
Samsung CLP-680 Series	OpenPrintingPPDs-postscript
Samsung CLP-770 Series	OpenPrintingPPDs-postscript
Samsung CLP-775 Series	OpenPrintingPPDs-postscript
Samsung CLX-2160	foo2zjs
Samsung CLX-3160	foo2zjs
Samsung CLX-3175	foo2zjs
Samsung CLX-3185	foo2zjs
Samsung CLX-3300 Series	OpenPrintingPPDs-postscript
Samsung CLX-4190 Series	OpenPrintingPPDs-postscript
Samsung CLX-6200 Series	OpenPrintingPPDs-postscript
Samsung CLX-6220 Series	OpenPrintingPPDs-postscript
Samsung CLX-6240 Series	OpenPrintingPPDs-postscript
Samsung CLX-6250 Series	OpenPrintingPPDs-postscript
Samsung CLX-6260 Series	OpenPrintingPPDs-postscript
Samsung CLX-8380 Series	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Samsung CLX-8385 Series	OpenPrintingPPDs-postscript
Samsung CLX-8385X Series	OpenPrintingPPDs-postscript
Samsung CLX-8540 Series	OpenPrintingPPDs-postscript
Samsung CLX-8640 8650 Series	OpenPrintingPPDs-postscript
Samsung CLX-9250 9350 Series	OpenPrintingPPDs-postscript
Samsung CLX-9252 9352 Series	OpenPrintingPPDs-postscript
Samsung CLX-92x1 93x1 Series	OpenPrintingPPDs-postscript
Samsung CLX-981x Series	OpenPrintingPPDs-postscript
Samsung CLX-982x Series	OpenPrintingPPDs-postscript
Samsung M262x 282x Series	OpenPrintingPPDs-ghostscript
Samsung M267x 287x Series	OpenPrintingPPDs-ghostscript
Samsung M332x 382x 402x Series	OpenPrintingPPDs-postscript
Samsung M337x 387x 407x Series	OpenPrintingPPDs-postscript
Samsung ML-85	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-200	OpenPrintingPPDs-ghostscript
Samsung ML-210	OpenPrintingPPDs-ghostscript
Samsung ML-1000	OpenPrintingPPDs-ghostscript
Samsung ML-1010	OpenPrintingPPDs-ghostscript
Samsung ML-1020	OpenPrintingPPDs-ghostscript
Samsung ML-1200	OpenPrintingPPDs-ghostscript
Samsung ML-1210	OpenPrintingPPDs-ghostscript
Samsung ML-1220	OpenPrintingPPDs-ghostscript
Samsung ML-1250	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-1410	OpenPrintingPPDs-ghostscript
Samsung ML-1430	OpenPrintingPPDs-ghostscript
Samsung ML-1440	OpenPrintingPPDs-ghostscript
Samsung ML-1450	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-1450PS	gutenprint-ppd
Samsung ML-1450PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-1450PS	OpenPrintingPPDs-postscript
Samsung ML-1510_700	OpenPrintingPPDs-ghostscript
Samsung ML-1520	OpenPrintingPPDs-ghostscript
Samsung ML-1610	OpenPrintingPPDs-ghostscript
Samsung ML-1650	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Samsung ML-1651N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-1710	OpenPrintingPPDs-ghostscript
Samsung ML-1740	OpenPrintingPPDs-ghostscript
Samsung ML-1750	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-2010	OpenPrintingPPDs-ghostscript
Samsung ML-2150	OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2150 Series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Samsung ML-2150PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2151N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-2151NPS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2152W	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-2152WPS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2250	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2550 Series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2551N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Samsung ML-2552W	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-2570 Series	OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Samsung ML-2571N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-2580 Series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-2850D	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-2851ND	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-2853 Series	OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript OpenPrintingPPDs-ghostscript
Samsung ML-3051N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-3051ND	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-3470 Series	OpenPrintingPPDs-postscript
Samsung ML-3470D	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-3471ND	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-3475 Series	OpenPrintingPPDs-postscript
Samsung ML-371x Series	OpenPrintingPPDs-postscript
Samsung ML-375x Series	OpenPrintingPPDs-postscript
Samsung ML-4050 Series	OpenPrintingPPDs-postscript
Samsung ML-4050N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-4055 Series	OpenPrintingPPDs-postscript
Samsung ML-4500	OpenPrintingPPDs-ghostscript
Samsung ML-451x 501x Series	OpenPrintingPPDs-postscript
Samsung ML-4550 Series	OpenPrintingPPDs-postscript
Samsung ML-4551N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-4551ND	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-4555 Series	OpenPrintingPPDs-postscript
Samsung ML-4600	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Samsung ML-5000a	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-5080	OpenPrintingPPDs-ghostscript
Samsung ML-551x 651x Series	OpenPrintingPPDs-postscript
Samsung ML-6000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-6040	OpenPrintingPPDs-ghostscript
Samsung ML-6060	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Samsung ML-6060N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-6060S	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Samsung ML-6100	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-7000	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-7000N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-7000P	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-7050	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung ML-7300	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-7300N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Samsung ML-8850 8950 Series	OpenPrintingPPDs-postscript
Samsung ML-8x00 Series	OpenPrintingPPDs-postscript
Samsung QL-5100A	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Samsung QL-6050	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Samsung SCX-470x Series	OpenPrintingPPDs-ghostscript
Samsung SCX-472x Series	OpenPrintingPPDs-ghostscript
Samsung SCX-483x 5x3x Series	OpenPrintingPPDs-postscript
Samsung SCX-4x24 Series	OpenPrintingPPDs-ghostscript
Samsung SCX-4x25 Series	OpenPrintingPPDs-ghostscript
Samsung SCX-4x26 Series	OpenPrintingPPDs-ghostscript
Samsung SCX-4x28 Series	OpenPrintingPPDs-postscript
Samsung SCX-5635 Series	OpenPrintingPPDs-postscript
Samsung SCX-5835 5935 5935X Series	OpenPrintingPPDs-postscript
Samsung SCX-6545 6545X Series	OpenPrintingPPDs-postscript
Samsung SCX-681x Series	OpenPrintingPPDs-postscript
Samsung SCX-6x45 Series	OpenPrintingPPDs-postscript
Samsung SCX-6x55 Series	OpenPrintingPPDs-postscript
Samsung SCX-6x55X Series	OpenPrintingPPDs-postscript
Samsung SCX-8030 8040 Series	OpenPrintingPPDs-postscript
Samsung SCX-8123 8128 Series	OpenPrintingPPDs-postscript
Samsung SCX-8230 8240 Series	OpenPrintingPPDs-postscript
Samsung SCX-881x Series	OpenPrintingPPDs-postscript
Samsung SCX-882x Series	OpenPrintingPPDs-postscript
Samsung SI-630A	OpenPrintingPPDs-ghostscript

Печатающие устройства производства Savin

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin 816	gutenprint-ppd
Savin 816 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 917 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 920 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2404WD PS3	OpenPrintingPPDs-postscript
Savin 2404WDP PS3	OpenPrintingPPDs-postscript
Savin 2406WD PS3	OpenPrintingPPDs-postscript
Savin 2522	gutenprint-ppd
Savin 2522 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2527	gutenprint-ppd
Savin 2527 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2532	gutenprint-ppd
Savin 2532 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2535/2235	gutenprint-ppd
Savin 2535/2235 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2545/2245	gutenprint-ppd
Savin 2545/2245 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2560	gutenprint-ppd
Savin 2560 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 2575	gutenprint-ppd
Savin 2575 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 3406WD PS3	OpenPrintingPPDs-postscript
Savin 3515	gutenprint-ppd
Savin 3515 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 40105	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin 40105 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4015	gutenprint-ppd
Savin 4015 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4018	gutenprint-ppd
Savin 4018 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4018d	gutenprint-ppd
Savin 4018d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4022	gutenprint-ppd
Savin 4022 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4027	gutenprint-ppd
Savin 4027 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4035/4135g	gutenprint-ppd
Savin 4035/4135g PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4035e/4135eG	gutenprint-ppd
Savin 4035e/4135eG PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4045/4145g	gutenprint-ppd
Savin 4045/4145g PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4045e/4145eG	gutenprint-ppd
Savin 4045e/4145eG PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4051	gutenprint-ppd
Savin 4051 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4060	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin 4060 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4075	gutenprint-ppd
Savin 4075 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 4090	gutenprint-ppd
Savin 4090 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 5100WD PS3	OpenPrintingPPDs-postscript
Savin 7025	gutenprint-ppd
Savin 7025 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 7140WD PS3	OpenPrintingPPDs-postscript
Savin 8016	gutenprint-ppd
Savin 8016 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8020	gutenprint-ppd
Savin 8020 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8020d	gutenprint-ppd
Savin 8020d PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8025	gutenprint-ppd
Savin 8025 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8025e	gutenprint-ppd
Savin 8025e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8030	gutenprint-ppd
Savin 8030 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8030e	gutenprint-ppd
Savin 8030e PS3	OpenPrintingPPDs-ghostscript
Savin 8030e PS3	OpenPrintingPPDs-postscript
Savin 8035/8035g	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin 8035/8035g PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8035e	gutenprint-ppd
Savin 8035e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8045/8045g	gutenprint-ppd
Savin 8045/8045g PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8045e	gutenprint-ppd
Savin 8045e PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8055	gutenprint-ppd
Savin 8055 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8060 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8065	gutenprint-ppd
Savin 8065 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8070 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8075	gutenprint-ppd
Savin 8075 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8080 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8090	gutenprint-ppd
Savin 8090 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8110	gutenprint-ppd
Savin 8110 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 8135	gutenprint-ppd
Savin 8135 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9016	gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin 9016 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9021d	gutenprint-ppd
Savin 9021d PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9025	gutenprint-ppd
Savin 9025 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9025b	gutenprint-ppd
Savin 9025b PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9033	gutenprint-ppd
Savin 9033 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9033b	gutenprint-ppd
Savin 9033b PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9040	gutenprint-ppd
Savin 9040 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9040b	gutenprint-ppd
Savin 9040b PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9050	gutenprint-ppd
Savin 9050 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9050b	gutenprint-ppd
Savin 9050b PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9060 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9070 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9080 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9090 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9228 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9233 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9240 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin 9250 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin C 230 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C 230SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C 240 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C 240SR PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C2408 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C2410 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C2524 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C2525 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C2532 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C2820 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C2824 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C2828 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C3030 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C3210 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C3210e PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C3224 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C3333 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C3528 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C3535 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin C3828 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin C4040 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C4535 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C4540 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C5050 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C6045 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C6055 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C7570 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9020 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9025 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9065 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9075 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9120 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9125 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9130 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9135 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9145 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9145A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9155 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin C9155A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin CLP1036 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP128 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin CLP131DN PS3	OpenPrintingPPDs-postscript
Savin CLP135 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP1620 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP17 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP18 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP22 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP240D PS3	OpenPrintingPPDs-postscript
Savin CLP26DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP27DN PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP28 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP31DN PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin CLP35 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin CLP350D PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin CLP42DN PS3	OpenPrintingPPDs-postscript
Savin CLP831 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin FAX3799/3799nf PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP145 PS3	OpenPrintingPPDs-postscript
Savin MLP150DN PS3	OpenPrintingPPDs-postscript
Savin MLP175n PS3	OpenPrintingPPDs-postscript OpenPrintingPPDs-postscript
Savin MLP25 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP25n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP26 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP26n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP28 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin MLP28n PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MLP31nL PS3	OpenPrintingPPDs-postscript
Savin MLP32 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP35n PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MLP37N PS3	OpenPrintingPPDs-postscript
Savin MLP45 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MLP75n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin MP 2352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 2501 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 2553 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 2852 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 301 PS3	OpenPrintingPPDs-postscript
Savin MP 3053 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 3352 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 3353 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 4002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 5002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 6002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 7502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP 9002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C305 PS3	OpenPrintingPPDs-postscript
Savin MP C2003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C2503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C3002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin MP C3003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C3502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C3503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C4502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C4502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C4503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C5502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C5502A PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C5503 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C6003 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C6502 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP C8002 PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin MP CW2200 PS3	OpenPrintingPPDs-postscript
Savin Pro 1106EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 1107EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 1356EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 1357EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 8100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 8110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 8120S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 906EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro 907EX PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin Pro C5100S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Savin Pro C5110S PS3	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin SDC555 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin SG3110DN	OpenPrintingPPDs-ghostscript
Savin SG3110DNw	OpenPrintingPPDs-ghostscript
Savin SG3110SFNw	OpenPrintingPPDs-ghostscript
Savin SGC 1506 PS3	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Savin SLP26 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin SLP26n PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin SLP32 PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin SLP38c PS3	manufacturer-PPDs OpenPrintingPPDs-postscript
Savin SP 4310N PS3	OpenPrintingPPDs-postscript
Savin SP 5200DN PS3	OpenPrintingPPDs-postscript
Savin SP 5200S PS3	OpenPrintingPPDs-postscript
Savin SP 5210DN PS3	OpenPrintingPPDs-postscript
Savin SP 5210SF PS3	OpenPrintingPPDs-postscript
Savin SP 5210SR PS3	OpenPrintingPPDs-postscript
Savin SP 8300DN PS3	OpenPrintingPPDs-postscript
Savin SP C320DN PS3	OpenPrintingPPDs-postscript
Savin SP C400DN PS3	OpenPrintingPPDs-postscript
Savin SP C730DN PS3	OpenPrintingPPDs-postscript
Savin SP C830DN PS3	OpenPrintingPPDs-postscript
Savin SP C831DN PS3	OpenPrintingPPDs-postscript

Печатающие устройства производства Seiko, Shinko, Sinfonia, SiPix, Sony

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Seiko	
Seiko SpeedJET 200	OpenPrintingPPDs-ghostscript gutenprint-ppd
Shinko	
Shinko CHC-S1245	gutenprint-ppd
Shinko CHC-S2145	gutenprint-ppd
Shinko CHC-S6145	gutenprint-ppd
Shinko CHC-S6245	gutenprint-ppd
Shinko CHC-S9045	gutenprint-ppd
Sinfonia	
Sinfonia CHC-S1245/E1	gutenprint-ppd
Sinfonia CHC-S6145/CS2	gutenprint-ppd
Sinfonia CHC-S6245/CE1	gutenprint-ppd
Sinfonia S2145/S2	gutenprint-ppd
SiPix	
SiPix Pocket Printer A6	OpenPrintingPPDs-ghostscript
Sony	
Sony All-in-One IJP-V100	OpenPrintingPPDs-hpijs
Sony DPP-EX5	gutenprint-ppd
Sony DPP-EX7	gutenprint-ppd
Sony IJP-V100	gutenprint-ppd
Sony UP-CR10L	gutenprint-ppd
Sony UP-DP10	gutenprint-ppd
Sony UP-DR100	gutenprint-ppd
Sony UP-DR150	gutenprint-ppd
Sony UP-DR200	gutenprint-ppd

Печатающие устройства производства Sharp

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Sharp AJ-1800	OpenPrintingPPDs-ghostscript
Sharp AJ-1805	OpenPrintingPPDs-ghostscript
Sharp AJ-2000	OpenPrintingPPDs-ghostscript
Sharp AJ-2005	OpenPrintingPPDs-ghostscript
Sharp AR-155FG	OpenPrintingPPDs-ghostscript
Sharp AR-155FG PS	OpenPrintingPPDs-postscript
Sharp AR-160/200 series	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Sharp AR-160M	OpenPrintingPPDs-ghostscript
Sharp AR-160M PS	OpenPrintingPPDs-postscript
Sharp AR-161	gutenprint-ppd
Sharp AR-163FG	OpenPrintingPPDs-ghostscript
Sharp AR-163FG PS	OpenPrintingPPDs-postscript
Sharp AR-163G	OpenPrintingPPDs-ghostscript
Sharp AR-163G PS	OpenPrintingPPDs-postscript
Sharp AR-200M	OpenPrintingPPDs-ghostscript
Sharp AR-200M PS	OpenPrintingPPDs-postscript
Sharp AR-205FG	OpenPrintingPPDs-ghostscript
Sharp AR-205FG PS	OpenPrintingPPDs-postscript
Sharp AR-205G	OpenPrintingPPDs-ghostscript
Sharp AR-205G PS	OpenPrintingPPDs-postscript
Sharp AR-266FP	OpenPrintingPPDs-ghostscript
Sharp AR-266FP PS	OpenPrintingPPDs-postscript
Sharp AR-266S	OpenPrintingPPDs-ghostscript
Sharp AR-266S PS	OpenPrintingPPDs-postscript
Sharp AR-311FP	OpenPrintingPPDs-ghostscript
Sharp AR-311FP PS	OpenPrintingPPDs-postscript
Sharp AR-311N	OpenPrintingPPDs-ghostscript
Sharp AR-311N PS	OpenPrintingPPDs-postscript
Sharp AR-311S	OpenPrintingPPDs-ghostscript
Sharp AR-311S PS	OpenPrintingPPDs-postscript
Sharp AR-351FP	OpenPrintingPPDs-ghostscript
Sharp AR-351FP PS	OpenPrintingPPDs-postscript
Sharp AR-351N	OpenPrintingPPDs-ghostscript
Sharp AR-351N PS	OpenPrintingPPDs-postscript
Sharp AR-351S	OpenPrintingPPDs-ghostscript
Sharp AR-351S PS	OpenPrintingPPDs-postscript
Sharp AR-451FP	OpenPrintingPPDs-ghostscript
Sharp AR-451FP PS	OpenPrintingPPDs-postscript
Sharp AR-451N	OpenPrintingPPDs-ghostscript
Sharp AR-451N PS	OpenPrintingPPDs-postscript
Sharp AR-451S	OpenPrintingPPDs-ghostscript
Sharp AR-451S PS	OpenPrintingPPDs-postscript
Sharp AR-555M	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Sharp AR-555M PS	OpenPrintingPPDs-postscript
Sharp AR-555S	OpenPrintingPPDs-ghostscript
Sharp AR-555S PS	OpenPrintingPPDs-postscript
Sharp AR-625M	OpenPrintingPPDs-ghostscript
Sharp AR-625M PS	OpenPrintingPPDs-postscript
Sharp AR-625S	OpenPrintingPPDs-ghostscript
Sharp AR-625S PS	OpenPrintingPPDs-postscript
Sharp AR-705M	OpenPrintingPPDs-ghostscript
Sharp AR-705M PS	OpenPrintingPPDs-postscript
Sharp AR-705S	OpenPrintingPPDs-ghostscript
Sharp AR-705S PS	OpenPrintingPPDs-postscript
Sharp AR-C170FP	OpenPrintingPPDs-ghostscript
Sharp AR-C170FP PS	OpenPrintingPPDs-postscript
Sharp AR-C172FP	OpenPrintingPPDs-ghostscript
Sharp AR-C172FP PS	OpenPrintingPPDs-postscript
Sharp AR-C260FP	OpenPrintingPPDs-ghostscript
Sharp AR-C260FP PS	OpenPrintingPPDs-postscript
Sharp AR-C261FP	OpenPrintingPPDs-ghostscript
Sharp AR-C261FP PS	OpenPrintingPPDs-postscript
Sharp AR-C262FP	OpenPrintingPPDs-ghostscript
Sharp AR-C262FP PS	OpenPrintingPPDs-postscript
Sharp AR-M150	OpenPrintingPPDs-ghostscript
Sharp AR-M150 PS	OpenPrintingPPDs-postscript
Sharp AR-M155	OpenPrintingPPDs-ghostscript
Sharp AR-M155 PS	OpenPrintingPPDs-postscript
Sharp AR-M160	OpenPrintingPPDs-ghostscript
Sharp AR-M160 PS	OpenPrintingPPDs-postscript
Sharp AR-M161	OpenPrintingPPDs-ghostscript
Sharp AR-M161 PS	OpenPrintingPPDs-postscript
Sharp AR-M162	OpenPrintingPPDs-ghostscript
Sharp AR-M162 PS	OpenPrintingPPDs-postscript
Sharp AR-M165	OpenPrintingPPDs-ghostscript
Sharp AR-M165 PS	OpenPrintingPPDs-postscript
Sharp AR-M205	OpenPrintingPPDs-ghostscript
Sharp AR-M205 PS	OpenPrintingPPDs-postscript
Sharp AR-M206	OpenPrintingPPDs-ghostscript
Sharp AR-M206 PS	OpenPrintingPPDs-postscript
Sharp AR-M207	OpenPrintingPPDs-ghostscript
Sharp AR-M207 PS	OpenPrintingPPDs-postscript
Sharp AR-M236	OpenPrintingPPDs-ghostscript
Sharp AR-M236 PS	OpenPrintingPPDs-postscript
Sharp AR-M237	OpenPrintingPPDs-ghostscript
Sharp AR-M237 PS	OpenPrintingPPDs-postscript
Sharp AR-M257	gutenprint-ppd
Sharp AR-M276	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Sharp AR-M276 PS	OpenPrintingPPDs-postscript
Sharp AR-M277	OpenPrintingPPDs-ghostscript
Sharp AR-M277 PS	OpenPrintingPPDs-postscript
Sharp AR-NB2	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Sharp AR-NB2 Sharp AR-NB2	manufacturer-PPDs OpenPrintingPPDs-postscript
Sharp AR-NB3 Sharp AR-NB3	manufacturer-PPDs OpenPrintingPPDs-postscript
Sharp AR-P17 Sharp AR-P17	manufacturer-PPDs OpenPrintingPPDs-postscript
Sharp AR-P19	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Sharp AR-P19 Sharp AR-P19	manufacturer-PPDs OpenPrintingPPDs-postscript
Sharp AR-P20	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Sharp AR-P20 Sharp AR-P20	manufacturer-PPDs OpenPrintingPPDs-postscript
Sharp AR-PK1 Sharp AR-PK1	manufacturer-PPDs
Sharp AR-PK4	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Sharp AR-PK4 Sharp AR-PK4	manufacturer-PPDs OpenPrintingPPDs-postscript
Sharp ARP350	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Sharp ARP450	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Sharp MX-2300FG	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-2300FG PS	OpenPrintingPPDs-postscript
Sharp MX-2300G	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-2300G PS	OpenPrintingPPDs-postscript
Sharp MX-2300N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-2300N PS	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Sharp MX-2700FG	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-2700FG PS	OpenPrintingPPDs-postscript
Sharp MX-2700G	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-2700G PS	OpenPrintingPPDs-postscript
Sharp MX-2700N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-2700N PS	OpenPrintingPPDs-postscript
Sharp MX-3500FN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-3500FN PS	OpenPrintingPPDs-postscript
Sharp MX-3500N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-3500N PS	OpenPrintingPPDs-postscript
Sharp MX-3501FN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-3501FN PS	OpenPrintingPPDs-postscript
Sharp MX-3501N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-3501N PS	OpenPrintingPPDs-postscript
Sharp MX-4500FN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-4500FN PS	OpenPrintingPPDs-postscript
Sharp MX-4500N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-4500N PS	OpenPrintingPPDs-postscript
Sharp MX-4501FN	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-4501FN PS	OpenPrintingPPDs-postscript
Sharp MX-4501N	manufacturer-PPDs OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Sharp MX-4501N PS	OpenPrintingPPDs-postscript

Печатающие устройства производства Tally, Tektronix, Texas Instruments, Toshiba

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Tally	
Tally LN45	OpenPrintingPPDs-postscript
Tally ML450	OpenPrintingPPDs-postscript
Tally MT908	OpenPrintingPPDs-ghostscript gutenprint-ppd
Tektronix	
Tektronix 4695	OpenPrintingPPDs-ghostscript
Tektronix 4696	OpenPrintingPPDs-ghostscript
Tektronix 4697	OpenPrintingPPDs-ghostscript
Tektronix Phaser 350	OpenPrintingPPDs-postscript
Tektronix Phaser 750DP	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Tektronix Phaser 750DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Tektronix Phaser 750N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Tektronix Phaser 750P	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Tektronix Phaser 780	OpenPrintingPPDs-postscript
Tektronix Phaser 850	OpenPrintingPPDs-postscript
Tektronix Phaser 850DP	OpenPrintingPPDs-postscript
Tektronix Phaser 850DX	OpenPrintingPPDs-postscript
Tektronix Phaser 850N	OpenPrintingPPDs-postscript
Tektronix Phaser IISX	OpenPrintingPPDs-postscript
Tektronix Phaser PX	OpenPrintingPPDs-postscript
Texas Instruments	
Texas Instruments microLaser PowerPro 12	OpenPrintingPPDs-postscript
Texas Instruments microLaser Pro 8	OpenPrintingPPDs-postscript
Texas Instruments microLaser Pro 600	OpenPrintingPPDs-postscript
Texas Instruments microLaser Pro E	OpenPrintingPPDs-postscript
Texas Instruments microLaser XL Basic	OpenPrintingPPDs-postscript
Texas Instruments microLaser XL PS17	OpenPrintingPPDs-postscript
Texas Instruments microLaser XL PS35	OpenPrintingPPDs-postscript
Texas Instruments microLaser XL Turbo	OpenPrintingPPDs-postscript
Toshiba	
Toshiba DP2570	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Toshiba e-Studio 162	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 162d	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 165	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 167	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 200L/202L	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 203L	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 205	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 220cp	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 230/232	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 233	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 237	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 280/282	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 281c	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 283	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 350	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 351c	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 352	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 353	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 450	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 450s	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 451c	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 452	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 453	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 500p	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 500s	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 520	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 523	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 523t	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 600	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 603	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 603t	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Toshiba e-Studio 720	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 723	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 723t	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 850	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 853	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 901	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 1101	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 1351	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 2500c	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 2830c	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 3500c	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 3510c	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 3511	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 3530c	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 4500c	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 4511	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba e-Studio 4520c	OpenPrintingPPDs-ghostscript
Toshiba e-Studio 5500c	OpenPrintingPPDs-ghostscript
Toshiba GL-1010	OpenPrintingPPDs-postscript
Toshiba GL-1020	OpenPrintingPPDs-postscript
Toshiba TEC Corp. GL-1010	manufacturer-PPDs OpenPrintingPPDs-postscript
Toshiba TEC Corp. GL-1020	manufacturer-PPDs OpenPrintingPPDs-postscript

Печатающие устройства производства Xante, Xerox

Установка драйверов из нижеприведенного перечня возможна с помощью следующей команды (требует права суперпользователя):
- если вы используете РЕД ОС версии 7.1 или 7.2:
sudo yum install , например:

```
$ sudo yum install foo2zjs
```

- если вы используете РЕД ОС версии 7.3 и старше:
sudo dnf install , например:

```
$ sudo dnf install foo2zjs
```

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xante	
Xante Accel-a-Writer 4G	OpenPrintingPPDs-postscript
Xante FilmMaker 4	OpenPrintingPPDs-postscript
Xante PlateMaker 4	OpenPrintingPPDs-postscript
Xerox	
Xerox 2700 XES	OpenPrintingPPDs-ghostscript
Xerox 3700 XES	OpenPrintingPPDs-ghostscript
Xerox 4045 XES	OpenPrintingPPDs-ghostscript
Xerox Able 1406	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Xerox CUPS v1.1	OpenPrintingPPDs-postscript
Xerox DocuColor 2006	OpenPrintingPPDs-postscript
Xerox Document Centre 400	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Xerox Document HomeCentre	OpenPrintingPPDs-ghostscript
Xerox DocuPrint	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Xerox DocuPrint 4508	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Xerox DocuPrint C6	OpenPrintingPPDs-ghostscript
Xerox DocuPrint C8	OpenPrintingPPDs-ghostscript
Xerox DocuPrint C11	OpenPrintingPPDs-ghostscript
Xerox DocuPrint C20	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox DocuPrint C55	OpenPrintingPPDs-postscript
Xerox DocuPrint N17	OpenPrintingPPDs-postscript
Xerox DocuPrint N24	OpenPrintingPPDs-postscript
Xerox DocuPrint N32	OpenPrintingPPDs-postscript
Xerox DocuPrint N40	OpenPrintingPPDs-postscript
Xerox DocuPrint M750	OpenPrintingPPDs-ghostscript
Xerox DocuPrint M760	OpenPrintingPPDs-ghostscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox DocuPrint N2125	OpenPrintingPPDs-postscript
Xerox DocuPrint N3225	OpenPrintingPPDs-postscript
Xerox DocuPrint N4025	OpenPrintingPPDs-postscript
Xerox DocuPrint N4512	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Xerox DocuPrint N4512PS	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox DocuPrint N4525	OpenPrintingPPDs-postscript
Xerox DocuPrint P8e	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Xerox DocuPrint P12	OpenPrintingPPDs-ghostscript gutenprint-ppd
Xerox DocuPrint P1202	gutenprint-ppd
Xerox DocuPrint XJ6C	OpenPrintingPPDs-ghostscript
Xerox DocuPrint XJ8C	OpenPrintingPPDs-ghostscript
Xerox FaxCenter 2121	OpenPrintingPPDs-postscript
Xerox FaxCentre 2218	OpenPrintingPPDs-postscript
Xerox Phaser 790	OpenPrintingPPDs-postscript
Xerox Phaser 860B	OpenPrintingPPDs-postscript
Xerox Phaser 860DP	OpenPrintingPPDs-postscript
Xerox Phaser 860DX	OpenPrintingPPDs-postscript
Xerox Phaser 860N	OpenPrintingPPDs-postscript
Xerox Phaser 1235	OpenPrintingPPDs-postscript
Xerox Phaser 2135	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 3010	foo2zjs
Xerox Phaser 3040	foo2zjs
Xerox Phaser 3110	OpenPrintingPPDs-ghostscript
Xerox Phaser 3124	OpenPrintingPPDs-ghostscript
Xerox Phaser 3150	OpenPrintingPPDs-ghostscript
Xerox Phaser 3160N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs
Xerox Phaser 3200MFP	OpenPrintingPPDs-postscript
Xerox Phaser 3400	OpenPrintingPPDs-postscript
Xerox Phaser 3450	OpenPrintingPPDs-postscript
Xerox Phaser 3500	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 4400B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4400DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4400DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4400N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4500B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4500DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4500DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4500N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4510	OpenPrintingPPDs-postscript
Xerox Phaser 4510B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4510DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 4510DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 4510N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 5500	OpenPrintingPPDs-postscript
Xerox Phaser 5500B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 5500DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 5500DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 5500DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 5500N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6110	foo2zjs
Xerox Phaser 6115 MFP	foo2zjs
Xerox Phaser 6120 PS	OpenPrintingPPDs-postscript
Xerox Phaser 6121 MFP	foo2zjs
Xerox Phaser 6130	OpenPrintingPPDs-postscript
Xerox Phaser 6130N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6180	OpenPrintingPPDs-postscript
Xerox Phaser 6180DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6180MFP-D	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 6200B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6200DP	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6200DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6200N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6250B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6250DP	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6250DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6250DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6250N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6300DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6300N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 6350DP	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6350DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6350DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6360	OpenPrintingPPDs-postscript
Xerox Phaser 6360DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 6360DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7300B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7300DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7300DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7300DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7300N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7400	OpenPrintingPPDs-postscript
Xerox Phaser 7400DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 7400DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7400DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7400DXF	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7400N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7700DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7700DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7700GX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7750B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7750DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7750DXF	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7750GX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7760	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 7760DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7760DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 7760GX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8200B	OpenPrintingPPDs-postscript
Xerox Phaser 8200DP	OpenPrintingPPDs-postscript
Xerox Phaser 8200DX	OpenPrintingPPDs-postscript
Xerox Phaser 8200N	OpenPrintingPPDs-postscript
Xerox Phaser 8400B	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8400BD	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8400DP	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8400DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8400N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8500DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8500N	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox Phaser 8550DP	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8550DT	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8550DX	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8560	OpenPrintingPPDs-postscript
Xerox Phaser 8560DN	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript gutenprint-ppd
Xerox Phaser 8860	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Xerox WC 4118	OpenPrintingPPDs-postscript
Xerox WC M20	OpenPrintingPPDs-postscript
Xerox WC PE120	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-postscript
Xerox WorkCentre 24	OpenPrintingPPDs-postscript
Xerox WorkCentre 450cp	OpenPrintingPPDs-ghostscript
Xerox WorkCentre 470cx	OpenPrintingPPDs-ghostscript
Xerox WorkCentre 3045	foo2zjs
Xerox WorkCentre 6015	foo2zjs
Xerox WorkCentre 7228	OpenPrintingPPDs-postscript
Xerox WorkCentre 7232	OpenPrintingPPDs-postscript
Xerox WorkCentre 7242	OpenPrintingPPDs-postscript
Xerox WorkCentre 7328	OpenPrintingPPDs-postscript
Xerox WorkCentre 7335	OpenPrintingPPDs-postscript
Xerox WorkCentre 7345	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs gutenprint-ppd
Xerox WorkCentre 7345	OpenPrintingPPDs-postscript
Xerox WorkCentre C2424	OpenPrintingPPDs-ghostscript OpenPrintingPPDs-hpijs OpenPrintingPPDs-postscript
Xerox WorkCentre M118	OpenPrintingPPDs-postscript gutenprint-ppd
Xerox WorkCentre M24	OpenPrintingPPDs-postscript
Xerox WorkCentre Pro 128	OpenPrintingPPDs-postscript

Модели (серии) устройств	RPM-пакеты с драйверами для данного устройства
Xerox WorkCentre Pro 133	OpenPrintingPPDs-postscript

Модели производителя ARBYTE

Платформы
Серверы
ARBYTE ALKAZAR R1D54 G3
ARBYTE ALKAZAR R1D55 G3
ARBYTE ALKAZAR R1D55 G5
ARBYTE ALKAZAR R1D56 G3
ARBYTE ALKAZAR R1D56 G5
ARBYTE ALKAZAR R2D55 G3
ARBYTE ALKAZAR R2D55 G5
ARBYTE ALKAZAR R2D56 G3
ARBYTE ALKAZAR R2D56 G5
ARBYTE ALKAZAR R2D57 G5
ARBYTE SILEX M115 G5
ARBYTE SILEX R115 G5
ARBYTE SILEX R133 G3
ARBYTE SILEX R231 G3
ARBYTE SILEX S133 G5
ARBYTE SILEX S231 G3
ARBYTE SILEX S231 G5
ARBYTE SILEX S233 G3
ARBYTE SILEX S233SM G5
ARBYTE SILEX T115 G5
ARBYTE ZEEGER Z121 G5
ARBYTE ZEEGER Z122 G5
ARBYTE ZEEGER Z122 RPS G5
Настольные системы
ARBYTE TEMPO TD4-B36X
ARBYTE TEMPO TD4-B460
ARBYTE TEMPO TD4-H110
ARBYTE TEMPO TD4-H310
ARBYTE TEMPO TD4-H370
ARBYTE TEMPO TD4-H410
ARBYTE TEMPO TD4-H470
ARBYTE TEMPO TD4-Q370
ARBYTE TEMPO TD4-X299
ARBYTE TEMPO TD4-Z390
ARBYTE TEMPO TD4-Z490
ARBYTE FORTE AIO-SoC D3
ARBYTE FORTE AIO4-H110
ARBYTE FORTE AIO4-H310
ARBYTE FORTE ND3
ARBYTE FORTE ND3 SoC
ARBYTE FORTE ND4-B360

ARBYTE FORTE ND4-H110
ARBYTE FORTE ND4-H310
ARBYTE FORTE ND4
ARBYTE FORTE SD4-B36X
ARBYTE FORTE SD4-B460
ARBYTE FORTE SD4-H110
ARBYTE FORTE SD4-H310
ARBYTE FORTE SD4-H370
ARBYTE FORTE SD4-H410
ARBYTE FORTE SD4-H470
ARBYTE FORTE SD4-Q370
ARBYTE FORTE SD4-Z390
ARBYTE FORTE SD4-Z490
ARBYTE FORTE SD4 SoC
ARBYTE QUINT MD4-B36X
ARBYTE QUINT MD4-B460
ARBYTE QUINT MD4-H110
ARBYTE QUINT MD4-H310
ARBYTE QUINT MD4-H370
ARBYTE QUINT MD4-H410
ARBYTE QUINT MD4-H470
ARBYTE QUINT MD4-Q370
ARBYTE QUINT MD4-Z390
ARBYTE QUINT MD4-Z490
ARBYTE CADStation WS 147

Часто задаваемые вопросы по РЕД ОС (FAQ)

Где находятся полезные материалы по РЕД ОС?

- База Знаний — https://redos.red-soft.ru/base/;
- Документация — https://redos.red-soft.ru/support/docs/ ;
- RuTube-канал — https://rutube.ru/channel/23912197/;
- Яндекс.Дзен — https://dzen.ru/redos;
- VK — https://vk.com/1redsoft.

Как узнать дату установки ОС?

Определить дату создания файловой системы:

```
sudo -E tune2fs -l $(df / | tail -1 | cut -f1 -d' ') | grep created
```

Определить дату создания самого старого каталога:

```
sudo -E ls --time-style=long-iso -clt / | tail -n 1 | awk '{ print $7, $6}'
```

Вывести даты установки пакетов:

```
rpm -qa --last
```

Как проверить диск на ошибки и исправить их?

Запустите ОС в **single mode**, для этого пропишите в меню загрузки **grub** параметр **init=/bin/bash** в конце строки, которая начинается на **linux16**.

Запустите проверку выполнив команду:

```
/usr/sbin/fsck -ACVfyv
```

Или запустите ОС сразу в режиме исправления ошибок диска, для этого в параметрах **grub** вместо **init=/bin/bash** пропишите **fsck.mode=force fsck.repair=yes**.

Более подробную информацию можно найти в наших инструкциях:

- для РЕД ОС 7.3 — «Проверка файловой системы на наличие ошибок»;
- для РЕД ОС 8 — «Проверка файловой системы на наличие ошибок».

Как в консоли смонтировать флешку?

Выведите список доступных дисков:

```
sudo -E fdisk -l
```

Примонтируйте флешку, например, в **mnt**:

```
sudo -E mount /dev/sdc1 /mnt/
```

Как посмотреть логи журналов в реальном времени?

Для просмотра можно воспользоваться командами:

```
sudo -E journalctl -f
sudo -E tail -f /var/log/messages
```

Как посмотреть статус службы?

Для просмотра статуса службы выполните команду:

```
systemctl status <имя_службы>
```

Более подробную информацию можно найти в наших инструкциях:

- для РЕД ОС 7.3 — «Менеджер сервисов Systemd»;
- для РЕД ОС 8 — «Менеджер сервисов Systemd».

Как запустить службу?

Для запуска службы выполните команду:

```
sudo -E systemctl start <имя_службы>
```

Более подробную информацию можно найти в наших инструкциях:

- для РЕД ОС 7.3 — «Менеджер сервисов Systemd»;
- для РЕД ОС 8 — «Менеджер сервисов Systemd».

Как остановить службу?

Для остановки запущенной службы выполните команду:

```
sudo -E systemctl stop <имя_службы>
```

Более подробную информацию можно найти в наших инструкциях:

- для РЕД ОС 7.3 — «Менеджер сервисов Systemd»;
- для РЕД ОС 8 —«Менеджер сервисов Systemd» .

Как добавить службу в автозагрузку?

Для добавления службы в автозагрузку выполните команду:

```
sudo -E systemctl enable <имя_службы>
```

Более подробную информацию можно найти в наших инструкциях:

- для РЕД ОС 7.3 — «Менеджер сервисов Systemd»;
- для РЕД ОС 8 — «Менеджер сервисов Systemd».

Как вывести список рабочих процессов?

Для просмотра списка запущенных процессов выполните команду:

```
top

или
```

```
ps -x
```

Как найти и завершить процесс?

Удобнее всего воспользоваться утилитами для мониторинга процессов, подробнее см. в наших инструкциях:

- для РЕД ОС 7.3 — «Интерактивные утилиты динамического мониторинга процессов»;
- для РЕД ОС 8 — «Интерактивные утилиты динамического мониторинга процессов».

Как открыть/установить диспетчер задач?

По умолчанию в РЕД ОС предустановлен пакет **mate-system-monitor**, также в репозитории присутствует альтернативный диспетчер задач **sysmontask**. Подробную информацию об установке и работе **sysmontask** см. в наших инструкциях:

- для РЕД ОС 7.3 — «SysMonTask - диспетчер задач»;
- для РЕД ОС 8 — «SysMonTask - диспетчер задач».

Как добавить программу в автозагрузку?

Для добавления какой-либо программы в автозагрузку воспользуйтесь нашими инструкциями:

- для РЕД ОС 7.3 — «Добавление команд в автозагрузку»;
- для РЕД ОС 8 — «Добавление команд в автозагрузку».

Как установить rpm-пакет?

Для установки пакета из репозитория выполните команду:

```
sudo -E dnf install <имя_пакета>
```

Для установки любых других пакетов, например, из сети Интернет, выполните команду:

```
sudo -E dnf install /<путь_до_пакета>/<имя_пакета.rpm>
```

Подробнее об установке пакетов можно посмотреть в наших инструкциях:

- для РЕД ОС 7.3 — «Установка или обновление пакета»;
- для РЕД ОС 8 — «Установка или обновление пакета».

Как удалить программу?

Для удаления программы выполните команду:

```
sudo -E dnf remove <имя_пакета>
```

Подробнее об удалении пакетов можно посмотреть в наших инструкциях:

- для РЕД ОС 7.3 — «Удаление установленного пакета»;
- для РЕД ОС 8 — «Удаление установленного пакета».

Как посмотреть наличие пакета в репозитории?

Для поиска пакета выполните команду:

```
dnf search <имя_пакета>
```

Подробнее ознакомиться с работой **dnf** можно в наших инструкциях:

- для РЕД ОС 7.3 — «Основные команды DNF»;
- для РЕД ОС 8 — «Основные команды DNF».

Как посмотреть наличие библиотеки или определенного файла в rpm?

Для просмотра статуса службы выполните команду:

```
dnf provides <имя_библиотеки>

или

dnf provides <имя_файла>
```

Подробнее ознакомиться с работой **dnf** можно в наших инструкциях:

- для РЕД ОС 7.3 — «Основные команды DNF»;
- для РЕД ОС 8 — «Основные команды DNF».

Как получить информацию о пакете?

Для получения информации о пакете выполните команду:

```
dnf info <имя_пакета>
```

Подробнее ознакомиться с работой **dnf** можно в наших инструкциях:

- для РЕД ОС 7.3 — «Основные команды DNF»;
- для РЕД ОС 8 — «Основные команды DNF».

Как получить информацию об используемых в системе репозиториях?

Для получения информации о репозиториях выполните команду:

```
dnf repolist
```

Подробнее ознакомиться с **rpm** и репозиториями можно в наших инструкциях:

- для РЕД ОС 7.3:
  - «Источники программ (репозитории)»;
  - «Основные команды DNF».
- для РЕД ОС 8:
  - «Источники программ (репозитории)»;
  - «Основные команды DNF».

Как проверить, установлен ли пакет в системе?

Для проверки установки пакета выполните команду:

```
rpm -qa | grep <имя_пакета>
```

Подробнее ознакомиться с **rpm** и репозиториями можно в наших инструкциях:

- для РЕД ОС 7.3 — «Источники программ (репозитории)»;
- для РЕД ОС 8 — «Источники программ (репозитории)».

Как сделать файл (bin, appimage и т. д.) исполняемым и выполнить запуск?

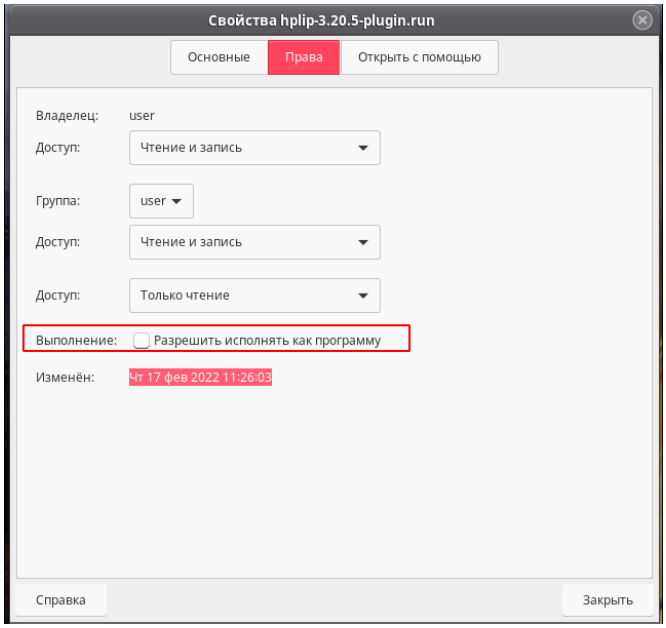
Чтобы назначить файлу права на исполнение, выполните команду:

```
chmod +x ./<имя_файла>
```

Запустить файл можно командой:

```
./<имя_файла>
```

В графическом варианте необходимо нажать ПКМ по нужному файлу, затем «**Свойства**» - «**Права**» и установить флаг «**Разрешить исполнять как программу**».



Подробную информацию о работе с **AppImage** можно посмотреть в наших инструкциях:

- для РЕД ОС 7.3 — «AppImage - запуск приложений без установки»;
- для РЕД ОС 8 — «AppImage - запуск приложений без установки».

Как отключить отображение подключенных носителей на рабочем столе?

Для отключения отображения подключенных носителей на рабочем столе выполните команду:

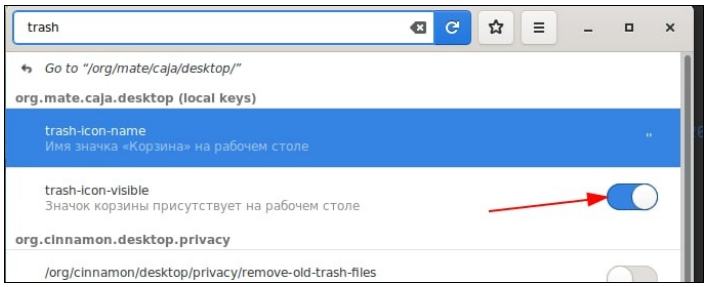
```
dconf write /org/mate/caja/desktop/volumes-visible false
```

Как убрать корзину и значки подключенных сетевых дисков с рабочего стола?

Для этого можно использовать утилиту **mate-tweak**:

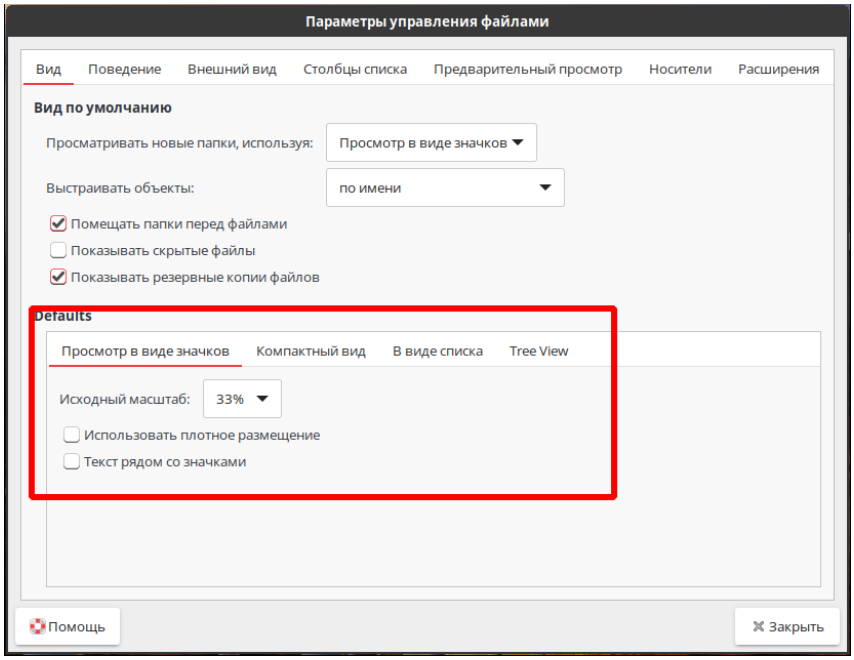
```
sudo -E dnf install mate-tweak
```

или утилиту **dconf-editor**, которая доступна из «**Главного меню**» - «**Администрирование**» - «**Редактор dconf**»:



Как на рабочем столе сделать размер иконок меньше?

Для изменения размеров иконок рабочего стола перейдите «**Главное меню**» - «**Параметры**» - «**Управление файловым просмотром**», на вкладке «**Вид**» будут доступны действия для настройки значков рабочего стола, в т.ч. их размеров.



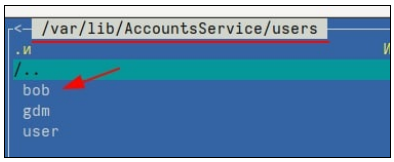
Как убрать лишних доменных пользователей с экрана входа?

Для этого выполните команду:

```
sudo -E sed -i s'|SystemAccount\=false|SystemAccount\=true|'g /var/lib/AccountsService/users/<имя_доменного_пользователя>
```

Перезагрузите систему.

Также можно удалить файл:



Однако данное действие может повлечь за собой последствия в виде **нарушения работы** некоторых системных утилит.

Как записать РЕД ОС на флешку?

Ознакомиться с возможностью записи РЕД ОС на флешку можно, прочитав наши инструкции:

- для РЕД ОС 7.3 — «Создание загрузочных носителей»;
- для РЕД ОС 8 — «Создание загрузочных носителей».

Как отформатировать флешку?

Для форматирования флешки воспользуйтесь утилитой **Gparted**. Подробную информацию о работе с утилитой см. в наших инструкциях:

- для РЕД ОС 7.3 — «Gparted - работа с дисковыми разделами»;
- для РЕД ОС 8 — «Gparted - работа с дисковыми разделами».

Как поставить РЕД ОС рядом с установленной Windows на один диск?

Ознакомиться с установкой РЕД ОС рядом с Windows можно в наших инструкциях:

- для РЕД ОС 7.3 — «Установка РЕД ОС на один диск с ОС Windows (dual-boot) »;
- для РЕД ОС 8 — «Установка РЕД ОС на один диск с ОС Windows (dual-boot) ».

Как обновить дистрибутив?

Для обновления пакетов воспользуйтесь нашими инструкциями:

- для РЕД ОС 7.3 — «Обновление всех установленных пакетов»;
- для РЕД ОС 8 — «Обновление всех установленных пакетов».

Для обновления дистрибутива воспользуйтесь подходящей для вас инструкцией из раздела «Обновление РЕД ОС».

Как получить права root?

Для перехода в сеанс пользователя **root** выполните команду:

```
su -
```

Подробная информация о правах и привилегиях в системе приведена в наших инструкциях:

- для РЕД ОС 7.3 — «Привилегии и root»;
- для РЕД ОС 8 — «Привилегии и root».

Как добавить постоянный маршрут?

Подробную информацию о настройке сети и добавлении постоянного маршрута см. в наших инструкциях:

- для РЕД ОС 7.3 — «Настройка сетевого адаптера»;
- для РЕД ОС 8 — «Настройка сетевого адаптера».

Вывести информацию об установленных сетевых интерфейсах

Выполните команду:

```
ifconfig

или

ip a
```

Как настроить сеть через консоль?

Отключите получение dns-адресов от **dhcp**:

```
nmcli connection modify eth0 ipv4.ignore-auto-dns true
```

Установите dns-адреса:

```
nmcli connection modify eth0 ipv4.dns "10.81.1.196"
```

Установите поисковый домен:

```
nmcli con mod eth0 ipv4.dns-search "win.redos"
```

Перезапустите сеть для применения настроек:

```
nmcli con down eth0 && nmcli con up eth0
```

Как добавить кнопку запуска (ярлык) на рабочий стол?

Подробную информацию о создании кнопки запуска см. в наших инструкциях:

- для РЕД ОС 7.3 — «Создание кнопки запуска доступа к сетевому ресурсу»;
- для РЕД ОС 8 — «Создание кнопки запуска доступа к сетевому ресурсу».

Как получить информацию о системе?

Для получения информации о системе выполните команду:

```
lsb_release -a
```

Как получить информацию об используемом системой ядре?

Для получения информации об используемом системой ядре выполните одну из следующих команд:

```
uname -a
uname -r
```

Также более подробную техническую информацию об используемом железе можно посмотреть в наших инструкциях:

- для РЕД ОС 7.3 — «Получение технической информации о ПК»;
- для РЕД ОС 8 — «Получение технической информации о ПК».

Как получить информацию об установленном cpu?

Для получения информации о cpu выполните команду:

```
lscpu
```

Как получить информацию о подключенных usb-устройствах?

Для получения информации о подключенных usb-устройствах выполните команду:

```
lsusb
```

Как получить информацию об устройствах использующих PCI-шину?

Для получения информации о PCI-устройствах выполните команду:

```
lspci
```

Как получить информацию о разделах?

Для получения информации о разделах выполните одну из следующих команд:

```
lsblk
df -h
sudo -E fdisk -l
findmnt --real
```

Более подробную информацию о работе с дисковыми утилитами см. в наших инструкциях:

- для РЕД ОС 7.3:
  - «Baobab - программа для анализа использования разделов диска»;
  - «Утилиты для работы с дисковым пространством»;
  - «FSlint - графическая утилита поиска дубликатов файлов».
- для РЕД ОС 8:
  - «Baobab - программа для анализа использования разделов диска»;
  - «Утилиты для работы с дисковым пространством»;
  - «FSlint - графическая утилита поиска дубликатов файлов».

Как посмотреть режим работы SELinux?

Для просмотра режима работы *SELinux* выполните команду:

```
sestatus
```

Подробную информацию о *SELinux* см. в наших инструкциях:

- для РЕД ОС 7.3:
  - «SELinux - система принудительного контроля доступа»;
  - «Отключение SELinux».
- для РЕД ОС 8:
  - «SELinux - система принудительного контроля доступа»;
  - «Отключение SELinux».

Как узнать имя хоста?

Для просмотра имени хоста выполните команду:

```
hostname

или

hostnamectl
```

Как изменить раскладку клавиатуры на US при входе пользователя?

Для изменения раскладки клавиатуры службы выполните команду:

```
sudo -u gdm localectl set-x11-keymap us,ru
```

На ПК стоит много ПО, что будет быстрее - обновиться или поставить с нуля?

Однозначный ответ, который подходит для всех случаев, дать невозможно. Многое зависит от специфики ПО, установленного на ПК.

Определенно, наиболее верным решением будет проведение тестирования обновления на тестовом стенде или в среде виртуализации. И уже в случае успеха делать выводы по времени, затрачиваемому на обновление или чистую установку и настройку ОС и ПО.

Что делать, если после обновления ядра или каких-либо еще пакетов перестала загружаться графика?

Сначала попробуйте запустить ОС на старом ядре, обычно в момент обновления оно остается доступным в меню **grub**.

Если данный вариант не помог, попробуйте запустить ОС в текстовом режиме или с **nomodeset**.

Дальше потребуется детальное изучение логов ОС, какие пакеты были обновлены, попробовать откатить пакеты на предыдущую версию и сравнить работоспособность ПК.

В случае, если проблематичные пакеты выявлены, необходимо сообщить в техническую поддержку РЕД ОС для исправления данных пакетов.

Также попробуйте воспользоваться рекомендациями из раздела «**Решение возникающих проблем**»:

- для РЕД ОС 7.3 — «Решение возникающих проблем»;
- для РЕД ОС 8 — «Решение возникающих проблем».

О, нет! Что-то пошло не так :(

Данная ошибка чаще всего встречается в средах виртуализации. Вы можете попробовать ее избежать, увеличив объем видеопамяти для виртуальной машины, а также сменив графический контроллер ВМ. Если же данная ошибка возникает на реальном ПК, потребуется изучение логов для понимания проблемы.

Также стоит попробовать вариант с заменой дисплей-менеджера на *sddm*, подробную информацию см. в наших инструкциях:

- для РЕД ОС 7.3 — «Менеджер входа в систему sddm»;
- для РЕД ОС 8 — «Менеджер входа в систему sddm».

Welcome to emergency mode!

Для решения вопросов, связанных с аварийным режимом, существует раздел по решению ошибок при загрузке ОС:

- для РЕД ОС 7.3 — «Решение возникающих проблем»;
- для РЕД ОС 8 — «Решение возникающих проблем».

Если указанные решения не помогут справиться с данным режимом, потребуется собрать логи с машины и провести детальное изучение, что именно не дает ОС загрузиться в штатном режиме.

Как изменить меню загрузки grub?

Подробную информацию см. в наших инструкциях:

- для РЕД ОС 7.3 — «grub-customizer - утилита редактирования загрузчика ОС»;
- для РЕД ОС 8 — «grub-customizer - утилита редактирования загрузчика ОС».

Как создать и подключить локальный репозиторий?

Для решения данного вопроса необходимо ознакомиться с разделом «**Обслуживание репозиториев**»:

- для РЕД ОС 7.3 — «Обслуживание репозиториев»;
- для РЕД ОС 8 — «Обслуживание репозиториев».

Запрос разблокировки связки ключей при работе с ОС. Что делать?

Для решения данного вопроса необходимо ознакомиться с нашими инструкциями:

- для РЕД ОС 7.3 — «Разблокировка связки ключей»;
- для РЕД ОС 8 — «Разблокировка связки ключей».

Как работать с WINE и префиксами?

Подробную информацию о работе с WINE и префиксами см. в наших инструкциях:

- для РЕД ОС 7.3 — «Работа с WINE»;
- для РЕД ОС 8 — «Работа с WINE».

Как работать с политиками polkit? Как отключить запрос пароля для добавления принтера?

Подробную информацию о работе с политиками *polkit* см. в наших инструкциях:

- для РЕД ОС 7.3 — «Работа с политиками Polkit»;
- для РЕД ОС 8 — «Работа с политиками Polkit».

Поддерживается ли железо ядром системы?

Подробную информацию о поддержке железа ядром см. в наших инструкциях:

- для РЕД ОС 7.3 — «Поддержка оборудования в ядре ОС»;
- для РЕД ОС 8 — «Поддержка оборудования в ядре ОС».

Как поставить принтер? Поддерживается ли данная модель? Поддерживается ли сканер?

Примеры установки принтеров описаны в разделе «**Настройка принтеров**».

- для РЕД ОС 7.3 — «Настройка принтеров»;
- для РЕД ОС 8 — «Настройка принтеров».

Поиск драйверов для принтеров осуществляется по названию модели в Базе Знаний, например, в разделе «Оборудование, совместимое с РЕД ОС».

Однако охватить полностью список печатающих и сканирующих устройств довольно проблематично, поэтому вы можете самостоятельно поискать драйвер под ваше устройство. Для этого достаточно ввести в браузере запрос формата `<модель_устройства> linux driver`. Если модель имеет поддержку *linux*, найти необходимый драйвер не составит труда.

Как подключить зеркала репозиториев?

Зеркала репозиториев РЕД ОС расположены по ссылкам:

- http://repo1.red-soft.ru/redos/;
- https://mirror.yandex.ru/redos/.

Где скачать установочные образы предыдущих версий РЕД ОС?

Скачать установочные образы можно по ссылке - http://repo1.red-soft.ru/redos/.

Например, РЕД ОС 7.3 - http://repo1.red-soft.ru/redos/7.3/x86_64/iso/.

Как переключиться в консольный режим?

Для переключения в консольный режим используйте сочетание клавиш «**Ctrl + Alt + F2..F6**».

Как отключить обнаружение сетевых принтеров и сканеров?

Для отключения сетевых принтеров и сканеров выполните команду (с правами суперпользователя):

```
systemctl disable avahi-daemon.service --now
systemctl disable avahi-daemon.socket --now
systemctl disable cups-browsed.service --now
```

Как посмотреть изменения в программах?

```
dnf repoquery --latest-limit 1 --changelogs <имя_пакета>
rpm -q --changelog <имя_локального_пакета>
```

Что делать, если не монтируется NTFS в LiveUSB?

```
dnf install ntfs-3g.x86_64
```

Как в менеджере входа по умолчанию установить английский язык?

Для смены в менеджере входа языка, используемого по умолчанию, на английский необходимо отредактировать файл, выполнив команду (с правами суперпользователя):

```
nano /etc/X11/xorg.conf.d/00-keyboard.conf
```

И привести строку `Option "XkbLayout" "ru,us"` к виду `Option "XkbLayout" "us,ru"`:

```
Section "InputClass"
        Identifier "system-keyboard"
        MatchIsKeyboard "on"
        Option "XkbLayout" "us,ru"
        Option "XkbVariant" ","
        Option "XkbOptions" "grp:alt_shift_toggle"
EndSection
```

Как проверить сертифицированность ОС?

Для проверки необходимо воспользоваться нашими инструкциями:

- для РЕД ОС 7.3:

- Контроль целостности системы;
- Сбор диагностической информации о РЕД ОС (loginfo).

- для РЕД ОС 8:
  - Контроль целостности системы;
  - Сбор диагностической информации о РЕД ОС (loginfo).

Описание программного продукта

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

РЕД Виртуализация позволяет управлять виртуальными машинами через веб-интерфейс, используя для администрирования библиотеку **libvirt**.

В состав *РЕД Виртуализации* входит реализация веб-интерфейса и служб, необходимых для управления виртуальными машинами. *РЕД Виртуализация* представляет собой образ ОС на основе РЕД ОС, в состав которого включены необходимые пакеты и репозиторий для установки и функционирования системы виртуализации.

РЕД Виртуализация позволяет создавать масштабируемую кластерную систему виртуализации с распределенной системой контроля ресурсов оборудования и полномочий пользователей.

Функции управления виртуальными машинами включают в себя выбор приоритета высокой доступности, живую миграцию, мгновенные снимки в реальном времени, клонирование виртуальных машин из моментальных снимков, создание шаблонов виртуальных машин, использование **cloud-init** для автоматической настройки во время подготовки и развертывания виртуальных машин. Поддерживаемые гостевые операционные системы включают *GNU / Linux*, *Microsoft Windows* и *FreeBSD*.

РЕД Виртуализация представляет собой программный продукт, состоящий из следующих компонентов:

- программные средства, предназначенные для установки на аппаратный сервер: гипервизор, базовую операционную систему, вспомогательные компоненты и утилиты;
- система управления виртуализацией *РЕД Виртуализация*;
- документация;
- драйверы паравиртуализации;
- клиентская часть для ОС Windows (версий от XP SP3 и выше);
- инструментарий для построения отчётов по журналам событий;
- утилиты и служебные программы;
- подсистема идентификации и аутентификации.

Документация

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

База знаний по **РЕД Виртуализации** периодически дополняется статьями, которые не были включены в основную документацию.

Полная и актуальная документация включает в себя следующие руководства:

- Руководство по установке и первичной настройке;
- Руководство по администрированию РЕД Виртуализации;
- Руководство по администрированию виртуальных машин РЕД Виртуализации;
- Руководство по созданию и восстановлению резервных копий системы управления РЕД Виртуализация.

Аппаратная часть

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Минимальные и рекомендуемые требования к оборудованию, описанные здесь, основаны на типичной установке малого и среднего размера. Точные требования по конкретной конфигурации различаются в разных случаях в зависимости от её размера и нагрузки.

Требования к оборудованию указаны в таблице 1.

Таблица 1. Минимальные и рекомендуемые требования к оборудованию

Конфигурация	Минимальная	Рекомендуемая
Процессор	Двухядерный процессор	Четырехъядерный процессор или несколько двухъядерных процессоров
Оперативная память	16 Гб установленной оперативной памяти	32 Гб установленной оперативной памяти
Жесткий диск	80 Гб доступного дискового пространства	100 Гб доступного дискового пространства
Сетевой интерфейс	1 сетевой интерфейс с пропускной способностью 1 Гбит/с	1 сетевой интерфейс с пропускной способностью 10 Гбит/с

Минимальных и рекомендуемых требований достаточно только для установки системы виртуализации, в которой управляющее ядро engine расположено непосредственно на хосте виртуализации. Дальнейшая работа системы виртуализации требует дополнительных ресурсов, в случае запуска кластера – отдельного сетевого хранилища.

Для расчета дополнительных ресурсов необходимых для работы системы виртуализации можно использовать следующие базовые единицы:

- 1 физическое ядро на каждую виртуальную машину;
- 4 ГБ оперативной памяти на каждую виртуальную машину;
- 30 ГБ свободного дискового пространства для каждой виртуальной машины.

При организации кластера необходимо подключать сетевое хранилище отдельным сегментом высокоскоростной сети.

ВАЖНО!

Для корректной работы РЕД Виртуализации требуется:

- физический сервер (установка РЕД Виртуализации в виртуальной машине также возможна, но не гарантируется ее корректная работа);
- готовое хранилище (программное или аппаратное);
- во время установки должен быть подключен только один сетевой интерфейс, управление которым будет передано гипервизору РЕД Виртуализации.

Аппаратное и программное оснащение клиентов

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Доступ к управлению виртуальными машинами можно получить с помощью веб-браузера. Имеется **портал администрирования** и **портал виртуальных машин**. Рекомендуется использовать одну из последних версий **Mozilla Firefox** или **Chromium**.

Доступ к консолям виртуальных машин можно получить с помощью поддерживаемых клиентов удаленного просмотра (**Virtual viewer**) в системах Linux и Windows. Рекомендуется использовать протокол **SPICE**. SPICE в настоящее время поддерживает максимальное разрешение **2560x1600** пикселей.

Для доступа к виртуальным машинам с терминальных клиентов используется специальный клиент, поставляемый в комплекте с программным обеспечением.

Гипервизор

Центральный процессор
Оперативная память
Жёсткие диски
PCI устройства
Требования к назначению устройств
Требования к vGPU
Требования к сети

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Центральный процессор

Все процессоры должны иметь поддержку расширений процессоров **Intel® 64** или **AMD64**, а также включенные расширения аппаратной виртуализации **AMD-V™** или **Intel VT®**. Также требуется поддержка настройки **No eXecute** (NX).

Поддерживаются следующие модели процессоров **AMD**:

- Opteron G1-G5;
- EPYC.

Поддерживаются следующие модели процессоров **Intel**:

- Nehalem;
- Westmere;
- SandyBridge;
- IvyBridge;
- Haswell;
- Broadwell;
- Cascadelake;
- Skylake;
- Icelake.

Поддерживаются следующие модели процессоров **AArch64**:

- Huawei Kunpeng 920.

Проверка, поддерживает ли процессор требуемые флаги, приведена далее.

Необходимо включить виртуализацию в BIOS, выключите питание и перезагрузите хост после этого изменения, чтобы убедиться, что оно применено. Далее:

1. Загрузитесь в операционную систему и зарегистрируйтесь под пользователем, имеющим административные права;

2. В командной строке определите, что ваш процессор имеет необходимые расширения и что они включены, выполнив эту команду:

```
grep -E 'svm|vmx' /proc/cpuinfo
```

Если отображается какой-либо вывод, то процессор поддерживает аппаратную виртуализацию. Если выходные данные не отображаются, процессор может по-прежнему поддерживать аппаратную виртуализацию, но она заблокирована в BIOS. Обратитесь к BIOS системы и руководству по материнской плате, предоставленному производителем.

Оперативная память

Минимальная необходимая оперативная память - **8 ГБ**. Максимальная поддерживаемая оперативная память составляет **4 ТБ**.

Однако объем требуемой оперативной памяти зависит от требований гостевой операционной системы, требований гостевых приложений, активности и использования гостевой памяти. **KVM** также может перерасходовать физическую оперативную память для виртуальных пользователей, позволяя вам предоставлять таким пользователям требования к оперативной памяти, превышающие те, что физически присутствуют, при условии, что пользователи не все работают одновременно при пиковой нагрузке. *KVM* делает это, только выделяя ОЗУ для пользователей по мере необходимости и перемещая контент неактивных пользователей в **swap** (файл подкачки, расположен на локальном физическом носителе хоста).

Жёсткие диски

Хосты требуют локального хранилища для хранения конфигурации, журналов, дампов ядра и для использования в качестве пространства подкачки.

Это минимальные требования к хранилищу для установки хоста РЕД Виртуализации. Мы рекомендуем использовать значения, превышающие те, что указаны ниже:

- /(root) - **6 ГБ**;
- /home - **1 ГБ**;
- /tmp - **1 ГБ**;
- /boot - **1 ГБ**;
- /var - **15 ГБ**;
- /var/crash - **10 ГБ**;
- /var log - **8 ГБ**;
- /var/log/audit- **2 ГБ**;
- swap - **1 ГБ**;
- резерв **20%** размера пула в группе томов для будущего расширения метаданных.

Минимальный общий объем - **75 ГБ**.

PCI устройства

Хосты должны иметь по крайней мере один сетевой интерфейс с минимальной пропускной способностью **1 Гбит/с**. Рекомендуется, чтобы каждый узел имел два сетевых интерфейса с одним выделенным для поддержки интенсивных сетевых действий, таких как миграция виртуальных машин. Производительность таких операций ограничена доступной пропускной способностью.

Требования к назначению устройств

Если вы планируете реализовать назначение устройств и передачу данных **PCI**, чтобы виртуальная машина могла использовать определенное устройство **PCI-e** с хоста, убедитесь, что выполнены следующие требования:

1. Процессор должен поддерживать **IOMMU** (например, VT-d или AMD-Vi);

2. Прошивка должна поддерживать перепрошиваемый модуль и использование IOMMU;

3. Корневые порты процессора должны поддерживать ACS или ACS-эквивалентные возможности;

4. PCI-e устройства должны поддерживать ACS или ACS-эквивалентные возможности.

Рекомендуется, чтобы все коммутаторы PCI-e и мосты между устройством PCI-e и корневым портом поддерживали ACS. Например, если коммутатор не поддерживает ICS, все устройства за этим коммутатором используют одну и ту же группу IOMMU и могут быть назначены только одной виртуальной машине.

Для поддержки графических процессоров используется назначение устройств PCI для **NVIDIA K-Series Quadro** (модель 2000 серии или выше), **GRID** и **Tesla** на основе PCIe в качестве графических устройств без **VGA**. В настоящее время к виртуальной машине может быть подключено до двух графических процессоров в дополнение к одному из стандартных эмулируемых интерфейсов VGA. Эмулируемая VGA используется для предварительной загрузки и установки, а графический процессор NVIDIA начинает работать после загрузки графических драйверов NVIDIA. Обратите внимание, что **NVIDIA Quadro 2000** не поддерживается, равно как и карта **Quadro K420**.

Требования к vGPU

Если вы планируете настроить узел, чтобы разрешить виртуальным машинам на этом узле устанавливать **vGPU**, необходимо выполнить следующие требования:

1. vGPU-совместимый графический процессор;

2. Ядро хоста с поддержкой GPU;

3. Установленный графический процессор с драйверами;

4. Предварительно заданный тип mdev_type соответствует одному из типов mdev, поддерживаемых устройством;

5. Драйверы с поддержкой vGPU, установленны на каждом узле кластера;

6. vGPU-поддерживается операционной системой виртуальной машины с установленными графическими драйверами.

Требования к сети

Система управления и все хосты должны иметь **полное доменное имя** и **полное прямое и обратное разрешение имен**. Настоятельно рекомендуется использовать **DNS**; использование файла **/etc/hosts** для разрешения имен обычно требует больше работы и большую вероятность ошибки.

Из-за широкого использования DNS в среде «РЕД Виртуализация» запуск службы DNS в качестве виртуальной машины, размещенной в среде, не поддерживается. Все службы DNS, используемые средой «РЕД Виртуализация» для разрешения имен, должны размещаться вне этой среды.

Хранилище

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

«РЕД Виртуализация» использует централизованную систему хранения для образов дисков виртуальных машин, файлов ISO и снимков. Сеть хранения данных может быть реализована с использованием:

- сетевой файловой системы **NFS**;
- **GlusterFS**;
- других POSIX-совместимые файловые системы;
- **iSCSI**;
- протокола Fibre Channel (**FCP**);
- параллельной NFS (**pNFS**).

Настройка хранилища является обязательным условием для нового центра обработки данных, поскольку центр обработки данных не может быть инициализирован, если домены хранения не подключены и не активированы.

Ограничения РЕД Виртуализации

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

На основе тестирования производительности РЕД Виртуализации как крупномасштабной среды определены также **максимальные рекомендуемые значения** для системы.

Для логических объектов РЕД Виртуализации предусмотрены следующие **ограничения**:

- *Дата-центр*:
  - максимальное количество одновременно работающих виртуальных машин на одном Engine с несколькими центрами обработки данных: **4000**;
  - максимальное количество центров обработки данных: **400**;
  - максимальное количество хостов: **250** на один центр обработки данных;
  - максимальное количество ВМ: **4000**.

- *Кластер*:
  - максимальное количество кластеров: **400** (400 кластеров в одном центре обработки данных либо по одному кластеру в каждом из 400 центров обработки данных);
  - максимальное количество ВМ: **4000**.

- *Сеть*:
  - на один хост: **200**;
  - на один кластер: **300**;
  - максимальное общее количество сетей: **100** на 150 хостах либо **60** на кластер с 250 хостами.

- *Место хранения*:
  - максимальное количество доменов на центр обработки данных: **50**. Однако каждый дополнительный домен хранения может приводить к некоторому снижению производительности.

    Рекомендуется использовать только необходимое для работы количество доменов хранения.
  - количество хостов на домен: **без ограничений**;
  - логических томов на блочный домен: **1500**;
  - максимальное количество LUN: **300**;
  - максимальный размер диска: **500 ТБ** (по умолчанию ограничен размером **8 ТБ**).

- *Хосты*:
  - максимальное количество хостов: **400**;
  - количество хостов на один центр обработки данных: **250**.

- *Виртуальные машины* (ВМ):
  - максимальное количество ВМ: **4000**.

  Общее количество ВМ зависит от оборудования хоста и потребляемых ресурсов.

Подготовка сетевого хранилища: NFS

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Чтобы **Engine** мог хранить данные в доменах хранения, представленных экспортируемыми каталогами, в них должны быть определенные учетные записи системных пользователей и их группы.

Дальнейшие действия выполняются на сервере с операционной системой РЕД ОС, который используется в качестве сетевого хранилища данных.

Если не установлен пакет NFS, его необходимо установить командой:

```
dnf install nfs-utils nfs4-acl-tools
```

Приведенная ниже процедура устанавливает разрешения для одного каталога (в примере **/data**). Вам необходимо повторить chown и chmod шаги для всех каталогов, которые вы собираетесь использовать в качестве доменов хранения в РЕД Виртуализации.

1. Создайте каталог **data**:

```
mkdir /data
```

2. Создайте группу **kvm**:

```
groupadd kvm -g 36
```

3. Создайте пользователя **vdsm** в группе **kvm**:

```
useradd vdsm -u 36 -g 36
```

4. Установите право собственности на экспортированный каталог на **36:36**, что дает **vdsm:kvm** право владения:

```
chown -R 36:36 /data
```

5. Измените режим каталога, чтобы права на чтение и запись были предоставлены владельцу, а права на чтение и выполнение были предоставлены группе и другим пользователям:

```
chmod 0755 /data
```

6. Все настройки сервера хранятся в файле **/etc/exports**. Откройте его на редактирование:

```
nano /etc/exports
```

и добавьте в конец файла строки вида (строк может быть произвольное количество):

```
/data 192.168.1.1/255.255.255.0(rw,insecure,nohide,all_squash,anonuid=36,anongid=36,no_subtree_check)
```

где:

- **/data** – путь к папке, для которой раздается доступ;
- **192.168.1.1** – IP-адрес, которому раздается доступ к папке (можно указать всю сеть, тогда запись примет вид **192.168.1.0/24**).

Чтобы запустить службу и добавить её в автозагрузку, выполните команду:

```
systemctl enable nfs-server.service --now
```

Примечание.

Если в системе, где происходит развёртывание хранилища **NFS** установлен и запущен **firewall**, внесите в него необходимые изменения:

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=mountd
```

```
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

Установка в режиме Standalone

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

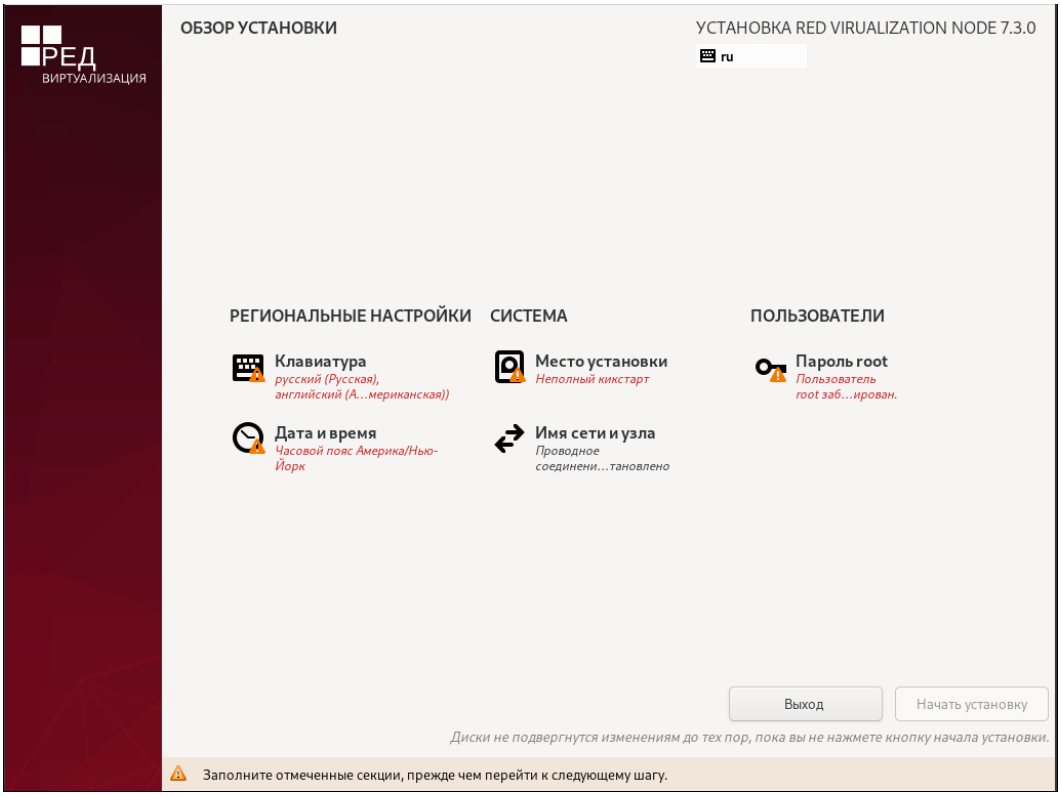
Примечание.

При установке в режиме **standalone** расширение до кластера невозможно.

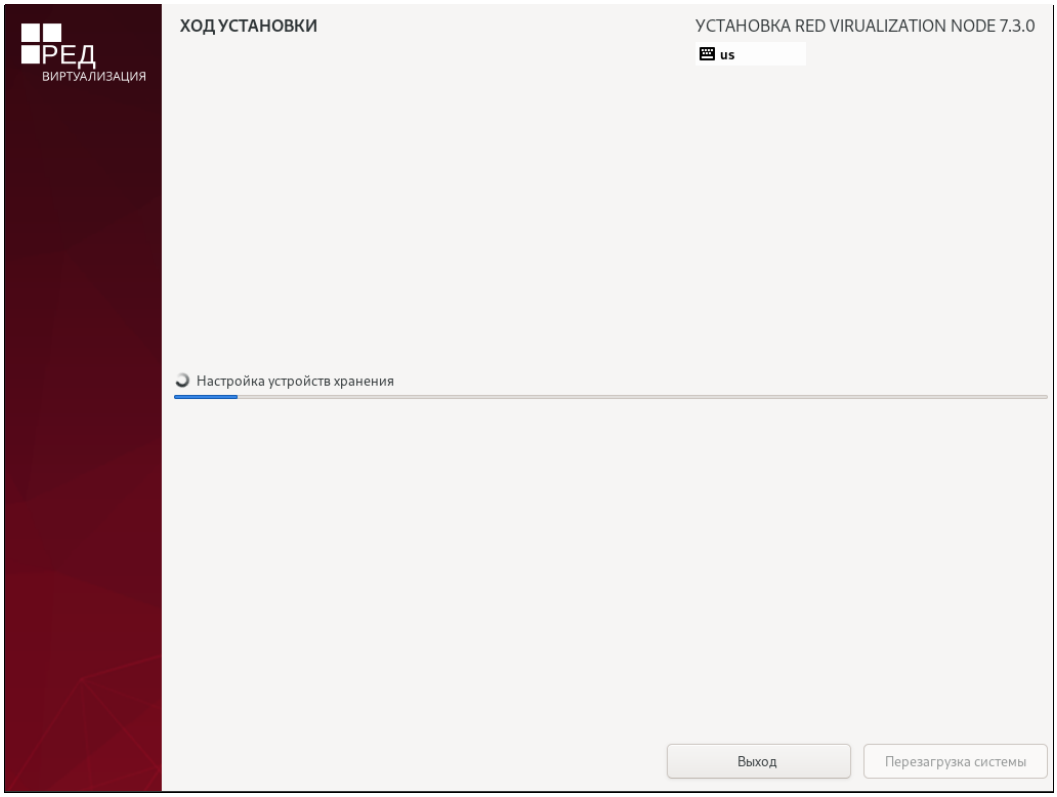
Для установки РЕД Виртуализации в режиме **standalone** после загрузки образа в меню установщика необходимо выбрать пункт «**Install RED Virtualization 7.3.0 Standalone Engine**».



Откроется стандартное окно установки РЕД Виртуализации, в котором необходимо настроить раскладку клавиатуры, установить дату и часовой пояс, выбрать устройства для установки системы виртуализации, активировать соединение с сетью и задать имя узла, а также задать пароль администратора **root**. Подробнее о необходимых настройках см. в статье «Установка РЕД Виртуализации в режиме Host».

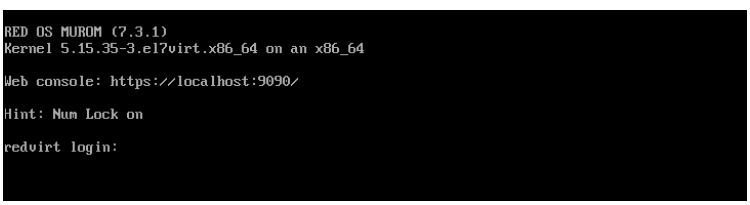


После определения всех необходимых настроек начинается этап установки РЕД Виртуализации. После данного шага программа установки будет работать с файлами только что установленной базовой системы.



После выполнения копирования файлов и настройки компонентов, пользователю будет предложено произвести перезагрузку кнопкой «**Перезагрузить систему**».

Затем откроется терминал установленной системы.



Далее необходимо настроить среду управления виртуализацией. Для этого войдите в систему под учетной записью **root**. Затем создайте каталог для хранилища и назначьте необходимые разрешения:

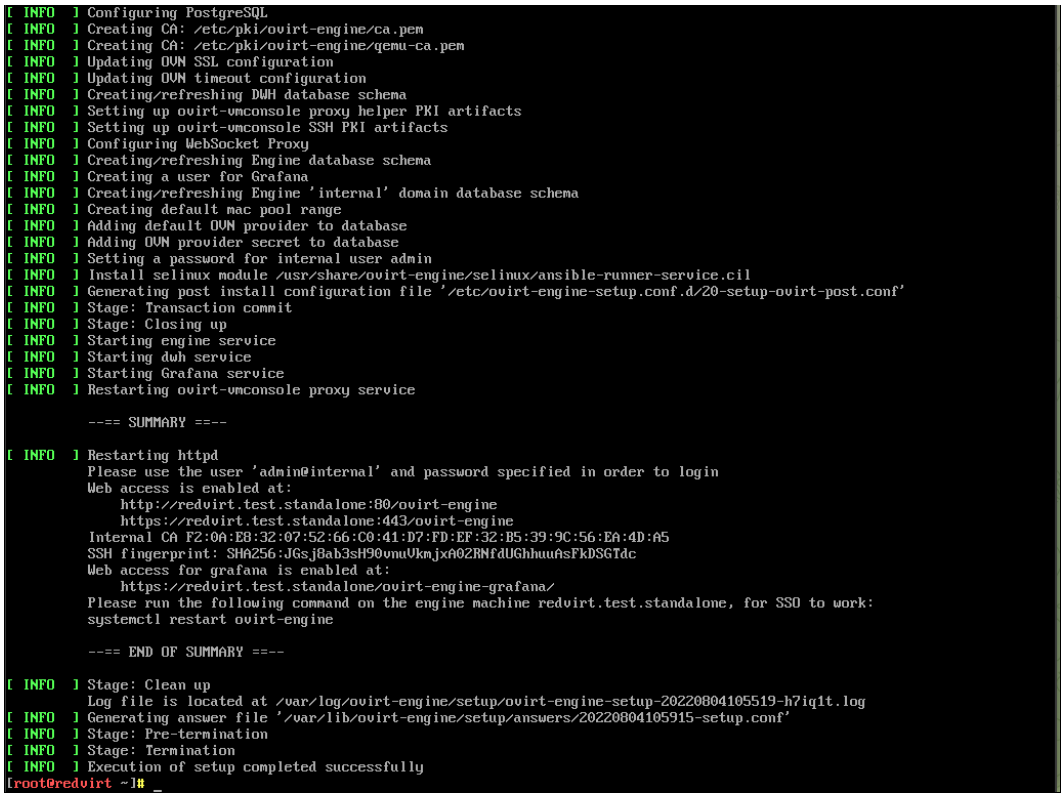
```
mkdir -p /srv/data
chown 36:36 /srv/data
chmod 0755 /srv/data
```

Далее запустите команду конфигурирования среды виртуализации:

```
engine-setup --accept-defaults
```

На запрос «**Engine admin password**» введите пароль администратора системы виртуализации, затем нажмите **Enter** и подтвердите его. Пароль должен иметь длину не менее 8 символов и содержать буквы, цифры и знаки.

После выполнения всех вышеуказанных действий будет произведена настройка среды управления виртуализацией.



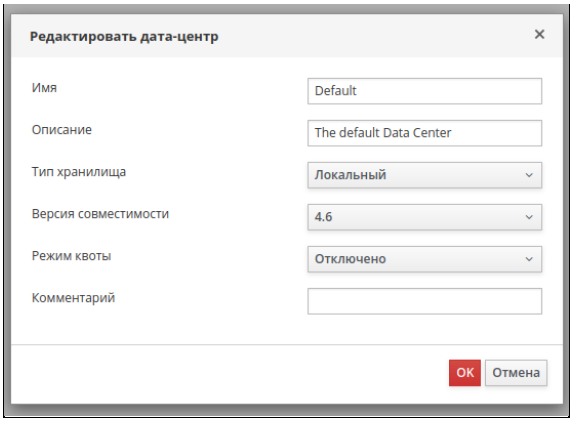
Затем необходимо произвести настройку возможности загрузки виртуальных дисков и iso-образов в систему РЕД Виртуализации. Для этого выполните команды:

```
engine-config -s ImageTransferProxyEnabled=false
systemctl restart ovirt-engine
```

Теперь система управления средой виртуализации доступна для запуска в веб-интерфейсе.

После успешной авторизации на веб-портале необходимо настроить хранилище. Перейдите в настройки дата-центра для включения возможности добавления локальных хранилищ.

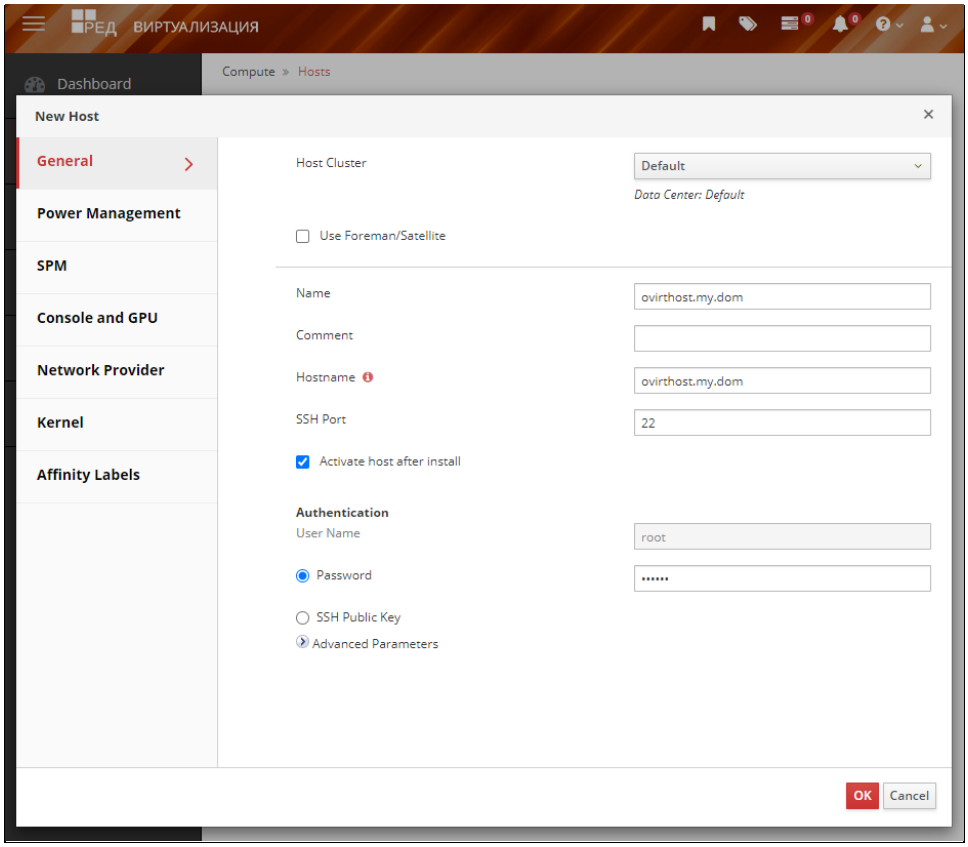
Откройте «**Виртуализация**» - «**Дата-центры**», нажмите «**Редактировать**» и в поле «**Тип хранилища**» выберите «**Локальный**». Нажмите «**ОК**».



Далее необходимо создать вычислительный хост.

Для этого откройте «**Виртуализация**» - «**Узлы**» и нажмите кнопку «**Новый**». В открывшемся окне в полях «**Name**» и «**Hostname**» впишите имя машины, на которую производится установка. В примере это **ovirthost.my.dom**.

В поле «**Password**» впишите действующий пароль **root**-пользователя. Нажмите «**OK**».

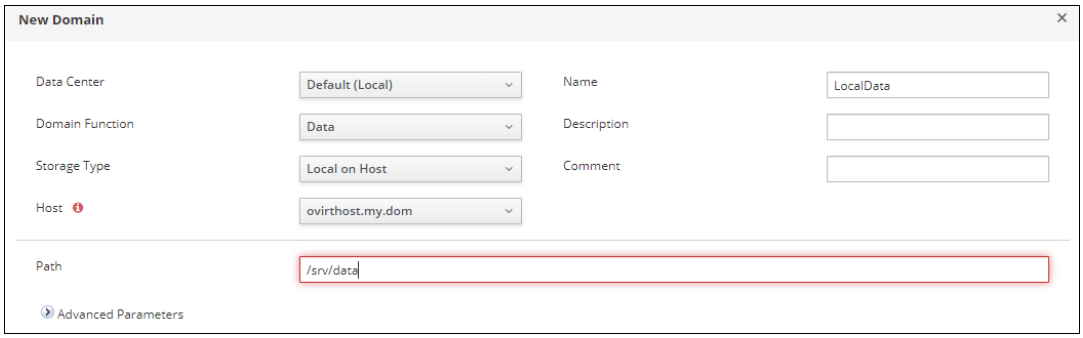


На вопрос «**You haven't configured Power Management for this Host. Are you sure you want to continue?**» нажмите «**OK**». Вы можете настроить политику питания позже.

Далее начнется настройка хоста, следить за процессом настройки можно, нажав на создаваемый хост и выбрав вкладку «**Events**».

После успешного запуска хоста создайте локальный домен хранения.

Откройте «**Хранилище**» - «**Домен**» и нажмите кнопку «**Новый**». В открывшемся окне в поле «**Name**» впишите имя создаваемого домена, например, «**Local**». В поле «**Storage Type**» выберите «**Local on Host**». В поле «**Path**» впишите **путь** к каталогу, который вы указывали ранее в командах консоли. Нажмите «**OK**».


New Domain
Data Center
Default (Local)
Name
LocalData
Domain Function
Data
Description
Storage Type
Local on Host
Comment
Host
ovirthost.my.dom
Path
/srv/data
Advanced Parameters

Установка в режиме Host

Подготовка к установке
Последовательность установки
Язык системы
Обзор установки
Клавиатура
Расположение установки
Задание пароля администратора системы
Дата и время
Сеть и имя узла
Установка системы виртуализации

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Подготовка к установке

Для выполнения установки у Вас должен быть дистрибутив РЕД Виртуализации 7.3.

Оборудование должно соответствовать требованиям, описанным в разделе «Системные требования».

Подключите дистрибутив к одному из хостов и загрузитесь в программу установки, выбрав носитель дистрибутива в качестве загружаемого устройства.

Последовательность установки

Программа установки РЕД Виртуализации работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования хоста завершилась успешно, будет запущен графический интерфейс программы-установщика (anaconda). Процесс установки реализован в виде «мастера» установки, представляющий из себя интерактивный графический интерфейс, в котором пользователю предлагается отвечать на вопросы и указывать необходимые опции установки. Мастер установки разделен на шаги, каждый шаг посвящен настройке или установке определенного сервиса системы.

Если по каким-то причинам возникла необходимость прекратить установку, выполните **Reset** на хосте. Помните, что совершенно безопасно прекращать установку только до нажатия кнопки «**Установить**», поскольку до этого момента не производится никаких изменений на жестком диске.

Технические сведения о ходе установки можно посмотреть, нажав **Ctrl+Alt+F1**, вернуться к программе установки - **Ctrl+Alt+F7**. По нажатию **Ctrl+Alt+F2** откроется отладочная виртуальная консоль.

Во время установки РЕД ОС выполняются следующие шаги:

- Установка предпочитаемой раскладки клавиатуры;
- Выбор типа накопителя хоста и подготовка разделов диска;
- Задание пароля администратора системы;
- Выбор часового пояса и установка даты и времени;
- Присвоение имени компьютера в сети и настройка сетевых интерфейсов;
- Сохранение настроек;
- Установка системы;
- Установка загрузчика;
- Перезагрузка системы;
- Завершение установки.

Язык системы

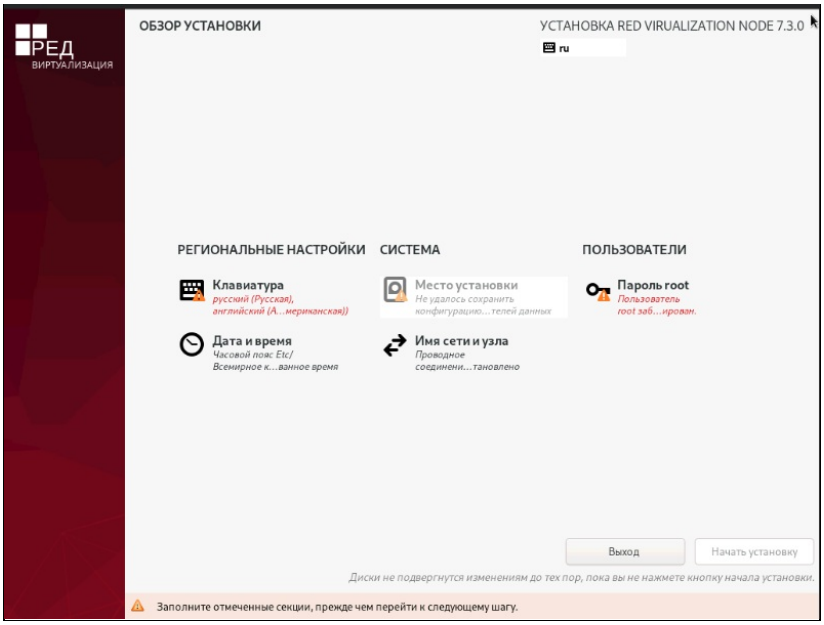
Язык интерфейса программы установки и графического интерфейса устанавливаемой системы виртуализации по умолчанию русский, не конфигурируется и не изменяется в процессе установки. Дополнительным языком является английский язык. Другие дополнительные языковые пакеты можно установить из репозитория после завершения установки системы.

Переключение раскладки клавиатуры при установке системы виртуализации выполняется нажатием комбинации функциональных клавиш **Alt** и **Shift** одновременно.

Обзор установки

После выбора языка необходимо произвести первоначальную конфигурацию установщика и параметров будущей системы виртуализации.

В этом окне необходимо задать региональные и системные настройки. Здесь и в последующих окнах установщика красным цветом выводятся подсказки у тех вкладок, которые должны быть обязательно заполнены до перехода к следующему шагу установки.



Клавиатура

В окне настройки клавиатуры можно выбрать используемые в системе раскладки.

В отдельном поле ввода можно проверить корректность отображения вводимых символов.

Первая раскладка в списке будет использоваться по умолчанию.

Здесь и далее возврат в предыдущее меню осуществляется с помощью кнопки «**Готово**».

Расположение установки

В меню выбора расположения установки можно выбрать устройство для установки хоста виртуализации.

Переход к этому шагу может занять некоторое время. Время ожидания может быть разным и зависит от производительности хоста, объёма и типов используемых накопителей, количества существующих разделов на них.

На этом этапе подготавливается площадка для установки хоста виртуализации, в первую очередь - выделяется свободное место на диске.

Можно выбрать и использовать профили разбиения диска. Профиль — это шаблон распределения места на диске для установки системы. Можно выбрать:

- создать разделы автоматически;
- настрою разделы;
- дополнительно (Blivet-GUI).

Первый профиль предполагает автоматическое разбиение диска. Будет выбрано оптимальное расположение.

Необратимые изменения разделов на жестком диске требуют подтверждения со стороны пользователя. После подтверждения внесенные изменения сохраняются на жестком диске/дисках хоста.

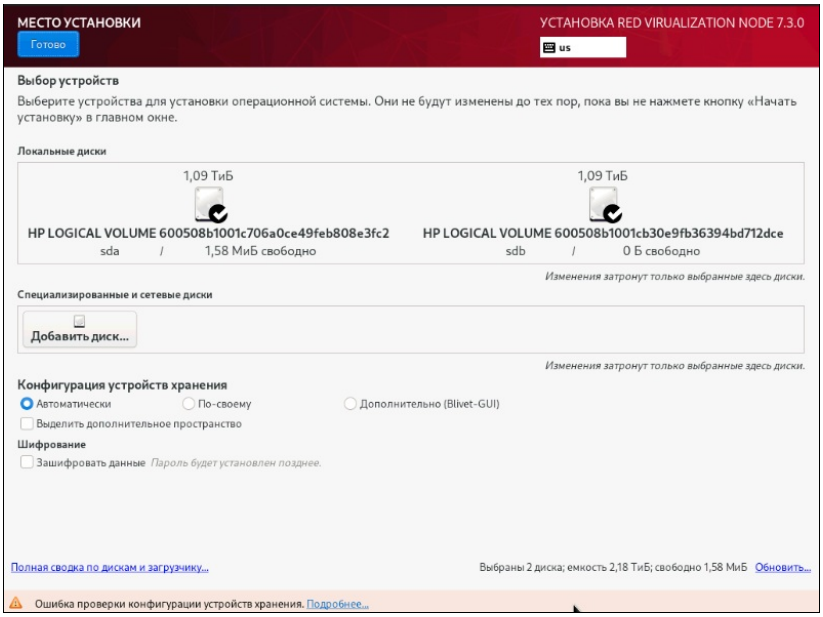
Если для применения одного из профилей автоматической разметки доступного места окажется недостаточно, будет выведено сообщение о невозможности выполнения операции разбиения диска.

При необходимости освободить часть дискового пространства, следует воспользоваться профилем разбиения вручную. Можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «**Готово**» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке «**Файловая система**».

Не следует форматировать разделы с теми данными, которые необходимо сохранить, например, с пользовательскими данными (/**home**). С другой стороны, отформатировать можно любой раздел, который необходимо «очистить» (т.е. удалить все данные).

Blivet-gui является обособленной реализацией механизмов управления разделами и дисками, снабжённой привычным интерфейсом в стиле **GParted**. Программа поддерживает управление дисковыми разделами и хранилищами **LVM2** (включая шифрованные разделы LUKS, логические тома и группы томов). Так же как и в **GParted**, изменения в **blivet-gui** применяются не сразу, а после подтверждения внесённого набора изменений.



Задание пароля администратора системы

Далее необходимо настроить пароль локального администратора **root**.

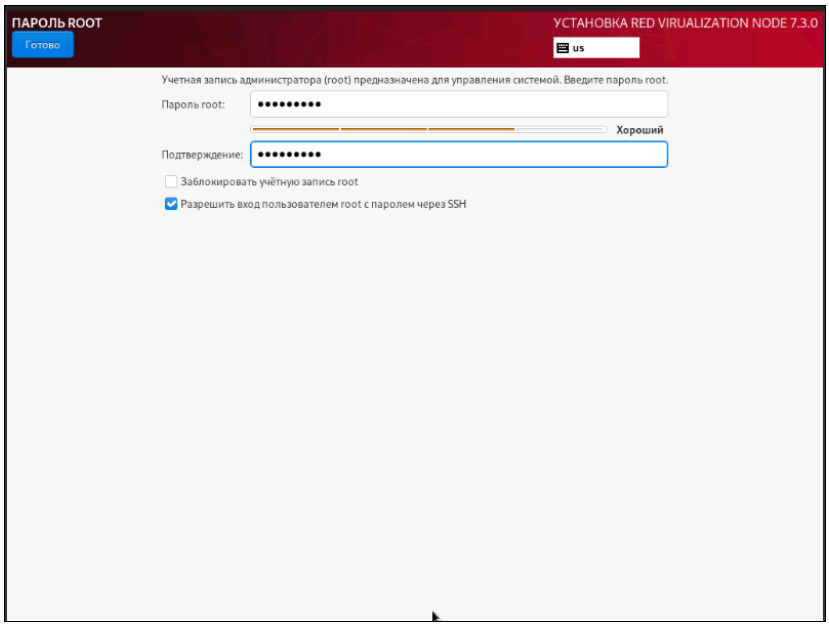
Необходимо запомнить пароль **root** - он необходим для авторизации и управления системой виртуализации.

Ввод пароля защищен, при наборе пароля вместо символов на экране отображаются специальные символы. Чтобы избежать опечатки при вводе пароля, его предлагается ввести дважды. К введенному паролю в режиме реального времени применяется политика сложности пароля, т.е. производится его проверка, и при слишком простом пароле или совпадении пароля с парольной последовательностью из словаря паролей системой будет предложено произвести смену пароля администратора.

ВАЖНО!

В поле «**Разрешить вход пользователем root с паролем через SSH**» должен быть установлен флажок, т.к. дальнейшая установка и настройка системы РЕД Виртуализации использует данную функцию в своей работе. Также данная функция требуется для доступа администратора к терминалу хоста.

Выбор пароля администратора - очень важный момент для безопасности: любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе.



Дата и время

В окне настройки даты и времени можно выбрать текущий регион и город и установить используемое локальное время, дату и формат времени.

Если установлена сеть, и есть доступ к глобальной сети, можно разрешить автоматическую настройку времени с помощью службы **ntp** — сетевое время.

Данную настройку можно изменить после завершения установки. По умолчанию устанавливается часовой пояс **UTC+03:00** (Европа/Москва).

Сеть и имя узла

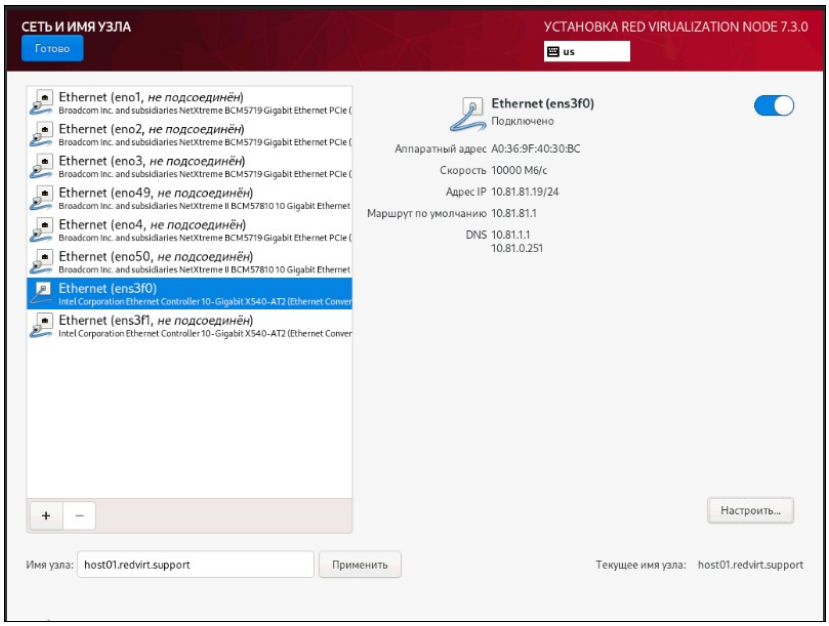
В меню выбора настройки сети можно активировать соединение с сетью и задать имя узла.

На данном этапе необходимо задать имя компьютера в сети (хоста). При наличии сети имя компьютера используется для однозначного определения каждого компьютера. Имя компьютера состоит непосредственно из имени компьютера и имени домена в сети, к которому принадлежит компьютер. Имя компьютера и имя домена разделяются знаком «**.**».

При наличии домена сети имя должно даваться полностью.

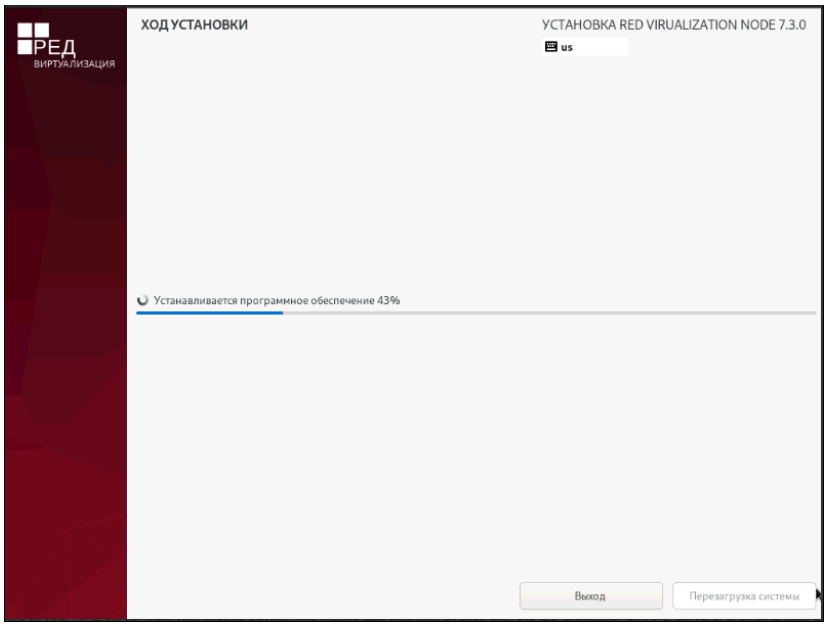
В качестве букв в имени компьютера разрешается только буквы латиницы. В имени компьютера не допускается использование заглавных букв, пробелов и специальных символов.

Также на данном этапе можно сконфигурировать параметры настройки сетевых интерфейсов: автоматическое включение интерфейсов, MAC-адреса сетевых интерфейсов, параметры сетевых протоколов.



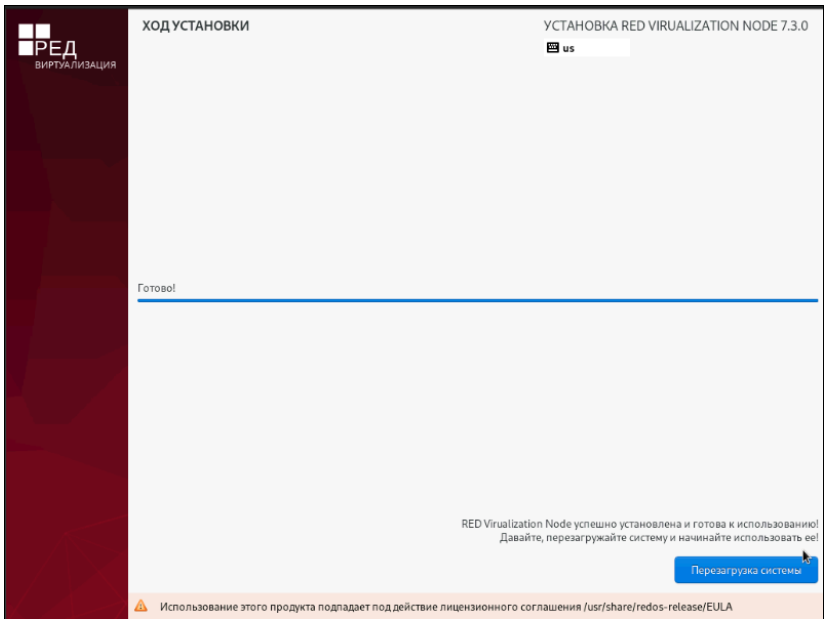
Установка системы виртуализации

После определения всех настроек начинается этап установки РЕД Виртуализации и представляет собой установку набора программ, необходимых для работы среды виртуализации.

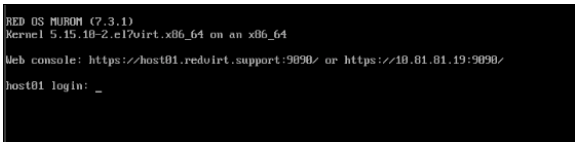


Начиная с этого шага, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить непосредственно на установленной ОС.

После выполнения копирования файлов и настройки компонентов, пользователю предлагается произвести перезагрузку кнопкой «**Перезагрузить систему**».



После перезагрузки откроется терминал установленной системы, где будет указан адрес веб-интерфейса, через который производится установка и настройка системы РЕД Виртуализация.



Примечание.

В случае, если во время установки системы вы по каким-то причинам не указали или указали неверно адрес хоста, необходимо выполнить следующие действия:

1. В открывшемся терминале установленной системы ввести логин (**root**) и *пароль* (созданный на этапе установки) для авторизации на сервере.

2. Установить имя хоста:

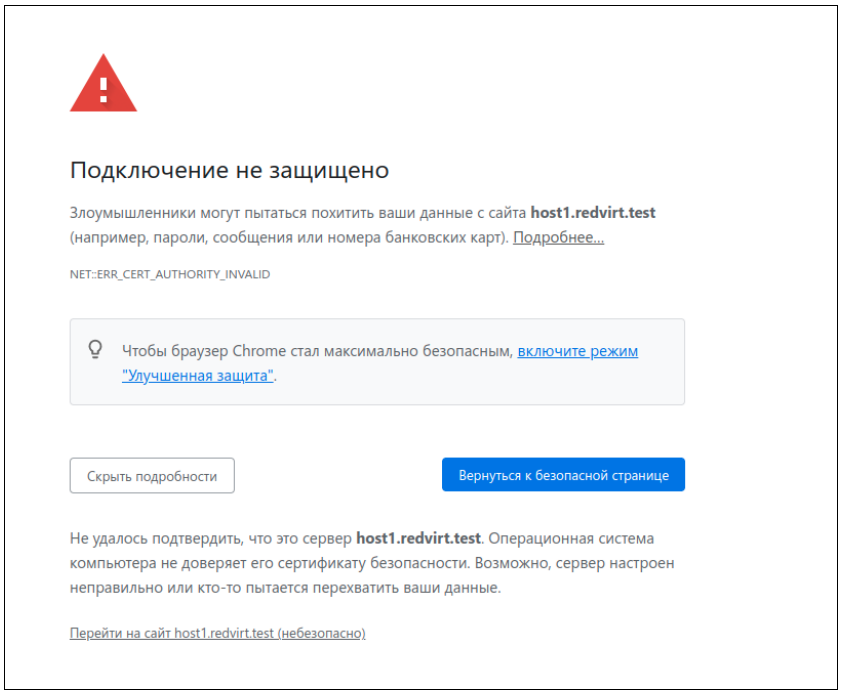
```
hostnamectl set-hostname host1.redvirt.test
```

3. Если DNS-сервер в сети не настроен, то в файле **/etc/hosts** нужно указать ip-адрес и имя будущей виртуальной машины управления системой РЕД Виртуализация. А также внести записи о самом хосте (хостах, если их несколько) и о хранилище.

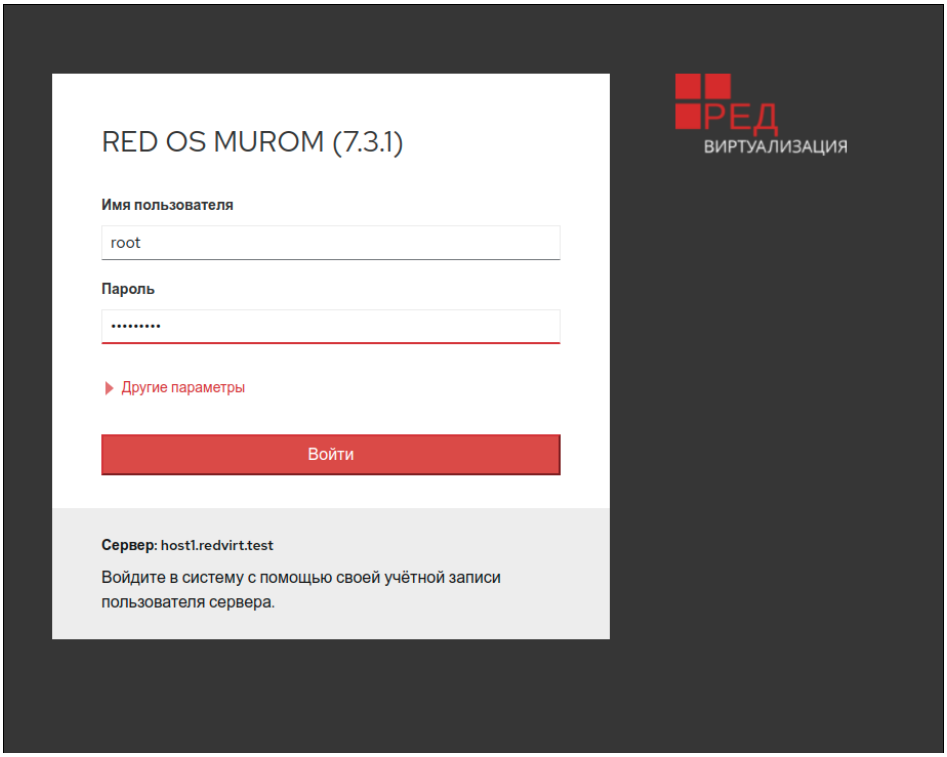
```
192.168.0.43 host1.redvirt.test *Хост*
192.168.0.44 nfs.redvirt.test *NFS-хранилище*
192.168.0.221 redvirt-engine1.test *Гипервизор РЕД Виртуализации*
```

После сохранения данных веб-интерфейс для установки и настройки системы РЕД Виртуализация будет доступен по адресу https://<имя_хоста>:9090 либо https://<IP-адрес_хоста>:9090.

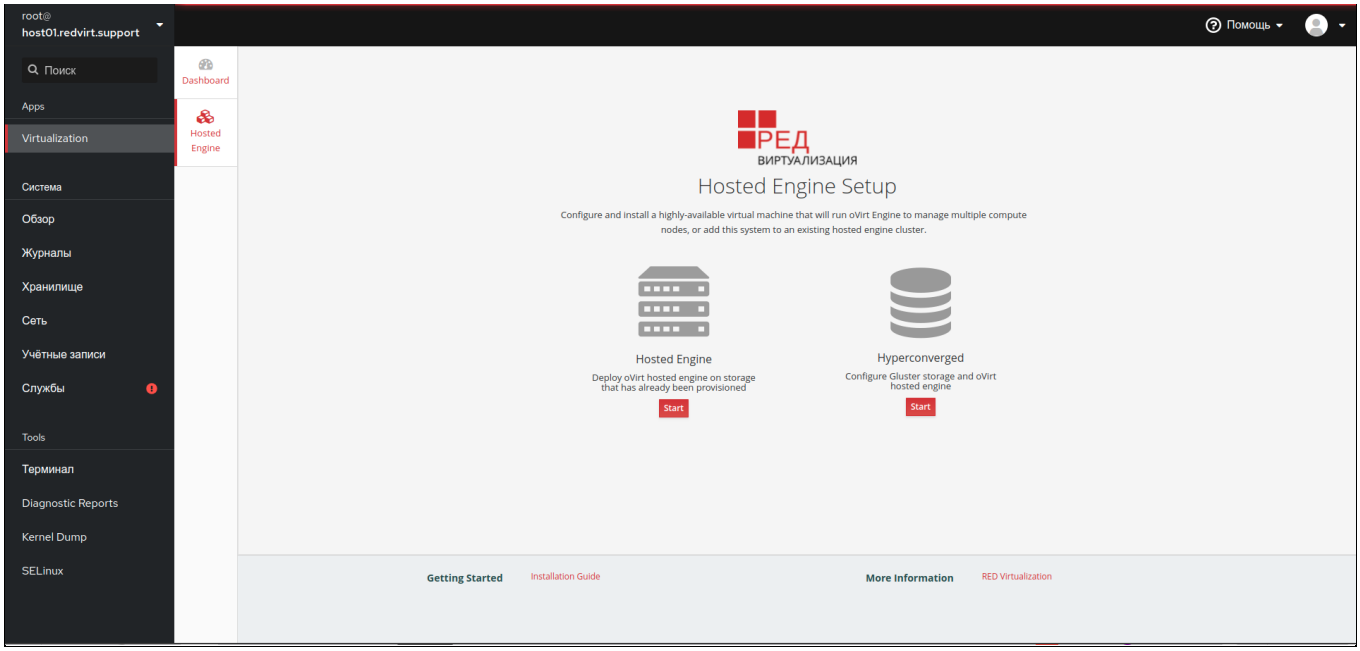
При попытке подключения к серверу будет выведено предупреждение о небезопасном соединении. Нажмите «**Перейти на сайт host1.redvirt.test (небезопасно)**» внизу страницы.



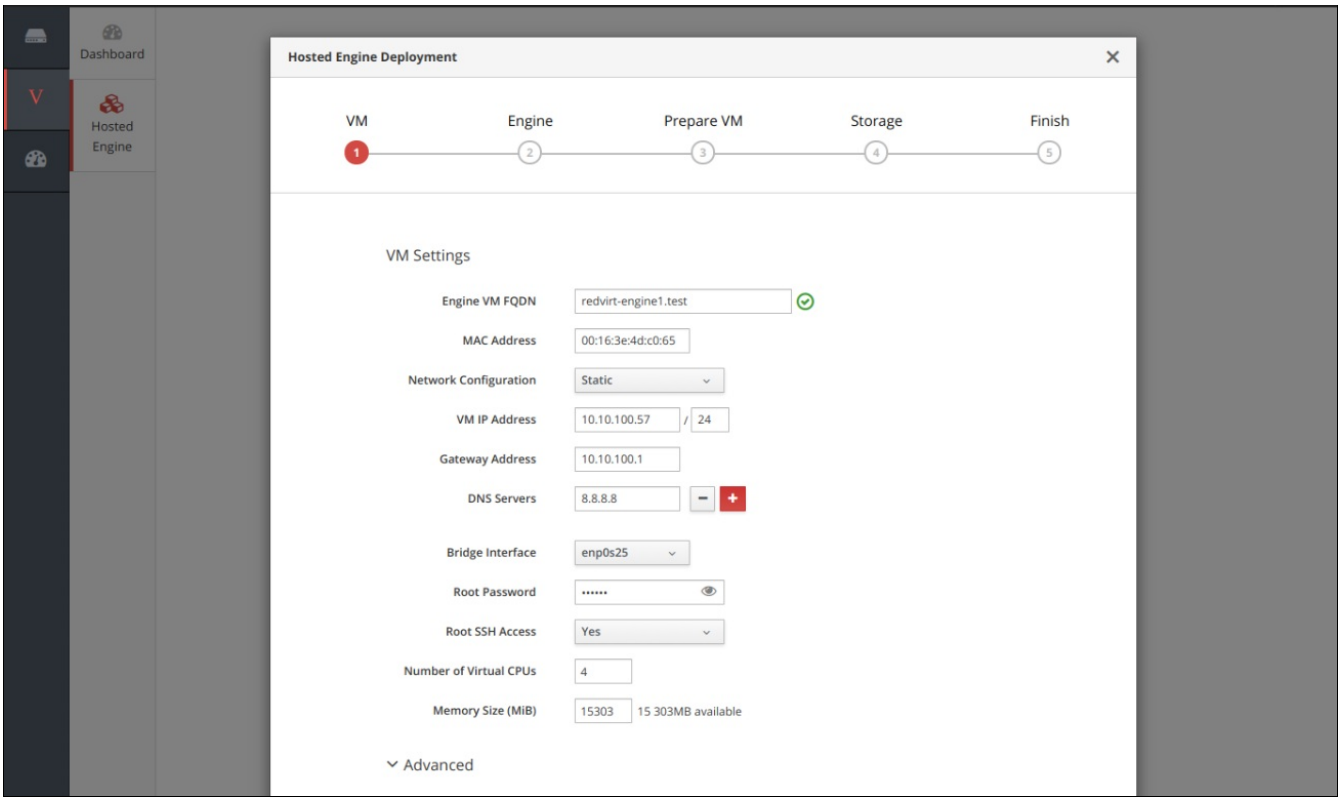
В окне авторизации введите имя пользователя - **root** и *пароль*, который был создан при установке системы.

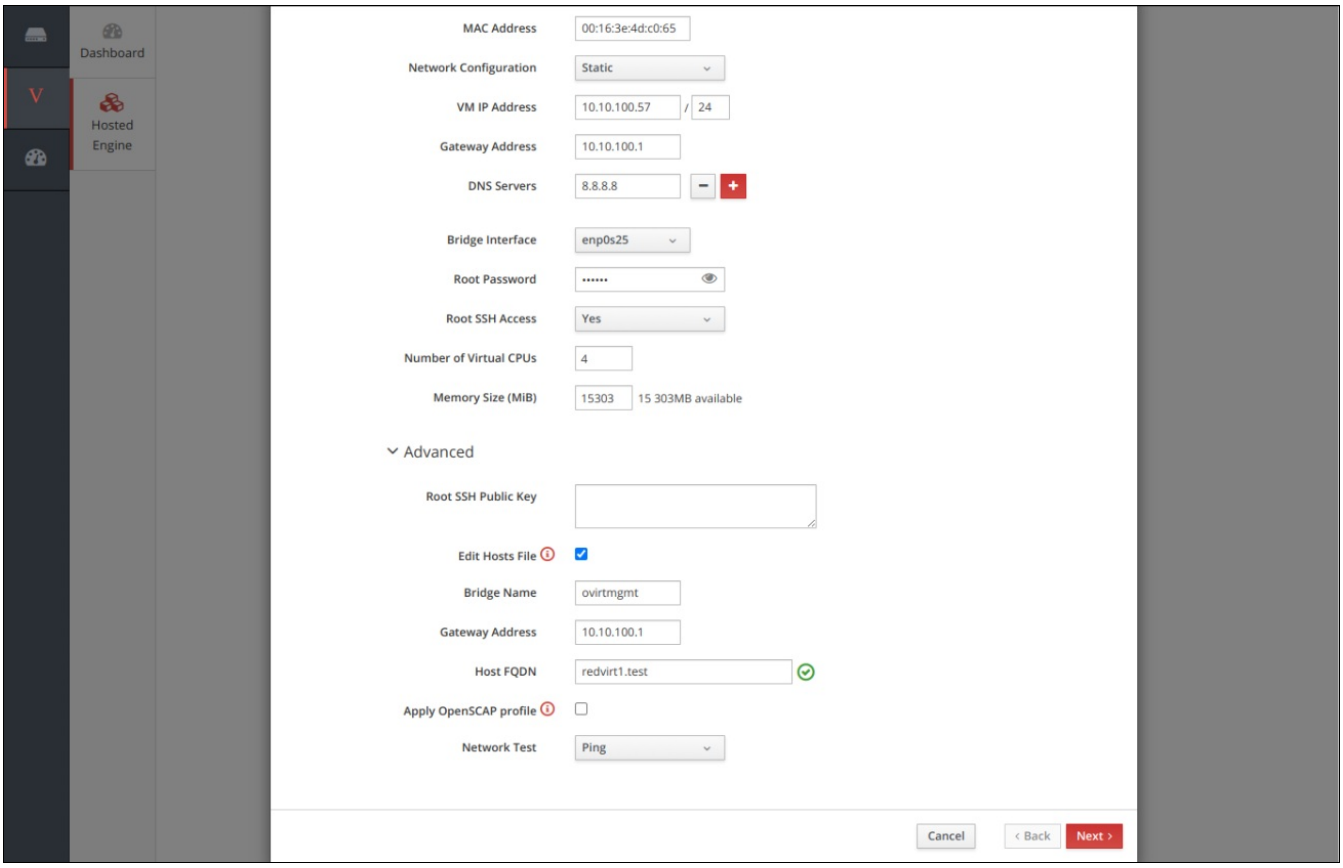


Перейдите во вкладку **Virtualization** – **Hosted Engine**.



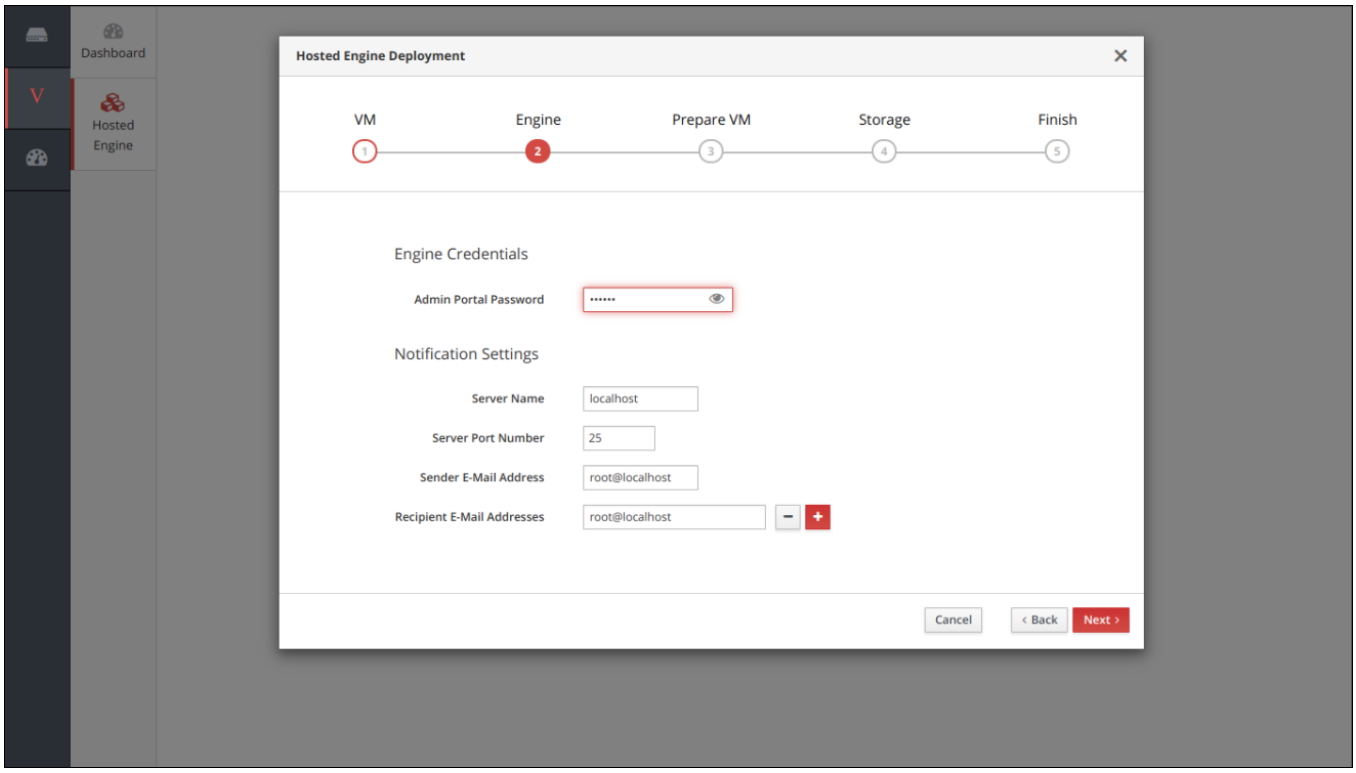
Нажмите **Hosted Engine** – **Start** и заполните поля на вкладке VM в соответствии с вашими параметрами сети.



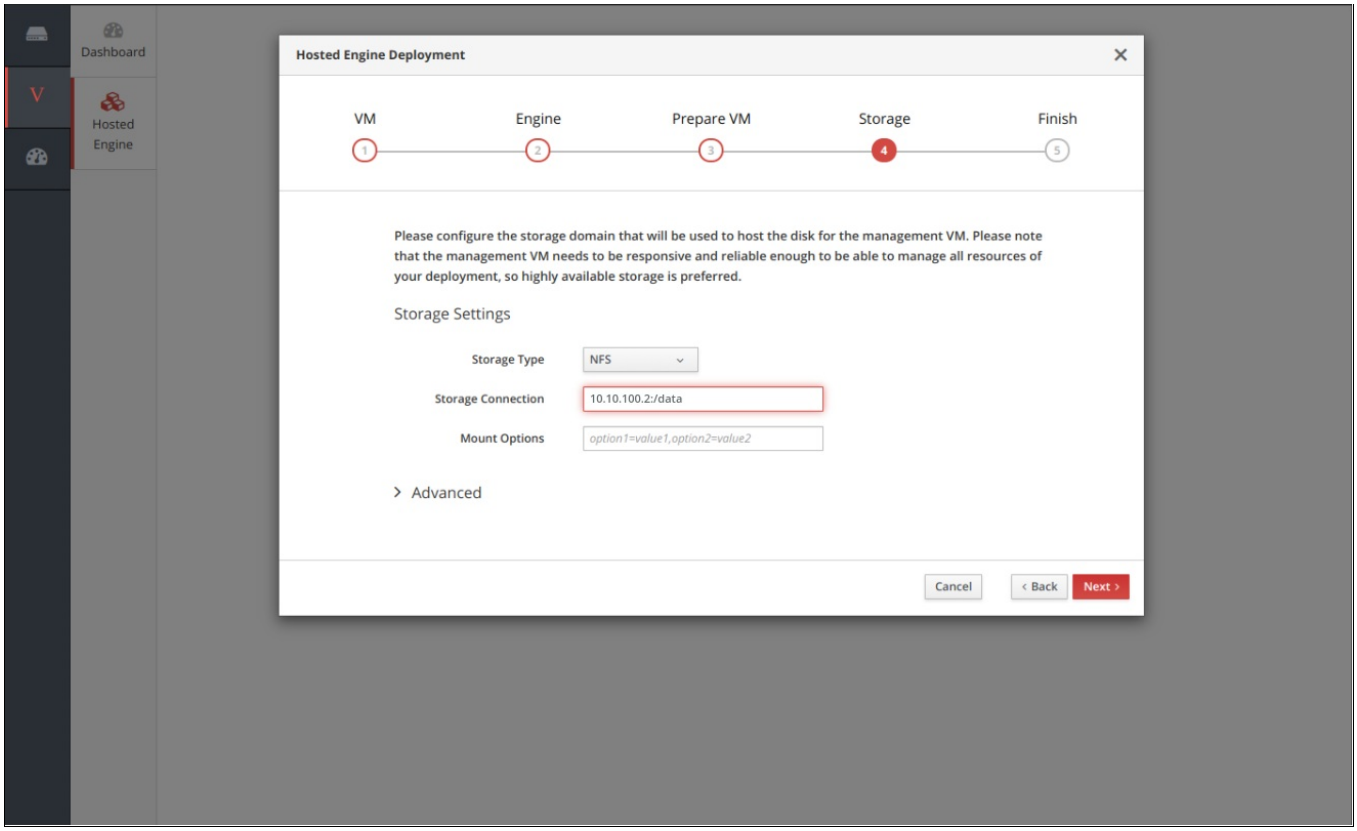


Нажмите **Next**.

Во вкладке **Engine** назначьте пароль администратору портала, а также настройте службу уведомлений.

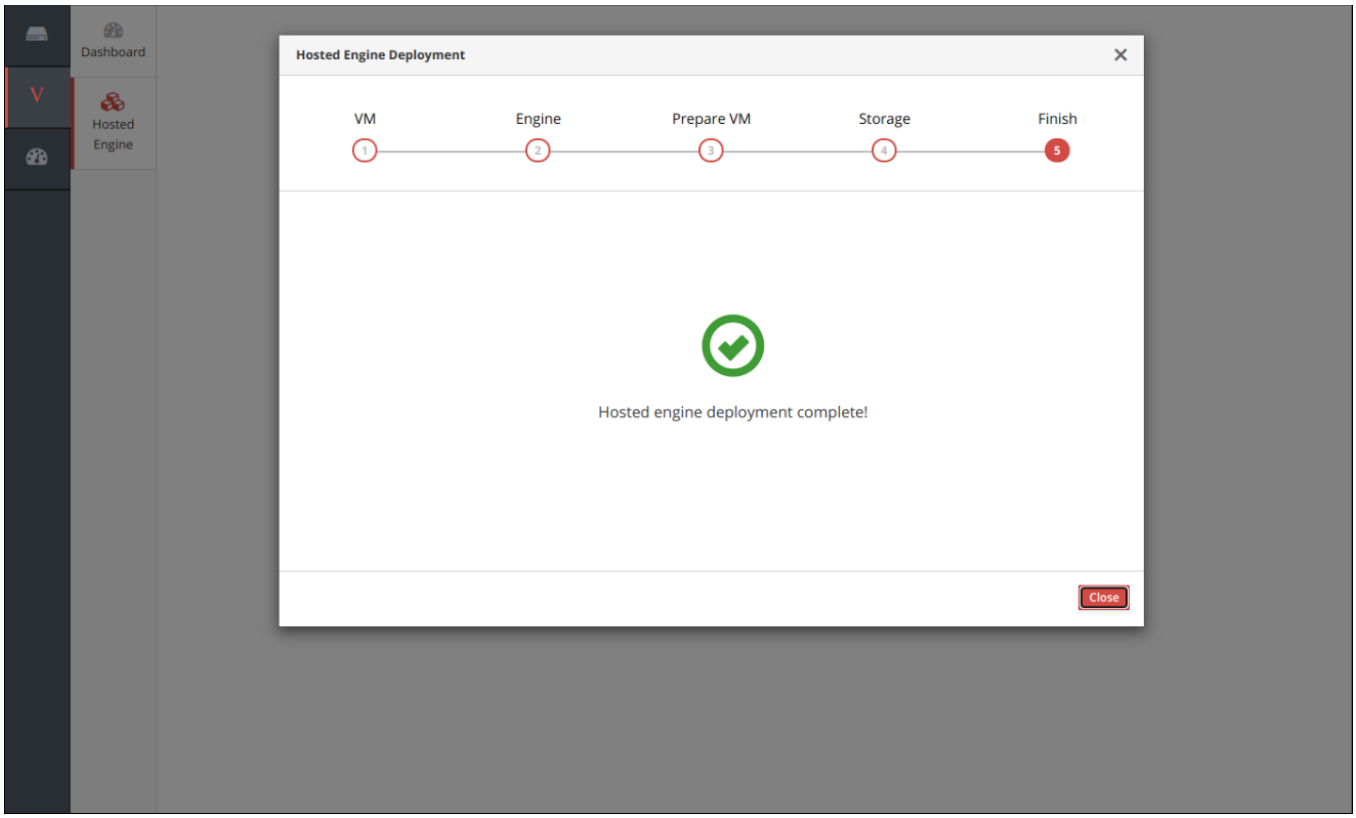


Во вкладке **Storage** добавьте хранилище.



Нажмите **Next**.

После успешной установки нажмите **Close**.



Установка в режиме Gluster Hyperconverged для одного узла

Предварительные требования
Развертывание на узле РЕД Виртуализации
Установка и настройка томов Gluster
Развертывание Hosted Engine

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Предварительные требования

Предварительные требования:

1. Хост РЕД Виртуализации, содержащий минимум один неразмеченный жесткий диск, на котором в процессе развёртывания будут созданы необходимые разделы **Gluster**.

2. На хосте должно быть как минимум 2 интерфейса, чтобы можно было разделить трафик на внешний (**frontend**) и внутренний (**backend**).

Наличие только одной сети приведет к тому, что мониторинг **Engine**, клиентский трафик, трафик ввода-вывода **Gluster** будут работать вместе и мешать друг другу. Чтобы разделить сеть **backend**, кластер **Gluster** формируется с использованием адресов сети **backend**, а узлы добавляются к **Engine** с использованием адресов сети **frontend**.

3. Подготовленное полное доменное имя для вашего **Engine** и хоста. В DNS должны быть установлены записи прямого и обратного поиска. **Engine** должен использовать ту же подсеть, что и сеть управления.

4. Беспарольный **ssh** от хоста к самому себе, так как роль **ansible** должна удаленно выполнять команды — обязательное условие. Для настройки выполните следующие действия на хосте, на котором планируется проведение установки кластера:

4.1. Сгенерируйте ключ доступа, выполнив следующую команду :

```
# ssh-keygen
```

ВАЖНО!

При генерации ключа нельзя использовать парольную фразу.

4.2. Скопируйте ключ на каждый хост кластера. Также выполните копирование на хост, на котором производится настройка беспарольного доступа. Для копирования ключа выполните следующую команду :

```
# ssh-copy-id root@<fqdn_адрес_хоста>
```

Развертывание на узле РЕД Виртуализации

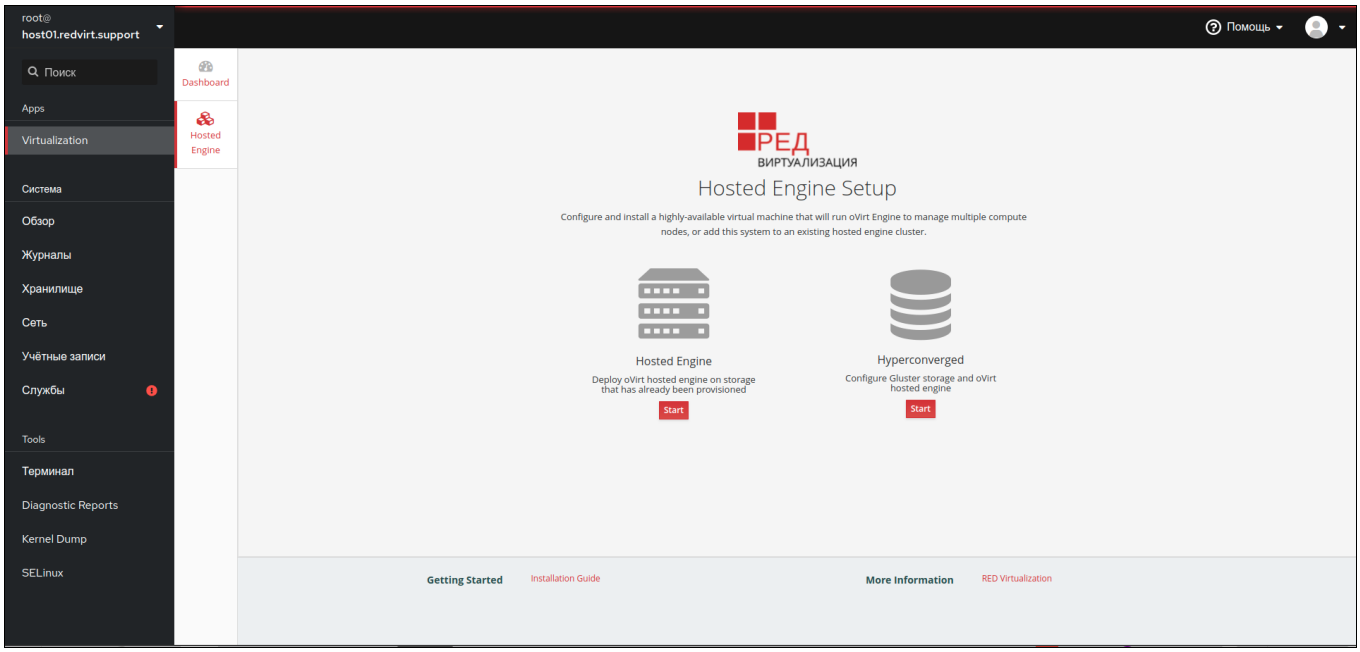
Узел РЕД Виртуализации содержит все необходимые пакеты для настройки гиперконвергентной среды. Вы можете начать настройку гиперконвергентной среды, если у вас есть хост на базе узла РЕД Виртуализации.

Установка и настройка томов Gluster

Тома **Gluster** должны быть созданы перед установкой **Hosted Engine**. Один из созданных томов используется для размещения виртуальной машины **Hosted Engine**. Используйте пользовательский интерфейс **Cockpit** для настройки развертывания с одним узлом.

1. Войдите в веб-консоль. Перейдите к интерфейсу управления веб-консоли первого гиперконвергентного хоста, например, https://<имя_хоста>:9090/ или https://<IP-адрес_хоста>:9090/, и войдите в систему, используя учетные данные суперпользователя **root**.

2. Перейдите во вкладку **Virtualization** – **Hosted Engine**.



3. Запустите мастер развертывания.

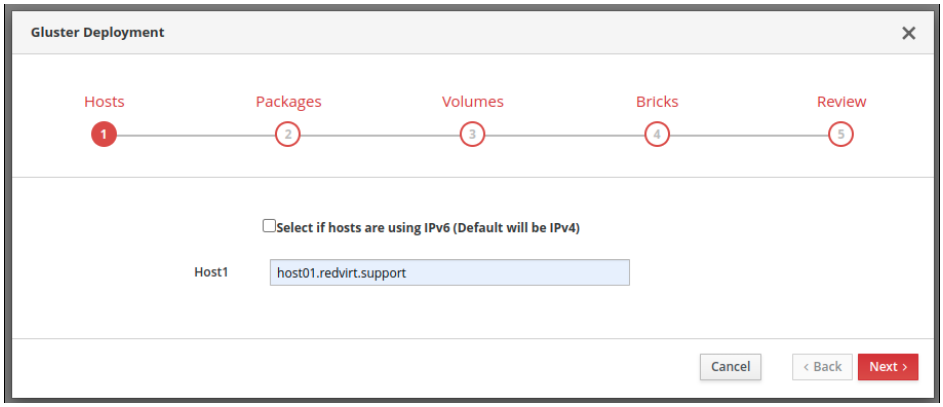
После запуска мастер развертывания предложит выбрать одно из дальнейших действий:

- Запустить мастер развертывания Gluster;
- Запустить мастер развертывания Gluster для единого узла.

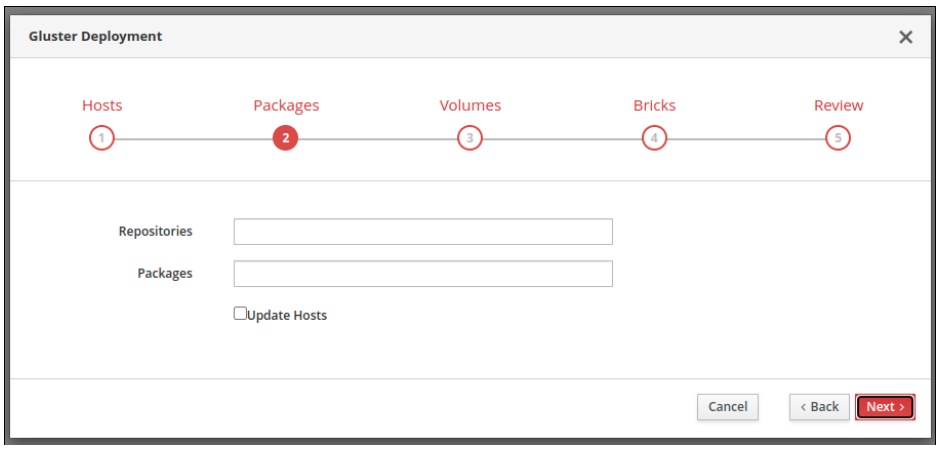
Выберите второй вариант.



4. Укажите имя хоста.

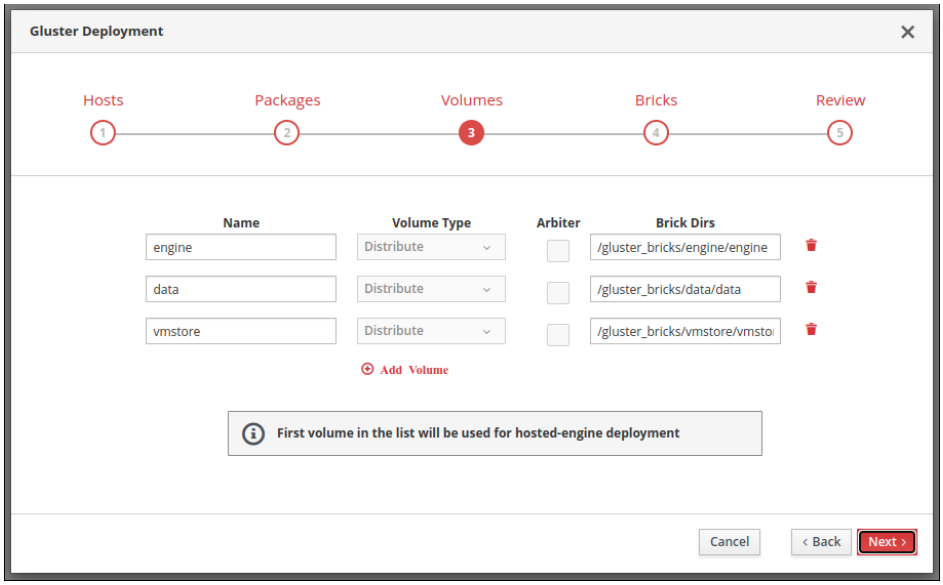


5. При необходимости загрузите репозитории и дополнительные пакеты.

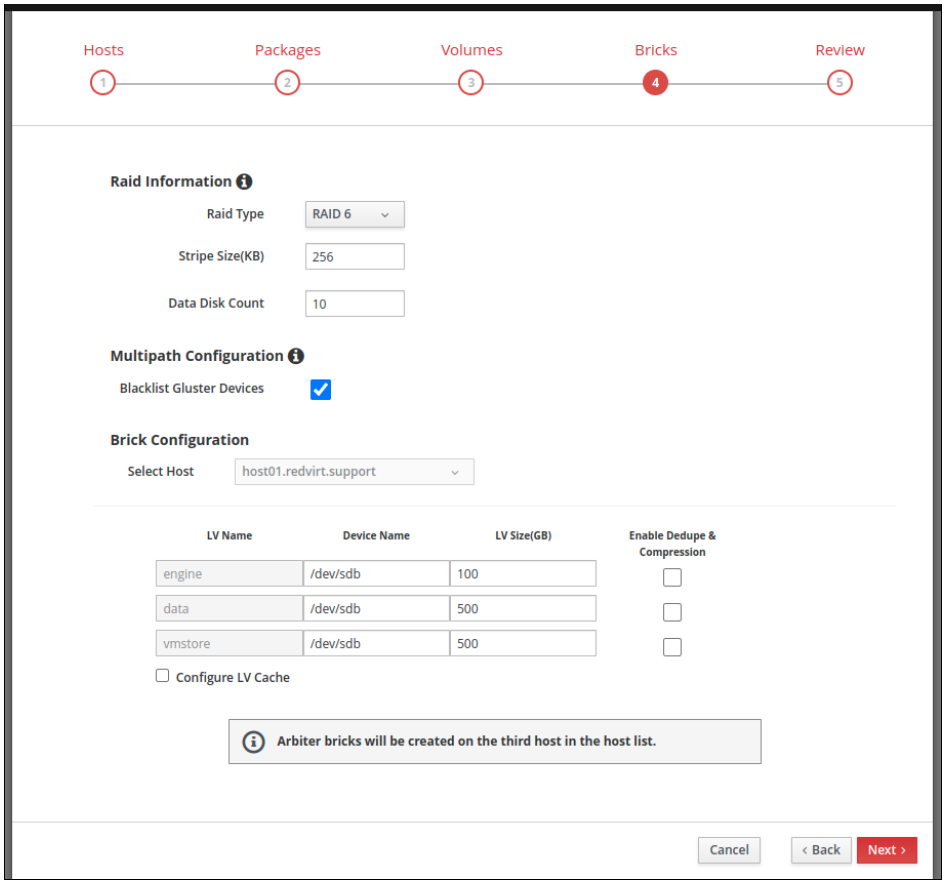


6. Определите необходимые тома.

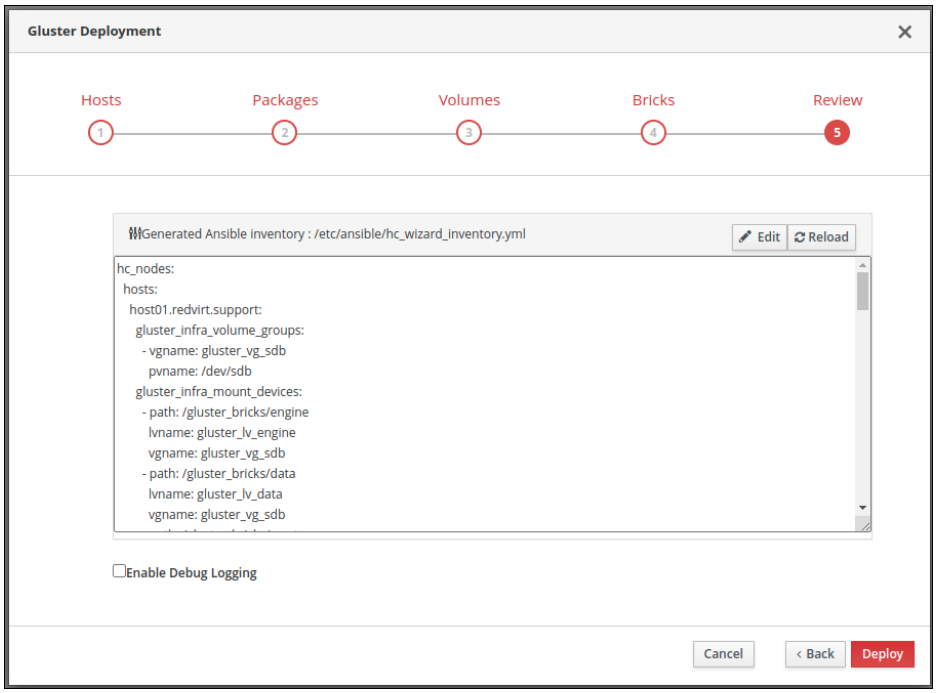
Обратите внимание, что первый указанный том будет использоваться для развертывания **Hosted Engine**.



7. Настройте жесткие диски — тип, наименование устройств и их размер.

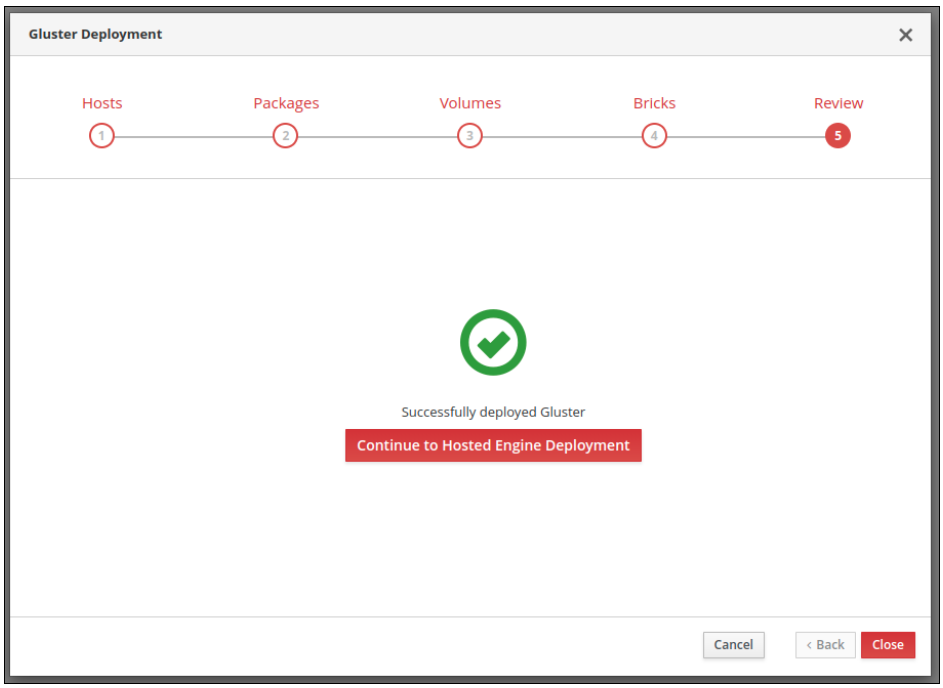


8. Проверьте установленные значения и характеристики, если все настроено верно, нажмите «**Deploy**».



Затем начнется процедура развертывания единого узла **Gluster**.

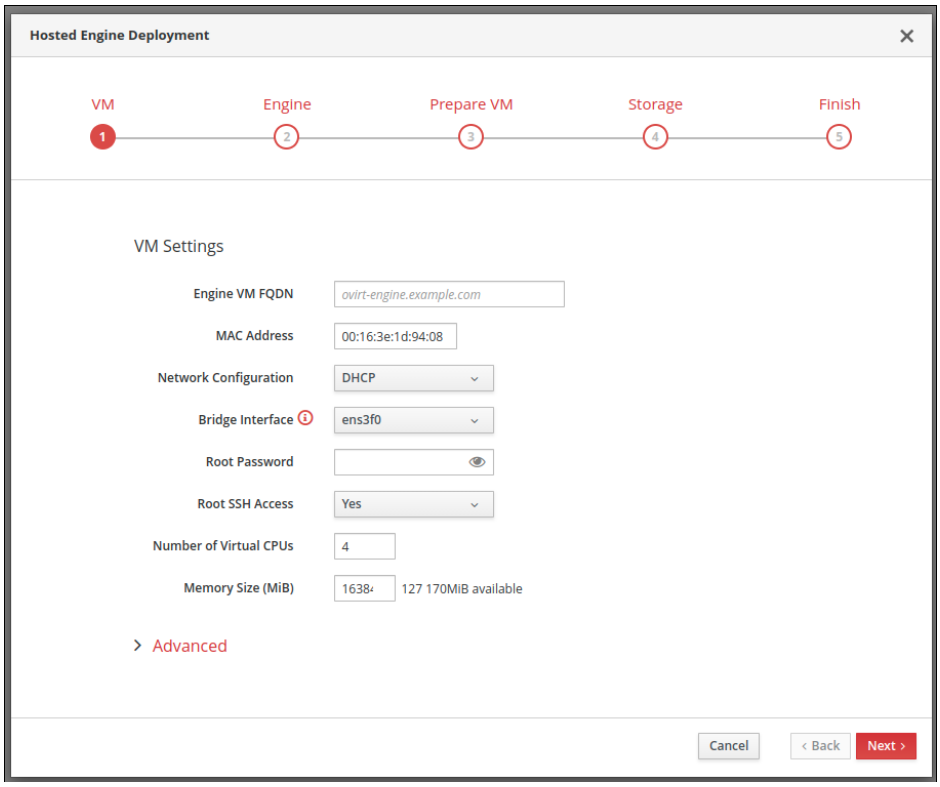
После успешной установки будет выведено соответствующее сообщение и предложено перейти к развёртыванию **Hosted Engine**.



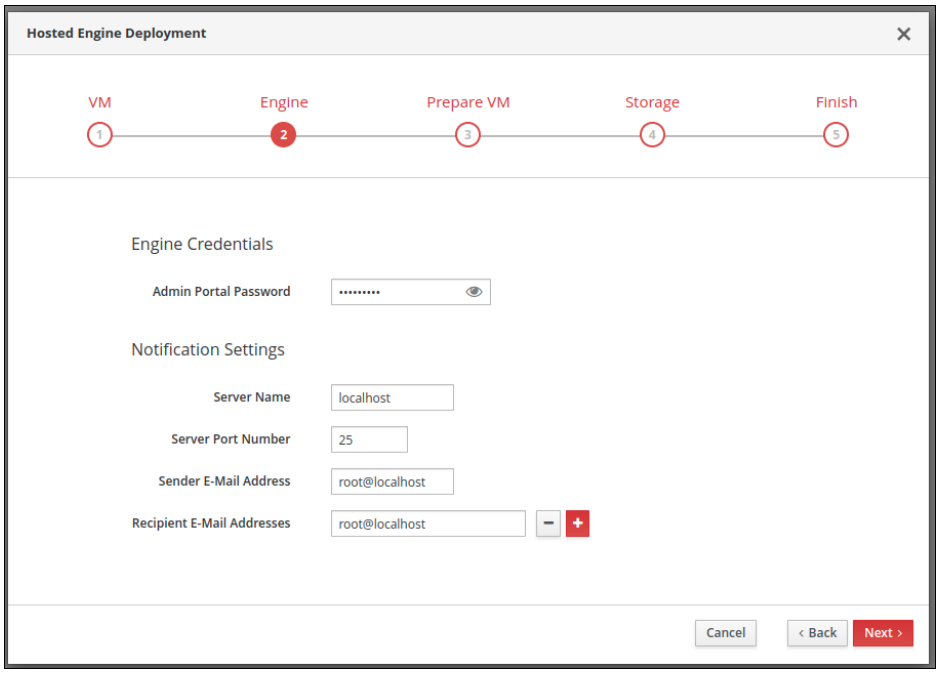
Развертывание Hosted Engine

Процедура настройки **Hosted Engine** стандартная.

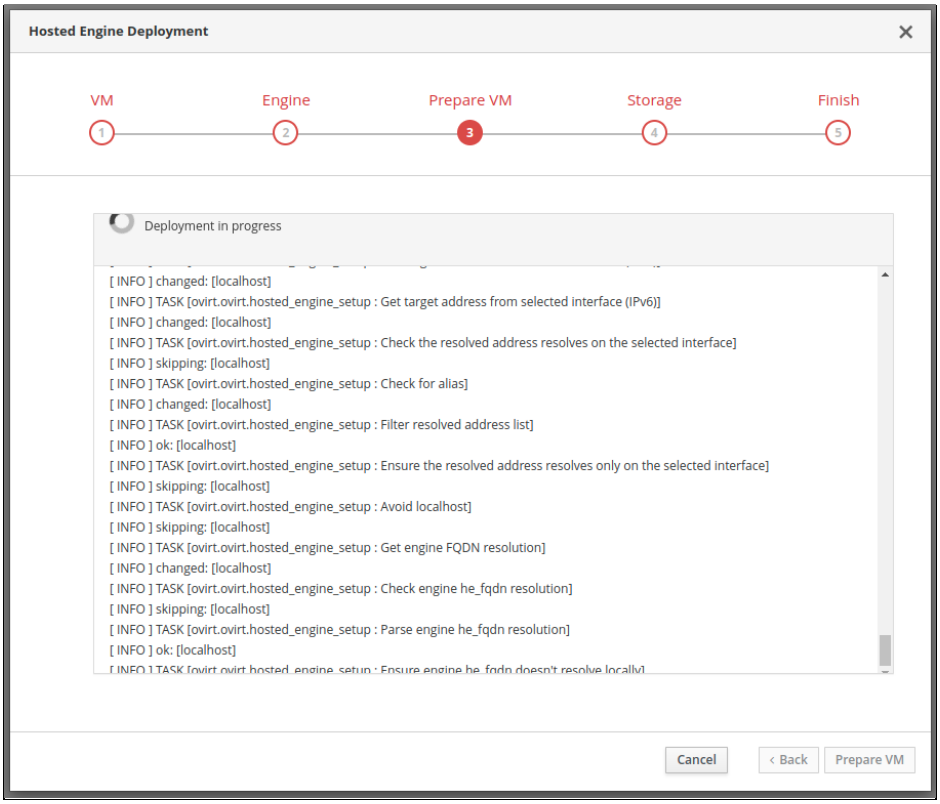
На вкладке **VM** заполните поля в соответствии с вашими параметрами сети. Нажмите **Next**.



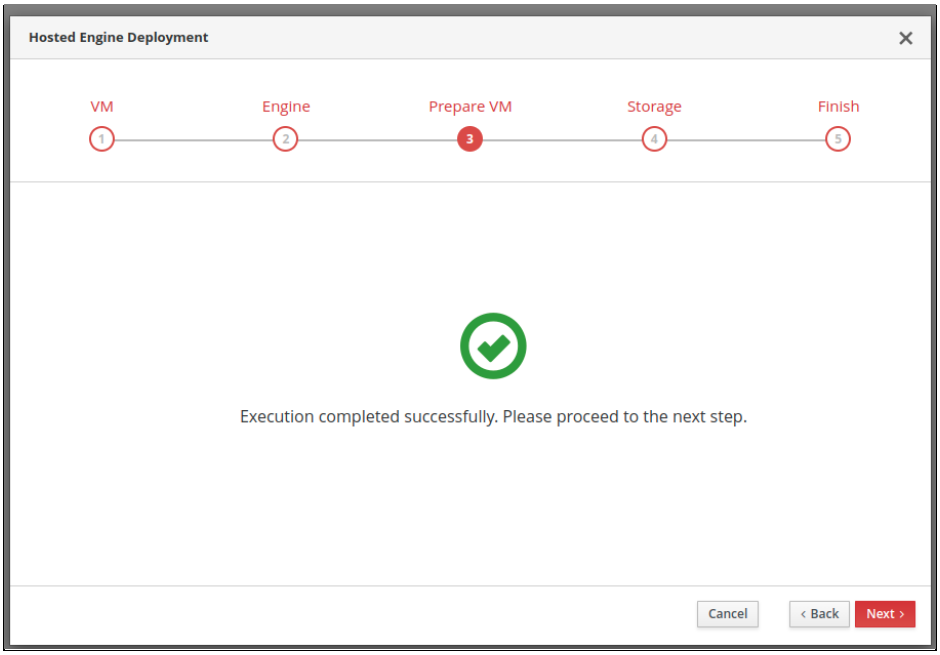
На вкладке **Engine** назначьте пароль администратору портала, а также настройте службу уведомлений.



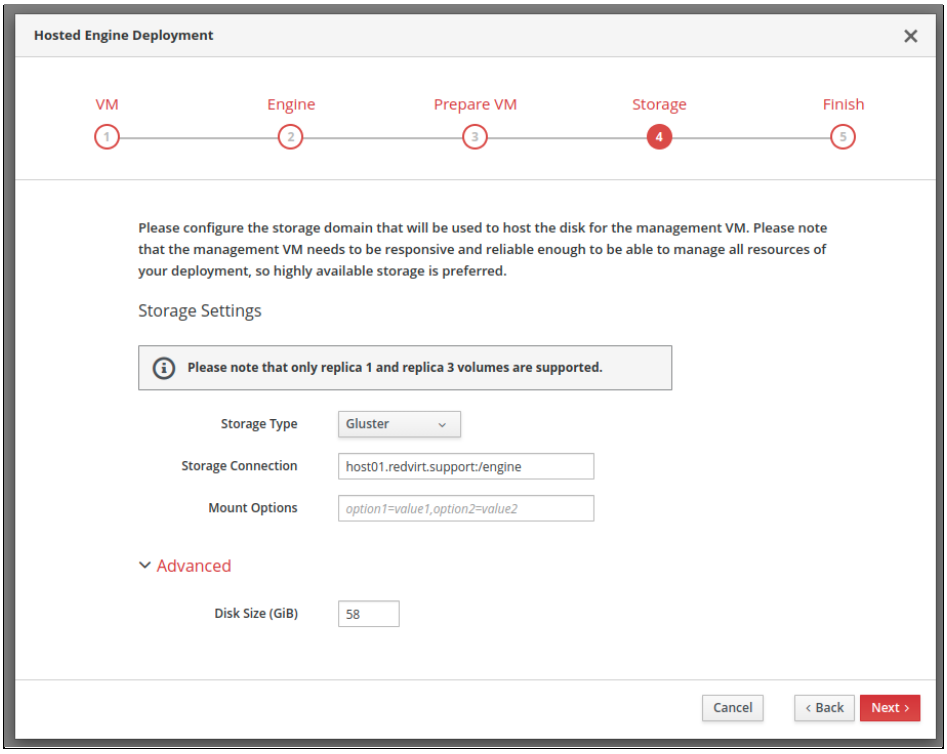
Во вкладке **Prepare VM** проверьте данные для ВМ и, если все настроено верно, нажмите кнопку «**Prepare VM**». Будет запущен процесс подготовки виртуальной машины и развертывание **Hosted Engine**.



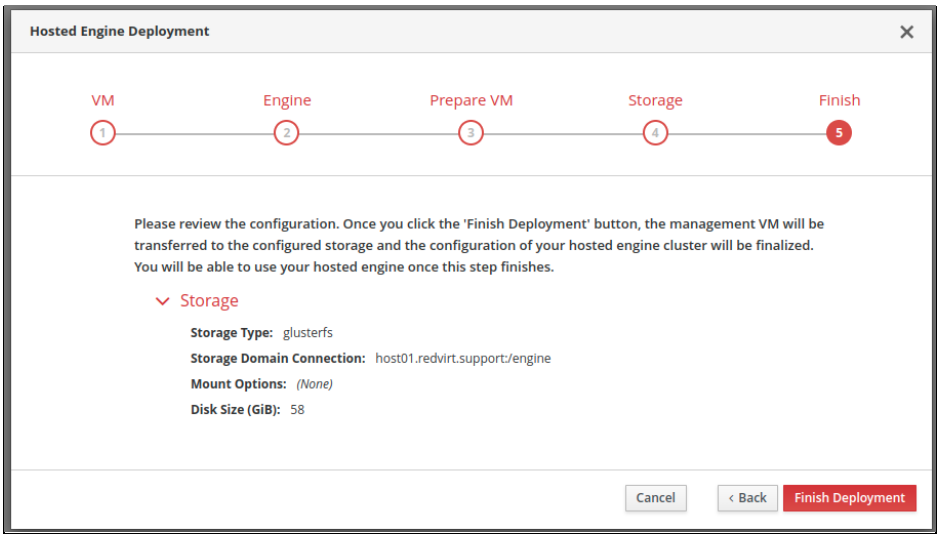
После успешного завершения процесса будет выведено соответствующее сообщение. Нажмите **Next**.



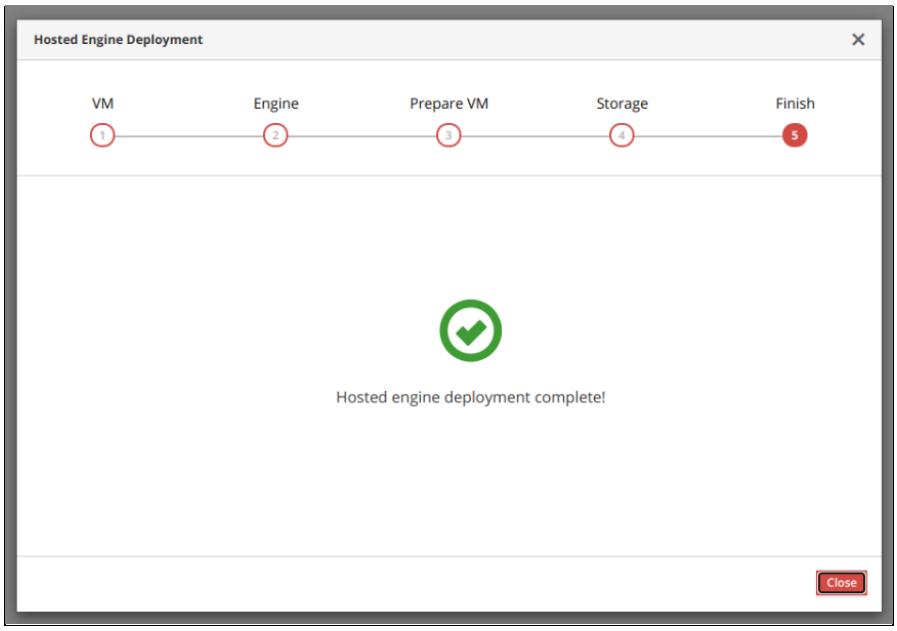
Во вкладке **Storage** будет автоматически определен ранее развернутый **Gluster** и предложение его подключить в качестве сетевого хранилища данных. Нажмите **Next**.



Для завершения развертывания проверьте данные хранилища, если все настроено верно, нажмите **Finish Deployment**.



После успешной установки нажмите **Close**.



Установка в режиме Gluster Hyperconverged для нескольких узлов

Предварительные требования
Развертывание на узле РЕД Виртуализации
Установка и настройка томов Gluster
Развертывание Hosted Engine

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Предварительные требования

Предварительные требования:

1. Хост РЕД Виртуализации, содержащий три неразмеченных жестких диска, на которых в процессе развёртывания будут созданы необходимые разделы **Gluster**.

2. На хосте должно быть как минимум 2 интерфейса, чтобы можно было разделить трафик на внешний (**frontend**) и внутренний (**backend**).

Наличие только одной сети приведет к тому, что мониторинг **Engine**, клиентский трафик, трафик ввода-вывода **Gluster** будут работать вместе и мешать друг другу. Чтобы разделить сеть **backend**, кластер **Gluster** формируется с использованием адресов сети **backend**, а узлы добавляются к **Engine** с использованием адресов сети **frontend**.

3. Подготовленное полное доменное имя для вашего **Engine** и хостов. В DNS должны быть установлены записи прямого и обратного поиска. **Engine** должен использовать ту же подсеть, что и сеть управления.

4. Беспарольный **SSH** от первого хоста к другим, так как роль **ansible** должна удаленно выполнять команды — обязательное условие. Для настройки выполните следующие команды:

```
# ssh-keygen
# ssh-copy-id root@gluster.host1
# ssh-copy-id root@gluster.host2
# ssh-copy-id root@gluster.host3
```

Развертывание на узле РЕД Виртуализации

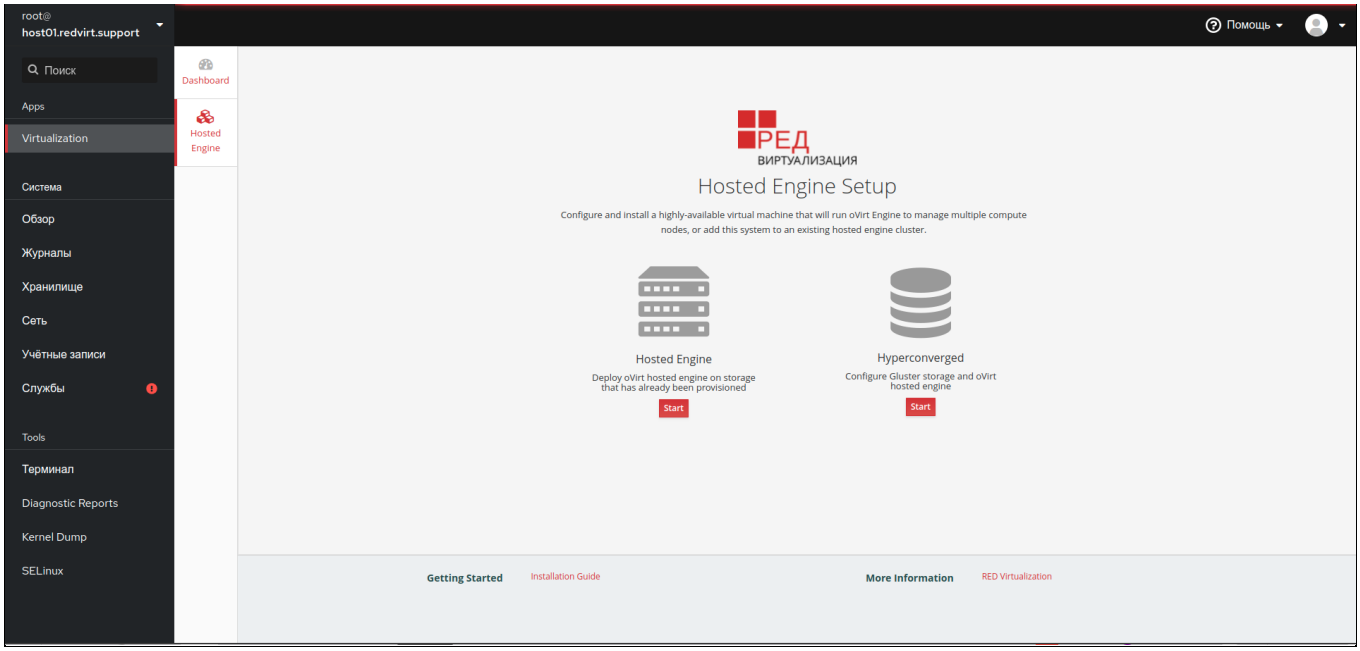
Хост РЕД Виртуализации содержит все необходимые пакеты для настройки гиперконвергентной среды. Начать настройку гиперконвергентной среды можно, если существует хотя бы один хост на базе РЕД Виртуализации.

Установка и настройка томов Gluster

Тома **Gluster** должны быть созданы перед установкой **Hosted Engine**. Один из созданных томов будет использован для размещения виртуальной машины **Hosted Engine**. Используйте пользовательский интерфейс **Cockpit** для настройки развертывания **Gluster** для нескольких узлов.

1. Войдите в веб-консоль. Перейдите к интерфейсу управления веб-консоли основного узла виртуализации, например, https://<имя_хоста>:9090/, и войдите в систему, используя учетные данные суперпользователя **root**.

2. Перейдите во вкладку **Virtualization** – **Hosted Engine** и нажмите **Start** в разделе **Hyperconverged**.



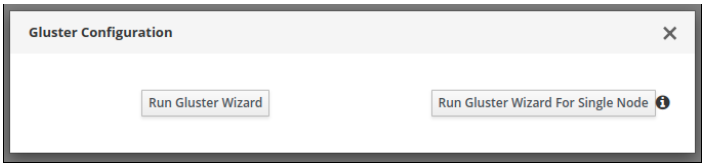
Откроется окно настройки **Gluster**.

3. Запустите мастер развертывания.

После запуска мастер развертывания предложит выбрать одно из дальнейших действий:

- Запустить мастер развертывания Gluster;
- Запустить мастер развертывания Gluster для одиночного узла.

Выберите первый вариант.



Откроется окно развертывания **Gluster** в режиме трех узлов.

4. Укажите имена хостов хранилища.

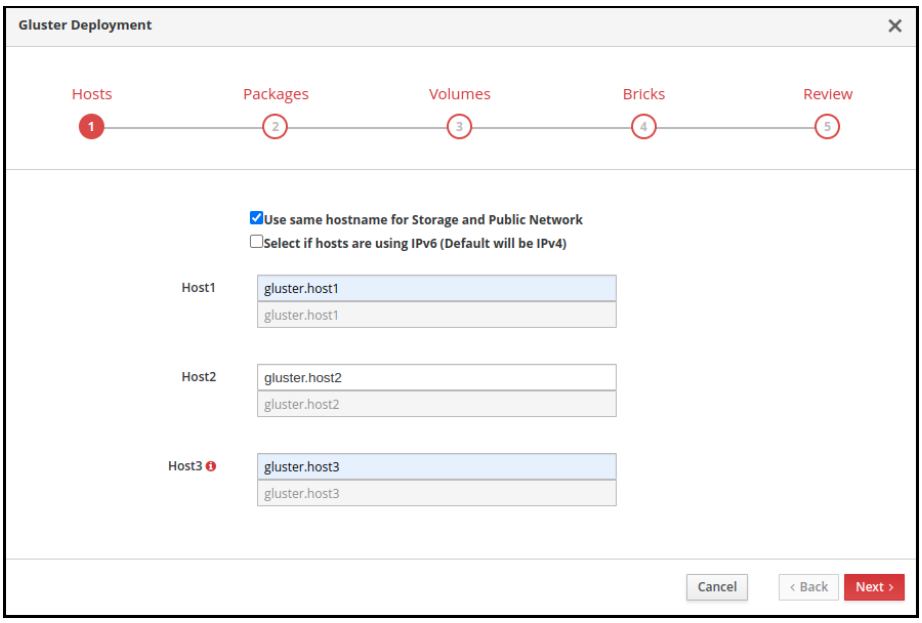
Укажите полные доменные имена сетевых хранилищ (не сети управления) для трех узлов виртуализации. Хост виртуализации, использующий авторизацию по **SSH** с помощью пар ключей, должен быть указан первым, так как именно на нем будет разворачиваться **Hosted Engine** и запускаться команда развертывания **Gluster**.

Примечание.

Для обеспечения высокой доступности требуется минимум два узла, но в случаях, когда два узла **не синхронизированы**, такой системе необходим третий компонент, называемый арбитром.

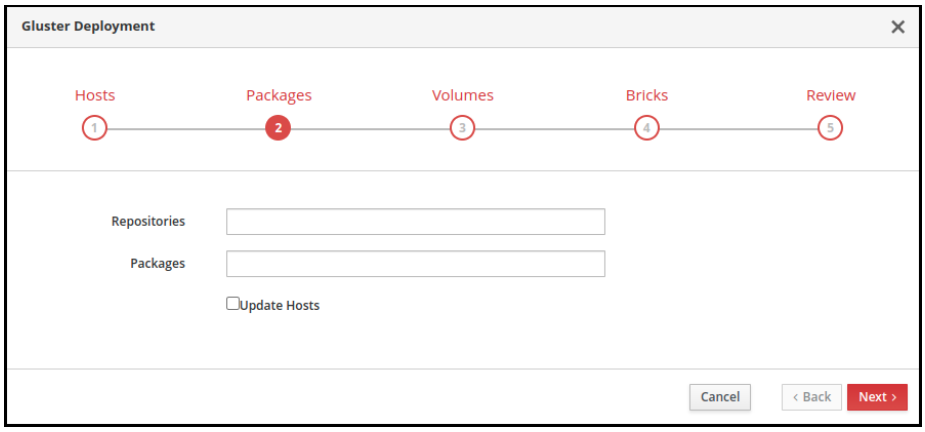
В случае потери прямой связи между узлами арбитр предотвращает состояние, когда на обоих узлах работают копии одних и тех же виртуальных машин и выполняется независимая модификация хранимых данных (**split brain**).

В роли арбитра на вкладке **Hosts** выступает указанный в поле **Host3** узел.



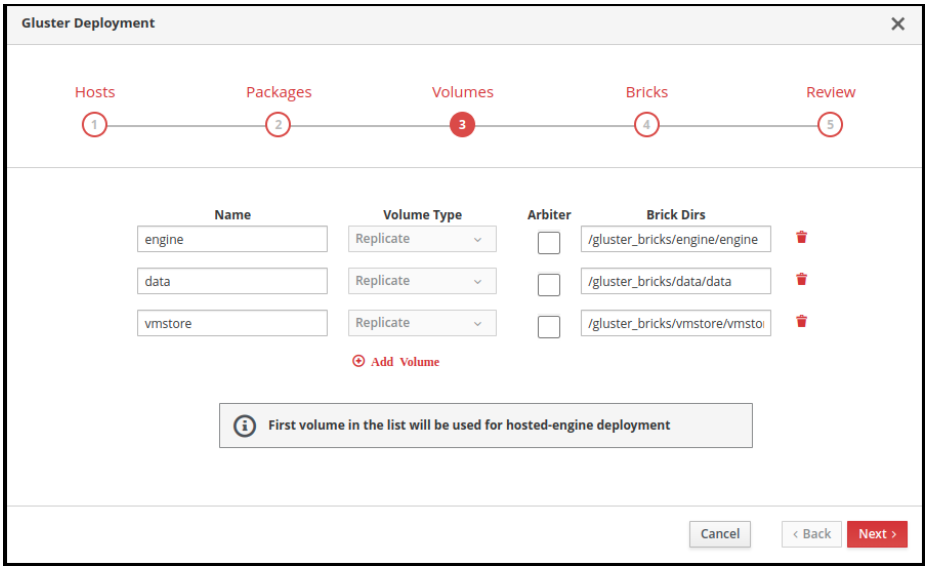
Нажмите **Next**.

5. При необходимости загрузите репозитории и дополнительные пакеты.



6. Определите необходимые тома.

Обратите внимание, что первый указанный том будет использоваться для развертывания **Hosted Engine**.

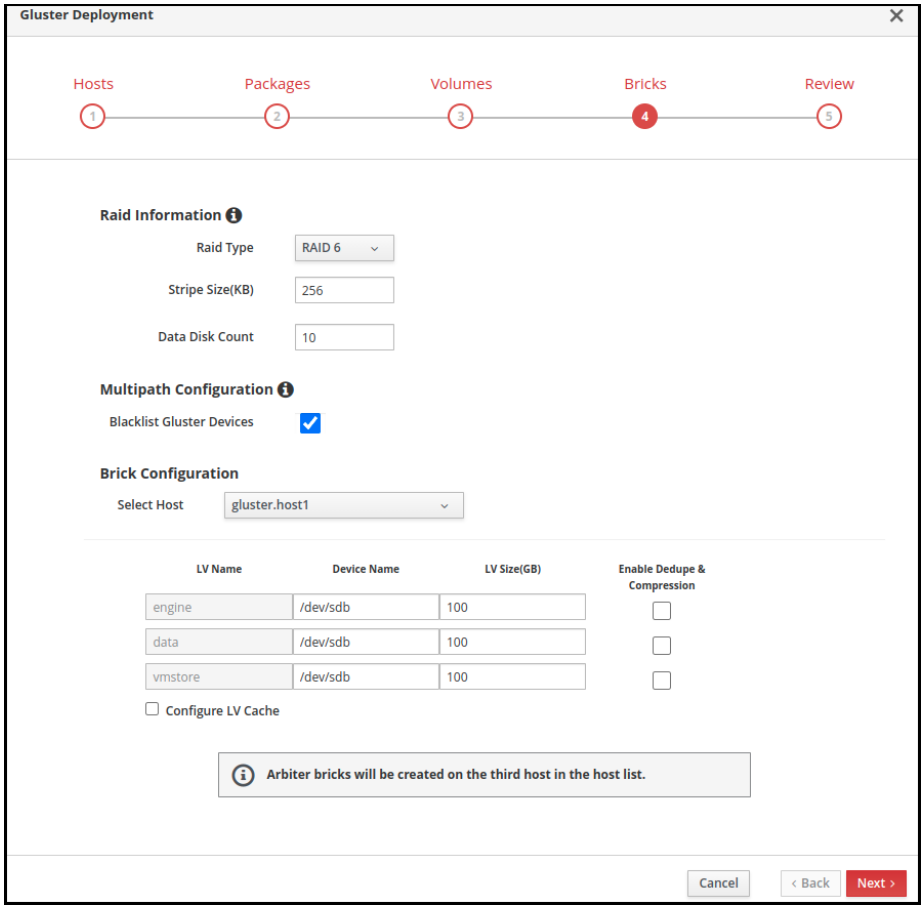


- **Name**: Имя создаваемого тома.
- **Volume Type**: Тип тома – **Replicate**. В данной версии поддерживаются только реплицированные тома.
- **Arbiter**: Необходимость создания тома с блоком арбитра. Если флаг установлен, на третьем диске будут храниться только метаданные.
- **Brick Dirs**: Каталог, содержащий блоки указанного тома.

В указанных полях можно оставить значения по умолчанию.

7. Настройте жесткие диски — укажите тип, наименование устройств и их размер.

Для редактирования информации о настраиваемом хосте можно использовать раскрывающееся меню **Select Host**.



В блоке **Raid Information** укажите:

- тип используемого массива **RAID** (он должен совпадать с используемым типом **RAID** на хосте);
- объем данных, записываемых **RAID**-контроллером на один диск в рамках одной полосы;
- количество дисков данных в массиве **RAID**.

В блоке **Brick Configuration** укажите:

- имя создаваемого тома (определяется автоматически из предыдущего шага);
- имя устройства, которое будет использовано (рекомендуется использовать неразмеченное устройство);
- размер создаваемого логического тома в ГБ (значение должно быть одинаковым для всех блоков в наборе, размер блока арбитра может быть меньше других блоков);
- необходимость использования на дисках дедупликации с технологией **VDO**.

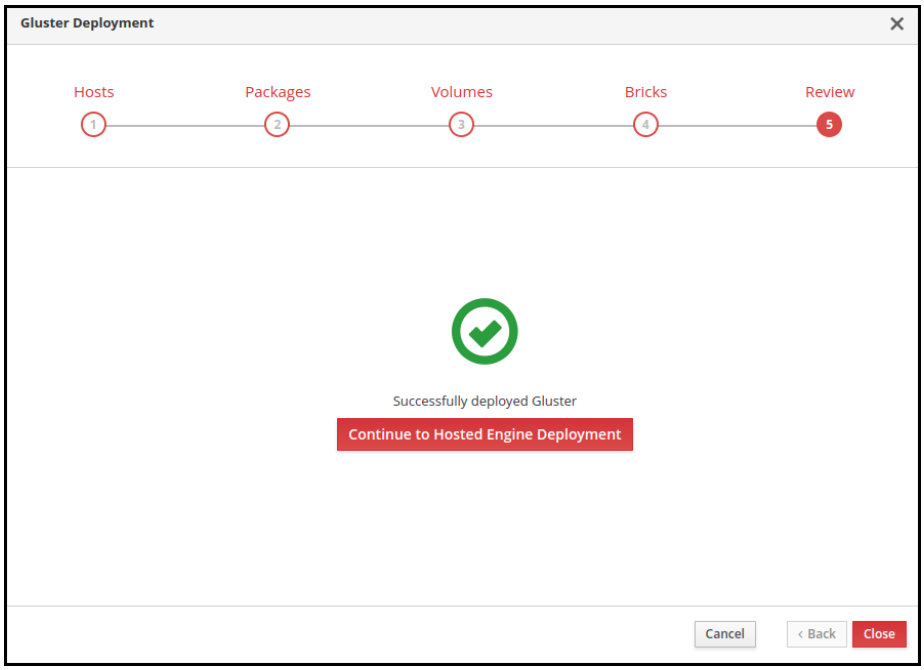
При активации параметра **Configure LV Cache** появляется возможность настройки **SSD**-кеширования.

SSD-кеширование — технология, когда твердотельные **SSD**-накопители используются в качестве буфера для часто запрашиваемых данных. Система определяет данные по степени востребованности и перемещает их на быстрый накопитель, используемый в качестве кеширующего диска. Кеш позволяет получать доступ к данным в несколько раз быстрее, чем если бы они были получены с более медленного жесткого диска.

8. Проверьте установленные значения и характеристики, если все настроено верно, нажмите **Deploy**.

Начнется процедура развертывания **Gluster**.

После успешной установки будет выведено соответствующее сообщение и предложено перейти к развёртыванию **Hosted Engine.**



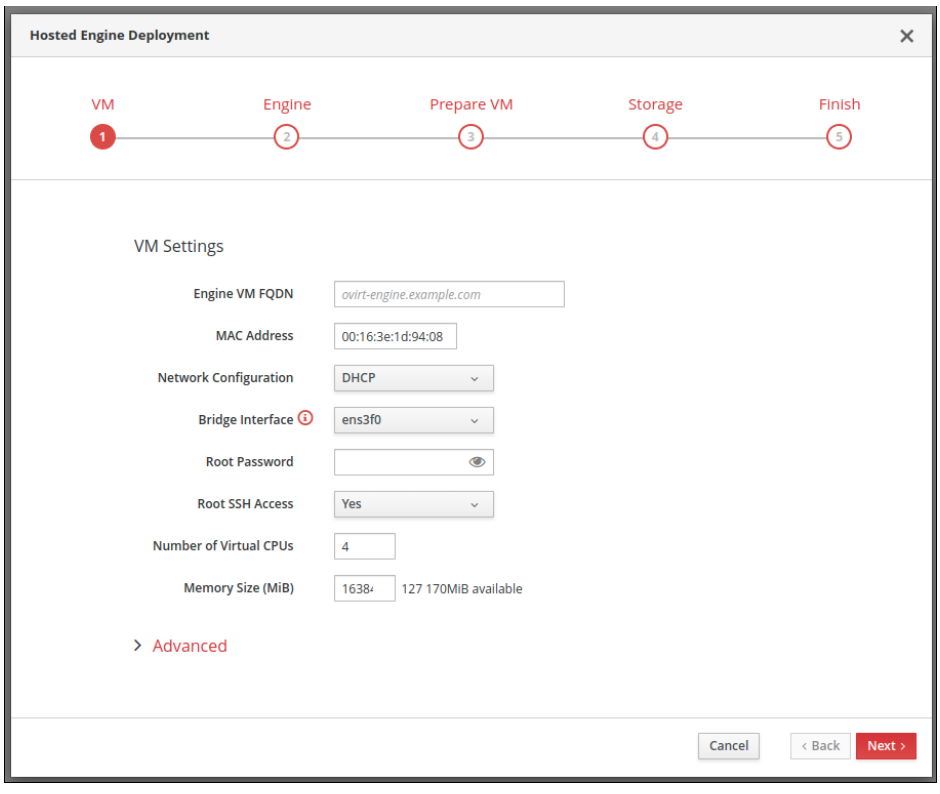
Примечание.

Если развертывание **Gluster** завершилось неудачей, нажмите кнопку **Redeploy**. Будет открыта вкладка **Review**, где с помощью кнопки **Edit** можно внести необходимые изменения в сгенерированный файл конфигурации **Gluster** и повторить попытку развертывания.

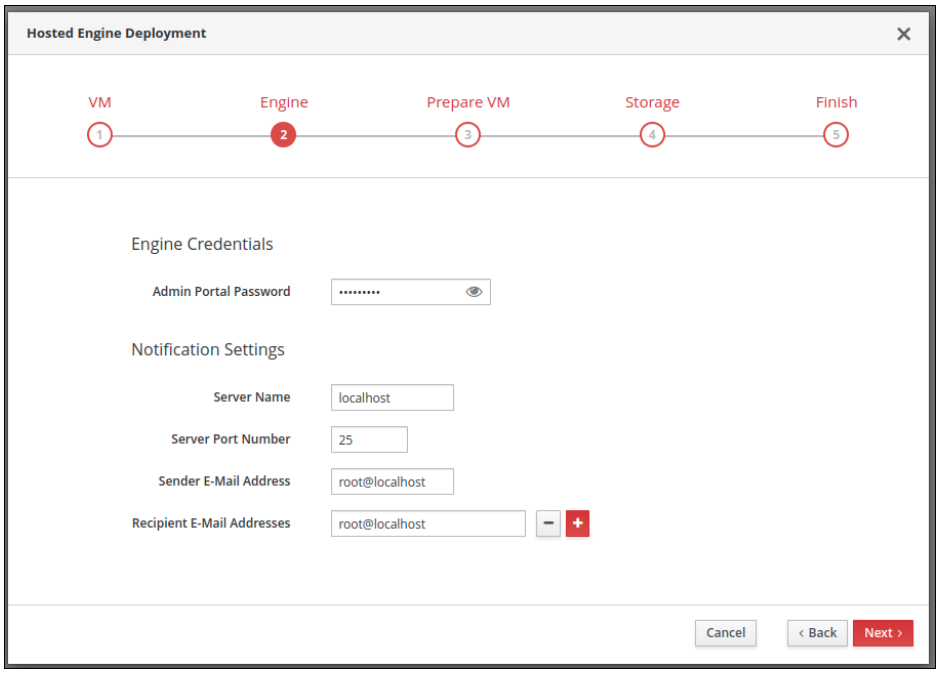
Развертывание Hosted Engine

Процедура настройки **Hosted Engine** стандартная.

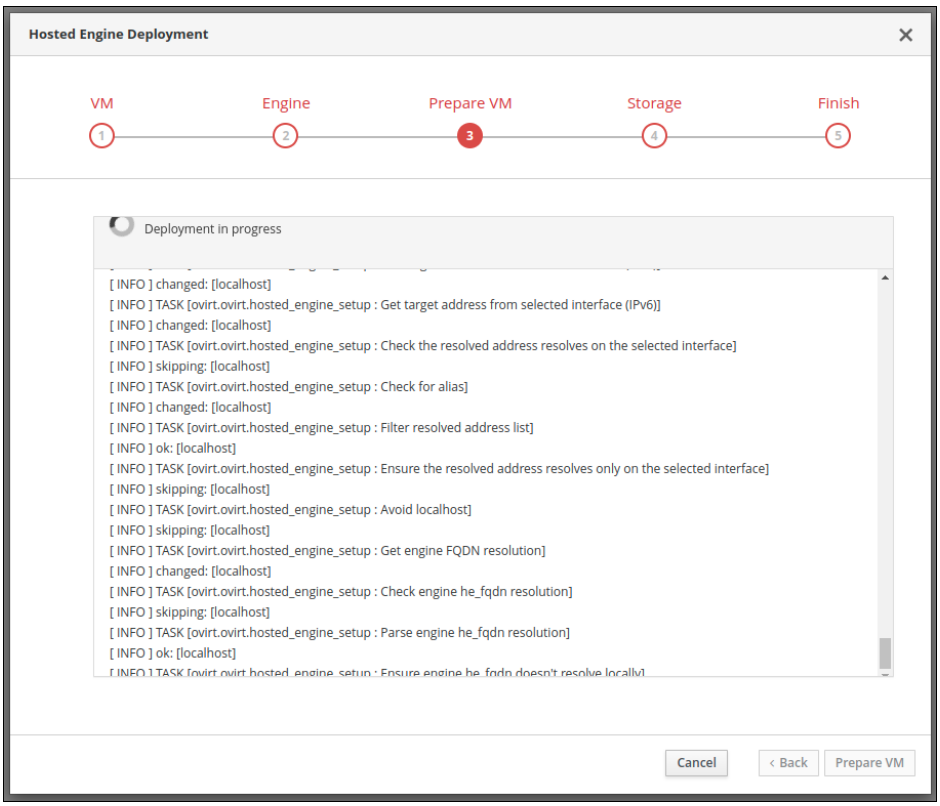
На вкладке **VM** заполните поля в соответствии с вашими параметрами сети. Нажмите **Next**.



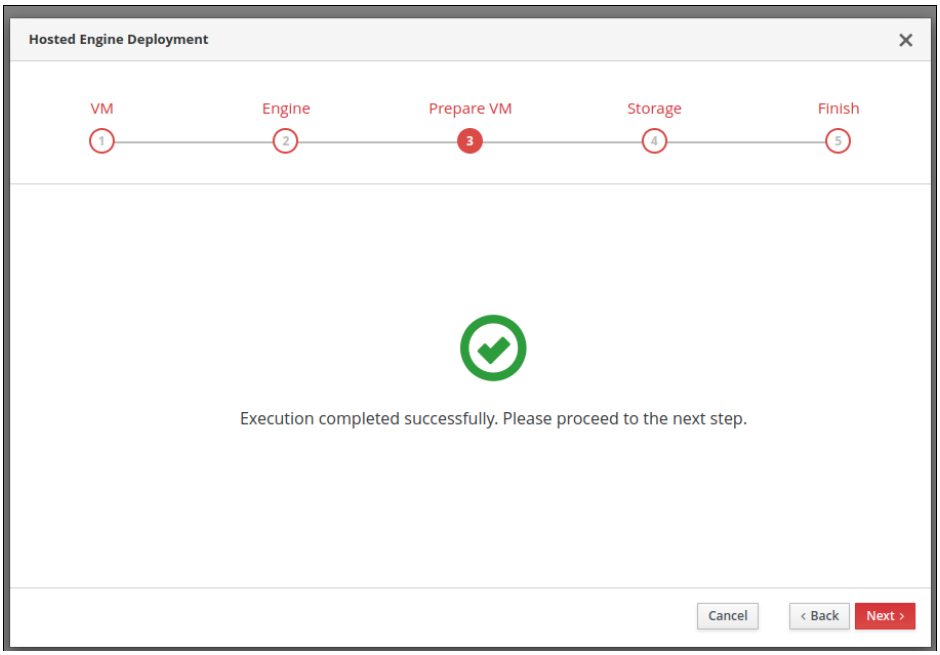
На вкладке **Engine** назначьте пароль администратору портала, а также настройте службу уведомлений.



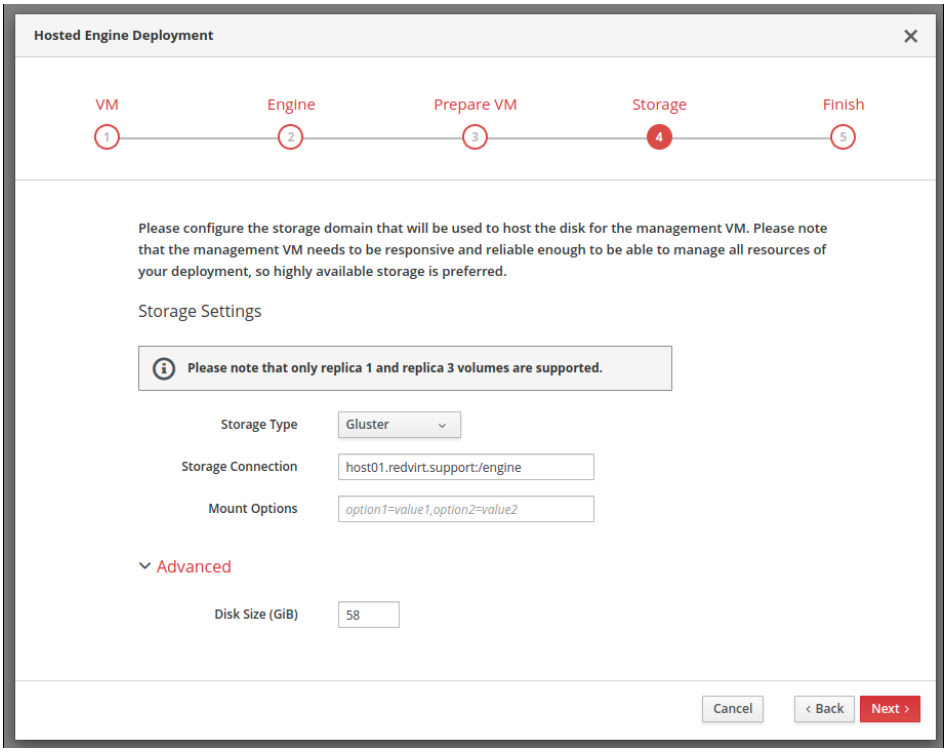
Во вкладке **Prepare VM** проверьте данные для ВМ и, если все настроено верно, нажмите кнопку «**Prepare VM**». Будет запущен процесс подготовки виртуальной машины и развертывание **Hosted Engine**.



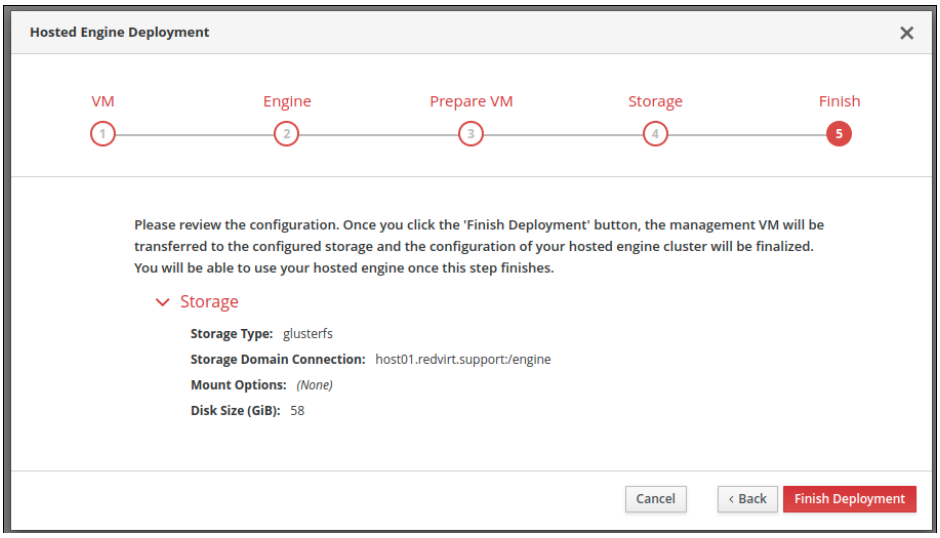
После успешного завершения процесса будет выведено соответствующее сообщение. Нажмите **Next**.



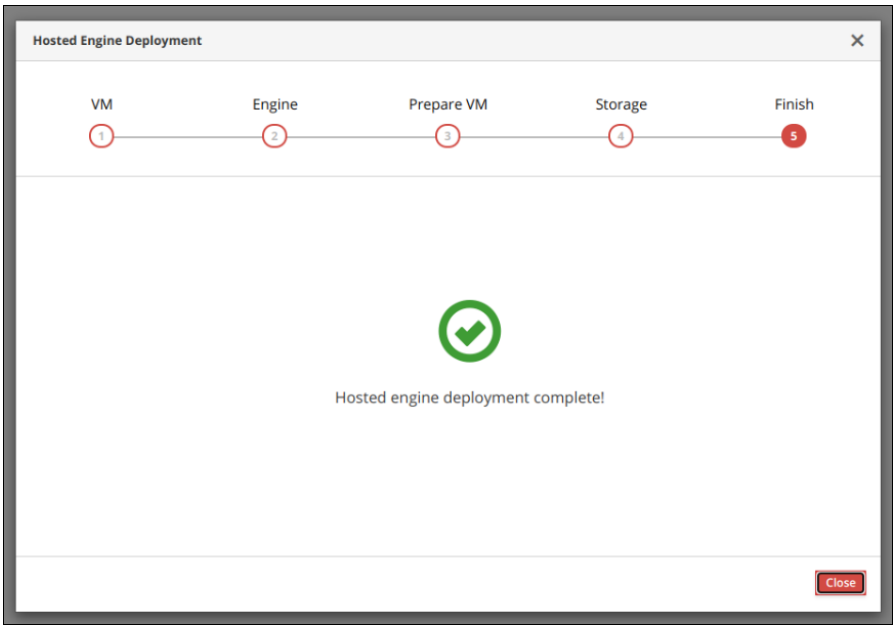
Во вкладке **Storage** будет автоматически определен ранее развернутый **Gluster** и предложение его подключить в качестве сетевого хранилища данных. Нажмите **Next**.



Для завершения развертывания проверьте данные хранилища, если все настроено верно, нажмите **Finish Deployment**.



После успешной установки нажмите **Close**.



Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Standalone с помощью стороннего центра сертификации

Создание центра сертификации
Добавление сертификата

Создание центра сертификации

Для создания локального центра сертификации в РЕД ОС 7.3 необходимо выполнить следующие действия:

1. Создать закрытый ключ **Root**:

```
openssl genrsa -des3 -out root.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
..............+++++
e is 65537 (0x010001)
Enter pass phrase for root.key: ********
Verifying - Enter pass phrase for root.key: ********
```

ВАЖНО!

Рекомендуется указать парольную фразу и защитить закрытый ключ.

2. Сгенерировать корневой сертификат. В процессе выполнения команды будет предложено ввести указанную на предыдущем шаге парольную фразу. После этого потребуется ввести некоторые данные для запроса сертификата - страну, область, город или другой населенный пункт, наименование организации, наименование подразделения организации и имя сертификата.

```
openssl req -x509 -new -nodes -key root.key -sha256 -days 7200 -out root.pem
```

где:

- **-x509**– экземпляр сертификата;
- **-new**– новый запрос сертификата;
- **-nodes**– отключить шифрование выходного ключа;
- **-key root.key**– файл ключа;
- **-sha256**– алгоритм подписи;
- **-days 7200**– период действия сертификата (в днях);
- **-out root.pem**– имя сгенерированного сертификата.

```
Enter pass phrase for root.key: ********
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:moscow
Locality Name (eg, city) [Default City]:moscow
Organization Name (eg, company) [Default Company Ltd]:redsoft
Organizational Unit Name (eg, section) []:drsp
Common Name (eg, your name or your server's hostname) []:Private RED Virt Authority
Email Address []:
```

3. Проверить содержание сгенерированного сертификата, выполнив команду:

```
openssl x509 -text -noout -in root.pem | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
```

```
60:05:f3:81:4d:b9:33:bd:a6:d7:34:9b:bb:31:40:d3:c3:8a:1d:86
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 6 13:29:10 2023 GMT
Not After : May 24 13:29:10 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

4. Убедиться в том, что был создан именно центр сертификации, выполнив команду:

```
openssl x509 -text -noout -in root.pem | grep CA:

CA:TRUE
```

5. Для использования созданного сертификата в качестве локального центра сертификации необходимо импортировать его на все доступные устройства. Корневой сертификат можно добавить в хранилище ключей/сертификатов ОС либо загрузить напрямую в браузер.

Существуют различные типы сертификатов (OV, EV, Wildcard и т. д.) и иерархии полномочий (Root, Intermediate, Sub CA и т. д.). В рамках приведенной инструкции будет рассмотрен вариант иерархии **Root Authority** с выпуском сертификата типа **Wildcard**, что позволит иметь один **SSL**-сертификат для всех внутренних доменов **redvirt.home**. Сертификат типа **Wildcard** может быть применен к домену и всем его поддоменам. Для генерации самоподписанного группового сертификата, необходимо создать файл с расширением **csr** и закрытый ключ.

Для создания закрытого ключа необходимо выполнить:

```
openssl genrsa -out wildcard.redvirt.home.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
.....................+++++
e is 65537 (0x010001)
```

6. Для создания запроса самоподписанного сертификата следует использовать файл конфигурации, содержимое которого приведено ниже.

В разделе **[alt_names]** необходимо определить расширение **Subject Alternative Name** (**SAN**).

```
nano openssl san.cnf
```

```
[req]
 distinguished_name=req_distinguished_name
 req_extensions=v3_req
 prompt=no

 [req_distinguished_name]
 C=ru
 ST=moscow
 L=moscow
 O=redsoft
 OU=drsp
 CN=*.redvirt.home

 [v3_req]
 keyUsage=keyEncipherment, dataEncipherment, digitalSignature
 extendedKeyUsage=serverAuth
 subjectAltName=@alt_names

 [alt_names]
 DNS.1 = *.redvirt.home
```

7. Сгенерировать корневой сертификат **wildcard.redvirt.home.csr** с помощью созданного файла конфигурации:

```
openssl req -new -out wildcard.redvirt.home.csr -key wildcard.redvirt.home.key -config opensslsan.cnf
```

8. Далее необходимо подписать файл с расширением csr собственным закрытым ключом.

```
openssl x509 -req -in wildcard.redvirt.home.csr -CA root.pem -CAkey root.key -CAcreateserial -out wildcard.redvirt.home.crt -days 7200 -sha256 -extensions v3_req -extfile opensslsan.cnf

Signature ok
subject=C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN =*.redvirt.home
Getting CA Private Key
Enter pass phrase for root.key:
```

9. Ввести пароль корневого закрытого ключа.

10. Проверить, что сертификат действителен и цепочка доверена.

```
openssl verify -CAfile root.pem wildcard.redvirt.home.crt

wildcard.redvirt.home.crt: OK
```

11. Проверить содержимое сертификата **Wildcard**, выполнив команду:

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
64:27:99:f3:81:3e:b3:ae:df:4c:35:78:b1:e6:0f:87:6e:01:eb:a6
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 7 08:14:35 2023 GMT
Not After : May 25 08:14:35 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = *.redvirt.home
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | grep DNS

DNS:*.redvirt.home
```

Сертификат выдан и будет действителен в течение следующих 20 лет. Все файлы, включая **wildcard.redvirt.home.crt** (сертификат), **wildcard.redvirt.home.key** (закрытый ключ) и **root.pem** (сертификат ЦС), будут использоваться для настройки **SSL** на любом из веб-серверов.

```
ll

-rw-r--r--. 1 root root 325 сен 6 16:39 opensslsan.cnf
-rw-------. 1 root root 1743 сен 6 16:27 root.key
-rw-r--r--. 1 root root 1375 сен 6 16:29 root.pem
-rw-r--r--. 1 root root 41 сен 7 11:14 root.srl
-rw-r--r--. 1 root root 1334 сен 7 11:14 wildcard.redvirt.home.crt
-rw-r--r--. 1 root root 1110 сен 7 11:14 wildcard.redvirt.home.csr
-rw-------. 1 root root 1679 сен 6 16:39 wildcard.redvirt.home.key
```

Добавление сертификата

Все последующие действия должны производиться на хосте, где развернута система РЕД Виртуализации, в каталоге **/tmp**.

Для добавления сертификата в систему РЕД Виртуализации необходимо:

1. Скопировать с созданного ранее центра сертификации файлы **wildcard.redvirt.home.crt**, **wildcard.redvirt.home.key**, **root.pem** на хост РЕД Виртуализации в папку **/tmp**.

2. Создать файл с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -export -out apache.p12 -inkey wildcard.redvirt.home.key -in wildcard.redvirt.home.crt
```

Пароль указывать не нужно.

3. Экспортировать ключ из созданного на предыдущем шаге файла с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -in apache.p12 -nocerts -nodes > apache.key
```

Пароль указывать не нужно.

4. Экспортировать файл с расширением cer из файла **apache.p12**:

```
openssl pkcs12 -in apache.p12 -nokeys > apache.cer
```

Теперь с точки зрения самоподписанного SSL-сертификата в системе РЕД Виртуализации существуют все необходимые файлы:

- **/tmp/root.pem;**
- **/tmp/apache.p12;**
- **/tmp/apache.key;**
- **/tmp/apache.cer.**

5. Затем создать резервную копию текущего файла **apache.p12**:

```
cp -p /etc/pki/ovirt-engine/keys/apache.p12 /tmp/apache.p12.bck
```

6. Заменить текущий файл **apache.p12** на созданный в п. 2 файл:

```
cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

7. Заменить имеющийся ЦС на созданный в п. 2 раздела 1 «Создание центра сертификации» корневой сертификат и обновить хранилище доверенных сертификатов:

```
cp /tmp/root.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

8. Удалить символическую ссылку и сохранить сертификат как apache-ca.pem в соответствующий каталог:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
cp /tmp/root.pem /etc/pki/ovirt-engine/apache-ca.pem
```

9. Создать резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

10. Скопировать выданный закрытый ключ и сертификат в соответствующие каталоги:

```
cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

11. Перезапустить сервер **apache**:

```
systemctl restart httpd.service
```

12. Создать новый файл конфигурации доверенного хранилища со следующим содержимым:

```
nano /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
 ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

13. Сохранить файл.

14. Отредактировать файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf**:

```
nano /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf
```

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

15. Перезапустить необходимые службы:

```
systemctl restart ovirt-provider-ovn.service
systemctl restart ovirt-websocket-proxy
systemctl restart ovirt-engine.service
```

Если все настроено верно, подключение к порталу администратора и порталу виртуальных машин будет производиться без вывода предупреждений о подлинности сертификата, используемого для шифрования **HTTPS**-трафика.

Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Hosted Engine с помощью стороннего центра сертификации

Создание центра сертификации
Добавление сертификата

Создание центра сертификации

Для создания локального центра сертификации в РЕД ОС 7.3 необходимо выполнить следующие действия:

1. Создать закрытый ключ **Root**:

```
openssl genrsa -des3 -out root.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
..............+++++
e is 65537 (0x010001)
Enter pass phrase for root.key: ********
Verifying - Enter pass phrase for root.key: ********
```

ВАЖНО!

Рекомендуется указать парольную фразу и защитить закрытый ключ.

2. Сгенерировать корневой сертификат. В процессе выполнения команды будет предложено ввести указанную на предыдущем шаге парольную фразу. После этого потребуется ввести некоторые данные для запроса сертификата - страну, область, город или другой населенный пункт, наименование организации, наименование подразделения организации и имя сертификата.

```
openssl req -x509 -new -nodes -key root.key -sha256 -days 7200 -out root.pem
```

где:

- **-x509**– экземпляр сертификата;
- **-new**– новый запрос сертификата;
- **-nodes**– отключить шифрование выходного ключа;
- **-key root.key**– файл ключа;
- **-sha256**– алгоритм подписи;
- **-days 7200**– период действия сертификата (в днях);
- **-out root.pem**– имя сгенерированного сертификата.

```
Enter pass phrase for root.key: ********
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:moscow
Locality Name (eg, city) [Default City]:moscow
Organization Name (eg, company) [Default Company Ltd]:redsoft
Organizational Unit Name (eg, section) []:drsp
Common Name (eg, your name or your server's hostname) []:Private RED Virt Authority
Email Address []:
```

3. Проверить содержание сгенерированного сертификата, выполнив команду:

```
openssl x509 -text -noout -in root.pem | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
```

```
60:05:f3:81:4d:b9:33:bd:a6:d7:34:9b:bb:31:40:d3:c3:8a:1d:86
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 6 13:29:10 2023 GMT
Not After : May 24 13:29:10 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

4. Убедиться в том, что был создан именно центр сертификации, выполнив команду:

```
openssl x509 -text -noout -in root.pem | grep CA:

CA:TRUE
```

5. Для использования созданного сертификата в качестве локального центра сертификации необходимо импортировать его на все доступные устройства. Корневой сертификат можно добавить в хранилище ключей/сертификатов ОС либо загрузить напрямую в браузер.

Существуют различные типы сертификатов (OV, EV, Wildcard и т. д.) и иерархии полномочий (Root, Intermediate, Sub CA и т. д.). В рамках приведенной инструкции будет рассмотрен вариант иерархии **Root Authority** с выпуском сертификата типа **Wildcard**, что позволит иметь один **SSL**-сертификат для всех внутренних доменов **redvirt.home**. Сертификат типа **Wildcard** может быть применен к домену и всем его поддоменам. Для генерации самоподписанного группового сертификата, необходимо создать файл с расширением **csr** и закрытый ключ.

Для создания закрытого ключа необходимо выполнить:

```
openssl genrsa -out wildcard.redvirt.home.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
.....................+++++
e is 65537 (0x010001)
```

6. Для создания запроса самоподписанного сертификата следует использовать файл конфигурации, содержимое которого приведено ниже.

В разделе **[alt_names]** необходимо определить расширение **Subject Alternative Name** (**SAN**).

```
nano openssl san.cnf
```

```
[req]
distinguished_name=req_distinguished_name
req_extensions=v3_req
prompt=no

[req_distinguished_name]
C=ru
ST=moscow
L=moscow
O=redsoft
OU=drsp
CN=*.redvirt.home

[v3_req]
keyUsage=keyEncipherment, dataEncipherment, digitalSignature
extendedKeyUsage=serverAuth
subjectAltName=@alt_names

[alt_names]
DNS.1 = *.redvirt.home
```

7. Сгенерировать корневой сертификат **wildcard.redvirt.home.csr** с помощью созданного файла конфигурации:

```
openssl req -new -out wildcard.redvirt.home.csr -key wildcard.redvirt.home.key -config opensslsan.cnf
```

8. Далее необходимо подписать файл с расширением csr собственным закрытым ключом.

```
openssl x509 -req -in wildcard.redvirt.home.csr -CA root.pem -CAkey root.key -CAcreateserial -out wildcard.redvirt.home.crt -days 7200 -sha256 -extensions v3_req -extfile opensslsan.cnf

Signature ok
subject=C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN =*.redvirt.home
Getting CA Private Key
Enter pass phrase for root.key:
```

9. Ввести пароль корневого закрытого ключа.

10. Проверить, что сертификат действителен и цепочка доверена.

```
openssl verify -CAfile root.pem wildcard.redvirt.home.crt

wildcard.redvirt.home.crt: OK
```

11. Проверить содержимое сертификата **Wildcard**, выполнив команду:

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
64:27:99:f3:81:3e:b3:ae:df:4c:35:78:b1:e6:0f:87:6e:01:eb:a6
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 7 08:14:35 2023 GMT
Not After : May 25 08:14:35 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = *.redvirt.home
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | grep DNS

DNS:*.redvirt.home
```

Сертификат выдан и будет действителен в течение следующих 20 лет. Все файлы, включая **wildcard.redvirt.home.crt** (сертификат), **wildcard.redvirt.home.key** (закрытый ключ) и **root.pem** (сертификат ЦС), будут использоваться для настройки **SSL** на любом из веб-серверов.

```
ll

-rw-r--r--. 1 root root 325 сен 6 16:39 opensslsan.cnf
-rw-------. 1 root root 1743 сен 6 16:27 root.key
-rw-r--r--. 1 root root 1375 сен 6 16:29 root.pem
-rw-r--r--. 1 root root 41 сен 7 11:14 root.srl
-rw-r--r--. 1 root root 1334 сен 7 11:14 wildcard.redvirt.home.crt
-rw-r--r--. 1 root root 1110 сен 7 11:14 wildcard.redvirt.home.csr
-rw-------. 1 root root 1679 сен 6 16:39 wildcard.redvirt.home.key
```

Добавление сертификата

Все последующие действия должны производиться на развернутом Engine РЕД Виртуализации, в каталоге **/tmp**.

Для добавления сертификата в систему РЕД Виртуализации необходимо:

1. Скопировать с созданного ранее центра сертификации файлы **wildcard.redvirt.home.crt**, **wildcard.redvirt.home.key**, **root.pem** на хост РЕД Виртуализации в папку **/tmp**.

2. Создать файл с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -export -out apache.p12 -inkey wildcard.redvirt.home.key -in wildcard.redvirt.home.crt
```

Пароль указывать не нужно.

3. Экспортировать ключ из созданного на предыдущем шаге файла с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -in apache.p12 -nocerts -nodes > apache.key
```

Пароль указывать не нужно.

4. Экспортировать файл с расширением cer из файла **apache.p12**:

```
openssl pkcs12 -in apache.p12 -nokeys > apache.cer
```

Теперь с точки зрения самоподписанного **SSL**-сертификата в системе РЕД Виртуализации существуют все необходимые файлы:

- **/tmp/root.pem;**
- **/tmp/apache.p12;**
- **/tmp/apache.key;**
- **/tmp/apache.cer.**

5. Затем создать резервную копию текущего файла **apache.p12**:

```
cp -p /etc/pki/ovirt-engine/keys/apache.p12 /tmp/apache.p12.bck
```

6. Заменить текущий файл **apache.p12** на созданный в п. 2 файл:

```
cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

7. Заменить имеющийся ЦС на созданный в п. 2 раздела 1 «Создание центра сертификации» корневой сертификат и обновить хранилище доверенных сертификатов:

```
cp /tmp/root.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

8. Удалить символическую ссылку и сохранить сертификат как apache-ca.pem в соответствующий каталог:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
cp /tmp/root.pem /etc/pki/ovirt-engine/apache-ca.pem
```

9. Создать резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

10. Скопировать выданный закрытый ключ и сертификат в соответствующие каталоги:

```
cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

11. Перезапустить сервер **apache**:

```
systemctl restart httpd.service
```

12. Создать новый файл конфигурации доверенного хранилища со следующим содержимым:

```
nano /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

13. Сохранить файл.

14. Отредактировать файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf**:

```
nano /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf
```

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

15. Переопределить конфигурацию **ovirt-engine /etc/ovirt-imageio/conf.d/50-engine.conf**:

```
cp /etc/ovirt-imageio/conf.d/50-engine.conf /etc/ovirt-imageio/conf.d/99-local.conf
```

16. Перезапустить необходимые службы:

```
systemctl restart ovirt-provider-ovn.service
systemctl restart ovirt-imageio
systemctl restart ovirt-websocket-proxy
systemctl restart ovirt-engine.service
```

17. Скопировать и установить сертификат **root.pem** в качестве корневого на машине, где будет производиться администрирование системы РЕД Виртуализация. Если все настроено верно, подключение к порталу администратора и порталу виртуальных машин будет производиться без вывода предупреждений о подлинности сертификата, используемого для шифрования **HTTPS**-трафика.

Инструмент для смены доменного имени Engine

Синтаксис команды
Процедура смены доменного имени Engine

Когда команда engine-setup запускается в чистой среде, она создает ряд сертификатов и ключей, в которых используется полное доменное имя Engine, указанное в процессе установки. Если полное доменное имя Engine позднее необходимо изменить (например, из-за переноса машины, на которой размещен Engine, в другой домен), записи полного доменного имени должны быть обновлены, чтобы отразить новое имя. Команда **ovirt-engine-rename** автоматизирует эту задачу.

Команда ovirt-engine-rename обновляет записи полного доменного имени Engine в следующих файлах:

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf;
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf;
- /etc/pki/ovirt-engine/cert.conf;
- /etc/pki/ovirt-engine/cert.template;
- /etc/pki/ovirt-engine/certs/apache.cer;
- /etc/pki/ovirt-engine/keys/apache.key.nopass;
- /etc/pki/ovirt-engine/keys/apache.p12.

Примечание.

В процессе обновления старое имя хоста должно быть разрешено. Если **Engine Rename Tool** выводит сообщение:

```
[ ERROR ] Host name is not valid: <OLD FQDN> did not resolve into an IP address
```

добавьте старое имя хоста в файл **/etc/hosts**, используйте **Engine Rename Tool**, а затем удалите старое имя хоста из файла **/etc/hosts**.

Синтаксис команды

Основной синтаксис команды ovirt-engine-rename:

```
/usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

Команда также принимает следующие параметры:

- **--newname=<новое_имя>** - позволяет указать новое полное доменное имя для Engine без взаимодействия с пользователем;
- **--log=<путь_к_файлу>** - позволяет указать путь и имя файла, в который должны быть записаны журналы операции переименования;
- **--config=<путь_к_файлу>** - позволяет указать путь и имя файла конфигурации для загрузки в операцию переименования;
- **--config-append=<путь_к_файлу>** - позволяет указать путь и имя файла конфигурации для добавления к операции переименования. Этот параметр можно использовать для указания пути и имени существующего файла ответов для автоматизации операции переименования.
- **--generate-answer=<путь_к_файлу>** - позволяет указать путь и имя файла, в который ovirt-engine-rename записываются ваши ответы и значения, измененные командой.

Процедура смены доменного имени Engine

Вы можете использовать команду ovirt-engine-rename для обновления записей полного доменного имени (**FQDN**) Engine.

Инструмент проверяет, предоставляет ли Engine локальный домен ISO или хранилище данных. Если предоставляет, инструмент предлагает пользователю извлечь, завершить работу или перевести в режим обслуживания любую виртуальную машину или домен хранения, подключенный к хранилищу, прежде чем продолжить операцию. Это гарантирует, что виртуальные машины не потеряют связь со своими виртуальными дисками, а домены хранения ISO не потеряют связь во время процесса переименования.

Для смены доменного имени Engine необходимо выполнить следующие действия:

1. Переведите всю систему РЕД Виртуализации в режим глобального обслуживания. Для этого на одном из хостов выполните команду:

```
hosted-engine --set-maintenance --mode=global
```

2. Подготовьте все DNS и другие соответствующие записи для создания нового полного доменного имени.

Если DNS не используется, внесите изменения в файлы с именем /etc/hosts как на хостах, так и на Engine.

3. Обновите конфигурацию DHCP-сервера, если используется DHCP.

4. Обновите имя в Engine:

```
hostnamectl set-hostname <новое_доменное_имя>
```

5. Запустите утилиту следующей командой:

```
/usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

6. При появлении запроса введите новое полное доменное имя для Engine:

```
New fully qualified server name:<новое_доменное_имя>
```

7. При появлении запроса нажмите «**Enter**», чтобы остановить обслуживание Engine:

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

После этого команда `ovirt-engine-rename` обновит записи полного доменного имени Engine.

8. Перезапустите службу загрузки образов, чтобы она обновила свои данные по сертификатам:

```
systemctl restart ovirt-imageio
```

9. Для **self-hosted Engine** выполните следующие дополнительные действия:

9.1. Выполните нижеприведенную команду на каждом существующем хосте **self-hosted Engine**:

```
hosted-engine --set-shared-config fqdn <новое_доменное_имя> --type=he_local
```

Данная команда изменяет полное доменное имя в локальной копии **/etc/ovirt-hosted-engine/hosted-engine.conf** каждого узла **self-hosted Engine**.

9.2. Выполните следующую команду на одном из хостов **self-hosted Engine**:

```
hosted-engine --set-shared-config fqdn <новое_доменное_имя> --type=he_shared
```

Данная команда изменяет полное доменное имя в основной копии **/etc/ovirt-hosted-engine/hosted-engine.conf** в общем домене хранения.

Теперь все новые и существующие узлы **self-hosted engine** будут использовать новое полное доменное имя.

10. Отключите режим глобального обслуживания. Для этого выполните на одном из улов команду:

```
hosted-engine --set-maintenance --mode=none
```

Хосты со статусом «Non Responsive»

Статус «**Non Responsive**» означает, что *HostedEngine* не получил своевременного ответа от службы **vdsmd**, запущенной на хосте.

ВАЖНО!

ВМ *HostedEngine* **запрещено** выключать и перезагружать!

1. Сначала необходимо убедиться, что все остальные ВМ работают. Например, проверить доступность через **ping**, подключение по **ssh** и т. д.

2. Выяснить причину, по которой *HostedEngine* не получил своевременного ответа (неполадки сети, блокировка или аварийное завершение службы **vdsmd**).

Для этого на хосте необходимо выполнить:

```
grep "Worker blocked" /var/log/vdsm/vdsm.log
grep -A20 "Traceback" /var/log/vdsm/vdsm.log
```

3. Журналы на момент инцидента передать в **Техническую поддержку РЕД Виртуализации**.

Файлы журналов находятся в папке **/var/log**.

4. Проверить доступность хоста и работоспособность его служб следующими командами:

- проверка работоспособности путей до СХД:

```
multipath -ll
```

- проверка доступных ресурсов:

```
top
```

- проверка блокировки областей памяти на хранилищах:

```
sanlock status
```

5. Проверить лог-файл **/var/log/messages** на наличие критических ошибок системы.

Для этого можно воспользоваться командой:

```
journalctl -b -p err
```

6. Выполнить проверку и перезапуск службы **vdsm**:

```
systemctl status vdsmd
systemctl restart vdsmd
```

Настройка параметров расширения "тонких" дисков ВМ

Для настройки параметров расширения "тонких" дисков необходимо выполнить следующий алгоритм действий:

1. Переведите хост в режим обслуживания, выбрав в веб-интерфейсе «**Управление** — **Обслуживание**».

2. Перейдите в терминал хоста.

3. Откройте файл:

```
nano /etc/vdsm/vdsm.conf.d/99-local.conf
```

4. Измените следующие параметры:

```
volume_utilization_percent=25
volume_utilization_chunk_mb=2048
```

здесь:

- `volume_utilization_percent=25` — процент заполнения блока, при достижении которого начнётся расширение виртуального диска;
- `volume_utilization_chunk_mb=2048` — размер блока, на который производится увеличение объема виртуального диска при достижении процента заполнения.

Т.е. при заполнении блока на 25% от его размера (2048 МБ) будет произведено увеличение виртуального диска на 2048 МБ.

5. Выполните команду применения настроек:

```
vdsm-tool configure --force
```

6. Выполните перезапуск сервиса **vdsm**:

```
systemctl restart vdsm
```

7. Выведите хост из режима обслуживания, выбрав в веб-интерфейсе «**Управление** — **Включить**».

Часто задаваемые вопросы (FAQ)

Как пользоваться РЕД Виртуализацией?

Через веб-интерфейс необходимо подключиться к «**Порталу виртуальных машин**» или «**Порталу администрирования**». При выборе нужной ВМ следует нажать кнопку «**Консоль**», работа с гостевой ОС будет осуществляться через программу **virt-viewer** (существует для Linux и Windows).

Какие гостевые системы поддерживает «РЕД Виртуализация»?

РЕД Виртуализация поддерживает гостевые операционные системы *GNU / Linux*, *Microsoft Windows* и *FreeBSD*.

Какими протоколами обеспечивается доступ к виртуальным машинам?

Доступ к ВМ обеспечивается протоколами **SPICE**, **VNC** или **RDP** (только для Windows). Рекомендуется использовать протокол **SPICE**, т.к. он поддерживает максимальное разрешение 2560x1600 пикселей, а также проброс USB с рабочего ПК пользователя в гостевую ОС.

Каким браузером пользоваться для доступа к веб-интерфейсу РЕД Виртуализации?

Мы рекомендуем использовать последние версии браузеров **Mozilla Firefox** или **Chromium**.

Как проверить, поддерживает ли процессор виртуализацию?

Необходимо включить виртуализацию в BIOS и перезагрузить хост. После этого:

- Загрузить ОС и зарегистрироваться под пользователем, имеющим права администратора;
- В командной строке выполнить следующую команду:

```
grep -E 'svm|vmx' /proc/cpuinfo
```

Если в ответе команды отображается какой-либо вывод, значит процессор поддерживает аппаратную виртуализацию.

Какие хранилища могут использоваться РЕД Виртуализацией?

Хранение данных может быть реализовано с использованием:

- сетевой файловой системы *NFS*;
- *GlusterFS*;
- других *POSIX*-совместимые файловые системы;
- *iSCSI*;
- *локального* хранилища, подключенного непосредственно к хостам виртуализации;
- протокола *Fibre Channel* (FCP);
- параллельной *NFS* (pNFS).

Настройка хранилища является **обязательным** условием для нового центра обработки данных, поскольку центр обработки данных не может быть инициализирован, если домены хранения не подключены и не активированы.

Чем подключиться к консоли ВМ?

На компьютере, с которого планируется подключение, должен быть установлен клиент удаленного просмотра «**Virt-viewer**». В операционной системе РЕД ОС его можно установить командой:

```
dnf install virt-viewer
```

Для Windows также существует версия данного приложения.

Какие типы процессоров поддерживаются системой РЕД Виртуализации?

Поддерживаются следующие модели процессоров **AMD**:

- Opteron G1-G5 (при развёртывании РЕД Виртуализации 7.3 по умолчанию поддерживаются только G4-G5);
- EPYC.

Поддерживаются следующие модели процессоров **Intel**:

- Nehalem;
- Westmere;
- SandyBridge;
- IvyBridge;
- Haswell;
- Broadwell;
- Cascadelake (поддерживается, но будет определяться как Skylake);
- Skylake.

Поддерживаются следующие модели процессоров **AArch64**:

- Huawei Kunpeng 920.

Как определить, может ли на хост мигрировать ВМ управления?

В списке хостов на панели администрирования РЕД Виртуализации рядом с именами тех хостов, которые могут принять на себя *Engine*, отображается значок короны. *Серебряный* означает, что хост может принять на себя ВМ управления, *золотой* — на хосте уже находится ВМ управления. Если значка *короны нет,* значит хост не может принимать ВМ *Engine*.

Что нужно для успешной миграции виртуальных машин в реальном времени?

Для успешной миграции виртуальных машин в реальном времени должны быть выполнены следующие условия:

- исходный и целевой хосты должны находиться в пределах одного кластера;

Примечание.

Живая миграция виртуальных машин между разными кластерами обычно не рекомендуется.

- хосты источника и назначения имеют статус **Up**;
- хосты источника и назначения имеют доступ к одним и тем же виртуальным сетям и VLAN;
- хосты источника и назначения имеют доступ к домену хранения данных, в котором находится виртуальная машина;
- у хоста назначения достаточно ЦП для поддержки требований виртуальной машины;
- у хоста назначения достаточно неиспользуемой ОЗУ для поддержки требований виртуальной машины;
- у переносимой виртуальной машины нет **cache!=none** настраиваемых свойств.

Что нужно для миграции высокодоступных виртуальных машин?

Для миграции высокодоступных виртуальных машин должны быть соблюдены следующие условия:

- для хостов, на которых запущены высокодоступные виртуальные машины, необходимо настроить управление питанием;
- хост, на котором запущена виртуальная машина с высокой доступностью, должен быть частью кластера, в котором есть другие доступные хосты;
- хост назначения должен быть запущен;
- хосты источника и назначения должны иметь доступ к домену данных, в котором находится виртуальная машина;
- хосты источника и назначения должны иметь доступ к одним и тем же виртуальным сетям и VLAN;
- на хосте назначения должно быть достаточно ЦП, которые не используются для поддержки требований виртуальной машины;
- на целевом хосте должно быть достаточно оперативной памяти, которая не используется для поддержки требований виртуальной машины.

Не получается загрузить ISO-образ в РЕД Виртуализации. После начала загрузки выводится сообщение вида «Приостановлено системой». Почему?

Для загрузки образов и дисков в систему необходимо загрузить в используемый браузер **сертификат** установленной РЕД

Виртуализации. Загрузка сертификата доступна на приветственной странице РЕД Виртуализации в поле «**Загрузки**» - «**Корневой сертификат**».

+ После скачивания сертификата РЕД Виртуализации и попытке его установить браузер не видит сертификат. Как исправить?

При загрузке сертификата через **Mozilla Firefox** сертификат сохраняется как файл без расширения. Чтобы браузер увидел сертификат в папке, достаточно выбрать отображение «**Все файлы**».

+ Как добавить пользователя в систему РЕД Виртуализации?

Пользователи в системе РЕД Виртуализация могут быть подключены извне, например, из домена, или созданы локально на виртуальной машине *HostedEngine*.

Для создания локального пользователя можно зайти в консоль *Engine* через веб-интерфейс «**Портал администратора**» или подключиться по *ssh*, после этого выполнить команду:

```
ovirt-aaa-jdbc-tool user add <username> --attribute=firstName=<First-Name> \ --attribute=lastName=<Last-Name>
```

Задать пароль новому пользователю можно командой:

```
ovirt-aaa-jdbc-tool user password-reset <username>
```

+ Почему после перезапуска системы РЕД Виртуализации не получается зайти под доменной учётной записью в веб-портал?

Такое случается, если отсутствует А-запись о домене на сервере *DNS*. Если нет возможности сделать такую запись, нужно прописать *IP* домена в **/etc/resolv.conf** на ВМ *Engine* первой записью.

+ В чём различие между предварительно распределённым виртуальным диском и тонким предоставлением виртуального диска?

Виртуальный диск с предварительно выделенным форматом (*RAW*) имеет значительно более высокую скорость записи, чем виртуальный диск с форматом тонкой подготовки (*QCOW2*).

Тонкая подготовка занимает значительно меньше времени для создания виртуального диска. Формат *thin provision* подходит для виртуальных машин, не требующих интенсивного ввода-вывода.

Предварительно выделенный формат рекомендуется для виртуальных машин с высокой скоростью записи ввода-вывода. Если виртуальная машина способна записывать более 1 ГБ каждые четыре секунды, по возможности используйте предварительно выделенные диски.

+ Как отключить и обратно подключить домен хранения к системе РЕД Виртуализации?

Для отсоединения домена хранения от центра обработки данных выполните следующий алгоритм действий:

1. Перейдите в **Storage** — **Domains**.
2. Нажмите на имя домена, будут открыты подробные сведения.
3. Выберите вкладку **Data Center**.
4. Нажмите «**Maintenance**».
5. Щелкните **OK**, чтобы перейти в режим обслуживания.
6. Выберите «**Detach**».
7. Нажмите **OK**, чтобы отсоединить домен.

Домен хранения будет отключен от дата-центра.

Для присоединения домена хранения к центру обработки данных выполните следующий алгоритм действий:

1. Перейдите в **Storage** — **Domains**.
2. Нажмите на имя домена, будут открыты подробные сведения.
3. Выберите вкладку **Data Center**.

4. Щелкните «**Attach**».
5. Выберите нужный дата-центр.
6. Щелкните **OK**.

Домен хранения присоединяется к центру обработки данных и активируется автоматически.

Образ РЕД Виртуализации 7.2 записан на флешку, но установить не получается. Почему?

ISO-образ РЕД Виртуализации 7.2 необходимо разместить на жёстком диске установленной системы РЕД ОС 7.2 конфигурации Сервер минимальный (без графики) и смонтировать в заранее подготовленную папку. После этого запустить установку можно файлом **install.run**.

Как увеличить время тикета для загрузки виртуальных дисков? По умолчанию он составляет 10 часов.

На ВМ HostedEngine необходимо выполнить команду с установкой жизни тикета в секундах:

```
engine-config -s ImageTransferClientTicketValidityInSeconds=180000
```

После этого следует перезапустить сервис командой:

```
systemctl restart ovirt-engine
```

Как настроить автоматический запуск виртуальных машин в случае перезапуска системы РЕД Виртуализации?

Необходимо сделать эти машины «высокодоступными» (*HA — high available*).

Высокая доступность должна быть настроена индивидуально для каждой виртуальной машины.

Для настройки высокодоступной виртуальной машины выполните следующие действия:

1. Нажмите **Виртуализация** — **Виртуальные машины** и выберите виртуальную машину.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Высокая доступность**.
4. Установите флажок **Высокая доступность**, чтобы включить высокую доступность виртуальной машины.
5. В раскрывающемся списке **No VM Lease** виртуальной машины выберите домен хранения, в котором будет храниться аренда виртуальной машины, или выберите **No VM Lease**, чтобы отключить эту функцию.
6. Выберите **AUTO_RESUME**, **LEAVE_PAUSED** или **KILL** из раскрывающегося списка **Resume Behavior**. Если вы определили аренду виртуальной машины, **Уничтожить** - единственный доступный вариант.
7. В раскрывающемся списке **Приоритет** выберите **Низкий**, **Средний** или **Высокий**. Когда запускается миграция, создается очередь, в которой сначала переносятся виртуальные машины с высоким приоритетом. Если в кластере не хватает ресурсов, переносятся только виртуальные машины с высоким приоритетом.
8. Нажмите **OK**.

Заканчивается место на виртуальной машине управления Hosted Engine. Что делать?

При активной работе с системой и виртуальными машинами в ней место могут занимать логи. Проверьте размер папки **/var/log**. При необходимости настройте ротацию логов в файле **/etc/logrotate.conf**.

Не пробрасывается USB с пользовательского ПК в гостевую ОС. Почему?

Необходимо проверить, по какому протоколу реализовано подключение к ВМ. **VNC** не пробрасывает USB, для этого нужно использовать протокол **SPICE**.

Есть ли встроенное решение по созданию бекапов ВМ в РЕД Виртуализации?

Нет, в данный момент такое решение от нашей компании разрабатывается для РЕД Виртуализации 7.3. Для резервного копирования можно воспользоваться сторонними решениями.

Как перенести виртуальный диск машины управления Engine в другое сетевое хранилище?

Через веб-интерфейс перенос диска ВМ управления невозможен.

Для переноса диска используется следующий алгоритм действий:

1. На *ВМ Engine* запускается резервное копирование «движка».
2. Резервная копия переносится на один из хостов и запускается развёртывание *Engine* из файла.
3. В процессе развёртывания указывается новый домен хранения.
4. После развёртывания запускается восстановленная система управления с диском в новом домене хранения.

Мне необходимо привязать к ВМ диск объёмом более 8 ТБ, но система не позволяет. Как можно увеличить размер диска?

На ВМ *HostedEngine* выполните команду:

```
engine-config -s MaxBlockDiskSizeInGibiBytes=16384
```

Примечание.

Стабильная работа виртуального диска размером более 8 ТБ не гарантируется.

На вычислительных нодах есть много свободного места на жёстких дисках. Как их подключить в качестве хранилища к системе РЕД Виртуализации?

Не рекомендуется использовать диски на вычислительных хостах РЕД Виртуализации для хранения данных.

Если вы принимаете риски, есть возможность настроить на ОС хоста *NFS* или *ISCSI*-сервисы. Следует учитывать, что после настройки необходимо внести эти сервисы в **firewall**. Пример команд *для nfs*:

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

Какие логи смотреть, когда что-то не работает в системе РЕД Виртуализации?

Основные данные по работе системы находятся на *ВМ Engine* по пути **/var/log/ovirt-engine**.

Данные по работе конкретного хоста РЕД Виртуализации находятся в папке **/var/log/vdsm/** на этом хосте.

Для полноценного анализа ошибки необходимы все логи из папки **/var/log** из *ВМ Engine* и хоста.

Хост подключен к системе РЕД Виртуализации, но после установки он переходит в состояние «Non Operational» и не запускается. Почему?

Возможно тип процессора нового хоста не соответствует типу ЦП, заданному в кластере. То есть ЦП кластера новее, чем тип ЦП нового узла. Для работы нового узла нужно указать тип ЦП в кластере такой же, как на новом хосте. Следует учитывать, что после этого все хосты кластера будут работать «на уровне» самого медленного узла.

Есть ли возможность установить РЕД Виртуализацию 7.3 не через веб-интерфейс, а через терминал?

Да, такая возможность есть. После установки образа системы РЕД Виртуализации 7.3 запустите установку командой:

```
ovirt-hosted-engine-setup
```

Что делать, если после установки меню Cockpit отличается от того, что указано в инструкции (нет пунктов

виртуализации, оформлено не в цветах РЕД Виртуализации)?

Для решения данной проблемы установите дополнительный модуль:

```
dnf install cockpit-ovirt-dashboard
```

При развёртывании Engine разрывается соединение с хостом. Почему?

В момент развертывания на сервере происходит создание виртуального сетевого интерфейса и переключение его «мостом» на физический интерфейс. Поскольку у нового интерфейса другой mac-адрес, он может получить другой IP, из-за этого возможна потеря связи с хостом.

Где я могу найти драйвера и гостевые агенты для гостевых ОС Windows?

Пакет драйверов можно найти в сети интернет.

Например: https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/.

Можно ли на серверах РЕД Виртуализации использовать программный продукт Secret Net?

SecretNet накладывает ограничения на использование конкретной версии ядра. С другой версией ядра **SecretNet** работать не будет (ОС, соответственно, тоже).

Поэтому использование **SecretNet** — это отключение обновлений ядра и связанных пакетов (то есть будет невозможно устранять уязвимости ИБ).

Работа с **SecretNet** обычно ведется на рабочих станциях. Применения **SecretNet** на серверах РЕД Виртуализации не предусмотрено.

В чём отличие между установкой РЕД Виртуализации в режиме Standalone и Host?

Установка **Standalone** подразумевает использование только одного вычислительного хоста. Вся структура управления разворачивается на хостовой ОС. ВМ управления РЕД Виртуализацией не создаётся. В качестве базового СХД может быть использовано локальное хранилище сервера. Дальнейшее расширение вычислительных мощностей до кластера невозможно. Только добавление дополнительных СХД.

Установка типа **Host** подразумевает развёртывание ВМ управления *HostedEngine*. Так же установка должна проходить на заранее подготовленное СХД. Локальные хранилища напрямую использовать не получится. Возможно дальнейшее расширение до кластера.

Что делать, когда при попытке доступа к своей ВМ пользователь получает всплывающее сообщение вида «Консоль используется другим пользователем, продолжить?».

При этом ни принятие положительного решения, ни перезагрузка ВМ не даёт результата.

Такое бывает, когда администратор РЕД Виртуализации подключается через консоль к рабочей ВМ пользователя для настройки гостевой ОС.

Чтобы после этого права на доступ к консоли вернулись к пользователю, необходимо в настройках ВМ установить флажок «**Выключить строгую проверку пользователей**». Для этого на вкладке «**Консоль**» разверните область «**Дополнительные параметры**».

Как переименовать существующий хост в системе РЕД Виртуализация?

Для смены имени существующего хоста в системе РЕД Виртуализация необходимо:

1. Удалить хост из системы РЕД Виртуализация:

- перейдите во вкладку «Виртуализация - Узлы»;
- переведите хост в режим обслуживания, выбрав пункт меню «Управление - Обслуживание»;
- нажмите кнопку «Удалить».

2. Сменить имя в хостовой ОС командой:

```
hostnamectl set-hostname <новое_имя_хоста>
```

3. Внести изменения имени в DNS или, если DNS не используется, во все файлы **/etc/hosts** (на хостах и на BM Engine).

4. Подключить хост к системе РЕД Виртуализации, используя новое имя.

Как можно мигрировать ВМ из Proxmox в РЕД Виртуализацию?

Прямое подключение Proxmox к РЕД Виртуализации не предусмотрено в силу отсутствия у PVE libvirt. Для переноса ВМ необходимо выгрузить её в формате **.ova** из Proxmox. После чего перенести образ на хост РЕД Виртуализации и произвести импорт из ova-файла.

Какой образ необходим, чтобы установить гостевые агенты, инструменты и драйверы на ВМ с операционными системами Windows XP и Windows Server 2003?

Для операционных систем Windows XP и Windows Server 2003 рекомендуем использовать ISO-образ oVirt-toolsSetup: https://share.red-soft.ru/index.php/s/qodTijx5DXtkNYn.

Как можно выяснить какая конфигурация гипервизора установлена на сервере?

Конфигурацию гипервизора можно проверить следующими способами:

1. По списку репозиториев.
   - При установке в режиме Standalone в директории /etc/yum.repos.d/ будут находиться следующие файлы репозиториев: **RedVirtualization-7.3-engine-updates.repo** и **RedVirtualization-7.3-host-updates.repo;**
   - При установке в режиме Host по пути /etc/yum.repos.d/ будет доступен только репозиторий **RedVirtualization-7.3-host-updates.repo**.

2. По содержанию логов.
   - По пути /var/log при установке в режиме Standalone будут находится папки vdsm и ovirt-engine, тогда как при установке в режиме Host только vdsm, ovirt-engine отсутствует.

Как можно получить список всех ВМ, у которых есть снимки диска?

Чтобы получить список всех ВМ, у которых есть снимки диска, выполните следующие действия:

1. На портале администрирования нажмите **«Хранилище»** – **«Домены»** .
2. Нажмите имя домена. Откроется окно сведений.
3. Выберите вкладку **«Снимки диска»** . Отобразится список всех ВМ, у которых есть снимки диска.

Не удалось осуществить подключение к графическому интерфейсу ВМ через SPICE консоль.

Для того, чтобы подключиться к графическому интерфейсу ВМ через SPICE консоль необходимо выполнить следующие условия:

1. В сети должны быть доступны следующие порты:
   - для SSH подключения к хосту 22 порт;
   - к консоли виртуальной машины 2222 порт (hosted-engine), 2223 порт (Standalone);
   - диапазон портов 5900-6923 для SPICE+VNC.

2. Необходимо разрешить все входящие соединения.

После успешной миграции ВМ из одного хранилища данных в другое необходимо отключить пустое хранилище данных из домена хранения. Как это корректно сделать?

Можно удалить LUN, переведя область хранения в режим обслуживания. Для этого необходимо выключить все виртуальные машины, работающие в домене хранения.

Для удаления LUN выполните следующие действия:

1. На портале администрирования нажмите **«Хранилище»** – **«Домены»**.
2. Нажмите имя домена. Откроется окно сведений.
3. Выберите вкладку **«Дата-центр»**.
4. Нажмите кнопку **«Обслуживание»**, затем нажмите **«OK»**.

Примечание.

Флажок **«Игнорировать сбой обновления OVF»** позволяет домену хранения перейти в режим обслуживания даже в случае сбоя обновления OVF.

После выполнения перечисленных выше действий домен хранения будет деактивирован и будет иметь состояние **«Неактивный»**. Теперь можно редактировать, отсоединять, удалять или повторно активировать неактивные домены хранения из центра обработки данных.

Почему при добавлении в РЕД Виртуализацию доменного пользователя, он не отображается в поиске?

Для того, чтобы пользователь отобразился на портале администрирования, необходимо в подключенном к РЕД Виртуализации Active Directory задать атрибут **«sn»**. В случае, если этого атрибута нет, то необходимо включить атрибут **«sAMAccountName»**.

Как исправить ошибку обновления в терминале хоста через dnf update?

У хоста есть доступ в Интернет. При попытке его обновления через терминальную команду **«dnf update»** выводится ошибка **«Error: Не удалось загрузить метаданные для репозитория 'virtualization-7.3-host-updates': repomd.xml parser error: Parse error at line: 15 (SYSTEM or PUBLIC, the URI is missing)»**. Это означает, что необходимо отключить или корректно настроить межсетевой экран, который блокирует доступ до репозитория РЕД Виртуализации.

Как поменять язык интерфейса?

После осуществления входа в веб-интерфейс открывается главная страница РЕД Виртуализации, где происходит выбор портала. На данной странице в выпадающем меню в левом нижнем углу можно выбрать желаемый язык интерфейса.

Как изменить часовой пояс в гостевой ОС?

Когда часовой пояс в гостевой ОС отличается от настроек конфигурации, напротив ВМ появляется предупреждение: **«Actual timezone in the guest differs from the configuration»**.

Для изменения часового пояса в гостевой ОС выполните следующие действия:

1. На портале администрирования нажмите **«Виртуализация»** – **«Виртуальные машины»**.
2. Выберите виртуальную машину, на которой необходимо изменить часовой пояс и нажмите **«Изменить»**.
3. Выберите вкладку **«Система»**.
4. Измените параметр смещения **«Смещение аппаратных часов»** на значение **«Russian Standart Time»**, затем нажмите **«OK»**.

Информация об обновлениях

UPD-20241230

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **vdsm-4.40.100.2-11.el7**
  - Устранена проблема установки на GlusterFS версий выше 10

Обновление ВМ управления:

- **java-11-openjdk-11.0.25.0.9-3.el7**
  - Устранены уязвимости CVE-2024-21235, CVE-2024-21210, CVE-2024-21208, CVE-2024-21217

UPD-20241129

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.167-2.el7virt**
  - Устранены множественные уязвимости
- **kmod-kvdo-1:6.2.9.1-8.el7virt**
  - Пакет пересобран для работы с новой версией ядра

Обновление ВМ управления:

- **kernel-lt-5.15.167-2.el7virt**
  - Устранены множественные уязвимости

UPD-20241126

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **ansible-2.9.27-5.el7**
  - Устранены множественные уязвимости (CVE-2021-3620, CVE-2023-5115, CVE-2024-0690)
- **expat-2.6.3-1.el7**
  - Устранены множественные уязвимости (CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-28757)
- **linux-firmware-2024101702.el7.3**
  - Обновление микропрограмм оборудования
- **pyOpenSSL-1:19.0.0-3.el7**
  - Понижена версия пакета, для устранения проблем с обновлением узлов в некоторых сборках
- **python3-3.8.20-2.el7**
  - Устранены множественные уязвимости (CVE-2024-7592, CVE-2024-8088, CVE-2024-4032, CVE-2024-6923, CVE-2024-0397, CVE-2023-52425, CVE-2024-0450, CVE-2023-6597, CVE-2023-27043)
    python-cryptography-1:3.2.1-5.el7
    - Устранены множественные уязвимости (CVE-2023-49083, CVE-2023-23931, CVE-2020-36242)
    - Понижена версия пакета, для устранения проблем с обновлением узлов в некоторых сборках
  - **python-jinja2-1:3.0.3-2.el7**
    - Устранена уязвимость CVE-2024-22195
  - **python-jwcrypto-1:0.6.0-3.el7**
    - Устранены множественные уязвимости (CVE-2024-28102, CVE-2023-6681, CVE-2022-3102)
    - Понижена версия пакета, для устранения проблем с обновлением узлов в некоторых сборках
  - **python-jwt-1:2.4.0-2.el7**
    - Пересобран с повышением эпохи, для устранения конфликтов с репозиториями РЕД ОС

- **python-paramiko-1:3.4.0-3.el7**
  - Устранена уязвимость CVE-2023-48795 (Terrapin Attack)

Обновление ВМ управления:

- **expat-2.6.3-1.el7**
  - Устранены множественные уязвимости (CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-28757)
- **postgresql-jdbc-1:42.2.8-4.el7**
  - Устранена уязвимость CVE-2022-41946
- **pyOpenSSL-1:19.0.0-3.el7**
  - Понижена версия пакета, для устранения проблем с обновлением узлов в некоторых сборках
- **python3-3.8.20-2.el7**
  - Устранены множественные уязвимости (CVE-2024-7592, CVE-2024-8088, CVE-2024-4032, CVE-2024-6923, CVE-2024-0397, CVE-2023-52425, CVE-2024-0450, CVE-2023-6597, CVE-2023-27043)

    python-cryptography-1:3.2.1-5.el7
    - Устранены множественные уязвимости (CVE-2023-49083, CVE-2023-23931, CVE-2020-36242)
    - Понижена версия пакета, для устранения проблем с обновлением узлов в некоторых сборках
  - **python-jinja2-1:3.0.3-2.el7**
    - Устранена уязвимость CVE-2024-22195
  - **python-jwcrypto-1:0.6.0-3.el7**
    - Устранены множественные уязвимости (CVE-2024-28102, CVE-2023-6681, CVE-2022-3102)
    - Понижена версия пакета, для устранения проблем с обновлением узлов в некоторых сборках
  - **python-jwt-1:2.4.0-2.el7**
    - Пересобран с повышением эпохи, для устранения конфликтов с репозиториями РЕД ОС
  - **python-paramiko-1:3.4.0-3.el7**
    - Устранена уязвимость CVE-2023-48795 (Terrapin Attack)

UPD-20241120

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **openssl-1.1.1q-10.el7**
  - Устранены множественные уязвимости (CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466)

Обновление ВМ управления:

- **ansible-2.9.27-5.el7**
  - Устранены множественные уязвимости (CVE-2021-3620, CVE-2023-5115, CVE-2024-0690)
- **gdk-pixbuf2-2.40.0-10.el7**
  - Устранена уязвимость CVE-2022-48622
- **libgsf-1.14.47-4.el7**
  - Устранены множественные уязвимости (CVE-2024-36474, CVE-2024-42415)
- **openssl-1.1.1q-10.el7**
  - Устранены множественные уязвимости (CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466)
- **python-werkzeug-3.0.3-1.el7**
  - Устранены множественные уязвимости (CVE-2023-23934, CVE-2023-25577, CVE-2023-46136, CVE-2024-34069)

UPD-20241118

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **openvswitch-2.11.3-91.el7**

- Устранены множественные уязвимости (CVE-2024-22563, CVE-2023-1668, CVE-2023-5366, CVE-2022-4337, CVE-2022-4338)

Обновление ВМ управления:

- **openvswitch-2.11.3-91.el7**
  - Устранены множественные уязвимости (CVE-2024-22563, CVE-2023-1668, CVE-2023-5366, CVE-2022-4337, CVE-2022-4338)
- **postgresql-jdbc-42.2.8-3.el7**
  - Устранена уязвимость CVE-2022-21724
  - Для установки необходимо внести изменения в файл /etc/dnf/plugins/versionlock.list (заменить postgresql-jdbc-42.2.8-2.el7.noarch на postgresql-jdbc-42.2.8-3.el7.noarch)

UPD-20240913

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **vdsm-4.40.100.2-7.el7**
  - Устранена утечка файловых дескрипторов.
- **sudo-1.9.15p5-1.el7**
  - Устранена уязвимость BDU-2023-07551.

Обновление ВМ управления:

- **sudo-1.9.15p5-1.el7**
  - Устранена уязвимость BDU-2023-07551.
- **python-PyMySQL-0.10.1-13.el7**
  - Устранена уязвимость CVE-2024-36039.

UPD-20240715

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **libtiff-4.5.1-8.el7**
  - Устранены уязвимости CVE-2023-6228, CVE-2023-52356.
- **openssh-8.9p1-12.el7**
  - Устранена уязвимость CVE-2024-6387.

Обновление ВМ управления:

- **libtiff-4.5.1-8.el7**
  - Устранены уязвимости CVE-2023-6228, CVE-2023-52356.
- **openssh-8.9p1-12.el7**
  - Устранена уязвимость CVE-2024-6387.

UPD-20240521

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **virt-v2v-1.45.90-5**
  - Исправлена ошибка миграции дисков из ESXi через SSH-соединение.
- **libvirt-7.6.0-10**
  - Устранено дублирование сообщения "Domain id= is tainted: custom-ga-command".

UPD-20240517

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **grub2-redos-theme-0.1-990.el7**
- **grub2-redvirt-theme-0.1-4.el7**
  - Заменена тема загрузки grub2.

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-27.el7**
  - Исправлены ошибки интерфейса.
  - Исправлена ошибка зависания загрузки диска в фазе "Завершение очистки".
  - Добавлена возможность использовать общие папки SPICE.

UPD-20240425

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-25.el7**
  - Исправлена ошибка с аутентификацией через внешний провайдер.
  - Устранена уязвимость CVE-2024-0822.

UPD-20240416

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-23.el7**
  - Исправлены ошибки работы сторонних продуктов через RESTful API, возникшей после обновления UPD-20240411.

UPD-20240411

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **selinux-policy-3.14.5-62.el7**
  - Исправлен контекст SELinux системных сервисов vdsmd и supervdsmd.
  - Устранена ошибка импорта ВМ из внешних источников.

- **python-aiohttp-3.9.3-1.el7**
  - Устранена уязвимость CVE-2024-23334.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **postgresql-*-12.18-2.el7**
  - Устранены множественные уязвимости CVE-2022-1552, CVE-2022-2625, CVE-2022-41862, CVE-2023-2454, CVE-2023-2455, CVE-2023-39417, CVE-2023-5868, CVE-2023-5869, CVE-2023-5870, CVE-2024-0985.

- **ovirt-engine-ui-extensions-1.2.7-3.el7**
  - Исправлены ошибки перевода.

- **ovirt-engine-4.4.10.8-21.el7**
- **ovirt-engine-extension-aaa-jdbc-tool-1.2.0-8.el7**
  - Исправлены множественные ошибки перевода.

- Добавлено отключаемое информационное окно о последних входах пользователя в систему.
- В окне настроек ВМ (а также шаблонов, экземпляров, пулов) добавлен переключатель совместимости с Termidesk.
- Добавлен запрет на удаление дата-центра, если есть хоть один ассоциированный с ним кластер.

- **ovirt-web-ui-1.7.2-3.el7**
  - Исправлены ошибки перевода.

UPD-20240226

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.131-2.el7virt**
  - Исправлена ошибка при обновлении.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **kernel-lt-5.15.131-2.el7virt**
  - Исправлена ошибка при обновлении.

Обновление включает зависимые пакеты.

UPD-20240206

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **openssh-8.9p1-11.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **openssh-8.9p1-11.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.

Обновление включает зависимые пакеты.

UPD-20240202

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **libssh-0.9.8-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.
- **libssh2-1.11.0-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.
- **traceroute-3:2.1.3-1.el7.x86_64**
  - Устранена уязвимость ROS-20231102-01, CVE-2023-46316.
- **kernel-lt-0:5.15.131-1.el7.3.x86_64**
  - Устранена уязвимость ROS-20231024-01, CVE-2023-4273.
- **glibc-0:2.28-9.el7.x86_64**
  - Устранена уязвимость ROS-20231020-10, CVE-2016-10228.
- **subscription-manager-0:1.29.0-3.el7.x86_64**
  - Устранена уязвимость ROS-20231018-03, CVE-2023-3899.

- **procps-ng-0:3.3.17-1.el7.x86_64**
  - Устранена уязвимость ROS-20231020-03, CVE-2023-4016.
- **curl-0:7.85.0-15.el7.3.x86_64**
  - Устранены множественные уязвимости CVE-2023-38546, CVE-2023-38545, ROS-20231016-05.

Обновление ВМ управления:

- **libssh-0.9.8-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.
- **libssh2-1.11.0-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.
- **traceroute-3:2.1.3-1.el7.x86_64**
  - Устранена уязвимость ROS-20231102-01, CVE-2023-46316.
- **kernel-lt-0:5.15.131-1.el7.3.x86_64**
  - Устранена уязвимость ROS-20231024-01, CVE-2023-4273.
- **glibc-0:2.28-9.el7.x86_64**
  - Устранена уязвимость ROS-20231020-10, CVE-2016-10228.
- **subscription-manager-0:1.29.0-3.el7.x86_64**
  - Устранена уязвимость ROS-20231018-03, CVE-2023-3899.
- **procps-ng-0:3.3.17-1.el7.x86_64**
  - Устранена уязвимость ROS-20231020-03, CVE-2023-4016.
- **curl-0:7.85.0-15.el7.3.x86_64**
  - Устранены множественные уязвимости CVE-2023-38546, CVE-2023-38545, ROS-20231016-05.

UPD-20231208

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-9-el7**
  - Исправлено отображение ассоциированных ВМ с дисками типа iso.
  - Добавлена панель с кнопками для отключения iso от ВМ.

UPD-20231127

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **vdsm-4.40.100.2-3.el7**
  - Исправлены ошибки, возникающие при попытке расширения тонких дисков.
  - Улучшена работа с сетью и подсистемой хранения.
- **ovirt-image-2.5.0-1.el7**
  - Улучшена работа с дисковой подсистемой.
  - Добавлена утилита для загрузки/выгрузки дисков из доменов хранения (ovirt-img).

Обновление включает зависимые пакеты.

UPD-20231009

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.117-4.el7**
- **kexec-tools-2.0.27-1.el7**

- **dracut-056-9.el7**
  - Исправлены ошибки в работе kdump.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **kernel-lt-5.15.117-4.el7**
- **kexec-tools-2.0.27-1.el7**
- **dracut-056-9.el7**
  - Исправлены ошибки в работе kdump.

Обновление включает зависимые пакеты.

UPD-20230925

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **expat-2.5.0-1.el7**
  - Устранена уязвимость с идентификаторами BDU:2023-02688 и CVE-2022-43680.

Обновление ВМ управления:

- **expat-2.5.0-1.el7**
  - Устранена уязвимость с идентификаторами BDU:2023-02688 и CVE-2022-43680.

UPD-20230915

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.117-3.el7virt**
  - Решена проблема аварийного завершения виртуальных машин с гостевой ОС Windows. Ранее для решения проблемы предоставлялось ядро kernel-lt-5.4.227-2.el7virt.
- **libguestfs-1.45.5-9.el7**
- **virt-v2v-1.45.90-4.el7**
  - Исправлена проблема импорта виртуальной машины с гостевой ОС Astra Linux.
- **rpm-4.17.0-9.el7.3**
  - Обновлен пакетный менеджер RPM.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-7.el7**
  - Исправлена логика сохранения переменных nvram.
- **rpm-4.17.0-9.el7.3**
  - Обновлен пакетный менеджер RPM.

Обновление включает зависимые пакеты.

Описание РЕД АДМ

РЕД АДМ Сервер
РЕД АДМ Клиент

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия РЕД АДМ**: 1.10

РЕД АДМ Сервер

РЕД АДМ Сервер позволяет управлять контроллером домена и автоматизирует типовые задачи администратора с парком рабочих станций и серверов на базе РЕД ОС. Система имеет веб-интерфейс управления.

Продукт имеет модульную структуру и может агрегировать в себе множество модулей администрирования различного назначения.

РЕД АДМ комплексно решает задачи:

- администрирования доменных учетных записей;
- централизованного управления рабочими станциями;
- журналирования операций.

Дистрибутив **РЕД АДМ Сервер** находится в стандартном репозитории РЕД ОС и представляет из себя rpm-пакет.

ВАЖНО!

Техническая поддержка по продукту РЕД АДМ из репозитория предоставляется **только** при действующем сертификате технической поддержки для РЕД ОС конфигурации «**Сервер**».

РЕД АДМ Клиент

РЕД АДМ Клиент – это клиентское приложение для взаимодействия с сервером РЕД АДМ.

РЕД АДМ Клиент необходим для применения распространяемых конфигураций на рабочей станции в автоматическом режиме (режим «pull»), а также для сбора статистики и лога с клиентских рабочих станций.

Дистрибутив **РЕД АДМ Клиент** находится в стандартном репозитории РЕД ОС и представляет из себя rpm-пакет.

Системные требования для РЕД АДМ

Системные требования для РЕД АДМ Сервер
Системные требования для РЕД АДМ Клиент
Требования к веб-управлению

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия РЕД АДМ**: 1.10

Системные требования для РЕД АДМ Сервер

РЕД АДМ Сервер устанавливается на РЕД ОС конфигурации **Сервер** версии **7.3 и выше**. Системные требования для **РЕД ОС Сервер 7.3** см. по ссылке на вкладке «**Системные требования**».

Конфигурация	Минимальные требования
Центральный процессор	4 ядра по 2 ГГц
ОЗУ	4 ГБ
Хранилище	100 ГБ (желательно SSD)

Системные требования для РЕД АДМ Клиент

Минимальные требования к оборудованию совпадают с требованиями к операционной системе, на которую устанавливается **РЕД АДМ Клиент**.

ВАЖНО!

РЕД АДМ Клиент устанавливается и полноценно поддерживается **только на РЕД ОС**.

Требования к веб-управлению

Для доступа к веб-управлению необходимо наличие одного из следующих браузеров:

- **Chromium** версии **90.x** или выше;
- **FireFox** версии **78.x** или выше:
- **Яндекс.Браузер** версии **22.7.5** или выше.

Подготовка окружения

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия РЕД АДМ**: 1.10

Для развертывания системы РЕД АДМ потребуется:

1. *Установленная операционная система* ***РЕД ОС*** *конфигурации* ***Сервер****, необходимая для установки* ***РЕД АДМ Сервер****.*

Системные требования для **РЕД ОС Сервер 7.3** см. по ссылке на вкладке «**Системные требования**».

Системные требования для **РЕД АДМ Сервер** указаны в разделе «Системные требования».

2. *Развернутый контроллер домена.*

Контроллер домена должен быть на базе *подсистемы службы каталогов РЕД АДМ* (**reddc**), *Samba DC* или *Microsoft Active Directory* (**MS AD**).

В целях безопасности рекомендуется создать *две сервисные учетные* записи:

- первая (**redadm**) — для администрирования РЕД АДМ;
- вторая (имя задается вручную) — для подключения к LDAP-каталогу домена.

Пользователю **redadm** необходимо предоставить права на чтение доменного каталога. С помощью этой учетной записи производится подключение к контроллеру домена и назначение роли администратора другим пользователям. После выполнения всех манипуляций необходимо выйти на сервере РЕД АДМ из этой учетной записи, после чего заблокировать этого пользователя в домене.

Вторая учетная запись, имя которой задается вручную, необходима для чтения LDAP-каталога домена и должна быть всегда активна.

> **Примечание.**
>
> Не рекомендуется использовать сервисную учетную запись для работы в РЕД АДМ. Оптимальным вариантом является настройка прав в ролевой системе РЕД АДМ для других учетных записей в домене.

В целях безопасности учетную запись **redadm** необходимо создавать со сложным паролем длиной **более 8 символов**, содержащим строчные (**a-z**) и прописные (**A-Z**) буквы, цифры (**0-9**), а также **хотя бы один специальный символ**, иначе во входе в веб-интерфейс РЕД АДМ будет отказано.

3. *Компьютеры (клиентские машины), на которые будет установлен* ***РЕД АДМ Клиент****.*

Эти машины необходимо ввести в ваш домен (к которому подключается РЕД АДМ).

РЕД АДМ требует прямого доступа по сети между сервером РЕД АДМ и клиентом по TCP-портам **22** и **80** (или **443** в случае использования *SSL*).

Клиентское приложение РЕД АДМ можно либо распространить встроенными средствами РЕД АДМ, либо установить из репозитория или rpm-пакета.

> **Примечание.**
>
> При установке **РЕД АДМ Клиент** из репозитория или rpm-пакета необходимо заполнить конфигурационный файл, подробную информацию см. в статье «Установка РЕД АДМ Клиент».

Установка РЕД АДМ Сервер

Установка РЕД АДМ Сервер
Настройка после установки
Дополнительные настройки при использовании домена MS AD

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия ПО**: redadm-1.10

Установка РЕД АДМ Сервер

Пакеты установки РЕД АДМ поставляются в составе стандартного репозитория.

Для установки **РЕД АДМ Сервер** в терминале перейдите в сеанс пользователя **root**:

```
su -
```

Обновите и перезагрузите систему:

```
dnf update
reboot
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Установка **РЕД АДМ Сервер** из репозитория производится командой:

```
dnf install redadm
```

Для установки **РЕД АДМ Сервер** из RPM-пакета необходимо открыть директорию с RPM-пакетом и выполнить команду:

```
dnf install <имя_пакета>.rpm
```

Настройка после установки

Настройка файла конфигурации сервера

Отредактируйте серверный конфигурационный файл **/etc/redadm/server.conf** командой:

```
nano /etc/redadm/server.conf
```

Основные настройки

Секция [BASE_SETTINGS] отражает основные настройки РЕД АДМ:

- CERT_PATH = *<путь_к_сертификату>* – сертификат используется для подключения по **ldaps** и **https**. По умолчанию указан демо-сертификат;
- SECRET_KEY = *<ключ>* – автогенерируемый параметр, отображается в зашифрованном виде. Представляет собой ключ приложения, который используется для шифрования паролей и создания токенов авторизации;
- DEFAULT_SSH_USER = *<имя_пользователя>* – в случае автоматического добавления клиентского хоста указанный пользователь будет использоваться для обращения к этому клиенту. Для данного пользователя должны быть заранее распространены ssh-ключи.

Секция [LDAP] отражает настройки подключения к вашему домену:

- LDAP_URL = ldaps://*<IP-адрес>:<порт>* – LDAP-адрес контроллера домена (по умолчанию используется *порт 636*);
- LDAP_DOMAIN_NAME = *<имя>* – LDaP-имя контроллера домена;
- LDAP_DC_END = *<имя>* – имя в формате DC;
- USERNAME_LDAP = *<имя_пользователя>* – имя доменного пользователя, с помощью которого РЕД АДМ будет совершать LDAP-запросы на чтение. Используется для работы механизма распространения конфигураций;

- PASSWORD_LDAP = *<пароль_доменного_пользователя>* – пароль доменного пользователя.

Для шифрования пароля доменного пользователя после сохранения конфигурационного файла выполните команду:

```
/opt/redadm/.venv/bin/python /opt/redadm/scripts/encrypt_config.py -a "PASSWORD_LDAP"
```

Дополнительные настройки

Секция [SYSLOG] отражает настройки ведения журналов:

- SYSLOG_ENABLE – включение syslog;
- SYSLOG_DEFAULT – директория для хранения логов;
- SYSLOG_IP – IP-адрес сервера syslog (должен быть настроен syslog backend и закомментирована строка с SYSLOG_DEFAULT);
- SYSLOG_PORT – порт сервера syslog.

Секция [OTHER] содержит дополнительные настройки:

- PULL_NUMBER_TASKS = *<число>* – число запросов на получение конфигураций в режиме «pull», которые **РЕД АДМ Сервер** будет обслуживать одновременно.

ВАЖНО!

Убедитесь, что в системе установлен правильный DNS-сервер, разрешающий A-записи DNS контроллера домена. Проверку разрешения A-записи можно запустить командой:

```
nslookup <имя_контроллера_домена>
```

либо

```
ping <имя_контроллера_домена>
```

При правильной настройке DNS-сервера в ответе команды будет выведена информация с IP-адресом домена, а запросы обработаны.

Установить DNS-сервер можно в настройках сетевого адаптера, проверить – в файле **/etc/resolv.conf**. Подробную информацию по настройке и проверке корректности конфигурации DNS-сервера см. в наших инструкциях «Настройка сетевого адаптера» и «Настройка DNS».

Также следует проверить синхронизацию времени с контроллером домена, это необходимо для обеспечения шифрованного подключения к LDAP-каталогу домена. Подробнее см. инструкцию «Настройка синхронизации времени».

Примечание.

Сценарий установки **РЕД АДМ Сервера** настроит параметры *Ansible* в файле конфигурации **/etc/ansible/ansible.cfg**.

Параметр **forks** отвечает за максимальное количество потоков, которые *Ansible* будет использовать для выполнения задач на целевых хостах. Это количество используется при распространении клиентского агента и VNC, а также в ручном режиме применения конфигураций.

Параметр **timeout** отвечает за время ожидания по умолчанию для подключающихся клиентов. Возникает в случаях недоступности клиентского хоста.

Для установки или обновления *Ansible* до версии **6.X** воспользуйтесь инструкцией «Ansible - система автоматизации настройки и развертывания ПО».

Настройка файла конфигурации клиента

Отредактируйте конфигурационный файл клиента **/etc/redadm/client.conf**.

ВАЖНО!

Синтаксис файла конфигурации **чувствителен** к регистру!

```
nano /etc/redadm/client.conf
```

```
[SETTINGS]
 # IP-адрес вашего сервера РЕД АДМ, к которому будут подключаться клиенты
 IP=10.1.1.2
 # порт, к которому будут подключаться клиенты РЕД АДМ
 # по умолчанию используется порт 80
 PORT=80
 # использование https для обращения клиентов к серверу
 # по умолчанию используется значение False
 ENABLED_SECURE=False
 # путь к сертификату сервера РЕД АДМ на клиентской машине
 SECURE_CERTIFICATE=<путь_к_сертификату>
```

Запуск служб

После редактирования файлов конфигурации сервера и клиента для применения внесенных изменений необходимо запустить и добавить в автозагрузку следующие службы:

```
systemctl enable --now redadm.service redis.service redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

Настройка HTTPS

Для настройки подключения с использованием **HTTPS** необходимо выполнить некоторые дополнительные настройки.

Самоподписанные сертификаты

Если центр сертификации отсутствует, можно использовать демо-сертификаты.

Для этого необходимо перейти в каталог с сертификатами:

```
cd /opt/redadm/configs/ssl
```

Здесь для дальнейшей работы потребуется непосредственно сам сертификат (**redadm-server.crt**) и ключ сервера (**redadm-server.key**), а также сертификат центра сертификации **DemoCA.pem**, который необходимо установить в качестве доверенного для браузера, где используется веб-интерфейс РЕД АДМ.

Если потребуется сгенерировать новые демо-сертификаты, необходимо запустить скрипт генерации из каталога **/opt/redadm/configs/ssl** командой:

```
./generate\_DemoCA.sh
```

После выполнения скрипта в выводе будут отображены полные пути сертификата и ключа, которые нужно прописать в конфигурационные файлы. Пример их заполнения приведен ниже.

> **Примечание.**
>
> При каждой новой генерации сертификата все имеющиеся в каталоге файлы будут зарезервированы в каталог с текущей датой.

Сторонний центр сертификации

Сгенерируйте сертификат для сервера РЕД АДМ в вашем центре сертификации. Требования к сертификату:

- значение параметра `cn` должно совпадать с доменным именем сервера РЕД АДМ;

- должны присутствовать поля alt_names, где прописаны все IP-адреса и DNS-имена, на которых будет доступен РЕД АДМ.

Пример конфигурационного файла параметров генерации для **openssl** можно просмотреть в файле **/opt/redadm/configs/ssl/ssl-conf.ext**.

Разместите сгенерированные сертификаты в каталог **/opt/redadm/configs/ssl**.

Настройка конфигурационных файлов

Настройте **nginx** в файле **/etc/nginx/nginx.conf**. Для этого закомментируйте секцию [HTTP]:

```
#[HTTP server]
 #
 # server {
 # listen 80;
 # ...
 #}
```

Затем раскомментируйте секцию [HTTPS]:

```
[HTTPS server]
 server {
 listen 443 ssl;
 server_name localhost;
 ssl_certificate /opt/redadm/configs/ssl/redadm-server.crt;
 ssl_certificate_key /opt/redadm/configs/ssl/redadm-server.key;
 ...
 }
```

В файле конфигурации сервера **/etc/redadm/server.conf** укажите путь к сгенерированному сертификату в поле CERT_PATH.

В файле конфигурации клиента **/etc/redadm/client.conf** отредактируйте следующие параметры:

- PORT = 443;
- ENABLE_SECURE = True;
- SECURE_CERTIFICATE = *<путь_к_сертификату_на_клиентской_машине>*.

Перезапустите службы **redadm** и **nginx**:

```
systemctl restart redadm.service nginx.service
```

Дополнительные настройки при использовании домена MS AD

В данном подразделе описано создание сертификатов для обеспечения безопасных подключений по **SSL** между **сервером РЕД АДМ** и контроллером домена **Microsoft Active Directory**. Здесь рассмотрены два случая:

- в домене уже имеется центр сертификации: например, эту роль выполняет контроллер домена Active Directory;
- сертификат создаётся самостоятельно.

Использование существующего центра сертификации

Если вы подключаете РЕД АДМ к Microsoft Active Directory, и в домене уже поднята роль «**Центр сертификации**», убедитесь, что параметр CNGHashAlgorithm имеет значение SHA256, иначе в браузере потребуется подтвердить ненадежное SSL-соединение.

Для проверки параметра CNGHashAlgorithm требуется в командной строке Windows (где располагается *Центр сертификации*) выполнить:

```
certutil -getreg ca\csp\CNGHashAlgorithm
```

Опционально: для установки SHA256 и пересоздания (!) нового корневого сертификата в командной строке требуется выполнить:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
net stop CertSvc
net start CertSvc
certutil -renewCert ReuseKeys
net stop CertSvc
net start CertSvc
```

Далее для выпуска SSL-сертификатов требуется:

1. На Windows (где располагается *Центр сертификации*) запустите оснастку **Сертификаты**.

В командной строке или в окне «**Выполнить**» введите команду:

```
certmgr.msc
```

2. Правой клавишей мыши щелкните по пункту «**Личное**», и далее перейдите по элементам «**Все задачи**» — «**Дополнительные операции**» — «**Создать настраиваемый запрос...**».

3. Выберите значения параметров:

- *Настраиваемый запрос*: Продолжить без политики регистрации;
- *Шаблон*: Ключ CNG (без шаблона);
- *Формат запроса*: PKCS #10;

4. Раскройте выпадающее меню «**Подробности**» и выберите «**Свойства**». Рассмотрим заполнение свойств на примере домена **wind.lan**.

> **Примечание.**
>
> Сервер РЕД АДМ может и не быть членом домена. Но обязательно должна быть создана A-запись в службе DNS с указанием IP-адреса сервера РЕД АДМ и именем, используемым в сертификате.

Общие

- *Имя*: redadm.wind.lan;
- *Описание*: SSL Certificate.

Субъект

- *Имя субъекта (Тип: Общее имя)*: redadm.wind.lan;
- *Дополнительное имя (Тип: Служба DNS)*: redadm.wind.lan;
- *Дополнительное имя (Тип: IP-адрес (v4))*: впишите IP-адрес сервера РЕД АДМ.

Закрытый ключ

- *Поставщик службы шифрования*: RSA, Microsoft Software Key Storage Provider;
- *Параметры ключа*:
  - *Размер*: 2048;
  - Сделать закрытый ключ экспортируемым.
- *Выберите хэш-алгоритм*: По умолчанию.

5. Сохраните файл запроса в формате **Base64**. Например: **C:\requests\redadm.wind.lan.req**.

6. Выпустите сертификат командой:

```
certreq -submit -attrib "CertificateTemplate:webserver" C:\requests\redadm.wind.lan.req C:\requests\redadm.wind.lan.cer
```

7. Добавьте выпущенный сертификат **redadm.wind.lan.cer** в «**Личное**».

Дважды щелкните по файлу сертификата, перейдите во вкладку «**Состав**» и нажмите «**Копировать в файл...**».

В открывшемся окне нажмите «**Далее**», выберите «**Да, экспортировать закрытый ключ**» и установите пароль.

Укажите путь и сохраните сертификат с расширением **pfx**. Например, **redadm.wind.lan.pfx**.

8. Экспортируйте корневой сертификат сервера, он понадобится для организации защищенного соединения между РЕД АДМ и компьютерами.

Перейдите на вкладку «**Доверенные корневые центры сертификации**» и нажмите на элемент «**Сертификаты**».

Дважды щелкните по корневому сертификату, перейдите во вкладку «**Состав**» и нажмите «**Копировать в файл...**».

> **Примечание.**
>
> У контроллера домена с именем **windc1.wind.lan** сертификат имеет вид **wind-WINDC1-CA**).

В открывшемся окне нажмите «**Далее**», выберите формат: **Файлы X.509 (.CER) в кодировке DER**.

Укажите путь и сохраните корневой сертификат с расширением **cer**. Например, **ca.cer**.

9. Загрузите файл полученного сертификата **pfx** и корневого сертификата **cer** на сервер с установленным РЕД АДМ и выполните следующие команды для извлечения сертификата и ключа. Потребуется вводить пароль, установленный на предыдущем шаге.

Извлеките сертификат:

```
openssl pkcs12 -in redadm.wind.lan.pfx -clcerts -nokeys -out redcert.crt
```

Извлеките ключ:

```
openssl pkcs12 -in redadm.wind.lan.pfx -nocerts -out temp.key
```

Удалите пароль с ключа:

```
openssl rsa -in temp.key -out redserver.key
```

Преобразуйте корневой сертификат в формат **crt**:

```
openssl x509 -inform DER -in ca.cer -out ca.crt
```

Скопируйте полученный сертификат в **/opt/redadm/configs/ssl/**:

```
cp redcert.crt /opt/redadm/configs/ssl/
cp redserver.key /opt/redadm/configs/ssl/
```

Установите владельца и права доступа:

```
chown redadm_local_service_user:redadm_local_service_user /opt/redadm/configs/ssl/redcert.crt
chown redadm_local_service_user:redadm_local_service_user /opt/redadm/configs/ssl/redserver.key
chmod 644 /opt/redadm/configs/ssl/redcert.crt
chmod 600 /opt/redadm/configs/ssl/redserver.key
```

Скопируйте преобразованный корневой сертификат **ca.crt** на клиентский компьютер в **/opt/redclient/**.

10. Откройте файл **/etc/nginx/nginx.conf** на сервере РЕД АДМ и закомментируйте секцию `[HTTP server]`:

```
# [HTTP server]
# server
# listen 80;
# ...
#
```

11. Раскомментируйте секцию `[HTTPS server]`:

```
# [HTTPS server]
server {
  listen 443 ssl;
  server_name redadm.wind.lan;
  ssl_certificate /opt/redadm/configs/ssl/redcert.crt;
  ssl_certificate_key /opt/redadm/configs/ssl/redserver.key;
  ...
}
```

12. В файле конфигурации сервера **/etc/redadm/server.conf** укажите путь к сгенерированному сертификату в поле `CERT_PATH`:

```
CERT_PATH=/opt/redadm/configs/ssl/redcert.crt
```

13. В файле конфигурации клиента **/etc/redadm/client.conf** отредактируйте следующие параметры:

```
PORT = 443
ENABLED_SECURE = True
SECURE_CERTIFICATE = /opt/redclient/ca.crt
```

14. Перезапустите службы **redadm** и **nginx**:

```
systemctl restart redadm.service nginx.service
```

15. Проверьте статус служб:

```
systemctl status redadm.service nginx.service
```

Самостоятельное создание сертификатов

Если у вас нет собственного центра сертификации, вы можете создать сертификат без ЦС и подписать его в РЕД АДМ. Для этого выполните следующие шаги:

1. Создайте в любом текстовом редакторе файл **request.inf** со следующим содержимым:

```
[Version]
 Signature="$Windows NT$
 [NewRequest]
 Subject = "CN=<DC_fqdn>"; укажите полное имя вашего домена
 KeySpec = 1
 KeyLength = 1024
 ; Can be 1024, 2048, 4096, 8192, or 16384.
 ; Larger key sizes are more secure, but have
 ; a greater impact on performance.
 Exportable = TRUE
 MachineKeySet = TRUE
 SMIME = False
 PrivateKeyArchive = FALSE
 UserProtected = FALSE
 UseExistingKeySet = FALSE
 ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
 ProviderType = 12
 RequestType = PKCS10
 KeyUsage = 0xa0
 [EnhancedKeyUsageExtension]
 OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
```

2. Сгенерируйте запрос на подпись через консоль **PowerShell**:

```
certreq -new request.inf request.csr
```

Поместите полученный сертификат на сервер РЕД АДМ в каталог **/opt/redadm/configs/ssl**.

3. Подпишите сертификат с помощью корневого сертификата РЕД АДМ (**DemoCA.pem**):

```
openssl x509 -req -in request.csr -CA DemoCA.pem -CAkey DemoCA.key -CAcreateserial -out request.crt -days 365 -sha256
```

4. Подписанный сертификат **request.crt** и корневой сертификат **DemoCA.pem** необходимо передать на контроллер домена Active Directory.

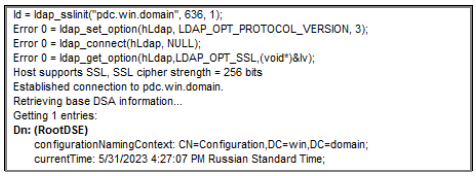
В оснастке «**Сертификаты**» на контроллере домена в разделе «**Доверенные корневые центры сертификации**» импортируйте сертификат **DemoCA.pem**.

Далее необходимо принять сертификат **request.crt**:

```
certreq -accept request.crt
```

Проверить работу **LDAPS** можно утилитой **ldp.exe**.

5. В меню «**Connections**» выберите «**Connect**», укажите *имя* вашего домена, *порт* 636 и наличие *SSL*. Вывод должен выглядеть примерно следующим образом:



6. Перезапустите сервер РЕД АДМ:

```
systemctl restart redadm.service
```

Подробную информацию о генерации сертификатов можно посмотреть в официальной документации Microsoft.

Установка РЕД АДМ Клиент

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия По**: redadm-client-1.10

Примечание.

Установка **РЕД АДМ Клиент** (клиентского приложения) возможна двумя способами:

- из веб-интерфейса РЕД АДМ;
- с помощью rpm-пакета.

Подробную информацию об установке **РЕД АДМ Клиент** из веб-интерфейса см. в *Руководстве администратора*.

Примечание.

При распространении клиентского приложения РЕД АДМ через веб-интерфейс дополнительных настроек в файле **/opt/redclient/client.conf** производить не требуется, т.к. в данном случае все настройки определяются сервером.

Для ручной установки **РЕД АДМ Клиент** в терминале перейдите в сеанс пользователя **root**:

```
su -
```

Установка **РЕД АДМ Клиент** из репозитория производится командой:

```
dnf install redadm-client
```

Для установки **РЕД АДМ Клиент** из RPM-пакета необходимо открыть директорию с RPM-пакетом и выполнить команду:

```
dnf install <имя_пакета>.rpm
```

Для настройки **РЕД АДМ Клиент** отредактируйте конфигурационный файл **/opt/redclient/client.conf**:

```
nano /opt/redclient/client.conf
```

```
[SETTINGS]
# IP-адрес вашего сервера РЕД АДМ, к которому будут подключаться клиенты
IP=10.1.1.2
# порт, к которому будут подключаться клиенты РЕД АДМ
# по умолчанию используется порт 80
PORT=80
# использование https для обращения клиентов к серверу
# по умолчанию используется значение False
ENABLED_SECURE=False
# путь к сертификату сервера РЕД АДМ на клиентской машине
SECURE_CERTIFICATE=<путь_к_сертификату>
```

Запустите клиентскую службу и добавьте ее в автозагрузку:

```
systemctl enable redclient-daemon.service --now
```

Получение конфигураций с сервера РЕД АДМ происходит при выполнении команды **gpupdate** на клиенте. Данная команда автоматически прописывается при установке пакета в сценарий запуска сессии пользователей. В случае с GDM — это **/etc/gdm/PreSession/Default**.

Если вы хотите получать конфигурации по расписанию, пропишите команду **gpupdate &** в crontab-файл.

Например, для получения конфигураций в 10 и 40 минут каждого часа, впишите следующую строку:

```
10,40 * * * * root /bin/gpupdate &
```

Обновление РЕД АДМ Сервер версии 1.9.1

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия ПО**: redadm-1.10

Для обновления **РЕД АДМ Сервер** версии 1.9.1 перейдите в сеанс пользователя **root**:

```
su -
```

Остановите активные службы:

```
systemctl stop redadm.service redadm-celery-worker.service redadm-celery-beat.service
```

Выполните команду обновления:

```
dnf update redadm
```

Отредактируйте файлы конфигурации сервера и клиента в соответствии с рекомендациями, описанными в пункте «Настройка после установки» в инструкции «Установка РЕД АДМ Сервер».

Запустите остановленные службы:

```
systemctl start redadm.service redadm-celery-worker.service redadm-celery-beat.service
```

Запустите и добавьте в автозагрузку службу веб-сервера:

```
systemctl enable --now nginx.service
```

ВАЖНО!

После обновления РЕД АДМ Сервер необходимо также обновить версии клиентских приложений на всех подключенных клиентах путем их повторного распространения.

Также клиентские приложения необходимо заново распространять после каждого изменения конфигурационного файла клиента **/etc/redadm/client.conf**.

Решение проблем после обновления

Если после обновления наблюдаются проблемы с наполнением журнала или неточности в настроенных конфигурациях, выполните нижеприведенные действия и сохраните их вывод для анализа проблемы.

Обновите базу данных командами:

```
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py makemigrations
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py migrate
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py create_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py update_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py update
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py update_1_9_2
```

Шаблонные файлы конфигурации можно найти в каталоге **/opt/redadm/configs**.

Для редактирования прав на файлы РЕД АДМ измените владельца следующих директорий:

```
chown -R redadm_local_service_user. /opt/redadm
chown -R redadm_local_service_user. /var/log/redadm
chown -R redadm_local_service_user. /etc/redadm
```

Обновление РЕД АДМ Сервер версии 1.10

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия ПО**: redadm-1.10

Для обновления **РЕД АДМ Сервер** версии 1.10 перейдите в сеанс пользователя **root**:

```
su -
```

Остановите активные службы:

```
systemctl stop redadm.service redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

Выполните команду обновления:

```
dnf update redadm
```

Запустите остановленные службы:

```
systemctl start redadm.service redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

ВАЖНО!

После обновления РЕД АДМ Сервер необходимо также обновить версии клиентских приложений на всех подключенных клиентах путем их повторного распространения.

Также клиентские приложения необходимо заново распространять после каждого изменения конфигурационного файла клиента **/etc/redadm/client.conf**.

Решение проблем после обновления

Если после обновления наблюдаются проблемы с наполнением журнала или неточности в настроенных конфигурациях, выполните нижеприведенные действия и сохраните их вывод для анализа проблемы.

Обновите базу данных командами:

```
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py makemigrations
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py migrate
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py create_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py update_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py update
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3 /opt/redadm/manage.py update_1_9_2
```

Шаблонные файлы конфигурации можно найти в каталоге **/opt/redadm/configs**.

Для редактирования прав на файлы РЕД АДМ измените владельца следующих директорий:

```
chown -R redadm_local_service_user. /opt/redadm
chown -R redadm_local_service_user. /var/log/redadm
chown -R redadm_local_service_user. /etc/redadm
```

Обновление РЕД АДМ Клиент

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия ПО**: redadm-client-1.10

Обновить РЕД АДМ Клиент можно из веб-интерфейса, заново распространив клиентское приложение с обновленной версии сервера.

> **Примечание.**
>
> После обновления РЕД АДМ Клиента до версии **1.9.1 и выше** таблица подключенных узлов будет пуста.
>
> Таблица будет заполнена значениями после распространения новой версии клиентского приложения либо при обращении клиента к серверу (при выполнении команды gpupdate).

Для обновления **РЕД АДМ Клиент** вручную перейдите в сеанс пользователя **root**:

```
su -
```

Остановите клиентскую службу:

```
systemctl stop redclient-daemon.service
```

Обновите пакет **РЕД АДМ Клиент**:

```
dnf update redadm-client
```

Проверьте параметры в файле **/opt/redclient/client.conf**.

```
[SETTINGS]
 # IP-адрес вашего сервера РЕД АДМ, к которому будут подключаться клиенты
 IP=10.1.1.2
 # порт, к которому будут подключаться клиенты РЕД АДМ
 # по умолчанию используется порт 80
 PORT=80
 # использование https для обращения клиентов к серверу
 # по умолчанию используется значение False
 ENABLED_SECURE=False
 # путь к сертификату сервера РЕД АДМ на клиентской машине
 SECURE_CERTIFICATE=<путь_к_сертификату>
```

Запустите клиентскую службу:

```
systemctl start redclient-daemon.service
```

Диагностика проблем

Окружение

- **Версия РЕД ОС**: 7.3
- **Версия РЕД АДМ**: 1.10

При сбоях в функционировании приложения РЕД АДМ в первую очередь стоит проверить статус сервиса **redadm**. Для этого выполните команду:

```
systemctl status redadm.service
```

В статусе должно отображаться **active (running)**.

Также можно просмотреть файл логов на предмет ошибок, выполнив команду:

```
cat /var/log/redadm/redadm.log
```

В случае возникновения проблем с распространением SSH-ключа просмотрите соответствующие логи, выполнив команды:

```
cat /var/log/redadm/ssh1.log
cat /var/log/redadm/ssh_key.log
```

В случае возникновения проблем с распространением конфигураций необходимо проверить статус служб, выполнив команды:

```
systemctl status redis.service
systemctl status redadm-celery-worker.service
```

В статусе должно отображаться **active (running)**.

В случае остановки служб необходимо перезапустить их, выполнив команды:

```
systemctl restart redis.service
systemctl restart redadm-celery-worker.service
```

Далее необходимо проверить корректность заполнения файла конфигурации клиентского приложения **/opt/redclient/client.conf**:

```
cat /opt/redclient/client.conf
```

В нем должны быть указаны *IP-адрес* и *порт* РЕД АДМ Сервер — параметры `IP` и `port` соответственно.

Часто задаваемые вопросы (FAQ)

Не удаётся получить доступ к web-интерфейсу РЕД АДМ

Проверьте статус сервиса **redadm** на сервере РЕД АДМ, скорее всего он не запущен. Запустите его следующей командой:

```
systemctl status redadm
systemctl enable redadm --now
```

Не запускаются сервисы redadm-celery-worker и redadm-celery-beat

1) Остановите сервисы:

```
systemctl stop redadm-celery-worker.service redadm-celery-beat.service
```

2) Выполните перезагрузку машины:

```
reboot
```

3) Выполните откат версии пакета **python3-click** до **7.1.2**:

```
dnf downgrade python3-click
```

4) Выполните запуск сервисов:

```
systemctl start redadm-celery-worker.service redadm-celery-beat.service
```

Какие принтеры можно подключить через конфигурацию РЕД АДМ?

Подключить через конфигурацию «**Установить принтер**» можно принтеры доступные по протоколу **ipp**.

Почему на вкладке «Конфигурации» видны не все подразделения?

Создание конфигураций допускается только в подразделениях, имеющих тип **Organization Unit - OU**.

Почему на вкладке «Настройки» - «Подключение узлов» не отображаются клиентские машины в домене?

Для того чтобы хост появился в списке и отображался его статус, клиентская машина должна находиться в домене и быть добавлена через соответствующее меню, вызываемое на кнопку «**Добавить**».

Не получается распространить конфигурацию «Подключение локального репозитория»

Возможно на клиентской машине не установлен пакет **redos-kernels-release**. Адрес локального репозитория вносится в уже существующий файл репозитория. Создайте конфигурацию для установки пакета **redos-kernels-release**.

Работает ли РЕД АДМ с доменом FreeIPA?

На данный момент РЕД АДМ работает только с доменами **Samba DC** и **Microsoft AD**. Добавление функционала взаимодействия с **FreeIPA** планируется в будущих обновлениях.

Машина с сервером РЕД АДМ должна быть введена в домен?

Нет, для работы РЕД АДМ и его взаимодействия с контроллером домена достаточно, чтобы в настройках сети был прописан **DNS-сервер**, разрешающий А-записи контроллера домена, и указан «**Поисковой домен**».

Влияет ли расположение конфигурации в дереве на что-то кроме того, что будет располагаться в области применения после ее создания?

Расположение конфигурации в древе влияет только на то, какое подразделение будет указано во вкладке «**Область применения**» по умолчанию.

Что необходимо прописывать в настройке конфигурации «Подключение локального репозитория»? (формат записи)

В полях конфигурации «**Подключение локального репозитория**» указываются URL-ссылки на ваши локальные репозитории.

В какой момент запускается выполнение конфигурации на клиентской машине?

Клиент запрашивает доступные конфигурации после выполнения команды **gpupdate**.

Команду **gpupdate** можно выполнить несколькими способами:

1. Вручную в терминале.

2. Добавив в автозапуск по расписанию, например, через **crontab**.

3. При входе в сессию под доменным пользователем - команда **gpupdate** добавляется в скрипт входа **gdm** после установки клиентской части.

Пользователю домена назначена роль, имеющая доступ к управлению учетными записями домена, но при создании подразделения/пользователя/компьютера появляется ошибка. Почему?

Роли в РЕД АДМ влияют только на доступность тех или иных модулей в веб-интерфейсе. Права на изменение объектов домена задаются на контроллере домена или добавлением пользователя в группу администраторов домена.

Не появляются записи на вкладке «Журналы» - «Задачи».

Записи в данном разделе появляются только после выполнения конфигураций на клиентских машинах. В них содержится результат их выполнения.

В конфигурации «Подключение сетевого каталога» необходимо задавать полный путь к каталогу?

Для конфигурации «**Подключение сетевого каталога**» в поле «**Сервер**» укажите доменное имя сервера с опубликованным сетевым каталогом, а в поле «**Сетевой каталог**» — имя директории на удалённом сервере.

Где создаётся каталог после выполнения конфигурации «Параметры пользователя» - «Системные настройки» - «Создание каталога»?

Каталог создаётся в домашнем каталоге пользователя с правами доступа для всех.

Описание продукта

СУБД Ред База Данных (далее СУБД или Ред База Данных) используется для упорядоченного хранения и обработки больших объемов информации. Ред База Данных представляет собой мощную современную СУБД с открытым кодом. Ядро Ред Базы Данных построено на основе одной из самых известных и распространенных в мире СУБД с открытым кодом – **Firebird**, которая используется в решениях различного масштаба: от встроенных аппаратных систем и решений для небольших компаний до IT-систем крупнейших транснациональных корпораций с размерами баз данных до десятков терабайт и десятками миллионов транзакций в день.

Назначение

СУБД Ред База Данных предоставляет пользователям следующие возможности:

- поддержка всех основных платформ и операционных систем (среди них: Windows, семейство Linux, BSD Unix, IBM AIX, HP-UX, Sun Solaris и др.);
- поддержка 64-битных систем;
- поддержка многопроцессорных и многоядерных аппаратных платформ;
- высокое быстродействие;
- возможность хранения базы данных в одном отдельном файле;
- возможность аутентификации и авторизации пользователей с использованием в качестве источников сведений об учетных записях пользователей защищенной БД пользователей или системного каталога;
- возможность «горячего» резервного копирования БД и инкрементного резервного копирования, в т.ч. с применением аппаратных решений для резервного копирования;
- наличие модулей сопряжения практически для всех используемых сред разработки, результатов тестов этих модулей и гарантия стабильной работы;
- возможность работы во «встроенном» ПО (**embedded**) в локальном режиме в виде библиотеки **DLL** без отдельной установки и настройки СУБД Ред База Данных, в том числе поддержка встраивания в виртуальную машину Java;
- возможность одновременной модификации базы данных несколькими пользователями;
- обратная совместимость с базами данных от предыдущих версий **Firebird**;
- многоверсионная архитектура;
- модульная архитектура;
- соответствие большинству требований стандарта ISO/ANSI SQL;
- низкие требования к аппаратному обеспечению для небольших баз данных;
- большие возможности по расширению функционала самой СУБД посредством модулей;
- ядро, изначально основанное на многоверсионной архитектуре (**MGA**);
- полное соответствие принципам атомарности, непротиворечивости, изоляции, долговечности (**ACID**).

Вы можете подробнее ознакомиться с установкой **СУБД РЕД База Данных**, а также пройти обучающий курс по работе с **СУБД РЕД База Данных**, просмотрев наши обучающие видео:

- на **RuTube**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».
- в **Яндекс.Дзен**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».

На наших каналах вы также сможете найти много другой полезной информации.

Документация

Наиболее полную, актуальную и регулярно дорабатывающуюся документацию можно найти на сайте **СУБД РЕД База Данных** в разделе «Документация».

Системные требования

Аппаратная часть
Программная часть

Аппаратная часть

Для установки и нормальной работы СУБД Ред База Данных персональный компьютер должен быть оснащен комплектующими со следующими характеристиками:

- Процессор **Intel Pentum D** и выше, процессор **AMD** с поддержкой **x86_64** или процессор **Intel** с поддержкой набора инструкций **EM64T** для архитектуры **x86_64**.
- Оперативная память от **2048Mb**.
- Запоминающее устройство объемом **не менее 16 Гб**.
- Клавиатура 101/102-х клавишная русская/латинская.
- Сетевая карта с поддержкой **Ethernet**.

Рекомендованные системные требования подбираются индивидуально в зависимости от размера базы данных, количества пользователей и характера нагрузки.

Программная часть

Для установки и эксплуатации СУБД в ОС семейства *Windows* не требуется установка дополнительного программного обеспечения.

Для установки и эксплуатации СУБД в ОС семейства Linux необходимы библиотеки: **glibc 2.4 и выше**, **libstdc++ от gcc 3.4.3 и выше**.

Установка РЕД База Данных (Открытая редакция)

Установка для Linux на примере РЕД ОС 7.3
Загрузка установочного файла на РЕД ОС 7.3
Последовательность установки СУБД на РЕД ОС 7.3
Установка для ОС Windows
Загрузка установочного файла на ОС Windows
Последовательность установки СУБД на ОС Windows

Вы можете подробнее ознакомиться с установкой **СУБД РЕД База Данных**, а также пройти обучающий курс по работе с **СУБД РЕД База Данных**, просмотрев наши обучающие видео:

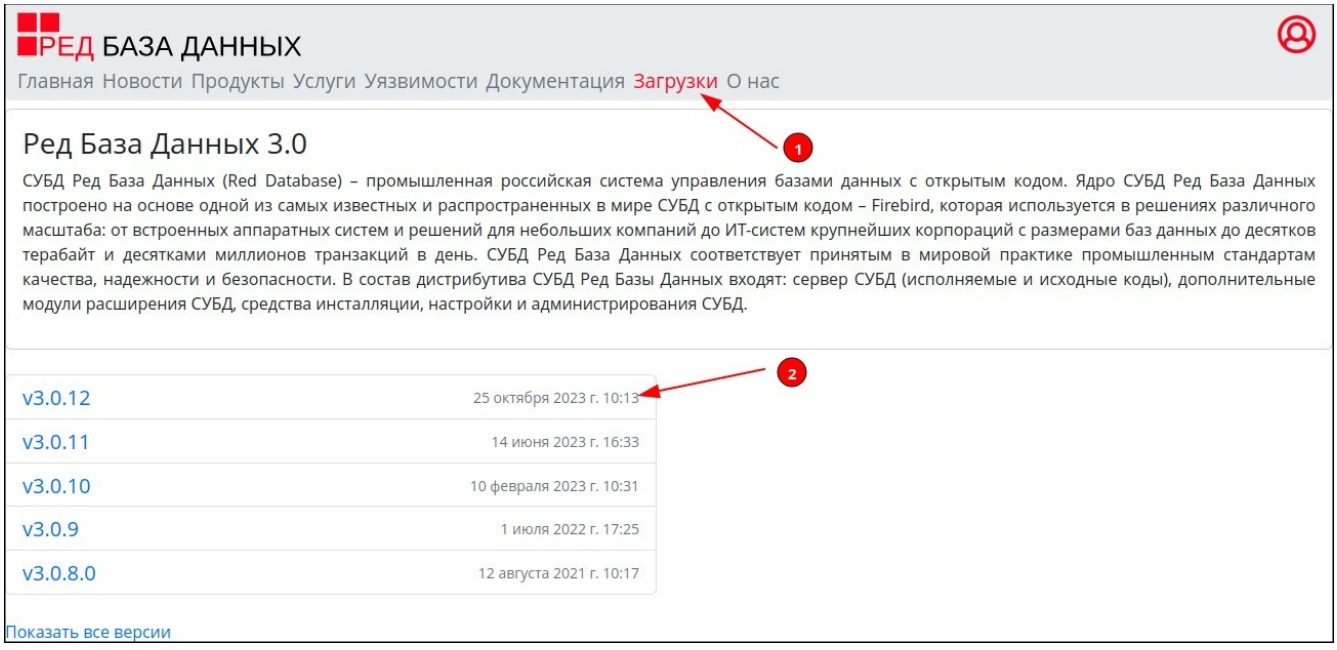
- на **RuTube**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».
- в **Яндекс.Дзен**:
  - Установка СУБД Ред База Данных на РЕД ОС;
  - Курс «Администрирование СУБД Ред База Данных 3.0».

На наших каналах вы также сможете найти много другой полезной информации.

Установка для Linux на примере РЕД ОС 7.3

Загрузка установочного файла на РЕД ОС 7.3

Скачать РЕД Базу Данных можно на официальном сайте компании в разделе «**Загрузки**».



Для скачивания необходимо авторизоваться или зарегистрироваться.

Для установки в РЕД ОС необходимо скачать бинарный файл нужной разрядности и назначить на него права:

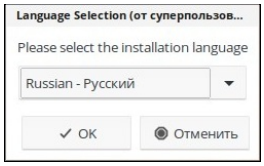
```
sudo chmod +x <путь_до_файла>
```

Для старта установки запустите установочный бинарный файл:

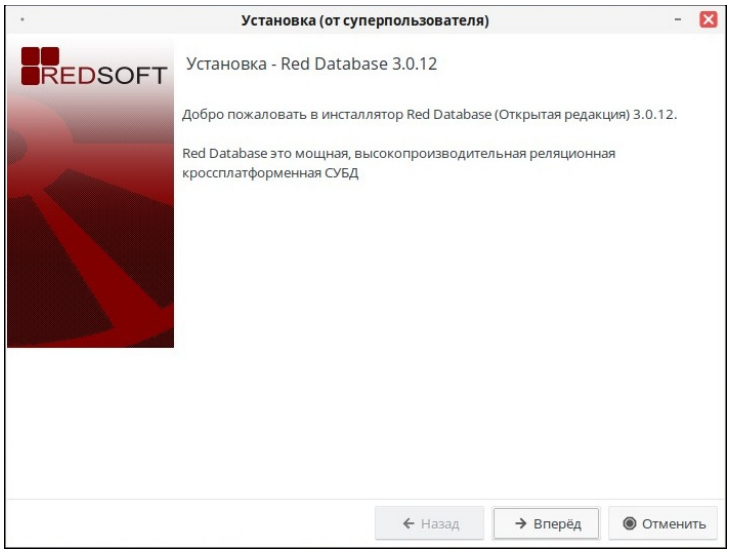
```
sudo ./rdb30-linux-x86_64-open-3.0.12.bin
```

Последовательность установки СУБД на РЕД ОС 7.3

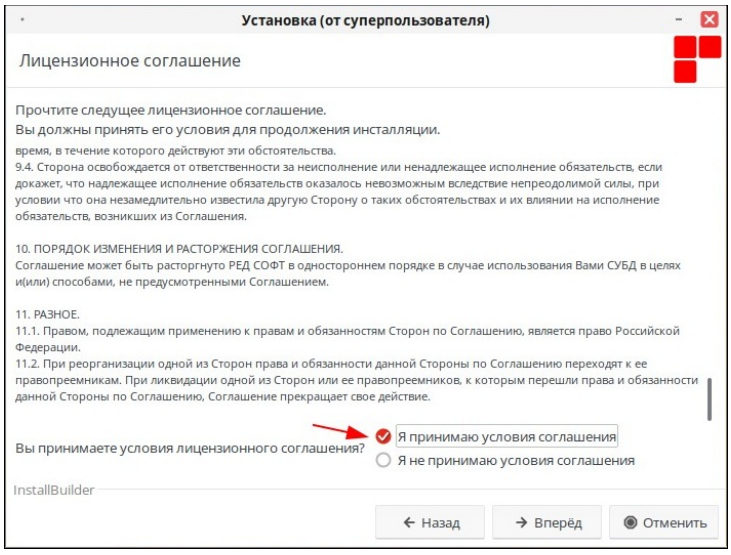
После запуска бинарного файла будет открыто окно настройки языка установщика. Выберите из списка необходимый язык и нажмите «**ОК**».



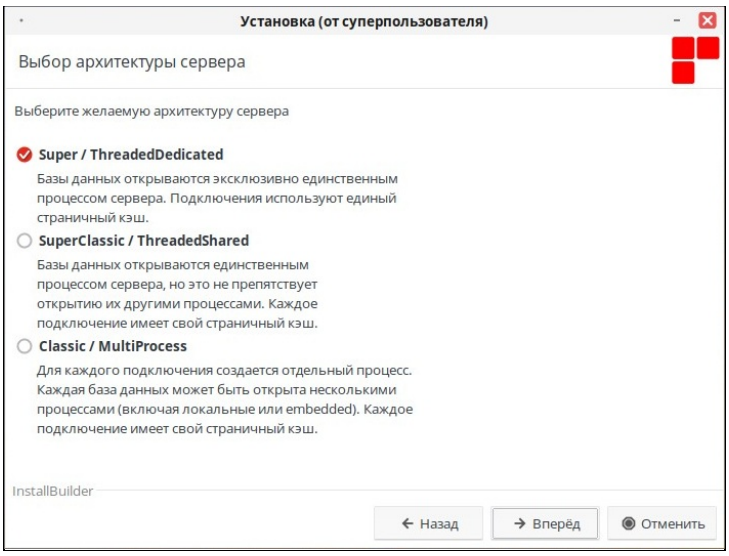
Будет открыто приветственное окно установщика. Нажмите «**Вперед**».



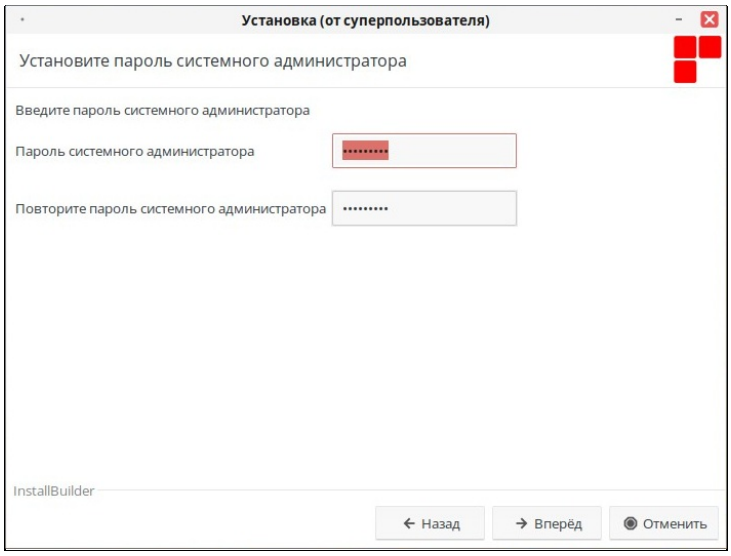
Далее прочтите и примите условия лицензионного соглашения, установив флаг для параметра «**Я принимаю условия соглашения**». Нажмите «**Вперед**».



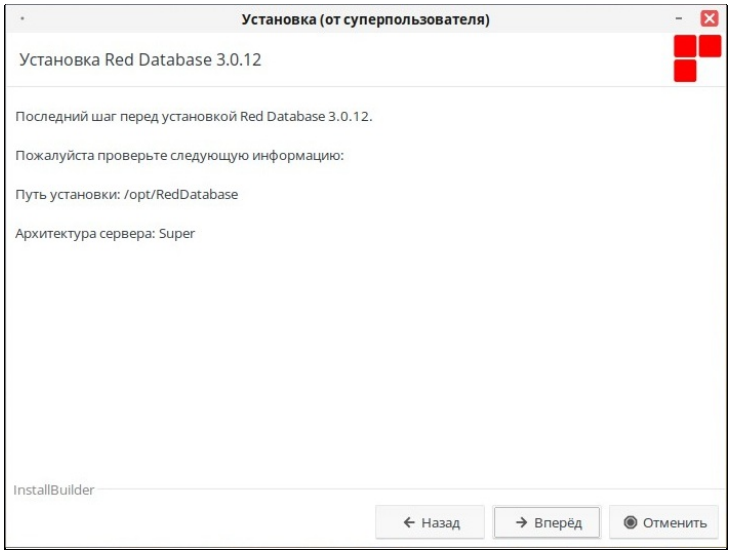
Выберите требуемую архитектуру сервера, установив флаг для соответствующего параметра. Нажмите «**Вперед**».



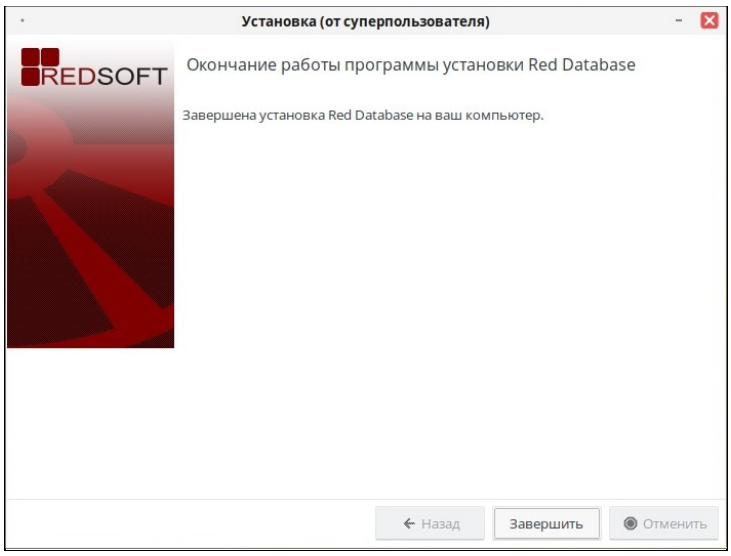
Установите пароль системного администратора. Пароль необходимо повторить для избежания опечаток. Нажмите «**Вперед**».



Проверьте указанные ранее параметры. Если все настроено верно, нажмите «**Вперед**» для запуска процесса установки. В противном случае нажмите «**Назад**» и внесите изменения в необходимые конфигурации.



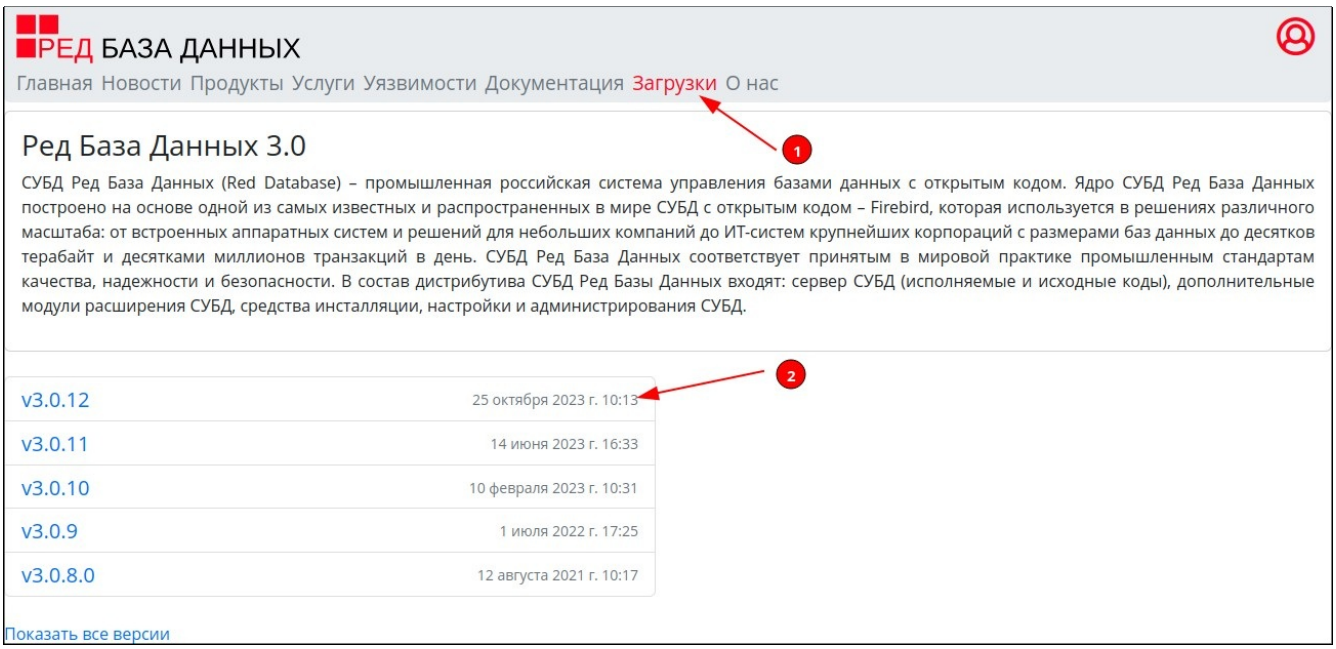
После завершения процесса установки будет выведено соответствующее сообщение. Нажмите «**Завершить**».



Установка для ОС Windows

Загрузка установочного файла на ОС Windows

Скачать РЕД Базу Данных можно на официальном сайте компании в разделе «**Загрузки**».

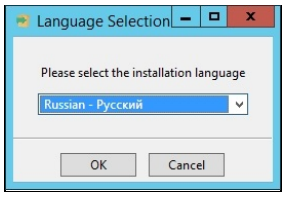


Для скачивания необходимо авторизоваться или зарегистрироваться.

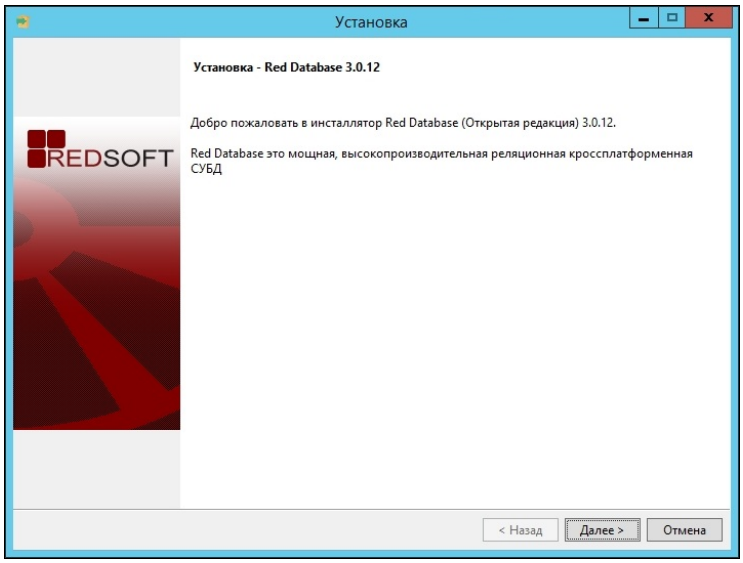
Для установки на Windows скачайте файл с расширением **.exe** нужной архитектуры. Далее от имени администратора запустите установщик.

Последовательность установки СУБД на ОС Windows

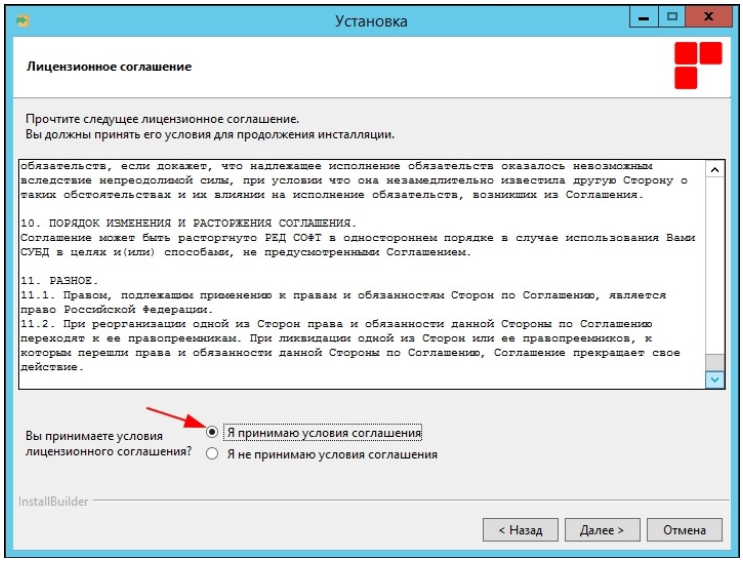
После запуска **exe**-файла будет открыто окно настройки языка установщика. Выберите из списка необходимый язык и нажмите «**OK**».



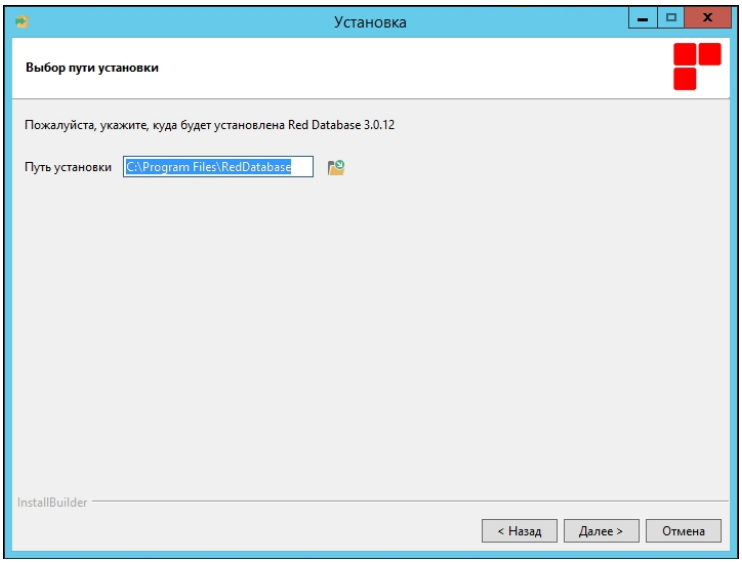
Будет открыто приветственное окно установщика. Нажмите «**Далее**».



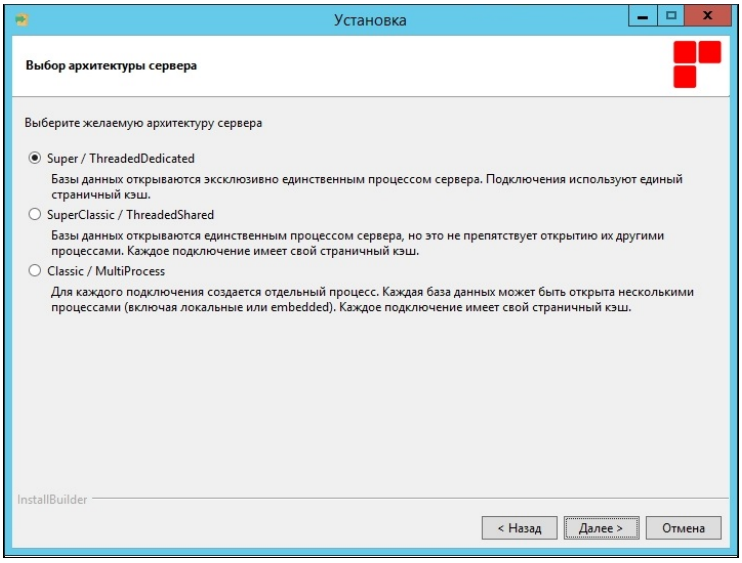
Далее прочтите и примите условия лицензионного соглашения, установив флаг для параметра «**Я принимаю условия соглашения**». Нажмите «**Далее**».



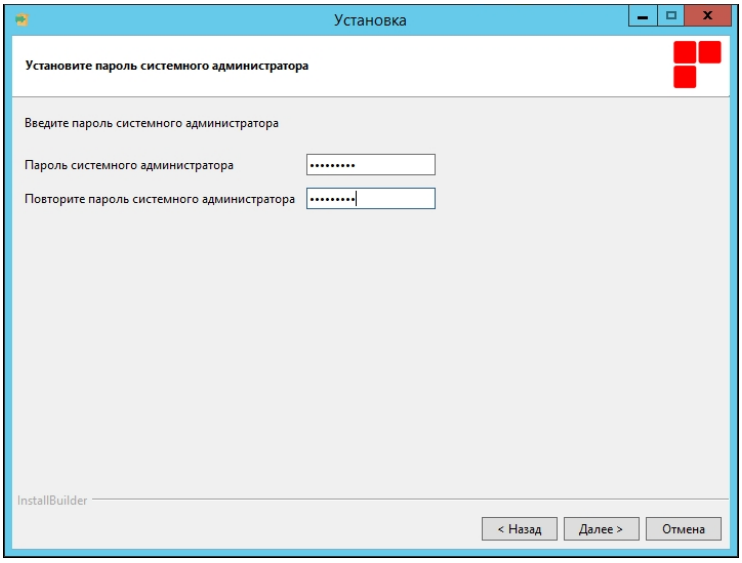
Выберите каталог для установки программы. По умолчанию используется **C:\Program Files\RedDatabase**.



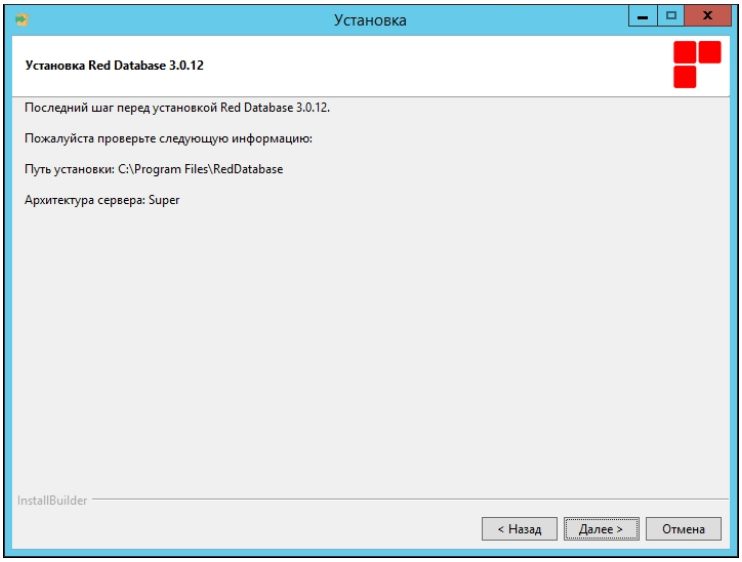
Выберите требуемую архитектуру сервера, установив флаг для соответствующего параметра. Нажмите «**Далее**».



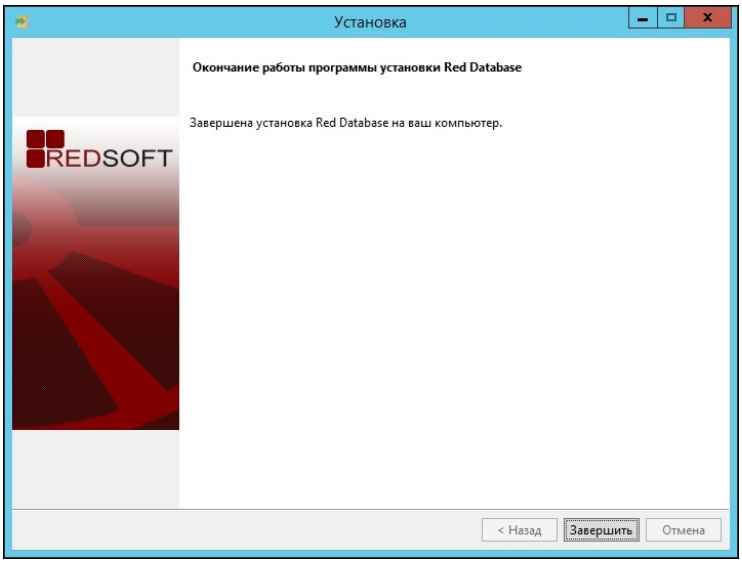
Установите пароль системного администратора. Пароль необходимо повторить для избежания опечаток. Нажмите «**Далее**».



Проверьте указанные ранее параметры. Если все настроено верно, нажмите «**Далее**» для запуска процесса установки. В противном случае нажмите «**Назад**» и внесите изменения в необходимые конфигурации.



После завершения процесса установки будет выведено соответствующее сообщение. Нажмите «**Завершить**».


Установка
Окончание работы программы установки Red Database
Завершена установка Red Database на ваш компьютер.
REDSOFT
< Назад
Завершить
Отмена

Обновление СУБД РЕД База Данных (Открытая редакция)

Скачать актуальную версию СУБД РЕД База Данных можно на официальном сайте компании.

Общий алгоритм обновления выглядит следующим образом:

1. Остановить СУБД Ред База Данных.

2. Проверить отсутствие подключений ко всем файлам баз данных на сервере и отсутствие процессов СУБД.

3. Сделать резервную копию каталога с СУБД (например, переименовав его).

4. Удалить текущую версию СУБД.

5. Выполнить установку новой версии СУБД.

6. Скопировать конфигурационные файлы со старой версии СУБД, дополнительно может потребоваться копирование плагинов (**plugins**) и *java* (**jar**) библиотек, которые не входят в типовой дистрибутив СУБД и устанавливаются и настраиваются отдельно.

Подробнее об обновлении СУБД можно ознакомиться в Руководстве администратора на сайте СУБД.

Диагностика проблем

Наличие мусора
Свободное место на диске
Оперативная память
Нагрузка на процессор
Нагрузка на диск
Таблица блокировок
Активность индексов
Поломка БД
Запрос дополнительной информации для первичной диагностики проблемы при обращении на ЛТП1

Анализ проблем производительности и поломки БД:

- Низкая производительность, симптомы:
  - долгое выполнение запросов;
  - долгое открытие окон в пользовательском интерфейсе;
  - жалобы на работу, вплоть до того, что вообще невозможно подключиться.
- Поломка БД, симптомы:
  - зависание процессов СУБД;
  - аварийное завершение процессов СУБД РБД при выполнении запросов;
  - ошибки в логе **firebird.log**.

Проблема производительности требует анализа на всех уровнях:

- прикладное ПО (толстый клиент, тонкий клиент, сервер приложений);
- сеть (проблемы и ошибки сети, загрузка сети, антивирусы и файерволы);
- гипервизор на сервере (конкуренция с другими ВМ, память, процессор);
- ОС СУБД (постоянное потребление процессора на уровне 100%, очереди к диску, сеть, файловая система);
- проблемы внутри БД (блокировки, мусор, отсутствие индексов, неоптимальные планы).

Все показатели требуется проверять в момент пиковой нагрузки на сервер или зависания и сравнивать с показателями системы, работающей в штатном режиме.

Примеры проведения диагностики проблем

Наличие мусора

Проверку наличия мусора можно осуществить утилитой **gstat**:

```
/opt/RedDatabase/bin/gstat -h /path/to/db.fdb
```

Пример вывода:

```
Database "/opt/db/red.fdb"
Gstat execution time Wed Jun 30 15:53:27 2021

Database header page information:
  Flags        0
  Generation       236121
  System Change Number       24
  Page size       16384
  Server       RedDatabase
  ODS version        12.0
  Oldest transaction       234835
  Oldest active       234836
  Oldest snapshot       234836
  Next transaction       234839
  Sequence number        0
```

```
    Next attachment ID      1604
    Implementation      HW=AMD/Intel/x64 little-endian OS=Linux CC=gcc
    Shadow count      0
    Page buffers      2048
    Next header page      0
    Database dialect      3
    Creation date       Aug 18, 2020 15:08:32
    Attributes      force write

      Variable header data:
    Database backup GUID:     {C45D8AFE-4293-4EEA-B798-F0360284C9D6}
    Sweep interval:     0
    Database GUID:     {A5D296A8-833A-4377-F496-187F6ABB0D5E}
    *END*
Gstat completion time Wed Jun 30 15:53:27 2021
```

Рекомендации:

- Большая разница между **OAT** (Oldest active) и **OIT** (Oldest transaction) — повод для принудительной сборки мусора с помощью команды `gfix -sweep`.
- Большая разница между **Oldest active** и **Next transaction** — долгие транзакции, рекомендуется обратиться к разработчикам прикладного ПО для исключения длинных транзакций. Если такое исключение невозможно, то рекомендуется принудительное завершение таких транзакций (например, каждый день завершать транзакции старше 12-24 часов) и сборка мусора командой `gfix -sweep`.

Свободное место на диске

Проверка наличия свободного места на диске, в том числе в каталоге **/tmp**, производится командой:

```
df -h
```

Рекомендации:

- при отсутствии или недостаточном объеме свободного места необходимо его физическое увеличение либо удаление ненужных файлов.

Оперативная память

Проверка наличия свободной оперативной памяти и занятость **swap** осуществляется командой

```
free -m
```

Использование файла подкачки — плохой признак, который также может быть причиной низкой производительности. Интенсивность использования **swap** можно оценить с помощью утилиты `atop`, см. параметры `swout` и `swin`, их активное изменение говорит о частом использовании **swap**.

Рекомендации:

- проверьте параметры конфигурационного файла **firebird.conf**:
    - `TempBlockSize` — минимальный размер блока сортировки и шаг его расширения (при необходимости). Позволяет несколько ускорить работу алгоритма сортировки за счёт выделения памяти большими блоками. Определение оптимальных для конкретной задачи настроек может быть произведено экспериментальным путем, принимая во внимание размеры файлов сортировки. При наличии больших сортировок рекомендуется увеличить значение параметра (максимально 2147483647 байт).
    - `TempCacheLimit` — для **SuperServer** и **SuperClassic** рекомендуется 64 Мб, для **Classic** = 8 Мб;
    - `TempDirectories` — указываются через точку с запятой, следуют в порядке очереди; пока не заполнится первая директория, вторая будет ожидать. Рекомендуется упорядочить каталоги по скорости доступа.
- Настройте использование **swap**:

Создайте файл **/etc/sysctl.d/ram.conf**:

```
nano /etc/sysctl.d/ram.conf
```

Со следующим содержимым:

```
vm.swappiness = 10
 vm.dirty_ratio = 60
 vm.dirty_background_ratio = 2
 vm.min_free_kbytes = 1048576
```

После сохранения изменений выполните перезагрузку операционной системы.

Нагрузка на процессор

Проверка нагрузки на процессор:

```
top (atop, nmon)
```

Длительная 100% загрузка одного ядра — признак зависания.

Рекомендации:

- принудительно завершите этот процесс (в случае с архитектурой **Classic**), предварительно сняв дамп для передачи на исследование разработчикам, после чего обратитесь в Техническую поддержку;
- выполните команду `gfix -sweep` без активных подключений к БД;
- проверьте активность индексов и выполните пересчет селективности индексов (рекомендуется выполнять минимум 1 раз в неделю в период минимальной нагрузки);
- низкая загрузка процессоров — ожидание блокировки, смотрите таблицу блокировок (см. п. «Таблица блокировок»).
- проверьте трейс, возможно необходимо добавление индекса.

Нагрузка на диск

Проверка нагрузки на диск осуществляется командой:

```
iostat -xz (iostat -p sda -x -t 1)
```

где **sda** - имя исследуемого блочного устройства ввода/вывода.

Важное значение имеет длина очереди к диску `aqu-sz` или `avgqu-sz` (название параметра зависит от версии утилиты) — средний размер очереди запросов к диску.

Рекомендации:

- Проверить опции монтирования для `SSD = noatime,discard` (не рекомендуется использовать опцию монтирования **discard** на программном рейде **mdadm** из **NVME SSD**).
- Необходимо понять, какие запросы выполняют наибольшее количество input/output-операций. В этом помогут таблицы мониторинга (`MON$`) и анализ трейса. Возможно, потребуется создание дополнительного индекса и пересчет селективности индексов (`SET STATISTICS INDEX INDEX_NAME`).

Если на ЭВМ, на котором установлена СУБД РЕД База Данных, используется схема реализации компьютерной памяти **NUMA** (Non-Uniform Memory Access), то работу архитектуры можно проверить с помощью утилиты **numastat**.

В выводе утилиты промахов по памяти (`numa_miss` — сколько раз промахнулись и вынуждены обращаться к памяти другого процессора) должно быть на порядок меньше попаданий (`numa_hit`), в идеале параметр `numa_miss` должен быть равен 0.

Рекомендации:

Если значение `numa_miss` высокое, следует привязать процессы Ред Базы к одному из процессоров (`numactl -C 0 /opt/RedDatabase/bin/rdbserver`), а к другому процессору можно привязать сервер приложений или веб-сервер, если он расположен на том же сервере.

Дополнительно необходимо протестировать производительность дисковой подсистемы с помощью утилиты **fio**:

```
fio fio.conf
```

Пример конфигурационного файла:

```
[ro]
 blocksize=16k
 directory=/mnt/ssd
 rw=randread
 direct=1
 size=15g
 ioengine=psync
 iodepth=5
 runtime=600
 iodepth=5
 ioengine=psync

 [wo]
 blocksize=16k
 directory=/mnt/ssd
 rw=randwrite
 direct=1
 size=15g
 ioengine=psync
 iodepth=5
 runtime=600
 iodepth=5
 ioengine=psync
```

Основные параметры конфигурационного файла:

- блоки `ro` и `wo` (на чтение и на запись) — размер блока 16Кб, можно установить 8Кб, если размер страницы в БД равен 8;
- `directory` — каталог, в котором будет проводиться тестирование;
- `rw-randread` — рандомное чтение/запись;
- `direct=1` — флаг `o_direct`;
- `size=100` — размер файла 100Мб (из этого файла производится рандомное чтение/запись);
- `runtime=60` — время тестирования;
- `iodepth=5` — глубина очереди к диску, которую **fio** выдает в файл;
- `ioengine=psync` — используемые функции чтения/записи, которыми пишет СУБД.

Параметры, на которые необходимо обратить внимание в выводе теста **fio**:

- `IOPS` — количество операций чтения и записи в секунду;
- `lat` — задержка диска, необходимо ориентироваться на среднее (**avg**) значение.

Таблица блокировок

Примеры использования:

- печать всей таблицы:

```
/opt/RedDatabase/bin/rdb_lock_print -a -d /path/to/db > /path/to/lock_table.txt
```

- печать блокировок с очередями

```
/opt/RedDatabase/bin/rdb_lock_print -n -l -o -d /path/to/db > /path/to/lock_table.txt
```

- поиск зависшего процесса

```
/opt/RedDatabase/bin/rdb_lock_print -q 30 -d /path/to/db
```

В выводе `rdb_lock_print -a -d` можно увидеть следующие параметры:

- Length — максимальный размер таблицы блокировок на момент снятия снапшота;
- Used — текущий размер таблицы блокировок;
- Mutex wait — время ожидания мьютексов в процентах;
- Hash slots — ширина хэш-таблицы, которая используется для поиска блокировок. Число должно быть простым, чтобы хэш-алгоритм производил хорошее распределение;
- Hash length (*min*/*avg*/*max*) — длина хэш-таблицы;
- Owners — число соединений к серверу.

Рекомендации:

- Если в пиковые нагрузки в параметре Hash length значения **avg > 3** или **max > 10**, то необходимо увеличивать параметр LockHashSlots (в **firebird.conf**), значение должно быть простым числом (максимум 65521).
- Высокий Mutex wait считается проблемой, нужно проверить селективность индексов и их активность.
- Встречается, что все процессы висят на ожидании одной блокировки. Это можно увидеть по выводу команды:

```
/opt/RedDatabase/bin/rdb_lock_print -c -n -l -o -d | grep "Pending"
```

Максимальное число и покажет проблемную блокировку. По типу и ключу можно попытаться понять, какая это блокировка, страница или другой ресурс. Это позволит предоставить рекомендации прикладному разработчику.

- Повисший процесс, который выдаст rdb_lock_print -q 30, рекомендуется завершить, предварительно сняв дамп.

Активность индексов

Определить неактивные индексы можно запросом:

```
select rdb$index_name from rdb$indices
    where (rdb$system_flag is null or rdb$system_flag = 0)
       and RDB$INDEX_INACTIVE > 0
    order by rdb$foreign_key nulls first
```

Рекомендации:

- активируйте все индексы:

```
EXECUTE BLOCK AS
  DECLARE VARIABLE stmt VARCHAR(1000);
BEGIN
  for select 'ALTER INDEX '||rdb$index_name ||' ACTIVE;'
    from rdb$indices
    where (rdb$system_flag is null or rdb$system_flag = 0)
      and RDB$INDEX_INACTIVE > 0
    order by rdb$foreign_key nulls first
    into :stmt do EXECUTE STATEMENT :stmt;
END
```

- активируйте нужные индексы вручную.

Поломка БД

Поломка БД — это изменения в файле, нарушающие целостность и приводящие к ошибкам.

Основные причины:

- аппаратные (память, диск);
- комплексные (батарейка рейд-контроллера);
- программные (ошибки в коде СУБД).

При поломке БД ошибки могут встречаться как непосредственно при работе пользователей, так и в файле **firebird.log**.

Критические ошибки в файле *firebird.log*:

- internal Firebird consistency check (cannot find tip page);
- Error while trying to read from file;
- Error while trying to write to file;
- internal Firebird consistency check (can't continue after bugcheck);
- internal Firebird consistency check (decompression overran buffer);
- Pointer page (sequence NUM) lost;
- Pointer page (sequence NUM) inconsistent;
- Missing index root page;
- Transaction inventory pages lost;
- Transaction inventory pages confused;
- internal Firebird consistency check (can't continue after bugcheck);
- internal Firebird consistency check (cannot continue after replication failure).

При подозрении на поломку необходимо выполнить проверку файла базы данных через утилиту **gfix**. Для проверки требуется монопольный доступ к базе (при сбоях проверки добавьте ключ -ignore):

```
/opt/RedDatabase/bin/gfix -v -full
```

Если ошибки не обнаружены, вывод команды будет пуст.

При обнаружении ошибок вывод команды будет иметь примерно следующий вид:

```
Summary of validation errors
Number of record level errors : 93
Number of data page errors : 25
Number of index page errors : 29
Number of database page errors : 14
```

Рекомендации:

- выполните проверку:

```
/opt/RedDatabase/bin/gfix -v -full
```

- проверьте лог **firebird.log** на предмет наличия ошибок или отправьте его в службу техподдержки;
- проверьте оборудование (диск, ОЗУ);
- выполните ремонт БД по результатам анализа проверки.

Запрос дополнительной информации для первичной диагностики проблемы при обращении на ЛТП1

Все показатели требуется смотреть в момент пиковой нагрузки на сервер или зависания. Сбор данных необходимо производиться под учетной записью с правами **администратора** (**sudo**). Для диагностики необходимо установить следующие пакеты:

```
sudo dnf install numactl sysstat atop htop fio
```

1. Подробное описание проблемы:

- проблема присутствует постоянно или в определенные моменты;
- снижение производительности — общее или при определенных операциях;
- проводились ли какие-либо работы на сервере (обновление, замена оборудования и пр.).

2. Характеристики оборудования (ОЗУ, ЦПУ, hdd или ssd).

3. Вывод команды:

```
df -h
```

4. Вывод команды:

```
sudo gstat -h /path/to/db.fdb
```

5. Вывод команды:

```
sudo rdb_lock_print -l -n -o -d /path/to/db.fdb
```

6. Вывод команды:

```
sudo rdb_lock_print -q 30 -d /path/to/db
```

7. Вывод утилиты top (atop, htop) для определения нагрузки на ЦПУ.

8. Вывод команды:

```
free -m
```

9. Вывод утилиты numastat (при наличии **NUMA**-архитектуры):

```
numastat
```

10. Вывод утилиты iostat для оценки очереди к диску (выполнение займет ~1 минуту):

```
iostat -xzm -t 1 60 > /tmp/iostat.txt
```

При этом сформируется файл **/tmp/iostat.txt**, который необходимо предоставить.

11. Копия **firebird.log**, **firebird.conf**, **databases.conf** и **replication.conf** (при наличии) из каталога установки СУБД.

12. Копия **/var/log/messages** за интервал наблюдения проблемы и в течение месяца до нее.

13. Копия **/etc/fstab**.

14. Вывод команд:

```
sudo dmesg -T > /tmp/dmesg.txt
```

```
sudo journalctl -p err > /tmp/journalctl.txt
```

При этом создадутся файлы **dmesg.txt** и **journalctl.txt** в каталоге **/tmp**.

15. Проверить активность индексов запросом:

```
select rdb$index_name from rdb$indices
where (rdb$system_flag is null or rdb$system_flag = 0)
and RDB$INDEX_INACTIVE > 0
order by rdb$foreign_key nulls first
```

16. Протестировать производительность дисковой подсистемы, на которой расположена БД. Сделать это можно с помощью утилиты fio:

```
sudo fio /tmp/fio.conf
```

Файл **fio.conf** необходимо создать с помощью любого текстового редактора, например nano:

```
sudo nano /tmp/fio.conf
```

Пример конфигурационного файла:

```
[ro]
 blocksize=16k
 directory=/mnt/ssd
 rw=randread
 direct=1
 size=15g
 ioengine=psync
```

```
iodepth=5
runtime=600
iodepth=5
ioengine=psync

[wo]
blocksize=16k
directory=/mnt/ssd
rw=randwrite
direct=1
size=15g
ioengine=psync
iodepth=5
runtime=600
iodepth=5
ioengine=psync
```

Основные параметры конфигурационного файла:

- блоки `ro` и `wo` (на чтение и на запись) — размер блока 16Кб, можно установить 8Кб, если размер страницы в БД равен 8;
- `directory` — каталог, в котором будет проводиться тестирование;
- `rw-randread` — рандомное чтение/запись;
- `direct=1` — флаг `o_direct`;
- `size=100` — размер файла 100Мб (из этого файла производится рандомное чтение/запись);
- `runtime=60` — время тестирования;
- `iodepth=5` — глубина очереди к диску, которую **fio** выдает в файл;
- `ioengine=psync` — используемые функции чтения/записи, которыми пишет СУБД.

Часто задаваемые вопросы по СУБД РЕД База Данных (FAQ)

Где скачать СУБД РЕД База Данных?

Единственным правильным источником для получения сборки является официальный сайт. Дистрибутивы из остальных источников использовать нежелательно, это может быть потенциально опасным.

Официальный источник (он же официальный сайт) — https://reddatabase.ru/ru/downloads/.

В разделе «Загрузки» можно увидеть все файлы, доступные для скачивания. Необходимо быть зарегистрированным пользователем. При этом, если учетная запись имеет соответствующие допуски, то список доступных для скачивания продуктов шире.

Чтобы релиз-кандидаты были доступны для скачивания, необходимо в своем профиле установить флаг для параметра «Показывать релиз-кандидаты», в этом случае можно видеть свежие версии, которые, вероятно, в последующем станут релизами. Это может потребоваться, если есть подозрения, что в релиз-кандидате была исправлена какая-либо серьезная ошибка. У каждой версии есть описание, можно просмотреть список изменений и исправленных проблем.

Клиентам выдается учетная запись (логин и пароль) с доступом к приобретенным продуктам.

Основные файлы на странице загрузки:

- ***.bin*** *— установочный файл для ОС семейства Linux;*
- **.tar.gz** — архив с файлами СУБД для ОС семейства Linux;
- ***.exe*** *— установочный файл для ОС семейства Windows;*
- **.zip** — архив с файлами СУБД для ОС семейства Windows;
- ***dbg-linux-x86_64.tar.gz** — отладочные символы для СУБД, установленной на ОС семейства Linux;
- ***dbg-windows-x86_64.zip** — отладочные символы для СУБД, установленной на ОС семейства Windows.

Где скачать документацию на СУБД РЕД База Данных?

Документация доступна на официальном сайте СУБД РЕД Базы Данных — https://reddatabase.ru/ru/documentation/.

Документация регулярно обновляется, исправляется и дополняется при обновлении СУБД, поэтому рекомендуется проверять новые версии документации.

Где найти видеоролики по СУБД РЕД Базе Данных?

Обучающие видеоролики доступны на официальных каналах СУБД РЕД База Данных:

- на **RuTube** — https://rutube.ru/channel/29879950/;
- на **Яндекс.Дзен** — https://dzen.ru/reddatabase.

Какие есть информационные ресурсы в Интернете по СУБД РЕД Базе Данных?

СУБД Ред База Данных в **Telegram** — https://t.me/reddatabase.

Канал СУБД Ред База Данных на **RuTube** — https://rutube.ru/channel/29879950/.

Канал СУБД Ред База Данных на **Яндекс.Дзен** — https://dzen.ru/reddatabase.

Список наиболее значительных изменений в новых версиях СУБД РЕД База Данных — https://reddatabase.ru/ru/news/.

Площадка для общения **СУБД РЕД База Данных** и **Firebird** — https://t.me/firebird_reddatabase.

Какую архитектуру СУБД выбрать?

Архитектура **Super** — рекомендована к использованию на версии **3.0.9+**. Имеет общий кеш, в версии **3.0** она стала действительно многопоточной, до этого она не была ориентирована на многоядерные процессоры. Страничный кеш общий, что дает увеличение производительности. Однако при аварийном завершении того самого единственного процесса, аварийно прекращает свою работу весь сервер.

Архитектура **Classic** — классическая архитектура, где каждый коннект происходит в отдельном процессе. Каждый процесс имеет собственный кеш данных, что является более надежным решением, но в то же время, в ряде случаев, показывает производительность ниже, чем архитектура **Super**.

Архитектура **Superclassic** — не рекомендована к использованию, в дальнейшем, возможно, будет изъята из дистрибутива.

Чем отличается текущая версия СУБД от Firebird?

Сравнение версии **3.0** с версией **2.6**, а также с **Firebird 3.0** находится на официальном сайте в разделе «Продукты» — https://reddatabase.ru/ru/comparison/.

Чем отличается одна редакция СУБД от другой?

Основные различия описаны на официальном сайте в разделе «Продукты» — https://reddatabase.ru/ru/editions/.

Как установить СУБД на Linux?

Необходимо предоставить права на выполнение. Далее можно выполнять установку в графическом либо в текстовом режиме.

Для назначения прав выполните команду:

```
sudo chmod a+x /path/to/rdb.bin
```

Для установки в графическом режиме выполните:

```
./rdb.bin
```

Далее следуйте инструкциям установщика.

Для установки в текстовом режиме выполните команду:

```
./rdb.bin --mode text
```

Далее следуйте инструкциям установщика.

В чем заключается типовая настройка СУБД после её установки?

Ключевые параметры конфигурационного файла **firebird.conf** для временных файлов:

- **TempTableDirectories** — это каталог, в котором будут создаваться файлы временных таблиц, сейчас они создаются в каталоге **/tmp**.
- **TempDirectories** — список временных каталогов для сортировок, временных таблиц и т. п., разделяются точкой с запятой (;), используются по порядку. При отсутствии параметра используются переменные окружения `FIREBIRD_TMP`, `TEMP`, `TMP`, поэтому в **systemd** необходимо прописать параметр `FIREBIRD_TMP`. Рекомендуется упорядочить каталоги по скорости доступа, сначала оперативная помять, затем **ssd**, затем **hdd**. Если оперативной памяти в избытке, первым можно указать каталог, смонтированный в ОЗУ. Рекомендуется временные каталоги размещать в разделах, отличных от размещения БД. После настройки необходимо следить за состоянием этих каталогов для своевременного исправления возникающих проблем. Пример:

  ```
  TempDirectories = /var/tmp;/mnt/ssd;/mnt/hdd_tmp
  ```

- **TempCacheLimit** — используется для ограничения объёма временного пространства, которое может быть кешировано в оперативной памяти. В этом пространстве будут сохраняться данные сортировок, буферов записи, небольших временных блобов перед материализацией и т.д. В целях увеличения производительности, желательно установить это значение больше длины временных файлов в каталогах **TempDirectories**, если это позволяет объем доступной оперативной памяти.

Ключевые параметры конфигурационного файла **firebird.conf** для кеширования:

- **DefaultDbCachePages** — количество страниц одной базы данных, находящихся в кеш-памяти одновременно. Супер-сервер использует единый кеш (по умолчанию 2048 страниц), т. е. `DefaultDbCachePages` общий для всех подключений. В архитектуре **Classic** используется свой кеш на каждый процесс, поэтому в архитектуре **Super** значение необходимо устанавливать больше. Измеряется в количестве страниц, поэтому от размера 1 страницы будет зависеть размер памяти, которая будет задействована под кеш.

  Предполагается использовать четверть ОЗУ для нужд кеша СУБД.

  Значение кеша задается параметром `page buffer` (см. вывод `gstat -h`) для каждой БД в отдельности, либо значением

DefaultDbCachePages из конфигурационного файла **firebird.conf** для всего сервера, либо параметром DefaultDbCachePages в конфигурационном файле **databases.conf**.

В приоритете - параметр page buffer, если page buffer = 0, то значение берется из конфигурационных файлов.

Архитектура **Super**:

```
MemorySize/(4*PageSize)
```

Архитектура **Classic**:

```
MemorySize/(4*ConnNum*PageSize)
```

Настройку можно уточнять по итогу мониторинга сервера: учесть объемы для сортировки, файловый кеш, ядро ОС, другие приложения. Самый важный параметр, на который стоит обратить внимание — это количество чтений (Read) страниц и количество Fetch страниц. **Fetch** — страница берется из кеша (из памяти), если в кеше её нет, то она читается с диска (что замедляет скорость работы). Чем ближе эти значения (write и cache) друг к другу, тем хуже. В идеально прогретом кеше чтений почти не будет, будет только запись — это в архитектуре "супер". В классике кеш у коннектов разный, поэтому чтений там больше. Это связано с необходимостью записи страниц.

- **FileSystemCacheThreshold** — если значение указано больше, чем в **DefaultDBCachePages**, то включается использование файлового кэша. Если значение меньше — отключается. Предопределённых рекомендаций не существует. Подбор оптимального значения параметра зависит от диска и нагрузки, поэтому необходимо наблюдать за использованием диска и подбирать оптимальное значение. Для **Classic** оптимальный параметр обязателен, для **Super** менее критичен.

Далее перечислены ключевые параметры, касающиеся авторизации:

- **AuthServer и AuthClient** — набор методов аутентификации, разрешенных на сервере и клиенте:
  - Безопасная парольная (Srp) аутентификация;
  - Традиционная (Legacy_Auth) аутентификация;
  - Доверительная (Win_Sspi) аутентификация для ОС Windows;
  - Многофакторная (Multifactor) аутентификация с применением политик безопасности;
  - Доверенная аутентификация через механизм GSSAPI (Gss)

- **UserManager** — плагин для работы с базой данных пользователей:
  - Srp;
  - Legacy_UserManager;
  - Multifactor_Manager.
  - Используется первый плагин из списка

- **DefaultUserManagers** — набор стандартных плагинов, в которых по умолчанию будет создаваться пользователь или менятся пароль у пользователя.

Прочие важные параметры **firebird.conf**:

- **ServerMode** — режим работы сервера (**Super**, **Classic**, **SuperClassic**), требуется перезапуск при изменении, при смене режима необходимо корректировать параметр кеша.
- **RemoteBindAddress** — позволяет привязать входящие соединения к определенному сетевому интерфейсу. При этом все входящие соединения через другие сетевые интерфейсы будут запрещены.
- **LockAcquireSpins** — количество попыток, которые будут сделаны в условном режиме захвата мьютекса таблицы блокировок. Этот параметр позволяет, вместо обращения к ядру, ждать некую атомарную переменную, что уменьшает количество тактов процессора на межпроцессорные вызовы.
- **LockHashSlots** — число слотов хэширования блокировок. Следует увеличивать если под нагрузкой в таблице блокировок много коллизий. См. позднее rdb_lock_print -d <database> | <alias> и Hash lengths. Как правило выставляется по максимуму, из опыта.

+ В чем заключается типовая настройка сервера после установки СУБД?

Для увеличения допустимого числа процессов СУБД и доступных им ресурсов:

- в **/etc/security/limits.conf** лимиты nproc и nofile для пользователя, от имени которого запускается СУБД (firebird), устанавливаются в 10000;
- параметр ядра vm.max_map_count необходимо увеличить до **256000**, написав в **/etc/sysctl.conf** строку:

  ```
  vm.max_map_count=256000
  ```

  Для немедленного применения настройки необходимо выполнить:

  ```
  sysctl -p
  ```

- для systemd-систем в **/usr/lib/systemd/firebird.service** пропишите:

```
Environment = FIREBIRD_TMP=/path/to/tmp
```

- При наличии достаточного объема **RAM** можно смонтировать в память временный каталог, куда сервер будет выгружать файлы. Для этого в **/etc/fstab** необходимо строку:

```
tmpfs /tmp tmpfs size=32G 0 0
```

  где **32G** — максимальный размер, до которого может расшириться временный каталог в памяти;
- отключить transparent Huge Pages, например, записав в **/etc/rc.local**:

```
echo never > /sys/kernel/mm/redhat_transparent_hugepage/enabled
```

Как понять, какая редакция СУБД Ред База данных у меня установлена?

Необходимо изучить содержимое каталога установки СУБД.

Актуально для **3.0+**:

- если есть **replication.conf** — это промышленная редакция;
- если его нет, но есть **jvm.args** — это стандартная редакция;
- иначе открытая.

Если есть возможность подключиться к любой БД на сервере, то редакцию можно определить, выполнив запрос:

```
select rdb$get_context('SYSTEM', 'EDITION') from rdb$database;
```

Как узнать установленную версию СУБД?

Для определения установленной версии СУБД можно воспользоваться утилитой **gfix** с ключом **-z**, например:

```
/opt/RedDatabase/bin/gfix -z
```

Пример вывода команды:

```
gfix version LI-V3.0.15.0 RedDatabase 3.0 rc.1 (8352144a3ce2165e0f798503c7af1b9d4f7279e1)
```

где **LI-V3.0.15.0 RedDatabase 3.0 rc.1** — версия СУБД.

Как обновить СУБД на Linux (минорное обновление)?

Для обновления СУБД на Linux необходимо:

- остановить СУБД и проверить статус службы командой:

```
sudo systemctl stop firebird
systemctl status firebird
```

- Закомментировать алиас в **databases.conf** и через **isql** проверить, что к БД нет подключений:

```
select count(*) from mon$attachments;
exit;
```

- Проверить, что БД никто не использует утилитой **lsof** (от **root** или **sudo**), не должны выводиться pid'ы процессов:

```
sudo lsof /path/to/db.fdb
sudo lsof /opt/RedDatabase/security3.fdb
```

- Переименовать **/opt/RedDatabase** в **/opt/RedDatabase_<старая_версия>**. Старую версию можно узнать например с помощью утилиты **gbak**:

```
/opt/RedDatabase/bin/gbak -z
```

Переименование:

```
sudo mv /opt/RedDatabase /opt/RedDatabase_3.0.5.116
```

- установить новую версию СУБД, используя установочный бинарный файл, для этого назначить необходимые права:

```
sudo chmod a+x /path/to/rdb.bin
```

и запустить установку:

```
./rdb.bin
```

- Из каталога со старой версией СУБД скопировать в новый каталог необходимые конфигурации (**directories.conf**, **databases.conf**, **firebird.conf**, **fbtrace_sec.conf**, **fbtrace_dba.conf**, **replication.conf**, **fbjava.yaml**), дополнительные плагины (если такие имеются) и базы данных безопасности (**security3.fdb**, **java-security.fdb**);
- раскомментировать алиас базы в **databases.conf**:
- запустить РЕД Базу Данных и проверить статус службы (должно быть **active (running)**);

```
sudo systemctl start firebird
systemctl status firebird
```

- проверить успешность подключения к базе по сетевому протоколу через **isql** (полный путь до файла БД):

```
/opt/RedDatabase/bin/isql -u sysdba -p masterkey localhost:alias
```

Как проверить БД на наличие ошибок?

Проверить БД на наличие ошибок можно утилитой **gfix**, требуется монопольный доступ к БД:

```
/opt/RedDatabase/bin/gfix -v -full /path/to/database.fdb
```

gfix может попытаться исправить некоторые некритичные ошибки. Для отмены исправления некритичных ошибок необходимо добавить ключ `-n`:

```
/opt/RedDatabase/bin/gfix -v -full -n /path/to/database.fdb
```

Какие ошибки можно считать критичными при проверке?

Все ошибки файла БД после проверки фиксируются в логе **/opt/RedDatabase/firebird.log**. Список наиболее критичных из них:

- `internal Firebird consistency check (cannot find tip page)` — нарушение некоторой целостности, например, не получается найти страницу, на которой отмечен статус транзакции, или находится не та страница;
- `Error while trying to {read from, write to} file` — не может прочитать/записать файл БД;
- `internal Firebird consistency check (decompression overran buffer)` — например, при декомпрессии какой-либо записи обнаруживается, что она превышает размер положенного буфера;
- `Pointer page (sequence NUM) {lost, inconsistent}` — потеряна страница указателей;
- `Missing index root page` — потеря **root page** для индекса;
- `Transaction inventory pages lost` — потерянная страница транзакций;
- `internal Firebird consistency check (cannot continue after replication failure)`.

В чем заключается типовой ремонт базы данных?

Типовой ремонт заключается в процедуре резервного копирования (`gbak -b -v -g`) и восстановления (`gbak -c -v -o`) поврежденной базы данных.

Ни в коем случае нельзя удалять поврежденную БД до полного завершения ремонта.

Что делать с ошибкой invalid request BLR при восстановлении резервной копии?

В данном случае можно попробовать перекомпилировать проблемные процедуры и еще раз сделать резервную копию. Если используется СУБД 3.0 и выше, восстановить такую резервную копию можно с ключом `-ig`, который восстановит процедуру с пустым **BLR**. Далее её необходимо перекомпилировать из исходников.

Что делать, если процесс создания резервной копии или процесс ее восстановления аварийно завершается при прохождении данных из определенной таблицы?

В данном случае БД можно восстановить с пропуском данных проблемной таблицы (или нескольких таблиц). Для этого используется ключ `-skip_d`. Пример команды:

```
/opt/RedDatabase/bin/gbak -user SYSDBA -pas masterkey -b -v -g -skip_d '(TABLE_NAME_1|TABLE_NAME_2)' /path/to/database.fdb
/path/to/backup.fbk -y /path/to/backup.log
```

При этом нужно помнить, что деактивируются внешние ключи, которые касаются таблиц с пропущенными данными. После восстановления БД таким способом необходимо загрузить недостающие данные и активировать вручную внешние ключи.

Как проверить наличие мусора в БД?

Утилитой `gstat` с ключом `-h`:

```
/opt/RedDatabase/bin/gstat -h /path/to/database.fdb
```

В выводе нужно обратить внимание на маркеры:

```
Oldest transaction, Oldest active, Oldest snapshot, Next transaction.
```

Разница между `Oldest transaction` и `Oldest snapshot` должна стремиться к единице. Однако зачастую разница этих параметров достигает больших значений, что негативно влияет на производительность. Для решения данной проблемы рекомендуется регулярная (ежедневная) сборка мусора.

Как принудительно собрать мусор в БД?

Принудительный сбор мусора в БД производится утилитой `gfix`:

```
/opt/RedDatabase/bin/gfix -sweep /path/to/database.fdb
```

Как сделать резервную копию базы данных?

Утилитой `gbak`, стандартная команда выглядит следующим образом:

```
/opt/RedDatabase/bin/gbak -user SYSDBA -pas masterkey -b -v -g /path/to/database.fdb /path/to/backup.fbk -y /path/to/backup.log
```

Для того чтобы убедиться, что процесс создания резервного копирования успешно завершился, необходимо проверить его лог, формирование которого определяется ключом `-y` (см. команду создания резервной копии) — **/path/to/backup.log**. При успешном завершении лог заканчивается следующими строками:

```
gbak:writing names mapping
gbak:closing file, committing, and finishing. 82432 bytes written
gbak:stopped at Mon Aug 22 11:37:08 2022
```

При аварийном завершении или наличии ошибок следует разбираться в проблеме предметно.

Как восстановить резервную копию БД?

Восстановление резервной копии БД производится утилитой `gbak`. Стандартная команда выглядит следующим образом:

```
/opt/RedDatabase/bin/gbak -user SYSDBA -pas masterkey -c -v -o /path/to/backup.fbk /path/to/database.fdb -y /path/to/restore.log
```

При необходимости нужно использовать ключ `-ig` — при ошибках с восстановлением **BLR** хранимых процедур и функций процесс создания резервной копии продолжается, при этом в логе останется запись о пропуске **BLR**.

Для того чтобы убедиться, что восстановление резервной копии успешно завершено, следует проверить его лог, формирование которого определяется ключом `-y` (см. команду восстановления резервной копии) — **/path/to/restore.log**.

При успешном завершении лог заканчивается следующими строками:

```
gbak:fixing views dbkey length
gbak:updating ownership of packages, procedures and tables
gbak:adding missing privileges
gbak:adjusting system generators
gbak:finishing, closing, and going home
gbak:adjusting the ONLINE and FORCED WRITES flags
gbak:stopped at Mon Aug 22 11:52:21 2022
```

БД переводится в ONLINE-режим.

При аварийном завершении или наличии ошибок следует разбираться в проблеме предметно.

Как установить на сервер отладочные символы для РЕД Базы данных и для чего они нужны?

Отладочные символы — специальные данные о связи адресов и исходных кодов, некие описания разных переменных, какая инструкция к какой строке кода относится. Нужны для анализа зависаний и получения стеков, чтобы разработчик смог посмотреть работу процесса в виде текстовой информации, которую он видит у себя в процессе разработки.

Для установки необходимо скачать нужный архив с официального сайта. В названии архива присутствует обозначение **dbg** и версия отладочных символов, например, **RedDatabase-3.0.9-dbg-linux-x86_64.tar.gz**.

ВАЖНО!

Версия СУБД и версия символов должны строго совпадать.

Далее архив необходимо распаковать в нужное место. Для этого:

- перейдите в **mc**;
- перейдите в папку с отладочными символами;
- откройте архив как обычную директорию;
- в подкаталогах из архива существуют скрытые папки **debug**, в которых как раз и находятся все отладочные символы. Скопируйте все каталоги из архива в директорию **RedDatabase** (каждый каталог из архива в соответствующий ему каталог в /opt/RedDatabase).

На этом установка закончена.

Как настроить сбор дампов на Linux?

Необходимо использовать **systemd-coredump** для автоматического сбора дампов:

https://redos.red-soft.ru/base/manual/utilites/coredump/?sphrase_id=285533

Что такое репликация и как её настроить?

Репликация — непрерывное копирование (реплицирование) данных (изменений этих данных) с одного сервера (*master*) на один или несколько других (*slave*, реплика, зеркало).

В СУБД Ред База Данных реализовано два вида логической репликации:

- **Синхронная** — обеспечивает прямое подключение к *slave* и отправку изменений на него непосредственно до коммита транзакции;
- **Асинхронная** — предполагает запись в промежуточный журнал, который передается на зеркало и там применяется.

Примеры настройки репликации описаны Руководстве администратора в подразделе "Настройка системы репликации".

Как проверить работу асинхронной репликации?

Утилита **rdblogmgr** – запускать на мастере:

```
sudo rdblogmgr -u sysdba -p masterkey -d /db/replicated.fdb
```

В выводе можно увидеть следующие параметры:

- *current sequence* – текущий сегмент;
- *last modified* – последнее изменение;
- *total log size* – всего в логе байт в 1 сегменте;
- *free segments* – свободных сегментов 1, полных сегментов 0, архивных 0.

Пример вывода:

```
Log status:

  Current sequence: 8
  Last modified: 2023-12-13 16:48:19
  Total log size: 946259 bytes in 2 segments
  Free segments: 2, full segments: 0, archived segments: 0
```

Утилита **rdbreplmgr** – запускать на зеркале с ключом `-s`:

```
sudo rdbreplmgr -u sysdba -p masterkey /db/replica.fdb -s
```

В выводе команды можно увидеть:

- *Control file* — контрольный файл, содержит текущие счетчики пролитых логов, сколько осталось, сколько активных транзакций (бывает так, что в одном сегменте транзакция стартует, а в другом завершается, и в итоге сегмент можно удалить, когда все транзакции в нем завершены), при переинициализации его нужно удалять;
- *Current segment* — количество обработанных сегментов, должно постоянно расти;
- *Oldest segment* — количество старых сегментов, должно быть в значении **absent**;
- *Oldest segment* — в идеале **absent**;
- Total segments in the queue — количество сегментов в очереди на обработку, в идеале должно стремиться к 0.

Пример вывода:

```
Status for replica /opt/db/red.fdb:
Master database: 192.168.1.10:/opt/db/red.fdb
Master GUID: {71615D98-0551-48D3-EE94-9441AFF3FE04}
Archive directory: /mnt/repl/logsrdb/arch/
Control file: /mnt/repl/logsrdb/arch/{71615D98-0551-48D3-EE94-9441AFF3FE04}
Current segment: 16 (as of 2020-06-17 09:36:35)
Oldest segment: absent
Total segments in the queue: 1
```

Почему при использовании репликации важно наличие первичных ключей в таблице?

Если на мастере создали таблицу без первичного ключа и уникального индекса, то репликационные журналы перестают вливаться на зеркале, при этом отображается ошибка вида:

```
my-server (slave) Tue Dec 22 11:24:35 2020
Database: /path/to/database.fdb
ERROR: Table MY_TABLE has no unique key
```

В конфигурационном файле **replication.conf** на мастере необходимо прописать параметр `exclude_without_pk = true`, при этом таблицы без первичного ключа не будут реплицироваться на базу зеркала.

Что такое трейс и как его запустить?

Трейс (аудит) — инструмент для аудита событий, происходящих внутри БД, позволяет просматривать:

- подключения (отключения) к БД;
- все стадии выполнения запросов, включая счетчики производительности;
- события безопасности;
- работа со службами;
- выполнение хранимых процедур, функций и триггеров;
- работа транзакций, параметры транзакций и многое другое.

Информации может быть много, поэтому в конфигурационном файле доступны различные фильтры (например, по подключению или по времени). Аудит можно сделать на уровне сервера (системный), а можно открыть интерактивную сессию аудита.

- системный аудит — запуск происходит с помощью раскомментирования и изменения параметра `enabled` в конфигурационном файле **fbtrace.conf** — `enabled = true`;
- интерактивный сеанс аудита — запуск происходит с помощью утилиты **rdbtracemgr** и заранее подготовленного конфигурационного файла.

```
rdbtracemgr <параметры_подключения> <действия> [<параметры>]
```

Пример команды:

```
/opt/RedDatabase/bin/rdbtracemgr -SE service_mgr -START -NAME my_trace -CONFIG my_cfg.txt
```

Как найти неактивные индексы?

Для этого необходимо подключиться к базе данных и выполнить SQL-запрос в любом менеджере БД:

```
select rdb$index_name from rdb$indices where (rdb$system_flag is null or rdb$system_flag = 0) and RDB$INDEX_INACTIVE > 0;
```

Как активировать все неактивные индексы?

С помощью SQL-запроса в любом менеджере БД:

```
EXECUTE BLOCK AS
DECLARE VARIABLE stmt VARCHAR (1000);
BEGIN
for select 'ALTER INDEX '||rdb$index_name ||' ACTIVE;'
from rdb$indices
where (rdb$system_flag is null or rdb$system_flag = 0)
and RDB$INDEX_INACTIVE > 0
order by rdb$foreign_key nulls first
into :stmt do EXECUTE STATEMENT :stmt;
END
```

Как получить структуру индексов определенной таблицы?

С помощью SQL-запроса в любом менеджере БД:

```
SELECT S.RDB$INDEX_NAME, S.RDB$FIELD_NAME FROM RDB$INDICES I NATURAL JOIN RDB$INDEX_SEGMENTS S WHERE
I.RDB$RELATION_NAME='MYTABLE' ORDER BY S.RDB$FIELD_POSITION
```

где вместо 'MYTABLE' необходимо указать имя нужной таблицы.

Как получить список ролей или пользователей, которые имеют права на вставку в таблицу?

С помощью SQL-запроса в любом менеджере БД:

```
SELECT RDB$USER FROM RDB$USER_PRIVILEGES WHERE RDB$RELATION_NAME='COUNTRY' AND RDB$PRIVILEGE='I' AND
RDB$USER_TYPE=13 AND RDB$OBJECT_TYPE=0
```

Как найти все подключения старше суток?

С помощью SQL-запроса в любом менеджере БД:

```
SELECT MON$ATTACHMENT_ID FROM MON$ATTACHMENTS
WHERE DATEDIFF (HOUR, MON$TIMESTAMP, CURRENT_TIMESTAMP) > 24
```

Для их принудительного завершения:

```
DELETE FROM MON$ATTACHMENTS
WHERE DATEDIFF (HOUR, MON$TIMESTAMP, CURRENT_TIMESTAMP) > 24
```

Как принудительно завершить подключения с транзакциями старше суток?

С помощью SQL-запроса в любом менеджере БД:

```
DELETE FROM MON$ATTACHMENTS
WHERE MON$ATTACHMENT_ID IN (
SELECT MON$ATTACHMENT_ID FROM MON$TRANSACTIONS
WHERE DATEDIFF (HOUR, MON$TIMESTAMP, CURRENT_TIMESTAMP) > 24)
```

Как принудительно завершить соединения с запросами старше суток?

С помощью SQL-запроса в любом менеджере БД:

```
DELETE FROM MON$ATTACHMENTS
WHERE MON$ATTACHMENT_ID IN (
SELECT MON$ATTACHMENT_ID FROM MON$STATEMENTS
WHERE DATEDIFF (HOUR, MON$TIMESTAMP, CURRENT_TIMESTAMP) > 24)
```

Как найти самые читающие с диска запросы?

С помощью SQL-запроса в любом менеджере БД:

```
SELECT MON$SQL_TEXT FROM MON$STATEMENTS
WHERE MON$STAT_ID = (SELECT FIRST 1 MON$STAT_ID FROM MON$IO_STATS WHERE MON$STAT_GROUP=3 ORDER BY
MON$PAGE_READS DESC)
```

Для их завершения:

```
DELETE FROM MON$ATTACHMENTS
WHERE MON$STAT_ID = (SELECT FIRST 1 MON$STAT_ID FROM MON$IO_STATS WHERE MON$STAT_GROUP=1 ORDER BY
MON$PAGE_READS DESC)
MON$RECORD_STATS
```

Как найти запросы, которые потребляют больше всего памяти?

С помощью SQL-запроса в любом менеджере БД:

```
SELECT MON$SQL_TEXT FROM MON$STATEMENTS
WHERE MON$STAT_ID = (SELECT FIRST 1 MON$STAT_ID FROM MON$MEMORY_USAGE WHERE MON$STAT_GROUP=3 ORDER BY
MON$MEMORY_USED DESC)
```

Как найти клиентские подключения, которые потребляют больше всего памяти?

С помощью SQL-запроса в любом менеджере БД:

```
SELECT MON$REMOTE_ADDRESS, MON$REMOTE_PROCESS
FROM MON$ATTACHMENTS
WHERE MON$STAT_ID = (SELECT FIRST 1 MON$STAT_ID FROM MON$MEMORY_USAGE WHERE MON$STAT_GROUP=1 ORDER BY MON$MEMORY_USED DESC)
```

Какие утилиты доступны "из коробки" для работы с файлом базы данных?

Для этих целей можно использовать утилиту isql. С помощью нее можно создавать базу данных, подключаться и выполнять SQL-запросы в базе данных.

Доступна в любой редакции СУБД, входит в состав дистрибутива.

ISQL — это утилита командной строки для работы с базами данных РЕД Базы Данных при помощи языка структурированных запросов (Structured Query Language — SQL).

Пример команды для подключения:

```
/opt/RedDatabase/bin/isql -u sysdba -p masterkey localhost:employee
```

где:

- *sysdba* — имя пользователя, от которого подключаемся к БД;
- *masterkey* — пароль этого пользователя;
- *employee* — алиас базы данных.

Подробное описание возможностей данной утилиты доступно в Руководстве администратора в разделе «**Утилита ISQL**».

Почему нужно следить за наличием свободного места на разделе с базой данных?

Нехватка места на разделе с базой данных чревата поломкой самой базы, поэтому рекомендуется на разделе иметь хотя бы 30% свободного места (минимум 10%). При этом в логе могут появляться ошибки вида:

```
my.server.local (master) Sun Sep 20 04:43:29 2020
Database: /path/to/database.fdb
ERROR: Log file /path/to/repl/logs/database.fdb.log-142 write failed (error 28)
my.server.local (master) Sun Sep 20 04:43:29 2020
Database: /path/to/database.fdb
WARNING: Slave is to be detached after error. Replica may become inconsistent at this point.
```

Что нужно отслеживать на сервере СУБД?

1. Наличие мусора и выполнение регулярной сборки мусора.

2. Наличие свободного места в ключевых разделах:

   - раздел с БД;
   - в корневом разделе;
   - в разделе с установленой СУБД;
   - наличие свободного места в каталоге **/tmp**.

3. Загрузку ОЗУ (параметр available в выводе free -m).

4. Лог **firebird.log** (сообщения об ошибках, остановках сервиса).

5. Системный лог (сообщения об аварийном завершении).

6. Проверка лога создания резервной копии и тестового восстановления резервной копии.

7. Поверка наличия долгих транзакций.

Как посмотреть размер объектов в БД?

Для проверки размера объектов в БД необходимо собрать статистику по файлу базы данных с помощью команды:

```
/opt/RedDatabase/bin/gstat -user sysdba -password masterkey -a -r -s my_database.fdb > /home/user/Загрузки/full_gstat.txt
```

По окончании выполнения команды будет сформирован файл **/home/user/Загрузки/full_gstat.txt**, используемый далее для подсчета размера объектов.

Пример вывода статистики:

```
Database "/databases/my_base.fdb"
Gstat execution time Fri Dec 22 11:15:11 2023

Database header page information:
        Flags                   0
        Generation              164
        System Change Number    0
        Page size               8192
        Server                  RedDatabase
        ODS version             12.3
        Oldest transaction      126
        Oldest active           127
        Oldest snapshot         127
        Next transaction        127
        Autosweep gap           1
        Sequence number         0
        Next attachment ID      27
        Implementation          HW=AMD/Intel/x64 little-endian OS=Linux CC=gcc
        Shadow count            0
        Page buffers            0
        Next header page        0
        Database dialect        3
        Creation date           Dec 22, 2023 10:36:15
        Attributes              force write

    Variable header data:
        Sweep interval:         20000
        Database GUID:  {EA77BD7A-868B-4459-F5A2-3E578634467F}
        *END*

...
DOCUMENT (132)
    Primary pointer page: 204, Index root page: 205
    Total formats: 1, used formats: 1
    Average record length: 524.10, total records: 1000000
    Average version length: 0.00, total versions: 0, max versions: 0
    Average fragment length: 0.00, total fragments: 0, max fragments: 0
    Average unpacked length: 1010.00, compression ratio: 1.93
    Pointer pages: 45, data page slots: 72056
    Data pages: 72056, average fill: 92%    Primary pages: 72056, secondary pages: 0, swept pages: 0
    Empty pages: 3, full pages: 72052
    Fill distribution:
        0 - 19% = 3
        20 - 39% = 0
        40 - 59% = 0
        60 - 79% = 0
        80 - 99% = 72053
```

Для определения размера таблицы в выводе следует обратить внимание на параметр Data pages, затем умножить количество Data pages нужной таблицы на размер страницы базы данных (размер страницы определяется параметром Page size из заголовка базы данных). В результате будет получен размер данных таблицы в байтах без учета блобов и индексов.

Например, таблица **DOCUMENT** по статистике имеет **72056 страниц**, размер одной страницы — **8192 Б**. Размер таблицы равен 72056 x 8192 = ~563 МБ, среднее заполнение 92%.

Размер блобов

Для определения размера блобов в выводе следует обратить внимание на строку Blobs, содержащую значение параметра total length. Если в таблице есть блобы, то в статистике таблицы будет присутствовать следующая строка:

```
Blobs: 1289124, total length: 12577030488, blob pages: 863868
```

Здесь параметр total length равен **12577030488** — т.е. примерно 11,7 ГБ.

Размер индексов

Для определения размера индексов следует обратить внимание на значение параметра leaf buckets, затем умножить значение параметра leaf buckets на размер страницы базы данных (размер страницы определяется параметром Page size из заголовка базы данных). В результате будет получен размер индекса. Например:

```
Index RDB$PRIMARY27 (0)
    Root page: 72963, depth: 3, leaf buckets: 1205, nodes: 1000000
      Average node length: 9.71, total dup: 0, max dup: 0
      Average key length: 6.72, compression ratio: 1.00
      Average prefix length: 3.01, average data length: 3.74
      Clustering factor: 999982, ratio: 1.00
      Fill distribution:
         0 - 19% = 1
        20 - 39% = 0
        40 - 59% = 0
        60 - 79% = 0
        80 - 99% = 1204
```

Здесь параметр leaf buckets имеет размер **1205 страниц**, размер одной страницы (из статистики) — **8192 Б**. Размер индекса равен 1205 x 8192 = ~9,4 МБ.